2024 年 10 月 29 日
株式会社テリロジー

テリロジー、独自DBを活用したWing Security社SSPMソリューション提供開始 ～社員が無断で使うシャドーSaaSやWebサービスを可視化、SaaS上の生成AIによる情報漏洩リスクも把握～

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、イスラエル Wing Security Ltd.（本社：テルアビブ、以下「Wing Security 社」）と日本における販売代理店契約を締結し、Wing Security Platform の販売を開始したことお知らせいたします。

現在 SaaS は、多くの企業において不可欠なツールとなっています。財務会計、営業管理、メール、チャット、ファイル共有、名刺管理等、企業単位で利用するものに加え、タスク管理やメモ等、個人単位で利用するものも普及しており、業務のあらゆるシーンで SaaS が活用されるようになりました。しかし、その利便性や導入の容易さも相まって、情報システム部門やセキュリティ管轄部門で管理・把握できていない SaaS の利用が企業内で増えています。その結果、情報漏洩やサイバー攻撃といったセキュリティリスクの増大に加え、SaaS の適切な管理や統制の課題に直面しています。このような課題に対応するためには、全社的に使用されている SaaS の可視性向上が不可欠であり、同時に、SaaS の利用を適切に制御してリスクを最小限に抑えるためのガバナンス体制の強化が求められます。

Wing Security は、社内で利用されている SaaS や Web サービス（以下、SaaS）を可視化し、リスクを分析することで、安全な SaaS 利用を実現するための SSPM ソリューションです。Google Workspace や Microsoft 365 など、企業の基幹業務に不可欠な SaaS に接続されている SaaS や、企業で使用を許可していないまたは把握できていない SaaS を自動的に検出します。検出された SaaS は、30 万件以上の情報を収録した Wing Security 社独自のデータベースにより安全性が評価されるため、リスクのある SaaS を簡単に特定することができます。また、SaaS 内で利用されている生成 AI の有無や SaaS 内のデータが AI の学習に活用される可能性についても確認します。さらに、検出された SaaS におけるユーザーの利用状況や権限設定、長期間未使用のアカウントなどの情報も可視化することができ、SaaS 管理としての機能も備えております。テリロジーは、Wing Security 社製品の提供を通じて、お客様の SaaS セキュリティの強化を積極的に支援してまいります。

■Wing Security 社について

Wing Security 社は、SaaS 関連の脅威から組織を守ることに特化したサイバーセキュリティソリューションのリーディングプロバイダです。最先端のテクノロジーと専門の研究者チームを擁する Wing Security 社は、各組織の独自のニーズに合わせた包括的なセキュリティソリューションを提供しています。

Wing Security 社の SaaS 脅威インテリジェンスおよびその他の機能の詳細については、https://wing.security 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/）

■Wing Security の製品機能

1.シャドーSaaS の自動検出
Google Workspace や Microsoft 365 など、企業の基幹業務に不可欠な SaaS に接続されているアプリケーションや、従業員が使用している SaaS を自動的に検出します。

2.30 万以上の SaaS が収録されている独自のデータベースによる安全性評価
検出された SaaS は Wing Security 社独自のデータベースと参照され、レピュテーション スコアを生成します。これにより、検出された SaaS が安全かを簡単に判断することができます。

3.SaaS 内データの漏洩に繋がるリスクの検知
現在、複数の SaaS を連携する仕組みである OAuth の利用が普及しています。この仕組みにより、ID やパスワードを入力せずに情報の受け渡しが SaaS 間でできるようになった一方、OAuth を悪用した攻撃によるデータ侵害のリスクが高まっています。Wing Security では、OAuth の高い権限が付与されている SaaS や、長期間利用されていないアカウント等、情報漏洩に繋がるリスクを検知します。

4.リスク管理の手間を削減する自動ワークフロー機能
Wing Security では、検出されたリスクに自動で対応するためのワークフロー機能を搭載しています。ワークフローはカスタマイズが可能になっており、お客様にて自社に適したプロセスを作成することができます。

5.生成 AI によるプライバシー侵害リスクの可視化
Wing Security では同社独自のデータベースを基に、検出された SaaS に生成 AI が利用されているか、その場合、SaaS 内のデータが AI の学習に活用されている可能性があるか、また、学習に関する設定が可能かを SaaS ごとに可視化します。

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：asat@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 齋藤清和
TEL：03-3237-3291、FAX：03-3237-3316
e-mail：marketing@terilogy.com