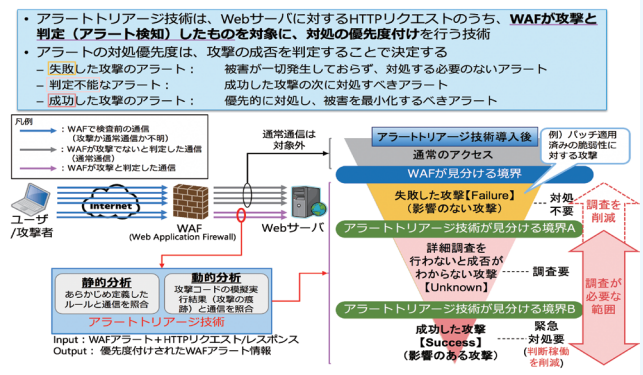
アラートトリアージ2020 技術

アラートトリアージ2020 技術について

アラートトリアージ2020 技術は、Webサーバに対する通信のうちWAFが攻撃と判定したもの（アラート）を対象に、対処の優先度付けを自動で行う技術です。

この技術は、通信に含まれる攻撃コードを疑似環境下で実行した結果＝攻撃成功時の痕跡情報を用いて攻撃の成否を判定し、アラートごとに対処の優先度付け情報を提供することで、数少ない専門家による詳細調査や緊急対応の監視業務を効率化します。

Webサービス等の外部公開サーバに対するサイバー攻撃への監視・調査・対策を実施する際に、本技術を導入することで、ICT機器利用やエネルギー利用の削減、監視稼働の削減に伴う環境負荷の低減が期待されます。



研究開発の概要

環境貢献度評価

●評価条件

本研究開発成果は、Webサーバに対する通信のうちWAF（Web Application Firewall）が攻撃と判定したもの（アラート）を対象に、対処の優先度付けを自動で行う技術です。

本技術により、通信に含まれる攻撃コードを疑似環境下で実行した結果＝攻撃成功時の痕跡情報を用いて攻撃の成否を判定し、アラートごとに対処の優先度付け情報を提供することで、数少ない専門家による詳細調査や緊急対応の監視業務を効率化することが可能になり、Webサービス等の外部公開サーバに対するサイバー攻撃への監視・調査・対策を実施する上で、ICT機器利用やエネルギー利用の削減、監視稼働の削減に伴う環境負荷の低減が期待できます。

評価は、攻撃を検知するWAFを用いた監視対策を行う際に、対処の必要性の調査を、専門家の人手のみで実施する場合と、開発技術を用いて、各アラートに対する攻撃の痕跡を調査し、攻撃の成否を判断し、対処の優先度判定を自動で行う場合でのライフサイクルにおけるCO_2排出量を比較することで、開発技術の環境貢献度を定量化しました。

【評価条件】

WAF機能により検出された、年間で27万6千件分のアラートの調査・分析を行い、対策の検討が必要かどうかを判定する。

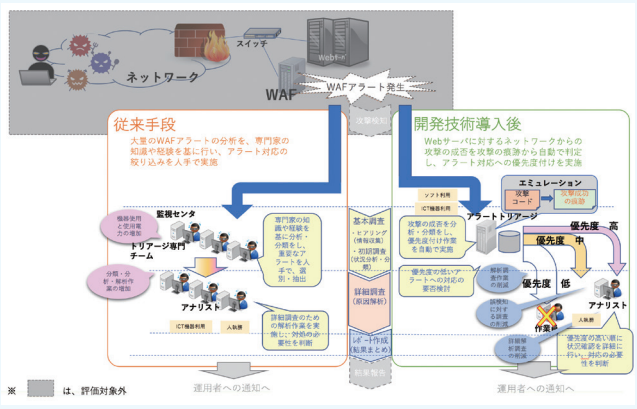
・従来手段：専門家の人手による調査を実施

・開発技術：攻撃コードを疑似環境下で実行し生成した結果を用いて、アラートトリアージを自動で行い、詳細調査の必要性を判定し、専門家による調査を実施

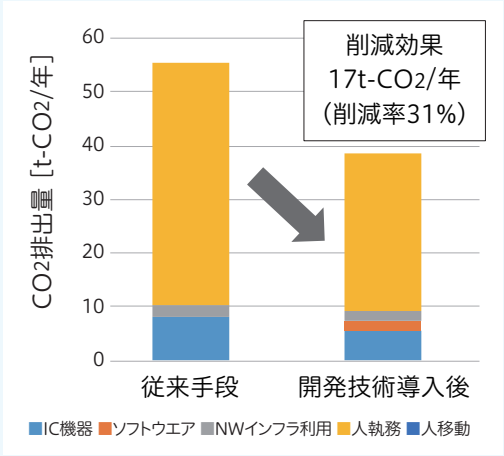
●評価結果

本技術による環境貢献度は、1年あたり約17t-CO_2（削減率：31%）でした。

主な削減要因は、開発技術を用いることで、専門家の人手による詳細調査とその必要性を判断する基本調査の稼働削減、さらには調査時に利用するICT機器の削減ができることであり、人執務、及びICT機器利用による負荷削減です。



評価モデル



評価結果グラフ