防衛セキュリティゲートウェイ(DSG)
サービス仕様書

富士通株式会社

第1.0版

目次

1. 本資料について

1. 本資料について

- 本資料では、防衛セキュリティゲートウェイの利用に際して、提供するサービス概要、サービス内容の説明、利用までの流れについて掲載しています。

1. 本資料の目的

- 本資料は、防衛セキュリティゲートウェイの利用を検討している防衛関連企業、防衛省職員及び各自衛隊員の、DSG提供サービス内容の理解促進を目的としています。

2. 本資料の対象者

- 防衛セキュリティゲートウェイの利用希望者
- 防衛関連企業の情報セキュリティに関する責任者
- 防衛省職員及び各自衛隊員

2. 改版履歴

2. 改版履歴

- 本資料に関する改版履歴を以下に記載します。

版数	発行日	改訂履歴
第1.0版	2024年4月12日	初版作成

3. サービス概要

3. サービス概要

1. サービス概要

○ 防衛セキュリティゲートウェイ(DSG)とは、防衛装備品の調達のうち、「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」を付帯した契約の中で取り扱う保護すべき情報を、防衛省と防衛関連企業の間で、電子データの形で安全かつ効率的に共有することを可能とする通信基盤です。

○ 防衛生産・技術基盤たる防衛関連企業は、いわば防衛力そのものであるとの基本姿勢のもと、防衛装備庁において「防衛産業サイバーセキュリティ基準」に従ったクラウドサービス基盤を整備し、これを防衛関連企業に利用してもらうことで、自社でこうした基盤を構築することが困難な企業も含め、総合的に防衛関連企業全体の情報セキュリティの強化を図ることを目指しています。

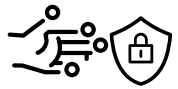
「防衛セキュリティゲートウェイの利用について(R5.12.8)」説明会資料より抜粋

2. サービスにより実現する事項

実現イメージは以下の通りです。

保護すべき情報の電子データ共有

多要素認証



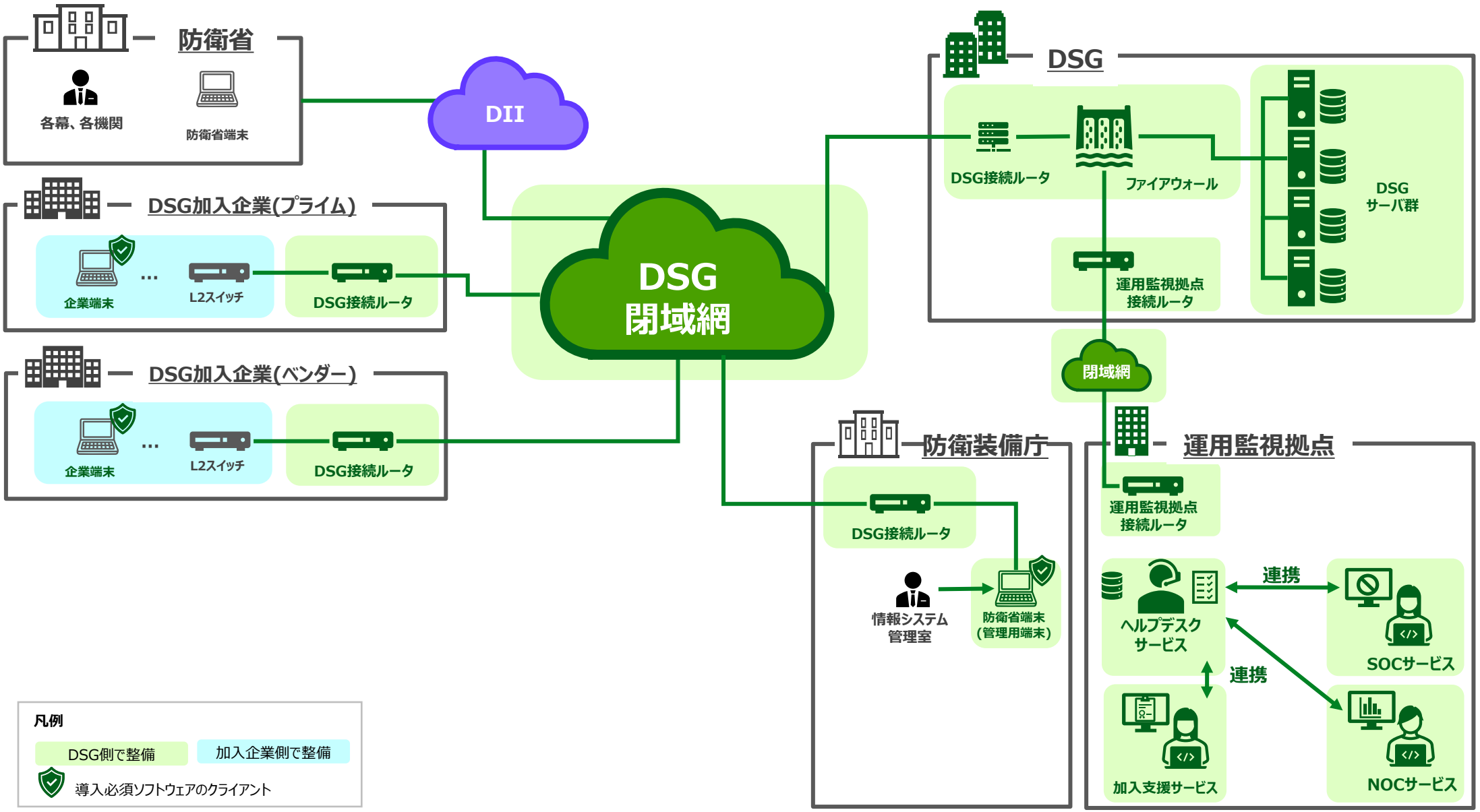
SOCでの常時監視

- 紙により授受をしていた保護すべき情報の電子共有
- DSGの利用に係る企業端末の監視、各種ログの取得、セキュリティ対策
- 企業側が行う保護システムの管理に必要な情報の提供(DSGで取得したものに限る。)
- 企業側が行う情報セキュリティに係るドキュメントの作成に必要な情報の提供(操作手順、運用要領等)
- 企業側に設置するDSG接続ルータの管理

3. サービス概要

3. DSGの全体像

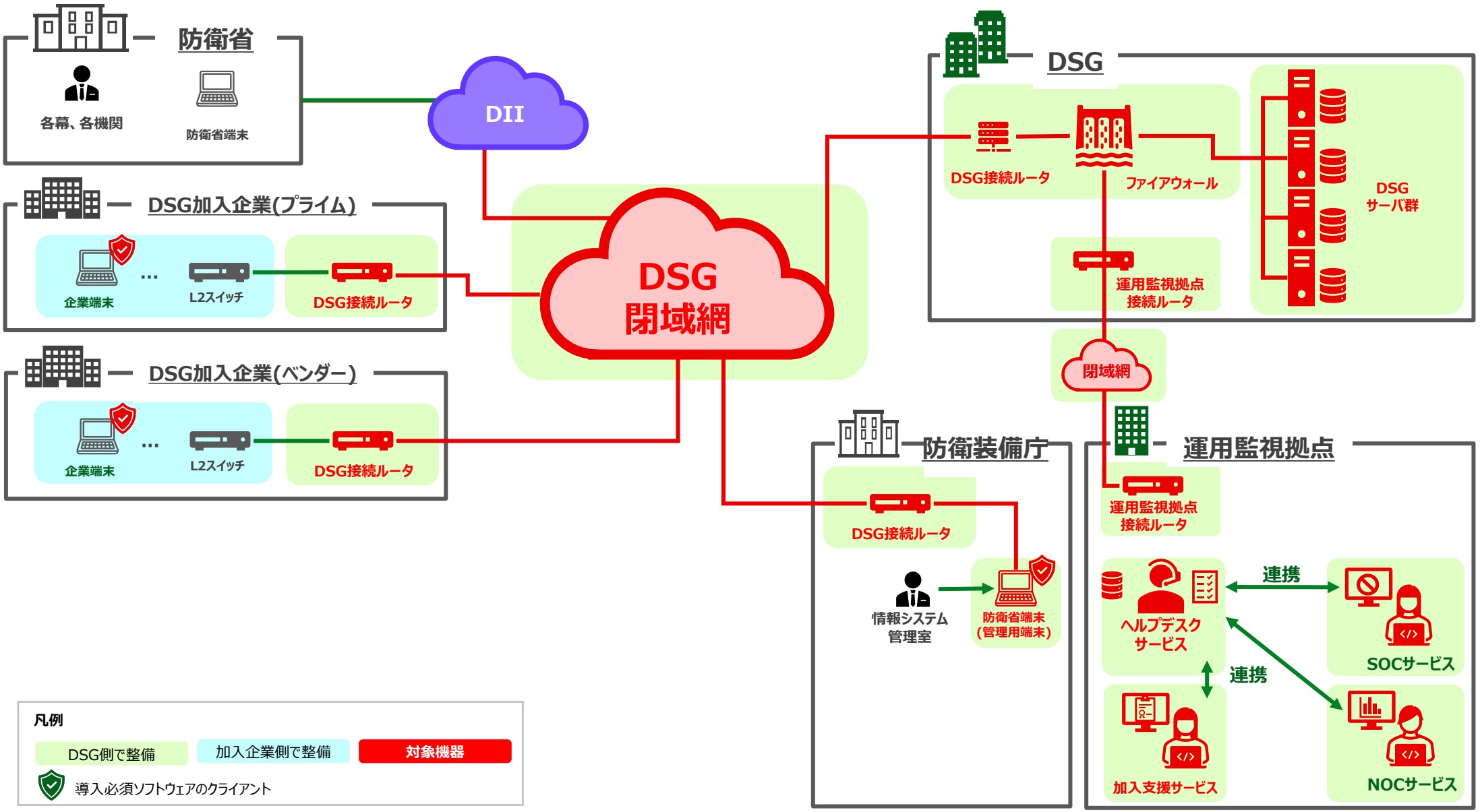
DSGの全体像は以下の通りです。



3. サービス概要

4. サービスの提供範囲

サービスの提供範囲は以下の通りです。



4. サービス内容

4.1 サービス一覧

DSGでは以下をサービスとして提供します。

(1/2)

#	サービス名	頁	サービスの概要
1	保護情報共有サービス	P.13	事業毎にアクセス可能な領域を作成することで、事業内の利用者間でのデータ閲覧及びデータ共有を行います。
2	アカウント管理サービス	P.18	アカウント管理に関する以下のサービスを提供します。 ・企業側の利用者及び官側の利用者から提出される申請書に基づき、 アカウントの登録、停止及び削除を実施します。 ・登録されたアカウントを使用してサービス利用時の認証サービスを提供します。 ・ログインに失敗した回数が一定回数を超えた場合、自動的にロックを実施します。 ・アカウントの管理操作(登録、停止及び削除)をログに記録します。
3	多要素認証サービス	P.22	多要素認証を用いて強固なセキュリティを提供します。 ※本サービスを官側の利用者が防衛省端末から利用する場合、生体認証は利用できません。
4	ファイアウォールサービス	P.25	セキュリティポリシーで通信を制御し、通信の正当性を確保します。また、許可されていない通信を遮断します。
5	マルウェア対策サービス	P.28	企業端末をマルウェアの脅威から防護するとともに、最新の定義体の配信を実施します。 また、許可されていない通信の遮断を行い、被害の拡散を抑制します。
6	脅威検知サービス	P.31	企業端末において、従来のエンドポイントセキュリティでは防ぎきれない未知の脅威を検知した際に SOCに通知するとともに、該当端末をネットワーク上から隔離し、証跡の保全や原因の特定に必要な解析等を行い、 被害の拡散を抑制します。
7	脆弱性監査サービス	P.34	企業端末の脆弱性監査を定期的に実施し、脆弱性の有無を確認します。 脆弱性監査結果は必要に応じて情報提供サービスにて加入企業に提供します。
8	構成管理サービス	P.37	企業端末での情報漏洩リスクの高い操作(印刷操作及び可搬記憶媒体へのデータ保存等)を抑止するとともに、 企業端末の操作履歴を記録します。また、企業端末のインベントリ収集、稼働実績管理及びライセンス管理を実施します。
9	NOCサービス (Network Operation Center)	P.42	ネットワークオペレーションに関する監視、障害検知、分析、対応、報告、問い合わせ対応、 必要な情報提供及び情報共有を実施します。
10	SOCサービス (Security Operation Center)	P.44	セキュリティ監視、分析、対応、通知、問い合わせ対応、必要な情報提供及び情報共有を実施します。

4.1 サービス一覧

DSGでは以下をサービスとして提供します。

(2/2)

#	サービス名	頁	サービスの概要
11	ヘルプデスクサービス	P.48	サービス利用に関する問い合わせ窓口(電話及びチャットボット等)を提供し、FAQの作成及び管理等を実施します。
12	加入支援サービス	P.51	サービスへの加入に関し、以下の支援を提供します。 ・サイトコンテンツの作成を実施します。 ・加入申請時に申請のあったアカウントの登録、停止及び削除を実施します。 ・DSGに加入するためのセットアップ手順書、利用マニュアル及びインストーラーを配布します。 ・ネットワークの開通を支援します。
13	回線・ルータ利用サービス	P.54	加入企業拠点とDSGを閉域網の専用回線で接続するとともに、仮想的なトンネルで隔絶し、通信を暗号化することで クローズドなネットワークを提供します。また、許可された企業端末以外の端末の接続を拒否します。
14	仮想化基盤サービス	P.57	DSGサービスの基盤となる各仮想マシンを稼働させることが可能です。
15	ストレージ利用サービス	P.60	仮想マシン、保護情報、バックアップ及び運用関連情報の保存先の領域を提供するとともに、 データの暗号化を行い、情報を保護します。
16	バックアップサービス	P.63	各サーバのデータを日々バックアップします。 不測の事態等でサーバに故障が発生した場合はバックアップからデータの復元を実施します。
17	セキュリティパッチ配信サービス	P.66	製品ベンダーからOS等のセキュリティパッチを取得し、企業端末に提供します。
18	DNSサービス (Domain Name System)	P.69	企業端末向けにポータルサイト、保護情報共有サービスのアクセス先となるドメイン名の名前解決を実施します。
19	NTPサービス (Network Time Protocol)	P.72	外部の信頼された機関から取得した標準時刻を企業端末に提供します。
20	ログ分析サービス	P.75	各種サービスより取得したログの収集及び相関分析を行い、セキュリティリスクの検出を実施します。
21	情報提供サービス	P.78	加入企業からの要請により、各種情報(構成情報、手順書、ログ情報、監査情報及び分析結果)を提供します。 (提供ログは別紙参照)

4.2 各サービスの説明
4.2.1 保護情報共有サービス

保護情報共有サービスでは以下をサービスとして提供します。

事業毎にアクセス可能な領域を作成することで、事業内の利用者間でのデータ閲覧及びデータ共有を行います。

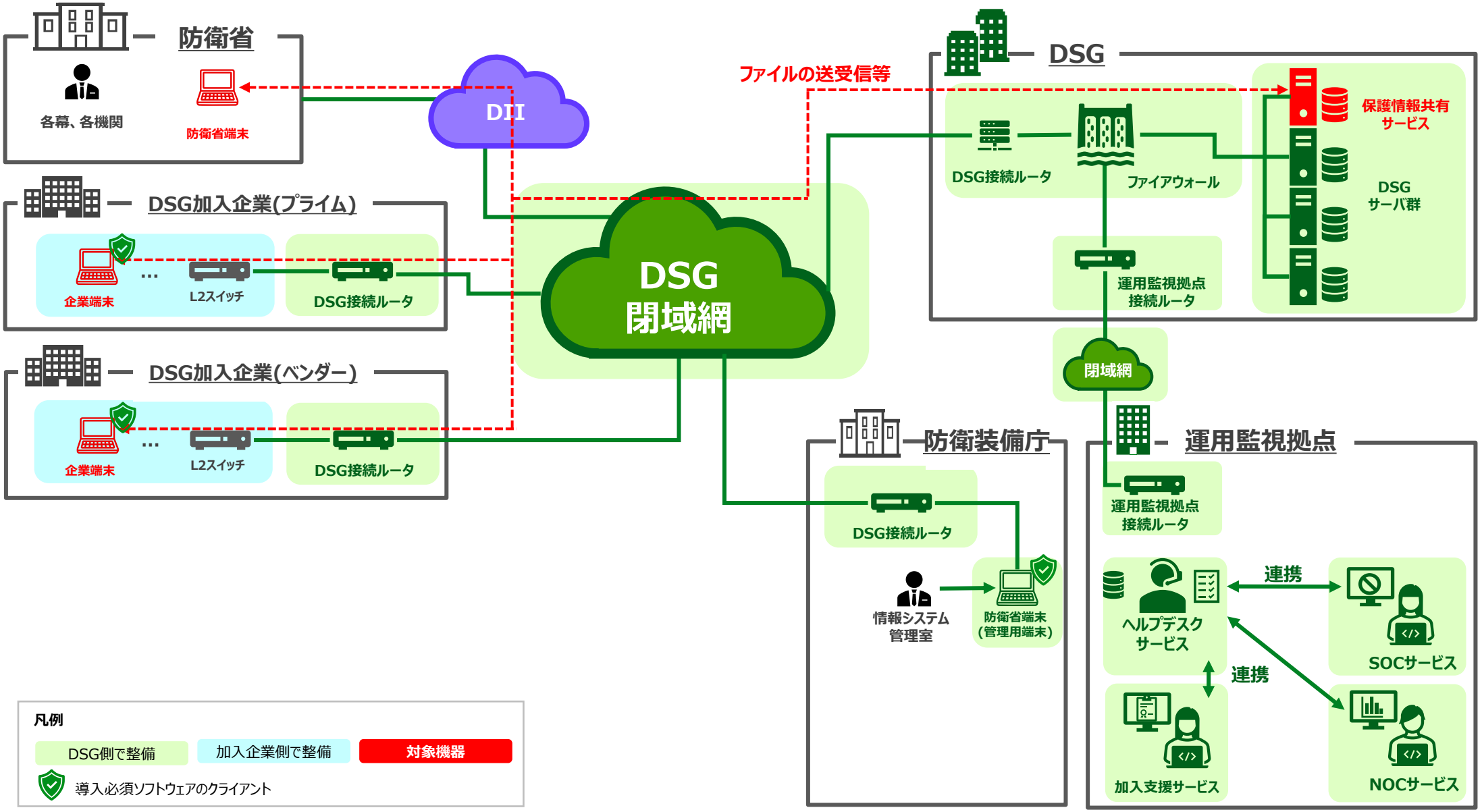
- **企業側の利用者及び官側の利用者のアカウント毎にサイトコンテンツ(事業毎に作成)のアクセス制御を実施し アクセス権限が付与されたサイトコンテンツにしかアクセスできない環境を提供します。**
- **企業端末及び防衛省端末からサイトコンテンツ(事業毎)の閲覧や、ファイルを登録して共有、検索が可能です。**
- **保護情報共有サービスで作成したファイルやフォルダのアクセス履歴の記録を実施します。**

本サービスで提供可能なログは以下の通りです。

- **監査ログ・カスタムレポートログ**
- **ポータルサイトアクセスログ**

4.2 各サービスの説明
4.2.1 保護情報共有サービス

保護情報共有サービスの概要図は以下の通りです。



4.2 各サービスの説明
4.2.1 保護情報共有サービス

保護情報共有サービスの利用イメージは下記の通りです。

ご利用のルール

- 24時間365日利用が可能です。(ただし、必要な場合は運用中断を行うことがあります)
- 取り扱い可能な情報のレベルは「保護すべき情報」以下です。
- 情報セキュリティ特約条項が付帯された契約の締結を前提に、当該契約の契約期間の間、利用が可能です。
- 契約毎、利用者毎にアカウントを付与します。また、利用者毎に生体認証登録が必要です。
- 利用申請時に企業側の契約プライム／ベンダー(サプライヤ)を把握し、それに対応した共通のフォルダ構成を提供します。
  フォルダ内では自由に新たなフォルダを作成いただけますが、アクセス制御が必要な場合は申請が必要です。
- 領域内にある情報は、閲覧のみとなります。
- 特定の拡張子(プログラム「.exe」やスクリプト「.ps1,.vbs」、メールデータ「.eml,.msg」等)のデータはアップロードできません。

4.2 各サービスの説明
4.2.1 保護情報共有サービス

保護情報共有サービスで利用を制限しているファイルの拡張子は以下の通りです。

利用不可拡張子一覧			
.ade	.ins	.ms-one-stub	.ws
.adp	.isp	.msp	.wsc
.asa	.its	.mst	.wsf
.ashx	.jse	.ops	.wsh
.asmx	.json	.pcd	.xamlx
.asp	.ksh	.pif	.7z
.bas	.lnk	.pl	.7zip
.bat	.mad	.prf	.afz
.cdx	.maf	.prg	.bz2
.cer	.mag	.printer	.bzip
.chm	.mam	.ps1	.bzip2
.class	.maq	.ps1xml	.cab
.cmd	.mar	.ps2	.gz
.cnt	.mas	.ps2xml	.gzip
.com	.mat	.psc1	.hqx
.config	.mau	.psc2	.lzh
.cpl	.mav	.pst	.rar
.crt	.maw	.reg	.sea
.csh	.mcf	.rem	.sit
.der	.mda	.scf	.sitx
.dll	.mdb	.scr	.tar.bz2
.eml	.mde	.sct	.tar.gz
.exe	.mdt	.shb	.tar.Z
.fxp	.mdw	.shs	.tbz
.gadget	.mdz	.shtm	.tgz
.grp	.msc	.shtml	.uu
.hlp	.msg	.soap	.Z
.hpj	.msh	.stm	.zip
.hta	.msh1	.svc	
.htr	.msh1xml	.url	
.htw	.msh2	.vb	
.ida	.msh2xml	.vbe	
.idc	.mshxml	.vbs	
.idq	.msi	.vsix	

4.2 各サービスの説明
4.2.1 保護情報共有サービス

保護情報共有サービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

本紙	内容
なし	
(以下空白)	

付紙	内容
第4-1	保護システムの領域の確定
第9-1-(1)-ア 第9-1-(1)-ア-(ア) 第9-1-(1)-ア-(イ)	システムログの取得
第9-2-(1)	システムログの管理
(以下空白)	

4.2 各サービスの説明
4.2.2 アカウント管理サービス

アカウント管理サービスでは以下をサービスとして提供します。

アカウント管理に関するサービスの提供を実施します。

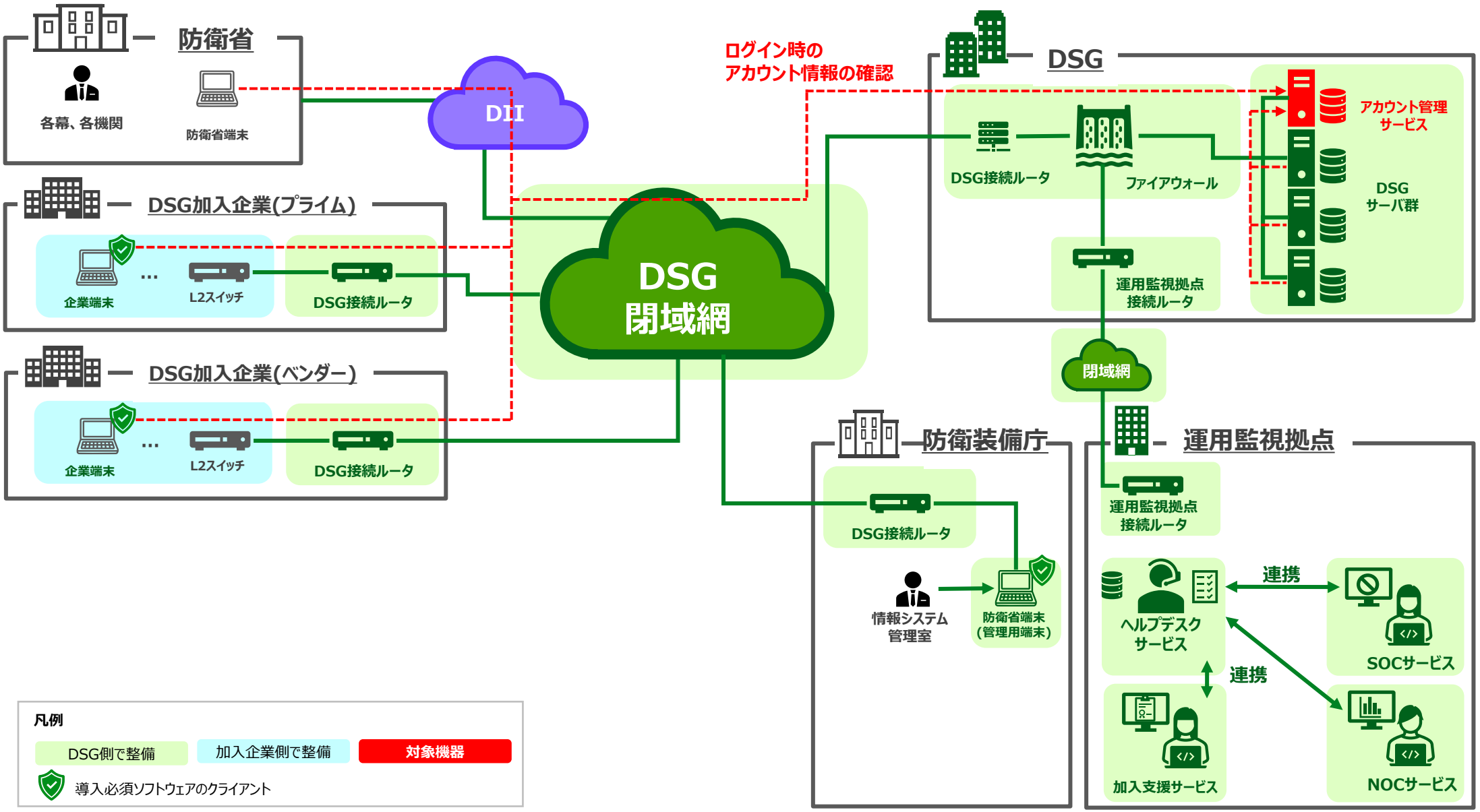
- **企業側の利用者及び官側の利用者から提出される申請書に基づき、アカウントの登録、停止及び削除を実施します。**
- **登録されたアカウントを使用してサービス利用時の認証サービスを提供します。**
- **ログインに失敗した回数が一定回数を超えた場合、自動的にロックを実施します。**
- **アカウントの管理操作(登録、停止及び削除)をログに記録します。**

本サービスで提供可能なログは以下の通りです。

- **アカウント管理操作ログ**

4.2 各サービスの説明
4.2.2 アカウント管理サービス

アカウント管理サービスの概要図は以下の通りです。



4.2 各サービスの説明
4.2.2 アカウント管理サービス

アカウント管理サービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

本紙	内容
なし	
(以下空白)	

付紙	内容
第2-1-(2)-オ	第５第１項第１号に規定するアクセス制御方針
第3-2-(3)-イ-(ア) 第3-2-(3)-イ-(イ)	アクセス権限の特定等
第4-4-(2)	管理者用機能と利用者用機能の分離
第4-4-(3)	管理者用機能の不正利用防止
第5-2-(1)-ア 第5-2-(1)-イ 第5-2-(1)-ウ 第5-2-(1)-エ 第5-2-(1)-オ-(ア) 第5-2-(1)-カ	アカウントの管理
第5-2-(3)-ア 第5-2-(3)-ウ	ユーザセッションの管理
(次頁へ続く)	

4.2 各サービスの説明
4.2.2 アカウント管理サービス

アカウント管理サービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

付紙	内容
第6-1-(1)-ア 第6-1-(1)-エ	識別の実施
第7-2-(2)-ア	保護すべき情報の通信制限
第9-4	システムログを取得するツールの保護
(以下空白)	

4.2 各サービスの説明
4.2.3 多要素認証サービス

多要素認証サービスでは以下をサービスとして提供します。

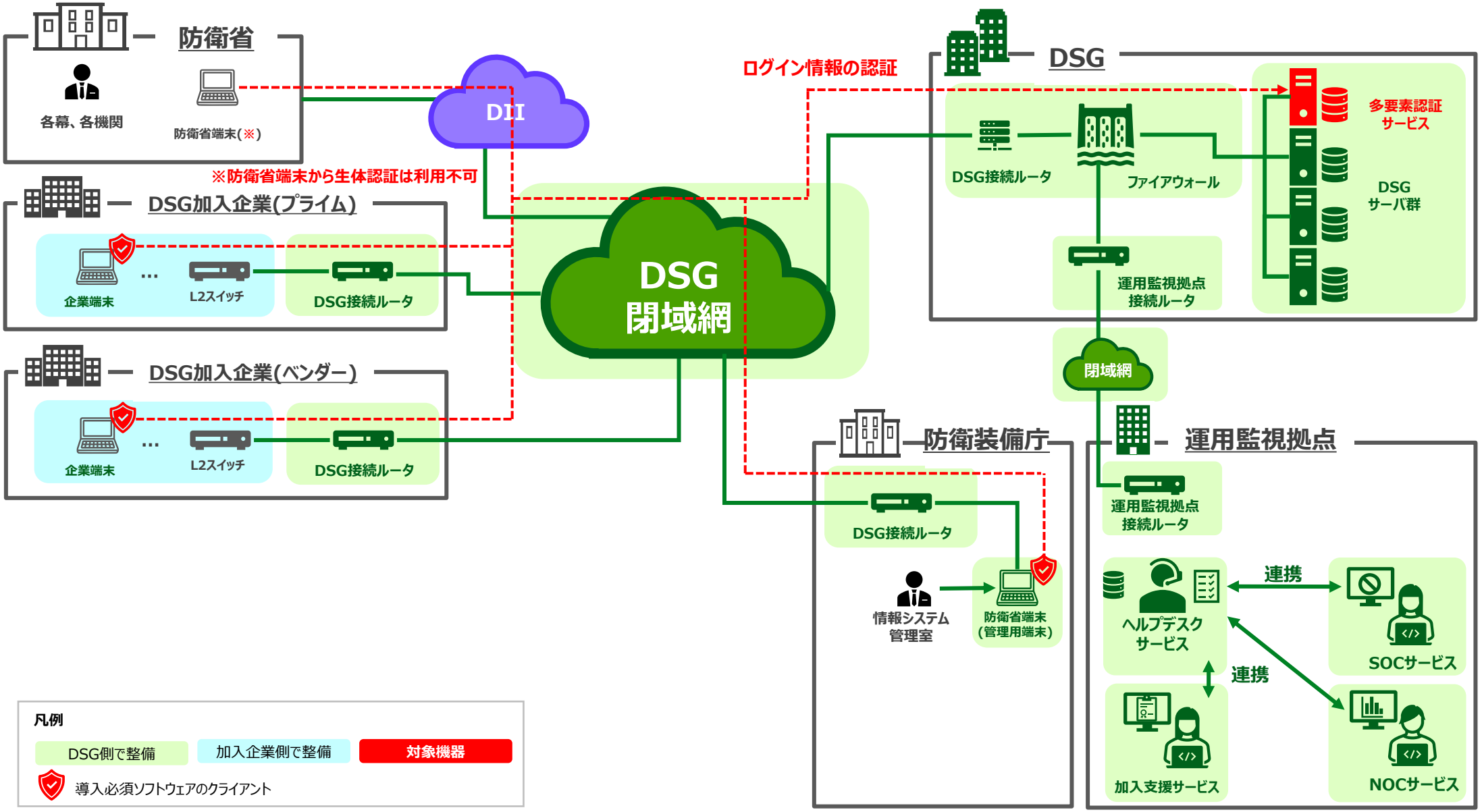
多要素認証を用いて強固なセキュリティを提供します。
※官側の利用者が防衛省端末からDSGサービスを利用する場合、生体情報による認証は利用しません。

・ユーザID＋パスワード＋生体情報による多要素認証を実施します。
・多要素認証サービスを利用して企業端末にログインした履歴を記録します。
・防衛産業サイバーセキュリティ基準に定める要件に合致したパスワードの発行管理を実施します。

本サービスで提供可能なログは以下の通りです。
・認証ログ(多要素認証)

4.2 各サービスの説明
4.2.3 多要素認証サービス

多要素認証サービスの概要図は以下の通りです。



4.2 各サービスの説明
4.2.3 多要素認証サービス

多要素認証サービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

本紙	内容
なし	
(以下空白)	

付紙	内容
第5-2-(2)-ア	ログオンの管理
第5-2-(2)-イ	ログオン試行
第5-2-(3)-エ	ユーザセッションの管理
第6-1-(2)-ア	認証の実施
第6-1-(3)-ア 第6-1-(3)-ウ 第6-1-(3)-エ-(ア) 第6-1-(3)-エ-(イ) 第6-1-(3)-エ-(ウ) 第6-1-(3)-カ	パスワードによる認証の実施
第6-2-(1)	識別及び認証におけるその他の留意事項
(以下空白)	

4.2 各サービスの説明
4.2.4 ファイアウォールサービス

ファイアウォールサービスでは以下をサービスとして提供します。

セキュリティポリシーで通信を制御し、通信の正当性を確保します。また、許可されていない通信を遮断します。

- **DSGと企業端末及び防衛省端末間の通信をセキュリティポリシーに従って制御し、DSG側で許可した通信以外を遮断します。(※)**
- **ネットワーク上の通信を監視し、侵入の兆候を検知／遮断し、不正なアクセスを防止します。**
- **ファイアウォールを通過した通信／遮断した通信をログに記録することを実施します。**

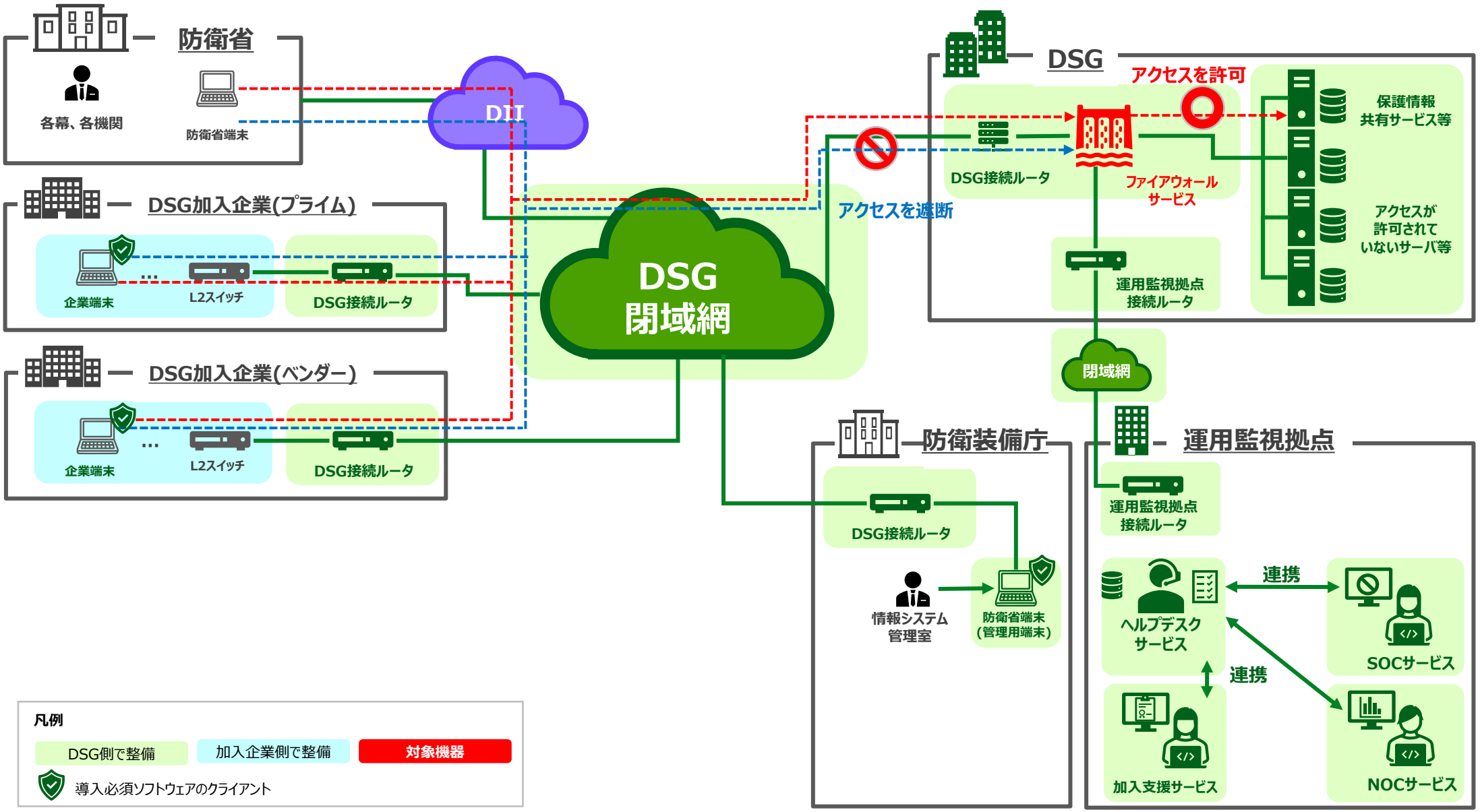
※ 本サービスではファイアウォールを通過する通信の内容(送信元／送信先／プロトコル／ポート番号等)を確認し、許可された通信以外を遮断します。

本サービスで提供可能なログは以下の通りです。

- **ファイアウォールログ**

4.2 各サービスの説明
4.2.4 ファイアウォールサービス

ファイアウォールサービスの概要図は以下の通りです。



4.2 各サービスの説明
4.2.4 ファイアウォールサービス

ファイアウォールサービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

本紙	内容
なし	
(以下空白)	

付紙	内容
第3-2-(3)-ウ	必要最小限度の機能等の設定
第4-4-(4)	仮想化技術の利用時の対策
第7-2-(1)-ア	保護すべき情報の通信制限
第8-2-(2)-ア-(ア) 第8-2-(2)-ア-(イ)	システム及び通信の監視方法
第9-4	システムログを取得するツールの保護
(以下空白)	

4.2 各サービスの説明
4.2.5 マルウェア対策サービス

マルウェア対策サービスでは以下をサービスとして提供します。

企業端末をマルウェアの脅威から防護するとともに、最新の定義体の配信を実施します。また、許可されていない通信の遮断を行い、被害の拡散を抑制します。

- **ファイルにアクセスする際に自動的にスキャンを実施し、マルウェア等の不正なプログラムの実行の抑止を実施します。**
- **ファイルにアクセスする際に自動的にスキャンを実施し、マルウェア等の不正なプログラムと判別した場合は対象ファイルの削除又は隔離処置を実施することで企業端末を保護します。**
- **企業端末内の情報を定期的にスキャンすることでマルウェア等の有無を確認し、企業端末を保護します。**
- **マルウェア等を検知した際、検知情報の記録を実施します。**
- **最新のマルウェア等に対応するため、最新の定義体の配信を実施します。**
- **企業端末の通信をセキュリティポリシーに従って制御し、DSG側で許可した通信以外を遮断します。(※)**

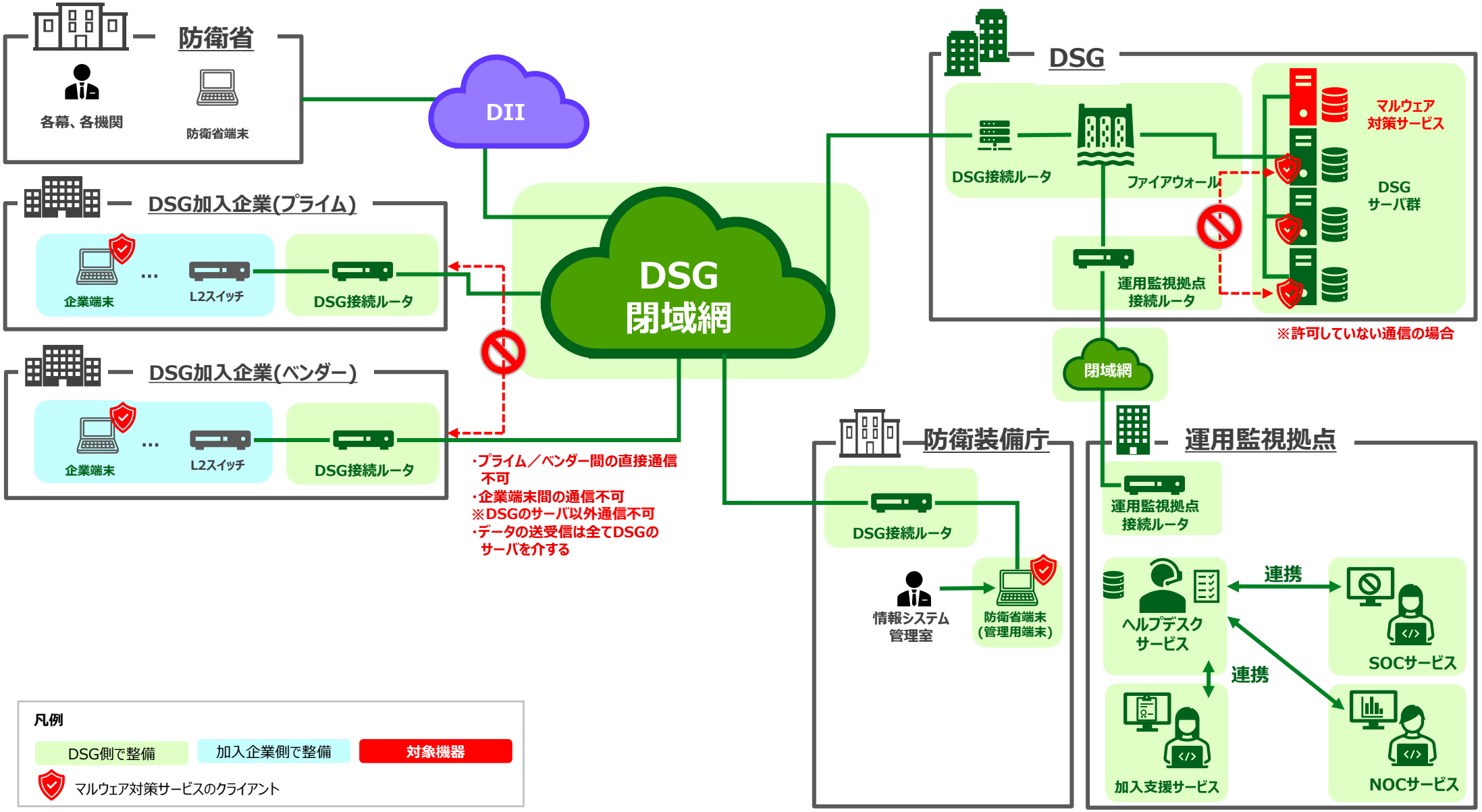
※ 本サービスでは企業端末間で直接実施される通信(DSG側のDSG接続ルータやファイアウォールまで届かない通信)を遮断します。そのため、DSGを利用するためにセットアップされた企業端末はDSGのサーバとしか通信できないように制御されます。

本サービスで提供可能なログは以下の通りです。

- **マルウェア検知ログ**

4.2 各サービスの説明
4.2.5 マルウェア対策サービス

マルウェア対策サービスの概要図は以下の通りです。



4.2 各サービスの説明
4.2.5 マルウェア対策サービス

マルウェア対策サービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

本紙	内容
なし	
(以下空白)	

付紙	内容
第8-2-(2)-イ-(ア) 第8-2-(2)-イ-(イ) 第8-2-(2)-イ-(ウ) 第8-2-(2)-イ-(エ)	悪意のあるコードの検知
(以下空白)	

4.2 各サービスの説明
4.2.6 脅威検知サービス

脅威検知サービスでは以下をサービスとして提供します。

企業端末において、従来のエンドポイントセキュリティでは防ぎきれない未知の脅威を検知した際にSOCに通知するとともに、該当端末をネットワーク上から隔離し、証跡の保全や原因の特定に必要な解析等を行い、被害の拡散を抑制します。

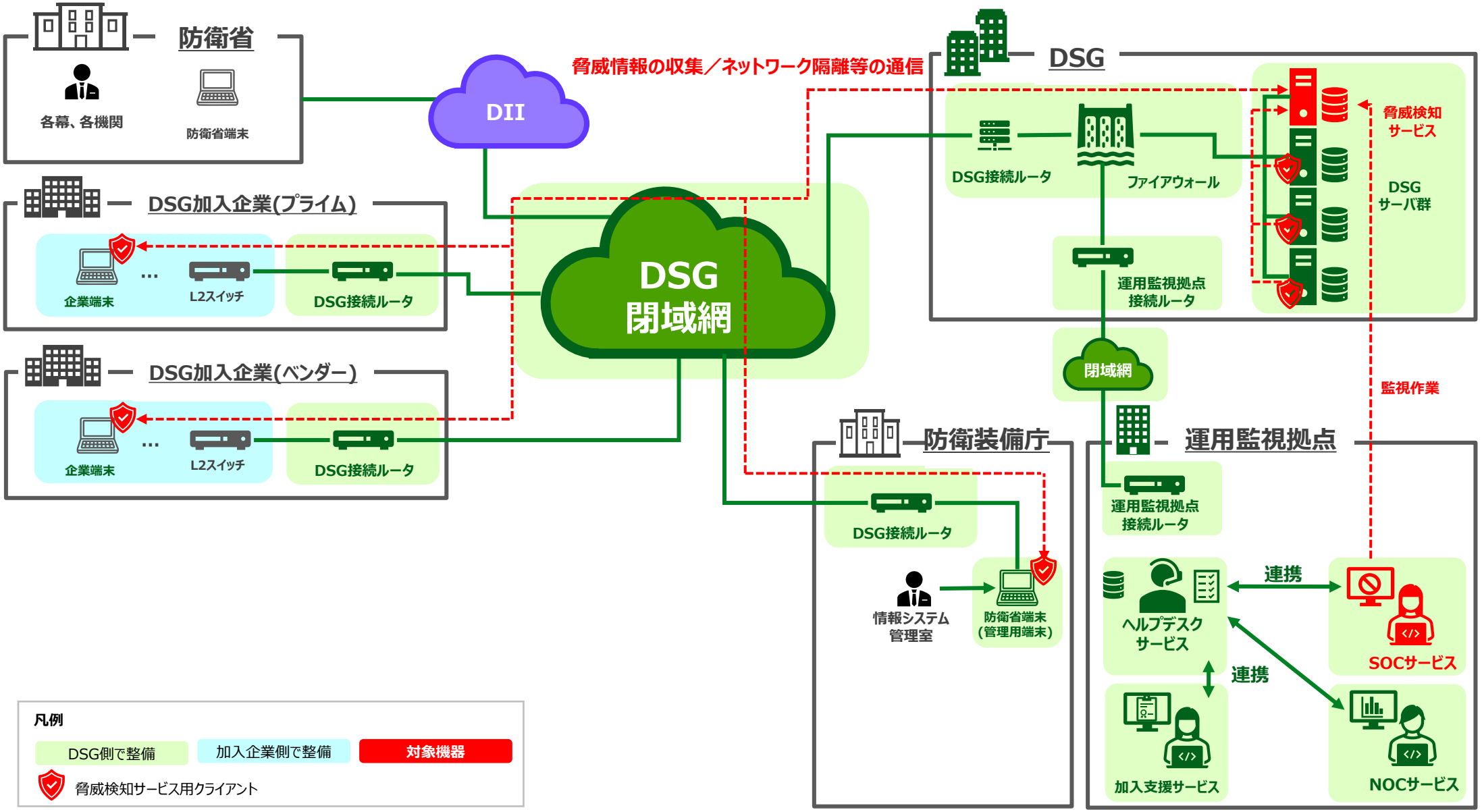
- **企業端末にインストールされているクライアントソフトから収集した端末情報から企業端末上の脅威情報を検知、記録を実施します。**
- **マルウェア対策サービスで検知できない未知のマルウェアや悪意のある操作等、企業端末上の挙動(振る舞い)を監視し、怪しい挙動が確認された企業端末については、DSG側から遠隔操作でネットワークから隔離措置を実施します。**

本サービスで提供可能なログは以下の通りです。

- **脅威検知ログ**

4.2 各サービスの説明
4.2.6 脅威検知サービス

脅威検知サービスの概要図は以下の通りです。



4.2 各サービスの説明
4.2.6 脅威検知サービス

脅威検知サービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

本紙	内容
第10-1-(1)-エ	情報セキュリティ事故等対処計画の策定
(以下空白)	

付紙	内容
第6-1-(1)-オ	識別の実施
第8-1 第8-1-(1) 第8-1-(2) 第8-1-(3) 第8-1-(4)	システム監視の実施
第8-2-(1)-イ	システム監視の実施に係る共通事項
第8-3	不正なアクセス等を検知した際の対応
(以下空白)	

4.2 各サービスの説明
4.2.7 脆弱性監査サービス

脆弱性監査サービスでは以下をサービスとして提供します。

企業端末の脆弱性監査を定期的に実施し、脆弱性の有無を確認します。
脆弱性監査結果は必要に応じて情報提供サービスにて加入企業に提供します。

- **企業端末に導入したクライアントで端末内部を定期的にスキャンし、端末内部の脆弱性の有無について確認を実施します。**

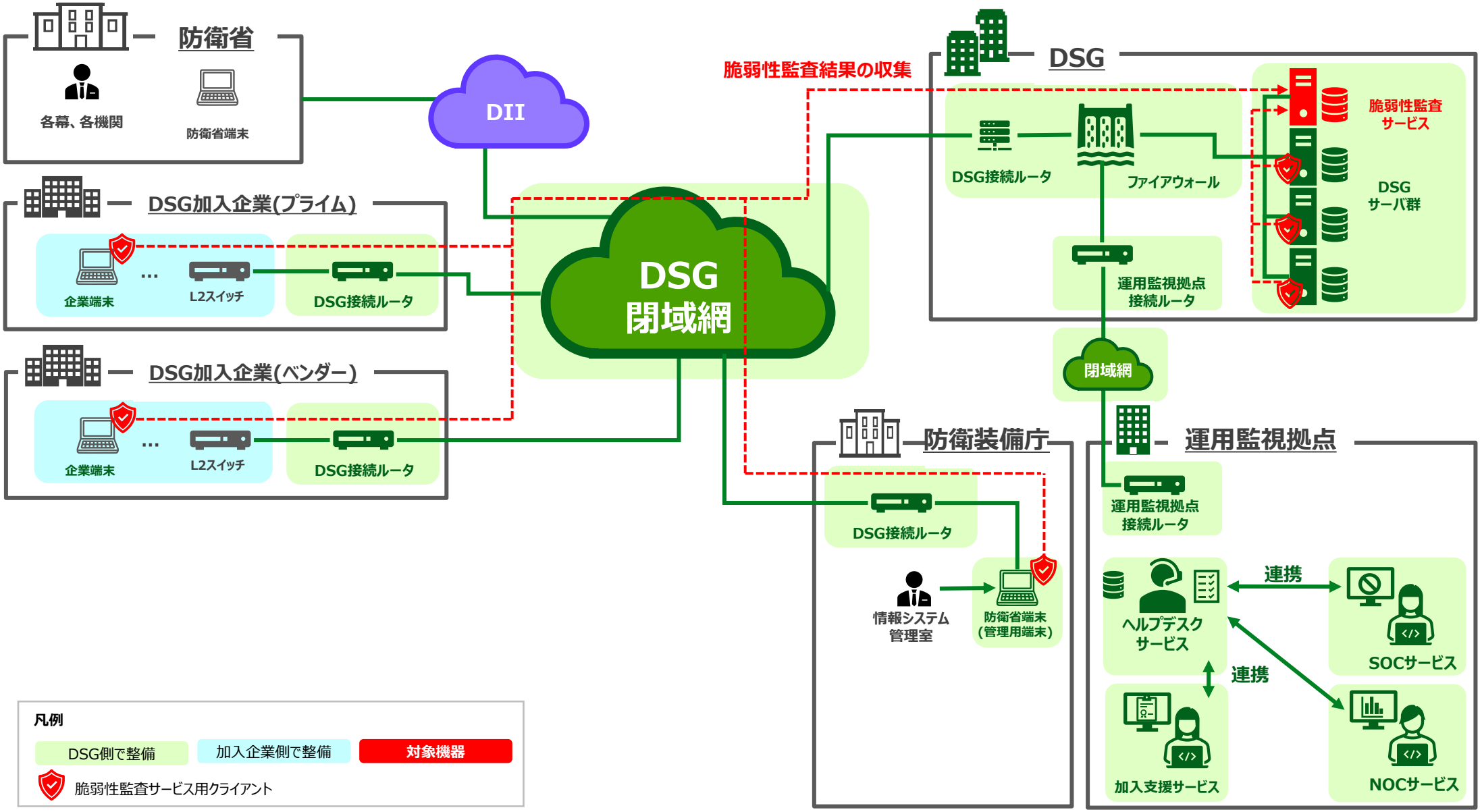
本サービスでは企業端末に存在する脆弱性を監査し、以下の項目を含む**脆弱性監査結果**を提供します。(※1)

- **脆弱性が検出された企業端末のIPアドレス及びホスト名**
- **検出された脆弱性の概要**
- **検出された脆弱性の対処案**
- **検出された脆弱性のCVSS(※2)**
- **検出された脆弱性の共通脆弱性識別子(CVE)(※3)**

※1 本サービスでは脆弱性監査結果を提供しますが、監査時のログの提供はできません。
※2 CVSS(Common Vulnerability Scoring System) : システムやソフトウェアに存在する脆弱性の深刻度を評価する国際的な指標
※3 CVE(Common Vulnerabilities and Exposures) : 発見された脆弱性に付与される一意の識別子

4.2 各サービスの説明
4.2.7 脆弱性監査サービス

脆弱性監査サービスの概要図は以下の通りです。



4.2 各サービスの説明
4.2.7 脆弱性監査サービス

脆弱性監査サービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

本紙	内容
なし	
(以下空白)	

付紙	内容
第3-3-(1)	ベースライン構成設定等の変更等
第10-1-(1) 第10-1-(2) 第10-1-(3)	脆弱性スキャンの実施
第10-2-(1) 第10-2-(2) 第10-2-(3)	分析結果等の利用
(以下空白)	

4.2 各サービスの説明
4.2.8 構成管理サービス

構成管理サービスでは以下をサービスとして提供します。

企業端末での情報漏洩リスクの高い操作(印刷操作及び可搬記憶媒体へのデータ保存等)を抑止するとともに、企業端末の操作履歴を記録します。また、企業端末のインベントリ収集、稼働実績管理及びライセンス管理を実施します。

- **企業端末の操作を記録します。**
- **原則として、情報漏洩リスクの高い操作を禁止します。(※1)**
  例：印刷操作、可搬記憶媒体へのデータ保存、PrintScreenキーの制限
- **企業端末の資産情報を収集します。**

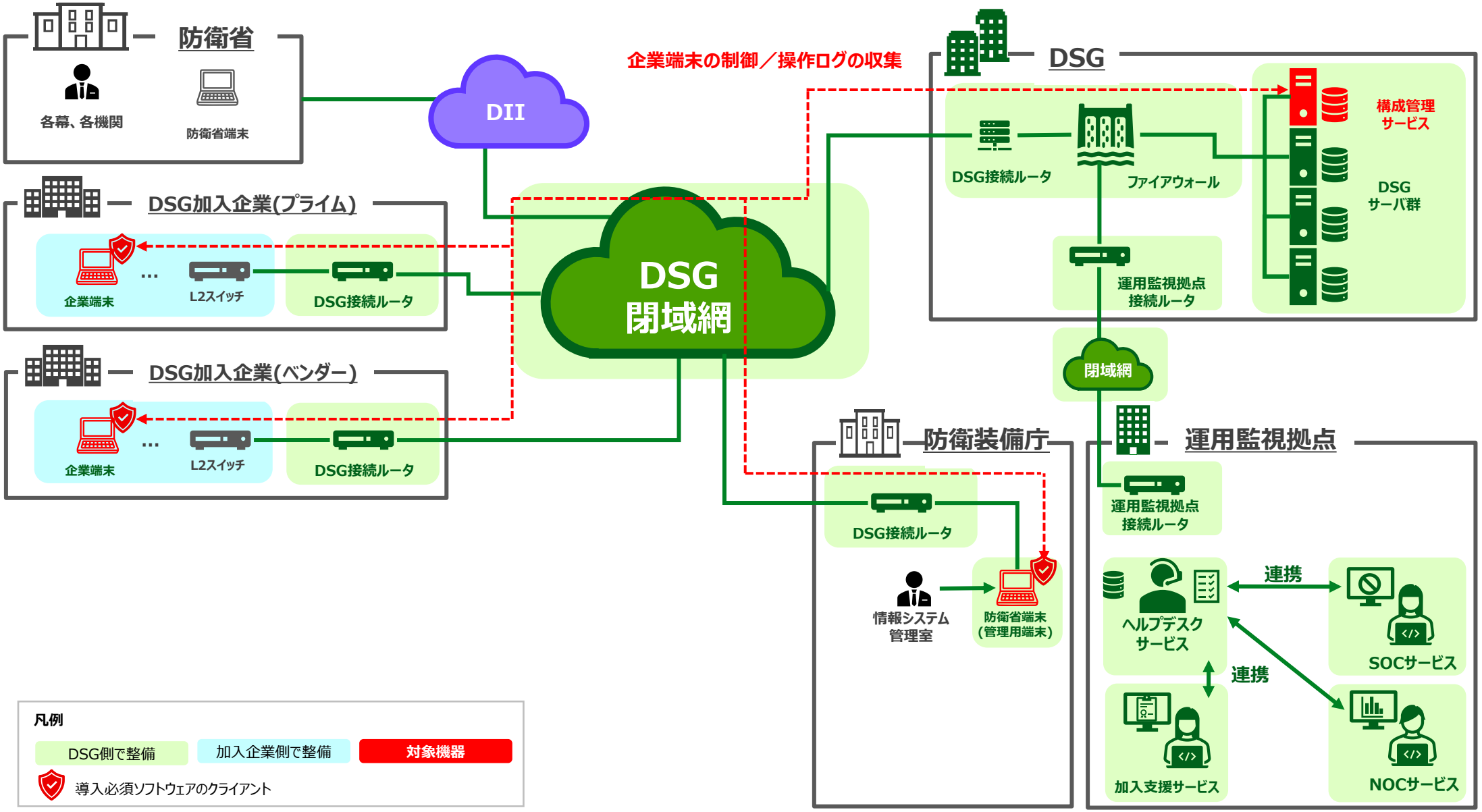
※1 サービス利用開始時は一律で印刷操作等の操作を禁止する制御を実施していますが、企業側から別途DSGに申請をいただくことで一時的に禁止操作の解除が可能です。

本サービスで提供可能なログ及び構成情報は以下の通りです。

- **操作ログ(起動、終了/クライアント操作/ファイルアクセス/ファイル操作/クリップボード/プリント/Webアクセス/ドライブ追加、削除/フォルダ共有)**
- **アプリケーションログ**
- **通信デバイスログ**
- **システムログ**
- **IT資産情報**
- **ベースライン構成**
- **ネットワーク構成図**

4.2 各サービスの説明
4.2.8 構成管理サービス

構成管理サービスの概要図は以下の通りです。



4.2 各サービスの説明
4.2.8 構成管理サービス

構成管理サービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

本紙	内容
第6-5-(3) 第6-5-(5) 第6-5-(6)	保護システムにおける可搬記憶媒体の使用制限
(以下空白)	

付紙	内容
第2-(2)-ア	第３第２項第１号に規定するベースライン構成設定
第2-(2)-イ	第３第２項第５号に規定するブラックリスト又はホワイトリスト
第2-(2)-ウ	第３第４項第１号に規定する構成設定目録
(次頁へ続く)	

構成管理サービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

付紙	内容
第3-2-(1)-ア 第3-2-(1)-イ 第3-2-(1)-ウ 第3-2-(2)	ベースライン構成設定等
第3-2-(3)-ア 第3-2-(3)-ウ	構成設定の方法
第3-2-(4)	構成設定の精査
第3-2-(5)-ア 第3-2-(5)-イ 第3-2-(5)-ウ 第3-2-(5)-エ	ブラックリスト又はホワイトリストの作成等
第3-4-(1)-ア-(ア)	目録の作成
第3-4-(1)-イ-(ア) 第3-4-(1)-イ-(イ)	目録の更新
第3-4-(2)	構成設定に係る記録
第4-3-(1)-イ	暗号化
(次頁へ続く)	

構成管理サービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

付紙	内容
第4-4-(1)-ア	ソフトウェアのインストール及びアップデートの制限等
第6-1-(1)-ア 第6-1-(1)-エ	識別の実施
第6-1-(2)-ウ	認証の実施
第9-1-(1)-ア-(ア) 第9-1-(1)-ア-(イ)	システムログの取得
(以下空白)	

4.2 各サービスの説明
4.2.9 NOCサービス

NOCサービスでは以下をサービスとして提供します。

ネットワークオペレーションに関する監視、障害検知、分析、対応、報告、問い合わせ対応、必要な情報提供及び情報共有を実施します。

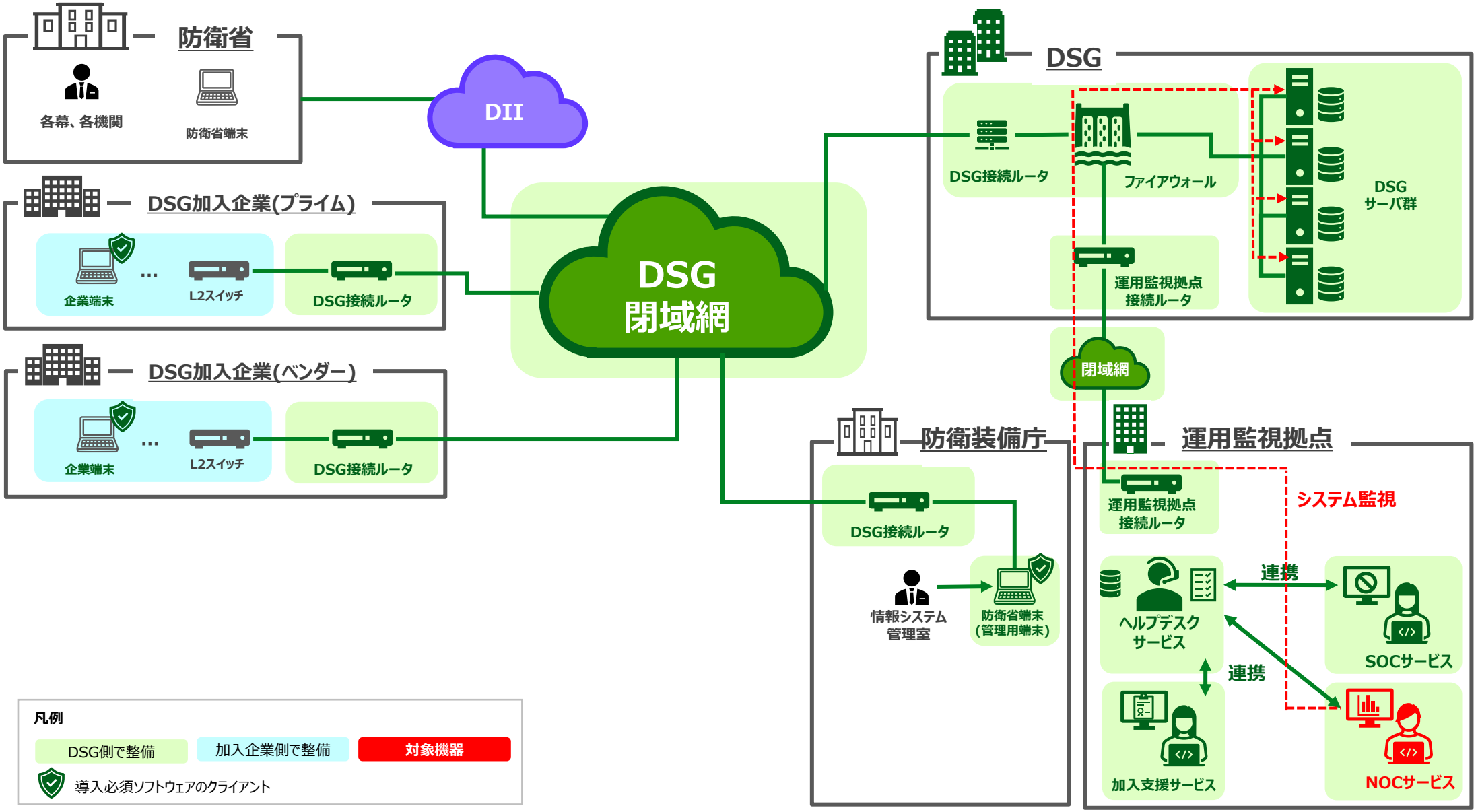
- **システムをトラブルから守るため、24時間365日でシステムの監視を実施します。**
- **システムで発生したインシデントの管理(※)を実施します。**

※ 発生したインシデントに対して、インシデントの発生から対策、解決(クローズ)までの一連の流れを管理し、コントロールを行います。

本サービスで提供可能なログはありません。

4.2 各サービスの説明
4.2.9 NOCサービス

NOCサービスの概要図は以下の通りです。



4.2 各サービスの説明
4.2.10 SOCサービス

SOCサービスでは以下をサービスとして提供します。

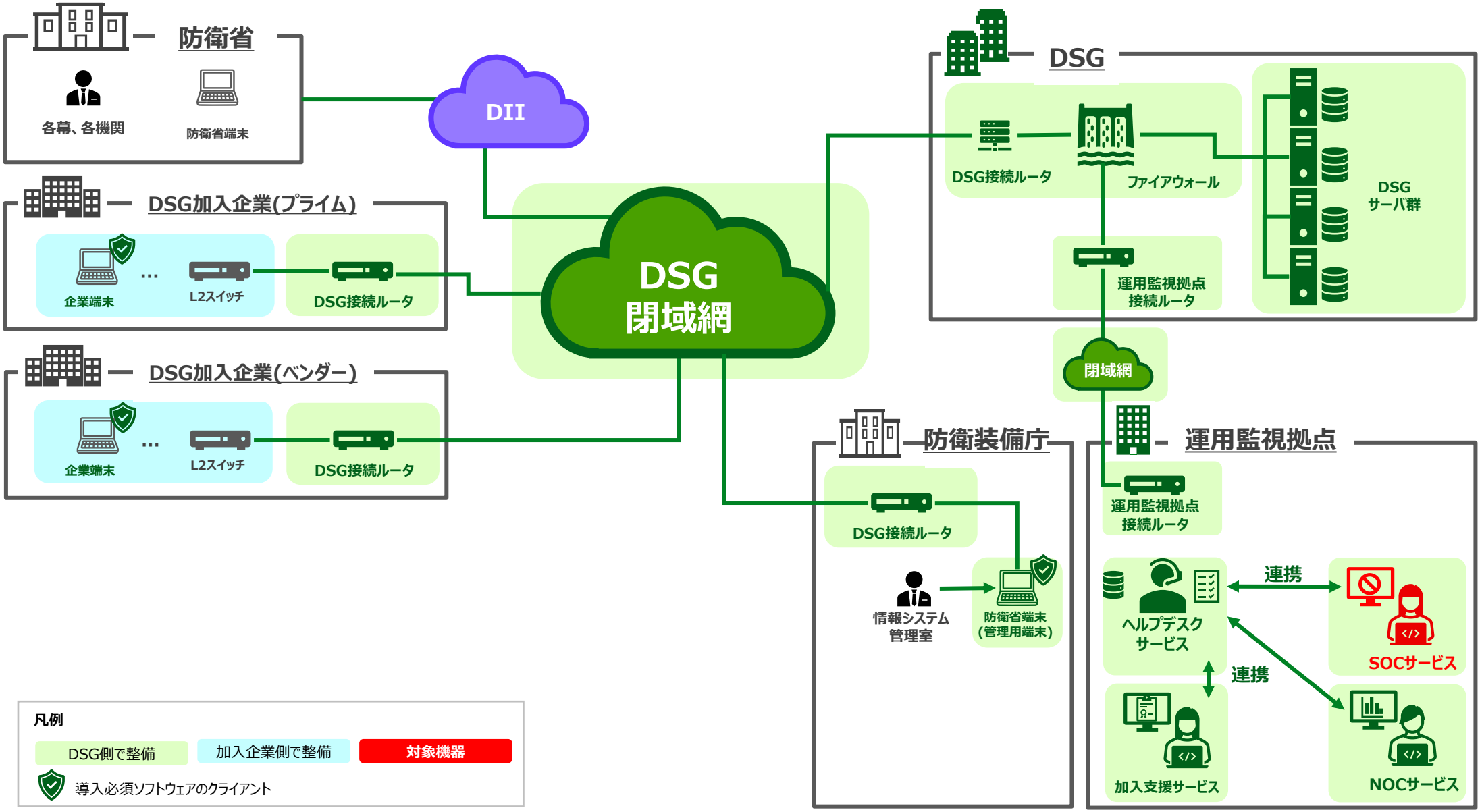
セキュリティ監視、分析、対応、通知、問い合わせ対応、必要な情報提供及び情報共有を実施します。

- **防衛産業サイバーセキュリティ基準を満たす専用のSOC体制を設置し、セキュリティ監視を実施します。**
- **企業端末のセキュリティイベントをログ分析サービスと連携して収集、監視、分析を実施し、検知した脅威に応じた対処(通知、隔離、復旧支援等)を実施します。**
- **情報セキュリティ事故を検知した場合は、情報提供を実施します。**

本サービスで提供可能なログはありません。

4.2 各サービスの説明
4.2.10 SOCサービス

SOCサービスの概要図は以下の通りです。



4.2 各サービスの説明
4.2.9 NOCサービス／4.2.10 SOCサービス

NOCサービス及びSOCサービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

本紙	内容
第10-1-(1)-ウ 第10-1-(1)-オ 第10-1-(1)-カ 第10-1-(2)-イ 第10-1-(2)-ウ 第10-1-(2)-エ	情報セキュリティ事故等対処計画の策定
第11-1-(2)	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
第11-2-(1) 第11-2-(2)	防衛省への報告
(以下空白)	

4.2 各サービスの説明
4.2.9 NOCサービス／4.2.10 SOCサービス

NOCサービス及びSOCサービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

付紙	内容
第8-2-(1)-ア 第8-2-(1)-イ 第8-2-(1)-ウ	システム監視の実施に係る共通事項
第8-4-(1)	システム監視により取得した情報の利用及び保管
第9-1-(1)-イ 第9-1-(1)-ウ 第9-1-(1)-オ	システムログの取得
第9-1-(2)-ア 第9-1-(2)-イ-(ア) 第9-1-(2)-イ-(イ) 第9-1-(2)-ウ 第9-1-(2)-エ 第9-1-(2)-オ	システムログの分析
(以下空白)	

4.2 各サービスの説明
4.2.11 ヘルプデスクサービス

ヘルプデスクサービスでは以下をサービスとして提供します。

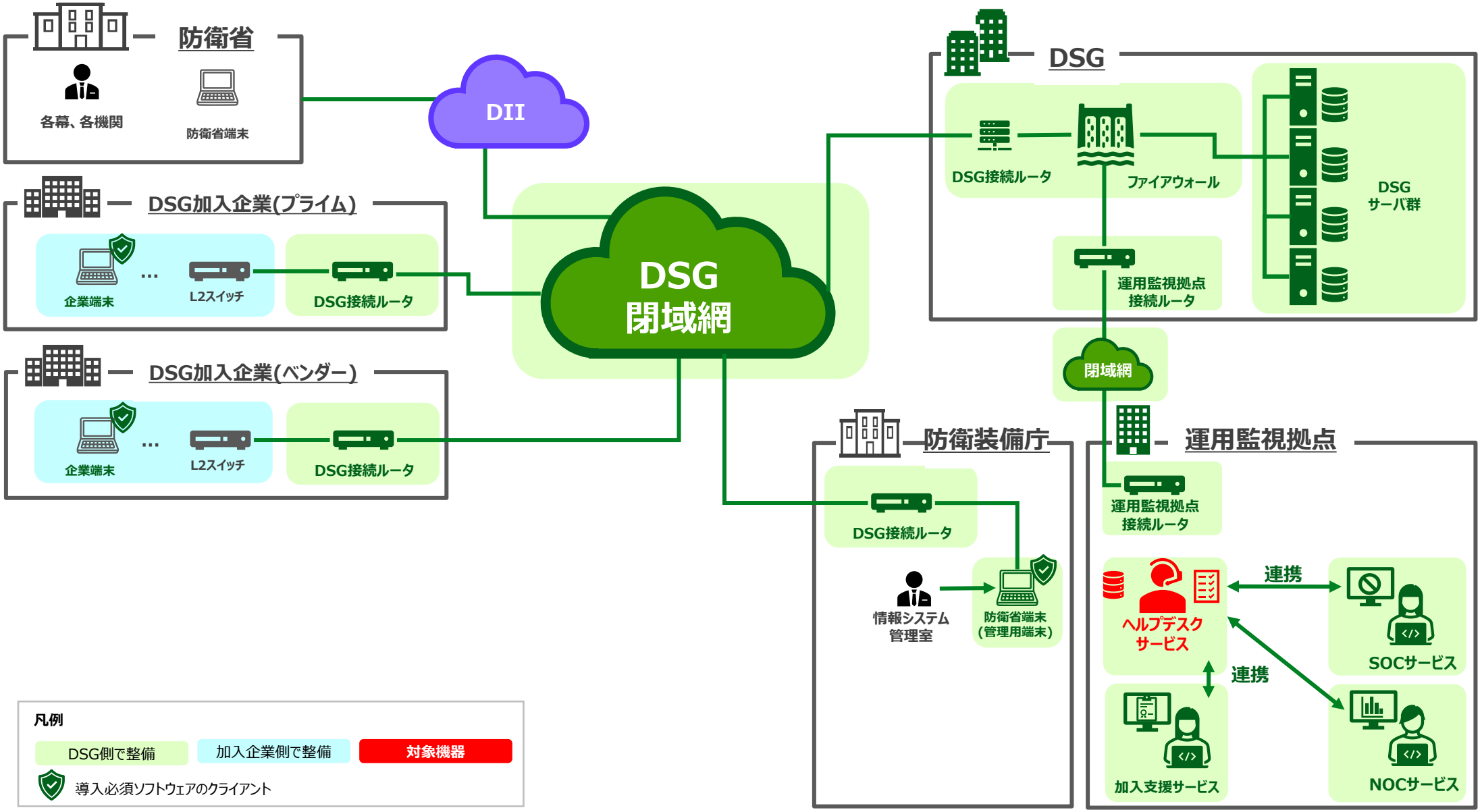
サービス利用に関する問い合わせ窓口(電話及びチャットボット等)を提供し、FAQの作成及び管理等を実施します。

- **防衛セキュリティゲートウェイポータルサイトに掲載する「お知らせ」を通じてサービスの提供状況を共有します。**
- **疑問やトラブルに即応する自動応答(チャットボット)と詳細な調査にも対応するヘルプデスク体制を提供します。**
- **蓄積したFAQはチャットボットで公開します。**

本サービスで提供可能なログはありません。

4.2 各サービスの説明
4.2.11 ヘルプデスクサービス

ヘルプデスクサービスの概要図は以下の通りです。



4.2 各サービスの説明
4.2.11 ヘルプデスクサービス

ヘルプデスクサービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

本紙	内容
第10-1-(2)-ア	情報セキュリティ事故等対処計画の策定
(以下空白)	

付紙	内容
なし	
(以下空白)	

4.2 各サービスの説明
4.2.12 加入支援サービス

加入支援サービスでは以下をサービスとして提供します。

サービスへの加入に関し、各種支援を実施します。

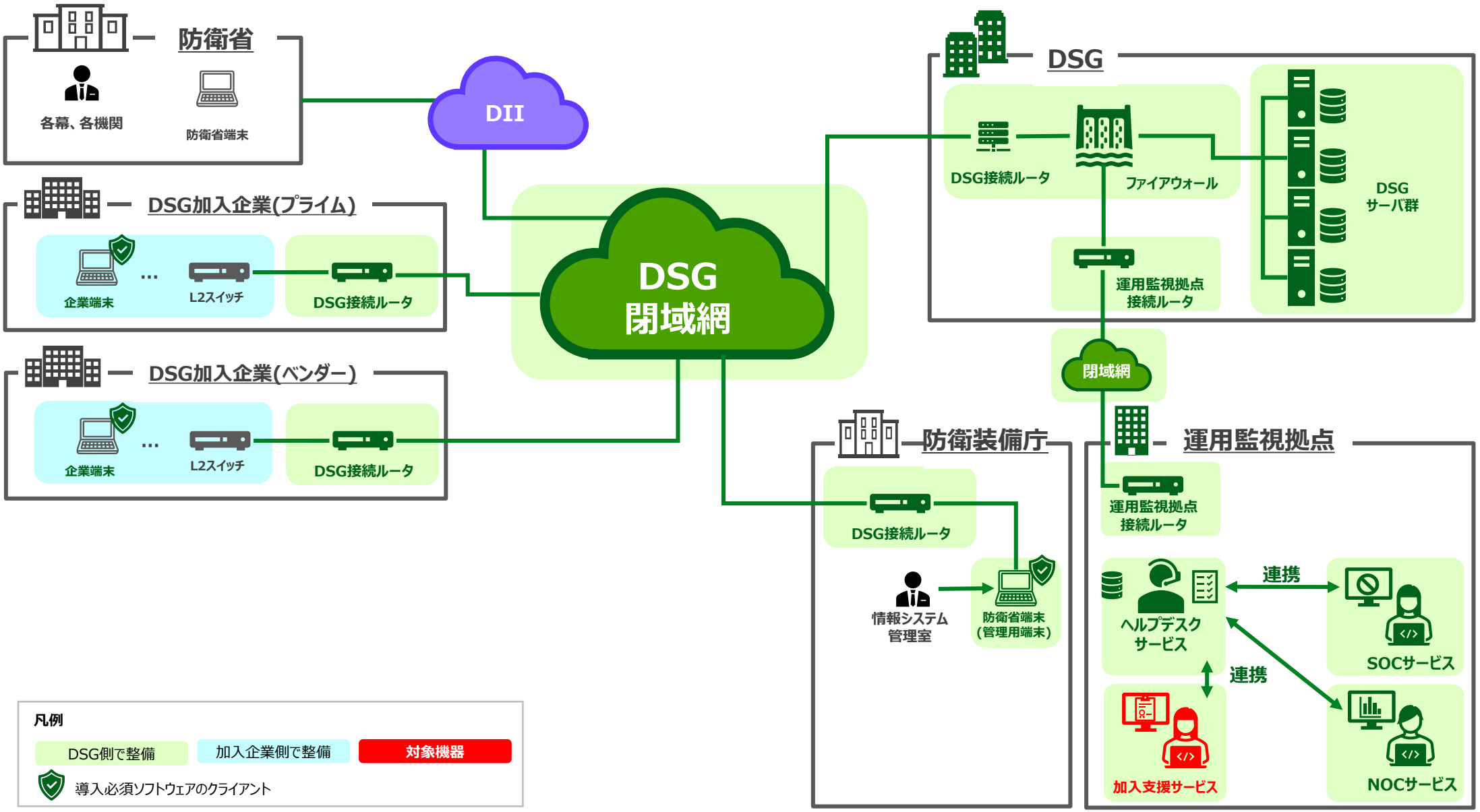
- **サイトコンテンツの作成を実施します。**
- **加入申請時に申請のあったアカウントの登録、停止及び削除を実施します。**
- **DSGに加入するためのセットアップ手順書、利用マニュアル及びインストーラーを配布します。**
- **ネットワークの開通を支援します。**

本サービスでは、以下の**構成情報**及び**手順書**を提供します。

- **ハードウェア一覧**
- **ソフトウェア一覧**
- **ホワイトリスト**
- **インストール手順書**
- **操作手順書**

4.2 各サービスの説明
4.2.12 加入支援サービス

加入支援サービスの概要図は以下の通りです。



4.2 各サービスの説明
4.2.12 加入支援サービス

加入支援サービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

本紙	内容
なし	
(以下空白)	

付紙	内容
第2-1-(2)-エ	第４第２項第１号に規定する操作手順書
第4-2-(1) 第4-2-(2)	保護システムの操作手順書の策定
第5-2-(1)-オ-(ウ)	アカウント失効日時等の記録を行うこと
第6-1-(3)-イ	パスワードによる認証の実施
(以下空白)	

4.2 各サービスの説明
4.2.13 回線・ルータ利用サービス

回線・ルータ利用サービスでは以下をサービスとして提供します。

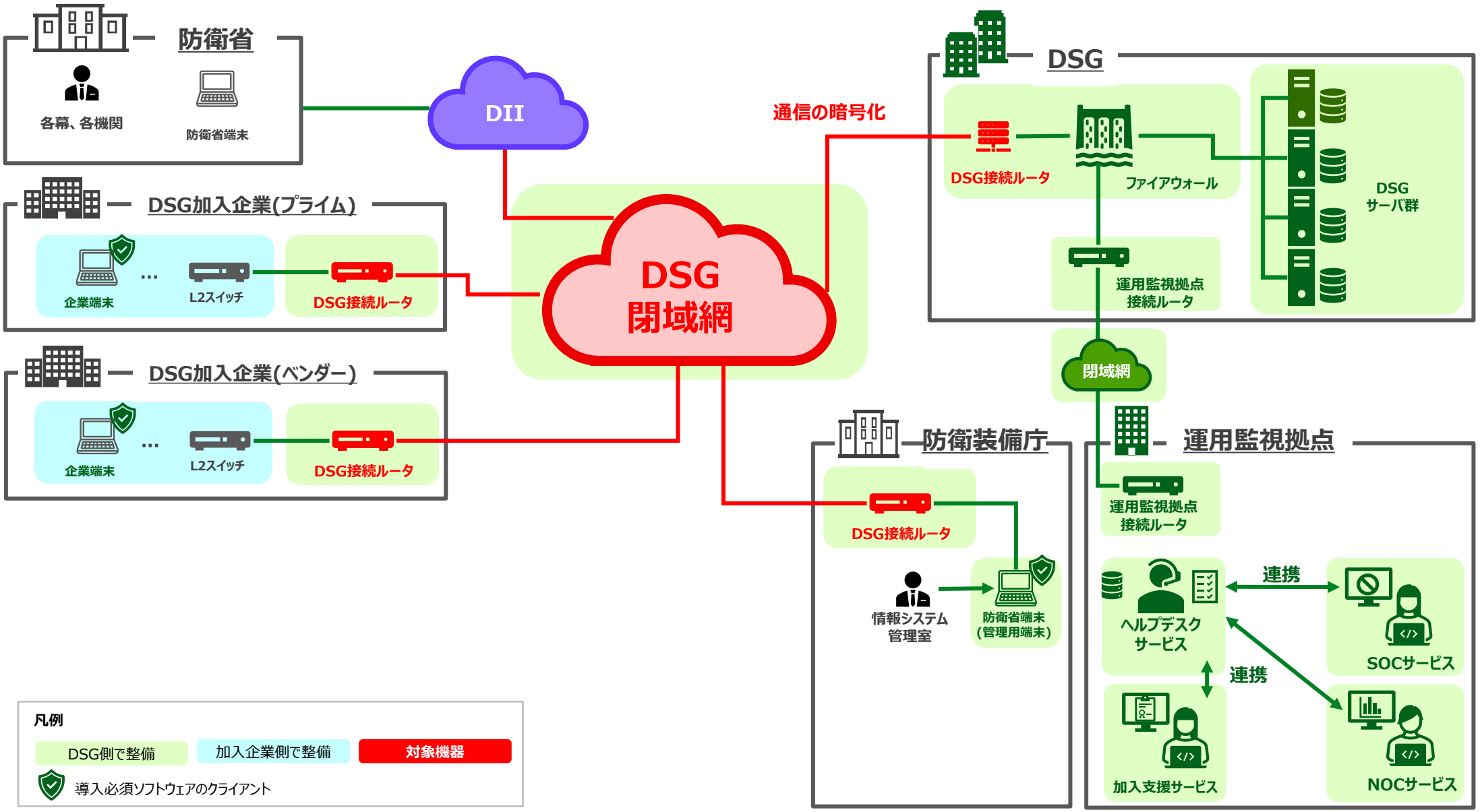
加入企業拠点とDSGを閉域網の専用回線で接続するとともに、仮想的なトンネルで隔絶し、通信を暗号化することでクローズドなネットワークを提供します。また、許可された企業端末以外の端末の接続を拒否します。

- **DSGの利用者から提出される申請書に基づき、以下を実施します。**
  ーDSG回線の敷設/撤去、DSG接続ルータの設置及び撤去
  ー企業端末の通信許可登録及び削除
- **企業端末からDSGへのアクセスサービスを提供します。**
  ーアクセス経路制御
- **DSG側のDSG接続ルータを通過した通信をログに記録します。**

本サービスで提供可能なログは以下の通りです。
- **ネットワークログ**

4.2 各サービスの説明
4.2.13 回線・ルータ利用サービス

回線・ルータ利用サービスの概要図は以下の通りです。



4.2 各サービスの説明
4.2.13 回線・ルータ利用サービス

回線・ルータ利用サービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

本紙	内容
なし	
(以下空白)	

付紙	内容
第4-1	保護システムの領域の確定
第6-1-(2)-ウ	認証の実施
第7-2-(1)-イ	保護すべき情報の通信制限
(以下空白)	

4.2 各サービスの説明
4.2.14 仮想化基盤サービス

仮想化基盤サービスでは以下をサービスとして提供します。

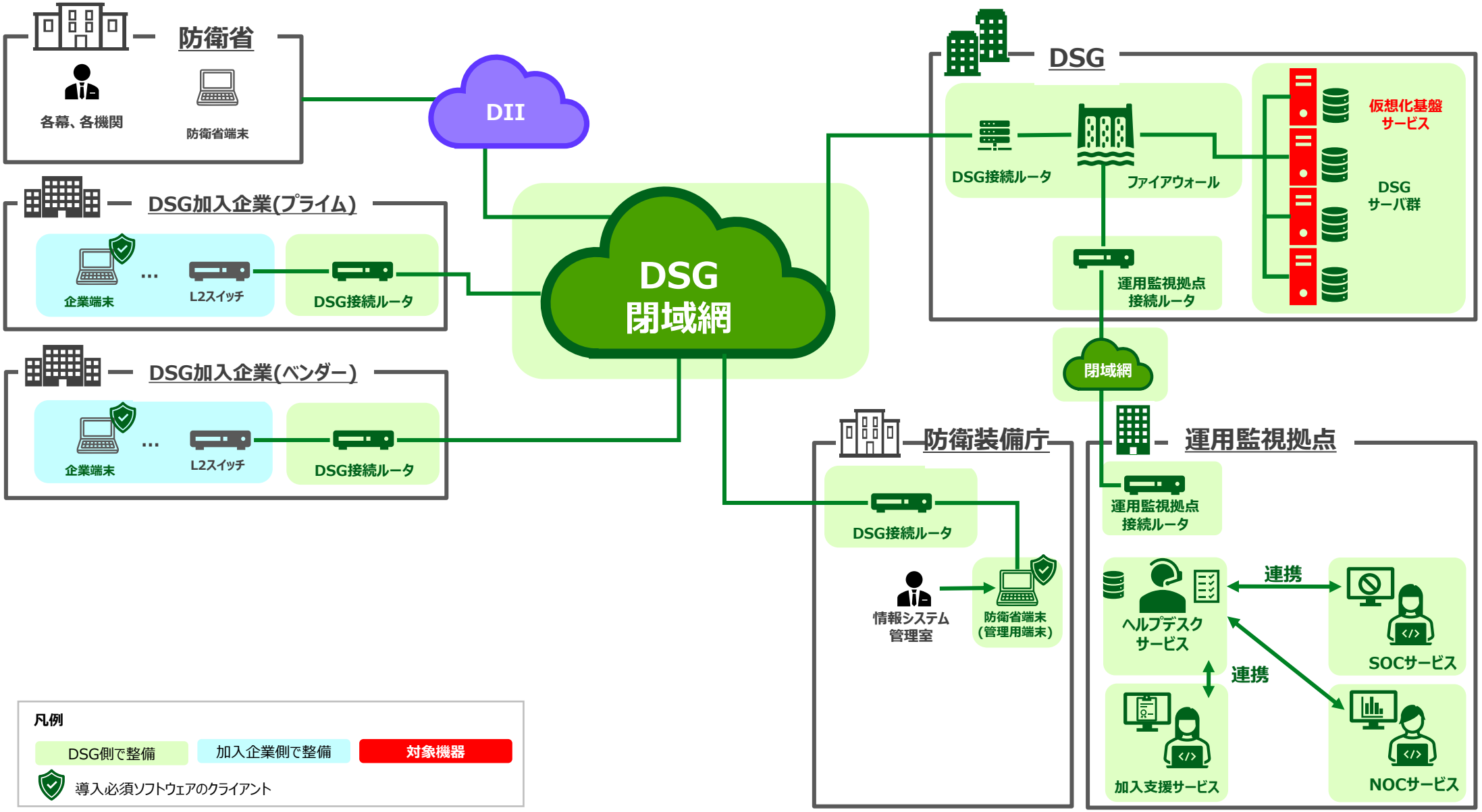
DSGサービスの基盤となる各仮想マシンを稼働させることが可能です。

・DSGで提供しているサービスを実現するためのサーバの仮想化を実現し、障害時等の迅速な復旧を実施します。
・仮想化基盤の性能情報を収集、監視を実施します。

本サービスで提供可能なログはありません。

4.2 各サービスの説明
4.2.14 仮想化基盤サービス

仮想化基盤サービスの概要図は以下の通りです。



4.2 各サービスの説明
4.2.14 仮想化基盤サービス

仮想化基盤サービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

本紙	内容
なし	
(以下空白)	

付紙	内容
なし	
(以下空白)	

4.2 各サービスの説明
4.2.15 ストレージ利用サービス

ストレージ利用サービスでは以下をサービスとして提供します。

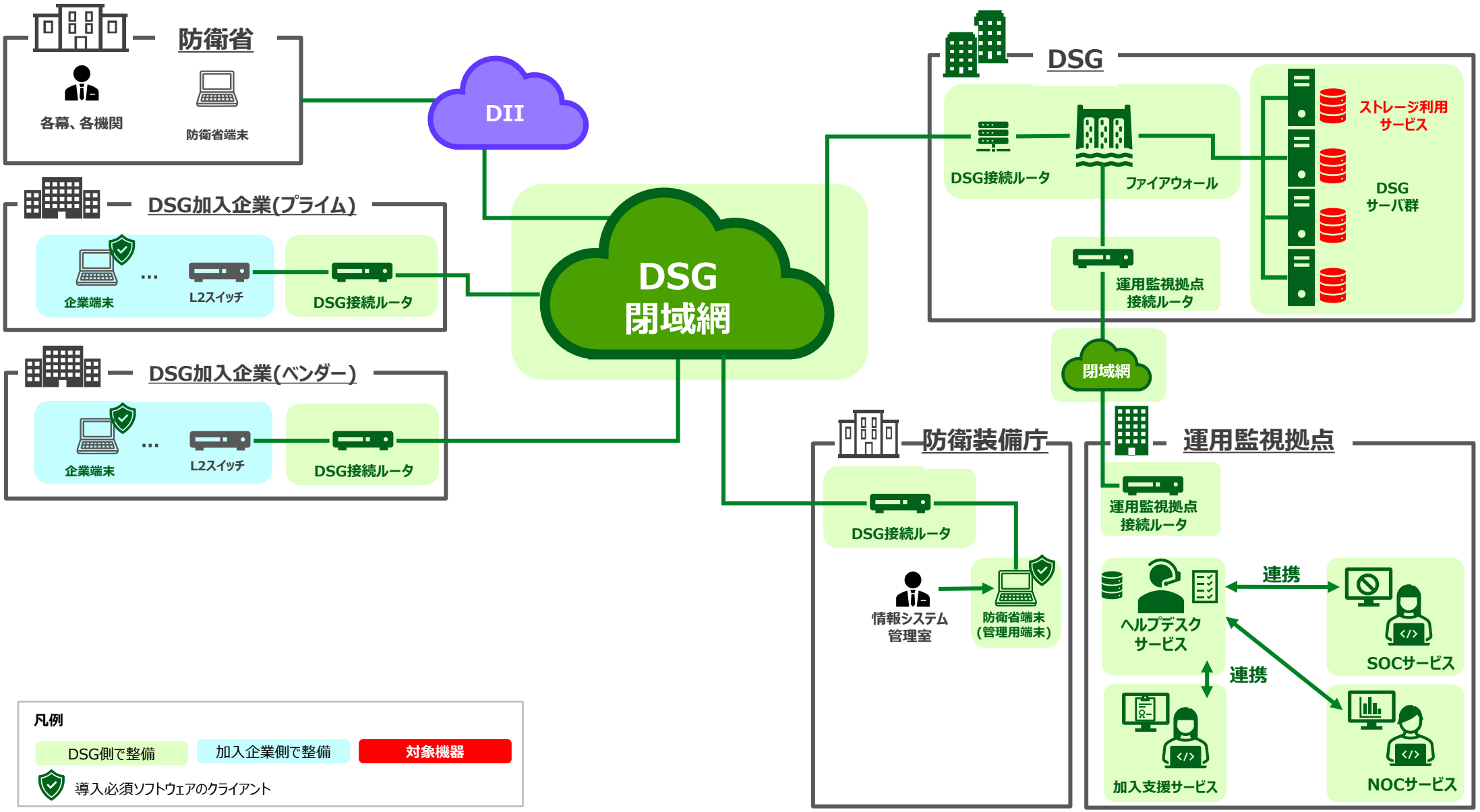
仮想マシン、保護情報、バックアップ及び運用関連情報の保存先の領域を提供するとともに、データの暗号化を行い、情報を保護します。

・利用者がアップロードしたデータの保存を実施します。
・保存されたデータの暗号化を行います。

本サービスで提供可能なログはありません。

4.2 各サービスの説明
4.2.15 ストレージ利用サービス

ストレージ利用サービスの概要図は以下の通りです。



4.2 各サービスの説明
4.2.15 ストレージ利用サービス

ストレージ利用サービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

本紙	内容
なし	
(以下空白)	

付紙	内容
第4-3-(1)-ア	暗号化
第4-3-(2)	暗号化の方法
第4-3-(3)	暗号鍵の管理
(以下空白)	

4.2 各サービスの説明
4.2.16 バックアップサービス

バックアップサービスでは以下をサービスとして提供します。

各サーバのデータを日々バックアップします。
不測の事態等でサーバに故障が発生した場合はバックアップからデータの復元を実施します。

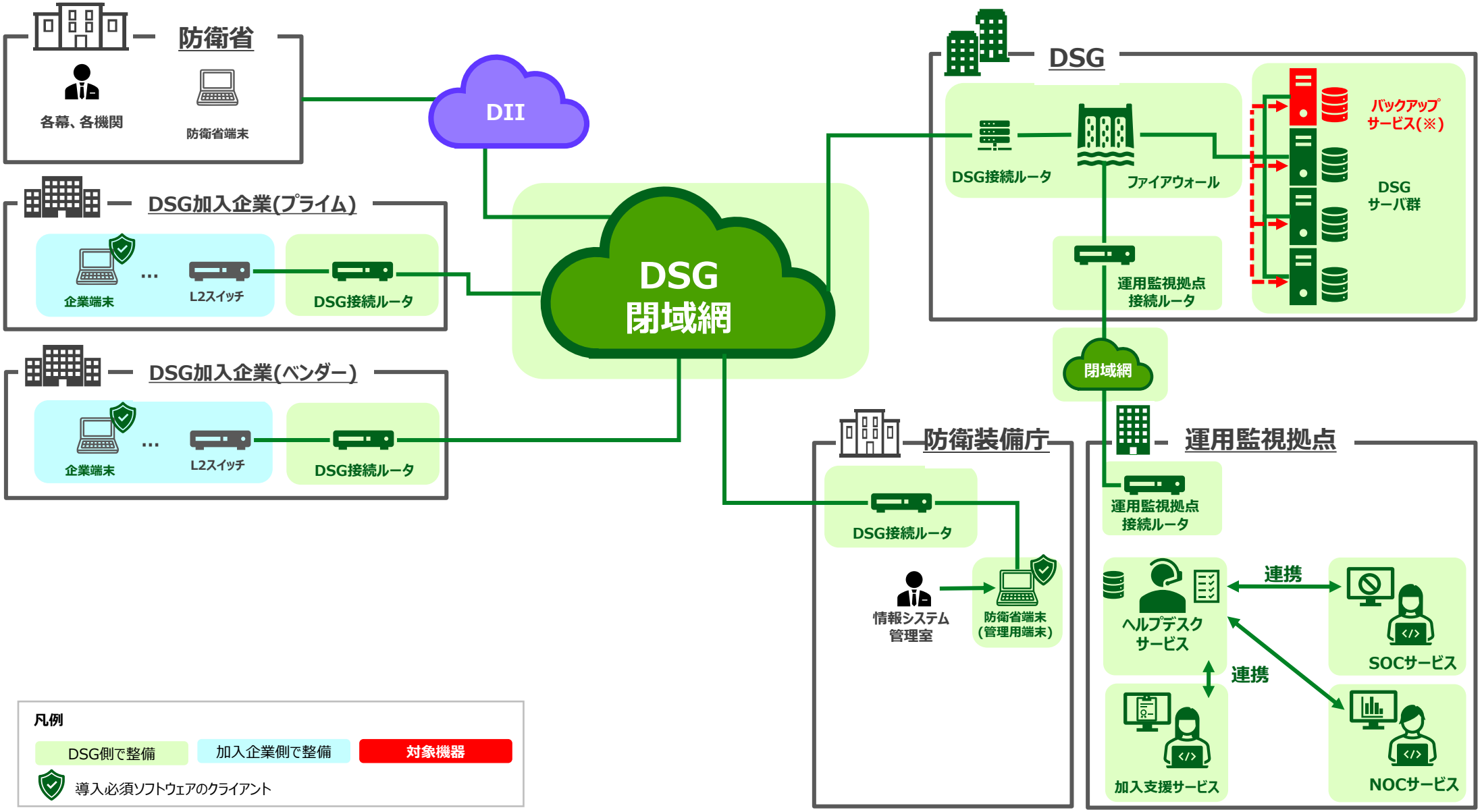
・DSGのサーバに保存されたデータを自動的にバックアップし、定められた期間データの保管を実施します。

※本サービスは防衛省端末及び企業端末内のデータのバックアップを取得するものではありません。

本サービスで提供可能なログはありません。

4.2 各サービスの説明
4.2.16 バックアップサービス

バックアップサービスの概要図は以下の通りです。



※本サービスは防衛省端末及び企業端末のバックアップを取得するものではありません。

4.2 各サービスの説明
4.2.16 バックアップサービス

バックアップサービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

本紙	内容
第6-2-(3)	目録等の保管
(以下空白)	

付紙	内容
第8-4-(2)	システム監視により取得した情報の利用及び保管
第9-2-(2) 第9-2-(3)	システムログの管理
第11-1 第11-2 第11-3 第11-4	バックアップ
(以下空白)	

4.2 各サービスの説明
4.2.17 セキュリティパッチ配信サービス

セキュリティパッチ配信サービスでは以下をサービスとして提供します。

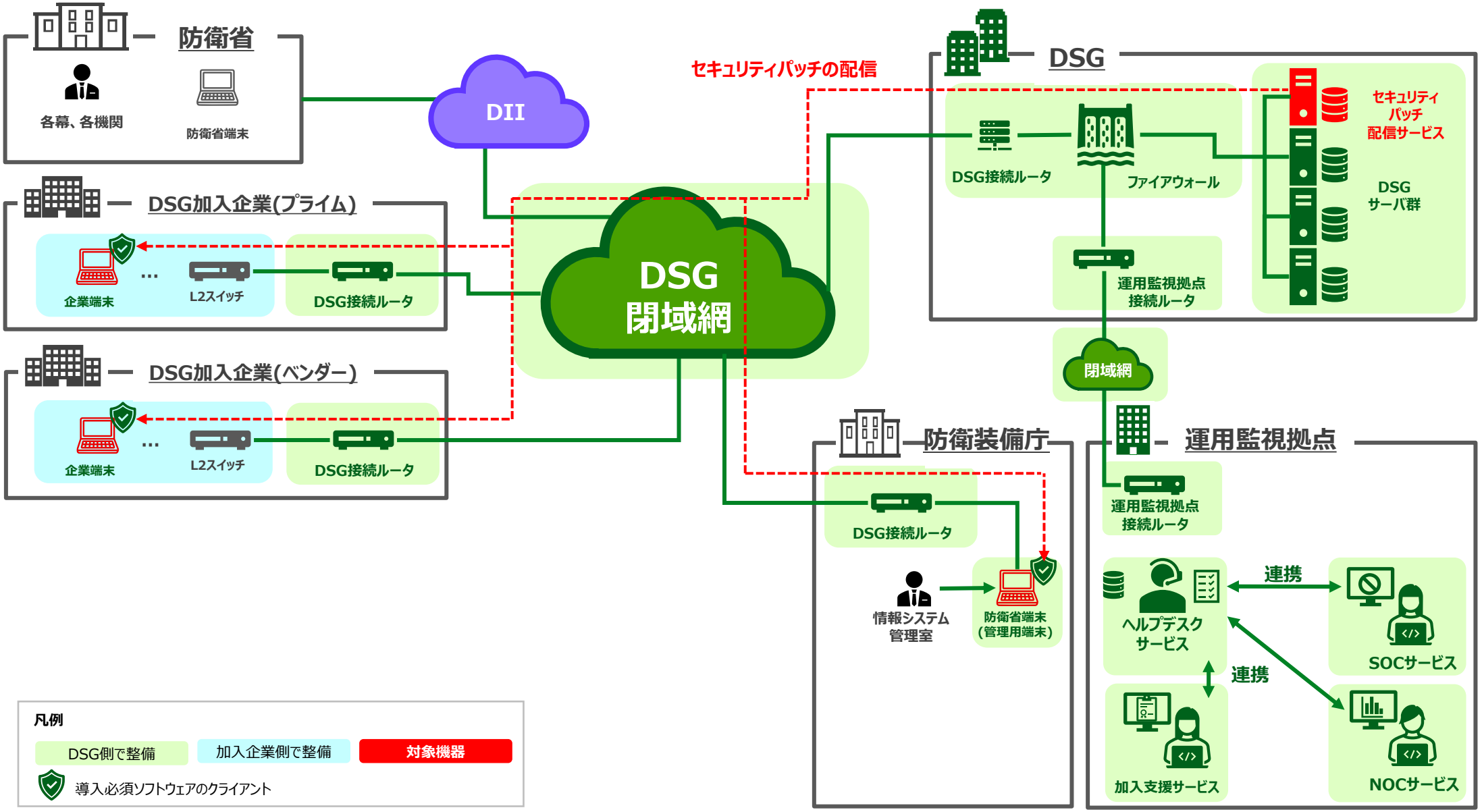
製品ベンダーからOS等のセキュリティパッチを取得し、企業端末に提供します。

- **企業端末へセキュリティパッチを配信します。**

本サービスで提供可能なログはありません。

4.2 各サービスの説明
4.2.17 セキュリティパッチ配信サービス

セキュリティパッチ配信サービスの概要図は以下の通りです。



4.2 各サービスの説明
4.2.17 セキュリティパッチ配信サービス

セキュリティパッチ配信サービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

本紙	内容
なし	
(以下空白)	

付紙	内容
第4-4-(1)-イ	ソフトウェアのインストール及びアップデートの制限等
(以下空白)	

4.2 各サービスの説明
4.2.18 DNSサービス

DNSサービスでは以下をサービスとして提供します。

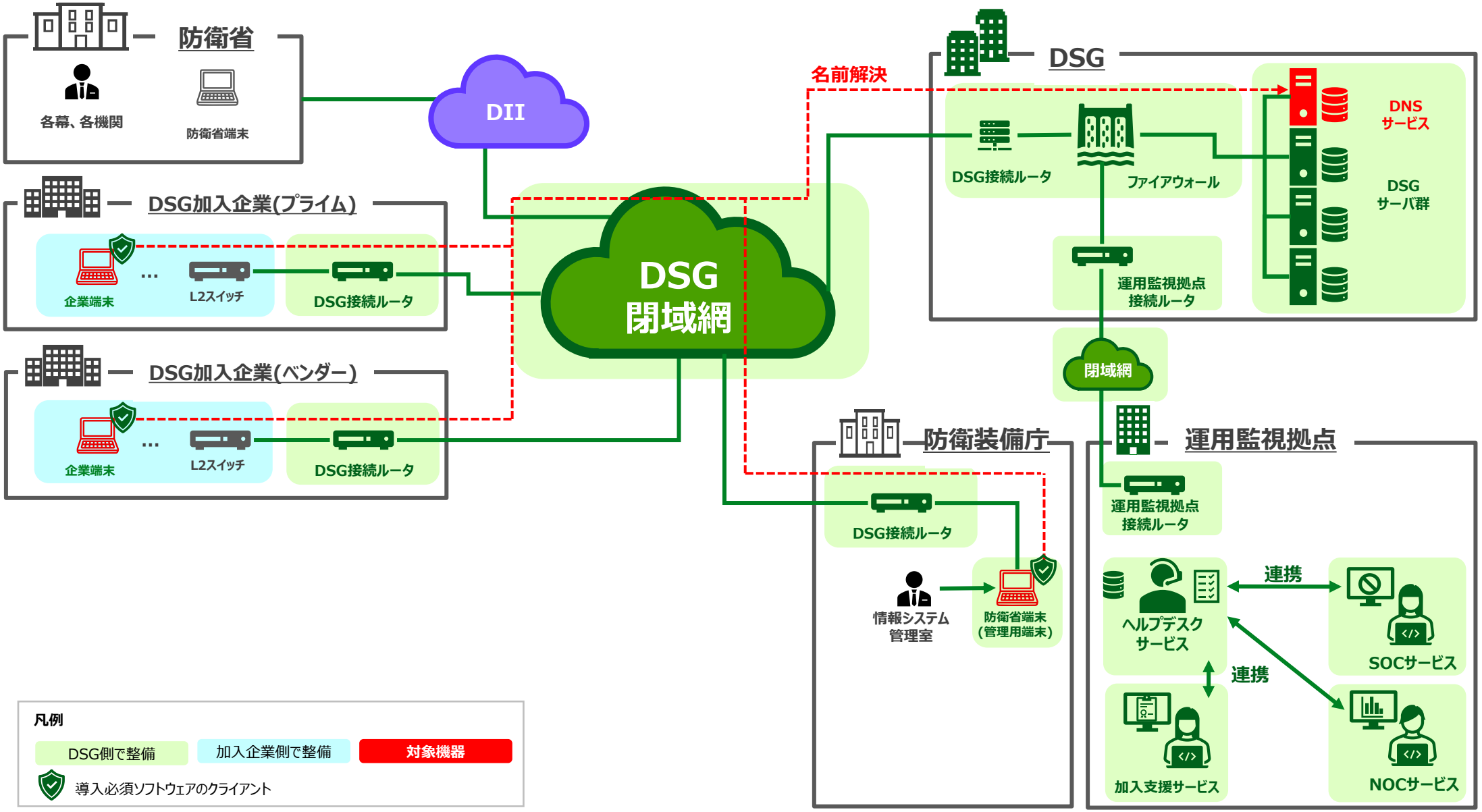
企業端末向けにポータルサイト、保護情報共有サービスのアクセス先となるドメイン名の名前解決を実施します。

- **企業端末からDSGにアクセスする際にドメイン名をIPアドレスに変換し、コンテンツに正常にアクセスする環境を提供します。**

本サービスで提供可能なログはありません。

4.2 各サービスの説明
4.2.18 DNSサービス

DNSサービスの概要図は以下の通りです。



4.2 各サービスの説明
4.2.18 DNSサービス

DNSサービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

本紙	内容
なし	
(以下空白)	

付紙	内容
なし	
(以下空白)	

4.2 各サービスの説明
4.2.19 NTPサービス

NTPサービスでは以下をサービスとして提供します。

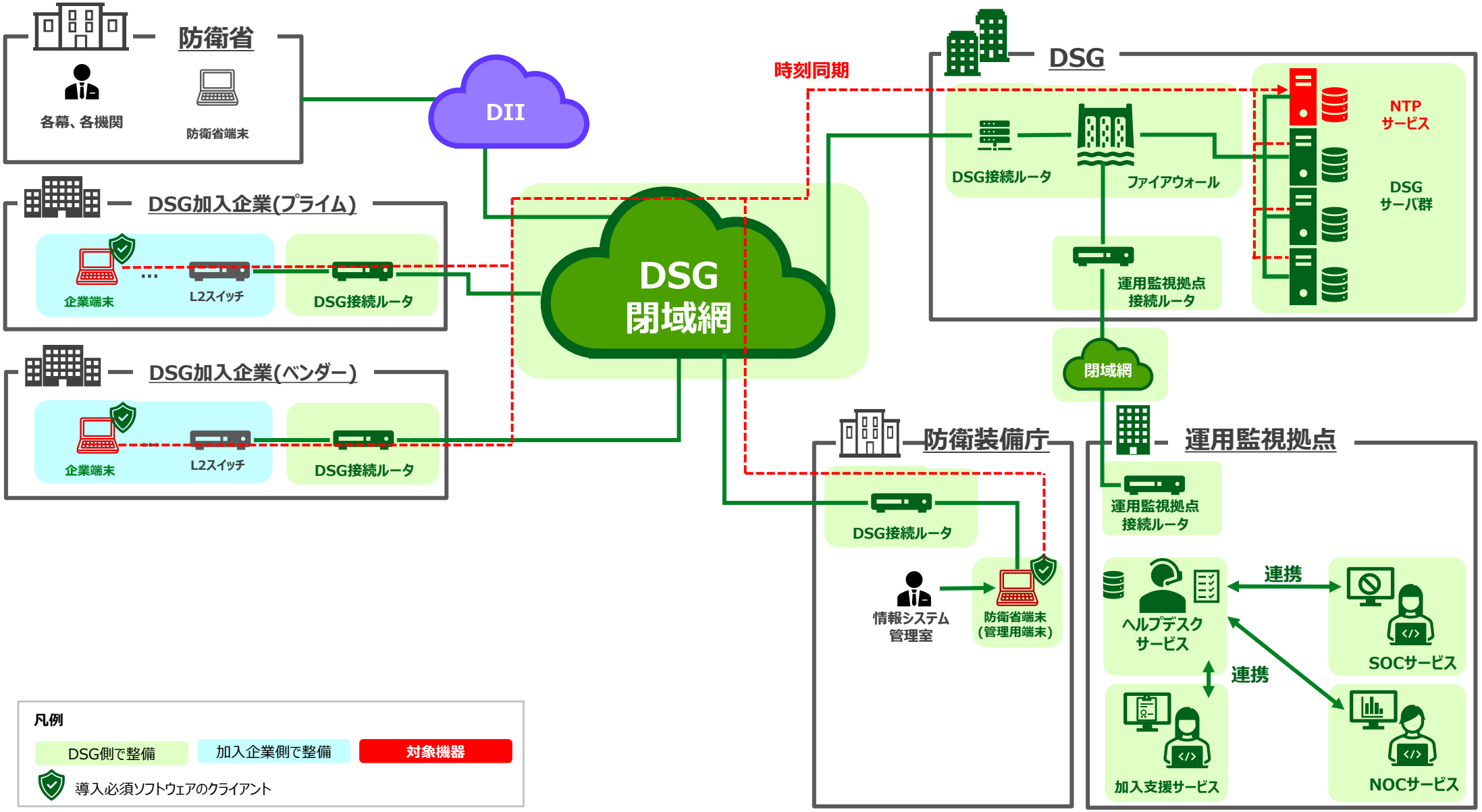
外部の信頼された機関から取得した標準時刻を企業端末に提供します。

- **DSGに接続されている全ての機器の時刻を同期し、ログに記録されるタイムスタンプの整合性を担保するため各加入企業の端末に対して正確な時刻で同期を実施します。**

本サービスで提供可能なログはありません。

4.2 各サービスの説明
4.2.19 NTPサービス

NTPサービスの概要図は以下の通りです。



4.2 各サービスの説明
4.2.19 NTPサービス

NTPサービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

本紙	内容
なし	
(以下空白)	

付紙	内容
第9-3-(1) 第9-3-(2) 第9-3-(3)	システムログに付与するタイムスタンプ
(以下空白)	

4.2 各サービスの説明
4.2.20 ログ分析サービス

ログ分析サービスでは以下をサービスとして提供します。

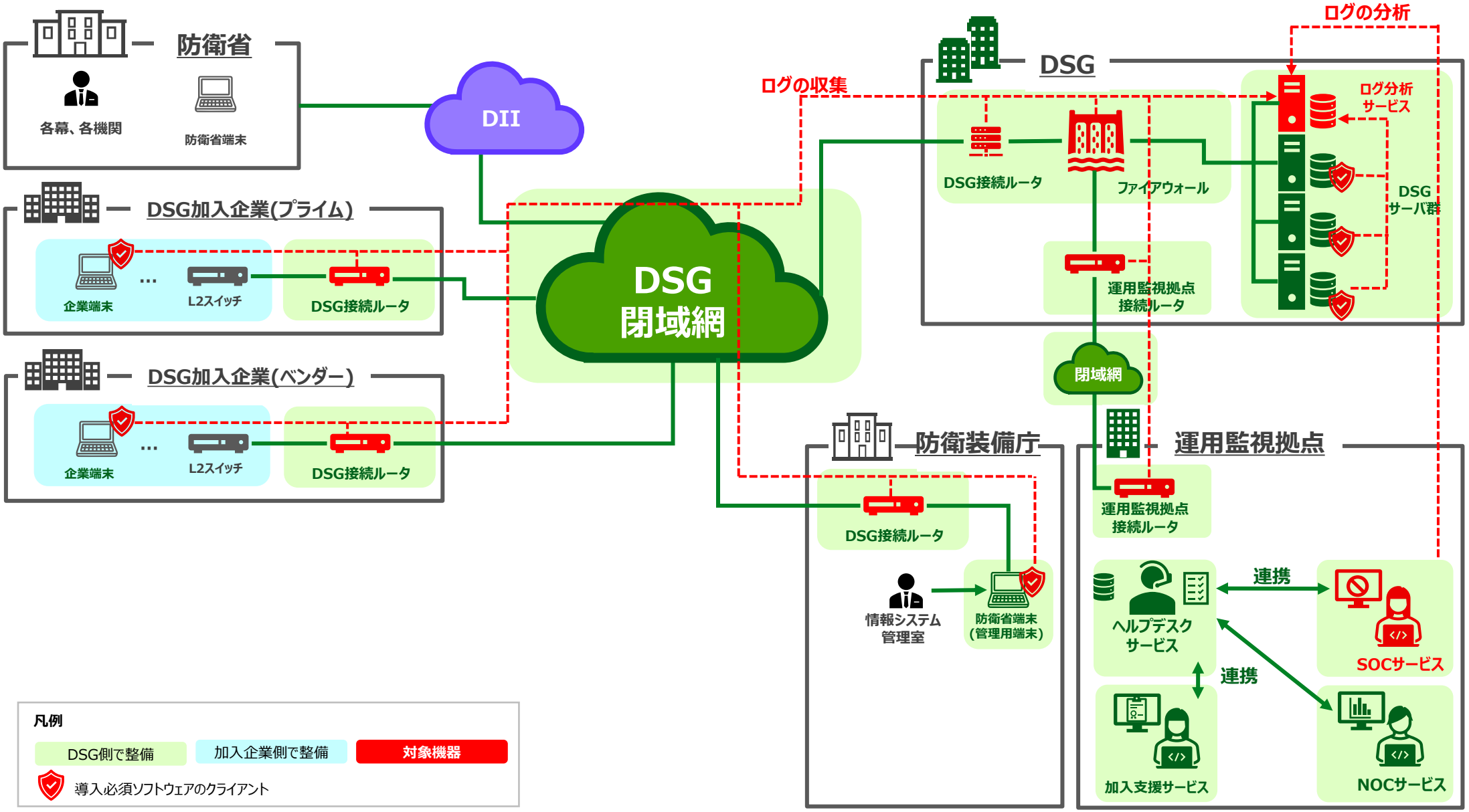
各種サービスより取得したログの収集及び相関分析を行い、セキュリティリスクの検出を実施します。

- **サーバやネットワーク機器、セキュリティ機器からログ収集を実施します。**
- **SOCサービスと連携してログの相関分析を行い、セキュリティリスクの検出を実施します。**

本サービスでは、**ログ分析結果**を提供します。

4.2 各サービスの説明
4.2.20 ログ分析サービス

ログ分析サービスの概要図は以下の通りです。



4.2 各サービスの説明
4.2.20 ログ分析サービス

ログ分析サービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

本紙	内容
なし	
(以下空白)	

付紙	内容
なし	
(以下空白)	

4.2 各サービスの説明
4.2.21 情報提供サービス

情報提供サービスでは以下をサービスとして提供します。

加入企業からの要請により、各種情報(構成情報、手順書、ログ情報、監査情報及び分析結果)を提供します。

- **提供する情報を以下に示します。**

(1/2)

情報			内容
1 構成情報			
	1-1	ハードウェア一覧	DSGから提供するハードウェアの情報(メーカー及び型番等)
	1-2	ソフトウェア一覧	DSGから提供するCOTSの情報(種別、バージョン及び対応OS等)
	1-3	ホワイトリスト	DSGの各サービスを利用するにあたりインストールが許可されたソフトウェアの情報
	1-4	ベースライン構成	DSGから提供するハードウェア及びCOTSの構成設定情報
	1-5	ネットワーク構成図	DSGネットワーク～加入企業に設置するDSG接続ルータまでのネットワーク構成図
2 手順書			
	2-1	インストール手順書	DSGから提供するCOTSのインストール手順
	2-2	操作手順書	DSGから提供するCOTSの操作手順

4.2 各サービスの説明
4.2.21 情報提供サービス

・ **提供する情報を以下に示します。「3 ログ情報」については、「別紙 提供ログ一覧」を参照ください。** (2/2)

情報		内容
3 ログ情報		
	3-1 端末操作ログ	構成管理サービスで取得した企業端末の操作ログ
	3-2 認証ログ(多要素認証)	多要素認証サービスで取得したDSG利用者の認証ログ
	3-3 アカウント管理操作ログ	アカウント管理サービスで取得した登録、更新及び削除等の操作ログ
	3-4 ポータルサイトアクセスログ	保護情報共有サービスで取得したポータルサイトのアクセスログ
	3-5 マルウェア検知ログ	マルウェア対策サービスで取得したログ(検知したファイル名等の情報)
	3-6 ファイアウォールログ	ファイアウォールサービスで取得した通信ログ(ブロック又は許可等の情報)
	3-7 脅威検知ログ	脅威検知サービスで取得したログ(検知したプログラムの挙動等の情報)
	3-8 ネットワークログ	DSGを構成するネットワーク機器(LAN機器、WAN機器及びロードバランサ)から出力されるログ
	3-9 監査ログ(カスタムレポート)	保護情報共有サービスで取得した保護情報共有サイトの監査ログ
4 監査情報		
	4-1 脆弱性監査結果	脆弱性監査サービスで監査した結果
5 分析結果		
	5-1 ログ分析結果	ログ分析サービスで収集、分析した結果又はSOCサービスで分析した結果

4.2 各サービスの説明
4.2.21 情報提供サービス

情報提供サービスが準じる防衛産業サイバーセキュリティ基準は以下の通りです。

本紙	内容
第6-2-(1)	目録の作成
第6-2-(2)-ア-(ア) 第6-2-(2)-ア-(イ) 第6-2-(2)-ア-(ウ) 第6-2-(2)-イ	目録の更新
(以下空白)	

付紙	内容
なし	
(以下空白)	

別紙 提供ログ一覧

DSGでは以下のログを取得しており、要求に応じて提供します。

(1/2)

#	ログの種類			取得内容
1	端末操作ログ	操作ログ	起動・終了ログ	ユーザ毎のログオン / ログオフや電源ON / OFF、操作開始 / 終了時刻。
2			クライアント操作ログ	アクティブ状態のウィンドウタイトルと稼働時間、業務で使用するアプリケーション。
3			ファイルアクセスログ	ローカルの共有フォルダへのアクセス、アクセスユーザ、操作種別。
4			ファイル操作ログ	ファイルの作成、上書き保存、削除、コピー、名前変更、ライティングソフトウェアを用いたCD-R/DVD-Rへの書き込み等、ファイルやフォルダ操作の履歴(MTP/PTP接続デバイスでファイルコピーしたログも取得)。
5			クリップボードログ	コピー＆ペーストしたときのクリップボードの内容。
6			プリントログ	印刷したドキュメントのプリンター名、プリントタイトル、印刷枚数、印刷対象のファイルパス、IPアドレス、ポート名。
7			Webアクセスログ	Mozilla Firefox、Google Chrome、Microsoft Edge(Chromium版)でアクセスしたURL、ウィンドウタイトル、稼働時間、Gmail送信ログ、WindowsアプリケーションやWebシステムへのログイン状況。
8			ドライブ追加・削除ログ	USBデバイス等のドライブの追加、削除及びドライブ種別等を記録。
9			フォルダ共有ログ	共有フォルダの作成、削除、共有元アドレス、共有名。
10		アプリケーションログ		ユーザが利用したアプリケーションの実行ファイル名や稼働時間、実行コマンド。
11		通信デバイスログ		ネットワークカードやBluetooth等の通信デバイスによる接続に関するログ。
12		システムログ		アラート設定変更を行った部署、変更内容、ログ未回収期間に達したクライアントPCのログ、リモート操作のログ(PC操作時、管理機操作時両方)。

別紙 提供ログ一覧

DSGでは以下のログを取得しており、要求に応じて提供します。

(2/2)

#	ログの種類		取得内容
13	端末操作ログ	IT資産情報	コンピューター名、ホスト名、ドメイン名(ワークグループ名) 、所有ADユーザ、死活監視状態、システム製造元、システムモデル、システムシリアル、BIOSバージョン、OSバージョン、OSバージョン(ビルド番号)、Microsoft Edgeバージョン、Firefoxバージョン、Google Chromeバージョン、Safariバージョン、IEバージョン、MACアドレス、IPアドレス、サブネットマスク、デフォルトゲートウェイ、DNSサーバー、CPU数、CPUコア数、CPUタイプ、メモリサイズ、ドライブ容量。
14	認証ログ(多要素認証)		イベント発生日時、コンピューター名、ユーザID、Windowsアカウント名、イベント内容、補足情報。
15	アカウント管理操作ログ		ログの名前(System、Application等)、ソース(アプリケーション名、プロセス名)、日付、イベントID、タスクのカテゴリ、ログのレベル(情報、警告、障害)、キーワード、ユーザ名、コンピューター名、イベントの詳細、共有名。
16	ポータルサイトアクセスログ		アクセス日時、アクセス元IPアドレス、URL、メソッド(GET等)、User-Agent(ブラウザ情報)、ステータスコード(200、404等)。
17	マルウェア検知ログ		検知した装置のIPアドレス、検知時間、検知したファイル等の情報。
18	ファイアウォールログ		送信元IPアドレス、送信先IPアドレス、ブロック又は許可情報等の情報。
19	脅威検知ログ		レジストリ情報(作成、削除、変更)、ネットワーク接続、デジタル署名情報、プロセス名、プロセスの開始 (又は終了) 、プロセスが別のプロセスへのハンドルを開こうとした情報、プロセスが別のプロセスにスレッドを挿入しようとした情報、プロセスを強制終了した情報、プロセスの実行がブロックされた情報、改ざんされた情報。
20	ネットワークログ	ネットワークログ (LAN機器)	時刻情報、ホスト名、ファシリティ情報、ログイン情報(モード推移等)。
21		ネットワークログ (WAN機器)	時刻情報、ホスト名、ファシリティ情報、ログイン情報(モード推移等)。
22		ネットワークログ (ロードバランサ)	時刻情報、ホスト名、ユーザ情報、送信元アドレス、プロトコル情報。
23	監査ログ・カスタムレポート		サイト ID、アイテム ID、アイテムの種類、ユーザ ID、ドキュメントの場所、発生時間 (GMT)、イベント、カスタム イベント名、イベント ソース、ソース名、イベント データ、アプリ ID。

5. サービス提供までの流れ

5. サービス提供までの流れ

1. サービス利用条件

加入要領及び利用要領に準拠します。

① サービス利用条件１　加入要件(加入企業向け)

『防衛セキュリティゲートウェイサービス加入要領(加入企業向け)』 より抜粋

#	要件	細部
1	実績等	加入希望企業において、防衛セキュリティゲートウェイサービスの利用が可能な契約の履行に従事することが十分に見込まれること。
2	設備	加入希望企業において、防衛セキュリティゲートウェイサービスの利用区画(以下「拠点」という。)として、防衛産業サイバーセキュリティ基準第８に準拠した取扱施設等を整備していること。(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第９条第５項に基づく適用の特例が認められた場合を除く。)
3	機器	⑴ 防衛装備庁が指定(防衛装備庁ホームページに掲載)する仕様を満たす所要の機器を用意し、前号に示す拠点内に設置できること。 ⑵ 用意する機器は、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。)が潜在することを知り又は知り得べきソースコード、プログラム、電子部品、機器等の埋込み又は組込みその他官の意図せざる変更が行われていないものに該当しないよう、配慮できること。
4	拠点地域	拠点は、日本国内に所在するものであること。

② サービス利用条件２　利用要件(加入企業向け)

『防衛セキュリティゲートウェイサービス利用要領(加入企業の利用者向け)』 より抜粋

#	要件
1	防衛セキュリティゲートウェイサービスへの加入が完了していること。(加入プロセスにおいて、最終現地確認後に情報システム管理室から発効される「加入完了通知書」を受領していること)
2	中央調達か地方調達かに関わらず、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が付帯された契約又は情報セキュリティ通達第８項の各号に該当する調達であって、「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」が付帯されていない契約の締結に伴い、当該契約の履行に従事することが決定していること。
3	利用者及び防衛省職員である利用者の双方が防衛セキュリティゲートウェイサービスを利用することについて合意が得られていること。

5. サービス提供までの流れ

③ サービス利用条件３　利用要件(防衛省職員向け)

『防衛セキュリティゲートウェイサービス利用要領(防衛省職員である利用者向け)』 より抜粋

#	要件
1	防衛情報通信基盤(防衛情報通信基盤の業務実施に関する訓令(平成１５年防衛庁訓令第１９号)第２条第１項に規定する防衛情報通信基盤をいう。)に接続したオープン系加入システムの電子計算機端末を利用できること。
2	中央調達か地方調達かに関わらず、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が付帯された契約又は情報セキュリティ通達第８項の各号に該当する調達であって、「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」が付帯されていない契約が締結されていること。
3	利用者及び契約相手方企業等の利用者の双方が防衛セキュリティゲートウェイサービスを利用することについて合意が得られていること。

5. サービス提供までの流れ

2. サービス利用に向けたステップ

DSG利用開始に向けた大きな作業の流れは以下になります。
具体的な手続きは『防衛セキュリティゲートウェイサービス加入要領（加入企業向け）』および『防衛セキュリティゲートウェイサービス利用要領（加入企業の利用者向け、防衛省職員である利用者向け）』をご参照ください。

1	2	3	4	5
事前準備	**加入申請**	**環境整備**	**利用申請**	**利用開始**
・取扱施設の準備 ・機器等の確認、準備 ・利用開始希望日の検討	・加入申請書の提出 ・官の事前現地確認 ・レイアウト図、ラック図、企業端末情報の提出	・回線現地調査 ・ 入線工事/終端装置（ONU）設置 ・通信ルータ設置 ・企業端末セットアップ ・保護システム管理者静脈登録 ・保護システム管理者DSG接続確認 ・官の最終現地確認	・該当契約の調達要求元部署と事前調整 ・利用者情報の収集（下請企業分含む） ・利用申請書の提出	・パラメータシートの受領 ・利用者の静脈登録 ・事業サイトの接続確認

「加入」
（加入企業のみ）

「利用」
（加入企業及び職員の利用者）

6. お問い合わせ先とサポート

6.1 お問い合わせ先

FUJITSU

1. お問い合わせ先

お問い合わせについては以下の各窓口までご連絡ください。

防衛セキュリティゲートウェイ全般に関するお問い合わせ	**防衛装備庁長官官房総務官付情報システム管理室** dsg-atla@atla.mod.go.jp
防衛産業サイバーセキュリティ基準に関するお問い合わせ	**防衛装備庁装備政策部装備保全管理課** industrial-cybersecurity-office@atla.mod.go.jp
防衛生産基盤強化法に関するお問い合わせ	**防衛装備庁装備政策部装備政策課** kibankyoukahou@atla.mod.go.jp
防衛セキュリティゲートウェイの加入手続き及び本資料に関するお問い合わせ	**DSGサポート窓口** contact-dsgsupport@cs.jp.fujitsu.com
防衛セキュリティゲートウェイへ加入済み企業のお問い合わせ	次ページに詳細を記載

防衛装備庁ホームページに、防衛セキュリティゲートウェイの各種資料等を掲載しております。
https://www.mod.go.jp/atla/dsg.html

6.2 サポート

2. サポート

DSG加入企業の利用者向けのサポートについては以下の通りです。

■ 各種ドキュメントについて

各種ドキュメントは防衛セキュリティゲートウェイポータルサイト内マニュアルサイトより参照ください。

■ 利用者向けサポートについて

詳細は防衛セキュリティゲートウェイ利用マニュアル(管理者編/利用者編を参照ください)

- 標準受付窓口：防衛セキュリティゲートウェイポータルサイト内お問い合わせフォームより受付
- 防衛セキュリティゲートウェイポータルサイト利用不可時連絡先(平日9時~18時)：電話受付
- 緊急連絡先：防衛装備庁　情報システム管理室：dsg-atla@atla.mod.go.jp

7. 用語集

7. 用語集

項番	用語	定義
1	防衛セキュリティゲートウェイ (DSG:Defense Security Gateway)	防衛装備品の調達のうち、情報セキュリティ特約条項を付帯した契約の中で取り扱う保護すべき情報を、防衛省と防衛関連企業の間で、電子データの形で安全かつ効率的に共有することを可能とする通信基盤をいう。
2	防衛セキュリティゲートウェイサービス	サービス提供事業者が防衛セキュリティゲートウェイを用いて提供するサービスをいう。
3	防衛産業サイバーセキュリティ基準	「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の確保に関する特約条項」第２条第１項で引用する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をいう。
4	情報セキュリティ特約条項	「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」をいう。
5	保護すべき情報	「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。)」第２項第１号に規定する保護すべき情報をいう。
6	保護システム管理者	防衛産業サイバーセキュリティ基準第５第２項第２号イ(ア)に規定する保護システム管理者をいう。
7	サービス提供事業者	防衛装備庁との契約に基づき、防衛セキュリティゲートウェイサービスを提供する事業者をいう。

7. 用語集

項番	用語	定義
8	取扱施設等	防衛産業サイバーセキュリティ基準第２第２５号に規定する取扱施設等をいう。
9	導入必須ソフトウェア	加入企業において、防衛セキュリティゲートウェイサービスを利用するために企業端末に導入しなければならないソフトウェア群をいう。
10	プライム	保護すべき情報を取り扱う契約において、防衛省、自衛隊との直接の契約の相手方をいう。
11	ベンダー	プライムから、保護すべき情報の取り扱いを伴う契約の履行の一部を受託した企業をいう。

FUJITSU