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）

（情報システム情報保証責任者）
防衛装備庁長官官房総務官

版	作成年月日	文書番号
初版	令和6年3月２９日	装官総第５６１６号

第１　総則

１　趣旨

本要領は、防衛セキュリティゲートウェイサービスの利用に必要な事項（加入企業の利用者向け）を定める。

２　用語の定義

本要領で使用する用語は、次の各号に定めるところによる。

⑴　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。

⑵　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。

⑶　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。

⑷　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。

⑸　サービス提供事業者

防衛セキュリティゲートウェイサービスを提供する企業をいう。

⑹　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。

⑺　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。

第２　防衛セキュリティゲートウェイサービスの概要

１　提供するサービスの種類

防衛セキュリティゲートウェイサービスは別紙第１のとおりとする。

２　取り扱う情報の種類

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する。

３　サービスの提供時間

⑴　運用時間

第１項に示す防衛セキュリティゲートウェイサービス（次項に示すヘルプデスクサービスを除く。）の運用時間は、原則として２４時間３６５日とする。

⑵　ヘルプデスク

ヘルプデスクサービスの運用時間は、原則として次のとおりとする。

ア　チャットボット

受付及び対応は、２４時間３６５日とする。

イ　電子メール

受付は、２４時間３６５日とし、対応は、平日９時から１８時までとする。

ウ　電話

受付及び対応は、平日９時から１８時までとする。

⑶　前２号の規定にかかわらず、運用上必要な場合にサービスの提供時間を変更することがある。この場合において、別に示す防衛セキュリティゲートウェイポータルサイトにて連絡、周知を行う。

４　サービスの利用に係る基本的事項

⑴　利用者は、あらかじめ登録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する。

⑵　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する。

⑶　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、削除等の整理を行うものとする。

⑷　データ整理期間終了後のデータの復旧や抽出の要望は受け付けない。

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する。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する。

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るが、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る。

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

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）は別紙第２のとおりとする。

⑻　利用者には、利用申請に基づき、利用者別及び契約別に固有のアカウント及びパスワードが付与される。パスワードについては、定期的に変更を行うものとする。

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、適切に管理を行わなければならない。第３号に掲げるデータ整理期間終了後において防衛セキュリティゲートウェイ上にデータを残置しないものとす

る。

5　防衛セキュリティゲートウェイサービスに係る連絡事項の把握

保護システム管理者は、防衛セキュリティゲートウェイポータルに掲載する連絡事項について、防衛セキュリティゲートウェイサービスを利用する契約の有無にかかわらず、適時閲覧して把握し、利用者への周知をするよう努めるものとする。

第３　サービス利用に係るセキュリティ対策

防衛セキュリティゲートウェイサービスにおいては、防衛産業サイバーセキュリティ基準（情報セキュリティ通達の別添「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」第２条第１号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。）付紙に定める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（以下「実施要領」という。）に基づき、次の対策を講じる。

1　構成管理（実施要領第３関係）

⑴　サービスの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する。

⑵　サービスを提供するために構築する全ての構成要素及び加入企業に設置した通信ルータ及び利用端末の構成要素について、構成管理を行う。

⑶　前号の構成管理の内容や目録について、加入企業からの申請に基づき、情報提供や情報共有を行う。

⑷　利用者に対し、該当契約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提供するとともに、利用者からの申請に基づき、適切なアクセス権限の付与を行う。

⑸　サービス利用に係るブラックリスト及びホワイトリストの作成、更新を行う。

2　保護システムの基本的防御（実施要領第４関係）

⑴　サービス利用に係る保護すべき情報を取り扱う領域を、契約毎に設定する。

⑵　サービス利用は、登録された利用端末以外からはできないよう制御するとともに、利用端末から防衛セキュリティゲートウェイ以外への通信を防御する。

⑶　サービス利用に係る操作手順書、利用マニュアル等を整備し、利用者に提供する。

⑷　第１号で設定した領域において、保護情報共有サービスで保存する保護すべき情報は、電子政府推奨暗号により暗号化を行うとともに、暗号鍵の厳格な管理を行う。

⑸　利用端末で使用する可搬記憶媒体は、事前に登録が必要なこととし、保護すべき情報の保存に当たっては暗号化を行う。

⑹　サービス利用のための導入必須ソフトウェア、ＯＳ及びＯｆｆｉｃｅ製品のインストール及びアップデートを行う。

⑺　加入企業が利用端末に対し独自にインストールを希望するソフトウェアについては、加入企業からの申請を受け、必要な検証を行った上で承認する。

⑻　アカウント管理サービスにより、管理者機能と利用者機能を分離し、不正利用を防止する。
⑼　仮想環境の構築に当たり、各サーバ間の通信をホスト型のファイアウォールを設けることで、データの不正な移動や意図しない移動を防止するとともに、外部システムとの接続を制限する。

3　アクセス制御（実施要領第５関係）
⑴　アカウント管理サービスにより、サービス利用に係るアカウント管理を適切に行う。
⑵　サービス利用に係るログオン試行の回数上限を定める。
⑶　サービス利用に係る、非アクティブ状態時間の上限を定め、それを超過した場合はユーザーセッションをロックする。ロック解除には多要素認証による認証を必要とする。
⑷　ログオフ時のユーザーセッションの自動切断を行う。

4　識別及び認証（実施要領第６関係）
⑴　利用者へのアカウント付与に際し、アカウント管理サービスにおいて、利用者の識別、管理を行う。
⑵　多要素認証（生体認証及びパスワード認証）を導入するとともに、登録された利用端末からのみ認証可能とする。
⑶　パスワードは必要な強度を満たしたものを、機密性に配慮した方法により配布する。また、利用者において、配布したパスワードの定期的な変更を行うこととする。
⑷　識別及び認証に使用する機器等は、防衛セキュリティゲートウェイサービスにおいて識別又は認証を行うソフトウェアに対応したものに限定する。

5　通信制御（実施要領第７関係）
⑴　セッションロック時のネットワーク接続の自動切断を行う。
⑵　脅威検知サービスにより、悪意のあるモバイルコードの検知、隔離等の対応を行う。

6　システム監視（実施要領第８関係）
⑴　サービスへの加入時に導入を必須とするソフトウェアをインストールし、これにより不正なアクセス等の検知（アラート設定を含む。）等、必要な監視及び対応を行う。
⑵　サービス利用に係るシステム上の挙動の監視を行う。
⑶　システム監視は、監視結果に応じて監視レベルの引き上げ等の対応を行う。
⑷　システム監視で取得した情報は、バックアップサービスにより暗号化の上、データにて保存する。

7　システムログ（実施要領第９関係）
⑴　サービスを提供するために構築する全ての構成要素及び利用端末に係る操作ログ、アクセスログを取得する。
⑵　前号で取得した各種ログについて、加入企業からの申請に基づき、情報提供や情報共有を行う。

⑶　取得したログ情報は、タイムスタンプを付与し、バックアップサービスにより暗号化の上、データにて保存する。
⑷　第１号で取得したログの定期的な確認、分析及び報告を行う。
⑸　脅威検知サービス及びマルウェア対策サービスにより、システムログを取得するツールへの不正なアクセス等を検知し、防護する。

８　脆弱性スキャン等（実施要領第１０関係）

⑴　サービスを提供するために構築する全ての構成要素及び利用端末に対して定期的な脆弱性監査を行うとともに、その結果の分析を行う。
⑵　前号の分析結果について、必要に応じ、情報提供や情報共有を行う。

９　バックアップ（実施要領第１１関係）

⑴　保護情報共有サービスで保存する保護すべき情報について、定期的にバックアップを取得し、適切な期間保存する。
⑵　取得したバックアップについては、適切な保護を行う。

１０　システムメンテナンス等（実施要領第１２関係）

⑴　サービスへの加入時に導入したソフトウェアについて、メンテナンスツールを提供する。
⑵　メンテナンスを行う人員に対し、メンテナンス期間に応じた多要素認証を行う。
⑶　メンテナンスの実施に伴うシステムログの取得及び分析を行うとともに、メンテナンス後の動作確認を行う。

第４　利用手続

１　利用要件

防衛セキュリティゲートウェイサービスの利用は、次の各号を全て満たしていなければならない。

⑴　防衛セキュリティゲートウェイサービスを利用する取扱施設等に係る、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）第２第２項第２号カ(ｴ)に規定する加入完了通知書を受領していること。
⑵　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。
⑶　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。

２　利用申請

⑴　利用申請書の提出

保護システム管理者は、第１項各号に該当し、防衛セキュリティゲートウェイサービスの利用を行う者は、防衛装備庁ホームページから最新版の申請様式（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（別紙様式

第１））を取得し、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ものとする。

なお、申請に当たっては、以下の点に留意されたい。

ア　利用申請は、前項第２号契約毎に提出する。

イ　利用申請は、前項第２号契約の契約締結日以降に行う。

ウ　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らない。

エ　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する。

⑵　アカウント情報の付与

利用申請後、申請内容の審査を行ったのち、サービス提供事業者から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アカウント情報を付与し、保護システム管理者に申請単位で送付する。送付は、防衛セキュリティゲートウェイ上の指定した送付用フォルダに格納することにより行う。

⑶　生体認証登録

ア　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、サービス提供事業者又は防衛装備庁長官官房総務官付情報システム管理室（以下、単に「情報システム管理室」という。）と調整の上、遠隔操作による登録（サービス提供事業者）又は防衛装備庁での登録（情報システム管理室）のいずれかにより生体認証登録を行うものとする。

ただし、利用申請時に既に生体認証登録を完了している者は、再度の登録は必要ない。

イ　登録者のなりすましを防止するため、前号の登録のうち、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、また、防衛装備庁での登録においては、情報システム管理室職員が立ち会うものとする。

ウ　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する。

エ　前号の本人確認の際、証跡の記録の観点から、キャプチャーした画像を取得し、情報システム管理室において保存する。

オ　登録を行う者は、前４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らない。

⑷　利用の開始

利用端末のブラウザ（Ｍｉｃｒｏｓｏｆｔ　Ｅｄｇｅ又はＧｏｏｇｌｅ　Ｃｈｒｏｍｅを推奨）から、指定する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、第２号で送付されたアカウント情報及び前号で登録した生体認証により、該当契約のライブラリにログインする。

３　利用の変更申請

防衛セキュリティゲートウェイサービスの利用期間中において、前項で提出した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）が生じた場合は、前項の利用申請と同一の様式及び要領により、新たに変更後の利用申請書を作成し提出するものとする。

なお、必要に応じ、変更内容を証する書類を添付すること。（利用者を追加する場合の取扱者名簿、保護システム利用者名簿等）

第５　アクセス権限の変更等

１　アクセス権限の変更

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する場合は、防衛装備庁ホームページから最新版の申請様式（アクセス権限設定申請書（別紙様式第２））を取得し、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するものとする。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うものとする。

２　フォルダの削除等

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、指定の電子メールアドレスに送信する。

３　前２項の申請等については、その内容の妥当性について、情報システム管理室が確認を行った上で処理される。

第６　可搬記憶媒体の登録・削除

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（別紙様式第３）を提出し、使用許可を得るものとする。申請様式は、防衛装備庁ホームページに掲載された最新版を使用するものとする。

⑴　提出書類及び提出の要領

保護システム管理者は、作成した申請書をＥｘｃｅｌ形式により、以下のいずれかの方法で提出するものとする。なお、イの方法による場合は、資料へのパスワード設定を行うものとし、パスワードは別電子メール又は別の手段により情報システム管理室に連絡するものとする。

ア　防衛セキュリティゲートウェイ上の指定された申請書等格納フォルダに格納のうえ、指定する電子メールアドレスに、資料を格納した旨を連絡するものとする。

イ　電子メールにて指定する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。）

⑵　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らない。

第７　利用制限事項

１　秘密データの取扱いの禁止

利用者は、利用端末等で秘密電子計算機情報（秘密保全に関する訓令（平成１９年防衛省訓令第３６号）第１４条第１項に規定する秘密電子計算機情報をいう。）、特定秘密電磁的記録（特定秘密の保護に関する訓令（平成２６年防衛省訓令第６４号）第２条に規定する特定秘密電磁的記録をいう。）及び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（平成１９年防衛省訓令第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をいう。）を取り扱ってはならない。

２　ユーザーＩＤ及びパスワードの不正利用の禁止

利用者は、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してはならない。また、利用者は、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てはならない。

３　禁止事項

利用者は、前２項に掲げるもののほか、防衛セキュリティゲートウェイサービスを利用するにあたり、次の行為を行ってはならない。情報システム管理室が次の行為に該当するか否かに関し調査が必要と判断した場合、その求めに応じ、利用者は調査に協力をするものとする。

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

第８　利用者による報告

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するものとする。

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

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・ＳＯＣ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、チャットポッド）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。
	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

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	

別紙様式第１（第４第２項第１号関係）

申請番号	（サービス提供事業者で採番）

防衛セキュリティゲートウェイ利用申請書

申請日　　年　　月　　日

利用管理番号（変更申請の場合にご記入ください）

１．申請種別

該当の種別で●を選択又はご記入ください。

	新規
	変更

※変更申請の場合、変更する項目に●を選択又はご記入ください。

２．企業種別

該当の種別で●を選択ください。

「下請負企業（ベンダ）」を選択の場合、元請負企業（プライム）名及び本申請内容を元請負企業と調整済みの場合はチェックを入れてください。

	元請負企業
	下請負企業

⇒　元請負企業名

	申請内容について 元請負企業と調整済

⇓ ３．契約情報

	①	加入企業名			
	②	防衛セキュリティゲートウェイを利用する下請負企業（ベンダ）の有無	※下請負企業のパラメータシートは、元請負企業から配布いただきます。申請書等格納サイト内での共有をご希望の場合、共用フォルダを作成します。各下請負企業の防衛セキュリティゲートウェイ利用者登録・削除申請書内の元請負企業記入欄にて、共用フォルダ作成希望の有無をお知らせください。		
	③	契約機関名			
	④	契約名			
	⑤	契約を特定できる番号 （契約番号、調達要求番号等）			
	⑥	契約日及び終了日 （西暦（yyyy/mm/dd）でご記入いただくと、和暦で表示されます。）	～	国歳（自動計算）	国 （1の場合は歳となる）
	⑦	連絡欄 ※記入任意			

＜利用にあたっての留意点＞

契約の契約期間を利用期間とし、利用期間終了後、１４日間（土日祝日を含まない。）のデータ整理のための期間を設け、当該期間中に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、利用者の責任において移動、削除等の整理を行っていただきますが、データ整理期間終了後にデータが残っていた場合、当該データは一定期間後削除します。詳細については、「防衛セキュリティゲートウェイサービス運用管理要領（加入企業の利用者向け）」をご確認ください。

防衛装備庁記入欄

サービス提供事業者記入欄

別紙様式第２（第５第１項関係）

申請番号 （サービス提供事業者で採番）

アクセス権限設定申請書

申請日　　年　　月　　日

利用管理番号＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
機関名（官のみ記入）
加入企業名（民のみ記入）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

部署名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
外線電話番号 / 内線代表番号（官のみ記入）
電話番号（民のみ記入）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

申請者氏名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

申請者E-mail（民のみ記入）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

１．対象となるフォルダ等の情報

①	サイトＵＲＬ	
②	サイト名（契約名）	
③	ライブラリ名 （右欄でリスト選択）	利用者共通
④	フォルダ名（パス）	

２．対象となる利用者

［記載要領］

・権限追加又は権限削除に●を記入してください。

・対象フォルダに対するアクセス権の追加または削除を希望する利用者のみをご記入ください。なお、記入のない利用者についてはアクセス権が付与されません。

権限追加	権限削除	番号	氏名（漢字） ※姓と名の間はスペースを空けること	氏名（カナ） ※姓と名の間はスペースを空けること	内線 （官のみ）	ＡＤアカウント（ＤＳＧ用ユーザーＩＤ）
		１				
		２				
		３				
		４				
		５				
		６				
		７				
		８				
		９				
		１０				
		１１				
		１２				
		１３				
		１４				
		１５				
		１６				
		１７				
		１８				
		１９				
		２０				

サービス提供事業者作業報告欄

下記の通り作業を完了いたしました。

作業完了日	作業者	確認日	確認者

備考欄

別紙様式第３（第６本文関係）

申請番号 （サービス提供事業者で採番）

可搬記憶媒体登録・削除申請書

申請日　　年　　月　　日

加入企業名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

拠点名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

ＤＳＧ加入管理番号＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿（利用申請後で加入管理番号が払い出されている場合のみご記入ください）

申請者氏名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

E-mail＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

１．可搬記憶媒体情報

本申請により登録/削除する可搬記憶媒体の総数　→　　個

可搬記憶媒体として登録又は削除する各メディアの情報をご記入ください。

登録又は削除申請の対象となるメディアは、**利用端末にＵＳＢ接続し利用する記憶媒体**です。

例）ＵＳＢメモリ、光学ドライブ（ＣＤ－ＲやＤＶＤなどの書き込み用）、ポータブルハードディスク、メモリーカード

可搬記憶媒体は申請前に初期化してください。

１０個目以降の情報については「複製用」のシートを適宜コピーした上でご記入ください。

登録／削除希望日
令和　　年　　月　　日

申請理由／目的

No.	登録／削除	USBデバイス名	ベンダID	プロダクトID	シリアルNo	利用端末ホスト名
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

２．自由記載欄

上記記載事項の補足及び連絡事項などがありましたらご記入ください。

サービス提供事業者作業報告欄

下記の通り作業を完了いたしました。

作業完了日	作業者	確認日	確認者
備考欄			