News Release

2016 年 1 月 28 日

「WideAngle」の人工知能（機械学習）基盤を大幅強化

～お客さま企業のセキュリティ脅威レベルの自動判定機能と脅威対策の情報連携機能を追加～

NTT コミュニケーションズ株式会社（略称：NTT Com）は、2016 年 2 月 10 日より、総合リスクマネジメントサービス「WideAngle」のマネージドセキュリティサービス運用基盤（SIEM）において、お客さま企業の IPS/IDS/FW/Proxy サーバーなどの IT 機器から取得したエンドポイント情報を活用し、セキュリティ脅威レベルを自動判定する機能、および情報漏洩の重篤度に応じた最適なセキュリティ対策を迅速に情報連携[*1] する機能を独自に開発・実装し、企業 ICT 環境へのサイバー攻撃に対する人工知能（機械学習）の検知・分析力を大幅に強化します。

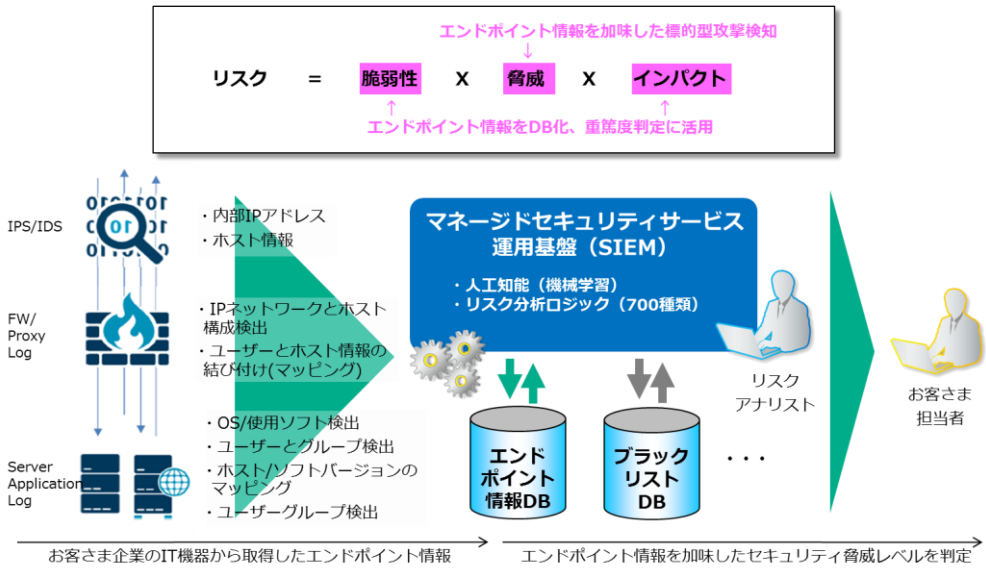
1．背景

企業の機密情報などを詐取する標的型攻撃をはじめとするサイバー攻撃は巧妙化、増加の一途をたどり、セキュリティ監視・分析業務の精度向上と迅速化が求められています。

こうした中、NTT Com では、2015 年 10 月より、リスクアナリストの分析業務を支援する人工知能（機械学習）による分析機能を独自開発し、マネージドセキュリティサービスの運用基盤（SIEM）への実装を進めてきました。

2．概要

2015 年 10 月に実装した、未知の悪性サイトを経由した攻撃者との不正通信を自動検知する機能に加えて、2016 年 2 月 10 日より、WideAngle の人工知能基盤へ 2 つの機能を実装し、高度なサイバー攻撃の検知率をさらに高めます。これにより、攻撃を受けた場合の報告内容の高度化や対応の迅速化を実現し、情報漏えいリスクを大幅に低減します。



NTT コミュニケーションズ株式会社　広報室
NTT Communications Corporation　Public Relations Office
〒100-8019　東京都千代田区内幸町 1-1-6
1-1-6 Uchisaiwai-cho, Chiyoda-ku, Tokyo 100-8019, Japan
Tel (03)6700-4010 International +81 3 6700 4010

（1）お客さま企業の IT 機器から取得したエンドポイント情報から、セキュリティ脅威レベルを自動判定

お客さま企業の ICT 環境に設置した通信機器の生成するログやトラフィックデータから、IP アドレス・ポート番号・ホスト情報などのエンドポイント情報に加えて、セッション情報なども分析することで、ネットワーク構成・ホスト種別・OS・ソフト情報などを加味し、セキュリティ脅威レベルを自動判定する機能を開発・実装します。リアルタイムに流れるトラフィックデータなどから自動判定するため、お客さま企業によるネットワークやシステム構成変更の際にも迅速・柔軟に対応可能です。

（2）情報漏洩の重篤度に対する最適なセキュリティ対策を即時情報連携

お客さま企業の IT 機器から取得した情報から自動判定したセキュリティリスクレベルを基に、対応不要な偽陽性アラートを自動判定・排除した上で、推奨対処法を即時情報連携する機能を開発・実装します。これにより、情報漏洩の重篤度に応じた最適な対処法を、リスクアナリストが迅速に判断し、お客さま企業に通知することが可能です。

3. 今後の予定

NTT Com では、引き続き、セキュリティ分析の精度向上、効率化や自動化を推進するため、人工知能（機械学習）に関わる研究・開発を実施していきます。通信ログなどから振る舞いの特徴を学習することにより、従来のセキュリティ対策製品では検知が難しいマルウェアの亜種や類似攻撃コードを検出する機能や、平常時の通信状況を分析し、異常通信が発生した場合、迅速に自動検知する機能（2016 年度第 2 四半期予定）、さらにそれらを進化させ、SD-WAN・IoT 関連ネットワークへの攻撃や脅威を検知する機能（2017 年予定）の開発に取り組みます。

*1: 情報連携のインターフェイスは、インテリジェンスを広く共有できるように、業界最先端の標準フレームワークを採用しています。各標準フレームワークは以下の通り。

- CybOX（Cyber Observable eXpression/サイバー攻撃観測記述形式）：サイバー攻撃の観測を記述する形式で、コンピュータとネットワークのアクティビティ、およびエンティティにおいて観測可能な属性の記述方法を規定します。
- STIX（Structured Threat Information eXpression/脅威情報構造化記述形式）：脅威情報アイテムと脅威のコンテキストの詳細を記述し、脅威情報を構造化するための XML ベースの標準言語です。なお、本 STIX 構文を記述するための言語の一つとして上述の CybOX を使用します。この標準化によりセキュリティの研究者や現場の実践者は、誤認のリスクを著しく下げながら脅威情報を交換することができ、その結果、特定の形式で脅威情報アイテムを自動処理することが可能となります。
- TAXII（Trusted Automated eXchange of Indicator Information/検知指標情報自動交換手順）：脅威情報のセキュアな転送と交換を提供する技術仕様です。