ATLA
Acquisition,Technology & Logistics Agency

R5.6.27
企業説明会資料

防衛セキュリティゲートウェイの運営について

（ Defense Security Gateway : DSG ）

令和５年６月

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６月２７日（火）１０：００～１１：３０　防衛省Ａ棟２階　講堂

- １０：００～１０：０５　土本防衛装備庁長官挨拶
- １０：０５～１０：４０　「防衛セキュリティゲートウェイの運営について」のご説明
- １０：４０～　質疑応答

«本日の時程»

令和５年６月２７日（火）１０：００～１１：３０　防衛省Ａ棟２階　講堂

- １０：００～１０：０５　土本防衛装備庁長官挨拶
- １０：０５～１０：４０　「防衛セキュリティゲートウェイの運営について」のご説明
- １０：４０～　質疑応答

«目次»

防衛セキュリティゲートウェイ（ＤＳＧ）の概要

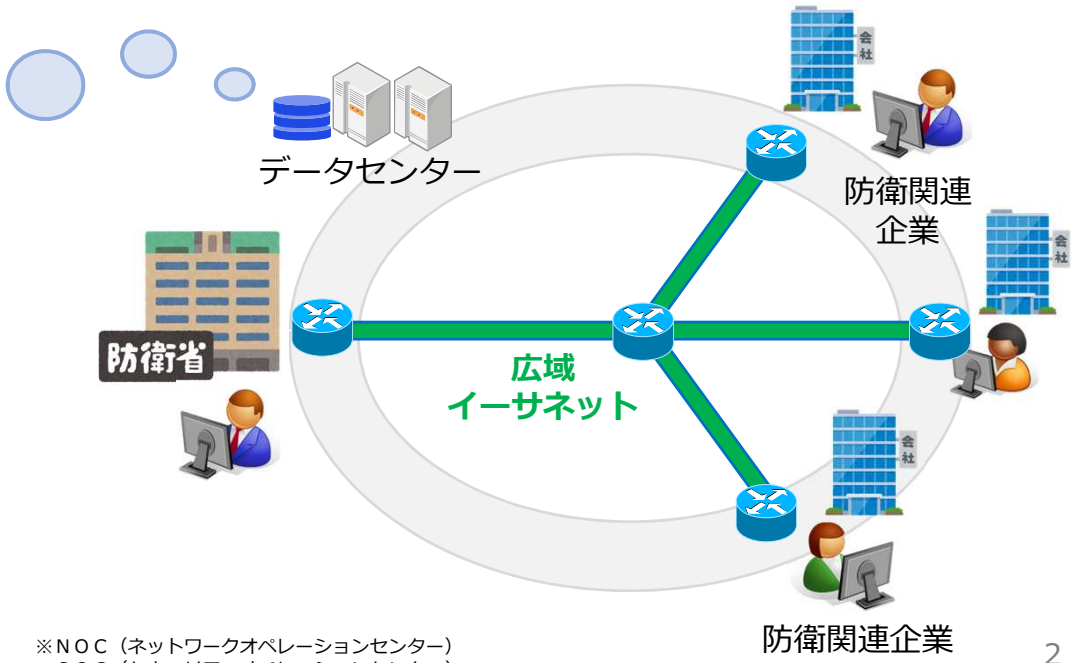
防衛装備品の調達に関しては、防衛省と防衛関連企業の間で、保護すべき情報を含む多くのデータを安全かつ効率的に共有する必要があります。

しかしながら、特に中小企業など個別の企業にとって、これらの情報の共有を可能とするセキュアなシステムを自社において整備するためには、極めて専門的かつ高度な知識が必要となることに加え、費用面においても大きな負担になります。

これを踏まえ、防衛省においては、安全かつ効率的に防衛関連企業との間で保護すべき情報の共有を可能とするために、「防衛産業サイバーセキュリティ基準」に従った官民間における情報共有を可能とする基盤を整備することとし、中小企業を含めた防衛関連企業に対する情報セキュリティの強化を図ることとしております。

ＤＳＧ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 ➢ ログ取得 ➢ 脆弱性スキャン ➢ デプロイメント管理 ➢ バックアップ
ＮＯＣ・ＳＯＣ※	➢ 脆弱性対応管理 ➢ 構成・資産管理、変更管理 ➢ インシデントレスポンス ➢ システム監視・点検
ヘルプデスク	➢ 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の整備範囲、費用負担

ＤＳＧの整備範囲は①情報管理機器、②官民情報共有機器、③通信機器、④取扱者用情報通信機器であり、①～③を防衛省が、④を防衛関連企業が整備します。

防 衛 省

改正 情報保証訓令　NIST SP-800-53準拠

防 衛 関 連 企 業

防衛産業サイバーセキュリティ基準　NIST SP-800-171準拠

整備範囲

① ＤＳＧ内の情報管理と監視のための情報管理機器
② ストレージ等の官民との情報共有機器
③ ネットワークを構築する通信機器　等

④ ＤＳＧの利用に必要なＤＳＧ接続用端末や通信ルータに接続するためのネットワークスイッチ等の取扱者用情報通信機器　等

費用負担

➢ ①～③の整備及び管理・運用に係る費用

① 情報管理機器

データ管理
セキュリティ
ＮＯＣ・ＳＯＣ
ヘルプデスク

② 官民情報共有機器

保護情報データ領域

データセンター

③ 通信機器

広域
イーサネット

通信ルータ　通信ルータ

➢ ④に示す機器の整備及び管理・運用に係る費用

④取扱者用情報通信機器

ＤＳＧ
接続用端末

認証用機器

ネットワーク
スイッチ

運用上の責任

➢ ＤＳＧ全体の監視
➢ 情報管理と情報セキュリティ事故発生時の対応、リスク査定
➢ 取扱者のセキュリティ確認と承認、ＤＳＧ接続用端末操作等の監視　等

なお、以下に示す費用については防衛関連企業側で別途負担いただきます。

➢ 次頁に示す「ＤＳＧ利用の基本的考え方」を満たすための費用（監視カメラ、入退管理等の物理的セキュリティ等）
➢ 取扱者用情報通信機器において防衛関連企業側で利用するソフトウェアの費用（OS、Office及びCAD等業務で利用するソフトウェアを含む）
➢ 防衛関連企業で独自に構築した保護システムに係る費用（端末、ソフトウェア、監視等）

防衛セキュリティゲートウェイにおけるセキュリティ確保（１／３）

ＤＳＧの利用に当たっては、情報漏えい防止、セキュリティ確保の観点から、防衛関連企業に「ＤＳＧ利用の基本的考え方」及び「セキュリティ実施要領」（※１）を順守いただくことになります。

「ＤＳＧ利用の基本的考え方」については下表のとおり、「セキュリティ実施要領」への対応は次頁から一覧表に示すサービス提供を予定しております。

細部の手順、要領については引き続き検討し、改めて提示させていただきます。

ＤＳＧ利用の基本的考え方

- 原則として、防衛産業サイバーセキュリティ基準（※２）に合致した物理的な対策が行われていることが確認された防衛関連企業が利用できます。（別添に示す取扱施設及び関連施設のセキュリティ要件等）
- 初回時は、防衛関連企業側からのＤＳＧ加入の申請を受け、防衛省で審査や調査、調整を行ったのち、必要な工事の実施や設定等を行って利用可能な環境を構築することになります。
- 次回以降（ＤＳＧが利用可能な環境が整っている場合）、原則として、情報セキュリティ特約条項（※３）が適用された契約の締結に伴い、当該契約毎、当該契約に係る取扱者が利用可能なファイル共有のための区画を防衛省側で作成し、必要な認証等を行った上で利用できるよう、防衛関連企業に環境を提供します。
- なお、防衛関連企業は、防衛省の定めた以下の運用ルールを順守してください。
  - **ＤＳＧは防衛関連企業側のシステムや端末等とは接続しません。**
    （そのため、データのＤＳＧへのＩＮ／ＤＳＧからのＯＵＴは可搬記憶媒体で行ってください。）
  - **ＤＳＧ接続用端末内でのみデータの編集が可能です。**また、**防衛関連企業側のＤＳＧ接続用端末に、防衛省が仕様を提供するもの以外の独自のソフトウェアをインストールする必要がある場合は、防衛省の許可を得て行ってください。**

（※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システムセキュリティ実施要領
（※２）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
（※３）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

防衛セキュリティゲートウェイにおけるセキュリティ確保（２／３）

セキュリティ実施要領の各項目に対応する主なＤＳＧ提供サービス及び防衛関連企業にご対応いただく事項

章	ＤＳＧが提供するサービス	防衛関連企業側でのご対応
第３_構成管理	➢ 防衛関連企業側保護区画の通信ルータ整備までの全てを提供 ➢ 必要な構成設定、構成管理及び記録、保全の実施	➢ 防衛関連企業側で使用するネットワークスイッチ及びＤＳＧ接続用端末、認証用機器は、防衛省が提示するスペックに合致するものを準備 ➢ 防衛関連企業側で必要になるソフトウェアの準備 ➢ それらの更新や変更を行う等の構成変更が発生する場合は防衛省に報告
第４_保護システムの基本的防御	➢ 保護すべき情報を取り扱う領域の設定 ➢ ＤＳＧ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、手順書を提供 ➢ 所要の暗号化及びその管理の実施	➢ 防衛関連企業側で必要になるソフトウェアのインストール及びそのアップデートの実施
第５_アクセス制御	➢ アクセス制御方針の策定 ➢ 防衛関連企業からのＤＳＧ利用申請の承認、アクセス権の付与 ➢ 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	➢ 必要の都度のＤＳＧ利用申請、アカウント付与申請の提出、利用状況の把握
第６_識別及び認証	➢ ＤＳＧで利用する機器の識別、管理の実施 ➢ 知的要素（ＩＤ／パスワード）と生体認証を利用したＭＦＡ（多要素認証）の実装	➢ 防衛関連企業側で準備する機器、ソフトウェア、可搬記憶媒体等の登録 ➢ 上記機器の厳格な管理 ➢ 実施要領に従ったパスワード管理
第７_通信制御	➢ 拠点間通信用閉域網の提供 ➢ 通信の暗号化 ➢ フィルタリングによる通信制御	➢ ＤＳＧ接続用端末と防衛関連企業が独自で構築した保護システムとのネットワーク接続の禁止

（次頁に続く）

防衛セキュリティゲートウェイにおけるセキュリティ確保（３／３）

章	ＤＳＧが提供するサービス	防衛関連企業側でのご対応
第８_システム監視	➢ ＤＳＧ関連サーバー、ネットワーク機器の他、防衛関連企業側ＤＳＧ接続用端末の監視 ➢ ２４時間３６５日の常時監視 ➢ セキュリティインシデント管理 ➢ 不正な通信の遮断、感染した端末の隔離	➢ 防衛省から提供されるシステム監視サービスの利用及び関連する各種対応（インシデント検知時の対応等）
第９_システムログ	➢ ＤＳＧ接続用端末、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	➢ 必要に応じ、ＤＳＧ接続用端末以外の防衛関連企業側端末、機器のログの収集、管理、防衛省への提供等 ➢ ＤＳＧが行う分析、管理への対応
第１０_脆弱性スキャン等	➢ 脆弱性診断の実施、分析、結果報告 ➢ 脆弱性が特定された場合の修正 ➢ ＤＳＧ接続用端末に脆弱性が確認された場合の通知	➢ 防衛省から脆弱性が通知された場合の対応 ➢ 自社で管理する保護システムの脆弱性管理（ＤＳＧ接続用端末以外に保護システムが存在する場合）
第１１_バックアップ	➢ バックアップ手順の策定 ➢ ＤＳＧデータのバックアップ管理 ➢ バックアップデータの保存	➢ 自社で管理する保護システムデータのバックアップ管理、データ保存
第１２_システムメンテナンス等	➢ ＤＳＧ関連サーバー、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	➢ 自社で管理するＤＳＧ接続用端末、ソフトウェア、アプリケーションの維持管理

（ここまで）

防衛セキュリティゲートウェイの利用に向けた手続き（１／２）

ＤＳＧの初回利用時は、防衛関連企業において①加入申請、②環境整備、③契約後手続き、④利用申請、⑤利用開始の５つのステップを実施いただくこととしております。
手順の詳細を引き続き検討し、利用ガイドライン等に文書化することを予定しております。

利用に向けたステップ（初回利用時）

加入申請

Step 1
（１ヶ月程度）

- 防衛装備庁（情報システム管理室）への加入申請と加入調査票の提出、申請内容許可連絡の受領

環境整備

Step 2
（数ヶ月程度）

- 防衛省が手配するＤＳＧサービス提供事業者による回線敷設工事への対応
- 防衛関連企業による取扱者用情報通信機器（ＤＳＧ接続用端末等）、立入制限及び入退管理機器の整備
- 防衛省（地方防衛局）による現地確認と承認

契約後手続き

Step 3
（１ヶ月程度）

- 情報セキュリティ特約条項付き契約の締結に基づく、防衛省（地方防衛局）への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の提出（又は確認申請）と承認

利用申請

Step 4
（必要の都度）

- 防衛装備庁（情報システム管理室）への利用予定ユーザー数等の提出

利用開始

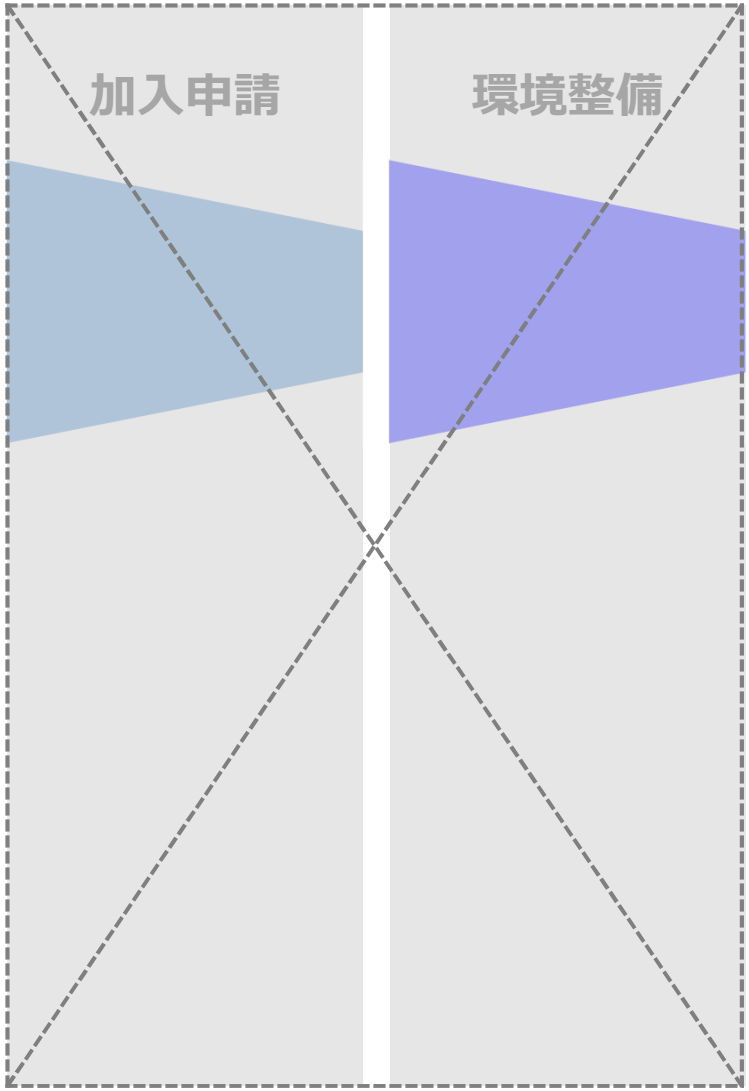
Step 5
（速やかに）

- 利用に必要な情報（ＤＳＧ用ユーザーＩＤ等）の受領

防衛セキュリティゲートウェイの利用に向けた手続き（２／２）

ＤＳＧの２回目以降利用時は、既に初回手続きにおいて利用環境は整っているとの前提のもと、防衛関連企業において①契約後手続き、②利用申請、③利用開始の３つのステップを実施いただくこととしております。

利用に向けたステップ（２回目以降利用時）



契約後手続き

Step 1
（１ヶ月程度）

- 情報セキュリティ特約条項付き契約の締結に基づく、防衛省（地方防衛局）への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の提出（又は確認申請）と承認

利用申請

Step 2
（必要の都度）

- 防衛装備庁（情報システム管理室）への利用予定ユーザー数等の提出

利用開始

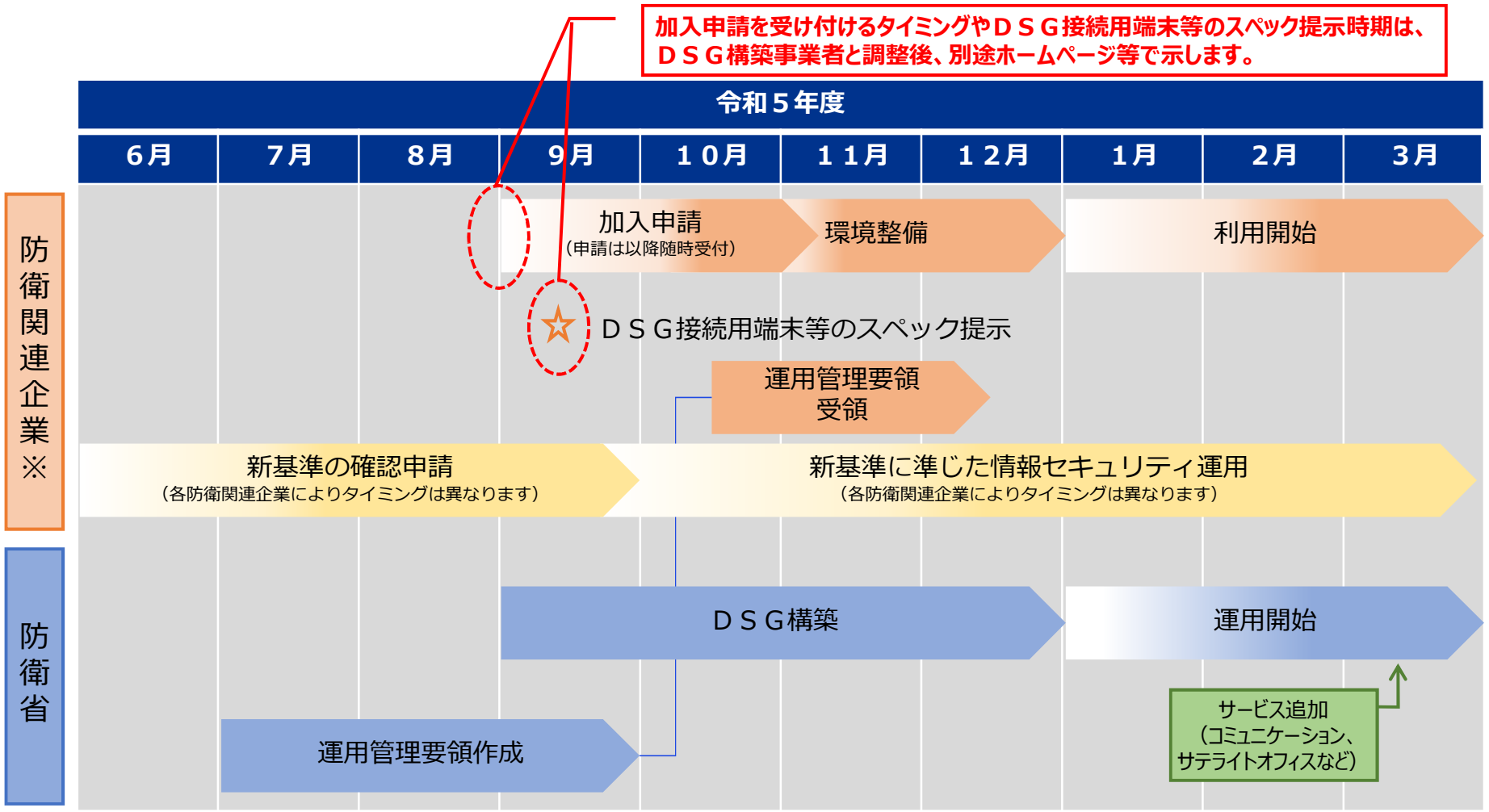
Step 3
（速やかに）

- 利用に必要な情報（ＤＳＧ用ユーザーＩＤ等）の受領

防衛セキュリティゲートウェイの利用開始に向けたスケジュール

ＤＳＧは、令和５年度中（R6.1.1目途）の運用開始を目指して整備事業を進めております。開始時期については確定次第改めてホームページ等でお知らせします。

ＤＳＧの利用にあたっては、防衛産業サイバーセキュリティ基準（新基準）での情報セキュリティ体制構築（特に物理的及び環境的セキュリティ）が前提となるため、利用開始前に確認申請等の手続きをお願いします。



※令和５年度にＤＳＧを利用開始する防衛関連企業の場合。令和６年度以降は随時の受付、利用開始となります。

その他必要な事項：防衛セキュリティゲートウェイに関する問い合わせ

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。

部署名：防衛装備庁　長官官房総務官付　情報システム管理室

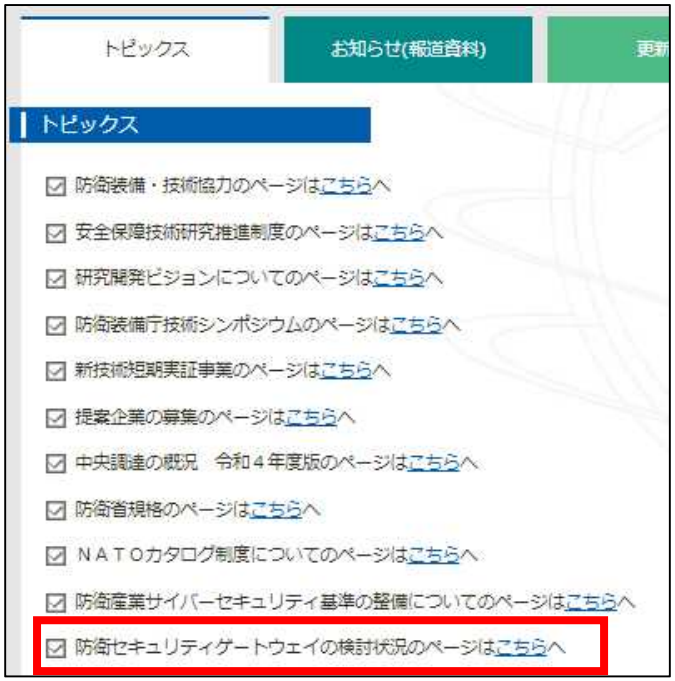
担当者 E-mail　kuwajima.atsushi.tl@atla.mod.go.jp　（桑嶋）

fujimatsu.kenta.oz@atla.mod.go.jp　（藤松）

防衛セキュリティゲートウェイの各種資料等は、防衛装備庁ホームページに掲載しております。

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

【　防　衛　装　備　庁　ホ　ー　ム　ペ　ー　ジ　】



（スライドなし）

ATLA
Acquisition,Technology &
Logistics Agency

取扱施設及び関連施設のセキュリティ要件

別添

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	－
2　取扱施設等に対する物理的セキュリティ対策	• 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。 • 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。 • 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。 • 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、入退の時間等所要の事項を記録簿に記載すること。 • 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。 • 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じること。 • 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等、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じること。 • 取扱施設においては、当該施設の画像、動画、音声等の情報の収集 ・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。
3　入退管理機器に対する物理的セキュリティ対策	• 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。
4　保護システムに対する物理的セキュリティ対策	• 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、必要な措置を講じるものとする。（補足：施錠可能なラックやセキュリティワイヤー等により固定・施錠、ロッカーに施錠保管 等） • 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。（補足：ケーブルをカバーで覆う、床下配線を行う 等）
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	• 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。

- **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をいう。
- **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をいう。

「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 第８ 物理的及び環境的セキュリティ」より抜粋

取扱施設及び関係施設のセキュリティ要件に基づくレイアウトイメージ