ASM ツール
アイデア提案レポート

電子遊戯部（１）.exe

新潟コンピュータ専門学校

目次

1. はじめに

1.1 背景と目的

シャドー IT による脆弱性リスクへの対応として、ASM（ATTACK SURFACE MANAGEMENT）ツールを提案します。シャドー IT とは、IT 部門の管理外で利用されている情報システムやサービスのことを指します。

考えられる課題は以下の三つです。

【課題】

- 自社に把握されていないサービスの存在
- IT 資産把握の困難さ
- セキュリティリスクの増大

1.2 チーム概要

メンバー	役割
小池歩（リーダー）	情報収集、レポート作成および全体指揮
権瓶元輝（サブリーダー）	情報収集、レポート骨子作成
馬場樹（メンバー）	情報収集、レポート修正
本間隆一（メンバー）	情報収集、レポート修正

1.3 解決アプローチ

1.3.1 管理外システムの把握

【現状の課題】

・把握されていないサービスの存在
・検証環境の管理不足
・クラウドサービスの把握困難

【解決の方向性】

・外部からの探索
・内部からの監視
・人的情報収集

1.3.2 IT 資産管理の複雑性

・クラウド活用の拡大による IT 資産の増加
・企業の IT 活用の広がりによる IT 資産の増加

1.3.3 IT 資産発見・管理の課題

・新規 IT 資産の継続的な発見
・管理外システムの網羅的な把握
・資産情報の定期的なアップデート

1.3.4 組織的な課題

・セキュリティ意識の不足

次章では、これらの課題に対する具体的な解決策として、複数のアプローチを統合した ASM ツールのアイデアを提案します。

2. ASM ツールのアイデア提案

2.1 アプローチの概要

1. 外部探索：インターネット上からアクセスできるツールを用いた情報収集
2. 内部検知：社内ネットワークのログ監視
3 人的収集：社員からの直接的な情報収集

2.2 統合システム

【解決の方向性】

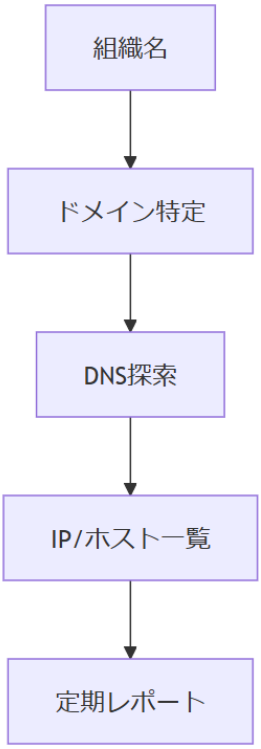
- 一般的なセキュリティフレームワーク（NIST CSF, ISO27001 等）の活用
- OSS の組み合わせ
- 標準的なログ収集・分析手法（SIEM 等）の採用

【各アプローチの特徴】

アプローチ	利点	課題	実現方法
外部探索	自社の公開情報を客観的に把握可能	探索範囲の制限が必要	DNS スキャン、WEB クローリング
内部検知	リアルタイムの監視と異常検知が可能	システム負荷の管理が必要	ログ分析、ネットワークモニタリング
人的収集	・現場の状況を直接把握可能 ・内部と外部で発見できない IT 資産の把握が可能	報告漏れのリスクへの対策が必要	勉強会とアンケートの組み合わせ

2.3 探索手法の詳細

2.3.1 外部からの探索



【基本アプローチ】

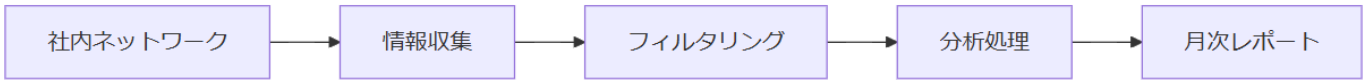
- 組織名からの段階的な探索
- 公開情報のみを利用
- 自動化された定期実行（月 1 回）

【制御方針】

- 探索範囲を自社ドメインに限定
- 業務時間外での実行
- 自動化された定期実行（月 1 回）

外部探索の網羅性向上のため、複数の OSS のツールを組み合わせます。一方で過剰な探索による外部への影響を最小限に抑えるよう、探索頻度等に制限を設けます。

2.3.2 内部からの検知



【基本アプローチ】

- 既存システムの活用
- 最小限[1]の情報収集
- 軽量[2]な分析処理

【運用方針】

- 定期的な自動収集
- 月次での分析実施

内部検知では、ネットワーク負荷の最小化を図るため、分析に必要な最小限のログに絞って効率的に収集します。

このようにして、内部検知を行う上での、情報収集～分析処理のプロセスごとの処理の効率化を図ります。

2.3.3 人的情報収集の詳細

【勉強会方式】

1. 開催形式

規模：部門単位の少人数制
頻度：定期開催（頻度は組織の状況に応じて調整）
時間：講義とディスカッションのバランスを考慮

1 最小限…現行システム、または必要に応じて行う再構築後のシステムにおいて、ピーク時でも、処理負荷が設定されたキャパシティを超えない、もしくは通常業務に支障をきたさない水準

2 分析処理は月次でバッチ処理として行い、システムの稼働、メインへの処理への影響が少ない

2. 内容構成

勉強会を開催する意図を明示してから
サイバーセキュリティ動向の共有を行うなどして、
あくまでもサイバーセキュリティの勉強会として開催し、

参加者の心理的安全性を確保することを前提に情報収集を行う。

【内容例】

・シャドーIT のリスクと対策

・情報資産管理の重要性と具体策

・質疑応答と講義内容についてのディスカッション

【情報収集の工夫】

1. アンケート設計

タイミング：勉強会の終了直後

形式：選択式を中心に、一部記述式を導入

所要時間：回答しやすい設計

2. 質問項目例

【google form 例】

【拡大版】

Q1. 業務で利用しているクラウドサービスを選択してください。[複数選択]

☐ クラウドストレージ

☐ プロジェクト管理ツール

☐ コミュニケーションツール

☐ 検証サーバー

☐ Web サーバー

☐ その他サーバー

☐ その他（自由記述）

Q2. 業務におけるシャドーIT のリスクについて、具体的な懸念があれば記入してください。[記述式]

Q3. 情報資産管理の課題について当てはまるものを選択してください。[複数選択]

☐ 管理対象の把握が不十分

☐ 棚卸/管理台帳の更新が滞っている

☐ 申請/承認プロセスが形骸化している

☐ 全社的な管理ルールが浸透していない

Q4. 本日の勉強会を踏まえて、あなた自身が報告していない IT 資産があれば教えてください。[記述式]

- IT 資産名：

- 用途：

- OS：

- 使用ソフトウェア：

- バージョン：

Q5. 業務をする上で使用を許可、または新しく導入してほしい IT 資産があれば教えてください。[記述式]

勉強会で基礎知識を身につけた上で、アンケートによる情報収集を行うことで、シャドーIT が存在することによるリスクの認識を高めつつ、報告漏れを最小限[3]に抑えることをねらいとしています。

勉強会の内容を現場の実態にマッチさせ、具体的な気付きにつなげることがポイントだと考えます。アンケートは平易に回答できるよう選択式を中心とし、一方で、記述式で現場の生の声を拾うことも重要と考えます。

3. フォローアップ

・個別ヒアリング：結果を基に必要に応じて個別ヒアリングを実施

4. 誤検知防止

・人から報告された資産が、外部/内部で発見されなかった場合

→詳しい情報とともに外部/内部へ差し戻し

・それでも発見できなかった場合

→誤情報と断定 または回答者にヒアリング

【情報収集の効果測定】

・アンケートの回答率

・人からのみ発見された資産の割合（内部/外部で発見済みのものを除く、管理対象資産の割合）

・資産未報告率（内部/外部で新規発見された管理対象資産が、人からの報告に含まれていない割合）

【効果測定の例】

・内部/外部から発見された資産 … A,B,C,D,E

・人の報告から発見された資産 … A,B,C,X

・全体で発見された資産 … A,B,C,D,E,X

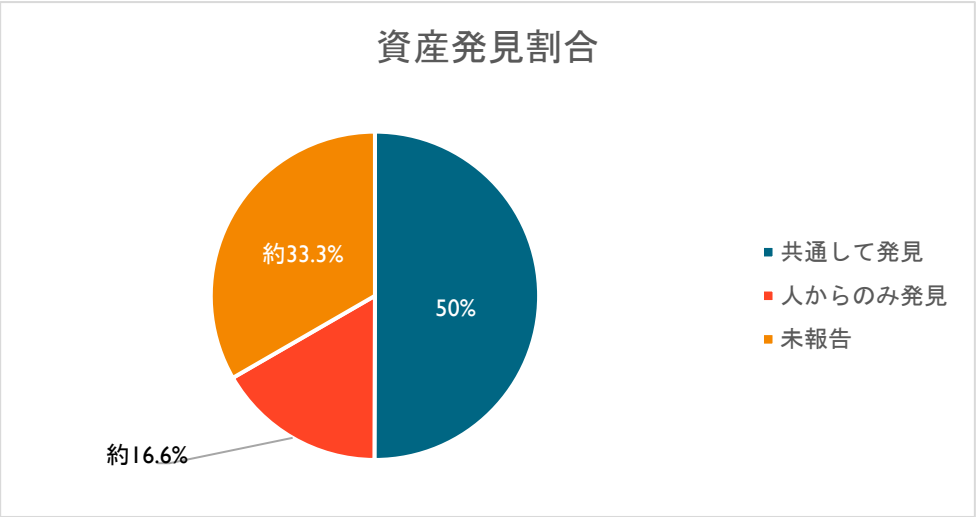
・人からのみ発見された資産 … X

・未報告の資産 … D,E

人からのみ発見された資産の割合 = 1 個 ÷ 6 個 = 約 16.6%

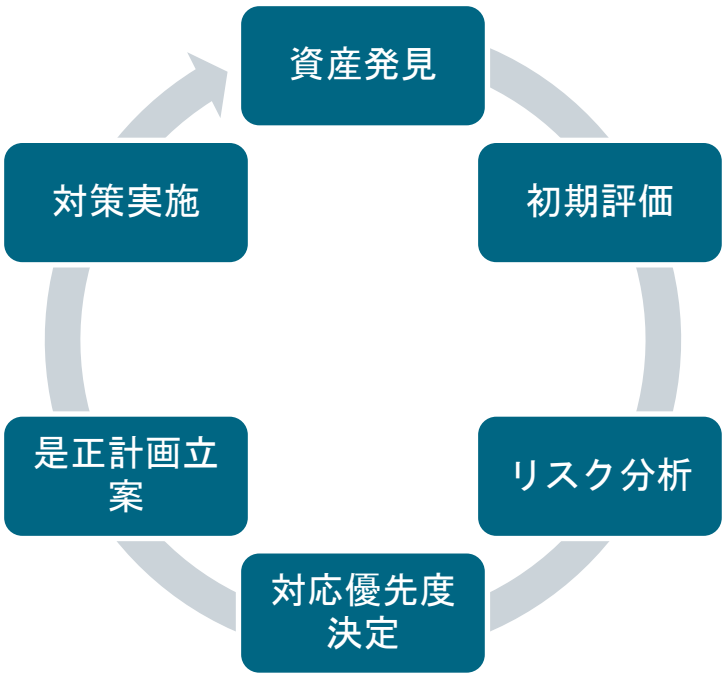
資産未報告率 = 2 個 ÷ 6 個 = 約 33.3%

[3] 資産未報告率 0%



2.4 発見資産の評価プロセス

三つのアプローチで収集したデータを統合し、リスクの分析・評価を行います。評価結果に基づき適切な対応を実施し、それをモニタリングしながら継続的に改善するようにサイクルを回していきます。



3. 期待される効果

3.1 セキュリティリスクの低減

【リスク低減効果】

・把握していない IT 資産およびシステムの排除

・社員のセキュリティ意識水準の向上

勉強会とアンケートの組み合わせによって、社員のセキュリティ意識向上とシャドー IT の リスクの可視化を同時に実現します。情報共有の活性化と部門間連携の強化にもつながると考えます

4. 今後の展望

4.1 技術的展望

★AI・機械学習による分析の高度化

4.2 運用面の展望

・プロセスの最適化

↳ 自動化による効率化

4.3 アイデア提案の展望

・OSS を用い、実際に検証を行い、その結果をフィードバックすることで、ASM ツールの実現性を高める

5. おわりに

本レポートでは、シャドーIT による脆弱性リスクへの対応として、外部・内部・人という 3 つの方向からアプローチする ASM ツールのアイデアを提案しました。特に、勉強会とアンケートを組み合わせた人的アプローチに重点を置き、現場の実態をより正確に把握することを目指しています。

ただし、人からの情報収集には報告漏れや認識の誤りといった課題も存在します。そのため、外部からの探索や内部からの検知による技術的アプローチと組み合わせることで、より確実な IT 資産の把握と管理を実現します。また、オープンソースツールの活用方法の具体化や法令への準拠性の確保など、設計や実装に向けてさらなる検討が必要です。

効果的なシャドーIT 対策の実現には、技術面からのアプローチと人的な取り組みの両方が不可欠です。本提案を基に、組織全体でバランスの取れた対策を進めていくことが重要だと考えます。また、対策の導入後も現場の声に耳を傾け、定期的な見直しと改善を行うことで、より効果的な対策の実現を目指していきます。

6. 【参考文献】

1. 情報処理推進機構. ″情報セキュリティ白書 2024″. 独立行政法人情報処理推進機構（IPA）, https://www.ipa.go.jp/publish/wp-security/2024.html, (参照 2024-11-05).

2. 情報処理推進機構. ″中小企業の情報セキュリティ対策ガイドライン 第 3 版″. 独立行政法人情報処理推進機構（IPA）, https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html, (参照 2024-11-05).

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″. 経済産業省 商務情報政策局 サイバーセキュリティ課 , https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf, (参照 2024-11-06) .