ATLA
Acquisition,Technology & Logistics Agency

# 防衛セキュリティゲートウェイの利用について

## （ Defense Security Gateway：DSG ）

令和５年１２月８日

防衛装備庁長官官房総務官付
情報システム管理室

**«本日の時程»**

令和５年１２月８日（金）１３：００～１４：３０
■ １３：００～１３：４０　「防衛セキュリティゲートウェイの利用について」のご説明
■ １３：４０～１４：３０　質疑応答

## «本日の時程»

令和５年１２月８日（金）１３：００～１４：３０

- １３：００～１３：４０　「防衛セキュリティゲートウェイの利用について」のご説明
- １３：４０～１４：３０　質疑応答

## «目次»

# 本説明会の位置付け

- 本日の企業説明会は、防衛セキュリティゲートウェイ（以下、「DSG」といいます。）のサービス開始にあたり、サービスのご利用を検討している防衛関連企業向けに現在の状況を共有するとともに、 DSGの利用に必要な環境整備や申請等について説明し、ご理解を深めていただく事を目的としています。

- 本日の説明は、ポイントをまとめた要約版となりますので、より詳細については、下記スケジュールで示す時期に公開予定の「加入要領」、「利用要領」及び「利用マニュアル」をご参照ください。

- また、本資料の説明内容は通常時のものであり、 DSG運用開始となる本年度においては、実施内容に一部順序の変更等が発生します。ご理解のほどよろしくお願いいたします。

## 今後のスケジュール

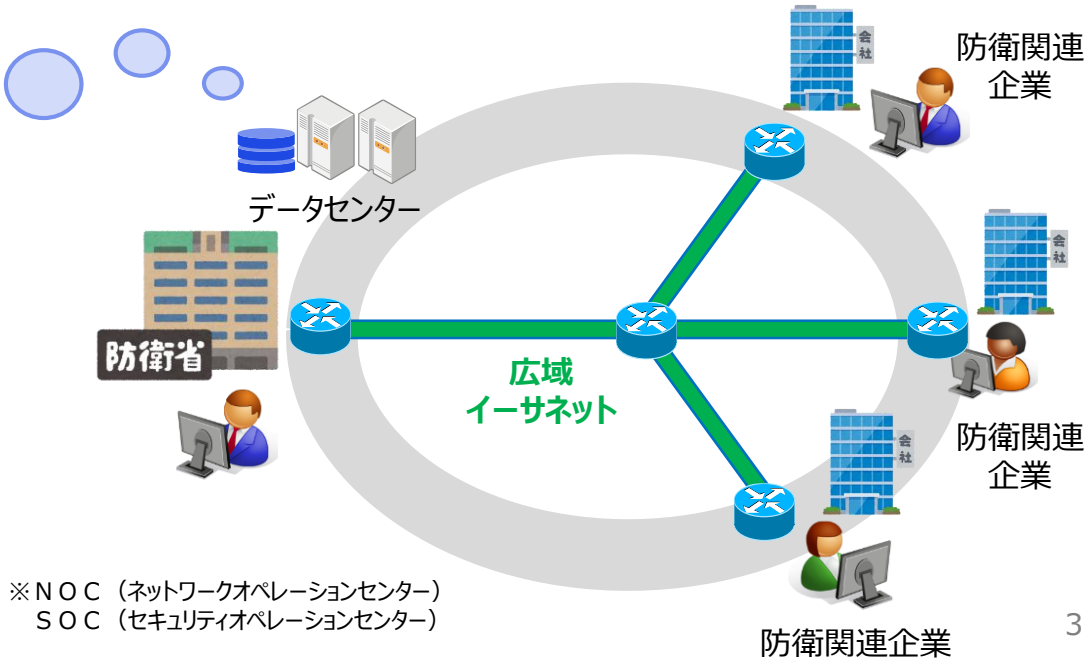
# 防衛セキュリティゲートウェイ（DSG）の概要

○　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 （ Ｄ Ｓ Ｇ ） の イ メ ー ジ

| ＤＳＧの提供サービス例 | |
|---|---|
| **データ管理** | ➢ データの保管・管理 |
| **セキュリティ** | ➢ アクセス管理、識別・認証<br>➢ ログ取得<br>➢ 脆弱性スキャン<br>➢ デプロイメント管理<br>➢ バックアップ |
| **ＮＯＣ・ＳＯＣ※** | ➢ 脆弱性対応管理<br>➢ 構成・資産管理、変更管理<br>➢ セキュリティインシデント対応<br>➢ システム監視・点検<br>➢ セキュリティ監視 |
| **ヘルプデスク** | ➢ DSGの利用に関する防衛関連企業からの問い合わせ対応 |
| **加入支援** | ➢ ＤＳＧ加入申請から利用開始までに関わる支援 |



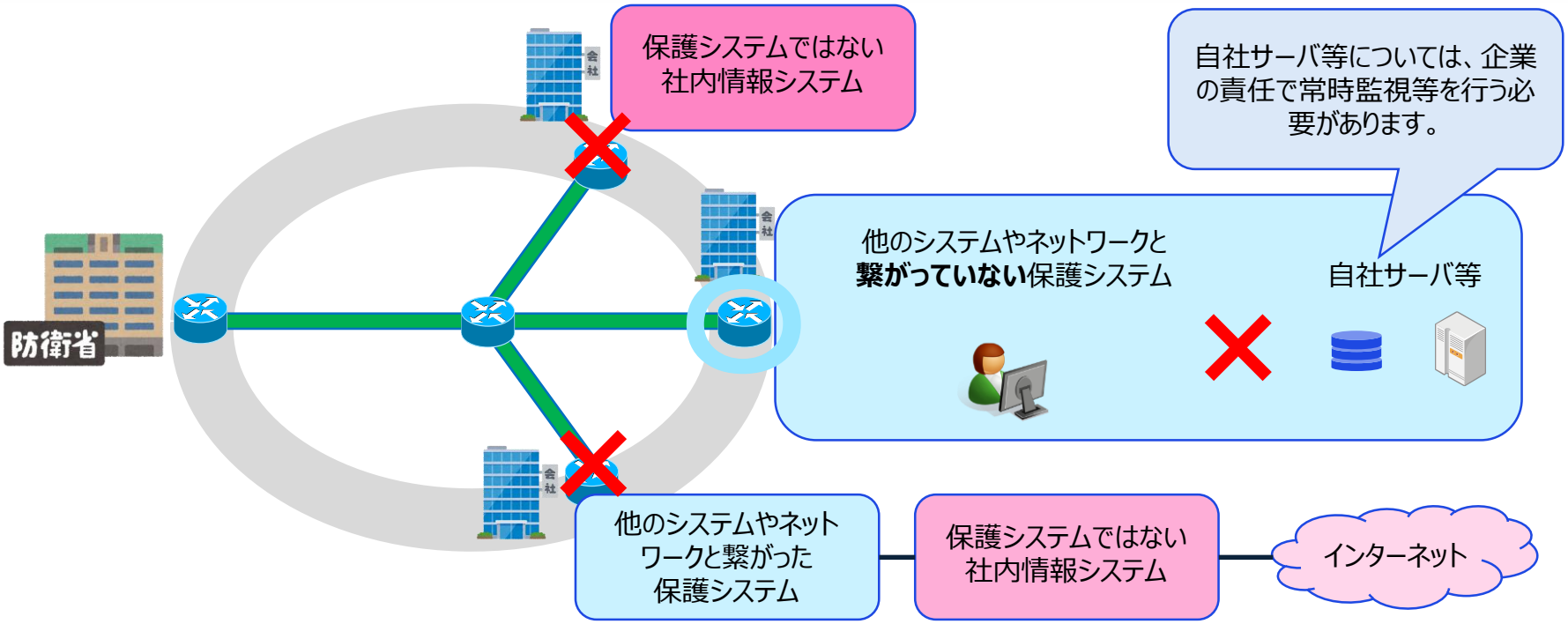

※ＮＯＣ（ネットワークオペレーションセンター）
　ＳＯＣ（セキュリティオペレーションセンター）

# 防衛セキュリティゲートウェイ（DSG）の概要

○　DSGに接続することが可能な情報システムは、防衛産業サイバーセキュリティ基準を満たした保護システムであって、インターネットや社内の情報システムと接続していないクローズドな保護システムに限られます。

○　DSGで常時監視等が可能な機器は、 DSGに接続する保護システムの端末に限られます。したがって、DSGに接続する保護システム内に自社サーバ等がある場合は、防衛産業サイバーセキュリティ基準を満たすため、企業の責任で当該自社サーバ等の常時監視等を行う必要があります。

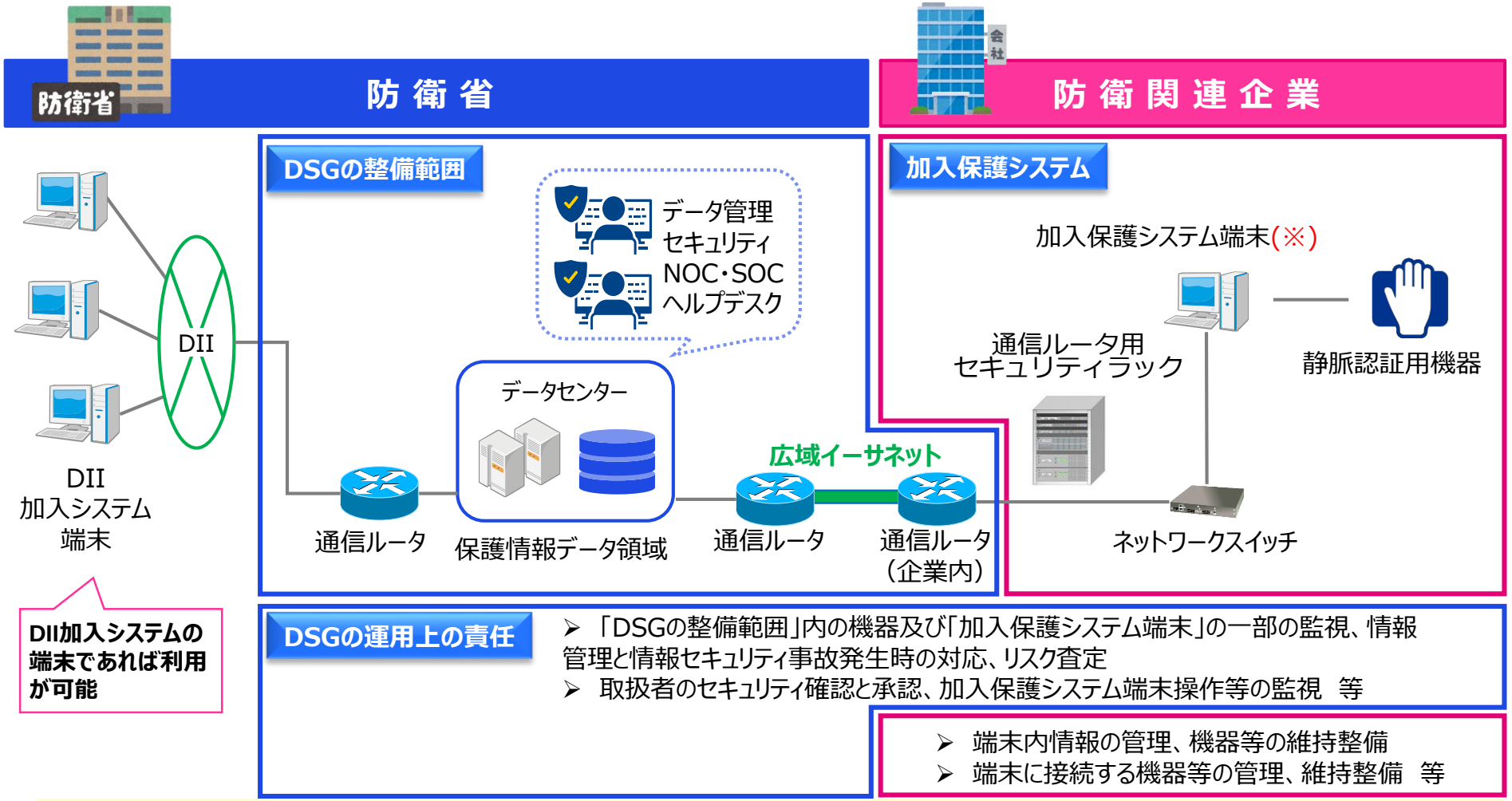
## ＤＳＧへ接続可能な情報システムのイメージ



# DSGの概要（DSGの構成、整備範囲、責任範囲）

DSGの構成、整備範囲及び責任範囲は図示のとおりです。

※ 企業がDSGを利用するための環境構築に要する費用は、防衛産業サイバーセキュリティ基準を満たすための取組みとして、防衛生産基盤強化法の財政措置の対象となる場合があります。




(※) 既存の保護システム端末の利用を基本としますが、ＤＳＧサービスを利用するためには、スペック要件に適合した端末である必要があります。

システム構成品の準備とは別に、防衛関連企業は、防衛産業サイバーセキュリティ基準を満たすため、端末等の機器等を設置する取扱施設に必要な物理的及び環境的セキュリティの構築（監視カメラ、入退管理機能等）を行う必要があります。

# DSGの概要（DSGが提供するサービス）

| サービス名 | 概要 |
|---|---|
| 1．データ管理サービス | |
| データファイル共有 ☞ ｽﾗｲﾄﾞ6 | 情報セキュリティ特約条項付き契約ごと、DSGサービス利用者（官・民）ごとにアクセス可能な領域（共有フォルダ）を作成し、利用者間でのデータ閲覧、データ共有を可能とする。 |
| 2．セキュリティサービス ☞ ｽﾗｲﾄﾞ7~14 | （※別スライドで説明） |
| 3．NOC・SOCサービス | |
| NOCサービス | 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、情報共有を行う。 |
| SOCサービス | セキュリティオペレーションに関する監視、セキュリティインシデント検知、分析、対応、通知、問い合わせ対応、必要な情報提供、情報共有を行う。 |
| 4．ヘルプデスクサービス ☞ ｽﾗｲﾄﾞ15 | DSGの利用に関する窓口対応、問い合わせ対応、FAQの作成、管理等を行う。 |
| 5．加入支援サービス | DSGへの加入に関し、必要な支援を行う。 |
| 6．基本基盤サービス | 各サービスを提供する仮想基盤として構築し、リソースの最適化による抗たん性を確保するとともに、通信およびデータの秘匿、アクセスログ解析、ウィルス対策用ソフトウェアの定義体、標準時刻等、基盤の基本機能を提供する。 |

# DSGの概要（データファイル共有機能について）


利用者は、それぞれの保護システム端末からDSGに接続した後、用途ごとに設定されたフォルダを用いて電子データを官民で共有します。

※各フォルダには利用者に応じたアクセス制限を設定


**端末内データは編集可能** | **領域内データは閲覧のみ** | **端末内データは編集可能**

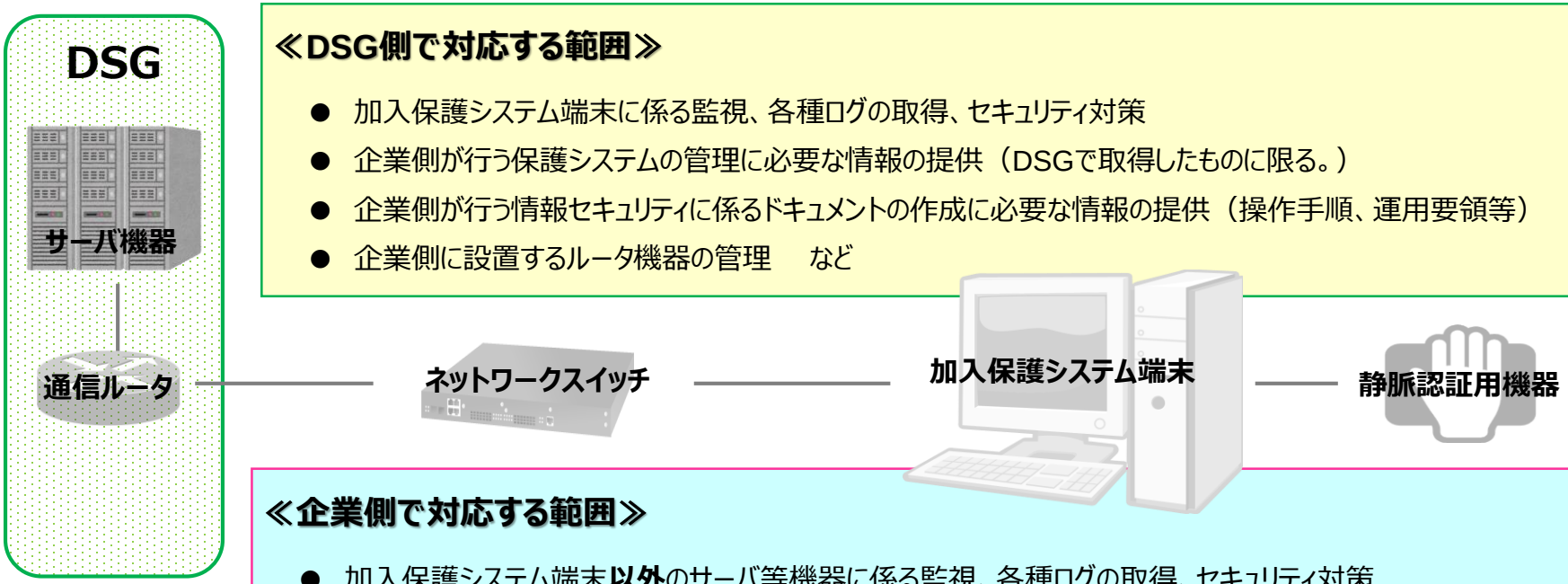
**ご利用のルール**

- 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（サプライヤ）の別など）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。

# DSGの概要（セキュリティサービス機能について（１／７））

加入保護システムの端末に対し、DSGのサービスとしてセキュリティ対策を提供します。

細部は防衛産業サイバーセキュリティ基準に則り、次頁以降で説明しますが、おおよそ次のような区別とする予定です。



# DSGの概要（セキュリティサービス機能について（２／７））

**「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」**とDSGが提供するサービスとの対応範囲

| 章番号 | 項目名 | 内容 | DSGが提供するサービス |
|---|---|---|---|
| 第１ | 趣旨 | | （なし） |
| 第２ | 定義 | | （なし） |
| 第３ | 対象 | | （なし） |
| 第４ | 情報セキュリティ基本方針等 | | （なし） |
| 第５ | 組織のセキュリティ | | （なし） |
| 第６ | 保護すべき情報の管理 | ２⑵目録の更新<br>５⑸可搬記憶媒体へのデータ複製の制御 | ➢ DSG利用に係る閲覧ログの提供<br>➢ 使用できる可搬記憶媒体の事前登録 |
| 第７ | 情報セキュリティ教育及び訓練 | | （なし） |
| 第８ | 物理的及び環境的セキュリティ | ４⑶送配線の物理的セキュリティ対策 | ➢ DSG加入に伴い行う回線工事で送配線に対する物理的セキュリティ対策の実施 |
| 第９ | 保護システムについての管理策 | ※「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システムセキュリティ実施要領」の対応表（次頁以降）で示す。 | |
| 第１０ | 情報セキュリティ事故等への対応 | 1-2全般 | ➢ 必要に応じDSG利用に係る閲覧ログの提供 |
| 第１１ | 情報セキュリティ事故等発生時の対応 | １⑸脆弱性に係る修正 | ➢ 必要に応じDSG利用に係る脆弱性情報の提供 |
| 第１２ | リスク査定 | 1-5全般 | ➢ 必要に応じリスク分析評価に必要なDSG利用に係る情報の提供 |
| 第１３ | セキュリティ監査 | | （なし） |
| 第１４ | 防衛省による監査 | | （なし） |

# DSGの概要（セキュリティサービス機能について（３／７））

**「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関するシステムセキュリティ実施要領」**とDSGが提供するサービスとの対応範囲

| 章番号 | 項目名 | 内容 | DSGが提供するサービス | 企業側の対応事項 |
|---|---|---|---|---|
| 第1_趣旨 | | | （なし） | （なし） |
| 第2_システムセキュリティ実装計画書 | 1_システムセキュリティ実装計画書の作成 | ➢ システムセキュリティ実装計画書の作成に関する内容<br>➢ システムセキュリティ実装計画書の運用に関する内容 | ➢ 必要に応じ、システムセキュリティ実装計画書に記載または添付するDSGの情報（操作手順書等）の提供 | ※ システムセキュリティ実装計画書全体の作成、運用 |
| | 2_システムセキュリティ実装計画書の定期的な確認 | | | |
| | 3_システムセキュリティ実装計画書の保存等 | | | |
| | 4_システムセキュリティ実装計画書の周知 | | | |
| | 5_システムセキュリティ実装計画書の防衛省への提出等 | | | |
| 第3_構成管理 | 1_セキュリティエンジニアリングの原則の適用 | ➢ 設計、開発、導入及び変更時のセキュリティエンジニアリング原則の適用 | ➢ DSG利用に係るセキュリティエンジニアリングの原則を適用 | ※加入保護システムに対する対応 |
| | 2_ベースライン構成設定等 | ➢ 保護システムの構成設定の要件、構成設定の方法、精査等<br>➢ ブラックリストまたはホワイトリストの作成 | ➢ 企業側取扱施設の通信ルータ整備までの全てを提供<br>➢ 必要な構成設定の実施<br>➢ ソフトウェアに係るホワイトリストの提供 | ➢ 加入保護システムの機器の構成設定 |

# DSGの概要（セキュリティサービス機能について（４／７））

| 章 | 項目名 | 内容 | DSGが提供するサービス | 企業側の対応事項 |
|---|---|---|---|---|
| 第3_構成管理（続き） | 3_ベースライン構成設定等の変更等 | ➢ ベースライン構成設定の変更時の実施事項に関する要件等 | ➢ DSGのベースライン構成要素が変更された場合の情報提供 | ➢ 加入保護システムのベースライン構成設定の変更時の対応 |
| | 4_構成設定に係る記録及び保存等 | ➢ ベースライン構成設定に係る現状を確認及び証明するための目録の作成、更新、保存に関する内容 | ➢ DSG構成機器のうち、DSG側で管理するものの目録の作成、更新、保存<br>➢ 構成設定目録の作成に必要なDSGの情報提供 | ➢ 加入保護システムの機器の目録の作成、更新、保存 |
| 第4_保護システムの基本的防御 | 1_保護システムの領域の確定 | ➢ 保護すべき情報を取り扱う領域の設定、ネットワーク制御等 | ➢ 保護すべき情報を取り扱う領域を提供 | ➢ DSGから取得した保護すべき情報であって、DSGネットワーク以外に保存する領域を定める場合の対応 |
| | 2_保護システムの操作手順書の策定 | ➢ 操作手順書の記載事項（手順及びセキュリティ上順守すべき事項等）等 | ➢ DSGサービス利用の手順及びセキュリティ上順守すべき事項等を定めた利用ガイドライン、手順書（利用者マニュアル）を提供 | ※ 加入保護システム以外の自社サーバ等に対する対応 |
| | 3_保護すべきデータの暗号化 | ➢ 保護システムにおけるデータ暗号化の方法、暗号鍵の管理等 | ➢ DSG内のデータの暗号化及びその管理の実施<br>➢ 可搬記録媒体へ保存する際の暗号化機能を提供 | ➢ 加入保護システム端末に保存する場合の暗号化（可搬記憶媒体を除く。） |

# DSGの概要（セキュリティサービス機能について（５／７））

| 章 | 項目名 | 内容 | DSGが提供するサービス | 企業側の対応事項 |
|---|---|---|---|---|
| 第4_保護システムの基本的防御（続き） | 4_その他 | ➢ 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<br>➢ 管理者用機能と利用者用機能の分離<br>➢ 管理者用機能の不正利用防止<br>➢ 仮想化技術利用時の対策<br>➢ 外部システムとの接続制限 | ➢ DSG必須ソフトウェアのアップデート及びアンチウイルスソフトの定義ファイル等の更新を提供<br>➢ 専用回線及びアクセス制御による外部システムとの接続制限の実施 | ➢ 企業独自のソフトウェアへの対応 |
| 第5_アクセス制御 | 1_アクセス制御方針 | ➢ アクセス制御方針の作成、管理に関する要件等 | ➢ アクセス制御方針の作成に必要なDSGの情報提供 | ※ アクセス制御方針全体の作成<br>※ 加入保護システム以外の自社サーバ等に対する対応 |
| | 2_アクセス制御方針に基づく管理策 | ➢ アカウントの管理<br>➢ ログオンの管理<br>➢ ユーザセッションの管理<br>➢ リモートアクセスの管理 | ➢ 利用企業からのDSG利用申請の承認、アクセス権の付与<br>➢ 実施要領に基づくアカウント管理、ログオン管理、ユーザーセッション管理、リモートアクセス管理機能の実装 | ※ 加入保護システム以外の自社サーバ等に対する対応 |
| 第6_識別及び認証 | 1_識別及び認証等の実施 | ➢ 識別の実施に関する要件等（対象、無効化等）<br>➢ 認証の実施に関する要件等<br>➢ パスワードによる認証の実施に関する要件等 | ➢ DSGで利用する機器の識別、構成管理、変更管理の実施<br>➢ 知的要素（ID／パスワード）と生体認証を利用した多要素認証の実装 | ※ 加入保護システム以外の自社サーバ等に対する対応 |
| | 2_識別及び認証におけるその他の留意事項 | ➢ 認証用機器に関する要件等 | ➢ 実施要領に基づく認証用機器を用いた生体認証の実装 | ※ 加入保護システム以外の自社サーバ等に対する対応 |
| 第7_通信制御 | 1_通信の制御 | ➢ 通信制御に関する要件等（ルーター等の設置） | ➢ 拠点間通信用閉域網の提供 | （なし） |

# DSGの概要（セキュリティサービス機能について（６／７））

| 章 | 項目名 | 内容 | DSGが提供するサービス | 企業側の対応事項 |
|---|---|---|---|---|
| 第7_通信制御（続き） | 2_通信データ及び通信セッションの保護 | ➢ 保護すべき情報の通信制限等通信セッションの保護 | ➢ 通信の暗号化<br>➢ フィルタリングによる通信制御 | （なし） |
| | 3_通信機能の利用制限 | ➢ モバイルコード、音声伝達、オフィス機器（電子ホワイトボード等）の利用要件の制定等 | ➢ モバイルコードの不正利用への対策（特定の拡張子の制限）の実施<br>➢ 当面、ネットワーク接続するオフィス機器の利用制限を実施 | （なし） |
| 第8_システム監視 | 1_システム監視の実施 | ➢ 不正アクセス等の検知に関する要件等 | ➢ DSG関連サーバ、ネットワーク機器の他、DSG利用時の企業側加入保護システム端末の監視 | ※ 加入保護システム以外の自社サーバ等に対する対応 |
| | 2_システム監視の実施方法 | ➢ システム監視の実施に関する要件等<br>➢ システム及び通信の監視方法 | ➢ 24時間365日の常時監視の実施（システム、通信全般） | ※ 加入保護システム以外の自社サーバ等に対する対応 |
| | 3_不正なアクセス等を検知した際の対応 | ➢ 不正アクセス検知時の対応（ブロック、隔離、ファイル削除等） | ➢ セキュリティインシデント管理<br>➢ 不正な通信の遮断、感染した端末の隔離 | ※ 加入保護システム以外の自社サーバ等に対する対応 |
| | 4_システム監視により取得した情報の利用及び保管 | ➢ システム監視により取得した情報の利用、保管に関する要件等 | ➢ DSG側の機器で取得した監視情報はDSGで保管<br>➢ 要すれば企業側への情報提供 | ※ 加入保護システム以外の自社サーバ等に対する対応<br>➢ 要すればDSG側への情報提供 |
| 第9_システムログ | 1_システムログの取得及び分析 | ➢ システムログの取得に関する要件等<br>➢ システムログの分析に関する要件等 | ➢ 加入保護システム端末の一部、ネットワーク機器、サーバー、ストレージ、アプリケーションのログの自動収集、管理、分析 | ※ 加入保護システム以外の自社サーバ等に対する対応 |

# DSGの概要（セキュリティサービス機能について（７／７））

| 章 | 項目名 | 内容 | DSGが提供するサービス | 企業側の対応事項 |
|---|---|---|---|---|
| 第9_システムログ（続き） | 2_システムログの管理 | ➢ システムログの管理に関する要件等 | ➢ DSG側の機器で取得したシステムログはDSGにて管理 | ※ 加入保護システム以外の自社サーバ等に対する対応 |
| | 3_システムログに付与するタイムスタンプ | ➢ システムログのタイムスタンプに関する要件等（JSTを基準、NTPサーバとの同期等） | ➢ DSG側の機器で取得するシステムログはDSGにてタイムスタンプを付与 | ※ 加入保護システム以外の自社サーバ等に対する対応 |
| 第10_脆弱性スキャン等 | 1_脆弱性スキャンの実施 | ➢ 脆弱性スキャンの実施に関する要件等（定期的な実施、結果の分析等） | ➢ 脆弱性診断の実施、分析、結果報告<br>➢ 脆弱性が特定された場合の修正<br>➢ 加入保護システム端末に脆弱性が確認された場合の企業への通知 | ➢ 認証機器等、企業で管理する機器及び企業独自のソフトウェアの脆弱性への対応<br>➢ 要すればDSG側への情報提供 |
| | 2_分析結果等の利用 | ➢ 分析結果等の利用に関する要件等 | | |
| 第11_バックアップ | - | ➢ バックアップの実施、保存等に関する要件 | ➢ DSGデータのバックアップ、管理<br>➢ バックアップデータの保存 | ※ 加入保護システム以外の自社サーバ等に対する対応 |
| 第12_システムメンテナンス等 | 1_システムメンテナンス等の計画 | ➢ システムメンテナンス等の計画に関する要件等（人員、対象、内容等） | ➢ DSG関連サーバ、ネットワーク機器や関連ソフトウェア、アプリケーション等の維持管理に関する運用計画を立案<br>➢ 要すれば企業側へ情報提供 | ➢ 認証機器等、企業で管理する機器及び企業独自のソフトウェアの脆弱性への対応<br>➢ 要すればDSG側への情報提供 |
| | 2_システムメンテナンス等の実施 | ➢ システムメンテナンスの実施に関する要件等） | ➢ DSGの運用計画に従いシステムメンテンナンスを実施 | |
| | 3_システムメンテナンス等の記録 | ➢ システムメンテナンス時の記録に関する要件等 | ➢ DSGのシステムメンテナンス時の記録を実施 | |

（ここまで）

# DSGの概要（ヘルプデスクサービスについて）

ヘルプデスクサービスについて、以下に示します。詳細は「利用要領」をご参照ください。

**ヘルプデスクサービス**

- 問い合わせの受付はメール、チャットボット、電話等にて可能です。
- 問い合わせの受付時間は、課業日の9:00～18:00です。またメール及びチャットボットによる受付を24時間365日実施します。（対応は問い合わせの受付時間に準じます。）
- DSGに関する問い合わせへの回答、各種申請受付等を実施します。
- その他、FAQ（よくある質問）を常時公開します。

# DSGの利用に向けた手続き（概要）（１／２）

- DSGの利用に当たり、まずはDSGへの加入及び環境整備が必要になります。（Step１・Step２）
- 加入及び環境が整ったら、利用の申請を行って利用を開始することができます。（Step３・Step４）

**利用に向けたステップ**

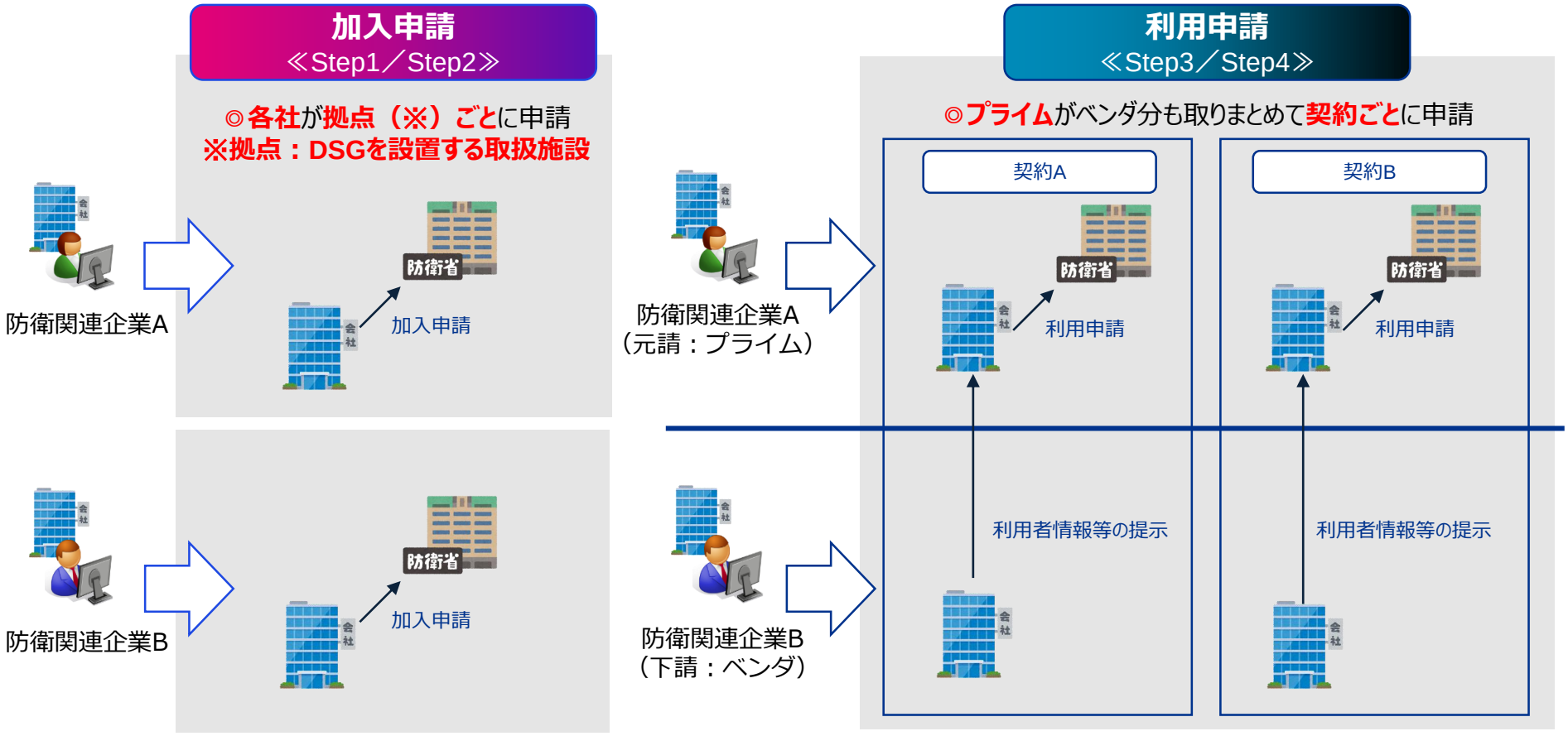
| Step 1 | Step 2 | Step 3 | Step 4 |
|---|---|---|---|
| **加入申請** | **環境整備** | **利用申請** | **利用開始** |
| ➢ ＤＳＧへの加入申請を防衛装備庁に提出（防衛装備庁にて必要な審査を行い加入の可否を決定） | ➢ 専用回線の回線敷設工事の実施<br>➢ 防衛関連企業が準備する機器等の準備<br>➢ 官の現地確認（２回）を実施 | ➢ 防衛装備庁へ利用申請を提出（防衛装備庁にてアカウント等を付与）<br>➢ 利用者の生体認証登録の実施 | ➢ サービスを提供 |
| **防衛関連企業側実施事項** | | | |
| ● 加入申請の提出 | ● 官による現地確認への対応<br>● 回線工事前に行う回線事業者による現地調査及び回線工事時への対応<br>● 機器等の準備、セットアップ作業の実施<br>⚠ 現地確認前に物理的・環境的セキュリティが整備されている必要があります。 | ● 利用申請の提出<br>● ログインに必要なアカウントの受領<br>● 利用者の静脈認証登録（初回時のみ）<br>⚠ 申請には、情報セキュリティ特約条項の付帯した契約の締結が必要です。 | ● 利用を開始 |

「加入要領」の記載範囲

「利用要領」の記載範囲

# DSGの利用に向けた手続き（概要）（２／２）

■　加入申請及び利用申請の大まかな流れは次のとおりです。




**申請ルール**

- 利用申請に当たり、ベンダ分の申請はプライムが取りまとめて実施してください。
- 原則として、ベンダのみの利用申請（プライムは利用しない）はできません。
- 締結した情報セキュリティ特約条項付き契約において、DSGを利用するかどうか、あらかじめ官民間でよくご調整の上、申請を行ってください。
- 官側職員の利用申請は官側で実施するため、防衛関連企業側からの申請内容に含める必要はありません。

# DSGの利用に向けた手続き（加入申請～環境整備）

「Step１ 加入申請」及び「Step２ 環境整備」の具体的なフローを以下に示します。
各項の詳細は「加入要領」をご参照ください。

## ① 事前準備

- 情報セキュリティ基準に対応している取扱施設（物理的及び環境的セキュリティ）の準備

## ①′ 加入申請書等の提出

- 加入申請様式及び端末登録申請様式の入手

  メールでの展開又はHPからのダウンロードを予定しています。

- 申請書類の提出（必要な添付書類の準備を含む。）


## ② 事前現地確認への対応

- 官側現地確認への対応

  取扱施設等が適切に準備されているかについて、現地での確認を行います。なお、既に官側（地方防衛局等）の監査結果がある場合、それを以て、現地確認の実施を省略する場合があります。


## ③ 回線工事への対応

- 回線工事（現地調査含む）

  DSG側が手配する事業者による回線工事及び事前の現地調査の立ち合いをお願いします。

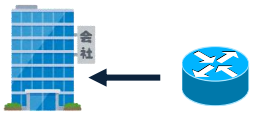
※付帯工事が必要となった場合は防衛関連企業側にて事業者を別途手配していただく可能性があります。


**※ ②までに取扱施設を整備する必要があります。**

## ④ 通信ルータ設置への対応

- 通信ルータ設置

  DSG側が手配する事業者が通信ルータを設置しますので、立ち合いをお願いします。




## ④′ 加入保護システム端末のセットアップ

- 必須ソフトウェアのインストール

  DSG側から提供するインストール媒体を用いて必須ソフトウェアのインストールをお願いします。（オフラインで可能なもののみルータ設置前に可能）

## ⑤ 接続、接続確認

- ルータ、端末その他機器を適切に接続
- 加入保護システム端末を用いてDSGへの接続を確認
- オンライン環境でインストールするソフトウェアのセットアップを実施

## ⑥ 最終現地確認への対応

- 官側の最終現地確認への対応

  全ての作業の終了後、現地での最終確認を行います。

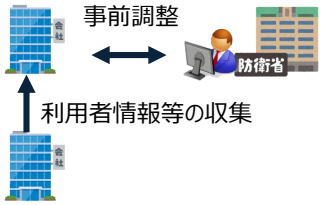

**※ ④までに防衛関連企業側で準備する機器等を準備する必要があります。**

# DSGの利用に向けた手続き（利用申請～利用開始）

「Step3 利用申請」及び「Step4 利用開始」の具体的なフローを以下に示します。
各項の詳細は「利用要領」をご参照ください。

### ① 事前調整、事前準備

- DSGの利用について事業元の部署と事前調整
- プライムはベンダから必要情報の取りまとめ




### ② 利用申請書の提出

- 利用申請様式及び利用者申請様式の入手

  メールでの展開又はHPからのダウンロードを予定しています。
- 申請書類の提出（必要な添付書類の準備を含む。）


### ③ 静脈登録等

- アカウント情報の受領
- 利用者の静脈情報の登録

  アカウント情報の受領後、利用者の静脈情報を登録いただきます。原則として加入保護システム端末に接続した認証機器による静脈登録を予定しています。

### ④ 利用開始

- DSGの利用開始

  DSG側から受領したアカウント及び登録した静脈情報をを用いてDSGをご利用ください。

**※　②までに情報セキュリティ特約付契約の締結が必要です。**

## （参考）利用中～利用終了まで

### 利用期限の表示

- 契約期間中、当該契約の設定領域のトップページに、常に利用期限が表示されます。
- 納期の変更等、利用期限を変更する必要がある場合、官側から申請を受け付けることにより設定変更を行います。

### データの整理期間への移行

- 利用期限後、データの整理のため、２週間程度の整理期間に移行します。
- 防衛関連企業側で保存が必要なデータがある場合は、バックアップを取得いただきます。

### 利用終了

- データ整理期間経過とともに、該当サイト、ライブラリ、フォルダ等へアクセスが不可となります

# DSGの利用に向けた手続き（その他申請）

加入申請又は利用申請と同じタイミングで必要となる可能性があるその他の申請についてご案内します。

## ①　加入保護システム端末に対するソフトウェアインストール申請


加入保護システム端末に対し、

・官指定ソフトウェア以外のソフトウェアを新たにインストールしたい場合

・ＤＳＧへ加入する以前から、既に官指定外のソフトウェアがインストールされている場合

などに必要となる申請です。詳細は「利用要領」をご参照ください。

（現在、申請不要でインストール可能なソフトウェア（Microsoft Office、Adobe Reader等）のリスト（ホワイトリスト）を整備中です。
運用開始時点の版を「加入要領」と併せて展開させていただき、今後は運用中に都度更新していきます。）

## ②　可搬記憶媒体登録・削除申請

他の保護システムとのデータのやり取りやデータの保管を行う場合などに使用する可搬記憶媒体（USBメモリなど）について、使用前に予め登録するための申請です。また、登録した媒体を使用しなくなり削除する場合の申請も兼ねます。詳細は「利用要領」をご参照ください。

# DSGの利用に向けた手続き（各種申請）

DSGの利用開始までに必要となる申請書等を以下にまとめました。
各申請書等の詳細については「加入要領」及び「利用要領」をご参照ください。

| # | 申請書等 | 概要 | 提出タイミング | | |
|---|---|---|---|---|---|
| | | | 加入申請 | 利用申請 | 必要時 |
| 1 | DSG加入申請書 | DSGの加入申請書（各社が拠点単位で申請） | ○ | | |
| | 官側（地方防衛局等）による監査結果通知書 | ※加入申請書の添付書類（ある場合のみ） | (○) | | |
| | レイアウト図記入票 | ※加入申請書の添付書類（取扱施設及び加入保護システム端末設置場所レイアウト） | ○ | | |
| 2 | 加入保護システム端末の登録・削除申請書 | DSG機能を利用する端末として登録する加入保護システム端末の申請書 | ○ | | ○ |
| 3 | DSGサービス利用申請書 | DSGのサービス利用申請書（契約単位で申請、プライムがベンダ分もまとめて申請） | | ○ | |
| 4 | DSG利用者登録・削除申請書 | DSGの利用者登録を行う申請書（契約単位で申請） | | ○ | ○ |
| 5 | 加入保護システム端末に対するソフトウェアインストール申請書 | 官指定以外のソフトウェアのインストールを希望する際の申請書 | | | ○ |
| 6 | 可搬記憶媒体登録・削除申請書 | 可搬記憶媒体の利用時に必要となる申請書 | | | ○ |

# 防衛関連企業側でご準備いただく機器等（必要物一覧）

防衛関連企業側で準備いただく機器等は下表のとおりです。詳細は別途提示するスペック情報資料を参照ください。

| # | 名称 | 概要 | 準備時期（スライド18参照） |
|---|---|---|---|
| 1 | 加入保護システム端末 | DSGへ加入する保護システムの端末<br>※ 既存の保護システム端末の利用を基本とします。ただし、導入済のソフトウェアとDSGで導入必須のソフトウェアが競合し正常動作しない可能性がありますので、**事前に端末のリカバリー**や**導入済みソフトウェアのアンインストール等**を推奨します。 | ④‘ 加入保護システム端末のセットアップまで |
| 2 | ネットワークスイッチ | 加入保護システム端末と通信ルータを接続するためのスイッチ<br>※端末台数が少なく、またルータと加入保護システム端末の配線距離が短い場合は使用しないことも可能です。 | |
| 3 | LANケーブル | 加入保護システム端末、ネットワークスイッチ、通信ルータを接続する為のケーブル | |
| 4 | 静脈認証用機器 | 端末に接続し、静脈認証を行うための機器 | |
| 5 | Webカメラ | 静脈認証時の本人確認を行うための機器 | |
| 6 | 通信ルータ用セキュリティラック | 通信ルータ等を収容するためのラック<br>※既存のラックに空きがあればそれを利用することも可能です。 | ④ 通信ルータ設置への対応まで |

上表に示す機器等以外で、企業が独自で加入保護システム端末に接続する必要があるとした機器（※）については、官側の確認を経た上で使用いただけます。

ただし、そうした機器の監視は、DSGの常時監視の範囲外となりますので、企業の保護システム管理者側にてご対応お願いいたします。

（※）プリンタ、スキャナなどを想定。

# 防衛関連企業側でご準備いただく機器等（端末要件）

以下に加入保護システム端末の要件を示します。詳細は別途提示するスペック情報資料を参照ください。

**加入保護システム端末のスペック要件**

| # | 項目 | 要件 |
|---|---|---|
| 1 | OS | Windows11 Pro 64bit(22H2以上) |
| 2 | CPU | Intel Core i3以上 (第12世代以上) またはPassMarkのスコアが12,000以上<br>動作クロックは1.5Ghz以上 |
| 3 | メモリ | 8GB以上 |
| 4 | ディスク | 256GB以上 |
| 5 | USBポート | TypeA x2ポート以上（カメラ等を外部接続する場合は3ポート以上推奨） |
| 6 | LANポート | RJ45×1ポート以上が内蔵されていること |

**導入必須ソフトウェア（DVD－Rメディアにて官側から提供予定）**

| # | ソフトウェア概要（具体的なソフトウェア名称については個別にご連絡します） |
|---|---|
| 1 | EPP（Endpoint Protection Platform）（マルウェア感染防止）用ソフトウェア |
| 2 | EDR（Endpoint Detection and Response）（マルウェア検知・分析）用ソフトウェア |
| 3 | 脆弱性監査用ソフトウェア |
| 4 | 端末管理用ソフトウェア |
| 5 | ログ収集用ソフトウェア |
| 6 | 生体認証用ソフトウェア |

# 防衛関連企業側でご準備いただく機器等（その他機器要件）

以下にその他機器の要件を示します。詳細は別途提示するスペック情報資料を参照ください。

| # | 対象 | 項目 | 要件 |
|---|---|---|---|
| 1 | ネットワークスイッチ | ー | ー |
| 2 | LANケーブル | ー | ー |
| 3 | 静脈認証用機器 | 全般 | DSGで導入する認証システムに対応する機器であること |
| 4 | Webカメラ | 全般 | 加入保護システム端末に内蔵もしくは外部接続できること |
| 5 | 通信ルータ用<br>セキュリティラック | 規格 | EIA規格19インチラック |
| | | セキュリティ | 施錠できること |
| | | 電源 | 3ピンタイプのアース付き電源コードが２口以上接続できること |
| | | マウント搭載可能ユニット（U）数 | 装置搭載箇所2U及びその上下に1Uずつ空きが確保できること（合計4U以上）<br>※DSG端末が多数（65台以上）となる場合は搭載機器が増えますので、搭載枠が更に必要となります。 |

# 防衛セキュリティゲートウェイに関する問い合わせ等

防衛装備庁では、防衛セキュリティゲートウェイに関する問い合わせを、以下の特設のメールアドレスにて随時受け付けております。疑問質問等ございましたら、いつでも気軽にご連絡ください。

dsg-atla@atla.mod.go.jp

（本件事業の担当者）

防衛装備庁長官官房総務官付情報システム管理室　桒嶋（くわじま）、藤松

03-3268-3111　内線32505，32503

また、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いますので、そちらもご参照いただけます。

ＵＲＬ：https://www.mod.go.jp/atla/dsg.html

# （参考）6/27説明会にていただいた質問への回答_抜粋

前回説明会において継続検討としていた質問内容についての回答をお示しします。

| | 質問 | 回答 |
|---|---|---|
| 1 | DSGは地方調達でも利用可能か？ | 地方調達でも利用可能。 |
| 2 | 加入保護システム端末でインストールできるソフトウェアの種類は？ | MS OfficeやAdobe Reader等の一般的なソフトウェアは、申請不要のホワイトリストとして提示。それ以外は申請・承認を経て利用可能。 |
| 3 | 紙での保護すべき情報の受け渡しはなくなるのか？ | 従来どおりの紙での受け渡しも可能。 |
| 4 | 利用申請から利用開始までにどのくらいかかるか？ | 個々の契約により異なるため一概には示せないが、申請後、できるだけ早期に利用開始となるよう配慮。 |
| 5 | 加入保護システム端末の台数制限はあるか？ | 台数制限はなし。 |
| 6 | プリンタ、スキャナといった機器は接続可能か？ | 官側の確認を経た上で可能。接続機器の管理は企業側で行うとともに、出力した情報は基準に基づき適切な管理を行うこと。 |
| 7 | 契約終了後の保護すべき情報の取り扱いは？ | 契約毎に設定した領域は契約の履行期間終了後、2週間程度でアクセス不可能とするため、それまでにデータ整理を行うこと。 |
| 8 | DSGは民間企業同士での情報共有にも利用可能か？ | 双方の企業が情報セキュリティ特約条項が付帯された同一の契約に利用者として登録されていれば可能。 |
| 9 | web会議等のコミュニケーションツールの導入予定はあるか？ | 何らかのコミュニケーションツールを今後サービスとして導入予定。 |
| 10 | 初回時は、履行中の契約がなくとも回線工事までは実施いただけるか？ | 加入申請の中で、保護すべき情報の取り扱いの可能性について審査を行った上で工事の必要性を判断。 |