事　務　連　絡
令和８年９月 25 日

各{都道府県／市／特別区}水道行政担当部（局）　御中

各国土交通大臣認可{水道事業者／水道用水供給事業者}　御中

国設専用水道の設置者　御中

（各地方整備局等経由）

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

水道施設に対するサイバーセキュリティ対策の徹底について

水道行政の推進につきましては、日頃から御協力を賜り、厚く御礼申し上げます。

昨今、サイバー攻撃等の脅威は年々高度化・巧妙化しており、米国においては、別紙のとおり、制御機器のパスワードが不正に変更され、機器の初期化が必要となった事案や、ポンプ場の停止により水圧の低下が生じた事案が発生しています。

これらの事案を踏まえ、各水道事業者及び水道用水供給事業者並びに国設置専用水道の設置者におかれましては、下記に示すサイバーセキュリティ対策の実施状況を改めて確認の上、対策の徹底をお願いします。

各都道府県におかれましては、貴管内の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に対して、各市及び特別区におかれましては、貴管内の専用水道の設置者に対して、この旨周知をお願いします。

記

１．水道施設の技術的基準を定める省令が求めるサイバーセキュリティ対策（令和７年２月 28 日付け国水水第 399 号水道事業課長通知）

（１）電子計算機へアクセスする者についての主体認証機能の導入
（２）アンチウイルスソフトウェア導入等の不正プログラム対策の実施
（３）サポートが終了した OS を使用しない
（４）電子計算機を他の区域から隔離し、人の入退出を管理

※（２）、（３）については、上記通知に定める代替措置でも可。

２．AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化（令和８年５月 25 日付け国土交通大臣官房上下水道審議官通知）

特に水道事業者及び水道用水供給事業者におかれては、以下の対策強化を行う。

（１）経営層のリーダーシップの下での対策
（２）基本的なサイバーセキュリティ対策の確実な実施及び更なる対策の強化
（３）高性能 AI により高速化する脆弱性の発見・修正等への対応

上記のほか、サイバーセキュリティ対策の具体例については、「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（第二版)」（令和８年５月 13 日付け事務連絡）も参考にしてください。

○参照すべき通知等

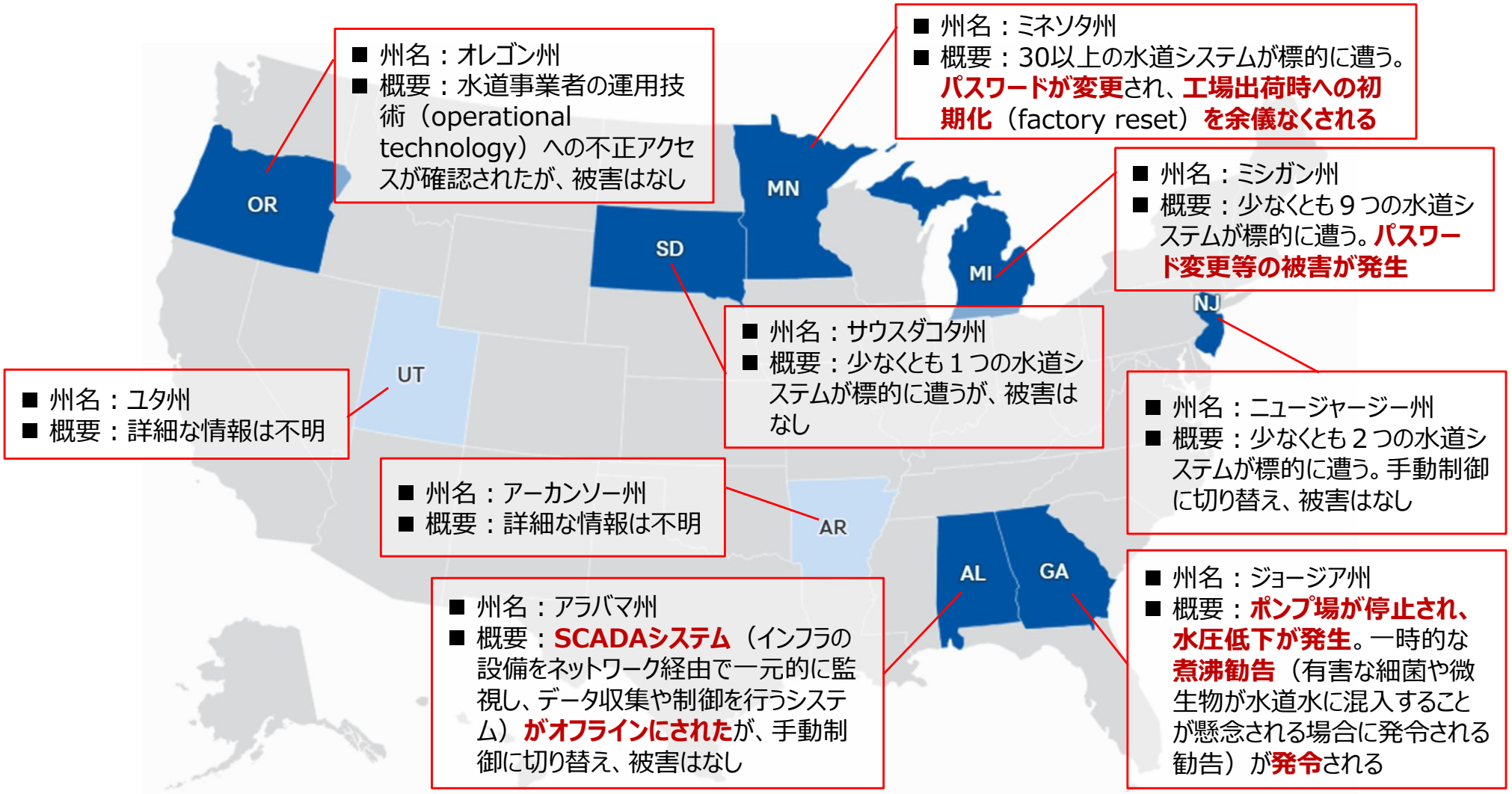
・「「水道施設の技術的基準を定める省令の一部改正について」の一部改正について」（令和７年２月 28 日付け国水水第 399 号）
・「「水道分野における情報セキュリティ確保に係る安全ガイドライン（第二版)」の送付について」（令和８年５月 13 日付け国土交通省水管理・国土保全局水道事業課企画専門官事務連絡）
・「AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化について」（令和８年５月 25 日付け国土交通大臣官房上下水道審議官通知）

（問合せ先）
○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
担当：渡邉、下平
TEL：03-5253-8111(内線 34436)
E-mail： hqt-suidoucyber@ki.mlit.go.jp

（別紙）米国の水道システムに対するサイバー攻撃事案

国土交通省

- 米国では、７月末以降、ミネソタ州を皮切りに少なくとも報道ベースでは12州（現時点で州名が明らかになっているのは９州）において水道システムを標的にしたサイバー攻撃が発生。
- ジョージア州ではポンプ場が停止されたほか、ミネソタ州やミシガン州ではインターネットに接続されたプログラマブル・ロジック・コントローラのパスワードが変更される等の被害が確認された。



出典：CSIS,”Mapping Iranian Cyberattacks on U.S. Water Systems” 等の公開情報を基に経済安全保障調査室にて作成