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。

■**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。

令和４年度は、「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」の改定が予定されており「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）」も改定となる予定。

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項（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**。