戦略的イノベーション創造プログラム（SIP）
重要インフラ等におけるサイバーセキュリティの確保
(b2)情報共有プラットフォーム技術

「情報共有デザインガイド　構築編」

2020 年 1 月

株式会社 日立製作所

本研究の一部は、内閣府が進める戦略的イノベーション創造プログラム（SIP）「重要インフラ等におけるサイバーセキュリティの確保」（管理法人：NEDO）によって実施されました。

戦略的イノベーションプログラム（SIP）：
重要インフラ等におけるサイバーセキュリティの確保　(b2)情報共有プラットフォーム技術
情報共有デザインガイド　構築編

2020 年 1 月 24 日
株式会社日立製作所

目次

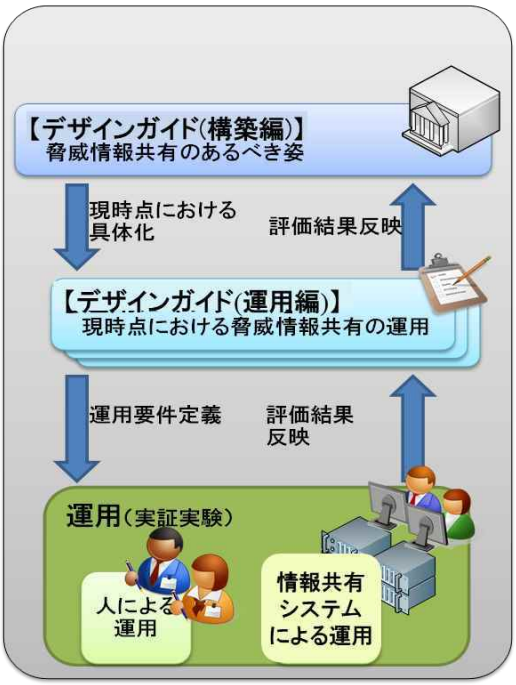
はじめに

サイバー攻撃が日々、高度化・巧妙化する中、企業・組織におけるセキュリティ対策には、外部の信頼できる情報機関から脅威情報をいち早く取得し、社内や関係会社と共有・連携しながら脅威の重要性や緊急性を迅速に分析・把握して対策を行うことが必要である。

一方で、こうした取り組みは個々の企業・組織が独自で対応していることが多く、重要インフラ分野を中心に、企業・組織の垣根を越え、より迅速かつ安全に脅威情報を共有できる体制や仕組みづくりが求められているのが現状である。

このような状況下で、NEDO が管理法人を務める内閣府事業「戦略的イノベーション創造プログラム（SIP）／重要インフラ等におけるサイバーセキュリティの確保（以下、「本事業」という）」において、株式会社日立製作所は日本の重要インフラにおけるサイバーセキュリティの脅威情報を共有する仕組み・体制づくりを促進するための研究開発を行った。

上記の研究開発の成果物の 1 つが、情報共有デザインガイド（以下、「本書」という）である。本書は、重要インフラに関連する各組織に対し、情報共有の仕組みを普及・啓発することを目的として、情報共有の効果や日本における情報共有のイメージ（仮説）を示すと共に、必要な仕組みなどを示したものである。主に、これから情報共有に関する取組みを積極的に実施しようと検討している企業・組織において活用されることを期待する。



成果物	活用時期	主な効果
デザインガイド（構築編）	情報共有未参加	・情報共有の仕組み普及・啓発 ・情報共有の参加促進
デザインガイド（運用編）	情報共有参加開始	・情報共有のための組織・情報システムの立ち上げ促進
情報共有システム	情報共有参加中	・機械処理可能な情報の共有

本書の使い方

近年増加している重要インフラ事業者を標的としたサイバー攻撃は、情報システムだけでなく制御システムを対象とする、ある業界の複数の事業者を同時多発的に狙う、などの特徴を持っている。このため、サイバー攻撃による重要インフラの停止を防止するためには、業界内、業界横断における重要インフラ事業者間の情報共有による集団防衛が重要である。この集団防衛を実現するための情報共有のイメージ(仮説)を示すために、本書は以下のような構成をとっている。

1 章では、サイバーセキュリティにおける情報共有の必要性について述べる。情報共有による効果が重要インフラ事業者に十分認識されておらず、海外と比較して日本の情報共有が活性化していない現状について示す。

2 章では、情報共有の海外事例について述べる。日本における情報共有のイメージを検討する上で、日本よりも情報共有の取組みが先行している海外の事例を紹介する。

3 章では、日本における情報共有について仮説を述べる。海外事例から得られた示唆や重要インフラ事業者に対するヒアリングから得られた要望をもとに、情報共有のイメージを構築する。

4 章では、日本における情報共有に必要な仕組みについて述べる。情報共有を実現する上で、必要と考えられる情報共有システムの機能を検討する。

5 章では、情報共有デザインガイドの評価について述べる。本事業で開発した情報共有システムを実際に重要インフラ事業者に運用してもらい、アンケートに回答して頂いた結果を紹介する。

本事業における調査を通じて、重要インフラ事業者の情報共有に対する認識レベルは、その事業者がいる業界によって大きく異なることが分かっている。そのため、本書の活用方法は、読者である重要インフラ事業者の現状に応じても異なるだろうことが想定される。そこで、読者の認識レベルで特に役立つと思われる情報共有デザインガイドの参考箇所を手引きとして示すことにした。これはあくまで一例であるので、手引きに示した参考箇所以外についても、読者に情報共有デザインガイドを大いに活用して頂ければ大変幸いである。

情報共有デザインガイドの活用手引き

業界による情報共有の認識レベル			情報共有デザインガイドの活用方法	
#	認識	内容	特に参考となる箇所	活用の効果
1	高	• 日常的にサイバー攻撃を受けており、情報共有による集団防衛の価値を認識している。 • 情報共有の仕組み・体制を構築、大手企業が主導的な役割を果たしている。	3章:3.2、3.3、3.4、3.5 4章:4.1、4.2 5章	主導的な企業が参照することで、情報共有の仕組み・体制の正しさを確認・再認識するために有効。
2	中	• 海外のサイバー攻撃による重大インシデントの発生などを背景に、情報共有の必要性を認識し始めている。 • 情報共有の仕組み・体制は確立していないが、人と人が緩やかに連携している。	2章 3章:3.2、3.3、3.4、3.5 4章:4.2	情報共有が集団防衛の第一歩であるという認識を促し、将来的な仕組み・体制の構築を補助するために有効。
3	低	• 国内のサイバー攻撃による重大インシデントの発生が顕在化していないために、情報共有を将来的な課題と捉えている。 • 各企業が個別にサイバーセキュリティ対策を実施している。	1章 3章:3.1 4章:4.2	情報共有の必要性を認識し、具体的な仕組み・体制のイメージを掴むために有効。

1. サイバーセキュリティにおける情報共有の必要性

1.1. 重要インフラ事業者に対するサイバー攻撃の現状

近年、サイバー攻撃の件数は増加している。その中でも、実行されているサイバー攻撃の特徴の一つとして、重要インフラ事業者が標的になっている点を挙げることができる[1]。重要インフラの停止は、人々の生活に及ぼす影響が大きいことに鑑みると、サイバー攻撃によってインフラが停止することを防止するための施策を事業者が実施することは、社会的に強く求められていると考えられる。実際、国内における ICT システムのサイバーセキュリティ政策を主導する内閣サイバーセキュリティセンター（NISC:National center of Incident readiness and Strategy for Cybersecurity）は、「機能が停止または低下した場合に多大なる影響を及ぼしかねないサービスは、重要インフラとして官民が一丸となり、重点的に防護していく必要がある」と表明している[2]。

上記以外の近年のサイバー攻撃の特徴として、攻撃者が戦略的且つ組織的に攻撃を行うようになっていることやゼロデイ攻撃が増加していることが挙げられる[3][4][5]。また、そのような攻撃は、事業者内の情報システムだけでなく制御システムを対象としていたり、ある分野の複数事業者を同時多発的に狙うものであったりということが近年の特徴である[5][6]。

(1) エネルギー分野の事例:

2010 年、イランのナタンズ核燃料施設がサイバー攻撃を受けた。スタックスネット・マルウェアが、USB メモリに組み込まれていたもので、施設の職員が、意識せずに USB メモリをコンピュータに接続したところ、施設内の制御コンピュータが感染した。その結果、ウラン濃縮用の遠心分離機が稼働不能となってしまった。従来、このような重要システムのネットワークは、公衆網と分離されて制御されていることから、サイバー攻撃を受けることは無い、という施設運営者の認識がある。そのためセキュリティ対策の意識が低くなりがちである。

このように、重要インフラの中では、電力・エネルギーシステムへの攻撃が最も多く発生している。

2003 年、米国のオハイオ原子力発電所で、SQL Server を狙ったワームが VPN(仮想の専用回線)から侵入して感染した。その結果、5～6 時間にわたり安全管理システムが停止、他の電力施設との通信が遮断された。発電所と協業しているコンサルタント会社の端末が感染しており、そこを経由して感染を起こした。

同 2003 年、米国の 265 の発電所で、監視用の SCADA システムが攻撃を受け、アラーム障害を発生。508 ユニット分の発電機が停止した。

2006 年、米国のブラウンズ・フェリー原子力発電所で、発電所の再循環水ポンプが制御不能になった。発電所統合ネットワークが DoS 攻撃を受け、制御装置が不調を来たしたものである。

2009 年には、米国のスマートメータが攻撃を受けた。インターネット上で調達可能なソフトウェアを用いて、簡易にスマートメータシステムに侵入され、電力消費の記録を改ざんされた。

2015 年、ウクライナ西部の都市である、イヴァーノ・フランキーウシク周辺で、140 万世帯が数時間の停電。Black Energy と呼ばれるマルウェアによるサイバー攻撃を受けた。

同 2015 年、トルコの首都アンカラなど、全 81 県のうち 45 県にわたり大規模停電が発生。12 時間にわたる停電で 4,000 万人以上に影響。住宅やオフィスの電気だけでなく、地下鉄、信号機、航空情報サービスなどが停滞。紛争で対立するグループからの報復によるサイバー攻撃の可能性が疑われる。

(2) 水分野の事例:

2007 年、米国の水路管理用 SCADA がマルウェアに感染した。その結果、水道経路が強制的に変更され、河川の増水に至った。水道設備では、ポンプやゲートなどから、水位の計測データを収集・監視し、ゲート開閉の制御を行うために SCADA システムが用いられている。水路システム管理者が、解雇されたことを受けて攻撃したものである。サイバー攻撃の意識が低いため、アクセス制限の管理という考えが不十分で、遠隔地から簡単に攻撃できるシステムになっていた。

(3) 自動車分野の事例:

2010 年、米国で、80 台以上の自動車において、エンジンが始動できなくなった。自動車ディーラーにおいて、解雇された従業員が攻撃したものである。もともとこのディーラーでは、自動車販売後、顧客が支払いを滞らせてしまう懸念を持っており、ディーラーからインターネット経由でイモビライザ(電子的な盗難防止システム)を操作できるようにしていた。このシステムに対するアクセス管理が不十分だったため、攻撃に使われてしまった。

(4) 鉄道分野の事例:

【事例 1: サンフランシスコ市営鉄道へのランサムウェア攻撃】

2016 年 11 月 28 日、米国サンフランシスコの市交通当局 (SFMTA) では、局内コンピュータがランサムウェアに感染し、約 900 台のコンピュータが被害にあった。これにより、メールなどのシステムが暗号化されてしまい、運用に支障が発生した。市営鉄道の安全運行には影響がないとされたが、金銭関連システムには支障が出ており、券売機などで攻撃者のメッセージが表示された。

ランサムウェアの感染は 25 日に判明した。28 日時点では、外部のシステム会社と連携してバックアップからシステム復旧を進めた。当初、職員の給与システムなど金銭関係システムへの影響が懸念され、SFMTA は 25 日から 27 日、駅の券売機を停止して、被害調査を行った。この間、乗車料金を無償化した。

SFMTA は、感染発覚の直後にランサムウェアを特定して、米国土安全保障省(DHS)に報告した。また、DHS や米国連邦捜査局(FBI)の調査にも協力した。サイバー攻撃者への身代金支払いは行っていない。駅の端末や券売機にランサムウェアの脅迫メッセージが表示され、暗号化状態を解除するための身代金 7 万 3,000 ドルを要求していた。

【事例 2: ソウルメトロで PC のマルウェア感染】

2015 年 10 月 5 日、韓国ソウルメトロの主要コンピュータサーバが、北朝鮮のサイバーテロ組織とみられるグループに、少なくとも 5 か月以上、掌握されていた。「ハッキング事故調査結果報告」によると、2014 年 7 月に、ソウルメトロの PC 管理プログラム運営サーバ 2 台がハッキングされ、PC213 台に異常な接続が行われ、PC58 台がマルウェアに感染していた。

PC 管理プログラム運営サーバは、ソウルメトロの全業務用 PC に必要なプログラムを運用管理するサーバであり、主要部門の PC (地下鉄のリアルタイム運行監視する総合管制所や、電力供給を担う電気通信事業所など)も含んでいる。

ソウルメトロへのサイバー攻撃は、2013 年に 18 万 4,578 件、2014 年に 37 万 713 件、2015 年には 9 月までで 35 万 188 件と増加していたが、実際のハッキング被害確認は今回初めてだった。

【事例 3: 米国鉄道会社のコンピュータ・システムにハッカー侵入】

2011 年 12 月、米国の鉄道会社のコンピュータがハッカー攻撃を受け、2 日間列車の運行に障害が発生した。ハッカーによるシステム侵入で、列車の運行スケジュールに 15 分の遅延が生じた。翌日もラッシュアワー前に攻撃を受けたが、その際は運行スケジュールへの影響は無かった。

調査の結果、海外から複数のハッカーが 3 つの IP アドレスを用いて鉄道会社のコンピュータ・システムに侵入したと判明した。その後 12 月 5 日に、事件経緯と 3 つの IP アドレスに関する警告通知を米国とカナダの交通機関に連絡した。米国土安全保障省(DHS)の分析によると、この攻撃はもともと無作為に行った攻撃であり、鉄道を標的にしていた訳では無かった。

【事例 4: 日本やポーランドのセキュリティ・インシデント】

2015 年 8 月 11 日、JR 北海道の PC が標的型メール攻撃でウイルスに感染した。JR 北海道によると、標的型攻撃メールを受信した PC で添付ファイルを開いたことでウイルスに感染、この PC を経由して他の

6 台にも感染が拡大した。翌 12 日に、社外から不審な通信を検知したとの通報があり、13 日に対策本部を設置した。ウイルスは情報を盗み出すタイプ(日本年金機構で確認された遠隔操作型 Emdivi)だが、鉄道運行システムへの影響や顧客情報の漏洩などは確認されていない。

実際に流出した情報は、通信量の合計が 6M バイト。本来情報を持ち出すために作成されていた圧縮ファイルは約 60M バイトあり、ファイルの送信に失敗していた。圧縮ファイルに鉄道の安全に関する機密情報は含まれていなかった。

2018 年、ポーランドでは、少年が線路のポイント切り替え機をハッキングした。14 歳の少年は、TV リモコンを改造して、列車線路のトラックポイントをハッキングして切り替えを変更した。その結果、4 台が脱線事故を起こし、また列車の急停止により 12 人のけが人を出した。少年は、電車システムを学習し、全連結部を制御できるようにリモコンを改造していた。

1.2. 拡大するセキュリティ・リスクと米国が主導するサイバー防衛

コネクテッドカーなど IoT の普及にともない、機器同士が相互接続するこれからの情報システムにおいては、末端機器の脆弱性を狙ったサイバー攻撃の影響が相互接続された機器を通じて急速に拡大し、重要インフラの停止といった重大インシデントに波及する可能性がさらに高まると考えられる。

日本国内では東京 2020 オリンピック・パラリンピック開催決定を契機に、政府主導のサイバー防衛体制の整備で先行する米国などと協力したセキュリティ情報共有が進んでいる。

(1) 自動車産業におけるコネクテッドカーの急速な普及にともない、サイバー・リスクが拡大

2020 年には、自動車 5 台に 1 台の割合で、コネクテッドカーが普及し、実数として 2.5 億台以上に拡大すると見込まれる。これに伴い、自動車のセキュリティリスクも多数顕在化してきている。

年	脅威の事例
2010	・ワシントン大学の研究者が、CAN (Car Area Network) 通信のハッキング手法を発表、2011 年にはハッキングによる遠隔操作可能性を発表
2013	・米ハッカー2 人が、トヨタ／プリウスのハッキング手法を動画公開 ・イスラエルのカーメルトンネルにサイバー攻撃。トンネル内の監視カメラがシャットダウンし、8 時間不通
2014	・米ハッカー2 人が、国際学会で「ハッキングされやすい 20 の車」発表 ・スペインの分析官 2 人が、国際会議で自律走行車のハッキング装置公表
2015	・米ハッカー2 人が、Jeep／チェロキーのハッキング手法を公開。Jeep は 140 万台をリコール(下記に詳細) ・国際学会で、トヨタ・日産・Ford・Tesla・VW への攻撃手法が紹介

【Jeep ハッキングの事例】

米国の 2 人のセキュリティ研究者が、Chrysler 社のコネクテッドカーシステム「Uconnect」の脆弱性を利用し、Jeep／チェロキーのハッキング(遠隔操作)が可能であることを発表した。

エンターテイメントシステムのチップセットのファームウェアを更新することで、エアコン・ワイパー・ブレーキ・変速機・ステアリングに干渉することが可能、バック中にはハンドル操作を奪取することが可能となる。また、ファームウェアを更新しなくても、ネットワーク内にある他の自動車情報を取得することができる。

Chrysler は、USB もしくは整備工場でパッチを提供してリコールに対応、ファームウェアを修正する。

(2) 自動車を取り巻く周辺のインフラ環境に対しても、攻撃リスクが顕在化

自動車のためのインフラ環境を管理する道路交通管制システムにおいても、サイバー攻撃リスクが高まっている。一方で、管制システムのオペレーターにはリスク認識が低く、システムは脆弱である。例えば、イ

ンサイダー(元従業員)のアクセス管理が不十分だったため、容易に攻撃されるケースもあった。

年	脅威の事例
2005	・米国で緊急車両用に赤外線信号制御システムを導入 ・制御用送信機がネット上に$500 で出回り、一般人が利用 ・2005 年に規制化し、緊急車両のみを認証するシステムに変更して対策
2006	・米／ロサンゼルスで、道路信号管理の技師が労働スト し、3,200 台の信号機制御するコンピュータアクセスをブロック ・2 人の技師がマネージャ認証番号を盗み、赤信号点灯を操作。4 つの主要交差点で交通が混乱
2014	・米／ミシガン大のデモにおいて、インテリジェント無線交通管理システムをハッキング。100 台の信号機を遠隔で操作 ・本システムに暗号や認証がなく、ID・PW もデフォルトのままで、ハッキング容易
2015	・米国の信号機制御システムで、道路交通量の計測データをセンタへ伝送する通信システムをハッキング ・交通量データとして偽情報が送られ、信号管理がかく乱

(3) IoT・ネットワーク機器の増加で高まるセキュリティ・リスク

IoT 技術が進展し、ネットワークにつながる機器が増えたことにより、ネットワーク機器へのサイバー攻撃も増加すると懸念されている。IoT でつながる機器は、2020 年に 250 億台に達すると推計され、従来インターネットに接続されなかった自動車、家電、電力メータ、産業機器やインフラそのものまでがネットワークに接続される。

年	脅威の事例
2014 年 2 月	・Linksys が、自社の無線 LAN ルータ製品への「The Moon」ウイルス感染を確認。対処方法を公表
2014 年 9 月	・ソフトウェア bash (Linux を搭載した機器に広く利用)の脆弱性 (Shellshock) を公表
2014 年 10 月	・セキュリティ企業 FireEye が、特定のネットワーク接続型のハードディスク機器(NAS)について、Shellshock を悪用されて乗っ取られる攻撃の確認を公表

(4) 脅威の高まりを背景に進む政府主導のセキュリティ対応

米国では、サイバー攻撃を戦争行為としてとらえ、政策・制度設計を政府主導で推進している。2013 年には、重要インフラのサイバーセキュリティの向上に関する大統領令を出し、重要インフラ 16 分野を対象にした国家インフラ防護計画や官民連携のサイバー情報共有・連携プログラムなどを策定した。

また、国境がないサイバー攻撃へは、単独国だけでの防御は困難であり、同盟国との協力関係も推進が必要である。米国と英国は、サイバー防衛協力を締結し、重要インフラのサイバーセキュリティ強化、サイバー防衛での連携強化などを推進している。

日本は、オリンピック開催決定を契機に、政府主導の対応を加速している。サイバーセキュリティ基本法に基づき施策運用を開始し、また米国との情報共有、イスラエルとの協力など連携を強化している。

1.3. 重要インフラ事業者による情報共有の現状

本書の使い方でも述べたように、重要インフラ事業者のセキュリティに対する認識レベルは、その事業者のいる業界によって大きく異なるのが現状である。

ネットワークインフラのセキュリティ対策が事業の根幹を支える通信キャリアやセキュリティベンダ、またテロなどを目的としたサイバー攻撃に対して従来よりセキュリティ対策を強化してきた航空などの業界は、セキュリティに

関する情報を収集するための仕掛けや大量にある情報から自事業者に関係する情報のみを選択・分析するだけの設備・人材といったリソースを事業者単独で保有している傾向がある。一方で、従来は制御ネットワークが外部ネットワークから隔離されていたために、サイバー攻撃に対するセキュリティ対策の必要性をあまり感じていなかった業界では、限られたリソースの中で自社 CSIRT(Computer Security Incident Response)を立ち上げるなどの対策を始めたばかりという事業者もある。

業界全体、さらには業界を横断する重要インフラを狙ったサイバー攻撃では、個別防衛よりも集団防衛の観点が重要であり、事業者単独のセキュリティ対策を脱し、セキュリティ情報共有の関係構築が必要となる。一方で、セキュリティ対策に比較的投資を行いやすい大企業に対し、十分な投資を行えない中小企業では、認識レベルが高くても十分なセキュリティ対策の体制を事実上構築できないといった事業体の規模に依存する課題もある。そのため、各重要インフラ事業者は、図 1-1 に示すような自社のセキュリティ対策組織のスキルに応じた情報共有の関係構築に取り組み、継続的に集団防衛の規模を拡大することが今後も重要な前提となる。

セキュリティ対策組織	通信キャリア・ セキュリティベンダ	情報システム部・ 情報システム会社を 保有するCSIRT	非IT部門で構成される CSIRT
受信者としてのセキュリティスキル • 情報を組織内で消化できるか？ • 情報の取捨選択・キュレーションができるか？	高 （可能）	⇔	低 （困難）
情報処理の手段	セキュリティ機器同士の 自動連携	⇔	セキュリティ機器へ 手作業で投入

情報発信者としての視点を強化
- 受信者のスキル・レベルを考慮して会話すること（分かってもらえることが重要）
- 受信者からのフィードバック
- 机上訓練・セミナーの主催

信頼関係の構築を強化
- 平常時のコミュニケーション
- Give&Take
- 共通の利害関係
- 情報発信力の強化
- 対面での会話による絆の構築

協力：ANAシステムズ株式会社

図 1-1 情報共有の関係構築に必要な取り組み

1.4. 情報共有の目的に応じた対策

表 1-1 に示すように、情報共有の主な目的としては、事故に遭わないため、事故に遭った時の早期復旧のため、さらに経営陣への説明・自社のベンチマークのため、などが考えられる。事故に遭わないためには情報の鮮度が重視される一方で、経営人への説明・自社ベンチマークのためには情報の確実性が重視されるなど、情報共有は目的に応じて、重視する性質、参照すべき情報源、共有すべき情報が異なる。

次節で述べる情報共有の効果を最大化するために、どのような情報が共有されるべきかの詳細については 3.5 節で述べるが、重要インフラ事業者は、共有すべき情報を目的に応じて自社で整理・管理する仕組み・方法を整備しておくことが求められる。

表 1-1 情報共有の目的と共有すべき情報

目的	事故に遭わないため	事故に遭った時の早期復旧のため	経営陣への説明・ 自社のベンチマークのため
重視する性質	鮮度 （予防・即効性・安全面を重視）	⇔	確実性 （対応もれの点検・ナレッジの蓄積・人材育成を重視）
参照すべき情報源	• 早期警戒情報 • インテリジェンス早期レポート	⇔	• 公的機関の発表 • インテリジェンス分析情報 • 事件・事故を起こした企業からの発表
共有すべき情報	予防に役立つ情報 • 各種インジケータ情報 • 脆弱性情報	インシデント発生時に役立つ情報 • 各種インジケータ情報	経営陣への説明・ 自社のベンチマークに役立つ情報 • 世間で起きている事象の解説
CSIRT間でよく交換される情報	• 事件・事故事例 • 対応策	• 対応・対処方法 • 気づかぬ被害状況の指摘	• 他社のセキュリティ対策状況 • 他社の法令対応の対策状況 • 情報の運用方法、キュレート手法
インテリジェンスから得られる情報	• 攻撃の最新手法 • 犯罪者の背景(攻撃を受ける確率判断として) • 自社に関する地下組織流通情報（将来攻撃を受ける可能性として）	• 攻撃の最新手法 • 犯罪者の背景(攻撃の目的の判断として)	-

協力：ANAシステムズ株式会社

1.5. 情報共有および対策の実行により事業者が得る効果

1.1 節で述べたように、サイバー攻撃が高度化・増加する傾向にあるなかで、外部の信頼できる情報機関から脅威情報を迅速に入手し、社内外の関係者と共有・連携しながら対策することが重要である。しかし、情報共有の取組みは、まだ十分に普及しているとは言えない状況であり、その一因としては、事業者が情報共有することによって得られる効果が、十分に理解されていないことも考えられる。

そこで、情報の共有および対策の実行により事業者が得る効果を、以下に示す。

1.5.1. 効果の考え方

情報の共有および対策の実行により事業者が得られる効果は、効果が発現するタイミングによって「(1)情報が共有されることのみで得られる効果」、「(2)共有によって得た情報を基にサイバー攻撃対策に取り組んだ場合に得られる効果」、「(3)(2)の効果が得られたことによって最終的に得られる効果」に分けることができる。

また、情報共有のシーン（【平時】、【インシデント発生時】、【平時、インシデント発生時共通】）によって異なると考えられる。

したがって、本書では、「効果が発現するタイミング」と「情報共有のシーン」の 2 軸に沿って、情報の共有および対策の実行により事業者が得る効果を整理する。

1.5.2. 効果の全体像

前述した 2 軸に沿って整理した、情報の共有および対策の実行により事業者が得る効果（仮説）を図 1-2 に示す。

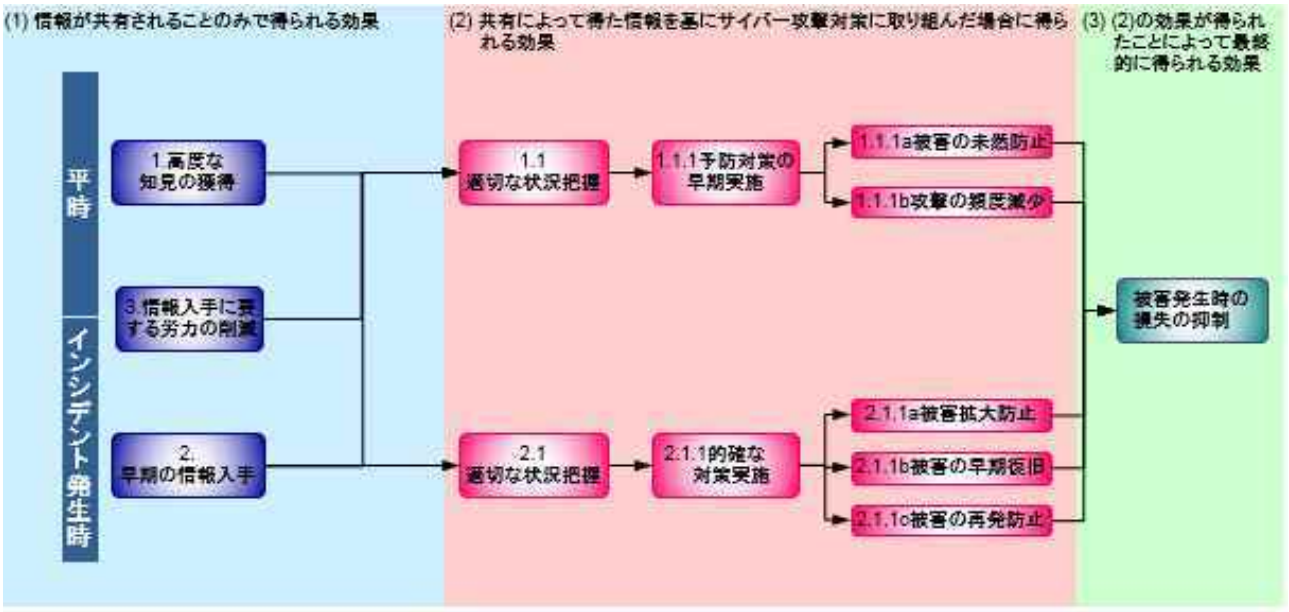


図 1-2 情報を共有することおよび対策に取り組むことによって得られる効果(仮説)

(1) 情報が共有されることのみで得られる効果

「1.高度な知見の獲得」(平時)、「2.早期の情報入手」(インシデント発生時)、「3.情報入手に要する労力の削減」(平時・インシデント発生時共通)の 3 つが挙げられる。

平時においては、他の事業者等で発生したサイバー攻撃について、単なる事実情報に加え、攻撃の分析結果や今後の予防策等の「高度な知見」を得ることができるようになると考えられる。

インシデント発生時においては、何よりもまずサイバー攻撃に関連する情報を入手することが必要であり、事業者が単独で収集するよりも早期に入手できるようになると考えられる。

また、平時、インシデント発生時に関わらず、有益な情報が随時必要なタイミングで得られるようになるため、各事業者で必要な情報の検索、収集等を行う労力を削減することができると考えられる。

(2) 共有によって得た情報を基にサイバー攻撃対策に取り組んだ場合に得られる効果

情報共有のシーンによって、以下のように整理することができる。以下の番号表記(1.1 等)は、図 1-2 情報を共有することおよび対策に取り組むことによって得られる効果(仮説)中のものと対応している。

【平時】

(1.1) 適切な状況把握

・ セキュリティに係る高度な知見(他の事業者等で発生したサイバー攻撃の分析結果、今後取るべき対応策等)を獲得できるようになるため、自組織の体制が十分でなくとも見落とし等を防ぎ、適切に状況を把握することができる

(1.1.1) 予防対策の早期実施

・ 適切に状況を把握できるようになるため、自組織のセキュリティ上の問題点に対して予防対策を早期に実施することができる

(1.1.1a) 被害の未然防止

・ 予防対策を早期に実施できるようになるため、対策を実施していない際に発生していたであろう被害を防止することができる

(1.1.1b) 攻撃の頻度減少

・ 予防対策を早期に実施できるようになるため、堅牢な環境になることにより、サイバー攻撃が困難化することで攻撃される頻度を減らすことができる

【インシデント発生時】
(2.1) 適切な状況把握
・ 早期に情報を入手することができるため、自組織で発生しているインシデントの状況を、適切に把握することができる
(2.1.1) 的確な対策実施
・ 発生しているインシデントについて適切に状況を把握することができるため、実施すべき的確な対策を実施することができる
(2.1.1a) 被害拡大防止
・ 的確な対策を実施しているため、自組織や他の事業者等への被害の拡大を防止できる
(2.1.1b)被害の早期復旧
・ 的確な対策を実施しているため、発生したインシデントから早期に復旧できる
(2.1.1c) 被害の再発防止
・ 的確な対策を実施しているため、類似障害が再度発生することを防止することができる

(3) (2)の効果が得られたことによって最終的に得られる効果:被害発生時の損失の抑制
前述した(2)の効果が得られることによって、平時においてもインシデント発生時の対応後においても、サイバー攻撃によって事業者が被害を受けた場合の損失を抑制できる。

以上に述べた内容は仮説であるが、サイバー攻撃が増加、高度化している現状に対し、サイバー攻撃の被害を最小化する等の効果が期待できることを踏まえ、情報共有を推進すべきと考える。

1.6. 日本の重要インフラ事業者における情報共有の現状
1.6.1. 重要インフラ事業者における情報入手の現状
従来、各事業者は、以下に挙げるような手段を用いてサイバー攻撃やその対策に関する情報を入手してきた。
- サイバー攻撃やそれらへの対策に関する情報の収集・提供を行う機関からの配信[7][8][9]
- 有識者で構成される非公開コミュニティでの共有[10]

サイバー攻撃に関する情報を、情報の収集・提供を行う機関からの配信等により入手しており、以下のような課題があるため、事業者による対策が遅延する可能性がある。
① 有識者がいない事業者は、情報の収集・提供を行う機関からの情報展開を待つしかない
② 情報の収集・提供を行う機関からの情報展開速度は、担当者の状況に依存する
③ 複数の組織から情報を入手した場合に、最新情報等の把握に時間がかかる

サイバー攻撃や対策に関する情報を上記のような手段によってしか入手できない場合、有識者がいない事業者では、情報の収集・提供を行う機関が展開する情報を受信するまで、対策を講じることができない。更に、情報の収集・提供を行う機関は、情報を配信する前に、得た情報の精査、分析等を行うのが一般的であるため、実際に情報を配信するまでにも一定の時間を要する。また、情報の収集・提供を行う機関からの情報の展開は、担当者からのメールや電話等で行われることも多く[11]、情報が伝わる速度は担当者が置かれている状況に依存するのが実態である。
一方で各事業者は、複数の組織から情報を受信する可能性があるため、同一の攻撃に関する最新の状況や対策等を含む情報がどれであるか把握するのに時間を要するといった点も、対策の実施が遅延する一因になっている。

1.6.2. 既存の情報共有に係る取組み

2015 年に閣議決定された「サイバーセキュリティ戦略」において、重要インフラをサイバー攻撃から守るために推進する事項として、「効果的かつ迅速な情報共有の実現」が掲げられており、年次計画である「サイバーセキュリティ 2018」において、具体的な施策が示されている。

2019 年 3 月時点で、重要インフラ分野における情報共有体制が複数活動しており、その代表的なものとして内閣官房、経済産業省および総務省の取組みを例示する。

(1) 内閣官房(NISC)

内閣官房の取組みとしては、NISC 主導のもと、重要インフラ事業者等の情報共有・分析機能および当該機能を担う組織である「セプター(CEPTOAR:Capability for Engineering of Protection, Technical Operation, Analysis and Response)」の活動を推進している。2018 年 4 月末時点で、各重要インフラ分野の業界団体等が事務局となり、全 14 分野、計 18 のセプターが活動している。セプターでは、重要インフラサービス障害の未然防止、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いる。また、分野横断的な情報共有の推進を目的として、各セプターの代表で構成される協議会である「セプターカウンシル」が設立されており、具体的な情報共有プロジェクトとして「C^{4}TAP:Ceptoar Councils Capability for Cyber Targeted Attack Protection[1]」等を運用している。

また、重要インフラ事業者は、法令等で義務付けられている事象は所管省庁へ直接報告する必要がある。情報共有の活性化に向けて、報告が義務付けられていない事象については、従来の所管省庁へ直接報告するルートに加え、セプター事務局を経由して所管省庁に報告するルートを新設した。セプター事務局を経由して所管省庁に報告するルートでは、セプター事務局において情報連絡元の匿名化等を実施することにより、事業者が情報共有を心理的障壁なく、実施することが期待できる。

(2) 経済産業省(IPA)

経済産業省の取組みとしては、IPA が発足させた「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)」が挙げられる。J-CSIP は、サイバー攻撃による被害拡大防止のため、重要インフラで利用される機器の製造業者を中心とする、情報共有と早期対応の場であり。2019 年 1 月 31 日時点では、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)、249 の参加組織による情報共有体制を確立し、サイバー攻撃に関する情報共有の実運用を行っている。IPA と各参加組織は秘密保持契約(NDA)を締結したうえで、検知したサイバー攻撃等の情報を IPA に集約している。その後、情報提供元等を匿名化し、IPA が分析情報を付加したうえで、情報提供元の承認を得て、参加組織間で共有している。

(3) 総務省

総務省の取組みとしては、一般社団法人 ICT-ISAC と連携した「サイバー攻撃の防御に向けた情報共有基盤に関する実証事業」が挙げられる。2017 年度は、STIX/TAXII での情報提供、情報共有基盤でのサイバー攻撃情報の集中管理等の運用について実証した。また、2018 年 6 月 29 日には、実証成果を踏まえて、ICT-ISAC が「脅威情報の情報共有基盤利用ガイドライン」を策定している。なお、2016 年 3 月に設立した ICT-ISAC は、サイバーセキュリティに関する情報収集・調査・分析をはじめとして、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等を推進している。

(4) ISAC

サイバーセキュリティに関する情報共有および分析を行う組織として、「ISAC:Information Sharing and Analysis

[1] セプターカウンシルにおける標的型攻撃が疑われるメールに関する情報共有体制

Center」の整備が進んでいる。ISAC は、前述した ICT-ISAC の他にも、金融 ISAC、電力 ISAC、J-AUTO-ISAC 等が既に整備されている。今後は、交通 ISAC を初めとして、他の分野でも整備が進むと想定される。

(a). ICT-ISAC

ICT に関わるさらに幅広い企業・団体と協力連携し、安全な ICT 社会の形成に寄与することを目的として、2016 年 3 月に設立された。ISP を含む通信事業者、放送事業者、ソフトウェアベンダー、情報提供サービス事業者、情報関連機器製造事業者が参加している。

(b). 金融 ISAC

金融機関の間でサイバーセキュリティに関する情報の共有・分析、および安全性の向上のための協働活動を行い、金融サービス利用者の安心・安全を継続的に確保することを目的として、2014 年 8 月に設立された。銀行、保険など 363 社(2019 年 1 月 30 日現在)が参加し、共同演習など 10 つのワーキンググループが活動している。

(c). 電力 ISAC

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、2017 年 3 月に設立された。電力・ガス業界の企業が参加している。

(d). J-AUTO-ISAC

日本国内の自動車におけるインシデントに対して、適切かつ迅速な対応をするために、2017 年 1 月に(一般社団法人)日本自動車工業会の安全・環境技術委員会の下に設立された。12 社の自動車メーカーが参加している。

(5) まとめ

上述のように、情報共有に関する複数の取組みが実施されている。「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」に記載されているとおり、一部の分野で情報共有が活性化しているものの、重要インフラ分野全体ではまだ十分な情報共有が実施されていないのが現状である。

1.6.3. 直近の動向

(1) サイバーセキュリティ対処調整センター(政府オリンピック・パラリンピック CSIRT)

日本は東京 2020 オリンピック・パラリンピック競技大会という国際的な注目度が高く、サイバー攻撃のターゲットとなる可能性が高いイベントを控えている。近年の国際的なイベントを振り返ると、2016 年リオデジャネイロオリンピック・パラリンピック競技大会では、大会期間中に、大会関連 Web サイトだけでなく、連邦政府や州政府など周辺の Web サイトも攻撃を受けた。また、2018 年平昌オリンピック・パラリンピック競技大会では、大会運営に重大な影響を与えるようなサイバー攻撃は発生していなかったが、大会準備期間に約 6 億件、大会期間に約 550 万件のサイバー攻撃が発生している。

そこで、NISC は関係組織に対して対処のための的確な情報共有を担う中核的組織として、サイバーセキュリティ対処調整センター(政府オリンピック・パラリンピック CSIRT)の整備を進めた。具体的には、2020 年東京オリンピック・パラリンピック競技大会におけるサイバーセキュリティ体制に関する体制検討会を通じ、政府/関連組織の役割を整理し、具体的な体制が検討された。2018 年 7 月 25 日に策定された「サイバーセキュリティ 2018」では、2018 年度末を目途にサイバーセキュリティ対処調整センター(政府オリンピック・パラリンピック CSIRT)を構築することが示されている。

2019 年度からは要員の訓練、情報共有システムのユーザーに対する操作訓練、情報共有訓練およびインシデント発生時の対応訓練支援が実施できるよう準備が進められ、大会直前まで重要サービス事業者等が参加

する訓練・演習を繰り返し、大会関係組織間で緊密に連絡調整を図るための態勢を整備し、大会までの大規模イベントである G20、ラグビーワールドカップ等において情報共有体制の試験運用を実施する予定としていた。

(2) サイバーセキュリティ基本法の一部を改正する法律(改正サイバーセキュリティ基本法)

2020 年東京オリンピック・パラリンピック競技大会の開催に向け、「サイバーセキュリティ協議会」を創設するなどの内容を含んだ「サイバーセキュリティ基本法の一部を改正する法律(以下、「改正サイバーセキュリティ基本法」という)」が、2018 年 12 月 5 日に参議院本会議で可決、成立し、2019 年 4 月に施行された。

サイバーセキュリティ協議会は、官民の多様な主体が相互に連携し、サイバーセキュリティに関する施策の推進に係る協議をするための協議会であり、国の行政機関や地方公共団体、重要インフラ事業者、サイバー関連事業者、教育研究機関、有識者などが構成員として想定されている。サイバーセキュリティ協議会では、情報共有のデメリットの除去に加え、協議会の運用ルールにより情報提供を行うメリットを付加することが検討されている。具体的には、情報共有のデメリットを除去するための措置として、構成員は協議会から情報提供の協力を要請された場合、それに応じる必要があり(情報提供義務)、罰則により担保された守秘義務を適用する。また、情報提供を行うメリットを付加するための措置として、提供者のモチベーションと提供される情報の質を維持するために、積極的な情報提供に能力と意欲を有する者を、一般の構成員と別に「特別貢献構成員(仮称)」としてグループ化する。特別貢献構成員(仮称)のメリットとしては、「提供した未確定の情報に対して相互にフィードバックを行うことで、提供した情報の確度を高めることができる」、「各主体がフィードバックだけでなく、自らも積極的に情報を提供するギブアンドテイクの原則を徹底することで、特別貢献構成員のみに共有される情報を得ることができる」といったことが挙げられている。

今後、サイバーセキュリティ協議会の組織および運営に関し必要な事項について、協議会の運用ルール(規約)で整備される予定である。

2. 情報共有の海外事例

日本全体としての情報共有のイメージ(仮説)を検討するうえで、情報共有の取組みが日本よりも先行している海外の情報共有事例が参考になる。

本書では、英国および米国の情報共有事例を紹介する。

2.1. 情報共有の海外事例(英国)

英国におけるサイバーセキュリティ対策は、従来、複数の省庁に機能が分散しており、それぞれが対応していたが、「国家サイバーセキュリティ戦略 2016」に基づいて、2016 年 10 月に政府通信本部(GCHQ)の配下に国家サイバーセキュリティセンター(NCSC:National Cyber Security Centre)を設立したことに伴い、政府のサイバーセキュリティに関する各種機能は NCSC に統合されている。

NCSC は、「オンラインでのビジネス、生活において、英国を最も安全な場所にすること」を使命としており、官民におけるサイバー脅威の情報共有を推進している。具体的な情報共有の取組みとしては、後述するサイバーセキュリティ情報共有パートナーシップ(CiSP:Cyber-security Information Sharing Partnership)を初めとして、CNI Sector and Wider Economy Information Exchanges(サイバー関連の動向や問題について定期的に話し合うグループ)、国家重要インフラ(CNI:Critical National Infrastructure)に対する脅威の評価レポートの共有、NCSC の Web サイトを通じたサイバー関連のニュース、アドバイス等の情報提供等を実施している。

図 2-1 に、NCSC におけるインシデント対応の流れを示す。

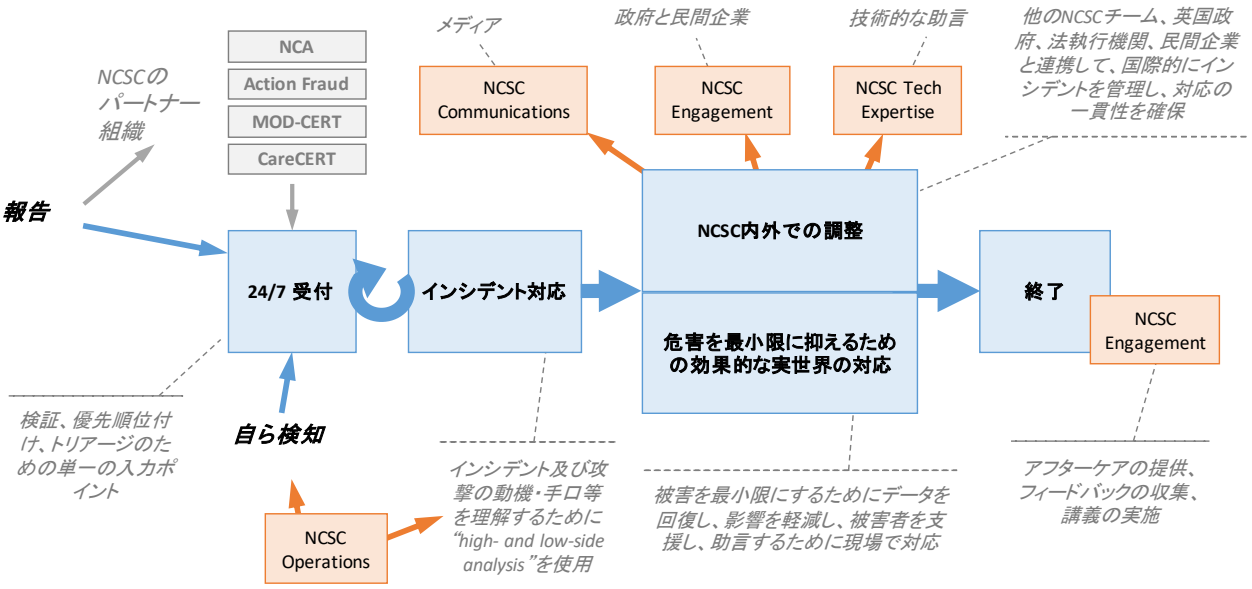


図 2-1 NCSC におけるインシデント対応の流れ

また、業界内における情報共有の取組みとして、ISAC は存在していないが、「Information Exchange」がある。これは、対面での情報共有が基本であり、TLP に即した電子メールでの情報交換も実施している。

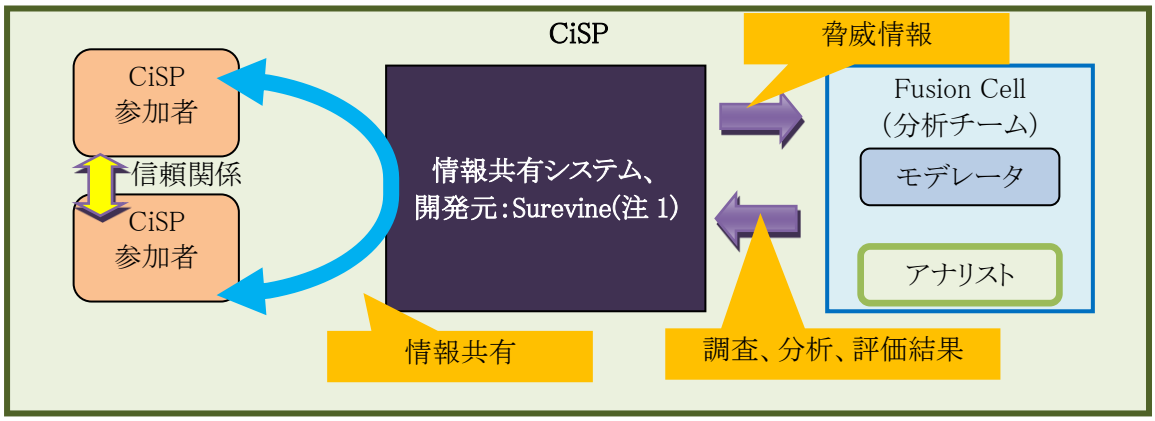
2.1.1. CiSP(英国)

(1) 概要

CiSP は、政府と企業の情報共有とインシデントの管理のための信頼関係にある組織間の情報共有の場として、2013 年 3 月に発足し、2019 年 3 月現在は NCSC が運営している。CiSP は、サイバー脅威の気づきと英国ビジネスへの影響を緩和するためにサイバー脅威と脆弱性情報を共有することを目的としている[1]。CiSP に参加できる組織は、英国に本社がある企業や英国における電気通信事業、政府組織により設立された組織である。また、個人の参加も可能であり、既存の CiSP 参加者からの推薦を受けることによって、参加することが可能となる。2019 年 3 月時点では 5,000 以上の組織、11,242 の個人が CiSP に参加している。

CiSP では、警告および勧告、NCSC の四半期毎・年次のレポート、マルウェアやフィッシングメールの分析、対面での簡潔な説明(ブリーフィング)、会員ネットワークの監視とオペレーターの支援、Fusion Cell からの CiSP データ(およびフィード)の強化、国際的なパートナーからのレポート等、様々なサービスを提供している。

CiSP の全体の概要を図 2-2 に示す。マルウェアの分析等を担当する Fusion Cell という組織(2019 年 2 月現在、30 名程度が所属)と、その組織に所属するモデレータ、アナリストがいる。



(注 1) Surevine 社は、2008 年 10 月 1 日に英国で設立された横断的な情報共有のためのシステムを開発し、提供する企業。英国政府の研究プロジェクトから独立した 20 人程度のサイバーセキュリティのスペシャリスト が所属。

図 2-2 CiSP の全体の概要

(2) CiSP を支える技術や運用

(i) 個人間でコミュニケーションを行うための情報共有システム

CiSP では、サイバー脅威情報について議論するために、SNS のように個人間でコミュニケーションを行うための機能を持つ情報共有システムを採用している。参加組織および個人は無料で CiSP の情報共有システムを利用することができる。

情報共有システムの主な機能としては、サイバーセキュリティインシデントやアラート、ベストプラクティスおよび分析情報の共有、メンバーでの議論の他、個人のメンバー同士のメッセージ送信、特定のメンバーに限定した「グループ」での情報共有、特定の論点に対する投票等がある。また、2019 年 2 月時点では STIX/TAXII を実装していないが、将来的には実装することを検討している。

図 2-3 に、CiSP で設定可能な「グループ」の種類を示す。

[1] SUREVINE, “case study”, https://www.surevine.com/wp-content/uploads/2016/02/cisp_case_study_web_2016.pdf

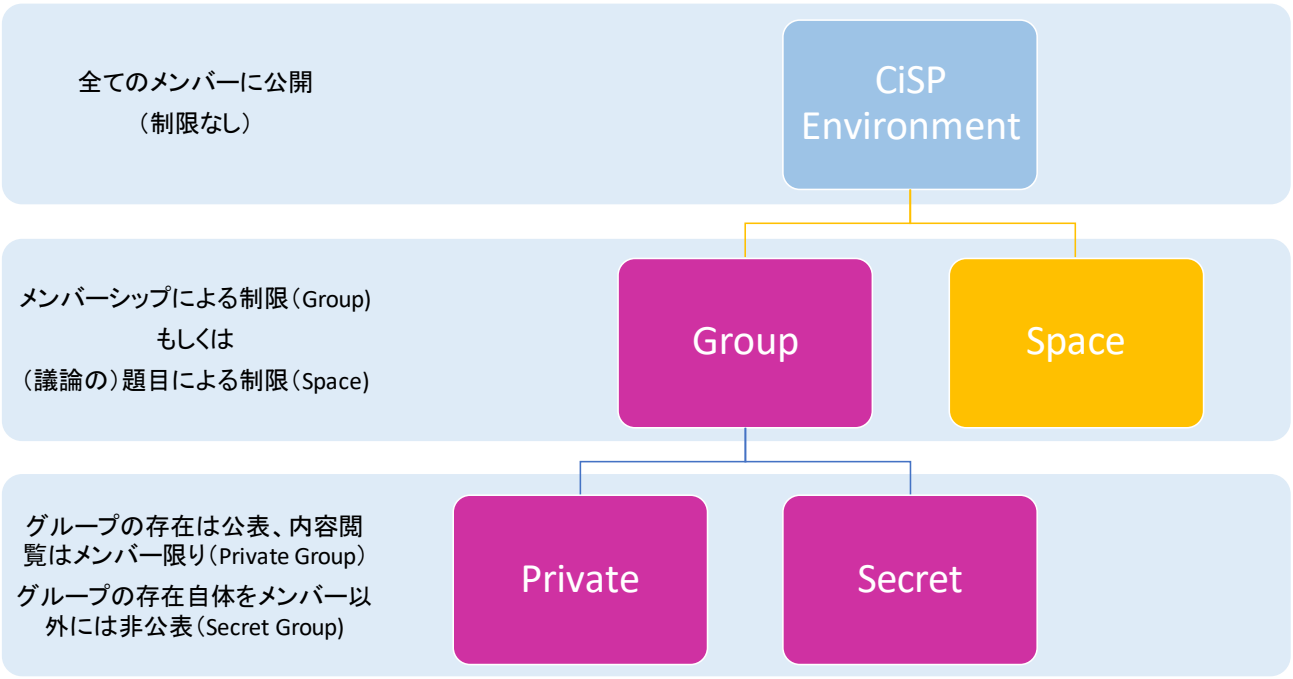


図 2-3 CiSP で設定可能な「Group」の種類

(ii) モデレータ

CiSP では、情報共有が円滑かつ効果的に行われるようにするために、モデレータという役割の参加者がいる。民間企業および政府から選出された数名が、モデレータとして登録されている。モデレータは、CiSP で共有されている全ての情報にアクセスすることができ、参加者の支援等を行っている。そのモデレータの活動の例を表 2-1 に示す。

表 2-1 モデレータの活動の例

#	役割	概要
1	投稿された情報の補完や投稿した参加者への支援	正しい回答を得ることができるようにコメントの付与や解決できる知識を持つ参加者を紹介する
2	投稿された情報の共有範囲の拡大	コミュニティと投稿者に許可をもらい、投稿された情報を匿名化して、別のコミュニティに紹介する
3	投稿された内容の確認や削除	第三者の著作権を無視した投稿や、個人情報が含まれる投稿等、問題がある投稿を削除する
4	参加者への指導	著作権や個人情報などが含まれる投稿をする参加に対して利用規約に従うように指導をする
5	参加者アカウントの無効化	利用規約に反した内容を投稿する参加者や悪意のある内容を頻繁に投稿する参加者のアカウントを無効にする

(iii) アナリスト

サイバー情報とデータフィードを調査し、分析を行い、状況に応じたサイバー脅威と脆弱性評価を提供する。官民のセキュリティアナリストがその役割を担っている。

(iv) TLP(Traffic Light Protocol)

情報提供者が提供する情報の共有範囲を指定する TLP を導入している。4 つの区分が定義されており、情報提供者は、自身が望む共有範囲に応じて、区分を指定する。

(v) 参加者間の信頼関係

CiSP に個人で参加するためには、既に CiSP に参加している人からの推薦が必要であり、このことが CiSP 参加者間における信頼醸成にある程度寄与している。

(3) ポイント

CiSP は、SNS を活用し、サイバーセキュリティ専門家だけでなく、様々な参加者を交えてサイバー脅威情報について議論することが可能であり、気軽に議論できる場を作り上げている。

共有される情報の量が多く、初歩的な情報から専門的な情報まで多種多様な内容を取り扱うために、モデレータを、サイバー情報とデータフィードの調査・分析および状況に応じたサイバー脅威と脆弱性評価を提供するためにアナリストを、それぞれ設置している。

CiSP の参加者は、TLP で自らが希望する共有範囲を設定して情報提供できること、メンバーを限定したグループでの議論ができること、個人の参加者は既存の参加者からの推薦を受けていること等により、安心して情報を提供できる。

2.2. 情報共有の海外事例（米国）

米国における情報共有の取組みは、業界毎の ISAC の設置を契機として始まった。その後、2015 年 2 月の大統領令 13691 号（PDD 13691：Presidential Decision Directive−13691）により、民間部門と政府間のより良いサイバーセキュリティ情報の共有を促進し、民間部門間の協力と情報共有を強化するために ISAO（Information Sharing and Analysis Organization）の設置が推奨された。

2015 年 10 月に成立したサイバーセキュリティ情報共有法（CISA：Cybersecurity Information Sharing Act）では、民間企業が情報共有する際の法的責任（顧客のプライバシー保護）が免除され、セキュリティ事故等が発生した場合の政府への情報提供を民間企業が拒否できない環境が整備された。

2018 年 11 月には、米国国土安全保障省（DHS：Department of Homeland Security）配下にサイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA：Cybersecurity and Infrastructure Security Agency）が設置され、サイバーセキュリティおよび重要なインフラのセキュリティプログラム、運用、および関連するポリシーを先導する責務を担っている。

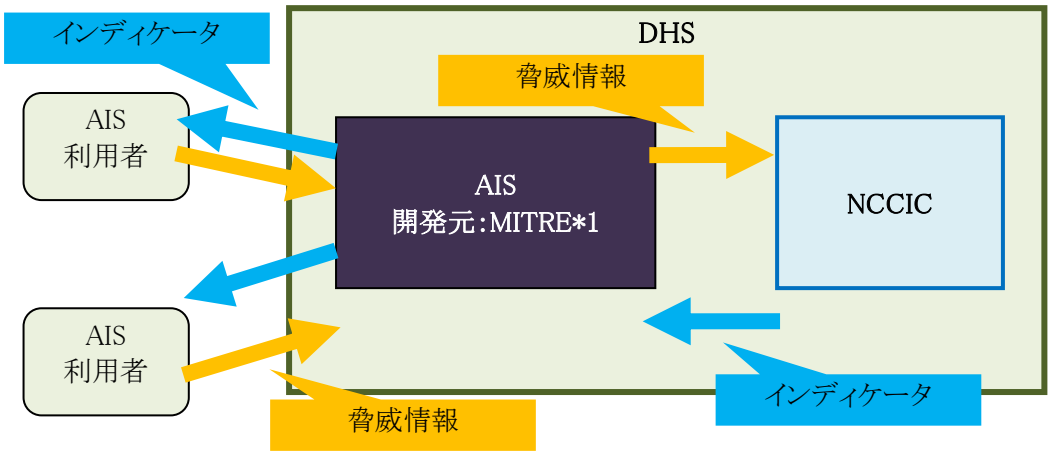
また DHS 配下の国家サイバーセキュリティ通信総合センター（NCCIC：National Cybersecurity and Communications Integration Center）は、重要インフラ分野を中心とするサイバー関連情報の集約機関であり、連邦政府や ISAC や ISAO、ベンダー等多様な情報源から可能な範囲で情報を収集し、分野横断の状況認識およびサイバー脅威の全体像の把握を行っている。

2.2.1. DHS AIS(米国)

(1) 概要

AIS（Automated Indicator Sharing）は、グローバルなサイバーセキュリティの対策能力の向上を目的とし、2016 年 3 月に DHS が提供を開始した情報共有システムである。概要のイメージを図 2-4 に示す。AIS では、攻撃指令サーバのドメインや IP アドレス、マルウェアのハッシュ値などのサイバー脅威情報を記述した検知指標(インディケータ)を収集すると共に、NCCIC で分析したサイバー脅威情報を記述した検知指標(インディケータ)を配信している。AIS にある検知指標(インディケータ)の数は、設立時から数えて 43,000 件あり、そのうちの大多数は米国連邦政府から提供された情報である。

なお、DHS は、AIS を用いて検知したサイバー脅威情報を集約し、検知指標(インディケータ)を自動的に作成し、リアルタイムに配信することを目標としている。



*1 米国の非営利団体。

図 2-4 AIS の概要

(2) AIS を支える技術や運用

(i) STIX や TAXII

AIS では、サイバー脅威情報を STIX 形式で表現して提供している。また、様々な企業や組織とサイバー脅威情報を交換することができるように、サイバー脅威情報を交換するための標準的なプロトコル TAXII を採用している。

標準の仕様を用いることで、情報を分析などで利用しやすくなる。また、標準プロトコルを用いることで、企業や組織のシステムと AIS との接続確認などが容易になる。

(3) ポイント

サイバー脅威情報を交換するための標準的な仕様(STIX/TAXII)を採用することにより、AIS との接続を容易とし、更に、受信者による受信した情報の分析も容易とすることを可能としている。

2.2.2. ISAC(米国)

ISAC のコンセプトは、1998 年 5 月 22 日に大統領令 63 号(PDD 63)の中で公表された。大統領令 63 号では、重要インフラ分野が攻撃される可能性を懸念して、所管組織の決定と情報共有の専門組織の設立を推奨しており、情報共有の専門組織の機能として、分野における脅威や脆弱性に関する情報を分野内で共有することを求めている。この要求に対応する形で、ISAC が設立された。2018 年 9 月時点、24 の ISAC が設立されている。米国の ISAC を表 2-2 に示す。

表 2-2 米国の ISAC 一覧

#	名称	分野
1	AUTOMOTIVE ISAC	自動車
2	AVIATION ISAC	航空
3	COMMUNICATIONS ISAC	通信
4	DEFENSE INDUSTRIAL BASE ISAC	防衛
5	DOWNSTREAM NATURAL GAS ISAC	天然ガス供給
6	ELECTRICITY ISAC	電力
7	EMERGENCY MANAGEMENT AND RESPONSE ISAC	緊急管理
8	FINANCIAL SERVICES ISAC	金融
9	HEALTH ISAC	健康
10	HEALTHCARE READY	医療
11	INFORMATION TECHNOLOGY ISAC	情報技術
12	MARITIME ISAC	海運
13	MULTI-STATE ISAC	自治体
14	National Defense ISAC	国防
15	OIL & NATURAL GAS ISAC	石油・天然ガス
16	REAL ESTATE ISAC	不動産
17	RESEARCH AND EDUCATION NETWORK ISAC	研究・教育
18	RETAIL CYBER INTELLIGENCE SHARING CENTER	小売
19	SURFACE TRANSPORTATION, PUBLIC TRANSPORTATION AND OVER-THE-ROAD BUS ISACS	輸送
20	WATER ISAC	水
21	Indiana ISAC	特定地域
22	Identity Theft Tax Refund Fraud -ISAC	税
23	Elections Infrastructure ISAC	選挙
24	Industrial Control System ISAC	制御システム

以下、ISAC のうち「AUTOMOTIVE ISAC（以下、「Auto-ISAC」という）」、「Electricity ISAC（以下、「E-ISAC」という）」、「Healthcare Ready」を例に、それぞれの概要等を示す。

【Auto-ISAC】

(1) 概要

Auto-ISAC は、自動車に係るサイバーセキュリティリスクへの対処に向けたグローバルな情報共有を目的として、乗用車の OEM メーカーによって設立された。図 2-5 に示すような、コネクテッドカーに係る脆弱性やインシデント、ベストプラティクス等を共有している。

当初の参加組織は、乗用車の OEM メーカーに限られていたが、自動車部品メーカーや大型トラックの OEM メーカー等に対象に拡大した。2019 年 3 月現在、自動車の OEM メーカー、自動車部品メーカーで、政府の管轄でない民間企業であり、サイバー犯罪法を持ち、積極的にサイバー犯罪者を訴追し、米国に対するテロ行為

や企業スパイを支持していない国に本社があれば、Auto-ISAC に参加することができる。米国だけでなく、日本、韓国、ドイツなどの 40 以上の組織が参加し、世界規模での情報共有を目指している。そこで、各地域が参加し易いように時差を考慮した時間帯に特定地域向けのアナリストワーキンググループを月次で開催しており、2019 年 2 月時点では、日本、韓国、欧州向けのワーキンググループを開催している。参加企業は、その売上高に応じた会費が定められており、プラチナ・ゴールド・シルバー・ブロンズの 4 つのランクに分かれている。OEM メーカーのゴールド会員とプラチナ会員は取締役会（Board of Directors）、商用車メーカーやサプライヤーのゴールド会員とプラチナ会員は諮問委員会（Affiliate Advisory Board）に参加することができる。

参加要件を満しておらず、Auto-ISAC に参加できないセキュリティベンダー、業界団体、研究者、政府機関、金融機関、トレーニング会社、および投資家等に対して、表 2-3 に示すパートナーシッププログラムを設けている。パートナーシッププログラムに参加することにより、Auto-ISAC が作成した TLP が White または Green のレポートを受け取れる、月次の電話会議に参加できる等のメリットを享受することができる。また、参加していない組織であっても、Auto-ISAC に対して情報提供することは可能である。参加していない組織からの情報も受け付けることによって情報源を多様化し、情報を可能な限り早期に入手することを目指している。

表 2-3 Auto-ISAC のパートナーシッププログラム

#	プログラム名	対象組織	概要
1	INNOVATOR	コネクテッドカーに係るサイバーセキュリティの製品やサービスを提供している企業	ISAC との連携 等
2	NAVIGATOR	業界団体	ガイダンスやサポートを受ける等
3	COLLABORATOR	政府系組織、他の ISAC 等	情報交換を実施する 等
4	BENEFACTOR	自動車業界に興味がある企業	月次で会議に参加する 等

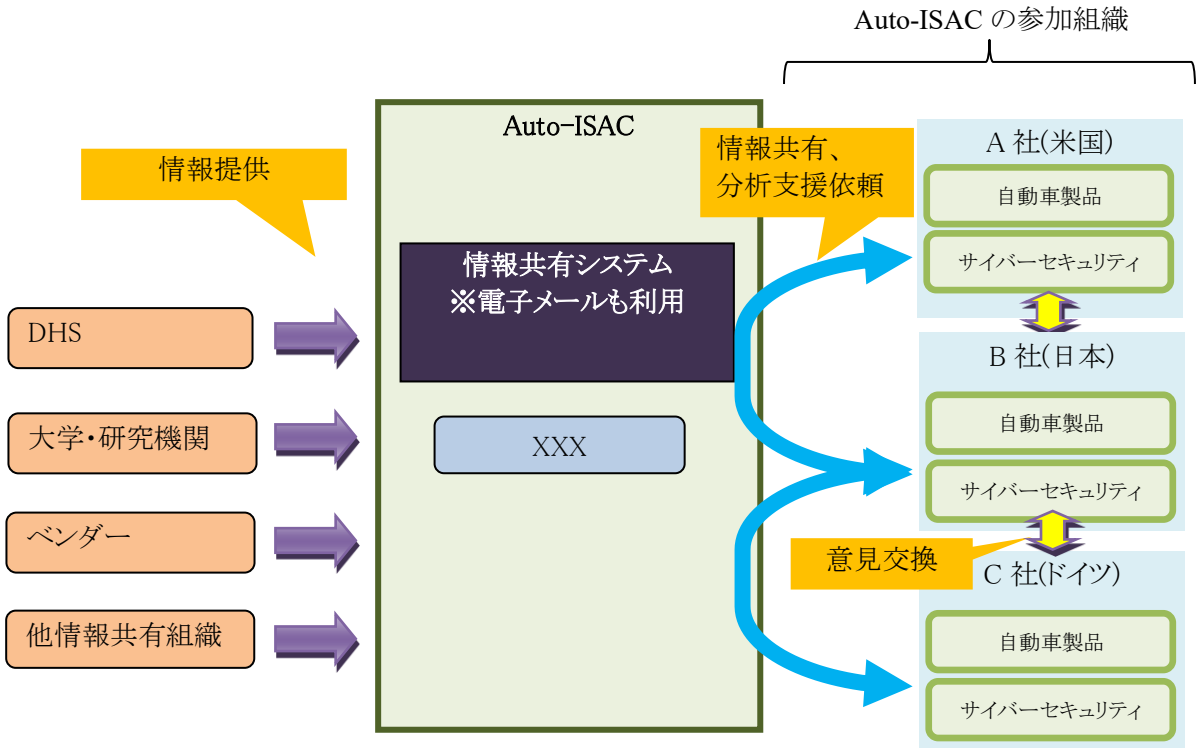


図 2-5 Auto-ISAC の情報共有の全体像

(2) Auto-ISAC を支える技術や運用

(i) 匿名化

参加組織は、Auto-ISAC に情報を共有する際に、匿名化を実施するかを選択することができる。また、ディスカッション機能においても匿名で発言することができる。

(ii) 参加組織の専門家による分析

Auto-ISAC の参加組織は、Auto-ISAC との窓口として「自動車製品」と「サイバーセキュリティ」の専門家を 1 人ずつ配置することなっており、参加組織から分析依頼等があった場合には、他の参加組織の専門家が協力し、解決している。各参加組織の専門家は、Auto-ISAC に長期間所属することにより信頼関係を構築し、直接やり取りをすることができるようになる。また、信頼関係を構築するために、毎月開催されるコミュニティコールなど対話する機会を多く設けている。

したがって、Auto-ISAC にはアナリストが所属する必要はなく、情報を仲介することが主な役割となっている。

(iii) 情報共有の活性化策

情報共有を活性化させるために、アナリストワーキンググループや情報共有常設委員会（the Information Sharing Standing Committee）を設置している。アナリストワーキンググループは、高頻度で会議を開催し、サイバーセキュリティにおける関心事項について議論している。

(iv) 複数の手段を活用した情報共有

Auto-ISAC では、参加組織との情報共有手段として、電子メールと情報共有システムを活用している。電子メールでは、機密性の低いイベント情報を配信している。情報共有システムでは、脅威情報やレポートなど機密性の高い情報の共有や参加組織同士のディスカッションを実施している。ディスカッションは活発に実施されており、毎日何かしらのトピックスについて投稿が行われている。

なお、情報共有システムに関し、一部の参加組織から STIX/TAXII を活用したいという要望があるため、将来的には導入することを検討している。

(3) ポイント

Auto-ISAC に対する情報発信や情報共有システムでのディスカッション時に、参加組織が匿名化の要否を選択することができるため、安心して情報共有に参加することができる。

各参加組織に所属する専門家同士の間で信頼関係を構築するうえで、対面で直接対話する機会（コミュニティーコール等）が大きな役割を果たしている。

情報共有の手段として用いている電子メール、情報共有システムのいずれも STIX/TAXII を用いていないが、将来的に STIX/TAXII に対応する可能性があることを見据えて、情報共有システムは容易に対応できる仕組みになっている。

Auto-ISAC の参加組織は、いずれも企業規模が比較的大きいため、Auto-ISAC にはアナリストを配置せず、各参加組織の専門家同士が連携することによって、自動車業界としてのバーチャルな分析組織を構築することができている。

【E-ISAC】

(1) 概要

E-ISAC は、北米電力信頼度協会によって、「政府等と協力して電気分野における自発的な協力と情報共有を促進すること」や「サイバー攻撃および物理的な脅威、脆弱性に対して、分野内の防護策を支援すること」により電力の安定供給を目的として、2000 年に設立された。電力の安定供給を目的としているため、サイバー攻撃に係わる情報だけでなく、電圧や周波数の急激な変化等についても共有することとなっている。北米電力信頼度協会に参加している事業者は、基本的に E-ISAC に参加しており、参加事業者は 1,900 以上となっている。

ISAC は主に、「分野内、国土安全保障省および他の政府機関との間で実在、潜在的脅威および脆弱性に関する情報の共有」、「収集した情報から傾向や、他分野との依存性、特定の対象に関する分析」、「他の ISAC との調整」、「電力分野における、サイバーインシデントの影響分析および対策の検討」を実施している。

(2) E-ISAC を支える技術や運用

(i) STIX／TAXII

E-ISAC では、サイバー脅威情報を STIX 形式で提供するシステムを導入している。また、様々な事業者や組織とサイバー脅威情報を交換することができるように、サイバー脅威情報を交換するための標準的なプロトコル TAXII を採用している。

(ii) 情報の匿名化、秘匿化

参加事業者から提供された情報をそのまま配信するのではなく、匿名化(インシデントやイベントの事象の名前は、通常明かさない)や秘匿化(情報提供元の機関と協議の上、必要に応じて一部情報の削除等)を実施している。

(iii) 情報の公開制限

政府機関に情報連携をする際には、情報提供者は「極秘」ラベルを付けることにより、一般への公開を制限することができる。

(3) ポイント

サイバー脅威情報を交換するための標準的な仕様（STIX/TAXII）を採用することで、情報共有の迅速化や効率化が図られている。

匿名化や秘匿化を実施することで、参加事業者が情報提供する際の障壁を排除している。

【Healthcare Ready】

(1) 概要

Healthcare Ready は、2005 年に発生したハリケーン・カトリーナの被害を踏まえ、災害前・災害中・災害後の各組織のレジリエンス強化を目的として、アメリカ赤十字社等により 2006 年に設立された非営利組織 Rx Response が、2015 年 8 月に改名したものである。元々は、災害に係る情報共有を実施していたが、近年、サイバーセキュリティに係る脅威が増加したため、サイバーセキュリティに係る情報共有も実施している。災害に係る情報とセキュリティに係る情報(サイバー、フィジカル)は、同一の手法(メール)で情報共有を実施しているが、サイバーセキュリティの情報は、STIX 化したうえでメールに添付して配信する場合もある。共有される情報量は、サイバーセキュリティが 40%、それ以外の情報が 60%を占めており、サイバーセキュリティに係る情報は 1 日に 2 件ほど共有されている。Healthcare Ready の参加組織は、災害発生時の経済的損失を最小化することや災害時に製品を必要としている患者に届けることを自組織の利益と捉え、情報提供を実施している。Healthcare Ready には、製薬事業者や業界団体、医薬品卸事業者、薬局の業界団体が参加している。

米国のヘルスケア分野に係る情報共有組織は、Healthcare Ready の他に Health Information Sharing and Analysis Center (H-ISAC)がある。この両者の差異を表 2-4 に示す。H-ISAC は医薬品や医療機器メーカや医療サービス団体を中心にヘルスケア分野におけるサイバーセキュリティの情報共有に重点を置いているが、Healthcare Ready はヘルスケアのサプライチェーンのセキュリテイに重点を置いた情報共有を実施する点が大きな違いである。H-ISAC と Healthcare Ready 間の情報共有は実施されていないため、両方に参加している組織は、どちらか一方への情報提供を判断している。Healthcare Ready は、製造者から、医療サービスを提供する末端まで、運命共同体として、お互いの一つの利益に向けた活動として、わかり易い組織の形態の一つといえる。

表 2-4 Healthcare Ready と H-ISAC の比較

#	組織名	形態	参加組織の分野	共有する情報の種類
1	Healthcare Ready	ISAC	ヘルスケアのサプライチェーンに係る企業(製薬、薬品卸、物流、薬局 等)	サイバーセキュリティ(サプライチェーンのセキュリティに重きを置く) フィジカルセキュリティ 災害に係る情報
2	H-ISAC	ISAC	医薬品や医療機器ベンダーや医療サービス団体を核としたヘルスケア分野の組織	サイバーセキュリティ フィジカルセキュリティ

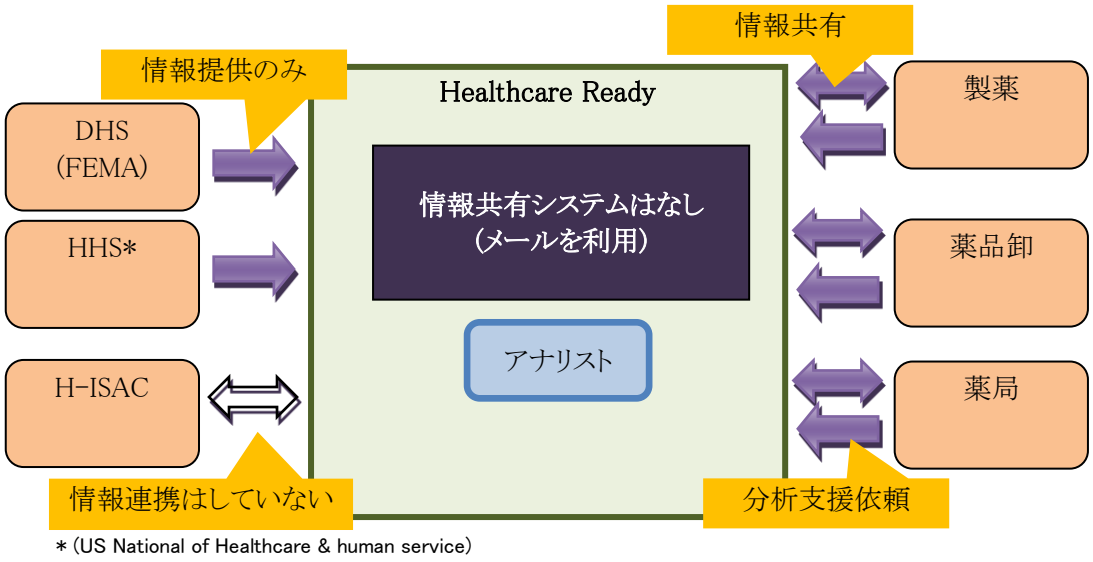


図 2-6 Healthcare Ready の情報共有の全体像

(2) Healthcare Ready を支える技術や運用

(i) アナリスト

常勤 8 人、非常勤 30 人のアナリストが所属しており、非常時や参加組織からの要請に応じて、参加組織を無料で支援する。また、DHS 等から取得した情報を分析し、参加組織に配信している。

(3) ポイント

Healthcare Ready には非常勤を含めて約 40 人のアナリストが所属しているため、サイバーセキュリティに関する十分な体制を確保できていない参加組織であっても、Healthcare Ready に支援依頼すれば分析結果を得ることができる。

Healthcare Ready では、災害対応に関する情報共有の枠組みが確立している状態で、サイバーセキュリティに関する情報の取扱いを開始したため、開始当初から円滑にサイバーセキュリティに関する情報共有を実施できている。

2.2.3. ISAO(米国)

(1) 概要

2015 年 2 月 13 日に発令された大統領令 13691 号により、情報共有、分析を実施する ISAO の創設が示された。また、大統領令を受けて、ISAO の設立を促す団体として、非政府組織である「ISAO 標準化機構」がテキサ

ス大学により設立された。ISAO 標準化機構は、標準化やガイドラインの提供の他、参加希望の団体が条件を満たす組織を ISAO として認定する組織である。

ISAO とは、ISAC と同様にサイバー脅威に関する情報を収集し、分析して、広めることを目的にした組織形態の総称である。ISAC との違いとしては、ISAC が業界毎に設置されるのに対して、ISAO は業界（IT 業界、金融業界、エネルギー業界等）に特化せずに、業種(例：医療等)ごと、地域ごと、企業規模ごと等、業界間を横断的に連携する活動を行う点が挙げられる。

(2) ISAO を支える技術や運用

(i) 情報共有の概念的フレームワーク

ISAO 標準化機構では、サイバーセキュリティ情報共有の概要や ISAO に関する情報共有を理解するための資料を提供している。表 2-5 に示すように、その資料において、ISAO および組織がとるべき行動を「目的（状況認識、意思決定、行動）」、「時間（即時、戦術的、戦略的）」という 2 つの軸で分類している。

表 2-5 情報共有の概念的フレームワーク

	状況認識	意思決定	行動
即時 （差し迫った脅威／新しい脆弱性／インシデントに対して行動を取る）	ISAOの行動： ・脅威、脆弱性、インシデントに関する情報を収集する ・情報を分析して推奨事項を作成する ・メンバーに情報を共有する メンバー組織の行動： ・情報を収集してISAOに共有する ・ISAOから情報を受信する	ISAOの行動： ・すべてのメンバーへの潜在的影響を評価する ・メンバーの問い合わせに対応する ・メンバー間で調整を行う ・実行可能な行動の提案／評価 メンバー組織の行動： ・関連性を確立する ・影響を評価する ・可能性のある行動をレビューする ・実行する行動を選択する	ISAOの行動： ・脅威への対応をサポートする ・共同対応を調整する ・行動の影響を評価する メンバー組織の行動： ・共有情報に対応する
戦術的 （既存のリソースを使用して状況認識の変化から保護する）	ISAOの行動： ・現状の状況認識と防衛手段の全体像を作成する ・情報を統合、強化、分析して推奨事項を作成する ・メンバーに情報を共有する メンバー組織の行動： ・ISAOから情報を受信する ・他のメンバーと情報をやり取りする ・防衛手段を共有する	ISAOの行動： ・すべてのメンバーまたは特定のメンバーへの潜在的影響を評価する ・メンバーの問い合わせに対応する ・メンバー間で調整を行う ・実行可能な行動の提案／評価 メンバー組織の行動： ・関連性を確立する ・脅威の現在の状況および状況認識の変化に対して、既存の防御手段の影響を評価する ・可能性のある行動をレビューする ・実行する行動を選択する	ISAOの行動： ・実施をサポートする ・共同行動を調整する ・行動の影響を評価する メンバー組織の行動： ・決定された行動方針を実施する ・レビューして調整する
戦略的 （将来の脅威環境に基づいてリソースを変更する）	ISAOの行動： ・情報を傾向分析する ・綿密な分析を公開する ・メンバーに情報を共有する メンバー組織の行動： ・ISAOから情報を受信する ・他のメンバーと情報をやり取りする ・戦略と計画を共有する	ISAOの行動： ・メンバーの問い合わせに対応する ・メンバー間で調整を行う ・実行可能な行動の提案／評価 メンバー組織の行動： ・将来の脅威環境に対して既存のリソースを評価する ・パートナーを評価する ・戦略／計画を設定する	ISAOの行動： ・実施をサポートする ・共同戦略を調整する ・行動の影響を評価する メンバー組織の行動： ・選択された戦略を実施する ・決定事項と行動をレビューして調整する

また、ISAO とメンバ間の情報共有はマシン対マシンで実施される可能性が示唆されており、その場合には、情報の構造化や標準化されたデータフォーマットとプロトコルの必要性が述べられている。データフォーマットの例として、STIX が挙げられている。

(3) ポイント

共有すべき情報は、情報収集や実行可能な行動を特定するといった「目的」や、すぐに対応するのか将来に向けて対応するのかといった「時間と適用」によって異なることが示されている。

また、メンバー間の情報共有には情報共有システムを活用し、情報の構造化や形式の標準化が必要であることが示されている。

2.2.4. ISAC と ISAO を仲介する組織「Global Resilience Federation」

(1) 概要

Global Resilience Federation (GRF)は、脅威情報を共有するコミュニティ(ISAC、ISAO、CERT)の発展と分野を跨いだ世界中のコミュニティ間の情報共有をコーディネートすることを目的として、2017 年 5 月に設立された民間の非営利組織である。FS-ISAC が情報共有を推進するなかで、分野を跨いだ情報共有の必要性を認識していたことから、FS-ISAC 内に 2014 年に設置された部門が独立して GRF を設立した。そのため、GRF は FS-ISAC と密接に連携している。GRF の使命は、重要インフラ事業者と個々の組織がサービスを提供する能力に重大な影響を及ぼす恐れがある行為に対して、回復力と事業継続性を保証することである。GRF には、米国の ISAC や ISAO が参加可能であり、米国以外の組織は参加にあたり、事前審査が必要となっている。現在、8 つのコミュニティ(Financial Services Information Sharing and Analysis Center、Oil and Natural Gas Information Sharing and Analysis Center、Energy Analytic Security Exchange、Health Information Sharing and Analysis Center、Legal Services Information Sharing and Analysis Organization、National Retail Federation Retail Information Sharing and Analysis Organization、Multi-State Information Sharing and Analysis Center、Retail Cyber Intelligence Sharing Center)が参加しており、各コミュニティ内の 38 カ国 7,000 組織が情報共有している。GRF から参加コミュニティに対して、1 年間で約 4,500 件の情報が共有されている。各参加コミュニティは、自組織が入手した全ての情報を GRF に提供しているわけではなく、共有する必要があると考える情報のみ GRF に提供している。また、GRF に参加していないコミュニティからの要望に基づき、情報共有に係る相談に応じており、当該相談内容に係る打ち合わせを非定期で開催している。

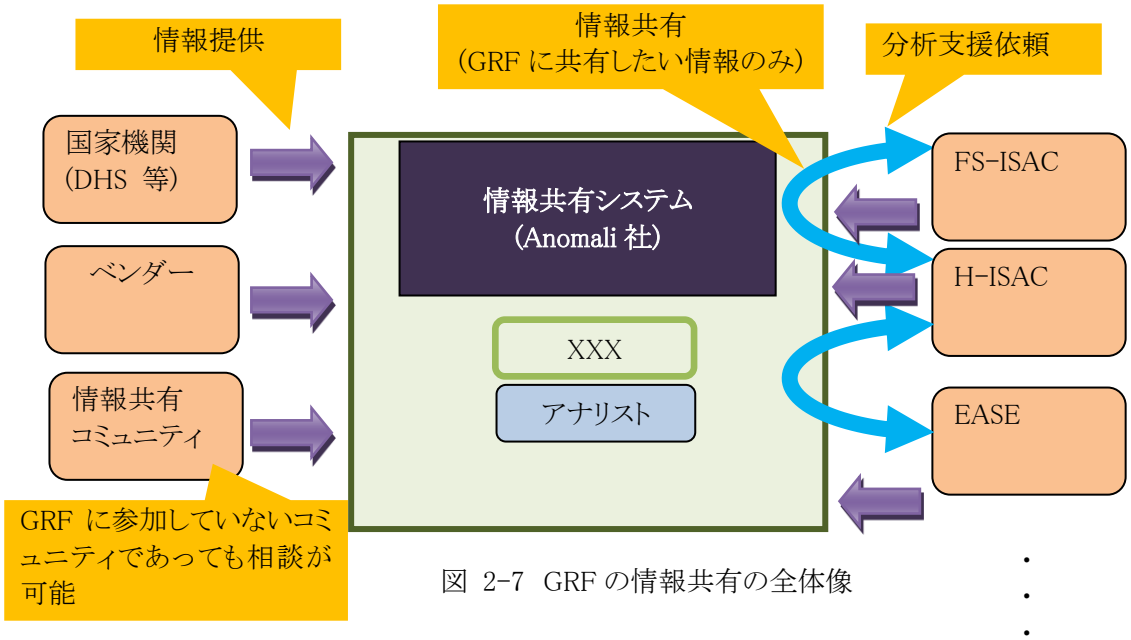


図 2-7 GRF の情報共有の全体像

(2) GRF を支える技術や運用

(i) 分野を跨いだ情報共有を促進する様々な専門家

GRF では、情報共有を促進するためにサイバーセキュリティ、フィジカルセキュリティ、地政学、OT やサプライチェーンなど様々な専門家が所属している。これにより、GRF はインシデント対応等の支援を実施可能な体制を整備することができ、参加コミュニティを惹きつけている。

また、参加コミュニティを惹きつける方策の一環として、参加コミュニティに係る業界知識が豊富な専門家も所属している。参加コミュニティは様々な専門家に支援を依頼することが可能であり、GRF への参加は自前で専門家を雇うことと比較して投資が少なくて済む。

表 2-6 GRF の職種

#	職種の名称	#	職種の名称
1	取締役	20	運用
2	幹部	21	調達
3	渉外	22	イベント管理・出張手配
4	業界のオピニオンリーダー／ 対象領域、トピック等の専門家	23	一般管理(人事・財務 等)
5	プログラムマネジメント	24	教育、演習
6	専門家(フィジカルセキュリティ)	25	アウトリーチ活動
7	専門家(サイバーセキュリティ)	26	テクニカルサポート
8	専門家(Operational Technology)	27	会員のエンゲージメント向上
9	専門家(自然災害)	28	会員サービス提供
10	分野を跨る情報共有支援	29	サプライチェーン
11	専門家(地政学)	30	特命担当
12	専門家(データ分析)	31	運用手順策定
13	専門家(各業界)※	32	コンプライアンス
14	リスク管理※	33	営業
15	業務要件、技術要件	34	秘書
16	技術	35	言語学者
17	マーケティング	36	ベンダー関係管理(VRM)
18	プライバシー・情報セキュリティ	37	設備管理
19	法律		

※別の職種にて当該役割を兼ねる可能性がある。

(ii) FS-ISAC との連携

GRF は FS-ISAC から独立する形で設立されたという経緯があるため、オフィスや情報を共有するなど、両組織は密接に連携している。

分析体制の構築においては、GRF に所属するアナリストは 20 人程度だが、FS-ISAC に所属している約 120 人のアナリストと連携することにより、GRF 参加コミュニティからの支援要請に応じた様々な事象に対応できる人的リソースを確保することが可能である。

(iii) 参加コミュニティが意図する範囲に限定した情報共有

GRF は参加コミュニティ間の情報共有を仲介する組織であり、情報共有の範囲は情報配信元が付与した TLP に基づいて決められている。情報配信元の意図に反して他のコミュニティに情報共有されることはないため、情報配信元は安心して情報を提供することができる。

(iv) 各コミュニティに合わせた情報共有手段の採用

GRF の参加コミュニティが情報共有する手段は、GRF が用いている情報共有システムに限定されておらず、GRF の情報共有システムを採用していない参加コミュニティも存在している。GRF は、情報共有システムを通じた情報共有だけでなく、メールによる情報共有など、各参加コミュニティの状況に合わせた複数の情報共有に対応できる柔軟性を持ち合わせている。

(v) STIX 形式を用いた情報配信

GRF は各参加コミュニティに合わせた情報共有手段を採用しているが、配信する情報のフォーマットは STIX 形式で統一されている。例えば、情報共有手段として電子メールを用いている参加コミュニティに情報配信する場合は、STIX 化した情報を電子メールに添付している。

(3) ポイント

GRF は、特定の分野に依存しない独立した民間の組織として、FS-ISAC と連携しつつ、様々な専門家が所属する充実した体制を整備している。これにより、分野を跨る情報共有の仲介、参加コミュニティからの要請に基づく分析および ISAC、ISAO 等の立ち上げ支援等を実施することができている。

GRF では、情報提供者が提供する情報の共有範囲を TLP で設定できるようにしている。

サイバー脅威情報のフォーマットとして STIX 形式を採用することにより、共有情報のフォーマットを標準化している。

2.3. 海外事例から得られた示唆

英国および米国の情報共有の取組み事例を踏まえ、日本における情報共有の取組みを検討するうえで参考にすべきと考えられる内容を、表 2-7 に示す。

表 2-7 海外事例から得られた示唆

#	海外事例から得られた示唆	概要	該当する海外事例
1	サイバー脅威情報のフォーマットを標準化することが必要	STIX/TAXII を既に導入している事例が多く見受けられた。また、現在は未導入であっても将来的な対応を検討していることを踏まえると、大半の事例で STIX/TAXII 対応が進んでいる。	DHS（AIS） E-ISAC GRF
2	情報提供に関する不安、障壁等を除去する工夫が必要	TLP で提供者が自ら共有範囲を設定できるようにしている	CiSP GRF
		情報提供者を匿名化できる	CiSP Auto-ISAC E-ISAC
		情報共有の取組み参加者同士の信頼関係を構築できるようにしている	CiSP Auto-ISAC
3	同じ分野だけではなく、分野を跨った情報共有の促進が必要	同一分野内の情報共有に加え、分野横断の情報共有を実施する仕組みが運営されている	CiSP GRF
4	事業者における情報共有を支援する役割が必要	事業者に配信する情報を STIX 化する	GRF
		情報共有の運用ルールが適切に遵守されているか、共有されている情報をチェックする	CiSP
		事業者のために分析し、分析結果を提供する	CiSP Healthcare Ready GRF

3. 日本における情報共有のイメージ(仮説)

3.1. 重要インフラ事業者から挙げられた情報共有に関する課題、要望

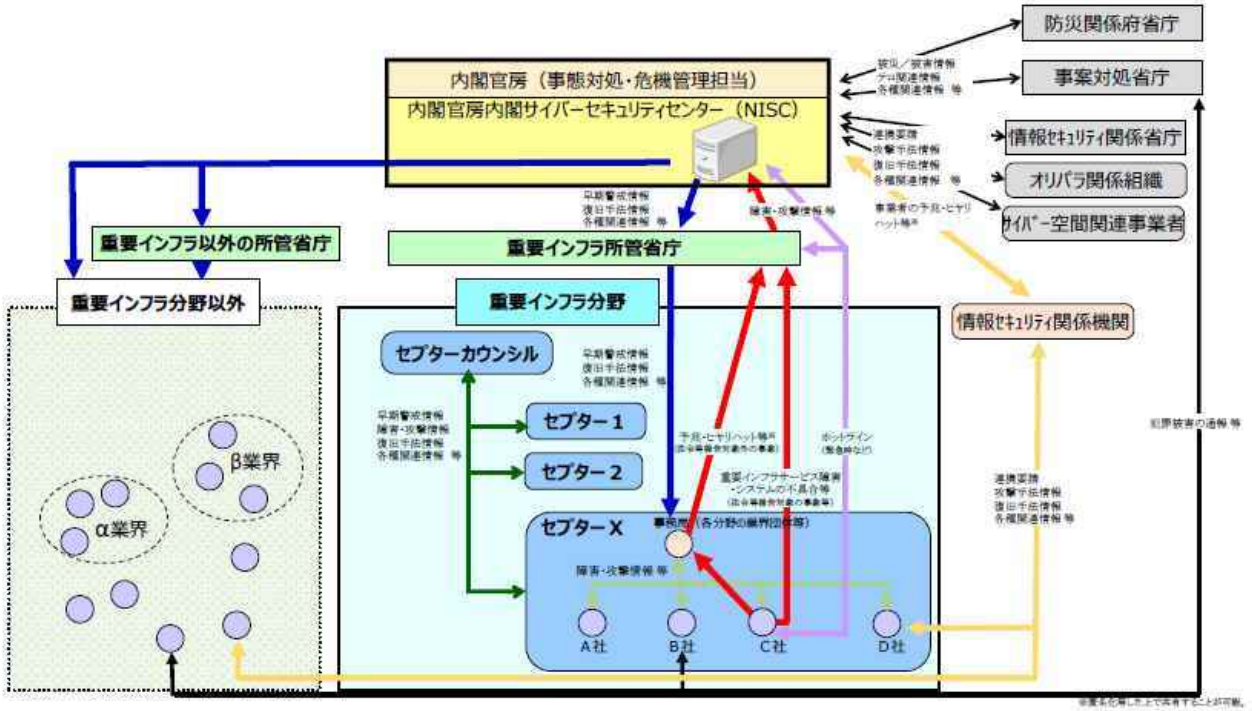
本事業では、重要インフラにおけるサイバーセキュリティの脅威情報を共有する仕組み・体制づくりを促進するための研究開発の一環で、事業開始当初に重要インフラ事業者に情報共有に関する課題や要望等について、ヒアリングを実施した。ヒアリングで把握できた主な課題、要望を、以下に示す。

【重要インフラ事業者から挙げられた情報共有についての課題、要望等】
- 迅速に情報が共有されていない
- 情報共有するための人的リソースが不足している
- 大量のサイバーセキュリティ関連情報を複数の機関から受信しており、「何が本当に自組織に必要な情報なのか」を判断する作業に手間がかかっている
- 警戒情報の続報が複数回にわたって提供された場合、何が更新されたのかすぐに判断できるようにし、過去の情報(第 1 報、第 2 報等)と紐付けてほしい

3.2. 重要インフラ事業者における情報共有のイメージ(仮説)

NISC が「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」として取りまとめた今後取り組む具体的な施策の 1 つとして「情報共有体制の強化」が挙げられており、2020 年の東京オリンピック・パラリンピックを見据えた情報共有体制を示している。

図 3-1 に、「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」における情報共有体制を示す。



※出典:平成 30 年 7 月 25 日サイバーセキュリティ戦略本部改定「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」
別紙 4-1 情報共有体制

図 3-1 情報共有体制

なお、情報共有体制の強化に向けた具体的な施策としては、以下のようなものが挙げられている。
- 連絡形態の多様化(情報連絡元の匿名化等を可能とするセプター事務局経由の省庁報告ルートの新設)による情報共有の障壁の排除
- 緊急時における内閣官房と重要インフラ事業者間のホットライン構築も可能な情報共有システム整備

・ 国内外のインシデントに関する情報収集・分析を行う「情報セキュリティ関係機関[1]」との密な連携　等

本書では、上述の情報共有体制を前提として、本事業の研究成果を加味した重要インフラ事業者における情報共有のイメージ（仮説）を検討した。

具体的には、3.1 に示した課題を解決するために、2 章で述べた海外事例から得られた示唆を踏まえて、表 3-1 のとおり、整理した。

なお、情報共有システムの機能については、表 3-1 に記載しているものを含め、4 章で後述する。

表 3-1 情報共有における課題と解決策

#	課題	解決策	補足
1	情報が迅速に共有されていない	STIX/TAXII 等の標準的なフォーマット・プロトコルに対応した情報配信	自動的に機械処理することができるため、迅速な情報共有が可能となる
2	情報共有するための人的リソースが不足している	モデレータやアナリストが所属する支援組織（横断的情報共有組織）の設置	#1 の「標準的なフォーマット」への変換は、横断的情報共有組織にて実施
3	大量のサイバーセキュリティ関連情報を複数の機関から受信しており、「何が本当に自組織に必要な情報なのか」を判断する作業に手間がかかっている	支援組織（横断的情報共有組織）または ISAC による判断 ※人手による作業ではなく、情報共有システムの機能（アグリゲーション）を用いる想定	情報提供組織が配信する情報を直接事業者が受信するケースがあるため、本解決策は事業者が受信する全ての情報を対象とするものではない
4	警戒情報の続報が複数回にわたって提供された場合、何が更新されたのかすぐに判断できるようにし、過去の情報（第 1 報、第 2 報等）と紐付けてほしい		

本節では、事業者による情報共有を支援する組織として、図 3-2 のとおり、「横断的情報共有組織」の存在を仮定したうえで、重要インフラ事業者に対する情報共有のイメージ（仮説）を整理する。

[1] 警察庁サイバーフォースセンター、国立研究開発法人情報通信機構（NICT）、国立研究開発法人産業技術総合研究所（AIST）、独立行政法人情報処理推進機構（IPA）、一般社団法人 ICT-ISAC、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）、一般財団法人日本サイバー犯罪対策センター（JC3）。

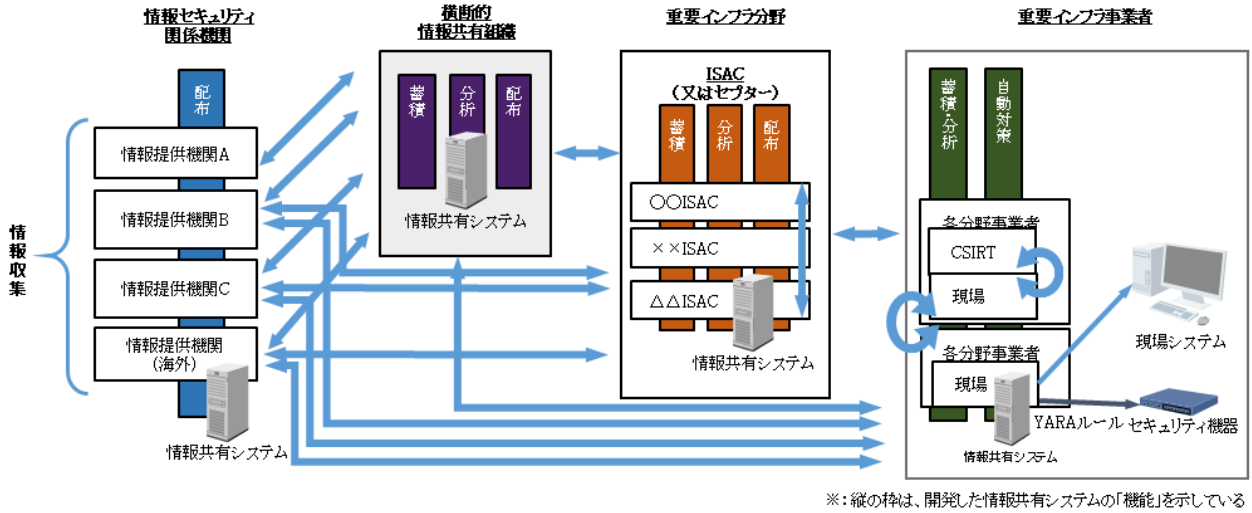


図 3-2 重要インフラ事業者に対する情報共有のイメージ（仮説）

図 3-2 における重要インフラ事業者に対する情報共有は、情報提供組織から配信されるサイバーセキュリティ関係情報のうち、横断的情報共有組織が受信した情報について、同一の情報の纏め（情報の仕分け）、続報情報の場合の更新内容の明確化、過去情報との関連付け等の前捌きを実施する。

情報提供組織から配信される情報が標準フォーマットではない場合、横断的情報共有組織にて標準フォーマットに変換したうえで、ISAC や重要インフラ事業者に配信する。

また、事業者が受信したサイバーセキュリティ関連情報について、実施すべき必要な対策等を自力で判断することができない場合等には、ISAC または横断的情報共有組織に支援依頼すると、分析結果を重要インフラ事業者に提供する。

このような流れで情報共有することができれば、各重要インフラ事業者が情報を受信した際の手間を軽減し、迅速に必要な対策等を講じることが可能になると考えられる。

上述の通り、横断的情報共有組織が存在することによるメリットはあるが、横断的情報共有組織を介することに伴って、情報共有するスピードが遅くなる等のデメリットが生じると想定される。その点については、技術等による改善が可能と考えており、技術的な改善の一例を、「4.1 情報共有システムの機能」にて後述する。

以下、情報提供組織、横断的情報共有組織、ISAC（またはセプター）、重要インフラ事業者それぞれの概要について、説明する。

(1) 情報提供組織

特定の分野に属さず、サイバー攻撃情報や対策方法に関する情報を収集し、ISAC（またはセプター）や重要インフラ事業者に送信する組織である。重要インフラ事業者は、当該組織が送信する情報を直接受信する場合もあれば、ISAC（またはセプター）を介して受信する場合もあると考えられる。

(2) 横断的情報共有組織

特定の分野に属さない、複数分野の事業者・組織間の情報共有を支援する組織である。情報提供組織が配信する情報やある ISAC（またはセプター）が把握した情報を、各分野の ISAC（またはセプター）や事業者に配信する役割を担う。

横断的情報共有組織から各重要インフラ事業者に対する情報配信は、各 ISAC（またはセプター）を経由して行われる場合と、ISAC（またはセプター）を経由せずに直接行われる場合がある。ISAC（またはセプター）での体制が十分ではない分野に関しては、横断的情報共有組織が ISAC（またはセプター）の役割も兼ねて、分野に特化した情報共有を実施する場合もある。

なお、横断的情報共有組織の役割を担う可能性がある組織としては、ICT-ISAC やセプターカウンシル、オリパラ CSIRT 等が考えられる。例えば、ICT-ISAC が横断的情報共有組織の役割を担う場合、IT ベンダーが所属している組織の特性を活かし、モデレータの機能を併せ持って情報の振り分けや配信等を担うことが想定される。

(3) ISAC(またはセプター)

各分野に設置され、サイバー攻撃や対策方法に関する情報の収集・分析や、それらの情報の分野内の事業者への展開を行う組織である。

重要インフラ事業者とは独立した ISAC(またはセプター)を各分野に設置し、ISAC(またはセプター)が情報を収集・分野内事業者に展開することにより、情報の知見化・集積化・体系化および利用等を図ることができると考えられる。

(4) 重要インフラ事業者

「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」では、わが国の重要インフラ事業者は情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、石油、クレジットの 14 分野と定義されている。本書においても、重要インフラ事業者(以下「事業者」)は上記 14 分野に含まれるものを想定する。各事業者は情報システムや制御システムを運用しているため、それらのシステムをサイバー攻撃から防御する必要がある。

3.3. 各組織が配置すべき人員の役割

3.2 節で述べた 4 つの組織において、情報共有を実施するうえで必要な役割を以下に示す。

(1) 情報提供組織

情報提供組織(国内)、情報提供組織(国外)の各組織が、それぞれ必要な役割を設けている。

(2) 横断的情報共有組織

横断的情報共有組織には、以下の役割を担う人員を配置する必要があると考える。

- モデレータ

当該組織が担っている役割、責任の範囲を把握するために以下の職務を遂行する。

+ 入手した情報の事業者, ISAC(またはセプター)への送信
+ 上記情報の送信前における送信すべき情報の取捨選択
+ 情報の定型フォーマットへの変換
+ 情報の一部秘匿化、情報の提供者に関する部分の匿名化等
+ 情報の発信が活発且つ適切に行われるようにするための助言
+ 情報交換の場に加えることが望ましいと考えられる有識者の提案
+ 情報交換の結果として得られる結論がより有効性の高いものとなるようにするための、他の情報交換の場の提案
+ 不適切と考えられる情報の削除
+ 他の事業者、他の組織等から送信された情報の受信

- アナリスト

サイバー攻撃情報の分析を行う。アナリストは、分析を行うサービスを提供する外部組織に所属する場合も考えられる。

なお、複数の ISAC(またはセプター)同士が、本組織を経由せずに直接情報を共有する場合も想定する。また、ISAC(またはセプター)または ISAC(またはセプター)と同等の役割を担う組織が設置されていない場合は、本組織が ISAC(またはセプター)と同様の役割を担うことも想定する。

(3) ISAC（またはセプター）

ISAC（またはセプター)内において、以下の役割を担う人員を配置する必要があると考える。

● モデレータ

横断的情報共有組織のモデレータと同様の役割を担い、また職務を遂行する。

● アナリスト

横断的情報共有組織のアナリストと同様の職務を遂行する。

尚、分野内の複数の事業者が、ISAC（またはセプター)を経由せずに直接情報を共有する場合も想定する。

(4) 重要インフラ事業者

各事業者内においてサイバー攻撃に関する情報収集・分析や対策の実施に関与する部門を以下に示す。

● 経営層

下位層(CSIRT，現場部門)からセキュリティ上の問題に関する報告を受け、事業継続計画（Business Continuity Plan:BCP)の観点から各システムの稼働継続や停止を決定し、下位層に指示する。また、平時には、情報セキュリティの各取組に必要な予算・体制・人材等の経営資源を継続的に確保し、適切に配分することにより、情報セキュリティ対策に取り組む姿勢が求められる。

● Computer Security Incident Response Team（CSIRT[1])

サイバー攻撃に関する情報の収集（左記の意味での監視）、分析、知見化、攻撃への対策方法の確定、収集した情報や確定した対策の関係部門や他事業者への展開などを行う。より詳細には、インシデント関連情報、脆弱性情報、攻撃予兆情報等の恒常的な収集・分析や、対策方法の確定等が、具体的に担う作業である。左記に加えて、本情報共有においては、現場部門から収集した情報の分析、判断、組織外への展開や、他の組織が発信した情報を現場部門への伝達も行う。事業者によっては CSIRT が複数存在することもあるが、その場合は取り纏めの CSIRT が存在することを前提とする。また、中小企業など CSIRT を設置しない企業もあることが想定される。CSIRT を設置しない企業は、現場部門が CSIRT の役割を担うことが想定される。CSIRT には、以下に挙げる 2 つの役割を担う者が存在する。

- モデレータ

  横断的情報共有組織のモデレータが実施する職務を外部組織だけでなく現場部門に対しても実施する。

- アナリスト

  サイバー攻撃情報の分析を行う。アナリストは、分析を行うサービスを提供する事業者外の組織である場合もある。

CSIRT における情報の送受信は、モデレータが担う。アナリストが他の事業者や他の組織のアナリストと直接情報を交換する場合、このアナリストはモデレータの役割も備える。

● 現場部門

システムの管理、運用、監視を実施する部門である。例を以下に示す。

- システム（情報システム、制御システム）運用者
- 業務運用管理者

業務運用管理者は、業務の運用状況を管理する者である。例えば鉄道分野の場合、鉄道の運行状況などを監視し、何か障害等の発生が検知された場合、対応方針を決定する役割を持つ者である。

3.4. 情報共有する組織の組合せパターン

図 3-2 の情報共有体制が実現した場合、4 つの組織における情報共有は、表 3-2 の組合せパターンが想定される。

[1] 日本政府は各事業者に対して CSIRT の設立を推奨している。実際、CSIRT を設立する事業者の数は増加している[12]。

表 3-2 情報共有する組織の組合せパターン

#	分類	パターン
1	社内	重要インフラ事業者における社内の情報共有
2	社外	重要インフラ事業者と重要インフラ事業者の情報共有
3		ISAC（またはセプター）を介した重要インフラ事業者の情報共有
4		ISAC（またはセプター）間の情報共有
5		横断的情報共有組織とISAC（またはセプター）の情報共有
6		横断的情報共有組織と重要インフラ事業者の情報共有
7		情報提供組織と横断的情報共有組織の情報共有
8		情報提供組織とISAC（またはセプター）の情報共有
9		情報提供組織と重要インフラ事業者の情報共有

上記 9 つのパターンは、情報共有する相手により「社内」と「社外」に分類することができる。社外の組織と情報共有する際には、社内における情報共有とは異なり「情報の秘匿化」や「共有範囲の限定」等の仕組みが必要になると考えられる。情報共有システムに必要となる仕組みについては、4.1 節で述べる。

3.5. 共有すべき情報

本節では、サイバー攻撃に関連する情報の中で、共有されることが特に望ましい情報を列挙する。共有することが望ましい情報の例として、文献[13]4.2 節から 4.12 節に記載されているものを挙げる。これらの情報が共有されることにより、1.5 節で述べた効果を得ることが期待できる。

なお、1.5 節では、「効果が発現するタイミング」と「情報共有のシーン（【平時】、【インシデント発生時】、【平時、インシデント発生時共通】）」の 2 軸で効果を整理しているが、ある情報が共有された場合の効果は、当該情報を受領した組織が置かれている状況によって異なる。

- 検知指標

  検知に有効なサイバー攻撃を特徴付ける情報である。サイバーセキュリティにおいて関心のある成果物および／または行動を示すための文脈情報と併せて特定のパターンを伝達し、関心のある活動を検出するために使用される。

  一般的に共有されるフィールドとして、「タイトル」、「説明」、「パターン」、「検知指標の信頼度」、「示されたTTP（Tactics, Techniques and Procedures）」、「有効な時間的位置（検知指標が有効である時間枠）」が挙げられる。

- 脆弱性情報

  特定のシステムやインフラの脆弱性、特定のアプリケーションの脆弱性、または一般的な種類の脆弱性に関する詳細を含む情報である。

  一般的に共有されるフィールドとして、「タイトル」、「説明」、「脆弱性 ID（共通脆弱性識別子（CVE）の脅威識別子またはその他の既知の識別子への参照）」、「スコア（対象の脆弱性に対する共通脆弱性評価システム（CVSS）の格付けスコアまたは同様のスコア）」、「影響を受けるソフトウェア」が挙げられる。

- 行動方針

  脅威を緩和したり、インシデントに対処したりするための具体的な手段に関する情報であり、特定の IP アドレスのブロックなどの比較的ターゲットを絞ったものである場合や、アプリケーションのホワイトリストの使用などの企業の手法を含む場合がある。

一般的に共有されるフィールドとして、「タイトル」、「説明」、「タイプ（訓練、監視、パッチ適用、ブロック等）」、「目標」、「影響」、「コスト」、「有効性」、「行動方針（ファイアウォールや侵入検知システムのルール、具体的な設定変更等）」が挙げられる。

- インシデント

サイバーセキュリティインシデントに関連する特定の情報、またはサイバーセキュリティインシデントの調査時や対応時に検出された特定の情報である。

一般的に共有されるフィールドとして、「タイトル」、「説明」、「カテゴリ（不適切な使用、スキャンまたは調査、サービス妨害等）」、「報告者」、「被害者」、「影響を受けた資産」、「影響の評価」、「関連指標（I`P アドレス、ファイルのハッシュ、ドメイン等）」、「使用された TTP（攻撃技術、マルウェア、ツール等）」、「原因となる脅威アクター」、「意図された効果（盗難、機能中断、アカウントの乗っ取り、詐欺等）」、「関連するインシデント」、「行動方針」が挙げられる。

- 脅威アクター

サイバー脅威を示す可能性のある、または以前から観測されていた、または既知のインシデントに関連している悪意のあるアクターが含まれる情報である。

一般的に共有されるフィールドとして、「名前（脅威アクターに使用される短い名前またはエイリアス）」、「説明（脅威アクターの文字による説明）」、「身元（アクターを識別する情報）」、「タイプ（ハッカー、ハクティビスト、政府アクター、電子犯罪アクター、内部脅威等）」、「動機（政治的、経済的または財政的、イデオロギー的、軍事的等）」、「熟練度（未経験者、常習者、専門家、革新者等）」、「意図された効果（軍事的、経済的、政治的な優位性、盗難、破壊、混乱等）」、「観測された TTP（アクターによる使用が観測されている TTP）」、「関連するキャンペーン（アクターに起因するキャンペーン）」が挙げられる。

- TTP（戦術、技術、および手順）

脅威アクターまたはキャンペーンの行動または能力の記述に使用される非常に広範な情報を表す。攻撃者が何をどのように行うかを明らかにするため、TTP には特定の攻撃者の行動、使用されたリソース、標的となる被害者の情報、および標的となる脆弱性または弱点が含まれる。

一般的に共有されるフィールドとして、「タイトル」、「説明」、「意図される効果」、「行動（特定の攻撃パターン、マルウェア、またはエクスプロイト）」、「リソース（ツール、インフラ、または登場人物）」、「対象の被害者（標的となっている人々）」、「キルチェーン フェーズ」、「関連する TTP」が挙げられる。

- キャンペーン

キャンペーンとは、長期間にわたって成功と失敗を繰り返しながら、標的とするネットワーク内に攻撃者が侵入、潜伏を試みる一連の活動を指す。キャンペーン情報によって、攻撃者またはグループが意図する効果についての情報を、攻撃者またはグループが使用するツール、関与していると考えられる脅威アクター、グループに関連付けられているインシデント、およびその他の関連するキャンペーンに関連付けることができる。

一般的に共有されるフィールドとして、「名前（キャンペーンに使用される短い名前またはエイリアス）」、「説明」、「意図された効果（軍事的、経済的、政治的な優位性、盗難、破壊、混乱等）」、「関連する TTP」、「関連するインシデント」、「関連付けられたキャンペーン」、「帰属（関連する脅威アクター）」が挙げられる。

- 分析レポート

具体例として「企業の中核機能に対する脅威の影響」、「攻撃ライフサイクルに関連する脅威活動の説明」、「組織のインフラに関連した悪意のある活動の傾向」、「緩和の有効性」、「サイバー脅威の傾向レポート」、「脅威分類レポート」、「事前対応（評価）レポートと事後対応（インシデントの事後分析）レポート」が挙げられ

る。

- 脅威インテリジェンスのレポート
  傾向の概要を示すレポートから特定のキャンペーンの詳細な分析まで幅広いカテゴリを持つサイバー脅威情報である。レポートには、キャンペーン、脅威アクター、TTP、および検知指標の情報が含まれることがある。

- セキュリティの勧告とアラート
  セキュリティ上の問題、問題による影響の説明、問題に対処するために推奨される緩和策等の情報である。国際的な CERT や政府、セキュリティベンダー等、様々な情報源によって公開されている。

- 運用上の手法
  ベストプラクティスまたは効果的な手法、効果的なアーキテクチャ、効果的または効果的でないシステム設定、人員配置戦略などが含まれる可能性がある情報である。このような情報を共有することにより、共有するメンバー同士で協力して信用を築き上げ、互いに学びあい、各組織が独自のサイバーセキュリティ手法を進展させることができるため、重要である。

4. 日本における情報共有のイメージ(仮説)に必要な仕組み

3 章で示した情報共有のイメージ(仮説)を実現するためには、情報共有システムと取り巻く環境の整備が必要となる。

4.1. 情報共有システムの機能

本節では、3.2 節で述べた情報共有のイメージ(仮説)を実現するうえで、2 章の海外事例や横断的情報共有組織、ISAC 等の役割を踏まえて必要と考えられる情報共有システムの機能を検討する。

機能が必要となる具体的なシーンを想定し、各役割に必要な機能を案出した。案出した機能を図 4-1 に示す。想定した具体的なシーンのイメージは、本書巻末の【参考】に記載した。

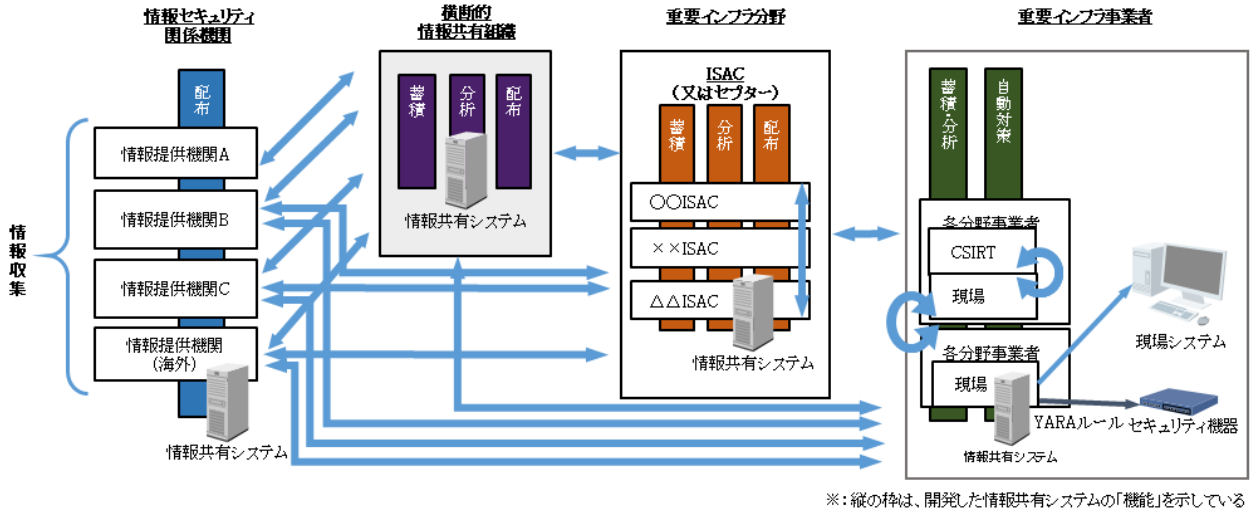


図 4-1 情報共有のイメージ(仮説)に必要となる機能(再掲)

【定型化】

- 標準化された表現形式で記述された情報の登録・蓄積と表示および左記情報の標準化されたプロトコルに従った送信と受信

事業者、ISAC(またはセプター)、横断的情報共有組織に導入されている情報共有システムは、異なる可能性がある。また、図 4-1 を実現した場合、横断的情報共有組織や ISAC(またはセプター)を介した情報共有の流れは、人手で対応すると情報共有のスピードが遅くなることが懸念される。

そこで、横断的情報共有組織および ISAC(またはセプター)を経ても迅速な情報共有を可能とするために、情報共有の機械化が必要であり、効率的な機械処理のためにはデータ形式の定型化が有効と考えられる。

したがって、情報共有システムには、標準化された表現形式で記述された情報を蓄積したり表示したりする機能、および左記情報を標準化されたプロトコルに沿って送受信する機能を備えていることが望まれる。STIX および TAXII は、それぞれ標準的な表現形式、プロトコルの代表的な例である。

【配布】

- 任意情報の入力と表示

情報共有システムは、標準化された表現形式で記述された情報とは別に、任意の表現形式で記述された情報も登録・蓄積したり、表示したりする機能も備えていることが望ましい。

- 情報閲覧可能者の制限

個々の情報の閲覧に関しては、ある特定のグループに所属する者だけが行えるようにする必要がある。そこで、情報共有システムには、新しい情報を登録する際に、それを閲覧できる者を制限できる機能が備えられている必要がある。

- 情報登録可能者の制限

情報共有システムに情報を登録できる人を制限しない場合、精度の低い情報が登録されたり、同一の事象に

関する情報が複数登録されたりする場合が増大する可能性がある。このような場合、閲覧者が必要な情報を把握することが困難になることが懸念される。このため、本システムには、情報を登録できる者を制限できる機能が備えられている必要がある。

● 情報登録可能者の複数グループへの所属

ある一事業者の現場部門と CSIRT の間で共有された情報を、他の事業者にも提供することを望まれる場合も想定される。このため、情報共有システムは、事業者の CSIRT, ISAC, 横断的情報共有組織のモデレータが複数のグループに所属できる機能、および、左記の者の一人が、自身が所属するあるグループ（G とする）で得たり発信したりした情報を、自身が所属する G とは別のグループにも発信できる機能を備えている必要がある。

● 情報の一部の匿名化や秘匿化

攻撃対象のシステムの IP アドレスや、情報提供者の情報については、外部へ発信することを望まない事業者、組織、情報提供者が存在するであろうと考えられる。そこで、情報共有システムは、情報を外部へ発信する場合、発信することを希望しない部分については、秘匿したり匿名化したりする機能を備えていることが望ましい。

● 誤操作防止

情報共有システムを用いて共有される情報には、有害なサイトの URL や IP アドレス, マルウェアを含むファイル等が含まれることが想定される。例えば有害なサイトの URL が展開された情報に含まれていた場合、情報の閲覧者が当該 URL をクリックしてしまう可能性がある。このため、情報共有システムは、そのような誤操作を防止する機能を備えていることが望ましい。

【アグリゲーション】

● 複数の情報の統合表示

情報共有システムは、関連する情報を統合して表示する機能を備えていることが望まれる。関連する情報の例としては、既に登録されたある情報に対して、それを補足する目的で入力された情報や、当初独立したものとして入力されたが、後に登録済みの別の独立した情報に関連していることが判明したような情報等が挙げられる。尚、統合表示する際、閲覧が許可されている人員や利用目的などの補足的な情報も合わせて表示する機能や、同一の情報が複数含まれていた場合には重複するものを排除して表示する機能も備えていることが望ましい。

また、事業者の CSIRT は、知見化されたサイバー攻撃や対策に関する情報を、必要に応じて経営層へ報告することが想定される。このため、情報共有システムは、共有された情報のうちの幾つかを適切に統合して表示する機能を備えていることが望ましい。

● 各情報への履歴情報の付与、および履歴情報に基づく表示

情報共有システムにおいて交換される情報は、膨大な量になる可能性がある。交換される情報の中には、過去に登録された対策手段に関する情報の更新版も含まれる可能性がある。当初ある対策を実行することで十分であったものが、後に不十分となった一方で、更に実施することが必要なことが判明した新たな対策は、そのような更新情報の一例である。情報共有システムは、情報の受信者がこのような最新の更新情報を漏れなく把握できるようにするための機能を備えていることが望まれる。左記は、新たな情報を登録する際に、各情報に履歴情報を付与し、付与された履歴情報に基づいて登録された情報を表示できれば、達成できると考えられる。従って、情報共有システムは、左記機能を備えていることが望ましい。

【検索・表示】

● 登録情報の検索

前々項および前項に記載したように、情報共有システムを用いて共有される情報は、膨大な量になることも想定される。このため、情報共有システムは、目的の情報を素早く検索し、結果を表示する機能を備えていることが望ましい。

【対策支援】

● ICT システムへの対策手段の自動送信

受信した情報が精度の高い対策手段を含んでいた場合、対策を実施する必要がある ICT システムの担当者に対しては、当該情報を自動的に送信する機能を情報共有システムは備えていることが望ましい。

【状況把握】

● 作業状況管理

CSIRT は、現場部門に指示を出すだけでなく、指示を出した現場部門が対策を実施していない場合には、フォローを実施する必要がある。このため、情報共有システムは CSIRT の指示と現場の対策実施状況を紐付けて管理し、表示できる機能を備えていることが望ましい。 表示する上で、CSIRT は膨大な量の情報を対処する必要があるため、自組織にとって必要な情報を絞り込み可能にすることが望ましい。

4.2. 情報共有を促す施策

情報共有システムを整備しただけでは、情報共有は実施されない。各組織や事業者が情報共有システムを活用し、情報を提供する必要がある。各組織や事業者の情報提供を促すためには、リスクの低減やインセンティブの付与といった施策が必要となる。

4.2.1. 情報共有において想定されるリスク

3 章で述べた情報共有のイメージ（仮説）が実現した場合、組織を跨る情報共有が頻繁に行われるようになるため、情報を発信する事業者・組織（発信者）や情報を受信する事業者・組織(受信者)それぞれの立場において、これまでには発生していなかった様々なリスク（適切な情報共有を妨げる障壁や問題等）が想定される。

そこで、国内外の情報共有に関連する文献や既存の情報共有の仕組み（SNS 等）利用時に発生する法的な課題等を調査し、それらを参考として適切な情報共有を妨げる障壁や問題を、発信者、受信者それぞれについて整理した。

具体的には、想定されるリスクを「情報が流れない」、「情報が過剰に流れる」、「不適切な情報が流れる」の 3 つに分類したうえで、リスクが発生する要因を、「技術的」、「人的」、「法的」の 3 つの観点で、表 4-1 のように整理した。

表 4-1　適切なセキュリティ情報共有を妨げる障壁や問題等のリスク事項と要因

分類		発生主体	
		情報発信側	情報受信側
情報が流れない	技術的要因	技術的な要因により情報を発信できない	技術的な要因により情報を受信できない
		発信者側のシステム障害（内部犯による犯行、外部からのサイバー攻撃、その他内部要因の障害、災害等）	• 受信者側のシステム障害（内部犯による犯行、外部からのサイバー攻撃、その他内部要因の障害、災害等） • 受信した内容の読込エラー（相互運用性）
	人的要因	心理的な要因により情報を発信したくない（発信の拒絶等）	—
		怠惰（必要なタイミングで発信しない、他者による発信を期待して発信しない等） • 受信者に対する信頼性の不足 • 情報が受信者側で改変される不安 • 受信者側で情報ソースを勝手に削除して転送されることの不安 • 競合他社の利益になる不安 • フリーライダーの利益になる不公平感 • 発信に対する責任を回避したい感情 • 自社の評判が低下すること（レピュテーションリスク）の回避 • SNS 等で、情報の利用権が運営者に付与されることに対する嫌悪感 • 匿名で発信しても受信者に特定されてしまう不安	—
		その他の人的な要因により情報が発信されない	—
		単純な発信の失念 シンタックス（構文）エラー等の誤入力 発信者の人員不足等	—
	法的要因	法的な要因により情報を発信できない（訴訟リスクの恐れ） ※通常の範囲での利用を想定する	—
		• 契約関係にあるセキュリティ業者等から有償で得た情報 • 個人情報、プライバシー等に関する情報が含まれる情報 • 業務妨害、信用毀損、誹謗中傷、名誉毀損等に該当する情報 • 情報発信者に著作権のない情報（新聞，雑誌，書籍等のコピーやウェブサイトや SNS の記事等の情報）※他の情報発信者から共有された情報は含まない • 営業秘密保護（不正競争防止法）や輸出管理（輸出規制法）に関する情報 • システム上の機密情報 • ウイルスの検体が含まれる情報	—
情報が	人的要	重複した内容の情報を発信してしまい無駄になる	重複した情報を受信してしまい対応が煩雑になる
		何度も同じような内容の情報を発信	※左記の要因による
		—	情報が多すぎて必要な情報が分からない

分類		発生主体	
		情報発信側	情報受信側
過剰に流れる	因	—	発信者側からの情報提供が多すぎる 受信者側の人員不足等
不適切な情報が流れる	人的要因	悪意ある人物が誤った情報（デマ情報等）を発信する	—
		• 組織に不満のある内部犯行者による改ざんやデマ発信等 • 悪意ある第三者（外部犯行者）による成りすまし、マルウェア配布等	—
		悪意なく誤った情報を発信してしまう	—
		• 単純な入力ミス • 事実誤認	—
		—	情報を誤解釈してしまう
		—	• 単純な誤解釈（情報発信側の記載が難解、情報受信側の理解力不足等） • 他言語の翻訳誤りやニュアンス相違による誤った解釈
		—	心理的な要因により情報を受信したくない（受信の拒絶等）
		—	• 発信者に対する信頼性の不足（情報の信憑性の不安） • 情報が発信者側で改変されている不安（情報の信憑性の不安）
		共有する情報が外部に漏れる	共有する情報が外部に漏れる
		• 発信側の内部の者による共有する情報の持出し • 外部からの進入（オンライン）による情報の窃盗 • 外部からの進入（オフライン）による情報の窃盗 • グループ外への不適切な転送	• 受信側の内部の者による共有する情報の持出し • 外部からの進入（オンライン）よる情報の窃盗 • 外部からの進入（オフライン）による情報の窃盗
		間違った相手に情報を発信してしまう	—
		• 宛先誤り，誤送信 • 情報受信者に成りすました悪意ある第三者への発信	—
	法的	法的に問題のある情報を発信してしまう ※通常の範囲での利用を想定する	法的に問題のある情報を受信し転送してしまう

分類		発生主体	
		情報発信側	情報受信側
	要因	• セキュリティ業者等と契約関係が無い第三者に提供してはいけない情報 • 個人情報，プライバシー等に関する情報が含まれる情報 • 業務妨害，信用毀損，誹謗中傷，名誉毀損等に該当する情報 • 情報発信者に著作権のない情報（新聞、雑誌、書籍等のコピーやウェブサイトや SNS の記事等の情報）※他の情報発信者から共有された情報は含まない • 営業秘密保護（不正競争防止法）や輸出管理（輸出規制法）に関する情報 • システム上の機密情報 • ウイルスの検体が含まれる情報	※左記の要因による

また、円滑な情報共有を促進し、サイバー攻撃によってもたらされる被害を小さく抑えるためには、これらのリスクを低減する施策を講じることが望ましい。そこで、「情報発信側」、「情報受信側」それぞれのリスクへの対応策（案）を、表 4-2 および表 4-3 に各リスクへの対応策（案）を整理した。対応策（案）はリスク事項毎に整理しており、特定のリスク事項のみに有効と考えられる場合は該当するリスクの〇囲み番号を冒頭に付して対応策（案）を記載している。なお、これらの対応策（案）は一般的に想起されるものを記載しているが、詳細については別途検討する必要がある。

表 4-2 「情報発信側」のリスクへの対応策(案)

分類		発生主体	対応策(案)	
		情報発信側	運用	システム
情報が流れない	技術的要因	技術的な要因により情報を発信できない ①発信者側のシステム障害(内部犯による犯行、外部からのサイバー攻撃、その他内部要因の障害、災害等)	・BCP 策定 ・運用フローによる防止 ・運用ルール等の規定と遵守(ID やパスワードの管理、退職者のアクセス制限、不審なメールの対応等) ・監査(運用ルール準拠、脆弱性の点検) ・誓約書の取り交わし(内部犯行の抑止) ・情報共有専用端末の設置	・アクセス権の設定 ・認証 ・各種ログ取得と分析(DNS、プロキシ、F/W、NetFlow、サーバ、ホスト等) ・冗長化、バックアップ取得、RAID 等 ・UPS ・WAF、IPS/IDS(NIDS,HIDS)、F/W 等による検知と抑止 ・SIEM の活用 ・負荷分散装置 ・信頼モデルの構築 ・ウイルス対策ソフトの導入 ・パッチマネジメントの実施
	人的要因	心理的な要因により情報を発信したくない(発信の拒絶等) ①怠惰(必要なタイミングで発信しない、他者による発信を期待して発信しない等) ②受信者に対する信頼性の不足 ③情報が受信者側で改変される不安 ④受信者側で情報ソースを勝手に削除して転送されることの不安 ⑤競合他社の利益になる不安 ⑥フリーライダーの利益になる不公平感 ⑦発信に対する責任を回避したい感情 ⑧自社の評判が低下すること(レピュテーションリスク)の回避 ⑨SNS 等で、情報の利用権が運営者に付与されることに対する嫌悪感 ⑩匿名で発信しても受信者に特定されてしまう不安	・運用フローによる防止 ・運用ルール等の規定と遵守(報告の義務化と罰則の規定、通報制度の規定等、③④:改変等の禁止、⑧:匿名による発信の許可、⑩:匿名発信者の特定の禁止等) ・運用に関する研修 ・監査(運用ルール準拠) ・相談窓口の設置 ・インセンティブ制度による奨励 ・受信者側との信頼関係の強化	—
		その他の人的な要因により情報が発信されない ①単純な発信の失念 ②シンタックス(構文)エラー等の誤入力 ③発信者の人員不足等	・運用ルール等の規定と遵守(①:即時報告等、②:入力方法等) ・運用に関する研修 ・監査(運用ルール準拠) ・【③】運用組織の強化	・【②】入力内容のシステムチェック
	法的要因	法的な要因により情報を発信できない(訴訟リスクの恐れ) ※通常の範囲での利用を想定する ①契約関係にあるセキュリティ業者等から	・運用ルール等の規定と遵守(投稿内容の制限の明確化等、⑦明示の義務化) ・運用に関する研修 ・法律に関する研修	—

分類		発生主体	対応策(案)	
		情報発信側	運用	システム
		有償で得た情報 ②個人情報、プライバシー等に関する情報が含まれる情報 ③業務妨害、信用毀損、誹謗中傷、名誉毀損等に該当する情報 ④情報発信者に著作権のない情報(新聞, 雑誌, 書籍等のコピーやウェブサイトや SNS の記事等の情報)※他の情報発信者から共有された情報は含まない ⑤営業秘密保護(不正競争防止法)や輸出管理(輸出規制法)に関する情報 ⑥システム上の機密情報 ⑦ウイルスの検体が含まれる情報	・監査(運用ルール準拠) ・相談窓口の設置(法律専門家等による) ・【②】法律等でサイバー脅威情報の共有から生じる個人情報漏えい等の法的責任を問わないことを規定(例:米国における「サイバーセキュリティ情報共有法(CISA)」) ・【⑦】専用受付フォーム等の整備	
情報が過剰に流れる	人的要因	重複した内容の情報を発信してしまい無駄になる ①何度も同じような内容の情報を発信	・運用ルール等の規定と遵守(内容の重複確認等) ・運用に関する研修 ・監査(運用ルール準拠)	・ 入力内容のシステムチェック
不適切な情報が流れる	人的要因	悪意ある人物が誤った情報(デマ情報等)を発信する ①組織に不満のある内部犯行者による改ざんやデマ発信等 ②悪意ある第三者(外部犯行者)による成りすまし、マルウェア配布等	・運用フローによる防止 ・運用ルール等の規定(ID やパスワードの管理、退職者のアクセス制限、不審なメールの対応等) ・監査(運用ルール準拠、脆弱性の点検等) ・【①】誓約書の取り交わし(内部犯行の抑止)	・信頼モデルの構築 ・各種ログ取得と分析(DNS、プロキシ、F/W、NetFlow、サーバ、ホスト等) ・WAF、IPS/IDS、F/W 等による検知と抑止 ・改ざん検出(ハッシュ、ブロックチェーンの活用) ・デジタル署名 ・【②】アクセス権の設定 ・【②】認証
		悪意なく誤った情報を発信してしまう ①単純な入力ミス ②事実誤認	・運用フローによる防止 ・運用ルール等の規定(複数人によるチェック等)	—
		共有する情報が外部に漏れる ①発信側の内部の者による共有する情報の持出し ②外部からの進入(オンライン)による情報の窃盗 ③外部からの進入(オフライン)による情報	・監査(運用ルール準拠、脆弱性の点検) ・【①】運用ルール等の規定(持ち出し禁止規定等) ・【①】誓約書の取り交わし(持ち出しの抑止) ・【③】防犯カメラ、入退室管理、物理的な	・外部出力の制限 ・各種ログ取得と分析(DNS、プロキシ、F/W、NetFlow、サーバ、ホスト等) ・SIEM の活用 ・【②】WAF、IPS/IDS(NIDS,HIDS)、F/W 等による検知と抑止

分類		発生主体	対応策(案)	
		情報発信側	運用	システム
		の窃盗 ④グループ外への不適切な転送	施錠等 ・【③】画面ロック ・【④】運用ルールの規定(転送禁止等)	・【③】認証
		間違った相手に情報を発信してしまう ①宛先誤り，誤送信 ②情報受信者に成りすました悪意ある第三者への発信	―	・【①】宛先確認画面の設定 ・【②】信頼モデルの構築
	法的要因	法的に問題のある情報を発信してしまう ※通常の範囲での利用を想定する ①セキュリティ業者などと契約関係がない第三者に提供してはいけない情報 ②個人情報，プライバシー等に関する情報が含まれる情報 ③業務妨害，信用毀損，誹謗中傷，名誉毀損等に該当する情報 ④情報発信者に著作権のない情報(新聞、雑誌、書籍等のコピーやウェブサイトや SNS の記事等の情報)※他の情報発信者から共有された情報は含まない ⑤営業秘密保護(不正競争防止法)や輸出管理(輸出規制法)に関する情報 ⑥システム上の機密情報 ⑦ウイルスの検体が含まれる情報	・ 運用ルール等の規定(投稿内容の制限の明確化等、⑦明示の義務化) ・ 運用に関する研修 ・ 法律に関する研修 ・ 監査(運用ルール準拠) ・ 相談窓口の設置(法律専門家等による) ・【⑦】専用受付フォーム等の整備	・ 入力内容のシステムチェック

表 4-3 「情報受信側」のリスクへの対応策(案)

分類		発生主体	対応策(案)	
		情報受信側	運用	システム
情報が流れない	技術的要因	技術的な要因により情報を受信できない ①受信者側のシステム障害(内部犯による犯行、外部からのサイバー攻撃、その他内部要因の障害、災害等) ②受信した内容の読込エラー(相互運用性)	・【①】BCP 策定 ・【①】運用ルール等の規定と遵守(運用フローによる確認、ID やパスワードの管理、退職者のアクセス制限、不審なメールの対応等) ・【①】監査(運用ルール準拠、脆弱性の点検等) ・【①】誓約書の取り交わし(内部犯行の抑止) ・【①】情報共有専用端末の設置 ・【②】情報発信者との連絡ルートの確保	・【①】各種ログ取得と分析(DNS、プロキシ、F/W、NetFlow、サーバ、ホスト等) ・【①】冗長化、バックアップ取得、RAID 等 ・【①】UPS ・【①】WAF、IPS/IDS(NIDS,HIDS)、F/W 等による検知と抑止 ・【①】SIEM の活用 ・【①】負荷分散装置 ・【①】信頼モデルの構築 ・【①】ウイルス対策ソフトの導入 ・【①】パッチマネジメントの実施 ・【②】技術仕様の統一、共通化
情報が過剰に流れる	人的要因	重複した内容の情報を受信してしまい無駄になる ※情報発信側の「何度も同じような内容の情報を発信」によって生じる	・情報発信者との連絡ルートの確保 ・相談窓口の設置	・入力内容のシステムチェック
		情報が多すぎて必要な情報が分からない ①発信者側からの情報提供が多すぎる ②受信者側の人員不足等	・情報発信者との連絡ルートの確保 ・相談窓口の設置 ・【②】運用組織の強化	入力内容のシステムチェック
不適切な情報が流れる	人的要因	情報を誤解釈してしまう ①単純な誤解釈(情報発信側の記載が難解、情報受信側の理解力不足等) ②他言語の翻訳誤りやニュアンス相違による誤った解釈	・情報発信者との連絡ルートの確保 ・運用フローによる防止 ・運用ルール等の規定(複数人による確認等) ・用語の統一、共通化 ・技術仕様の統一、共通化 ・【②】専門家による翻訳 ・【②】言語の統一、共通化	・【②】高精度な自動翻訳ソフトの導入
		心理的な要因により情報を受信したくない(受信の拒絶等) ①発信者に対する信頼性の不足(情報の信憑性の不安) ②情報が発信者側で改変されている不安(情報の信憑性の不安)	・情報発信者との連絡ルートの確保 ・相談窓口の設置 ・発信者側との信頼関係の強化	・【①】デジタル署名 ・【②】改ざん検出(ハッシュ、ブロックチェーンの活用)
		共有する情報が外部に漏れる ①受信側の内部の者による共有する情報の持出し ②外部からの進入(オンライン)よる情報の	・監査(運用ルール準拠、脆弱性の点検) ・【①】運用ルール等の規定(持ち出し禁止規定等) ・【①】誓約書の取り交わし(持ち出しの抑	・外部出力の制限 ・各種ログ取得と分析(DNS、プロキシ、F/W、NetFlow、サーバ、ホスト等) ・SIEM の活用

分類		発生主体	対応策(案)	
		情報受信側	運用	システム
		窃盗 ③外部からの進入(オフライン)による情報の窃盗	止) ・【③】防犯カメラ、入退室管理、物理的な施錠等 ・【③】画面ロック	・【②】WAF、IPS/IDS(NIDS,HIDS)、F/W 等による検知と抑止 ・【③】認証
	法的要因	法的に問題のある情報を受信し転送してしまう ※情報発信者側の「法的に問題のある情報発信してしまう」によって生じる	・運用ルール等の規定と遵守(投稿内容の制限の明確化等) ・運用に関する研修 ・監査(運用ルール準拠) ・相談窓口の設置(法律専門家等による) ・【⑥】法的に問題の無い情報共有方法の整備(専用受付フォーム等)	・入力内容のシステムチェック

4.2.2. 情報発信の活性化施策

- 0 節で述べたように、情報共有によって、「高度な知見の獲得」、「早期の情報入手」、「情報入手に要する労力の削減」という効果を得られる可能性が高い。その結果として、被害発生時における社会全体の損失を抑制することが期待できる。上記の効果は、ある事業者に属する人員間での情報共有というよりも、異なる事業者に属する人員間での情報共有によって得られるものである。
- 共有される情報には、以下の 2 種類がある。サイバー攻撃やセキュリティ対策に関する情報の発信頻度を上げる施策を考えるに当たっては、下記 2 種類の情報を想定するべきである。
  - 過去に発信されたいずれかの情報に関する新しい情報(補足情報)
  - 過去に発信されたいずれの情報とも無関係の情報(新規情報)
- サイバー攻撃やその対策に関する情報の共有は、何らかのグループに属する人員間で行われる。グループに属する人員の数が多くなることによって、グループ間での情報交換だけではなく、そのグループ内で発信される情報の総数も増加すると考えると、事業者が既存のグループに新たに加わることを促進するような施策も、情報共有を活性化する施策として有用である。このような考え方に基づく施策は、情報共有を阻害する要因を低減したり、事業者が情報共有することで得られる効果を更に高めたりすると期待できる。

以上をまとめると、情報共有を活性化するには、下記のような効果を促す施策の実行が有用と考えられる。

【情報共有を活性化させるために必要な効果】

(1) 補足情報の発信を促進する
(2) 新規情報の発信を促進する
(3) グループ間での情報交換を促進する
(4) 情報を共有するためのいずれかのグループへの加入を促進する
(5) 情報共有の阻害要因を低減する

図 4-2 は、上記 5 つの効果のうち、(1), (2), (4)を模式的に示したものである。

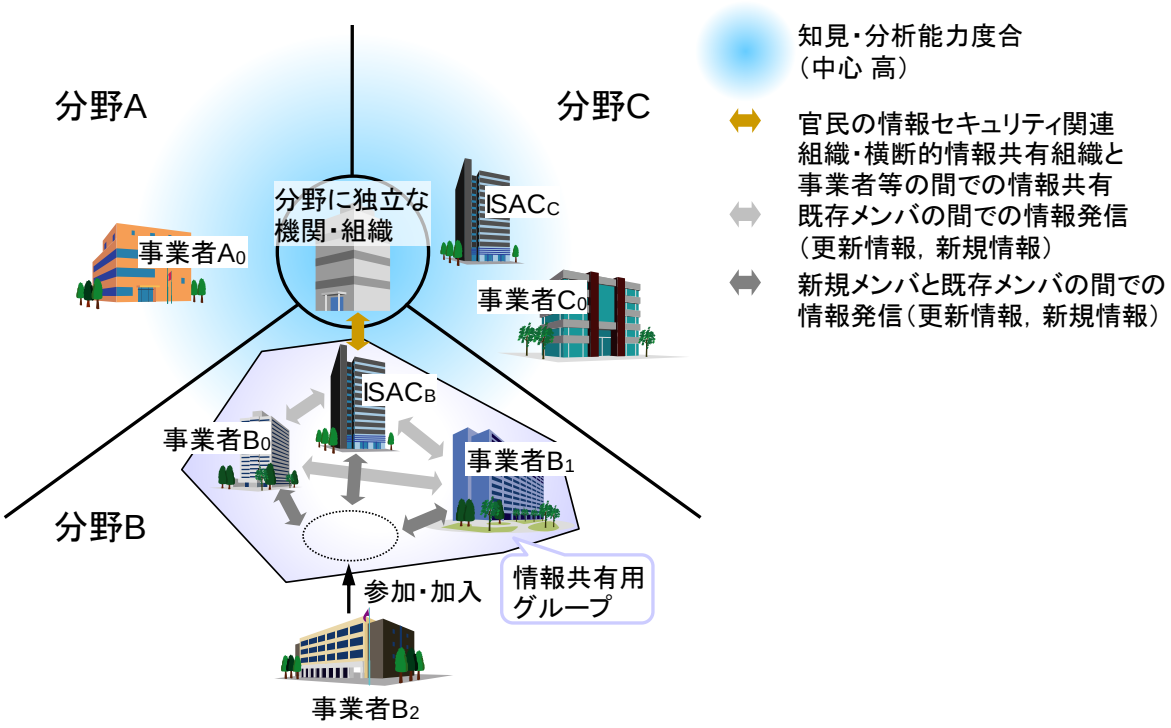


図 4-2　情報共有の活性化施策によってもたらされる効果 3 種((1),(2),(4))

表 4-4 に、情報共有を活性化すると考えられる具体的な施策（20 種）と、各々の施策がもたらす効果（上述 5 種）との対応を示す。

表 4-4　情報共有の活性化施策と活性化施策が備える特性

項番	施策詳細	施策がもたらす効果				
		効果1	効果2	効果3	効果4	効果5
1	情報共有に関する規定を策定する（例: NDA や MOA の締結、組織への参加基準の策定、運用ガイドライン作成、参加事業者・組織間や分野間での規定の作成）	○	○	○		○
2	情報共有を行う範囲を情報提供者が選択できる仕組みを設ける	○	○	○		○
3	情報提供者が情報提供者を匿名化して情報を提供できる仕組みを設ける		○	○		○
4	未参加の事業者等に対して情報共有の枠組みの必要性、有用性を訴求する（例: ホームページへの記載、説明会の実施等）				○	
5	情報共有プラットフォームに参加している事業者同士が、対面で情報を共有できる場を整備する（例: コミュニティのメンバーを集めて定例会議、WG、フォーラム等を開催し、メンバー間の信頼を醸成する）					○
6	情報共有に際して用いられる用語や情報を共有するための技術の仕様を規定する	○	○	○		○
7	類似情報を検索できる機能を実装する	○	○	○		○
8	信頼できる機関が匿名で提供された情報を選別して、不適切な情報を排除する		○	○		
9	専門機関が情報を分析する（例: 重要な情報を取りまとめる（分野毎等）、共有された情報の分析を行い、その結果を提供する）				○	
10	専門機関が情報を分析する（例: 分野別に重要な情報を取りまとめて該当分野に配信する、各情報に重要度を付加する重要な情報をラベル付けする）				○	○
11	専門機関が情報を分析する（例: セキュリティに関する専門家がいなくても、情報提供ができるようにする等）				○	
12	各事業者・組織の要求を踏まえて、共有情報の傾向をレポートにまとめて参加メンバーに提供する				○	○
13	情報共有システムを構築する	○	○	○		○
14	24 時間 365 日運営のサポートセンターを設置する	○	○	○		○
15	ポイントを付与し、ポイントに応じて特典を提供する（例: 会員クラスのランクアップ、補助金の給付等）	○	○	○		○
16	情報に対する評価機能を実装する	○	○	○		○
17	政府が主導で、情報共有の枠組みをつくる				○	
18	機密情報を含んだ情報共有が求められる場合の条件を、政府が法律やガイドラインによって規定する		○	○	○	○

19	情報共有への貢献によって、法人税の一部免除等の優遇措置を取る	○	○	○	○	○
20	インシデント情報等を適切に情報共有していた場合、訴訟等において免責される	○	○	○	○	○

効果1: 補足情報の発信を促進する

効果2: 新規情報の発信を促進する

効果3: グループ間での情報交換を促進する

効果4: 情報を共有するためのいずれかのグループへの加入を促進する

効果5: 情報共有の阻害要因を低減する

5. 情報共有デザインガイドの評価

ここまでで示した日本における情報共有のイメージを検証するために、本事業では、必要な仕組みを有した情報共有システムを開発し、これを実際に重要インフラ事業者に利用もらう運用検証を実施した。その結果は、アンケートによって検証した。本章ではこのアンケートによる検証の結果から、3 章、4 章で示した仮説に対する評価を行った。

なお、上記の運用検証時点において、横断的情報共有組織は存在していないため、横断的情報共有組織のモデレータが担う役割（情報の送信前における送信すべき情報の取捨選択）は、本事業で開発した「脅威情報選択配信技術（追加情報の付与、優先度付け等を行った上で、重要インフラ事業者に配信できる技術）」を用いて代替した。

(1) データフォーマットについて

本事業における情報共有システムの運用検証では、情報提供組織が配信している情報を標準化されたフォーマット（STIX/TAXII）に変換したうえで、重要インフラ事業者への配信を実施した。

標準化されたフォーマット利用によるメリットとして、「自組織内外と機械処理で簡単に脅威情報のやり取りができた」、「(STIX により)整理されて蓄積された脅威情報を、関連性分析機能で解析した結果が見やすく表示された」といった点がアンケート回答として得られたことから、STIX/TAXII という標準化されたフォーマットで配信し蓄積できる機能として、情報提供組織や横断的情報共有組織が「定型化」し、これを活用することの有用性を確認することができた。

一方で、STIX/TAXII の導入予定に関するアンケート回答としては、「導入するために必要なシステム環境が未整備」、「機械処理の運用が未定義」といった理由により、多くの事業者が「未定」であった。一度システムを構築すると、既存システムの更新は容易でないことが想定される為、この段階で幅広く、長期間利用可能なフォーマットとして STIX/TAXII を利用するシステムを構築することが望ましい。

(2) 脅威情報の利用について

本事業における情報共有システムの運用検証において、重要インフラ事業者は ISAC から情報を受信しており、各情報の発信元がどこなのか、重要インフラ事業者が確認できる仕組みを準備した。

実際に受信した脅威情報を用いた重要インフラ事業者の対応は、ファイアウォールへの不正接続先アドレスの登録等の「予防対策」、インシデントから過去事例を確認する等の「的確な対策実施」といったものがアンケート回答として得られた。一方で、受信した脅威情報の活用に関する運用が定まっていない等の理由で受信後の対応が不明確な重要インフラ事業者も存在した。そこで、本書の付属文書である運用ガイドラインでは、具体的にインシデント情報からその対処方法を提案する仕組みや、インシデント情報を機器設定情報へ変換する仕組みを示した。この運用ガイドラインを参照いただき、脅威情報の利活用の運用を構築することが望ましいと考える。

また、重要インフラ事業者が受信した情報を信頼した根拠として「発信元が国内外の公的機関である」といった回答が得られた。情報共有における情報受信側の課題の1つとして「発信者に対する信頼性の不足（情報の信憑性の不安）」があったが、対応策として「発信元の明示」が有用であることを確認できた。

(3) 情報共有における情報の発信について

本事業における情報共有システムの運用検証では、重要インフラ事業者に対する脅威情報の配信のみを実施したが、アンケートでは検証期間に限らない、情報発信の実態について確認した。

自ら発信している重要インフラ事業者は少なく、その理由として「発信すべき脅威情報を保有していない」、「脅威情報として外部に発信すべきか判断する基準や体制等がない」ことが確認できた。情報共有における情報発信側の課題の 1 つに、「心理的な要因により情報を発信したくない（発信の拒絶等）」があると想定している。今回の結果、対応策として「運用ルール等の規定と遵守（報告の義務化等）」の一環で、外部に発信すべき情報を判断する基準を規定することが重要であることが確認できた。

(4) 脅威情報選択配信技術について

脅威情報選択配信技術を用いた評価検証では、外部から大量に提供される脅威情報について、脅威情報の属性（信頼度や危険度）に基づいてフィルタリングしたうえで、重要インフラ事業者に配信した。今回の運用検証では、72 万件のデータを 656 件にまで絞り込めた。フィルタリング前の状態ではあまりに情報量が膨大であり、重要インフラ事業者が確認できていないため、フィルタリング前後で比較するという観点での検証はできなかったが、実運用で確認できる件数にまで絞り込めたことは有用であったと考える。

また、重要インフラ事業者からは「脅威情報は、インディケータだけではなく背景情報も欲しい」、「情報源を明示してほしい」、「どこで発見された脅威なのかが分かるとよい」等の意見が挙げられた。今後、情報を共有するシステムとして、これらも踏まえたサービスとして提供されることが、より利用者の希望に沿うことと考えられる。

参考

1. 想定される情報共有に関連した特性

サイバー攻撃によってもたらされる被害を小さく抑えるには、攻撃や対策の情報を、事業者内（サイバー攻撃を実際に検知し、対策を実施する現場と経営層の人員の間）だけでなく、複数の組織間（複数事業者間，サイバー攻撃等に関する情報の収集・分析・展開などを専門に行う組織と事業者の間）で共有することが望ましい。2つの情報共有の特性には、違いがあると考えられる。そこで以下では、各々について想定される特性を分析する。

1.1. 一事業者内における情報共有において想定される特性

事業者がサイバー攻撃を受ける場合の対象は、事業者が保有する情報システムや制御システムである。これらのシステムは、セキュリティ的観点からは、経営層，CSIRT，現場部門によって管理されるのが一般的である。

現場部門がサイバー攻撃を検知すると、可能であれば現場部門で対策を実行する。しかし、現場部門だけでは対策方法を確定できない場合は、CSIRT に攻撃の内容を報告し、対策方法の提示を依頼する。CSIRT は、報告を受けたサイバー攻撃を分析の上、対策方法を現場部門へ提示する。また、当該攻撃がシステムに及ぼす影響が甚大で、システムの稼働継続／停止の判断等を経営層に仰ぐ必要がある場合は、サイバー攻撃による被害状況や課題、経営上のリスク等を経営層に報告する。経営層は、上述の通り、BCP の観点からサイバー攻撃を受けたシステムの稼働継続や停止を決定し、情報システムの運用者や制御システムの運用者に、結果を指示する。

上記はサイバー攻撃を検知した場合に行われる措置の流れであるが、平時においても、CSIRT はサイバー攻撃に関する情報の収集（左記の意味での監視），分析，知見化等の作業を行っている。

以上に述べた処理の流れは、図のようにまとめられる。

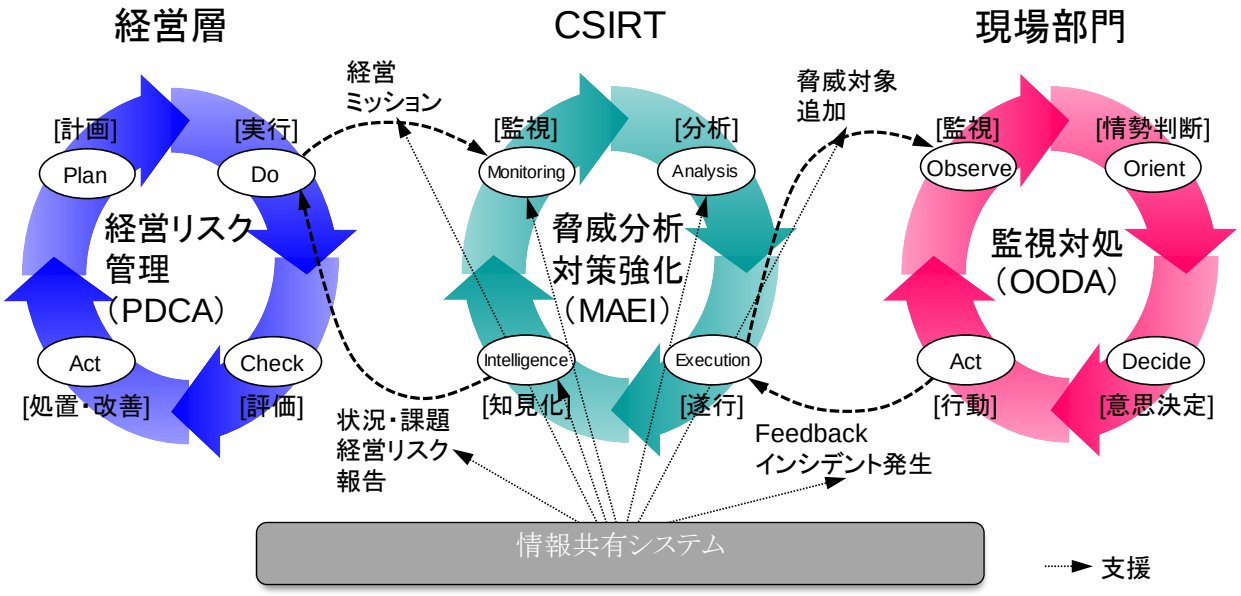


図 1-1 サイバー攻撃を検知後、対策を実施するまでの間に事業者内で実施される処理と情報交換

図 1-1 に示したように、上述の 3 つの部門で行われる処理や部門間で行われる情報の伝達について、これらを支援する仕組みを事業者が導入できれば、当該処理に関する情報や外部組織から入手した情報の伝達をより迅速に達成することができると考えられる。また、その結果として、インシデント発生時にはサイバー攻撃検知から対策の実施までに要する時間の短縮化やシステムの停止が必要となるような事態に陥る可能性の低減、平時には被害発生の事前抑止がそれぞれ期待できる。

1.2. 複数組織間における情報共有において想定される特性

ある分野に属する複数の事業者が同時並列的にサイバー攻撃を受ける事態は実際に発生している。従って、分野内の事業者間で、サイバー攻撃やその対策手段を共有できれば、迅速に対策を実施できるため、生じる被害の規模をより小さく抑えることが期待できる。

一方で、異分野の事業者間でサイバー攻撃情報が共有できるようになると、上記とは違った利点があると考えられる。その一例は、供給連鎖管理(Supply Chain Management)上の利点である。例えば、情報通信分野に属する複数のプロバイダ事業者(Aとする)がサイバー攻撃を受け、情報の送受信が滞る事態が生じたとする。その場合、他の分野の攻撃を受けていない事業者(B とする)のシステム[1]も、必要な処理を十分に実行できなくなる可能性がある。この時、事業者 A と事業者 B の間で当該攻撃に関する情報が共有されていれば、事業者 B は早期に対策を講じることができるため、上記のような事態を生じる可能性を低く抑えることができる。このような推察から、異分野に属する事業者間でも迅速に情報を共有できる仕組みを整備することは、有用であると考えられる。

ところで、事業者が異なれば、両者に導入されている情報を蓄積するための仕組みは異なっている状況も想定する必要がある。従って、このような状況にある事業者間でも情報を共有できるようにするために、両事業者の間には、標準化された記述体系で表現された情報を標準化された手順で行う仕組みが存在することが望ましい。

事業者間で行われる情報の共有を支援する仕組みが存在すれば、情報の共有をより迅速に達成することができると考えられる。その結果として、サイバー攻撃に対する対策の早期実施および供給連鎖の途切れを生じる可能性の抑制が期待できる。

ここまで述べた内容については、情報セキュリティ関係機関等のサイバー攻撃等に関する情報の収集・分析・展開などを専門に行う組織と事業者の間で実施する情報共有についても同様である。

2. 情報共有基盤が備えるべき仕組み

本章では、 4 つのグループ内での情報共有を対象として、事業者が担う役割を図示すると共に、その実現のために情報共有基盤が備えていることを望まれる仕組みの概要について述べる。

なお、以下で述べるいずれのグループ内の情報共有であっても、各組織が異なる情報共有システムを使用している可能性があるため、情報共有基盤は、標準化された記述方式、プロトコルに沿って送受信できる仕組みを備えていることが望ましい。

2.1. 事業者内での情報共有

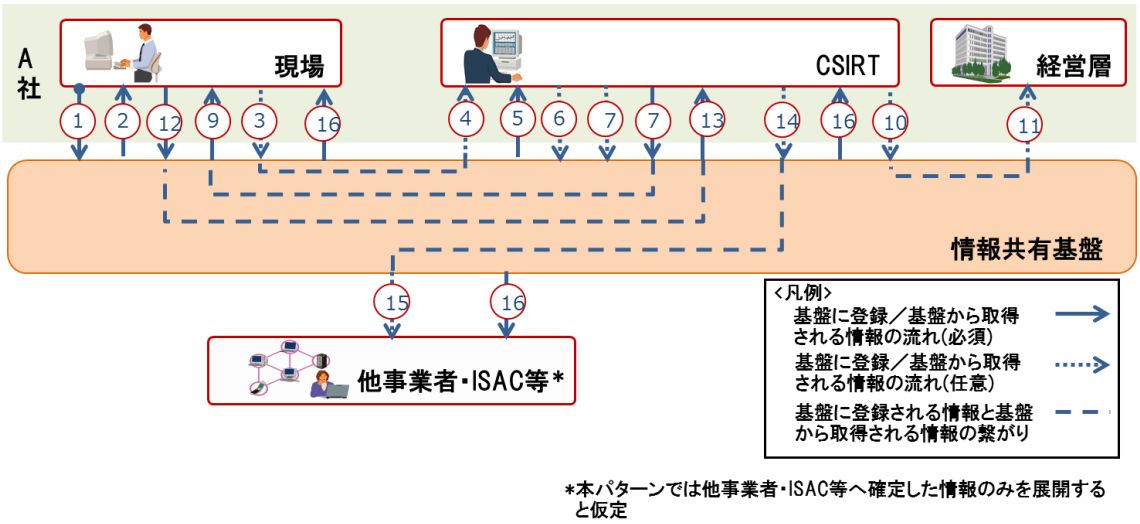
本情報共有は、ある事業者の CSIRT のメンバーと現場部門のメンバーを含むグループを用いて行われる。ここでは、当該事業者の現場部門が監視等を行う過程でサイバー攻撃や疑義を検知した場合を想定した処理の流れを示す。

なお、現場部門から CSIRT に検知した情報が共有された場合において、CSIRT は所属する分野の ISAC のアナリスト等に技術的な支援を依頼することがある。したがって、本節では「事業者内で対応が完結する場合」、「外部に支援を仰ぐ場合」の 2 つに分けて、整理している。

図 2-1 に「事業者内で対応が完結する場合」の情報共有の例を、表 2-1 に示した情報共有を実現するために情報共有基盤に必要な仕組みを示す。なお、図および表の丸囲み数字は対応づけて整理している。

[1] 金融システムや信号システムは、その一例である。

【事業者内で対応が完結する場合】



実施者		番号	概要
A 社	現場	①	発生したインシデントの情報を登録する
		②	情報を収集し、対応策を検討する
		③	対応策を確定できない場合、CSIRT が取得できるような形式で、インシデントの情報を登録する
		⑨	CSIRT が登録した分析結果や対応策を取得する
		⑫	CSIRT が取得できるような形式で、インシデントへの対応の内容を登録する
		⑯	A 社で発生したインシデントに関する最新の情報を取得する
	CSIRT	④	現場が登録した場合、インシデントの情報を取得する
		⑤	情報を収集した上で、共有された情報を分析し、対応策を検討する
		⑥	必要に応じて、分析結果にもとづき、識別子や重要度の付与を実施する
		⑦	必要に応じて、蓄積されている情報と紐付けや統合を実施する
		⑧	現場が取得できるような形式で、分析結果や対応策を登録する
		⑩	必要に応じて、経営層が取得できるような形式で、分析結果を纏めて、報告用レポートとして登録する
		⑬	現場が登録したインシデントへの対応の内容を取得する
		⑭	必要に応じて、他事業者や ISAC 等が取得できる形式で、インシデントの情報を登録する
		⑯	自社で発生したインシデントに関する最新の情報を取得する
	経営層	⑪	CSIRT が登録した報告用レポートを取得する
他事業者 ISAC 等		⑮	CSIRT が登録した場合、インシデントの情報を取得する
		⑯	A 社で発生したインシデントに関する最新の情報を取得する

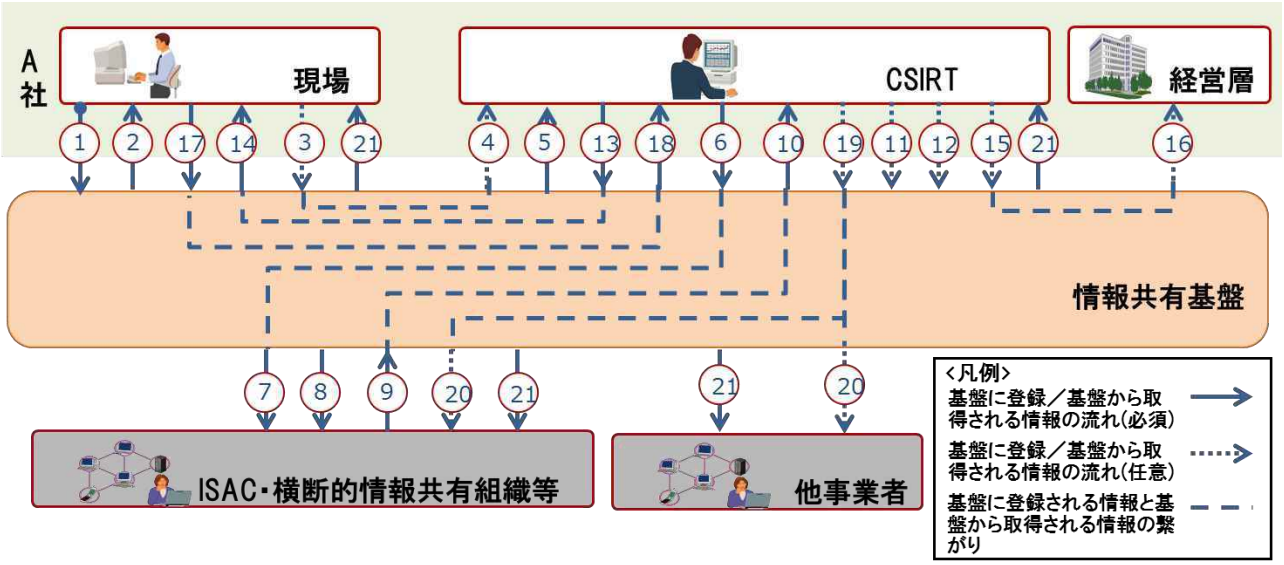
図 2-1　事業者内での情報共有(事業者内で対応が完結する場合)

表 2-1　事業者内での情報共有(事業者内で対応が完結する場合)に必要な仕組み

No	情報共有基盤に必要な仕組み	必要なシーン
1	迅速且つ正確に情報を登録できる仕組み (例: 定型のフォーマット)	①、③、⑧、⑩、⑫、⑭
2	蓄積されている情報から、サイバー攻撃への対策方法を迅速に検索できる仕組み	②、⑤
3	分析に必要な情報(有害サイトのURL、マルウェア、システムのログに関する情報等)を安全に共有する仕組み	③、④、⑧、⑨、⑭、⑮
4	情報に識別子や重要度を付与する仕組み	⑥
5	新しい情報を、蓄積されている情報と関連付けたり、統合する(あるいはそれを支援する)仕組み	⑦
6	組織として対処すべきこと(通知した対応策等)を常時表示する仕組み	⑧
7	報告をまとめる作業を支援する仕組み	⑩、⑪
8	各組織や対象システムへの対策の実施状況を可視化する仕組み	⑫、⑬
9	大量の情報から、必要な情報を絞り込んで表示する仕組み	⑬、⑯
10	あるグループ内で共有された情報の全体または一部を、別のグループ内でも容易に共有できる仕組み	⑭、⑮
11	情報の一部を秘匿する仕組み	⑭、⑮
12	ある事象に関する最新の情報を容易に把握できる仕組み	⑯

図 2-2 に外部に支援を仰ぐ場合の情報共有の例を、表 2-2　事業者内での情報共有(外部に支援を仰ぐ場合)に必要な仕組みに示した情報共有を実現するために情報共有基盤に必要な仕組みを示す。

【外部に支援を仰ぐ場合】



実施者		番号	概要
A 社	現場	①	発生したインシデントの情報を登録する
		②	情報を収集し、対応策を検討する
		③	対応策を確定できない場合、CSIRT が取得できるような形式で、インシデントの情報を登録する
		⑭	CSIRT が登録した分析結果や対応策を取得する
		⑰	CSIRT が取得できるような形式で、インシデントへの対応の内容を登録する
		㉑	自社で発生したインシデントに関する最新の情報を取得する
	CSIRT	④	現場が登録した場合、インシデントの情報を取得する
		⑤	情報を収集した上で、共有された情報を分析し、対策を検討する
		⑥	ISAC・横断的情報共有組織等が取得できるような形式で、技術的な支援依頼を登録する
		⑩	ISAC・横断的情報共有組織等が登録した分析結果や対応策を取得する
		⑪	必要に応じて、分析結果にもとづき、識別子や重要度の付与を実施する
		⑫	必要に応じて、蓄積されている情報と紐付けや統合を実施する
		⑬	現場が取得できるような形式で、分析結果や対応策を登録する
		⑮	必要に応じて、経営層が取得できるような形式で、分析結果を纏めて、報告用レポートを登録する
		⑱	現場が登録したインシデントへの対応の内容を取得する
		⑲	必要に応じて、ISAC・横断的情報共有組織・他事業者等が取得できるような形式で、インシデントの情報を登録する
		㉑	自社で発生したインシデントに関する最新の情報を取得する
	経営層	⑯	CSIRT が登録した報告用レポートを取得する
他事業者		⑳	CSIRT(A 社)が登録した A 社で発生したインシデントの情報を取得する
		㉑	A 社で発生したインシデントに関する最新の情報を取得する

ISAC・横断的情報共有組織等	⑦	CSIRT(A 社)が登録した技術的な支援依頼を取得する
	⑧	情報を収集した上で、共有された情報を分析し、対応策を検討する
	⑨	依頼元の CSIRT(A 社)が取得できるような形式で、分析結果や対応策を登録する
	⑳	CSIRT(A 社)が登録したインシデントの情報を取得する
	㉑	A 社で発生したインシデントに関する最新の情報を取得する

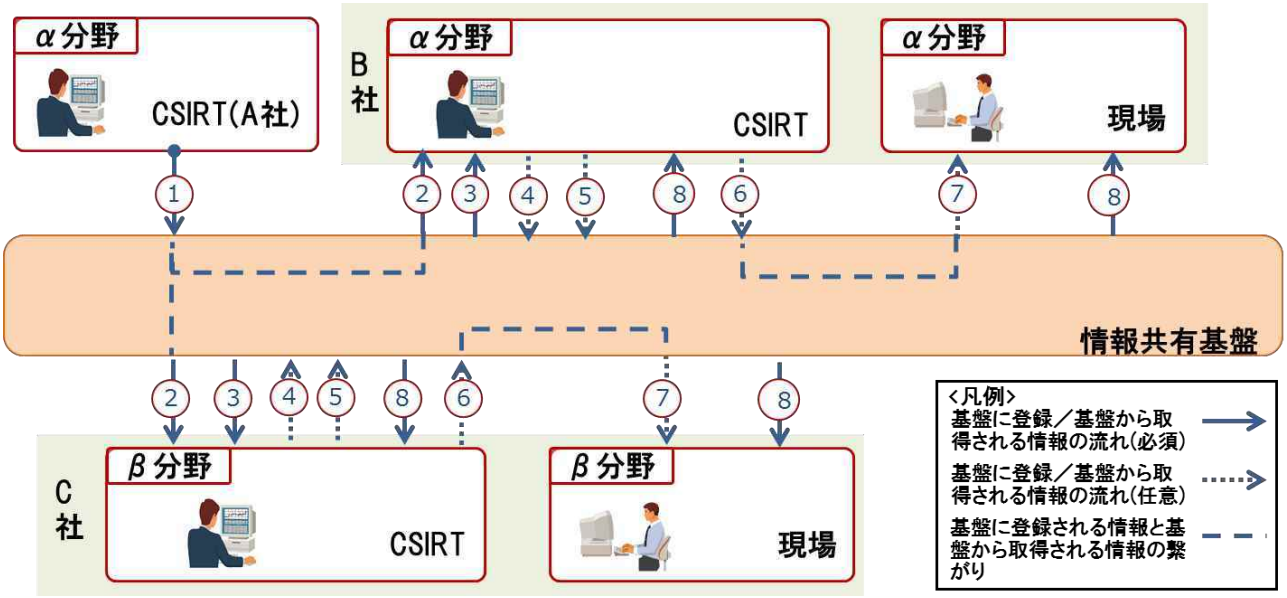
図 2-2　事業者内での情報共有(外部に支援を仰ぐ場合)

表 2-2　事業者内での情報共有(外部に支援を仰ぐ場合)に必要な仕組み

No	情報共有基盤に必要な仕組み	必要なシーン
1	迅速且つ正確に情報を登録する仕組み (例: 定型のフォーマット)	①、③、⑥、⑨、⑬、⑮、⑰、⑲
2	蓄積されている情報から、サイバー攻撃への対策方法を迅速に検索する仕組み	②、⑤、⑧
3	分析に必要な情報(有害サイトのURL、マルウェア、システムのログに関する情報等)を安全に共有する仕組み	③、④、⑥、⑦、⑨、⑩、⑬、⑭、⑰、⑱、⑲、⑳
4	情報の一部を秘匿する仕組み	⑥、⑦、⑲、⑳
5	情報に識別子や重要度を付与する仕組み	⑪
6	新しい情報を、蓄積されている情報の中で関連があるものと関連付けたり、統合する(あるいはそれを支援する)仕組み	⑫
7	組織として対処すべきこと(通知した対応策等)を常時表示する仕組み	⑬
8	報告をまとめる作業を支援する仕組み	⑮、⑯
9	各組織や対象システムへの対策の実施状況を可視化する仕組み	⑰、⑱
10	大量の情報から、必要な情報を絞り込んで表示する仕組み	⑱、㉑
11	ある事象に関する最新の情報を容易に把握できる仕組み	㉑

2.2.　分野内および分野外の複数の事業者が直接行う情報共有

本情報共有は、ある事業者が把握した情報を、当該事業者が所属する分野の他事業者や他の分野の事業者との間で達成されるものである。以下に情報共有の例を図示する。



実施者		番号	概要
A 社 (α 分野)	CSIRT	①	CSIRT(B 社)や CSIRT(C 社)が取得できるような形式で、サイバー攻撃やそれらへの対策に関する情報を登録する
B 社 (α 分野) C 社 (β 分野)	CSIRT	②	CSIRT(A 社)が登録したサイバー攻撃やそれらへの対策に関する情報を取得する
		③	情報を収集した上で、共有された情報を分析し、対応策を検討する
		④	必要に応じて、分析結果にもとづき、識別子や重要度の付与を実施する
		⑤	必要に応じて、蓄積されている情報と紐付けや統合を実施する
		⑥	必要に応じて、現場が取得できるような形式で、分析結果や対応策を登録
		⑧	A 社が展開したサイバー攻撃やそれらへの対策に関する最新の情報を取得する
	現場	⑦	自社の CSIRT が登録した場合、分析結果や対応策を取得する
		⑧	A 社が展開したサイバー攻撃やそれらへの対策に関する最新の情報を取得する

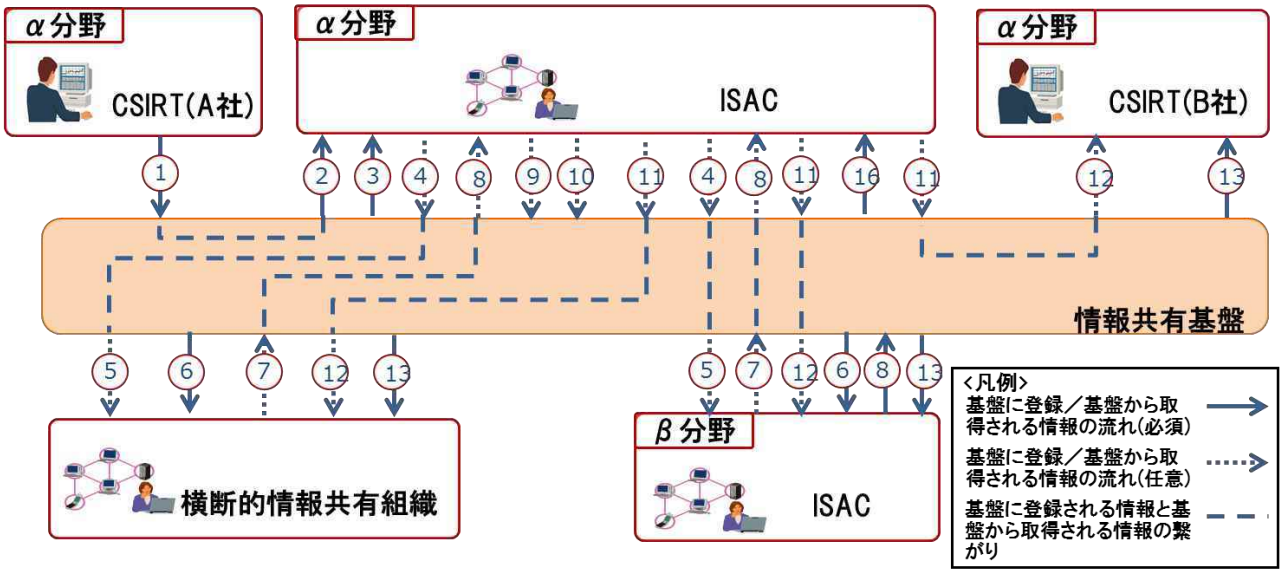
図 2-3　分野内および分野外の複数の事業者が直接行う情報共有

表 2-3　分野内および分野外の複数の事業者が直接行う情報共有に必要な仕組み

No	情報共有基盤に必要な仕組み	必要なシーン
1	迅速且つ正確に情報を登録する仕組み （例: 定型のフォーマット）	①、⑥
2	分析に必要な情報（有害サイトのURL、マルウェア、システムのログに関する情報等）を安全に共有する仕組み	①、②、⑥、⑦
3	情報の一部を秘匿する仕組み	①、②
4	蓄積されている情報から、サイバー攻撃への対策方法を迅速に検索する仕組み	③
5	情報に識別子や重要度を付与する仕組み	④
6	複数の事業者や組織が展開した情報の中で関連があるものを関連付けたり、統合する仕組み	⑤
7	ある事象に関する最新の情報を容易に把握できる仕組み	⑧
8	大量の情報から、必要な情報を絞り込んで表示する仕組み	⑧

2.3.　分野内の複数事業者が ISAC を介して行う情報共有

本情報共有は、ある事業者が把握した情報を、当該事業者が所属する分野の ISAC を介して分野内の複数の事業者との間で達成されるものである。以下に情報共有の例を図示する。



実施者		番号	概要
A 社 (α 分野)	CSIRT	①	所属する分野の ISAC が取得できるような形式で、サイバー攻撃やそれらへの対策に関する情報を登録する
ISAC (α 分野)		②	CSIRT(A 社)が登録したサイバー攻撃やそれらへの対策に関する情報を取得する
		③	情報を収集した上で、共有された情報を分析し、対応策を検討する
		④	必要に応じて、他分野の ISAC(β 分野)や横断的情報共有組織が取得できるような形式で、技術的な支援依頼を登録する
		⑧	ISAC(β 分野)や横断的情報共有組織が登録した分析結果や対応策を取得する
		⑨	必要に応じて、分析結果にもとづき、識別子や重要度の付与を実施する
		⑩	必要に応じて、蓄積されている情報と紐付けや統合を実施する
		⑪	必要に応じて、同じ分野の CSIRT(B 社)、横断的情報共有組織や他分野の ISAC(β 分野)が取得できるような形式で、サイバー攻撃情報やそれらへの対策に関する情報を登録する
		⑬	A 社が展開したサイバー攻撃やそれらへの対策に関するに関する最新の情報を取得する
横断的情報 共有組織		⑤	ISAC(α 分野)が登録した場合、技術的な支援依頼を取得する
		⑥	情報を収集した上で、共有された情報を分析し、対応策を検討する
		⑦	ISAC(α 分野)が取得できるような形式で、分析結果や対応策を登録する
		⑫	ISAC(α 分野)が登録した場合、サイバー攻撃情報やそれらへの対策に関する情報を取得する
		⑬	A 社が展開したサイバー攻撃やそれらへの対策に関するに関する最新の情報を取得する
ISAC (β 分野)		⑤	ISAC(α 分野)が登録した場合、技術的な支援依頼を取得する
		⑥	情報を収集した上で、共有された情報を分析し、対応策を検討する
		⑦	ISAC(α 分野)が取得できるような形式で、分析結果や対応策を登録する

		⑫	ISAC(α分野)が登録した場合、サイバー攻撃情報やそれらへの対策に関する情報を取得する
		⑬	A社が展開したサイバー攻撃やそれらへの対策に関するに関する最新の情報を取得する
B社 (β 分野)	CSIRT	⑫	ISAC(α分野)が登録した場合、サイバー攻撃情報やそれらへの対策に関する情報を取得する
		⑬	A社が展開したサイバー攻撃やそれらへの対策に関するに関する最新の情報を取得する

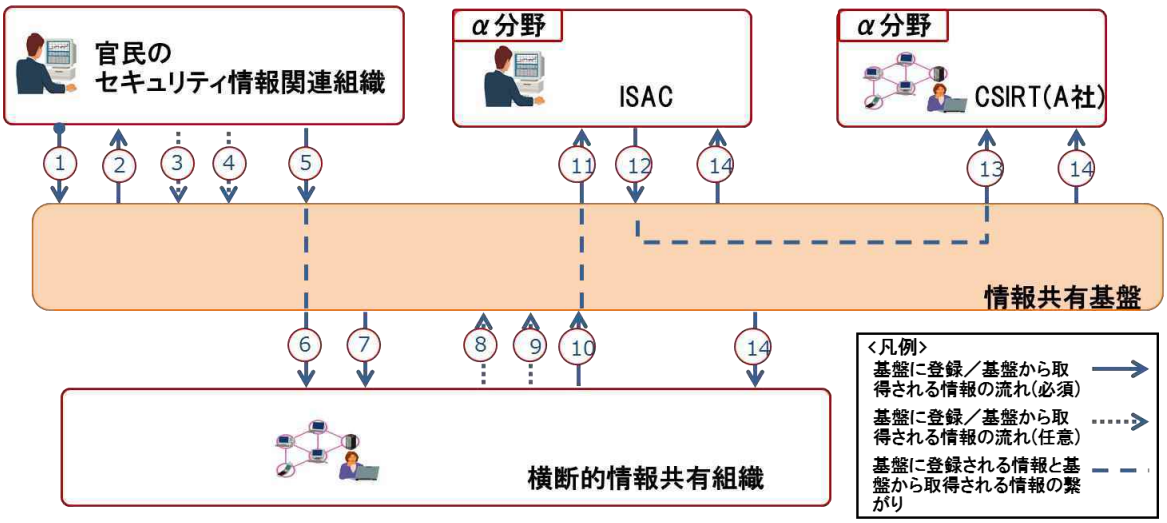
図 2-4　分野内の複数事業者が ISAC を介して行う情報共有

表 2-4　分野内の複数事業者が ISAC を介して行う情報共有に必要な仕組み

No	情報共有基盤に必要な仕組み	必要なシーン
1	迅速且つ正確に情報を登録する仕組み (例: 定型のフォーマット)	①、④、⑦、⑪
2	分析に必要な情報(有害サイトのURL、マルウェア、システムのログに関する情報等)を安全に共有する仕組み	①、②、④、⑤、⑦、⑧、⑪、⑫
3	情報の一部を秘匿する仕組み	①、②、④、⑤、⑦、⑧、⑪、⑫
4	蓄積されている情報から、サイバー攻撃への対策方法を迅速に検索する仕組み	③、⑥
5	情報に識別子や重要度を付与する仕組み	⑨
6	複数の事業者や組織が展開した情報の中で関連があるものを関連付けたり、統合する仕組み	⑩
7	ある事象に関する最新の情報を容易に把握できる仕組み	⑬
8	大量の情報から、必要な情報を絞り込んで表示する仕組み	⑬

2.4.　官民のセキュリティ情報関連組織と横断的情報組織や ISAC，事業者との間で行われる情報共有

官民のセキュリティ情報関連組織は、サイバー攻撃や対策の情報を収集し、横断的情報共有組織や ISAC、事業者へ展開することが考えられる。以下に情報共有の例を図示する。



実施者		番号	概要
官民のセキュリティ情報関連組織		①	収集したサイバー攻撃、それらへの対策、ソフトウェアの脆弱性に関する情報等を登録する
		②	情報を収集した上で、共有された情報を分析し、対応策を検討する
		③	必要に応じて、分析結果にもとづき、識別子や重要度の付与を実施する
		④	必要に応じて、蓄積されている情報と紐付けや統合を実施する
		⑤	横断的情報共有組織が取得できるような形式で、サイバー攻撃、それらへの対策、ソフトウェアの脆弱性に関する情報等を登録する
横断的情報共有組織		⑥	官民のセキュリティ情報関連組織が登録したサイバー攻撃、それらへの対策、ソフトウェアの脆弱性に関する情報等を取得する
		⑦	情報を収集した上で、共有された情報を分析し、対応策を検討する
		⑧	必要に応じて、分析結果にもとづき、識別子や重要度の付与を実施する
		⑨	必要に応じて、蓄積されている情報と紐付けや統合を実施する
		⑩	ISAC が取得できるような形式で、サイバー攻撃、それらへの対策、ソフトウェアの脆弱性に関する情報等を登録する
		⑭	官民のセキュリティ情報関連組織が展開したサイバー攻撃、それらへの対策、ソフトウェアの脆弱性等に関する最新の情報を取得する
ISAC（α 分野）		⑪	横断的情報共有組織が登録したサイバー攻撃情報を取得する
		⑫	CSIRT(A 社)が取得できるような形式で、分析結果や対応策を登録する
		⑭	官民のセキュリティ情報関連組織が展開したサイバー攻撃、それらへの対策、ソフトウェアの脆弱性等に関する最新の情報を取得する
A 社（α 分野）	CSIRT	⑬	ISAC が登録した分析結果や対応策を取得する
		⑭	官民のセキュリティ情報関連組織が展開したサイバー攻撃、それらへの対策、ソフトウェアの脆弱性等に関する最新の情報を取得する

図 2-5　官民のセキュリティ情報関連組織と横断的情報共有組織や ISAC，事業者との間で行われる情報共有

表 2-5　官民のセキュリティ情報関連組織と横断的情報共有組織や ISAC，事業者との間で行われる情報共有に必要な仕組み

No	情報共有基盤に必要な仕組み	必要なシーン
1	迅速且つ正確に情報を登録する仕組み （例: 定型のフォーマット）	①、⑤、⑩、⑫
2	蓄積されている情報から、サイバー攻撃への対策方法を迅速に検索する仕組み	②、⑦
3	情報に識別子や重要度を付与する仕組み	③、⑧
4	複数の事業者や組織が展開した情報の中で関連があるものを関連付けたり、統合する仕組み	④、⑨
5	分析に必要な情報（有害サイトのURL、マルウェア、システムのログに関する情報等）を安全に共有する仕組み	⑤、⑥、⑩、⑪、⑫、⑬
6	情報の一部を秘匿する仕組み	⑤、⑥、⑩、⑪、⑫、⑬
7	ある事象に関する最新の情報を容易に把握できる仕組み	⑭
8	大量の情報から、必要な情報を絞り込んで表示する仕組み	⑭

3.　規制・制度を伴うセキュリティ規格等の概要

重要インフラ(制御・ヘルスケア・金融・公共・情報)において、規制・制度を伴うセキュリティ規格について、概要を整理する。

3.1.　制御

規格	内容	発行元	認証制度の名称，機関等
電力制御システムセキュリティガイドライン (ガイド・日本)	電力制御システム等のサイバーセキュリティ確保を目的として、電気事業者が実施すべきセキュリティ対策の要求事項について規定	JESC	—
SAE J-3061 (規格・米)	自動車向けのサイバーセキュリティ標準プロセスおよび技術のベストプラクティス	SAE International	—
NIST サイバーセキュリティフレームワーク (ガイド・米)	サイバーセキュリティの効果的・効率的なリスク低減を実現するために、適切なサイバーセキュリティ管理の一つの在り方を示唆	NIST	—
NIST IR 7628 (ガイド・米)	スマートグリッド向けのセキュリティガイドライン。スマートグリッドに関わる全電気事業者が参照可能	NIST	—
CFATS (規制・米)	高リスクな化学業界・化学施設におけるセキュリティ基準を設けた規制	DHS	—
NERC CIP (規制・米)	北米電力信頼性評議が、重要インフラ(発電、化学薬品、水、石油、ガス等)のうち、発電に関わる事業を遂行する上で実施すべきセキュリティ規準。大規模発電および送電施設を対象としたサ	NERC NIST	—

	イバーセキュリティに関する義務		
IEC 62443 (国際標準規格)	制御システムセキュリティの全レイヤ/プレイヤーをカバーした規格	IEC	—
IEC 62443-1 (国際標準規格)	IEC62443 の中で用いられる用語解説、制御システムセキュリティ動向、SCADA モデル一般論などを記載 IEC62443-1-1:用語、コンセプト、モデル定義の技術仕様書 IEC62443-1-2:用語、略語の技術報告書 IEC62443-1-3:システム安全性評価基準の文書		
IEC 62443-2 (国際標準規格)	設備所有者・組織を対象としたセキュリティ要求事項の規定 IEC62443-2-1:制御システムのセキュリティプログラム確立方法について規定 IEC62443-2-2:制御システムのセキュリティプログラム運用ガイドライン規定 IEC62443-2-3:制御システムにおけるパッチ管理方法に関するガイドラインの技術報告書 IEC62443-2-4:制御システム提供者に対するセキュリティ要求事項を規定	IEC	CSMS 適合製評価制度(日) JIPDEC(認定機関)
IEC 62443-3 (国際標準規格)	複数機能の組合せによる制御システム、インテグレータを対象とした規格 IEC62443-3-1:一般的セキュリティ技術のうち制御システムで適用可能なものの技術報告書 IEC62443-3-2:領域(ゾーン)やそれを連結するコンジットに関するセキュリティの規定文書 IEC62443-3-3:制御システムのセキュリティ機能要件を規定	IEC	SSA 認証
IEC 62443-4 (国際標準規格)	制御システムの個別コンポーネント単位の規格 IEC62443-4-1:コンポーネントの開発要件を規定 IEC62443-4-2:コンポーネントのセキュリティ要件を規定	IEC	EDSA 認証
ISO/IEC 29192 (国際標準規格)	リソースが限られた計算機環境に適した暗号に関する規格。規格書は、パート 1:「総論」、パート 2「ブロック信号」、パート 3:「ストリーム信号」、パート 4:「公開鍵暗号技術を使うメカニズム」の 4 部構成	ISO/IEC	—
DO-178 (ガイド・米)	航空機のソフトウェア信頼性、安全性に係るガイド。A、B、C が存在	RTCA	FAA 認証
IEEE 1686 (標準規格・米)	変電所内のインテリジェント電子機器 (IED)のサイバーセキュリティに関する規格	IEEE	—
IEC 62351	電力システム制御操作のための情報セキュリティ	IEC	—

(国際標準規格)	をスコープとし、通信プロトコルのセキュリティ標準を規定		
IEEE 2030 (標準規格・米)	電力システム、アプリケーション、電力機器にかかわるエネルギー技術と情報技術の運用について、スマートグリッドの相互運用性を定めるための指針	IEEE	—
IEC 61850 (国際標準規格)	スマートグリッドに関する通信プロトコルとそのサービスについて規定。また、システム設定情報を交換するためのアプリケーションの情報モデル、および、標準化された、XML ベースの言語を含む 14 のパートから構成	IEC	—
IEC 62351 (国際標準規格)	電力システム制御操作のための情報セキュリティをスコープとし、通信プロトコルのセキュリティ標準を規定	IEC	—
IEC 62278 (国際標準規格)	鉄道システムにおける安全規格・ガイドライン	IEC	RAMS
IEC 62280 (国際標準規格)	鉄道用安全システムの通信における規格	IEC	—

3.2. ヘルスケア

規格	内容	発行元	認証制度の名称, 機関等
MDS2 (標準規格・米)	医療機器製造業者が、ヘルスケア事業者に対してセキュリティ関連情報を開示するための記載様式を提供するセキュリティ宣言書	NEMA、HIMSS	—
ANSI/UL 2900-2-1 (標準規格・米)	医療機器業界向けサイバーセキュリティの個別規格。ネットワーク接続型の医療機器のセキュリティ確保	UL Inc.	FDA 認定
IEC 62304 Amd1 Ed.1 (国際標準規格)	医療機器ソフトウェアの開発・保守において実施すべきプロセスを規定した規格	IEC	—
IEC 80001 シリーズ (国際標準規格)	医療機器の情報セキュリティニーズに関する事項を網羅、医療機器の IT ネットワークリスク管理	IEC	—
IEC 82304-1 (国際標準規格)	ヘルスケアソフトウェア製品の安全性を確保することを目的に、ライフサイクルプロセス規格である IEC62304 に加え、ソフトウェア製品の安全性とセキュリティについての製造業者への要求事項を定めた規格	IEC	—
医療情報システムの安全管理に関するガイドライン (ガイド・厚生労働省)	医療機関が主体となって医療情報システムの機密性・完全性・可用性を確保するために医療情報システムの安全管理を行うためのガイドライン	厚生労働省	—
「医療機器におけるサイバーセキュリティの確保について」	医療機器製造業者が主体となって、サイバーリスクに対する医療機器の機能性と患者の安全を保持するためのセキュリティ通知	厚生労働省	—

(通知・厚生労働省)			
HIPAA (規制・米)	1996 年に米国 DHHS(保健社会福祉省)が策定した医療情報のプライバシー保護とセキュリティ確保を目的とした法規制	DHHS	—
HITECH (規制・米)	2009 年に制定された、経済的および臨床的健全性のための医療情報技術に関する法規制。HIPPA における罰則規定を大幅に追加	DHHS	—
EU データ保護規則 (GDPR) (規則・EU)	個人データに関する自然人の保護および同データの自由な移動に関する規則。EU データ保護指令(Directive95/46/EC)が廃止され、GDPR へ	EC	—

3.3. 金融・公共

規格	内容	発行元	認証制度の名称, 機関等
PIPEDA (規制・カナダ)	個人情報保護と電子文書に関する法規制。民間企業の情報収集・使用・開示を規制。パスワードの使用や暗号化などの技術的な対策を含み、情報の重要度に適した安全予防手段で個人情報を保護することを義務付けられている	Canadian Standards Association	—
PCI-DSS (規格・国際)	加盟店やサービスプロバイダにおいて、クレジットカード会員データを安全に取り扱う事を目的として策定された、クレジットカード業界のセキュリティ基準	PCI SSC	PCI SSC 審査
GISP (プロジェクト・米)	テレコミュニケーションのセキュリティポリシーを含んだグローバル研究プロジェクト	The Stilwell Center	—

3.4. 情報

規格	内容	発行元	認証制度の名称, 機関等
ISO/IEC 15408 (国際標準規格)	情報技術に関連した製品およびシステムが適切に設計され、かつその設計が正しく実装されているかどうかを評価するための国際的なセキュリティ基準	ISO/IEC	JISEC(日本) IPA(認証機関)CCRA(*1)に参加
ISO/IEC 19790 (国際標準規格)	米国およびカナダが運営する暗号モジュール試験および認証制度(CMVP)で採用されている FIPS 140-2 を基に作成された暗号モジュールのセキュリティを確保するための要求事項を定めた国際規格	ISO/IEC	(*2) ・JCMVP(日本) IPA(認証機関) ・CMVP NIST、カナダ CSEC(認証機関)

ISO/IEC 24759 **(国際標準規格)**	暗号モジュールのセキュリティ試験要件を決めている規格	ISO/IEC	(*2) ・JCMVP（日本） IPA（認証機関） ・CMVP NIST、カナダCSEC(認証機関)
ISO/IEC 27001 **(国際標準規格)**	情報セキュリティマネジメントシステムの要件を示した規格。組織の情報セキュリティ目標のもと，保有する情報セキュリティに係るリスクの特定・評価結果に基づき，セキュリティ施策を実装・改善するしくみを提供	ISO/IEC	ISMS 適合性評価制度（日本） JIPDEC，JAB（認定機関）
ISO/IEC 27002 **(国際標準規格)**	情報セキュリティ施策を 11 のカテゴリ，35 の管理目的，および 114 の管理策として示したガイドライン規格。ISO/IEC 27001の付属書で示される管理目的・管理策の解説書に相当	ISO/IEC	—
FIPS 140-2 **(ガイド・米)**	機密かつ未分類のデータを使用するにあたり、IT製品が準拠する必要のある暗号化および関連する安全上の要件を示した米国政府が定める基準	—	CMVP NIST（米，認証機関） CSE（加，認証機関）
FISMA **(規制・米)**	連邦情報セキュリティマネジメント法。連邦政府機関への情報セキュリティ強化を義務付ける法律。そのための規格やガイドラインの開発はNISTに義務付け。FIPS や SP シリーズがそれらにあたる	DHS	—

(*1) CC に基づいたセキュリティ評価・認証の加盟国間での相互承認に関する協定

(*2) 但し、JCMVP と CMVP は、共同認証で合意

参考文献・情報

[1] 内閣サイバーセキュリティセンター. 主要公表資料 “サイバーセキュリティ政策に係る年次報告(2015 年度)”, http://www.nisc.go.jp/active/kihon/pdf/jseval_2015.pdf

[2] サイバーセキュリティ戦略本部,” 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 30 年 7 月 25 日改定,https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r1.pdf

[3] JPCERT/CC. “高度サイバー攻撃(APT)への備えと対応ガイド”, https://www.jpcert.or.jp/research/20160331-APTguide.pdf

[4] ビジネス + IT. “門林雄基氏県談 – 攻撃側や利用者側の変化に伴い、新局面へ突入した IT セキュリティ対策”, 2012 年 9 月 10 日, http://www.sbbit.jp/article/cont1/25361

[5] Symantec. インターネットセキュリティ脅威レポート 第 21 号, 2016 年 4 月, https://www.symantec.com/ja/jp/security_response/publications/threatreport.jsp

[6] ITPro. “韓国激震、サイバー攻撃が同時多発”, http://itpro.nikkeibp.co.jp/article/COLUMN/20130328/466648/?rt=nocnt

[7] JPCERT/CC. 情報提供 “注意喚起”, https://www.jpcert.or.jp/at/2016.html

[8] JPCERT/CC. 情報提供 “早期警戒情報の提供について”, https://www.jpcert.or.jp/wwinfo/

[9] 情報処理推進機構. “サイバー情報共有イニシアティブ(J-CSIP(ジェイシップ))”, https://www.ipa.go.jp/security/J-CSIP/

[10] “攻めの防御 サイバーインテリジェンス”, 日経コンピュータ, pp. 20 – 37, 2016 年 6 月 9 日

[11] 内閣サイバーセキュリティセンター.「セプターカウンシル」の活動 “重要インフラ セプター一覧表”, http://www.nisc.go.jp/active/infra/pdf/cc_ceptoar.pdf

[12] 独立行政法人 情報処理推進機構. “企業の CISO や CSIRT に関する実態調査 2016 -調査報告書-”, https://www.ipa.go.jp/files/000052362.pdf

[13] ISAO Standards Organization. “ISAO 300-1 Introduction to Information Sharing”, Sept. 30, 2016, https://www.isao.org/products/isao-300-1-introduction-to-information-sharing/