

新27002への対応

MITER ATT&CK[®]を活用した“脅威インテリジェンス”

2024. 6. 14

JSSA

情報セキュリティ研究プロジェクト

目次

1. 情報セキュリティ研究プロジェクトの活動

- (1) 2023年度 研究テーマと概要
- (2) 研究プロジェクトメンバー
- (3) 2023年度 研究の発端と目的

2. ISO/IEC 27002 : 2022の管理策

- (1) 改訂
- (2) 追加された管理策
- (3) 管理策 5.7 Threat intelligence
- (4) 脅威インテリジェンスと連関する管理策

3. 脅威インテリジェンス

- (1) ISO/IEC 27002-2022 – 5.7項 –
- (2) NIST の定義及びセキュリティ要件
- (3) 脅威インテリジェンスに対応する組織担当と役割

4. 脅威と脆弱性

- (1) 脅威と脆弱性
- (2) 脆弱性情報

5. ATT&CK®の活用例

- (1) MITRE ATT&CK®（マイターアタック）とは
- (2) MITRE ATT&CK®のNavigate
- (3) 脅威インテリジェンスをATT&CK®にマッピングするロードマップ
- (4) ATT&CK®のサイト構成
- (5) ATT&CK®開発・維持に協力を要請
- (6) ATT&CK®利用ガイダンス
- (7) ATT&CK®のフレームワークの構成内容
- (8) Tactics（攻撃者の戦術）と攻撃手法 – Matrix

6. サイバー攻撃の実態とATT&CK®フレームワーク

- (1) サイバー攻撃の実態 標的型攻撃とランサムウェア
- (2) サイバー攻撃の実態 EMOTET
- (3) EMOTETの攻撃実態
- (4) 攻撃者“Wizard Spider”が用いるソフトウェア
- (5) EMOTET攻撃者の行動とATT&CKフレームワーク

7. まとめ

8. 2024年度 PJ研究テーマ

1. 情報セキュリティ研究プロジェクトの活動

(1) 2023年度 研究テーマと概要

- ・情報セキュリティ管理策の国際規格ISO27002は2022年の改訂にて新たなサイバーセキュリティへの管理策が追加され、規格名称も「情報セキュリティ, サイバーセキュリティ及びプライバシー保護 – 情報セキュリティ管理策」に改められた。

- ・“脅威インテリジェンス”はその追加された管理策の一つである。

情報セキュリティ研究プロジェクトでは、“脅威インテリジェンス”についての研究を行うとともに、代表的な情報源であるMITER ATT&CK®の利用方法を検討した。

(2) 研究プロジェクトメンバー

成田 和弘（代表者）、山本 孟（発表者）、芳仲 宏、 木村 裕一

1. 情報セキュリティ研究プロジェクトの活動

(3) 2023年度 研究の発端と目的

- a. ISO/IEC 27002;2022では、新たなサイバーセキュリティへの管理策が追加され、規格名称も「情報セキュリティ、サイバーセキュリティ及びプライバシー保護 – 情報セキュリティ管理策」に改めたうえで、具体的管理策が求められている。（Sheet 6 参照）

11個の管理策を追加 ⇒ 組織的管理策3個、物理的管理策1個、技術的管理策7個

例えば、プライバシー保護をタイトル表記し、情報削除やデータマスキングを管理策とする

- b. “脅威インテリジェンス”はその追加された組織的管理策の一つである。

組織としてサイバースキルの向上を求め、組織能力の獲得・定着、更に獲得するCTI *の検証を課題とする。

- c. 情報セキュリティ研究プロジェクトでは、“脅威インテリジェンス”について探求するとともに、CTI獲得の実践については、次に着眼して情報源・ツールであるMITER ATT&CK®の利用を検討した。

- ① 脅威インテリジェンスには情報セキュリティポリシーと両輪をなす取組みが求められる
- ② システム監査においてもCTI獲得ツールの手法が情報収集・分析と検証に生かせる

* Cyber Threat Intelligence (CTI)

2. ISO/IEC 27002:2022の管理策

ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls

(1) 改訂

- タイトル

Information security, cybersecurity and privacy protection — Information security controls

- カテゴリ

組織的管理策、人的管理策、物理的管理策、技術的管理策

- 要求事項

管理策の連関、情報とデータ、（外的）制度要求の考慮

2. ISO/IEC 27002:2022の管理策

ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls

(2) 追加された管理策

組織的	脅威インテリジェンス	5. 7	情報セキュリティの脅威に関する情報を収集・分析し、脅威インテリジェンスを作成する必要がある。
	クラウドサービス利用時の情報セキュリティ	5. 23	クラウドサービスの調達、利用、管理、終了のプロセスは、組織の情報セキュリティ要件に従って確立する必要がある。
	事業継続のためのICT対応	5. 30	ICTの準備状況は、ビジネス継続性の目標とICT継続性の要件に基づいて計画、実装、維持、およびテストする必要がある。
物理的	物理的なセキュリティ監視	7. 4	許可されていない物理的アクセスがないか、施設を継続的に監視する必要がある。
技術的	構成管理	8. 9	ハードウェア、ソフトウェア、サービス、およびネットワークのセキュリティ構成を含む構成は、確立、文書化、実装、監視、およびレビューする必要がある。
	情報削除	8. 1	情報システム、デバイス、またはその他の記憶媒体に保存された情報は、不要になったら削除する必要がある。
	データマスキング	8. 11	データマスキングは、該当する法律を考慮して、アクセス制御に関する組織のトピック固有のポリシーおよびその他の関連するトピック固有のポリシー、およびビジネス要件に従って使用する必要がある。
	データ漏洩防止	8. 12	機密情報を処理、保存、または送信するシステム、ネットワーク、およびその他のデバイスには、データ漏洩防止対策を適用する必要がある。
	モニタリング活動	8. 16	ネットワーク、システム、およびアプリケーションの異常な動作を監視し、潜在的な情報セキュリティインシデントを評価するために適切な措置を講じる必要がある。
	Webフィルタリング	8. 23	悪意のあるコンテンツへの露出を減らすために、外部Webサイトへのアクセスを管理する必要がある。
	セキュアコーディング	8. 28	ソフトウェア開発には、安全なコーディングの原則を適用する必要がある。

[Source] ISO, ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls, ISO, 2022, pp.143-145 Annex B, Table B.1を参考に研究プロジェクトメンバが作成)

2. ISO/IEC 27002:2022の管理策

(3) 管理策 5.7 Threat intelligence – 脅威インテリジェンス

コントロール

- 情報セキュリティの脅威に関連する情報は、脅威インテリジェンスを作成するために収集および分析される必要がある

目的

- 適切な軽減措置を講じられるように、組織の脅威環境についての認識を提供する

ガイダンス

- 既存または新たな脅威に関する情報を収集および分析する目的
 - a) 脅威が組織に損害を与えることを防ぐために、情報に基づいた行動を促進する
 - b) そうした脅威の影響を軽減する
- 脅威インテリジェンスは3つの層に分けることができ、すべてを考慮する必要がある
 - a) 戦略的脅威インテリジェンス: 変化する脅威状況（攻撃者の種類や攻撃の種類など）に関する高レベルの情報の交換
 - b) 戦術的脅威インテリジェンス: 関与する攻撃者の手法、ツール、テクノロジーに関する情報
 - c) 運用上の脅威インテリジェンス: 技術指標を含む、特定の攻撃に関する詳細
- 脅威インテリジェンスがそなえる要件
 - a) 関連性がある（つまり、組織の保護に関連している）
 - b) 洞察力に優れている（すなわち、組織に脅威の状況）;
 - c) コンテキスト、状況認識を提供する（つまり、情報に基づいてコンテキストを追加する、出来事の発生時期、発生場所、過去の経験、同様の組織での蔓延）
 - d) 実用的である（つまり、組織は情報に基づいて迅速かつ効果的に行動できる）。 →次頁に続く

[Source] ISO, ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls, ISO, 2022, pp.15-16 5.7 Threat intelligenceを参考に研究プロジェクトメンバが仮訳を作成)

2. ISO/IEC 27002:2022の管理策

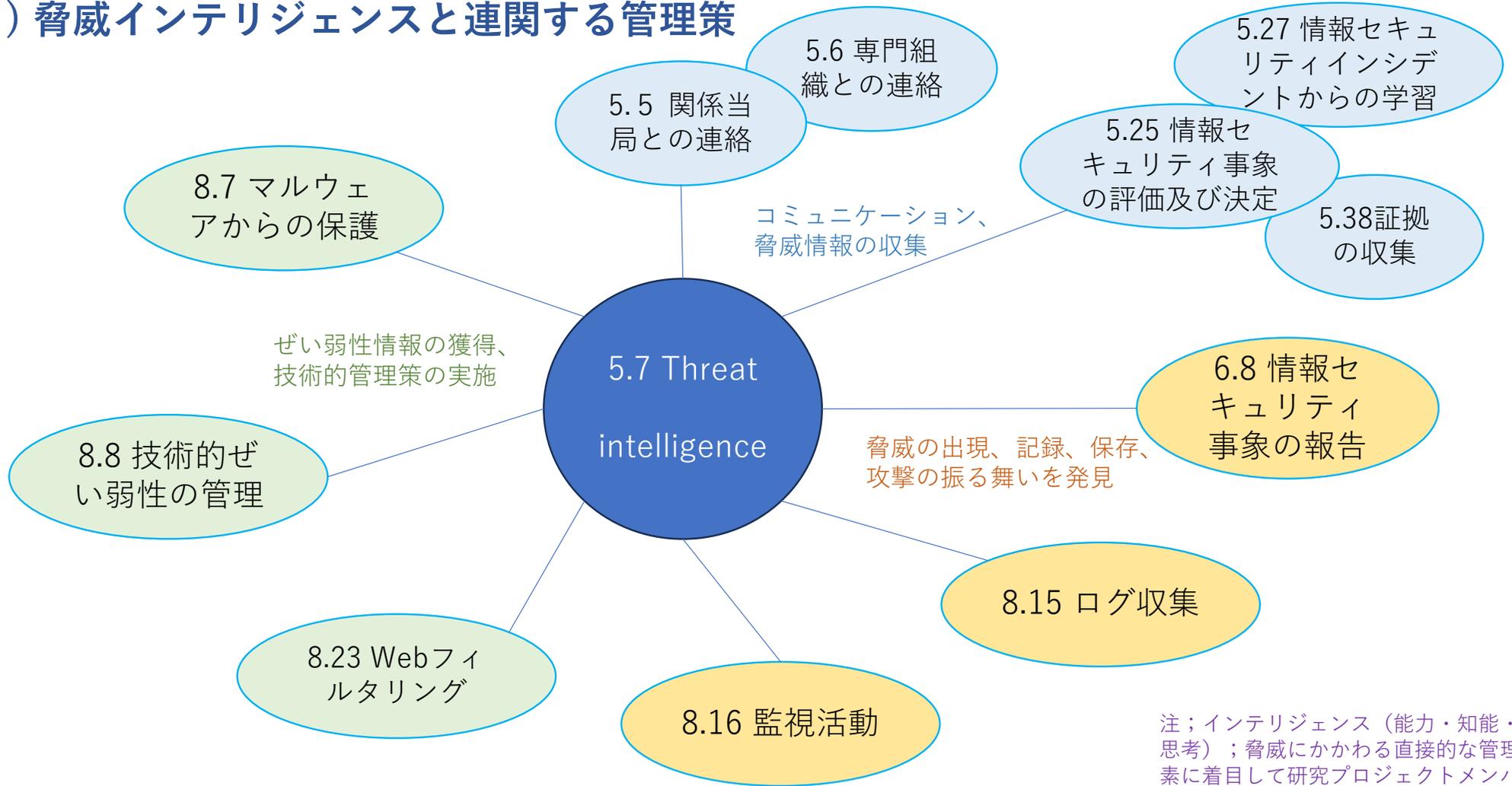
→前頁から続く

- 脅威インテリジェンス活動
 - a) 脅威インテリジェンス生成の目標を確立する
 - b) 脅威インテリジェンスの作成に必要な情報を提供するために必要かつ適切な内部および外部の情報ソースを特定、精査、選択する
 - c) 内部および外部の選択されたソースから情報を収集する
 - d) 収集した情報を処理して分析に備える（情報の翻訳、フォーマット、裏付けなど）
 - e) 情報を分析して、それが組織にとってどのように関係し、意味があるのかを理解する
 - f) 理解できる形式で関係者に伝達および共有する
- 脅威インテリジェンスを分析、活用
 - a) 脅威インテリジェンス ソースから収集した情報を組織の情報セキュリティ リスク管理プロセスに組み込むプロセスを実装することによって
 - b) ファイアウォール、侵入検知システム、マルウェア対策ソリューションなどの技術的な予防および検出制御への追加入力として
 - c) 情報セキュリティテストプロセスおよび技術への入力として
- 他の組織と相互ベースで脅威インテリジェンスを共有（組織は、全体的な脅威インテリジェンスを向上させるために）
- 組織は脅威インテリジェンスを使用して、脅威を防止、検出、または脅威に対応できる
組織は脅威インテリジェンスを生成でき、より一般的には、他のソースによって生成された脅威インテリジェンスを受信して利用する
- 脅威インテリジェンスは、多くの場合、独立したプロバイダーやアドバイザー、政府機関、または共同の脅威インテリジェンスグループによって提供される
- 5.25、8.7、8.16、8.23 などの制御の有効性は、利用可能な脅威インテリジェンスの品質によって異なる

[Source] ISO, ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls, ISO, 2022, pp.15-16 5.7 Threat intelligenceを参考に研究プロジェクトメンバが仮訳を作成)

2. ISO/IEC 27002:2022の管理策

(4) 脅威インテリジェンスと連関する管理策



注；インテリジェンス（能力・知能・思考）；脅威にかかわる直接的な管理策の要素に着目して研究プロジェクトメンバが作成

3. 脅威インテリジェンス

(1) ISO/IEC 27002-2022 – 5.7項 – (脅威インテリジェンス Threat intelligence)

- この管理策は、組織に対し、脅威に関する情報を収集・分析し、脅威インテリジェンスを構築するよう求めている。
- 脅威に関する情報例：特定のサイバー攻撃に関するデータや、攻撃者が用いる手法、攻撃タイプなど
- 脅威を適切に緩和する情報セキュリティリスク対応の組織的管理策としなければならない。

3. 脅威インテリジェンス

(2) NIST の定義及びセキュリティ要件

a. NIST 関連用語と定義

用語	NIST定義
脅威 (threat) [SP 800-30]	情報の認可されていないアクセス、破壊、開示、変更、および／またはサービス妨害により、システムを通じて、組織の運営、組織の資産、個人、他の組織、または国家に有害なインパクトを与える可能性のある状況または事象。
脅威情報 (threat information) [SP 800-150]	組織が脅威から組織自身を防御する、または行為者の行為を検知するのに役立つ可能性のある、脅威に関連するあらゆる情報。脅威情報の主なタイプには、兆候、TTP、セキュリティアラート、脅威インテリジェンスレポート、およびツール構成が含まれる。
脅威インテリジェンス (threat intelligence) [SP 800-150]	意思決定プロセスに必要なコンテキストを提供するために集約、変換、分析、解釈、または補強された脅威情報。

[Source] (以下の資料を参考に研究プロジェクトメンバが仮訳を作成)

1) NIST, SP800-30 Rev.1 Guide for Conducting Risk Assessments, NIST, 2012, <https://doi.org/10.6028/NIST.SP.800-30r1>, p B-13

2) NIST, SP 800-150 Guide to Cyber Threat Information Sharing, NIST, 2016, <https://doi.org/10.6028/NIST.SP.800-150>, .p.31

- ・ [SP 800-150]は、脅威情報と脅威インテリジェンスを区別している。
- ・ 脅威情報とは、組織が脅威から組織自身を防御する、または脅威行為者の行為を検知するのに役立つ可能性のある、脅威に関連するあらゆる情報である。
- ・ 脅威インテリジェンスとは、リスクベースの意思決定プロセスに必要なコンテキストを提供するために集約、変換、分析、解釈、または補強された脅威情報である。

[Source] NIST, SP 800-172 Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171(IPA訳), IPA, 2021, <https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000093059.pdf>, p.10 脚注

3. 脅威インテリジェンス

(2) NIST の定義及びセキュリティ要件

b. NIST セキュリティ要件 – NIST SP800-172

識別子； 3.11.5 e

分類； リスクアセスメント

【要件】 現在のおよび蓄積された**脅威インテリジェンス**に基づいて、組織のシステムおよび組織に対して予想されるリスクに対処するために、セキュリティソリューションの有効性を [設定：組織が定める頻度 = 組織が定めるパラメータ] でアセスメントする。

【詳細】 組織の脅威に関する認識とリスクアセスメントは、動的で継続的であり、システムの運用、システムのセキュリティ要件、およびそれらの要件を満たすために採用されたセキュリティソリューションに情報提供する。

脅威インテリジェンス（すなわち、意思決定に必要なコンテキストを提供するために集約、変換、分析、解釈、または補強された脅威情報）は、動的な脅威環境に対処するため必要な変更を特定するために、組織のリスクアセスメント 処理と情報セキュリティ運用に注入される。

- **NIST SP 800-172**； NIST SP 800-171 基本および派生セキュリティ要件に加えて実装されるセキュリティ要件。追加のセキュリティ要件として、(1)侵入耐性アーキテクチャ、(2)被害局限化運用、(3)サイバーレジリエンス生存可能性の3つのコンポーネントを提供する。
3.11.5 e は、(2)被害局限化運用に分類されている。

【参考】脅威インテリジェンスの定義の例・捉え方

a. What is threat intelligence?

[What is Threat Intelligence? | IBM](#)

Threat intelligence—also called "cyberthreat intelligence" (CTI) or "threat intel"—is detailed, actionable threat information for preventing and fighting cybersecurity threats targeting an organization.

[Source] IBM , What is threat intelligence?, IBM, <https://www.ibm.com/topics/threat-intelligence#:~:text=Threat%20intelligence%20is%20detailed%2C%20actionable%20threat%20information,for%20preventing%20and%20fighting%20cyberthreats%20targeting%20an%20organization.> (access 2024/5/24)

b. Definition: Threat Intelligence

[Definition: Threat Intelligence \(gartner.com\)](#)

Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.

[Source] Gartner , Definition: Threat Intelligence, Gartner, <https://www.gartner.com/en/documents/2487216> (access 2024/5/24)

【参考】脅威インテリジェンスの定義の例・捉え方

c. Microsoft

- ・サイバー脅威インテリジェンスが定義されました
- ・デジタルトランスフォーメーションは大規模なデータ資産を生み出し、サイバー犯罪者に新たな攻撃の道を開きます。
- ・悪質なアクターの手口は巧妙で、進化を続けているため、企業が新たな脅威の先に行くことは困難です。サイバー脅威インテリジェンスでは、会社が継続的に防御を強化するために必要な情報と機能が提供されます。
- ・サイバー脅威インテリジェンスは、サイバー攻撃からの組織の保護を強化するのに役立つ情報です。これには、セキュリティチームが攻撃に対する準備、検出、対応方法に関する十分な情報に基づいて意思決定を行えるよう、脅威の状況を包括的に把握できるデータと分析が含まれています。アクターの行動、ツールやテクニック、悪用、ターゲットとする脆弱性、新たな脅威に焦点を当てた情報を得ることで、組織のセキュリティ対策に優先順位付けするのに役立ちます。

[Source]

<https://www.microsoft.com/ja-jp/security/business/security-101/what-is-cyber-threat-intelligence> (access 2024/5/24)

3. 脅威インテリジェンス

(3) 脅威インテリジェンスに対応する組織担当と役割

組織担当	役割
システム管理者	保護機能および検知機能を最適化し、防御を強化する ・セキュリティ製品と統合する ・不正なIP、URL、ドメイン、ファイルなどをブロックする
運用管理者	組織を標的とする脅威アクターを発見し追跡する ・侵入の証拠をより広範に、詳しく調査する ・脅威アクターに関するレポートを確認して、より適切に検知する
経営者層	組織が直面するリスクと、その影響に対処するための方法を理解する ・組織の全体的な脅威レベルを評価する ・セキュリティロードマップを策定する
SOC	組織に対するリスクと影響に基づいてインシデントに優先順位を付ける ・アラートを強化する ・アラートをインシデントにリンクする ・新たに展開されたセキュリティコントロールを調整する
CSIRT	インシデントの調査、管理、優先順位付けを促進させる ・誰が/何を/なぜ/いつ/どのようにインシデントを発生させたか、その詳細を調べる ・根本原因を分析してインシデントの範囲を特定する

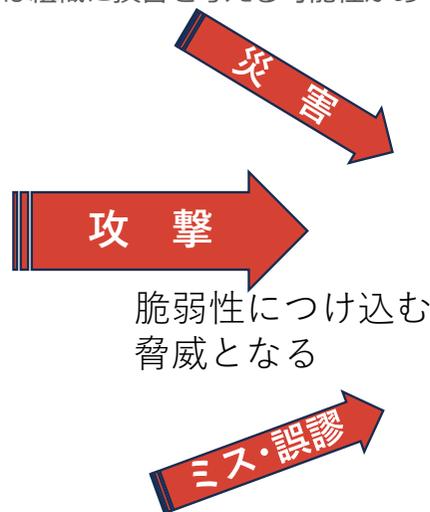
[Source] CROWDSTRIKE,サイバー脅威インテリジェンスとは?, <https://www.crowdstrike.jp/cybersecurity-101/threat-intelligence/> (access 2024/5/24) を参考にプロジェクトメンバーが作成

4. 脅威と脆弱性

(1) 脅威と脆弱性

脅威 Threat

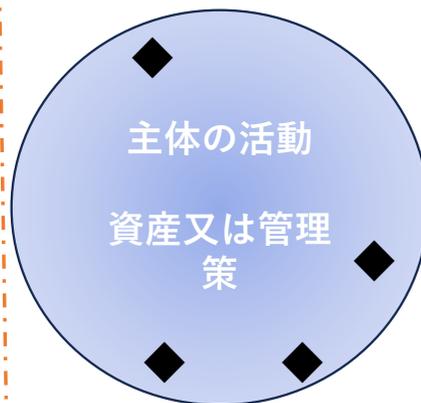
= 情報セキュリティインシデントの潜在的な原因、システムまたは組織に損害を与える可能性がある因子



- ・ 外的要因；外部に位置する
- ・ 想定し難い
- ・ 多々あり過ぎる

脆弱性 Vulnerability

= 一つ以上の脅威によってつけ込まれる可能性がある、資産又は管理策の弱点



点在する脆弱性◆
脅威に脅かされる

インシデント
脅威/脆弱性 ⇒ ハザードの表出

- ・ 内的要因；内部に潜み、自分のこととしてとらえやすい
- ・ 想定し易い
- ・ 結果、事象として理解可能

👉 情報セキュリティにおけるインテリジェンスの獲得を、脅威か脆弱性かのどちらにスポットを当てて検討するかは、まさに管理策対応の役割分担・責任に委ねられる。その前提にインテリジェンス獲得を図るアプローチの議論が必要。

4. 脅威と脆弱性

(2) 脆弱性情報

脅威に対処するために；脆弱性を知る（有り無しを）⇒脆弱性を理解する（内容、対象を特定）

No.	名称	運営*	内容	備考
1	脆弱性対策情報ポータルサイト JVN (Japan Vulnerability Notes)	IPA・JPCERT/CC(JVN)	・ソフトウェアなどの脆弱性関連情報とその対策情報を提供	
2	共通脆弱性評価システム CVSS (Common Vulnerability Scoring System)	FIRST IPA	・脆弱性の深刻度を評価するための指標	
3	共通脆弱性識別子 CVE(Common Vulnerabilities and Exposures)	JVN	・一つ一つの脆弱性を識別するための共通の識別子 ・『プログラム上のセキュリティ問題』を一意に識別するため、識別番号を付与	CVE-ID、JVN-ID、JVN iPediaの3つを括りつける
4	共通脆弱性タイプ一覧 CWE (Common Weakness Enumeration)	MITRE	・脆弱性の種類を識別するための共通の脆弱性タイプの一覧	

* 「運営」に記載の組織はシート18に補足

4. 脅威と脆弱性

JPCERT/CC ; Japan Computer Emergency Response Team Coordination Center

- 日本国内に関する①インシデント等の報告の受け付け、②対応の支援、③発生状況の把握、④手口の分析、⑤再発防止のための対策の検討や助言などを、⑥技術的な立場から行なっている
- 特定の政府機関や企業からは独立した中立の組織として、日本における情報セキュリティ対策活動の向上に積極的に取り組んでいる
- 日本の窓口

JVN ; iPediaが使用する脆弱性タイプ

- JVN (Japan Vulnerability Notes) 使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供、情報セキュリティ対策に資することを目的とする脆弱性対策情報ポータルサイト
- 脆弱性関連情報の受付と安全な流通を目的とした「情報セキュリティ早期警戒パートナーシップ」に基いて、2004年7月よりJPCERT コーディネーションセンターと独立行政法人情報処理推進機構 (IPA)が共同で運営している
- JVN では、「情報セキュリティ早期警戒パートナーシップ」制度に基づいて報告され調整した脆弱性情報や、CERT/CC など海外の調整機関と連携した脆弱性情報を公表しています。掲載内容は、脆弱性が確認された製品とバージョン、脆弱性の詳細や分析結果、製品開発者によって提供された対策や関連情報へのリンクなどで、対策にはパッチだけではなく回避策（ワークアラウンド）が掲載される事もある

MITRE ; 米国の非営利組織

- 米国国立標準技術研究所 (NIST) の連邦研究開発センター (Federally funded research and development center : FFRDC) の運営を行う
- 国土安全保障省(DHS)の配下で、CVE (Common Vulnerabilities and Exposures 共通脆弱性識別子) の運用を行う

FIRST ; 政府機関、商業組織、教育機関のさまざまなコンピュータセキュリティインシデント対応チームを結集

- インシデント防止における協力と調整を促進、インシデント対応、メンバーとコミュニティ全体の情報共有を促進することが目的
- CVSSの管理母体

【ご注意】この資料は定例研究会の説明のためだけに作成したもので、他の用途への利用は想定しておりません。ご参加者ご本人限りにてお願いいたします。また翻訳内容には誤りがある可能性がありますので、正確な内容は原文をご参照ください。

【参考】JVN iPedia 脆弱性タイプの一覧

CWE-200 情報の漏えいとは、情報の漏えいの原因と影響、情報の漏えいの防止方法を示す

#	CWE識別子	脆弱性タイプ
1	CWE-16	環境設定
2	CWE-20	不適切な入力確認
3	CWE-22	パス・トラバーサル
4	CWE-59	リンク解釈の問題
5	CWE-78	OSコマンド・インジェクション
6	CWE-79	クロスサイト・スクリプティング(XSS)
7	CWE-89	SQLインジェクション
8	CWE-94	コード・インジェクション
9	CWE-119	バッファエラー (バッファオーバーフロー)
10	CWE-134	書式文字列(フォーマット文字列)の問題
11	CWE-189	数値処理の問題(整数オーバーフロー)

#	CWE識別子	脆弱性タイプ
12	CWE-200	情報漏えい
13	CWE-255	証明書・パスワード管理
14	CWE-264	認可・権限・アクセス制御
15	CWE-287	不適切な認証
16	CWE-310	暗号の問題
17	CWE-352	クロスサイト・リクエスト・フォージェリ(CSRF)
18	CWE-362	競合状態
19	CWE-399	リソース管理の問題
20	CWE-Other	その他 (#1~#19)以外のCWE分類
21	CWE-nocwe	CWE以外(CWEで分類できない脆弱性)
22	CWE-noinfo	情報不足
23	CWE-DesignError	システム設計上の問題

CWE; ソフトウェアの脆弱性を分類し (タイプ)、階層構造で詳細化している

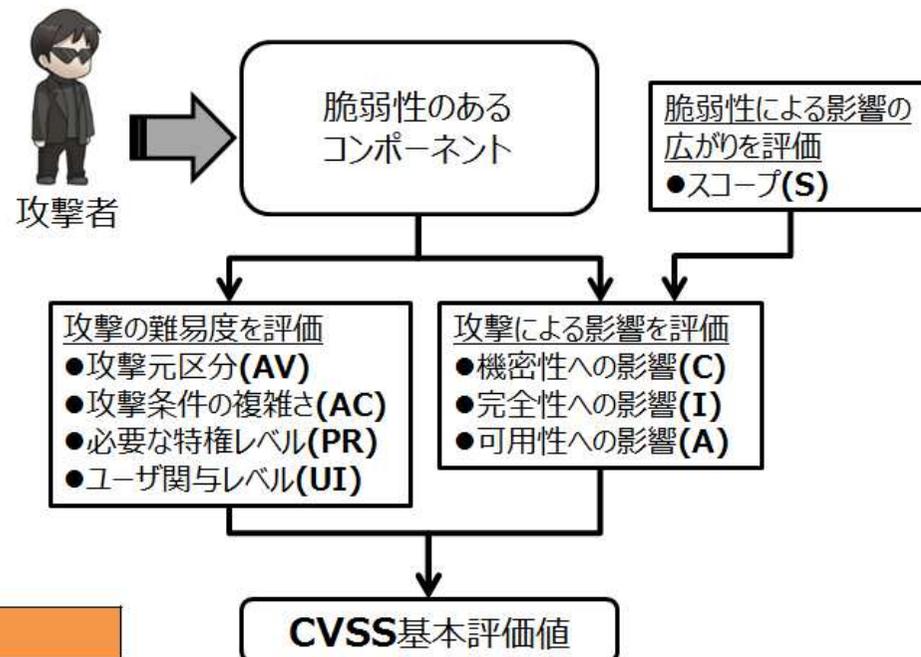
脆弱性タイプ; ビューView, カテゴリーCategory, 脆弱性Weakness, 複合要因Compound Element に分類
現在、View 22個、Category 105個、Weakness 638個、Compound Element 12個、合計777個

[Source] IPA, 共通脆弱性タイプ一覧CWE概説, <https://www.ipa.go.jp/security/vuln/CWE.html> (access 2024/5/24)を参考にプロジェクトメンバーが作成

【参考】CVSS 共通脆弱性評価システム

CVSS概要 Common Vulnerability Scoring System

- 脆弱性の深さを、同一の基準の下で定量的に比較できるようになる
- CIAに対する影響を、脆弱性の特性、ネットワークから攻撃可能かどうか、攻撃コードの出現有無と対策情報の利用可否、ユーザが脆弱性への対応を決めるために評価する基準
- FIRSTがCVSSの管理母体



CVSS v2		CVSS v3	
攻撃の難易度	どこから攻撃可能であるか 攻撃元区分 (AV: Access Vector)	どこから攻撃可能であるか 攻撃元区分 (AV: Attack Vector)	
	攻撃する際に必要な条件の複雑さ 攻撃条件の複雑さ (AC: Access Complexity)	攻撃する際に必要な条件の複雑さ 攻撃条件の複雑さ (AC: Attack Complexity)	
	攻撃するために認証が必要であるか 攻撃前認証要否 (Au: Authentication)	攻撃する際に必要な特権レベル 必要な特権レベル (PR: Privileges Required)	
		攻撃する際に必要なユーザ関与レベル ユーザ関与レベル (UI: User Interaction)	

[Source] IPA, 共通脆弱性評価システムCVSS v3概説, <https://www.ipa.go.jp/security/vuln/scap/cvssv3.html> (access 2024/5/24)

5. ATT&CK®の活用例

(1) MITRE ATT&CK®（マイターアタック）とは

- 実攻撃の観察に基づいて、攻撃（敵対）者の方法（戦術）と技術を理解し、対策モデルを構築するための知識ベースを提供する。
- セキュリティ技術者などの専門家が攻撃手法を理解し、適切な対策を講じるために情報を提供する。

⇒ MITRE社が、コミュニティを結集し、ナレッジベースATT&CK®を提供する。

ATT&CK®は、実世界の観察に基づく攻撃者の戦術と手法に関するグローバルにアクセス可能なナレッジベースであり、民間部門、政府、サイバーセキュリティ製品およびサービスコミュニティにおいて、特定の脅威モデルと方法論を開発するための基盤として提供し、使用できる。

⇒ATT&CK®は、サイバー攻撃者の行動と、ライフサイクル全体にわたる攻撃の分類に関する知識ベースを提供する。

⇒半年ごとに更新（注； Resourceのバージョン履歴に「更新プログラム ページに表示される半年ごとのコンテンツ リリース」とする。）

<https://attack.mitre.org/resources/versions/> 参照

5. ATT&CK®の活用例

(2) MITRE ATT&CK®活用のNavigate

a. 活用の目的に向けて

MITRE ATT&CKのフレームワークは、攻撃者の視点からサイバー攻撃が記述されたツールであることから、脅威を分析し、セキュリティ防御の強化策につなげる活用を可能とするため、フレームの構成内容を理解する。

b. 脅威インテリジェンスの獲得

実測されたサイバー攻撃を攻撃者の活動フェーズ（Tactics 戦術）ごとに攻撃手法（Techniques）を分類したフレームワーク、マトリックスより、脅威となる技術的要素、攻撃のプロセスと手法から理解すべき事項を抽出できるようにする。

攻撃の視点（攻撃グループ、攻撃ソフト、攻撃シナリオなど）から脅威を把握し、防御策の達成を検証可能にする。

c. アプローチ

ATT&CKロードマップによってサイバー攻撃に備えた防御策を確実なものとするため、攻撃そのものの進化、未知の攻撃を予測して継続的な取り組みが行え、他の脅威インテリジェンス獲得及び方法に目を向けるスキルも必要といえる。

注記； Sheet 23～37の [Source]

<https://attack.mitre.org/> MITRE ATT&CK (MITRE ATT&CK®) のサイト及びそのリンク先を参照してプロジェクトメンバーが作成
(access 2023/1/23、2024/5/24)

5. ATT&CK®の活用例

(3) 脅威インテリジェンスをATT&CK®にマッピングするロードマップ

今日インテリジェンスを獲得する目的のアプローチとしては、手順 STEP00~05のロードマップを示す。



ロードマップとして、Best PRACTICEとWorst PRACTICEを示し、使用にあたっての犯しやすい過ちを回避するよう注意を促している。

【ご注意】この資料は定例研究会の説明のためだけに作成したもので、他の用途への利用は想定しておりません。ご参加者ご本人限りにてお願いいたします。また翻訳内容には誤りがある可能性がありますので、正確な内容は原文をご参照ください。

5. ATT&CK®の活用例

(4) ATT&CK®のサイト構成

[Source] Sheet24-28 ; <https://attack.mitre.org/> からのリンク

MITRE | ATT&CK®

Thank you to SOC Prime for becoming ATT&CK's first Benefactor.

Matrices | Tactics | Techniques | Defenses | CTI | Resources | Benefactors | Blog

Search

① ホームポジション
• <https://attack.mitre.org/>

② 開発・維持の協力要請

③ 利用ガイダンス

④ フレームワークの構成内容

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve cybersecurity problems for a safer world – by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

⑤ Tacticstと Techniquesのマトリックス

ATT&CK Matrix for Enterprise

layout: flat | show sub-techniques | hide sub-techniques

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create Account (2)		Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Data from Cloud Storage	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Physical	Endpoint Denial of Service (4)
Search Open Technical	Stage	Supply Chain				Direct Volume Access		Container and Resource Discovery	Data from	Data from		Financial Theft	Firmware
						Domain Policy Modification (2)							

5. ATT&CK®の活用例

(5) ATT&CK®開発・維持に協力を要請

②

Home > Resources > Engage with ATT&CK > Contribute

Contribute

ATT&CK is in a constant state of development. We are always on the lookout for new information to help refine and extend what is covered. If you have additional techniques, know about variations on one already covered, have examples of techniques in use, or have other relevant information, then we would like to hear from you.

We are looking for contributions in the following areas, but all contributions and feedback to ATT&CK are appreciated. If you think you may have something you think may be useful, please reach us at attack@mitre.org.

Due to the high volume of contributions, we cannot accept every contribution. We recommend you submit your contributions on a regular basis (e.g., monthly) so that we get the right details for our approach to maintaining ATT&CK.

[Submit a contribution](#)

What we're looking for

Sub-Techniques and Techniques	Threat Intelligence	Website Content Errors
Let us know what new variations of behaviors real adversaries are using in the wild! Please share a brief description of the behavior, any references or knowledge about how it works and was used, and how this behavior is not already captured in ATT&CK.	We map Group and Software examples on our site, and appreciate your help with referenced information about how Groups and Software samples use ATT&CK techniques. Please share the sub-technique or technique name, group or associated group name, a brief description of how the technique is implemented, and the publicly-available reference.	If you find errors or typos on the site related to content, please let us know by submitting the url where you found the error and a short description. Examples include typos and syntax errors, improperly formatted web pages, and 404 errors when links are clicked.
See an example	See an example	See an example

MITRE社は、ATT&CKの開発を続け、協力者には利用方法の紹介を呼びかけている。（コンテンツの更新は6か月ごと）

攻撃者の行動、使用する技術情報の収集と共有

CTI情報提供の協力を呼びかけ

5. ATT&CK® の活用例

(6) ATT&CK®利用ガイダンス

③

ATT&CKでは攻撃者の行動を体系的に分類し、知識ベースとして習得できるフレームワークを提供する。

“MITRE ATT&CK”とは
攻撃者の視点からサイバー攻撃を記述するフレームワーク、脅威を分析し、セキュリティ防御を強化するため。

“ATT&CK”は攻撃者の行動を体系的に分類するモデル；モデルの構成要素は、Tactics(戦術=攻撃者が行動する理由)、Techniques(目標達成の技術)、Sub-techniques、Procedures(攻撃技術の実装、使用)

Key Concepts

ATT&CK is a model that attempts to systematically categorize adversary behavior. The main components of the model are:

- **Tactics**, represents “why” or the reason an adversary is performing an action
- **Techniques**, represents “how” adversaries achieve tactical goals by performing an action
- **Sub-techniques**, a more specific or lower-level description of adversarial behavior
- **Procedures**, specific implementation or in-the-wild use the adversary uses for techniques or sub-techniques

ATT&CK is organized in a series of technology domains, the ecosystem an adversary operates within. Currently, there are three **technology** domains:

- **Enterprise**, representing traditional enterprise networks and cloud technologies
- **Mobile** for mobile communication devices
- **ICS** for industrial control systems

Within each domain are **platforms**, which may be an operating system or application (e.g. Microsoft Windows). Techniques and sub-techniques can apply to multiple platforms.

For more information on the principles behind ATT&CK, its creation, and its ongoing maintenance, read the ATT&CK Philosophy Paper. For additional information focused on ATT&CK for ICS, including the unique elements and commonalities with ATT&CK, read the ATT&CK for ICS Extension.

- [MITRE ATT&CK Roadmap](#)
Last updated October 2022
- [MITRE ATT&CK Matrix Poster](#)
Last updated April 2023

⑥ [ロードマップを示す](#)

How can I use ATT&CK?

The following four use cases are the most common way that users report applying ATT&CK to their work.

- [Detections and Analytics](#)
- [Threat Intelligence](#)

What is ATT&CK?

ATT&CK is knowledge base of adversarial techniques based on real-world observations. ATT&CK focuses on how adversaries interact with systems during an operation, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target.

Read the ATT&CK 101 Blog post for more information on the basics of ATT&CK and check the short video below.



5. ATT&CK®の活用例

(7) ATT&CK®のフレームワークの構成内容

④
Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Resources ▾ Benefactors
Blog [↗](#)

Search

MATRICES

Enterprise ^

- PRE
- Windows
- macOS
- Linux
- Cloud ^
 - Office 365
 - Azure AD
 - Google Workspace
 - SaaS
 - IaaS
 - Network
 - Containers
- Mobile ^
 - Android
 - iOS
 - ICS

Matrices	Tactics	Techniques	Defenses	CTI	Resources	Benef
Enterprise	Enterprise	Enterprise	Data Source	Groups	Get Started	
Mobile	Mobile	Mobile	Mitigations	Software	Learn More about ATT&CK	
ICS	ICS	ICS	Assets	Campaigns	ATT&CK Data & Tools	
					FAQ	
					Engage with ATT&CK	
					Version History	
					Legal & Branding	

ID	Name
TA0043	Reconnaissance
TA0042	Resource Development
TA0001	Initial Access
TA0002	Execution
TA0003	Persistence
TA0004	Privilege Escalation
TA0005	Defense Evasion
TA0006	Credential Access
TA0007	Discovery
TA0008	Lateral Movement
TA0009	Collection
TA0011	Command and Control
TA0010	Exfiltration
TA0040	Impact

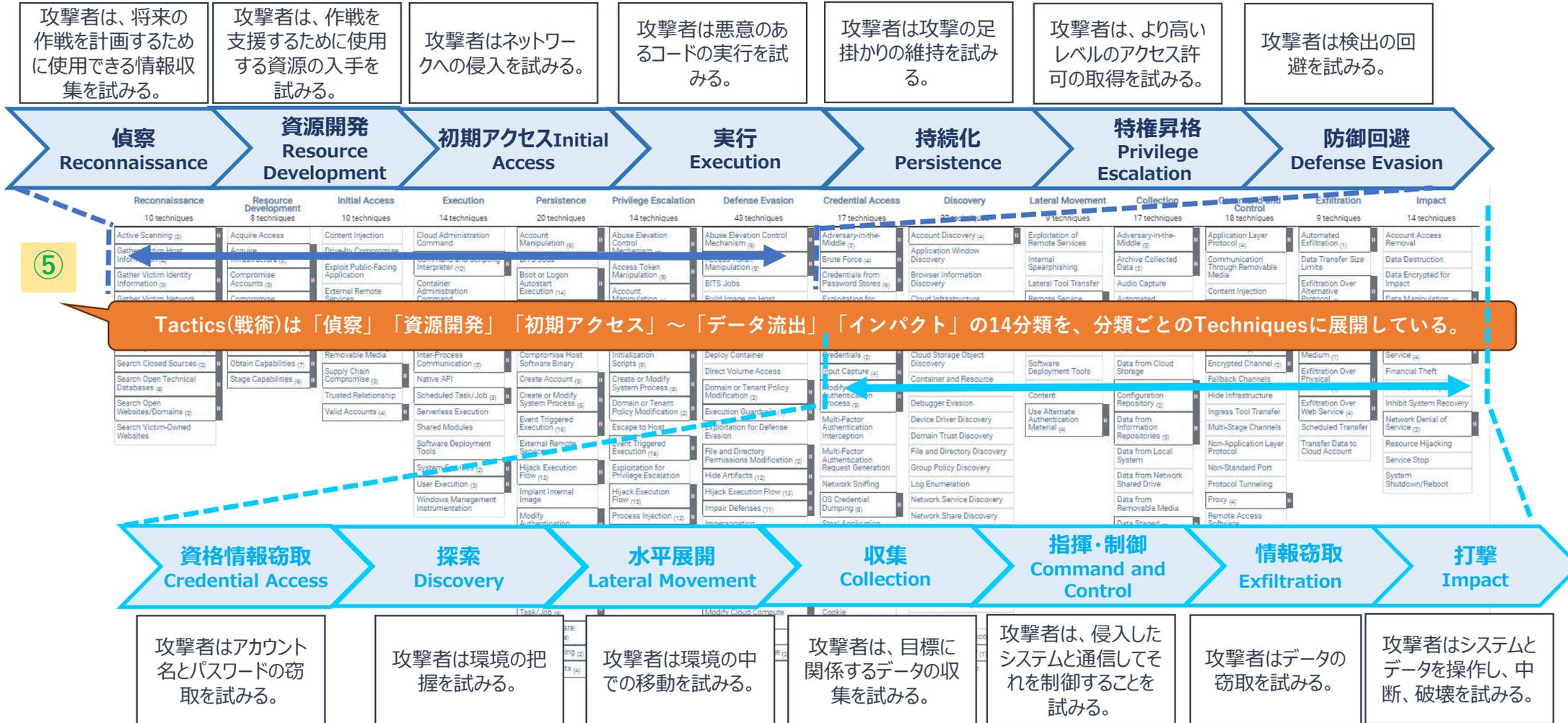
Tactics ; 14の戦術を表記 (Ver 9_Enterprise)

Matrices, Tactics, Techniques
 これら3つの領域は、すべて、企業向け、モバイル用、産業用制御システム (ICS)の別に展開している。

【ご注意】この資料は定例研究会の説明のためだけに作成したもので、他の用途への利用は想定しておりません。ご参加者ご本人限りにてお願いいたします。また翻訳内容には誤りがある可能性がありますので、正確な内容は原文をご参照ください。

5. ATT&CK®の活用例

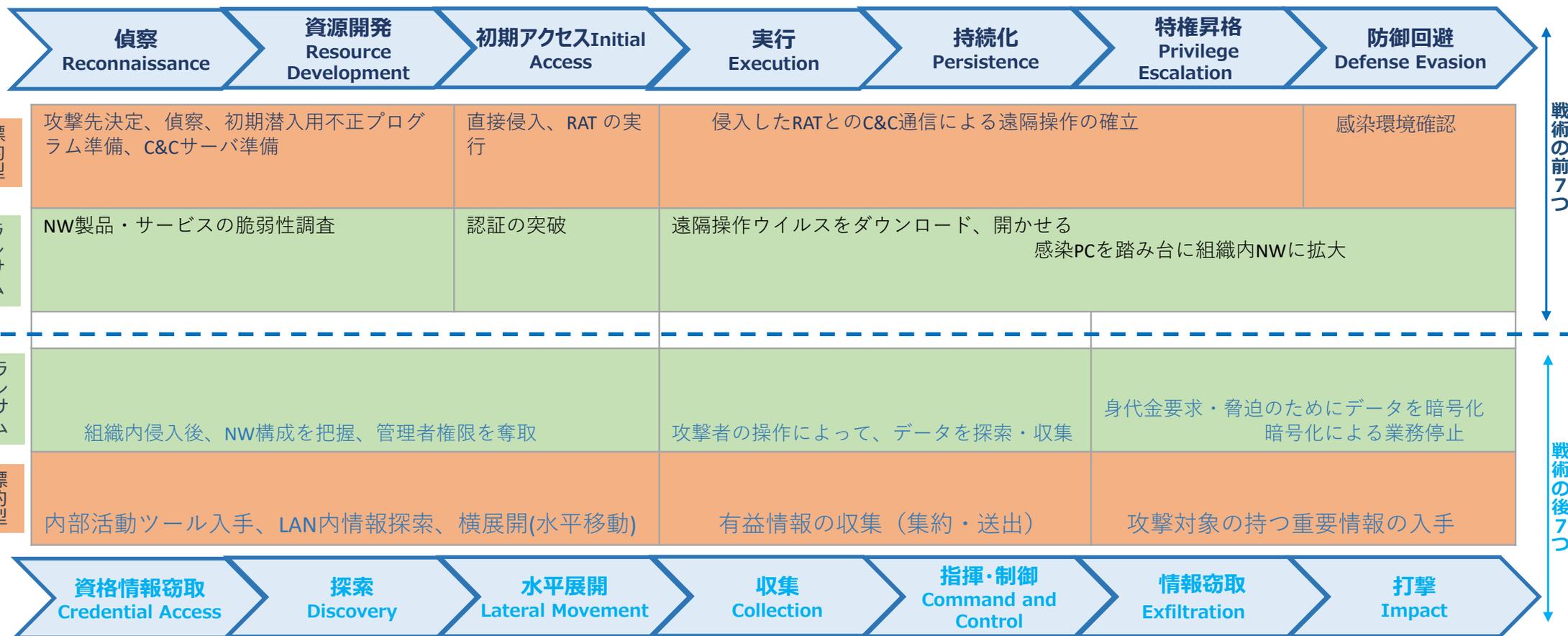
(8) Tactics (攻撃者の戦術) と攻撃手法 – Matrix



6. サイバー攻撃の実態とATT&CK®フレームワーク

(1) サイバー攻撃の実態 標的型攻撃 と ランサムウェア

・ 攻撃者は何をするのか？（MITRE ATT&CK Tacticstとの対応）

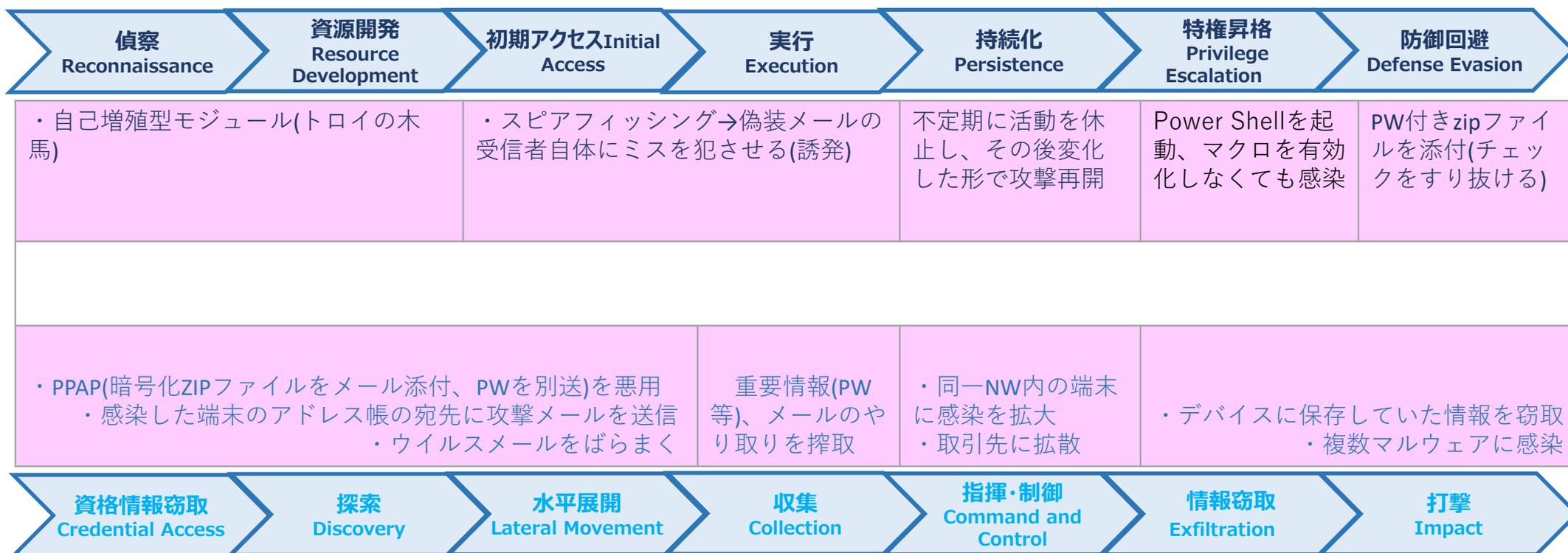


[Source] MITRE , MITRE ATT&CK, MITRE, <https://attack.mitre.org/>, (access 2023/1/23)

6. サイバー攻撃の実態とATT&CK®フレームワーク

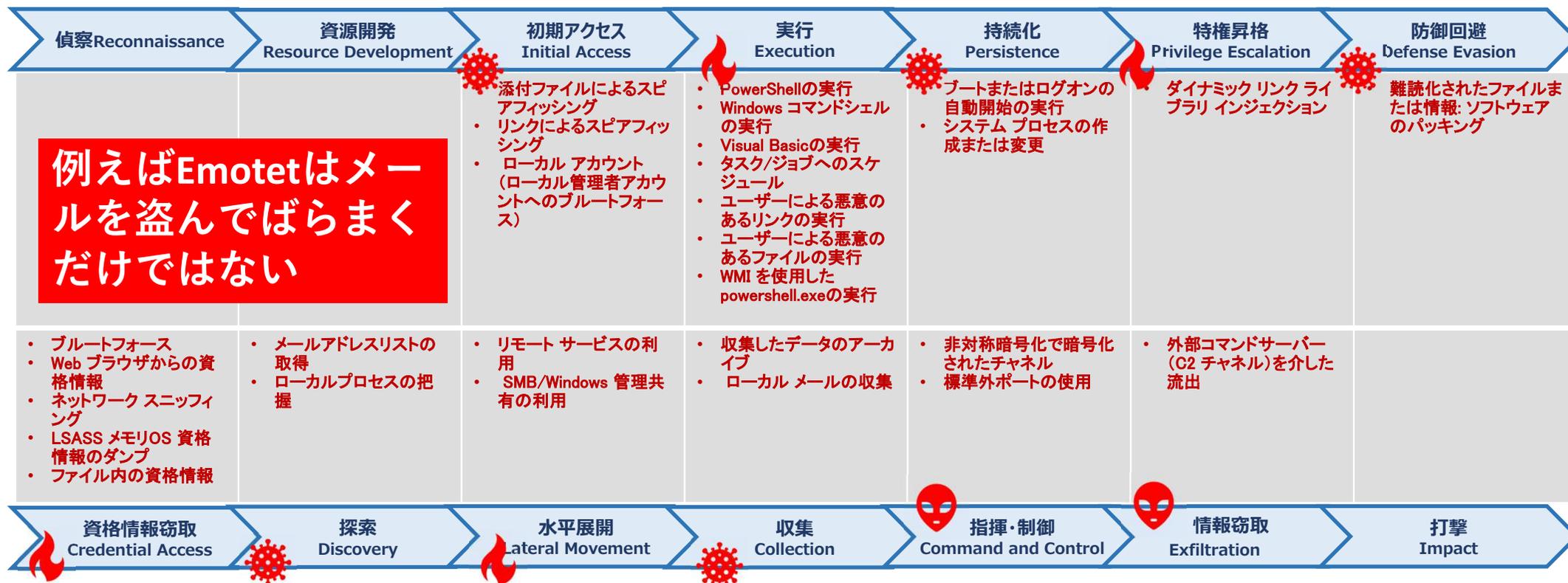
(2) サイバー攻撃の実態 **EMOTET**

・ 攻撃者は何をするのか？ (MITRE ATT&CKフレーム Tacticsとの対応)



6. サイバー攻撃の実態とATT&CK®フレームワーク

(3) EMOTETの攻撃実態



[Source] MITRE , MITRE ATT&CK, MITRE, <https://attack.mitre.org/>, (access 2023/1/23)

6. サイバー攻撃の実態とATT&CK®フレームワーク

(4) 攻撃者“Wizard Spider”が用いるソフトウェア

攻撃者は侵入後にEmotetだけでなく、いろいろな道具を使う



Wizard Spiderの使用するソフトウェア

AdFind	Active Directory から情報を収集するために使用できる無料のコマンドライン クエリ ツール	GrimAgent	Ryuk ランサムウェアが展開される前に使用されるバックドア
Bazar	ダウンローダーおよびバックドア	Mimikatz	Windows アカウント ログインパスワードを取得
BloodHound	Active Directory (AD) 偵察ツール	Net	Windows オペレーティング システムのユーティリティコンポーネント
Cobalt Strike	汎用標的型攻撃ツール	Nltest	ドメイン コントローラを一覧表示するWindowsコマンドユーティリティ
Conti	Ransomware-as-a-Service (RaaS) . Conti を使用する攻撃者は、侵害されたネットワークから情報を盗み、データの身代金を要求する	Ping	ネットワーク接続のトラブルシューティングと検証に一般的に使用されるオペレーティング システム ユーティリティ
Dyre	金銭目的で使用されるバンキング型トロイの木馬	PsExec	別のコンピュータでプログラムを実行する無料のMicrosoft ツール
Emotet	モジュール式のマルウェアで、主に TrickBot や IcedID などの他のマルウェアのダウンローダとして使用される	Ryuk	事業体攻撃用に設計されたランサムウェア
Empire	オープンソースのクロスプラットフォームのリモート管理およびエクスプロイト後のフレームワーク. 公開ハッキング ツール	TrickBot	トロイの木馬型スパイウェア プログラム



[Source] MITRE , MITRE ATT&CK, MITRE, <https://attack.mitre.org/>, (access 2023/1/23)

【ご注意】この資料は定例研究会の説明のためだけに作成したもので、他の用途への利用は想定しておりません。ご参加者ご本人限りにてお願いいたします。また翻訳内容には誤りがある可能性がありますので、正確な内容は原文をご参照ください。

6. サイバー攻撃の実態とATT&CK®フレームワーク

(5) EMOTET攻撃者の行動とATT&CKフレームワーク (本Sheet30~32をMAITRE社ナビゲータと検証)

Tactics	RECONNAISSANCE 10 techniques	RESOURCE DEVELOPMENT 7 techniques	INITIAL ACCESS 9 techniques	EXECUTION 13 techniques	PERSISTENCE 19 techniques	PRIVILEGE ESCALATION 13 techniques	DEFENSE EVASION 42 techniques	CREDENTIAL ACCESS 17 techniques	DISCOVERY 30 techniques	LATERAL MOVEMENT 9 techniques	COLLECTION 17 techniques	COMMAND AND CONTROL 16 techniques	EXFILTRATION 9 techniques	IMPACT 13 techniques
Techniques	Active Scanning	Acquire Infrastructure	Valid Accounts	Scheduled Task/Job	Valid Accounts	Hijack Execution Flow	Modify Authentication Process	Network Sniffing	System Service Discovery	Remote Services	Data from Local System	Data Obfuscation	Exfiltration Over Other Network Medium	Data Destruction
	Gather Victim Host Information	Compromise Accounts	Replication Through Removable Media	Windows Management Instrumentation	Account Manipulation	OS Credential Dumping	Input Capture	Application Window Discovery	Software Deployment Tools	Data from Removable Media	Fallback Channels	Scheduled Transfer	Inhibit System Recovery	Data Encrypted for Impact
	Gather Victim Identity Information	Compromise Infrastructure	Trusted Relationship	Software Deployment Tools	Event Triggered Execution	Brute Force	System Network Configuration Discovery	Internal Spearphishing	Replication Through Removable Media	Input Capture	Proxy	Data Transfer Size Limits	Service Stop	Defacement
	Gather Victim Network Information	Develop Capabilities	Supply Chain Compromise	Shared Modules	Event Triggered Execution	Rootkit	System Owner/User Discovery	Use Alternate Authentication Material	Internal Spearphishing	Screen Capture	Communication Through Removable Media	Exfiltration Over C2 Channel	Resource Hijacking	Firmware Corruption
	Gather Victim Org Information	Establish Accounts	Hardware Additions	User Execution	Account Manipulation	Obfuscated Files or Information	System Network Connections Discovery	Lateral Tool Transfer	Internal Spearphishing	Clipboard Data	Web Service	Exfiltration Over Physical Medium	Network Denial of Service	Endpoint Denial of Service
	Phishing for Information	Obtain Capabilities	Exploit Public-Facing Application	Exploitation for Client Execution	Process Injection	Abuse Elevation Control Mechanism	Taint Shared Content	Automated Collection	Internal Spearphishing	Audio Capture	Ingress Tool Transfer	Exfiltration Over Web Service	System Shutdown/Reboot	System Shutdown/Reboot
	Search Closed Sources	External Remote Services	External Remote Services	System Services	Access Token Manipulation	Abuse Elevation Control Mechanism	Exploitation of Remote Services	Remote Service Session Hijacking	Internal Spearphishing	Traffic Capture	Data Encoding	Automated Exfiltration	Account Access Removal	Disk Wipe
	Search Open Technical Databases	Command and Scripting Interpreter	Drive-by Compromise	Command and Scripting Interpreter	Browser Extensions	Escape to Host	File and Directory Discovery	Adversary-in-the-Middle	Internal Spearphishing	Browser Session Hijacking	Traffic Signaling	Exfiltration Over Alternative Protocol	Data Manipulation	Data Manipulation
	Search Open Websites/Domains	Native API	Inter-Process Communication	Native API	Traffic Signaling	Exploitation for Privilege Escalation	Peripheral Device Discovery	Virtualization/Sandbox Evasion	Internal Spearphishing	Data from Information Repositories	Non-Standard Port	Transfer Data to Cloud Account		
	Search Victim-Owned Websites	Inter-Process Communication	Container Administration Command	Inter-Process Communication	BITS Jobs	Server Software Component	Network Share Discovery	Cloud Service Dashboard	Internal Spearphishing	Archive Collected Data	Encrypted Channel			
		Deploy Container	Serverless Execution	Deploy Container	Server Software Component	Pre-OS Boot	Password Policy Discovery	Software Discovery	Internal Spearphishing	Data from Network Shared Drive	Non-Application Layer Protocol			
					Pre-OS Boot	Compromise Client Software Binary	Browser Bookmark Discovery	Query Registry	Internal Spearphishing	Data from Cloud Storage Object				
					Internal	Modify Authentication Process	Debugger Evasion	System Location Discovery	Internal Spearphishing	Data from Configuration Repository				

・ “ATT&CK ENTERPRISE FRAMEWORK” に EMOTETの攻撃者の行動をMAITRE社がナビゲートした結果を示す。

・ Tactics(戦術=攻撃者が行動する理由)に検出されたTechniques(目標達成の技術)をプロットした

プロットから、EMOTETにおいては、初期アクセスから情報窃取に至るフェーズ (Tactics) に複合する攻撃手法 (Techniques) が用いられる。

- 【凡例】
- [Red Circle] ; 検出されたEMOTET攻撃者行動
 - [Pink Box] フレームワークは <https://attack.mitre.org/> を基本とするバージョンの差異あり (Web翻訳可能)
 - 参照したナビゲータ [ATT&CK® Navigator \(mitre-attack.github.io\)](https://mitre-attack.github.io)

【ご注意】この資料は定例研究会の説明のためだけに作成したもので、他の用途への利用は想定しておりません。ご参加者ご本人限りにてお願いいたします。また翻訳内容には誤りがある可能性がありますので、正確な内容は原文をご参照ください。

【参考】MITRE ATT&CK®の使い方（EMOTETを調べてみる）

(1) EMOTETを把握する（手順①～④、表示画面）

(1)_① HPにアクセス
<https://attack.mitre.org/>

(1)_② Searchをクリック
検索Windowが開く

(1)_③ “EMOTET”を検索 → 結果

- Software S0367
- EMOTETの実行、確認事象を表示 (黄色網掛け)

(1)_④ “S0367”をクリック
EMOTET の概要説明

EMOTET(SOFT) 概説

- EMOTET(SOFT) 概説 S0367
- 関連ソフト
- 使用した攻撃手法

EMOTET(SOFT) 概説

- ID: S0367
- ① Associated Software: Geodo
- ① Type: MALWARE
- ① Platforms: Windows
- Contributors: Omkar Gudhate
- Version: 1.5
- Created: 25 March 2019
- Last Modified: 29 September 2022

Associated Software Descriptions

Name	Description
Geodo	[2]

Techniques Used

Domain	ID	Name	Use
Enterprise	T1134	.001 Access Token Manipulation: Token Impersonation/Theft	Emotet h

[Source] MITRE , MITRE ATT&CK, MITRE, <https://attack.mitre.org/>, (access 2024/5/24)

【ご注意】この資料は定例研究会の説明のためだけに作成したもので、他の用途への利用は想定しておりません。ご参加者ご本人限りにてお願いいたします。また翻訳内容には誤りがある可能性がありますので、正確な内容は原文をご参照ください。

【参考】MITRE ATT&CK®の使い方（EMOTETを調べてみる）

(2) EMOTET 攻撃手法の把握 – ブルートフォースに着目（手順①、表示画面）

The image shows a screenshot of the MITRE ATT&CK interface. On the left, the 'SOFTWARE' list includes Emotet, Empire, EnvyScout, Epic, Escobar, esentutil, eSurv, EventBot, EvilBunny, EvilGrab, EVILNUM, Exaramel for Linux, Exaramel for Windows, Exobot, Exodus, and Expand. The 'Techniques Used' table is displayed, with the following data:

Domain	ID	Name	Use
Enterprise	T1071	.001 Application Layer Protocol: Web Protocols	Emotet has
Enterprise	T1560	Archive Collected Data	Emotet has
Enterprise	T1547	.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Emotet has
Enterprise	T1110	.001 Brute Force: Password Guessing	Emotet has
Enterprise	T1059	.001 Command and Scripting Interpreter: PowerShell	Emotet has
		.003 Command and Scripting Interpreter: Windows Command Shell	Emotet has

A callout box with a dashed border points to the 'Brute Force: Password Guessing' row in the table, containing the text: (2)_① EMOTETの攻撃手法 “Brute Force”に着目しT110をクリック. Another callout box points to the 'Brute Force' technique in the 'TECHNIQUES' sidebar, containing the text: • Brute Force を概説 テクニックの概要、属性 • 攻撃のテクニック（4つ）を解説 Password Guessing Password Cracking Password Spraying Credential Stuffing それぞれの攻撃手順の例、緩和策、検出法を示している.

[Source] MITRE , MITRE ATT&CK, MITRE, <https://attack.mitre.org/>, (access 2024/5/24)

【ご注意】この資料は定例研究会の説明のためだけに作成したもので、他の用途への利用は想定しておりません。ご参加者ご本人限りにてお願いいたします。また翻訳内容には誤りがある可能性がありますので、正確な内容は原文をご参照ください。

【参考】MITRE ATT&CK®の使い方（EMOTETを調べてみる）

(3) ブルートフォース – パスワード推測攻撃（手順①～⑤、表示画面）

The screenshot shows the MITRE ATT&CK interface. On the left, a navigation menu lists various attack techniques, with 'Brute Force' expanded to show 'Password Guessing'. A purple box labeled '(3)_① "Brute Force"攻撃の Password Guessingをクリック' points to this menu item. The main content area displays the 'Brute Force' page, including a table of 'Procedure Examples' and a 'Mitigations' table. A purple box labeled '(3)_② 手順例に "EMOTET" S0367 が確認できる' points to the 'Emotet' entry in the Procedure Examples table. A purple box labeled '(1)_④ "M1036"をクリック' points to the 'M1036' entry in the Mitigations table. On the right, a 'Mitigation' detail page for 'Account Use Policies' is shown, with a purple box labeled '(3)_⑤ ブルートフォースT1110の アカウント使用ポリシー T1036、緩和策によって対処できることが示される' pointing to the 'T1036' entry in the 'Techniques Addressed by Mitigation' table.

ID	Name	Description
S0020	China Chopper	China Chopper's server component can perform brute force password guessing against authentication portals. ^[7]
S0488	CrackMapExec	CrackMapExec can brute force passwords for a specified user on a single target system or across an entire network. ^[8]
S0367	Emotet	Emotet has been observed using a hard coded list of passwords to brute force user accounts. ^{[9][10][11][12][13][14]}
S0698	HermeticWizard	HermeticWizard can use a list of hardcoded credentials in an attempt to authenticate to SMB Shares. ^[15]

ID	Mitigation	Description
M1036	Account Use Policies	Set account lockout policies in environments un-usable, with all accounts used in the brute force being locked-out. Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges. ^[22]
M1032	Multi-factor Authentication	Use multi-factor authentication. Where available, require MFA for all users.
M1027	Password Policies	Refer to NIST guidelines when creating passwords.
M1051	Update Software	Upgrade management services to the latest versions to address known vulnerabilities in the passwords.

Domain	ID	Name	Use
Enterprise	T1110	Brute Force	Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy may create a denial of service condition and render environments unusable, with all accounts used in the brute force being locked-out. Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges. ^[1]
	.001	Password Guessing	Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy may create a denial of service condition and render environments unusable, with all accounts used in the brute force being locked-out. Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges. ^[1]
	.003	Password Spraying	Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy may create a denial of service condition and render environments unusable, with all accounts used in the brute force being locked-out. Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges. ^[1]
	.004	Credential Stuffing	Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy may create a denial of service condition and render environments unusable, with all accounts used in the brute force being locked-out. Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges. ^[1]
Enterprise	T1621	Multi-Factor Authentication Request Generation	Enable account restrictions on non-compliant devices or from outside defined organization IP ranges.
Enterprise	T1078	Valid Accounts	Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges. ^[1]
	.004	Cloud Accounts	Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges. ^[1]

[Source] MITRE , MITRE ATT&CK, MITRE, <https://attack.mitre.org/>, (access 2024/5/24)

【ご注意】この資料は定例研究会の説明のためだけに作成したもので、他の用途への利用は想定しておりません。ご参加者ご本人限りにてお願いいたします。また翻訳内容には誤りがある可能性がありますので、正確な内容は原文をご参照ください。

【参考】MITRE ATT&CK®の使い方（EMOTETを調べてみる）

(4) EMOTET 検知 – ブルートフォースに連携して（手順①～②、表示画面）

The screenshot shows the MITRE ATT&CK website interface. On the left, a navigation menu is visible with 'Brute Force' expanded to show 'Password Guessing'. A callout box points to 'Password Guessing' with the text: (4)_① “Brute Force”攻撃の Password Guessingをクリック. The main content area shows search results for 'Brute Force' with entries for S0374 (SpeakUp) and S0341 (Xbash). Below this is a 'Mitigations' section with a callout box: ・検出法 DS0015 アプリケーションログ DS0002 ユーザアカウントの試行失敗監視. The 'Detection' section contains a table with the following data:

ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Monitor authentication logs for system access to a system using legitimate credentials.
DS0002	User Account	User Account Authentication	Monitor for many failed authentication attempts.

Below the table is a 'References' section with a list of links. On the right, the 'Data Components' section for DS0015 is shown, with a callout box: (4)_② “Data Component”の各項目をクリックして、ログの構成内容を確認. The 'Data Components' table lists various log entries with their domains, IDs, names, and detection details.

[Source] MITRE , MITRE ATT&CK, MITRE, <https://attack.mitre.org/>, (access 2024/5/24)

7. まとめ

1. ISO/IEC 27002:2022の改訂にみる表題及び追加管理策から、サイバーセキュリティとプライバシー保護が強調されるもとの、具体的な管理策が追加（11項目）された。

特に追加された脅威インテリジェンスは、情報セキュリティ方針と両輪を成し、組織・経営を方向付ける情報セキュリティの核になる。その重要さに対応した脅威の認識、情報の収集・分析、インテリジェンスを構築することが求められている。

2. 脅威インテリジェンス（CTI）の獲得・構築には、攻撃者の行動を体系的に、かつ攻撃者が使用し検出された手法を具体的なknowledgeとする営みが必要といえる。

CTIの情報共有には、関係者・専門家と協調し、論理性を持った指導とアプローチをToolの活用によって確実とする。客観的、公明性を得、また監査・モニタリングを担保することも可能といえる。何よりも、CTIに潜む不確実性、エントロピー増大を制する。

研究部会では、MITER社ATT&CK®を対象に、これまでの脆弱性情報と分別する検証を試み、EMOTETをサンプルにして、ATT&CKのフレームワークを適用した。

結論に至っていないが、適用にあたっては、①攻撃に対する事前知識の整理、②攻撃者の行動を割り付けるフレームの定義と攻撃手法のマッピング、③インシデント対応の根拠付けが要点となる。

3. 攻撃者の行動をモデル化することはインシデントの後付けと考える。脅威インテリジェンスは、①攻撃者の行動（振る舞い）を表出し、共有できる、②攻撃者の手法が検出できる、③予知できることが対応策を確実にする、を狙いに構築する。

本研究が少しでも皆様のお役に立つことを願い、研究を継続し、さらなる成果を皆様と共有したいと思います。

8. 2024年度 PJ研究テーマ

・ 情報セキュリティ研究 – 継続的な探究学習

継続的な研究	サイバーインシデント対応を軸に継続的に研究、テーマ選定を実施 <これまでの研究テーマ> <ul style="list-style-type: none">・ 2021～2022年度 ゼロトラスト・ 2023年度 27001改訂と脅威インテリジェンス
研究テーマと概要	情報セキュリティの確立と強化のための有効な考え方、具体的実施策の、幅広い研究と提案 昨今のサイバーリスクに対する環境を踏まえたテーマの選定、関係する情報の収集と分析、多様な見解を尊重した意見交換により、参加者それぞれの研究を促進するとともに、研究プロジェクトとして研究成果にまとめ、公表・発表する。 <テーマ> <ul style="list-style-type: none">・ 「サイバーインシデント対応」にかかる情報の収集と発信・ 改訂JISQ27002 (ISO/IEC27002) の深読み・ サイバーセキュリティ, 事業継続と情報セキュリティ, デジタルフォレンジック, サプライチェーンセキュリティ, ソフトウェア開発の外部委託と情報セキュリティ 等
計画日程	原則月1回の頻度でZoomオンライン会議にて開催する。 1. 情報セキュリティ、事業継続、リスクマネジメント等にかかる事例、国内外の基準・標準の動向調査等の情報共有 2. 各人の研究関連情報および事例に関する意見交換

8. 2024年度 PJ研究テーマ

● 「サイバーインシデント対応」にかかる情報の収集と発信

● 2024年度 研究テーマ

継続して「サイバーインシデント対応」を研究テーマに予定します。

研究の過程で、情報セキュリティを取り巻く環境変化、インシデントやリファレンスの動向により、また、究明する重点を判断しテーマのステップアップを図ります。

● 取組み

情報セキュリティの確立と強化のための有効な考え方、具体的実施策の、幅広い研究と提案に取り組みます。

監査に関する実施基準、ISO/IEC 27001やNISTなど標準となるガイドライン、昨今のサイバーリスクに対する環境を踏まえたテーマの選定し、関係する情報の収集と分析、多様な見解を尊重した意見交換により、参加者それぞれの研究を促進するとともに、研究プロジェクトとして研究成果にまとめ、公表・発表します。

情報セキュリティ、事業継続、リスクマネジメント等にかかる事例、国内外の基準・標準の動向調査等の情報共有、及び各人の研究関連情報および事例に関する意見交換を行います。

参加メンバーの募集

・PJ実施のシナリオ

● 計画日程

原則 月1回の頻度でZoomオンライン会議を開催します。

学会の研究会、研究大会において、研究結果・成果を報告します。

● 研究のアプローチ

(1) 目標の設定・設定そのものの議論、周辺知識の取得、論題・疑問点の設定

(2) 参考文献、根拠資料の収集と明示、引用の区別

(3) 学会員としてパーソナリティ、オリジナリティを活かし、かつ、協調を醸すコミュニケーション・論議

(4) 業務に役立たせる情報、シンキングツールの発信

・PJ参加の申込

● システム監査学会HP>研究活動>研究プロジェクトの登録 登録フォームからお申し込みください。

(随時受け付けています。非会員の方は、会員になってプロジェクトに参加しませんか。)



Fine