令和６年３月２９日作成

（Defense Security Gateway）

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）

防衛装備庁長官官房総務官付情報システム管理室

目 次

１．使用する用語

この要領で使用する主な用語の定義は次のとおりです。

#	用語	定義
1	防衛セキュリティゲートウェイ	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。以下「情報セキュリティ通達」という。）第２項第１号に定める保護すべき情報を、防衛省と当該契約を履行する防衛関連企業の間で、電子データの形で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	利用者	防衛セキュリティゲートウェイサービスを利用する者のうち、防衛関連企業に所属する利用者をいう。
4	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。
5	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。
6	フォルダ	保護情報共有サービスの領域中、第２階層に所在するライブラリ（第１階層に作成される領域をいう。）の中に作成される個別のフォルダをいう。
7	利用端末	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の電子計算機端末をいう。

２．サービスの概要

① サービスの種類

防衛セキュリティゲートウェイサービスが提供するサービスは次のとおりです。それぞれのサービスの詳細は別紙第１をご参照ください。

- **データ管理サービス**

  保護情報共有サービス ／ アカウント管理サービス ／ 多要素認証サービス

- **セキュリティサービス**

  ファイアウォールサービス ／ マルウェア対策サービス ／ 脅威検知サービス ／ 脆弱性監査サービス ／ 構成管理サービス

- **ＮＯＣ・ＳＯＣサービス**

  ＮＯＣサービス ／ ＳＯＣサービス

- **ヘルプデスクサービス**

- **加入支援サービス**

- **基本基盤サービス**

  回線・ルータ利用サービス ／ 仮想化基盤サービス ／ ストレージ利用サービス ／ バックアップサービス ／ セキュリティパッチ配信サービス ／ ＤＮＳサービス ／ ＮＴＰサービス ／ ログ分析サービス ／ 情報提供サービス

② サービスの提供時間（基本）

#	サービス名称	提供時間
1	データ管理サービス	24 時間 365 日
2	セキュリティサービス	24 時間 365 日
3	NOC・SOC サービス	24 時間 365 日
4	ヘルプデスクサービス	（チャットボット） 受け付け、対応とも 24 時間 365 日 （電子メール） 受け付けは 24 時間 365 日、対応は平日 9 時～18 時 （電話） 受け付け、対応とも平日 9 時～18 時
5	加入支援サービス	24 時間 365 日
6	基本基盤サービス	24 時間 365 日

③ サービス利用に係る基本的事項

⑴ 防衛セキュリティゲートウェイサービスで取り扱う情報は、保護すべき情報以下の情報とします。

⑵ 利用者は、予め登録（利用端末の登録申請：加入要領を参照）した利用端末により、防衛セキュリティゲートウェイサービスの利用を行うものとします。

⑶ 利用者間の情報共有を行うための保護情報共有サービスは、「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を前提に、当該契約の契約期間内を利用期間とします。

⑷ 利用者は、利用期間終了後に引き続き設けられる１４日間（土日祝日を含まない。）のデータ整理期間において、防衛セキュリティゲートウェイ上にあるデータについて、移動、削除等の整理を確実に行ってください。データ整理期間終了後は当該領域の全てのデータは削除されます。

⑸ 保護情報共有サービスにおいては、契約毎に固有の領域が設定され、これにより利用者間での情報共有を行うものとします。なお、当該領域には、利用申請時の契約相手方等の契約履行体制に応じ、適切なアクセス権限を設定した規定のフォルダを標準として提供します。

利用者は、既定のフォルダ内に任意でフォルダを作成することができますが、作成したフォルダのアクセス権限は、原則として当該フォルダが所属するフォルダと同一となります。

⑹ フォルダ内のデータは閲覧のみとします。編集等が必要な場合は、利用端末にダウンロードしてから行うなど、ライブラリ以外の領域で行うものとします。

⑺ 保護情報共有サービスで取り扱うことのできないデータの形式（拡張子）があります。詳細は別紙第２をご参照ください。

⑻ 利用者には、利用申請に基づき、利用者別・契約別に固有のアカウント及びパスワードが付与されます。

⑼ 保護情報共有サービスを利用して取り扱うデータは、利用者の責任において、適切に管理を行ってください。

３．利用の要件

防衛セキュリティゲートウェイサービスの利用に当たっては、次の３つの要件を全て満たす必要があります。

#	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。

４．利用の手続き

防衛セキュリティゲートウェイサービスの利用を希望する企業は、利用の要件を満たすことを確認の上、次に示す①～④の手続きを行ってください。

① 利用申請書の提出

保護システム管理者は、防衛装備庁ホームページに掲載された利用申請書の様式に必要事項を記載し、提出してください。

【提出する書類】
- 防衛セキュリティゲートウェイサービス利用・登録・削除申請書（利用者登録書を含む。）

【提出要領】
提出書類一式をＰＤＦ形式で作成し、防衛セキュリティゲートウェイポータルサイトの「申請書等格納フォルダ」に格納のうえ、下の電子メールアドレスに、資料を格納した旨を連絡してください。

送付先メールアドレス：dsg-atla@atla.mod.go.jp

【留意事項】
⑴ 利用申請は、契約毎に提出してください。
⑵ 利用申請は、契約締結日以降に行ってください。
⑶ 利用者は、保護すべき情報の取扱者として取扱者名簿及び保護システム利用者名簿に登録されている者でなければなりません。（事業元においてチェックを行います。）
⑷ 下請負企業がサービスを利用する場合、元請負企業は、下請負企業の利用申請書を取りまとめて提出するものとします。

② アカウント情報の付与

利用申請が受理され、事業元において適切か否かを確認したのち、サービス提供事業者において、アカウント情報が付与されます。

※次頁に続く。

※前頁から続き

【アカウント情報の受領】

保護システム管理者に対し、サービス提供事業者が利用申請書に基づき作成したアカウント情報を「パラメーターシート」の形で送付します。送付は、防衛セキュリティゲートウェイポータルサイトの「申請書等格納フォルダ」への格納により行います。（サービス提供事業者から保護システム管理者に対し、チャットボットで連絡を行います。）

下請負企業のアカウント情報については、当該下請負企業が「申請書等格納フォルダ」に拠点の固有フォルダを有する場合は当該フォルダ及び元請負企業のフォルダにサービス提供事業者が格納します。下請負企業が固有フォルダを有しない場合は元請負企業のフォルダのみにサービス提供事業者が格納します。（この場合、下請負企業への展開は元請負企業が行ってください。）

③ 生体認証登録（静脈認証登録）

アカウントが付与された利用者であって、防衛セキュリティゲートウェイサービスにログインするために必要となる生体認証（静脈認証）登録が未登録の者にあっては、以下の要領で生体認証登録を行ってください。（利用申請時に既に生体認証登録を完了している者は、再度の登録は不要です。）

⑴ 静脈認証の登録作業は、登録場所（東京都新宿区）に来訪しての登録とリモート（遠隔）による登録のいずれかを選択いただけます。
⑵ 登録者のなりすましを防止するため、遠隔操作による登録においては、登録を行う者のほか保護システム管理者が立ち会うものとします。（対面の場合は防衛装備庁職員立ち会いのもとで実施します。）
⑶ 遠隔操作にて登録を行う者は、利用端末に内蔵又は接続されたＷｅｂカメラの前で写真付き身分証明書を提示して本人確認を受けるとともに、本人確認に引き続いて登録作業を行うものとします。
⑷ 前号の本人確認において、証跡の記録の観点から、身分証提示時のキャプチャした画像を取得し、情報システム管理室において保存します。
⑸ 登録を行う者は、前各号の実施（登録を行う者の個人情報の取得を含む。）について、利用申請時に同意するか否かを明確にしなければなりません。

④ 利用の開始

②で送付されたパラメーターシートに記載された、ＵＲＬを入力して防衛セキュリティゲートウェイサービスのトップページにアクセスし、利用対象の事業を選択してください。

使用するブラウザは、Microsoft Edge 又は Google Chrome を推奨します。

※　標準として、①②（利用申請書提出からアカウント情報付与）におおよそ１週間、その後の③（生体認証登録）にも相応の時間が必要ですので、防衛セキュリティゲートウェイサービスを利用したい契約の締結の時期を勘案し、逆算して準備を進めてください。

５．利用申請内容の変更

防衛セキュリティゲートウェイサービスの利用中、以下の内容に変更が生じた場合は利用申請内容の変更の手続きを行ってください。

① 変更の申請が必要となる場合

- 利用申請書の記載内容に変更（利用者の追加・削除、利用者個人の登録情報の変更、利用期間の変更等）

② 変更手続き

保護システム管理者は、防衛装備庁ホームページに掲載された利用申請書の様式（変更の申請の様式を兼ねています。）に必要事項を記載し、提出してください。

【提出する書類】

- 防衛セキュリティゲートウェイサービス利用・登録・削除申請書（利用者登録書を含む。）
- 必要な場合、変更内容を証する書類

【提出要領】

提出書類一式をＰＤＦ形式で作成し、防衛セキュリティゲートウェイポータルサイトの「申請書等格納フォルダ」に格納のうえ、下の電子メールアドレスに、資料を格納した旨を連絡してください。

送付先メールアドレス：dsg-atla@atla.mod.go.jp

【その他】

変更内容に応じて、情報システム管理室又はサービス提供事業者から必要な対応や提出する書類を依頼することがあるので、保護システム管理者は必要な対応を行ってください。

６．その他の申請等

利用中に必要な場合は、以下に示す申請等も行ってください。

① アクセス権限の設定等

保護システム管理者は、利用者が契約毎に設定された領域のライブラリ内に作成したフォルダについて、そのアクセス権限を変更したい場合は、防衛セキュリティゲートウェイポータルサイトの「マニュアル等」のページにあるアクセス権限設定申請書に必要事項を記入の上、防衛セキュリティゲートウェイ上の指定された申請書提出用フォルダに格納するとともに、指定する電子メールアドレスに格納した旨を連絡してください。

なお、下請負企業に係る申請は、元請負企業が取りまとめて行ってください。

【提出する書類】

・ アクセス権限設定申請書

【提出要領】

提出書類一式をＰＤＦ形式で作成し、防衛セキュリティゲートウェイポータルサイトの「申請書等格納フォルダ」に格納のうえ、下の電子メールアドレスに、資料を格納した旨を連絡してください。

メールアドレス：dsg-atla@atla.mod.go.jp

【その他の手続】

利用者が作成したフォルダについて、フォルダの削除又はフォルダ名を変更する場合は、保護システム管理者は変更の内容を明らかにした上で、上記の電子メールアドレスに送信してください。

② 可搬記憶媒体の登録・削除申請

保護システム管理者は、利用端末においてＵＳＢメモリ等の可搬記憶媒体の使用を希望する場合、以下に示す要領で、可搬記憶媒体登録・削除申請書を提出し、使用許可を得てください。

【提出する書類】

・ 可搬記憶媒体登録・削除申請書

※次頁に続く。

※前頁から続き

【提出要領】
提出書類をＥｘｃｅｌ形式で作成し、次のいずれかの方法で提出してください。

- 防衛セキュリティゲートウェイポータルサイトの「申請書等格納フォルダ」に格納のうえ、下の電子メールアドレスに、資料を格納した旨を連絡する。
- 電子メールにて電子メールアドレスに送付する。（フォルダへの格納ができない場合に限る。）

なお、電子メールにて提出する場合、加入申請書の提出に準じてパスワード設定及び連絡を行ってください。

送付先メールアドレス：dsg-atla@atla.mod.go.jp

【留意事項】
防衛セキュリティゲートウェイサービスで使用する可搬記憶媒体は、特定可能なシリアルナンバーが付与されているものでなければなりません。
そのため、識別ができない記憶媒体（CD-ROM やシリアル管理されていない USB メモリ等）は使用できません。

7．禁止事項

防衛セキュリティゲートウェイサービスの利用に当たって、以下を禁止します。

#	禁止事項
1	【保護すべき情報以上の秘密区分の情報の取り扱い】 例） ➢ 秘密電子計算機情報 （秘密保全に関する訓令（H19 防衛省訓令第 36 号）第 14 条第 1 項に規定する秘密電子計算機情報） ➢ 特定秘密電磁的記録 （特定秘密の保護に関する訓令（H26 防衛省訓令第 64 号）第 2 条に規定する特定秘密電磁的記録） ➢ 特別防衛秘密電子計算機情報 （特別防衛秘密の保護に関する訓令（H19 防衛省訓令第 38 号）第 13 条第 1 に規定する特別防衛秘密電子計算機情報）
2	【ユーザーＩＤ及びパスワードの不正利用】 他人のユーザーＩＤ及びパスワードを用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行為 又は自身のユーザーＩＤ及びパスワードを用いて、他人に防衛セキュリティゲートウェイサービスを利用させる行為

#	禁止事項
3	【その他の禁止行為】 ⑴ 公序良俗に反する行為 ⑵ 犯罪行為に結びつく行為又はそのおそれのある行為 ⑶ 法律、条例に違反する行為又はそのおそれのある行為 ⑷ 他の防衛関連企業、利用者及び防衛セキュリティゲートウェイ又は防衛セキュリティゲートウェイサービスを誹謗、中傷する行為 ⑸ 防衛セキュリティゲートウェイサービスの運用を妨げる行為 ⑹ 防衛セキュリティゲートウェイ及び管理組織の信頼を損なう行為 ⑺ 情報を改ざんする行為 ⑻ 秘密漏えい又はそのおそれのある行為 ⑼ 防衛セキュリティゲートウェイサービスに接続した電子計算機等の装置を無線、有線等の手段によりインターネットプロバイダ等の部外又は許可されていない情報システムに接続する行為 ⑽ ネットワークスキャン、ポートスキャン等の行為 ⑾ 利用資格のない電子計算機に対するアクセス行為 ⑿ 業務以外の目的による防衛セキュリティゲートウェイサービスの使用 ⒀ その他本要領に違反する行為

８．利用者の報告義務

利用者は、防衛セキュリティゲートウェイサービスの利用に際し、以下に該当する情報に接した場合には、直ちに保護システム管理者を通じて情報システム管理室に報告してください。

⑴ この要領に定められた規定に関する違反が発生し又は発生した恐れがある情報

⑵ 防衛セキュリティゲートウェイサービスの運用に影響を与える可能性のある情報

（連絡先）

防衛装備庁長官官房総務官付情報システム管理室
電話番号：03-3268-3111（内線 32503、32505）
メールアドレス：dsg-atla@atla.mod.go.jp

９．お問い合わせ先

防衛セキュリティゲートウェイサービスへの加入に関するお問い合わせは、サービス提供事業者が提示する連絡先又は以下の連絡先にお願いします。

防衛装備庁長官官房総務官付情報システム管理室
電話番号：03-3268-3111（内線 32503、32505）
メールアドレス：dsg-atla@atla.mod.go.jp

（別紙第１）防衛セキュリティゲートウェイサービス一覧

No.	サービス名	サービスの概要
1	データ管理サービス	
1-1	保護情報共有サービス	利用者間でのデータ共有を行うための領域、ライブラリを提供し、利用端末からファイルを登録して共有する。
1-2	アカウント管理サービス	アカウント管理に関する以下のサービスを提供する。 ・サービス利用のためのアカウントの作成、更新、停止及び削除を行う。 ・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する。また、ログイン試行が一定回数を超えた場合に自動ロックを実施する。 ・アカウントをグループ管理し、グループ毎に権限を設定する。
1-3	多要素認証サービス	サービス利用のための多要素認証（生体認証及びパスワード認証）を提供し、アカウント管理サービスと連携してユーザーの生体情報の登録及び管理、ログオン履歴の管理を行う。
2	セキュリティサービス	
2-1	ファイアウォールサービス	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する。また、許可されていない通信を遮断する。
2-2	マルウェア対策サービス	利用端末をマルウェアの脅威から防護するとともに、最新の定義体を配信する。また、許可されていない通信の遮断により被害の拡散を軽減する。
2-3	脅威検知サービス	利用端末において、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、被害の拡散を軽減する。
2-4	脆弱性監査サービス	利用端末の脆弱性監査を実施し、脆弱性の有

No.		サービス名	サービスの概要
			無を確認する。取得した脆弱性監査結果を、必要に応じて加入企業に提供する。
	2-5	構成管理サービス	利用端末の端末情報の取得、情報漏えいリスクの高い操作の抑止、操作履歴の取得を行う。取得した端末情報、履歴を、必要に応じて加入企業に提供する。
3		NOC（Network Operation Center）・SOC（Security Operation Center）サービス	
	3-1	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。
	3-2	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	サービス利用に関する問い合わせ窓口（電話、チャットボット）を提供し、ＦＡＱの作成・管理等を行う。
5		加入支援サービス	サービスへの加入に関し、以下の支援を提供する。 ・保護情報共有サイトの作成を支援する。 ・利用者アカウントの登録、更新、削除を行う。 サービスに加入するためのセットアップ手順書、利用マニュアル、インストーラーを配布する。 ・ネットワークの開通を支援する。
6		基本基盤サービス	
	6-1	回線・ルータ利用サービス	加入企業の拠点とサービスを提供する機器等の設置拠点までの間を専用回線で接続するとともに、専用の通信ルータを提供する。通信を暗号化し、通信内容の秘匿化を行う。また、許可された利用端末以外の端末の接続を拒否するとともに、許可した通信以外を遮断する機能を提供する。
	6-2	仮想化基盤サービス	各サービスを提供するための仮想化基盤を提供する。

No.	サービス名	サービスの概要
6-3	ストレージ利用サービス	保護情報共有サービス等で保存するデータの格納先となるストレージを提供する。また、保存するデータの暗号化を行う。
6-4	バックアップサービス	機器等のシステムデータ、保護情報共有サービスで提供される領域、アクセスログ等のバックアップを行う。（利用端末のバックアップは対象外）
6-5	セキュリティパッチ配信サービス	ＯＳ（オペレーティングシステム）等のセキュリティパッチを取得し、利用端末に提供する。
6-6	ＤＮＳサービス	利用端末向けにドメイン名とＩＰアドレスを管理し、相互変換を行う。
6-7	ＮＴＰサービス	利用端末向けに標準時刻を提供する。
6-8	ログ分析サービス	各種サービスで取得したログを収集、相関分析を行い、セキュリティリスクの検出を行う。
6-9	情報提供サービス	必要に応じ、各種情報（操作履歴、ログ、脆弱性監査結果等）の提供を行う。

（別紙第２）保護情報共有サービスで使用できないデータ形式

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