



国水第 399 号

令和 7 年 2 月 28 日

各都道府県水道行政担当部（局）長 殿
各国土交通大臣認可 { 水道事業者 } 殿
 水道用水供給事業者 }
国設専用水道の設置者 殿
（各地方整備局等水道担当経由）

国土交通省水管理・国土保全局水道事業課長

（公 印 省 略）

「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」の一部改正について

令和元年 9 月 30 日に公布された、水道施設の技術的基準を定める省令の一部を改正する省令（令和元年厚生労働省令第 59 号）については、水道施設におけるサイバーセキュリティ対策を強化することを目的として、令和 2 年 4 月 1 日から施行されたところであり、「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 号厚生労働省医薬・生活衛生局水道課長通知。以下「課長通知」という。）により、水道施設が備えるべき要件のうち、サイバーセキュリティを確保するために必要な措置に係る留意事項を示しているところである。

水道を含む重要インフラに対するサイバー攻撃等の脅威は年々高度化・巧妙化しており、これを踏まえて、今般、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に係る行動計画」や「重要インフラのサイバーセキュリティに係る安全基準等策定指針」等が新たに策定された。これを受けて、水道施設においても不正プログラム対策としてサイバーセキュリティの確保に必要と認められる措置を追加し、また、オペレーティングシステムに係る措置を厳格化するなど、外部からのサイバー攻撃等によるシステムへの侵入等に係る考え方を見直すこととしたため、課長通知の一部を別紙のとおり改正し、令和 7 年 2 月 28 日から適用することとしたため通知する。

国土交通大臣認可の水道事業者及び水道用水供給事業者並びに国設専用水道の設置者においては、御了知の上、遺漏なきよう期されるとともに、各都道府県においては、本通知について、貴管内の市及び特別区、都道府県知事認可の水道事業者及び水道用水供給事業者並びに専用水道の設置者（国設専用水道の設置者を除く。）に対して周知されたい。また、水道事業及び水道用水供給事業の認可、専用水道の確認並びに改善の指示等の事務を行うに当たっては、サイバーセキュリティに係る施設基準への適合について本通知の内容を踏まえて指導に遺漏のないようにされたい。

なお、本通知は、地方自治法（昭和 22 年法律第 67 号）第 245 条の 4 第 1 項の規定に基づく技術的助言である旨申し添える。

(別紙)

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 号厚生労働省医薬・生活衛生局水道課長通知）

新旧対照表

改正後	改正前
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 (前文略) 記 第一 (略) 第二 (略) 第三 留意事項 一 (略) 二 制御系システムに使用されている電子計算機について、次の措置が講じられていること。 ・ 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とともに、自動検査機能が有効となっていること <u>(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)。</u>	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 (前文略) 記 第一 (略) 第二 (略) 第三 留意事項 一 (略) 二 制御系システムに使用されている電子計算機について、次の措置が講じられていること。 ・ 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<u>こと。また、自動検査機能</u>が有効となっていること。

- ・ 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（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）。
- ・ 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。

- ・ 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の物理的な分離、USBメモリ等の外部記憶媒体からの感染防止対策等、不正プログラムの進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、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、常に携帯することなど、盗難等のおそれがないよう適切に管理すること。