令和8年6月10日　　支担官第１２２号

支出負担行為担当官
防衛省大臣官房会計課
会計管理官　平下　一三
（公　印　省　略）

公　　告

下記により入札を実施するので、入札心得及び契約条項等を了承の上、参加されたい。

記

１．入札に付する事項

調達番号	件名	内容	履行場所	履行期限
R8-K4-0005	防衛省ＯＡシステム基盤運用管理役務	仕様書のとおり	仕様書のとおり	自：契約締結日 至：令和１２年３月３１日

２．入札方式　　一般競争入札（総合評価落札方式、電子調達システム（政府電子調達（ＧＥＰＳ））対象案件）

３．入札日時　　令和８年７月３１日(金)　（１０：３０）

４．入札場所　　防衛省市ヶ谷庁舎Ｅ２棟３階入札室

５．参加資格　（１）予算決算及び会計令第７０条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。
（２）予算決算及び会計令第７１条の規定に該当しない者であること。
（３）令和07・08・09年度防衛省競争参加資格（全省庁統一資格）「役務の提供等」のＣ等級以上に格付けされ、関東・甲信越地域の競争参加資格を有するもの。
（４）防衛省から「装備品等及び役務の調達に係る指名停止等の要領」に基づく指名停止の措置を受けている期間中の者でないこと。
（５）前号により、現に指名停止を受けている者と資本関係又は人的関係のある者であって、当該者と同種の物品の売買又は製造若しくは役務請負について防衛省と契約を行おうとする者でないこと。
（６）上記（３）の等級かかわらず、防衛省所管契約事務取扱細則（平成１８年防衛庁訓令第１０８号）第１８条第４項各号のいずれかに該当する者（具体的には、以下ア～キのいずれかに該当する者）であること。なお、要件に該当する者で入札に参加しようとするものについては、　令和８年６月２３日（火）　１２：００　までに下記ア～キに記載する書類等を防衛省大臣官房会計課契約係へ提出すること。

ア　当該入札に係る物品と同等以上の仕様の物品を製造した実績等を証明できる者

イ　資格審査の統一基準により算定された総合審査数値に以下の技術力の評価の数値を加算した場合に、当該入札に係る等級に相当する数値となる者

項　目	基　準	数　値
入札物品等（訓令第１８条第４項に規定する契約の対象となる物品又は役務をいう。以下同じ）に関連する特許保有件数	３件以上 ２件 １件	15 10 5
入札物品の製造等（訓令第１８条第４項に規定する契約の対象となる物品の製造又は役務の提供等をいう。以下同じ）に携わる技術士資格保有者数	９人以上 ７～８人 ５～６人 ３～４人 １～２人	15 12 9 6 3
入札物品の製造等に携わる技能認定者数（特級、一級、単一級）	11人以上 ９～10人 ７～８人 ５～６人 ３～４人 １～２人	6 5 4 3 2 1

注：１　特許には、海外で取得したものを含む。
２　技術士には、技術士と同等以上の科学技術に関する外国の資格のうち文部科学省令で定めるものを有する者であって、技術士の業務を行うのに必要な相当の知識及び能力を有すると文部科学大臣が認めたものを含む。

ウ　ＳＢＩＲ制度の特定新技術補助金等の交付先中小企業者等であり、当該入札に係る物品又は役務に関する分野における技術力を証明できる者

エ　株式会社産業革新投資機構、独立行政法人中小企業基盤整備機構、株式　会社地域経済活性化支援機構、株式会社農林漁業成長産業化支援機構、株式会社民間資金等活用事業推進機構、官民イノベーションプログラム、株式会社海外需要開拓支援機構、一般社団法人環境不動産普及促進機構における耐震・環境不動産形成促進事業、株式会社日本政策投資銀行における特定投資業務、株式会社海外交通・都市開発事業支援機構、国立研究開発法人科学技術振興機構、株式会社海外通信・放送・郵便事業支援機構、一般社団法人グリーンファイナンス推進機構における地域脱炭素投資促進ファンド事業及び株式会社脱炭素化支援機構の支援対象事業者又は当該支援対象事業者の出資先事業者であり、当該競争に係る物品又は役務に関する分野における技術力を証明できる者

オ　国立研究開発法人（科学技術・イノベーション創出の活性化に関する法律（平成２０年法律第６３号）第２条第９項に規定する研究開発法人のうち、同法別表第３に掲げるものをいう。）が同法第３４条の６第１項の規定により行う出資のうち、金銭出資の出資先事業者又は当該出資先事業者の出資先事業者であり、当該競争に係る物品又は役務に関する分野における技術力を証明できる者

カ　国立研究開発法人日本医療研究開発機構による「創薬ベンチャーエコシステム強化事業（ベンチャーキャピタルの認定）」又は国立研究開発法人新エネルギー・産業技術総合開発機構による「研究開発型スタートアップ支援事業（ベンチャーキャピタル等の認定）」において採択された者の出資先事業者であり、当該競争に係る物品又は役務に関する分野における技術力を証明できる者

キ　グローバルに活躍するスタートアップを創出するための官民による集中プログラム（Ｊ－Ｓｔａｒｔｕｐ又はＪ－Ｓｔａｒｔｕｐ地域版）に選定された事業者であり、当該競争に係る物品又は役務に関する分野における技術力を証明できる者

６．入札方法　　落札決定に当たっては、入札書に記載された金額に当該金額の１０％に相当する額を加算した額（当該金額に１円未満の端数があるときは、その端数金額を切り捨てるものとする。）をもって落札価格とするので、入札者は、消費税等に係る課税事業者であるか免税業者であるかを問わず、見積もった契約金額の１１０分の１００に相当する金額を入札書に記載すること。

７．入札保証金及び契約保証金　　免　除

８．入札の無効　　５の参加資格のない者のした入札または入札に関する条件に反した入札は無効とする。

９．契約書作成の要否　　要

10．適用する契約条項　　役務等契約条項、談合等の不正行為に関する特約条項、
暴力団排除に関する特約条項、
装備品等及び役務の調達における情報セキュリティの確保に関する特約条項
情報システムの調達に係るサプライチェーン・リスク対応に関する特約条項
保有個人情報等の取扱いに関する特約条項

11．その他
（１）細部入札要領については別途配布する「一般競争入札の案内について」（以下、入札案内）のとおり。
（２）入札案内受領の際、資格審査結果通知書（全省庁統一資格）の写しを提示すること。
（３）原則、現に指名停止を受けている者の下請負については認めないものとする。ただし、真にやむを得ない事由を防衛省が認めた場合には、この限りではない。
（４）入札に関する条件　仕様書6.2 b)～g)に定める本業務の実施体制並びに仕様書8.3 m) 1)～3)に定める契約の履行体制に関する資料を提出し、適合すると認められること
（提出期限：令和８年　６月 ２５日 （木）　１２：００　必要に応じ追加資料の提出を求めることがある。）。
（４）この一般競争（総合評価落札方式）に参加を希望するものは、応札資料作成要領に定める提出物を　令和８年　７月 ７日 （火）　１２：００　までに提出しなければならない。
（５）本案件は、府省共通の「電子調達システム」（https://www.p-portal.go.jp）を利用した応札及び入開札手続により実施するものとする。ただし、電子調達システムによりがたい者は、「紙」による入札書等の提出も可とするが、郵便入札については、 令和８年　７月 ２９日 （水）までに、下記担当者必着分を有効とする。
（６）落札者が、１０に掲げる契約条項のほか、中小企業信用保険法第２条第１項に規定する中小企業者である場合は、「債権譲渡制限特約の部分的解除のための特約条項」を別途適用する。
（７）入札案内の交付場所、契約条項を示す場所及び問合せ先
〒162-8801　東京都新宿区市谷本村町５－１　（庁舎Ａ棟10階）※顔写真付の身分証明書を

持参すること。
　受付時間　９：３０～１８：１５（１２：００～１３：００までの間を除く）

<u>また、入札案内のメール配布を希望する者は、以下のとおりメールを送信</u>すること。
　　メールアドレス：naikyoku_chotatsu_mailmagazine@ext.mod.go.jp
　　メール件名　　：「件名：○○○」　入札案内送信依頼
　　添付ファイル　：資格審査結果通知書（全省庁統一資格）の写し
　　防衛省大臣官房会計課契約係　新保　電話　03-3268-3111　内線20822

調達要求番号：

調達仕様書			
件名	防衛省ＯＡシステム基盤運用管理役務（０８運用）	仕様書番号	
		変更年月日	令和　　年　　月　　日
		作成年月日	令和　　年　　月　　日
		作 成 部 署	

1.　総則

1.1　適用範囲

この仕様書は，令和８年度に換装した**防衛省ＯＡシステム基盤借上（０７換装）**にて整備する防衛省ＯＡシステム基盤（以下「省ＯＡ（０７換装）」という。），省ＯＡ（０７換装）に接続して継続利用される省ＯＡシステム共通基盤（各増設・延長含む），加えて令和８年度内に増設される**防衛省ＯＡシステム基盤借上（０８増設）**にて設置される機器の運用管理役務（以下「本役務」という。）について規定する。

1.2　本仕様書を構成する文書

本仕様書を構成する文書を以下に示す。

- **付図１**　全体スケジュール
- **付図２**　システム構成図（**ア**による。）
- **付表１**　省ＯＡ機能一覧
- **付表２**　省ＯＡ利用拠点（**イ**による。）
- **付表３**　運用管理対象機器一覧（**ウ**による。）
- **付表４**　役務実施週次報告内容
- **付表５**　役務実施月次報告内容
- **付表６**　役務実施年間報告内容
- **付表７**　システム利用状況報告内容
- **付表８**　月次セキュリティ報告内容
- **付表９**　運用業務一覧
- **付表１０**　業務フロー
- **付表１１**　運用作業実施スケジュール案
- **付表１２**　既存物品管理情報（Ｅｘｃｅｌ台帳）

1.3　別冊

防衛省ＯＡシステム基盤運用管理役務 別冊

1.4　本仕様書における別冊の参照

本仕様書における**カタカナ**は，**防衛省ＯＡシステム基盤運用管理役務 別冊**によるものとする。

1.5　用語の定義

この仕様書で用いる用語の定義は，**表１**によるほか**1.6**の引用文書等による。

表１－用語の定義

用語	定義
防衛省内	省ＯＡの設置場所
防衛省市ヶ谷地区	市ヶ谷駐屯地・基地
各機関等	防衛省本省の内部部局，統合幕僚監部，陸上幕僚監部，海上幕僚監部，航空幕僚監部，情報本部，防衛監察本部，防衛装備庁，防衛研究所，北関東防衛局及び九州防衛局をいう。ただし，組織改編や組織名称に変更があった場合は，最新のものを適用する。
利用者	省ＯＡを利用する職員
システム担当者	省ＯＡを利用する各機関及び各課室の運用を担当する職員
省ＯＡ	防衛省内において運用している府省内ＬＡＮシステム「防衛省ＯＡシステム基盤」の略称
省ＯＡシステム共通基盤	省ＯＡおいて，仮想化技術によりオンプレミスに構築したＩａａＳ基盤であり，他システムとの基盤集約を効率的に行うため，共通の仕様により構築するもの。
加入システム	省ＯＡが提供する省ＯＡシステム共通基盤上で稼働する防衛省システム
加入システム管理者	加入システムの管理を担当する職員
ＤＩＩ	Ｄｅｆｅｎｓｅ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ（防衛情報通信基盤）の略名で，自衛隊が共通に使用する音声通信網及びデータ通信網を指す。また，データ通信網に接続を承認された情報システムに必要なサービスを提供するもの。
部内系	各種行政事務の処理，文書作成などの業務を遂行し，省内外における電子メール送受信及び政府共通ネットワークとの通信を行う論理ネットワーク。
部外系	ＤＩＩを経由したインターネットを利用したＷｅｂ閲覧，部外系連接システムの利用及び電子メール送受信を行う論理ネットワーク
端末類	個人端末，特殊用途端末Ｉ型，特殊用途端末Ⅱ型
個人端末	防衛省ＯＡシステム基盤（０７換装）及び防衛省ＯＡシステム基盤借上（０８増設）で整備される端末のうち，利用者が使用する，端末と個人のアカウントが１対１に紐付き，個人が占有して利用する端末であり，部内系による業務を行うもの。また，部外系においては仮想端末を利用するもの。
特殊用途端末Ｉ型	防衛省ＯＡシステム基盤（０７換装）及び防衛省ＯＡシステム基盤借上（０８増設）で整備される端末のうち，10 人までの利用者が共有して利用する端末であり，部内系による業務を行うもの。また，部外系においては仮想端末を利用するもの。

表１－用語の定義（続き）

用語	定義
特殊用途端末Ⅱ型	防衛省ＯＡシステム基盤（０７換装）及び防衛省ＯＡシステム基盤借上（０８増設）で整備される端末のうち，10 人を越える利用者が共有して利用する端末であり，部内系による業務を行うもの。また，部外系においては仮想端末を利用するもの。
仮想端末	部外系システムで提供される仮想デスクトップ（ＶＤＩ端末）
官品	官側が保有するハードウェア，ソフトウェア及び備品等
可搬記憶媒体	パソコン又はその周辺機器に挿入又は接続して情報を保存することができる媒体又は機器のうち，可搬型のもの。
キッティング	端末等に各種設定，ソフトウェアのインストールなどを行い，それぞれの環境に最適な状態にセットアップすること。
巡回	地方防衛局の各拠点を定期的に訪問すること。

1.6　引用文書等

この仕様書における引用文書は，この仕様書に規定する範囲内において，この仕様書の一部をなすものであり，引用文書に定める項目が本仕様書と相違する場合は，この仕様書を優先する。

なお，引用文書及び関連文書で定義された用語については，引用文書内で適用されるものとする。

また，公告期間内において，この仕様書における引用文書及び関連文書等の閲覧を必要とする場合は，整備計画局サイバー整備課デジタル化推進班（以下「官側」という。）に対して申し出るものとする。

なお，引用文書及び関連文書は，入札書又は見積書の提出時における最新版とする。

1.6.1　引用文書

a）法令等

1) 著作権法（昭和４５年法律第４８号）
2) 個人情報の保護に関する法律（平成１５年法律第５７号）
3) デジタル・ガバメント推進標準ガイドライン（令和７年５月２７日更新）（以下「標準ガイドライン本編」という。）
4) デジタル・ガバメント推進標準ガイドライン実践ガイドブック（令和７年５月２７日更新）（以下「標準ガイドライン実践ガイドブック」という。）
5) デジタル・ガバメント推進標準ガイドライン解説書（令和７年５月２７日更新）（以下「標準ガイドライン解説書」という。）
6) 情報システムにおけるリスク管理枠組み（ＲＭＦ）実施要領（令和６年１１月２０日）（以下「ＲＭＦ実施要領」という。）
7) 装備品等及び役務の調達における情報セキュリティの確保について（通達）（防装庁（事）第１３７号。令和４年３月３１日）（以下「情報セキュリティ通達」という。）
8) 情報システムに関する調達に係るサプライチェーン・リスク対応のための措置について

（通達）（防装庁（事）第３号。平成３１年１月９日）

9) 情報システムに関する調達に係るサプライチェーン・リスク対応のための措置の細部事項について（通知）（装プ武第１８８号（平成３１年１月９日））

10) 環境物品等の調達の推進に関する基本方針（変更閣議決定（令和８年２月３日））

1.6.2 関連文書

a) 仕様書等

1) 防衛省ＯＡシステム基盤借上（０３換装）（０７延長）

2) 防衛省ＯＡシステム基盤借上（０４増設）

3) 防衛省ＯＡシステム基盤借上（０５増設）

4) 防衛省ＯＡシステム基盤借上（０６増設）

5) 防衛省ＯＡシステム基盤借上（０７換装）

6) 防衛省ＯＡシステム基盤（設置機材の維持管理）（その３）

7) 防衛省ＯＡシステム基盤（設置機材の維持管理）（その４）
※上記の仕様書に定められる事業者の提出文書も含む

8) 防衛情報通信基盤（ＤＩＩ）オープン系詳細設計書「注意」（２０２１年（令和３年）２月）

9) 防衛情報通信基盤（ＤＩＩ）収容設計書（令和５年度）「注意」（２０２２年（令和４年）３月）

10) 防衛省ＯＡシステム基盤プロジェクト計画書

b) 法令等

1) 知的財産基本法（平成１４年法律第１２２号）

2) 防衛省の情報保証に関する訓令（防衛省訓令第１６０ 号（平成１９年９月２０日））

3) 防衛省の情報保証に関する訓令の運用について（通達）（防運情第９２４８号（平成１９年９月２０日））

4) 防衛情報通信基盤データ通信網管理運用規則（自衛隊統合達第１５号（平成２９年７月２０日））

5) 防衛省業務継続計画について（通達）（最終改正　防官文第４３６３号。２０２２年（令和４年）３月１６日）

6) 政府機関等のサイバーセキュリティ対策のための統一基準群（令和５年度版）（以下「統一基準群」という。）

7) 電子政府における調達のために参照すべき暗号のリスト（２０２３年（令和５年）３月３０日）

8) 防衛省クラウド整備指針（令和５年９月１３日）

9) 政府情報システムにおけるセキュリティ・バイ・デザインガイドライン（デジタル庁（令和６年１月３１日））

10) 政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針（デジタル社会推進会議幹事会決定（令和４年９月３０日））

11) 国等による環境物品等の調達の推進等に関する法律（平成１２年法律第１００号）

12) 「公用文作成の考え方」の周知について（内閣文第１号（令和４年１月１１日））

c）その他

1) 政府共通ネットワーク利用ガイド（２０１９年（令和元年）８月３１日）

2) 日本産業規格（ＪＩＳ）（ＪＩＳ　Ｚ　８３０１）

2. 調達の概要

2.1 契約期間

省ＯＡの運用管理に係る契約期間は，契約締結日から令和１２年３月３１日までとする。

2.2 省ＯＡにおける提供機能及び利用拠点

省ＯＡの提供機能については**付表１**を参照すること。**付表１**に係る機器及びサービスを本役務における運用管理対象とする。また，省ＯＡのシステム構成概要は**ア**を参照とし，利用拠点及び本役務の運用管理対象については**イ**及び**ウ**を参照すること。

3. 関連調達案件

3.1 関連調達案件の調達単位等

省ＯＡに関係する主な案件名及び役割については，**表２**のとおり。関連調達に係るスケジュールは**付図１**を参照のこと。

表２－関連調達案件の調達単位等

No.	調達単位	実施期間	役　割
1	防衛省ＯＡシステム基盤借上（０４増設）	令和４年９月～令和９年２月	省ＯＡシステム共通基盤に令和４年度加入システムを集約するための増設を実施
2	防衛省ＯＡシステム基盤（設置機材の維持管理）（その２）	令和５年４月～令和１０年２月	第１センターの設置機材の維持管理を実施
3	防衛省ＯＡシステム基盤借上（０５増設）	令和５年７月～令和１０年２月	省ＯＡシステム共通基盤に令和５年度加入システムを集約するための増設を実施
4	防衛省ＯＡシステム基盤借上（０６増設）	令和６年７月～令和１１年２月	省ＯＡシステム共通基盤に令和６年度加入システムを集約するための増設を実施
5	防衛省ＯＡシステム基盤のプロジェクト管理支援役務	令和７年４月～令和９年３月	省ＯＡに関連する複数事業のプロジェクト管理支援及び調達支援等を実施
6	防衛省ＯＡシステム基盤借上（０７換装）	令和７年１０月～令和１２年３月	省ＯＡ（０７換装）の構築及びハードウェア／ソフトウェアの借上を実施
7	インターネット回線の維持管理役務	令和７年１０月～令和１２年３月	省ＯＡで使用する市ヶ谷センター及び第２センターからインターネットに接続される回線の維持管理を実施
8	防衛省ＯＡシステム基盤（設置機材の維持管理）（その４）	令和８年２月～令和１２年３月	第１センターの設置機材の維持管理を実施
9	防衛省ＯＡシステム基盤（設置機材の維持管理）（その３）	令和８年３月～令和１２年３月	第２センターの設置機材の維持管理を実施

表２－関連調達案件の調達単位等（続き）

No.	調達単位	実施期間	役　割
10	防衛省ＯＡシステム基盤借上（０３換装）（０７延長）	令和８年３月～令和９年２月	防衛省ＯＡシステム基盤の借上（０３換装）で借り上げたハードウェア／ソフトウェア等及び北関東・九州局ＯＡのハードウェア／ソフトウェア等の延長
11	防衛省ＯＡシステム基盤データ移行支援役務（０８移行）	令和８年４月～令和８年１０月	防衛省ＯＡシステム基盤の換装に当たって，防衛省ＯＡシステム基盤の借上（０３換装）の借り上げ機器から省ＯＡ（０７換装）へのデータ移行を実施
12	防衛省ＯＡシステム基盤運用管理役務（０８運用） ※本役務	令和８年８月～令和１２年３月	省ＯＡの運用管理業務を実施
13	防衛省ＯＡシステム基盤借上（０８増設）	令和８年８月～令和１２年３月	主に地方防衛局（北関東局及び九州局）職員の省ＯＡの利用開始に伴う，利用者の増加に対応するため端末類，サーバ，プリンタ及びネットワークスイッチ等の増設を実施
14	北関東・九州局ＯＡシステムデータ移行支援役務	令和８年９月～令和９年３月	地方防衛局（北関東局及び九州局）の省ＯＡの利用開始に当り，防衛局ＯＡシステム（北関東・九州）から省ＯＡへのデータ移行を実施
15	インターネット回線の維持管理役務（北関東・九州）	令和８年８月～令和１２年３月	省ＯＡで使用する地方防衛局（北関東局及び九州局）からインターネットに接続される回線の維持管理を実施
16	防衛省ＯＡシステム基盤借上（０４増設）（０８延長）	令和９年３月～令和１０年２月	防衛省ＯＡシステム基盤の借上（０４増設）で借り上げたハードウェア／ソフトウェア等及び南関東・沖縄局ＯＡのハードウェア／ソフトウェア等の延長

（凡例：太枠は本調達案件）

3.2　調達案件間の入札制限

標準ガイドラインに基づき，調達の透明性及び公正性を確保するため，**表２**欄中**No.5**「防衛省ＯＡシステム基盤のプロジェクト管理支援役務」の契約相手方及び入札公告時点における前年度及び今年度の防衛省デジタル統括アドバイザ業務の受注業者は，本調達の入札に参加することはできないものとする。

4.　役務の内容

4.1　基本的な留意事項

契約相手方は，業務全般において次に示す事項に留意して進めること。

a）業務の実施に当たっては，**標準ガイドライン本編**，**標準ガイドライン解説書**及び**標準ガイ**

ドライン実践ガイドブックを参照し，対応すること。

b) 官側の指示の下，**表２**に示す関連調達案件における契約相手方と適宜情報連携を行い，必要に応じて調整を行いながら対応すること。

c) 本役務で導入するソフトウェアについて，情報の漏えい若しくは破壊又は機能の不正な停止，暴走その他の障害等のリスク（未発見の意図せざる脆弱性を除く。以下「障害等リスク」という。）が潜在すると契約相手方が知り，又は知り得べきソースコード，プログラム，電子部品，機器等（以下「ソースコード等」という。）の埋込み又は組込みその他官側の意図せざる変更が行われていないものでなければならない。

d) 本役務で導入するソフトウェアについて，障害等リスクが潜在すると契約相手方が知り，又は知り得べきソースコード等の埋込み又は組込みその他官側の意図せざる変更が行われない相応の管理その他の契約相手方（下請負者，再委託先等を含む。）による適正な品質管理の下で製作されたものであって，その品質を保証されたものでなければならない。

e) 提出文書については，官側の指摘を反映し**レビュー等実施記録等**，官側と合意した形式でレビュー記録を残したうえで防衛省に提出することとする。なお，詳細は**7.** を参照すること。

f) 提出文書については，必要に応じて想定する記載内容や構成等を整理した骨子を作成の上，事前に官側に提示し，承認を得ること。

g) 書類等の紛失を未然に防止するため，各実施場所の机上及び引き出し内の整理整頓を適宜実施すること。

h) 携帯型情報通信･記録機器等及びパソコン等並びに可搬記憶媒体については，本役務の契約の履行に必要な場合を除き，**5.1**に持ち込み及び持ち出さないこと。

i) 本役務員が利用する端末へ保存する業務関係書類のデータについては，その内容について，あらかじめ官側の了解を得るものとする。なお，業務関係書類とは，契約相手方が本役務の契約に基づき作成する全ての書類とする。

j) 契約相手方は，本役務の契約期間終了に伴い，次の運用管理役務の契約相手方が決まった場合は，障害対応の状況，当該役務が管理対象とする各種台帳や問題の管理状況，各種報告書等運用管理に必要な業務内容等，次の運用管理役務が業務を遂行するために引継ぎが必要と思われる事項及び引継ぎ計画を検討した上で官側と合意すること。合意した内容にもとづき，引継ぎを実施するものとする。

k) 契約相手方は，運用開始前までに防衛省ＯＡシステム基盤借上（０７換装）の契約相手方から本役務の契約の履行に支障がないよう，必要なシステム利用手順及び省ＯＡ（０７換装）の暫定運用期間における対応内容等に関する引継ぎを受けるものとする。また，運用開始後に調達される防衛省ＯＡシステム基盤借上（０８増設）の契約相手方からも引継ぎを受けるものとする。

l) 感染症による業務履行に支障を来すことがないよう，感染症対策に配慮するとともに予めリスク管理表に対応策について記載すること。

4.2 役務要件

a) 本役務の業務については**付表９及び付表１０**の内容を基準とすること。

b) 運用業務において，以下の条件により**付表９及び付表１０**の内容の変更が必要となった場合，変更理由及び変更内容を官側に説明し，合意の上変更すること。

1) 官側の業務負荷軽減または運用業務の改善のため
2) 官から変更の要望があった場合
3) 運用上の課題解決のため変更が必要な場合
4) 利用者及び利用拠点の追加等の変化に対応するため

c) b)の変更において，業務項目の削除については許容しない。

d) 地方防衛局（北関東局及び九州局）以外の地方拠点における，現地作業については都度，現地のシステム担当者と調整し，対応すること。

e) 運用期間中に換装される，ＤＩＩ提供サービスを省ＯＡの端末から利用するための手順書を，必要に応じて作成すること。

4.3 運用立ち上げ

令和８年１０月の運用開始前までに，以下について対応し，官側の承認を得ること。

4.3.1 運用計画書及び運用実施要領書の作成

4.4.1及び**4.4.2**を作成し官側の承認を得ること。

4.3.2 ユーザ支援サイトの更新

換装前の省ＯＡで運用されていたユーザ支援サイトについて，防衛省ＯＡシステム基盤データ移行支援役務（０８移行）にてＳｈａｒｅ　ＰｏｉｎｔＯｎｌｉｎｅ上に移行を行う。移行されたユーザ支援サイトについては，掲載されているコンテンツや情報は換装前のシステムで運用されていた状態のままとなるため，移行されたユーザ支援サイトに対して以下を実施すること。

a) 防衛省ＯＡシステム基盤データ移行支援役務（０８移行）にて移行したサイトの現状の調査を実施すること。

b) a)の調査結果に基づいて，コンテンツの分類及びページレイアウト等，利用者の利便性を向上するための改善について検討し，改善内容について，官側と合意すること。

c) a)及びb)の結果を踏まえ，以下の現状掲載されているコンテンツから省ＯＡ（０７換装）に則した内容に変更するにあたって，変更対象と内容について検討し，官側と合意すること。また，合意した内容に基づいて変更を行うこと。

1) お知らせ
省ＯＡに関する障害情報，メンテナンス情報及びアップデート情報等を利用者向けの周知事項を掲載

2) 各種マニュアル・ツール
省ＯＡを利用するために必要な利用者向けのマニュアル等を掲載

3) よくあるご質問
省ＯＡへ利用者から寄せられる質問のうち，頻度が高いものに関する回答を掲載

4) 出張・テレワークをご利用になる前に
省ＯＡの端末を省外で利用する際の注意事項及びテレワーク環境の利用手順等を掲載

5) 課室担当者・機関担当者の皆様へ
省ＯＡの申請管理機能におけるシステム担当者向けの注意事項及び依頼事項等について

掲載

6) ＦＡＱ

省ＯＡへ利用者から寄せられる省ＯＡ構成品に関するトラブル等に関する対処法について掲載

7) お問い合わせ

省ＯＡへの問い合わせ方法，対応時間，窓口及び連絡先について掲載

4.3.3 官品を物品管理機能に登録

Ｅｘｃｅｌ台帳で管理されている官保有のハードウェア及びソフトウェアを物品管理機能に登録すること。また，貸し出し中の物品について所在の確認を行い，物品管理用のラベルを払い出し，管理対象のハードウェアへラベルの貼り付けを行うこと。所在を確認の上，管理情報を最新化すること。物品管理機能へ登録する対象となる台帳は**付表１２**のとおり。

4.3.4 各種報告書作成

4.4.3の報告書の様式を作成すること。

4.3.5 各種台帳の整理

付表９において，業務上必要となる管理台帳の管理項目を検討し，テンプレートを作成し官側の合意を得ること。

4.3.6 各種手順の更新

以下のＤＩＩ提供サービスを省ＯＡ（０７換装）の端末から利用するための利用手順書を必要に応じて更新すること。

1) Ｏｕｔｌｏｏｋ（部外のみ）の利用手順

2) Ｊａｂｂｅｒ（リアルタイムコミュニケーション）の利用手順

3) 部外テレビ電話サービス（Ｃｉｓｃｏ Ｍｅｅｔｉｎｇ Ｓｅｒｖｉｃｅ）

4) 部外系ＤＩＩパスワードの初期化手順

4.3.7 運用承認の支援

省ＯＡの運用にあたり，官側が実施するＲＭＦにおける運用承認手続きの支援として，ＲＭＦのセキュリティ計画書に定義された各要求項目のうち，運用での対応とされている項目について，運用承認に必要となる文書作成に対する情報提供を，**ＲＭＦ実施要領**に基づき主体的に行うこと。

4.3.8 運用役務場所等に関する調整

運用役務場所レイアウト及び配布前の省ＯＡの構成品の保管場所について検討し，官側と調整すること。

4.3.9 プレイブックの検討・実装

省ＯＡのセキュリティ運用自動化機能を用いて，運用開始前の時点で自動化可能な業務を検討したうえで，官側に提案し，承認を得ること。実装することとなったプレイブックについては，運用立ち上げ期間において実装すること。

4.4 文書作成

4.4.1 防衛省ＯＡシステム基盤運用計画書の作成

a) **防衛省ＯＡシステム基盤運用計画書**（以下「運用計画書」という。）を作成すること。

b) **運用計画書**は，以下の項目について記載すること。また，以下の項目以外に運用役務を遂行するうえで定める必要がある事項が生じた場合は官側に提案の上，追加すること。

1) 運用管理対象（構成品目単位）

2) ＳＬＯ（Ｓｅｒｖｉｃｅ Ｌｅｖｅｌ Ｏｂｊｅｃｔｉｖｅ）
運用役務の稼働目標及びユーザ支援の対応（一次回答等）の目標値について定義すること。

3) 作業体制
本調達事業者のみならず，関連する機関又は組織とそれぞれの関係性，役割，責務を記載すること。

4) 運用業務実施スケジュール
運用業務について定期的な作業については，**付表１１**を基準とし，実施スケジュールを記載すること。また，スケジュールの計画においては官側の年間のイベントに考慮したスケジュールとすること。

5) 運用作業の条件（実施可能な時間帯，業務影響等）
運用業務の運用形態（オンサイト，リモート等），運用環境（本番，災対）等について記載すること。また，運用中に段階的に地方防衛局が拠点として追加されることを考慮すること。

6) 成果物に関する事項
本役務にて納品対象となる成果物の内容（記載する項目等），担当者，納品期限，納品方法，納品部数等について記載すること。

4.4.2 防衛省ＯＡシステム基盤運用実施要領書の作成

a) 本役務の業務を遂行するためのに必要な管理体系，管理方法及び必要な管理項目等について定義し，**防衛省ＯＡシステム基盤運用実施要領書**（以下「運用実施要領書」という。）を作成すること。

b) **運用実施要領書**は，以下の項目について記載すること。また，以下の項目以外に運用役務を遂行するうえで定める必要がある事項が生じた場合は官側に提案の上，追加すること。

1) コミュニケーション管理
省ＯＡに係る機関及び関係事業者との連絡調整に関する方法，当該役務が参加する会議，開催頻度，議事録等の管理等について記載すること。また，各種作業実施時，インシデント発生時及び障害発生時の連絡及び報告について明記すること。

2) 体制管理
当該役務における体制図及び作業体制の管理方法について記載すること。

3) 作業管理
運用に係る作業と作業における品質の管理手法等について記載すること。

4) リスク管理
運用に係る作業で発生しうるリスクについて，管理手法及び顕在化した際の対処手法に

ついて記載すること。

5) 課題管理

運用に係る課題，問題発生時の管理手法及び対応方針について記載すること。

6) システム構成管理

当該役務にて実施する作業に係るシステム構成（ハードウェア，ソフトウェア，ネットワーク等）の変更管理について記載すること。

7) 変更管理

6)に示すシステム構成を除く，運用に関する作業概要，作業理由，変更対象，実施日，再委託業者，変更対象ドキュメント，関連チケット等の管理手法について記載すること。

8) 情報セキュリティ対策

当該役務における情報漏えい対策等，セキュリティ対策に係る事項について記載すること。

9) 物品管理

本役務にて管理対象となる物品（官品を含む）の管理方法，棚卸しの手法等について記載すること。

10) 本役務の業務改善

本役務の業務改善について，運用上の課題の抽出方法，改善に資する判断基準等について記載すること。

4.4.3 定期報告

a) 省ＯＡのシステム運用状況に関する報告として，予め官と合意した報告対象期間に対して**役務実施週次報告書**を作成し，週１回は官側への報告会を実施すること。また、最終週の週次報告の報告対象期間については、別途官側と協議の上決定すること。なお，当該報告書に記載する項目は**付表４**を基準とすること。

b) 省ＯＡのシステム運用状況に関する報告として，予め官と合意した報告対象期間に対して**役務実施月次報告書**を作成し，月１回は官側への報告会を実施すること。また、最終月の月次報告の報告対象期間については、別途官側と協議の上決定すること。なお，当該報告書に記載する項目は**付表５**を基準とすること。

c) 省ＯＡのシステム運用状況に関する報告として，各年度単位の**役務実施年間報告書**を作成し，毎年度末に官側へ報告すること。また、最終年度の報告対象期間については、別途官側と協議の上決定すること。なお，当該報告書に記載する項目は**付表６**を基準とすること。

d) 省ＯＡのシステム稼働に関する報告として，予め官と合意した報告対象期間に対して**システム利用状況報告書**を作成し，月１回は官側への報告会を実施すること。また、最終月の報告対象期間については、別途官側と協議の上決定すること。なお，当該報告書に記載する項目は**付表７**を基準とすること。

e) 省ＯＡのセキュリティに関する報告として，予め官と合意した報告対象期間に対して**月次セキュリティ報告書**を作成し，月１回は官側へ報告すること。また、最終月の報告対象期

間については、別途官側と協議の上決定すること。なお，当該報告書に記載する項目は**付表８**を基準とすること。

f) **a)～e)**に記載する項目について，集計表はグラフ等を用いて視覚的にわかりやすく記載するものとする。

g) **a)～e)**の報告書作成において，機関担当者へ棚卸し及び状況調査に係る協力を得る場合，事前に各機関担当者への周知及び必要に応じて説明を実施すること。

4.4.4 作業実施計画書の作成

サーバやネットワーク機器，クラウドサービス等，省ＯＡの基盤に対して変更加える作業については，原則，**作業実施計画書**を作成すること。また，その必要性については，官側と協議し合意すること。なお，**作業実施計画書**を作成する際には，以下の項目と基準とし，追加が必要と考えられる項目が生じた場合は官側に提案の上，追加すること。

a) 作業概要

実施する作業の目的，作業内容，業務影響の有無及び想定される作業結果について記載すること。

b) 作業体制

作業日の体制について記載すること。

c) スケジュール

作業日のスケジュール概要を記載すること。

d) 作業対象

対象機器のホスト名，種別等について記載すること。

e) 作業手順

作業手順について記載すること。手順書があらかじめある場合は，使用する手順書を付帯すること。

f) 切り戻し手順

切り戻し手順について記載すること。

g) 切り戻し判定基準

切り戻し判定基準と判断に係る所要時間について記載すること。

h) その他

その他，周知事項及び調整事項等について記載すること。

4.4.5 作業結果報告書の作成

本役務にて作業実施後，**作業結果報告書**を作成し，官側の合意を得ること。また，**作業結果報告書**に記載する項目は，以下の項目を基準とすること。

a) 作業者名

作業実施者の氏名を記載すること。

b) スケジュールの実績

事前に作成したスケジュールに対し，作業の実績時間を記載すること。

c) 作業結果

作業実施後の作業結果について記載すること。

5. 運用業務に関する要件

5.1 実施場所

a) 年末年始（１２月２９日から１月３日までの間）及び土日祝日を除く８：３０－２１：００（以下「平日日中帯」という。）は，防衛省市ヶ谷地区の官側が指定する場所（以下「省内実施場所」という。）でシステム運用の業務を実施すること。

b) 平日日中帯を除く休日夜間帯のシステム運用及びセキュリティ運用の実施場所は**情報セキュリティ通達**に基づく，防衛省が求めるセキュリティ要件を満たす保護情報の取扱施設（以下「役務事務所」という。）とすること。

c) なお、夜間休日帯であっても，官側が指示した場合及び障害発生時等の緊急を要する場合については，必要に応じ，省内実施場所で対応するものとする。

d) 役務事務所は，令和８年１０月１日の運用開始までに用意すること。

e) 本役務の業務のうち第１センターまたは第２センターにおいて現地対応が必要な作業については，第１センターまたは第２センターの入館手続き方法による申請と承認を得たうえで，役務員が現地に出向くこととする。この時，省内実施場所及び役務事務所と第１センターまたは第２センター間の交通費は契約相手方が負担するものとする。

5.2 役務時間

２４時間３６５日（うるう年は３６６日）を基準とし，機器の交換対応等，夜間休日の対応が不可となる場合は，翌開庁日に対応することを可とする。

6. 本業務の実施に伴うプロジェクト実施体制の整備

6.1 事業者の要件

6.1.1 一般事項

本業務を担当するに当たり，会社全体又は統括役務員が所属する部門が，以下のいずれかの要件を満たしていること。資格については，それを証明する書面（認定証等）の写しを提出すること。

6.1.2 情報セキュリティに係る公的認証

ＩＳＭＳ認証（ＪＩＳＱ２７００１（ＩＳＯ／ＩＥＣ２７００１）を保有していること。

6.1.3 委託実績

a) 官公庁及び独立行政法人において，端末５０００台規模以上のＬＡＮシステムの運用の受託実績を有すること。

b) 官公庁及び独立行政法人におけるＬＡＮシステムにおいて，直近５年以内に３件以上の運用の受託実績を有すること。

c) 利用場所が１箇所に集約されておらず，都道府県を跨ぐ複数の場所（１０箇所以上）で利用される情報システムの運用の受託実績を有すること。

6.2 実施体制

契約相手方の体制は，以下に示す条件を満たすこと。なお，業務体制全般，特に，業務実施責任者については，本役務の成功（予定どおりの稼働，品質の担保）に向け，積極的・主体的な業務の推進や提案等を求める。

a) 契約締結後速やかに引継ぎのスケジュール及び内容を明確にした引継計画を立案の上，官

側の承認を得ること。

b) 本役務の契約相手方は，**6.3**を満たすことを証明する「**業務従事者名簿**及び**職務経歴書等**」を入札前に提出すること。提出に係る細部は入札説明書による。

c) 履行に必要な情報を取り扱うにふさわしい契約を履行する業務に従事する個人（以下「業務従事者」という。）を確保すること。

d) 業務従事者が履行に必要若しくは有用な，又は背景となる経歴，知見，資格，語学（母語及び外国語能力），文化的背景（国籍等），業績等を有すること。

e) 業務従事者が他の手持ち業務等との関係において履行に必要な業務所要に対応できる体制にあること。

f) 運用開始直後及び職員の異動時期（主に毎年３月，４月及び８月）等の利用者からの問合せが急増する時期，並びに加入システムの検証期間及び本番運用開始直後の問合せが急増する時期でも対応可能な体制を構築すること。

g) 本役務の業務のうち防衛省市ヶ谷地区において対応する必要のある業務を実施できる体制を確保すること。

6.3 業務従事者の要件

6.3.1 全般事項

a) 要員は，本仕様書に示す役務内容を円滑に遂行できる能力を有すること。

b) 官側において，要員の変更の必要があると判断したときは，１ヶ月前までに契約相手方に通知の上，変更させるものとする。

c) 要員の変更に際しては，いずれの要員においても十分な引継ぎ期間を設けるなど，業務を円滑に持続できるように十分な配慮を行うこと。

d) 契約相手方は，常に業務従事者の服装，勤務態度，風紀及び衛生等について万全の監督を行うこと。

e) 業務従事者は，業務実施場所の整理整頓を随時行い，業務環境の整備に努めること。

f) 日本国籍を有していること。

g) 官側からの省ＯＡに係る技術相談に対し，技術又は運用管理の観点から官側を支援すること。

h) システム運用体制とセキュリティ運用体制のそれぞれを組成すること。

6.3.2 統括役務員

a) 本役務の作業全体を管理監督し，業務の遂行を主体的に推進すること。

b) 業務の遂行に問題が生じていないかを確認し，問題が発生する兆候が発覚又は問題が発生した場合は，速やかに官側に報告すること。加えて，原因分析を行った上で是正案を検討・報告し，官側の承認を得ること

c) 官公庁及び独立行政法人における利用者５０００名以上のＬＡＮシステムの運用業務において，業務実施責任者（プロジェクトマネージャ及び同補佐等，同等の経歴を含む。）以上としての経験を５年以上有すること。

d) 契約期間中は、省ＯＡに係る業務に専任すること。

e) 以下の**1)**～**2)**のいずれかおよび**3)**～**4)**のいずれかの資格を有すること。

1) ＩＴＩＬ　ｖ３　Ｆｏｕｎｄａｔｉｏｎ又はＩＴＩＬ４　Ｆｏｕｎｄａｔｉｏｎ以上
2) 基本情報技術者試験（ＩＰＡ）以上
3) 情報処理技術者試験（プロジェクトマネージャ）
4) ＰＭＰ（プロジェクト・マネジメント・プロフェッショナル）

6.3.3 副統括役務員（システム運用体制）

a) システム運用の要員に対し，業務上必要な教育を実施し，業務が問題なく遂行できるよう要員を管理監督するとともに，業務の遂行を主体的に推進すること。
b) 業務の遂行上の問題が発生する兆候が発覚又は問題が発生した場合は，適宜統括役務員へ報告し，早期に解決するよう対応すること。なお，必要に応じ，統括役務員に代わって官側への報告を行うこと。
c) 官公庁及び独立行政法人におけるＬＡＮシステムの運用業務に，業務実施責任者（プロジェクトマネージャ及び同補佐等，同等の経歴を含む。）以上としての経験を３年以上有すること。
d) 契約期間中は，省ＯＡに係る業務に専任すること。
e) 以下の1)～5)のいずれかの資格を有すること。
1) ＩＴＩＬ　ｖ３　Ｅｘｐｅｒｔ
2) ＩＴＩＬ４　Ｐｒａｃｔｉｃｅ　Ｍａｎａｇｅｒ
3) ＩＴＩＬ４　Ｍａｎａｇｉｎｇ　Ｐｒｏｆｅｓｓｉｏｎａｌ
4) ＩＴＩＬ４　Ｓｔｒａｔｅｇｉｃ　Ｌｅａｄｅｒ
5) ＩＴサービスマネージャ試験（ＩＰＡ）

6.3.4 運用役務員（システム運用体制）

a) システム運用に係る業務全般の実作業を担当すること。
b) システム運用の業務経験を１年以上有すること。
c) 以下の1)～4)の資格を有すること。なお，複数人で満たすことを可とする。
1) ＣＣＮＡ（Ｃｉｓｃｏ　Ｃｅｒｔｉｆｉｅｄ　Ｎｅｔｗｏｒｋ　Ａｓｓｏｃｉａｔｅ）以上
2) Ｍｉｃｒｏｓｏｆｔ　３６５　Ｃｅｒｔｉｆｉｅｄ　Ｆｕｎｄａｍｅｎｔａｌｓ（ＭＳ－９００）相当以上
3) Ｍｉｃｒｏｓｏｆｔ　Ｃｅｒｔｉｆｉｅｄ　Ａｚｕｒｅ　Ｆｕｎｄａｍｅｎｔａｌｓ（ＡＺ－９００）相当以上
4) ＩＴＩＬｖ３　Ｆｏｕｎｄａｔｉｏｎ又はＩＴＩＬ４　Ｆｏｕｎｄａｔｉｏｎ

6.3.5 副統括役務員（セキュリティ運用体制）

a) ＳＯＣ担当者及びＣＳＩＲＴ担当者に対し，業務上必要な教育を実施し，業務が問題なく遂行できるよう要員を管理監督するとともに，業務の遂行を主体的に推進すること。
b) 業務の遂行上の問題が発生する兆候が発覚又は問題が発生した場合は，適宜統括役務員へ報告し，早期に解決するよう対応すること。なお，必要に応じ，統括役務員に代わって官側への報告を行うこと。
c) セキュリティ運用設計及びセキュリティ運用体制の責任者として従事した経験を３年以上

有すること。

d) 契約期間中は，省ＯＡに係る業務に専任すること。

e) 以下の1)～3)のいずれかの資格を有すること。

1) 情報処理安全確保支援士試験（ＩＰＡ）

2) ＣＩＳＳＰ（Ｃｅｒｔｉｆｉｅｄ Ｉｎｆｏｒｍａｔｉｏｎ Ｓｙｓｔｅｍｓ Ｓｅｃｕｒｉｔｙ Ｐｒｏｆｅｓｓｉｏｎａｌ）

3) ＣｏｍｐＴＩＡ ＣＡＳＰ＋

6.3.6 ＳＯＣ担当者（セキュリティ運用体制）

a) 省ＯＡのセキュリティ機能（ＳＩＥＭ・ＳＯＡＲ等）を用いて，継続的なセキュリティ監視・検知を行うこと。

b) セキュリティインシデントを未然に防ぐための対策を行うこと。

c) 検知したセキュリティインシデントに対して，調査・分析を行うこと。

d) 最新の脅威情報，脆弱性情報を収集し，セキュリティレベルの強化や対策を検討すること。

e) ＳＯＣとしての勤務経験を３年以上有する要員を１名以上配置すること。

f) 以下の1)～3)のいずれかの資格を有する要員を１名以上配置すること。

1) Ｍｉｃｒｏｓｏｆｔ Ｓｅｃｕｒｉｔｙ，Ｃｏｍｐｌｉａｎｃｅ，ａｎｄ Ｉｄｅｎｔｉｔｙ Ｆｕｎｄａｍｅｎｔａｌｓ（ＳＣ－９００）相当以上

2) 情報セキュリティマネジメント試験（ＩＰＡ）

3) ＣｏｍｐＴＩＡ Ｓｅｃｕｒｉｔｙ＋

6.3.7 ＣＳＩＲＴ担当者（セキュリティ運用体制）

a) 発生したセキュリティインシデントの被害を最小限に抑えるため，調査・分析を行うこと。また，調査・分析結果に応じて必要な対策・再発防止策について検討し，必要な指示を行うこと。

b) ＳＯＣ担当者が収集した脅威情報及び脆弱性情報に対して，評価・分析及び対応方針の検討を行うこと。

c) 利用者５０００名以上のＬＡＮシステムにおいて，ＣＳＩＲＴとしての勤務経験を５年以上有する要員を１名以上配置すること。

d) 以下の1)～3)のいずれかの資格を有する要員を１名以上配置すること。

1) 情報処理安全確保支援士

2) ＣＩＳＳＰ（Ｃｅｒｔｉｆｉｅｄ Ｉｎｆｏｒｍａｔｉｏｎ Ｓｙｓｔｅｍｓ Ｓｅｃｕｒｉｔｙ Ｐｒｏｆｅｓｓｉｏｎａｌ）

3) ＣｏｍｐＴＩＡ ＣｙＳＡ＋

6.4 業務従事者名簿の提出

各種業務を実施する業務従事者について，契約締結後速やかに，本役務を実施する作業者について**業務従事者名簿**を作成し，官側に報告，承認を得ること。

7. 提出文書の範囲，提出期限等

7.1 運用役務における提出文書

表３に示す文書は，毎年度末に電子媒体（ＣＤ－Ｒ又はＤＶＤ－Ｒ）での提出を原則とするが，都度提出が必要な文書については官側と合意した形式で提出し，官側の承認を得ること。また，作業の実施に当たり，当該文書の記載事項に疑義が生じた場合，速やかに該当箇所を修正し，官側の承認を得ること。

表３－運用役務における提出文書

No.	文書名	部数	提出時期
1	運用計画書	電子媒体：各１	契約締結後，１０営業日以内を基準とする。
2	運用実施要領書	電子媒体：各１	契約締結後，１０営業日以内を基準とする。
3	業務従事者名簿	電子媒体：各１	契約締結後，１０営業日以内を基準とする。 業務従事者の変更があった場合その都度提出とする。
4	役務実施週次報告書	電子媒体：各１	報告対象期間から５営業日以内を基準とする。 最終週の報告書は令和１２年３月２９日までとする。
5	役務実施月次報告書	電子媒体：各１	報告対象期間から１５営業日以内を基準とする。 最終月の報告書は令和１２年３月２９日までとする。
6	役務実施年間報告書	電子媒体：各１	翌年度４月末日までとする。 最終年度の報告書は令和１２年３月２９日までとする。
7	月次セキュリティ報告書	電子媒体：各１	報告対象期間から１５営業日以内を基準とする。 最終月の報告書は令和１２年３月２９日までとする。
8	システム利用状況報告書	電子媒体：各１	報告対象期間から１５営業日以内を基準とする。 最終月の報告書は令和１２年３月２９日までとする。
9	作業実施計画書	電子媒体：各１	作業実施前までに提出とする。
10	作業実施結果報告書	電子媒体：各１	各作業実施後，提出時期は官側との協議による。
11	議事録	電子媒体：各１	開催から３営業日以内に都度提出とする。

7.2 提出方法

a) 提出文書は，全て日本語で作成すること。ただし，英字で表記することが一般的な文言については，英字で表記することができるものとする。

b) 用字・用語・記述符号の表記については，**公用文作成の要領**に準拠すること。

c) 情報処理に関する用語の表記については，原則，日本産業規格（ＪＩＳ）の規定に準拠すること。

d) 提出文書は電磁的記録媒体（ＣＤ-Ｒ又はＤＶＤ－Ｒ）により作成し，**表３**に示す提出部数を提出すること。また，電磁的記録媒体はウイルスチェックを実施した上で，追記不可の処置を施し提出するものとする。

e) 提出文書の用紙サイズは，原則として日本産業規格Ａ列４番とするが，必要に応じて日本産業規格Ａ列３番を使用すること。

f) 官側による印刷時に，レイアウト崩れやページの飛び等が生じないように作成すること。

g) 電磁的記録媒体による提出について，納品時点における最新のＭｉｃｒｏｓｏｆｔ　Ｗｏｒｄ，同Ｅｘｃｅｌ，同ＰｏｗｅｒＰｏｉｎｔで編集可能な形式で作成し，提出すること。ただし，官側が他の形式による提出を求める場合は，調整の上，これに応じること。なお，契約相手方側で他の形式を用いて提出する必要があるファイルがある場合は，編集可能となる方策について検討し，官側と調整すること。

h) 提出後，官側において改変が可能となるよう，図表等の元データも併せて提出すること。

i) 提出文書の作成に当たって，特別なツールを使用する必要がある場合は，事前に官側の承認を得ること。

7.3 提出場所

提出文書は，原則として以下の場所に提出すること。ただし官側が別途指定する場合はこの限りではない。

（提出先）

〒１６２－８８０１　東京都新宿区市谷本村町５－１

防衛省 整備計画局 サイバー整備課 デジタル化推進班

8. 個人情報保護及び秘密保全等

8.1 個人情報保護等

a) 契約相手方は，官側から提供された個人情報及び業務上知り得た個人情報について，**個人情報の保護に関する法律**に基づき，適切な管理を行わなくてはならない。また，当該個人情報については，本業務以外の目的のために利用してはならない。

b) 生存する個人に関する情報であり，当該情報に含まれる氏名，生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ，それにより特定の個人を識別することができることとなるものを含む。）は個人情報として取り扱うこと。

c) 個人情報，個人関連情報，特定個人情報等，仮名加工情報及び行政機関等匿名加工情報（以下「個人情報等」という。） の取扱いに係る事項について官側と協議の上決定し，書面にて提出すること。なお，以下の事項を記載すること。

- 管理体制
- 個人情報等の管理状況の検査に関する事項（検査時期，検査項目，検査結果において問題があった場合の対応等）

d) 本業務の遂行において，安全性や確実性を考慮し，仕様外の個人情報等を取得し，取り扱う必要性や有用性がある場合は，官側と協議してその妥当性を検討し，承認を得た上でこれを行うこと。また，官側と協議の上で当該個人情報等の利用目的と性質を考慮し，保持期間を定めること。当該保持期間が経過した後は，業務仕様にしたがって遅滞なく消去し又は匿名化すること。

e) 本業務の遂行に際して個人情報等を取得し取り扱う場合，本業務のために定められた利用目的外の利用を厳に慎み，本業務のために供する個人情報等は他の個人情報等と分別して保管し，官側と協議のうえで書面により定めた環境下で所定の仕様に依拠して遂行すること。また，本業務を遂行する業務従事者にあってもこれを実効あらしめるものとするた

め，必要な管理監督及び教育を行うこと。

f) 個人情報等を本業務のために定められた利用目的外で複製する際には，事前に官側の許可を得ること。なお，複製の実施は必要最小限とし，複製が不要となり次第，その内容が絶対に復元できないように破棄・消去を実施すること。なお，受託者は廃棄作業が適切に行われた事を確認し，その保証をすること。

g) 個人情報等の取扱いに際して，その本人によるデータの入力，本人による情報システムの利用に伴うデータの生成，その他本人による関与を通じてデータ処理が行われる場合には，その処理の記録（システム上のログによるもの等）を残すこと。

h) 受託者が本業務のために取り扱う個人情報等に関して，利用者等から個人情報等の保護に関する法律その他適用ある法令上の請求が行われた場合には，速やかに官側に通知してその指示を受けること。また，官側による法令上の請求への対応のために必要な個人情報等の抽出，変更，削除その他合理的な協力を行い，これを可能とする体制及び仕様を維持すること。

i) 作業を派遣労働者に行わせる場合を含め直接雇用していない第三者の使用人等に業務従事させる場合には，本業務の一部を再委託する場合の手続きに準じて労働者派遣契約書に秘密保持義務など個人情報等の適正な取扱いに関する事項を明記し，作業実施前に教育を実施し，認識を徹底させること。なお，受託者はその旨を証明する書類を提出し，官側の承認を得た上で実施すること。

j) 官側が必要と認めた場合であってその態様が受託者の業務その他の営業を著しく妨げるものでないとき，官側またはこれが指定した者による個人情報等の取扱いの状況及び管理体制の監査を受け入れ，合理的に必要と認められる資料の提出を行うこと。

k) 受託者は，本業務を履行する上で個人情報等の漏えい等安全確保の上で問題となる事案又はそのおそれのある事案を把握した場合には，直ちに被害の拡大を防止等のため必要な措置を講ずるとともに，官側に事案が発生した旨，被害状況，復旧等の措置及び本人への対応方針等について直ちに報告すること。

l) 個人情報等の取扱いにおいて適正な取扱いが行われなかった場合は，本業務の契約解除の措置を受けるものとする。

8.2 情報システム監査

情報システムの監査の要件を以下に示す。

a) 本調達において整備又は管理を行う情報システムに伴うリスクとその対応状況を客観的に評価するために，官側が情報システム監査の実施を必要と判断した場合は，官側が定めた実施内容（監査内容，対象範囲，実施者等）に基づく情報システム監査を契約相手方は受け入れること。（官側が別途選定した事業者による監査を含む）。

b) 情報システム監査で問題点の指摘又は改善案の提示を受けた場合には，対応案を担当部署と協議し，指示された期間までに是正を図ること。

8.3 秘密保全等

a) 契約相手方は，本業務の実施に伴い知り得た保護情報の取扱いに当たっては，**情報セキュリティ通達**に基づき，**エ**に示す保護すべき情報（以下「保護情報」という。）を適切に管

理するものとし，その効力はこの契約終了後も継続するものとする。また，保護情報は，省内実施場所でのみ取り扱うものとし，持ち出す場合は必要な措置，手続きを講ずるものとする。

b) 契約相手方は，**情報システムに関する調達に係るサプライチェーン・リスク対応のための措置の細部事項について（通知）**別添「情報システムの調達におけるサプライチェーン・リスク対応に関する特約条項」に基づき，サプライチェーン・リスク対応を実施すること。

c) **a)**から**b)**のほか，官側は契約相手方に対し，本業務の適正かつ確実な実施を確保するために必要な範囲で，秘密を適正に取り扱うための措置を採るべきことを指示することができるものとする。

d) 契約相手方は，本業務の契約の履行に必要であると官側が承認した場合を除き，情報を契約相手方の事務所以外の省外に持ち出してはならない。

e) 契約相手方は，本業務の契約の履行に必要であると官側が承認した場合を除き，外部から省内実施場所へデータを持込んではならない。

f) 本業務の実施において情報セキュリティが侵害され，又はその恐れがある場合には，適切な措置を講じるとともに，直ちに把握し得る限りの全ての内容を，その後速やかにその詳細を官側に報告すること。

g) 本業務の実施における情報セキュリティ対策の履行状況について，官側から実績の報告を求めた場合には，速やかに提出すること。

h) 本業務の実施において，契約相手方における情報セキュリティ対策の履行が不十分であると認められる場合には，契約相手方は官側の求めに応じ，協議を行い，必要な対策を講じること。

i) 官側が定める立入禁止の掲示がある場所及び官側が定める立入制限場所等（以下「立入禁止場所等」という。）へ立ち入る技術員等は，当該立入禁止場所等への立入手続等に関する通達又は，官側等又はその指定した者が定める手続に従い，立ち入りを許可された者でなければならない。

j) 契約相手方は，官側から貸付けを受けた文書及び電子データについては，当該業務終了時に官側に返却すること。また，提供を受けた文書及び電子データについては，当該業務終了前までに消去又は廃棄して，速やかにその旨を書面で報告すること。

k) 本契約に係る情報及び情報システム以外の官側が所管する情報及び情報システムに不要なアクセスを実施しないこと。

l) 立入禁止場所等への携帯電話，パソコン及び可搬記憶媒体の持込みについては，官側と協議の上，その指示に従うこと。

m) 契約相手方は，この契約の履行に際し知り得た保護すべき情報（**情報セキュリティ通達**第２項第１号に規定する情報をいう。）その他の非公知の情報（以下「保護すべき情報等」という。）の取扱いに当たっては，**情報セキュリティ通達**における添付資料「装備品等及び役務の調達における情報セキュリティの確保に関する特約条項」及び別紙「装備品等及び役務の調達における情報セキュリティ基準」に基づき（保護すべき情報に該当しない非

公知の情報にあっては，これらに準じて），適切に管理するものとする。この際，特に，保護すべき情報等の取扱いについては，次の履行体制を確保し，これを変更した場合には，遅滞なく官側に通知するものとする。

1) 契約を履行する一環として契約相手方が収集，整理，作成等した情報が，保護すべき情報（**情報セキュリティ通達**第５項第４号の規定に基づく解除をしようとする場合に，同号に規定する確認を行うまでは保護すべき情報として取り扱うものとする。）として取り扱われることを保障する履行体制をとること。

2) 官側の同意を得て指定した取扱者以外の者に取り扱わせないことを保障する履行体制をとること。

3) 官側が書面により個別に許可した場合を除き，契約相手方に係る親会社，地域統括会社，ブランド・ライセンサー，フランチャイザー，コンサルタントその他の契約相手方に対して指導，監督，業務支援，助言，監査等を行う者を含む一切の契約相手方以外の者に対して伝達又は漏えいされないことを保障する履行体制をとること。

9. 提出文書の取扱い

9.1 知的財産権の帰属

9.1.1 著作権

a) 契約相手方は，本業務の提出文書に関し，官側に提出したとき**著作権法**第２７条及び第２８条を含む著作権の全てを官側に無償で譲渡するものとする。

b) 契約相手方は，防衛省が承認した場合を除き，提出文書に関する著作者人格権を行使しないものとする。また，契約相手方は，当該著作物の著作者が契約相手方以外の者であるときは，当該著作者が著作者人格権を行使しないよう必要な措置をとるものとする。

c) a)及びb)の規定は，契約相手方の固有の技術資料（契約の相手方が第三者から提供を受けた技術資料を含む。以下同じ。）に係る著作権には適用しない。

d) 提出文書に第三者が権利を有する著作物が含まれる場合には，契約相手方が当該著作物の使用に必要な費用の負担及び使用許諾契約等に係る一切の手続きを行うものとする。

e) c)及びd)において，官側は納入された著作物を自ら利用するために必要と認められる範囲で，翻案，翻訳，複製及び貸与することができるものとする。

f) 本業務の提出文書等に関し，第三者との間に著作権に係る権利侵害の紛争が生じた場合には，当該紛争の原因が専ら官側の責めに帰す場合を除き，契約相手方の責任と負担において一切を処理すること。この場合において，官側は当該紛争の事実を知ったときは，契約相手方に必要な範囲で訴訟上の対応を契約相手方に委ねるなどの協力措置を求めるものとし，契約相手方はこれに協力するものとする。

g) 官側は，この契約の履行中及び終了後５年間は，契約書又は仕様書等の定めるところにより官側に提出された契約相手方の固有の技術資料に係る著作物につき，この契約に関して防衛省又は防衛装備庁が行う監督，検査，調査，試験若しくはその結果の評価その他これに類する業務のため必要がある場合は，防衛省又は防衛装備庁の内部において利用し及び複製（契約相手方の指定するものの複製を除く。）することができる。

9.1.2 権利義務の帰属等

a) 本業務の実施が第三者の特許権，著作権その他の権利と抵触する場合は，契約相手方は，その責任において，必要な措置を講じなくてはならない。

b) 契約相手方は，本業務の実施状況を第三者に提供し，又は公表しようとする場合は，あらかじめ，官側の承認を受けなければならない。

c) 省内実施場所で生成した情報は，防衛省の所有に属するものとする。

9.2 契約不適合責任

契約不適合責任の要件を以下に示す。

a) 本業務における提出物等について，種類，品質又は数量が契約書，本調達仕様書その他合意された要件（以下「契約書等」という。）の内容に適合しないもの（以下「不適合」という。）である場合，その不適合が官側の責に帰すべき事由による場合を除き，契約の相手方は，自己の費用で，官側の選択に従い，その修補，代替物の引渡し又は不足分の引渡しによる履行の追完（以下「履行の追完」という。）をすること。なお，契約の相手方は如何なる場合であっても，官側の選択と異なる方法で履行の追完をする場合は，官側の事前の承諾を受けること。

b) 契約相手方は，本業務の契約の履行に必要であると防衛省が承認した場合を除き，情報を役務事務所以外の省外に持ち出してはならない。

c) 契約の相手方は，その具体的な履行の追完の実施方法，完了時期，実施により発生する諸制限事項について，官側と協議し，承諾を得てから履行の追完を実施するものとし，完了時には，その結果について官側の承諾を受けること。

d) 契約の相手方が官側から相当の期間を定めた履行の追完の催告を受けたにもかかわらず，その期限内に履行の追完を実施しない場合，官側は，その不適合の程度に応じて代金の減額を請求することができる。ただし，次に掲げる場合，契約の相手方に対して履行の追完の催告なく，直ちに代金の減額を請求することができる。

1) 履行の追完が不能であるとき。

2) 契約の相手方が履行の追完を拒絶する意思を明確に表示したとき。

3) 本業務の性質又は契約書等の内容により，特定の日時又は一定の期間内に履行をしなければ契約をした目的を達することができない場合において，契約の相手方が履行の追完をしないでその時期を経過したとき。

4) 3)に掲げる場合のほか，前項の催告をしても履行の追完を受ける見込みがないことが明らかであるとき。

10. 再委託

a) 契約相手方は，本業務の実施に当たり，その全部を一括して再委託してはならない。

b) 契約相手方は，本業務の実施に当たり，その一部について再委託を行う場合には，再委託先の事業者名，再委託先に委託する業務の範囲，再委託を行うことの合理性及び必要性，再委託先の履行能力並びに報告徴収，個人情報の管理その他運営管理の方法（以下「再委託先名等」という。）について記載した文書を提出し，官側の承認を受けなければならない。

c) 契約相手方は，契約締結後やむを得ない事情により再委託を行う場合には，再委託先名等

を明らかにした上で，官側の承認を受けなければならない。

d) 契約相手方は，b)又はc)により再委託を行う場合には，契約相手方が官側に対して負う義務を適切に履行するため，再委託先の事業者に対し8.に掲げる事項について，必要な措置を講じさせるとともに，再委託先から必要な報告を聴取しなければならない。

e) b)又はc)に基づき再委託先の事業者に義務を実施させる場合は，全て契約相手方の責任において行うものとし，再委託先の事業者の責に帰すべき事由については，契約相手方の責に帰すべき事由とみなして契約相手方が責任を負うものとする。

f) 契約相手方は，本業務の契約の履行に当たり，第三者を従事させる必要がある場合は，**情報システムの調達におけるサプライチェーン・リスク対応**に関する特約条項に基づき必要な手続きを実施する。

11. 資料の貸与

11.1 設置・調整における貸与

契約相手方は，本業務の実施に当たり必要な官側の保有する資料等について，官側の許可を得た上で，閲覧又は貸与を受けることができる。官側が保有する資料の閲覧又は貸与を受ける場合は，取扱いに留意し，法令及び関連規則等に従い，官側が指定する条件を遵守すること。

12. 官側の支援

12.1 国有財産の利用

契約相手方は，本役務の履行に当たって必要な場合，官側が認める範囲内において，次に示す官側の支援を無償で使用することができる。

a) 現地調査に関する事項

b) 防衛省内における搬入器材の保管

c) 防衛省内における電力，水，スペース等の使用

d) 防衛省内における施設の利用

e) 防衛省内における官側の保有する関連器材の使用

f) 防衛省内の回線

g) 機能確認に関する事前調整及び現地確認時の支援

h) その他，官側が認めた必要な事項

12.2 国有財産の使用制限

a) 契約相手方は，12.1で示す国有財産について，本業務の実施及び実施に付随する業務以外の目的で使用し，又は利用してはならない。

b) 契約相手方は，あらかじめ官側と協議した上で，官側の業務に支障を来さない範囲内において，施設内に本業務の実施に必要な設備等を持ち込むことができる。

c) 契約相手方は，b)で設備等を設置した場合は，設備等の使用を終了又は中止した後，直ちに必要な原状回復を行う。

d) 契約相手方は，既存の建築物，工作物等に汚損，損傷（機器の故障等を含む。以下同じ。）等を与えないよう十分に注意し，損傷が生じるおそれがある場合は，養生を行うものとする。損傷が生じた場合は，契約相手方の責任と負担において速やかに復旧しなければならない。

13. その他特記事項

a) 本業務の推進に当たり，官側の指示に従うとともに，細部にわたり官側と密接な連絡を保ち，作業が良好，かつ安全に実施できるよう努めること。

b) 契約相手方は，本業務契約の履行に当たり，第三者を従事させる必要がある場合には，**情報システムに関する調達に係るサプライチェーン・リスク対応のための措置について（通達）**に定める特約条項を適用する。

c) 引用文書及び関連文書を閲覧する必要が生じた場合は，官側と協議すること。

d) 本仕様書について疑義を生じた場合は，速やかに契約担当官側等と協議すること。

e) 各機関等の長が定めた立入禁止場所等に立ち入る場合は，各機関等の立入手続に従い手続を実施するものとする。

f) 7.に示す提出文書が，**環境物品等の調達の推進に関する基本方針**の基準を満たすものであること。

付図１　全体スケジュール

No	調達件名	令和８年度				令和９年度				令和１０年度				令和１１年度			
		令和８年				令和９年				令和１０年				令和１１年			
		4-6	7-9	10-12	1-3	4-6	7-9	10-12	1-3	4-6	7-9	10-12	1-3	4-6	7-9	10-12	1-3
1	防衛省ＯＡシステム基盤借上（０４増設）	保守															
2	防衛省ＯＡシステム基盤(設置機材の維持管理）（その２）	維持管理															
3	防衛省ＯＡシステム基盤借上（０５増設）	保守															
4	防衛省ＯＡシステム基盤借上（０６増設）	保守															
5	防衛省ＯＡシステム基盤のプロジェクト管理支援役務	プロジェクト管理支援															
6	防衛省ＯＡシステム基盤借上（０７換装）	初度作業			保守												
7	インターネット回線の維持管理役務	維持管理															
8	防衛省ＯＡシステム基盤（設置機材の維持管理）（その４）	維持管理															
9	防衛省ＯＡシステム基盤（設置機材の維持管理）（その３）	維持管理															
10	防衛省ＯＡシステム基盤借上（０３換装）（０７延長）	保守（省ＯＡ分）															
		保守（北関東・九州局ＯＡ															
11	防衛省ＯＡシステム基盤データ移行支援役務（０８移行）	データ移行															
12	防衛省ＯＡシステム基盤運用管理役務(０８運用）		立上		運用												
13	防衛省ＯＡシステム基盤借上（０８増設）		初度作業		保守												
14	北関東・九州局ＯＡシステムデータ移行支援役務		データ移行														
15	インターネット回線の維持管理役務（北関東・九州）		初度作業		維持管理												
16	防衛省ＯＡシステム基盤借上（０４増設）（０８延長）					保守（南関東・沖縄局ＯＡ分）											

付表１ 省ＯＡ機能一覧

No.	系	機能分類	機能名	備考
1	部内	利用者向け	無線ＬＡＮ機能	市ヶ谷LAN設置箇所は対象外
2			メール機能	
3			メール転送機能	
4			利用者向け情報配信機能	
5			インターネットWeb閲覧機能	
6			アカウント管理機能	
7			多要素認証機能	
8			申請管理機能	
9			ファイル共有機能	
10			ファイル検索機能	
11			系間データ移動機能	
12			大容量ファイル転送機能（他府省庁向け）	
13			大容量ファイル転送機能（インターネット向け）	
14			認証印刷機能	
15			外国語翻訳機能	
16			出退表示機能	
17			官品モバイル端末利用機能	
18			テレワーク接続機能	
19			Microsoft 365機能	
20			Microsoft Entra ID	
21			Exchange Online	
22			Microsoft 365 Apps for Enterprise	
23			OneDrive for Business	
24			SharePoint Online	
25			Microsoft 365 Mobile App	
26			Microsoft Forms	
27			Microsoft Teams	
28			Microsoft To Do / Planner / Lists	
29			Power Apps for Office 365	
30			Power Automate	
31			Microsoft Stream	
32			OneNote	
33			Microsoft Loop	
34			Microsoft 365 Copilot	
35			Microsoft 365 CopilotStudio	
36			Power BI	
37		セキュリティ	デバイス制御機能	
38			メールセキュリティ対策機能	
39			クラウドプロキシ機能	
40			Webセキュリティ対策機能	
41			セキュリティパッチ適用機能（Windows）	
42			セキュリティパッチ適用機能（Linux）	
43			エンドポイントセキュリティ機能	
44			端末検疫機能	
45			不正侵入検知・防御（IDS・IPS）機能	
46			統合ログ分析機能	
47			情報漏洩対策（DLP）機能	
48			メール監査機能	
49			Web監査機能	
50			共有フォルダ管理機能	
51			ログ収集機能	
52			セキュリティ運用自動化機能	
53			管理者権限制御機能	
54			ネットワークフォレンジック機能	
55			証明書管理機能	
56			Microsoft365	
57			Data Loss Prevention	
58			Teams Data Loss Prevention	
59			Microsoft Purview Information Protection	
60			Microsoft Purview Insider Risk Management	
61		運用	システム監視機能	
62			インシデント管理機能	
63			構成管理機能	
64			資源配布機能	
65			リモート操作機能	
66			物品管理機能	
67			バックアップ機能	
68			ライセンス認証機能	
69			DNS機能	
70			DHCP機能	
71			NTP機能	
72		共通基盤	集約対象システム向け仮想化基盤管理機能	

73	部外	利用者向け	仮想端末提供機能	
74			アカウント管理機能	
75			系間データ移動機能	
76			多要素認証機能	
77		セキュリティ	デバイス制御機能	
78			セキュリティパッチ適用機能	
79			ログ収集機能	
80			管理者権限制御機能	
81			証明書管理機能	
82		運用	システム監視機能	
83			構成管理機能	
84			資源配布機能	
85			リモート操作機能	
86			バックアップ機能	
87			DNS機能	
88			DHCP機能	
89			NTP機能	
90		共通基盤	集約対象システム向け仮想化基盤管理機能	

付表４ 役務実施週次報告内容

No.		報告内容	報告内容詳細
1		情報セキュリティ管理業務	
	(1)	脆弱性情報管理	脆弱性対応状況の報告　管理表から更新のあったものを報告（新規・継続・クローズ）
			官によるペネトレテスト・脆弱性検査実施後の指摘修正の対応状況（実施後）
			官によるマネジメント監査の支援実施後の指摘修正の対応状況（実施後）
	(2)	不正接続検知	SKYSEAのアラート件数報告（接続元・機器名）
	(3)	端末検疫	ウイルス検知件数
			検知の内容と対処結果
			端末不正接続のアラート報告（接続元・機器名）
			パッチ適用状態検査結果（ポリシー違反）
2		要求実現管理業務	
	(1)	個人アカウント登録・個人端末利用等申請書	申請種別件数
			ステータス別件数
			機関別アカウント登録・変更・削除件数
			機関別端末払出・返却件数
	(2)	共有アカウント登録等申請書	申請種別件数
			ステータス別件数
			機関別共有アカウント登録・変更・削除件数
			部内系DIIメールアドレス作成・削除件数
			階層型アドレス表示登録件数
	(3)	特殊用途端末利用等申請書	申請種別件数
			ステータス別件数
			機関別端末払出・返却件数
	(4)	部外系仮想端末・部外系DIIメールサービス利用等申請書	申請種別件数
			ステータス別件数
			部外系仮想端末登録・変更・削除件数
			部外系DIIメールアドレス登録件数
	(5)	共有メールボックス登録等申請書	申請種別件数
			ステータス別件数
			共有メールボックスの新規作成・変更・削除件数
	(6)	システム連接申請書	申請種別件数
			ステータス別件数
			許可・拒否の件数と設定内容
	(7)	DII提供サービス利用等申請書	申請種別件数
			ステータス別件数
	(8)	組織変更等申請書	申請種別件数
			ステータス別件数
			新規・変更内容詳細
			階層型アドレス表示登録件数
	(9)	機器貸出・増設・移設等申請書	申請種別件数
			ステータス別件数
			機器種別件数
	(10)	官品デバイス利用登録等申請書	申請種別件数
			ステータス別件数
			機器種別件数
	(11)	ソフトウェアインストール申請書	申請種別件数
			ステータス別件数
			インストール詳細（ソフトウェア名・ホスト名）
	(12)	機関共有フォルダ作成等申請書	申請種別件数
			ステータス別件数
			機関別フォルダ作成・変更・削除件数
			機関別アクセス権付与件数
	(13)	Outlook会議室登録等申請書	申請種別件数
			ステータス別件数
	(14)	Web公開サービス利用申請書	申請件数
			ステータス別件数
			申請内容別件数（例：加入システム・各サブディレクトリ）
	(15)	端末持ち出し許可申請書	申請理由別件数
			ステータス別件数
	(16)	機能制限端末払出等申請書	申請理由別件数
			ステータス別件数
	(17)	課室等担当者登録等申請書	申請種別件数
			ステータス別件数
	(18)	機関担当者登録等申請書	申請種別件数
			ステータス別件数
			機関別件数
	(19)	インターネットWeb閲覧ホワイトリスト登録等申請書	申請種別件数
			ステータス別件数
			設定内容（アカウント名、許可・削除のURL、ドメイン）
	(20)	Teams チーム登録等申請書	新規申請件数
			ステータス別件数
	(21)	トナー等消耗品払出依頼（Formsで依頼受付）	申請種別件数
			ステータス別件数
			消耗品別払出件数
	(22)	ICカード発行等申請書	申請種別件数
			ステータス別件数
	(23)	その他依頼等申請書	申請種別件数
			ステータス別件数
			依頼元・実施内容

付表４ 役務実施週次報告内容

No.		報告内容	報告内容詳細
	(24)	Teamsチーム用Sharepoint領域拡張申請書	チーム種別件数（所属組織・個別）
			ステータス別件数
			機関別拡張量
	(25)	S/MIME証明書発行等申請書	発行件数
			ステータス別件数
			メールアドレス種別件数（個人・共有）
	(26)	個人アカウント利用休止申請書	申請種別件数
			ステータス別件数
3		問合せ管理業務	
	(1)	問合せ対応	カテゴリ別・ステータス別件数
4		ハードウェア・ソフトウェア保守管理業務	
	(1)	計画停電対応	計画停電の予定
			計画停電の作業結果
5		インシデント管理業務	
	(1)	インシデント対応	インシデントレベル別発生件数
			インシデント概要と対処状況
			監視（アラート件数）
6		リスク管理業務	
	(1)	リスクと機会の特定・対策の実施	リスクと対策の報告
			管理表から更新のあったものを報告（新規・継続・クローズ）
7		課題管理業務	
	(1)	課題の抽出、対策立案、対応の実施	課題の報告
			管理表から更新のあったものを報告（新規・継続・クローズ）
8		変更管理	
	(1)	システム変更に係る変更・リリース対応	システム変更（変更・リリース対応）の報告
			管理表から更新のあったものを報告（新規・継続・クローズ）
9		その他	
	(1)	次回の開催日を記載	

付表5 役務実施月次報告内容

No.		報告内容	報告内容詳細
1		サービスレベル管理業務	
	(1)	サービスレベル分析・評価・報告	各項目の達成/未達
			未達要因
			是正計画
			前月比較
2		サービス継続性及び可用性管理業務	
	(1)	大規模障害切替訓練	訓練を実施したことを報告（詳細な訓練結果については訓練後に別途報告済）
3		情報セキュリティ管理業務	
	(1)	脆弱性情報管理	脆弱性対応状況の報告　管理表から更新のあったものを報告（新規・継続・クローズ）
	(2)	不正接続検知	SKYSEAのアラート件数
	(3)	端末検疫	ウイルス検知件数
			端末不正接続件数
			パッチ適用状態検査結果（ポリシー違反）件数
	(4)	アカウント・ファイル共有アクセス権の棚卸	棚卸し結果、是正件数
	(5)	特権ID管理（PIM）	承認・却下件数、対象アカウント
	(6)	RMF対応　※年4回程（実施後の月次で報告）	RMFセキュリティ計画書・継続監視計画書・将来対応計画更新結果
			件数・概要
4		要求実現管理業務	
	(1)	個人アカウント登録・個人端末利用等申請書	申請種別件数
			ステータス別件数
			機関別アカウント登録・変更・削除件数
			機関別端末払出・返却件数
	(2)	共有アカウント登録等申請書	申請種別件数
			ステータス別件数
			機関別共有アカウント登録・変更・削除件数
			部内系DIIメールアドレス作成・削除件数
			階層型アドレス表示登録件数
	(3)	特殊用途端末利用等申請書	申請種別件数
			ステータス別件数
			機関別端末払出・返却件数
	(4)	部外系仮想端末・部外系DIIメールサービス利用等申請書	申請種別件数
			ステータス別件数
			部外系仮想端末登録・変更・削除件数
			部外系DIIメールアドレス登録件数
	(5)	共有メールボックス登録等申請書	申請種別件数
			ステータス別件数
			共有メールボックスの新規作成・変更・削除件数
	(6)	システム連接申請書	申請種別件数
			ステータス別件数
			許可・拒否の件数と設定内容
	(7)	DII提供サービス利用等申請書	申請種別件数
			ステータス別件数
	(8)	組織変更等申請書	申請種別件数
			ステータス別件数
			新規・変更内容詳細
			階層型アドレス表示登録件数
	(9)	機器貸出・増設・移設等申請書	申請種別件数
			ステータス別件数
			機器種別件数
	(10)	官品デバイス利用登録等申請書	申請種別件数
			ステータス別件数
			機器種別件数
	(11)	ソフトウェアインストール申請書	申請種別件数
			ステータス別件数
			インストール詳細（ソフトウェア名・ホスト名）
	(12)	機関共有フォルダ作成等申請書	申請種別件数
			ステータス別件数
			機関別フォルダ作成・変更・削除件数
			機関別アクセス権付与件数
	(13)	Outlook会議室登録等申請書	申請種別件数
			ステータス別件数
	(14)	Web公開サービス利用申請書	申請件数
			ステータス別件数
			申請内容別件数（例：加入システム・各サブディレクトリ）
	(15)	端末持ち出し許可申請書	申請理由別件数
			ステータス別件数
	(16)	機能制限端末払出等申請書	申請理由別件数
			ステータス別件数
	(17)	課室等担当者登録等申請書	申請種別件数
			ステータス別件数
	(18)	機関担当者登録等申請書	申請種別件数
			ステータス別件数
			機関別件数
	(19)	インターネットWeb閲覧ホワイトリスト登録等申請書	申請種別件数
			ステータス別件数
			設定内容（アカウント名、許可・削除のURL、ドメイン）

No.		報告内容	報告内容詳細
	(20)	Teams チーム登録等申請書	新規申請件数
			ステータス別件数
	(21)	トナー等消耗品払出依頼（Formsで依頼受付）	申請種別件数
			ステータス別件数
			消耗品別払出件数
			消耗品別の在庫数
	(22)	ICカード発行等申請書	申請種別件数
			ステータス別件数
			ICカードの在庫数
	(23)	その他依頼等申請書	申請種別件数
			ステータス別件数
			依頼元・実施内容
	(24)	Teamsチーム用Sharepoint領域拡張申請書	チーム種別件数（所属組織・個別）
			ステータス別件数
			機関別拡張量
	(25)	S/MIME証明書発行等申請書	発行件数
			ステータス別件数
			メールアドレス種別件数（個人・共有）
	(26)	個人アカウント利用休止申請書	申請種別件数
			ステータス別件数
5		問合せ管理業務	
	(1)	問合せ対応	カテゴリ別・ステータス別件数
			分析や傾向、前月からの推移
	(2)	省OAユーザ支援サイト・共通基盤ポータルサイトの更新	新規登録数（周知・FAQ）
6		システム構成管理業務	
	(1)	システム構成情報の棚卸	棚卸し結果
			是正件数
7		資産管理業務	
	(1)	資産情報の棚卸	棚卸し結果
			是正件数
8		設備管理業務	
	(1)	データセンター入館受付	受付件数
			承認実施件数
9		オペレーション管理業務	
	(1)	地方防衛局の巡回役務　※隔月で報告	実施作業別件数
10		ハードウェア・ソフトウェア保守管理業務	
	(1)	計画停電対応	計画停電件数
11		インシデント管理業務	
	(1)	インシデント対応	インシデントレベル別発生件数
			監視（アラート件数）
12		リスク管理業務	
	(1)	リスクと機会の特定・対策の実施	リスクと対策の報告
			管理表から更新のあったものを報告（新規・継続・クローズ）
13		課題管理業務	
	(1)	課題の抽出、対策立案、対応の実施	課題の報告
			管理表から更新のあったものを報告（新規・継続・クローズ）
14		変更管理	
	(1)	システム変更に係る変更・リリース対応	システム変更（変更・リリース対応）の報告
			管理表から更新のあったものを報告（新規・継続・クローズ）
15		継続的サービス改善管理業務	
	(1)	継続的サービス改善	改善の計画・実績・効果の報告（依頼による改善・運用検討による改善）
		※各運用業務・依頼による改善については本項目で報告	管理表から更新のあったものを報告（新規・継続・クローズ）
16		体制管理報告	
	(1)	体制稼働状況および工数管理	各役務員の勤務時間および役務員全体の作業工数を報告
17		その他	
	(1)	次回の開催日を記載	

付表6 役務実施年次報告内容

No.		報告内容	報告内容詳細
1		情報セキュリティ管理業務	
	(1)	特権ID管理（PIM）	承認・却下件数
	(2)	脆弱性情報管理	脆弱性管理台帳の報告（新規・継続・クローズ）年間総数
	(3)	不正接続検知	SKYSEAのアラート件数
	(4)	端末検疫	ウイルス検知件数
			端末不正接続件数
			パッチ適用状態検査結果（ポリシー違反）件数
2		要求実現管理業務	
	(1)	(1)個人アカウント登録・個人端末利用等申請書	申請種別件数
			ステータス別件数
			機関別アカウント登録・変更・削除件数
			機関別端末払出・返却件数
	(2)	(2)共有アカウント登録等申請書	申請種別件数
			ステータス別件数
			機関別共有アカウント登録・変更・削除件数
			部内系DIIメールアドレス作成・削除件数
			階層型アドレス表示登録件数
	(3)	(3)特殊用途端末利用等申請書	申請種別件数
			ステータス別件数
			機関別端末払出・返却件数
	(4)	(4)部外系仮想端末・部外系DIIメールサービス利用等申請書	申請種別件数
			ステータス別件数
			部外系仮想端末登録・変更・削除件数
			部外系DIIメールアドレス登録件数
	(5)	(5)共有メールボックス登録等申請書	申請種別件数
			ステータス別件数
			共有メールボックスの新規作成・変更・削除件数
	(6)	(6)システム連接申請書	申請種別件数
			ステータス別件数
	(7)	(7)DII提供サービス利用等申請書	申請種別件数
			ステータス別件数
	(8)	(8)組織変更等申請書	申請種別件数
			ステータス別件数
	(9)	(9)機器貸出・増設・移設等申請書	申請種別件数
			ステータス別件数
			機器種別件数
	(10)	(10)官品デバイス利用登録等申請書	申請種別件数
			ステータス別件数
			機器種別件数
	(11)	(11)ソフトウェアインストール申請書	申請種別件数
			ステータス別件数
	(12)	(12)機関共有フォルダ作成等申請書	申請種別件数
			ステータス別件数
			機関別フォルダ作成・変更・削除件数
			機関別アクセス権付与件数
	(13)	(13)Outlook会議室登録等申請書	申請種別件数
			ステータス別件数
	(14)	(14)Web公開サービス利用申請書	申請件数
			ステータス別件数
			申請内容別件数（例：加入システム・各サブディレクトリ）
	(15)	(15)端末持ち出し許可申請書	申請理由別件数
			ステータス別件数
	(16)	(16)機能制限端末払出等申請書	申請理由別件数
			ステータス別件数
	(17)	(17)課室等担当者登録等申請書	申請種別件数
			ステータス別件数
	(18)	(18)機関担当者登録等申請書	申請種別件数
			ステータス別件数
			機関別件数
	(19)	(19)インターネットWeb閲覧ホワイトリスト登録等申請書	申請種別件数
			ステータス別件数
	(20)	(20)Teams チーム登録等申請書	新規申請件数
			ステータス別件数
	(21)	(21)トナー等消耗品払出依頼（Formsで依頼受付）	申請種別件数
			ステータス別件数
			消耗品別払出件数
	(22)	(22)ICカード発行等申請書	申請種別件数
			ステータス別件数
	(23)	(23)その他依頼等申請書	申請種別件数
			ステータス別件数
	(24)	(24)Teamsチーム用Sharepoint領域拡張申請書	チーム種別件数（所属組織・個別）
			ステータス別件数
			機関別拡張量
	(25)	(25)S/MIME証明書発行等申請書	発行件数
			ステータス別件数
			メールアドレス種別件数（個人・共有）

付表6 役務実施年次報告内容

No.		報告内容	報告内容詳細
	(26)	(26)個人アカウント利用休止申請書	申請種別件数
			ステータス別件数
3		問合せ管理業務	
	(1)	問合せ対応	カテゴリ別・ステータス別件数
			1年を通した傾向（繁忙期・特異点）
	(2)	省OAユーザ支援サイト・共通基盤ポータルサイトの更新	新規登録数（周知・FAQ）
4		設備管理業務	
	(1)	データセンター入館受付	受付件数
			承認実施件数
5		オペレーション管理業務	
	(1)	地方防衛局の巡回役務	実施作業別件数
6		ハードウェア・ソフトウェア保守管理業務	
	(1)	計画停電対応	計画停電件数
7		インシデント管理業務	
	(1)	インシデント対応	インシデントレベル別発生件数
			監視（アラート件数）
8		リスク管理業務	
	(1)	リスクと機会の特定・対策の実施	新規の年間総件数
9		課題管理業務	
	(1)	課題の抽出、対策立案、対応の実施	新規の年間総件数
10		変更管理	
	(1)	システム変更に係る変更・リリース対応	新規の年間総件数
11		継続的サービス改善管理業務	
	(1)	継続的サービス改善	年次の総括（実施した改善案概要・満足度アンケート結果）
12		体制管理報告	
	(1)	各役務員の勤務時間および役務員全体の作業工数を報告	役務員の年間工数・体制変動
			工数増大（繁忙期）の要因
			次年度に向けた体制課題
13		次年度運用スケジュール	
	(1)	次年度の運用スケジュールを提示	年間の主要イベント（更新月／棚卸し／点検／訓練など）
			次年度の計画カレンダー

付表７ システム利用状況報告内容

No.	大分類	報告項目	詳細	備考
1	ネットワーク	（市ヶ谷）	通信量	
		政府共通NW向けのトラフィック利用状況	集計した情報を基に傾向分析を実施し、傾向や懸念点を報告	サーバ接続ファイアウォール装置Ⅰ型
		DII向けのトラフィック利用状況		ＤＩＩ接続ファイアウォール装置Ⅰ型
		SASE向けのトラフィック利用状況		ＳＤ－ＷＡＮ接続ファイアウォール装置Ⅰ型
		（第2センター）		
		政府共通NW向けのトラフィック利用状況		ＤＩＩ接続ファイアウォール装置Ⅱ型
		DII向けのトラフィック利用状況		ＤＩＩ接続ファイアウォール装置Ⅱ型
		SASE向けのトラフィック利用状況		ＳＤ－ＷＡＮ接続ファイアウォール装置Ⅱ型
		（各拠点）		
		各拠点からのトラフィック利用状況		DII統合ルータに接続しているスイッチ
		市ヶ谷ー第1センター間の利用状況		
2	スイッチ・ファイアウォール	メモリ	使用率	
	※スイッチは機関向けまで		集計した情報を基に傾向分析を実施し、傾向や懸念点を報告	
3	サーバ・ストレージ装置	CPU	使用率	
		メモリ	集計した情報を基に傾向分析を実施し、傾向や懸念点を報告	
		ストレージ		
4	仮想化基盤	CPU	使用率	
		メモリ	集計した情報を基に傾向分析を実施し、傾向や懸念点を報告	
		ストレージ		
5	クラウド基盤（IaaS）	CPU	使用率	
		メモリ	集計した情報を基に傾向分析を実施し、傾向や懸念点を報告	
		ストレージ		
		Blob		
6	集約対象システム向け仮想化基盤	CPU	使用率	
		メモリ	集計した情報を基に傾向分析を実施し、傾向や懸念点を報告	
		ストレージ		
7	サーバOS	サーバOSセキュリティパッチ適用状況	対象の更新プログラムと適用実施の報告、次月の予定	
8	メール機能	メールボックスの使用容量	しきい値に近い、超えている利用者	
		メールの送受信	部内メールの送受信件数、部外メールの送受信件数	
9	Microsoft 365機能	テナントのリソース状況	ライセンス利用数	
			SharePoint Onlineのサイト単位のストレージ空き容量	
			OneDriveの使用量（上位10までを報告）	
10	Microsoft Teams	チーム用領域の使用容量	チームごとのチームサイトの使用容量（全報告ではなく上位10チーム）	
11	ファイル共有機能	ファイル共有の空き容量	各ドライブ毎の機関別フォルダの使用量・使用率、Azure Filesの全体空き容量	
12	ファイル検索機能	管理者レポート機能	検索件数の推移、検索ワードランキング、ゼロヒット（検索結果0件、キーワード検索元ランキング	
13	物理端末	OSセキュリティパッチ適用状況	適用率、未適用端末の報告	
14	仮想端末	OSセキュリティパッチ適用状況	適用率、未適用端末の報告	
15	複合機・プリンタ・スキャナ	複合機・プリンタの利用状況	機関（課室）ごとの印刷枚数（プリント白黒カラー・コピー白黒カラー・FAX）	
16	資産管理	ライセンス・証明書・プロファイルの利用状況	使用量と残量	
			CipherCraft/Mail 7	
			ARCACLAVIS Ways	
			SPSE PRINT SCOPE クライアントライセンス	
			Veeam Backup for Microsoft 365	
			Microsoft 365 E5	
			Microsoft Teams Premium	
			Microsoft 365 Copilot	
			Microsoft Copilot Studio	
			Microsoft Exchange Online Plan 2	
			Intune Suite	
			S/MIME	
			市ヶ谷LANの証明書　利用数と残数報告	
			11名以上登録されている場合に報告	
			特殊用途端末Ⅰ型のWindows Helloプロファイル	
17	情報保全	メール	監査対象となったメール件数	
			実施結果（承認・否認）	
		ファイルアップロード	監査実施件数、実施結果	
		Teams　ポリシー違反検知・対応	ファイルのアップロード、Teamsネットワークから外部へのアクセス試行状況	
		Web	ブロック数　送信元・宛先URL上位5件	

付表8 月次セキュリティ報告内容

No.		報告内容	報告内容詳細
1		本報告期間におけるセキュリティ状況	
	(1)	本システムのセキュリティ状況について	システムのセキュリティ状態について報告サマリー
2		相関分析における分析結果	
	(1)	相関分析ルールによる検知及び防御状況 分析結果	相関分析ルールによる検知結果サマリー
	(2)	相関分析による結果詳細	フェーズ1：攻撃準備/偵察活動 検知結果サマリー
			フェーズ2：初期侵入 検知結果サマリー
			フェーズ3：端末制御 検知結果サマリー
			フェーズ4：情報探索 検知結果サマリー
			フェーズ5：情報集約 検知結果サマリー
			フェーズ6：情報送出 検知結果サマリー
			フェーズ7：証拠隠滅 検知結果サマリー
			その他 検知結果サマリー
3		検知及び防御製品別 分析結果	
3-1		境界防御関連 検知及び防御状況 傾向分析（インターネット外側[インターネット⇔省内 通信]）	
	(1)	IPS（侵入検知防御サービス 不正侵入検知・防御 Cortex XDR）	分析結果サマリー
			検知及び防御イベント・詳細分析
			(1)Threat:Vulnerability（脆弱性）
			(2)Threat:Virus
			(3)Threat:spyware
	(2)	ファイアウォール（侵入検知防御サービス アクセス制御 Cortex XDR）	分析結果サマリー
			検知及び防御イベント・詳細分析
			(1)ファイアウォールブロックイベント
3-2		境界防御関連 検知及び防御状況 傾向分析（インターネット 内側[インターネット又は政府共通ネットワーク⇔省内 通信]）	
	(1)	ファイアウォール（侵入検知防御サービス アクセス制御 FortiGate）	分析結果サマリー
			検知及び防御イベント・詳細分析
			(1)]ブロック件数
3-3		境界防御関連 検知及び防御状況 傾向分析（政府共通ネットワーク側[政府共通ネットワーク⇔省内 通信]）	
	(1)	IPS（侵入検知防御サービス 不正侵入検知・防御 Cortex XDR）	分析結果サマリー
			検知及び防御イベント・詳細分析
			(1)Threat:Vulnerability（脆弱性）
			(2)Threat:Virus
	(2)	ファイアウォール（侵入検知防御サービス アクセス制御 Cortex XDR）	分析結果サマリー
			(1)ファイアウォールブロックイベント
			検知及び防御イベント・詳細分析
3-4		メール関連 検知及び防御状況 傾向分析	
	(1)	マルウェア対策（メール Exchange Online Protection）	分析結果サマリー
			検知及び防御イベント・詳細分析
			(1)メール経路上でのマルウェア検知件数
			(2)フリーメールドメインへのメール転送状況
	(2)	サンドボックスによるマルウェア対策	分析結果サマリー
			検知及び防御イベント・詳細分析
			(1)サンドボックスによるマルウェア検知件数
	(3)	メールストア上でのマルウェア対策	分析結果サマリー
			検知及び防御イベント・詳細分析
			(1)メールストア上でのマルウェア検知件数
	(4)	不審メール通報機能により提出されたメールの解析状況	分析結果サマリー
			検知及び防御イベント・詳細分析
3-5		Web関連 検知及び防御傾向分析（インターネット側[インターネット⇔省内 通信]）	
	(1)	マルウェア対策（インターネット（WEB分離））	分析結果サマリー
			検知及び防御イベント・詳細分析
			(1)マルウェア検知件数
			(2)サンドボックスによるマルウェア検知件数
	(2)	セキュアブラウザサービス（Revo Works Browser）	分析結果サマリー
			検知及び防御イベント・詳細分析
			(1)RWBによるマルウェア検知件数
3-6		Web関連 検知及び防御傾向分析（政府共通ネットワーク側[政府共通ネットワーク⇔省内 通信]）	
	(1)	マルウェア対策（政府共通）	分析結果サマリー
			検知及び防御イベント・詳細分析
3-7		SASE関連 検知及び防御傾向分析	
	(1)	Cisco Secure Acsess	分析結果サマリー
			検知及び防御イベント・詳細分析
			(1)不正アクセス・侵害の検知状況
			(2)クラウド／リモート環境におけるユーザー行動の失敗・不審行動
			(3)ポリシー逸脱・設定ミスの検出
3-8		端末及びサーバ関連 検知及び防御傾向分析	
	(1)	マルウェア対策（端末・サーバ）	分析結果サマリー
			検知及び防御イベント・詳細分析
			(1)端末及び物理サーバマルウェア検知件数（Cortex XDR）
			(2)ファイル共有 マルウェア検知件数
			(3)エンドポイント挙動監視・インシデント対応機能（Cortex XSIAM）
	(2)	マルウェア対策（仮想デスクトップ Cortex XDR Agent）	分析結果サマリー
			検知及び防御イベント・詳細分析
			(1)マルウェア検知件数
	(3)	環境における挙動・不審な操作	分析結果サマリー
			不正端末検知サマリー
			不審アプリケーション関連サマリー
3-9		DDoS攻撃対策関連 検知及び防御傾向分析	
	(1)	DDoS攻撃対策機能	分析結果サマリー
			検知及び防御イベント・詳細分析
3-10		Microsoft Teams関連 検知	
	(1)	検知イベント一覧	検知イベントサマリー
			認証・アカウント監視サマリー
			Teams操作・利用行動の監視サマリー
			外部連携・ゲストアクセス監視サマリー
			アプリ・Bot・コネクタ監視サマリー
			設定変更・管理操作監視サマリー
			DLP・情報漏えい監視サマリー
			マルウェア／フィッシング監視サマリー
4		セキュリティインシデント対応状況	
	(1)	インシデント対応状況サマリー	セキュリティ対策製品検知イベント起点によるインシデント対応サマリー
			NOC起点によるインシデント対応サマリー
			その他の報告起点によるインシデント対応サマリー
			セキュリティトピックスサマリー
5		リスク評価サマリー	
	(1)	リスク評価サマリー	対象とする個所
			リスク分析内容
			分析結果サマリー
			対応方針
6		脆弱性対応関連	
	(1)	当月の脆弱性情報状況サマリー	リスク評価実施時の脆弱性対象への対応
			定期的な脆弱性情報からの適用対象外及びパッチ適用対象サマリー
			当月の対応状況(SOCとしての視点で検知・評価・指示の状況)　具体的な対応についてはシステム運用側で報告
			対象への未適用時評価・見解
7		管理者関連	
	(1)	システム管理者に対するサマリー	検知状況サマリー
			不審挙動監視サマリー
			権限操作系サマリー
			ポリシー違反サマリー
8		セキュリティトピックス	
	(1)	最新のセキュリティ状況	セキュリティに関する最新の話題など
9		その他	
	(1)	その他	その他特記事項

付表9 運用業務一覧
運用業務一覧

No.	業務項目			実施時期		運用形態	運用環境	関係者												関連ドキュメント	
								官					08運用事業者				その他事業者				
	区分	業務名	業務概要	頻度	時期等補足	運用形態（オンサイト／リモート）	運用環境（通常環境／災対環境）	他システム担当者（A）	システム管理者（B）	機関等担当者・地方防衛局担当者（C）	課室等担当者（D）	省OA利用者（E）	運用業務実施責任者（F）	システム運用担当者（G）	SOC担当者（H）	CSIRT担当者（I）	保守事業者（J）	データセンタ事業者（K）	業務フロー	関連ドキュメント
1	サービスレベル管理	サービスレベル分析・評価・報告	定められたサービスレベル（問合せ対応率、申請依頼に対する対応率、障害通知時間、システム稼働率等）について、測定、評価して目標値に対する達成状況を確認、月次および年次報告にてシステム管理者へ報告する。	月次	－	オンサイト	通常環境		□				●	○			△		サービスレベル分析・評価・報告	月次報告書
2	サービス継続性及び可用性管理	大規模障害対応	メインサイトが災害や大規模障害により機能不全に陥り、容易に復旧ができない場合に、バックアップサイトへ切替を行うことでシステム稼働の継続を図る。	随時	－	オンサイト	通常環境	□	□	□	□	□	●	○	△	△	△	△	大規模障害対応	復旧計画
3		大規模障害切替訓練	大規模障害（災害）が発生した際のシステム切り替え作業等について有事の際に滞りなく対応が行えるようにするため、平時のうちに「訓練」として手順や連絡体制を確認することで、運用員の業務習熟と問題点の改善を図る。	年次	－	オンサイト	通常環境		□				●	○	△		△		大規模障害切替訓練	大規模障害切替訓練計画 訓練実施報告書
4	情報セキュリティ管理	アカウント・ファイル共有アクセス権の棚卸	人事異動等に伴う不要アカウントや不要ライセンスを排除し、適正なアカウント状態を維持するとともに、共有フォルダのセキュリティグループに属するアカウントの妥当性を確認する。	年次	－	オンサイト	通常環境		△	△	△		●	○	△		△		アカウント・ファイル共有アクセス権の棚卸	棚卸結果報告書
5		リスク管理枠組み情報提供支援	RMFのセキュリティ計画書に定義された各要求項目のうち運用での対応とされている項目の対応について、各要求項目ごとに定義された頻度に従い、その実施状況を確認、評価する。実施が不十分と判断された項目について、将来対応計画書へ起票しセキュリティ管理策の実装計画を検討する。	－	管理策ごとに定めた頻度で実施	オンサイト	通常環境	□	□				●	○	△		△		リスク管理枠組み情報提供支援	セキュリティ計画書 継続監視計画書 将来対応計画書
6		官によるペネトレーションテスト・脆弱性検査の支援	官によるペネトレーションテスト・脆弱性検査として実際のサイバー攻撃を模擬してシステムへの侵入を試み、具体的な弱点（脆弱性）の発見、セキュリティ対策の有効性評価、および攻撃による被害範囲の特定が行われる。指摘事項に対する対応方針の検討、対応について、運用観点での支援を行う。	随時	－	オンサイト	通常環境	□	□				●	○	△		△		官によるペネトレーションテスト・脆弱性検査の支援	ペネトレ検査のヒアリングシート
7		官によるマネジメント監査の支援	「政府機関等のサイバーセキュリティ対策のための統一基準群」に基づく施策の取り組み状況について、NCOマネジメント監査にて検証し、改善のために必要な助言が行われる。指摘事項への対応について、運用観点での支援を行う。	随時	－	オンサイト	通常環境	□	□				●	○	○		○		官によるマネジメント監査の支援	質問管理表 指摘対応結果報告
8	要求実現管理	個人アカウント登録・個人端末利用等申請書	個人アカウントの新規作成、情報の変更・削除、個人端末の貸与・返却が必要となる場合に実施される申請。アカウントに関する処理は申請管理機能により実施される。端末の払出や返却の対応を実施する。	随時	－	オンサイト	通常環境		□	□	□			○					個人アカウント登録・個人端末利用等申請書	
9		共有アカウント登録等申請書	共有アカウントの新規作成、情報の変更、削除が必要となる場合に実施される申請。アカウントに関する処理は申請管理機能により実施される。	随時	－	オンサイト	通常環境		□	□	□			○					共有アカウント登録等申請書	
10		特殊用途端末利用等申請書	特殊用途端末Ⅰ型またはⅡ型の貸与・返却が必要な場合に実施される申請。端末の払出や返却の対応を実施する。	随時	－	オンサイト	通常環境		□	□	□			○					特殊用途端末利用等申請書	
11		部外系仮想端末・部外系DIIメールサービス利用等申請書	部外系仮想端末の貸与・返却が必要な場合に実施される申請。部外系仮想端末の払出や返却、部外系DIIメールサービスの代理申請、メールアカウントの受領、払出や返却をセットで実施する。	随時	－	オンサイト	通常環境		□	□	□			○					部外系仮想端末・部外系DIIメールサービス利用等申請書	
12		共有メールボックス登録等申請書	共有メールボックスの新規作成、利用者の追加、削除が必要となる場合に実施される申請。Exchange Online上で共有メールボックスの作成や削除、設定変更を実施する。	随時	－	オンサイト	通常環境		□	□	□			○					共有メールボックス登録等申請書	
13		システム連接申請書	省OAの端末から連接システム等を利用したい場合に、必要に応じて実施される申請。ファイアウォール装置の設定変更など、NWの変更が必要な場合に本申請で依頼を受け付け必要な対応を検討、実施する。	随時	－	オンサイト	通常環境		□	□	□		●	○	△	△	△		システム連接申請書	システム連接設定作業計画 システム設定書（パラメータシート）
14		DII提供サービス利用等申請書	DII提供サービスの「省外とのテレビ電話サービス」を新規に利用開始または利用終了したい場合に実施される申請。申請されたアカウントが「省外とのテレビ電話サービス」を利用できるように設定変更を実施する。	随時	－	オンサイト	通常環境		□	□	□			○					DII提供サービス利用等申請書	ライセンスの管理台帳
15		組織変更等申請書	組織変更による新規組織（課室等）の設置、既存組織の名称の変更、既存組織の廃止等があった場合に実施される申請。部署共有フォルダの作成、階層型アドレス帳の組織階層の修正、Teamsの組織チーム作成を実施する。	随時	－	オンサイト	通常環境	△	□	□	□			○					組織変更等申請書	
16		機器貸出・増設・移設等申請書	省OA調達の機器の貸出、増設、返却、移設が必要となる場合に実施される申請である。端末周辺機器（モニタ、キーボード、ICカードリーダ）、ネットワークスイッチ、無線LANアクセスポイント、プリンタ類（複合機、プリンタ、スキャナ）が対象となる。	随時	－	オンサイト	通常環境		□	□	□			○					機器貸出・増設・移設等申請書	配線図 フロア図

No.	業務項目			実施時期		運用形態	運用環境	関係者											関連ドキュメント	
								官					08運用事業者				その他事業者			
	区分	業務名	業務概要	頻度	時期等補足	運用形態（オンサイト／リモート）	運用環境（通常環境／災対環境）	他システム担当者（A）	システム管理者（B）	機関等担当者・地方防衛局担当者（C）	課室等担当者（D）	省ＯＡ利用者（E）	運用業務実施責任者（F）	システム運用担当者（G）	ＳＯＣ担当者（H）	ＣＳＩＲＴ担当者（I）	保守事業者（J）	データセンタ事業者（K）	業務フロー	関連ドキュメント
17	要求実現管理（続き）	官品デバイス利用登録等申請書	機関や課室で購入した機器（官品プリンタ、官品スキャナ等）や官品デバイス（USBメモリ、SDカード等）を、省OAに接続するための登録、解除をおこなうための申請。申請者が持ち込んだUSB接続機器を登録、管理シールを貼付する。持ち込み不可の場合、SDカード以外はリモートで対応する。ネットワーク接続機器はIPアドレス、管理シールを払出し、許可設定する。	随時	－	オンサイト	通常環境		□	□	□	△		○					官品デバイス利用登録等申請書	
18		ソフトウェアインストール申請書	省OA端末に標準でインストールされていないソフトウェアのインストール、アンインストール、バージョンアップが必要となる場合に実施される申請。申請者にてインストーラファイルや手順書を所定のパスに格納、関係者含め調査・検討し、承認された場合、リモートでインストールを実施する。	随時	－	オンサイト	通常環境		□	□	□		△	○	△	△	△		ソフトウェアインストール申請書	
19		機関共有フォルダ作成等申請書	「000_機関共有 」フォルダ（端末のVドライブにマウント）の直下に特定のシステム利用者のみがアクセス可能な共有フォルダを作成、変更、削除する場合に実施される申請。アクセスを許可するアカウントのセキュリティグループを作成、共有フォルダを作成、アクセス権を付与する。	随時	－	オンサイト	通常環境		□	□	□			○					機関共有フォルダ作成等申請書	
20		Outlook会議室登録等申請書	Outlook会議室の新規作成、情報変更、削除する場合に実施される申請。本申請をもとに省OAのExchange Online上に会議室（リソースメールボックス）を作成する。	随時	－	オンサイト	通常環境		□	□	□			○					Outlook会議室登録等申請書	
21		Web公開サービス利用申請書	DII提供サービスの「Web公開サービス」を代理申請を依頼したい場合に実施される申請。申請者にてWeb公開サービス利用申請様式（Excel）に必要事項を入力、提出、その申請様式をDIIへ代理申請する。	随時	－	オンサイト	通常環境	△	□	□	□			○					Web公開サービス利用申請書	
22		端末持ち出し許可申請書	省OA端末を省外に持ち出す（テレワーク、出張等）場合に実施される申請。	随時	－	オンサイト	通常環境		□	□	□			○					端末持ち出し許可申請書	
23		機能制限端末払出等申請書	出張先の国が特定の注意が必要な国である各機関にて判断される場合に利用する、機能制限端末を払い出す場合に実施される申請。端末・ローカルアカウントの準備、利用者から共有されたファイルの格納、払出を実施する。返却時にはファイルの取り出し、受け渡しを実施する。	随時	－	オンサイト	通常環境		□	□	□	△		○					機能制限端末払出等申請書	
24		課室等担当者登録等申請書	課室担当者を新規登録、削除する場合に実施される申請。課室担当者に必要な権限の付与、課室担当者一覧の更新を実施する。	随時	－	オンサイト	通常環境		□	□	□			○					課室等担当者登録等申請書	
25		機関担当者登録等申請書	機関担当者を新規登録、削除する場合に実施される申請。課室担当者に必要な権限の付与、機関担当者一覧の更新を実施する。	随時	－	オンサイト	通常環境		□	□	□			○					機関担当者登録等申請書	
26		インターネットWeb閲覧許可申請書	Web監査機能にて閲覧不可とするカテゴリのうち、特定のサイトをホワイトリストに登録して閲覧可能にする場合に実施される申請。申請内容について関係者含め調査・検討し、承認された場合、ホワイトリストの登録、パラメータシートの更新を実施する。	随時	－	オンサイト	通常環境		□	□	□		△	○	△	△	△		インターネットWeb閲覧許可申請書	システム設定書（パラメータシート）
27		Teams チーム登録等申請書	組織のTeamsチーム以外の、プロジェクト管理や情報共有の目的で利用する個別のTeamsチームを作成する場合に実施される申請。Teamsチームの作成は申請管理機能により自動で実施される。	随時	－	オンサイト	通常環境		□	□	□			○					Teams チーム登録等申請書	
28		ICカード発行等申請書	特殊用途端末Ⅱ型のログイン認証に使用するログイン専用ICカードを新規発行、再発行、返却する場合に実施される申請。ICカードの払出を実施する。在庫が少なくなっている場合はシステム管理者へ補充依頼を実施する。	随時	－	オンサイト	通常環境		□	□	□			○					ICカード発行等申請書	
29		Teamsチーム用SharePoint領域拡張申請書	Teamsのチームに紐づくSharePoint領域を拡張する場合に実施される申請。申請内容に基づき、拡張作業を実施する。	随時	－	オンサイト	通常環境		□	□	□			○					Teamsチーム用Sharepoint領域拡張申請書	
30		S/MIME証明書発行等申請書	外部にメールを送信する際に使用するS/MIME証明書を発行する場合に実施される申請。申請管理機能により自動で処理が実施され、利用者に証明書発行用のメールが送付される。	随時	－	オンサイト	通常環境		□	□	□			○					S/MIME証明書発行等申請書	

No.	業務項目			実施時期		運用形態	運用環境	関係者												関連ドキュメント	
								官					08運用事業者				その他事業者				
	区分	業務名	業務概要	頻度	時期等補足	運用形態（オンサイト／リモート）	運用環境（通常環境／災対環境）	他システム担当者（A）	システム管理者（B）	機関等担当者・地方防衛局担当者（C）	課室等担当者（D）	省ＯＡ利用者（E）	運用業務実施責任者（F）	システム運用担当者（G）	ＳＯＣ担当者（H）	ＣＳＩＲＴ担当者（I）	保守事業者（J）	データセンタ事業者（K）	業務フロー	関連ドキュメント
31	要求実現管理（続き）	個人アカウント利用休止申請書	育休や休職などにより、長期間本システムを利用しない個人アカウントを利用休止・復帰する場合に実施される申請。申請内容に基づき適用希望日に個人アカウントの無効化（ロックアウト）、有効化を実施する。	随時	－	オンサイト	通常環境		□	□	□			○					個人アカウント利用休止申請書	
32		監査担当者登録等申請書	監査担当者を新規登録、削除する場合に実施される申請。問合せとして依頼を受け付ける。監査担当者に必要な権限の付与、課室担当者一覧の更新を実施する。	随時	－	オンサイト	通常環境	□	□					○					監査担当者登録等依頼	
33		トナー等消耗品払出申請	トナー等の、プリンタに関連する各種消耗品の払出が必要な場合に実施される依頼。依頼をFormsにより受け付け、払出日次の調整、払出を実施する。在庫が少ない場合にはシステム管理者へ補充を依頼する。本依頼は内部部局からのみ受け付ける。	随時	－	オンサイト	通常環境		□		□	□		○					トナー等消耗品払出依頼	
34		申請ワークフロー新規作成	利用者の問合せ状況・件数やシステム管理者からの指示に基づき、利用者利便性向上や運用業務効率化のため、専用の申請ワークフローを新たに作成する。定期的に省OA利用者からの問合せ状況等を鑑み、新規申請ワークフロー化の検討を行う（年2回程度を想定）。また、システム管理者から新規ワークフロー作成の追加指示を受けた際に随時検討を行う。	随時	年2回の検討 加えて依頼に基づき随時検討	オンサイト	通常環境		□			□	●	○			○		申請ワークフロー新規作成	変更管理台帳
35	問合せ管理	問合せ対応	インシデント管理機能のWebフォームより省OA利用者等からの問合せを受け付け、回答する。障害により端末やインシデント管理機能が利用できない場合や、省OA端末を利用していない、省OAシステム基盤利用者からの問合せはメールで受け付ける。	随時	－	オンサイト	通常環境	□	□	□	□	□	●	○	△		△		問合せ対応	
36		省OAユーザ支援サイト・共通基盤ポータルサイトの更新	情報掲載等の各種更新やナレッジの更新依頼、障害情報の共有を基に省OAユーザ支援サイト及び共通基盤ポータルサイトを更新する。	随時	－	オンサイト	通常環境	□	□	□	□	□	●	○	□		□		省OAユーザ支援サイト・共通基盤ポータルサイトの更新	週次報告書 月次報告書
37	システム構成管理	システム構成情報の棚卸	システム構成情報と実態の差異を定期的に確認し、反映、報告する。システム構成書、システム設定書、構成図、NW機器の設定ファイルは、変更管理台帳をもとに、運用および保守が実施した変更が反映されていることを確認する。ケーブル配線図は、課室等担当者に変更の有無の確認と、差分があれば更新を依頼する。	年次	－	オンサイト	通常環境		□	△			●	○			△		システム構成情報の棚卸	変更管理台帳 月次報告書
38	資産管理	資産情報の棚卸	システム構成情報と実態の差異を定期的に確認し、反映、報告する。借上品や官品のハードウェアについては、申請管理機能、物品管理機能、構成管理機能と実態の差異を確認する。運用で保管する在庫は運用で確認し、払出済みの機器は機関担当者等に確認を依頼する。ソフトウェアについては、ライセンスの超過の有無、原因の分析、是正対応を実施する。	年次	－	オンサイト	通常環境		□	△			●	○					資産情報の棚卸	棚卸結果報告書
39	キャパシティ管理（容量・能力管理）	システムリソース利用状況の分析・評価	システムリソースの利用状況を日次で監視し、データを収集、評価、報告、必要に応じて保守へエスカレーションする。サーバ類のCPU使用率、メモリ使用率、ディスク使用容量、ディスクI/O、主要なネットワーク境界に設置されたファイアウォール装置のトラフィックを監視する。	日次	－	オンサイト	通常環境							○				△		システムリソース利用状況の分析・評価	システム利用状況報告書
40	設備管理	データセンター入館受付	第1センター及び第2センターの入館申請に対し代理承認、代理申請を実施する。	随時	－	オンサイト	通常環境						○	□			□		データセンター入館受付	入館申請台帳
41	オペレーション管理	地方防衛局の巡回役務	保守事業者にて修理済みの端末のキッティング、リモートでの実施が不可のSDカードの登録、申請により払い出した機器や返却された機器の在庫状況の確認を実施する。隔月で本局および支局、加えて修理済み機器のあるその他拠点を訪問する。	隔月	－	オンサイト	通常環境		□	□			□	○			△		地方防衛局の巡回役務	現地対応作業報告書
42	データバックアップ・リストア管理	バックアップ取得状況の確認	想定外のバックアップ失敗が発生した際にも早期の対処を図るため、自動実行されるバックアップジョブの成否の確認を日次で実施する。	日次	－	オンサイト	通常環境							○					バックアップ取得状況の確認	

運用業務一覧（続き）

No.	業務項目			実施時期		運用形態	運用環境	関係者												関連ドキュメント	
								官					08運用事業者				その他事業者				
	区分	業務名	業務概要	頻度	時期等補足	運用形態（オンサイト／リモート）	運用環境（通常環境／災対環境）	他システム担当者（A）	システム管理者（B）	機関等担当者・地方防衛局担当者（C）	課室等担当者（D）	省ＯＡ利用者（E）	運用業務実施責任者（F）	システム運用担当者（G）	ＳＯＣ担当者（H）	ＣＳＩＲＴ担当者（I）	保守事業者（J）	データセンタ事業者（K）	業務フロー	関連ドキュメント
43	ハードウェア・ソフトウェア保守管理	予防運用・保守管理（ランプチェック）	市ヶ谷、第1センター、第2センターのサーバー室に設置された省OA機器の正常性確認を実施するため、ランプチェックを実施する。	日次	－	オンサイト	通常環境						●	○					ランプチェック	
44		計画停電対応	市ヶ谷庁舎や各通信所、駐屯地等における計画停電が行われる際に、計画停電の予定を把握し、ユーザ支援サイトへの掲載、監視の静観対応、復電後の動作確認、結果のとりまとめ、運用状況報告での報告を実施する。	随時	－	オンサイト	通常環境		□	□	□		●	○					計画停電対応	週次報告書 月次報告書
45	インシデント管理	インシデント対応	インシデント発生時における、影響度合いの調査や復旧にかかる各作業、随時タイミングの状況報告などの諸対応を実施する。	随時	－	オンサイト	通常環境	□	□	□	□	□	●	○	△	△	○		インシデント対応	変更管理台帳 構成管理台帳
46	リスク管理	リスクと機会の特定・対策の実施	想定されるリスクとそのリスクが起こり得るタイミングの特定と対策、および経過観察を実施する。	随時	－	オンサイト	通常環境		□				●	○	△	△	△		リスクと機会の特定・対策の実施	
47	課題管理	課題の抽出、対策立案、対応の実施	問題発生時の課題の整理と抽出、抽出した課題の立案と対応を実施する。	随時	－	オンサイト	通常環境		□				●	○	△	△	△		課題の抽出、対策立案、対応の実施	
48	変更管理	標準変更	定常作業にて実施する事前承認された変更で、追加の承認を必要とせずに作業を実施する。	随時	－	オンサイト	通常環境		□					○					システム変更に係る変更・リリース対応	
49		通常変更	サービスの停止および省OA全体に影響がある変更で、標準変更と緊急変更以外の変更を指す。通常変更は、変更手順の検討、検証環境での適用、変更策の策定を実施しシステム管理者に確認を依頼する。承認を得られた場合、変更策を実施、動作確認、完了報告を実施する。	随時	－	オンサイト	通常環境		□				●	○			○		システム変更に係る変更・リリース対応	
50		緊急変更	システム管理者等からの緊急対応依頼や、重大なインシデント障害対応における暫定対処を実施する場合の変更で、緊急変更も適用後のリスクは十分に検証を行った上でリリースを行う方針とする。ただし、緊急性に応じて検証の範囲や変更予定日等はシステム管理者と協議の上、決定する。	随時	－	オンサイト	通常環境		□				●	○			○		システム変更に係る変更・リリース対応	
51	リリース・展開管理	リリース対応	変更管理で承認された変更策を、本番環境へ安全かつ確実に展開するために、準備や承認、展開の一連の活動を実施する。	随時	－	オンサイト	通常環境		□				●	○			○		システム変更に係る変更・リリース対応	
52	継続的サービス改善管理	継続的サービス改善	運用業務の品質向上のため、継続的に業務改善を実施する。改善アイディアの発案、収集から、改善提案の内容検討、改善計画の検討、実行、結果報告までを実施する。	随時	－	オンサイト	通常環境		□				●	○	○	○			継続的サービス改善	
53	ナレッジ管理	ナレッジの収集、分析・抽出、報告、活用	インシデント管理等で蓄積した運用業務対応履歴を精査・検討のうえで選抜し、ナレッジとして登録・活用することで、運用業務の効率化を図る。また、問合せ内容から件数の多いものや、その他、有用と判断したものを利用者向けのQ&Aとして公開することで、利用者の利便性向上を図る。	随時	－	オンサイト	通常環境						●	○					ナレッジの収集、分析・抽出、報告、活用	
54	コミュニケーション管理	週次運用状況報告	週次での運用業務の実施状況を正確に把握し報告するために、1週間分の運用業務の実績を収集、精査し、週次運用状況報告書の作成、共有、報告を実施する。	週次	－	オンサイト	通常環境		□				●	○					週次報告書作成	週次報告書
55		月次運用状況報告	月次での運用業務の実施状況を正確に把握し報告するために、1か月分の運用業務の実績を収集、精査、分析し、問合せの傾向、S10の達成状況などの分析項目を含めた、月次運用状況報告書の作成、共有、報告を実施する。	月次	－	オンサイト	通常環境		□				●	○					月次報告書作成	月次報告書
56		年次運用状況報告	年次での運用業務の実施状況を総合的に把握し報告するために、1年分の運用業務の実績を収集、精査したうえで、課題および翌年度に向けた改善施策を取りまとめ、年次運用状況報告書の作成、共有、報告を実施する。	年次	－	オンサイト	通常環境		□				●	○					年次報告書作成	年次報告書
57		システム利用状況報告	利用者によるシステム利用状況を把握し報告するために、1か月分のシステム利用情報を収集、精査し、システム利用状況報告書の作成、共有、報告を実施する。	月次	－	オンサイト	通常環境		□				●	○			△		システム利用状況報告書	システム利用状況報告書

No.	業務項目			実施時期		運用形態	運用環境	関係者												関連ドキュメント	
								官					08運用事業者				その他事業者				
	区分	業務名	業務概要	頻度	時期等補足	運用形態（オンサイト／リモート）	運用環境（通常環境／災対環境）	他システム担当者（A）	システム管理者（B）	機関等担当者・地方防衛局担当者（C）	課室等担当者（D）	省ＯＡ利用者（E）	運用業務実施責任者（F）	システム運用担当者（G）	ＳＯＣ担当者（H）	ＣＳＩＲＴ担当者（I）	保守事業者（J）	データセンタ事業者（K）	業務フロー	関連ドキュメント
58	セキュリティ運用	セキュリティ監視と検知	各種セキュリティ機能からのアラートをトリガーとして、脅威レベルの確認、検知背景の確認によるアラートの正当性判断、検知内容・事象確認を実施し、インシデント判定を実施する。必要に応じて、検体ファイルを取得し危険性の有無について分析を実施する。セキュリティインシデントと判定されたものは対処に進む。	随時	24時間365日	オンサイト	通常環境		□	△	△	△	□	△	○	○			セキュリティ監視と検知	変更管理台帳 構成管理台帳
59		セキュリティインシデント対応	セキュリティ監視やシステム監視、セキュリティイベントの分析、官からの連絡により発覚したセキュリティインシデントについて、初動対応を実施し、続けて封じ込めを検討、実施、駆除・復旧を検討、実施する。インシデントが解消した後、再発防止策を検討、実施する。	随時	－	オンサイト	通常環境	△	□	△	△	△	●	△	○	○			セキュリティインシデント対応	セキュリティインシデント報告書
60		脅威・脆弱性管理	脆弱性情報の定期的な収集、定期リスク診断から導出された脆弱性情報をもとに、それぞれに脆弱性について分析、評価、対応方針の検討を実施する。検討した方針に従い、検証環境での適用、本番環境への適用を実施する。	随時	定期的な脆弱性情報の収集は週次、緊急の対応は随時	オンサイト	通常環境		□				●	○	△	△			脅威・脆弱性管理	変更管理台帳
61		月次セキュリティ報告	月次での、脅威検知や防御の状況、ログ分析の結果、セキュリティインシデントの対応状況を報告する。攻撃深度を表す「フェーズ」ごとの相関分析の結果、セキュリティ製品やシステム境界ごとの傾向分析の結果、トリガーごとのセキュリティインシデントの対応状況を報告に含める。	月次	－	オンサイト	通常環境		□				●		○	○			月次セキュリティ報告	月次セキュリティ報告書
62		定期SIEM分析	リアルタイム監視では見落とされる可能性のある複合的な不審な兆候を特定するために、ログに対して定期的にフィルターを適用し脅威の検出の有無を確認する。検出に対して検知背景の確認による正当性判断、検知内容・事象確認を実施し、インシデント判定を実施する。必要に応じで、追加のヒアリングやログ確認を実施する。セキュリティインシデントと判定されたものは対処に進む。	日次	－	オンサイト	通常環境		□				□	△	○	○			定期SIEM分析	変更管理台帳 構成管理台帳
63		システムリスク評価とセキュリティ教育	定期的なリスク評価を行い、システムの構成に対する評価や更新の必要性を確認する。また、職員のセキュリティ意識の向上のため、セキュリティ教育計画やポリシーの見直しを実施する。	－	リスク評価は半年に1回 セキュリティ教育は省OA利用開始時と4半期に1回	オンサイト	通常環境		□				●		△	○			システムリスク評価 セキュリティ教育	

●:責任者　○:主担当　□:報告先、依頼元　△:支援

付表9　運用業務一覧
【参考】申請及び問い合わせ件数

（業務実施状況）　（件）

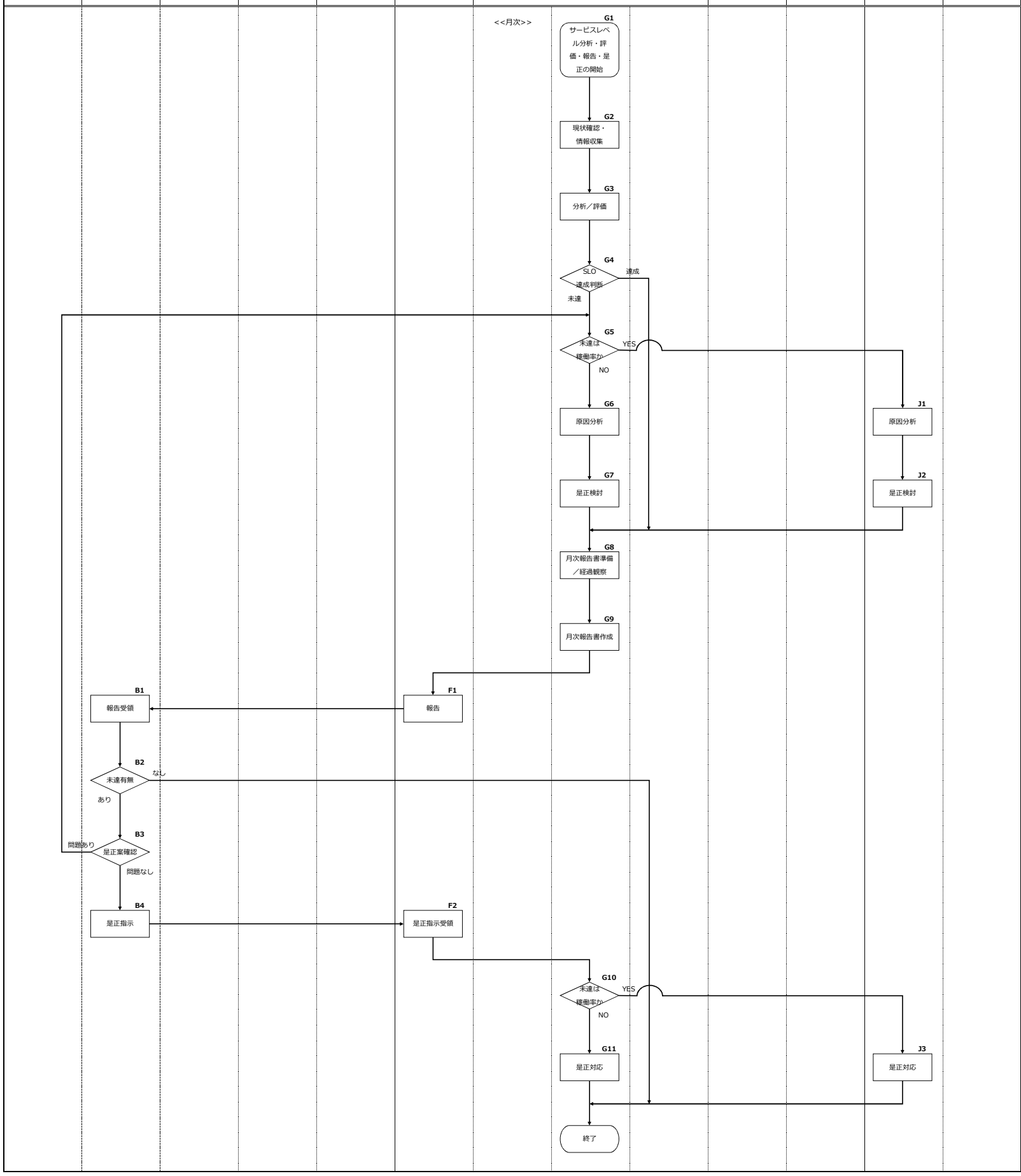
令和7年度		4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	計
申請件数	03換装	3751	2316	1974	2678	2800	1610	1638	1680	1283	1224	1760	5122	27836
	04増設													0
	05増設基盤(IaaS基盤)	0	1	0	0	0	0	0	1	0	1	1	0	4
	05端末増設	80	77	81	61	70	76	62	101	104	53	57	441	1263
	06増設													0
	Teams維持管理	255	119	335	289	316	201	162	163	109	162	147	342	2600
問い合わせ件数	03換装	3242	1640	1818	1607	2014	1381	1395	1798	1256	1458	1537	1833	20979
	04増設													0
	05増設基盤(IaaS基盤)	9	11	6	8	8	6	4	10	7	8	10	7	94
	05端末増設	104	63	61	65	58	45	46	66	38	57	73	57	733
	06増設													0
	Teams維持管理	358	156	392	300	341	243	256	176	105	147	124	217	2815

（注記事項）
・「04増設」「06増設」（基盤のみ）については、対応する事業が存在しないため、お問い合わせや申請が発生した場合は「03換装」のお問い合わせとして扱い、申請件数に合算されております。
・「05増設」は「05増設基盤」と「05端末増設」に分けて対応しているため、それぞれの件数に分割しております。

（注記事項）

付表１０　業務フロー
サービスレベル分析・評価・報告・是正

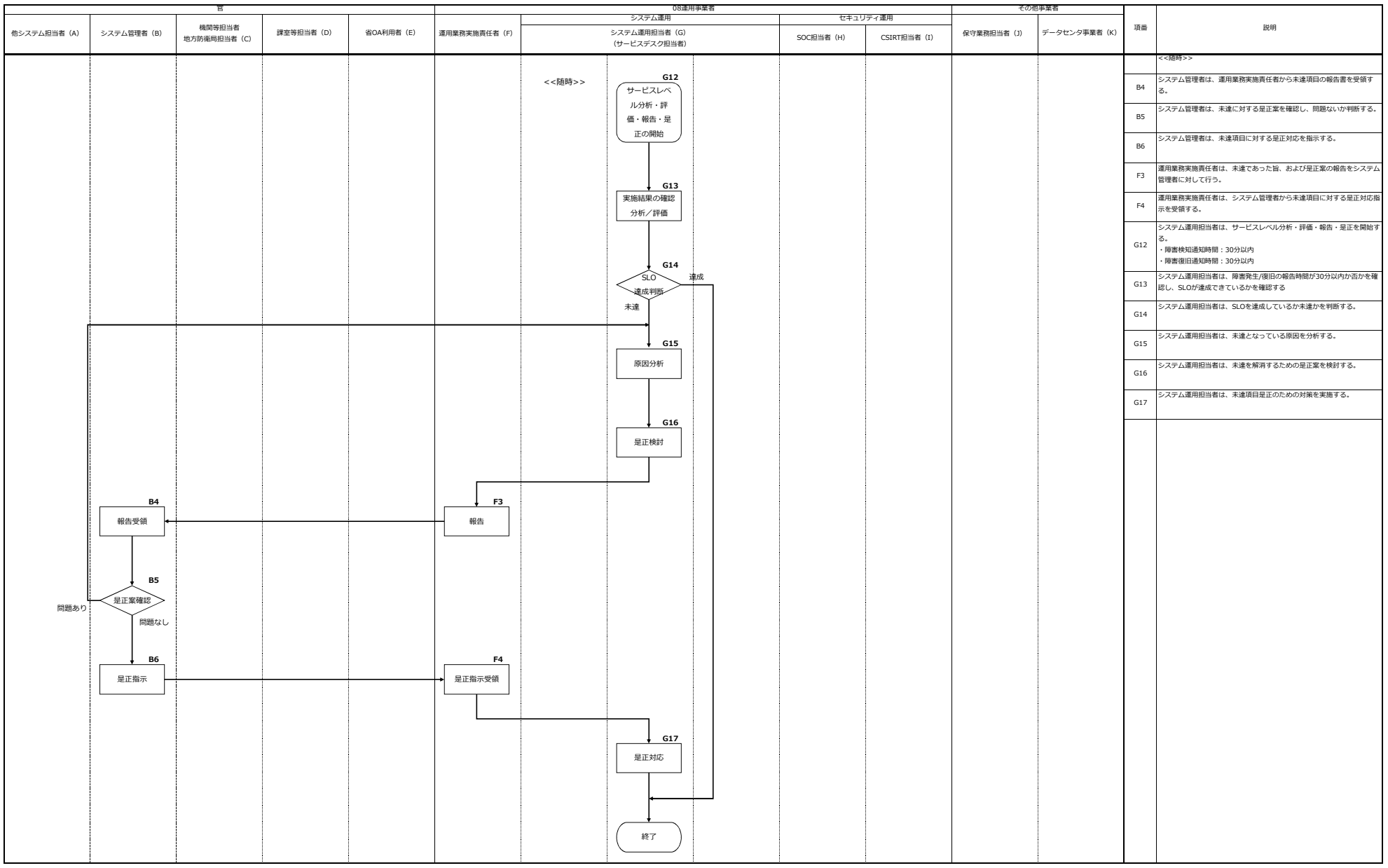
フロー名称	説明	作業トリガー
サービスレベル分析・評価・報告・是正	サービスレベルの分析・評価・報告・是正を行うためのフローを示す。	・月次：月1回の定期報告時 ・随時：障害発生時



項番	説明
	<<月次>>
B1	システム管理者は、運用業務実施責任者から月次報告書を受領する。
B2	システム管理者は、未達項目があるか否かを判断する。
B3	システム管理者は、未達項目に対する是正案の内容を確認し、問題がないか判断する。
B4	システム管理者は、運用業務実施責任者に対して未達項目に対する是正対応を指示する。
F1	運用業務実施責任者は、月次報告をシステム管理者に対して行う。
F2	運用業務実施責任者は、システム管理者から未達項目に対する是正対応指示を受領する。
G1	システム運用担当者は、サービスレベル分析・評価・報告・是正を開始する。 ・サービス稼働率：月間99.9%以上 ・問合せ対応回答率：月間90%以上 ・申請依頼に対する対応率：月間95%以上
G2	システム運用担当者は、現在のサービスの品質やパフォーマンスを測定し、サービスレベルの評価に必要な情報を収集する。
G3	システム運用担当者は、収集した情報から各サービスレベル評価項目の目標値に対する状況を分析し、目標に達しているかを評価する。 また、是正があった場合、是正対策の経過に問題がないかを評価する。 （是正対策経過確認期間：3ヶ月）
G4	システム運用担当者は、SLOを達成しているか未達かを判断する。
G5	システム運用担当者は、未達となっているのは稼働率か否かを判断する。
G6	システム運用担当者は、未達となっている原因を分析する。
G7	システム運用担当者は、未達を解消するための是正案を検討する。
G8	システム運用担当者は、未達項目の状況、原因、是正案を月次報告書にまとめる。 すでに未達対策済のものについては是正対応に問題がないか経過観察を行う。（経過観察：3ヶ月）
G9	システム運用担当者は、月次報告書を作成する。
G10	システム運用担当尾者は、未達となっているのは稼働率か否かを判断する。
G11	システム運用担当者は、未達項目是正のための対策を実施する。
J1	保守業務担当者は、未達となっている原因を分析する。
J2	保守業務担当者は、未達を解消するための是正案を検討する。
J3	保守業務担当者は、未達項目是正のための対策を実施する。

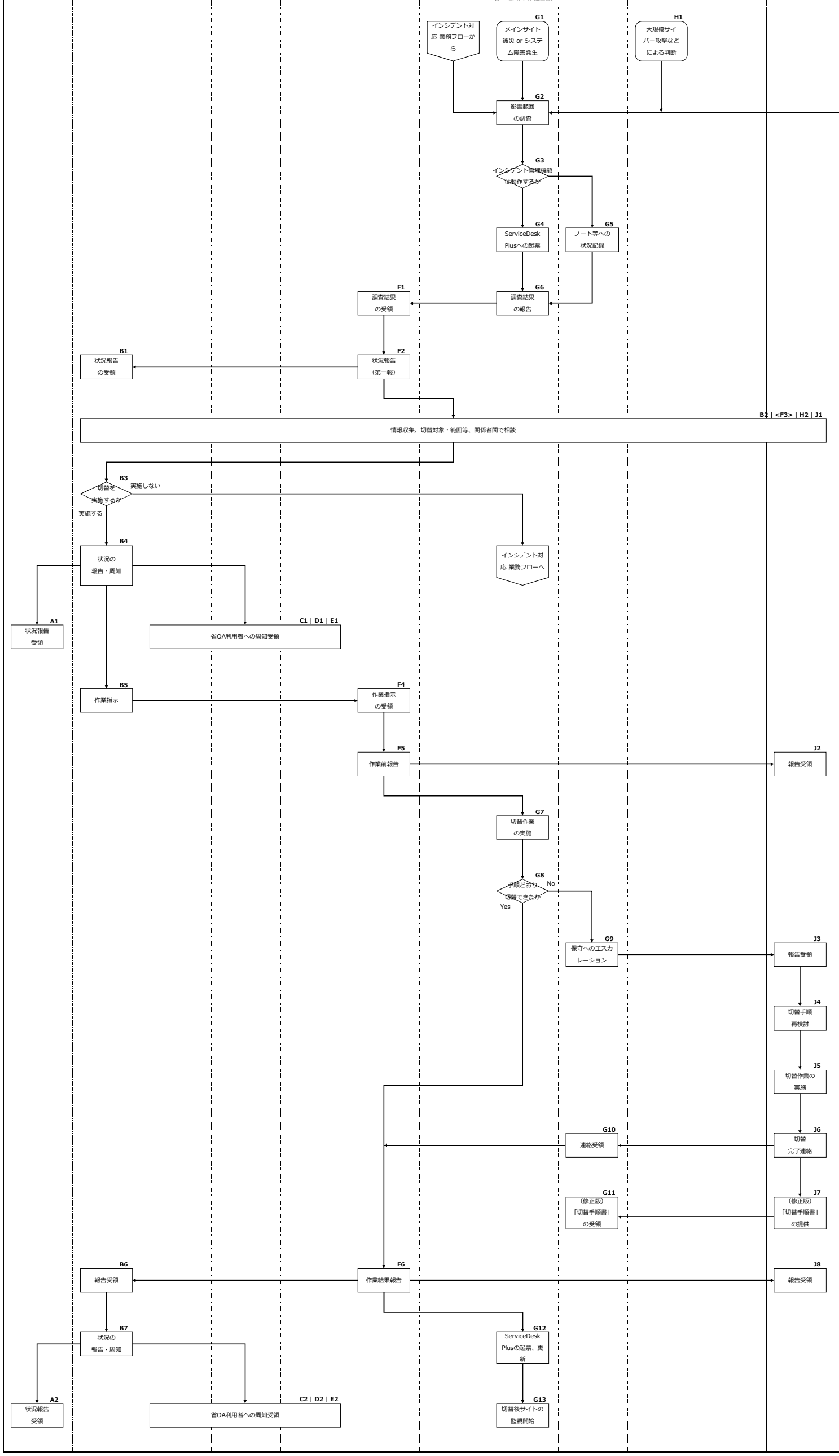
付表１０　業務フロー（続き）
サービスレベル分析・評価・報告・是正（続き）

フロー名称	説明	作業トリガー
サービスレベル分析・評価・報告・是正	サービスレベルの分析・評価・報告・是正を行うためのフローを示す。	・月次：月1回の定期報告時 ・随時：障害発生時



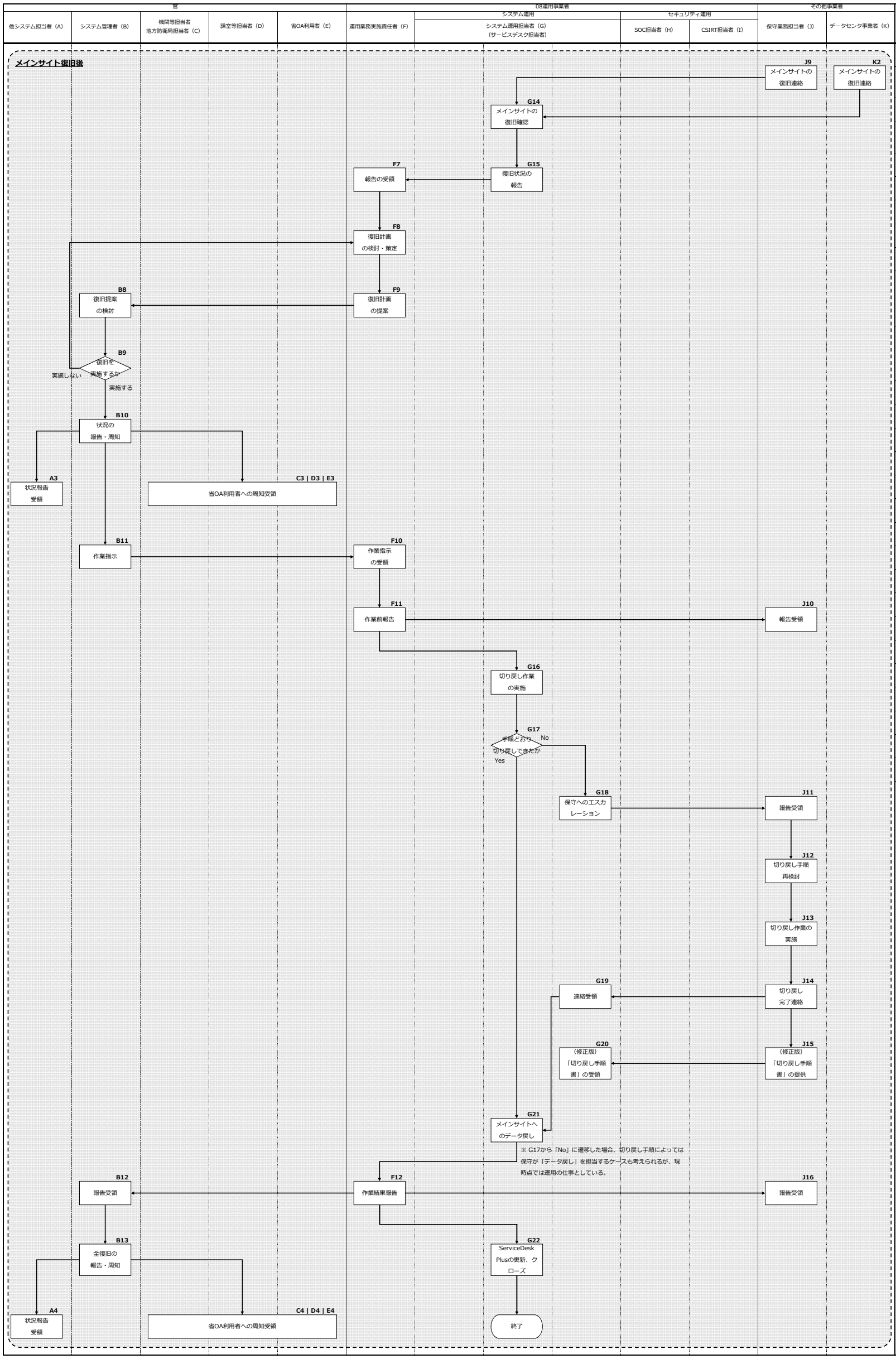
項番	説明
	<<随時>>
B4	システム管理者は、運用業務実施責任者から未達項目の報告書を受領する。
B5	システム管理者は、未達に対する是正案を確認し、問題ないか判断する。
B6	システム管理者は、未達項目に対する是正対応を指示する。
F3	運用業務実施責任者は、未達であった旨、および是正案の報告をシステム管理者に対して行う。
F4	運用業務実施責任者は、システム管理者から未達項目に対する是正対応指示を受領する。
G12	システム運用担当者は、サービスレベル分析・評価・報告・是正を開始する。 ・障害検知通知時間：30分以内 ・障害復旧通知時間：30分以内
G13	システム運用担当者は、障害発生/復旧の報告時間が30分以内か否かを確認し、SLOが達成できているかを確認する
G14	システム運用担当者は、SLOを達成しているか未達かを判断する。
G15	システム運用担当者は、未達となっている原因を分析する。
G16	システム運用担当者は、未達を解消するための是正案を検討する。
G17	システム運用担当者は、未達項目是正のための対策を実施する。

フロー名称	説明	作業トリガー
大規模障害対応	メインサイトが災害や大規模障害により機能不全に陥り、容易に復旧ができない場合、 バックアップサイトへ切替を行うことでシステムの稼働を継続する業務を示す。	メインサイト被災時若しくはシステム障害発生時



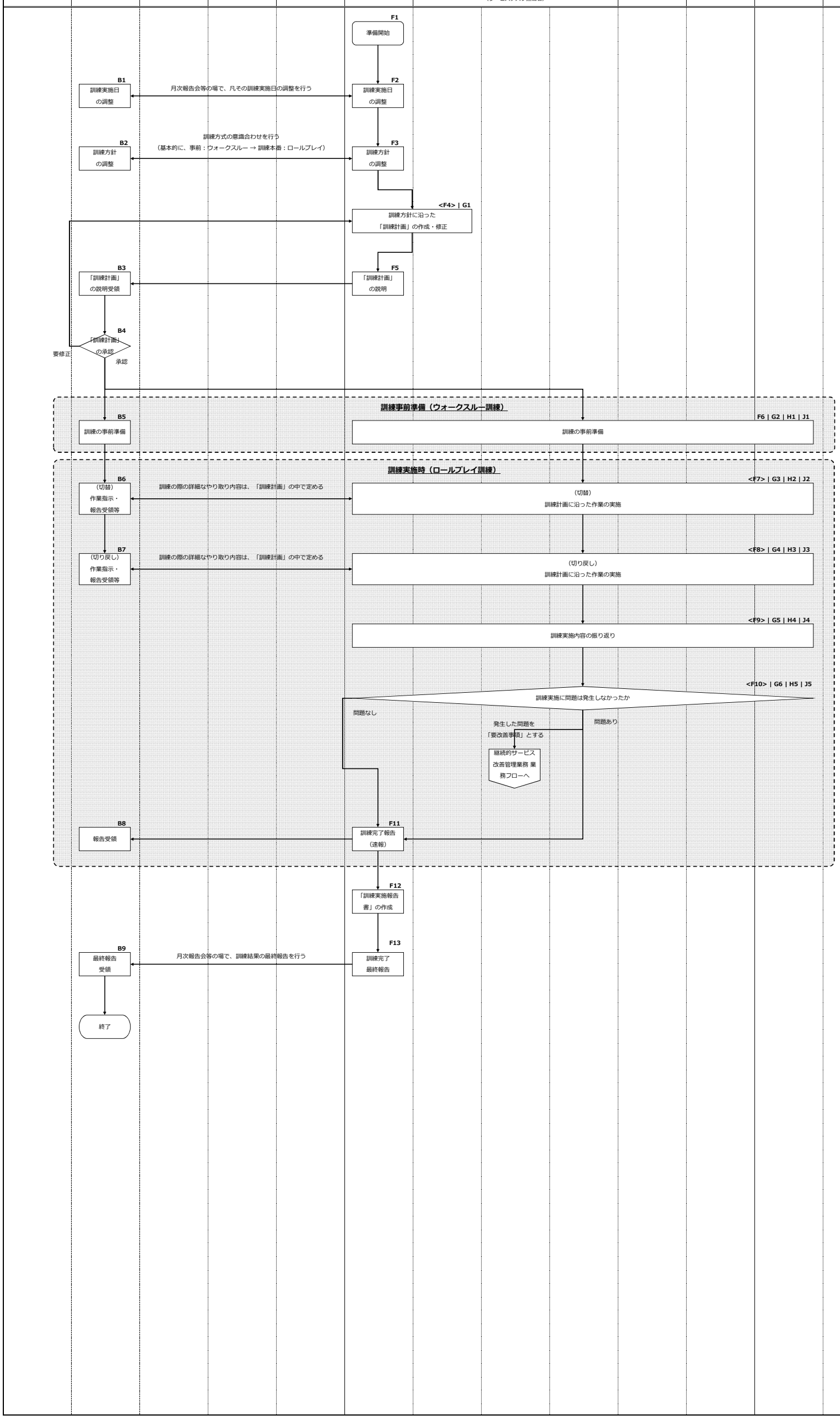
項番	説明
A1	他システム担当者は、システム管理者より「バックアップサイトへの切替が行われる旨」の報告を受ける。
A2	他システム担当者は、システム管理者より「バックアップサイトへの切替が完了した旨」の報告を受ける。
A3	他システム担当者は、システム管理者より「メインサイトへの切り戻しが行われる旨」の報告を受ける。
A4	他システム担当者は、システム管理者より「全復旧が完了した旨」の報告を受ける。
B1	システム管理者は、運用業務実施責任者よりメインサイトの状況についての報告を受ける。 なお、ここで受ける報告は第一報であり、追って詳細な報告を切替提案と共に受けるものとする。
B2	運用業務実施責任者のもとで関係者間で切替を判断するための情報収集を行い、切替判断に至るための事前相談を実施する。相談事項は以下のとおり。 ・被災状況、障害状況の整理 ・切替対象とする範囲や対象システム ・切替要否の判断
B3	システム管理者はバックアップサイトへの切替判断を行う。
B4	システム管理者は、バックアップサイトへの切替を決定した旨を他システム担当者や省OA利用者に連絡・周知を行う。
B5	システム管理者は、バックアップサイトへの切替作業を実施するよう、運用業務実施責任者に指示を行う。
B6	システム管理者は、「バックアップサイトへの切替が完了した旨」の報告を、運用業務実施担当者より受ける。
B7	システム管理者は、「バックアップサイトへの切替を完了した旨」を他システム担当者や省OA利用者に連絡・周知を行う。
B8	システム管理者は、運用業務実施責任者より受けたメインサイトへの切り戻し提案を基に、切り戻しを実施するかの検討を行う。
B9	システム管理者はメインサイトへの切り戻し判断を行う。
B10	システム管理者は、「メインサイトへの切り戻しを行う旨」を他システム担当者や省OA利用者に連絡・周知を行う。
B11	システム管理者は、メインサイトへの切り戻し作業を実施するよう、運用業務実施責任者に指示を行う。
B12	システム管理者は、「メインサイトへの切り戻しが完了した旨」の報告を、運用業務実施担当者より受ける。
B13	システム管理者は、「全復旧が完了した旨」を他システム担当者や省OA利用者に連絡・周知を行う。
C1	機関等担当者、地方防衛局担当者は、システム管理者より「バックアップサイトへの切替が行われる旨」の周知を受ける。
C2	機関等担当者、地方防衛局担当者は、システム管理者より「バックアップサイトへの切替が完了した旨」の周知を受ける。
C3	機関等担当者、地方防衛局担当者は、システム管理者より「メインサイトへの切り戻しが行われる旨」の周知を受ける。
C4	機関等担当者、地方防衛局担当者は、システム管理者より「全復旧が完了した旨」の周知を受ける。
D1	課室等担当者は、システム管理者より「バックアップサイトへの切替が行われる旨」の周知を受ける。
D2	課室等担当者は、システム管理者より「バックアップサイトへの切替が完了した旨」の周知を受ける。
D3	課室等担当者は、システム管理者より「メインサイトへの切り戻しが行われる旨」の周知を受ける。
D4	課室等担当者は、システム管理者より「全復旧が完了した旨」の周知を受ける。
E1	省OA利用者は、システム管理者より「バックアップサイトへの切替が行われる旨」の周知を受ける。
E2	省OA利用者は、システム管理者より「バックアップサイトへの切替が完了した旨」の周知を受ける。
E3	省OA利用者は、システム管理者より「メインサイトへの切り戻しが行われる旨」の周知を受ける。
E4	省OA利用者は、システム管理者より「全復旧が完了した旨」の周知を受ける。
F1	運用業務実施責任者は、システム運用担当者からシステム稼働状況に関する調査結果を受領する。
F2	運用業務実施責任者は、調査結果を基に、システム管理者へ状況の報告を行う。 なお、ここでの報告は第一報であり、追って詳細な報告を切替提案と共に行う。
F3	運用業務実施責任者のもとで関係者間で切替を判断するための情報収集を行い、切替判断に至るための事前相談を実施する。相談事項は以下のとおり。 ・被災状況、障害状況の整理 ・切替対象とする範囲や対象システム ・切替要否の判断
F4	運用業務実施責任者は、システム管理者からのバックアップサイトへの切替指示を受領し、切替作業を開始する。
F5	運用業務実施責任者は保守業務担当者に、バックアップサイトへ切替を実施することになった旨の作業前報告を行う。
F6	運用業務実施責任者は、「バックアップサイトへの切替を完了した旨」をシステム管理者及び保守業務担当者に報告する。
F7	運用業務実施責任者は、メインサイトの復旧状況に関する報告を、システム運用担当者より受ける。
F8	運用業務実施責任者は、報告を受けた状況を踏まえメインサイトへの切り戻しを行うための「復旧計画」を検討・策定する。
F9	運用業務実施責任者は、策定した「復旧計画」を基に、システム管理者へ説明を行い、メインサイトへの切り戻しを提案する。
F10	運用業務実施責任者は、システム管理者からのメインサイトへの切り戻し指示を受領し、切り戻し作業を開始する。
F11	運用業務実施責任者は保守業務担当者に、メインサイトへ切替を実施する旨の作業前報告を行う。
F12	運用業務実施責任者は、「メインサイトへの切り戻しが完了した旨」をシステム管理者及び保守業務担当者に報告する。
G1	システム運用担当者は、大規模障害発生を検知する。
G2	システム運用担当者は、障害や被災の結果生じた影響の範囲調査を行う。
G3	システム運用担当者は、運用対応の記録のためインシデント管理機能を用いるが、この機能が利用できる状況か（障害等で機能不全に陥っていないか）確認する。
G4	インシデント管理機能を利用できる場合は、システム運用担当者は、ServiceDesk Plusへの起票を行う。
G5	インシデント管理機能を利用できない場合は、システム運用担当者は、ノートやローカルPC上のファイルに起票を行い、運用対応記録を残す。
G6	システム運用担当者は、メインサイトの稼働状況に関する調査結果を、運用業務実施責任者に報告する。
G7	システム運用担当者は、運用業務実施責任者の指示の下で、バックアップサイトへの切替作業を実施する。切替完了後は、システム正常動作の確認を実施する。
G8	切替作業は手順どおりに正しく実施できたか。
G9	作業の結果、手順どおりに操作できなかった・正常動作が確認できなかった等の場合は、保守業務担当者にエスカレーションを行い、切替方法の確認・再検討を依頼する。
G10	システム運用担当者は、保守業務担当者よりバックアップサイトへの切替が完了した旨の連絡を受ける。
G11	システム運用担当者は、保守業務担当者より修正された「切替手順書」を受領し、管理するドキュメントを更新する。
G12	システム運用担当者は、ServiceDesk Plusのデータ更新を行う。 なお、これまでにインシデント管理機能が利用できていなかった場合は、新たに起票し、他で付けていた記録を転記する。
G13	システム運用担当者は、切替後はバックアップサイトで稼働するシステムの監視も開始し、障害発生等に備える。
G14	（メインサイト側の問題が解消され(復旧がされた後) システム運用担当者はメインサイトの状況を調査し、システムが稼働できる状況であることを確認する。

フロー名称	説明	作業トリガー
大規模障害対応	メインサイトが災害や大規模障害により機能不全に陥り、容易に復旧ができない場合、 バックアップサイトへ切替を行うことでシステムの稼働を継続する業務を示す。	メインサイト被災時若しくはシステム障害発生時



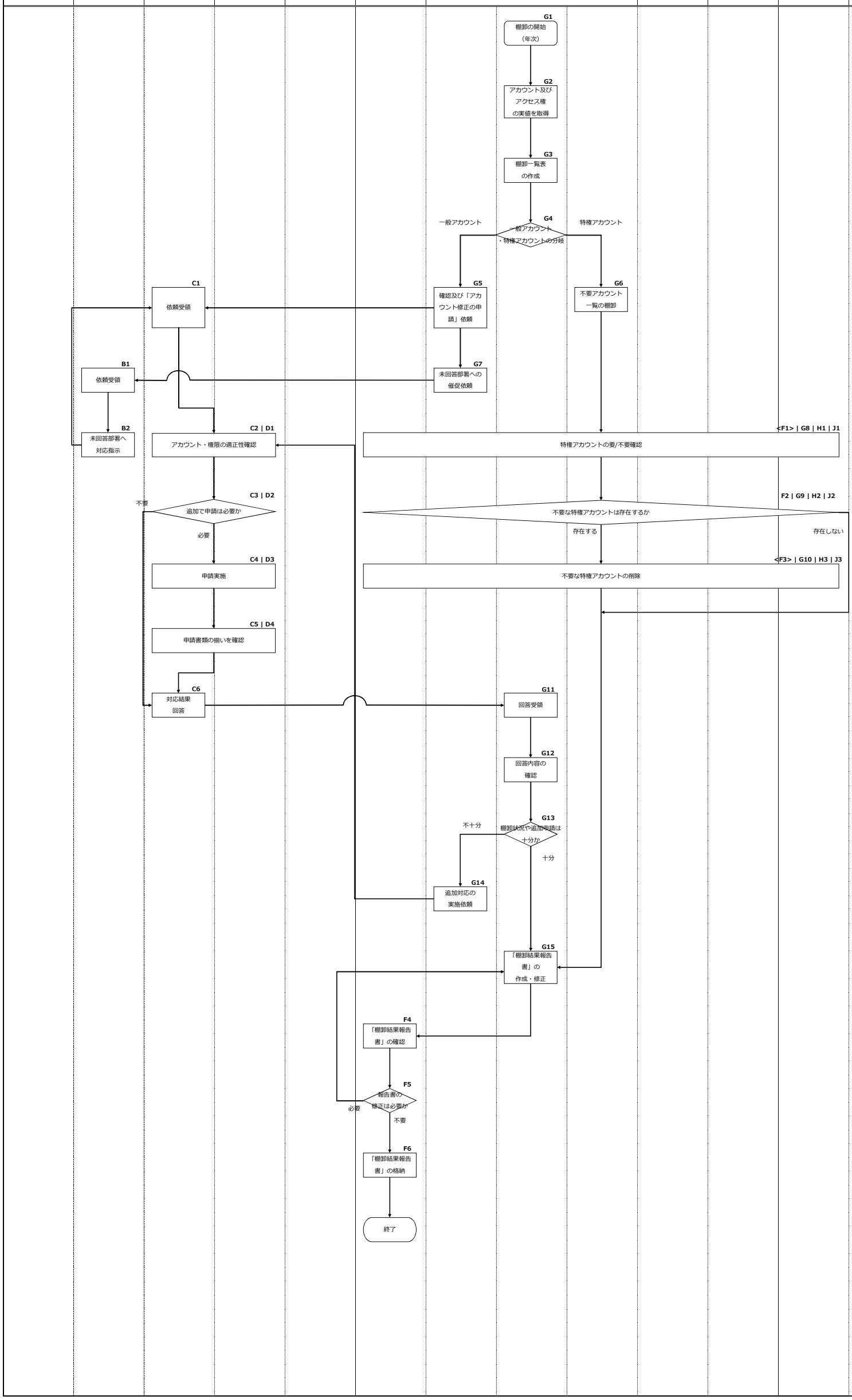
項番	説明
G15	システム運用担当者は、メインサイト復旧状況の調査結果を、運用業務実施責任者に報告する。
G16	システム運用担当者は、運用業務実施責任者の指示の下で、メインサイトへの切り戻し作業を実施する。切り戻し完了後は、システム正常動作の確認を実施する。
G17	切り戻し作業は手順どおりに正しく実施できたか。
G18	作業の結果、手順どおりに操作できなかった・正常動作が確認できなかった等の場合は、保守業務担当者にエスカレーションを行い、切り戻し方法の確認・再検討を依頼する。
G19	システム運用担当者は、保守業務担当者よりメインサイトへの切り戻しが完了した旨の連絡を受ける。
G20	システム運用担当者は、保守業務担当者より修正された「切り戻し手順書」を受領し、管理するドキュメントを更新する。
G21	バックアップサイトでの運用時に保存されたデータのうち、必要なものをメインサイトへデータ移行する。
G22	システム運用担当者は、一連の運用対応の経緯・結果を ServiceDesk Plusに記録し、クローズ処理を行う。
H1	大規模なサイバー攻撃等により、SOCによる判断で切替が必要と判断した場合は、その旨をシステム運用担当者に連絡する。
H2	運用業務実施責任者のもとで関係者間で切替を判断するための情報収集を行い、切替判断に至るための事前相談を実施する。相談事項は以下のとおり。 ・被災状況、障害状況の整理 ・切替対象とする範囲や対象システム ・切替要否の判断
J1	運用業務実施責任者のもとで関係者間で切替を判断するための情報収集を行い、切替判断に至るための事前相談を実施する。相談事項は以下のとおり。 ・被災状況、障害状況の整理 ・切替対象とする範囲や対象システム ・切替要否の判断
J2	保守業務担当者は、運用実施責任者よりバックアップサイトへ切替を行う旨の報告を受領する。
J3	保守業務担当者は、切替作業上で問題が発生した連絡を受領する。
J4	保守業務担当者は、切替作業の手順の再検討を行い、有効な切替手順を確立する。
J5	保守業務担当者は、更新した切替手順を基にバックアップサイトへのシステム切替を実施する。
J6	保守業務担当者は、システム運用担当者へバックアップサイトへの切替が完了した旨を連絡する。
J7	保守業務担当者は新たに確立した切替手順を「切替手順書」に反映し、この更新版の手順書をシステム運用担当者に提供する。
J8	保守業務担当者は、運用実施責任者よりバックアップサイトへ切替が完了した旨の報告を受領する。
J9	保守業務担当者は、システム運用担当者に対して問題の発生していたメインサイトの復旧が完了した旨の報告を行う。
J10	保守業務担当者は、運用実施責任者よりメインサイトへ切り戻しを行う旨の報告を受領する。
J11	保守業務担当者は、切り戻し作業上で問題が発生した連絡を受領する。
J12	保守業務担当者は、切り9戻し作業手順の再検討を行い、有効な切り戻し手順を確立する。
J13	保守業務担当者は、更新した切り戻し手順を基にメインサイトへのシステム切り戻しを実施する。
J14	保守業務担当者は、システム運用担当者へメインサイトへの切り戻しが完了した旨を連絡する。
J15	保守業務担当者は新たに確立した切り戻し手順を「切り戻し手順書」に反映し、この更新版の手順書をシステム運用担当者に提供する。
J16	保守業務担当者は、運用実施責任者よりメインサイトへ切り戻しが完了した旨の報告を受領する。
K1	データセンタ事業者は、メインサイトの障害や被災が発生した際に、システム運用担当者にその旨を連絡する。
K2	データセンタ事業者はシステム用担当者に、メインサイトで発生していた問題が解決、復旧した旨を連絡する。

フロー名称	説明	作業トリガー
大規模障害切替訓練	大規模障害（災害）が発生した際のシステム切り替え作業等について 有事の際に滞りなく対応が行えるようにするため、 平時のうちに「訓練」として手順や連絡体制を確認することで、 運用員の業務習熟と問題点の改善を図る。	運用計画で定めたスケジュールに則って、年次で実施する。



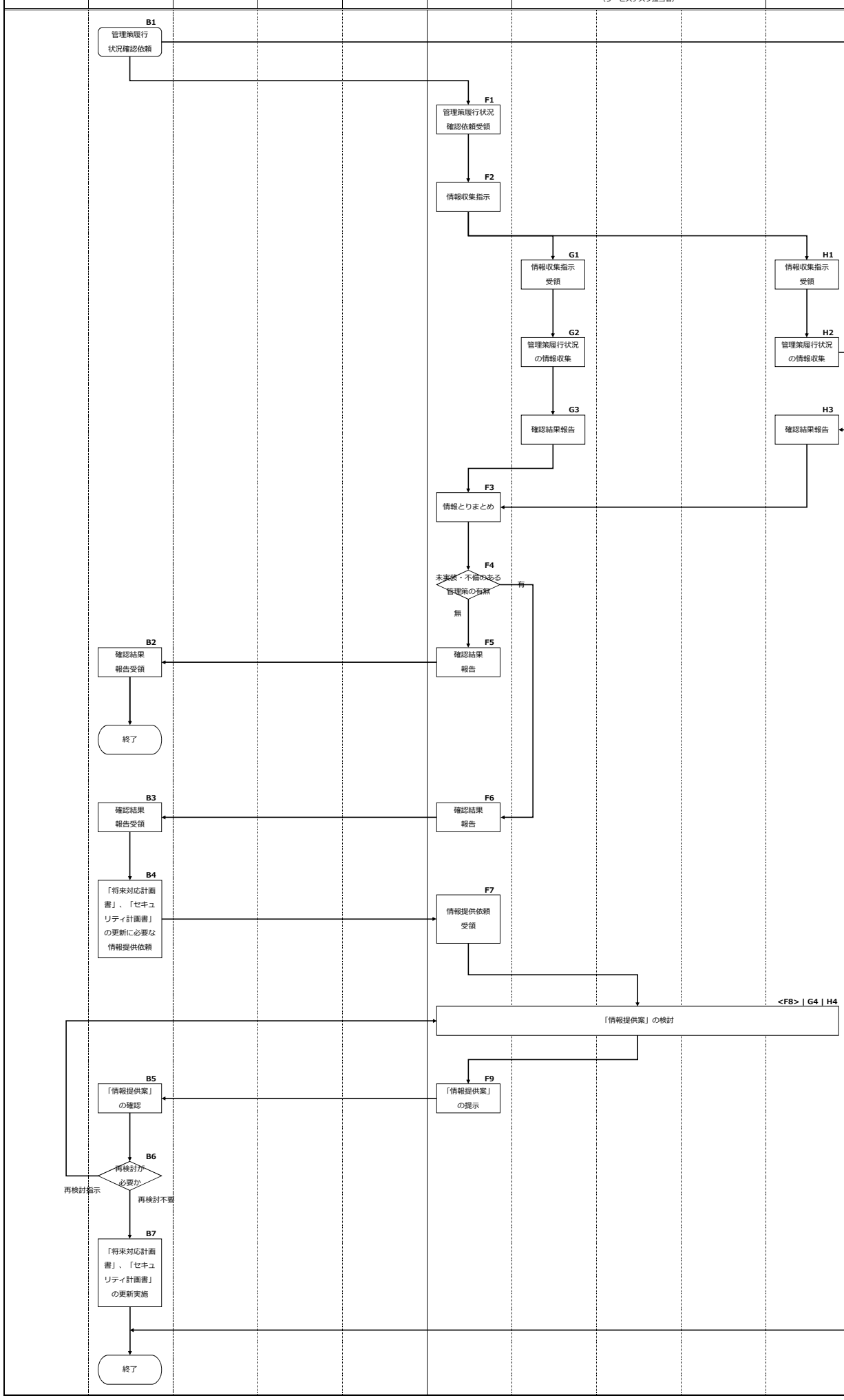
項番	説明
B1	システム管理者は、月次報告会等の場で、運用業務実施責任者より「大規模障害切替訓練」の時期が近付いてきたことを説明され、凡その具体的実施日時の調整・決定を行う。
B2	システム管理者は、実施する訓練の方針を決定する。 ※ 詳細は、F3の説明欄を参照のこと。
B3	システム管理者は、運用実施責任者より「大規模障害切替訓練計画」の説明を受ける。
B4	システム管理者は、説明を受けた「訓練計画」の是非について判断を行い、必要に応じて訓練計画の見直し等を指示する。
B5	システム管理者は、「訓練計画」に基づき訓練実施日までに事前準備（必要なマニュアルや計画書の確認、各自の役割分担の確認）を行う。
B6	（切替訓練）システム管理者は、訓練実施当日に「訓練計画」で定められた役割に沿って、業務実施の指示や、システム運用からの報告受け等、役割を模擬的に演じる。
B7	（切り戻し訓練）システム管理者は、訓練実施当日に「訓練計画」で定められた役割に沿って、業務実施の指示や、システム運用からの報告受け等、役割を模擬的に演じる。
B8	訓練実施完了後、システム管理者は運用業務実施責任者より、訓練実施内容について報告を受ける。ここでは、訓練終了時の「速報」レベルの報告を受けるものとし、詳細な訓練結果の報告は後日再度受ける。
B9	システム管理者は運用業務実施責任者より、訓練実施内容について最終報告を受ける。
F1	運用業務実施責任者は、年次スケジュールに沿って大規模障害切替訓練を実施すると定めた時期の約2か月前に訓練準備を開始する。まずは、計画作成のために具体的な実施日を決定する。
F2	運用業務実施責任者は、月次報告会等の場で、システム管理者に「大規模障害切替訓練」の時期が近付いてきたことを説明し、凡その具体的実施日時の調整・決定を行う。
F3	運用業務実施責任者は、実施する訓練の方針を決定する。 ・ウォークスルー： マニュアルや計画書に沿って、各役割と活動を確認する訓練である。平時の要員教育に準ずるものであり、本訓練の中では「訓練の事前準備」において、訓練実施時に備え必要なマニュアルや計画書の確認、各自の役割分担の確認を実施する。 ・ロールプレイ： 特定のシナリオに基づいて、メンバーがそれぞれの役割を模擬的に演じる訓練である。本訓練ではシステム切替に伴う利用者影響を考慮し、このロールプレイを基本的な訓練方針とする。 ・フルインタラプション： 実際にシステム切替/切り戻しを実施する等、本番に最も近い形で行われるシミュレーション訓練である。切替/切り戻しを実施した場合、利用者影響が発生するため、本訓練ではフルインタラプションは基本的に実施しない。
F4	運用業務実施責任者は、訓練実施日、訓練方針の決定後、システム運用担当者を指揮して「大規模障害切替訓練計画」の作成を行う。訓練計画の中では以下の事項を定める。また、必要に応じて計画内容の修正を行う。 ・訓練の目的 ・どのような障害、災害が発生したと想定するか ・訓練対象とするシステム範囲 ・作業日程や時間（タイムススケジュール） ・実施体制（参加メンバーと役割） ・具体的訓練作業内容 ・訓練実施後の対応内容
F5	運用業務実施責任者は、作成した「大規模障害切替訓練計画」をシステム管理者に説明を行い、訓練への参加を依頼する。
F6	運用業務実施管理者は、「訓練計画」に基づき訓練実施日までに事前準備（必要なマニュアルや計画書の確認、各自の役割分担の確認）を行う。
F7	（切替訓練）運用業務実施管理者は、「大規模障害切替訓練計画」で定めた内容に沿って、訓練を実施・監督する等、役割を模擬的に演じる。
F8	（切り戻し訓練）運用業務実施管理者は、「大規模障害切替訓練計画」で定めた内容に沿って、訓練を実施・監督する等、役割を模擬的に演じる。
F9	運用業務実施管理者は、訓練作業の完了後、実施内容の振り返りを行う。
F10	運用業務実施責任者は、訓練内容の振り返りの中から、「想定通りに作業できなかった点」、「手順書、フロー、チェックリストなどドキュメントの不備」、「システムの動作が想定どおりいかなかった」、「連絡体制上の障害」等、切り替え作業を実施するに当たって見出した問題の有無を判定する。問題があった場合は、「継続的サービス改善業務」の「要改善事項」としてエントリーさせ、問題の改善活動を実施する。
F11	運用業務実施責任者は、訓練完了後に実施内容・結果の概略をシステム管理者に対して報告を行う。ここでの報告は、訓練実施日における速報レベルの報告であり、後日報告書に内容を纏めて正式な報告を再度行うものとする。
F12	運用業務実施責任者は、訓練実施の後日（概ね1月以内）、訓練内容について「訓練実施報告書」としてまとめる。
F13	運用業務実施責任者は、作成した「訓練実施報告書」を基に訓練結果をシステム管理者に対して最終報告する。この最終報告は、月次報告会の場などを用いて行う。
G1	システム運用担当者は、訓練実施日、訓練方針の決定後、運用業務実施責任者の指揮のもと「大規模障害切替訓練計画」の作成を行う。訓練計画の中では以下の事項を定める。また、必要に応じて計画内容の修正を行う。 ・訓練の目的 ・どのような障害、災害が発生したと想定するか ・訓練対象とするシステム範囲 ・作業日程や時間（タイムススケジュール） ・実施体制（参加メンバーと役割） ・具体的訓練作業内容 ・訓練実施後の対応内容
G2	システム運用担当者は、「訓練計画」に基づき訓練実施日までに事前準備（必要なマニュアルや計画書の確認、各自の役割分担の確認）を行う。
G3	（切替訓練）システム運用担当者は、「大規模障害切替訓練計画」で定めた内容に沿って、運用業務実施管理者の指揮下で大規模障害切替に際しての役割を模擬的に演じる。
G4	（切り戻し訓練）システム運用担当者は、「大規模障害切替訓練計画」で定めた内容に沿って、運用業務実施管理者の指揮下で大規模障害切り戻しに際しての役割を模擬的に演じる。
G5	システム運用担当者は、訓練作業の完了後、運用業務実施管理者の指揮下で実施内容の振り返りを行う。
G6	システム運用担当者は、訓練内容の振り返りの中から、「想定通りに作業できなかった点」、「手順書、フロー、チェックリストなどドキュメントの不備」、「システムの動作が想定どおりいかなかった」、「連絡体制上の障害」等、切り替え作業を実施するに当たって見出した問題の有無を判定する。
H1	SOC担当者は、「訓練計画」に基づき訓練実施日までに事前準備（必要なマニュアルや計画書の確認、各自の役割分担の確認）を行う。
H2	（切替訓練）SOC担当者は、「大規模障害切替訓練計画」で定めた内容に沿って、運用業務実施管理者の指揮下で大規模障害切替に際しての役割を模擬的に演じる。
H3	（切り戻し訓練）SOC担当者は、「大規模障害切替訓練計画」で定めた内容に沿って、運用業務実施管理者の指揮下で大規模障害切り戻しに際しての役割を模擬的に演じる。
H4	SOC担当者は、訓練作業の完了後、運用業務実施管理者の指揮下で実施内容の振り返りを行う。
H5	SOC担当者は、訓練内容の振り返りの中から、「想定通りに作業できなかった点」、「手順書、フロー、チェックリストなどドキュメントの不備」、「システムの動作が想定どおりいかなかった」、「連絡体制上の障害」等、切り替え作業を実施するに当たって見出した問題の有無を判定する。
J1	保守業務担当者は、「訓練計画」に基づき訓練実施日までに事前準備（必要なマニュアルや計画書の確認、各自の役割分担の確認）を行う。
J2	（切替訓練）保守業務担当者は、「大規模障害切替訓練計画」で定めた内容に沿って、運用業務実施管理者の指揮下で大規模障害切替に際しての役割を模擬的に演じる。
J3	（切り戻し訓練）保守業務担当者は、「大規模障害切替訓練計画」で定めた内容に沿って、運用業務実施管理者の指揮下で大規模障害切り戻しに際しての役割を模擬的に演じる。
J4	保守業務担当者は、訓練作業の完了後、運用業務実施管理者の指揮下で実施内容の振り返りを行う。
J5	保守業務担当者は、訓練内容の振り返りの中から、「想定通りに作業できなかった点」、「手順書、フロー、チェックリストなどドキュメントの不備」、「システムの動作が想定どおりいかなかった」、「連絡体制上の障害」等、切り替え作業を実施するに当たって見出した問題の有無を判定する。

フロー名称	説明	作業トリガー
アカウント・ファイル共有アクセス権の棚卸	人事異動等に伴う不要アカウントや不要ライセンスを排除し、適正なアカウント状態を維持するとともに、共有フォルダのセキュリティグループに属するアカウントの妥当性を確認する手順を示すものである	年次処理（人事異動後）



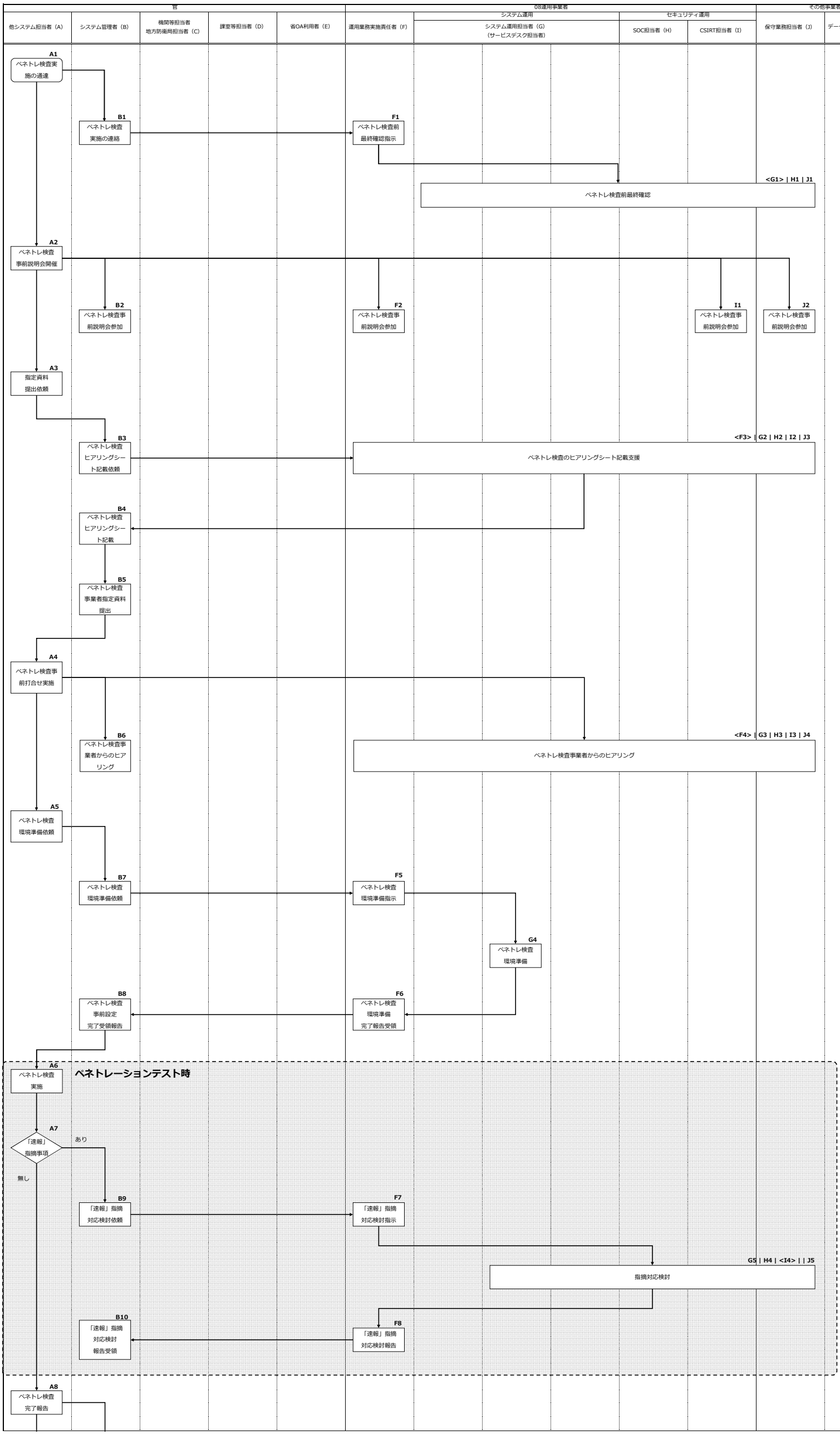
項番	説明
B1	システム管理者は、システム運用担当者より依頼された未回答部署への督促依頼を受領する。
B2	システム管理者は、アカウント・ファイル共有アクセス権の棚卸依頼に回答していない機関等担当者、地方防衛局担当者に対して、依頼対応を行うよう連絡する。
C1	機関等担当者、地方防衛局担当者は、システム運用担当者より、アカウント権限の棚卸（確認）依頼を受領する。
C2	機関等担当者、地方防衛局担当者は受領した調査依頼を基に、課室等担当者と連携し、以下の観点で権限の要否を判定する： ・現在の業務に必要な権限か ・不要な共有フォルダへの閲覧権限が残っていないか ・前任者の権限を誤って引き継いでいないか ・管理者権限が不適切に付与されていないか 必要に応じて「削除」「権限レベル変更」の要望を一覧表に記入する。
C3	機関等担当者、地方防衛局担当者は、確認結果から追加で申請が必要かを判断する。
C4	機関等担当者、地方防衛局担当者は、確認結果から追加申請の必要性が判明した場合は、申請書の作成及び提出の対応を行う。想定される申請書は以下のとおり。 ・個人アカウントの改廃が必要な場合 → 個人アカウント登録・個人端末利用等申請書 ・共有フォルダに対する権限の改廃が必要な場合 → 機関共有フォルダ作成等申請書
C5	機関等担当者、地方防衛局担当者は、依頼した申請が揃っているか確認する。
C6	機関等担当者、地方防衛局担当者は調査結果を反映したアカウント・権限棚卸確認対象者一覧をシステム運用担当者へ回答する。
D1	課室等担当者は、機関等担当者、地方防衛局担当者と連携し、以下の観点で権限の要否を判定する： ・現在の業務に必要な権限か ・不要な共有フォルダへの閲覧権限が残っていないか ・前任者の権限を誤って引き継いでいないか ・管理者権限が不適切に付与されていないか 必要に応じて「削除」「権限レベル変更」の要望を一覧表に記入する。
D2	課室等担当者は、確認結果から追加で申請が必要かを判断する。
D3	課室等担当者は、確認結果から追加申請の必要性が判明した場合は、申請書の作成及び提出の対応を行う。想定される申請書は以下のとおり。 ・個人アカウントの改廃が必要な場合 → 個人アカウント登録・個人端末利用等申請書 ・共有フォルダに対する権限の改廃が必要な場合 → 機関共有フォルダ作成等申請書
D4	課室等担当者は、依頼した申請が揃っているか確認する。
F1	運用業務実施責任者は、棚卸結果から特権アカウントを洗い出し、それぞれのアカウントの必要性を主体的に評価・判定する。
F2	確認結果、不要な特権アカウントが「存在するか」「存在しないか」で処理が分岐する。
F3	運用業務実施責任者は、不要な特権アカウントの削除を行う。
F4	運用業務実施責任者は、システム運用担当者が作成した「棚卸結果報告書」の内容を確認する。
F5	運用業務実施責任者は、「棚卸結果報告書」の確認結果、修正を要する箇所があればシステム運用担当者にその旨を指示する。
F6	運用業務実施責任者は、「棚卸結果報告書」を、月次報告用フォルダに規定の形式および命名規則に従って格納する。 ※ システム管理者は、この結果を受け、必要に応じて機関等担当者に連絡を行う。
G1	システム運用担当者は、人事異動後の年次処理として棚卸業務を開始する。
G2	離任者・着任者アカウントおよび対象フォルダ・サイトのアクセス権、特権アカウントを、実システム（アクティブディレクトリサービス／ファイルサーバー）から直接参照して取得する。 以下のデータを収集する： ・対象ユーザー・グループに対して実システム上で現在付与されているアクセス権の実値 ・継承設定の有無、および例外的に付与されている固有権限
G3	離任者・着任者ごとに、現在保持しているアカウント・権限棚卸確認対象者一覧を作成する。 前任者の権限が引き継がれていないか、グループ設定に過不足がないかを整理する。
G4	一般アカウントと特権アカウントで棚卸処理を分岐する。
G5	各部門ごとに整形した一覧表を各部門へ送付し、離任者・着任者が必要な権限のみ保持しているかを確認依頼する。 また、確認結果から追加申請が必要な際は、「個人アカウント登録・個人端末利用等申請書」や「機関共有フォルダ作成等申請書」の提出を行うよう依頼する。 ※ 回答期限（例：5営業日）を明記し、未回答部署にはリマインドを実施する。
G6	取得した特権アカウント一覧をもとに、不要となったアカウントが存在しないかを確認する。システム運用で使用の特権アカウントに限らず、構築時の残存特権アカウント、作業時の残存特権アカウントなど、変更対応が必要な特権アカウントを確認する。
G7	システム運用担当者は、必要に応じて未回答の部門へ催促のため、システム管理者に督促協力を依頼する。
G8	システム運用担当者は、運用業務実施責任者と連携し、棚卸の結果でリストアップされた特権アカウント（システム運用関連アカウント）の要不要について確認する。
G9	確認結果、不要な特権アカウントが「存在するか」「存在しないか」で処理が分岐する。
G10	システム運用担当者は、運用業務実施責任者と連携し、不要な特権アカウントの削除を行う。
G11	システム運用担当者は、各部門から提出された棚卸回答を受領する
G12	システム運用管理者は、機関等担当者、地方防衛局担当者から受領した回答内容を精査し、適切に処理がされているか（確認事項への回答が十分か、必要な追加申請がなされているか）を確認する。
G13	前項の確認結果により処理が分岐する。
G14	システム運用担当者は、機関等担当者、地方防衛局担当者から受領した回答内容が「不十分」であったことから、追加対応の実施を求める。
G15	システム運用担当者は、以下の対応結果を「棚卸結果報告書」としてとりまとめる。 また、運用業務実施責任者から内容の修正を指示された際は対応する。 ・「個人アカウント登録・個人端末利用等申請書」及び 「機関共有フォルダ作成等申請書」の回答結果 ・特権アカウントの要不要確認検討結果
H1	SOC担当者は、運用業務実施責任者と連携し、棚卸の結果でリストアップされた特権アカウント（SOC運用関連アカウント）の要不要について確認する。
H2	確認結果、不要な特権アカウントが「存在するか」「存在しないか」で処理が分岐する。
H3	SOC担当者は、運用業務実施責任者と連携し、不要な特権アカウントの削除を行う。
J1	保守業務担当者は、運用業務実施責任者と連携し、棚卸の結果でリストアップされた特権アカウント（保守業務関連アカウント）の要不要について確認する。
J2	確認結果、不要な特権アカウントが「存在するか」「存在しないか」で処理が分岐する。
J3	保守業務担当者は、運用業務実施責任者と連携し、不要な特権アカウントの削除を行う。

フロー名称	説明	作業トリガー
リスク管理枠組み情報提供支援	「継続監視」とは、セキュリティ計画書で定めた管理策が、適切に機能していることを継続的・体系的に確認し、課題を発見した際は対応・見直しを行う活動である。 本フローは、見直し結果を反映し「継続監視計画書」「将来対応計画書」「セキュリティ計画書」の更新に必要な情報を提供する支援業務である。	官の更新スケジュールに則って、四半期ごとに実施する。



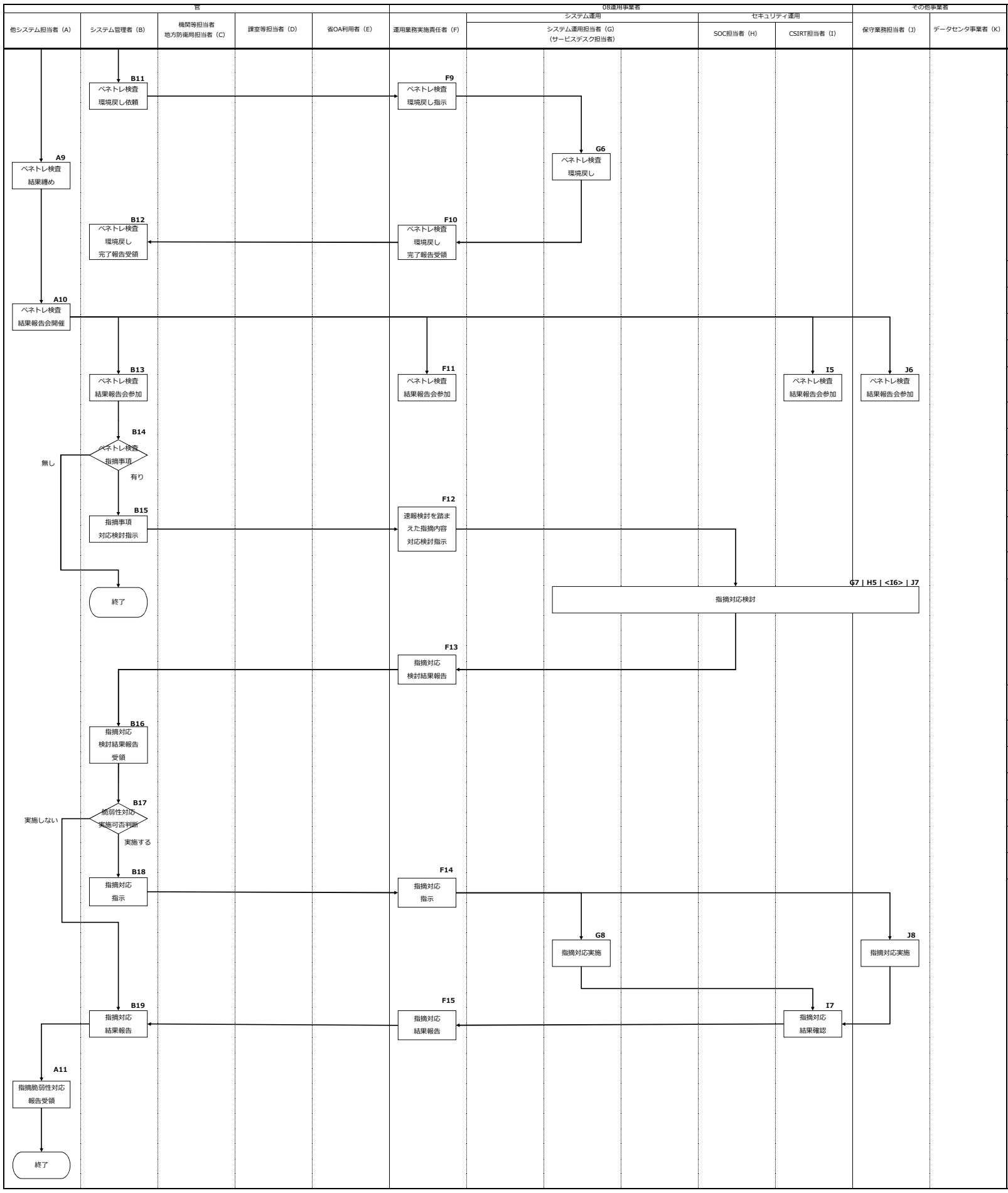
項番	説明
B1	システム管理者は、官の更新スケジュールに沿って「セキュリティ計画書」に定められた管理策の履行状況について、期限を定めて情報提供を依頼する。 ※運用、保守の確認期間として、原則として1カ月前を目安の依頼とする
B2	システム管理者は、運用業務実施責任者より「セキュリティ計画書」に定められた管理策が正しく履行されている旨の報告を受ける。
B3	システム管理者は、運用業務実施責任者より「セキュリティ計画書」に定められた管理策のうち、未実装または不備のある管理策があることについて報告を受ける。
B4	システム管理者は報告内容を踏まえ、「セキュリティ計画書」の未実装または不備のある管理策について「将来対応計画書」「セキュリティ計画書」の更新に必要な情報の提供を運用業務実施責任者に依頼する。
B5	システム管理者は、運用業務実施責任者から提示された「将来対応計画書」「セキュリティ計画書」の「情報提供案」を確認する。
B6	システム管理者は、提示された「情報提供案」を確認し、再検討の要不要を判断する。 ・再検討が必要：運用業務実施責任者その旨を指示する。 ・再検討は不要：「情報提供案」を参考に「将来対応計画書」「セキュリティ計画書」の更新を実施する。
B7	システム管理者は、「情報提供案」を参考に「将来対応計画書」「セキュリティ計画書」の更新を実施する。
F1	運用業務実施責任者は、システム管理者より「セキュリティ計画書」の管理策の履行状況について、確認依頼を受領する。
F2	運用業務実施責任者は、システム運用担当者、SOC担当者に、「セキュリティ計画書」の管理策の履行状況について、情報収集を指示する。
F3	運用業務実施責任者は、システム運用担当者およびSOC担当者から情報収集の確認結果を受けとり、情報のとりまとめを行う。 実施日と確認結果を継続監視結果報告書に記載する。
F4	運用業務実施責任者は、「セキュリティ計画書」に定められた管理策の履行状況の確認結果に基づき、未実装や不備の有無によって、その後の対応が分岐する。
F5	運用業務実施責任者は、「セキュリティ計画書」に定められた管理策が正しく履行されていることを、システム管理者へ報告する。
F6	運用業務実施責任者は、「セキュリティ計画書」に定められた管理策のうち、未実装または不備のある管理策があることを、システム管理者へ報告する。
F7	運用業務実施責任者は、システム管理者より「セキュリティ計画書」の未実装または不備のある管理策について、「将来対応計画書」「セキュリティ計画書」の更新に必要な情報提供の依頼を受ける。
F8	運用業務実施責任者は、システム運用担当者及びSOC担当者と協力し、「将来対応計画書」「セキュリティ計画書」の「情報提供案」を検討する。
F9	運用業務実施責任者は、「将来対応計画書」「セキュリティ計画書」の「情報提供案」を提示する。
G1	システム運用担当者は、「セキュリティ計画書」に定められた管理策の履行状況について、情報収集の指示を受ける。
G2	システム運用担当者は、「セキュリティ計画書」に定められた管理策の履行状況について、情報を収集する。 ※エビデンスを取得すること
G3	システム運用担当者は、情報収集の確認結果を運用業務実施責任者へ報告する。
G4	システム運用担当者は、運用業務実施責任者の指示の下、「将来対応計画書」「セキュリティ計画書」の「情報提供案」を検討する。
H1	SOC担当者は、「セキュリティ計画書」に定められた管理策の履行状況について、情報収集の指示を受ける。
H2	SOC担当者は、「セキュリティ計画書」に定められた管理策の履行状況について、情報を収集し、CSIRT担当者へ報告内容を確認する。 ※エビデンスを取得すること
H3	SOC担当者は、情報収集の確認結果を運用業務実施責任者へ報告する。
H4	SOC担当者は、運用業務実施責任者の指示の下、「将来対応計画書」「セキュリティ計画書」の「情報提供案」を検討する。
I1	CSIRT担当者は、SOC担当者より報告内容に関する確認依頼を受け、内容を精査した上で対応指示を行う。
J1	保守業務担当者は、システム管理者より「セキュリティ計画書」の管理策の履行状況について、確認依頼を受領する。
J2	保守業務担当者は、「セキュリティ計画書」に定められた管理策の履行状況について調査する。
J3	保守業務担当者は、「セキュリティ計画書」に定められた管理策履行状況の調査結果をシステム管理者へ報告する。

フロー名称	説明	作業トリガー
官によるペネトレーションテスト、脆弱性検査の支援	官からペネトレーションテスト、脆弱性検査（以下「ペネトレ検査」という）の 支援依頼があった際の対処フローを示す	官からのペネトレーションテスト、脆弱性検査の支援依頼



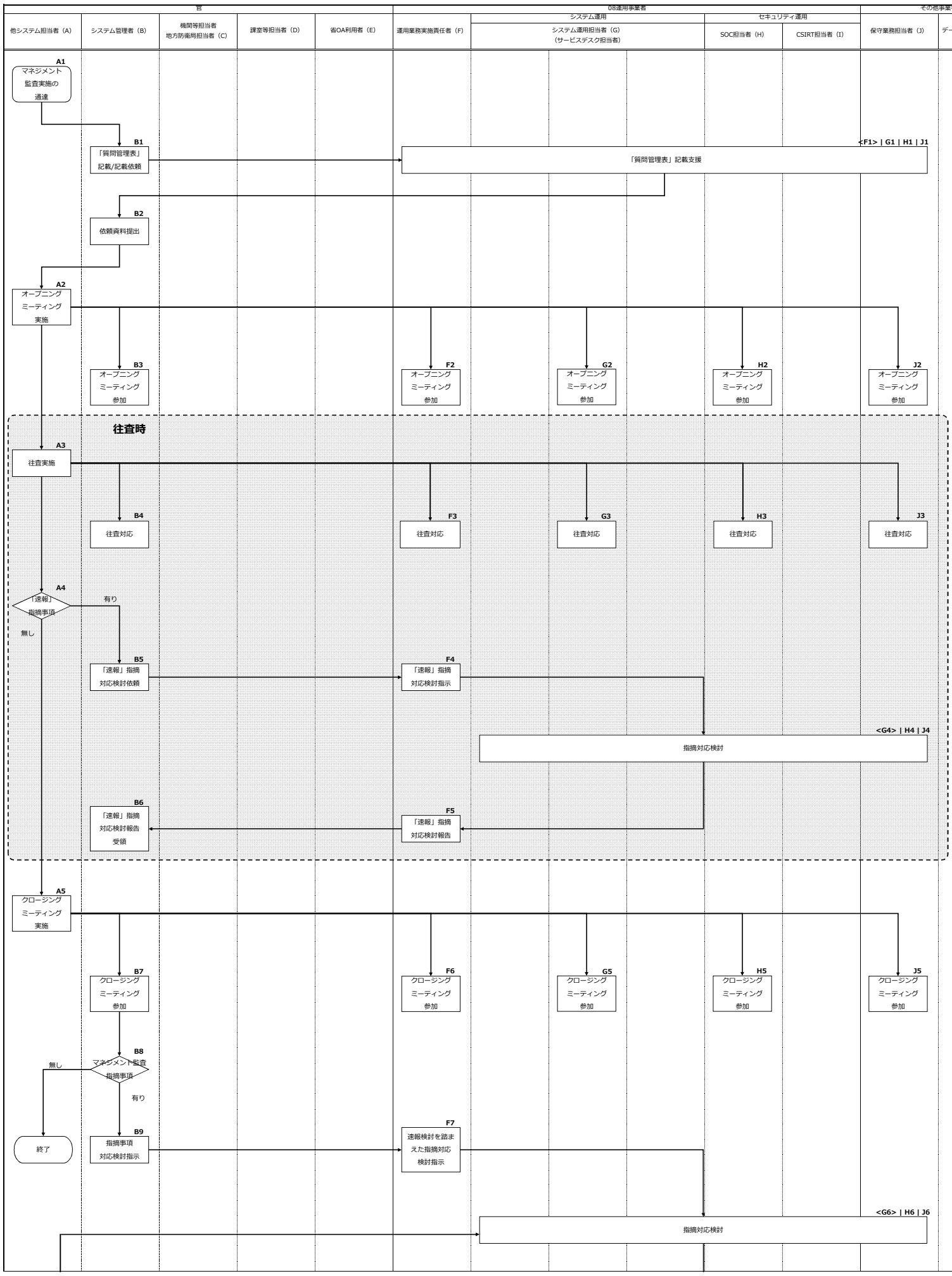
項番	説明
A1	ペネトレーション実施事業者は、ペネトレーションテスト、脆弱性検査の実施を対象システム管理者へ通達する。
A2	ペネトレーション実施事業者は、ペネトレーションテスト、脆弱性検査の事前説明会を実施する。
A3	ペネトレーション実施事業者は、システム構成が分かる指定資料の提出依頼とヒアリングシート記載の依頼を行う。
A4	ペネトレーション実施事業者は、提出された資料とヒアリングシートに基づいてシステム担当者へヒアリングを実施する。
A5	ペネトレーション実施事業者は、検査当日までに準備してほしい項目を連携する。また、準備に必要な情報をシステム管理者へ連携する。 ・検査作業員作業場所の確保依頼 ・アカウントの払い出し依頼 ・IPアドレス払い出し依頼 ・持ち込み端末のネットワーク接続許可設定依頼 ・当日検査担当者情報提供 ・持ち込み端末情報提供、など
A6	ペネトレーション実施事業者は、ペネトレーションテスト、脆弱性検査を実施する。 検査当日はペネトレーションテスト・脆弱性検査実施中を意識したシステム監視を依頼しておき、検査の影響だと思われるアラートが発生したら連携してもらう。
A7	ペネトレーション実施事業者は、検査の途中で速報すべき脆弱性を発見したら検査完了を待たずにシステム管理者へ連携を行う。
A8	ペネトレーション実施事業者は、予定した検査が完了したことを報告する。
A9	ペネトレーション実施事業者は、予定した検査が完了した後に検査結果の纏めを行う。
A10	ペネトレーション実施事業者は、ペネトレーションテスト、脆弱性検査の結果報告会を開催する。
A11	ペネトレーション実施事業者は、ペネトレーションテスト、脆弱性検査で指摘した項目に対する対応結果を受領する。
B1	システム管理者は、ペネトレーションテスト、脆弱性検査実施の通達、実施時期の調整依頼が有り次第、運用事業者にその予定を伝え、支援依頼を行う。
B2	システム管理者は、ペネトレーションテスト、脆弱性検査の事前説明会に参加する。
B3	システム管理者は、ペネトレーション実施事業者から依頼されたヒアリングシートの記載支援依頼を行う。
B4	システム管理者は、ペネトレーション実施事業者から依頼されるヒアリングシートの記載を行う。
B5	システム管理者は、記載したヒアリングシートとペネトレーション実施事業者から提出を求められた資料を提出する。
B6	システム管理者は、提出した資料とヒアリングシートに基づいてペネトレーション実施事業者からヒアリングを受ける。
B7	システム管理者は、ペネトレーション実施事業者から検査に必要な準備の依頼、検査担当者や持ち込み端末の情報を受領する。 検査に必要な環境準備を運用事業者へ依頼する。
B8	システム管理者は、検査に必要な環境準備完了の報告を受ける。
B9	システム管理者は、「速報」として報告を受けた脆弱性の対応検討依頼を行う。
B10	システム管理者は、「速報」として対応検討依頼を行った結果報告を受領する。
B11	システム管理者は、ペネトレ検査のために行った環境準備の戻し対応を依頼する。
B12	システム管理者は、ペネトレ検査のために行った環境準備の戻し対応完了報告を受領する。
B13	システム管理者は、ペネトレーションテスト、脆弱性検査の結果報告会に参加する。
B14	システム管理者は、ペネトレーションテスト、脆弱性検査の結果報告会の内容を踏まえ脆弱性の指摘事項確認する。
B15	システム管理者は、ペネトレーションテスト、脆弱性検査の結果報告会で指摘を受けた脆弱性の対応検討依頼を行う。
B16	システム管理者は、指摘対応検討の報告を受領し、指摘脆弱性対応でのシステムへ影響有無や対応スケジュールを確認する。
B17	システム管理者は、指摘対応検討の報告を受領し、実施するかの判断を行う。
B18	システム管理者は、指摘対応検討の結果を踏まえ、脆弱性の対応依頼を行う。
B19	システム管理者は、運用事業者から脆弱性の対応報告を受領し、ペネトレーション実施事業者へ報告を行う。
F1	運用業務実施責任者は、システム管理者からペネトレーションテスト、脆弱性検査の支援依頼を受けた後、システム運用担当者、SOC担当者、保守業務担当者へペネトレ検査前の最終確認を依頼する。
F2	運用業務実施責任者は、システム管理者と共にペネトレーションテスト、脆弱性検査の事前説明会に参加する。システムに関して技術的な質問があった際に適宜回答を行う。
F3	運用業務実施責任者が主体となり、ペネトレーションテスト、脆弱性検査のヒアリングシート記載支援を行う。 記載する内容に応じて担当者のアサインを行う。
F4	運用業務実施責任者が主体となり、提出した資料とヒアリングシートに基づいてペネトレーション実施事業者からヒアリングを受ける。 ヒアリング内容に応じて担当者のアサインを行う。
F5	運用業務実施責任者は、ペネトレ検査環境準備の依頼を行う。
F6	運用業務実施責任者は、ペネトレ検査環境準備の完了報告を行う。
F7	運用業務実施責任者は、「速報」として指摘を受けた脆弱性の対応検討依頼を行う。
F8	運用業務実施責任者は、「速報」として指摘を受けた脆弱性の対応検討結果と、緊急性が高く即時対応可能な脆弱性対応を行う旨を報告する。
F9	運用業務実施責任者は、ペネトレ検査環境戻しの依頼を行う。
F10	運用業務実施責任者は、ペネトレ検査環境戻しの完了報告を行う。
F11	運用業務実施責任者は、ペネトレーションテスト、脆弱性検査の結果報告会に参加する。
F12	運用業務実施責任者は、ペネトレーションテスト、脆弱性検査の結果報告会の内容を受け、速報の指摘以外の対応検討依頼を行う。
F13	運用業務実施責任者は、脆弱性対応を行った際のシステム影響有無や実施スケジュールなどの対応検討結果の報告を行う。
F14	運用業務実施責任者は、システム管理者から依頼を受けた脆弱性の対応依頼を行う。
F15	運用業務実施責任者は、脆弱性対応結果の報告を行う。
G1	システム運用担当者が主体となり、ペネトレーションテスト、脆弱性検査実施の連絡を受けた際に検査前の最終確認を行う。 ・脆弱性対応パッチが未適用のサーバ/機器が無いかの確認。 ・不要なアカウントが無いかの確認。 ・パスワードの管理台帳を見て、複雑なPWになっているか、ＰＷの使いまわしがないか、ドメイン管理者の数が合致しているか、の確認。 ・ユーザ/パスワードの情報が平文で各サーバやファイルサーバに置かれていないかの確認。 ・業務上必要ない管理画面へアクセス出来るなど、余計な通信が許可されていないかの確認。
G2	システム運用担当者は、ペネトレーションテスト、脆弱性検査のヒアリングシート記載支援を行う。
G3	システム運用担当者は、提出した資料とヒアリングシートに基づいてペネトレーション実施事業者からヒアリングを受ける。
G4	システム運用担当者は、ペネトレーション実施事業者から依頼された環境準備を行う。 ・アカウントの払い出し ・IPアドレス払い出し ・持ち込み端末のネットワーク接続許可設定 など

フロー名称	説明	作業トリガー
官によるペネトレーションテスト、脆弱性検査の支援	官からペネトレーションテスト、脆弱性検査（以下「ペネトレ検査」という）の 支援依頼があった際の対処フローを示す	官からのペネトレーションテスト、脆弱性検査の支援依頼



項番	説明
G5	システム運用担当者は、指摘された脆弱性対応を行った際のシステム影響確認や、実施可能なスケジュール立案などの脆弱性対応検討を行う。
G6	システム運用担当者は、ペネトレーション実施事業者から依頼された環境準備の戻し作業を行う。
G7	システム運用担当者は、指摘された脆弱性対応を行った際のシステム影響確認や、実施可スケジュール計画など、脆弱性対応検討を行う。
G8	システム運用担当者は、指摘された脆弱性対応を行う。
H1	SOC担当者は、ペネトレーションテスト、脆弱性検査実施の連絡を受けた際に検査前の最終確認を行う。 ・脆弱性対応パッチが未適用のサーバ/機器が無いかの確認。 ・不要なアカウントが無いかの確認。 ・パスワードの管理台帳を見て、複雑なPWになっているか、ＰＷの使いまわしがないか、ドメイン管理者の数が合致しているか、の確認。 ・ユーザ/パスワードの情報が平文で各サーバやファイルサーバに置かれていないかの確認。 ・業務上必要ない管理画面へアクセス出来るなど、余計な通信が許可されていないかの確認。
H2	SOC担当者は、ペネトレーションテスト、脆弱性検査のヒアリングシート記載支援を行う。
H3	SOC担当者は、提出した資料とヒアリングシートに基づいてペネトレーション実施事業者からヒアリングを受ける。
H4	SOC担当者は、指摘された脆弱性対応を行った際のシステム影響確認を行う。
H5	SOC担当者は、指摘された脆弱性対応を行った際のシステム影響確認を行う。
I1	CSIRT担当者は、システム管理者と共にペネトレーションテスト、脆弱性検査の事前説明会に参加する。システムに関して技術的な質問があった際に適宜回答を行う。
I2	CSIRT担当者は、ペネトレーションテスト、脆弱性検査のヒアリングシート記載支援を行う。
I3	CSIRT担当者は、提出した資料とヒアリングシートに基づいてペネトレーション実施事業者からヒアリングを受ける。
I4	CSIRT担当者は主体となり、指摘された脆弱性対応を行った際のシステム影響確認を行う。 指摘の内容により主体が変更となる場合もある。
I5	CSIRT担当者は、ペネトレーションテスト、脆弱性検査の結果報告会に参加する。
I6	CSIRT担当者は主体となり、指摘された脆弱性対応を行った際のシステム影響確認を行う。 指摘の内容により主体が変更となる場合もある。
I7	CSIRT担当者は、指摘された脆弱性対応実施後に対応結果に問題が無いか確認する。
J1	保守業務担当者は、ペネトレーションテスト、脆弱性検査実施の連絡を受けた際に検査前の最終確認を行う。 ・脆弱性対応パッチが未適用のサーバ/機器が無いかの確認。 ・不要なアカウントが無いかの確認。 ・パスワードの管理台帳を見て、複雑なPWになっているか、ＰＷの使いまわしがないか、ドメイン管理者の数が合致しているか、の確認。 ・ユーザ/パスワードの情報が平文で各サーバやファイルサーバに置かれていないかの確認。 ・業務上必要ない管理画面へアクセス出来るなど、余計な通信が許可されていないかの確認。
J2	保守業務担当者は、システム管理者と共にペネトレーションテスト、脆弱性検査の事前説明会に参加する。システムに関して技術的な質問があった際に適宜回答を行う。
J3	保守業務担当者は、ペネトレーションテスト、脆弱性検査のヒアリングシート記載支援を行う。
J4	保守業務担当者は、提出した資料とヒアリングシートに基づいてペネトレーション実施事業者からヒアリングを受ける。
J5	保守業務担当者は、指摘された脆弱性対応を行った際のシステム影響確認や、実施可能なスケジュールの立案など、脆弱性対応検討を行う。
J6	保守業務担当者は、ペネトレーションテスト、脆弱性検査の結果報告会に参加する。
J7	保守業務担当者は、指摘された脆弱性対応を行った際のシステム影響確認や、実施可スケジュール計画など、脆弱性対応検討を行う。
J8	保守業務担当者は、指摘された脆弱性対応を行う。

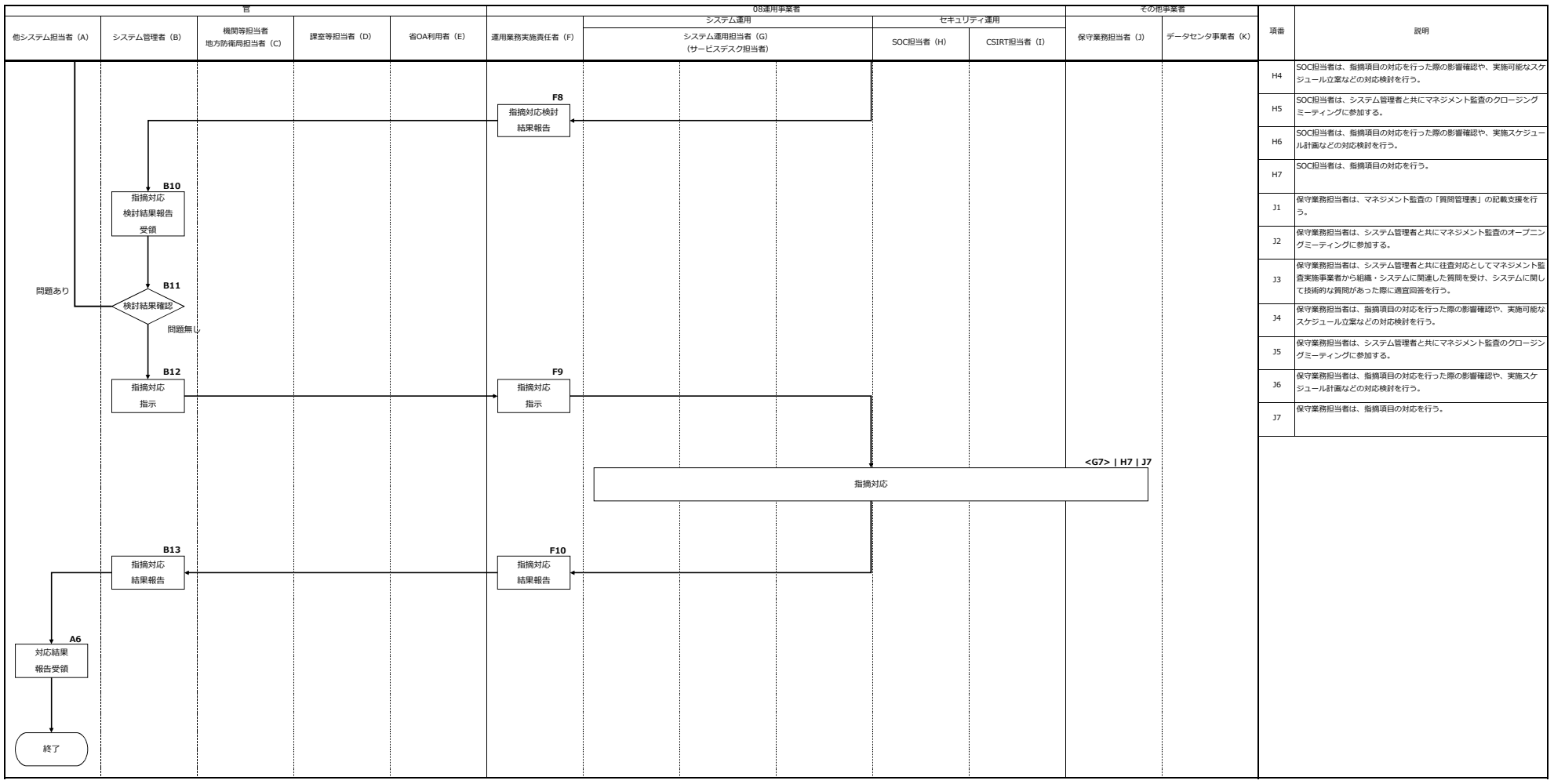
フロー名称	説明	作業トリガー
官によるマネジメント監査の支援	「政府機関等のサイバーセキュリティ対策のための統一基準群」に基づく省OAシステムにおける施策の取り組み状況について、NCOによるマネジメント監査が実施されることがある。 このマネジメント監査を受けるに当たり、官から支援依頼があった際の対処フローを示す。	官からのマネジメント監査の支援依頼



項番	説明
A1	マネジメント監査実施事業者は、マネジメント監査実施を対象システム管理者へ通達し、事前準備の依頼を行う。 ・「依頼資料管理表」記載資料の準備と共有 ・「質問管理表」に記載の質問への回答 ・ミーティング及びインタビューへ適切な担当者へのアサインとスケジュール確保 ・サーバ室視察の実施調整 ・会議スペースの確保（電源確保）
A2	マネジメント監査実施事業者は、オープニングミーティングを実施する。 ・往査中のスケジュール概要説明 ・依頼事項の確認 ・事前準備資料の確認
A3	マネジメント監査実施事業者は、往査を実施する。往査は数日に渡って行われる。 ・対象組織・システムに関連した共有資料に関わる質問 ・サーバ室の視察 など
A4	マネジメント監査実施事業者は、発見事項について往査当日に速報レベルでシステム管理者へ共有する。
A5	マネジメント監査実施事業者は、クロージングミーティングを実施して監査の総括と今後の進め方に関する概要説明を行う。
A6	マネジメント監査実施事業者は、マネジメント監査で指摘した項目に対する対応結果を受領する。
B1	システム管理者は、マネジメント監査実施事業者から依頼される事前資料送付と「質問管理表」の記載を行う。 また、運用事業者へ「質問管理表」記載支援の依頼を行う。
B2	システム管理者は、記載した「質問管理表」とマネジメント監査実施事業者から提出を求められた資料を提出する。
B3	システム管理者は、マネジメント監査のオープニングミーティングに参加する。
B4	システム管理者は、往査対応としてマネジメント監査実施事業者から組織・システムに関連した質問を受ける。 また、サーバ室視察の立会を行う。
B5	システム管理者は、「速報」として報告を受けた指摘の調査、対応検討を運用実施責任者に対して行う。
B6	システム管理者は、「速報」として報告を受けた指摘の対応検討結果を、運用業務実施責任者から受領する。
B7	システム管理者は、マネジメント監査のクロージングミーティングに参加する。
B8	システム管理者は、クロージングミーティングの監査の総括と結果を踏まえ指摘事項の確認を行う。
B9	システム管理者は、クロージングミーティングで指摘を受けた項目の対応検討を運用実施責任者に対して行う。
B10	システム管理者は、クロージングミーティングで指摘を受けた項目の対応検討結果を受領する。
B11	システム管理者は、指摘対応検討の報告を受領し、検討結果に問題が無いかの判断を行う。
B12	システム管理者は、対応検討結果を踏まえて指摘対応依頼を運用実施責任者に対して行う。
B13	システム管理者は、指摘を受けた項目の対応結果を受領し、マネジメント監査側へ報告する。
F1	運用業務実施責任者が主体となり、マネジメント監査の「質問管理表」の記載支援を行う。
F2	運用業務実施責任者は、システム管理者と共にマネジメント監査のオープニングミーティングに参加する。
F3	運用業務実施責任者は、システム管理者と共に往査対応としてマネジメント監査実施事業者から組織・システムに関連した質問を受け、システムに関して技術的な質問があった際に適宜回答を行う。
F4	運用業務実施責任者は、「速報」として報告を受けた指摘事項の対応検討をシステム運用担当者、SOC担当者、保守業務担当者へ行う。
F5	運用業務実施責任者は、各担当者からの対応検討報告を受け、その結果をシステム管理者へ報告する。
F6	運用業務実施責任者は、システム管理者と共にマネジメント監査のクロージングミーティングに参加する。
F7	運用業務実施責任者は、クロージングミーティングで報告を受けた指摘事項の内、速報で指摘を受けたもの以外の対応検討依頼を行う。対応検討をシステム運用担当者、SOC担当者、保守業務担当者へ行う。
F8	運用業務実施責任者は、各担当者からの対応検討報告を受け、その結果をシステム管理者へ報告する。
F9	運用業務実施責任者は、指摘事項の対応依頼をシステム運用担当者、SOC担当者、保守業務担当者へ行う。
F10	運用業務実施責任者は、各担当者からの対応結果報告を受け、その結果をシステム管理者へ報告する。
G1	システム運用担当者は、マネジメント監査の「質問管理表」の記載支援を行う。
G2	システム運用担当者は、システム管理者と共にマネジメント監査のオープニングミーティングに参加する。
G3	システム運用担当者は、システム管理者と共に往査対応としてマネジメント監査実施事業者から組織・システムに関連した質問を受け、システムに関して技術的な質問があった際に適宜回答を行う。
G4	システム運用担当者は主体となり、指摘項目の対応を行った際の影響確認や、実施可能なスケジュール立案などの対応検討を行う。
G5	システム運用担当者は、システム管理者と共にマネジメント監査のクロージングミーティングに参加する。
G6	システム運用担当者は主体となり、指摘項目の対応を行った際の影響確認や、実施スケジュール計画などの対応検討を行う。
G7	システム運用担当者は主体となり、指摘項目の対応を行う。
H1	SOC担当者は、マネジメント監査の「質問管理表」の記載支援を行う。
H2	SOC担当者は、システム管理者と共にマネジメント監査のオープニングミーティングに参加する。
H3	SOC担当者は、システム管理者と共に往査対応としてマネジメント監査実施事業者から組織・システムに関連した質問を受け、システムに関して技術的な質問があった際に適宜回答を行う。

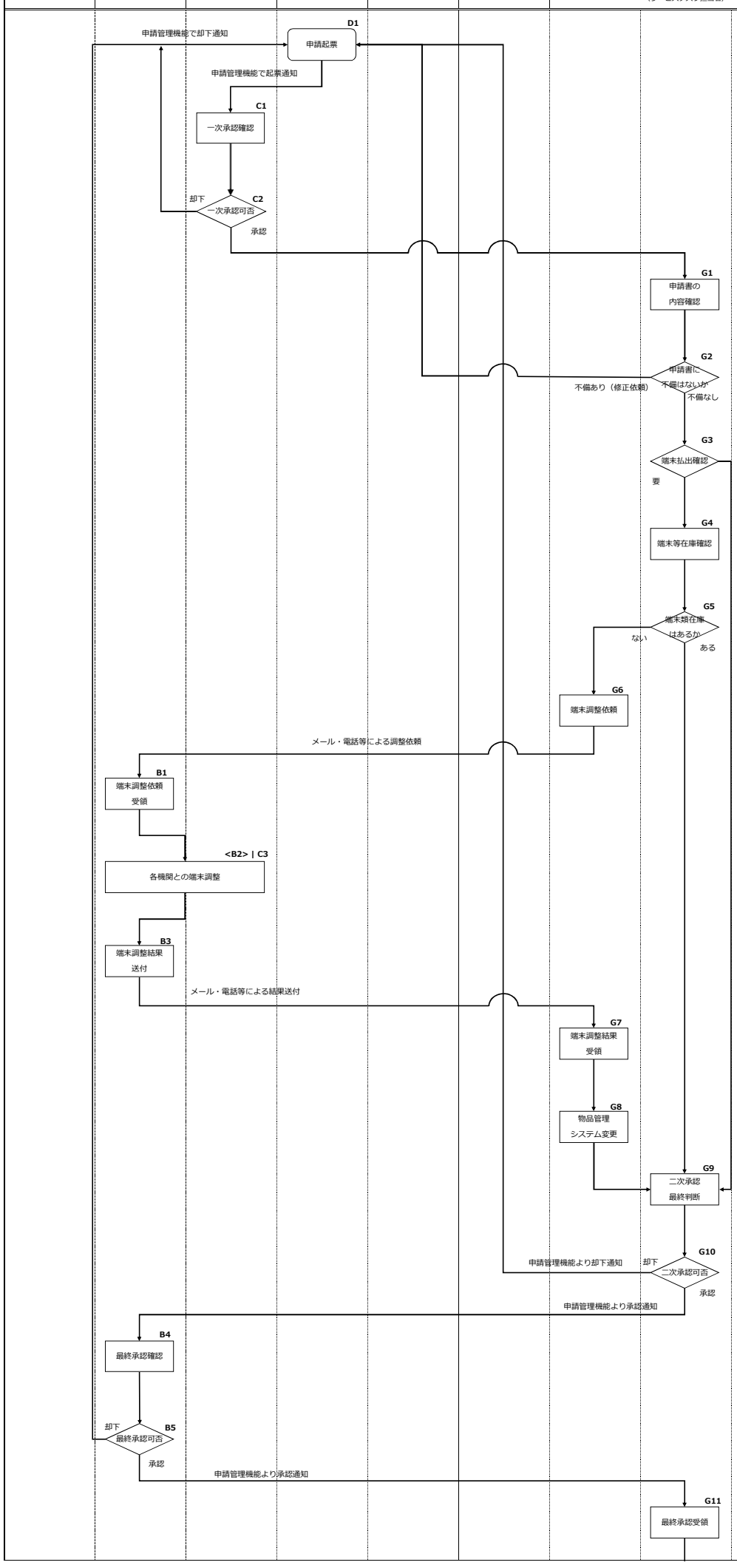
付表１０　業務フロー（続き）
官によるマネジメント監査の支援（続き）

フロー名称	説明	作業トリガー
官によるマネジメント監査の支援	「政府機関等のサイバーセキュリティ対策のための統一基準群」に基づく省OAシステムにおける施策の取り組み状況について、NCOによるマネジメント監査が実施されることがある。 このマネジメント監査を受けるに当たり、官から支援依頼があった際の対処フローを示す。	官からのマネジメント監査の支援依頼



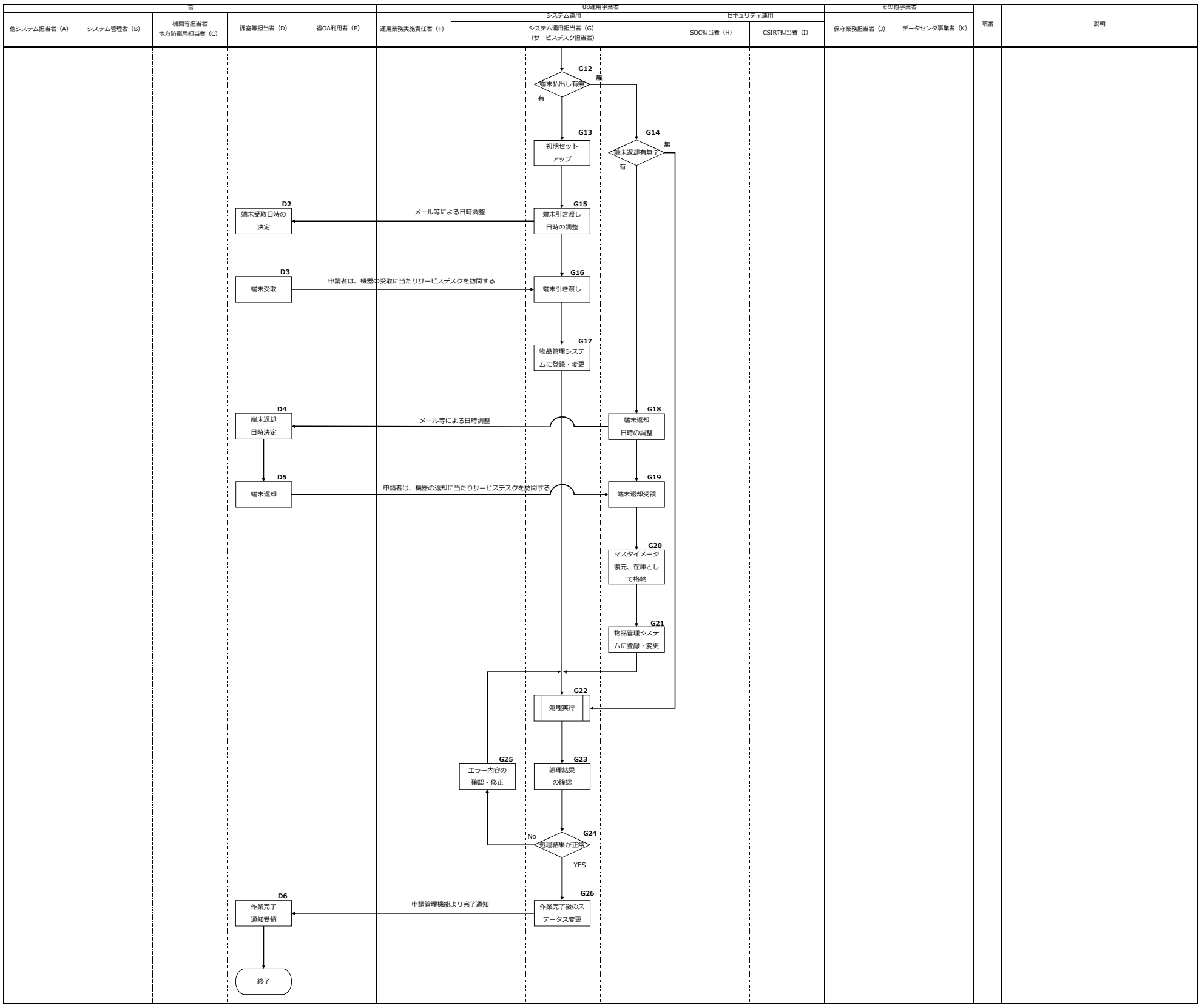
項番	説明
H4	SOC担当者は、指摘項目の対応を行った際の影響確認や、実施可能なスケジュール立案などの対応検討を行う。
H5	SOC担当者は、システム管理者と共にマネジメント監査のクロージングミーティングに参加する。
H6	SOC担当者は、指摘項目の対応を行った際の影響確認や、実施スケジュール計画などの対応検討を行う。
H7	SOC担当者は、指摘項目の対応を行う。
J1	保守業務担当者は、マネジメント監査の「質問管理表」の記載支援を行う。
J2	保守業務担当者は、システム管理者と共にマネジメント監査のオープニングミーティングに参加する。
J3	保守業務担当者は、システム管理者と共に往査対応としてマネジメント監査実施事業者から組織・システムに関連した質問を受け、システムに関して技術的な質問があった際に適宜回答を行う。
J4	保守業務担当者は、指摘項目の対応を行った際の影響確認や、実施可能なスケジュール立案などの対応検討を行う。
J5	保守業務担当者は、システム管理者と共にマネジメント監査のクロージングミーティングに参加する。
J6	保守業務担当者は、指摘項目の対応を行った際の影響確認や、実施スケジュール計画などの対応検討を行う。
J7	保守業務担当者は、指摘項目の対応を行う。

フロー名称	説明	作業トリガー
個人アカウント登録・個人端末利用等申請書対応	「個人アカウント登録・個人端末利用等申請書」の起票に係る、 アカウント登録や端末払出に係るフローを示す	省OA課室担当者からの申請依頼

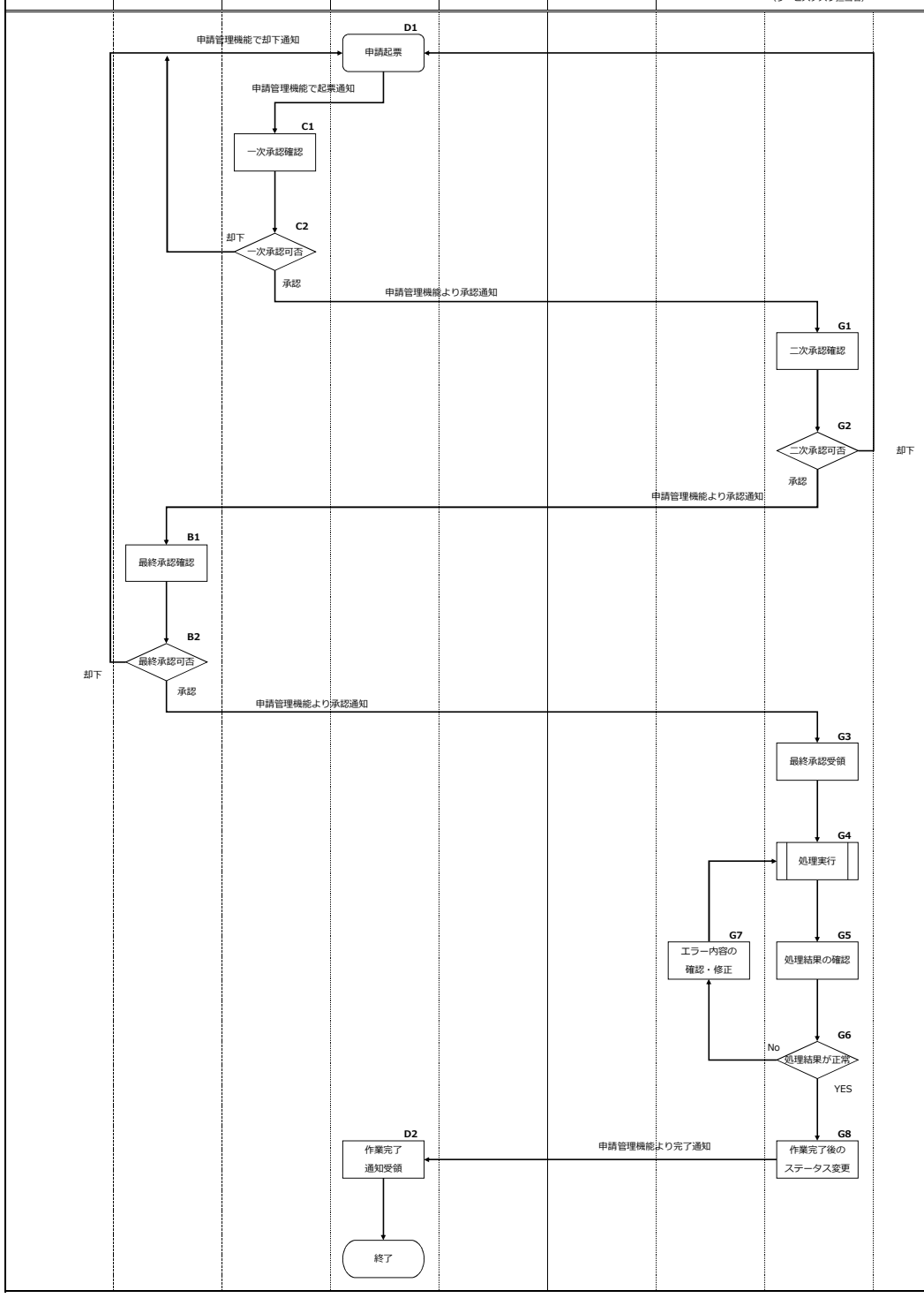


項番	説明
B1	システム管理者は、システム運用担当者より端末調整依頼を受領する。
B2	システム管理者が主体となり、機関等担当者と端末調整を行う。
B3	システム管理者は、システム運用担当者へ端末調整結果を送付する。
B4	システム管理者は、「個人アカウント登録・個人端末利用等申請書」の内容を確認し、申請内容に関する処理の実施可否の最終判断を行う。
B5	システム管理者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C1	機関等担当者は、起票された「個人アカウント登録・個人端末利用等申請書」の内容を確認し、その妥当性や、申請内容に不備が無いか確認を行う。
C2	機関等担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C3	機関等担当者は、システム管理者と端末調整を行う。
D1	課室等担当者は、申請管理機能で個人アカウント登録・個人端末利用等申請を起票する。
D2	課室等担当者は、システム運用担当者からの連絡を受けて、端末受取日時の決定を行う。
D3	課室等担当者は、申請者は、サービスデスクを訪問し端末の受取を行う。
D4	課室等担当者は、システム運用担当者からの連絡を受けて、端末返却日時の決定を行う。
D5	課室等担当者は、サービスデスクを訪問し端末の返却を行う。
D6	課室等担当者は、「個人アカウント登録・個人端末利用等申請書」の申請処理がすべて完了した旨を、申請管理機能上で確認する。
G1	システム運用担当者は、二次承認確認を行う ・申請理由が適切かどうか確認する ・個人端末の要・不要について確認する ・実施希望日を確認する ・特記事項に、考慮しなくてはならない事項が記載されてないか確認する ・端末返却有無について確認する ・不備、漏れや誤字などないか確認する
G2	システム運用担当者は、申請書の不備の有無の確認結果、不備があった場合はその個所の指摘と共に申請者に戻す。
G3	システム運用担当者は、申請書を基に、端末の払出の要不要の判断を行う。
G4	システム運用担当者は、申請内容に端末の払い出しを求めるものであった場合、払い出し可能な端末の予備在庫があるか確認する。
G5	システム運用担当者は、確認結果、端末の予備在庫の「ある」「ない」により、以後の対応内容が分岐する。
G6	システム運用担当者は、端末の予備在庫が「ない」場合、システム管理者へ端末調整依頼を行う。
G7	システム運用担当者は、システム管理者より端末調整結果を受領する。
G8	システム運用担当者は、端末調整結果を基に、物品管理システムの変更作業を行う。
G9	システム運用担当者は、ここまでの一連のやり取りを踏まえ、申請内容を受理するか判断を行う。
G10	システム運用担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。 ・却下する場合は、却下理由と共に申請者に戻す。 ・承認する場合は、システム管理者に申請管理機能により申請内容の最終判断の依頼を行う。
G11	システム運用担当者は、システム管理者からの申請内容に関する最終承認を受け、申請内容の処理に入る。
G12	システム運用担当者は、端末払出作業が発生するかの確認を行う
G13	システム運用担当者は、端末に対して初期セットアップを行う
G14	システム運用担当者は、端末返却有無の判断を行う
G15	システム運用担当者は、払出端末の引き渡し日時の調整を行う。申請者に対しメールや電話を用い連絡する。
G16	システム運用担当者は、申請者に対して、端末の引き渡しを行う。
G17	システム運用担当者は、物品管理システムに対して登録・変更作業を行う。
G18	システム運用担当者は、返却端末の返却日時の調整を行う。申請者に対しメールや電話を用い連絡する。
G19	システム運用担当者は、申請者より端末返却を受領する。
G20	システム運用担当者は、端末初期化作業、マスタイメージ復元、在庫として格納在庫として所定の配置場所に返却端末を格納する。
G21	システム運用担当者は、物品管理システムに対して登録・変更作業を行う。
G22	申請管理機能より、個人アカウントの「他機能連携」による自動処理が行われる。
G23	システム運用担当者は、処理結果のステータス確認を行う。
G24	システム運用担当者は、自動処理の「成功」、「失敗」の判断を行う。 ・「YES」の場合は、「作業完了後のステータス変更」へ ・「NO」の場合は、「エラー内容の確認・修正」へ
G25	システム運用担当者は、エラー内容の確認・修正作業を行う。
G26	システム運用担当者は、処理状態の確認後、「完了」への処理状態の変更操作を行う

フロー名称	説明	作業トリガー
個人アカウント登録・個人端末利用等申請書対応	「個人アカウント登録・個人端末利用等申請書」の起票に係る、 アカウント登録や端末払出に係るフローを示す	省OA課室担当者からの申請依頼

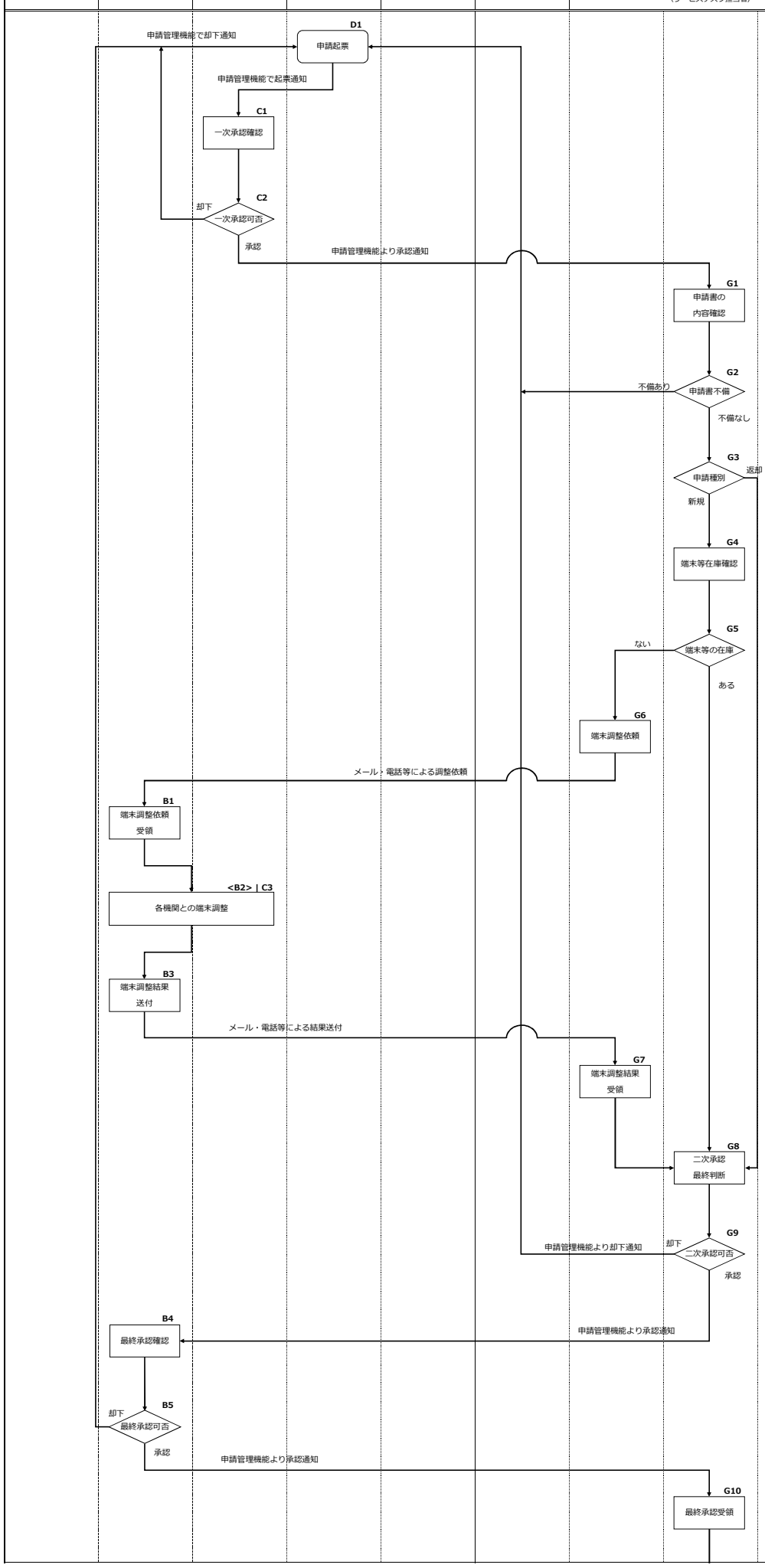


フロー名称	説明	作業トリガー
共有アカウント登録等申請書対応	「共有アカウント登録等申請書」の起票に係る、 共有アカウントの登録や変更に係るフローを示す	課室等担当者からの申請依頼



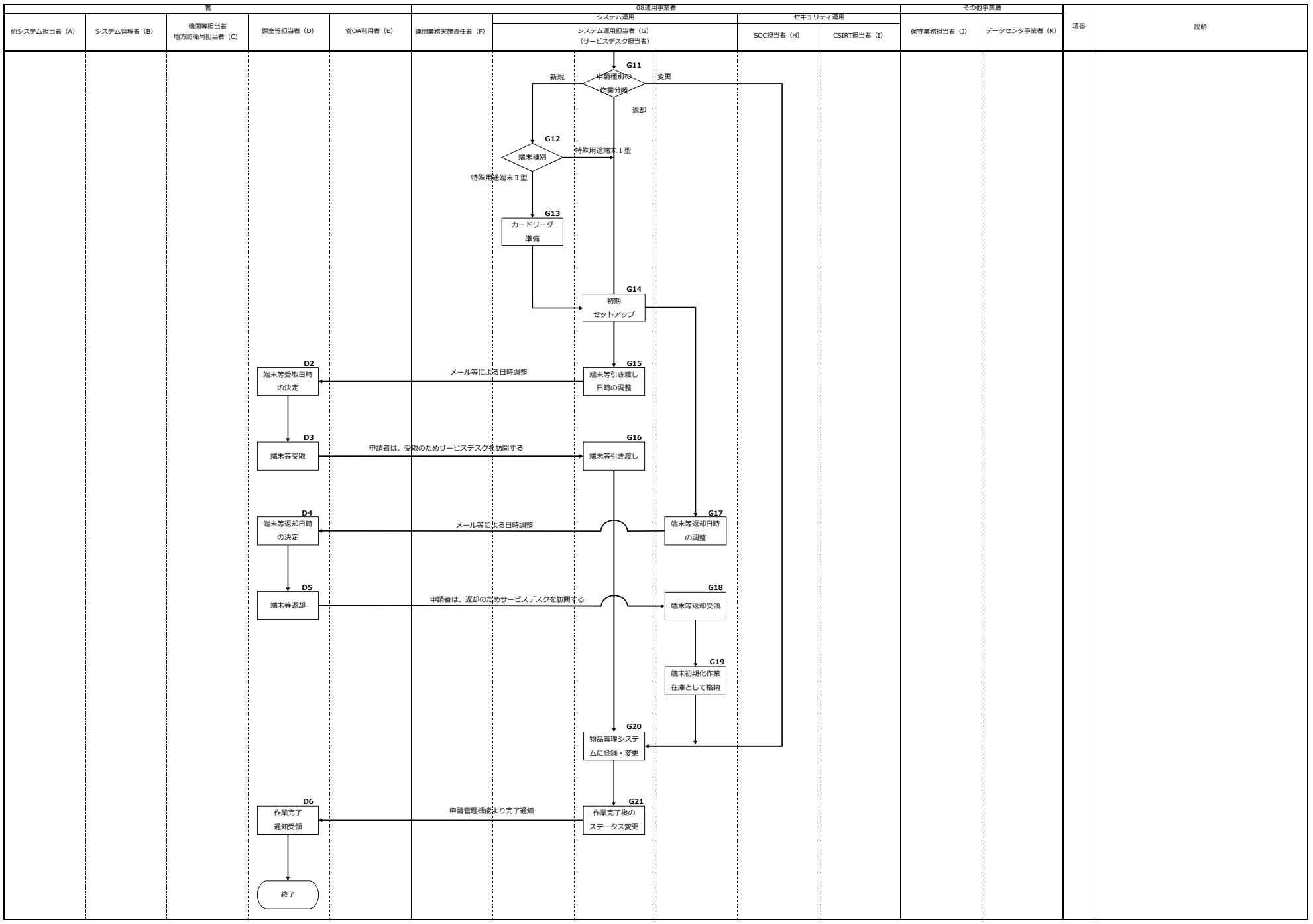
項番	説明
B1	システム管理者は、「共有アカウント登録等申請書」の内容を確認し、申請内容に関する処理の実施可否の最終判断を行う。
B2	システム管理者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C1	機関等担当者、地方防衛局担当者は、起票された「共有アカウント登録等申請書」の内容を確認し、その妥当性や、申請内容に不備が無いか確認を行う。
C2	機関等担当者、地方防衛局担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
D1	課室等担当者は、申請管理機能で共有アカウント登録等申請を起票する。
D2	課室等担当者は、「共有アカウント登録等申請書」の申請処理がすべて完了した旨を、申請管理機能上で確認する。
G1	システム運用担当者は、二次承認確認を行う ・部内系DIIメールのライセンス超過チェックを実施する ・申請種別を確認する ・申請理由が適切かどうか確認する ・希望するメールアドレスを確認する（ユニークチェック） ・実施希望日を確認する
G2	システム運用担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。 ・却下する場合は、却下理由と共に申請者に戻す。 ・承認する場合は、システム管理者に申請管理機能により申請内容の最終判断の依頼を行う。
G3	システム運用担当者は、最終承認を受領する
G4	システム運用担当者は、申請管理機能より、「他機能連携」による自動処理が行われる。
G5	システム運用担当者は、処理結果のステータス確認を行う。
G6	システム運用担当者は、自動処理の「成功」、「失敗」の判断を行う。 ・「YES」の場合は、「作業完了後のステータス変更」へ ・「NO」の場合は、「エラー内容の確認・修正」へ
G7	システム運用担当者は、エラー内容の確認・修正作業を行う。
G8	システム運用担当者は、「完了」への処理状態の変更操作を行う。

フロー名称	説明	作業トリガー
特殊用途端末利用等申請書	「特殊用途端末利用等申請書」の起票に係る、 特殊用途端末の払出し、端末の管理者の登録・返却に係るフローを示す	・省OA課室担当者からの申請依頼

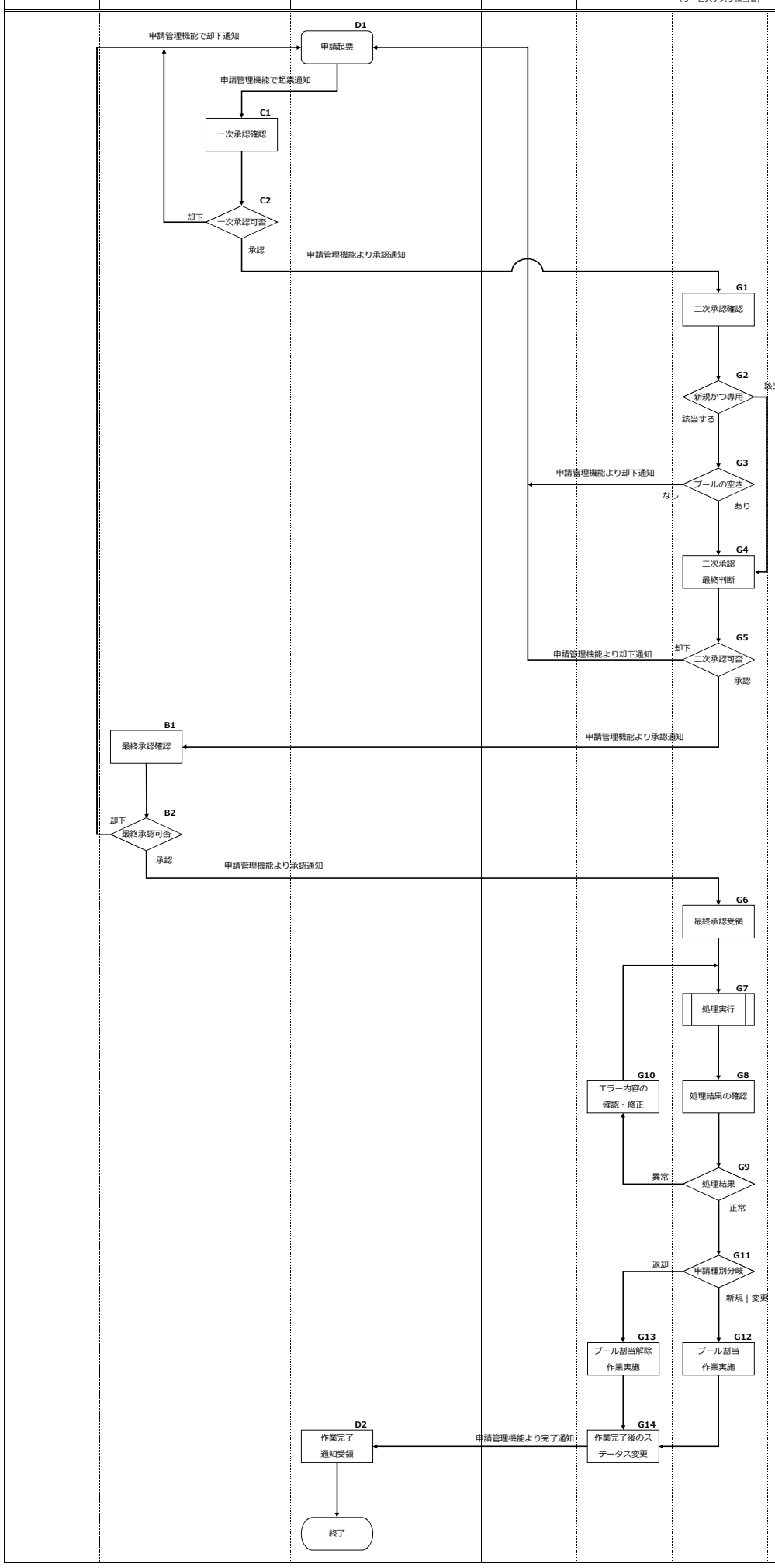


項番	説明
B1	システム管理者は、システム運用担当者より、端末調整依頼を受領する。
B2	システム管理者は、機関等担当者、地方防衛局担当者と連携し、各機関との端末調整を行う。
B3	システム管理者は、システム運用担当者へ端末調整結果を送付する。
B4	システム管理者は、「特殊用途端末利用等申請書」の内容を確認し、申請内容に関する処理の実施可否の最終判断を行う。
B5	システム管理者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C1	機関等担当者、地方防衛局担当者は、起票された「特殊用途端末利用等申請書」の内容を確認し、その妥当性や、申請内容に不備が無いか確認を行う。
C2	機関等担当者、地方防衛局担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C3	機関等担当者、地方防衛局担当者は、各機関との端末調整を行う。
D1	課室等担当者は、申請管理機能を用いて「特殊用途端末利用等申請書」として起票する。
D2	課室等担当者は、運用担当者からの連絡を受けて、端末等の受取日時の決定を行う。
D3	課室等担当者は、サービスデスクを訪問し端末等の受取を行う。
D4	課室等担当者は、運用担当者からの連絡を受けて、端末等の返却日時の決定を行う。
D5	課室等担当者は、サービスデスクを訪問し端末等の返却を行う。
D6	課室等担当者は、「特殊用途端末利用等申請書」の申請処理がすべて完了した旨を、申請管理機能上で確認する。
G1	システム運用担当者は、二次承認確認を行う。 ・申請理由：適切な内容が記載されているか ・端末のホスト名：変更｜返却の場合、ホスト名が正しいものか ・端末ログインに使用するアカウントの種別： 個人アカウント→特殊用途端末Ⅰ型 共有アカウント→特殊用途端末Ⅱ型 ・利用区分： 常設 or 一時利用 ・利用想定人数： 10名以下→特殊用途端末Ⅰ型（個人アカウント） 11名以上→特殊用途端末Ⅱ型（共有アカウント） ※特殊用途端末Ⅱ型の場合「カードリーダ」払い出しが必要 ・実施希望日：5営業日以降の日程が希望されているか ・返却予定日：利用区分が一時利用の場合、日程が記載されているか
G2	システム運用担当者は、申請書の不備の有無の確認結果、不備があった場合はその個所の指摘と共に申請者に戻す。
G3	システム運用担当者は、申請内容に端末の払い出しを求めるものであった場合、払い出し可能な端末の予備在庫があるか確認する。
G4	申請種別により対応が分岐する。新規の場合、端末在庫確認を行う。
G5	確認結果、端末の予備在庫の「ある」「ない」により、以後の対応内容が分岐する。
G6	システム運用担当者は、端末の予備在庫が「ない」場合、システム管理者へ端末調整依頼を行う。
G7	システム運用担当者は、システム管理者より端末調整結果を受領する。
G8	システム運用担当者は、ここまでの一連のやり取りを踏まえ、申請内容を受理するか判断を行う。
G9	システム運用担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。 ・却下する場合は、却下理由と共に申請者に戻す。 ・承認する場合は、システム管理者に申請管理機能により申請内容の最終判断の依頼を行う。
G10	システム運用担当者は、システム管理者からの申請内容に関する最終承認を受け、申請内容の処理に入る。
G11	申請種別に応じた対応が分岐する。 ・新規：物品手配 ・返却：物品返却 ・変更：利用場所、利用区分、返却予定日の変更箇所の変更実施
G12	システム運用担当者は、払い出す端末の種別に応じた対応を行う。
G13	システム運用担当者は、特殊用途端末Ⅱ型の場合、カードリーダおよび白カードを準備する。
G14	システム運用担当者は、所定の手順書を参照し、端末に対して初期セットアップを行う。
G15	システム運用担当者は、申請者に連絡し、端末等の引き渡し日時の調整を行う。
G16	システム運用担当者は、申請者に対して、端末等の引き渡しを行う。
G17	システム運用担当者は、申請者に連絡し、端末等の返却日時の調整を行う。
G18	システム運用担当者は、申請者より端末返却を受領する。
G19	システム運用担当者は、端末初期化作業及び在庫として所定の配置場所に返却端末を格納する。
G20	システム運用担当者は、物品管理システムに対して登録・変更作業を行う。
G21	システム運用担当者は、申請管理機能の本申請に係るステータスを完了にし、運用対応を終了する。

フロー名称	説明	作業トリガー
特殊用途端末利用等申請書	「特殊用途端末利用等申請書」の起票に係る、 特殊用途端末の払出し、端末の管理者の登録・返却に係るフローを示す	・省OA課室担当者からの申請依頼

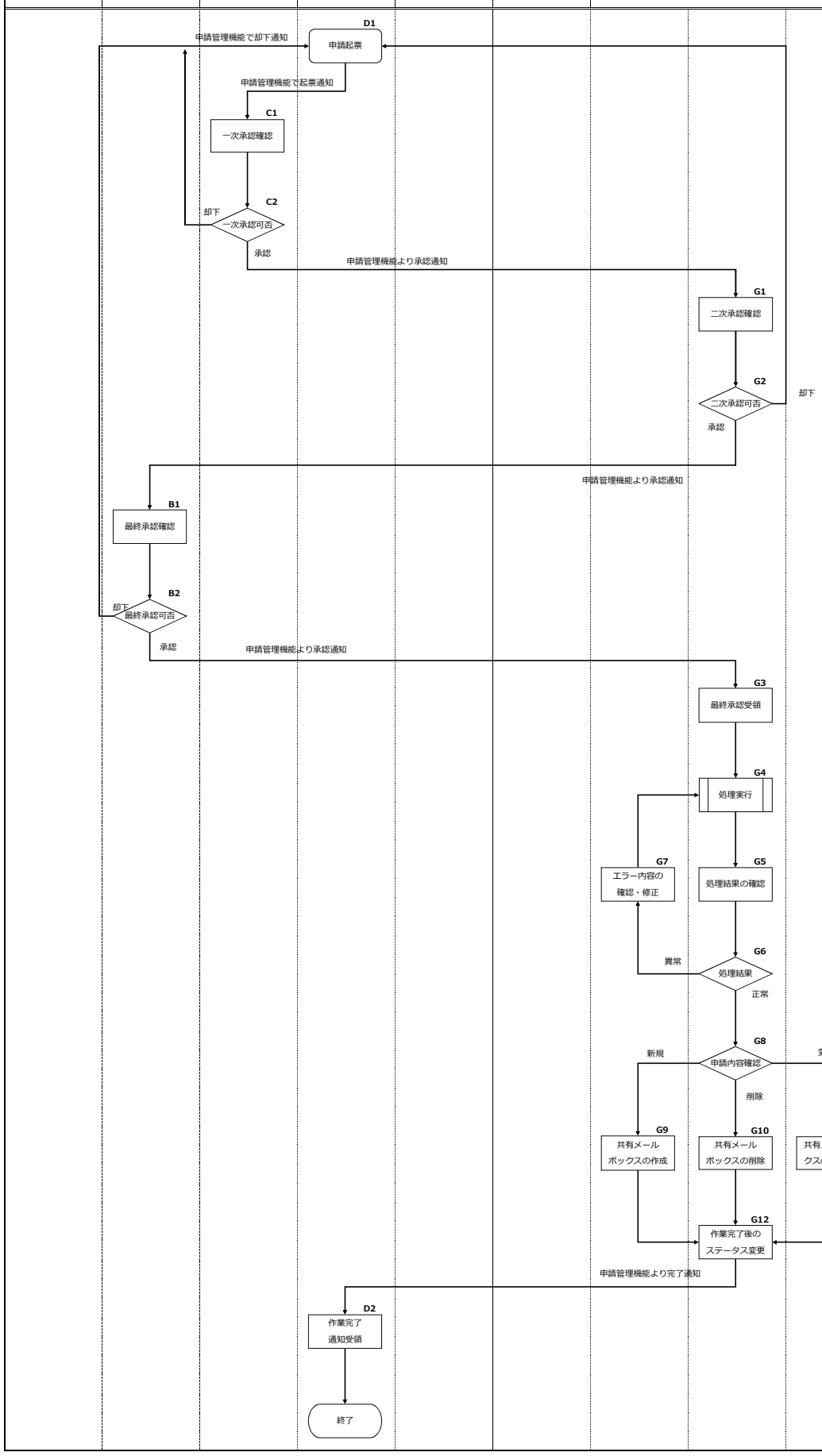


フロー名称	説明	作業トリガー
部外系仮想端末・部外系DIIメールサービス利用等申請書	「部外系仮想端末・部外系DIIメールサービス利用等申請書」の起票に係る、 部外系仮想端末の払出し・返却のフローを示す	・省OA課室担当者からの申請依頼



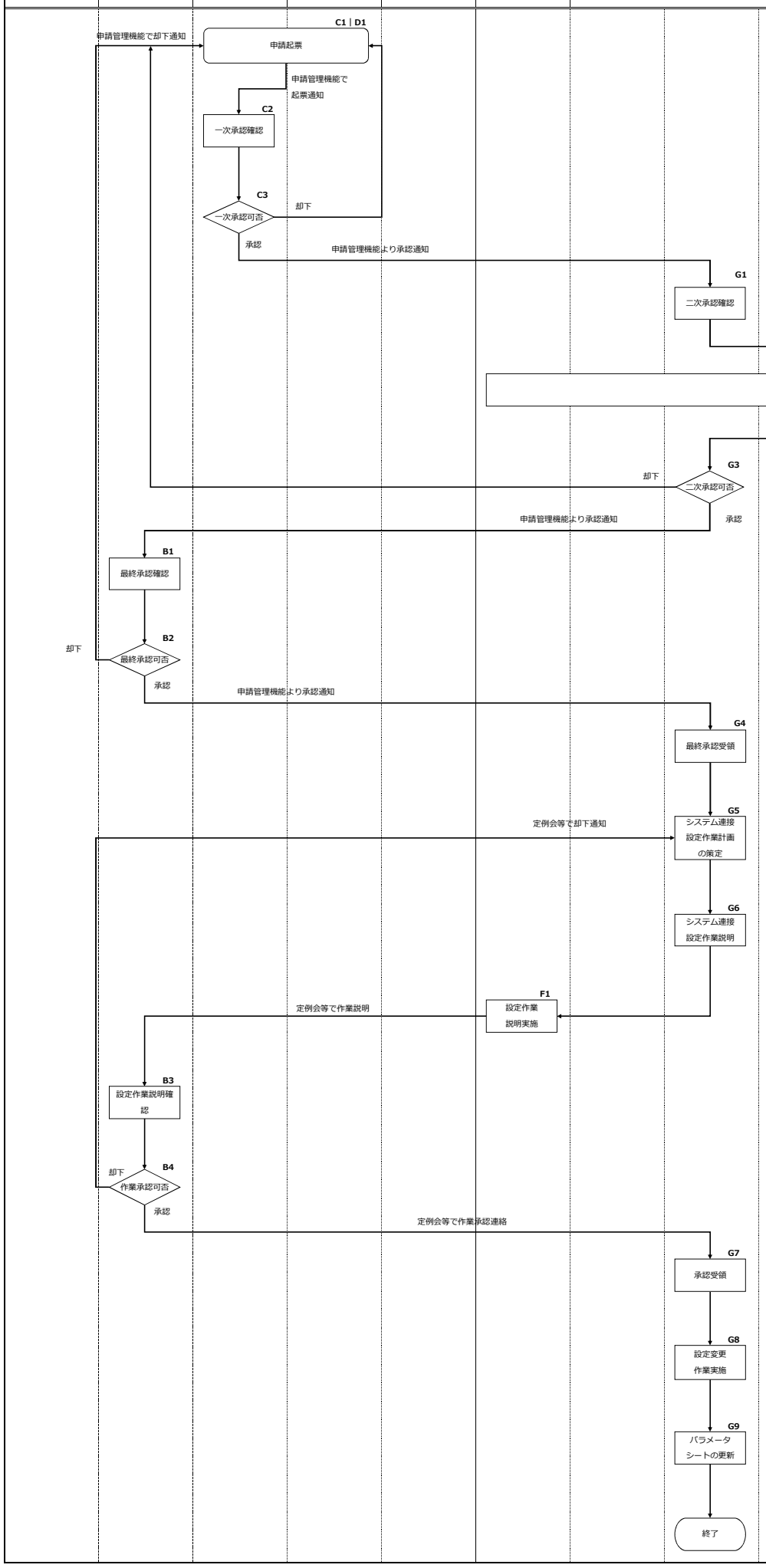
項番	説明
B1	システム管理者は、「部外系仮想端末・部外系DIIメールサービス利用等申請書」の内容を確認し、申請内容に関する処理の実施可否の最終判断を行う。
B2	システム管理者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C1	機関等担当者、地方防衛局担当者は、起票された「部外系仮想端末・部外系DIIメールサービス利用等申請書」の内容を確認し、その妥当性や、申請内容に不備が無いか確認を行う。
C2	機関等担当者、地方防衛局担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
D1	課室等担当者は、申請管理機能を用いて「機部外系仮想端末・部外系DIIメールサービス利用等申請書」として起票する。
D2	課室等担当者は、「部外系仮想端末・部外系DIIメールサービス利用等申請書」の申請処理がすべて完了した旨を、申請管理機能上で確認する。
G1	システム運用担当者は、二次承認確認を行う。 ・申請理由：適切な内容が記載されているか ・デスクトッププール名：プール表示名が記載されているか ・実施希望日：5営業日以降の日程が希望されているか
G2	システム運用担当者は、申請種別「新規」かつデスクトッププール名より割り当て方式が「専用」に該当する場合、判断を行う。
G3	システム運用担当者は、申請書に記載の「デスクトッププール名」に記載のプールの空き状況を確認する。空きがない場合は、変更申請であれば可能な旨を含めて却下とする。
G4	システム運用担当者は、ここまでの一連のやり取りを踏まえ、申請内容を受理するか判断を行う。
G5	システム運用担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。 ・却下する場合は、却下理由と共に申請者に戻す。 ・承認する場合は、システム管理者に申請管理機能により申請内容の最終判断の依頼を行う。
G6	システム運用担当者は、システム管理者からの申請内容に関する最終承認を受け、申請内容の処理に入る。
G7	システム運用担当者は、申請管理機能にて他機能連携の自動処理が実施される。
G8	システム運用担当者は、申請内容に沿った処理が正しく行われたか確認する。
G9	システム運用担当者は、処理結果を確認する。その結果により分岐する。 ・正常：そのまま申請種別分岐に移る。 ・異常：修正作業を行う。
G10	システム運用担当者は、処理結果に問題がある場合、エラー内容の確認・修正作業を行う。
G11	システム運用担当者は、申請種別（新規｜返却｜変更）を確認する。 ・新規｜変更：次の展開方式の確認に進む。 ・返却：そのままプール割当作業実施に進む。
G12	システム運用担当者は、所定の手順書を参照し、申請種別（新規｜変更）に応じたプール割当の作業を実施する。
G13	システム運用担当者は、所定の手順書を参照し、プール割当解除の作業を実施する。
G14	システム運用担当者は、申請管理機能の本申請に係るステータスを完了にし、運用対応を終了する。

フロー名称	説明	作業トリガー
共有メールボックス登録等申請書	「共有メールボックス登録等申請書」の起票に係る、 共有メールボックス登録等の申請に係るフローを示す	・省OA課室担当者からの申請依頼



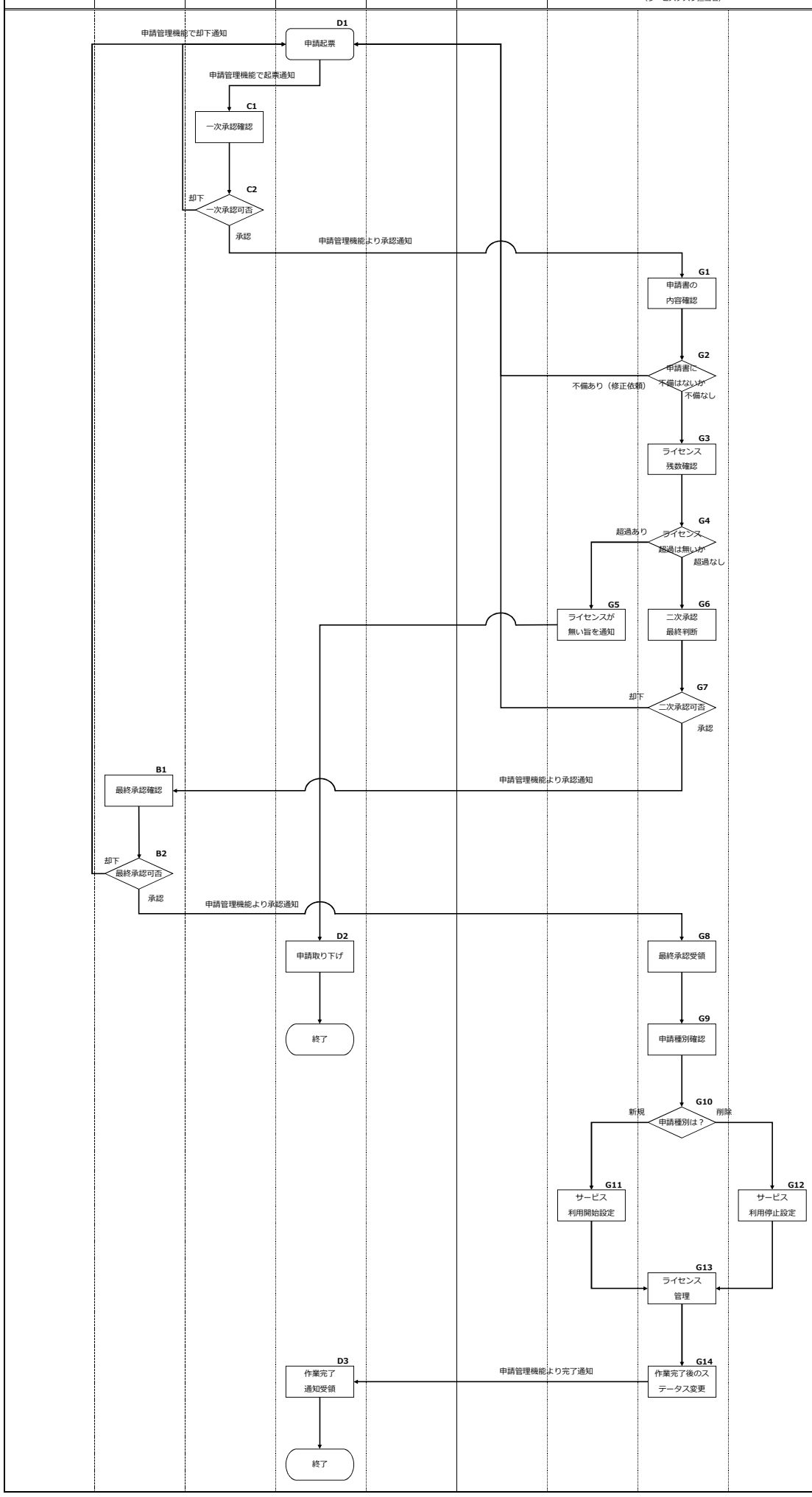
項番	説明
B1	システム管理者は、最終承認確認を行う。
B2	システム管理者は、各申請の項目に基いて、最終承認可否の判断を行う。
C1	機関等担当者、地方防衛局担当者は、一次承認確認を行う
C2	機関等担当者、地方防衛局担当者は、各申請の項目に基いて、一次承認可否の判断を行う
D1	課室等担当者は、申請管理機能で各申請を起票する。
D2	課室等担当者は、作業完了報告を受領する
G1	システム運用担当者は、申請管理機能で提出された申請内容を確認する。 申請に当たって必要事項の欠落や誤った記載がないか確認する。 以下項目の内容を確認する。 1 申請種別：選択されていることを確認する 2 申請理由：明確な理由が入力されていることを確認する 3 共有メールボックス名：入力または選択されていることを確認する 4 共有メールボックスのアドレス：入力されていることを確認する 5 共有メールボックスの管理者の所属・役職：申請種別が「削除」以外の場合に、選択されていることを確認する 6 共有メールボックスの管理者名：申請種別が「削除」以外の場合に、選択されていることを確認する 7 利用者の所属・役職：申請種別が「削除」以外の場合に、選択されていることを確認する 8 利用者名：申請種別が「削除」以外の場合に、選択されていることを確認する 9 利用者の追加削除種別：申請種別が「削除」以外の場合に、選択されていることを確認する 10 階層型アドレス帳への表示：申請種別が「削除」以外の場合に、選択されていることを確認する 11 実施希望日：実施希望日が運用対応可能か確認する
G2	システム運用担当者は、各申請の項目に基いて、二次承認可否の判断を行
G3	システム運用担当者は、システム管理者からの申請内容に関する最終承認を受領し、請内容の処理に入る
G4	自動連携処理が実施される 共有メールボックス監査用アカウントの作成、変更、削除
G5	システム運用担当者は、自動化処理が正常終了しているかを確認する。
G6	処理の確認結果により分岐する。 ・正常：次の処理へ遷移する ・異常：異常部分の修正を行う
G7	システム運用担当者は、エラー内容の確認・修正を実施する。
G8	申請内容により分岐する。 ・新規：共有メールボックスの作成 ・削除：共有メールボックスの削除 ・変更：共有メールボックスの設定変更
G9	システム運用担当者は、共有メールボックスを作成する。 Exchange管理センター（EAC）にて共有メールボックスの作成を行う。
G10	システム運用担当者は、共有メールボックスを削除する。 Exchange管理センター（EAC）にて共有メールボックスの削除を行う。
G11	システム運用担当者は、共有メールボックスを削除する。 Exchange管理センター（EAC）にて共有メールボックスの設定変更を行う。
G12	システム運用担当者は、申請管理機能のステータスを完了にする。

フロー名称	説明	作業トリガー
システム連接申請書	「システム連接申請書」の起票に係る、 ネットワーク関連設定変更フローを示す	・省OA課室担当者からの申請依頼



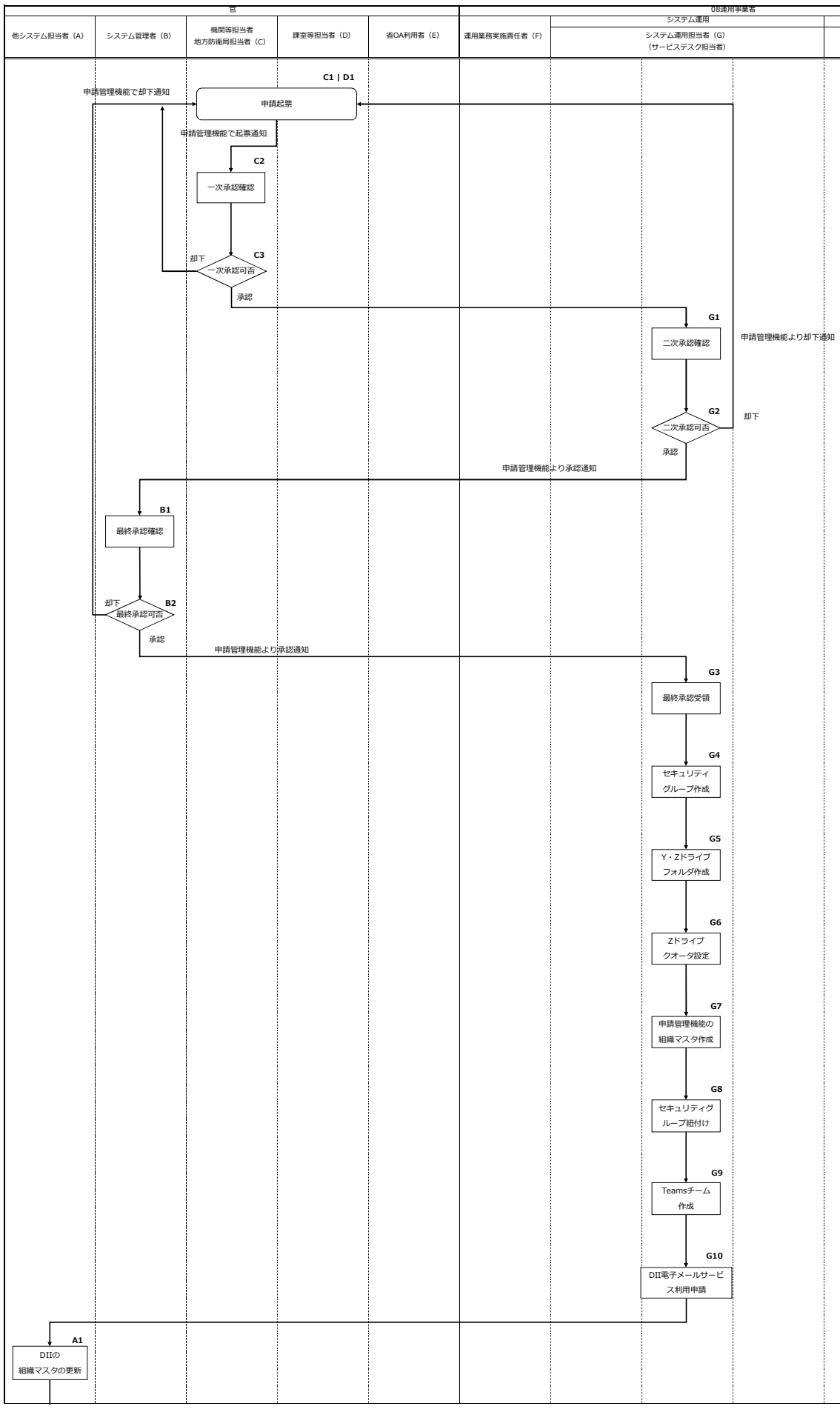
項番	説明
B1	システム管理者は、「システム連接申請書」の内容を確認し、申請内容に関する処理の実施可否の最終判断を行う
B2	システム管理者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す
B3	システム管理者は、システム連接設定作業計画の内容を確認する。
B4	システム管理者は、確認結果を基に、作業内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に作業計画策定者に戻す。
C1	機関等担当者、地方防衛局担当者は、申請管理機能でシステム連接設定変更申請を起票する。
C2	機関等担当者、地方防衛局担当者は、起票された「システム連接申請書」の内容を確認し、その妥当性や、申請内容に不備が無いか確認を行う。
C3	機関等担当者、地方防衛局担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
D1	課室等担当者は、申請管理機能でシステム連接設定変更申請を起票する。
F1	運用業務実施責任者は、システム連接申請の項目に基いて、省OA関係者（システム運用、SOC運用、保守事業者）を招集し調査・検討を実施する。
F2	運用業務実施責任者は、作業内容を確認後、官側システム担当者に作業説明を実施する。
G1	システム運用担当者は、二次承認確認を行う。 ・実施希望日を確認する ・利用希望サービスを確認する（DIIの部内/部外） ・添付ファイルの以下項目の記載不備チェック （１）通信要件 （２）許可/拒否の内容
G2	システム運用担当者は、運用業務実施責任者の招集に応じ、システム連接申請項目の調査・検討を実施する。
G3	システム運用担当者は、システム連接申請の項目に基いて、関係者の調査・検討の結果を受け、実現可否を判断を行う。
G4	システム運用担当者は、システム管理者からの申請内容に関する最終承認を受領し、申請内容の処理に入る。
G5	システム運用担当者は、作業計画の策定を行う。 （１）作業目的・背景：なぜ変更が必要か（業務要件、セキュリティ対応など） （２）作業範囲：対象機器、対象ルール、影響範囲 作業手順：設定変更の具体的な手順（CLI/GUI操作、確認方法） （３）リスク評価：障害発生時の影響、回避策 （４）バックアウトプラン：問題発生時の復旧手順 （５）作業日・作業時間帯：業務影響を最小化する時間帯（例：深夜、休日） （６）必要リソース：担当者、権限、ツール
G6	システム運用担当者は、システム連接設定作業説明を運用業務実施責任者に対し実施する。
G7	システム運用担当者は、作業承認を受領する。
G8	システム運用担当者は、設定変更作業実施を実施する。
G9	システム運用担当者は、パラメータシートを更新する。
H1	SOC担当者は、運用業務実施責任者の招集に応じ、システム連接申請項目の調査・検討を実施する。
I1	CSIRT担当者は、運用業務実施責任者の招集に応じ、システム連接申請項目の調査・検討を実施する。
J1	保守業務担当者は、運用業務実施責任者の招集に応じ、システム連接申請項目の調査・検討を実施する。

フロー名称	説明	作業トリガー
DII提供サービス利用等申請書	システム利用者が「省外とのテレビ電話サービス」を新規に利用を始める際に、 申請を行うことで該当機能の利用を可能とする。 また、利用が不要になった際は同じく申請を行うことで、該当機能の利用を停止する。	省OA課室担当者からの申請起票があった場合に実施する。



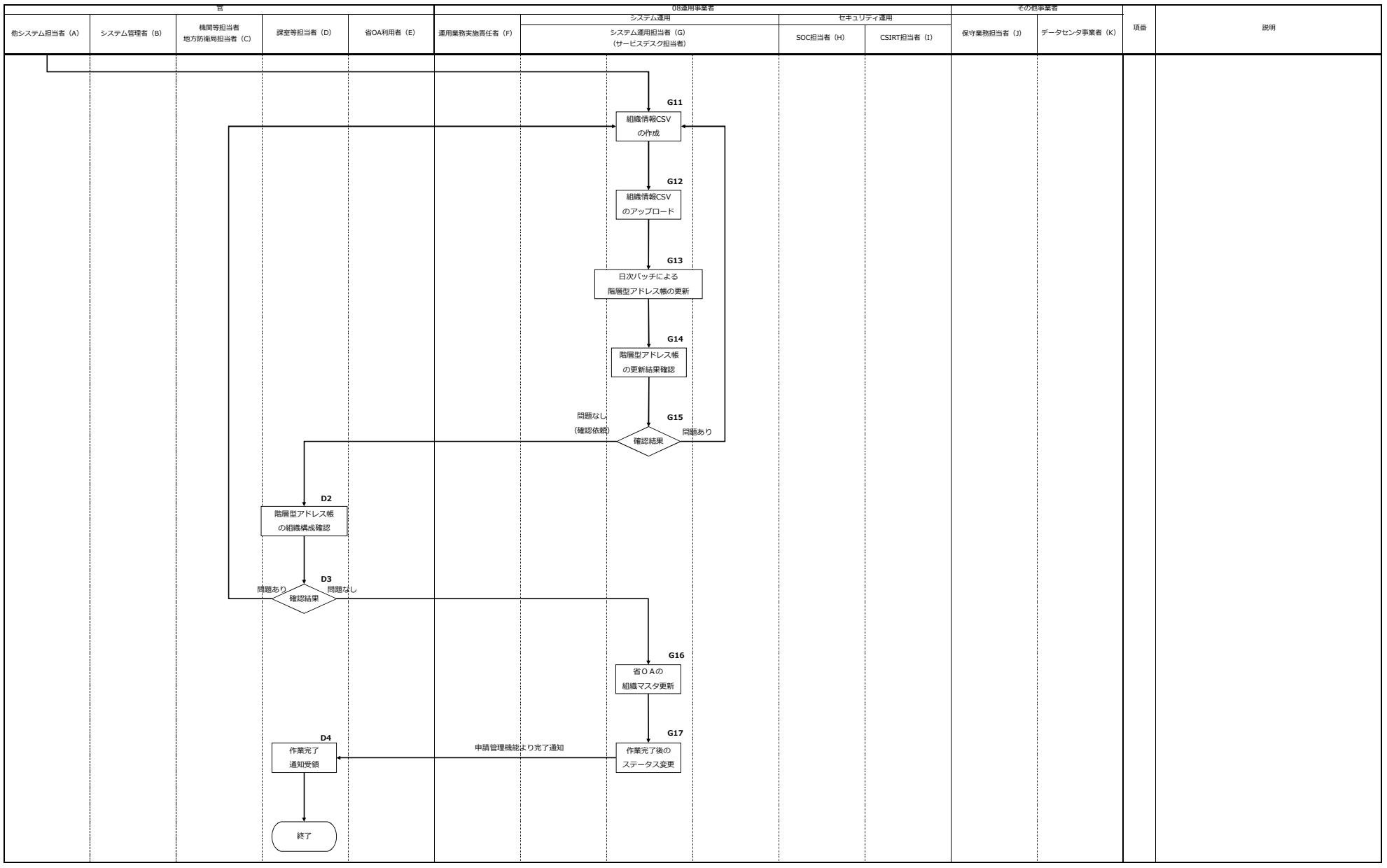
項番	説明
B1	システム管理者は、「DII提供サービス利用等申請書」の内容を確認し、申請内容に関する処理の実施可否の最終判断を行う。
B2	システム管理者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C1	機関等担当者、地方防衛局担当者は、起票された申請内容を確認し、その妥当性や、申請内容に不備が無いか確認を行う。
C2	機関等担当者、地方防衛局担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
D1	課室等担当者は、希望する「DII提供サービス利用等申請書」に係る申請を、申請管理機能を用いて起票する。
D2	課室等担当者は、ライセンスの残りが無い旨の連絡を受領し、「DII提供サービス利用等申請書」に係る申請を取り下げる。
D3	課室等担当者は、「DII提供サービス利用等申請書」の申請処理がすべて完了した旨を、申請管理機能上で確認する。
G1	システム運用担当者は、申請管理機能で提出された申請内容を確認する。 申請に当たって必要事項の欠落や誤った記載がないか確認する。 1 申請種別：入力があることを確認する。 2 申請理由：適切な「申請理由」が入力されていることを確認する。 3 アカウントの種別：入力があることを確認する。 4 利用者の所属・役職：「3 アカウントの種別」が個人アカウントである場合、入力があることを確認する。 5 利用者名：（入力は必須ではない。） 6 共有アカウント名：「3 アカウントの種別」が共有アカウントである場合、入力があることを確認する。 7 利用対象サービス：「省外とのテレビ電話サービス」のみ。 8 利用開始日：運用対応上、不可能な日程が入力されていないか確認する。 9 その他特記事項：（必要に応じて記載内容を確認する。）
G2	システム運用担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。 ・却下する場合は、却下理由と共に申請者に戻す。 ・承認する場合は、システム管理者に申請管理機能により申請内容の最終判断の依頼を行う。
G3	システム運用担当者は、申請を受け、「省外とのテレビ電話サービス」にかかるライセンスの残数確認を行う。
G4	システム運用担当者は、ライセンス残数の確認結果、 ・超過なし：二次承認最終判断に移行する。 ・超過あり：ライセンス残数が無い旨を申請者に通知する。
G5	システム運用担当者は、申請者にライセンスの残数が無い旨を通知する。
G6	システム運用担当者は、ここまでの一連のやり取りを踏まえ、申請内容を受理するか判断を行う。
G7	システム運用担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。 ・却下する場合は、却下理由と共に申請者に戻す。 ・承認する場合は、システム管理者に申請管理機能により申請内容の最終判断の依頼を行う。
G8	システム運用担当者は、システム管理者の最終承認を受領する。
G9	システム運用担当者は、申請管理機能で提出された申請内容のうち「申請種別」を確認し、必要な運用対応が「新規」であるか「削除」であるか確認する。
G10	システム運用担当者は、申請種別に応じた運用作業を実施する。 ・新規：省外とのテレビ電話サービスの「利用**開始**設定」 ・削除：省外とのテレビ電話サービスの「利用**停止**設定」
G11	システム運用担当者は、「DII提供サービス利用等申請書」に記載されたアカウントが、省外とのテレビ電話サービスを利用できるように設定を行う。
G12	システム運用担当者は、「DII提供サービス利用等申請書」に記載されたアカウントの、省外とのテレビ電話サービス利用を停止する設定を行う。
G13	システム運用担当者は、対応の結果、増減したライセンスを管理台帳に反映する。
G14	システム運用担当者は、申請管理機能の本申請に係るステータスを完了にし、運用対応を終了する。

フロー名称	説明	作業トリガー
組織変更等申請書	組織改編による新組織の編成や既存変更に伴う各種登録や変更のフローを示す。	機関担当者からの新組織情報の連絡

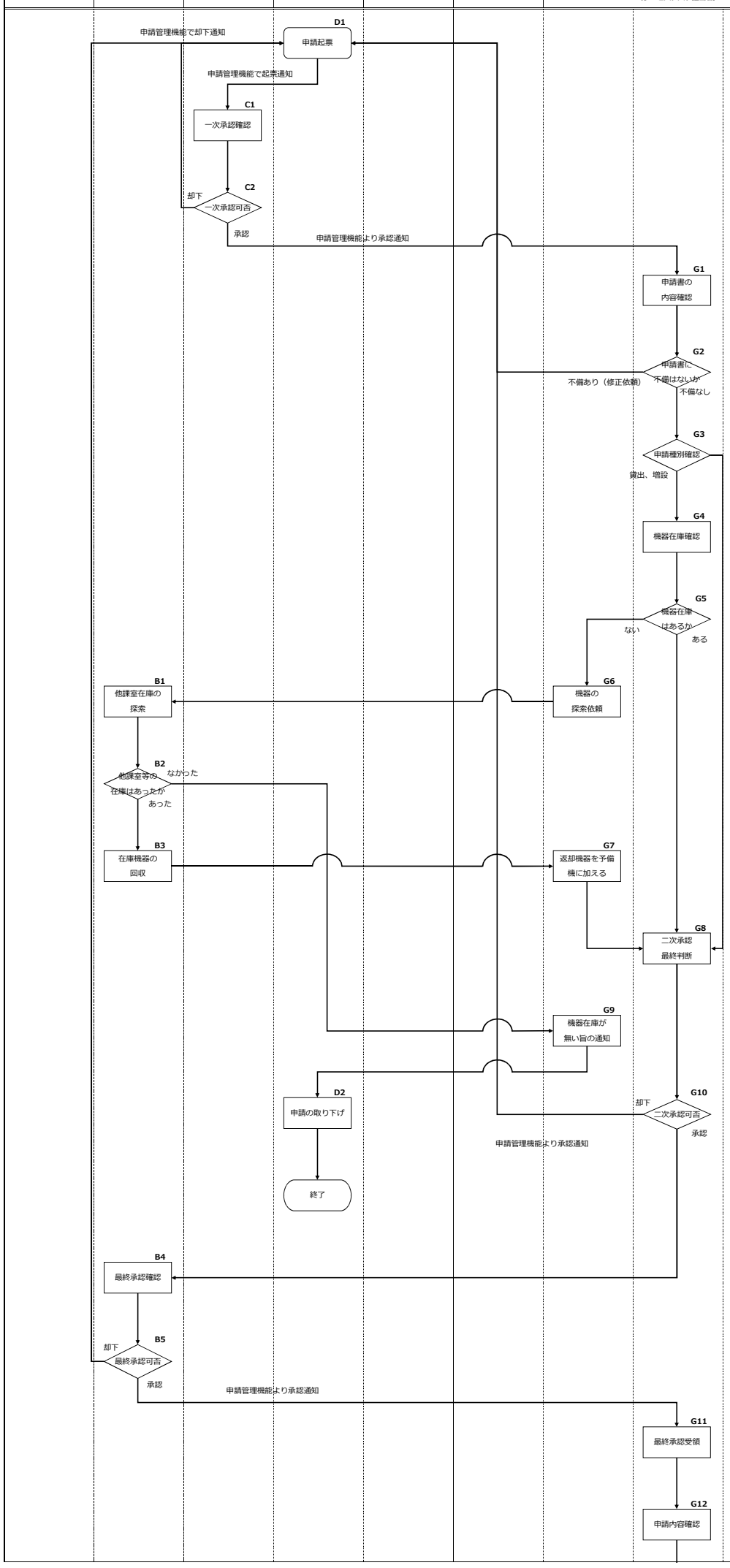


項番	説明
A1	ＤＩＩ管理者は、システム運用担当者からのＤＩＩ電子メールサービス利用申請を受けて、ＤＩＩが管理する組織マスタの登録・変更・削除および組織コードの割り当てを行い、更新後の組織マスタ情報をシステム運用担当者に通知する。
B1	システム管理者は、「組織変更等申請書」の内容を確認し、申請内容に関する処理の実施可否の最終判断を行う。
B2	システム管理者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C1	機関等担当者、地方防衛局担当者は組織情報に変更がある場合、申請管理機能を用いて「組織変更等申請書」として起票する。
C2	機関等担当者、地方防衛局担当者は、起票された「組織変更等申請書」の内容を確認し、その妥当性や、申請内容に不備が無いか確認を行う。機関等担当者、地方防衛局担当者が申請者の場合はここでの確認は実施しない。
C3	機関等担当者、地方防衛局担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
D1	課室等担当者は組織情報に変更がある場合、申請管理機能を用いて「組織変更等申請書」として起票する。
D2	課室等担当者は、Outlookで階層型アドレス帳を表示して階層型アドレス帳の組織構成が課室等担当者の想定通りとなっているか確認する。 ※「組織変更等申請書」の記載誤りにより、階層型アドレス帳の更新はできているが、課室等担当者が想定した組織構成となっていない場合を想定している。
D3	階層型アドレス帳の組織構成が課室等担当者の想定と合っている場合は、システム運用担当者に問題無いことを連絡する。 階層型アドレス帳の組織構成が課室等担当者の想定と異なっている場合は、システム運用担当者に修正を依頼する。
D4	課室等担当者は、「組織変更等申請書」の申請処理がすべて完了した旨を、申請管理機能上で確認する。
G1	システム運用担当者は、申請管理機能で提出された「組織変更等申請書」の内容を確認する。申請に当たって必要事項の欠落や誤った記載がないか確認する。 また以下の内容についても確認する。 ・Yドライブフォルダ構成・アクセス権 ・Zドライブフォルダ構成・アクセス権・クオータ値 ・階層型アドレス帳の階層構成・表示位置 ・メールアドレス命名規則
G2	システム運用担当者は、申請内容を「承認」するか、「却下」するか判断する。 ・却下する場合は、却下理由と共に申請者に戻す。 ・承認する場合は、システム管理者に申請管理機能により申請内容の最終判断の依頼を行う。
G3	システム運用担当者は、システム管理者からの申請内容に関する最終承認を受け、申請内容の処理に入る。
G4	システム運用担当者は、ドメイン管理グループの課室セキュリティグループを作成または変更する。
G5	システム運用担当者は、新組織の課室フォルダ（Yドライブ・Zドライブ）を作成または変更する。 作成したフォルダにG6で作成したセキュリティグループを紐づける。
G6	システム運用担当者は、Zドライブクオータを設定する。
G7	システム運用担当者は、申請管理機能の組織マスタを作成または変更する。
G8	システム運用担当者は、申請管理機能の組織マスタと作成または変更したセキュリティグループを紐づける。
G9	システム運用担当者は、Teamsのチームを作成または変更する。 課室担当者を管理者として設定する。
G10	システム運用担当者は、「組織変更等申請書」の内容をもとにＤＩＩ電子メールサービス利用申請を作成し、ＤＩＩに対してＤＩＩが管理する組織マスタへの登録・更新・削除を申請する。
G11	システム運用担当者は、「組織変更等申請書」の申請内容とＤＩＩから受信した更新後の組織マスタ情報をもとに、省ＯＡの階層型アドレス帳を更新するための組織情報CSVを作成する。
G12	システム運用担当者は、階層型アドレス帳の更新処理を実施する共有フォルダ管理サーバに組織情報CSVをアップロードする。
G13	システム運用担当者は、日次処理にて以下の階層型アドレス帳の更新処理を実施する。 ・組織情報CSVの内容をもとに、Exchange Onlineに登録されている階層型アドレス帳用の「メールが有効なセキュリティ グループ」の登録・編集・削除を実施する。 ・Entra IDアカウントのinfo属性から組織コードを取得し、階層型アドレス帳用の「メールが有効なセキュリティ グループ」のメンバに登録・削除を実施する。
G14	システム運用担当者は、日次処理が正常終了しエラーが出ていないことを確認する。
G15	システム運用担当者は、日次処理が正常終了している場合は、課室等担当者に階層型アドレス帳の内容確認を依頼する。 日次処理でエラーが発生した場合は、エラー内容を確認して組織情報CSVを修正し、階層型アドレス帳の更新処理を再度実行する。
G16	システム運用担当者は、階層型アドレス帳の組織構成が正しく反映された事を確認後、ＤＩＩから受信した更新後の組織マスタ情報をもとに、省ＯＡの申請管理機能で管理している組織マスタを更新する。 ※省ＯＡの組織マスタを更新する方法は申請管理機能の手順書を参照する。
G17	システム運用担当者は、申請管理機能の本申請に係るステータスを完了にし、運用対応を終了する。

フロー名称	説明	作業トリガー
組織変更等申請書	組織改編による新組織の編成や既存変更に伴う各種登録や変更のフローを示す。	機関担当者からの新組織情報の連絡



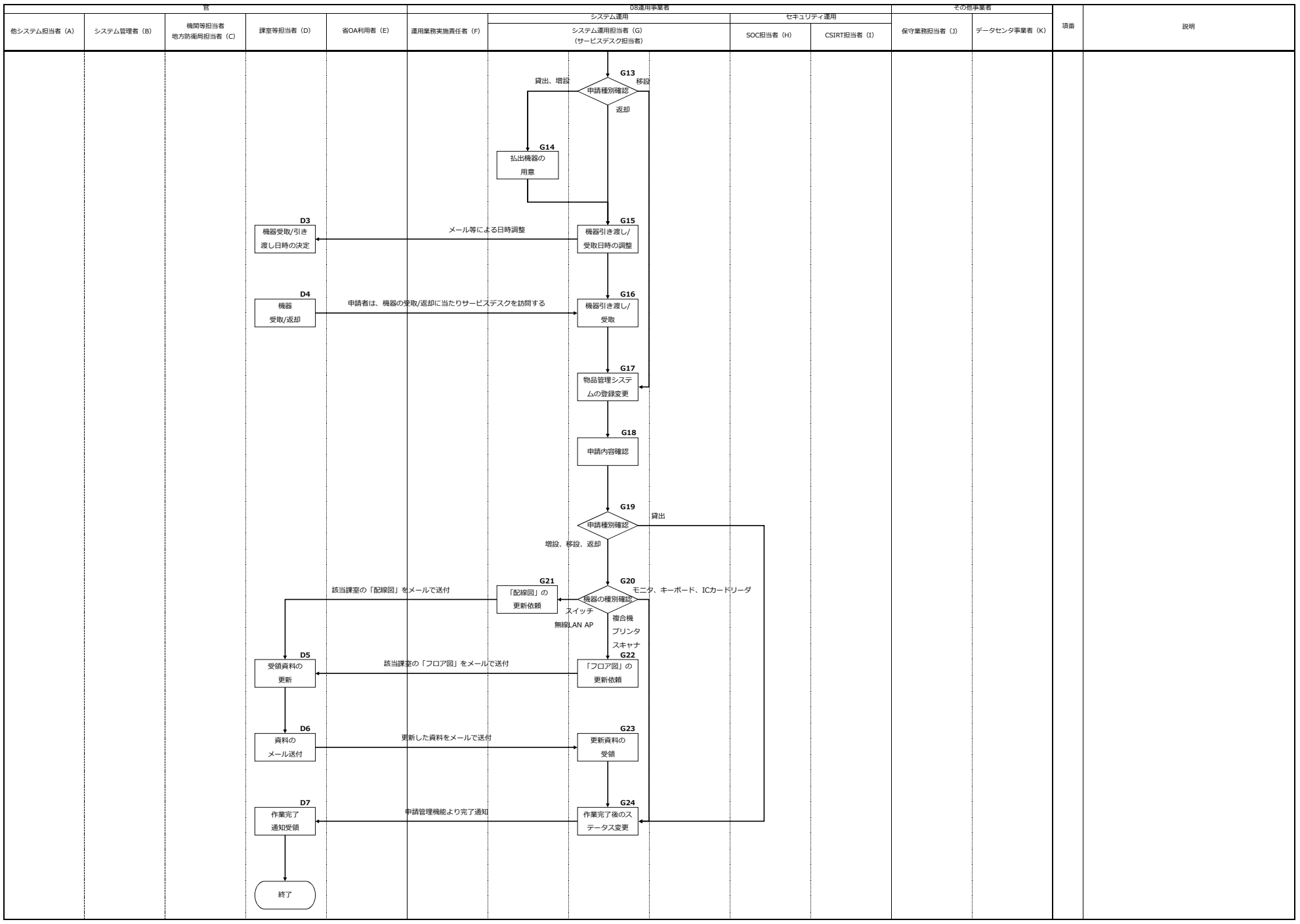
フロー名称	説明	作業トリガー
機器貸出・増設・移設等申請書	「機器貸出・増設・移設申請書」の起票に係る、 機器の払い出しや移設（登録情報の変更）のフローを示す。	省OA課室担当者からの申請起票があった場合に実施する。



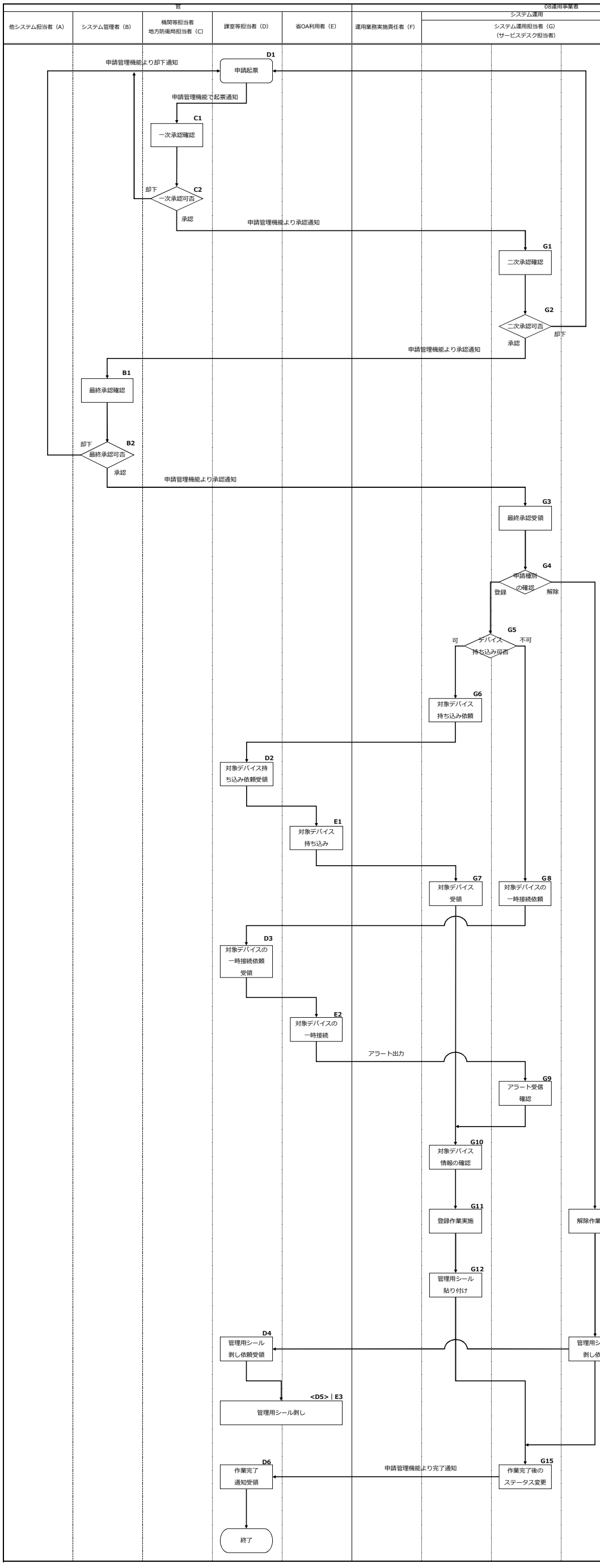
項番	説明
B1	連絡を受けたシステム担当者は、省内の他の課室に照会を行い、不使用機器が保管されていないか確認を行う。
B2	システム管理者は、省内の他課室の不使用機器の在庫を確認した結果、 ・在庫があった：該当機器を回収し、サービスデスクに返却する。 ・在庫が無かった：無い旨をサービスデスクに連絡する。
B3	システム管理者は、他課室等に保管されていた不使用端末を回収し、サービスデスクに返却する。
B4	システム管理者は、「機器貸出・増設・移設等申請書」の内容を確認し、申請内容に関する処理の実施可否の最終判断を行う。
B5	システム管理者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C1	機関等担当者、地方防衛局担当者は、起票された「機器貸出・増設・移設等申請書」の内容を確認し、その妥当性や、申請内容に不備が無いか確認を行う。
C2	機関等担当者、地方防衛局担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
D1	課室等担当者は、希望する機器の申請を、申請管理機能を用いて「機器貸出・増設・移設等申請書」として起票する。
D2	課室等担当者は、連絡を受け今回の依頼を取り下げる。
D3	課室等担当者は、システム運用からの連絡を受け、機器の受取日時を決定する。
D4	課室等担当者は、サービスデスクを訪問し機器の受取を行う。
D5	課室等担当者は、依頼を受け申請対象機器の配置場所を資料に反映する。 【資料】 ・スイッチ、無線APの場合：配線図 ・複合機、プリンタ、スキャナの場合：フロア図
D6	課室等担当者は、更新した資料をメールで送付する。
D7	課室等担当者は、「機器貸出・増設・移設申請書」の申請処理がすべて完了した旨を、申請管理機能上で確認する。
G1	システム運用担当者は、申請管理機能で提出された「機器貸出・増設・移設等申請書」の内容を確認する。申請に当たって必要事項の欠落や誤った記載がないか確認する。 1 申請種別：入力がされているか確認する 2 所属・役職：入力がされているか確認する 3 利用者名：（必要に応じて入力内容を確認する） 4 機器の種別：本申請の対象機器が入力されているか確認する 5 ホスト名：「移設、返却」の場合に入力されていることを確認する。 6 利用場所：（必要に応じて入力内容を確認する） 7 利用開始日（または、移設日）：入力があるか確認する。 また、開始日が払出に要する日数（5営業日）以降であるか確認する。 8 利用終了予定日：「貸出」の場合に入力がされているか確認する。
G2	システム運用担当者は、申請書の不備の有無の確認結果、不備があった場合はその個所の指摘と共に申請者に戻す。
G3	システム運用担当者は、申請内容を基に、申請種別が「貸出・増設」（新規に機器の払い出しを伴う）か「移設・返却」であるかを確認する。
G4	システム運用担当者は、申請区分が新規に機器の払い出しを求めるものであった場合、払い出し可能な機器の予備在庫があるか確認する。
G5	システム運用担当者は、確認結果、機器の予備在庫の「ある」「なし」により、以後の対応内容が分岐する。
G6	システム運用担当者は、「課室等から、機器の払い出し依頼があったが運用在庫も課室等での保管も無かった」旨をシステム担当者に連絡し、他の課室等で不使用の機器が保管されていないか確認を依頼する。
G7	システム運用担当者は、返却された不使用機器を払い出し可能な在庫とする。この際、誤って該当機器を他の課室等に払い出してしまわないよう回収した機器に「特定の申請用に回収した機器であり、他へ払い出ししない旨」を記載した紙を貼り付ける。
G8	システム運用担当者は、ここまでの一連のやり取りを踏まえ、申請内容を受理するか判断を行う。
G9	システム運用担当者は、申請内容をかなえる機器の在庫が省内に無い旨を申請者に連絡する。
G10	システム運用担当者は、確認結果を基に申請内容を「承認」するか、「却下」するか判断する。 ・却下する場合は、却下理由と共に申請者に戻す。 ・承認する場合は、システム管理者に申請管理機能により申請内容の最終判断の依頼を行う。
G11	システム運用担当者は、システム管理者からの申請内容に関する最終承認を受け、申請内容の処理に入る。
G12	システム運用担当者は、申請内容を確認する。 ※ 確認内容：G13「申請種別」
G13	システム運用担当者は、申請内容を基に、申請種別が「貸出・増設」（新規に機器の払い出しを伴う）か「移設」か「返却」であるかを確認する。
G14	システム運用担当者は、申請内容が「貸出・増設」であった場合は、申請内容に応じて払出機器の用意を行う。
G15	システム運用担当者は、払い出し対象機器/返却対象機器の引き渡し/受取日時の調整を行う。申請者に対しメール等を用い連絡する。
G16	システム運用担当者は、申請者に対して、申請された機器の引き渡し/受取を行う。
G17	システム運用担当者は、物品管理システム上の登録情報を申請内容に沿って変更する。
G18	システム運用担当者は、クロージング処理のため、申請内容を確認する。 ※ 確認点は、G19及びG20に記載する。
G19	システム運用担当者は、「申請種別」が「貸出」か「増設、移設、返却」か確認する。
G20	システム運用担当者は、「機器の種別」が、以下のどれに当たるか確認する。 ・スイッチ、無線LAN AP、 ・複合機、プリンタ、スキャナ ・モニタ、キーボード、ICカードリーダ
G21	スイッチ、無線LAN APの場合は、システム運用担当者は配線図の更新依頼を行う。
G22	複合機、プリンタ、スキャナの場合は、システム運用担当者はフロア図の更新依頼を行う。
G23	システム運用担当者は、更新された資料を受領し、運用で管理する。
G24	システム運用担当者は、申請管理機能の本申請に係るステータスを完了にし、運用対応を終了する。

付表１０　業務フロー（続き）
機器貸出・増設・移設等申請書（続き）

フロー名称	説明	作業トリガー
機器貸出・増設・移設等申請書	「機器貸出・増設・移設申請書」の起票に係る、 機器の払い出しや移設（登録情報の変更）のフローを示す。	省OA課室担当者からの申請起票があった場合に実施する。

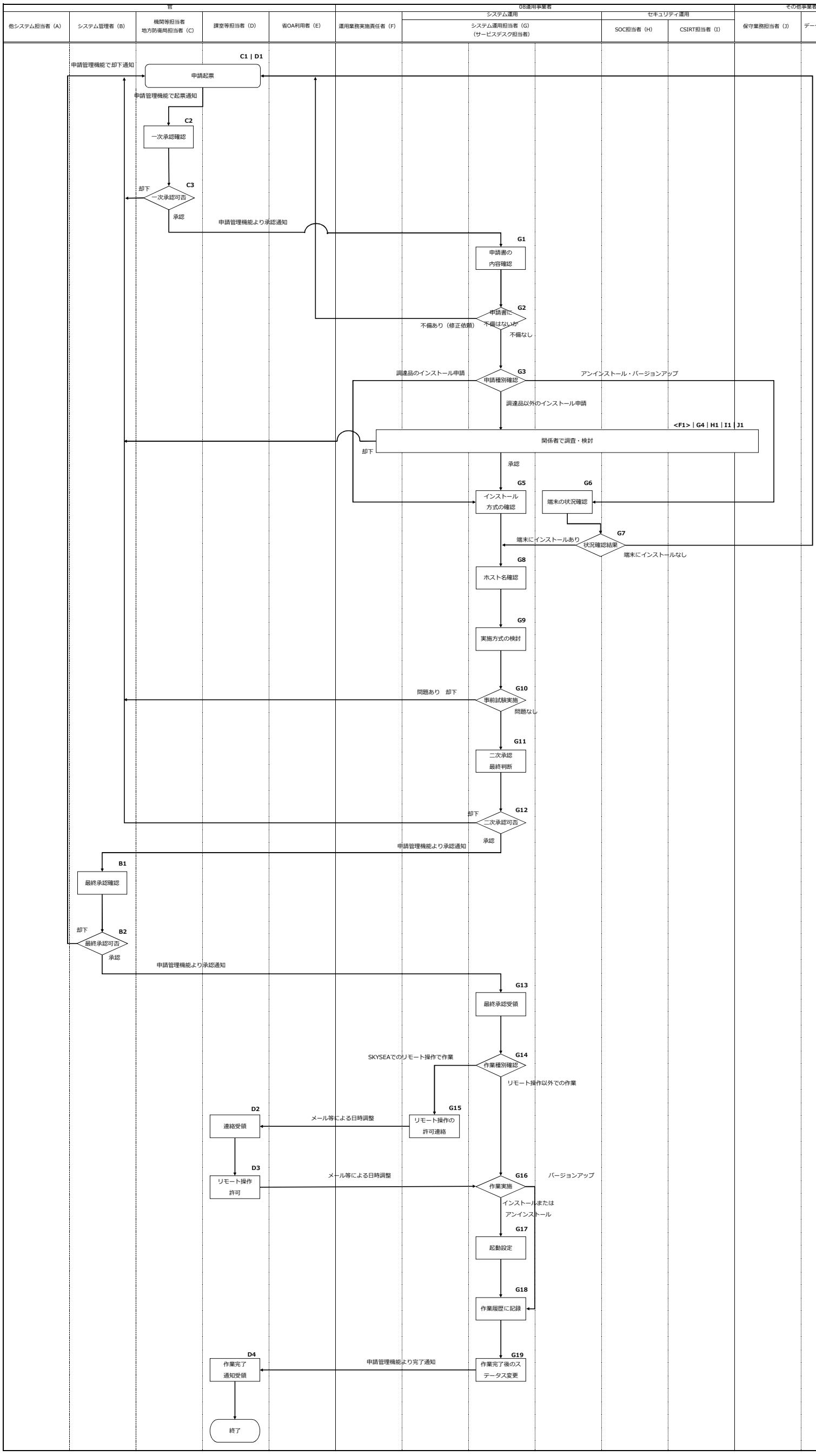


フロー名称	説明	作業トリガー
官品デバイス利用登録等申請書	「官品デバイス利用登録等申請書」の起票に伴う、 官品デバイス利用登録、解除のフローを示す。	省OA課室担当者からの申請依頼



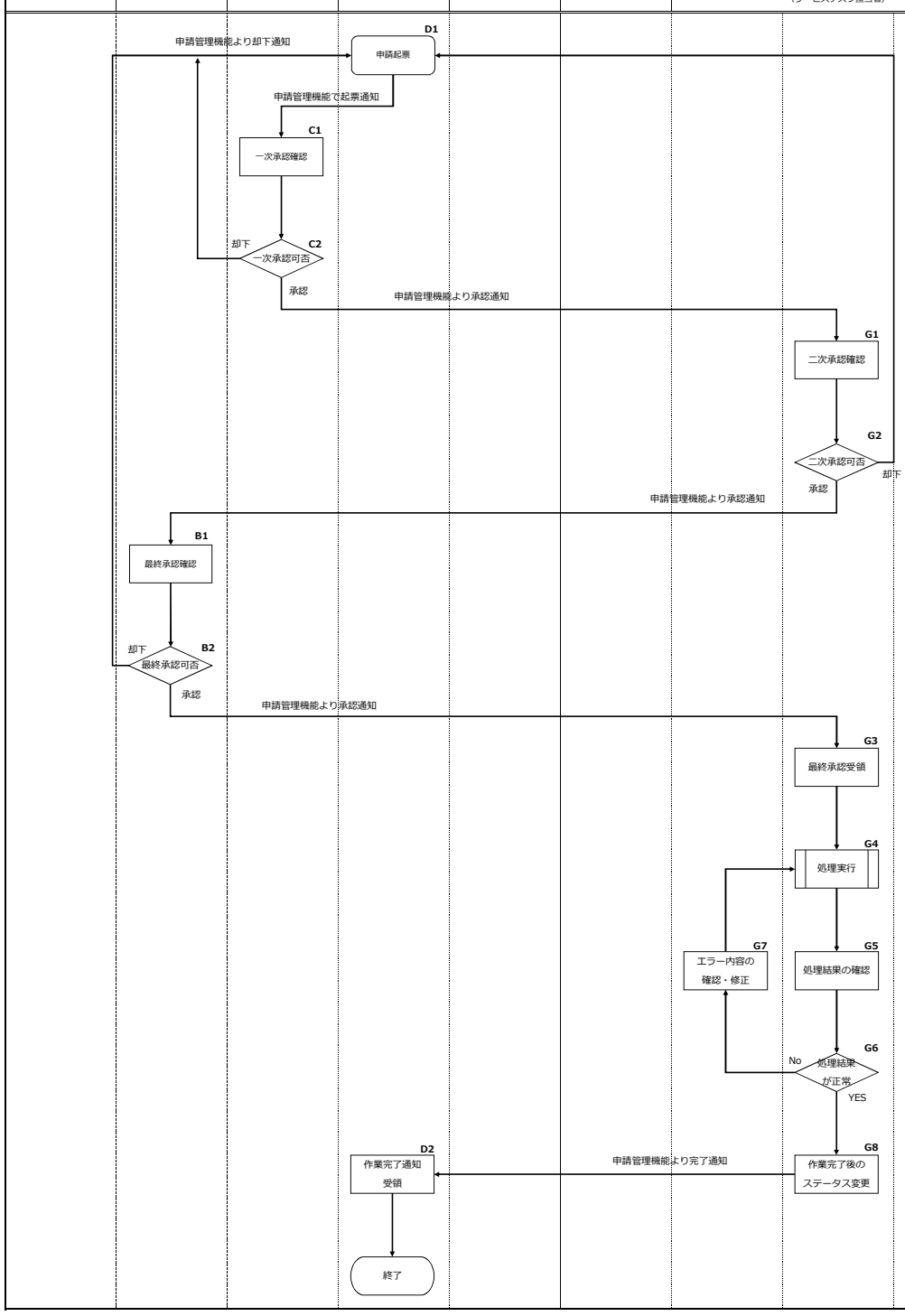
項番	説明
B1	システム管理者は、最終承認確認を行う。
B2	システム管理者は、申請書の内容に基づき、最終承認可否の判断を行う。
C1	機関等担当者、地方防衛局担当者は、一次承認確認を行う。
C2	機関等担当者、地方防衛局担当者は、申請書の内容に基づき、一次承認可否の判断を行う。
D1	課室等担当者は、申請管理機能で申請を起票する。
D2	課室等担当者は、対象デバイスのシステム運用部への持ち込み依頼を受領する。
D3	課室等担当者は、一時的に対象デバイスをシステムに接続する依頼を受領する。
D4	課室等担当者は、棚卸管理用に張られたシールを剥す依頼を受領する。
D5	課室等担当者は、省OA利用者に指示をして棚卸管理用に張られたシールを剥す。
D6	課室等担当者は、作業完了報告を受領する。
E1	省OA利用者は、対象デバイスをシステム運用部へ持ち込む。
E2	省OA利用者は、指定された日時に対象デバイスを一時的にシステムに接続する。
E3	省OA利用者は、課室等担当者の指示のもと棚卸管理用に張られたシールを剥がす。
G1	システム運用担当者は、二次承認確認を行う。 下記の必須項目が申請書に入力されているかを確認する。 ・申請種別 ・機器の種別 ・機器の管理者の所属・役職 ・デバイス持ち込み可否 ・実施希望日 また、入力された項目内容の妥当性を確認する。
G2	システム運用担当者は、申請書の内容に基づき、二次承認可否の判断を行う。
G3	システム運用担当者は、最終承認を受領する。
G4	システム運用担当者は、申請種別が「登録」か「解除」かを確認する。
G5	システム運用担当者は、デバイスの持ち込みが「可」か「不可」かを確認する。 ※SDカード、USBデバイスの場合は機器を管理機へ接続する必要があるため、持込が必要
G6	システム運用担当者は、デバイス情報(申請書の下記任意項目)を確認するため、対象デバイスの持ち込みを申請元へ依頼する。 ・型番 ・MACアドレス
G7	システム運用担当者は、持ち込まれた対象デバイスを受領する。
G8	システム運用担当者は、利用許可登録に必要な情報を取得するため、申請元に対して「日時指定で一時的に対象デバイスをシステムに接続する」依頼を行う。
G9	システム運用担当者は、未登録のデバイスがシステムに接続された旨のアラート(ドライブ種別、パス等）が出力されたことを確認する。
G10	システム運用担当者は、持ち込まれた対象デバイス、又は出力されたアラートより、対象デバイスの利用許可登録に必要な情報を確認する。
G11	システム運用担当者は、申請書の内容に基づき、対象デバイスの利用許可登録作業を実施する。 手順書に従って、SKYSEAデバイス画面にて対象機器の登録を行う。 ・デバイス名(型番) ・デバイス種別(機器の種別) ・管理状態（使用可能）
G12	システム運用担当者は、棚卸時に官品デバイスに識別番号、または登録済みであることがわかるようなシールを貼り付ける。
G13	システム運用担当者は、申請書の内容に基づき、対象デバイスの利用許可解除作業を実施する。 手順書に従って、SKYSEAデバイス画面にて対象機器の管理状態を使用可能から使用不可能に変更する。
G14	システム運用担当者は、棚卸管理用に張られたシールを剥がすよう申請元に依頼する。
G15	システム運用担当者は、申請管理機能のステータスを完了にする。

フロー名称	説明	作業トリガー
ソフトウェアインストール申請書	「ソフトウェアインストール申請書」の起票に係る、 ソフトウェアのインストール・アンインストール・バージョンアップのフローを示す	課室等担当者及び機関担当者、地方防衛局担当者からの申請依頼



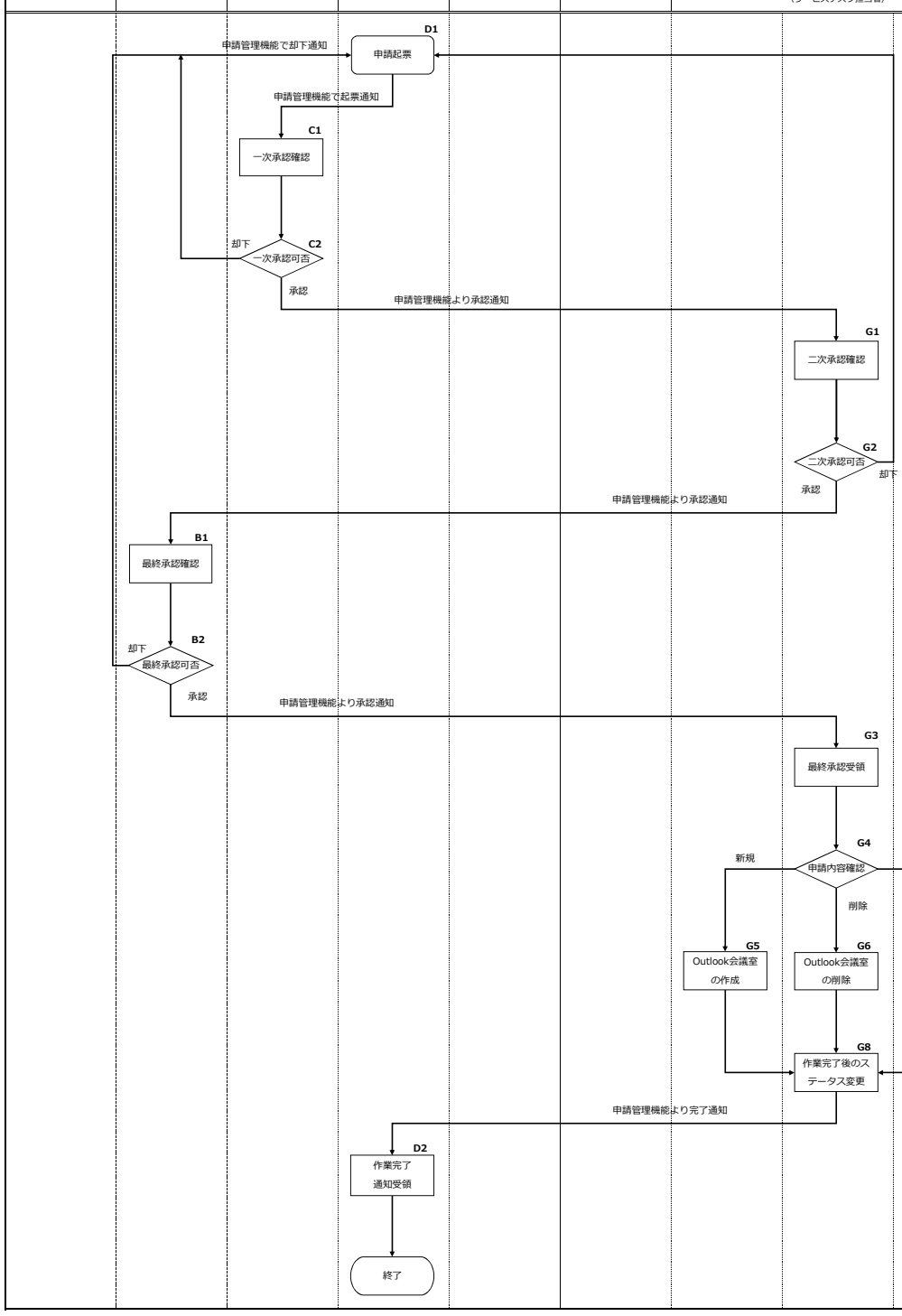
項番	説明
B1	システム管理者は「ソフトウェアインストール申請書」の内容を確認し、申請内容に関する処理の実施可否の最終判断を行う。
B2	システム管理者は確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C1	機関等担当者、地方防衛局担当者はインストール・アンインストール・バージョンアップしたいソフトウェアがある場合、申請管理機能を用いて「ソフトウェアインストール申請書」として起票する。
C2	機関等担当者、地方防衛局担当者は起票された「ソフトウェアインストール申請書」の内容を確認し、その妥当性や、申請内容に不備が無いか確認を行う。機関等担当者、地方防衛局担当者が申請者の場合はここでの確認は実施しない。
C3	機関等担当者、地方防衛局担当者は、確認結果を基に申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。機関等担当者、地方防衛局担当者が申請者の場合には自己承認を実施する。
D1	課室等担当者はインストール・アンインストール・バージョンアップしたいソフトウェアがある場合、申請管理機能を用いて「ソフトウェアインストール申請書」として起票する。
D2	課室等担当者はソフトウェアインストールのためSKYSEAのリモート操作の許可連絡をシステム運用担当者から受領する。
D3	課室等担当者はSKYSEAのリモート操作を許可する。
D4	課室等担当者は「ソフトウェアインストール申請書」の申請処理がすべて完了した旨を、申請管理機能上で確認する。動作確認後、問題があった場合は問合せを実施する。
F1	運用業務実施責任者はソフトウェアインストール申請の内容に基いて、省OA関係者（システム運用、SOC運用、保守事業者）を招集し調査・検討を実施する。
G1	システム運用担当者は、申請管理機能で提出された申請内容を確認する。 申請に当たって必要事項の欠落や誤った記載がないか確認する。 ・申請種別を確認する ・利用者名とホスト名に齟齬がないかを確認する ・申請理由が適切かどうか確認する ・実施希望日が運用作業が可能な日付かを確認する ・インストール依頼の場合は、インストーラの格納パスにファイルが格納されていることを確認する ・対象のソフトウェアがフリーソフトや無償ソフトウェアか、調達品かを確認する。
G2	システム運用担当者は、申請書の不備の有無の確認結果、不備があった場合はその個所の指摘と共に申請者に戻す。フリーソフトや無償ソフトウェアの場合は技術相談をする。調達品の場合は技術相談をせず次の確認へ進む。
G3	システム運用担当者は、申請種別を確認する。インストールかアンインストールかバージョンアップかを確認し、インストールの場合調達品かそれ以外かも確認する。
G4	システム運用担当者は、ソフトウェアインストール申請の内容に基いて、ソフトウェアの調査・検討を実施する。
G5	システム運用担当者は、インストール方式について対象のソフトウェアがサイレントインストールか非サイレントインストールかを確認する。
G6	システム運用担当者は、SKYSEAにて該当の端末にソフトウェアがインストールされているかどうかを確認する。
G7	システム運用担当者は、確認の結果、該当の端末にソフトウェアがインストールされていない場合はその旨を記載し申請を却下する。
G8	システム運用担当者は、インストール対象が部内系か部外系かを確認する。
G9	システム運用担当者は、インストールの実施方法について検討する。 ・対象台数（5台以下の場合はリモート操作での配布） ・部内系か部外系か ・サイレントインストール対象か 条件によって配布方式を検討する。 （Intune、Microsoft Configration Manager、SKYSEA配布、SKYSEAのリモート操作）
G10	システム運用担当者は、インストール依頼の場合、事前試験を実施する。インストーラの不具合等でインストールに問題が生じた場合はその旨を記載し却下する。
G11	システム運用担当者は、ここまでの一連のやり取りを踏まえ、申請内容を受理するか判断を行う。
G12	システム運用担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。 ・却下する場合は、却下理由と共に申請者に戻す。 ・承認する場合は、システム管理者に申請管理機能により申請内容の最終判断の依頼を行う。 技術相談検討会の結果が否の場合は却下とする。
G13	システム運用担当者は、システム管理者からの申請内容に関する最終承認を受け、申請内容の処理に入る。
G14	システム運用担当者は、事前に検討した実施方法を確認する。 （SKYSEAのリモート操作かそれ以外か）
G15	システム運用担当者は、SKYSEAのリモート操作での作業の場合は事前に利用者に接続時間を連絡する。
G16	システム運用担当者は、事前に検討した実施方法にて作業を実施する。
G17	システム運用担当者は、インストールしたソフトウェアをSKYSEAで起動許可、アンインストールした場合は起動拒否に設定する。
G18	システム運用担当者は、作業日時、ソフトウェア名、ホスト名等をソフトウェア作業管理台帳に記載する。
G19	システム運用担当者は、申請管理機能の本申請に係るステータスを完了にし、運用対応を終了する。
H1	SOC担当者は、運用業務実施責任者の招集に応じ、ソフトウェアの調査・検討を実施する。
I1	CSIRT担当者は、運用業務実施責任者の招集に応じ、ソフトウェアの調査・検討を実施する。
J1	保守業務担当者は、運用業務実施責任者の招集に応じ、ソフトウェアの調査・検討を実施する。

フロー名称	説明	作業トリガー
機関共有フォルダ作成等申請書	「機関共有フォルダ作成等申請書」の起票に伴う、 機関共有フォルダ新規追加／変更／削除のフローを示す。	省OA課室担当者からの申請依頼



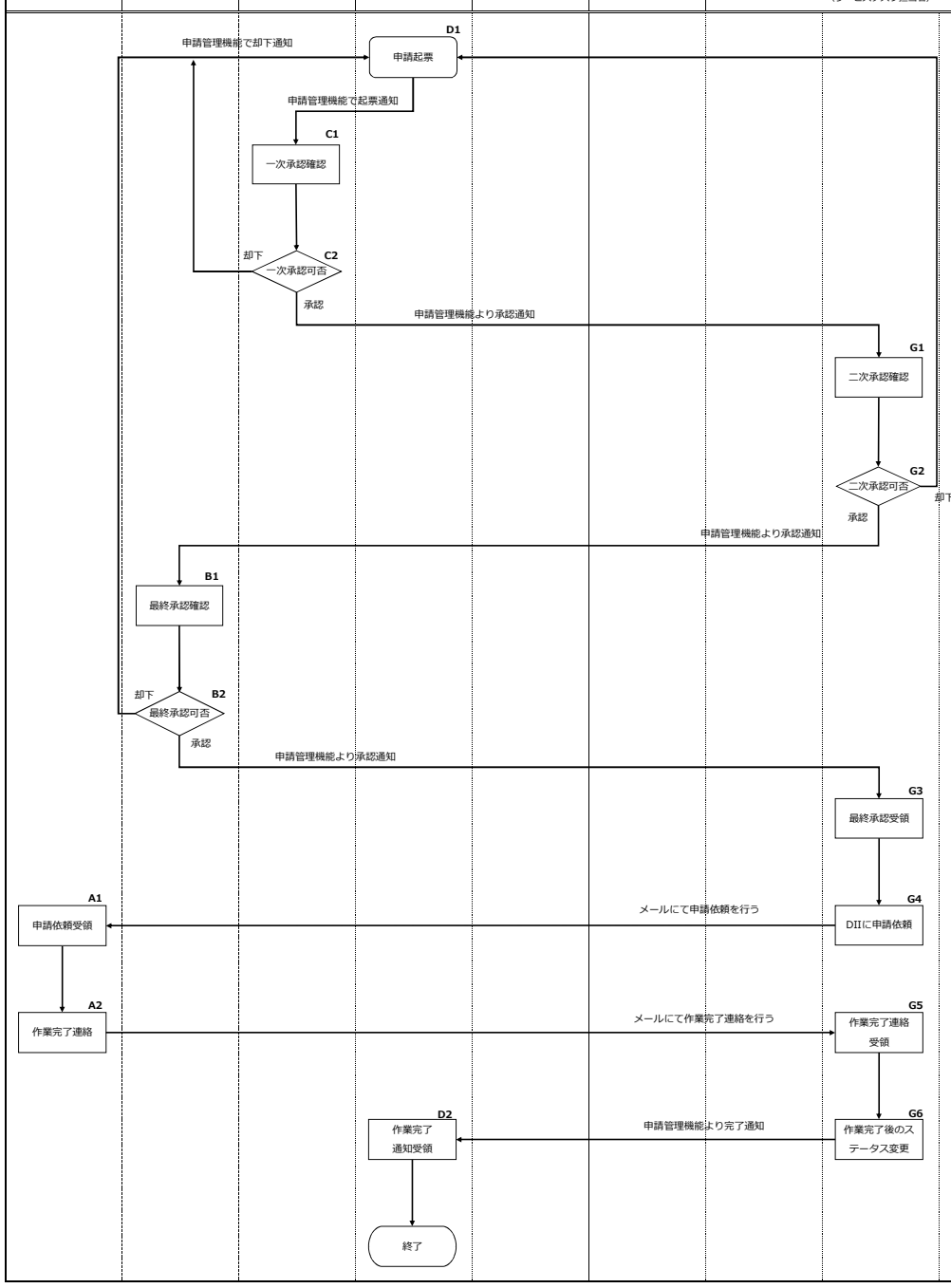
項番	説明
B1	システム管理者は、最終承認確認を行う。
B2	システム管理者は、申請書の内容に基づき、最終承認可否の判断を行う。
C1	機関等担当者、地方防衛局担当者は、一次承認確認を行う。
C2	機関等担当者、地方防衛局担当者は、申請書の内容に基づき、一次承認可否の判断を行う。
D1	課室等担当者は、申請管理機能で申請を起票する。
D2	課室等担当者は、作業完了報告を受領する。
G1	システム運用担当者は、二次承認確認を行う。 下記の必須項目が申請書に入力されているかを確認する。 ・申請種別 ・申請理由 ・共有フォルダ名 ・実施希望日 また、申請種別が削除以外の場合に、下記項目が申請書に入力されているかを確認する。 ・管理者の所属・役職 ・管理者の利用者名 ・利用者の所属・役職 ・利用者の利用者名 ・アクセス権 ・追加削除種別 ・利用終了予定日 上記入力された各項目内容の妥当性を確認する。
G2	システム運用担当者は、申請の項目に基づき、最終承認可否の判断を行う。
G3	システム運用担当者は、最終承認を受領する。
G4	申請管理機能より、「他機能連携」による自動処理が行われる。 【新規】 ・機関共有フォルダ用セキュリティグループ(読み取りのみ/書き込み可の2種類)の作成 ・機関共有フォルダの作成 機関共有フォルダ名：【使用期限YYYYMMDD】共有フォルダ名 ・アクセス権の設定 【変更】 ・個人アカウント又は共有アカウントを機関共有フォルダ用セキュリティグループのメンバーに追加またはメンバーから削除 【削除】 ・機関共有フォルダ用セキュリティグループの削除 ・共有フォルダのアクセス権から「機関共有フォルダ用セキュリティグループ」を削除 ・共有フォルダを非表示化（隠しフォルダ）に変更 ※非表示化してから30日経過した共有フォルダを削除
G5	システム運用担当者は、処理結果のステータス確認を行う。
G6	システム運用担当者は、自動処理の「成功」、「失敗」の判断を行う。 ・「YES」の場合は、「作業完了後のステータス変更」へ ・「NO」の場合は、「エラー内容の確認・修正」へ
G7	システム運用担当者は、エラー内容の確認・修正作業を行う。
G8	システム運用担当者は、申請管理機能のステータスを完了にする。
	【利用期限を延長する場合】 ・機関共有フォルダ作成等申請書にて新規機関共有フォルダ作成を依頼 ・機関共有フォルダ作成完了後、依頼元にて旧機関共有フォルダから新機関共有フォルダへファイルの移動を実施 ・ファイルの移動完了後、機関共有フォルダ作成等申請書にて旧機関共有フォルダの削除を依頼

フロー名称	説明	作業トリガー
Outlook会議室登録等申請書	「Outlook会議室登録等申請書」の起票に係る、 Outlook会議室登録等の申請に係るフローを示す	・省OA課室担当者からの申請依頼



項番	説明
B1	システム管理者は、「Outlook会議室登録等申請書」の内容を確認し、申請内容に関する処理の実施可否の最終判断を行う。
B2	システム管理者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C1	機関等担当者、地方防衛局担当者は、起票された「Outlook会議室登録等申請書」の内容を確認し、その妥当性や、申請内容に不備が無いか確認を行う。
C2	機関等担当者、地方防衛局担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
D1	課室等担当者は、申請管理機能でOutlook会議室登録等申請書を起票する。
D2	課室等担当者は、「Outlook会議室登録等申請書」の申請内容が反映されていることを確認する。
G1	システム運用担当者は、申請管理機能で提出された申請内容を確認する。 申請に当たって必要事項の欠落や誤った記載がないか確認する。 以下項目の内容を確認する。 1 申請種別：選択されていることを確認する 2 Outlook会議室名：入力されていることを確認する 3 Outlook会議室名(変更後)：申請種別が変更の場合、入力されていることを確認する 4 Outlook会議室その他の情報(場所)：入力されていることを確認する 5 Outlook会議室その他の情報(会議室の内線)：入力されていることを確認する 6 Outlook会議室その他の情報(Outlook会議室の管理者)：予約時の制限が手動承認の場合、選択されていることを確認する 7 Outlook会議室その他の情報(予約時の制限)：予約時に管理者による承認制にするのか、承認不要とするのかを選択する 9 Outlook会議室その他の情報(Outlook会議室を利用できるシステム利用者)：Outlook会議室を利用できるシステム利用者の追加・削除がある場合、選択されていることを確認する 10 実施希望日：実施希望日が運用対応可能か確認する
G2	システム運用担当者は、申請内容を「承認」するか、「却下」するか判断する。 ・却下する場合は、却下理由と共に申請者に戻す。 ・承認する場合は、システム管理者に申請管理機能により申請内容の最終判断の依頼を行う。
G3	システム運用担当者は、システム管理者からの申請内容に関する最終承認を受領し、請内容の処理に入る
G4	申請内容の確認 新規：Outlook会議室の作成 削除：Outlook会議室の削除 変更：Outlook会議室の設定変更
G5	システム運用担当者は、Outlook会議室を作成する 手順書に従い、Exchange管理センター（EAC）にてOutlook会議室の作成を行う。
G6	システム運用担当者は、Outlook会議室を削除する 手順書に従い、Exchange管理センター（EAC）にてOutlook会議室の削除を行う。
G7	システム運用担当者は、Outlook会議室を変更する 手順書に従い、Exchange管理センター（EAC）にてOutlook会議室の設定変更を行う。
G8	システム運用担当者は、申請管理機能の本申請に係るステータスを完了にし、運用対応を終了する。

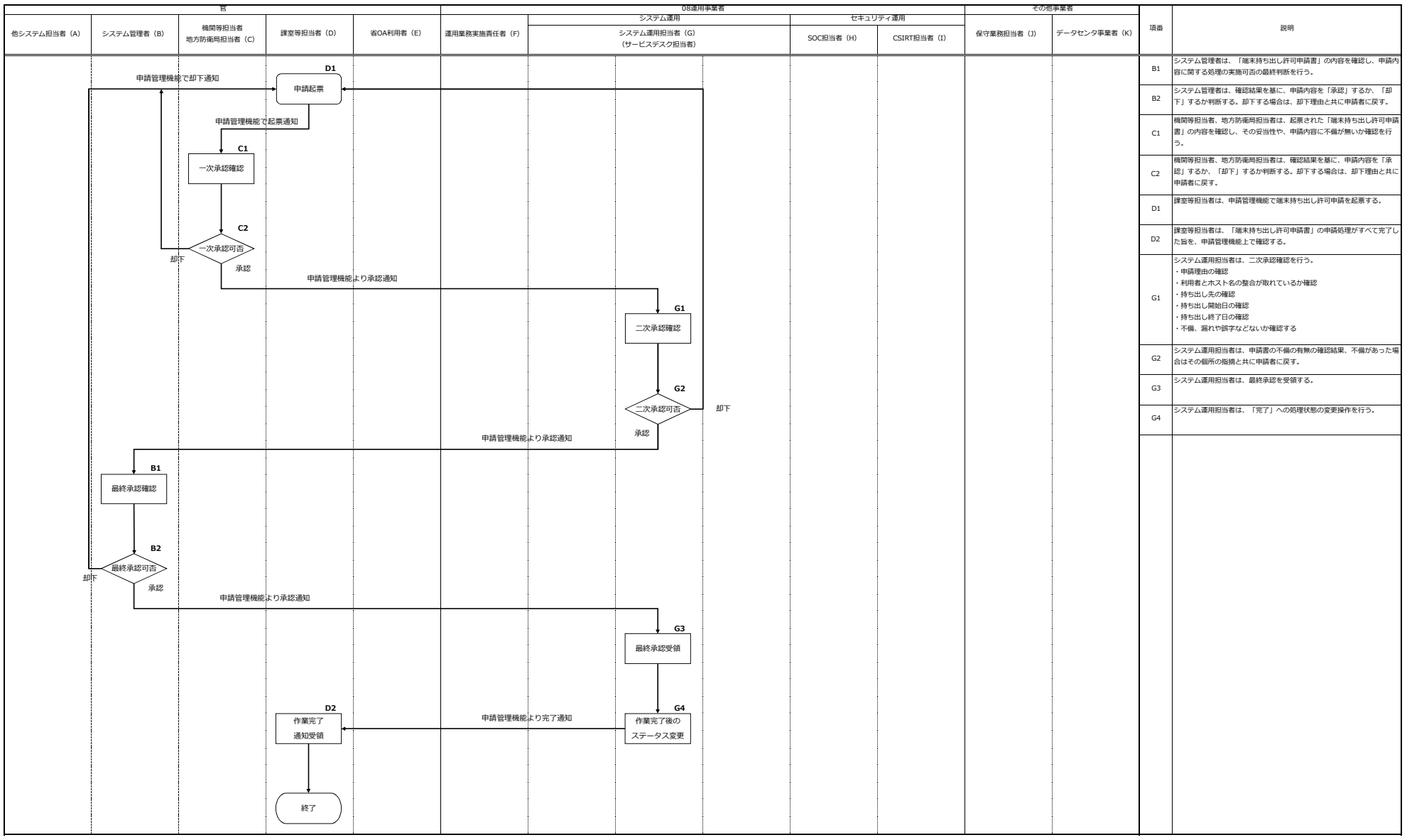
フロー名称	説明	作業トリガー
Web公開サービス利用申請書	「Web公開サービス利用申請書」の起票に係る、 DIIに対して代理申請に係るフローを示す	課室等担当者からの申請依頼



項番	説明
A1	DII担当者は、申請依頼を受領する。
A2	DII担当者は、作業完了の連絡を行う。
B1	システム管理者は、「Web公開サービス利用申請書」の内容を確認し、申請内容に関する処理の実施可否の最終判断を行う。
B2	システム管理者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C1	機関等担当者、地方防衛局担当者は、起票された「Web公開サービス利用申請書」の内容を確認し、その妥当性や、申請内容に不備が無いか確認を行う。
C2	機関等担当者、地方防衛局担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
D1	課室等担当者は、申請管理機能で共有アカウント登録等申請を起票する。
D2	課室等担当者は、「共有アカウント登録等申請書」の申請処理がすべて完了した旨を、申請管理機能上で確認する。
G1	システム運用担当者は、二次承認確認を行う。 ・添付ファイルの確認(必要項目が埋まっているか) 　├加入システム全般に係る申請項目 　├各サブディレクトリに係る申請項目 　├省外Webサーバに配置するフォームメールに係る申請項目 　└省内WebサーバでのID/パスワード認証による閲覧制限に係る申請項目 　　※全てかいずれかのファイルが添付されている ・実施希望日を確認 ・不備、漏れや誤字などないか確認
G2	システム運用担当者は、申請書の不備の有無の確認結果、不備があった場合はその個所の指摘と共に申請者に戻す。
G3	システム運用担当者は、最終承認を受領する。
G4	システム運用担当者は、DII担当者に添付ファイルを送付して申請依頼を行う。
G5	システム運用担当者は、DII担当者より作業完了連絡を受領する。
G6	システム運用担当者は、「完了」へ処理状態の変更操作を行う。

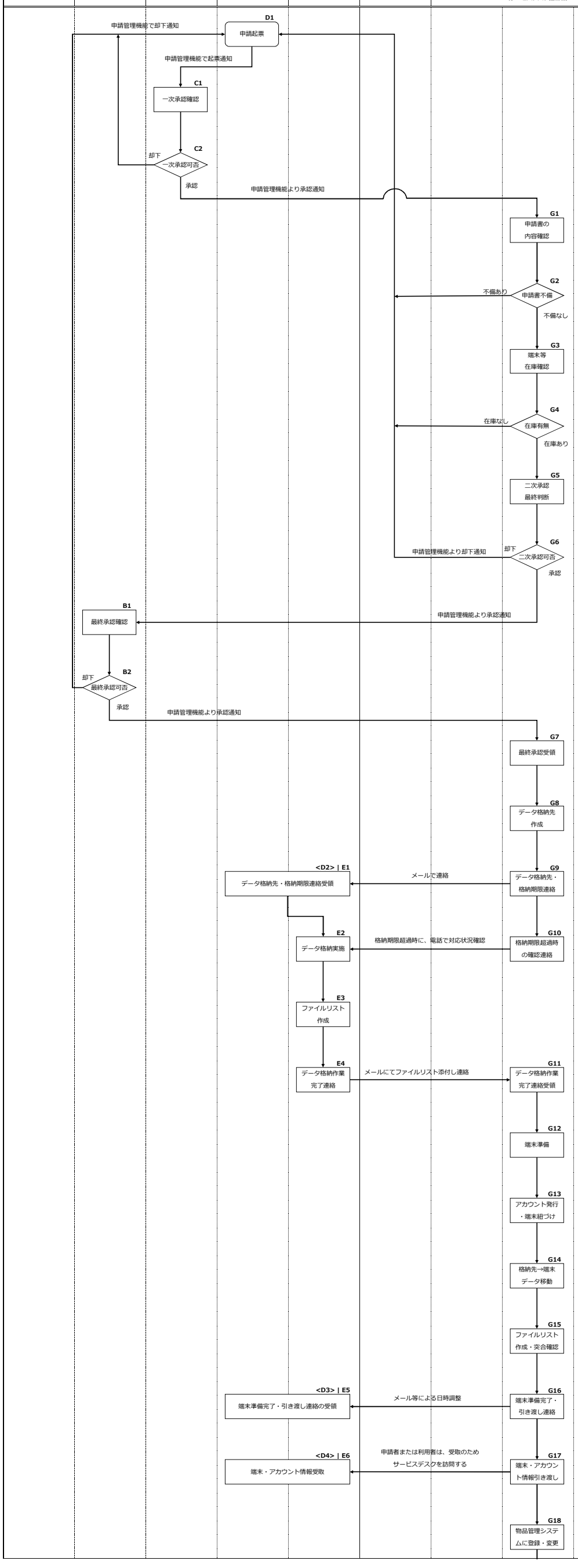
付表９　業務フロー（続き）
端末持ち出し許可申請書（続き）

フロー名称	説明	作業トリガー
端末持ち出し許可申請書	「端末持ち出し許可申請書」の起票に係る、 端末の持出に係るフローを示す	課室等担当者からの申請依頼



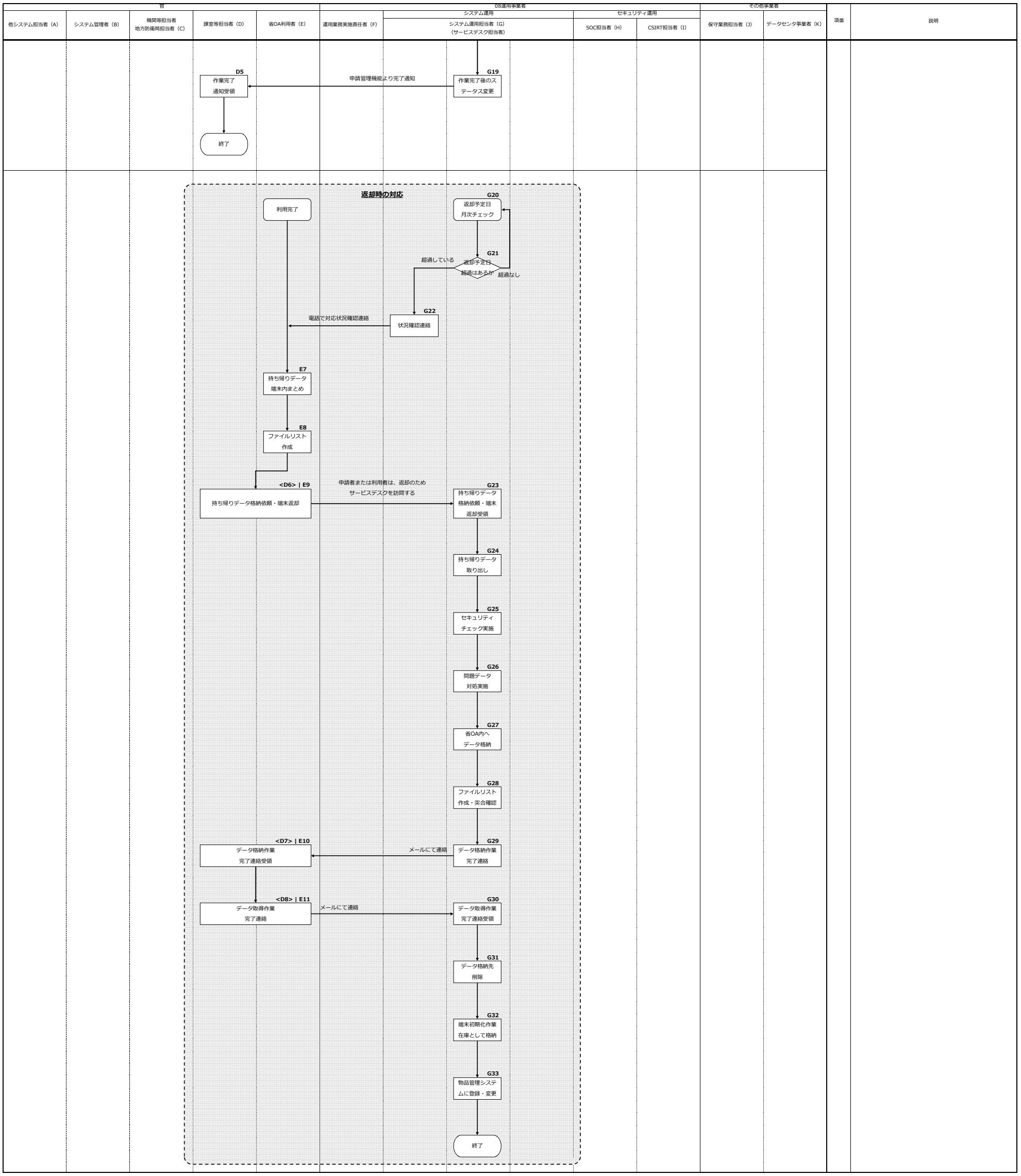
項番	説明
B1	システム管理者は、「端末持ち出し許可申請書」の内容を確認し、申請内容に関する処理の実施可否の最終判断を行う。
B2	システム管理者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C1	機関等担当者、地方防衛局担当者は、起票された「端末持ち出し許可申請書」の内容を確認し、その妥当性や、申請内容に不備が無いか確認を行う。
C2	機関等担当者、地方防衛局担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
D1	課室等担当者は、申請管理機能で端末持ち出し許可申請を起票する。
D2	課室等担当者は、「端末持ち出し許可申請書」の申請処理がすべて完了した旨を、申請管理機能上で確認する。
G1	システム運用担当者は、二次承認確認を行う。 ・申請理由の確認 ・利用者とホスト名の整合が取れているか確認 ・持ち出し先の確認 ・持ち出し開始日の確認 ・持ち出し終了日の確認 ・不備、漏れや誤字などないか確認する
G2	システム運用担当者は、申請書の不備の有無の確認結果、不備があった場合はその個所の指摘と共に申請者に戻す。
G3	システム運用担当者は、最終承認を受領する。
G4	システム運用担当者は、「完了」への処理状態の変更操作を行う。

フロー名称	説明	作業トリガー
機能制限端末払出等申請書	「機能制限端末払出等申請書」の起票に係る、 機能制限端末の払出しと機能制限端末用アカウントを払い出すために係るフローを示す	・省OA課室担当者からの申請依頼

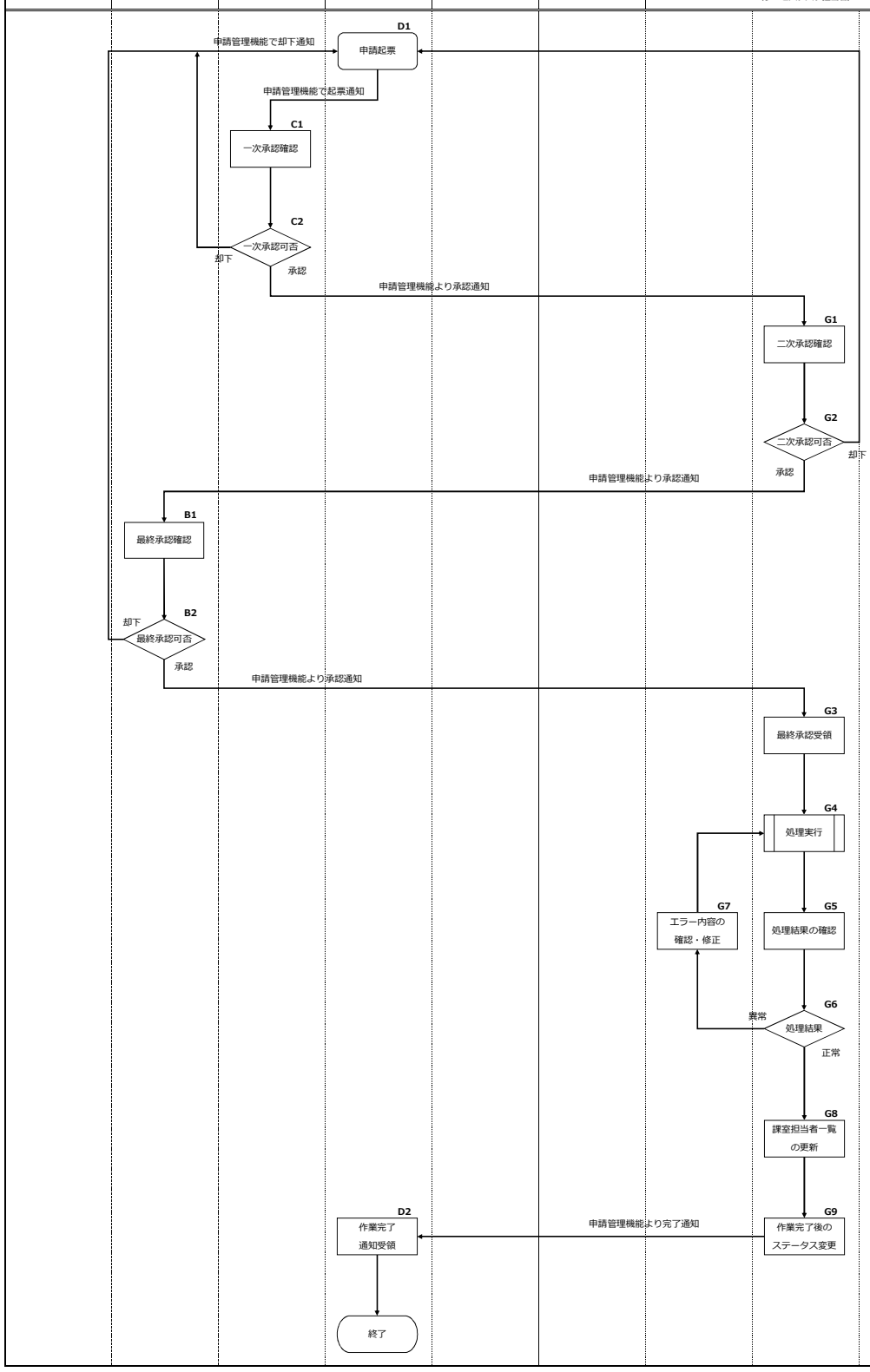


項番	説明
B1	システム管理者は、「機能制限端末払出等申請書」の内容を確認し、申請内容に関する処理の実施可否の最終判断を行う。
B2	システム管理者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C1	機関等担当者、地方防衛局担当者は、起票された「機能制限端末払出等申請書」の内容を確認し、その妥当性や、申請内容に不備が無いか確認を行う。
C2	機関等担当者、地方防衛局担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
D1	課室等担当者は、申請管理機能を用いて「機能制限端末払出等申請書」として起票する。
D2	課室等担当者は、データ格納先フォルダ情報と格納期限の連絡を受領する。
D3	課室等担当者は、システム運用担当者より、端末準備完了および端末の引き渡し日時の連絡を受領する。
D4	課室等担当者は、申請者または省OA利用者は、サービスデスクを訪問し、端末およびアカウント情報を受領する。
D5	課室等担当者は、「機能制限端末払出等申請書」の端末払出の申請処理が完了した旨を、申請管理機能上で確認する。
D6	課室等担当者は、システム運用担当者へ持ち帰りデータの格納依頼を連絡し、ファイルリストを送付する。サービスデスクを訪問し、端末を返却する。
D7	課室等担当者は、システム運用担当者よりデータ格納作業が完了した旨と、ファイルリストの突合結果を受領する。
D8	課室等担当者は、データ取得後、システム運用担当者へデータ取得作業が完了した旨を連絡する。
E1	省OA利用者は、データ格納先フォルダ情報と格納期限の連絡を受領する。 （急ぎの対応や課室等担当者が不在の際などの対応とする）
E2	省OA利用者は、データ格納先フォルダへ持ち出しデータを格納する。
E3	省OA利用者は、ファイルリスト作成補助ツールで持ち出しデータのファイルリストを作成する。
E4	省OA利用者は、システム運用担当者へデータ格納作業が完了した旨を連絡し、ファイルリストを送付する。
E5	省OA利用者は、システム運用担当者より、端末準備完了および端末の引き渡し日時の連絡を受領する。（急ぎの対応や課室等担当者が不在の際などの対応とする）
E6	省OA利用者は、申請者または省OA利用者は、サービスデスクを訪問し、端末およびアカウント情報を受領する。（急ぎの対応や課室等担当者が不在の際などの対応とする）
E7	省OA利用者は、持ち帰り要望のファイルを、端末の格納フォルダを決め、とりまとめる。
E8	省OA利用者は、ファイルリスト作成補助ツールで持ち帰りデータのファイルリストを作成する。
E9	省OA利用者は、システム運用担当者へ持ち帰りデータの格納依頼を連絡し、ファイルリストを送付する。サービスデスクを訪問し、端末を返却する。（急ぎの対応や課室等担当者が不在の際などの対応とする）
E10	省OA利用者は、システム運用担当者よりデータ格納作業が完了した旨と、ファイルリストの突合結果を受領する。（急ぎの対応や課室等担当者が不在の際などの対応とする）
E11	省OA利用者は、データ取得後、システム運用担当者へデータ取得作業が完了した旨を連絡する。（急ぎの対応や課室等担当者が不在の際などの対応とする）
G1	システム運用担当者は、二次承認確認を行う。 ・貸出希望日：5営業日以降の日程が記載されているか ・返却予定日：返却予定日が記載されているか
G2	システム運用担当者は、申請書の不備の有無の確認結果、不備があった場合はその個所の指摘と共に申請者に戻す。
G3	システム運用担当者は、申請内容に端末の払い出しを求めるものであった場合、払い出し可能な端末の予備在庫があるか確認する。
G4	払い出し可能な端末の在庫有無により対応が分岐する。
G5	システム運用担当者は、ここまでの一連のやり取りを踏まえ、申請内容を受理するか判断を行う。
G6	システム運用担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。 ・却下する場合は、却下理由と共に申請者に戻す。 ・承認する場合は、システム管理者に申請管理機能により申請内容の最終判断の依頼を行う。
G7	システム運用担当者は、システム管理者からの申請内容に関する最終承認を受け、申請内容の処理に入る。
G8	システム運用担当者は、データ格納先フォルダを作成する。 アクセス許可は、省OA利用者とシステム運用担当者/運用業務実施責任者とする。
G9	システム運用担当者は、申請者に対しデータ格納先フォルダ情報と格納期限を連絡する。
G10	システム運用担当者は、格納期限を超過した際に、電話にて対応状況の確認連絡を行い、速やかにデータ格納を実施するよう依頼する。
G11	システム運用担当者は、申請者よりデータ格納作業の完了とファイルリストを受領する。
G12	システム運用担当者は、機能制限端末を準備する。 ※ファイルリスト作成補助ツールを格納する
G13	システム運用担当者は、機能制限端末用アカウントを発行し、機能制限端末と紐づけを実施する。
G14	システム運用担当者は、データ格納先フォルダより、可搬記憶媒体を介し、端末へ持ち出しデータを移動する。
G15	システム運用担当者は、ファイルリスト作成補助ツールでデータ格納先フォルダへ格納した持ち出しデータのファイルリストを作成し、省OA利用者より受領したファイルリストと突合確認を行い、突合結果を保存する。
G16	システム運用担当者は、申請者に対し端末準備完了および端末の引き渡し可能日時を連絡する。
G17	システム運用担当者は、申請者に対し機能制限端末および機能制限端末用アカウント情報の引き渡しを行う。
G18	システム運用担当者は、物品管理システムに対して登録・変更作業を行う。
G19	システム運用担当者は、申請管理機能の本申請に係るステータスを完了にする。
G20	システム運用担当者は、月次にて休止終了者（申請一覧より、持ち出し終了日を超過した申請）の有無をチェックする。
G21	持ち出し終了日を超過したかどうかにより、以降の対応内容が分岐する。超過せず次工程が実施されれば問題ないが、超過した場合は状況確認を行う。
G22	システム運用担当者は、申請者に対し状況確認連絡を実施する。
G23	システム運用担当者は、申請者より持ち帰りデータの格納依頼および対象となるファイルリストの連絡を受領し、端末返却を受領する。
G24	システム運用担当者は、機能制限端末より、可搬記憶媒体（USB）へ持ち帰りデータを取り出す。
G25	システム運用担当者は、可搬記憶媒体（USB）の持ち帰りデータに対し、ネットワークから切り離した運用端末にてセキュリティチェックを実施する。
G26	システム運用担当者は、セキュリティチェックで問題が発生した場合、データ削除やフルスキャンなど、必要な対応を実施する。
G27	システム運用担当者は、セキュリティチェックで問題がなかったデータをデータ格納先へ格納する。
G28	システム運用担当者は、ファイルリスト作成補助ツールでデータ格納先フォルダへ格納した持ち帰りデータのファイルリストを作成し、省OA利用者より受領したファイルリストと突合確認を行い、突合結果を保存する。
G29	システム運用担当者は、申請者に対しデータ格納作業の完了の連絡と、ファイルリストの突合結果を送付する。データ削除等を行い持ち込めなかったファイルは、該当ファイルと理由を明記する。
G30	システム運用担当者は、申請者よりデータ取得作業の完了連絡を受領する。
G31	システム運用担当者は、データ格納先フォルダを削除する。
G32	システム運用担当者は、端末初期化作業及び在庫として所定の配置場所に返却端末を格納する。
G33	システム運用担当者は、物品管理システムに対して登録・変更作業を行う。

フロー名称	説明	作業トリガー
機能制限端末払出等申請書	「機能制限端末払出等申請書」の起票に係る、 機能制限端末の払出しと機能制限端末用アカウントを払い出すために係るフローを示す	・省OA課室担当者からの申請依頼

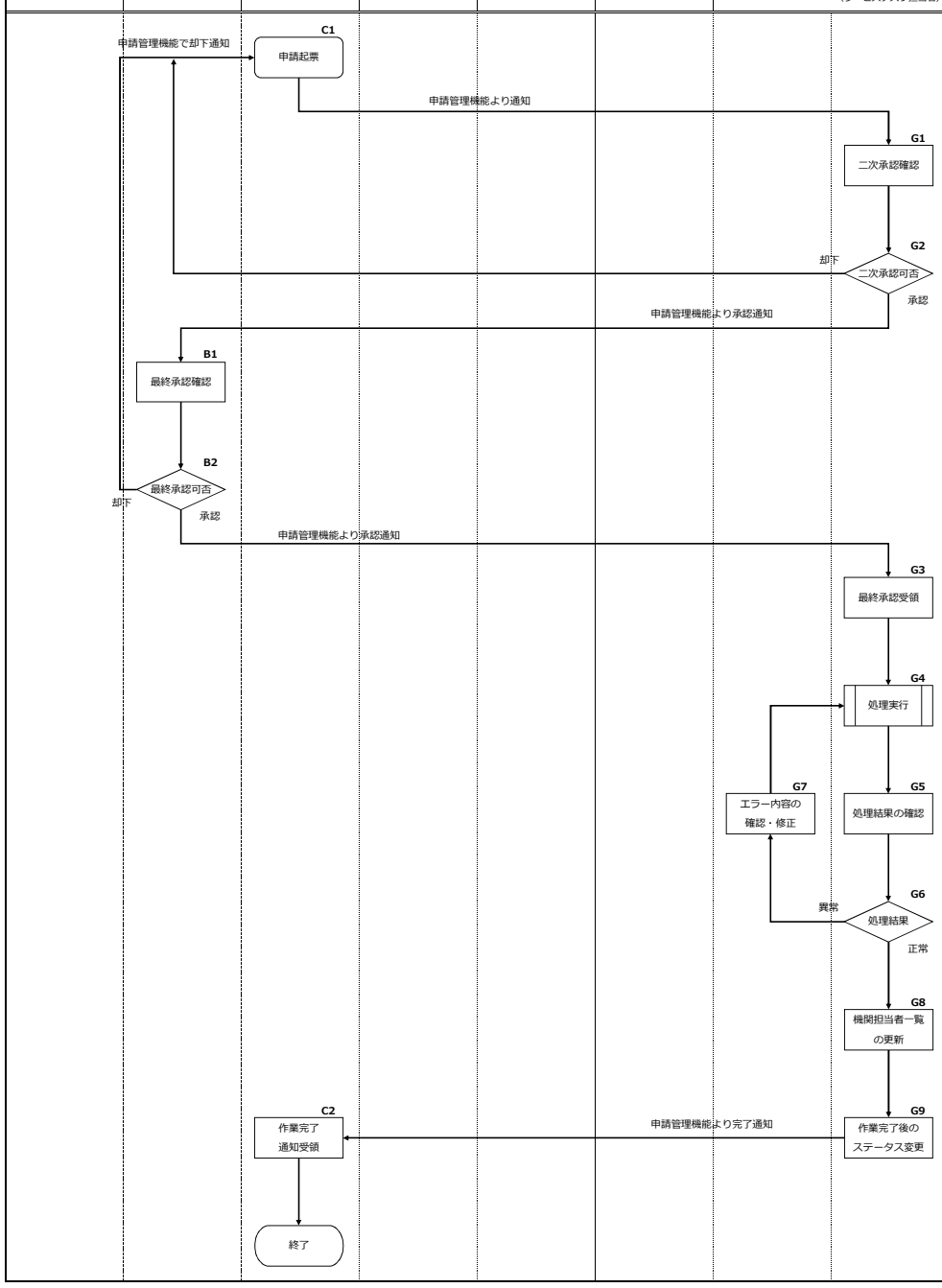


フロー名称	説明	作業トリガー
課室等担当者登録等申請書	「課室等担当者登録等申請書」の起票に係る、 課室等担当者登録等の申請に係るフローを示す	・省OA課室担当者からの申請依頼



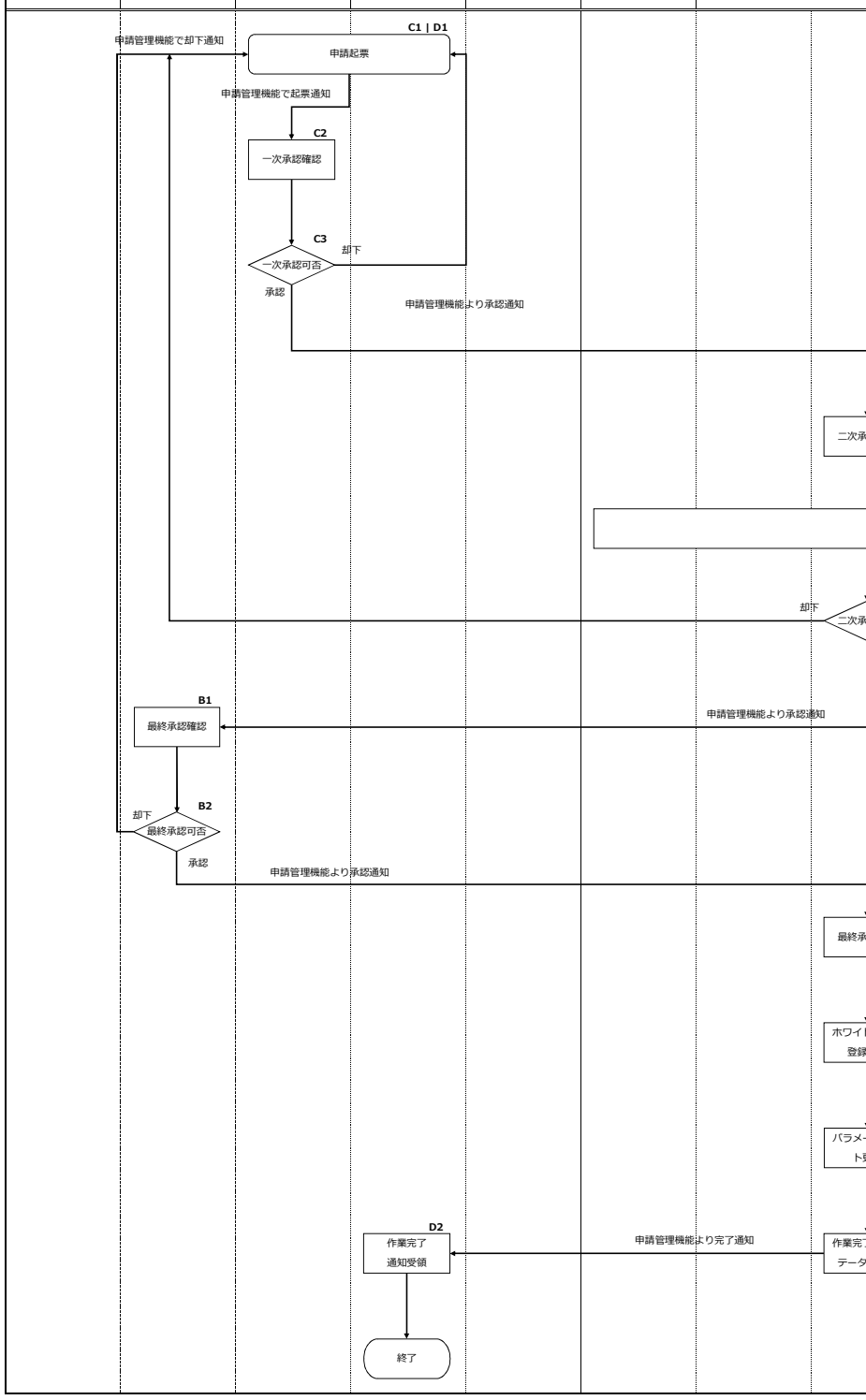
項番	説明
B1	システム管理者は、「課室等担当者登録等申請書」の内容を確認し、申請内容に関する処理の実施可否の最終判断を行う。
B2	システム管理者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C1	機関等担当者、地方防衛局担当者は、起票された「課室等担当者登録等申請書」の内容を確認し、申請理由と記載内容が正しいかを確認する。
C2	機関等担当者、地方防衛局担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
D1	課室等担当者は、申請管理機能で課室等担当者登録等申請を起票する。
D2	課室等担当者は、「課室等担当者登録等申請書」の申請処理がすべて完了した旨を、申請管理機能上で確認する。
G1	システム運用担当者は、二次承認確認を行う。 ・申請種別 ・対象課室 ・担当者名 ・実施希望日 ・不備、漏れや誤字などないか確認する
G2	システム運用担当者は、課室等担当者登録等申請の項目に基いて、二次承認可否の判断を行う。
G3	システム運用担当者は、システム管理者からの申請内容に関する最終承認を受領し、請内容の処理に入る。
G4	課室等担当者登録処理が自動実行される。
G5	システム運用担当者は、課室等担当者登録処理結果の確認を行う。
G6	システム運用担当者は、課室等担当者登録処理結果より正常終了・異常終了の判断を行う。
G7	システム運用担当者は、異常終了時、エラー内容を確認し、修正を行う。
G8	システム運用担当者は、課室担当者一覧（機関毎）の更新を行う。 管理項目は以下のとおり。 （職員マスタを参照し、以下情報を補完する） ・氏名 ・ふりがな ・アカウントID ・機関 ・所属 ・階級 ・内線番号 ・追加変更実施日
G9	システム運用担当者は、申請管理機能のステータスを完了にする。

フロー名称	説明	作業トリガー
機関担当者登録等申請書	「機関担当者登録等申請書」の起票に係る、 機関担当者登録等の申請に係るフローを示す	省OA機関等担当者からの申請依頼があった時



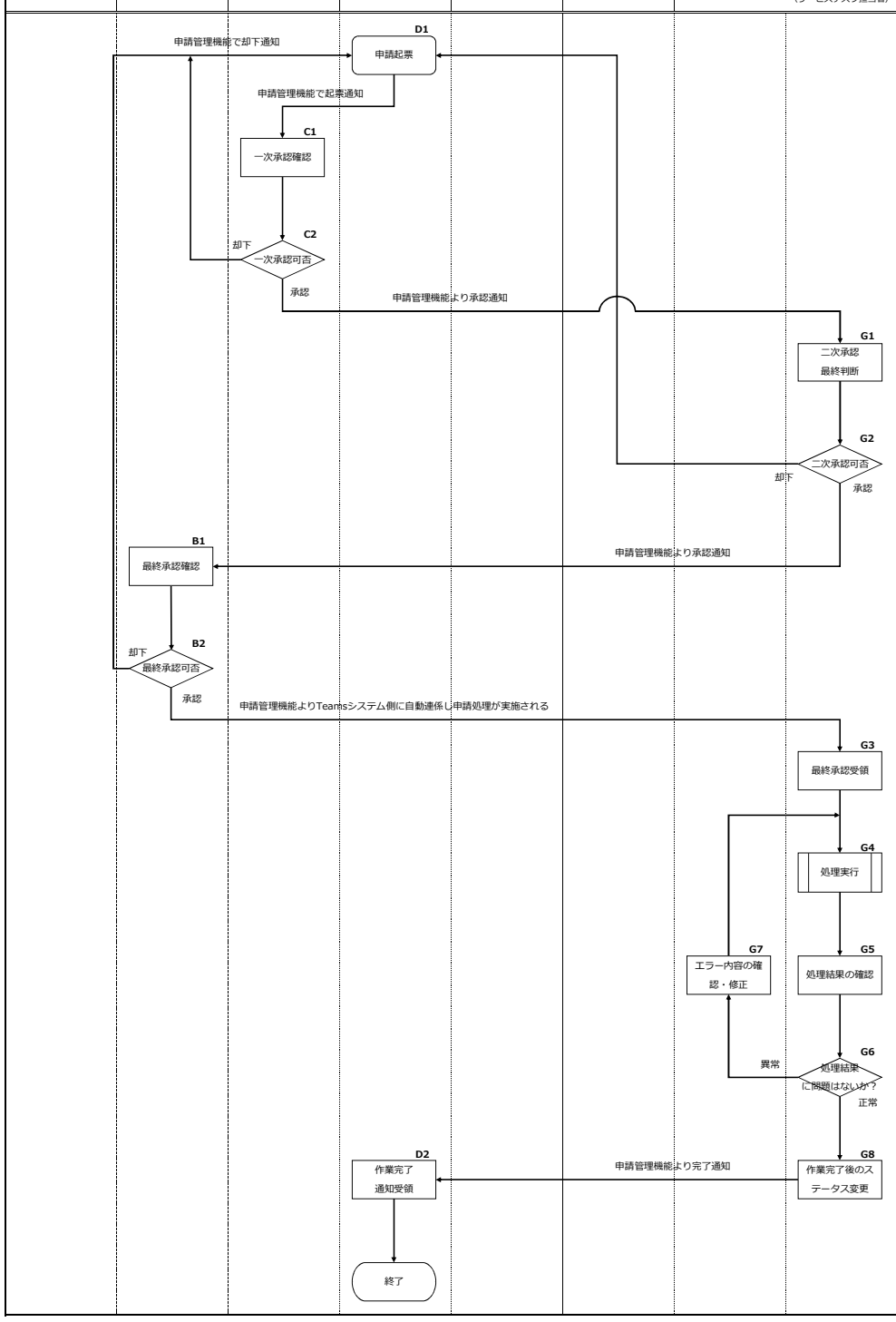
項番	説明
B1	システム管理者は、「機関担当者登録等申請書」の内容を確認し、申請内容に関する処理の実施可否の最終判断を行う。
B2	システム管理者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C1	機関等担当者、地方防衛局担当者は、申請管理機能で機関担当者登録等申請を起票し、既存の機関担当者が後任担当者を登録する。
C2	機関等担当者、地方防衛局担当者は、「機関担当者登録等申請書」の申請処理がすべて完了した旨を、申請管理機能上で確認する。
G1	システム運用担当者は、二次承認確認を行う。 ・申請種別を確認する ・対象機関を確認する ・担当者名 ・実施希望日 ・不備、漏れや誤字などないか確認する
G2	システム運用担当者は、機関担当者登録等申請の項目に基いて、二次承認可否の判断を行う。
G3	システム運用担当者は、システム管理者からの申請内容に関する最終承認を受領し、請内容の処理に入る。
G4	機関担当者登録処理が自動実行される。
G5	システム運用担当者は、機関担当者登録処理結果の確認を行う。
G6	システム運用担当者は、機関担当者登録処理結果より正常終了・異常終了の判断を行う。
G7	システム運用担当者は、異常終了時に、エラー内容を確認し、修正を行う。
G8	システム運用担当者は、機関担当者一覧（機関毎）の更新する。管理項目は以下のとおり。 （職員マスタを参照し、以下情報を補完する） ・氏名 ・ふりがな ・アカウントID ・機関 ・所属 ・階級 ・内線番号 ・追加変更実施日
G9	システム運用担当者は、申請管理機能のステータスを完了にする。

フロー名称	説明	作業トリガー
インターネットWeb閲覧許可申請書	「インターネットWeb閲覧許可申請書」の起票に係る、 Web監査機能における、閲覧不可カテゴリ内の特定サイトをホワイトリストに登録し、閲覧可能とするための申請フローを示す	省OA課室担当者からの申請依頼



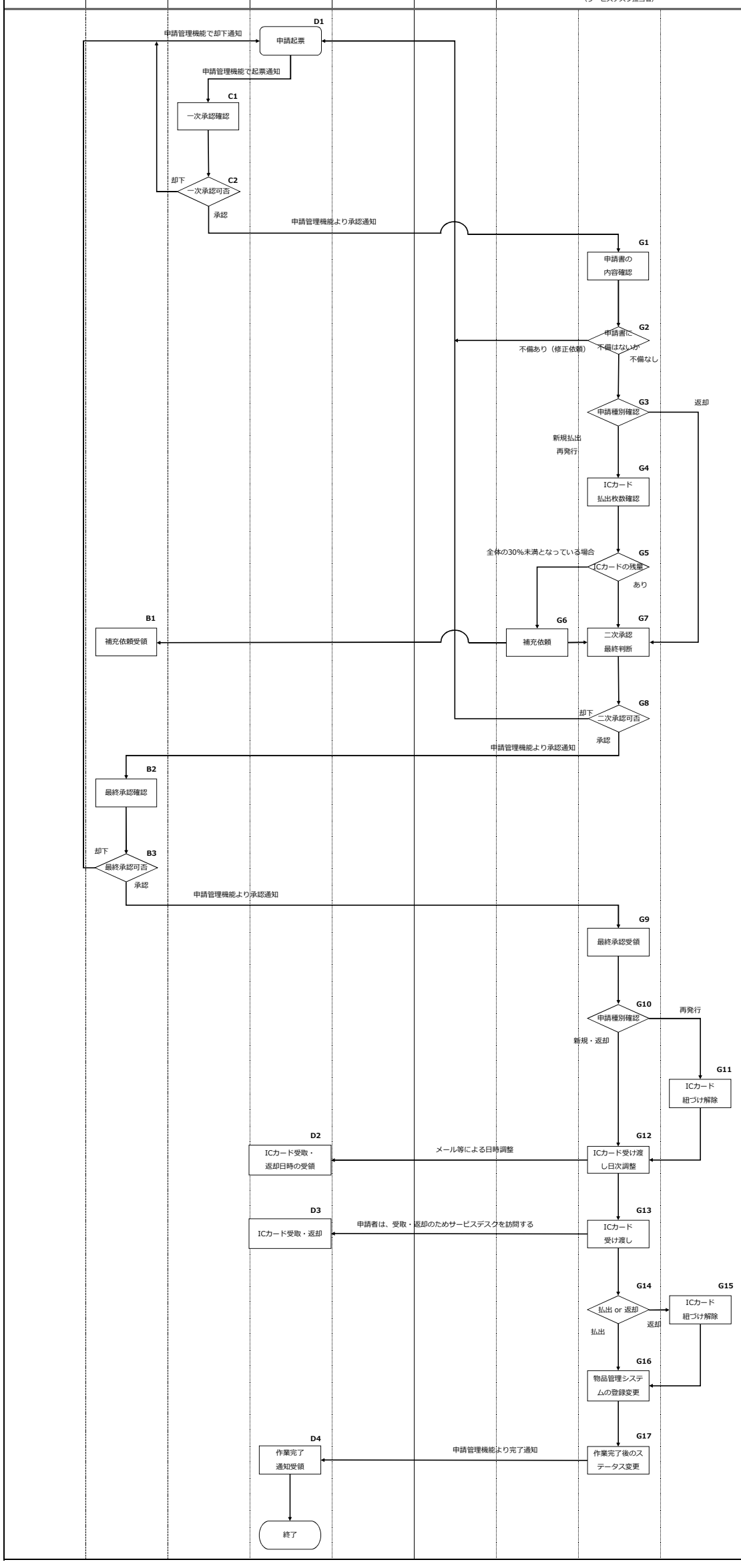
項番	説明
B1	システム管理者は、「インターネットWeb閲覧許可申請書」の内容を確認し、申請内容に関する処理の実施可否の最終判断を行う。
B2	システム管理者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C1	機関等担当者、地方防衛局担当者は、申請管理機能を用いて「インターネットWeb閲覧許可申請書」として起票する。
C2	機関等担当者、地方防衛局担当者は、起票された「インターネットWeb閲覧許可申請書」の内容を確認し、その妥当性や、申請内容に不備が無いか確認を行う。機関等担当者・地方防衛局担当者が申請者の場合は自動承認となる。
C3	機関等担当者、地方防衛局担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
D1	課室等担当者は、申請管理機能を用いて「インターネットWeb閲覧許可申請書」として起票する。
D2	課室等担当者は、「インターネットWeb閲覧許可申請書」の申請処理がすべて完了した旨を、申請管理機能上で確認する。
F1	運用業務実施責任者は、インターネットWeb閲覧許可申請の項目に基いて、省OA関係者（システム運用、SOC運用、保守事業者）を招集し調査・検討を実施する。
G1	システム運用担当者は、二次承認確認を行う。 ・申請種別：新規or削除 ・申請理由：適切な内容が記載されているか ・接続を許可するURLまたはドメイン：適切な形式で記載されているか ・判定方式：部分一致or完全一致 ・機関、局、部、課室等：記載されているか ・アカウント名：記載されているか ・実施希望日：過去日付ではないか ・有効期限日：過去日付ではないか、有効期限日が記載されているか
G2	システム運用担当者は、運用業務実施責任者の招集に応じ、インターネットWeb閲覧許可申請項目の調査・検討を実施する。
G3	システム運用担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。 ・却下する場合は、却下理由と共に申請者に戻す。 ・承認する場合は、システム管理者に申請管理機能により申請内容の最終判断の依頼を行う。
G4	システム運用担当者は、システム管理者からの申請内容に関する最終承認を受け、申請内容の処理に入る。
G5	システム運用担当者は、所定の手順書を参照し、インターネットWeb閲覧ホワイトリスト登録作業を実施する。
G6	システム運用担当者は、パラメータシートを更新する。
G7	システム運用担当者は、申請管理機能の本申請に係るステータスを完了にし、運用対応を終了する。
H1	SOC担当者は、運用業務実施責任者の招集に応じ、インターネットWeb閲覧許可申請項目の調査・検討を実施する。
I1	CSIRT担当者は、運用業務実施責任者の招集に応じ、インターネットWeb閲覧許可申請項目の調査・検討を実施する。
J1	保守業務担当者は、運用業務実施責任者の招集に応じ、インターネットWeb閲覧許可申請項目の調査・検討を実施する。

フロー名称	説明	作業トリガー
Teams チーム登録等申請書	「Teams チーム登録等申請書」の起票に係る、 MS Teams上のチーム作成/削除フローを示す。	省OA課室担当者からの申請起票があった場合に実施する。



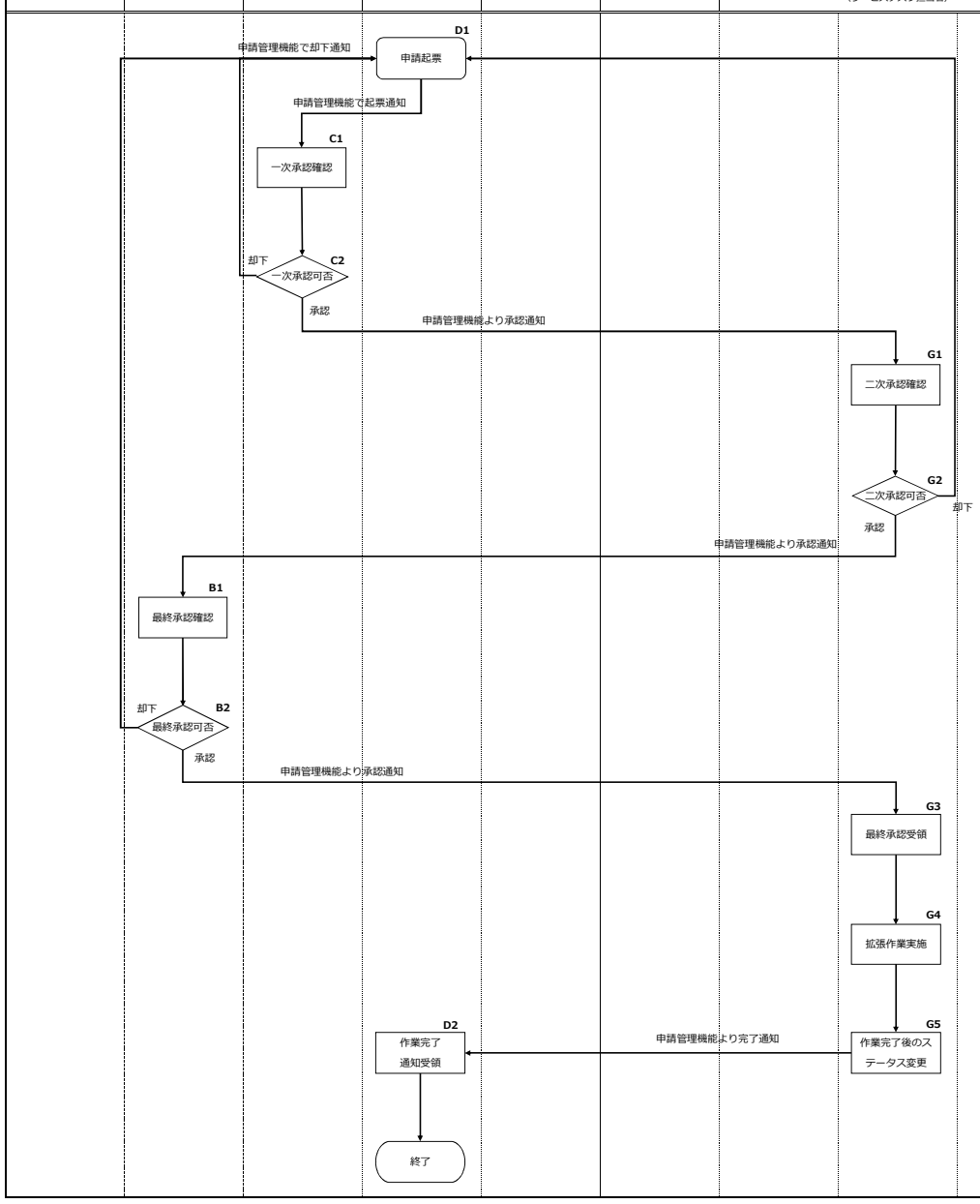
項番	説明
B1	システム管理者は、「Teams チーム登録等申請書」の内容を確認し、申請内容に関する処理の実施可否の最終判断を行う。
B2	システム管理者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C1	機関等担当者、地方防衛局担当者は、起票された申請内容を確認し、その妥当性や、申請内容に不備が無いか確認を行う。
C2	機関等担当者、地方防衛局担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
D1	課室等担当者は、希望する「Teams チーム登録等申請書」に係る申請を、申請管理機能を用いて起票する。
D2	課室等担当者は、「Teams チーム登録等申請書」の申請処理がすべて完了した旨を、申請管理機能上で確認する。
G1	システム運用担当者は、申請管理機能で提出された申請内容を確認する。 申請に当たって必要事項の欠落や誤った記載がないか確認する。 1 申請種別：入力されていることを確認する 2 申請理由：明確な理由が入力されていることを確認する 3 Teamsチーム名：入力されていることを確認する 4 チーム管理者の所属・役職：申請種別が「削除」以外の場合に、入力されていることを確認する 5 チーム管理者名：（必要に応じて入力内容を確認する） 8 Teamsチーム有効期限日：申請種別が「新規」の場合に、入力されていることを確認する 9 実施希望日：実施希望日が運用対応可能か確認する
G2	システム運用担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。 ・却下する場合は、却下理由と共に申請者に戻す。 ・承認する場合は、システム管理者に申請管理機能により申請内容の最終判断の依頼を行う。
G3	システム運用担当者は、システム管理者の最終承認を受領する。
G4	システム運用担当者は、システム管理者による最終承認の後、申請管理機能とMS Teamsは自動連係し、申請内容の処理を行う。
G5	システム運用管理者は、その自動連係の処理結果を確認し、申請に沿った処理が正しく行われているか確認する。
G6	処理結果の確認結果、 ・正常：そのまま申請管理機能ステータス完了に移る。 ・異常：修正作業を行う。
G7	システム運用担当者は、自動連係の処理結果に問題があった場合、問題箇所の修正作業を行う。
G8	システム運用担当者は、申請管理機能の本申請に係るステータスを完了にし、運用対応を終了する。

フロー名称	説明	作業トリガー
ICカード発行等申請書	「ICカード発行等申請書」の起票に係る、 ICカードの新規払出・再発行・返却フローを示す	課室等担当者からの申請依頼



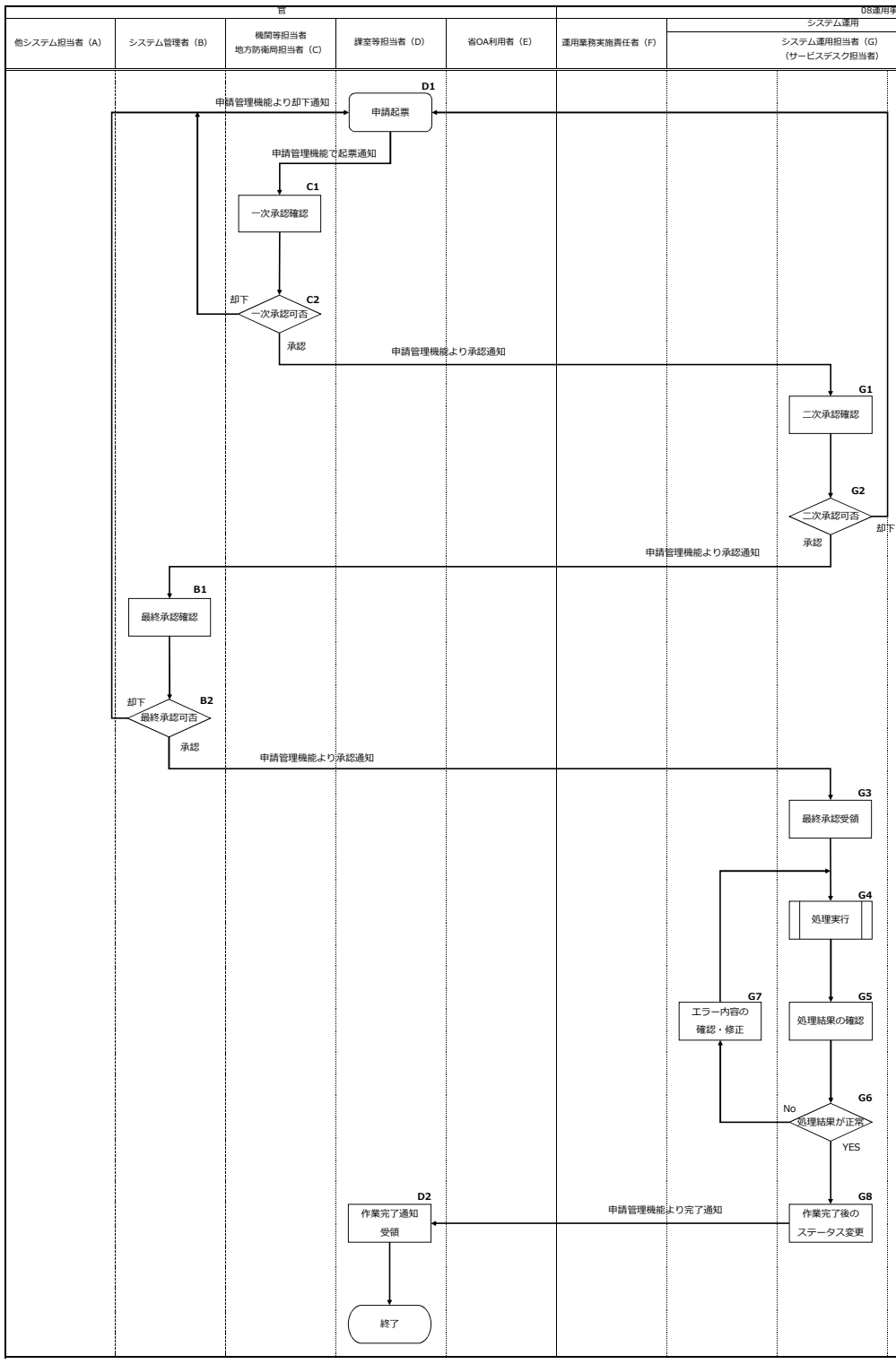
項番	説明
B1	システム管理者は、システム運用担当者からICカードの補充依頼を受領する。
B2	システム管理者は、「ICカード発行等申請書」の内容を確認し、申請内容に関する処理の実施可否の最終判断を行う。
B3	システム管理者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C1	機関等担当者、地方防衛局担当者は、起票された「ICカード発行等申請書」の内容を確認し、その妥当性や、申請内容に不備が無いか確認を行う。
C2	機関等担当者、地方防衛局担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
D1	課室等担当者は、ICカードを新規払出・再発行・返却したい場合に申請管理機能を用いて「ICカード発行等申請書」として起票する。
D2	課室等担当者は、ICカード受け渡しの日時を決定する。
D3	課室等担当者は、ICカード受け渡しのためサービスデスクを訪問する。
D4	課室等担当者は、「ICカード発行等申請書」の申請処理がすべて完了した旨を、申請管理機能上で確認する。
G1	システム運用担当者は、申請管理機能で提出された申請内容を確認する。 申請に当たって必要事項の欠落や誤った記載がないか確認する。 ・申請種別を確認する ・ICカードと紐づけをする、または解除する共有アカウントが記載されているかを確認する ・実施希望日を確認する
G2	システム運用担当者は、申請書の不備の有無の確認結果、不備があった場合はその個所の指摘と共にに申請者に戻す。
G3	システム運用担当者は、申請種別を確認する。
G4	システム運用担当者は、ICカードの払出・再発行の場合、払出枚数を確認する。
G5	システム運用担当者は、ICカードの残量を確認する。
G6	システム運用担当者は、Iカードの残量が全体の30%未満となっていた場合にはシステム管理者に補充依頼をする。
G7	システム運用担当者は、ここまでの一連のやり取りを踏まえ、申請内容を受理するか判断を行う。
G8	システム運用担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。 ・却下する場合は、却下理由と共に申請者に戻す。 ・承認する場合は、システム管理者に申請管理機能により申請内容の最終判断の依頼を行う。
G9	システム運用担当者は、システム管理者からの申請内容に関する最終承認を受け、申請内容の処理に入る。
G10	システム運用担当者は、申請種別を確認する。
G11	システム運用担当者は、再発行の場合は以前のICカードと共有アカウントの紐づけを解除する。
G12	システム運用担当者は、ICカードの受け渡し日時を調整する。
G13	システム運用担当者は、ICカードの受け渡しを行う。
G14	システム運用担当者は、払出又は返却によって後続作業を実施する。
G15	システム運用担当者は、返却されたICカードの共有アカウントとの紐づけを解除する。
G16	システム運用担当者は、払出・返却等により変動した在庫数を物品管理システムに登録する。
G16	システム運用担当者は、申請管理機能の本申請に係るステータスを完了にし、運用対応を終了する。

フロー名称	説明	作業トリガー
Teamsチーム用Sharepoint領域拡張申請書	「Teamsチーム用Sharepoint領域拡張申請書」の起票に係る、 Teamsのチームに紐づくCopilot学習用SharePoint領域を拡張に係るフローを示す	・各サイトのストレージ使用率が90%に達して、 管理者ユーザにメールが送付されたタイミング ・SharePoint管理者ユーザが管理センターから使用率を確認して、 領域拡張と判断した場合



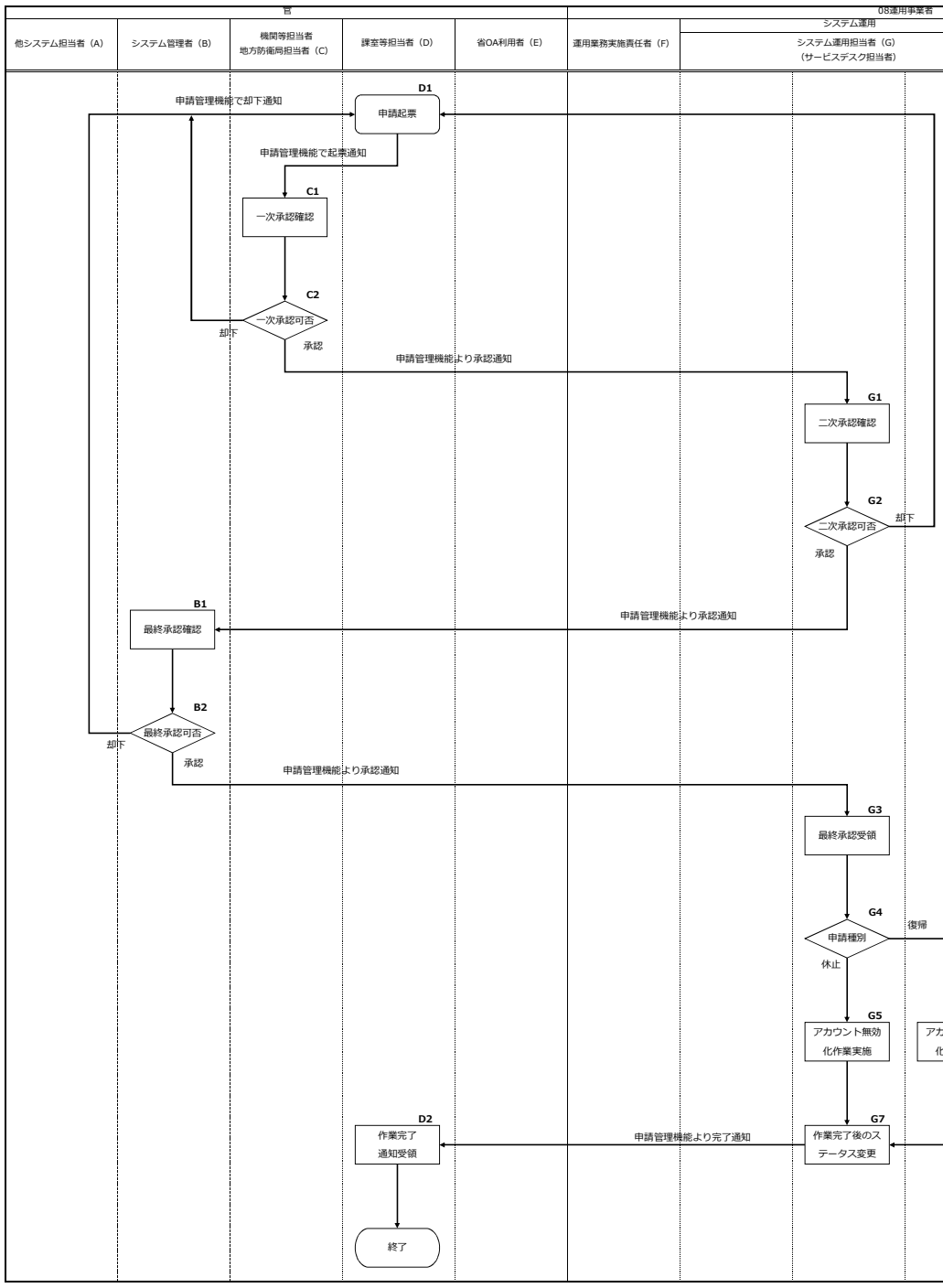
項番	説明
B1	システム管理者は、「Teamsチーム用Sharepoint領域拡張申請書」の内容を確認し、申請内容に関する処理の実施可否の最終判断を行う。
B2	システム管理者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C1	機関等担当者、地方防衛局担当者は、起票された「Teamsチーム用Sharepoint領域拡張申請書」の内容を確認し、その妥当性や、申請内容に不備が無いか確認を行う。
C2	機関等担当者、地方防衛局担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
D1	課室等担当者は、申請管理機能で「Teamsチーム用Sharepoint領域拡張申請書」に係る申請を、申請管理機能を用いて起票する。
D2	課室等担当者は、「Teamsチーム用Sharepoint領域拡張申請書」の申請処理がすべて完了した旨を、申請管理機能上で確認する。
G1	システム運用担当者は、二次承認確認を行う。 ・チーム種別 ・機関等｜局／部｜課｜室／班／係等 ・個別申請チーム名 ・実施希望日
G2	システム運用担当者は、申請書の不備の有無の確認結果、不備があった場合はその個所の指摘と共に申請者に戻す。
G3	システム運用担当者は、最終承認を受領する。
G4	システム運用担当者は、「(仮)Teamsのチームに紐づくCopilot学習用SharePoint領域拡張手順書」に基いて作業を実施する。
G5	システム運用担当者は、「完了」への処理状態の変更操作を行う。

フロー名称	説明	作業トリガー
S/MIME証明書発行等申請書	「S/MIME証明書発行等申請書」の起票に伴う、 S/MIME証明書発行・失効のフローを示す。	・省OA課室担当者からの申請依頼



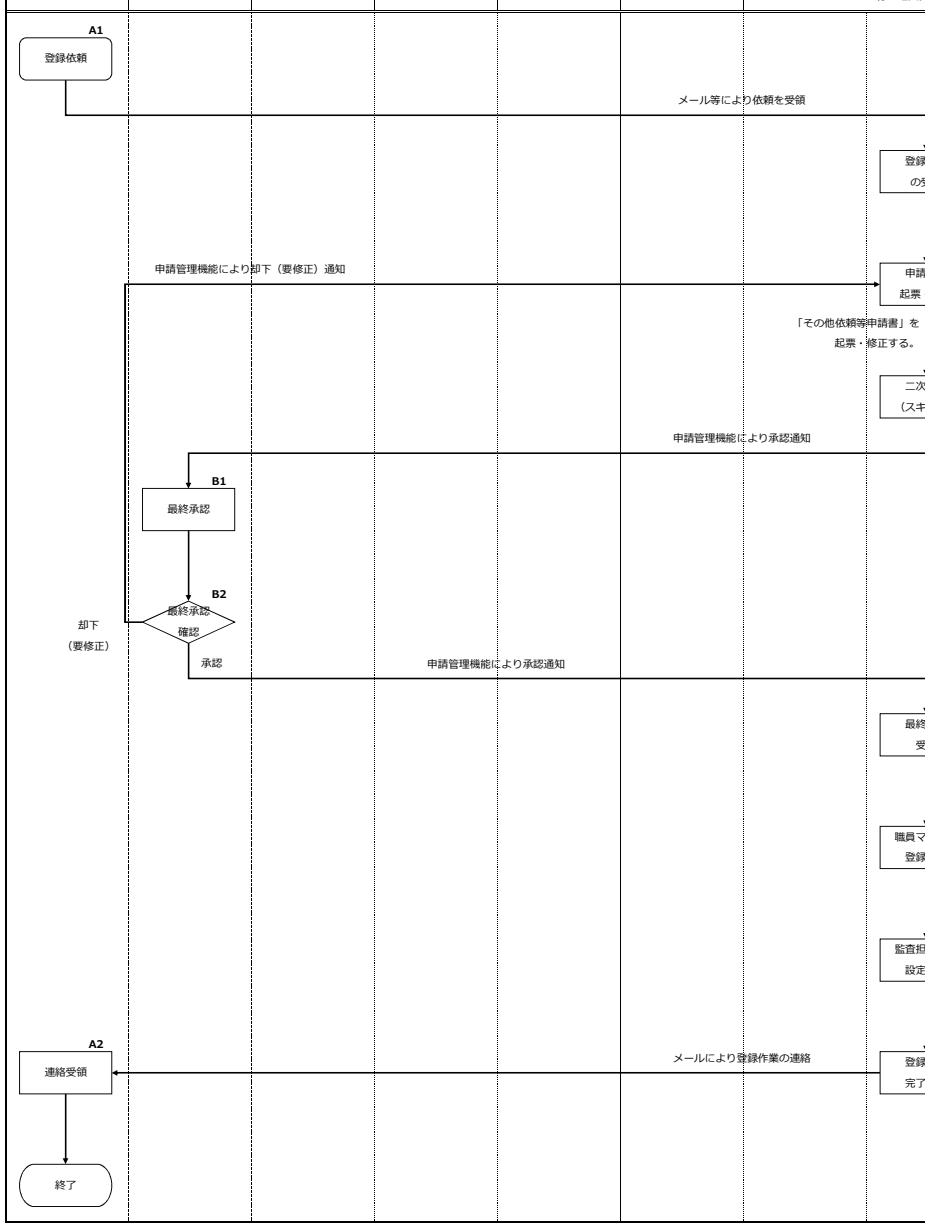
項番	説明
B1	システム管理者は、最終承認確認を行う。
B2	システム管理者は、申請書の内容に基づき、最終承認可否の判断を行う。
C1	機関等担当者、地方防衛局担当者は、一次承認確認を行う。
C2	機関等担当者、地方防衛局担当者は、申請書の内容に基づき、一次承認可否の判断を行う。
D1	課室等担当者は、申請管理機能で申請を起票する。
D2	課室等担当者は、作業完了報告を受領する。
G1	システム運用担当者は、二次承認確認を行う。 入力された各項目内容の妥当性を確認する。
G2	システム運用担当者は、申請の項目に基づき、最終承認可否の判断を行う。
G3	システム運用担当者は、最終承認を受領する。
G4	申請管理機能より、「他機能連携」による自動処理が行われる。 ・連携用CSVにS/MIME証明書を発行用のレコードを追加 ・S/MIME証明書発行連携
G5	システム運用担当者は、処理結果のステータス確認を行う。
G6	システム運用担当者は、自動処理の「成功」、「失敗」の判断を行う。 ・「YES」の場合は、「作業完了後のステータス変更」へ ・「NO」の場合は、「エラー内容の確認・修正」へ
G7	システム運用担当者は、エラー内容の確認・修正作業を行う。
G8	システム運用担当者は、申請管理機能のステータスを完了にする。

フロー名称	説明	作業トリガー
個人アカウント利用休止・復帰申請書	「個人アカウント利用休止・復帰申請書」の起票に係る、 育休や休職などにより、長期間本システムを利用しない個人アカウントを無効化するために係るフローを示す	省OA課室担当者からの申請依頼があった時



項番	説明
B1	システム管理者は、「個人アカウント利用休止・復帰申請書」の内容を確認し、申請内容に関する処理の実施可否の最終判断を行う。
B2	システム管理者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
C1	機関等担当者、地方防衛局担当者は、起票された「個人アカウント利用休止・復帰申請書」の内容を確認し、その妥当性や、申請内容に不備が無いか確認を行う。
C2	機関等担当者、地方防衛局担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。却下する場合は、却下理由と共に申請者に戻す。
D1	課室等担当者は、申請管理機能を用いて「個人アカウント利用休止・復帰申請書」として起票する。
D2	課室等担当者は、「個人アカウント利用休止・復帰申請書」の申請処理がすべて完了した旨を、申請管理機能上で確認する。
D3	課室等担当者は、休止アカウントの有効化作業完了の連絡をシステム運用担当者より受領する。
G1	システム運用担当者は、二次承認確認を行う。 ・申請種別：適切な内容が選択されているか ・適用希望日：5営業日以降の日程が記載されているか
G2	システム運用担当者は、確認結果を基に、申請内容を「承認」するか、「却下」するか判断する。 ・却下する場合は、却下理由と共に申請者に戻す。 ・承認する場合は、システム管理者に申請管理機能により申請内容の最終判断の依頼を行う。
G3	システム運用担当者は、システム管理者からの申請内容に関する最終承認を受け、申請内容の処理に入る。
G4	システム運用担当者は、申請種別に応じた対応が分岐する。 ・休止：アカウント無効化 ・復帰：アカウント有効化
G5	システム運用担当者は、所定の手順書を参照し、個人アカウント無効化作業を実施する。
G6	システム運用担当者は、所定の手順書を参照し、個人アカウント有効化作業を実施する。
G7	システム運用担当者は、申請管理機能の本申請に係るステータスを完了にし、運用対応を終了する。

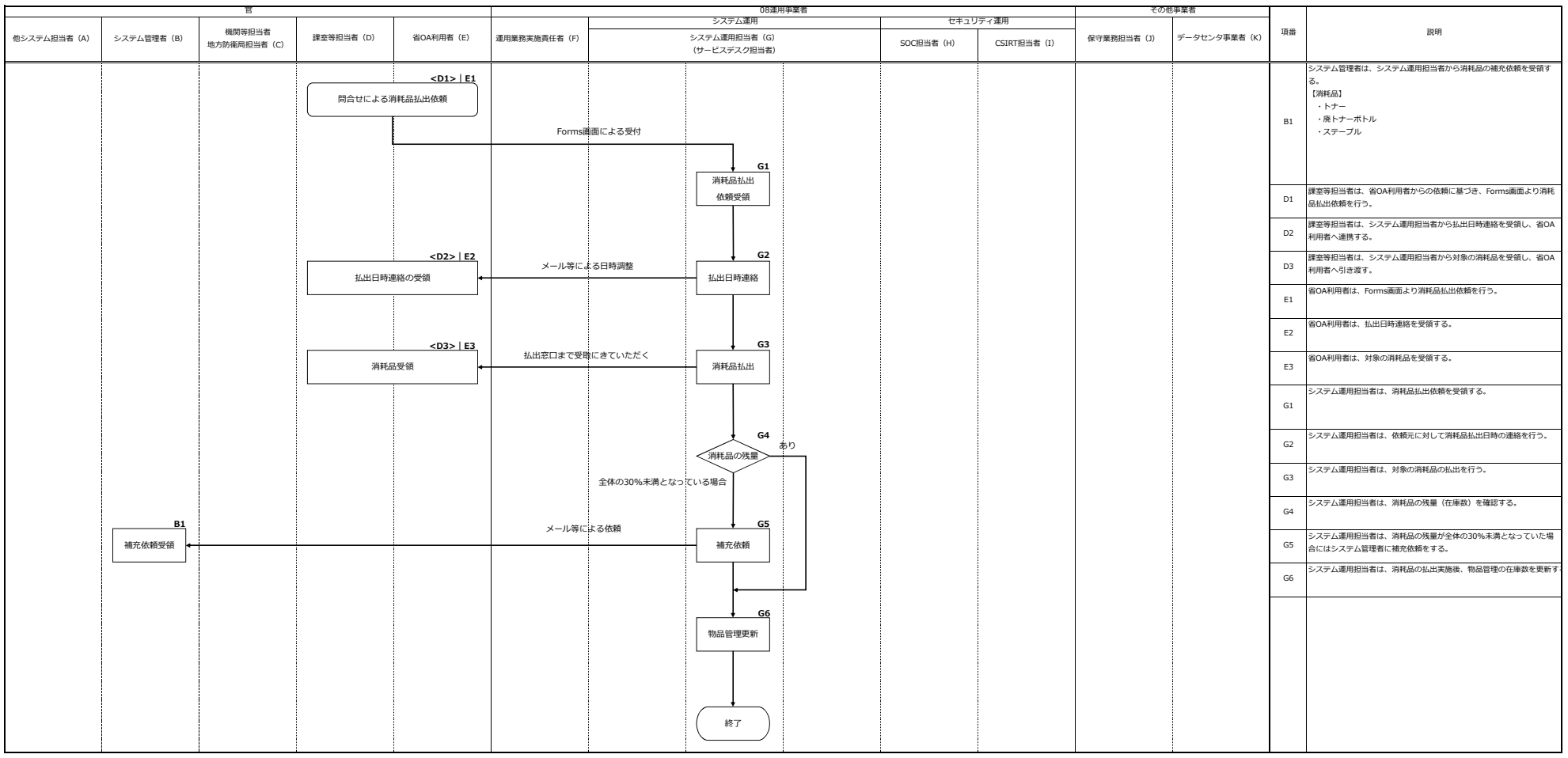
フロー名称	説明	作業トリガー
監査担当者登録等依頼	省OA利用者が「メール送信、Web閲覧、ファイルアップロード」を行う際、 監査機能により危険度が高いと判断されたアクションは、承認者による目視監査の対象となる。 この承認者を追加設定する依頼があった際に、本フローに沿って運用対応を行う。	省OA課室担当者からの登録依頼があった場合に実施する。



項番	説明
A1	以下に示す監査機能の承認部署は、メール等により「監査機能の承認者の追加登録」をシステム運用担当者に依頼する。 ・陸・海・空・統・（情本）の監査部隊 ・統幕及びその他機関における監査担当部署
A2	以下に示す監査機能の承認部署は、本申請に係る登録処理が完了した旨の連絡を受領する。 ・陸・海・空・統・（情本）の監査部隊 ・統幕及びその他機関における監査担当部署
B1	システム管理者は、代理申請された「その他依頼等申請書（内容：監査機能の承認者の追加登録）」を申請管理機能で受領し、最終承認判断を行う。
B2	システム管理者は、申請内容の確認を行い、「承認」、「却下」の判断を行う。 「却下」の場合は、その理由と共に通知を行う。
G1	システム運用担当者は、監査部署の担当者より「監査機能の承認者の追加登録」依頼を受領する。
G2	システム運用担当者は、受領した依頼内容を基に、申請管理機能の「その他依頼等申請書」を起票する。また、内容の修正が必要な場合は、その対応を行う。
G3	本件は代理申請をしているため、承認処理はスキップとなる。
G4	システム運用担当者は、システム管理者からの申請内容に関する「最終承認」を受け、申請内容の処理に入る。
G5	システム運用担当者は、申請内容に基づき「職員マスタへの情報登録」を実施する。
G6	システム運用担当者は、申請内容に基づき「監査担当者の設定」を実施する。
G7	システム運用担当者は、申請に基づく登録作業が終了した旨をメールにより申請元の監査部門の担当者に連絡する。

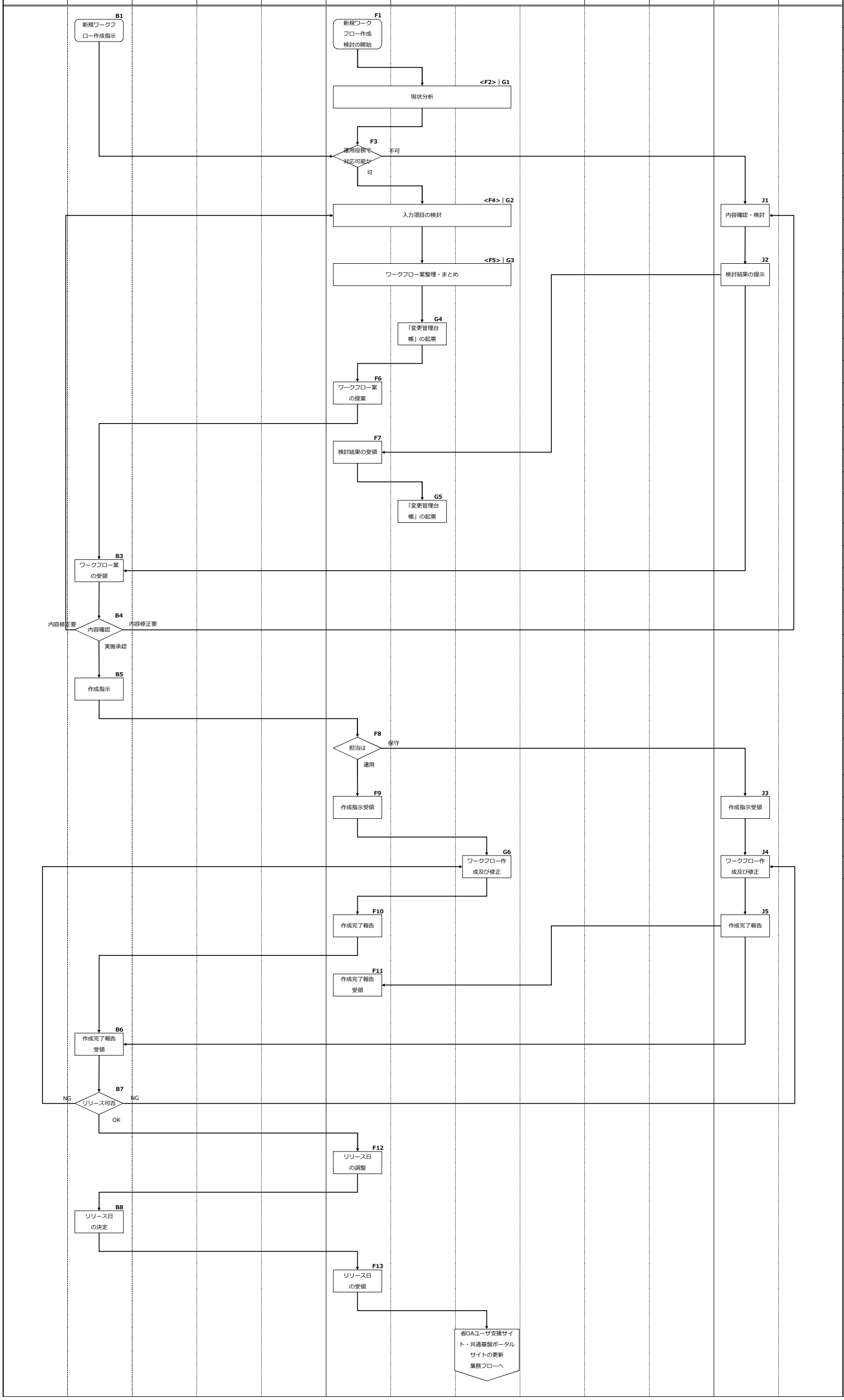
付表９　業務フロー（続き）
トナー等消耗品払出依頼（続き）

フロー名称	説明	作業トリガー
トナー等消耗品払出依頼	各種消耗品（プリンターに関連するもの）等の払出依頼での在庫数確認・報告を行うフローを示す。	・消耗品（プリンターに関連するもの）の払出依頼が発生した時



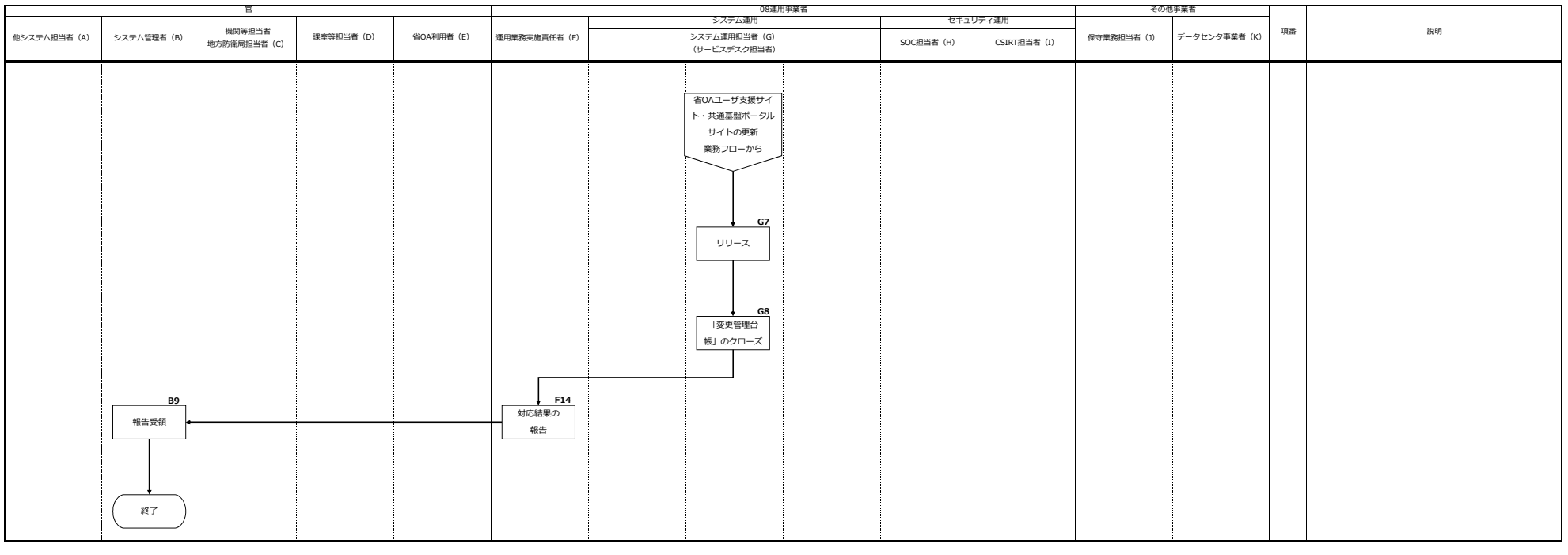
項番	説明
B1	システム管理者は、システム運用担当者から消耗品の補充依頼を受領する。 【消耗品】 ・トナー ・廃トナーボトル ・ステープル
D1	課室等担当者は、省OA利用者からの依頼に基づき、Forms画面より消耗品払出依頼を行う。
D2	課室等担当者は、システム運用担当者から払出日時連絡を受領し、省OA利用者へ連携する。
D3	課室等担当者は、システム運用担当者から対象の消耗品を受領し、省OA利用者へ引き渡す。
E1	省OA利用者は、Forms画面より消耗品払出依頼を行う。
E2	省OA利用者は、払出日時連絡を受領する。
E3	省OA利用者は、対象の消耗品を受領する。
G1	システム運用担当者は、消耗品払出依頼を受領する。
G2	システム運用担当者は、依頼元に対して消耗品払出日時の連絡を行う。
G3	システム運用担当者は、対象の消耗品の払出を行う。
G4	システム運用担当者は、消耗品の残量（在庫数）を確認する。
G5	システム運用担当者は、消耗品の残量が全体の30%未満となっていた場合にはシステム管理者に補充依頼をする。
G6	システム運用担当者は、消耗品の払出実施後、物品管理の在庫数を更新す

フロー名称	説明	作業トリガー
申請ワークフロー新規作成	利用者の問合せ状況・件数やシステム管理者からの指示に基づき、 利用者利便性向上や運用業務効率化のため、専用の申請ワークフローを新たに作成する。	・定期的に省OA利用者からの問合せ状況等を鑑み、新規申請ワークフロー化の検討を行う（年2回程度を想定） ・システム管理者から新規ワークフロー作成の追加指示を受けた際に検討を行う（随時）

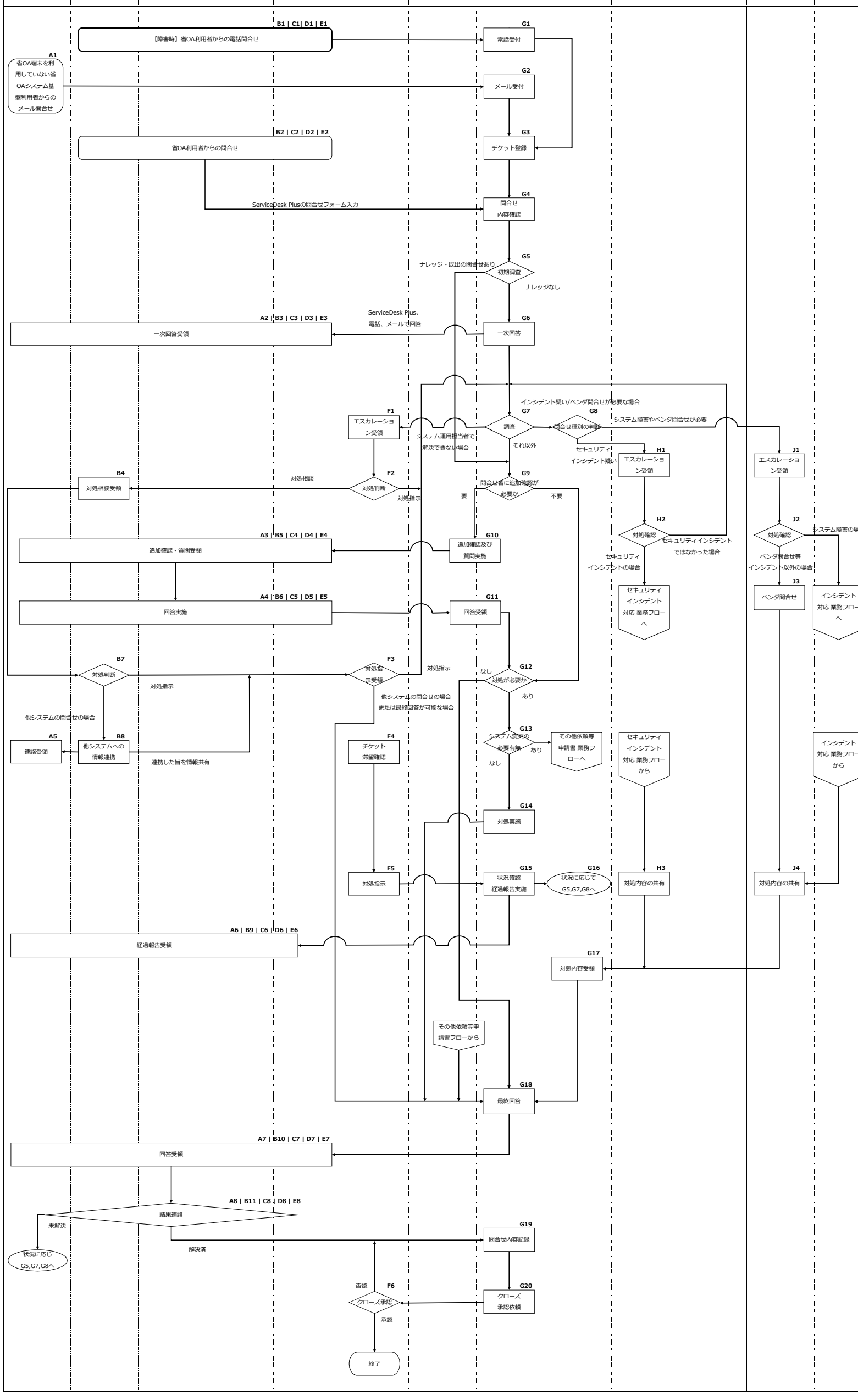


項番	説明
B1	システム管理者は、必要に応じて新規申請ワークフロー作成検討を、運用業務実施責任者及びシステム運用担当者に対して指示する。
B2	システム管理者は、運用業務実施責任者から新規申請ワークフロー作成不可の連絡を受領する。
B3	システム管理者は、運用業務実施責任者または保守業務担当者から「ワークフロー案」の提案を受領する。
B4	システム管理者は、「ワークフロー案」の内容を確認し問題がないかを判断する。内容の修正を要すると判断した場合は、その旨を運用業務実施責任者及びシステム運用担当者に指示する。
B5	システム管理者は、提案された「ワークフロー案」に問題が無いと判断した場合は、運用業務実施責任者または保守業務担当者へ新規申請ワークフロー作成を指示する。
B6	システム管理者は、運用業務実施責任者または保守業務担当者から「新規申請ワークフローの作成を完了した」旨の報告を受領する。
B7	システム管理者は、新たに作成された申請ワークフローを確認し、利用者向けにリリースして問題がないかを判断する。
B8	システム管理者は、運用業務実施責任者と協議し、新規申請ワークフローのリリース日を決定する。
B9	システム管理者は、運用業務実施責任者から本件の対応内容について報告を受ける。
F1	運用業務実施責任者は、定期的（年2回）に省OA利用者からの問合せ状況等を鑑み、システム運用担当者に対して新規申請ワークフロー作成のための検討を開始する指示を出す。
F2	運用業務実施責任者は、主体となってシステム運用担当者と共に問合せ状況等現状の分析を行い、新規申請ワークフロー作成の要否を検討する。
F3	運用業務実施責任者は、予め準備された予備ワークフローを使用して、新規申請ワークフローが作成可能かどうかを判断する。
F4	運用業務実施責任者は、主体となってシステム運用担当者と共に新規申請ワークフローの実現案（処理フローや必要な入力項目等）の検討を行う。
F5	運用業務実施責任者は、主体となってシステム運用担当者と共に検討結果を基に申請ワークフロー新規作成案を整理し、提案資料にまとめる。
F6	運用業務実施責任者は、申請ワークフロー新規作成に係る検討結果を取りまとめ、案としてシステム管理者に提示する。
F7	運用業務実施責任者は、保守業務担当者から新規申請ワークフロー作成に関する検討結果を受領する。
F8	新規申請ワークフローの作成担当はシステム運用担当者か保守業務担当者かを判断する。
F9	運用業務実施責任者は、システム管理者より新規申請ワークフロー作成の指示を受領する。
F10	運用業務実施責任者は、システム管理者に対して新規申請ワークフロー作成完了の報告を行う。
F11	運用業務実施責任者は、保守業務担当者から「新規申請ワークフローの作成を完了した」旨の報告を受領する。
F12	運用業務実施責任者は、システム管理者と協議し、新規申請ワークフローのリリース日を調整する。
F13	運用業務実施責任者は、システム管理者から新規申請ワークフローのリリース日を受領する。新規申請ワークフローのリリースについて省OA利用者向けにユーザ支援サイトへ情報掲載を行う。
F14	運用業務実施責任者は、申請ワークフロー新規作成に係る対応結果を取りまとめ、システム管理者に報告する。
G1	システム運用担当者は、運用業務実施責任者と共に問合せ状況等現状の分析を行い、新規申請ワークフロー作成の要否を検討する。
G2	システム運用担当者は、運用業務実施責任者と共に新規申請ワークフローの実現案（処理フローや必要な入力項目等）の検討を行う。
G3	システム運用担当者は、運用業務実施責任者と共に検討結果を基に申請ワークフロー新規作成案を整理し、提案資料にまとめる。
G4	新規申請ワークフローを作成することが決まったら、システム運用担当者は「変更管理台帳」を起票し、作成に係る諸対応の記録を行う。
G5	システム運用担当者は、保守業務担当者から新規申請ワークフロー案を受領した後、「変更管理台帳」を起票し、作成に係る諸対応の記録を行う。
G6	システム運用担当者は、申請ワークフローの新規作成を行い、動作確認を実施する。 また、システム管理者のリリース判断でNGとなった場合、新規申請ワークフローの修正を行う。
G7	システム運用担当者は、ユーザ支援サイト掲載により省OA利用者向けに周知した後、新規申請ワークフローを省OA利用者向けにリリースする。
G8	システム運用担当者は「変更管理台帳」に対応経緯を記録し、クローズ処理を行う。
J1	保守業務担当者は、申請ワークフロー新規作成に関する内容等を確認し、新規申請ワークフローの実現案（処理フローや必要な入力項目等）の検討を行う。検討にあたっては、システム管理者、08運用事業者と適宜相談・調整を行う。
J2	保守業務担当者は、申請ワークフロー新規作成に係る検討結果を取りまとめ、システム管理者および運用業務実施責任者に提示する。
J3	運用業務担当者は、システム管理者より新規申請ワークフロー作成の指示を受領する。
J4	保守業務担当者は、申請ワークフローの新規作成を行い、動作確認を実施する。 また、システム管理者のリリース判断でNGとなった場合、新規申請ワークフローの修正を行う。
J5	保守業務担当者は、システム管理者および運用業務実施責任者に対して新規申請ワークフロー作成完了の報告を行う。

フロー名称	説明	作業トリガー
申請ワークフロー新規作成	利用者の問合せ状況・件数やシステム管理者からの指示に基づき、 利用者利便性向上や運用業務効率化のため、専用の申請ワークフローを新たに作成する。	・定期的に省OA利用者からの問合せ状況等を鑑み、新規申請ワークフロー化の検討を行う（年2回程度を想定） ・システム管理者から新規ワークフロー作成の追加指示を受けた際に検討を行う（随時）



フロー名称	説明	作業トリガー
問合せ対応	省OA利用者からの問合せがあった際の対処フローを示す	省OA利用者等からの問合せ



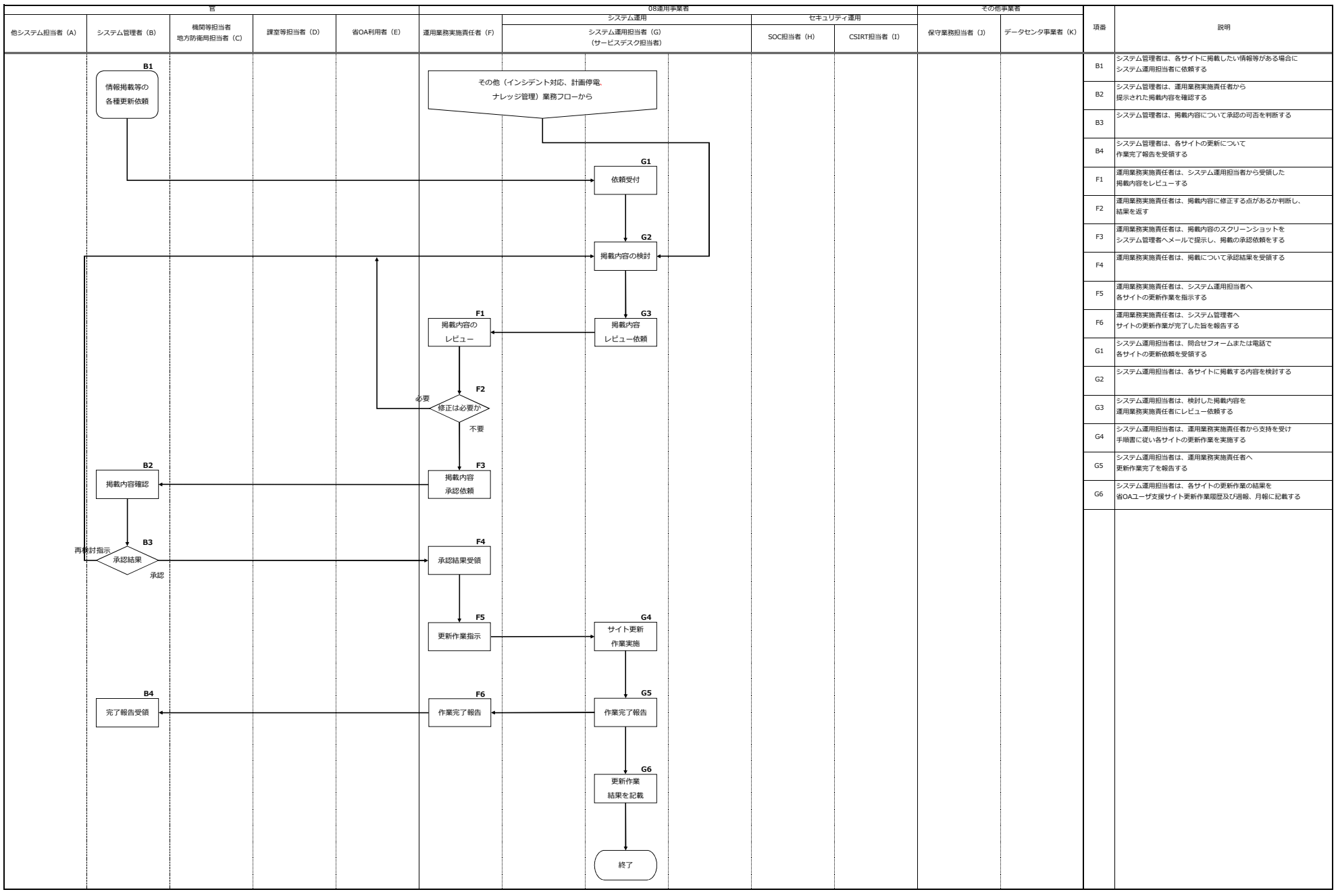
項番	説明
A1	省OA端末を利用していない省OAシステム基盤利用者は、ServiceDesk Plusの問合せフォームが利用できないためメールで問合せを実施する。 平時はメールでの受付けとし、メールが利用出来ない場合には電話で問合せを実施する。
A2	省OA端末を利用していない省OAシステム基盤利用者は、システム運用担当者から対処期限と初期調査結果を受領する。
A3	省OA端末を利用していない省OAシステム基盤利用者は、システム運用担当者から問合せに関する追加の確認依頼や質問を受領する。
A4	省OA端末を利用していない省OAシステム基盤利用者は、システム運用担当者に回答を実施する。
A5	省OA端末を利用していない省OAシステム基盤利用者は、他システムの問合せだった場合、システム担当者からの問合せの情報連携を受領する。
A6	省OA端末を利用していない省OAシステム基盤利用者は、システム運用担当者から途中経過報告を受領する。
A7	省OA端末を利用していない省OAシステム基盤利用者は、システム運用担当者から回答を受領する。
A8	省OA端末を利用していない省OAシステム基盤利用者は、回答内容を確認し、問合せが解決したかどうかをサービスデスクに回答する。
B1	システム管理者は、問合せフォームの障害、端末故障により問合せフォームが物理的に使用できない場合、システム運用担当者に電話で問合せを実施する。
B2	システム管理者は、ServiceDesk Plusの問合せフォームの該当カテゴリから問合せ内容を入力しチケットを登録する。
B3	システム管理者は、システム運用担当者から対処期限と初期調査結果を受領する。
B4	システム管理者は、運用業務実施責任者からの対処相談を受領する。
B5	システム管理者は、システム運用担当者から問合せに関する追加の確認依頼や質問を受領する。
B6	システム管理者は、システム運用担当者に回答を実施する。
B7	システム管理者は、受領した対処相談について運用業務実施責任者に対処指示をする。他システムの問合せだった場合はシステム担当者から他システム担当者に情報連携する。
B8	システム管理者は、他システム担当者へ問合せの情報連携をする。 運用業務実施責任者には他システム担当者へ連絡したことを情報共有する。
B9	システム管理者は、システム運用担当者から途中経過報告を受領する。
B10	システム管理者は、システム運用担当者から回答を受領する。
B11	システム管理者は、回答内容を確認し、問合せが解決したかどうかをサービスデスクに回答する。
C1	機関等担当者、地方防衛局担当者は、問合せフォームの障害、端末故障により問合せフォームが物理的に使用できない場合、システム運用担当者に電話で問合せを実施する。
C2	機関等担当者、地方防衛局担当者は、ServiceDesk Plusの問合せフォームの該当カテゴリから問合せ内容を入力しチケットを登録する。
C3	機関等担当者、地方防衛局担当者は、システム運用担当者から対処期限と初期調査結果を受領する。
C4	機関等担当者、地方防衛局担当者は、システム運用担当者から問合せに関する追加の確認依頼や質問を受領する。
C5	機関等担当者、地方防衛局担当者は、システム運用担当者に回答を実施する。
C6	機関等担当者、地方防衛局担当者は、システム運用担当者から途中経過報告を受領する。
C7	機関等担当者、地方防衛局担当者は、システム運用担当者から回答を受領する。
C8	機関等担当者、地方防衛局担当者は、回答内容を確認し、問合せが解決したかどうかをサービスデスクに回答する。
D1	課室等担当者は、問合せフォームの障害、端末故障により問合せフォームが物理的に使用できない場合、システム運用担当者に電話で問合せを実施する。
D2	課室等担当者は、ServiceDesk Plusの問合せフォームの該当カテゴリから問合せ内容を入力しチケットを登録する。
D3	課室等担当者は、システム運用担当者から対処期限と初期調査結果を受領する。
D4	課室等担当者は、システム運用担当者から問合せに関する追加の確認依頼や質問を受領する。
D5	課室等担当者は、システム運用担当者に回答を実施する。
D6	課室等担当者は、システム運用担当者から途中経過報告を受領する。
D7	課室等担当者は、システム運用担当者から回答を受領する。
D8	課室等担当者は、回答内容を確認し、問合せが解決したかどうかをサービスデスクに回答する。
E1	省OA利用者は、省OA利用者は、問合せフォームの障害、端末故障により問合せフォームが物理的に使用できない場合、システム運用担当者に電話で問合せを実施する。
E2	省OA利用者は、ServiceDesk Plusの問合せフォームの該当カテゴリから問合せ内容を入力しチケットを登録する。
E3	省OA利用者は、システム運用担当者から対処期限と初期調査結果を受領する。
E4	省OA利用者は、システム運用担当者から問合せに関する追加の確認依頼や質問を受領する。
E5	省OA利用者は、システム運用担当者に回答を実施する。
E6	省OA利用者は、システム運用担当者から途中経過報告を受領する。
E7	省OA利用者は、システム運用担当者から回答を受領する。
E8	省OA利用者は、回答内容を確認し、問合せが解決したかどうかをサービスデスクに回答する。
F1	運用業務実施責任者は、システム運用担当者からのエスカレーションを受領する。 他システムの問合せだった場合は他システム担当者に情報連携をする。
F2	運用業務実施責任者は、サービスデスクに追加調査等の対処を指示する。 他システム問合せの場合や、内容によってシステム管理者に対処相談や確認を実施する。
F3	運用業務実施責任者は、システム管理者から対処相談した結果を受領し、システム運用担当者に対処指示をする。他システムの問合せだった場合、または最終回答が可能な場合は申告者にその旨回答するようシステム運用担当者に指示をする。
F4	運用業務実施責任者は、滞留しているチケットの通知が来ている場合は内容を確認する。 (5営業日滞留で通知)
F5	運用業務実施責任者は、滞留しているチケットについて、担当者もしくは別担当者に問合せ者に状況等を回答するよう指示をする。
F6	運用業務実施責任者は、システム運用担当者からクローズ承認依頼を受領しチケット内容を確認し 内容に問題がない場合は承認する。 チケット内容に不備や不明な点がある場合はサービスデスクに確認する。
G1	システム運用担当者は、電話で問合せ内容を受け付ける。 障害等緊急を要する、またはServiceDesk Plusが利用出来ない場合のみ電話受付可とする。
G2	システム運用担当者は、メールまたは電話で問合せ内容を受け付ける。
G3	システム運用担当者は、電話でヒアリングした内容をServiceDesk Plusでチケット登録する。
G4	システム運用担当者は、問合せ内容を確認し、確認したシステム運用担当者はServiceDesk Plusで担当者の登録をする。
G5	システム運用担当者は、過去の問合せやナレッジを確認など初期調査を実施する。

付表１０　業務フロー（続き）
問合せ対応（続き）

フロー名称	説明	作業トリガー
問合せ対応	省OA利用者からの問合せがあった際の対処フローを示す	省OA利用者等からの問合せ

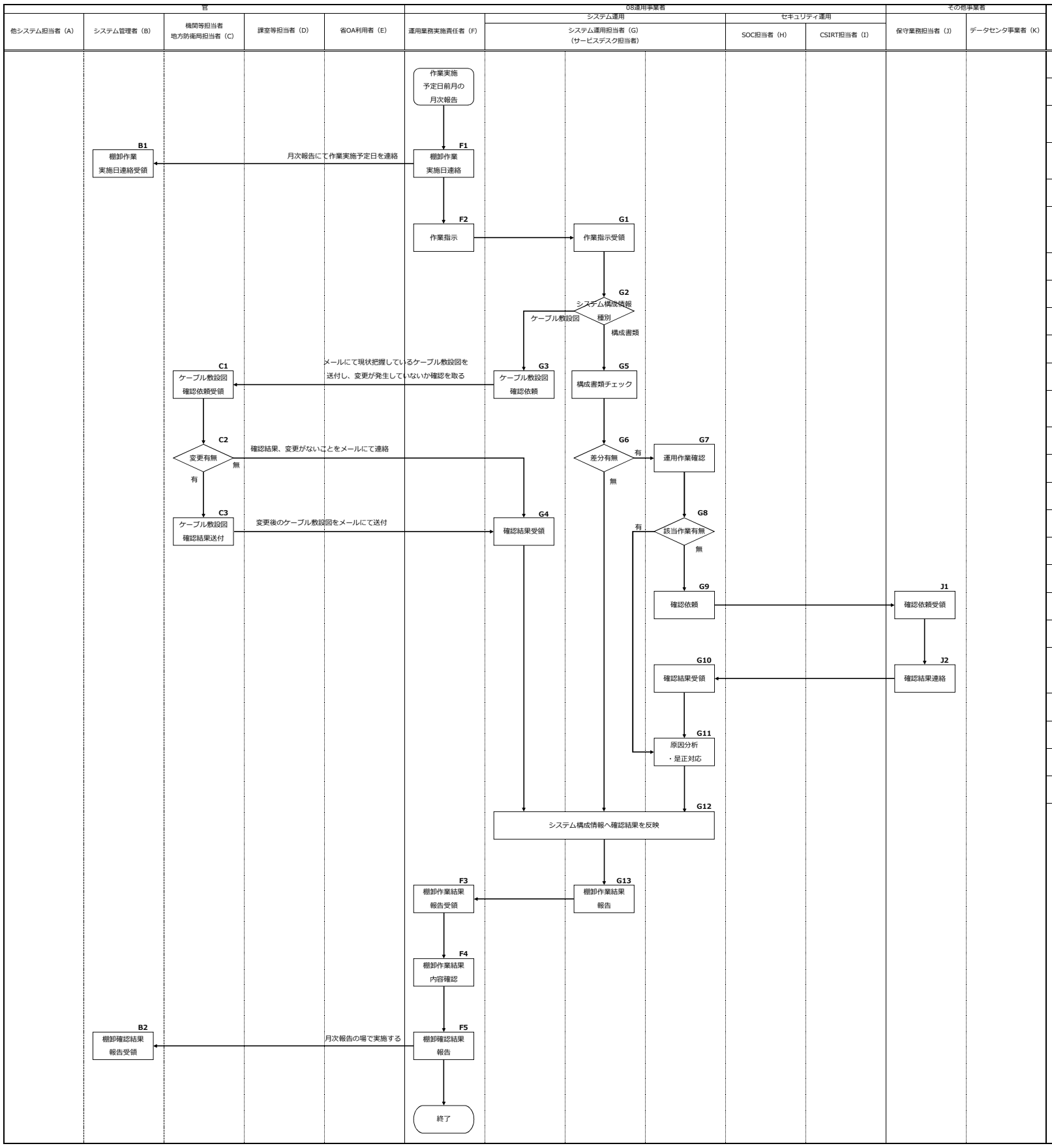
官					08運用事業者						その他事業者		項番	説明
						システム運用			セキュリティ運用					
他システム担当者（A）	システム管理者（B）	機関等担当者 地方防衛局担当者（C）	課室等担当者（D）	省OA利用者（E）	運用業務実施責任者（F）	システム運用担当者（G） （サービスデスク担当者）			SOC担当者（H）	CSIRT担当者（I）	保守業務担当者（J）	データセンタ事業者（K）		
													G6	システム運用担当者は、初期調査を実施し回答までに時間を要すると判断した場合は対処期限と初期調査結果をServiceDesk Plusで回答する。 電話での問合せや緊急の場合は電話で回答する。 メールで受領した場合はメールで回答する。
													G7	システム運用担当者は、セキュリティインシデントやシステム障害の発生有無など技術的な観点も含めた調査を実施する。 調査の結果、インシデント疑いの場合やベンダ問合せが必要な場合やシステム運用担当者で解決できない場合、各担当者にエスカレーション実施する。
													G8	システム運用担当者は、インシデントがセキュリティインシデントかシステム障害なのか、またはインシデントではなくベンダに問合せが必要なのかを確認しSOC担当者・保守業務担当者にエスカレーションを実施する。
													G9	システム運用担当者は、調査の結果、問合せ者に追加で確認が必要な情報があるかを確認する。
													G10	システム運用担当者は、追加で確認が必要な情報について問合せ者に質問する。
													G11	システム運用担当者は、問合せ者からの回答を受領する。
													G12	システム運用担当者は、調査した結果、システム運用担当者として対処が必要かどうかを確認する。
													G13	システム運用担当者は、システム変更が必要な場合は「その他依頼等申請書」を起票する。
													G14	システム運用担当者は、調査の結果対処が必要な場合には適宜対処を実施する。
													G15	システム運用担当者は、更新が滞留しているチケットの確認を運用実施責任者から受領した場合、該当チケットの状況について確認し、問合せ者に経過報告を実施する。
													G16	システム運用担当者は、滞留しているチケットについて状況に応じて対処実施する。初期調査や技術的な観点も含めた調査等を実施する。
													G17	システム運用担当者は、SOC担当者、保守業務担当者からインシデント等の対処内容について受領する。
													G18	システム運用担当者は、問合せの申告者にServiceDesk plusで最終回答を実施する。 電話での問合せや緊急の場合は電話で回答する。
													G19	システム運用担当者は、対処した内容をServiceDesk plusに記録する。
													G20	システム運用担当者は、解決済となった問合せのチケットについて、ServiceDesk plusで運用業務実施責任者にクローズ承認依頼する。
													H1	SOC担当者は、システム運用担当者からのエスカレーションを受領する。
													H2	SOC担当者は、問合せ内容に応じて調査や障害対応を実施する。 確認の結果、セキュリティインシデントの場合はセキュリティインシデント対処フローで対処し、セキュリティインシデントではなかった場合はシステム運用担当者にその旨を連絡する。
													H3	SOC担当者は、対処した内容をServiceDesk plusに記録するためシステム運用担当者に共有する。
													J1	保守業務担当者は、システム運用担当者からのエスカレーションを受領する。
													J2	保守業務担当者は、問合せ内容に応じて調査や障害対応等の必要な対処を確認する。 ソフトウェア等のベンダに問合せが必要な場合は問合せを実施する。 システム障害の場合はインシデント対処フローで対処する。
													J3	保守業務担当者は、対処確認の結果、仕様の確認や機能について等ベンダへの問合せが必要な場合は問合せを実施する。
													J4	保守業務担当者は、対処した内容をServiceDesk plusに記録するためシステム運用担当者に共有する。

フロー名称	説明	作業トリガー
省OAユーザ支援サイト・共通基盤ポータルサイトの更新	情報掲載等の各種更新やナレッジの更新依頼、障害情報を基に 省OAユーザ支援サイト及び共通基盤ポータルサイトを更新する業務	情報掲載等の各種更新依頼 ナレッジ情報の更新依頼 障害情報の更新



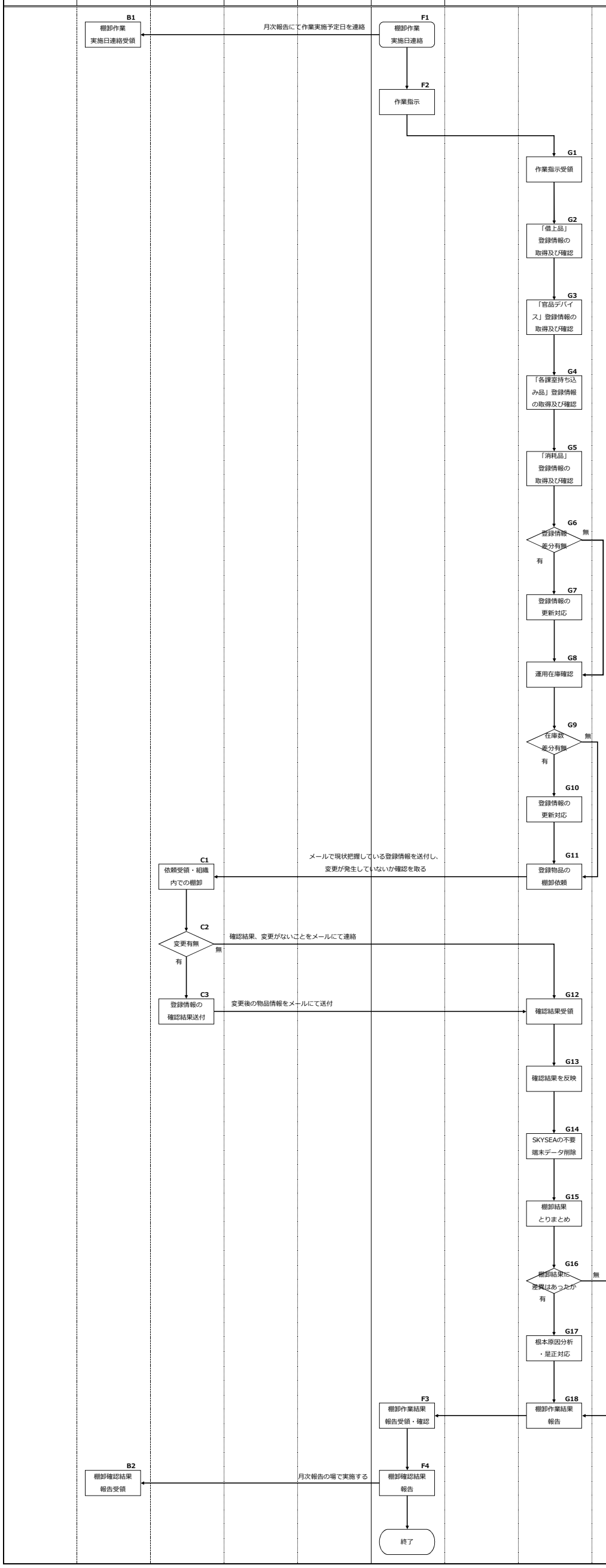
項番	説明
B1	システム管理者は、各サイトに掲載したい情報等がある場合に システム運用担当者に依頼する
B2	システム管理者は、運用業務実施責任者から 提示された掲載内容を確認する
B3	システム管理者は、掲載内容について承認の可否を判断する
B4	システム管理者は、各サイトの更新について 作業完了報告を受領する
F1	運用業務実施責任者は、システム運用担当者から受領した 掲載内容をレビューする
F2	運用業務実施責任者は、掲載内容に修正する点があるか判断し、 結果を返す
F3	運用業務実施責任者は、掲載内容のスクリーンショットを システム管理者へメールで提示し、掲載の承認依頼をする
F4	運用業務実施責任者は、掲載について承認結果を受領する
F5	運用業務実施責任者は、システム運用担当者へ 各サイトの更新作業を指示する
F6	運用業務実施責任者は、システム管理者へ サイトの更新作業が完了した旨を報告する
G1	システム運用担当者は、問合せフォームまたは電話で 各サイトの更新依頼を受領する
G2	システム運用担当者は、各サイトに掲載する内容を検討する
G3	システム運用担当者は、検討した掲載内容を 運用業務実施責任者にレビュー依頼する
G4	システム運用担当者は、運用業務実施責任者から支持を受け 手順書に従い各サイトの更新作業を実施する
G5	システム運用担当者は、運用業務実施責任者へ 更新作業完了を報告する
G6	システム運用担当者は、各サイトの更新作業の結果を 省OAユーザ支援サイト更新作業履歴及び週報、月報に記載する

フロー名称	説明	作業トリガー
システム構成情報の棚卸	システム構成情報の棚卸作業における対応フローを示す。	・定期作業（年間スケジュールにて作業予定を提示）



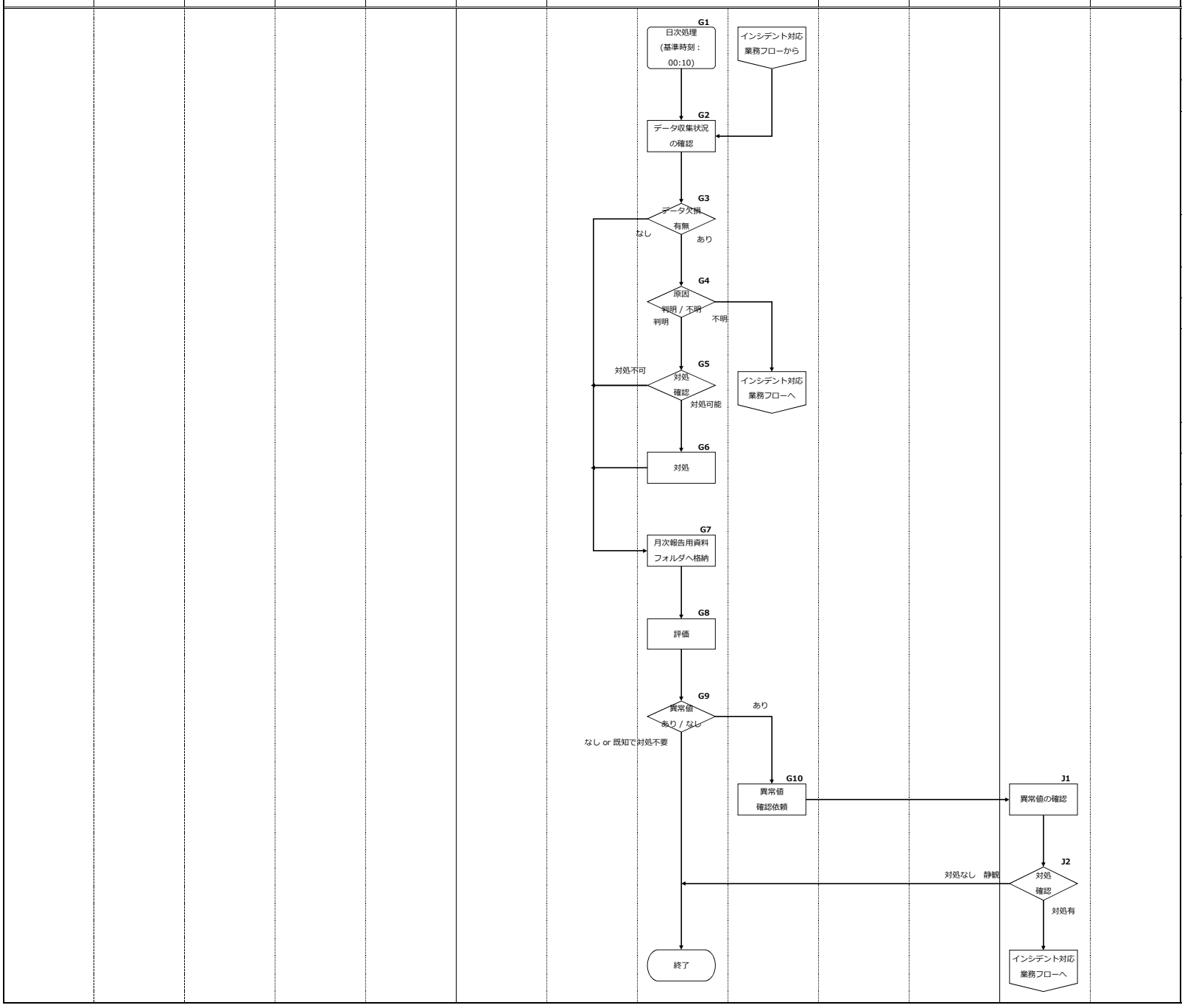
項番	説明
B1	システム管理者は、月次報告にて、運用業務実施責任者より棚卸作業実施日を受領する。
B2	システム管理者は、運用業務実施責任者より棚卸作業結果報告を受領する。
C1	機関等担当者、地方防衛局担当者は、システム運用担当者より、ケーブル敷設図変更有無の確認連絡を受領する。 これを受け、課室等担当者へケーブル敷設図に変更がないか確認する。
C2	機関等担当者、地方防衛局担当者は、変更有無を判断する。変更が無ければ変更がない旨を連絡し、変更が有るのであれば、ケーブル敷設図を更新し送付する。
C3	機関等担当者、地方防衛局担当者は、ケーブル敷設図に変更がある場合、更新したケーブル敷設図を送付する。
F1	運用業務実施責任者は、年間スケジュールで提示した作業実施予定日について、その前月に実施される月次報告において、システム管理者へ棚卸作業実施予定日を連絡する。 ※日程に問題が生じた場合は個別調整
F2	運用業務実施責任者は、システム運用担当者へ、システム管理者と最終合意した作業日を含め、棚卸作業の実施を指示する。
F3	運用業務実施責任者は、システム運用担当者より、棚卸作業結果報告を受領する。
F4	運用業務実施責任者は、棚卸作業結果を確認する。必要に応じ、システム運用担当者へ実施内容について確認を行う。
F5	運用業務実施責任者は、月次報告の場で、システム管理者へ棚卸作業結果を報告する。
G1	システム運用担当者は、運用業務実施責任者より、棚卸作業の作業指示を
G2	システム運用担当者は、システム構成情報の種別により対応が分岐する。
G3	システム運用担当者は、機関等担当者へケーブル敷設図に変更が発生していないか確認連絡を行う。
G4	システム運用担当者は、機関等担当者より、問題ない旨、または更新されたケーブル敷設図を受領する。
G5	システム運用担当者は、構成書類のドキュメントについて、変更管理台帳の更新内容が反映され、差分がないかチェックを実施する。
G6	構成書類のドキュメントと変更管理台帳の整合性チェックの結果、その差分有無で対応が分岐する。
G7	システム運用担当者は、運用が行った変更を伴う作業について変更管理台帳にて確認し、差分の要因がないか確認する。
G8	運用作業の中に差分の原因に該当する作業があったかどうかで対応が分岐する。
G9	システム運用担当者は、確認を取った運用作業以外にシステム構成情報の差分がある場合、保守業務担当者へ確認を依頼する。
G10	システム運用担当者は、保守業務担当者より確認結果を受領する。
G11	システム運用担当者は、差分となった原因を分析し、必要に応じて是正対応を実施する。 保守事業者側に原因があった際は、保守事業者が原因分析および是正対応を行うこととする。
G12	システム運用担当者は、棚卸作業結果として、システム構成情報へ確認結果を反映する。
G13	システム運用担当者は、運用業務実施責任者へ、棚卸作業結果を報告する。
J1	保守業務担当者は、システム運用担当者よりシステム構成情報の差分について確認依頼を受領する。
J2	保守業務担当者は、システム運用担当者へ確認結果を連絡する。

フロー名称	説明	作業トリガー
資産情報の棚卸	運用において時間経過とともに管理情報と実態にずれが生じる可能性があるため、定期的に棚卸をを行い、不整合を解消する活動を実施する。その際の対応フローを示す。	・年1回（年間スケジュールで作業予定をあらかじめ提示）、棚卸作業実施日の前月の月次報告において作業実施日を連絡、合意を以て作業トリガーとする。



項番	説明
B1	システム管理者は運用業務実施責任者より、月次報告の中で棚卸作業実施日の連絡を受ける。
B2	システム管理者は運用業務実施責任者より、月次報告の中で棚卸作業結果の報告を受ける。
C1	機関等担当者/地方防衛局担当者は、システム運用担当者より、貸出物品の棚卸依頼を受ける。 それを受け、課室等担当者へ棚卸の実施を指示する。
C2	機関等担当者/地方防衛局担当者は、棚卸結果を連絡する。当初、システム運用担当者から受領した情報との差異の有無を連絡する。
C3	機関等担当者/地方防衛局担当者は、登録情報に変更がある場合、更新した登録情報を送付する。
F1	運用業務実施責任者は、年間スケジュールで提示した作業実施予定日について、その前月に実施される月次報告において、システム管理者へ棚卸作業予定日を連絡する。 ※日程に問題が生じた場合は個別調整する。
F2	運用業務実施責任者は、システム管理者と最終合意した作業日を含め、システム運用担当者へ棚卸作業の実施を指示する。
F3	運用業務実施責任者はシステム運用担当者より、棚卸作業結果の報告を受け内容を確認する。
F4	運用業務実施責任者は、月次報告の場で、システム管理者へ棚卸作業結果を報告する。
G1	システム運用担当者は、運用業務実施責任者より、棚卸作業の実施指示を受ける。
G2	システム運用担当者は、「物品管理システム」より「借上品」の現状の登録情報を取得し、「申請管理システム」上のデータとの整合性を確認する。
G3	システム運用担当者は、「物品管理システム」より「官品デバイス」の現状の登録情報を取得し、「申請管理システム」上のデータとの整合性を確認する。
G4	システム運用担当者は、「SKYSEA」より「各課室持ち込み品」の 現状の登録情報を取得し、「申請管理システム」上のデータとの 整合性を確認する。 ※最終起動日が3か月経過したものは確認対象として、該当の登録物品に絞って確認依頼を出す
G5	システム運用担当者は、「物品管理システム」より「消耗品」の現状の登録情報を取得し、「申請管理システム」上のデータとの整合性を確認する。
G6	「物品管理システム」の登録情報と「申請管理システム」上のデータとの差分の有無、「申請管理システム」上のデータと「SKYSEA」登録情報との差分の有無で対応が分岐する。
G7	システム運用担当者は、差分について、「物品管理システム」、 「SKYSEA」に登録されているデータの更新対応を実施する。根本原因については、G21で原因分析・是正対応を行う。
G8	システム運用担当者は、運用在庫の現物確認を行い「物品管理システム」の登録数との整合性の確認と、「SKYSEA」登録数との整合性を確認する。
G9	システム運用担当者は、運用在庫の現物確認結果と「物品管理システム」の登録情報との差分の有無、「SKYSEA」登録情報との差分の有無で対応が分岐する。
G10	システム運用担当者は、差分について、「物品管理システム」、 「SKYSEA」登録情報の更新対応を実施する。根本原因についてはG21で原因分析・是正対応を行う。
G11	システム運用担当者は、「物品管理システム」の登録情報および 「SKYSEA」の登録情報を基に機関等担当者へ情報を送付し、棚卸を依頼する。 ※利用終了予定日を超過しているものは返却または期限延長など、対応が漏れている申請があれば対応するよう依頼する
G12	システム運用担当者は、機関等担当者より、変更箇所または変更がない旨の連絡を受領する。
G13	システム運用担当者は、「物品管理システム」、「SKYSEA」登録情報へ、確認結果を反映する。
G14	システム運用担当者は、「SKYSEA」上で管理している端末データと「申請管理システム」上のデータの整合性を確認する。故障交換などで存在しなくなった端末データの削除が漏れていないか確認し、不要なデータが残存していた場合は削除する。
G15	システム運用担当者は、棚卸結果のとりまとめを実施する。
G16	システム運用担当者は、今回の対応の中で是正対応が発生していたかどうかで対応が分岐する。
G17	システム運用担当者は、登録情報と実態との差異が発生した根本原因を分析し、必要に応じて是正対応を実施する。
G18	システム運用担当者は、運用業務実施責任者へ棚卸作業結果を報告する。

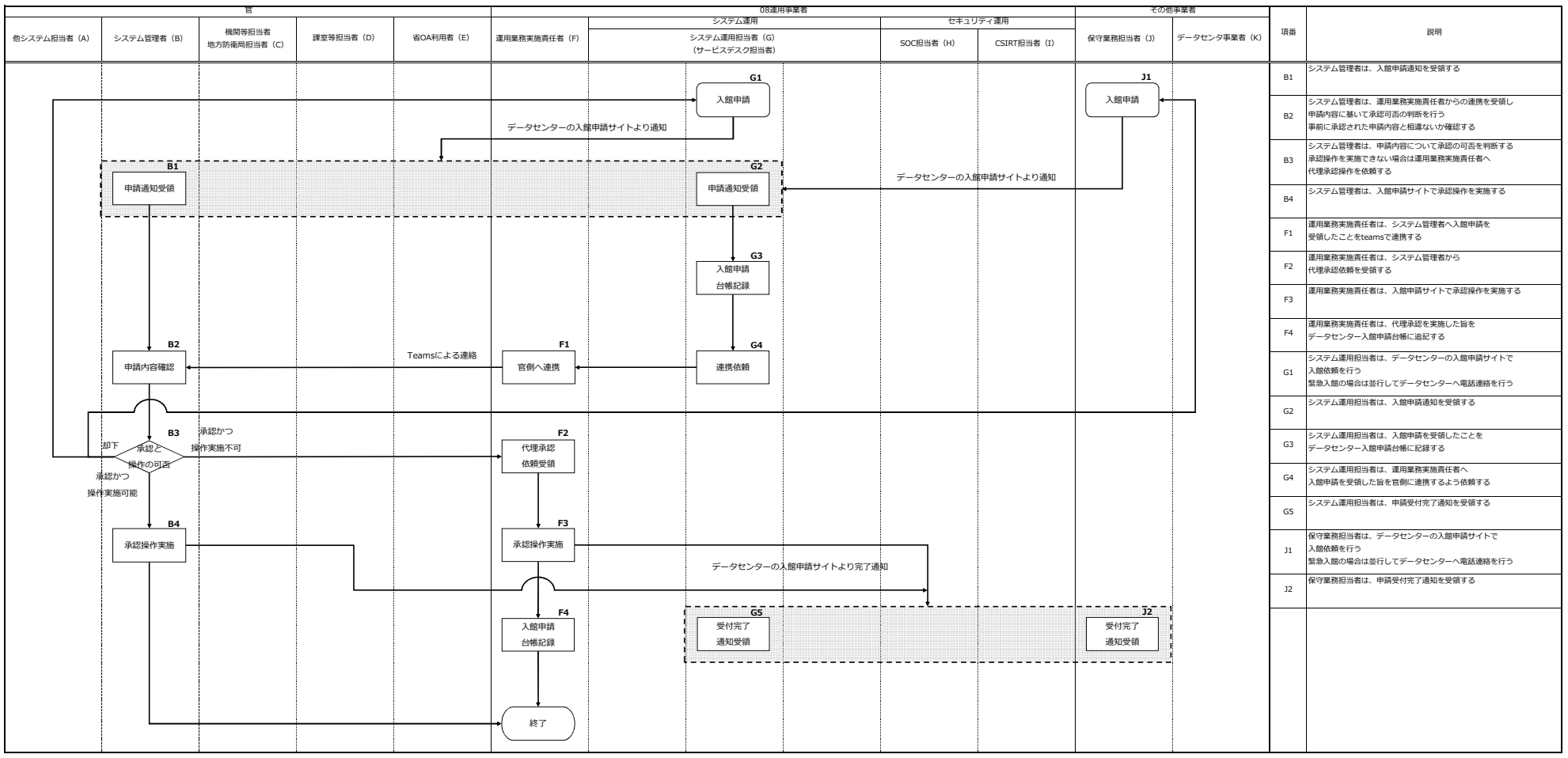
フロー名称	説明	作業トリガー
システムリソース利用状況の分析・評価	システムリソース利用状況の分析・評価に係る、 監視データの収集、分析結果に基づく評価までのフローを示す	日次処理



項番	説明
G1	本処理は日次で1回実施する。基準時刻は00:10（変更可）で、対象データは前日分（00:00–24:00）。
G2	システム運用担当者は、夜間バッチ処理でシステムリソースデータが収集された後、手順書を参照し、データ収集状況を確認し、チェックシートに記載する。
G3	システム運用担当者は、データ欠損確認をする。
G4	システム運用担当者は、データ欠損原因について、既知事象か、原因不明かを判断する。 その際以下を事前確認しておく。 ・直近の運用作業・ジョブ異常・設定変更有無 ・周辺システム・連携元のメンテ/障害情報 原因不明の場合はインシデント対応フローにて対応する。 インシデント対応フローにて対応した後は再度データ収集状況を確認する。
G5	システム運用担当者は、原因を特定した場合は、さらに対処可能かどうかを確認する。 作業影響などで欠損しており対処が出来ない場合は、システム利用状況報告書にその旨を記載する。
G6	システム運用担当者は、対処可能場合は、可能な限り欠損データを復旧する。
G7	システム運用担当者は、リソースデータを所定のフォルダに格納する
G8	システム運用担当者は、システムリソースデータを評価し、チェックシートに記載する ・CPU使用率：スパイク（急上昇）や不自然な高止まりはないか ・メモリ利用率：解放されずに右肩上がり（階段状）になっていないか ・ディスク容量：1日で数%以上の急激な増加はないか ・ディスクI/O：特定の時間帯に異常な高負荷が続いていないか ・NWトラフィック：業務時間外に不自然な大量通信はないか
G9	システム運用担当者は、異常値の有無を確認する。異常値有でも既知のもので対処不要かどうかも確認する。
G10	システム運用担当者は、異常値があった場合、保守業務担当者に原因などの確認を依頼する。
J1	保守業務担当者は、システム運用担当者から異常値の確認依頼を受領する。
J2	保守業務担当者は、対処が必要かどうかを確認する。 対処不要の場合は静観依頼をシステム運用担当者に伝え、対処が必要な場合はインシデント対応フローへと進む。

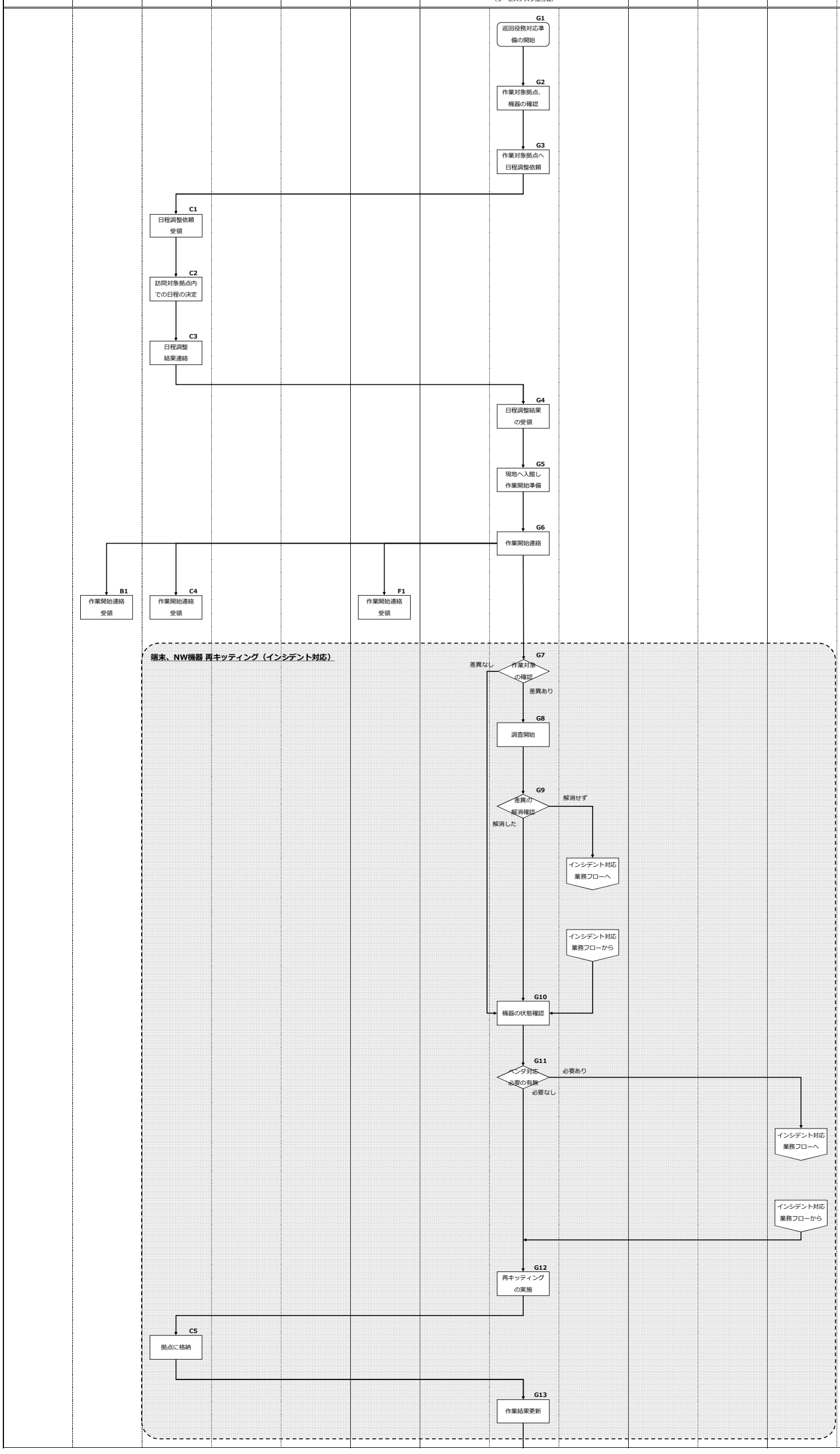
付表９　業務フロー（続き）
データセンター入館受付（続き）

フロー名称	説明	作業トリガー
データセンター入館受付	第1センター及び第2センターへの入館申請を受け付け、 官側への連携と、官側で対応できない場合に代理で承認操作を実施する業務 変更依頼も同じフローで対応する	データセンターへの入館申請



項番	説明
B1	システム管理者は、入館申請通知を受領する
B2	システム管理者は、運用業務実施責任者からの連携を受領し 申請内容に基いて承認可否の判断を行う 事前に承認された申請内容と相違ないか確認する
B3	システム管理者は、申請内容について承認の可否を判断する 承認操作を実施できない場合は運用業務実施責任者へ 代理承認操作を依頼する
B4	システム管理者は、入館申請サイトで承認操作を実施する
F1	運用業務実施責任者は、システム管理者へ入館申請を 受領したことをteamsで連携する
F2	運用業務実施責任者は、システム管理者から 代理承認依頼を受領する
F3	運用業務実施責任者は、入館申請サイトで承認操作を実施する
F4	運用業務実施責任者は、代理承認を実施した旨を データセンター入館申請台帳に追記する
G1	システム運用担当者は、データセンターの入館申請サイトで 入館依頼を行う 緊急入館の場合は並行してデータセンターへ電話連絡を行う
G2	システム運用担当者は、入館申請通知を受領する
G3	システム運用担当者は、入館申請を受領したことを データセンター入館申請台帳に記録する
G4	システム運用担当者は、運用業務実施責任者へ 入館申請を受領した旨を官側に連携するよう依頼する
G5	システム運用担当者は、申請受付完了通知を受領する
J1	保守業務担当者は、データセンターの入館申請サイトで 入館依頼を行う 緊急入館の場合は並行してデータセンターへ電話連絡を行う
J2	保守業務担当者は、申請受付完了通知を受領する

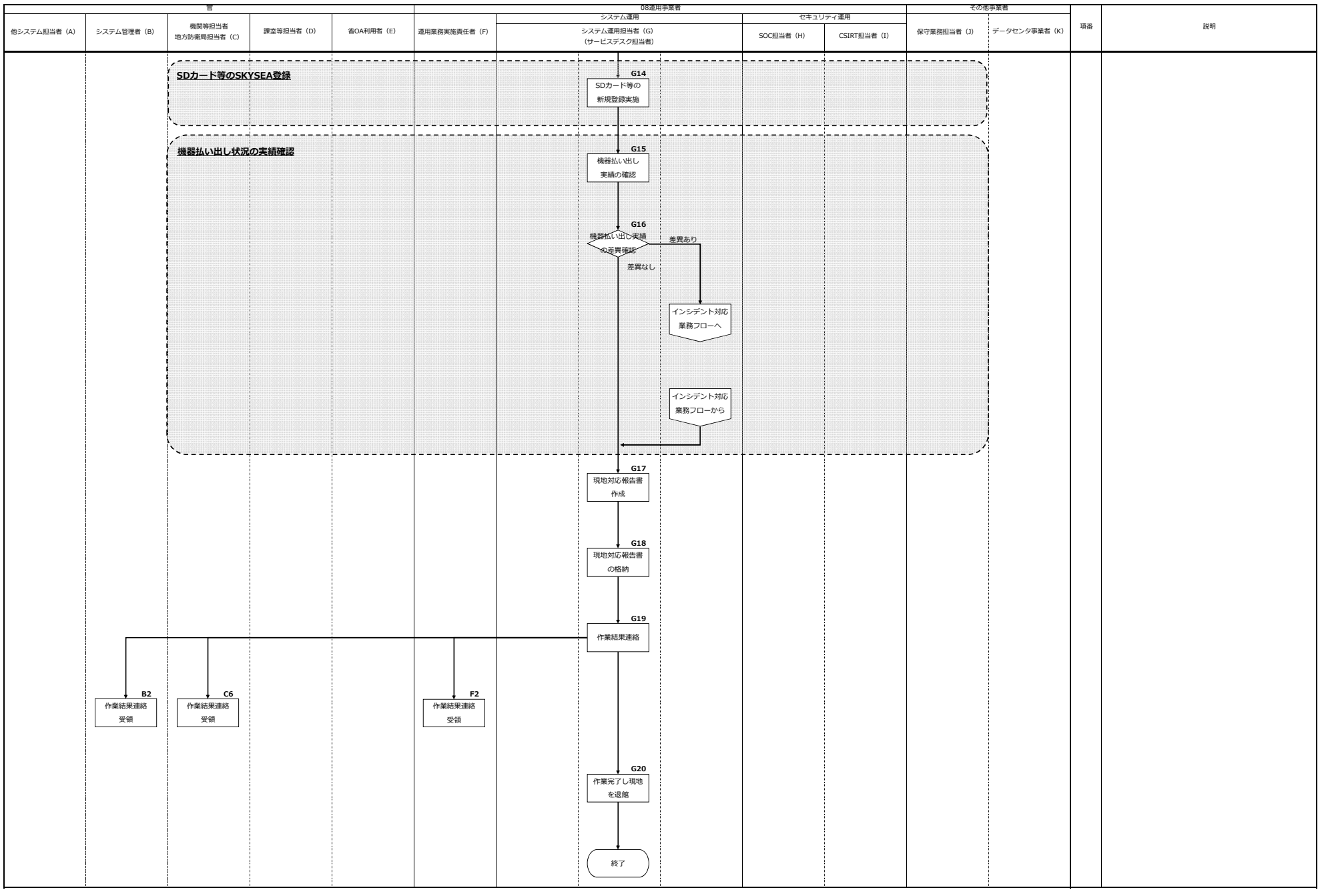
フロー名称	説明	作業トリガー
地方防衛局の巡回役務	地方防衛局へ主に隔月で巡回する役務作業についてフローを示す 端末、NW機器の再キッティング、SDカード等のSKYSEA登録作業についてフローを示す	隔月処理



項番	説明
B1	システム管理者はシステム運用担当者より訪問拠点への入館、現地作業の対応予定内容と開始連絡を受領する。
B2	システム管理者は、システム運用担当者より訪問拠点での現地作業内容と完了報告、拠点退館の連絡を受領する。
C1	地方防衛局担当者は、システム運用担当者より訪問拠点での日程調整依頼を受領する。
C2	地方防衛局担当者は訪問拠点に対し、作業場所を調整し、作業日程を決定する。
C3	地方防衛局担当者は、システム運用担当者に訪問拠点での日程調整の結果を連絡する。
C4	地方防衛局担当者に対し、システム運用担当者より訪問拠点への入館、現地作業の対応予定内容と開始連絡を受領する。
C5	システム運用担当者より再キッティングが完了した端末、NW機器を受領し、拠点内にて格納する。
C6	地方防衛局担当者に対し、システム運用担当者より訪問拠点での現地作業内容と完了報告、拠点退館の連絡を受領する。
F1	地方防衛局担当者に対し、システム運用担当者より訪問拠点への入館、現地作業の対応予定内容と開始連絡を受領する。
F2	地方防衛局担当者に対し、システム運用担当者より訪問拠点での現地作業内容と完了報告、拠点退館の連絡を受領する。
G1	システム運用担当者は、再キッティング・機器修理・機器の払い出し返却があった拠点に対し、現地での巡回役務対応準備を開始する。（訪問は二カ月ごとを基本とする）
G2	システム運用担当者は、現地訪問時のキッティング作業対象となる端末、NW機器のリストを作成し確認する。
G3	システム運用担当者は、地方防衛局担当者に訪問拠点での日程調整依頼を実施する。
G4	システム運用担当者は、地方防衛局担当者から決定した訪問拠点での日程調整結果を受領する。
G5	システム運用担当者は作業対象の訪問拠点に入館し、予定作業開始の準備をする。
G6	システム運用担当者は、地方防衛局担当者に訪問拠点への入館、作業開始の連絡を行う。
G7	システム運用担当者は、作業対象の機器名、員数等を確認し事前情報と差異が無いことを確認する。
G8	作業対象の機器、員数等に事前情報と差異があった場合、入館したシステム運用担当者にて事象解決に向けての対応を実施する。
G9	システム運用担当者は対応の結果、事象が解決したか判断する。
G10	システム運用担当者は、作業対象の端末・NW機器に対し、再キッティング作業前に状態確認を実施する。
G11	システム運用担当者は、作業対象機器の状態を確認し、ベンダ対応の必要有無を確認する。ベンダ対応が必要な場合、ベンダ問い合わせに必要なログ等を採取し、問い合わせの上で対応の日程調整等を実施する。
G12	システム運用担当者は、作業対象の端末・NW機器に対し再キッティング作業を実施する。
G13	システム運用担当者は現地作業報告書の作業結果を更新する。
G14	システム運用担当者は、SDカード等の新規調達メディアがある場合、SKYSEA管理機を用意し、新規登録を行う。
G15	システム運用担当者は、地方防衛局担当者にて行っている機器払い出しの実績について、申請対応の中で現地の課室担当者および地方防衛局担当者に依頼した内容と実態に乖離が無いかを確認する。 「官品デバイス等登録申請」で登録した官品デバイスに貼り付けけるシールについても、保管場所からの持ち出しの実績を確認する。
G16	システム運用担当者は、地方防衛局担当者にて行っている機器払い出しの実績と申請の差異の有無を確認する。
G17	システム運用担当者は、予定していた作業が全て完了したことを確認できたら、現地対応作業報告書を作成する。
G18	システム運用担当者は作成した現地対応作業報告書を対象フォルダに格納する。
G19	システム運用担当者は地方防衛局担当者に訪問拠点での作業完了、訪問拠点からの退館の連絡を行う。
G20	システム運用担当者は作業対象の訪問拠点より退館する。

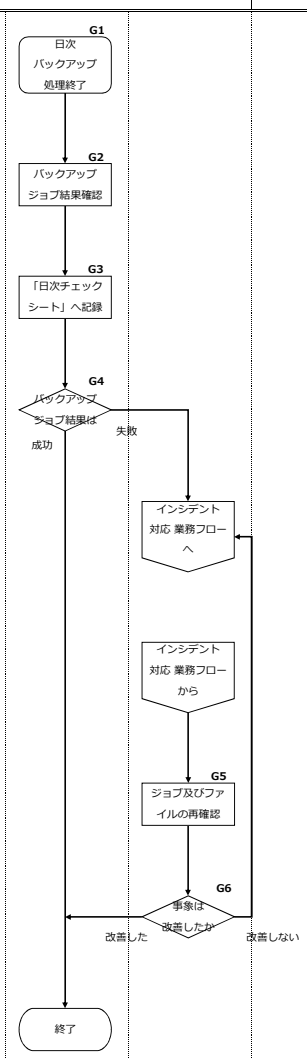
付表１０　業務フロー（続き）
地方防衛局の巡回役務（続き）

フロー名称	説明	作業トリガー
地方防衛局の巡回役務	地方防衛局へ主に隔月で巡回する役務作業についてフローを示す 端末、NW機器の再キッティング、SDカード等のSKYSEA登録作業についてフローを示す	隔月処理



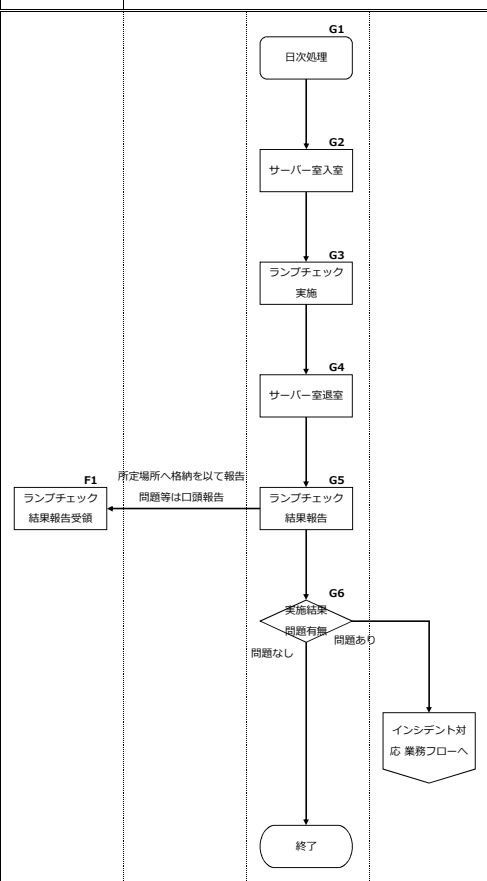
付表１０　業務フロー（続き）
バックアップ取得状況の確認（続き）

フロー名称	説明	作業トリガー
バックアップ取得状況の確認	自動実行されるバックアップジョブの成否を日次で確認することで、 想定外のバックアップ失敗が発生した際に、早期の対処を図る業務である。	日次処理

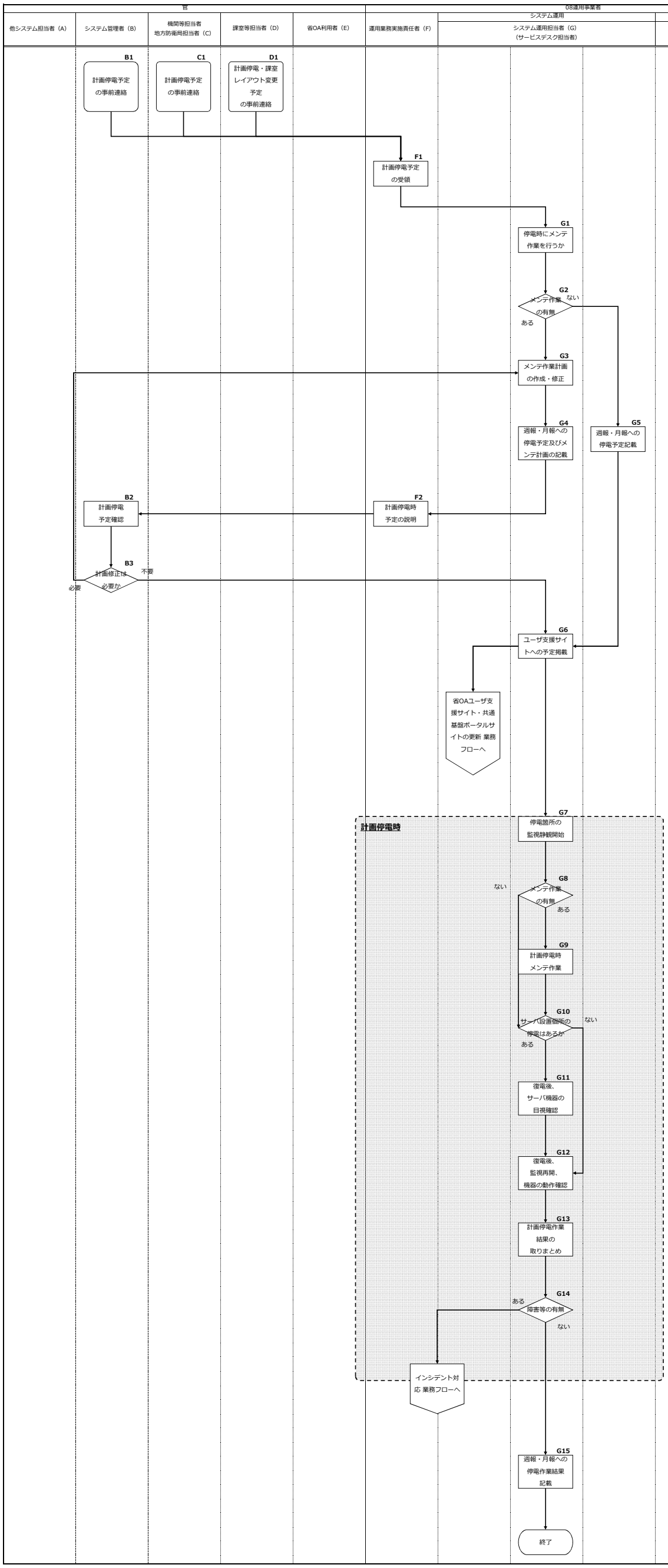
官					08運用事業者				その他事業者		項番	説明
他システム担当者（A）	システム管理者（B）	機関等担当者 地方防衛局担当者（C）	課室等担当者（D）	省OA利用者（E）	運用業務実施責任者（F）	システム運用 システム運用担当者（G） （サービスデスク担当者）	セキュリティ運用 SOC担当者（H）	セキュリティ運用 CSIRT担当者（I）	保守業務担当者（J）	データセンタ事業者（K）		
											G1	システム運用担当者は、日次処理として本業務を開始する。日次の最後のバックアップジョブが終了した直後のタイミングで本業務を実施する。
											G2	システム運用担当者は、バックアップ管理アプリケーションを用いてバックアップジョブの処理結果を確認する。
											G3	システム運用担当者は、バックアップジョブの確認結果を「日次チェックシート」に記録する。
											G4	バックアップジョブの確認結果、処理が「成功」していたか「失敗」していたかで、その後の対処が分岐する。 ・成功：本業務は終了する。 ・失敗：「インシデント対応」へ繋ぎ、失敗の原因特定及び失敗したバックアップの再取得を行う。 ※バックアップジョブが遅延していても、それだけで失敗にはならない。失敗判定は “後続ジョブに影響が出たか” で判断する。
											G5	システム運用担当者はインシデント対応の後、バックアップジョブの結果及びバックアップファイルの実在確認を行い、バックアップ失敗事象が改善しているか判断する。
											G6	再確認結果、バックアップ失敗事象が「改善」したか否かで、その後の対処が分岐する。 ・改善した：本業務は終了する。 ・改善しない：「インシデント対応」へ戻り、失敗の原因特定及び失敗したバックアップの再取得対応を継続する。

フロー名称	説明	作業トリガー
ランプチェック	本システム機器に対する定期点検として、市ヶ谷、第1センター、第2センターでの、目視確認、正常性確認を実施するランプチェック業務における対応フローを示す。	日次処理

官					08運用事業者				その他事業者		項番	説明
						システム運用	セキュリティ運用					
他システム担当者（A）	システム管理者（B）	機関等担当者 地方防衛局担当者（C）	課室等担当者（D）	省OA利用者（E）	運用業務実施責任者（F）	システム運用担当者（G） （サービスデスク担当者）	SOC担当者（H）	CSIRT担当者（I）	保守業務担当者（J）	データセンタ事業者（K）	F1	運用業務実施責任者は、システム運用担当者が所定の格納場所へ、ランプチェックシートを格納されたことにより、実施完了を確認する。
											G1	本処理は日次で１回実施する。
											G2	システム運用担当者は入館、サーバー室に入室する。 ※あらかじめ入室申請を完了したメンバーが対応可能
											G3	システム運用担当者は、ランプチェックシートに従って作業実施する。
											G4	システム運用担当者はサーバー室より退室、退館する。
											G5	システム運用担当者は、実施したランプチェックシートを所定の場所へ格納し、運用業務実施責任者へのランプチェック完了の報告とする。 チェック結果に問題や懸念がある場合、運用業務実施責任者へ口頭で問題および懸念の内容について報告する。
											G6	システム運用担当者のランプチェック実施結果、問題あり/なしを判断し、判断結果で対応が分岐する。問題ありの場合、インシデント対応業務フローで対応を実施する。

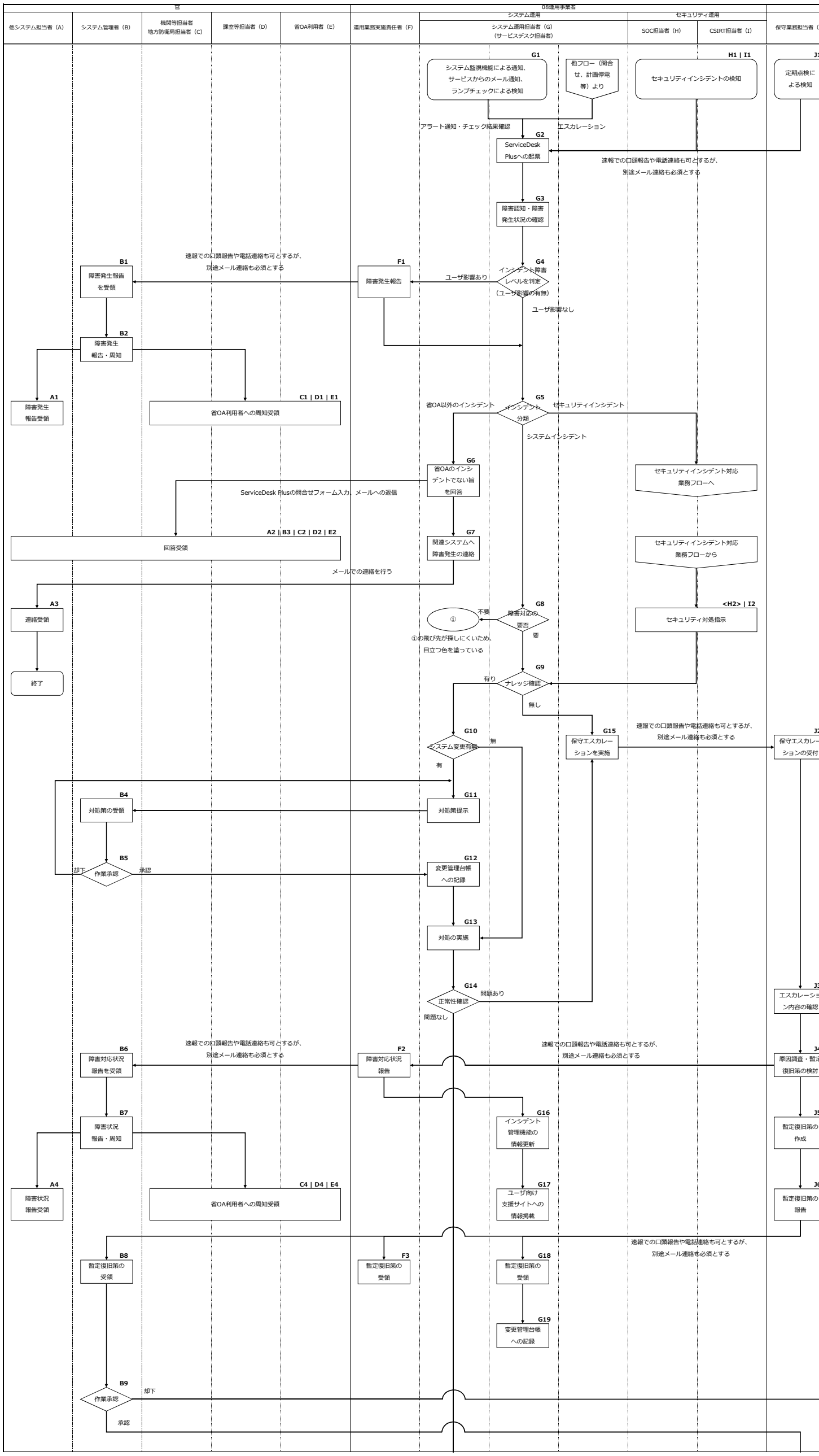


フロー名称	説明	作業トリガー
計画停電対応	市ヶ谷庁舎や各通信所、駐屯地等における計画停電が行われる際の対応を定義する。	官から計画停電や課室レイアウト変更の予定連絡を受けた時 及び計画停電の実施前後



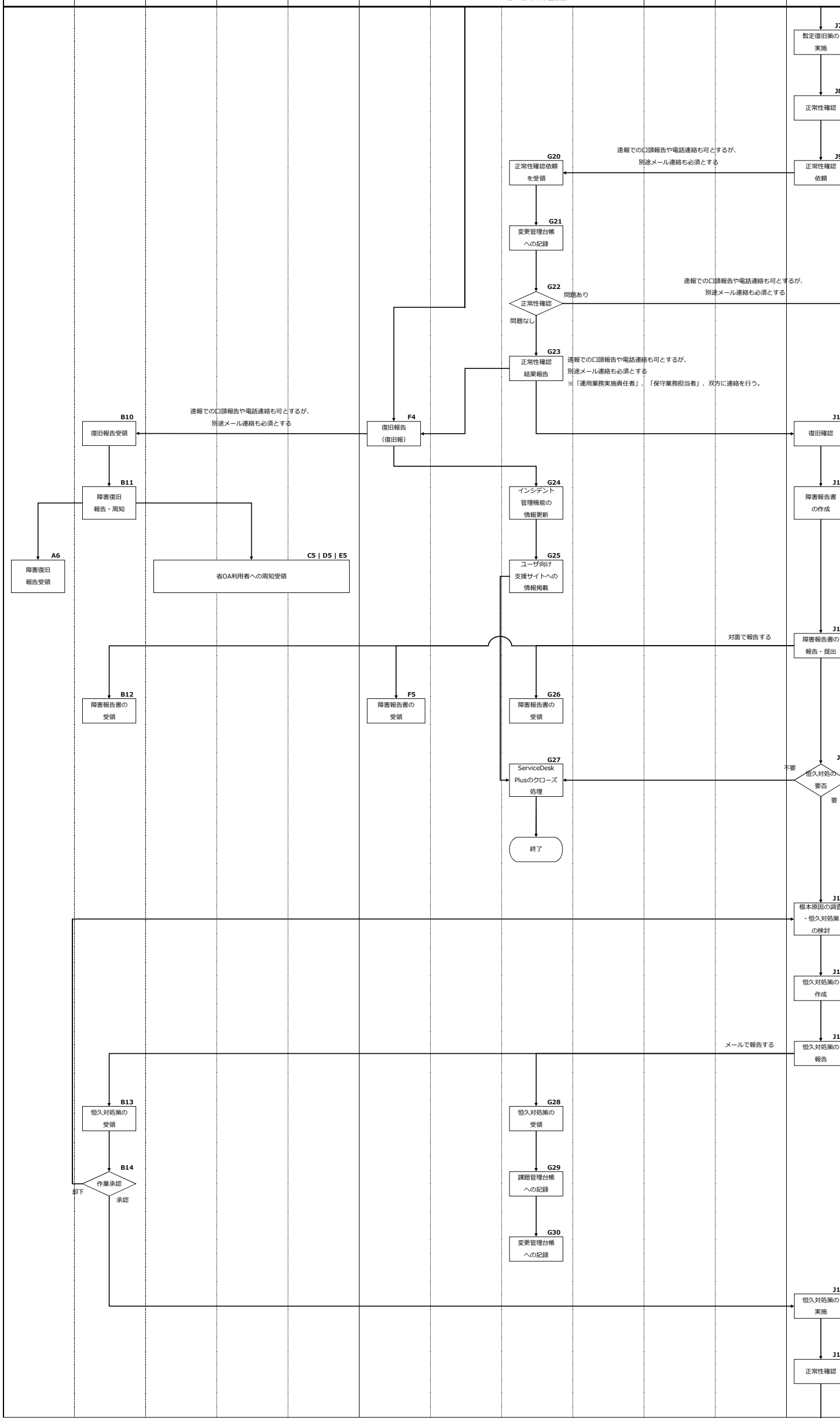
項番	説明
B1	システム管理者は、庁舎の計画停電予定が決まったら、事前に08運用事業者にその予定を伝え、対応依頼を行う（毎年1～2月頃にその年の予定を伝える）。また、年の途中でも新たな計画停電予定が発生した際は、追加で通達を行う。
B2	システム管理者は、計画停電時の作業予定の説明を受け、その内容の承認を行う。
B3	システム管理者は、説明を受けた計画停電作業予定内容の修正要否を判断する。
C1	機関等担当者、地方防衛局担当者は、庁舎の計画停電予定が決まったら、事前に08運用事業者にその予定を伝え、対応依頼を行う。
D1	課室等担当者は、庁舎の計画停電予定や課室レイアウト変更予定が決まったら、事前に08運用事業者にその予定を伝え、対応依頼を行う。
F1	運用業務実施責任者は、システム担当者や機関等担当者、地方防衛局担当者、課室等担当者から、その年の計画停電予定の通達を受ける。
F2	運用業務実施責任者は、計画停電時に同時に行うシステムメンテナンス作業がある場合は、その作業内容の説明をシステム管理者に対して行う。説明タイミングは、週報や月報時を想定するが、個別に説明が必要な場合は別途時間を設ける。
G1	システム運用担当者は、計画停電のタイミングを利用して、パッチ適用やソフトウェアバージョンアップ等のシステムメンテナンス作業の実施を行うかどうか検討する。
G2	システム運用担当者は、システムメンテナンス作業を計画停電時に実施するか、判断する。
G3	システム運用担当者は、計画停電時にシステムメンテナンス作業を実施する場合は、その作業計画を作成する。システム管理者より作業計画の修正を求められた際は、修正対応を行う。
G4	システム運用担当者は、週報や月報資料に、計画停電予定やシステムメンテナンス作業予定を記載する。
G5	システム運用担当者は、週報や月報資料に、計画停電予定を記載する。
G6	システム運用担当者は、ユーザ支援サイトに計画停電や（実施する場合）システムメンテナンスの予定を掲載し、利用者向けに周知する。
G7	システム運用担当者は、計画停電の時間帯は、該当箇所に存在する機器から上がってくるアラートを停電影響として「静観」する。
G8	システム運用担当者は、計画停電時に「システムメンテナンス作業」を実施するか。
G9	システム運用担当者は、計画していたシステムメンテナンス作業を実施する。
G10	システム運用担当者は、計画停電の範囲にB2棟等のサーバが設置されている箇所が含まれているか。
G11	システム運用担当者は、復電後に、サーバ機器について実機の目視確認を行い、異常等が発生していないか確認する。
G12	システム運用担当者は、計画停電の電源復電後に、監視を再開し、停止していた機器等の動作状況を確認する。正常に再起動しているか、監視等の仕組みを利用して確認する。
G13	システム運用担当者は、計画停電時に実施した、各作業結果の取りまとめを行う。
G14	システム運用担当者は、計画停電の各種対応作業の結果、障害等の発生はあったか。
G15	システム運用担当者は、計画停電の対応作業結果を、週報・月報等に記載する。

フロー名称	説明	作業トリガー
インシデント対応	障害インシデント発生時における、影響度合いの調査や復旧にかかる各作業、 随時タイミングの状況報告などの、諸対応フローを示す。	OA利用者からの障害連絡、システム監視機能による通知、 サービスからのメール通知、ランプチェックによる検知、 他フロー（問合せ、計画停電等）からのエスカレーション セキュリティインシデントの検知、定期点検による検知



項番	説明
A1	他システム担当者は、システム管理者より、障害発生の情報連を受領する。
A2	他システム担当者は、当初のシステム運用担当者への問合せに対し、「省OAの障害でない」旨の回答を受領する。
A3	他システム担当者は、システム運用担当者より、省OA以外のインシデントである旨の回答を受領する。
A4	他システム担当者は、システム管理者より、障害状況の情報連携を受領する。
A5	他システム担当者は、システム管理者より、障害復旧の情報連携を受領する。
B1	システム管理者は、運用業務実施責任者より、障害発生報告を受領する。
B2	システム管理者は、他システム担当者へ情報連携、省OAユーザへ周知を行う。
B3	システム管理者は、当初のシステム運用担当者への問合せに対し、「省OAの障害でない」旨の回答を受領する。
B4	システム管理者は、システム運用担当者より、対処策を受領する。
B5	システム管理者は、作業承認を判定する。承認｜却下をシステム運用担当者に連絡する。
B6	システム管理者は、運用業務実施責任者より、障害対応状況の報告を受領する。
B7	システム管理者は、他システム担当者へ情報連携、省OAユーザへ周知を行う。
B8	システム管理者は、保守業務担当者より、暫定復旧策の報告を受領する。
B9	システム管理者は、作業承認を判定する。承認｜却下を保守業務担当者に連絡する。
B10	システム管理者は、運用業務実施責任者より、障害復旧報告を受領する。
B11	システム管理者は、他システム担当者へ情報連携、省OAユーザへ周知を行う。
B12	システム管理者は、保守業務担当者より、障害報告書を受領する。
B13	システム管理者は、保守業務担当者より、恒久復旧策の報告を受領する。
B14	システム管理者は、作業承認を判定する。承認｜却下を保守業務担当者に連絡する。
B15	システム管理者は、保守業務担当者より、作業完了報告を受領する。
B16	システム管理者は、運用業務実施責任者より、作業計画を受領する。
B17	システム管理者は、作業承認の判定を行う。 判定結果の 承認｜却下を運用業務実施責任者に連絡する。
B18	システム管理者は、運用業務実施責任者より、作業完了報告を受領する。
C1	機関等担当者、地方防衛局担当者は、システム管理者より、障害発生の周知を受領する。
C2	機関等担当者、地方防衛局担当者は、当初のシステム運用担当者への問合せに対し、「省OAの障害でない」旨の回答を受領する。
C3	機関等担当者、地方防衛局担当者は、システム管理者より、障害発生の周知を受領する。
C4	機関等担当者、地方防衛局担当者は、システム管理者より、障害復旧の周知を受領する。
D1	課室等担当者は、システム管理者より、障害発生の周知を受領する。
D2	課室等担当者は、当初のシステム運用担当者への問合せに対し、「省OAの障害でない」旨の回答を受領する。
D3	課室等担当者は、システム管理者より、障害発生の周知を受領する。
D4	課室等担当者は、システム管理者より、障害復旧の周知を受領する。
E1	省OA利用者は、システム管理者より、障害発生の周知を受領する。
E2	省OA利用者は、当初のシステム運用担当者への問合せに対し、「省OAの障害でない」旨の回答を受領する。
E3	省OA利用者は、システム管理者より、障害発生の周知を受領する。
E4	省OA利用者は、システム管理者より、障害復旧の周知を受領する。
F1	運用業務実施責任者は、ユーザ影響がある場合、システム管理者へ障害発生報告を行う。
F2	運用業務実施責任者は、保守業務担当者からの原因調査・暫定復旧策の報告内容を受け、システム管理者へ障害対応状況の報告を行う。
F3	運用業務実施責任者は、保守業務担当者より、暫定復旧策の報告を受領する。
F4	運用業務実施責任者は、システム運用担当者からの正常性確認の結果に問題ない報告を受け、システム管理者へ、原因および復旧に向け行った対応について報告を行う。
F5	運用業務実施責任者は、保守業務担当者より、障害報告書を受領する。
F6	運用業務実施責任者は、保守業務担当者より、作業完了報告を受領する。
F7	運用業務実施責任者は、システム運用担当者が作成した作業計画を確認し、システム管理者へ作業計画の承認依頼を行う。
F8	運用業務実施責任者は、システム運用担当者からの正常性確認の結果に問題ない旨の報告を受け、システム管理者へ作業完了報告を行う。
G1	システム運用担当者は、システム監視からの各種アラート通知、各種クラウドサービスからのメール通知、システム運用によるランプチェックの結果で障害を検知した場合に障害の起票を行う。
G2	システム運用担当者は、各検知内容をServiceDesk Plusに起票処理する。
G3	システム運用担当者は、障害を認知、障害発生状況を確認する。
G4	システム運用担当者は、システムインシデントの場合、インシデント障害レベルを判定する。 ユーザ影響がある場合（レベル2以上）、速やかに運用業務実施責任者へ発生報告する。 障害レベル [レベル４] ・省内全体で発生、ユーザ影響が全体 [レベル３] ・機関レベル、またはフロアレベルで障害発生。 ・省内全体で発生、ユーザ影響が広範囲 ・サービスのダウン(ユーザ影響大) [レベル２] ・課室レベルでの障害発生 ・省内の一部で発生、ユーザ影響が狭範囲 ・サービスの1部ダウン(ユーザ影響小) [レベル１] ユーザ影響はないが、運用影響ありの場合 ・サーバへのping疎通やリモートログイン不可 ・Webアクセス画面へのアクセス不可
G5	インシデントの分類により、その後の対応が異なる。
G6	システム運用担当者は、省OA以外のインシデントの場合、省OAのインシデントでない旨を他システム担当者に回答する。
G7	システム運用担当者は、障害の発生した関連システムに、障害発生の連絡（情報共有）を行う。
G8	システム運用担当者は、障害対応要否を判定する。監視アラートの内容が静観でよい場合のみ不要とし、①対応を行う。

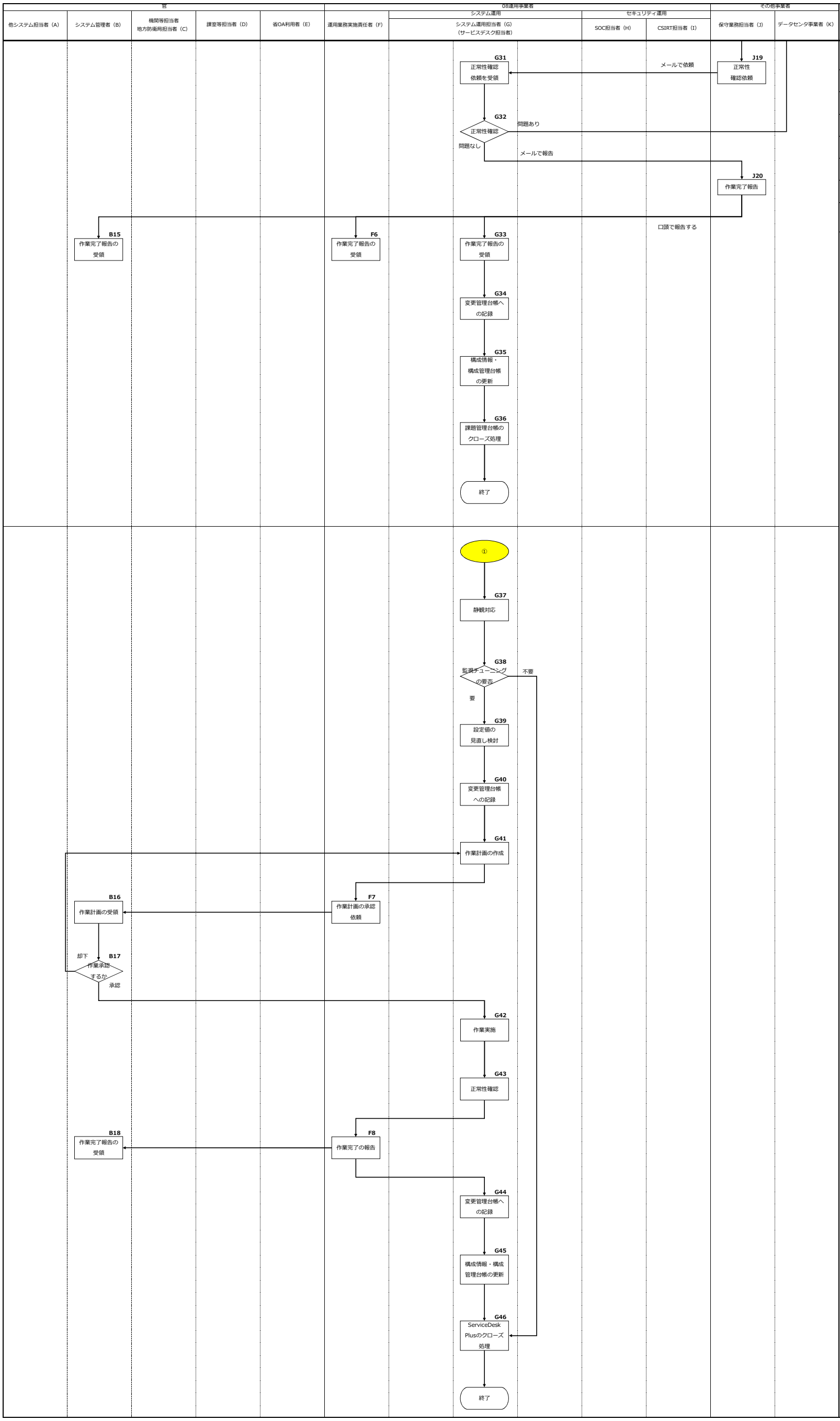
フロー名称	説明	作業トリガー
インシデント対応	障害インシデント発生時における、影響度合いの調査や復旧にかかる各作業、 随時タイミングの状況報告などの、諸対応フローを示す。	OA利用者からの障害連絡、システム監視機能による通知、 サービスからのメール通知、ランプチェックによる検知、 他フロー（問合せ、計画停電等）からのエスカレーション セキュリティインシデントの検知、定期点検による検知



項番	説明
G9	システム運用担当者は、ナレッジを確認する。確認結果によりその後の対応が異なる。
G10	システム運用担当者は、ナレッジの対処策が、システム変更を伴うものかどうかにより、その後の対応が異なる。
G11	システム運用担当者は、システム管理者へ対処策を報告する。
G12	システム運用担当者は、変更管理台帳を更新する。
G13	システム運用担当者は、ナレッジを基に対処を実施する。
G14	システム運用担当者は、正常性確認の結果、問題あり｜問題なし を判定し、報告を行う。 問題あり：「保守業務担当者」に報告を行う。 問題なし：「運用業務実施責任者」に報告を行う。
G15	システム運用担当者は、ナレッジがない場合、保守業務担当者へエスカレーションを実施する。
G16	システム運用担当者は、インシデント管理機能の情報を更新する。
G17	システム運用担当者は、ユーザ向け支援サイトへ障害発生の情報を掲載する。
G18	システム運用担当者は、保守業務担当者より暫定復旧策の報告を受領する。
G19	システム運用担当者は、変更管理台帳を更新する。
G20	システム運用担当者は、保守業務担当者より正常性確認依頼を受領する。
G21	システム運用担当者は、変更管理台帳を更新する。
G22	システム運用担当者は、正常性確認の結果、問題あり｜問題なし を判定し、報告を行う。 問題あり：「保守業務担当者」に報告を行う。 問題なし：「運用業務実施責任者」および「保守業務担当者に報告を行う。
G23	システム運用担当者は、運用業務実施責任者および保守業務担当者へ、正常性確認の結果、問題がなかったことを報告する。
G24	システム運用担当者は、インシデント管理機能の情報を更新する。
G25	システム運用担当者は、ユーザ向け支援サイトへ障害復旧の情報を掲載する。
G26	システム運用担当者は、保守業務担当者より、障害報告書を受領する。
G27	システム運用担当者は、ServiceDesk Plusの本インシデントに関するクローズ処理を行う。
G28	システム運用担当者は、保守業務担当者より、恒久復旧策の報告を受領する。
G29	システム運用担当者は、恒久対策実施の連絡受領を踏まえ、課題管理台帳を更新する。
G30	システム運用担当者は、変更管理台帳を更新する。
G31	システム運用担当者は、保守業務担当者より正常性確認依頼を受領する。
G32	システム運用担当者は、正常性確認の結果、問題あり｜問題なし を判定し、報告を行う。 問題あり：保守業務担当者に報告を行う 問題なし：運用業務実施責任者および保守業務担当者に報告を行う。
G33	システム運用担当者は、保守業務担当者より、作業完了報告を受領する。
G34	システム運用担当者は、変更管理台帳を更新する。
G35	システム運用担当者は、構成情報・構成管理台帳を更新する。
G36	システム運用担当者は、課題管理台帳を更新し、クローズ処理を行う。
G37	システム運用担当者は、システム運用担当者は、静観対応を実施する。
G38	システム運用担当者は、監視チューニングの要｜不要 を判定する。
G39	システム運用担当者は、監視チューニングが要の場合、設定値の見直しを検討する。
G40	システム運用担当者は、変更管理台帳を更新する。
G41	システム運用担当者は、作業計画を作成し、運用業務実施責任者へ報告する。
G42	システム運用担当者は、システム管理者の作業承認を受け、作業を実施する。
G43	システム運用担当者は、正常性確認を実施し、結果を運用業務実施責任者へ報告する。
G44	システム運用担当者は、変更管理台帳を更新する。
G45	システム運用担当者は、構成情報・構成管理台帳を更新する。
G46	システム運用担当者は、ServiceDesk Plusの本インシデントに関するクローズ処理を行う。
H1	SOC担当者は、セキュリティインシデントを検知した場合にインシデント対応依頼を行う。
H2	SOC担当者は、セキュリティ運用からシステム運用担当者へ、セキュリティ対処指示を実施する。（基本的にSOC担当者が実施する）
I1	CSIRT担当者は、セキュリティインシデントを検知した場合にインシデント対応依頼を行う。
I2	CSIRT担当者は、セキュリティ運用からシステム運用担当者へ、セキュリティ対処指示を実施する。（基本的にSOC担当者が実施する）
J1	保守業務担当者は、定期点検実施時に障害を検知した場合にインシデント対応依頼を行う。
J2	保守業務担当者は、システム運用担当者より、エスカレーションを受領する。
J3	保守業務担当者は、エスカレーション内容を確認する。
J4	保守業務担当者は、原因調査・暫定復旧策の検討を実施する。
J5	保守業務担当者は、暫定復旧策を作成する。
J6	保守業務担当者は、暫定復旧策をシステム管理者およびシステム運用担当者へ報告する。
J7	保守業務担当者は、システム管理者の作業承認を受け、暫定復旧策を実施する。
J8	保守業務担当者は、正常性確認を実施する。
J9	保守業務担当者は、システム運用担当者へ正常性確認依頼を実施する。
J10	保守業務担当者は、システム運用担当者からの正常性確認の結果に問題ない報告を受け、復旧確認を実施する。
J11	保守業務担当者は、障害報告書を作成する。障害レベルに応じて、作成する報告書のレベルを決定する。具体的には、軽度の障害では保守業務担当名義の報告、重篤な障害の場合は、通常の週次・月次報告や課題管理上の報告とは別に、別個で「障害報告書」を作成する。
J12	保守業務担当者は、障害報告書をシステム管理者およびシステム運用担当者へ報告する。

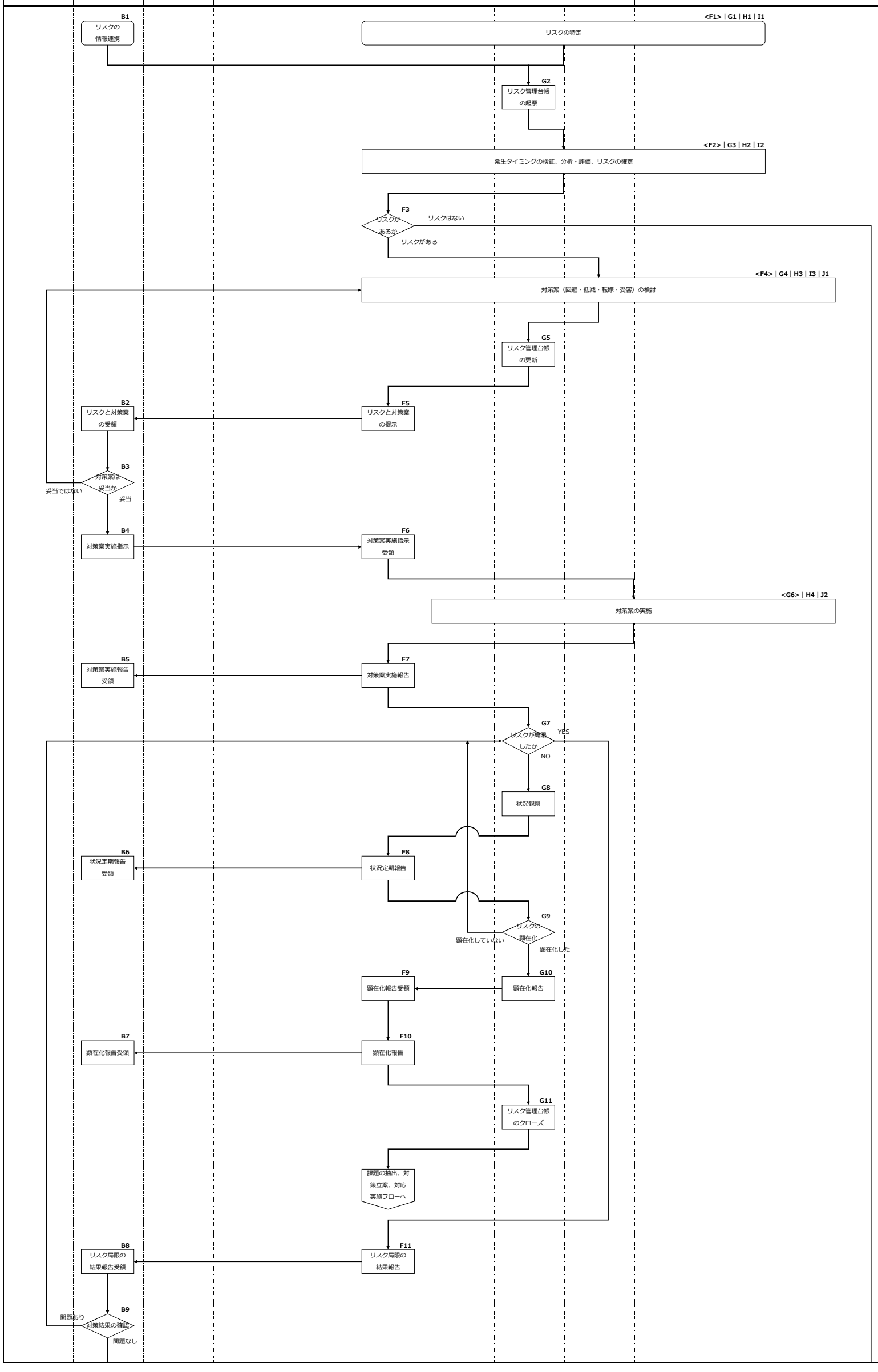
付表１０　業務フロー（続き）
インシデント対応（続き）

フロー名称	説明	作業トリガー
インシデント対応	障害インシデント発生時における、影響度合いの調査や復旧にかかる各作業、 随時タイミングの状況報告などの、諸対応フローを示す。	OA利用者からの障害連絡、システム監視機能による通知、 サービスからのメール通知、ランプチェックによる検知、 他フロー（問合せ、計画停電等）からのエスカレーション セキュリティインシデントの検知、定期点検による検知



項番	説明
J13	保守業務担当者は、恒久対処の要否にて対応が分岐する。要の場合、恒久対処の対応を行う。
J14	保守業務担当者は、根本原因を調査し、恒久対処策を検討する。
J15	保守業務担当者は、恒久対処策を作成する。
J16	保守業務担当者は、恒久対処策をシステム管理者およびシステム運用担当者へ報告する。
J17	保守業務担当者は、システム管理者の作業承認を受け、恒久復旧策を実施する。
J18	保守業務担当者は、正常性確認を実施する。
J19	保守業務担当者は、システム運用担当者へ正常性確認依頼を実施する。
J20	保守業務担当者は、システム運用担当者からの正常性確認の結果に問題ない報告を受け、システム管理者およびシステム運用担当者へ作業完了報告を実施する。

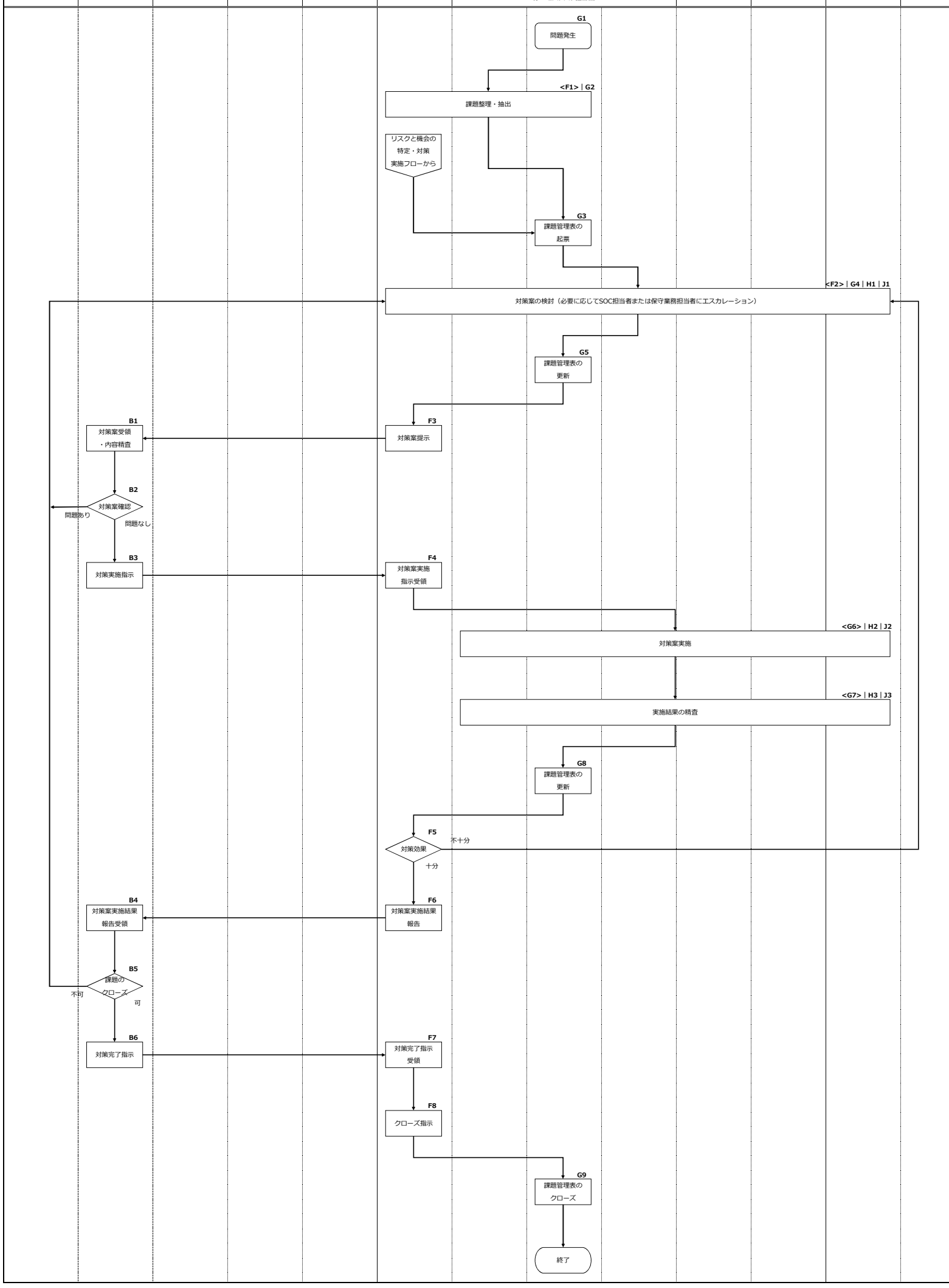
フロー名称	説明	作業トリガー
リスクと機会の特定・対策の実施	想定されるリスクとそのリスクが起こり得るタイミングの特定と対策、および経過観察を行うフローを示す。	・リスクが予測された場合



項番	説明
B1	システム管理者は、リスクが予測された場合、運用業務実施責任者に対策の指示をする。
B2	システム管理者は、運用業務実施責任者から想定されるリスク及び発生タイミング、リスクに対する対策案の提示を受領する。
B3	システム管理者は、運用業務実施責任者から提示された対策案が有効か否かを判断する。
B4	システム管理者は、運用業務実施責任者に対策案の実施を支持する。
B5	システム管理者は、運用業務実施責任者から対策案実施の報告を受領する。
B6	システム管理者は、運用業務実施責任者から対策案実施後の状況に関する定期報告を受領する。
B7	システム管理者は、運用業務実施担当者からリスク顕著化の報告を受領する。
B8	システム管理者は、運用業務実施責任者からリスクが局限したことの結果報告を受領する。
B9	システム管理者は、対策結果を確認し想定されるリスクが局限したことでクローズするか否かを判断する。
B10	システム管理者は、運用業務実施責任者に対してクローズ指示行う。
F1	運用業務実施責任者は、リスクが予測された場合、主体となって内容、対策案の検討を開始する。
F2	運用業務実施責任者は、主体となってシステム運用担当者と共に想定されるリスクが発生し得るタイミング、発生条件、分析・評価等について検証し、リスクとなり得るかを確定する。
F3	運用業務実施責任者は、発生タイミングの検証・リスクの確定において、リスクとなったか否かの判断を行う。
F4	運用業務実施責任者は、主体となってシステム運用担当者と共にリスクに対して、回避・低減・転嫁・受容の対策を検討、決定する。 またシステム運用だけでは対応が難しい場合、SOC担当者または保守業務担当者とエスカレーションして検討を進める。
F5	運用業務実施責任者は、リスク、発生タイミング、その対策案について、随時システム管理者に提示する。
F6	運用業務実施責任者は、システム管理者から対策案実施の指示を受領する。
F7	運用業務実施責任者は、システム管理者に対して対策案の実施報告を行う。
F8	運用業務実施責任者は、システム管理者に対して対策案実施後の状況（リスクが顕在化したか否か）の定期報告を行う。
F9	運用業務実施責任者は、システム運用担当者からリスク顕著化の報告を受領する。
F10	運用業務実施責任者は、システム管理者にリスクの顕著化を報告する。
F11	運用業務実施責任者は、システム管理者に対して、リスクが局限したことの結果報告を行う。
F12	運用業務実施責任者は、システム管理者よりクローズ指示を受領する。
F13	運用業務実施責任者は、システム運用担当者に対してリスクのクローズを指示する。
G1	システム運用担当者は、リスクが予測された場合、内容、対策案の検討を開始する。
G2	システム運用担当者は、リスクと想定発生タイミングについて「リスク管理台帳」に起票する。
G3	システム運用担当者は、運用業務実施責任者と共に想定されるリスクが発生し得るタイミング、発生条件、分析・評価等について検証し、リスクとなり得るかを確定する。
G4	システム運用担当者は、運用業務実施責任者と共にリスクに対して、回避・低減・転嫁・受容の対策案を検討、決定する。 またシステム運用だけでは対応が難しい場合、SOC担当者または保守業務担当者とエスカレーションして検討を進める。
G5	システム運用担当者は、リスクに対する対策案記入のため、「リスク管理台帳」を更新する。
G6	システム運用担当者は、主体となってリスクに対する対策案を実施する。
G7	システム運用担当者は、リスクが局限したか否かを判断する。
G8	システム運用担当者は、リスクが実際に現実のものとなっていないか、状況を観察する。
G9	システム運用担当者は、リスクが顕在化したか否かを判断する。 顕在化した場合、「課題管理」にて対応を行う。
G10	システム運用担当者は、リスクが顕著化した場合、その旨を運用業務実施責任者に報告する。
G11	システム運用担当者は、対象リスクについて、「リスク管理台帳」のステータスをクローズとする。
G12	システム運用担当者は、対象リスクについて、「リスク管理台帳」のステータスをクローズとする。
H1	SOC担当者は、リスクが予測された場合、運用業務実施責任者に対策の依頼をする。
H2	SOC担当者は、必要に応じて運用業務実施責任者およびシステム運用担当者と連携し、想定されるリスクが発生し得るタイミング、発生条件、分析・評価等について検証し、リスクとなり得るかを確定する。
H3	SOC担当者は、必要に応じて運用業務実施責任者およびシステム運用担当者と連携し、リスクに対して、回避・低減・転嫁・受容の対策案を検討、決定する。
H4	SOC担当者は、リスクに対する対策案を実施する。
I1	CSIRT担当者は、リスクが予測された場合、運用業務実施責任者に対策の依頼をする。
I2	CSIRT担当者は、必要に応じて運用業務実施責任者およびシステム運用担当者と連携し、想定されるリスクが発生し得るタイミング、発生条件、分析・評価等について検証し、リスクとなり得るかを確定する。
I3	CSIRT担当者は、必要に応じて運用業務実施責任者およびシステム運用担当者と連携し、リスクに対して、回避・低減・転嫁・受容の対策案を検討、決定する。
J1	保守業務担当者は、必要に応じて運用業務実施責任者およびシステム運用担当者と連携し、リスクに対して、回避・低減・転嫁・受容の対策案を検討、決定する。
J2	保守業務担当者は、リスクに対する対策案を実施する。

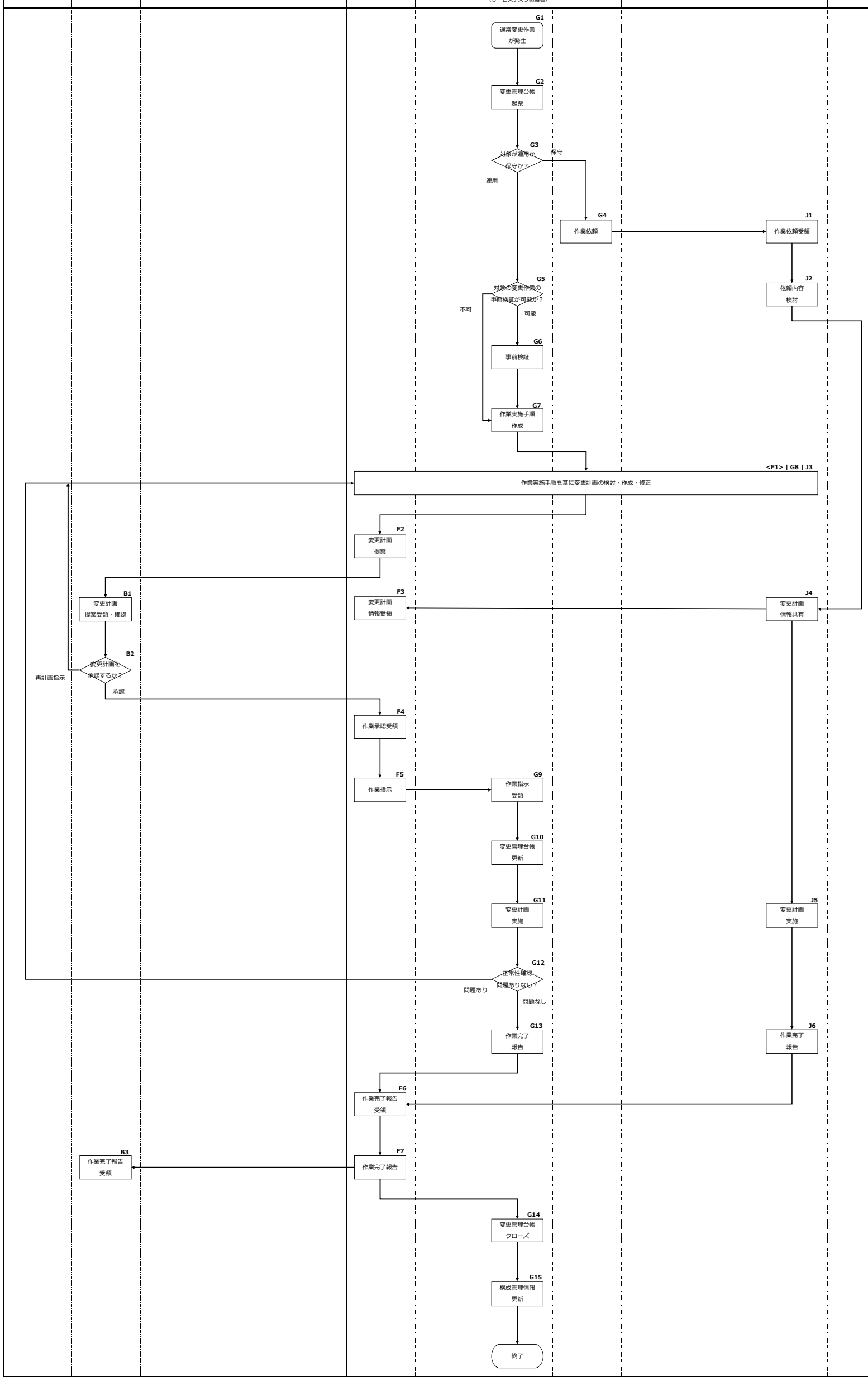
フロー名称	説明	作業トリガー
リスクと機会の特定・対策の実施	想定されるリスクとそのリスクが起こり得るタイミングの特定と対策、および経過観察を行うフローを示す。	・リスクが予測された場合

フロー名称	説明	作業トリガー
課題の抽出、対策立案、対応の実施	問題発生時の課題の整理と抽出、抽出した課題の立案と対応実施に関する業務フローを示す。	・問題の発生時 ・リスクが顕著化した時



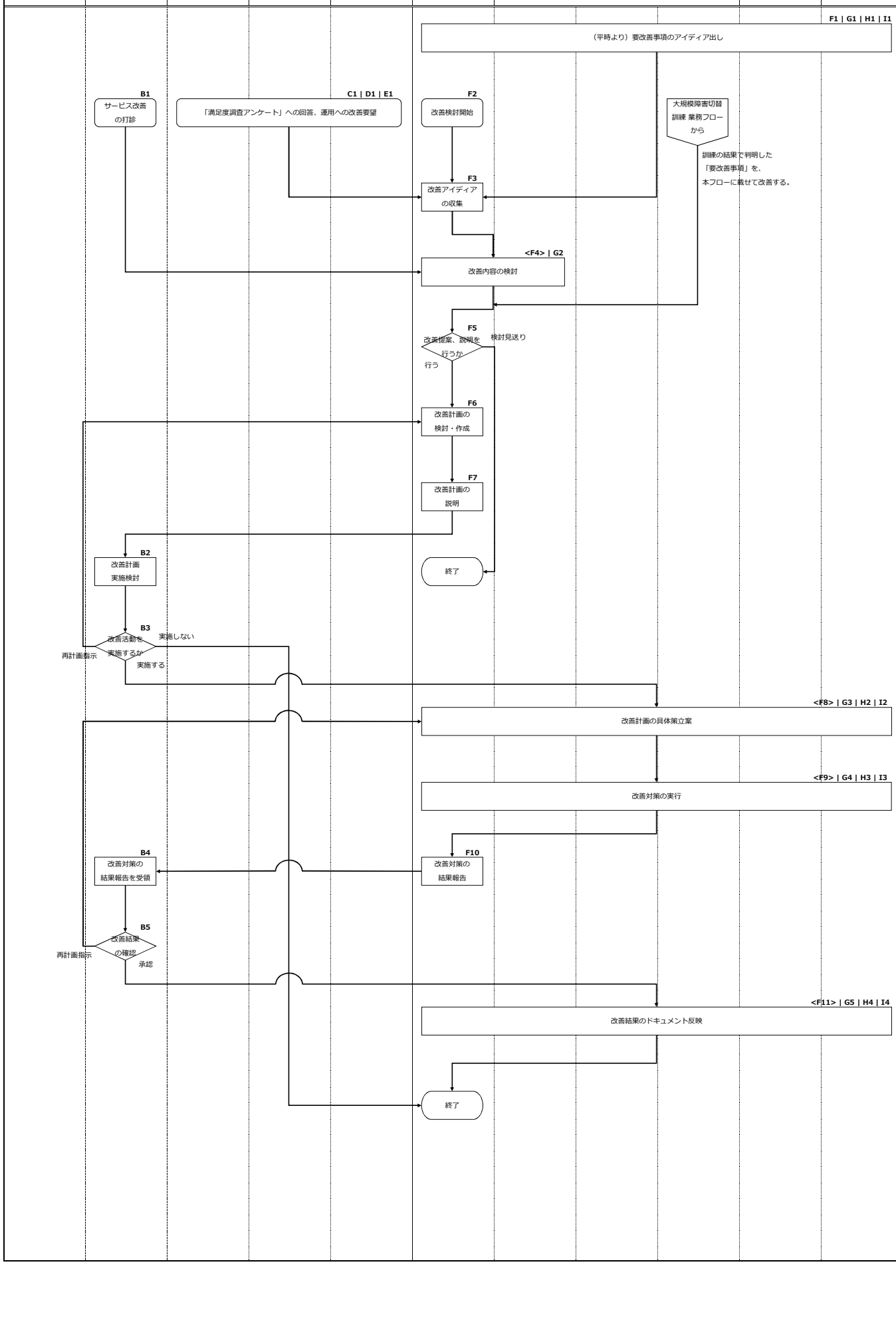
項番	説明
B1	システム管理者は、抽出した課題に対する対策案を運用業務実施責任者から受領し、対策案の内容を精査する。
B2	システム管理者は、運用業務実施責任者から提案された対策案を実施しても問題がないかを判断する。
B3	システム管理者は、運用業務実施責任者に対して提案された対策案を実施する指示を出す。
B4	システム管理者は、運用業務実施責任者から対策案の実施結果を受領する。
B5	システム管理者は、課題のクローズ可否を判断する。
B6	システム管理者は、運用業務実施責任者に課題対策完了の指示をする。
F1	運用業務実施責任者は、主体となってシステム運用担当者と共に問題に対する課題を整理・抽出する。
F2	運用業務実施責任者は、主体となってシステム運用担当者と共に抽出した課題に対して対策案を検討する。 またシステム運用のみで対応できない場合、SOC担当者または保守業務担当者とエスカレーションしながら対策案を検討する。
F3	運用業務実施責任者は、システム管理者に対して随時課題に対する対策案を提示する。
F4	運用業務実施責任者は、システム管理者から対策案の実施指示を受領する。
F5	運用業務実施責任者は、対策案実施後に対策の効果が出ているか否かを判断する。
F6	運用業務実施責任者は、システム管理者に対して対策案の実施結果（効果）を報告する。
F7	運用業務実施責任者は、システム管理者から対策案の実施指示を受領する。実施責任者は、システム管理者から課題対策完了指示を受領する。
F8	運用業務実施責任者は、システム運用担当者に「課題管理表」のクロース指示をする。
G1	システム運用担当者は、問題が発生した場合、課題の洗い出しを開始する。
G2	システム運用担当者は、運用業務実施責任者と共に問題に対する課題を整理・抽出する。
G3	システム運用担当者は、抽出した課題を「課題管理表」に起票する。
G4	システム運用担当者は、運用業務実施責任者と共に抽出した課題に対して対策案を検討する。 またシステム運用のみで対応できない場合、SOC担当者または保守業務担当者とエスカレーションしながら対策案を検討する。
G5	システム運用担当者は、対策案の検討結果を記載するため、「課題管理表」を更新する。
G6	システム運用担当者は、主体となって対策案を実施する。
G7	システム運用担当者は、主体となって対策案実施後にその効果が出ているかを精査する。
G8	システム運用担当者は、対策案実施結果を記載するため、「課題管理表」を更新する。
G9	システム運用担当者は、「課題管理表」のステータスをクローズにする。
H1	SOC担当者は、必要に応じて運用業務実施責任者及びシステム運用担当者と連携し、抽出した課題に対して対策案を検討する。
H2	SOC担当者は、対策案を実施する。
H3	SOC担当者は、対策案実施後にその効果が出ているかを精査する。
J1	保守業務担当者は、必要に応じて運用業務実施責任者及びシステム運用担当者と連携し、抽出した課題に対して対策案を検討する。
J2	保守業務担当者は、対策案を実施する。
J3	保守業務担当者は、対策案実施後にその効果が出ているかを精査する。

フロー名称	説明	作業トリガー
システム変更に係る変更・リリース対応	事前に作業内容・手順・影響・切り戻し作業を確認し、変更計画を作成し承認を得てから実施する変更・リリース作業を示すものである。	・通常変更作業が発生



項番	説明
B1	システム管理者は、運用業務実施責任者からの変更計画の提案を受領し、内容の確認を行う。
B2	システム管理者は変更計画を精査後に、作業を「承認」するか、 「再計画指示」として再計画を指示するかの判断をする。 ・「承認」の場合、「作業承認受領」へ ・「再計画指示」の場合は、「手順を基に変更計画の検討・作成・修正」へ
B3	システム管理者は、運用業務実務責任者より変更計画の作業完了報告を受領する。
F1	運用業務実施責任者が主体となり、システム運用担当者、保守業務担当者と協力して、作業実施手順を基に変更計画の検討(例:作業日、リリース内容、作業者、切り戻し、完了条件を検討)・作成・修正を行う。
F2	運用業務実施責任者は、システム管理者に変更計画の提案を行う。
F3	運用業務実施責任者は、保守業務担当者からの変更計画の情報を受領する。
F4	運用業務実施責任者は、システム管理者からの変更計画の作業承認を受領する。
F5	運用業務実施責任者は、システム運用担当者に変更計画の作業指示を行う。
F6	運用業務実施責任者はシステム運用担当者又は保守業務担当者より作業完了報告を受領する。
F7	運用業務実施責任者は、システム管理者に変更計画の作業完了報告を行う。
G1	■通常変更作業：標準変更でも緊急変更でもないすべての変更 以下に示す事前に標準化されていない変更作業を対象とする。 <例示> ・その他問合せ等に伴う設定変更、導入作業の対応 ・ペネトレーションテストの事前環境準備作業、事後環境戻し作業の対応
G2	システム運用担当者は、通常変更作業が発生した場合、変更管理台帳を起票する。(変更ID、変更概要、詳細、理由・目的、対象、変更の種類「通常変更」、ステータスを「作業準備」と入力する) ※変更管理台帳を必要に応じて更新する。
G3	システム運用担当者は 対象が「運用」か「保守」かの判定を行う。 「運用」の場合、「対象の変更作業の事前検証が可能か？」へ 「保守」の場合は、保守業務担当者へ「作業依頼」を行う ※基本的には、システム変更は保守業務担当者が行うが、例外的に協議や手順書の有無等により作業担当部署が変わる場合がある。 ※保守で運用に依頼したい作業の場合は、手順書を連携して運用に依頼する場合がある。
G4	システム運用担当者は、保守業務担当者へ変更作業の作業依頼を行う。
G5	システム運用担当者は、 事前検証が「可能」か「不可」の確認を行う。 「可能」の場合、「事前検証」へ 「不可」の場合、「作業実施手順作成」へ
G6	システム運用担当者は、対応作業の事前検証を行う。
G7	システム運用担当者は、対応作業の作業実施手順の作成を行う。
G8	システム運用担当者は、運用業務実施責任者の指揮のもと、保守業務担当者に協力を仰ぎながら、作業実施手順を基に変更計画の検討(例:作業日、リリース内容、作業者、切り戻し、完了条件)・作成・修正を行う。
G9	システム運用担当者は、運用業務実施責任者からの作業指示を受領する。
G10	システム運用担当者は、変更管理台帳のステータスを「承認済み」に更新する。
G11	システム運用担当者は、作成した変更計画を基に変更作業を実施する。
G12	システム運用担当者は正常性確認作業を行い、 「問題なし」の場合、「作業完了報告」へ 「問題あり」の場合は、「作業実施手順を基に変更計画の検討・作成・修正」へ
G13	システム運用担当者は運用業務実施責任者に、作業完了報告を行う。(作業エビデンスを添付する)
G14	システム運用担当者は変更管理台帳をクローズする。(クローズ日、ステータスを「作業完了」と入力する)
G15	システム運用担当者は構成管理情報の更新を行う。(システム設定書、システム構成書)
J1	保守業務担当者は、システム運用担当者より変更作業の作業依頼を受領する。
J2	保守業務担当者は、変更作業の依頼内容の検討を行う。
J3	保守業務担当者は、運用業務実施責任者の指揮のもと、手順を基にシステム運用担当者が行う変更計画の検討(例:作業日、リリース内容、作業者、切り戻し、完了条件)・作成・修正の支援を行う。
J4	保守業務担当者は、運用業務実施責任者に作成した変更計画の情報共有を行う。
J5	保守業務担当者は、作成した変更計画を基に変更作業を実施する。
J6	保守業務担当者は運用業務実施責任者に、作業完了報告を行う。(作業エビデンスを添付する)

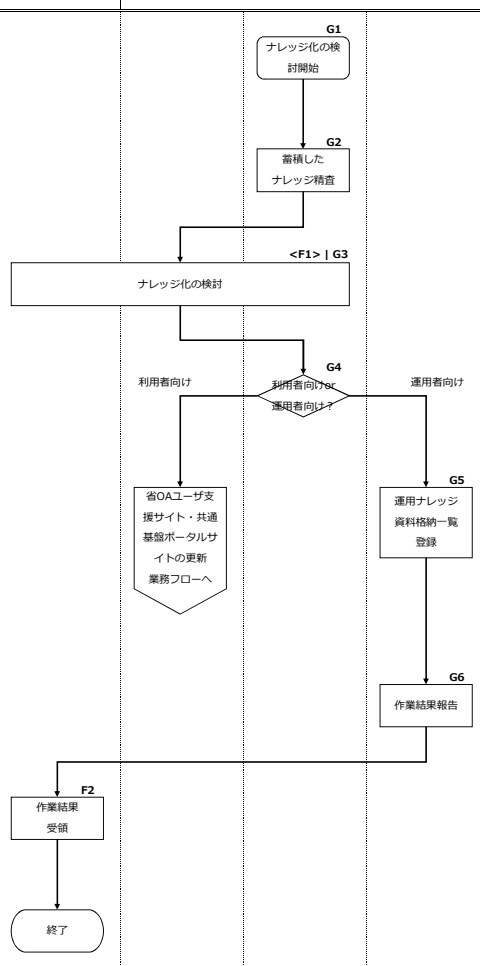
フロー名称	説明	作業トリガー
継続的サービス改善管理	運用保守業務の品質向上のため、継続的に業務改善を行う。	月次や年次報告、大規模障害切替訓練実施後のタイミングに合わせ検討を行う。 また、システム管理者に改善を求められた場合や利用者からの 「満足度アンケート」回答内容や問合せ内容に要改善事項があった際にも実施する。



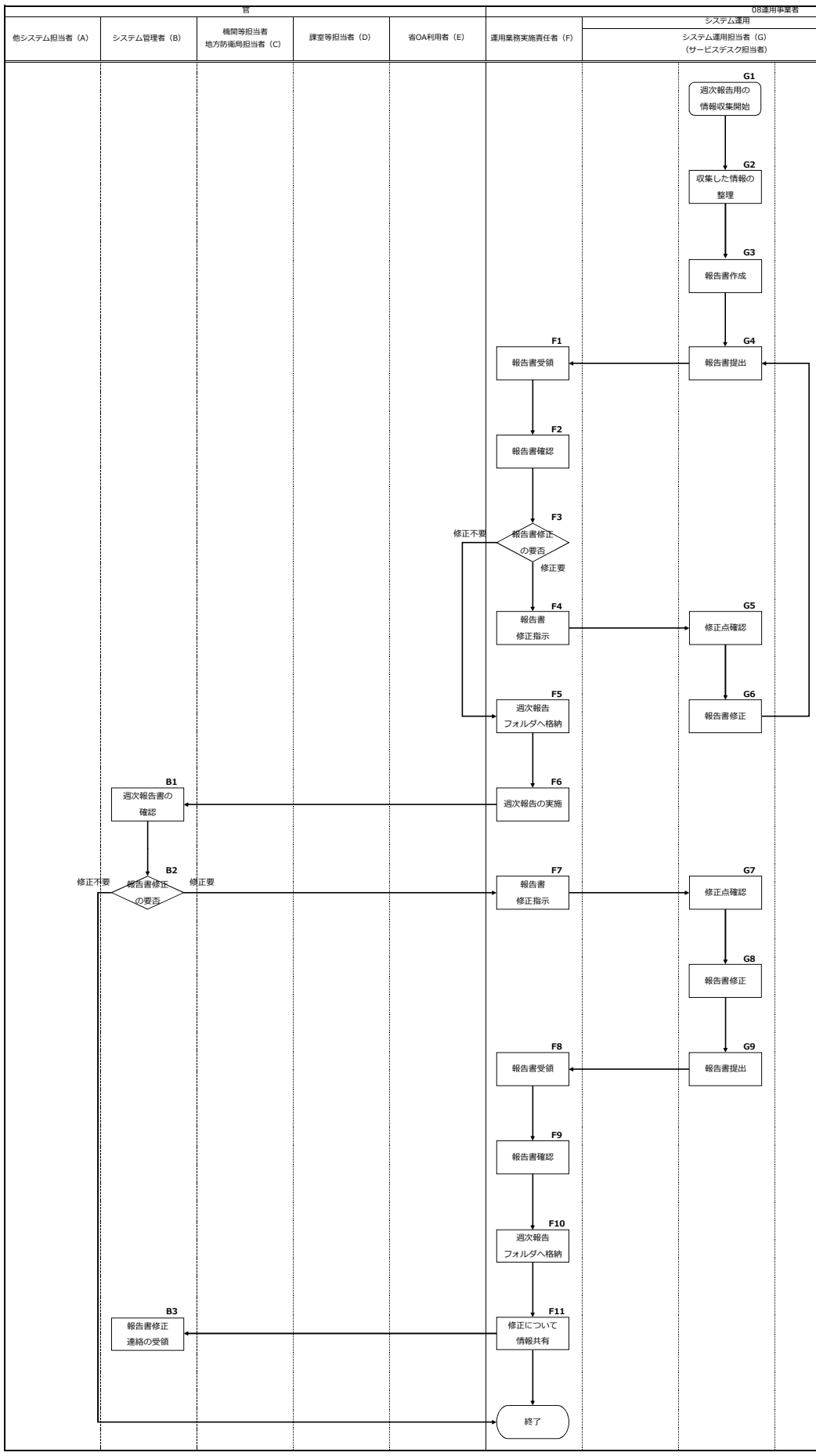
項番	説明
B1	システム管理者は、運用業務に関してサービス改善が必要と判断した場合、その打診を行う。
B2	システム管理者は、運用実施責任者から提案を受けた改善計画の内容を検討し、改善活動を行うか判断を行う。
B3	システム管理者は、改善提案に対して、以下の判断を行う。 ・実施する：改善活動の実行を承認する。 ・実施しない：改善活動を実行しない ・再計画指示：提案された計画内容の部分修正が必要と判断した際は、その旨を指示する。
B4	システム管理者は、運用業務実施責任者から改善活動の実施状況の報告を受け、目的とした改善がなされているか確認する。
B5	システム管理者は、この改善活動の取り組み結果について承認を行うか判断する。 ・承認：改善活動の成果が当初目標とした水準以上であった場合、今回の活動を終了することを承認する。 ・再計画指示：改善活動の成果が当初目標とした水準に達していない場合、改善活動の具体的計画の段階から再度やり直すように指示する。
C1	機関等担当者、地方防衛局担当者は、年次で実施されるサービスデスクに対する「満足度調査アンケート」に回答する。 また、サービスデスクへの問い合わせを通じて改善要望を出す。
D1	課室等担当者は、年次で実施されるサービスデスクに対する「満足度調査アンケート」に回答する。 また、サービスデスクへの問い合わせを通じて改善要望を出す。
E1	省OA利用者は、年次で実施されるサービスデスクに対する「満足度調査アンケート」に回答する。 また、サービスデスクへの問い合わせを通じて改善要望を出す。
F1	運用業務実施責任者は、日々の運用業務を進める中で、運用の効率化や品質向上、業務負荷削減などを目的とした要改善事項（業務の進め方、台帳の記載の仕方、報告の仕方、利用者への対応方法等）の抽出を意識する。 必要に応じ、各担当者は気づきをメモするなど、検討実施に備える。
F2	運用業務実施責任者は、月次報告及び年次報告のタイミングで、報告の一環としてサービス改善提案を実施する。
F3	運用業務実施責任者は、提案に資する改善アイディアが無いか08運用事業者内のメンバーに確認を行う。 また、年次で実施される各利用者からの「満足度調査アンケート」回答内容から、業務上の改善事項とすべき内容が含まれていないかも確認する。
F4	運用業務実施責任者はシステム運用担当者を指揮して、集まったアイディアを基に実現可能性や効果の検討を行う。
F5	運用業務実施責任者は、検討の結果、今回の報告タイミングで改善提案を行うか判断する。 ・システム管理者の打診で検討を開始した際は、検討結果の報告を行う。 ・発生している事象の優先度付けを行い、比較的対応優先度の低いものは今回の検討は見送りとする。
F6	運用業務実施責任者は、官に説明するための改善計画を作成する。この時点では、提案する内容によるが、説明のための概略的な計画程度でもよい。官の指示により改善計画の作成、修正を行う場合は、その指示内容に沿って計画を作成する。
F7	運用業務実施責任者は、業務改善の内容をシステム管理者に対して説明を行い、改善実施に当たっての実行許可を得る。
F8	関連メンバー（システム運用担当者、SOC担当者、CSIRT担当者）は、運用業務実施責任者の指揮の下で、改善計画の実施に向け対応内容を具体的に立案する。
F9	運用業務実施責任者は、改善計画に沿って、改善活動を実行する。随時、改善計画の実施状況を確認し、効果測定を行う。
F10	運用業務実施責任者は、月次報告等のタイミング（他、必要に応じ随時）で、改善の実施結果の報告をシステム管理者に対して行う。
F11	運用業務実施責任者は、一連の改善活動の結果を踏まえ、関連するドキュメントの更新（設計書やマニュアルを想定）を行う。
G1	システム運用担当者は、日々の運用業務を進める中で、運用の効率化や品質向上、業務負荷削減などを目的とした要改善事項（業務の進め方、台帳の記載の仕方、報告の仕方、利用者への対応方法等）の抽出を意識する。 必要に応じ、各担当者は気づきをメモするなど、検討実施に備える。
G2	システム運用担当者は運用業務実施責任者の指揮の下で、集まったアイディアを基に実現可能性や効果の検討を行う。
G3	関連メンバー（システム運用担当者、SOC担当者、CSIRT担当者）は、運用業務実施責任者の指揮の下で、改善計画の実施に向け対応内容を具体的に立案する。
G4	システム運用担当者は、運用業務実施責任者の指揮の下で、改善計画に沿って、改善活動を実行する。
G5	システム運用担当者は、運用業務実施責任者の指示を受け関連するドキュメントの更新（設計書やマニュアルを想定）を行う。
H1	SOC担当者は、日々の運用業務を進める中で、運用の効率化や品質向上、業務負荷削減などを目的とした要改善事項（業務の進め方、台帳の記載の仕方、報告の仕方、利用者への対応方法等）の抽出を意識する。必要に応じ、各担当者は気づきをメモするなど、検討実施に備える。
H2	関連メンバー（システム運用担当者、SOC担当者、CSIRT担当者）は、運用業務実施責任者の指揮の下で、改善計画の実施に向け対応内容を具体的に立案する。
H3	SOC担当者は、運用業務実施責任者の指揮の下で、改善計画に沿って、改善活動を実行する。
H4	SOC担当者は、運用業務実施責任者の指示を受け関連するドキュメントの更新（設計書やマニュアルを想定）を行う。
I1	CSIRT担当者は、日々の運用業務を進める中で、運用の効率化や品質向上、業務負荷削減などを目的とした要改善事項（業務の進め方、台帳の記載の仕方、報告の仕方、利用者への対応方法等）の抽出を意識する。必要に応じ、各担当者は気づきをメモするなど、検討実施に備える。
I2	関連メンバー（システム運用担当者、SOC担当者、CSIRT担当者）は、運用業務実施責任者の指揮の下で、改善計画の実施に向け対応内容を具体的に立案する。
I3	CSIRT担当者は、運用業務実施責任者の指揮の下で、改善計画に沿って、改善活動を実行する。
I4	CSIRT担当者は、運用業務実施責任者の指示を受け関連するドキュメントの更新（設計書やマニュアルを想定）を行う。

付表９　業務フロー（続き）
ナレッジの収集、分析・抽出、報告、活用（続き）

フロー名称	説明	作業トリガー
ナレッジの収集、分析・抽出、報告、活用	インシデント管理で蓄積した運用業務対応履歴を精査・検討のうえで選抜し、 「ナレッジ」として登録・活用することで、運用業務の効率化を図る。 また、問い合わせ内容から件数の多いもの、他有用と判断したものを 利用者向けのQ&Aとして公開することで、利用者の利便性向上を図る。	確認時期到来により検討を開始する

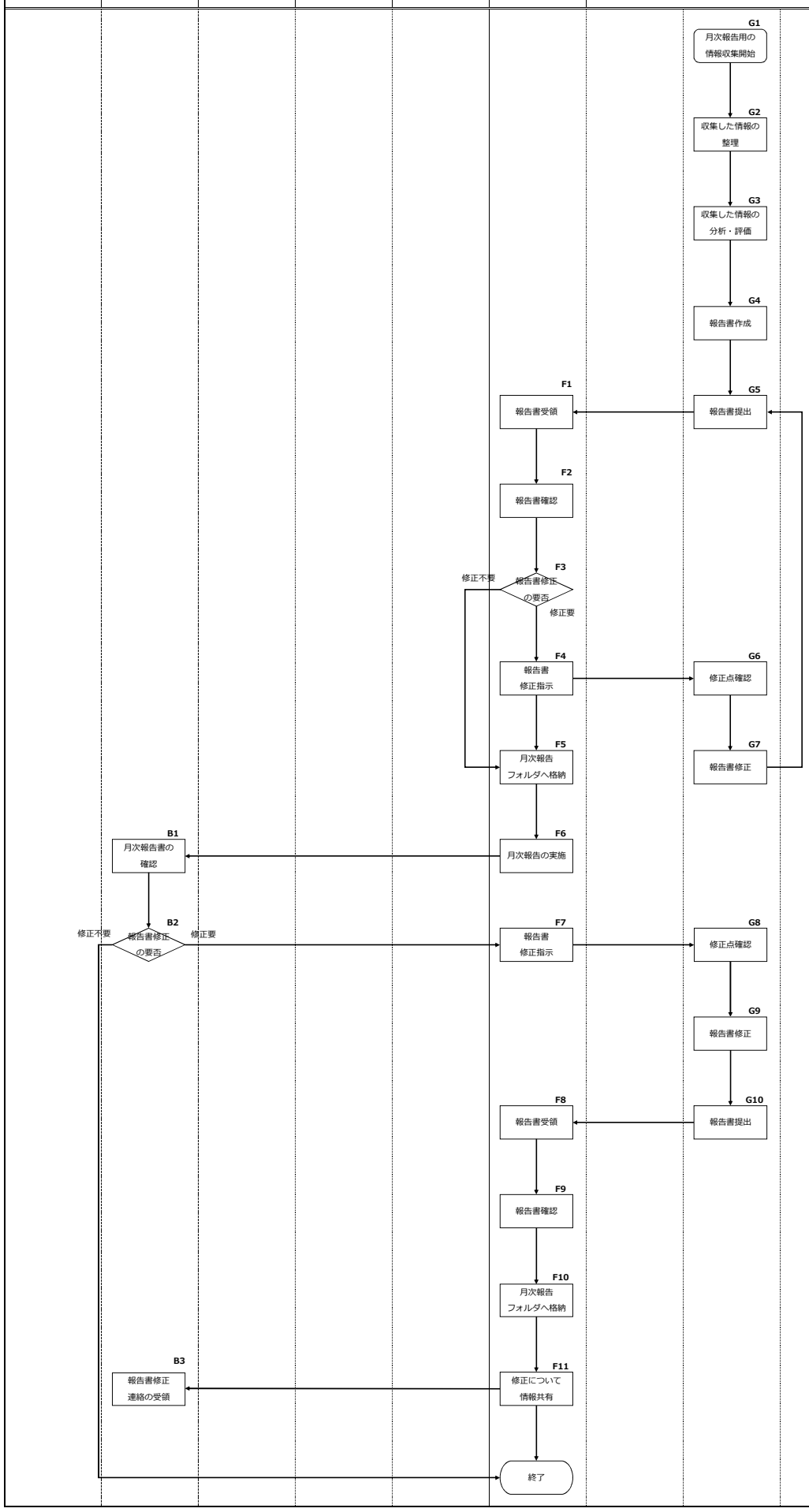
官					08運用事業者					その他事業者		項番	説明
他システム担当者（A）	システム管理者（B）	機関等担当者 地方防衛局担当者（C）	課室等担当者（D）	省OA利用者（E）	運用業務実施責任者（F）	システム運用 システム運用担当者（G） （サービスデスク担当者）		セキュリティ運用 SOC担当者（H）	 CSIRT担当者（I）	保守業務担当者（J）	データセンタ事業者（K）		
											F1	運用業務実施責任者が主体となり、日々蓄積したナレッジの精査後に、ナレッジを取り入れるか？取り入れないかの？検討を共に行う。 検討の結果、取り入れることが決まったナレッジについて、手順の作成が必要な場合は、作成を行う。
												F2	運用業務実施責任者は、システム運用担当者より運用ナレッジを登録した作業結果を受領する。
												G1	システム運用担当者は日々蓄積されたナレッジを基に、検討を開始する。 (1ヵ月に1回を想定) 収集元は以下 ・インシデント管理機能 ・変更管理台帳
												G2	システム運用担当者は収集したナレッジ情報の精査を行う。 インシデントのナレッジ、問合せのナレッジ、変更・リリースのナレッジをシステム運用で必要なナレッジか？利用者に必要なナレッジか？精査を行う。 以下は精査例 ■運用で必要なナレッジ精査 ・同様のインシデントが多発したので、対応作業を運用ナレッジに登録の精査 ・監視アラートの内容が同じで対処が同じため、運用ナレッジに登精精査 ・変更・リリース対応で作業がパターン化できるものを運用ナレッジに登録の精査 ■利用者に必要なナレッジ精査 ・同じ問い合わせが頻発しているので、ユーザ支援サイトの掲載の精査 ・大規模人事異動に向けて、問い合わせの傾向を以前の情報から抽出して、あらかじめユーザ支援サイトへの掲載の精査
												G3	システム運用担当者は日々蓄積したナレッジの精査後に、ナレッジを取り入れるか？取り入れないかの？検討を共に行う。 検討の結果、取り入れることが決まったナレッジについて、手順の作成が必要な場合は、作成を行う。
												G4	システム運用担当者は取り入れることが決定したナレッジの内、利用者向けor運用者向けかの判定を行う ・「利用者向け」取り入れの場合、「省OAユーザ支援サイト・共通基盤ポータルサイトの更新　業務フローへ」へ ・「運用者向け」取り入れの場合、「運用ナレッジ登録」へ
												G5	システム運用を行う上で有用なナレッジを、OneNote「運用ナレッジ資料格納一覧」に運用チーム向けナレッジとして登録する。ナレッジ番号、ナレッジ名、概要、資料名、手順書名、リンクを登録する。 SharePoint上の所定の格納場所にナレッジ番号でフォルダを切り、資料、作成した場合は手順書を配置する。 ※「運用ナレッジ資料格納一覧」の見直しは、随時行う。
												G6	システム運用担当者は作業結果を、運用業務実施責任者に報告する。

フロー名称	説明	作業トリガー
週次報告作成	週次におけるシステム運用状況を正確に把握するため 運用実績を収集・精査し、週次報告書を作成・共有し報告会を実施およびその完了までのフローを示す	週次処理



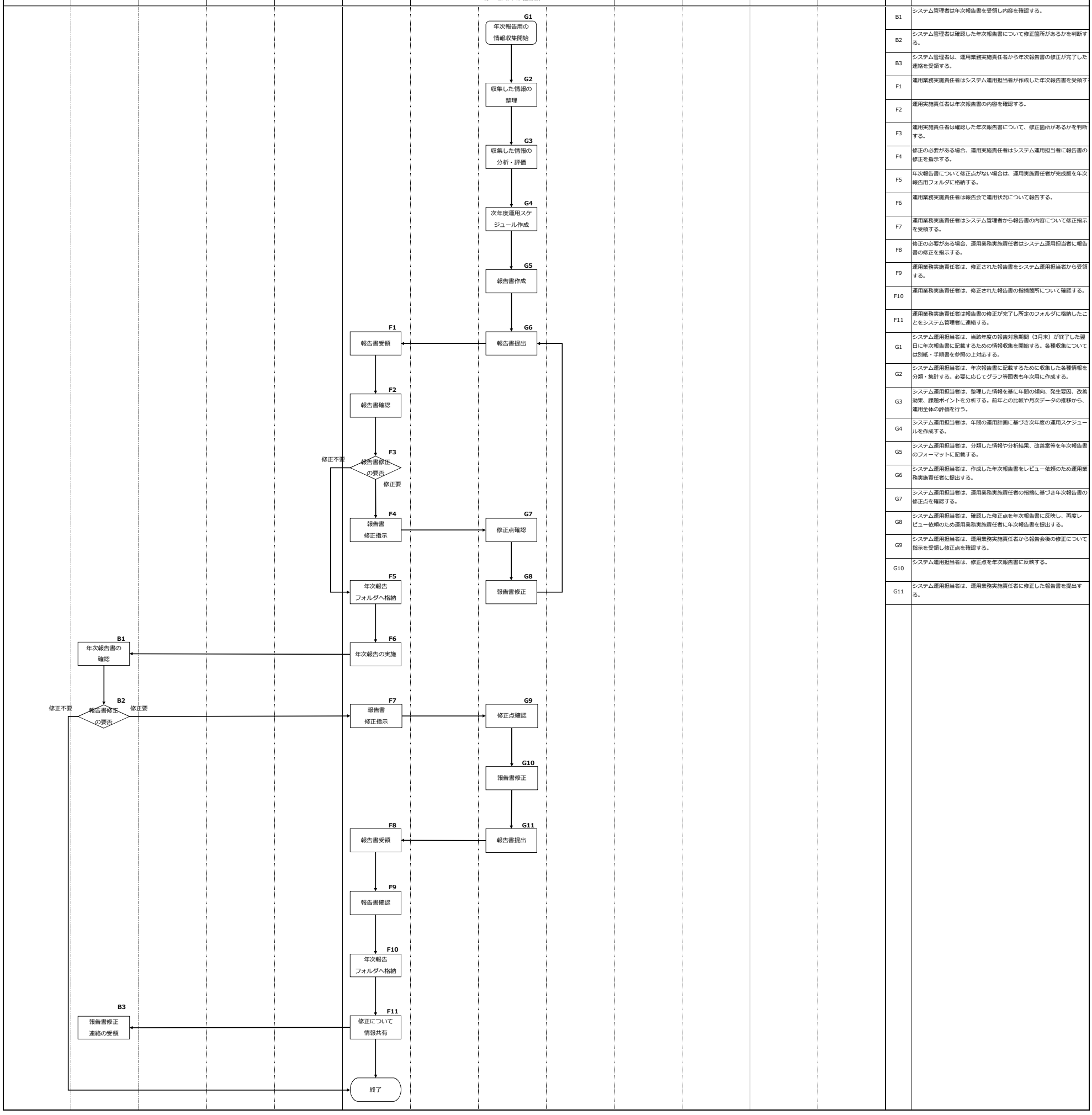
項番	説明
B1	システム管理者は週次報告書を受領し内容を確認する。
B2	システム管理者は確認した週次報告書について修正箇所があるかを判断する。
B3	システム管理者は、運用業務実施責任者から週次報告書の修正が完了した連絡を受領する。
F1	運用業務実施責任者はシステム運用担当者が作成した週次報告書を受領する。
F2	運用業務実施責任者は週次報告書の内容を確認する。
F3	運用業務実施責任者は確認した週次報告書について、修正箇所があるかを判断する。
F4	修正の必要がある場合、運用業務実施責任者はシステム運用担当者に報告書の修正を指示する。
F5	週次報告書について修正点がない場合は、運用業務実施責任者が完成版を週次報告用フォルダに格納する。
F6	運用業務実施責任者は報告会で運用状況について報告する。
F7	運用業務実施責任者はシステム管理者から報告書の内容について修正指示を受領する。
F8	修正の必要がある場合、運用業務実施責任者はシステム運用担当者に報告書の修正を指示する。
F9	運用業務実施責任者は、修正された報告書をシステム運用担当者から受領する。
F10	運用業務実施責任者は、修正された報告書の指摘箇所について確認する。
F11	運用業務実施責任者は報告書の修正が完了し所定のフォルダに格納したことをシステム管理者に連絡する。
G1	システム運用担当者は、当該週の報告対象期間が終了した翌日に週次報告書に記載するための情報収集を開始する。各種収集については別紙・手順書を参照の上対応する。
G2	システム運用担当者は、週次報告書に記載するために収集した各種情報を必要に応じて分類する。
G3	システム運用担当者は、分類した情報を基に週次報告書のフォーマットに記載する。
G4	システム運用担当者は、作成した週次報告書をレビュー依頼のため運用業務実施責任者に提出する。
G5	システム運用担当者は、運用業務実施責任者の指摘に基づき週次報告書の修正点を確認する。
G6	システム運用担当者は、確認した修正点を週次報告書に反映し、再度レビュー依頼のため運用業務実施責任者に週次報告書を提出する。
G7	システム運用担当者は、運用業務実施責任者から報告会後の修正について指示を受領し修正点を確認する。
G8	システム運用担当者は、修正点を週次報告書に反映する。
G9	システム運用担当者は、運用業務実施責任者に修正した報告書を提出する。

フロー名称	説明	作業トリガー
月次報告作成	月次におけるシステム運用状況を把握するため、1か月間の運用実績を集計・分析し問合せの傾向、SLA達成状況などの月次分析項目を含めて月次報告書を作成・共有し報告会を実施およびその完了までのフローを示す	月次処理



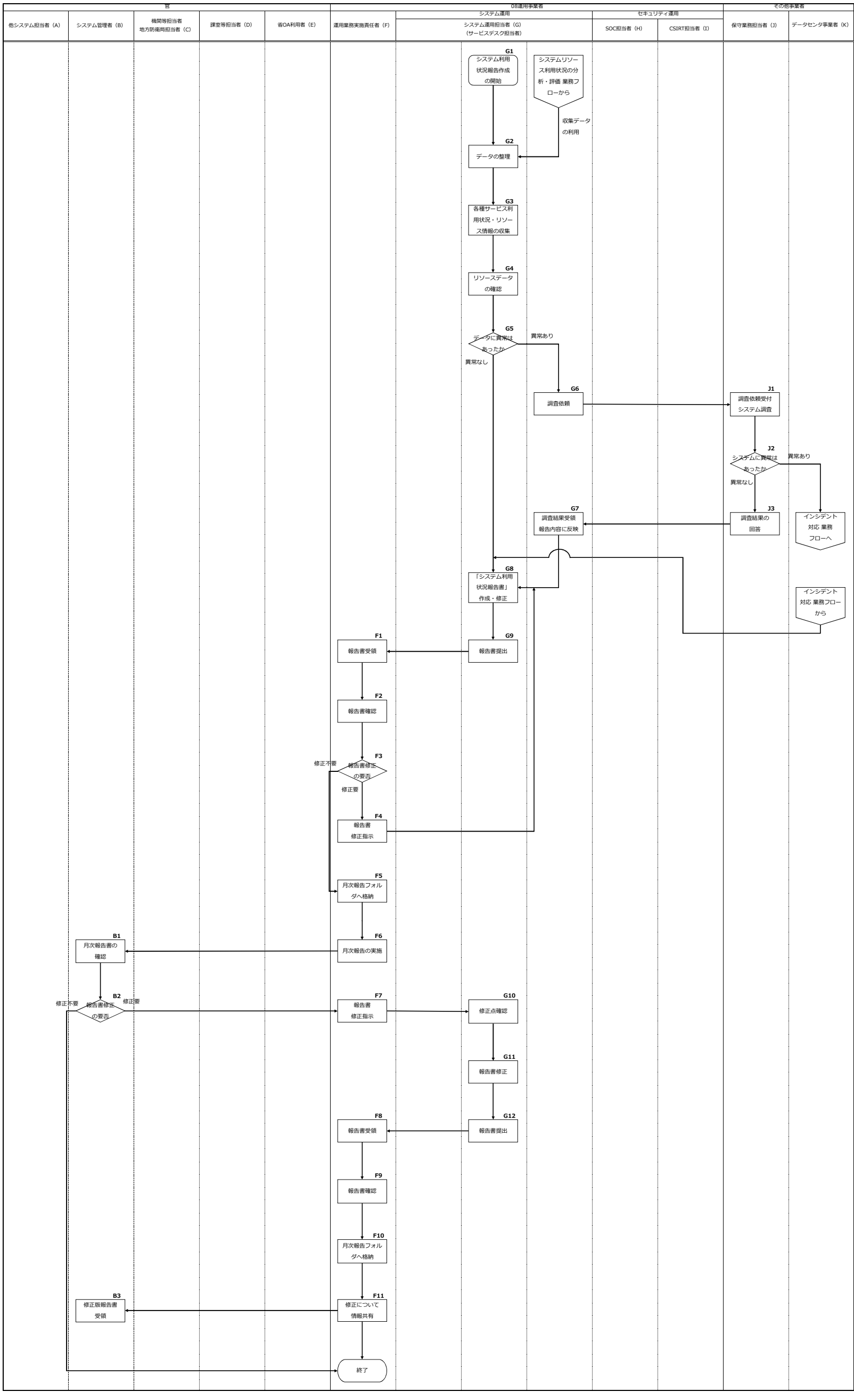
項番	説明
B1	システム管理者は月次報告書を受領し内容を確認する。
B2	システム管理者は確認した月次報告書について修正箇所があるかを判断する。
B3	システム管理者は、運用業務実施責任者から月次報告書の修正が完了した連絡を受領する。
F1	運用業務実施責任者はシステム運用担当者が作成した月次報告書を受領する。
F2	運用業務実施責任者は月次報告書の内容を確認する。
F3	運用業務実施責任者は確認した月次報告書について、修正箇所があるかを判断する。
F4	修正の必要がある場合、運用業務実施責任者はシステム運用担当者に報告書の修正を指示する。
F5	月次報告書について修正点がない場合は、運用業務実施責任者が完成版を月次報告用フォルダに格納する。
F6	運用業務実施責任者は報告会で運用状況について報告する。
F7	運用業務実施責任者はシステム管理者から報告書の内容について修正指示を受領する。
F8	修正の必要がある場合、運用業務実施責任者はシステム運用担当者に報告書の修正を指示する。
F9	運用業務実施責任者は、修正された報告書をシステム運用担当者から受領する。
F10	運用業務実施責任者は、修正された報告書の指摘箇所について確認する。
F11	運用業務実施責任者は報告書の修正が完了し所定のフォルダに格納したことをシステム管理者に連絡する。
G1	システム運用担当者は、当該月の報告対象期間（当月末）が終了した翌日に月次報告書に記載するための情報収集を開始する。各種収集については別紙・手順書を参照の上対応する。
G2	システム運用担当者は、月次報告書に記載するために収集した各種情報を分類する。必要に応じてグラフ等図表も作成する。
G3	システム運用担当者は、収集した情報を月次報告書に記載するために分析・評価する。問合せ傾向や前月比、障害の原因分析、SLAの達成状況の確認を実施する。
G4	システム運用担当者は、分類した情報やグラフ等図表類、分析結果を月次報告書のフォーマットに記載する。
G5	システム運用担当者は、作成した月次報告書をレビュー依頼のため運用業務実施責任者に提出する。
G6	システム運用担当者は、運用業務実施責任者の指摘に基づき月次報告書の修正点を確認する。
G7	システム運用担当者は、確認した修正点を月次報告書に反映し、再度レビュー依頼のため運用業務実施責任者に月次報告書を提出する。
G8	システム運用担当者は、運用業務実施責任者から報告会後の修正について指示を受領し修正点を確認する。
G9	システム運用担当者は、修正点を月次報告書に反映する。
G10	システム運用担当者は、運用業務実施責任者に修正した報告書を提出する。

フロー名称	説明	作業トリガー
年次報告作成	年度のシステム運用状況を総合的に把握することを目的とし、年間の運用実績を収集・精査した上で 年次報告書として作成・共有し報告会を実施およびその完了までのフローを示す	年次処理



項番	説明
B1	システム管理者は年次報告書を受領し内容を確認する。
B2	システム管理者は確認した年次報告書について修正箇所があるかを判断する。
B3	システム管理者は、運用業務実施責任者から年次報告書の修正が完了した連絡を受領する。
F1	運用業務実施責任者はシステム運用担当者が作成した年次報告書を受領する。
F2	運用実施責任者は年次報告書の内容を確認する。
F3	運用実施責任者は確認した年次報告書について、修正箇所があるかを判断する。
F4	修正の必要がある場合、運用実施責任者はシステム運用担当者に報告書の修正を指示する。
F5	年次報告書について修正点がない場合は、運用実施責任者が完成版を年次報告用フォルダに格納する。
F6	運用業務実施責任者は報告会で運用状況について報告する。
F7	運用業務実施責任者はシステム管理者から報告書の内容について修正指示を受領する。
F8	修正の必要がある場合、運用業務実施責任者はシステム運用担当者に報告書の修正を指示する。
F9	運用業務実施責任者は、修正された報告書をシステム運用担当者から受領する。
F10	運用業務実施責任者は、修正された報告書の指摘箇所について確認する。
F11	運用業務実施責任者は報告書の修正が完了し所定のフォルダに格納したことをシステム管理者に連絡する。
G1	システム運用担当者は、当該年度の報告対象期間（3月末）が終了した翌日に年次報告書に記載するための情報収集を開始する。各種収集については別紙・手順書を参照の上対応する。
G2	システム運用担当者は、年次報告書に記載するために収集した各種情報を分類・集計する。必要に応じてグラフ等図表も年次用に作成する。
G3	システム運用担当者は、整理した情報を基に年間の傾向、発生要因、改善効果、課題ポイントを分析する。前年との比較や月次データの推移から、運用全体の評価を行う。
G4	システム運用担当者は、年間の運用計画に基づき次年度の運用スケジュールを作成する。
G5	システム運用担当者は、分類した情報や分析結果、改善案等を年次報告書のフォーマットに記載する。
G6	システム運用担当者は、作成した年次報告書をレビュー依頼のため運用業務実施責任者に提出する。
G7	システム運用担当者は、運用業務実施責任者の指摘に基づき年次報告書の修正点を確認する。
G8	システム運用担当者は、確認した修正点を年次報告書に反映し、再度レビュー依頼のため運用業務実施責任者に年次報告書を提出する。
G9	システム運用担当者は、運用業務実施責任者から報告会後の修正について指示を受領し修正点を確認する。
G10	システム運用担当者は、修正点を年次報告書に反映する。
G11	システム運用担当者は、運用業務実施責任者に修正した報告書を提出する。

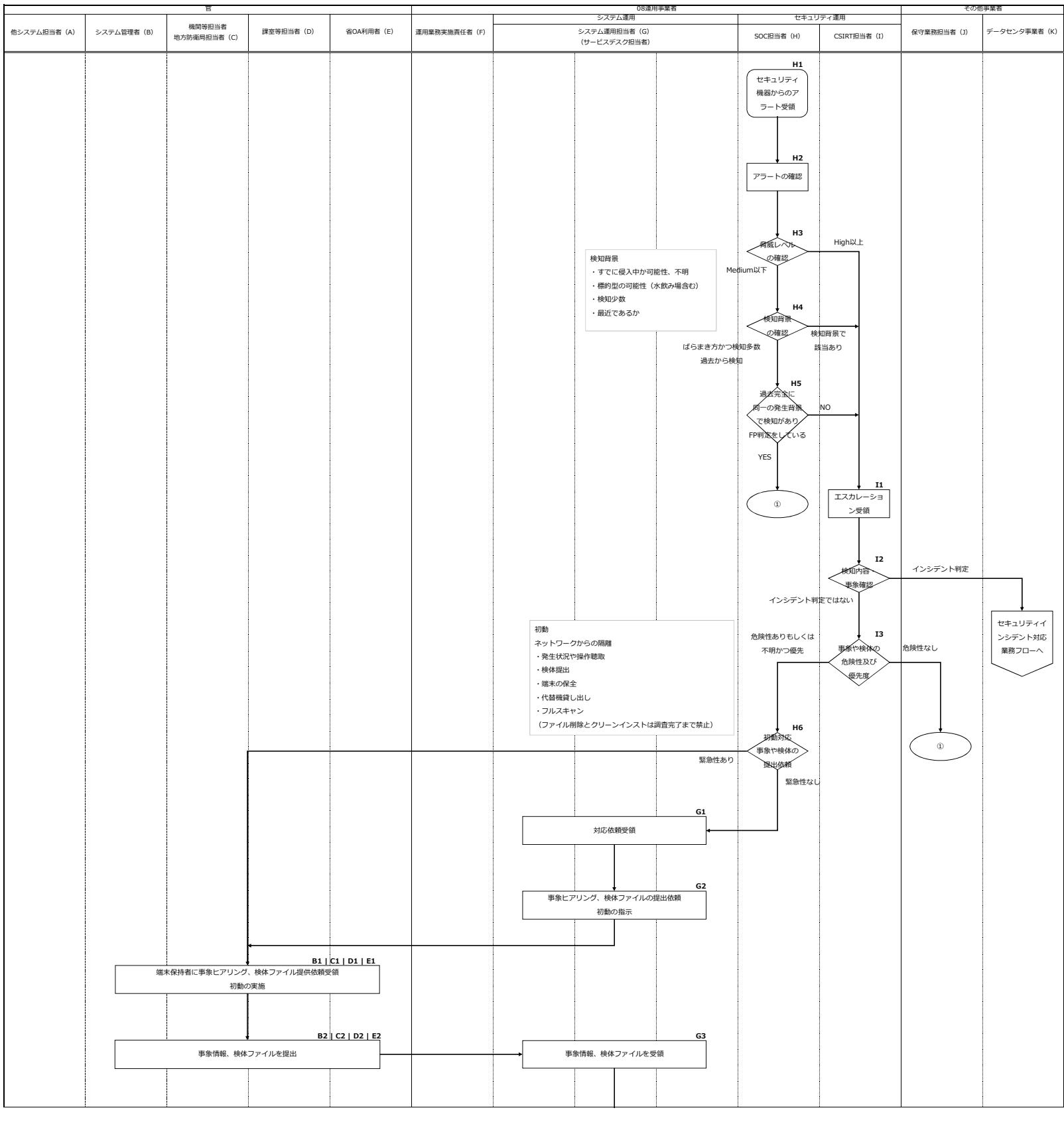
フロー名称	説明	作業トリガー
システム利用状況報告	月次報告を実施するために必要となる報告書の作成、確認、および提出の一連の手続きを示したものである。	月次処理



項番	説明
B1	システム管理者は、運用の健全性や安全性に問題がないか、また将来的なリスクの兆候がないかを把握する目的で、月次報告書を確認する。
B2	システム管理者は、報告書修正の要否を判断する。
B3	システム管理者は、月次報告会で指摘した修正版報告書を受領する。
F1	運用業務実施責任者は、システム運用担当者から提出された月次報告書を受領し、確認作業に向けて準備を行う。
F2	運用業務実施責任者は、受領した報告書の内容を精査し、 ・記載の正確性 ・分析内容の妥当性 ・報告書としての体裁 などを確認する。
F3	運用業務実施責任者は、確認内容をもとに 「報告書に修正が必要かどうか」を判断する。
F4	運用業務実施責任者は、報告書の修正をシステム運用者に指示する。
F5	運用業務実施責任者は、修正が不要、または修正後の報告書を確認して問題がないと判断した後、月次報告用フォルダ（管理フォルダ）へ正式版として格納する。
F6	運用業務実施責任者は、システム運用状況の情報共有を目的として、月次報告会を実施する。
F7	運用業務実施責任者は、運用業務実施責任者へ修正指示を行う。
F8	運用業務実施責任者は、システム運用担当者から提出された報告書を受領する。
F9	運用業務実施責任者は、受領した報告書の内容を最終確認する。
F10	運用業務実施責任者は、確認済みの報告書を月次報告フォルダに格納し、保管する。
F11	運用業務実施責任者は、修正について情報共有を実施する。
G1	システム運用担当者は、あらかじめ設定された日時トリガーによって、システム利用状況報告作成を開始する。
G2	システム運用担当者は、「システムリソース利用状況の分析・評価 業務フロー」等で収集したデータから、不要な項目やノイズを除きトレンド分析やスパイクが確認できるようにデータを整理・加工する。
G3	サーバOS、メール、Microsoft 365、Teams、ファイル共有、検索、端末、複合機、ライセンス、情報保全ログなど、各サービスの利用状況・リソース状況・パッチ適用状況を収集する。 容量・使用率・件数・上位利用状況・未適用状況・監査結果など、月次報告で必要となる指標をまとめる。
G4	システム運用担当者は、整形データに対し、リソース異常、容量の逼迫、利用状況の急変、パッチ未適用、ライセンス過不足、監査ログの異常増加など、サービス横断で異常兆候がないか確認する。
G5	各種リソースの確認結果、異常や懸念が認められた場合は 保守業務担当者へ調査を依頼する。
G6	システム運用担当者は、保守業務担当者に異常が認められたシステムリソースデータの調査を依頼する。
G7	システム運用担当者は、保守業務担当者から受領した調査結果を確認し、「システム利用状況報告書」の報告内容に反映する。
G8	システム運用担当者は、リソースデータの確認結果や保守業務担当者からの回答内容を基に、月次報告に含める「システム利用状況報告書」として適切なフォーマットに仕上げる。必要に応じて、過去月との比較、主要トピックの追記なども行う。 また、運用実施責任者の指示に沿って内容の修正も行う。
G9	システム運用担当者は、完成した報告書を管理者へ提出する。
G10	システム運用担当者は、運用業務実施責任者からの修正指示内容を確認し、指示された修正箇所を把握する。
G11	システム運用担当者は、修正指示に基づき報告書を修正し、内容を整備する。
G12	システム運用担当者は、修正後の報告書を運用業務実施責任者へ再提出する。
J1	保守業務担当者は、システム運用担当者からの調査依頼を受け付け、依頼された異常が認められたリソースデータの調査を行う。
J2	システム調査の確認結果、異常や懸念が認められた場合はインシデント対応フローに遷移する。
J3	保守業務担当者は、システム運用担当者に調査結果を回答する。

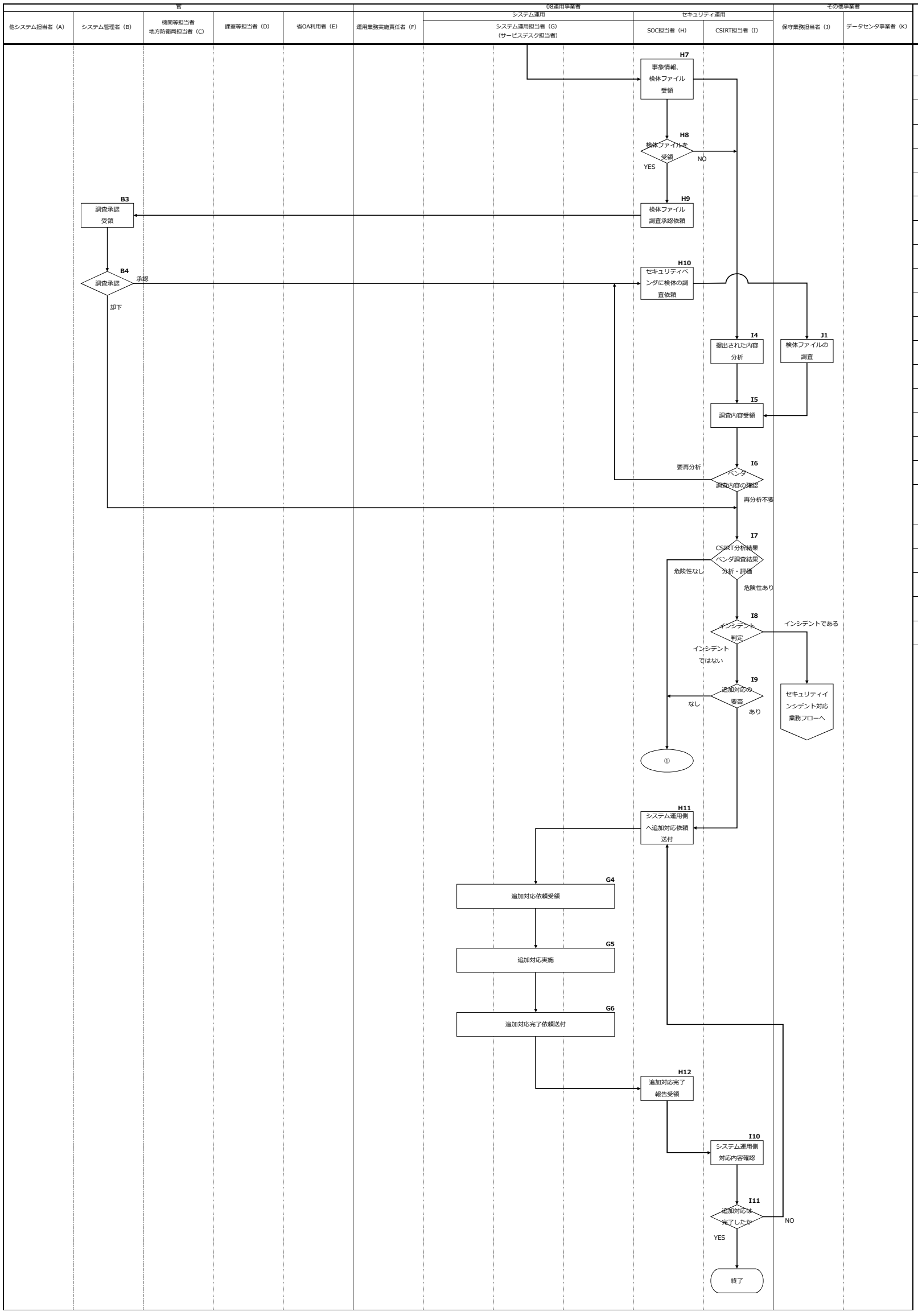
付表１０　業務フロー（続き）
セキュリティ監視と検知（続き）

フロー名称	説明	作業トリガー
セキュリティ監視と検知	各作業トリガーを契機とする24/365リアルタイム監視の業務フローを示す。	・セキュリティ監視機能によるアラートの受領



項番	説明
B1	システム管理者は、インシデント発生端末保持者にヒアリング、検体ファイルの提供依頼受領する。 また、初動の対応を実施する。
B2	システム管理者は、システム運用担当者へ、事象情報、検体ファイルの提出する。
B3	システム管理者は、SOC担当者より検体ファイルの調査依頼を受領する。
B4	システム管理者は、調査依頼を承認するか否かを判断する。
B5	システム管理者は、SOC担当者より作業計画を受領する。
B6	システム管理者は、作業計画を承認するか否かを判断する。
B7	システム管理者は、作業完了報告を受領する。
C1	機関等担当者、地方防衛局担当者は、インシデント発生端末保持者にヒアリング、検体ファイルの提供依頼受領する。 また、初動の対応を実施する。
C2	機関等担当者、地方防衛局担当者は、システム運用担当者へ、事象情報、検体ファイルの提出する。
D1	課室等担当者は、インシデント発生端末保持者にヒアリング、検体ファイルの提供依頼受領する。 また、初動の対応実施する。
D2	課室等担当者は、システム運用担当者へ、事象情報、検体ファイルの提出する。
E1	省OA利用者は、インシデント発生端末保持者にヒアリング、検体ファイルの提供依頼受領する。 また、初動の対応を実施する。
E2	省OA利用者は、システム運用担当者へ、事象情報、検体ファイルの提出する。
G1	システム運用担当者は、SOC担当者より初動対応、事象や検体の提出依頼を受領する。
G2	システム運用担当者は、各種システム担当者へ事象ヒアリング、検体ファイルの提供依頼する。 また、初動の対応実施指示送付する。
G3	システム運用担当者は、各種システム担当者より事象情報、検体ファイル受領する。 SOC担当者へ事象情報、検体ファイルの送付する。
G4	システム運用担当者は、SOC担当者より追加の対応依頼受領する。
G5	システム運用担当者は、追加の対応を実施する。
G6	システム運用担当者は、SOC担当者へ追加の対応完了報告を送付する。
G7	システム運用担当者は、正常性の確認を行う。。
H1	SOC担当者は、セキュリティベンダ機器からのアラートを受領する。
H2	SOC担当者は、アラートの内容を確認する。
H3	SOC担当者は、脅威レベルの判定を行う。
H4	SOC担当者は、検知背景の確認を行う。
H5	SOC担当者は、過去完全に同一の発生背景で検知がありFP判定をしているかの確認を行う。
H6	SOC担当者は、CSIRTより事象や検体ファイルの提出依頼、初動対応指示を受領する。 SOC担当者は、緊急性に応じて、システム管理者、システム運用担当者へ事象や検体ファイルの提出依頼、初動対応指示を送付する。 SOC担当者は、初動対応の時点で、緊急性を要する何かがあった場合は、自サ防等に情報連携を実施する。
H7	SOC担当者は、システム運用担当者より事象情報、検体ファイル受領する。 SOC担当者は、その内容をCSIRTに連携を行う。
H8	SOC担当者は、検体ファイルを受領しているか確認を行う。
H9	SOC担当者は、システム管理者に受領した検体ファイルの調査依頼をセキュリティベンダに行ってよいかの承認依頼を行う。
H10	SOC担当者は、セキュリティベンダに受領した検体ファイルの調査依頼を送付する。
H11	SOC担当者は、システム運用担当者に追加の対応依頼を送付する。
H12	SOC担当者は、システム運用担当者より追加の対応完了報告を受領する。
H13	SOC担当者は、静観対応をCSIRT担当者と連携し行う。
H14	SOC担当者は、監視・分析の調整が必要かCSIRT担当者と連携し判断をする。

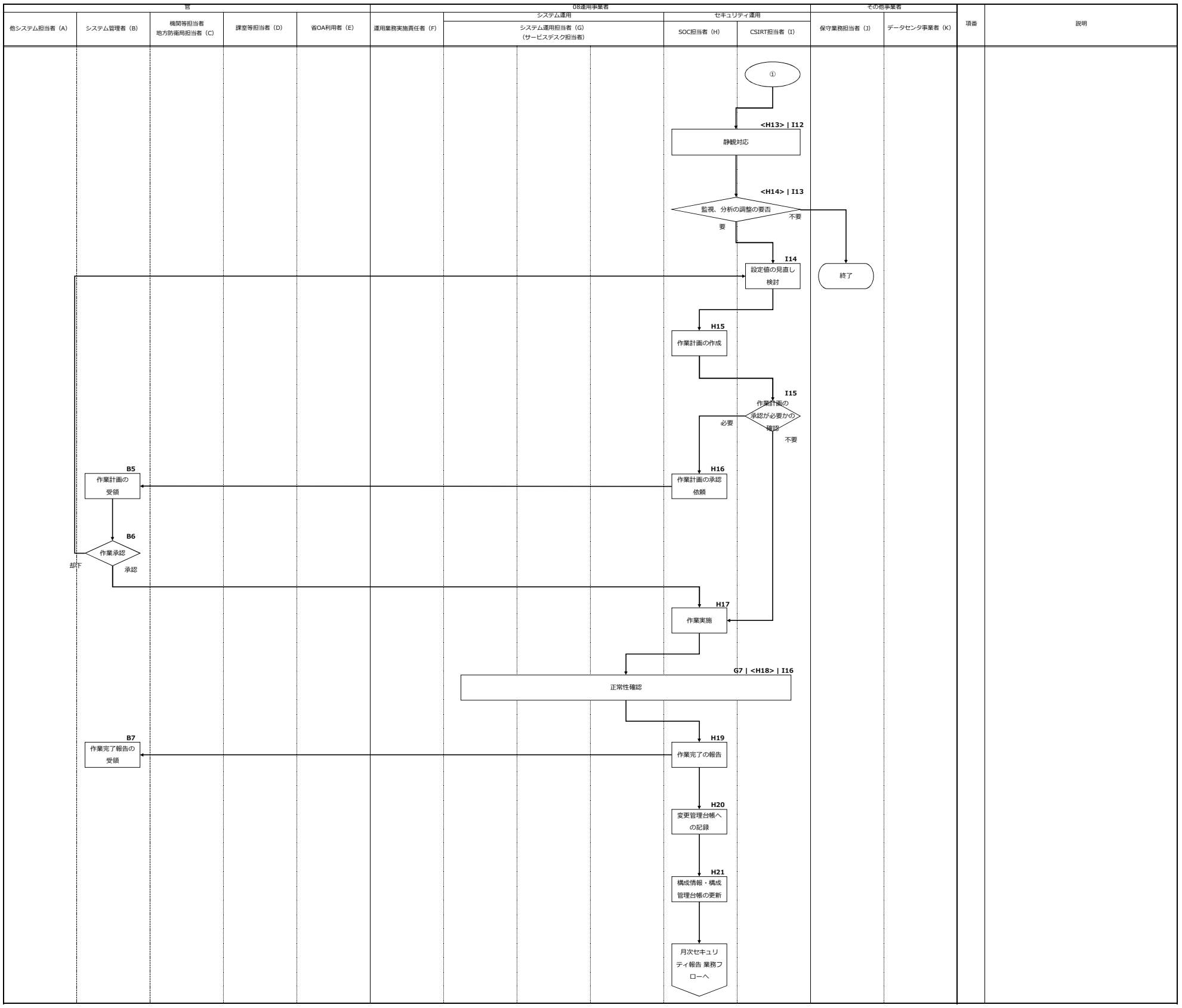
フロー名称	説明	作業トリガー
セキュリティ監視と検知	各作業トリガーを契機とする24/365リアルタイム監視の業務フローを示す。	・セキュリティ監視機能によるアラートの受領



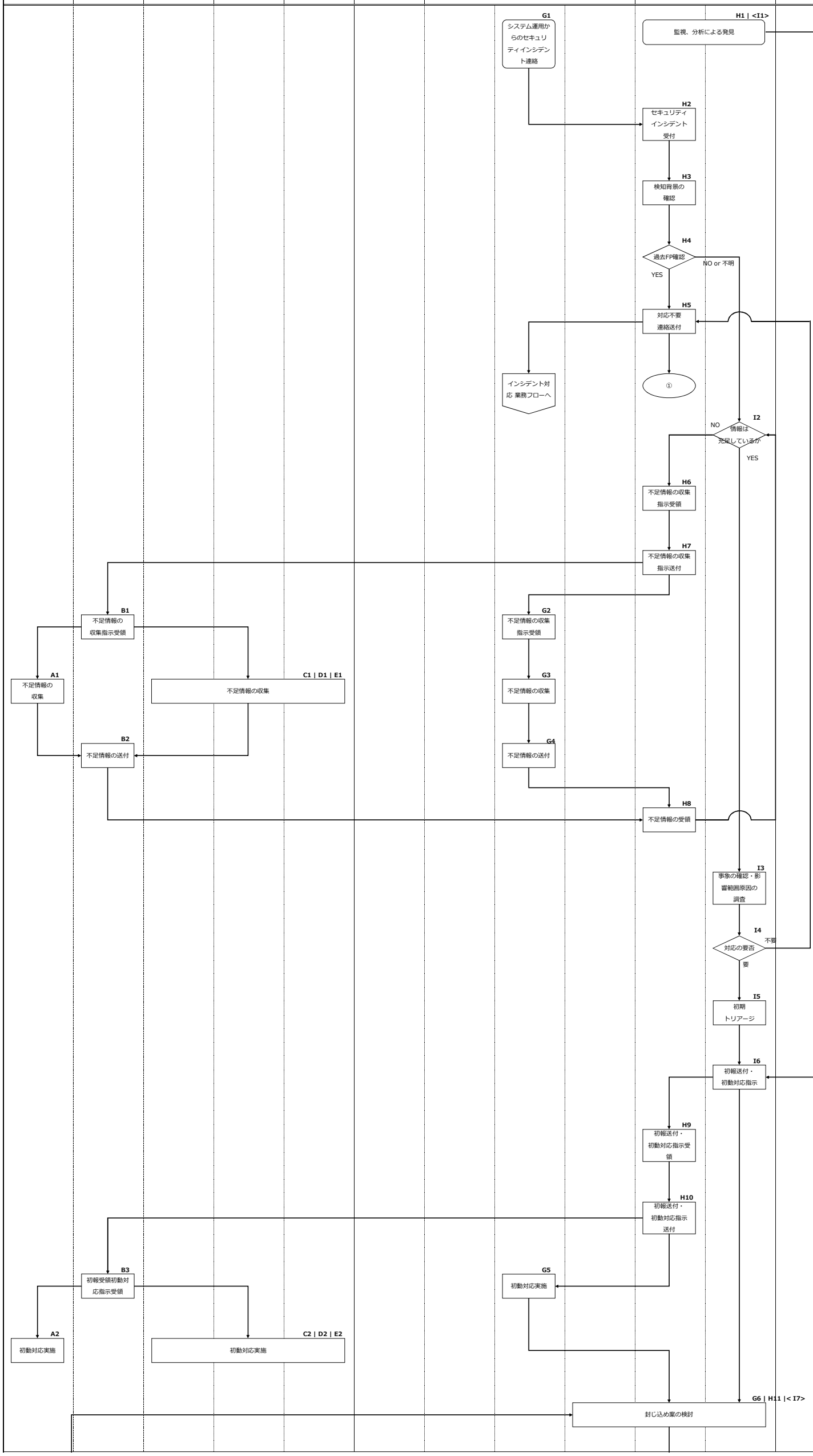
項番	説明
H15	SOC担当者は、作業計画の作成を行う。
H16	SOC担当者は、システム管理者に作業計画の承認依頼を送付する。
H17	SOC担当者は、作業計画を元に作業を実施する。
H18	SOC担当者は、各担当者と正常性の確認を行う。
H19	SOC担当者は、作業完了報告を行う。
H20	SOC担当者は、変更管理台帳へ記録をする。
H21	SOC担当者は、構成情報・構成管理台帳を更新する。
I1	SOC担当者よりエスカレーション受領する。
I2	CSIRT担当者は、検知内容・事象の確認を行い、インシデントかの判断を行う。
I3	CSIRT担当者は、事象や検体の危険性及び優先度の判断を行う。
I4	CSIRT担当者は、提出された情報の内容の分析を行う。
I5	CSIRT担当者は、セキュリティベンダからの調査内容を受領する。
I6	CSIRT担当者は、セキュリティベンダの調査内容の確認を行う。
I7	CSIRT担当者は、CSIRT側の分析結果とセキュリティベンダの調査結果を踏まえて分析・評価を行う。
I8	CSIRT担当者は、インシデントかの判断を再度行う。
I9	CSIRT担当者は、追加対応が必要かどうかの判断を行う。
I10	CSIRT担当者は、システム運用側の追加対応の内容を確認する。
I11	CSIRT担当者は、追加対応が完了しているかの判断を行う。
I12	CSIRT担当者は、静観対応を行う。
I13	CSIRT担当者は、監視・分析の調整が必要かの判断をする。
I14	CSIRT担当者は、設定値の見直しを行う。
I15	CSIRT担当者は、システム管理者に作業計画の承認が必要か判断を行う。
I16	CSIRT担当者は、正常性の確認を行う。
J1	保守業務業者のアンダーにいるセキュリティベンダーは、検体ファイルの調査を実施する。

付表１０　業務フロー（続き）
セキュリティ監視と検知（続き）

フロー名称	説明	作業トリガー
セキュリティ監視と検知	各作業トリガーを契機とする24/365リアルタイム監視の業務フローを示す。	・セキュリティ監視機能によるアラートの受領

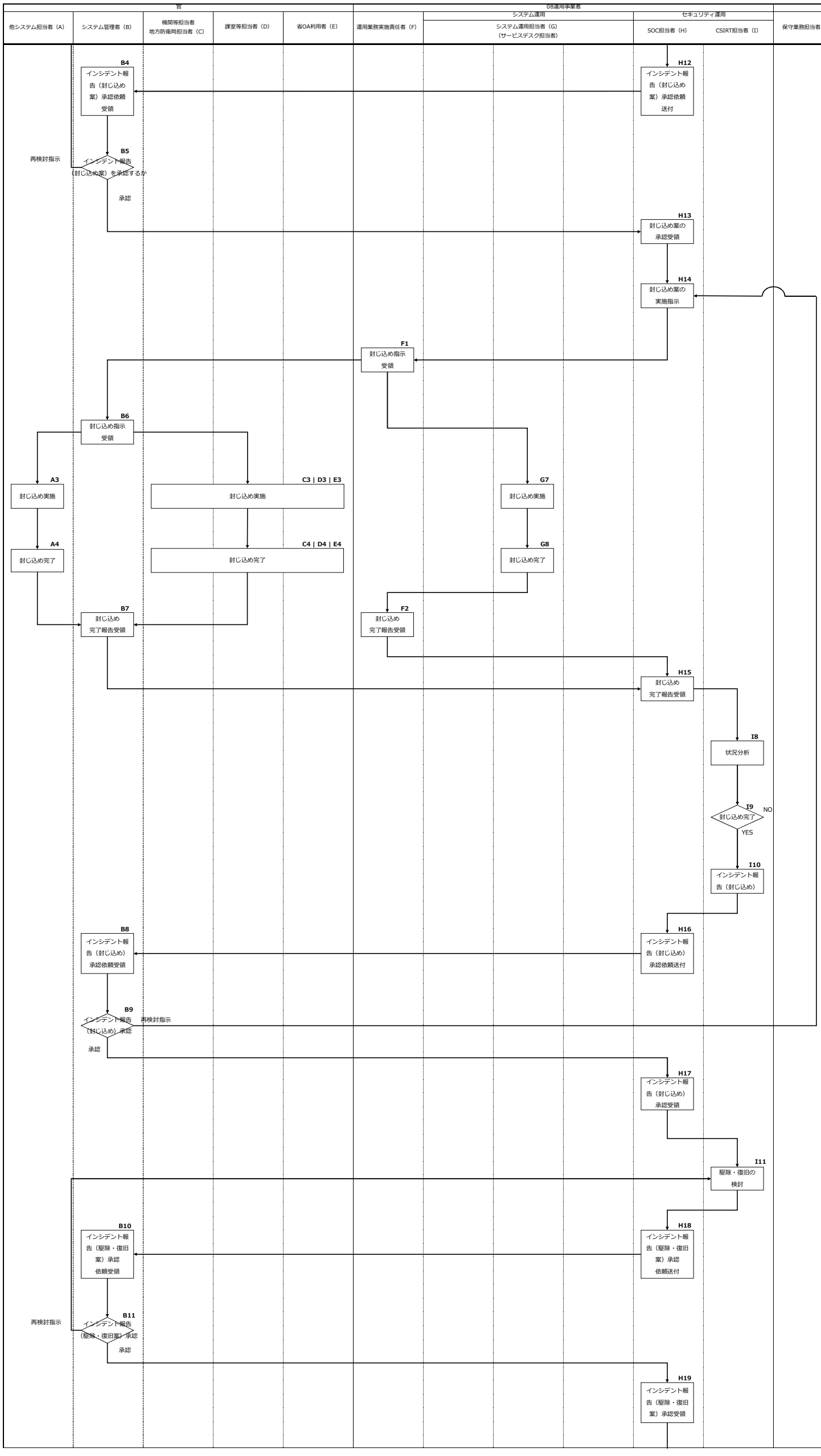


フロー名称	説明	作業トリガー
セキュリティインシデント対応	各作業トリガーを契機とするセキュリティインシデント対応フローを示す。	・セキュリティ監視機能による発見 ・イベント・提供情報分析による発見 ・システム運用からの連絡



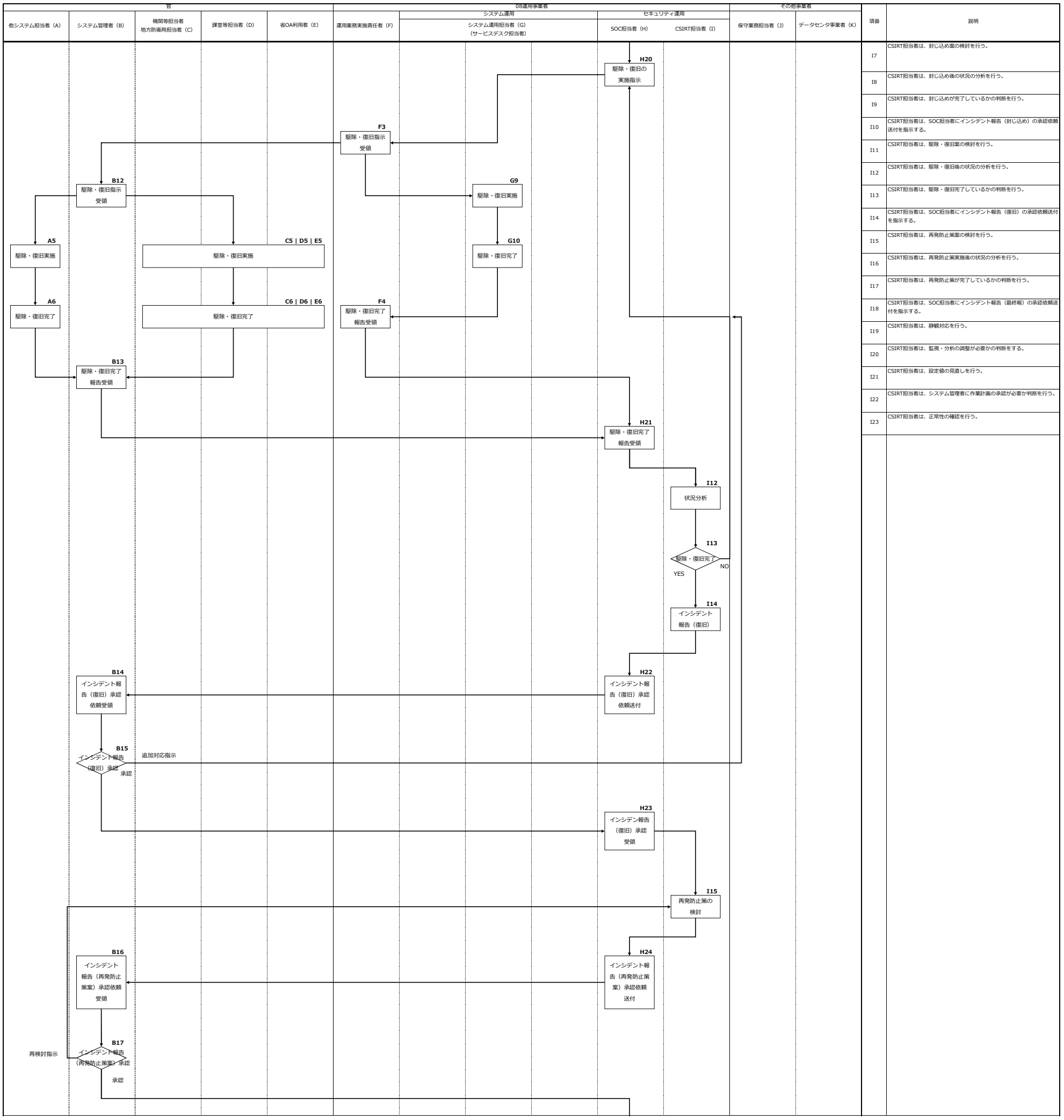
項番	説明
A1	他システム担当者は、システム管理者より不足情報収集指示を受領し、情報の収集を実施する。
A2	他システム担当者は、システム管理者より初動指示を受領し、初動対応を実施する。
A3	他システム担当者は、システム管理者より封じ込め指示を受領し、封じ込め対応を実施する。
A4	他システム担当者は、封じ込め対応を完了させる。
A5	他システム担当者は、システム管理者より駆除・復旧指示を受領し、駆除・復旧対応を実施する。
A6	他システム担当者は、駆除・復旧対応を完了させる。
A7	他システム担当者は、システム管理者より再発防止策実施指示を受領し、再発防止策を実施する。
A8	他システム担当者は、再発防止策対応を完了させる。
B1	システム管理者は、SOC担当者より不足情報収集指示を受領し、各システム担当者へ収集を指示する。
B2	システム管理者は、各システム担当者より不足情報を受領し、SOC担当者へ送付する。
B3	システム管理者は、運用業務実施責任者より初報を受領する。 また初動対応指示を受領し、各システム担当者へ初動対応を指示する。
B4	システム管理者は、SOC担当者よりインシデント報告（封じ込め案）の承認依頼を受領する。
B5	システム管理者は、インシデント報告（封じ込め案）を承認するか否かを判断する。
B6	システム管理者は、運用業務実施責任者より封じ込め指示を受領する また各システム担当者へ封じ込め対応を指示する。
B7	システム管理者は、各システム担当者より封じ込め完了報告を受領し、SOC担当者へ送付する。
B8	システム管理者は、SOC担当者よりインシデント報告（封じ込め）の承認依頼を受領する。
B9	システム管理者は、インシデント報告（封じ込め）を承認するか否かを判断する。
B10	システム管理者は、SOC担当者よりインシデント報告（駆除・復旧案）の承認依頼を受領する。
B11	システム管理者は、インシデント報告（封じ込め案）を承認するか否かを判断する。
B12	システム管理者は、運用業務実施責任者より駆除・復旧指示を受領する また各システム担当者へ駆除・復旧対応を指示する。
B13	システム管理者は、各システム担当者より封じ込め完了報告を受領し、SOC担当者へ送付する。
B14	システム管理者は、SOC担当者よりインシデント報告（復旧）の承認依頼を受領する。
B15	システム管理者は、インシデント報告（復旧）を承認するか否かを判断する。
B16	システム管理者は、SOC担当者よりインシデント報告（再発防止策案）の承認依頼を受領する。
B17	システム管理者は、インシデント報告（再発防止策案）を承認するか否かを判断する。
B18	システム管理者は、運用業務実施責任者より再発防止策案対応指示を受領する。また各システム担当者へ再発防止策案対応を指示する。
B19	システム管理者は、各システム担当者より再発防止策案対応完了報告を受領し、SOC担当者へ送付する。
B20	システム管理者は、SOC担当者よりインシデント報告（最終報）の承認依頼を受領する。
B21	システム管理者は、インシデント報告（最終報）を承認するか否かを判断する。
B22	システム管理者は、SOC担当者より作業計画を受領する。
B23	システム管理者は、作業計画を承認するか否かを判断する。
B24	システム管理者は、作業完了報告を受領する。
C1	機関等担当者、地方防衛局担当者は、システム管理者より不足情報収集指示を受領し、情報の収集を実施する。
C2	機関等担当者、地方防衛局担当者は、システム管理者より初動指示を受領し、初動対応を実施する。
C3	機関等担当者、地方防衛局担当者は、システム管理者より封じ込め指示を受領し、封じ込め対応を実施する。
C4	機関等担当者、地方防衛局担当者は、封じ込め対応を完了させる。
C5	機関等担当者、地方防衛局担当者は、システム管理者より駆除・復旧指示を受領し、駆除・復旧対応を実施する。
C6	機関等担当者、地方防衛局担当者は、駆除・復旧対応を完了させる。
C7	機関等担当者、地方防衛局担当者は、システム管理者より再発防止策実施指示を受領し、再発防止策を実施する。
C8	機関等担当者、地方防衛局担当者は、再発防止策対応を完了させる。
D1	課室等担当者は、システム管理者より不足情報収集指示を受領し、情報の収集を実施する。
D2	課室等担当者は、システム管理者より初動指示を受領し、初動対応を実施する。
D3	課室等担当者は、システム管理者より封じ込め指示を受領し、封じ込め対応を実施する。
D4	課室等担当者は、封じ込め対応を完了させる。
D5	課室等担当者は、システム管理者より駆除・復旧指示を受領し、駆除・復旧対応を実施する。
D6	課室等担当者は、駆除・復旧対応を完了させる。
D7	課室等担当者は、システム管理者より再発防止策実施指示を受領し、再発防止策を実施する。
D8	課室等担当者は、再発防止策対応を完了させる。
E1	省OA利用者は、システム管理者より不足情報収集指示を受領し、情報の収集を実施する。
E2	省OA利用者は、システム管理者より初動指示を受領し、初動対応を実施する。
E3	省OA利用者は、システム管理者より封じ込め指示を受領し、封じ込め対応を実施する。
E4	省OA利用者は、封じ込め対応を完了させる。
E5	省OA利用者は、システム管理者より駆除・復旧指示を受領し、駆除・復旧対応を実施する。
E6	省OA利用者は、駆除・復旧対応を完了させる。
E7	省OA利用者は、システム管理者より再発防止策実施指示を受領し、再発防止策を実施する。
E8	省OA利用者は、再発防止策対応を完了させる。
F1	運用業務実施責任者は、SOC担当者より封じ込め指示を受領する また各システム運用担当者へ封じ込め対応を指示する。
F2	運用業務実施責任者は、各システム運用担当者より封じ込め完了報告を受領し、SOC担当者へ送付する。
F3	運用業務実施責任者は、SOC担当者より駆除・復旧指示を受領する また各システム運用担当者へ駆除・復旧対応を指示する。
F4	運用業務実施責任者は、各システム運用担当者より駆除・復旧完了報告を受領し、SOC担当者へ送付する。

フロー名称	説明	作業トリガー
セキュリティインシデント対応	各作業トリガーを契機とするセキュリティインシデント対応フローを示す。	・セキュリティ監視機能による発見 ・イベント・提供情報分析による発見 ・システム運用からの連絡



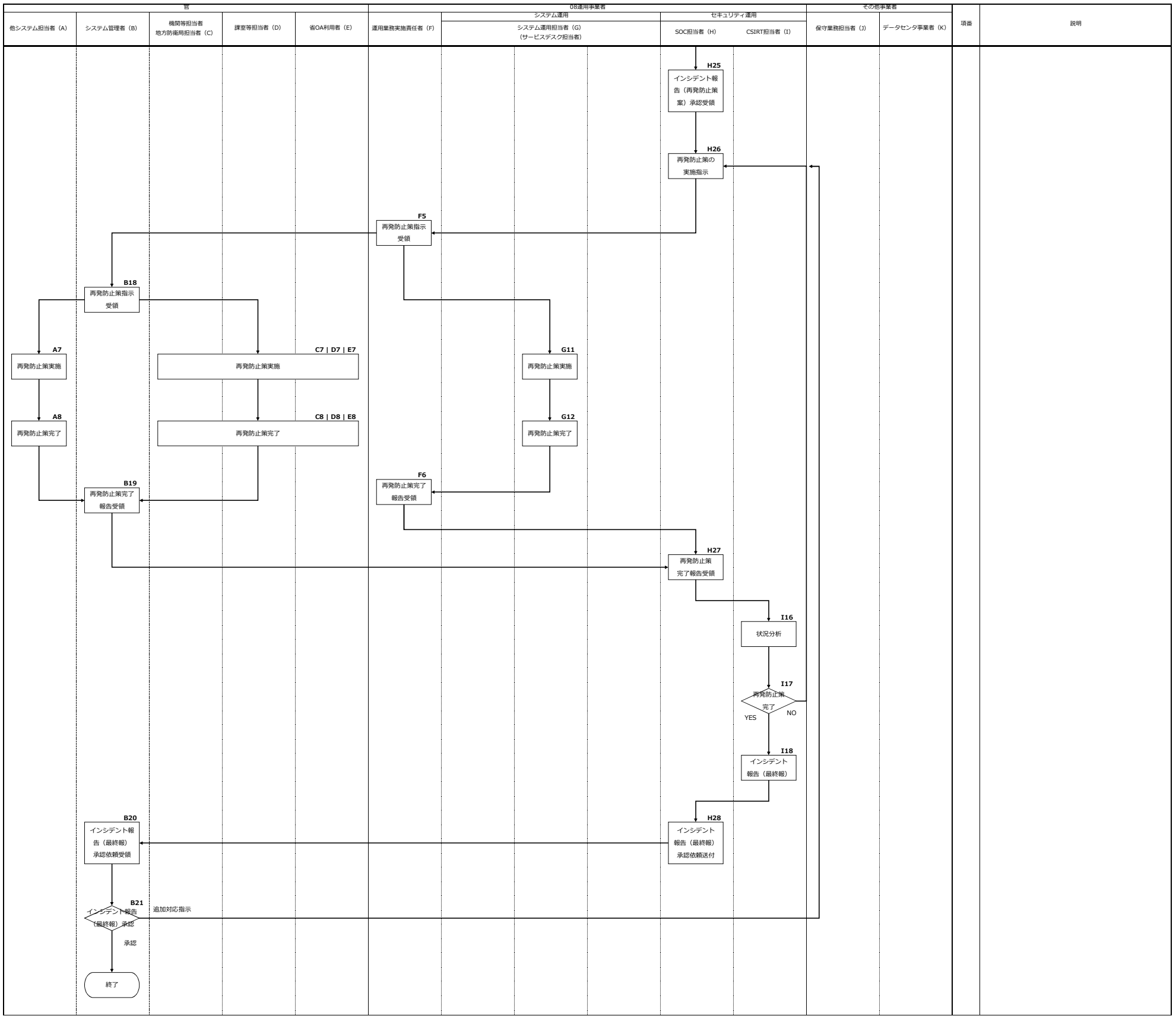
項番	説明
F5	運用業務実施責任者は、SOC担当者より再発防止策対応指示を受領するまた各システム運用担当者へ再発防止策対応を指示する。
F6	運用業務実施責任者は、各システム運用担当者より再発防止策対応完了報告を受領し、SOC担当者へ送付する。
G1	システム運用担当者は、セキュリティインシデント発生を連絡する。
G2	システム運用担当者は、SOC担当者より不足情報収集指示を受領する。
G3	システム運用担当者は、不足情報の収集を実施する。
G4	システム運用担当者は、不足情報をSOC担当者へ送付する。
G5	システム運用担当者は、運用業務実施責任者より初動指示を受領し、初動対応を実施する。
G6	システム運用担当者は、封じ込め案の検討を行う。
G7	システム運用担当者は、運用業務実施責任者より封じ込め指示を受領し、封じ込め対応を実施する。
G8	システム運用担当者は、封じ込め対応を完了させる。
G9	システム運用担当者は、運用業務実施責任者より駆除・復旧指示を受領し、封じ込め対応を実施する。
G10	システム運用担当者は、駆除・復旧対応を完了させる。
G11	システム運用担当者は、運用業務実施責任者より再発防止策対応指示を受領し、封じ込め対応を実施する。
G12	システム運用担当者は、再発防止策対応を完了させる。
G13	システム運用担当者は、正常性の確認を行う。
H1	SOC担当者は、監視・分析により発見されたセキュリティインシデントの連携を行う。
H2	SOC担当者は、システム運用担当者からセキュリティインシデントの連絡を受け付ける。
H3	SOC担当者は、セキュリティインシデントの検知背景の確認を行う。
H4	SOC担当者は、セキュリティインシデントが過去にFP判定だったかの判断を行う。
H5	SOC担当者は、セキュリティインシデントの対応不要連絡を各担当者に送付する。
H6	SOC担当者は、CSIRT担当者より不足情報収集指示を受領する。
H7	SOC担当者は、不足情報収集指示を各担当者に送付する。
H8	SOC担当者は、各担当者より不足情報を受領する。
H9	SOC担当者は、CSIRT担当者より初報を送付、初動対応指示を受領する。
H10	SOC担当者は、システム管理者、システム運用担当者へ初報の送付、初動対応指示を送付する。
H11	SOC担当者は、封じ込め案の検討を行う。
H12	SOC担当者は、システム管理者へインシデント報告（封じ込め案）の承認依頼を送付する。
H13	SOC担当者は、システム管理者よりインシデント報告（封じ込め案）の承認を受領する。 ※「封じ込め、駆除・復旧、再発防止」が並行対応となる可能性もある
H14	SOC担当者は、各担当者へ封じ込め対応指示を送付する。
H15	SOC担当者は、各担当者より封じ込め対応完了報告を受領し、CSIRT担当者へ完了報告する。
H16	SOC担当者は、システム管理者へインシデント報告（封じ込め）の承認依頼を送付する。
H17	SOC担当者は、システム管理者よりインシデント報告（封じ込め）の承認を受領する。
H18	SOC担当者は、システム管理者へインシデント報告（駆除・復旧案）の承認依頼を送付する。
H19	SOC担当者は、システム管理者よりインシデント報告（駆除・復旧案）の承認を受領する。
H20	SOC担当者は、各担当者へ駆除・復旧対応指示を送付する。
H21	SOC担当者は、各担当者より駆除・復旧完了報告を受領し、CSIRT担当者へ完了報告する。
H22	SOC担当者は、システム管理者へインシデント報告（復旧）の承認依頼を送付する。
H23	SOC担当者は、システム管理者よりインシデント報告（復旧）の承認を受領する。
H24	SOC担当者は、システム管理者へインシデント報告（再発防止策案）の承認依頼を送付する。
H25	SOC担当者は、システム管理者よりインシデント報告（再発防止策案）の承認を受領する。
H26	SOC担当者は、各担当者へ再発防止策対応指示を送付する。
H27	SOC担当者は、各担当者より再発防止策完了報告を受領し、CSIRT担当者へ完了報告する。
H28	SOC担当者は、システム管理者へインシデント報告（最終報）の承認依頼を送付する。
H29	SOC担当者は、静観対応を行う。
H30	SOC担当者は、監視・分析の調整が必要かの判断をする。
H31	SOC担当者は、作業計画の作成を行う。
H32	SOC担当者は、システム管理者に作業計画の承認依頼を送付する。
H33	SOC担当者は、作業計画を元に作業を実施する。
H34	SOC担当者は、正常性の確認を行う。
H35	SOC担当者は、作業完了報告を行う。
H36	SOC担当者は、変更管理台帳へ記録をする。
H37	SOC担当者は、構成情報・構成管理台帳を更新する。
I1	CSIRT担当者は、監視・分析により発見されたセキュリティインシデントの連携を行う。
I2	CSIRT担当者は、インシデントの判定を行う。上で情報が充足しているかの確認を行う。
I3	CSIRT担当者は、事象の確認・影響範囲、原因の調査を行う。
I4	CSIRT担当者は、対応が必要かの判断を行う。
I5	CSIRT担当者は、初期トリアージを行う。
I6	CSIRT担当者は、SOC担当者に初報を送付、各担当者への初動対応を指示する。

フロー名称	説明	作業トリガー
セキュリティインシデント対応	各作業トリガーを契機とするセキュリティインシデント対応フローを示す。	・セキュリティ監視機能による発見 ・イベント・提供情報分析による発見 ・システム運用からの連絡



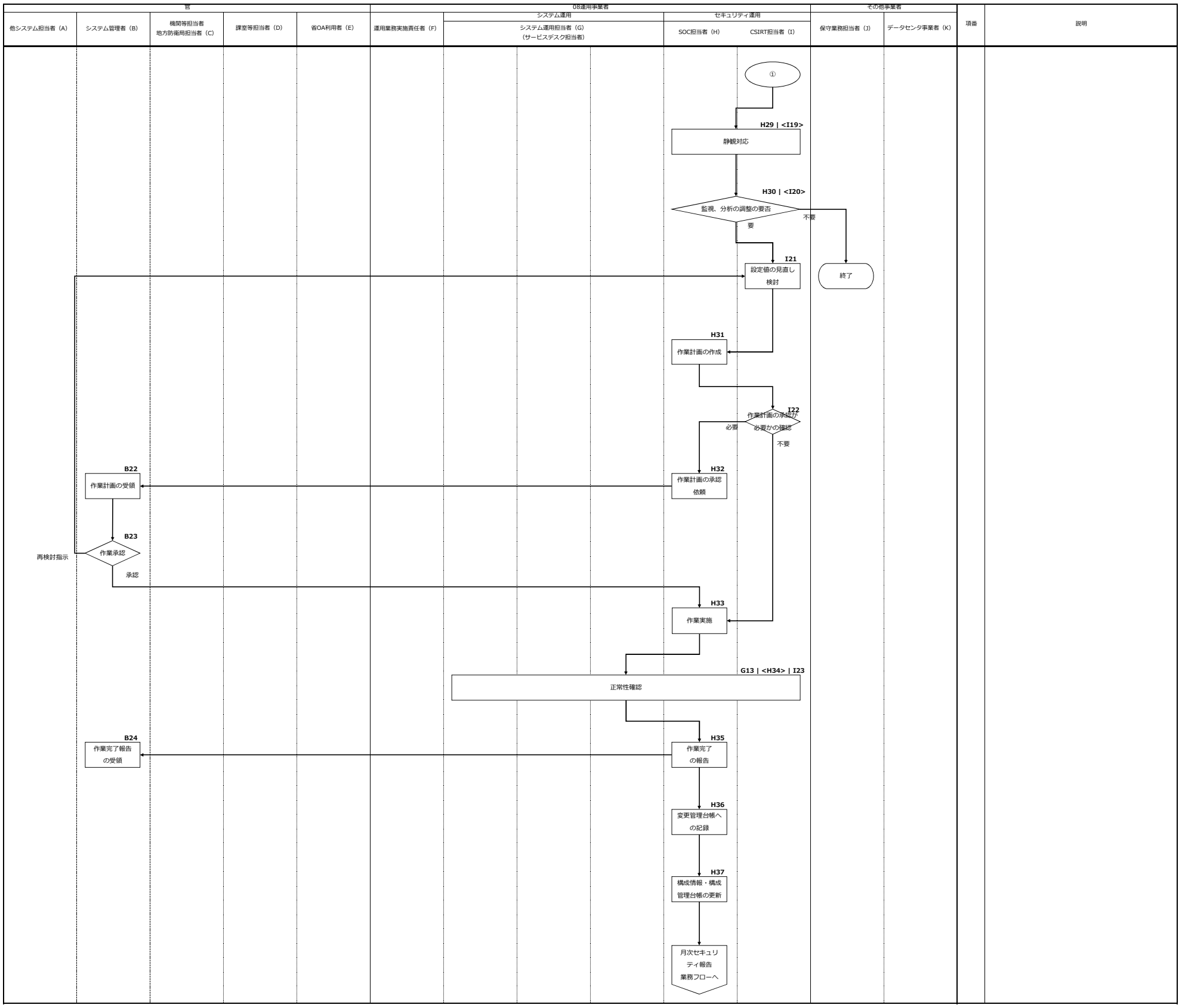
項番	説明
I7	CSIRT担当者は、封じ込め案の検討を行う。
I8	CSIRT担当者は、封じ込め後の状況の分析を行う。
I9	CSIRT担当者は、封じ込めが完了しているかの判断を行う。
I10	CSIRT担当者は、SOC担当者にインシデント報告（封じ込め）の承認依頼送付を指示する。
I11	CSIRT担当者は、駆除・復旧案の検討を行う。
I12	CSIRT担当者は、駆除・復旧後の状況の分析を行う。
I13	CSIRT担当者は、駆除・復旧完了しているかの判断を行う。
I14	CSIRT担当者は、SOC担当者にインシデント報告（復旧）の承認依頼送付を指示する。
I15	CSIRT担当者は、再発防止策案の検討を行う。
I16	CSIRT担当者は、再発防止策実施後の状況の分析を行う。
I17	CSIRT担当者は、再発防止策が完了しているかの判断を行う。
I18	CSIRT担当者は、SOC担当者にインシデント報告（最終報）の承認依頼送付を指示する。
I19	CSIRT担当者は、静観対応を行う。
I20	CSIRT担当者は、監視・分析の調整が必要かの判断をする。
I21	CSIRT担当者は、設定値の見直しを行う。
I22	CSIRT担当者は、システム管理者に作業計画の承認が必要か判断を行う。
I23	CSIRT担当者は、正常性の確認を行う。

フロー名称	説明	作業トリガー
セキュリティインシデント対応	各作業トリガーを契機とするセキュリティインシデント対応フローを示す。	・セキュリティ監視機能による発見 ・イベント・提供情報分析による発見 ・システム運用からの連絡

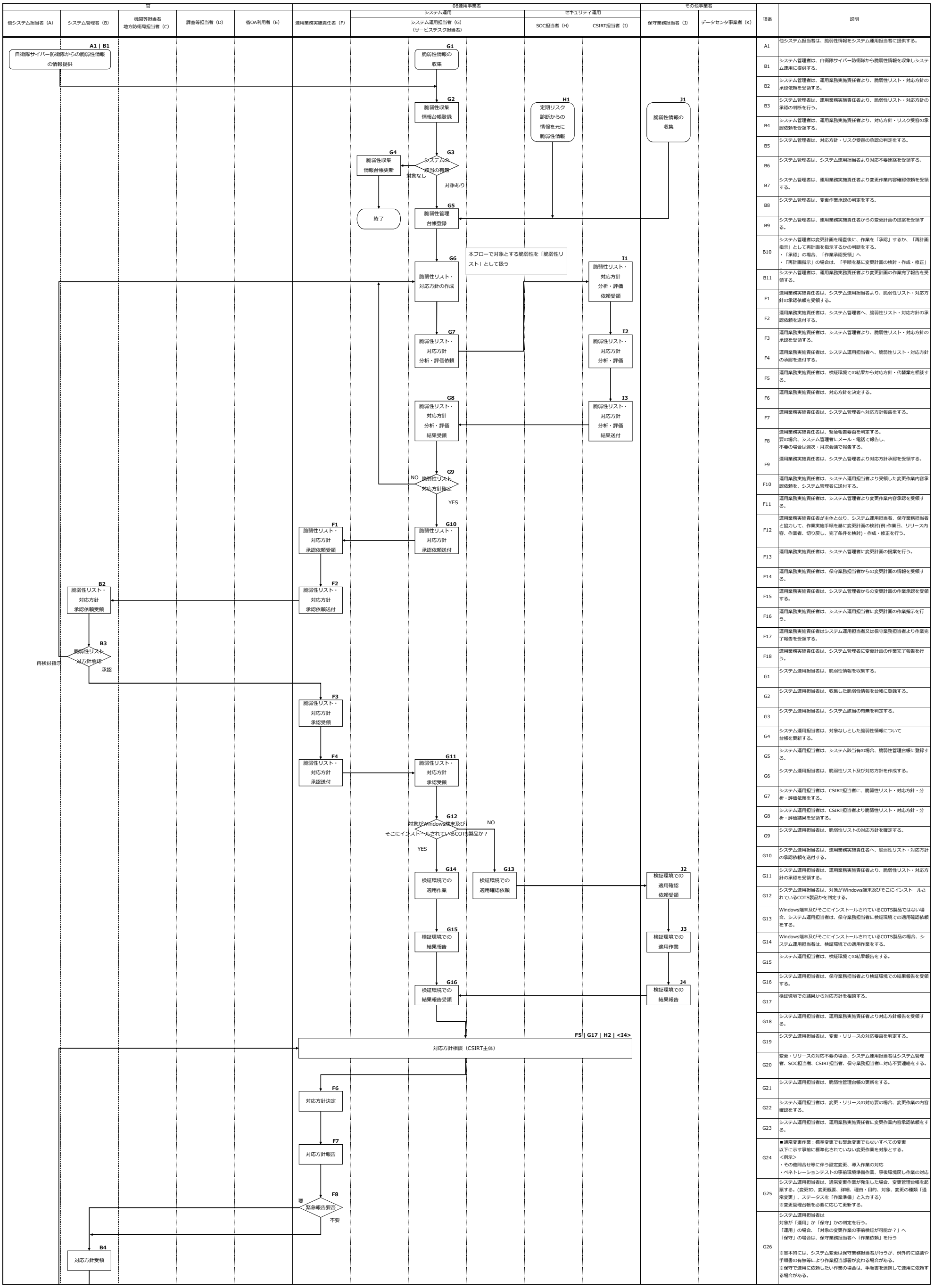


付表１０　業務フロー（続き）
セキュリティインシデント対応（続き）

フロー名称	説明	作業トリガー
セキュリティインシデント対応	各作業トリガーを契機とするセキュリティインシデント対応フローを示す。	・セキュリティ監視機能による発見 ・イベント・提供情報分析による発見 ・システム運用からの連絡

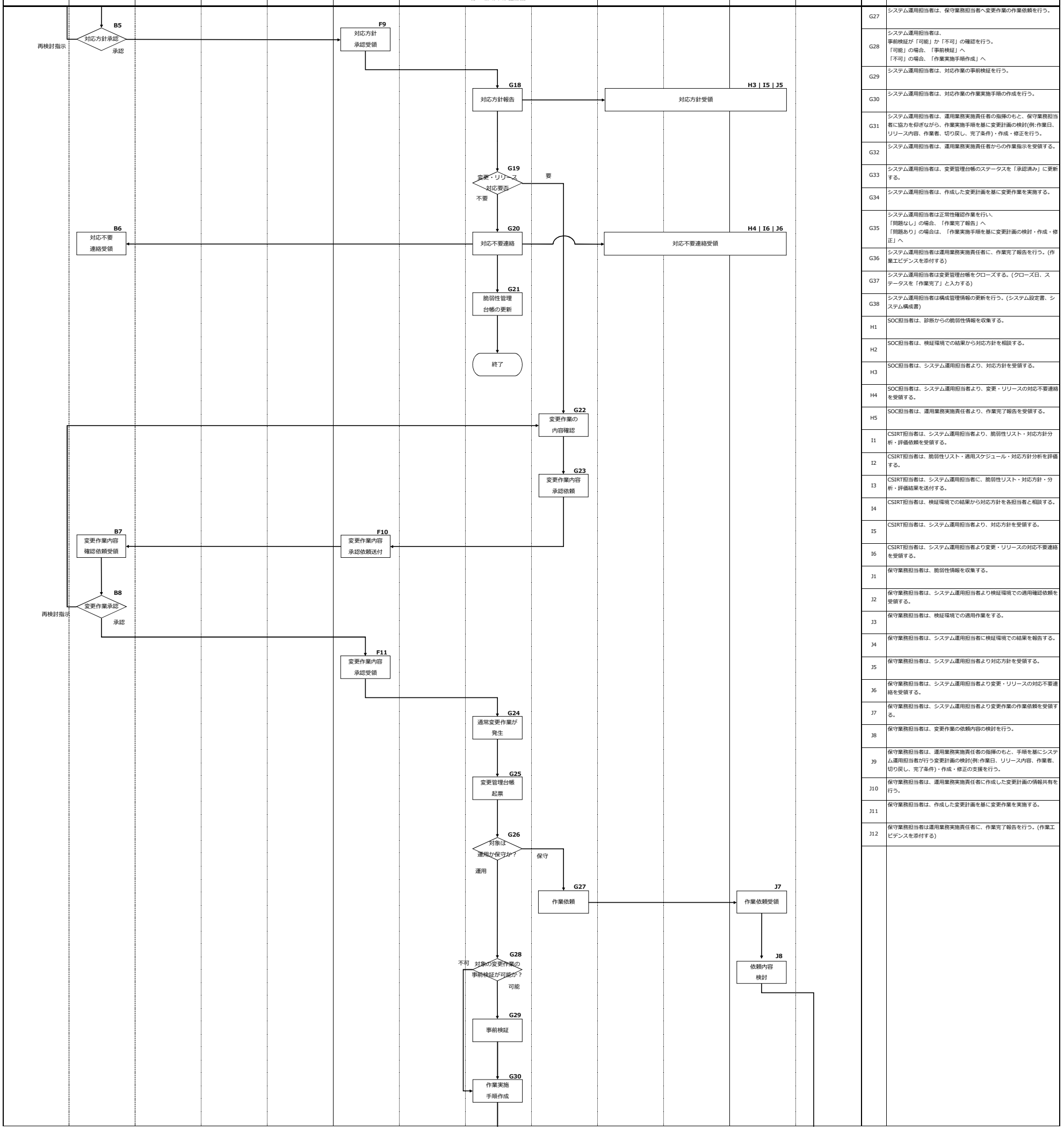


フロー名称	説明	作業トリガー
脅威・脆弱性管理	各作業トリガーを契機とする脆弱性の対応フローを示す。	・脆弱性情報を取集する定常業務をトリガーとする



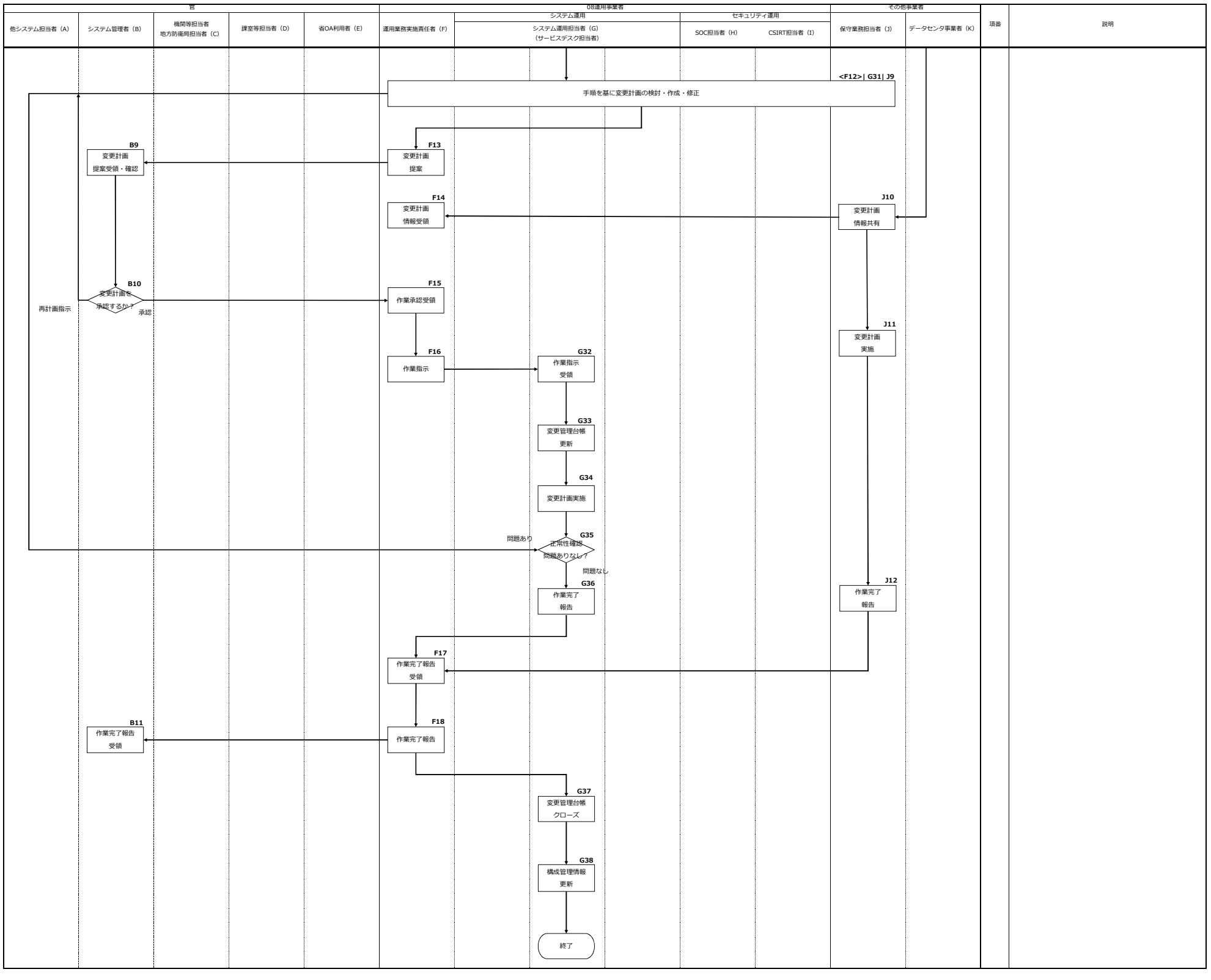
項番	説明
A1	他システム担当者は、脆弱性情報をシステム運用担当者に提供する。
B1	システム管理者は、自衛隊サイバー防衛隊から脆弱性情報を収集しシステム運用に提供する。
B2	システム管理者は、運用業務実施責任者より、脆弱性リスト・対応方針の承認依頼を受領する。
B3	システム管理者は、運用業務実施責任者より、脆弱性リスト・対応方針の承認の判断を行う。
B4	システム管理者は、運用業務実施責任者より、対応方針・リスク受容の承認依頼を受領する。
B5	システム管理者は、対応方針・リスク受容の承認の判定をする。
B6	システム管理者は、システム運用担当者より対応不要連絡を受領する。
B7	システム管理者は、運用業務実施責任者より変更作業内容確認依頼を受領する。
B8	システム管理者は、変更作業承認の判定をする。
B9	システム管理者は、運用業務実施責任者からの変更計画の提案を受領する。
B10	システム管理者は変更計画を精査後に、作業を「承認」するか、「再計画指示」として再計画を指示するかの判断をする。 ・「承認」の場合、「作業承認受領」へ ・「再計画指示」の場合は、「手順を基に変更計画の検討・作成・修正」
B11	システム管理者は、運用業務実務責任者より変更計画の作業完了報告を受領する。
F1	運用業務実施責任者は、システム運用担当者より、脆弱性リスト・対応方針の承認依頼を受領する。
F2	運用業務実施責任者は、システム管理者へ、脆弱性リスト・対応方針の承認依頼を送付する。
F3	運用業務実施責任者は、システム管理者より、脆弱性リスト・対応方針の承認を受領する。
F4	運用業務実施責任者は、システム運用担当者へ、脆弱性リスト・対応方針の承認を送付する。
F5	運用業務実施責任者は、検証環境での結果から対応方針・代替案を相談する。
F6	運用業務実施責任者は、対応方針を決定する。
F7	運用業務実施責任者は、システム管理者へ対応方針報告をする。
F8	運用業務実施責任者は、緊急報告要否を判定する。 要の場合、システム管理者にメール・電話で報告し、 不要の場合は週次・月次会議で報告する。
F9	運用業務実施責任者は、システム管理者より対応方針承認を受領する。
F10	運用業務実施責任者は、システム運用担当者より受領した変更作業内容承認依頼を、システム管理者に送付する。
F11	運用業務実施責任者は、システム管理者より変更作業内容承認を受領する。
F12	運用業務実施責任者が主体となり、システム運用担当者、保守業務担当者と協力して、作業実施手順を基に変更計画の検討(例:作業日、リリース内容、作業者、切り戻し、完了条件を検討)・作成・修正を行う。
F13	運用業務実施責任者は、システム管理者に変更計画の提案を行う。
F14	運用業務実施責任者は、保守業務担当者からの変更計画の情報を受領する。
F15	運用業務実施責任者は、システム管理者からの変更計画の作業承認を受領する。
F16	運用業務実施責任者は、システム運用担当者に変更計画の作業指示を行う。
F17	運用業務実施責任者はシステム運用担当者又は保守業務担当者より作業完了報告を受領する。
F18	運用業務実施責任者は、システム管理者に変更計画の作業完了報告を行う。
G1	システム運用担当者は、脆弱性情報を収集する。
G2	システム運用担当者は、収集した脆弱性情報を台帳に登録する。
G3	システム運用担当者は、システム該当の有無を判定する。
G4	システム運用担当者は、対象なしとした脆弱性情報について 台帳を更新する。
G5	システム運用担当者は、システム該当有の場合、脆弱性管理台帳に登録する。
G6	システム運用担当者は、脆弱性リスト及び対応方針を作成する。
G7	システム運用担当者は、CSIRT担当者に、脆弱性リスト・対応方針・分析・評価依頼をする。
G8	システム運用担当者は、CSIRT担当者より脆弱性リスト・対応方針・分析・評価結果を受領する。
G9	システム運用担当者は、脆弱性リストの対応方針を確定する。
G10	システム運用担当者は、運用業務実施責任者へ、脆弱性リスト・対応方針の承認依頼を送付する。
G11	システム運用担当者は、運用業務実施責任者より、脆弱性リスト・対応方針の承認を受領する。
G12	システム運用担当者は、対象がWindows端末及びそこにインストールされているCOTS製品かを判定する。
G13	Windows端末及びそこにインストールされているCOTS製品ではない場合、システム運用担当者は、保守業務担当者に検証環境での適用確認依頼をする。
G14	Windows端末及びそこにインストールされているCOTS製品の場合、システム運用担当者は、検証環境での適用作業をする。
G15	システム運用担当者は、検証環境での結果報告をする。
G16	システム運用担当者は、保守業務担当者より検証環境での結果報告を受領する。
G17	検証環境での結果から対応方針を相談する。
G18	システム運用担当者は、運用業務実施責任者より対応方針報告を受領する。
G19	システム運用担当者は、変更・リリースの対応要否を判定する。
G20	変更・リリースの対応不要の場合、システム運用担当者はシステム管理者、SOC担当者、CSIRT担当者、保守業務担当者に対応不要連絡をする。
G21	システム運用担当者は、脆弱性管理台帳の更新をする。
G22	システム運用担当者は、変更・リリースの対応要の場合、変更作業の内容確認をする。
G23	システム運用担当者は、運用業務実施責任者に変更作業内容承認依頼をする。
G24	■通常変更作業：標準変更でも緊急変更でもないすべての変更 以下に示す事前に標準化されていない変更作業を対象とする。 <例示> ・その他問合せ等に伴う設定変更、導入作業の対応 ・ペネトレーションテストの事前環境準備作業、事後環境戻し作業の対応
G25	システム運用担当者は、通常変更作業が発生した場合、変更管理台帳を起票する。(変更ID、変更概要、詳細、理由・目的、対象、変更の種類「通常変更」、ステータスを「作業準備」と入力する) ※変更管理台帳を必要に応じて更新する。
G26	システム運用担当者は 対象が「運用」か「保守」かの判定を行う。 「運用」の場合、「対象の変更作業の事前検証が可能か？」へ 「保守」の場合は、保守業務担当者へ「作業依頼」を行う ※基本的には、システム変更は保守業務担当者が行うが、例外的に協議や手順書の有無等により作業担当部署が変わる場合がある。 ※保守で運用に依頼したい作業の場合は、手順書を連携して運用に依頼する場合がある。

フロー名称	説明	作業トリガー
脅威・脆弱性管理	各作業トリガーを契機とする脆弱性の対応フローを示す。	・脆弱性情報を取集する定常業務をトリガーとする



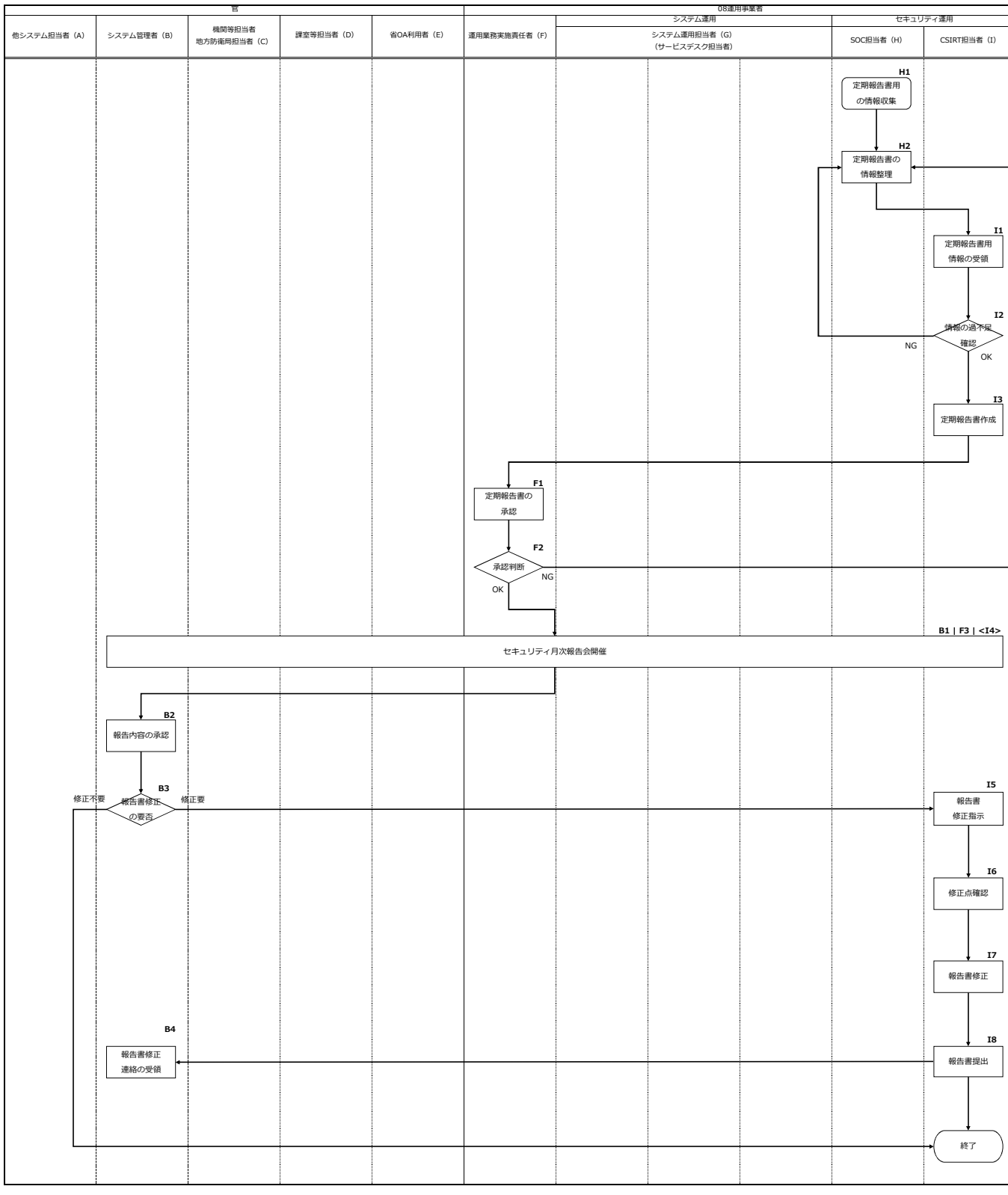
項番	説明
G27	システム運用担当者は、保守業務担当者へ変更作業の作業依頼を行う。
G28	システム運用担当者は、 事前検証が「可能」か「不可」の確認を行う。 「可能」の場合、「事前検証」へ 「不可」の場合、「作業実施手順作成」へ
G29	システム運用担当者は、対応作業の事前検証を行う。
G30	システム運用担当者は、対応作業の作業実施手順の作成を行う。
G31	システム運用担当者は、運用業務実施責任者の指揮のもと、保守業務担当者に協力を仰ぎながら、作業実施手順を基に変更計画の検討(例:作業日、リリース内容、作業者、切り戻し、完了条件)・作成・修正を行う。
G32	システム運用担当者は、運用業務実施責任者からの作業指示を受領する。
G33	システム運用担当者は、変更管理台帳のステータスを「承認済み」に更新する。
G34	システム運用担当者は、作成した変更計画を基に変更作業を実施する。
G35	システム運用担当者は正常性確認作業を行い、 「問題なし」の場合、「作業完了報告」へ 「問題あり」の場合は、「作業実施手順を基に変更計画の検討・作成・修正」へ
G36	システム運用担当者は運用業務実施責任者に、作業完了報告を行う。(作業エビデンスを添付する)
G37	システム運用担当者は変更管理台帳をクローズする。(クローズ日、ステータスを「作業完了」と入力する)
G38	システム運用担当者は構成管理情報の更新を行う。(システム設定書、システム構成書)
H1	SOC担当者は、診断からの脆弱性情報を収集する。
H2	SOC担当者は、検証環境での結果から対応方針を相談する。
H3	SOC担当者は、システム運用担当者より、対応方針を受領する。
H4	SOC担当者は、システム運用担当者より、変更・リリースの対応不要連絡を受領する。
H5	SOC担当者は、運用業務実施責任者より、作業完了報告を受領する。
I1	CSIRT担当者は、システム運用担当者より、脆弱性リスト・対応方針分析・評価依頼を受領する。
I2	CSIRT担当者は、脆弱性リスト・適用スケジュール・対応方針分析を評価する。
I3	CSIRT担当者は、システム運用担当者に、脆弱性リスト・対応方針・分析・評価結果を送付する。
I4	CSIRT担当者は、検証環境での結果から対応方針を各担当者と相談する。
I5	CSIRT担当者は、システム運用担当者より、対応方針を受領する。
I6	CSIRT担当者は、システム運用担当者より変更・リリースの対応不要連絡を受領する。
J1	保守業務担当者は、脆弱性情報を収集する。
J2	保守業務担当者は、システム運用担当者より検証環境での適用確認依頼を受領する。
J3	保守業務担当者は、検証環境での適用作業をする。
J4	保守業務担当者は、システム運用担当者に検証環境での結果を報告する。
J5	保守業務担当者は、システム運用担当者より対応方針を受領する。
J6	保守業務担当者は、システム運用担当者より変更・リリースの対応不要連絡を受領する。
J7	保守業務担当者は、システム運用担当者より変更作業の作業依頼を受領する。
J8	保守業務担当者は、変更作業の依頼内容の検討を行う。
J9	保守業務担当者は、運用業務実施責任者の指揮のもと、手順を基にシステム運用担当者が行う変更計画の検討(例:作業日、リリース内容、作業者、切り戻し、完了条件)・作成・修正の支援を行う。
J10	保守業務担当者は、運用業務実施責任者に作成した変更計画の情報共有を行う。
J11	保守業務担当者は、作成した変更計画を基に変更作業を実施する。
J12	保守業務担当者は運用業務実施責任者に、作業完了報告を行う。(作業エビデンスを添付する)

フロー名称	説明	作業トリガー
脅威・脆弱性管理	各作業トリガーを契機とする脆弱性の対応フローを示す。	・脆弱性情報を取集する定常業務をトリガーとする



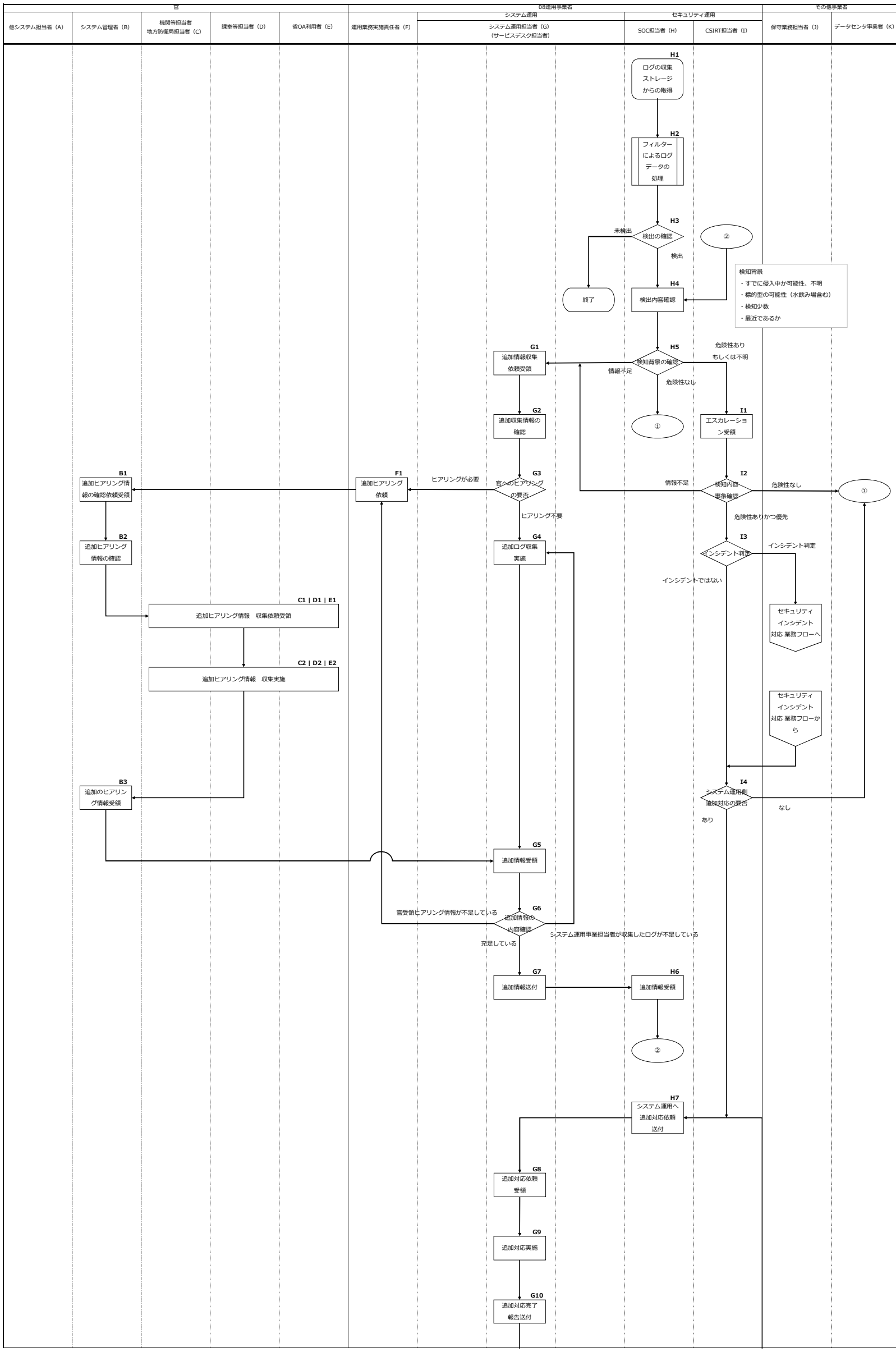
付表9　業務フロー（続き）
月次セキュリティ報告（続き）

フロー名称	説明	作業トリガー
月次セキュリティ報告	各作業トリガーを契機とするレポート報告対応フローを示す。	・月次報告会といった定期報告に備えて実施する。 ・本業務の実施タイミングは、定期報告の取り決めによる。



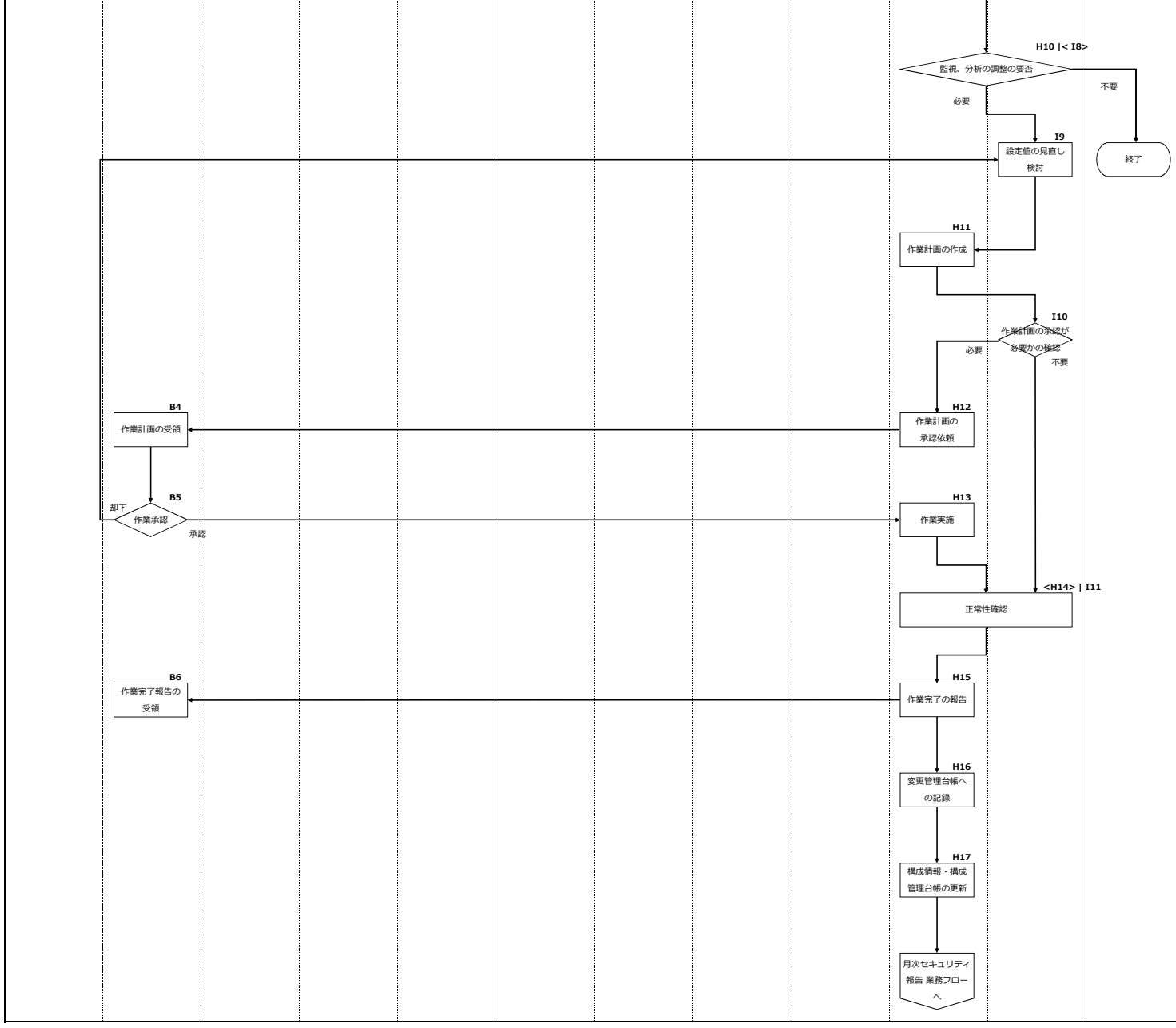
項番	説明
B1	システム管理者は、セキュリティ月次報告会に参加する。
B2	システム管理者は、月次報告の内容を承認する。
B3	システム管理者は確認した月次報告書について修正箇所があるかを判断する。
B4	システム管理者は、運用業務実施責任者から月次報告書の修正が完了した連絡を受領する。
F1	運用実務実施責任者は、定期報告書の内容を確認し承認判断をする。
F2	運用実務実施責任者は、承認判断にて、問題無い場合はセキュリティ月次報告会の資料とする。問題ありの場合は、CSIRT担当者へ差し戻す。
F3	運用実務実施責任者は、セキュリティ月次報告会に参加する。
H1	SOC担当者は、前月分のセキュリティインシデントの情報、定期報告書用の情報を収集する。
H2	SOC担当者は、セキュリティインシデント情報、定期報告書用情報を整理する。日付ごとのソート、情報の更新などを行う。
I1	CSIRT担当者は、SOC担当者にて整理したセキュリティインシデント情報、定期報告書用情報を受領する。
I2	CSIRT担当者は、受領したセキュリティインシデント情報、定期報告書用情報に過不足が無いかを確認する。不足が有る場合はSOC担当者へ再度整理の依頼をする。過不足無しであれば、定期報告書の作成を実施する。
I3	CSIRT担当者は、定期報告書の作成を実施する。
I4	CSIRT担当者は、セキュリティ月次報告会を開催する。
I5	運用業務実施責任者はシステム管理者から報告書の内容について修正指示を受領する。
I6	システム運用担当者は、運用業務実施責任者から報告会後の修正について指示を受領し修正点を確認する。
I7	システム運用担当者は、修正点を月次報告書に反映する。
I8	システム運用担当者は、運用業務実施責任者に修正した報告書を提出する。

フロー名称	説明	作業トリガー
定期SIEM分析	各作業トリガーを契機とするSIEMや製品管理コンソールによるセキュリティ分析の業務フローを示す。	・ログレビューによる異常の発見 ・日時の定例業務（時間をトリガーとする） ・月次セキュリティ報告書の作成のための分析

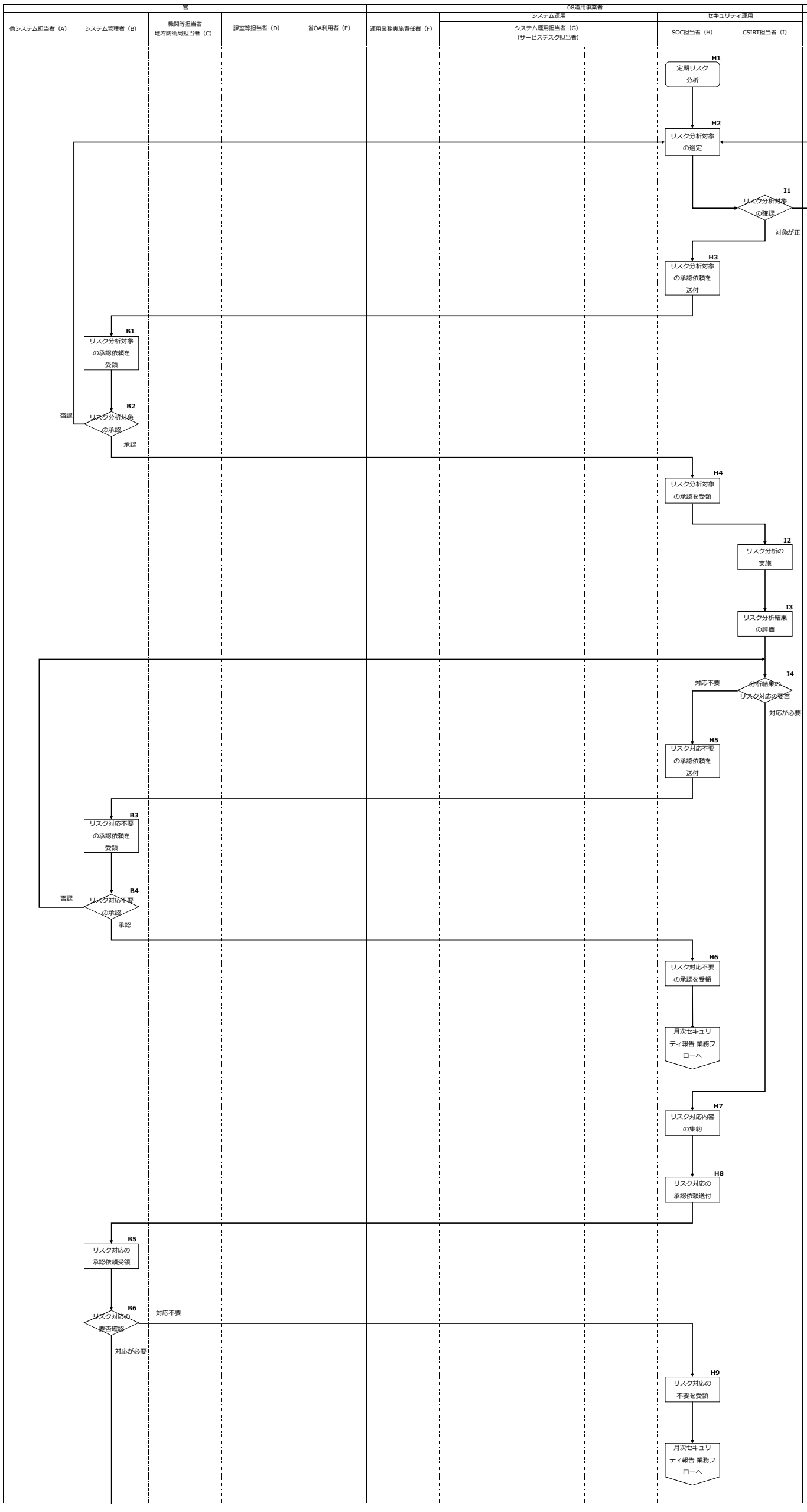


項番	説明
B1	システム管理者は、運用業務実施責任者より追加ヒアリング情報収集依頼を受領する。
B2	システム管理者は、各システム担当者へ追加ヒアリング情報の確認を実施する。
B3	システム管理者は、各担当者より追加ヒアリング情報を受領し、その情報をシステム運用担当者に送付する。
B4	システム管理者は、SOC担当者より作業計画を受領する。
B5	システム管理者は、作業計画を承認するか否かを判断する。
B6	システム管理者は、SOC担当者より作業完了報告を受領する。
C1	機関等担当者・地方防衛局担当者は、システム管理者より追加ヒアリング情報収集依頼を受領する。
C2	機関等担当者・地方防衛局担当者は、追加ヒアリング情報収集を実施する。
D1	課室等担当者は、システム管理者より追加ヒアリング情報収集依頼を受領する
D2	課室等担当者は、追加ヒアリング情報収集を実施する。
E1	省OA利用者は、システム管理者より追加ヒアリング情報収集依頼を受領する。
E2	省OA利用者は、追加ヒアリング情報収集を実施する。
F1	運用業務実施責任者は、SOC担当者からの追加ヒアリング情報収集依頼をシステム管理者へ送付する。
G1	システム運用担当者は、SOC担当者より追加情報収集依頼を受領する。
G2	システム運用担当者は、追加収集情報の確認を実施する。
G3	システム運用担当者は、システム担当者側に追加ヒアリングが必要かを判断する。
G4	システム運用担当者は、追加のログ収集を実施する。
G5	システム運用担当者は、システム管理者より追加ヒアリング情報を受領する。
G6	システム運用担当者は、追加情報の内容を確認し、情報が充足しているか確認を実施する。
G7	システム運用担当者は、追加情報をSOC担当者に送付する。
G8	システム運用担当者は、SOC担当者より追加対応依頼を受領する。
G9	システム運用担当者は、追加対応を実施する。
G10	システム運用担当者は、SOC担当者へ追加対応完了報告を送付する。
H1	SOC担当者は、ログの収集を実施する。ストレージから情報を取得する。
H2	自動処理により、異常を検知する。
H3	SOC担当者は、検出内容に異常があるかの確認を実施する。
H4	SOC担当者は、検出内容の確認を実施する。
H5	SOC担当者は、検知背景の内容の確認を実施する。
H6	SOC担当者は、システム運用担当者より追加情報を受領する。
H7	SOC担当者は、CSIRT担当者より追加対応依頼を受領し、システム運用担当者へ追加対応依頼を送付する。
H8	SOC担当者は、システム運用担当者より追加対応完了報告を受領し、CSIRT担当者へ追加対応完了報告を送付する。
H9	SOC担当者は、静観対応を実施する。
H10	SOC担当者は、監視・分析の調整が必要かの判断を実施する。
H11	SOC担当者は、作業計画を作成する。
H12	SOC担当者は、システム管理者に作業計画の承認依頼を送付する。
H13	SOC担当者は、作業計画を基に作業を実施する。
H14	SOC担当者は、正常性の確認を実施する。
H15	SOC担当者は、作業完了報告を実施する。
H16	SOC担当者は、変更管理台帳へ記録をする。
H17	SOC担当者は、構成情報・構成管理台帳を更新する。
I1	CSIRT担当者は、SOC担当者よりエスカレーションを受領する。
I2	CSIRT担当者は、検知内容と事象の確認を行い、危険性を判断する。
I3	CSIRT担当者は、インシデントか否かを判断する。
I4	CSIRT担当者は、システム運用側で追加の対応が必要かどうかを判断する。
I5	CSIRT担当者は、システム運用側での対応内容の確認を実施する。
I6	CSIRT担当者は、追加の対応が完了しているかを判断する。
I7	CSIRT担当者は、SOC担当者と確認し静観対応を実施する。
I8	CSIRT担当者は、SOC担当者と確認し監視・分析の調整が必要かを判断する。
I9	CSIRT担当者は、設定値の見直しを実施する。
I10	CSIRT担当者は、作業計画にシステム管理者の承認が必要かを判断する。
I11	CSIRT担当者は、SOC担当者と正常性の確認を実施する。

フロー名称	説明	作業トリガー
定期SIEM分析	各作業トリガーを契機とするSIEMや製品管理コンソールによるセキュリティ分析の業務フローを示す。	・ログレビューによる異常の発見 ・日時の定例業務（時間をトリガーとする） ・月次セキュリティ報告書の作成のための分析



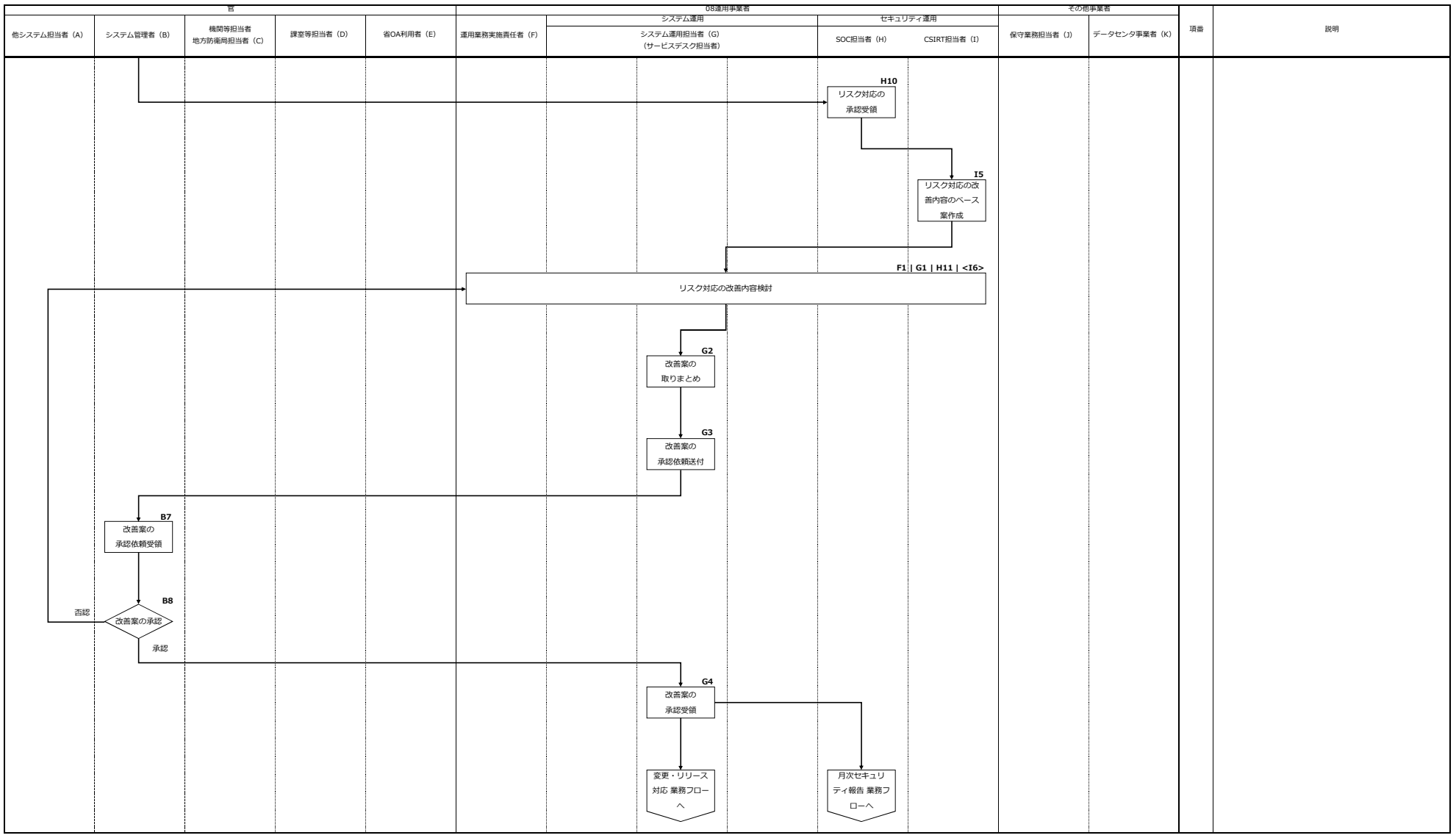
フロー名称	説明	作業トリガー
情報セキュリティリスク評価	定期リスク分析をトリガーとするリスク分析評価の対応フローを示す。 半年に1回、システムの構成や機能より対象を選定し、官と合意した上でリスク評価を行うこととする。	・定期リスク分析



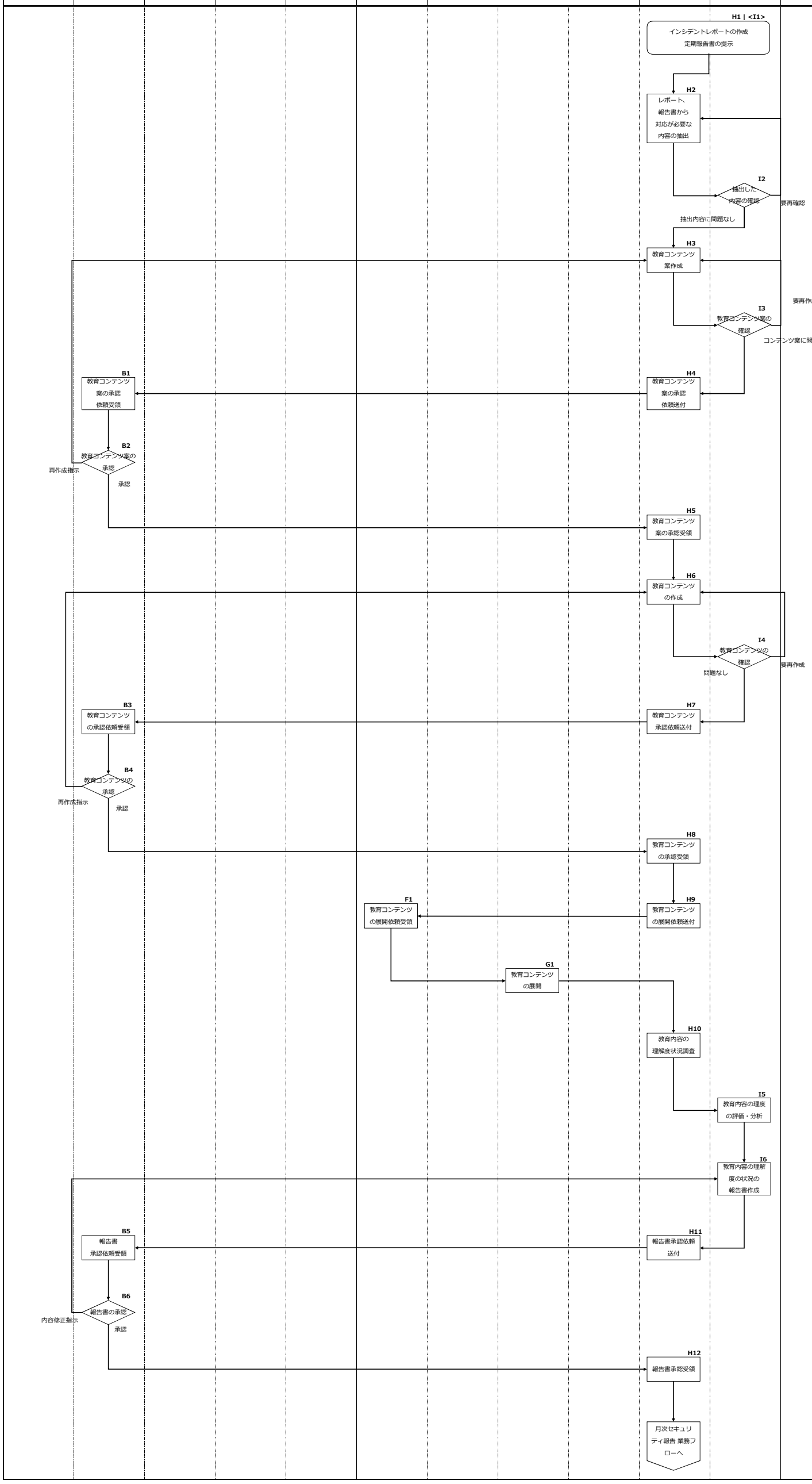
項番	説明
B1	システム管理者は、SOC担当者より、リスク分析対象の承認依頼を受領する。
B2	システム管理者は、リスク分析対象の承認の判断を行う。
B3	システム管理者は、SOC担当者より、リスク対応不要の承認依頼を受領する。
B4	システム管理者は、リスク対応不要の承認の判断を行う。
B5	システム管理者は、SOC担当者より、リスク対応の承認依頼を受領する。
B6	システム管理者は、リスク対応の要否の判断を行う。
B7	システム管理者は、SOC担当者より、改善案の承認依頼を受領する。
B8	システム管理者は、改善安良承認の判断を行う。
F1	運用業務実施責任者は、リスク対応の改善内容を検討する。
G1	システム運用担当者は、リスク対応の改善内容を検討する。
G2	システム運用担当者は、リスク対応の改善案の取りまとめを行う。
G3	システム運用担当者は、システム管理者へ、改善案の承認依頼を送付する。
G4	システム運用担当者は、システム管理者より、改善案の承認を受領する。
H1	SOC担当者は、定期リスク分析を行う。 ※定期リスク分析の実施頻度に関しては、運用設計内で調整
H2	SOC担当者は、リスク分析対象の選定を行う。 ※前回のリスク分析対象も今回の対象として含める
H3	SOC担当者は、システム管理者へ、リスク分析対象の承認依頼を送付する。
H4	SOC担当者は、システム管理者より、リスク分析対象の承認を受領する。
H5	SOC担当者は、システム管理者へ、対応する必要が無いためリスク対応不要とする場合、および、リスク受容の上対応不要とする承認依頼を送付する。 ※対応不要な理由を申請時に明記し、「リスク受容」「対応不要」がわかるように依頼する。
H6	SOC担当者は、システム管理者より、リスク対応不要の承認依頼を受領する。
H7	SOC担当者は、リスク対応内容の取りまとめを行う。
H8	SOC担当者は、システム管理者より、リスク対応の承認依頼を送付する。
H9	SOC担当者は、システム管理者より、リスク対応不要の連絡を受領する。
H10	SOC担当者は、システム管理者より、リスク対応承認を受領する。
H11	SOC担当者は、リスク対応の改善内容を検討する。
I1	CSIRT担当者は、SOC担当者が選定したリスク分析対象の確認を行う。
I2	CSIRT担当者は、リスク分析を行う。
I3	CSIRT担当者は、リスク分析結果の評価を行う。
I4	CSIRT担当者は、リスク分析結果から対応の要否を判断する。
I5	CSIRT担当者は、リスク対応の改善内容のベースを作成する。
I6	CSIRT担当者は、「リスク対応の改善内容のベース案」の内容を基に他担当者に協力を仰ぎつつ、リスク対応の改善内容を検討する。

付表１０　業務フロー（続き）
情報セキュリティリスク評価（続き）

フロー名称	説明	作業トリガー
情報セキュリティリスク評価	定期リスク分析をトリガーとするリスク分析評価の対応フローを示す。 半年に1回、システムの構成や機能より対象を選定し、官と合意した上でリスク評価を行うこととする。	・定期リスク分析



フロー名称	説明	作業トリガー
セキュリティ教育	インシデントレポート・月次セキュリティ報告などをまとめて、 省OA利用開始時、四半期に1回実施するセキュリティ教育対応フローを示す。	・インシデントレポートの提出 ・定期報告書の提示



項番	説明
B1	システム管理者は、SOC担当者より、教育コンテンツ案の承認依頼を受領する
B2	システム管理者は、教育コンテンツ案の承認の判断を行う
B3	システム管理者は、運用業務実施責任者より、教育コンテンツの承認依頼を受領する
B4	システム管理者は、教育コンテンツの承認の判断を行う
B5	システム管理者は、運用業務実施責任者より、報告書の承認依頼を受領する
B6	システム管理者は、報告書の承認の判断を行う
F1	運用業務実施責任者は、SOC担当者より、教育コンテンツの展開指示を受領し、システム運用担当者に展開を指示する
G1	システム運用担当者は、運用業務実施責任者より、教育コンテンツの展開指示を受領し、展開を行う ※教育コンテンツの展開方法に関しては、運用設計内で調整
H1	SOC担当者は、インシデントレポートの作成、定期報告書の提示を行う（緊急や重大インシデントの臨、臨時対応も含む）
H2	SOC担当者は、インシデントレポート、定期報告書から対応必要なものを抽出する
H3	SOC担当者は、教育コンテンツ案を作成する
H4	SOC担当者は、システム管理者へ、教育コンテンツ案、教育対象選定結果の承認依頼を送付する
H5	SOC担当者は、システム管理者より、教育コンテンツ案の承認を受領する
H6	SOC担当者は、教育コンテンツを作成する
H7	SOC担当者は、システム管理者へ、教育コンテンツの承認依頼を送付する
H8	SOC担当者は、システム管理者より、教育コンテンツの承認を受領する
H9	SOC担当者は、運用業務実施責任者へ、教育コンテンツの展開依頼を送付する
H10	SOC担当者は、教育内容の理解度の遵守状況の調査を行う
H11	SOC担当者は、システム管理者へ、報告書の承認依頼を送付する
H12	SOC担当者は、システム管理者より、報告書の承認を受領する
I1	CSIRT担当者は主体となり、インシデントレポートの作成、定期報告書の提示を行う
I2	CSIRT担当者は、SOC担当者が抽出した内容、セキュリティ教育対象の選定の確認を行う。
I3	CSIRT担当者は、SOC担当者が作成した教育コンテンツ案の確認を行う
I4	CSIRT担当者は、SOC担当者が作成した教育コンテンツの確認を行う
I5	CSIRT担当者は、教育の理解度状況の評価・分析を行う
I6	CSIRT担当者は、教育の理解度状況と教育が必要と思われる内容の選定結果の報告書の作成を行う

■ フロー内で用いる図形の凡例

図形サンプル	図形に関する説明
<開始処理>	当該フローの起点は、角の取れた四角形を用いる。 なお、起点は「開始」と記載せず、具体的な処理内容を記載する。
<処理>	<処理> に記載されている作業を実施する。 なお、作業内容の詳細は運用マニュアルに記載する。
<F4> | G1 <複数処理>	複数の登場人物に跨る処理の場合、その処理の主体となる者には、 右肩の**採番に <> を付与**する。 なお、特定の主体が存在せず並行的な処理の場合は、何も付与しない。
<自動処理>	人手を介さずシステムの自動処理で実施する場合に用いる。 <自動処理> に記載されている作業を自動処理させる。
<分岐>	<分岐> に記載されている判断を行い、処理を分岐させる。 分岐は左右もしくは下に分かれ、条件が一致する先の処理を行う。
<数字>	**同フロー内**の <数字> に記載されている番号に接続する。 または、接続される。
<別フロー>	処理を <別フロー> に記載されている**別フローへ**接続する。 または、**別フローから**派生して本フローに接続される。
	フロー内で矢印線が交差する場合は、 横向きの矢印線に図形サンプルで示す飛び越えを行わせる。
終了	当該フローの処理を終了する。

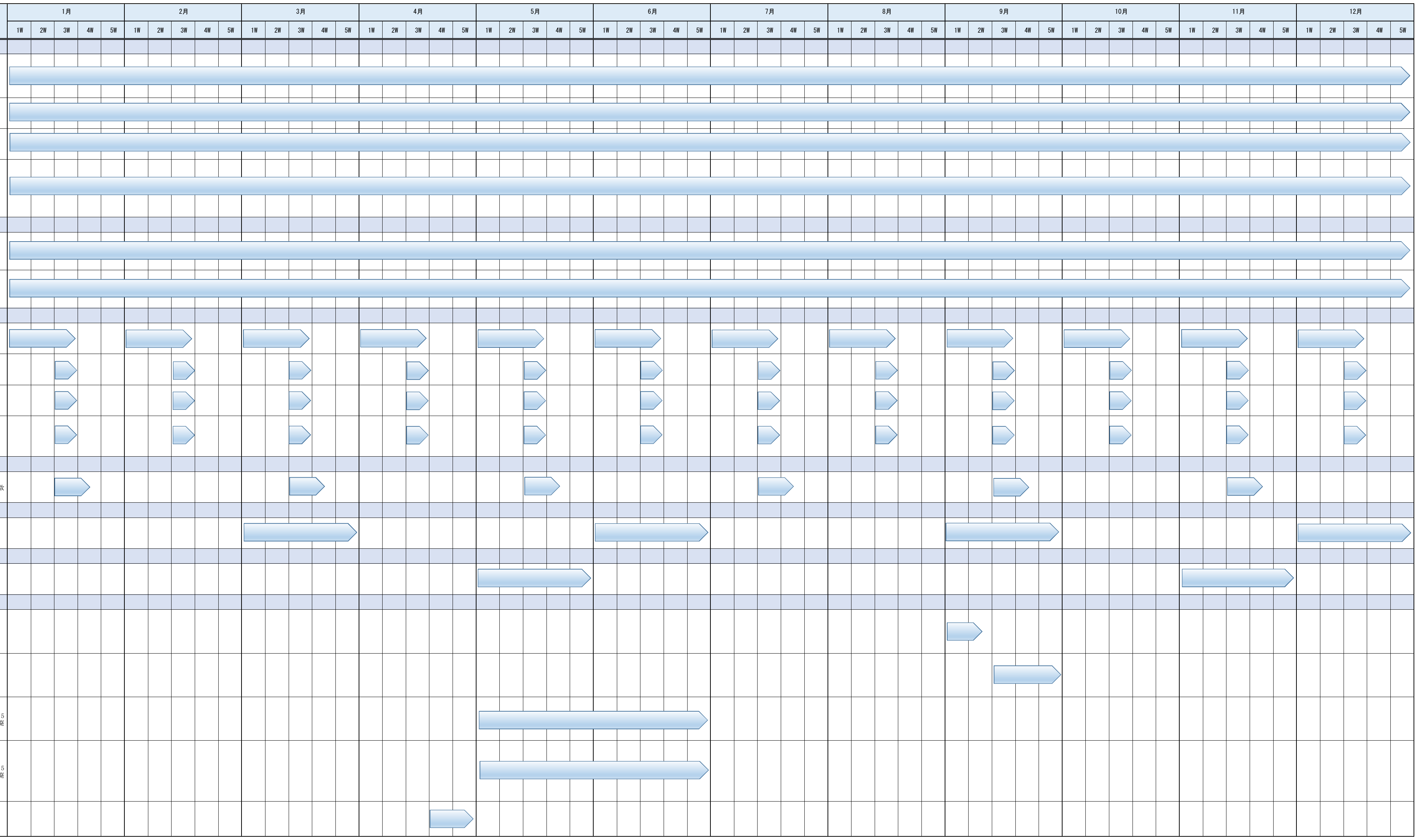
付表１１　運用作業実施スケジュール案
全体スケジュール

	作業項目	業務概要	実施タイミング	令和8年						令和9年												令和10年												令和11年												令和12年		
				7月	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
	全体作業																																														
1	運用立ち上げ	本番運用前の運用立ち上げ	令和8年8月～9月																																												
2	運用承認後の脆弱性診断（RMF）	※運用承認後の脆弱性診断を実施する。	仮）令和9年8月～9月（官からの依頼に基づく）																																											
3	サービスレベル目標値見直し	※運用開始後3カ月のサービスレベル測定の実測値をもとにサービスレベル目標値を適宜更新する。	本運用開始後の10～12月の結果を基に1月に更新																																											
4	04増設基盤運用	令和4年度に増設された省OAIaaS基盤に係る運用管理業務を実施する。	～令和10年2月																																											
5	05増設基盤運用	令和5年度に増設された省OAIaaS基盤に係る運用管理業務を実施する。	～令和10年2月																																											
6	06増設基盤運用	令和6年度に増設された省OAIaaS基盤に係る運用管理業務を実施する。	～令和11年2月																																											
7	北関東、九州防衛局統合	北関東、九州防衛局統合	令和9年3月～運用開始																																											
8	Feature Update適応対応	メーカサポート継続のために端末のOSにFeature Updateを適用する必要がある。検証環境にて検証を行い、省OA利用がが利用中の端末含めた全端末への適用を計画し、実施する。	部外端末：令和9年10月までに実施（24H2サポート期限） 部内端末：令和10年10月までに実施（25H2サポート期限）													部外端末										部内端末																					
9	運用引継ぎ	次の運用役務への引継ぎ	令和12年3月																																												

付表１１　運用作業実施スケジュール案

年間スケジュール

区分	No.	作業項目	業務概要	実施タイミング
定常業務		**日次作業**		
	1	システムリソース利用状況の分析・評価	システムリソースの利用状況を日次で監視し、データを収集、評価、報告、必要に応じて保守へエスカレーションする。サーバ類のCPU使用率、メモリ使用率、ディスク使用容量、ディスクI/O、主要なネットワーク境界に設置されたファイアウォール装置のトラフィックを監視する。	毎日実施
	2	バックアップ取得状況の確認	想定外のバックアップ失敗が発生した際にも早期の対処を図るため、自動実行されるバックアップジョブの成否の確認を日次で実施する。	毎日実施
	3	予防運用・保守管理（ランプチェック）	市ヶ谷、第1センター、第2センターのサーバー室に設置された省OA機器の正常性確認を実施するため、ランプチェックを実施する。	毎日実施
	4	【SOC】定期SIEM分析	リアルタイム監視では見落とされる可能性のある複合的な不審な兆候を特定するために、ログに対して定期的にフィルターを適用し脅威の検出の有無を確認する。検出に対して検知背景の確認による正当性判断、検知内容・事象確認を実施し、インシデント判定を実施する。必要に応じで、追加のヒアリングやログ確認を実施する。セキュリティインシデントと判定されたものは対処に進む。	毎日実施
		週次作業		
	1	週次運用状況報告	週次での運用業務の実施状況を正確に把握し報告するために、1週間分の運用業務の実績を収集、精査し、週次運用状況報告書の作成、共有、報告を実施する。	週に一度実施 （実施日は協議のうえ、決定する）
	2	【SOC】脅威・脆弱性管理	脆弱性情報の定期的な収集、定期リスク診断から導出された脆弱性情報をもとに、それぞれに脆弱性について分析、評価、対応方針の検討を実施する。検討した方針に従い、検証環境での適用、本番環境への適用を実施する。	定期的な脆弱性情報の収集は週に一度実施 （実施日は協議のうえ、決定する） ※緊急の場合は随時実施
		月次作業		
	1	サービスレベル分析・評価・報告	定められたサービスレベル（問い合わせ回答時間、作業応動時間、障害復旧時間、システム可用性等）について、測定、実績値の評価して目標値に対する達成状況を確認、月次報告および年次報告にてシステム管理者へ報告する。	分析は月上旬、評価・報告は中旬 （実施日は協議のうえ、決定する）
	2	月次運用状況報告	月次での運用業務の実施状況を正確に把握し報告するために、1か月分の運用業務の実績を収集、精査、分析し、問合せの傾向、SLAの達成状況などの分析項目を含めた、月次運用状況報告書の作成、共有、報告を実施する。	仮）先月分を翌月中旬に実施 （実施日は協議のうえ、決定する）
	3	システム利用状況報告	利用者によるシステム利用状況を把握し報告するために、1か月分のシステム利用情報を収集、精査し、システム利用状況報告書の作成、共有、報告を実施する。	仮）先月分を翌月中旬に実施 （実施日は協議のうえ、決定する）
	4	【SOC】月次セキュリティ報告	月次での、脅威検知や防御の状況、ログ分析の結果、セキュリティインシデントの対応状況を報告する。攻撃深度を表す「フェーズ」ごとの相関分析の結果、セキュリティ製品やシステム境界ごとの傾向分析の結果、トリガーごとのセキュリティインシデントの対応状況を報告に含める。	仮）先月分を翌月中旬に実施 （実施日は協議のうえ、決定する）
		隔月作業		
	1	地方防衛局の巡回役務	保守事業者にて修理済みの端末のキッティング、リモートでの実施が不可のSDカードの登録、申請により払い出した機器や返却された機器の在庫状況の確認を実施する。隔月で本局および支局、加えて修理済み機器のあるその他拠点を訪問する。	奇数月中旬に実施 （4月と8月に人事異動があるため、偶数月ではなく奇数月に実施）
		四半期作業		
	1	【SOC】セキュリティ教育	職員のセキュリティ意識の向上のため、セキュリティ教育計画やポリシーの見直しを実施する。	仮）12月、3月、6月、9月に実施 （実施日は協議のうえ、決定する） ※省OA利用開始時は随時実施
		半期作業		
	1	【SOC】情報セキュリティリスク評価	定期的なリスク評価を行い、システムの構成に対する評価や更新の必要性を確認する。	仮）5月、11月に実施 （リスク分析は次年度以降から実施）
		年次作業		
	1	大規模障害切替訓練	大規模障害（災害）が発生した際のシステム切り替え作業等について有事の際に滞りなく対応が行えるようにするため、平時のうちに「訓練」として手順や連絡体制を確認することで、運用員の業務習熟と問題点の改善を図る。	仮）9月上旬に実施 （実施日は協議のうえ、決定する）
	2	アカウント・ファイル共有アクセス権の棚卸	人事異動等に伴う不要アカウントや不要ライセンスを排除し、適正なアカウント状態を維持するとともに、共有フォルダのセキュリティグループに属するアカウントの妥当性を確認する。	仮）8月人事異動後の9月下旬に実施 （実施日は協議のうえ、決定する）
	3	システム構成情報の棚卸	システム構成情報と実態の差異を定期的に確認し、反映、報告する。システム構成書、システム設定書、構成図、NW機器の設定ファイルは、変更管理台帳をもとに、運用および保守が実施した変更が反映されていることを確認する。ケーブル配線図は、課室等担当者に変更の有無の確認と、差分があれば更新を依頼する。	5月、6月 （2月末に局の統廃合があり、繁忙期の3～4月を避け、5～6月でシステム構成情報の棚卸をし、8月の次の局統廃合までに情報を整理する）
	4	資産情報の棚卸	システム構成情報と実態の差異を定期的に確認し、反映、報告する。借上品や官品のハードウェアについては、申請管理機能、物品管理機能、構成管理機能と実態の差異を確認する。運用で保管する在庫は運用で確認し、払出済みの機器は機関担当者等に確認を依頼する。ソフトウェアについては、ライセンスの超過の有無、原因の分析、是正対応を実施する。	5月、6月 （2月末に局の統廃合があり、繁忙期の3～4月を避け、5～6月でシステム構成情報の棚卸をし、8月の次の局統廃合までに情報を整理する）
	5	年次運用状況報告	年次での運用業務の実施状況を総合的に把握し報告するために、1年分の運用業務の実績を収集、精査したうえで、課題および翌年度に向けた改善施策を取りまとめ、年次運用状況報告書の作成、共有、報告を実施する。	仮）昨年分を4月末に報告 ※最終年度は2月分までを3月末に報告 （報告事項が決まってから報告のタイミングを決定する）



付表１２ 既存物品管理情報（Excel台帳）

No.	物品管理情報名	台帳ファイル名	内容	対象(数量)
1	官品据え置きモニター	据え置き官品モニタ(官品)_内局買取端末のみ利用可.xlsx	官品モニタの貸出管理	据え置きモニタ(50)
2	モバイルモニター管理台帳	モバイルモニタ(官品).xlsx	官品モバイルモニタの貸出管理	モバイルモニタ(20)
3	モバイルスキャナー管理台帳	モバイルスキャナ(官品).xlsx	官品モバイルスキャナの貸出管理	モバイルスキャナ(10)
4	官品DVDドライブ管理台帳	【官品】DVDドライブ管理台帳.xlsx	官品DVDドライブとBlu-rayドライブの貸出管理	DVDドライブ(109)
				Blu-rayドライブ(9)
5	消耗品管理台帳	01.USB-HUB管理台帳.xlsx	消耗品関連の在庫管理	LANケーブルなど45種類(複数)
		02.VGAアダプタ台帳.xlsx		
		消耗品管理台帳【プルダウン修正版】.xlsx		
6	ヘッドセット・カメラ・スピーカマイク管理台帳	カメラ&ヘッドセット&スピーカーマイク管理台帳.xlsx	ヘッドセット、カメラ、スピーカマイクなどの貸出管理	ヘッドセット(161)
				カメラ(120)
				スピーカマイク(65)
				会議用スピーカフォン(30)
				広角カメラ(30)
				大会議用Webシステム(20)
				集音マイク(3)
				スピーカ(4)
7	ログイン専用カード管理台帳	ログイン専用カード管理台帳.xlsx	ログイン専用カードの貸出管理	ログイン専用カード(1897)
8	ルータ台帳	2025年度_ルーター管理台帳.xlsx	ルータの貸出管理	ルータ(119)
9	移動端末用鞄管理台帳	移動端末用カバン管理台帳.xlsx	移動端末に紐づいた鞄とインナーケースの貸出管理	ハード(9)
				ソフト(59)
				インナーケース(149)
10	トナー台帳	トナー台帳_202509以降.xlsx	プリンタ機種に対応したトナー各色の在庫管理 （借上4機種、官品1機種RICOH P C320）	官品1機種(RICOH P C320)の下記トナー
				・Black(-1)
				・Cyan(10)
				・Magenta(16)
				・Yellow(15)
				・廃トナーボトル(19)