2025 年 2 月 12 日

報道各位

株式会社テリロジー

# テリロジーが国内で販売するSumo Logic社「次世代クラウドSIEM」と Ｓｋｙ社「SKYSEA Client View」の組み合わせによる内部不正対策ソリューションの提供を開始

～同「内部不正対策ソリューション」のマネージドセキュリティサービスもテリロジーとアイティーエム社の共創により同時に提供開始～

株式会社テリロジー（本社：東京都千代田区、代表取締役社長：鈴木 達、以下「テリロジー」）が国内で販売する Sumo Logic 社の次世代クラウド SIEM（注 1）とＳｋｙ株式会社（東京本社：東京都港区、大阪本社：大阪市淀川区、代表取締役：大浦 淳司、以下「Ｓｋｙ」）が提供する SKYSEA Client View を連携させて実現する内部不正対策ソリューションの提供開始と、それらのマネージドセキュリティサービス、以下「MSS」をグループ会社のアイティーエム株式会社（本社：東京都新宿区、代表取締役社長：河本 剛志、以下「アイティーエム」）と共創し、2025 年 2 月より提供開始したことをお知らせいたします。

## ■ 背景

昨今、企業規模を問わずに取り組むべき重要なセキュリティ対策が「内部不正対策」です。IPA が毎年公表する「情報セキュリティ 10 大脅威 2024」（組織編）では、「内部不正による情報漏えい等の被害」が 3 位となり 9 年連続でトップ 10 にランクインしております。

最近では、大規模な情報漏えいの被害事例が数多く報告されており、内部不正が起きてしまうと、企業経営に甚大な影響を与え、企業価値の毀損につながるリスクが高まり、社会的信用が大きく低下してしまいます。自組織の重要な情報資産を守るためには、外部からの脅威対策とともに内部に存在するリスクへの対策も必要不可欠となっています。

そこで、当社は、内部リスクを把握する有効な手段として、Ｓｋｙの SKYSEA Client View で管理しているクライアント端末の操作ログと Sumo Logic 社の次世代クラウド SIEM を組み合わせて、内部不正の疑いがあるユーザの特定と行動を可視化し、内部不正の抑止に繋がるソリューションを開発しました。加えて、疑いのあるユーザを検知した後の調査報告と月次レポートなどを MSS で提供開始することといたしました。

## ■ 本サービスの概要

テリロジーが提供する内部不正対策ソリューションと MSS の主な特徴

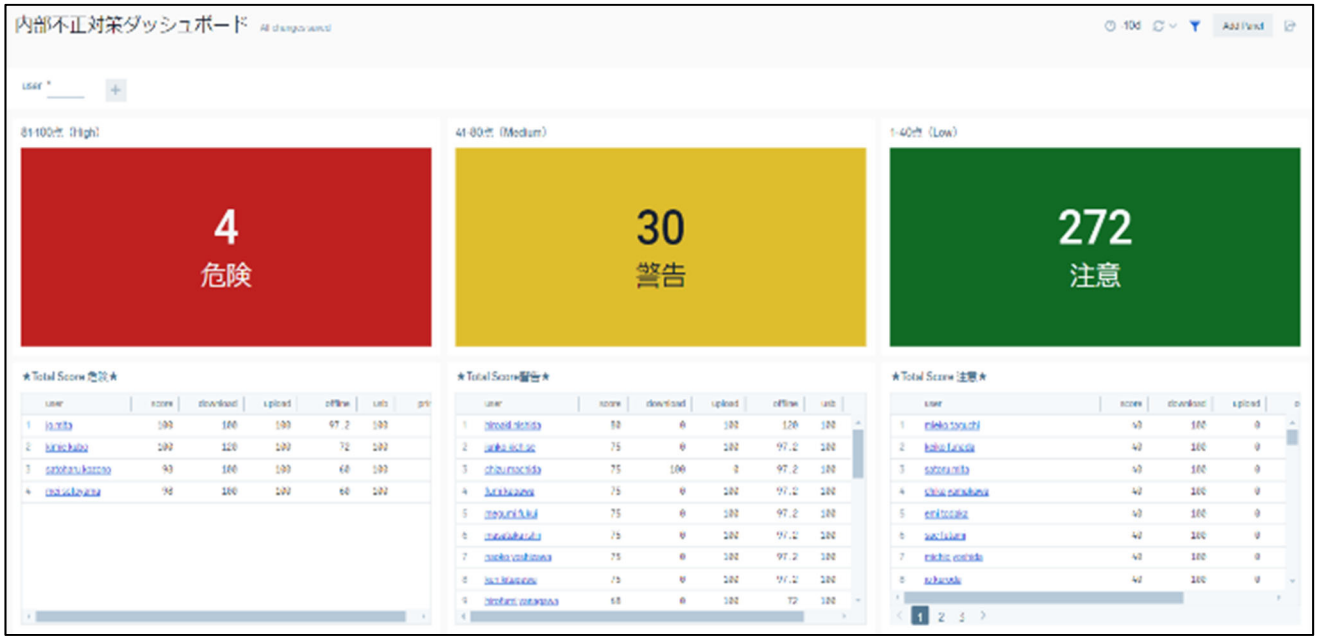
- **疑わしいユーザの特定**
  SKYSEA Client View のログを Sumo Logic に取り込み、当社が作成した内部不正に関連するルールを基に分析し、スコアリングを行うことで、疑わしいユーザを絞り込み、アラート発報することが可能
- **ユーザの行動分析と可視化するダッシュボードの提供**
  疑わしいユーザが行った行動や退職者の行動履歴が可視化可能なダッシュボードを提供
- **MSS による疑わしいユーザの調査報告と月次レポートの提供**
  内部不正対策ソリューションで検知した疑わしいユーザを調査した結果をお客様に報告と調査結果をまとめた月次レポートを提供
- **低コストで内部不正対策を実現**
  導入済みの SKYSEA Client View を活用することで、投資額を抑えて内部不正対策の実現が可能
- **Sumo Logic を統合ログ管理ソリューションとして活用可能**
  SKYSEA Client View 以外のログを統合管理するプラットフォームとしても利用可能な為、管理がバラバラなログを統合管理することでインシデント発生時の調査に効果的

国内で多くの導入実績を持つ SKYSEA Client View と Sumo Logic 社次世代クラウド SIEM を連携させることで、多くの企業が課題に感じている内部不正対策を低コストで導入可能です。

加えて、アイティーエムの運用オペレーションの専門知識と、当社の先進的なセキュリティ技術とサイバーセキュリティに関する技術力を融合した MSS を提供開始いたしました。今後も、次世代のセキュリティ対策を支える基盤を構築するとともに、多様な MSS ソリューションの提供を行ってまいります。

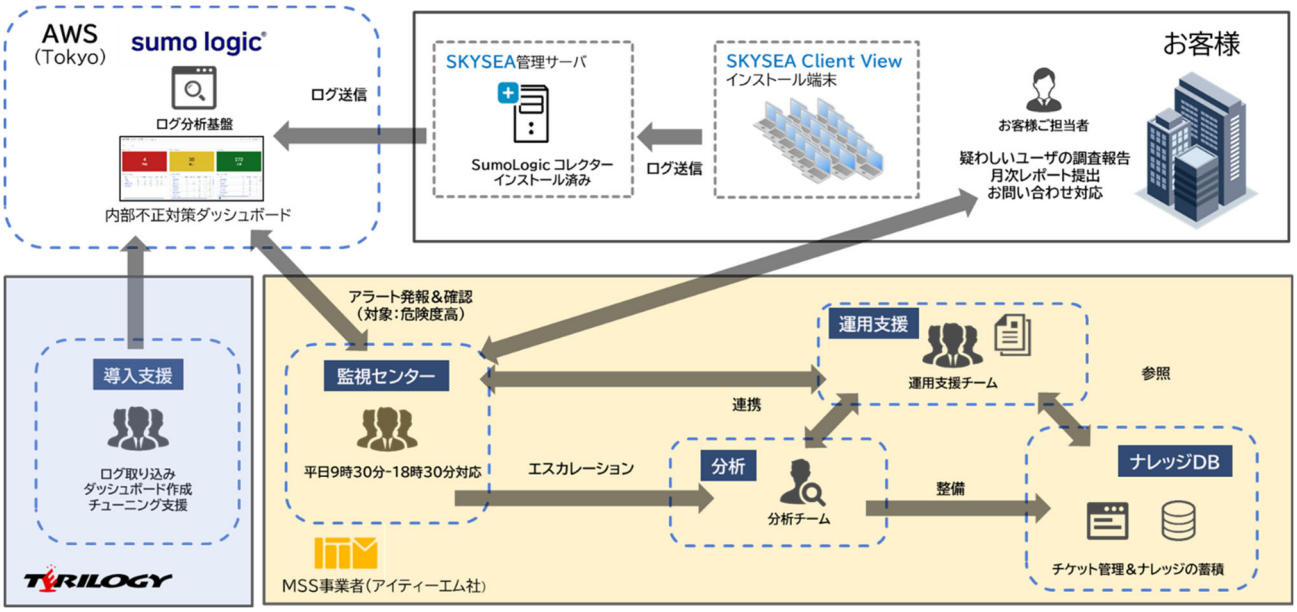
## ■ サービスイメージ

内部不正対策ダッシュボード（イメージ）




<ダッシュボードの内容について>
・内部不正に関連するルールを当社で作成
・ルール毎にスコア付けを行い、当社で算出したトータルスコアによって危険、警告、注意に分類
・内部不正対策ダッシュボードを用いて可視化と調査を行うことが可能
・特定の行動(例：ファイル大量ダウンロード)では、危険と判断出来ない場合も複数のルールスコアを
組み合わせることで疑わしいユーザを特定

## ■ MSS 提供イメージ




<サービス内容>
・疑わしいユーザの調査と報告
・月次レポートの提供
・報告内容に関するお問い合わせ対応
・内部不正対策ダッシュボードを用いて可視化と調査
・対応時間は、平日 9 時 30 分～18 時 30 分

注１）SIEM（Security Information and Event Management）は、セキュリティ機器などのログデータを収集し、サイバー攻撃やマルウェア感染などの脅威をリアルタイムに自動で検出し、通知する仕組み。



## ■ 株式会社テリロジーについて

株式会社テリロジー（1989 年設立、本社：東京都千代田区）は、セキュリティ、ネットワーク、モニタリング、ソリューションサービスの 4 分野を中核に、多様な顧客ニーズに対応した製品とサービスを提供するテクノロジーバリュークリエイターです。大手企業や通信事業者を中心に 300 社以上のお客様との取引実績を誇ります。
（https://www.terilogy.com/）

## ■ アイティーエム株式会社について

アイティーエム株式会社は、さくらインターネットグループの事業会社で MCSSP（Managed Cloud & Security Service Provider）事業を展開しております。27 年にわたる IT システム運用ソリューションの運用実績とノウハウ、24 時間 365 日体制による安定したオペレーションおよび 18 年にわたる脆弱性診断サービスをはじめとするセキュリティサービス等を強みに、金融・製造・通信・公共・サービス等多岐にわたる業種・業態のお客様のビジネスの成功を支え続け、国内エンタープライズを中心に多くのお客様で実績がございます。
（https://www.itmanage.co.jp/）

【製品・サービスに関するお問い合わせ先】
株式会社テリロジー
クラウドセキュリティ事業部
TEL：03-3237-3291、FAX：03-3237-3293
e-mail：asat@terilogy.com

アイティーエム株式会社
カスタマーリレーション本部
e-mail：pr@itmanage.co.jp

【報道関係者お問い合わせ先】

株式会社テリロジー
広報宣伝
担当 齋藤
TEL：03-3237-3291、FAX：03-3237-3316
e-mail：marketing@terilogy.com