緊急度の高い脅威情報を迅速に配信し、重要インフラ事業者を防御

株式会社日立製作所
セキュリティ事業統括本部
本部員
高見（たかみ）　穣（ゆたか）

株式会社日立製作所
セキュリティ事業統括本部
主任技師
勝家（かついえ）　由樹（ゆき）

1. はじめに

近年、重要インフラシステムへのサイバー攻撃は高度化し、その影響が広範にわたるため、個々の重要インフラ事業者が単独でセキュリティ対策を講じていては対処しきれない。2015年9月に閣議決定された「サイバーセキュリティ戦略」においても、重要インフラを防御するため「効果的かつ迅速な情報共有の実現」が項目として掲げられている。

脅威やインシデント等の情報及び他組織で発生した事象や兆候を重要インフラ事業者間で迅速に共有して第二・第三の被害を未然に防止すること、対策技術を共有して事前に対処できる耐性の強いシステム運用を実現することが期待されている。

効果的に情報共有を行うためには、次の課題を解決する必要がある。

- 重要インフラ事業者等に対する情報提供のインセンティブ確保
- 情報の迅速な共有と活用
- セキュリティ対策に不足する情報の補完

上記課題の解決のため、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」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研究開発を2015年度～2019年度まで行った。

本稿では、実施した研究開発の内容について、記述する。

2. 研究開発の目的

近年、重要インフラシステムに対するサイバー攻撃が増加、高度化しており、実被害が発生するようになってきた。

国内では、2015年6月に年金機構においてマルウェア感染による大規模な情報漏えい事故が発生している。本事件では、同一のマルウェアに多数の組織が感染し、被害を拡大させたが、その原因の一つに、他組織での被害の状況や原因などの脅威の情報が共有されなかったために対策が後手に回ったことが挙げられる。

高度化しその影響が広範にわたる重要インフラへのサイバー攻撃の脅威へ対抗するためには、個々の重要インフラ事業者が単独でセキュリティ対策を講じている現状では対処しきれない状況になってきている。

このような状況に対し、2015年9月に閣議決定された「サイバーセキュリティ戦略」においても重要インフラを防御するため、「効果的かつ迅速な情報共有の実現」が項目として掲げられた。

このように、関連する重要インフラ事業者等の間で脅威やインシデント等の情報を共有し、他組織で発生した事象や兆候をいち早く共有することで第二・第三の被害を未然に防止すること、さらには、対策技術も共有して事前対処性にも優れた耐性の強いシステム運用を実現することが期待されている。

我が国のサイバーセキュリティ対策の促進に貢献することを目的として、本研究開発を実施した。

3. 研究開発の内容

年々高度化するサイバー攻撃に対処するため、異なる重要インフラ事業者間で脅威やインシデント等の情報を迅速に共有することが必要とされている。

重要インフラ事業者が提供しているサービスのログ分析・バックドア解析・モデル解析等により得られた情報を、重要インフラ事業者ごとに情報共有・分析を行う「事業者内情報共有」、重要インフラ分野内の他の事業者と情報共有する「分野内情報共有」、重要インフラ事業者等全体で情報共有する「分野横断情報共有」が重要となると考えられる。さらに、この情報共有と分析を行う体制（例えば重要インフラ分野のISAC[*1]）と国内外の関係機関との連携により情報を統合することで、さらに詳細な情報共有・分析機能を実現できると考えられる。

研究対象は、重要インフラ事業者等（「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」）のサイバーセキュリティとした。特に、それらの制御・通信機器及び制御ネットワークを対象とした。

実施した項目は、主に以下の2点である。

(1) 情報共有ツールの開発

ISAC組織や事業者が脅威情報を取り扱うにあたり、受信する「データ形式がバラバラで統一的に扱えない」点や「データベース化されていないため、大量情報の分析及び重要度に応じた選別や対応が困難である」という課題が生じている。

本研究では、以下の方向性をめざし、国内インフラ事業者のニーズに沿うよう、日本語対応、添付資料の配信可能等、国内情報発信組織の配信情報に特化した情報共有ツールを開発した。

- 情報提供機関より、定型フォーマットで脅威情報をISAC（中継組織）へ提供し、脅威情報DBへ蓄積する。蓄積された情報は、事業者側へも提供され活用される。
- 定型フォーマットで上記の運用を実現することにより、対策までのリードタイムを短縮できる。

(2) 社会実装に向けた関係組織の支援

重要インフラ事業者間で脅威情報等を安全に共有する機能を実現するための、日本での情報共有の在り方を検討し、諸外国動向調査や関係団体へのヒアリング調査等で得られた結果を踏まえて、その妥当性を検証した。

国内外の重要インフラに対するサイバー攻撃事例、情報共有制度、情報共有プラットフォーム等の調査結果に基づき、事業者及び有識者との議論を繰り返し、セキュリティ情報共有の認識・目的・体制の整理、再構築を実施した。

これらの研究内容を踏まえ、情報共有機能の立ち上げを支援するドキュメントとして、「情報共有デザインガイド（構築編）」と「情報共有デザインガイド（運用編）」を作成した。

実施した研究項目の関係を、**図1**に示す。

4. 研究開発の成果

(1) 情報共有ツールの開発

国際的な標準フォーマットであるSTIX*2/TAXII*3を採用した情報共有のためのツールとして、商用化に向けた必要機能や重要インフラ事業者が要望する機能をも含めた社会実装版プロトタイプを開発した。

開発したプラットフォームは、以下の特徴を有する。

- 情報を機械処理可能な標準フォーマットとすることで、事業者/ISAC間で機械的に情報処理が可能である。
- 情報の標準フォーマットとして、最新の国際標準であるSTIX/TAXIIを採用し、海外との情報共有も容易に可能とする。

この社会実装版プロトタイプを用いて、参加事業者間で脅威情報を共有するための情報共有プラットフォームの実

■図1. 研究項目の関係性

*1　Information Sharing and Analysis Center（アイザック）
業界ごとにサイバーセキュリティに関する情報を共有し、サイバー攻撃への対策及び安全性向上のために協働活動を行う民間組織。
*2　Structured Threat Information eXpression (trademark of The MITRE Corporation)
*3　Trusted Automated eXchange of Indicator Information (trademark of The MITRE Corporation)

運用実験を実施した。運用実験の結果は、開発した情報共有プラットフォームに反映した。

実施した運用実験のイメージを図2に示す。

(2) 情報共有デザインガイドの作成

国内外の情報共有に関する調査を実施し、社会実装に利する情報共有デザインガイド（構築編/運用編）を作成した。

「情報共有デザインガイド（構築編）」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）を示すとともに、必要な仕組みなどを示したものである。

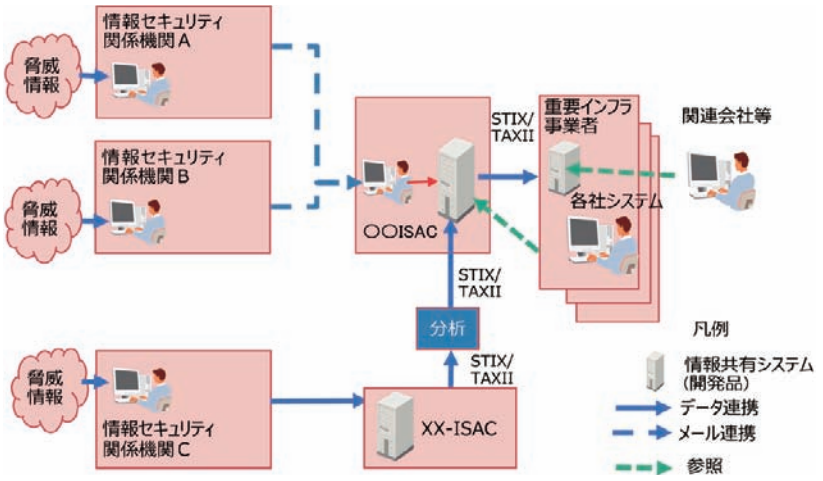
情報共有デザインガイド（構築編）として策定した内容を表に示す。

なお、「情報共有デザインガイド（構築編）」は、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し、以下のサイトにて公開している。

https://www.nedo.go.jp/content/100904081.pdf

5. 実用化事例

研究開発の成果である情報共有ツールを活用したプラットフォームに、検証結果を反映し、情報分析等の付帯サービスを組み合わせた「SHIELD 情報共有サービス」として



■図2. 運用実験のイメージ

■表. 情報共有デザインガイド（構築編）の内容

章	記載内容
1章 サイバーセキュリティにおける情報共有の必要性	・重要インフラ事業者に対するサイバー攻撃の現状 ・情報の共有及び対策の実行により事業者が得る効果 ・日本の重要インフラ事業者における情報共有の現状
2章 情報共有の海外事例	・情報共有の海外事例 ・海外事例から得られた示唆
3章 日本における情報共有のイメージ（仮説）	・重要インフラ事業者からの情報共有に関する課題、要望 ・重要インフラ事業者における情報共有のイメージ（仮説） ・各組織が配置すべき人員の役割 ・情報共有のパターン ・共有すべき情報
4章 日本における情報共有のイメージ（仮説）に必要な仕組み	・情報共有システムの機能 ・情報共有を促す施策
5章 情報共有デザインガイドの評価	・データフォーマットについて ・脅威情報の利用について ・情報共有における情報の発信について ・脅威情報選択配信技術について
参考情報	・想定される情報共有に関連した特性 ・情報共有基盤が備えるべき仕組み ・規制・制度を伴うセキュリティ規格等の概要

2018年5月より商用サービス化した。

このSHIELD情報共有サービスについて、以下に述べる。

(1) 概要

本研究開発を通じて、世界中から報告されるセキュリティ情報を異なる組織間で迅速かつ安全に共有するための情報共有基盤を開発した。株式会社日立システムズより、この基盤を実装した「SHIELD 情報共有サービス」を重要インフラ事業者やサイバーセキュリティ関連組織向けに提供開始した。

(2) 本研究開発の成果

今回開発した情報共有基盤は、外部の情報機関からの提供や他の企業・組織が共有したサイバーセキュリティ情報を蓄積し、利用者が必要な時に必要な情報を検索・周知するための基盤である。本基盤は、国際標準規格であるSTIX・TAXIIを採用しているため、国内外の脅威情報及び対策方法について、STIX・TAXIIを採用する他の情報機関から受信し、注意喚起として一斉自動配信する機能を備えている。

(3) SHIELD 情報共有サービス

本研究開発の成果を活用し、株式会社日立システムズは、同社のサイバーセキュリティソリューション「SHIELD」のラインアップの一つに「SHIELD 情報共有サービス」を追加し、提供を開始した。今後継続し展開する。

SHIELD 情報共有サービスは、情報発信機関・ISAC・事業者の各組織の連携により、サイバー攻撃に対し全体のレジリエンスを向上させ、業種横断でサイバー攻撃に備えることができる。対象となる企業／団体としては、各種ISAC、重要インフラ事業者、脅威情報配信機関等を想定している。

https://www.hitachi-systems.com/solution/s0308/threat_share/index.html

①概要・特長

セキュリティ脅威情報やインシデントの情報共有システムをクラウド環境で提供する。

○情報共有システム

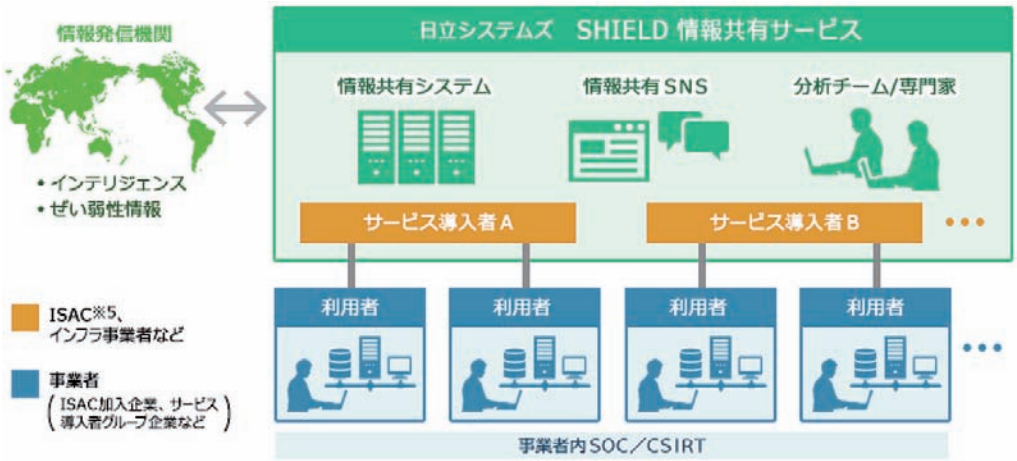
- 定型フォーマット（STIX/TAXII）にて脅威情報を受信し、利用者に配信することが可能。
- 脅威情報を蓄積し、関連性分析機能で簡易解析を行うことができる。
- 脅威情報からセキュリティ機器の設定形式に変換（YARA*4ルール）することが可能。

○組織内SNS*5

利用者間で脅威の傾向や攻撃兆候の議論、組織内での作業指示などのディスカッションを行うことができる。

○サービス提供イメージ

サービス提供イメージを、図3に示す。



■図3. SHIELD 情報共有サービス提供イメージ

*4　マルウェア解析・検知ツール。YARAルールという文字列と条件/条件演算子/正規表現などを用いてマルウェアを検出する。
*5　Social Networking Service

②機能詳細

SHIELD情報共有サービスは、以下の機能を有する。

・脅威情報の蓄積・検索

脅威情報を蓄積することにより、特定のメッセージを検索することが可能。また、過去の脅威情報を確認することにより、対策判断の時間を短縮することができる。

・脅威情報のアグリゲーション

大量の脅威情報に埋もれないように、重複情報や過去の類似脅威情報を確認することができる。脅威情報の閲覧時に重複や類似の情報が確認できるため、対策判断の時間短縮にもつながる。

・ファイルの添付、ダウンロード機能

脅威情報の新規作成時にMicrosoft Word、Excelファイルなどを添付することが可能。また、情報提供機関が添付したファイルもダウンロードして参照することができる。

・脅威情報のエクスポート

脅威情報の一覧をCSV形式でエクスポートすることができる。また、脅威情報の詳細をJSON及びCSV形式でエクスポートすることが可能で、その情報を他システムへ提供することにより、対策管理の工数低減が可能。

・機器設定支援

脅威情報からセキュリティ機器の設定形式に変換（YARAルール）することができる。YARAルールに対応したセキュリティ機器であれば、対策の適用が容易となる。

6. おわりに

重要インフラをサイバー攻撃から防御するためには、関連する重要インフラ事業者等の間で脅威やインシデント等の情報を共有し、他組織で発生した事象や兆候をいち早く共有することで第二・第三の被害を未然に防止すること、さらには、対策技術も共有して事前対処性にも優れた耐性の強いシステム運用を実現することが求められている。

これらの情報共有によって効果を上げるために、本研究開発では、異なる重要インフラ分野の事業者間で円滑に情報共有を行うための日本における情報共有の在り方の検討及び情報共有プラットフォーム技術の開発を行い、以下の課題の解決に寄与することができたと考える。

①重要インフラ事業者等に対する情報提供のインセンティブ確保

日本に加え、米国や欧州の情報提供の活性化施策を調査し、明らかにした。これらの活性化施策を参考に、情報提供を積極的に推進し、社会全体の合意とすることで、重要インフラ事業者等が情報を提供する際に、自身の信頼や評判を損なうといった心理的障壁を排除することが可能となる。

②情報の迅速な共有と活用

情報の迅速な共有と活用を行うために、サイバー脅威情報の記述・共有技術を調査し、機械処理可能な脅威情報構造化記述形式（STIX）や検知指標情報自動交換手順（TAXII）といった情報のデータ形式が有用であることを見出した。さらに、これらを実装した情報共有プラットフォームを構築し、共有すべき情報をコンピュータ処理可能な形式で交換/活用する環境を整備して実運用の中で洗練した。これにより、サイバー攻撃を検知した組織から関係する組織にいち早く情報を展開し、対策につなげられる環境を構築可能とした。

③セキュリティ対策に不足する情報の補完

欧米での大規模イベント対策事例や情報共有の事例を調査し、分野横断での情報共有が各所で始まっていること、また、組織横断的な情報共有を実現することによる直接的な効果として、事業者の得られる知見の高度化・成熟化があることを明らかにした。これらの結果から、日々発生する脅威情報の迅速な把握と、組織横断的に情報共有することで、不足している情報の補完を可能とする。

※記載された社名及び商品名は各社の商標または登録商標である。

謝辞

本研究は、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。