診断員による ASMのすすめ

【第10回】サイバーセキュリティ勉強会2024冬 in 塩尻

2024/02/03 幸田 将司

Who am I?

幸田将司:

セキュリティ屋さん:

- 株式会社Levii
- 株式会社バラエナテック 代表取締役
- SecuriST(R) 認定診断士 試験委員会 / ISOG-J(WG1)
- 診断 / 開発 / ISMS支援 ...etc

SNS:

- @halkichisec

Contents

1. ASM検討

2. 攻撃可能領域の探し方

内容

- 脆弱性診断員から見た、組織の攻撃対象領域のお話
  - 診断しながらこれやったら良いのになといつも考えています。

- 誰向け?
  - 脆弱性診断をたくさん発注する組織/企業様
  - ◯SIRTに携わる方
  - 診断員

ASMとはなんぞや

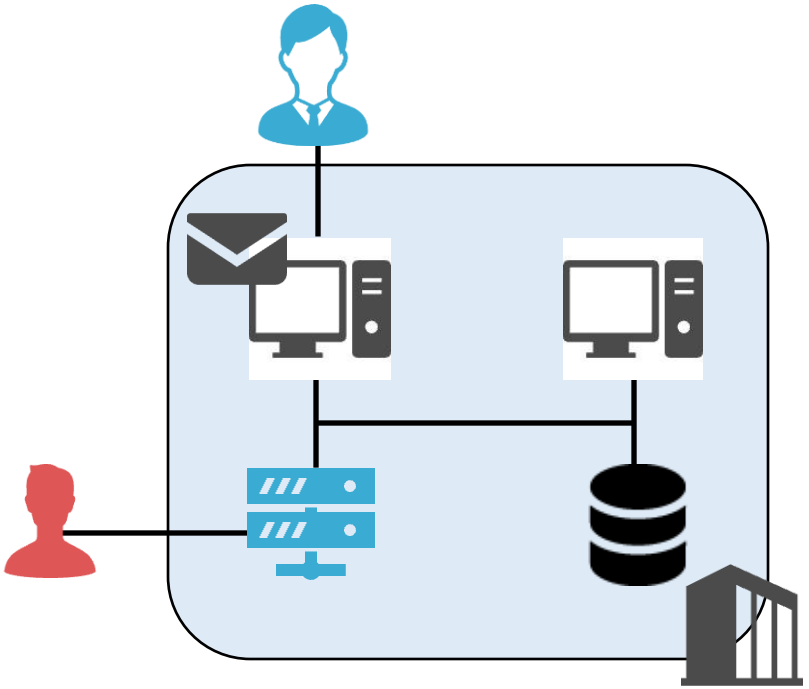
- 攻撃表面管理(Attack Surface Management)
  - 組織が自身の情報セキュリティ上の脆弱性や攻撃可能な範囲(攻撃表面)を管理/把握する。
  - 攻撃者がシステムやネットワークに侵入できる可能性のあるすべての経路や要因を特定する
  - インターネットに公開されているものが対象

ASMとはなんぞや

- 攻撃表面にはどんなものがあるか?

- 例:
  - コーポレートサイト
  - 自社サービス
  - メール/VPN/ファイルサーバ等
  - ネットワークカメラ等のIoT機器
  - 担当者のメールアドレス

  - 攻撃者から見えているものは多い



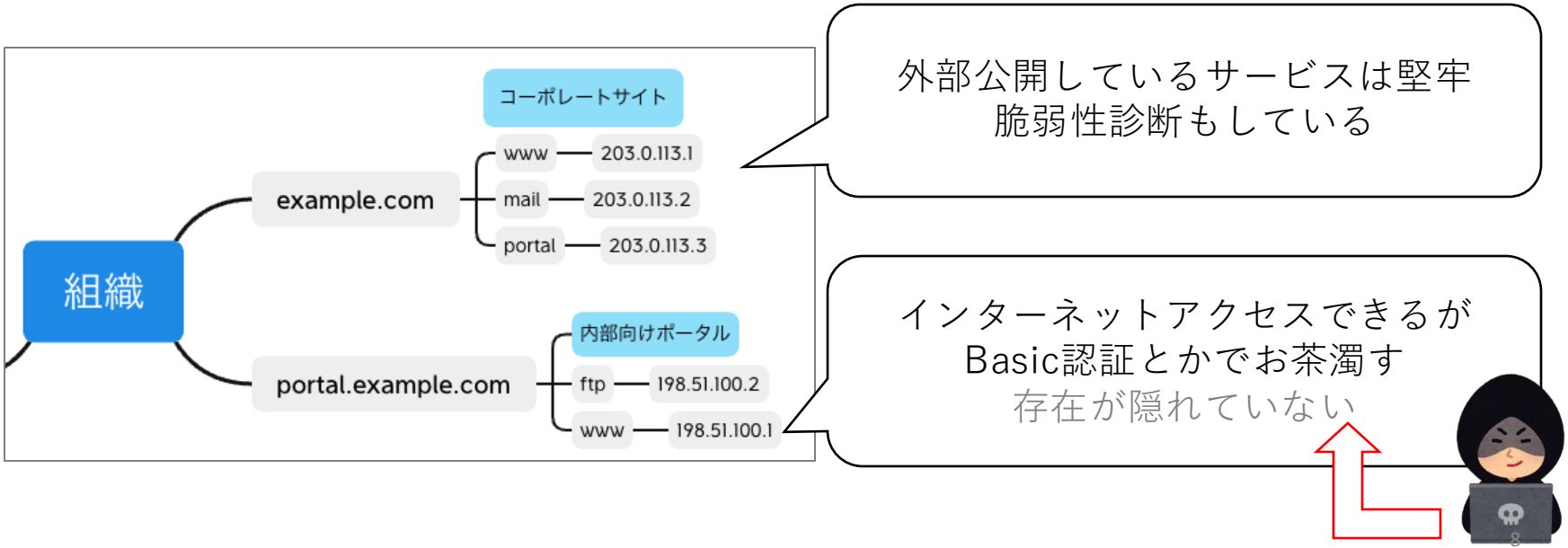
攻撃者の行動を考える

- Cyber Kill Chain (標的型攻撃のモデル)
  - ターゲットに対して行う攻撃の段階的な手順を示すモデル
  - 外部からの情報収集で集められる情報が少ないに越したことはない

  - 攻撃者はより多くの情報を集めてくる
  - 自組織がどのように見えているのか把握することが重要

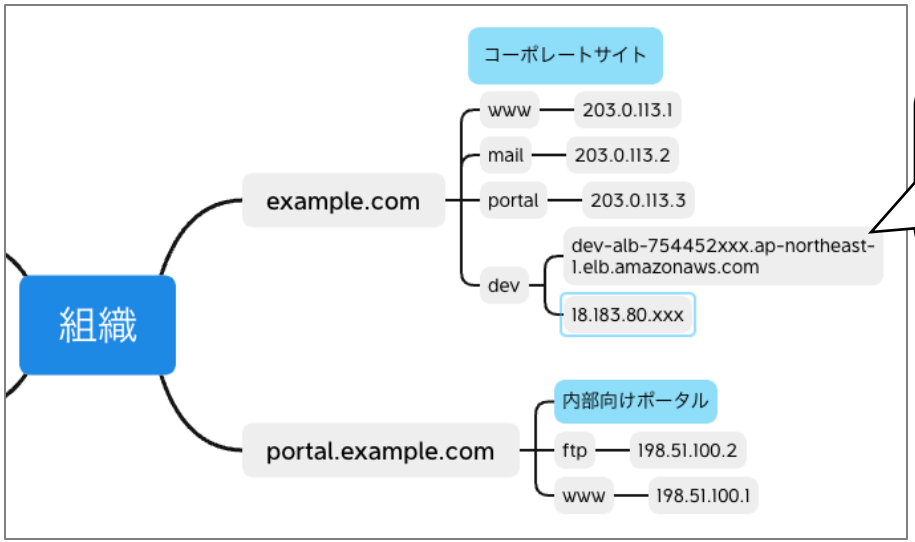
攻撃表面の例1

- コーポレートサイトや自社サービスに付随するコンテンツは存在がわかりやすいが、堅牢にされていることが多い。



攻撃表面の例2

- 自社サービスに紐づいているが、管理が忘れ去られているコンテンツ等



ベンダーのために
開けておいた経路

※IPに紐づくコンテンツサーバがなくともサブドメインテイクオーバーの温床になる可能性も。CNAME、Aレコード等

バグバウンティではよく報告されている

攻撃可能領域の探し方(内部)

- 内部からの調査は部署を横断する必要がある。

- インシデント例
  - (2021年)内閣サイバーセキュリティセンター(NISC)の情報漏洩
  - 内部で使用していたプロジェクト情報共有ツールへの不正アクセス

- 組織内部で使用している端末やツールの特定を行う
  - ISMS(ISO27001)を取得しているなら情報資産管理/リスク台帳があるはず
  - 管理している部署と連携をとることを推奨
  - シャドーITの制限も忘れずに

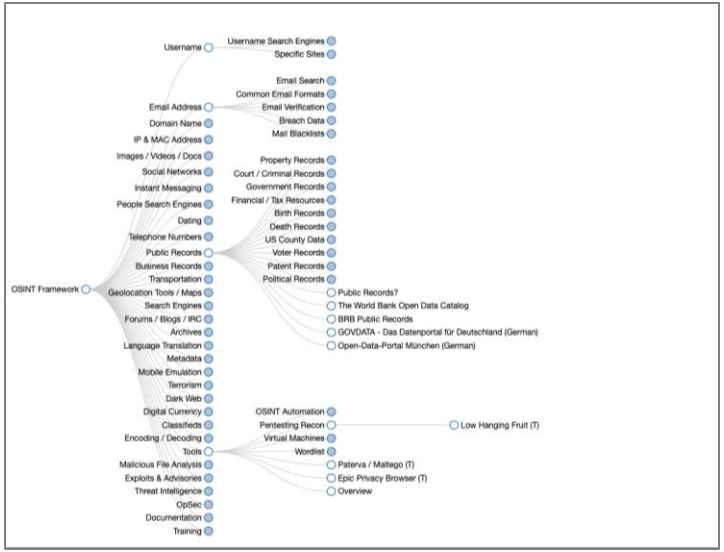
攻撃可能領域の探し方(外部)

- 外部からの調査の例として、OSINTは効果的

- OSINTツールの使用
  - Recon-ng
  - Maltego

- OSINTテクニックを使う
  - OSINTフレームワーク

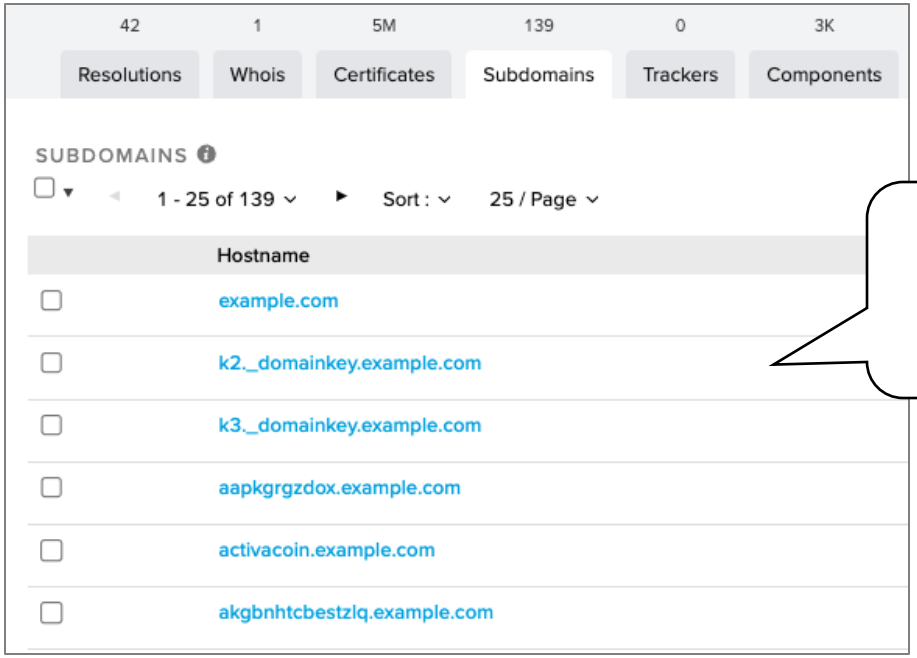
- 診断ベンダーへの依頼(OSINT診断)



OSINT Frameworkの例

- インターネッツから見えるものは多い
  - WHOIS、DNS、サーバ証明書のサブジェクト代替名...etc

- 情報集積サービス
  - 例えばRiskIQやCencys



ドメインに紐づいた、
サブドメインの一覧を列挙

←は例示用ドメインですが、
dev.{顧客名}.{自社ドメイン}の設計にしている
ベンダーの顧客名めちゃくちゃ見えてる

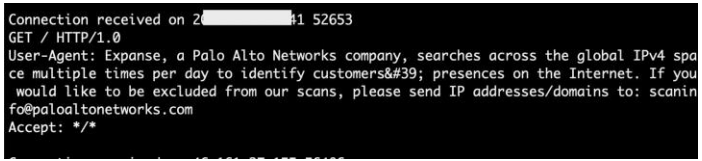
- Censysの例

- ドメイン/IPで検索できる理由:

- CensysやSHODANに代表される情報集積サービスはインターネットへネットワークスキャンを行なっている。

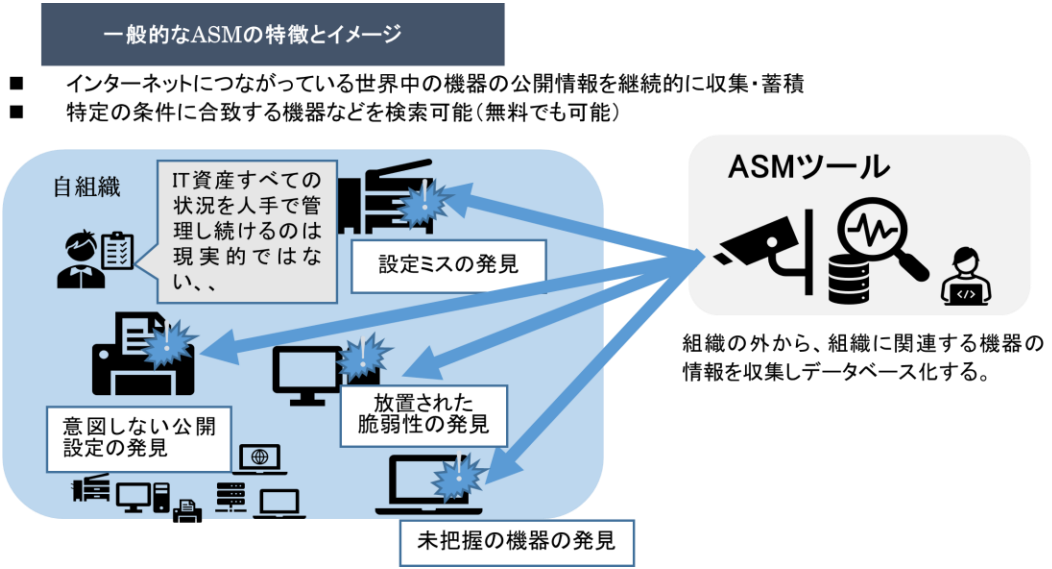
1. IPアドレスにポートスキャン
2. 443/tcp等にアクセス
3. 証明書のドメインを確認
4. ドメインの名前解決を行い、存在すればサイトにインデックス

一応、HTTPの時はヘッダで教えてくれる。
以下はPaloAltoの例



というわけでASMしよう

- 攻撃表面を把握するのは困難
- ツールを用いた管理を推奨(経済産業省)。



出典: 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～
https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

ASMツールの例

パッシブスキャンを
する例(選択化)

- Mandiant / 株式会社マクニカ
- Detect /サイファーマ株式会社

- Amass / OWASP
  - OSS、どのテクノロジーを使用するか設定が可能、脆弱性調査はしない

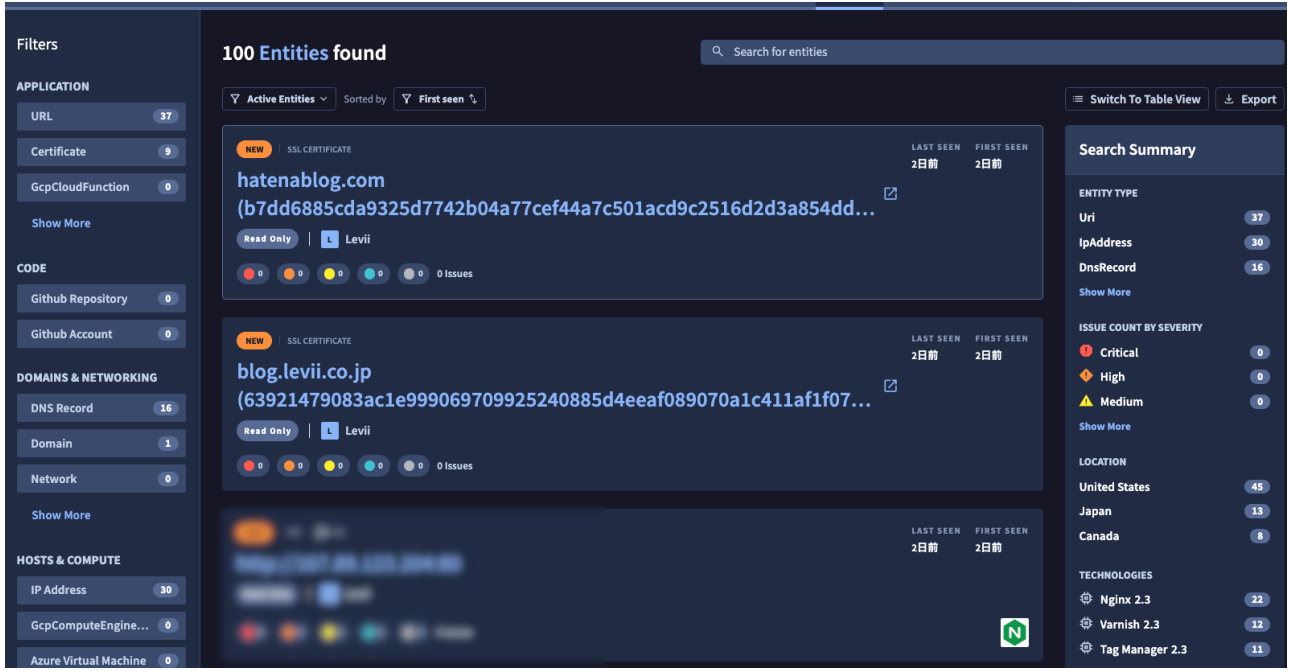
アクティブスキャン例

- サイバー攻撃ネットde診断 / GMOサイバーセキュリティ
  byイエラエ株式会社

- Sn1per / Sn1perSecurity LLC.
  - OSSだが、すべての機能を使うにはライセンス購入が必要

ASMツールで把握できるもの

- 公開情報の把握
  - 使用感としては、自社情報だけにフィルターしたSHODANに近い



ASMツールがやっていること

- Sn1perの例
- ネットワーク調査系
  - ping調査
  - ポートスキャン (nmap)
  - 単純な脆弱性調査 (nmap –A)
- OCINT系
  - DNS情報の収集
  - サブドメインテイクオーバーの確認
- 脆弱性診断系
  - ZAP / GVM / SSL Scan / smbdump …etc

使用感は

Reconツール
＋
ネットワークスキャナー

- 関係ないIPもトラッキングする可能性はあった。

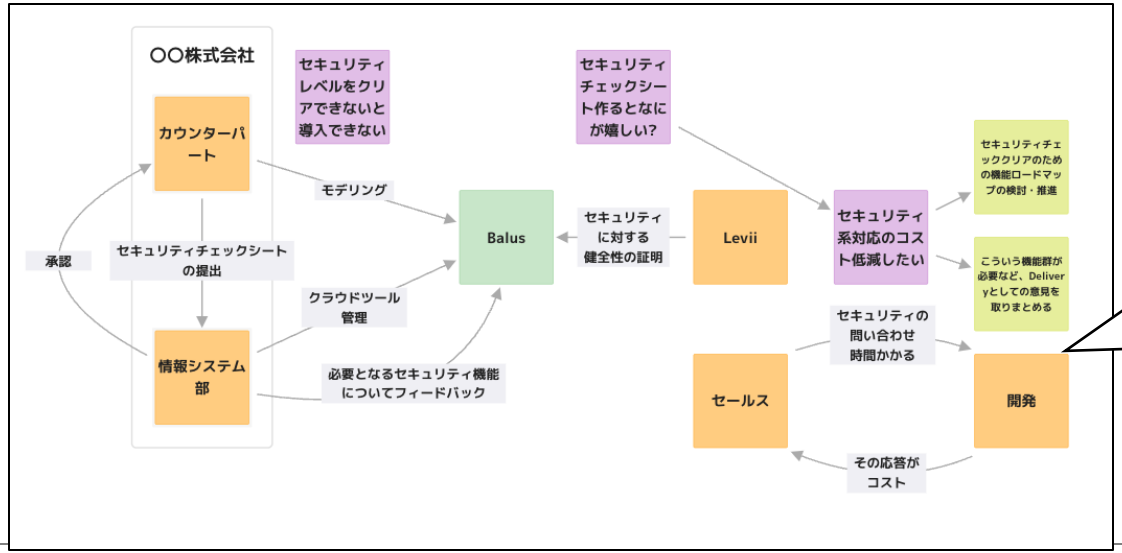
ASMでも担保できない箇所

- 従業員教育
  - 組織の窓口にいる担当者がうっかりメールを開く
- シャドーIT
  - 内部に持ち込まれ接続された端末や、勝手に使用しているツール
- 情報資産管理(ISMS)や、リテラシー向上教育で組織を巻き込んで管理したい。

参考：組織を巻き込む

- そもそも職務により目的/視点が違うため、各チームの代表をまきこんでモデリングすると、少しスムーズに進むかも

- サービスのセキュリティチェックシートを作る際のMTGの例



それぞれのロールの
背景や目的を同じ視点でみる
ための手法(構造化)

おわり

- ご清聴ありがとうございました