水道分野における情報セキュリティ確保に係る安全ガイドライン
概要版

国土交通省 水管理・国土保全局

水道事業課

令和７年３月

安全ガイドラインについて

国土交通省

- 本ガイドラインは、これまで厚生労働省において策定・改訂されてきた「水道分野における情報セキュリティガイドライン」を、**政府の行動計画・指針等の策定や水道行政の移管に伴って抜本的に見直し**、国土交通省所管の他の重要インフラ分野と同様のフォーマットで「水道分野における情報セキュリティ確保に係る安全ガイドライン（第一版）」として新たに策定したものです。

- 本ガイドラインは、関係法令に準じて国が定める「ガイドライン」として、（強制基準ではなく）**推奨事項を列挙**しているものであり、事業分野の特性に鑑み、重要インフラ事業者等が**自らのセキュリティ管理策を実施する際に参考資料として活用することを想定**しています。

- このため、別紙３等に記載されている対策例については、必ずしもその全てを実施しなければならないというものではなく、**各水道事業者等の置かれている状況等に鑑みて、できることから実施**していくことが望ましいものです。

- 本ガイドラインは、７つの章と３つの別紙から構成されています。中でも、他の章とは異なって、**第２章は、水道分野に固有の現状と課題**を踏まえて書かれています。**「閉域網」の考え方**については、ご一読の程をお願いします。

- また、**コラム２（本概要版では11～13頁）は、サイバーセキュリティに係る水道施設の技術的基準を定める省令について、その留意事項に焦点を当てて、かみ砕いて解説**したものです。こちらは、**法令において定められた、遵守すべき技術的基準**ですので、水道技術管理者を始め、水道事業者・水道用水供給事業者・専用水道の設置者は、法令の遵守に当たり遺漏のないようにお願いします。

水道事業者等の担当者の皆様へ

国土交通省

- 本ガイドラインでは、特に、サイバーセキュリティ責任者を任命すべきであるとしており、その任命に当たっては、経営層の責任において実施するものとしています（3.4.1 サイバーセキュリティ責任者の任命）。

- サイバーセキュリティ責任者は、セキュリティ管理策の運用が可能となる組織のまとまり毎の取りまとめの責任者であり、例えば、組織のまとまりの単位が水道局の場合は局長クラス、浄水場単位の場合は場長クラスが相当しますが、組織の実態に合わせて、また、意思決定プロセスや役職においてより上位である最高情報セキュリティ責任者（CISO。事業者内における情報セキュリティ対策の推進の責任者であり、民間企業では役員クラスの幹部職員等）の役職を踏まえて、役職のレベルを設定することとしています（1.1.6 責任者・組織等の役割）。

- サイバーセキュリティ責任者は、その役割として、組織のセキュリティ管理策を推進及び運用するため、組織内の体制整備及び事務を行います。また、組織内の実施手順を策定するとともに、セキュリティ管理策の運用実態を十分踏まえ、実務レベルでの管理の仕組みを確立し、全ての取扱者への責務の周知や教育を行う等、個別対策を機能させる環境を整備することとします。サイバーセキュリティ責任者の役割が具体的に示されている箇所を例示すると以下のとおりであり、主に「サイバーセキュリティ責任者」を主語とする文章で示されています。

  ○サイバーセキュリティ責任者の役割が示されている箇所の例
  3.6 監査・モニタリング；3.8 継続的改善；4 リスクマネジメントの活用と危機管理；5.1 組織的対策
  5.2 人的対策；5.3 物理的対策；5.4 技術的対策；5.6 委託先管理；別紙1 1 情報の取扱いについての規定化

- 自らの組織内で役職上位の管理職員等に本ガイドラインのことを紹介するに当たっては、**本ガイドラインの位置付け（推奨事項を列挙しているもの）**を説明し、**目次構成を参照しながら重要インフラ事業者として求められていることを概観**した上で、すでにサイバーセキュリティ責任者が定められている場合には、**サイバーセキュリティ責任者の役割として求められていることを中心に説明することが一案**として考えられます。一方で、サイバーセキュリティ責任者（に相当する責任者）が定められていない場合には、まずはサイバーセキュリティ責任者を定めることを検討いただくことが考えられます。（あくまで一案であり、これに限ることなく、各水道事業者等の実情に合わせるようお願いします）

安全ガイドラインの目次構成

国土交通省

サイバーセキュリティ戦略本部が決定した「安全基準等策定指針」に則り、構成を以下のとおりとしている

はじめに ～ 1.「安全ガイドライン」策定の背景（1）

国土交通省

- 国民生活及び社会経済活動は、様々な社会インフラによって支えられており、その機能を実現するために情報システムが幅広く用いられている。こうした中で、機能が停止または低下した場合に多大なる影響を及ぼしかねないサービスは、重要インフラとして官民が一丸となり、重点的に防護していく必要がある
- 国土交通省では、所管する**重要インフラ５分野（鉄道、航空、空港、物流、水道）**における各事業分野及び関連事業者のセキュリティ管理策の現状に配慮しながら、各事業分野におけるセキュリティ管理策の向上に資する望ましいセキュリティ管理策の水準をまとめ、**サイバーセキュリティ確保に係る安全ガイドラインを策定**しており、**指針の改正や世の中の情勢を踏まえ、適宜、本ガイドラインを改定**することとしている

「安全ガイドライン」の目的と形態

目的

重要インフラ事業者等は、重要インフラサービスを安全かつ持続的に提供するという社会的責任を負う立場であり、**任務保証の考え方**を踏まえ、以下に例示する必要な対策に取り組むことが重要である

- ❒ サイバーセキュリティに係るリスクへの備えを経営戦略として位置づけ
- ❒ リスクマネジメントにおいてサイバーセキュリティも取り扱う
- ❒ サイバーセキュリティリスクへの必要な備えの実践
- ❒ 有事の際の適切な対処の実現　等

<任務保証の考え方>
企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方。
「重要インフラのサイバーセキュリティに係る行動計画」より抜粋

形態

サイバーセキュリティ戦略本部決定の「安全基準等策定指針」においては、重要インフラ事業者等が参考とする文書類を「安全基準等」と呼び、次の①～④に分類している

① 関係法令に基づき国が定める「強制基準」
② 関係法令に準じて国が定める「推奨基準」及び「ガイドライン」
③ 関係法令や国民からの期待に応えるべく、業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」
④ 関係法令や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める「内規」等

- 本ガイドラインは②に対応し、国が定める「ガイドライン」として**推奨事項を列挙**しているもの
- 事業分野の特性に鑑み、重要インフラ事業者等が自らのセキュリティ管理策を実施する際に**参考資料として活用することを想定**

1.「安全ガイドライン」策定の背景（2）

国土交通省

策定の背景

○「重要インフラのサイバーセキュリティに係る行動計画」（令和6年3月8日サイバーセキュリティ戦略本部改定）

- ✓ 重要インフラにおいて、任務保証の考え方を踏まえ、重要インフラサービスの継続的提供を不確かなものとするサイバー攻撃等をリスクとして捉え、リスクを許容範囲内に抑制すること及び障害発生時に迅速な復旧を図ることの両面から、強靭性を確保し、重要インフラサービスの安全かつ持続的な提供を実現すること（重要インフラ防護の目的）

○「重要インフラのサイバーセキュリティ確保に係る安全基準等策定指針」（令和5年7月4日サイバーセキュリティ戦略本部決定）

- ✓ 上記行動計画の内容を踏まえ、経営層の責務としてのセキュリティガバナンスや、サプライチェーンを含むリスクマネジメントにおけるサイバーセキュリティ確保、リスクアセスメントを行う際の考慮事項等を整理
- ✓ 構成面では、経営層が取り組む事項とセキュリティ責任者が取り組む事項でそれぞれの項目を作成し、ISO/IEC 27002:2022のセキュリティ管理策や昨今のインシデント事例を踏まえ、対策項目を整理するとともに、「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書」を新規に作成し、策定指針で示すセキュリティ確保に向けた取組についての参考情報を提供

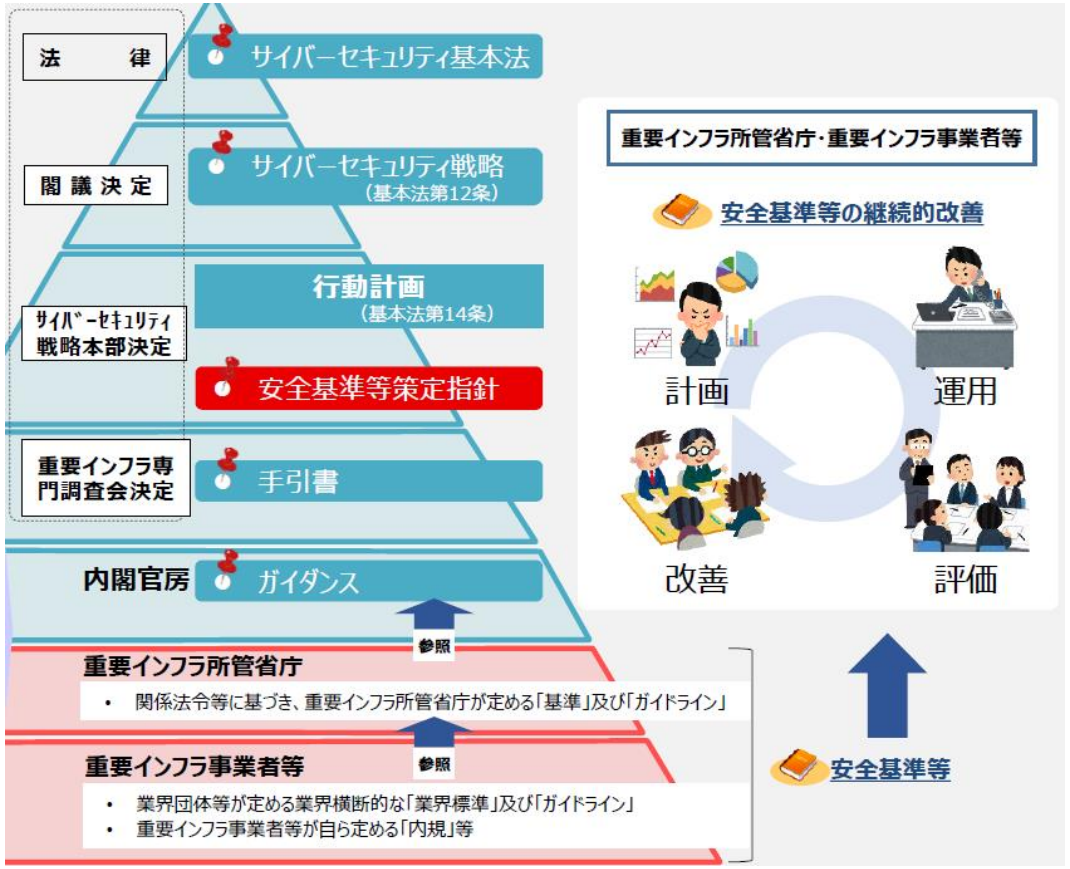
○その他参照規定の改定を反映

- ✓ 「政府機関のサイバーセキュリティ対策のための統一基準群」（令和5年7月4日サイバーセキュリティ戦略本部決定）
- ✓ 「サイバーセキュリティ経営ガイドライン Ver3.0」（令和5年3月24日経済産業省・独立行政法人情報処理推進機構改訂）

1.「安全ガイドライン」策定の背景（3）

国土交通省

- ✓ 水道事業者は、サイバーセキュリティ基本法が規定する重要インフラ事業者（重要社会基盤事業者）として、「任務保証の考え方」を踏まえ、水道事業における重要インフラサービスの継続性を維持するため、サイバーセキュリティ確保に取り組むことが重要である
- ✓ 本ガイドラインは、個々の重要インフラ事業者等が自主的に取組や対策を実施し、検証に当たっての目標を定めることを目的として策定されている



※「重要インフラのサイバーセキュリティに係る行動計画」の概要より抜粋
https://www.nisc.go.jp/pdf/policy/infra/cip_policy_abst_2022.pdf

2. 水道分野における「安全ガイドライン」の概要（1）

- ✓ 本ガイドラインの対象とする範囲は、水道分野において、**国民生活や社会経済活動への影響が大きく、事業継続に対する取組の対象となる情報システム及び情報資産**である
- ✓ 例えば、重要インフラサービス障害の発生によって水道サービスに影響を及ぼす以下の表の重要システム及びその中で利活用される情報資産が挙げられる（これら以外についても、**事業者の責任において検討し、抽出する必要**がある）

#	システム名称	概要
1	浄水場の監視制御システム	浄水処理を適切に行うために、各種機器の働きを制御する一連のシステム
2	ポンプ場の運転システム	ポンプ吐出圧（水量）、運転台数等を制御するシステム
3	水運用システム	地区毎の水需要（推定値）を基に、複数の浄水場、配水場等からの送配水量について効率的に調整するためのシステム
4	管路情報システム	地理情報システムを利用して配水管等の位置情報及び施設情報を管理するシステム
5	電子ファイリングシステム	配水管工事竣工図、写真等イメージデータを管理するシステム
6	給水台帳システム	給水装置の情報（使用者の個人情報を含む）を管理するシステム
7	設備管理システム	浄水場や配水場等の機械、電気・計装設備の情報を管理するシステム
8	設計・積算システム	管路等の設計を支援するCADシステムと作成した設計図面を基に積算を行う2つのシステムから成る
9	管網解析システム	配水管網内の水理状況、水質状況をシミュレーションするシステム
10	検針・水道料金システム	水道使用者のメータ水量を検針するためのシステム及び検針した値を使用者の個人情報等とともに一元的に管理するシステム
11	財務会計システム	予算、契約、決算等について管理するシステム
12	資産管理システム	水道事業者等の有する資産について償却状況、今後の見込み等を管理するシステム
13	人事管理システム	職員の個人情報、人事考課、給与算定等を管理するシステム
14	文書管理システム	予算、契約、決算等について管理するシステム

2. 水道分野における「安全ガイドライン」の概要（2）

- ✓ 水道分野において、国民生活や社会経済活動に影響を及ぼして事業継続の取り組み対象となるような重要システムには**「浄水場の監視制御システム」、「ポンプ場の運転システム」及び「水運用システム」**等がある
- ✓ 水道サービスの提供に係る情報システム、データセンター等の設備については、**各種災害による障害が発生しにくい適切な場所を設置の際に検討**するとともに、**災害が発生した場合であっても被害を低減できるような防止対策を事前に検討・実施**する等、適切な設備及び管理を行う仕組みを構築する必要がある
- ✓ 外部ネットワークと内部ネットワークとの**境界による防御には限界**があることから、従来の境界型のセキュリティ管理策に加え、**内部ネットワークにも脅威が存在し得ることを前提としたゼロトラストの考え方**に基づき、データや機器等の単位でのセキュリティ管理策が必要である
- ✓ それぞれの事業者が**目標とするセキュリティ水準**に向けたセキュリティ管理策の**継続的改善の実施**が必要である
- ✓ 閉域網を前提とした情報システムに関するリスクについてもまた重要である。**閉域網について正しく理解**していなければ「閉域網（であると自らが考えているもの・見せかけの閉域網を含む）であれば外部のインターネットとの接続は無い・安全である」といった過信から、洗い出すべきリスク源・対処すべきリスクを見落とすことに繋がりかねない

閉域網の一般的な定義

- 閉域網は**物理的にインターネット（公衆網）に接続していないネットワーク**のこと
- 水道の制御系システムでいえば、そのサーバ、端末、そして周辺機器等が接続しているネットワークが**物理的にインターネットと隔離**されていることが求められる
- 物理的な隔離としては、まず、**独自の回線や情報システムを構築し、物理的に外部のインターネットから遮断されている場合**がある。また、電気通信事業者が用意する専用の通信網である**広域イーサネット**や、その他の仮想的な専用線（VPN）の中でも**IP-VPNやエントリーVPN**は、厳密には論理的ではあるが、本ガイドラインにおいては、実態に鑑みて物理的に隔離されたものとして扱うこととする（**インターネットVPNの利用は、物理的に隔離されたものとみなさない**）
- ファイアウォールやルータ等のネットワーク機器による隔離は、「物理的に」インターネットから隔離していることに当たらない

2. 水道分野における「安全ガイドライン」の概要（3）

- ✓ 以下の各ケースは**閉域網を構築していることにはならない**ことに留意のこと
  - × ネットワークが**ファイアウォールやルータ等のネットワーク機器**によってインターネットとの通信を制限しているケース
  - × 専用線等により閉域網を構築していたネットワークが、**インターネットに接続している他のネットワークに接続**するケース。接続先のネットワークがネットワーク機器によってインターネットとの通信を制限していても、物理的にインターネットから隔離していることにはならなくなる。**接続先のネットワークにおいてどこか１地点でもインターネットと接続**していてもまた、物理的にインターネットから隔離していることにはならなくなる。閉域網とするには、接続先のネットワークにおいて、インターネットとの物理的な隔離が必要となる
  - × ネットワークが**インターネットVPN（SSL-VPN、IPsec-VPN）**によってインターネットからアクセス可能となっているケース
  - × 専用線等により閉域網を構築していたネットワークが、**インターネットVPNによりインターネットからアクセス可能となっている他のネットワークに接続**するケース。**接続先のネットワークにおいてどこか１地点でもインターネットVPNでインターネットと接続**可能となっていれば、物理的にインターネットから隔離していることにはならなくなる
- ✓ 水道情報システムにおける**制御系システムは、役務の提供の根幹となる重要な要素**であるため、セキュリティの観点からは、外部からの不正アクセス等のリスクを軽減するために、**インターネットとの接点を排除することが望ましい**

リスクに対処するためのセキュリティ対策の例

対策	概要
閉域網の利用によるシステムの保護	制御系システムは極力インターネットとの接点を排除して閉域網を構築することが望ましい
通信経路の保護	専用の通信網として広域イーサネットや、その他の仮想的な専用線（VPN）の中でもIP-VPNやエントリーVPNを利用するなど、通信経路の暗号化・認証機能の適用によって保護することが望ましい
やりとりされるデータの保護	情報システム内でやりとりするデータそのものを暗号化することが望ましい

水道施設の技術的基準（サイバーセキュリティ）（1）

国土交通省

- ✓ 「水道施設の技術的基準を定める省令」では、**水道施設の運転管理をする電子計算機**に関して、**サイバーセキュリティを確保するための必要な措置が講じられていること**が具備すべき要件として規定されている

- ✓ 具体的には、**制御系システム（浄水場の監視制御、ポンプ場の運転、水運用等）に使用されている電子計算機***について、次の**４点の措置**が講じられているよう、留意事項が示されている（令和７年２月28日付け国水水第399号国土交通省水管理・国土保全局水道事業課長通知による一部改正後のもの）（*コンピューター全般を指し、情報システムを構築するサーバ、端末、周辺機器等の装置全般）

  ① 電子計算機へアクセスする者について**主体認証を行うことができる機能を有する**こと

  ② 不正プログラム対策として、**アンチウイルスソフトウェアが導入され、常に最新の状態が保たれているとともに、自動検査機能が有効**となっていること（**外部ネットワークから物理的に分離し、かつ、ＵＳＢメモリ等の外部記憶媒体からの感染防止対策が行われている場合**その他不正プログラムの侵入を防ぐ措置が講じられている場合はこの限りではない）

  ③ **セキュリティ更新プログラムの提供等のサポートが終了したオペレーティングシステム（ＯＳ）が使用されていない**こと（**外部ネットワークから物理的に分離し、かつ、ＵＳＢメモリ等の外部記憶媒体からの感染防止対策が行われている場合**その他不正プログラムの侵入を防ぐ措置が講じられている場合はこの限りではない）

  ④ 電子計算機は、障壁、施錠等により**他の区域から隔離**され、**人の入退出を管理することができる場所に設置**すること。可搬性のある電子計算機（モバイルパソコン、携帯端末等）についてはこの限りではないが、施錠できる保管庫で保管すること、常に携帯すること等、盗難等のおそれがないよう適切に管理すること

水道施設の技術的基準（サイバーセキュリティ）（2）

国土交通省

① 電子計算機へアクセスする者について**主体認証を行うことができる機能を有する**こと

④ 電子計算機は、障壁、施錠等により**他の区域から隔離**され、**人の入退出を管理することができる場所に設置**すること。可搬性のある電子計算機（モバイルパソコン、携帯端末等）についてはこの限りではないが、施錠できる保管庫で保管すること、常に携帯すること等、盗難等のおそれがないよう適切に管理すること

- ①と④は、**電子計算機へのアクセスについてのセキュリティ対策**を求めたもの
- **①で、電子計算機にアクセスできる者を識別**できるよう、パスワード等の主体認証情報を用いることができるになっていることに加え、**④で、そもそも電子計算機に物理的にアクセスできる者を管理・制限**していること（持ち運びできる電子計算機については、盗難等のおそれのないこと）を求めている
- ①と④の対策を併せて講じることにより、**アクセスすることを認められた特定の者以外の者が電子計算機に物理的に近づくことや、電子計算機にアクセスして不正な行為等をすることが防止**され、セキュリティ対策が強化される
- ④において入退室管理等をしていることをもって、①の代替措置とすることはできないことに留意のこと。**①は**、④とは異なって、電気計算機にアクセスすることの認められていない者が物理的にアクセスできないようにすることを求めているのではなく、万一、**電子計算機まで物理的にアクセスすることができてしまった場合においても対応できるようになっているか**否かを問うものである

水道施設の技術的基準（サイバーセキュリティ）（3）

国土交通省

② 不正プログラム対策として、**アンチウイルスソフトウェアが導入され、常に最新の状態が保たれているとともに、自動検査機能が有効**となっていること（**外部ネットワークから物理的に分離し、かつ、ＵＳＢメモリ等の外部記憶媒体からの感染防止対策が行われている場合**その他不正プログラムの侵入を防ぐ措置が講じられている場合はこの限りではない）

③ **セキュリティ更新プログラムの提供等のサポートが終了したオペレーティングシステム（ＯＳ）が使用されていない**こと（**外部ネットワークから物理的に分離し、かつ、ＵＳＢメモリ等の外部記憶媒体からの感染防止対策が行われている場合**その他不正プログラムの侵入を防ぐ措置が講じられている場合はこの限りではない）

- ②と③ではいずれも、**代替措置**を括弧書きで併記
- 代替措置とはすなわち、「**外部ネットワークから物理的に分離し、『かつ』、ＵＳＢメモリ等の外部記憶媒体からの感染防止対策が行われている場合**」（※「かつ」の前後いずれかではなく、前後両者を実施している場合）**等、不正プログラムの侵入を防ぐ措置**が講じられている場合
- 外部ネットワークから分離をしているのみでは、制御システムのある中央監視室に内部侵入され、不正プログラムの入ったUSBメモリ等を電子計算機に接続されて不正プログラム感染や不正侵入等を受けるといったことを防ぎきれず、不十分
- アンチウイルスソフトが有効に機能するにはウイルス定義ファイルの定期的な更新が欠かせない。閉域網下でウイルス定義ファイルを更新するためには、USBメモリを挿入したり、一時的にインターネットに接続したりすることが必要となるが、**USBメモリからデータを読み取ったり、インターネットに接続したりすること自体がリスクを孕んだ行為**であることに留意が必要
- そうするよりも、**外部ネットワークから分離し、かつ、USB等の外部記憶媒体のポートを無効化して常時使えないようにする**（物理的に一切挿し込めないようにすることを含む。USBを使用しないよう周知しているのみで挿し込めば使用できる場合は不可）方が、安全な環境と考えられる

3. 組織統治におけるサイバーセキュリティ（1）

ガイドラインの記載内容

【組織方針とサイバーセキュリティ】

✓ **リスクを許容水準まで低減**することは、水道事業者等として果たすべき**社会的責任**であり、その実践は**経営層としての責務**である

【経営リスクとしてのサイバーセキュリティリスクの管理】

✓ 組織内のガバナンスや内部統制、その他の**リスクマネジメントにおけるコミュニケーションの一部として**、サイバーセキュリティに関する環境変化、インシデントの発生状況・得られた教訓、セキュリティ対策の実施状況・有効性評価等に関し、経営層と担当者層との間で定期的な対話の機会等を設ける

組織方針とサイバーセキュリティ

事業者へ求めること

経営層は、組織方針（経営方針・リスクマネジメント方針等）にあたる文書に、重要インフラのサイバーセキュリティ確保に関する事項も組み入れ、あわせて維持するサービス範囲・水準を示すことが望ましい

組織方針に組み入れる事項の例

- ❒ 日々進化するサイバー攻撃に備え、多層防御の継続的強化の実施
- ❒ サイバー攻撃の結果、生産活動やサービス提供に影響が生じるリスクを考慮し、サイバーセキュリティ推進体制を構築

経営方針等への記載例

- ❒ 経営方針等にサイバーセキュリティ確保に関する事項として「日々進化するサイバー攻撃に備え、多層防御の継続的強化の実施」等を記載し、そのKPI（重要業績評価指標）として「システム障害によるサービス停止からサービス復旧までの時間○○時間以内」等を記載する

経営層の会議等においてサイバーセキュリティリスクを取り扱い、適切にリスク管理することを経営方針等に明記する

経営リスクとしてのサイバーセキュリティリスクの管理

事業者へ求めること

組織内におけるその他の経営リスク管理体制と整合をとり、サイバーセキュリティに関する責任及び権限（次スライド参照）を明確にした上で、リスク管理体制を構築する

サイバーセキュリティリスク管理の例

- ❒ CISO*等が、組織内に設置された経営リスクに関する委員会に参加する
- ❒ 取締役、監査役はサイバーセキュリティリスク管理体制が適切に構築・運用されているかを監査する
- ❒ 内部統制の観点から、サイバーセキュリティ対策の有効性や信頼性確保等の目的達成を保証するための役割を体制内で明確化する

*最高情報セキュリティ責任者（Chief Information Security Officer）

リスク管理の一つとして、セキュリティ対策を推進する最終決定権をもつ責任者。役員クラスが相当

サイバーセキュリティリスクも経営リスクの一つであるという考え方

3. 組織統治におけるサイバーセキュリティ（2）

ガイドラインの記載内容

【責任及び権限の割当て】

✓ 全ての者が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることでサイバーセキュリティは実現される。そのため、それらの**権限と責務を明確**にし、**必要となる組織・体制を確立**することが望ましい

✓ 特に、**サイバーセキュリティ責任者や最高情報セキュリティ責任者（CISO）を任命すべき**である

【情報開示】

✓ 組織の情報開示の体制において、**サイバーセキュリティに関する取組も可能な範囲で開示**することは、ステークホルダーの信頼・安心感の醸成に繋がる

責任及び権限の割当て

事業者へ求めること

サイバーセキュリティリスクの管理について、担当する部署及び従業員を決定するとともに、役割及び権限を割り当てる。サイバーセキュリティを確立するためには、兼務してはいけない役割が存在する（「承認・許可事案の申請者とその承認者・許可者」や「監査を受ける者とその監査を実施する者」等）

設置する組織の例

- ❒ 情報セキュリティ委員会
  （セキュリティに関する自組織の関連事項を整理し、役員へ定期的に報告する会議体）
- ❒ CSIRT：Computer Security Incident Response Team
  （セキュリティインシデントが発生した際に対応するチーム。システム復旧だけでなく、社内調整、広報業務、組織外との情報共有などが主な役割となる）

割り当てる役割の例

- ❒ 脅威情報等の収集*及び関係主体との情報共有担当
- ❒ 事業継続計画の実行担当

*脆弱性情報やサイバー攻撃集団の活動認知

情報開示

事業者へ求めること

経営層には、平時におけるサイバーセキュリティ確保の取組に対する姿勢や、インシデント発生時の対応に関する情報の開示に取り組むことが望まれる。ただし、開示する情報に際しては、機密情報推測のリスクなどを踏まえ、経営判断に委ねるべきであることに留意する

開示することが望ましいサイバーセキュリティに関する情報

- ❒ 組織方針・サイバーセキュリティ方針
- ❒ インシデントの発生状況及び対応状況
- ❒ 維持するサービス範囲・水準（前スライド参照）
- ❒ リスク管理体制
- ❒ セキュリティ対策に必要な資源の確保（予算・人材等）

3. 組織統治におけるサイバーセキュリティ（3）

ガイドラインの記載内容

【資源の確保】

✓ 必要な予算・体制・人材等の**経営資源を継続的に確保**し、**リスクを考慮して適切に配分**すること

✓ 十分な資源の確保が難しい場合には、中小企業向けのサイバーセキュリティ対策の導入・運用の支援を目的とした、**サイバーセキュリティお助け隊サービス制度*等の活用を検討**する

*https://www.ipa.go.jp/security/sme/otasuketai-about.html

【監査・モニタリング】

✓ サイバーセキュリティは、事業継続を念頭に置いた全社的なリスクマネジメントの一部であることを踏まえ、**リスクマネジメントとセキュリティ対策が整合する取組となるように留意**する

✓ **内部監査人による定期的な監査を実施**する。実施に当たっては**必要に応じて、外部の専門知識を有する者の支援を受けて状況確認**をする

セキュリティ対策の監査の実施例

<サイバーセキュリティ確保の取組全般に対する内部監査担当者>
- 監査の基本的な方針として、年度情報セキュリティ監査計画を整備
- 監査実施計画を立案し、監査を実施。実際の運用がサイバーセキュリティ関係規程に準拠しているかを確認
- 監査結果については、報告書として文書化

<最高情報セキュリティ責任者>
- 報告書の内容を踏まえ、指摘事項に対する改善計画の策定等をサイバーセキュリティ責任者に指示

<サイバーセキュリティ責任者*>
- 必要な措置を行った上で改善計画を策定
- 措置結果及び改善計画を最高情報セキュリティ責任者に報告

*セキュリティ管理策の運用が可能となる組織のまとまり毎の取りまとめの責任者。組織のまとまりの単位が水道局である場合は局長クラス、浄水場単位である場合は場長クラスが相当するが、組織の実態に合わせて、また、意思決定プロセスや役職においてより上位である最高情報セキュリティ責任者（CISO）の役職を踏まえて、役職のレベルを設定すること

✓ 経営層は、監査の結果等により、目標未達や進捗遅延、セキュリティ管理策の**要改善点等が確認された場合は、改善指示を行う**

✓ これらを**繰り返し実施し、サイバーセキュリティの取組の効果を高める**

4. リスクマネジメントの活用と危機管理（1）

ガイドラインの記載内容

【組織状況の理解】

- ✓ 組織状況の理解はリスクマネジメントの中で非常に重要である
- ✓ **水道サービスの特性を理解**するとともに、以下に例示する、サイバーセキュリティ対処態勢の実態把握を行うのが望ましい
  - **自組織が果たすべき役割・機能**と、それを踏まえて**維持・継続することが必要なサービス**
  - 最低限提供する**サービスの範囲・水準**
  - サービス提供を維持するために**必要な業務や経営資源**

内部状況・外部状況の理解

事業者へ求めること

以下に例示する内部・外部の状況及び特性を理解する

内部状況の例

- ❒ 組織体制、経営戦略、セキュリティ方針
- ❒ リスクマネジメント戦略、リスク許容度
- ❒ 水道サービス等に係る各種システム、データ
- ❒ セキュリティ投資が可能な資源状況
- ❒ リスク分析や対応に必要な技術や人的資源
- ❒ セキュリティリスクに対する、部署や立場による認識の差異
- ❒ 従業員のセキュリティリテラシー

外部状況の例

- ❒ 関連する法令の改正状況（事業法、個人情報保護法等）
- ❒ 所管省庁や規制当局における基準の策定、改正状況
- ❒ 関連団体における基準やガイドラインの策定、改正状況
- ❒ 重要インフラサービスの利用者に与える影響
- ❒ 国内外におけるセキュリティインシデントの発生事例や、その報道等による社会からのセキュリティ認識の広まり
- ❒ 外部取引先との契約における、セキュリティに関する要求事項
- ❒ 任務保証を達成するために必要な他の重要インフラサービス
- ❒ 自組織と他組織の相互依存関係

重要インフラサービス継続に係る特性の理解

事業者へ求めること

内部状況及び外部状況を踏まえ、以下に例示するような自組織の重要インフラサービス継続に係る特性を理解する

重要インフラサービス継続に係る特性

- ❒ 水道サービス等の停止が経済社会に与える影響
- ❒ サービス継続に係る重要なシステムや機能
- ❒ 重要なシステムや機能を支える業務
- ❒ 業務を支える資源及び知識（予算、人員、設備、技術、資産の脆弱性情報）
- ❒ 他の重要インフラとの相互依存関係
- ❒ 水道サービス等の障害時における、復旧までの許容可能な時間
- ❒ 水道に関わる各種システムの特性

水道事業者等の役割

- ● システムの不具合等に関する情報について、必要に応じて所属するセプター内で共有するとともに、重要インフラ所管省庁への連絡を行う。なお、被害にあった場合は、自主的な判断により事案対処省庁への通報を行う
- ● 特に経営層は、平時及び緊急時のいずれにおいてもサイバーセキュリティ対策を実施するために、平時から組織内外の関係者とサイバーセキュリティリスクや対策に関する気づきや課題の共有等のコミュニケーションを積極的に行う

4. リスクマネジメントの活用と危機管理（2）

ガイドラインの記載内容

【リスクアセスメントの実施】

✓ 組織の状況と資産を踏まえ、**任務保証の考え方に基づくリスクアセスメント**を実施する

✓ **制御システムについても適切にリスクアセスメント**を実施する

【目標とする将来像の設定】

✓ リスクアセスメントの結果や、自組織の目標、組織の状況、ステークホルダーからの要求事項等を踏まえ、**目標とする将来像を決定**する

リスクアセスメントの実施

事業者へ求めること

組織状況や特性（前スライド参照）を踏まえ、重要インフラサービスの提供に影響を与えるセキュリティリスクを適切に管理すべく、リスクアセスメントを実施する（次スライド参照）。個々のサイバーセキュリティリスクに対し、「サービス・業務への影響度」や「事象の発生頻度」等を踏まえて、「低減」、「回避」、「移転」、「保有」の対応を選択する

リスクアセスメントを踏まえた対応の選択

- ❒ 低減：リスクの発生確率を下げる対策
  （重要な情報へのアクセス制御、多要素認証）
- ❒ 回避：リスクの発生可能性を除去する対策
  （情報漏洩回避策として、個人所有端末へのデータ保存禁止）
- ❒ 移転：リスクを他者に移す対策
  （クラウドサービスの利用、サイバー保険への加入）
- ❒ 保有：リスクを把握しながら具体的な対策を取らない

重要インフラサービスの提供に制御システムが使用されている場合には、制御システムについてもリスクアセスメントを実施する
（例）
一般的に、制御システムは可用性（安全、安定稼働）が最優先される。パッチ適用やバージョンアップ、暗号化などのリスク低減策の実施が、制御システムの安定稼働に影響を与えると判断できる場合には、ログや通信の監視等の代替策の実施によりリスク低減を図る

目標とする将来像の決定

事業者へ求めること

リスクアセスメントの結果等を踏まえ、サイバーセキュリティ確保のための目標とする将来像を決定する。現状把握（前スライド参照）と同様に、サイバーセキュリティに関する成熟度を参考とし、自組織が目指すべきサイバーセキュリティ対処態勢を定める

目標とする将来像の例

- ❒ 重大なインシデント発生時に、○○時間以内に経営層までエスカレーションされること
- ❒ 資産管理を行い、脆弱性を把握し、適切な脆弱性管理を行うこと
- ❒ セキュリティ委員会を常設、定期開催することとし、必ずCISOが参加すること

◆目標とする将来像の考え方における留意点

成熟度をはかる上での参考文書（前スライド）では、様々なセキュリティ管理策が示されているが、幅広く対応することを目的とするのではなく、組織の特性を踏まえて必要な対応を選択することが重要である

（例）

✓ 従業員が多く、異動等による入れ替わりも多いため、アカウント管理、アクセス制御の定期的な見直しや人的対策を重視する

✓ 一部の重要サービスについては、運用をグループ組織に委託しているため、脆弱性管理は行わないこととするが、情報共有窓口を明確にして、有事の際の迅速なエスカレーションを重視する

4. リスクマネジメントの活用と危機管理（3）

ガイドラインの記載内容

✓ 具体的なプロセスについては、NISC「機能保証のためのリスクアセスメント・ガイドライン 1.0 版」等を参考にしながら、リスクの特性に応じたリスク分析手法によってリスクを評価する

リスクアセスメントプロセス	
①リスクアセスメントの対象の特定	絶えず変化する自組織を取り巻く状況及び関係主体等のニーズを踏まえ、重要インフラサービスの提供に必要な業務の範囲・水準等を明らかにするとともに、当該業務の遂行に必要な情報システム等の経営資源を特定する。また、その過程で自組織のリスクに対する態度・リスク許容度を分析する
②リスク特定	情報システム等の経営資源に対する「サイバーセキュリティリスク」を特定する
③リスク分析	リスクに対する態度・リスク許容度等を考慮しつつ、「事象の結果によるサービス・業務への影響度合い」や「事象の発生可能性」等を評価軸として策定されるリスク基準を活用して、特定されたリスクの大きさを確認する。重要インフラサービスの継続提供を不確かなものとするシナリオを作成し、リスク分析を実施することが望ましい。重要インフラサービスの継続的提供を不確かなものとするリスクとしては、自然災害、管理不良、サイバー攻撃や、重要インフラを取り巻く環境変化、感染症やテロ・戦争、システム障害、労災・事故、内部不正等があり、リスクの特性に応じたリスク分析手法を選択する
④リスク評価	基準値以上の大きさのリスクを抽出するとともに、個別事情も考慮してリスク対応の対象とするリスクを抽出する

✓ 抽出したサイバーセキュリティリスクに対し、「サービス・業務への影響度」や「事象の発生頻度」等を踏まえて、「低減」、「回避」、「移転（共有）」、「保有（需要）」のいずれかの具体的な対応を決定する

4. リスクマネジメントの活用と危機管理（4）

ガイドラインの記載内容

【サイバーセキュリティリスク対応】

- ✓ 環境変化や日々のセキュリティ対策の運用状況に応じて適宜見直さなければ、新たな脅威に対応できない。そのため、**セキュリティ対策の運用においてリスクアセスメント**を行う必要がある
- ✓ **システム運用中**も、サイバー攻撃に関する新たな脅威の発生等の環境変化に応じて適宜リスクアセスメントを実施し、**本来あるべき状況や要件を検討・目標とする将来像を決定**することが重要

サイバーセキュリティリスク対応

事業者へ求めること

目標とする将来像と現状の実態とのギャップを埋めるためのセキュリティ管理策を検討し、優先順位付けを行う

個別方針の策定

❒ 実施すべきセキュリティ管理策について、遵守すべき行為や判断等の基準を個別方針（アクセス制御方針、情報分類方針等）としてとりまとめ、関係者へ伝達する

リスク対応計画の策定

❒ とりまとめた個別方針に基づき、サイバーセキュリティの達成目標を定めて、ロードマップ及び詳細化したリスク対応計画を作成し、サイバーセキュリティに係る取組を進める

リスク対応計画に記載することが望ましい項目
- ✓ 目標とする将来像
- ✓ 実施事項
- ✓ 必要な資源（予算、人員）
- ✓ 責任者（策定した方針の実行責任者）
- ✓ 達成期限
- ✓ 結果の評価方法

現状

目標とする将来像

現状のサイバーセキュリティ対処態勢の実態の例

- ❒ 情報システム部の課長がセキュリティ対策に関する責任者を兼任している
- ❒ 従業員が業務上便利だからとクラウドサービスを自由に利用している
- ❒ 標的型メール訓練を行ったときに、ダミーのメールを開いてしまった従業員の割合が20%で報告率が40%である
- ❒ 前の部署で使用していた業務フォルダに、今でもアクセスすることがある

現状に対して、目標とする将来像の設定の例

- ❒ 専任でCISOを任命し、定期的な経営会議においてサイバーセキュリティを付議する
- ❒ 情報資産を棚卸し、定期的に見直し、シャドーIT*を防止する
- ❒ 標的型メール訓練を行ったときのダミーメール開封率5%、報告率100%を目標とする
- ❒ 人事異動や退職時に、不要なアクセス権を適切に削除するよう、アカウント管理、アクセス制御ポリシーの運用体制を整備する

*企業・組織側が把握せずに従業員または部門が業務に利用しているデバイスやクラウドサービスなどの情報技術

サイバーセキュリティに係る取組が自らのサイバーセキュリティに限らない**既存の各種計画等と整合的なものになるようにする**とともに、監査やリスクアセスメント等の**個々の取組を既存の計画等の中に位置付けたり、紐付けたりする**ことを通じて、**サイバーセキュリティに係る取組が持続可能なものとなるように留意**すること

4. リスクマネジメントの活用と危機管理（5）

ガイドラインの記載内容

【サプライチェーンリスクマネジメント】

✓ 直接の供給者を対象に、**事業者間の契約において、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化**する

【情報共有】

✓ **サイバー攻撃被害とその被害に関連する情報**、その他の重要インフラ事業者等に影響を及ぼすおそれのある**システム不具合に関する情報等**を**関係主体と共有すること**が望ましい

サプライチェーンリスクマネジメント

事業者へ求めること

法務部等と連携し、条項を検討の上、供給者との契約に含めることが望ましい

サプライヤーへの要求事項、仕様書の記載例

❒ 委託先のサプライチェーン・リスクに係る管理体制が適切であることを確認するために必要な情報を、委託先に提示させる

（仕様書の記載例）
受注者は、資本関係・役員の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報を提示すること

❒ サプライチェーン・リスクに係るセキュリティインシデントを認知した場合に、委託先の作業プロセス又は成果物を立入検査等で確認する

（仕様書の記載例）
再委託を行う場合は、再委託先において意図せざる変更が加えられないための管理体制について発注者の確認（立入調査）を随時受け入れること

代表的なサプライチェーンに係る脅威への対策も検討する
（例）
✓ 委託先の管理不良による機密情報の意図しない公開
（対策例：機密情報への厳格なアクセス制御の徹底）
✓ 成熟度の高くないグループ組織や取引先を経由したサイバー攻撃
（対策例：なりすましを防ぐための多要素認証の仕組みの導入）

情報共有

事業者へ求めること

情報共有の取組については、「重要インフラのサイバーセキュリティに係る行動計画」に従って実施するものとする。具体的には、「行動計画に基づく手引書」を参照し、実施すること（次スライド参照）

国土交通省への情報連絡を要するケース

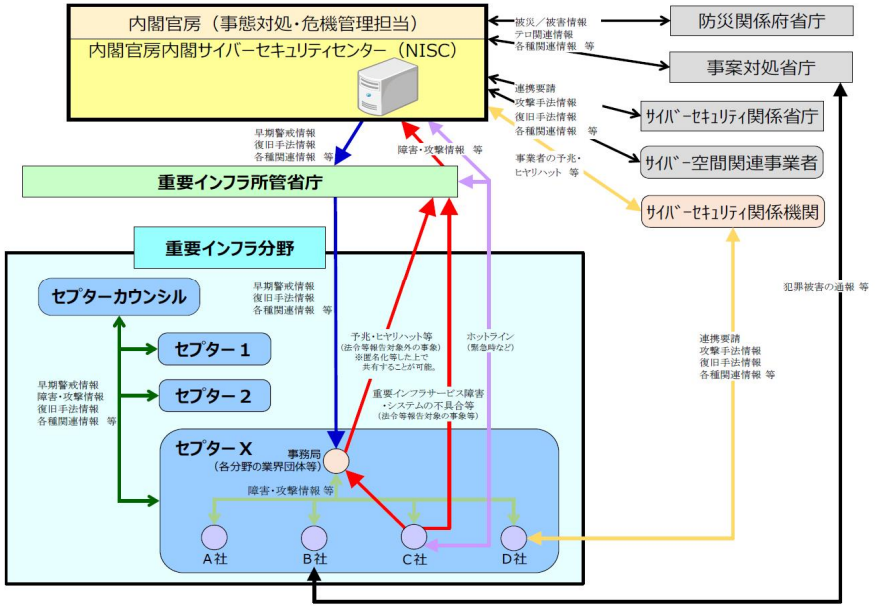
❒ 法令等で国土交通省への報告が義務付けられている場合
❒ 国民生活や重要インフラサービスに深刻な影響があると判断され、重要インフラ事業者等が情報共有を行うことが適切と判断した場合
❒ 上記に該当するかどうか不明な場合については、国土交通省に相談することが望ましい

予兆・ヒヤリハットや法令等で報告が義務付けられていない事象を国土交通省に報告することで、政府機関からの指導等に繋がるのではないかといった懸念を払拭できず、情報共有の活性化を阻害する一因ともなっていたと考えられることから、重要インフラ事業者等が国土交通省に直接報告する形態に加え、法令等で報告が義務付けられていない事象については、セプター事務局経由で情報連絡元の匿名化等を行った上で国土交通省に報告することも可能としている

4. リスクマネジメントの活用と危機管理（6）

「重要インフラのサイバーセキュリティに係る行動計画」に基づく情報共有手引書より抜粋

別紙４－２　情報共有体制(大規模重要インフラサービス障害対応時)

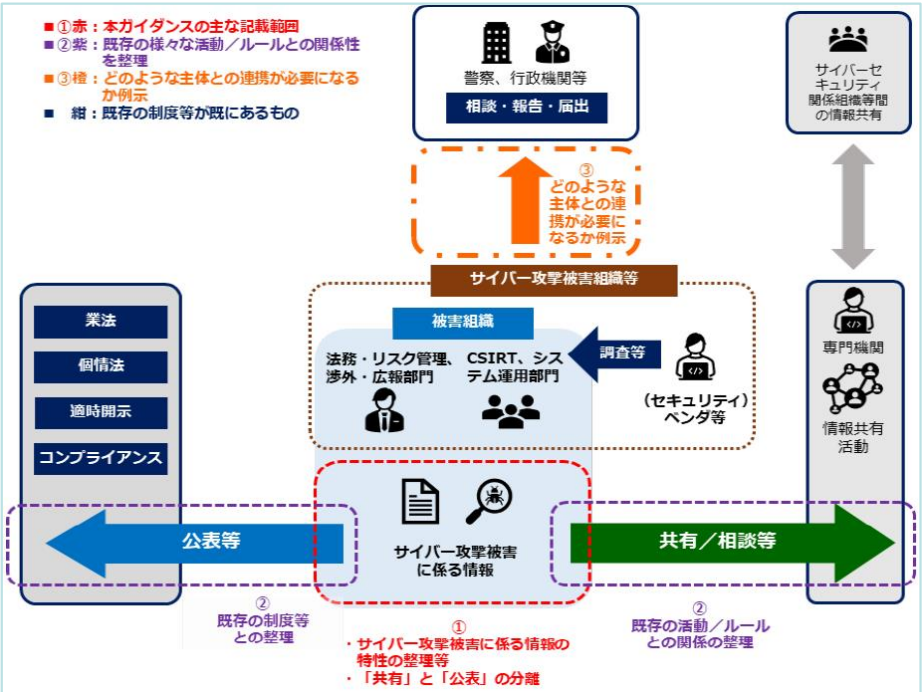


別紙４－３　情報共有体制における各関係主体の役割

関係主体	通常時における各関係主体の役割	大規模重要インフラサービス障害対応時における[注]各関係主体の役割
○ 内閣官房（事態対処・危機管理担当）	重要インフラに関連する事案の情報につき、ＮＩＳＣと相互に情報の共有を行う。	通常時の役割に加え、ＮＩＳＣと一体化し、事案対処省庁及び防災関係府省庁から提供される被害情報、対応状況情報等を集約し、ＮＩＳＣと相互に情報の共有を行う。
○ 内閣官房（ＮＩＳＣ）	重要インフラ所管省庁、サイバーセキュリティ関係省庁、事案対処省庁、防災関係府省庁、サイバーセキュリティ関係機関及びサイバー空間関連事業者等と相互にシステムの不具合等に関する情報の共有を行う。	内閣官房（事態対処・危機管理担当）と一体化し、重要インフラ所管省庁、サイバーセキュリティ関係省庁、事案対処省庁、防災関係府省庁、サイバーセキュリティ関係機関及びサイバー空間関連事業者等と相互にシステムの不具合等に関する情報の共有を行う。
○ 重要インフラ所管省庁	所管する重要インフラ事業者等から受領したシステムの不具合等に関する情報をＮＩＳＣ及び必要に応じ該当するセプターに連絡する。ＮＩＳＣから受領したシステムの不具合等に関する情報を該当するセプターに提供する。	通常時の役割に加え、必要に応じて大規模重要インフラサービス障害対応時の体制に協力する。
○ セプターカウンシル	セプターカウンシルは、政府機関を含め他の機関の下位に位置付けられるものでなく独立した会議体であり、各セプターの主体的な判断により連携するものである。 主体的な判断により各セプターが積極的に参画し、重要インフラ事業者等におけるサービスの維持・復旧に向けた幅広い情報共有を行う。	通常時の役割に加え、必要に応じて大規模重要インフラサービス障害対応のための体制を構築し、セプター間をはじめとした関係機関との連携を図る。
○ セプター事務局	重要インフラ所管省庁、事案対処省庁、防災関係府省庁、サイバーセキュリティ関係機関、セプターカウンシル及び重要インフラ事業者等と連携し、相互にシステムの不具合等に関する情報の共有を行う。	通常時の役割に加え、必要に応じて大規模重要インフラサービス障害対応のための体制を構築し、内閣官房をはじめとした関係機関との連携を図る。
○ 重要インフラ事業者等	システムの不具合等に関する情報について、必要に応じて所属するセプター内で共有するとともに、「別添：情報連絡・情報提供について」に基づき重要インフラ所管省庁への連絡を行う。なお、犯罪被害にあった場合は、自主的な判断により事案対処省庁への通報を行う。	通常時の役割に加え、必要に応じて大規模重要インフラサービス障害対応のための体制を構築し、内閣官房をはじめとした関係機関との連携を図る。

注　災害やテロ等に起因する大規模重要インフラサービス障害が発生した場合、当該緊急事態における情報の集約及び共有として、「緊急事態に対する政府の初動対処体制について」（平成15年11月21日閣議決定）に基づき、関係府省庁間で情報を集約及び共有する。

サイバー攻撃被害に係る情報の共有・公表ガイダンスより抜粋



情報共有と被害公表における情報の種類のチェックリスト（簡易版）

	情報共有	被害公表
タイミング	可能な限り早期のタイミング	ケースバイケース ※二次被害発生のおそれなど注意喚起を目的とする速報が必要な場合はただちに公表
被害内容・対応情報 ・被害組織名 ・被害業種／規模 ・被害内容 ・対応のタイムライン	―	○
中間の情報 ・攻撃のタイムライン ・攻撃対象システムについて ・脆弱性悪用の情報等	△ ※共有に必要なものは専門機関への相談等を踏まえて共有することが望ましい	○
攻撃技術情報 ・マルウェア ・不正通信先 ・その他攻撃手法に関する情報	○	△

○：主な内容となる情報　　△：内容／状況による　　―：基本的に対象外

4. リスクマネジメントの活用と危機管理（7）

ガイドラインの記載内容

【人材育成・意識啓発】

✓ **「サイバーセキュリティは全員参加（Cybersecurity for All）」**との考え方の下、全ての従業員がサイバーセキュリティの内規等への理解を深め、また、部署・役職に応じて必要な水準のサイバーセキュリティに関する能力を確保できるよう、**人材育成・意識啓発**を行う

【CSIRT等の整備】

✓ **CSIRT（または同等の機能をもつ組織）を重要インフラ事業者等内に整備し、役割分担や対応手順等について、あらかじめ関連部門と合意しておく**ことが重要である

人材育成・意識啓発

事業者へ求めること

以下に例示する事項を実施することが望ましい

人材育成において実施することが望ましい具体例

- ❒ 組織の全ての従業員を対象としたトレーニングを年1回以上実施する。フィッシング、ビジネスメール詐欺、パスワードセキュリティなど基本的な概念を網羅し、組織内での文化醸成に努める
- ❒ セキュリティ対策が不十分であった場合の影響例を示すなど、セキュリティ対策の重要性について啓発を行う
- ❒ セキュリティ対策業務に従事する人材に対する「情報処理安全確保支援士」等の資格取得の推進
- ❒ 制御システムに関するセキュリティ人材に対する、ICSCoE*による中核人材育成プログラムの活用の検討

*ICSCoE：IPA産業サイバーセキュリティセンター

CSIRT等の整備

事業者へ求めること

最高情報セキュリティ責任者は、セキュリティインシデントに備えた体制の整備を行うこと

具体例

- ❒ CSIRT等は、役割分担や対応手順を関連部門と合意する
- ❒ セキュリティインシデントに対処するための責任者としてCSIRT責任者を置くこと
- ❒ セキュリティインシデントが発生した際、直ちに報告が行われる体制を整備すること

制御システムを保有する場合には、制御システム関連部門とも連携できる体制を整備することが望ましい

4. リスクマネジメントの活用と危機管理（8）

ガイドラインの記載内容

【モニタリング及びレビュー】

- ✓ 取組むセキュリティ管理策について、モニタリング及び監査（または自己点検）を実施し、**継続的な見直し・改善を行う**
- ✓ 継続的に実施するため、**モニタリング及びレビューのプロセスを計画に組み込む**
- ✓ セキュリティ対策の自己点検は、取扱者が自ら実施すべき対策事項の確認だけではなく、**組織全体のセキュリティ水準の確認**という目的もあることから、適切に実施することが重要
- ✓ **自己点検の結果を踏まえ**、各当事者は、それぞれの役割の責任範囲において、**必要となる改善策を実施**する必要がある

セキュリティ対策の自己点検の実施例

<サイバーセキュリティ責任者>：年度自己点検計画に基づき、取扱者に自己点検の実施を指示

↓

<取扱者>：サイバーセキュリティ責任者から指示された自己点検票及び自己点検の手順を用いて自己点検を実施

↓

<サイバーセキュリティ責任者>：結果の分析を行い、評価結果を**<最高情報セキュリティ責任者>**へ報告

↓

<最高情報セキュリティ責任者>：自己点検結果を全体として評価し、自己点検の結果により明らかになった問題点について、**<サイバーセキュリティ責任者>**に改善を指示し、改善結果の報告を受ける

↓

自己点検の結果は、サイバーセキュリティ関係規程やサイバーセキュリティ確保のための取組の更新に活用する

- ✓ 実施計画は、以下の各項目を含むことが望ましい
  - 実施頻度、実施時期、確認及び評価の方法、実施項目

5. 対策項目（組織的対策）

ガイドラインの記載内容

【マルウェアからの保護】

✓ **マルウェアに感染した情報システム**は、他への情報システムの再感染を引き起こす可能性のほか、迷惑メールの送信やサービス不能攻撃等の踏み台として利用される危険性等、**他者に対するセキュリティ脅威の原因となり得る**。このため、**マルウェア対策を行うことが重要**である

【バックアップ】

✓ 緊急事態発生時には、通常業務に**必要なデータの欠落や不整合による障害**が発生するおそれがある。これらを防ぐための**詳細な復帰計画をあらかじめ策定**しておくことが重要である

マルウェアからの保護

事業者へ求めること

システム管理者は、マルウェア感染の回避を目的とし、以下の留意事項を含む日常的実施事項を定めることが望まれる

マルウェア対策における具体例

- ❒ マルウェアに関する情報の収集に努める。特段の対処が必要な場合には、対処の実施に関する指示を行うこと
- ❒ 速やかなパッチ適用による脆弱性対策を講じること
- ❒ サーバ装置、端末及び想定されるマルウェアの感染経路に対するマルウェア対策ソフトウェア等の導入
- ❒ マクロ等の埋め込みコードの実行を既定で無効とする。業務においてコードを実行する必要がある場合、許可されたユーザが特定の状況で実行できることを承認する仕組みを構築すること
- ❒ ネットワークセグメントの分割、IPS/プロキシサーバ、EDR*等を導入すること
- ❒ ベンダーなどとの関係者との協力関係の構築
- ❒ 攻撃が発覚した際には所管省庁や警察へ連絡し、逐次時系列で状況を保存できる体制構築

*Endpoint Detection and Response
PCやサーバといったエンドポイント（端末）におけるインシデント発生後の対応を、明確化・迅速化する機能を持つセキュリティ製品

バックアップ

事業者へ求めること

必要な情報のバックアップを取得し、バックアップ元と先が同時に被災しないように保存する

バックアップにおいて考慮することが望まれる具体例

- ❒ バックアップ稼働・切り替え計画、復帰計画の策定
- ❒ バックアップを保存する媒体の種類
- ❒ バックアップの頻度、世代管理の方法
- ❒ 使用するバックアップツール
- ❒ 定期的なバックアップリカバリー検査の実施
- ❒ 運用に必要なシステムについて、年1回以上の定期的なバックアップを実施

5. 対策項目（人的／物理的対策）

ガイドラインの記載内容

【リモートアクセス管理】

✓ リスクを踏まえ、**リモートアクセス環境導入に関する対策基準**を定める必要がある

【セキュリティ確保が求められる領域】

✓ 情報処理設備を含む領域を保護するために、**セキュリティ境界を明確に定め**、**適切な入退管理策**によって**セキュリティの保たれた領域（要管理対策区域）を保護**することが望ましい

リモートアクセス環境（人的対策）

事業者へ求めること

システム管理者は、リモートアクセス環境をテレワークに適用する場合には、以降の事項を含む対策を講ずることが望ましい

具体例

❒ リモートアクセス元で利用する無線LANルータ等の機器について、ファームウェアを最新版にするよう周知する

❒ 無線LANルータ等の機器を利用する場合は、適切なセキュリティ方式（WPA2、WPA3等）や第三者に推測されにくいパスワードを利用するよう周知する

❒ 以下に例示するトピックについて方針を定め、従業員が遠隔作業している場合のセキュリティ対策を実施すること

- リモートアクセスの申請手続の整備
- 通信内容の暗号化
- 主体認証ログの取得及び管理
- リモートワイプ*の仕組みの導入

*パソコンやモバイル機器等の端末の、紛失や盗難の際に、遠隔操作で端末内のデータを全て消去すること

セキュリティ確保が求められる領域（物理的対策）

事業者へ求めること

セキュリティの保たれた領域（要管理対策区域）に、以下に例示する対策を講ずることが望ましい

職員の入退室管理

❒ 要管理対策区域への全ての者の入退出を記録・管理し、立入りは業務上必要な者に限定すること
（例：入室・退室共にIDカード等による認証を行い、時刻を記録）

❒ 立入りに際しては、本人認証や責任者による事前承認などの管理を実施すること
（例：生体認証等の信頼度の高い本人確認を行う）

❒ 立入りを許可された者については随時見直し、入室が不要となった者については、速やかに登録許可を解除すること
（例：異動、退職により入室が不要となった者の登録削除）

訪問者及び受渡業者の管理

❒ 許可されていない者の入室手続きを定めること
（例：従業員が必ず帯同すること）

❒ 情報システムに関連する機器の要管理対策区域への持込み及び要管理対策区域からの持出には、システム管理者の承認を求めること

❒ 情報システムに関連する機器の不正な持ち出しが行われていないかを確認するために定期的又は不定期に施設からの退出時に持ち物検査を行うこと

5. 対策項目（技術的対策）

ガイドラインの記載内容

【情報システム等のアクセス制御】

✓ どの主体がどの情報にアクセスすることが可能なのかを**情報毎にアクセス制御**する必要がある

✓ 全ての情報システムについて、**アクセス制御を行う必要性の有無を検討**して、アクセス制御を行う機能を設けることが重要である

【多層防御】

✓ 従来型の境界防御のみでは侵入を検知することが困難であるため、**複数の対策を組み合わせ、一つの対策で防御できなくても次の対策で防御または検知**するという考え方の下、セキュリティ対策を検討することが重要である

情報システム等のアクセス制御

事業者へ求めること

各重要システムについて、アクセス制御を行う必要性の有無を検討し、アクセス制御を行う機能を設けることが重要である

具体例

- ❒ 同一主体による複数アクセスの制限
- ❒ IP アドレスによる端末の制限
- ❒ ネットワークセグメントの分割によるアクセス制御
- ❒ 公開サーバなど、インターネット上の資産では、悪用可能なサービス（RDP、SSH、SMB* 等）を使用しない。また、インターネットに接続された情報資産では、不要なアプリケーションやネットワークプロトコルを全て無効化する
- ❒ 失敗したログインを記録し、複数回連続して失敗したログインについてはセキュリティ担当者に通知されるようにする。短時間に連続して失敗したログインについては、アカウントロックされるよう設定する

* RDP（Remote Desktop Protocol）
→ コンピュータをリモートで使用するための技術
SSH（Secure Shell）
→ コンピュータやネットワーク装置をリモートで使用するための技術
SMB（Server Massage Block）
→ 主にWindowsの環境で、ネットワークを介してファイル共有を行う技術

多層防御

事業者へ求めること

重要業務を行う端末、ネットワーク、システムまたはサービスには、多層防御を導入することが望ましい

入口対策

- ❒ 不要なサービスについて機能を削除又は停止する
- ❒ 不審なプログラムが実行されないよう設定する
- ❒ パーソナルファイアウォール等を用いて、サーバ装置及び端末に入力される通信及び出力される通信を必要最小限に制限する

内部対策

- ❒ 重要サーバについては、組織内ネットワークを複数セグメントに区切った上で、重要サーバ類専用のセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定する。また、インターネットに直接接続しない。
- ❒ 不要な管理者権限アカウントを削除する。
- ❒ 管理者権限アカウントのパスワードは、容易に推測できないものに設定する
- ❒ EDR等によるソフトウェアの挙動監視により未知のマルウェア等を検知する

5. 対策項目（その他）

ガイドラインの記載内容

【クラウドサービス】

✓ インターネットを介したサービス（クラウドサービス等）等、**新しい技術を利用する際には、国内外の法令や評価制度等の存在について留意**することが重要である

【委託先管理】

✓ 重要情報の漏えいや不正アクセス等のリスクは、自組織のみでリスク対応をしていても、外部委託先等を経由して間接的に顕在化するおそれがある。このことから、外部委託先に係る管理において、**委託先の適切な選定、責任分界点の明確化、重要インフラサービス障害発生時の対処態勢等を整備**する

クラウドサービス

事業者へ求めること

利用者が制御できない環境や領域が存在するクラウドサービスでは、クラウド事業者の作業によってインシデントが発生する場合がある。クラウド事業者が開示する情報の把握や変更管理などを適切に行うことが望ましい

クラウドサービスを利用する際の考慮事項 例

- ❒ 脆弱性対策の実施内容を確認できる
- ❒ 情報の暗号化が確認できる（保存データ及び通信回線の暗号化）
- ❒ 情報の確実な削除・廃棄が確認できる

クラウドサービス利用において、インシデント発生時に、関連するステークホルダーとの連携が行える体制を整備することが望ましい

（サイバー攻撃を検知した場合）

- ◘ 影響範囲に応じてシステムの停止も検討する
- ◘ 顧客、構築ベンダー、クラウド事業者の窓口への情報共有
- ◘ 監督官庁への報告

（脆弱性や設定不備の場合）

- ◘ クラウド事業者の最新のサポート（サービス）情報の確認する
- ◘ ゼロデイ攻撃のリスクがある新たな脆弱性の場合には、緩和策や回避策を確認し、組織内での対応を検討できる体制

委託先管理

事業者へ求めること

委託先の選定の際や、委託先への要求事項を整備する際、以下を参考とすること

業務委託（共通事項）

- ❒ セキュリティインシデント発生時の対処方法や体制報告
- ❒ 業務委託終了時の対策（情報が返却、破棄又は抹消されたことの確認等）
- ❒ 監査の受け入れやサービス品質の保証
- ❒ セキュリティ脅威に対処するための継続的なリスク評価

情報システムに関する業務委託

- ❒ 委託先に提供する情報を必要最低限とし、情報の格付けに従って、適切なセキュリティ管理策を講ずること
- ❒ 委託先によって情報システムに意図しない変更が加えられないための対策
- ❒ 情報システムの構築の段階や運用・保守の段階において、脆弱性の混入を防止するための対策

5. 対策項目(その他)・別紙1. 情報の取扱い・個人情報保護

✓ 令和６年７月、複数の水道事業者等からの委託を受けていた民間企業において、委託業務で保管していた水道や下水道の使用者に関する個人情報が流出した可能性があるとの発表があった
✓ 当該水道事業者等の中には、過年度の委託業務における情報が含まれ得るとするところもあり、委託終了時の情報の適切な廃棄等について委託業者に改めて確認するなどの管理徹底をすること

委託先管理（続き）

事業者へ求めること

使用者の個人情報を管理するための各種システムについて、外部からの不正アクセスに対するセキュリティ対策が適切に講じられているか、**委託業者に改めて確認するなどセキュリティ対策の管理徹底をする**こと。外部委託の実施に当たっては、以下の項目を含む外部委託契約を取り交わすこと

外部委託の実施における手続きの遵守

- ❒ 委託先に請け負わせる業務におけるセキュリティ対策
- ❒ **機密保持（情報の目的外利用の禁止、委託終了時の適切な廃棄等を含む）**
- ❒ 重要インフラサービス障害に対する対処手順
- ❒ セキュリティ対策の履行が不十分である場合の対処手順

委託先に適用するサイバーセキュリティ確保の仕組みの整備

- ❒ 委託先に提供する情報の委託先における目的外利用の禁止
- ❒ 委託業務における情報の適正な取扱いのためのセキュリティ管理策
- ❒ 委託先におけるセキュリティ管理策の実施内容及び管理体制
- ❒ 委託先企業またはその従業員、再委託先もしくは第三者による意図しない変更が加えられないための管理体制
- ❒ 委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（サイバーセキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供
- ❒ 委託先における重要インフラサービス障害に対する対処方法
- ❒ 委託先におけるセキュリティ管理策その他の契約の履行状況の確認方法
- ❒ 委託先におけるセキュリティ管理策の履行が不十分な場合の対処方法
- ❒ 情報セキュリティインシデント発生時の対処方法や報告体制
- ❒ 監査の受け入れやサービス品質の保証（取り扱う情報や業務内容等を勘案して必要な場合）
- ❒ セキュリティ脅威に対処するための継続的なリスク評価（取り扱う情報や業務内容等を勘案して必要な場合）
- ❒ **業務委託終了時の対策（情報が返却、破棄または抹消されたことの確認等）**

個人情報を委託する場合の対策

事業者へ求めること

サイバーセキュリティ責任者は、適切な委託先管理を実施するために、個人データの安全管理、取扱時の報告義務、責任の範囲及び非開示義務について、委託契約時に明確にすべき内容を規定すること

個人情報を委託する場合の対策

- ❒ 個人データの安全管理に関する事項
  - ● 個人データの漏えい等の防止、盗用の禁止に関する事項
  - ● 委託契約範囲外の加工、利用の禁止
  - ● 委託契約範囲外の複写、複製の禁止
  - ● 委託期間
  - ● **委託終了後の個人データの返還・消去・破棄に関する事項**
- ❒ 個人データの取扱いの再委託を行うに当たっての委託元への報告とその方法
- ❒ 個人データの取扱状況に関する委託者への報告の内容及び頻度
- ❒ 委託契約の内容、期間が遵守されていることの確認
- ❒ 委託契約の内容、期間が遵守されなかった場合の措置
- ❒ 個人データの漏えい等の事故が発生した場合の報告・連絡に関する事項
- ❒ 個人データの漏えい等の事故が発生した場合における委託元と委託先の責任の範囲

個人情報を委託する場合の委託先の監督

- ❒ 個人データの取扱いの全部または一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行うこと
- ❒ 委託する事業の規模及び性質並びに個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じる

主な用語集

※その他、【1.1.5「安全ガイドライン」における用語の定義】及び【7 専門用語集】参照

国土交通省

用語	定義
重要インフラ事業者等	サイバーセキュリティ基本法第12条第2項第3号に規定する重要社会基盤事業者等であり、具体的には、重要社会基盤事業者（重要インフラ事業者）及びその組織する団体並びに地方公共団体から構成される。
重要インフラサービス障害	システムの不具合により、重要インフラサービスの安全かつ持続的な提供に支障が生じることをいう。
重要インフラ利用者	重要インフラ事業者等が提供する重要インフラのサービスを利用する者をいう。
取扱者	重要インフラ事業者等が保有する重要インフラに関する情報システム及び情報資産を取り扱う重要インフラ事業関係者（情報資産や情報システムを直接扱う者を監督する立場にある者（経営層や幹部等）、委託先の関係者等を含む）をいう。
情報システム	ハードウェア及びソフトウェアから成るシステムであって、情報処理または通信の用に供するものをいう。サーバ装置、端末、通信回線装置、複合機、IoT機器を含む特定用途機器（フィールド機器や監視・制御システム等の制御システム等で使われるものを含む）、ソフトウェアが含まれる。
制御システム	水道インフラの重要システムを構成する機械や設備を制御する端末及び重要システム等とネットワークで接続されている機械や設備、その構成要素を指す。
情報資産	以下の2つの情報をいう。 • 取扱者が業務上使用することを目的として重要インフラ事業者等が調達し、または開発した情報システムもしくは外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む） • 重要インフラ事業者等が調達し、または開発した情報システムの設計もしくは運用管理に関する情報
任務保証	重要インフラ事業者等や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方をいう。
サプライチェーン	一般的には、取引先との間の受発注、資材の調達から在庫管理、製品の配送まで、いわば事業活動の川上から川下に至るまでのモノや情報の流れのこと。広義では海外拠点やグループ会社、関連団体も含まれる。これらに加えてさらに、ITにおけるサプライチェーンでは、製品の設計段階や、情報システム等の運用・保守・廃棄段階を含めてサプライチェーンと呼ばれることがある。
セプター	重要インフラ事業者等の情報共有・分析機能のこと。また、当該機能を担う組織のこと。重要インフラ毎に整備される。水道分野のセプターの事務局は、公益社団法人日本水道協会が担っている。Capability for Engineering of Protection, Technical Operation, Analysis and Responseの略称(CEPTOAR)。
セプターカウンシル	各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。政府機関を含む他の機関の下位に位置付けられるものではなく、独立した会議体。
IT-BCP	重要インフラサービスの提供に必要な情報システムに関する事業継続計画（関連マニュアル類を含む）。IT（Information Technology）は情報技術。BCP（Business Continuity Plan）は事業継続計画のことであり、企業等のリスクマネジメントの一部であり、災害や情報システムのトラブルに対して事業を形成する業務プロセスや資産を的確に守るための計画のことを指す。
コンティンジェンシープラン	重要インフラ事業者等が重要インフラサービス障害の発生またはそのおそれがあることを認識した後に経営層や職員等が行うべき初動対応(緊急時対応)に関する方針、手順、態勢等をあらかじめ定めたもの。インシデント発生時の被害の軽減と早期の復旧を目指す計画の総称。