

中小企業向けサイバーセキュリティ事後対応支援実証事業

(地域名:石川県、富山県、福井県)

成果報告書

請負事業者:株式会社PFU

内容

1	お助け隊実証事業の全体概要	4
(ア)	実証地域	4
(イ)	実証地域の選定	4
(ウ)	参加企業数	4
(エ)	実施スケジュール	5
2	事業説明会の開催	6
(ア)	集客方法	6
①	計画時の集客方法	6
②	集客施策	7
③	集客活動の課題	8
④	実証対象地域を拡大して集客を促進	8
⑤	地域拡大における集客方法	8
⑥	事業説明会開催結果	11
(イ)	集客結果	13
①	集客施策タイプ別の効果	13
②	県別の集計	13
③	業種別の集計	13
④	規模別の集計	14
⑤	監視対象への参加・不参加の理由	14
⑥	本事業の対象外企業からの参加依頼の対応	17
(ウ)	中間報告会の概要	18
①	各県ごとの参加企業数	18
②	報告会の開催概要	18
③	アンケート項目	18
(エ)	最終成果報告会の概要	19
①	各県ごとの参加企業数	19
②	報告会の開催概要	19
③	アンケート項目	20
3	中小企業の実態把握	20
(ア)	実態把握の方法	20
(イ)	当社採用のエンドポイント型の脅威検知位置 (UTM との違い)	21
(ウ)	セキュリティ意識調査アンケート	22
①	集計対象の母数	22
②	診断結果の傾向	23
(エ)	ベンチマーク診断 (IPA 自社診断シート)	41
①	診断結果の傾向	41
②	個社毎の指導 (報告書送付)	50
③	SECURITY ACTION 取得状況の結果	51
(オ)	公開サイト上の脆弱性診断による状況把握	52

①	レンタルサーバの脆弱性適用の責任範囲	52
②	実施状況	52
③	検出された脅威と傾向	53
④	多く検知されている問題の周知	53
⑤	参加企業の対応結果	54
(カ)	パソコン上の脆弱性監視ツールによる状況把握	55
①	サポート切れ / サポート切れ間近な OS の利用率	55
②	Windows10 でもサポート切れがあることの周知	56
③	脆弱性更新の適用状況 (Windows Update で対応可能なもの)	56
④	脆弱性更新の適用状況 (Windows Update で対応不可能なもの)	57
⑤	業種・従業員数別の脆弱性未対処 (放置) 状況	57
(キ)	パソコン上のセキュリティソフトの導入状況	58
(ク)	パソコン上の脅威検知ツールによる状況把握	59
①	脅威の検知位置について (既存対策をすり抜けた脅威)	59
②	検出された脅威について	60
③	駆け付け対応支援	61
4	中小企業向けサイバーセキュリティ事後対応支援体制の構築	62
(ア)	機能ごとの体制構築	62
①	相談窓口体制	62
②	パソコンの脆弱性検知と報告	62
③	パソコンの脅威検知と報告	62
④	駆け付け対応支援 (インシデント初動対応)	62
⑤	公開サイトの脆弱性診断と報告	63
⑥	その他 (契約からサービス開始までの事務局体制)	63
⑦	その他 (インストールモジュール作成と送付の事務局体制)	63
(イ)	運用フローの構築	64
5	地域実証の実施	65
(ア)	契約からサービス開始までの流れ	65
(イ)	運営で得られた課題	65
①	契約からサービス開始の課題	65
②	インストールモジュール作成時と送付時の課題	66
③	インストールモジュール導入時の課題	66
④	相談窓口の課題	67
⑤	公開サイトの脆弱性報告の課題	71
⑥	パソコンの脆弱性報告の課題	71
⑦	パソコンの脅威報告の課題	72
⑧	駆け付け対応支援 (インシデント初動対応) の課題	72
(ウ)	顧客担当者または公開サーバの委託先保守業者のスキルレベル	73
①	対応スキルは仮説どおりか	73
②	脆弱性情報を通知する粒度はスキルレベルに見合っているか	73
(エ)	サービス実施中の注意喚起	74

(オ)	サービス満足度と不満点	75
①	公開サイトの脆弱性診断	75
②	パソコンの脆弱性検知	76
③	駆け付けサービス	76
④	本事業に参加して良かったこと	77
⑤	本事業で改善すべきこと	78
⑥	今後の有償サービスに向けて期待すること	79
⑦	今後の有償サービスに向けて改善すべきこと	80
6	実証結果を踏まえた検討の実施	81
(ア)	中小企業のサイバーセキュリティ対策が進まない要因分析	81
(イ)	中小企業へのサイバーセキュリティサービスの検討（事後対応支援）	82
(ウ)	提供サービス（事後対応支援）	84
(エ)	機能毎の体制	85
①	相談窓口体制	85
②	パソコンの脆弱性検知と報告	85
③	パソコンの脅威検知と報告	85
④	駆け付け対応支援（インシデント初動対応）	86
⑤	公開サイトの脆弱性診断と報告	86
⑥	その他（契約からサービス開始までの事務局体制）	86
⑦	その他（インストールモジュール作成と送付の事務局体制）	86
(オ)	顧客が委託する公開サーバ保守業者のスキルレベル	87
(カ)	IT シルバー人材センターのスキル調査	87
①	必要スキルを有する人材有無、対象となる人数の確認結果	87
②	サービス価格を抑える対策として効果	88
(キ)	前提とするセキュリティ対策の適用増加とサービス価格の検討	88
①	企業規模、業種ごとの地域実証期間の対策の進捗と、企業からのコール数が減少する仮説	88
②	前提とするセキュリティ対策状況が進むことでコール数の減少する仮説が正しいか（サービス側の対応人数は現状で可能か）	88
(ク)	中小企業向けのサイバー保険検討	89
①	中小企業におけるセキュリティ投資金額に見合った対策と保険価格	89
②	サービスの加入条件、実施条件、免責事項	90
③	サイバー保険がカバーすべき内容	91
④	サイバー保険を付帯したセキュリティ対策サービスの商品案	92
(ケ)	全国展開	93
①	各地域に必要な体制と規模間（人数）を決める指標	93
②	各地域の体制構築に向けた必要なスキルの育成を行う教育内容と教育計画	93

1 お助け隊実証事業の全体概要

(ア) 実証地域

石川県、富山県(※)、福井県(※)

本実証地域においては、株式会社 PFU（以下「PFU」）という。）が請負事業として実施した。

※当初、実証地域を石川県のみとしていたが、早期の目標達成、効果的な実証実現に向けて、後に富山県、福井県に対象地域を拡大している。

(イ) 実証地域の選定

【選定理由】 石川県の産業構造の特徴

- 製造業が占める割合が 20%と多い、これは全国平均の 10%より高い数値
- 製造業は、生産用機械製造業、電子部品・デバイス・電子回路製造業が多い

【石川県の中小企業】

中小企業数： **40,430** 社

20 人以下の小規模除く企業数 **5,398** 社

(ウ) 参加企業数

120 社の実証事業参加申し込みを得てアンケートによる実態把握を実施。このうち、ツールを導入した監視サービス実施企業は 97 社。また、監視サービスを始めることができなかった監視サービス辞退企業数 23 社からは不参加理由を収集し、「2 (イ)⑤監視対象への参加・不参加の理由」に記載。

表 1-1. 実証事業参加状況

実証事業参加状況	活動成果	社数
実証事業参加企業数	実態把握	120 社
監視サービス辞退企業数（不参加理由の収集）	実態把握	23 社
監視サービス実施企業数（実機調査による）	実態把握	97 社

(エ) 実施スケジュール

実証実施期間：

2019年7月26日～2020年2月14日

うち監視・駆け付け対応（事後対応支援）期間：

2019年8月1日～2020年1月31日

表 1-2. 実施スケジュール

	7月	8月	9月	10月	11月	12月	1月
事業説明会の開催	1回	3回	1回	3回	2回		
・石川県 5回	1回	3回	1回				
・富山県 3回				2回	1回		
・福井県 2回				1回	1回		
中小企業の実態把握							
・意識調査	●————— 1回目					●—————	2回目
・ベンチマーク診断	●—————▶						
監視・駆け付け対応							
・コールセンター		●—————▶					
・パソコン脅威検知		●—————▶					
・パソコン脆弱性監視		●—————▶					
・駆け付け対応支援		●—————▶					
・公開サーバ診断		●—————▶					
中間報告会							
・3県各1回開催					3県 各1回		
成果報告会							
・3県各1回開催							3県 各1回

2 事業説明会の開催

事業説明会、中間報告会、および最終成果報告会の開催内容を説明する。

(ア) 集客方法

実証参加企業 100 社に向け、下記の集客活動を実施した。

① 計画時の集客方法

石川県を対象として、各市町の産業政策、商業振興系課、産官学連携部署にサイバーセキュリティ対策の必要性を説明して協力体制を構築、直接企業に働きかけてもらうための行政との協力体制を築く。

(活動地域：金沢市、小松市、加賀市、能美市、野々市市、白山市、輪島市)

また、以下の地域コミュニティ、および業界団体への声かけを行う。

- 一般社団法人コード・フォー・カナザワ
(地域課題を IT で解決する取組み)
- 地域財界のコミュニティ
- 各業界団体への声かけ
 - ・石川県情報システム工業会
 - ・石川県鉄工機電協会
 - ・石川県経営者協会
 - ・北陸経済連合会
- 損害保険ジャパン日本興亜株式会社 金沢支店との連携活動
(本実証事業の協力損保会社。以下「損保ジャパン」という。)

集客にあたっては、石川県地域における IT 活用を中心とした地域振興を推進するアイパブリッシング株式会社 (以下「アイパブリッシング」) という。) との連携により活動を行う。

事業説明会を石川県内で 4 回開催する。

② 集客施策

広く周知することで効果的に事業説明会に参加企業を誘導できると考え、以下の行政、団体への働きかけを中心とした周知活動を実施。

表 2-1. 石川県における集客活動施策一覧

施策種別	協力/連携先	備考
メディア	株式会社北國新聞社	記事掲載
メディア	日本経済新聞社 金沢支局	北陸版 記事掲載
メディア	日刊工業新聞社 金沢支局	記事掲載
行政、団体への働きかけ	国立研究開発法人 情報通信研究機構	
行政、団体への働きかけ	中部経済産業局	石川県及び関連機関へ連携
行政、団体への働きかけ	独立行政法人中小企業基盤整備機構	
行政、団体への働きかけ	石川県	
行政、団体への働きかけ	総務省 北陸総合通信局	
行政、団体への働きかけ	石川県商工会議所連合会	
行政、団体への働きかけ	石川県鉄工機電協会	PFU 加盟団体
行政、団体への働きかけ	石川県産業創出支援機構 (ISICO)	PFU 加盟団体
行政、団体への働きかけ	石川県繊維協会	
行政、団体への働きかけ	石川県食品協会	
行政、団体への働きかけ	北陸経済連合会	
行政、団体への働きかけ	JAIST MatchingHUB 事務局	
行政、団体への働きかけ	金沢:中央会若手 G	
行政、団体への働きかけ	金沢:若手経営者会	
行政、団体への働きかけ	金沢:IT ビジネスプラザ武蔵	
行政、団体への働きかけ	金沢:石川県情報システム工業会 (ISA)	PFU 加盟団体
行政、団体への働きかけ	金沢:石川県中小企業団体中央会	
行政、団体への働きかけ	金沢:野々市商工会	
行政、団体への働きかけ	金沢:金沢市商業振興課	
行政、団体への働きかけ	金沢:金沢商工会議所	
行政、団体への働きかけ	金沢:白山市商工会	
行政、団体への働きかけ	金沢:かほく市商工会	
行政、団体への働きかけ	金沢:津端町商工会	
行政、団体への働きかけ	金沢:内灘町商工会	
行政、団体への働きかけ	金沢:石川県警	
行政、団体への働きかけ	加賀:JAIST 産学連携センター	
行政、団体への働きかけ	加賀:小松商工会議所	
行政、団体への働きかけ	加賀:地場運輸会社	
行政、団体への働きかけ	能登:七尾まちづくりセンター	
行政、団体への働きかけ	能登:能登鹿北商工会	

施策種別	協力/連携先	備考
行政、団体への働きかけ	能登: 地方信金	
行政、団体への働きかけ	能登:七尾市商工観光課	
行政、団体への働きかけ	能登:七尾商工会議所ななお経営支援センター	
行政、団体への働きかけ	能登:地方銀行	
行政、団体への働きかけ	能登:宝達志水商工会	
行政、団体への働きかけ	能登:和倉温泉旅館協同組合	
本事業請負会社の関係先※	PFU の関係先	
本事業請負会社の関係先※	個社アプローチ (9 社)	

※ PFU、損保ジャパン、アイパブリッシング

③ 集客活動の課題

数多くの企業が目に触れるメディア掲載や行政・団体からのメルマガ・Web 掲載では計画より 1 回多い計 5 回の事業説明会を開催したが 52 社の実証参加申込数に留まり目標には届かなかった。

メルマガや Web 掲載から誘導する方法は効率的ではあるが確実性には乏しいことが結果に現れた。また、対面で説明する機会を得ても、当時はその場で事業参加の誘導をせず、事業説明会に誘導する運営方法であったため機会を逃すことにもなっていたと分析している。

表 2-2. 石川県における事業説明会の集客状況及び実証参加申込数

開催日	開催場所	説明会参加数	実証参加申込数
7/26	金沢市	22 社	9 社
8/28	七尾市	7 社	1 社
8/29	能美市	30 社	16 社
8/30	金沢市	48 社	21 社
9/25	金沢市	6 社	5 社
	計	113 社	52 社

④ 実証対象地域を拡大して集客を促進

石川県で、県内の各業界団体・各商工会・各コミュニティの協力を得て集客を図ったが目標の半数程度の 47 社（実証参加申込 52 社から辞退 5 社）となった。参加企業を増加させる必要性から富山県、福井県に実証対象地域を拡大した。

⑤ 地域拡大における集客方法

新規対応エリアの富山県・福井県については、行政・団体への働きかけから事業説明会へ誘導する方法により、意識の高い顧客を短期間でまとめて集客する方法を実施。加えて、集客効果が高いと考えサプライチェーン上位企業への働きかけ（石川県を含む）を施策として取り入れた。さらに対面説明による直接勧誘をするため、地域に顧客を多く持つ地域販社との連携や PFU の関係先企業への個別アプローチ

を実施した。

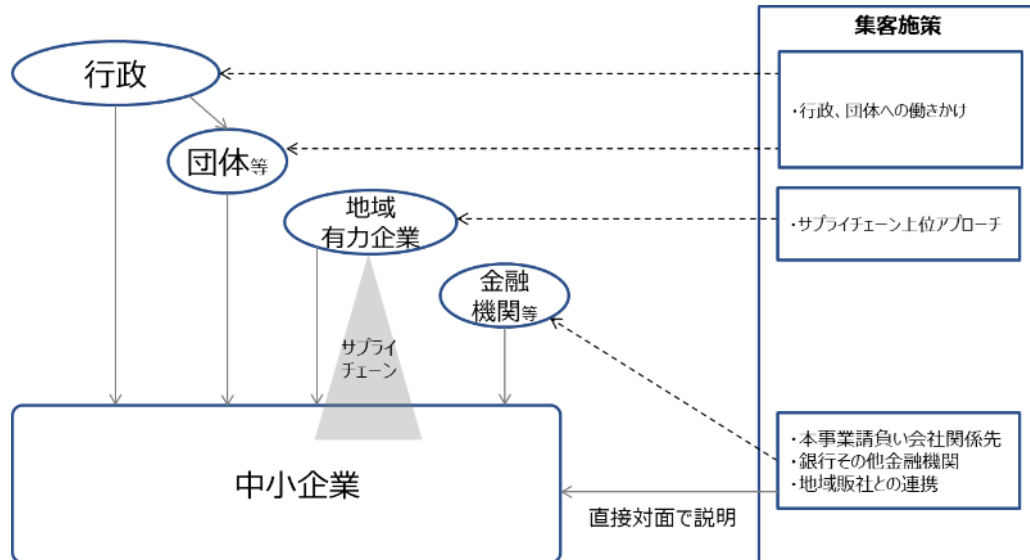


図 2-1. 集客方法の概要図

表 2-3. 地域拡大における集客活動施策一覧

施策種別	協力/連携先	集客ターゲット
行政、団体への働きかけ	(一社) 石川県情報システム工業会	再アプローチ（直接対話による紹介機会獲得のため） 会員顧客のうち、協力をしてくれそうな企業 16社
行政、団体への働きかけ	富山県商工労働部	富山県IoT推進コンソーシアム
行政、団体への働きかけ	富山県中小企業団体中央会	富山県精密機械工業協同組合 富山県金型協同組合 富山県生コンクリート工業組合 婦中鉄工業団地協同組合 滑川工業団地協同組合 協同組合福岡金属工業団地 富山企業団地協同組合 高岡銅器団地協同組合 大門企業団地協同組合 協同組合とやまオムニパーク 協同組合高岡食品業務団地 富山市ホテル旅館事業協同組合 富山県情報ネットワーク事業協同組合
行政、団体への働きかけ	富山商工会議所	富山商工会議所会員
行政、団体への働きかけ	高岡商工会議所	高岡商工会議所メルマガ登録会員
行政、団体への働きかけ	富山県食品産業協会	会員
行政、団体への働きかけ	公益財団法人富山県新世紀産業機構	
行政、団体への働きかけ	経済産業省 中部経済産業局 電力・ガス事業北陸支局	(一社) 富山県機電工業会 (一社) 富山県葉業連合会 (一社) 富山県情報産業協会 富山県プラスチック工業会 (一社) 富山県繊維協会 富山県中小企業団体中央会

施策種別	協力/連携先	集客ターゲット
行政、団体への働きかけ	経済産業省 中部経済産業局 電力・ガス事業北陸支局	(一社) 富山県葉業連合会 (一社) 富山県情報産業協会 富山県プラスチック工業会 (一社) 富山県繊維協会
行政、団体への働きかけ	福井県 産業労働部 新産業創出課	福井県 IoT 推進ラボ ・福井県情報産業協会 ・福井県機械工業青年会 ・(一社)福井県眼鏡協会
行政、団体への働きかけ	福井県 産業労働部 新産業創出課	福井県工業技術センター
行政、団体への働きかけ	福井県繊維協会	福井県織物工業組合 一般社団法人福井県染色同業会 一般社団法人福井県繊維卸商協会 福井県ニット工業組合 福井県撚糸工業組合 福井県繊維産元協同組合 福井県編レース工業組合
行政、団体への働きかけ	総務省 北陸総合通信局	ふくい産業支援センター
行政、団体への働きかけ	協力) IPA 経由近畿経済産業局	福井情報システム工業会
行政、団体への働きかけ	協力) IPA 経由近畿経済産業局	福井管内の商工会議所
行政、団体への働きかけ	協力) IPA 経由近畿経済産業局	近畿局管内情報関連団体
行政、団体への働きかけ	協力) IPA 経由近畿経済産業局	近畿局メルマガ
行政、団体への働きかけ	協力) 経産省 商務情報政策局	地域未来牽引企業への周知
地域販社との連携	地域販社 A 社	A 社の顧客 ターゲット 15 社
地域販社との連携	地域販社 B 社	B 社の顧客 ターゲット 10 社
本事業請負会社の関係先 ※	PFU 加入団体及び PFU グループ関係先	関係先企業への働きかけ
本事業請負会社の関係先 ※	保険会社	保険会社の代理店 (福井、富山) 保険会社の既加入者 銀行その他金融機関 福井県保険代理業協同組合青年部、等
サプライチェーン上位へのアプローチ	協力) 経産省 商務情報政策局	サプライチェーン上位企業 17 社

※PFU、損保ジャパン、アイパブリッシング

⑥ 事業説明会開催結果

事業説明会は下記の内容で開催した。

表 2-4. 事業説明会の開催内容

時間	内容	講演者
5分	ご挨拶、趣旨説明	PFU
20分	中小企業におけるサイバーセキュリティ対策普及に向けた国等の支援事業について	金沢市1回目：IPA 福井市1回目：IPA その他：PFU
40分	身近に迫っているサイバーセキュリティ脅威と対策の必要性 ・世の中の動向 ・攻撃と被害の実演デモで体感	金沢市1回目：JAIST 能美市：JAIST その他：PFU
40分	本事業について ・本事業の目的 ・本事業の説明 ・参加メリットの説明 ・参加申し込み方法 ※当日の配布資料を別紙添付	PFU
15分	意識調査アンケート、事業説明会アンケート兼参加申込書 ※当日の配布資料を別紙添付	PFU

石川県、富山県、福井県で実施した事業説明会全数の結果をまとめる。

表 2-5. 事業説明会参加企業の県別企業数

開催日	開催場所	説明会参加数	実証参加申込数
7/26	金沢市	22 社	9 社
8/28	七尾市	7 社	1 社
8/29	能美市	30 社	16 社
8/30	金沢市	48 社	21 社
9/25	金沢市	6 社	5 社
10/8	福井市	7 社	4 社
10/10	高岡市	6 社	4 社
10/11	富山市	24 社	17 社
11/7	富山市	5 社	1 社
11/8	福井市	7 社	5 社
	計	① 162 社	② 83 社

事業説明会参加企業が実証参加を申し込む確率は 51% (②÷①) であった。行政、団体への働きかけを中心とし、メルマガ、Web 掲載、チラシ配布等の方法で集客する事業説明会だけでは目標 100 社達成は難しかった。他の施策、サプライチェーン上位へのアプローチ、地域販社との連携など他の施策も必要である。

上記の事業説明会による集合説明会に加え、地域販社の協力を得て個社訪問活動したこと等により、最終的に **223 社への声掛け**となり、実証参加申し込み 120 社、そのうち監視サービス実施企業 **97 社の参加申し込み**を得た。

(イ) 集客結果

① 集客施策タイプ別の効果

表 2-6. 集客施策別の実証参加申込数、および監視サービス実施企業数

集客施策	実証参加社数	監視サービス 実施企業数
本事業請負会社の関係先 ※	28	22
行政、団体への働きかけ	22	16
地域販社との連携による集客	20	17
サプライチェーン上位へのアプローチ	13	6
IPA ウェブサイト	5	4
PFU ウェブサイト	2	2
実証参加企業からの紹介	2	2
不明	28	28
合計	120	97

※PFU、損保ジャパン、アイパブリッシング

② 県別の集計

表 2-7. 監視サービス実施企業の県別企業数

所在地	社数
石川県	68
富山県	20
福井県	9

③ 業種別の集計

表 2-8. 監視サービス実施企業の業種別の割合

業種別	参加割合
製造業	60%
卸売業・小売業	14%
学術研究・専門・技術サービス業	5%
建設業	5%
サービス業（その他）	5%
情報通信業	4%
金融業・保険業	3%
運輸業・郵便業	1%
複合サービス事業	1%
電気工事	1%
宿泊業・飲食業	1%

④ 規模別の集計

表 2-9. 監視サービス実施企業の規模別の割合

従業員数	参加割合
1~5	12%
6~10	6%
11~20	9%
21~50	20%
51~100	16%
101~200	20%
201~300	10%
301~500	5%
501~900	2%

⑤ 監視対象への参加・不参加の理由

中間報告会、最終報告会のアンケート結果を集計した。また、不参加企業においては、電話ヒアリングの結果も加味して下記に集約した。

【参加理由】

● 参加の動機

- ◇ 社内セキュリティ規約を立案しようとしていたタイミングで、事業を知ったから
- ◇ 興味を感じたから
- ◇ 今後サイバー保険を扱うため
- ◇ 石川県庁からのお誘い
- ◇ 当社で対応できない事に対して対応してほしい
- ◇ サイバー攻撃が増え、被害が起こりそうのため
- ◇ 現状を確認したかったため
- ◇ 取引先からの要請
- ◇ 社内事業により
- ◇ セキュリティに対して危機感があるため
- ◇ 興味があった他社の動向
- ◇ 自社セキュリティ妥当性の確認
- ◇ 他社取組状況の把握、自社対策を第三者的視点で評価するため
- ◇ 当社のセキュリティ対策がどういうレベルなのかを知りたい
- ◇ 取り組みの内容に興味があったため
- ◇ グループ会社からの紹介
- ◇ セキュリティ対策の一環として
- ◇ 支店長の意向
- ◇ 社内のセキュリティのマニュアルが無いに等しいため
- ◇ 実際のセキュリティリスクがどれくらいあるのか調べたいため

- ◇ セキュリティ対策に不安がある
- ◇ 経済産業省からの紹介
- ◇ 当社ホームページリニューアルにあたり、セキュリティ対策を実施する必要性があった
- ◇ 現状の把握
- ◇ 会社的にセキュリティそのものに対する考えがほぼないから
- ◇ 客先の取引先診断等で情報セキュリティ管理体制の検討が必要になった
- ◇ セキュリティ診断をしていただける
- ◇ 社のセキュリティ体制を外部から診断して頂きたかった
- ◇ 自社の情報セキュリティ対策の構築

● 参加してよかったこと

- ◇ 情報セキュリティ自社診断の結果に対するフィードバックを入手できた事
- ◇ サイバーセキュリティについての知識が高まった
- ◇ 今まで知らなかったことも多くあり、勉強になった
- ◇ 現状を知れた
- ◇ Web サイトの Check で問題がなかった
- ◇ 対応すべき作業 (Adobe 更新)がわかったこと
- ◇ まだわからない
- ◇ 自社診断のキッカケとなった
- ◇ 他社と比較して自社のセキュリティ対策が劣っている認識ができたこと
- ◇ 取り組みで来ている所、不足している所が洗い出しできた
- ◇ 社内の意識向上に役立てられた
- ◇ プログラムの配布は GPO の勉強になった (直接関係はありませんが)
- ◇ サイバーセキュリティに対する知識が深まった
- ◇ 上層部の意識が (少し) 向上した
- ◇ 情報漏洩への不安
- ◇ 他社の対応状況がわかり社内で進めやすい
- ◇ 無償でサービスを受けられること
- ◇ アンチウイルス対策のソフトからすり抜けたものがない事がわかって安心した
- ◇ 動機付けに良い機会だった
- ◇ IPA の事後対応マニュアル等役立つ情報が入手できた
- ◇ 自社がセキュリティに問題があるのかわかりません！
- ◇ 社のセキュリティ体制の客観的診断を元に社内へ展開できた
- ◇ 客観的なご指摘をいただける

【不参加理由】

- 工数問題（7件）
 - ◇ 本サービスを受けることでセキュリティの問題が明らかになり、強化を行わなくてはならなくなるが、その予算を捻出するだけの体力がないと経営判断
 - ◇ 本件に**対応する工数**を確保できないと経営判断、過去に同様の案件を実施したが、あまり効果が無かった
 - ◇ この事業を行っても**対応できる部署**が存在しないため
 - ◇ 消費税率変更での想定外のシステム対応、OS のサポート終了によりアプリケーションの改修・検証など通常業務以外の対応が続いていて**手が回らない**(流通業)
 - ◇ 事業説明では世の中の脅威を多く学べたが、**対応工数がさけない**ため見合わせ
 - ◇ 販売管理システムの入替えて IT 部門に**時間がさけない**（流通業）
 - ◇ 作業できる**社内体制が整わない**ため参加できない
- 中小企業基本法の定義で条件不適合（4件） ※断念頂いた
 - 協同組合は小規模な製造企業群の営業窓口を担っているが条件不適
 - 中小企業クラスの**医療法人**であるが条件不適
 - **社団法人**（非営利な事業）を行っているが参加できないのか
 - **屋号の無い活動**を行っているが参加できないのか
- 現状で問題なし（3件）
 - 現状で**問題ない**ため、導入を見送る方針を経営判断
 - **必要性を感じていない**ため
 - **導入効果が薄い**気がするので、今回は見送りたい
- 外部の助言（2件）
 - 導入済セキュリティベンダーから**検討の必要なし**と助言を受ける
 - 取り扱いセキュリティベンダーから**参加不要**との助言あり
- パソコン上の制限（2件）
 - ソフトウェアを追加インストールは許可がおりない
 - mac OS や iPad で業務をしているが、Windows しか参加できない
- 事業エリア（1件）
 - 本社地域ではなく**北陸以外の工場**を含めたサービスを求めている
また、**海外の工場**を含めたサービスを求めている
- 事業期間が短い（1件）
 - 11 月開始では、工数をかけて導入しても 2 か月程度では効果が望めない
- 業務への負荷（1件）
 - ネット帯域問題、ファイアウォールの問題
（影響がない旨の説明を行った）
- 求める内容が異なる（1件）
 - 会社が行いたい事と方向性が異なるため

- 自助努力で実施（1件）

- 自社でも同様のサービス開発し導入し始めた(情報処理業)

⑥ 本事業の対象外企業からの参加依頼の対応

前項、不参加理由の「**中小企業基本法の定義で条件不適合**」に記載。

(ウ) 中間報告会の概要

7～10月の実証事業で得た知見を、参加企業へフィードバックする場を設けた。

① 各県ごとの参加企業数

表 2-10. 中間報告会参加企業の県別企業数

開催日	開催場所	中間報告会参加数	実証参加企業数
11/20	福井市	1社(1名)	1社(1名)
11/21	金沢市	17社(21名)	15社(19名)
11/22	富山市	9社(13名)	9社(13名)
資料送付	-	6社(6名)	6社(6名)
	計	33社(41名)	31社(39名)

・急な出張により参加できなかった参加企業には資料送付を実施した

② 報告会の開催概要

下記の内容で実施した。

表 2-11. 中間報告会の開催内容

時間	内容	講演者
5分	ご挨拶、趣旨説明	PFU
20分	中小企業における情報セキュリティ対策支援のご紹介	福井：IPA 石川：PFU 富山：PFU
40分	中間報告 ・事業参加企業の分布 ・セキュリティ意識調査 ・IPAベンチマーク診断 ・サイバー攻撃被害(アンケート) ・ヒアリング結果と実態の差 ※当日の配布資料を別紙添付	PFU
20分	サイバー保険の概要と今後の方向性について	損保ジャパン
5分	中間報告会アンケート ※当日の配布資料を別紙添付	PFU

③ アンケート項目

下記の項目をヒアリングした。

- ・参加の動機
- ・参加して良かったこと

- ・参加して悪かったこと
- ・有償サービスに向けて改善すべきこと
- ・有償サービスに向けて期待すること

※本アンケートの結果は、「5(オ)サービス満足度と不満点」において結果を報告する。

(エ) 最終成果報告会の概要

中間報告会の結果に加え、11～12月の実証事業で得られた知見を、参加企業へフィードバックする場を設けた。

① 各県ごとの参加企業数

表 2-12. 最終成果報告会参加企業の県別企業数

開催日	開催場所	最終報告会参加数	実証参加企業数
1/29	富山市	9社(16名)	8社(11名)
1/30	金沢市	18社(25名)	16社(21名)
1/31	福井市	2社(2名)	1社(1名)
資料送付	-	3社(3名)	3社(3名)
	計	32社(46名)	28社(36名)

- ・急な出張により参加できなかった参加企業は、資料送付を実施した

② 報告会の開催概要

下記の内容で実施した。

表 2-13. 最終成果報告会の開催内容

時間	内容	講演者
5分	ご挨拶、趣旨説明	PFU
30分	中小企業における情報セキュリティ対策支援のご紹介	福井：PFU 石川：IPA 富山：PFU
70分	最終成果報告 ※当日の配布資料を別紙添付	PFU
10分	今後の事業展開について ※当日の配布資料を別紙添付	PFU
5分	最終成果報告会アンケート ※当日の配布資料を別紙添付	PFU

③ アンケート項目

下記の項目をヒアリングした。

- ・本事業へのご意見（自由回答）
- ・不参加企業の方限定：参加しなかった理由

※本アンケートの結果は、「5(オ)サービス満足度と不満点」において結果を報告する。

3 中小企業の実態把握

(ア) 実態把握の方法

適切なサイバーセキュリティ事後対応支援体制を構築するため「中小企業がさらされているサイバー攻撃の実態」と「現在のセキュリティ対策状況」を3つの方法で調査・収集する。

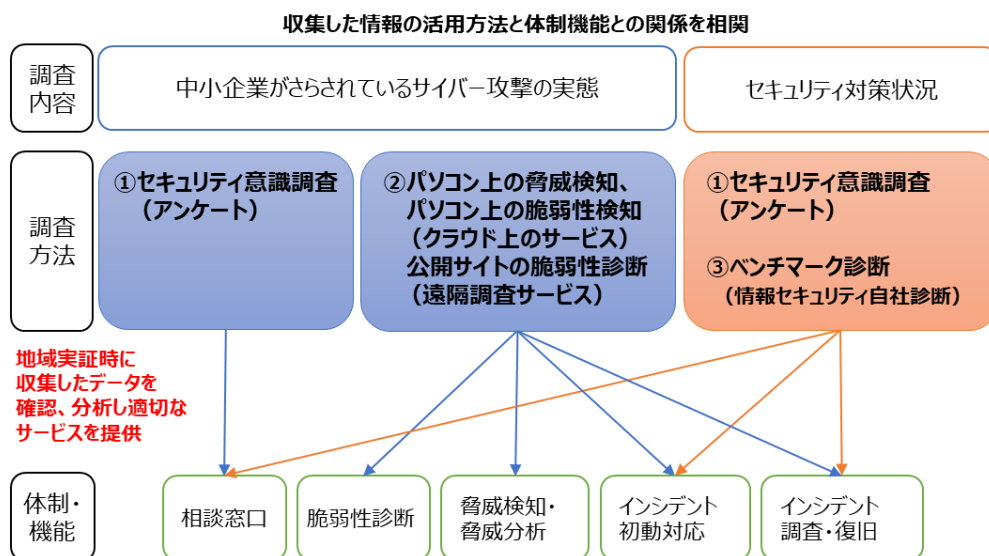


図 3-1. 中小企業の実態把握方法

(イ) 当社採用のエンドポイント型の脅威検知位置 (UTM との違い)

本事業の「脅威の検知数」に関しては、社内と社外ネットワークの境界位置で行うファイアウォールや UTM 装置等で防御されなかった検知数となる。さらに、パソコン上においても、既存のセキュリティ対策製品が検出・対処された脅威は件数に含まれず、全ての既存対策をすり抜けた脅威の検知数を報告している。

既存対策をすり抜けた脅威、重要度や確度の低い脅威を排除して参加企業IT担当者へ通知

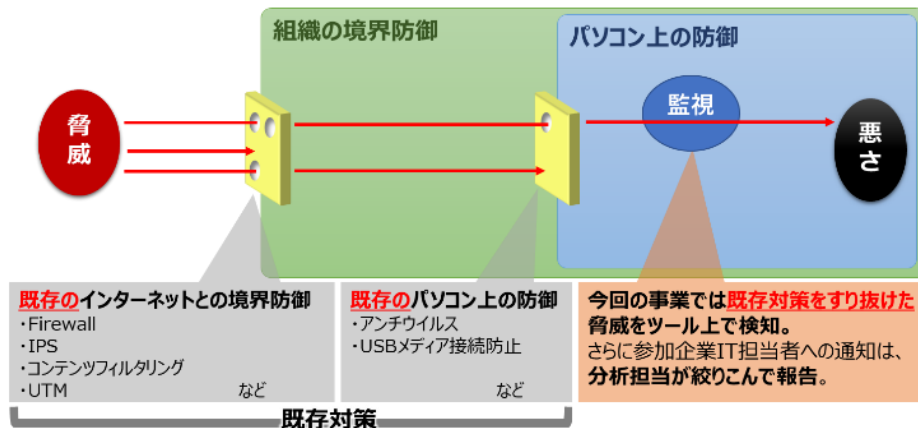


図 3-2. 当社サービスの脅威検知位置

さらに、既存対策と同居する本事業で使用する検知ツールは、確度や重要度の異なる多くの通知を行っている。これらの通知を全て参加企業に転送せず、大手・中堅企業で培った知見を活かし、重要度が低い警告のフィルタリング、外部インテリジェンスを活用して低い確度をフィルタリング、さらに分析担当の知見でフィルタリングし、参加企業 IT 担当者の負担を軽減している。



図 3-3. 当社サービスの脅威警告における抑制

(ウ) セキュリティ意識調査アンケート

意識調査アンケートは、脅威、脆弱性検知等のお助け隊サービスを実施されなかった参加企業を含め1回目のアンケートを実施し、2回目のアンケート（事業終了前）では、お助け隊サービス実施頂いている企業様に1回目で得られなかった部分をさらに深堀してアンケートを実施する。本アンケートは機微な質問も存在するため、無記名式とする。

① 集計対象の母数

集計対象となる回答母数は下記のとおり。

※ 各社1シートの提出を依頼したが、一部複数名で回答されているケースも想定される（無記名式のため除外していない）。

表 3-1. 意識調査アンケートの母数

アンケート	母数となる回答企業数
1回目（7～12月）	185
2回目（12～1月）	37

表 3-2. 意識調査アンケートの業種別割合

業種	1回目 （事業開始時）	2回目 （事業終了時）
製造業（その他）	40.7%	54.1%
卸売業、小売業サービス業	12.9%	8.1%
サービス業（他に分類されないもの）	6.2%	8.1%
金融業、保険業	5.2%	
その他	5.2%	
情報通信業	4.6%	2.7%
学術研究・専門・技術サービス業	3.6%	5.4%
製造業（自動車）	2.1%	5.4%
運輸業、郵便業	1.0%	
生活関連サービス業・娯楽業	1.0%	
教育、学習支援業	1.0%	2.7%
製造業（防衛産業）	0.5%	2.7%
電気・ガス・熱供給・水道製造業	0.5%	
不動産業、物品賃貸業	0.5%	
宿泊業	0.5%	2.7%
飲食サービス業		2.7%
医療、福祉		2.7%
複合サービス事業		2.7%
農業・林業		
漁業		
鉱業・採石業・砂利採取業		

② 診断結果の傾向

表中のパーセンテージは、特に断りがないものは、設問に「はい」「持っている」「実施している」「行っている」と肯定する企業の割合を表している。縦軸は、工程する業種の多いもの順でソートしている。

1 サイバーセキュリティ対策の状況											
1.1	セキュリティに関する困りごとがあった際に相談できる窓口は、57%の組織で持っている。相談先は取引のあるITベンダーと推察される。										
平均 / Q1.1		従業員数									
業種	~5	~10	~20	~50	~100	~200	~300	~500	~1000	~5000	総計
生活関連サービス業・娯楽業					100%			100%			100%
製造業(防衛産業)		100%									100%
医療、福祉							100%				100%
学術研究・専門・技術サービス業	50%	100%		100%	100%						86%
金融業、保険業	100%	50%	50%	100%							71%
サービス業(他に分類されないもの)	50%	50%	100%	100%	100%	0%					64%
その他	100%	0%		75%		50%					63%
卸売業、小売業	25%	0%	80%	100%	58%	67%	100%	0%			59%
製造業(その他)		100%	0%	50%	56%	59%	55%	50%	0%	100%	54%
運輸業、郵便業				50%							50%
製造業(自動車)						100%	0%	50%			50%
情報通信業	50%		25%	100%	50%			100%			50%
建設業		0%	0%	50%							25%
電気・ガス・熱供給・水道製造業							0%				0%
複合サービス事業					0%						0%
不動産業、物品賃貸業			0%								0%
総計	54%	58%	47%	64%	60%	57%	53%	55%	0%	100%	57%
1.2	PCのOSやソフトウェアは常に最新状態に保つ仕組みを、56%の組織で持っている。										
平均 / Q1.2		従業員数									
業種	~5	~10	~20	~50	~100	~200	~300	~500	~1000	~5000	総計
製造業(防衛産業)		100%									100%
生活関連サービス業・娯楽業								100%			100%
学術研究・専門・技術サービス業	100%	100%		100%	100%						100%
情報通信業	100%		50%	100%	100%			100%			80%
建設業		100%	100%	50%							75%
サービス業(他に分類されないもの)	50%	100%	50%	100%	100%	50%					73%
その他	0%	100%		50%		100%					67%
金融業、保険業	100%	50%	0%	100%							57%
製造業(その他)		0%	100%	36%	50%	48%	55%	100%	0%	100%	51%
製造業(自動車)						0%	0%	100%			50%
卸売業、小売業	50%	0%	60%	100%	25%	67%	100%	0%			45%
不動産業、物品賃貸業			0%								0%
医療、福祉							0%				0%
複合サービス事業					0%						0%
運輸業、郵便業				0%							0%
電気・ガス・熱供給・水道製造業							0%				0%
総計	69%	75%	50%	50%	47%	53%	47%	91%	0%	100%	56%
1.3	マルウェアの侵入などのサイバー攻撃を検知する仕組みは、65%の組織で持っている。										
平均 / Q1.3		従業員数									
業種	~5	~10	~20	~50	~100	~200	~300	~500	~1000	~5000	総計
電気・ガス・熱供給・水道製造業							100%				100%
製造業(防衛産業)		100%									100%
生活関連サービス業・娯楽業								100%			100%
医療、福祉							100%				100%
学術研究・専門・技術サービス業	100%	100%		100%	100%						100%
複合サービス事業					100%						100%
サービス業(他に分類されないもの)	100%	100%	50%	100%	100%						90%
製造業(自動車)						0%	100%	100%			75%
情報通信業	100%		75%	0%	100%			0%			70%
その他	0%	100%		50%		100%					67%
製造業(その他)		100%	100%	57%	50%	68%	82%	83%	0%	100%	66%
卸売業、小売業	25%	0%	20%	100%	67%	67%	100%	0%			52%
運輸業、郵便業				50%							50%
金融業、保険業	50%	0%	50%	100%							43%
建設業		100%	0%	0%							25%
不動産業、物品賃貸業			0%								0%
総計	62%	75%	44%	57%	64%	70%	87%	73%	0%	100%	65%

1.4 PC がマルウェアに感染している疑いがあった場合に、それを分析する仕組みは、28%の組織しか持っていない。準備できる仕組みは、後術する対策製品の一覧を加味すると、アンチウイルスソフトや、UTM/IPS/ファイアウォール製品と推察する。

平均 / Q1.4	従業員数										総計
業種	~5	~10	~20	~50	~100	~200	~300	~500	~1000	~5000	
複合サービス事業					100%						100%
電気・ガス・熱供給・水道製造業							100%				100%
生活関連サービス業・娯楽業								100%			100%
医療、福祉							100%				100%
学術研究・専門・技術サービス業	50%	100%		0%	100%						71%
情報通信業	50%		25%		50%			0%			33%
卸売業、小売業	25%	0%	0%	100%	33%	33%	0%	0%			28%
サービス業(他に分類されないもの)	0%	50%	0%	0%	100%	0%					27%
製造業(その他)		100%	50%	21%	38%	19%	27%	17%	0%	100%	27%
製造業(自動車)						0%	0%	50%			25%
金融業、保険業	0%	0%	0%	100%							14%
その他	0%	0%		25%		0%					13%
不動産業、物品賃貸業			0%								0%
運輸業、郵便業				0%							0%
製造業(防衛産業)		0%									0%
建設業		0%	0%	0%							0%
総計	23%	42%	12%	26%	44%	17%	33%	27%	0%	100%	28%

1.5 サイバー攻撃被害があった場合の対応を規定化されている組織は、17%に留まる。事故発生時は、業務を止めるか否かなど判断に迷うことがあるため、規定化しておくことが重要と考える。

平均 / Q1.5	従業員数										総計
業種	~5	~10	~20	~50	~100	~200	~300	~500	~1000	~5000	
医療、福祉							100%				100%
情報通信業	50%		50%		50%			100%			56%
製造業(自動車)						0%	0%	100%			50%
金融業、保険業	50%	0%	0%	100%							29%
学術研究・専門・技術サービス業	50%	0%		100%	0%						29%
卸売業、小売業	0%	0%	0%	100%	25%	0%	100%	0%			21%
サービス業(他に分類されないもの)	0%	50%	0%	0%	0%	50%					18%
製造業(その他)		0%	0%	0%	19%	7%	0%	33%	100%	0%	10%
運輸業、郵便業				0%							0%
電気・ガス・熱供給・水道製造業							0%				0%
製造業(防衛産業)		0%									0%
生活関連サービス業・娯楽業								0%			0%
不動産業、物品賃貸業			0%								0%
複合サービス事業					0%						0%
その他	0%	0%		0%		0%					0%
建設業		0%	0%	0%							0%
総計	23%	8%	12%	15%	21%	8%	13%	45%	100%	0%	17%

1.6 サイバー攻撃の被害状況の調査や復旧に向けた対応を進める仕組みを持つ組織は、18%に過ぎない。組織内で CSIRT の構築し、権限を与える必要がある。

平均 / Q1.6	従業員数										総計
業種	~5	~10	~20	~50	~100	~200	~300	~500	~1000	~5000	
電気・ガス・熱供給・水道製造業							100%				100%
製造業(防衛産業)		100%									100%
医療、福祉							100%				100%
学術研究・専門・技術サービス業	50%	0%		100%	100%						43%
サービス業(他に分類されないもの)	50%	50%	50%	0%	50%	0%					36%
情報通信業	50%		0%		50%			100%			33%
製造業(自動車)						0%	0%	50%			25%
卸売業、小売業	0%	0%	0%	100%	17%	0%	100%	0%			17%
金融業、保険業	0%	0%	50%	0%							14%
その他	0%	0%		0%		50%					13%
製造業(その他)		0%	0%	14%	19%	7%	18%	0%	0%	0%	11%
運輸業、郵便業				0%							0%
不動産業、物品賃貸業			0%								0%
複合サービス事業					0%						0%
生活関連サービス業・娯楽業								0%			0%
建設業		0%	0%	0%							0%
総計	23%	17%	12%	19%	24%	9%	33%	18%	0%	0%	18%

2	セキュリティに対する意識																																																																																																																																																																																																																																																																																																																																																																																																																																																																										
2.1	<p>自社がサイバー攻撃被害に遭う可能性があると考える組織は、85%を占める。多くの組織で危機感は持たれている。</p> <table border="1"> <thead> <tr> <th rowspan="2">平均 / Q2.1 業種</th> <th colspan="10">従業員数</th> <th rowspan="2">総計</th> </tr> <tr> <th>~5</th> <th>~10</th> <th>~20</th> <th>~50</th> <th>~100</th> <th>~200</th> <th>~300</th> <th>~500</th> <th>~1000</th> <th>~5000</th> </tr> </thead> <tbody> <tr><td>製造業(防衛産業)</td><td></td><td>100%</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>100%</td></tr> <tr><td>情報通信業</td><td>100%</td><td></td><td>100%</td><td>100%</td><td>100%</td><td></td><td></td><td>100%</td><td></td><td></td><td>100%</td></tr> <tr><td>電気・ガス・熱供給・水道製造業</td><td></td><td></td><td></td><td></td><td></td><td></td><td>100%</td><td></td><td></td><td></td><td>100%</td></tr> <tr><td>医療、福祉</td><td></td><td></td><td></td><td></td><td></td><td></td><td>100%</td><td></td><td></td><td></td><td>100%</td></tr> <tr><td>生活関連サービス業・娯楽業</td><td></td><td></td><td></td><td></td><td>100%</td><td></td><td></td><td>100%</td><td></td><td></td><td>100%</td></tr> <tr><td>運輸業、郵便業</td><td></td><td></td><td></td><td>100%</td><td></td><td></td><td></td><td></td><td></td><td></td><td>100%</td></tr> <tr><td>学術研究・専門・技術サービス業</td><td>100%</td><td>100%</td><td></td><td>100%</td><td>100%</td><td></td><td></td><td></td><td></td><td></td><td>100%</td></tr> <tr><td>複合サービス事業</td><td></td><td></td><td></td><td></td><td>100%</td><td></td><td></td><td></td><td></td><td></td><td>100%</td></tr> <tr><td>サービス業(他に分類されないもの)</td><td>100%</td><td>50%</td><td>100%</td><td>100%</td><td>100%</td><td>100%</td><td></td><td></td><td></td><td></td><td>91%</td></tr> <tr><td>その他</td><td>0%</td><td>100%</td><td></td><td>100%</td><td></td><td>100%</td><td></td><td></td><td></td><td></td><td>89%</td></tr> <tr><td>卸売業、小売業</td><td>50%</td><td>0%</td><td>100%</td><td>100%</td><td>100%</td><td>50%</td><td>100%</td><td>100%</td><td></td><td></td><td>86%</td></tr> <tr><td>製造業(その他)</td><td></td><td>0%</td><td>100%</td><td>71%</td><td>81%</td><td>89%</td><td>82%</td><td>100%</td><td>100%</td><td>100%</td><td>84%</td></tr> <tr><td>製造業(自動車)</td><td></td><td></td><td></td><td></td><td></td><td>100%</td><td>100%</td><td>50%</td><td></td><td></td><td>75%</td></tr> <tr><td>金融業、保険業</td><td>100%</td><td>50%</td><td>50%</td><td>100%</td><td></td><td></td><td></td><td></td><td></td><td></td><td>71%</td></tr> <tr><td>建設業</td><td></td><td>0%</td><td>0%</td><td>50%</td><td></td><td></td><td></td><td></td><td></td><td></td><td>25%</td></tr> <tr><td>不動産業、物品賃貸業</td><td></td><td></td><td>0%</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>0%</td></tr> <tr><td>総計</td><td>77%</td><td>58%</td><td>82%</td><td>82%</td><td>91%</td><td>89%</td><td>87%</td><td>91%</td><td>100%</td><td>100%</td><td>85%</td></tr> </tbody> </table>	平均 / Q2.1 業種	従業員数										総計	~5	~10	~20	~50	~100	~200	~300	~500	~1000	~5000	製造業(防衛産業)		100%									100%	情報通信業	100%		100%	100%	100%			100%			100%	電気・ガス・熱供給・水道製造業							100%				100%	医療、福祉							100%				100%	生活関連サービス業・娯楽業					100%			100%			100%	運輸業、郵便業				100%							100%	学術研究・専門・技術サービス業	100%	100%		100%	100%						100%	複合サービス事業					100%						100%	サービス業(他に分類されないもの)	100%	50%	100%	100%	100%	100%					91%	その他	0%	100%		100%		100%					89%	卸売業、小売業	50%	0%	100%	100%	100%	50%	100%	100%			86%	製造業(その他)		0%	100%	71%	81%	89%	82%	100%	100%	100%	84%	製造業(自動車)						100%	100%	50%			75%	金融業、保険業	100%	50%	50%	100%							71%	建設業		0%	0%	50%							25%	不動産業、物品賃貸業			0%								0%	総計	77%	58%	82%	82%	91%	89%	87%	91%	100%	100%	85%																																																																																																																																																																																																																																								
平均 / Q2.1 業種	従業員数										総計																																																																																																																																																																																																																																																																																																																																																																																																																																																																
	~5	~10	~20	~50	~100	~200	~300	~500	~1000	~5000																																																																																																																																																																																																																																																																																																																																																																																																																																																																	
製造業(防衛産業)		100%									100%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
情報通信業	100%		100%	100%	100%			100%			100%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
電気・ガス・熱供給・水道製造業							100%				100%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
医療、福祉							100%				100%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
生活関連サービス業・娯楽業					100%			100%			100%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
運輸業、郵便業				100%							100%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
学術研究・専門・技術サービス業	100%	100%		100%	100%						100%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
複合サービス事業					100%						100%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
サービス業(他に分類されないもの)	100%	50%	100%	100%	100%	100%					91%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
その他	0%	100%		100%		100%					89%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
卸売業、小売業	50%	0%	100%	100%	100%	50%	100%	100%			86%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
製造業(その他)		0%	100%	71%	81%	89%	82%	100%	100%	100%	84%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
製造業(自動車)						100%	100%	50%			75%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
金融業、保険業	100%	50%	50%	100%							71%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
建設業		0%	0%	50%							25%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
不動産業、物品賃貸業			0%								0%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
総計	77%	58%	82%	82%	91%	89%	87%	91%	100%	100%	85%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
2.2	<p>脆弱性診断やサイバー保険など、セキュリティ対策を実施されている組織は、24%と少ない。次項で、アンチウイルス製品やUTM/IPS/ファイアウォールの導入までが多数という結果が出ている。</p> <table border="1"> <thead> <tr> <th rowspan="2">平均 / Q2.2 業種</th> <th colspan="10">従業員数</th> <th rowspan="2">総計</th> </tr> <tr> <th>~5</th> <th>~10</th> <th>~20</th> <th>~50</th> <th>~100</th> <th>~200</th> <th>~300</th> <th>~500</th> <th>~1000</th> <th>~5000</th> </tr> </thead> <tbody> <tr><td>医療、福祉</td><td></td><td></td><td></td><td></td><td></td><td></td><td>100%</td><td></td><td></td><td></td><td>100%</td></tr> <tr><td>生活関連サービス業・娯楽業</td><td></td><td></td><td></td><td></td><td>0%</td><td></td><td></td><td>100%</td><td></td><td></td><td>50%</td></tr> <tr><td>サービス業(他に分類されないもの)</td><td>0%</td><td>100%</td><td>50%</td><td>100%</td><td>0%</td><td>0%</td><td></td><td></td><td></td><td></td><td>36%</td></tr> <tr><td>製造業(自動車)</td><td></td><td></td><td></td><td></td><td></td><td>100%</td><td>0%</td><td>0%</td><td></td><td></td><td>33%</td></tr> <tr><td>卸売業、小売業</td><td>25%</td><td>0%</td><td>0%</td><td>100%</td><td>45%</td><td>0%</td><td>0%</td><td>100%</td><td></td><td></td><td>33%</td></tr> <tr><td>製造業(その他)</td><td></td><td>0%</td><td>0%</td><td>36%</td><td>25%</td><td>19%</td><td>20%</td><td>50%</td><td>0%</td><td>0%</td><td>24%</td></tr> <tr><td>情報通信業</td><td>50%</td><td></td><td>25%</td><td>0%</td><td>0%</td><td></td><td></td><td>0%</td><td></td><td></td><td>20%</td></tr> <tr><td>学術研究・専門・技術サービス業</td><td>50%</td><td>0%</td><td></td><td>0%</td><td>0%</td><td></td><td></td><td></td><td></td><td></td><td>14%</td></tr> <tr><td>その他</td><td>0%</td><td>0%</td><td></td><td>25%</td><td></td><td>0%</td><td></td><td></td><td></td><td></td><td>11%</td></tr> <tr><td>製造業(防衛産業)</td><td></td><td>0%</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>0%</td></tr> <tr><td>運輸業、郵便業</td><td></td><td></td><td></td><td>0%</td><td></td><td></td><td></td><td></td><td></td><td></td><td>0%</td></tr> <tr><td>電気・ガス・熱供給・水道製造業</td><td></td><td></td><td></td><td></td><td></td><td></td><td>0%</td><td></td><td></td><td></td><td>0%</td></tr> <tr><td>不動産業、物品賃貸業</td><td></td><td></td><td>0%</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>0%</td></tr> <tr><td>複合サービス事業</td><td></td><td></td><td></td><td></td><td>0%</td><td></td><td></td><td></td><td></td><td></td><td>0%</td></tr> <tr><td>金融業、保険業</td><td>0%</td><td>0%</td><td>0%</td><td>0%</td><td></td><td></td><td></td><td></td><td></td><td></td><td>0%</td></tr> <tr><td>建設業</td><td></td><td>0%</td><td>0%</td><td>0%</td><td></td><td></td><td></td><td></td><td></td><td></td><td>0%</td></tr> <tr><td>総計</td><td>23%</td><td>17%</td><td>12%</td><td>32%</td><td>26%</td><td>17%</td><td>21%</td><td>50%</td><td>0%</td><td>0%</td><td>24%</td></tr> </tbody> </table>	平均 / Q2.2 業種	従業員数										総計	~5	~10	~20	~50	~100	~200	~300	~500	~1000	~5000	医療、福祉							100%				100%	生活関連サービス業・娯楽業					0%			100%			50%	サービス業(他に分類されないもの)	0%	100%	50%	100%	0%	0%					36%	製造業(自動車)						100%	0%	0%			33%	卸売業、小売業	25%	0%	0%	100%	45%	0%	0%	100%			33%	製造業(その他)		0%	0%	36%	25%	19%	20%	50%	0%	0%	24%	情報通信業	50%		25%	0%	0%			0%			20%	学術研究・専門・技術サービス業	50%	0%		0%	0%						14%	その他	0%	0%		25%		0%					11%	製造業(防衛産業)		0%									0%	運輸業、郵便業				0%							0%	電気・ガス・熱供給・水道製造業							0%				0%	不動産業、物品賃貸業			0%								0%	複合サービス事業					0%						0%	金融業、保険業	0%	0%	0%	0%							0%	建設業		0%	0%	0%							0%	総計	23%	17%	12%	32%	26%	17%	21%	50%	0%	0%	24%																																																																																																																																																																																																																																								
平均 / Q2.2 業種	従業員数										総計																																																																																																																																																																																																																																																																																																																																																																																																																																																																
	~5	~10	~20	~50	~100	~200	~300	~500	~1000	~5000																																																																																																																																																																																																																																																																																																																																																																																																																																																																	
医療、福祉							100%				100%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
生活関連サービス業・娯楽業					0%			100%			50%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
サービス業(他に分類されないもの)	0%	100%	50%	100%	0%	0%					36%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
製造業(自動車)						100%	0%	0%			33%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
卸売業、小売業	25%	0%	0%	100%	45%	0%	0%	100%			33%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
製造業(その他)		0%	0%	36%	25%	19%	20%	50%	0%	0%	24%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
情報通信業	50%		25%	0%	0%			0%			20%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
学術研究・専門・技術サービス業	50%	0%		0%	0%						14%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
その他	0%	0%		25%		0%					11%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
製造業(防衛産業)		0%									0%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
運輸業、郵便業				0%							0%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
電気・ガス・熱供給・水道製造業							0%				0%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
不動産業、物品賃貸業			0%								0%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
複合サービス事業					0%						0%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
金融業、保険業	0%	0%	0%	0%							0%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
建設業		0%	0%	0%							0%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
総計	23%	17%	12%	32%	26%	17%	21%	50%	0%	0%	24%																																																																																																																																																																																																																																																																																																																																																																																																																																																																
2.3	<p>行われている対策は、アンチウイルス、UTM が大半を占める。 (単位：回答企業数)</p> <table border="1"> <thead> <tr> <th rowspan="2">合計 / 件数</th> <th colspan="16">業種・従業員数</th> <th rowspan="2">総計</th> </tr> <tr> <th colspan="4">製造業(その他)</th> <th colspan="4">製造業(自動車)</th> <th colspan="4">卸売業、小売業</th> <th colspan="4">サービス業(他に分類されないもの)</th> <th>医療、福祉</th> <th>学術研究・専門・技術サービス業</th> <th>金融業、保険業</th> <th>情報通信業</th> <th>その他</th> </tr> <tr> <th></th> <th>~50</th> <th>~100</th> <th>~200</th> <th>~300</th> <th>~500</th> <th>~1000</th> <th>~200</th> <th>~10</th> <th>~50</th> <th>~100</th> <th>~200</th> <th>~500</th> <th>~10</th> <th>~200</th> <th>~300</th> <th>~500</th> <th>~5</th> <th>~20</th> <th>~50</th> <th>~200</th> </tr> </thead> <tbody> <tr><td>導入された対策</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>エンドポイントセキュリティ(アンチウイルスソフト)</td><td>1</td><td>2</td><td>3</td><td>4</td><td>3</td><td>1</td><td>1</td><td>1</td><td>1</td><td>3</td><td>1</td><td>1</td><td>1</td><td>1</td><td></td><td></td><td>1</td><td>1</td><td>1</td><td>1</td><td>25</td></tr> <tr><td>UTM</td><td>1</td><td>1</td><td>3</td><td>2</td><td>2</td><td></td><td></td><td></td><td></td><td>1</td><td>1</td><td>1</td><td></td><td></td><td></td><td></td><td>1</td><td></td><td></td><td></td><td>12</td></tr> <tr><td>ファイアウォール</td><td>1</td><td>2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>5</td></tr> <tr><td>サイバー保険</td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>2</td><td>1</td><td>1</td><td></td><td></td><td></td><td></td><td>1</td><td>5</td></tr> <tr><td>脆弱性診断</td><td>1</td><td>1</td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>3</td></tr> <tr><td>IT資産管理(デバイス制御)</td><td></td><td></td><td></td><td>1</td><td>1</td><td></td><td></td><td></td><td></td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>3</td></tr> <tr><td>バックアップ</td><td></td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td></td><td>2</td></tr> <tr><td>専門業者とのコンサルタント契約</td><td></td><td></td><td>1</td><td></td><td></td><td></td><td></td><td></td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>2</td></tr> <tr><td>OS・アプリケーションの脆弱性更新</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td></td><td></td><td></td><td></td><td>1</td></tr> <tr><td>ログ監視</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td></tr> <tr><td>セキュリティサービス(サーバ運営者)</td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td></tr> <tr><td>権限管理(Active Directory)</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td></tr> <tr><td>エンドポイントセキュリティ(アンチウイルス・情報漏洩・Web脅威)</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td></tr> <tr><td>イントラネット化</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td></td><td></td><td></td><td></td><td>1</td></tr> <tr><td>管理委託、任せきり</td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td></tr> <tr><td>ISO27001に準ずる諸々の対策</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td></td><td></td><td></td><td></td><td>1</td></tr> <tr><td>総計</td><td>6</td><td>7</td><td>8</td><td>7</td><td>6</td><td>2</td><td>1</td><td>1</td><td>2</td><td>6</td><td>3</td><td>1</td><td>2</td><td>3</td><td>3</td><td>3</td><td>1</td><td>1</td><td>2</td><td>1</td><td>1</td><td>2</td><td>66</td></tr> </tbody> </table>	合計 / 件数	業種・従業員数																総計	製造業(その他)				製造業(自動車)				卸売業、小売業				サービス業(他に分類されないもの)				医療、福祉	学術研究・専門・技術サービス業	金融業、保険業	情報通信業	その他		~50	~100	~200	~300	~500	~1000	~200	~10	~50	~100	~200	~500	~10	~200	~300	~500	~5	~20	~50	~200	導入された対策																						エンドポイントセキュリティ(アンチウイルスソフト)	1	2	3	4	3	1	1	1	1	3	1	1	1	1			1	1	1	1	25	UTM	1	1	3	2	2					1	1	1					1				12	ファイアウォール	1	2																			5	サイバー保険	1												2	1	1					1	5	脆弱性診断	1	1	1																		3	IT資産管理(デバイス制御)				1	1					1											3	バックアップ		1																	1		2	専門業者とのコンサルタント契約			1						1												2	OS・アプリケーションの脆弱性更新																1					1	ログ監視														1							1	セキュリティサービス(サーバ運営者)	1																				1	権限管理(Active Directory)										1											1	エンドポイントセキュリティ(アンチウイルス・情報漏洩・Web脅威)									1												1	イントラネット化																1					1	管理委託、任せきり	1																				1	ISO27001に準ずる諸々の対策																1					1	総計	6	7	8	7	6	2	1	1	2	6	3	1	2	3	3	3	1	1	2	1	1	2	66
合計 / 件数	業種・従業員数																総計																																																																																																																																																																																																																																																																																																																																																																																																																																																										
	製造業(その他)				製造業(自動車)				卸売業、小売業				サービス業(他に分類されないもの)					医療、福祉	学術研究・専門・技術サービス業	金融業、保険業	情報通信業	その他																																																																																																																																																																																																																																																																																																																																																																																																																																																					
	~50	~100	~200	~300	~500	~1000	~200	~10	~50	~100	~200	~500	~10	~200	~300	~500	~5	~20	~50	~200																																																																																																																																																																																																																																																																																																																																																																																																																																																							
導入された対策																																																																																																																																																																																																																																																																																																																																																																																																																																																																											
エンドポイントセキュリティ(アンチウイルスソフト)	1	2	3	4	3	1	1	1	1	3	1	1	1	1			1	1	1	1	25																																																																																																																																																																																																																																																																																																																																																																																																																																																						
UTM	1	1	3	2	2					1	1	1					1				12																																																																																																																																																																																																																																																																																																																																																																																																																																																						
ファイアウォール	1	2																			5																																																																																																																																																																																																																																																																																																																																																																																																																																																						
サイバー保険	1												2	1	1					1	5																																																																																																																																																																																																																																																																																																																																																																																																																																																						
脆弱性診断	1	1	1																		3																																																																																																																																																																																																																																																																																																																																																																																																																																																						
IT資産管理(デバイス制御)				1	1					1											3																																																																																																																																																																																																																																																																																																																																																																																																																																																						
バックアップ		1																	1		2																																																																																																																																																																																																																																																																																																																																																																																																																																																						
専門業者とのコンサルタント契約			1						1												2																																																																																																																																																																																																																																																																																																																																																																																																																																																						
OS・アプリケーションの脆弱性更新																1					1																																																																																																																																																																																																																																																																																																																																																																																																																																																						
ログ監視														1							1																																																																																																																																																																																																																																																																																																																																																																																																																																																						
セキュリティサービス(サーバ運営者)	1																				1																																																																																																																																																																																																																																																																																																																																																																																																																																																						
権限管理(Active Directory)										1											1																																																																																																																																																																																																																																																																																																																																																																																																																																																						
エンドポイントセキュリティ(アンチウイルス・情報漏洩・Web脅威)									1												1																																																																																																																																																																																																																																																																																																																																																																																																																																																						
イントラネット化																1					1																																																																																																																																																																																																																																																																																																																																																																																																																																																						
管理委託、任せきり	1																				1																																																																																																																																																																																																																																																																																																																																																																																																																																																						
ISO27001に準ずる諸々の対策																1					1																																																																																																																																																																																																																																																																																																																																																																																																																																																						
総計	6	7	8	7	6	2	1	1	2	6	3	1	2	3	3	3	1	1	2	1	1	2	66																																																																																																																																																																																																																																																																																																																																																																																																																																																				
	<p>【2回目のアンケート】 具体的なインターネットとの境界防御と、パソコン上のエンドポイント対策は、予想以上にしっかりした製品が導入されている。</p> <ul style="list-style-type: none"> ● インターネットとの境界防御対策 ● パソコン上のエンドポイント対策 																																																																																																																																																																																																																																																																																																																																																																																																																																																																										

2.4 それらセキュリティ対策は十分（自社に適している）という組織は、17%しかなく、もっと強化したいと考えている。

平均 / Q2.4 業種	従業員数										総計
	~5	~10	~20	~50	~100	~200	~300	~500	~1000	~5000	
学術研究・専門・技術サービス業	0%	67%	100%	0%	0%	0%	0%	0%	0%	0%	43%
卸売業、小売業	25%	0%	0%	50%	30%	33%	0%	100%	0%	0%	26%
製造業(自動車)						0%	0%	50%			25%
建設業		100%	0%	0%							25%
サービス業(他に分類されないもの)	0%	50%	50%	0%	0%	0%					20%
金融業、保険業	50%	0%	0%	0%							14%
製造業(その他)	0%	0%	50%	21%	6%	15%	10%	17%	0%	0%	14%
その他	0%	0%	0%	0%		50%					13%
情報通信業	0%		0%	100%	0%			0%			10%
電気・ガス・熱供給・水道製造業							0%				0%
製造業(防衛産業)		0%									0%
複合サービス事業					0%						0%
不動産業、物品賃貸業			0%								0%
医療、福祉							0%				0%
運輸業、郵便業				0%							0%
生活関連サービス業・娯楽業					0%			0%			0%
総計	15%	33%	12%	21%	12%	18%	7%	27%	0%	0%	17%

2.5 セキュリティ対策にかけることができる月額費用は平均 5.8 万円（年間 70 万円）だった。従業員数や年商が多いと掛けられる金額も想定どおり増している。

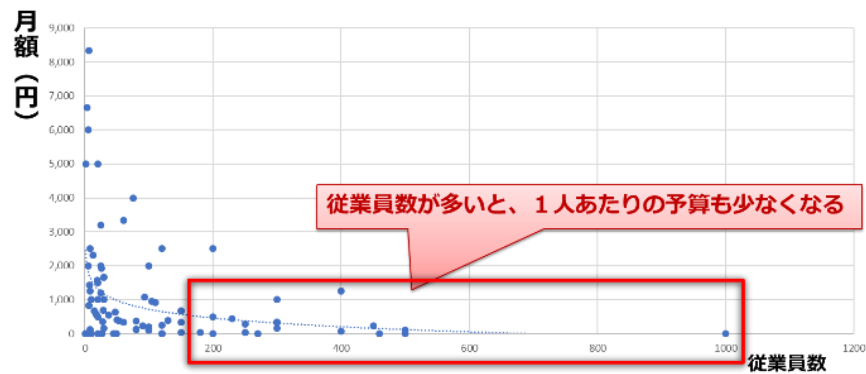
(単位：万円)

平均 / Q2.5 業種	従業員数										年商			総計
	~5	~10	~20	~50	~100	~200	~300	~500	~1000	~1億	1~10億	10億~		
医療、福祉							30.0					30.0	30.0	
生活関連サービス業・娯楽業								10.0				10.0	10.0	
製造業(自動車)						9.0		10.0				9.5	9.5	
製造業(その他)		2.0	2.0	6.4	1.1	11.3	8.4	14.5	10.0	3.0	2.8	9.6	7.5	
卸売業、小売業	1.5	0.5	2.0	2.8	8.9	5.0	10.0	3.0		1.0	1.4	8.5	5.7	
情報通信業	1.8		4.7	0.0	10.0					1.8	3.5	10.0	3.9	
製造業(防衛産業)		3.0									3.0		3.0	
サービス業(他に分類されないもの)	1.0	3.0				5.0				1.0	5.3	0.0	3.0	
金融業、保険業	1.0	0.1	1.0	8.0						0.7	8.0	0.0	2.5	
その他	2.0			2.5		0.0				1.0	2.7	2.0	2.0	
学術研究・専門・技術サービス業	1.0	1.0		3.0						1.0	3.0		1.7	
運輸業、郵便業				1.5							1.5		1.5	
電気・ガス・熱供給・水道製造業							1.0					1.0	1.0	
建設業		1.0								1.0			1.0	
不動産業、物品賃貸業			0.0								0.0		0.0	
総計	1.4	1.7	2.5	4.2	5.5	9.1	9.8	11.6	10.0	1.2	2.6	9.2	5.8	

従業員数が多い分だけ費用も増える

年商が多い分だけ費用も増える

1人あたり月額 988 円であった。



ただし、インターネットとの境界防御と、パソコン上のエンドポイント対策の区別なく質問を行っているため注意が必要。

【2回目のアンケート】

インターネット境界防御に年間 50.6 万円、パソコン上のエンドポイント対策は年間 7,710 円(月額 643 円)であった。

インターネット境界防御に掛けられる年間費用

業種	平均 / 境界セキュリティ対策費用 (万円/年)								総計
	~10	~20	~50	~100	~200	~300	~500	~1000	
情報通信業				100.0					100.0
製造業(その他)	15.0	0.0	0.7	1.5	68.0	33.0	270.0	72.0	59.5
製造業(自動車)				0.0	60.0				30.0
学術研究・専門・技術サービス業				24.0					24.0
教育、学習支援業	10.0								10.0
卸売業、小売業サービス業					0.0				0.0
宿泊業						0.0			0.0
総計	12.5	0.0	0.7	25.4	57.1	24.8	270.0	72.0	50.6

パソコン上のエンドポイント対策に掛けられる 1人あたりの年間費用

業種	平均 / エンドポイント対策 (円/1人・1年)								総計
	~10	~20	~50	~100	~200	~300	~500	~1000	
卸売業、小売業サービス業			2,857		3,000				2,929
学術研究・専門・技術サービス業				20,000					20,000
教育、学習支援業	5,000								5,000
宿泊業						4,000			4,000
情報通信業				4,000					4,000
製造業(その他)	5,000	4,000	4,750	50,000	2,674	2,750	4,340	0	8,332
製造業(自動車)				0	11,000				5,500
総計	5,000	4,000	4,371	24,800	3,910	3,063	4,340	0	7,710

3 サイバー攻撃被害の実態

3.1 自社内で発生したサイバー攻撃を 31%の組織が認識していた。それ以外は、既存の対策で対処できている範囲であれば、事故に至らず、気づく事もないと考えることもできる。

業種	平均 / Q3.1										総計
	~5	~10	~20	~50	~100	~200	~300	~500	~1000	~5000	
電気・ガス・熱供給・水道製造業							100%				100%
医療、福祉							100%				100%
金融業、保険業	100%	0%	100%	0%							57%
運輸業、郵便業				50%							50%
サービス業(他に分類されないもの)	0%	0%	50%	0%	100%	100%					45%
情報通信業	50%		25%	0%	50%			100%			40%
製造業(その他)		0%	50%	36%	40%	35%	27%	17%	100%	0%	34%
製造業(自動車)						0%	0%	100%			33%
学術研究・専門・技術サービス業	0%	0%		100%	100%						29%
卸売業、小売業	50%	0%	0%	50%	17%	0%	100%	0%			21%
その他	0%	0%		25%		0%					11%
不動産業、物品賃貸業			0%								0%
複合サービス事業					0%						0%
製造業(防衛産業)		0%									0%
生活関連サービス業・娯楽業					0%			0%			0%
建設業					0%						0%
総計	38%	0%	29%	32%	35%	31%	40%	30%	100%	0%	31%

3.2 認識している被害は下記のとおり。

ランサムウェア	8件
Webサーバの侵害(改ざん)	7件
メール乗っ取り(なりすましメール)	5件
マルウェア付きメールの開封	4件
迷惑メールが届く	4件
フィッシングメール	3件
被害・攻撃はない	3件
マルウェア感染拡大(共有フォルダ)	2件
サービス妨害攻撃(DoS)	2件
標的型メール	2件

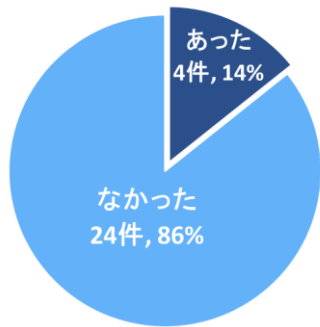
(単位：件数)

合計/件数	業種・従業員数															総計								
	製造業(その他)					製造業(自動車)					サービス業		情報通信業		運輸業・郵便業		卸売業・小売業	学術研究・専門・技術サービス業	金融業・保険業	電気・ガス・熱供給・水道業				
	~20	~50	~100	~200	~300	~500	~1000	~500	~200	~100	~200	~5	~20	~100	~500	~50	~5	~50	~100	~5	~20	~300	~50	
被害内容																								
ランサムウェア		1	1	2	1			1																8
Webサーバの侵害(改ざん)		3							2	1	1													7
メール乗っ取り(なりすましメール)		2							1															5
マルウェア付きメールの開封				1	1	1																		4
迷惑メールが届く	1			2																				4
フィッシングメール			2	1																				3
被害・攻撃はない			1			1	1																	3
マルウェア感染拡大(共有フォルダ)						1																1		2
サービス妨害攻撃(DoS)				1									1											2
標的型メール						1																1		2
ウイルス感染								1																1
メールボックスが消失した																								1
サービス妨害攻撃(VPN、メール)																								1
サービス妨害攻撃(ルータ攻撃)																								1
公開FTPサーバへのマルウェア感染																								1
(IPA IlugScannerで攻撃の形跡を発見)																								1
ウイルス感染(USB経由)																								1
なりすましメール																								1
データ破壊																								1
ロイの木馬																								1
総計	1	7	7	10	5	2	1	1	1	2	2	1	1	1	1	1	2	1	1	2	1	1	1	53

3.3 被害を認識した際の対応内容は下記のとおり。

- ランサムウェアへの対応
 - ・ バックアップデータから復旧
 - ・ あきらめてバックアップに戻す、感染PCのHDDを物理隔離
 - ・ 全てのPCのLANケーブルを抜き、ウイルス対策ソフトでスキャンして被害状況を確認し、その後、感染していないPCのみ復旧、感染PCの再セットアップ
 - ・ 数年前のバックアップがあったそうで、それで復活したとのこと
 - ・ 感染PCのリカバリとサーバ内のファイルをバックアップから復元
 - ・ データ復旧とWindowsセキュリティ設定、ルータの強化
 - ・ 感染パソコンの特定と隔離、パソコンの再インストール
- データ破壊への対応
 - ・ 他のパソコンへウイルス感染していないか調査、および感染したパソコンのウイルスの駆除
- その他のマルウェア感染への対応
 - ・ ネットワークから分離(LANケーブルを直ぐ抜く)
 - ・ ウイルス対策ソフトで対応(ウイルス対策ソフト導入)
 - ・ 駆除・除去(グループ会社協力の元、感染した1台1台駆除)
 - ・ データ破壊、バックアップデータからの復旧
 - ・ メールサーバによる隔離
 - ・ 開かずに削除した

- 標的型メールへの対処・迷惑メールの対処
 - ・ ウイルス対策ソフトで対応、ファイアウォールで対応
- なりすましメール・フィッシングメール（受信）への対処
 - ・ 削除（自動）、および IT 管理者による把握
 - ・ 削除（自動）、および IT 管理者による把握
 - ・ 不審なメールは開かない、Web サイトのリンクには飛ばないなど口頭で案内
 - ・ サプライチェーン間でルールを決める
 - ・ Gmail に変更、対策ソフトの導入
- なりすましメール（発信）への対処
 - ・ 業者に見てもらった
 - ・ ソフトで駆除
- メール乗っ取りへの対処
 - ・ 県警に被害届を提出
 - ・ 2週間後にレンタルサーバからの連絡で気づいた、放置、全パスワード変更
 - ・ 2段階認証とパスワードの抹消をした
- メール不正アクセスへの対処
 - ・ 無視している
- サポート詐欺(Web サイト)への対処
 - ・ ブラウザを終了させた上で、念のためアンチウイルスソフトでスキャンを掛けた
- サービス妨害攻撃(DoS)への対処
 - ・ LAN を外した
 - ・ 原因調査のみ
 - ・ ルータの設定変更の実施
 - ・ ファイアウォールによる発信元のアクセス制限
- 公開サイト侵害・改ざんへの対処
 - ・ サーバ管理会社で対応
 - ・ アクセス元の特定と制限
 - ・ バックアップから修復、プログラムの変更を行った
- ログ分析ツールで見つかった攻撃への対処
 - ・ IP を調べて不正な IP はブロック
- Web 問い合わせフォームのメールアドレス宛ての大量メールへの対処
 - ・ メールアドレスのフィルタリング、後日 Web フォームの変更
- OS 起動不可への対処
 - ・ 廃棄処分とした
- その他
 - ・ 何もしていない
 - ・ 想定した事が無い

	<p>【2回目のアンケート】</p> <p>この事業期間中に 14%の企業でマルウェア感染を経験し、下記のような対処を行われていた。</p> <div style="display: flex; align-items: center;">  <div style="margin-left: 20px;"> <ul style="list-style-type: none"> ● Emotet に感染 本事業の駆け付け対応で駆除を実施 ● Emotet と思われるメールを受信 関係者に対しウイルスフルスキャンを実施し、1名でトロイ型ウイルスを検出・駆除 ● フィッシングサイトからウイルス感染 端末の初期化を実施 </div> </div>
3.4	<p>自社内で保有する情報が漏洩した場合に、各企業で想定している被害は下記のとおり。</p> <ul style="list-style-type: none"> ● マルウェア感染による情報漏洩被害を受けた会社 <ul style="list-style-type: none"> ・ 事業活動の停止、取引先等の個人情報の流出 ・ 重要技術情報（図面等）による膨大な営業被害（売上） ・ 「分からない」が流出する可能性のある情報としては「従業員、役員の個人情報」「インターネットバンキング関連」「取引先の連絡文、取引実績等、実際の取引として必ずしも一致しない」 ・ 技術資料の流出、BtoC 部門における個人情報の流出から販売事業の停止など ● ランサムウェアによる被害を受けた会社 <ul style="list-style-type: none"> ・ 特にない ・ 不明 ・ 分かりません ・ 情報漏洩はまだ、してないと思うが漏洩したら会社の経営に大損害 ・ 社外秘の図面情報が流出するかと思います ・ 顧客の信頼の失墜と取引停止、最悪の場合経営危機に至る ● 共有フォルダへの感染拡大の被害を受けた会社 <ul style="list-style-type: none"> ・ 事業の一時的な停止（最大1週間程度）、信頼の失墜、売上額の減少、採用へのダメージ ● マルウェア感染によるデータ破壊を受けた会社 <ul style="list-style-type: none"> ・ 顧客・取引先との仕事内容や金額、当社の財務状況 ● マルウェア感染によるその他被害を受けた会社 <ul style="list-style-type: none"> ・ 億単位の賠償 ・ 取引先（お客様）との取引停止 ● 不審メール受信による被害を受けた会社 <ul style="list-style-type: none"> ・ 顧客情報最大 3000 人の漏洩リスク、社員の個人情報の謝罪、または賠償の費用 ・ 想定できていない ● なりすましメール（発信）による被害を受けた会社

- ・ 自社を取り巻く会社に迷惑を掛け信頼を落とす、場合によっては、損害賠償が生じる
- なりすましメール（受信）による被害を受けた会社
 - ・ 不明
- メール乗っ取り被害を受けた会社
 - ・ 情報量が多いため想像がつかない
 - ・ 売り上げ半分
- フィッシングメールの被害を受けた会社
 - ・ 5000万円（年商10億円～）
 - ・ **取引停止により利益損失**
 - ・ 内容による
- メール喪失を受けた会社
 - ・ 金額的な面はわからないが、取引先への電話や詫言状、担当の時間と労力がかかると考えている
- 個人のメールアドレスへのサービス妨害攻撃を受けた会社
 - ・ 個人のメールアドレスに攻撃されたので「無い」と思っている
- 問い合わせメールアドレスへの大量メールを受けた会社
 - ・ 取引先からの**品質管理能力の疑義**、**最悪損害賠償請求**
- サービス妨害攻撃による業務停止(メール・VPNの利用不可)を受けた会社
 - ・ 被害は大きい
 - ・ 倒産
- 標的型メールの攻撃を受けた会社
 - ・ 想定していない
- OS起動しなくなった会社
 - ・ どの程度まで「大丈夫」が判断困難
- 公開サイト侵害・改ざん対処
 - ・ 現状は軽微
- 特に被害がない会社
 - ・ **想定できていない**
 - ・ 想定していない
 - ・ わからない
 - ・ わかりません
 - ・ **社会的信用失墜**、取引先減少、新卒人材減少、実数のイメージはできない
 - ・ 信頼失墜、被害の拡大
 - ・ 信頼をそこねると売り上げは落ちる
 - ・ 取引先からの信頼失墜、取引停止、賠償責任
 - ・ 取引先企業の信用を失う
 - ・ 数千万円から数億円の実被害が出ると想定している
 - ・ 取引停止、賠償、社員の士気低下、離職、社会的制裁、金額的には数千万～数十億

- ・ 売り上げや財務データ流出、客先の技術、営業データ流出による損害賠償、新規受注低下や同業他社との競争不利状態

3.5 セキュリティ対応を進める上で、日々の監視サービスを望まれる企業は54%、復旧サービスは49%と半数がメリットを感じると回答された。しかし、被害に対する補償（サイバー保険）は29%にとどまった。

日々の監視サービス

全般的に期待されているが従業員数が多くなると期待も高くなる。

平均 / Q3.5.1	従業員数										総計
業種	~5	~10	~20	~50	~100	~200	~300	~500	~1000	~5000	
製造業(防衛産業)		100%									100%
複合サービス事業					100%						100%
医療、福祉							100%				100%
製造業(自動車)						100%	100%	50%			75%
金融業、保険業	100%	50%	100%	0%							71%
サービス業(他に分類されないもの)	50%	100%	0%	100%	50%	100%					64%
製造業(その他)		100%	50%	36%	50%	64%	82%	50%	100%	0%	58%
生活関連サービス業・娯楽業					0%			100%			50%
その他	0%	100%		33%		67%					50%
運輸業、郵便業				50%							50%
建設業		0%	0%	100%							50%
卸売業、小売業	50%	0%	40%	50%	50%	33%	100%	0%			45%
学術研究・専門・技術サービス業	50%	0%		100%	100%						43%
情報通信業	0%		50%		0%			100%			33%
不動産業、物品賃貸業			0%								0%
電気・ガス・熱供給・水道製造業							0%				0%
総計	46%	50%	41%	46%	49%	65%	80%	55%	100%	0%	54%

復旧サービス

全般的に期待されているが従業員数が 200~500 の規模が特に期待されている。

平均 / Q3.5.2	従業員数										総計
業種	~5	~10	~20	~50	~100	~200	~300	~500	~1000	~5000	
複合サービス事業					100%						100%
製造業(防衛産業)		100%									100%
不動産業、物品賃貸業			100%								100%
医療、福祉							100%				100%
金融業、保険業	100%	100%	50%	0%							71%
情報通信業	50%		75%		50%			0%			56%
製造業(その他)		100%	50%	29%	50%	50%	73%	83%	0%	0%	51%
生活関連サービス業・娯楽業					0%			100%			50%
製造業(自動車)						0%	100%	50%			50%
サービス業(他に分類されないもの)	50%	50%	0%	100%	0%	100%					45%
卸売業、小売業	0%	0%	40%	50%	58%	33%	100%	100%			45%
その他	0%	0%		33%		67%					38%
学術研究・専門・技術サービス業	50%	0%		0%	100%						29%
建設業		0%	0%	50%							25%
電気・ガス・熱供給・水道製造業							0%				0%
運輸業、郵便業				0%							0%
総計	38%	42%	47%	31%	51%	51%	73%	73%	0%	0%	49%

被害に対する補償（サイバー保険）

監視・復旧より期待が少ないが、従業員数に関わらず期待がある。

平均 / Q3.5.3	従業員数										総計
業種	~5	~10	~20	~50	~100	~200	~300	~500	~1000	~5000	
サービス業(他に分類されないもの)	100%	50%	50%	100%	50%	50%					64%
その他	0%	0%		33%		33%					25%
医療、福祉							0%				0%
運輸業、郵便業				0%							0%
卸売業、小売業	25%	100%	40%	50%	17%	33%	0%	0%			28%
学術研究・専門・技術サービス業	50%	0%		100%	0%						29%
金融業、保険業	0%	50%	50%	0%							29%
建設業		0%	0%	50%							25%
情報通信業	50%		25%		50%			0%			33%
生活関連サービス業・娯楽業					0%			0%			0%
製造業(その他)		100%	0%	21%	13%	36%	27%	50%	0%	0%	28%
製造業(自動車)						0%	0%	50%			25%
製造業(防衛産業)		0%									0%
電気・ガス・熱供給・水道製造業							100%				100%
不動産業、物品賃貸業			0%								0%
複合サービス事業					0%						0%
総計	38%	33%	29%	31%	17%	35%	27%	36%	0%	0%	29%

3.6 情報漏洩が発生した場合に、取引先、顧客、市場等に対してとられる可能性のある対応内容は下記のとおり。

- 専門家へ相談
 - ・ 弁護士さんなどに相談の上決定になろうかと思えます
- サービス停止
 - ・ お詫びや通販サイトの停止
 - ・ 漏洩した情報の公開、関連会社への通達、サーバのコネクション遮断
- 調査・報告
 - ・ 報告と送信済みメールのチェック
 - ・ 極力、全内容を開示
 - ・ 告知
 - ・ 公表
 - ・ 報告
 - ・ 顧客への連絡、および報告書（対策、影響など）の提出
 - ・ 謝罪、補償、漏洩原因を分析し、対策を講じ、説明
 - ・ 偽りなく正確な情報公開と謝罪
 - ・ 攻撃方法の周知、二次被害を外に出さない、通知
 - ・ 情報の開示、補償に関しては不明
 - ・ 取引先、お客様への説明責任、保証
 - ・ 迅速な連絡対応・経過報告等
 - ・ 取引先（お客様）への連絡、情報開示、今後の対策結果を報告
- 謝罪・賠償・対策の報告
 - ・ 事象の説明、今後の対策の通知、
場合によっては費用を支払う
 - ・ 取引先に直接謝罪、顧客・市場へ HP 上でのお詫び
 - ・ 個別のお詫びや補償、記者会見
 - ・ 詫び状や社告等に対応
 - ・ 謝罪告知
 - ・ ①お詫びに回る、②サービス料の減額
 - ・ 早期の連絡、被害への補償、公式な謝罪
 - ・ 事実案内とお詫び、今後の対応について
 - ・ 謝罪補償
 - ・ 謝罪、損害賠償
 - ・ 損害賠償 ×3
 - ・ 賠償
 - ・ 謝罪 ×2
 - ・ 謝罪メール
 - ・ 謝罪と信用回復
 - ・ 謝罪後に個別対応
 - ・ 謝罪、損害賠償
 - ・ 謝罪と場合によっては賠償の可能性

- ・ 客先への謝罪くらいかと
 - ・ 損害賠償等に発展する可能性があるかと考えている
 - ・ 謝罪、再発防止
 - ・ 公開、謝罪、賠償、復旧、リビルド、情報遮断
 - ・ 電話での謝罪、HPでの詫言告知
 - ・ 取引先に連絡をし、二次被害がないか確認、さらに個々の被害状況の確認を行い、対応しなければならない
 - ・ 現状漏洩の経験がないので金銭的問題が出る可能性はあると思う
 - ・ 自社のセキュリティ対策に関する取組みを公開し、一定の改善を行う、賠償の交渉に応じる
 - ・ 謝罪はしますが、責任は免除していただきます
- 不明
- ・ 不明 ×3
 - ・ 分からない ×5
 - ・ よくわからない
 - ・ 想像がつかない
 - ・ 今の状況だと発生してみないと分かりません
 - ・ 未考慮
 - ・ 考慮していない
 - ・ 規定していない、想定していない
 - ・ 明確な規定なし
 - ・ 必要に応じて

4.4 セキュリティ対策、運用に関わる「担当者」は平均 1.5 名である。
(単位：担当者数)

平均 / Q4.4 業種	従業員数										
	~5	~10	~20	~50	~100	~200	~300	~500	~1000	~5000	総計
医療、福祉							5.0				5.0
情報通信業	1.5		1.5	1.0	4.0			4.0			2.0
電気・ガス・熱供給・水道製造業							2.0				2.0
製造業(自動車)						1.0	1.0	3.0			2.0
卸売業、小売業	0.8	0.0	0.2	1.5	2.8	2.0	2.0	3.0			1.8
製造業(その他)		0.3	1.0	0.9	1.6	1.0	2.3	3.8	3.0	6.0	1.6
学術研究・専門・技術サービス業	0.5	1.0		3.0	1.0						1.2
その他	0.0	2.0		1.0	1.5						1.1
複合サービス事業					1.0						1.0
製造業(防衛産業)		1.0									1.0
生活関連サービス業・娯楽業					1.0			1.0			1.0
運輸業、郵便業				1.0							1.0
サービス業(他に分類されないもの)	0.0	1.0	0.5		1.0	2.5					1.0
建設業		0.0	1.0	2.0							1.0
金融業、保険業	0.5	0.0	1.5	1.0							0.7
不動産業、物品賃貸業			0.0								0.0
総計	0.6	0.6	0.8	1.1	2.1	1.3	2.3	3.4	3.0	6.0	1.5

従業員数が多い企業、年商の大きい企業は、セキュリティ担当者も自然と多くなる。200名以下は、概ね「1人情報システム担当者」の状態となっている。

【2回目のアンケート】

セキュリティ対策、運用に関わる担当者は平均 1.7 名、製造業（その他）の従業員数~100 名、~500 名、年商 10 億円以上の欄だけが「専任担当者」と回答があった。それ以外は他業務と兼務されている。

(単位：担当者数)

平均 / セキュリティ担当者(名)	従業員数								年商			総計
	~10	~20	~50	~100	~200	~300	~500	~1000	~1億円	1~10億円	10億円以上	
情報通信業				3.0					3.0			3.0
学術研究・専門・技術サービス業				2.0					2.0	2.0		2.0
教育、学習支援業	2.0								2.0	2.0		2.0
製造業(その他)	0.2	1.0	1.5	1.0	1.6	1.7	2.0	5.0	1.7	1.5	1.7	1.7
製造業(自動車)				2.0	1.0				1.5		1.5	1.5
卸売業、小売業サービス業			1.0		2.0				1.5	1.0	2.0	1.5
製造業(防衛産業)	1.0								1.0	1.0		1.0
宿泊業						1.0			1.0		1.0	1.0
総計	1.1	1.0	1.4	1.8	1.6	2.0	5.0	1.7	2.0	1.4	1.7	1.7

5 サプライチェーン

5.1 取引企業から取引にあたり、一定レベルのセキュリティ対策が要件に含まれているケースがある企業は、42%だった。製造業(その他)、医療・福祉、金融業・保険業が多い傾向にある。

平均 / Q5.1	従業員数										総計
業種	~5	~10	~20	~50	~100	~200	~300	~500	~1000	~5000	
製造業(防衛産業)		100%									100%
医療、福祉							100%				100%
金融業、保険業	100%	50%	50%	100%							71%
学術研究・専門・技術サービス業	0%	67%		100%	100%						57%
サービス業(他に分類されないもの)	100%	50%	50%		50%	50%					56%
情報通信業	100%		0%	100%	100%						50%
製造業(その他)		0%	100%	33%	47%	42%	67%	17%	100%	0%	44%
卸売業、小売業	25%	0%	0%	100%	40%	67%	100%				38%
建設業		0%	100%	0%							25%
その他	0%	0%		50%		0%					22%
電気・ガス・熱供給・水道製造業							0%				0%
複合サービス事業					0%						0%
生活関連サービス業・娯楽業					0%			0%			0%
不動産業、物品賃貸業				0%							0%
運輸業、郵便業				0%							0%
サービス業(他に分類されないもの)	0%			0%							0%
製造業(自動車)						0%	0%				0%
総計	46%	42%	29%	42%	45%	39%	62%	14%	100%	0%	42%

5.2 現在の対策でその要件を満たしている企業は、73%だった。

平均 / Q5.2	従業員数										総計
業種	~5	~10	~20	~50	~100	~200	~300	~500	~1000		
生活関連サービス業・娯楽業								100%			100%
情報通信業	100%		100%	100%	100%						100%
製造業(防衛産業)		100%									100%
医療、福祉							100%				100%
金融業、保険業	100%	100%	100%	100%							100%
学術研究・専門・技術サービス業		100%		100%	0%						75%
サービス業(他に分類されないもの)	100%	100%	100%	100%	100%	0%					75%
製造業(その他)		0%	50%	71%	70%	73%	83%	100%	100%		73%
その他	0%			100%							67%
卸売業、小売業	50%		67%	50%	71%	50%	100%				65%
建設業		100%	0%								50%
不動産業、物品賃貸業			0%								0%
運輸業、郵便業				0%							0%
総計	78%	86%	60%	75%	70%	63%	88%	100%	100%		73%

5.3 満たしていないものは下記の要件。

業種	従業員数	理由
製造業（その他）	～20	個人情報保護に対する規定・運用
	～50	パスワード付きの添付ファイル受送信
	～100	メールがみられる
		ウイルス対策ソフト導入
		セキュリティ運用規定の策定等
	～200	OSのバージョンなど
～300	個人情報に関する運用等	
卸売業、小売業	～100	機密文書の暗号化と社内規定の有無
	～200	仕入れ先、委託先情報
サービス業 （他に分類されないもの）	～200	教育
医療、福祉	～300	覚えていません

6 サイバー保険

6.1 サイバー保険の存在を知っている企業は、33%にとどまった。

平均 / Q6.1 業種	従業員数										総計
	～5	～10	～20	～50	～100	～200	～300	～500	～1000	～5000	
医療、福祉							100%				100%
金融業、保険業	100%	100%	100%	100%							100%
学術研究・専門・技術サービス業	100%	33%		100%	0%						57%
サービス業(他に分類されないもの)	0%	100%	50%	100%	0%	100%					55%
生活関連サービス業・娯楽業					0%			100%			50%
情報通信業	50%		25%	0%	100%			0%			40%
卸売業、小売業	25%	0%	0%	50%	25%	67%	100%	0%			28%
製造業(その他)		0%	0%	29%	19%	22%	36%	33%	100%	100%	27%
製造業(自動車)						0%	100%	0%			25%
建設業		0%	0%	50%							25%
その他	0%	0%		25%		0%					11%
不動産業、物品賃貸業			0%								0%
電気・ガス・熱供給・水道製造業							0%				0%
運輸業、郵便業				0%							0%
複合サービス事業					0%						0%
製造業(防衛産業)		0%									0%
総計	46%	42%	24%	36%	23%	28%	47%	27%	100%	100%	33%

6.2 既存のサイバー保険やサービスの価格帯は高いと思われる企業は 46%に達している。



高い

業種	従業員数	理由
サービス業	～200	思う
卸売業、小売業	～200	はい
金融業、保険業	～10	実際の被害額と被害状況が大手の企業ばかりで関係ないと思っている、だから高いと感じる
	～20	高いと思う
情報通信業	～20	高いと思います
	～100	高い
製造業（その他）	～100	高い
	～100	高いイメージがある
	～100	大体高いイメージ
	～200	本格的に検討していないが高いイメージ
	～200	高い × 2
	～300	高いと思う
	～500	高い
	～500	高いと思う
製造業（自動車）	～500	おそらく高いのではないのでしょうか

判らない

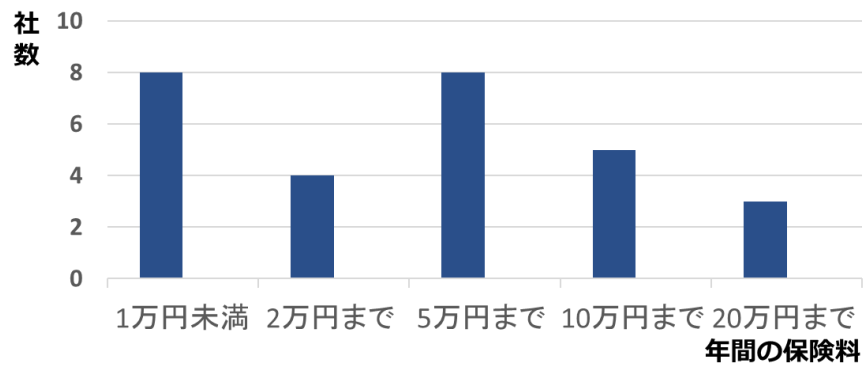
業種	従業員数	理由
卸売業、小売業	～10	わからない
	～100	不明
	～100	価格帯の調査を行っていない
	～300	不明
学術研究・専門・技術サービス業	～5	調査、検討したことがないので判断できない
	～50	詳細理解しておらず
建設業	～50	詳細はまだわかっていない
製造業	～50	内容次第
	～100	不明
	～100	わからない
	～200	わからない
	～300	わかりません
	～1000	価格まではしらない
建設業	～50	わかりません
情報通信業	～5	まったくわからない状況

高くない

業種	従業員数	理由
サービス業	～10	思わない
	～20	思わない
情報通信業	～5	高くはない
生活関連サービス	～500	適正
製造業（その他）	～300	高いと思わない
医療、福祉	～300	いいえ

【2回目のアンケート】

年間の保険料は下記のような分布である。



次のコメントがあった。

- ・ 未検討であるため回答不可
- ・ 正直話題にしたことがないのでわからない
- ・ またこういった類のものは、痛みを伴わないと優先度が上がらないので

6.3 サイバー攻撃の被害にあった場合は多額の費用が必要となるケースがある中、メリットを感じる補償内容は、損害賠償が36%、調査・復旧が24%、損失補填が11%、対策費用が8%、弁護士費用が3%、その他が3%、特にわからないが15%ある。

● 損害賠償（36%）

業種	従業員数	内容
サービス業	～10	セキュリティ強化費用
製造業（その他）	～300	問題のあった事項への対策費用
		セキュリティ対策改善のための費用

● 調査・復旧（24%）

業種	従業員数	内容
卸売業、小売業	～200	復旧
製造業（自動車）	～500	復元作業の代行など
製造業（その他）	～100	費用よりデータ
	～300	調査、復旧
	～300	データの復旧
		データ復旧
～500	復旧費用	
卸売業、小売業	～5	データの復旧

● 損失補填（11%）

業種	従業員数	内容
卸売業、小売業	～200	損失の補填
製造業（自動車）	～300	サーバ、IoT 機器のついた工場設備が停止することによる損害（売上損失額に対する）
製造業（その他）	～200	社内への保障
製造業（その他）	～300	サービス停止に対する売上補償

● 対策費用（8%）

業種	従業員数	内容
サービス業	～10	セキュリティ強化費用
製造業（その他）	～300	問題のあった事項への対策費用
		セキュリティ対策改善のための費用

● 弁護士費用（3%）

業種	従業員数	内容
製造業（その他）	～300	弁護士費用等の対外費用

● その他（3%）

業種	従業員数	内容
製造業（その他）	～5000	被害証明が難しく本当に保険が出るか不安である

● 特にない・分からない (15%)

業種	従業員数	内容
サービス業	～20	特にない
卸売業、小売業	～10	わからない
製造業（その他）	～300	分からない
建設業	～50	わかりません
その他	～10	わからない

【2回目のアンケート】

保険で想定する損害賠償は下記のとおり甲乙付け難い（複数回答あり）

賠償内容	件数
製造ライン停止による取引先への賠償	18
設計図面など機微情報の漏洩による情報元への賠償	18
サービス停止に伴う顧客・取引先への賠償	16
大量の個人情報漏洩による個人への賠償	17
未検討であるため回答不可	1

【2回目のアンケート】

加入の一番の決め手となるものは、保険料水準、付帯サービス（緊急時のコンシェルジュ機能など）の順番である。

加入の決め手	件数
保険料水準	20
付帯サービス（緊急時の対応のコンシェルジュ機能など）	15
加入方法の簡便さ	0
その他	0

7 損失想定額のヒアリング（参考）

機微な情報を持っている業種や、規模の大きな会社は損失想定額も高額となる。

（単位：円）

平均 / 損失想定額	従業員数										総計
業種	～5	～10	～20	～50	～100	～200	～300	～500	～1000	～5000	
医療、福祉							-48,060,000,000				-48,060,000,000
その他				-189,300,000		-36,000,000,000					-18,094,650,000
生活関連サービス業・娯楽業								-513,000,000			-513,000,000
電気・ガス・熱供給・水道製造業							-312,780,000				-312,780,000
サービス業（他に分類されないもの）	-6,000,000	-1,200,000	-170,000,000	0		-1,199,988,000					-275,437,600
製造業（その他）		-360,000		-21,036,250	-23,841,091	-311,379,067	-392,072,000	-53,020,000	-12,000,000	-524,000,000	-190,312,163
製造業（自動車）						0	-120,000,000	-319,000,000			-146,333,333
卸売業、小売業	-4,400,000		-40,662,500		-77,526,725	-764,750,000	-124,000,000	-14,700,000			-135,835,903
金融業、保険業	-38,400,000	-25,380,000	-19,000,000	-216,000,000							-59,363,333
不動産業、物品賃貸業			-41,000,000								-41,000,000
製造業（防衛産業）		-15,300,000									-15,300,000
建設業		-1,750,000	-3,600,000	-17,400,000							-10,037,500
学術研究・専門・技術サービス業	-6,000,000	-8,800,000		0	-4,524,000						-6,154,000
情報通信業	-60,000		-5,556,667	-600,000	-6,320,000						-3,753,750
運輸業、郵便業				-1,680,000							-1,680,000
総計	-11,346,667	-8,798,750	-35,993,333	-47,057,059	-37,228,818	-3,780,960,667	-4,011,186,769	-167,626,667	-12,000,000	-524,000,000	-1,252,188,318

※ アンケートで頂いた個人情報種別毎の保有数、ビジネス機会損失、法令違反（GDPR）、事故対応費用、純利益への影響、時価総額の減少の各情報を元に、一般社団法人 日本サイバーセキュリティ・イノベーション委員会が公開する「サイバーリスク指標モデル 想定損失額の目安（簡易版）」にて算出を行った。

※ 回答が未記載である項目は、損失に計上していない。

※ 業務停止期間は、5日間と想定する。

(エ) ベンチマーク診断 (IPA 自社診断シート)

5分でできる！情報セキュリティ自社診断の回答：有効回答数 86 社

先頭の平均点の表を除き、Q1～Q25 の表中は、各社の「4：実施している」「2：一部実施している」「0：実施していない/わからない」の回答を平均したものとなる。

① 診断結果の傾向

平均	平均は 51 点であり、対策が行き届いていないとされる 69 点以下が殆どで、それ以上の得点は「金融・保険業」「情報通信業」の 2 業種である。																																																																																																																																																										
	<table border="1"> <thead> <tr> <th>平均 / 総合点</th> <th colspan="9">従業員数</th> <th></th> </tr> <tr> <th>業種</th> <th>～5</th> <th>～10</th> <th>～20</th> <th>～50</th> <th>～100</th> <th>～200</th> <th>～300</th> <th>～500</th> <th>～900</th> <th>総計</th> </tr> </thead> <tbody> <tr> <td>金融業・保険業</td> <td>82</td> <td>98</td> <td>74</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>85</td> </tr> <tr> <td>情報通信業</td> <td>66</td> <td></td> <td>84</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>72</td> </tr> <tr> <td>学術研究・専門・技術サービス業</td> <td>76</td> <td>66</td> <td></td> <td>60</td> <td>52</td> <td></td> <td></td> <td></td> <td></td> <td>64</td> </tr> <tr> <td>飲食業</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>54</td> <td></td> <td></td> <td>54</td> </tr> <tr> <td>サービス業</td> <td>72</td> <td></td> <td>57</td> <td>62</td> <td>24</td> <td>44</td> <td></td> <td></td> <td></td> <td>53</td> </tr> <tr> <td>卸売業・小売業</td> <td>50</td> <td></td> <td>54</td> <td>44</td> <td>53</td> <td>62</td> <td></td> <td></td> <td></td> <td>52</td> </tr> <tr> <td>建設業</td> <td>90</td> <td></td> <td></td> <td>19</td> <td></td> <td></td> <td>64</td> <td></td> <td></td> <td>48</td> </tr> <tr> <td>製造業</td> <td></td> <td>46</td> <td>53</td> <td>47</td> <td>46</td> <td>44</td> <td>50</td> <td>61</td> <td>62</td> <td>48</td> </tr> <tr> <td>運輸業・郵便業</td> <td></td> <td></td> <td></td> <td>38</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>38</td> </tr> <tr> <td>電気・ガス・熱供給・水道業</td> <td></td> <td></td> <td></td> <td>34</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>34</td> </tr> <tr> <td>複合サービス事業</td> <td>18</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>18</td> </tr> <tr> <td>総計</td> <td>61</td> <td>61</td> <td>61</td> <td>44</td> <td>46</td> <td>45</td> <td>52</td> <td>61</td> <td>62</td> <td>51</td> </tr> </tbody> </table>	平均 / 総合点	従業員数										業種	～5	～10	～20	～50	～100	～200	～300	～500	～900	総計	金融業・保険業	82	98	74							85	情報通信業	66		84							72	学術研究・専門・技術サービス業	76	66		60	52					64	飲食業							54			54	サービス業	72		57	62	24	44				53	卸売業・小売業	50		54	44	53	62				52	建設業	90			19			64			48	製造業		46	53	47	46	44	50	61	62	48	運輸業・郵便業				38						38	電気・ガス・熱供給・水道業				34						34	複合サービス事業	18									18	総計	61	61	61	44	46	45	52	61	62	51
平均 / 総合点	従業員数																																																																																																																																																										
業種	～5	～10	～20	～50	～100	～200	～300	～500	～900	総計																																																																																																																																																	
金融業・保険業	82	98	74							85																																																																																																																																																	
情報通信業	66		84							72																																																																																																																																																	
学術研究・専門・技術サービス業	76	66		60	52					64																																																																																																																																																	
飲食業							54			54																																																																																																																																																	
サービス業	72		57	62	24	44				53																																																																																																																																																	
卸売業・小売業	50		54	44	53	62				52																																																																																																																																																	
建設業	90			19			64			48																																																																																																																																																	
製造業		46	53	47	46	44	50	61	62	48																																																																																																																																																	
運輸業・郵便業				38						38																																																																																																																																																	
電気・ガス・熱供給・水道業				34						34																																																																																																																																																	
複合サービス事業	18									18																																																																																																																																																	
総計	61	61	61	44	46	45	52	61	62	51																																																																																																																																																	
Q1	「Windows Update を行うなどのように、常に OS やソフトウェアを安全な状態にしている」の問いは、平均 73 点である。一部の企業を除き、概ね実施されている。																																																																																																																																																										
	<table border="1"> <thead> <tr> <th>平均 / Q1</th> <th colspan="9">従業員数</th> <th></th> </tr> <tr> <th>業種</th> <th>～5</th> <th>～10</th> <th>～20</th> <th>～50</th> <th>～100</th> <th>～200</th> <th>～300</th> <th>～500</th> <th>～900</th> <th>総計</th> </tr> </thead> <tbody> <tr> <td>運輸業・郵便業</td> <td></td> <td></td> <td></td> <td>4.0</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>4.0</td> </tr> <tr> <td>電気・ガス・熱供給・水道業</td> <td></td> <td></td> <td></td> <td>4.0</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>4.0</td> </tr> <tr> <td>サービス業</td> <td>4.0</td> <td></td> <td>3.0</td> <td>4.0</td> <td>4.0</td> <td>4.0</td> <td></td> <td></td> <td></td> <td>3.7</td> </tr> <tr> <td>建設業</td> <td>4.0</td> <td></td> <td></td> <td>3.0</td> <td></td> <td></td> <td>4.0</td> <td></td> <td></td> <td>3.5</td> </tr> <tr> <td>情報通信業</td> <td>3.0</td> <td></td> <td>4.0</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>3.3</td> </tr> <tr> <td>金融業・保険業</td> <td>4.0</td> <td>4.0</td> <td>2.0</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>3.3</td> </tr> <tr> <td>学術研究・専門・技術サービス業</td> <td>4.0</td> <td>4.0</td> <td></td> <td>2.0</td> <td>2.0</td> <td></td> <td></td> <td></td> <td></td> <td>3.2</td> </tr> <tr> <td>卸売業・小売業</td> <td>2.5</td> <td></td> <td>4.0</td> <td>4.0</td> <td>2.0</td> <td></td> <td></td> <td></td> <td></td> <td>2.8</td> </tr> <tr> <td>製造業</td> <td></td> <td>3.3</td> <td>3.3</td> <td>1.8</td> <td>3.3</td> <td>2.9</td> <td>2.3</td> <td>3.0</td> <td>2.0</td> <td>2.7</td> </tr> <tr> <td>飲食業</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>2.0</td> <td></td> <td></td> <td>2.0</td> </tr> <tr> <td>複合サービス事業</td> <td>0.0</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>0.0</td> </tr> <tr> <td>総計</td> <td>2.9</td> <td>3.7</td> <td>3.3</td> <td>2.4</td> <td>3.0</td> <td>3.0</td> <td>2.4</td> <td>3.0</td> <td>2.0</td> <td>2.9</td> </tr> </tbody> </table>	平均 / Q1	従業員数										業種	～5	～10	～20	～50	～100	～200	～300	～500	～900	総計	運輸業・郵便業				4.0						4.0	電気・ガス・熱供給・水道業				4.0						4.0	サービス業	4.0		3.0	4.0	4.0	4.0				3.7	建設業	4.0			3.0			4.0			3.5	情報通信業	3.0		4.0							3.3	金融業・保険業	4.0	4.0	2.0							3.3	学術研究・専門・技術サービス業	4.0	4.0		2.0	2.0					3.2	卸売業・小売業	2.5		4.0	4.0	2.0					2.8	製造業		3.3	3.3	1.8	3.3	2.9	2.3	3.0	2.0	2.7	飲食業							2.0			2.0	複合サービス事業	0.0									0.0	総計	2.9	3.7	3.3	2.4	3.0	3.0	2.4	3.0	2.0	2.9
平均 / Q1	従業員数																																																																																																																																																										
業種	～5	～10	～20	～50	～100	～200	～300	～500	～900	総計																																																																																																																																																	
運輸業・郵便業				4.0						4.0																																																																																																																																																	
電気・ガス・熱供給・水道業				4.0						4.0																																																																																																																																																	
サービス業	4.0		3.0	4.0	4.0	4.0				3.7																																																																																																																																																	
建設業	4.0			3.0			4.0			3.5																																																																																																																																																	
情報通信業	3.0		4.0							3.3																																																																																																																																																	
金融業・保険業	4.0	4.0	2.0							3.3																																																																																																																																																	
学術研究・専門・技術サービス業	4.0	4.0		2.0	2.0					3.2																																																																																																																																																	
卸売業・小売業	2.5		4.0	4.0	2.0					2.8																																																																																																																																																	
製造業		3.3	3.3	1.8	3.3	2.9	2.3	3.0	2.0	2.7																																																																																																																																																	
飲食業							2.0			2.0																																																																																																																																																	
複合サービス事業	0.0									0.0																																																																																																																																																	
総計	2.9	3.7	3.3	2.4	3.0	3.0	2.4	3.0	2.0	2.9																																																																																																																																																	

Q2 「パソコンにはウイルス対策ソフトを入れてウイルス定義ファイルを自動更新するなどのように、パソコンをウイルスから守るための対策を行っていますか？」との問いは、平均 83 点である。「電気・ガス・熱供給・水道業」「建設業」「飲食業」「金融業・保険業」の業種では十分な対策を行っていた。

平均 / Q2	従業員数									総計
	~5	~10	~20	~50	~100	~200	~300	~500	~900	
業種										
電気・ガス・熱供給・水道業				4.0						4.0
建設業	4.0			4.0			4.0			4.0
飲食業							4.0			4.0
金融業・保険業	4.0	4.0	4.0							4.0
卸売業・小売業	3.0		4.0	4.0	4.0	4.0				3.6
サービス業	4.0		2.0	4.0	4.0	4.0				3.3
情報通信業	3.0		4.0							3.3
製造業		4.0	3.3	2.2	3.0	3.6	3.7	4.0	4.0	3.3
学術研究・専門・技術サービス業	4.0	3.0		2.0	4.0					3.2
運輸業・郵便業				2.0						2.0
複合サービス事業	0.0									0.0
総計	3.1	3.7	3.3	2.7	3.4	3.6	3.8	4.0	4.0	3.3

Q3 「パスワードは自分の名前、電話番号、誕生日など推測されやすいものを避けて複数のウェブサービスで使い回しをしないなどのように、強固なパスワードを設定していますか？」との問いは、平均 55 点である。「情報通信業」「金融・保険業」では、概ね注意されている。

平均 / Q3	従業員数									総計
	~5	~10	~20	~50	~100	~200	~300	~500	~900	
業種										
情報通信業	4.0		2.0							3.3
金融業・保険業	4.0	4.0	2.0							3.3
学術研究・専門・技術サービス業	0.0	4.0		2.0	4.0					2.8
卸売業・小売業	2.5		2.0	2.0	2.0	2.0				2.2
製造業		2.7	2.0	2.5	2.0	1.7	1.7	3.0	2.0	2.1
運輸業・郵便業				2.0						2.0
飲食業							2.0			2.0
電気・ガス・熱供給・水道業				2.0						2.0
サービス業	2.0		1.0	2.0	4.0	0.0				1.7
建設業	4.0			0.0			2.0			1.5
複合サービス事業	0.0									0.0
総計	2.5	3.3	1.8	2.1	2.3	1.6	1.8	3.0	2.0	2.2

Q4 「ネットワーク接続の複合機やハードディスクの共有設定を必要な人だけに限定するなどのように、重要情報に対する適切なアクセス制限を行っていますか？」との問いは、平均 65 点である。

平均 / Q4	従業員数									総計
	~5	~10	~20	~50	~100	~200	~300	~500	~900	
業種										
電気・ガス・熱供給・水道業				4.0						4.0
飲食業							4.0			4.0
学術研究・専門・技術サービス業	4.0	3.0		4.0	4.0					3.6
情報通信業	3.0		4.0							3.3
金融業・保険業	2.0	4.0	4.0							3.3
建設業	4.0			1.0			4.0			2.5
卸売業・小売業	2.5		4.0	2.0	1.0	4.0				2.4
製造業		1.3	2.0	2.2	2.5	2.8	2.0	3.0	4.0	2.4
サービス業	2.0		1.0	4.0	4.0	2.0				2.3
運輸業・郵便業				2.0						2.0
複合サービス事業	0.0									0.0
総計	2.5	2.3	2.5	2.3	2.5	2.8	2.4	3.0	4.0	2.6

Q5 「利用中のウェブサービスや製品メーカーが発信するセキュリティ注意喚起を確認して社内共有するなどのように、新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？」との問いは、平均 35 点にとどまった。他業務と兼務されている担当者としては、注意喚起などをウォッチしつづけることが難しいと推察する。

平均 / Q5	従業員数									総計
	~5	~10	~20	~50	~100	~200	~300	~500	~900	
業種										
学術研究・専門・技術サービス業	4.0	1.0		4.0	4.0					2.8
建設業	4.0			1.0			2.0			2.0
情報通信業	2.0		2.0							2.0
金融業・保険業	2.0	4.0	0.0							2.0
製造業		1.3	1.3	1.8	1.3	1.3	1.4	1.5	2.0	1.5
サービス業	2.0		0.0	2.0	2.0	0.0				1.0
卸売業・小売業	0.5		2.0	0.0	0.0	2.0				0.7
複合サービス事業	0.0									0.0
電気・ガス・熱供給・水道業				0.0						0.0
飲食業							0.0			0.0
運輸業・郵便業				0.0						0.0
総計	1.6	1.7	1.0	1.6	1.3	1.3	1.3	1.5	2.0	1.4

Q6 「受信した不審な電子メールの添付ファイルを安易に開いたり本文中のリンクを安易に参照したりしないようにするなど、電子メールを介したウイルス感染に気をつけていますか？」との問いは、平均 73 点であった。

平均 / Q6	従業員数									総計
	~5	~10	~20	~50	~100	~200	~300	~500	~900	
業種										
運輸業・郵便業				4.0						4.0
金融業・保険業	4.0	4.0	4.0							4.0
学術研究・専門・技術サービス業	4.0	3.0		4.0	4.0					3.6
情報通信業	3.0		4.0							3.3
サービス業	4.0		3.0	2.0	4.0	2.0				3.0
建設業	4.0			2.0			4.0			3.0
卸売業・小売業	3.5		4.0	4.0	1.0	2.0				2.9
製造業		3.3	2.7	2.9	2.5	2.4	3.1	2.5	4.0	2.7
飲食業							2.0			2.0
複合サービス事業	2.0									2.0
電気・ガス・熱供給・水道業				2.0						2.0
総計	3.5	3.3	3.3	2.9	2.5	2.4	3.1	2.5	4.0	2.9

Q7 「電子メールを送る前に目視にて送信アドレスを確認するなどのように、宛先の送信ミスを防ぐ仕組みを徹底していますか？」との問いは、平均 45 点にとどまった。

平均 / Q7	従業員数									総計
	~5	~10	~20	~50	~100	~200	~300	~500	~900	
業種										
サービス業	4.0		4.0	2.0	4.0	0.0				3.0
学術研究・専門・技術サービス業	4.0	2.0		4.0	2.0					2.8
金融業・保険業	4.0	4.0	0.0							2.7
情報通信業	2.0		2.0							2.0
電気・ガス・熱供給・水道業				2.0						2.0
飲食業							2.0			2.0
卸売業・小売業	2.5		0.0	2.0	1.0	4.0				2.0
製造業		1.3	2.7	2.5	1.3	0.9	2.0	1.0	2.0	1.6
建設業	4.0			0.0			2.0			1.5
複合サービス事業	0.0									0.0
運輸業・郵便業				0.0						0.0
総計	2.7	2.0	2.3	2.1	1.5	1.1	2.0	1.0	2.0	1.8

Q8 「重要情報をメールで送る時は重要情報を添付ファイルに書いてパスワード保護するなどのように、重要情報の保護をしていますか？」との問いは、平均 33 点にとどまった。

平均 / Q8	従業員数									総計
	~5	~10	~20	~50	~100	~200	~300	~500	~900	
業種										
情報通信業	3.0		4.0							3.3
電気・ガス・熱供給・水道業				2.0						2.0
サービス業	2.0		1.0	2.0	4.0	2.0				2.0
飲食業							2.0			2.0
学術研究・専門・技術サービス業	4.0	0.0		2.0	4.0					2.0
金融業・保険業	2.0	2.0	2.0							2.0
卸売業・小売業	1.5		2.0	0.0	2.0	2.0				1.6
建設業	4.0			0.0			2.0			1.5
製造業		0.7	1.3	0.7	0.8	0.8	1.4	2.0	0.0	1.0
複合サービス事業	0.0									0.0
運輸業・郵便業				0.0						0.0
総計	2.2	0.7	1.8	0.8	1.5	0.9	1.6	2.0	0.0	1.3

Q9 「無線 LAN を利用する時は強固な暗号化を必ず利用するなどのように、無線 LAN を安全に使うための対策をしていますか？」との問いは、平均 63 点である。

平均 / Q9	従業員数									総計
	~5	~10	~20	~50	~100	~200	~300	~500	~900	
業種										
飲食業							4.0			4.0
情報通信業	3.0		4.0							3.3
金融業・保険業	2.0	4.0	4.0							3.3
製造業		1.3	4.0	2.4	1.5	2.9	4.0	3.5	4.0	2.8
サービス業	2.0		3.0	0.0	4.0	4.0				2.7
学術研究・専門・技術サービス業	4.0	2.0		4.0	0.0					2.4
卸売業・小売業	1.0		0.0	2.0	2.0	4.0				1.6
建設業	4.0			0.0			2.0			1.5
運輸業・郵便業				0.0						0.0
複合サービス事業	0.0									0.0
電気・ガス・熱供給・水道業				0.0						0.0
総計	2.0	2.0	3.3	1.8	1.7	3.1	3.8	3.5	4.0	2.5

Q10 「業務端末でのウェブサイトの閲覧や SNS への書き込みに関するルールを決めておくなどのように、インターネットを介したトラブルへの対策をしていますか？」との問いは、平均 33 点にとどまった。

平均 / Q10	従業員数									総計
	~5	~10	~20	~50	~100	~200	~300	~500	~900	
業種										
金融業・保険業	4.0	4.0	0.0							2.7
学術研究・専門・技術サービス業	4.0	2.0		0.0	4.0					2.4
建設業	4.0			1.0			2.0			2.0
飲食業							2.0			2.0
運輸業・郵便業				2.0						2.0
情報通信業	2.0		2.0							2.0
サービス業	2.0		1.0	0.0	4.0	4.0				2.0
卸売業・小売業	1.0		0.0	2.0	0.0	4.0				1.1
製造業		0.0	2.0	1.1	0.3	0.9	1.1	1.5	2.0	1.0
複合サービス事業	0.0									0.0
電気・ガス・熱供給・水道業				0.0						0.0
総計	2.0	1.3	1.3	1.0	0.8	1.3	1.3	1.5	2.0	1.3

Q11 「重要情報のバックアップを定期的に行うなどのように、故障や誤操作などに備えて重要情報が消失しないような対策をしていますか？」との問いは、平均 75 点である。

平均 / Q11	従業員数									総計
	~5	~10	~20	~50	~100	~200	~300	~500	~900	
業種				4.0						4.0
運輸業・郵便業				4.0						4.0
情報通信業	3.0		4.0							3.3
金融業・保険業	2.0	4.0	4.0							3.3
製造業		2.0	2.7	3.1	3.5	3.3	2.9	3.5	4.0	3.2
建設業	4.0			2.0			4.0			3.0
卸売業・小売業	2.5		4.0	2.0	4.0	0.0				2.7
学術研究・専門・技術サービス業	4.0	2.0		0.0	4.0					2.4
サービス業	4.0		1.0	2.0	4.0	2.0				2.3
電気・ガス・熱供給・水道業				2.0						2.0
複合サービス事業	2.0									2.0
飲食業							2.0			2.0
総計	2.9	2.3	2.8	2.7	3.7	3.1	2.9	3.5	4.0	3.0

Q12 「重要情報を机の上に放置せず書庫に保管し施錠するなどのように、重要情報の紛失や漏洩を防止する対策をしていますか？」との問いは、平均 55 点である。

平均 / Q12	従業員数									総計
	~5	~10	~20	~50	~100	~200	~300	~500	~900	
業種										
金融業・保険業	4.0	4.0	4.0							4.0
サービス業	2.0		3.0	4.0	4.0	2.0				3.0
製造業		3.3	2.0	2.4	2.5	1.6	2.0	2.5	0.0	2.1
運輸業・郵便業				2.0						2.0
電気・ガス・熱供給・水道業				2.0						2.0
卸売業・小売業	2.0		2.0	2.0	2.0	2.0				2.0
情報通信業	2.0		2.0							2.0
学術研究・専門・技術サービス業	2.0	2.0		0.0	4.0					2.0
飲食業							2.0			2.0
建設業	4.0			0.0			2.0			1.5
複合サービス事業	0.0									0.0
総計	2.2	3.0	2.5	2.0	2.7	1.6	2.0	2.5	0.0	2.2

Q13 「重要情報を社外へ持ち出す時はパスワード保護や暗号化して肌身離さないなどのように、盗難や紛失の対策をしていますか？」との問いは、平均 35 点にとどまった。

平均 / Q13	従業員数									総計
	~5	~10	~20	~50	~100	~200	~300	~500	~900	
業種										
金融業・保険業	4.0	4.0	4.0							4.0
運輸業・郵便業				2.0						2.0
情報通信業	2.0		2.0							2.0
サービス業	2.0		2.0	2.0	4.0	0.0				2.0
学術研究・専門・技術サービス業	2.0	2.0		0.0	2.0					1.6
卸売業・小売業	2.0		0.0	0.0	2.0	2.0				1.6
建設業	4.0			0.0			2.0			1.5
製造業		1.3	1.3	2.0	0.3	0.3	1.1	3.0	2.0	1.1
飲食業							0.0			0.0
複合サービス事業	0.0									0.0
電気・ガス・熱供給・水道業				0.0						0.0
総計	2.2	2.0	1.8	1.4	1.0	0.4	1.1	3.0	2.0	1.4

Q14 「離席時にコンピュータのロック機能を利用するなどのように、他人に使われないようにしていますか？」との問いは、平均 43 点にとどまった。

平均 / Q14	従業員数									総計
業種	~5	~10	~20	~50	~100	~200	~300	~500	~900	
金融業・保険業	4.0	4.0	4.0							4.0
サービス業	4.0		2.0	4.0	4.0	2.0				3.0
学術研究・専門・技術サービス業	4.0	2.0		4.0	2.0					2.8
情報通信業	2.0		4.0							2.7
運輸業・郵便業				2.0						2.0
電気・ガス・熱供給・水道業				2.0						2.0
卸売業・小売業	2.0		0.0	2.0	2.0	0.0				1.6
建設業	4.0			0.0			2.0			1.5
製造業		2.0	2.0	0.9	1.0	1.3	1.1	2.0	4.0	1.3
複合サービス事業	0.0									0.0
飲食業							0.0			0.0
総計	2.5	2.3	2.3	1.3	1.5	1.3	1.1	2.0	4.0	1.7

Q15 「事務所で見知らぬ人を見かけたら声をかけるなどのように、無許可の人の立ち入りがないようにしていますか？」との問いは、平均 75 点である。

平均 / Q15	従業員数									総計
業種	~5	~10	~20	~50	~100	~200	~300	~500	~900	
電気・ガス・熱供給・水道業				4.0						4.0
サービス業	4.0		4.0	4.0	4.0	4.0				4.0
飲食業							4.0			4.0
金融業・保険業	4.0	4.0	4.0							4.0
卸売業・小売業	4.0		4.0	2.0	4.0	4.0				3.8
情報通信業	3.0		4.0							3.3
学術研究・専門・技術サービス業	4.0	2.0		4.0	4.0					3.2
製造業		4.0	2.7	3.5	3.0	2.7	1.7	2.0	2.0	2.8
建設業	4.0			2.0			2.0			2.5
複合サービス事業	2.0									2.0
運輸業・郵便業				2.0						2.0
総計	3.6	3.3	3.5	3.2	3.3	2.8	2.0	2.0	2.0	3.0

Q16 「退社時に机の上のノートパソコンや備品を引き出しに片付けて施錠するなどのように、盗難防止対策をしていますか？」との問いは、平均 25 点にとどまった。

平均 / Q16	従業員数									総計
業種	~5	~10	~20	~50	~100	~200	~300	~500	~900	
金融業・保険業	4.0	4.0	4.0							4.0
情報通信業	2.0		2.0							2.0
建設業	4.0			0.0			2.0			1.5
卸売業・小売業	1.0		2.0	4.0	1.0	0.0				1.3
サービス業	0.0		2.0	0.0	2.0	2.0				1.3
製造業		2.7	0.7	0.9	1.5	0.3	0.3	1.0	0.0	0.8
学術研究・専門・技術サービス業	0.0	2.0		0.0	0.0					0.8
複合サービス事業	0.0									0.0
電気・ガス・熱供給・水道業				0.0						0.0
飲食業							0.0			0.0
運輸業・郵便業				0.0						0.0
総計	1.5	2.7	1.8	0.8	1.3	0.4	0.4	1.0	0.0	1.0

Q17 「最終退出者は事務所を施錠し退出の記録（日時、退出者）を残すなどのように、事務所の施錠を管理していますか？」との問いは、平均 58 点である。

平均 / Q17	従業員数									
	～5	～10	～20	～50	～100	～200	～300	～500	～900	総計
業種										
金融業・保険業	4.0	4.0	4.0							4.0
卸売業・小売業	3.5		4.0	4.0	3.0	4.0				3.6
情報通信業	2.0		4.0							2.7
サービス業	4.0		3.0	0.0	4.0	0.0				2.3
製造業		1.3	2.7	1.8	2.3	2.1	2.6	4.0	2.0	2.3
学術研究・専門・技術サービス業	0.0	2.0		2.0	2.0					1.6
建設業	4.0			0.0			2.0			1.5
飲食業							0.0			0.0
電気・ガス・熱供給・水道業				0.0						0.0
複合サービス事業	0.0									0.0
運輸業・郵便業				0.0						0.0
総計	2.7	2.0	3.3	1.4	2.5	2.1	2.2	4.0	2.0	2.3

Q18 「重要情報を廃棄する場合は、書類は細断したり、データは消去ツールを使ったりするなどのように、重要情報が読めなくなるような処分をしていますか？」との問いは、平均 70 点である。

平均 / Q18	従業員数									
	～5	～10	～20	～50	～100	～200	～300	～500	～900	総計
業種										
金融業・保険業	4.0	4.0	4.0							4.0
卸売業・小売業	3.0		2.0	2.0	4.0	2.0				2.9
製造業		2.0	2.0	2.0	3.5	2.9	3.7	3.5	4.0	2.9
情報通信業	2.0		4.0							2.7
サービス業	4.0		2.0	4.0	2.0	2.0				2.7
建設業	4.0			2.0			2.0			2.5
電気・ガス・熱供給・水道業				2.0						2.0
学術研究・専門・技術サービス業	4.0	2.0		2.0	0.0					2.0
複合サービス事業	2.0									2.0
飲食業							2.0			2.0
運輸業・郵便業				0.0						0.0
総計	3.1	2.3	2.5	2.0	3.2	2.8	3.3	3.5	4.0	2.8

Q19 「従業員を採用する際に守秘義務や罰則規定があることを知らせるなどのように、従業員に秘密を守らせていますか？」との問いは、平均 65 点である。

平均 / Q19	従業員数									
	～5	～10	～20	～50	～100	～200	～300	～500	～900	総計
業種										
飲食業							4.0			4.0
金融業・保険業	4.0	4.0	4.0							4.0
情報通信業	3.0		4.0							3.3
サービス業	4.0		3.0	4.0	4.0	2.0				3.3
卸売業・小売業	3.0		4.0	0.0	4.0	4.0				3.1
学術研究・専門・技術サービス業	4.0	2.0		4.0	2.0					2.8
建設業	4.0			1.0			4.0			2.5
製造業		3.3	2.7	2.7	1.5	2.1	2.9	2.5	4.0	2.4
複合サービス事業	2.0									2.0
運輸業・郵便業				0.0						0.0
電気・ガス・熱供給・水道業				0.0						0.0
総計	3.3	3.0	3.3	2.2	2.2	2.2	3.1	2.5	4.0	2.6

Q20 「情報管理の大切さなどを定期的に説明するなどのように、従業員に意識付けを行っていますか？」との問いは、平均 40 点である。

平均 / Q20	従業員数									
業種	～5	～10	～20	～50	～100	～200	～300	～500	～900	総計
金融業・保険業	4.0	4.0	4.0							4.0
情報通信業	3.0		4.0							3.3
サービス業	4.0		3.0	2.0	4.0	0.0				2.7
運輸業・郵便業				2.0						2.0
飲食業							2.0			2.0
複合サービス事業	2.0									2.0
学術研究・専門・技術サービス業	4.0	2.0		2.0	0.0					2.0
建設業	4.0			0.0			2.0			1.5
製造業		1.3	2.0	2.2	1.3	1.1	1.1	1.0	2.0	1.4
卸売業・小売業	1.0		2.0	0.0	1.0	0.0				0.9
電気・ガス・熱供給・水道業				0.0						0.0
総計	2.5	2.0	2.8	1.6	1.3	0.9	1.3	1.0	2.0	1.6

Q21 「社内外での個人所有のパソコンやスマートフォンの業務利用を許可制にするなどのように、業務で個人所有端末の利用の可否を明確にしていますか？」との問いは、平均 38 点にとどまった。

平均 / Q21	従業員数									
業種	～5	～10	～20	～50	～100	～200	～300	～500	～900	総計
飲食業							4.0			4.0
金融業・保険業	4.0	4.0	4.0							4.0
サービス業	2.0		4.0	4.0	0.0	2.0				2.7
情報通信業	3.0		2.0							2.7
運輸業・郵便業				2.0						2.0
学術研究・専門・技術サービス業	4.0	1.0		2.0	0.0					1.6
建設業	4.0			0.0			2.0			1.5
製造業		0.7	0.7	0.8	1.0	1.1	1.7	2.0	4.0	1.2
卸売業・小売業	0.5		0.0	0.0	2.0	4.0				1.1
複合サービス事業	0.0									0.0
電気・ガス・熱供給・水道業				0.0						0.0
総計	2.0	1.3	2.0	0.9	1.0	1.3	2.0	2.0	4.0	1.5

Q22 「契約書に秘密保持（守秘義務）の項目を盛り込むなどのように、取引先に秘密を守ることを求めていますか？」との問いは、平均 48 点にとどまった。

平均 / Q22	従業員数									
業種	～5	～10	～20	～50	～100	～200	～300	～500	～900	総計
飲食業							4.0			4.0
情報通信業	3.0		4.0							3.3
サービス業	4.0		2.0	4.0	4.0	0.0				2.7
複合サービス事業	2.0									2.0
建設業	4.0			0.0			4.0			2.0
運輸業・郵便業				2.0						2.0
製造業		1.3	2.0	1.0	1.5	1.7	2.6	3.0	4.0	1.8
卸売業・小売業	1.5		4.0	0.0	3.0	0.0				1.8
学術研究・専門・技術サービス業	4.0	0.0		4.0	0.0					1.6
金融業・保険業	0.0	4.0	0.0							1.3
電気・ガス・熱供給・水道業				0.0						0.0
総計	2.4	1.3	2.3	1.2	1.8	1.5	2.9	3.0	4.0	1.9

Q23 「クラウドサービスなど外部サービスを利用する時は利用規約やセキュリティ対策を確認するなどのように、サービスの安全・信頼性を把握して選定していますか？」との問いは、平均 60 点である。

平均 / Q23	従業員数									総計
	~5	~10	~20	~50	~100	~200	~300	~500	~900	
業種										
情報通信業	3.0		4.0							3.3
サービス業	2.0		3.0	4.0	4.0	2.0				3.0
卸売業・小売業	1.5		4.0	4.0	4.0	4.0				2.9
製造業		1.3	2.7	2.6	3.3	2.1	2.0	3.0	2.0	2.4
学術研究・専門・技術サービス業	4.0	2.0		4.0	0.0					2.4
電気・ガス・熱供給・水道業				2.0						2.0
複合サービス事業	2.0									2.0
運輸業・郵便業				2.0						2.0
飲食業							2.0			2.0
金融業・保険業	0.0	4.0	0.0							1.3
建設業	0.0			0.0			2.0			0.5
総計	1.8	2.0	2.8	2.5	3.2	2.2	2.0	3.0	2.0	2.4

Q24 「秘密情報の漏洩や紛失、盗難があった場合の対応手順書を作成するなどのように、事故が発生した場合に備えた準備をしていますか？」との問いは、平均 20 点にとどまった。

平均 / Q24	従業員数									総計
	~5	~10	~20	~50	~100	~200	~300	~500	~900	
業種										
金融業・保険業	4.0	4.0	4.0							4.0
情報通信業	2.0		4.0							2.7
複合サービス事業	2.0									2.0
運輸業・郵便業				2.0						2.0
サービス業	2.0		2.0	0.0	4.0	0.0				1.7
卸売業・小売業	1.0		0.0	0.0	1.0	2.0				0.9
製造業		0.0	0.7	0.4	0.3	0.4	0.9	1.5	0.0	0.5
建設業	0.0			0.0			2.0			0.5
学術研究・専門・技術サービス業	0.0	0.0		2.0	0.0					0.4
飲食業							0.0			0.0
電気・ガス・熱供給・水道業				0.0						0.0
総計	1.5	0.7	1.8	0.5	0.7	0.5	0.9	1.5	0.0	0.8

Q25 「情報セキュリティ対策(上記 1 ~ 24 など)を会社のルールにするなどのように、情報セキュリティ対策の内容を明確にしていますか？」との問いは、平均 25 点にとどまった。

平均 / Q25	従業員数									総計
	~5	~10	~20	~50	~100	~200	~300	~500	~900	
業種										
飲食業							4.0			4.0
金融業・保険業	4.0	4.0	4.0							4.0
情報通信業	3.0		4.0							3.3
サービス業	2.0		2.0	2.0	4.0	2.0				2.3
建設業	2.0			0.0			2.0			1.0
卸売業・小売業	0.5		0.0	0.0	1.0	2.0				0.7
製造業		0.0	1.3	0.2	0.8	0.5	0.6	1.5	2.0	0.6
学術研究・専門・技術サービス業	0.0	0.0		2.0	0.0					0.4
運輸業・郵便業				0.0						0.0
複合サービス事業	0.0									0.0
電気・ガス・熱供給・水道業				0.0						0.0
総計	1.5	0.7	2.0	0.4	1.0	0.7	1.1	1.5	2.0	1.0

② 個社毎の指導（報告書送付）

SECURITY ACTION の星を宣言されていない企業に、ご回答頂いた回答内容を分析担当が報告書を作成し、強化ポイントのアドバイスと、自己宣言方法の指導を64社に実施した。

参加企業に回答依頼



分析担当が強化ポイントを報告



自己宣言方法の説明



③ SECURITY ACTION 取得状況の結果

事業参加企業の中で一つ星を取得されている企業数： 21 社
 事業参加企業の中で二つ星を取得されている企業数： 9 社

一つ星 (★) を取得できない理由	
今後取得	<ul style="list-style-type: none"> ・ 手続きをしていない ・ 今後の取得を検討している ・ 今後取得予定 ・ 近々取得予定 ・ 一つ星の情報セキュリティ 5 か条を含めた社内セキュリティポリシー策定中で、正式に実施してから、SECURITY ACTION を検討したため
<u>必要性無し</u>	<ul style="list-style-type: none"> ・ 客先より要求されていない ・ まだ必要性を感じられないから ・ 必要性がまだ感じない ・ 特に理由はなし
<u>勘違い?</u>	<ul style="list-style-type: none"> ・ 取得できる <u>レベルに達していないため</u> ・ まだ周知徹底できる段階にいない ・ 事情があって最新の OS に更新できていない端末があるため ・ 星を取得したかどうか不明
<u>業務多忙</u>	<ul style="list-style-type: none"> ・ 業務多忙のためと、取得するメリットが分からないため
その他	<ul style="list-style-type: none"> ・ 一つ星をとばして、二つ星宣言をしたため
二つ星 (★★) を取得できない理由	
今後申請	<ul style="list-style-type: none"> ・ まだ行っていない ・ 今後の取得を検討している ・ これから申請取得予定 ・ まだ周知徹底できる段階にいない ・ 「基本方針」や「規程」が未だ会社に承認されていない、社内公開に至っていない
<u>必要性無し</u>	<ul style="list-style-type: none"> ・ <u>IT 補助金に絡まない</u> ・ <u>経営層が必要性を感じていない</u> ・ まだ必要性を感じられないから ・ 必要性がまだ感じない
<u>勘違い?</u>	<ul style="list-style-type: none"> ・ 事情があって最新の OS に更新できていない端末があるため ・ 星を取得したかどうか不明
一つ星から	<ul style="list-style-type: none"> ・ 一つ星を取得していないため ・ 一つ星を取得していないため ・ まずは一つ星の取得からと考えているため ・ SECURITY ACTION 一つ星がまだ

(オ) 公開サイト上の脆弱性診断による状況把握

① レンタルサーバの脆弱性適用の責任範囲

参加企業が構築する公開サイトのほとんどはクラウド上に構築するレンタルサーバで運用されている。このケースでは大きく PaaS、IaaS に分かれるが、各種サーバ製品の脆弱性を業者側で管理する PaaS と異なり、IaaS では初期インストールや初期設定までは行うものの、以降の脆弱性管理は参加企業側で実施することになる。また、自社コンテンツ内にサーバサイドで実行されるコードが含まれるケースもあり、脆弱性を管理しなければならない事もある。このような管理を、開発業者に任せることもあるが、新規・追加開発が中心で、設定やアプリケーションの脆弱性が行われているか悩ましいところである。公開サイトの上の脆弱性診断では、中小企業における対策状況を把握する。

	クラウド(PaaS)	クラウド(IaaS)	クラウド(IaaS)	オンプレミス (自社サーバ)
脆弱を日々 ウォッチして 管理が必要	自作コンテンツ 環境設定	自作コンテンツ 環境設定	自作コンテンツ 環境設定	自作コンテンツ 環境設定
環境の準備、 脆弱性更新の 運用・管理は レンタル業者	Web、 CMS、 EC、 DBサーバ等	Web、CMS、 EC、(DB) サーバ <small>初期の導入と 初期設定のみ</small>	Web、 CMS、 EC、 (DB) サーバ等	Web、 CMS、 EC、 (DB) サーバ等
	OS	OS <small>初期の導入と 初期設定のみ</small>	OS	OS
	仮想環境	仮想環境	仮想環境	仮想環境
	ハードウェア	ハードウェア	ハードウェア	ハードウェア

脆弱性の定期診断を推奨

図 3-4. 稼働環境と脆弱性の適用責任範囲

② 実施状況

診断回数は下記のとおり。

表 3-3. 公開サイト脆弱性診断の実施状況

実施済	実施予定	サイト無し (診断不要含む)	レンタルサーバ業者から診断不可の回答 (※)
33 社/1 回 12 社/2 回	7 社	35 社	21 社

※ 自社資源ではなく、レンタルサーバを利用されている企業へは、他社と資源を共有することからレンタルサーバ運営業者へ診断実施の確認をして頂き、業者側から断られたケースも示す。

③ 検出された脅威と傾向

危機的 504 件、深刻 1,198 件、中度 203 件の合計 1,905 件の問題が検出され、1 社平均 42 件の問題点が存在した。

各脆弱性には 3 つの深刻度レベル（危機的、深刻、中度）が存在します。脆弱性評価基準（CVSSv2）のスコアが 0～3.4 を中度、3.5～7.4 を深刻、7.5～10 を危機的に分類しています。

※CVSS とは <https://www.ipa.go.jp/security/vuln/CVSS.html>

④ 多く検知されている問題の周知

表 3-4. 多く検知されている問題

脆弱性名	件数	深刻度
ssl-static-key-ciphers	41	中度
ssl-cve-2011-3389-beast	39	深刻
tls1_0-enabled	39	深刻
tls1_1-enabled	36	中度
pop-plaintext-auth	29	深刻
ftp-plaintext-auth	28	深刻
tls-dh-prime-under-2048-bits	27	中度
smtp-plaintext-auth	25	深刻
certificate-common-name-mismatch	20	深刻
imap-plaintext-auth	20	深刻
ssl-3des-ciphers	20	中度
ssl-des-ciphers	19	深刻
ssl-cve-2016-2183-sweet32	17	深刻
http-options-method-enabled	17	中度
tls-dh-primes	17	中度
ssl3-supported	15	深刻
rc4-cve-2013-2566	10	深刻
ssl3-cve-2014-3566-poodle	10	深刻
php-cve-2019-6977	10	深刻
php-cve-2019-9020	9	危機的
php-cve-2019-9021	9	危機的
php-cve-2019-9023	9	危機的
php-cve-2019-9641	9	危機的
tls-untrusted-ca	9	深刻
http-php-obsolete	8	危機的
php-cve-2014-9426	8	危機的
php-cve-2015-4601	8	危機的
php-cve-2016-7124	8	危機的
php-cve-2016-7126	8	危機的
php-cve-2016-7127	8	危機的

※以降の検出名は省略

⑤ 参加企業の対応結果

本事業で検知された脆弱性レベルは、対処が急がれる危機的が 504 件検出された。本事業では、検知した問題点について、修正確認を行うため 2 回の診断機会を提供している。2 回実施した企業は、1/3 程度の実施であり、危機的が 273 件であったが、修正後の確認では 9 件まで大幅に削減できていた。

表 3-5. 公開サイト脆弱性診断の効果

脆弱性レベル	指摘総数	総数のうち、修正確認まで 2 回実施	
		初回	修正後
危機的	504	273	9
深刻	1198	570	144
中度	203	62	50
合計 (1 社平均)	1905 (42)	905 (75)	203 (17)

表 3-6. 公開サイト脆弱性診断の対策状況 (詳細)

2 回目(修正確認)を実施した 12 社		
診断を有効に活用して対策実施	6 社	
対策が未実施 (危機的は無い)	5 社	
初回から問題なし	1 社	
2 回目(修正確認)を辞退した 5 社		
対処未実施 (期間内に対処できない)	3 社	
対策未実施 (危機的は無い)	1 社	
初回から問題なし	1 社	
その他 2 3 社		
これから実施	19 社	(1 回目 6 社、2 回目 13 社)
期間的に不可	3 社	
他業務で忙しい	1 社	

(カ) パソコン上の脆弱性監視ツールによる状況把握

PFU製のiNetSec Inspection Center(PC脆弱性検査ソフトウェア)を参加企業のPCに導入することで、PCからの検査結果を自動的に監視し、PC上の脆弱性に関する是正箇所を含めた報告書を作成し月次報告として参加企業へメールする。

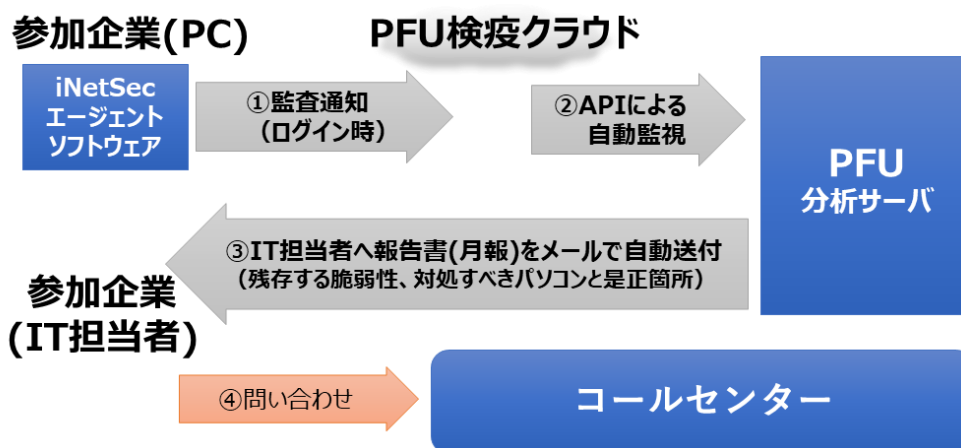


図 3-5. パソコン上の脆弱性監視サービス提供イメージ

日々社員の画面に脆弱性に関する問題点を通知する機能があるが、参加企業によっては管理者だけに通知してほしいとの要望が多数あり、管理者がPC利用者から多くの問い合わせを受けたくないという要望からである。本事業では、参加企業毎にPC利用者への通知をする／しないについて選択できるようにした。多くの企業では管理者に送付する月次報告書(問題のあるパソコンと、改善点を列挙)のみの送付を選択されている。日々社員に通知することで管理者が介在しなくとも善処の指導を行う予定であったが、本業最優先を選択されることが分かった。

① サポート切れ / サポート切れ間近な OS の利用率

2019年10月と、2020年1月で定点観測したところ、サポート切れ間近なWindows 7は世の中の注意喚起もあり進捗したが、Windows10におけるサポート切れOSが悪化した。

表 3-7. パソコン上のサポート切れ / サポート切れ間近な OS

	OSサポート状況		
	期限内	終了間近	終了
Windows 7		42 → 24 (改善)	
Windows 8.1	1 → 1		
Windows 10	40 → 52	40 → 50 (悪化)	29 → 26 (改善)

② Windows10 でもサポート切れがあることの周知

参加企業からの問い合わせにおいても、なぜ Windows10 がサポート切れやサポート切れ間近（サポート期間が残り 6 か月未満）と指摘を受けるのか質問を受けた。中間報告会において、Windows10 内のバージョン（半期アップデート）においてサポート切れになるバージョンが存在することを啓発した。

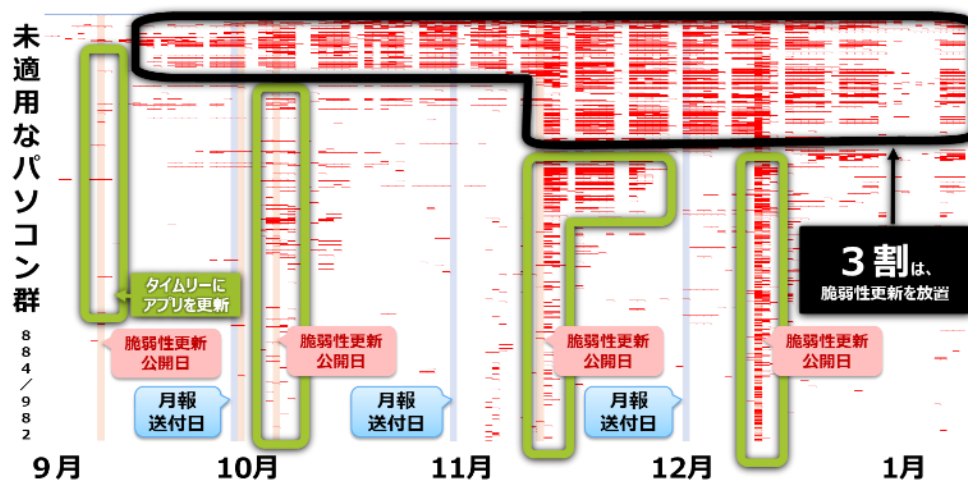
表 3-8. パソコン上のサポート切れ / サポート切れ間近な OS（詳細）

製品バージョン	Microsoft社のOSサポート状況		利用状況		
	Home, Pro, Pro Education, Pro for Workstations	Enterprise, Education	サポート期限内	サポート終了間近	サポート終了
Windows 10 Version 1909	2021年5月11日	2022年5月10日	512 (68%)	204 (27%)	38 (5%)
Windows 10 Version 1903	2020年12月8日	2020年12月8日			
Windows 10 Version 1809	2020年5月12日	2021年5月11日			
Windows 10 Version 1803	2019年11月12日	2020年11月10日			
Windows 10 Version 1709	2019年4月9日	2020年4月14日			
Windows 10 Version 1703	2018年10月9日	2019年10月8日			
Windows 10 Version 1607	2018年4月10日	2019年4月9日			
Windows 10 Version 1511	2017年10月10日	2017年10月10日			
Windows 10 Version 1507	2017年5月9日	2017年5月9日			
製品バージョン	メインストリームサポート	延長サポート契約			
Windows 8.1	2018年1月9日	2023年1月10日	14 (93%)	0	1 (7%)
Windows 8	2016年1月13日	※8.1への移行	0	0	0
Windows Vista	2012年4月10日	2017年4月11日	0	0	0
Windows 7 Service Pack 1	2015年1月13日	2020年1月14日	0	171 (23%)	0
Windows 7	2013年4月9日	※SP1への移行			

- ※ 2020/1/10 現在: Windows7 延長サポート切れ直前の状況。
- ※ Windows10 Enterprise LTSC/LTSB エディションは下記 URL を参照のこと。
<https://support.microsoft.com/ja-jp/help/13853/windows-lifecycle-fact-sheet> (11/18 現在)
- ※ Windows Server 2012, 2012R2, 2016 が監視対象となっておりますが、表には掲載していません。

③ 脆弱性更新の適用状況（Windows Update で対応可能なもの）

Microsoft Windows OS や Microsoft Office など OS の更新メカニズムで対応ができる脆弱性は、3 割程度は定期的な更新が行われていなかった。横軸は時間、縦軸は未適用なパソコン 1 台毎で非適用な時間帯を赤くしている。

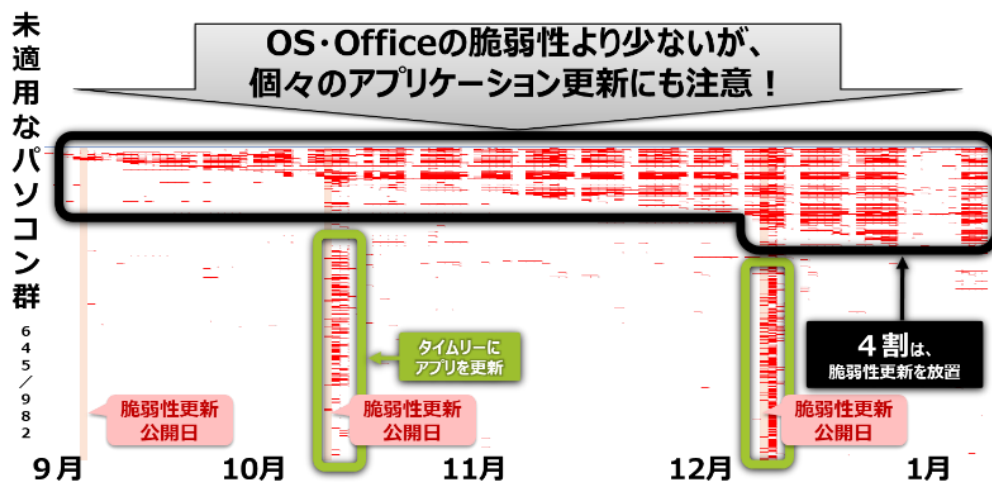


- ※ パソコン 982 台のうち、1 回でも期間中に脆弱性を見つけたパソコンの台数が 884 台。

図 3-6. Microsoft Windows や Office の脆弱性の検知状況

④ 脆弱性更新の適用状況（Windows Update に対応不可能なもの）

Adobe Reader, Adobe Flash や Oracle Java のようなサードパーティアプリケーション毎の更新が必要な脆弱性は、Windows OS や Office の脆弱性程台数は多くないが、4 割程度が定期的に更新を行っていない。横軸は時間、縦軸は未適用なパソコン 1 台毎で非適用な時間帯を赤くしている。



※ パソコン 982 台のうち、1 回でも期間中に脆弱性を見つけたパソコンの台数が 645 台。

図 3-7. サードパーティアプリケーションの脆弱性の検知状況

⑤ 業種・従業員数別の脆弱性未対処（放置）状況

表 3-9. パソコン上の脆弱性未対処状況（業種・従業員数別）

業種	従業員数									総計	
	平均 / 未対処(放置)	~5	~10	~20	~50	~100	~200	~300	~500		~1000
宿泊業・飲食店								100%			100%
情報通信業	67%		75%		100%						76%
電気・ガス・熱供給・水道業					60%						60%
建設業	0%			60%			60%				57%
サービス業(その他)		50%	57%	65%	33%	54%					56%
学術研究・専門・技術サービス業	25%	17%		56%	93%						55%
卸売業・小売業	21%		0%	100%	30%	50%					44%
製造業		56%	31%	41%	21%	38%	33%	49%	50%		36%
金融業・保険業	30%	0%	50%								29%
運輸業・郵便業				0%							0%
総計	35%	44%	45%	53%	30%	40%	37%	49%	50%		41%

(キ) パソコン上のセキュリティソフトの導入状況

監視サービス実施企業 97 社のパソコン 982 台に導入されているセキュリティソフト名について、Windows Management Instrumentation (WMI) インタフェースを通して得られた名称で列挙する（具体名が特定できないものは名称不明として記載）。2020 年 1 月に調査したため Windows10 への移行が進んでいることもあり、OS 上で無償提供されている Windows Defender が半数近くを占めていた。少数ではあるが、ウイルスバスター2010 のようなサポートが切れていると思われる対策ソフトを使い続けているパソコンも存在した。

表 3-10. パソコン上のセキュリティソフトの導入状況

セキュリティソフトウェア名	導入割合
Windows Defender (無償)	43.9%
トレンドマイクロ ウイルスバスター コーポレートエディション	20.1%
ESET Security	10.3%
ESET Endpoint Security	4.6%
ビジネスセキュリティクライアント	3.3%
Microsoft Security Essentials (無償)	3.2%
Symantec Endpoint Protection	2.2%
名称不明	2.2%
ウイルスバスター クラウド	2.1%
ESET Endpoint Antivirus 5.0	1.5%
Computer Protection by F-Secure	1.1%
マカフィー ウイルススキャン	1.1%
ESET Internet Security	0.6%
ESET Endpoint Antivirus	0.6%
AssetView	0.4%
McAfee Endpoint Security (anti-virus)	0.4%
FortiClient AntiVirus	0.4%
カスペルスキー インターネット セキュリティ	0.3%
セキュリティエージェント	0.2%
ESET Endpoint Antivirus 6.4.2014.2	0.2%
McAfee Endpoint Security	0.2%
ウイルスセキュリティ	0.2%
CylancePROTECT	0.1%
ウイルスバスター2010	0.1%
Norton Internet Security	0.1%
セキュリティ対策ツール	0.1%
ノートン セキュリティ	0.1%
Symantec Endpoint Protection	0.1%
ESET Smart Security 4.2	0.1%
Trend Micro Apex One	0.1%
マカフィー アンチウイルスとアンチスパイウェア	0.0%

(ク) パソコン上の脅威検知ツールによる状況把握

参加企業の PC に WEBROOT 社 SecureAnywhere Business を導入し、クラウド上で管理する方式でサービスを提供した。ソフトウェアは、通常のアнтиウイルスソフトの機能に加えて、未知の脅威を識別でき、クラウド上から隔離操作（処置）ができる機能がある。

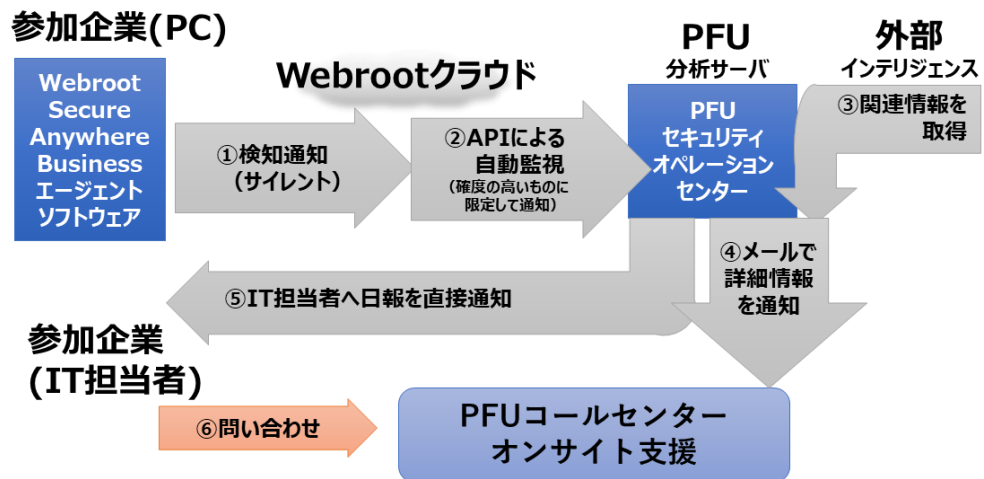


図 3-8. パソコン上の脅威検知サービス提供イメージ

① 脅威の検知位置について（既存対策をすり抜けた脅威）

前記、「3(イ)当社採用のエンドポイント型の脅威検知位置（UTM との違い）」で説明したとおり、他事業者と検知位置の違いにより、既存対策をすり抜けた脅威、かつ確度や重要度が高いと分析担当が判断するものを絞り込んで報告するため、相対的に検出数は少なくなっている。

② 検出された脅威について

下記の一覧は、検知したマルウェアであるが、前記メカニズムにより IT 担当者が疲弊しないよう、確度が高く重要性が大きい脅威のみ担当者へ通報を行った。パソコン上の脆弱性に比べ直ちに対処すべき脅威は少なく、当初想定した程の通報はなく、先頭3つの通報にとどまった。

表 3-11. パソコン上の脅威検知状況

検知内容	説明	件数	報告
Win32/Emotet	<ul style="list-style-type: none"> ● 金融機関への ID やパスワード、PC 内の情報窃取を行う ● (現在はメール本文や、送受信したことのあるメールアドレスも窃取) ● 別のマルウェアのダウンロード、および実行機能 	1	通報
Win32/Spy.Shiz	<ul style="list-style-type: none"> ● 金融機関への ID やパスワードを窃取するバンキングマルウェア 	1	
Win32/FlyStudio	<ul style="list-style-type: none"> ● 実行ファイルのダウンロードや攻撃者からの制御を可能とするプログラム 	1	
Win32/NetFilter	<ul style="list-style-type: none"> ● ブラウザの設定を変更し、ブラウザに拡張機能をインストールして、ブラウザからのインターネットアクセスを誘導するプログラム 	2	通報対象外
PUA.Mindspark	<ul style="list-style-type: none"> ● ブラウザにツールバーを追加 	80	
W32.MyWebSearch	<ul style="list-style-type: none"> ● ブラウザからキーワードを検索すると、意図しない検索エンジンに問い合わせる 		
W32.Adware.Gen	<ul style="list-style-type: none"> ● この問い合わせの結果、メジャーな検索エンジンでは表示されないような広告されることがあり、この広告を経由してマルウェアが配信される 		
W32.Downloader.Gen	<ul style="list-style-type: none"> ● 汎用的なダウンローダという名称 (PFU で詳細を調査したところ、これは InstallCore という種類のアドウェアだった) ● アドウェアというのはユーザの望まない広告表示活動を行うものであり、『あなたの PC の速度が低下しています』や『あなたの PC でエラーが見つかりました』といったメッセージと合わせて『これを改善するにはここをクリック』のような広告を表示することが多い 	1	
W32.Deceptor.Clean-pc-pro	<ul style="list-style-type: none"> ● システムに大量の問題があるという診断結果を表示して、有料の Clean PC Pro を購入させようとする (詐欺と思われる) ソフトウェア ● 元々問題がないシステムで偽の診断結果を出しているだけであり、有料の Clean PC Pro を買って何もうならない 	1	

③ 駆け付け対応支援

参加企業の PC がマルウェアに感染し、参加企業自身で対処できないと判断した場合、駆け付け対応要員が参加企業事業所に駆け付けて状況調査やマルウェア駆除支援などの初動対応支援を実施する。また、初動対応支援により、さらに詳細な影響範囲の調査や安全宣言に向けた復旧作業等が必要な場合には、高度な分析調査を行うことができる技術員を派遣し対応する。本実証では 1 件の駆け付け対応を実施しており、初動対応支援の範囲であった。

駆け付け対応支援の経緯

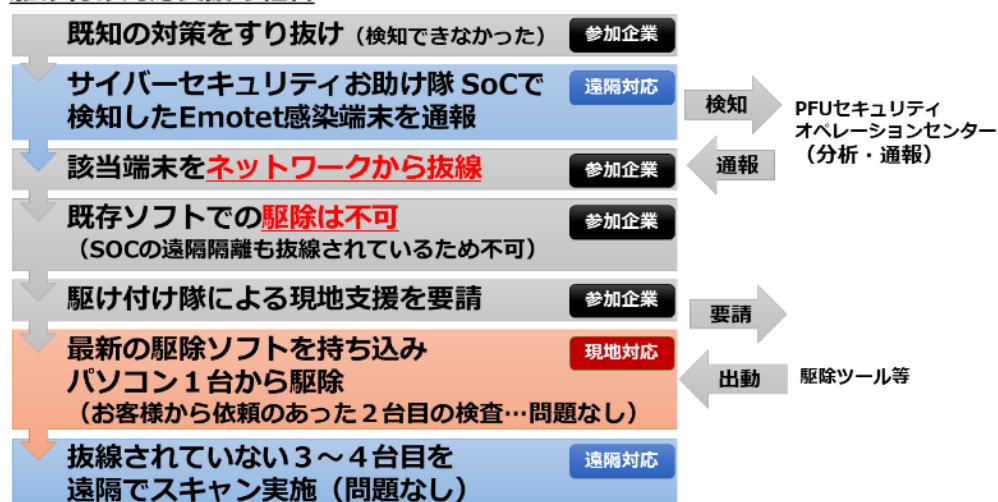


図 3-9. 駆け付け対応支援内容

4 中小企業向けサイバーセキュリティ事後対応支援体制の構築

(ア) 機能ごとの体制構築

当社内の各作業を行う部門内に本事業を実施する体制を構築する。

① 相談窓口体制

(イ) 必要なスキル

1. 一般的なビジネススキル（電話対応・メール作成）+PCスキル+セキュリティに関する知識
 - ・日本コンタクトセンター検定 オペレーション
 - ・CompTIA A+, Network+, Security+
2. 技術的なサービス内容や脅威内容に関して回答を実施するスキル
 - ・CISSP（参加企業からの質疑対応・事業説明など）
 - ・**情報処理安全確保支援士（サービス実行の対応）**

(ロ) 必要な人数

サービス開設時間：9～17時（12～13時を除く）

サービス開設日：平日のみ（土日祝日・夏季冬季の休暇日を除く）

1. コールセンター：4名（常時2名、必要に応じて応援2名）
2. サービス実行部隊：4名（常時2、必要に応じて応援2名）

② パソコンの脆弱性検知と報告

(イ) 必要なスキルと人数

完全に自動化されており、特別なスキルは必要としない。

③ パソコンの脅威検知と報告

(イ) 必要なスキルと人数

パソコン上での検知、および外部インテリジェンスを活用した脅威の確度を確認する部分は、システム化されており、特別なスキルや対応者は不要。最後に、過去の知見から参加企業に報告すべきか最終判断するために、分析担当1名が必要。

④ 駆け付け対応支援（インシデント初動対応）

(イ) 現地駆け付け対応要員へ指示するSOC側に必要なスキル

脅威・脆弱性に対する回答スキル

- ・CompTIA A+, Network+, Security+

(ロ) 現地駆け付け要員のスキル

一般的なPC操作・顧客対応スキルに関する知識。

最新のオフラインアンチウイルスソフトを持ち込んで実施すること、必要に応じてセキュリティオペレーションセンター技術員からの遠隔指示により、作業を実施できるスキルを必要とする。

・ CompTIA A+, Network+, Security+

(ハ) 現地駆け付け要員の人数

サービス開設時間：9～17時（12～13時を除く）

サービス開設日：平日のみ（土日祝日・夏季冬季の休暇日を除く）

駆け付け隊：県毎に1名待機（必要に応じて増員、最大時は地域に2名）

⑤ 公開サイトの脆弱性診断と報告

(イ) 必要なスキル

参加企業の脆弱性・脅威の分析・報告書の作成に関する知識。

・脆弱性診断士の経験、報告書作成のスキル

(ロ) 必要な人数

・診断者、および報告作成者1名

・報告書の確認者1名（別要員）

⑥ その他（契約からサービス開始までの事務局体制）

(イ) 必要なスキル

・一般的なビジネススキル（電話対応・メール作成）

・必要に応じて法務部門に個別相談（個別、秘密保持契約など）

(ロ) 必要な人数

サービス開設時間：9～17時（12～13時を除く）

サービス開設日：平日のみ（土日祝日・夏季冬季の休暇日を除く）

受付業務：1名

⑦ その他（インストールモジュール作成と送付の事務局体制）

(イ) 必要なスキル

手順書に従い、参加企業から回答頂いたサービスヒアリングシートに従い、会社毎の設定を行ったインストールモジュール作成を行う。特別なスキルは不要。

(ロ) 必要な人数

サービス開設時間：9～17時（12～13時を除く）

サービス開設日：平日のみ（土日祝日・夏季冬季の休暇日を除く）

作成業務：1名（依頼時5分程度）

確認業務：1名（依頼時5分程度）

(イ) 運用フローの構築

前記機能間の運用フローを構築した。

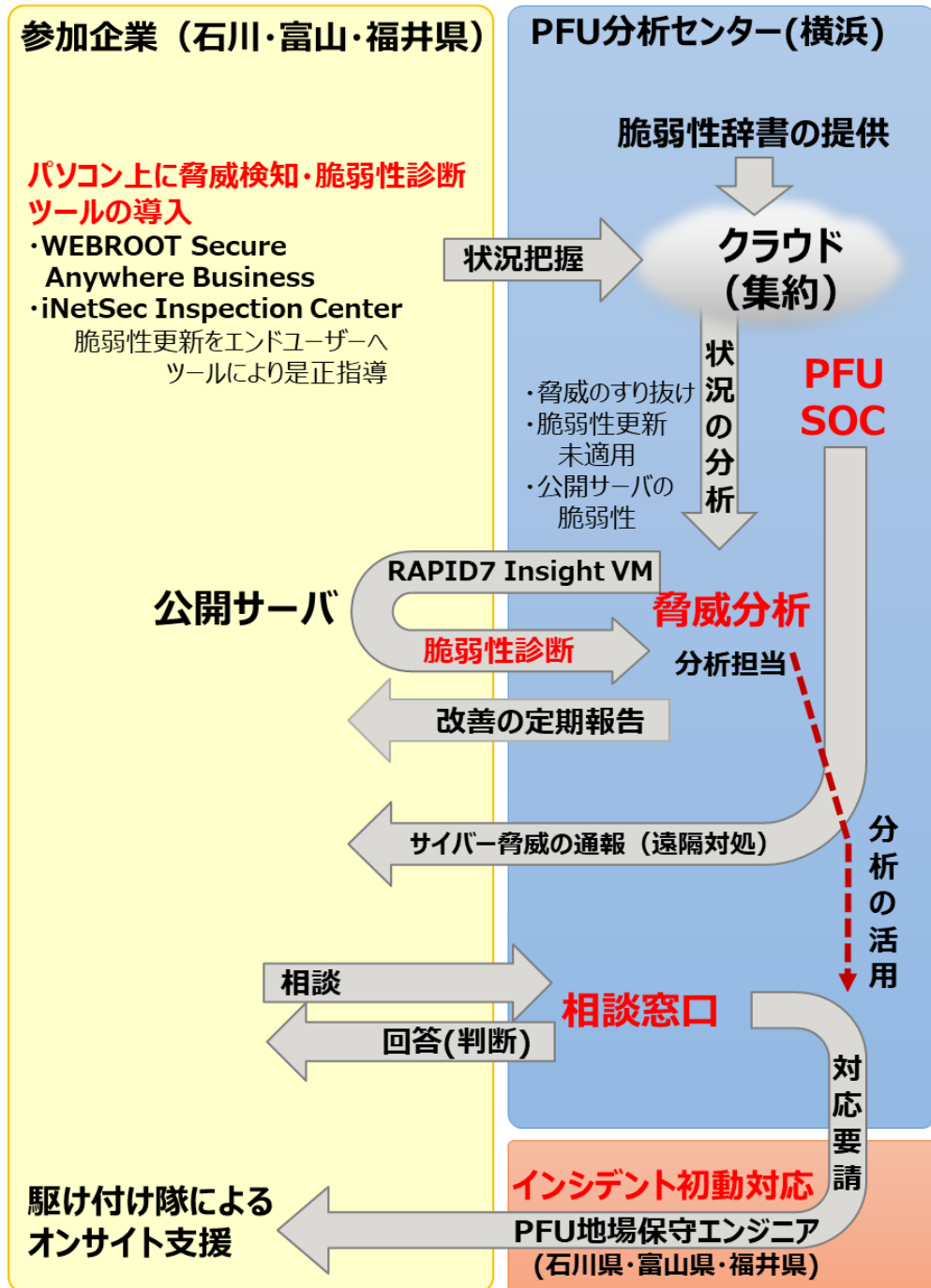


図 4-1. 機能間の運用フロー

5 地域実証の実施

(ア) 契約からサービス開始までの流れ

1. 参加企業に事業説明会への参加、訪問による説明により事業内容の把握を頂き、参加企業から仮申し込みと共に、意識調査アンケート、5分でできる情報セキュリティ自社診断の提出を頂く。この時点で、今後やり取りする添付ファイルのパスワードも合わせてオフラインで回答して頂く。
2. 申込頂いた参加企業に対して、ソフトウェア借用書（契約書）への社印、サービスヒアリングシート（ソフトウェアを実行するための参加企業環境の調査）をお渡しし、参加企業にご回答を頂く。
3. サービスヒアリングシートに従い、インストールモジュールの作成（参加企業の環境設定済）を作成し、参加企業へ送付する（ファイルは1で得たパスワードで暗号化）。
4. 送付したモジュールのインストール後、参加企業から連絡を頂き、PFUの遠隔監視サービスの対象となったか回答させて頂く
5. 公開サイトの脆弱性診断に関しては、レンタルサーバをご利用の参加企業に対して、レンタルサーバ業者へ診断実施の許可を頂く（例文をPFUから送付）。

(イ) 運営で得られた課題

① 契約からサービス開始の課題

(イ) 契約作業の課題

- ・インターネット上の申込フォームによる申請はハードルが高い（5社）
 - ちらし裏面にFAX申込用紙を掲載、FAXによる申し込みを受け付け
 - 手書きでは、名前・連絡先の読み取りが難しい事も
- ・参加企業側の文面による秘密保持契約の締結の依頼（3社）
 - PFU 法務部門により個社毎に締結するが、参加企業が用意する文面では審査に1～2週間を要するため締結まで時間を要する
- ・ソフトウェア借用書（契約書）に社印を必要とするが、参加企業会社内での手続きに時間を要し、社長決裁（役員決済）を得られないケースも存在する

(ロ) サービス開始に必要なヒアリングの課題

- ・プロキシの有無や設定など、ネットワーク環境について設問が設けられているが「調べ方がわからない」という問い合わせも多い

- ブラウザの設定確認と必要に応じて一部設定を変えて頂き、社外サイトが閲覧できるか確認する手順書を提供した
- 手順書を見ても作業できない参加企業もあり、一部の参加企業でエンジニア派遣も必要となった

② インストールモジュール作成時と送付時の課題

(イ) 作成時とモジュール送付時の課題

- ・ 個社毎に設定ファイルを追記した自動インストールモジュールを作成し、個社毎に宅急便で送付していたが届くまで1～2日程度の時間がかかっていた
 - 電子メールでの送付を検討したが、ファイルサイズ的に難しい
 - 業務多忙からツールのダウンロード期限(最大7日)を迎えてしまい再送を実施(8社)
 - グループ会社のファイル送付用クラウドサービスを使う送付方法へ切り替え、参加企業がタイムリーに作業頂けるように作業手順を変更した
 - URL 通知し、パスワード入力後に ZIP ファイルをダウンロードして、展開頂くことで、インストール手順書とモジュールを得られるが、ファイルダウンロードサービスへの接続が許可されておらず、CD-ROM によるオフライン送付を希望される参加企業もおられた

③ インストールモジュール導入時の課題

(イ) 参加企業スキルの課題

- ・ インストール手順書が難しい
 - 操作画像入りの手順書に改版
- ・ インストール作業は業者に依頼しているため、社内メンバーでは行えない
 - 駆け付け隊派遣によるインストール支援を実施(5社)
 - 執務室への保守員の入室に懸念を示される参加企業(1社)

(ロ) 大量導入時の課題

- ・ Active Directory による多数台インストール手順において、対象パソコンへのファイルコピーを説明している箇所が分からない
 - 設定例を入れた説明を追加

(ハ) セキュリティツールの課題

- ・ インストール後に、複写されるべきファイルの一部がシステムに入っていない
 - 参加企業の環境で接続先設定などの画面を表示しないため、定義ファイルを事前に作成して同梱していたが、既設のアンチウイルス製品により、複写が

禁止された可能性がある。事前設定した定義ファイルを手動複写することで対処

- ・インストール後にブルースクリーンが発生、動作遅延が発生、業務遅延が発生（3社）
 - PFU ソフトの CPU 利用率やメモリ使用量は大きくないが、業務影響も考え、参加企業の希望もあり本事業ではツールのアンインストールを実施（遅延については PC スペック以外について継続調査）

(二) 中止時のアンインストールの課題

- ・インストールはワンクリックで行っているが、ここでインストールされる 2 種類のツールのうち、1 種類はクラウド経由による遠隔アンインストールが行えるが、残る 1 種類は、参加企業が各パソコンで操作を行う必要がある
 - 参加企業の負担あり（遠隔操作で全てが行えるようにするべきであった）

④ 相談窓口の課題

(イ) 対応人数の結果

事業参加される企業が一挙に増えず、徐々に参加された事で、想定どおりの対応を行うことができ、人数に対する課題はなかった。

(ロ) 問い合わせ内容

表 5-1. 問い合わせ件数

対応月	対応件数	参考) 対象社数
8月	9件	5社
9月	27件	20社
10月	44件	49社
11月	46件	74社
12月	56件	92社
1月	14件	97社
合計	196件	

表 5-2. コールセンター対応、インシデント対応件数

対応種別	アラート種別	発生件数	特記事項
コールセンター対応	実証参加に関する問い合わせ	21	
	セキュリティ機器設置等の問い合わせ	111	ソフトのインストール、モジュール再送、接続確認、ヒアリング項目の記載方法等
	セキュリティ対応の相談	5	
	その他		
	計	137	
インシデント等対応	電話、およびリモートによるインシデント対応	48	うちパソコンの脆弱性 17 件、公開サイトの脆弱性 18 件含む
	訪問によるインシデント対応	1	Emotet の駆除対応
	機器設置等のトラブル対応	10	現地でのソフトウェアインストール支援
	その他	0	
	計	59	
総計		196	

以下に情報を補足する。

- コールセンター対応 – 実証事業の問い合わせ：21 件
- コールセンター対応 – セキュリティ機器設置等の問い合わせ：111 件
 - ・ 動作確認
 - ツールインストール後のセキュリティオペレーションセンターからの監視が行えているか動作確認を実施
 - ・ インストール関連
 - インストールが上手く行かない、動作遅延やフリーズが発生した（パソコンの脅威検知の項で解説）
 - ・ ツール関連
 - ツールの仕様や挙動に関する質問・解凍後あるべきファイルが見当たらない・Active Directory を利用する方法が分からない

(パソコンの脅威検知の項で解説)

- その他
 - ヒアリングシートの記載方法が分からない、調査方法の解説資料の送付を行ったがそれでも難しい場合、エンジニアリングを派遣した
 - 添付ファイルを展開するパスワードを忘却され、郵送にて担当者宛てに再送した
 - モジュールのダウンロード期日が切れてしまったので再送して欲しいとの依頼で、想定の7日では足りず、モジュールの再送を実施

- コールセンター対応 - セキュリティ対応の相談：5件

- インシデント等対応 - 電話、およびリモートによるインシデント対応
(パソコンの脅威検知：13件)
 - ご利用中の既存対策ソフトで Emotet に感染した
 - ご利用中の既存対策ソフトで WinThruster を検知したと表示される
 - ご利用中の既存対策ソフトで「ARP キャッシュポイズニング攻撃がブロックされた」と表示される
 - 既存対策ソフトでのフルスキャンの実施方法を説明

 - 日次の脅威検知レポートが届いていない
 - システム不備 (停電や移設等)

- インシデント等対応 - 電話、およびリモートによるインシデント対応
(パソコンの脆弱性：17件)
 - Windows のサポートが終了間近となっている・使っているバージョンを知りたい
 - 月次報告書に、パソコン毎にOSバージョンが古いと記載はあるが、具体的なインストールされているバージョンと、どのバージョンに更新すれば良いのか記載がなかったため電話対応で調査方法を解説
 - Windows のパッチが当たっていない・当て方が分からない
 - Java のパッチが当たっていない・当て方が分からない
 - 電話対応で実施方法を説明

- インシデント等対応 - 電話、およびリモートによるインシデント対応
(公開サイト脆弱性：18件)
 - レポートの内容が専門的すぎて具体的な対処方法が不明
 - 電話にて不明点を伺いメールにて回答
 - サーバ管理会社がレポートの授受を拒否する

- 業者が報告書ではなく、具体的な指示を求めるとのことであり、報告書に記載した対処方法を中心に、参加企業担当者へ問題点と対処方法を説明
- ・ 対処が間に合わないので次回の診断日時を変更したい
 - 再度実施日を設定、事業終盤は診断日の空きがなくキャンセル待ち状態となり参加企業の対処時間から考えると実証事業期間が短かった
- インシデント等対応 – 訪問によるインシデント対応：1 件
 - ・ Emotet 感染の初動対応（駆除）
- インシデント等対応 – 機器設置等のトラブル対応
(訪問によるツールインストール支援:10 件(11回))

(ハ) 問い合わせを減らすための仕組み

- ・ 回答内容のデータベース化
 - 同一内容は、コールセンター内で折り返し回答を実施
 - ✓ インストールの正しい手順
 - ✓ トラブルシューティング、およびヒアリングガイド
 - ✓ Windows のパッチの適用方法、各種ログの採取方法
 - コールセンター内で問い合わせ内容・回答の定期的な棚卸と勉強会を実施
- ・ インストール手順書の改版
 - Active Directory を使ったインストール手順において問い合わせのあったファイル複写部分について例示
- ・ 日次の脅威報告メールにおいてメール本文を見ないと脅威の有無が判らない部分を改善
 - メール の 題名 に 脅 威 有 り の 場 合 は、 強 調 し て 表 記
- ・ コールセンターで受け付けた日次の脅威報告メールにおいてメール本文を見ないと脅威の有無が判らない部分を改善
 - メール の 題名 に 脅 威 有 り の 場 合 は、 強 調 し て 表 記

⑤ 公開サイトの脆弱性報告の課題

(イ) 診断を実施できない課題

- ・レンタルサーバを利用しており、脆弱性診断の実施を確認したが他利用者に影響の懸念があるためレンタル業者から拒否された
 - 実施内容の説明文書、これまでに影響がなかったことを伝えて頂いたが許可が下りなかったケースもある

(ロ) 診断時間の課題

- ・参加企業の環境で PFU からの診断通信が遮断されることで十分な診断を実施できないケースが存在する (PFU の IP アドレスからの遮断解除は不可とのこと)

(ハ) 報告書の課題

- ・レポートの内容が専門的すぎて具体的な対処方法が不明
- ・サーバ管理会社がレポートの授受を拒否する
 - 対処方法の記載箇所の説明と、サイト保守業者・担当者に説明する箇所を説明 (3社)
 - 保守業者やサーバ管理担当にお渡し頂ければ理解頂けると想定していたが、業者への説明を社長自ら説明を行わなければならないケースもあり、専門用語をどう伝えるかが課題
- ・レポートの詳細編に英文のままの箇所があった、英語で書かれるとわからない
 - サービス価格を下げるため、できるだけツールが出力する報告文面を使用した。今後の改善に努める必要あり、今回は適宜技術者が解説を実施した

(ニ) 再診断の課題

- ・対処が間に合わないため修正確認を行う次回診断日時を変更したい
 - 診断日の再調整を実施 (事業期間後半では診断日の空きがなくなるケースあり)

⑥ パソコンの脆弱性報告の課題

(イ) 報告書の課題

- ・Windows10 がサポート対象外と通知されるが、Windows10 内に半期アップデートのバージョンがあり、どのバージョンがサポート外で、どのバージョンにすれば良いのかが報告書ではわからない

→ 報告書の改善が必要

⑦ パソコンの脅威報告の課題

(イ) 脅威検知の報告レベル

「3(イ)当社採用のエンドポイント型の脅威検知位置 (UTM との違い)」で解説したとおり、インターネット境界位置、パソコン上の既存対策 (ファイアウォール、アンチウイルス) で対処されているものは検知対象とならない。

(ロ) 診断ツールの情報のみでは悪意のあるマルウェアであるか判断できないケースが地域実証中に発生するか

「3(イ)当社採用のエンドポイント型の脅威検知位置 (UTM との違い)」で解説したとおり、ツールが検知した脅威は全て通報するのではなく、確度が高く、外部インテリジェンスや PFU 分析担当の知見のフィルタリングの上、参加企業に通知しており、今回の実証事業の中では、特に判断できないケースは存在しなかった。

(ハ) 大手・中堅企業と中小企業の分析対応件数の差を可能な範囲で明らかにする

これまで大手・中堅企業のパソコン上へ本ツールを導入し、活用した調査では、多くの脅威を検知して、報告書作成にも時間を要していた。本事業を開始するにあたり、このようなケースが発生しないよう、前記「ロ」で記載したフィルタリングを実施したところ、想定以上に通報するような脅威は存在しなかった。既存対策で概ね対策ができていたことが伺える。

(ニ) マニュアルによる効率化が行えるか

地域の駆け付け対応要員が基本的な作業が実施できるよう、作業手順書の整備を実施したことで、多能工スキルを持っている保守エンジニアが作業を行えるようにした。

(ホ) 脆弱性診断に対する対策が進むことで検知件数が減少すること

今回は、通報する脅威が想定以上に少なかったことで、脆弱性対策が進んだことで減少しているかの判断には、母数が足りず、本項目の見解を出すに至らなかった。

⑧ 駆け付け対応支援 (インシデント初動対応) の課題

(イ) 地域実証中にこのような対処が必要となる件数

Emotet マルウェアの駆除作業 (1 回出動)

(ロ) 初動対応の総時間

対応調整: 60~90 分 (参加企業、サービス実行部隊、駆け付け対応要員)

対処時間: 往路 2 時間、対処 2 時間 (参加企業事業所)、帰路 2 時間

・ Emotet 感染パソコンからのオフライン駆除

・他パソコン2台の感染確認

対処日： 翌営業日以降で対応日時の調整

(ハ) その他

脅威への初動対応では上記のとおりであったが、これ以外に参加企業の環境を事前調査させていただくサービスヒアリングシートへの記載で、駆け付け対応要員の出勤依頼や、インストール作業において出勤依頼を求められている。脅威以外の出勤をどう取り扱うべきか検討が必要。

(ウ) 顧客担当者または公開サーバの委託先保守業者のスキルレベル

① 対応スキルは仮説どおりか

仮説は下記のとおり。

1. オンプレミスサーバを自社で保守されている企業

→ 担当者は構築実績があり、対処方法として設定変更や、サーバアプリケーションのバージョンアップを実施できると想定

2. レンタルサーバでコンテンツ開発業者に委託している企業

→ 問題点と対処方法が記載された報告書を渡すことで対処を実施頂けると想定

実際は、レンタルサーバの利用が殆どであり、サーバアプリケーションの管理まで業者側で行われている PaaS 環境では問題点の検出が少ないか、指摘することで対応頂ける。しかし、IaaS 環境のケースでは、サーバアプリケーションの初期インストールや初期設定のみ業者側で行われるものの、その後のサーバアプリケーションの保守が行われていないケースが考えられる。参加企業は保守を自身で行うのか、委託すべきか確認が必要と考える。ただし、参加企業自身で行うには、報告書に記載されている専門用語が多いという印象を受けられている。報告の内容を改善すべきか再検討も必要。

② 脆弱性情報を通知する粒度はスキルレベルに見合っているか

対応の優先度を考え、「危機的」「深刻」「中度」という分類で報告を実施。対処も危機的から実施されており、スキルに合わせた粒度で報告できたと考える。

(エ) サービス実施中の注意喚起

実証事業に参加されている参加企業に向けて下記の注意喚起を実施した。

2019/11/20~22 中間報告会: サポート終了、終了間近な OS の利用者について (注意喚起)
パソコン 509 台中、終了間近な Windows 7 が 118 台、Windows10 が 37 台。終了した Windows10 が 4 台。
2019/11/20~22 中間報告会: BlueKeep の脆弱性について (注意喚起)
パソコン 120 台中、WannaCry の再来かといわれている BlueKeep の脆弱性が公表され 6 か月経っても未適用な Windows7 が 6 台
2019/11/28: 中小企業への「Emotet」マルウェア感染拡大に関する注意喚起
2019/12/02: 中小企業への「Emotet」マルウェア感染拡大に関する注意喚起【追加情報】
情報処理推進機構、JPCERT/CC から発信された「Emotet」の注意喚起をお知らせ
2019/12/12: 中小企業への「Emotet」マルウェア感染拡大に関する注意喚起 (第 3 報)
55 社 パソコン 718 台中、Emotet から実行される攻撃者 2 次ツールが使う脆弱性(既報)が未適用 19 社 76 台
2019/12/26: 主要 Web ブラウザにおける TLS1.0/1.1 サポート終了について (注意喚起)
公開サイトの脆弱性診断を受けている参加企業の環境で、多く指摘されている ・ TLS Server Supports TLS version 1.0 (tls1_0-enabled) ・ TLS Server Supports TLS version 1.1 (tls1_1-enabled) について、2020 年 3 月からブラウザ側が非サポートになるため Web サイト等を TLS1.2 以降に対応させることを強く推奨。

(オ) サービス満足度と不満点

中間報告会、および最終成果報告会で得たアンケート結果から集約した。
 (フリーフォーマットで自由に記載されている情報を分類した。)

① 公開サイトの脆弱性診断

質問：サービスの効果	企業数
<ul style="list-style-type: none"> ● <u>意識が向上した(担当者や業者と脆弱性に対して対策を実施)</u> 	12
<ul style="list-style-type: none"> ● <u>意識は向上しなかった (理由を記載してください)</u> <ul style="list-style-type: none"> ・ <u>今後診断</u>を実施予定 ×2 ・ <u>脆弱性についての報告なし</u> ・ <u>既知の問題</u>が指摘されたが、<u>経営層</u>にとってはあまり<u>意識</u>されていない ・ サービスを活用したが、今のところ<u>何も変化がない</u> ・ 対応すべき<u>課題が多く優先度が上がりきらない</u> ・ <u>診断結果が専門的過ぎて</u>、サイト管理者が対処できる内容ではなかった ・ 今後確認予定で対策も必要と感じていますが<u>説明会がある</u> <u>とありがたい</u> 	8
<ul style="list-style-type: none"> ● <u>公開サイトの脆弱性診断を活用できなかった理由</u> <ul style="list-style-type: none"> ・ <u>公開サイトは無い</u> ・ <u>外部業者へ委託</u>していて他サービス利用顧客へ<u>影響がある</u> と困るため<u>委託先から断られた</u>ため ・ <u>レンタルサーバ</u>のため、他に<u>影響が出る</u>可能性ある ・ 公開サイトの運用を<u>外部サーバ</u>で行っているため ・ <u>管理会社に委託</u>しているため ・ <u>クラウドサービス利用</u>のためできなかった ・ 公開サイトが<u>外部のレンタルサーバ</u>上にあるため ・ サーバ切替えや複合機入替え時期と重なり通信不具合解消が優先となったため (<u>優先業務発生</u>) 	8

② パソコンの脆弱性検知

サービスの効果	企業数
<ul style="list-style-type: none"> ● 効果は全社に及んだ <ul style="list-style-type: none"> ・ 組織内で積極的に脆弱性の更新を行うようになった ・ セキュリティ対策の重要性の意識が高まった 具体的な動きをとるきっかけとなった ・ Windows <u>セキュリティが停止している端末があることに気づいた</u> 	<p>6</p> <p>1</p> <p>1</p>
<ul style="list-style-type: none"> ● 効果は管理者（担当者） <ul style="list-style-type: none"> ・ 管理者は問題点を把握できたが、組織内では特に変化はない 	13
<ul style="list-style-type: none"> ● 効果が得られなかった <ul style="list-style-type: none"> ・ 脆弱性を認識しつつも、使用中のアプリとの相性など更新を妨げる要因あり ・ 特に問題となる脆弱性は無かった ・ 1月から実施予定のため 	<p>1</p> <p>8</p> <p>1</p>

③ 駆け付けサービス

サービスの効果	企業数
<ul style="list-style-type: none"> ● 必要と感じる <ul style="list-style-type: none"> ・ サービスヒアリングシートの記載事項のヒアリング ・ インストール作業 ・ マルウェア駆除作業 ・ 今回の事業では、サイバー攻撃に伴うマルウェア駆除等の機会がなかった ・ 監視ツールで問題発生時の対処方法 ・ 他社セキュリティ機器の設定方法など指導してほしい ※今回の事業では対象外で回答 	<p>8</p> <p>7</p> <p>20</p> <p>1</p> <p>1</p> <p>1</p>
<ul style="list-style-type: none"> ● 要検討 <ul style="list-style-type: none"> ・ 費用と内容のバランス、類似サービスがあれば比較もしたい（必要と思うが検討して決定） ・ 企業規模に対する維持費用が下がれば必要 	<p>1</p> <p>1</p>
<ul style="list-style-type: none"> ● 必要ない <ul style="list-style-type: none"> ・ グループ企業に委託しているため ・ 疑問点・弊社の間違いに対するリカバリ対応もメールで十分対応して頂いた ・ 執務室に他業者の立ち入りは好ましくない（業務パソコン内を触る） 	<p>1</p> <p>1</p> <p>1</p>

④ 本事業に参加して良かったこと

良かったこと	企業数
<ul style="list-style-type: none"> ● 自社の現状を認識（社内の意識向上） ● 情報セキュリティ自社診断の結果に対するフィードバックを入手できた事 ● 情報セキュリティ自社診断のキッカケとなった ● 社のセキュリティ体制の客観的診断を元に社内へ展開できた ● 現状を知れた ● 現状の状況が見える化できた ● 他社と比較して自社のセキュリティ対策が劣っている認識ができたこと ● 他社の対応状況がわかり社内で進めやすい ● 客観的なご指摘をいただいた ● 取り組み出来ている所、不足している所が洗い出しできた ● 社内の意識向上に役立てられた ● 上層部の意識が（少し）向上した ● 動機付けに良い機会だった 	<p>1</p> <p>1</p> <p>1</p> <p>1</p> <p>1</p> <p>1</p> <p>1</p> <p>1</p> <p>1</p> <p>1</p> <p>1</p> <p>1</p>
<ul style="list-style-type: none"> ● セキュリティの知識向上 ● サイバーセキュリティに対する知識が高まった（深まった） ● 今まで知らなかったことも多くあり、勉強になった ● 情報漏洩への不安（わかった） 	<p>2</p> <p>1</p> <p>1</p>
<ul style="list-style-type: none"> ● 公開サイトの脆弱性を認識 ● Web サイトの Check で問題がなかった 	<p>1</p>
<ul style="list-style-type: none"> ● パソコンの脆弱性を認識 ● 対応すべき作業（Adobe 更新）がわかったこと 	<p>1</p>
<ul style="list-style-type: none"> ● 既存対策をすり抜ける脅威を認識 ● アンチウイルス対策のソフトからすり抜けたものがない事がわかって安心した 	<p>1</p>
<ul style="list-style-type: none"> ● 無料サービス ● 無償でサービスを受けられること 	<p>1</p>
<ul style="list-style-type: none"> ● その他 ● IPA の事後対応マニュアル等役立つ情報が入手できた ● プログラムの配布は Active Directory グローバルポリシーの勉強になった 	<p>1</p> <p>1</p>

⑤ 本事業で改善すべきこと

改善すべきこと	企業数
<ul style="list-style-type: none"> ● パソコンへのツール多数導入の負担（アンインストール負担） <ul style="list-style-type: none"> ・ 1人情報システム担当で、50台のPCにクライアントを短期間で導入するのは不可能だった ・ Active Directory による導入方法が掛かっているが設定で悩んだ 	<p>1</p> <p>1</p>
<ul style="list-style-type: none"> ● パソコンへの導入失敗 <ul style="list-style-type: none"> ・ インストール後に、一部の設定ファイルが複写されておらず監視サービスに繋がらない 	<p>1</p>
<ul style="list-style-type: none"> ● 環境調査が難しい <ul style="list-style-type: none"> ・ プロキシサーバの有無や IP アドレス、ポート番号の確認を求められたが調査方法が分からない（説明書をもらったが調査しにきてほしい） 	<p>1</p>
<ul style="list-style-type: none"> ● 業務影響が発生 <ul style="list-style-type: none"> ・ 低スペックのPCのCPU負荷が高く動作が遅くなった ・ PCに入れたソフトの影響か、社内ほとんどのPCの動作が重くなった ・ 各端末で動作の遅くなるソフトや作業が見受けられる ・ インストール直後、OSの再起動に時間がかかった（15分弱） ・ ソフトの起動に時間がかかる 	<p>1</p> <p>1</p> <p>1</p> <p>1</p> <p>1</p>
<ul style="list-style-type: none"> ・ 業務アプリが起動できなくなった （提供された脅威検知ツールをアンインストールしたら起動できるようになった） 	<p>1</p>
<ul style="list-style-type: none"> ● 用語が難しい <ul style="list-style-type: none"> ・ アンケートの質問や、システムの設定が、分からないことが多い 	<p>1</p>
<ul style="list-style-type: none"> ● 指摘に対する対策が分かりづらい <ul style="list-style-type: none"> ・ どのように対策するのが不明（公開サイトの診断） ・ 自社がセキュリティに問題があるのかわかりません 	<p>1</p> <p>1</p>
<ul style="list-style-type: none"> ● 社内への意識づけ <ul style="list-style-type: none"> ・ 社内参加を任意にしたところ参加率が悪い 	<p>1</p>
<ul style="list-style-type: none"> ● コンサルティング <ul style="list-style-type: none"> ・ 当社の使用するパソコン状況を教えてくれること 	<p>1</p>

⑥ 今後の有償サービスに向けて期待すること

期待すること	企業数
<ul style="list-style-type: none"> ● 定額制 <ul style="list-style-type: none"> ・ 定額制（PC台数ではなく、サイト数で低価格が望ましい） 	1
<ul style="list-style-type: none"> ● 低価格 <ul style="list-style-type: none"> ・ 1ライセンス年間 3000 円以下（月額 250 円以下）であって欲しい ・ <u>低価格</u>、わかりやすさ ・ 低コスト（ライトプラン等） 	1 1 1
<ul style="list-style-type: none"> ● 指摘事項を分かりやすく説明（公開サイト診断） <ul style="list-style-type: none"> ・ Web 診断結果は、200 ページ以上の資料を頂いても、対応できないので、もっと<u>噛み砕いた説明</u>があると助かります！ 	1
<ul style="list-style-type: none"> ● 業務影響のない軽さ <ul style="list-style-type: none"> ・ もう少し軽く動作してほしい！ 	1
<ul style="list-style-type: none"> ● 保険・診断・検知・遮断/駆除に加え、社内教育セミナーをセット <ul style="list-style-type: none"> ・ 保険と年 1～2 回のセキュリティ診断、<u>社員への外部教育セミナーをセット</u>にしたサービスがあるとよい ・ 予想される事業や、講習 ・ 定期的なセミナーがあると理解しやすいと思う ・ 侵入検知、拡大防止、対策のアドバイス（代行あれば良）、社内教育補助、維持サポート 	1 1 1 1
<ul style="list-style-type: none"> ● 社員のセキュリティ意識調査（メール訓練） <ul style="list-style-type: none"> ・ 社員への不正メールテストでセキュリティ意識調査 	1
<ul style="list-style-type: none"> ● 社内環境の脆弱性診断 <ul style="list-style-type: none"> ・ インフラや社内 NW への攻撃テストなどをして対策状況をテスト 	1
<ul style="list-style-type: none"> ● アセスメントサービス <ul style="list-style-type: none"> ・ 自社の対策が十分なものなのか、第 3 者の視点での評価が欲しい 	1
<ul style="list-style-type: none"> ● トータルなサービス <ul style="list-style-type: none"> ・ UTM,保険、BCP 等を総合的に、安価にできるサービス等もあれば良いかと思う 	1
<ul style="list-style-type: none"> ● 脅威の検知対象の拡充 <ul style="list-style-type: none"> ・ 未知の脅威 	1
<ul style="list-style-type: none"> ● データ保護機能の追加 <ul style="list-style-type: none"> ・ お客様情報などのデータの保護 ・ 全従業員がメールで情報を送る時のファイルのパスワードを保護する事 	1 1 1
<ul style="list-style-type: none"> ● 迅速な対応 <ul style="list-style-type: none"> ・ 迅速な対応など 	1

⑦ 今後の有償サービスに向けて改善すべきこと

改善すべきこと	企業数
<ul style="list-style-type: none"> ● 日刊レポートを充実させる <ul style="list-style-type: none"> ・ 毎日のレポートをもっと詳細な方が良い、ある/ない の一文のみでなく、PC 名もしくは IP で区別した一覧表でレポートになっていると便利 	1
<ul style="list-style-type: none"> ● 管理者用の管理画面の提供 <ul style="list-style-type: none"> ・ 管理者向けの監視アプリケーション 	1
<ul style="list-style-type: none"> ● 対策が分かりづらい <ul style="list-style-type: none"> ・ 対応を簡潔にしてほしい（公開サイトの脆弱性診断） ・ 対策の日本語化の精度をアップ！（公開サイトの脆弱性診断） 	1
<ul style="list-style-type: none"> ● ツールの導入が難しい <ul style="list-style-type: none"> ・ PC の知識がない人でもクライアントのインストール、アンインストールができるようにしてほしい ・ アンインストールは一部、依頼しないと行えなかった 	1
<ul style="list-style-type: none"> ● 業務影響 <ul style="list-style-type: none"> ・ ソフトを入れた時点で PC の動作が遅くなったところ！ ・ （ソフトの）高速化 ・ インストールしたアプリの安定化 	1
<ul style="list-style-type: none"> ● サービス分割してオプション化 <ul style="list-style-type: none"> ・ いくつかのメニュー（コース）を選択できるといいかもしれない ・ 保険と同じでパッケージ化されていると管理しやすい 	1
<ul style="list-style-type: none"> ● サービス分割して低価格化 <ul style="list-style-type: none"> ・ 低価格であると導入しやすい（納得できる価格） ・ 月額費用が高いと導入できない 	1
<ul style="list-style-type: none"> ● 公開サイト脆弱性診断の低価格化 <ul style="list-style-type: none"> ・ 公開サイトに対するセキュリティ対策費は、会社規模やサイトに対する比重に関係なく高額でやりたくても手をだせないのが実態、その点を考慮した価格体系を望む 	1

6 実証結果を踏まえた検討の実施

本実証で得た情報をもとに、中小企業に向けた最適なサービスを検討する。

(ア) 中小企業のサイバーセキュリティ対策が進まない要因分析

今回の実証を通じ、アンケート、および顧客や IT サービスを販売する地域販社からの情報をもとに、中小企業に向けたサービスを検討するうえで考慮すべきポイントを挙げる。

<顧客の状況（傾向）>

- ・ 経営層がサイバーセキュリティ対策の重要性を意識していない
- ・ 情報システム担当者がいない、体制・スキルが無いなど、具体的な検討に入る前提が整っていない
- ・ 対策に割り当てられる費用は限られている
- ・ 対策製品を導入したが、アラート内容等を購入先に問い合わせても返答がない
考察：販売側の課題、アンチウイルス製品と同じ感覚で販売している
- ・ 他社の対策状況はとても気になる

*実証における対応例

実証参加募集活動において、現場担当の判断で実証参加を申請したが経営層の理解を得られず参加取りやめとなったケース、総務部長が IT 担当であるケースが多く、業務多忙で参加取りやめとなったケース。

<地域の IT サービス販売会社の状況> 提案スキルのある人材が不足

- ・ 顧客の現状把握、最適な提案、どちらも難しい
- ・ 商談が長引く、最終的に成約に至らないケースが多い
- ・ お助け隊のサービスは提案しやすい印象（提案スキル、手離れの良さ）
考察：対策機能+対策サービス+最後まで面倒をみる駆け付け対応まで含むコンセプト。国が推奨する対策の安心感。

*実証における対応例

実証参加募集活動において、勧誘に成功する確率は、PFU 対応要員 > IT サービス地域販社 > 保険会社の順と捉えている（定性的）。対策サービス普及に向けては、販売側のサイバー対策に関するスキル向上が必要であること、相反することだが専門スキルをなるべく排除した分かり易い商品仕立てにすることの両面が重要となる。

(イ) 中小企業へのサイバーセキュリティサービスの検討（事後対応支援）

事後対応支援について、サービスを普及させるために考慮すべき要件を整理する。

- ・ 専門スキルがない販売者と購入者間でも販売が成立できる分かり易さ
- ・ 最後まで面倒をみるサービスを目指すこと
- ・ サービス提供中、技術的に難しい作業や判断をなるべく顧客にさせないこと
- ・ 安価に提供すること

PC 脅威検知におけるエンドポイント型（以下、「EP 型」という。）と UTM 型の比較

当初の仮説を以下に示す。当社はマルウェアが検知された場合に、なるべく顧客側に作業負担をかけないようにリモートで対処でき、かつ、駆け付け対応出動回数を少なく抑えられること、これによりトータルで安くできるという仮説をもとに EP 型を選択している。

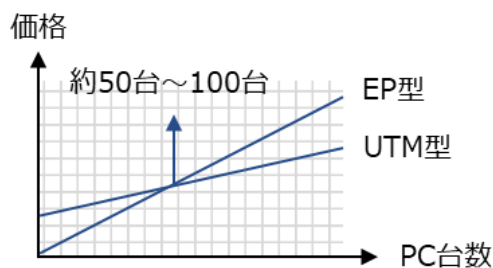
表 6-1. EP 型と UTM 型の比較

	EP 型	UTM 型	備考
初期導入	△	△	EP 型は PC にソフトを導入展開する必要あり。UTM はネットワーク遮断を伴う。
攻撃検知時の分析 （問題の特定）	○	△	インシデントの多くは PC 上で起こるが、UTM は間接的に検知するため、PC 実機の調査を顧客に依頼する必要がある。
端末調査・マルウェア隔離	○	×	EP 型は遠隔対応可能
マルウェア拡散状況把握	○	×	EP 型は特定したマルウェアのハッシュ値で拡散状況を把握。
駆け付け対応出動確率 （初動対応）	○	×高い	UTM は顧客に端末の状況を聞くケースがあるので確率が高いと想定される。
対策製品のトータルコスト	○小規模 ×大規模	×小規模 ○大規模	様々な価格帯の製品があるため、本情報は傾向を表す。*小規模・大規模は 1~500 名の範囲内の分類。

EP 型は、導入作業が負担であるという実証参加者の声があった。また、様々な PC 環境に導入するため、正常に動作しないケースや、PC の動きが遅くなった等の問い合わせがコールセンターの負担にもなった。

また、本実証では駆け付け対応は想定よりも少なかった。このことから、駆け付け対応（インシデント初動対応）はコスト高となる想定だったが絶対数が少ないため UTM 型であっても大きなデメリットにはならない可能性がある。多少中小企業側に確認作業等を強いるかもしれないが、企業規模が大きくなるにつれ価格優位性のある UTM 型がサービスタータルコストでも優位となるかもしれない。EP 型、UTM 型の両方を用意することで多くの中小企業をカバーできるためサイバーセキュリティ対策を普及させるためには 2 タイプを用意することが有効な手段と考えられる。

図 6-1. EP 型・UTM 型の価格特性イメージ



<PC 上の脆弱性監視機能について>

当初の仮説では、現在のサイバーセキュリティ脅威検知技術では 100%検知はできないことから、PC の脆弱性対応力（パッチ最新化率）を高めておき、マルウェアに感染しても被害にならない耐性強化をすることで、駆け付け対応による調査や復旧にかかるコストを低減し、サービスの低価格化と保険費用の低価格化にも貢献すると想定した。

実証を経て、Windows10 以降ではパッチ自動適用されるためこのサービス機能の価値低下が考えられるが、今後も自動適用しない PC も残ると考えられるため当面有効性があると考えている。

<PC の脆弱性に関する機能概要>

- | | |
|----------------------|----------------|
| ・ Windows 脆弱性 | 今後サービス価値低下の可能性 |
| ・ Office 脆弱性 | 今後サービス価値低下の可能性 |
| ・ Java 脆弱性 | 引き続き有効 |
| ・ Adobe 脆弱性 | 引き続き有効 |
| ・ サポート切れ OS 通知 | 引き続き有効 |
| ・ サポート切れが近い OS の事前通知 | 引き続き有効 |

(ウ) 提供サービス（事後対応支援）

実証を踏まえ、以下のサービスを提供する。

表 6-2. 中小企業に向けた考慮すべき要件への対応方針

中小企業に向けた考慮すべき要件	当社の対応
専門スキルがない販売者と購入者間でも販売が成立できる分かり易さ	・オールインワンサービス
最後まで面倒をみるサービスを目指すこと	・駆け付け対応 ・保険付きサービス
技術的に難しい作業や判断をなるべく顧客にさせないこと	・EP型をラインナップ ・駆け付け対応
安価に提供すること	継続的な取り組み課題 ・QA対応の省力化と人件費

表 6-3. 提供サービス（事後対応支援）

提供内容	顧客現状	EP型	UTM型
①ウイルス対策機能	○	○※1	—
②FW機能	○	—	○
③サイバー脅威検知機能	—	○PC	○NW
④遠隔からみまもり（SOC）	—	○	○
⑤相談窓口	—	○	○
⑥駆け付け対応（全国）	—	○※2	○※2
⑦PC脆弱性監視	—	○	○
⑧ベンチマーク診断・他社比較（年1回）	—	○	○
⑨サイバー保険	—	○※3	○※3
価格 （商品体系・価格）			

※1 既存のアンチウイルスソフトに重ねて導入できる。

※2 初動対応を行う（拡散防止処置、マルウェア隔離等はこの範囲）。本対応範囲は早期処置が必要であり、保険適用の可否判断の工程を挟むことで対応が遅れるデメリットがあるため保険適用範囲としない考え。

※3 悪性のマルウェアと判断し、デジタルフォレンジックやマルウェア解析、などを伴う詳細調査が必要となった場合、大量のPCへの処置が必要となる場合に保険を適用する考え。

<公開サイトの脆弱性診断>

必要とする顧客としない顧客があることから、独立したサービスとして提供する。今後、事後対応支援サービス契約者への優遇価格等を検討していく。

表 6-4. 提供サービス（公開サイトの脆弱性診断）

提供内容	中小企業向け価格
リモート診断・基本サービス（1 IP 付き）	※ ¥80,000/回
リモート診断・1 IP 追加	※ ¥20,000/回

※ サービス内容を見直しさらなる低価格化を推進する。

(エ) 機能毎の体制

「5(イ)運営で得られた課題」に記載した運営体制で実施可能である。

① 相談窓口体制

(イ) 必要なスキル

1. 一般的なビジネススキル（電話対応・メール作成）+PCスキル+セキュリティに関する知識
 - ・日本コンタクトセンター検定 オペレーション
 - ・CompTIA A+, Network+, Security+
2. 技術的なサービス内容や脅威内容に関して回答を実施するスキル
 - ・CISSP（参加企業からの質疑対応・事業説明など）
 - ・**情報処理安全確保支援士（サービス実行の対応）**

(ロ) 必要な人数

サービス開設時間：9～17時（12～13時を除く）

サービス開設日：平日のみ（土日祝日・夏季冬季の休暇日を除く）

1. コールセンター：4名（常時2名、必要に応じて応援2名）
2. サービス実行部隊：4名（常時2、必要に応じて応援2名）

② パソコンの脆弱性検知と報告

(イ) 必要なスキルと人数

完全に自動化されており、特別なスキルは必要としない。

③ パソコンの脅威検知と報告

(イ) 必要なスキルと人数

パソコン上での検知、および外部インテリジェンスを活用した脅威の確度を確認する部分は、システム化されており、特別なスキルや対応者は不要。最後に、過去の知見から参加企業に報告すべきか最終判断するために、分析担当1名が必要。

④ 駆け付け対応支援（インシデント初動対応）

(イ) 現地駆け付け対応要員へ指示する SOC 側に必要なスキル

脅威・脆弱性に対する回答スキル

・ CompTIA A+, Network+, Security+

(ロ) 現地駆け付け要員のスキル

一般的な PC 操作・顧客対応スキルに関する知識。

最新のオフラインアンチウイルスソフトを持ち込んで実施すること、必要に応じてセキュリティオペレーションセンター技術員からの遠隔指示により、作業を実施できるスキルを必要とする。

・ CompTIA A+, Network+, Security+

(ハ) 現地駆け付け要員の人数

サービス開設時間：9～17時（12～13時を除く）

サービス開設日：平日のみ（土日祝日・夏季冬季の休暇日を除く）

駆け付け隊：県毎に1名待機（必要に応じて増員、最大時は地域に2名）

⑤ 公開サイトの脆弱性診断と報告

(イ) 必要なスキル

参加企業の脆弱性・脅威の分析・報告書の作成に関する知識。

・脆弱性診断士の経験、報告書作成のスキル

(ロ) 必要な人数

・診断者、および報告作成者1名

・報告書の確認者1名（別要員）

⑥ その他（契約からサービス開始までの事務局体制）

(イ) 必要なスキル

・一般的なビジネススキル（電話対応・メール作成）

・必要に応じて法務部門に個別相談（個別、秘密保持契約など）

(ロ) 必要な人数

サービス開設時間：9～17時（12～13時を除く）

サービス開設日：平日のみ（土日祝日・夏季冬季の休暇日を除く）

受付業務：1名

⑦ その他（インストールモジュール作成と送付の事務局体制）

(イ) 必要なスキル

手順書に従い、参加企業から回答頂いたサービスヒアリングシートに従い、個社毎の設定を行ったインストールモジュール作成を行う、特別なスキルは不要

(ロ) 必要な人数

サービス開設時間：9～17時（12～13時を除く）

サービス開設日：平日のみ（土日祝日・夏季冬季の休暇日を除く）

作成業務：1名（依頼時5分程度）

確認業務：1名（依頼時5分程度）

(オ) 顧客が委託する公開サーバ保守業者のスキルレベル

「5(イ)⑤公開サイトの脆弱性報告の課題」に記載のとおり、構築した社内担当者が報告書を見て対処されるケースと、サーバ保守業者に報告書の対処を依頼するケースを想定していたが、会社代表が理解し、サーバ保守業者へ依頼するケースも存在した。本事業では電話対応で解説したが、参加企業が報告書を読んで理解して、業者へ依頼が行えるよう、専門用語を更に排除して理解頂けるよう改善する必要がある。

(カ) IT シルバー人材センターのスキル調査

① 必要スキルを有する人材有無、対象となる人数の確認結果

公益社団法人石川県シルバー人材センター連合会（配下 18 地域のセンター）
公益社団法人富山県シルバー人材センター連合会（配下 15 地域のセンター）
公益社団法人福井県シルバー人材センター連合（配下 15 地域のセンター）
上記 3 センターへヒアリングした結果、石川県、福井県から回答あり。

【期待するスキル】

- ソフトウェアインストール、アンインストール作業（手順書に従った作業）
- パソコンから調査資料を採取（遠隔で指示された情報の採取）
- パソコンのマルウェア（ウイルス）駆除作業（ツール実行を期待）

【在籍されている人材】

- ソフトウェア開発（プログラマー）の職歴のある人材として、福井市 17 名、坂井市 1 名が在籍していました。予定がなければ翌日対応も可能（福井県）
- 石川県内のいくつかのシルバー人材センターへ問い合わせしてみたところ、ご質問の作業に対応できる人材はほとんどいないとの回答だった（石川県）
※同会社への再雇用や、他社への再就職を行うなど、IT 会社に所属されていた人材は登録自体が少ない

【秘密保持契約等の個別契約】

- センターとしても会員としても可能（福井県）
- 危険を伴う仕事や責任が重い仕事について、原則として請けないようにしている。このため、秘密保持契約が必要な仕事というのは、シルバー人材センターの会員にとっては責任が重いため、契約することは難しいのではないかと考える（石川県）

【作業費用感（福井県の回答例）】

- ソフトウェアインストール、アンインストール作業（手順書に従った作業）
- パソコンから調査資料を採取（遠隔で指示された情報の採取）



- パソコンのマルウェア（ウイルス）駆除作業（ツール実行を期待）



② サービス価格を抑える対策として効果

シルバー人材センター連合会は個人情報取り扱いの問題もあり、また、人材データベースにはアクセスできないこともあり、実際は県内に点在する各地域センターと人材の確認や契約を行う必要がある。作業品質に関しての課題として、参加企業のパソコン内の操作を行うにあたり、秘密保持契約の締結が必要な事、顧客環境破壊を起こさないための教育の課題がある。秘密保持契約に関しては、ヒアリングの中でも「荷が重い」という意見があった。さらに操作誤りによる顧客環境破壊等に関してはITに詳しい人材がそもそも少ないという現状もありハードルが高い。事業責任者として現状のまま活用する選択は難しい。当社でもIT会社として定年後の再雇用制度を持っており、このような当社に帰属するシルバー人材世代の人材を生かすことで、秘密保持契約や操作内容の担保が行えるものと考え、低価格化と品質の両面を実現できると考える。

(キ) 前提とするセキュリティ対策の適用増加とサービス価格の検討

- ① 企業規模、業種ごとの地域実証期間の対策の進捗と、企業からのコール数が減少する仮説
- ② 前提とするセキュリティ対策状況が進むことでコール数の減少する仮説が正しいか（サービス側の対応人数は現状で可能か）

※①、②は、脆弱性の対策が進み、脅威の問い合わせが減る想定を行っていたが、本事業では脅威の通知数が少なかったことから、この相関を得ることができなかった。本事業で構築したサービス体制で特に人員不足は発生しなかった。

(ク) 中小企業向けのサイバー保険検討

アンケートの傾向では、情報漏洩等により引き起こされる損害賠償は、大きな損失の可能性を感じやすいことから保険の必要性を直感的に感じる傾向にあるが、発生の頻度が想像しづらいことや、サイバー保険が普及していない実情から保険加入に踏み切るだけの具体性がイメージできていないと考えられる。

一方、インシデント対応（調査・復旧）については、損害賠償と比べてかかる費用をイメージしやすいため費用対効果の感覚を得やすいが、莫大な損失までには至らないという感覚を持たれている可能性がある。保険の普及に向けては、身近な損失をリアルに伝えることが重要と考える。

一つのアプローチ方法として、対策をしてもサイバー攻撃によるインシデント対応（調査・復旧）は無くならないこと、運悪く悪性のマルウェアに侵された場合はデジタルフォレンジック等の高額な調査サービスをうける必要があること等、ITサービスベンダーであるPFUが年間何件も対応している事実として伝えていくこともサイバー保険加入のきっかけにできると考える。

① 中小企業におけるセキュリティ投資金額に見合った対策と保険価格

(イ) 企業規模と業種におけるセキュリティ投資額

「3(ウ)②診断結果の傾向」 の 2.5 を参照

(ロ) リスク軽減策（予防・検知対策費用）とリスク移転策（サイバー保険費用）のバランス

サイバー保険への加入条件として最低限のサイバーセキュリティ対策をしていることが前提となるが、これからサイバーセキュリティ対策の導入を検討する多くの中小企業向けには「対策サービス+保険付帯」の形態とすることで保険検討のきっかけとなり、また、サイバーセキュリティ対策サービスを提供するベンダーとしてもインシデント初動対応から情報漏洩調査までシームレスに対応できることから費用が無いから調査ができないといった状況に陥らず十分なサポートが可能となる。

尚、「対策サービス+保険付帯」の場合、保険部分は景品類として扱われるため保険範囲は小さくなる（費用は安いが補償も小さい）。以下のようにまず身近に発生しうるインシデント対応費用の一部を補填することで保険加入のきっかけになると考える。

- ・事故対応関連費用： 例) インシデント対応までとし情報漏洩調査は範囲を限定
- ・損害賠償関連費用： 例) 保険に含めない（保険単品商品として保険会社が売る）

表 6-5. インシデント対応時の費用負担

	インシデント初動対応	情報漏洩等の高度分析 (専門技術者)
セキュリティサービス費用	●	—
サイバー保険費用	—	●

実証事業における駆け付け対応実績は 1 件でインシデント初動対応にて問題解決したため、上記のサイバー保険費用と定義する作業の機会は無かった。

② サービスの加入条件、実施条件、免責事項

(イ) 保険費用を抑える条件の明確化 (必要なセキュリティ対策等)

保険費用を抑えるにあたっては、「セキュリティ対策を講じていること」や「過去に漏洩事故がないこと」の観点で事前チェックをすることを検討している。今回の実証事業を踏まえ、下記観点により保険費用を抑えることが可能。

- セキュリティ対策を講じていること
「対策サービス+保険付帯」の形で提供することで条件をクリアできる。
- 過去に漏洩事故がないこと
加入前の診断・アンケート等による確認をすることで状況を把握する。今回の実証では、北陸三県の駆け付け対応実績は 1 件、インシデント初動対応の範囲で問題は解決している。日常的に発生するものではなく稀に発生するという感覚、確率的には想定よりも少ない感触を得ている。

③ サイバー保険がカバーすべき内容

(イ) 過去のサイバー攻撃被害と対応内容から保険が必要なケースの明確化

企業にとっては予算化できない突発的に発生する高額な調査・復旧と損害のリスクに備えることができるサイバー保険は基本的に有効である。調査・復旧に高額な費用が掛かるケースを列挙する。

表 6-6. 調査・復旧に高額な費用が掛かるケース

対応事例	保険の有効性	概算費用
重要データを持たない公開サーバがアタックされ踏み台にされた。	○有効	数百万円
サーバがアタックされた形跡があり、複数年分のログ調査、影響範囲調査、情報漏洩調査を数週間にわたり実施。	○有効	数百万円
マルウェアとしては認識されていない不審な動作をするプログラムを調べてほしい。	○有効	数百万円
1 台の PC から既知のマルウェアが検知され、駆け付け対応により拡散防止処置と駆除を実施。	△IT サービスでも対応可	数万円
公開サーバに脆弱性がありサイバー攻撃に遭う危険性があるので対処したい。	×IT サービスの対応範囲	数十万円

④ サイバー保険を付帯したセキュリティ対策サービスの商品案

以下、インシデント対応と情報漏洩の疑いを調査するところまでの最低限の範囲を中小企業向けサイバー保険とする案である。これにより日常的な対策と運用にかかるコストの安定化が図れる。

表 6-7. 中小企業向けのサイバー保険検討（案）

No.	内容	インシデント 対応	情報漏洩 対応	中小向け 選定案	オンサイト 初動対応
1	サイバーシテの有無判断ため外部調査依頼費用	レ	レ	○	初動範囲
2	事故現場に専門家を派遣する人件費、交通費 等	レ	レ	○	初動範囲
3	事故の拡大の防止に努めるために要した費用	レ	レ	○	初動範囲
4	事故の原因調査および再現実験に要する費用	レ	レ	○	初動範囲
5	第三者へのコンサルティグ、指導等の費用	レ	レ	○	初動範囲
6	弁護士等への相談費用	レ	レ	○	-
7	事故現場の保存、事故の状況調査等の費用	-	レ	○	-
8	調査状況等の文書作成の費用	-	レ	○	-
9	再発防止策を実施する費用	-	レ	○	-
10	コールセンターの設置、運営等の費用	-	レ	×	-
11	謝罪文の作成・送付に要する費用	-	レ	×	-
12	信頼回復のための会見、発表、広告等の費用	-	レ	×	-
13	他人に対して損害賠償請求を行うための争訟費用	-	レ	×	-
14	見舞金、品購入費用および発送費用	-	レ	×	-
15	漏えいした情報の不正使用を監視するための費用	-	レ	×	-
16	データ復旧費用	-	レ	○	-
17	情報機器等修理費用	-	レ	○	-

表 6-8. 中小企業向けのサイバー保険考慮すべき事項

分類	検討項目	検討手法・今後
補償内容 ／保険料	中小企業に適 した補償内容	セキュリティ意識調査とベンチマーク診断による要望・要件確認し、実態に合う補償内容の検討。補償内容は、賠償とインシデント対応（調査・復旧）についての費用でも全てを網羅するのではなく範囲を絞り設計することが望ましい。 （保険料を抑えることにも関連）
商品形態	中小企業が利用しやすいサイバー保険の商品形態	加入の簡便さに重きをおく企業もあり、セキュリティ対策に付帯する形態で保険がついているようなプランがあれば望ましいとの声が多くみられた。

(ケ) 全国展開

① 各地域に必要な体制と規模間（人数）を決める指標

各地域では、駆け付け対応支援するエンジニアが該当するが、各県ごとに在籍するサーバ製品、ネットワーク製品の保守や導入サービスを提供する保守エンジニアの多能工化により人員整備することができる。各県の人員数は、受け持つ企業数に比例するが、本事業では100社2名体制で運営することができた。

必要な人員配備計画の考え方は、本実証におけるインシデント対応に要した駆け付け対応の所要時間は約5H（1回出動＝移動含み約5H）であり一般的な月間総稼働時間160Hのうち有償稼働率75%の120Hを実働可能時間とすると4.2%程度となり、**2名体制で2,380社**程度まで対応できる計算となる。

② 各地域の体制構築に向けた必要なスキルの育成を行う教育内容と教育計画

「5(イ)運営で得られた課題」に記載したスキルを事前に習得し、事業フローの説明を、社内教育システム(e-learning)を使い実施する。分析担当については、セキュリティオペレーションセンター側に集約されているため、実施者からの指導によりオンザジョブトレーニングを実施する。