News Release

国立研究開発法人新エネルギー・産業技術総合開発機構
株式会社日立製作所
株式会社日立システムズ

2018.5.30

異なる組織間でサイバーセキュリティ情報を共有できる基盤を開発
―日立システムズが重要インフラ分野向けサービスとして提供開始―

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）日立製作所は（株）日立システムズと連携し、重要インフラ事業者が他の企業や組織との間でサイバーセキュリティに関する脅威情報や対策方法を共有するための情報共有基盤を開発しました。

この成果を活用し、（株）日立システムズは、複数の企業・組織間でサイバー攻撃に関する情報を効率的に共有し迅速なサイバーセキュリティ対策を実施できる「SHIELD 情報共有サービス」を、本日より提供開始します。

1. 概要

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す。しかしながら、現在、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ます。

このような背景のもと、NEDOが管理法人を務める内閣府事業において、株式会社日立製作所は株式会社日立システムズと連携し、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ています。今般、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ました。

さらに、（株）日立システムズより、本基盤を実装した「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本日より提供開始し、重要インフラ分野におけるサイバーセキュリティ対策強化に貢献します。

本研究開発は、サイバーセキュリティ強化を目的とした、内閣府事業「戦略的イノベーション創造プログラム（SIP）※1／重要インフラ※2等におけるサイバーセキュリティの確保」の取り組みの一つであり、NEDOは内閣府の指定を受けて本プロジェクトの管理法人を担っています。

2. 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す。本基盤は、

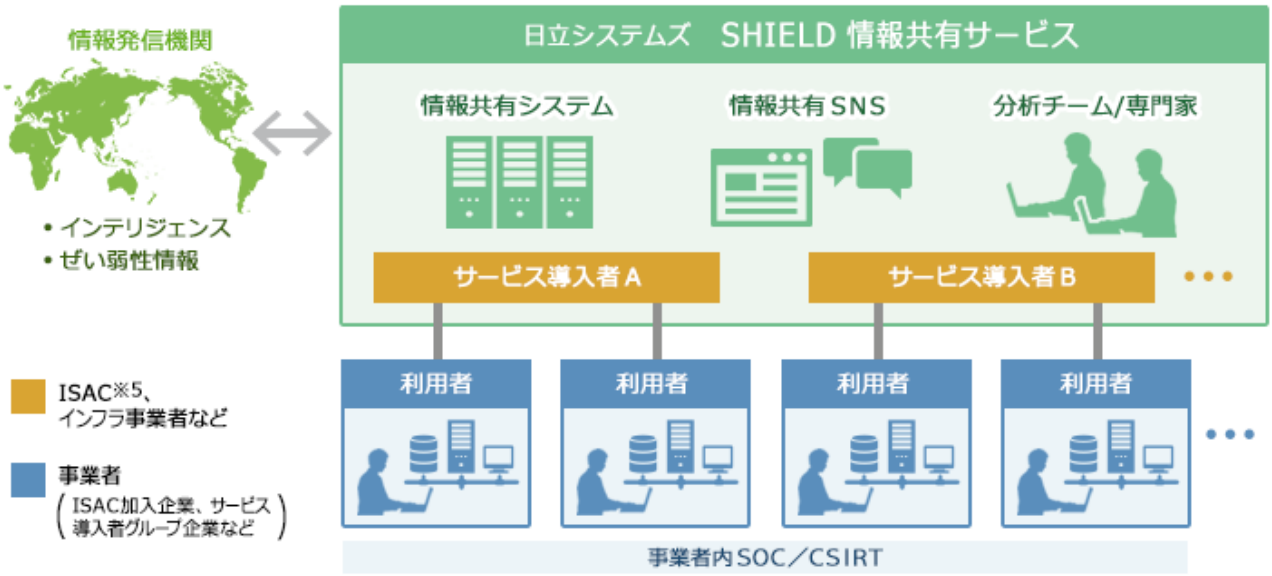
国際標準規格であるSTIX※3・TAXII※4を採用しているため、国内外の脅威情報および対策方法について、STIX・TAXIIを採用する他の情報機関から受信し、注意喚起として一斉自動配信する機能を備えています。

また基盤開発に加え、各組織に対して情報共有の仕組みを普及・定着させるため、外部の情報発信機関、業界ISAC※5、企業のCSIRT※6といった立場ごとに、脅威情報取得時の対応や役割などを明確化したグランドデザインを策定するとともに、今回開発した情報共有基盤を実際の運用環境で検証・評価し、その結果や専門家の知見を反映した運用ガイドラインを作成しました。

研究開発の成果を活用し、(株)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、本日より提供開始します。

3.「SHIELD 情報共有サービス」の特長

「SHIELD 情報共有サービス」は、国内外の公的情報発信機関(例:米国国土安全保障省が推進するサイバー攻撃脅威情報共有の枠組みであるAIS※7など)や、民間の情報発信機関から配信される情報を、STIX・TAXIIで収集・蓄積し、情報の重要度を自動でランク付けします。また、関連情報を直感的に分かるように仕分けし、グルーピングを施して提供します。本サービスを利用することにより、脅威情報や対策方法の共有を図る企業・組織は、蓄積された情報の中から過去の類似事例の検索・閲覧や、SNSのような仕組みを利用して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ます。さらに、脅威情報に関する他システムとの連携や、セキュリティ機器の設定ファイル形式への変換が可能なため、脅威情報に基づいたセキュリティ対策の実行を迅速化できます。



「SHIELD 情報共有サービス」の概要図

【注釈】

※1 戦略的イノベーション創造プログラム(SIP)

Cross-ministerial Strategic Innovation Promotion Programの略称で、内閣府の総合科学技術・イノベーション会議が自らの司令塔機能を発揮して、府省の枠や旧来の分野の枠を超えたマネジメントに主導的な役割を果たすことを通じて、科学技術イノベーションを実現するために新たに創設するプログラム。自動走行や防災分野など11の課題テーマに対し、府省・官民

分野の枠を越え、それぞれ基礎研究から実用化・事業化までを見据えた取り組みを推進している。

※2 重要インフラ

NISC（内閣サイバーセキュリティ―センター）が「重要インフラの情報セキュリティ対策に係る第3次行動計画」において定めている分野であり、「情報通信」、「金融」、「航空」、「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」および「石油」の13分野。

※3 STIX

Structured Threat Information eXpression（脅威情報構造化記述形式）の略称で、サイバー攻撃情報を表すためのフォーマット仕様。標準化された方法で記述することで、サイバー空間における脅威や攻撃の分析等に関する情報を共有可能とする。

※4 TAXII

Trusted Automated eXchange of Indicator Information（検知指標情報自動交換手順）の略称で、サイバー脅威情報を送受信するプロトコル。本プロトコルを用いることで、プログラムによるサイバー脅威情報の自動交換を可能とする。

※5 ISAC（Information Sharing and Analysis Center）

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、対策および安全性向上のために協働活動を行う民間組織。

※6 CSIRT（Computer Security Incident Response Team）

サイバーセキュリティに関する事故が発生したときに対応したり、リスクが高まった場合などに、システムやネットワークなどに問題が起きていないかなどを調査・対策する組織。

※7 AIS（Automated Indicator Sharing）

米国の国土安全保障省が運営しているサイバー攻撃の脅威情報を共有するための枠組み。米連邦政府と米国内外の民間企業・団体などとの間で、脅威情報の迅速な共有を促進する。100組織以上が加入している。

4. （株）日立システムズの「SHIELD 情報共有サービス」に関するウェブサイト

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

5. 問い合わせ先

（本ニュースリリースの内容についての問い合わせ先）

NEDO IoT 推進部 担当：山形、千代延 TEL：044-520-5211

（株）日立製作所 セキュリティに関するお問い合わせフォーム

https://www8.hitachi.co.jp/inquiry/it/security/form.jsp?q=toi04/

（株）日立システムズ CSR 本部 コーポレート・コミュニケーション部 担当：杉山

TEL：03-5435-5002 E-mail：press.we@ml.hitachi-systems.com

（その他NEDO事業についての一般的な問い合わせ先）

NEDO 広報部 担当：藤本、髙津佐、坂本 TEL：044-520-5151 E-mail：nedo_press@ml.nedo.go.jp