

• プレスブリーフィング・2026年8月

AIによって加速される攻撃時代における サプライチェーン防衛

Dr. Uriel Cohen

Chief Executive Officer, Sling. 最高経営責任者

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



現状

セキュリティ境界は自社ネットワークにとどまらない。
依存するすべてのベンダーこそが新たな境界である。

現代のエンタープライズ企業は単独で完結して機能してはいない。関与するすべてのサプライヤー、物流パートナー、およびクラウドサービスが、潜在的な侵入経路となり得る。攻撃者もこれに合わせて手法を変化させている。強固に防御された標的を直接侵害するのではなく、その企業のサプライチェーン上で「最も監視の行き届いていない弱い環（リンク）」すなわち、単一のサプライヤー、地域のベンダー、あるいは共有されている物流インフラを狙うのである。

世界のCISOの

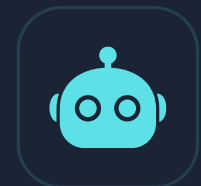
60%

過去1年間でサードパーティ関連のセキュリティインシデントの増加を報告。

日本もこの傾向の例外ではない。過去1年で、日本を代表する有名ブランドの数々が、まさにこの種の脆弱性を突かれて被害を受けている。

AIがサプライチェーンリスクを生んだのではない。 AIはそれを加速させた。

AIはサプライチェーンの両側（防衛・攻撃の双方）において戦場へと参入している。すなわち、ベンダーの技術スタック（システム基盤）内部で自律的に機能するアクターとして、そしてそれらを標的とする攻撃者の「フォース・マルチプレイヤー（能力増幅器）」として機能しているのである。



ベンダーのシステム内で稼働するエージェント型AI

自律型エージェントが意思決定を行い、認証情報を保持し、APIを呼び出すことで、あらゆるサードパーティ内部の攻撃対象領域を拡大させている。



AIモデルを悪用する攻撃者

LLMを活用した偵察、フィッシング、エクスプロイト生成が、裾野の広いサプライヤー群への侵害のハードルを下げている。

2026年上半期 AI脅威情勢レポートの全貌

 389%

AI関連ランサムウェア被害
の前年比増加率

FORTINET 2026 GLOBAL THREAT LANDSCAPE REPORT

 80~90%

AIエージェントによる
侵入自動化率

GTG-1002 ケーススタディ

 100万件以上

KELA確認の感染端末数
(2026年1~5月)

KELA CIC テレメトリー

 77,722+

2026年macOS被害端末数

KELA CIC テレメトリー

 49,700件以上

ダークウェブ流通中の
AIセッションCookie数

KELA CIC DARKNET MONITORING

 10%

AI活用グループの世界ラン
サムウェア被害シェア

「THEGENTLEMEN」チャット流出

脆弱性の発見から悪用までの期間は、数か月・数年単位から数時間単位にまで短縮された。

3つの業界。共通する一つの死角。

主要な物流インフラ 2023年7月 脅威アクター LockBit 3.0 損失額 非公表 業務停止日数 2.5日間 5つのコンテナターミナルが全面停止 流出件数 報告なし OT(制御システム)の障害であり、データ漏えいではない 影響を受けたサードパーティ 自動車および物流業界をはじめとする企業	食品・飲料業界 2025年9月 脅威アクター Qilin 損失額 50億円(約3,140万ドル) 業務停止日数 約2か月 出荷のみでも約2週間の停止 流出件数 115,000件以上 当初評価では最大190万件 影響を受けたサードパーティ 全国の小売・流通パートナー	大手食品メーカー 2026年7月～継続中 脅威アクター RansomHouse 損失額 非公表 評価継続中 業務停止日数 約2～3週間 本稿執筆時点で復旧作業継続中 流出件数 確認済み 範囲は未公表 影響を受けたサードパーティ 食品・小売業界のパートナー企業 約5,000社
---	--	--

いずれも標的そのものではなかった。それぞれが、最も侵入しやすい入り口であり、下流のすべてを最速で混乱させる手段だった

当社のソリューション

脅威アクターの視点でサプライヤー（取引先）を調査する

01

ディスカバリー

ドメイン名だけを起点に、企業に紐づくすべてのドメイン、サブドメイン、公開資産をエージェントレスでマッピング。

02

収集・分析

KELAのサイバー・インテリジェンス・センターによる10年以上の独自インテリジェンスをもとに、ダークネットのフォーラムやチャンネルを24時間365日監視。

03

評価

SlingはASM(攻撃対象領域管理)とCTI(サイバー脅威インテリジェンス)のシグナルを統合し、0~100の単一スコアにまとめ、最優先で対応すべき事項を明確にする。

04

実行可能なアウトプット

リアルタイムアラート、監査対応可能なレポート、是正措置のステップを提供。新たな対応待ちの案件を増やすことはない。

オンボーディングに必要なのは企業ドメインのみ。評価対象ベンダーによる協力やソフトウェアのインストールは一切不要で、24時間以内にリスクの全体像を可視化。

Risk Information

Date: 2025-12-15

Severity: Medium

Type: Ransomware Attack

Asset: [REDACTED]

Title: [REDACTED]

[REDACTED] claimed as victim of Qilin ransomware

Source: Darknet platforms

Description:

On December 15, 2025, the operators of Qilin ransomware claimed to have compromised [REDACTED]
[REDACTED]

日本企業に関する実際のダークネットアラート
(機密保持のため一部を編集)

現場からの実証結果【実例】

これは机上の空論ではない。 実際のアラートを紹介する。

2025年12月、Slingのダークネット監視により、ランサムウェアグループQilinがこの企業を被害者として名指しした投稿を検知した。情報の出所はダークネット上のプラットフォームでの実際の活動である。

この顧客は多くの日本企業のサプライヤーであり、Slingは被害拡大を防ぐため速やかに通知を行った。

識別情報は編集済み。被害を受けた企業は、日本の大手企業グループの地域子会社である。

SLINGは、報道や重大事件として大きく取り沙汰される前に、攻撃者の間で交わされている情報を先回りして可視化する。

現場からの証明 - 成功事例

一つの脅威アクター、一つのサードパーティ

脅威アクター「ShinyHunters」が一次取引先経由でコンサル・金融企業のネットワーク領域へ侵入。二次取引先（4th party）による影響力と、サードパーティ・リスク管理の重要性を示す実例である。

ShinyHunters ブログ

シグナル1 - 2026年第1四半期

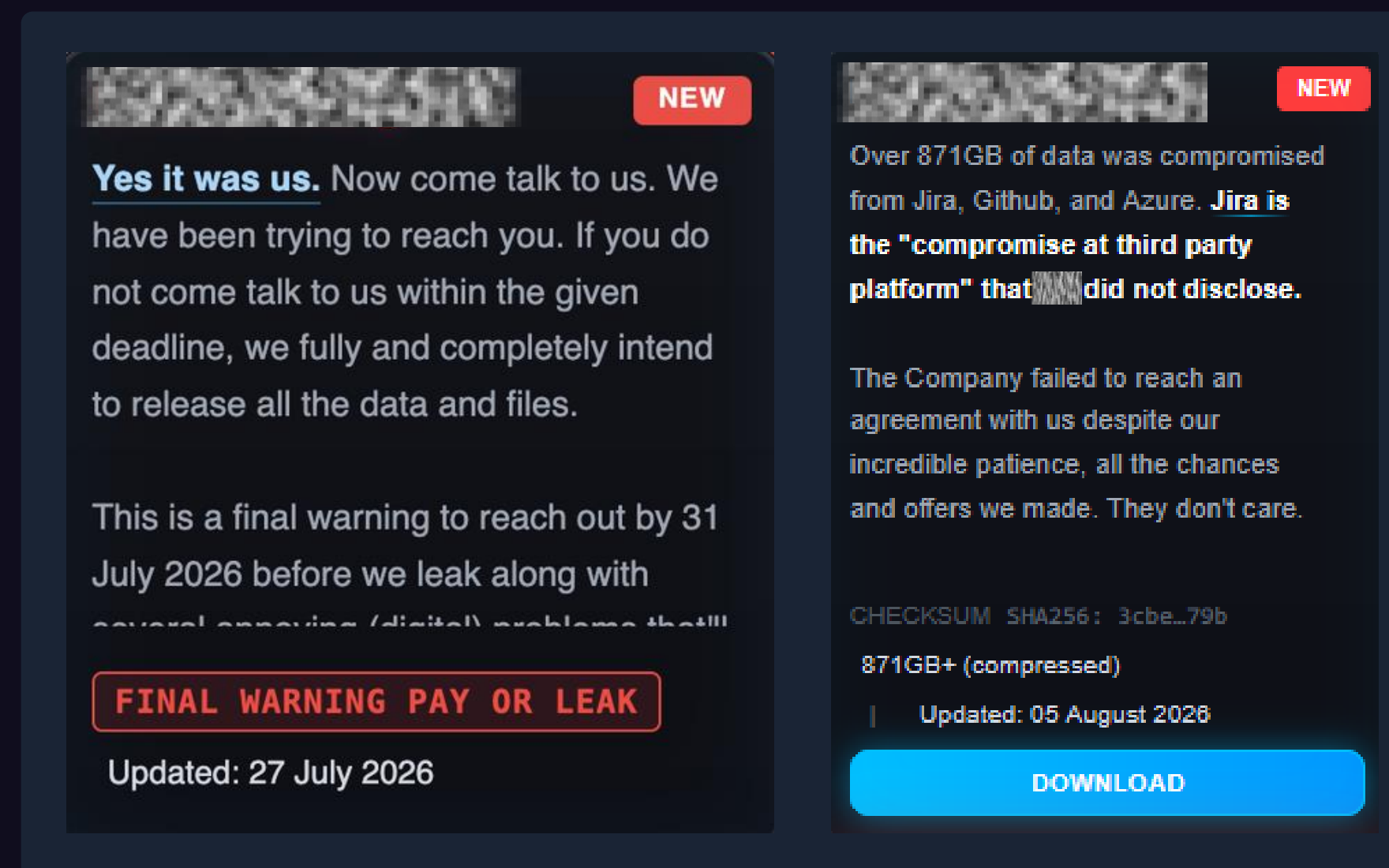
アカウント侵害の警告とスコア低下

シグナル2 - 2026年第2四半期

データベース流出によりダークネット監視で早期の兆候を検知。ベンダー自身の公表に先立ち、4社すべての顧客にSlingが通知した。

シグナル3 - 2026年第3四半期

脅威アクターが侵害の犯行声明を出したことでサイバーランサム事案を検知。公表前のリアルタイムで顧客に通知した。



The screenshot displays two blog posts from ShinyHunters. The left post, dated 27 July 2026, is a 'FINAL WARNING PAY OR LEAK' with a deadline of 31 July 2026. The right post, dated 05 August 2026, reports that over 871GB of data was compromised from Jira, Github, and Azure, and that the company failed to reach an agreement with the attackers despite offers.

Yes it was us. Now come talk to us. We have been trying to reach you. If you do not come talk to us within the given deadline, we fully and completely intend to release all the data and files.

This is a final warning to reach out by 31 July 2026 before we leak along with several annoying (digital) problems that!!!

FINAL WARNING PAY OR LEAK

Updated: 27 July 2026

Over 871GB of data was compromised from Jira, Github, and Azure. **Jira is the "compromise at third party platform" that [redacted] did not disclose.**

The Company failed to reach an agreement with us despite our incredible patience, all the chances and offers we made. They don't care.

CHECKSUM SHA256: 3cbe...79b

871GB+ (compressed)

Updated: 05 August 2026

DOWNLOAD

現場からの証明 - 成功事例

一つの共有ベンダー。事前に守られた4社の顧客。

無関係な4社のSling顧客が、同一のグローバルプロフェッショナルサービスベンダーを利用していた。このベンダーが侵害された際、SlingのCTI監視がベンダー自身の公表およびランサム犯行声明の公開に先立ち、3回にわたり早期に検知した。



当社のソリューション 規制コンプライアンス

プラットフォームから直接セキュリティ質問票を送付できる。標準フレームワークにも、特定ベンダー向けにカスタマイズした質問票にも対応し、回答はそのベンダーのSlingスコアと合わせて管理される。



標準フレームワーク

FSA、NIS2、DORA、ISO 27001、HIPAAなど、導入後すぐに送信可能。



完全カスタム質問票

特定のベンダー、規制当局、または社内ポリシーに合わせて作成できる。



スコアと並べて回答を確認

回答は別の受信箱ではなく、そのベンダーのSlingスコアと並べて表示される。

FSA Questionnaire

サイバーセキュリティセルフアセスメントの

点検票（2024 年度）

サイバーセキュリティに関する経営層の関与

【問1】 サイバーセキュリティに関する経営方針について、あてはまるものを選択してください。

- ☐ 1. 経営トップ（頭取・社長・理事長等）の関与のもと、経営方針としてサイバーセキュリティの確保を掲げており、ディスクロージャーやHP等で对外公表している
- ☐ 2. 経営トップ（頭取・社長・理事長等）の関与のもと、経営方針としてサイバーセキュリティの確保を掲げている（对外公表はしていない）
- ☐ 3. 今後、経営方針としてサイバーセキュリティの確保を掲げる予定がある

経済産業省（METI）が規制・ガイドラインの枠組みに本格参入



経済産業省（METI）は現在、サイバーサプライチェーンリスクにおける主要な規則策定機関となっており、NIS2、DORA、HIPAA、SEC情報開示規則のもとで既に運用されている「継続的な監視モデル」と同等の基準へと日本企業を追従・順応させている。

サプライチェーンに対する説明責任

組織は自社だけでなく、サプライヤーのサイバーセキュリティ態勢についても責任を負う。

継続的モニタリング

重要産業全体で義務化され、年次の自己評価アンケートにとどまらない取り組みが求められる。

根拠に基づく報告

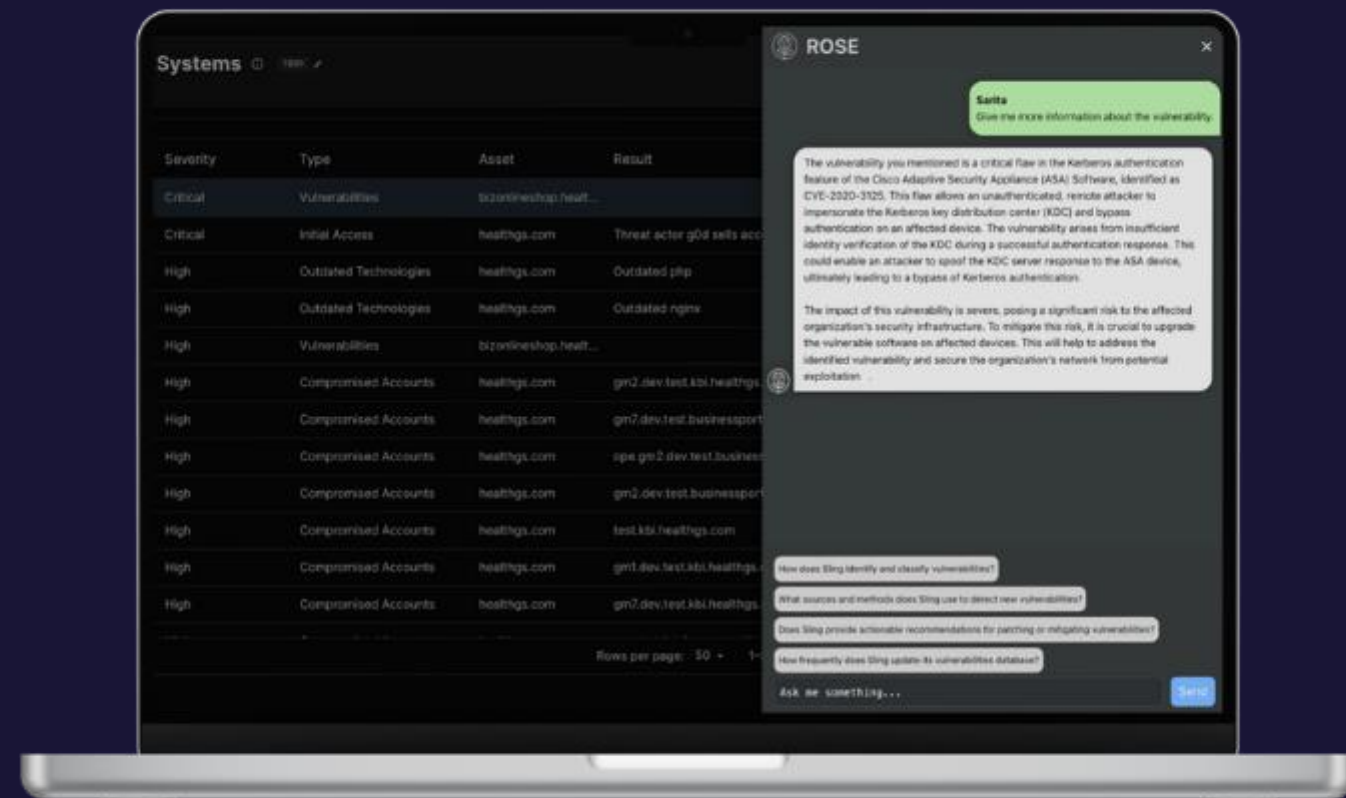
自己申告のみに頼らず、文書化されたリスクスコアリングと是正措置を実施する。

対象セクター

金融、製造、エネルギー、重要インフラ事業者が直接の対象となる。

当社のソリューション

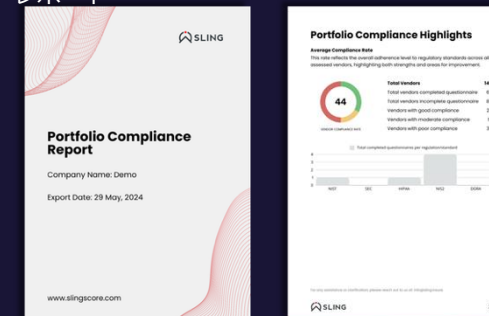
AIネイティブなリスクの詳細分析



ROSE AI

- 特定リスクと検知に関するインサイトを提供。
- コンテキストと是正措置のライブエンリッチメント。

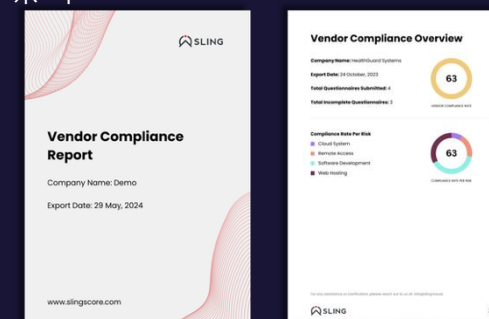
Sling ポートフォリオ・コンプライアンス・レポート



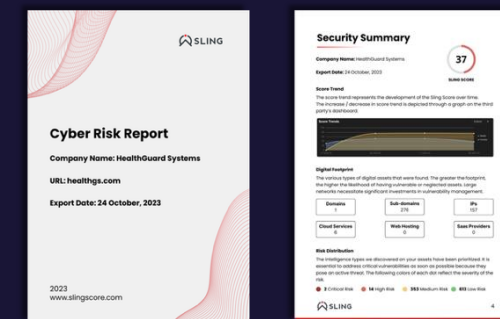
Sling ポートフォリオ概要レポート



Sling ベンダー・コンプライアンス・レポート



Sling サイバーリスク・レポート



レポート

- 実行可能なインサイト、監査対応レポート、是正措置のガイドライン。

なぜSlingなのか

グローバル視野に基づいたセキュリティ運用向上を狙った設計・開発

SLING

競合他社

ネイティブな日本語対応

インターフェース、検知結果、レポートはすべてネイティブな日本語に対応。英語、スペイン語、ポルトガル語にも対応。

多くの場合、英語が優先されており、日本語対応があっても部分的、またはドキュメントのみにとどまることが多い。

完全統合された24時間365日のCTI

24時間365日のダークネット監視と、10年以上の独自CTIデータを保有。

インテリジェンスは多くの場合、サードパーティのフィードや買収によるアドオンとして提供され、スコアの重み付けが開示されることはほとんどない。

高い操作性と組み込み型マルチテナント機能

エージェントレスでドメインのみでオンボーディング可能。24時間以内に完全なリスク像を把握でき、マルチテナント機能がアーキテクチャに組み込まれている。

深さの多くはベンダーの協力次第であり、事業部門ごとの分離には通常、追加の設定作業が必要となる。

一目瞭然のスコアリング

0~100の単一スコアで表示。攻撃の発生確率を予測し、次に悪用される可能性が最も高い順に検知結果をランク付けする設計。

アルファベット評価や幅広い数値尺度では、ニュアンスが大まかな区分に圧縮されてしまう。

ロードマップ

Slingの今後の展望



AI生成レポート

プラットフォームの検出結果から直接生成される、文章形式のリスクリポート・概要



ベンダーの自動検出

組織のサードパーティおよびフォースパーティを自動的に特定し、Slingの資産検出をベンダー層にまで拡張する



ROIと事業継続への影響

サイバーリスクを、企業収益への潜在的影響という観点から定量化する。



SLING

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