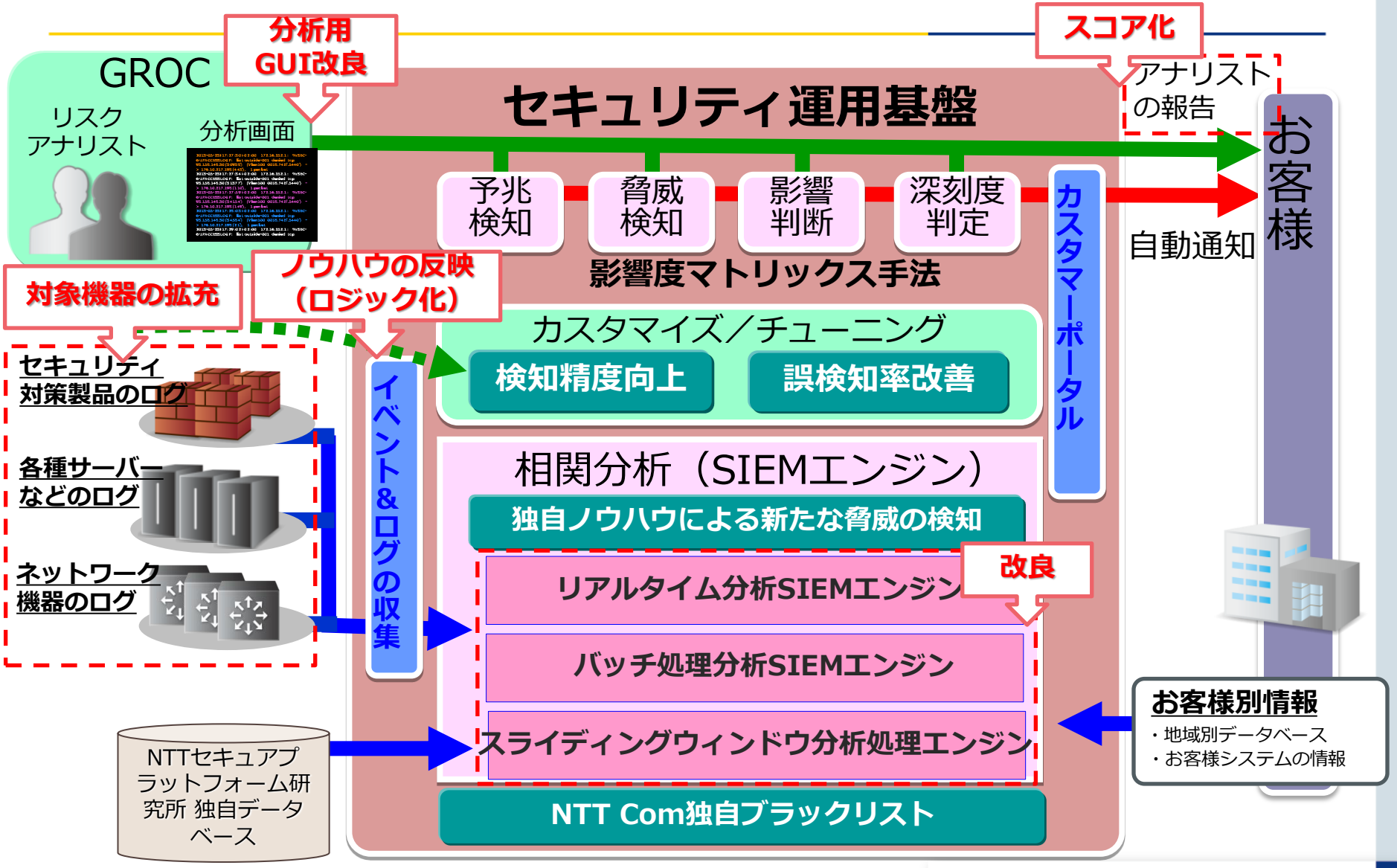
# 【別紙１】WideAngle MSS セキュリティ運用基盤



# 【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**

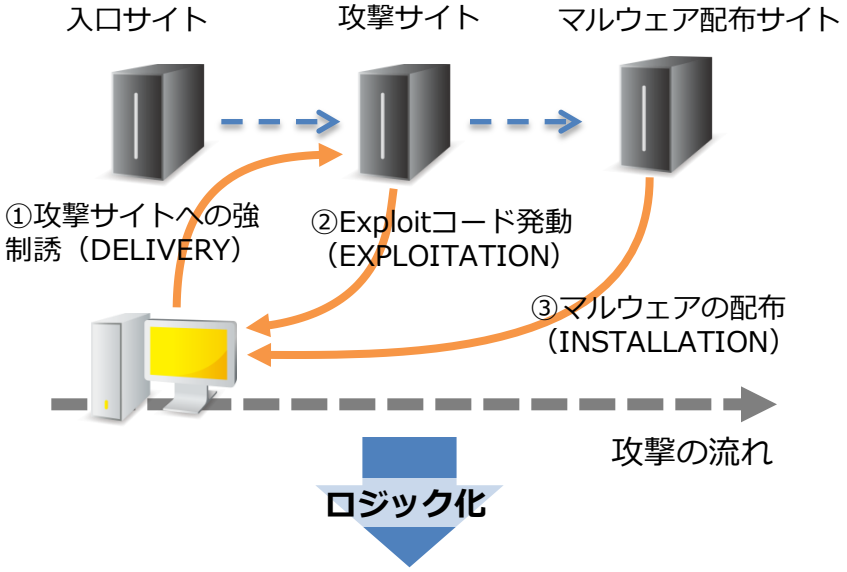
NTT Communications　Global ICT Partner
Innovative. Reliable. Seamless.

# 【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