MITRE ATT&CK®を用いたセキュリティインシデント実例の分析と,コストを考慮したセキュリティ対策の提言

田中啓介[†1]　東結香[†1]　上原哲太郎[†2]

概要：本研究では,セキュリティ対策に十分な費用を割くことが難しい組織が，効果的な対策を実施できることを目的とし,MITRE ATT&CK を用いてセキュリティインシデント実例で観測された攻撃手法と対策を整理した.また,各対策を実施するコストについての評価を合わせて実施した.

キーワード：セキュリティインシデント，セキュリティ対策，インシデント対応，MITRE ATT&CK

Proposal for cost effective security countermeasure from recent security incident and MITRE ATT&CK®

KEISUKE TANAKA[†1]　YUKA HIGASHI[†1]　TETSUTARO UEHARA[†2]

Abstract: In this study, we sorted out the attack methods and countermeasures observed in the security incidents by using MITRE ATT&CK in order to enable the organizations which are difficult to allocate enough money for security measures to implement effective measures. In addition, we evaluated the cost of implementing the countermeasures with MITRE ATT&CK.

Keywords: Security Incident，Security countermeasure，Incident Response，MITRE ATT&CK

1. はじめに

(1) 背景

企業や組織において，事業活動を行う為に利用者端末やサーバ機のインターネットや社内ネットワーク接続は前提となっており，そういった環境を踏まえ金銭や情報窃取を目的とした不正アクセスや不正プログラムによるサイバー攻撃等のセキュリティインシデント事例が継続的に発生している[1].

また，そういったセキュリティインシデント発生をリスクと捉えて正しくセキュリティ対策を実施する為には，最低限の情報セキュリティ知識や，専任の IT 管理者，IT セキュリティ担当者の配備や教育が必要となるが，人材確保や費用の観点からそれらの配備が難しい組織が多く存在すると考えられる[2]. 実際に, セキュリティ対策に十分な費用を割くことが難しい中小企業において，基本的なセキュリティ対策が施されていないことに起因し，大規模な感染や事業被害に遭っていると考えられる事案もある.

昨今では MITRE ATT&CK[3]というフレームワークがセキュリティソフトウェアの性能評価や企業におけるセキュリティ対策状況の評価等に用いられるようになってきており，本フレームワークを各企業が活用しセキュリティ対策に反映することができれば各企業の大規模なセキュリティ被害を防げると考えられる．しかしながら，本フレームワークを読み解いてセキュリティ対策を実装するには，技術的な前提知識が必要となる為，本研究で対象としたいセキュリティ対策に十分な費用を割けない企業においては活用が難しいのではないかと考えた.

上記の背景を踏まえ，著者らが関わった実際のセキュリティインシデントで観測された複数の攻撃手法を MITRE ATT&CK で整理し，様々な組織・企業において効果的なセキュリティ対策を明らかにしたいと考えた.

(2) 概要

本研究では，2019 年 1 月から 2020 年 6 月末に著者らの所属組織において支援を実施した不正プログラム感染を起点とするセキュリティインシデントを, MITRE ATT&CK の Tactics, Techniques, Mitigations に当てはめて整理した．その後，より具体的で実装可能な対策を導き出すために，著者らが 2020 年 7 月に実施した研究「セキュリティインシデント実例を元にした各種ガイドラインの対策評価と，効果的なセキュリティ対策の提言」[4]で提言を行った技術的対策項目と突き合わせ，実装のコストを考慮したセキュリティ対策を導き出す.

†1 トレンドマイクロ株式会社
Trend Micro Incorporated
†2 立命館大学
Ritsumeikan University

© 2020 Information Processing Society of Japan

(3) 貢献

本研究で目指す貢献は以下のとおりである．

・企業のセキュリティ担当者が，学習や選定の手間をかけずに効果的なセキュリティ対策を実施できる
・MITRE ATT&CK を用いた実践的なセキュリティ対策を検討しているセキュリティ担当者が, MITRE ATT&CK の活用方法について理解を深められる

(4) MITRE ATT&CK の概要

MITRE ATT&CK とは，MITRE 社が 2013 年に開発した ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) フレームワーク及びナレッジベースであり, サイバー攻撃に用いられた攻撃手法を網羅的に整理したものである．「MITRE ATT&CK: Design and Philosophy[5]」によれば，フレームワークの主となる構成要素は以下の 5 要素となる。

- Adversary Group：攻撃グループ
- Software：攻撃者の利用ツール
- Techniques：攻撃に使われる技術，戦法
- Tactics：攻撃の目的
- Mitigation：緩和策

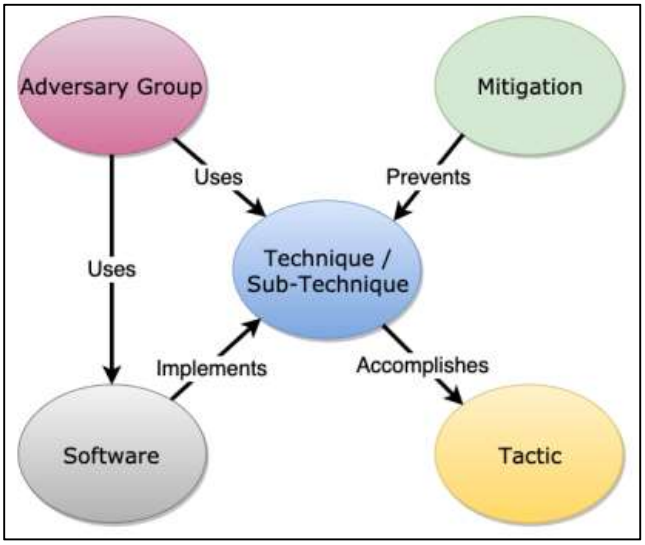


図 1 構成要素(ATT&CK: Design and Philosophy,P17)

Techniques には Mitigations と呼ばれる緩和策が紐づいている為，セキュリティ対策について検討する場合には，自組織に対して攻撃を行ってくることが想定される Adversary Group,及びその利用 Techniques を洗い出し，Techniques に紐づく Mitigations を参考にすることで有効な対策を導き出すことが可能となっている．それぞれの項目には一意の ID が付与されているため，企業の管理者やセキュリティベンダが会話をする際の共通言語としても活用可能となっている．

なお，「図 2 Tactics > Techniques > Mitigations の関係性」の通り，Tactics には複数の Techniques が紐づいており，Techniques には単数あるいは複数の Mitigations が紐づいているが，有向非巡回グラフ(DAG)の構成となっており，Mitigations が複数の Techniques に紐づいていることもある（図 2 の Mitigation3 の赤線）．この点は後述する対策項目評価に大きく関わる点となる．

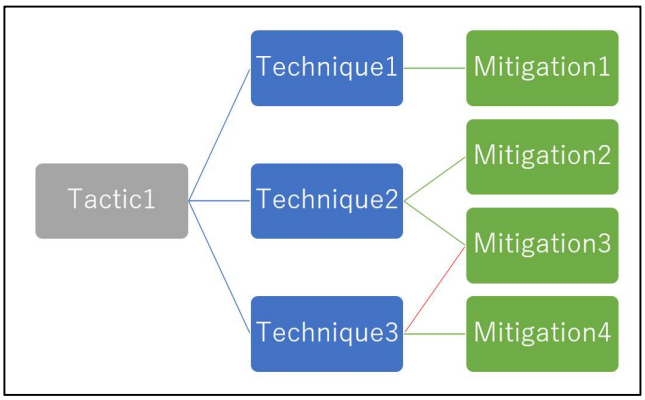


図 2 Tactics > Techniques > Mitigations の関係性

(5) 著者らが実施した先行研究の概要

2020 年 7 月に著者らが実施した「セキュリティインシデント実例を元にした各種ガイドラインの対策評価と，効果的なセキュリティ対策の提言」では，2019 年に著者らが支援を実施した 9 件のセキュリティインシデント(a-i)の被害原因の技術的な共通項を整理した上で，公開されている著名なガイドライン等で提言されているセキュリティ対策を 16 個(No1-16)選定し，a-i のインシデントにおいて効果的であったかを A-B の 3 段階で評価した．また，併せてその対策を実施する運用コストを以下の H-M-L の 3 段階で評価した(表 1).

表 1 先行研究におけるセキュリティ対策の評価

		事案(a-m)と評価(A-C)									合計		
No	対策項目	a	b	c	d	e	f	g	h	i	A	B	C
1	運用管理専用の端末設置とネットワーク分離	A	B	C	C	C	C	C	C	C	1	1	7
2	管理者権限アカウントのキャッシュ禁止（管理者権限の分離）	A	C	C	C	C	C	C	C	C	1	0	8
3	認証プロキシ機能・リーバの導入	C	C	C	C	C	C	C	C	C	0	0	9
4	443ポート以外へのConnectメソッド通信の遮断	C	C	C	C	C	C	C	C	C	0	0	9
5	OSやソフトウェアを常に最新の状態にする	C	C	A	C	C	A	A	C	A	4	0	5
6	ウイルス対策ソフトを導入し定義ファイルを最新の状態にする	C	A	B	C	B	A	B	B	B	2	5	2
7	管理者アカウントに複雑性を満たすパスワードを設定している	B	B	C	C	A	C	C	A	B	2	3	4
8	ホワイトリスティングによる不審なプログラムの実行抑止	A	A	A	A	A	A	A	A	A	9	0	0
9	自動再生（オートラン）機能の無効化	C	C	C	C	C	C	C	C	C	0	0	9
10	OSの悪用防止機能(DEP,ASLR等)を有効にする	B	B	B	B	B	B	B	B	B	0	9	0
11	すべてのリモートログインに多要素認証の使用を義務付ける	C	B	C	C	C	B	B	A	C	1	3	5
12	ワークステーション同士の通信を無効にする	B	B	A	C	C	A	A	A	A	5	2	2
13	SMBプロトコルを中心としたネットワーク設計の見直し	B	C	B	C	C	A	A	A	A	4	2	3
14	許可されていない無線アクセスポイントへの接続制御	C	A	C	C	C	C	A	C	C	2	0	7
15	ホスト型IPS(脆弱性検知機能)の導入	C	C	A	C	C	A	A	C	A	4	0	5
16	ソフトウェアの利用制限(Internet Exploler,Adobe,Java等)	C	C	C	C	C	C	C	C	C	0	0	9

2. 手法と評価

本研究内の対象を明確にする目的で先に用語の定義を行い，その後に評価ステップを 4 段階で記載した．

2.1 本研究内における用語の定義

・セキュリティインシデント

不正プログラム感染による情報セキュリティインシデントを対象とする．機密情報の紛失や内部不正といったものは対象外となる．

・セキュリティ対策

セキュリティ対策は管理体制やガバナンスといったものから対策技術や運用・対応フローなど多岐に渡るが，本研究においては,「不正プログラム感染に対する技術的な対策」をセキュリティ対策とする．具体的には NIST Cyber Security Framework[6]で定義されている 5 つのカテゴリ「識別，防御，検知，対応，復旧」のうち，カテゴリ「防御，検知」の保護技術(PR，PT)，検知プロセス（DE，DP）を対象としている(表 2).

表 2　NIST Cyber Security Framework 機能カテゴリ(引用)

機能の識別子	機能	カテゴリーの識別子	カテゴリー
ID	識別	ID.AM	資産管理
		ID.BE	ビジネス環境
		ID.GV	ガバナンス
		ID.RA	リスクアセスメント
		ID.RM	リスクマネジメント戦略
		ID.SC	サプライチェーンリスクマネジメント
PR	防御	PR.AC	アイデンティティ管理とアクセス制御
		PR.AT	意識向上およびトレーニング
		PR.DS	データセキュリティ
		PR.IP	情報を保護するためのプロセスおよび手順
		PR.MA	保守
		PR.PT	保護技術
DE	検知	DE.AE	異常とイベント
		DE.CM	セキュリティの継続的なモニタリング
		DE.DP	検知プロセス
RS	対応	RS.RP	対応計画の作成
		RS.CO	コミュニケーション
		RS.AN	分析
		RS.MI	低減
		RS.IM	改善
RC	復旧	RC.RP	復旧計画の作成
		RC.IM	改善
		RC.CO	コミュニケーション

2.2 手法概要

MITRE ATT&CK，及び著者らが実施した先行研究には以下の課題があると考える．

MITRE ATT&CK：

・対策手法(Mitigations)を具体的にどのような技術や設定値で実装するかについては自身で読み解く必要がある

・対策手法(Mitigations)を実装するにあたっての費用や労力は自身で算出する必要がある

著者らの先行研究：

・各種ガイドラインから抜き出した対策項目の網羅性や妥当性の担保，評価が難しい

上記 3 点の課題を解決した上で有効な対策案を導き出す為に，以下の 4 段階にて整理と評価を実施した．

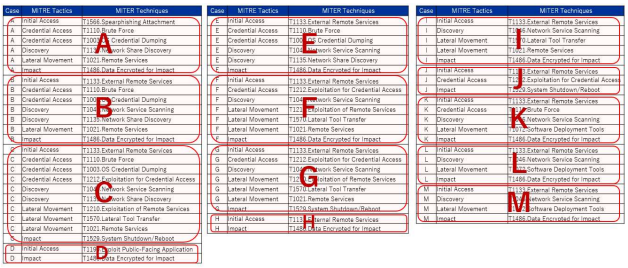
1. インシデント情報を MITRE ATT&CK で整理
2. セキュリティ対策項目(Mitigations)の整理
3. セキュリティ対策項目の評価
4. 実装コストの評価

2.2.1.インシデント情報を MITRE ATT&CK で整理

まず，2019 年 1 月から 2020 年 6 月迄に著者らが所属する組織のインシデント対応チームで支援を行ったセキュリティインシデント対応の内，ある程度全体像や詳細な攻撃手法・侵入起点が判明している事案を A から M の 13 件洗い出した（Appendix1）．なお，標的型攻撃インシデントは単一対策での防御が難しいことが多い為除いている．

その後，これらの事案で確認された攻撃手法を MITRE ATT&CK の Tactics, Techniques で整理した(表 3，及び Appendix2)． Tactics についてはフレームワークでは 12 個存在するが，整理するにあたり十分な情報が存在し，かつ重要な対策ポイントとなる「Initial Access，Credential Access，Discovery，Lateral Movement，Impact」の 5 個を利用した．

表 3　MITRE ATT&CK による整理



Case	MITRE Tactics	MITRE Techniques
A	Initial Access	T1566.Spearphishing Attachment
A	Credential Access	T1110.Brute Force
A	Credential Access	T1003.OS Credential Dumping
A	Discovery	T1135.Network Share Discovery
A	Lateral Movement	T1021.Remote Services
A	Impact	T1486.Data Encrypted for Impact
B	Initial Access	T1133.External Remote Services
B	Credential Access	T1110.Brute Force
B	Credential Access	T1003.OS Credential Dumping
B	Discovery	T1046.Network Service Scanning
B	Discovery	T1135.Network Share Discovery
B	Lateral Movement	T1021.Remote Services
B	Impact	T1486.Data Encrypted for Impact
C	Initial Access	T1133.External Remote Services
C	Credential Access	T1110.Brute Force
C	Credential Access	T1003.OS Credential Dumping
C	Credential Access	T1212.Exploitation for Credential Access
C	Discovery	T1046.Network Service Scanning
C	Discovery	T1135.Network Share Discovery
C	Lateral Movement	T1210.Exploitation of Remote Services
C	Lateral Movement	T1570.Lateral Tool Transfer
C	Lateral Movement	T1021.Remote Services
C	Impact	T1529.System Shutdown/Reboot
D	Initial Access	T1190.Exploit Public-Facing Application
D	Impact	T1486.Data Encrypted for Impact
E	Initial Access	T1133.External Remote Services
E	Credential Access	T1110.Brute Force
E	Credential Access	T1003.OS Credential Dumping
E	Discovery	T1046.Network Service Scanning
E	Discovery	T1135.Network Share Discovery
E	Impact	T1486.Data Encrypted for Impact
F	Initial Access	T1133.External Remote Services
F	Credential Access	T1212.Exploitation for Credential Access
F	Discovery	T1046.Network Service Scanning
F	Lateral Movement	T1210.Exploitation of Remote Services
F	Lateral Movement	T1570.Lateral Tool Transfer
F	Lateral Movement	T1021.Remote Services
F	Impact	T1486.Data Encrypted for Impact
G	Initial Access	T1133.External Remote Services
G	Credential Access	T1212.Exploitation for Credential Access
G	Discovery	T1046.Network Service Scanning
G	Lateral Movement	T1210.Exploitation of Remote Services
G	Lateral Movement	T1570.Lateral Tool Transfer
G	Lateral Movement	T1021.Remote Services
G	Impact	T1529.System Shutdown/Reboot
H	Initial Access	T1133.External Remote Services
H	Impact	T1486.Data Encrypted for Impact
I	Initial Access	T1133.External Remote Services
I	Discovery	T1046.Network Service Scanning
I	Lateral Movement	T1021.Remote Services
I	Impact	T1486.Data Encrypted for Impact
J	Initial Access	T1133.External Remote Services
J	Credential Access	T1212.Exploitation for Credential Access
J	Impact	T1529.System Shutdown/Reboot
K	Initial Access	T1133.External Remote Services
K	Credential Access	T1110.Brute Force
K	Discovery	T1046.Network Service Scanning
K	Lateral Movement	T1072.Software Deployment Tools
K	Impact	T1486.Data Encrypted for Impact
L	Initial Access	T1133.External Remote Services
L	Discovery	T1046.Network Service Scanning
L	Lateral Movement	T1072.Software Deployment Tools
L	Impact	T1486.Data Encrypted for Impact
M	Initial Access	T1133.External Remote Services
M	Discovery	T1046.Network Service Scanning
M	Lateral Movement	T1072.Software Deployment Tools
M	Impact	T1486.Data Encrypted for Impact

また，どの事案でどの Techniques が利用されたか，及び何回利用されたかを可視化するために表 4 で整理を行った．

表 4　Tactics, Techniques と事案 A-M の突合

	Case													
Tactics > Techniques	A	B	C	D	E	F	G	H	I	J	K	L	M	総計
Initial Access	1	1	1	1	1	1	1	1	1	1	1	1	1	13
T1133.External Remote Services		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	11
T1190.Exploit Public-Facing Application				✓										1
T1566.Spearphishing Attachment	✓													1
Credential Access	2	2	3		2	1	1			1	1			13
T1003.OS Credential Dumping	✓	✓	✓		✓									4
T1110.Brute Force	✓	✓	✓		✓						✓			5
T1212.Exploitation for Credential Access			✓			✓	✓			✓				4
Discovery	1	2	2		2	1	1		1		1	1	1	13
T1046.Network Service Scanning		✓	✓		✓	✓	✓		✓		✓	✓	✓	9
T1135.Network Share Discovery	✓	✓	✓		✓									4
Lateral Movement	1	1	3			3	3		2		1	1	1	16
T1021.Remote Services	✓	✓	✓			✓	✓		✓					6
T1072.Software Deployment Tools											✓	✓	✓	3
T1210.Exploitation of Remote Services			✓			✓	✓							3
T1570.Lateral Tool Transfer			✓			✓	✓		✓					4
Impact	1	1	1	1	1	1	1	1	1	1	1	1	1	13
T1486.Data Encrypted for Impact	✓	✓		✓	✓	✓		✓	✓		✓	✓	✓	10
T1529.System Shutdown/Reboot			✓				✓			✓				3

2.2.2.セキュリティ対策項目(Mitigations)の整理

次に，Techniques には単数から複数の Mitigations（対策項目）が紐づいているため，過去事例で利用があった Techniques と紐づく Mitigations の一覧を作成した(Appendix3).

また, 先行研究で選定した 16 個のセキュリティ対策を, 適切であると思われる Mitigations と紐づけた(表 5).

表 5 先行研究の対策項目と Mitigations の紐づけ

No	対策項目	Mitigations
1	運用管理専用の端末設置とネットワーク分離	M1030.Network Segmentation
2	管理者権限アカウントのキャッシュ禁止（管理者権限の分離）	M1043.Credential Access Protection
3	認証プロキシ機能・サーバの導入	M1037.Filter Network Traffic
4	443ポート以外へのConnectメソッド通信の遮断	M1037.Filter Network Traffic
5	OS やソフトウェアを常に最新の状態にする	M1051.Update Software
6	ウイルス対策ソフトを導入し定義ファイルを最新の状態にする	M1049.Antivirus/Antimalware
7	管理者アカウントに複雑性を満たすパスワードを設定している	M1027.Password Policies
8	ホワイトリスティングによる不審なプログラムの実行抑止	M1038.Execution Prevention
9	自動再生（オートラン）機能の無効化	M1038.Execution Prevention
10	OSの悪用防止機能(DEP,ASLR等)を有効にする	M1050.Exploit Protection
11	すべてのリモートログインに多要素認証の使用を義務付ける	M1032.Multi-factor Authentication
12	ワークステーション同士の通信を無効にする	M1035.Limit Access to Resource Over Network
13	SMBプロトコルを中心としたネットワーク設計の見直し	M1035.Limit Access to Resource Over Network
14	許可されていない無線アクセスポイントへの接続制御	M1012.Enterprise Policy
15	ホスト型IPS(脆弱性検知機能)の導入	M1031.Network Intrusion Prevention
16	ソフトウェアの利用制限(Internet Exploler,Adobe,Java等)	M1033.Limit Software Installation

2.2.3. セキュリティ対策項目の評価

2.2.1 で算出した，事案 A-M で攻撃者に利用された Techniques の利用回数と，Techniques に紐づく Mitigations の登場回数を「MI Score」（MI : Mitigation of Incident）と名付け評価を行った（表 6）.

表 6　Mitigations の評価(MI Score)

Mitigations	MI Score
M1030.Network Segmentation	27
M1032.Multi-factor Authentication	25
M1042.Disable or Remove Feature or Program	23
M1018.User Account Management	14
M1031.Network Intrusion Prevention	14
M1027.Password Policies	12
M1051.Update Software	11
M1035.Limit Access to Resource Over Network	11
M1026.Privileged Account Management	11
M1053.Data Backup	10
M1050.Exploit Protection	8
M1048.Application Isolation and Sandboxing	8
M1017.User Training	8
M1019.Threat Intelligence Program	7
M1015.Active Directory Configuration	7
M1036.Account Use Policies	5
M1043.Credential Access Protection	4
M1016.Vulnerability Scanning	4
M1028.Multi-factor Authentication	4
M1037.Filter Network Traffic	4
M1028.Operating System Configuration	4
M1041.Encrypt Sensitive Information	4
M1025.Privileged Process Integrity	4
None	3
M1029.Remote Data Storage	3
M1021.Restrict Web-Based Content	1
M1049.Antivirus/Antimalware	1

例えば，Mitigation 「M1030.Network Segmentation」は，5 つの Techniques の対策として紐づいており，この 5 つの Techniques は実際のインシデントで合計 27 回利用されているため，MI Score は 27 としている(表 7).

表 7　MI Score 算出例 (M1030.Network Segmentation)

Techniques	登場回数
T1133.External Remote Services	11
T1190.Exploit Public-Facing Application	1
T1046.Network Service Scanning	9
T1072.Software Deployment Tools	3
T1210.Exploitation of Remote Services	3
合計	27

その後，先行研究で選定した 16 個のセキュリティ対策項目について「MI Score」を紐づけた(表 8).

表 8　先行研究の対策項目と Mitigations, MI Score の突合

No	対策	Mitigations	MI Score
1	運用管理専用の端末設置とネットワーク分離	M1030.Network Segmentation	27
2	管理者権限アカウントのキャッシュ禁止（管理者権限の分離）	M1043.Credential Access Protection	4
3	認証プロキシ機能・サーバの導入	M1037.Filter Network Traffic	4
4	443ポート以外へのConnectメソッド通信の遮断	M1037.Filter Network Traffic	4
5	OS やソフトウェアを常に最新の状態にする	M1051.Update Software	11
6	ウイルス対策ソフトを導入し定義ファイルを最新の状態にする	M1049.Antivirus/Antimalware	1
7	管理者アカウントに複雑性を満たすパスワードを設定している	M1027.Password Policies	12
8	ホワイトリスティングによる不審なプログラムの実行抑止	M1038.Execution Prevention	0
9	自動再生（オートラン）機能の無効化	M1038.Execution Prevention	0
10	OSの悪用防止機能(DEP,ASLR等)を有効にする	M1050.Exploit Protection	8
11	すべてのリモートログインに多要素認証の使用を義務付ける	M1032.Multi-factor Authentication	25
12	ワークステーション同士の通信を無効にする	M1035.Limit Access to Resource Over Network	11
13	SMBプロトコルを中心としたネットワーク設計の見直し	M1035.Limit Access to Resource Over Network	11
14	許可されていない無線アクセスポイントへの接続制御	M1012.Enterprise Policy	0
15	ホスト型IPS(脆弱性検知機能)の導入	M1031.Network Intrusion Prevention	14
16	ソフトウェアの利用制限(Internet Exploler,Adobe,Java等)	M1033.Limit Software Installation	0

2.2.4. 実装コストの評価

また, 各対策項目について導入や運用におけるコストを算出するため,「機能導入」,「設定変更」,「監視」の必要有無を Yes, No(Y/N)で評価付けを行った（表 9）. また, Y の数に応じてコストを Small, Low, Middle, High(S,L,M,H) の 4 段階でラベリングした. 本評価にあたっては, インシデントレスポンス及び対策提言の経験が 3 年以上あるメンバ 3 名で実施した.

表 9　セキュリティ対策のコスト算出

No	対策項目	導入・運用コスト評価			合計(Y)	コスト
		機能導入	設定変更	監視		
1	運用管理専用の端末設置とネットワーク分離	Y	Y	N	2	M
2	管理者権限アカウントのキャッシュ禁止（管理者権限の分離）	N	Y	N	1	L
3	認証プロキシ機能・サーバの導入	Y	Y	N	2	M
4	443ポート以外へのConnectメソッド通信の遮断	N	Y	N	1	L
5	OS やソフトウェアを常に最新の状態にする	N	N	N	0	S
6	ウイルス対策ソフトを導入し定義ファイルを最新の状態にする	N	N	N	0	S
7	管理者アカウントに複雑性を満たすパスワードを設定している	N	Y	N	1	L
8	ホワイトリスティングによる不審なプログラムの実行抑止	Y	Y	Y	3	H
9	自動再生（オートラン）機能の無効化	N	Y	N	1	L
10	OSの悪用防止機能(DEP,ASLR等)を有効にする	N	Y	N	1	L
11	すべてのリモートログインに多要素認証の使用を義務付ける	Y	Y	N	2	M
12	ワークステーション同士の通信を無効にする	N	Y	N	1	L
13	SMBプロトコルを中心としたネットワーク設計の見直し	N	Y	N	1	L
14	許可されていない無線アクセスポイントへの接続制御	N	Y	N	1	L
15	ホスト型IPS(脆弱性検知機能)の導入	Y	N	Y	2	M
16	ソフトウェアの利用制限(Internet Exploler,Adobe,Java等)	N	Y	N	1	L

3.　評価結果

2.2.1 から 2.2.4 の整理及び評価を経て, 16 件のインシデント情報を MITRE ATT&CK 及び実装コストで評価したものをスコア順に並び替えた（表 10）.

表 10 評価結果(MI Score 降順)

No	対策項目	MI Score
1	運用管理専用の端末設置とネットワーク分離	27
11	すべてのリモートログインに多要素認証の使用を義務付ける	25
15	ホスト型IPS(脆弱性検知機能)の導入	14
7	管理者アカウントに複雑性を満たすパスワードを設定している	12
5	OS やソフトウェアを常に最新の状態にする	11
12	ワークステーション同士の通信を無効にする	11
13	SMBプロトコルを中心としたネットワーク設計の見直し	11
10	OSの悪用防止機能(DEP,ASLR等)を有効にする	8
2	管理者権限アカウントのキャッシュ禁止（管理者権限の分離）	4
3	認証プロキシ機能・サーバの導入	4
4	443ポート以外へのConnectメソッド通信の遮断	4
6	ウイルス対策ソフトを導入し定義ファイルを最新の状態にする	1
8	ホワイトリスティングによる不審なプログラムの実行抑止	0
9	自動再生（オートラン）機能の無効化	0
14	許可されていない無線アクセスポイントへの接続制御	0
16	ソフトウェアの利用制限(Internet Exploler,Adobe,Java等)	0

また, コストが低く(S,L), MI Score が 10 以上のもので絞り込むと 4 件のセキュリティ対策が導き出された(表 11). これらの対策は実装が容易かつ, 効果の高いセキュリティ対策であると考えられる.

表 11 評価結果 (コスト S,L かつ MI Score 10 以上)

No	対策項目	MI Score	コスト
7	管理者アカウントに複雑性を満たすパスワードを設定している	12	L
5	OS やソフトウェアを常に最新の状態にする	11	S
12	ワークステーション同士の通信を無効にする	11	L
13	SMBプロトコルを中心としたネットワーク設計の見直し	11	L

4.　考察

4-1.評価に利用しなかった Tactics について

12 個の Tactics の内、本研究では Initial Access, Credential Access, Discovery, Lateral Movement, Impact の 5 個を整理に利用した. 参考までに事案 A における Tactics 及び Techniques の整理例を表 12 に記載した.

表 12　事案 A における 12 項目の洗い出し

MITRE Tactics	A
Initial Access	T1566.Spearphishing Attachment
Execution	T1204.User Execution T1059.Command and Scripting Interpreter
Persistence	
Privilege Escalation	
Defense Evasion	
Credential Access	T1110.Brute Force T1003.OS Credential Dumping
Discovery	T1135.Network Share Discovery
Lateral Movement	T1021.Remote Services
Collection	
Command and control	
Exfiltration	
Impact	T1486. Data Encrypted for Impact

4-2.その他 MI Score の高かった Mitigations

表 13 の 4 項目が, MI Score が 10 以上かつ, 先行研究で洗い出した 16 項目に当てはまらなかったものとなる.

表 13　16 項目以外に評価の高かった Mitigations

Mitigations	MI Score
M1042.Disable or Remove Feature or Program	23
M1018.User Account Management	14
M1026.Privileged Account Management	11
M1053.Data Backup	10

M1042 は「No16. ソフトウェアの利用制限(Internet Explorer, Adobe, Java 等)」に近い. また M1018,M1053 も「No2. 管理者権限アカウントのキャッシュ禁止（管理者権限の分離）」や「No7.管理者アカウントに複雑性を満たすパスワードを設定している」と近いが，いずれも厳密には異なる．また，M1018,1053 はいずれも「Management」ということで技術的な対策というよりは管理的・人的な対策に近く，先行研究において技術的な対策項目に特化した項目選定を行っているため，16 個の対策には合致しなかった．

M1053 についてはランサムウェア等によるデータ暗号化の Impact に対する Mitigation 項目となるが，先行研究において感染時の業務影響の軽減ではなく「攻撃を止められたかどうか」を目的とした項目選定を行っているため，16 個の対策には合致しなかった．

5. 結論

本研究では，著者らが 2019 年から 2020 年 6 月にかけて支援を行った 13 件のインシデント実例を MITRE ATT&CK で整理し，利用された Techniques から効果があると考えられる Mitigations を導き出した．また，著者らの先行研究で著名ガイドラインから抜き出した 16 件の対策項目と今回導き出された Mitigations の突合を行い，コストを考慮した具体性のある対策項目を 4 件導き出した．

本研究が，IT セキュリティに費用を割けない組織における技術的なセキュリティ対策レベル向上の一助となることを期待する．

6. 今後の課題

6-1.MI Score の算出方法

今回の評価ではインシデント事案において利用された Techniques の回数に Mitigations を乗じて「MI Score」として対策の重みを算出したが，この Score では Tactics による重みは考慮されていない．例えば Initial Access と Lateral Movement に紐づく Techniques 及び Mitigations が同じスコアであるかは組織毎の考え方等によって変動があると考えられる為，今後考慮・改善すべき項目とする．

6-2.セキュリティ対策実装コスト評価の妥当性

各セキュリティ対策の実装コストについて「機能導入」，「設定変更」，「監視」の 3 項目で評価を行ったが，今回は著者を含むインシデント対応を主軸においているメンバでの評価を行っている．今後各対策項目のコスト評価について実際に組織でセキュリティ対策を実施している有識者へのヒアリング等を行うことで，より現実的に実装可能な対策を提言できるようにする．

6-3.評価対象とするインシデント

2019 年から 2020 年 6 月までの著者らが支援したインシデントの内，標的型攻撃以外，かつある程度インシデントの全体像が把握できているものを選別しているため，件数が不十分であるという点と，著者らの組織に支援依頼があったものという点で網羅性に問題がある可能性がある．今後評価対象とするインシデント件数を増やすことや，公開情報等を元に評価対象インシデントが世の中の動向とどの程度一致しているか，確認する必要があると考える．

謝辞

セキュリティ対策コストについて共に評価を実施し，都度助言や激励をいただいた同僚の門田英嗣氏，三好太郎氏，木村仁美氏に，謹んで感謝の意を表します．

参考文献

[1] 独立行政法人情報処理通信機構，“情報セキュリティ白書 2019” https://www.ipa.go.jp/files/000079041.pdf, (2019/7/10).
[2] 経済産業省，“IT 人材の最新動向と将来推計に関する調査結果” https://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_summary.pdf, (2016/6/10)
[3] MITRE,”MITRE ATT&CK”, https://attack.mitre.org/
[4] 田中啓介，東結香，上原哲太郎，”セキュリティインシデント実例を元にした各種ガイドラインの対策評価と，効果的なセキュリティ対策の提言”，Vol-2020-IOT50,(2020/7/10)
[5] MITRE,”MITRE ATT&CK: Design and Philosophy”, https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf, (2020/3)
[6] National Institute of Standards and Technology，“Cyber Security Framework 1.1” https://doi.org/10.6028/NIST.CSWP.04162018, (2018/4)

Appendix1.セキュリティインシデント一覧

ID	侵入起点	拡散手法			最終目的	感染（拡大）原因
		認証	ツール	プロトコル		
A	メール添付	パスワード	PsExec,Powershell	SMB	ランサムウェア	不審メール添付ファイル開封、平易な管理者パスワード
B	リモートデスクトップ	パスワード	リモートデスクトップ	RDP	ランサムウェア	リモートデスクトップサービスの外部公開
C	リモートデスクトップ	MS17-010	マルウェア(Radmin)	SMB	コインマイナー	OSのパッチ適用をしていなかった
D	Web脆弱性	N/A	N/A	N/A	ランサムウェア	Webサービスのゼロデイ脆弱性
E	リモートデスクトップ	N/A	N/A	N/A	ランサムウェア	リモートデスクトップサービスの外部公開
F	不明	MS17-010	マルウェア(Radmin)	SMB	ランサムウェア	パターンファイル未更新、OSのパッチ未適用
G	不明	MS17-010	マルウェア(Radmin)	SMB	不明	パターンファイル未更新、OSのパッチ未適用
H	リモートデスクトップ	パスワード	不明	N/A	ランサムウェア	リモートデスクトップサービスの外部公開
ID	不明	MS17-010	不明	SMB	不明	OSのパッチ適用をしていなかった
J	リモートデスクトップ	パスワード	HackingTool	RDP	ランサムウェア	RDPの解放
K	リモートデスクトップ	不明	HackingTool,グループポリシー	RDP,SMB	ランサムウェア	RDP開放、グループポリシーによる拡散
L	リモートデスクトップ	不明	グループポリシー	RDP,SMB	ランサムウェア	グループポリシーによる拡散
M	リモートデスクトップ	不明	HackingTool,グループポリシー	RDP,SMB	ランサムウェア	グループポリシーによる拡散

Appendix2.MITRE ATT&CK による整理

Case	MITRE Tactics	MITER Techniques
A	Initial Access	T1566.Spearphishing Attachment
A	Credential Access	T1110.Brute Force
A	Credential Access	T1003.OS Credential Dumping
A	Discovery	T1135.Network Share Discovery
A	Lateral Movement	T1021.Remote Services
A	Impact	T1486.Data Encrypted for Impact
B	Initial Access	T1133.External Remote Services
B	Credential Access	T1110.Brute Force
B	Credential Access	T1003.OS Credential Dumping
B	Discovery	T1046.Network Service Scanning
B	Discovery	T1135.Network Share Discovery
B	Lateral Movement	T1021.Remote Services
B	Impact	T1486.Data Encrypted for Impact
C	Initial Access	T1133.External Remote Services
C	Credential Access	T1110.Brute Force
C	Credential Access	T1003.OS Credential Dumping
C	Credential Access	T1212.Exploitation for Credential Access
C	Discovery	T1046.Network Service Scanning
C	Discovery	T1135.Network Share Discovery
C	Lateral Movement	T1210.Exploitation of Remote Services
C	Lateral Movement	T1570.Lateral Tool Transfer
C	Lateral Movement	T1021.Remote Services
C	Impact	T1529.System Shutdown/Reboot
D	Initial Access	T1190.Exploit Public-Facing Application
D	Impact	T1486.Data Encrypted for Impact

Case	MITRE Tactics	MITER Techniques
E	Initial Access	T1133.External Remote Services
E	Credential Access	T1110.Brute Force
E	Credential Access	T1003.OS Credential Dumping
E	Discovery	T1046.Network Service Scanning
E	Discovery	T1135.Network Share Discovery
E	Impact	T1486.Data Encrypted for Impact
F	Initial Access	T1133.External Remote Services
F	Credential Access	T1212.Exploitation for Credential Access
F	Discovery	T1046.Network Service Scanning
F	Lateral Movement	T1210.Exploitation of Remote Services
F	Lateral Movement	T1570.Lateral Tool Transfer
F	Lateral Movement	T1021.Remote Services
F	Impact	T1486.Data Encrypted for Impact
G	Initial Access	T1133.External Remote Services
G	Credential Access	T1212.Exploitation for Credential Access
G	Discovery	T1046.Network Service Scanning
G	Lateral Movement	T1210.Exploitation of Remote Services
G	Lateral Movement	T1570.Lateral Tool Transfer
G	Lateral Movement	T1021.Remote Services
G	Impact	T1529.System Shutdown/Reboot
H	Initial Access	T1133.External Remote Services
H	Impact	T1486.Data Encrypted for Impact

Case	MITRE Tactics	MITER Techniques
I	Initial Access	T1133.External Remote Services
I	Discovery	T1046.Network Service Scanning
I	Lateral Movement	T1570.Lateral Tool Transfer
I	Lateral Movement	T1021.Remote Services
I	Impact	T1486.Data Encrypted for Impact
J	Initial Access	T1133.External Remote Services
J	Credential Access	T1212.Exploitation for Credential Access
J	Impact	T1529.System Shutdown/Reboot
K	Initial Access	T1133.External Remote Services
K	Credential Access	T1110.Brute Force
K	Discovery	T1046.Network Service Scanning
K	Lateral Movement	T1072.Software Deployment Tools
K	Impact	T1486.Data Encrypted for Impact
L	Initial Access	T1133.External Remote Services
L	Discovery	T1046.Network Service Scanning
L	Lateral Movement	T1072.Software Deployment Tools
L	Impact	T1486.Data Encrypted for Impact
M	Initial Access	T1133.External Remote Services
M	Discovery	T1046.Network Service Scanning
M	Lateral Movement	T1072.Software Deployment Tools
M	Impact	T1486.Data Encrypted for Impact

Appendix3. Techniques と Mitigations の紐づけ

Tactics > Techniques	Mitigation(ID,Description)
Initial Access	
T1133.External Remote Services	M1042.Disable or Remove Feature or Program
T1133.External Remote Services	M1035.Limit Access to Resource Over Network
T1133.External Remote Services	M1032.Multi-factor Authentication
T1133.External Remote Services	M1030.Network Segmentation
T1190.Exploit Public-Facing Application	M1048.Application Isolation and Sandboxing
T1190.Exploit Public-Facing Application	M1050.Exploit Protection
T1190.Exploit Public-Facing Application	M1030.Network Segmentation
T1190.Exploit Public-Facing Application	M1026.Privileged Account Management
T1190.Exploit Public-Facing Application	M1051.Update Software
T1190.Exploit Public-Facing Application	M1016.Vulnerability Scanning
T1566.Spearphishing Attachment	M1049.Antivirus/Antimalware
T1566.Spearphishing Attachment	M1031.Network Intrusion Prevention
T1566.Spearphishing Attachment	M1021.Restrict Web-Based Content
T1566.Spearphishing Attachment	M1017.User Training
Credential Access	
T1003.OS Credential Dumping	M1015.Active Directory Configuration
T1003.OS Credential Dumping	M1043.Credential Access Protection
T1003.OS Credential Dumping	M1041.Encrypt Sensitive Information
T1003.OS Credential Dumping	M1028.Operating System Configuration
T1003.OS Credential Dumping	M1027.Password Policies
T1003.OS Credential Dumping	M1026.Privileged Account Management
T1003.OS Credential Dumping	M1025.Privileged Process Integrity
T1003.OS Credential Dumping	M1017.User Training
T1110.Brute Force	M1036.Account Use Policies
T1110.Brute Force	M1032.Multi-factor Authentication
T1110.Brute Force	M1027.Password Policies
T1110.Brute Force	M1018.User Account Management
T1212.Exploitation for Credential Access	M1048.Application Isolation and Sandboxing
T1212.Exploitation for Credential Access	M1050.Exploit Protection
T1212.Exploitation for Credential Access	M1019.Threat Intelligence Program
T1212.Exploitation for Credential Access	M1051.Update Software

Tactics > Techniques	Mitigation(ID,Description)
Discovery	
T1046.Network Service Scanning	M1042.Disable or Remove Feature or Program
T1046.Network Service Scanning	M1031.Network Intrusion Prevention
T1046.Network Service Scanning	M1030.Network Segmentation
T1135.Network Share Discovery	M1028.Multi-factor Authentication
Lateral Movement	
T1021.Remote Services	M1032.Multi-factor Authentication
T1021.Remote Services	M1018.User Account Management
T1072.Software Deployment Tools	M1015.Active Directory Configuration
T1072.Software Deployment Tools	M1032.Multi-factor Authentication
T1072.Software Deployment Tools	M1030.Network Segmentation
T1072.Software Deployment Tools	M1027.Password Policies
T1072.Software Deployment Tools	M1026.Privileged Account Management
T1072.Software Deployment Tools	M1029.Remote Data Storage
T1072.Software Deployment Tools	M1051.Update Software
T1072.Software Deployment Tools	M1018.User Account Management
T1072.Software Deployment Tools	M1017.User Training
T1210.Exploitation of Remote Services	M1048.Application Isolation and Sandboxing
T1210.Exploitation of Remote Services	M1042.Disable or Remove Feature or Program
T1210.Exploitation of Remote Services	M1050.Exploit Protection
T1210.Exploitation of Remote Services	M1030.Network Segmentation
T1210.Exploitation of Remote Services	M1026.Privileged Account Management
T1210.Exploitation of Remote Services	M1019.Threat Intelligence Program
T1210.Exploitation of Remote Services	M1051.Update Software
T1210.Exploitation of Remote Services	M1016.Vulnerability Scanning
T1570.Lateral Tool Transfer	M1037.Filter Network Traffic
T1570.Lateral Tool Transfer	M1031.Network Intrusion Prevention
Impact	
T1486.Data Encrypted for Impact	M1053.Data Backup
T1529.System Shutdown/Reboot	None