Vol.2020-IOT-50 No.4
2020/7/10

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

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，効果的な対策を選定できることを目的とし，各種セキュリティガイドライン内で提言されている対策項目が，実際に発生したセキュリティインシデントの事例で有効であるかどうかの評価を行った．評価は，当該対策が施されていればセキュリティインシデント発生を防げていたかどうか，及び当該対策を施す難易度を踏まえて実施した．

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

Evaluate security countermeasure from security incident and security guidelines

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

Abstract: This research is for company who can't select and apply better security countermeasure because of expense.We picked up security countermeasures from security guideline and evaluate them with recent security incident.We also consider difficulty of each security countermeasures.

Keywords: Security Incident, Security countermeasure, Incident Response

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.

一方でセキュリティインシデントを防ぐための手順やガイドラインが国内外の様々な組織より情報公開されており，これらを各企業が適切に確認しセキュリティ対策に反映することができれば大規模なセキュリティ被害は防げると考えられる．しかしながら，実施すべき事項が多岐に渡っており，技術的な前提知識もある程度必要となる為，専任の担当者不在の状況で各種ガイドラインを読み解いてセキュリティ対策の選定と実装を行うコストをかけることが難しい組織が一定数以上存在するのではないかと考えた.

上記の背景を踏まえ，過去のセキュリティインシデント被害原因の技術的な共通項を整理し，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の効果を評価することで，様々な組織・企業において効果的なセキュリティ対策が明らかになると考えた.

(2) 概要

本研究では，2019 年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における，感染原因及び感染拡大原因を整理した．その後，整理した結果と，著名なセキュリティ対策に関するガイドラインにて提言されている技術的対策項目を照らし合わせ，昨今のセキュリティインシデントの防止に有効と思われるセキュリティ対策項目を洗い出した. なお，「セキュリティ対策」については組織としてのガイドラインやポリシーなどの整備や従業員の教育などの管理的対策は除く，技術的な対策に特化した.

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

(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 IT 管理者や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

・基本的なセキュリティ対策項目がセキュリティインシデント防止に効果が高いことを立証し，基本的対策の必要性が再認識され，各組織で促進される

(4) 先行研究

佐藤ら[3]は最適なセキュリティ対策の選定を行うために，組織内で起きた過去インシデントを整理し，損失額や発生原因から最適な対策を選定する手法を提案している．研究の目的は我々の研究と近しい一方で，対策選定までを 3 段階に分けており，1 段階目の組織内の過去インシデントの整理と原因分析にある程度の母数を確保する時間と，情報を整理する工数がかかる点と，2 段階目の対策項目と対策技術の選定は外部のセキュリティ専門家に意見を求める必要がある為，専任の IT 担当者が不在である場合や，セキュリティ専門家に相談をするコストを割けない組織においては実現が難しいと考えられる．

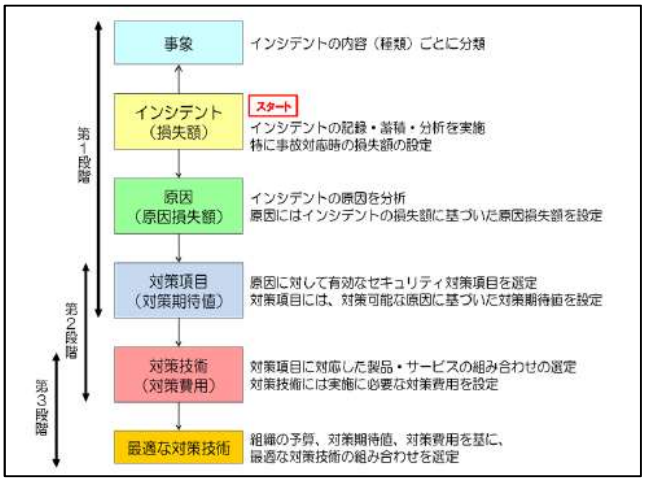

図 1 対策選定のステップ（[3]より引用）

柴田ら[4]は Attack Tree を用い，効果的なセキュリティ対策選定の為に，攻撃者視点での目的達成までの攻撃パスをツリーで整理し，ボトルネックとなるノードに対策を施すことを提案している．柴田らは「LAN 内の端末に侵入」「マルウェア感染」を最も対策すべきノードであるとしており，いずれのノードも我々の研究が提案対象としている範囲である．また，過去の実インシデント情報にて分析を実施した結果としては“最も大きなボトルネックとなった「LAN 内の端末に感染」ノードにおいては単一の対策により簡易に解決を示すことが出来なかった”としている．

我々の研究では，佐藤らの研究の前提条件であった組織内の過去インシデントの整理及び対策項目検討といったコストを省き，かつ柴田らによると単一の解決策提示が難しいとされた「LAN 内の端末感染」における技術的対策を提示する．

2. 提案

国内外の公的機関等において様々なセキュリティガイドラインが公開されているが，各ガイドライン内で提示されている対策の効果や重みは明確でないことが多く，各組織がリスクの分析等を行った上で，費用との兼ね合いで対策の手法と対策箇所を選別していく必要がある．

この「セキュリティ対策の重みづけ」について，直近で発生したセキュリティインシデント実例において，インシデント防止あるいは軽減に効果があったか，を評価することで行えないかと考えた．また，各セキュリティ対策が単一あるいは複数のガイドラインで提言されている対策であるかどうかと，運用コストを加味して整理することで，IT 担当者が組織内で効果的な対策を推進しやすくなるのではないかと考えた．

3. 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．

(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[5]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 1).

表 1　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)　手法詳細

以下の 4 段階にて対策の選別と評価を実施した.

1. 2019 年のインシデント情報の整理
2. セキュリティガイドラインの選定と確認
3. 技術的セキュリティ対策の抜き出し
4. セキュリティ対策の評価

3-1.2019 年のインシデント情報の整理

まず，2019 年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 9 件洗い出した（表 2）. 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.

表 2　2019 年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
i	不明	MS17-010	不明	SMB	不明	OSのパッチ適用をしていなかった

3-2.セキュリティガイドラインの選定と確認

次に，公開されている技術的なセキュリティ対策が記載されているガイドラインの内，著名であり，具体的なセキュリティ対策が記載された以下ア~オの 5 つのガイドライン及び文献を精査した.

ア:『高度標的型攻撃』対策に向けたシステム設計ガイド[6]
イ:中小企業のセキュリティ対策ガイドライン[7]
ウ:政府機関等の対策基準策定のためのガイドライン[8]
エ:CIS Controls[9]
オ:標的型攻撃セキュリティガイド[10]

3-3.技術的セキュリティ対策の抜き出し

選別した各種ガイドラインから，技術的なセキュリティ対策を 16 項目抜き出した(表 3). 別のガイドラインで近しい内容を提言しているものについては同一の対策として一項目に統一した．また，先述の通り「技術的なセキュリティ対策」が対象となる為，体制や手順・フローや教育といった管理的な対策や，ログの監視などの「検知」対策はこの段階で省いている.

表 3　ガイドラインから抜粋したセキュリティ対策一覧

No	対策項目	言及しているガイド					
		ア	イ	ウ	エ	オ	計
1	運用管理専用の端末設置とネットワーク分離	○					1
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）	○					1
3	認証プロキシ機能・サーバの導入	○					1
4	443ポート以外へのConnectメソッド通信の遮断	○					1
5	OS やソフトウェアを常に最新の状態にする		○	○	○		3
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		○	○	○		3
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		○	○			2
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			○	○	○	3
9	自動再生（オートラン）機能の無効化			○			1
10	OSの悪用防止機能(DEP,ASLR等)を有効にする				○		1
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				○		1
12	ワークステーション同士の通信を無効にする	○			○	○	3
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	○			○	○	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				○		1
15	ホスト型IPS(脆弱性検知機能)の導入					○	1
16	ソフトウェアの利用制限(Internet Exploler,Adobe,Java等)					○	1

3-4. セキュリティ対策の評価

インシデント一覧（表 2，a-i）について，各対策項目(表 3，No.1-16)が事前に行われていた場合に感染及び感染拡大が発生しなかったか, という観点で評価を実施した(表 4). 評価は，以下 A-C の 3 段階で，評価は著者自身を含む，セキュリティインシデント対応の経験が 3 年以上あるメンバ 3 名で実施した.

A:この対策があれば感染が起きなかった, あるいは感染台数を大幅に減らせた
B:感染活動の一部を止められた可能性がある
C:直接的な効果が見込めない, あるいは情報不足による判定不可

また，併せて同メンバにて，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. 端末の台数や種別，業務上の重要性など一様に運用コストの試算が難しい為，自動化が可能であれば L，手動対処が必要になる場合は M あるいは H といった評価基準とした.

H:頻繁に設定変更や対処，監視などの手動対処が必要
M:頻繁ではないが定期的な手動対処が必要
L:構築時に設定をすれば自動化可能で手動対処が不要

表 4　評価結果　一覧

No	対策項目	a	b	c	d	e	f	g	h	i	A	B	C	運用
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	L
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	L
3	認証プロキシ機能・サーバの導入	C	C	C	C	C	C	C	C	C	0	0	9	L
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	L
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	H
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	L
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	M
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	H
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	L
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	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	C	B	C	C	C	B	B	A	C	1	3	5	L
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	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	B	C	B	C	C	A	A	A	A	4	2	3	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	C	A	C	C	C	C	A	C	C	2	0	7	L
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	L
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	M

4. 評価結果

A 評価が多い技術的対策，つまり実施されていればインシデントそのものを起こさずに済むか大幅な感染台数減が見込めた対策は以下項目となる．評価の高い順に降順としている．

表 5　評価結果（A 評価 降順）

No	対策項目	a	b	c	d	e	f	g	h	i	A	B	C	運用
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	H
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	L
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	H
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	L
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	L

その内，以下 3 つの対策については運用コストも L であり，本研究の目的である「効果的なセキュリティ対策」に合致すると考えられる．

No12.ワークステーション同士の通信を無効にする
No 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
No 15.ホスト型 IPS(脆弱性検知機能)の導入

次に， B 評価が多い対策，つまり実施されていればインシデントの一部を止められた可能性のある対策は以下項目となる．評価の高い順に降順としている．

表 6 評価結果（B 評価 降順）

No	対策項目	a	b	c	d	e	f	g	h	i	A	B	C	運用
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	L
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	L
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	M
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	L

No 10.OS の悪用防止機能(DEP，ASLR 等)を有効にする
No6.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
No 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
No 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

5. 考察

(1) A 評価が多いが運用コストが高い対策の補足

以下 2 つの対策については運用コストが高いが，ホワイトリスティングに関しては重要サーバのみ，OS 最新化はクライアントのみといった実施対象の限定により運用コスト軽減が考えられる為，まずは対策箇所を絞った実施の検討を推奨する．

No8.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
No5.OS やソフトウェアを常に最新の状態にする

(2) 評価時の議論についての補足

セキュリティ対策の効果，及び運用コストについて評価を行った際，議論になったポイントについて記載する．意見が割れたものは無かったが，以下のような点が議論により調整された．

・No6 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　について，攻撃実行中に不正プログラムの駆除が行えたとしても，パターン対応が行われていない不正プログラムやツール群をリアルタイムに代替利用されたケースなどでは完全な防御策とならない点を加味し，一部における評価を A→B に変更した．

・No11 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　について，感染端末がそもそも外部からリモートログオン出来ることをユーザ及び管理者が把握できていなかった事案については義務付けても対策が漏れる可能性が考えられるため，リモートログインが起点となった事案の一部における評価を A→C に変更した．

・No14 許可されていない無線アクセスポイントへの接続制御について，一部のインシデントで感染起点を防御できるという観点で，本対策項目自体を新規に追加した．

(3) その他対策の補足

結論で触れられなかった対策について，今回 C 評価の数が少ない順にて以下表 1 表 7 に記載する．

表 7　評価結果（C 評価 昇順）

No	対策項目	事案(a-i)と評価(A-C) a	b	c	d	e	f	g	h	i	合計 A	B	C	運用
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	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	C	A	C	C	C	A	C	C	C	2	0	7	L
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	L
3	認証プロキシ機能・サーバの導入	C	C	C	C	C	C	C	C	C	0	0	9	L
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	L
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	L
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	M

No1.運用管理専用の端末設置とネットワーク分離

運用管理端末が起点となった一部のインシデントで効果が高かったと考えられた．

No14.許可されていない無線アクセスポイントへの接続制限

個人のポータブル Wi-Fi やスマートフォンのテザリング機能が起点となって感染したと思われるインシデントでは A 評価であるものの，それ以外は C 評価であった．

No2.管理者権限アカウントのキャッシュ禁止

脆弱性攻撃(MS17-010)の事案が多かったことや，そもそも管理者権限のパスワードが容易であったことから，キャッシュ禁止の有効性は評価が行えないケースがほとんどであった．脆弱性対策及びパッチ適用，パスワードの複雑性を満たしている組織で検討すべき対策と考えられる．

No3.認証プロキシ機能の導入

対策が提言された当時に比べプロキシ対応の不正プログラムを作成することが低コストかつ容易になっている点，及び各インシデントにおいて発見された不正プログラムのプロキシ対応有無確認が必要であるため低評価となった．

No4.443 ポート以外への Connect メソッド通信の遮断

評価対象としたインシデントにおいて当該の方法で疎通を行う不正プログラムが確認されていない為低評価となっている．

No9.自動再生（オートラン）機能の無効化

評価対象としたインシデントにおいて USB メモリやストレージデバイスを起点とした感染が 0 件であった為低評価となっている．

No16.ソフトウェアの利用制限

評価対象としたインシデントにおいて特定のクライアントアプリケーションの脆弱性を起点とした感染が 0 件であった為低評価となっている．

(4)　対策方法等についての補足

No12.ワークステーション（クライアント）同士の通信無効化についてはクライアント端末間での通信要件は多くないと考えられる点と，脆弱性による大規模な感染から，標的型攻撃による感染拡大まで防げる点を加味し，今回の対策の中で最も推奨できるものであると考える．一方で，クライアントからサーバへの不正通信は本設定では防御出来ない為，その点は考慮しておく必要がある．実施においては，Active Directory のグループポリシー機能を利用した管理者ログオンの禁止や，ワークステーション端末上のファイアウォール機能による IP 帯での遮断などが手法として考えられる．

No15.ホスト型 IPS については MS17-010 を利用した攻撃が未だ継続していることと，OS の脆弱性パッチ適用が行われていない対象インシデントが多かったこと，ゲートウェイに IPS が存在する組織は多いが端末間やホストに IPS を展開している組織が少ない為，評価が高い状況となった．運用コストは Low としているが，導入時の検証やライセンス費用等のコストが想定される為，後述する No3 にてクライアント OS のみのパッチ最新化などでの代用が望ましいと考える．

No6.ウイルス対策ソフトの定義ファイル最新化は攻撃の一部に定義ファイルで対応済みのツールが利用されることが多く，攻撃の一部あるいは全てを駆除できる可能性が高い為評価が上がっている．既に導入済みの組織が多いと思われる為，定義ファイルが最新になっているかの確認及び，最新になっていない場合にアラートが上がる仕組みなどを確認すればよいと考える．

No13.SMB プロトコルの通信見直しに関しては，クライアント間に関しては No12 で対策するとすれば，クライアントサーバ間の SMB 通信の見直しとなる．ファイルサーバや Active Directory サーバやバックアップ用サーバ等，SMB が必須となるサービスは多い為難易度が高いと考えられるが，段階的な仕様の確認と制御を推奨する．

No7.管理者アカウントのパスワード複雑性については，特に標的型攻撃では必要不可欠な対策となるが，今回の評価対象インシデントでは認証を必要としない脆弱性（MS17-010）による感染拡大事案が多かった為，B 評価が多い状況となっている．ドメイン及びローカルの管理者アカウントを洗い出し，複雑性を満たしておらず容易に変更可能なものから変更することと，定期的に見直されるよう手順やポリシーを整備することが望ましい．

No10.OS の悪用防止機能については，各インシデントで利用された不正プログラムやツールごとの検証が必要となる点と，具体的に差している機能は何なのか(例：Windows

Defender Credential Guard，Exploitation guard)等により評価が難しく，一様に B 評価となった．有効化出来るのであれば有効化することが望ましいと考える．

No11.リモートログインへの多要素認証に関しては，侵入元が外部公開されたリモートデスクトップ接続が原因であったものについては直接防御が可能であるため高評価となっている．一方で多要素認証を検討する前段階として，自組織が公開している IP アドレスやサービスを洗い出し整理することや，一要素目（パスワード）が初期値で運用されている等の状況を見直した上で検討することが望ましい．

6. おわりに

本研究では，著名な 5 つのセキュリティガイドラインから 16 件の技術的セキュリティ対策項目を抜き出し，2019 年に発生した 9 件のインシデント実例における対策の有効性評価を実施した．その結果，3 つの対策が「効果的かつ運用コストが低い対策」という結論が得られた．また，各ガイドラインから精査し抜き出した対策の一覧及び効果の重みづけは再利用が可能であると考える．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．

また，今後は評価対象となるインシデントを増やす，あるいはセキュリティ対策の網羅性や妥当性の担保の為に時間を費やすことで更なる改善を考えている．また，今後も攻撃手法やその傾向は変わっていくことが考えられる為，引き続き関連研究を継続する．

今後改善が可能な点：
・評価対象とするインシデントの数の増加
・評価元のガイドラインや対策項目の網羅性
・セキュリティ対策の運用負荷評価の妥当性
・セキュリティ対策の導入コスト

今後実施を検討する研究：
・標的型攻撃や Web 改ざん等，攻撃種別に特化した評価

謝辞

本研究のセキュリティ対策の評価及び運用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] 佐藤智裕，田中英彦，“インシデント情報を使用した最適なセキュリティ対策の選定” Vol.2015-CSEC-68 No.5，(2015/3/5)
[4] 柴田理洋，大久保隆夫，“Attack Tree を用いたクリティカルパス検出による効果的対策の提案”CSS2016，(2016/11)
[5] National Institute of Standards and Technology，“Cyber Security Framework 1.1”https://doi.org/10.6028/NIST.CSWP.04162018，(2018/4)
[6] 独立行政法人情報処理通信機構，“『高度標的型攻撃』対策に向けたシステム設計ガイド” https://www.ipa.go.jp/security/vuln/newattack.html，(2014/9/30)
[7] 独立行政法人情報処理通信機構，“中小企業のセキュリティ対策ガイドライン” https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html，(2019/12/19)
[8] 内閣サイバーセキュリティセンター，“政府機関等の対策基準策定のためのガイドライン” https://www.nisc.go.jp/active/general/pdf/guide30.pdf, (2018/7/25)
[9] Center For Internet Security，“CIS Controls” https://learn.cisecurity.org/control-download，(2018/3/19)
[10] 岩井博樹，“標的型攻撃セキュリティガイド”SoftBank Creative, 8-2.恒久対策 P307-P313，2013