Ministry of Health, Labour and Welfare of Japan

水道分野における
サイバーセキュリティ対策について

ひと、くらし、みらいのために

厚生労働省
Ministry of Health, Labour and Welfare

水道分野におけるサイバーセキュリティ対策

○　ICTへの依存度が高まるにつれ、サイバー攻撃に対するセキュリティを含む情報セキュリティへの取組の必要性が増大。
○　水道施設のサイバーセキュリティ対策については、平成25年６月に公表した「水道分野における情報セキュリティガイドライン（第３版）」により、水道事業者等において実施すべき適切な情報セキュリティ対策を推進。
○　それ以降、政府のサイバーセキュリティ戦略本部において、「重要インフラのサイバーセキュリティ対策に係る行動計画（令和４年６月）」や「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）改訂版（令和元年５月）」等が策定。

■**水道分野における情報セキュリティガイドライン（第４版）**の策定　（平成31年３月29日）

- 水道分野における情報セキュリティ確保に係る安全基準等として位置づけ。
- 水道事業者において実施することが必要な、又は望まれる情報セキュリティ対策の項目及び水準を示す。

■水道施設の技術的基準を定める省令の一部改正　（令和２年４月１日施行予定）

- 第４次行動計画に基づく情報セキュリティ対策に関する関係法令等の保安規制への位置づけ。
- 水道事業の施設基準を示す省令において、サイバーセキュリティ対策を強化する観点から、新たな規定を整備。

「重要インフラのサイバーセキュリティ対策に係る行動計画」が策定されたことを受け、
今後「水道分野における情報セキュリティガイドライン（第４版）」が改定となる予定。

水道分野における情報セキュリティガイドライン（第４版）の概要

○　サイバーセキュリティ戦略本部による「重要インフラの情報セキュリティ対策に係る第４次行動計画（平成29年６月）」や「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）（平成30年４月）」等を踏まえ、**「水道分野における情報セキュリティガイドライン（第４版）」**を平成31年３月に策定。

○　安全基準等策定指針では、重要インフラ事業者が、分野の特性に応じた必要な、又は望まれる情報セキュリティ対策を着実に実施するとともに、対策を継続的に改善していくことの重要性を指摘。

○　ガイドラインでは、水道事業者において実施することが必要な、又は望まれる情報セキュリティ対策の項目及び水準を示した。

<u>改訂のポイント</u>

① PDCAサイクルによる情報セキュリティ対策の実施と見直しの考え方の充実。
② 情報セキュリティの取組における経営層の役割の追加、最高情報セキュリティ責任者の役割の充実。
③ インシデント発生時における対応の追加。(対応計画の事前策定の必要性等)
④ 平時及びインシデント発生時における関係機関との連携体制の追加。
⑤ 制御系システムにおける対応として、多層的な防御の実施の必要性を強調するとともに、古いバージョンのOSのアップデート等の具体的対策を追記。

水道施設の技術的基準を定める省令改正の概要

○　サイバーセキュリティ基本法に基づく施策の一環として、「重要インフラの情報セキュリティ対策に係る第４次行動計画」において、必要に応じて情報セキュリティ対策を関係法令等の保安規制に位置づけることが求められている。
○　これを踏まえ、水道施設の技術的基準を定める**省令を改正**し、水道施設の施設基準においても、サイバーセキュリティ対策を強化するために必要な措置を講じる旨を規定。

■水道施設の技術的基準を定める省令　第１条第１１の２号（新設）

（施行期日：令和２年４月１日）

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（サイバーセキュリティ基本法（平成26年法律第104号）第２条に規定するサイバーセキュリティをいう。）を確保するために必要な措置が講じられていること。

■「水道施設の技術的基準を定める省令の一部改正について」

（令和元年9月30日付け薬生水発0930第7号）

○ 対象とするシステムは、水の供給に影響を与える**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**※。
○ サイバーセキュリティを確保するために必要な措置とは、以下をいう。
- 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。
- 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こと。
- 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が使用されていない**こと。
  （外部ネットワークからの分離、USBメモリ等の外部記憶媒体からの感染防止対策等、**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はこの限りではない**）
- 電子計算機は、部外者がみだりに立ち入ることができないよう、障壁、施錠等により他の区域から隔離され、**人の入退室を制限することができる場所に設置**されること。

※電子計算機とは、コンピューター全般を指し、情報システムを構成するサーバ、端末、周辺機器等の装置全般。

省令改正に関するよくあるご質問について

Q1　「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」とは具体的に何か。

ここでは、IDとパスワードといった**主体認証の機能自体を有していること**を指します。このため、機能を有していればハード・ソフト面の限定はなく、個別の利用者で認証を行わない共用識別コード等の方法でも構いません。

なお、共用識別コードを利用する場合、職員以外のもののアクセスを制限・管理する必要があるため、「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の設置」以外にも、設置場所に職員等が夜間・休日等に不在となる場合に**電子計算機にアクセスする際に再度主体認証を求める等、より安全な管理が望ましい**です。

Q2　「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こと。」について、外部ネットワークから切り離されている場合はどうか。

不正プログラム対策として、**外部ネットワークからの分離による対策が有効に機能している場合、**アンチウイルスソフトウェアの導入に代えて、**同等の対策を実施していると捉えて構いません**。

一方、外部メモリ等の外部記憶媒体の使用等、**外部ネットワーク以外に不正プログラムの感染経路がある場合**、外部記憶媒体に対し、アンチウイルスソフトウェアを有する他の情報処理端末により安全を確認した後に使用する等、**必要な対策を追加で実施してください**。

Q3　「ネットワークから分離されている」とはどういった状態を指すか。

「ネットワークから分離されている」とは、物理的に外部と接続されていない場合を指します。

なお、特殊な接続方法をはじめ、外部からの不正プログラムの侵入を防ぐための必要な措置が講じられている場合、同様に取り扱って構いません。

Q4　外部メモリ等の感染防止対策について、具体的にどういった対策が必要か。

例えば、**アンチウイルスソフトウェアを有する他の情報処理端末により安全を確認した後に使用する、USBの挿し口を物理的にふさぐ、特定のUSBメモリ以外読み込まないソフトウェアを導入する等**の対策があります。

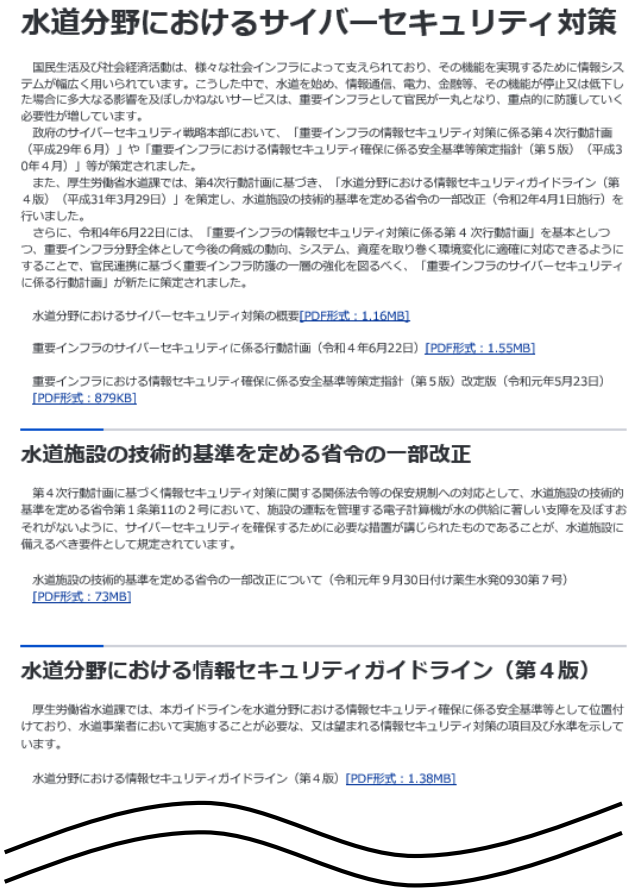
外部メモリ等の外部記憶媒体からの感染防止が**実質的に図られる対策であれば構いません**。

水道分野におけるサイバーセキュリティ対策のウェブページについて

○　厚生労働省では、水道分野におけるサイバーセキュリティ対策のウェブページを開設しました。
○　サイバーセキュリティ対策への厚生労働省や政府の取組を掲載しています。

URLはこちら

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/topics/bukyoku/kenkou/suido/kikikanri/sisin.0005.html



水道分野におけるサイバーセキュリティ対策

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ます。こうした中で、水道を始め、情報通信、電力、金融等、その機能が停止又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性が増しています。
政府のサイバーセキュリティ戦略本部において、「重要インフラの情報セキュリティ対策に係る第４次行動計画（平成29年６月）」や「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）（平成30年４月）」等が策定されました。
また、厚生労働省水道課では、第4次行動計画に基づき、「水道分野における情報セキュリティガイドライン（第４版）（平成31年3月29日）」を策定し、水道施設の技術的基準を定める省令の一部改正（令和2年4月1日施行）を行いました。
さらに、令和4年6月22日には、「重要インフラの情報セキュリティ対策に係る第４次行動計画」を基本としつつ、重要インフラ分野全体として今後の脅威の動向、システム、資産を取り巻く環境変化に適確に対応できるようにすることで、官民連携に基づく重要インフラ防護の一層の強化を図るべく、「重要インフラのサイバーセキュリティに係る行動計画」が新たに策定されました。

水道分野におけるサイバーセキュリティ対策の概要[PDF形式：1.16MB]

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４年6月22日）[PDF形式：1.55MB]

重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）改定版（令和元年5月23日）[PDF形式：879KB]

水道施設の技術的基準を定める省令の一部改正

第４次行動計画に基づく情報セキュリティ対策に関する関係法令等の保安規制への対応として、水道施設の技術的基準を定める省令第１条第11の２号において、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たものであることが、水道施設に備えるべき要件として規定されています。

水道施設の技術的基準を定める省令の一部改正について（令和元年９月30日付け薬生水発0930第７号）[PDF形式：73MB]

水道分野における情報セキュリティガイドライン（第４版）

厚生労働省水道課では、本ガイドラインを水道分野における情報セキュリティ確保に係る安全基準等として位置付けており、水道事業者において実施することが必要な、又は望まれる情報セキュリティ対策の項目及び水準を示しています。

水道分野における情報セキュリティガイドライン（第４版）[PDF形式：1.38MB]

2）セプター

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を、英語名称（Capability for Engineering of Protection, Technical Operation, Analysis and Response ）の略称として、セプター（CEPTOAR）と呼んでいます。
具体的には、IT 障害の未然防止、発生時の被害拡大防止・迅速な復旧および再発防止のため、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することで、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しています。水道分野では、公益社団法人日本水道協会が水道セプターとしての役割を担っています。

セプターカウンシル総会資料（セプターカウンシルの概要）[リンク]
（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）

サイバーセキュリティ対策強化に向けた取組

1）分野横断的演習

「重要インフラのサイバーセキュリティに係る行動計画」の主要５施策のうち「防護基盤の強化」の中に位置付けられるものであり、実際の事案発生を模擬することにより、重要インフラ行動計画に従って日頃より強化に取り組む障害対応体制が有効に機能するかどうかを確認し、改善につなげていくことを目的として毎年度実施しています。複数の水道事業者の皆様に御参加いただいていますが、NISCは、より多くの水道事業者の参加を呼びかけています。

分野横断的演習[リンク]

2）サイバーセキュリティ月間

政府では、サイバーセキュリティに関する普及啓発強化のため、２月１日から３月１８日までを「サイバーセキュリティ月間」とし、国民の皆様にサイバーセキュリティについての関心を高め、理解を深めるため、サイバーセキュリティに関する様々な取組を集中的に行っています。

サイバーセキュリティ月間[リンク]

報告書、資料等

令和2年度水道分野におけるサイバーセキュリティ対策（ISAC調査）[PDF形式：1.93MB]