

## 防衛セキュリティゲートウェイ（DSG）に関するFAQ 【令和6年2月1日時点】

分類	公開用質問	回答
1	DSGへの加入 加入時点において履行中の契約がない（受注前）場合であっても、加入申請及び回線敷設工事は実施可能ですか。	契約締結（受注）が見込まれるのであれば加入申請を先に受け付けるケースもあり得ます。加入申請を受け付けた後、どのような装備品のどのような作業において、どのような保護すべき情報を扱うことが見込まれるか等を把握確認し、工事の必要性及び実施時期を判断します。
2	DSGへの加入 今後DSGを使用する取引が発生することを見越して加入申請及び回線敷設工事を行った場合、結果的にDSGを利用しない状態が続いても問題ありませんか。	国費の有効活用の観点から、会社として、DSGの利用（保護すべき情報の電子データでの受け渡し）が十分に見込まれる場合に申請を行っていただくようお願いします。また、官側においても必要な確認等を行います。（No.1の回答も参照ください。）
3	DSGへの加入 「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」は防衛調達の業務に従事する部門のみ対応すればよいですか。	「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」（実施要領）は、防衛調達に関する保護すべき情報をシステム上で取扱う場合に、当該情報システムのセキュリティ確保に関して必要な事項を定めるものとなります。よって、実施要領の対象範囲は保護システムを扱う全ての部門となります。
4	DSGへの加入 経過措置で旧基準を適用中の場合、DSG利用の前提となる物理的及び環境的セキュリティも旧基準のもので問題ないでしょうか。	DSG利用の前提となる物理的及び環境的セキュリティは新基準（取扱施設として確立された場所、および入退室において個人特定をすること）が望ましいですが、経過措置においては、旧基準に示す対策が講じられていればDSG利用は可能です。
5	DSGへの加入 複数拠点の加入要望がある場合、1企業から複数拠点分の申請をすることは可能ですか。	可能です。
6	DSGへの加入 DSGの提供サービスである「加入支援」は、運用開始後であっても利用可能でしょうか。	利用可能です。
7	DSGへの加入 加入申請及び利用申請のリードタイムを教えてください。	事前現地確認後から回線敷設までにおおむね3～4カ月要します。（ただし、状況により前後します。） そのため、必要な事務処理の期間も踏まえ、導入時期から逆算してご検討ください。
8	DSGへの加入 加入申請について、申請受付時期を教えてください。随時受け付けていますか。	随時申請が可能で、随時受け付けます。
9	DSGへの加入 8月29日付のご案内資料の中に、「情報セキュリティ特約条項第9条に基づき適用の特例を申請し、それが認められた場合は、当該期間中は、旧基準に示す対策が講じられていればDSGは利用可能とします。」とあります。 弊社では当面の間、旧基準での対応が認められております。物理セキュリティ面でも現行環境（鍵による施錠管理。監視カメラはなし）でも良いとの理解で合っていますでしょうか。	ご理解のとおりですが、事業計画に基づき計画的な新基準への移行をお願いします。

## 防衛セキュリティゲートウェイ（DSG）に関するFAQ 【令和6年2月1日時点】

分類	公開用質問	回答
10	DSGへの加入 旧基準での対応環境下でDSGを利用することにした場合、保護システム関連が大きく変わりますので、旧基準ベースの社内規程（実施手順等）について保護システム関連の部分を更新することが運用前に必要となる、との理解で合っていますでしょうか。	ご理解のとおりです。
11	DSGへの加入 防衛関連企業側で用意する各種機器等の準備時期について、物理的及び環境的セキュリティを確認する官側事前現地確認までに揃っている必要がありますか。	官による現地確認時までにはすべての機器が揃っている必要はありませんが、機器のセットアップや設定の関係上、通信ルータの設置までには準備をいただくようお願いします。
12	DSGの利用 DSGを利用しての情報の受け渡しの要否の判断は誰が行うのでしょうか。	保護すべき情報の受け渡し方法に関して要求元から指示（要望）があることも想定されますので、個々の契約において要求元と調整を行ってください。
13	DSGの利用 DSGは地方調達（自衛隊基地での契約など）でも利用可能でしょうか。	中央調達、地方調達を問わずDSGは利用できます。
14	DSGの利用 DSGは防衛関連企業でない団体（一般社団法人等）でも利用できますか。	保護すべき情報を取り扱う可能性がある場合は、利用は可能です。
15	DSGの利用 下請企業もDSGの利用申請を行えますか。また、企業間でのデータ共有はできますか。	下請企業からの利用申請も行っていただけます。企業間のデータ共有は、双方の企業がDSGを利用可能な環境が整っており、かつ「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」（情報セキュリティ特約条項）が付帯された同じ契約に双方が利用者として登録されていれば可能です。
16	DSGの利用 プライム企業と下請企業がDSGを利用する場合、プライム企業側でまとめて申請すべき、下請企業が申請すべきといった推奨はありますか。	プライム企業がまとめて申請をお願いいたします。
17	DSGの利用 利用申請から利用開始までにどのくらいの日数がかかりますか。	申請する利用者数等にもよりますが、利用申請からアカウント付与まで概ね1週間程度を見込んでいます。
18	DSGの利用 初回利用時、環境整備と並行して利用申請（ID等の交付申請）を行うことはできますか。	利用申請は契約締結日以降に行ってください。
19	DSGの利用 利用申請を契約の都度ではなく年度毎にまとめて行うことはできますか。	契約により利用者が異なること、契約毎のアクセスエリアを区分するため、年度毎の申請はできないものと考えています。契約毎に利用申請を行っていただくようお願いします。
20	DSGの利用 同一人物（作業従事者）が異なる契約に携わる場合、契約毎に異なるDSG用のユーザーIDが払い出されますか。	ご認識のとおりです。案件毎、利用者毎にアカウントを付与します。
21	DSGの利用 利用端末のOSのアカウント管理（アカウントの登録、停止、パスワードの配付等）は企業側が行うことになりますか。	OSのログオンアカウントの管理は企業側で行っていただくことを想定しています。
22	DSGの利用 特約条項が付帯された契約の契約期間（契約締結日～最終納期）に対してDSGを利用できる期間を教えてください。また利用期間終了後はDSGに保存したデータへアクセスすることは可能でしょうか。	契約後、利用申請を行っていただき、IDやパスワード等の必要な情報を受領後利用可能となります。また、契約履行期間終了後も、一定期間（土日を含めない14日間）はアクセス可能とすることを予定しています。

## 防衛セキュリティゲートウェイ（DSG）に関するFAQ 【令和6年2月1日時点】

	分類	公開用質問	回答
23	DSGの利用	契約終了後のDSG内の領域や保護すべき情報の取り扱いはどのようになりますか。	契約履行期間終了後も、一定期間（土日を含めない14日間）はアクセス可能とすることを予定しています。 一定期間経過後は、データの復旧や取り出しの要望は受け付けません。
24	DSGの利用	契約終了後に防衛関連企業側で外付けHDD等に保護すべき情報を移管した場合、当該情報は、特にDSGの利用期間中でなくともDSG端末で閲覧できますか。	可搬記憶媒体に保管した情報は、保護システム内で閲覧等は可能です。
25	DSGの利用	情報セキュリティ特約が付帯した契約した事業が契約満了になった場合、通信ルータは返納する必要があるのでしょうか。	今後も情報セキュリティ特約を締結する予定がある場合は、通信ルータはそのまま設置したままにし、ネットワークを遮断する予定です。防衛事業から撤退するなどにより、情報セキュリティ特約を今後長期にわたり締結する予定がなくなった企業については、通信ルータを回収する予定です。
26	DSGの利用	端末のアップデート等実施のため、契約に紐づかなくても、保護システム管理者や担当者にDSGのアカウントを払い出して頂くことは可能でしょうか。	DSG加入時の接続確認のため、保護システム管理者等にアカウントを払い出すこととなります。契約の有無にかかわらず、それをを用いてポータルサイトにアクセスいただけます。
27	DSGの利用	利用申請について、ベンダの追加・削除は随時申請可能ですか。	随時申請が可能です。
28	DSGの利用	どのような契約であっても、官側はDSGを利用する体制が整っている認識で合っていますか。	ご認識のとおりです。
29	DSGの利用	端末PCは使わないときには電源OFFにする運用でしょうか。それとも、24時間365日、電源ONにする必要があるでしょうか。	日々の業務終了後は電源を落としていただいておりますが、長期間に渡り利用端末を使用しない場合は、セキュリティパッチやウイルス定義体を最新化するため、定期的に起動するようにお願いします。
30	DSGの利用	利用申請書等、申請をする者は誰か決まっていますでしょうか。申請者はDSGアカウント情報を知る（プライムはベンダ分も）事になりますので、保護システム管理者（アカウント管理者）等を指定して実施させる等が必要になるかと存じます。	別途ご提示する運用管理要領等において規定しますが、保護システム管理者から実施いただくことを想定しています。
31	DSGの利用	登録できる利用者数に制限はあるのですか。プロジェクト離脱等にもなう利用者の削除の手続きはあるのですか。	利用者数の制限は特段ございません。利用者の増減時の申請書があります。
32	アクセス制御・権限	要求元からの保護情報の配付や、防衛関連企業の契約終了時の納入・提出をDSGにて行うことは可能ですか。要求元も同じ領域にアクセス可能でしょうか。	いずれも可能です。
33	アクセス制御・権限	プライム企業と下請企業は、DSG内に保管される保護すべき情報に対して同じアクセス権限が付与されますか。	プライム企業と下請企業の双方がアクセスできる領域内の保護すべき情報に対しては、同じアクセス権限が付与されます。契約毎利用者毎にアカウントが付与され、アクセス権限がある領域にのみに入れる設定です。
34	アクセス制御・権限	DSGのシステム運用管理担当者は保管されるデータの閲覧権限を持っていないという理解で良いでしょうか。	管理業務の一部はSOCとして部外委託となりますが、フォルダ内情報の保全は官側で規定し順守させることとします。
35	アクセス制御・権限	フォルダへのアクセス権限に関し、各利用者が許可されている作業を指定して設定を行うことは可能でしょうか。（例：利用者Aは閲覧、編集、アップロード、印刷が可能、利用者Bは閲覧のみ可能等）	設定は、利用者の行為ではなく、アクセス権限（誰がどのフォルダにアクセス可能か）の単位になります。

## 防衛セキュリティゲートウェイ（DSG）に関するFAQ 【令和6年2月1日時点】

	分類	公開用質問	回答
36	アクセス制御・権限	利用者が作成したフォルダへのアクセス権限の申請方法を教えてください。	「アクセス権限設定申請書」を提出いただけます。
37	アクセス制御・権限	DSGの共有フォルダは自由に作成できるかと思いますが、アクセス制限についても申請すれば自由に設定できるのでしょうか。 企業側で作成したフォルダについて、特定のユーザー間だけアクセスさせたい場合の制御もできるのでしょうか。	「アクセス権限設定申請書」を提出いただければ設定が可能です。
38	暗号化	企業側に設置する利用端末に対しては、DSG側から必要な暗号化ツールは提供してもらえますか。	暗号化はDSG側で行うことを想定しています。
39	暗号化	DSGで保管されるデータは暗号化されていると想定しておりますが、利用端末から可搬記憶媒体に書き出す前に復号されるのでしょうか。また、暗号化の方式（利用権付暗号化、パスワード設定等）を教えてください。	可搬記憶媒体に書き出す際に暗号化し、パスワードにより復号化します。
40	暗号化	DSGでは暗号化を行うとのことですが、暗号キーのコントロール権限は防衛関連企業側で管理できるのでしょうか。	DSG側で管理します。
41	暗号化	DSGから提供されるUSBメモリ等可搬記憶媒体への暗号化機能について、DSGにログインしていない状態でも利用端末上で復号できますか。また、DSGに接続していない社内の別の保護システムでもこの暗号は使用（USBメモリでの暗号化/復号）できますか。	可搬記憶媒体にデータを保存する際の暗号鍵は都度設定する形になります。また、DSGにログインしていない状態で復号可能です。
42	暗号化	可搬記憶媒体で保存する際の暗号化機能を提供頂けるとのことですが、暗号の単位がファイル一つ一つに対してなのか、フォルダ単位で一括して暗号化されるのかをご教授頂きたいと願致します。大量のファイルを一括してやり取りすることを想定しており、一括での暗号化を希望致します。	一括での暗号化も可能です。
43	インシデント対応	インシデント等が検知され、防衛関連企業側に通知された場合、対応に求められる速度の目安を教えてください。	インシデントの対応速度に関しては、防衛産業サイバーセキュリティ基準に則り対応してください。
44	インシデント対応	ネットワーク障害等により保護すべき情報の通信が不可能となった場合を考慮し、端末内に保存された保護すべき情報を外部記憶媒体へ出力することは可能でしょうか。	可能です。
45	インシデント対応	2023年12月実施の説明会資料「防衛セキュリティゲートウェイの利用について」のp.13に記載の表中 第8章 3項目 DSGが提供するサービス「不正な通信の遮断、感染した端末の隔離」について、防衛関連企業側の対応として、接続線脱却等の物理的隔離は不要でしょうか。	ウイルス感染の兆候が確認された場合には、影響拡大を防止するため、速やかに感染端末のケーブルを抜線する等し、感染拡大防止に努めてください。

## 防衛セキュリティゲートウェイ（DSG）に関するFAQ 【令和6年2月1日時点】

	分類	公開用質問	回答
46	回線敷設工事	回線敷設工事の概要と費用負担について教えてください。	加入申請後敷設工事実施の決定後、現地調査を行い、どのような工事が必要かを決定します（設置工事、付帯工事等）。その後、工事実施日を企業側と調整の上決定し、工事を実施することになります。なお、必要に応じ、企業担当者及び建物所有者等の立ち会いをお願いします。工事完了確認は官側で行います。現地調査の結果、防衛関連企業において付帯工事を実施する等の対応を求める場合がございます。
47	回線敷設工事	取扱施設を2年後に更新する予定です。2年後でも回線設置工事の対応は可能でしょうか。	対応可能です。利用希望の時期を踏まえ、適切な時期に加入申請を行って下さい。
48	回線敷設工事	通信ルータから利用端末までの間のLAN配線ルートに保護情報取扱施設以外の区画が含まれても問題ないでしょうか。	原則として、ルータから利用端末までの間のLAN配線ルートも含めた全てを保護情報取扱施設内で設置する予定です。
49	回線敷設工事	有線の回線敷設工事が難しい場合、無線での対応も可能ですか。	現段階では無線の利用を想定しておりません。
50	回線敷設工事	提供いただける通信ルータは一台だけでしょうか。	拠点数や規模等にもよるため、状況に応じて検討いたします。
51	回線敷設工事	「付帯工事」とはどのような工事が想定されますか。	光回線を引き込むにあたっての配管や保護器具（ダクトやモール）、配線の為の壁や天井の穴あけ等が必要な場合が想定されます。
52	回線敷設工事	複数拠点でDSGを利用する場合、各拠点の工事は対応していただけるのでしょうか。	各拠点で現地確認を実施し、それぞれ工事の要否を判断のうえ、対応します。
53	機器・ソフトウェア	利用端末の設置台数に制限はありますか。	特に台数の制限はありません。
54	機器・ソフトウェア	利用端末や認証用機器のスペックが提示される際に、各機材のシステム設定についても条件等が提示されるのでしょうか。	必要な機器やその仕様等については、防衛装備庁ホームページに掲載する最新版の資料を参照してください。
55	機器・ソフトウェア	アンチウイルスソフトウェアはDSG側、企業側のどちらで用意しますか。	アンチウイルスソフトウェア及びアンチウイルスソフトウェアのアップデート等は、DSG側から加入企業へライセンスと定義ファイル等を配布することを予定しております。
56	機器・ソフトウェア	利用端末でインストールできるソフトウェアはどのようなものがありますか。	独自のソフトウェアについては、防衛関連企業からの申請に基づいて、個別に防衛省側で許可します。
57	機器・ソフトウェア	利用端末のソフトウェアやOSのアップデートはどのように行いますか。	基本的に、利用端末等のスペックを提示する際に併せて示すソフトウェアやOSのアップデートはDSG側で行いますが、企業で個別に許可を受けてインストールしているソフトウェアは企業でアップデートを行っていただくことになります。

## 防衛セキュリティゲートウェイ（DSG）に関するFAQ 【令和6年2月1日時点】

	分類	公開用質問	回答
58	機器・ソフトウェア	防衛関連企業側が独自で使用するソフトウェアの費用は負担いただけますか。	防衛関連企業側が独自で使用するソフトウェアに要する費用は本DSG事業での負担はございません。企業負担で準備いただきます（本事業以外の防衛省の支援措置の対象となる場合があります）。
59	機器・ソフトウェア	認証用機器も各防衛関連企業で用意しますか。また、機器の仕様を教えてください。	認証用機器も企業側で準備いただくこととなります。DSGで導入する認証システムについては、加入申請を受けた評価後に細部を提示します。
60	機器・ソフトウェア	専用のプリンター／複合機を設置することは可能ですか。	プリンター／複合機の接続は可能です。必要なプリンタドライバは、ソフトウェアのインストールとして必要な申請、許可を受けて下さい。操作ログはDSGで収集、管理します。なお、出力した情報は防衛産業サイバーセキュリティ基準に基づき適切な管理を行ってください。
61	機器・ソフトウェア	利用端末のローカルディスクにデータを保存する際のファイルの暗号化ソフトウェアは企業側で準備しますか。推奨する暗号化ソフトウェアはありますか。	ホワイトリストには、暗号化ソフトウェアも含まれます。
62	機器・ソフトウェア	防衛省から提供される通信ルータ、通信ルータ用セキュリティラック、防衛関連企業側で用意する利用端末は、取扱施設内に設置しなければなりませんか。	ご認識のとおりです。
63	機器・ソフトウェア	利用端末内の保護すべきデータを削除するためのデータ消去ツールやプリンタドライバーは申請不要のソフトウェアに含まれますか。	ログオフ／シャットダウン時のデータ消去ツールはDSGのサービスとしての提供を検討中です。端末を初期化する際のデータ消去については提供の予定はありません。また、ソフトウェアは申請によりインストールしていただくこととなりますので、プリンタドライバーにつきましても同様に申請いただきます。
64	機器・ソフトウェア	可搬記憶媒体の登録が必要とのことですが、外付けのCD／DVDドライブの登録も必要でしょうか。	外付けのCD／DVDドライブはハードウェアとなりますので、登録は不要です。なお、CD／DVDは閲覧用となり、書き込みは制限されています。
65	機器・ソフトウェア	DSGから提供される導入必須ソフトウェアが、どのような機能を有し、導入することで防衛産業サイバーセキュリティ基準のどこに対応するのかを示していただくことは可能でしょうか。	加入申請を受けた評価後に個別に提示します。
66	機器・ソフトウェア	通信ルータ用セキュリティラックは、取扱施設内に設置していても更に施錠可能なことが必須でしょうか。	産業サイバーセキュリティ基準に基づき、施錠は必須とします。
67	機器・ソフトウェア	官側から提供する導入必須ソフトウェアについて、ベンダ（下請負者）への配布やアップデートはどのように行いますか。	DSGから提供するソフトウェアやウイルスパターンへの更新は、プライム／ベンダの別に関わらず加入拠点ごとに、オンラインで自動実行されます。
68	機器・ソフトウェア	「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）」の提示時期を教えてください。	ホワイトリスト・ブラックリストは、初期セットアップ手順書等配布時に、メディアに格納して展開しますが、最新版はマニュアル格納サイト等でも公開致します。
69	機器・ソフトウェア	防衛関連企業側で準備する機器等のスペック情報はどこで確認できますか。	防衛装備庁のホームページに掲載しております。 <a href="https://www.mod.go.jp/atla/dsg.html">https://www.mod.go.jp/atla/dsg.html</a>

## 防衛セキュリティゲートウェイ（DSG）に関するFAQ 【令和6年2月1日時点】

	分類	公開用質問	回答
70	機器・ソフトウェア	官側から提供する導入必須ソフトウェアの導入や運用に係る費用はDSG側で負担していただけますか。	導入必須ソフトウェアの導入・運用に係る費用はDSGで負担します。ただし、導入に際し必要となる作業（インストールや設定など）に費用を要する場合は、企業側の負担となります。
71	機器・ソフトウェア	スペック要件としてUSBに「TYPE-A」とありますが、「TYPE-C」は使用可能でしょうか。	静脈認証用機器をUSB接続する場合を考慮し、TYPE-Aの記載をしております。ハブを経由して接続することも可能と思われませんが、動作を保証できません。
72	機器・ソフトウェア	利用端末はデスクトップ型、ノート型それぞれ選定可能でしょうか。	デスクトップ型でもノート型でも性能要件を満たしていれば問題はありません。
73	機器・ソフトウェア	利用端末の製造メーカーで選定不可のメーカーはありますか。	利用要領の機器の要件に関する条項をご参照ください。
74	機器・ソフトウェア	利用端末は契約毎に用意する認識だが、契約終了後は使い回しをして良いでしょうか。	問題ありません。
75	機器・ソフトウェア	防衛関連企業独自のソフトウェアのインストールや脆弱性への対応のため、インターネットに繋いで必要なファイルのダウンロードが必要な場合の手続きや要領を教えてください。	企業独自のソフトウェアのインストールには申請が必要となりますが、オンラインのみのアップデートとなるようなソフトウェアは承認されません。
76	機器・ソフトウェア	保護システム端末の交換、破棄の際は、記憶媒体の破棄も必要ですか。	記憶媒体の破棄は必須ではありません。破棄する際、記憶媒体への処置については、登録削除の申請書に項目を設けているため、そちらで把握する想定です。
77	機器・ソフトウェア	利用端末の要件に関する質問です。 2023年12月実施の説明会資料「防衛セキュリティゲートウェイの利用について」P23に端末要件が記載されていますが、近年リースを開始した当社標準仕様のノートPCでは、GPU性能が要件を満たしていませんでした。 やはり厳密に要求を満たしていないPCは使用しない方が良いのか、要件未達（CPU性能）の端末使用での問題点等について、ご教授頂けると助かります。	端末要件は、導入必須ソフトウェアのシステム要件を基に算出していますので、ご用意いただく端末のスペックがDSG側からご提示している端末要件に満たない場合、その動作に支障（動作が重くなる、予期せぬエラーの発生等）が出る恐れがあります。
78	機器・ソフトウェア	利用する可搬記憶媒体（USBメモリ等）をDSG側に登録すれば未登録媒体をPCIに接続しようとするエラーとなるように制限はしますでしょうか。 DSG未接続状態のDSG接続PCなら未登録媒体でも利用できますでしょうか。	未登録の可搬記憶媒体を端末に接続した場合、エラー画面が表示されて利用できません。DSG未接続状態でも同じです。
79	機器・ソフトウェア	ルーターラックについて、「搭載1Uの上下に1ずつ空いている事」と指定されていますが、理由をご教授ください。	ケーブル取り回し（ONU設置含む）、排熱の観点からの推奨事項となります。

## 防衛セキュリティゲートウェイ（DSG）に関するFAQ 【令和6年2月1日時点】

	分類	公開用質問	回答
80	機器・ソフトウェア	端末故障等にもない利用端末を削除する手続きはあるのですか。	利用端末の増減時の申請書があります。
81	機器・ソフトウェア	利用端末の購入にあたり仕様を検討し、USBポートの不足が懸念されました。USBポートの不足を解消するため、USBハブを利用したいと考えております。利用端末にてUSBハブの利用は可能でしょうか。また、利用端末にUSBにて接続する機器は可搬型記憶媒体（USBメモリ）と同様に登録申請することで利用可能となるという認識でよろしいでしょうか。	・USBハブの利用は問題ございません。 ・利用端末にUSBポートにて接続する機器のうち、記憶領域を持つものは可搬型記憶媒体登録申請をすることで利用可能となります。
82	識別・認証	DSGへアクセスする際のMFA（多要素認証）について、認証方式や登録方法を教えてください。	多要素認証として、知識情報と生体情報による認証を行うこととしています。なお、生体認証の方法やその登録方法等々の詳細については、セットアップ手順書や利用マニュアルにて、別途お知らせします。
83	識別・認証	静脈認証用機器について、「DSGで導入する認証システムに対応する機器」のスペックや規格を具体的に提示してください。	認証用機器のスペックやその適合品は、加入申請を受けた評価後に個別に提示します。Webカメラについては特に推奨製品はございません。外付け型、内蔵型のいずれでも可能です。
84	識別・認証	表中 第6章 DSGが提供するサービス「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」において、端末への機能実装は官の作業による実装（インストール含む）でよろしかったでしょうか（弊社作業は不要でよろしかったでしょうか）。DSGが提供するサービスとして表に記載されていたため、念のためご確認するものです。	インストーラや設定手順等はDSGから提供しますが、端末へのインストール作業や設定は加入企業側で実施いただけます。
85	識別・認証	「静脈認証時の本人確認を行うための機器」としてWebカメラの用意が求められていますが、同機器の用途を教えてください。	静脈登録時の登録者の本人確認、本人による登録手続の確認のためにWebカメラを利用します。ログイン時は登録した静脈認証を使用するため、ログインの度にWebカメラを使用することはございません。
86	識別・認証	Webカメラを使用した静脈認証時の本人確認のイメージを教えてください。	利用登録者ご本人の顔画像と、免許証や社員証等の写真付き身分証とを横並びに見て確認するとともに、確認できた本人に登録作業を実施していただくことを想定しています。
87	識別・認証	複数契約を担当する利用者について、契約毎に複数のアカウントが付与されますか。また、その都度生体認証登録を行う必要がありますか。	複数契約を担当する利用者には、複数のアカウントが付与されます。一方、生体認証登録は初回利用時の一度のみであり、当該登録情報に複数のアカウントを紐づける措置を行います。
88	識別・認証	利用者の静脈認証登録の流れ、登録後のログオン時の認証の流れを提示してください。	別途ご提示する利用要領や利用マニュアル等において規定します。
89	識別・認証	静脈認証は、Windowsのログインに使用できますか。	端末起動時に静脈認証及びWindowsログイン認証を行います。そのため、DSGを利用する場合はドメインのユーザで、ローカルを使用したい場合はローカルユーザでログインいただくこととなります。（ローカルユーザの場合は静脈認証不要とするよう手順を定める予定です。）
90	識別・認証	SSOでDSGまでアクセス可能でしょうか。その場合、ドメインアカウントのIDの管理やドメインサーバはDSGで対応・管理していただけますか。	ご認識のとおりです。



## 防衛セキュリティゲートウェイ（DSG）に関するFAQ 【令和6年2月1日時点】

	分類	公開用質問	回答
91	情報の取り扱い	DSGは保護すべき情報以外の情報の共有にも利用できますか。	保護すべき情報以外の情報（業務上のやり取りの中で必要な情報等）の共有でのDSG利用も可能です。他方で、システム上、保護情報とそれ以外の情報の区別が困難であるため、DSGを利用してやり取りする情報は、保護情報でなくとも基本的には保護情報とみなして取り扱っていただくことを考えています。
92	情報の取り扱い	会社保有の技術情報が防衛省殿の規則等で「秘」又は「注意」（部内限り含む）に該当するような内容のものである場合、DSG上で取り扱うことは可能でしょうか。	「注意」は利用可能ですが、「秘」以上はDSG上で取り扱うことはできません。
93	情報の取り扱い	DSGの運用開始以降は、紙媒体による保護すべき情報の受け渡しはなくなるのでしょうか。	従来どおり、紙媒体での受け渡しも可能です。
94	情報の取り扱い	保護すべき情報を紙媒体のみで受け渡しする場合、DSGの申請は不要という認識でよいでしょうか。	ご認識のとおりです。
95	情報の取り扱い	大容量データ且つ多量のファイルをDSGで授受する場合、従来通りHDDを手持ちで運搬する運用を併用して行うことは可能でしょうか。	状況に応じ、適切に使い分けを行っていただいても構いません。
96	情報の取り扱い	DSG上の保護すべき情報について、管理状況（接受、閲覧、送達、破棄等）はDSG側のログとして記録されるため、防衛関連企業側で目録を作成する必要はないということでしょうか。	防衛関連企業での目録の作成に必要な情報は、DSG側から提供する予定です。
97	情報の取り扱い	保護すべき情報が含まれる成果物等を提出する際は、「官民情報共有機器」に保存することで受け渡しを行うということでしょうか。	DSGを用いて共有する場合はご理解のとおりです。
98	情報の取り扱い	異なる契約を跨いだ共通の区画を作成することは可能でしょうか。	基本的に契約期間での利用を想定しているため、現時点では事業をまたがる共通の区画を設けることは考えておりません。
99	情報の取り扱い	DSG内のデータの編集はどのように行いますか。	DSGサーバー内においてはデータ編集はできません。利用端末にダウンロード又は可搬記憶媒体で防衛関連企業の保護システムに移動し編集することは可能です。編集後はDSGサーバーに保存してください。
100	情報の取り扱い	利用端末にダウンロードしたデータは閲覧・編集後に削除されますか。	端末にダウンロードしたデータは、ログオフ、シャットダウンするときには、データの削除を行うこととなります。具体的な手順は、別途お示しします。
101	情報の取り扱い	説明会にて、利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や、データのDSGへのIN/DSGからのOUTは可搬記憶媒体で行うとありますが、これらは恒久的な措置でしょうか。将来的に条件が整えば企業側の保護システムと接続できるようになる可能性はありますか。	今後の拡張性については、利用者の要望を踏まえ検討します。
102	情報の取り扱い	日を跨ぐ編集作業を行う場合、利用端末のCドライブ等に置いたままの作業、または登録済のUSBメモリ等に保管しながらの作業は可能でしょうか。	ログオフ・シャットダウン時にはデータの削除をしていただくこととなります。端末のローカルディスクにデータを残置することは、情報保証の観点から認められません。
103	情報の取り扱い	官側と共有するフォルダに官側が保存したデータについても、防衛関連企業側の保護すべき情報の目録に含める必要があるのでしょうか。	DSG上の保護すべき情報は官側で管理し、要すれば保護すべき情報の目録を加入企業に情報提供します。

## 防衛セキュリティゲートウェイ（DSG）に関するFAQ 【令和6年2月1日時点】

	分類	公開用質問	回答
104	情報の取り扱い	「特定の拡張子（プログラム「.exe」やスクリプト「.ps1,.vbs」、メールアドレス「.eml,.msg」等）のデータはアップロードできません」とありますが、これらのデータをやり取りする場合は、DSGを使用せずに媒体等でのやり取りと考えると良いのですか。	そうした運用も可能です。
105	脆弱性診断	利用端末の脆弱性診断は、DSG側からリモートで実施しますか。それとも防衛関連企業側で実施しますか。	DSG側からリモートで実施します。
106	脆弱性診断	脆弱性スキャンの対象は何ですか。	SOCから把握できる範囲はネットワークスイッチも含め全て対象とする予定です。細部は別途お示しします。
107	脆弱性診断	脆弱性スキャンの結果はどのように通知されますか。	通知方法については現在検討中です。
108	その他	DSG利用に際し、防衛関連企業側で保護システム管理者を指定する必要がありますか。	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が前提となるため、新基準に従いシステム管理者の指定をしていただきます。
109	その他	DSG利用範囲に関わる防衛関連企業側の費用負担（器材等）について、防衛省の支援措置の対象となりますか。	ご認識のとおり、2023年6月実施の説明会資料p.3に記載の「④取扱者用情報通信機器」については防衛省の支援措置の対象となる可能性があります。個別案件の内容によりますが、財政措置の活用を検討されている具体的案件がありましたら個別にご相談いただければと存じます。財政措置の活用を検討される場合は、防衛装備庁Webサイトの“防衛生産基盤強化法について”ページから個別にご相談ください。経費率に関する件は、防衛装備庁HPの防衛産業サイバーセキュリティ基準相談窓口（industrial-cybersecurity-office@ext.atla.mod.go.jp）にお問い合わせください。
110	その他	利用端末は防衛関連企業の保護システムという位置付けであり、即ちシステムセキュリティ実装計画書の作成・提出が必要でしょうか。必要な場合は記入要領は今後示されますか。また、防衛省実地監査の対象となりますでしょうか。	ご認識のとおりです。防衛省実地監査の対象となります。なお記入要領については、別途提示する予定です。
111	その他	システムセキュリティ実施要領「第3 構成管理」に、ソフトウェアのバージョン変更（構成変更）の場合も含まれますか。またこれに伴う構成設定目録の更新も防衛省への報告する必要がありますか。	独自にインストールしたソフトウェアのバージョン変更を含みます。また、構成設定目録の更新も報告する必要があります。細部は別途お知らせします。
112	その他	利用端末の時刻の同期は、DSG側にNTPサーバを立てて提供するのでしょうか。防衛関連企業側で実施するのでしょうか。	DSG側で実施します。
113	その他	コミュニケーションツール（Web会議、メール等）の導入予定はありますか。	コミュニケーションツールも含め、拡張性については、利用者のニーズを踏まえ、今後サービスとしての導入を検討していきます。

## 防衛セキュリティゲートウェイ（DSG）に関するFAQ 【令和6年2月1日時点】

	分類	公開用質問	回答
114	その他	サテライトオフィスは設置される予定ですか。	拡張性については、利用者のニーズを踏まえ、今後サービスとしての導入を検討していきます。
115	その他	DSGの官側内部（省内）向けの説明はいつ頃を想定していますか。	随時実施しております。
116	その他	DSGのストレージ容量が多い場合、加入企業側による負担の変化はありますか。	ストレージサーバを含め、DSGの機能は、防衛省側で整備し無償で提供しますので、加入企業側に負担はないと考えております。
117	その他	DSGのストレージの利用容量について、事業途中からの容量の変更は可能ですか。	可能です。
118	その他	SOCは防衛省内に設置しますか。また、SOC業務は防衛省職員が実施するのですか。	防衛省職員において人的な管理ができるように、SOCは防衛省職員が監督できる場所に設置する予定です。SOC業務については、大部分を民間に委託する予定です。
119	その他	DSGは企業内のローカルネットワークに接続できますか。	社内LAN等には接続できません。
120	その他	論理的にネットワークを分離する等の形で企業側の保護システムに接続することは可能ですか。	旧情報セキュリティ基準適用中の場合、ネットワーク接続は基本的に不可です。新情報セキュリティ基準適用中の場合、官側の審査（接続方式やデータが混ざらない仕組み等）を経て許可します。
121	その他	2023年12月実施の説明会資料「防衛セキュリティゲートウェイの利用について」p.4で、DSGに「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」は接続できるとしつつも、p.22、p.26では、プリンター、スキャナについてはUSB接続に限るとしています。複数の利用端末で印刷する場合は、いちいちUSBケーブルを差し替える必要がありますか。プリンターをネットワークSWに接続してはいけなんでしょうか。	旧情報セキュリティ基準適用中の場合、ネットワーク接続は基本的に不可です。新情報セキュリティ基準適用中の場合、官側の審査（接続方式やデータが混ざらない仕組み等）を経て許可します。
122	その他	2023年12月実施の説明会資料「防衛セキュリティゲートウェイの利用について」p.22、p.26では、プリンター、スキャナについてはUSB接続に限るとしていますが、DSGに接続する利用端末をクローズドなネットワークで構成した場合、1台の利用端末に接続したプリンター、スキャナーをネットワーク共有して使用することは可能ですでしょうか。	旧情報セキュリティ基準適用中の場合、ネットワーク接続は基本的に不可です。新情報セキュリティ基準適用中の場合、官側の審査（接続方式やデータが混ざらない仕組み等）を経て許可します。
123	その他	『DSGへ接続可能な情報システム』について、6月のFAQ_53では「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や、データのDSGへのIN/DSGからのOUTは可搬記憶媒体で」でしたが、今回、基準を満たす企業側のクローズド保護システムはネットワーク接続が可能と変更された理解でよいでしょうか。	旧情報セキュリティ基準適用中の場合、ネットワーク接続は基本的に不可です。新情報セキュリティ基準適用中の場合、官側の審査（接続方式やデータが混ざらない仕組み等）を経て許可します。
124	その他	ネットワークスイッチに接続した複数の利用端末間での通信・アクセスは可能でしょうか。DSGから利用端末Aにダウンロードしたデータを、利用端末B・C・Dが共有して閲覧や編集作業を行うことが可能でしょうか。	旧情報セキュリティ基準適用中の場合、ネットワーク接続は基本的に不可です。新情報セキュリティ基準適用中の場合、官側の審査（接続方式やデータが混ざらない仕組み等）を経て許可します。
125	その他	保護すべきデータを扱う防衛関連企業にとって、DSGへの加入は義務でしょうか。	加入義務とすることは考えておりませんが、可能な限りDSGをご利用いただきたいと考えております。

## 防衛セキュリティゲートウェイ（DSG）に関するFAQ 【令和6年2月1日時点】

	分類	公開用質問	回答
126	その他	防衛省内はDSGとDIIが繋がっていますが、装備庁殿は要求元となる防衛省内各部署に対しても、積極的にDSGを使って保護情報データを官民で共有して行くようにご指示または推奨されているのでしょうか。今後、要求元が企業側へ加入を強く要望する流れもあり得るのでしょうか。	防衛省内の各機関各部署に対しても、DSGの利用を推奨しております。そのため、ご認識のような、要求元からの要望ということもあり得ると考えています。
127	その他	新情セキ基準が求める多要素認証やシステム常時監視、監視カメラ等の物理的環境が整っているかどうかを官側で現地確認をお願いする時の調整窓口はどこになりますか。	防衛装備庁情報システム管理室になります。（防衛装備庁ホームページをご覧ください。）
128	その他	現在、政府クラウドで国内企業が採用されたらと話題になっていますが、防衛セキュリティゲートウェイのクラウドサービスはどちらの企業のサービスを利用されるのでしょうか。	サービス提供の防衛省との契約相手方は富士通株式会社です。
129	その他	「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。」とありますが、WindowsOSのサーバはDSGでの監視対象にはならない、との理解で合っていますでしょうか。また、要望ですが、現状ではWindowsOSのサーバはDSG監視対象にはならないが正しいとして、今後、DSG監視対象に加えていただくことを希望いたします。	防衛関連企業内の自社サーバはDSGによる監視対象外となります。ご要望については今後の検討といたします。
130	バックアップ	利用端末のシステムデータのバックアップは防衛関連企業側で行いますか。	利用端末のシステムデータのバックアップは企業側で実施していただきます。
131	バックアップ	バックアップの世代数の指定などはありますか。	必要な世代管理は実施する予定です。細部は別途お示しします。
132	ログ	利用端末へのエージェントインストールやログの提出は必要ですか。	利用端末へのエージェントインストールについて、利用端末のOSやエージェントなど、DSG使用において必要となるソフトウェアの情報を防衛省が提示し、防衛関連企業側でその内容に合致する端末を準備いただき、エージェントインストールを実施いただきます。防衛関連企業側でのログ情報も必要に応じて提出を依頼することがあります。
133	ログ	利用端末のログ取得の設定、取得、分析結果の記録は、防衛省が実施したものを提供いただけますか。	必要な情報はDSG側から提供する予定です。
134	ログ	DSGでログの分析、管理について、防衛関連企業ではどのような対応が想定されますか。	DSGでログの分析、管理を行うに当たり、必要があれば利用者たる企業に問い合わせを行うこともあると考えており、それに対し対応いただくことを想定しています。（企業側に何か能動的な作業を求める意図ではありません）
135	ログ	機器ログの保存期間を教えてください。	別途運用要領でお知らせします。
136	ログ	DSGから提供されるログの種類を教えてください。防衛関連企業側で取得・管理しなければならないログはありますか。	DSG未接続の場合においても端末内にログは保存されており、DSG接続後にその保存したログをDSG側で取得します。よって、企業側での対応は特に想定しておりません。
137	ログ	DSGから提供されるログの細部種類を明示して頂けますでしょうか。	別途ご提示します。

## 防衛セキュリティゲートウェイ（DSG）に関するFAQ 【令和6年2月1日時点】

	分類	公開用質問	回答
138	取扱施設・関係施設	取扱施設の中に、企業内のネットワークを共存させることは可能でしょうか。	同一の取扱施設内に共存して設置することは可能です。 旧情報セキュリティ基準適用中の場合、ネットワーク接続は基本的に不可です。 新情報セキュリティ基準適用中の場合、官側の審査（接続方式やデータが混ざらない仕組み等）を経て許可します。
139	取扱施設・関係施設	通信ルータと防衛関連企業で準備するネットワークスイッチの間に、ファイアウォールのような通信を制御するような機器の導入は必要でしょうか。各社の利用端末に限り接続できるようDSG環境内で通信を制御しているため、各社での通信制御を実施する必要はないのでしょうか。	企業側でファイアウォールの設置や通信制御を実施いただく必要はございません。
140	取扱施設・関係施設	入退管理機器や監視カメラのスペックは、利用端末と同様2023年9月頃に提示されますか。	物理的セキュリティに必要な機器は、DSGの構成機器ではないため、入退管理機器や監視カメラのスペックは各防衛関連企業様の方針や設置環境により配置するものとなります。スペック提示は予定しておりません。新情報セキュリティ基準では目安となる指標をお示しすることは可能ですので、ご不明点は、防衛装備庁HPの防衛産業サイバーセキュリティ基準相談窓口（industrial-cybersecurity-office@ext.atla.mod.go.jp）にお問い合わせください。）
141	取扱施設・関係施設	新基準では、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が要求されていますが、DSGを利用する場合はICカードによる入退口の取得が必須でしょうか。 ※2023年6月実施の説明会資料の取扱施設のレイアウトイメージを例示したが、そこにICカードの記載があったため。	ICカードに限定しているわけではなく、警備員等を配置して入退記録簿を運用管理することも可能です。いずれにしても、入退室のログについては加入企業側で取得する必要があります。詳細は、防衛装備庁HPの防衛産業サイバーセキュリティ基準相談窓口（industrial-cybersecurity-office@ext.atla.mod.go.jp）にお問い合わせください。）
142	取扱施設・関係施設	入退室を鍵で管理し、手書きで入退室を管理する体制を取れば、監視カメラを設置しなくても良いのでしょうか。	入退記録としては不十分です。新情報セキュリティ基準では、鍵の管理者を指名し、鍵の受け渡しから管理してください。一人で完結するような運用は認められません。詳細は、防衛装備庁HPの防衛産業サイバーセキュリティ基準相談窓口（industrial-cybersecurity-office@ext.atla.mod.go.jp）にお問い合わせください。
143	取扱施設・関係施設	利用端末は契約毎に用意しますか。同じ利用端末で異なる契約の保護情報を取り扱うことは可能でしょうか。同じ部屋の中で別契約の端末を使用することは可能でしょうか。	契約毎の保護情報が混ざらないように契約毎にアカウントを発行するため、同じ利用端末で別契約の保護情報を扱うことも可能です。
144	システムセキュリティ実装計画書	「4 構成設定に係る記録及び保存等」のDSGが提供するサービスに「構成設定目録の作成に必要なDSGの情報提供」とありますが、例えば、DSGのデータセンター内のストレージデバイスが交換、追加等された場合に、その情報を企業側に提供する、ということでしょうか。これらのデバイスも企業の保護システムの構成要素に含まれるということでしょうか。含まれる場合、DSG側のデバイスの変更のたびに企業側が「システムセキュリティ実装計画書」を修正し、防衛省に報告しなければならないのでしょうか。	防衛関連企業に対して提供する「構成設定目録の作成に必要な情報」には、DSGサーバ側のデバイスは構成要素として含まれません。それらはDSGで構成管理しますので、企業の対応は不要です。