事　務　連　絡
令和８年 10 月１日

特定社会基盤事業者　殿

国土交通省水管理・国土保全局
水道事業課水道計画指導室

サイバー対処能力強化法に基づく水道分野におけるインシデント報告の扱いについて

重要電子計算機に対する不正な行為による被害の防止に関する法律（令和７年法律第 42 号。以下、「サイバー対処能力強化法」という。）について、本年 10 月１日より施行されました。これを踏まえ、サイバー対処能力強化法に基づき、水道分野における特別社会基盤事業者による特定侵害事象等の報告（以下、「インシデント報告」という。）の実務的運用について、以下のとおり周知します。

記

１．インシデント報告の方法について

サイバー対処能力強化法の施行に伴い、特定社会基盤事業者は、特定重要電子計算機に対するサイバーインシデントの発生を認知した際、サイバー対処能力強化法第５条に基づき、国土交通省及び内閣府両方にインシデント報告を行う必要があります。この報告について、以下（１）及び（２）のとおりの方法でご対応いただけますようお願いいたします。

（１）官民連携基盤を活用したインシデント報告

サイバーセキュリティ戦略（令和７年 12 月 23 日閣議決定）に基づき、インシデント報告等のための官民連携基盤が整備されています。本報告を行うにあたっては、同基盤を活用したインシデント報告が想定されているところ、同基盤を積極的にご活用いただけますようお願いいたします。同基盤の活用が難しい場合には、本事務連絡の担当まで個別にご連絡ください。

（２）従来の方法によるインシデント報告（メール送信の上、電話連絡等）

特定侵害事象等の事案については、「健康危機管理の適正な実施並びに水道施設への被害情報及び水質事故等に関する情報の提供について」（令和６年４月３日付国土交通省水管理・国土保全局水道事業課長通知。令和８年４月３日一部改正）で定める６．（２）に該当し、迅速な対応・支援のための情報提供をお願いしているところです。

上記（１）で定める官民連携基盤を活用したインシデント報告は、現時点で導入段階にあり、利用の習熟や運用の定着には一定の期間を要することが見込まれます。それまでの間、情報伝達の遅延や漏れ等を防止し、切れ目のない対応を行うためには、既存の報告手段を併用することが適切であると考えられます。

このことから、当面の間、サイバー対処能力強化法によるインシデント報告を行う場合には、官民連携基盤を活用した報告のみならず、同通知に定める方法（メール送信の上、電話連絡等）による報告についても引き続き実施いただけますようお願いいたします。その際、以下の方法により報告をお願いいたします。

・様式（別紙１）へ記入し、パスワードを設定の上での提出
（別紙１はサイバー対処能力強化法に基づくインシデント報告の様式と同一）

・報告先について各地方整備局等水道担当の他、以下内閣府担当の追加

宛先	内閣府（サイバー安全保障担当） 対処調整・官民連携等ユニット
メールアドレス	ciip@cyber.go.jp

２．事前相談の活用について

サイバー対処能力強化法に基づくインシデント報告の対象有無などについての疑義が生じた際には、上記１（２）と同様、各地方整備局等水道担当及び内閣府担当へ相談を行っていただきますようお願いいたします。

３．サイバー対処能力強化法に基づくインシデント報告等の制度の説明資料について

サイバー対処能力強化法の概要や具体的な手続きについては、「サイバー対処能力強化法に基づく特別社会基盤事業者による特定侵害事象等の報告等に関する制度の解説（特定重要電子計算機の届出及び特定侵害事象等の報告）（令和８年 10 月１日内閣府・総務省・法務省・財務省・厚生労働省・農林水産省・経済産業省・国土交通省）」（別紙２）が定められたところ、こちらについてもご参照いただけますようお願いいたします。

以上

【連絡先】
国土交通省水管理・国土保全局水道事業課水道計画指導室
サイバーセキュリティ対策担当（渡邉、下平）
TEL　代表 03-5253-8111（内線 34436）
E-Mail hqt-suidouwss@ki.mlit.go.jp

DDoS攻撃事案共通様式

年　　月　　日
時　　分

（報告先機関の長）殿

以下の報告根拠に基づき、別添のとおり報告いたします。

報告根拠：
☐ 法令等に基づく報告（「本様式の対象となる手続等」から該当手続名を記載すること。）

☐ 上記選択肢以外（自主判断による情報提供を目的とした任意報告等）
※任意報告の同報先がある場合は、以下に同報先機関を記載すること。

【報告の区分】
（１）報告の版：第　　報
（２）速報/続報/詳報の別：　☐ 速報(新規)　☐ 続報　☐ 詳報(確報)
（前回報告：　　年　　月　　日　　時　　分）
（受付番号※：　　）
※個人情報保護委員会より通知されている場合

本様式に記載いただいた内容は、報告先機関から、内閣官房国家サイバー統括室に共有されます。内閣官房国家サイバー統括室は、報告された内容を整理分析の上、被害者が分からないようにした上で、被害の拡大防止のため、注意喚起等に活用することがあります。
記載内容の全部又は一部について、内閣官房国家サイバー統括室との共有等を希望しない場合は、その旨及び共有等を希望しない内容について以下に記載してください。

☐　内閣官房国家サイバー統括室への共有等を希望しない。
共有等を希望しない内容：

（注）重要電子計算機に対する不正な行為による被害の防止に関する法律第５条に基づく報告である場合は、「共有等を希望しない」とした場合でも、同法に基づき内閣官房国家サイバー統括室等に情報提供されることがあります。
（注）報告を行う者が、重要インフラのサイバーセキュリティに係る行動計画（2022年６月17日サイバーセキュリティ戦略本部決定）に定める重要インフラ事業者等である場合は、同行動計画に基づき、「共有等を希望しない」とした場合でも、内閣官房国家サイバー統括室に共有されることがあります。

１．記載の手引き
（１）本様式の対象となる手続等
報告根拠に記載する法令、ガイドライン等（重要インフラのサイバーセキュリティに係る行動計画において重要インフラ分野として指定されている分野の法令、ガイドライン等を含む）については、次のウェブサイトに記載。ただし、具体的な提出先や提出方法、追加的な報告事項の有無については、各法令、ガイドラインや、各省庁が公表する方法に従うこと。また、業法等の固有の報告項目については、様式本体の「６．その他特記事項」に記載すること。このほか、警察への相談を行う場合や、その他所管省庁から本様式により報告を行うよう要請等があった場合についても、本様式を利用することができる。

https://www.cyber.go.jp/policy/group/cyber/policy.html

（２）記載事項
報告をしようとする時点で把握している範囲で、１から６までの内容を記載してください。また、続報として提出する場合には、前回の報告から記載を変更した箇所に下線を引くなど、変更箇所が分かるようにしてください。

１．報告者の概要

報告者の氏名 又は名称	（フリガナ） （氏名は旧姓での記載を可とする）	
法人番号（13桁）		
業種・業種番号		
報告者の住所 又は居所	〒　－	
代表者の氏名 （報告者が法人等の場合に限る。）	（フリガナ） （氏名は旧姓での記載を可とする）	
事務連絡者の氏名	（フリガナ） （氏名は旧姓での記載を可とする） 所属部署　　電話番号 E-mail	

２．事案の概要（業務への影響）

（１）事案の概要

発生日時：　　年　　月　　日　　時　　分

発覚日時：　　年　　月　　日　　時　　分

（２）重要インフラサービス維持レベルについて（重要インフラのサイバーセキュリティに係る行動計画（2022年６月17日サイバーセキュリティ戦略本部決定）に定める重要インフラ事業者等に該当する場合に記載すること。該当しない場合は記載を要さない。）

・重要インフラサービスのサービス維持レベルの逸脱の有無：　□ 有　□ 無

・他の事業者等への波及の可能性：　□ 有　□ 無

（３）事実経過（時系列）

３．影響のあるシステム（強化法第５条による報告の場合、特定侵害事象等が発生した特定重要電子計算機について記載）

４．事案に関する技術的な事項（攻撃技術情報）
※記入可能な項目を記載してください。また、間隔を空けて別種の攻撃（波）がある場合は、攻撃（波）毎に本項目を作成することも可能。

（１）観測期間

攻撃発生：	月	日	時	分
攻撃収束：	月	日	時	分
特記事項：				

（２）攻撃類型

①分類（複数選択）（※選択肢は、MITRE ATT&CKのTechniquesを参照しています。）

- ☐ ネットワークへのサービス拒否攻撃　Network Denial of Service (T1498)
  ※以下に記載のT1498-001又はT1498-002のいずれに該当するかが不明な場合
- ☐ ネットワークへのフラッド攻撃（UDPフラッド攻撃等）　Direct Network Flood (T1498-001)
- ☐ ネットワークへのリフレクション攻撃（DNSリフレクション攻撃等）　Reflection Amplification (T1498-002)
- ☐ エンドポイントへのサービス拒否攻撃　Endpoint Denial of Service (T1499)
  ※以下に記載のT1499-001からT1499-004までのいずれに該当するかが不明な場合
- ☐ OS枯渇フラッド（TCPステート枯渇攻撃等）　OS Exhaustion Flood (T1499-001)
- ☐ サービス枯渇フラッド（HTTPフラッド攻撃等）　Service Exhaustion Flood (T1499-002)
- ☐ アプリケーション枯渇フラッド　Application Exhaustion Flood (T1499-003)
- ☐ アプリケーション又はシステムの脆弱性悪用によるサービス妨害攻撃 Application or System Exploitation (T1499-004)
- ☐ その他（　　）
- ☐ 不明

②詳細

（３）通信プロトコル

（４）送信元情報

（５）送信先情報

（６）通信量

※送信元IPアドレスなど、記載内容が多数になる場合は別ファイルで御提出ください。

５．事案への対応に関する事項

（１）公表の実施状況

事案の公表：　□　実施済　　【公表日：　　年　　月　　日】

公表URL：

□　実施予定　　【公表予定日：　　年　　月　　日】

□　検討中

□　予定無し

公表の方法：　□　ホームページに掲載

□　記者会見

□　報道機関等への資料配付

□　その他：　　（　　）

公表文：

（２）今後の予定

□　事象継続中

□　対応策を継続中

□　対応完了

（３）外部機関による調査の実施状況

□　実施済又は実施中

□　実施予定

□　検討中

□　予定なし

（詳細：　　）

６．その他特記事項

ランサムウェア事案共通様式

年　　月　　日
時　　分

（報告先機関の長）殿

以下の報告根拠に基づき、別添のとおり報告いたします。

報告根拠：
□ 法令等に基づく報告（「本様式の対象となる手続等」から該当手続名を記載すること。）

□ 上記選択肢以外（自主判断による情報提供を目的とした任意報告等）
※任意報告の同報先がある場合は、以下に同報先機関を記載すること。

【報告の区分】
（１）報告の版：第　　報
（２）速報/続報/詳報の別：　□ 速報(新規)　□ 続報　□ 詳報(確報)
（前回報告：　　年　　月　　日　　時　　分）
（受付番号※：　　）
※個人情報保護委員会より通知されている場合

本様式に記載いただいた内容は、報告先機関から、内閣官房国家サイバー統括室に共有されます。内閣官房国家サイバー統括室は、報告された内容を整理分析の上、被害者が分からないようにした上で、被害の拡大防止のため、注意喚起等に活用することがあります。
記載内容の全部又は一部について、内閣官房国家サイバー統括室との共有等を希望しない場合は、その旨及び共有等を希望しない内容について以下に記載してください。

□　内閣官房国家サイバー統括室への共有等を希望しない。
共有等を希望しない内容：

（注）重要電子計算機に対する不正な行為による被害の防止に関する法律第５条に基づく報告である場合は、「共有等を希望しない」とした場合でも、同法に基づき内閣官房国家サイバー統括室等に情報提供されることがあります。

（注）報告を行う者が、重要インフラのサイバーセキュリティに係る行動計画（2022年６月17日サイバーセキュリティ戦略本部決定）に定める重要インフラ事業者等である場合は、同行動計画に基づき、「共有等を希望しない」とした場合でも、別紙１から別紙３までの内容を除き、内閣官房国家サイバー統括室に共有されることがあります。

１．記載の手引き
（１）本様式の対象となる手続等
報告根拠に記載する法令、ガイドライン等（重要インフラのサイバーセキュリティに係る行動計画において重要インフラ分野として指定されている分野の法令、ガイドライン等を含む）については、次のウェブサイトに記載。ただし、具体的な提出先や提出方法、追加的な報告事項の有無については、各法令、ガイドラインや、各省庁が公表する方法に従うこと。また、業法等の固有の報告項目については、様式本体の「６．その他特記事項」に記載すること。このほか、警察への相談を行う場合や、その他所管省庁から本様式により報告を行うよう要請等があった場合についても、本様式を利用することができる。

https://www.cyber.go.jp/policy/group/cyber/policy.html

（２）記載事項
①共通
報告をしようとする時点で把握している範囲で、１から６までの内容を記載してください。また、続報として提出する場合には、前回の報告から記載を変更した箇所に下線を引くなど、変更箇所が分かるようにしてください。
②個人情報の保護に関する法律第26条第１項の規定による漏えい等報告を行う場合
別紙１も記載してください。
③個人情報の保護に関する法律第68条第１項の規定による漏えい等報告を行う場合
別紙２も記載してください。
④行政手続における特定の個人を識別するための番号の利用等に関する法律第29条の４第１項の規定による漏えい等報告を行う場合
別紙３も記載してください。

２．ランサムウェア感染時の留意事項
被害拡大防止、原因究明・再感染防止のため、初期対応時において、感染端末に対して以下の対応を御検討いただくことを推奨します。感染経路が分からなくなると、復旧に支障が生じる場合があります。
・感染端末及び感染が疑われる端末からLANケーブルを抜くとともに、無線LANを無効にすること。
・感染端末等の再起動や電源オフをしないこと。既に感染端末等の電源がオフの場合はオンにしないこと。
・ウイルス対策ソフトによる感染端末等のフルスキャンをしないこと。
・ネットワーク機器の再起動や電源オフをしないこと。
・ファームウェアやOSのアップデートをしないこと。

１．報告者の概要

報告者の氏名 又は名称	（フリガナ） （氏名は旧姓での記載を可とする）	
法人番号（13桁）		
業種・業種番号		
報告者の住所 又は居所	〒　－	
代表者の氏名 （報告者が法人等の場合に限る。）	（フリガナ） （氏名は旧姓での記載を可とする）	
事務連絡者の氏名	（フリガナ） （氏名は旧姓での記載を可とする） 所属部署　　電話番号 E-mail	

２．事案の概要（業務への影響）

（１）事案の概要

発生日時：　　年　　月　　日　　時　　分

発覚日時：　　年　　月　　日　　時　　分

（２）重要インフラサービス維持レベルについて（重要インフラのサイバーセキュリティに係る行動計画（2022年６月17日サイバーセキュリティ戦略本部決定）に定める重要インフラ事業者等に該当する場合に記載すること。該当しない場合は記載を要さない。）

・重要インフラサービスのサービス維持レベルの逸脱の有無：　□ 有　□ 無

・他の事業者等への波及の可能性：　□ 有　□ 無

（３）個人データ、保有個人情報又は特定個人情報の漏えい等について（報告を行う様式にチェックすること。個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律に基づく漏えい等報告を同時に行う場合は、両方チェックし、それぞれの様式に記載すること。）

□　別紙１（個人情報取扱事業者における個人データ等の漏えい等報告）
【民間事業者・個人情報の保護に関する法律第58条第１項各号に掲げる法人等（いわゆる規律移行法人）の方】

□　別紙２（行政機関等における保有個人情報の漏えい等報告）【行政機関等の方】

□　別紙３（特定個人情報の漏えい等報告）【民間事業者・行政機関等共通】

（４）事実経過（時系列）

３．影響のあるシステム（強化法第５条による報告の場合、特定侵害事象等が発生した特定重要電子計算機について記載）

４．事案に関する技術的な事項（攻撃技術情報）
（※報告時点で記入可能な項目を記載してください。不明箇所は空白で構いません。）

（１）ランサムノート（身代金を要求する文言等）

（２）暗号化されたファイルの拡張子

（３）ランサムウェアの類型

（４）攻撃の手口・侵入経路・攻撃の時系列

※システム構成が分かる図やフォレンジック結果報告書を提出する場合は別ファイルとしてください。

（５）ランサムウェアの特徴（インディケータ情報）

※IPアドレスやログ情報など、記載内容が多数になる場合は別ファイルで御提出ください。

（６）悪用された脆弱性

・製品開発者への報告の有無：　□　有　　□　無

５．事案への対応に関する事項

（１）公表の実施状況

事案の公表：　□　実施済　　【公表日：　　年　　月　　日】
公表URL：
□　実施予定　　【公表予定日：　　年　　月　　日】
□　検討中
□　予定無し

公表の方法：　□　ホームページに掲載
□　記者会見
□　報道機関等への資料配付
□　その他：　（　　）

公表文：

（２）今後の予定

□　事象継続中
□　対応策を継続中
□　対応完了

（３）外部機関による調査の実施状況

□　実施済又は実施中
□　実施予定
□　検討中
□　予定なし
（詳細：　　）

６．その他（特記事項等）

別紙1（個人情報取扱事業者における個人データ等の漏えい等報告）
【民間事業者・個人情報の保護に関する法律第58条第1項各号に掲げる法人等（いわゆる規律移行法人）の方】

※　いずれの項目も、報告をしようとする時点で把握している内容を記載すること。

（１）報告の種別

速報又は確報の別：　□　速報　□　中間報　□　確報

（２）事態の概要

発生事案：　□　漏えい　□　漏えいのおそれ
□　滅失　□　滅失のおそれ
□　毀損　□　毀損のおそれ

発見者：　□　自社/委託先　□　取引先　□　顧客/会員
□　カード会社/決済代行会社　□　その他　（　　）

規則第７条各号該当性：　□　第１号（要配慮個人情報）
□　第２号（財産的被害）
□　第３号（不正の目的）
□　第４号（千人超）
□　非該当（上記に該当しない場合の報告）

報告者に個人データの取扱いを委託した者（委託元）の有無：
□　有（名称：　　）
（住所：　　）
（電話：　　）
□　無

報告者から個人データの取扱いの委託を受けた者（委託先）の有無
□　有（名称：　　）
（住所：　　）
（電話：　　）
□　無

（３）漏えい等が発生し、又は発生したおそれがある個人データの項目（該当する□に印を付けること。）

媒体：　□　紙　□　電子媒体　□　その他（　　）
種類：　□　顧客情報　□　従業員情報　□　その他（　　）
項目：　□　氏名　□　生年月日　□　性別
□　住所　□　電話番号　□　メールアドレス
□　クレジットカード情報　□　パスワード
□　その他（　　）

（４）漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数

状況：　□　人数判明　□　確認中（概算含む）　□　不明
人数：（　　）人　うちクレジットカード情報含む（　　）人

（５）発生原因（該当する□に印を付けること。）

主体：　□　報告者　□　委託先　□　不明

原因：　□　不正アクセス

（攻撃箇所：（　　））
（攻撃手法：（　　））

詳細：

（６）二次被害又はそのおそれの有無及びその内容（該当する□に印を付けること。）

有無：　□　有　□　無　□　不明

詳細：

（７）本人への対応の実施状況（該当する□に印を付けること。）

本人への対応（通知を含む。）：　□　対応済（対応中）　□　対応予定　□　予定なし

詳細（予定なしの場合は、理由を記載）：

（８）再発防止のための措置

実施済の措置：

今後実施予定の措置（長期的に講ずる措置を含む。）及び完了予定時期：

（９）その他参考となる事項

別紙2（行政機関等における保有個人情報の漏えい等報告）【行政機関等の方】

※　いずれの項目も、報告をしようとする時点で把握している内容を記載すること。

（１）報告の種別

速報又は確報の別：　□　速報　□　中間報　□　確報

報告者の組織区分：　□　行政機関等　□　地方公共団体等

（２）事態の概要

発生事案：　□　漏えい　□　漏えいのおそれ

□　滅失　□　滅失のおそれ

□　毀損　□　毀損のおそれ

発見者：　□　自組織/委託先　□　取引先

□　取引先以外の外部指摘（国民等からの指摘）

□　カード会社/決済代行会社　□　その他　（　　）

規則第43条各号該当性：　□　第１号（要配慮個人情報）

□　第２号（財産的被害）

□　第３号（不正の目的）

□　第４号（百人超）

□　第５号（条例要配慮個人情報）

□　非該当（上記に該当しない場合の報告）

報告者に保有個人情報の取扱いを委託した者（委託元）の有無：

□　有（名称：　　）

（住所：　　）

（電話：　　）

□　無

報告者から保有個人情報の取扱いの委託を受けた者（委託先）の有無

□　有（名称：　　）

（住所：　　）

（電話：　　）

□　無

（３）漏えい等が発生し、又は発生したおそれがある保有個人情報の項目（該当する□に印を付けること。）

媒体：　□　紙　□　電子媒体　□　その他（　　）

種類：　□　国民等　□　職員　□　その他（　　）

項目：　□　氏名　□　生年月日　□　性別

□　住所　□　電話番号　□　メールアドレス

□　クレジットカード情報　□　パスワード

□　その他（　　）

（４）漏えい等が発生し、又は発生したおそれがある保有個人情報に係る本人の数

状況：　□　人数判明　□　確認中（概算含む）　□　不明

人数：（　　）人　うちクレジットカード情報含む（　　）人

（５）発生原因（該当する□に印を付けること。）

主体：　□　報告者　□　委託先　□　不明

原因：　□　不正アクセス

（攻撃箇所：（　　））

（攻撃手法：（　　））

詳細：

（６）二次被害又はそのおそれの有無及びその内容（該当する□に印を付けること。）

有無：　□　有　□　無　□　不明

詳細：

（７）本人への対応の実施状況（該当する□に印を付けること。）

本人への対応（通知を含む。）：　□　対応済（対応中）　□　対応予定

□　予定なし

詳細（予定なしの場合は、理由を記載）：

（８）再発防止のための措置

実施済の措置：

今後実施予定の措置（長期的に講ずる措置を含む。）及び完了予定時期：

（９）その他参考となる事項

別紙3（特定個人情報の漏えい等報告）【民間事業者・行政機関等共通】

※　いずれの項目も、報告をしようとする時点で把握している内容を記載すること。

（１）報告の種別

速報又は確報の別：　□ 速報　□ 中間報　□ 確報

報告者の組織区分：　□ 行政機関　□ 独立行政法人等　□ 地方公共団体等　□ 事業者

（２）事態の概要

事務の内容：　□ 個人番号利用事務　□ 個人番号関係事務　□ その他

事務の名称：　（　　）

特定個人情報保護評価の実施の有無：　□ 実施（義務）　□ 実施（任意）　□ 実施していない

評価の種類：　□ 基礎項目評価　□ 重点項目評価　□ 全項目評価

発生事案：　□ 漏えい　□ 漏えいのおそれ
□ 滅失　□ 滅失のおそれ
□ 毀損　□ 毀損のおそれ
□ 法第９条違反　□ 法第９条違反のおそれ
□ 法第19条違反　□ 法第19条違反のおそれ
□ その他　（　　）

発見者：　□ 報告者　□ 委託者
□ その他　（　　）

規則第２条各号該当性：　□ 第１号（情報提供ネットワークシステム等）
□ 第２号（不正の目的）
□ 第３号（不特定多数の者に閲覧）
□ 第４号（百人超）
□ 非該当（上記に該当しない場合の報告）

報告者に特定個人情報の取扱いを委託した者（委託元）の有無：

□ 有（名称：　　）
（住所：　　）
（電話：　　）

□ 無

報告者から特定個人情報の取扱いの委託を受けた者（委託先）の有無

□ 有（名称：　　）
（住所：　　）
（電話：　　）

□ 無

（３）特定個人情報の項目（該当する□に印を付けること。）

媒体：　□ 紙　□ 電子媒体　□ その他（　　）

種類：　□ 顧客情報　□ 住民情報　□ 従業員情報
□ その他（　　）

項目：　□ 氏名　□ 生年月日　□ 性別
□ 住所　□ 電話番号　□ メールアドレス
□ パスワード　□ その他（　　）

（４）特定個人情報に係る本人の数

状況：　□ 人数判明　□ 確認中（概算含む）　□ 不明

人数：（　　）人

（５）発生原因（該当する□に印を付けること。）

主体：　□ 報告者　□ 委託先　□ 不明

原因：　□ 不正アクセス

（攻撃箇所：（　　））

（攻撃手法：（　　））

詳細：

（６）二次被害又はそのおそれの有無及びその内容（該当する□に印を付けること。）

有無：　□　有　□　無　□　不明

詳細：

（７）本人への対応の実施状況（該当する□に印を付けること。）

本人への対応（通知を含む。）：　□　対応済（対応中）　□　対応予定　□　予定なし

詳細（予定なしの場合は、理由を記載）：

（８）再発防止のための措置

実施済の措置：

今後実施予定の措置（長期的に講ずる措置を含む。）及び完了予定時期：

（９）その他参考となる事項

その他サイバー攻撃等事案共通様式
（不正アクセス、情報窃取等）

年　　月　　日
時　　分

（報告先機関の長）殿

以下の報告根拠に基づき、別添のとおり報告いたします。

報告根拠：
□ 法令等に基づく報告（「本様式の対象となる手続等」から該当手続名を記載すること。）

□ 上記選択肢以外（自主判断による情報提供を目的とした任意報告等）
※任意報告の同報先がある場合は、以下に同報先機関を記載すること。

【報告の区分】
（１）報告の版：第　　報
（２）速報/続報/詳報の別：　□ 速報(新規)　□ 続報　□ 詳報(確報)
（前回報告：　　年　　月　　日　　時　　分）
（受付番号※：　　）
※個人情報保護委員会より通知されている場合

本様式に記載いただいた内容は、報告先機関から、内閣官房国家サイバー統括室に共有されます。内閣官房国家サイバー統括室は、報告された内容を整理分析の上、被害者が分からないようにした上で、被害の拡大防止のため、注意喚起等に活用することがあります。
記載内容の全部又は一部について、内閣官房国家サイバー統括室との共有等を希望しない場合は、その旨及び共有等を希望しない内容について以下に記載してください。

□　内閣官房国家サイバー統括室への共有等を希望しない。
共有等を希望しない内容：

（注）重要電子計算機に対する不正な行為による被害の防止に関する法律第５条に基づく報告である場合は、「共有等を希望しない」とした場合でも、同法に基づき内閣官房国家サイバー統括室等に情報提供されることがあります。
（注）報告を行う者が、重要インフラのサイバーセキュリティに係る行動計画（2022年６月17日サイバーセキュリティ戦略本部決定）に定める重要インフラ事業者等である場合は、同行動計画に基づき、「共有等を希望しない」とした場合でも、別紙１から別紙３までの内容を除き、内閣官房国家サイバー統括室に共有されることがあります。

１．記載の手引き
（１）本様式の対象となる手続等
報告根拠に記載する法令、ガイドライン等（重要インフラのサイバーセキュリティに係る行動計画において重要インフラ分野として指定されている分野の法令、ガイドライン等を含む）については、次のウェブサイトに記載。ただし、具体的な提出先や提出方法、追加的な報告事項の有無については、各法令、ガイドラインや、各省庁が公表する方法に従うこと。また、業法等の固有の報告項目については、様式本体の「６．その他特記事項」に記載すること。このほか、警察への相談を行う場合や、その他所管省庁から本様式により報告を行うよう要請等があった場合についても、本様式を利用することができる。

https://www.cyber.go.jp/policy/group/cyber/policy.html

（２）記載事項
①共通
報告をしようとする時点で把握している範囲で、１から６までの内容を記載してください。また、続報として提出する場合には、前回の報告から記載を変更した箇所に下線を引くなど、変更箇所が分かるようにしてください。
②個人情報の保護に関する法律第26条第１項の規定による漏えい等報告を行う場合
別紙１も記載してください。
③個人情報の保護に関する法律第68条第１項の規定による漏えい等報告を行う場合
別紙２も記載してください。
④行政手続における特定の個人を識別するための番号の利用等に関する法律第29条の４第１項の規定による漏えい等報告を行う場合
別紙３も記載してください。
※②から④までの報告を行う場合においては、サイバー攻撃事案に伴う漏えい等事案に伴う報告であることに留意する。（ただし、所管省庁から別途要請等があった場合はこの限りでない。）

２．マルウェア感染時の留意事項
被害拡大防止、原因究明・再感染防止のため、初期対応時において、感染端末に対して以下の対応を御検討いただくことを推奨します。感染経路が分からなくなると、復旧に支障が生じる場合があります。
・感染端末及び感染が疑われる端末からLANケーブルを抜くとともに、無線LANを無効にすること。
・感染端末等の再起動や電源オフをしないこと。既に感染端末等の電源がオフの場合はオンにしないこと。
・ウイルス対策ソフトによる感染端末等のフルスキャンをしないこと。
・ネットワーク機器の再起動や電源オフをしないこと。
・ファームウェアやOSのアップデートをしないこと。

１．報告者の概要

報告者の氏名 又は名称	（フリガナ） （氏名は旧姓での記載を可とする）	
法人番号（13桁）		
業種・業種番号		
報告者の住所 又は居所	〒　－	
代表者の氏名 （報告者が法人等の場合に限る。）	（フリガナ） （氏名は旧姓での記載を可とする）	
事務連絡者の氏名	（フリガナ） （氏名は旧姓での記載を可とする）	
	所属部署 E-mail	電話番号

２．事案の概要（業務への影響）

（１）事案の概要

発生日時：　　年　　月　　日　　時　　分

発覚日時：　　年　　月　　日　　時　　分

（２）重要インフラサービス維持レベルについて（重要インフラのサイバーセキュリティに係る行動計画（2022年６月17日サイバーセキュリティ戦略本部決定）に定める重要インフラ事業者等に該当する場合に記載すること。該当しない場合は記載を要さない。）

・重要インフラサービスのサービス維持レベルの逸脱の有無：　□ 有　□ 無

・他の事業者等への波及の可能性：　□ 有　□ 無

（３）個人データ、保有個人情報又は特定個人情報の漏えい等について（報告を行う様式にチェックすること。個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律に基づく漏えい等報告を同時に行う場合は、両方チェックし、それぞれの様式に記載すること。）

□　別紙１（個人情報取扱事業者における個人データ等の漏えい等報告）
【民間事業者・個人情報の保護に関する法律第58条第１項各号に掲げる法人等（いわゆる規律移行法人）の方】

□　別紙２（行政機関等における保有個人情報の漏えい等報告）【行政機関等の方】

□　別紙３（特定個人情報の漏えい等報告）【民間事業者・行政機関等共通】

（４）事実経過（時系列）

３．影響のあるシステム（強化法第５条による報告の場合、特定侵害事象等が発生した特定重要電子計算機について記載）

４．事案に関する技術的な事項（攻撃技術情報）
（※報告時点で記入可能な項目を記載してください。不明箇所は空白で構いません。）

（１）攻撃の手口・侵入経路・攻撃の時系列

※システム構成が分かる図やフォレンジック結果報告書を提出する場合は別ファイルとしてください。

（２）サイバー攻撃等の類型

（３）サイバー攻撃等の特徴（インディケータ情報）

※IPアドレスやログ情報など、記載内容が多数になる場合は別ファイルで御提出ください。

（４）悪用された脆弱性

・製品開発者への報告の有無：　□　有　　□　無

５．事案への対応に関する事項

（１）公表の実施状況

事案の公表：　□　実施済　　【公表日：　　年　　月　　日】
公表URL:
□　実施予定　　【公表予定日：　　年　　月　　日】
□　検討中
□　予定無し

公表の方法：　□　ホームページに掲載
□　記者会見
□　報道機関等への資料配付
□　その他：　　（　　）

公表文：

（２）今後の予定

□　事象継続中
□　対応策を継続中
□　対応完了

（３）外部機関による調査の実施状況

□　実施済又は実施中
□　実施予定
□　検討中
□　予定なし
（詳細：　　）

６．その他（特記事項等）

別紙1（個人情報取扱事業者における個人データ等の漏えい等報告）
【民間事業者・個人情報の保護に関する法律第58条第1項各号に掲げる法人等（いわゆる規律移行法人）の方】

※　いずれの項目も、報告をしようとする時点で把握している内容を記載すること。

（１）報告の種別

速報又は確報の別：　□　速報　　□　中間報　　□　確報

（２）事態の概要

発生事案：　□　漏えい　　□　漏えいのおそれ
□　滅失　　□　滅失のおそれ
□　毀損　　□　毀損のおそれ

発見者：　□　自社/委託先　　□　取引先　　□　顧客/会員
□　カード会社/決済代行会社　　□　その他　（　　）

規則第７条各号該当性：　□　第１号（要配慮個人情報）
□　第２号（財産的被害）
□　第３号（不正の目的）
□　第４号（千人超）
□　非該当（上記に該当しない場合の報告）

報告者に個人データの取扱いを委託した者（委託元）の有無：
□　有（名称：　　）
（住所：　　）
（電話：　　）
□　無

報告者から個人データの取扱いの委託を受けた者（委託先）の有無
□　有（名称：　　）
（住所：　　）
（電話：　　）
□　無

（３）漏えい等が発生し、又は発生したおそれがある個人データの項目（該当する□に印を付けること。）

媒体：　□　紙　　□　電子媒体　　□　その他（　　）
種類：　□　顧客情報　　□　従業員情報　　□　その他（　　）
項目：　□　氏名　　□　生年月日　　□　性別
□　住所　　□　電話番号　　□　メールアドレス
□　クレジットカード情報　　□　パスワード
□　その他（　　）

（４）漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数

状況：　□　人数判明　　□　確認中（概算含む）　　□　不明
人数：（　　）人　　うちクレジットカード情報含む（　　）人

（５）発生原因（該当する□に印を付けること。）

主体：　□　報告者　　□　委託先　　□　不明
原因：　□　不正アクセス
（攻撃箇所：（　　））
（攻撃手法：（　　））
詳細：

（６）二次被害又はそのおそれの有無及びその内容（該当する□に印を付けること。）

有無：　□　有　□　無　□　不明

詳細：

（７）本人への対応の実施状況（該当する□に印を付けること。）

本人への対応（通知を含む。）：　□　対応済（対応中）　□　対応予定　□　予定なし

詳細（予定なしの場合は、理由を記載）：

（８）再発防止のための措置

実施済の措置：

今後実施予定の措置（長期的に講ずる措置を含む。）及び完了予定時期：

（９）その他参考となる事項

別紙2（行政機関等における保有個人情報の漏えい等報告）【行政機関等の方】

※　いずれの項目も、報告をしようとする時点で把握している内容を記載すること。

（１）報告の種別

速報又は確報の別：　□ 速報　□ 中間報　□ 確報

報告者の組織区分：　□ 行政機関等　□ 地方公共団体等

（２）事態の概要

発生事案：　□ 漏えい　□ 漏えいのおそれ
□ 滅失　□ 滅失のおそれ
□ 毀損　□ 毀損のおそれ

発見者：　□ 自組織/委託先　□ 取引先
□ 取引先以外の外部指摘（国民等からの指摘）
□ カード会社/決済代行会社　□ その他　（　　）

規則第43条各号該当性：　□ 第１号（要配慮個人情報）
□ 第２号（財産的被害）
□ 第３号（不正の目的）
□ 第４号（百人超）
□ 第５号（条例要配慮個人情報）
□ 非該当（上記に該当しない場合の報告）

報告者に保有個人情報の取扱いを委託した者（委託元）の有無：

□ 有（名称：　　）
（住所：　　）
（電話：　　）

□ 無

報告者から保有個人情報の取扱いの委託を受けた者（委託先）の有無

□ 有（名称：　　）
（住所：　　）
（電話：　　）

□ 無

（３）漏えい等が発生し、又は発生したおそれがある保有個人情報の項目（該当する□に印を付けること。）

媒体：　□ 紙　□ 電子媒体　□ その他（　　）

種類：　□ 国民等　□ 職員　□ その他（　　）

項目：　□ 氏名　□ 生年月日　□ 性別
□ 住所　□ 電話番号　□ メールアドレス
□ クレジットカード情報　□ パスワード
□ その他（　　）

（４）漏えい等が発生し、又は発生したおそれがある保有個人情報に係る本人の数

状況：　□ 人数判明　□ 確認中（概算含む）　□ 不明

人数：（　　）人　うちクレジットカード情報含む（　　）人

（５）発生原因（該当する□に印を付けること。）

主体：　□ 報告者　□ 委託先　□ 不明

原因：　□ 不正アクセス

（攻撃箇所：（　　））

（攻撃手法：（　　））

詳細：

（６）二次被害又はそのおそれの有無及びその内容（該当する□に印を付けること。）

有無：　□ 有　□ 無　□ 不明

詳細：

（７）本人への対応の実施状況（該当する□に印を付けること。）

本人への対応（通知を含む。）：　□　対応済（対応中）　□　対応予定

□　予定なし

詳細（予定なしの場合は、理由を記載）：

（８）再発防止のための措置

実施済の措置：

今後実施予定の措置（長期的に講ずる措置を含む。）及び完了予定時期：

（９）その他参考となる事項

別紙3（特定個人情報の漏えい等報告）【民間事業者・行政機関等共通】

※　いずれの項目も、報告をしようとする時点で把握している内容を記載すること。

（１）報告の種別

速報又は確報の別：　□ 速報　□ 中間報　□ 確報

報告者の組織区分：　□ 行政機関　□ 独立行政法人等　□ 地方公共団体等　□ 事業者

（２）事態の概要

事務の内容：　□ 個人番号利用事務　□ 個人番号関係事務　□ その他

事務の名称：　（　　）

特定個人情報保護評価の実施の有無：　□ 実施（義務）　□ 実施（任意）　□ 実施していない

評価の種類：　□ 基礎項目評価　□ 重点項目評価　□ 全項目評価

発生事案：　□ 漏えい　□ 漏えいのおそれ
□ 滅失　□ 滅失のおそれ
□ 毀損　□ 毀損のおそれ
□ 法第９条違反　□ 法第９条違反のおそれ
□ 法第19条違反　□ 法第19条違反のおそれ
□ その他　（　　）

発見者：　□ 報告者　□ 委託者
□ その他　（　　）

規則第２条各号該当性：　□ 第１号（情報提供ネットワークシステム等）
□ 第２号（不正の目的）
□ 第３号（不特定多数の者に閲覧）
□ 第４号（百人超）
□ 非該当（上記に該当しない場合の報告）

報告者に特定個人情報の取扱いを委託した者（委託元）の有無：

□ 有（名称：　　）
（住所：　　）
（電話：　　）

□ 無

報告者から特定個人情報の取扱いの委託を受けた者（委託先）の有無

□ 有（名称：　　）
（住所：　　）
（電話：　　）

□ 無

（３）特定個人情報の項目（該当する□に印を付けること。）

媒体：　□ 紙　□ 電子媒体　□ その他（　　）

種類：　□ 顧客情報　□ 住民情報　□ 従業員情報
□ その他（　　）

項目：　□ 氏名　□ 生年月日　□ 性別
□ 住所　□ 電話番号　□ メールアドレス
□ パスワード　□ その他（　　）

（４）特定個人情報に係る本人の数

状況：　□ 人数判明　□ 確認中（概算含む）　□ 不明

人数：（　　）人

（５）発生原因（該当する□に印を付けること。）

主体：　□ 報告者　□ 委託先　□ 不明

原因：　□ 不正アクセス

（攻撃箇所：（　　））

（攻撃手法：（　　））

詳細：

（６）二次被害又はそのおそれの有無及びその内容（該当する□に印を付けること。）

有無：　□　有　□　無　□　不明

詳細：

（７）本人への対応の実施状況（該当する□に印を付けること。）

本人への対応（通知を含む。）：　□　対応済（対応中）　□　対応予定　□　予定なし

詳細（予定なしの場合は、理由を記載）：

（８）再発防止のための措置

実施済の措置：

今後実施予定の措置（長期的に講ずる措置を含む。）及び完了予定時期：

（９）その他参考となる事項

サイバー対処能力強化法に基づく
特別社会基盤事業者による特定侵害事象等
の報告等に関する制度の解説
（特定重要電子計算機の届出
及び特定侵害事象等の報告）

令和8年10月1日

内閣府・総務省・法務省・財務省・厚生労働省・
農林水産省・経済産業省・国土交通省

目次

1. 本解説の概要 5
1-1 目的 5
1-2 対象事業者 5
1-3 構成 5
2. 特定重要電子計算機の範囲（法第2条第2項第2号等） 7
2-1 範囲の概要（法第2条第2項第2号） 7
2-1-1 特定社会基盤事業者が使用する電子計算機 8
2-1-2 電子計算機に組み込まれたプログラム 9
2-2 特定重要電子計算機の類型（政令第1条第3項等） 9
2-2-1 ①特定重要設備である電子計算機又は特定重要設備の一部を構成する電子計算機（一号電子計算機）（政令第1条第3項第1号） 14
2-2-2 ②特定重要設備と接続されている電子計算機（政令第1条第3項第2号及び主務省令第1条第1項） 14
2-2-3 ③USB やクラウドサービス等の特定重要設備にデータを入力可能な電子計算機（政令第1条第3項第3号及び主務省令第1条第2項） 18
3. 特定重要電子計算機の届出（法第4条） 19
3-1 新規届出（法第4条第1項、主務省令第2条等） 19
3-1-1 届出対象（主務省令第2条第1項） 21
アプライアンスの場合 21
アプライアンス以外の電子計算機の場合 21
アプライアンス以外の電子計算機については、当該電子計算機に組み込まれた 21
専用設計品である場合 21
広く一般的に使用されている製品である場合（主務省令第2条第1項ただし書） 22
3-1-2 届出期限（主務省令第2条第1項等） 23
3-1-3 届出方法 24
3-1-4 届出事項（主務省令第2条第5項） 24
3-1-5 記載例（主務省令様式第1） 27
3-1-6 経済安全保障法に基づく導入等届出を行っている場合の取扱い（主務省令第2条第4項） 29
3-2 変更届出（法第4条第3項、主務省令第3条） 29
3-2-1 届出期限（主務省令第3条第1項等） 31
3-2-2 届出方法 31
3-2-3 届出事項（主務省令様式第2） 31
3-2-4 記載例（主務省令様式第2） 32

3-2-5 経済安全保障法に基づく導入等届出や変更の報告を行っている場合の取扱い（主務省令第3条第2項において準用する第2条第4項及び第3条第3項）.....33
4. 補足事項 届出手順の一例.....35
4-1 ステップ 1 特定重要設備と関連システムの特定.....35
4-1-1 ステップ 1-1 対象範囲の理解.....36
4-1-2 ステップ 1-2 関係者との事前調整.....36
4-1-3 ステップ 1-3 対象範囲の特定.....36
4-2 ステップ 2 届出対象の特定.....36
4-3 ステップ 3 届出用システム概略図の整理.....36
4-3-1 ステップ 3-1 システム概略図（全体版）の作成.....37
4-3-2 ステップ 3-2 システム概略図（詳細版）の作成.....38
4-4 ステップ 4 届出用資産一覧の整理.....43
4-4-1 ステップ 4-1 電子計算機の一覧化.....43
4-4-2 ステップ 4-2 届出を求める電子計算機の抽出.....43
4-4-3 ステップ 4-3 届出資産一覧の作成.....43
4-5 ステップ 5 資産届出の実施.....43
5. 特定侵害事象等の範囲等.....44
5-1 特定侵害事象（法第2条第4項、第5項）.....44
5-1-1 マルウェアの供用（法第2条第4項第1号、第5項）.....44
5-1-2 不正アクセス（法第2条第4項第2号、第5項）.....45
5-1-3 業務妨害等（法第2条第4項第3号、第5項）.....48
5-2 特定侵害事象の原因となり得る事象（法第5条）.....49
5-2-1 特定重要設備等における特定侵害事象の原因となり得る事象（法第5条、主務省令第4条第1項第1号）.....51
5-2-2 特定重要設備等以外における特定侵害事象の原因となり得る事象（法第5条、主務省令第4条第1項第2号）.....52
5-3 一般的なサイバー攻撃の類型との関係.....52
5-3-1 DDoS 攻撃事案.....53
5-3-2 ランサムウェア事案.....53
5-3-3 その他サイバー攻撃事案（不正アクセス、情報窃取等）.....53
5-4 特定侵害事象等に該当しない事象.....54
5-5 特定侵害事象等の発生の認知.....54
6. 報告手続.....55
6-1 報告対象（法第5条、主務省令第4条第2項）.....56
6-2 報告期限（法第5条、主務省令第4条第2項）.....57
6-3 報告方法.....57
6-4 報告事項.....58

7. 補足事項 59
7-1 FAQ 59
他の法令との関係.....61
8. 付録.....62
8-1 サイバー攻撃の脅威 62
海外の重要情報インフラ事業者へのサイバー攻撃事例 62
8-2 参考となる他ガイドライン 63
個人情報の保護に関する法律についてのガイドライン 63
経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度の解説 63
制御システムのセキュリティリスク分析ガイド 第 2 版（令和 8 年 4 月 6 日情報処理推進機構） 63
独立行政法人情報処理推進機構「情報システム・モデル取引・契約書（第二版）」 63
独立行政法人情報処理推進機構「制御システム関連のサイバーインシデント事例」シリーズ 63
The MITRE Corporation「MITRE ATT&CK」 64
ISA/IEC 62443.....64
8-3 用語の解説.....64

1. 本解説の概要

1-1 目的

本解説は、特別社会基盤事業者による特定重要電子計算機の届出及び特定侵害事象等を認知した際の報告が円滑に行われるよう支援すること、及び当該支援により特別社会基盤事業者の特別社会基盤事業等におけるサイバーセキュリティの確保をより確実なものとすることを目的として、法第2条第2項第2号、第4条及び第5条の届出等に関する事項等を解説するものである。

本解説において記述した具体例は、事業者の理解を助けることを目的として典型的なものを示したものであり、全ての事案を網羅したものでなく、記述した内容に限定する趣旨で記述したものでもない。また、記述した具体例においても、個別ケースによっては別途考慮すべき要素もあり得るので注意を要する。

1-2 対象事業者

本解説の対象事業者は、特別社会基盤事業者である。

1-3 構成

本解説の構成は、以下のとおりである。

1. 本解説の概要

   本解説の目的、対象事業者及び構成について記載している。

2. 特定重要電子計算機の範囲

   法の対象となる特定重要電子計算機の範囲を定めている。

3. 特定重要電子計算機の届出

   法第4条の規定に基づく特定重要電子計算機の届出の方法等を定めている。

4. 補足事項　届出手順の一例

   特定重要電子計算機の届出に当たり、望ましい手順の一例を示している。なお、4.の内容については、従わなかったことをもって法違反と判断されることはない。

5. 特定侵害事象等の範囲

   法第5条の規定に基づく報告が必要な特定侵害事象等の範囲を定めている。

6. 報告手続

   法第5条の規定に基づく特定侵害事象等の報告の方法等を定めている。

7. 補足事項

   法第5条の規定に基づく特定侵害事象等の報告におけるFAQ等を定めている。

8. 付録

   本解説の付録として、参考となる資料等を示している。

【省略用語例】

この解説において使用した次の省略用語は、それぞれ次に掲げる法令を示すものである。

・法……重要電子計算機に対する不正な行為による被害の防止に関する法律（令和7年法律第 42 号）（別称：サイバー対処能力強化法）

・政令……重要電子計算機に対する不正な行為による被害の防止に関する法律施行令（令和8年政令第 47 号）

・主務省令…重要電子計算機に対する不正な行為による被害の防止に関する法律に基づく特別社会基盤事業者による特定侵害事象等の報告等に関する命令（令和8年内閣府・総務省・法務省・財務省・厚生労働省・農林水産省・経済産業省・国土交通省令第4号）

2. 特定重要電子計算機の範囲（法第2条第2項第2号等）

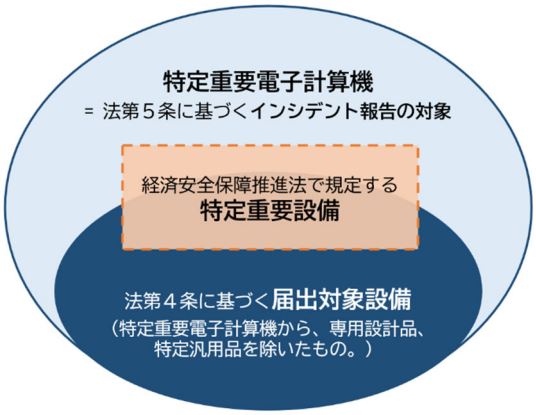
2-1 範囲の概要（法第2条第2項第2号）

○法 （定義） 第二条 （略） 2 この法律において「重要電子計算機」とは、次の各号のいずれかに該当する電子計算機（当該電子計算機に組み込まれたプログラム（電子計算機に対する指令であって、一の結果を得ることができるように組み合わされたものをいう。第四十二条第一項及び第二項において同じ。）を含む。以下同じ。）をいう。 一 （略） 二 特定社会基盤事業者（経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和四年法律第四十三号）第五十条第一項に規定する特定社会基盤事業者をいう。次項において同じ。）が使用する電子計算機のうち、そのサイバーセキュリティが害された場合において、同条第一項に規定する特定重要設備の機能が停止し、又は低下するおそれがあるものとして政令で定めるもの（当該特定重要設備の一部を構成するものを含む。） 三 （略） 3～9 （略）

法第2条第2項第2号においては、特定重要電子計算機の範囲について、特定社会基盤事業者が使用する電子計算機（同項柱書において、当該電子計算機に組み込まれたプログラム（電子計算機に対する指令であって、一の結果を得ることができるように組み合わされたものをいう。以下同じ。）を含むとされている。）のうち、そのサイバーセキュリティが害された場合において、特定重要設備の機能が停止し、又は低下するおそれがあるものとして政令で定めるもの（当該特定重要設備の一部を構成するものを含む。）と定めている。「特定社会基盤事業者が使用する電子計算機」については 2-1-1、「電子計算機に組み込まれたプログラム」については 2-1-2 を参照されたい。

なお、特定重要電子計算機に該当する場合であっても、第4条の規定に基づく届出の対象とならない場合があり、詳細は、3-1-1 を参照されたい。また、特別社会基盤事業者は、特定重要電子計算機ではない機器についても任意での届出を行うことが可能である。特定重要設備、特定重要電子計算機及び届出対象設備の関係は、図1のとおりである。

図1　特定重要設備、特定重要電子計算機及び届出対象設備の関係



※特定重要設備のうち電子計算機ではない設備については、重要電子計算機には該当しない

2-1-1　特定社会基盤事業者が使用する電子計算機

法第2条第2項第2号に該当する特定重要電子計算機は、特定社会基盤事業者が使用する電子計算機が対象である。「特定社会基盤事業者が使用する電子計算機」とは、必ずしも当該電子計算機を所有している必要はなく、特定社会基盤事業者が現にその事業に使用している電子計算機を指す。例えば、以下のような場合も、特定重要電子計算機に該当し得る。

実質的に他組織（グループ会社、システムベンダー、その他の供給者等）が所有している場合

なお、他組織に対し、届出等に必要な情報の提供を求めるに当たっては、私的独占の禁止及び公正取引の確保に関する法律（昭和 22 年法律第 54 号）、製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律（昭和 31 年法律第 120 号）並びに特定受託事業者に係る取引の適正化等に関する法律（令和5年法律第 25 号）等に違反することがないよう留意する。

クラウドサービスを使用する場合

なお、クラウドサービス事業者に対し、届出等に必要な情報の提供を求めるに当たっては、私的独占の禁止及び公正取引の確保に関する法律、製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律並びに特定受託事業者に係る取引の適正化等に関する法律等に違反することがないよう留意する。

日本国外に存在する場合

なお、諸外国においてはデータの国内保管義務や国外へのデータ移転を制限する（いわゆるデータローカライゼーション）法律が施行されていることがあるため、この対応に留意する。

他の特別社会基盤事業者と共同利用している場合又は共同で構築されている場合

該当する電子計算機を複数の特別社会基盤事業者が利用している、又は異なる特別社会基盤事業者が該当する電子計算機を共同で構築した場合でも、当該電子計算機は特別社会基盤事業者各社が使用する電子計算機に該当し、当該特別社会基盤事業者各社が届出等の義務を負う。

災害復旧サイトである場合

災害復旧サイト（DR サイト、被災時やサイバー攻撃を受けた際に備えて、通常稼働するシステムとは異なる環境下に予備機器やシステムを設置するケースを指し、同環境下における冗長性確保とは異なることに留意する。）についても、2-2-2 及び 2-2-3 に定める類型に該当する場合には、特定重要電子計算機に該当する。

2-1-2 電子計算機に組み込まれたプログラム

法第2条第2項においては、特定重要電子計算機には、当該電子計算機に組み込まれたプログラム（電子計算機に対する指令であって、一の結果を得ることができるように組み合わされたものをいう。）を含むとしており、ハードウェアのみならず、ファームウェア、オペレーティングシステム、ミドルウェア、アプリケーション等、ハードウェアに指令を与える無体物も特定重要電子計算機に含まれうる。

2-2 特定重要電子計算機の類型（政令第１条第３項等）

○政令

（重要電子計算機）

第一条 （略）

２ （略）

３ 法第二条第二項第二号の政令で定める電子計算機は、経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和四年法律第四十三号）第五十条第一項に規定する特定社会基盤事業者が使用する電子計算機のうち、次に掲げるものとする。

一 特定重要設備（経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律第五十条第一項に規定する特定重要設備をいう。以下この項において同じ。）である電子計算機又は特定重要設備の一部を構成する電子計算機

二 特定重要設備と電気通信回線で直接又は間接に接続されている電子計算機（前号に掲げる電子計算機を除く。）であって、当該特定重要設備に対し、当該特定重要設備の機能に影響を与える電磁的記録（法第二条第八項第二号に規定する電磁的記録をいう。次号において同じ。）を送信する機能を有するものとして主務省令（特別社会基盤事業所管大

臣（法第四条第一項に規定する特別社会基盤事業所管大臣をいう。第三条第一項において同じ。）及び内閣総理大臣の発する命令をいう。次号において同じ。）で定めるもの

三　第一号に掲げる電子計算機（以下この号において「一号電子計算機」という。）による情報処理の用に供される電磁的記録を作成するために用いられる電子計算機（前二号に掲げる電子計算機を除く。）のうち、当該電磁的記録が一定の期間ごとに当該一号電子計算機に入力されるものであって、当該電磁的記録が当該一定の期間ごとに当該一号電子計算機に入力されなくなった場合には当該一号電子計算機に係る特定重要設備の機能が停止し、又は低下することとなるものとして主務省令で定めるもの

4　（略）

〇主務省令

（重要電子計算機）

第一条　重要電子計算機に対する不正な行為による被害の防止に関する法律施行令（以下この条において「令」という。）第一条第三項第二号の主務省令で定める電子計算機は、特定重要設備（経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和四年法律第四十三号。以下「経済安全保障推進法」という。）第五十条第一項に規定する特定重要設備をいう。以下同じ。）と電気通信回線（公衆の用に供されているものを除く。）で直接又は間接に接続されている電子計算機（令第一条第三項第一号に掲げるものを除く。）であって、次のいずれかに該当するものとする。

一　特定重要設備に電磁的記録（重要電子計算機に対する不正な行為による被害の防止に関する法律（以下「法」という。）第二条第八項第二号に規定する電磁的記録をいう。以下同じ。）を送信する機能を有する電子計算機であって、当該電磁的記録を送信するに当たり、経路制御（電気通信信号を送信するに当たり、宛先に至る経路のうちから、経路の状況等に応じて最も適切と判断したものに電気通信信号を送信すること（送信することのできる二以上の経路のうちから、宛先ごとに一に定められた経路に電気通信信号を送信することを除く。）をいう。次号において同じ。）がされないもの

二　ルーティング機器（電気通信信号を送受信する機器であって、経路制御を行う機能を有するものをいう。以下この号において同じ。）のうち、他のルーティング機器を介さずに一号電子計算機（令第一条第三項第三号に規定する一号電子計算機をいう。以下同じ。）に電気通信信号を送信するもの

三　ファイアウォール等（電気通信信号を送受信する機器であって、受信した電気通信信号のうち当該電気通信信号に使用されるプログラム（法第二条第二項に規定するプログラムをいう。以下この号並びに次条第一項第一号及び第四項において同じ。）又は当該プログラムを識別するために割り当てられる番号、記号その他の符号が一定の基準に適合するもののみを当該機器に接続されている他の電子計算機に送信する機能を有するものをいう。以下この号及び次号において同じ。）であって、他のファイアウォール等を介さずに一号電子計算機に電気通信信号を送信するもの

四　特定重要設備に送信される電磁的記録を一時的に保存する機能を有する電子計算機であって、ファイアウォール等を介してのみ当該電磁的記録を送受信することができるもの及び当該ファイアウォール等

五　次に掲げるもののいずれかを保存する電子計算機（一時的に保存するものを除く。）

イ　一号電子計算機及びこの条に規定する電子計算機（このイに掲げるものを保存するものを除く。）の総体に係るネットワーク構成図（これらの電子計算機のアイ・ピー・アドレス（電気通信事業法（昭和五十九年法律第八十六号）第百六十四条第二項第三号に規定するアイ・ピー・アドレスをいう。第七号及び次項第二号において同じ。）又は通信の当事者が電気通信信号の送信先となる電気通信設備（同法第二条第二号に規定する電気通信設備をいう。第七号及び同項第二号において同じ。）を識別するために使用する番号、記号その他の符号が記載されているものに限る。）

ロ　一号電子計算機又はこの項に規定する電子計算機（このロに掲げるものを保存するもの及び次号に規定するものを除く。）のうちの一の電子計算機の利用に係る全ての識別符号（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号。以下「不正アクセス禁止法」という。）第二条第二項に規定する識別符号をいう。第四条第一項第一号ロ、ハ及びホにおいて同じ。）

六　一号電子計算機又はこの項に規定する電子計算機（前号ロに掲げるものを保存するもの及びこの号に規定するものを除く。）に係るアクセス制御機能（不正アクセス禁止法第二条第三項に規定するアクセス制御機能をいう。以下同じ。）を有する電子計算機

七　アイ・ピー・アドレスを割り当てられた電気通信設備である電子計算機

2　令第一条第三項第三号の主務省令で定める電子計算機は、一号電子計算機による情報処理の用に供される電磁的記録を作成するために用いられる電子計算機（一号電子計算機及び前項各号に規定するものを除く。）であって、当該電磁的記録が一定の期間ごとに当該一号電子計算機に入力されるもののうち、次のいずれかに該当するものとする。

一　次号に規定する電子計算機に係るアクセス制御機能を有する電子計算機

二　アイ・ピー・アドレスを割り当てられた電気通信設備である電子計算機

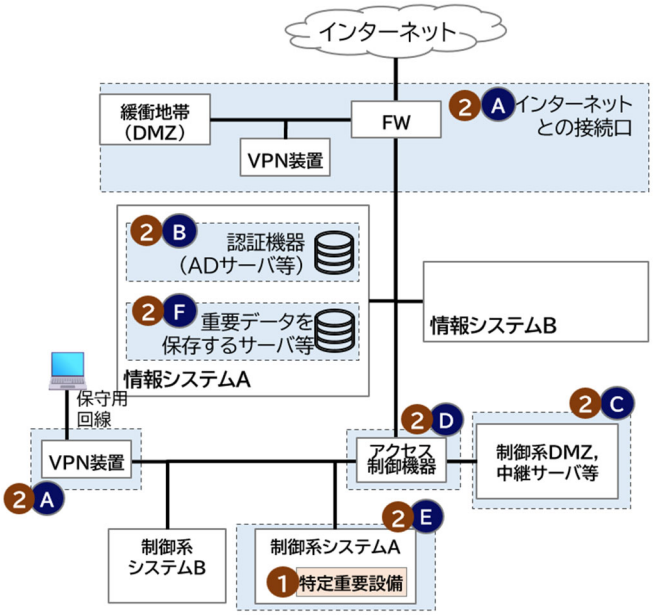
政令及び主務省令において、以下の表1及び図2のとおり特定重要電子計算機の類型を定めている。それぞれの詳細を 2-2-1 から 2-2-3 までにおいて示す。

表1　特定重要電子計算機の類型の全体像

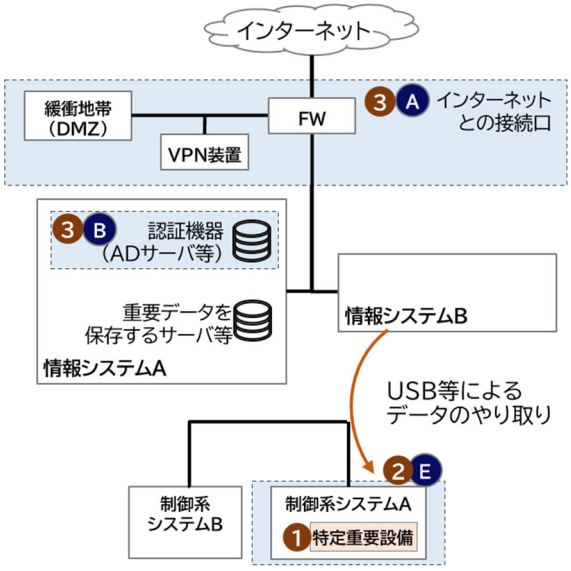
政令の類型	省令の類型
①特定重要設備である電子計算機等（一号電子計算機） （政令第1条第3項第1号）	—
②特定重要設備と接続されている電子計算機 （政令第1条第3項第2号）	[A]インターネットとの接続口の機器（アタックサーフェス） （主務省令第1条第1項第7号）
	[B]特定重要電子計算機に係るシステムの認証を提供する機器 （主務省令第1条第1項第6号）
	[C]特定重要設備を含むセグメントの DMZ その他当該セグメントにアクセス可能な機器 （主務省令第1条第1項第4号）
	[D]特定重要設備を含むセグメントへの通信を制御する機器 （主務省令第1条第1項第3号）
	[E]特定重要設備と同一セグメントの機器 （主務省令第1条第1項第1号及び第2号）
	[F]特定重要電子計算機に関する重要データを保存している機器 （主務省令第1条第1項第5号）
③USB やクラウドサービス等の特定重要設備にデータを入力可能な電子計算機 （政令第1条第3項第3号）	[A]インターネットとの接続口の機器 （主務省令第1条第2項第2号）
	[B]特定重要電子計算機に係るシステムの認証を提供する機器 （主務省令第1条第2項第1号）

図2　特定重要電子計算機の類型のイメージ

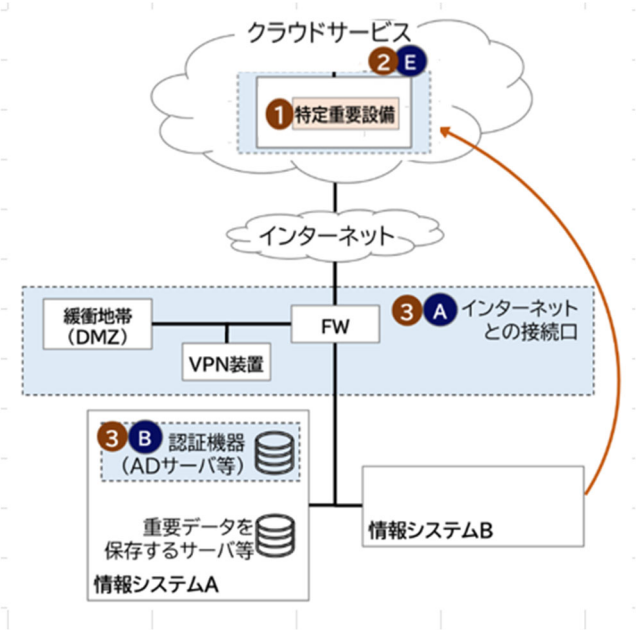
（特定重要設備と電子計算機が電気通信回線で接続される場合）



（特定重要設備と USB 等で定期的なデータのやり取りがある場合）



（クラウドサービスを使用する特定重要設備とインターネットで
定期的なデータのやり取りがある場合）



2-2-1 ①特定重要設備である電子計算機又は特定重要設備の一部を構成する電子計算機（一号電子計算機）（政令第１条第３項第１号）

「特定重要設備の一部を構成する電子計算機」とは、特定重要設備が電子計算機その他の設備等により構成されている場合に、当該電子計算機を指す。具体例としては、特定重要設備が複数の電子計算機から構成された一連のシステムを指す場合に当該複数の電子計算機が該当する。構成設備である電子計算機もこれに含まれる。

2-2-2 ②特定重要設備と接続されている電子計算機（政令第１条第３項第２号及び主務省令第１条第１項）

特定重要設備と電気通信回線で直接又は間接に接続されている電子計算機（①の電子計算機を除く。）であって、当該特定重要設備に対し、当該特定重要設備の機能に影響を与えるデータを送信する機能を有するものとして主務省令で定めるものである。

ここでいう電気通信回線とは、有線・無線、物理・仮想の別を問わず、その管理主体も問わない。ただし、主務省令第1条において、公衆の用に供されている電気通信回線を除くこととしており、特定重要設備とインターネット等を介して接続する電子計算機（IP-VPN や IPsec 等により閉域網と同等の形態で接続している場合を除く。）は、②の対象とはならない。

また、「直接に接続」とは、当該電子計算機が、他の電子計算機や情報システムとの間で他の電子計算機や情報システムが介在することなく電気通信回線で接続されている場合をいい、「間

接に接続」とは、当該電子計算機が、他の電子計算機や情報システムとの間で他の電子計算機や情報システムを介して電気通信回線で接続されている場合をいう。

具体的には次の[A]から[F]までの電子計算機が該当する。

[A] インターネットとの接続口の機器（アタックサーフェス）（主務省令第１条第１項第7号）

いわゆるグローバル IP アドレスを割り当てられた機器が該当し、具体例は以下のとおりである。

なお、VPN 機器については、VPN の方式（インターネット VPN、IP-VPN、広域イーサネット、エントリーVPN 等）に関わらず、グローバル IP アドレスを割り当てられているものは対象である。

1. インターネットとの接続部に設置され、グローバル IP アドレスを利用して電気通信が到達可能な機器（Web サーバー、メールサーバー等）
2. Web サーバーへの電気通信を中継する機器（WAF、リバースプロキシー等）
3. 1.及び 2.に関する通信を制御する機器（FW、UTM 等）
4. 特定重要設備の保守に利用する機器（インターネット接続が可能な保守端末等）

なお、以下の機器は特定重要電子計算機に含まれないが、法目的に照らすと、アタックサーフェスに類する機器として任意で届出を行うことが望ましい。

5. インターネット接続部に設置された、グローバル IP アドレスを保有する機器（リバースプロキシー等）に中継されることで、インターネットからの電気通信が到達可能な機器（リバースプロキシー配下の Web サーバー等）
6. 1.、2.、及び 5.に関する電気通信のうち、異常な電気通信を制限する機器（IPS 等）
   ※なお、電気通信の監視のみ行う機器（IDS 等）は 6. に該当しないが、電気通信を制限する機能と監視する機能を共に有する場合は、6.に該当するものとする。

[B] 特定重要電子計算機に係るシステムの認証を提供する機器（主務省令第１条第１項第6号）

①の電子計算機及び②の特定重要設備と接続されている電子計算機（[B]特定重要電子計算機に係るシステムの認証を提供する機器及び[F]特定重要電子計算機に関する重要データを保存している機器のうち(ロ)認証情報を保存する機器を除く。）のアクセス制御を行う電子計算機が対象である。

具体的には、識別符号や権限設定を用いて、アクセスを求めるユーザーが正当であることの確認（認証）、及びアクセスの許可（認可）を行う機器（AD サーバー、LDAP サーバー、Kerberos サーバー、SAML や OAuth 2.0 の構成機器、生体認証サーバー等）が該当する。また、SaaS 形態で提供されている IDaaS 等も該当する。ただし、特定社会基盤役務に明らかに関わらない機器（特定重

要設備若しくは構成設備に対し通信を行わない、送付データを生成しない、又はコマンド送信を行わない機器等）に関する認証機器は本定義の対象外である。

なお、認証等を一元的に管理する機器が対象であり、間接的に認証機能を保有する機器（端末、Web サーバー、メールサーバー等）、及び通常業務を間接的にサポートするうえで認証機能を備える機器（プリンター、会議室予約、電子錠、いわゆる OA 系等）全てを指すものではない。内部通信を目的とした機器同士の相互認証は含めないことに留意する。

[C] 特定重要設備を含むセグメントの DMZ その他当該セグメントにアクセス可能な機器（主務省令第１条第１項第４号）

特定重要設備に送信されるデータを一時的に保存し、ファイアウォール等を介してのみ当該データを送受信することができるもの及び当該ファイアウォール等が該当する。ここでいう「ファイアウォール等」とは、電気通信信号を送受信する機器であって、受信した電気通信信号に使用されるプログラム又は当該プログラムを識別するために割り当てられる番号が一定の基準に適合するもののみを当該機器に接続されている他の電子計算機に送信する機能を有するものをいい、具体的には、狭義の FW、WAF 等が該当する。

具体的には、信頼性が異なる二つ以上のネットワークにおける境界に設けられ、特定重要設備若しくは構成設備に対する通信の中継を担う領域にある機器が該当する。ISA/IEC 62443 で”Industrial DMZ”（L3.5）として定義される領域にある機器と捉えてもよい。特定重要設備若しくは構成設備に対してアクセス制御機器によってのみ中継される何らかの通信（参照、更新、コマンド送付、データ送信等）を行う機器（踏み台サーバー、FTP サーバー、監視サーバー等）が対象となる。

[D] 特定重要設備を含むセグメントへの通信を制御する機器（主務省令第１条第１項第３号）

ファイアウォール等であって、他のファイアウォール等を介さずに①の電子計算機に電気通信信号を送信するものが該当する。

具体的には、接続元の IP アドレスやセグメントを参照し、通信を許可、又は拒否すべきか制御を行う機器（情報ダイオード、UTM、IPS、WAF、アクセス制御用アプライアンス、アクセス制御を行っている HMI、SaaS の場合は CASB、IAP、MDM、WAF 等）が該当する。

なお、通信経路にある全てのアクセス制御機器が対象ではなく、あくまで特定重要設備の直近にあるものが対象であること（UTM と複数の L3SW が存在する場合は、L3SW は該当せず、UTM が該当する。L3SW のみで制御されている場合は、L3SW が該当する等）に留意する。また、制御機能を持たない通信機器（ノンインテリジェントハブ、ノンインテリジェントスイッチ等）は、[D]には該当しない（[E]の要件に該当する場合もあることに留意。）。

[E] 特定重要設備と同一セグメントの機器（主務省令第１条第１項第１号及び第２号）

以下の2つの機器が該当する。

(イ)特定重要設備にデータを送信する機能を有する電子計算機であって、当該データを送信するに当たり、ルーティングがされないもの

具体的には、①の電子計算機と同一サブネット上の機器又は同一 VLAN 上の機器と捉えてもよい。なお、同一サブネット、又は同一 VLAN 上の機器であっても、何らかの方法（論理的な方法を含む。）で通信が一方向化されており、①の電子計算機への通信が行えない場合は該当しない。

(ロ) ルーティング機器のうち、他のルーティング機器を介さずに①の電子計算機に電気通信信号を送信するもの

具体的には、L3SW 等が該当する。

[F] 特定重要電子計算機に関する重要データを保存している機器（主務省令第１条第１項第５号）

特定重要電子計算機のサイバーセキュリティを確保する観点から重要な以下の情報（ネットワーク構成図、認証情報）を保存している機器であり、以下の2つの機器が該当する。なお、これらの情報を保存する機器が対象であり、保存された情報そのものや機器の設定（UTM 内のルーティング設定、端末内の MAC アドレス、サーバー内の接続許可リスト等）は対象でない。

(イ)ネットワーク構成図を保存する機器

ここでいうネットワーク構成図は、（ｉ）特定重要電子計算機（(イ)ネットワーク構成図を保存する機器を除く。）の総体にかかるもののうち（ⅱ） IP アドレス（ここでは、いわゆるグローバル IP アドレスのほか、ローカル IP アドレスも含む。）が記載されているものであって(ⅲ)一時的に保存されるもの以外のものに限られる。例えば、特別社会基盤事業者の使用する特定重要電子計算機のうち一部の特定重要電子計算機のネットワーク構成図しか保存しないもの、IP アドレスが記載されていないもの、社内外への情報共有等のために一時的に作られたものはこれに該当しない。

(ロ)認証情報を保存する機器

（ｉ）一の特定重要電子計算機（(ロ)認証情報を保存する機器及び[B]特定重要電子計算機に係るシステムの認証を提供する機器を除く。）の識別符号（ID、パスワード等）の全部を保存しているものであって （ⅱ）一時的に保存されるもの以外のものが該当する。例えば、ID・パスワードのうち一部のみを保存するもの、一時的に ID・パスワードを保存するものを除く。

2-2-3 ③USB やクラウドサービス等の特定重要設備にデータを入力可能な電子計算機（政令第１条第３項第３号及び主務省令第１条第２項）

①の電子計算機による情報処理の用に供されるデータを作成するために用いられる電子計算機（①及び②の電子計算機を除く。）のうち、当該データが一定の期間ごとに当該①に入力されるものであって、当該データが当該一定の期間ごとに当該①に入力されなくなった場合には当該①に係る特定重要設備の機能が停止し、又は低下することとなるものとして主務省令で定めるものである。

例えば、特定重要設備の保守等の目的で、作成したデータを定期的に USB を介して特定重要設備に入力する場合や、特定重要設備においてクラウドサービスを使用しており、オンプレの社内設備において作成したデータを定期的にインターネットを介して当該特定重要設備に入力する場合等が該当する。

具体的には次の[A]及び[B]の電子計算機が該当する。

[A] インターネットとの接続口の機器（アタックサーフェス）（主務省令第１条第２項第２号）

いわゆるグローバル IP アドレスを割り当てられた機器が該当し、具体例は、2-2-2[A]のとおりである。

[B] 特定重要電子計算機に係るシステムの認証を提供する機器（主務省令第１条第２項第１号）

2-2-3[A]に係るアクセス制御機能を有する機器が該当し、具体例は、2-2-2[B]のとおりである。

3. 特定重要電子計算機の届出（法第4条）

3-1 新規届出（法第4条第1項、主務省令第2条等）

○法

（特定重要電子計算機の届出）

第四条　特別社会基盤事業者は、特定重要電子計算機を導入したときは、主務省令で定めるところにより、特定重要電子計算機の製品名及び製造者名その他の主務省令で定める事項を特別社会基盤事業（特別社会基盤事業者が行う経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律第五十条第一項に規定する特定社会基盤事業をいう。）を所管する大臣（以下「特別社会基盤事業所管大臣」という。）に届け出なければならない。

2～4　（略）

附　則

（特定重要電子計算機の届出に関する経過措置）

第四条　この法律の施行の際現に特定重要電子計算機を導入している特別社会基盤事業者に対する第四条第一項の規定の適用については、同項中「特定重要電子計算機を導入したときは」とあるのは、「この法律の施行の日から六月以内に」とする。

○主務省令

（特定重要電子計算機の届出）

第二条　法第四条第一項の規定による届出は、次に掲げる特定重要電子計算機について、当該特定重要電子計算機を導入した日から四月以内に、様式第一による届出書を特別社会基盤事業所管大臣に提出して行うものとする。ただし、当該特定重要電子計算機が一の特別社会基盤事業者若しくは複数の特別社会基盤事業者のうち、親法人等（経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律施行令（令和四年政令第三百九十四号）第十条第三項に規定する親法人等をいう。以下この項において同じ。）が同一であるもの若しくは一方の者が他方の者の親法人等であるものの事業の用に供されるものである場合又は広く一般に使用されているものとして特別社会基盤事業所管大臣及び内閣総理大臣が指定するものである場合は、この限りでない。

一　アプライアンス（特定の用途に供されるプログラムが組み込まれた特定重要電子計算機であって、当該プログラム以外のプログラムが通常組み込まれないものをいう。次号において同じ。）に係るハードウェア

二　アプライアンス以外の特定重要電子計算機に組み込まれたオペレーティングシステム、ミドルウェア及びアプリケーション

2　特別社会基盤事業者が経済安全保障推進法第五十条第一項の規定による指定を受けた日から二月以内に導入した特定重要電子計算機（当該指定に係る特定社会基盤事業（同項に

規定する特定社会基盤事業をいう。第四条第二項第一号において同じ。）の用に供される特定重要設備に係るものに限る。）に対する前項の規定の適用については、同項中「当該特定重要電子計算機を導入した日から四月以内」とあるのは、「経済安全保障推進法第五十条第一項の規定による指定を受けた日から六月以内」とする。ただし、当該特別社会基盤事業者が経済安全保障推進法第五十三条第一項各号のいずれかに掲げる事由により経済安全保障推進法第五十条第一項の主務省令で定める基準に該当することとなった者である場合は、この限りでない。

3　経済安全保障推進法第五十条第一項の特定重要設備を定める主務省令の改正により新たに特定重要電子計算機となった電子計算機であって、当該特定重要電子計算機となった日から二月以内に導入したものに対する第一項の規定の適用については、同項中「当該特定重要電子計算機を導入した日から四月以内」とあるのは、「経済安全保障推進法第五十条第一項の特定重要設備を定める主務省令の改正により新たに特定重要電子計算機となった日から六月以内」とする。

4　特定重要設備又は構成設備（経済安全保障推進法第五十二条第二項第二号ハの主務省令で定める設備、機器、装置又はプログラムをいう。以下この項及び次条第三項において同じ。）である特定重要電子計算機に係る第一項の届出書については、経済安全保障推進法第五十二条第一項又は第十一項の規定による当該特定重要設備の導入の届出を行っている場合（当該特定重要設備又は当該構成設備の名称が当該特定重要電子計算機の製品名（クラウド・コンピューティング・サービス（情報通信技術を活用した行政の推進等に関する法律（平成十四年法律第百五十一号）第二十三条第一項に規定するクラウド・コンピューティング・サービスをいう。以下この項において同じ。）の使用に係る特定重要電子計算機にあっては、当該クラウド・コンピューティング・サービスの名称。次項第四号及び次条第三項において同じ。）と同一であり、かつ、当該特定重要設備又は当該構成設備の供給者の名称又は氏名が当該特定重要電子計算機の製造者名（クラウド・コンピューティング・サービスの使用に係る特定重要電子計算機にあっては、当該クラウド・コンピューティング・サービスを提供する事業者名。次項第五号において同じ。）と同一である場合に限る。）には、当該届出に係る経済安全保障推進法第五十二条第一項に規定する導入等計画書（経済安全保障推進法の規定による変更をしたときは、その変更後のもの）又は同条第十一項に規定する緊急導入等届出書（経済安全保障推進法の規定による変更をしたときは、その変更後のもの）及び特別社会基盤事業者の連絡先を記載した書面の提出をもって、当該特定重要電子計算機に係る第一項の規定による届出書の提出に代えることができる。

5　法第四条第一項の主務省令で定める事項は、次に掲げる事項とする。

一　特別社会基盤事業者の概要

二　特定重要電子計算機に係る特定重要設備の区分

三　特定重要電子計算機の区分

四　特定重要電子計算機の製品名

五　特定重要電子計算機の製造者名

附　則

（経過措置）

2　この命令の施行の際現に導入されている特定重要設備に係る特定重要電子計算機（この命令の施行の際現に導入されている特定重要電子計算機を除く。）であって、当該施行の日から二月以内に導入したものに対する第二条第一項の規定の適用については、同項中「当該特定重要電子計算機を導入した日から四月以内」とあるのは、「この命令の施行の日から六月以内」とする。

特別社会基盤事業者は、特定重要電子計算機を導入したときは、特定重要電子計算機の製品名及び製造者名等を特別社会基盤事業所管大臣に届け出なければならない。

3-1-1　届出対象（主務省令第2条第1項）

届出対象となるものは、特定重要電子計算機のうち、以下のものである。

なお、新規に導入した特定重要電子計算機のほか、既に使用している電子計算機であって、法の施行、経済安全保障推進法第 50 条第1項に基づく特定社会基盤事業者の指定等により、新たに特定重要電子計算機となったものについても、届出対象であることに留意する。

アプライアンスの場合

アプライアンスとは、特定の用途に供されるプログラムが組み込まれた特定重要電子計算機であって、当該プログラム以外のプログラムが通常組み込まれないものをいう。ソフトウェアとハードウェアを包含した設備が届出対象となり、アプライアンスに組み込まれた各種プログラムは届出の対象外である。

アプライアンス以外の電子計算機の場合

アプライアンス以外の電子計算機については、当該電子計算機に組み込まれたオペレーティングシステム、ミドルウェア及びアプリケーションが届出の対象となり、ハードウェアは届出の対象外である。なお、ファームウェアは届出の対象外である。

ただし、上記の届出対象に該当する場合であっても、以下に該当するものは届出の対象とならない。

専用設計品である場合

一の特別社会基盤事業者若しくは複数の特別社会基盤事業者のうち、親法人等が同一であるもの又はグループ会社の関係等にある複数の特別社会基盤事業者の事業の用に供されてい

るものを指し、典型的には製品情報が市場に流通していないものを想定する。ここでいう「グループ会社の関係等にある複数の特別社会基盤事業者」とは、具体的には以下を指す。

・親法人等（経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律施行令（令和4年政令第 394 号）第 10 条第3項に規定する親法人等をいう。以下同じ。）が同一である複数の特別社会基盤事業者

・一方の者が他方の者の親法人等である複数の特別社会基盤事業者

なお、一般に流通する製品のカスタマイズやアドオン、プラグイン及び設定変更等により開発されたものは、専用設計品に含まず、届出の対象とする。

○経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律施行令 （法第五十二条第一項の政令で定める者） 第十条　（略） ２　（略） ３　前項に規定する「親法人等」とは、他の法人等（会社、組合その他これらに準ずる事業体をいう。以下この項において同じ。）の財務及び営業又は事業の方針を決定する機関(株主総会その他これに準ずる機関をいう。以下この項において「意思決定機関」という。)を支配している法人等として主務省令で定めるものをいい、前項に規定する「子法人等」とは、親法人等によりその意思決定機関を支配されている他の法人等をいう。この場合において、親法人等及び子法人等又は子法人等が他の法人等の意思決定機関を支配している場合における当該他の法人等は、その親法人等の子法人等とみなす。

広く一般に使用されている製品である場合（主務省令第２条第１項ただし書）

主務省令第2条第1項ただし書の「広く一般に使用されているものとして特別社会基盤事業所管大臣及び内閣総理大臣が指定するものである場合は、この限りでない」とは、多くの特別社会基盤事業者が導入、使用している製品（汎用品）である場合については、届出を不要とするものである。「特別社会基盤事業所管大臣及び内閣総理大臣が指定するもの」については、「重要電子計算機に対する不正な行為による被害の防止に関する法律に基づく特別社会基盤事業者による特定侵害事象等の報告等に関する命令（令和八年内閣府・総務省・法務省・財務省・厚生労働省・農林水産省・経済産業省・国土交通省令第四号）第二条第一項ただし書の特別社会基盤事業所管大臣及び内閣総理大臣が指定するもの（令和八年内閣府・総務省・法務省・財務省・厚生労働省・農林水産省・経済産業省・国土交通省告示第一号）」で定めており、以下に掲げる製品を指定している。

表2　広く一般に使用されている製品

製造者名	製品名
マイクロソフト・コーポレーション	Windows Windows Server

※製品のバージョン情報による取り扱いの差異はない。

3-1-2　届出期限（主務省令第2条第1項等）

届出期限は、原則特定重要電子計算機を導入した日から4月以内である。ただし、以下に掲げる特定重要電子計算機については、それぞれ以下に掲げる期限とする。

表3　届出期限の特例

法の施行（令和8年10月1日）の際現に導入している特定重要電子計算機	法の施行から6月以内（令和9年3月 31 日） （法附則第4条）
法の施行（令和8年10月1日）の際現に導入している特定重要設備に係る特定重要電子計算機であって、当該施行の日から2月以内に導入したもの （例）令和8年10月1日時点で既に導入している特定重要設備のアタックサーフェスに当たる機器を令和8年 11 月 15 日に新たに導入した場合等	法の施行から6月以内（令和9年3月 31 日） （主務省令附則第2項）
経済安全保障推進法第 50 条第1項の規定による指定を受けた日から2月以内に導入した特定重要電子計算機※1	特定社会基盤事業者の指定を受けた日から6月以内 （主務省令第2条第2項）
経済安全保障推進法第 50 条第1項の特定重要設備を定める主務省令の改正により新たに特定重要電子計算機となった電子計算機であって、当該特定重要電子計算機となった日から2月以内に導入したもの※2	当該特定重要電子計算機となった日から6月以内 （主務省令第2条第3項）

※1　特別社会基盤事業者が経済安全保障推進法第 53 条第1項各号のいずれかに掲げる事由（以下の事由）により経済安全保障推進法第 50 条第1項の主務省令で定める基準に該当することとなった者である場合を除く。

・他の特定社会基盤事業者から当該指定に係る特定社会基盤事業を譲り受けたこと。

・他の特定社会基盤事業者について合併又は分割があった場合において、当該合併後存続する法人、当該合併後存続する法人、当該分割により当該指定に係る特定社会基盤事業を承継した法人のいずれかの法人であること。

なお、既に使用されている電子計算機が、経済安全保障推進法第 50 条第1項の指定により新たに特定重要電子計算機となった場合は、当該指定を受けた日から6月以内に届け出ることとなる。

※2 既に使用されている電子計算機が、経済安全保障推進法第 50 条第1項の特定重要設備を定める主務省令の改正により新たに特定重要電子計算機となった場合は、当該特定重要電子計算機となった日から6月以内に届け出ることとなる。

届出期限が行政機関の休日(日曜日及び土曜日、国民の祝日に関する法律(昭和 23 年法律第 178 号)に規定する休日並びに 12 月 29 日から翌年の1月3日までの日)に当たるときは、行政機関の休日の翌日をもってその期限とみなす(行政機関の休日に関する法律(昭和 63 年法律第 91 号)第2条)。その他、期限の計算については、民法(明治 29 年法律第 89 号)第1編第6章の例による。

3-1-3 届出方法

届出方法については、官民連携基盤を介した提出を想定しており、手続きについては、当該基盤に係るマニュアルを参照する。その他、資産届出情報を格納したDVD 等による届出等の手続きについて、所管省庁に確認を行う。

3-1-4 届出事項(主務省令第2条第5項)

以下に掲げる事項を所定の様式に記載の上、所管大臣宛に提出しなければならない。

(a)特別社会基盤事業者の概要

特別社会基盤事業者の名称及び連絡先を記載する。

(b)特定重要電子計算機に係る特定重要設備の区分

特定重要電子計算機が経済安全保障推進法の主務省令で規定する特定重要設備のうち、どの特定重要設備に関連するものかを記載する(複数記載可)。

(c)特定重要電子計算機の区分

特定重要電子計算機の類型①から③まで、A から F まで、(イ)・(ロ)のうち、該当するもの(複数の重要電子計算機に該当する場合は、当該複数の重要電子計算機)を記載する。

特定重要電子計算機の区分の類型一覧

類型①:政令第1条第3項第1号

類型②A:主務省令第1条第1項第7号

類型②B：主務省令第1条第1項第6号
類型②C：主務省令第1条第1項第4号
類型②D：主務省令第1条第1項第3号
類型②E（イ）：主務省令第1条第1項第1号
類型②E（ロ）：主務省令第1条第1項第2号
類型②F（イ）：主務省令第1条第1項第5号のうちネットワーク構成図を保存するもの
類型②F（ロ）：主務省令第1条第1項第5号のうち認証情報を保存するもの
類型③A：主務省令第1条第2項第2号
類型③B：主務省令第1条第2項第1号

(d)特定重要電子計算機の製品名

製品名は正確に記載する。クラウドサービスを使用する場合は、当該クラウドサービスの名称（EC2、RDS 等）を記載する。

(e)特定重要電子計算機の製造者名

クラウドサービスを使用する場合は、当該クラウドサービスを提供する事業者名を記載する。

また、添付資料として、各特定重要電子計算機と他の特定重要電子計算機又は特定重要設備との関係を示す資料（システムの概略を記載した資料等、既存資料でも可。2-2-2[F](イ)に記載している IP アドレスが記載された詳細なネットワーク構成図の提出は必須ではない。）を提出しなければならない。

このほか、以下の事項については、届出義務はないが、可能な範囲で備考欄等に記載の上、提出することが望ましい。

表4　任意で届け出ることが望ましい事項

情報の種類	情報の内容
届出対象分類	届出を行う資産の分類を「アプライアンス製品」、「ソフトウェア」、「クラウドサービス」、「その他」の中から選択する。 ※「クラウドサービス」の分類は、利用しているクラウドサービスそのものの届出を行う際に使用する。当該クラウドサービスにインストールされているソフトウェアの情報の届出を行う場合には、「ソフトウェア」の分類を使用する。 ※「その他」の分類は、アプライアンス製品を除く、ソフトウェアの情報が収集できなかったシステム及び機器の情報を記入するために使用する。（他社が管理しており、搭載されたソフトウェアの情報を収集できないシステム等。）

情報の種類	情報の内容
（添付資料上の）システム名又は領域名	添付資料において、届出資産が搭載されている機器が含まれているシステムの名称、又は機器が設置されている領域の名称を記入する。システムの名称又は領域の名称は、システム概略図上の記載と完全に一致している必要がある。 ※システム概略図上の設置位置をより正確に紐づけるため、可能な限り、「システム名又は領域名」は、拠点名や機器ごとの通し番号等を付記した一意な名称とすることが望ましい。 ※システム概略図上において、当該資産が複数のシステムや複数の領域に含まれている場合は、複数のシステム名及び領域名を記載してもよい。
（添付資料上の）機器名	システム概略図において、届出資産、又は届出資産がインストールされている機器の名称を記入する。機器の名称は、システム概略図上の記載と完全に一致している必要がある。「製品名」とは異なり、当該機器が何の機器を指しているかが、届出者において判断できる粒度の名称が記入されていればよい。（例：FW、ファイルサーバー、保守端末等）
アプライアンス製品の概数	同一のアプライアンス製品を一つの行にまとめて記入した場合に、まとめた機器の概数を記入する。 アプライアンス製品の概数は、当該製品の脆弱性が発見された際、届出者への影響を把握する目的で使用する想定であるため、おおよその設置数が分かればよい。 ※他の届出対象分類については、概数の算出が困難であることから、アプライアンス製品のみ可能な範囲で記載することが望ましい。
バージョン情報	当該資産のバージョン情報（OS/ファームウェア/ミドルウェア/アプリケーションのバージョン等）を記入する。 ※バージョン情報の入力がない場合には、政府が提供する脆弱性情報の絞り込みができないため、政府から届出事業者に対し、過去を含めた当該資産の全バージョンに関連する脆弱性情報を提供することが困難となる。そのため、届出者において、提供された脆弱性情報の取捨選択が必要となる可能性がある。 ※同名の資産であるものの、バージョン情報だけが異なる資産がある場合は、行を分けて記載する。 （同一の行に複数のバージョン情報は記入できない。）

情報の種類	情報の内容
グローバル IP アドレス[1]	2-2-2[A]に規定するインターネットとの接続口の機器（アタックサーフェス）については、割り当てられたグローバル IP アドレスを備考欄に記入する。又は、機器と紐づかない形で特定重要電子計算機に関するグローバル IP アドレスをリスト化し、別紙に記載する。
資産設置環境の管理主体	当該資産を管理するための権限(運用管理権限やセキュリティ管理権限)を持つ主体の組織名を記入する。（自組織名又は委託先等の事業者名）
管理主体と届出者の関係性	届出者から見た当該資産の管理主体について、その関係性を記入する。

3-1-5 記載例（主務省令様式第１）

様式の記載例は以下のとおりである。なお、代表者の氏名は、旧姓でも差し支えない。連絡先については、本件における担当部局の連絡先を記載し、備考欄に「担当部局・担当者」を記載する。

[1] 特定重要電子計算機に関するグローバル IP アドレスを、政府が保有するサイバー脅威の情報と突合等し、潜在被害を発見するなど、被害の防止に資する分析を行う。

様式第一（第二条第一項関係）

特定重要電子計算機届出書

令和○年○月○日

○○大臣　　殿

住　　所　　東京都○○
名　　称　　株式会社○○
代表者の氏名　　○○　○○

重要電子計算機に対する不正な行為による被害の防止に関する法律第4条第1項の規定により、次のとおり届け出ます。

1.　特別社会基盤事業者の概要

特別社会基盤事業者の名称	（フリガナ）　カブシキガイシャ　○○ 株式会社　○○
連絡先	電話番号　○○-○○○○-○○○○　E-mail　○○○○@○○.co.jp

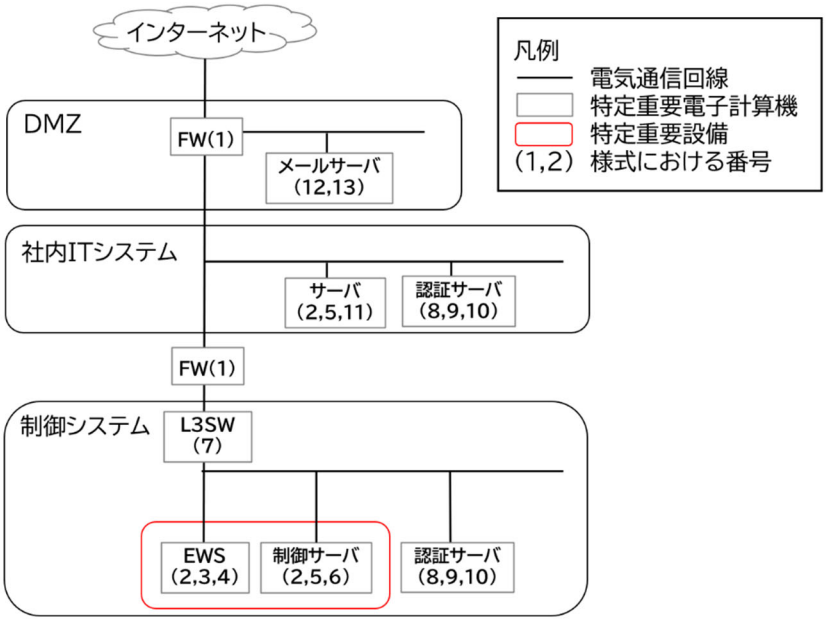
2.　特定重要電子計算機に係る特定重要設備の区分並びに特定重要電子計算機の区分、製品名及び製造者名

番号	特定重要設備の区分	特定重要電子計算機の区分	特定重要電子計算機の製品名	特定重要電子計算機の製造者名	備考
1	○○設備	②A ②E(イ)	xxxx-000	△△社	アプライアンス製品 5個
2	○○設備	②C	yyyy-111	□□工業	ソフトウェア バージョン：YYY
3	○○設備	②D	ZZZZ-222	□□工業	ソフトウェア バージョン：ZZZ
4	○○設備	③A	AAAA-333	××社	アプライアンス製品 2個

備考

担当：○○課　△△ 管理主体：株式会社○○システム（子会社）

また、添付資料の記載例は以下のとおりである。



3-1-6　経済安全保障推進法に基づく導入等届出を行っている場合の取扱い（主務省令第2条第4項）

経済安全保障推進法第 52 条第1項又は第 11 項の規定による当該特定重要設備の導入の届出を行っている場合には、以下の書類をもって、特定重要電子計算機のうち、特定重要設備又は構成設備であるものの届出書に代えることができる。

・導入等計画書（同条第1項に規定する導入等計画書（経済安全保障推進法の規定による変更をしたときは、その変更後のもの）をいう。）又は緊急導入等届出書（同条第 11 項に規定する緊急導入等届出書（経済安全保障推進法の規定による変更をしたときは、その変更後のもの）をいう。）

※当該特定重要設備又は当該構成設備の名称が当該特定重要電子計算機の製品名と同一であり、かつ、当該特定重要設備又は当該構成設備の供給者の名称が当該特定重要電子計算機の製造者名と同一である場合に限る。

・特別社会基盤事業者の連絡先を記載した書面

3-2　変更届出（法第4条第3項、主務省令第3条）

○法

（特定重要電子計算機の届出）

第四条　（略）

2　（略）

3　特別社会基盤事業者は、第一項の規定により届け出た事項に変更があったときは、主務省令で定めるところにより、その旨を特別社会基盤事業所管大臣に届け出なければならない。ただし、その変更が主務省令で定める軽微なものであるときは、この限りでない。

4　（略）

○主務省令

（変更の届出）

第三条　法第四条第三項の規定による変更の届出は、当該変更の日から四月以内に、様式第二による届出書を特別社会基盤事業所管大臣に提出して行うものとする。

2　前条第三項及び第四項の規定は、前項の変更の届出について準用する。この場合において、同条第三項中「当該特定重要電子計算機を導入した日」とあるのは、「当該変更の日」と読み替えるものとする。

（第2条第3項（読替後））

3　経済安全保障推進法第五十条第一項の特定重要設備を定める主務省令の改正により新たに特定重要電子計算機となった電子計算機であって、当該特定重要電子計算機となった日

から二月以内に導入したものに対する第一項の規定の適用については、同項中「当該変更の日から四月以内」とあるのは、「経済安全保障推進法第五十条第一項の特定重要設備を定める主務省令の改正により新たに特定重要電子計算機となった日から六月以内」とする。

（第2条第4項）

4　特定重要設備又は構成設備（経済安全保障推進法第五十二条第二項第二号ハの主務省令で定める設備、機器、装置又はプログラムをいう。以下この項及び次条第三項において同じ。）である特定重要電子計算機に係る第一項の届出書については、経済安全保障推進法第五十二条第一項又は第十一項の規定による当該特定重要設備の導入の届出を行っている場合（当該特定重要設備又は当該構成設備の名称が当該特定重要電子計算機の製品名（クラウド・コンピューティング・サービス（情報通信技術を活用した行政の推進等に関する法律（平成十四年法律第百五十一号）第二十三条第一項に規定するクラウド・コンピューティング・サービスをいう。以下この項において同じ。）の使用に係る特定重要電子計算機にあっては、当該クラウド・コンピューティング・サービスの名称。次項第四号及び次条第三項において同じ。）と同一であり、かつ、当該特定重要設備又は当該構成設備の供給者の名称又は氏名が当該特定重要電子計算機の製造者名（クラウド・コンピューティング・サービスの使用に係る特定重要電子計算機にあっては、当該クラウド・コンピューティング・サービスを提供する事業者名。次項第五号において同じ。）と同一である場合に限る。）には、当該届出に係る経済安全保障推進法第五十二条第一項に規定する導入等計画書（経済安全保障推進法の規定による変更をしたときは、その変更後のもの）又は同条第十一項に規定する緊急導入等届出書（経済安全保障推進法の規定による変更をしたときは、その変更後のもの）及び特別社会基盤事業者の連絡先を記載した書面の提出をもって、当該特定重要電子計算機に係る第一項の規定による届出書の提出に代えることができる。

（第3条第3項）

3　構成設備である特定重要電子計算機の製品名に係る第一項の届出書については、経済安全保障推進法第五十四条第四項（同条第五項において準用する場合を含む。）の規定による当該構成設備に関する事項の変更の内容の報告を行っている場合（当該構成設備の名称が当該特定重要電子計算機の製品名と同一である場合に限る。）には、当該報告をもって、当該届出書の提出に代えることができる。

（第3条第4項）

4　法第四条第三項ただし書の主務省令で定める軽微な変更は、前条第五項第一号に掲げる事項のうち、特別社会基盤事業者の名称の変更とする。

特別社会基盤事業者は、3-1 により届け出た情報に変更があったときは、特別社会基盤事業所管大臣に届け出なければならない。ただし、特別社会基盤事業者の名称の変更については、変更の届出は不要である（主務省令第3条第4項）。

変更届出が必要なのは、届け出た情報（製品名、製造者名等）に変更があった場合のほか、特定重要設備が撤去されない限りにおいては、当該特定重要設備に係る新たな特定重要電子計算機の導入についても変更届出の対象となる。

なお、新たに特定重要設備が導入された場合には、特定重要電子計算機の外延が新しく定まることから、当該導入に伴う特定重要電子計算機の届出については、第1項に基づく新規届出とする。

また、任意で届け出ることが望ましい事項に変更があった場合には、可能な限り変更届出をすること。（政府から古い情報に基づく脆弱性情報等が提供されることを回避するため）

3-2-1 届出期限（主務省令第3条第1項等）

届出期限は、3-1-2 と同様、原則変更の日から4月以内であるが、経済安全保障推進法第 50 条第1項の特定重要設備を定める主務省令の改正により新たに特定重要電子計算機となった電子計算機であって、当該特定重要電子計算機となった日から2月以内に導入したものについては、特定重要電子計算機となった日から6月以内に届け出ればよい。

変更の日から4月以内の届出の運用においては、例えば、四半期ごとに特定重要電子計算機の棚卸しを行い、1月でその結果をとりまとめて届け出るといったことも可能である。

なお、届出期限が行政機関の休日に当たるときは、行政機関の休日の翌日をもってその期限とみなす（行政機関の休日に関する法律第2条）。その他、期限の計算については、民法第1編第6章の例による。

3-2-2 届出方法

届出方法については、官民連携基盤を介した提出を想定しており、手続については、当該基盤に係るマニュアルを参照する。その他、資産届出情報を格納した DVD 等による届出などの手続きについては、所管省庁に確認を行う。

3-2-3 届出事項（主務省令様式第2）

以下に掲げる事項を所定の様式に記載の上、所管大臣宛に提出しなければならない。

(a)特別社会基盤事業者の概要

特別社会基盤事業者の名称及び連絡先を記載する。

(b)特定重要電子計算機の届出をした年月日その他の当該届出を特定するに足りる事項

3-1 の初回の届出をした年月日を記載する。

同日に複数の届出書を提出した場合（事業所ごとに提出した場合等）には、所管省庁に相談の上、どの届出書かが特定できる情報を記載する。

(c)変更事項

届出事項のうちどの事項を変更するかを記載する。

(d)変更の内容

変更の内容を新旧対照表形式で記載する。

なお、「別紙に記載」等と記載した上で、様式第1により作成した電子計算機のリスト（変更事項のない電子計算機を含んでいても差し支えない。）を添付する形で提出しても差し支えない。

また、(d)変更の内容を踏まえ、3-1-4 の添付資料に変更があれば更新して提出すること。

3-2-4 記載例（主務省令様式第2）

様式の記載例は以下のとおりである。なお、代表者の氏名は、旧姓でも差し支えない。連絡先については、本件における担当部局の連絡先を記載し、備考欄に「担当部局・担当者」を記載する。また、変更事由が発生した期間についても備考欄に記載する。

様式第二（第三条第一項関係）

特定重要電子計算機変更届出書

令和○年○月○日

○○大臣　　殿

住　　所　東京都○○
名　　称　株式会社○○
代表者の氏名　○○　○○

重要電子計算機に対する不正な行為による被害の防止に関する法律第4条第3項の規定により、次のとおり届け出ます。

1. 特別社会基盤事業者の概要

特別社会基盤事業者の名称	（フリガナ）　カブシキガイシャ　○○
	株式会社　○○
連絡先	電話番号　○○－○○○○－○○○○　E-mail　○○○○@○○.co.jp

2. 特定重要電子計算機の届出をした年月日その他の当該届出を特定するに足りる事項

令和○年○月○日

3. 変更事項

特定重要電子計算機に係る特定重要設備の区分並びに特定重要電子計算機の区分、製品名及び製造者名

4. 変更の内容

変更前

番号	特定重要設備の区分	特定重要電子計算機の区分	特定重要電子計算機の製品名	特定重要電子計算機の製造者名	備考
1	○○設備	②A ②E（イ）	xxxx-000	△△社	アプライアンス製品 ５個
2	○○設備	②C	yyyy-111	□□工業	ソフトウェア バージョン：YYY
49	○○設備	③A	zzzz-333	□□工業	ソフトウェア バージョン：ZZZZ

変更後

番号	特定重要設備の区分	特定重要電子計算機の区分	特定重要電子計算機の製品名	特定重要電子計算機の製造者名	備考
1	○○設備	②A ②E（イ）	xxxx-000	△△社	アプライアンス製品 ５個
2	○○設備	②C	yyyy-222	□□工業	ソフトウェア バージョン：YYY
49	○○設備	③A	zzzz-333	□□工業	ソフトウェア バージョン：ZZZZ
50	○○設備	③B	zzzz-334	□□工業	アプライアンス製品 ３個

備考

担当：○○課　○○
変更事由が発生した期間：令和○年○～○月

記載要領

届出書の用紙は、日本産業規格A列4番とし、該当欄に全部を記載することができない場合は、その欄に別紙に記載する旨を記載し、この様式に定める規格の用紙に適宜記載すること。

3-2-5　経済安全保障推進法に基づく導入等届出や変更の報告を行っている場合の取扱い（主務省令第3条第2項において準用する第2条第4項及び第3条第3項）

経済安全保障推進法第 52 条第1項又は第 11 項の規定による当該特定重要設備の導入の届出を行っている場合には、以下の書面をもって、特定重要電子計算機のうち、特定重要設備又は構成設備であるものの届出書に代えることができる。

・導入等計画書（同条第1項に規定する導入等計画書（経済安全保障推進法の規定による変更をしたときは、その変更後のもの）をいう。）又は緊急導入等届出書（同条第 11 項に規定する緊急導入等届出書（経済安全保障推進法の規定による変更をしたときは、その変更後のもの）をいう。）

※当該特定重要設備又は当該構成設備の名称が当該特定重要電子計算機の製品名と同一であり、かつ、当該特定重要設備又は当該構成設備の供給者の名称が当該特定重要電子計算機の製品名及び製造者名と同一である場合に限る。

・特別社会基盤事業者の連絡先を記載した書面

また、経済安全保障推進法第 54 条第4項（同条第5項において準用する場合を含む。）の規定による当該構成設備に関する事項の変更の内容の報告を行っている場合には、以下の書面をもって、特定重要電子計算機のうち、構成設備であるものの製品名の変更の届出書に代えることができる。

・当該報告に係る書面

※当該構成設備の名称が当該特定重要電子計算機の製品名と同一である場合に限る。

4. 補足事項　届出手順の一例

特定重要電子計算機の届出に当たっては、以下の5つのステップを通じて、届出対象となる特定重要電子計算機の特定、システム概略図と資産一覧の整備、及び政府への提出を行うことが望ましい。

本章では、届出の全体像を示し、4-1 から 4-5 までにおいて、ステップごとの詳細を記載する。

ステップ1．特定重要設備と関連システムの特定

- 特別社会基盤事業者が保有する情報（システム構成図、ネットワーク構成図、システム担当者知見等）より、特定重要設備、及び特定重要設備と直接的又は間接的につながる情報システムを特定する。

ステップ2．届出対象の特定

- ステップ1にて特定したシステムに対し、特別社会基盤事業者が保有する情報（機器構成図、機器管理リスト、システム担当者知見等）を 2.の特定重要電子計算機の範囲及び 3-1-1 の届出対象と照合し、資産届出対象を特定する。

ステップ3．届出用システム概略図の整理

- ステップ1及び2にて収集した情報を基に、届出用のシステム概略図を用意する。
  ※ システム構成の全体より特定重要設備の位置が分かる「全体版」、特定重要電子計算機になり得る機器が把握可能な「詳細版」を作成することが望ましい。なお、ステップ1及び2にて整理した資料でこれらを把握可能である場合は、既存資料でも差し支えない。

ステップ4．届出用資産一覧の整理

- ステップ1及び2にて収集した情報を基に、届出用の資産一覧を用意する。
  ※ 政府が定める様式での届出を求める。

ステップ5．資産届出の実施

- ステップ3及び4にて用意した届出資料を提出する。

次章より、各ステップについて解説する。

4-1　ステップ1　特定重要設備と関連システムの特定

特別社会基盤事業者が保有する情報（システム関連図、システム構成図、システム担当者知見等）より、特定重要設備、及び特定重要設備と直接的又は間接的につながる情報システムを特定する。

4-1-1 ステップ 1-1　対象範囲の理解

本制度では、その脆弱性が侵害された場合に、特定重要設備が影響を受ける可能性のある資産が届出対象となることから、特定重要設備と論理的に接続するシステムの範囲が対象範囲となることを理解する。

4-1-2 ステップ 1-2　関係者との事前調整

特定重要設備、及び関連システムの情報を収集する上で協力を得るべき関係者を整理し、本制度に対する理解を得ることが望ましい。

対象範囲の特定、及び後続における資産届出対象の特定を行うには、特定重要設備のシステム管理者だけではなく、関連システムの管理者、又は関連システムの構成や設置場所によってはグループ会社や業務委託先等の他会社の協力が必要となる場合があるため、関係者を明確に特定し、後続作業の進め方や各資料の作成イメージ等を共有しておくことが望ましい。

4-1-3 ステップ 1-3　対象範囲の特定

対象範囲における特定重要設備、及び関連システムのネットワーク構成に関する情報（システム構成図、ネットワーク構成図、システム担当者知見等）を、関係者と協力して収集する。本章の段階で収集する情報は、システムの全体像、及び資産届出対象範囲となる、特定重要設備と関連システムにおける論理的接続の関係性が特定できる程度で十分である。

4-2　ステップ2　届出対象の特定

特別社会基盤事業者が保有する情報（機器構成図、機器管理リスト、システム担当者知見等）と2.の特定重要電子計算機の範囲及び 3-1-1 の届出対象とを照合し、届出対象を特定する。

4-3　ステップ3　届出用システム概略図の整理

これまでに整理した情報を基にシステム概略図を用意することが望ましい。システム概略図は、届出を実施する特別社会基盤事業者が、自組織の特定重要設備と関係のあるネットワークの全体像を理解し、特定重要設備に関するリスクを把握するためにも重要である。

システム概略図は以下の二つを作成することが望ましい。なお、ステップ1及び2にて整理した資料でこれらを把握可能である場合は、既存資料をもって代えてもよい。

① 全体版：届出対象範囲のシステム、及びそのシステム間の接続を整理した図

② 詳細版：届出対象資産が存在するシステム内の資産構成（主要な機器とその通信経路）を整理した図

4-3-1 ステップ 3-1 システム概略図（全体版）の作成

システム概略図（全体版）を作成する。システム概略図（全体版）には、表5に記載した情報を記載することが望ましい。

図3 システム概略図（全体版）サンプル

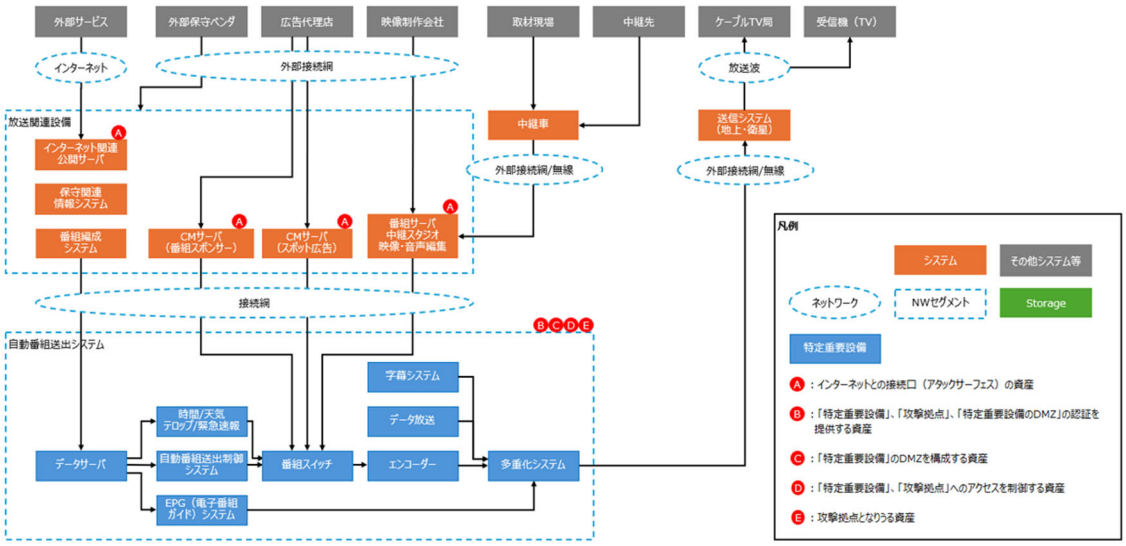


表5 全体版に記載することが望ましい情報

	項目	説明
1	システム名又は領域名（可能な限り一意な名称）	対象範囲のシステムのこと。 ※特定重要設備が存在する位置が分かるようにする。
2	通信路（ネットワーク）	各システム間の接続経路のこと。
3	該当カテゴリー	特定重要電子計算機のカテゴリー[A]から[F]までの条件に合致し、届出対象となった資産を保有するシステムが分かるように記載する。
4	回線種別（外部回線）（例：インターネット、専用線等）	専用線や閉域網で接続されている場合はそれを記載する。また、インターネットとの接続場所が分かるようにする。

4-3-2 ステップ 3-2 システム概略図（詳細版）の作成

届出対象となった資産が存在するシステム（又は規模が大きくなる場合は、システムをセグメント単位で区分し、届出対象となった資産が存在するセグメントでもよい。）については、更に詳細な構成が分かるシステム概略図（詳細版）を作成することが望ましい。

届出対象と特定された資産を有するシステム内の構成要素を整理し、同様の役割や機能を持つ資産をまとめることで、主要構成要素が把握できるように記載する。また、それらの資産間の接続関係も明確に記載する。

なお、システム概略図作成に当たっては特別社会基盤事業者のシステムの構成を踏まえて作成することが重要となる。特別社会基盤事業者のシステムの構成の典型的なパターンを、参考として掲載する。

図4 オンプレミスにある情報系と制御系のシステムが DMZ を介して接続するパターン

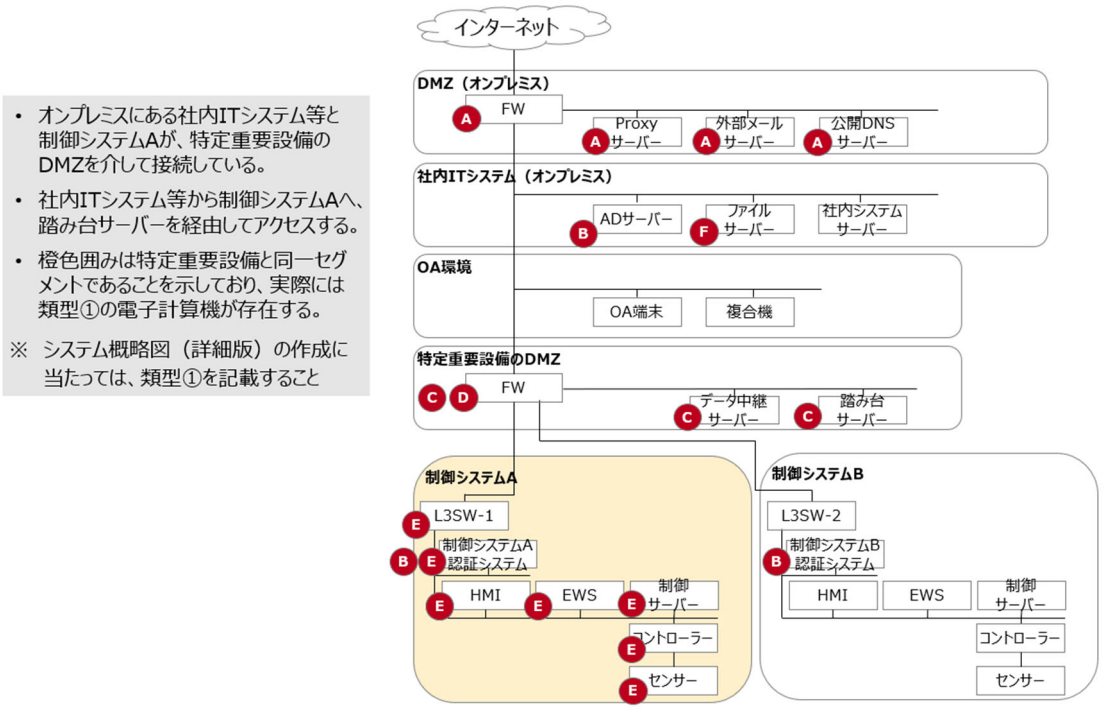


図5　クラウド環境を含む情報系と制御系システムが DMZ を介して接続するパターン

- オンプレミスにある社内ITシステム等と制御システムAが、特定重要設備のDMZを介して接続している。
- 社内ITシステム等はクラウド上にも存在する。
- クラウドとルーターは専用線（又は閉域網経由）で接続している。
- 橙色囲みは特定重要設備と同一セグメントであることを示しており、実際には類型①の電子計算機が存在する。

※　システム概略図（詳細版）の作成に当たっては、類型①を記載すること

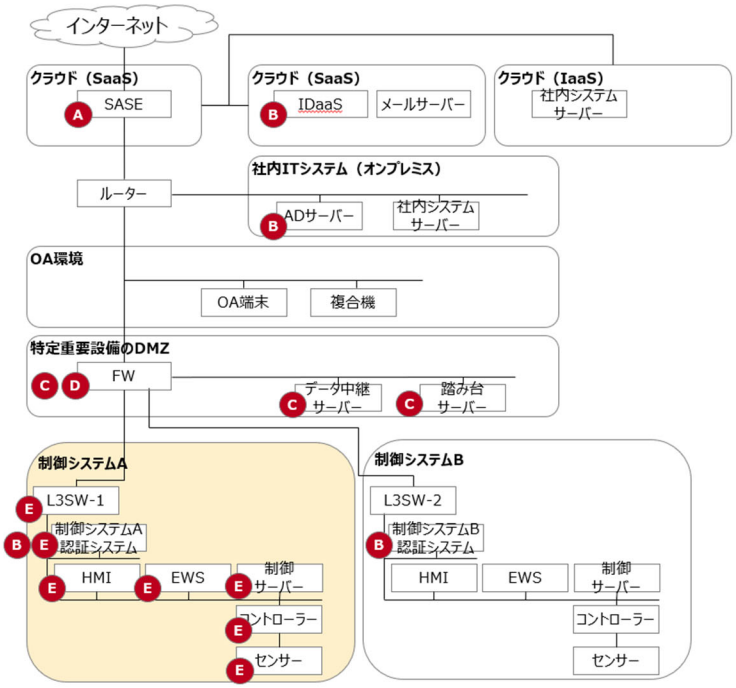


図6　情報系と制御系のシステムが物理的に分離しており、媒体でデータを移送するパターン

- 社内ITシステム等と制御システムAが接続していない。（エアギャップが存在している。）
- 社内ITシステム等と制御システムAとの間でデータ移送には、USBメモリ等の媒体を用いる。
- クラウドとルーターは専用線（又は閉域網経由）で接続している。
- 橙色囲みは特定重要設備と同一セグメントであることを示しており、実際には類型①の電子計算機が存在する。

※　システム概略図（詳細版）の作成に当たっては、類型①を記載すること

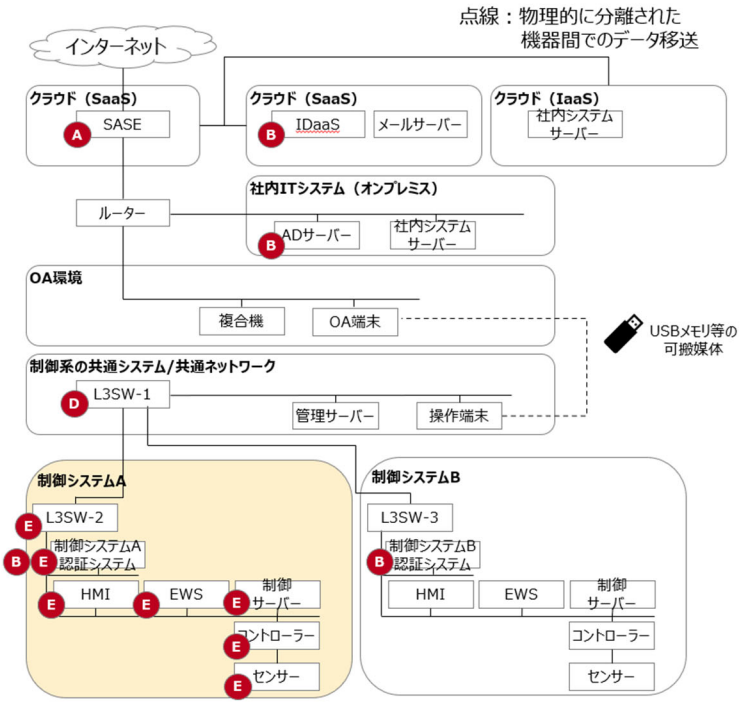


図7　情報系と制御系のシステムの通信が一方向に限定されているパターン

- 社内ITシステム等と制御システムAが接続しているものの、データダイオードで物理的に通信を一方向に制限している。
  （制御システムAから社内ITシステム等への一方向での通信のみを許可している。）
- クラウドとルーターは専用線（又は閉域網経由）で接続している。
- 橙色囲みは特定重要設備と同一セグメントであることを示しており、実際には類型①の電子計算機が存在する。

※　システム概略図（詳細版）の作成に当たっては、類型①を記載すること

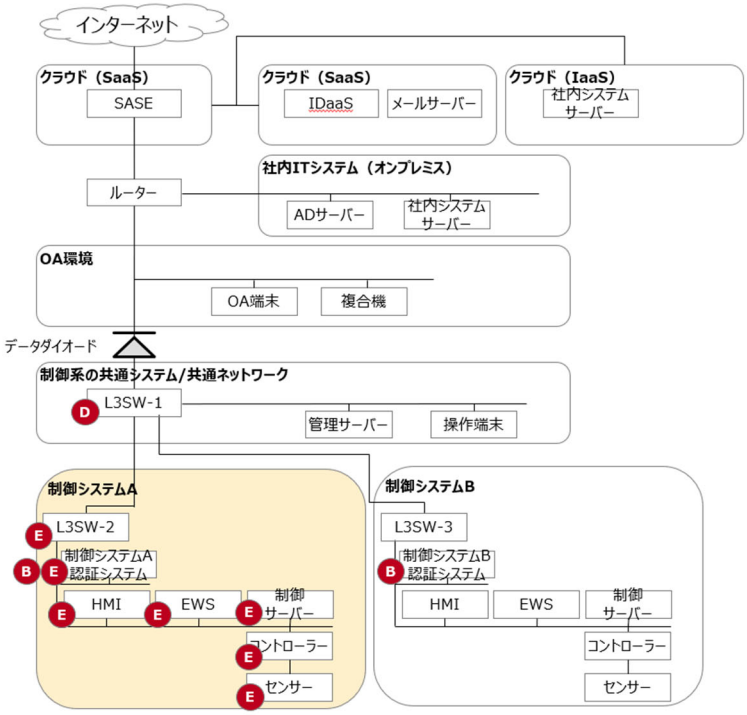


図8　制御系システムに常時リモートアクセスがあるパターン

- リモートオペレーションセンターから制御システムAへ、閉域網（IP-VPN等）経由でリモートアクセスをする。
- クラウドとルーターは専用線（又は閉域網経由）で接続している。
- 橙色囲みは特定重要設備と同一セグメントであることを示しており、実際には類型①の電子計算機が存在する。

※　システム概略図（詳細版）の作成に当たっては、類型①を記載すること

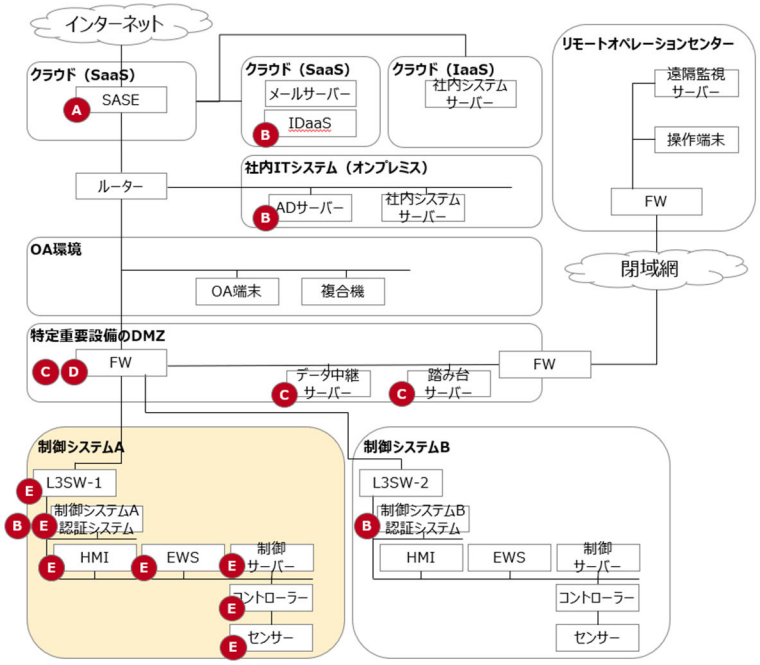


図9　制御系システムに一時的なリモートアクセスがあるパターン

- ベンダー拠点Aから制御システムAへ、インターネットVPN経由でリモートアクセスをする。
- ベンダー拠点Bから制御システムAへ、特定重要設備のDMZを経由せずにアクセスすることがある。
- クラウドとルーターは専用線（又は閉域網経由）で接続している。
- 橙色囲みは特定重要設備と同一セグメントであることを示しており、実際には類型①の電子計算機が存在する。

※　システム概略図（詳細版）の作成に当たっては、類型①を記載すること

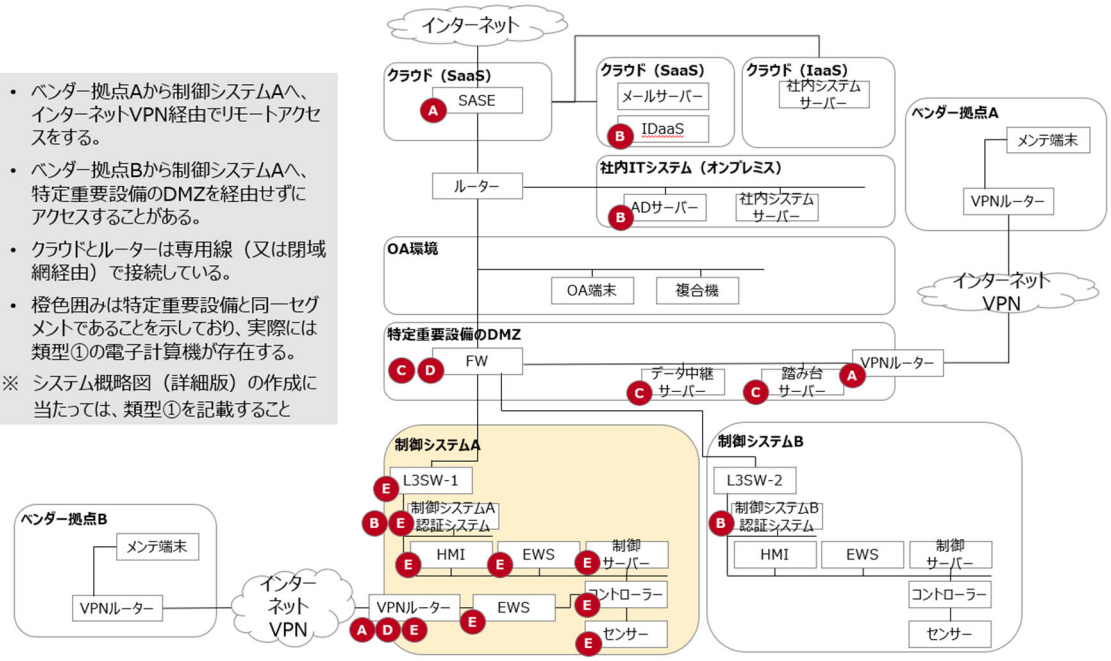


図 10　制御系システムから、情報系システム経由でクラウド上へデータ連携するパターン

- 社内システムサーバーとデータ分析基盤は、異なるIaaS環境上にある。
- 制御システムAからクラウド上にあるデータ分析基盤へ、特定重要設備のDMZを介してデータが送られている。
- クラウドとルーターは専用線（又は閉域網経由）で接続している。
- 橙色囲みは特定重要設備と同一セグメントであることを示しており、実際には類型①の電子計算機が存在する。

※　システム概略図（詳細版）の作成に当たっては、類型①を記載すること

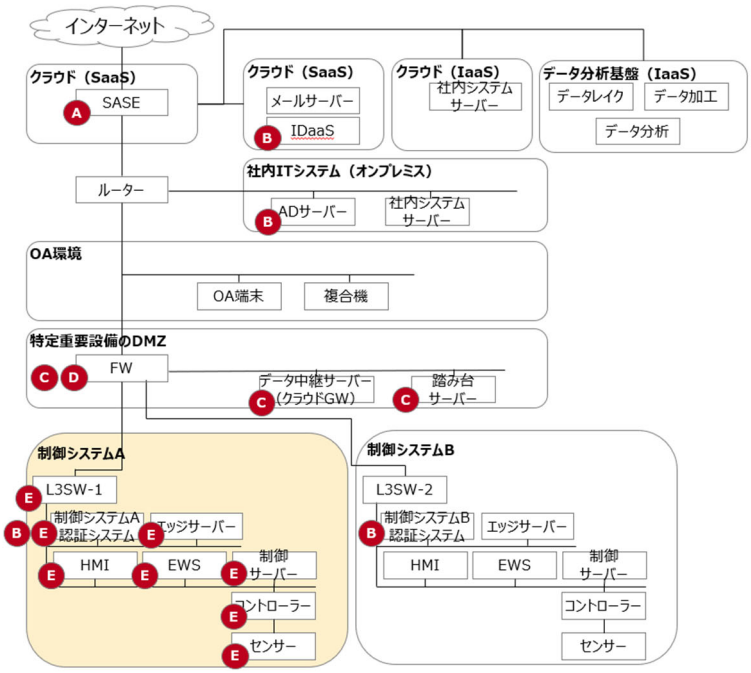
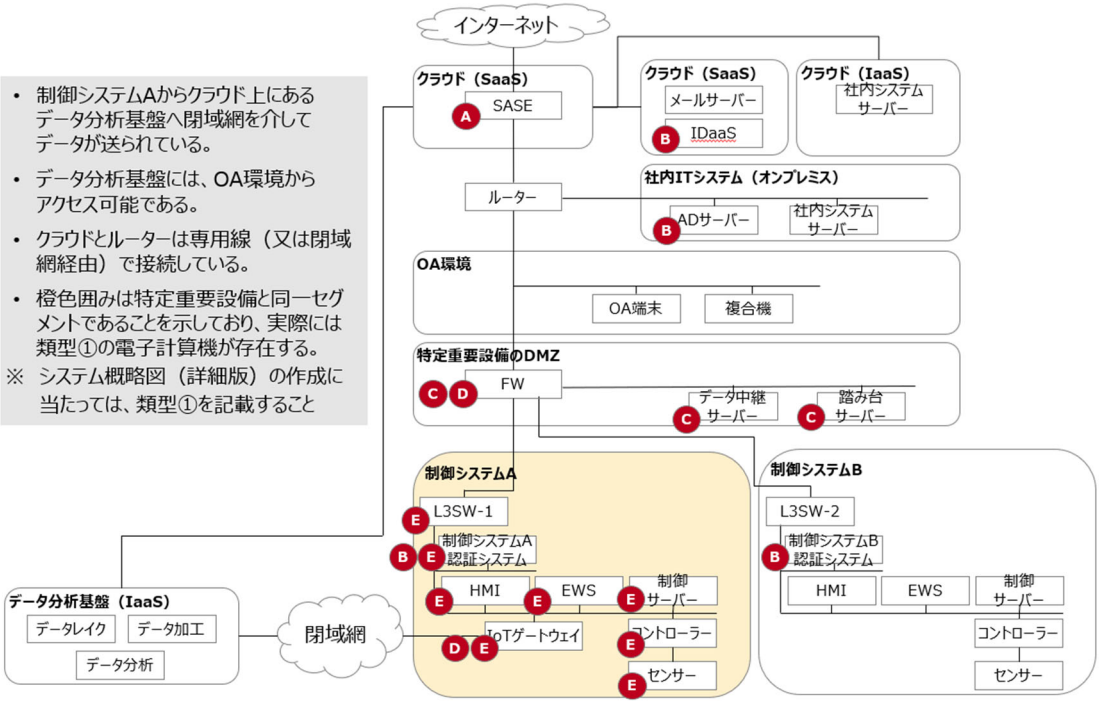


図 11　制御系システムから、情報系システムを経由せずクラウド上へデータ連携するパターン



4-4 ステップ4 届出用資産一覧の整理

4-4-1 ステップ 4-1 電子計算機の一覧化

ステップ3で作成した届出用システム概略図を確認し、届出対象となる電子計算機を一覧化する。

4-4-2 ステップ 4-2 届出を求める電子計算機の抽出

ステップ 4-1 にて作成した電子計算機の一覧から、届出が免除される資産を除外し、届出対象に該当する電子計算機を抽出する。

4-4-3 ステップ 4-3 届出資産一覧の作成

ステップ 4-2 にて抽出した電子計算機について、資産届出に必要な情報を収集し、届出資産一覧を作成する。資産届出に必要な情報は、3-1-4 を参照すること。

4-5 ステップ5 資産届出の実施

ステップ4で整理した資産の届出情報と、ステップ3で作成したシステム概略図の届出を行う。

5. 特定侵害事象等の範囲等

法第5条の報告対象となる事象は、特定重要電子計算機に対する特定侵害事象又は当該特定侵害事象の原因となり得る事象として主務省令で定めるもののいずれかである。以下、5-1 において特定侵害事象、5-2 において特定侵害事象の原因となり得る事象の範囲を示す。

5-1 特定侵害事象（法第2条第4項、第5項）

○法
（定義）
第二条 （略）
2・3 （略）
4 この法律において「特定不正行為」とは、次の各号のいずれかに該当する行為をいう。
一 刑法（明治四十年法律第四十五号）第百六十八条の二第二項の罪に当たる行為
二 不正アクセス行為（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第二条第四項に規定する不正アクセス行為をいう。第八十条第一項において同じ。）
三 電子計算機を用いて行われる業務に係る刑法第二編第三十五章の罪に当たる行為であって、当該電子計算機のサイバーセキュリティを害することによって行われるもの（当該電子計算機に接続された電気通信回線の機能に障害を与えることによって行われるものを含む。）
5 この法律において「特定侵害事象」とは、重要電子計算機に対する特定不正行為により、当該重要電子計算機のサイバーセキュリティが害されることをいう。
6～9 （略）

「特定侵害事象」とは、重要電子計算機に対する特定不正行為により、当該重要電子計算機のサイバーセキュリティが害されることをいう。具体的には、以下の事象を指す。

5-1-1 マルウェアの供用（法第2条第4項第1号、第5項）

特定重要電子計算機に対する刑法（明治 40 年法律第 45 号）第 168 条の2第2項の罪に当たる行為により、重要電子計算機のサイバーセキュリティが害される事象をいう。

刑法第 168 条の2第2項の罪に当たる行為とは、正当な理由がないのに、人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録を人の電子計算機における実行の用に供する行為である。

具体的には、被害者が意図せずマルウェアをダウンロードし、そのマルウェアが実行され得る状態に置かれることが該当する。アンチウィルス製品等のリアルタイムスキャンにより即時削除された場合やマルウェアの実行ファイルを添付したメールがその者のメールボックスに記録されるに止まった場合は該当しない。

以下のような事例が該当する。

- 例 1)マルウェア等の実行ファイルを Web サイト上でダウンロード可能な状態に置き、事情を知らない被害者に Web サイトの閲覧時に当該ファイルをダウンロードさせ、被害者の電子計算機上で実行可能な状態に置く場合
- 例 2)マルウェア等の実行ファイルを添付した電子メールを送信し、当該ファイルについて事情を知らず、かつ、実行する意思のない受信者の電子計算機上で、当該ファイルを実行可能な状態に置く場合

○刑法 （不正指令電磁的記録作成等） 第百六十八条の二 （略） 一 人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録 二 （略） 2 正当な理由がないのに、前項第一号に掲げる電磁的記録を人の電子計算機における実行の用に供した者も、同項と同様とする。 3 （略）

5-1-2 不正アクセス（法第2条第4項第2号、第5項）

特定重要電子計算機に対する不正アクセス行為により、当該特定重要電子計算機のサイバーセキュリティが害される事象をいう。

不正アクセス行為とは、不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）第2条第4項に規定する行為であり、具体的には以下の3類型がある。

①アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為

※ 当該アクセス制御機能を付加したアクセス管理者がするもの、当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするもの及び国立研究開発法人情報通信研究機構法（平成 11 年法律第 162 号）第 18 条第6項第1号に規定する認可特定アクセス行為等実施計画に基づき同条第1項第1号に掲げる業務に従事する者がする同条第7項第1号に規定する特定アクセス行為を除く。

②アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為

※ 当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。

③電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為

※ 当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。

※ アクセス管理者：電気通信回線に接続している電子計算機（以下「特定電子計算機」という。）の利用（当該電気通信回線を通じて行うものに限る。以下「特定利用」という。）につき当該特定電子計算機の動作を管理する者。

※ 識別符号：特定電子計算機の特定利用をすることについて当該特定利用に係るアクセス管理者の許諾を得た者及び当該アクセス管理者（以下「利用権者等」という。）に、当該アクセス管理者において当該利用権者等を他の利用権者等と区別して識別することができるように付される符号であって、次のいずれかに該当するもの又は次のいずれかに該当する符号とその他の符号を組み合わせたもの。

一　当該アクセス管理者によってその内容をみだりに第三者に知らせてはならないものとされている符号

二　当該利用権者等の身体の全部若しくは一部の影像又は音声を用いて当該アクセス管理者が定める方法により作成される符号

三　当該利用権者等の署名を用いて当該アクセス管理者が定める方法により作成される符号

※ アクセス制御機能：特定電子計算機の特定利用を自動的に制御するために当該特定利用に係るアクセス管理者によって当該特定電子計算機又は当該特定電子計算機に電気通信回線を介して接続された他の特定電子計算機に付加されている機能であって、当該特定利用をしようとする者により当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号（識別符号を用いて当該アクセス管理者の定める方法により作成される符号と当該識別符号の一部を組み合わせた符号を含む。）であることを確認して、当該特定利用の制限の全部又は一部を解除するもの。

具体的には、識別符号を用いた認証システムによるアクセス制御（いわゆるユーザー認証等）を何らかの方法によって回避して行われる行為が該当する。

- 例 1）VPN の認証情報をダークウェブ等から取得し、VPN 機器にアクセスする場合
- 例 2）無効化が漏れていた退職者アカウントの ID/パスワードを悪用し、システムにアクセスする場合
- 例 3）アクセス制御機能を持つ機器の脆弱性に対してその脆弱性を悪用する情報又は指令を入力し、認証を回避して当該機器へアクセスする場合、又は同行為によりアクセス制御機能によって保護されたデータを不正取得する場合

- 例 4)正常な接続時の URL 等のクエリ末尾に不正な SQL 文等を付加することで、アクセス先機器に本来公開されていないデータを応答させ、データを不正取得する場合

○不正アクセス行為の禁止等に関する法律

（定義）

第二条　この法律において「アクセス管理者」とは、電気通信回線に接続している電子計算機（以下「特定電子計算機」という。）の利用（当該電気通信回線を通じて行うものに限る。以下「特定利用」という。）につき当該特定電子計算機の動作を管理する者をいう。

2　この法律において「識別符号」とは、特定電子計算機の特定利用をすることについて当該特定利用に係るアクセス管理者の許諾を得た者（以下「利用権者」という。）及び当該アクセス管理者（以下この項において「利用権者等」という。）に、当該アクセス管理者において当該利用権者等を他の利用権者等と区別して識別することができるように付される符号であって、次のいずれかに該当するもの又は次のいずれかに該当する符号とその他の符号を組み合わせたものをいう。

一　当該アクセス管理者によってその内容をみだりに第三者に知らせてはならないものとされている符号

二　当該利用権者等の身体の全部若しくは一部の影像又は音声を用いて当該アクセス管理者が定める方法により作成される符号

三　当該利用権者等の署名を用いて当該アクセス管理者が定める方法により作成される符号

3　この法律において「アクセス制御機能」とは、特定電子計算機の特定利用を自動的に制御するために当該特定利用に係るアクセス管理者によって当該特定電子計算機又は当該特定電子計算機に電気通信回線を介して接続された他の特定電子計算機に付加されている機能であって、当該特定利用をしようとする者により当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号（識別符号を用いて当該アクセス管理者の定める方法により作成される符号と当該識別符号の一部を組み合わせた符号を含む。次項第一号及び第二号において同じ。）であることを確認して、当該特定利用の制限の全部又は一部を解除するものをいう。

4　この法律において「不正アクセス行為」とは、次の各号のいずれかに該当する行為をいう。

一　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）

二　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る

状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。）

三　電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為

5-1-3　業務妨害等（法第2条第4項第3号、第5項）

特定重要電子計算機を用いて行われる業務に係る刑法第2編第 35 章の罪に当たる行為であって、当該特定重要電子計算機のサイバーセキュリティを害することによって行われるもの（当該特定重要電子計算機に接続された電気通信回線の機能に障害を与えることによって行われるものを含む。）により、当該特定重要電子計算機のサイバーセキュリティが害されることをいう。

刑法第2編第 35 章の罪に当たる行為とは、以下の①②などである。

①不正な手段を用いて人の業務を妨害する行為（偽計業務妨害又は威力業務妨害）

②人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し、若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害する行為（電子計算機損壊等業務妨害）

いわゆる DDoS 攻撃による機器や回線の機能停止や機能低下を一時的にもたらす行為や、システム内のファイルを暗号化や削除する行為等、機器を用いた業務を妨害する行為が該当する。

- 例1）サーバーの処理速度を遅くし、ウェブサイトの機能を低下させるに足りる程度に、サーバーの設置者が想定する処理能力を超えるデータを送り付けるような場合（DDoS 攻撃）
- 例2）サーバーや端末にランサムウェアやワイパー型マルウェアを感染させ、それらの機器内のファイル等を暗号化・消去等をするような場合（ランサムウェア攻撃、ワイパー攻撃）

※例2)は、5-1-1 に該当する場合もある。

なお、②には未遂の罪に当たる行為（電子計算機の動作が阻害されていない場合等）も含まれるが、主務省令第4条第2項第3号において、特定重要電子計算機（①特定重要設備及び②[E]特定重要設備と同一セグメントの機器を除く。）に対する②の未遂の罪のみに当たる行為については、6-1 に記載のとおり、報告対象外としている。

○刑法

第三十五章　信用及び業務に対する罪

（信用毀損及び業務妨害）

第二百三十三条　虚偽の風説を流布し、又は偽計を用いて、人の信用を毀損し、又はその業務を妨害した者は、三年以下の拘禁刑又は五十万円以下の罰金に処する。

（威力業務妨害）

第二百三十四条　威力を用いて人の業務を妨害した者も、前条の例による。

（電子計算機損壊等業務妨害）

第二百三十四条の二　人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し、若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害した者は、五年以下の拘禁刑又は百万円以下の罰金に処する。

2　前項の罪の未遂は、罰する。

5-2　特定侵害事象の原因となり得る事象（法第5条）

特定侵害事象の原因となり得る事象とは、5-1 に挙げた特定侵害事象には至らないものの、そのおそれとなる事象を指している。主務省令においては、特定重要設備等に該当する特定重要電子計算機とそれ以外の特定重要電子計算機とで報告対象とする事象を分けている。前者においては、他のカテゴリーと異なり、サイバー攻撃の成否を問わず、攻撃の試行を認知した場合も報告対象としている。なお、特定重要設備等は、一号電子計算機（類型①）並びに第一条第一項第一号（類型②E（イ））及び第二号（類型②E（ロ））のことである。

○法

（特定侵害事象等の報告）

第五条　特別社会基盤事業者は、特定重要電子計算機に係る特定侵害事象又は当該特定侵害事象の原因となり得る事象として主務省令で定めるものの発生を認知したときは、主務省令で定めるところにより、その旨及び主務省令で定める事項を特別社会基盤事業所管大臣及び内閣総理大臣に報告しなければならない。

○主務省令

（特定侵害事象等の報告）

第四条　法第五条の主務省令で定める事象は、次の各号に掲げる特定重要電子計算機の区分に応じ、当該各号に定める事象とする。

一　一号電子計算機並びに第一条第一項第一号及び第二号に規定する特定重要電子計算機　次に掲げる事象

イ　正当な理由がないのに、特定重要電子計算機に対し、特別社会基盤事業者が当該特定重要電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録を受信させる行為が行われる事象

ロ　アクセス制御機能を有する特定重要電子計算機に対し、電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号が入力される事象（当該アクセス制御機能を付加したアクセス管理者（不正アクセス禁止法第二条第一項に規定するアクセス管理者をいう。以下このロ及びハにおいて同じ。）によりされるもの、当該アクセス管理者又は当該識別符号に係る同条第二項に規定する利用権者の承諾を得てされるもの及び国立研究開発法人情報通信研究機構法（平成十一年法律第百六十二号）第十八条第六項第一号に規定する認可特定アクセス行為等実施計画に基づき同条第一項第一号に掲げる業務に従事する者がする同条第七項第一号に規定する特定アクセス行為を除く。）

ハ　アクセス制御機能を有する特定重要電子計算機に対し、電気通信回線を通じて当該アクセス制御機能による特定利用（不正アクセス禁止法第二条第一項に規定する特定利用をいう。ニにおいて同じ。）の制限を免れることができる情報（識別符号であるものを除く。）又は指令が入力される事象（当該アクセス制御機能を付加したアクセス管理者によりされるもの及び当該アクセス管理者の承諾を得てされるものを除く。ニにおいて同じ。）

ニ　電気通信回線で直接又は間接に接続されている他の特定重要電子計算機が有するアクセス制御機能によりその特定利用を制限されている電子計算機に対し、電気通信回線を通じてその制限を免れることができる情報又は指令が入力される事象

ホ　不正アクセス禁止法第二条第四項第一号に該当する行為の用に供する目的で、特定重要電子計算機のアクセス制御機能に係る他人の識別符号が取得される事象（当該特定重要電子計算機のサイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。次項第三号において同じ。）を害することによって行われるものに限る。）

ヘ　特定侵害事象又はイからホまでに掲げる事象の痕跡が記録される事象

二　前号に掲げる特定重要電子計算機以外の特定重要電子計算機　特定侵害事象の痕跡が記録される事象

2・3　（略）

5-2-1　特定重要設備等における特定侵害事象の原因となり得る事象（法第5条、主務省令第4条第1項第1号）

[イ]特定重要電子計算機に対し、特別社会基盤事業者が当該特定重要電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録が受信される事象

5-1-1 の原因となり得る事象であり、具体的には、マルウェアのダウンロードや不正コード実行が該当する。（アンチウィルス製品等のリアルタイムスキャンによる即時削除やコード実行停止がされた場合も含む。）

[ロ]アクセス制御機能を有する特定重要電子計算機に対し、電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号が入力される事象

※　当該アクセス制御機能を付加したアクセス管理者によりされるもの、当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てされるもの及び認可特定アクセス行為等実施計画に基づく特定アクセス行為を除く。

[ハ]アクセス制御機能を有する特定重要電子計算機に対し、電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令が入力される事象

※　当該アクセス制御機能を付加したアクセス管理者によりされるもの及び当該アクセス管理者の承諾を得てされるものを除く。

[ニ]電気通信回線で直接又は間接に接続されている他の特定重要電子計算機が有するアクセス制御機能によりその特定利用を制限されている電子計算機に対し、電気通信回線を通じてその制限を免れることができる情報又は指令が入力される事象

※　当該アクセス制御機能を付加したアクセス管理者によりされるもの及び当該アクセス管理者の承諾を得てされるものを除く。

※　[ロ]から[ニ]までについては、5-1-2 の原因となり得る事象であり、具体的には、無効化されていない退職者のユーザーアカウントが入力される事象や、SQL インジェクション等の脆弱性を悪用してアクセス制御機能を無効化しようとする情報又は指令が入力される事象が該当する。行為が失敗し認証が突破されなかった場合も含む。

[ホ]不正アクセス禁止法第二条第四項第一号に該当する行為の用に供する目的で、特定重要電子計算機のアクセス制御機能に係る他人の識別符号が取得される事象

※　当該特定重要電子計算機のサイバーセキュリティを害することによって行われるものに限る。

※　[ロ]から[ニ]までと同じく5-1-2 の原因となり得る事象であり、具体的には、特定重要設備等の認証情報がサイバー攻撃者に窃取された場合が該当する。

[へ]特定侵害事象又はイからホまでに掲げる事象の痕跡が記録される事象

特定重要設備等において、5-1 の特定侵害事象が発生したこと又は 上記[イ]から[ホ]までの事象が発生したことが、セキュリティ監視のアラートやフォレンジック調査等から蓋然性が高いことを指す。

5-2-2 特定重要設備等以外における特定侵害事象の原因となり得る事象（法第5条、主務省令第4条第1項第2号）

5-1 の特定侵害事象が発生したことが、セキュリティ監視のアラートやフォレンジック調査、脅威ハンティング等から蓋然性が高いことを指す。

なお、本項では 5-2-1[イ]から[ホ]までに掲げる事象の痕跡が記録される事象が発生した際の報告義務はないが、5-2-1 と同様に報告することが望ましい。

5-3 一般的なサイバー攻撃の類型との関係

特定侵害事象等の範囲は以上に記載したとおりであるが、これらは一般的なサイバー攻撃の類型で分類すると、①DDoS 攻撃事案、②ランサムウェア事案、③その他サイバー攻撃事案（不正アクセス又はマルウェア感染等）の 3 種類のいずれかの攻撃過程や最終被害において発生する事象である。特定侵害事象等と 5-1 及び 5-2 のサイバー攻撃の類型との対応関係は、以下のとおりである。特定侵害事象等の報告様式は①から③までに対応する3種類があるところ、いずれの様式を用いるかについては以下を参照し、適切な様式を用いて報告を行うこと。

表6 特定侵害事象等と一般的なサイバー攻撃の類型との対応関係

法令において指定している事象			① DDoS 攻撃	②ランサムウェア攻撃	③その他サイバー攻撃
特定侵害事象		5-1-1	×	○	○
		5-1-2	×	○	○
		5-1-3	○	○	○
特定侵害事象の原因となり得る事象	特定重要設備等関係（5-2-1）	[イ]	×	○	○
		[ロ]	×	○	○
		[ハ]	×	○	○
		[ニ]	×	○	○
		[ホ]	×	○	○
		[へ]	○	○	○
	特定重要設備等以外関係（5-2-2）		×	○	○

5-3-1 DDoS 攻撃事案

多数の機器から攻撃目標の機器やネットワークに一斉の大量通信を行い、攻撃対象が利用できない状況に陥らせた事案を指す。特に、複数の通信元から分散して大量通信が行われる場合は DDoS（Distributed Denial of Service）攻撃と呼ばれる。DDoS 攻撃に該当するのは、以下のいずれかの場合である。

i. DDoS 攻撃（又は DoS 攻撃）により機能停止又は機能低下が発生した。

ii. 機能停止又は機能低下には至らなかったが、そのおそれがある DDoS 攻撃（又は DoS 攻撃）が発生した。

i.は 5-1-3 に、ⅱ.は 5-2-1[へ] 又は 5-2-2 に該当する。

なお、ⅱは電子計算機の動作が阻害されていないため（未遂）、特定重要設備等に該当する特定重要電子計算機以外の特定重要電子計算機で発生した事象である場合は、6-1 に記載のとおり報告の必要はない。

5-3-2 ランサムウェア事案

機器内のファイル暗号化による可用性の阻害が行われた事案を指す。具体的には、マルウェアの機能によってシステム内のファイルを暗号化し業務を妨害した上で、暗号化したファイルの復号を対価として身代金（Ransom）を要求する場合がこれに当たる。

ランサムウェア攻撃は、攻撃過程においてマルウェアの供用、ファイル暗号化等による業務妨害、ランサムノート等による身代金脅迫といった行為が行われうるため、5-1 及び 5-2 の特定侵害事象等のいずれにも該当し得る。

5-3-3 その他サイバー攻撃事案（不正アクセス、情報窃取等）

DDoS 攻撃やランサムウェア攻撃以外にも、特定重要設備を構成するシステムの破壊や重要データの窃取、継続的な情報窃取や将来的な破壊活動を目的としたネットワーク内部への長期潜伏といった侵害も報告対象となる。その他サイバー攻撃に該当するのは、以下のいずれかの場合である。

i. マルウェアの供用等により、機密情報が攻撃者から閲覧可能な状態となった。又は外部持ち出しされた。

ii. 長期潜伏を目的とした不正アクセスの永続化（事業者が機器の再起動・認証情報の変更等を行った場合でも攻撃者が不正アクセスを継続できる状態）が行われた。

iii. 上記 i.、ii.の事象までには至らないものの、マルウェアの供用・不正アクセス・その他サイバー攻撃等の特定侵害事象のおそれとなり得る事象が発生した。

その他のサイバー攻撃事案は、攻撃過程においてマルウェアの供用、不正アクセス等の行為が行われ得るため、5-1 及び 5-2 の特定侵害事象等のいずれにも該当し得る。

5-4 特定侵害事象等に該当しない事象

法第5条では、特定重要電子計算機の侵害を対象としているため、特定重要電子計算機に該当しない機器の侵害のみであれば、報告義務は発生しない。ただし、特定重要電子計算機に該当しない機器を経由して特定重要電子計算機が侵害された場合等、侵害された範囲に特定重要電子計算機が含まれている場合は、当該特定重要電子計算機への侵害については、報告の対象となる。

上記の報告基準には該当しないものの、脆弱性情報等の被害の防止のために効果的な情報を提供することその他政府による必要な対応を実施する観点から、以下のような事象があった場合については任意による報告を行うことを推奨する。

- 特定重要電子計算機には該当しないものの自組織にとって特定重要設備に準じる重要な設備又は特定重要電子計算機に準じる重要な電子計算機において発生した場合
- 特定侵害事象等に該当しないものの自組織を対象とした標的型攻撃の痕跡を発見した場合

5-5 特定侵害事象等の発生の認知

法第5条では、特定侵害事象又は当該特定侵害事象の原因となり得る事象の発生を認知した時に報告を求めている。

発生の認知とは、監視におけるイベントやアラートの発報のみをもって直ちに該当するものではないが、当該イベントやアラートの内容等を踏まえ、法第5条における特定侵害事象等に該当すると合理的に判断できる状態を指す。また、一般的にイベントやアラートの発報から特定侵害事象等の該当性判断は速やかに行われることが望ましい。

6-2 で説明する報告期限の起算は、サイバーインシデント発生を認知した日から行う。

なお、サイバーインシデントの発生の主な認知方法の例としては、以下が挙げられる。

A) 特定重要電子計算機の死活監視等で機能停止又は機能低下が確認され、その原因がサイバー攻撃によるものと判明した。

B) SOC（Security Operation Center）等がセキュリティイベント等を検知し、そのイベントが法第5条のインシデント基準を満たす事象と判定された。

C) フォレンジック調査、脅威ハンティング等の活動により、サイバー攻撃を受けていた痕跡が確認され、その痕跡から想定される発生事象が特定侵害事象等と判定された。

D) 特定重要電子計算機に該当するクラウドサービス等について、クラウドサービス事業者等からインシデント通知があり、そのインシデントが特定侵害事象等と判定された。

上記の事象を最初に認知するのは自社外組織（クラウドサービス事業者、回線事業者、システム運用や監視等を担当する委託先事業者 等）となる場合もあり、特別社会基盤事業者が速やかにインシデント発生を認知する体制整備が不可欠となる。そのため、体制上、インシデント発生を初期に認知することになる自社外組織から、どのような場面でどのようなインシデント通知が為されるかを確認することが望ましい（例：SLA 定義書、クラウドサービス利用規約、システム共同利用契約書 等）。

6.　報告手続

○法

（特定侵害事象等の報告）

第五条　特別社会基盤事業者は、特定重要電子計算機に係る特定侵害事象又は当該特定侵害事象の原因となり得る事象として主務省令で定めるものの発生を認知したときは、主務省令で定めるところにより、その旨及び主務省令で定める事項を特別社会基盤事業所管大臣及び内閣総理大臣に報告しなければならない。

○主務省令

（特定侵害事象等の報告）

第四条　（略）

2　法第五条の規定による報告は、特定侵害事象又は前項の事象（次に掲げる事象を除く。以下この条において「特定侵害事象等」という。）の発生を認知した後、速やかに、特別社会基盤事業所管大臣及び内閣総理大臣に次項に掲げる事項（同項第三号から第七号までに掲げる事項については、報告をしようとする時点において認知しているものに限る。）を記載した報告書（特別社会基盤事業所管大臣及び内閣総理大臣が定める様式による報告書をいう。以下この項において同じ。）を提出するとともに、当該特定侵害事象等の発生を認知した日から三十日以内に、特別社会基盤事業所管大臣及び内閣総理大臣に次項に掲げる事項を記載した報告書を提出して行うものとする。

一　特別社会基盤事業者（経済安全保障推進法第五十三条第一項各号のいずれかに掲げる事由により経済安全保障推進法第五十条第一項の主務省令で定める基準に該当することとなった者を除く。）が同項の規定による指定を受けた日から六月以内に発生した事象（当該指定に係る特定社会基盤事業の用に供される特定重要設備に係る特定重要電子計算機において発生した事象に限る。）

二　経済安全保障推進法第五十条第一項の特定重要設備を定める主務省令の改正により新たに特定重要電子計算機となった日から六月以内に発生した事象（当該特定重要電子計算機において発生した事象に限る。）

三　特定重要電子計算機（一号電子計算機並びに第一条第一項第一号及び第二号に規定するものを除く。）に対する法第二条第四項第三号に該当する行為（刑法（明治四十年法律第四十五号）第二百三十四条の二第二項の罪に当たる行為に係るものに限る。）により、当該特定重要電子計算機のサイバーセキュリティが害される事象（他の特定不正行為（法第二条第四項に規定する特定不正行為をいう。）に係る事象又は当該事象の痕跡が記録される事象に該当するものを除く。）

3　法第五条の主務省令で定める事項は、次に掲げるもの（特定侵害事象等の発生を認知した後速やかに報告する場合における第三号から第七号までに掲げる事項については、報告をしようとする時点において認知しているものに限る。）とする。

一　報告の区分
二　特別社会基盤事業者の概要
三　特定侵害事象等の概要
四　特定侵害事象等が発生した特定重要電子計算機
五　特定侵害事象等に関する技術的な事項
六　特定侵害事象等への対応に関する事項
七　その他特記事項

○重要電子計算機に対する不正な行為による被害の防止に関する法律に基づく特別社会基盤事業者による特定侵害事象等の報告等に関する命令第四条第二項の特別社会基盤事業所管大臣及び内閣総理大臣が定める様式を定める件（令和8年内閣府・総務省・法務省・財務省・厚生労働省・農林水産省・経済産業省・国土交通省告示第2号）

重要電子計算機に対する不正な行為による被害の防止に関する法律に基づく特別社会基盤事業者による特定侵害事象等の報告等に関する命令第四条第二項の特別社会基盤事業所管大臣及び内閣総理大臣が定める様式は、次の各号に掲げる事象の区分に応じ、当該各号に定める様式とする。

一　「サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ」（令和七年五月二十八日関係省庁申合せ。以下「関係省庁申合せ」という。）2. に規定するDDoS攻撃事案に該当する事象　関係省庁申合せ別添様式1
二　関係省庁申合せ2. に規定するランサムウェア事案に該当する事象　関係省庁申合せ別添様式2
三　前二号に掲げる事象以外の事象　関係省庁申合せ別添様式3

6-1　報告対象（法第5条、主務省令第4条第2項）

特別社会基盤事業者は、5-1 及び 5-2 に記載した事象の発生を認知した際は、事業所管大臣及び内閣総理大臣に報告する。ただし、以下の事象については、特定侵害事象等に該当しない事象として取り扱われるため、報告を要さない。

① 特別社会基盤事業者（経済安全保障推進法第 53 条第1項各号のいずれかに掲げる事由（事業承継・合併・分割）により経済安全保障推進法第 50 条第1項の主務省令で定める基準に該当することとなった者を除く。）が経済安全保障推進法第 50 条第1項の規定による指定を受けた日から6月以内に発生した事象（当該指定に係る特定社会基盤事業の用に供される特定重要設備に係る特定重要電子計算機において発生した事象に限る。）

② 経済安全保障推進法第 50 条第1項の特定重要設備を定める主務省令の改正により新たに特定重要電子計算機となった日から6月以内に発生した事象（当該特定重要電子計算機において発生した事象に限る。）

③　特定重要電子計算機（①特定重要設備及び②[E]特定重要設備と同一セグメントの機器を除く。）に対する法第2条第4項第3号に該当する行為（刑法第 234 条の2第2項の罪に当たる行為に係るものに限る。）により、当該特定重要電子計算機のサイバーセキュリティが害される事象（他の特定不正行為に係る事象又は当該事象の痕跡が記録される事象に該当するものを除く。）

③の事象は、電子計算機損壊等業務妨害の未遂の罪に当たる行為に係る特定侵害事象等であり、このうち①特定重要設備及び②[E]特定重要設備と同一セグメントの機器以外で発生したものであって、他の特定侵害事象等の類型に該当しないものは、報告の必要はない。

6-2　報告期限（法第5条、主務省令第4条第2項）

サイバーインシデントの報告義務は、事象の発生の報告を速やかに行う「速報」と、サイバー攻撃や被害の全容を整理した「詳報」の2回の報告を求めている。ただし、速報から詳報の間や詳報後に判明した情報等がある場合は、速報・詳報とは別に、続報を行うことが望ましい。

「速報」の報告は、サイバー攻撃の類型によって以下の期限内の報告を要する。

- DDoS 攻撃事案は、認知後に可能なかぎり速やかな報告を行う。
- ランサムウェア事案やその他サイバー攻撃事案は、認知した日から3～5日以内に報告を行う。

「詳報」の報告は、認知した日から 30 日以内の報告を要する。

なお、報告期限が行政機関の休日（日曜日及び土曜日、国民の祝日に関する法律に規定する休日並びに 12 月 29 日から翌年の1月3日までの日）に当たるときは、行政機関の休日の翌日をもってその期限とみなす（行政機関の休日に関する法律第2条）。その他、期限の計算については、民法第1編第6章の例による。

DDoS 攻撃、パスワードスプレー攻撃・ブルートフォース攻撃等は、一定期間中に断続的に行われることもあるため、同一と思われるサイバー攻撃者からの攻撃の速報はその初回分のみ報告を行い、2回目以降の攻撃については詳報でまとめて報告すること。

同一インシデントにおいて新たな特定侵害事象又は特定侵害事象の原因となり得る事象を認知した場合には、一つのインシデントを単位として報告を継続し、新たに判明した内容は続報として報告すること。

6-3　報告方法

報告方法については、官民連携基盤を介した提出を想定しており、手続きについては、当該基盤に係るマニュアルを参照する。その他、電子メールでの提出については、所管省庁及び内閣府に確認を行う。

6-4 報告事項

特定侵害事象等の報告における主務省令で定める報告事項は、表7に示す報告様式に記載欄を設けており、報告に当たっては本様式を使用する。報告事項の全量が未把握又は未確定である場合は、報告時点で把握している事項を記載すればよい。また、既に行った報告に誤り等があった場合は、続報等で訂正・補足することが望ましい。

サイバー脅威の分析に資する以下の事項の詳細等が判明した場合は、詳報の提出後であっても続報として報告を行い、その際、表7に示す様式に記載しきれない場合には、別紙に記載の上で報告することができる。また、報告について、内閣府又は関係省庁等からの内容の確認があった場合は適切に対応する。

- インディケータ情報（侵害の痕跡）
  攻撃元の IP アドレス・ポート、攻撃先（被害システム）の IP アドレス・ポート、関連する URL・ドメイン、マルウェアのハッシュ値やマルウェア本体等
- 攻撃の手口・侵入経路
  想定される攻撃手法、悪用された脆弱性情報、攻撃対象の機器・ソフトウェアの名称・バージョン等、攻撃対象のシステム等が取扱う情報や有する機能、攻撃対象のアカウント（ID）・アカウント利用者の属性等
- システム構成が分かる図
- 攻撃の時系列
- インシデントに関係するフォレンジック結果報告書
- その他サイバー脅威の分析に有用な情報

なお、速報時点で DDoS 攻撃か、ランサムウェア攻撃か不明な事象は「その他サイバー攻撃事案」として「サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ」（令和7年5月 28 日関係省庁申合せ。以下「関係省庁申合せ」という。）別添様式3により提出を行い、その後 DDoS 攻撃又はランサムウェア攻撃と発覚した場合であっても、引き続き「その他サイバー攻撃事案」として扱い、別添様式3により続報又は詳報を提出することができる。なお、この場合であっても、別添様式1又は別添様式2に記載すべき情報と同程度に詳細な情報を記載することが望ましい。

表7　報告様式

事象	様式
関係省庁申合せ2. に規定するDDoS攻撃事案	関係省庁申合せ別添様式1
関係省庁申合せ2. に規定するランサムウェア事案	関係省庁申合せ別添様式2
上記以外の事案	関係省庁申合せ別添様式3

※関係省庁申合せ及び別添様式（記載例を含む。）
https://www.cyber.go.jp/policy/group/cyber/policy.html

7. 補足事項

7-1　FAQ

Q1. 特定侵害事象等の報告対象となる電子計算機は、法第4条（特定重要電子計算機の届出）に基づき届出された電子計算機が対象なのか。

A. 届出を行った電子計算機は報告対象となるが、特定重要電子計算機に該当する電子計算機であれば、届出を行っていなくても報告対象となる。例えば、専用設計品や広く一般に使用されている製品として届出を行わなかった電子計算機も、特定侵害事象等の報告の対象となる。

Q2. 委託先会社が管理している特定重要電子計算機が侵害された場合も報告の対象となるか。

A. 特別社会基盤事業者が管理している特定重要電子計算機が侵害された場合と同様に、特定侵害事象等の報告の対象となる。特別社会基盤事業者は、委託先会社から侵害の事実の通知を受け次第、特定侵害事象等であるかを判定する。報告対象であった場合は、報告に必要な情報の共有を受け、法第5条に基づく報告を行う。報告に当たっては、中小受託取引適正化法（製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律。昭和31 年法律第 120 号）第5条で禁止行為とされる「不当な経済上の利益の提供要請」に該当しないよう留意する。

Q3. 共同利用している特定重要電子計算機が侵害された場合も報告の対象となるか。

A. 複数の特別社会基盤事業者が共同で利用している特定重要電子計算機が侵害された場合、当該複数の特別社会基盤事業者が特定侵害事象等の報告をする必要がある。

共同利用によって運営されている特定重要電子計算機のセキュリティ監視が自組織以外の共同利用をしている組織によって行われている場合等、特別社会基盤事業者が能動的に侵害

の発生を認知できない場合は、セキュリティ監視等のシステム管理を行う事業者から侵害の事実の通知を受け次第、特定侵害事象等の報告に必要な情報の共有を受け、法第5条に基づく報告を行う。

Q4. クラウドサービスで構成する特定重要電子計算機が侵害された場合も報告の対象となるか。

A. 特別社会基盤事業者が管理している特定重要電子計算機が侵害された場合と同様に、特定侵害事象等の報告の対象となる。

クラウドサービスには、SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）等の様々なサービス形態があり、サービス形態によってサービス契約者（本解説においては特別社会基盤事業者）とクラウドサービス事業者の責任分界点が異なっている。

サービス単位で契約を行う SaaS の場合はデータ（データ及びユーザーアカウント）のみ責任分界が契約者側となり、アプリケーション、ミドルウェア、OS への侵害の発生については特別社会基盤事業者が能動的に認知できない場合も考えられる。そのため、SaaS のサービス形態となる特定重要電子計算機の侵害は、クラウドサービス事業者から侵害の事実の通知を受け次第、特定侵害事象等の報告に必要な情報の共有を受け、法第5条に基づく報告を行う。

一方、プラットフォーム単位で契約を行うPaaSの場合はアプリケーションまで、情報通信インフラ単位で契約を行う IaaS の場合はアプリケーションに加えてミドルウェア及び OS の責任分界が契約者側となるため、それらの特定重要電子計算機の侵害が発生し、特別社会基盤事業者の監視等により事象を認知した際は、法第5条に基づく報告を行う。（ただし、PaaS についても OS 及びミドルウェアへの侵害の場合は、特別社会基盤事業者が侵害の発生を能動的に認知できないと考えられるため、クラウドサービス事業者からの侵害の事実の通知を受けた場合は、速やかに報告を行うこととなる。）

サイバーインシデントやサービス障害発生時の通知に関する事項が定められているか否かはクラウドサービス事業者によって異なる。そのため、契約しているクラウドサービスの SLA（サービスレベル合意書）、SLO（サービスレベル目標）、利用規約にサイバーインシデントまたはサービス障害発生時に契約者に対する通知の詳細（通知する事象の種類、通知方法、事象発生から通知までの時間）が定義されているか確認することが望ましい。

Q5. 侵害された機器が日本国外に存在する場合も報告の対象となるか。

A. 侵害された特定重要電子計算機が日本国外に存在する場合も、特定侵害事象等の報告の対象となる。ただし、諸外国においてはデータの国内保管義務や国外へのデータ移転を制限する法律（いわゆるデータローカライゼーション規制）が施行されていることがあるため、この対応に留意する。

Q6. 災害復旧サイトの機器のみが侵害された場合も報告の対象となるか。

A. いわゆる主系の機器は侵害されず、災害復旧サイト(副系)のみが侵害された場合であっても、侵害された機器が特定重要電子計算機に該当するのであれば、特定侵害事象等の報告の対象となる。

Q7. 特定重要電子計算機が感染しマルウェアが動作したものの、EDR 製品の振る舞い検知が即座に動作したため適切に隔離・削除が行われた。この場合は報告対象に当たるか。

A. 当該特定重要電子計算機が①特定重要設備又は②[E]特定重要設備と同一セグメントの機器である場合には、特別社会基盤事業者が当該特定重要電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録が受信される事象等に該当し、報告の対象である。

当該特定重要電子計算機が①特定重要設備又は②[E]特定重要設備と同一セグメントの機器でない場合は、特定侵害事象等に該当しないため、報告は不要である。

Q8. 侵害の痕跡からマルウェア検体を確保した。報告時に提出は必要か。また、どのような方法で提出すればよいか。

A. マルウェア検体の提出は必須でないが、当該マルウェア検体の解析結果や、他の事業者から報告されたインシデント事案報告について集約・分析することで、サイバー脅威情勢を正しく認識したうえで、提出した事業者のセキュリティ確保に資するのみならず、他の事業者向けにも効果的な被害未然防止・被害拡大防止に資する情報共有や注意喚起につながることから、可能な限りマルウェア検体を提出することが望ましい。マルウェア検体の取扱いは注意が必要であるため、提出する際は内閣府及び所管省庁と相談すること。

他の法令との関係

特別社会基盤事業者の業法等に基づく事故報告

サイバーインシデントの発生したときは、法第5条に基づく報告のほか、各業法やガイドライン、分野内情報共有組織(ISAC 及び CEPTOAR 等)において事故報告が求められる場合がある。

個人データ漏えい等に伴う個人情報保護法に基づく報告及び番号法に基づく報告

個人情報取扱事業者は、取り扱う個人データの漏えい等であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護委員会への報告が必要となる(個人情報保護法(平成 15 年法律第 57 号)第 26 条第1項、第 68 条第1項)。また、特定個人情報ファイルに記録された特定個人情報の漏えい、滅失、毀損その他の

特定個人情報の安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときにも、個人情報保護委員会への報告が必要となる（行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）第29条の4第1項）。

8. 付録

8-1 サイバー攻撃の脅威

海外の重要情報インフラ事業者へのサイバー攻撃事例

海外における重要情報インフラへのサイバー攻撃の事例を紹介する。

① 2021年米国最大手のパイプラインのランサムウェア被害[2]

2021年5月7日米国最大手のパイプライン企業 Colonial Pipeline がランサムウェアによるサイバー攻撃を受けた。被害は情報系であり、パイプライン制御システムそのものは直接の影響を受けていなかったが、予め決められていた全社的なインシデント対応プロセスに則って、パイプラインは予防保全的に停止された。

② 2022年衛星通信サービスの機能停止[3]

米 Viasat 社は、仏 Eutelsat S.A.が保有する通信衛星 KA-SAT を利用した衛星ブロードバンド接続サービスを主にヨーロッパと中東の 10 万人を超える顧客に提供している。このサービスの利用者の中には、ウクライナの軍や警察機関も含まれていた。

2022年2月 24 日午前3時2分頃、ロシアがウクライナへ侵攻を開始する1時間前に、突然 KA-SAT ネットワークが利用できなくなった。

③ Stuxnet:制御システムを標的とする初めてのマルウェア[4]

2010 年9月に、イランのナタンズに所在する核燃料施設のウラン濃縮用遠心分離機を標的として、サイバー攻撃があったことが公表され、世界初の制御システムを標的とするサイバー兵器とも言われた。

---

[2] 制御システムのセキュリティリスク分析ガイド補足資料：「制御システム関連のサイバーインシデント事例」シリーズ 【事例9】2021 年 米国最大手のパイプラインのランサムウェア被害
https://www.ipa.go.jp/security/controlsystem/ug65p900000197wa-att/000093825.pdf

[3] 制御システムのセキュリティリスク分析ガイド補足資料：「制御システム関連のサイバーインシデント事例」シリーズ 【事例 10】2022 年 衛星通信網へのサイバー攻撃の事例
https://www.ipa.go.jp/security/controlsystem/ug65p900000197wa-att/incident_10.pdf

[4] 制御システムのセキュリティリスク分析ガイド補足資料：「制御システム関連のサイバーインシデント事例」シリーズ 【事例4】Stuxnet：制御システムを標的とする初めてのマルウェア
https://www.ipa.go.jp/security/controlsystem/ug65p900000197wa-att/000080701.pdf

Stuxnet と呼ばれるマルウェアが核燃料施設に持ち込まれ、マルウェアに感染させられたコンピュータによって、遠心分離機を制御するPLCの設定ロジックが改ざんされ、周波数変換器が攻撃されたことにより、約 8,400 台の遠心分離機のうち約 1,000 台が稼働不能に陥り、操業が一時停止する事態となった。

8-2 参考となる他ガイドライン

個人情報の保護に関する法律についてのガイドライン

個人情報保護法第 26 条第1項に基づく報告等について解説する。

https://www.ppc.go.jp/personalinfo/legal/

経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度の解説

経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和4年法律第 43 号）第3章の特定社会基盤役務の安定的な提供の確保に関する制度について、導入等計画書の事前届出等に関する事項等を解説する。

制御システムのセキュリティリスク分析ガイド 第 2 版（令和8年4月6日情報処理推進機構）

制御システムのセキュリティリスク分析について解説する。

独立行政法人情報処理推進機構「情報システム・モデル取引・契約書（第二版）」

有事の際に委託先会社等の外部組織と適切なコミュニケーションを取りながらサイバーインシデント報告を行うために、平時に結ぶことが望ましい契約内容等が掲載されている。

https://www.ipa.go.jp/digital/model/model20201222.html

独立行政法人情報処理推進機構「制御システム関連のサイバーインシデント事例」シリーズ

海外における重要インフラに相当する制御システムに対するセキュリティインシデントの詳細が解説された資料である。

https://www.ipa.go.jp/security/controlsystem/incident.html

The MITRE Corporation「MITRE ATT&CK」

サイバー空間の観測に基づいた、サイバー攻撃者の戦術と手法に関するナレッジデータベースである。

https://attack.mitre.org/

ISA/IEC 62443

OT 環境のセキュリティを確保するための推奨事項を規定した国際標準規格。

8-3 用語の解説

本解説に登場する用語

用語	説明
特定社会基盤事業者	経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和4年法律第 43 号）の第 50 条第1項に基づき、主務大臣から指定を受けた者。 ※特定社会基盤事業者に指定されている事業者の一覧は、内閣府ホームページの「基幹インフラ役務の安定的な提供の確保に関する制度」[5] に掲載されている。
特別社会基盤事業者	特定社会基盤事業者のうち、特定重要電子計算機を使用する者。（法第2条第3項）
特定重要設備	特定社会基盤事業の用に供される設備、機器、装置又はプログラムのうち、特定社会基盤役務を安定的に供給するために重要であり、かつ、我が国の外部から行われる特定社会基盤役務の安定的な提供を妨害する行為の手段として使用されるおそれがあるものとして経済安全保障推進法第 50 条第1項の主務省令で定めるもの。
構成設備	経済安全保障推進法第 52 条第2項第2号ハの主務省令で定める設備、機器、装置又はプログラム。
特定重要電子計算機	特定社会基盤事業者が使用する電子計算機のうち、そのサイバーセキュリティが害された場合において、特定重要設備の機能が停止し、又は低下するおそれがあるものとして政令で定めるもの（当該特定重要設備の一部を構成するものを含む。）（法第2条第2項）。
特定重要設備等	令第1条第3項第1号に規定する電子計算機及び主務省令第1条第1項第1号、2号に規定する電子計算機をいう。

[5] 内閣府ホームページ「基幹インフラ役務の安定的な提供の確保に関する制度」
https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/infra.html

用語	説明
特定侵害事象	重要電子計算機に対する特定不正行為により、当該重要電子計算機のサイバーセキュリティが害されること。(法第2条第5項)
特定侵害事象等	特定侵害事象及び特定侵害事象の原因となり得るものとして主務省令で定める事象
特定不正行為	以下いずれかに該当する行為。(法第2条第4項) ● 刑法(明治 40 年法律第 45 号)第 168 条の2第2項(不正指令電磁的記録供用等)の罪に当たる行為 ● 不正アクセス行為(不正アクセス行為の禁止等に関する法律(平成 11 年法律第 128 号)の第2条第4項に規定する行為) ● 電子計算機を用いて行われる業務に係る刑法 第 233 条(偽計業務妨害)、第 234 条(威力業務妨害)、第 234 条の2(電子計算機損壊等業務妨害)の罪に当たる行為であって、当該電子計算機のサイバーセキュリティを害することによって行われるもの ※当該電子計算機に接続された電気通信回線の機能に障害を与えることによって行われるものを含む。
サイバーセキュリティ	電子的方式、磁気的方式その他人の知覚によっては認識することができない方式(電磁的方式)により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置(電磁的記録媒体を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。)が講じられ、その状態が適切に維持管理されていること。(サイバーセキュリティ基本法(平成 26 年法律第 104 号)第2条)
アタックサーフェス(Attack Surface)	組織の外部(インターネット)からアクセス可能な IT 資産のこと。
資産	システムを構成する物理的な機器、機器に格納されている情報資産(ソフトウェア)、サービスを指す。攻撃者による攻撃から防御すべき事業者の所有物である。
FW	Firewall(ファイアウォール)の略。ネットワークの境界等に設置され、内外の通信を中継・監視し、外部の攻撃から内部を保護するためのソフトウェアや機器、システム等のこと。

用語	説明
IPS	Intrusion Prevention System の略。サーバーやネットワークの外部との通信を監視し、侵入の試み等の不正なアクセスを検知して遮断することで、攻撃を未然に防ぐシステムのこと。
UTM	Unified Threat Management の略。FW や IPS、アンチウィルス、アンチスパム、Web フィルタリング等の複数のセキュリティ機能を一つのハードウェアに統合し、ネットワークを効率的かつ包括的に保護するハードウェアやアプライアンス等のこと。
WAF	Web Application Firewall の略。Web アプリケーションの脆弱性を悪用した攻撃から Web サイトを保護するシステムのこと。Web サーバーとインターネット等の外部との中間に設置してサーバーと外部との通信を監視し、攻撃と判断した通信を遮断する機能を持つ。
IaaS	Infrastructure as a Service の略。クラウドコンピューティングの一形態で、物理的なサーバー、ストレージ、ネットワーク等のインフラストラクチャをインターネット経由で提供するサービスである。
PaaS	Platform as a Service の略。クラウドコンピューティングの一形態で、アプリケーション開発やデプロイに必要なプラットフォームをクラウド上で提供するサービス。
SaaS	Software as a Service の略。クラウドコンピューティングの一形態で、インターネットを通じてソフトウェアを提供するサービスである。ユーザーはソフトウェアを購入してインストールするのではなく、月額や年額のサブスクリプション形式で料金を支払って利用する。
閉域網	通信事業者が管理するネットワークを利用し、VPN 等で特定の接続点間のみの通信に限定した仮想的なネットワーク（エントリーVPN、IP-VPN、広域イーサネット）のこと。なお、インターネット VPN（SSL-VPN、IPsec-VPN）はインターネット接続として扱う。
専用線	事業者が自ら敷設し管理する、自社専用の物理的なネットワーク又は通信事業者等により提供され特定の利用者が占有的に利用する通信回線のこと。
イーサネット	有線接続でコンピュータネットワークを構築するための標準的な通信技術、規格である。LAN（ローカルエリアネットワーク）内のデバイス同士を接続するために広く使用され、通常はイーサネットケーブルとスイッチやルーター等のネットワーク機器を介して接続される。
VPN	Virtual Private Network の略。主にインターネット上で、認証技術や暗号化等の技術を利用し、保護された仮想的な専用線環境を構築する仕組み。
DMZ	Demilitarized Zone の略。直訳すると「非武装地帯」。組織の内部ネットワークと外部ネットワーク（通常はインターネット）の間に配置される中間領域のことである。DMZ の主な目的は、外部からアクセスされるサービス（例えば、Web サーバー、

用語	説明
	メールサーバー、DNS サーバー等を指す。)を配置し、内部ネットワークを直接攻撃から保護することである。
L3SW	ネットワークの中継機器の一つで、プロトコル階層でいうネットワーク層(第3層)とリンク層(第2層)の両方の制御情報に基づいてデータの転送先を決定する。
EC2	Amazon Elastic Compute Cloud の略。 AWS(Amazon Web Services) が提供する仮想サーバー構築のクラウドサービスのこと。
RDS	Relational Database Service の略。AWS(Amazon Web Services) が提供するクラウド上のリレーショナルデータベースサービスのこと。
AD サーバー	Active Directory サーバーの略。Windows サーバーに搭載されているディレクトリサービスの一種で、管理するネットワーク上に存在する様々な資源やその利用者の情報、権限等を一元管理することができるサーバーのこと。
LDAP サーバー	Lightweight Directory Access Protocol サーバーの略。インターネット等の IP ネットワークを通じてディレクトリサービスにアクセスするためのプロトコル(LDAP)に基づき、システム上の資源や利用者の情報を集約し、一元管理することができるサーバーのこと。
Kerberos	ネットワークを通じてコンピュータ間で利用者認証を行う方式の一つで、シングルサインオンを実現する方式として普及している。複数のサーバーで共通の認証情報を利用することができ、通信経路を暗号化して認証情報を安全に送受信することができる。
SAML	Security Assertion Markup Language の略。異なるインターネットドメインの間での利用者の認証や認可に関する情報を伝達するための XML ベースの標準規格の一つ。
OAuth 2.0	運営主体の異なる複数の Web サイトやネットサービス、ソフトウェア等の間で、データや機能へのアクセス権限の認可情報(アクセストークン)を送受信するためのプロトコルの一つ。
HMI	Human Machine Interface の略。制御システムを構成する資産の一つで、コントローラーからの測定値を監視し、設定値(目標値)を入力する端末である。
サイバー攻撃者	特定不正行為を行う者。 特定組織・機関のみを狙った国家背景型、金銭窃取を目的とした犯罪組織型、思想・信条に基づく活動を行うハクティビスト型等、様々な主体が存在する。
マルウェア	人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録。(いわゆる、コンピュータウィルスと呼ばれる不正プログラム。)

用語	説明
フィッシング	実在する組織を騙って、ユーザー名、パスワード、アカウント ID、暗証番号といった情報を詐取する攻撃。 電子メールのリンクから偽サイト（フィッシングサイト）に誘導し情報を入力させる手口や、メールにマルウェアが混入した添付ファイルを付加しファイルを動作させる手口が一般的に使われている。
脆弱性	ソフトウェア製品等におけるセキュリティ上の問題箇所。 特に不正アクセス行為やマルウェア等により、この問題箇所が攻撃されることで、そのソフトウェア製品の本来の機能や性能を損なう原因となり得るものを指す。
DDoS 攻撃	情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体を通じた電子計算機に対する攻撃のうち、送信先の電気通信設備の機能に障害を与える電気通信の送信により行われるもの。
ランサムウェア攻撃	ランサムウェアと呼ばれる感染した機器内のファイル等を暗号化するマルウェアを用いて、ファイル等の復号と引替に身代金（Ransom）を要求するための攻撃。 近年ではランサムウェアを用いずに、窃取した情報の暴露や DDoS 攻撃を行うことを仄めかし、身代金を要求する攻撃もある。
ワイパー攻撃	攻撃対象機器内のファイル等を上書き等の方法で削除し、機器を恒久的に動作不良に陥らせる攻撃。
潜伏型攻撃（長期潜伏）	不正アクセス行為やマルウェア感染の事実が発覚しないようバックドア設置やセキュリティ検知の無力化等を行いながら、継続的な情報窃取や、サイバー攻撃者の任意のタイミングでネットワーク内部の破壊活動を行える状態を維持する攻撃。
標的型攻撃	特定の事業者や組織を狙ったサイバー攻撃。 対義語として、不特定多数の事業者や組織を狙ったばらまき型攻撃がある。
MITRE ATT&CK	米国の非営利組織の MITRE 社が提唱する、サイバー攻撃者の戦術と手法に関するフレームワーク。 サイバー攻撃の段階を示す Tactics や各段階における詳細な攻撃手法を示す Techniques 等が体系的に整理されている。

以 上