

# 大学・学術研究機関における ASM 調査結果と運用のありかた

中島 彬<sup>1)</sup> 阿部 信児<sup>2)</sup>

1) KELA 株式会社 2)株式会社ソフトクリエイト

## ASM Survey results and how to operate them at universities and academic research institution

Akira Nakashima<sup>1)</sup>, Abe Shinji<sup>2)</sup>

1) Kela, KK. 2)Softcreate Corp.

### 概要

近年、初期の攻撃経路として脆弱性の悪用や不正に窃取されたアカウントを悪用した事案が増加している。また、初期侵入から目的達成までの時間も短くなってきている。これらを踏まえ、「侵害された後にいかにインシデントをハンドリングするか」という対策の重要性が増大する一方で、「いかにして攻撃者と同様の観点で組織を保護するか」という対策の重要性も語られることが多くなってきた。産業界においては「アタックサーフェスマネジメント」と呼ばれる、外部から収集される情報をもとに、対処する脆弱性等の優先順位づけを行う試みが盛んに議論・導入・運用され始めている。一方、大学・学術研究機関においては、限定的なリソースの中で、学内の各種システムそれぞれに関連するステークホルダーの所有デバイス、または、ユーザーアカウントを企業のように細かく管理する難しさもある。そこで、本稿では実際に「アタックサーフェスマネジメント」ツールに類される製品で調査を行なった結果を共有するとともに、効果的な運用に求められる要件を提供する。

### Abstract

In recent years, the number of cases in which vulnerabilities are exploited or illegally stolen accounts are exploited as initial attack routes has increased. In addition, the time between the initial intrusion and the achievement of the objective is becoming shorter. In light of these trends, the importance of countermeasures for “how to handle incidents after a breach” is increasing, while the importance of countermeasures for “how to protect the organization from the same perspective as the attacker” is also being discussed more and more. In the industrial world, “attack surface management,” an attempt to prioritize vulnerabilities to be addressed based on information collected from outside, has been actively discussed, introduced, and operated. On the other hand, universities and academic research institutes have limited resources, and it is difficult to manage the devices and user accounts of stakeholders related to each of the various systems on campus in as much detail as companies do. Therefore, in this survey, we will share the results of an actual survey of “attack surface management” tools and examine the requirements for effective operation.

## 1. はじめに

近年、サイバー攻撃は多様化・高度化しており、初期侵入経路として脆弱性の悪用や不正に窃取されたアカウントの利用が顕著に増加している。[1] これらの攻撃者の手法は、組織内におけるセキュリティ対策の脆弱な部分を的確に突いており、侵入後から目的達成までの期間も短縮傾向にある。

[2] このような背景から、単に「侵害を防ぐ」のではなく、「侵害された後にいかに迅速かつ適切に対応するか」という事後対応能力の強化が重要視されている。また同時に、「攻撃者と同様の視点でリスクを特定・評価し、予防的に対策を講じるアプローチ」への関心も高まっている。今回は、後者の予防的な施策に対する検討・事例紹介を行う。

## 2. アタックサーフェスマネジメントの概念

経済産業省は、2023年に「ASM（Attack Surface Management）導入ガイドンス～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」[3]を発表した。これによると、「ASM（Attack Surface Management）は、組織の外部（インターネット）からアクセス可能なIT資産を発見し、それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセス」と定義されている。これを踏まえ、産業界においては、ASMの有用性が認識されはじめており、特に大規模な企業ではその導入・運用が進んでいる。ASMツールは、脆弱性評価やクラウド資産のリスク評価、外部の脅威インテリジェンスとの統合など、いくつかの導入目的と整合性を調整の元、施行されている。一方で、こうした手法を大学や学術研究機関で活用するには、いくつかの特有の課題が存在する。たとえば、大学は多くの場合、限定的なリソースで複数のシステム、クラウドサービスを管理している。また、場合によっては、教員や学生といった所有デバイスを限定することが好ましくない状況や、ユーザーアカウントが複数にわたり、これらを統合的に把握することが難しいといった課題が挙げられる。これらを踏まえ

ると、企業のように高度なASMプロセスを適用することはしばしば困難である可能性が高い。一方、2024年に大学機関より報告された不正アクセスに関連する公表を調査すると、「メールアカウントの不正アクセス」「研究室サーバーの不正アクセス」「外部公開サイトの改ざん」といった事案が発表されている。

## 3. 調査結果

今回調査を行なった対象機関は今年8月以降に不正アクセスにまつわるプレスリリースを行なった大学機関を調査した。11機関を調査した結果、11機関のうち全てにダークウェブに流出しているメールアドレスがあることが確認されている。ここでダークウェブと記載している対象は必ずしも特定のブラウザにてのみアクセスしうる先のみと定義しているわけではなく、一部のSNSツールにて構成されるグループチャット等も調査対象に含めている。また、情報窃取型マルウェアに関連している流出情報を集計した結果、Redlineを筆頭に、Lumma、Vidar、Racoon2、RacoonとSetalC、MetaStealerといったマルウェアからの流出情報が確認される。本パートはむやみに関係者を驚かせることを目的としておらず、あくまでも現状把握のプロセスの一環として報告していることに留意いただきたい。そもそも、アカウントの流出は必ずしも不正なプログラムに基づいて該当のデバイスから流出するだけでなく、登録先のサービスの侵害に紐づいた共有等からも発生する。しかしながら、情報窃取マルウェアから窃取された情報の共有等、即座に悪用可能な流出の形態も確認されている事案が増加しており、注意をするべき領域である。実情を踏まえた対策としては、二要素認証の徹底をはじめ、流出が確認されたタイミングでのパスワードのリセットなど、インフラストラクチャ側から提供されている流出有無情報も一つの参考情報となる。また、今回対象とした11機関の関連資産より調査を行なった結果、全2908アセットのうち、ポート21(FTP)の開放は156件、ポート22(SSH)の開

放は110件、ポート3389(RDP)のか違法は0件確認された。関連ドメインの探索ロジックは必ずしも組織の保護責任を持つ資産と同等の数量発見されるわけではないため、組織の攻撃面と同義ではないものの、一定数の対処資産が存在することが想定される。今回は一部割愛して記載しているため、組織のアセットを探索する手法については、改めて経済産業省の定義するASM導入ガイダンスを参照されたい。

#### 4. 考察

これらのツールは外部からの攻撃リスクの「可視化」において一定の効果を発揮することが確認された。一方で、このアタックサーフェスマネジメントに関連する分野が明らかにする組織課題は必ずしも新しい技術領域であるわけではなく、これまでも有用性が確認されている取り組みであることは明らかである。一方、オンラインにおける組織の情報資産を取り巻く状況は刻一刻と変化し続けており、組織の境界を一度定義したとしても、その境界の元運用が永劫続くとは到底安心できない。また、学術機関のようなリソース制約下における実運用には、リスクとして可視化するだけにとどまらず、優先順位付を行なった上で、関係者との合意形成と、リスク種別に応じた対応フローを構築することが求められる。一例を挙げると、教職員アカウントのダークウェブへの漏洩と、適切でないネットワーク設定が明らかになった際、通常のセキュリティ製品がアラートを発砲しないとは限らない。対処指示を並行して行うには、根本となる運用方針や、適切な合意プロセスに基づいた理解を得る必要がある。アタックサーフェスマネジメントに関連する製品についてはプロアクティブな活動であることを念頭に起きつつ、他のセキュリティ製品のように、侵害が疑わしいアラートや、侵害後のアラートではない点との対処タイムラインを定義づけるとともに、導入・運用部門の検討並びにゴールイメージを確保することが必要である。

#### 5. 参考文献

[1] IBM、X-Force 脅威インテリジェンス・インデックス 2024、

8ページ、2024年

[2] Mandiant、M-Trends2024、8ページ、2024年

[3] 経済産業省、ASM (Attack Surface Management) 導入ガイダンス 外部から把握出来る情報を用いて 自組織の IT 資産を発見し管理する、2023年