Managed Security & IoT Security

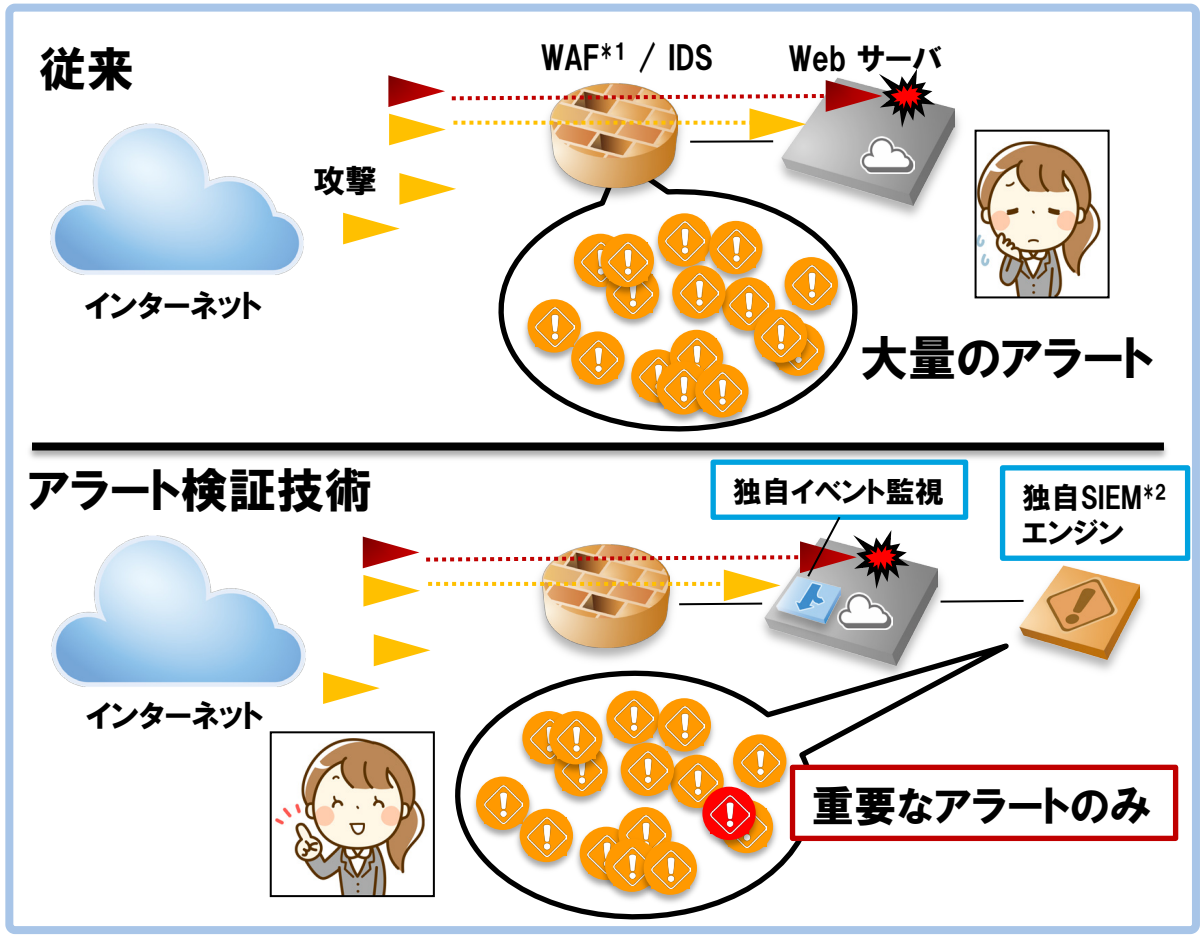
C－20

Webアプリケーションセキュリティの先進的な「アラート検証技術」

大量のアラートから「ささる」サイバー攻撃を特定します

NTT R&D FORUM 2017

Webアプリケーションの脆弱性を狙ったサイバー攻撃は日常的に発生しており、従来の対策であるWAF*1は大量のアラートを出力してしまうため、運用者は影響の特定に追われています。本展示は、それらの中から真に悪影響を与える「ささる」サイバー攻撃を特定します。無害なアラートへの調査や対応を削減することで、インシデント対応の劇的な効率化を実現します。



特　徴

- WAFの攻撃アラートとシステム内部のイベントログの相関分析により、「ささる」攻撃のアラートを正確に特定
- 攻撃アラート発生後、「ささる」攻撃かどうかが即座に判明
- 必要な情報を自動的に学習して分析を行うため、運用中のシグネチャの管理は不要
- 「ささる」攻撃の影響によって発生したシステム内部のイベントも含めた、インシデントの全貌を可視化

利用シーン

- Webサービス事業者：自社Webサービスへの攻撃の監視・防衛
- クラウドサービス事業者：クラウド基盤への組み込みによる、顧客の仮想マシン保護
- マネージドセキュリティサービス事業者：WAF運用サービスとの連携による、アラートへの対応の効率化

*1 WAF（Web Application Firewall）：Webアプリケーションの脆弱性を悪用した攻撃などからWebアプリケーションを保護するシステム
*2 SIEM（Security Information and Event Management）：ネットワーク機器、サーバなどからログを収集し、それらを分析して異常を検知し、管理者に通知するシステム

Innovative R&D by NTT

〈問い合わせ先〉sv-forum@lab.ntt.co.jp