組織規模の脆弱性情報から脅威を把握する手法の実現

安藤　謙[†1]　岡村　耕二[†1]

概要：ASM は，組織が外部へ公開する資産を継続的に発見し，脆弱性や設定不備等の指摘を収集して管理する取り組みである．資産増加により結果が膨大となり，一覧提示のみでは把握と優先度判断が難しい．本研究は XCockpit EASM の Risk Factor 各 1 行をイベントとし，Asset，severity，type，subject で集約して HeatMap と TreeMap で俯瞰可視化する．九州大学が管理するホストサーバ群が共通的に使用している IP アドレスの資産群を用いて比較し，type 構成と severity 分布の差を短時間で把握できた．外部観測ノイズや濃淡比較の制約に留意し，除外規則と subject 統合を今後の課題とする．

キーワード：ASM, EASM, 脆弱性管理, 可視化

Implemantation of a method for getting threats from Organization scale vulnerability information

Ken Ando[†1]　Koji Okamura[†1]

Abstract: Attack Surface Management (ASM) is an approach in which an organization continuously discovers externally exposed assets and collects and manages findings such as vulnerabilities and misconfigurations. As the number of assets increases, the results become enormous, and presenting them only as a list makes it difficult to understand the overall situation and determine priorities. In this study, each row of Risk Factors in XCockpit EASM is treated as an event, aggregated by Asset, severity, type, and subject, and visualized at a glance using heatmaps and treemaps. Using asset groups that share a common IP address across a set of host servers managed by Kyushu University, we conducted a comparative analysis and were able to quickly identify differences in type composition and severity distribution. Taking into account external observation noise and limitations in comparing color intensity, we consider the definition of exclusion rules and the integration of subjects as future work.

Keywords: Attack Surface Management, External Attack Surface Management, Vulnerability Management, Visualization, Implementation

[†1] 現在，九州大学工学部電気情報工学科
Presently with Kyushu University

1. はじめに

組織の成長に伴いインターネット上のサービスは多様化し，外部へ公開される資産（ドメイン等）も増加している．大学のように部局・プロジェクト単位で個別運用される環境では，管理主体が分散し，把握漏れや意図しない公開により攻撃対象領域が拡大しやすい．

従来は台帳管理や監査，内部ログ監視により資産とリスクを把握してきたが，クラウド利用やサービス分散により公開範囲が継続的に変化し，内部情報のみで外部露出資産を一貫して把握することは難しい．結果としてリスク発見が遅れ，重大なインシデントに発展する可能性がある．

この課題に対し，外部視点で公開資産を継続的に発見し，脆弱性や設定不備等の指摘を収集・管理する ASM が注目されている [2]．本研究では CyCraft 社 XCockpit EASM を対象とし，得られる検出結果（イベント）を分析に用いる．一方で EASM の結果は膨大でノイズも含み得るため，一覧提示のみでは全体把握や優先度判断が難しい [3]．

そこで本研究は，XCockpit EASM の検出結果を整理・要約し，資産群と `severity`，`type` の分布と偏りを把握できる HeatMap ／ TreeMap を設計・実装して，運用上の意思決定を支援することを目的とする．

2. 関連研究

2.1 ASM/EASM

Attack Surface Management（ASM）は，外部観測に基づき組織に紐づくインターネット公開資産を継続的に把握し，脆弱性や設定不備等のリスク要因の検出と管理を支援する枠組みである [2]．External ASM（EASM）は外部から観測可能な資産の発見と継続観測に重点を置く．一方で観測対象の増加により検出結果が膨大となり，一覧提示のみでは問題の集中箇所や対応優先度を短時間で把握しにくい．

2.2 大学環境における ASM 運用

大学環境では部局単位の多様な運用や研究活動により資産が増えやすく，外部観測に基づく継続的な把握が有効と報告されている?．このとき，得られる検出結果を運用判断へ接続するための要約と提示が重要となる．

2.3 検出結果の集約と可視化

EASM は外部観測に基づき資産を発見・推定するため，観測条件や時期に起因して重複，誤検出等のノイズを含み得る．これらは可視化処理のみで完全に除去することが難しく，一覧のままでは重要な指摘が埋もれやすい．そこで，集約単位（例：ドメイン）と重要度指標（`severity`）を組み合わせ，件数と重大度を同時に把握できる形へ整理することが望ましい．本研究では，分布把握のために HeatMap を，重点領域抽出のために TreeMap を用いる．

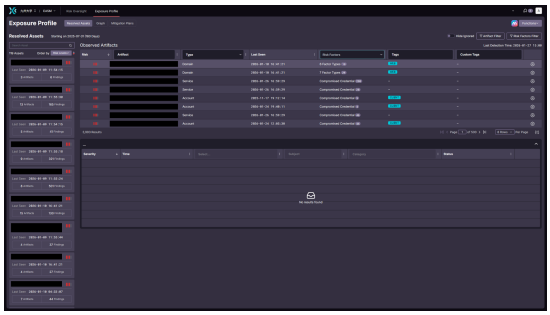

図 1 XCockpit EASM Exposure Profile

2.4 可視化による俯瞰と意思決定支援

多数資産に対する検出結果の分布や偏りを短時間で把握するために，可視化は有効である．とくに，複数の集約単位を横断して「どこに問題が集中しているか」を示す表現は，優先度判断の初動を支援する．本研究では，ドメイン ×`severity` の分布を示す HeatMap により，領域ごとの偏りと重点箇所を直感的に把握できるようにする．また，`subject` 単位の量と重要度を同時に表す TreeMap により，全体の構成比と重点領域を俯瞰できるようにする．

以上を踏まえ，次章では，本研究で対象とする CyCraft 社 XCockpit EASM の検出結果を分析用に定義し，運用判断へ接続するための集約と可視化手法を提案する．

3. EASM イベント分布に基づく資産群比較の可視化手法

3.1 手法の全体像

本章では，XCockpit EASM が出力する検出結果を，組織規模の観点から俯瞰可能にし，優先度判断につながる形で整理・要約・可視化する手法を提案する．本研究は ASM プロセスのうち，検出結果を運用判断へ接続するための集約と提示に焦点を当てる．まず，XCockpit EASM の検出結果を入力とし，Asset 表記のゆらぎを抑える前処理として空白整形を行い，URL スキーム，パス，クエリ，ポート番号等を除去してドメイン形式へ正規化する．ついで，Asset，severity，type，subject を軸にイベント件数を集約し，分析に適した形式へ変換する．最後に，可視化として HeatMap により資産群ごとの severity 分布と偏りを俯瞰し，TreeMap により subject 単位の構成比と重点領域を把握する．実装は第 4 章，評価は第 5 章で述べる．図 2 に提案手法の処理パイプラインを示す．

3.2 対象システムと分析単位

3.2.1 XCockpit EASM における資産と指摘

本研究が対象とする XCockpit EASM では，外部観測に基づく資産を Domain，Service，Account，IP Address 等のタイプとして扱い，資産に紐づく指摘を Risk Factor とし

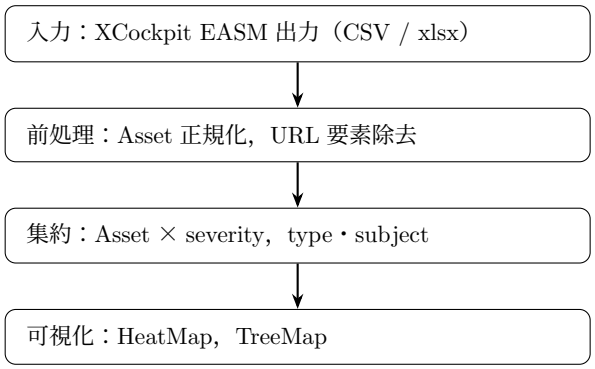

図 2 提案手法の処理パイプライン

て整理する [3]．Risk Factor は，一覧画面において Severity（Color & Number），Time，Subject，Category 等の項目として提示される [3]．

3.2.2 event の定義

本研究では，外部公開資産（Asset）は主にドメインを指す．XCockpit EASM の Risk Factor 一覧の 1 行を分析単位（event）とし，各 event は Severity（severity），Event Type（type），Subject（subject）等の属性を持つものとして集約・可視化を行う．XCockpit EASM が提示する Exposure Profile の 1 行を，分析上の最小単位であるイベント（event）として扱う．各 event は，観測対象資産（Asset）に紐づき，分類軸として type，subject，severity 等の属性をもつものとする．以降の集約と可視化は，event の属性に基づき行う．

3.3 分類軸の定義

3.3.1 type の定義と一覧

本研究では，XCockpit EASM User Guide に示される分類体系に基づいて ASM 出力を整理する [3]．type は，EASM が提示する Risk Factor の大分類であり，本研究では次の 11 種類を用いる．本研究で用いるデータでは，type は Event Type 列に対応する．

- Weakness
  - Certificate Weakness
  - Cipher Weakness
  - Email Weakness
  - DNS Weakness
  - Website Weakness
  - Network Weakness
  - Software Weakness
- Misconfiguration
  - Website Security
  - Network Security
  - Certificate Security
- Vulnerability
  - Exploited Vulnerability

図 3 XCockpit EASM における severity の色・数値と区分（文献 [3] より）

3.3.2 subject の定義と一覧の扱い

本研究では，subject を type に属する下位項目として定義する．User Guide では，各 type に対して Description が与えられており，その中で列挙される具体的な指摘内容（例：missing SPF record 等）を，原則としてカンマ区切りで分割して得られる要素として subject を定める [3]．本研究で用いるデータでは，subject は Subject 列に対応する．なお，Description 中の列挙は文章表現であり，分割規則によって粒度が変化し得るため，本研究では表記ゆれの正規化を併用し，subject を分析用ラベルとして整備する．subject 一覧は付録に示す（付録??）．

3.3.3 severity の取り扱い

XCockpit EASM では，Risk Factor の severity が数値と色を伴って提示され，通知条件としても severity の閾値（例：6〜10 等）を設定可能である [3]．図 3 に示すように，severity は 1〜10 で表され，1〜6 を Low，7〜8 を Medium，9〜10 を High として区分される．本研究では，event に付与された severity を危険度指標として用い，type および subject との組合せで分布と偏りを可視化する．

3.4 資産群（Group）の定義

本研究では，組織内の資産を 2 群に分けて比較する．Group A は特定の IP アドレス（133.5.12.221）に割り当てられているドメイン群，Group B はそれ以外の資産群である．この 2 群に対して，type，subject，severity の分布を同一の手順で可視化し，群間差を俯瞰する．群の詳細と対象データの条件は第 5 章で述べる．

3.5 可視化設計

3.5.1 HeatMap による分布と偏りの俯瞰

HeatMap は，行に Asset（ドメイン），列に severity を配置し，各セルに当該ドメインにおける当該 severity のイベント件数（counts）を割り当てた行列として構成する．本研究では，type（例：Certificate Weakness，Email Weakness 等）ごとに色相を割り当て，さらに同一 type 内で件数に応じて濃淡を変化させる．これにより，特定 type のイベントが「どの severity 帯に集中し，どのドメイン群に偏在しているか」を俯瞰できるようにする．また，Group A/B で同様の可視化を作成することで，群間の分布差を比

較できる．

3.5.2 TreeMap による重点領域の俯瞰

TreeMap は，subject を矩形として配置し，矩形面積にイベント件数を割り当てることで，全体に占める構成比と重点領域を同時に俯瞰するために用いる．本研究では，type を上位階層，subject を下位階層として階層構造を構成し，矩形面積に件数，色に危険度指標として severity に基づく値を割り当てる．これにより，「件数が多く，かつ危険度が高い領域」を優先的に発見できる表現とする．

3.6 提案手法の整理

本章では，XCockpit EASM の検出結果を `event` として定義し，`type`，`subject`，`severity` を分類軸として用いることを示した．また，2 群（Group A/B）に対する比較を前提として，HeatMap および TreeMap による要約表現を設計した．次章では，本手法を実現するデータ取得・正規化・描画処理の実装について述べる．

4. XCockpit EASM データ処理パイプラインと可視化実装

4.1 実装方針と処理フロー

本研究では，XCockpit EASM から取得した検出結果（Risk Factor）を入力として，提案手法（第 3 章）で定義した `event`，`type`，`subject`，`severity` に基づく集約と可視化を行う．実装は Python で行い，入力データの統合と前処理，集約処理，および可視化用 JSON の生成までを自動化する．生成した JSON は HTML（JavaScript）から読み込み，HeatMap および TreeMap として描画することで，ブラウザ上で可視化結果を閲覧可能とする．

処理の流れは，(1) 入力シートの統合，(2) 前処理（正規化と除外条件の適用），(3) 集約（HeatMap 用・TreeMap 用），(4) 可視化用 JSON 生成，(5)HTML による描画，である．以降，各処理の内容を述べる．

4.2 入力データ仕様（スキーマ）

本実装は，XCockpit EASM の Risk Factor 一覧を入力として受け付ける．取得元は CSV 形式であるが，処理系では CSV または同一列構造を持つ xlsx を入力として扱う．xlsx の場合，複数シートに分割されていてもよく，全シートを縦結合して 1 つの `event` 集合として処理する．

必須列は `Asset`，`Severity`，`Event Type`，`Subject` である．各行を Risk Factor の 1 行に対応する `event` とみなし，以降の前処理・集約はこれらの列に基づいて行う．（`Time` 等の他列は本研究の集約では使用しない．）

4.3 前処理（正規化と整形）

集約結果の安定化のため，`Asset` 等の文字列に対して前後空白の除去，連続空白の縮約を行う．また `Asset` 列にはドメイン以外の表現が混入し得るため，URL スキーム（`http://`等），パス，クエリ，ポート番号等を除去し，ドメイン形式へ整形する．一方，`Asset` が IP アドレス形式で表される行については，本研究では除外せずに集約対象として扱う．ただし，ドメイン形式の `Asset` と IP アドレス形式の `Asset` は観測・解釈の前提が異なり得るため，後続の比較では同一視せず，分布の読み取りに注意を要する．これらの処理により，同一資産が表記ゆれにより分割されることを抑制する．

4.4 集約処理

可視化の目的に応じて，2 種類の集約を行う．第一に，HeatMap 作成のため，ドメインと `severity` の組に対するイベント件数を集約する．これにより，資産（ドメイン）ごとの危険度分布と偏りを行列として表現できる．第二に，TreeMap 作成のため，`subject` 単位でイベント件数を集約し，併せて当該 `subject` に付随する `severity` の代表値を算出する．これにより，`subject` ごとの規模（件数）と重要度（危険度）を同一画面で俯瞰できる．

4.5 可視化用 JSON の生成

4.5.1 HeatMap 用 JSON

HeatMap 用 JSON は，ドメイン一覧 `domains`, `severity` 一覧 `severities`，および `domains`×`severities` の件数行列 `matrix` から構成する．`matrix` の各要素は，当該ドメインにおいて当該 `severity` で観測されたイベント件数（`counts`）を表す．さらに，描画時の詳細表示に利用するため，各ドメインに紐づく `subject` 一覧を `domain_subjects` として保持する．

4.5.2 TreeMap 用 JSON

TreeMap 用 JSON は，`type` を上位階層，`subject` を下位階層とする階層構造で構成し，各 `subject` ノードにイベント件数と `severity` 代表値を付与する．これにより，面積で件数，色で危険度を表現でき，重点領域の抽出を支援する．

4.6 HTML による描画

生成した JSON を HTML（JavaScript）から読み込み，HeatMap と TreeMap を描画する．HeatMap は `matrix` を色で表し，ドメインごとの `severity` 分布と偏りを俯瞰する．TreeMap は `subject` ごとの件数（規模）と `severity`（危険度）を同時に示し，構成比と重点領域を把握できる．これにより，膨大な検出結果を短時間で要約し，運用上の意思決定に接続しやすくする．

表 1　2 群比較における Group A/Group B の定義

群	定義	ドメイン数	イベント数
Group A	IP アドレス集合に 133.5.12.221 を含む資産群（複数 IP を持つ場合は集合に含まれるかで判定）	244	812
Group B	IP アドレス集合に 133.5.12.221 を含まない資産群	176	2831

注：ドメイン数は前処理後の *Asset* のユニーク数を表し，イベント数は *EASM* 上の件数である．

5. 資産群（Group A/B）に対するイベント分布比較実験

5.1 実験目的

本研究の目的は，EASM が出力する膨大な検出結果を，組織全体を俯瞰できる形へ要約し，運用上の意思決定（重点領域の把握，優先度判断）に接続しやすくすることである．本章では，提案する HeatMap および TreeMap が，(1) 分布と偏りの把握，(2) 重点領域の特定，(3) 資産群間の差分理解，に有効であるかを確認する．

また評価として，IP アドレスに特定のホスト IP アドレス（133.5.12.221）を含むドメイン群（Group A）と，含まないドメイン群（Group B）を比較し，可視化表現が群間差の説明に寄与するかを検討する．

5.2 実験データ

実験データは，XCockpit EASM から取得した Risk Factor 一覧である．本研究では，Risk Factor 一覧の 1 行を 1 件の `event` として扱い，`Asset`，`Severity`，`Event Type`，`Subject` を用いて解析する．データ規模は表 1 に示すとおりである．

なお，実験では再現性と管理の都合上，取得した一覧を xlsx として保存して用いたが，入力列の仕様および処理方法は第 4 章で述べたとおりであり，ファイル形式自体は本質ではない．

5.3 実験条件

5.3.1 可視化対象と集約単位

可視化の集約単位と割当（HeatMap：Asset × severity，TreeMap：type → subject 階層，面積＝件数，色＝ severity 代表値）は，第 3 章で定義した仕様に従う．本章では，Group A/B に対して同一仕様の可視化を生成し，分布形状と重点領域の差分に着目して比較する．

5.3.2 2 群比較の定義

比較評価では，IP アドレスに 133.5.12.221 を含むドメイン群を Group A，含まないドメイン群を Group B として 2 群に分割し，両群に対して同一仕様の可視化を生成する．IP アドレスは DNS 解決等によりドメインへ付与した IPv4 アドレスの集合であり，複数 IP を持つ場合は集合に含まれるか否かで判定する．

5.4 実験手順

(1) XCockpit EASM からイベント一覧を取得する．
(2) 入力データを前処理し，必要な列（`Asset`，`Severity`，`Event Type`，`Subject` 等）を抽出する．
(3) 集約処理を行い，HeatMap 用および TreeMap 用の可視化データを生成する．
(4) 可視化データを JSON へ変換し，HTML から読み込んで HeatMap と TreeMap を描画する．
(5) IP アドレスの条件により 2 群へ分類し，両群の可視化結果を比較する．

5.5 評価観点

提案表現の有効性を確認するため，以下の観点で評価する．

- 分布把握：高 `severity`（例：7 以上）のイベントが集中するドメイン領域を短時間で特定できるか．
- 重点領域把握：TreeMap により，イベント数が多い `subject`，または高 `severity` が多い `subject` を俯瞰的に把握できるか．
- 比較容易性：Group A と Group B において，分布の差分や重点領域の差分を直感的に説明できるか．

補助的な定量情報として，総イベント数，`severity` 別件数，高 `severity`（例：7 以上）のイベント件数，および該当ドメイン数を算出し，可視化結果の解釈を支援する．

5.6 データ概要

本研究では，EASM 上のイベント数を集計の基礎として扱う．Group A の EASM 上のイベント数は 812，Group B は 2831 である．また，本章で示す `counts` は観測されたイベントの頻度（繰り返しを含む）を反映する集計値であり，ユニークな弱点数を直接表すものではない点に留意する．

5.7 可視化結果

5.7.1 HeatMap（Group A：IP アドレスに 133.5.12.221 を含む）

図 4 に Group A の HeatMap を示す．行は `Asset`（ドメイン），列は `severity` であり，各セルは当該ドメインにおける当該 `severity` の観測件数（`counts`）を表す．本可視化では `type` ごとに色相を割り当て，同一 `type` 内で `counts` に応じて濃淡を変化させた．このため，`severity` の高低だけでなく，「どの `type` が，どの `severity` 帯に，どのドメイン群として現れているか」を俯瞰できる．

Group A では，`Certificate Weakness` に対応する領

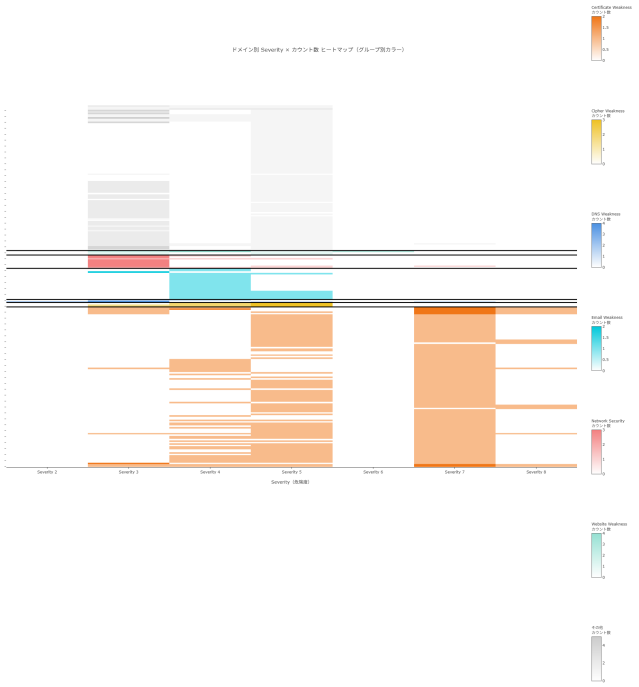

図 4 HeatMap（Group A：IP アドレスに 133.5.12.221 を含む）

域が相対的に多く観測され，とくに高 severity 側（例：severity=7 付近）にまとまって出現する傾向が見られる．なお，本研究では証明書関連 subject の意味づけや原因の深掘りは行わず，定義・判定基準は XCockpit EASM User Guide に従うものとする．

5.7.1.1 注意（読み取り上の制約）

本図は type ごとに配色および濃淡スケール（カラーバー）が独立に設定されているため，**異なる type 間で濃淡を直接比較して件数大小を判断することはできない**．比較は同一 type 内で行う必要がある．また，色が高 severity 側に目立って見える場合でも，それは「当該 type 内で高 severity に分布が寄っている」ことを示すものであり，他 type の総量との大小関係を直接意味しない．

5.7.2 HeatMap（Group B：IP アドレスに 133.5.12.221 を含まない）

図 5 に Group B の HeatMap を示す．Group B では，中 severity 帯（例：severity 4–6 付近）を中心とした分布が目立ち，Group A で観測された高 severity 側のまとまりとは異なる傾向が確認できる．とくに Website Weakness や Cipher Weakness 等において，中 severity 帯の指摘が複数ドメインへ広く分布している様相が観察される．このことは，Group B では「一部ドメインに高 severity が集中する」というよりも，「複数ドメインに中 severity の設定不備が分散している」状態を示唆する．

また Group B 側には IP アドレス形式の Asset も含まれるが，本研究ではこれらを除外せずに扱う方針とする．ただし，ドメイン形式の Asset と IP アドレス形式の Asset は観測・解釈の前提が異なり得るため，分布の読み取りで

図 5 HeatMap（Group B：IP アドレスに 133.5.12.221 を含まない）

は同一視しないよう注意を要する．

5.7.3 HeatMap（2 群比較）

図 4（Group A）と図 5（Group B）は，IP アドレス条件で分割した 2 群に対し，同一仕様で生成した HeatMap である．比較に先立ち，Asset の表記ゆれを正規化し，URL 要素（スキーム・パス・クエリ・ポート等）を除去して資産キーを整形した．この正規化により，同一資産が表記差で別資産として集計されることを抑え，群間比較の解釈を安定化した．なお本図は type ごとに配色および濃淡スケール（カラーバー）が独立であるため，**異なる type 間で濃淡を直接比較して件数の大小を判断することはできない**．比較は同一 type 内の分布（どの severity 帯に偏るか，どの資産に集中するか）を中心に行う．

データ規模として，Group A のドメイン数は 244，Group B は 176 であり，イベント数（EASM 上）はそれぞれ 812，2831 である（表 1）．群の規模が異なるため，単純な総量比較だけでなく，severity 帯への偏りや，特定 type の集中の有無といった分布形状に着目して比較する．

観察結果として，Group A では Certificate Weakness が高 severity 側（例：7 付近）にまとまって出現する傾向が見られ，特定 severity 帯への偏りが視覚的に確認できる．一方 Group B では，中 severity 帯（例：4–5 付近）を中心として複数の type が広い資産範囲に分散しており，「一部資産への高 severity 集中」というより「中 severity の指摘が多資産に広く分布する」様相が観察される．以上より，本 HeatMap は，群ごとの type 構成と severity 分布の差分を短時間で把握し，運用上の重点領域（偏在か分散か）を説明する要約表現として有用である．

5.7.4 TreeMap（Group A：IP アドレスに 133.5.12.221 を含む）

図 6 に Group A の TreeMap を示す．本図は，矩形面積に unique_assets（当該 subject が観測された資産数），

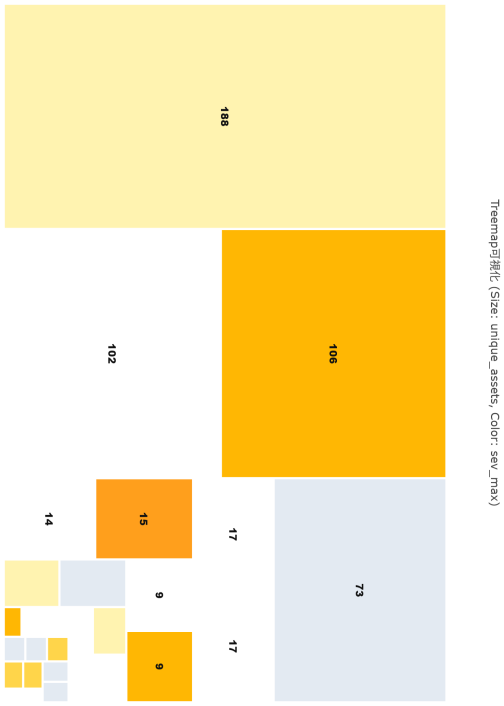

図 6 TreeMap（Group A：IP アドレスに 133.5.12.221 を含む）

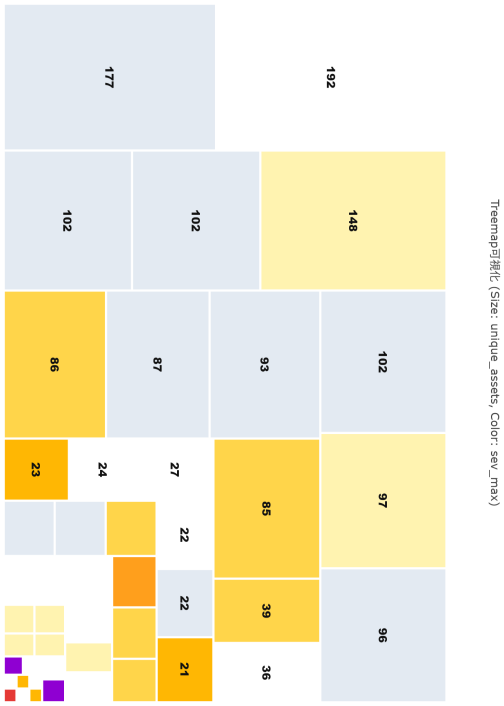

図 7 TreeMap（Group B：IP アドレスに 133.5.12.221 を含まない）

色に危険度を表す指標（実装では sev_max）を割り当てている．Group A では，大きな矩形が少数存在し，それらが全体の面積（出現範囲）を占める一方で，その他は小規模な矩形が点在する構成となっている．このことは，特定の subject が相対的に多くの資産で観測され，重点領域が比較的限定される可能性を示唆する．

5.7.5 TreeMap（Group B：IP アドレスに 133.5.12.221 を含まない）

図 7 に Group B の TreeMap を示す．Group B では，中規模以上の矩形が複数存在し，全体として矩形が広く分散して配置されている．これは，複数の subject が一定規模の資産範囲で観測され，重点領域が分散する傾向を示す．また，色の分布から，危険度指標が高い領域（暖色系）の subject が複数存在することが視覚的に確認できる．

5.7.6 TreeMap（2 群比較）

図 6 と図 7 を比較することで，2 群における「出現範囲の大きい subject」と「危険度指標が高い subject」の差分を俯瞰できる．本比較では 2 群のドメイン数（母数）が同一であるため，矩形面積（unique_assets）の大小を群間で比較しやすい．観察として，Group A は少数の大規模 subject が目立つ一方，Group B は中規模の subject が複数存在して分散する構成であり，重点領域の現れ方が異なる．以上より，TreeMap は群ごとの重点領域（広く出現する領域/危険度の高い領域）の説明に有効な要約表現である．

5.8 可視化結果の要点整理

本章では，IP アドレス条件により資産群を 2 群に分割し，HeatMap および TreeMap を同一仕様で生成して比較した．HeatMap では，資産をドメイン単位で行に配置し，列に severity をとってイベント件数を可視化することで，各ドメインがどの severity 帯でどの程度指摘を受けているかを把握できる．さらに，type ごとに色相を割り当てているため，危険度分布に加えて，全体としてどの type の指摘が多いかを俯瞰できる．一方，TreeMap では subject 単位で件数を集計し，矩形の面積で件数規模を，色の段階で severity 代表値を表すことで，どの subject が多く観測され，それらがどの程度の危険度に位置づくかを同時に把握できる．

その結果，2 群で type 構成および severity 分布が異なることを，可視化により短時間で把握できることを確認した．次章では，得られた差分の解釈と運用上の活用可能性，ならびに本手法の適用上の制約について考察する．

6. 考察

6.1 提案表現の有効性

TreeMap は subject ごとの規模（件数）と危険度（severity）を同時に示すため，運用者が重点領域（件数が多い／危険度が高い）を短時間で抽出できる．HeatMap は Asset × severity 分布を可視化し，指摘が偏在する資産や深刻度帯を把握しやすい．両者は「重点領域抽出（TreeMap）」と「分布把握（HeatMap）」を分担し，EASM 出力の要約表現として相補的に機能する．

2 群比較では，type 構成と severity 分布の差が可視化から確認できた（例：Group A は CertificateWeakness 等が目立ち，severity=7 帯が多い一方，Group B は WebsiteWeakness が支配的で severity=4 帯に集中する）．また TreeMap 上位の subject から，Group A では証明書設定や外部公開構成に関する指摘，Group B では Web 応答ヘッダやソフトウェア起因の指摘が重点領域として抽出された．

6.2 適用上の制約と留意点

本研究は外部観測に基づく EASM 出力を扱うため，EASM の検出特性に起因して資産帰属の誤りや一時的ノイズ，誤検出を含み得る．この点は本研究の可視化手法そのものの欠陥というより，外部観測に依存する EASM の性質上の制約である．したがって，本可視化は厳密な原因同定や網羅的な真偽判定を目的とせず，「分布の偏り」や「重点領域の抽出」を中心に解釈する必要がある．

また，本研究のイベント数および HeatMap の counts は観測頻度の集計であり，同一 subject が繰り返し記録されれば増加するため，ユニークな弱点数を直接表すものではない．このため，厳密な弱点件数の比較には用いず，傾向把握の指標として扱う．

さらに HeatMap は type ごとに配色・濃淡スケールが独立であるため，異なる type 間で濃淡を比較して件数大小を判断できない．総量比較や順位付けは，別途集計表等の補助情報と併用することが望ましい．

加えて，type，subject は User Guide の記述を分割して定義していることを留意したい．

6.3 今後の課題

今後は，(1) ノイズ低減のための除外規則の精緻化，(2)subject 粒度を安定させる辞書整備・同義語統合，(3)type 横断比較を補助する定量集計（例：type 別件数や高 severity 件数）の併記，を検討する．加えて，外部観測に起因する誤検出の影響を把握するため，(4) 他の ASM/EASM 製品や資産台帳・構成管理データベース，あるいは手動検証結果との突合により誤検出率や適合率等の精度指標に基づいて EASM 出力の妥当性を評価することも課題である．

7. 結論

本研究では，ASM/EASM が出力する検出結果を運用判断へ接続しやすい形で俯瞰可能にすることを目的として，可視化用の集約処理を行い，HeatMap および TreeMap による要約表現を提案した．HeatMap により Asset×severity の分布を可視化し，重点的に確認すべき資産領域の抽出を支援できることを示した．また TreeMap により，subject の構成比と危険度を同時に俯瞰し，優先的に確認すべき指摘内容の抽出に寄与し得ることを示した．

さらに，IP アドレス条件で分割した 2 群比較により，type 構成および severity 分布が異なることが可視化から確認できた．このことは，提案表現が実運用での比較・把握（状況認識と初動トリアージ）に有用である可能性を支持する．

一方で，外部観測に基づく EASM 出力にはノイズや誤検出が含まれ得るため，本研究の結果は検出真偽の確定を意図するものではなく，分布の偏りや重点領域の抽出に主眼を置く．今後は，重複を含む件数指標の併記，詳細表示への導線整備，および subject 統合の高度化に加え，他のシステムや資産台帳等との突合による誤検出評価を行うことで，意思決定支援効果をさらに高めることが課題である．

参考文献

[1] 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〜』を取りまとめました」，2023 年 5 月 29 日，参照日：2026-01-27.
[2] 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―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 5 月 29 日（初版），PDF，参照日：2026-01-27.
[3] CyCraft, *XCockpit EASM User Guide*, (社内配布資料), 参照日：2026-01-27.
[4] 細川 達己，「大学環境における攻撃対象領域管理の導入とその活用」，大学 ICT 推進協議会 2025 年度年次大会（AXIES 2025）論文（2AM2B-5），2025 年.