News Release

2014 年 6 月 18 日
NTT コミュニケーションズ株式会社
NTT Com Security AG

「WideAngle マネージドセキュリティサービス」の 総合ログ分析・リスク検知機能を強化し検知率を大幅に向上

～標的型攻撃を含む未知のセキュリティ脅威に対する検知率 500%向上を実現～

NTT コミュニケーションズ（略称：NTT Com）は、WideAngle マネージドセキュリティサービスのセキュリティ運用基盤において、お客さまの各種 ICT 機器から収集したログを分析する SIEM*1 エンジン（別紙 1）を強化し、セキュリティ脅威に対する検知率を大幅に向上させたサービスの提供を、2014 年 6 月より開始します。

今回の機能強化では、セキュリティ脅威の分析を担う SIEM エンジンにおいて、ログ収集対象機器の拡張や、大量のログを相関分析・自動検知するロジックを 300 種以上に拡充することにより、標準型攻撃を含む、未知のセキュリティ脅威の検知率 500%向上*2 を実現しました。

1. 背景

新種のウィルスが蔓延し、巧妙な手口による不正アクセスなどのセキュリティリスクが増加するなか、企業が機密情報や顧客情報を守るためには、未知のサイバー攻撃により万が一侵入されたとしてもそれらを検知し、情報漏えいを水際で防ぐことができる情報セキュリティ対策が必要不可欠となっています。（別紙 2）

こうした中、NTT Com は、企業の情報セキュリティ運用を担う「WideAngle マネージドセキュリティサービス（MSS）」の完全自社開発である SIEM エンジンをバージョンアップすることにより、巧妙化するセキュリティ脅威に対する検知率を大幅に向上させました。

2.概要

WideAngle マネージドセキュリティサービスは、ファイヤーウォール（FW）・侵入防御装置（IPS）・アンチウィルスソフトウェアなどのセキュリティ機器によって実現している発見済みウィルスや過去にあった攻撃とパターンマッチングする分析に加えて、これら複数のセキュリティ機器から生成されるログと、Web サーバー・認証サーバー・Web プロキシーサーバー・データベースサーバー・ネットワーク機器などの非セキュリティ機器から生成される膨大なログを相関分析することで、未知の脅威も含めた高精度の検知機能を有しています。

今回、この検知機能・検知スピードの更なる向上のため、リスクアナリストの知見を相関分析ロジックとして 300 種以上に拡充、SIEM エンジンへ組み込むことで自動分析機能を大幅に改善しました。また、リスクアナリストの詳細分析をアシストする機能も強化し、検知漏れや

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

誤検知・脅威の見逃しを改善、標的型攻撃を含む未知のセキュリティ脅威に対して、検知率 500%向上を実現するともに重篤度をランク化し対応優先度をわかりやすくしました。

(1) 多角的な分析ロジックの追加（別紙 3）

標的型攻撃では、サーバーなどの新たな脆弱性を突いて攻撃を開始し、攻撃者の設置したサーバーから攻撃用のマルウェアをダウンロードして PC やサーバーを感染させ、その後感染機器を拡大したり、重要データへのアクセスを試みたりする連続的な攻撃行動「キルチェーン」が見られます。FW や IPS/IDS などのセキュリティ機器向けの分析ロジックに加え、そのような攻撃ステップを解析する「キルチェーン検知」などのロジックを追加することにより、情報漏洩前に遮断することが可能となります。

また、他サイトから漏洩した ID とパスワードの組み合わせを同一の IP アドレスから大量に試行する「リスト型攻撃」は、従来、既存のセキュリティ機器では検知することが困難でしたが、数時間単位の長い期間での攻撃状況をスコア化し、不審な動作を検知したり、攻撃の段階、被害範囲、感染源となる攻撃者の IP アドレス、感染が確実となった PC やサーバーを即時特定する「ブースト（傾向分析）」などのロジックを追加することにより、その後の攻撃の遮断、早期対応が可能となります。

(2) 3 種類の時系列分析の改良（別紙 4）

機器の通信や動作ログを即時解析する「リアルタイム検知」や過去のログを一定期間経過後に分析する「バッチ処理検知」に加え、攻撃された疑いのあるログを基に、以後発生する関連ログを継続的に分析する「スライディングウィンドウ処理検知」など、過去・現在・未来の一連の流れに着眼したアプローチにより、分析ロジックを改良します。

本改良により、分散させた攻撃箇所からの攻撃や、なりすましによるログインなど時間軸とロケーションなどの複合的な分析による、脅威の早期検知、対応が可能となります。

(3) セキュリティ検知対象機器の拡充

WideAngle プラットフォームにてセキュリティ監視・分析可能な機器ラインナップを 8 社/66 機種に拡大し、より多くのお客さまへ「WideAngle マネージドセキュリティサービス」の提供が可能になります。

3. 料金

既存の「WideAngle マネージドセキュリティサービス」をご利用のお客さまについて、本バージョンアップに伴う、料金変更はございません。

※本バージョンアップ機能を効果的にご利用いただくには、非セキュリティ機器との相関分析サービス（CLA）をご契約いただくことをお勧めします。

4. 提供開始日

2014 年 6 月提供開始

5. 今後の展開

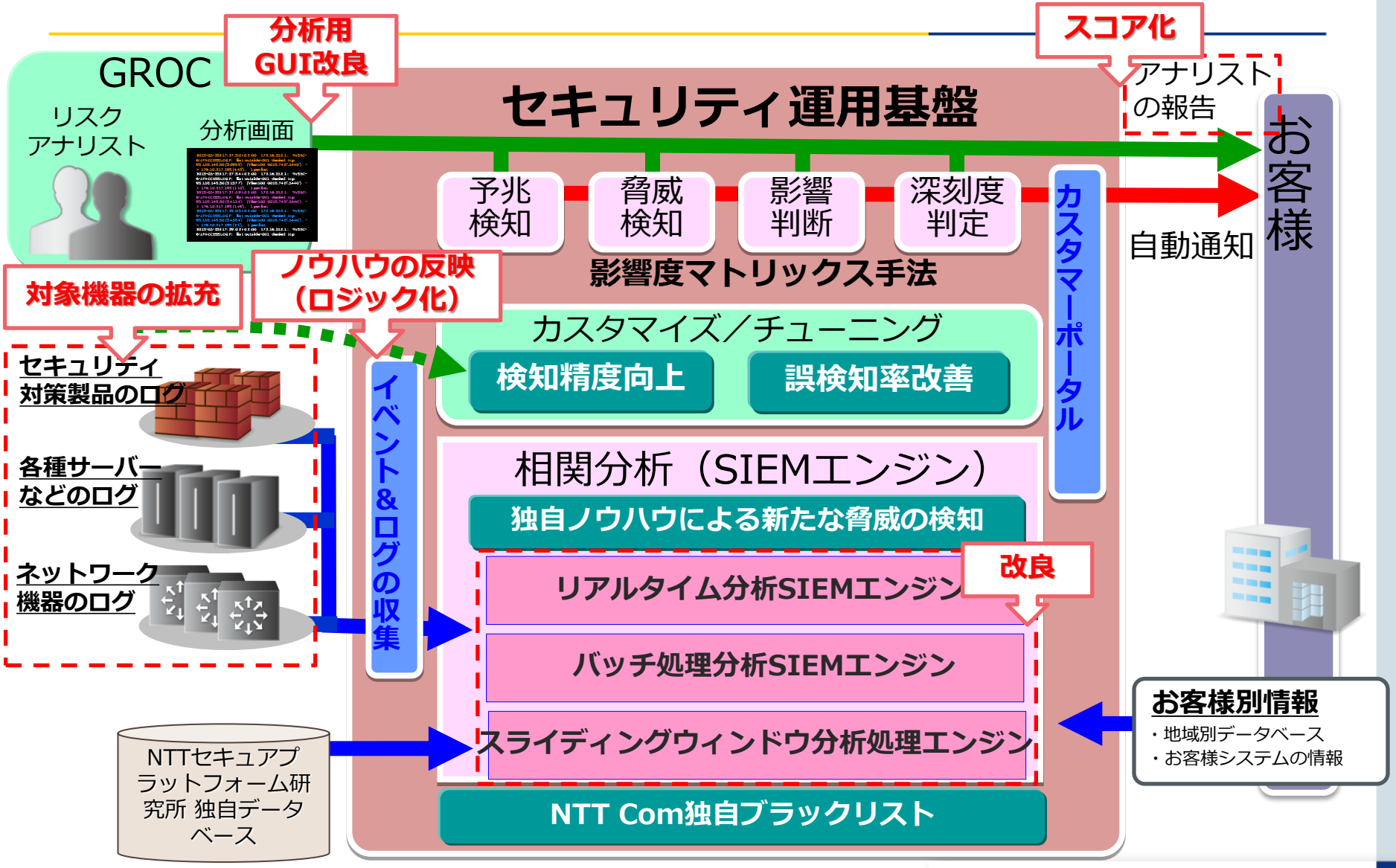
「WideAngle マネージドセキュリティサービス（MSS）」のセキュリティ運用基盤における SIEM エンジンバージョンアップだけではなく、セキュリティ分析ログをお客さま企業内で保管したまま、NTT Com にてセキュリティ脅威に対する分析ができるようにしたオンプレミス張出型ログ処理・SIEM 処理装置（Mini-PoD*3）の提供（2014 年 7 月予定）、自動脅威通知レポートの重要度に基づく発出や内容の詳細化、分析可能な対象設備の拡大、個別のお客さま向けの検知ロジック投入、リスクアナリストの分析業務で得たノウハウを検知ロジックとして SIEM エンジンに定期的に取り込むなど、継続的な最適化と機能拡充に努めていきます。

*1：Security Information and Event Management（セキュリティ関連の各種情報の管理、相関分析）の略称。

*2：当社比。

*3：Production On Demand（パッケージ化したセキュリティ運用基盤）の略称。

【別紙１】WideAngle MSS セキュリティ運用基盤



【別紙2】サイバー攻撃対策における4フェーズ

巧妙化するサイバー攻撃では、あらゆる事前対策を講じた上でも完全に防ぐことのできない「侵入ありき」を前提とした対策強化（②以降）が重要です。

【サイバー攻撃対策4フェーズ】

WIDE ANGLE
INFORMATION SECURITY AND RISK MANAGEMENT

①準備

侵入されないよう備える

②検知・分析

侵入されてもすぐに察知できる

③根絶・復旧・封じ込め

侵入された場合の被害を最小限に、すぐビジネスを復旧させる

④インシデント発生後の対応

再発防止と最終水際対策を考える

プロフェッショナルサービス

・コンサルティング　・脆弱性診断

セキュリティ対策機器/ソフトウェアの導入サービス

マネージドセキュリティサービス

・NWセキュリティ
・コンテンツセキュリティ
・VMセキュリティ
・脆弱性マネジメント
・プロファイリング
・リアルタイムマルウェア検知
・**CLA**

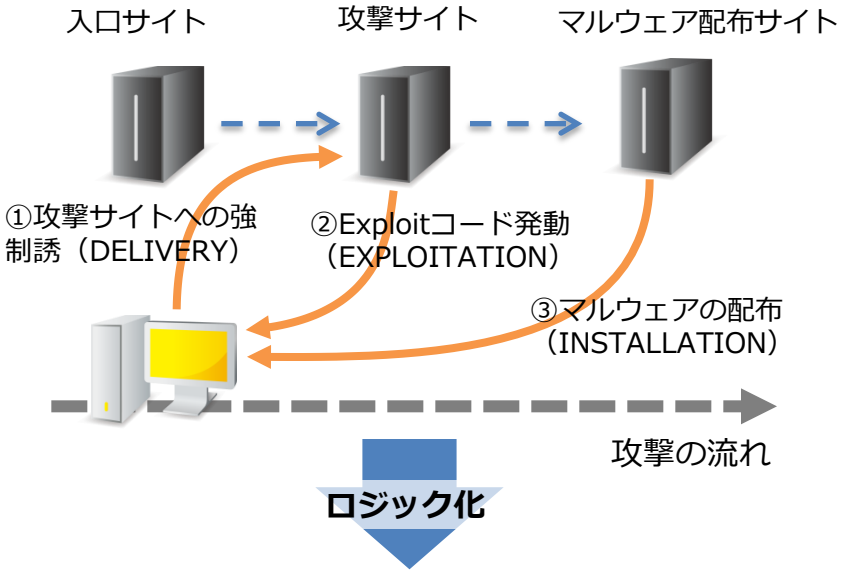
NTT Communications　Global ICT Partner
Innovative. Reliable. Seamless.

【別紙３】分析ロジック例

30年以上のセキュリティログの分析ノウハウに基づき、様々な独自の分析ロジックを開発し、SIEMに搭載しています。代表例として、標的型攻撃等で用いられる手法（キルチェーン）の検知ロジック、及び攻撃検知を避けるために時間をかけた攻撃を検知するロジックを示します。

＜キルチェーン＞

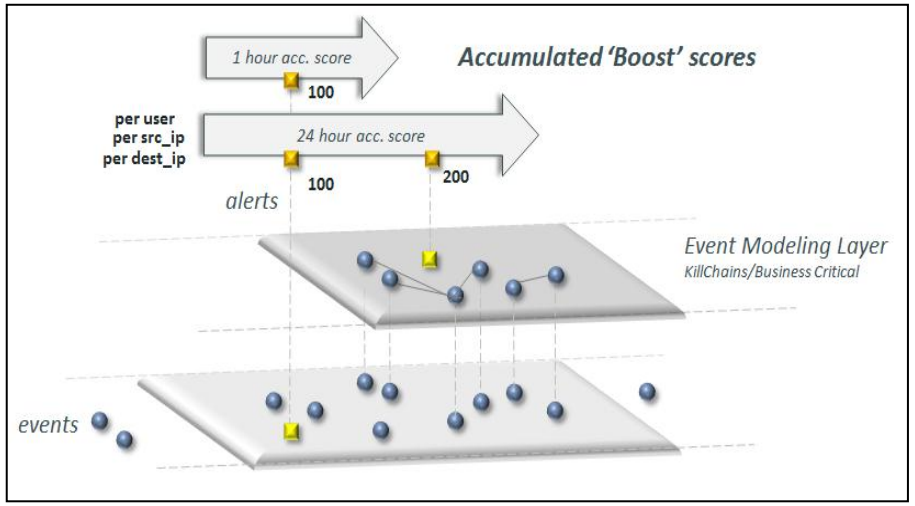
- 攻撃プロセスを解析し、その流れをロジック化することで、一つのイベントで判断するのではなく、複数のイベントの発生パターンをベースに不審な振る舞いを発見




```
KillChainEvent(kcstate=KillChainState.DELIVERY)
KillChainEvent(kcstate=KillChainState.EXPLOITATION)
KillChainEvent(kcstate=KillChainState.INSTALLATION)
```

＜ブースト（傾向分析）＞

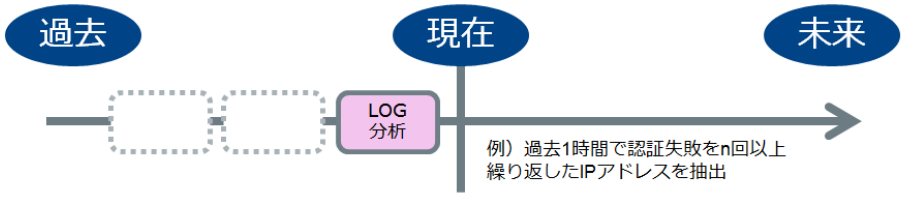
- 分析エンジンに含まれる様々なアルゴリズムによる検知に対し、さらにスコアを付け、数時間という長いスパンでの積算を行い、瞬間的な検知では発見できない不審な挙動を検出



【別紙 4】 3 種類の時系列分析の概要

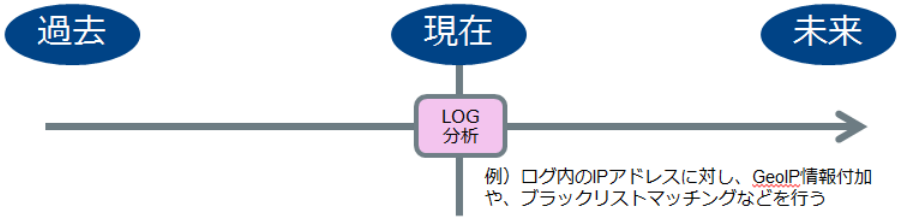
時間軸を踏まえた複数の時系列分析により様々な攻撃の検知に対応します。

①バッチ処理：定期的に過去のログを分析処理



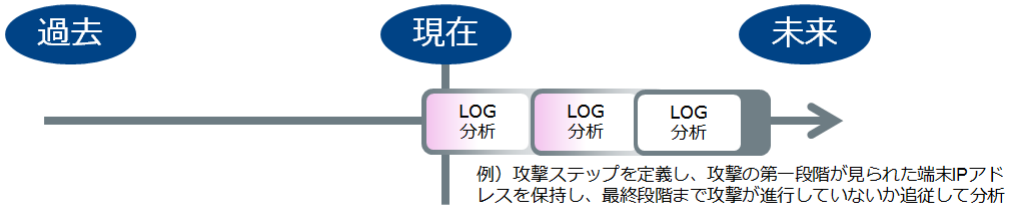
バッチ分析エンジンは，一定期間のログデータを取込み，時系列の中で攻撃もしくは攻撃の予兆と思われるものを検知します。例えば，一定時間内に特定国との接続を繰り返しているパターン，一定のデータ量通信を繰り返しているパターン等を自動検知しています。これにより，ある「過去」時点でのリアルタイム検知をかいくぐった，時間をおいて「未来」に活動するタイプの攻撃を検出します。

②リアルタイム処理：複数装置からのログに対し相関性を分析処理



リアルタイム分析エンジンは，機器のログデータをリアルタイムで取込み，独自に開発したシグネチャならびにルール(ロジック)を適用することにより「現在」発生している脅威を検知します。例えば，データ転送のないコネクション，ブラックリスト登録先への TCP/UDP コネクション等の検出や，オフィス時間外のサーバログイン，複数回のログイン試行等を自動検知しています。これはセキュリティ機器の検知を非セキュリティ機器のログ及び独自の知見により補完し，リスクアナリストによる検証を支援します。

③スライディングウィンドウ処理：特定ログをトリガーに分析を開始/追従



スライディングウィンドウ分析エンジンは、典型的な攻撃パターンの一部が見られたログを基に、特定 PC やサーバーの動作を継続的に追跡調査し、攻撃の進展を検知します。