

報道関係者各位

2026年8月18日
KELA株式会社

**SLING、サードパーティリスク管理(TPRM)プラットフォームを大幅拡張
～独自の対話型AI「ROSE AI」および経済産業省・金融庁ガイドライン対応機能を新たに統合。企業サプライチェーン全体のサイバーリスク対応を加速～**

サイバー脅威インテリジェンス(CTI)およびサードパーティリスク管理(TPRM)ソリューションを提供するKELA株式会社(本社:東京都千代田区、事業拠点:東京都港区、執行役員兼COO:廣川 裕司、以下「KELA」)は、グループ会社であるSLINGが開発するサードパーティリスク評価・管理プラットフォームの大型アップデートを発表いたします。

本最新リリースでは、対話型AI機能「ROSE AI」の実装、日本の最新の経済産業省(METI)および金融庁(FSA)のサイバーセキュリティ指針への対応、さらに大手企業グループやMSSP(マネージド・セキュリティ・サービス・プロバイダー)向けの「マルチテナント管理パネル」が新たに統合されました。

■ 背景: AI脅威の急増と日本におけるサプライチェーン攻撃

AIを活用したサイバー攻撃の自動化・高度化が進む中、委託先やサプライヤーなどサードパーティを標的としたサプライチェーン攻撃が日本全国で急増しています。グローバルな調査によると、以下の実態が明らかになっています。

- CISOの60%が、過去1年でサードパーティに起因するインシデントが増加したと回答。
- KELAのCyber Intelligence Center(CIC)の観測では、AI悪用型サイバー犯罪に関連するランサムウェア被害件数が前年比**389%**増を記録。
- 脆弱性の発見から実際の攻撃に至るまでの時間が、従来の数か月から「数時間」へと大幅に短縮。

国内においても、主要インフラ拠点における運行停止、大手食品・飲料メーカーにおける出荷停止および数十億円規模の直接損害、大手食品物流企業における数千社におよぶパートナー企業への影響など、サプライチェーンを標的とした攻撃事例が相次いでいます。1社の主要サプライヤーや委託先が侵害されることで、ビジネスエコシステム全体に甚大な波及効果(被害の連鎖)をもたらす実態を示しています。

■ 中核機能: ダークウェブ・インテリジェンスによるリアルタイムTPRM

SLINGは、企業が依存するサプライチェーン全体のリスクを継続的に監視することで、これらの課題を解決します。アタックサーフェスマネジメントKELA独自の脅威インテリジェンス(CTI)およびダークウェブ監視を融合させることで、客観的かつリアルタイムなリスク評価スコア「Sling Score」及び「アラート情報」を提供します。

【実証事例(ケーススタディ)】

SLINGは最近、脅威アクターグループ「ShinyHunters」による大手グローバルプロフェッショナルサービスファーム へのサイバー攻撃において、早期警戒を発令することでその実効性を実証しました。継続的なASM監視とKELAのリアルタイムCTIデータを組み合わせることで、サードパーティが悪用する前に、脅威の兆候や侵害指標(IoC)をリアルタイムアラートとして顧客に即座に通知し、能動的な防御を実現しました。

■ 今回のリリースにおける新機能(主な拡張ポイント)

従来のコアプラットフォームに加え、日本企業向けに最適化された4つの主要機能が正式にリリースされます。

1. 経済産業省(METI) & 金融庁(FSA)ガイドライン対応アンケート機能: 経済産業省のガイドラインおよび金融庁の「サイバーセキュリティセルフアセスメント点検票」に準拠したアンケート機能を搭載。プラットフォーム上から問診票を直接送付・回収し、回収結果とSLINGの技術的スコア(Sling Score)を同一画面で一元管理可能になりました。
2. マルチテナント管理パネル: エンタープライズグループ企業、持ち株会社、MSSP向けに開発された管理機能。テナントごとに分離されたアクセス制御のもと、複数の子会社や顧客企業のリスクを、危険度・事業重要度・部門別に一元管理できます。
3. 「ROSE AI」によるAIネイティブな脅威分析: プラットフォームにネイティブ統合された対話型AIアシスタント。複雑な脅威の検出結果を平易な言葉に翻訳し、危険度や文脈(コンテキスト)を解説するとともに、優先度の高い具体的な修復ステップを即座に提示します。
4. 日本語ネイティブなユーザー体験: UI、セキュリティアラート、ROSE AIの応答、経営層向けレポートに至るまで完全日本語化。言語の壁を取り払い、国内のSOCやリスク管理チームの運用負担を劇的に削減します。

■ 今後の製品ロードマップ

サプライチェーンのレジリエンス(回復力)を継続的に強化するため、SLINGは以下の機能を順次展開予定です。

- **AI自動生成リスクレポート**(現在ベータ版、来月一般提供開始): 統合されたLLMを活用し、ビジネス文脈に合わせた経営層向けのサマリーや分析結果を文章で自動生成。
- **サプライヤー自動発見 (Autodiscovery)**: 企業のデジタルアセット情報から、AIが3rdパーティおよび4thパーティ(委託先の委託先)との連携関係をマッピングし、サプライチェーン全体を可視化。
- **事業継続性および財務インパクト分析**: サードパーティリスクが事業継続や売上高に及ぼす潜在的な財務・運用上の影響を数値化する定量モデルの提供。

■ SLING CEO Dr. Uriel Cohen(ウリ・コーエン)のコメント

「現代企業の境界線は、自社ネットワークの枠を超え、接続されているすべてのサプライヤー、パートナー、サービスプロバイダーにまで広がっています。攻撃者はAIを駆使し、サプライチェーンの最も弱い『結び目』を狙っています。KELAが誇る高度な脅威インテリジェンスと最新のAI分析を組み合わせることで、SLINGは日本企業にリアルタイムの可視性と実行力を提供し、インシデントが発生する前にサプライチェーン・サイバーリスクを無効化できるよう貢献してまいります。」

■ KELA株式会社について

<https://www.kelacyber.com/ja/>

サイバー脅威インテリジェンス企業として数々の受賞歴を誇る KELAの使命は、サイバー犯罪のアンダーグラウンドからの脅威に関して、実用的なインテリジェンスを提供し、サイバー攻撃の防止と無力化をサポートすることです。2009年に設立されたKELAは、独自の自動化テクノロジーと、高度な技術を持つサイバーインテリジェンスのアナリストを擁しており、数々の成功を収めています。世界中で信頼を得ているKELAのテクノロジーは、隠れたアンダーグラウンドに侵入し、脅威を徹底的に監視、追跡、調査することで、実際のリスクを明らかにし、プロアクティブな保護を可能にします。KELAの革新的なソリューションは、攻撃者の目から見た、高度にコンテキスト化されたインテリジェンスを顧客に提供し、プロアクティブなネットワーク防御、ならびにブラインドスポットの排除を実現します。KELAの日本法人は、2019年に設立されました。(本社:東京都千代田区、事業拠点:東京都港区)

※KELAグループのULTRA RED、SLINGの詳細は以下をご参照ください。

<https://ultrared.jp/>

<https://slingscore.com/ja/>

■ 本件に関するお問い合わせ先

KELA株式会社 広報担当(前田・中村)

TEL: 03-6634-7836

Email: jp-pr@ke-la.com