水道分野におけるサイバーセキュリティ対策調査一式

報　告　書

令和3年3月

厚生労働省

医薬・生活衛生局　水道課

目次

1. 調査目的

情報通信技術（ICT）の発展に伴い、社会全体においてサイバー攻撃の脅威が高まっており、世界各国でサイバーセキュリティ対策が進められているところである。我が国においても日本のサイバーセキュリティに関する施策に関し基本理念を定めるサイバーセキュリティ基本法が 2014 年に制定され、国際情勢や ICT の進化に応じて改正が続いている。また同法律において内閣官房長官を本部長とするサイバーセキュリティ戦略本部が設置され、同時に内閣官房組織令に基づき内閣サイバーセキュリティセンター（NISC）が設置された。

NISC が中心となって推進している重要インフラの対策に係る第４次行動計画[1]において、水道分野は他に代替することが著しく困難なサービスを提供する、事業が形成する国民生活及び社会経済活動の基盤であるとされる重要インフラ14分野の１つとして特定され、情報共有体制の強化及び各種施策を行ってきている。

一方で重要インフラ分野の一部では ISAC（Information Sharing and Analysis Center）と呼ばれる、同じ業界の民間事業者や公的機関の間でサイバーセキュリティに関する情報を共有し、サイバー攻撃への防御力を高めることを目指して活動する非営利組織を設立している事例がある。水道分野においても米国において連邦政府主導で ISAC が設立されている。

こうした背景から、本業務は我が国の水道分野における ISAC 等のサイバーセキュリティ対策に関する情報共有のあり方について検討を行うものである。

- 海外事例に関する調査
  - 水道分野において ISAC を導入している代表事例として米国の Water-ISAC について、行政機関との関係を含む運営体制、活動内容の詳細、会員からの徴収額を含む予算規模等を調査する。調査にあたっては、調査事項を厚生労働省医薬・生活衛生局水道課（以下「水道課」という。）と調整の上、ホームページを含む既存文献を確認した。
- 国内の他分野に関する調査
  - 我が国の「情報通信」、「金融」及び「電力」においては、ICT-ISAC、金融 ISAC、電力 ISAC として ISAC を導入している事例があり、それぞれの分野のセプターとの役割分担を含めた運営体制、活動内容の詳細、予算規模等を調査する。調査にあたっては、調査事項を水道課と調整の上、ホームページや文献調査、必要に応じてヒアリング調査等により実施した。
- 我が国の水道分野におけるサイバーセキュリティ対策の在り方検討
  - 上記の調査結果を元に、我が国の水道分野におけるサイバーセキュリティ対策の状況と比較分析する。調査にあたっては、ホームページを含む既存文献を確認した上で、調査事項を水道課と調整の上、ホームページや文献調査、必要に応じてヒアリング調査等により実施。

[1] 内閣サイバーセキュリティセンター「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」[https://www.nisc.go.jp/active/infra/outline.html]（最終検査日：2021 年１月 22 日）。

2. 事例調査

2.1. 海外事例調査（米国 ISAC）

米国においては日本におけるセプター活動（2.2.1 にて後述）にあたるものは確認できず、政府主導のもと重要インフラ分野において ISAC が設立されており、ISAC 国家評議会（the National Council of ISACs）を通じて約 20 の ISAC が活動している。

【ISAC とは】

ISAC（Information Sharing and Analysis Center）は、重要インフラに対するサイバーセキュリティ上の脅威を収集し、民間部門と公的機関の間で双方向の情報共有を行うための非営利団体である。National ISAC Council によると ISAC が提供するものとして以下があるとしている[2]。

- 24 時間年中無休の脅威警告及びインシデント報告機能
- インシデント・脅威・脆弱性に関するその分野独自の情報を共有・分析
- その分野の重要なサイバー情報の収集・分析・インシデント・レポート
- その分野におけるインシデント・脅威・脆弱性の影響を関係政府機関に説明する機能
- サイバー・物理を問わず重要インフラ保護のための信頼できる情報共有システム

2.1.1. 概要

米国・水道情報共有・分析センター（WaterISAC）は、上下水道セクター唯一の総合セキュリティ・ネットワークである。米国上下水道セクターの主要全国組織および研究財団が米国環境保護庁（the US Environment Protection Agency/EPA）と協力して 2002 年に設立したもので、同年の「米国バイオテロ法（the Bioterrorism Act）」（2002 年6月 12 日）[3] により議会承認された。水道セクター調整評議会（the Water Sector Coordinating Council）の指定情報共有・運用部門である[4]。

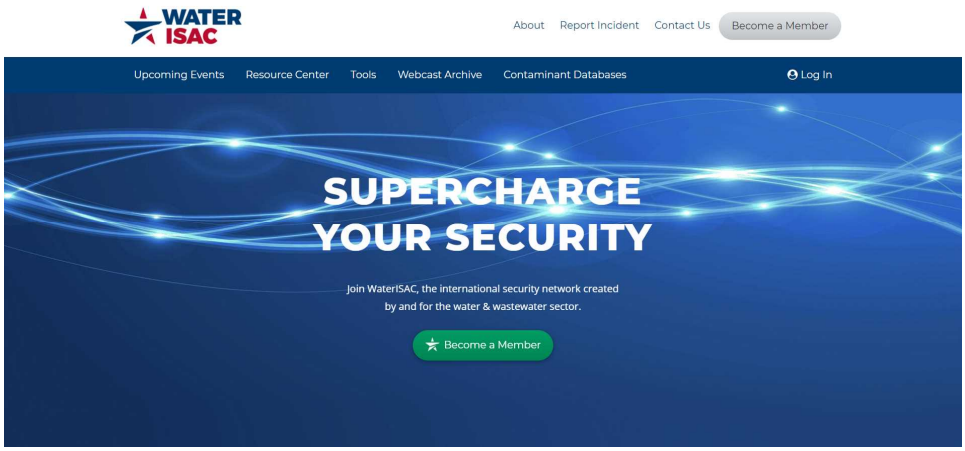


図 1 WaterISAC の HP

[2] National Council of ISACs, “About ISACs,” [https://www.nationalisacs.org/about-isacs]（最終検査首：2021 年３月 11 日）。

[3] The 107th Congress of the United States of America, “The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (the Bioterrorism Act),” PUBLIC LAW 107–188, JUNE 12, 2002 [https://www.energy.gov/sites/prod/files/2014/03/f12/PL107-188.pdf]（最終検索日：2021 年1月 22 日）。

[4] WaterISAC, “About Us,” [https://www.waterisac.org/about-us]（最終検索日：2021 年1月 22 日）。

2.1.2.　設立の背景・目的

WaterISAC は 2002 年 12 月に設立された非営利団体で、所在地はワシントン特別区（Washington, D.C.）である。上下水道セクターの全脅威に対応するためゼロから構築された組織で、セクターのニーズを理解しサポートする独自の立場にある。

【根拠法令等】

上下水道インフラおよび WaterISAC に関連する法令としては、まずクリントン政権による「**重要インフラ保護に関する大統領令第 63 号**（1998 年5月 22 日）（Presidential Decision Directive/NSC-63）」[5]が挙げられる。本大統領令は、「水システム（water systems）」を含む「重要インフラ」とそれらの相互依存性や増大する脆弱性等を定義[6]した上で、既存組織の「国家インフラ保護センター（National Infrastructure Protection Center/NIPC）」への機能拡大・再編の承認と、民間セクターおよび政府機関とのパートナーシップ推進に資する「情報共有・分析センター（ISAC）」構築が強力に奨励されている。本大統領令において、ISAC は既存の成功事例である「疫病管理予防センター」等の機関の、とりわけ民間・非連邦部門との広範な交流の例に倣い、高度な技術的フォーカスや専門性、非規制・非法執行の任務を担うものとして、各種インフラに関するベースライン統計とパターンの確立、セクター内およびセクター間の情報交換所としての機能、また適切なデータのライブラリーを提供することが想定されている。

また、2001 年９月に発生した「米国同時多発テロ事件」による米国史上最悪の人的・インフラ資産の喪失の教訓を踏まえ、米国内では多数の対策法令が成立しているが、上下水道インフラのサイバーセキュリティに関連するものとして、前述した 2002 年６月の「**米国バイオテロ法**」に続き、「**重要インフラの特定、優先順位付け、および保護に関する国土安全保障省（DHS）大統領指令第7号**（2003 年 12 月 17 日）（Homeland Security Presidential Directive 7）」が挙げられる。ジョージ・W・ブッシュ政権（第 43 代）による本大統領指令は、連邦各省庁が重要インフラを特定し、優先順位を付け、テロ攻撃から保護するための国家政策を確立し[7]、関連用語の定

---

[5] Federation of American Scientists, “Presidential Decision Directive/NSC-63,” Washington, May 22, 1998, [https://fas.org/irp/offdocs/pdd/pdd-63.htm]（最終検索日：2021 年1月 22 日）。

[6] 「「重要インフラ」とは、経済と政府機能の最小限の運用に不可欠な物理的およびサイバーベースのシステムであり、政府と民間の双方が提供する以下を含むが、これらに限定されない：電気通信、エネルギー、銀行および金融、運輸、**水システム**、および緊急サービス。これら国家重要インフラの多くは、歴史的には物理的および論理的に分離されたシステムであり、相互依存性はほとんど存在しなかったが、情報技術の進歩と効率性改善の必要性の結果として、これらはますます自動化され、相互関連するようになった。またこうした進歩により、機器の故障、人為的ミス、天候その他の自然要因、物理的およびサイバー攻撃に対する新たな脆弱性が誕生した。これらの脆弱性に対処するには、必然的に、公共セクターと民間セクターの双方にまたがり、国内・国際安全保障の両方を保護する、柔軟で進化的なアプローチが必要となる。」 “I. A Growing Potential Vulnerability” （“Presidential Decision Directive/NSC-63,” 1998）。

[7] 「【政策】アメリカ合衆国政策として、以下の可能性のあるテロ行為に対する米国重要インフラと主要リソースの保護を強化すること：大量破壊兵器の使用に匹敵する壊滅的な健康影響もしくは大量死傷者を誘発する；重要な任務遂行もしくは公衆の健康と安全確保のための連邦各省庁の能力を損なう；秩序の維持、最低限必要な公共サービスの提供をする州および地方政府の能力を損なう；経済の秩序ある機能と不可欠なサービスの提供を確保するための民間部門の能力を損なう；他の重要インフラと主要リソースの連鎖的な混乱を通じて、経済に悪影響を及ぼす；もしくは、我が国の経済的・政治的制度に対する国民の士気と信頼を損なう。」「連邦各省庁は、重要インフラと主要リソースの保護を特定・優先順位付け・調

義と 31 のポリシー・ステートメント（本指令の対象範囲と、指令実行時に各連邦、州、地方関連機関が果たす役割を定義）を提供している。また、本大統領指令における DHS 長官の責務として、IT を含む重要インフラの保護活動の調整を行い、連邦・州・地方政府や民間、学術業界、国際機関等と連携してサイバーセキュリティの中心的機能を発揮する組織の維持・支援を実施すること、と明記されている。

2.1.3. 所管省庁

WaterISAC の所管省庁は、米国環境保護庁（Environment Protection Agency/EPA）である。前述「2003 年大統領指令第7号」において、上下水道システムの特定所管当局（Sector Specific Agency/SSA）は EPA と定められており、DHS 長官のガイダンスの下、SSAs は関連する連邦・州・地方政府や法務当局、インフラ関連民間セクターらと協力してセクターの脆弱性評価を実施・促進し、重要インフラおよび主要リソースへの攻撃からの保護や影響の緩和のためのリスク管理戦略を奨励すること[8]、と明記されている。

WaterISAC のメンバーシップは、国内数百のユーティリティやその他組織で構成されている。「ユーティリティ・メンバー（会員）」は、米国内のほとんどと、カナダ、オーストラリア、ニュージーランドで上下水道サービスを提供しており、英国とオランダの組織にもメンバーシップが開放されている。「ユーティリティ・メンバー」のほか、地方の州政府（米ステート／加プロヴィンス）および連邦機関、法執行機関、諜報機関、DHS、コンサルティング／エンジニアリング会社、およびユーティリティ関連組織がメンバーに含まれる。

また、機密分類されたセキュリティ情報へのアクセスのため、DHS、とりわけ DHS 国家サイバーセキュリティ・コミュニケーション統合センター（DHS National Cybersecurity and Communications Integration Center/NCCIC）、連邦捜査局（Federal Bureau of Investigation/FBI）、EPA、各州情報融合センター（state intelligence fusion centers）、その他連邦・州政府機関との安全かつ緊密な双方向コミュニケーションを維持・確立している。また ISAC 国家評議会（the National Council of ISACs）を通じて約 20 の他の ISACs、とりわけ電力 ISAC とも連携しているほか、厳選されたセキュリティ専門家、上下水道業界団体、ニュースメディア、および WaterISAC メンバーから寄せられるインテリジェンスとリソースを蓄積している。独自の会員向け各種サービスやツイッター（@WaterISAC）等も活用して、随時情報を提供している。

2.1.4. 運営体制

WaterISAC は非営利団体であり、パートナー組織によって任命された上下水道ユーティリティ管理者と州飲料水管理者（drinking water administrators）で構成される理事会（Board of Managers）によって管理され、主にメトロポリタン水道エージェンシー協会（the Association of Metropolitan Water Agencies）の職員の兼務によって運営

整し、これらを破壊・無力化、もしくは悪用する意図的な取り組みの影響を防止、抑止、および軽減する。連邦各省庁は、この目的達成のために州政府、地方政府、および民間セクターと協力する。連邦各省庁は、国土安全保障プログラムが米国の総合的な経済的安全を損なうことがないようにする。連邦各省庁は、2002 年の国土安全保障法およびその他関連法令と一致する重要インフラおよび主要リソースのテロリストによる標的化を容易にするような、自発的に提供された情報および情報処理を含む、本指令の実行に関連する情報を適切に保護する。連邦各省庁は、米国人の権利保護を含め、関連法令の規定と一致する方法で、本指令を実施するものとする。」Cybersecurity & Infrastructure Security Agency (CISA), "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection," [https://www.cisa.gov/homeland-security-presidential-directive-7]（最終検索日：2021 年1月 22 日）。

[8] Homeland Security Presidential Directive 7, 2003。

されている[9]。

図 2 WaterISAC のパートナー組織

理事会（Board of Managers）は、理事長（Chairman）（ボストン上下水道委員会（Boston Water & Sewer Commission）選出の人物）および会計（Treasurer）（テキサス州トリニティ河川局（Trinity River Authority）選出）以下、理事6名（カリフォルニア州水資源管理委員会、タコマ・ウォーター、ケンタッキー州ケーブランド環境局、アメリカン・ウォーター、サウスカロライナ州スパルタンバーグ・ウォーター、デビッドソン・ウォーター株式会社からそれぞれ選出）で構成されている。

また、スタッフ8名（事務局長（Executive Director）、取締役ディレクター（Managing Director）、アカウント担当マネージャー（Manager, Accounts）、庶務・管理担当マネージャー（Manager, Administration）、危機対策・対応担当ディレクター（Director, Preparedness & Response）、メンバー・リレーションズ担当マネージャー（Manager, Member Relations）、レジリエンス・プログラム担当マネージャー（Manager, Resilience Programs）、サイバーセキュリティ・リスク・アナリスト（Cybersecurity Risk Analyst）で構成）を擁する。

【運営主体】

WaterISAC の運営を実質的に担っているのは、メトロポリタン水道エージェンシー協会（the Association of Metropolitan Water Agencies/AMWA）で、米国最大の公営水道供給システム組織（供給人口1億 5600 万人以上[10]）である。AMWA は、大都市の水道事業者による業界団体であり、1981 年に、大規模公営水道事業者の関心が中央政治に反映されることを目指した関係者によって、ワシントン特別区に設立された。AMWA メンバーの代表は、これら大規模水道事業者の経営者（general managers）および CEO である。活動内容は、ユーティリティ管理分野における水道供給事業者のより効果的・効率的な成功を支援する各種プログラム（カンファレンスやウェビナー開催等）、出版物（月曜朝のブリーフィング、月刊の国会レポート、規制関連レポート、持続可能性＆安全性レポート、隔週の「水道ユーティリティ・エクゼクティブ」ニュース、各種調査報告書等）、その他サービスの提供

[9] Association of Metropolitan Water Agencies, “About AMWA,” [https://www.amwa.net/about-amwa]（最終検索日：2021 年1月 22 日）。

[10] AMWA, “About AMWA”。

である。AMWA は、国内全地域を代表する理事会（Board of Directors）によって管理され、ユーティリティ管理・規制・法律・持続可能性・セキュリティに関する各個別委員会が、持続可能な運営や健全な科学と飲料水の安全性を支援する費用対効果の高い法則等に基づく規制を含む、水道供給事業者の目標達成のための専門知識を提供している。

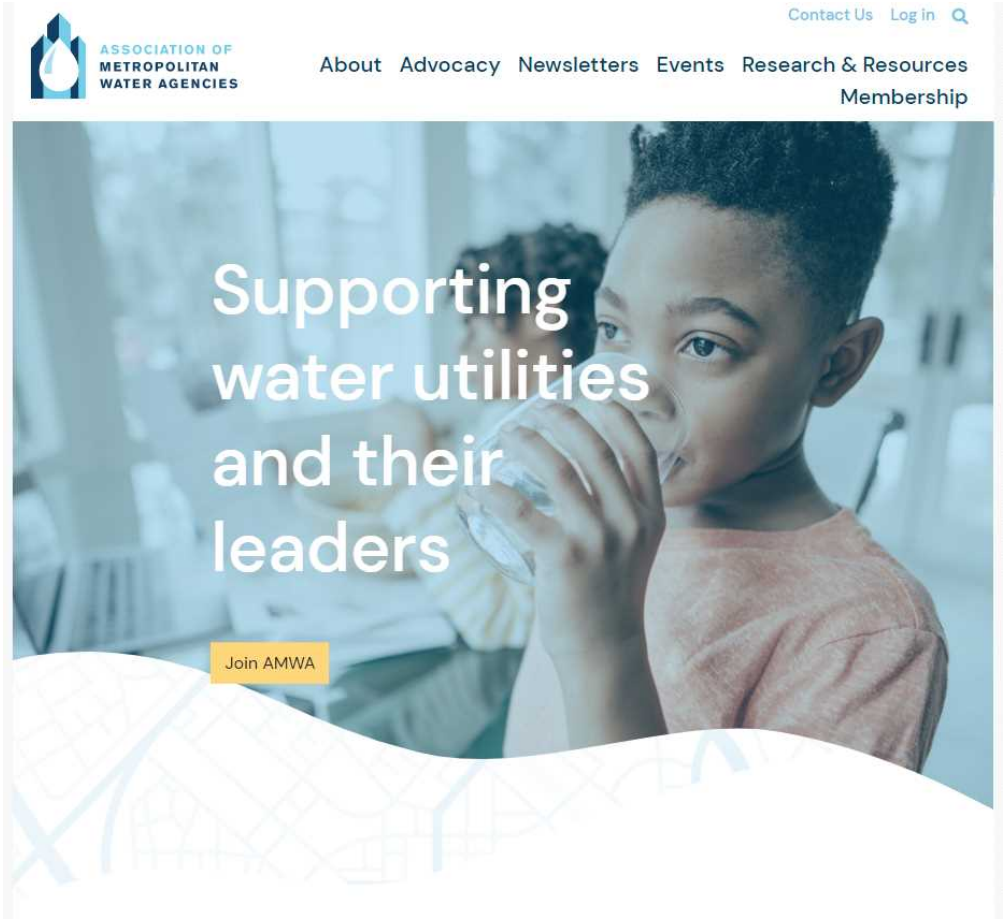


図 3 AMWA の HP

2.1.5. 規約

【WaterISAC メンバーシップ：利用規約（Terms and Conditions）[11]】

1. **センシティブ情報の機密性**：WaterISAC は、セキュリティの観点から、機密的もしくは独占的な情報、物資、知識、および事実（以降、「センシティブ情報」と呼ぶ）を保有あるいは使用、配布、保管する許可を有する。
    a. 「センシティブ情報」の分類レベルには、とりわけ、「機密（Confidential）」、「秘密（Secret）」、「極秘（Top Secret）」、「独占（Proprietary）」、「センシティブ（Sensitive）」、「非常にセンシティブ（Very Sensitive）」、および「公用に限る（For Official Use Only）」、もしくはこれらの組み合わせが含まれる場合がある。
    b. 以下の場合を除き、メンバーは「センシティブ情報」を開示することはできない：
        i. 他の WaterISAC メンバーと共同で、もしくは、

[11] WaterISAC, “Terms and Conditions,” [https://www.waterisac.org/terms-conditions]（最終検索日：2021 年 1 月 22 日）。

ii. 公衆衛生もしくは安全性に対する差し迫った脅威の防止もしくは対応の目的で、他者と共同で。

c. メンバーは、「センシティブ情報」閲覧のためメンバー組織による承認を受け、かつそのような情報を知る必要がある従業員、監督者、代理人、役員、もしくは請負業者にのみ、当該情報を開示することができる。

d. メンバーの組織は、本「利用規約」に記載の状況以外での「センシティブ情報」の配布を防止および禁止するためのプロトコルを導入しなければならない。

2. **より制限的な管理**：メンバーは、「センシティブ情報」に付随する可能性のある、連邦政府およびその他第三者機関によって適用されるものを含む、特定の取り扱い指示に従わなければならない。
3. **商用利用制限**：WaterISAC によって作成された業務成果物は、WaterISAC とのライセンス契約、もしくは WaterISAC の他の書面による明示的な同意がある場合を除き、転売もしくは商業目的で使用することはできない。他の組織によって作成された情報の商用利用は、作成者の商用利用制限の対象となる。
4. **公開開示法令**：メンバーは、パラグラフ1（b）（ii）に規定されている場合を除き、公開から保護することができない「センシティブ情報」の保持、記録、もしくは印刷をすることはできない。
5. **機密情報の返却**：WaterISAC によるいつ何時、いかなる理由による要求に対しても、メンバーは、その所有する形式や媒体を問わず、原本およびすべての複製（コピー）を含む、「センシティブ情報」を返却しなければならない。
6. **メンバーシップの終了**：メンバーは、メンバーシップ終了後も、これらの「利用規約（Terms and Conditions）」の対象であり続ける。
7. **違反**：「センシティブ情報」の無許可開示は、WaterISAC、国および個別の上下水道ユーティリティとその消費者に、WaterISAC がその損害を合理的もしくは適切に補償できない修復不可能な損害を引き起こす可能性がある。したがって、WaterISAC は、そのような開示を防ぐために差止救済を求める権利を有し、本「利用規約」に違反した場合は、WaterISAC のメンバーシップと参加を取り消すことができる。
8. **免責事項**：WaterISAC が提出もしくは配布する情報は、評価も検証もなされていない場合がある。WaterISAC は、そのような情報の正確性、完全性、もしくは最新性に関して、いかなる代理もしくは保証をも行わず、そのような情報に関して、もしくはそれに関連するいかなる責任をも負わないものとする。メンバーは、そのような情報に基づく行動を起こすか否かに関する全責任を独自に負い、かつそれに伴う全リスクおよび負債を自ら引き受ける。

WaterISAC に参加することにより、メンバーは、いかなる修正をも含む、これら「利用規約」を完全に遵守することに合意し、本「合意」の規定を遵守することとする。個人は、WaterISAC メンバーシップのメンバー申請に関連して提供された情報が真実かつ正確であることを確認する。

【メンバーシップ会員資格[12]】

次の条件を満たす場合、WaterISAC への参加資格がある：

1. 参加希望者の職務に、管理、セキュリティ、もしくは緊急時の対応を含む、および
2. 参加希望者は、米国、カナダ、オーストラリア、ニュージーランド、英国、もしくはオランダに拠点を置き、

[12] WaterISAC, “Become A Member,” [https://www.waterisac.org/membership]（最終検索日：2021 年1月 22 日）。

次のいずれかのタイプの組織で就労している:

- 小売もしくは卸売の、上下水道サービス・プロバイダー;
- 水資源、セキュリティ、緊急事態管理、公衆衛生、もしくは環境の健全性もしくは法執行の責務を有する、地方、州政府もしくは連邦政府機関;
- ユーティリティの運営、もしくは管理、あるいは重要インフラ保護プログラムの開発や実施支援のために上下水道ユーティリティと契約した、コンサルティング会社、もしくはエンジニアリング会社;
- 上下水道ユーティリティ業界団体。

3. 参加希望者は、センシティブ情報の取り扱いに関する WaterISAC「利用規約（Terms and Conditions）」に従うことに同意する。

【メンバーシップ会費[13]】

4種類のメンバーシップが設定されており、組織の種類と規模に応じて年会費は 261 米ドル～7,349 米ドルの間で規定されている。会費は米ドルで支払うこととされている。メンバー組織は、WaterISAC のメンバー専用コンテンツへのアクセスと、WaterISAC 各種通信サービス受信のために、任意の数の従業員をサインアップすることができる。

- **ユーティリティ・メンバー**:政府所有、非営利、株式非公開、投資家所有の小売および卸売双方の各水道プロバイダーおよび／もしくは下水道サービス・プロバイダー。

表 1 ユーティリティ・メンバーの会費

供給人口**	水道のみもしくは下水道のみ	上下水道統合システム
20,000 人未満	261 ドル	524 ドル
20,000～49,999 人	524 ドル	1,049 ドル
50,000～99,999 人	1,049 ドル	2,099 ドル
100,000～499,999 人	2,099 ドル	3,149 ドル
500,000～999,999 人	3,149 ドル	5,249 ドル
100 万人以上	5,249 ドル	7,349 ドル

**「供給人口」とは、システムによって直接的・間接的に提供される「個人」（契約口座数やメーター数ではなく）を指す。

- **政府機関メンバー**:公共・民間を問わず、上下水道サービスの全プロバイダーは、メンバーシップの「ユーティリティ」カテゴリーに分類される。この「政府機関」カテゴリーは、「非ユーティリティ」用である。

表 2 政府機関メンバーの会費

組織タイプ	年会費
州・地方（Regional）・地域（Local）政府機関*	524 ドル
国土安全保障省とフュージョン・センター**	該当なし
連邦政府機関	ユーザーあたり 1,049 ドル

* 上下水道事業者は含まない。

[13] WaterISAC, “Become A Member”。

** WaterISAC と脅威およびインシデント情報を共有することをいとわない法執行機関もしくは諜報機関の特別会員制（Courtesy Membership）。

- **コンサルティング＆エンジニアリング・ファーム・メンバー**：ユーティリティの運営もしくは管理、あるいは重要インフラ保護プログラムの開発や実施支援のために上下水道ユーティリティと契約した、コンサルティング会社もしくはエンジニアリング会社。

表 3 コンサルティング＆エンジニアリング・ファーム・メンバーの会費

上下水道事業者への年間売上高	年会費
100 万ドル未満	1,049 ドル
100 万ドルから 1000 万ドル未満	2,099 ドル
1,000 万ドルから 5,000 万ドル未満	3,149 ドル
5,000 万ドルから 1 億ドル未満	4,199 ドル
1 億ドルから 50 万ドル未満	5,249 ドル
5 億ドルから 10 億ドル未満	6,299 ドル
10 億ドル以上	7,349 ドル

- **アソシエーション・メンバー**：主に上下水道ユーティリティおよび／もしくはその職員で構成される非営利団体。年会費は 524 ドル。

【会員特典[14]】

WaterISAC メンバーは、以下を特徴とする包括的プラットフォームへの無制限アクセスによる利益を享受することができる：

- 上下水道システムに対する物理的、サイバー、およびその他の脅威に関する詳細（テロ活動、IT／OT の脅威、自然災害、COVID-19 など新たな脅威）；
- 何千ものリソースを備えた、検索可能な膨大な知識のライブラリー（「WaterISAC リソースセンター」）（脅威分析、緩和戦略、ベストプラクティス、対応と復旧のガイダンス）；
- 水道セクターの脅威分析（6か月ごとに発行、「インシデント・レポート」に基づく分析）；
- リスクを特定および管理するための一連のツール（業界および政府による主要ツールおよびアプリへのリンク）；
- 週2回発行の「WaterISAC セキュリティ＆レジリエンス・アップデート」（上下水道システムのセキュリティをサポートする最新のアドバイザリー、ツール、レポート、ニュース）；
- モバイルデバイスによる WaterISAC へのフルアクセス（外出先で WaterISAC コンテンツにアクセスし、アカウントの管理が可能）；
- セキュリティの専門家を特集したブリーフィングとウェビナー（WaterISAC、DHS、および民間サイバーセキュリティ企業のアナリストによる、毎月のサイバー脅威ウェブ・ブリーフィング；ユーティリティを保護し、災害やその他の危険への対処に役立つ各種ウェビナー開催）；

[14] WaterISAC, “Become A Member”。

- 保健衛生および環境に脅威を与える化学／生物汚染物質のデータベース（700 を超える汚染物質を含む、3つの化学／生物データベースへのシームレスなアクセス；脅威、インシデント、流出への対応に貢献）。

【メンバーシップ加盟方法】

オンライン上のフォームメール（以下画像参照）で情報登録し、会員資格の有無等に基づく審査の後、メンバーシップが承認されると、WaterISAC から電子メールでアカウントへのアクセスが提供される。また、60 日間のトライアルも利用することができる。

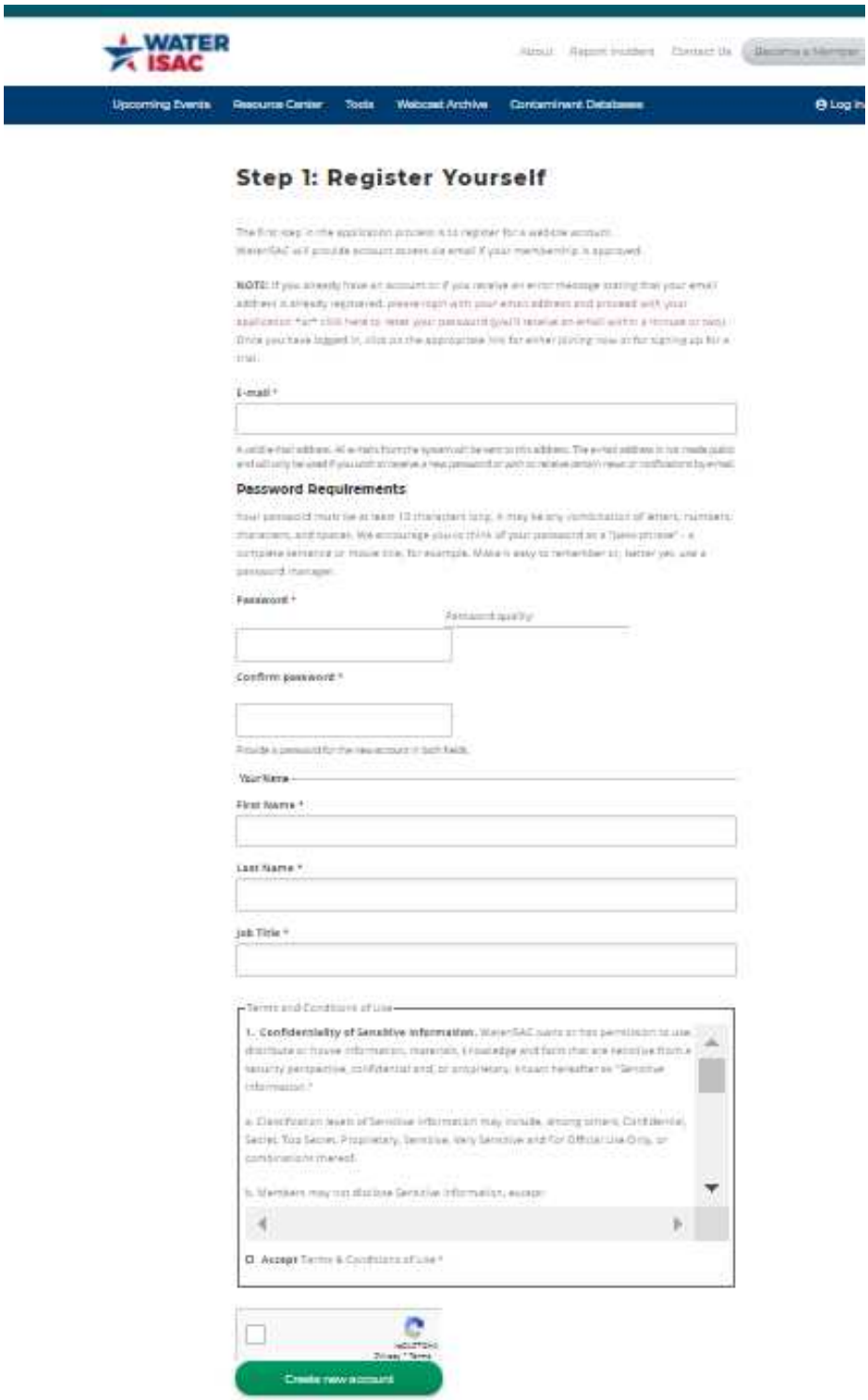


図 4 メンバーシップへの申込フォーマット

2.1.6. 活動内容

【情報発信】

会員特典には、6か月ごとに発行される水道セクターの「脅威分析（Threat Analyses」）（インシデント・レポート（四半期ごとの「インシデント・サマリー」）に基づく分析）、隔週発行の「WaterISAC セキュリティ＆レジリエンス・ア

ップデート」、セキュリティ専門家によるブリーフィングやウェビナー（月刊のサイバー脅威ウェブ・ブリーフィングと各種ウェビナー）などの情報発信サービスが含まれる。

このほか、「週次フラッシュポイント・インテリジェンス・レポート」（メンバーのみ）、最近被害が拡大している「SolarWinds」（ソフトウェア会社）のネットワーク監視＆管理ソフトウェア（“Orion”）に関する一連のアップデート（SolarWinds 製品経由でのサイバー攻撃とその影響に関する理解促進、および対応と復旧アクションの通知のため、連邦政府パートナー（Cybersecurity and Infrastructure Security Agency/CISA、FBI、National Security Agency/NSA）およびサイバーセキュリティ会社（SolarWinds、FireEye、他）から入手した情報および推奨事項（「リソース」）と、最新の「デイリー・アップデート」および関連する過去の勧告等（必要に応じて随時更新される「アップデート」から成る）、その他の関連業界情報等がウェブ上で公開されている（一部メンバー限定）。また最新情報は、ツイッター（@WaterISAC）でも随時発信されている。

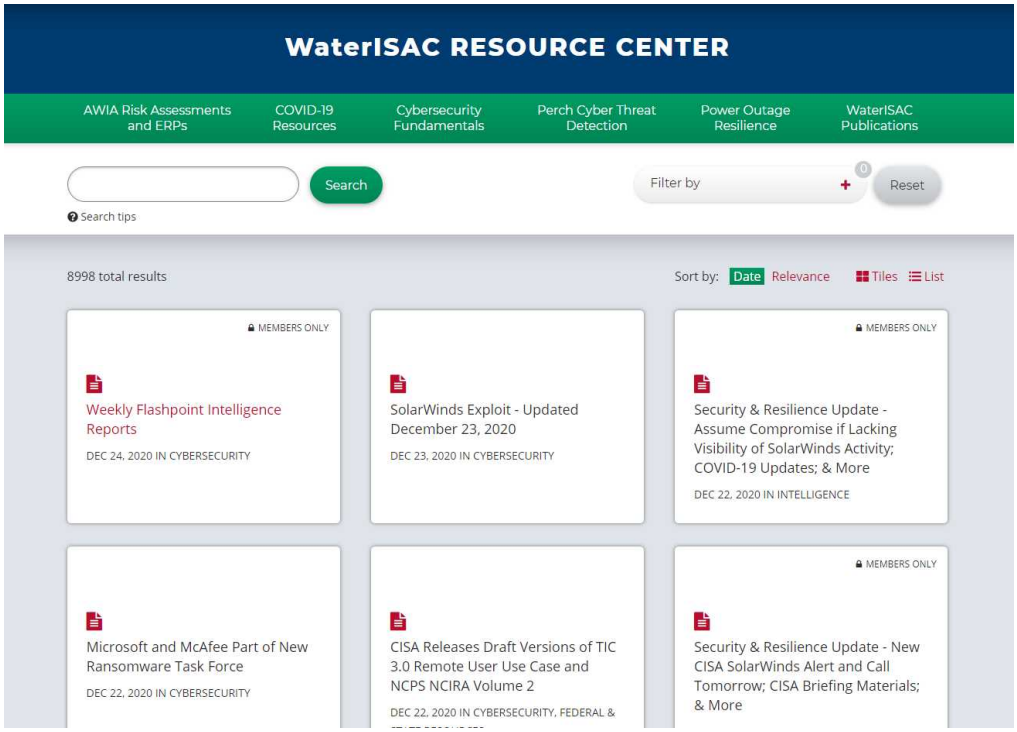


図 5 HP 上での情報公開イメージ

また WaterISAC は、一部のセキュリティベンダーが開発・提供する、上下水道に特化したサイバー脅威の迅速な検出やスムーズな情報共有を目的とした、以下のサイバー・セキュリティ・インテリジェンス（CTI）製品（Perch Security）と提携している[15]。

[15] WaterISAC, “Perch Security - Threat Detection + SIEM + SOC,” [https://www.waterisac.org/portal/perch-security]（最終検索日：2021 年 1 月 22 日）。

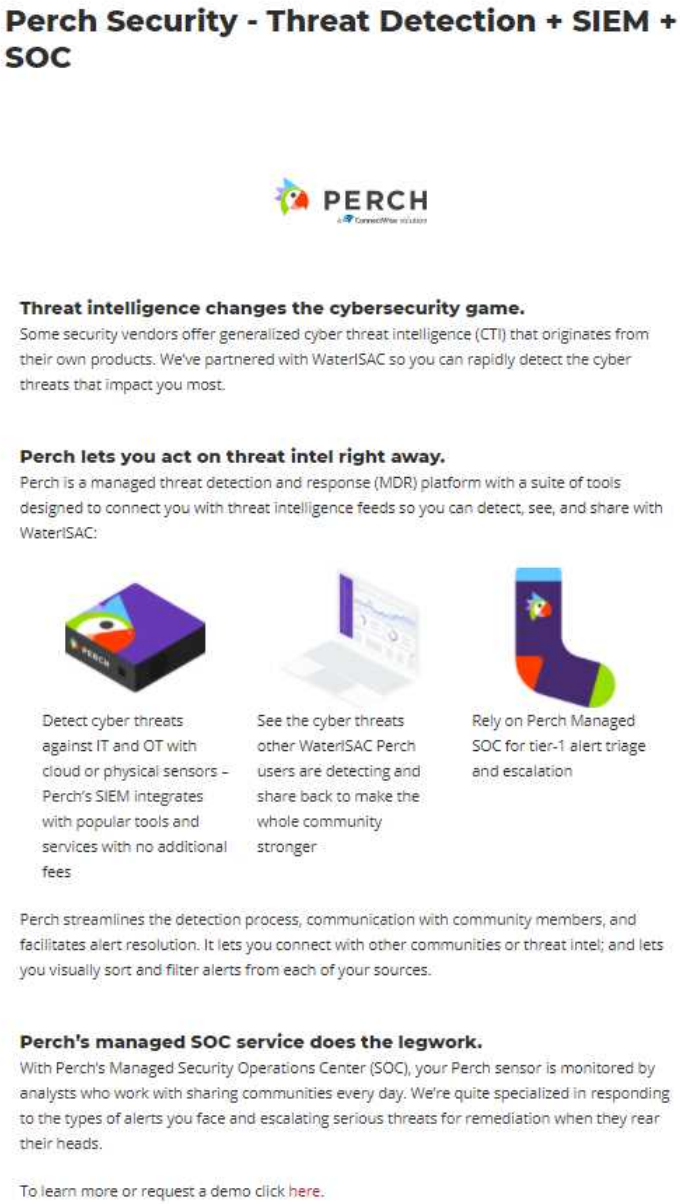


図 6 WaterISAC HP 上でのサイバー・セキュリティ・インテリジェンス製品紹介

【上下水道安全性管理の各種関連リソースへの一元的アクセス】

WaterISAC は、「上下水道ユーティリティのサイバーセキュリティ 15 の基礎」[16]において基礎的なサイバーセキュリティ対策の指針の提供や、ユーティリティによる緊急対応計画や標準操作手順、水道研究所同盟対応計画

[16] 上下水道ユーティリティのサイバーセキュリティ 15 の基礎:「1. 資産インベントリーの実行、2. リスク評価、3. 制御システムの露出を最小限に抑える、4. ユーザーアクセス制御の実施、5. 不正な物理的アクセスからの保護、6. 独立したサイバーフィジカル安全システムのインストール、7. 脆弱性管理の採用、8. サイバーセキュリティ文化の構築、9. サイバーセキュリティのポリシーと手順の開発・実施、10. 脅威の検出と監視の導入、11. インシデント・緊急事態・災害の各計画作成、12. インサイダー脅威への取り組み、13. サプライチェーンの確保、14. すべてのスマートデバイス(IoT、IIoT、モバイルなど)への対応、15. 情報共有とコラボレーションコミュニティへの参加。」WaterISAC, "15 Cybersecurity Fundamentals for Water and Wastewater Utilities" (June 3, 2019 - 13:26) [https://www.waterisac.org/fundamentals](最終検索日:2021 年1月 22 日)。

（WLA-RP）等の作成支援のための EPA による「分析的準備対策大演習（AP-FSE）ツールキット」[17]、重要インフラ業界に対する通常業務運用の維持と中断時の復旧促進のための各種演習を含む FEMA による「業務遂行計画セット」[18]など、WaterISAC と政府関連機関が提供する各種ツールをウェブ上で公開している。

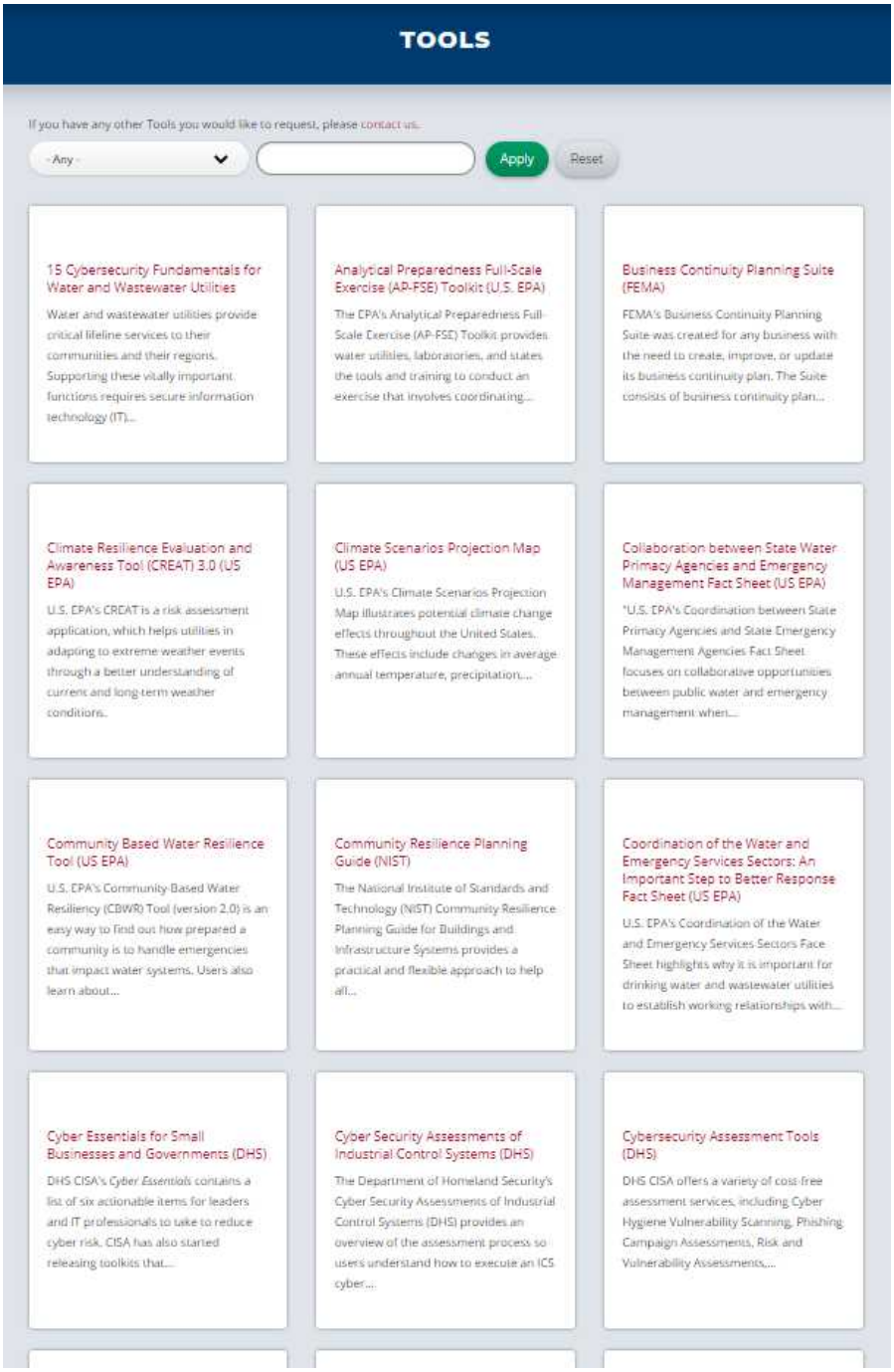


図 7 WaterIsac HP で公開している各種ツール

[17] WaterISAC, "Analytical Preparedness Full-Scale Exercise (AP-FSE) Toolkit (U.S. EPA)," Thursday, September 27, 2018 - 17:05, [https://www.waterisac.org/portal/analytical-preparedness-full-scale-exercise-ap-fse-toolkit-us-epa]（最終検索日：2021 年 1 月 22 日）。

[18] WaterISAC, "Business Continuity Planning Suite (FEMA)," Monday, September 4, 2017 - 15:26, [https://www.waterisac.org/portal/business-continuity-planning-suite-fema]（最終検索日：2021 年 1 月 22 日）。

また、「汚染物質データベース」ページ[19]は、上下水道汚染事案に関する「US EPA Water Contaminant Information Tool（WCIT）」（米国メンバーのみ）、英国 WRC plc が管理する 600 を超える化学物質情報である「UKWIR 毒性データシート（UKWIR Toxicity Datasheets）」、そして WRC と英国 Health Protection Agency/HPA が管理する微生物情報である「UKWIR 微生物学データシート（UKWIR Microbiology Datasheets）」の3つの主要汚染物質データベースへのアクセスの入口となっている。メンバーは、再度サインインすることなくこれらデータベースにアクセスが可能で、WaterISAC のホームページはこうした上下水道の安全性管理の関連各種リソースへのアクセスを一元的に集約した、利便性の高いサイトとなっている。

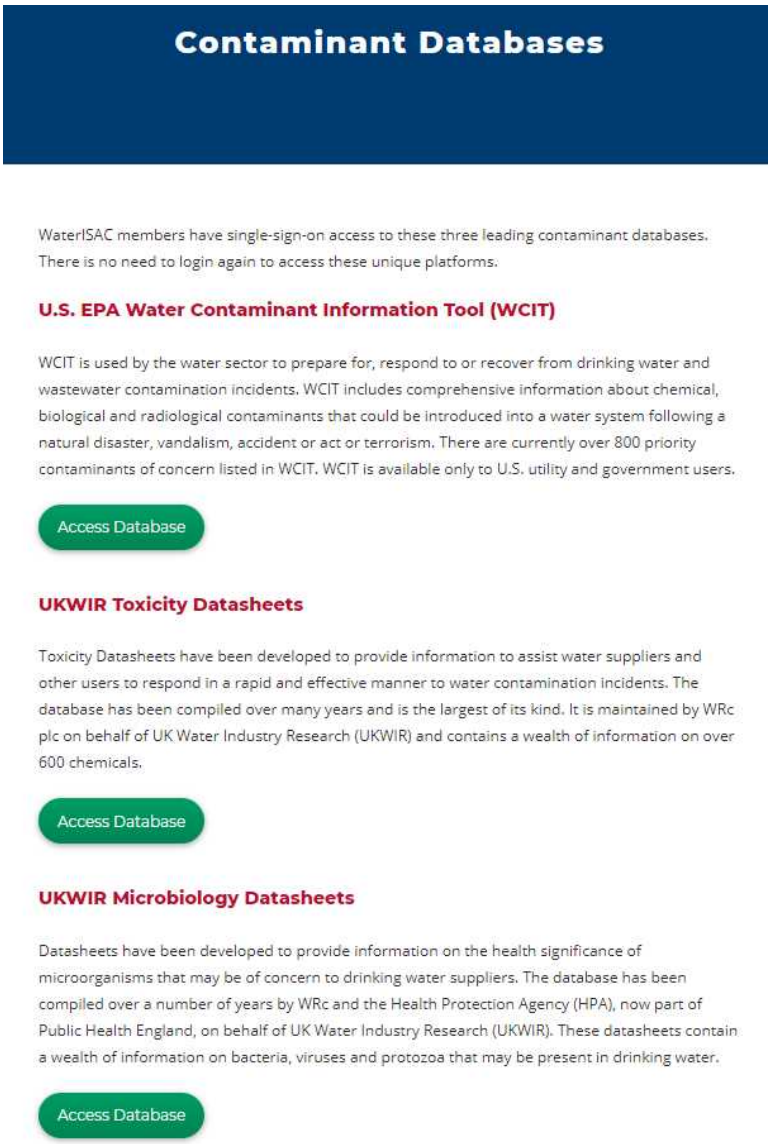


図 8 汚染物質データベース

【機密事案報告フォーム[20]】

各メンバーからの報告以外にも、ウェブ上のフォームメール（以下画像参照）や電話（866-H2O-ISAC）、電子メ

[19] WaterISAC, “Contaminant Databases,” [https://www.waterisac.org/portal/contaminant-databases]（最終検索日：2021 年1月 22 日）。

[20] WaterISAC, “Confidential Incident Reporting Form,” [https://www.waterisac.org/report-incident]（最終検索日：2021 年1月 22 日）。

ール（analyst @ waterisac.org）を使用した匿名による通報も可能となっている。報告機関、部門、会社、もしくは個人の身元に関する情報は機密情報として取り扱われ、通報を受領次第、WaterISAC アナリストがコンタクトを取る。またフォームの一部フィールド（赤字※以外）は、匿名性保持のため空白にすることができる。

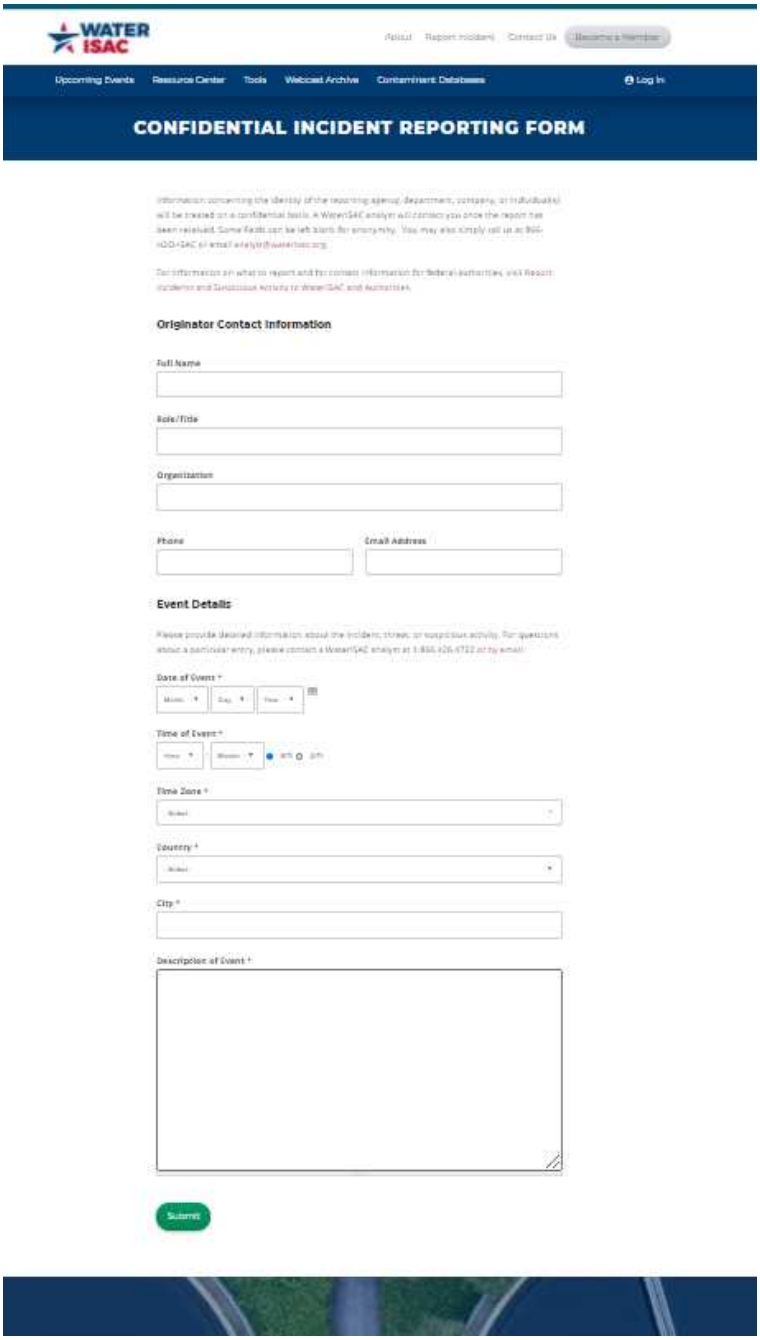


図 9 WaterIsac への機密事項報告フォーム

通報すべき内容および連邦当局の連絡先については、WaterISAC および当局への「サイバー脅威事案もしくは疑わしい活動の通報」に、以下のような詳細が記載されている[21]:

WaterISAC は、ユーティリティおよび上下水道セクターのその他ステークホルダーに、サイバー脅威事案もしく

[21] WaterISAC, “Report Incidents and Suspicious Activity to WaterISAC and Authorities,” [https://www.waterisac.org/report-incidents-and-suspicious-activity-waterisac-and-authorities]（最終検索日：2021 年 1 月 22 日）。

は疑わしい活動についてアナリストに通報するよう要請している。この通報により、WaterISAC が脅威とレジリエンスを識別し、他のメンバーやパートナーに警告することができ、セクターのレジリエンス強化に役立つ。共有される情報は、WaterISAC によるウェビナーやレポートなどの製品やサービスの形成にも役立ち、ユーティリティの安全性維持に役立つ。

WaterISAC は提供情報の機密性を維持する。WaterISAC が分析もしくは他の製品において当該事案を共有しようとする場合、WaterISAC は最初に情報提供者の明示的な許可を確保し、次に共有情報を匿名化する。民間の非営利団体である WaterISAC は公記録法（public records law）の非対象主体であり、レポートの機密性をさらに保護することができる。

場合によっては、とりわけ提供者が調査もしくは復旧への支援を求める場合には、WaterISAC はサイバー脅威事案もしくはその疑いがある事案について連邦当局への通報を推奨する場合がある。WaterISAC は、連絡先情報やその他のガイダンスを提供することにより支援が可能である。犯罪は、常に適切な当局に報告されるべきである。

WaterISAC が求める通報内容は、サイバーセキュリティ事案と物理的事案の両方、および疑わしい活動に関するものである：

- サイバーセキュリティ事案：企業の IT システムもしくは産業用制御システムのサイバー攻撃もしくは侵害であり、以下の事象を指す：
  - ✓ ランサムウェア攻撃もしくはクロース・コール［ヒヤリハット、間一髪］の成功；
  - ✓ マルウェアのインストールが成功し、ユーティリティのビジネス遂行や運用能力に影響を与えた、もしくは影響を与えた可能性があるもの；
  - ✓ エグゼクティブ、エグゼクティブ・アシスタント、SCADA エンジニア、IT 管理者、もしくはその他特権ユーザーへのスピア・フィッシングの成功もしくは未遂を含む、フィッシング・キャンペーン；
  - ✓ アカウントの乗っ取りや経営幹部のなりすましなど、ビジネスメールの侵害の成功もしくは試み；
  - ✓ データの盗難；
  - ✓ ソーシャル・エンジニアリングが、担当者から機密情報の収集を試みたもの。
- 物理的セキュリティ事案：次のいずれかの誘発を目的とした事案を含む：
  - ✓ 従業員もしくは顧客への身体的危害；
  - ✓ 公衆衛生への影響；
  - ✓ 環境への重大な損害；
  - ✓ ユーティリティの運用への影響；
  - ✓ 組織への 10,000 ドル以上（事案あたり）の経済的損失。

  これらの事案の具体例は以下のとおり：
  - ✓ 意図的な給排水の汚染；
  - ✓ 妨害／改ざん；
  - ✓ 盗難；
  - ✓ 暴行；
  - ✓ 監視もしくは疑わしい質問；
  - ✓ 脅威。

情報提供者がサイバー脅威事案もしくは疑わしい活動について通報すると、WaterISAC は詳細をフォローアッ

プし、WaterISAC レポートに当該情報を掲載してもよいか承諾を得る。答えが「了承」の場合、当該事案の提供者もしくは提供者の所属ユーティリティに帰する個別の詳細を削除し、共有情報を匿名化する。共有情報は、保護データベースに保存され、匿名化された情報は WaterISAC 脅威分析レポートに通知するため使用される。

【連邦およびその他の報告メカニズム】

- アメリカ

国土安全保障省国立サイバーセキュリティ・通信統合センター（DHS National Cybersecurity and Communications Integration Center/NCCIC）に電子メール（NCCICCUSTOMERSERVICE@hq.dhs.gov）か電話（888-282-0870）で当該情報を報告する。DHS は、要望があれば、チームと共有される機密情報を保護することができる。事案が発生し、NCCIC との直接的なコンタクトを WaterISAC に調整依頼する場合は、電子メール（analyst @ waterisac.org）もしくは電話（866-H2O-ISAC）で要請する。

NCCIC の「追跡＆事案対応チーム（Hunt and Incident Response Team）」は、サイバー侵害の即時調査と解決を必要とする組織に、オンサイトのインシデント対応を無料提供している。

連邦捜査局（FBI）は、インターネット犯罪の被害者が FBI の現地事務所に連絡することを奨励している。犯罪の苦情は、www.ic3.gov にある FBI インターネット犯罪苦情センター（IC3）に申し立てることもできる。

- オーストラリア

オーストラリアのユーティリティは、電話（1300-CYBER1）もしくは電子メール（info @ cert.gov.au）により、オーストラリアのサイバーセキュリティセンターの一部門である CERT オーストラリアに事案を報告することができる。

- カナダ

カナダのユーティリティは、電話（1-833-CYBER-88）もしくは電子メール（contact @ cyber.gc.ca）により、カナダ・サイバー・インシデント・レスポンス・センターに事案を報告することができる。

2.1.7. 具体事例（フロリダにおけるハッキング事案）

【事案概要】

2021 年 2 月 5 日、米国フロリダ州タンパ近郊のオールズマー（Oldsmar）市（※タンパベイ・ウォーター社が水道供給元）において、水道局のコンピューター（SCADA コントロール・システムを導入）に2回に分けて異常なアクセスがあり、水質調整用薬剤である苛性ソーダ（sodium hydroxide）を通常の約 100 倍（100 ppm から 11,100 ppm）に増やすという“ハッキング事案”が発生した[22]。監視員が異常な水質の発生をすぐに察知し対処したため、直接的な被害はなかった[23] ものの、監視員は「突然コンピューターに誰かが遠隔アクセスしているとのポップア

[22] Dale Greenstein, “Hacker Changed Chemical Levels at Florida Water Treatment Plant, Sheriff Says,” *Spectrum Bay News 9*, 2:03 PM ET FEB. 08, 2021, [https://www.baynews9.com/fl/tampa/news/2021/02/08/pinellas-sheriff--hacker-changed-chemical-levels-at-city-s-water-treatment-plant?web=1&wdLOR=c48266931-C898-4CC3-B87D-6616A2C616A5]（最終検索日：2021 年3月 11 日）。

[23] 水道局側は、「仮に誰も異常値に気づかなかったとしても、汚染された水が飲料水として市内に届くまでには丸１日以上かかるため、被害が発生することはなかっただろう」と述べ、また「水の pH 値が異常になれば監視システム上で警報装置が作動するため、問題の水が市民に供給されることはありえない」と述べている。しかし、「今回の事例は「SolarWinds」IT 管理ソフトウェアを通じた約1万 8000 企業へのハッキング事案と比較すると規模も被害も小さなものだが、もし監視体制が脆弱で異常値検出用システムまで無効化されていた場合は、地域の1万 5000 人の健康被害問題

ップ表示が出て、すぐにマウスカーソルが勝手に動いて苛性ソーダの添加量を 100 倍に設定したと報告」した[24]。当時、同水道局のコンピューターは、メンテナンスのために TeamViewer と呼ばれるリモートデスクトップ・ソフトウェアによる遠隔操作が可能な状態に設定されており、権限を持つ人物であればアクセス可能であったため、今回の操作を行っていた人物は当該コンピューターの設定を知っており、既に相応の権限を奪っていたものと考えられている。

通報を受けた現地警察当局は、FBI のサイバーユニットと米国シークレットサービスにも協力を要請し、直ちに犯罪捜査を開始した[25]。いくつかの心当たりが捜索されたものの該当人物の逮捕には至っておらず、また攻撃者の物理的アクセスポイント（IP アドレス）の特定（米国内からか国外からか）、犯行の動機・意図（なぜオールズマー市の水道システムが狙い撃ちされたのか）、他地域の水道システムにも同様の危険が迫っているのか、当該人物の知的・IT レベル等についても不明なままであるとしている。

【WaterISAC の対応】

WaterISAC は本件について、２月８日夜時点で第一報[26]を HP で公開し、本件は残念な事案ではあるものの、ICS（産業コントロール・システム）のサイバーセキュリティ・コミュニティではこうした事案発生を長年警告しており、WaterISAC の「上下水道ユーティリティのサイバーセキュリティ 15 の基礎」にも「想定し得るシナリオ」として「化学物質追加の試み」参照例が記載されていること、またその中で、プロセス機器への物理的アクセスの防止とそれぞれ独立したサイバー及び物理的な安全性システムの導入により対処できると注意喚起している。また、WaterISAC からの続報を待つ間にも、以下の対策の実施を推奨している:

- 悪意のあるユーザーが行う前に、インターネット検索を使用して、ネットワーク上のインターネットにアクセス可能な OT デバイスを特定する。
- ネットワーク・セグメンテーションを導入する。
- リモートアクセスがどうしても必要な場合は、安全に構成された VPN を使用する。
- ホワイトリストやジオ・ブロッキングなどの方法でトラフィックをフィルタリングして、許可されていない人や場所からのアクセスを防ぐ。
- トラフィックを暗号化する。
- 簡単すぎない認証方法を使用する。
- 強力なパスワードを適用する。
- タスク実行のための絶対に必要な人のみに特権を与えるユーザーアカウントのアクセス網を構成する。

このほか、不審な事案や疑わしい活動を発見したメンバーに対し、まず現地関連当局へ通報し、それから

に至っていた可能性もゼロとは言い切れない。」 Munenori Taniguchi「フロリダの水道局システムがハッキング、飲料水に 100 倍の薬剤投入　幸いにも被害はなし」、*Engadget* 日本版、2021 年 02 月 9 日午後 12:30、[https://japanese.engadget.com/hackers-contaminate-florida-water-supply-033022797.html?guccounter=1]（最終検索日：2021 年３月 11 日）。

[24] Engadget 日本版 2021 年２月９日記事。

[25] Pinellas Sheriff, “Treatment Plant Intrusion Press Conference,” *YouTube*, 2021/02/09 [https://www.youtube.com/watch?v=MkXDSOgLQ6M]（最終検索日：2021 年３月 11 日）。

[26] WaterISAC, “Malicious Actor Compromises U.S. Water Treatment Plant, Changes Chemical Level,” Monday, February 8, 2021, 18:52, [https://www.waterisac.org/portal/malicious-actor-compromises-us-water-treatment-plant-changes-chemical-level]（最終検索日：2021 年 3 月 11 日）。）

WaterISAC への情報提供を依頼している。

また、翌日の続報において、WaterISAC は今回の行動に及んだ“ハッカー”について、「洗練性を欠いている（a lack of sophistication on the part of the “actor”）」と評し[27]、計画的に企図した行動というよりは日和見的、だが最初のアクセス時（朝8時）にオールズマーのシステムにおいてどこをどのように操作すると重要箇所の変更が可能かを発見し、2回目のアクセス時（午後1時半頃）にそれを実行するに至る程度には IT に習熟している人物であると推察している。さらに、ひょっとすると正当に権限を保有する人物による適正な操作であったかもしれず、人的エラーによる数値入力ミスの可能性も捨てきれないとしている。いずれにせよ、重要インフラのリモートアクセスにおける更なる強固な安全性確保が急務であることは疑う余地はなく、2020 年に発生したイスラエルの水インフラへのサイバーテロ攻撃と同様、米国に対してもこうした攻撃は起こり得ると警告し、改めて基本的な対策の徹底を推奨している。

更に、3月2日の WaterISAC 続報[28]では、依然として「オールズマー事案」の犯人や動機等は不明ながらも、米国内で極右勢力や過激派の台頭とともにこうした事案が注目を集めており、「ベース（the Base）」と呼ばれる暴力的白人至上主義者グループの創設者が「テレグラム」メッセンジャーへ、「水中への毒物混入の陰謀は、より大きな何かを可能にするテンプレートである」と書き込みをした、と報じた『ニューヨークタイムズ』紙の記事[29]を紹介している。

なお、この「フロリダ水道処理場ハッキング事案」については、様々なサイバー関連ニュースサイト等で重要インフラに対するリモートアクセス環境下のセキュリティ対策不備（リモートアクセス用パスワードが全端末で同一だったこと、いかなるファイアーウォール等の保護措置もとられていなかったこと、不満を持つ元従業員であれば容易に実行可能な行動であること、TeamViewer ソフトウェアの使用を半年前に停止したにもかかわらずインストールしたままにしていたこと、マイクロソフト社がセキュリティ・アップデートのサポートを停止した Windows 7 を未だに使用していたこと等）についての多数の批判と、その一方で、小規模公共ユーティリティにおける共通の課題（インフラ設備の老朽化、低予算、専門性を有する従業員の不足、セキュリティシステム制御力の欠如によるサードパーティーへの丸投げ等）への懸念の声が上がっている[30]。

---

[27] Water ISAC, “Considerations Regarding Oldsmar, Florida Water Treatment Plant Compromise,” Tuesday, February 9, 2021, 14:43, [https://www.waterisac.org/portal/considerations-regarding-oldsmar-florida-water-treatment-plant-compromise]（最終検索日：2021 年 3 月 11 日）。

[28] WaterISAC, “Greater Preparedness and Security in Light of Oldsmar, Regardless of Intent or Motivation,” Tuesday, March 2, 2021, 12:26, [https://www.waterisac.org/portal/greater-preparedness-and-security-light-oldsmar-regardless-intent-or-motivation]（最終検索日：2021 年 3 月 11 日）。

[29] “Mr. Nazzaro, out of the reach of U.S. law enforcement in Russia, wrote on Telegram that the water poisoning plot was a possible template for something larger.” In Neil MacFarquhar, “Far-Right Groups Are Splintering in Wake of the Capitol Riot,” *The New York Times*, Published March 1, 2021, Updated March 3, 2021, [https://www.nytimes.com/2021/03/01/us/extremism-capitol-riot.html]（最終検索日：2021 年 3 月 11 日）。

[30] Sean Hollister and Mitchell Clark, “Turns out that Florida water treatment facility left the doors wide open for hackers: Can you even call this a hack?” *The Verge*, Feb 10, 2021, 7:46pm EST, [https://www.theverge.com/2021/2/10/22277300/florida-water-treatment-chemical-tamper-teamviewer-shared-password]（最終検索日：2021 年 3 月 12 日）。その後の CyberNews 等の調査により、オールズマー水道処理場の関係者のものと思われる 11 セットの個人情報を含む、COMB（“compilation of many breaches”）と呼ばれる侵害されたユーザー名・パスワードの膨大な一式（32.7 億セット）が、本件発生数日前の2月2日にオンライン上でリークされていることが判明している。本件との直接的な関連性は不明ながらも、オールズマー以外の処理場関連のクレデンシャル情報もリークされている点は特筆すべき現象であるとのこと。Elizabeth Montalbano, “Florida Water Plant Hack: Leaked Credentials Found in Breach Database,” *ThreatPost*, February 12, 2021, 10:34 am, [https://threatpost.com/florida-water-plant-hack-credentials-

2.2. 国内事例調査

我が国においては、サイバーセキュリティ基本法をはじめとして、サイバーセキュリティに関して各種施策が進められてきた。重要インフラ分野においては、情報通信、電力、金融、交通の4分野で ISAC が設立されている。

2.2.1. 国内サイバーセキュリティの動向

【サイバーセキュリティ基本法】

サイバーセキュリティ基本法は、2014 年（平成 26 年）に成立し、2015 年（平成 27 年）1月から施行されている[31]。この法律は、サイバーセキュリティに関する施策を総合的かつ効率的に推進するため、基本理念や国の責務、サイバーセキュリティ戦略をはじめとする施策の基本となる事項を規定したものである。ただし、あくまで“基本”を示したものであり、具体的な戦略は「内閣サイバーセキュリティセンター（NISC）」（後述）の活動や他の法律にゆだねられている。

◆基本理念

サイバーセキュリティ基本法では、以下のとおり基本理念を第3条で示しており、これらの理念のもと、施策が実施されることとしている。

- 情報の自由な流通の確保を基本に、官民が連携して積極的に対応すること
- 国民1人ひとりがサイバーセキュリティに関する認識を深め、自発的な対応をすること、強靭な体制を構築すること
- 高度情報通信ネットワークの整備および IT の活用によって活力ある経済社会を構築すること
- サイバーセキュリティに関する国際的な秩序の形成等のために先導的な役割を担い、国際的協調の下に実施すること
- 国民の権利を不当に侵害しないこと

【内閣サイバーセキュリティセンター（NISC）】

2015 年（平成 27 年）1月、同法に基づき内閣に「サイバーセキュリティ戦略本部」が設置された。同本部は、内閣官房長官をはじめとする関係閣僚や有識者によって構成されている。内閣官房組織令により内閣官房に内閣サイバーセキュリティセンターを置き、事務局は従来の「情報セキュリティセンター（NISC）」を改め、「内閣サイバーセキュリティセンター（NISC）」を組織した。内閣サイバーセキュリティセンターは内閣官房組織令第4条において次の事務をつかさどると定められている。

- 情報通信ネットワーク又は電磁的記録媒体を通じて行われる行政各部の情報システムに対する不正な活動の監視及び分析に関すること。
- 行政各部におけるサイバーセキュリティの確保に支障を及ぼし、又は及ぼすおそれがある重大な事象の原因究明のための調査に関すること（内閣情報調査室においてつかさどるものを除く。）。
- 行政各部におけるサイバーセキュリティの確保に関し必要な助言、情報の提供その他の援助に関するこ

---

breach/163919/]; Bernard Meyer, “Oldsmar, Florida water facility credentials contained in COMB data leak,” *Cybernews*, 11 February 2021, [https://cybernews.com/news/oldsmar-florida-water-facility-credentials-contained-in-comb-data-leak/]（最終検索日：2021 年 3 月 12 日）。

[31] サイバーセキュリティ基本法 [https://elaws.e-gov.go.jp/document?lawid=426AC1000000104]（最終検索日：2021 年1月 22 日）。

と。

- 行政各部におけるサイバーセキュリティの確保に関し必要な監査に関すること。
- 行政各部の施策に関するその統一保持上必要な企画及び立案並びに総合調整に関する事務のうちサイバーセキュリティの確保に関するもの（国家安全保障局、内閣広報室及び内閣情報調査室においてつかさどるものを除く。）

◆NISC の活動

2015 年 9 月に閣議決定された「サイバーセキュリティ戦略」は、我が国のサイバーセキュリティに関する国家戦略である。NISC では本戦略に基づき、サイバーセキュリティ政策に関する総合調整を行いつつ、「自由、公正かつ安全なサイバー空間」の創出に向け、下記グループの活動[32]をしている。

- 基本戦略グループ
  - ✓ サイバーセキュリティ政策に関する中長期計画や年度計画の立案
  - ✓ 国際戦略グループ
  - ✓ サイバーセキュリティ政策に関する国際連携の窓口機能
  - ✓ 政府機関総合対策グループ
  - ✓ 政府機関等の情報セキュリティ対策を推進するための統一的な基準の策定、運用及び監査
- 情報統括グループ
  - ✓ サイバー攻撃等に関する最新情報の収集・集約
  - ✓ 政府関係機関情報セキュリティ横断監視・即応調整チーム（GSOC）の運用
- 重要インフラグループ
  - ✓ 重要インフラ行動計画に基づく情報セキュリティ対策の官民連携
  - ✓ サイバーセキュリティ技術動向等の調査・研究分析
- 事案対処分析グループ
  - ✓ 標的型メール及び不正プログラムの分析
  - ✓ その他サイバー攻撃事案の調査分析
- 東京 2020 グループ
  - ✓ 2020 年東京オリンピック・パラリンピック競技大会に向けたサイバーセキュリティ対策の推進

◆重要インフラ分野

「重要インフラ」とは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるものをいう。

第４次行動計画では、「重要インフラ分野」として、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」及び「石油」の 14 分野を特定している。

重要インフラグループは、我が国の国民生活と社会経済活動が大きく依存する重要インフラの情報セキュリテ

[32] 内閣サイバーセキュリティセンター「活動内容」 [https://www.nisc.go.jp/active/index.html]（最終検索日：2021 年1月 22 日）。

ィ対策を推進するため、「サイバーセキュリティ戦略」及び「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」（第4次行動計画）に基づき、次に示す5つの施策を進めている。

- 安全基準等の整備及び浸透
  重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進
- 情報共有体制の強化
  連絡形態の多様化や共有情報の明確化等による官民・分野横断的な情報共有体制の強化
- 障害対応体制の強化
  官民が連携して行う演習等の実施、演習・訓練間の連携による重要インフラサービス障害対応体制の総合的な強化
- リスクマネジメント
  リスク評価やコンティンジェンシープラン策定等の対処態勢の整備を含む包括的なマネジメントの推進
- 防護基盤の強化
  重要インフラに係る防護範囲の見直し、広報広聴活動、国際連携の推進、経営層への働きかけ、人材育成等の推進

◆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）と呼んでいる。

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してる。これによって、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る。

平成 29（2017）年4月現在、各重要インフラ分野の業界団体等が事務局となって、全 13 分野で、計 18 のセプターが活動している。

◆セプターカウンシル

セプターカウンシルは、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です。分野横断的な情報共有の推進を目的として、平成 21（2009）年 2 月 26 日に設立された。

重要インフラのIT障害の未然防止等のため、重要インフラ事業者等に密接に関連する情報を提供するための体制の調整及び管理に取り組むとともに、具体的な情報共有プロジェクトとして、Web サイト応答時間計測システム（HP レスポンス観測活動）や C4TAP（セプターカウンシルにおける標的型攻撃に関する情報共有体制）を運用し、情報共有を推進してる。

なお、セプターカウンシルは、政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体であって、各セプターの主体的な判断によって、セプター間での情報共有等を行っています。NISC はセプターと連携しつつ、セプターカウンシルの運営及び活動に対する支援を実施している。

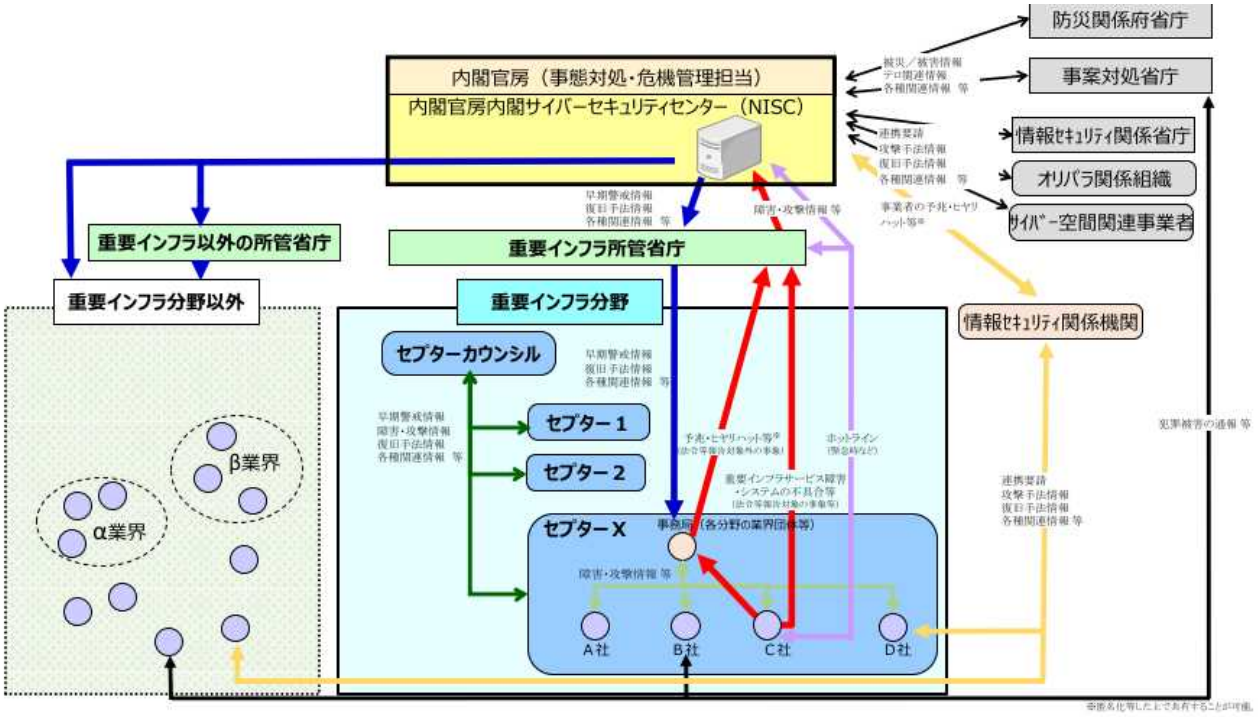


図 10 国内セプター活動の情報共有体制

表 4 情報共有体制における各主体の役割

関係主体	平時における各関係主体の役割	大規模重要インフラサービス障害対応時における※各関係主体の役割
○ 内閣官房（事態対処・危機管理担当）	重要インフラに関連する事案の情報につき、ＮＩＳＣと相互に情報の共有を行う。	平時の役割に加え、ＮＩＳＣと一体化し、事案対処省庁及び防災関係府省庁から提供される被害情報、対応状況情報等を集約し、ＮＩＳＣと相互に情報の共有を行う。
○ 内閣官房（ＮＩＳＣ）	重要インフラ所管省庁、情報セキュリティ関係省庁、事案対処省庁、防災関係府省、情報セキュリティ関係機関及びサイバー空間関連事業者等と相互にシステムの不具合等に関する情報の共有を行う。	内閣官房（事態対処・危機管理担当）と一体化し、重要インフラ所管省庁、情報セキュリティ関係省庁、事案対処省庁、防災関係府省庁、情報セキュリティ関係機関及びサイバー空間関連事業者等と相互にシステムの不具合等に関する情報の共有を行う。
○ 重要インフラ所管省庁	所管する重要インフラ事業者等から受領したシステムの不具合等に関する情報をＮＩＳＣ及び必要に応じ該当するセプターに連絡する。ＮＩＳＣから受領したシステムの不具合等に関する情報を該当するセプターに提供する。	平時の役割に加え、必要に応じて大規模重要インフラサービス障害対応時の体制に協力する。
○ セプターカウンシル	セプターカウンシルは、政府機関を含め他の機関の下位に位置付けられるものでなく独立した会議体であり、各セプターの主体的な判断により連携するものである。 主体的な判断により各セプターが積極的に参画し、重要インフラ事業者等におけるサービスの維持・復旧に向けた幅広い情報共有を行う。	平時の役割に加え、必要に応じて大規模重要インフラサービス障害対応のための体制を構築し、セプター間をはじめとした関係機関との連携を図る。
○ セプター事務局	重要インフラ所管省庁、事案対処省庁、防災関係府省、情報セキュリティ関係機関、セプターカウンシル及び重要インフラ事業者等と連携し、相互にシステムの不具合等に関する情報の共有を行う。	平時の役割に加え、必要に応じて大規模重要インフラサービス障害対応のための体制を構築し、内閣官房をはじめとした関係機関との連携を図る。
○ 重要インフラ事業者等	システムの不具合等に関する情報について、必要に応じて所属するセプター内で共有するとともに、「別添：情報連絡・情報提供について」に基づき重要インフラ所管省庁への連絡を行う。なお、犯罪被害にあった場合は、自主的な判断により事案対処省庁への通報を行う。	平時の役割に加え、必要に応じて大規模重要インフラサービス障害対応のための体制を構築し、内閣官房をはじめとした関係機関との連携を図る。

※災害やテロ等に起因する大規模重要インフラサービス障害が発生した場合、当該緊急事態における情報の集約及び共有として、「緊急事態に対する政府の初動対処体制について」（平成 15 年 11 月 21 日閣議決定）に基づき、関係府省庁間で情報を集約及び共有する。

2.2.2. 国内 ISAC の動向

国内においては 2016 年に初めて電気通信・放送分野において ICT-ISAC が設立され、その後電力、金融、交通の分野で ISAC が設立されている。

国内の各 ISAC の活動内容はそれぞれで若干違いがあるものの、主に「情報収集」「情報の調査・分析」「情報発信」の機能を持っている。セプターと異なる点としては、会員から会費を集めて活動をしている点が挙げられるが、特に、会員資格が複数のカテゴリーに分かれている点にも着目可能である。例えば、「アフィリエイト会員」や「賛助会員」といった形で、当該 ISAC の分野を本業としているわけではないものの、サイバーセキュリティの専門的な知見を活かした活動ができる者が参加可能な会員資格が設けられている可能性がある。また、そうした会員は、正会員よりも高い会費を支払う前提となっている ISAC（例としては金融 ISAC）も存在している。また、予算執行その他の機関意思決定のための理事会を備えている点もセプターとの相違点として挙げられる。

表 5 国内 ISAC 概要

名称	一般社団法人 ICT-ISAC	電力 ISAC	一般社団法人金融 ISAC	一般社団法人交通 ISAC
事業の範囲	電気通信、放送	電力	銀行、保険、証券	交通、運輸
設立	2016 年 3 月 9 日	2017 年 3 月 28 日	2018 年 8 月	2020 年 4 月 1 日
事務局／役員等	理事長： 齊藤 忠夫 (東京大学名誉教授) 理事：澁谷 直樹 (日本電信電話株式会社) 理事：田中 孝司 (KDDI 株式会社) 監事：向井 健太郎 (富士通株式会社) 顧問：飯塚 久夫 顧問：中尾 康二	代表理事：岩見 章示 (中部電力株式会社) 理事澁谷：隆司 (九州電力株式会社) 理事谷口：浩 (東京電力ホールディングス株式会社) 理事名部：正彦 (関西電力株式会社) 理事：新田 哲 (JFE ホールディングス株式会社) 監事：平山 成治 (東北電力株式会社) 監事：松浦 英行 (電源開発株式会社)	理事長：谷合 通宏 専務理事：鎌田 敬介 理事：大日向 隆之 理事：黒山 康治 理事：真鍋 敬士 監事：稲垣 隆一	理事長：佐々木 敬介 (東日本旅客鉄道株式会社) 理事：黒木 敏英 (全日本空輸株式会社) 理事：平岡 和巳 (成田国際空港株式会社) 理事：由水 研二 (株式会社 NYK Business Systems) 監事：樋口 賢 (阪急電鉄株式会社) 監事：田中 一三 (日本通運株式会社)
構成員（主な構成企業、企業数）	43 会員 オブザーバー：総務省 国立研究開発法人情報通信研究機構 一般社団法人日本インターネットプロバイダー協会 一般社団法人テレコムサービス協会 一般社団法人電気通信事業者協会 一般財団法人日本データ通信協会 一般社団法人日本民間	正会員 41 会員（電力の小売、送配電、発電事業者） 特別会員 2 会員（電力広域的運営推進機関及び日本卸電力取引所） テクニカル会員 8 会員（セキュリティシステム企業、コンサルティング会社等）	正会員 416 会員（年会費 80 万円） 賛助会員 1 会員 アフィリエイト会員（ゴールド）12 会員（年会費 300 万円） アフィリエイト会員（シルバー）10 会員（年会費 200 万円） アフィリエイト会員（ブロンズ）4 会員（年会費 100 万円） （※アフィリエイト会員	正会員 67 会員（年会費 50 万円） 賛助会員 2 会員（年会費 50 万円 オブザーバー会員 10 会員（年会費なし） （※正会員は、交通関係団体であり、賛助会員は、正会員向けにサイバーセキュリティに関する情報や知見等を積極的かつ自発的に提

	放送連盟 一般社団法人日本ケーブルテレビ連盟		は、金融機関以外の法人であって、IT セキュリティに関連する企業等）	供できる者である）
主な活動内容	・サイバーセキュリティに関する情報収集・調査・分析 ・会員間の情報共有と共同対処 ・セキュリティ人材の育成、セキュリティ啓発 ・セキュリティガイドライン等の整備に関する活動 ・認定送信型対電気通信設備サイバー攻撃対処協会としての活動	・サイバーセキュリティに関する情報の収集 ・収集した情報の内容を踏まえた情報の分析 ・収集・分析の結果の会員間での共有 ・会員間での情報共有に伴う、ルールの策定及び相互協調活動の促進 ・電力セプター事務局その他当会の目的を達成するために必要な事業	・日々発生するインシデントや脆弱性を会員間で共有する『コレクティブインテリジェンス』と、共通の課題に対しリソースを共有し、協働しながら対策を検討を進めていく『リソース・シェアリング』の２つを活動の柱 ・金融 ISAC では専用のポータルサイトを通じ、日々のインシデントや脆弱性情報等をリアルタイムに共有。特定の重要課題について、テーマごとにワーキンググループ（WG)を設け、会員共同で対策検討等を行いながら、知見と対応力を高めている。これらの成果をワークショップやアニュアルカンファレンス等の場で発表、ポータルサイトに成果物の蓄積を行っている	・サイバーセキュリティに関する情報の収集、共有及び提供 ・サイバーセキュリティに関する課題に対する共通認識の醸成及び共同対処 ・その他当法人の目的を達成するために必要な事業
アクセス／連絡先	・HP 問い合わせフォーム ・住所 〒105-0001 東京都港区虎ノ門 2-5-5 一般社団法人ＩＣＴ－ＩＳＡＣ事務局	・電話 03-5220-1133 ・メール info@je-isac.jp ・住所 東京都千代田区大手町 1 丁目 3 番 2 号	・電話 03-6269-9521 ・ファクス 03-6269-9603 ・メール info@f-isac.jp	・電話 03-5422-1045 ・メール(各種問合せ) t-isac-sec@t-isac.or.jp ・メール（入会申込） entry@t-isac.or.jp

本業務においては、監視や制御体制が類似していると考えられるインフラ分野の電力 ISAC について詳細に情報収集を行った。

2.2.3. 電力 ISAC 設立の背景・目的

電力 ISAC は 2017 年 3 月 28 日付で電気事業者間のサイバーセキュリティに関する情報共有及び分析を行う組織として設立された。「電気の安定供給に重要な役割を担う事業者間で、信頼と互助の精神に基づきサイバーセキュリティに関する情報等を交換、分析することにより、事故の未然防止、発生した事故に対する迅速な対応等を実現することを目的として設立した組織」としている。また、 海外における同等の機関との連携等も視野に入れ、情報共有を推進していくとしている。さらに第４次行動計画に基づく電力分野のセプター事務局[33]として

[33] 「事務局の役割:（平時）重要インフラ所管省庁、事案対処省庁、防災関係府省、情報セキュリティ関係機関、セプターカウンシル及び重要インフラ事業者等と連携し、相互にシステムの不具合等に関する情報の共有を行う。（大規模障害対応時）平時の役割に加え、必要に応じて大規模重要

の役割を持ち、重要インフラ事業者と政府機関との連携を担っていくとしている[34]。

図 11 電力 ISAC の HP

2.2.4. 関連機関

電力 ISAC は電力セプター事務局の役割を持ち、内閣官房（NISC）が定める第 4 次行動計画に則り活動を行っているため、NISC が事実上の所管であると考えられる。一方で電力 ISAC の事務局は電気事業連合会の職員が兼務しており（後述）、METI とも綿密な連携がなされていると想定される。

電力セプター事務局としては、重要インフラ所管省庁、事案対処省庁、防災関係府省、情報セキュリティ関係機関、セプターカウンシル及び重要インフラ事業者等と連携し、相互にシステムの不具合等に関する情報の共有を行っている。また有事の際は平時の役割に加え、必要に応じて大規模重要インフラサービス障害対応のための体制を構築し、内閣官房をはじめとした関係機関との連携を図る役割も求められる。

【関係機関】

電力 ISAC は国内外の情報セキュリティに関する組織・機関との総合的な窓口となり、情報収集・共有をするとともにコネクションの維持も行っている。

インフラサービス障害対応のための体制を構築し、内閣官房をはじめとした関係機関との連携を図る。」内閣サイバーセキュリティセンター「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」セプター [https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r2.pdf]（最終検索日：2021 年１月 22 日）。

[34] 経済産業省「電力 ISAC の設立について」（電力・ガス基本政策小委員会第４回総合資源エネルギー調査会電力・ガス事業分科会、2017 年７月７日）[https://www.meti.go.jp/shingikai/enecho/denryoku_gas/denryoku_gas/pdf/004_07_02.pdf]（最終検索日：2021 年１月 22 日）。

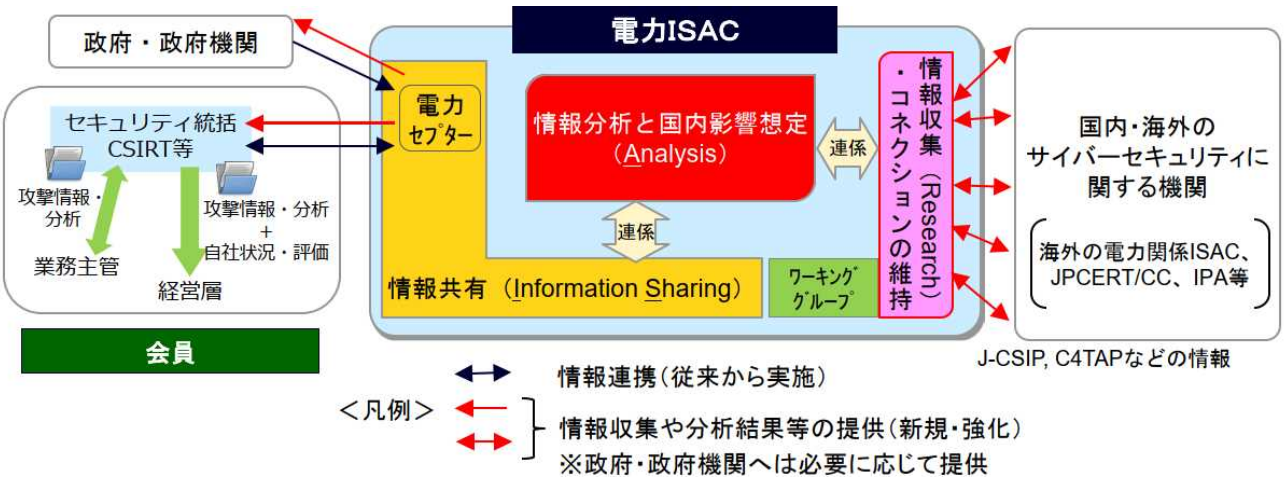


図 12 電力 ISAC とステークホルダーの関係

- 日本電気技術規格委員会（JESC）

  日本電気技術規格委員会（英名：Japan Electrotechnical Standards and Codes Committee，略称：JESC（ジェスク））は，1997 年に設立され，公正性，客観性，透明性及び技術的能力・管理能力を有する民間規格評価機関として，電気工作物の保安及び公衆の安全並びに電気関連事業の一層の効率化に資することを目的とした委員会。具体的には，「電気事業法」の技術基準等に民間の技術的知識，経験等を迅速に反映すること，自主的な保安確保に資する民間規格等を評価し，その活用を推進することなどの活動を行っている。

  電力分野のサイバーセキュリティに関するガイドラインを電気事業法下の技術基準等に組み込み、ハード・ソフト両面の対策を推進している。

- CSIRT（Computer Security Incident Response Team、シーサート）[35]

  コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をしている。

- IPA[36]

  独立行政法人情報処理推進機構（IPA：Information-technology Promotion Agency, Japan）とは、情報処理の促進に関する法律に基づき、IT 社会推進のための技術や人材についての振興を行う独立行政法人（経済産業省所管）。1970 年 10 月に特別認可法人情報処理振興事業協会として創立され、2004 年に現在の形に改組された。

- IPA-ICSCoE

  IPA 産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence/ICSCoE）は 2017 年4月1日に設立され、模擬プラントを用いた演習や、攻撃防御の実践経験、最新のサイバー攻撃情報の調査・分析等を通じて、社会インフラ・産業基盤へのサイバーセキュリティリスクに対応する人材・組織

[35] 日本シーサート協議会（CSIRT） [https://www.nca.gr.jp/outline/index.html]（最終検索日：2021 年1月 22 日）。

[36] 情報処理推進機構（IPA） [https://www.ipa.go.jp/about/ipajoho/gaiyo.html]（最終検索日：2021 年1月 22 日）。

・システム・技術を生み出していくための組織である。

- JPCERT/CC[37]

「一般社団法人 JPCERT コーディネーションセンター 」の略称。PCERT コーディネーションセンター（JPCERT/CC）は、技術的な立場における日本の窓口 CSIRT である。インターネットを介して発生する侵入やサービス妨害などのコンピュータセキュリティインシデント（以下、インシデント）について、日本国内に関する報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行なっている。主な活動は「インシデント対応」「脆弱性情報ハンドリング」「インターネット定点観測システムの運用」「早期警戒」「国際連携」「アーティファクト分析」「制御システムセキュリティ」「国内の関係組織やコミュニティとの連携」の８つがある。

- J-CSIP[38]

サイバー情報共有イニシアティブ（J-CSIP/Initiative for Cyber Security Information sharing Partnership of Japan）は、2011 年 10 月 25 日、IPA がサイバー攻撃による被害拡大防止のために、経済産業省の協力のもと、重工、重電等、重要インフラで利用される機器の製造業者を中心に、情報共有と早期対応の場として発足させた。その後、全体で 13 の SIG（Special Interest Group、類似の産業分野同士が集まったグループ）、263 の参加組織による情報共有体制と、IPA が特定業界内の情報共有活動を支援する2つの「情報連携体制」をそれぞれ確立し、現在、サイバー攻撃に関する情報共有の実運用を行っている。

- C4TAP[39]

標的型攻撃に関する情報共有体制（C4TAP：Ceptoar Councils Capability for Cyber Targeted Attack Protection）とは、重要インフラ事業者において、標的型攻撃が疑われるメールについての一定情報を共有することで、より多くの標的型攻撃に関する情報を収集・共有し、重要インフラサービスへの標的型攻撃の未然防止、もしくは被害軽減、サービスの維持、早期復旧を容易にすることを目指す取組み。

- 海外電力 ISAC

電力 ISAC は、2017 年 5 月 16 日にオランダハーグにて、ヨーロッパにおける電力 ISAC：The European Energy-Information Sharing & Analysis Centre (EE-ISAC) (chair：Aurélio Blanquet) と友好関係構築を目的とした覚書（MOU/Memorandum Of Understanding）を締結。

また 2018 年 10 月 17 日にはアメリカ合衆国ラスベガスで開催された GridSecCon2018 にて、米国における電力 ISAC：Electricity - Information Sharing & Analysis Center（E-ISAC）も加え、日米欧のサイバーセキュリティの確保に向けて国際的な協力関係を築くため覚書（MOU）を締結している。

---

[37] JPCERT/CC [https://www.jpcert.or.jp/about/brief/]（最終検索日：2021 年1月 22 日）。

[38] 情報処理推進機構（IPA）サイバー情報共有イニシアティブ[https://www.ipa.go.jp/security/J-CSIP/index.html]（最終検索日：2021 年1月 22 日）。

[39] 内閣サイバーセキュリティセンター（NISC）[https://www.nisc.go.jp/active/infra/pdf/cc_c4tap.pdf]（最終検索日：2021 年1月 22 日）。

写真 1 2018 年 10 月 17 日 調印式後握手を交わす日米欧の代表者

（左から JE-ISAC（阿部克之氏）、NERC（Jim Robb 氏）、EE-ISAC（Johan Rambi 氏）

2.2.5. 運営体制

【総会】

電力 ISAC は総会（定時総会及び臨時総会）を開催し、理事及び監事の選任、事業計画及び予算の承認等を行っている。定時総会は年1回（毎事業年度の終了後 3 か月以内）としている。事業年度は毎年4月1日から翌年 3 月 31 日までとしている。

総会は正会員、特別会員をもって構成され、議決権は正会員にのみ配分される。総会の定足数は総議決件数の2分の1以上とし、総会に出席した正会員の議決権の過半数で決議される。

【理事会・役員】

理事会では下記の職務を基本にし、会の運営を行っている。理事会は6か月に1回以上行うものとしている。

（1）総会の開催日時・場所及び議事に付すべき事項の決定

（2）本会及び理事会の運営等に係る規則・細則等の制定・改廃

（3）中期取組方針の承認

（4）本会への入会の承認

（5）前各号に定めるもののほか、本会の業務執行の決定

（6）代表理事の選任及び解任

役員としては理事5名以下、監事2名を置くこととし、理事のうち1名は代表理事としている。任期は基本的に2年間とし、役員報酬は無しとなっている。

【事務局】

常勤体制の事務局を置き、各活動（2.2.7 活動内容にて後述）を推進している。事務局職員については電気事業

連合会との兼務職員となっている。
事務局としては事務局長及び所要の職員を置くとしており、事務局長は理事会の承認を経て任免される。

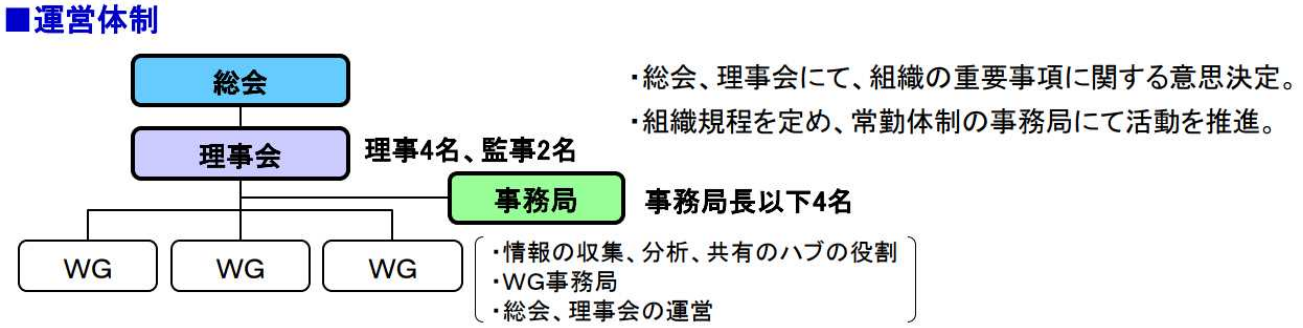


図 13 電力 ISAC の運営体制図

2.2.6. 規約

規約では電力 ISAC の目的や事業内容の他、会員、総会、役員、理事会、資産・会計等について定めている。

【会員】

電力 ISAC では正会員、特別会員、テクニカル会員の3つがあり、それぞれ会員資格について定められている（規約第4条）。また入会する場合は理事会が定める入会申込書により申込み、総海外定める入会資格審査基準に基づき理事会の承認を受けて会員になる（規約第5条）。
正会員およびテクニカル会員は総会で定める会費を毎年支払う（第6条）としているが、具体的な金額については公開されていない。
議決権は正会員にのみ配分され、テクニカル会員は総会に参加は可能であるが議決権を持たない。しかし、電力 ISAC に関する各種活動・情報へのアクセスについては正会員と同様にテクニカル会員も可能である。

第4条 本会の会員となる資格を有する者は、次の各号に該当する者とする。
（1）正会員 アからエまでに掲げる法人であって、本会の目的に賛同して入会した者
ア 一般送配電事業者（電気事業法第2条第9号）
イ 送電事業者（同条第 11 号）、特定送配電事業者（同条第 13 号）、発電事業者（同条第 15 号）及び小売電気事業者（同条第3号）
ウ アからイまでに掲げる者の発行済み株式の全部又は持分の全部を有する者
エ アからウまでに掲げる者が営む事業と関連する事業を営む者であって、本規約前文及び本会の目的（本規約第2条）に照らし、特にその入会が望ましいと理事会が判断した者
（2）特別会員 正会員となる資格を有しない法人であって、本会の目的達成のために欠くべからざる事業を営み、本会の目的に賛同し、かつ、特にその入会が望ましいと理事会が判断した者
（3）テクニカル会員 正会員及び特別会員となる資格を有しない法人であって、サイバーセキュリティに関し専門的な技術・知識を保有し、かつ、本会の目的に賛同し、特にその入会が望ましいと理事会が判断した者

第5条 1. 正会員、特別会員、又はテクニカル会員として入会しようとする者は、理事会が別に定める入会申込

書により申し込み、総会が定める入会資格審査基準に基づき理事会の承認を受けた時に正会員、特別会員、又はテクニカル会員となる。
2. 正会員となる資格を有する複数の者は、代表法人を定め、理事会が別に定める書式により、入会申し込みとあわせて、同一のグループとしての特例的な処理（以下「グループ処理」という。）を申し込むことができる。ただし、申し込みを行うことができるのは、代表法人以外のものが、次の各号のいずれかに該当する場合に限る。
（1）代表法人の親法人
（2）代表法人の子法人
（3）代表法人の親法人の子法人
（4）代表法人の関連法人
（5）代表法人の親法人の関連法人

2.2.7. 活動内容

電力 ISAC の活動は下記の通りである（規約第3条）[40]。

- 情報の収集
  JPCERT/CC 等の国内機関との協力体制や情報収集、ネットワークの強化を行う。海外の電力関係 ISAC との連携に向けた、カンファレンスへの参加や情報交換などの交流推進を行う。
- 情報の分析
  国内電気事業者への影響想定や対策案の検討ができるような体制づくりやセキュリティ専門事業者の活用を行う。
- 収集・分析した情報の共有
  公開情報や J-CSIP・C4TAP などの情報を会員へ迅速・タイムリーに情報提供・注意喚起を行う。
- 会員間での情報共有に伴う、ルールの策定及び相互協調活動の促進
  共有する情報の範囲・定義の明確化（TLP 等のルール制定とその運用） を行う。
- 電力セプター事務局
  第4次行動計画に基づく、NISC・経産省と事業者間の情報連絡、連携の窓口となる。
- その他、目的を達成するために必要な事業

情報収集の観点では電力セプターと大きな相違はないものの、情報展開についてはより広く周知できるようになっている（電力 ISAC ヒアリング）。

また電力 ISAC では総会の他に会員同士が直接的なコミュニケーションにより強固な信頼関係を構築し、積極的にサイバーセキュリティ情報を共有できるよう、WG 活動の場を提供している。

[40] 経済産業省「電力 ISAC の設立について」。

表 6 電力 ISAC が提供する WG

カテゴリ	WGテーマ	
専門分野（Ⅰ）	Ⅰ－1．課題検討WG	電気事業の各分野（発電、送配電、ITなど）の取組みで、サイバーセキュリティに係る課題事項に関する意見交換
情報交換（Ⅱ）	Ⅱ－1．ベストプラクティス共有WG	JESCガイドラインへの対応や取組みの外部有識者を交えた客観的レビューおよびベストプラクティスに関する会員間の情報交換
	Ⅱ－2．セキュリティ教育WG	社内のセキュリティ教育やそのコンテンツ等に関する情報交換
	Ⅱ－3．セキュリティ製品WG	ベンダーが提供するセキュリティ製品のベンチマーク、評価に関する情報共有
情報解説（Ⅲ）	Ⅲ－1．セキュリティトレンドWG	定期レポートの内容に関する解説およびサイバー攻撃のトレンドや各社の対応状況に関する情報交換

表 7 電力 ISAC のニュースリリース一覧[41]

日時	内容
2020 年 8 月 20 日	会員の加入について
2020 年 5 月 1 日	会員の加入について
2020 年 4 月 1 日	会員の加入について
2019 年 12 月 2 日	2019 年度電力 ISAC サイバーセキュリティ演習の実施について
2019 年 5 月 30 日	第2回電力 ISAC 定時総会の開催について
2019 年 4 月 1 日	会員の加入について
2018 年 10 月 23 日	日米欧電力関係 ISAC 間の MOU 締結について
2018 年 7 月 20 日	2018 年度 WG 活動について
2018 年 5 月 30 日	第1回電力 ISAC 定時総会の開催について
2018 年 4 月 3 日	新会員の入会について
2018 年 4 月 3 日	代表理事の交代について
2017 年 7 月 14 日	セキュリティトレンド WG の開催について
2017 年 5 月 16 日	The European Energy-Information Sharing & Analysis Centre（EE-ISAC）との MOU 締結について
2017 年 3 月 28 日	電力 ISAC の設立について

[41] 電力 ISAC「お知らせ」[https://www.je-isac.jp/news/index.html]（最終検索日：2021 年1月 22 日）。

写真 2　第1回定時総会の様子(2018 年 5 月 29 日)

写真 3　第1回リスクアセスメント WG の様子(2018 年 7 月 11 日)

2017 年度の活動

表 8 電力 ISAC の 2017 年度活動

WGテーマ	概要
課題検討WG	電気事業の各分野（発電、送配電、ＩＴなど）の取組みで、サイバーセキュリティに係る課題事項に関する意見交換
ベストプラクティス共有WG	ＪＥＳＣガイドラインへの対応や取組みの外部有識者を交えた客観的レビューおよびベストプラクティスに関する会員間の情報交換
セキュリティ教育WG	社内のセキュリティ教育やそのコンテンツ等に関する情報交換
セキュリティ製品WG	ベンダーが提供するセキュリティ製品のベンチマーク、評価に関する情報共有
セキュリティトレンドWG	定期レポートの内容に関する解説およびサイバー攻撃のトレンドや各社の対応状況に関する情報交換

表 9 電力 ISAC の 2018 年度活動

WG名	概要
火力システムWG	火力の発電所監視制御システム等のサイバーセキュリティに関するグッドプラクティス等を共有し、課題解決に向けた意見交換を行う。
水力システムWG	水力の発電所監視制御システム等のサイバーセキュリティに関するグッドプラクティス等を共有し、課題解決に向けた意見交換を行う。
需給・系統システムWG	需給制御システム及び系統制御システムのサイバーセキュリティに関するグッドプラクティス等を共有し、課題解決に向けた意見交換を行う。
共通・ITシステムWG	最新のサイバーセキュリティに関するトレンドや電力分野に係るIT/OT全般に関するグッドプラクティス等を共有し、課題解決に向けた意見交換を行う。
リスクアセスメントWG	様々なリスクアセスメント手法の概要・特徴を理解し、各社で効果的に実施していくために、課題の共有とともに解決に向けた意見交換を行う。
SMシステム脆弱性情報共有WG	スマートメーターシステムに関して、重大な脆弱性・セキュリティ事故・事象が発生した際に、必要に応じて関係者間で情報交換を行う。

表 10 電力 ISAC の 2019 年度活動

日時	活動内容	概要
2019 年 12 月2日	2019 年度電力 ISAC サイバーセキュリティ演習	東京五輪・パラリンピックの期間中に電力設備がサイバー攻撃を受けたと想定した防護演習

3. 我が国の水道分野サイバーセキュリティ対策の在り方に関する検討

3.1. 水道分野の動向

前述の通りサイバーセキュリティ基本法制定及び内閣サイバーセキュリティセンター（NISC）が設立され、これを受けて水道分野においては、サイバーセキュリティガイドラインの策定やセプター活動を行っている。

3.1.1. サイバーセキュリティガイドライン

内閣官房に設置されている情報セキュリティ基本問題委員会では、平成 17 年 4 月 22 日の第 2 次提言において、従来の重要インフラ分野を情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービスに加えて、医療、水道、物流を追加すべきとされた。情報セキュリティ政策会議が平成 17 年 12 月 13 日に策定した「重要インフラの情報セキュリティ対策に係る行動計画」（その後、平成 21 年 2 月 3 日に「重要インフラの情報セキュリティ対策に係る第 2 次行動計画」に改訂。）において、各重要インフラ分野において望ましい情報セキュリティ対策の水準を「安全基準等」として明示するよう努力することとされた。

また、平成 24 年 4 月 26 日の同行動計画（改定版）においては、①東日本大震災発生時における複数の IT システムの同時的な障害発生及びその際の事業継続計画（BCP）の実施、②政府関係機関や重要インフラ事業者等への IT システム（制御システムを含む）に対するサイバー攻撃等、いくつかの環境変化について、早期に取組を強化・補強すべき点についても反映が行われた。

このような中で、情報セキュリティ政策会議は、各重要インフラ分野における「安全基準等」の策定・改定を支援するために「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」策定にあたっての指針」（以下「指針」という。）及び同対策編（以下「対策編」という。）を策定している。指針では、それぞれの事業分野においてその特性に応じた必要または望ましい情報セキュリティ対策の水準を「安全基準等」という形で明示し、個々の事業者が重要インフラの担い手として自主的に取り組むことにより、その「安全基準等」を満たすべく努力し、また満たしているかを自ら検証することが必要とされている。

厚生労働省では、水道事業者が情報セキュリティ対策を行うため、平成 18 年 10 月 31 日に「水道分野における情報セキュリティガイドライン」（以下「ガイドライン」という。）を策定し、その後第 4 版（2019 年 3 月）まで改定が行われている。

第4版ガイドラインにおいては、国内水道分野のサイバーセキュリティについて 4 つの柱及び 5 つの重点項目を策定している。

◆ 4 つの柱

ア 組織・体制及び資源の確保

イ 情報についての対策（情報の格付け、ライフサイクルに着目した取扱い）

ウ 情報セキュリティ要件の明確化に基づく対策

エ 情報システムについての対策

◆ 5 つの重点項目

ア IT 障害の観点から見た事業継続性確保のための対策

イ 情報漏えい防止のための対策

ウ 外部委託における情報セキュリティ確保のための対策

エ IT 障害発生時の利用者の対応のための情報の提供等の対策
オ IT に係る環境変化に伴う脅威のための対策

3.1.2. 水道セプター[42]

我が国における水道セプターの事務局は公益社団法人日本水道協会が担っており、8 水道事業体が構成員となっている。構成員は日本水道協会への会員水道事業体のうち会長都市並びに地方支部長都市で構成されている。

水道セプターの主な活動内容としては、各種会合への参加、国内水道分野における各種サイバー情報の収集及び情報展開等がある。

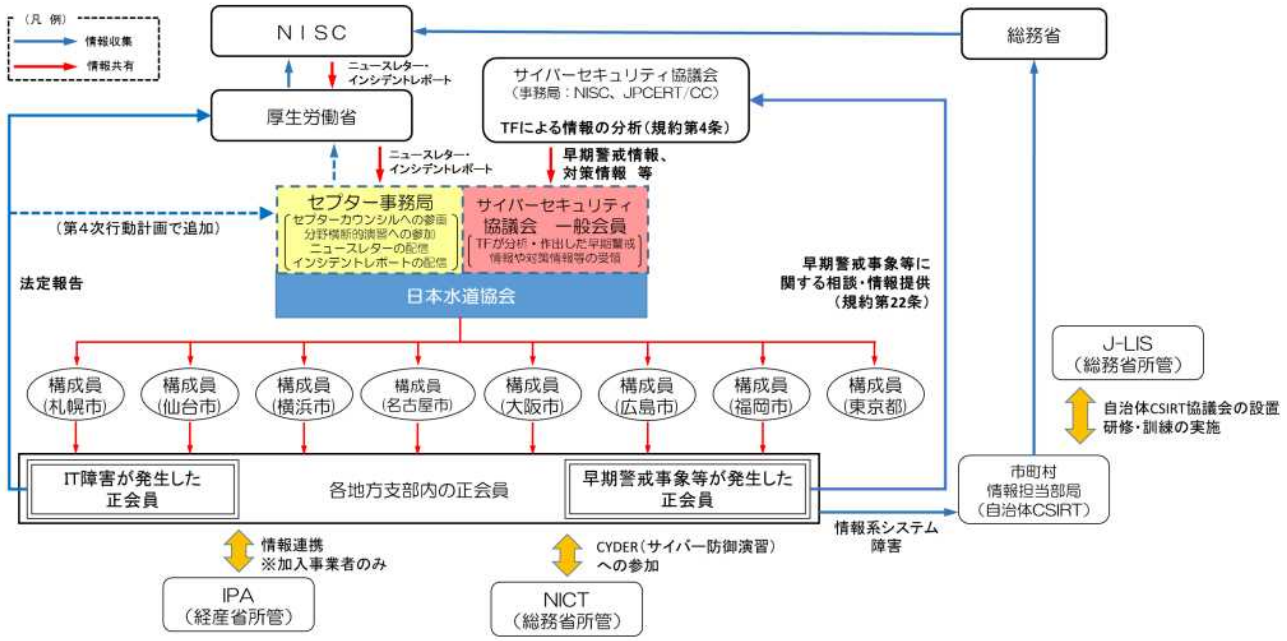


図 14 水道分野における体制図

【各種会合への参加】

水道セプター事務局の活動としてセプターカウンシル（総会、運営委員会等）へ参加をしている。加えて相互理解 WG（他セプターの施設等の視察）、情報収集 WG（他セプターの取組共有）、JPCERT/CC 等が主催するセミナー・勉強会など（年間数回程度）への参加をしている。これらの会合への参加はインシデント情報の収集活動を兼ねている。

その他、水道セプター事務局の活動として、下記の訓練活動に参加している。

・セプター訓練（年1回、厚労省・セプター事務局・構成員との間におけるメールによる情報伝達訓練）
・分野横断的演習（年1回、NISC が主催する訓練）

【情報収集】

水道セプターとしては、取り扱う情報を政府機関から提供された IT 障害情報（水道水の供給に重大な障害を

[42] 日本水道協会提供資料

もたらす、またはその可能性のある、水道施設の監視・制御システム、水道水の監視システム等の障害に限る)、日本水道協会正会員等で発生したIT障害情報と定義し、下記の方法で情報を収集している。

(情報収集方法)
・会員からのインシデント情報の収集
・NISCからの情報共有(週1回程度)
・サイバーセキュリティ協議会を通じた情報収集(ほぼ毎日配信)
※公開不可の場合がほとんどのため、情報共有は行っていない
・各種会議への出席(年間10回程度、セプターカウンシル・勉強会等)
・その他
不定期な情報交換ではあるが、2018年6月にAWWA総会にて協会間の連携を通じAWWA担当者と米国Water-ISACの現状や両国のサイバー対策等について、情報交換をした実績がある。
なお、国内の水道協会会員から提供されたサイバー情報は年間数件程度である。

表 11 水道セプターへ報告されたサイバー情報事例(H29~R1年度)

日付	事業体	内容
平成29年9月6日	長野県阿智村	水道施設中央監視システムにおける障害
平成30年4月26日	東京都水道局	ウェブページの改ざん
平成30年4月27日	千葉県八千代市	水位監視カメラへのハッキング
平成30年11月14日	東京都新島	調整池の水位計監視用ウェブカメラの障害
令和元年10月24日	静岡県静岡市	PCの第三者不正利用

【情報展開】
情報提供対象は構成員に加え、情報レベルにより日本水道協会の正会員(1,329団体の水道事業体)へ周知している。また正会員によって経営されている簡易水道事業者は正会員経由で情報が展開できている状況である。特別会員(学術系有識者)、賛助会員(コンサルタント、メーカー各社)及び正会員の経営ではない非会員の簡易水道事業者、専用水道保有者等には情報提供を行っていない。
情報展開方法については使用が可能な場合においては基本的にEメールを使用しているが、必要に応じて電話、FAX等を使用している(一部の情報については日本水道協会HPにて公表も可能としている)。
取り扱う情報は、不必要に情報の共有範囲を広げることにより、情報セキュリティの脅威を増大する恐れのある情報等が含まれる場合がある。そのため、適切に共有範囲を限定する必要があることから、情報の重要度と共有可能な範囲を示す「情報共有レベル」を付与することとし、そのレベルは、情報の重要性、影響度等を勘案し、事務局が厚生労働省と協議のうえ決定している。
また政府機関から事務局に提供される情報(他インフラ分野のIT障害情報等)は、政府機関における情報連絡・情報提供の手続きに適用される『「重要インフラの情報セキュリティ対策に係る行動計画」の情報連絡・情報提供に関する実施細目』に定められている4段階の情報共有レベルに基づき連絡されるため、それに従って取り扱うこととしている。

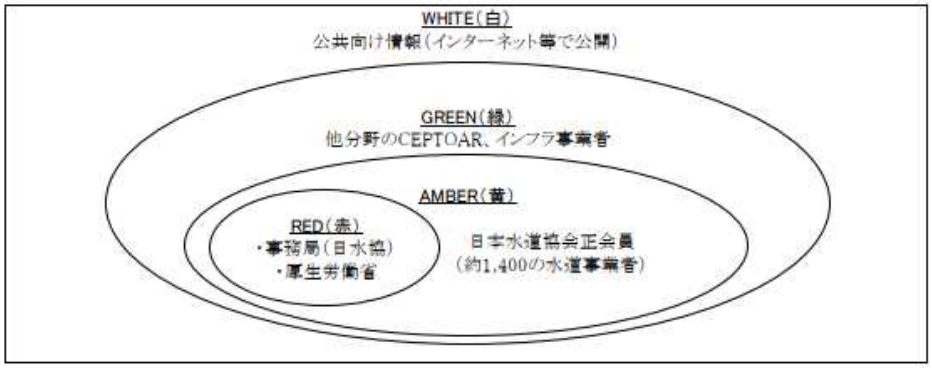
＜取り扱う情報のレベル＞

情報レベルは4つに分類され、一番厳しい①RED（赤）では厚生労働省と事務局の 2 者のみに限定するレベル、一番ゆるい④WHITE（白）では公共向けの情報として広く公表するレベル、など定めている。

表 12 情報レベルと共有可能範囲

レベル	情報の共有可能範囲
① RED（赤）	非公開情報であり、情報の共有は情報提供元である厚生労働省と事務局の 2 者のみに限定する。
② AMBER（黄）	RED（赤）情報の共有範囲に加え、全ての日本水道協会の正会員との間で共有が可能な情報とする。 ※情報連絡は、障害の影響度、地域性等を考慮し、その情報を知る必要がある者に対して行う。
③ GREEN（緑）	AMBER（黄）情報の共有範囲に加え、他インフラ分野の CEPTOAR 並びにそれを構成する重要インフラ事業者等と共有が可能な情報とする。 ※情報連絡は、障害の影響度、地域性等を考慮し、その情報を知る必要がある者に対して行う。
④ WHITE（白）	公共向けの情報であり、著作権を適正に扱う限りにおいて、分配、出版、インターネット上での公開及び放送に供することも可能な情報とする。 ※日本水道協会ホームページ、プレス発表等により情報を公開する。

※上記のうち、① RED（赤）以外の情報連絡に際しては、事務局より、日本水道協会地方支部長都市である 7 構成員に対し、各地方支部内の正会員に対する情報連絡を要請する場合がある。



情報共有レベルと共有可能範囲のイメージ

図 15 情報共有レベルと共有可能範囲のイメージ

＜政府機関が情報発信元の場合＞

事務局が政府機関から情報を得た場合は、政府機関において設定された当該情報の共有レベルに基づき構成員等に連絡する。

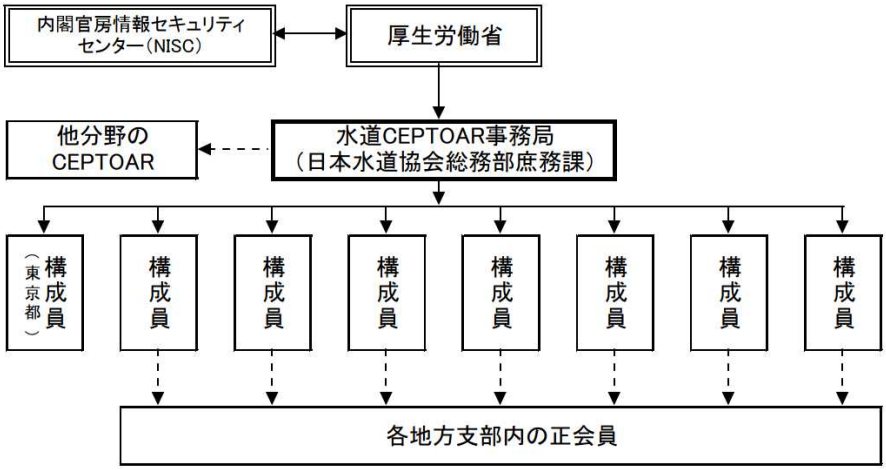


図 16 政府機関から情報発信された場合の情報提供フロー

＜水道事業体が情報発信元の場合＞

IT 障害が発生した水道事業体は、（都道府県知事認可の場合は都道府県を通じて働省に事故等の概要を報告する。事務局は、厚生労働省より IT 障害に関する情報の提供を受け、同省と協議のうえ当該情報の共有レベル及び具体的な情報連絡先を決定し、それに基づき構成員等に連絡する地方支部長都市である 7 構成員が事務局からの情報提供を受けた場合は基づく判断により決定された範囲の地方支部内の正会員に連絡する。

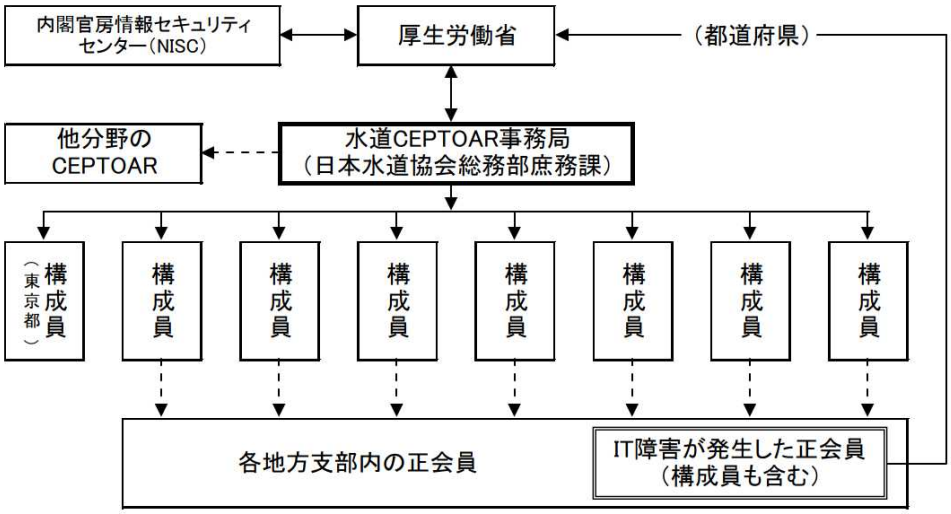


図 17 水道事業体から情報発信された場合の情報提供フロー

3.2. 水道分野におけるサイバーセキュリティに関する情報共有のあり方についての検討

水道分野における情報共有のあり方について、情報共有内容、情報共有体制の観点から分析を行った。

【情報共有内容】

情報収集、情報分析、情報展開の観点から、下記の検討を行った。

- 情報収集

  現在の水道セプターにおいては、会員からのインシデント情報の収集、NISC からの情報共有、サイバーセキュリティ協議会を通じた情報収集、各種会議への出席等によって情報収集を行っている。また米国 Water-ISAC とのコネクションも有しており、他組織からのサイバー情報の入手手段も一定持っている状況である。

  現状の水道分野においては日本水道協会会員 1,329 団体（国内の認可水道事業者の約 90%以上をカバー）からの情報収集体制を有しているが、年間1～3件のインシデントが報告されるのみである。またその内容も多くはウェブページや監視カメラのハッキングであり、水道事業の根幹である浄水・配水機能等の運営に直接影響する攻撃ではない。これは現在水道事業体が導入している監視・制御システムのほとんどがオンプレミス型のオフラインでシステム構築されていることに起因しているものと考えられる。一方、海外の水道 ISAC 等の事例においては、より幅広い関係者から情報収集を行っている場合もある。

- 情報分析

  水道セプターにおいては事実上情報分析機能がなく、収集された情報をその情報レベルに合わせて情報展開する機能のみとなっている。上述のとおり、現状では発生インシデント数が極めて少数であり、かつ、水道事業の根幹である浄水・配水機能等の運営に直接影響する攻撃ではないことから、水道セプターではなくインシデント発生事業体でそれぞれ個別に問題の分析、対策が実施できる状況にあると想定される。今後、仮に水道事業体のサイバーセキュリティ環境が変化し、発生インシデント数が増加・複雑化した場合においては、個別にインシデント対応をすることが難しくなる可能性も想定される。

  一方、海外の水道 ISAC 等の事例においては、水道事業者以外にも監視制御やセキュリティシステムに関する企業やコンサルティング会社等の民間セクターの関係者が参画しており、こういった者の参加により、インシデント事例の情報分析能力が強化できる可能性がある。

- 情報展開

  上述の通り、現在はインシデント情報について日本水道協会会員である 1,329 団体（水道事業体）に対してメールでの情報提供を行っている。一方、海外の水道 ISAC 等の事例においては、より幅広い関係者に情報提供を行っている場合もある。

【情報共有体制】

現状セプター事務局としての活動は年間 10 数回の各種会議や勉強会等への参加、インシデント情報が報告された場合の各種メール対応等がメインである。インシデント情報も年間数件程度のため、実質的には会議参加がメインである。そのため現状の体制としては十分であると考えられるが、将来、水道分野を取り巻くサイバーセキュリティに関するリスクが増大した場合には、改めて情報共有体制のあり方について検討することも考えられる。

4. まとめ

- 本業務では、サイバーセキュリティに関する情報収集・分析等を行う組織である ISAC（Information Sharing and Analysis Center）に関するヒアリング調査等を実施し、今後の我が国の水道分野におけるサイバーセキュリティ対策に関する情報共有のあり方について検討を行った。
- 米国においては大統領令により重要インフラ分野において ISAC が設立されており、水道分野においては WaterISAC が設立されている。HP 上に一元的にサイバーセキュリティの各種関連情報を集約する、インシデント・レポートやウェビナー開催をするなど、広く米国中のサイバー情報を収集・分析・展開する体制を整えている。また日本国内におけるセプターカウンシルと同等の機能と考えられる ISAC 国家評議会があり、そこを通じて約 20 の他の ISACs と連携をとりながら活動を行っている。
- 日本では4つの重要インフラ分野（情報通信、電力、金融、交通）において ISAC が設立されている。一般的に ISAC は、主に情報収集機能、情報分析機能、情報展開機能を有している。日本における電力 ISAC を例にとると、サイバーセキュリティに関する情報等を交換・分析することにより、事故の未然防止、発生した事故に対する迅速な対応等を実現するための組織として設立されている。電力 ISAC としての情報収集機能はセプターと違いがないものの、セキュリティ専門事業者の活用など情報分析機能を確保しており、情報展開はセプター活動以上に広く展開できるようになっている。
- 日本における水道事業のサイバーセキュリティ対策の状況としては、水道セプターがサイバーセキュリティに関する情報収集機能及び情報展開機能を有している。現状の水道セプターでは情報分析機能がないものの、現状のインシデント数は年間数件程度であり、個別に問題の分析・対策がなされている。
- 将来的に水道事業者を取り巻くサイバーセキュリティの環境が変わり、インシデント数の増加・複雑化が生じた場合においては、海外の水道 ISAC の事例や他分野の ISAC の事例によれば、水道事業体以外の様々なステークホルダーを情報共有の枠組みに加えることにより、情報収集、情報分析及び情報展開機能の強化を図ることができる可能性がある。