Vol.2022-IOT-56 No.43
2022/3/8

中小企業における情報セキュリティ対策状況のインタビュー調査

田中啓介[†1] 古川佳和[†2] 野田幹稀[†2] 上原哲太郎[†3]

概要：昨今の企業や組織へのサイバー攻撃や情報漏洩に関する被害事例は枚挙に暇がない．今回，中小企業において情報セキュリティ専任担当者の有無や企業規模・業態によってセキュリティ対策状況や課題が異なっているか等の現状や傾向を把握する目的で，大阪商工会議所と合同で企業にインタビューを行った．その結果から中小企業のセキュリティ対策の現状と課題について整理，考察した．

キーワード：セキュリティ対策， 中小企業， 実態調査， インタビュー

Interview survey on the status of information security measures in small and medium-sized enterprises

KEISUKE TANAKA[†1] YOSHIKAZU FURUKAWA[†2]
MOTOKI NODA [†2] TETSUTARO UEHARA[†3]

Abstract: In recent years， there have been many cases of cyber-attacks and information leaks against enterprises and organizations． This time， we conducted interviews with small and medium-sized enterprises jointly with the Osaka Chamber of Commerce and Industry in order to understand the current status and trends of security measures and issues depending on the existence or non-existence of full-time information security personnel， the size of the enterprise and the type of business． Based on the results， the current status and issues of security measures for small and medium-sized enterprises are summarized and discussed.

Keywords: Security measures， SMEs， fact-finding survey， interviews

1. はじめに

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．情報処理推進機構(IPA)が国内の企業や個人から受け付けているコンピュータウイルスや不正アクセスの被害届出はいずれも 2019 年から比較して増加傾向にあるとされる[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，専任の情報システム管理者，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，86．2%の企業がセキュリティ対策に従事する人材が不足していると回答しているといった調査結果も存在する[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．

本研究では，複数の中小企業にインタビュー調査を実施し，中小企業の情報セキュリティに関する実態や課題を明らかにするとともに，専任の情報システム管理者の有無や企業の規模，業種などによってセキュリティ対策の状況や課題に差異があるかの調査を実施した．また，調査結果をもとに中小企業において情報セキュリティ対策レベルを向上していくことに繋がる考察を導き出した．本研究で目指す貢献は以下のとおりである．

- 中小企業の情報セキュリティ対策の実態や課題を本論文の読者が学習，理解出来る
- 企業が取り組むべき情報セキュリティ対策を考察することで，中小企業の情報システム管理者や情報セキュリティに関するサービス提供者が参考に出来る

本研究では 2021 年 11 月に中小企業 12 社へインタビュー調査を実施し，その結果整理・考察した．インタビュー対象の企業は 1 社を除き大阪商工会議所が提供している「サイバーセキュリティお助け隊」サービスを導入している大阪あるいは和歌山の企業であり，情報システム専任担当者有無・従業員数・業種に偏りの無いよう選定した．

†1 立命館大学 大学院 情報理工学研究科,トレンドマイクロ株式会社
†2 大阪商工会議所
†3 立命館大学 情報理工学部

2. 先行研究

経済産業省近畿経済産業局が実施した「関西におけるサイバーセキュリティ対策の実態把握」[3]では，関西の中小企業に対し 1522 件のアンケートを実施しており，24 の設問について回答を得ている．サイバーセキュリティ対策の取り組みや人材の状況についてバランスよく質問を行なっており，本調査結果により中小企業の実情をある程度理解することは可能だが，企業規模や担当者の有無などの属性によるセキュリティ対策状況の傾向などについては分析されておらず，またインタビューによる課題の深掘り等の質的な要素の調査については実施されていない．

高正らが実施した研究[4]では，北陸地域において，サイバー攻撃の対策状況と被害状況の分析を試みている．大学と地元の商工会議所が連携し，中小企業の安心感を得ながら調査を実施している点は我々の研究と実施形態や目的が近しく，無記名のアンケートにて 241 件の回答を得ており，またアンケート結果をもとに 2 社の企業に追加インタビューを行っている．対策項目はアンチウイルス，ファイアウォール，クラウド，ソフトウェア導入制限，セキュリティパッチの更新の５点に絞られており，分析結果についてはクラウド導入やソフトウェア導入制限は被害状況に対し負の係数となった，つまり効果があると考えられるとしている．一方で企業規模や業種，担当者有無と対策状況の関係性については考察されていない．

これらの先行研究を踏まえ当研究では，半構造化インタビュー調査によりセキュリティ対策状況と企業規模や担当者有無等の属性の傾向を分析し，提言に繋げる．

3. 調査詳細

3.1 リサーチクエスチョン

インタビュー調査を実施するにあたり，以下 4 点のリサーチクエスチョンを事前設定した．

Q1．専任の情報システム担当者がいる中小企業の方が，IT 担当者不在の企業に比べてセキュリティ対策の実施状況が優れているのではないか？(専任担当者の有無)

Q2．企業規模が大きいほどセキュリティ対策の実施状況が優れているのではないか？（企業規模の違い）

Q3．企業の業種とセキュリティ対策の実施状況に関連性があるのではないか？（業種の違い）

Q4．上記に関係なくセキュリティ対策の実施状況が優れている企業に特徴はあるか？（その他の傾向）

3.2 インタビュー手法詳細

インタビューは以下「表 1　インタビュー詳細」の通り実施した．

表 1　インタビュー詳細

項目	内容
実施時期	2021 年 11 月
対象企業数	12 社
企業規模	従業員数 10-200
インタビュー時間	1 時間
インタビュー方式	対面・半構造化インタビュー
インタビュー項目	12 項目

インタビューの前に，出来るだけ現状を正確に話してもらう為に，調査の目的やインタビュアーの自己紹介等を必ず行い，信頼関係の構築を試みた．また，インタビュアーと面識がないと警戒されてしまい本音を話してもらえない可能性を鑑み，必ずインタビュー対象の担当者と事前のやり取りや面識がある大阪商工会議所の共著者のいずれかがアポイントメントを取得した上で，当日もインタビュアーとして同席をしている．

対象企業は以下のような特徴・分布となっている．

[専任担当者]

あり	8 社
なし	4 社

[業種]

サービス業	1 社
卸売業	3 社
建設業	2 社
情報通信業	1 社
製造業	4 社
不動産業	1 社

[おおよその従業員数]

10 名	2 社
50 名	5 社
100 名	3 社
250 名	2 社

3.3 インタビュー項目

各企業において以下の 12 項目のインタビュー項目のヒアリングを実施した.

表 2　インタビュー項目一覧

No	カテゴリ	ヒアリング内容
1	現状の対策	全ての端末にウイルス対策ソフトはインストールされていますか
2		最新のセキュリティパッチやパターンファイルが適用されていますか
3		Webアクセス時のフィルタリングや通信先評価などは行われていますか
4		メールやメールの添付ファイルなどのセキュリティ対策は行っていますか
5	体制・リソース	インシデント発生時の手順・体制等は決まっていますか
6		セキュリティ上の規定はありますか？ある場合、周知されていますか
7		担当者を増やしてほしい、セキュリティ対策予算が欲しいと思うことはありますか
8	セキュリティに対する認識/今後の計画	日々の業務等の中でセキュリティに対して不安を感じることはあるでしょうか
9		現在足りていないと思うセキュリティ対策項目はあるでしょうか
10		今後検討したいセキュリティ製品や機能はあるでしょうか
11		こういうセキュリティ製品やサービスがあったらいい、というものはありますか
12		サイバーセキュリティ関連のニュースを見て自組織の対策を見直すことはありますか

インタビュー時には，単に項目の一覧を提示するのではなく，カテゴリごとに噛み砕いた説明を入れた手元資料を利用し，情報システム担当者でないインタビュー対象者においても理解しやすいように努めた．また，機械的にインタビュー項目を聞いていくのではなく，回答に対して本音や本質を聞き出せるような投げかけや，あえてインタビュー項目と脱線した話題についても会話を広げるといった半構造化のインタビューで，質的要素や本音が拾えるよう努めた．

図 1　インタビュー概要（インタビュー時の資料より）

4. 調査結果

4.1 結果

調査の結果概要をインタビュー項目の分類毎に以下より記載する．

[セキュリティ対策]

セキュリティ対策の実施有無という観点では No1, 3, 4 については実施率が 100%であった．No2 については 3 社のみ古い Windows7 が残存していたが，それ以外の端末は最新の状態を維持していた．

1	全ての端末にウイルス対策ソフトはインストールされていますか
・はい：12 社	
2	最新のセキュリティパッチやパターンファイルが適用されていますか
・はい：9 社　　いいえ：3 社（一部のみ未適用）	
3	Web アクセス時のフィルタリングや通信先評価などは行われていますか
・はい：12 社	
4	メールやメールの添付ファイルなどのセキュリティ対策は行っていますか
・はい：12 社	

[セキュリティ体制]

セキュリティインシデント発生時の手順や体制，またセキュリティに関する規定が存在する企業は非常に少なかった．しかしながら，規定はなくとも Web ニュース等で得られた情報を従業員に都度周知をしているといった企業が多数見受けられた．また，情報システムの担当者についてはあえて人数を増やしたり専任担当者を雇用したりしたいというよりは，企業の規模や売り上げ等を鑑みて増やすメリットが現時点では感じられない，といった回答が多く見受けられた．

5	インシデント発生時の手順・体制等は決まっていますか
・はい：3 社　　いいえ：9 社（うち作成中：1 社）	
6	セキュリティ上の規定はありますか？ある場合，周知されていますか
・はい：2 社　いいえ：10 社	
7	担当者を増やしてほしい，セキュリティ対策予算が欲しいと思うことはありますか
・はい：2 社　いいえ：10 社	

[セキュリティへの認識・今後の計画]

実際にセキュリティインシデントに遭遇したことがない企業においては，日々メールで受信している Emotet 等の脅威や，ニュースで見聞きする大手企業や同業のサイバー攻撃被害等で不安を感じていることが多く見受けられた．また，今後のセキュリティ対策強化の観点では，企業規模が大きくなるほど資産管理がアナログな手法では困難となり，資産管理ソフトウェア等を導入済み，あるいは導入を検討しているという傾向が見受けられた．

なお，本カテゴリの質問項目については定性的な回答や，一部近しい質問であるため重複した回答が多数存在したため，回答の合計が母数の 12 社となっていない項目がある．

8	日々の業務等の中でセキュリティに対して不安を感じることはあるでしょうか
・Emotet 等の不審メール：6 社 ・大手企業のサイバー攻撃被害ニュース：3 社 ・取引先企業のランサムウェア感染：1 社	
9	現在足りていないと思うセキュリティ対策項目はあるでしょうか
・モバイル端末のセキュリティ対策：4 社 ・資産，証跡管理製品：2 社 ・拠点へのセキュリティ対策（UTM 等）：2 社	
10	今後検討したいセキュリティ製品や機能はあるでしょうか
・標的型メール訓練の実施：3 社 ・共有フォルダの権限最小化：1 社 ・生体認証：1 社 ・メールの添付ファイルの検査：1 社 ・リモートワーク関連の強化：1 社	
11	こういうセキュリティ製品やサービスがあったらいい，というものはありますか
・BCP や復旧計画や手順作成等の支援：1 社 ・全体を見てアドバイスしてくれるサービス：2 社	
12	サイバーセキュリティ関連のニュースを見て自組織の対策を見直すことはありますか
・ない：5 社 ・ないが，社内周知に活用：6 社 ・見直したことがある：1 社	

次に，リサーチクエスチョンに対する回答の事前処理として，各企業の対策レベルをより実態に則して数値化するために，インタビュー時に深堀した質問やインタビュー項目以上に話が発展した内容なども含めて整理し，インタビュー項目よりも詳細なセキュリティ対策と，その対策を実施することで各企業において効果が見込めるかを「表 3　改善余地スコアの算出（対策例×ヒアリング結果）」にてマッピングした．各列の最下部の「改善余地スコア」が高い企業ほど改善の余地があり，各行の右端の合計値が高い対策は各企業において導入率が低い対策項目である．

表 3　改善余地スコアの算出（対策例×ヒアリング結果）

↓対策例 / ヒアリング企業→	1	2	3	4	5	6	7	8	9	10	11	12	計
ウイルス対策の設定・ログ集約	○	○	−	−	−	○	○	−	○	−	−	○	6
挙動検知系の対策機能	−	−	−	−	○	−	−	−	−	−	−	○	2
メール解析（スパム対策）	○	−	○	○	−	○	○	○	−	○	−	○	8
メール解析（サンドボックス）	○	○	○	○	○	○	○	○	○	○	○	○	12
Webアクセスの制御（本社）	−	−	−	−	−	−	−	−	−	−	−	−	0
Webアクセスの制御（拠点）	−	−	−	○	−	−	−	−	−	○	−	−	2
ID/Password管理 （AD）	○	○	−	○	○	○	○	○	○	−	○	○	10
資産管理の導入(Patch管理等)	○	○	−	○	○	○	○	○	○	−	○	○	10
改善余地スコア	5	4	2	5	4	5	5	4	4	3	3	6	

本表の説明や評価方法については Appendix1 に記載している．本表を元に，事前に設定したリサーチクエスチョンの回答を整理する．

Q1．専任の情報システム担当者がいる中小企業の方が，IT 担当者不在の企業に比べてセキュリティ対策の実施状況が優れているのではないか？(専任担当者の有無)

担当者が存在する企業は改善余地スコアが低い，つまり対策状況が優れている傾向が確認された.「表 4　担当者有無と改善余地の分析」において，担当者なしの社数は 4，改善余地スコア平均値は最右列の「4．8」 であるのに対し，担当者ありの企業は社数 8，改善余地スコア平均値は最右列の「3．9」であり，1 ポイント低い，つまり対策状況が優れているといえる．

表 4　担当者有無と改善余地の分析

担当者	社数	改善余地	改善余地/社数
あり	8	31	3．9
なし	4	19	4．8

Q2．企業規模が大きいほどセキュリティ対策の実施状況が優れているのではないか？（企業規模の違い）

企業規模が大きくなるほど，改善余地スコアが低い，つまり対策状況が優れている傾向が確認された.「表 5　企業規模と改善余地の分析」に記載の通り，企業規模が 10 名前後の企業が 2 社あり，最右列の改善余地スコアが「5．0」であるのに対し，最下行の企業規模 250 名前後の企業 2 社においては最右列の改善余地スコアが「3．5」であり，1．5 ポイントの差が確認された．

表 5　企業規模と改善余地の分析

企業規模	社数	改善余地	改善余地/社数
10	2	10	5．0
50	5	23	4．6
100	3	10	3．3
250	2	7	3．5

Q3．企業の業種とセキュリティ対策の実施状況に関連性があるのではないか？（業種の違い）

製造業については「表 6　業種と改善余地の分析」の通り母数が 4 社の中で改善余地スコア平均値が「3．0」と低い，つまり対策状況が優れている傾向が見られた．情報通信業，不動産業，建設業は，製造業やサービス業に比べ改善余地スコア平均値が「5．0」と高い，つまり対策に改善が必要

な状況に見受けられた.

表 6　業種と改善余地の分析

業種	社数	改善余地	改善余地/社数
製造業	4	12	3．0
サービス業	1	4	4．0
卸売業	3	14	4．7
建設業	2	10	5．0
情報通信業	1	5	5．0
不動産業	1	5	5．0

Q4. 上記に関係なくセキュリティ対策の実施状況が優れている企業に特徴はあるか？（その他の傾向）

まずは, Q3 までのリサーチクエスチョンで見えた傾向の中で，担当者が不在であるか，企業規模が小さい場合に改善余地スコアが高い，つまり対策状況に改善が必要な傾向が見受けられた．その為，逆に担当者が不在であるか，企業規模が小さいにも関わらず改善余地スコアが低い，つまり対策状況が優れている企業が存在するかを Q 4．1，Q4．2 として確認した．その後，最も改善余地スコアが低い，つまり対策状況が優れていた No3 の企業の特徴や傾向を Q4．3 として確認した.

Q4.1 専任の担当者が不在であるのに改善余地スコアが低い，つまり対策状況が優れている企業はあるか？

専任の担当者が不在の 4 社（企業 1，4，6，9）の内訳を確認すると，いずれも改善余地スコアは 5 あるいは 4 であった．改善余地スコアが 4 で比較的対策が優れている企業 No9 については，専任の担当者は不在であるものの，機器等の導入業社にセキュリティに詳しい担当者がおり，困った際などにいつでも相談が可能なようで，そういった点が対策状況に影響していると考えられる.

表 7　専任担当者不在企業の改善余地

企業	改善余地
1	5
4	5
6	5
9	4

Q4.2 企業規模が小さいにも関わらず改善余地スコアが低い，つまり対策状況が優れている企業はあるか？

従業員数が 10-50 名前後の企業の改善余地スコアは 6～4 であり，No2，5，9 の 3 社が改善余地スコア 4 と比較的優れている状況であった．それぞれの企業の対策が比較的優れている理由として考えられる点は以下のとおりである.

No2 の企業：専任の担当者がおり，かつ学生時に情報系の専攻をしていた関係で IT リテラシが高い. セキュリティ製品の選定においても，開発国や開発プログラム言語などにこだわっていた.
No5 の企業：前職でシステムエンジニアを経験している方が情報システム担当を兼任していた.
No9 の企業 : 先述の Q4．1 に記載の通り外部に相談可能な担当者が存在した.

表 8　企業規模と改善余地の一覧

企業規模-企業	改善余地スコア
10	
1	5
6	5
50	
2	4
5	4
7	5
9	4
12	6
100	
3	2
4	5
11	3
250	
8	4
10	3

Q4.3 最も改善余地スコアが低い, つまり対策状況が優れていた企業に特徴はあるか？

改善余地スコアが 2 で対策状況が最も優れていた No3 の企業は，製造業，従業員数が 100 名前後，専任の担当者が存在するという，本研究で導き出されたセキュリティ対策が優れている企業の傾向・条件を全て満たしている．更に加え，専任 1 名，兼任で経営層の担当者が 1 名という体制となっており，また今回 12 社の中で唯一，不正な機器接続を検知する装置を導入していた.

また，改善余地スコアが次点の 3 であった No10，11 の企業についても，No3 の企業と同様に，製造業，従業員数が 100 名から 250 名前後，専任の担当者がいるという条件を満たしている.

ここまでの Q 4.1，4.2，4.3 の確認結果より，Q4 のリサーチクエスチョン「セキュリティ対策の実施状況が優れている企業に特徴はあるか？」への回答は「担当者が前職経験や業種傾向等から IT スキルが高い場合に，セキュリティ対策状況にプラスに影響する」と言える．

4.2 考察：中小企業のセキュリティ強化に向けた課題

調査実施前には専任の情報システム担当者を求む声であったり，追加の人員をどうにか手配したいといった声が多くあることを想像していたが，実際にはどの企業においても，「担当者を増員することはもちろん望ましいが，企業の経営状況や予算などを鑑みるとこれ以上対策を強化したり人員を追加する必要性は感じていない」という冷静で地に足のついた回答がほとんどであった．

No1 の企業：
「企業の規模的に専任担当を置いたりすることは難しい．もちろん新入社員が入ってきて IT 担当を引き受けてくれたら嬉しい．ただ，企業規模が小さいからこそ，しっかり理解している担当者が 1 人でもいれば逆に目が届く範囲を管理できると考えている」

No5 の企業：
「会社の売り上げなど鑑みるとこれ以上費用をかけることは考えにくい」

また，今回のインタビュー対象企業においては，代表や本部長など経営層にかなり近い立ち位置で情報セキュリティの維持や強化を担当している方が半数程度存在した．また，企業規模が小規模である故に従業員の様子が見え，情報セキュリティの強化が会社経営や従業員，あるいは自分自身を守ることに直結することがイメージしやすいのではないかと感じた．つまり，担当者が必要と感じるセキュリティ機能さえあれば，導入を進言する役割とモチベーションを既に持っている状態の企業が多数見受けられた．

現に No5 の企業においては従業員 50 名以下の規模ながら兼務担当者の IT リテラシが非常に高く，UTM を活用して従業員のアクセス URL を原則許可制とする負荷の高い運用を行いつつ，感染しても影響のないスタンドアロン端末を各拠点に用意し，リスクのある行動を業務端末で行わないように誘導するといった施策等を推し進めていた．

No5 の企業：
セキュリティ人材として特化するのではなく，兼務であることで会社全体の状況や IT，セキュリティの必要性が分かり理解が早い．

その為，中小企業において更なるセキュリティ強化を行うためには，人員追加や予算追加ではなく，まず自組織のセキュリティ対策が十分であるか，足りない点が何であるかを客観的に可視化して担当者や経営層が理解できる状態にすること，そして更なるセキュリティ対策の必要性を担当者が強く感じられるようにすることが，解決すべき課題であると考える．

No9 の企業においては，サイバーセキュリティお助け隊の UTM を無料の評価期間に試用し不正通信が可視化されたことで，経営層に必要性を訴えることが出来たとのことであった．

No9 の企業：
「最初無料で使えて可視化できて，効果が目に見えていた中で，かつ本導入のときも，かなり安く買えたのが採用の決め手となった」

また，アセスメントサービス等で自社に必要な対策は何であるかの提案や，対策状況が十分であるかを評価して欲しいといった声も聞かれた．これらの企業も，自社が実施すべき対策項目が明確になり，その必要性さえ理解出来れば，すぐにでも対策を実施したいといった気概を感じた．

No1 の企業：
「状況をアセスメントしてすぐ実施できる対策を提案してくれるようなサービスがあれば利用したい」

No3 の企業：
「何がいいのか，全体を見てアドバイスをくれるサービスや，全てをお任せできるようなサービスが欲しい」

5. 今後の課題

今後のインタビュー調査について，対象地域の拡大や対象社数を単純に増やすことも当初視野に入っていたが，今回のインタビューで当初設定していたリサーチクエスチョンに対する解が得られ，この結果はインタビュー規模を拡大したとしても大きく変わらないと予想している．一方，インタビュー対象企業が大阪商工会議所のサイバーセキュリティお助け隊サービス及び UTM 機器を導入企業であった点は，通常の中小企業よりセキュリティに対する意識が高い母集団であると考えられ，偏りがあったと考える．また，OS やセキュリティソフトウェアの設定値等の技術的に詳細な項目については口頭のインタビューのみでは把握が困難であった．その為，今後の研究では以下のいずれかあるいは両方を継続して進める．

1．インタビュー対象や詳細レベルの変更
・サイバーセキュリティお助け隊サービス未導入企業への追加インタビューや，OS やセキュリティソフトウェアの設定値等，技術的に詳細なインタビューの検討

2. 具体的な脅威の可視化手法や対策手法の検討
・OS やソフトウェアの設定値等のリスクや, 外部からの脅威を可視化する手法，あるいは具体的な対策手法の提言や実証

6. 結論

本研究では，12 社の中小企業にインタビューを実施し，中小企業の情報セキュリティ対策についての実情と課題を整理した．調査の結果，情報セキュリティ対策の実施状況は企業の規模が大きい，あるいは専任担当者が存在する場合，または業種が製造業である場合等に対策実施状況が優れていることが分かった．また，担当者が過去の職務経験や学習経験から IT リテラシが高い場合や, 外部に相談可能な専門人材が存在する場合には，企業の規模や専任担当者有無に関わらずセキュリティ対策状況が優れていることが分かった．今後更に中小企業がセキュリティ対策を進めていくにあたっては，自組織のセキュリティ対策状況が十分であるかどうかを安価に可視化し，足りない点にどういった機能や対策が必要であるかをわかりやすく提言するような仕組みやサービスが必要であると考える．本研究が，中小企業の情報システム管理者やセキュリティサービス提供事業者の今後のより良いサービス検討や提供の一助となることを期待する．

謝辞

本研究は，研究の目的に賛同いただき，インタビューに協力いただいた企業の皆様なくしては実現しておりません．年末の多忙な時期にインタビューに時間を割き，現状をありのままに回答いただいた企業の皆様に，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 2021” https://www．ipa．go．jp/files/000094186．pdf, (2021/7/30).
[2] NRI Secure，“NRI Secure Insight 2020” https://www．nri-secure．co．jp/hubfs/NRIS/download/pdf/NRISecure_Insight2020_Report．pdf， (2020/12/15)
[3] 経済産業省近畿経済産業局，“「令和 2 年度中小企業サイバーセキュリティ対策促進事業 （関西サイバーセキュリティ促進強化事業)」 関西におけるサイバーセキュリティ対策の実態把握（アンケート調査結果）” https://www．kansai．meti．go．jp/2-7it/k-cybersecurity-network/210317press_report2．pdf， (2021/03/17)
[4] 高正智，岡田政則， “北陸地域の企業・団体等における情報セキュリティ管理”，情報処理学会第 81 回全国大会，(2019/3/14)

Appendix1．改善余地スコアの算出

↓対策例 / ヒアリング企業→	1	2	3	4	5	6	7	8	9	10	11	12	計
ウイルス対策の設定・ログ集約	○	○	―	―	―	○	○	―	○	―	―	○	6
挙動検知系の対策機能	―	―	―	―	○	―	―	―	―	―	―	○	2
メール解析（スパム対策）	○	―	○	○	―	○	○	○	―	○	―	○	8
メール解析（サンドボックス）	○	○	○	○	○	○	○	○	○	○	○	○	12
Webアクセスの制御（本社）	―	―	―	―	―	―	―	―	―	―	―	―	0
Webアクセスの制御（拠点）	―	―	―	○	―	―	―	―	―	○	―	―	2
ID/Password管理 （AD）	○	○	―	○	○	○	○	○	○	―	○	○	10
資産管理の導入(Patch管理等)	○	○	―	○	○	○	○	○	○	―	○	○	10
改善余地スコア	5	4	2	5	4	5	5	4	4	3	3	6	

[各項目の解説]
ヒアリング企業(列)：12 社各社の対策状況を評価
対策例(行)：セキュリティ対策
計（最右列）：数値が高いほど各企業に有効な対策
改善余地スコア（最下行）：各企業の改善余地．低いほどセキュリティ対策が優れており，高いほど追加のセキュリティ対策が必要
○：その対策を実施する余地がある
―：対策実施済み

[対策の解説]
ウイルス対策の設定・ログ集約：法人向け製品を利用している場合は実施済み(―)と評価
挙動検知系の対策機能：利用ソフトウェアの初期設定値を確認し，初期設定値より変更がないものと判断し評価
メール解析（スパム対策）：メールのホスティングサービスを利用しておりサービス内でスパム評価を行っている企業を実施済み(―)と評価
メール解析（サンドボックス）：サンドボックスによる添付ファイル解析を行っているかどうかを評価
Web アクセスの制御（本社）/（拠点）：UTM やアプリケーションで Web アクセスを制御しているかを評価
ID/Password 管理（AD）：Active Directory 等により ID やパスワードを一元管理している企業を実施済み(―)と評価
資産管理の導入（Patch 管理等）：端末にインストールする資産管理ソフトウェアを利用しているか企業を実施済み(―)と評価