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の解説①

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情報セキュリティ基準について

第１．１版

令和５年７月１２日

防衛装備庁装備政策部

改版履歴

版数	改版日	改版内容	備考
1.0	令和５年６月２日	新規作成	
1.1	令和５年7月１２日	組織改編に基づく改版、その他誤字等修正	装備保全管理官⇒装備保全管理課長

はじめに

１．目的

本資料は、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（防装庁（事）第１３７号。令和４年３月３１日。）別添装備品等及び役務の調達における情報セキュリティ確保に関する特約条項（以下「特約条項」という。）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」の解説資料として作成しています。

２．記載内容

資料本編の各ページには、特約条項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の規定、規定制定の解説等を記載しています。

３．その他注意事項

・目次の項番（「第〇」の部分）は、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の項番と対応しています。

目　　次

第４　情報セキュリティ基本方針等　・・・・Ｐ 1

第５　組織のセキュリティ　・・・・Ｐ 2

第６　保護すべき情報の管理　・・・・Ｐ 6

第７　情報セキュリティ教育及び訓練　・・・・Ｐ 12

第８　物理的及び環境的セキュリティ　・・・・Ｐ 13

第９　保護システムについての管理策　・・・・Ｐ 20

第10　情報セキュリティ事故等への対応　・・・・Ｐ 21

第11　情報セキュリティ事故等発生時の対応　・・・・Ｐ 37

第12　リスク査定　・・・・Ｐ 40

第13　セキュリティ監査　・・・・Ｐ 42

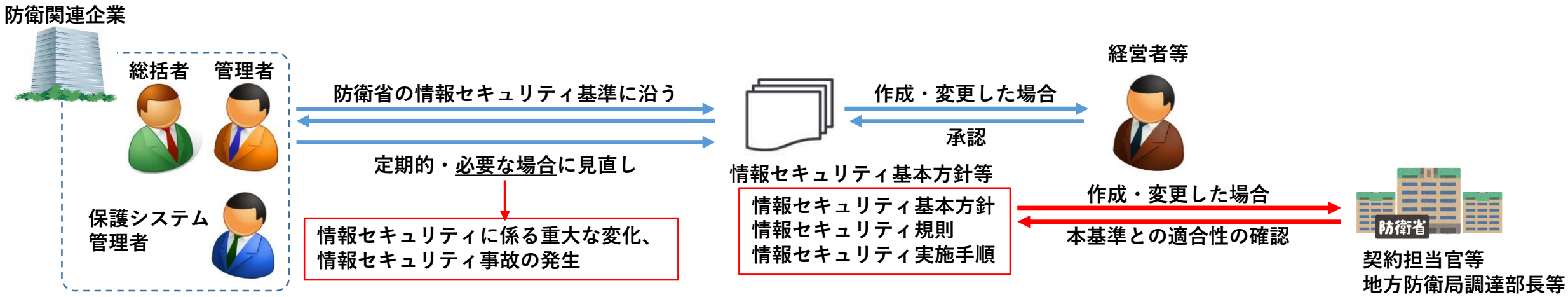
第14　防衛省による監査　・・・・Ｐ 46

（付録）　用語の解説

第４　情報セキュリティ基本方針等

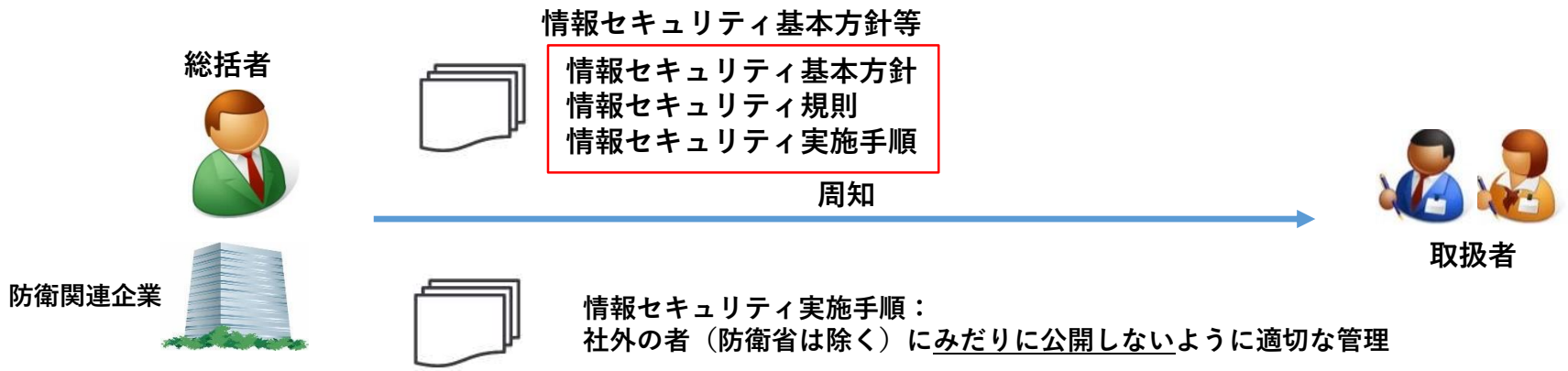
1　情報セキュリティ基本方針等の作成及び変更

(1) 防衛関連企業は、本基準の内容に沿った情報セキュリティ基本方針等を作成し、経営者等の承認を得るものとする。
(2) 防衛関連企業は、情報セキュリティ基本方針等を適切、有効及び妥当なものとするため、定期的な見直しを実施するとともに、情報セキュリティに係る重大な変化及び情報セキュリティ事故が発生した場合は、その都度見直しを実施し、必要に応じて情報セキュリティ基本方針等を変更し、経営者等の承認を得るものとする。
(3)防衛関連企業は、情報セキュリティ基本方針等を作成又は変更する場合は、本基準との適合性に関する防衛省の確認を受けるものとする。



2　情報セキュリティ基本方針等の周知等

(1) 保護すべき情報の管理全般に係る総括的な責任を負う者（以下「総括者」という。）は、情報セキュリティ基本方針等を取扱者に周知するものとする。
(2) 防衛関連企業は、情報セキュリティ実施手順を社外の者（契約に関係する防衛省の職員を除く。）にみだりに公開しないよう適切に管理するものとする。



第５　組織のセキュリティ

１　経営者等の職責

経営者等は自社の情報セキュリティに係る最高かつ最終的な権限及び責任を有するものとする。

２　経営者等及び取扱者の責務

(1) 取扱者の指定等

ア　経営者等は、保護すべき情報の取扱者の指定の範囲を業務の遂行上必要最小限度に制限するとともに、次に掲げる事項に合意した者の中からふさわしい者を取扱者に指定するものとする。

(ｱ) 在職中及び離職後において、業務上知り得た保護すべき情報を、第三者に漏えいしないこと（以下「守秘義務」という。）

(ｲ) 守秘義務に違反した場合に法律上の責任を負うこと。

(ｳ) 守秘義務の内容を理解し、かつ、承諾すること。

イ　経営者等は、保護すべき情報に係るすべての情報セキュリティの責任を明確にするため、取扱者のうち、ふさわしいと認める者を次に掲げる者に指定するものとする。

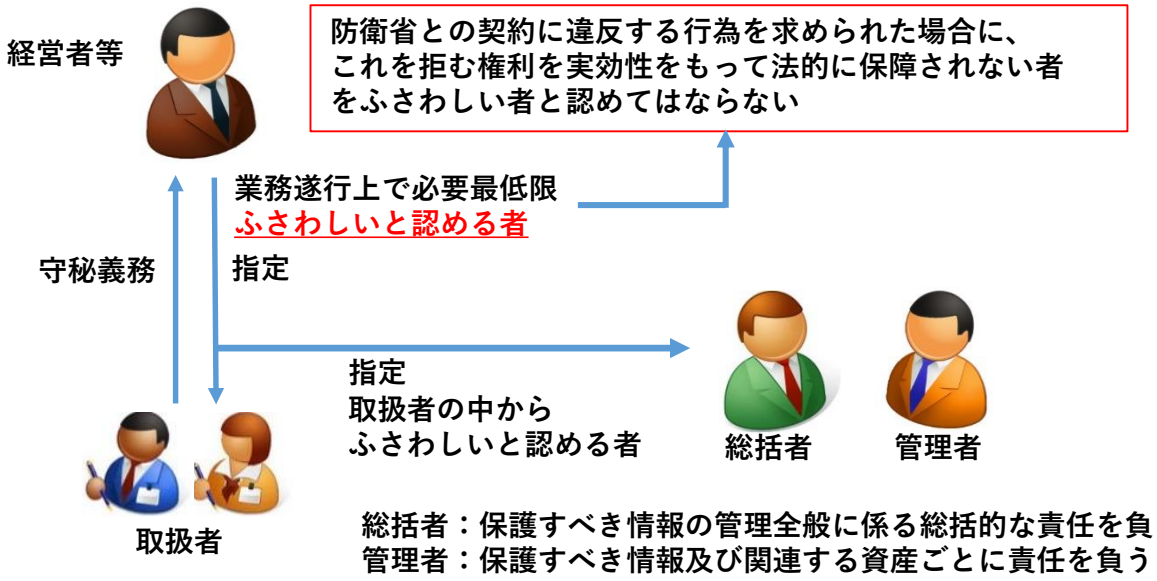
(ｱ) 総括者

(ｲ) 保護すべき情報及びこれに関連する資産ごとに、それぞれ管理責任を負う者（以下「管理者」という。）

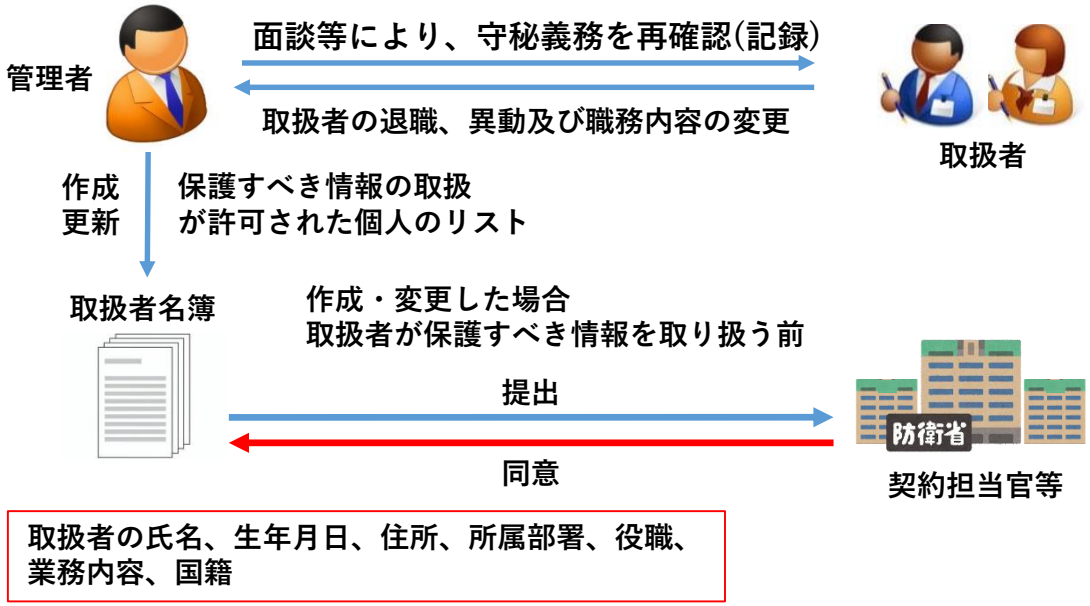
ウ　経営者等は、防衛省との契約に違反する行為を求められた場合に、これを拒む権利を実効性をもって法的に保障されない者をふさわしい者と認めてはならない。

エ　管理者は、取扱者として指定した個人の氏名、生年月日、所属する部署、役職、国籍等を記載したリスト(以下「取扱者名簿」という。)を作成又は更新し、取扱者に保護すべき情報を取り扱わせる前に、防衛省の確認を受けるものとする。

オ　管理者は、取扱者の退職、異動及び職務内容の変更などの理由により、保護すべき情報にアクセスする必要がなくなった場合は、取扱者名簿を更新するとともに、当該取扱者との面談等により、守秘義務を再確認するものとする。



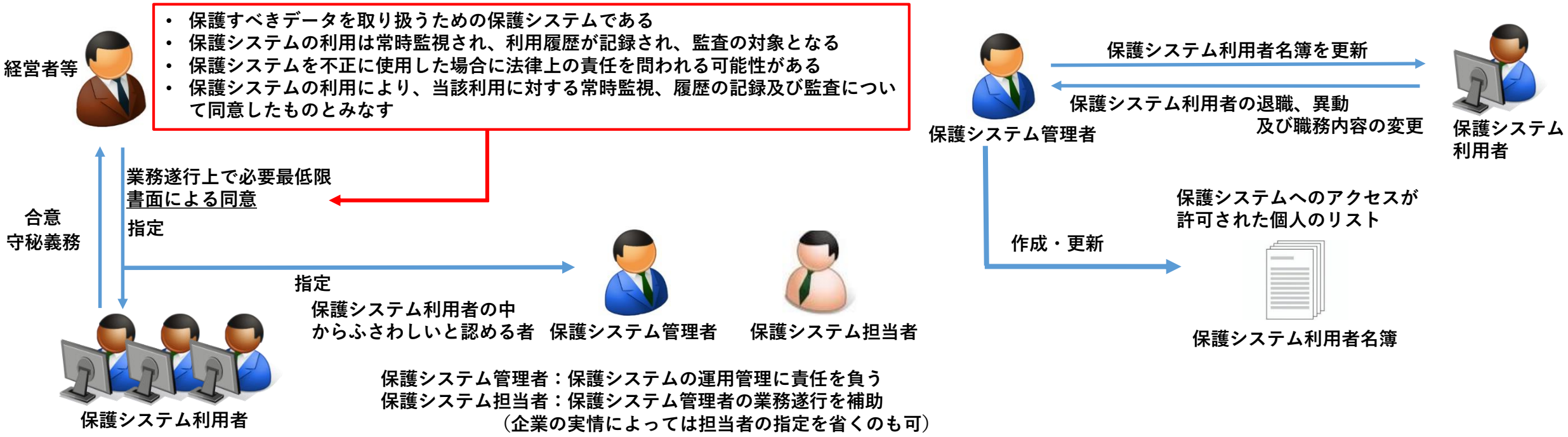
総括者：保護すべき情報の管理全般に係る総括的な責任を負う
管理者：保護すべき情報及び関連する資産ごとに責任を負う



取扱者の氏名、生年月日、住所、所属部署、役職、
業務内容、国籍

２　経営者等及び取扱者の責務

(2) 保護システム利用者の指定等
ア　経営者等は、保護システム利用者を指定するものとし、その指定の範囲を業務の遂行上必要最小限度に制限するものとする。その際、次に掲げる事項に関し書面による同意を得るものとする。なお、保護システムの利用により、当該利用に対する常時監視、履歴の記録及び監査について同意したものとみなす。
(ｱ) ログオンする情報システムが、保護すべきデータを取り扱うための保護システムであること
(ｲ) 保護システムの利用は常時監視されるとともに、利用履歴が記録され、監査の対象となること
(ｳ) 保護システムを不正に使用した場合に法律上の責任を問われる可能性があること
イ　経営者等は、保護システムに係るすべての情報セキュリティの責任を明確にするため、保護システム利用者のうち、ふさわしいと認める者を次に掲げる者に指定するものとする。
(ｱ) 保護システムの運用管理に責任を負う者（以下「保護システム管理者」という。）
(ｲ) 保護システム管理者の業務遂行を補佐する者（以下「保護システム担当者」という。）
ウ　保護システム管理者は、アに掲げる保護システム利用者の名簿（「保護システム利用者名簿」という。）を作成するものとし、保護システム利用者の退職、異動及び職務内容の変更などの理由により、保護システムを利用する必要がなくなった場合は、保護システム利用者名簿を更新するものとする。



保護システム管理者：保護システムの運用管理に責任を負う
保護システム担当者：保護システム管理者の業務遂行を補助
（企業の実情によっては担当者の指定を省くのも可）

２　経営者等及び取扱者の責務

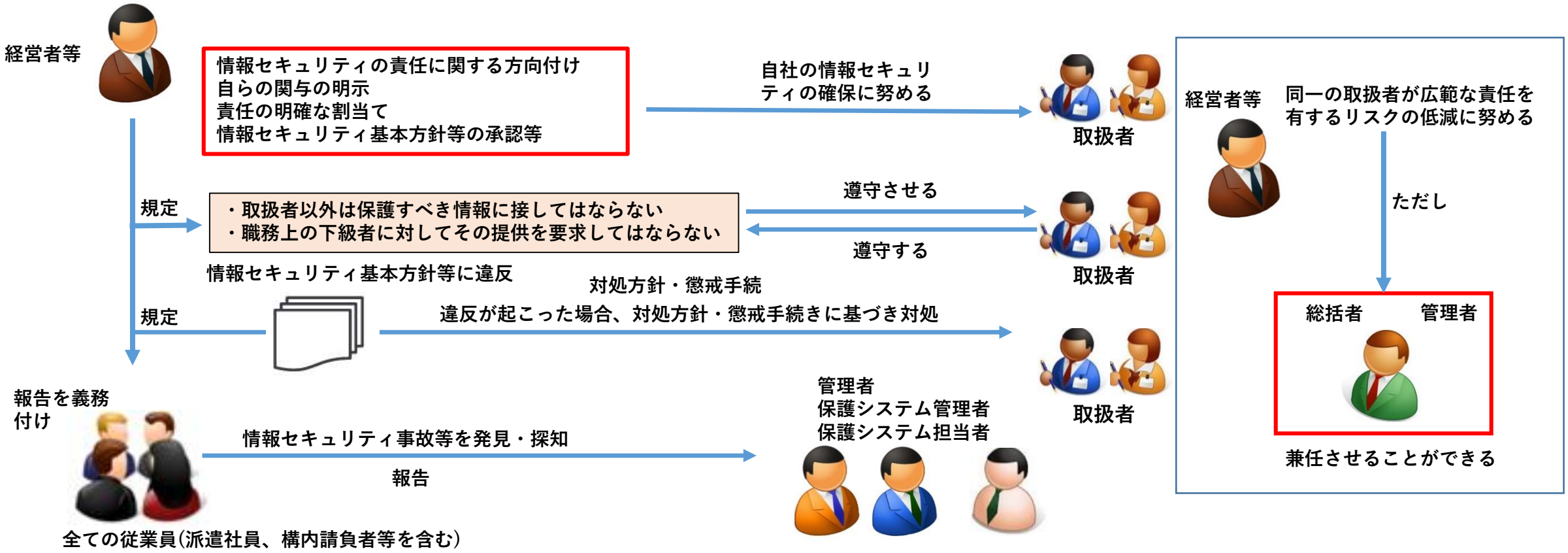
(3) 情報セキュリティの確保

ア　経営者等は、情報セキュリティの責任に関する明瞭な方向付け、自らの関与の明示、責任の明確な割当て及び情報セキュリティ基本方針等の承認等を通じ、自社における情報セキュリティの確保に努めるものとする。また、組織内において、取扱者以外の役員、管理職員等を含む従業員、その他の全ての構成員に対して、取扱者以外の者は保護すべき情報に接してはならず、かつ、職務上の下級者等に対してその提供を要求してはならないことを定めるものとする。

イ　経営者等は、全ての従業員に対し、情報セキュリティ事故等を発見又は検知した場合は、管理者（保護システムに係る情報セキュリティ事故等にあっては保護システム管理者又は保護システム担当者を含む。）に直ちに報告するよう義務付け、全ての従業員は、その義務を果たすものとする。

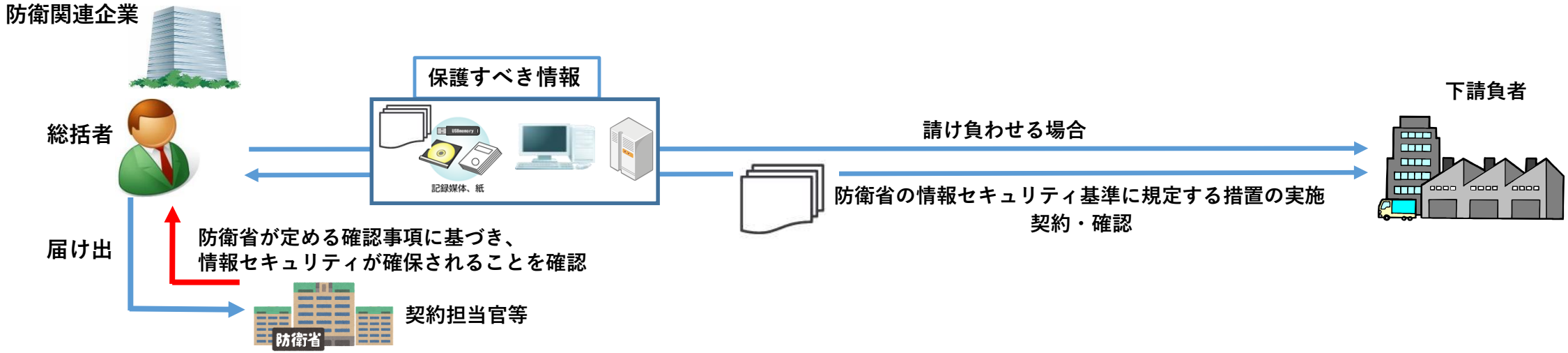
ウ　経営者等は、情報セキュリティ基本方針等に違反した取扱者に対する対処方針及び懲戒手続を定め、違反が生じた場合には、当該対処方針及び懲戒手続に基づき対処するものとする。

エ　経営者等は、前２号に規定する者、その他の責任の割当てについて、当該責任を業務の遂行上必要最小限に分割して割り当て、同一の取扱者に広範な責任を持たせてはならない。ただし、総括者及び管理者については、兼任させることができる。



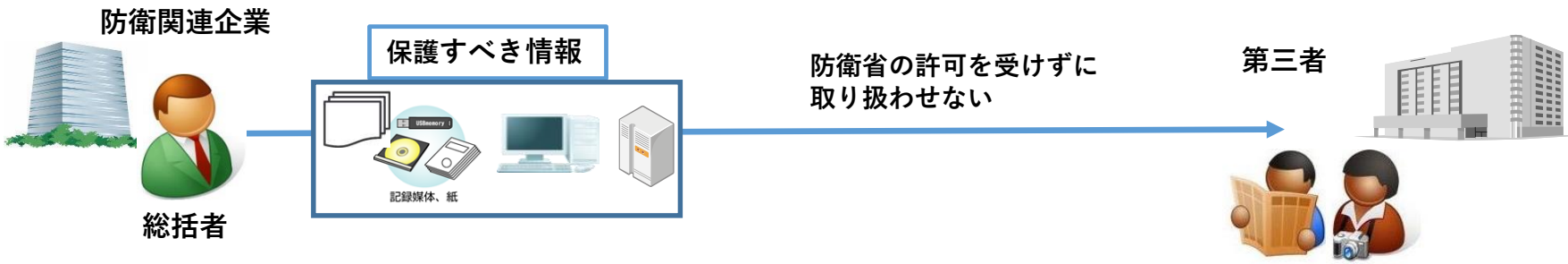
3　保護すべき情報を取り扱う下請負者

防衛関連企業は、契約の履行に当たり、保護すべき情報を取り扱う業務の下請負者に請け負わせる場合は、本基準に規定する措置の実施を当該下請負者との間で契約し、当該業務を始める前に、防衛省が定める確認事項に基づき、当該下請負者において情報セキュリティが確保されることを確認した後、防衛省に申請することとする。ただし、輸送その他保護すべき情報を知り得ないと防衛関連企業が認める業務を請け負わせる場合は、この限りでない。



4　第三者

(1) 第三者の保護すべき情報の取扱い
防衛関連企業は、防衛省の許可を受けずに第三者に保護すべき情報を取り扱わせてはならない。
(2) 第三者との約定からの保護すべき情報の除外
防衛関連企業は、第三者との契約において防衛関連企業の保有又は知り得た情報を伝達、交換、共有、提供する約定がある場合は、約定から保護すべき情報を除くものとする。ただし、事前に防衛省の許可を得た場合は、この限りでない。



第三者との契約において：
保有又は知り得た情報を伝達、交換、共有、提供する約定がある場合は、約定から保護すべき情報を除く（事前に防衛省の許可を受けた場合は、この限りでない）

※第三者の詳細は「（付録）用語の説明」ご参照。

第６　保護すべき情報の管理

１　保護すべき情報の分類

防衛関連企業は、保護すべき情報を他の情報から明確に区別できるよう適切に分類し、厳格に管理するものとする。

防衛関連企業

管理者

厳格に管理

保護すべき情報を他の情報から明確に区別して分類

保護すべき情報

２　保護すべき情報の目録の作成等

(1) 目録の作成

管理者は、保護すべき情報を保管した場所又は保存した保護システム、可搬記憶媒体等、保護すべき情報の管理状況を記載した目録を作成するものとする。

(2) 目録の更新

ア　管理者は、下記の（ｱ）から（ｳ）に掲げる措置（以下「接受等」という。）を実施する場合は、保護すべき情報の目録を更新するものとする。

(ｱ) 保護すべき情報を接受、作成、製作、複製（バックアップを含む。以下同じ。）

(ｲ) 保護すべき情報の閲覧又は持ち出し（取扱施設の外に持ち出すことをいい、貸出を含む。以下同じ。）

(ｳ) 保護すべき情報を送達、返却、提出又は廃棄

イ　目録には、接受等を行った者の氏名、所属及び所在等を記載するものとする。ただし、保護システムにおける保護すべきデータの閲覧については、システムログの記録により代用することができる。

(3) 目録等の保管

管理者は、保護すべき情報の目録は、不正なアクセス、改ざん及び盗難等から保護するため、文書により保管する場合は、施錠したロッカー等（第８第５項第２号の規定により鍵及び解錠キーを厳格に管理するものとする。以下同じ。）により、データで保存する場合には、暗号化により必要な期間保存又は保管するものとする。

防衛関連企業

管理者

（保管場所、保存した情報システム・可搬記憶媒体等）

保護すべき情報の管理状況を記載した目録を**作成**

保護すべき情報を接受、作成、製作、複製、閲覧、持ち出し、
送達、返却、提出、破棄する場ば、目録を**更新**

保護すべき情報の目録

接受等を行った者の氏名、所属、所在等

目録を更新

（会社内の取扱者の接受等については所在は省略可）

保護システムにおける保護すべきデータの閲覧については、
システムログの記録により代用することができる。

必要な期間

保存又は保管

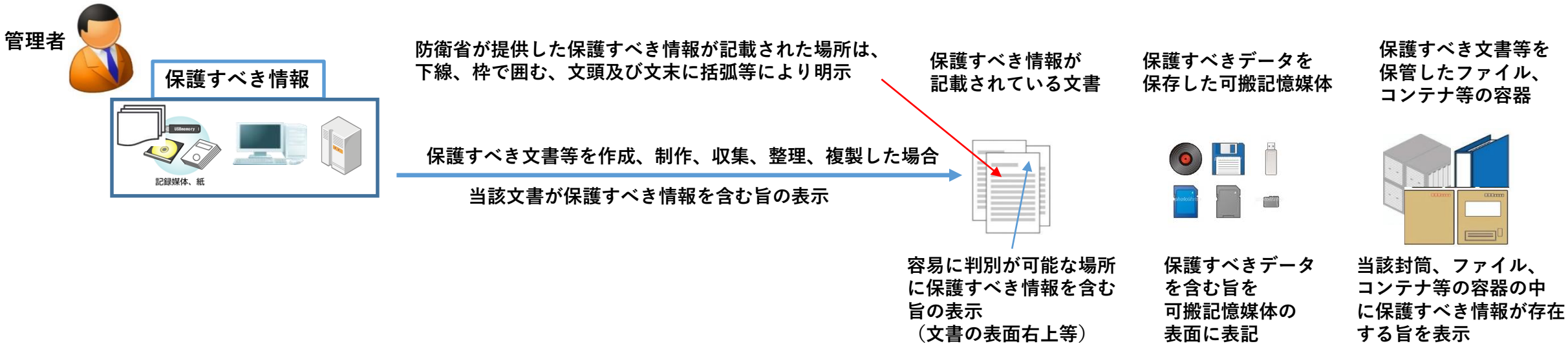
集中保管

文書で保管：
施錠 したロッカー

データで保存：暗号化

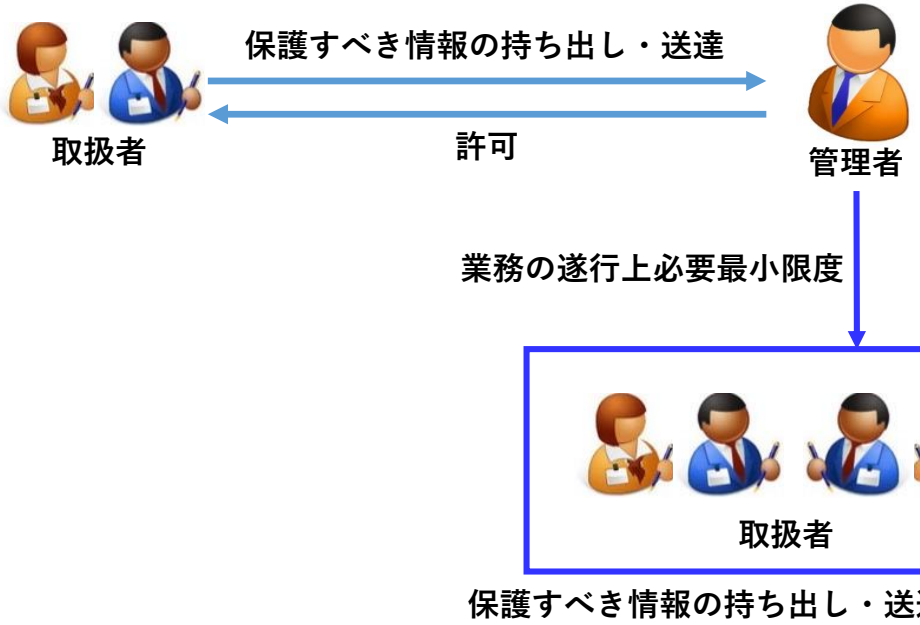
３　保護すべき情報の表示等

(1) 保護すべき文書等への表示
　　管理者は、保護すべき文書等を作成、製作、収集、整理又は複製(以下「作成等」という。)した場合は、次に掲げる措置を講じるものとする。
ア　当該文書等が保護すべき情報を含む旨の表示を行うこととし、当該表示は、文書の表面右上に記載する等、容易に判別可能なものとすること。
イ　当該文書等の中で、保護すべき情報が記録された箇所に、下線を引く、枠で囲む又は文頭及び文末に括弧を付す等により明示すること。
ウ　当該文書等のうち、保護すべきデータが保存された可搬記憶媒体についても、保護すべきデータを含む旨を同媒体の表面に表示すること。
(2) その他の表示
　　管理者は、封筒又はコンテナ等の容器に保護すべき文書等を格納して保管する場合は、当該封筒、ファイル又はコンテナ等の容器の中に保護すべき情報が存在する旨を表示するものとする。



４　保護すべき文書等の持ち出し及び送達

(1) 持ち出し及び送達の方法
　ア　保護すべき情報の持ち出し及び送達を行う場合は、管理者の許可を得るものとする。
　イ　保護すべき情報を持ち出し又は送達する場合は、施錠等により物理的に保護された容器に格納するものとする。
(2) 送達することができる者の制限
　　管理者は、保護すべき情報を持ち出し及び送達することができる者を業務の遂行上必要最小限度に制限するものとする。
(3) 持ち出し及び送達の際の表示
　ア　保護すべき情報を持ち出し及び送達する場合は、封筒、コンテナ等の容器に、その中に保護すべき情報が含まれる旨を表示しないものとする。
　イ　保護すべき情報の送達は、当該情報を受け取ることができる者の氏名等を相手にあらかじめ明示し、直接の手交（郵送の場合にあっては書留）により、必ずその者によって受け取られるようにするものとする。

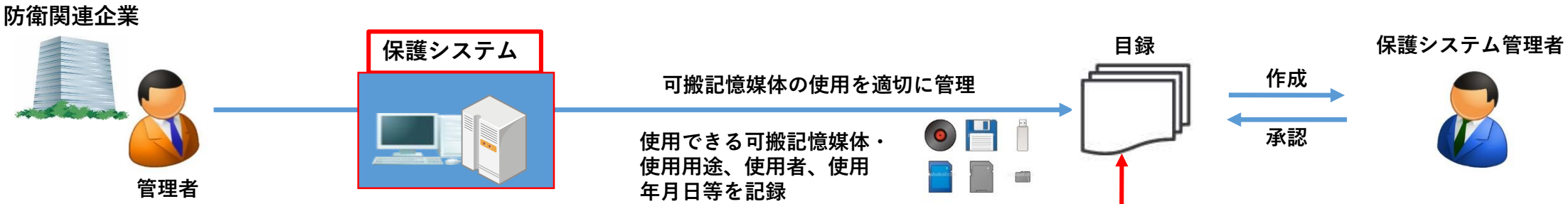


保護すべき情報を持ち出し及び送達する場合は

輸送：施錠等により物理的に保護された容器で輸送
送達：当該情報を受け取る者の氏名を明示し直接手交（郵便の場合は書留等）
送達者：取扱者の中で業務遂行上必要最小限に制限(個人の特定、業務単位での制限でも可)
表示：封筒・コンテナ容器で輸送する場合は、その中に保護すべき情報が含まれる旨を表示しない
郵送：書留等により当該情報が受けとることができる氏名等を表示し、その者が受け取れるようにする

５　保護システムにおける可搬記憶媒体等の使用制限

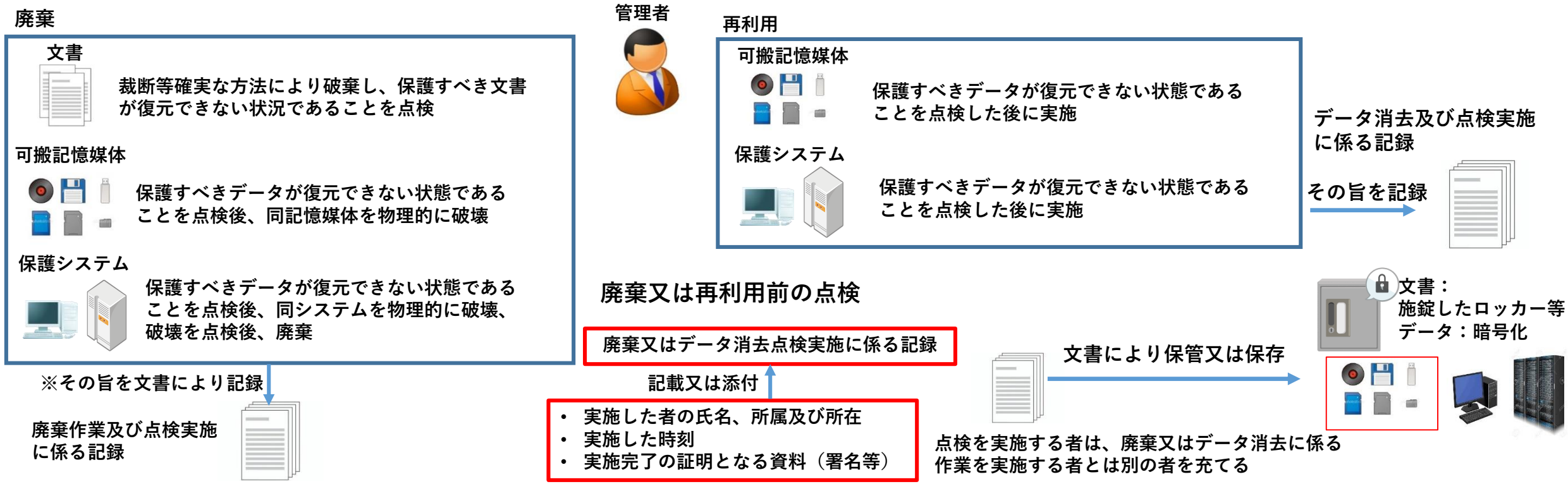
管理者は、保護システムにおいて可搬記憶媒体を使用する場合は、次の各号に掲げる措置を講じるものとする。
(1) 使用できる可搬記憶媒体及びその用途などを記載した目録を作成し、保護システム管理者の承認を得ること。
(2) 前号に規定する目録は、定期的に、及び保護システムにおいて使用できる可搬記憶媒体、その用途等に変更があった場合など必要があると認められる場合にその都度精査し、必要に応じ、更新する。
(3) 個人の所有又は所有者若しくは管理者が明確でない可搬記憶媒体を保護システムにおいて使用しないこと。
(4) 保護システムにおいて可搬記憶媒体を使用することができる者を業務の遂行上必要最小限度に制限すること。
(5) 可搬記憶媒体の使用が、第1号に規定する目録に従って実施されることを確保するため、保護すべきデータの可搬記憶媒体への複製をソフトウェア制御等で技術上の措置をすること。
(6) 第１号の規定により承認を得た可搬記憶媒体の保護システム以外の情報システムへの接続を制限すること。



- 目録は定期的（1年に1回以上)及び必要があると認められる場合に精査し、必要に応じて変更
- 個人の所有又は所有者もしくは管理者が明確でない可搬記憶媒体は保護システムに使用しない
- 保護システムにおいて可搬記憶媒体を使用できる者を業務上必要最小限に制限
- 可搬記憶媒体が目録に従って実施されることを確保する技術的な措置の実施（保護すべきデータの可搬記憶媒体への複製を制御するソフトウェアの導入等）
- 承認を得た可搬記憶媒体について、保護システム以外への情報システムの接続を制限（保護システムにデータを取り込む場合などは使用可）

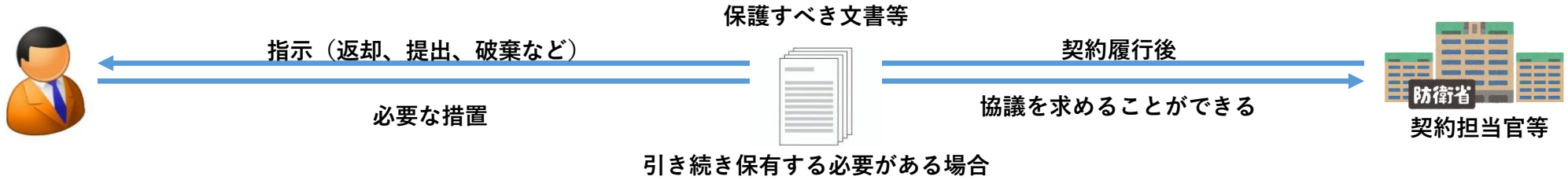
６　保護すべき情報を記録した媒体の廃棄又は再利用

(1) 保護すべき文書等（この号において、データを除く）の廃棄
　防衛関連企業は、保護すべき文書等を廃棄する場合は、裁断等確実な方法により破棄し、保護すべき文書等が復元できない状態であることを点検したうえで、その旨を記録するものとする。
(2) 可搬記憶媒体の廃棄又は再利用
　防衛関連企業は、保護すべきデータの保存に利用した可搬記憶媒体を廃棄する場合は、保護すべきデータが復元できない状態であることを点検したうえで、可搬記憶媒体を物理的に破壊し、その旨を記録するものとする。また、再利用する場合は、保護すべきデータが復元できない状態であることを点検した後に実施するものとする。
(3) 保護システムの廃棄又は再利用
　防衛関連企業は、保護システムを廃棄する場合は、保護すべきデータが復元できない状態であることを点検したうえで、記憶媒体を物理的に破壊し、その旨を記録するものとする。
　また、再利用する場合は、保護すべきデータが復元できない状態であることを点検した後に実施するものとする。
(4) 廃棄又は再利用前の点検
　ア　管理者は、前各号における点検の記録は、廃棄又はデータを復元できなくした者の氏名、所属及び所在等、実施時刻並びに実施完了の証明となる資料（署名等）について記載又は添付し、文書により保管又は保存するものとする。
　イ　前各号における点検を実施する者は、廃棄又はデータの消去を実施した者とは別の者を充てるものとする。



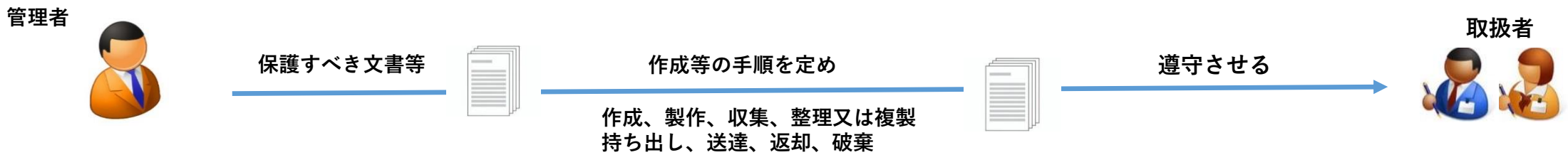
7　保護すべき文書等の防衛省への返却等

(1) 管理者は、契約履行後、防衛省の指示に従い、保護すべき文書等の返却、提出、廃棄など必要な措置を講じるものとする。
(2) 防衛関連企業は、契約履行後、当該文書等を引き続き保有する必要がある場合は、その理由を添えて防衛省に協議を求めるものとする。



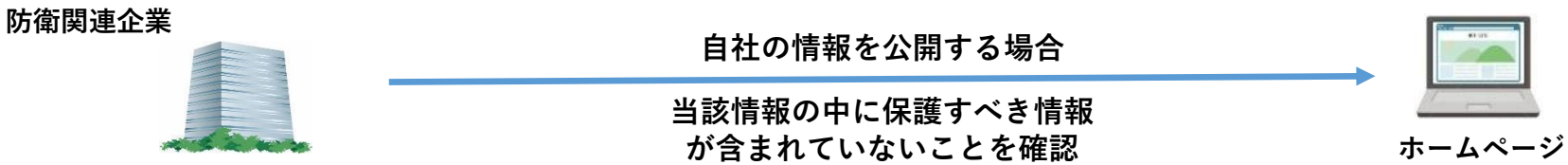
8　保護すべき文書等の作成等の手順の作成

管理者は、保護すべき文書等の作成等及びその持ち出し、送達、返却及び破棄に係る手順を定めるものとする。



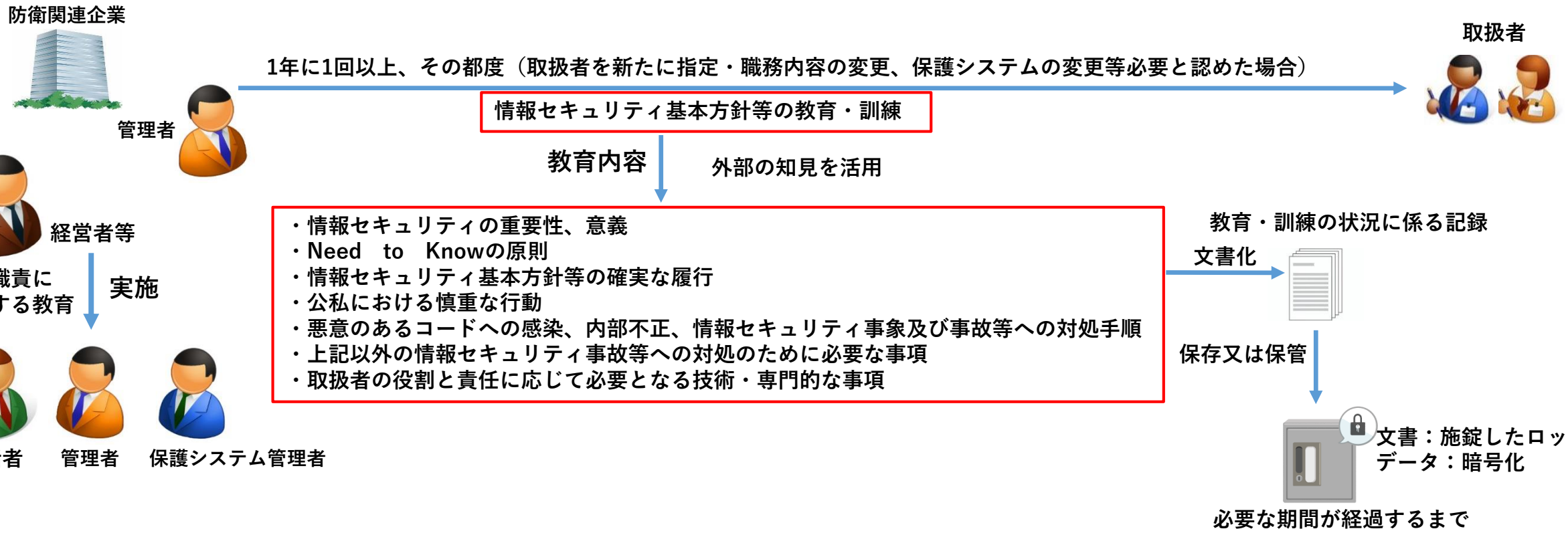
9　防衛関連の情報を公開する場合の措置

防衛関連企業は、ホームページへの掲載、その他の方法により自社の情報を公開する場合は、当該情報の中に保護すべき情報が含まれていないことを確認するものとする。



第７　情報セキュリティ教育及び訓練

1　防衛関連企業は、取扱者に対し、次に掲げる項目を含む教育及び訓練を１年に１回以上に行うものとする。なお、教育及び訓練については、専門性の高い教育項目も含め、外部の知見を活用するなど適切に実施するものとする。
(1) 情報セキュリティの重要性、意義（情報セキュリティ意識のかん養含む。）
(2)「need to knowの原則」（「情報は知る必要がある者のみに伝え、知る必要ない者には伝えない」という原則）の確実な履行
(3) 情報セキュリティ基本方針等の確実な履行
(4) 公私における慎重な行動
(5) 悪意のあるコードへの感染、内部不正、情報セキュリティ事象及び同事故等への対処手順
(6) 前号に掲げる事項のほか、情報セキュリティ事故等への対処のために必要な事項
(7) 第１号から第６号までに掲げる事項のほか、取扱者の役割と責任に応じて必要となる技術的・専門的な事項
2　経営者等は、総括者、管理者、保護システム管理者、保護システム担当者に対しては、前項に掲げる事項に加え、経営者等がそれぞれの職責等に関する教育を行うものとする。
3　管理者は、新たな取扱者の指定、取扱者の異動及び職務内容、保護システムに変更が生じる場合、その他必要があると判断する場合に第１項に規定する教育及び訓練を行うものとする。
4　管理者は、前各号に規定する教育及び訓練の実施に係る状況を記録した文書を作成し保管するものとし、文書により保管する場合は、施錠したロッカー等により、データで保存する場合は、暗号化により、必要な期間が経過するまで保管又は保存するものとする。



第８　物理的及び環境的セキュリティ

１　物理的セキュリティ対策の方針

(1) 管理責任者(取扱施設等の物理的セキュリティに責任を有する者で、管理者の中から総括者が指定した者をいう。以下同じ。)は、次に掲げる施設及び情報システム等に対する物理的セキュリティを確保するため、第２項から第５項までに掲げる事項に係る物理的セキュリティの対策の方針を作成するものとする。

ア　取扱施設及び関係施設
イ　取扱施設等の入退を管理するための鍵及び電子錠等の機器（以下「入退管理機器」という。）
ウ　保護システム
エ　保管された保護すべき文書等

(2) 管理責任者は、情報セキュリティ事故など物理的な情報セキュリティに重大な影響を及ぼす事象が発生した場合は、物理的セキュリティ対策の方針を精査し、必要に応じて修正を行うものとする。

管理責任者（管理者の中から総括者が指定）

物理的セキュリティを確保するための管理策を定める

物理的セキュリティ対策の方針

精査

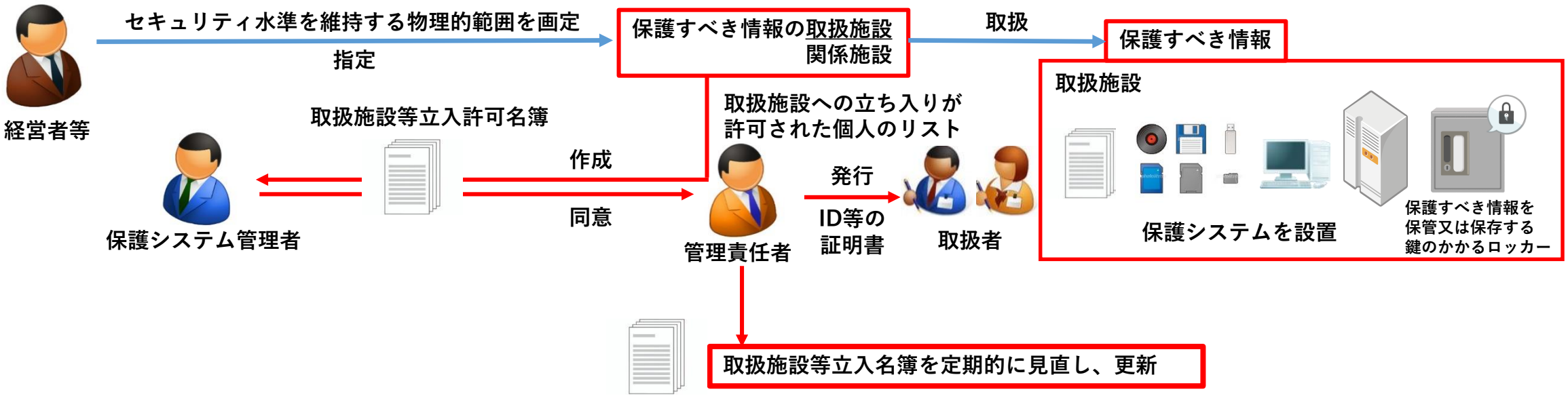
情報セキュリティ事故及び物理的セキュリティに重大な影響を及ぼす事象が発生した場合

必要に応じて見直し

- 取扱施設等（取扱施設及び関係施設）
- 入退管理機器（取扱施設等の入退を管理する機器）
- 保護システム
- 保管又は保存された保護すべき文書等

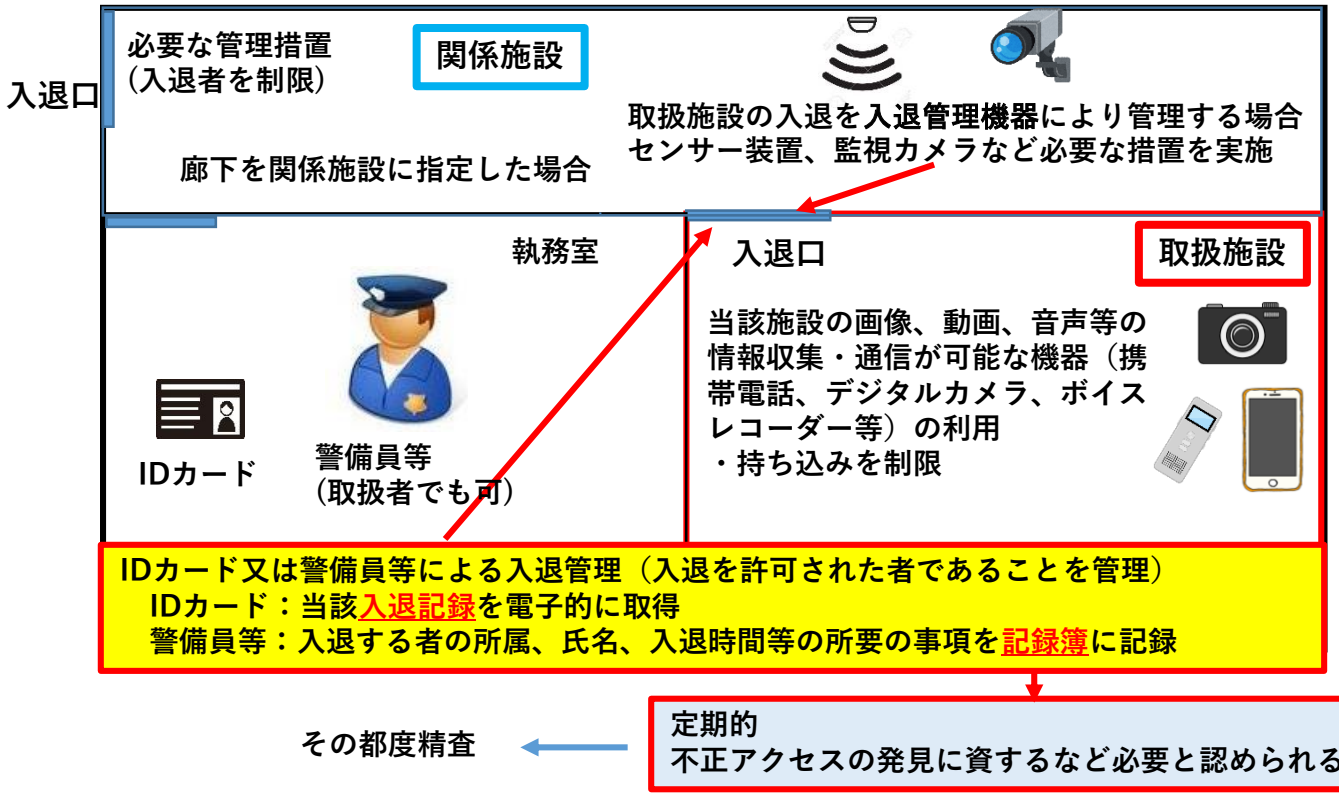
２　取扱施設等に対する物理的セキュリティ対策

(1) 取扱施設等の指定
ア　経営者等は、自社のセキュリティ水準を維持する物理的範囲を画定するため、保護すべき情報の取扱施設に加え、関係施設を指定するものとする。
イ　経営者等は、取扱施設内に保護システム(保護すべき情報の保存又は当該情報へのアクセスを可能とする機器に限る。第４項において同じ。)を設置し、当該施設内で保護すべき情報を取り扱うものとする。
ウ　管理責任者は、取扱施設等への立ち入りが許可された者の名簿(以下「**取扱施設等立入名簿**」という。) を作成し、保護システム管理者の同意を得ることとする。
エ　管理責任者は、取扱施設等立入名簿に基づき取扱施設等への立ち入りを許可する証明書を発行するものとし、当該立ち入りを許可する者については、業務の遂行上必要最小限に制限するものとする。
オ　管理責任者は、取扱施設等立入名簿を定期的に見直し、必要に応じて更新するものとする。



２　取扱施設等に対する物理的セキュリティ対策

(2) 管理責任者は、取扱施設等に対する物理的セキュリティを確保するため、次に掲げる措置を実施するものとする。
- ア　取扱施設と関係施設の境界に入退口を設置し、入退管理機器又は警備員等により、入退する者が当該入退を許可された者であることを管理（識別及び認証を含む。以下この号において同じ。）すること。
- イ　関係施設の外側境界に入退口を設置し、必要な管理措置により入退者を制限すること。
- ウ　取扱施設への入退をＩＤカードにより管理する場合は、当該入退の記録を電子的に取得すること。
- エ　取扱施設への入退を警備員等により管理する場合は、必要に応じて入退する者の所属、氏名及び入退の時間等所要の事項を記録簿に記載すること。
- オ　ウ及びエの規定により取得した記録は、定期的に、及び保護すべき情報等への不正なアクセスの発見に資するなど必要と認められる場合には、その都度精査すること。
- カ　取扱施設等において敷地を指定した場合は、十分な高さ及び強度のあるフェンス等を設置するなど必要な措置を講ずること。
- キ　取扱施設の入退をＩＣカードのみで管理する場合は、当該施設の境界を警備員、センサー装置又は監視カメラによる監視など必要な措置を講ずること。
- ク　取扱施設においては、当該施設の画像、動画、音声等等の情報の収集・通信が可能な機器（携帯電話、デジタルカメラ、ボイスレコーダー等）の利用（持ち込みを含む）を制限すること。



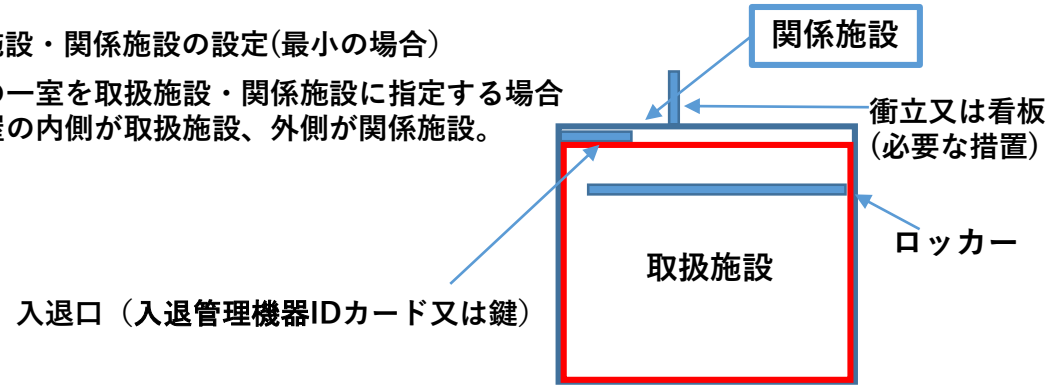
取扱施設・関係施設の指定

敷地を設定した場合

十分な高さ及び強度のあるフェンス等を設置

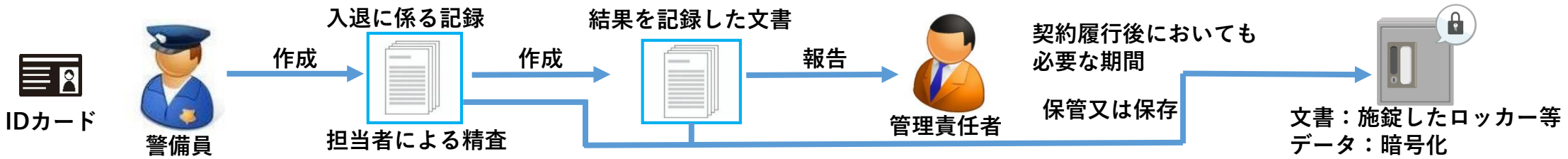
取扱施設・関係施設の設定(最小の場合)

建物の一室を取扱施設・関係施設に指定する場合
・部屋の内側が取扱施設、外側が関係施設。

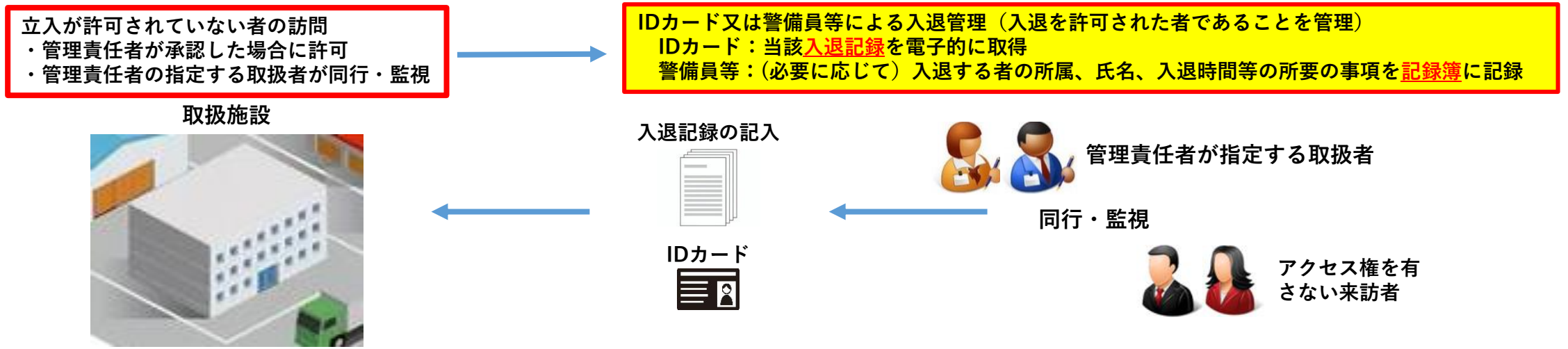


２　取扱施設等に対する物理的セキュリティ対策

(3) 警備員等は、第２号オの規定により入退に係る記録を精査した場合は、その結果を記録した文書を作成し、管理責任者に報告するものとする。
(4) 管理責任者は、第２号ウ及びエに規定する入退に係る記録並びに前号に規定する当該記録を精査した結果を記録した文書を保管するものとし、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により契約履行後においても必要な期間保管又は保存するものとする。



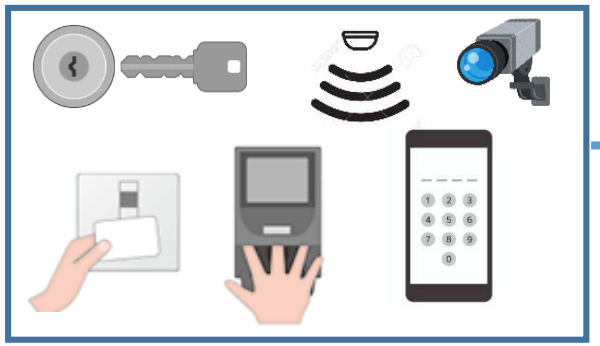
(5) 立入りが許可されていない者による取扱施設への立入りは、管理責任者が承認した場合に限り許可することとし、管理責任者の指定した者が同行して監視するとともに、第２号ウ又エの措置を行うものとする。



３　入退管理機器に対する物理的セキュリティ対策

管理責任者は、入退管理機器に対する不正なアクセス等を防止及び検知するため、以下の措置を講じるものとする。
(1) 入退管理機器の現状を記録した目録を作成し保管するものとし、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により必要な期間保管すること。
(2) 前号に規定する目録は、定期的に、及び入退管理機器の変更など必要があると認める場合には、その都度精査し、必要に応じ更新すること。
(3) 入退管理機器として暗証番号等を併用する場合は、定期的に、及び当該暗証番号等を配布されていた者が、異動等により取扱施設等への立ち入り権限を失うなど必要があると認める場合には、その都度当該暗証番号等を変更すること。
(4)入退管理機器として錠を併用する場合は、鍵の紛失など必要があると認める場合に、当該錠を変更すること。

入退管理機器



作成

現状を記録した目録

必要な期間

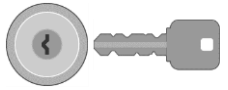
文書：暗号化又は施錠したロッカー等
データ：暗号化

定期的及び必要な場合（入退管理機器の変更など)に精査、
必要に応じ更新

暗証番号等を併用する場合

定期的(1年に1回程度）及び必要がある場合（暗証番号を付与されていた者が物理的なアクセス権限を失った場合（人事異動等））は、その都度、暗証番号を変更

鍵を併用する場合



鍵の紛失など必要と認める場合に、
鍵を交換

４　保護システムに対する物理的セキュリティ対策

(1) 保護システム管理者は、保護システムを構成するハードウェア及び記憶媒体について、不正な移動、持ち出し等を防止するため、必要な措置を講ずるものとする。
(2) 保護システムの取扱施設外への持ち出しは、保護システム管理者が管理責任者と調整の上許可することとし、当該持ち出しを行う者が保護システム利用者でない場合は、保護システム管理者の指定する保護システム利用者が同行して監視し、記録するものとする。
(3) 保護システムに接続された送配線は、関係施設において破壊、情報窃取を防止又は検知できる物理的セキュリティ対策を講じるものとする。
(4) その他の保護システムに対する管理策については第９に定めるところによる。

保護システム管理者

- 保護システムに接続された配電線
- 関係施設において、不正なアクセスを防止又は検知できる物理的な保護策により防護

保護システムを構成するハードウェア及び記憶媒体

パソコン

可搬記憶媒体

レザープリンター

サーバーラック

保護すべき情報を保管又は保存する鍵のかかるロッカー

必要な措置

- 保護システムの配置については機密性を配慮
- ハードウェア、記憶媒体→施錠できるラック又はセキュリティワイヤ等により固定・施錠　※データレスPCは固定不要であるが適切な管理が必要
- 固定が困難な場合→業務上使用しないものをロッカー等に保管し施錠
- ラック・ロッカー等の鍵→厳格に管理（保護システム管理者又はその指定する者の許可なく開錠できないよう）必要と認める場合に、鍵を変更
- 保護システムの施設外への持ち出し
  →保護システム管理者と管理責任者が調整の上許可
  保護システム利用者以外の者が持ち出す場合は、保護システム管理者が指定する保護システム利用者が同行・監視・記録

その他の保護システムに対する管理策については付紙（システムセキュリティ実施要領）で定める。

５　保管された保護すべき情報の物理的セキュリティ対策

(1) 保護すべき情報の保管
　ア　保護すべき情報を文書等により保管する場合は、取扱施設内の施錠したロッカー等に保管するものとする。
　イ　保護すべきデータを保護システムに保存する場合は、第4項第1号に定める措置を行うものとする。

保存

- 文書 → 保管 → 取扱施設内の施錠したロッカー
- 可搬記憶媒体 → 保管 → 取扱施設内の施錠したロッカー
- 保護システム

・保護システムの配置については機密性を配慮
・ハードウェア、記憶媒体→施錠できるラック又はセキュリティワイヤ等により固定･施錠
・固定が困難な場合→業務上使用しないものをロッカー等に保管し施錠
・ラック・ロッカー等の鍵→厳格に管理（情報システム管理者又はその指定する者の許可なく開錠できないよう）必要と認める場合に、鍵を変更
・保護システムの施設外への持ち出し→保護システム管理者と管理責任者が調整の上許可
保護システム利用者以外の者が持ち出す場合は、保護システム管理者が指定する保護システム利用者が同行・監視・記録

(2) 鍵等の管理
　第１号に規定するロッカー等の鍵を保管するのは、管理責任者（保護システムに関連する場合にあっては保護システム管理者を含む。以下本項において同じ。）及び管理者が指定した者のみとし、それ以外の者により解錠されることがないよう厳格に管理するものとする。

管理責任者　保護システム管理者

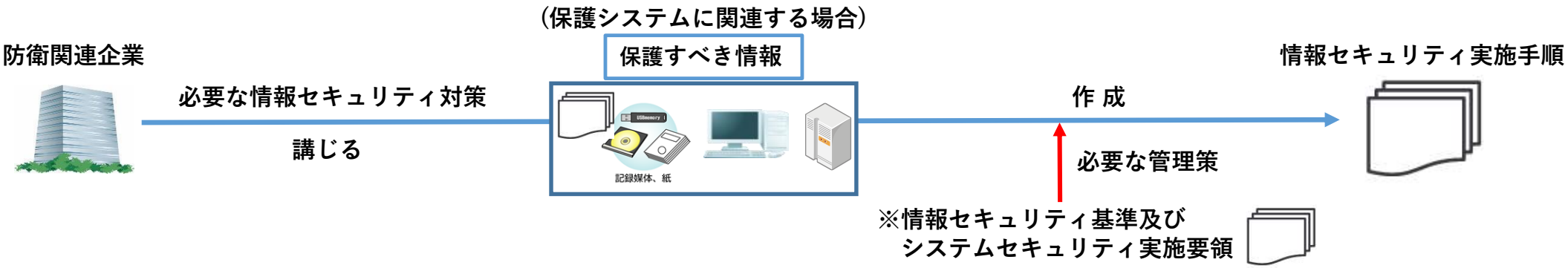
（保護システムに関連する場合）厳格に管理
指定する者の許可なく解錠されることがないよう

鍵により施錠
保護すべき情報を保管又は保存する鍵のかかるロッカー

鍵を変更
当該鍵の紛失など必要があると認める場合は

第９　保護システムについての管理策

1 防衛関連企業は、自社の保有又は使用する保護システムに、保護すべき情報を適切に取扱うために必要と認める情報セキュリティ対策を講じるものとする。
2 防衛関連企業は、前項の規定に基づき情報セキュリティ対策を講じる際は、本基準及び付紙に規定する管理策を盛り込んだ情報セキュリティ実施手順を定めるものとする。



第10　情報セキュリティ事故等への対応

1　情報セキュリティ事故等へ対処計画の策定

(1) 経営者等は、情報セキュリティ事故及び情報セキュリティ事象（以下「事故等」という。）の発生に備え、情報セキュリティ事故等対処計画を定めるものとし、総括者は、次に掲げる事故等対処の各段階に対処し得る体制、責任及び手順を定めるものとする。
- ア　事故等への対処の準備
- イ　事故等の発見、検知時の報告・連絡要領
- ウ　事故等の監視（システム監視を含む。）及び分析　※インターネットの接続状況、保護システムの設定環境、自社システムの設定環境の監視を想定
- エ　事故等による被害及び影響の抑制並びに局限
- オ　事故等に係る証拠の保存及び原因の究明　※原因の特定は重要なので、社会的にも納得を得ることができるよう調査を尽くすことが必要と考えている
- カ　事故等からの復旧（復旧に要する時間の目標を含む。）※復旧目標は各社で定めることができるが、奨励する時間を示す。

(2) 情報セキュリティ事故等対処計画においては、前号の規定による対処体制等のほか、次に掲げる事項についての措置を定めるものとする。
- ア　保護システム管理者の下にヘルプデスク等を設置し、保護システム利用者に対し、情報セキュリティ事故等に関する必要な情報の提供等を行うこと。
- イ　情報セキュリティ事故等の詳細を把握するため、デジタルフォレンジック技術の利用等により必要な情報を収集及び分析すること。
- ウ　保護システムを含め、自社のネットワークにおけるすべての情報システムの分析及び精査（システムログの取得及び分析を含む。）を行い、当該情報システム内の構成要素、データ及びアカウント等の中から、悪意のあるコードへの感染又は不正アクセスなどの情報セキュリティ事故等が発生した原因を特定すること。
- エ　情報セキュリティ事故等への対処の要領及び結果（当該事故等に対する分析、原因究明等の結果を含む。）並びに当該対処により取得した情報等を記録した文書の作成及び保管に関すること。
- オ　情報セキュリティ事故等への対処において収集した情報の分析結果を踏まえ、当該対処に係る教訓を取りまとめ、情報セキュリティ教育及び訓練、情報セキュリティ事故等対処計画及び情報セキュリティ事故等対処テストの内容に反映させること。

(3) 事業継続計画を策定している場合は、当該計画と情報セキュリティ事故等対処計画との整合性を確保するものとする。

経営者等

定める

事故等対処の各段階に対処し得る体制・責任・手順

総括者の業務

- 事故等への対処の準備
- 事故等の発見、探知、連絡
- 事故等の監視（システム監視を含む）・分析
- 事故等による被害・影響の抑制・局限
- 事故等に係る証拠の保存及び原因の究明
- 事故等からの復旧（復旧に要する時間の目標を含む）

事業継続計画を策定している場合：
同計画と情報セキュリティ事故等対処計画との整合性を確保

情報セキュリティ事故等対処計画

保護システム管理者の業務

ヘルプデスクの設置：
保護システム利用者に情報セキュリティ事故に関する必要な情報の提供

情報セキュリティ事故等の詳細の把握：
デジタルフォレンジック技術の使用等による情報収集及び分析

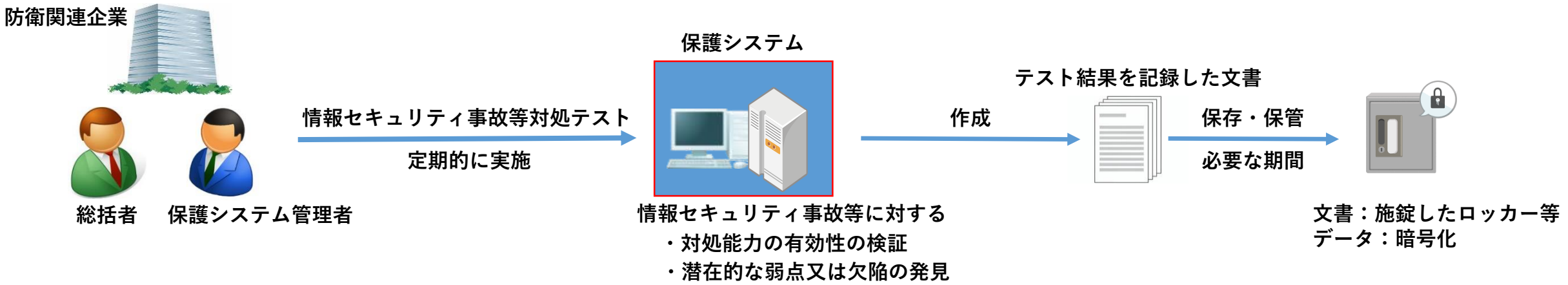
情報セキュリティ事故等の原因の特定：
自社のネットワークにおけるすべての情報システムの分析・精査(※保護システムと接続されている全ての情報システムを対象、事故原因の特定はマスト)

文書の作成・保管：
情報セキュリティ事故等への対処の要領及び結果、当該対処により得た情報

当該対処に係る教訓の取りまとめ：
情報セキュリティ教育及び訓練、情報セキュリティ事故等対処計画及び情報セキュリティ事故等対処テストの内容に反映

2　情報セキュリティ事故等への対処テスト

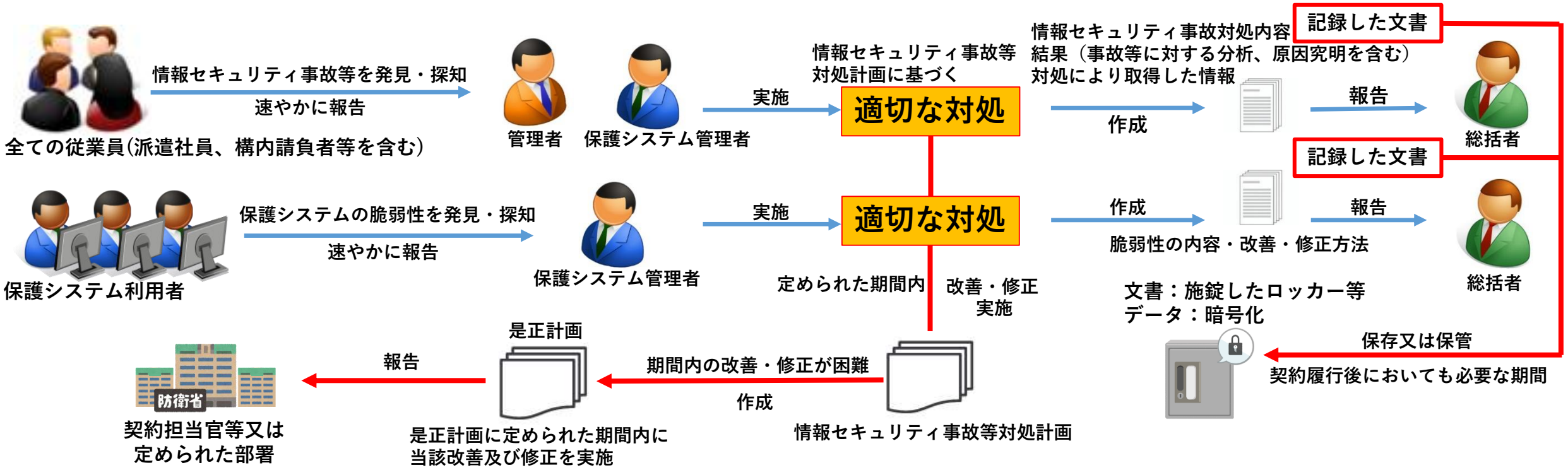
(1) 防衛関連企業は、情報セキュリティ事故等に対する保護システムの対処能力の有効性を検証し、潜在的な弱点又は欠陥を発見するため、情報セキュリティ事故等対処テストを定期的に実施するものとする。
(2) 前号に規定する情報セキュリティ事故等対処テストを実施した場合は、当該テストの結果を記録した文書を作成し、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により、必要な期間保管又は保存するものとする。



第11　情報セキュリティ事故等発生時の対応

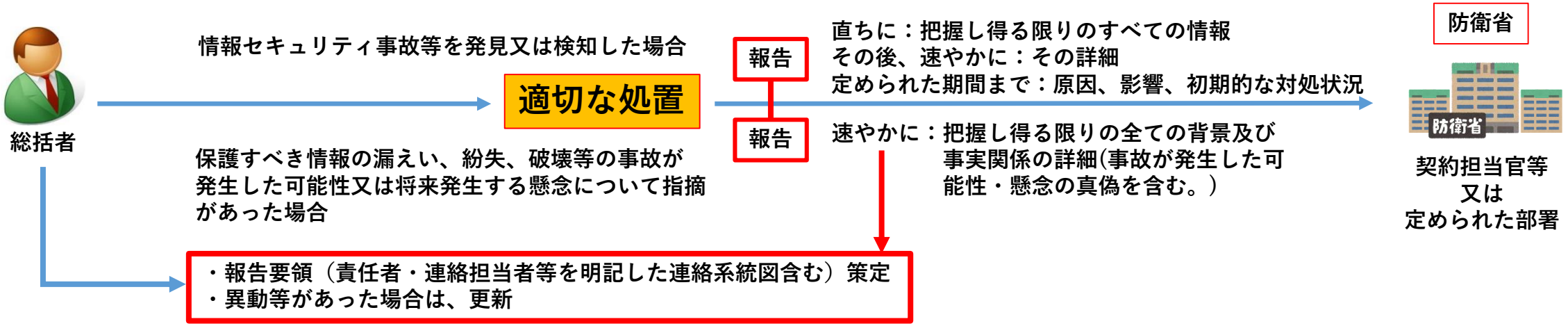
1　情報セキュリティ事故等を発見又は検知した場合の処置

(1) 全ての従業員は、情報セキュリティ事故等を発見又は検知した場合は、速やかに管理者（保護システムに係る場合は保護システム管理者）に報告するものとし、管理者は情報セキュリティ事故等対処計画に基づき適切に対処するとともに、その内容及び結果（当該事故等に対する分析及び原因究明等の結果を含む。）並びに当該対処により取得した情報等を記録した文書を作成し、総括者に報告するものとする。
(2) 保護システム利用者が保護システムの脆弱性の発見又は探知した場合は、速やかに保護システム管理者に報告するものとし、保護システム管理者は、適切な対処を行うとともに、その内容、修正の方法を記載した文書を作成し、総括者に報告するものとする。
(3) 保護システム管理者は、前２号の規定により作成した文書は、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により、契約履行後においても必要な期間保管又は保存するものとする。
(4) 総括者は、第１号及び第２号による情報セキュリティ事故等対処計画に基づく対処を行う場合は、同計画に定められた期間内に行うものとする。なお、当該期間までの改善又は修正が困難と認める場合は、是正計画を作成し、同計画に定められた期間内に修正を実施するとともに防衛省に報告するものとする。
(5) 防衛関連企業は、保護システムの脆弱性に係る修正を実施する場合は、第１２に規定するリスク査定の結果及び公開されている脆弱性情報データベース等を活用するものとし、当該脆弱性が保護システムのセキュリティに重大な影響を及ぼす場合には、可能な限り速やかに修正を実施するものとする。



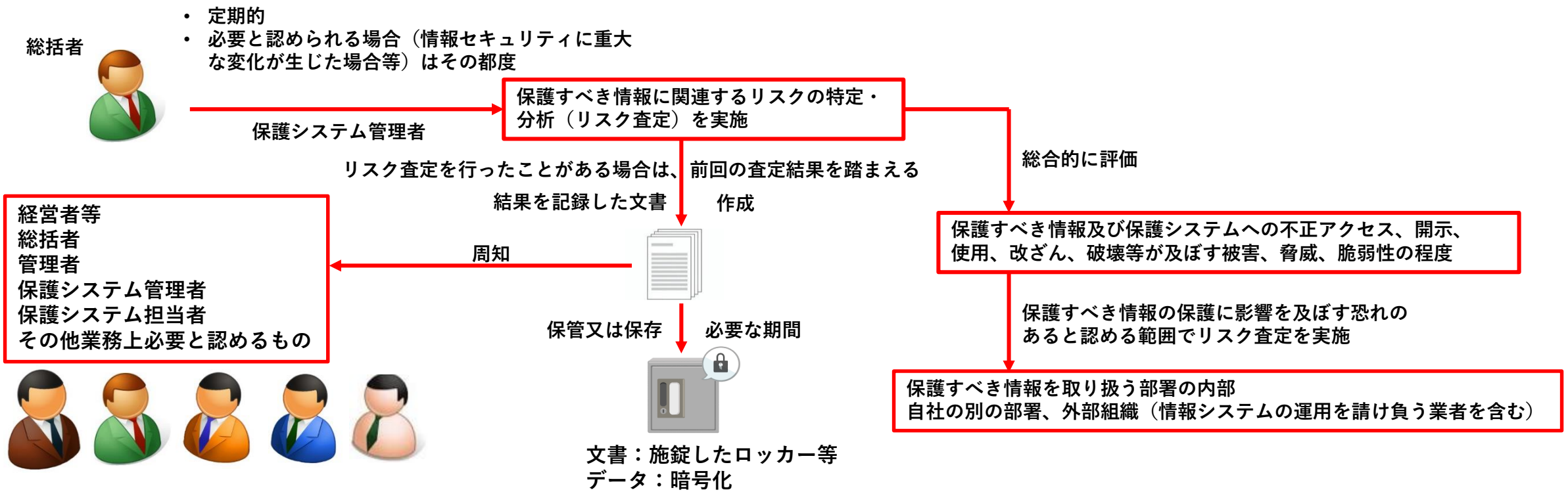
2　防衛省への報告

(1) 総括者は、前項第１号及び第２号に掲げる情報セキュリティ事故等の報告を受けた場合は、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防衛省(契約担当官等又は防衛装備庁長官が別に定めた部署の職員。以下同じ。)に報告するものとする。
(2) 総括者は、前号のほか、防衛関連企業の内部又は、外部から保護すべき情報の漏えい、紛失若しくは破壊等の事故が発生した可能性又は将来発生する懸念の指摘があった場合は、当該可能性又は懸念の真偽を含む把握し得る限りの全ての背景及び事実関係の詳細を速やかに防衛省に報告するものとする。
(3) 総括者は、前2号に規定する防衛省への報告においては、それぞれ責任者及び連絡担当者等を明示した連絡系統図を含めた報告要領を定め、責任者及び連絡担当者等に異動等があった場合にはこれを更新するものとする。
(4) 総括者は、第1号の規定による情報セキュリティ事故等の詳細の防衛省への報告は、情報セキュリティ事故等対処計画に定められた期間までにそれらの原因（当該情報セキュリティ事故等の原因となった悪意のあるコード等の検体を取得している場合には、当該検体を含む。）及び影響並びにそれらに対する初期的な対処状況について行うものとする。



第12　リスク査定

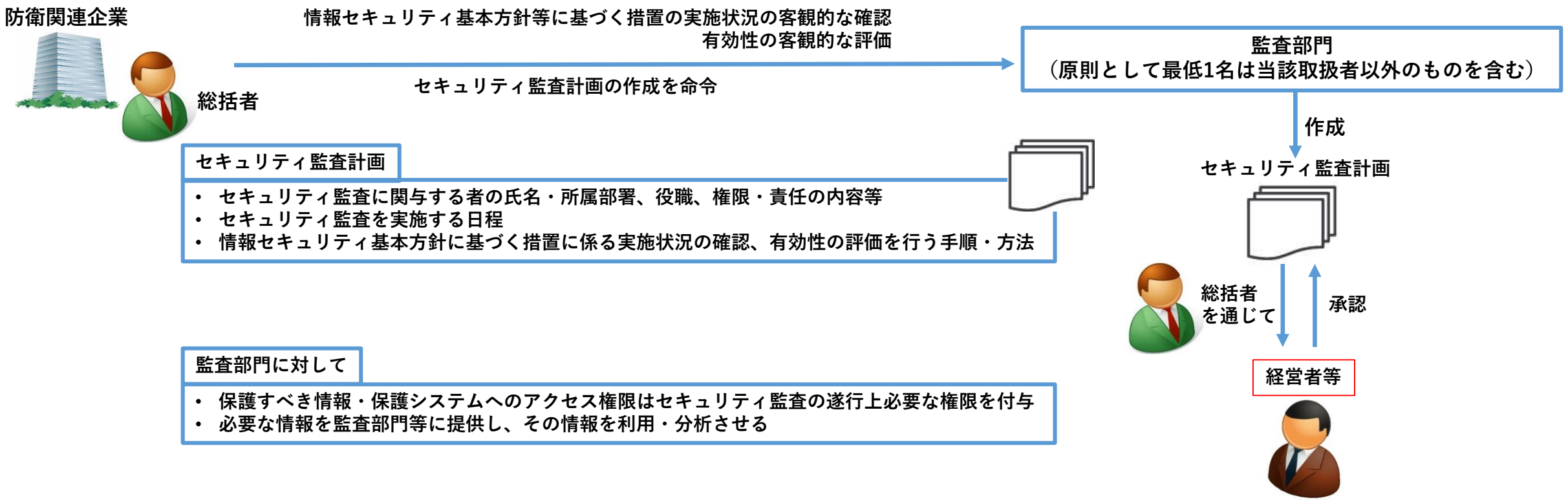
1　総括者は、保護すべき情報に関連するリスクを特定、分析及び評価するため定期的に、自社の情報セキュリティに重大な変化が生じた場合など必要と認められた場合にはその都度、リスク査定を実施するものとする。
2　総括者は、前項に規定するリスク査定を実施した場合は、速やかにその結果を記録した文書を作成し、当該文書を経営者等、管理者、保護システム管理者及び保護システム担当者その他の業務の遂行上必要と認める者に周知するものとする。
3　総括者は、第1項に規定するリスク査定結果を記録した文書について、文書により保管する場合は施錠したロッカー等により、データで保存する場合には、暗号化により、必要な期間保管又は保存するものとする。
4　総括者は、第1項に規定するリスク査定を実施する場合は、保護すべき情報及び保護システムへの不正なアクセス、開示、使用、改ざん及び破壊等が及ぼす被害、脅威及び脆弱性の程度を複合的に評価するものとする。
5　総括者は、前各項の規定によりリスク査定を実施する場合は、保護すべき情報を取り扱う部署の内部のほか、保護すべき情報の保護に影響を及ぼすおそれがあると認める範囲内で、自社の別の部署及び外部の組織（情報システムの運用を請け負う業者等を含む。）におけるリスクを特定、分析及び評価するものとする。



第13　セキュリティ監査

1　セキュリティ監査計画の作成等

(1) 防衛関連企業は、情報セキュリティ基本方針等に基づく措置の実施状況の確認及び有効性の評価を客観的に行うため、監査部門を設置し、同部門には原則として最低１名は監査を受ける部署以外の取扱者を含めるものとする。
(2) 監査部門は、次に掲げる事項を記載したセキュリティ監査計画を作成し、総括者を通じて経営者等の承認を得るものとする。
　ア セキュリティ監査に関与する者の氏名、所属する部署、役職並びに権限及び責任の内容等
　イ セキュリティ監査を実施する日程
　ウ 情報セキュリティ基本方針等に基づく措置に係る実施状況の確認及び有効性の評価を行うための手順及び方法
(3) 前号アの規定によりセキュリティ監査に関与する者に対する保護すべき情報及び保護システムに対するアクセス権限について、総括者は当該セキュリティ監査の遂行上必要な権限を付与するものとする。
(4) 総括者は、セキュリティ監査を適切に実施するために必要な情報を監査部門に提供し、その情報を利用及び分析させるものとする。

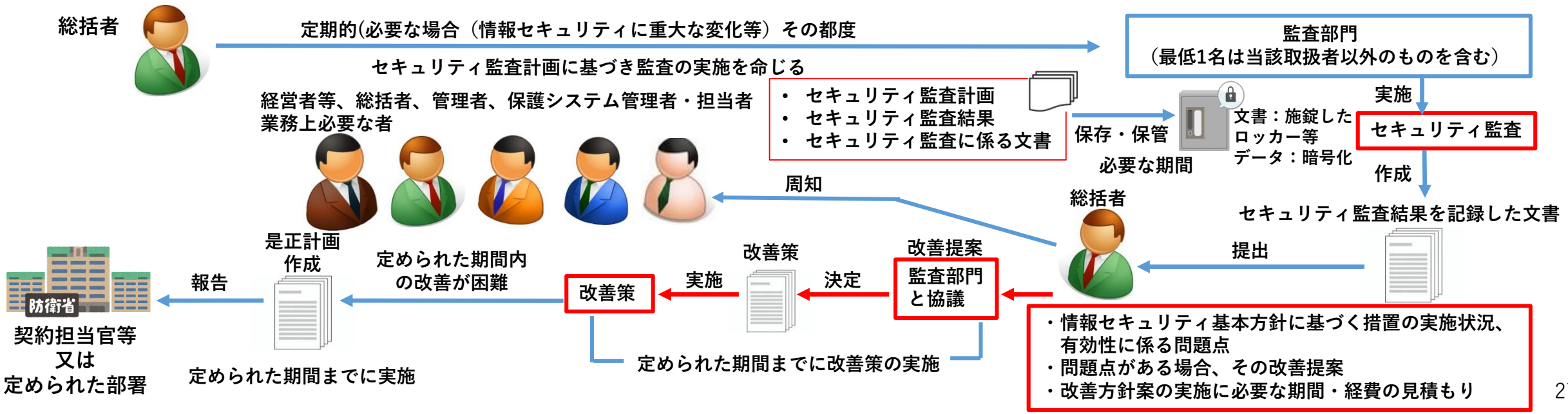


2　セキュリティ監査の実施

総括者は、１年に１回以上及び自社の情報セキュリティに重大な変化が生じた場合など必要と認めた場合に、監査部門に対し、前項に規定するセキュリティ監査計画に基づくセキュリティ監査を実施させるものとする。

3　セキュリティ監査結果の報告等

(1) 総括者は、監査部門に、セキュリティ監査終了後、速やかにその結果を記録した文書を作成及び提出させ、当該文書を経営者等、管理者、保護システム管理者及び保護システム担当者その他の業務の遂行上必要と認める者に周知するものとする。
(2) 総括者は、前号に規定するセキュリティ監査の結果を記録した文書には、次に掲げる事項を明記させるものとする。
　ア　情報セキュリティ基本方針等に基づく措置の実施状況及び有効性に係る問題点の有無及びその内容
　イ　アに規定する問題点がある場合は、その改善提案
　ウ　イに規定する改善提案を踏まえた改善の実施に必要な期間
(3) 総括者は、前号イの規定により監査部門から改善提案が示された場合は、当該措置を実施する部門と監査部門との間で協議させたうえで改善策を決定し、同協議で定められた期間までに当該改善策を実施するものとする。
(4) 前号に規定する改善策が監査部門との協議の結果、定められた期間内に実施することが困難と認められた場合には、総括者は速やかに是正計画を作成し、同計画に定められた期間内に当該改善策を実施するとともに防衛省に報告するものとする。
(5) 総括者は、セキュリティ監査計画、セキュリティ監査の結果を記録した文書その他のセキュリティ監査に係る重要な文書は、文書により保管する場合は、施錠したロッカー等により、データで保存する場合には、暗号化により、必要な期間保存又は保管するものとする。



第１４　防衛省による監査

1　監査の受け入れ

防衛関連企業は、防衛省によるセキュリティ対策に関する監査の要求があった場合は、これを受け入れるものとする。

2　監査への協力

防衛間企業は、防衛省が監査を実施する場合は、防衛省の求めに応じ必要な協力（監査官の取扱施設への立入り及び監査官による書類の閲覧等）を行うものとする。

契約担当官等
又は
定められた部署

監査の要求

監査官の受け入れ　必要な協力

監査官の取扱施設への立ち入り
監査官による書類閲覧等

防衛関連企業

（付録）　用語の説明

#	名　称	説　明
1	**情報セキュリティ**	保護すべき情報の機密性、完全性及び可用性を維持すること。
2	**保護すべき情報**	装備品等及び役務の調達に関する情報のうち、防衛省が企業に保護を求める情報として指定したもの。
3	**保護すべきデータ**	保護すべき情報が電子的な状態にあるもの。
4	**防衛関連企業**	保護すべき情報を取扱う契約相手方企業（団体及び個人を含む。）。
5	**保護システム**	保護すべき情報の保存又は当該情報へのアクセスを可能とする機器。 保護すべき情報を取り扱う情報システム。
6	**総括者**	保護すべき情報の管理全般に係る総括的な責任を負う者。
7	**管理者**	保護すべき情報及びこれに関連する資産ごとに、それぞれ管理責任を負う者。
8	**取扱者**	保護すべき情報を取り扱う者として、経営者等が指定したもの。
9	**保護システム管理者**	保護システム利用者のうち、保護システムの運用管理に責任を負う者。
10	**保護システム担当者**	保護システム利用者のうち、保護システム管理者の業務遂行を補佐する者。
11	**保護システム利用者**	経営者等が指定する保護システムを利用する者。
12	**情報セキュリティ基本方針等**	・情報セキュリティ基本方針 ・情報セキュリティ規則 ・情報セキュリティ実施手順　　をいう。
13	**経営者等**	防衛関連企業の経営者又は受注案件を処理する部門責任者。
14	**下請負者**	契約の履行に係る作業に従事する全ての事業者（防衛省と直接契約関係にある者を除く。）。
15	**情報セキュリティ基本方針**	本基準に基づき、防衛関連企業が情報セキュリティへの取組の方針を定めたもの。

16	**情報セキュリティ規則**	本基準及び情報セキュリティ基本方針に基づき、防衛関連企業が実施する情報セキュリティ対策について定めたもの。
17	**情報セキュリティ実施手順**	本基準及びシステムセキュリティ実施要領に基づき、防衛関連企業が保有又は使用する保護システムに対する管理策を定めたもの。
18	**第三者　※**	法人又は自然人としての防衛省と直接契約関係にある者以外の全ての者をいい、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防衛省と直接契約関係にある者に対して指導、監督、業務支援、助言、監督等を行うものを含む。
19	**伝達**	知識を相手方に伝えることであって、有体物である文書等の送達を伴わないもの。
20	**送達**	取扱施設の外に所在する者に送り届けることをいい、輸送（社外の事業者との契約に基づき、当該事業者が保護すべき情報を特定の相手方に送達することをいう。以下同じ。）を含む。
21	**保護すべき文書等**	保護すべき情報に属する文書（保護すべきデータが保存された可搬記憶媒体を含む。）、図画及び物件。
22	**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。
23	**情報システム**	ハードウェア（サーバ、パソコン、モニタ、携帯端末、プリンタ、スキャナ等を含む。以下同じ。）、ソフトウェア（プログラムの集合体をいい、ファームウェアを含む。以下同じ。）、ネットワーク（暗号化により公衆回線に作られる仮想的な専用ネットワークを含む。）又は記憶媒体で構成されるものであって、これら全体で業務処理を行うもの。
24	**悪意のあるコード**	情報システムが提供する機能を妨害するプログラムの総称であり、コンピュータウイルス及びスパイウェア等。
25	**情報セキュリティ事象**	情報セキュリティ事故のおそれ並びに情報セキュリティ事故に至らない情報セキュリティ基本方針等への違反及びそのおそれのある状態。
26	**情報セキュリティ事故**	保護すべき情報の漏えい、紛失、破壊等の事故。
27	**取扱施設**	保護すべき情報の取扱い及び当該情報に属する文書等の保管を行う場所として、本基準の規定に従って防衛関連企業が指定する建物又は敷地の一部又は全部。
28	**関係施設**	取扱施設の外側に隣接する場所であって、本基準の規定に基づき防衛関連企業が指定する建物又は敷地の一部又は全部。
29	**取扱施設等**	取扱施設及び関係施設。
30	**システムログ**	情報システムにおける動作履歴に関する記録。

31	**ベースライン構成設定**	保護システムとシステムコンポーネントの構成の把握並びに保護システムの更新及び変更時のベース(基準)となる構成設定。
32	**ブラックリスト**	保護システムにインストール又は保護システムで実行してはならないソフトウェアのリスト。
33	**ホワイトリスト**	保護システムにインストール及び保護システムで実行してもよいソフトウェアのリスト。
34	**構成設定**	情報システムを構成する構成要素（ハードウェア、ソフウェア、ネットワーク及び記憶媒体）の機種、バージョン等及び当該構成要素の機能並びに動作等を制御する設定値を決定すること。
35	**リプレイ攻撃**	利用者の確認に用いられる認証データの通信を盗聴し得られたデータをそのまま用いてその利用者になりすます方式
36	**モバイルコード**	インターネット等のネットワークを通じて、自動的にダウンロード及び実行されるプログラム。
37	**外部ネットワーク**	インターネットその他の防衛関連企業によって管理されないネットワーク。
38	**機密性**	認可されていないものに対して、情報を使用不可又は非公開にする特性。
39	**完全性**	情報の正確さ及び完全さを保護する特性。
40	**可用性**	認可されたものが要求したときに、アクセス及び使用が可能である特性。
41	**電子政府推奨暗号等**	電子政府推奨暗号リストに記載されている暗号等又は電子政府推奨暗号選定の際の評価方法により評価した場合に電子政府推奨暗号と同等以上の解読困難な強度を有する秘匿化の手段。
42	**管理者権限**	情報システムの管理（情報システム利用者の登録、削除、及びアクセス制御等）を行うために付与される権限。
43	**外部システム**	防衛関連企業によって管理されないシステム（クラウドサービス事業者によるクラウドサービス、及び請負業者の情報システム等を含む。）。
44	**ユーザセッション**	保護システム利用者が実行する各アプリケーションの論理的な経路。
45	**タイムスタンプ**	電子データの取得、作成等を行った時刻に関する情報。

46	**取扱者名簿**	取扱者として指定した個人の氏名、生年月日、所属する部署、役職及び国籍等を記載したリスト。
47	**IDカード**	持ち主の氏名、所属、顔写真等が記載されたカードで、個人の身分証明書として機能するもの。
48	**ICカード**	情報の記録や演算をするための集積回路（IC）を組み込んだカード。個人の身分証明にはならない。
49	**デジタルフォレンジック技術**	対象となるパソコン、サーバ等の電子機器に残る記録・情報を分析してその法的な証拠性を明らかにする技術。

※第三者（契約相手方及び防衛省を除いた全ての企業及び個人）と下請負者の関係の補足説明