News Release

2025 年 5 月 27 日
SCSK セキュリティ株式会社

攻撃者視点での脆弱性把握と悪用可能性に基づく分析を実施する「ASM(アタック・サーフェイス・マネジメント)」を提供開始
～攻撃者の視点を踏まえたリスクの調査と評価～

SCSK セキュリティ株式会社(本社:東京都江東区、代表取締役社長:小峰　正樹、以下 SCSKセキュリティ)は、外部公開 IT 資産と脆弱性の適切な管理に貢献する新サービス「ASM(アタック・サーフェイス・マネジメント)」の提供を開始いたします。

1. 背景

近年、企業の IT 資産管理において、外部公開資産の脆弱性がサイバー攻撃の主要な入口として注目されています。DX、クラウド化の推進に伴い外部に公開される IT 資産が増加していることから、企業が把握しきれない「管理漏れ資産」や「野良サーバ」が発生しやすくなり、これらがセキュリティ対策の盲点となるケースが増えています。このような背景から、外部公開資産を継続的に監視し、脆弱性や潜在的なリスクを特定・管理する手法である ASM の必要性が高まっています。

従来の ASM では、CVSS/B などのスコアリングを基に脆弱性の優先順位を付けることが一般的でしたが、実際の被害リスクを把握することが困難でした。検出された脆弱性の利用されやすさ(攻撃方法が公開されているなど)や、実際の攻撃実績など、いわゆる「悪用可能性」を考慮して評価しなければ、正しいリスクを把握することはできません。

今回提供予定の ASM サービスは、従来の ASM とは異なり、この「悪用可能性」に基づいた評価ができる点が特長です。例えば、ランサムウェアに関連する脆弱性や、過去の攻撃事例がある脆弱性、リモートコード実行が可能な脆弱性など、攻撃者が悪用する可能性の高い脆弱性を優先的に特定することができます。これにより、実際のリスクを見極め、効率的かつ効果的なリスク対応を実現できるのが、この ASM サービスの大きな特長といえます。

2. サービス概要

SCSK セキュリティが提供する ASM では、攻撃者目線での脆弱性の発見と「悪用可能性」に基づく分析を通じて、発見した脆弱性に対して適切な優先順位付けを行い、効率的な検証を実施できるように支援します。ツールの導入から悪用可能性の分析と検証までトータルに対応することが可能です。

3. サービスの特長

SCSK セキュリティの ASM では外部公開 IT 資産に関する脆弱性について「検知」と「優先順位付け」を実施することで実践的な脆弱性管理を支援します。

1. 「検知」
ASM ツールを用いて、外部公開 IT 資産とその脆弱性を網羅的に特定・検知します。自動スキャンにより継続的に外部公開 IT 資産と脆弱性を把握可能にします。

2. 「優先順位付け」
検出された脆弱性に対してエクスポージャ分析(※)を実施し、ビジネスへの影響度や攻撃の容易さを考慮した悪用可能性に基づいて対処の優先順位を設定します。
※検出した脆弱性のうち悪用可能な脆弱性に絞り込み、脆弱性の概要から対策まで調査・整理する。

結果として、分析結果から悪用可能性の高い脆弱性が明確になるため、この分析結果を活かして、例えばペネトレーションテストの実施に繋げ、脆弱性に対する「検証」を実施することも可能です。

このように脆弱性の検知から検証のサイクルを継続的に回し続けることにより、お客様の適切な脆弱性管理の実現に寄与します。

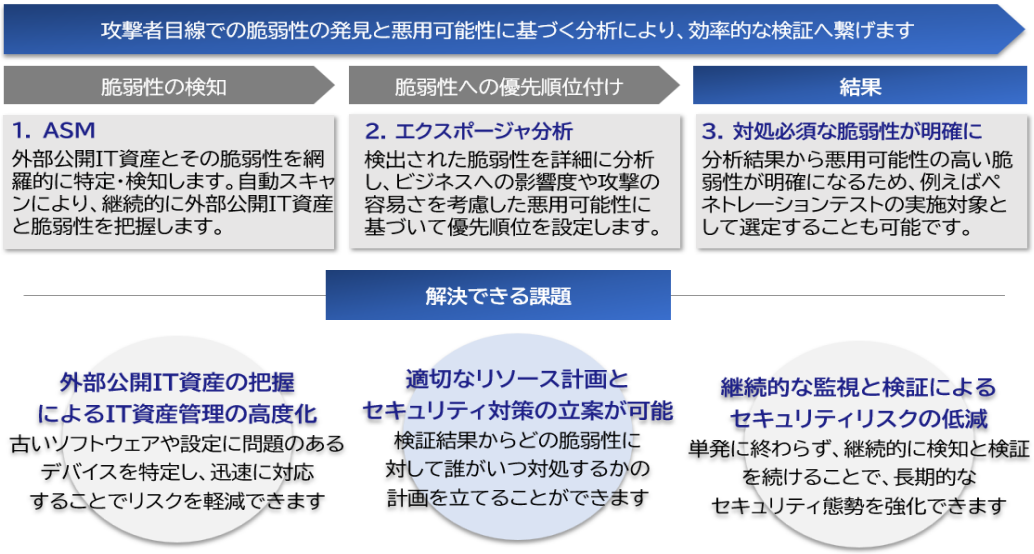
4. サービスメニュー

「検知」「優先順位付け」を含んだ ASM サービスを 130 万円～で提供します。「検証」についてはオプションでペネトレーションテストを利用していただくことで、実施することが可能です。

【標準サービス】
・ASM ライセンス ※1
・エクスポージャ分析
・分析結果報告レポート

【オプション】
・ペネトレーションテスト
・スキャン結果の精査 ※2
・定期運用サービス ※3

その他、別途お客様ニーズに合わせてサービスメニューをご用意させていただきます。
※1…標準サービスでは、50 資産まで外部公開 IT 資産を検知可能です
※2…検知した外部公開 IT 資産がお客様資産かどうかの精査を実施させていただきます
※3…弊社にて都度、エクスポージャ分析を実施し、報告書を提出させていただきます



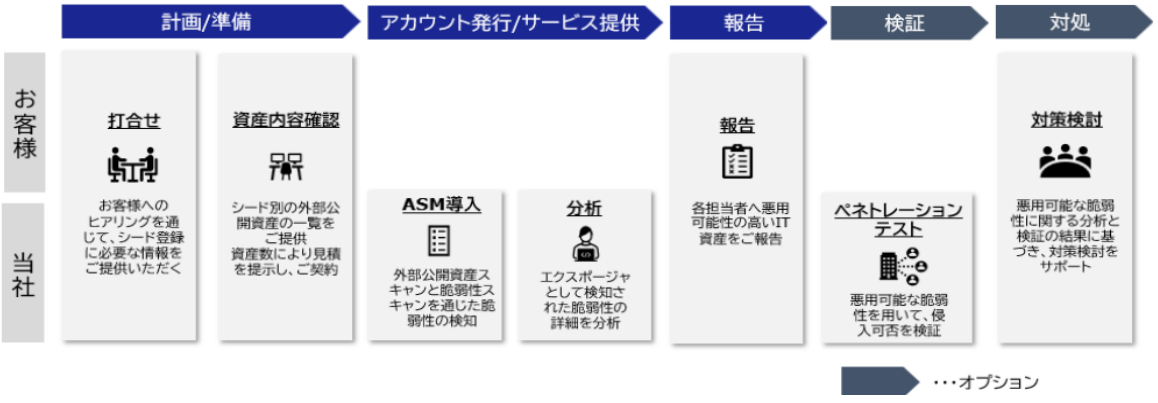
5. サービス提供の流れ

当社 ASM サービスでは、以下のプロセスを通じてお客様のシステムの安全性を徹底的にサポートいたします。

まず、診断の基盤となるスキャン用シードをご提供いただいた後、ASM ツールへの登録を迅速に実施いたします。その後、ツールによるスキャン結果を取りまとめたレポートをご提出し、さらに、悪用される可能性のある脆弱性に関する詳細な分析レポートを提供いたします。

また、オプションサービスとして、ペネトレーションテストをご用意しており、これによりお客様のセキュリティ対策状況をより深く評価し、具体的な対策検討をサポートすることが可能です。

これらのプロセスを通じて、お客様のシステムが直面する潜在的なリスクを可視化し、最適なセキュリティ対策を実現するため支援いたします。



6. 今後のサービス展開

SCSK セキュリティは、IT 資産管理ツールとの連携による IT 資産管理の自動化を目指し、本サービスメニューを順次強化していく予定です。

7.SCSKセキュリティについて

SCSKセキュリティは、サイバーセキュリティ対策に特化したSCSKグループの専門事業会社です。SI事業で培ったコンサルティング・基盤構築・運用サービスと、最新技術を活用した高品質なプロダクトを組み合せることで、顧客企業のサイバーセキュリティリスクを低減するとともに、セキュリティ領域における投資対効果を最大化させ、安心・安全な社会の実現に貢献いたします。

商号	:SCSKセキュリティ株式会社
代表者	:代表取締役社長 小峰 正樹
本社所在地	:東京都江東区豊洲 3-2-20
出資比率	:SCSK株式会社 100%
事業内容	:セキュリティサービス開発・販売(コンサルティング、脆弱性診断/評価、トレーニング等)、セキュリティ製品販売
URL	:https://scsksecurity.co.jp/

8.SCSKグループのマテリアリティ

SCSKグループは、経営理念「夢ある未来を、共に創る」の実現に向けて、社会と共に持続的な成長を目指す「サステナビリティ経営」を推進しています。

社会が抱えるさまざまな課題を事業視点で評価し、社会とともに成長するために、特に重要と捉え、優先的に取り組む課題を7つのマテリアリティとして策定しています。

本取り組みは、「安心・安全な社会の提供」「多様なプロフェッショナルの活躍」に資するものです。

－高度化・巧妙化するサイバー攻撃への対策強化による、サイバーセキュリティリスクの低減

－最新かつ高度な知見の提供による、セキュリティレベルの向上

9.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】
SCSKセキュリティ株式会社
ビジネス開発本部 ビジネス開発部 ASM 担当
E-mail:sys-info@scsksecurity.co.jp

【報道関係お問い合わせ先】
SCSKセキュリティ株式会社
管理本部 コーポレートマネジメント部 広報担当 森田、太田
E-mail :Yasuyuki.Morita@scsksecurity.co.jp
:Sayaka.Ohta@scsksecurity.co.jp