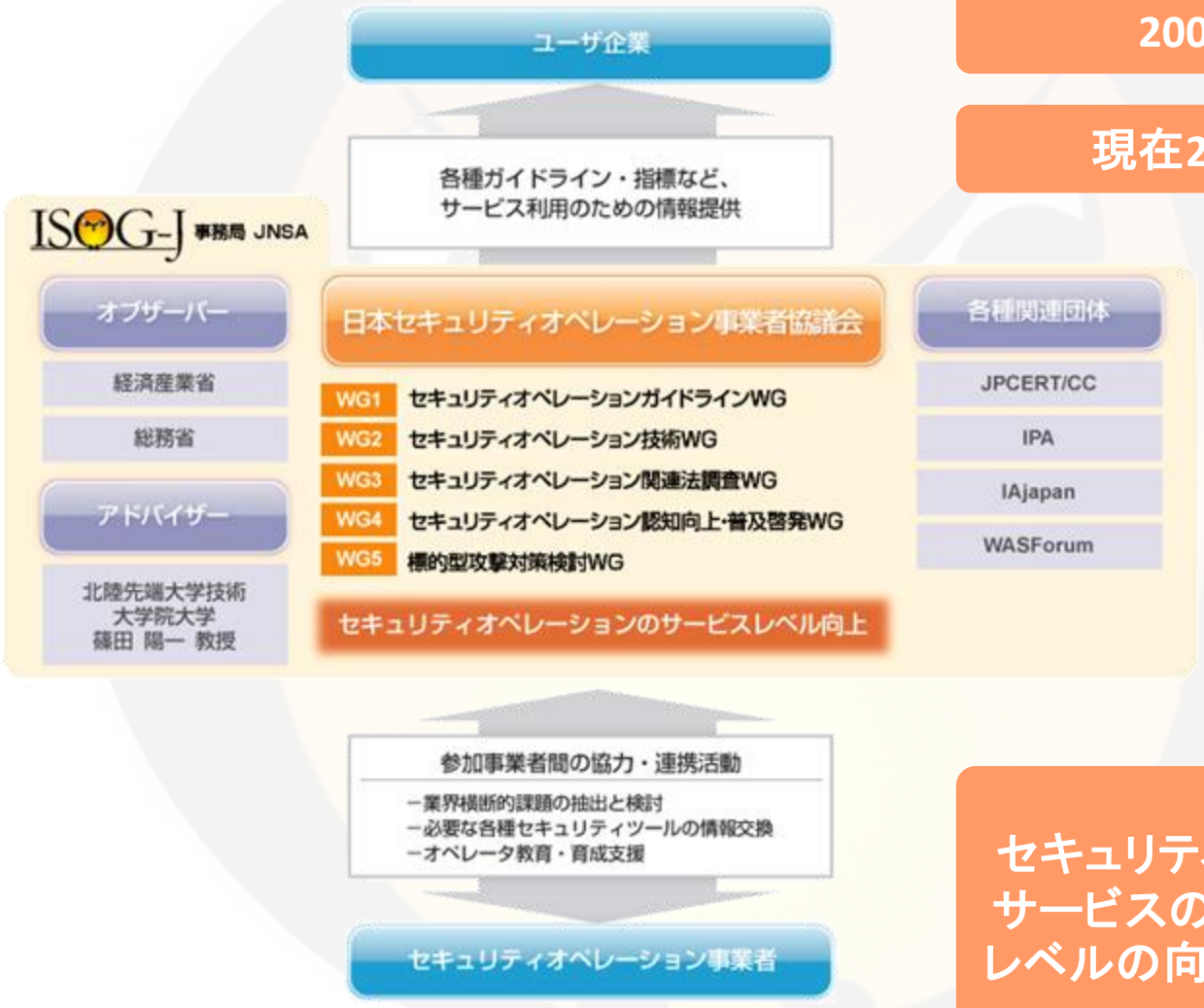
SOCから見たインシデントレスポンス

日本セキュリティオペレーション事業者協議会(ISOG-J)
NTTコムセキュリティ株式会社
阿部　慎司

ISOG-Jとは？



2008年発足

現在27社が参加

**セキュリティオペレーション
サービスの普及とサービス
レベルの向上を目的に活動**

© 2014 日本セキュリティオペレーション事業者協議会（ISOG-J） & NTTコムセキュリティ株式会社

SOCとは？

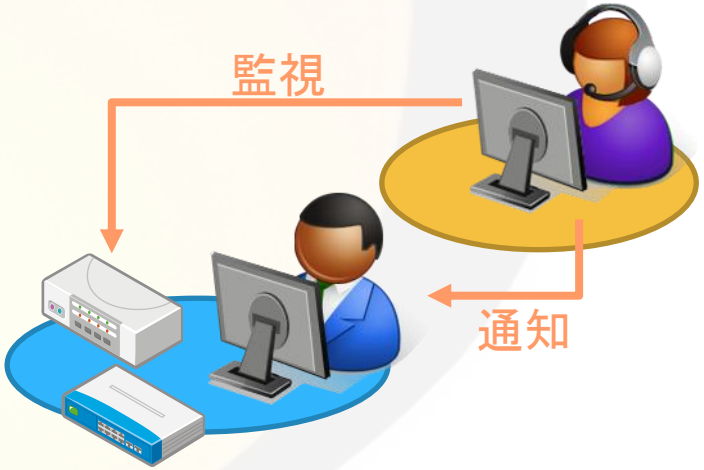
セキュリティに関する高度な知識・スキルを有し、様々な経験を持つ技術者が、セキュリティ機器を **24 時間 365 日の体制**で運用する組織

SOCのタイプは大きく2つ

内部（プライベート）SOC

セキュリティ機器の監視/運用を
全て自社内で実施するタイプ

外部SOC

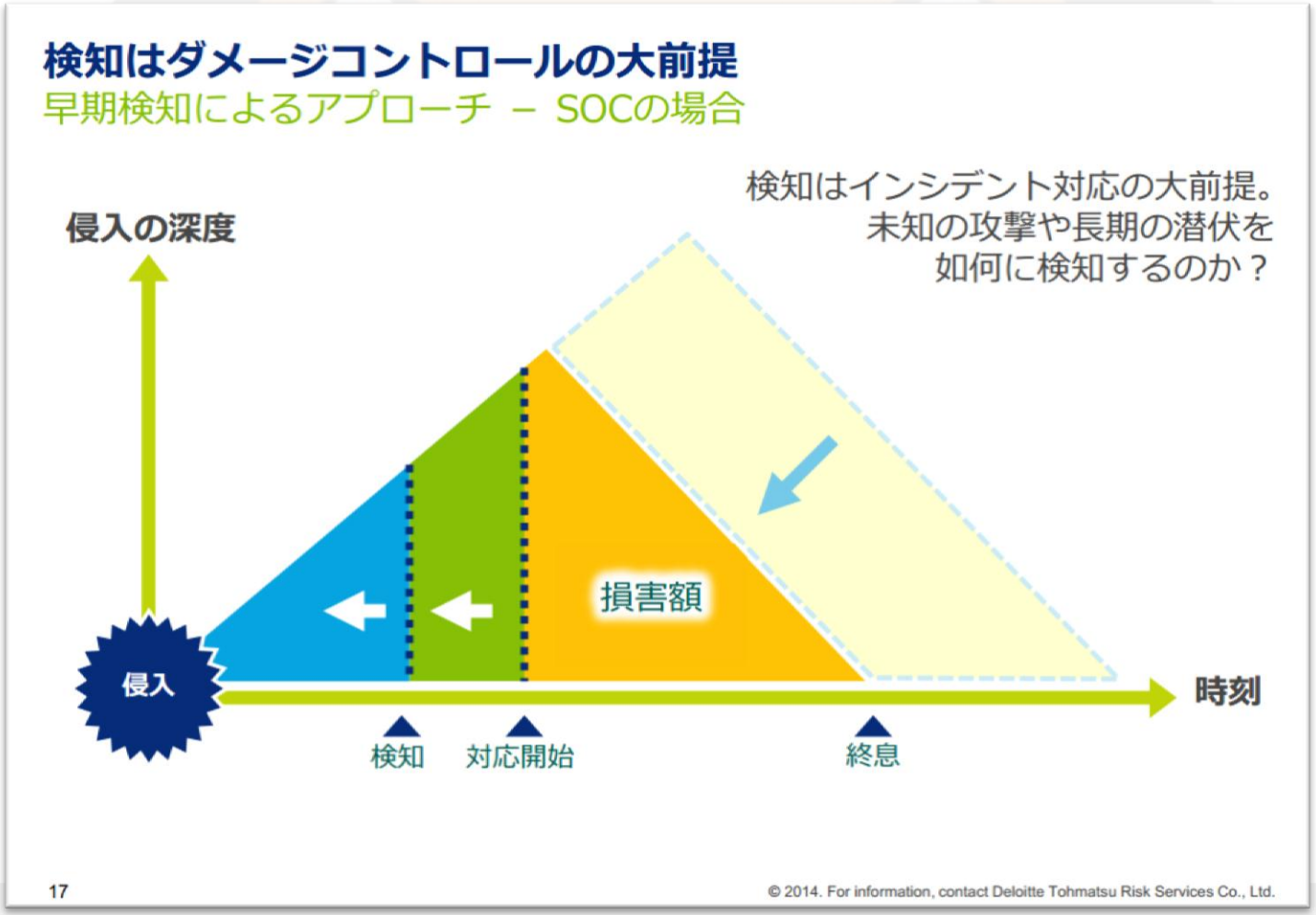


セキュリティ機器の監視/運用を
アウトソースで実施するタイプ

© 2014 日本セキュリティオペレーション事業者協議会（ISOG-J） & NTTコムセキュリティ株式会社

インシデントレスポンスにおいてSOCが担うべき役割

発見（検知）の早期化と精度向上



© 2014 日本セキュリティオペレーション事業者協議会（ISOG-J） & NTTコムセキュリティ株式会社

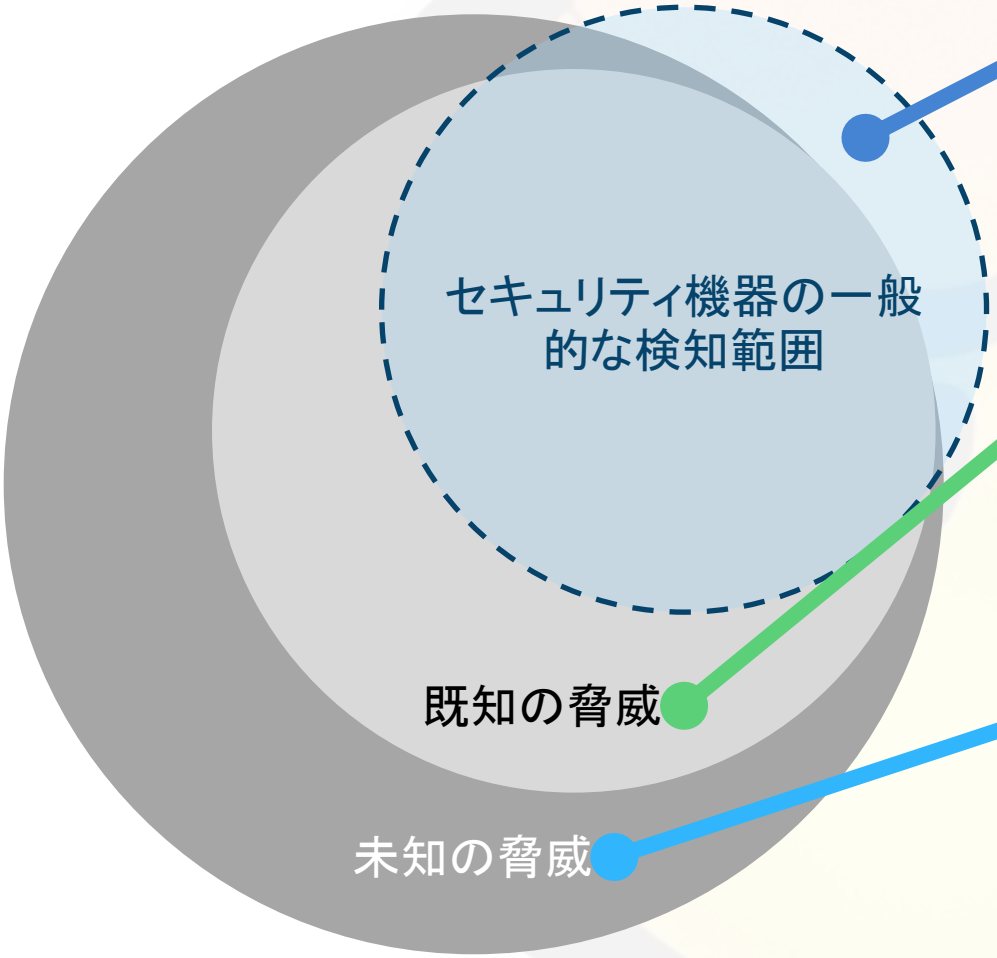
SOCがインシデントレスポンスにおいて直面する3大問題

オオカミ少年

見逃し

気付けない

© 2014 日本セキュリティオペレーション事業者協議会（ISOG-J） & NTTコムセキュリティ株式会社



オオカミ少年

誤検知が多くなると、不要な通知が増え、そのうち誰も信じてくれなくなる問題。

見逃し

セキュリティ機器のログを活用しきれず、脅威を見逃してしまう問題。

気付けない

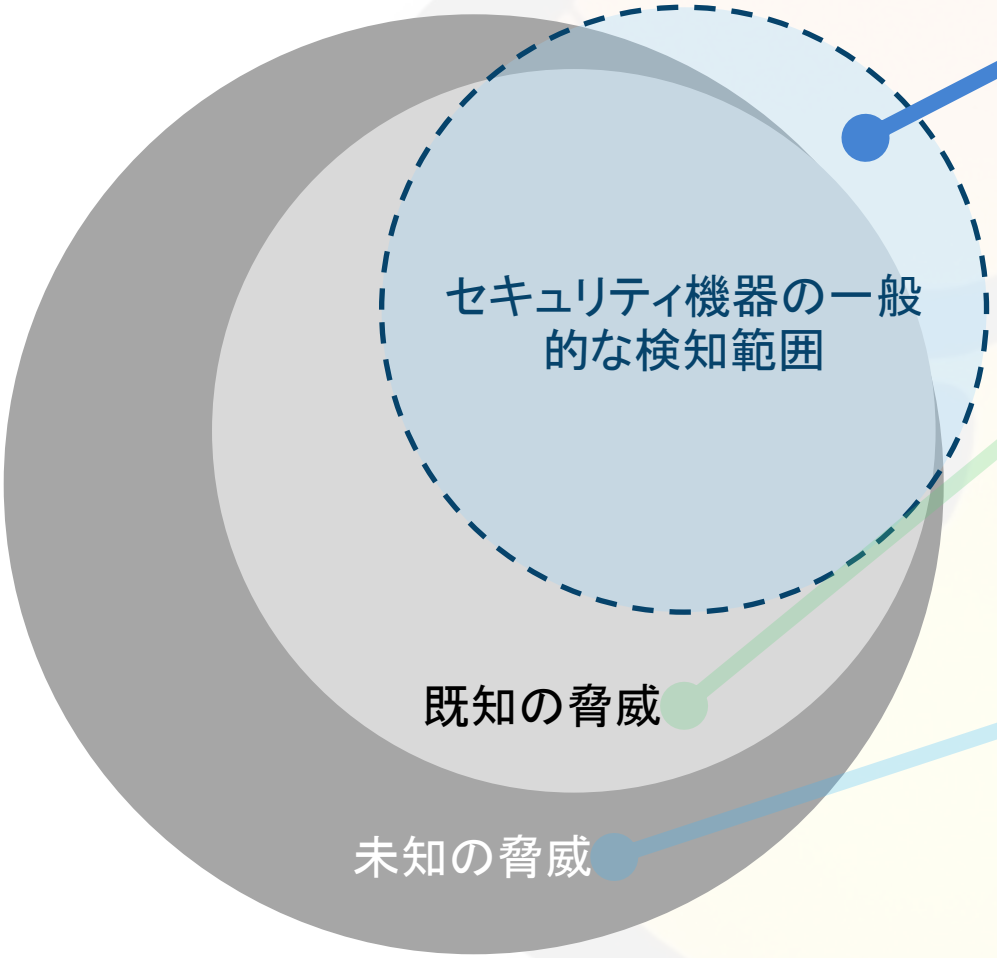
従来型のセキュリティ機器だけではゼロデイ攻撃や未知のウイルスに全く気付くことができない問題。

© 2014 日本セキュリティオペレーション事業者協議会（ISOG-J） & NTTコムセキュリティ株式会社

我々はどう解決しているか

5つの武器で戦う

© 2014 日本セキュリティオペレーション事業者協議会（ISOG-J） & NTTコムセキュリティ株式会社



オオカミ少年

誤検知が多くなると、不要な通知が増え、そのうち誰も信じてくれなくなる問題。

見逃し

セキュリティ機器のログを活用しきれず、脅威を見逃してしまう問題。

気付けない

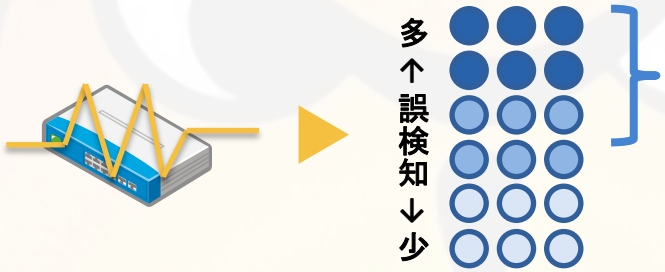
従来型のセキュリティ機器だけではゼロデイ攻撃や未知のウイルスに全く気付くことができない問題。

© 2014 日本セキュリティオペレーション事業者協議会（ISOG-J） & NTTコムセキュリティ株式会社

オオカミ少年 ▶ 誤検知を減らす

デバイスチューニング

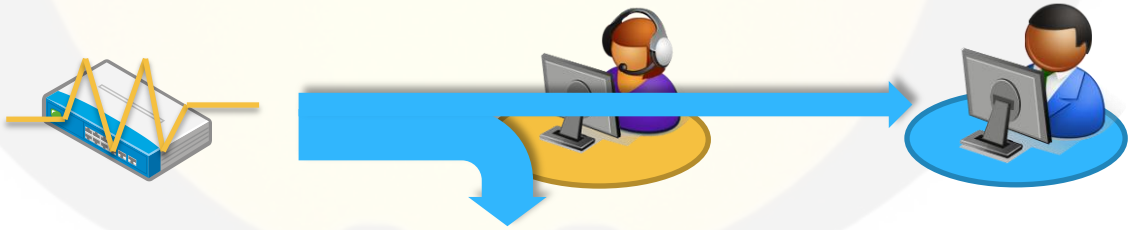
・セキュリティ対策製品におけるチューニング
　実トラフィックの検知傾向に基づいた適切なセベリティ設定



誤検知の多いシグネチャのセベリティは低く設定する。

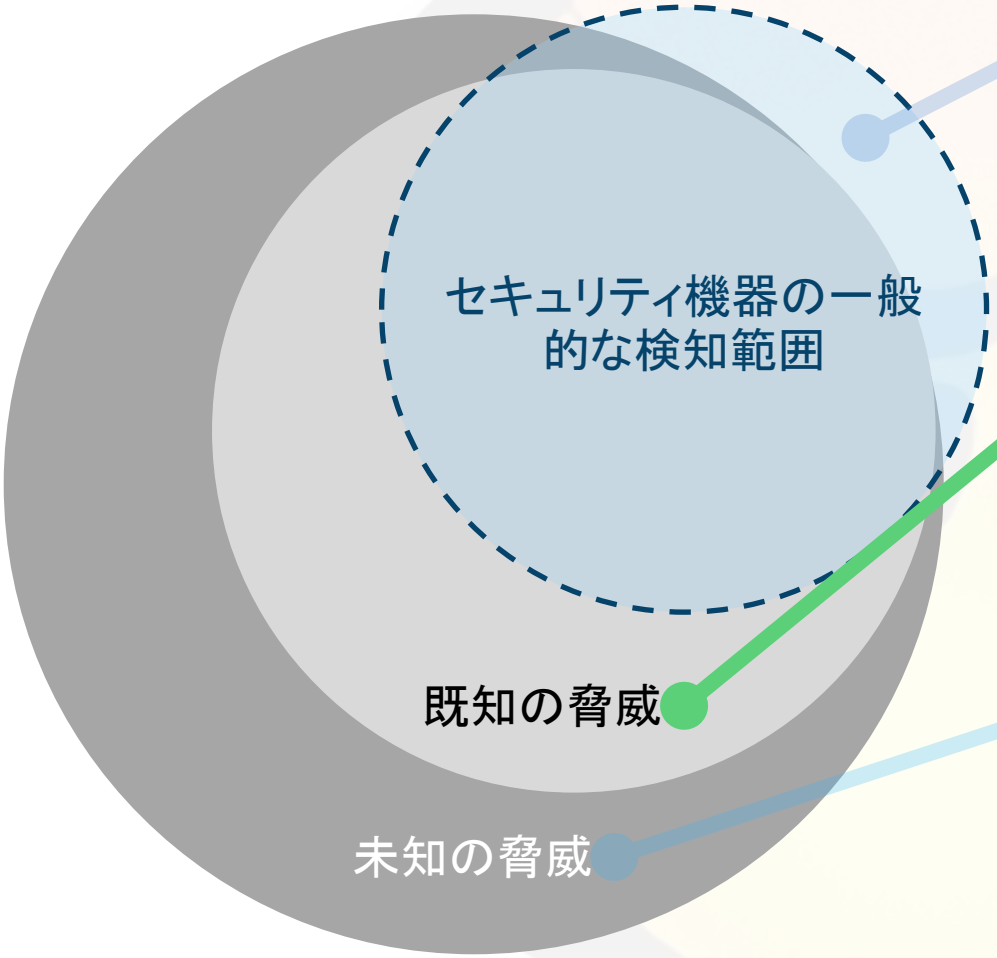
セキュリティアナリスト

・セキュリティアナリストによる詳細判断
　装置だけでは判定できない場合、「人」が判断する



真にリスクの高い検知に絞ったエスカレーションを行う。

© 2014 日本セキュリティオペレーション事業者協議会（ISOG-J） & NTTコムセキュリティ株式会社



オオカミ少年

誤検知が多くなると、不要な通知が増え、そのうち誰も信じてくれなくなる問題。

見逃し

セキュリティ機器のログを活用しきれず、脅威を見逃してしまう問題。

気付けない

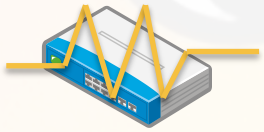
従来型のセキュリティ機器だけではゼロデイ攻撃や未知のウイルスに全く気付くことができない問題。

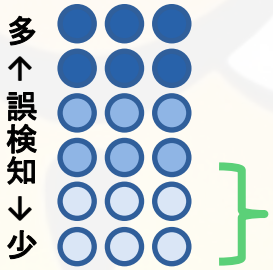
© 2014 日本セキュリティオペレーション事業者協議会（ISOG-J） & NTTコムセキュリティ株式会社

見逃し ▶ セキュリティ機器を効果的に活用する

デバイス
チューニング

・セキュリティ機器におけるチューニング
　実トラフィックの検知傾向に基づいた適切なセベリティ設定





誤検知の少ないシグネチャのセベリティは高く設定する。

誤検知もあるが、
「当たり」もあるものはどうするか？

© 2014 日本セキュリティオペレーション事業者協議会（ISOG-J） & NTTコムセキュリティ株式会社

誤検知に「当たり」を埋もれさせない

カスタム シグネチャ

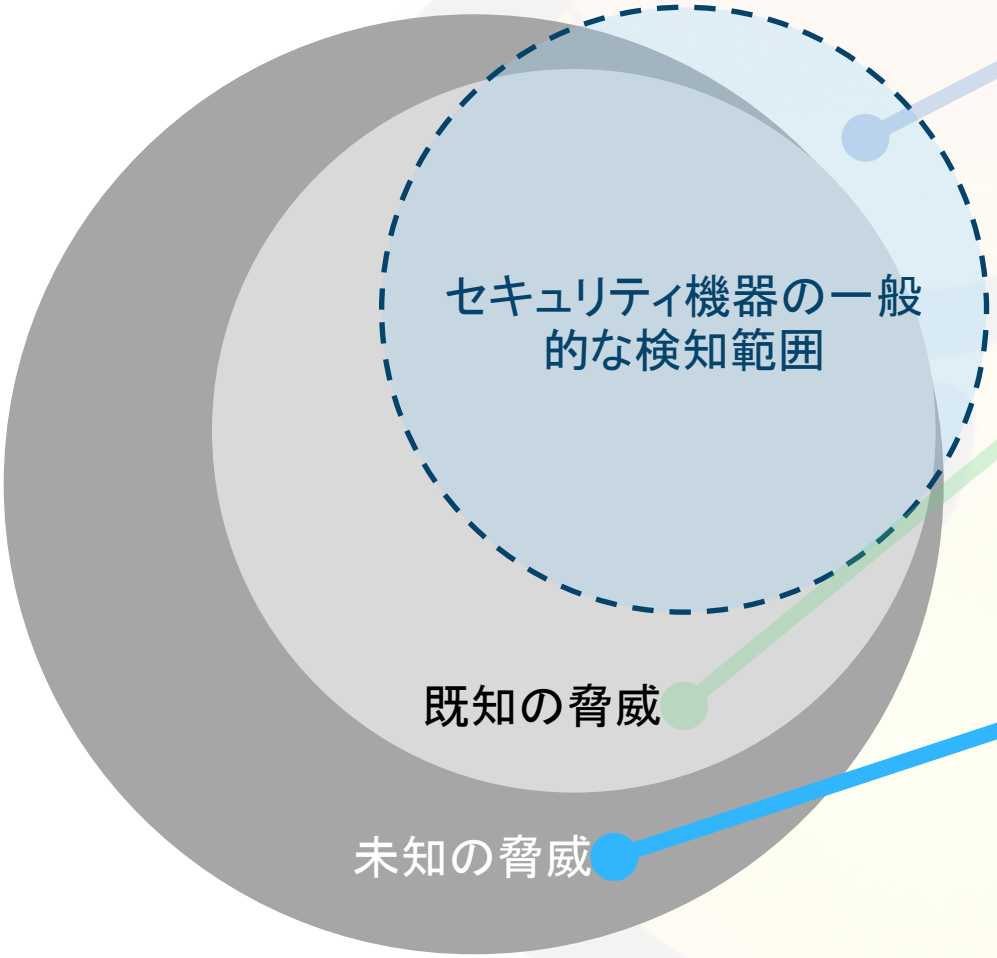
・カスタムシグネチャ機能の活用
　シグネチャを改良し、精度を上げることで「当たり」を引き出す

誤検知のある シグネチャ ＋ 実運用から 見えた 特徴パターン － 実運用から 見えた 誤検知パターン ＝ 高精度 カスタム シグネチャ

SIEM

・SIEMによる検知ロジックの強化
　複数種類のログを組合わせた分析ロジックにより「当たり」を浮かび上がらせる

© 2014 日本セキュリティオペレーション事業者協議会（ISOG-J） & NTTコムセキュリティ株式会社



オオカミ少年

誤検知が多くなると、不要な通知が増え、そのうち誰も信じてくれなくなる問題。

見逃し

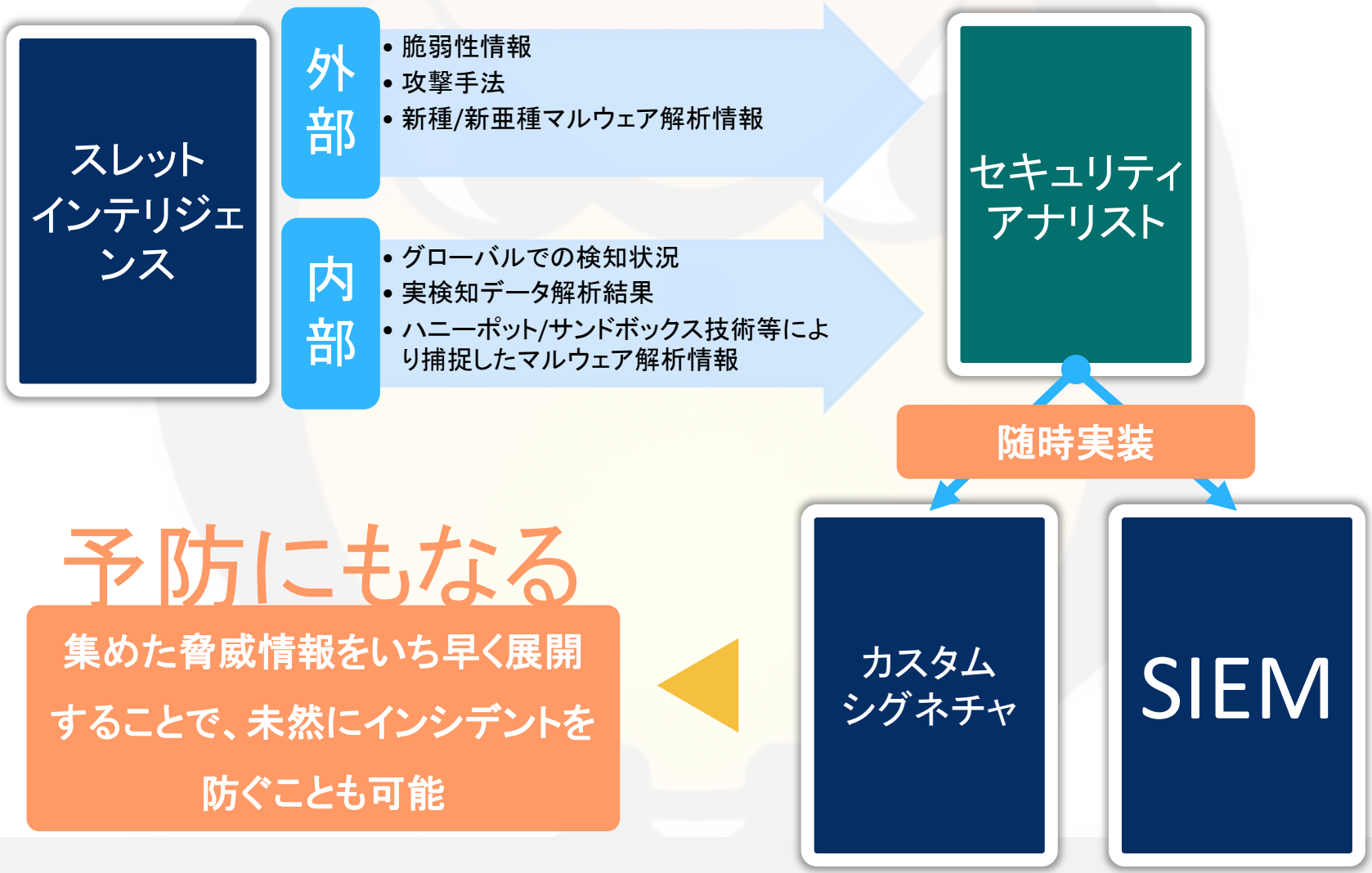
セキュリティ機器のログを活用しきれず、脅威を見逃してしまう問題。

気付けない

従来型のセキュリティ機器だけではゼロデイ攻撃や未知のウイルスに全く気付くことができない問題。

© 2014 日本セキュリティオペレーション事業者協議会（ISOG-J） & NTTコムセキュリティ株式会社

気付けない ▶ いち早く脅威情報をキャッチアップする

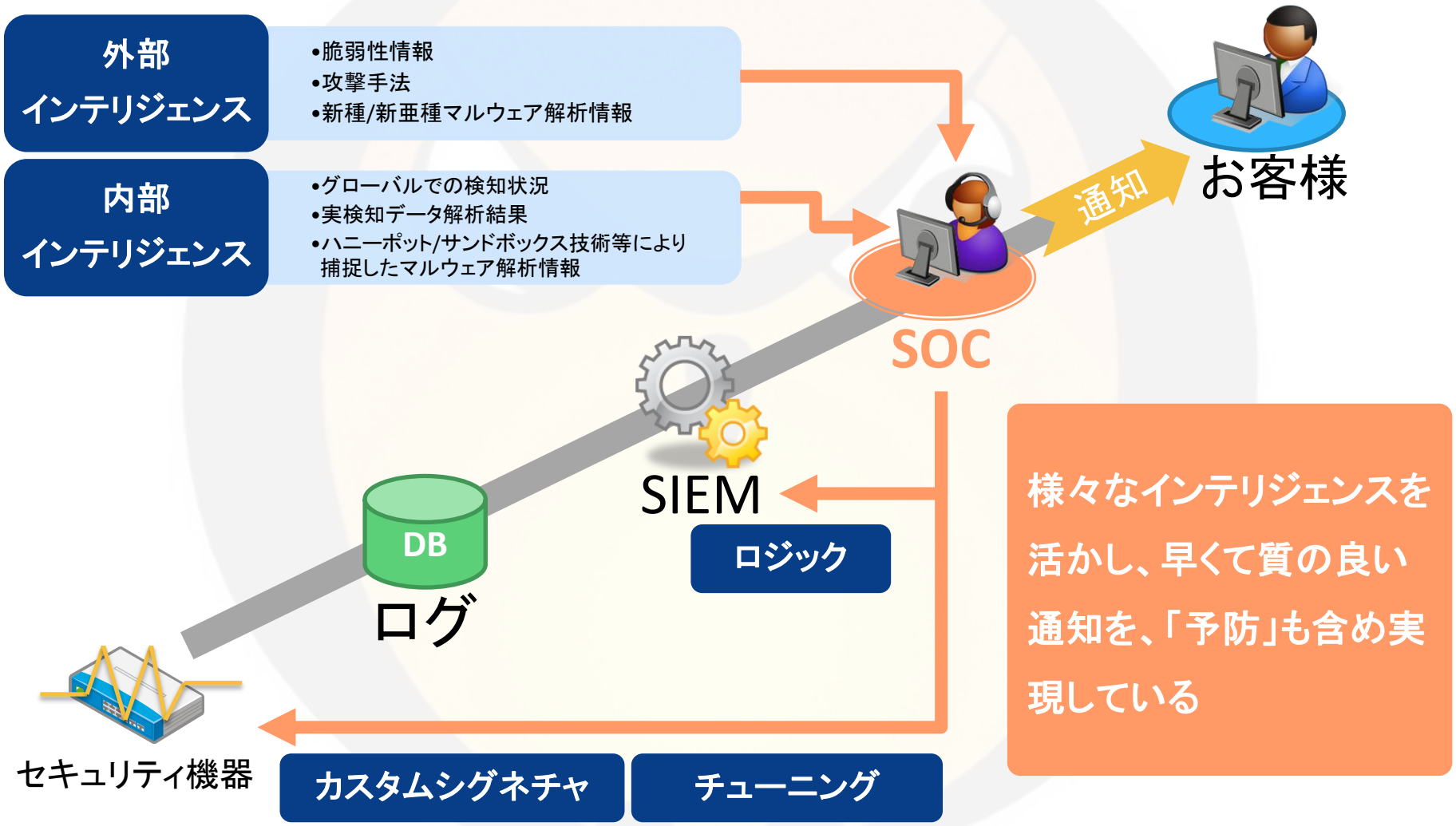


予防にもなる

集めた脅威情報をいち早く展開することで、未然にインシデントを防ぐことも可能

© 2014 日本セキュリティオペレーション事業者協議会（ISOG-J） & NTTコムセキュリティ株式会社

SOCにおける「インシデント発見」までのフロー



様々なインテリジェンスを活かし、早くて質の良い通知を、「予防」も含め実現している

© 2014 日本セキュリティオペレーション事業者協議会（ISOG-J） & NTTコムセキュリティ株式会社

インシデント発見後のSOCの取り組み

トリアージ支援

脆弱性診断結果

アセット情報

SOC

アセット情報や脆弱性診断結果を活用し、影響度合いを加味、執るべき具体的対処をアドバイス。

レスキュー対応

駆け付け
or
リモート

SOC

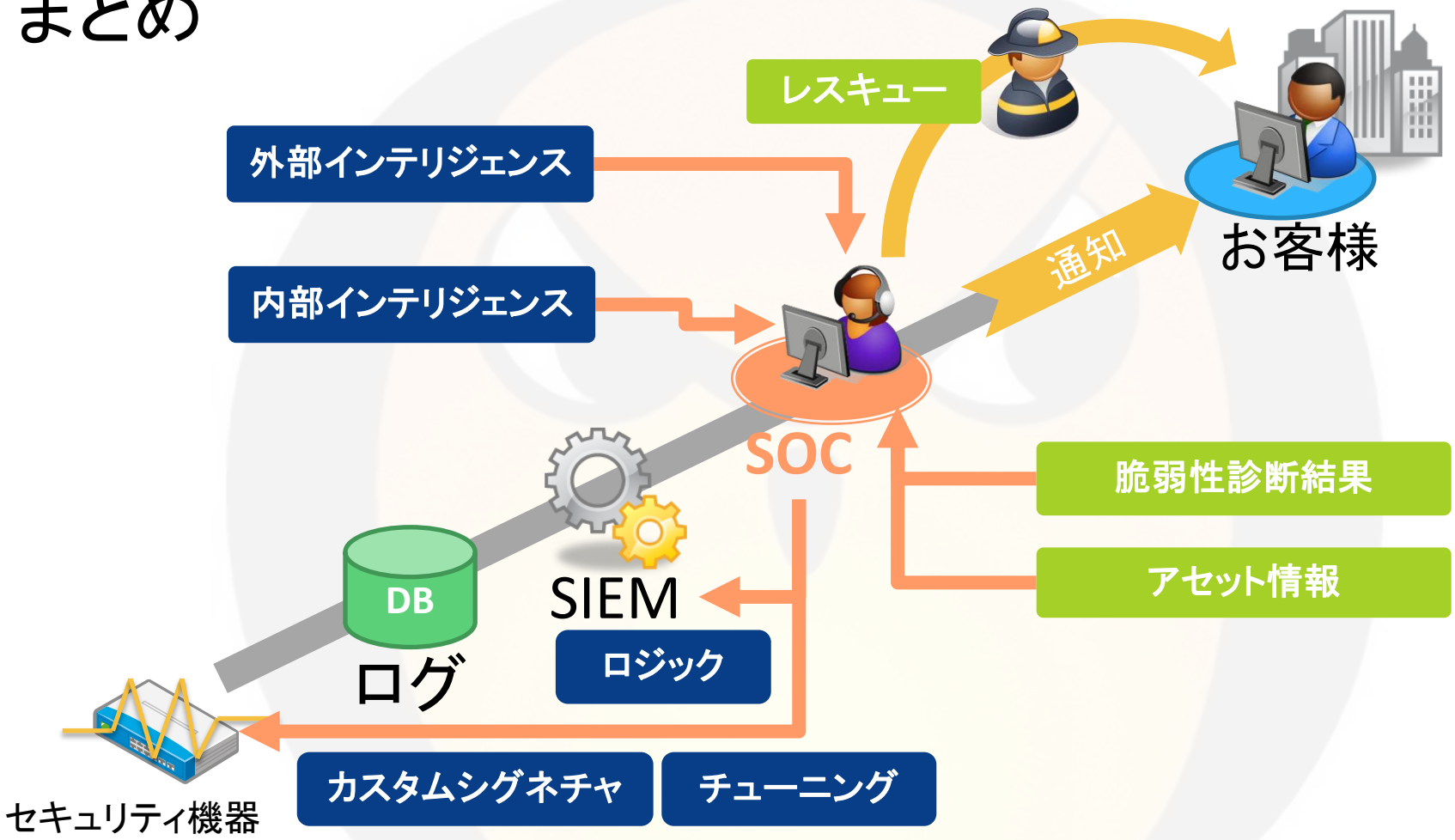
初動対応 情報整理、事象把握、調査、被害拡大防止

調査・分析 原因・侵入手法、影響範囲を明確化

改善提案 調査内容を総括し、再発防止に向けた改善提案

© 2014 日本セキュリティオペレーション事業者協議会（ISOG-J） & NTTコムセキュリティ株式会社

まとめ



セキュリティのプロフェッショナルとして、
被害の予防、通知、発見後まで
トータルにインシデントレスポンスをサポート

© 2014 日本セキュリティオペレーション事業者協議会（ISOG-J） & NTTコムセキュリティ株式会社