戦略的イノベーション創造プログラム（SIP）

【日立製作所】

3－2 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

社会実装技術

脅威情報を機械処理可能な定型フォーマットとし、迅速な配信を実現。
重要インフラ事業者のより早い防御を可能とする情報共有システムを開発。

特長

① 定型フォーマットによる迅速な配信
機械が判断可能な最新の国際標準仕様である定型フォーマット（STIX※1/TAXII※2）を採用し、システムが受信した情報を事業者へ迅速に配信可能。

② 脅威の関連情報や重要度がわかる
システムで蓄積した脅威情報を、関連性分析機能で簡易解析し、関連情報や重要度を見やすく表示。

③ セキュリティ対策の自動化を支援
脅威情報をセキュリティ機器の設定形式である「YARA※3ルール」で出力することで対策の省力化が可能。

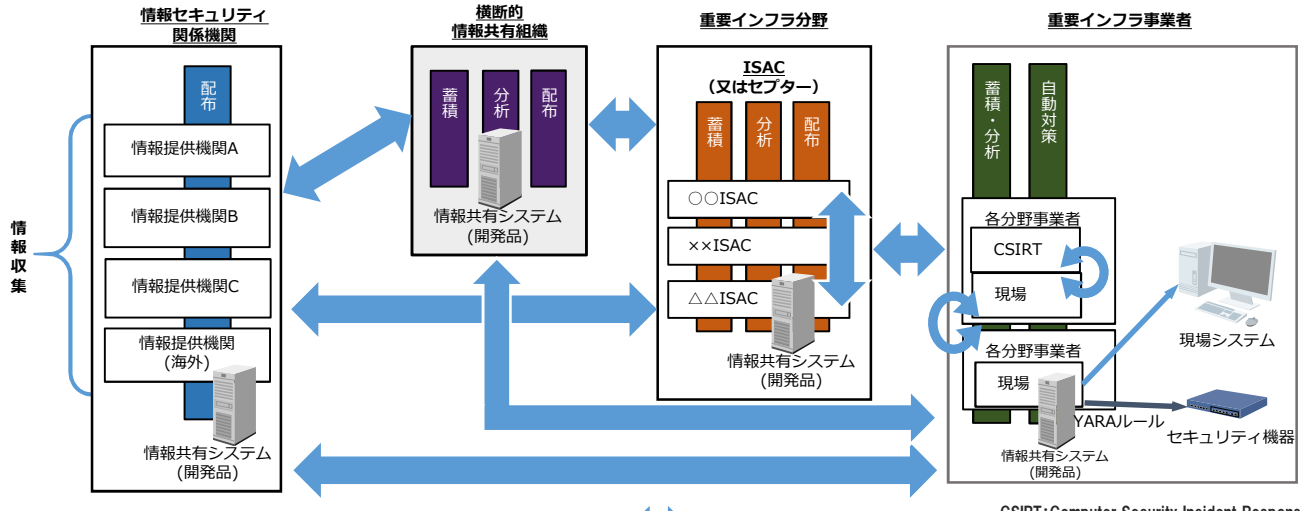
④ 導入ガイドの提供
組織の実情に応じた情報共有の構築を助ける補助ツールとしてデザインガイドを用意。

背景と目的

課題	対応
課題① 現状、メールで受信する脅威情報を、人が判断して、転送しているため、時間がかかる。	①定型フォーマットによる迅速な配信により、機械が判断するため、迅速な転送が可能となり、重要インフラ事業者は、早く対策できる。
課題② サイバー攻撃の情報を収集し、事前対策に役立てたいが、情報が多過ぎて、取捨選択に人手が必要。	②脅威の関連情報や重要度がわかることで、自組織に必要な情報の取捨選択が容易となる。
課題③ セキュリティ機器への対策設定に、手間がかかる。	③セキュリティ対策の自動化支援により機器対策の設定の人手と手間が省ける。
課題④ どのように情報共有を始めればよいかわからない。	④組織の実情にあわせた情報共有を補助ツールであるデザインガイドに沿って構築。

適用イメージ

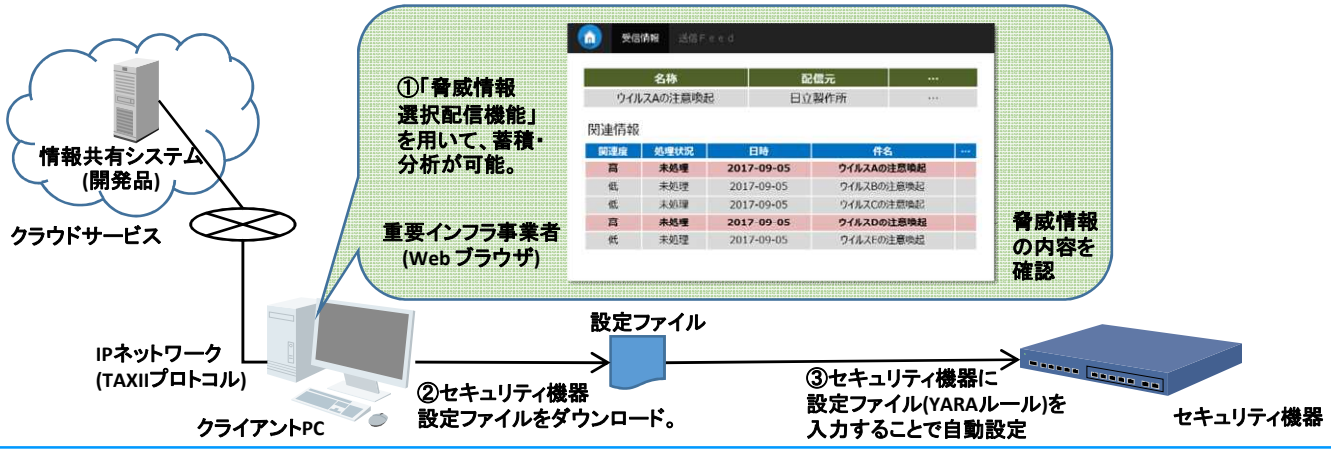
◆情報共有システムを連携して利用する仕掛けを構築することで、脅威情報の入手から配信と対策までをスピードUP。



（※1） 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。
（※2） 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。
（※3） システムのセキュリティ対策で使われるマルウェア解析・検知用ソフトウェアで、用いられる条件フォーマットセットを示す。

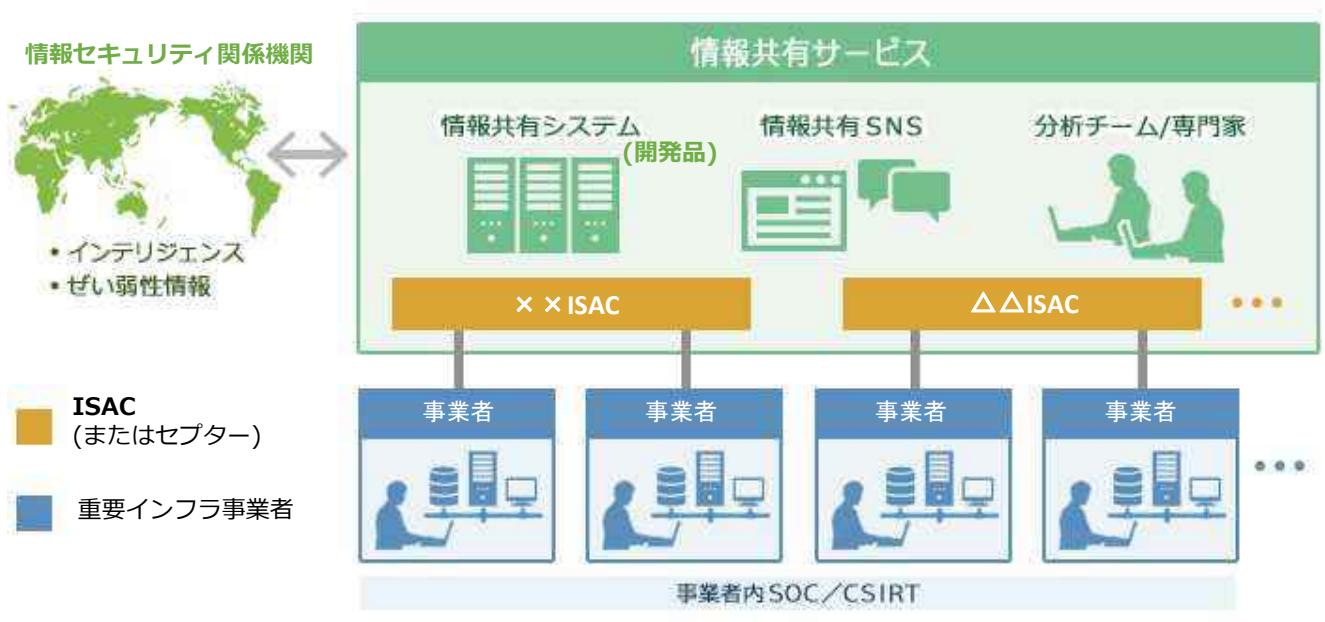
製品イメージ

◆複数のユーザーが、どこからでも情報共有システムを使えるよう、クラウド環境で提供



導入イメージ

◆情報共有システムをコアとして、国内外の情報セキュリティ関係機関から配信される情報を、STIX・TAXIIで収集・蓄積し、情報の重要度をランク付け。関連情報を直感的にわかるように仕分けし、グルーピングを施すサービスとして提供。



スケジュール

◆2017年度に情報共有システムを開発し、重要インフラ事業者等において評価検証を実施。
2018年度に、2017年度の評価検証結果を織り込んだものを実用化し、社会実装する。

◆2020年4月以降は、本格的な普及展開を図る。

2017年度	2018年度	2019年度	2020年度
評価検証	継続開発	実用化	新規機能の運用