2013 年 2 月7日

（報道発表資料）

NTT コミュニケーションズ株式会社
Integralis AG
Secode AB
日本電信電話株式会社

標的型攻撃など未知のセキュリティリスクも対応可能なセキュリティ運用基盤の構築および総合リスクマネジメントサービスのグローバル展開について

NTT コミュニケーションズ（略称：NTT Com）、セキュリティ事業を展開する海外子会社の Integralis 社(本社：ドイツ)および Secode 社（本社：スウェーデン）は、NTT のセキュアプラットフォーム研究所（略称：NTT 研究所）と共同で、標的型攻撃などセキュリティリスクの検知・分析機能を強化した「セキュリティ情報・イベント管理エンジン（SIEM エンジン）」を開発し、新たなセキュリティ運用基盤として 2013 年 3 月より導入します。

NTT Com グループでは、本基盤のもと、お客さまの ICT 環境におけるセキュリティ対策をトータルで請け負うマネージドセキュリティサービスを高度化・低廉化し、あらゆるセキュリティリスクの調査・改善・モニタリングを総合的にコンサルティング・運用する「総合リスクマネジメントサービス」として、2013 年 3 月より米国および日本で提供開始し、順次グローバル展開を拡大していきます。

1.背景

スマートフォンやタブレット型端末の急速な普及やクラウド化の進展などにより、場所や端末を問わないシームレスな ICT の利用環境が実現する一方で、不正アクセスやウィルス感染、情報漏えいなどのセキュリティリスクの高まりが社会問題化しており、多様な ICT 環境に応じたセキュリティ対策が急務となっています。特に、標的型攻撃に代表される未知の脅威は日々増加しており、それらのリスクを迅速に把握し管理する手法が求められています。

こうした中、NTT Comグループでは、2003 年[*1]よりセキュリティのコンサルティングやセキュリティ設備の構築、マネージドセキュリティサービス、モバイルデバイス管理サービスなどを提供しておりますが、これまで培ったノウハウとNTT研究所の先端技術を融合させた新たなセキュリティ運用基盤を構築し、未知のセキュリティリスクへの対応を含むセキュリティサービスの高度化に取り組むこととしました。

2.新セキュリティ運用基盤の概要(別紙 1 参照)

(1)未知の脅威にも対応可能な SIEM エンジンを開発

NTT Com グループのセキュリティ運用ノウハウに基づく分析手法を活用し、高度な自動相関分析によるセキュリティリスクの検知や脅威レベルの自動評価機能をもつ SIEM エンジンを開発しました。SIEM エンジンには、NTT 研究所が開発した、長時間のログの変化から攻撃を検知する「相関通信時系列分析エンジン」や悪性サイトを効率的に発見する「ブラックリスト共起分析エンジン」など最先端の独自技術に加え、研究所が独自に収集したセキュリティ情報データベースを組み込みます。

さまざまな ICT 機器から収集される通信履歴などの膨大なセキュリティ情報を自動で相関分析できるため、これまでエンジニアの知見と経験に頼っていたセキュリティリスクの検知から影響度合いの分析、レポートを迅速に行うことができ、これまで検知が困難であった未知の脅威の見える化をはじめ、漏れのないセキュリティリスクの検知・対応を実現します。

なお、新セキュリティ運用基盤の SIEM エンジンと自動レポート機能により、これまでに比べてはるかに廉価にセキュリティ情報を通知するサービスも提供する予定です。

(2)グローバルシームレスなセキュリティ運用基盤

新セキュリティ運用基盤は、NTT Com、Integralis 社、Secode 社のグループ統一のセキュリティサービスプラットフォームとして、日本、米国、欧州、アジアに展開します。これにより、地域ごとに特色のある脅威に対するきめ細かな対処や、グローバルで検知情報を共有することによるリスクの未来予測や事前の対処などを提供できます。

3.総合リスクマネジメントサービスの概要(別紙 2 参照)

「Global Enterprise Methodology(GEM)」というグローバルで統一したリスク分析・評価手法を採用し、お客さまの ICT 環境のあらゆるリスクを洗い出し、改善計画の立案や継続的なモニタリングなどをトータルでコンサルティング・運用する総合リスクマネジメントサービスを提供します。GEM は以下の 5 つのフェーズから成り立っており、新セキュリティ運用基盤はその最終段階である「セキュアオペレーションによる継続的モニタリング」に適用していきます。

フェーズ１：企業環境の現在の「ガバナンス、リスク及びコンプライアンス（GRC）」レベルを調査
フェーズ２：資産管理やコンプライアンスなど 12 項目の視点から評価し、同一業界の平均レベルとのギャップ分析、到達目標の設定
フェーズ３：改善計画立案
フェーズ４：導入
フェーズ５：セキュアオペレーションによる継続的モニタリング

4.今後の展開

セキュリティの運用体制については、現在のセキュリティオペレーションセンタ(日本、米国、シンガポール、英国、スウェーデン、ノルウェーの計 6 ヵ所)をグローバルリスクオペレーションセンタ(マレーシアを追加し計 7 ヵ所)に改編し、高度なリスク分析官によるセキュリティ監視を実施します。(別紙 3 参照)

今後も引き続き、新セキュリティ運用基盤で対応可能なセキュリティ機器・サービスの拡大、相関分析でのインシデント検知能力やリスクレベルの自動判定機能の向上、各種関連データベースのアップデートなど継続的な開発を実施し、総合リスクマネジメントサービスの高度化を目指していきます。

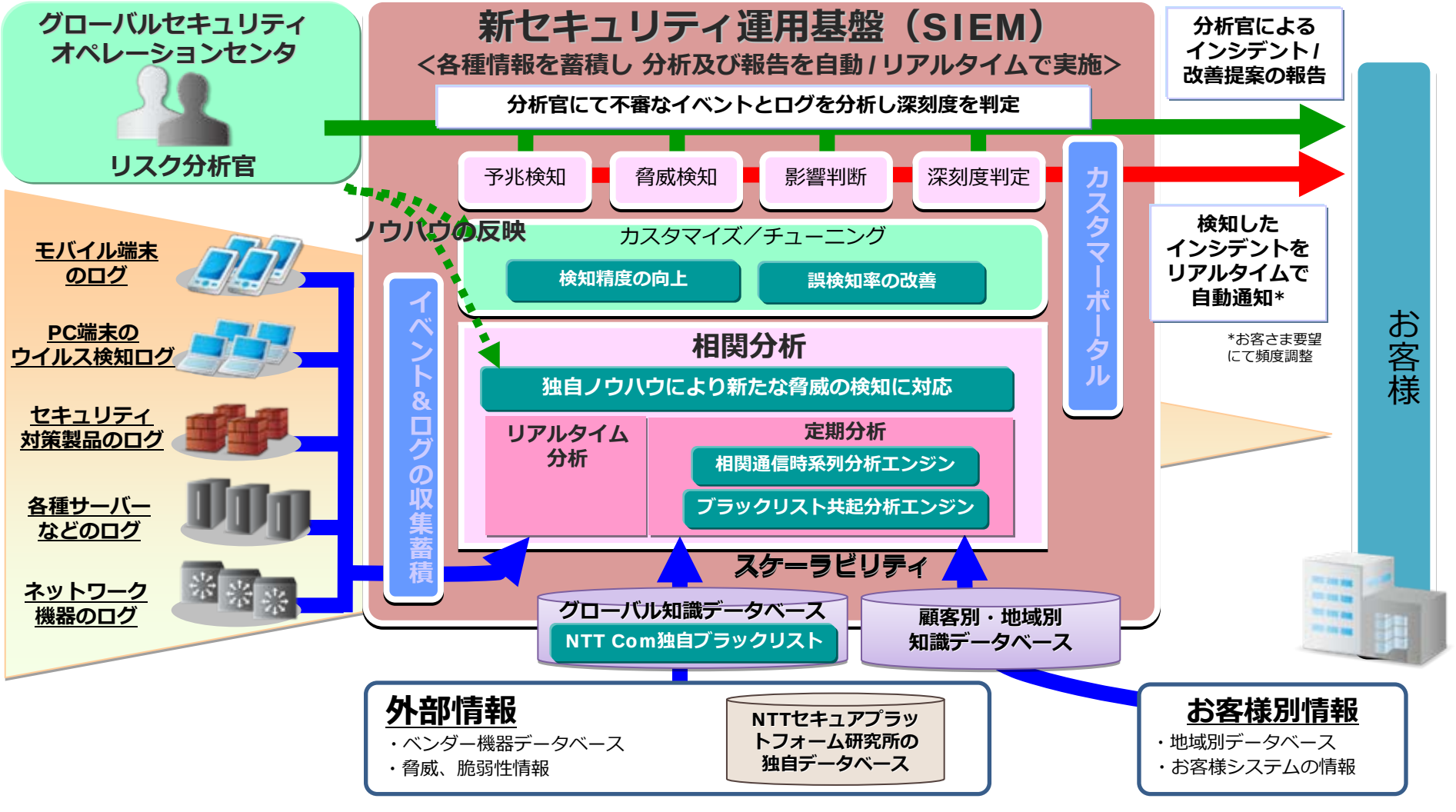
5.その他

2013 年 2 月 14 日(木)、15 日(金)に NTT 主催で開催される「NTT R&D フォーラム 2013」において「SIEM 分析エンジン」および「サイバー攻撃監視技術」として展示予定です。
http://labevent.ecl.ntt.co.jp/forum2013/info/index.html

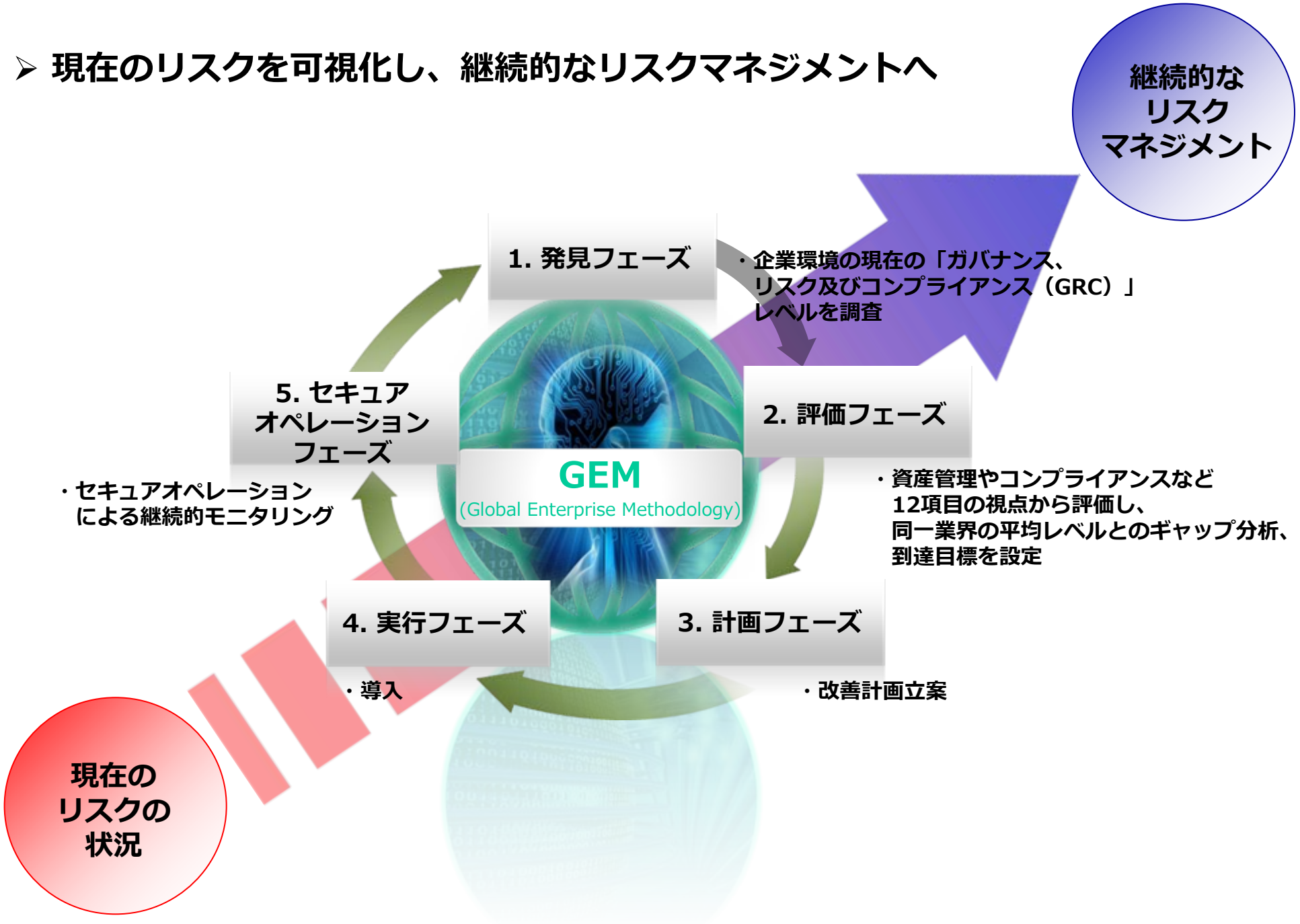
*1：Integralis 社（1988 年～）・Secode 社（2000 年～）はともにマネージドセキュリティサービスを提供しています。

別紙 1　新セキュリティ運用基盤

- NTT Com、Integralis社、Secode社の持つノウハウとNTTセキュアプラットフォーム研究所の先端技術を融合し開発
- 独自開発のSIEMエンジンを含む新たなセキュリティ運用基盤により、セキュリティに関するイベント及びログの自動分析/判定/報告を行いエンジニアの処理より高速・低コストを実現
- 併せて高度リスク分析官による高度な分析と深刻度判定により新たな脅威の発見と対処を実現

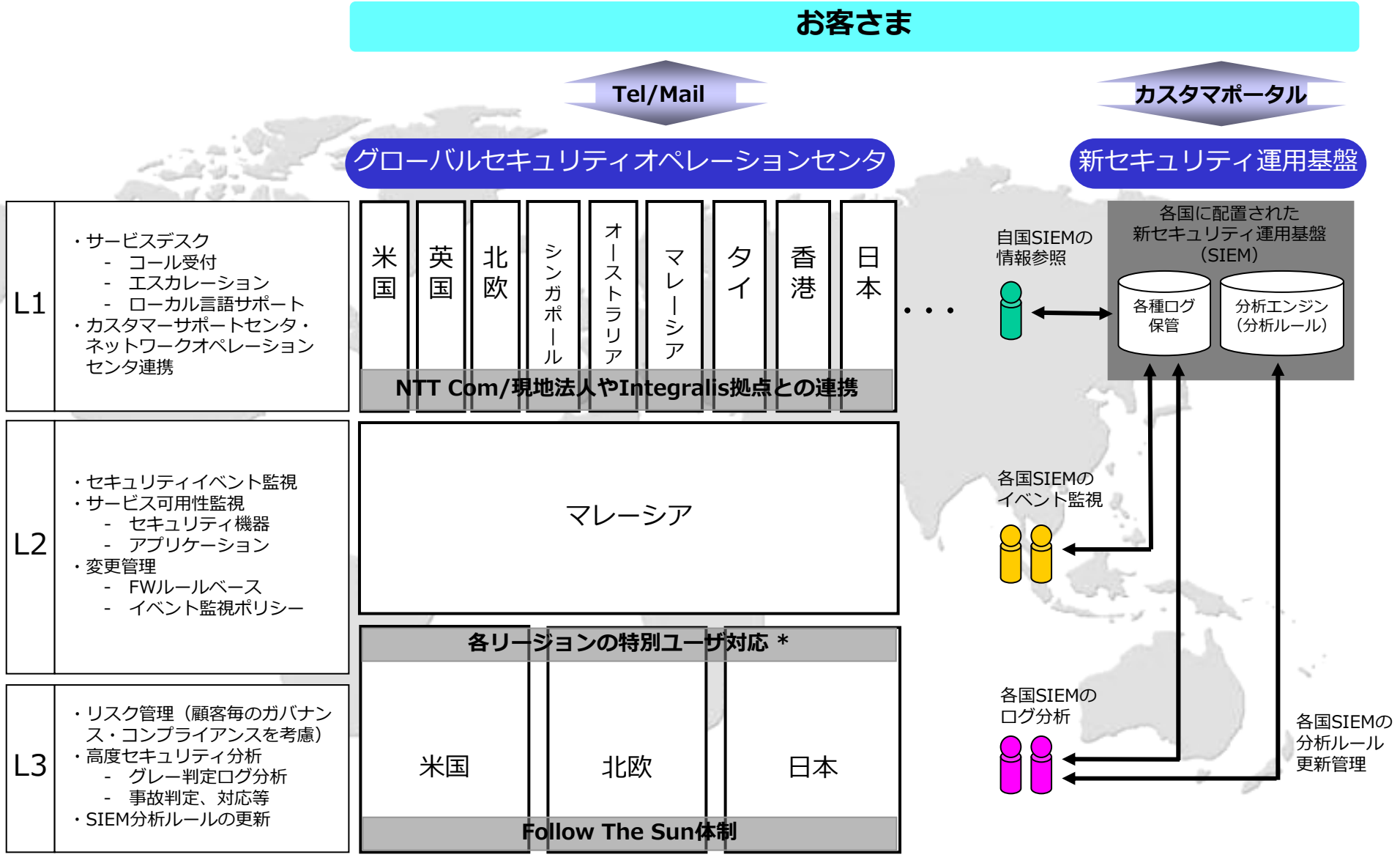


➢ 現在のリスクを可視化し、継続的なリスクマネジメントへ



別紙 3　グローバルリスクオペレーションセンタ（GROC）の体制

➢ グローバルシームレスに高度なリスクオペレーションを24時間365日提供



＊ 日本、米国、シンガポール、英国、スウェーデン、ノルウェー