



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。

$$\text{脅威インテリジェンス} = \text{脅威} + \text{インテリジェンス}$$

- **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？

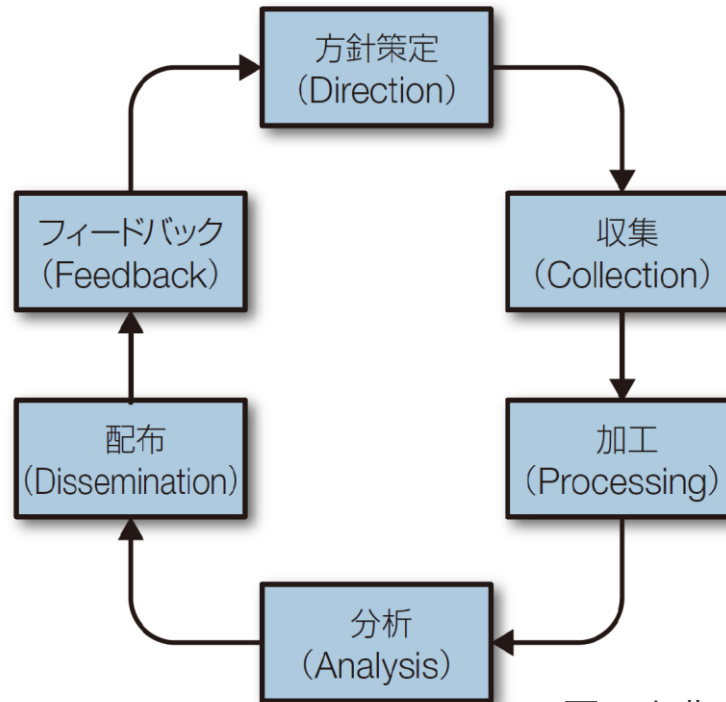
## 1-1 : 脅威インテリジェンスの定義

- 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。

$$\text{脅威インテリジェンス} = \text{脅威} + \text{インテリジェンス}$$

- **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

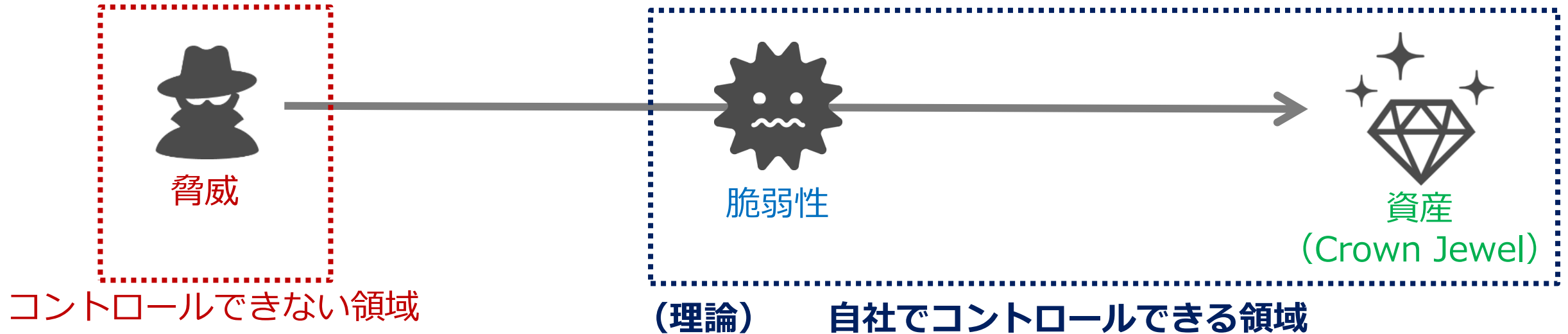
- **良いインテリジェンスの4要件 : 4A**

- **A**ccurate (正確な)
- **A**udience Focused (利用者/消費者目線である)
- **A**ctionable (アクションナブル)
- **A**dequate Timing (適切なタイミング)



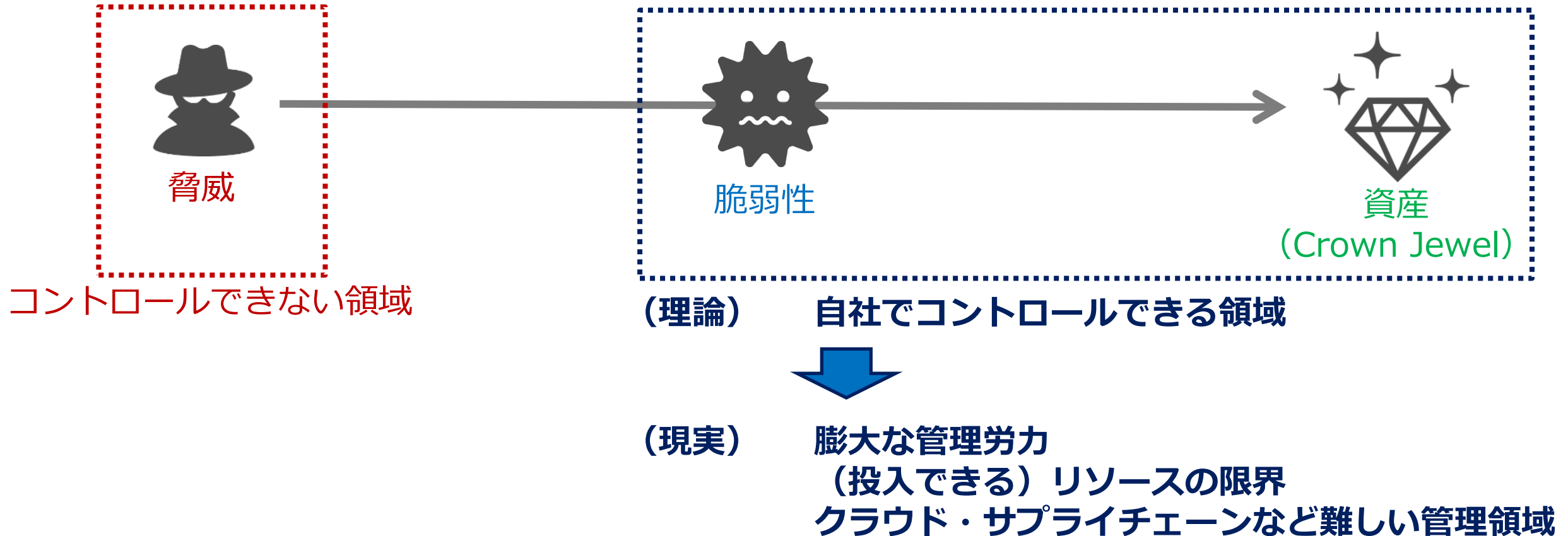
## 1-2 : 脅威インテリジェンスの目的・必要性

- 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**



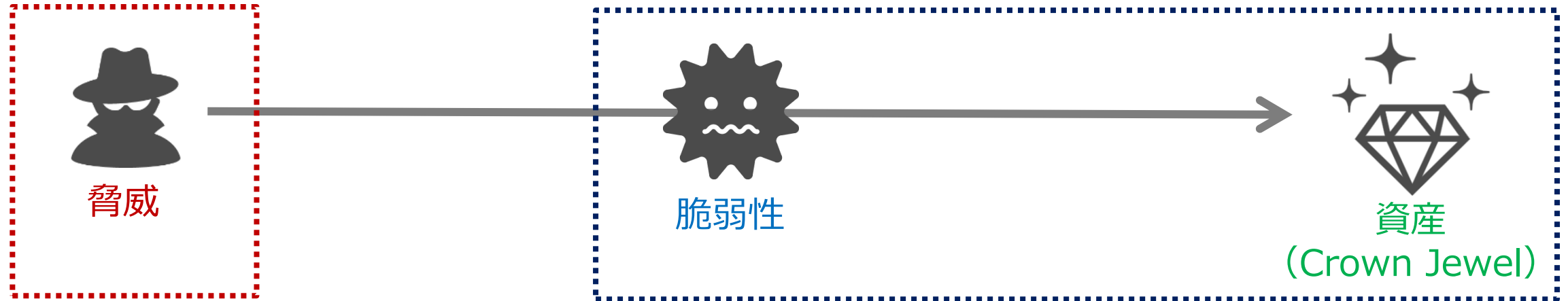
## 1-2：脅威インテリジェンスの目的・必要性

- 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**



## 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。

Long Term



## *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。

Short Term



## *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なため、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/>

*T*actics



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)

*T*echniques



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**

*P*rocedures



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 **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（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](#)』

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Deploy Container	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Web Service (2)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)	Create Account (3)	Domain Policy Modification (2)	Direct Volume Access	Man-in-the-Middle (2)	Container and Resource Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Endpoint Denial of Service (4)	Firmware Corruption
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Domain Trust Discovery	Modify Authentication Process (4)	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Endpoint Denial of Service (2)	Inhibit System Recovery
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Execution Guardrails (1)	File and Directory Permissions Modification (2)	Network Sniffing	Network Service Scanning	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Endpoint Denial of Service (2)	Network Denial of Service (2)
Search Victim-Owned Websites			System Services (2)	External Remote Services	Exploitation for Privilege Escalation	Hide Artifacts (7)	OS Credential Dumping (8)	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol	Resource Hijacking	Service Stop
			User Execution (3)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Steal Application Access Token	Network Sniffing		Data from Network Shared Drive	Non-Standard Port	Resource Hijacking	System Shutdown/Reboot
			Windows Management Instrumentation	Implant Internal Image	Process Injection (11)	Process Injection (11)	Steal or Forge Kerberos Tickets (4)	Password Policy Discovery		Data from Removable Media	Protocol Tunneling	Resource Hijacking	System Shutdown/Reboot
				Modify Authentication Process (4)	Scheduled Task/Job (7)	Scheduled Task/Job (7)	Steal Web Session Cookie	Peripheral Device Discovery		Data Staged (2)	Proxy (4)	Resource Hijacking	System Shutdown/Reboot
					Valid Accounts (4)	Valid Accounts (4)	Two-Factor	Process Discovery		Email Collection (3)	Remote Access Software	Resource Hijacking	System Shutdown/Reboot
							Query Registry	Query Registry		Input Capture (4)	Traffic Signaling (1)	Resource Hijacking	System Shutdown/Reboot
										Man in the Browser	Web Service (3)	Resource Hijacking	System Shutdown/Reboot

# 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

ATT&CK Matrix for Enterprise

layout: side show sub-techniques hide sub-techniques

### (1) Tactics (戦術)

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Deobfuscate/Decode Files or Information	Credentials from Memory (4)	Application Window	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Deploy Container	Forced Authentication	Cloud Infrastructure Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Direct Volume Access	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Clipboard Data	Data from Cloud Storage Object	Data Manipulation (3)	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browse Extensions	Create or Modify System Process (4)	Domain Policy Modification (2)	Input Capture (4)	Cloud Service Discovery	Remote Services (6)	Data from Configuration Repository (2)	Dynamic Resolution (3)	Exfiltration Over C2 Channel	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Execution Guardrails (1)	Man-in-the-Middle (2)	Container and Resource Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Encrypted Channel (2)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)	Create Account (3)	Escape to Host	File and Directory Permissions Modification (2)	Modify Authentication Process (4)	Domain Trust Discovery	Software Deployment Tools	Data from Local System	Fallback Channels	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Trusted Relationship	Valid Accounts (4)	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Firmware Corruption
Search Open Websites/Domains (2)	Software Deployment Tools		Software Deployment Tools	Event Triggered Execution (15)	Exploit for Privilege Escalation	Hide Artifacts (7)		Network Service Scanning	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Inhibit System Recovery	
Search Victim-Owned Websites	System Services (2)		System Services (2)	External Remote Services	Hijack Execution Flow (11)	Hijack Execution Flow (11)		Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol	Network Denial of Service (2)	Resource Hijacking
	User Execution (3)		User Execution (3)	Hijack Execution Flow (11)	Process Injection (11)	Impair Defenses (7)		Network Sniffing		Data Staged (2)	Non-Standard Port	Scheduled Transfer	Service Stop
	Windows Management Instrumentation		Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (7)	Indicator Removal on Host (6)		Password Policy Discovery		Per Dis	Protocol Tunneling	Transfer Data to Cloud Account	System Shutdown/Reboot
	Modify Authentication Process (4)		Modify Authentication Process (4)	Office Application Startup (6)	Valid Accounts (4)	Indirect Command Execution		Per Dis		Per Dis			
	Office Application Startup (6)		Office Application Startup (6)			Masquerading (6)		Process Discovery		Query Registry			
								Query Registry		Man in the Browser	Traffic Signaling (1)		
								Remote System Discovery		Man-in-the-Middle	Web Service (3)		

### (2) Techniques (戦術)

### (2') Sub-Techniques


- OS Credential Dumping (8)
  - LSASS Memory
  - Security Account Manager
  - NTDS
  - DCSync
  - Proc Filesystem
  - /etc/passwd and /etc/shadow
  - Cached Domain Credentials
  - LSA Secrets

# 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 2018

D2-3 知れば組織が強くなる！ペネトレーションテスト  
で分かったセキュリティ対策の抜け穴

### 丸ごとわかるペネトレーションテストの今

2018年11月28日

NRIセキュアテクノロジーズ株式会社  
サイバーセキュリティサービス事業本部  
サイバーセキュリティサービス部

セキュリティコンサルタント

石川 朝久, Ph.D., CISSP, CSSLP, CISA, CISM, CFE, PMP



### 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/>



Tokio Marine Holdings

To Be a Good Company

Internet Week 2019

D2-3 組織を更に強くする「攻めの」サイバー攻撃対策

### 攻撃者をあぶりだせ！！ プロアクティブなセキュリティアプローチ

2019年11月27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



# 3 : Operational Intelligence

~ Threat Intelligence for Defensive Architecture ~



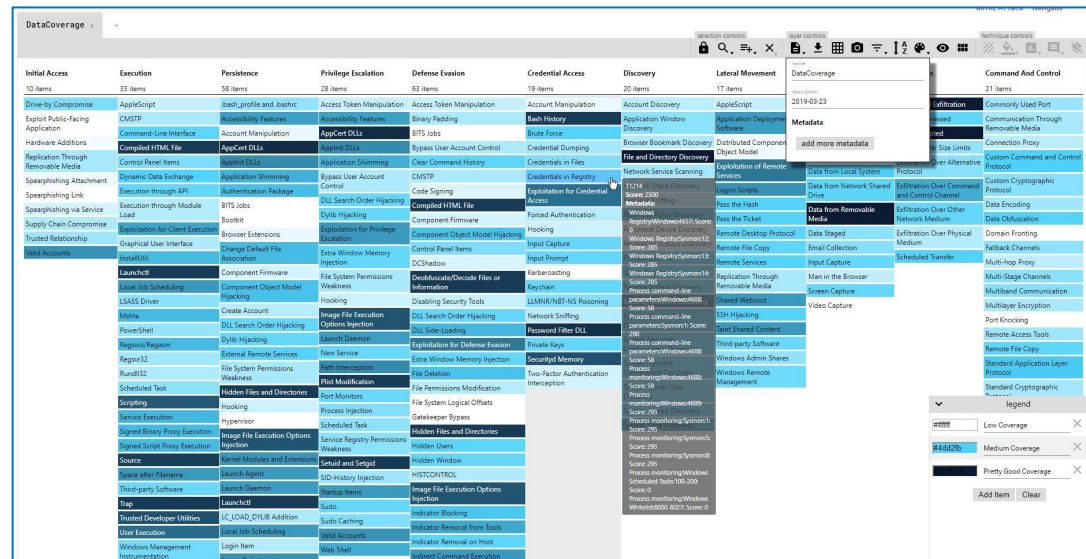
# 3-2 : Threat Intelligence for Defensive Architecture

- **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

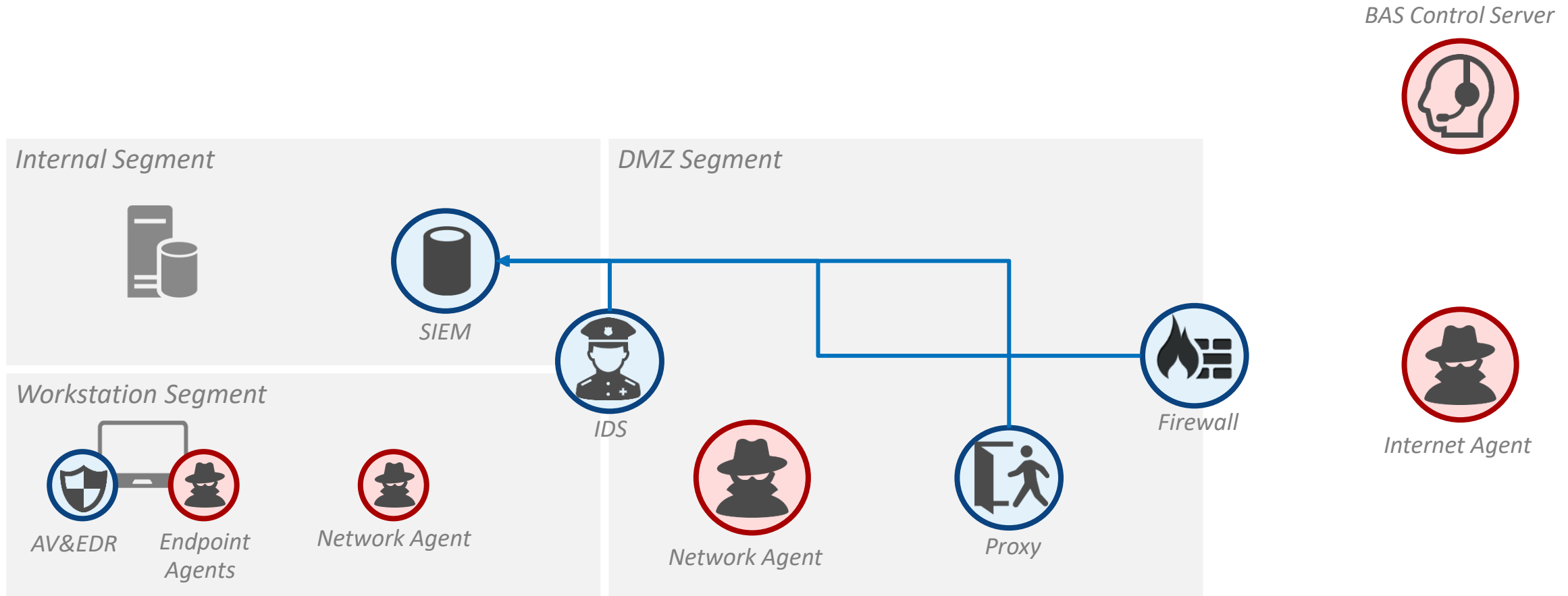
The screenshot displays the MITRE ATT&CK Navigator interface. The main area is a grid of attack techniques, each represented by a colored cell. The columns are categorized by attack phase: Initial Access (10 items), Execution (33 items), Persistence (58 items), Privilege Escalation (28 items), Defense Evasion (63 items), Credential Access (19 items), Discovery (20 items), Lateral Movement (17 items), and Command And Control (21 items). A tooltip for the 'DataCoverage' technique is open, showing its name, description (2019-03-23), and a 'Metadata' section with an 'add more metadata' button. A legend in the bottom right corner defines coverage levels: #ffffff for Low Coverage, #4d2fb for Medium Coverage, and #1f4e79 for Pretty Good Coverage. The interface also includes various control panels for selection, layer, and technique controls.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Command And Control
10 items	33 items	58 items	28 items	63 items	19 items	20 items	17 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Exfiltration
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Commonly Used Port
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Communication Through Removable Media
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Connection Proxy
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Custom Command and Control Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Sniffing	Pass the Hash	Custom Cryptographic Protocol
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Peripheral Device Discovery	Pass the Ticket	Data Encoding
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Process Discovery	Remote Desktop Protocol	Data Obfuscation
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Process command-line parameters: Windows:4657: Score: 0	Remote File Copy	Domain Fronting
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Control Panel Items	Input Capture	Process command-line parameters: Sysmon:12: Score: 285	Remote Services	Fallback Channels
	InstallUtil	Change Default File Association	File System Permissions Weakness	DCShadow	Input Prompt	Process command-line parameters: Sysmon:13: Score: 285	Replication Through Removable Media	Multi-hop Proxy
	Launchctl	Component Firmware	Image File Execution Options Injection	DLL Search Order Hijacking	Kerberoasting	Process command-line parameters: Sysmon:14: Score: 285	Shared Webroot	Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Launch Daemon	DLL Side-Loading	Keychain	Process command-line parameters: Windows:4688: Score: 58	Taint Shared Content	Multiband Communication
	LSASS Driver	Create Account	New Service	Exploitation for Defense Evasion	LLMNR/NBT-NS Poisoning	Process command-line parameters: Windows:4688: Score: 58	Third-party Software	Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Path Interception	Extra Window Memory Injection	Network Sniffing	Process command-line parameters: Sysmon:1: Score: 290	Windows Admin Shares	Port Knocking
	PowerShell	Dylib Hijacking	Plist Modification	File Deletion	Password Filter DLL	Process command-line parameters: Windows:4688: Score: 58	Windows Remote Management	Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Port Monitors	File Permissions Modification	Private Keys	Process command-line parameters: Sysmon:5: Score: 295		Remote File Copy
	Regsvr32	File System Permissions Weakness	Process Injection	Gatekeeper Bypass	Securityd Memory	Process command-line parameters: Sysmon:8: Score: 295		Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Scheduled Task	Hidden Files and Directories	Two-Factor Authentication Interception	Process command-line parameters: Sysmon:1: Score: 295		Standard Cryptographic Protocol
	Scheduled Task	Hidden Files and Directories	Service Registry Permissions Weakness	Hidden Users		Process monitoring: Windows:4689: Score: 295		
	Scripting	Hooking	Setuid and Setgid	Hidden Window		Process monitoring: Sysmon:5: Score: 295		
	Service Execution	Hypervisor	SID-History Injection	HISTCONTROL		Process monitoring: Windows Scheduled Tasks:100-200: Score: 0		
	Signed Binary Proxy Execution	Image File Execution Options Injection	Startup Items	Image File Execution Options Injection		Process monitoring: Windows Whitelist:8000-8027: Score: 0		
	Signed Script Proxy Execution	Image File Execution Options Injection	Sudo	Indicator Blocking				
	Source	Kernel Modules and Extensions	Sudo Caching	Indicator Removal from Tools				
	Space after Filename	Launch Agent	Valid Accounts	Indicator Removal on Host				
	Third-party Software	Launch Daemon	Web Shell	Indirect Command Execution				
	Trap	Launchctl						
	Trusted Developer Utilities	LC_LOAD_DYLIB Addition						
	User Execution	Local Job Scheduling						
	Windows Management Instrumentation	Login Item						
		Logon Scripts						

## 3-2 : Threat Intelligence for Defensive Architecture

### BAS : Breach & Attack Simulation

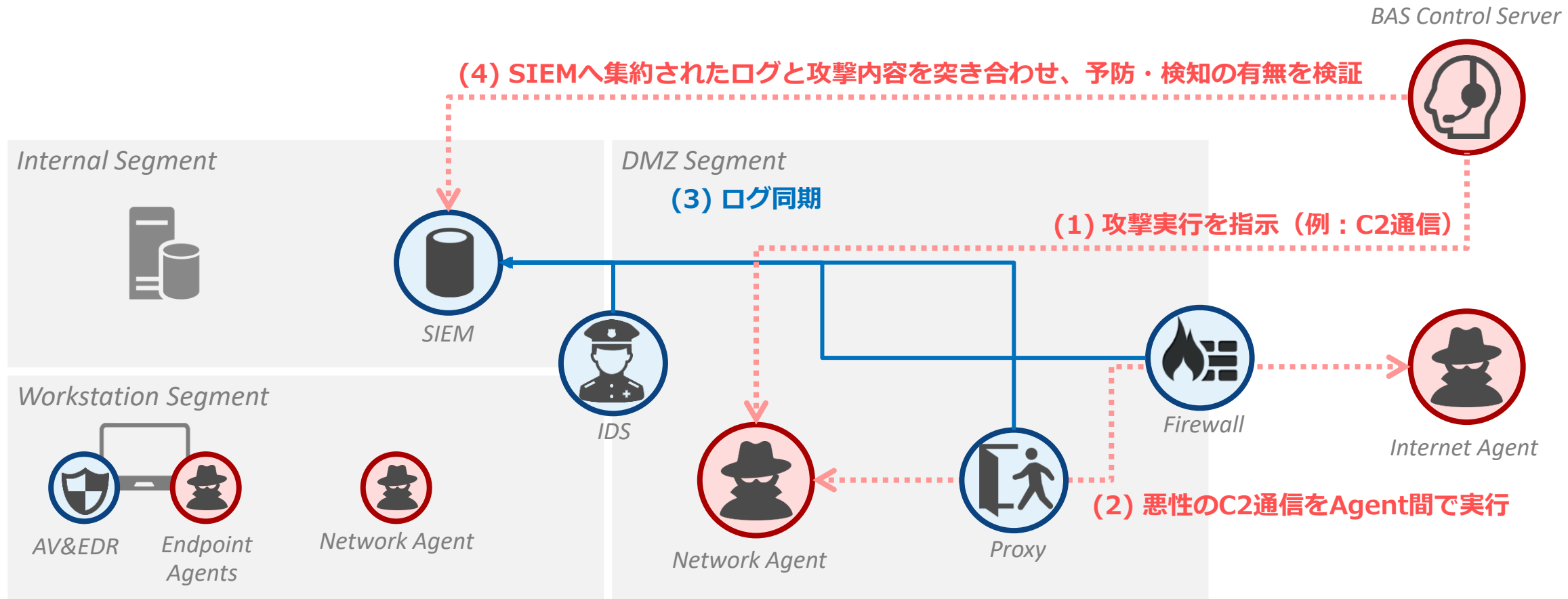
- 一般的な展開と挙動は以下の通り。
  - BASは、Control ServerとAgent（Network・Endpoint）で構成されている。
  - 基本的には、Agent間で悪意のある挙動（Malicious Activity）を実行し、その予防・検知状況をSIEMと突合して検証するメカニズムで動いている。



## 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

ATTACK IQ

VERODIN  
NOW PART OF FIREEYE

SafeBreach

RELIAQUEST

TEAR  
DROP

PCYSYS

PICUS

XM CYBER

Cymulate

### Open-Source Alternatives

Uber  
METTA



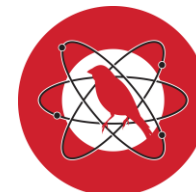
RTA  
Red Team Automation

MITRE  
CALDERA

UN/FETTER

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

Tactic	Technique
Reconnaissance	Acquire Infrastructure
Reconnaissance	Compromise Accounts
Reconnaissance	External Remote Services
Reconnaissance	Develop Capabilities
Reconnaissance	Establish Accounts
Reconnaissance	Obtain Capabilities
Reconnaissance	Stage Capabilities
Reconnaissance	Search Open Technical Databases
Reconnaissance	Search Open Websites/Domains
Reconnaissance	Search Victim-Owned Websites
Resource Development	Acquire Infrastructure
Resource Development	Compromise Accounts
Resource Development	External Remote Services
Resource Development	Develop Capabilities
Resource Development	Establish Accounts
Resource Development	Obtain Capabilities
Resource Development	Stage Capabilities
Resource Development	Search Open Technical Databases
Resource Development	Search Open Websites/Domains
Resource Development	Search Victim-Owned Websites
Initial Access	Drive-by-Compromise
Initial Access	Digital Public-Facing Application
Initial Access	External Remote Services
Initial Access	Hardware Additions
Initial Access	Phishing
Initial Access	Replication Through Removable Media
Initial Access	Supply Chain Compromise
Initial Access	Trusted Relationship
Initial Access	Valid Accounts
Execution	Command and Scripting Interpreter
Execution	Container Administration Command
Execution	Deploy Container
Execution	Exploitation for Client Execution
Execution	Inter-Process Communication
Execution	Native API
Execution	Scheduled Task/Job
Execution	Shared Modules
Execution	Software Deployment Tools
Execution	System Services
Execution	User Execution
Execution	Windows Management Instrumentation
Persistence	Account Manipulation
Persistence	BITS Jobs
Persistence	Boot or Logon Autostart Execution
Persistence	Boot or Logon Initialization Scripts
Persistence	Browser Extensions
Persistence	Compromise Client Software Binary
Persistence	Create Account
Persistence	Create or Modify System Process
Persistence	Event Triggered Execution
Persistence	Exploitation for Privilege Escalation
Persistence	External Remote Services
Persistence	Hijack Execution Flow
Persistence	Implant Internal Image
Persistence	Modify Authentication Process
Persistence	Office Application Startup
Persistence	Pre-OS Boot
Persistence	Scheduled Task/Job
Persistence	Valid Accounts
Privilege Escalation	Abuse Elevation Control Mechanism
Privilege Escalation	Access Token Manipulation
Privilege Escalation	Boot or Logon Autostart Execution
Privilege Escalation	Boot or Logon Initialization Scripts
Privilege Escalation	Browser Extensions
Privilege Escalation	Create or Modify System Process
Privilege Escalation	Domain Policy Modification
Privilege Escalation	Domain Policy Modification
Privilege Escalation	Escape to Host
Privilege Escalation	Event Triggered Execution
Privilege Escalation	Exploitation for Privilege Escalation
Privilege Escalation	Hijack Execution Flow
Privilege Escalation	Process Injection
Privilege Escalation	Scheduled Task/Job
Privilege Escalation	Valid Accounts
Defense Evasion	Abuse Elevation Control Mechanism
Defense Evasion	Access Token Manipulation
Defense Evasion	Build Image on Host
Defense Evasion	Deobfuscate/Decode Files or Information
Defense Evasion	Deploy Container
Defense Evasion	Direct Volume Access
Defense Evasion	Domain Policy Modification
Defense Evasion	Domain Policy Modification
Defense Evasion	Execution Guardrails
Defense Evasion	Exploitation for Defense Evasion
Defense Evasion	Hide Artifacts
Defense Evasion	Hijack Execution Flow
Defense Evasion	Impair Defenses
Defense Evasion	Indicator Removal on Host
Defense Evasion	Indirect Command Execution
Defense Evasion	Masquerading
Credential Access	Brute Force
Credential Access	Credentials from Password Stores
Credential Access	Exploitation for Credential Access
Credential Access	Forced Authentication
Credential Access	Forge Web Credentials
Credential Access	Input Capture
Credential Access	Man-in-the-Middle
Credential Access	Modify Authentication Process
Credential Access	Network Sniffing
Credential Access	OS Credential Dumping
Credential Access	Steal Application Access Tokens
Credential Access	Steal or Forge Kerberos Tickets
Credential Access	Steal Web Session Cookie
Credential Access	Two-Factor Authentication Interception
Credential Access	Unsecured Credentials
Discovery	Account Discovery
Discovery	Application Window Discovery
Discovery	Browser Bookmark Discovery
Discovery	Cloud Infrastructure Discovery
Discovery	Cloud Service Dashboard
Discovery	Cloud Service Discovery
Discovery	Container and Resource Discovery
Discovery	Domain Trust Discovery
Discovery	File and Directory Discovery
Discovery	Network Service Scanning
Discovery	Network Share Discovery
Discovery	Network Sniffing
Discovery	OS Credential Dumping
Discovery	Steal Application Access Tokens
Discovery	Steal or Forge Kerberos Tickets
Discovery	Steal Web Session Cookie
Discovery	Two-Factor Authentication Interception
Discovery	Unsecured Credentials
Discovery	Remote System Discovery
Lateral Movement	Exploitation of Remote Services
Lateral Movement	Internal Spearphishing
Lateral Movement	Lateral Tool Transfer
Lateral Movement	Remote Services
Lateral Movement	Software Deployment Tools
Lateral Movement	Taint Shared Content
Lateral Movement	Use Alternate Authentication Material
Collection	Archive Collected Data
Collection	Audio Capture
Collection	Automated Collection
Collection	Clipboard Data
Collection	Data from Cloud Storage
Collection	Data from Configuration Repository
Collection	Data from Information Repositories
Collection	Data from Local System
Collection	Data from Network Shared Drive
Collection	Data from Removable Media
Collection	Data Staged
Collection	Email Collection
Collection	Input Capture
Collection	Man in the Browser
Collection	Man-in-the-Middle
Collection	Screen Capture
Command and Control	Application Layer Protocol
Command and Control	Communication Through Removable Media
Command and Control	Data Encoding
Command and Control	Data Obfuscation
Command and Control	Dynamic Resolution
Command and Control	Fallback Channels
Command and Control	Ingress Tool Transfer
Command and Control	Multi-Stage Channels
Command and Control	Non-Application Layer Protocol
Command and Control	Non-Standard Port
Command and Control	Protocol Tunneling
Command and Control	Remote Access Software
Command and Control	Traffic Signaling
Command and Control	Web Service
Exfiltration	Automated Exfiltration
Exfiltration	Data Transfer Size Limits
Exfiltration	Exfiltration Over Alternative Protocol
Exfiltration	Exfiltration Over C2 Channel
Exfiltration	Exfiltration Over Other Network Medium
Exfiltration	Exfiltration Over Physical Medium
Exfiltration	Exfiltration Over Web Service
Exfiltration	Scheduled Transfer
Exfiltration	Transfer Data to Cloud Account
Impact	Account Access Removal
Impact	Data Destruction
Impact	Data Encrypted for Impact
Impact	Data Manipulation
Impact	Defacement
Impact	Disk Wipe
Impact	Endpoint Denial of Service
Impact	Firmware Corruption
Impact	Inhibit System Recovery
Impact	Network Denial of Service
Impact	Resource Hijacking
Impact	Service Stop
Impact	System Shutdown/Reboot

(\*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=yslIqfOKCU>

## 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

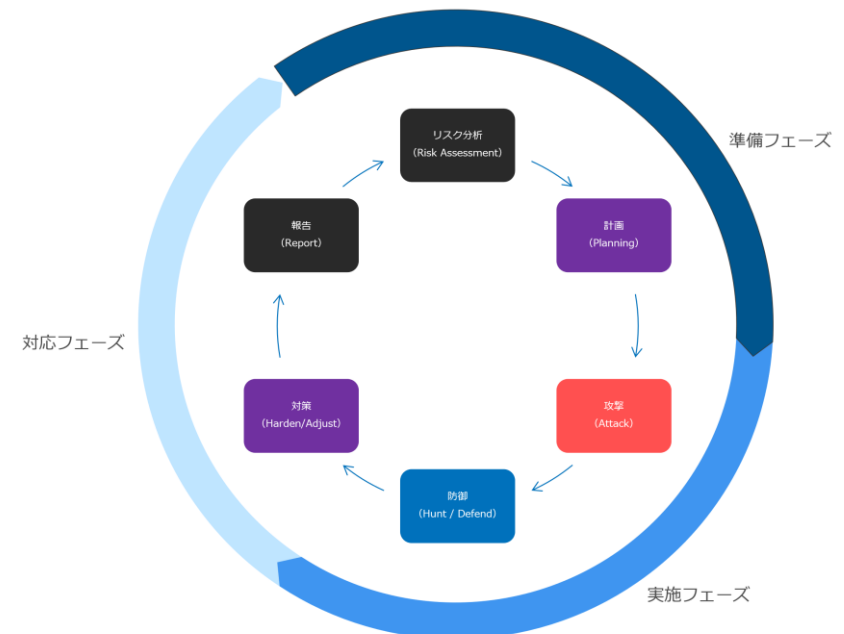
Attack Commands: Run with **powershell** ! Elevation Required (e.g. root or admin)

```
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



## 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

<b>P</b> <i>olitical</i>		<b>政治的要因</b> 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。
<b>E</b> <i>conomic</i>		<b>経済的要因</b> 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。
<b>S</b> <i>ocial</i>		<b>社会的要因</b> 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。
<b>T</b> <i>echnological</i>		<b>技術的要因</b> 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。
<b>L</b> <i>egal</i>		<b>法的要因</b> （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。
<b>E</b> <i>nvironmental</i>		<b>環境要因</b> 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、敵を知ることが大事だが、「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！**



**IG1** is the definition of basic cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

**56**  
Cyber defense Safeguards



**IG2** assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

**74**  
Additional cyber defense Safeguards



**IG3** assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

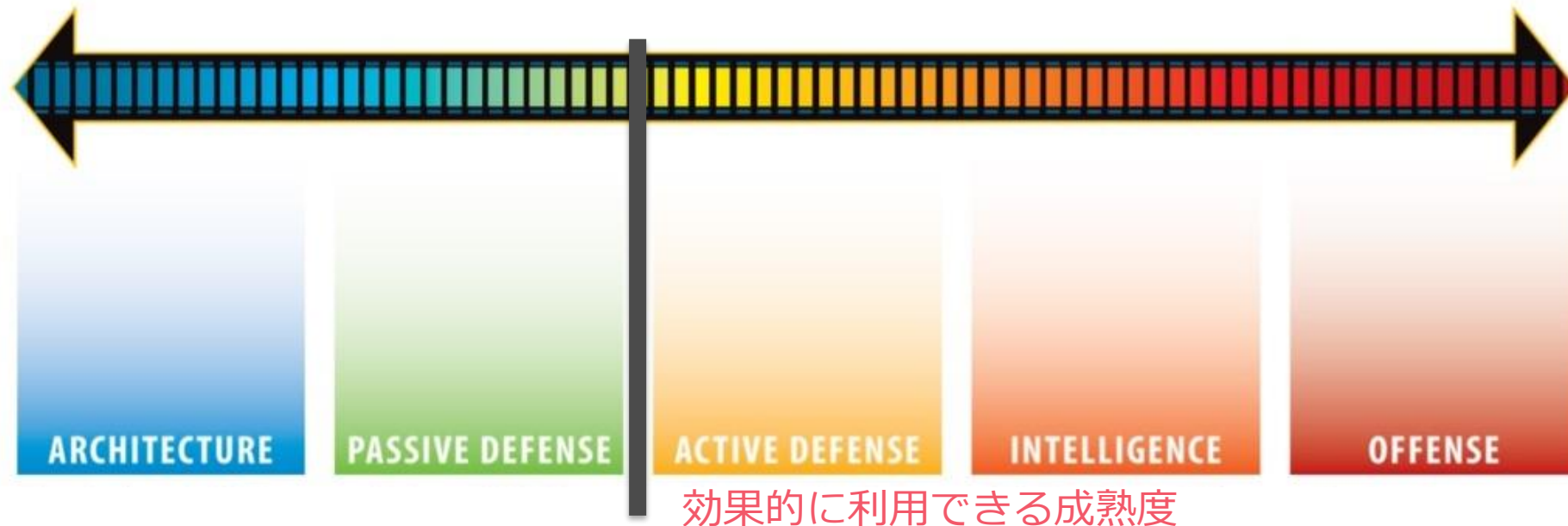
**23**  
Additional cyber defense Safeguards

Total Safeguards **153**

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!***