Tokio Marine Holdings

Internet Week ショーケース　オンライン2021

C4：脅威インテリジェンスの実践的活用法

2021年7月9日

東京海上ホールディングス株式会社
IT企画部 リスク管理グループ
石川 朝久, Ph.D., CISSP, CSSLP, CISA, CISM, CFE, PMP

今日のテーマとお話したいこと

テーマ：脅威インテリジェンスの活用

- 攻撃者へのプロアクティブな対応のため、脅威インテリジェンスが必要不可欠！
- 一方、脅威インテリジェンスも具体的活用に悩む企業も多い。
- 本講演では、「脅威インテリジェンス」の活用方法について解説する。

※ Internet Week 2020から一部内容を変更しています。
過去の講演： https://www.nic.ad.jp/ja/materials/iw/2020/proceedings/

アジェンダ

- 1：脅威インテリジェンスとは？
- 2：Tactical Intelligence
- 3：Operational Intelligence
- 4：Strategic Intelligence
- 5：まとめ

自己紹介：石川　朝久

- **所属　：東京海上ホールディングス株式会社　IT企画部　リスク管理グループ**
- **専門　：不正アクセス技術・インシデント対応・セキュリティ運用・グローバルセキュリティ戦略 etc.**
- **資格　：**博士（工学）, 情報処理安全確保支援士、CISSP, CSSLP, CISA, CISM, CDPSE, CFE, PMP
- 　　GIACs（GSEC, GSNA, GPEN, GWAPT, GREM, GCIH, GCFA）
- **経歴　：**
  - 2009.04 – 2019.03　　：某セキュリティ企業
    - 侵入テスト（Red Team）・インシデント対応・脆弱性管理・セキュア開発、セキュリティ教育 etc.
    - １年間、米国金融機関セキュリティチームに所属した経験あり
  - 2019.04 – 現在　　：東京海上ホールディングス株式会社
    - 国内外グループ企業のセキュリティ支援・CSIRT運用・セキュリティプロジェクト企画・グローバルセキュリティ戦略 etc.
- **対外活動（抜粋）：**
  - SANSFIRE 2011 Speaker（2011）
  - DEFCON 24 SE Village Speaker (2016)
  - Internet Week 2018 – 2020 (2018-2020)
  - IPA 情報処理技術者試験委員・情報処理安全確保支援士試験委員（2018~）
  - IPA 「10大脅威執筆者会」メンバー（2010～2014, 2019~）
  - オライリー社『インテリジェンス駆動型インシデントレスポンス』翻訳・監訳
  - オライリー社『初めてのマルウェア解析』翻訳

注意・ご連絡

- 本プレゼンテーションの内容は、全て講演者個人の見解であり、所属企業、部門、その他所属組織の見解を代表するものではありません。

- 講演の内容については、講演者の研究、グループ会社などの取り組みなどを参考にしながら作成しています。

- 製品名・ベンダー名などが登場した場合、講演者にて推奨しているわけではありません。利用については各組織にて判断をお願いします。

1 ：脅威インテリジェンスとは？

1-1：脅威インテリジェンスの定義

- 脅威インテリジェンスは、以下のように分類可能である。

脅威インテリジェンス ＝ 脅威 ＋ インテリジェンス

- **要素１：脅威とは？**
  - 脅威インテリジェンスとは、この３要素に関連する情報を集めること

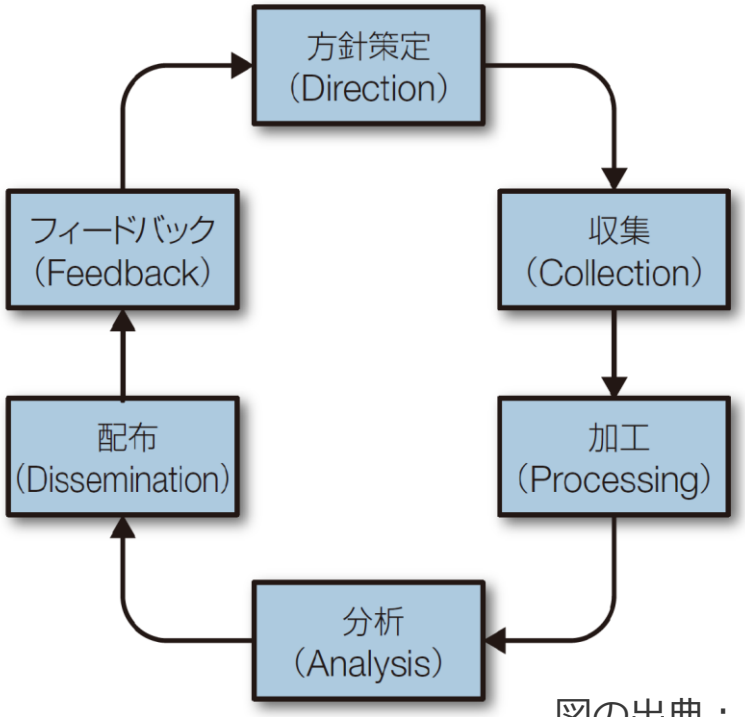
- 各要素の説明（SANSの定義）
  - **意図　　：どんな攻撃者が、どんな動機で自社を狙うのか？**
    - 自社の「資産」に基づいて、動機や意図が決定される
  - **能力　　：攻撃者はどのような攻撃手法を使うのか？**
    - 自社の「環境」や「脆弱性」により、利用する攻撃手法が決定される
  - **機会　　：攻撃を実現する環境・条件が整っているか？**
    - 自社の環境において攻撃可能な脆弱性が公開されているか？

1-1：脅威インテリジェンスの定義

- 脅威インテリジェンスは、以下のように分類可能である。

脅威インテリジェンス ＝ 脅威 ＋ インテリジェンス

- **要素２：インテリジェンスとは？**
  - 情報・データを以下の要件を満たすように分析・加工したもの
  - 分析プロセス：**インテリジェンス・サイクル**



図の出典：『インテリジェンス駆動型インシデントレスポンス』

1-1：脅威インテリジェンスの定義

- 脅威インテリジェンスは、以下のように分類可能である。

脅威インテリジェンス ＝ 脅威 ＋ インテリジェンス

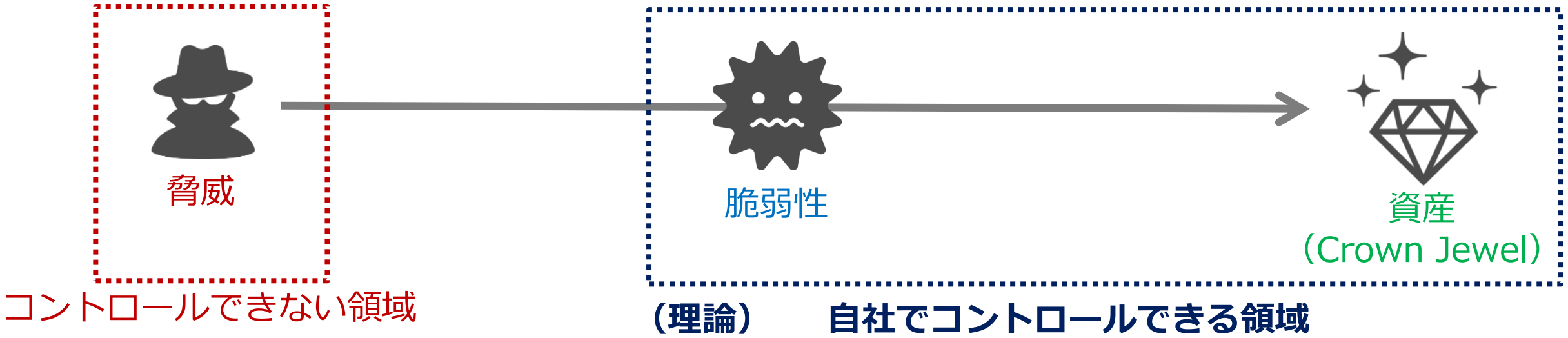
- **要素２：インテリジェンスとは？**
  - 情報・データを以下の要件を満たすように分析・加工したもの

  - **良いインテリジェンスの４要件：４A**
    - **A**ccurate（正確な）
    - **A**udience Focused（利用者/消費者目線である）
    - **A**ctionable（アクショナブル）
    - **A**dequate Timing（適切なタイミング）

1-2：脅威インテリジェンスの目的・必要性

- なぜ脅威インテリジェンスが必要なのか？
  - より高度（効率的・効果的）な「**セキュリティリスク管理**」のため

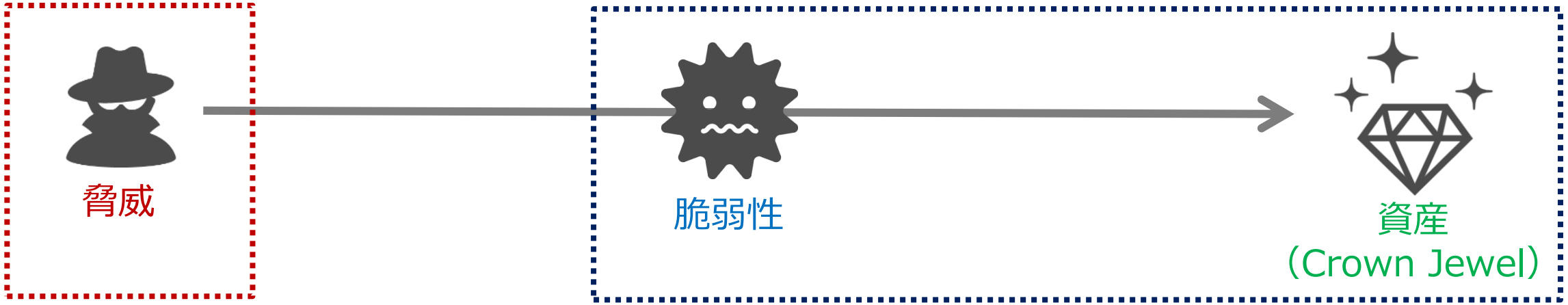
- **リスク = 脅威 × 脆弱性 × 資産**



1-2：脅威インテリジェンスの目的・必要性

- なぜ脅威インテリジェンスが必要なのか？
  - より高度（効率的・効果的）な「**セキュリティリスク管理**」のため

- **リスク = 脅威 × 脆弱性 × 資産**



コントロールできない領域

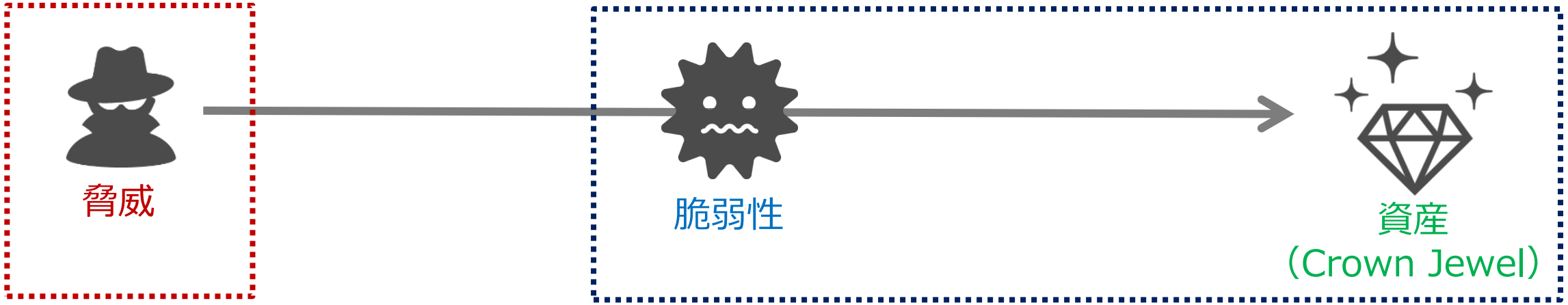
（理論）　自社でコントロールできる領域

（現実）　膨大な管理労力
（投入できる）リソースの限界
クラウド・サプライチェーンなど難しい管理領域

1-2：脅威インテリジェンスの目的・必要性

- なぜ脅威インテリジェンスが必要なのか？
  - より高度（効率的・効果的）な「**セキュリティリスク管理**」のため

- **リスク = 脅威 × 脆弱性 × 資産**

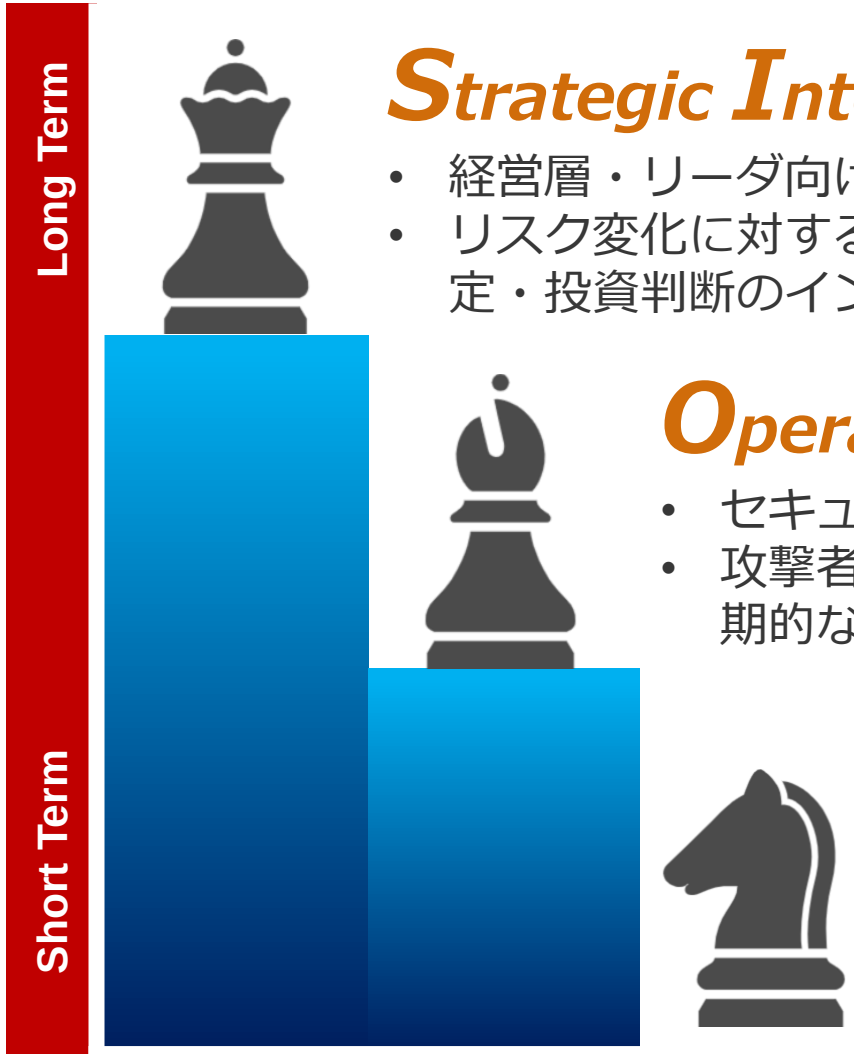


「リスク管理」の優先度をつけるため、「脅威」に注目する。（＝敵を知る）

- 結局、サイバーリスクのドライバー（起点）となるのは、「脅威」である。
- セキュリティリソース（人・モノ・金・時間）は限られるため、全方位に十分な対策を行うことが難しい。そのため、具体的な脅威へ対応することを優先する。

1-3：脅威インテリジェンスの活用と分類

- 脅威インテリジェンス活用は、種類・目的を理解する点にある。（誰に価値を提供するか？）
  - DoDモデル：米国国防総省の３分類を採用し、筆者研究に基づき対象者・役割を定義している。



Strategic Intelligence

- 経営層・リーダ向け
- リスク変化に対するハイレベルな情報を提供することで、セキュリティに関する適切な意思決定・投資判断のインプットとする。

Operational Intelligence

- セキュリティアーキテクト・管理者・SOC担当者向け
- 攻撃者のプロファイル、攻撃手法（TTPs）など攻撃者の手法を理解し、短期～中期的なセキュリティ改善活動に活用する。

Tactical Intelligence

- SOC担当者向け
- 日々のセキュリティ運用において、（セキュリティ製品に反映される前の）攻撃シグニチャ（IOC）を取得・設定することでインシデントを未然に防ぐ。

2 : Tactical Intelligence

2-1： IOC活用による予防・検知・対応

- **IOCとは？（Indicator of Compromise・侵害指標）**
  - 実際に発生した脅威・攻撃手法を特定するための技術的特性情報（=シグニチャ）
    - 例）ハッシュ値・IPアドレス・ドメイン名・マルウェアがPC上に残る痕跡（例：レジストリ）

- **IOCの分類：Network Indicator × Host Indicator**

<Network Indicator>
IPアドレス
ドメイン名

<Host Indicator>
ハッシュ値
ファイルのパス
レジストリ

2-1： IOC活用による予防・検知・対応

- **IOCの活用方法：**
  - （予防）将来、同様の攻撃が行われた場合に備え、Deny Listへ登録する。
  - （検知）現在・過去の時点で、自分の組織が同様の攻撃を受けていないことを確認する。
  - （対応）攻撃を受けていた場合、IOCを調査の起点として分析する。

- **IOCの有効性と制約：**
  - IOC活用により、シグニチャ化していない業界固有の脅威を予防・発見できる。
  - 但し、こうした脅威情報は製品ベンダーも収集しており、時間が経過すればシグニチャとして提供される。そのため、IOC活用の意義は、**ゼロデイ期間**（=シグニチャ化されるまでの期間）に攻撃を予防・検知することにある。IOCの鮮度は、数時間～数日程度だと考えられる。
  - IOCの利用には不確実性が伴う。（確実に悪性であることが判明した場合、IOCとしての価値は低くなる）また、IOCは時間経過とともに性質・判断が変わっていくため、継続的評価も必要となる。
  - 実運用の観点では、**情報量とスピードが重要のため、SOARなどを活用した自動化**が望ましい！！

3 : Operational Intelligence

3-1：TTPs

- Operational Intelligenceとは、「攻撃者のプロファイル、攻撃手法（TTPs ・Capability）など攻撃者を理解し、短期～中期的なセキュリティ改善に活用すること」と定義される。
- **TTPs（Tactics, Techniques and Procedures）**
  - 攻撃者が使う攻撃手法のこと。 MITRE社のATT&CKフレームワークで体系化されている。
  - ATT&CK：**A**dversarial **T**actics, **T**echniques, **and C**ommon **K**nowledge
    - TTPsを体系化した攻撃手法ナレッジ集
    - https://attack.mitre.org/

Tactics

Techniques（技術）を用いて、攻撃者が達成したい目的（=What?）
例）Credential Access（認証情報へのアクセス）、Privilege Escalation（権限昇格）

Techniques

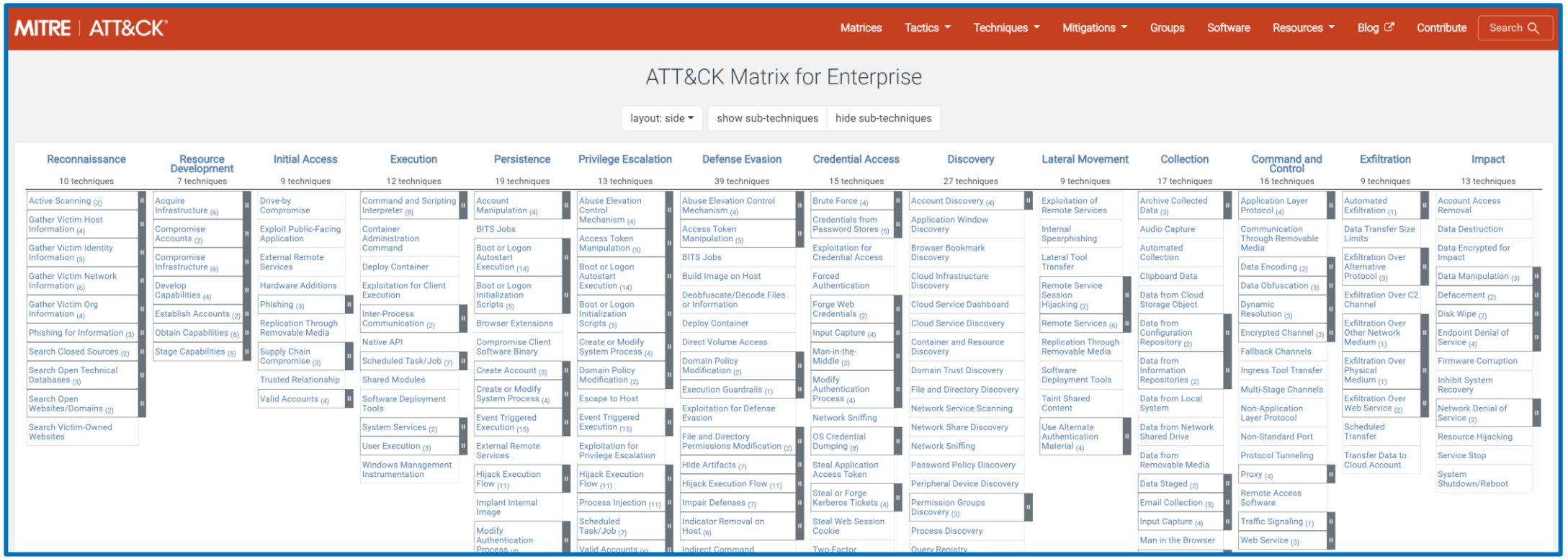
Tactics（戦術）を達成するために、攻撃で実際に使われる技術（=How?）
例）（Tactics）Credential Access →（Techniques）Credential Dumping
→（Sub-Techniques）Security Account Manager

Procedures

Tactics・Techniquesを実現するための一連のアクション
例）（Techniques）Credential Dumping - Security Account Manager
→ Mimikatzを使い、SAM（Security Account Manager）から情報をダンプする。

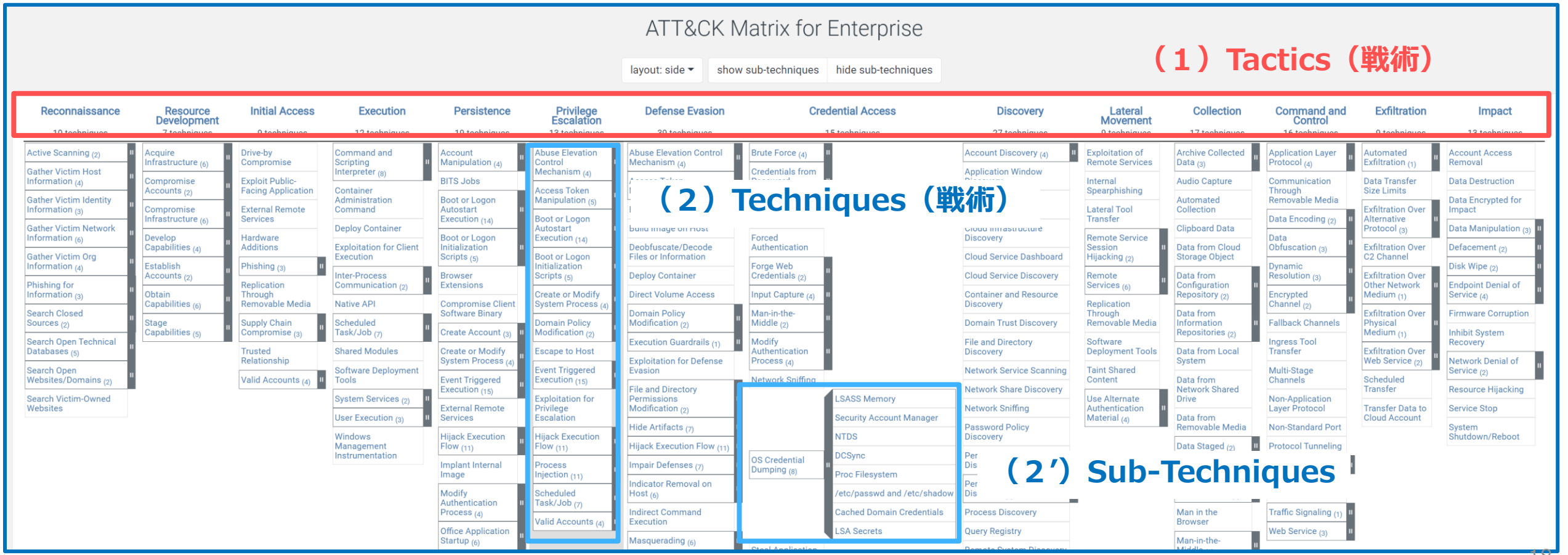
3-1：TTPs

- **MITRE ATT&CKフレームワーク**
  - Adversarial Tactics, Techniques, and Common Knowledge
  - TTPsを体系化した攻撃手法ナレッジ集（Common Knowledge = 前述のProceduresに相当する）
  - 活用に当たり、以下のドキュメントを推奨する。
    - MITRE社　　：『MITRE ATT&CK：DESIGN AND PHILOSOPHY』
    - MITRE社　　：『Getting Started with ATT&CK』
    - SANSFIRE 2019：『Leveraging MITRE ATT&CK - Speaking the Common Language』



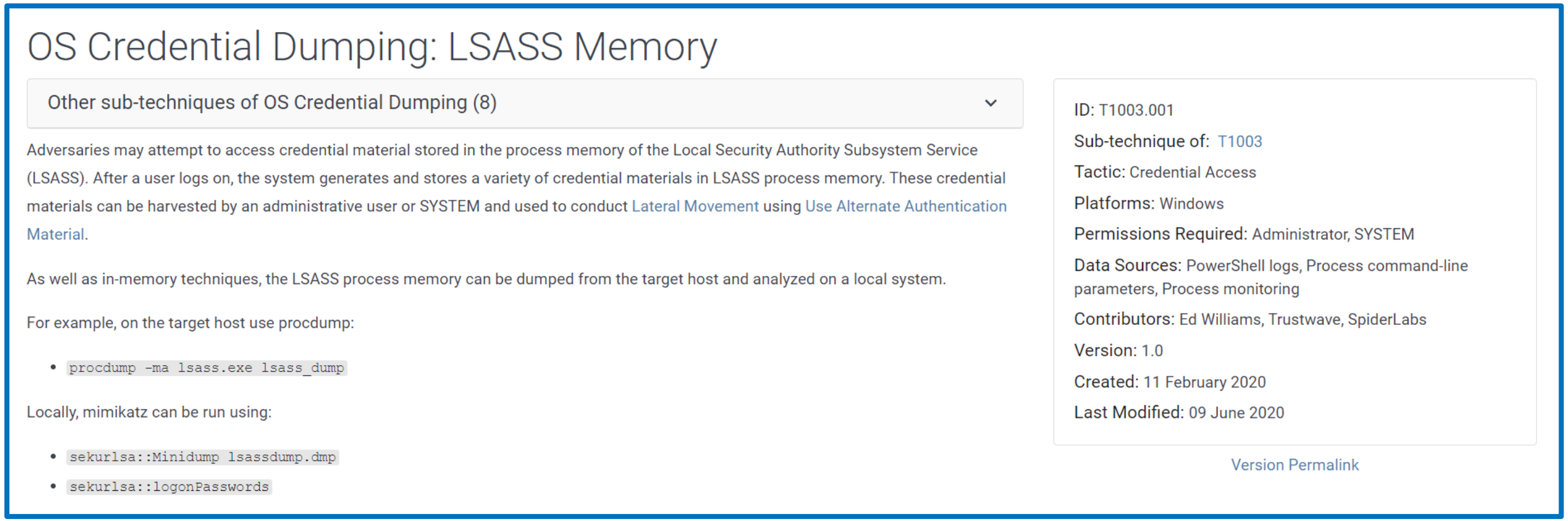
3-1：TTPs

- **MITRE ATT&CKフレームワーク**
  - MITRE ATT&CKを読み解くキーワードは大きく３種類ある。
  - **（１）Tactics（戦術）**　：（既に述べた通り）攻撃者の目的
  - **（２）Techniques（技術）**　：（既に述べた通り）攻撃に実際に利用する技術
  - **（２’）Sub-Techniques**　：（２）Techniquesのさらに詳細な技術



3-1：TTPs

- **MITRE ATT&CKフレームワーク**
  - MITRE ATT&CKを読み解くキーワードは大きく３種類ある。
  - **（３）Common Knowledge（手順）**　　：各Techniquesの詳細・具体的手順
    - 当該ページに、当該Techniquesに関連する（４）Group（５）Software（６）Mitigation、あるいは検知する手法なども記載されている。



OS Credential Dumping: LSASS Memory

Other sub-techniques of OS Credential Dumping (8)

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct Lateral Movement using Use Alternate Authentication Material.

As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system.

For example, on the target host use procdump:

- `procdump -ma lsass.exe lsass_dump`

Locally, mimikatz can be run using:

- `sekurlsa::Minidump lsassdump.dmp`
- `sekurlsa::logonPasswords`

ID: T1003.001

Sub-technique of: T1003

Tactic: Credential Access

Platforms: Windows

Permissions Required: Administrator, SYSTEM

Data Sources: PowerShell logs, Process command-line parameters, Process monitoring

Contributors: Ed Williams, Trustwave, SpiderLabs

Version: 1.0

Created: 11 February 2020

Last Modified: 09 June 2020

Version Permalink

3-1：TTPs

- Operational Intelligenceの観点から、MITRE ATT&CK（TTPs）をどのような活用を行うか、実務に即した活用が重要となる。

→ 具体的な、事例を１つピックアップしてご紹介します！

No.	分類	担当者	応用方法	内容
A	予防	GRC担当	リスク評価 (Risk Assessment)	リスク評価において、新しい攻撃手法・シナリオ（TTPs）を利用して評価を行うことで、最新の攻撃シナリオへの対応を可視化できる。
B		SOC担当者	侵入テスト (Adversary Emulation)	実際の攻撃シナリオに基づいて侵入テストを実施し、脅威を防ぐ態勢（予防・検知・対応）を確認する手法。攻撃シナリオ構築に攻撃者のプロファイル・攻撃手法（TTPs）を利用する。
C		セキュリティアーキテクト	アーキテクチャの改善 (Defensive Architecture)	Defensive Architectureとは、攻撃を予防・検知・対応できるアーキテクチャである。攻撃手法（TTPs）を活用し、セキュリティ態勢（製品・プロセス・人）の改善検討へ利用する。
D	検知	SOC担当者	脅威ハンティング (Threat Hunting)	既存のセキュリティ対策を回避する高度な脅威を検知・隔離するため、能動的・再帰的にネットワーク内を探索するプロセス。既存の知見（TTPs）を起点に、新しい脅威を見つけ出す。
E	対応	SOC担当者	インシデント対応 (Incident Response)	インシデント対応を行う際、攻撃手法（TTPs）を活用して効率的な対応を行う手法。

ご参考：

- 侵入テスト（Adversary Emulation）、脅威ハンティング（Threat Hunting）については、過去のInternet Week の講演で紹介していますので、そちらを参照してください。

Internet Week 2018
丸ごとわかるペネトレーションテストの今

https://www.nic.ad.jp/ja/materials/iw/2018/proceedings/d2/

Internet Week 2019
攻撃者をあぶりだせ！！　プロアクティブなアプローチ

https://www.nic.ad.jp/ja/materials/iw/2019/proceedings/d2/

3 : Operational Intelligence

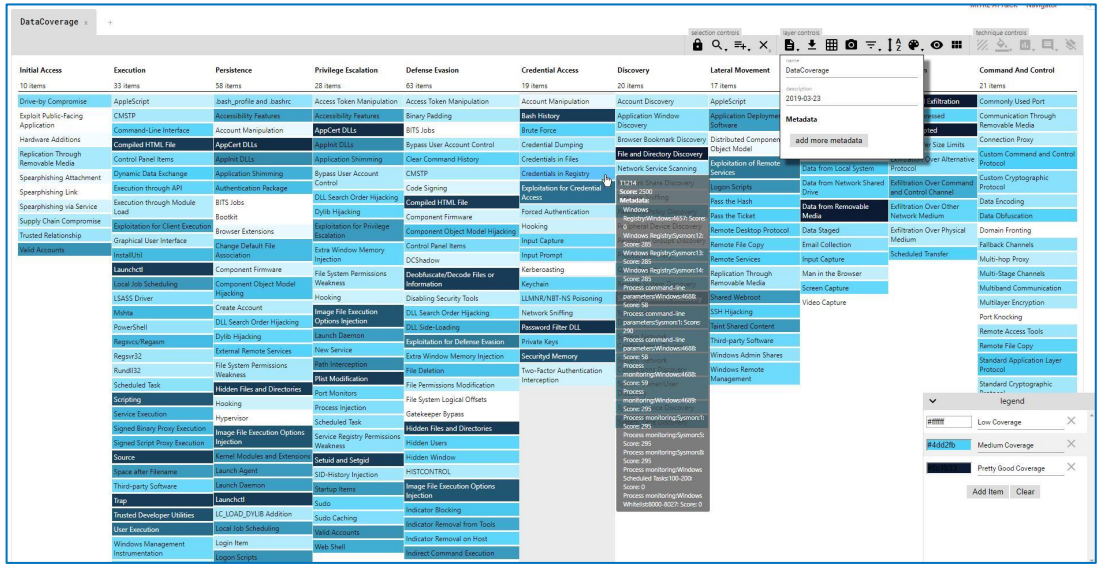
~ Threat Intelligence for Defensive Architecture ~

3-2 : Threat Intelligence for Defensive Architecture

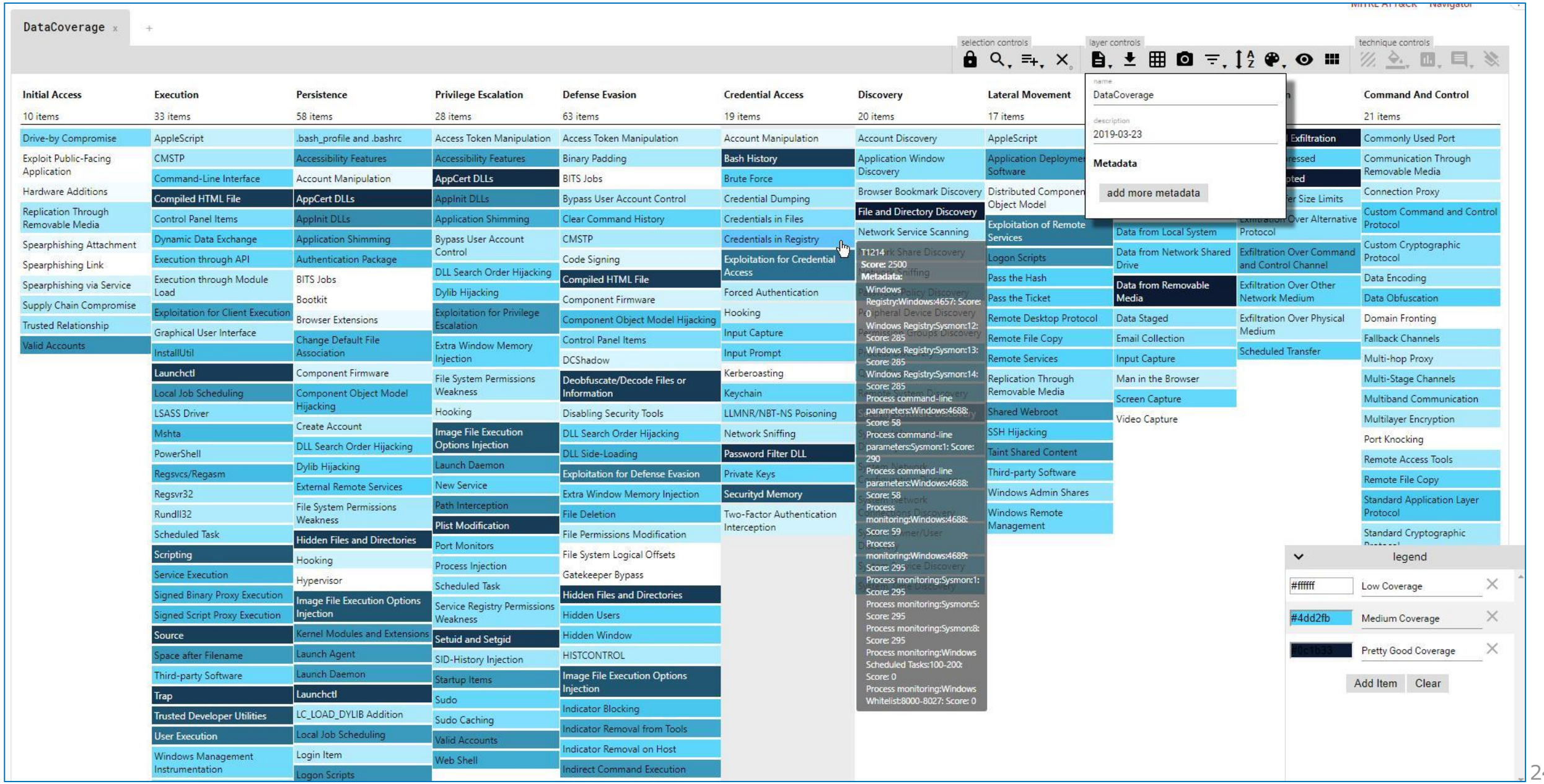
- **Defensive Architectureとは？**
  - 新しい攻撃手法（TTPs）に対し、柔軟に予防・検知・対応ができる技術アーキテクチャのこと。
  - そのためには、現行の防御アーキテクチャの有効性がいつでも評価できる仕組みが必要となる。

- **BAS : Breach & Attack Simulation**
  - 攻撃手法のシミュレーション（Adversary Emulation）をすることで、**セキュリティコントロールの有効性を検証**し、セキュリティ態勢（Security Posture）を把握するツール。

  - MITRE ATT&CKフレームワークの活用方法として、@Cyb3rWard0g などが提案した「検知能力の可視化」（Detection Capability）が挙げられ、複数のプロジェクトが存在する。



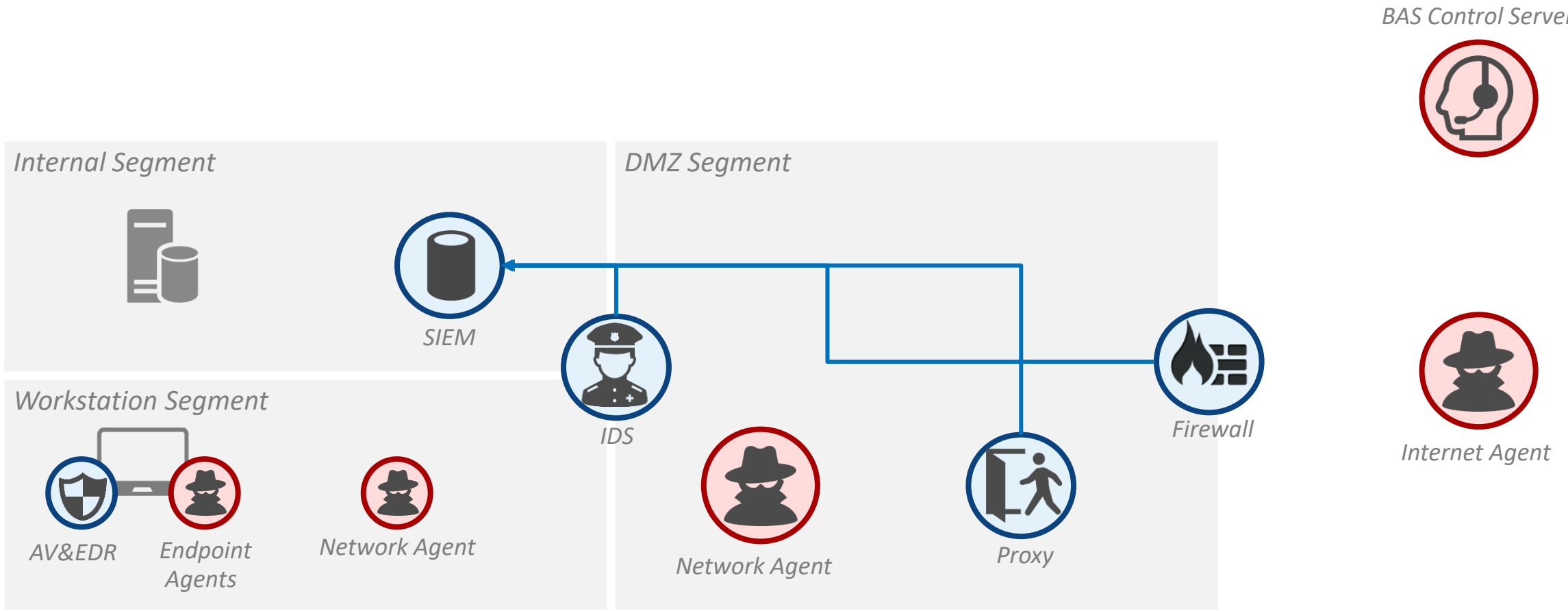
3-2 : Threat Intelligence for Defensive Architecture



3-2 : Threat Intelligence for Defensive Architecture

BAS : Breach & Attack Simulation

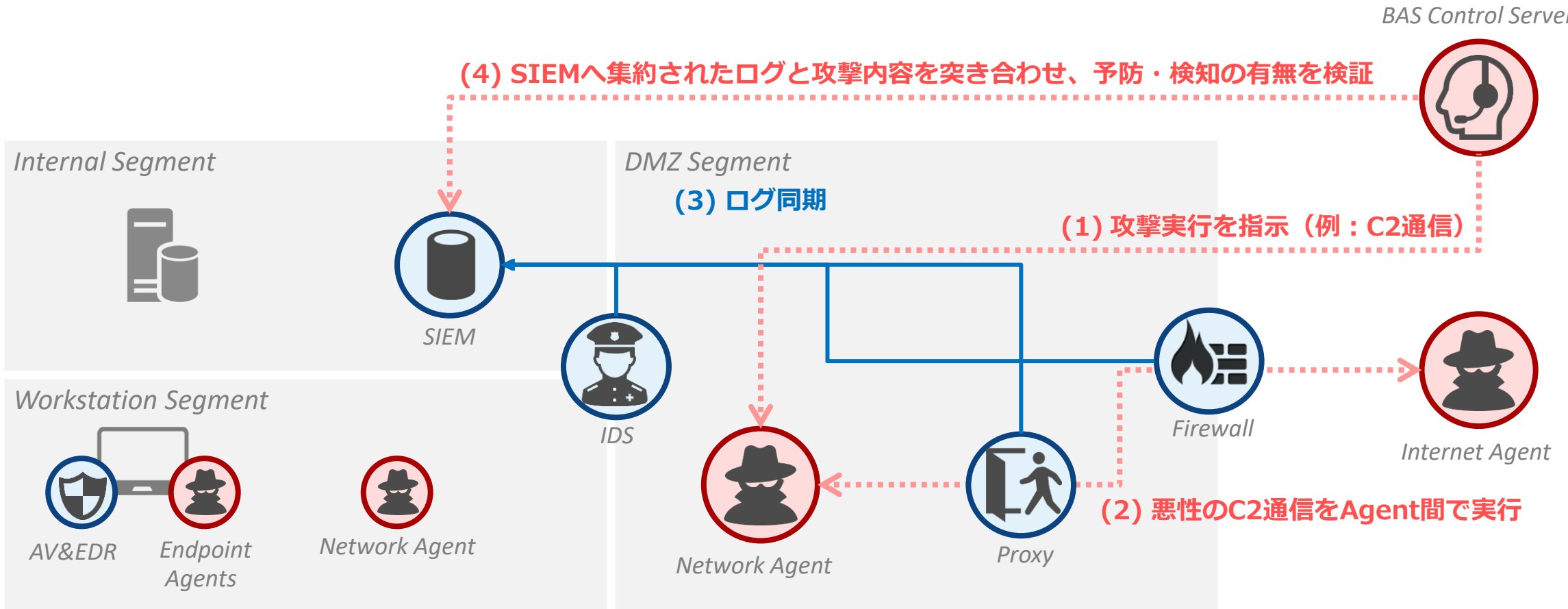
– 一般的な展開と挙動は以下の通り。
  - BASは、Control ServerとAgent（Network・Endpoint）で構成されている。
  - 基本的には、Agent間で悪意のある挙動（Malicious Activity）を実行し、その予防・検知状況をSIEMと突合して検証するメカニズムで動いている。



3-2 : Threat Intelligence for Defensive Architecture

BAS : Breach & Attack Simulation

– 一般的な展開と挙動は以下の通り。
  - BASは、Control ServerとAgent（Network・Endpoint）で構成されている。
  - 基本的には、Agent間で悪意のある挙動（Malicious Activity）を実行し、その予防・検知状況をSIEMと突合して検証するメカニズムで動いている。



3-2 : Threat Intelligence for Defensive Architecture

BAS : Breach & Attack Simulation

– BAS製品としては、商用・オープンソース共に存在する。

COTS : Commercial Product

ATTACKIQ

VERODIN
NOW PART OF FIREEYE

SafeBreach

RELIAQUEST

TEAR DROP

PCYSYS

PICUS

XM CYBER

Cymulate

Open-Source Alternatives

Uber METTA

RTA
Red Team Automation

MITRE CALDERA

UNFETTER

Infection Monkey
powered by Guardicore

nextron systems
APT Simulator

Invoke-Adversary

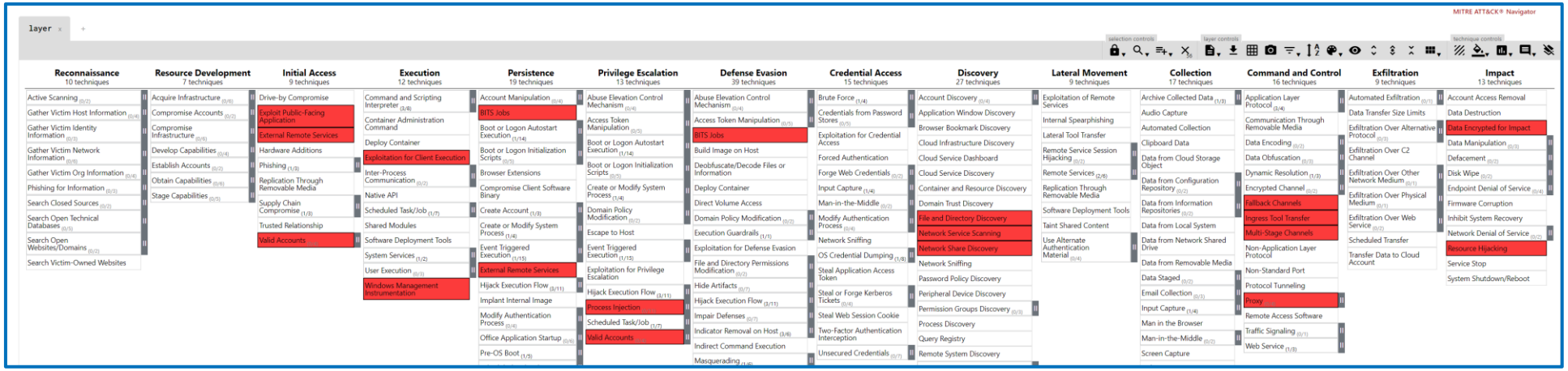
Network Flight Simulator

3-2：Threat Intelligence for Defensive Architecture

- **背後にある考え方①：Purple Teaming**
  - 攻撃側（**Red Team**）と 防御側（**Blue Team**）が**侵入テスト（Adversary Emulation）**の結果などを持ち寄り、何が問題なのか、どうすれば改善できるのか議論し、改善につなげていく活動
  - Microsoft John Lambert氏 (*1) 「侵入テストの報告書は成績表ではない、改善を行うインプットである」
  - 侵入テストは、攻撃グループの攻撃シナリオに沿って、MITRE ATT&CKの一連のTacticsを実施する為、脅威への態勢を評価できる。但し、準備・改善等も踏まえると、年１回しか実現することが難しい。

→ 最新の脅威に追従することが難しい…！？

MITRE ATT&CK Navigatorを使い、APT41の攻撃手法をマッピングした例



（*1）MITRE ATT&CKcon 2018　Keynote
https://www.slideshare.net/attackcon2018/mitre-attckcon-2018-keynote-advancing-infosec-john-lambert-microsoft
https://www.youtube.com/watch?v=yslLIqfOKCU

3-2：Threat Intelligence for Defensive Architecture

- **背後にある考え方②：Atomic Purple Teaming**
  - **Atomic Red Teaming**　：https://github.com/redcanaryco/atomic-red-team
    - 攻撃者が利用するテクニックを簡単にテストする手法をまとめたプロジェクト。
    - これを使うことにより、自社のセキュリティコントロールが機能するか簡単にチェックできる。
  - **Atomic Purple Teaming**　：https://github.com/DefensiveOrigins/AtomicPurpleTeam
    - Atomic Red Teamingを発展させた考え方。「特定の攻撃手法を実施 → 検知有無を確認 → 対策」というサイクルを回していく考え方で、最新の脅威に対応しやすくなる。この実現に、BASを活用することができる。

T1003.001
OS Credential Dumping (LSASS Memory)

Atomic Test #3 - Dump LSASS.exe Memory using comsvcs.dll

The memory of lsass.exe is often dumped for offline credential theft attacks. This can be achieved with a built-in dll.

Upon successful execution, you should see the following file created $env:TEMP\lsass-comsvcs.dmp.

Supported Platforms: Windows

auto_generated_guid: 2536dee2-12fb-459a-8c37-971844fa73be

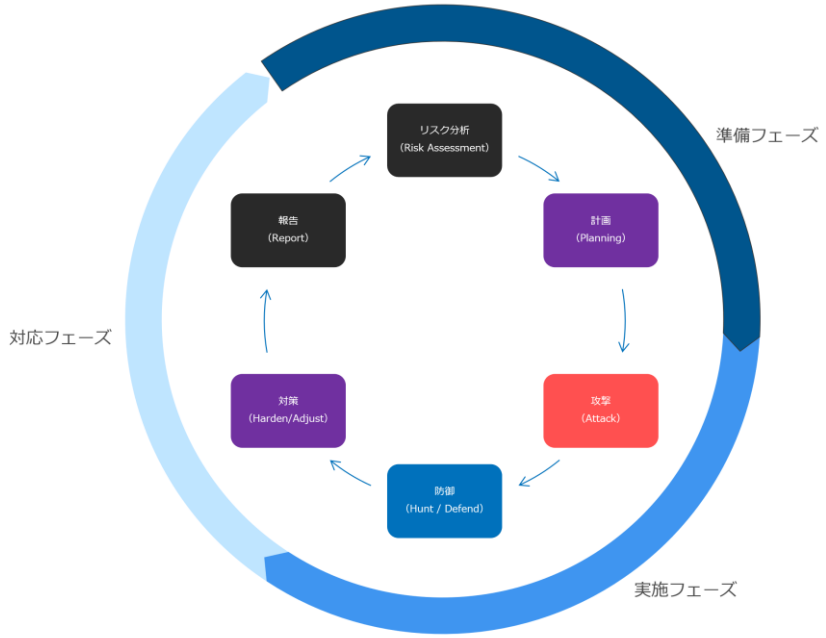
Attack Commands: Run with `powershell` ! Elevation Required (e.g. root or admin)

```
C:\Windows\System32\rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump (Get-Process lsass).id $env:TEMP\lsass-comsvcs.dmp full
```

Cleanup Commands:

```
Remove-Item $env:TEMP\lsass-comsvcs.dmp -ErrorAction Ignore
```

Atomic Purple Teaming Cycle



https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1003.001/T1003.001.md

4 : Strategic Intelligence

4-1：Strategic Intelligence

経営層・リーダに、セキュリティリスクの意思決定・投資判断を行うためには、以下の３点を適切に伝える必要がある。

- **（１）サイバー攻撃に関する傾向・トレンド**
  - Ex）二重脅迫型ランサムウェアについて
  - Ex）他社・他業種における攻撃動向について

- **（２）外部マクロ環境に関する情報**
  - 経営者が意思決定する一つの基準として、同業他社の動向、法的規制、世間動向などには非常に敏感となる。そのため、適切な情報のインプットを行うことで、判断基準を形成していく必要がある。
    - Ex）規制・新しい技術動向・他社の取り組みなど
    - Ex）Zero-Trust Architectureについて
  - **PESTLEフレームワーク**を応用すると整理しやすい（もともとは、マーケティング用語）

- **（３）内部環境に関する情報（= KPI/KRI）**
  - Strategic Intelligenceを提供し、投資・意思決定の必要性を理解していると、次は必ず「うちはどうなっているんだ？」と質問されるはずである。そのため、KPI・KRIを使い、自社のセキュリティリスク（**内部情報**）をインプットしておく必要がある。
  - KPI作成例：BAS（Breach & Attack Simulation）

4-1：Strategic Intelligence

PESTLEフレームワーク：外部マクロ環境を構成する６つの観点

Political	**政治的要因**とは、自社に関連する政治的醸成（訴訟・特定の国・組織・団体とのトラブル）を分析し、必要なリスクを訴求する。
Economic	**経済的要因**とは、他社事例の被害額、自社データの価値などを算出しながら、必要な投資やリスクを訴求する。
Social	**社会的要因**とは、セキュリティに対する世論の考え方・反応・意見、および同業他社・異業種の取り組みを参考にしながら、自社のセキュリティ状況と比較し、投資やリスクを訴求する。
Technological	**技術的要因**では、新しい技術動向・トレンド情報から、必要なセキュリティ投資やリスクを訴求する。
Legal	**法的要因**（政府方針・業界団体による規制・ガイドライン）などをトリガーに、必要なセキュリティ投資やリスクを訴求する。
Environmental	**環境要因**では、他社攻撃情報・脅威動向をもとに、必要なセキュリティ投資やリスクを訴求する。

5：まとめ

5：脅威インテリジェンス活用の目的

- **「脅威インテリジェンス」の目的（再掲）**
  - 「**より高度（効率的・効果的）なセキュリティリスク管理**」のため
  - 一方、脅威は所詮「管理できない要素」である。そのため、敵を知ることは大事だが、「リスク管理」の高度化という目的から外れないように注意する必要がある。
  - 「誰にとって役立つ情報を提供するか？」、「満たすべき要件は何か？」を確認する。
    - Strategic・Operational・Tactical
    - 4A条件（Accurate・Audience-Focused・Actionable・Adequate Timing）

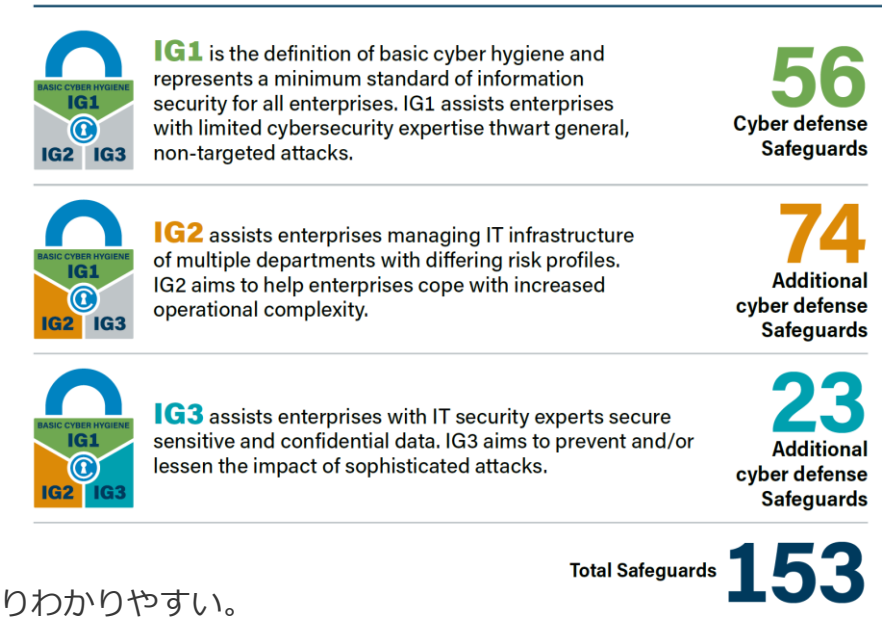
5：脅威インテリジェンス活用に向けた組織の成熟度

- **脅威インテリジェンスの最大活用には、一定の成熟度が必要！**
  - **Cyber Hygiene（サイバー公衆衛生）**＋“**Passive Defense**”ができる程度の成熟度は必要

- **Cyber Hygiene（サイバー公衆衛生）：セキュリティ基本対策の徹底**
  - 以前：CIS Controlsの1~6を実装すること（by CIS Critical Security Control）@ V7

  - **2021年５月に公表されたCIS Control V8では、CSCの定義が大きく変わったので注意が必要！**
    - Critical Security Control の数　：20個 → 18個
    - 各CIS Controlへ小項目（Safeguards）を定義　：153種類
    - 153種類の小項目を３つのグループに分類　：IG1~IG3

    - IG1（Implementation Group 1）に分類される56個の施策
    → **Basic Cyber Hygieneとして定義！**

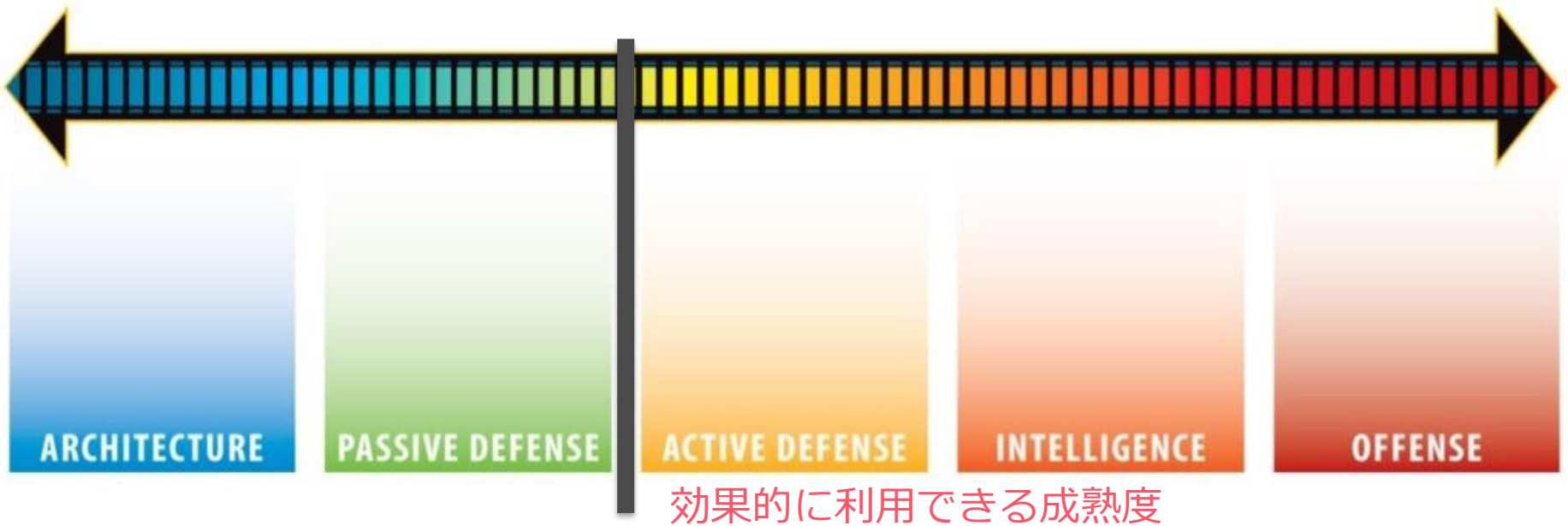


詳細は、以下を参照のこと。『CIS Controls v8 Implementation Groups』がコンパクトにまとまっておりわかりやすい。
https://www.cisecurity.org/controls/v8/

5：脅威インテリジェンス活用に向けた組織の成熟度

- **脅威インテリジェンスの最大活用には、一定の成熟度が必要！**
  - **Cyber Hygiene（サイバー公衆衛生）**＋“**Passive Defense**”ができる程度の成熟度は必要

- **Sliding Scale of Cybersecurity：サイバーセキュリティ態勢の成熟度モデル**
  - SANS InstructorのRobert M. Leeにより、2015年に提唱されたモデル
  - **Architecture**　：セキュリティを念頭にシステム計画・構築・維持を行う態勢があること
  - **Passive Defense**　：人が継続的に関与せず、一貫性のある防御メカニズムを有している状態
    ⇒ シグニチャベース（+一部の振る舞い検知）の検知・対応



Thank You!