大学環境における攻撃対象領域管理の導入とその活用

細川 達己 [1)]

1) 慶應義塾 CSIRT

hosokawa@keio.jp

Implementing and Leveraging Attack Surface Management in a University Environment

Tatsumi Hosokawa [1)]

1) CSIRT, Keio University

概要

大学の情報セキュリティに関しては、従来から大学という組織特有のさまざまな事情からその強化を妨げる要因が多数存在していたが、昨今のクラウド化や暗号化技術の普及によって、大学環境の制限下で取り組んできた対策が、さらに困難なものとなってきた。

慶應義塾では、この問題への対抗策の一つとして、攻撃対象領域管理（ASM）を導入した。これは、重大なインシデントに発展する可能性のある、軽微なインシデントの早期発見を目的としたものである。

本稿では ASM の導入決定に至った理由やその導入に関係して考慮した各種事項、そして 1 年間の運用を経た後の評価などについて述べる。

1 はじめに

近年、経済産業省から導入ガイダンスが公開される[1]など、注目されている情報セキュリティ関連ソリューションの 1 つが攻撃対象管理（Attack Surface Management、以下 ASM）である。

慶應義塾では、2022 年度から 2024 年度にかけて ASM を導入し、現在 CSIRT の日常業務に広く活用している。

本稿では、本学における ASM の導入に至る背景と実際の導入過程、導入後の効果などについてまとめ、報告する。

2 背景

2.1 慶應義塾における従来のセキュリティ強化

以前より、大学における情報セキュリティ強化には、一般企業と比較して多くの不利な要因があった。以下に例を挙げる。

1. 大学という環境の自由さ
2. 教員や学生に対する情報ガバナンスのレベル
3. 資産管理の困難さ
4. 非常に多数の IP アドレス
5. 非常に高速なネットワーク
6. 情報システムを利用するユーザの多さ

このうち 1.から 3.は組織の性質に起因する問題であり、4.から 6.は機器やサービス導入時のコストに関連する問題である。

このような制約の中で、本学ではネットワークの通信トラフィックや DNS、統合認証などのログを監視対象とすることで、様々な情報セキュリティ上の問題を外部の指摘によらず発見するための手段としてきた。

その手段として、2003 年から PostgreSQL ベースのログ収集サーバなどを内製し[2][3]、常に改良を加えながら運用してきた。このシステムは学内のサブネット管理者に、管理対象ネットワークのトラフィック情報を提供するシステムを兼ねている。現在では約半年分のログに相当する約 4,000 億行のデータを高速に検索可能なシステムとなっており、状況に応じてネットワーク機器に対する自動的な操作を行う機能も付加されている。

2.2 近年出現してきた多くの制約

ところが、近年ではこれらの対策の効果を低減させる技術が多数出現し、普及が進んでいる。以下に例を挙げる。

- クラウドを利用するサーバの増加
- 常時 TLS の一般化
- DNS over HTTPS（以下 DoH）

- SNI 暗号化
- 匿名 VPN の一般化

クラウド利用の増加は、それらのサーバの通信を直接監視することが不可能となる。常時 TLS は、Web トラフィック監視におけるパケット内部の分析を無効化する。DoH は DNS ログの監視と DNS セキュリティを回避する。SNI 暗号化は、常時 TLS 化の中でわずかに残ったパケット内部の手がかりを無効化する。匿名 VPN はクライアントからの通信に関して、トラフィック監視と DNS ログの監視、DNS セキュリティの全てを完全に無効化する。

これらの例のうち、クラウド利用以外は全て、ISP や第三者による検閲・監視への懸念から発生している暗号化ベースの技術であり、大学が学術の自由を尊重する場であるがゆえに、企業ネットワークのように一律で暗号化通信を禁止、解読することには難しい側面がある。

また DNS over HTTPS は、現在では多くのブラウザや OS の標準リゾルバに統合されている。匿名 VPN は、多数の商用アンチウイルスソフトの機能の一部として提供されており、ユーザが意識せずに利用している場合も多いほか、Apple 社の iCloud+ （iCloud プライベートリレー）などの一般的サービスにも含まれている。

一方で、研究上の機密情報や多様な個人情報などを持つ組織としての大学のネットワークを管理する立場から考えると、大部分のトラフィックや DNS 情報が監視できなくなることは、潜在的に大きな問題である。

2.3 これらの新しい制約への一般的な対応

このような新しい制約が普及していく中で、一般的には次のような対策が考えられる。

- 暗号化通信の通信経路上での解読
- 端末への EDR/XDR エージェント導入

しかしこれらの対策はいずれも、大学においては（職員環境以外に）広範囲に導入するには、主に以下に挙げる理由により、大きな困難を伴う。

- BYOD 端末や研究室の機器、自宅設置の機器など、統一された導入体制や管理体制にない情報機器が非常に多い。
- 特に学生の利用する情報機器などにおいて、暗号解読や端末上の詳細な情報の収集にはプライバシーの観点から大きな問題がある。
- 教員、学生の人数が多く、また使っている情報機器の数も膨大であり、費用的な問題が大きい。

また、これらの新しい暗号化技術等の利用をユーザに禁止して、ファイアウォールによるアクセス制限を行うことで対応することも考えられるが、新技術が必要なユーザにはそれらの利用を困難なものとしてしまう上に、完全な排除は技術的に非常に難しい。一方悪意ある攻撃者からは容易に制限の回避が可能であり、効果は限定的である。

3 インテリジェンスを重視する方針

このような問題意識のもと、本学では 2019 年からインテリジェンスを重視する別のアプローチを検討し、複数のシステムを導入してきた。

大きく分けて、サイバー脅威インテリジェンス（Cyber Threat Intelligence、以下 CTI）と、本稿の主題でもある攻撃対象管理（Attack Surface Management、以下 ASM）である。

3.1 本学における CTI の利用状況

CTI とは、NIST の定義によると「意思決定に資するよう文脈化された脅威情報」であるが[4]、本稿ではこのような目的で集約、変換、分析、解釈、強化された脅威情報を、顧客に対して提供するサービスのことを指す。

本学では CTI を 2020 年から導入開始しており、現在では複数の CTI を利用している。現在の主な利用目的を以下に挙げる。

- 自組織に関連する脅威情報アラートの把握
- クレデンシャル漏洩情報の入手
- 不審な現象が発見された場合の便利な統合調査ツール
- 匿名 VPN・レジデンシャルプロキシ等からのアクセスの調査ツール
- ログ収集サーバへの IoC 情報のインポートと、自動的なネットワーク機器操作の判断基準となるスコア情報の提供

これらの項目には CTI の定義には該当しないものもあるが、そのサービスの一部として提供されており、日々の運用において有効活用されている。

3.2 本学における ASM の利用状況

ASM とは、経済産業省のガイドラインによると、「外部（インターネット）からアクセス可能な自組織の IT 資産を継続的に発見し、そこに存在する脆弱性等のリスクを検出・評価する一連のプロセス」と定義されており、対象の「攻撃対象（Attack Surface）」は外部公開 IT 資産に限定するとされている[1]。

現在、本学においてASM（もしくはASMに類似するもの）として主に利用しているサービスは、Recorded Future Attack Surface Intelligence（2023年11月トライアル利用、2024年4月正式導入）とShadowserever（2022年12月導入）、Shodan Monitor（2022年5月導入）の3つである。

- Recorded Future Attack Surface Intelligence（以下 RF-ASI）
  商用CTIであるRecorded Future（2020年導入）のASMモジュールであり、Recorded Futureの一機能として提供される。
- Shadowserver
  非営利組織のShadowserver Foundationが提供する、非商用サービス。
  無償で利用可能だが、加入にはAS番号またはCIDRの所有権確認が必要。
- Shodan Monitor
  Shodanが提供する、一定のアドレス集合における新たなアセットや脆弱性等の発見を、継続的にモニターすることができる機能である。大学のネットワーク管理者に対してはAcademic Plusと言う、最大で16ビットマスクのネットワークを、無償で2つまで監視できるプランも提供されている。

無償サービスは、機能は限られるが、RF-ASIを補完する存在として、現在でも重用されている。

本稿では、主に商用サービスの導入とその活用を紹介するが、本学同様、まずは無償のサービスをしばらく利用し、その上で商用サービスの導入を検討するのは良い方針であると考える。

3.3 ASMの導入理由

本学がASMを導入した理由は主に2つ挙げられる。1つは「軽微なインシデントへの対応重視」であり、もう1つは「資産管理の困難さ」である。

「軽微なインシデントへの対応重視」とは、かつて本学で大きなインシデントが発生した際に、その初期段階として、漏洩したクレデンシャルを用いたと思われる不正ログインや、外部からアクセス可能な脆弱性への攻撃が観察されていたことから着想を得たポリシーである。

軽微なインシデントに対して素早く対応することで、それらが重大なインシデントに発展することを防ぐことを目的としている。ASMはこのうち、外部からアクセス可能な脆弱性を減らす効果が期待できる（一方、クレデンシャル漏洩は主にCTIで対応している）。

もう一つの「資産管理の困難さ」であるが、大学には広大なIPアドレス（近年ではさらにクラウドを含む）に多数のIT資産が分散しており、各部門の管理者自身が把握していない資産も多い。また資産の増減も絶えず発生し続けている。セキュリティ対策に利用するため、常に最新の状況を把握しておくためには、情報部門のみならず、部門管理者の人的コストも膨大なものとなってしまう。

そのため、少なくとも外部公開のIT資産に関して、攻撃者側と同じ視点から脆弱性を調査することで、完璧な一覧でもリアルタイム反映でもないものの、セキュリティ対策にはより有用な、資産の把握ができることが期待できる。

4 商用ASM導入検討時の問題

4.1 トライアル段階での問題

商用ASMの導入検討時、複数のシステムを試用したが、その際にフル機能を一定期間利用できる場合と、試用のための調査項目が決まっていて、それ以外のテストがほとんどできない場合（そもそもWeb UIを試用できないケースも含む）があった。

ASMのテストを行うことで、ユーザ側は自組織の脆弱性についての広い知識を得ることができるが、製品評価段階であるが故にトライアルで得た情報を元にしたインシデント対応を行わない、などということは通常考えられない。

フル機能のテストは、原理的にはそれを用いて現状の問題点を全てトライアル期間内で解決できてしまう可能性があることを意味するのではあるが、そもそもASMは単発利用のサービスではない。継続的に利用することで、新しく判明した脅威や新しく出現した、もしくは発見されたアセットに対して対応していくためのツールである。そのためトライアルで多くの情報を提供しても、その後の本格導入が無価値になるわけではない。

製品の提供側としては難しい判断が必要と思われるが、トライアル期間中の大幅な利用機能の制限は、ASMを評価していく上での大きな課題であると考えている。

4.1 課金体系の問題

また、課金体系がIPアドレス単位である場合やアセット数単位である場合は、広いIPアドレス空間を持つ大学の場合だと、非常に高価なライセンス費用となってしまう場合があるので検討が必要

である。いずれもトライアルなどで概数を推計することになるが、トライアルでの推計値は導入後の設定変更により大きく上振れする可能性があるうえ、より多くの対象を管理したくなった場合に、ライセンス費用の上昇とのトレードオフとなる可能性がある。

本学が最終的に導入した RF-ASI は、トライアル期間中にほぼ完全な機能のテストが可能で、なおかつアナリスト数単位の課金体系であったため、人数としては小規模な本学の CSIRT には、非常に適した課金体系であった。

5 商用 ASM 導入後の現状と考察

5.1 クラウドに出ていった情報資産

現在、RF-ASI が認識している IP アドレスベースで約 7%（1,000 件以上）が学外に存在しており、そのほとんどがサーバである。

学外のアセットの検出は非常に有用であるが、限界もある。特に大学の公式ドメイン以外の独自ドメインを取得して、学外の IP アドレスでサービスを運用しているケースの把握は難しい。

独自ドメインでも、ドメインの WHOIS 情報やサーバの TLS 証明書情報から発見できる場合もあるが、これも限界がある。

昨今は WHOIS 情報がプライバシーのために隠されることが多くなっており、特に過去の WHOIS 履歴が存在しない、比較的新しく作成された独自ドメインは、ますます把握が難しくなっている。

TLS 証明書による発見も、Let's Encrypt などで組織情報を持たない証明書が運用されるケースが増加している（学内でのシェアは不明だが、2025 年 9 月現在、TLS 証明書における Let's Encrypt のシェアは 63.3%と見られる[5]）ため、以前と比較して有用性が著しく低下している。

独自ドメインに関しては、ドメイン廃止後の第三者による取得と再利用に伴う問題もあるため、安易な取得をさせないための方策を用意する必要がある。また、独自ドメインを取得した場合には、可能な限り情報センターや CSIRT 側で把握できるようにする制度づくりなどが必要になると思われる。

5.2 アセットのスコアリングの実際

RF-ASI に発見されたアセットの問題点（主に脆弱性）は、そのレベルによって Critical, Medium, Informational の 3 段階にスコアリングされる。導入直後は Critical な脆弱性への対応を中心としていたが、運用経験を積む中で、より重要な視点が必要なことが判明してきた。

その一つは、「場違い」な Medium や Informational な脆弱性に注目する必要があるということである。たとえば、Apache HTTPD の Indexes オプションが有効化されている状態（標準サンプル設定にも入っている）はもちろん Critical な脆弱性ではないが、重要な Web アプリケーションのサーバでこの設定が検出された場合は、情報漏洩を含む重大な設定ミスが含まれる可能性がある。

また、複数の Medium や Informational な脆弱性が組み合わされることで、Critical な問題に繋がる可能性があることも重要である。たとえば Web 公開ディレクトリに無防備に置かれた.git/のディレクトリも、データベースのポートの外部公開もいずれも Critical な脆弱性ではないが、Git のリポジトリをそこから復元され、もしスクリプトのソースやデータベースのアクセス情報が入っていた場合、スクリプトの脆弱性を直接悪用される可能性や、データベースの内容を直接アクセスで漏洩される可能性もある。

現実環境で脆弱性が実質的に Critical かどうかは、実際は脆弱性自体の危険度と脆弱性が発見された場所の双方が関連する上に、複数の脆弱性が組み合わさった上で Critical なインシデントに発展することも多い。一般的な危険度が低い脆弱性だが、それが存在してはならない場所に発見された場合、当該問題を解決することはまさに「軽微なインシデントへの対応重視」という方針の、最も典型的な実践と言えるだろう。

5.3 履歴情報の重要性

導入初期の「発見された脆弱性を重要なものから処理していく」というフェーズが落ち着いたら、必要性が増してくるのが脆弱なアセットの追加履歴と解消履歴のチェックである。

アセットが新たに発見されたり、設定変更で脆弱性が出現したり、新しい検出項目に合致した場合に脆弱なアセットは追加され、アセットが消滅したり、脆弱性を解決したり、検出項目が削除されると脆弱なアセットは解消される。

これを常にチェックすることで、新しいアセットや脆弱性の発見、脆弱性解消のチェックができるだけではなく、ユーザが脆弱性を一旦解消したにもかかわらず、しばらくしたらまた同じ脆弱性を復活させてしまう現象に対しても、重要なチェック手段となる。

このような現象は、システム再起動時に元に戻ってしまう方法でインシデント対応してしまった場合や、システムトラブルで古いバックアップからリストアした場合、そして OS の変更などでシステムの再構築を行った際に、誤って修正前のバージョンのアプリケーションをインストールしてしまった場合など、しばしば発生する。そのため、これを比較的容易にチェックできる点でも、ASM は有用である。

5.5 その他導入後の問題点

ASM 導入後に感じられたその他の問題点として、以下の例が挙げられる。

- 日本国内でローカルな人気のあるソフトウェアの脆弱性への対応は、グローバルなソフトウェアに比べてレベルが落ちる傾向があるように思われる。
- 強い副作用や破壊的な調査を行わないと発見できない脆弱性は、ASM から発見できない。より積極的な調査を行う脆弱性スキャナが必要である。

6 CSIRT 業務における ASM の位置付け

2024 年度に、本学の CSIRT が対応した事象に関して、着手のきっかけとなった契機の内訳を図 1 に示す（具体的な件数は非公表）。

かつてはそのほとんどを占めていた「ログ監視」「ユーザからの連絡」「外部組織からの連絡」を差し置いて、2024 年度は ASM が 37%、CTI が 30%を占めている。

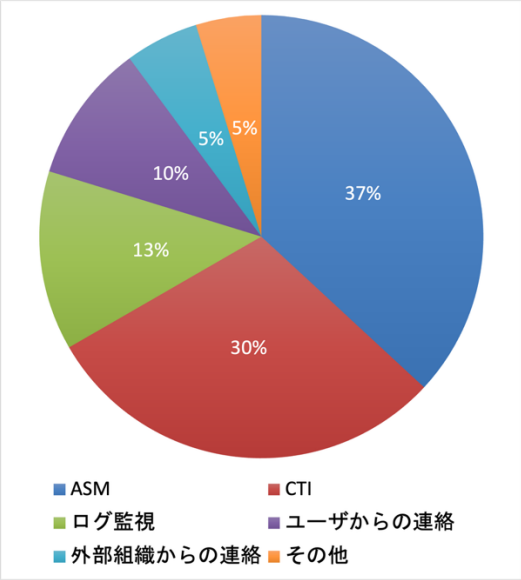

図 1　事象に対する対応の契機別比率（2024 年度）

ただし、このデータは RF-ASI 導入初年度のものであるため、導入初期に検出された多くの脆弱性をまとめて対応したことで、ASM からの対応数が実態以上に増えてしまっている可能性も否定できない。

そこで、2025 年度の概ね前半にあたる、2025 年 4 月 1 日から 9 月 22 日までの期間で暫定集計した同様のデータを図 2 に示す。

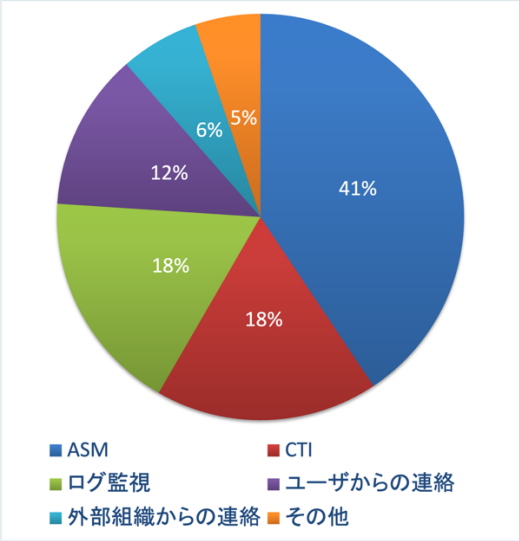

図 2　2025 年度前半の契機別比率

これを見ると、全体的な傾向はそれほど変わっておらず、さらに ASM を契機としてインシデント対応を開始する比率は、むしろ前年度より増えている（37%→41%）ことがわかる。この要因としては、以下の 3 つの理由が考えられる。

- 導入初期にまとめて行う対応に関しては、実は 2023 年度のトライアル時に、すでにかなりの数を実行してしまっていたため。
- RF-ASI を 1 年運用した結果、より効率的に ASM を活用するための経験が溜まってきたため。
- CTI からのクレデンシャル漏洩の処理件数が年々減少傾向にあるため（既出情報が多いので、対応を進めることで件数が減っていく）。

このように、本年度も全体的な傾向の変化は見られないようなので、これらの対応契機が、それぞれどのようなインシデントの対応に役立っているのかについて、2024 年度のデータをもとに分析する。

現在本学の CSIRT では、対応したインシデントの重大性に関して、以下のグループ A～D の 4 種に分類している。これらは、A が最も重大、D が最

も軽微と考えられる分類となっている。

- グループ A：重要情報の窃取、Web 改ざんなど
- グループ B：メール大量送信、踏み台利用など
- グループ C：フィッシング被害、マルウェア感染など
- グループ D：誤設定、脆弱性、クレデンシャル漏洩など

図 1 に示した、2024 年度のそれぞれの対応契機から、最終的にどのレベルのインシデントの対応に至ったかについて集計した比率を図 3 に示す（具体的な件数は非公表）。また調査の結果、対応の必要なインシデントではないと判断されたものは除外している。

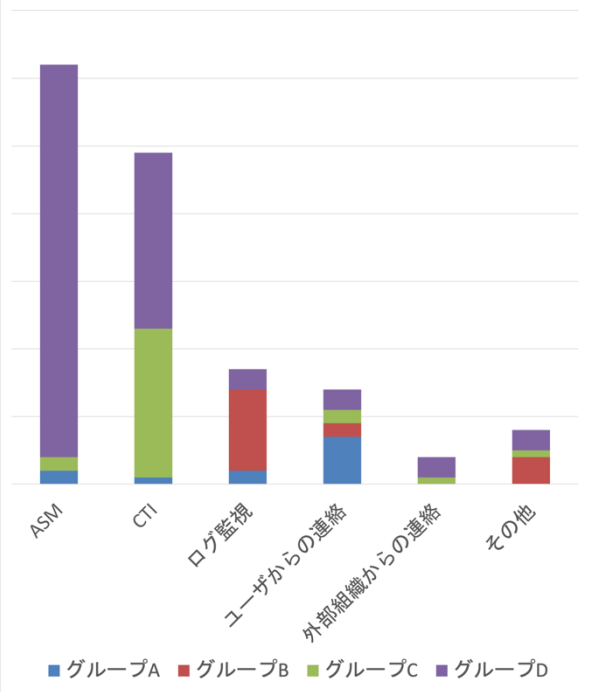

図 3　対応契機別インシデント重要度（2024 年度）

この結果から、本学において ASM はほとんどのケースでグループ D の、最も軽度なインシデントの発見に役立っていることがわかる。これは導入当初から想定されていた通りの効果であり、より重大なインシデントに進展する可能性のある問題点に対処しているものと考えられる。

なお、CTI も同様の位置付けではあるが、グループ C が比較的多数含まれているのは、クレデンシャル漏洩の原因がインフォスティーラーなどのマルウェアであったことが明らかになった場合は、グループ C に分類しているためである。

一方で、ASM からも CTI からも、わずかではあるがグループ A に分類されるに至ったインシデントが発見されているが、これらの場合は ASM や CTI が、より早急に重要なインシデントを発見することに役に立った、と考えることができるだろう。

7 結論・今後の課題

近年普及が進んだサービスのクラウド化や、さまざまな暗号化技術によって、以前から難度の高かった大学のセキュリティ対策がさらに困難になってきてしまったため、インテリジェンスを重視するという文脈のもとで、CTI に続いて ASM を本格的に導入した。

その結果、ASM は主に設定ミスや脆弱なシステムの発見などの軽微なインシデントを発見するために大きな役割を果たしており、CTI とともに「重要なインシデントに発展する小さな芽を摘む」という、導入時の想定通りの役目を担っていると考えられる。

今後の課題としては、現在は RF-ASI を全て Web UI 経由で利用しているため、今後は API を用いた、現在の手順の一部自動化や、危険なアセットの情報に対して、ログサーバ内のデータ検索と組み合わせた自動アラート機能などを実現したいと考えている。

また、RF-ASI は、「SQL Explorer for ASI」という ASI 内のデータをクエリするための SQL ライクなインターフェースも持っている。この機能は現在、ASI 内での各種条件設定などで利用しているが、さらなる活用が可能と思われるため、今後さまざまなテストをしていきたいと考えている。

参考文献

[1] 経済産業省 商務情報政策局 サイバーセキュリティ課「ASM (Attack Surface Management) 導入ガイダンス」、https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html 、2023.

[2] 細川 達己，金子 康樹「大学ネットワークにおけるサブネット管理者とのネットワークセキュリティ・トラフィック情報の共有」大学 ICT 推進協議会 2017 年度年次大会 論文集、2017.

[3] 細川 達己，金子 康樹「『トラフィック情報提供システム』の機能強化」大学 ICT 推進協議会 2018 年度年次大会 論文集、2018.

[4] Chris Johnson, Lee Badger, David Waltermire, Julie Snyder, Clem Skorupka. “Guide to Cyber Threat Information Sharing”, NIST SP 800-150, 2016.

[5] W^{3}Techs. “Usage statistics and market shares of SSL certificate authorities for websites”, https://w3techs.com/technologies/overview/ssl_certificate, 2025.