TERILOGY NEWS RELEASE

2025 年 11 月 4 日
株式会社テリロジー

テリロジー、SaaSセキュリティのリーディングカンパニーである
Obsidian Securityと販売代理店契約を締結
～業界最大級のSaaS侵害データベースにより、SaaS環境の脅威と設定ミスを
包括的に管理、企業のサイバー防御力を強化～

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」）は、Obsidian Security, Inc.（本社：米国カリフォルニア州、以下「Obsidian Security 社」）と日本における販売代理店契約を締結し、Obsidian Security 社製品の販売を開始したことをお知らせいたします。

近年、クラウドサービス、とりわけ SaaS アプリケーションは企業活動に不可欠な基盤となり、その導入が加速しています。一方で、設定ミス、不適切な権限管理、把握されていないシャドーIT や生成 AI アプリケーションといった脆弱性が拡大し、組織のセキュリティリスクを高めています。さらに、SaaS を標的とした攻撃はユーザーアカウントの認証情報の窃取を狙う傾向が強く、従来型の境界防御やエンドポイント対策では防ぎきれない新たな脅威となっています。

こうした状況を踏まえ、当社は、SaaS 環境における脅威検知とリスク管理に特化した Obsidian Security の取り扱いを開始しました。Obsidian Security は、SaaS アプリケーションの設定や権限管理を可視化・最適化し、誤設定やコンプライアンス違反を防ぐ SaaS セキュリティ体制管理（SaaS Security Posture Management, SSPM）と、アカウント乗っ取りや認証情報の窃取など、アイデンティティを狙った攻撃の検知・対応（Identity Threat Detection and Response, ITDR）の 2 軸で、SaaS 環境における高度な脅威を抑止します。

また、これらの機能を支えているのは、Obsidian Security 社が保有する業界最大級の SaaS 侵害データリポジトリです。これは、同社独自のデータ収集および分析基盤により構築されたもので、これまでに 500 件を超えるインシデントレスポンスへの関与を通じ、SaaS がどのように侵入されるのかに関する膨大なデータを蓄積してきました。こうして形成された豊富なデータリポジトリにより、SaaS に内在するリスクを**網羅的かつ高精度**に評価することが可能となっています。

テリロジーは、Obsidian Security 社製品の提供を通じてお客様の SaaS 環境を守り、安全で信頼性の高い社会の実現に貢献します。

■ Obsidian Security 社について

Obsidian Security 社は、SaaS 環境の脅威検知とリスク管理に特化したソリューションを提供し、アカウント乗っ取りや設定ミス、不適切な権限管理などによる SaaS 関連のサイバーリスクを抑制します。

同社は Menlo Ventures や Norwest Venture Partners、Greylock などの著名な投資家からの出資を受け、これまでに累計 1 億 1,950 万ドルの資金調達を実施しています。

Obsidian Security 社の詳細については、https://www.obsidiansecurity.com/をご覧ください。

■ 株式会社テリロジーについて

株式会社テリロジーは、1989 年に会社設立、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つのセグメントを中核に、市場および顧客ニーズに対応したハードウェアからソフトウェア、サービス提供までの幅広い製品を取り扱うテクノロジーバリュークリエイターです。顧客は大企業や通信事業者を中心に 300 社を超え、ネットワーク関連ビジネスならびにサイバーセキュリティ分野にて豊富な経験と実績を有しています。
（https://www.terilogy.com/）

■ Obsidian Security の製品機能

1. SaaS のポスチャー管理（SSPM）
   従業員が利用する SaaS アプリケーションの設定ミスやコンプライアンス遵守状況を継続的に可視化・評価します。アプリケーションの設定データやユーザーアクティビティを定期的に取得し、常に最新の状態を把握します。

2. アイデンティティ脅威検出と対応（ITDR）
   機械学習モデルにより、ユーザーアカウントや認証情報の悪用、不正アクセスなど、アカウントを狙った異常な行動や脅威をリアルタイムで特定します。アプリケーション設定が適切であっても発生し得るトークンやセッションの盗難、多要素認証（Multi-Factor Authentication, MFA）の回避といった残存リスクを低減します。

3. シャドーSaaS と生成 AI アプリケーションの管理
   企業が利用を把握していない SaaS や、データ漏洩リスクを伴う生成 AI アプリケーションの利用をブラウザレベルで検出・可視化します。これによりアタックサーフェスを縮小し、企業情報の流出を防止します。

4. スピアフィッシング攻撃からの防御
   特定の個人や組織を狙った巧妙なフィッシング攻撃に対し、ブラウザ拡張機能がリアルタイムで不正サイトを検出し、資格情報が入力される前にブロックします。メールセキュリティをすり抜く攻撃や MFA の回避といった高度な手口に対しても有効です。

5. サードパーティーリスクの可視化と管理
   SaaS アプリケーションに接続されているサードパーティー製アプリケーションや連携サービスを特定し、サプライチェーン経由の攻撃リスクを評価します。これにより、想定外の外部侵入経路を特定・管理できます。

6. 運用効率化とロールベースアクセス制御（Role-Based Access Control, RBAC）
   SaaS アプリケーションの各オーナーが役割に応じて適切なアクセス権限を持てるよう、きめ細かなアクセス制御を実現します。また、検出された脅威やポスチャー上の問題に対し、優先順位を付けた修復手順を提示することで、セキュリティインシデント対応を最適化します。

本件に関するお問い合わせ先

【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
担当部署：事業推進本部
クラウドセキュリティ事業部
TEL：03-3237-3291、FAX：03-3237-3293
e-mail：cloudsolution@terilogy.com

【報道関係者お問い合わせ先】
株式会社テリロジー
マーケティング（広報宣伝）
担当 齋藤
TEL：03-3237-3291、FAX：03-3237-3316
e-mail：marketing@terilogy.com