資料３－３

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

厚生労働省におけるサイバーセキュリティに関する取り組み

Ministry of Health, Labour and Welfare of Japan

「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

官民連携による重要インフラ防護の推進

・任務保証の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供を実現
・官民が一体となって重要インフラのサイバーセキュリティの確保に向けた取組を推進

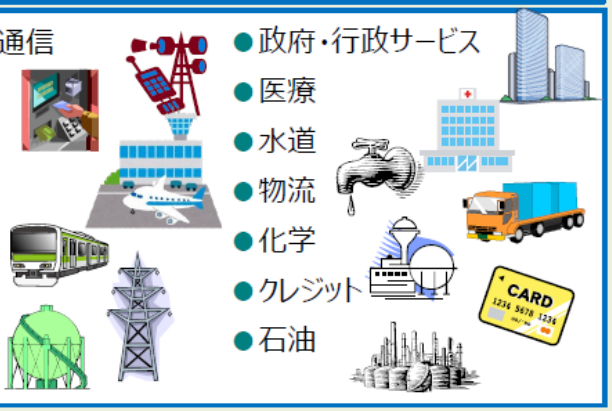
NISCによる総合調整

重要インフラ所管省庁

- 金融庁
  ［金融］
- 総務省
  ［情報通信、行政］
- 厚生労働省
  ［医療、水道］
- 経済産業省
  ［電力、ガス、化学、クレジット、石油］
- 国土交通省
  ［航空、空港、鉄道、物流］

重要インフラ(全14分野)

- 情報通信
- 金融
- 航空
- 空港
- 鉄道
- 電力
- ガス
- 政府・行政サービス
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油



関係機関等

- サイバーセキュリティ関係省庁
  ［総務省、経済産業省等］
- 事案対処省庁
  ［警察庁、防衛省等］
- 防災関係府省庁
  ［内閣府、各省庁等］
- サイバーセキュリティ関係機関
  ［NICT、IPA、JPCERT/CC等］
- サイバー空間関連事業者
  ［サプライチェーン等に関わるベンダー等］

「重要インフラのサイバーセキュリティに係る行動計画」における主な取組

障害対応体制の強化

経営層、CISO、戦略マネジメント層、システム担当等、組織全体での取組となるよう、組織統治の一部としての障害対応体制の強化を推進

安全基準等の整備及び浸透

重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

情報共有体制の強化

官民間や分野内外間における情報共有体制の更なる強化

リスクマネジメントの活用

自組織の特性を明確化し、適した防護対策が継続的に実施されるようリスクマネジメントを活用

防護基盤の強化

分野横断的演習の推進、国際連携の推進、広報広聴活動の推進等の取組によるサイバーセキュリティ全体の底上げ

出典：内閣サイバーセキュリティセンターのウェブサイトより引用

厚生労働省所管の重要インフラ分野における主な取組

➢ 「重要インフラのサイバーセキュリティに係る行動計画」に基づき、内閣サイバーセキュリティセンター（NISC）と連携して、以下のとおりサイバーセキュリティ対策に取り組んでいる。

	障害対応体制の強化	安全基準等の整備及び浸透	情報共有体制の強化	リスクマネジメントの活用	防護基盤の強化
医療	➢ インシデント発生時の駆けつけ機能の確保	➢ 「医療情報システムの安全管理に関するガイドライン」を策定・周知	➢ 医療・水道事業者が、セプター※等を通じて、最新の情報セキュリティ動向を把握するための情報共有体制を整備 ➢ NISCが実施する情報共有の確認訓練（セプター※等における受信状況等を確認する訓練）に参加	➢ 医療機関のセキュリティ対策に関する調査事業を実施	➢ 医療機関向けサイバーセキュリティ対策研修 ➢ NISCが実施するサイバー攻撃による障害発生を想定した実践的な演習（分野横断的演習）に参加
水道	➢ 水道事業者等におけるサイバーセキュリティ対応マニュアルの作成の推進	➢ 水道施設の技術的基準を定める省令にサイバーセキュリティ対策を位置づけ ➢ 「水道分野における情報セキュリティガイドライン」を策定・周知		➢ リスクの評価、インシデント報告・対処体制の可視化及び訓練等について、事業者が自ら実施することができるようツールを作成中	➢ 日本水道協会と連携したサイバーセキュリティ対策に係る講演等を実施

※セプター（CEPTOAR）　Capability for Engineering of Protection,Technical Operation,Analiysis and Response
・重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。
・重要インフラサービス障害の未然防止、発生時の被害拡大防止・迅速な復旧及び再発防止のため、政府等から提供される情報について、適切に重要インフラ事業者等に提供し、関係者間で情報を共有。これにより、各重要インフラ事業者等のサービスの維持・復旧能力の向上に資する活動を目指す。

医療分野におけるサイバーセキュリティ対策

予防対応

① 医療機関向けサイバーセキュリティ対策研修の充実

– 「医療情報セキュリティ研修及びサイバーセキュリティインシデント発生時初動対応支援・調査事業一式」において、**医療従事者や経営層等へ階層別のサイバーセキュリティ対策に関する研修の実施**や、本事業において作成される**ポータルサイトを通じた研修資材の提供**により、医療従事者や経営層等のサイバーセキュリティ対策の意識の涵養を図る。

② 脆弱性が指摘されている機器・ソフトウェアの確実なアップデートの実施

– 医療法第25条第１項の規定に基づく**立入検査の実施により確認**を行う。また、例年発出している「医療法第25条第１項の規定に基づく立入検査の実施について」（医政局長通知）において、令和４年度は**サイバーセキュリティ対策の強化に関する事項について記載**した。**令和４年度中に医療機関等の管理者が遵守すべき事項に位置付けるための省令改正**を行う。

– NISCより情報提供のあった脆弱性情報について、医療セプターを通じた情報提供を引き続き行う。

③ 医療分野におけるサイバーセキュリティに関する情報共有体制（ISAC）の構築

– 他分野のISAC関係者の協力を得つつ、医療関係者数名のコアメンバーによる**検討**を行う。

④ 検知機能の強化

– **不正侵入検知・防止システム（IPS／IDS）の設置・活用を進める**よう、医療情報システムの安全管理に関するガイドライン**改定の検討**を行う。

⑤ G-MISを用いた医療機関への定期調査の実施

– 医療機関に対する**サイバーセキュリティ対策の実態調査**を実施する。

【質問項目（例示）】

・医療法に基づく立入検査の留意事項を認識し、必要な措置を講じているか。

・（許可病床数が400床以上の保険医療機関に対して）診療録管理体制加算の見直しを受けて、専任の医療情報システム安全管理責任者を配置しているか。

医療分野におけるサイバーセキュリティ対策

初動対応

① インシデント発生時の駆けつけ機能の確保

– 200床**以下**の医療機関に対し、**サイバーセキュリティお助け隊の活用を促進するための周知・広報**を行う

– 200床**以上**の医療機関に対し、「医療情報セキュリティ研修及びサイバーセキュリティインシデント発生時初動対応支援・調査事業一式」において、**サイバーセキュリティインシデントが発生した医療機関の初動対応支援**を行う。

② 行政機関等への報告の徹底

– **医療情報セキュリティ研修およびG-MIS調査を通じ**、医療情報システムの安全管理に関するガイドラインに基づいた**厚生労働省への報告の徹底**や、個人情報保護法改正に伴う**個人情報保護委員会への報告義務化の周知**を図る。

– 厚生労働省より、医療情報システムの安全管理に関するガイドラインに基づいて医療機関より報告のあったサイバーインシデント事案について、攻撃先が同定されない程度に報告内容を適時情報提供し、攻撃手法や脅威について分析を行い、全国の医療機関へ情報発信・注意喚起を行う。

復旧対応

① バックアップの作成・管理の徹底

– 医療情報セキュリティ研修およびG-MIS調査を通じ、**バックアップの具体的な作成が明記**された医療情報システムの安全管理に関するガイドライン（５．２版）の周知を行う。

– 令和３年６月28日発出「医療機関を標的としたランサムウェアによるサイバー攻撃について(注意喚起)」の記載事項に留意し、データ・システムのバックアップを行う。

– 令和4年度診療報酬改定における診療録管理体制加算に係る報告書（７月報告）により、**バックアップ保管に係る体制等の確認**を行う。

② 緊急対応手順の作成と訓練の実施

– 「医療情報セキュリティ研修及びサイバーセキュリティインシデント発生時初動対応支援・調査事業一式」において、**サイバーセキュリティインシデントが発生した際の対応手順の調査**を行い、**適切な対応フローの整理**を行う。また、整理した対応フローをもとに**サイバーセキュリティインシデントに備えたBCPの提案**を行う。

医療情報セキュリティ研修及びサイバーセキュリティインシデント発生時初動対応支援・調査事業（令和４年度）

背景

医療分野のサイバーセキュリティについては、近年その脅威が高まっていることから、令和４年度厚生労働省事業において、医療機関向け研修やサイバーセキュリティインシデント発生時の初動対応の支援等を行う。

事業概要

（１）サイバーセキュリティ対策にかかる医療機関向け研修の実施
　：医療機関職員の階層（初学者、経営層、システム･セキュリティ管理者等）に応じた研修の実施
（２）継続的な教育支援
　：医療情報システム安全管理者が研修に活用できる教育コンテンツ作成･収集と公開
（３）平時のサイバーセキュリティインシデント対応手順の調査および既存BCPの見直し提案
　：サイバーセキュリティインシデント発生時の適切な対応フローの整理、BCP（Business Continuity Plan）の提案
（４）サイバーセキュリティインシデントが発生した医療機関の初動対応支援
　：サイバーセキュリティインシデントが発生した医療機関の原因究明や早期診療復帰を目的に、初動対応支援を実施

受託者

一般社団法人　ソフトウェア協会
：約700社のソフトウェア製品に係わる企業が集まり、ソフトウェア産業の発展に係わる事業を通じて、我が国産業の健全な発展と国民生活の向上に寄与することを目的とした一般社団法人
（サイバーセキュリティに関する主な活動内容）
・ソフトウェアやサイバーセキュリティに関連したセミナー、研修の実施　　・サイバーセキュリティに関する情報交換・周知
・サイバーセキュリティボランティア制度の創設・運用

水道分野におけるサイバーセキュリティ対策の概要

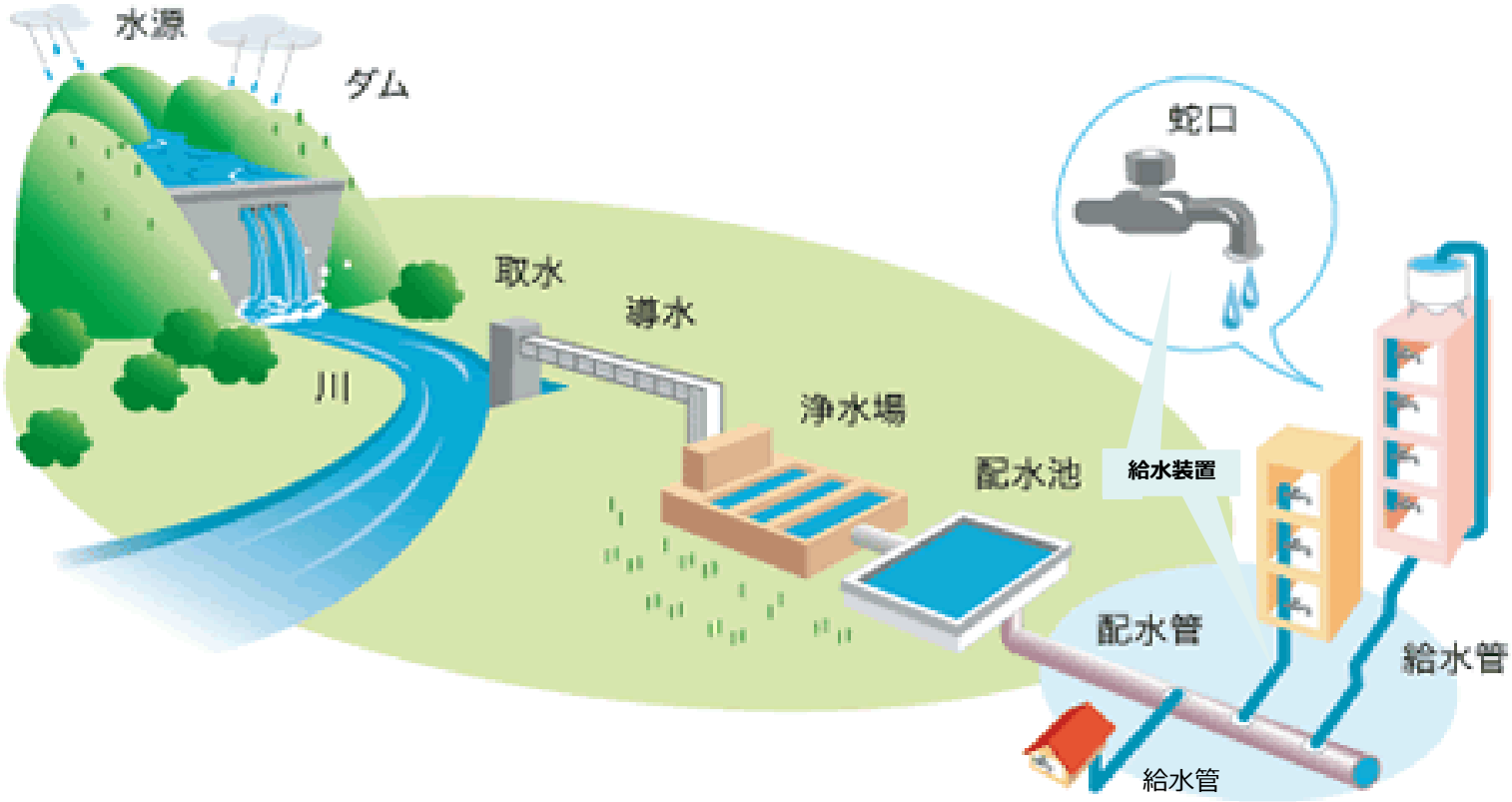
1　水道事業について

（１）水道とは、導管及びその他の工作物により、水を人の飲用に適する水として供給する施設の総体

（２）水道事業は、原則として市町村が経営

※水道事業者に水道用水を供給する水道用水供給事業者と併せて、本資料では水道事業者等と表記

（３）水道法においては、水道施設の備えるべき要件を「水道施設の技術的基準を定める省令」で定めている



水道分野におけるサイバーセキュリティ対策の概要

2　水道施設のサイバーセキュリティ対策

（１）水道施設の技術的基準

水道施設の技術的基準を定める省令において、「施設の運転を管理する電子計算機が水の供給に著しい支障を及ぼすおそれがないように、サイバーセキュリティを確保するために必要な措置が講じられていること」を規定。

（２）水道分野における情報セキュリティガイドラインの策定

「水道分野における情報セキュリティガイドライン」を策定し、水道事業を経営する市町村等におけるサイバーセキュリティ対策への取組を支援。

なお、ガイドラインにおいては、以下の事項について取組方法を解説。

① サイバーセキュリティ対応に必要な体制の整備
② 電子計算機等の情報システムのリスク分析とその結果を用いた対策の実施
③ インシデント発生時の対応
④ 関係機関との連携
⑤ インシデントを想定した訓練の実施、担当者の教育訓練
⑥ サイバーセキュリティ対策の実施状況の監査　ほか

水道分野におけるサイバーセキュリティ対策の概要

2　水道施設のサイバーセキュリティ対策

（３）厚生労働省重要インフラ分野におけるサイバーセキュリティ体制強化の支援事業

- サイバーセキュリティリスクの評価、インシデント報告・対処体制の可視化及び事業の特殊性を踏まえた実践的な訓練等について、水道事業者等が自ら実施することができるようツールを作成中
- 一部水道事業者等に試用いただき、ツールの有効性等を検証中
  （厚生労働省としても、これら水道事業者等の取り組み状況を、実例として把握。）
- 今後、全国の水道事業者等に展開予定。

（４）その他

①　サイバーセキュリティインシデント発生時の対応

・水道事業においてサイバーセキュリティインシデントが発生した場合は、水道事業者等から厚生労働省に報告を行うよう事務連絡を発出済み。

※　厚生労働大臣が認可している水道については厚生労働省に直接報告。都道府県知事が認可している水道事業者等については、都道府県を経由して報告。

②　情報セキュリティマニュアルの作成の推進

③　普及啓発活動の推進

・全ての水道事業者等を対象に、厚生労働省のサイバーセキュリティ対策について説明。

・日本水道協会と連携したサイバーセキュリティ対策に係る講演等を実施。

（参考）
厚生労働省重要インフラ分野におけるサイバーセキュリティ体制強化の支援事業

- 重要インフラ分野（医療、水道）の事業者が①サイバーセキュリティリスクの評価、②インシデント報告・対処体制の可視化、③事業の特殊性を踏まえた実践的な訓練等を行うためのツールを、厚生労働省において作成・提供することにより、各事業者のサイバーセキュリティ体制強化を支援。
- 令和４年度はツールの作成・検証中。令和５年度から各事業者にツールを提供予定。

①リスク評価支援

各分野におけるリスクアセスメントの様式・記載例を提供することで、事業者が記載例を参考にしながら、リスク評価やその結果を踏まえた対策を行えるよう支援する。

(効果)

リスクアセスメントにより、自組織のリスクを把握した上で、改善すべき点を明確化することができる。

②対処体制等の可視化

インシデント発生時のエスカレーション（報告体制）、責任と役割分担、障害に応じた対処項目等のテンプレートを提供し、事業者のインシデント報告･対処体制を整理・可視化する。

（効果）

インシデント発生時における報告先や対処体制等を可視化することで、対応の迅速化を図ることができる。

③訓練実施

それぞれの分野において代表的なインシデントをベースとした訓練シナリオを提供し、事業者が訓練の実施・評価を行う。

（効果）

訓練により、インシデント発生時における対処能力の向上を図ることができる。

今後の課題（厚生労働省関係）

医療分野

（予防対応）
- 医療分野におけるサイバーセキュリティ人材育成の充実

（初動対応）
- サイバーセキュリティインシデント発生時の駆けつけ機能の更なる強化

（復旧対応）
- 緊急対応手順の作成と訓練の実施

（その他）
- 医療機関とベンダーの責任範囲の明確化

水道分野

（予防対応）
- 水道事業者等におけるサイバーセキュリティ対策マニュアルの充実に向けた支援の実施

（初動対応）
- インシデントが発生した際の対処・報告体制の可視化の推進