写

事　務　連　絡
令和８年３月 24 日

各{都道府県／市／特別区}水道行政担当部（局）　殿

各国土交通大臣認可{水道事業者／水道用水供給事業者}殿

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
水道事業課水道計画指導室

サイバーセキュリティ対策に係る水道施設の技術的基準に関してよくある質問（FAQ）について（令和８年３月 24 日時点版）

水道行政の推進につきましては、日頃から格別の御協力を頂き御礼申し上げます。

水道における情報セキュリティ対策につきましては、令和７年２月 28 日付国水水第 399 号国土交通省水管理・国土保全局水道事業課長通知（「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）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きたところです。

今般、これまでにいただいた質問等を踏まえて「サイバーセキュリティ対策に係る水道施設の技術的基準に関してよくある質問(FAQ)について」を作成しましたので送付します。

つきましては、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きましては、本 FAQ を参考に、引き続き情報セキュリティ対策の徹底をお願いいたします。また、都道府県におきましては、貴管内の都道府県知事認可の水道事業者、水道用水供給事業者及び専用水道の設置者（国設専用水道の設置者を除く。）並びに町村に対して、市及び特別区におきましては、貴管内の専用水道の設置者（国設専用水道の設置者を除く。）に対して、本 FAQ を参考に、引き続き情報セキュリティ対策を徹底するよう周知をお願いいたします。

【連絡先】
国土交通省水管理・国土保全局水道事業課水道計画指導室
サイバーセキュリティ対策担当（池本、小林、小泉）
TEL　代表 03-5253-8111（内線 34439）

サイバーセキュリティ対策に係る水道施設の技術的基準に関してよくある質問（FAQ）について

令和８年３月 24 日時点
国土交通省水管理・国土保全局水道事業課水道計画事業室

本 FAQ は、令和７年２月 28 日付国水水第 399 号国土交通省水管理・国土保全局水道事業課長通知（「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）に記載の留意事項に関してよくある質問について解説するものです。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の高度化・巧妙化や、政府の行動計画や指針等、さらには水道事業者等のサイバーセキュリティ対策の実態等を踏まえて今後変更のあり得るものですので、最新のものを参照いただくようご留意ください。

●本 FAQ における用語の定義

・中央監視室

サイバーセキュリティ対策に係る水道施設の技術的基準を定める省令の対象となる、水施設の運転管理をする電子計算機のある場所のこと。中央管理室等ともいう。本 FAQ においては便宜上、浄水場の敷地内にあることとする。

●全般的事項

問１

外部ネットワークからの物理的な分離（閉域網の構築）さえすれば十分か。

（答）

○　十分とは言えない。ゼロトラストの考え方も参考に、ネットワークの内部が侵害されることも想定し、ネットワークの内部は安全であるという前提を暗黙的に信用しないことが肝要である。

○　とりわけ留意事項の２点目及び３点目において、括弧書きの中の代替措置の実施により水道施設の技術的基準に適合しようとする場合には、外部ネットワークからの物理的な分離による外部侵入対策のみならず、内部侵入対策を同時に講じることが必要不可欠であることに留意のこと。

問２

代表的な水道施設においてのみ対策していれば良いか。

（答）

○　不可。サイバーセキュリティ対策に係る水道施設の技術的基準は、代表的な水道施設にのみ適用されるものではなく、全ての水道施設（制御系システムに使用されている全ての電子計算機）に適用されるものである。

●留意事項１点目関連

留意事項１点目：
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。

問３

中央監視室の入口で主体認証をしていれば良いか。

（答）

○　中央監視室の入り口や浄水場の入り口において主体認証により入退出の管理をしていることのみをもって、電子計算機へアクセスする者について主体認証をしていることにはならないことに留意のこと。また、中央監視室の入り口や浄水場の入り口において主体認証をしていることのみをもって電子計算機へアクセスする者についての主体認証を行うことができる機能を有していることにはならないことに留意のこと（場所の入退出管理のための主体認証は、電子計算機での主体認証とは認められない)。

●留意事項２点目・３点目関連（括弧書きの中の代替措置等）

留意事項２点目：
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）。

留意事項３点目：
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）。

問４

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とは。

（答）

○　この留意事項においては、「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」の例示として「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」が示されている。このため、外部ネットワークからの物理的な分離と同等の「外部侵入対策」及び USB メモリ等の外部記憶媒体からの感染防止対策と同等の「内部侵入対策」の両者を講じている必要があり、具体的には個別に判断されるものになる。「外部侵入対策」または「内部侵入対策」のいずれか一方では不十分であることに留意のこと。

○　ここで、外部侵入対策とは、インターネット等の外部ネットワークから制御系システムへの不正な侵入を防止または抑止し、万一侵入された場合であっても被害を最小化するための措置をいう。その一類型として、外部ネットワークとの接点を一切持たない「閉域網の構築」が挙げられる。一方、閉域網を構築できず、外部ネットワークを介して遠隔監視・制御を行う場合には、外部からの侵入が発生し得ることを前提に、適切な外部侵入対策が講じられている必要がある。

○　その具体的な対策例としては、以下の組合せによる多層防御が考えられる。
・外部ネットワークから制御系システムへの接続経路を必要最小限に限定すること
・通信内容を制御・検査すること

・外部から接続する主体に対する厳格な認証を行うこと
・接続端末が適切に管理された状態にある場合のみ接続を許可すること
・操作の記録・監視等により万一の侵入時の被害拡大を抑止すること　等

○　なお、これらの対策はいずれか単独では外部侵入対策としては十分とは言えず、複数を組み合わせて実施することが重要であることに留意のこと。

問５

外部ネットワークからの物理的な分離（閉域網）について気を付けることは。

（答）

○　インターネットから物理的に遮断されていない部分との接続がある場合には、閉域網には当たらないことに留意のこと。

○　留意事項に関連して閉域網の構築を考える際には、システム全体の一部分のみを切り出して、その一部分が閉域網を形成している・いない、というように考えるのではなく、制御系システム及び当該システムと繋がっている部分を含めたシステム全体として、インターネットとの接点が一切無いかどうか、物理的に遮断されていない接続のある部分があるか否かを確認することが懲憩される。

○　「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」においては、「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」とし、閉域網を構築していることにはならないケースとして、「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」を例示している。つまり、ファイアウォールによる不正アクセス対策は、論理的な遮断であって、外部との接続を物理的に遮断していることにはならない。また、「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」としている。

○　このことに関連して、タブレットやスマートフォン等の端末を用いて浄水場の内外から遠隔で浄水場の運転や浄水処理の状況等を監視・制御する事例について取り上げることとする。例えば、浄水場の外部から浄水場内のネットワークにアクセスできれば、中央監視室や現場に常駐しなくとも外部から管理できるようになり、異常発生時に外部にいても速やかに状況の把握等の初動対応が容易に行えるといったメリットが考えられるが、そうした利便性の獲得と引き換えに、サイバーセキュリティの確保の観点においては脆弱性が増大し得るというデメリット要素をも含んだものであるということに留意のこと。すなわち、遠隔で使用する端末がインタ

ーネット等、専用ネットワーク以外のネットワークに接続可能であったり、テザリングにより他の端末を遠隔利用のためのネットワークに接続可能であったりする機能を有する場合には（そうした機能を実際に使用するか否かを問わず）、浄水場内のネットワークは、インターネットから物理的に遮断されていない部分との接続があることになり、閉域網を構築していることにはならないことになる。

○　とりわけ、遠隔で使用する端末が、水道事業者等の管理下にある専用端末ではなく、使用者個人のスマートフォン等（いわゆる BYOD 端末）である場合には、端末を浄水場の外部に持ち出して遠隔で監視・制御を行う運用が想定される。この場合、当該端末は、モバイルデータ通信や公衆無線 LAN 等の外部のネットワークに接続して遠隔アクセスを行うこととなるため、システム全体としてインターネットとの接点を完全に断つことはできず、外部ネットワークから物理的に分離しているものとは整理できない点に留意のこと。

○　したがって、BYOD 端末を用いて浄水場の外部から遠隔監視・制御を行う場合には、外部からの侵入を前提とした対策（例えば、前述の多層防御等）を講じることが求められる。

○　なお、MDM（Mobile Device Management）や UEM（Unified Endpoint Management）等により、OS レベルで「遠隔利用のための専用ネットワーク以外のネットワークに接続できない状態」及び「テザリング等により他の端末を遠隔利用のための専用ネットワークに接続させることができない状態」を構築し、管理者側で設定・確認をした上で使用者に端末を配布し、使用者がそうした「できない状態」を解除できないようにすることは、遠隔監視・制御を行う場合の一つの方策である。

○　一方で、BYOD 端末については、水道事業者等が当該端末の管理者権限を確保できない場合や、設定の変更・初期化等により管理状態が失われる場合があることから、上記のような「できない状態」を恒常的に担保することが困難となり得る。このため、万一、端末が初期化されたり、ジェイルブレイクやルート化等によって端末の管理者権限が奪取されたりした場合には、当該端末を遠隔監視・制御に使用できなくなる、または、遠隔利用のための専用ネットワークに接続不能とするなど、管理状態の喪失を自動的に検知して遠隔利用を不可とする仕組みが講じられていれば、閉域網を構築しているものとみなすこととする（閉域網相当）。

※　後述の問８「ホワイトリスト方式とは何か、外部侵入対策及び内部侵入対策として十分か。」も参照のこと。

問６

外部記憶媒体の具体例は。

（答）

○　例示をしているUSB以外に、CDやDVD、ブルーレイディスク、フロッピーディスク、ハードディスク、SSD等を含む。

問７

USB メモリ等の外部記憶媒体からの感染防止対策について、USB ポートを箱等に収納すれば良いか。（USBをUSBポートに接続する場合を例にするが、USB以外の外部記憶媒体についても同様）

（答）

○　USBポートが鍵付きの蓋・箱・棚等の中にある場合、「USBメモリ等の外部記憶媒体からの感染防止対策」を満たすのは、以下の（１）または（２）、（３）または（４）、（５）または（６）、（７）または（８）の４点の組合せにおいては、（１）・（３）・（５）・（７）の組合せ（（１）・（３）・（５）・（７）の４点を同時に満たすもの）のみである。

施錠される蓋・箱・棚等の中には、

（１）USBポートしかない

（２）USBポートの他に、電子計算機の操作盤等がある

鍵は、

（３）接続することが認められたUSBを接続するときにのみ使用が許可され、誰がいつ使用するかも管理されている

（４）USB の接続以外の目的（電子計算機の操作・メンテナンス等）のためにも使用される

蓋・箱・棚等は、

（５）USBを接続するときにのみ開錠される

（６）USBを接続するとき以外にも開錠される（電子計算機の操作・メンテナンス時等）

接続するUSBは、

（７）登録されたUSBのみ使用が可能であり、誰がどのUSBをいつ使用するかも管理されている

（８）管理されていない

問８

ホワイトリスト方式とは何か。外部侵入対策及び内部侵入対策として十分か。

（答）

○　ホワイトリスト方式とは、事前に許可したプログラム・通信等のみを利用・実行可能とする方式のことで、許可されていないものは全て拒否することにより、未知の脅威を防止する手段として採用される。許可されている対象のリスト（ホワイトリスト）を作成することが特徴であるが、設定の変更の多い環境等においてはリストの管理に手間がかかるなど、一定の運用負荷が掛かる。

○　ホワイトリスト方式の制御の対象としては、アプリケーション実行やネットワーク通信等があり、例えばアプリケーションのみをホワイトリスト化し、通信はファイアウォール等で論理的に制御する、といったように、現場の環境に応じて制御の対象を選択する運用がなされる。

○　ここで、アプリケーションのホワイトリスト化のみでは、外部侵入対策や内部侵入対策としては不十分であることに留意のこと。すなわち、不正通信が防げないことにより、アプリケーションの実行は制御できても、不正な外部サーバへの接続等、想定外の通信が成立するおそれがある。また、正規アプリの脆弱性を突いて許可されたアプリの内部で悪意のある動作を実行すること（Living off the Land, LOTL）も考えられる。水道事業者等においては、監視のためのネットワーク通信を完全には制御しない運用である場合に、監視用の通信経路が外部侵入の入口になること等が考えられる。

○　このように、ホワイトリスト方式において制御の対象が限定的である場合には、外部侵入対策や内部侵入対策としては不十分であることに留意のこと。

○　また、ホワイトリスト方式においてアプリケーション実行とネットワーク通信の両者を制御する場合については、現時点において、留意事項２点目・３点目の括弧書きの中の代替措置における「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」を満たすものとして扱う（外部侵入対策及び外部侵入対策の両者を講じているものとみなす）こととする。

●留意事項４点目関連

留意事項４点目：
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。

問９

他の区域からの隔離について教えてほしい。

（答）

○　中央監視室自体が他の区域から隔離されていることを求めたもの。中央監視室のある浄水場が近隣施設から離れていることのみをもって、中央監視室が他の区域から隔離されているということにはならないことに留意のこと。

問 10

人の入退出の管理について気を付けることは。

（答）

○　中央監視室に出入りする人（職員・職員以外を問わず）一人ひとりについて、「入」と「出」の両方を管理すること。中央監視室のある浄水場の出入り口での入退室ではないことに留意のこと。

○　中央監視室の入り口や浄水場の入り口において主体認証により入退出の管理をしていることのみをもって、電子計算機へアクセスする者について主体認証をしていることにはならないことに留意のこと。また、中央監視室の入り口や浄水場の入り口において主体認証をしていることのみをもって電子計算機へアクセスする者についての主体認証を行うことができる機能を有していることにはならないことに留意のこと（場所の入退出管理のための主体認証は、電子計算機での主体認証とは認められない）。【問３より再掲】

以上