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：大阪府、京都府、兵庫県）

成果報告書

請負事業者：大阪商工会議所

目　次

１．事業の全体像

（１）事業実施にあたっての現状認識

①京阪神の中小企業におけるサイバー攻撃およびサイバーセキュリティの現状

（イ）概観

京阪神は各分野の主導的企業とそのサプライチェーンに属するあらゆる業種の中小企業が集積し、京阪神のみならず全国・世界に商品・サービスを供給している。

（ロ）大阪商工会議所の事前調査（本実証事業前に独自実施）から見えてきたこと

○大阪商工会議所が 2017 年 6 月、関西の中小企業 315 社に行った「中小企業におけるサイバー攻撃対策に関するアンケート調査」では、

(a)「現状のセキュリティ対策で十分でない」と考える企業が約 7 割（68%）。その理由として「経費がかけられない」が 60%、「専門人材がいないのでわからない」が 48%など、経費と人材の課題が明らかになった。

(b) ファイアウオールや UTM の導入企業は 56%、情報漏洩賠償責任保険等に加入している企業は 9%。事前対応、事後対応ともに不十分なのが実態。

(c) 4 社に 1 社が実際にサイバー攻撃の被害を経験（標的型攻撃メール 18%、ランサムウエア 7%）。中小企業にも攻撃が及んでいることが明らかになった。

○中小企業へのサイバー攻撃の実態を更に詳細かつ客観的に調べるため、大阪商工会議所は神戸大学と東京海上日動火災保険株式会社（以下「東京海上日動」という。）との共同研究により、大阪の多様な業種、規模の中小企業等 30 社にて 2018 年 10～1 月、「中小企業を狙ったサイバー攻撃の実態を調査・分析する実証事業」を行い下記が明らかになった。

(a) 30 社全てでなんらかの不正な通信があった旨を示すアラートのログがあった。

(b) 8 種類の脆弱性やポートを狙った攻撃があり、外部から端末をリモート操作されている事例、社内端末と外部悪性サイトが双方向通信している事例、暗号化通信を解読できる状態にされていた事例等が確認された。

○いわゆる「サプライチェーン攻撃」の深刻化をふまえ、大阪商工会議所は全国の大企業・中堅企業 118 社に対し 2019 年 2～4 月、「サプライチェーンにおける取

引先のサイバーセキュリティ対策等に関する調査」を行い下記が明らかになった。

（a）大企業・中堅企業の約７割（68%）は、取引先におけるサイバーセキュリティやサイバー攻撃被害について「あまり把握していない。」

（b）４社に１社が「取引先がサイバー攻撃被害を受け、それが自社に及んだ経験」があり、７%は被害も出た（情報漏えい、システムダウン、データ損壊等。）

（c）「取引先がサイバー攻撃を受けその被害が自社に及んだ場合に採り得る当該取引先への対処」として挙げられたのは、損害賠償請求（47%）、セキュリティソフト・ハード導入の依頼／要件化（37 %）、取引停止（29%）など。

②京阪神の中小企業において必要なサイバーセキュリティ（目指すべき方向性）

上記①より、京阪神の中小企業のセキュリティニーズは下記のとおり整理された。

（イ）自社へのサイバー攻撃に対する「気付き」と「実態把握」が必要

必要性を感じないのは、現実が正しく把握できていないからに他ならない。
客観的にサイバー攻撃を観測し見える化できるソフトやハードの導入が必要。

（ロ）「安価かつ簡便」なサイバーセキュリティサービスが必要

中小企業はお金と人材が不足し、ベンダーは安価なサービスを提供できていない。
安価かつ簡便なサービスを提供できる支援体制、サービス内容の検証が必要。

（ハ）「何を？」の前に「なぜ？」の理解が必要

セキュリティを“売上を産まない経費”と捉えがち。“会社の社会的信用を高める投資”という意識を持っていただくため、セミナーの開催で意識向上支援が必要。

（ニ）サイバーセキュリティ対策を持続的に有効とする「日常的運用」が必要

アンチウイルスソフトは入れているが「入れっぱなし」の事例が散見される。人材と時間が乏しいことに鑑み、運用（監視や更新）まで含むお任せ型サービスが必要。

（ホ）攻撃や被害を受けることを前提とした「事業継続力向上」が必要

「攻撃が被害化しないこと」「被害が実害化しないこと」「実害が事業停滞を招かないこと」が肝要。事前対策としてのアプライアンス（機器）と事後対策としてのインシュアランス（保険）の両立により事業継続力を高めることが必要。

（ヘ）供給側も需要側も「all or nothing」を乗り越えることが必要

既存のサイバーリスクに関する保険は加入社数こそ増加傾向にあるものの、依然低調であり、加入企業の保険金請求も少ない。前者は既存の保険が損害賠償やフォレンジックなどに備える本格的なものであり保険料が高いこと、後者は保険発動事由が発生している事実に気付いていないため請求をしないことなどが原因であると考えられる。今後は all or nothing ではなく、その中間的存在の保険商品の提供が望まれる。そのためには、加入と請求のしやすい、専ら費用損害を補償する簡易的保険も必要。

（ト）「点」でなく「線」でサイバーセキュリティを進めることが必要

中小企業と取引する大企業は「中小企業側が自己防衛すべき」と考え、中小企業は「取引要件でもないのにお金をかけて行動を起こしにくい」と考えている。しかしインシデント発生時には損害賠償請求や取引停止に遭う可能性もあり、中小企業での対策は急務である。そのためには、サプライチェーン全体でサイバーセキュリティを進めていくことが必要。

（２）実証事業目的・事業スキーム

①本実証事業の目的

上記の課題意識のもと、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：大阪府/京都府/兵庫県）（以下「本実証事業」という。）は、下記を事業目的とした。

（イ）京阪神における中小企業へのサイバー攻撃の最新実態や対策ニーズの詳細な把握
（ロ）中小企業が利用しやすい、安価・簡便かつ総合的なサイバーセキュリティサービス（事後対応の視点を重視した簡易的な保険が付帯するもの）の開発
（ハ）地域サイバーセキュリティ支援体制の構築と地域セキュリティ産業の振興
（ニ）サプライチェーンを構成する中小企業のサイバーセキュリティと信用力の向上

②本実証事業のスキーム・事業実施方法およびその特徴

上記事業目的を実現するため、下記の事業概要と実施方法にて実施した。実施にあたり、業務ごとに我が国で最も先導的と考えられる企業に再請負・提携して頂いた。

（イ）実証事業概要と各業務の実施者（助ける側）　表１

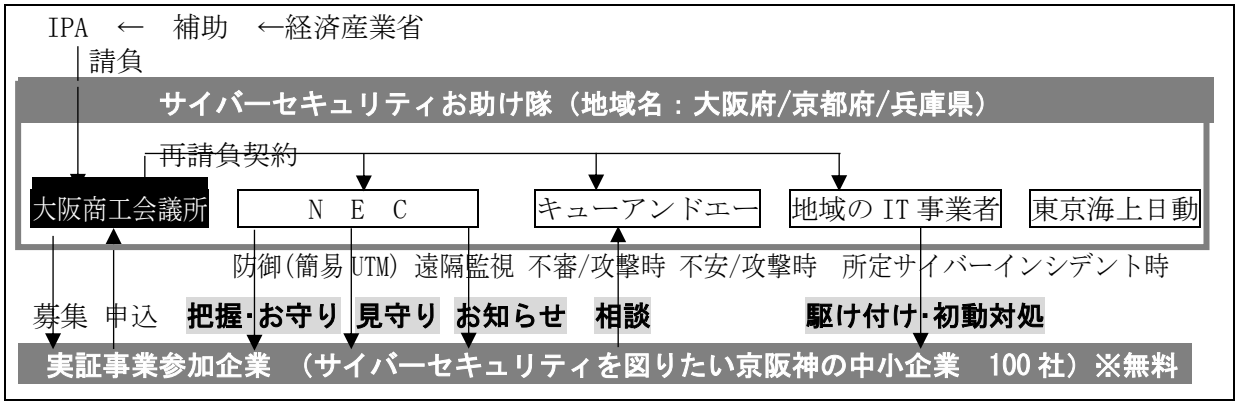
実証事業概要	主な実施者
(a) 簡易 UTM 設置によるサイバー攻撃の検知・観測・記録【把握】 ※設置・観測を以て実証への参加とする	日本電気株式会社（以下「NEC」という。）
(b) サイバー攻撃からの防御【お守り】	同上
(c) 簡易 SOC によるサイバー攻撃遠隔監視とアラート通知【見守り・お知らせ】	同上
(d) 電話やメールでの相談受付【相談窓口】	キューアンドエー（以下「キューアンドエー」という。）
(e) 所定サイバーインシデント発生時のお助け実働隊（地域 IT 事業者）（以下、お助け実働隊）によるオンサイトサポート・初動対処【駆け付け】	地域の IT 事業者、情報処理安全確保支援士等 11 者（詳細は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　参照）
(f) 中小企業が利用しやすいサイバーリスクに関する保険の検討（含む、発動しやすい簡易的な保険の検討）【保険】	東京海上日動

（ロ）実証事業参加企業（助けられる側）

大阪府、兵庫県、京都府のあらゆる業種・業態・規模の中小企業（中小企業基本法に基づく）で原則として UTM を設置していない企業 100 社。サプライチェーンを構成していると考えられる企業を中心とする。

（ハ）実証事業スキーム概略図

図１



（ニ）実証事業の実施方法（ここでは概要のみ）

○大阪商工会議所が実証事業の実施主体となり、IPA の仕様書および契約書に基づき全体の統括・運営を行うとともに参加企業の募集・応募受理・管理等の業務も行った。

○NEC は、上記（イ）の（a）（b）（c）部分を担い、本実証事業のために、既存商品をベースに、新しい特別な簡易 UTM を設計・製造した。この簡易 UTM は、導入と運用の簡便さを追求した機器であり、情報システム担当がいない、いわゆる「ゼロ情シス」の中小企業ですら容易に設置できること、ユーザー企業が能動的にアップデートを行う必要がないことを目指している。これにより、UTM を宅配便でユーザー企業に送り、分かり易い設置マニュアルに基づきユーザー企業自身が設置するという手法で実施し、その有効性を実証することとした。（上手く機能すればサービス提供価格を下げることが可）

○キューアンドエーは、上記（イ）の（d）を担い、参加企業からの相談や問い合わせを電話やメールで受ける役割を担った。NEC との密接な連携のもと能動的なお知らせも行った。相談の量、頻度、内容などをふまえ、対応人数や対応するうえでのスキルの検証を行い、商用化した場合の原価や売価の検討を行った。

○お助け実働隊を担う地域の IT 事業者は、大阪商工会議所と再請負契約を締結した

11 者により構成され、上記（イ）の（e）を担うほか、参加企業が自力で UTM を設置できない場合の訪問設置支援も行った。地域においてこのようなお助け実働隊を組織化し運用したのは、当実施体制の最大の特徴である。

○東京海上日動は、上記（イ）の（f）を担い、特に簡易的な保険の組成に向けた発動要件等の検証を行った。保険の対象になるか否かの審査を人手により個別に行うことはコストがかかるうえ審査担当者の主観的要素が入るため、UTM が観測した客観的なデータをもとに自動的に審査し決定できる手法の確立を目指した。

本実証事業が国費で実施される関係上、実際の損害保険金を参加企業に支払うフローは実施せず、保険種別の選定、保険の適用案件の特定、保険料・保険金の額の検討、発動要件の策定、保険金の支払いフローなどにつき実証の中で検討を行った。

２．事業説明会の開催

（１）第１回説明会（事業開始）

○日程：2019 年 7 月 5 日（於　大阪商工会議所）

○目的：（イ）地域の中小企業を対象に、本実証事業の周知及び参加を呼び掛けること

（ロ）サイバーセキュリティに関する普及啓発、セキュリティ意識向上

○概要：ユーザー向け（助けられる側）14:00～15:30

（イ）最近のサイバー攻撃の動向　【NEC】

（ロ）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【IPA】

（「SECURITY ACTION」及び「中小企業の情報セキュリティ対策ガイドライン」の説明含む）

（ハ）サイバーセキュリティ事後対応支援実証事業　【大阪商工会議所】

お助け隊実働隊向け（助ける側）16:00～17:00

（イ）お助け実働隊の募集概要および仕様概要説明【大阪商工会議所】

○成果：（イ）ユーザー向け 69 社(80 名)、お助け隊実働隊向け 29 社(38 名)出席。

（ロ）本実証事業への参加申込がユーザー39 社、お助け隊実働隊 16 社あった。

（ハ）アンケートでの中小企業のサイバー攻撃／対策・ニーズの最新状況把握

（２）第２回説明会（中間報告）

○日時：2019 年 11 月 6 日（水）14:00～16:00（於　大阪商工会議所）

○目的：（イ）地域の中小企業を対象に、本実証事業の中間報告を行うこと

（ロ）サイバーセキュリティに関する普及啓発、セキュリティ意識向上

○概要：（イ）「サイバーセキュリティお助け隊（京阪神）」での攻撃観測情報

（本実証を通じて収集した情報のフィードバック及び説明）

【大阪商工会議所、NEC、東京海上日動】

（ロ）中小企業における情報セキュリティ対策支援のご紹介　【IPA】

（「SECURITY ACTION」及び「中小企業の情報セキュリティ対策ガイドライン」の説明含む）

（ハ）「中小企業を狙ったサイバー攻撃の現状とその深刻さ」

【神戸大学大学院教授】

○成果：（イ）116 社（127 名）出席。3 社からユーザー追加参加申込があった。

（ロ）アンケートでの中小企業のサイバー攻撃／対策・ニーズの最新状況把握

（3）第3回（成果報告）

○日時：2020 年 2 月 12 日（水）14:00～16:00（於　大阪商工会議所）

○目的：（イ）地域の中小企業を対象に、本実証事業の成果報告を行うこと

（ロ）サイバーセキュリティに関する普及啓発、セキュリティ意識向上

○概要：（イ）「サイバーセキュリティお助け隊（京阪神）」での攻撃観測情報

【NEC、東京海上日動、大阪商工会議所】

（本実証を通じて収集した情報のフィードバック及び説明）

（ロ）中小企業における情報セキュリティ対策支援のご紹介【IPA】

（「SECURITY ACTION」及び「中小企業の情報セキュリティ対策ガイドライン」の説明含む）

（ハ）「セキュリティインシデントへの対応とそなえ」

【大阪大学情報セキュリティ本部兼大学院情報科学研究科　教授】

○成果：（イ）79 社（86 名）出席。

（ロ）サイバーセキュリティお助け隊（京阪神）の成果及び京阪神における最新のサイバー攻撃実態の紹介とそれを通じた啓発

（4）本実証事業を通じて収集した情報のフィードバック及び説明

○上述のとおり、本実証事業を通じて収集したサイバー攻撃ならびにサイバーセキュリティに係る情報を、参加企業を含む京阪神の幅広い中小企業に対し、事業説明会の場で説明（参加企業で不参加社には資料をメール送信）したほか、参加企業に対し、不定期にメールや訪問での注意喚起（IPA からの案内に基づく Emoted 関係情報提供、新型コロナウイルスを題材とした攻撃メールの情報提供など）を行い、中小企業におけるサイバーセキュリティの意識向上を図った。

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　参加企業各位（サンプル）

いつもお世話になり有難うございます。大阪商工会議所です。
このほどＩＰＡより、「Emotet」マルウエア感染について専門の相談窓口の案内が寄せられましたので、下記のとおり、ご案内申し上げます。

（中略）

2014 年に初めて確認されたバンキングトロジャン「Emotet」マルウエアは、
広く拡散し柔軟に変化するマルウエアとして、今日まで数年間にわたって流行を続け被害をもたらしています。

（中略）

IPA 情報セキュリティ安心相談窓口
メール　　（以下略）
電話

図２

３．中小企業の実態把握

（１）本実証事業でのアンケート等による把握

①京阪神の中小企業におけるサイバーセキュリティおよびサイバー攻撃の実態

下記アンケート調査により、京阪神の中小企業におけるサイバーセキュリティの実態やニーズの最新動向が明らかになった。

表２

Ⅰ．情報システム担当者の有無	7/5 第１回説明会 n=69（参加企業以外も含まれている）※複数回答あり	11/6 第２回説明会 n=118（参加企業以外も含まれている）	11 月中間アンケート	１月最終アンケート n=105（参加企業）
専任者がいる	20（29%）	29（25%）	―	9（9%）
兼任者しかいない	24（35%）	53（45%）	―	34（32%）
１人もおらず経営層が直轄	18（26%）	24（20%）	―	52（50%）
１人もおらず IT 業者に外注	8（12%）	12（10%）	―	10（10%）

表３

Ⅱ．サイバー対策年間経費（正社員情シス担当者人件費除く）	7/5 第１回説明会 n=61（参加企業以外も含まれている）	11/6 第２回説明会 n=101（参加企業以外も含まれている）		11 月中間アンケート n=65（参加企業）		１月最終アンケート n=104（参加企業）	
				１万円未満	22（33%）	１万円未満	36（35%）
				１～３万	18（28%）	１～３万	27（26%）
５万以内	31（51%）	５万未満	28（28%）	４～６万	９（14%）	４～６万	13（12%）
６～10 万	10（16%）	５～10 万	24（24%）	７～10 万	６（9%）	７～10 万	８（8%）
11～15 万	7（11%）	11～20 万	14（14%）	11～20 万	３（5%）	11～20 万	９（9%）
16～20 万	2（3%）						
21～50 万	5（8%）	21～50 万	15（15%）	21～30 万	４（6%）	21～30 万	４（4%）
				31～50 万	０	31～50 万	３（3%）
51～100 万	2（3%）	51 万以上	20（20%）	51～90 万	１（2%）	51～90 万	２（2%）
101 万～	4（7%）			100 万以上	２（3%）	100 万以上	２（2%）

表４

Ⅲ．サイバー攻撃対策のセキュリティ実施状況	7/5 第１回説明会 n=69（参加企業以外も含まれている）※複数回答あり	11/6 第２回説明会 n=124（参加企業以外も含まれている）※複数回答あり	11 月中間アンケート	１月最終アンケート n=105（参加企業）※複数回答あり
アンチウイルスソフト	67（97%）	101（81%）	―	91（87%）
ファイアウオール	37（53%）	65（52%）	―	40（38%）
UTM	7（10%）	34（27%）	―	実証 UTM 除く８（8%）
その他 IT ベンダー提供のセキュリティサービス	6（9%）	19（15%）	―	3（3%）
データのパスワード設定	22（32%）	32（26%）	―	16（14%）
データの暗号化	9（13%）	28（23%）	―	6（6%）
物理的管理の徹底	9（13%）	16（13%）	―	6（6%）
社員教育・研修	18（26%）	29（23%）	―	14（14%）
専門人材育成	2（3%）	3（2%）	―	1（1%）
ISMS（ISO/IEC27001・27002）・CSMS	1（1%）	6（5%）	―	0
SECURITY　ACTION	4（6%）	10（8%）	―	11（11%）
サイバー攻撃損害保険	1（1%）	2（2%）	―	0
取引先との情報管理契約	7（10%）	11（9%）	―	3（3%）
サプライチェーンでの規定等の制定・参加	0	1（1%）	―	1（1%）
特に実施していない	1（1%）	0	―	3（3%）

表5

Ⅳ. SECURITY ACTION の登録状況	7/5 第1回説明会	11/6 第2回説明会	11月中間アンケート n=64（参加企業）	1月最終アンケート n=91（参加企業）
一つ星登録済	—	—	9(14%)	17(19%)
二つ星登録済	—	—	1(2%)	5(5%)
登録は検討していない	—	—	46(72%)	56(62%)
一つ星登録申請検討中	—	—	6(9%)	8(9%)
二つ星登録申請検討中	—	—	2(3%)	5(5%)

表6

Ⅴ. 取引先からサイバー攻撃対策を求める意思表示の有無	7/5 第1回説明会 n=65（参加企業以外も含まれている）	11/6 第2回説明会 n=107（参加企業以外も含まれている）	11月中間アンケート n=65（参加企業）	1月最終アンケート
取引先の要件化とされつつある	11(17%)	21(20%)	4(6%)	—
指示されつつある	6(9%)	14(13%)	3(5%)	—
依頼されつつある	12(18%)	24(22%)	7(11%)	—
その動向はない	36(55%)	48(45%)	51(78%)	—

表7

Ⅵ. サイバーセキュリティ対策として最も重要視していること	7/5 第1回説明会 n=69（参加企業以外も含まれている） ※複数回答あり	11/6 第2回説明会 n=124（参加企業以外も含まれている） ※複数回答あり	11月中間アンケート n=66（参加企業） ※複数回答あり	1月最終アンケート
価格	45(65%)	71(57%)	54(82%)	—
機能	48(70%)	84(68%)	41(62%)	—
使い勝手	32(46%)	52(42%)	31(47%)	—
相談窓口	19(28%)	25(20%)	24(36%)	—
駆け付け	10(14%)	14(11%)	8(12%)	—
その他	1(1%)	3(2%)	0	—

表8

Ⅶ. サイバーインシデント発生時に必要となること	7/5 第1回説明会	11/6 第2回説明会 n=124（参加企業以外も含まれている） ※複数回答あり	11月中間アンケート n=66（参加企業） ※複数回答あり	1月最終アンケート
電話や遠隔ＰＣ操作による相談・ウイルス除去等の簡易処置対応	—	56(45%)	48(73%)	—
IT事業者等の駆け付けによる相談・ウイルス除去等の簡易処置対応	—	51(41%)	31(47%)	—
感染したPCの初期化・クリーンナップ対応	—	39(31%)	26(39%)	—
感染したPCの買い替え対応	—	7(6%)	2(3%)	—
インシデントの影響範囲や原因などの外部調査依頼	—	40(32%)	27(41%)	—
再発防止のためのセキュリティ強化	—	45(36%)	27(41%)	—
従業員へのサイバーセキュリティ教育	—	38(31%)	10(15%)	—
インシデントによる損害を補償するサイバー保険加入	—	10(8%)	6(9%)	—

表9

Ⅷ. サイバー攻撃・被害の経験有無	7/5 第１回説明会 n=69（参加企業以外も含まれている） ※複数回答あり	11/6 第２回説明会 n=124（参加企業以外も含まれている） ※複数回答あり	11 月中間アンケート	１月最終アンケート n=105（参加企業） ※複数回答あり
ＨＰ接続不能/大量メール受信	4（6%）	13（10%）	―	6（6%）
標的型攻撃メール/ビジネスメール詐欺	19（28%）	27（22%）	―	25（24%）
ランサムウエア（暗号化・身代金）	10（14%）	15（12%）	―	8（8%）
導入したシステムや製品にウイルスが混入	3（4%）	2（2%）	―	6（6%）
その他攻撃	1（1%）	8（6%）	―	8（8%）
情報漏えい被害	0	0	―	2（2%）
システムダウン被害	1（1%）	1（1%）	―	0
データ損壊被害	2（3%）	3（2%）	―	5（5%）
金銭拠出被害	1（1%）	0	―	0
流通途絶被害	1（1%）	0	―	0
わからない	30（43%）	44（35%）	―	58（55%）

②京阪神の中小企業におけるサイバーセキュリティおよびサイバー攻撃の実態に係る考察

（イ）人材についての現状〔Ⅰより〕

○情報システム担当者を配置している割合は、参加企業を対象とした１月の最終アンケートで 41%（専任 9%、兼任 32%）。2017 年 6 月の大阪商工会議所アンケート調査（母集団は異なるが）の 48%と比べても低い。約半数は 1 人もおらず経営層が直轄している。

（ロ）予算についての現状〔Ⅱ、Ⅵより〕

○サイバーセキュリティに係る年間経費は、額が少なくなるほど比率が上がり、本実証事業の参加企業では 3 分の 1 以上が年１万円未満（月ではない）、年 11 万円以上は 20%にすぎず、セキュリティにお金をかけていない実態が改めて明白化した。

（ハ）技術的対応（事前対応）についての現状〔Ⅲより〕

○アンチウイルスソフトの導入率は 87%（2017 年調査 78%）。但し定義ファイル更新等の運用が適切になされているか否かは定かではない。

○UTM の導入率は、参加企業以外もあわせた 11 月の第２回説明会のアンケートで 27%。サイバー攻撃の巧妙化とマルウエアの多種化の動向に鑑みれば、UTM 普及率の低さは課題といえる。なお、本実証事業実施にあたり、約 50 の中小企業を実地訪問したところ、UTM 設置企業でも、実質的にはファイアウオール的な運用しかしていない企業や“入れっぱなし”の企業も散見された。

（ニ）業務フロー面の対策・第三者認証等についての現状〔Ⅲ、Ⅳより〕

○ISMS は 10%に満たない。SECURITY ACTION は本実証事業の参加企業を対象

とした１月の最終アンケートで一つ星 19%、二つ星 5%と、ISMS に比べると多いながらも低調。

○両者の中間的な対外的信用担保要素として「サイバーセキュリティお助け隊」（の利用）が位置付けられ、認知されるとすれば有意義であろう。

（ホ）リスク転嫁（事後対応）についての現状〔Ⅲより〕

○サイバーリスクに関する保険の加入率は、どのアンケートを見ても 1～2%と非常に低い。事後対応への優先順位が低いことの表れであり、攻撃を受けることを前提としていないこと、受けていてもその事実に気付いておらず当事者意識を抱きにくいこと、などが要因として考えられる。

○保険料の高さも要因の一つ。既存の本格的サイバーリスクに関する保険（主に高額な費用や賠償対策）とは異なる簡易的な保険（主に費用損害対策、初動対処対策）の新設が望まれる。

（ヘ）サプライチェーンでの対策についての現状〔Ⅲ、Ⅴより〕

○「取引先との情報管理契約」や「サプライチェーンでの規定等の制定・参加」は約１割に満たない。「取引先からサイバー攻撃対策を求める意思表示の有無」は「その動向はない」が概ね過半数で推移している。「サプライチェーンの弱点を悪用した攻撃の高まり」が IPA の「情報セキュリティ 10 大脅威 2020」に４位にランクインした事実に照らせば、心許ない状況といえる。

○一方で「取引先の要件化とされつつある」「指示されつつある」も、最大で 33%あり、サプライチェーンの中での取り組みが一部では行われていることが伺える。

○サプライチェーン上の中小企業が、本件についての改善を提唱・主導したりできる力関係にないことを考慮すれば、サプライチェーンの頂点に位置する大企業もしくは業界団体等が一定のリーダーシップを担い、この改善に努める必要性があろう。

○ここで障壁になるのが独占禁止法及び下請法における優越的地位の濫用の禁止。被害拡大時の全体的、中期的な悪影響の総和に鑑み、サプライチェーンが一体的にサイバーセキュリティを進める手法を官民挙げて検討するべき時期であろう。

（ト）事後対応についてのニーズ〔Ⅶより〕

○本設問は現状ではなくニーズを聞いている。「電話や遠隔ＰＣ操作による相談・ウイルス除去等の簡易処置対応」「IT 事業者等の駆け付けによる相談・ウイルス除去等の簡易処置対応」など、速やかかつ実効性ある初動対処へのニーズが高い。

○「インシデントの影響範囲や原因などの外部調査依頼」などフォレンジック調査の範疇に入る対応へのニーズも一定程度ある。この種の調査は中小企業では手が出ない程に高額であるため本格的なサイバーリスクに関する保険で対応せざるを得ないであろう。

○事前および事後の教育も重視されており、セミナー等の定期的開催等によるフォローアップが望まれている。サイバーリスクに関する保険は、ここでも低調であり、１割に満たない。

（チ）サイバー攻撃・被害の経験有無〔Ⅷより〕

○上記のような対策とニーズを有している京阪神の中小企業が、結果として現時点でどのような攻撃もしくは被害を受けているか、の調査である。注目すべきは「わからない」が多いこと。少ない場合でも 35%、多い場合では 55%が占めている。2017 年調査の 72%と比して少ないとはいえ依然多い。また、上記（ハ）にてアンチウイルスソフトの導入率が 87%であることと整合しない。

○攻撃については、「ＨＰ接続不能／大量メール受信（D-DoS 攻撃等）」6～10%は、2017 年調査の 2%から悪化。「標的型攻撃メール/ビジネスメール詐欺」22～28%は 2017 年調査の 18%から悪化。「ランサムウエア」8～14%は 2017 年調査の 7%から悪化。

○被害については、「システムダウン被害」「データ損壊被害」など顕在化する被害が少々ある程度であり、「情報漏えい被害」など顕在化しないものも僅少となっている。

（２）簡易 UTM による防御と観測（把握）

①把握および分析に係る方法論と簡易 UTM の機能（お守り）

（イ）実態把握のため使用した UTM について

○本実証事業では、NEC の既存 UTM をベースに、中小企業が容易に設置、運用できるよう設計・製造した UTM を使用した。

○本実証では､UTM をインターネット接続機器(ONU やブロードバンドルーターなど、PPPoE を終端している機器。以下、ブロードバンドルーターと記載）と監視対象端末（パソコンやモバイル機器など）の間に設置する想定とした。

○ブロードバンドルーターの無線機能を使用している場合､端末からの通信はブロードバンドルーター配下に設置した UTM は経由しないため､UTM による監視はできない。そのため、ブロードバンドルーターの無線機能は無効にし、UTM の無線機能を使用する必要がある。ブロードバンドルーターの無線機能ではなく、別の無線 LAN アクセスポイントを用意している場合は､無線 LAN アクセスポイントとブロードバンドルーターの間に UTM を設置することで､無線 LAN アクセスポイントの設定や配下につながっている端末の設定変更なしで監視できる。

（ロ）UTM の設置について

○中小企業の実態を把握するため、ブロードバンドルーターと監視対象端末の間に UTM を設置し、企業 LAN とインターネットの通信を監視した。

設置例１：ブロードバンドルーターなどの配下に HUB を使用している場合

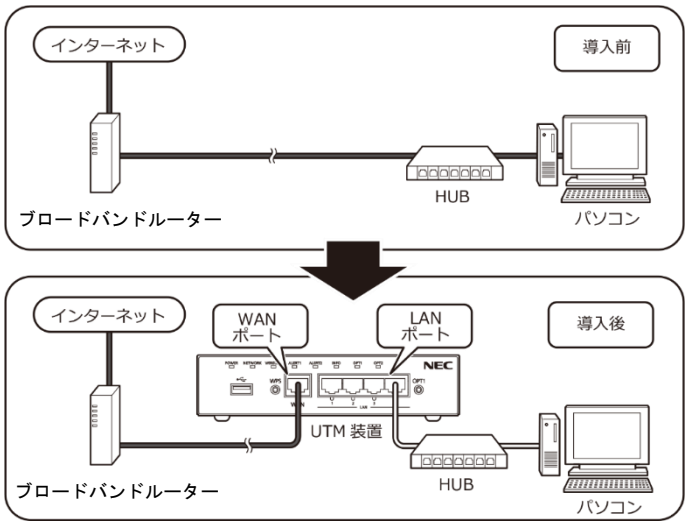


図 3　ブロードバンドルーターなどの配下に HUB 等を設置している場合の UTM 接続位置

設置例 2：ブロードバンドルーター等の配下に無線 LAN(親機)を使用している場合

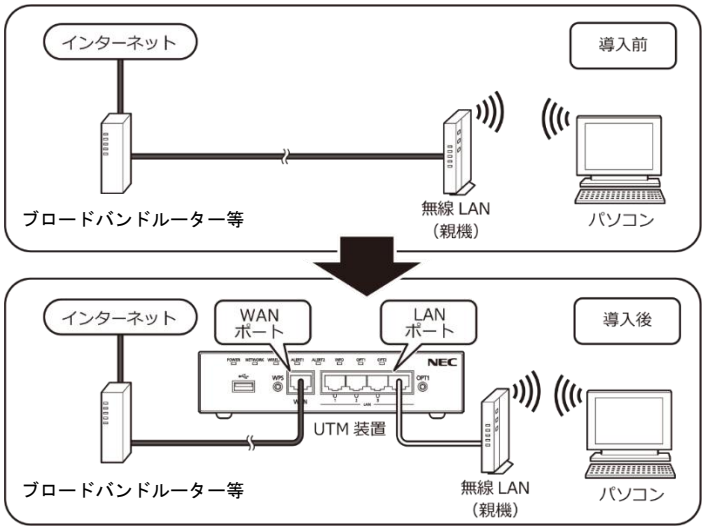


図 4 ブロードバンドルーター等の配下に無線 LAN(親機)を使用している場合の UTM 接続位置

(ハ) 使用した UTM のセキュリティ機能、運用手法

○UTM では、下記の 5 種類のセキュリティ機能を使用した。以降、各セキュリティ機能は表の略称にて記載する。

表 10　使用した UTM のセキュリティ機能一覧

セキュリティ機能	略称	説明
不正侵入防止	IPS	ネットワーク通信で攻撃と判断されたコードなどの異常なデータが含まれていることを検知し防御する機能。
アンチウイルス	AV	マルウエアや危険なコードが含まれるファイルを検知した場合に内容を書き換え無害化する機能。
Webガード	WG	フィッシングサイトや閲覧によってマルウエア感染を起すなどの有害なWebサイトへのアクセスを遮断する機能。
URLフィルタリング	UF	あらかじめ用意されているWebサイトのカテゴリに該当するWebサイトへのアクセスを検知する。

セキュリティ機能	略称	説明
アプリケーション ガード	APG	ファイル交換ソフトやメッセンジャーアプリなど、不特定多数の個人が情報交換可能なアプリケーションを利用した際の通信を検知する。

〇UTM のセキュリティ機能のうち、IPS、AV、WG で検知した通信を遮断することにより、外部からの攻撃（不正アクセスやマルウエアの侵入）や、外部への不正通信（マルウエア感染等による企業内部から外部への被害拡大）を防ぐ。

〇UTM が攻撃通信を防御、検知したアラート情報をクラウドで収集した。

〇IPS、AV、WG で検知、遮断した際、参加企業の管理者に通知を行い、注意を促す。

〇マルウエアへの感染が疑われるアラートをクラウドで自動判定し、検知したアラートの内容および参加企業が実施する必要がある対処内容を記載し、「重要アラート」として、参加企業あてにメール通知した。

〇UTM のセキュリティ機能のうち、UF、APG を使用し、Web アクセスやアプリケーションの使用状況を確認した。なお、どのサイト／アプリケーションを許可するべきか、企業により異なるため、全企業一律のポリシーで防御した場合、業務影響がでることが考えられる。そのため、本実証では、ログのみ取得し、防御はしない。

〇各セキュリティ機能と検知内容と説明、通知方法の関係は以下の通り。

表 11　セキュリティ機能

略称	検知した通信	説明
IPS	外部からの攻撃	インターネットからイントラネットへの通信データ内に攻撃コードなどの異常なデータが含まれていることを検知し、通信を遮断
	外部への不正通信	社内の端末がマルウエアに感染したことによるインターネットへの不正通信を遮断

略称	検知した通信	説明
	内部の脆弱性	ルーター宛など内部の通信で、脆弱なパスワード（デフォルトのパスワードを使用など）を使用した HTTP Basic 認証の通信を検知・遮断
AV	外部からの攻撃	エンドユーザーによるメール受信、その他のアプリケーションの通信を監視し、ダウンロードするファイルにウイルスが含まれていることを検知し、ファイルの内容を書き換え無害化
	外部への不正通信	エンドユーザーによるメール送信、その他のアプリケーションの通信を監視し、アップロードするファイルにウイルスが含まれていることを検知し、ファイルの内容を書き換え無害化
WG	外部への不正通信	マルウエアによる攻撃者が用意した外部サーバーへの通信や、エンドユーザーによるウェブ閲覧によってマルウエア感染を起こすなどの有害な Web サイトに対するアクセスを検知し通信を遮断
UF	外部の Web サイトへのアクセス	あらかじめ用意されている Web サイトのカテゴリに該当する Web サイトへのアクセスを検知
APG	外部へのアプリケーションを使用した通信	ファイル交換ソフトや動画共有アプリ、メッセンジャーアプリなど、不特定多数の個人が情報交換可能なアプリケーションを利用した際の通信を検知

②監視企業数、監視期間

○UTM による監視は、7 月 8 日から順次開始。監視社数の遷移は以下の通り。

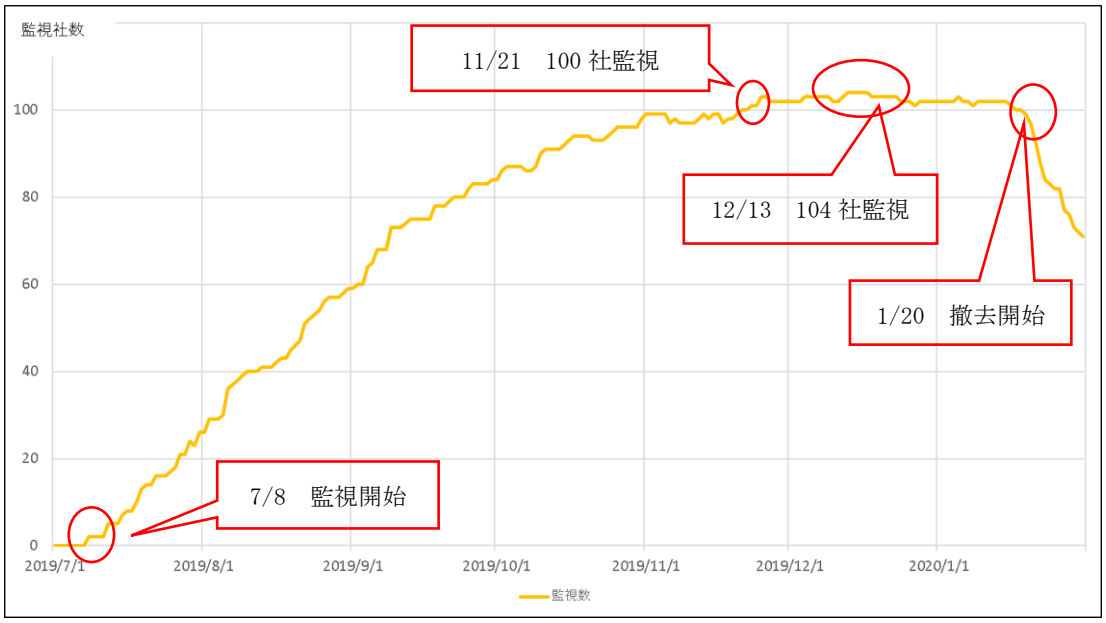


図 5　UTM 監視社数の遷移

- 11 月 21 日に監視対象が 100 社に達した。
  10 月 31 日に 100 社で設置完了したが、UTM を取り外された企業や、UTM からログが送信されていない企業があった。
  それら企業は、UTM が取り外している、あるいは、ログが送信されていない期間は監視社数から除外している。100 社監視中になったのは 11 月 21 日。
- ピークは、12 月 13 日で 104 社監視実施。
- 実証期間中のべ 110 社で監視実施。（112 社中の 2 社は簡易 UTM を設置しオンラインにはなったものの、ログが上がってこなかった）
- 1 月 20 日以降、商用サービスへ移行しない企業は取り外しを開始。

○平均監視期間は 145 日であった。

表 12　UTM 監視期間

監視期間	社数
30 日未満	4（4%）
30 日以上 60 日未満	3（3%）
60 日以上 90 日未満	10（9%）
90 日以上 120 日未満	13（12%）
120 日以上 150 日未満	23（21%）
150 日以上 180 日未満	33（29%）
180 日以上	26（23%）
計	112

・105 社で 60 日以上監視実施（最大 208 日監視実施）

③参加企業におけるサイバー攻撃の検知状況

（イ）簡易 UTM での検知状況（参加企業全体）

参加企業に設置した UTM のうち IPS、AV、WG で外部からの攻撃や外部への不正通信を検知・遮断した社数は以下の通り。

表 13　簡易 UTM での検知社数

検知状況	検知した通信	社数
あり	外部からの攻撃	64
	外部への不正通信	31
	（内、外部からの攻撃と外部への不正通信の両方を検知した社数）	（21）
	合計	95
	合計（重複を除く）	**74（66%）**
	内部の脆弱性	47
	検知あり合計（重複を除く）	**88（79%）**
なし		24（21%）
	合計（重複を除く）	**112**

○上記には、攻撃の探索活動であるポートスキャンは除いている。
中小企業では、ブロードバンドルーター配下にプライベート IP アドレスを設定した端末を接続する構成が一般的である。この場合、ブロードバンドルーターに特殊な設定がされている場合以外はブロードバンドルーターの外部からプライベート IP アドレスにアクセスできない。このため、外部からのポートスキャン攻撃はブロードバンドルーターで止まり、ブロードバンドルーターは以下の UTM には到達せず、検知されない。なお、UTM でポートスキャンを検知できる構成としては、UTM 配下に公開サーバーなど、外部から企業内部へアクセス可能な端末がある場合となる。

○上記想定通り UTM に到達するポートスキャンがないか確認するため、12 月 23 日から UTM のポートスキャン検知機能を有効として調査を実施した。その結果、外部からのポートスキャンと検知したのは、2 社（31 件）であった（2 社とも<u>グローバル IP アドレスが付与され、外部からアクセス可能な機器</u>があった企業）。

○外部からの攻撃を検知している参加企業のうち、1 日あたりの検知・遮断件数トップ 10 は以下のようになっている。なお、1 日あたりの平均検知・遮断件数は、0.99 件であった。特に検知の多い 2 社を除いた 1 日あたりの平均検知・遮断件数は 0.37 件であった。

表 14　外部から攻撃が多い企業トップ 10

企業	1 日あたりの件数	UTM 設置日数	業種	従業員数	端末数
企業 1	40.82	187	製造業	30	13
企業 2	30.11	194	建設業	46	32
企業 3	7.04	163	サービス業	1	2
企業 4	6.83	18	サービス業	7	12
企業 5	5.90	183	製造業	197	250
企業 6	4.07	145	小売飲食	70	10
企業 7	3.44	165	製造業	230	40
企業 8	2.93	191	サービス業	8	8
企業 9	2.12	153	卸売業	3	2
企業 10	1.42	67	製造業	95	100

・1 日あたり 30 件以上ある 2 社（企業 1、企業 2）に関しては、現地調査を実施した結果、グローバル IP アドレスを付与され、外部からアクセス可能な機器が設置されていた。また、企業 3 に関しても UTM のログからグローバル IP を使用し、外部から直接アクセス可能な機器があると判断。グローバル IP を付与して、外部からアクセス可能な機器があると攻撃は多くなる傾向がある。
・2 社に対しては、外部からアクセス可能な機器がある場合、多種多様な攻撃を受けリスクがある旨説明し、外部からアクセスする必要な場合は、必要な通信のみ許可すること、バージョンアップ等を行うこと、などの注意喚起を実施した。
・企業 4 以下に関しては、特に傾向はなく、攻撃が多い原因は不明である。

○外部への不正通信を検知した 31 社のうち、企業内の端末がマルウエアに感染し被害が発生していると考えられるアラート（重要度★★★）は、7 社（7 件）で検知した（重要度の詳細は、3.(2)⑥参加企業に対するアラート通知とその基準を参照）。

○重要度★★★アラートの対処結果、3 社にてマルウエアを検出・駆除した。ウイルス対策ソフトが入っているにもかかわらず、数百件のマルウエアが見つかったケースや、パターンファイルが更新されていないケースもあり、適切にウイルス対策ソフトが運用されていないことが判明した。

○外部からの攻撃と外部への不正通信の両方とも検知していない企業は24社あった。

- 1社は1日しか設置ができていない。
- 2社で通信ログが出力されていなかった。設置位置が不適切であったことが推測される。
- 残り21社は、通信ログは出力されていたため、端末の監視はできているが、端末台数が少なく使用頻度が少なく、攻撃となる通信が発生していなかったと推測される。

（ロ）簡易UTMでのサイバー攻撃の検知・遮断件数（参加企業全体）

○UTMのIPS、AV、WGでの検知・遮断件数、ならびに社数は以下の通り。なお、1回のインシデントで複数件、検知・遮断することもある。その場合でも、検知・遮断した件数分カウントしている。

表15　UTMでの検知・遮断件数と社数

検知した通信	機能	件数	社数	外部からの攻撃が多い2社除く件数(※2)
外部からの攻撃	IPS	18,325	48	4,894
	AV(※1)	775	34	732
外部への不正通信	IPS	683	31	683
	AV(※1)	1	1	0
	WG	8	5	2
内部の脆弱性	IPS	1,254	47	1,254
合計		**21,046**	**—**	**7,565**

(※1)2019年11月4日（月）から電子メール添付ファイルのアンチウイルススキャン機能を追加した。UTMでは、パスワード付きファイルや暗号化されたファイルからマルウエアを検出できないため、実証開始時は、HTTPとFTP通信のファイルを対象とし、メールの添付ファイルは対象外としていた。しかし、一部ファイル（パスワードで保護されていない、暗号化されていないなど）に対するマルウエアは検出できるため、電子メールの添付ファイルに対するアンチウイルススキャン機能を有効化した。

(※2)外部からの攻撃が極端に多い企業が2社あり。2社のみで全企業の攻撃総数の約7割を占めていた。調査した結果、グローバルIPアドレスが付与され、外部からアクセス可能な機器が設置されていた。

（ハ）簡易 UTM でのサイバー攻撃の検知状況（業種別）

○参加企業の業種により、外部からの攻撃や外部への不正通信の検知状況に傾向があるか確認した。業種別の検知状況は以下の通り。

表 16　業種別 UTM での検知社数

検知状況	検知した通信	社数					
		製造業 参加構成比 39%	サービス業 参加構成比 32%	卸売業 参加構成比 16%	建設業 参加構成比 7%	小売飲食 参加構成比 5%	運輸業 参加構成比 1%
あり	外部からの攻撃	26	22	8	5	2	1
	外部への不正通信	15	9	2	4	1	0
	（内、外部からの攻撃と外部への不正通信の両方を検知した社数）	(11)	(7)	(1)	(2)	(0)	(0)
	合計	41	31	10	9	3	1
	合計（重複を除く）	30 **検知率 42%**	24 **検知率 32%**	9 **検知率 12%**	7 **検知率 9%**	3 **検知率 4%**	1 **検知率 1%**
	内部の脆弱性	16	16	6	5	4	0
	検知あり合計（重複を除く）	**35 検知率 40%**	**27 検知率 31%**	**13 検知率 15%**	**7 検知率 8%**	**5 検知率 6%**	**1 検知率 1%**
なし		9	8	5	1	1	0
合計（重複を除く）		44	35	18	8	6	1

○今回の実証では製造業やサービス業は対象社数（絶対数）が多いため、それに応じて検知社数（絶対数）が多くなっている。

○どの業種でも一定の割合で外部からの攻撃や外部への不正通信を検知しており、業種による偏りは見受けられなかった（業種ごとの参加構成比率と検知率がほぼ同じ）。

（ニ）簡易 UTM でのサイバー攻撃の検知・遮断件数（業種別）

○UTM の IPS、AV、WG での業種毎の検知・遮断件数、ならびに、1 社 1 日あたりの検知・遮断件数は次の通り（外部から攻撃が多い 2 社を除く）。

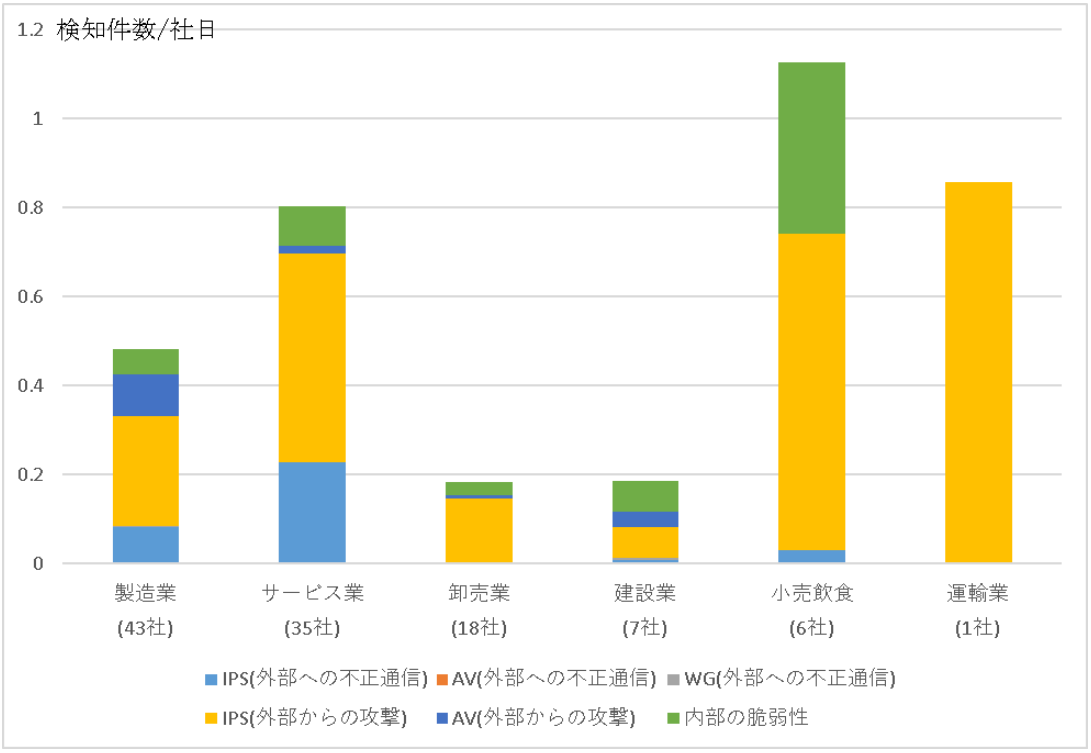


図 6　1 社 1 日あたりの検知・遮断件数（業種別）

○小売飲食業は 1 社 1 日あたりの検知・遮断件数が多く、卸売業、建設業は他の業種に比べ少ない傾向があった。

○運輸業は 1 社のみのため、業種の傾向としては、判断できない。

○小売飲食業が多いのは、外部から攻撃が多い企業トップ 10 の企業 6 が 1 日あたり 4 件検知しており、本業種の値を上げている。
同企業を　除くと、0.001 件となり、ほぼ攻撃を受けていないこととなる。

○サービス業の端末数平均は 11 台と他業種と比べ多くはない。
（製造業 28 台、卸売業 14 台、建設業 22 台、小売飲料 6 台、運輸業 17 台）
Web アクセスが多く、攻撃を検知する機会も多くなると推測する。

（ホ）簡易 UTM でのサイバー攻撃の検知・遮断件数（端末数別）

○UTM の IPS、AV、WG での端末数毎の検知・遮断件数、ならびに、1 社 1 日あたりの検知・遮断件数は次の通り（外部から攻撃が多い 2 社を除く）。

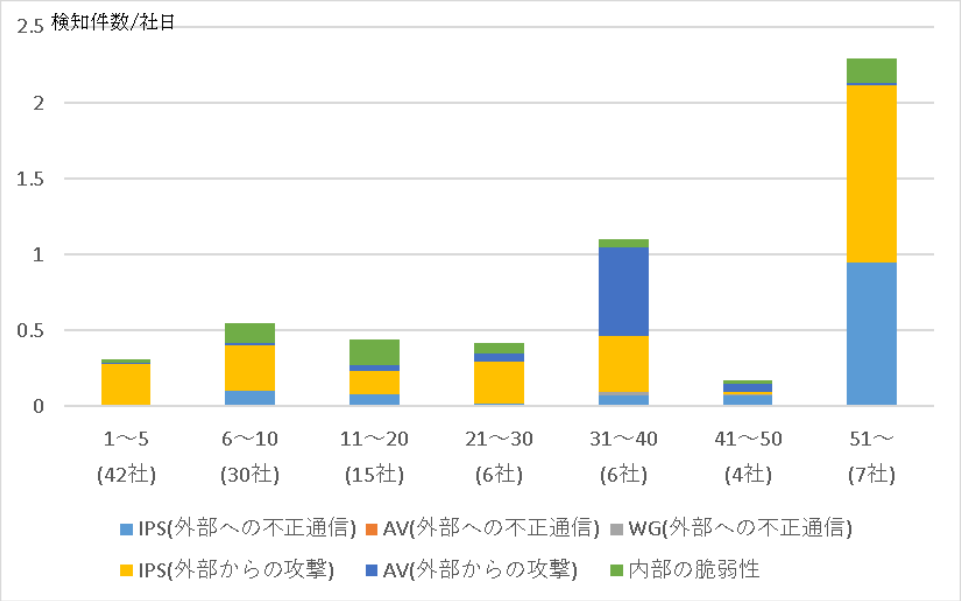


図 7　1 社 1 日あたりの検知・遮断件数（端末数別）

○端末台数が増えるほど、検知・遮断件数が多くなる傾向がある。

○端末台数 50 台以上の企業における検知・遮断件数は、端末台数 31～40 台の企業の倍になっている。これは、1 社で 1 日あたり約 6 件検知している企業があり、端末台数 50 台以上の企業数が少ないことから 1 社あたりの平均に影響を与えている（外部から攻撃が多い企業トップ 10 の企業 5 の企業）。
同企業を除けば、1 社 1 日あたり 1.2 件となり、端末台数 31～40 台と近しい状況となる。

○端末数 41～50 台の企業の攻撃検知・遮断件数は少ない原因は不明である。

○端末台数が増加すると、Web アクセスも増加するため、攻撃の検知が多くなる傾向があると推測される。ただし、端末数が少ないと言ってもなくなるわけではない。

④参加企業におけるサイバー攻撃の観測実態（ＡＶ、ＩＰＳ、ＷＧ）

（イ）簡易 UTM でのサイバー攻撃の検知・遮断と考察（月別）

○UTM の IPS、AV、WG での月毎の検知・遮断件数、ならびに、月毎の遮断件数を監視社数で割った値（1 社 1 日あたりの遮断件数）は次の通り。

○全企業の検知・遮断件数、1 社 1 日あたりの検知・遮断件数は以下の通り。

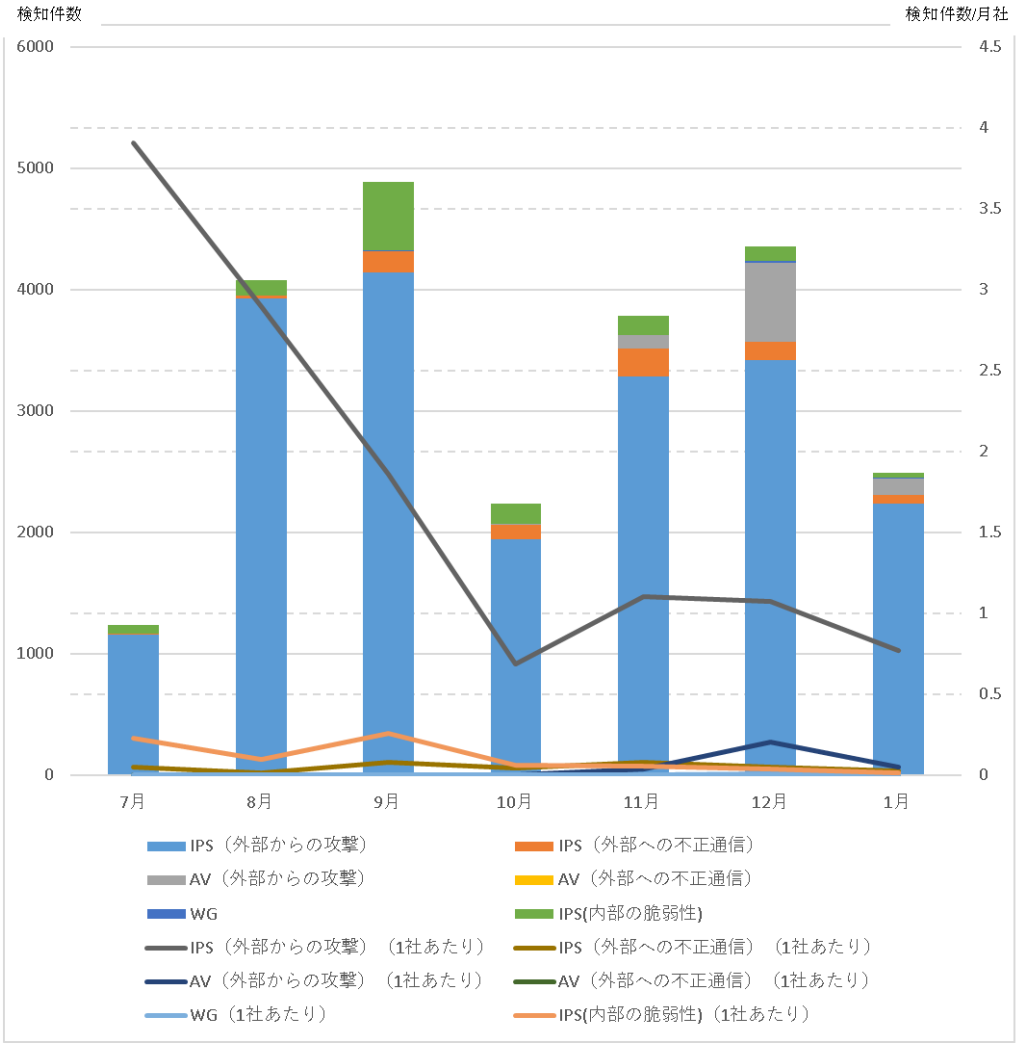


図 8　月毎の検知・遮断件数と、1 社 1 日あたりの検知・遮断件数

○外部から攻撃が多い 2 社を除いた検知・遮断件数、1 社 1 日あたりの検知・遮断件数は以下の通り。

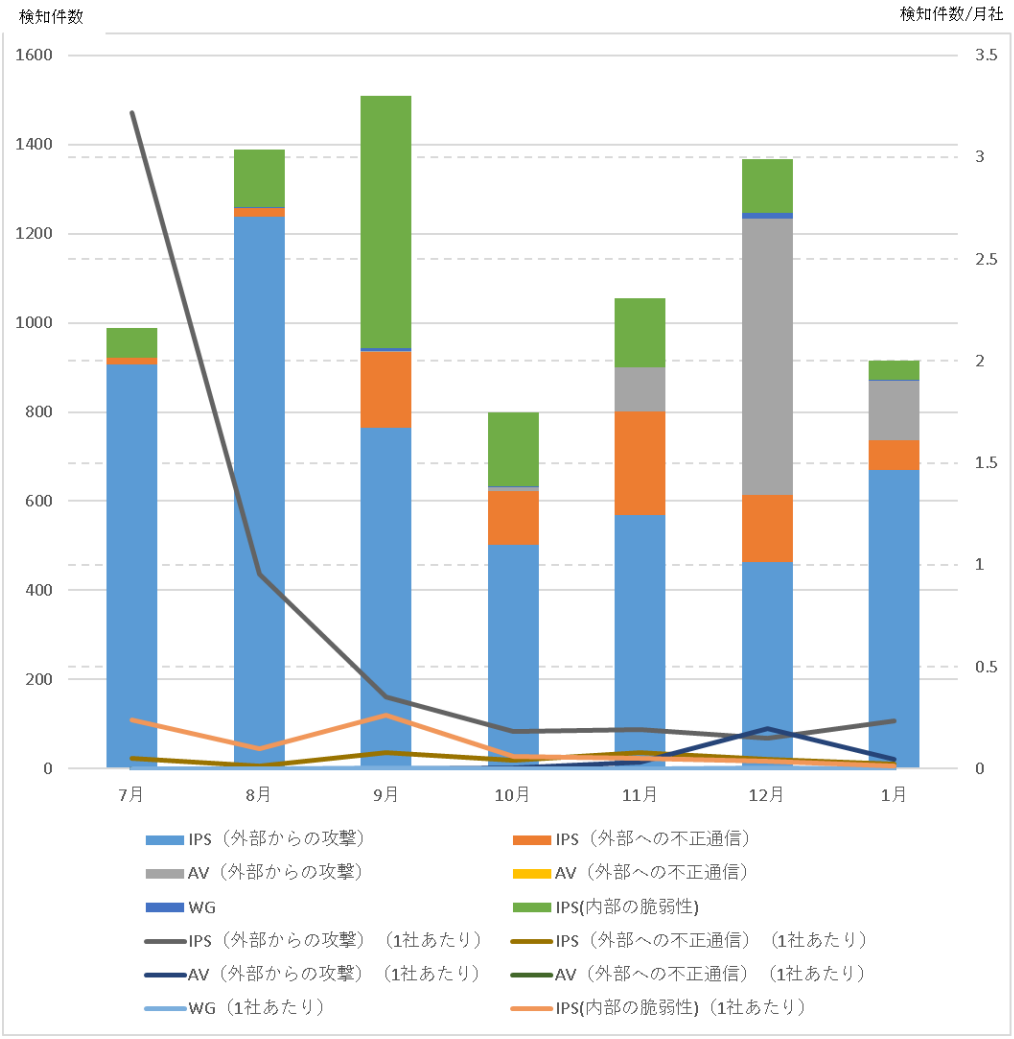


図 9　月毎の検知・遮断件数と、1 社 1 日あたりの検知・遮断件数（外部からの攻撃が多い 2 社除く）

○9 月に IPS（内部の脆弱性）が他の月と比べ多数検知した。これは、脆弱なパスワードを使用した Basic 認証の通信を 1 社で設置当日に 303 件検知したことが影響している。同アラートは設置当日以外検出していないため、対処されたと推測する。

○10 月に IPS（外部からの攻撃）が他の月と比べ、減少している。これは、グローバル IP を付与し、外から直接アクセス可能となっている機器を保有していた 2 社に対しての攻撃が減少していたことが影響している。減少した理由は不明である。

○11 月以降 AV（外部への不正通信）の検知・遮断件数が増えているのは、電子メールの添付ファイルをアンチウイルスのスキャン機能を追加したため。これにより 10 月から感染が拡大した Emotet 感染が疑われるファイルも検出し効果があった。

○1 社 1 日あたりの外部からの攻撃件数が 7 月以降減少傾向にある。監視期間中に外部からの攻撃の TOP10 の月ごとの検知件数を確認し、傾向があるか確認した。

表 17　UTM の検知内容と遮断件数

No	検知内容	7 月	8 月	9 月	10 月	11 月	12 月	1 月	合計
1	SIP 攻撃に用いられる検証ツールのスキャンを検知	245	1,075	1,407	979	1,348	1,291	756	7,101
2	特定ルーターの UDP ポートに接続できる不具合を狙った疑いのある通信を検知	262	825	719	79	584	502	300	3,271
3	利用者が入力時に不正なスクリプトを挿入できる脆弱性をついて行われる攻撃を検知	0	3	59	397	543	519	719	2,240
4	特定ルーターに存在するコマンド実行の脆弱性を悪用した疑いのある通信を検知	64	248	530	74	245	280	194	1,635
5	Web アプリケーションの脆弱性を悪用した SQL インジェクション攻撃を検知	2	273	289	99	165	94	161	1,083
6	Microsoft Media Player に対する脆弱性を悪用した疑いのある通信を検知	0	911	0	0	0	0	0	911
7	Internet Explorer 9 の脆弱性を悪用したとみられる通信を検知	560	0	2	0	11	0	1	574
8	Web アプリケーションに存在する脆弱性をつき、リモートから任意の PHP コードを注入したとみられる試みを検知	9	48	82	86	80	65	64	434
9	プログラミング言語 PHP を使用したプログラムに対する攻撃の疑いがある通信を検知	0	0	0	0	0	241	2	243
10	特定 Web サイトからネットワークトラフィックを悪質なプロキシにリダイレクトし、侵入先のコンピュータから機密情報を盗み取るトロイの木馬による通信を検知	0	0	123	0	0	0	0	123

各アラートの概要については、⑤参加企業におけるサイバー攻撃の実例・考察に示すが、詳細については割愛する。

○No1, 2, 4, 8 は、グローバル IP アドレスを付与し外部からアクセス可能な機器が設置されていた企業で検知していた。10 月に一旦減少している原因は不明。

○No3, 5 は、月毎検知・遮断件数に差はあるものの毎月検知しており、特に傾向はないと推測する。

○No6 は、9 月のみ 1 社で 911 件検知していた。同一サイトに同一クライアントからアクセスされていた。アクセスしたサイトが表示されないため、繰り返しアクセスを行っていたのではないかと推測する。

○No7 は、7 月に 2 社で計 560 件検知していた。アクセス先サイトは 2 社で異なるが、企業内では同一サイトであった。サイトが正しく表示されないため、繰り返しアクセスを行っていたのではないかと推測する。また、9 月、11 月、1 月に攻撃を検知していたが、検知した企業は異なる。

○No9 は、12 月に 1 社で検知していた。この企業は 9 月に UTM を設置しており、設置後から月 100 件前後、外部からの攻撃を検知していた。UTM で検知した通信の宛先は、ローカル IP アドレスの 80 番ポートであった。そのため、外部に向け公開している機器があり、ブロードバンドルーターで NAT 変換されていると考える。機器の MAC アドレスからベンダーを確認したところ、海外のメーカーであり、通信キャリアから割り当てられる IP アドレスが変わっても外部から使用できる機器・サービスを提供していた。この機器・サービスを企業外部から使用していたが、同時に攻撃の対象としてねらわれていたと推測する。

○No10 の攻撃は、9 月に 1 社で検知していた。アクセス先は同一サイトであったが複数の端末からアクセスされていた。サイトが正しく表示されないため、繰り返しアクセスを行っていたのではないかと推測する。

○No1,2,4,8,9 は、外部から脆弱性を付く攻撃であり、グローバル IP アドレスを付与し外部からアクセスできる機器が設置された環境であるため、発生している。

○No3,5,6,7,10 は、Web アクセスをトリガーに発生している。不正なスクリプトなどが埋め込まれたサイトにアクセスし、攻撃を受けていると推測する。

○上記より、7 月～9 月で多く検知した No6,7,10 は、サイトが正しく表示されないため、繰り返しアクセスされ、検知件数が増えていると推測する。

外部から攻撃が多い 2 社と単月で検知している No6,7,10 を除くと、以下のように 1 社 1 日あたり 0.1～0.3 件となり、7 月～9 月で減少している傾向はみられなくなる。そのため、7 月～9 月で外部からの攻撃が減少しているように見えたのは、単月で発生している検知が影響していたと推測する。

表 18　UTM での検知・遮断件数と 1 社あたりの検知・遮断件数

	7 月	8 月	9 月	10 月	11 月	12 月	1 月
攻撃を検知した件数（特定の企業、攻撃を除く）	21	326	642	503	569	464	669
1 か月間の UTM 監視社・日	282	1,294	2,171	2,776	2,919	3,122	2,846
1 社 1 日あたりの検知数	0.07	0.25	0.30	0.18	0.19	0.15	0.07

⑤参加企業におけるサイバー攻撃の実例・考察【事例紹介含む】

（イ）外部からの攻撃で検知遮断した内容

(a) 外部からの攻撃のうち IPS で検知した内容と件数は以下の通り。

表 19　IPS で検知遮断した検知内容と件数

No	検知内容	件数
1	SIP 攻撃に用いられる検証ツールのスキャンを検知	7,101
2	特定ルーターの UDP ポートに接続できる不具合を狙った疑いのある通信を検知	3,271
3	利用者が入力時に不正なスクリプトを挿入できる脆弱性をついて行われる攻撃を検知	2,240
4	特定ルーターに存在するコマンド実行の脆弱性を悪用した疑いのある通信を検知	1,635
5	Web アプリケーションの脆弱性を悪用した SQL インジェクション攻撃を検知	1,083
6	Microsoft Media Player に対する脆弱性を悪用した疑いのある通信を検知	911
7	Internet Explorer 9 の脆弱性を悪用したとみられる通信を検知	574
8	SNMP コマンドのネットワーク・リソースからテーブルのすべての行を取得するためのコマンドを検知	434
9	プログラミング言語 PHP を使用したプログラムに対する攻撃の疑いがある通信を検知	243
10	特定 Web サイトからネットワークトラフィックを悪質なプロキシにリダイレクトし、侵入先のコンピュータから機密情報を盗み取るトロイの木馬による通信を検知	123
11	Web アプリケーションに存在する脆弱性をつき、リモートから任意の PHP コードを注入したとみられる試みを検知	122
12	対象のコンピュータにインストールされている特定アンチウイルスの脆弱性を悪用した通信を検知	86
13	特定ルーターに存在するコマンド実行の脆弱性を狙った疑いのある通信を検知	75
14	Apache Struts 2 のリモートで任意のコード実行可能な脆弱性を狙った攻撃の疑いのある通信を検知	61

No	検知内容	件数
15	特定デバイスに存在するコマンド実行の脆弱性を狙った疑いのある通信を検知	44
16	特定マルウエアに感染した疑いのある通信を検知	36
17	トロイの木馬による通信を検知。	33
18	Apache Struts2 の任意のコードを実行される脆弱性を狙った攻撃の疑いのある通信を検知	31
19	Apache Struts 2 のリモートで任意のコードが実行される脆弱性を悪用した通信を検出	28
20	Null パスワードによるログインができる脆弱性をついた攻撃を検知（バッファオーバーフロー/無認証ログイン）	25
21	特定マルウエア活動（Activity-1）と疑わしい通信を検知	23
22	特定マルウエア活動（Activity-10）と疑わしい通信を検知	22
23	Web トラフィックの中に、Basic 認証(基本認証)を使い、不正アクセスを試みようとする疑いのあるコードを検知	18
24	特定製品の脆弱性に対する攻撃の疑いがある通信を検出	15
25	Internet Information Services（IIS）において存在する脆弱性をついたリモートからの不正操作を検知	14
26	特定マルウエア活動（Activity-6）と疑わしい通信を検知	9
27	Apache Struts 2 のリモートで任意のコードが実行される脆弱性を悪用した疑いのある通信を検知	8
28	特定コンテンツマネジメントシステムの任意のコードを実行される脆弱性を狙った疑いのある通信を検知	8
29	マルウエアと疑わしい通信を検知	8
30	Android 上で動作する FTP Server の脆弱性を狙った攻撃の疑いのある通信を検知	5
31	Adobe Acrobat Reader 9.0 のバッファオーバフローの脆弱性を狙った攻撃の疑いのある通信を検知	4
32	Apache Struts のリモートで任意のコードが実行される脆弱性を狙った攻撃の疑いのある通信を検知	4
33	OpenSSL の SSL の死活を監視する機能の脆弱性を狙った攻撃の疑いのある通信を検知	4
34	光通信規格のルーターの脆弱性を狙った攻撃の疑いのある通信を検知	4
35	Apache Struts2 の任意のコードを実行される脆弱性を狙った攻撃の疑いのある通信を検知	4
36	シェルプログラム Bash の脆弱性を狙った攻撃の疑いのある通信を検知	4
37	仮想通貨マイニングスクリプトをダウンロードさせる攻撃の疑いのある通信を検知	3
38	特定コンテンツマネジメントシステムにおいて PHP の任意のコードを実行される脆弱性を狙った疑いのある通信を検知	3
39	Solaris 8 に搭載された FTP Sserver の脆弱性を狙った攻撃の疑いのある通信を検知	2
40	特定製品に存在する認証回避の脆弱性を狙った疑いのある通信を検知	2

No	検知内容	件数
41	ボットによる指令サーバー(C&C サーバー)からの疑いのある通信を検知	2
42	Web トラフィックの中に、Basic 認証(基本認証)を使い、不正アクセスを試みようとする疑いのあるコードを検知	1
43	Windows サーバーにおいて古いバージョンの NTP を使用している場合に、サービス停止を狙った攻撃の疑いのある通信を検知	1
44	特定コンテンツマネジメントシステムの任意のコードを実行される脆弱性を狙った疑いのある通信を検知	1

○外部からの攻撃に関しては、以下の 2 パターンとなる。

①ほとんどの企業は、不審なサイトへのアクセスに伴った攻撃で、ブラウザの脆弱性（InternetExploer 574 件）を狙った攻撃やブラウザを経由して端末にインストールされたソフトウェアの脆弱性（Media Player 911 件、アンチウイルスソフト 86 件、Adobe Acrobat Reader 4 件など）を狙った攻撃などである（計 3,156 件）

②グローバル IP アドレスを付与した端末が設置されており、外部からアクセス可能な環境では、それら端末を狙った攻撃が非常に多く来ていた。(計 15,169 件)。

－SIP をターゲットとしたスキャン　　7,101 件

－ルーターなどの機器の脆弱性を狙った攻撃　　5,002 件

－Web サービス（Apache Struts など）の脆弱性を狙った攻撃　　952 件

など

また、ポートスキャンについても 31 件検知した。

○不審なサイトへのアクセスに起因し攻撃を受けているため、従業員に教育を行い、セキュリティに対する意識向上が必要であると考える。

○グローバル IP を付与した端末を外部に公開する場合は、最新のパッチを適用する、必要な通信だけを許可するなどの対策が必要であると考える。

(b) 外部からの攻撃のうち AV で検知した内容と件数は以下の通り。

表 20　AV（外部からの攻撃）で検知内容と遮断した件数

No	検知内容	件数
1	MSOffice におけるトロイの木馬の疑いのあるファイルの通信を検知	371
2	MSWord におけるトロイの木馬の疑いのあるファイルの通信を検知	197
3	特定ハッキングツールでウイルス、ワーム、トロイの木馬などを生成し、他の端末をハッキングする疑いのあるファイルの送受信を検知	57
4	銀行口座番号などの個人情報や秘匿情報を窃取するトロイの木馬の疑いのあるファイルの送受信を検知	18

No	検知内容	件数
5	銀行口座番号などの個人情報や秘匿情報を窃取する Windows のトロイの木馬の疑いのあるファイルの送受信を検知	16
6	感染した Windows 端末のファイルを暗号化し、身代金を要求する疑いのあるファイルの送受信を検知	15
7	ウイルス、ワーム、トロイの木馬などを生成し、他の端末をハッキングする疑いのあるファイルの送受信を検知	14
8	銀行口座番号などの個人情報や秘匿情報を窃取するトロイの木馬の疑いのあるファイルの送受信を検知	12
9	トロイの木馬の疑いのあるファイルの通信を検出	10
10	銀行口座番号などの個人情報や秘匿情報を窃取するトロイの木馬の疑いのある MSWord ファイルの送受信を検知	10

○上記一覧は UTM でマルウエアを検知できたものの抜粋である。

○UTM で検知・駆除したマルウエアの大半は、Microsoft 社の Office に仕組まれたマクロウイルスであった。内訳は以下である。

表 21　AV（外部からの攻撃）で検知したマルウエアの割合

マルウエア種類	検出件数	割合
Office ファイルに仕込まれたマクロウイルス	682	88%
マルウエアをダウンロードさせる Web スクリプト	62	8%
Windows 端末内のファイルを暗号化して身代金を要求するマルウエア（ランサムウエア）	16	2%
PDF ファイルに組み込まれたスクリプト	15	2%
合計	**775**	**100%**

○マルウエアに感染しないためにも、不審なサイトへアクセスしない、不審なファイルは開かないなど従業員に教育を行い、セキュリティに対する意識向上が必要であると考える。

（ロ）外部への不正通信で検知遮断した内容

○外部への不正通信では、検知内容に重要度を定義し、参加企業が対処の必要性が一目でわかり、駆け付け発動判断ができるようにした。詳細は、「3.(2) ⑥参加企業に対するアラート通知とその基準（見える化による意識変容）」を参照。

- ★★★：マルウエアの振る舞いを検知したもの。至急対処が必要
- ★★☆：攻撃の振る舞いとして検知したもの。対処を推奨
- ★☆☆：それ以外。至急の対処は不要

（c）外部への不正通信のうち IPS で検知した内容と件数は以下の通り。

表 22　IPS（外部への不正通信）で検知遮断した内容と件数

No	検知内容	重要度	件数
1	特定製品の脆弱性に対する攻撃の疑いがある通信	★★☆	143
2	仮想通貨採掘マルウエア への感染の疑いのある通信	★★★	116
3	インスタントメッセンジャーなどを介して個人情報などを搾取する特定ウイルスに感染の疑いのある通信	★★☆	113
4	マルウエアへの感染の疑いのある通信	★★☆	97
5	攻撃の対象となりやすいツールで作成された Web サイトから実行ファイルをダウンロードしようとする通信	★☆☆	96
6	特定ルーターに存在するコマンド実行の脆弱性を狙った疑いのある通信	★★☆	94
7	特定 WiFi カメラに存在する認証情報漏えいの脆弱性を狙った攻撃の疑いのある通信	★★☆	40
8	特定ルーターに存在するコマンド実行の脆弱性を狙った疑いのある通信	★★☆	13
9	特定マルウエアに感染した疑いのある通信	★★☆	13
10	Microsoft Office の脆弱性に対する攻撃の疑いがある通信。	★★☆	11
11	Solaris 8 に搭載された FTP Sserver の脆弱性を悪用した疑いのある通信	★★☆	9
12	特定マルウエアへの感染の疑いがある通信	★★★	9
13	コンピュータからの通信で脆弱性を悪用した疑いのある通信を検知	★★☆	6
14	Android 上で動作する FTP Server の脆弱性を悪用した疑いのある通信を検知	★★☆	5
15	Adobe Flash Player の脆弱性を狙った攻撃の疑いのある通信を検知	★★☆	3
16	Web サーバーの機密ファイルの読み取りの試みの疑いのある通信を検知	★★☆	3
17	特定マルウェア 感染時の攻撃を指示･制御するサーバーとの通信	★★☆	2
18	マルウエア感染の疑いのある通信	★★☆	2
19	特定マルウエアへの感染の疑いがある通信	★★☆	1
20	Internet Information Services (IIS) の脆弱性を悪用した疑いのある通信	★★☆	1
21	Web サーバーなどの設定ファイルの不正なアップロードや不正な書き換えを狙った疑いのある通信を検知	★★☆	1
22	Windows サーバーの特定ファイルを取得もしくは改竄しようとする攻撃の疑いのある通信を検知	★★☆	1

○外部への不正通信で検知遮断したもののうち、40 件でエンドポイントにてウイルススキャン実施。6 件でマルウエアを検出。なお、1 回の検知で複数のアラートを検知することもあり、1 回のウイルススキャンで複数のアラートに対応していることもある。引き続きアラート精度向上を行う必要がある。

○ウイルス対策ソフトを導入していても、マルウエア感染が疑われる、マルウエア感染に伴い脆弱性を狙ったと疑われる通信を検知し、実際マルウエアを検出したケースもある。ウイルス対策ソフトを導入していても、パターンファイルを更新していない企業も見受けられた。従業員のセキュリティに対する意識を向上させる必要もあると考える。

(d) 外部への不正通信のうち AV で検知した内容と件数は以下の通り。

表 23　AV（外部への不正通信）で検知遮断した内容と件数

No	検知内容	件数
1	トロイの木馬の疑いのあるファイルの通信を検出	1

○メールに添付されたファイルにて検出。対象端末でウイルススキャンを実施したところ、Emotet が検出され駆除した。ウイルス対策ソフトを導入していても、パターンファイルを更新していないケースもあり、従業員のセキュリティに対する意識を向上させる必要があると考える。

(e) 外部への不正通信のうち WG で検知した内容と件数は以下の通り。

表 24　WG で検知遮断した内容と件数

No	検知内容	件数
1	アンチウイルスソフトの動作テスト用ファイルを作成しているサイトへの通信を検出	1
2	フィッシングの疑いのあるサイトへの通信を検出	5
3	マルウエアを含む疑いのあるサイトへの通信を検出	1
4	フィッシング(ユーザーネーム、パスワード、クレジットカード番号など)の疑いのあるサイトの通信を検出	1

○マルウエアに感染しないためにも、不審なサイト、業務に関係しないサイトにはアクセスしないなど、従業員のセキュリティに対する意識を向上させる必要があると考える。

（ハ）内部の脆弱性で検知遮断した内容

○内部の脆弱性では、脆弱なパスワードを使用した（デフォルトのパスワードを使用、短いパスワードを使用など）HTTP Basic 認証の通信を検知している。これは、ルーターなどのパスワードを変更せずに使用している場合に検知(1,254 件)。

○デフォルトのパスワードのまま使用しない、短い文字数や単純なパスワードは使用しないなど、従業員のセキュリティ意識を向上させる必要があると考える。

⑥参加企業に対するアラート通知とその基準（見える化による意識変容）

（イ）重要度の定義

○本実証事業開始当初は検知内容に重みづけを行わず、参加企業にアラートメールを送信してしたが、「緊急で対処すべきか判断できない」「お助け実働隊による対応の権利があるか分からない」という意見があった。また、開始当初は、アラートメール送信＝駆け付け発動（保険発動）と考えていたが、参加企業で対処できないものも含んでおり、駆け付け発動の定義を見直す必要があった。

○そのため、検知内容に重要度を定義し、参加企業が対処の必要性が一目でわかり、駆け付け発動判断ができるように 11 月 15 日に重要度を定義した。

表 25　重要度の定義

重要度	定義	お客様の対応
★★★	・内部(お客様環境)からの通信で、マルウエアの振る舞いとして検知したもの(特定のマルウエア通信と一致 または 酷似したもの)	ユーザーは至急マルウエアへの対処が必要
★★☆	・内部からの通信で、マルウエアの振る舞いであることの特定にまで至らないが攻撃の振る舞いとして検知したもの ・特定のソフトウェアや機器の脆弱性に対しての振る舞いとして検知したもの	マルウエアによる攻撃の可能性があるため、通信元や通信先に対しのマルウエア感染の確認や使用ソフトウェアや機器の利用状況確認などが必要
★☆☆	・通常の通信かマルウエア感染による通信かの判断が初見では難しいが、セキュリティ上リスクがある通信であるため UTM で遮断するもの	UTM が遮断していることもあり、ユーザーはセキュリティ的には至急の対処は不要

（ロ）アラート通知状況

○外部への不正通信を検知・防御した場合は、既に企業内の端末がマルウエアに感染しているなど被害が発生している可能性があり、企業側で対処が必要と考え、ログの記録に加え、重要アラートとして参加企業の管理者宛てにメール通知し対処を促した。

○重要度★★★は、企業内部の端末がマルウエアに感染している可能性があるため、参加企業において至急対処が必要なものであり、商用化時には、保険の対象となると想定している。そのため、アラート通知メール送信後、相談窓口から、ウイルススキャ

ン等対処の依頼を実施。参加企業にて対処できない場合は、相談窓口に問い合わせいただき、必要に応じ対処を代行する駆け付け事業者を紹介した。

○しかしながら、アラートの重要度が参加企業に伝わっていない、参加企業での対処の実施状況が不明などあり、システムからの重要アラート自動送信後に人手を介して能動的に参加企業へ当該重要アラートに対してのフォロー連絡を入れるようにした。

○具体的には、企業内の端末がマルウエアに感染している可能性が高い場合、被疑端末の具体的情報を参加企業に連絡、被疑端末への確実なウイルススキャン（フルスキャン）を実施いただく、フルスキャン実施後の対処結果の確認など、検知した脅威により対処方法を伝え、結果までを確実にフォローをできるようにした。

○実証期間中に送信したアラート通知メールは以下の通り

表 26　月別アラート通知メール数

セキュリティ機能	重要度	7 月	8 月	9 月	10 月	11 月	12 月	1 月	合計
IPS	★☆☆	27	81	130	111	97	68	50	564
	★★☆	4	6	24	18	35	21	69	177
	★★★	0	0	1	1	15	8	1	26
	IPS 計	31	87	155	130	147	97	120	767
AV		0	0	0	0	0	1	0	1
WG		0	1	3	1	0	1	1	7
合計		**31**	**88**	**158**	**131**	**147**	**99**	**121**	**775**

○アラート通知メールの 98%が IPS による検知であった。また、IPS の 73%が参加企業にて緊急の対応は不要のもの★☆☆であった。商用化時には、本通知に対する扱いを検討する必要がある。

○重要度★★★を 11 月 12 月計 23 件通知している。1 社、対処に時間を要し、対処されるまで同じアラートが複数回発生したためである。

⑦参加企業における Web サイトアクセス、アプリケーション使用状況

（イ）Web サイトアクセス状況

○Web サイトへアクセス状況を確認するため、UTM の UF 機能を使用し、本 UTM で保有するカテゴリにマッチした Web アクセスの通信ログを取得した。

○実証期間中のアクセス状況は以下の通り。

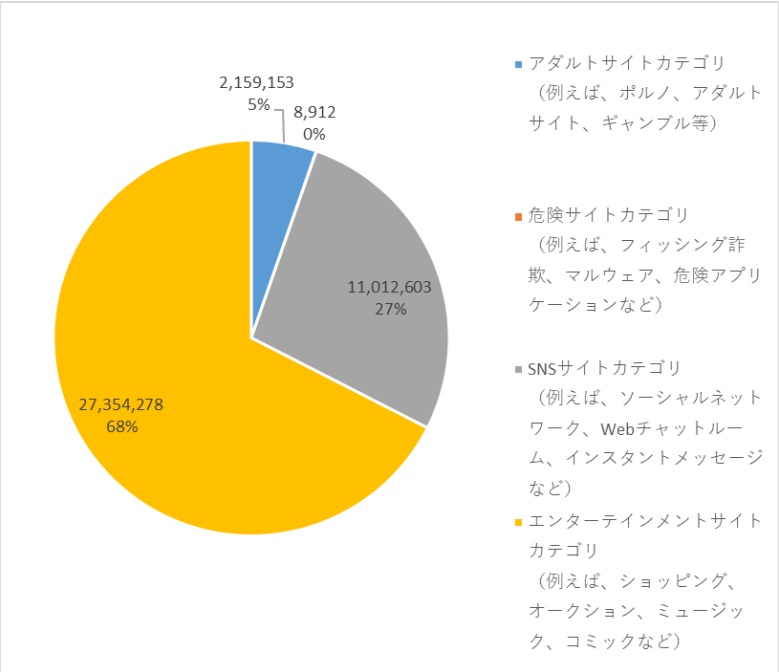


図 10　カテゴリ別 Web サイトアクセス状況

○会社の福利厚生の一環で、私有端末の社内無線 LAN への接続を許可している企業がある。私有端末の利用許可や業務端末によるアクセスでも一般サイトで広告表示などもあり、一概に問題ということはできないが、不審なサイトを閲覧することにより攻撃を受ける可能性がある。業務での利用時に加え、私有端末の利用時に対する注意喚起も必要と考える。

（ロ）アプリケーション使用状況

○ファイル交換ソフトや動画共有アプリ、メッセンジャーアプリなど、不特定多数の個人が情報交換可能なアプリケーションの利用状況を確認するため、UTM の APG 機能を使用し、UTM で保有するカテゴリにマッチしたアプリケーションの通信ログを取得した。

○実証期間中のアプリケーション使用状況は以下の通り

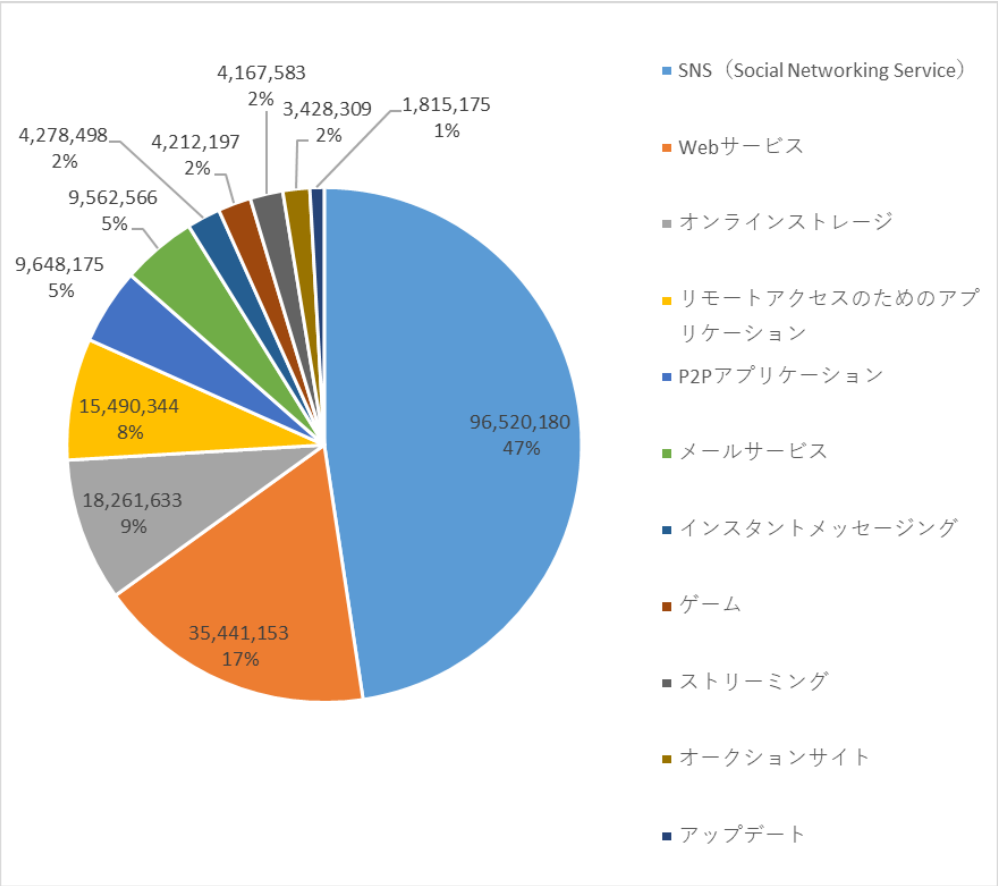


図 11　カテゴリ別アプリケーション使用状況

○Web サイトへアクセス状況と同様、私有端末の利用を許可している企業や、Windows OS 標準でインストールされているゲームが通信しているケースもあるため、一概に問題ということはできないが、業務での利用時に加え、私有端末の利用時に対する注意喚起も必要と考える。

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

（１）京阪神における事後対応支援体制構築の概要（継続的サービス展開、安価なサービス提供を実現するための工夫）

①実施体制構築のねらい・概要・特徴

（イ）各分野の主導的企業、商工会議所、有識者による実施体制（商工会議所起点）

セキュリティで我が国随一の技術を誇る NEC、損保会社として我が国最大手グループに属し業界に先駆けてサイバーリスクに関する保険を商品化した東京海上日動、IT に強いコールセンターであるキューアンドエー、中小企業向けサイバー攻撃対策支援事業を展開してきた大阪商工会議所が実施体制を構築し、神戸大学、大阪大学の専門家にアドバイザーを委嘱し、地域支援体制の礎としたこと。

（ロ）既存リソースの有効活用によるヒト・モノ・カネを節減しての新サービス開発

NEC の既存の UTM や監視サービスインフラ、東京海上日動の既存のサイバーリスクに関する保険、キューアンドエーの既存コールセンター、大阪商工会議所の既存のサイバーセキュリティ事業のネットワークを“発射台”（課題解決の起点）とし、これら既存リソースとポテンシャルを最大限いかしつつも、全体としては全く新しいサイバーセキュリティ・サービスを実証・開発すること。

②地域支援体制構築のねらい・概要・特徴

（ハ）サイバーセキュリティ需給の“地産地消”

サイバーセキュリティの「助ける側」と「助けられる側」の仲介および域内取引を推進（地産地消）すること。その結節点を商工会議所が担うこと。

（ニ）“総合病院”と“町医者”の緩やかな連携

「助ける側」を、地域 IT 事業者（町医者／お助け実働隊）と実施体制組成先の大手 IT 企業等（総合病院／お助け指令隊＝NEC・キューアンドエー）に分類し、両者の緩やかな連携体を構築すること。その結節点を商工会議所が担うこと。

（ホ）母数の力で対応可能エリアと対応可能時間を拡大

各地域の中小 IT 事業者や情報処理安全確保支援士等に出来るだけ多数ご協力頂き、空間軸において対応可能エリアを広げるとともに、時間軸においていずれかのタイミングでいずれかの事業者が駆け付け可能な地域支援体制（母数）を確保すること。

（ヘ）固定費の変動費化による持続可能性向上

特定の中堅 SIer と専属契約を締結すると、実務運営上、効率的であり、駆け付け要員の常時待機・即時対応、訴訟時の対応力などの担保は図れるが、契約金などの初期費用がかかるうえ、サービス単価も高くなり、要員待機に係る固定費なども発生する。これら原価コストは売価に転嫁せざるを得ず、「安価なサービスと中小企業への浸透」という事業目的を達成できない。売価に転嫁しないとなると販売主体の収益性を圧迫し、事業の持続可能性が危うくなる。また、地域サイバーセキュリティ産業の振興への寄与が限定的となる。上記（ハ）～（ホ）の手法を採ることで、初期費用を極小化し、単価を可能な限り下げ、固定費を変動費化する。

（２）事前対応機器としての簡易 UTM の開発と設計

①導入の手軽さ

○“最初の第一歩”が踏み出せないために IT 化が進展しないのが日本の IT 推進上の課題の一つである。とりわけ UTM は、一般的には、設置するだけで時間と手間がかかるという性質があり、この課題を克服しなければ中小企業への普及は困難である。

○よって、本実証事業においては、「ゼロ情シス」の中小企業でも自身で（IT ベンダー等のオンサイトサポートがなくても）UTM 設置ができることを目指し、参加企業において、最低限の設定、最低限の作業となるよう、UTM の設計を行い、NEC にて必要なセキュリティ設定をあらかじめ行った簡易 UTM を参加企業に配送した。

○簡易 UTM を受け取った参加企業は、個別設定が必要な場合のみ設定を実施し、それ以外は LAN ケーブルの結線、アクティベーションの実施（ボタンの押下）だけで簡易 UTM が使用できるものである。

②運用の手軽さ

○“最初の第一歩”を乗り越えられたとして次に課題となるのが“運用の大変さ”。実際、大阪商工会議所が 2018 年 10～1 月に実施した「中小企業を狙ったサイバー攻撃の実態を調査・分析する実証事業」においても、アンチウイルスソフトや UTM を入れてはあるが、運用していない（更新していない）ことによりサイバー攻撃・被害が発生している事例が少なくなかった。

○しかしセキュリティソフトの運用は、「ゼロ情シス」や「ひとり情シス」が多い中小企業では容易なことではない。よって、本実証事業では、参加企業における UTM の運用が必要ないよう、脅威を検知するシグネチャーの自動更新、リモートでのセキュリティ機能の設定変更を可能にし、参加企業は、設置後、特に設定変更などをする必要がないようにした。

（３） 相談窓口の構築（中小企業からの相談受付及び対応、相談内容がサイバーインシデント等であるかの判断）

①役割・機能

○中小企業のサイバーセキュリティに関する悩み相談やインシデント発生時の対処の支援として相談窓口を設置した。相談窓口では、状況が不明瞭なお客様の話を聞くことで、不安を受け止める役割を果たしている。また、インシデント発生時には状況を把握し、対象 PC のネットワークからの切り離しやウイルススキャンなど初動対処をご案内。被害拡大防止の役割を担っている。

②運用手法

○専用フリーダイヤルを準備、土日祝日を除く 9:00～18:00 を受付時間とした。コールセンターは専用席を用意。1 名を専任担当者として電話・メールによる受付を行い、リテラシーが高くない参加企業にはリモートサポートを活用した。

③相談内容がサイバーインシデント等であるかの判断

○相談内容がサイバーインシデント等であるかの判断は、簡易 UTM の検知内容、参加企業からのヒアリング内容を総合して慎重に検討することにより行った。

○アラート通知メールは相談窓口にも送信される仕組みとなっているが、この場合、必要に応じて相談窓口（キューアンドエー）と NEC が緊密に連携して情報交換を行い、参加企業から聴取したネットワーク環境や発生事象などを突き合わせながら判断を行った。

○一方、アラート通知メールを受信していない参加企業から「少しおかしいので相談したい」といった相談が寄せられた際は、先ずは相談窓口の方で、当該参加企業から情報収集し、相談内容がサイバーインシデント等であるか否かを、電話、メール、リモートデスクトップなどを用いて調査し、切り分け、もし疑われる場合は、NEC とも連携し、当該参加企業に係る簡易 UTM 検知情報と突き合わせるなどして判断を行った（なお、サイバーインシデント等であるかの判断に係る考え方については、第３章の（２）簡易 UTM による防御と観測、第５章の（２）簡易 SOC による監視などを参照）。

（４）駆け付け（お助け実働隊）体制の構築（サイバーインシデント等が発生した際の支援の提供）

①役割・要求スキル・対価など

○上記スキームで本実証事業を実施するうえで成否のカギを握るのが事後対応の中核である「駆け付け」を担うお助け実働隊（地域 IT 事業者）である。お助け実働隊には「所定サイバーインシデント駆け付け・初動対処」と「簡易 UTM 設置支援」のうちいずれか一方又は両方を対応頂いた。

表 27

	所定の簡易 UTM 設置支援	所定サイバーインシデント駆け付け・初動対処
役割	参加企業での、所定の簡易 UTM の設置、撤去	参加企業に所定のサイバーインシデントが発生した場合の①駆け付け（24H365D でなくても可）、②状況判断、③暫定対処　等
要求スキル等	◎ＮＷ・ＮＷ製品、ＩＣＴ関係のＨＷ製品の知識と実務経験を有する IT 事業者、IT に強い電気工事業者、情報処理安全確保支援士　等	◎UTM 設置支援の要求スキルを備えていること ◎サイバー攻撃・マルウエア感染等に係る状況判断（他のインシデントとの判別）、現場レベルの暫定対処（ネットワーク切り離し、エンドポイントセキュリティのフルスキャン、OS クリアインストール、その他顧客の IT 環境や意向に応じた対処）ができる IT 事業者、情報処理安全確保支援士　等
	◎大阪商工会議所と所定委託契約が締結できること ◎所定の技術的対応力、顧客対応力があり、大阪商工会議所等と緊密に連携し、所定の仕様と参加企業の意向に基づき業務を履行して頂けること ◎第三者に再請負することなく、委託業務の全部を自己完結的に対応できること	
対価	交通費込 15,000 円（税別） ※追加料金等は支払わない ※２回までは出動回分支払う	交通費込み 35,000 円（税別） ※追加料金等は一切支払わない ※同一案件で２回までは出動回分支払う

②お助け実働隊の集客・選定・契約

○お助け実働隊の集客は説明会、個別依頼、メディア報道等に呼応した先方からの個別エントリー、紹介により行った。

表 28

	エントリー	最終エントリー	採用	契約	実働
先方からエントリー（説明会）	29 社	21 社	12 社	11 社	10 社
先方から個別エントリー（個別説明）	2 社				
当方から個別依頼	5 社				
紹介	1 社				

○結果的に契約締結をしたお助け実働隊の概要は下記のとおり。事業者の所在地の地域的バランス、京阪神の都市部が概ねカバーできること、対応可能曜日に漏れがないことなど、何とか本実証事業を遂行できる布陣を確保できた。しかし兵庫、京都の地域 IT 事業者とは出会うことができず、大阪以外の地域へのヨコ展開には課題となる。

表 29

サイバーセキュリティお助け隊実証事業お助け実働隊の地域 IT 事業者（契約締結）一覧									
	所在地	対応可能内容		対応可能エリア			対応可能曜日	対応可能時間	プロフィール
		UTM	駆付	大阪	京都	兵庫			
1	高槻市	○	○	大阪府全域	京都府南部	兵庫県南部	全	9～21 時	情報処理安全確保支援士、システム監査技術者、IT ストラテジスト、１級販売士、プロジェクトマネージャー、中小企業診断士
2	豊中市	○	○	大阪市内、北摂	—	兵庫県南部	全	9～19 時半	商工会議所 IT 支援推進室アドバイザー
3	大阪市	○	○	大阪市内	—	—	木金除く	10～20 時	情報処理安全確保支援士、情報セキュリティスペシャリスト、ネットワークスペシャリスト、IT ストラテジスト、中小企業診断士
4	大阪市	○	○	大阪府全域	—	兵庫県南部	月～金	10～18 時	中小・中堅企業の IT インフラ整備を支援。パソコン初期設定や社内 LAN 構築、情報セキュリティ診断も対応可能
5	大阪市	○	○	大阪府全域	—	兵庫県南部	全	24 時間対応可能	SOC 受託、SIRT 構築や ISMS 認証のコンサル。情報セキュリティマネジメント有資格者や 5 年以上の経験者で構成。
6	大阪市	○	○	大阪府全域	—	—	月～金	9 時半～5 時半	IT インフラシステム構築、保守業務等。小規模から大規模のシステムに対応可能。
7	大阪市	○		大阪市内全域	—	—	月～土	9～18 時	システム開発、IT インフラ構築、セキュリティ製品販売、ＡＩサービス
8	八尾市		○	大阪市内全域、河内	—	—	土日祝	9～20 時	IT サポート、コンサルチーム。情報処理安全確保支援士、現役 CSIRT 職員などセキュリティ最前線のプロで構成
9	堺市	○	○	大阪府全域	—	—	月水金	9～20 時	情報処理安全確保支援士、IT 経営コンサルティング、情報セキュリティコンサルティング、中小企業診断士
10	貝塚市	○	○	大阪府全域	ご相談	神戸市内全域	月～土	10～18 時	パソコンや IT 駆け付けサポート 20 年の実績。大阪府下なら最短 60 分以内で駆け付け
11	貝塚市	○	○	大阪府全域	—	—	全	13～21 時	過去 4 年間で 70 件程度のレスキューサービス経験あり

③駆け付け（お助け実働隊）体制構築に係る直面課題と解決法

（イ）「誰が」やるのか？（お助け実働隊の担い手）

○当初は「UTM 設置支援」や「駆け付け」を、各参加企業がそれぞれ独自に契約している IT 事業者にご協力頂くという案もあったが、本実証事業の趣旨への理解という観点、簡易 UTM 設置方法への理解という観点、一般的な IT 事業者がサイバーセキュリティに詳しいとは限らないという観点、地域サイバーセキュリティ産業の振興という観点、単価抑制という観点、などから、サイバーセキュリティに一定の知識と技能を有する地域 IT 事業者等を大阪商工会議所が独自に募ることとした。

○必要かつ十分なスキルセットとしては、参加企業の多くでネットワーク構成図が存在しないことを前提に、その環境下でも適切な位置に適切な方法で UTM を設置でき、インシデントの切り分けや初動対処ができる IT・NW 関係知識と、参加企業とのコミュニケーション能力などを想定した。また、ネットワーク構成やハードウエア、ソフトウェアが各参加企業にとって機密事項であることをふまえ、信頼関係が何より大切であることから、人間的な側面や事業歴も選定・契約上の判定基準とした。また本実証事業が中小企業へのサイバーセキュリティの普及・啓発も目的の一つとしていることをふまえ、セキュリティに係る指導力も重視した。

（ロ）「何を」「どこまで」やるのか？（業務内容と業務範囲）

○「事後対応支援」「安価かつ簡便なサイバーセキュリティサービスの構築」という本実証事業の趣旨および予算的制約から「初動対処」に限定し、インシデントの原因と状況の特定、マルウエアのエンドポイントにおけるフルスキャンおよび駆除とそれらに付随する最低限の対応、に限定し、本格調査や根治療法は含まないこととした。これにより、お助け実働隊でも、時間的、技能的に概ね対応可能となる。

○初動対処は、インシデントの種類と参加企業側の状況により、作業内容や時間が大幅に異なる。フルスキャンや OS クリアインストールは、端末台数によっては長時間を要す。役務提供対価（後述）及び本実証事業の事業目的とするところを量的にも質的にも「上回った分」をどうするかが最大の焦点である。お助け実働隊同士の平等性の観点、参加企業同士の平等性の観点も必要である。また訴訟リスクもある。

○「上回る部分」の作業は「本実証事業の対応範囲を超えるので対応できない」ことをお助け実働隊が参加企業にその場で説明すること、参加企業が「上回る部分」の作業実施を希望するなら、見積書を提示するとともに当該作業が「トラブルが生じても大阪商工会議所は責任を負わないこと」をお助け実働隊が説明し、参加企業から発注の意思表示があった場合のみ対応することを原則化し、仕様書にて明記した。

（ハ）「どのように」「いつ」やるのか？（出動タイミング）

○所定サイバーインシデントと認定（後述）された場合、参加企業にメール等で通知し、参加企業が駆け付けを希望する場合は、お助け実働隊リストを提示し、参加企業自身にお助け実働隊を選択してもらい、両者の都合の良い日時に駆け付けを行うこととした。依頼を受けたお助け実働隊は相談窓口から UTM 観測情報の提供を受けるとともに、大阪商工会議所から発注を受けることで駆け付けを行う流れとした。この際ポイントは、救急車のごとく即時に駆け付けを行うことを要件化しなかった

ことである。参加企業側にも本件了解のもと参加申込して頂いた。24 時間 365 日の待機と即時駆け付けを前提にすると、事業の持続可能性が危うくなるからである。

○そこまでの体制を構築する必要がない理由としては、技術的には、簡易 UTM が「内→外」のアウトバウンド通信を遮断するため、被害（マルウエア等の侵入と作動）が実害化（C&C サーバー等への情報流出や D-DoS 攻撃への加担等）することの防止又は“時間稼ぎ”ができるためである。体制的には、お助け実働隊を一定数リストに掲載しておくことにより、参加企業が依頼したA社が即応できない場合でも、次にB社、C社、、、と順番に打診していくことにより（顧客満足度は低下するが）、いずれかのお助け実働隊が即応できるような母数を確保できたためである。

（ニ）「なんぼで」やっていただくのか？（役務提供対価）

○UTM 設置を業務として請け負っている中小 IT 事業者は少なく、またサイバーインシデントに限定したオンサイトサポートを専業的に行っている中小 IT 事業者も僅少であるため相場が判然としなかった。そこで、検討の結果、試行的に時給１万円と想定し、UTM 設置に１時間（NEC の想定した設置時間 30 分に、ネット環境のヒアリング 20 分、実施報告書執筆 10 分を加算）、インシデント駆け付けに 3 時間を要するという想定のもと、移動時間の機会損失補償とみなし交通費を便宜上 5 千円相当と仮定し、消費税別、交通費込で、UTM 設置 1 万 5 千円、所定サイバーインシデント駆け付け 3 万 5 千円の一律料金とした。

○時給制でも作業内容に応じた計算方式でもなく一律料金とした理由は、(a) 支出予算の見通しが立てやすいこと、(b) 請求額がお助け実働隊や案件ごとにまちまちであれば金額の妥当性査定に手間がかかること、(c) 国費で行われる本実証事業の性質に鑑み一律定額である方が平等性、公正性の観点から望ましいこと、(d) お助け実働隊には複数回出動頂くことを想定していたため、ある現場では一律料金を上回る仕事であったとしても、ある現場では下回る仕事となることもありえ、中期的にはプラスマイナスゼロに収斂していくであろうと考えられること、(e) 上記（ロ）の当実証事業の対応範囲を「上回る部分」の作業実施に係る対価は本実証事業とは別の枠組みで参加企業自身が支払うこと、などによる。

○UTM 設置も、所定インシデント駆け付けも２回までの支払を可能とした。参加企業にネットワーク構成図が存在しないことが予想されること、フルスキャン等に長時間を要することが理由である。とりわけ中小企業では、ウイルス対策ソストを最新の定義ファイルにアップデートしていないケースが多数想定されることを

見越し、フルスキャンの前段階としてアップデート作業を前置せねばならないことも想定されたためである。（実証の結果、事実こういったケースは多かった）

（ホ）どうやって集めるのか？（集客）

○サイバーセキュリティのオンサイトサポートは一般的な IT 事業者が対応できるとは限らない。実際、中小企業からよく聞く声として「どこに、優秀で良心的なセキュリティベンダーがいるか分からないので、相談も発注もできない」といったもの。本実証事業の目的の一つは、地域中小 IT 事業者とユーザー中小企業をつなぐことである。しかし、大阪商工会議所としても、事業者がどこにいるかよくわからないのが実情である。なぜなら、同産業分野には有力な業界団体などが殆どなく、まとめて所在を把握したり打診したりすることが困難だからである。今回は、本実証事業の第 1 回説明会の中で地域中小 IT 事業者向けの説明会も併催し 29 社 38 名が出席。21 社がエントリーし最終的に 11 社と契約をするに至った。

（ヘ）スキルをどう評価するのか？求めるスキルはどのようなものか？（採否）

○地域 IT 事業者がエントリーしても、その事業者の採否基準が次の課題となる。IPA の仕様書には IT シルバー人材の登用が挙げられていたが、経験則上、IT シルバー人材にサイバーセキュリティの現場対応業務を依頼するのは少々心許ないものがある。リカレント教育を行うことも事業スキーム、予算上、想定していない。

○そこで一つの目安として、情報処理安全確保支援士のほか、情報セキュリティスペシャリストなどの資格保有もしくはそれと同等と考えられる現場経験のある法人もしくは個人をコア・ターゲットとして、説明会の案内、個別依頼を行った。

○参加企業の多くは「ゼロ情シス」「兼任情シス」であることが予想され、サイバーセキュリティに係る専門用語を理解できないことをふまえ、コミュニケーション能力を重視した。それを担保するスキルとして想定したのが中小企業診断士と情報処理安全確保支援士の両方の資格を持つ「サイバーセキュリティに強いコンサルタント」である。中小企業に寄り添い、難解なサイバーセキュリティの話を平易に伝え、駆け付け対応と啓発を両輪で行えるスキルを有する事業者である。

○情報処理安全確保支援士の士会は、まだ全国的に組織化が進んでおらず、2019 年に中央組織が設立されたことは第一歩である。今後は府県で組織化が進むことが予想されるが、商用化に向け、同会の地方支部との連携が期待されるところである。

（ハ）出動要請はどれくらいあるのか？（需給バランス）

○お助け実働隊の採否は、保有スキルや対応可能事項以外に需給バランスも考慮する必要がある。契約先を多数にすると供給過剰となり、お助け実働隊としての“出番”が少なくなる。この需給バランスの事前予想が困難だったため、一時にして多数の地域 IT 事業者と契約を締結するのではなく、事業開始時点では少数に抑え、事業進捗の中で出動頻度を見極めながら、必要に応じ順次契約締結を進めた。

○需要予測は、UTM 設置で 7 割、UTM 撤去で 3 割、所定インシデント駆け付けで 3 割とし、予算化もこれに基づいて行った。（実証の結果、良くも悪くもこの予想は大幅に外れた。本件に関する詳細は後述）

（ニ）利害調整をどうするのか？（契約の一律化）

○お助け実働隊を多数確保することが、早期対応力の確保、対応可能エリアの拡大、サービス料の低単価化といった点で重要となるが、ここで課題となるのが、契約先が複数であるがゆえの利害調整。契約内容を各者各様のものとすると、大阪商工会議所として事務的に煩雑となるばかりか、共通の条件でのガバナンスが困難になる。そこで、委託契約書の内容を、大阪商工会議所と IPA が締結した請負契約にほぼ準拠させた内容とすることにより、原契約における大阪商工会議所と IPA との法的関係性と、各事業者と大阪商工会議所との法的関係性を整合させる必要性がある点を強調するなどし、一律に共通の契約書での締結を依頼することとした。その結果、12 者中 11 者とは契約できたが 1 者とは折り合いがつかず、結果的に契約締結に至らなかった。

（ホ）作業ミス等に係るリスクの査定およびリスクヘッジ

○お助け実働隊が駆け付け先の参加企業で何らかのミスをしてしまい、実害が生じる場合、ミスや実害としてどのようなものがありえるか、また、そのリスク回避手法としてどのようなことがありえるかを検討することは頗る困難であった。

○契約締結要件として、お助け実働隊に各自一定の損害保険に加入して頂くことも検討し、損害保険会社に売上高ごとの保険金・保険料のシミュレーション見積りを依頼したところ、予想以上に保険料額が高いことが分かり、要件化を見送った。

○そこで、大阪商工会議所が加入する損害保険が、大阪商工会議所自身に起因する案件のみならず、委託先たるお助け実働隊に起因する案件に係る当該委託先の損害賠償責任までカバーされることを以て一定の担保とした。

５．地域実証の実施

（１）参加中小企業（ユーザー：助けられる側）の集客

①ターゲット

（イ）仕様書に定められた参加対象

○中小企業基本法の中小企業（一般社団法人、学校法人から参加希望が計４件あったが謝絶）で、サプライチェーンを構成する企業を中心とする。（目標：概ね８割）

（ロ）目標とした参加企業数

○100 社（大阪府・兵庫県・京都府）

②集客手法と集客状況

（イ）集客方法と工夫Ⅰ（Whole Sale 的手法）

○「サプライチェーン」上位の大企業等に集客の協力要請を行い、大企業等から（a）取引先に案内頂く、（b）取引先を個別紹介頂く、（c）取引先への説明の場を提供頂く、などを依頼した。

○サプライチェーンを活用しての集客を見越し、2019 年 2～4 月に大企業・中堅企業を対象に「サプライチェーンにおける取引先のサイバーセキュリティ対策等に関する調査」を戦略的に実施。本実証事業での集客の協力依頼を後刻行うことを前提に、可能な限り訪問による対面調査を行い、人間関係を構築しておいた。

○京阪神の商工会議所等に一斉案内もしくは個別紹介の協力要請を行った。

○プレス発表による広報、大阪商工会議所の広報紙、ＦＡＸ、メール等での広報を行った。

○上記を可能な限り説明会開催前に行い、説明会に誘導し、一括的に事業案内した。

（ロ）集客方法と工夫Ⅱ（Retail Sale 的手法）

○本実証事業は商用化を前提としているため、商用化段階での運用をふまえた上で実施すべきものではあるが、一方で本実証事業は経済産業省の重要施策にも位置付けられていることもあり、本実証事業それ自体を着実に成功させることも至上命題である。よって、進捗状況を見極めながら、もし前項（イ）の手法が不振である場合のことを想定し、保険的に人手のかかる個別案内的手法をも併用した。

○これは大阪商工会議所が有するここ数年のサイバーセキュリティ関係事業の利用企業を中心にプロファイルした候補リストから１件１件電話でアポを取得し担当者が訪問のうえ説明する手法で、人手を要する手法だが、着実な手法であった。

（ハ）集客で注意した点

○設置時、ファームウエアアップデート時にネットワーク瞬断がある点の説明

○設置は概ね容易であるものの IT 環境により時間がかかる場合があることの説明

○採取する通信情報の説明（電気通信事業法の通信の秘密の侵害に抵触しない旨）

○UTM 起因の何らかのネットワーク障害及びそれに起因する損害への免責の説明

（ニ）集客に要した日数、広報タイミングとの相関関係

○集客の推移（申込書記入日）は下記グラフのとおり。目標の 100 社に達したのは 9 月中旬。広報開始から約 3 か月後であった。（簡易 UTM 設置日ではない）

図 12

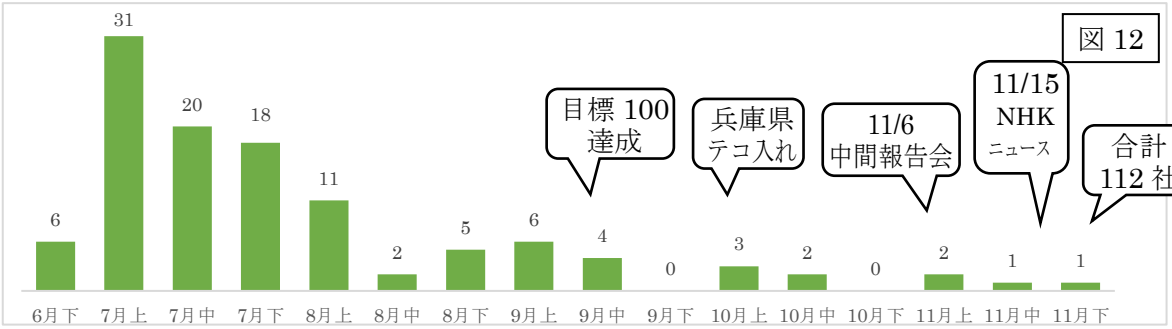


図 13

（ホ）集客の具体的方法と集客結果

○具体的な広報・集客チャネルとその結果は下記表のとおり。

表 30

Whole Sale 的手法 約 63 件 (56%) 由来が一部推定。一部重複含む	広報紙記事（6/10, 7/10：3 万社）、広報紙同梱チラシ(6/25：3 万社)・HP(6～7 月)、DM(6/21:1324 社)、FAX（6/12:4915 社）、尼崎 FAX（8 月：1075 社）、一斉 Mail（6/21:8835 社）、プレス発表（7/3: 5 紙掲載・NHK 報道 7/8, 11/15, 11/27）	約 39 社
	事業説明会（7/5: 78 社参加）、中間報告会（11/6:127 名参加）	実質新規のみ約 20 社
	経済産業省近畿経済産業局主催「サイバーセキュリティソリューション地域別講座」(7/22 京都・29 大阪・30 神戸：計約 150 社)、NEC iEXPO（7/12）	約 2 社
	大阪商工会議所以外の商工会議所（豊中・京都・神戸・尼崎・明石等）	9 社
	大阪商工会議所の議員会社である地域有力企業に紹介依頼	5 社
	その他（神戸大学、お助け実働隊、地域中堅 IT 企業、東京海上日動の有力代理店の紹介）	6 社

重複有

Retail Sale 的手法 約 49 件（44%） 由来明瞭の確定値。重複無	大阪商工会議所 17 年度サイバーセキュリティ関係アンケート回答企業（tel78 社→訪問 19 社）	13 社
	大阪商工会議所 18 年度サイバー実態調査実証企業（全 30 社→説明会 11 社・訪問 10 社）	15 社
	大阪商工会議所のサイバー関係事業以外の事業利用企業（tel120 社→訪問 15 社）	11 社
	大阪商工会議所の提携先（訪問 1 社）	1 社
	大阪商工会議所職員の知己（訪問 8 社）	6 社
	大阪商工会議所の入会年の浅い会員（258 社プロファイル→TEL69 社→訪問 8 社）	3 社

③参加企業のあらまし

（イ）参加企業数とその概要

表 31

参加申込企業数（代表者印押印申込書提出）	実証実施企業数（UTM での観測・防御等）	目標（達成率）	府県	サプライチェーン構成有無	業種	規模
112 社	112 社	100 社（112%）	大阪 95 社（85%） 兵庫 14 社（12%） 京都 3 社（3%）	構成 89 社（79%） 非構成 23 社（21%）	製造 44 社（39%） サービス 35 社（32%） 卸売 18 社（16%） 建設 8 社（7%） 小売飲食 6 社（5%） 運輸 1 社（1%）	社員数 平均値 29.3 人 中央値 11.5 人

（ロ）業種の詳細

○製造……金属系 9 社、機械･機器･装置系 8 社、部品･工具系 5 社、化学･素材系 4 社、生活･事務用具系 4 社、食品系 4 社、紙･印刷系 3 社、什器･備品系 3 社、プラスチック系 2 社、繊維 1 社、その他 1 社

○サービス…IT 系 9 社、士業系 8 社、メディア系 3 社、不動産 2 社、エネルギー系 2 社、旅行業 2 社、人材系 2 社、専門技術系 2 社、個人医 1 社、その他 4 社

○卸売……化学･薬品･素材系 6 社、飲食料品系 4 社、建材系 2 社、その他 6 社

○建設……内装系 3 社、総合系 2 社、工事系 2 社、塗装系 1 社

（ハ）府県別、大阪府内の市別の構成

表 32

大阪府大阪市	72 社（64%）	〃 枚方市	1 社（1%）	〃 京都市	1 社（1%）
〃 豊中市	5 社（4%）	〃 東大阪市	2 社（2%）	兵庫県神戸市	7 社（6%）
〃 箕面市	3 社（3%）	〃 松原市	1 社（1%）	〃 尼崎市	1 社（1%）
〃 吹田市	2 社（2%）	〃 八尾市	1 社（1%）	〃 西宮市	1 社（1%）
〃 摂津市	1 社（1%）	〃 堺市	1 社（1%）	〃 伊丹市	1 社（1%）
〃 茨木市	2 社（2%）	〃 大阪狭山市	1 社（1%）	〃 宝塚市	2 社（2%）
〃 高槻市	1 社（1%）	〃 阪南市	1 社（1%）	〃 川西市	1 社（1%）
〃 門真市	1 社（1%）	京都府京田辺市	2 社（2%）	〃 明石市	1 社（1%）

（ニ）企業規模の詳細

○規模別の参加状況は下記のとおり。本実証事業で使用した簡易 UTM のスループットに鑑み、推奨端末台数は 100 台程度としたが、100 台を上回る企業のうち参加を希望する企業も参加を受理し、UTM の性能限界等も実証の対象とした。

表33

0～5人	6～10人	11～20人	21～30人	31～40人	41～50人
35社(31%)	20社(18%)	12社(11%)	10社(9%)	13社(12%)	5社(4%)
51～60人	61～70人	71～80人	81～90人	91～100人	101人以上
2社(2%)	3社(3%)	3社(3%)	2社(2%)	2社(2%)	5社(4%)

④集客およびその結果に係る考察

（イ）サプライチェーンを通じた集客

○サプライチェーン上位の大企業に、参加企業集客の協力要請を行い、メールでの取引先等への転送案内、調達方針説明会での説明機会付与、候補先企業リストの提供などの協力を得た。しかし、候補先企業リスト以外は奏功しなかった。その理由は、大企業といえども取引先のサイバーセキュリティを把握・管理できていない（上述）こと、独禁法や下請法における優越的地位の濫用に抵触する恐れがあり取引先に具体的な指示がやりにくいこと、などに因るものと考えられる。

（ロ）各地商工会議所（大阪商工会議所以外）を通じた集客

○個別に会員企業に対して説明を行い、参加を募った大阪商工会議所での集客は順調であったが、大阪商工会議所以外の商工会議所での集客は厳しい結果だった。この点は、商工会議所ルートの募集であっても、お助け隊認証制度や補助金など更なる普及支援策が必要となろう。

（ハ）UTM と集客

○電話での個別案内の際に、UTM の設置有無を確認のうえ未設置の企業のみを訪問した。しかし、いざ訪問してみると UTM が設置されているケースが約 2 割あった。UTM を UTM と認識せずに使用しているわけである。

○電話でのアポ取得にあたり、UTM 設置有無を問うことは、企業の機密に関する質問なので、ほぼ初対面の相手に対するテレアポのプロトコルとしては不躾であるばかりか、情報セキュリティを啓発しそのサービスを販売していく主体としては自己矛盾ともいえる。架電者が大阪商工会議所だから警戒心を抱かないのかもしれないが、商用化段階においては、販売・営業上の大きな障壁となりえる。

（ニ）ニーズのありそうな業種・業態

○IT 業は 9 社、士業は 8 者と、比較的多数の参加申込があった。IT 業界といえどもサイバーセキュリティを専門としているわけではないこと、士業については個人情報やセンシティブ情報の取り扱いが多いことなどに因るものと考えられる。

（ホ）参加企業のリテラシー

○参加申込書にネットワーク環境（例：プロキシサーバーの有無、ホームゲートウェイがルーターと一体型の ONU で構成されているか否か、IP アドレスは固定か DHCP か等）の質問欄を付設した。これに対し、完全記入（又はほぼ完全記入）は 28 社（25%）、部分記入は 10 社（9%）、無記入（又は「不明」で回答）は 74 社（66%）だった。参加企業はサイバーセキュリティについて一定の意識を有している企業といえるが、そうした企業ですら、自社のネットワークのごく基礎的な概要も把握していない実態が明らかになった。これは商用化においても大きな足枷となろう。しかし、そうしたレイヤーの中小企業をこそ支援するのが大阪商工会議所および本実施体制の使命であるともいえる。

（2）簡易 SOC による監視（見守り）

①実証中に実施したサービス内容の改善

○当初は、簡易 SOC として、アナリストによるログ解析を前提とせず、システムによる自動判定の範囲でサービスを提供することを想定していた。しかし、マルウエアに感染していない端末での過検知による重要アラートメールが頻発したため、発生した重要アラートはいったん NEC のアナリストが解析する運用に変更した。これにより、過検知であるものはユーザーに連絡しない運用とした。

○当初は、重要アラートの対象はすべて対処が必要である、という方針であったが、マルウエアへの感染とは直接関係ないアラートが頻発したため、以下の 3 段階にアラートを分類した。

- ★★★：マルウエアの振る舞いを検知したもの。至急対処が必要
- ★★☆：攻撃の振る舞いとして検知したもの。対処を推奨
- ★☆☆：それ以外。至急の対処は不要

○実証で行ったアラート通知には、重要度★☆☆のユーザーによる緊急対処が不要なものを大量に含んでいる。アラート通知メールが大量に届くとなると、ユーザーによる対処が必要な重要度★★☆、★★★のアラート通知を開封すらしなくなる恐れがある。実証ではフォローを行ったが、商用時の対応を検討する必要がある。

②サービス改善に向けた継続検討事項

○検知結果として過検知と思われる事例も数社において判明した。商用化においてはこういった危険性のない過検知を抑制し、アラート精度向上策を実施していく必要がある。

○また、簡易 UTM だけではどうしてもセキュリティインシデントの問題を特定できないケースがあり（UTM はあくまでネットワーク上のパケットでの監視でエンドポイントを直接監視できていない)、この場合においても商用化時には、エンドポイントセキュリティと組合せたインシデント原因究明を検討していく。

○実証時においては、簡易 UTM のファームウェアの更新は、決まった時刻に再起動が発生する仕組みであったが、この運用では、参加企業がネットワークを止めたくない時間に勝手に簡易 UTM の再起動が実施されてしまいネットワークの停止が出てしまう。こういった参加企業には実証時は個別に簡易 UTM 再起動時間を調整して

いたが、商用化時には参加企業側自身が再起動を伴う更新を任意のタイミングで実施できるようにする必要がある。

○アラート通知の中には、検知した端末の IP アドレスと MAC アドレスを記載している。しかしながら、端末特定に至らず、全端末にウイルススキャンを実施したケースもあった。

- DHCP を使用している環境で、対処を行おうとしたときには端末の IP アドレスが変わっている
- 無線アクセスポイントを使用している環境で MAC アドレスが無線アクセスポイントのものになってしまう

対処が必要な端末の特定を、中小企業にもわかりやすく伝える方法を検討する必要がある。

○ポータルサイトへのログインには、セキュリティ強化のため、多要素認証を行っている。多要素認証には、ID パスワードに追加し、携帯電話スマートフォンの SMS を使用する方法と QR コードを読み取って認証させる方法から選択していただくこととした。しかしながら、私有端末しかないため使用したくない、使用しても SMS が届かないなどの問題が発生した。商用化時には、携帯電話やスマートフォンが使用できないケースも想定する必要がある。

○実証時では、1 台でも監視対処となり通信ログが取得できれば問題ないとし、参加企業が監視したい端末をすべて監視できる位置に UTM を設置できているかは確認していない。商用化時においては、保険の対象範囲にも影響するため、どの端末を監視できているかユーザーも把握できる仕組みを引き続き検討する必要がある。

③監視に係る考察

○「3.(2)③参加企業におけるサイバー攻撃の検知状況」に記載した通り、参加企業 112 社中 74 社で外部への不正通信と外部からの攻撃を遮断した。なお、UTM はブロードバンドルーターの内側に設置しており、不特定多数を対象とした攻撃の大部分はブロードバンドルーターで遮断される環境だった。このことから、少なくとも 66%の企業が、実証事業中に危険性の高いサイバー攻撃を受けていたことが分かる。

○大阪商工会議所が本実証前に実施した神戸大学と東京海上日動との共同研究[1]において、30 社中 30 社でなんらかの不正通信を検出しているが、本実証との大きな違いは、以下である。これが攻撃を受けた企業の割合に影響を及ぼしていると考える。

・ ブロードバンドルーターが、PPPoE によりグローバル IP アドレスを取得し、ブロードバンドルーター配下にプライベート IP アドレスを配布している構成では、ポートスキャンがブロードバンドルーター配下まで到達せず、検出できない。

○マルウエアへの感染が疑われるアラートが発生したユーザーのエンドポイントでウイルススキャンを実施した結果、6 社で実際にマルウエアへの感染が確認された。ウイルス対策ソフトを導入していても更新が行われていなかったり、持ち込まれた端末がマルウエアに感染していたりするケースもあった。さらに、参加企業の経営者の親族が経営する別法人と無線 LAN を共有しているような、ネットワーク管理に問題を抱えているようなケースも確認された。このように、中小企業におけるセキュリティ対策の不十分さが浮き彫りとなった。

[1] 2018 年 10 月~19 年 1 月までの約 4 か月間、大阪府内の多様な業種・規模の中小企業 30 社のルーターと PC 群（ハブ）の間にセンサーを設置し、インバウンド、アウトバウンドの通信記録を観測・記録し詳細に分析

（3）相談窓口

①電話・メールによる相談の内容・傾向・件数【事例紹介含む】

各月の入電・メール問合せ推移、問い合わせ内訳は下記の通りとなる。 表 34

項目	7 月	8 月	9 月	10 月	11 月	12 月	1 月	累計
入電件数	32 件	54 件	54 件	42 件	48 件	43 件	18 件	291 件
応答件数	28 件	53 件	52 件	42 件	46 件	42 件	17 件	280 件
応答率	87.5%	98.1%	96.3%	100%	95.8%	97.6%	94.4%	96.2%

※入電件数と応答件数の差は、対応中に入電が重なり担当者に繋がらなかったため。

表 35

項目	7 月	8 月	9 月	10 月	11 月	12 月	1 月	累計
メール問合せ数	10 件	14 件	14 件	17 件	4 件	13 件	3 件	75 件

※メール問い合わせ数はユニーク件数。

表 36

お問合せ内容	7 月	8 月	9 月	10 月	11 月	12 月	1 月	累計
UTM 設置関連	12 件	24 件	26 件	8 件	3 件	1 件	0 件	74 件
ポータルサイト関連	6 件	26 件	7 件	7 件	1 件	0 件	0 件	47 件
アラート関連	3 件	5 件	6 件	4 件	7 件	0 件	2 件	27 件
セキュリティ関連	2 件	3 件	9 件	0 件	1 件	1 件	0 件	16 件
UTM 撤去関連	0 件	0 件	0 件	0 件	0 件	0 件	3 件	3 件
その他	6 件	1 件	1 件	12 件	8 件	21 件	9 件	58 件

※問い合わせ内容は応答件数のユニーク数とメール問合せ数の合算。

○お問い合わせの 7 割が電話による相談、残り 3 割がメールによる相談となっている。電話による相談が過半数とはなるが、営業時間内に問い合わせすることが難しい企業や電話ではなくメールによるやり取りを希望される企業があり、結果としてメールでの問い合わせも一定の割合を占めた。

○お問い合わせ内容は UTM 設置時の問い合わせが最も多く、参加企業の内約 30%から問い合わせを頂いている。内容としては「配線位置が分からない」「配線したがアクティベーションができない」等となっている。またポータルサイト関連についても設置時と同タイミングでの入電が多く、「ポータルへのログイン分からない」「2 段階認証ができない」等の入電となっている。設置後は徐々に入電が減少していき、問い合わせ内容もアラート関連やセキュリティ関連へ変化している。

○参加企業自身で UTM の設置が完了しないケースとして、ほとんどが配線位置を間違えており、PPPoE セッション（プロバイダ情報）が設定されている機器（ルーターなど）よりも手前に UTM を接続しているため、UTM の通信がインターネット上に接続できない状態となっていた。

○相談窓口にて、参加企業担当者の方と配線の確認や取り付け依頼を行うものの、「自社のネットワーク環境を把握していない」との申告から配線の案内に時間がかかるケースや担当者のリテラシーが不足し「電話案内にて作業を行えるか不安」との理由で、最初から駆け付け設置を希望されるケースもあった。

○アラート関連の問い合わせで特徴的なのは、重要アラートの中で危険度が高い通知でも企業からの問い合わせが少なく、定期的なアラートチェックもされていない企業がいるなどセキュリティ意識の低さが見受けられた。結果的に当初業務フローでは想定していなかった相談窓口から対象の企業へ連絡する対応が多く、その際、相談窓口から連絡を入れるも企業担当者不在で対応が遅れるようなこともしばしばあった。

○今回の実証を通じて設置マニュアルをより分かりやすい表記にすることや、ユーザー環境パターンによる設置事例などを追加するなど工夫が必要であることが分かる。また、アラート発生時に迅速に対応出来るよう、参加企業においても定期的なアラートチェックを含めてセキュリティに関する意識向上が必要であると感じる。

②各関係者の連携

相談窓口では問い合わせ頂いた際に、登録・設置に関する内容かトラブルかを判断し、各関係者と以下の様に連携を行った。

（イ）ポータルサイト登録、UTM 設置に関する対応

○電話またはリモートで対応し、解決に至らないケースは駆け付け提案を行い、参加企業が希望する場合は駆け付け IT 事業者に環境情報などの情報共有を行った。

（ロ）UTM 設置後のトラブルやインシデント対応

○電話またはリモートで対応し、解決に至らないケースは NEC にエスカレーションを行い、対応方針を仰ぎ、それを元に参加企業への回答を行った。駆け付け対応の場合は、①同様に駆け付け IT 事業者に情報共有を行っている。

（4）簡易 UTM 設置

①簡易 UTM の自社設置率

○実証前の仮説として簡易 UTM の設置支援として 70%（自社設置率 30%）を予測したが、実証の結果、お助け実働隊による設置支援率は 31%（35 社 37 件※1 社あたり 2 回出動した場合もある）で、自社設置率は 69%（77 社）であった。
これは仮説とした 30%を大幅に上回った。

○69%の自社設置企業は、全てが完全自力で設置できたわけではない。中間アンケート（回収率は 59%）によると、少なくとも 28%は相談窓口に相談して設置。

表 37

簡易 UTM 設置にあたり相談窓口に相談し、設置できた	17 社（n=61　28%）
簡易 UTM 設置にあたり相談窓口に相談したが、設置できなかった	8 社（n=61　13%）
簡易 UTM 設置にあたり相談窓口に相談しなかった	36 社（n=61　59%）
アンケート回答社（66 社）の中でこの質問に無回答	5 社

○簡易 UTM を自力でもお助け実働隊でもなく、自社契約の IT 事業者が設置した割合は特異的に少なく、これは仮説を大幅に下回った。本件については、実証実施前に争点となった。即ち「実証の趣旨・内容と簡易 UTM については良く知っているけど参加企業のことやそのネットワーク環境を全く知らないお助け実働隊」か「実証の趣旨・内容と簡易 UTM への理解は乏しいけど参加企業やそのネットワーク環境を熟知している参加企業側契約 IT 事業者」か、どちらが有用で安全なのか。適切性については本実証事業では検証していないが、少なくとも、事実として、圧倒的多数の参加企業がお助け実働隊を選択する結果となった。

②簡易 UTM の設置および設置支援に係る考察

（イ）中小企業は何を求めているか

○中小企業が「サイバーセキュリティ対策として最も最重視していること」は、価格、機能、使い勝手が上位を占めている。

表 38

サイバーセキュリティ対策として最も重要視していること（再掲）	7/5 第 1 回説明会 n=69（参加企業以外も含まれている）※複数回答あり	11/6 第 2 回説明会 n=124（参加企業以外も含まれている）※複数回答あり	11 月中間アンケート n=66（参加企業）※複数回答あり
価格	45（65%）	71（57%）	54（82%）
機能	48（70%）	84（68%）	41（62%）
使い勝手	32（46%）	52（42%）	31（47%）
相談窓口	19（28%）	25（20%）	24（36%）
駆け付け	10（14%）	14（11%）	8（12%）
その他	1（1%）	3（2%）	0

○本実証事業では、機能が良く、価格が「安価」で、使い勝手も良い UTM の設計と運用を実証した。中小企業での普及には「導入」と「運用」が「簡便」なものが必須である。これが実現できると、通常なら UTM 導入に要する IT 業者の派遣・設置費が節減でき、その分の売価転嫁が少なく、結果として「安価」も実現できる。

○「導入」の簡便は、簡易 UTM が顧客に宅配便で届くところからそれを設置し導通するまでの一連のプロセスが、短時間、簡便、安価に実施できることを目指したものである。「簡便」の定義は、専任の情報システム担当者がいない、「兼任情シス」、「ゼロ情シス」の中小企業でも、設置マニュアルに基づき設置ができる、というレベルをイメージしている。そんな簡易 UTM を本実証事業のために NEC が特別に設計、開発し、実証の結果、「導入の簡便さ」が明らかになった。

（ロ）簡易 UTM は、どのくらい簡易だったか

○自社設置率の 69%という成績は、改善の余地があるとはいえ、「UTM は通常 IT ベンダーが設置するもの」という業界常識に鑑みれば、画期的な数値である。では、どの程度簡易だったのかを定量的に把握してみると下記のとおりとなる。

中間アンケート回答者のうち自社設置と回答した 51 社に対し難易を聞いている。

表 39

自社設置（容易だった）	41 社（n=51 80%）	平均値 20 分、中央値 10 分
自社設置（困難だった）	10 社（n=51 20%）	平均値 77 分、中央値 60 分

○自社設置と回答した 51 社中 80%である 41 社が「容易だった」と回答している。この母集団では中央値 10 分、平均値 20 分で設置できている。NEC の実証前の予測時間は 30 分だったので、簡易 UTM の簡易たる所以が実証で明らかとなった。

○簡易 UTM の自社設置率を大きく左右するのが、同封の「設置マニュアル」の存在である。下記結果は商用化に向けて大いに改善の余地がある。

表 40

簡易 UTM「設置マニュアル」は分かり易かった	37 社（実回答者 n=55 67%）
同　分かりにくかった	18 社（実回答者 n=55 33%）

○なお、簡易 UTM を宅配便で送付することの前提は、UTM 自体が小型で、軽量で、かつ頑丈であることである。こうあってこそ、安価かつ簡便な納入手法であるところの宅配便での輸送が可能となる。かかる物理的、品質的な特徴を前提に、本実証事業では実際に宅配便で 112 社に送付したが、故障、支障、不調などが一件もなく、交換も 0 件であった。宅配便による輸送という安価かつ簡便な納入方式が商用段階においても運用できそうであることを示している。

（ハ）簡易 UTM の設置は、どこが難しかったか

○「自社社員が設置（困難だった)」も回答社中 10 社 20%ある。平均で 77 分要しており、この低減が課題である。では具体的に、どういうところが難しかった、である。実際の意見としては以下のようなものが挙げられた。

表 41

・既設ケーブルの整理に時間を要した	・設置の位置が分からなかった
・簡易 UTM への固定ＩＰの設定	・無線ＬＡＮ設定
・アクティベーションが上手くいかなかった	・設置後にネットの作動が遅くなった

○「既設ケーブルの整理」というのは、中小企業が UTM をはじめとするセキュリティ機器を導入するうえでの“最初の第一歩”である。物理的に整理整頓できていないので論理的にも把握できておらず、ネットワーク構成図が作れない。この部分は中小企業が“意識はあるけど行動を起こせない”要因となっていると考えられる。

○本実証事業で、お助け実働隊に設置依頼をした理由として「設置の方法が分からないから」というよりは「設置の位置が分からないから」という企業が多かった。「相談窓口」での相談も、参加企業の回線環境の確認に多くの時間が費やされた。これは一義的には参加企業側の問題であり、サプライヤー側としてはいかんともし難い問題ではあるが、さりとてそれが中小企業の現実である以上、この部分のフォローもサービスの重要なパートと位置付ける必要性があるといえよう。

○簡易 UTM 設置のハードルとなると考えられる典型的ケースは下記３つである。しかし、本当の意味でのハードルは、下記のごとき個別設定を難しいと回答した企業の数や率の高さではなく、下記の設問への回答率の低さである。66 社の回答企業のうち無線 LAN を運用している企業も固定 IP の企業も、もっと多くあるはずである。察するに、設問の意味を理解せずに回答している（もしくは確認をせず無回答）ため、下記表では絶対数も割合も小さい数値になっていると考えられる。

表 42

プロキシ設定	1 社
固定ＩＰアドレス設定	9 社（n=66 14%）
無線ＬＡＮ設定	11 社（n=64 17%）
アンケート回答社（66 社）の中でこの質問に無回答（上記３つに該当がない、ということを意味するものではなかろう）	45 社

○実際、固定 IP か DHCP かを把握していないケースも少なくなかった。お助け実働隊が参加企業へのヒアリングに基づき DHCP を前提に作業を進めていっても UTM がアクティベイトしない（IP を受け取れない)。この場合の業務フローとし

てはUTM自体の瑕疵を疑い、交換を検討することになる。ところが長時間の悪戦苦闘の末、参加企業側から「こんなものが出てきたのですが」といって固定IP表が手渡された。またPPPoEの終端が判然とせず苦戦することもあった。

（ニ）お助け実働隊の対応は、良かったか（該当企業のみ）

○（UTM設置支援と所定サイバーインシデント駆け付けを区分せずに聞いているものであるが）大阪商工会議所の契約事業者ということで一定の信用があるものの“全く知らないIT事業者”が自社の機密部分であるネットワークを触りに初訪問したことに対する印象としては、概ね良好であった。

表43

お助け実働隊の対応は良かったか	最終アンケ n=回答者 26	備考
はい	25 (回答者中96%)	丁寧（親切・誠実）だった…… 3 分かり易かった（的確・しっかり）…… 4 敏速だった（すぐ対応してもらえた）… 6 課題が解決した（最後まで対応してくれた）…1 役立つ情報を得た…… 1
いいえ	1 (回答者中 4%)	「複数のPCを調べていたが具体的に何をしたのか説明が無かった」

（ホ）お助け実働隊自身は、UTM設置支援をどう感じたか

○ネットワークやサイバーセキュリティの専門家ではあるものの、UTM 設置それ自体を専業として実施しているわけではなく、かつ訪問先参加企業とは面識がなく、ネットワーク環境を把握しているわけでもなく、ネットワーク構成図も殆どなく、さらには参加企業側担当者とも会話があまり噛み合わない中、暗中模索で実施したお助け実働隊の声は下記のとおりである。

表44

簡易UTMの設置場所はすぐ分かったか		
はい	27件（84%）	・サーバーでPPPoEが終端
いいえ（最終的には分かったが）	5件（16%）	・NW構成図が無かった

表45

簡易UTMの設置は容易だったか		
非常に容易だった	10件（31%）	・配線切替えとボタン1つで設置完了できた ・無線ＬＡＮの接続機器把握に時間を要した ・ＯＮＵ、ルーター付近に近づけない
やや容易だった	12件（38%）	
あまり容易ではなかった	5件（16%）	
容易ではなかった	5件（16%）	

（５）所定サイバーインシデント駆け付け・初動対処

①所定サイバーインシデントの基準づくり（サイバーリスクに関する保険との連動）

（イ）所定サイバーインシデントの定義

○保険が相互扶助の精神に基づくものである以上、損害を受けた特定の被保険者に支払われる保険金総額が、保険加入者から広く薄く集めてきた保険料総額を上回るようでは保険として成り立たなくなる。よって、保険組成には、保険料額、加入者数、保険発動事由発生確率、保険金額などを同時に考慮する必要がある。

○本実証事業の目的の一つは、既存のサイバーリスクに関する保険とは異なる新たな簡易的な保険、即ち高額な費用や賠償損害より気軽に利用できる費用損害に焦点を当てた少額の保険の構築である。保険対象については、本実証事業が「事前対応」より「事後対応」に主眼を置く関係上、インシデント時における初動対処の費用を候補とした。次に、初動対処も色々な形態があるが、中小企業に寄り添う観点から、「駆け付け」が京阪神の中小企業のニーズに合致するだろう、との仮説を立て、この実証を行うこととした。

○「駆け付け」のニーズは高いと思われるが、お金も時間も労力もかかる。よって、本当に「駆け付け」が必要なのか否かを事前判定し“空振り”を最小限化するめに簡易 UTM の観測・検知機能を最大限に用いるとともに、「相談窓口」による事後対応支援を前置させる必要がある。これらで解決できなかった場合のみ、保険発動対象としての「所定サイバーインシデント」として認定される仕組みとした。

（ロ）所定サイバーインシデントの「所定」の定義

○「被害」の「実害化」を防ぐことがキーワード。マルウエア侵入（被害）を前提に考え、簡易 UTM が「外→内」の侵入を防御（事前対応）する。問題は簡易 UTM 設置前から潜んでいたマルウエアや、設置後に侵入したマルウエア。かかるマルウエアが C&C サーバーと交信し情報を窃取する際の当該「内→外」の通信こそが「実害」。当該通信も簡易 UTM は遮断するものの、マルウエアの存在を放置するわけにはいかないので、「相談窓口」の支援に基づき、先ず参加企業自身がウイルス対策ソフトでスキャンし隔離・駆除を行うが、それを行えない場合や、行ったけど“気持ち悪いと感じる”場合、感染範囲が気になる場合、ウイルス対策ソフトが最新の定義ファイルにアップデートされているか否か自信がない場合などは「所定サイバーインシデント」として「駆け付け」対象とし、当該「駆け付け」に係るお助け実働隊の出動費用を簡易的な保険により補償することとした。

②お助け実働隊による駆け付け・初動対処の実施結果とその考察【事例紹介含む】

（イ）お助け実働隊による駆け付け・初動対処の実施実例

表 46

	①A社	②B社
UTM 検知機能	IPS	IPS
アラート概要	マルウエア（リモートアクセス型トロイの木馬（RAT））感染疑いのある通信	Cisco ASA の脆弱性に対する攻撃の疑いがある通信
アラート発生	8 月 29 日【UTM 設置 39 日後】	9 月 13 日【UTM 設置 8 日後】
駆け付け日時	8 月 30 日 【1 日後に駆け付け】	10 月 8 日【25 日後に駆け付け】
現認発生事象	・再現性なし ・他機器での発生なし	・再現性なし ・他機器での発生なし
対処概要	・ウイルス対策ソフトのバージョンを確認し、通信元の PC と通信先の PC のウイルススキャン実施 ・事前にユーザーによるウイルススキャンで検出していなかったため他社ウイルス対策ソフトでスキャン実施	・ウイルス対策ソフトのバージョンを確認し、通信元の PC と通信先の PC のウイルススキャン実施 ・事前にユーザーによるウイルススキャンで何も検出していなかったため、他社ウイルス対策ソフトでスキャンを実施
対処結果	ウイルス検出なし【過検知】	ウイルス検出なし【過検知】
検出マルウエア	―	―
対処時間	200 分	300 分
保険対象適否	否	否

表 47

	③C社	④D社
UTM 検知機能	IPS	IPS
アラート概要	admin などの類推されやすいパスワードを使用した BASIC 認証を試みる通信が、特定端末から定期的に発生	オンライン銀行詐欺ツール型マルウエア(UPATRE/DYRE) への感染の疑いがある通信を UTM で検知
アラート発生	9 月 27 日【UTM 設置 71 日後】	11 月 5 日【UTM 設置 20 日後】
駆け付け日時	9 月 27 日【当日に駆け付け】	11 月 8 日 【3 日後に駆け付け】 11 月 11 日
現認発生事象	・定期的に発生 ・他機器での発生なし	・再現性なし ・他機器での発生なし
対処概要	・不明プログラムのインストール状況確認 ・該当端末でのウイルススキャン実施 ・パケットキャプチャ実施	・UTM で検知した IP アドレスはルーターであったため、ルーター配下にある全PC でウイルススキャン実施
対処結果	・不明なプログラムのインストールなし ・ウイルス検出なし【過検知】	2 台の PC でウイルスを検出し駆除
検出マルウエア	―	・Win64/DriverReviver.A の亜種 ・Win32/Toolbar.Conduit.AR の亜種 ・Win32/Toolbar.Conduit.B の亜種
対処時間	80 分	215 分
保険対象適否	否	対象

表 48

	⑤E社	⑥F社
UTM 検知機能	IPS	アンチウイルス
アラート概要	インスタントメッセンジャーなどを介して個人情報などを搾取するマルウエア(Dorkbot)への感染の疑いがある通信を UTM で検知	メールに添付されたファイルにウイルスが含まれていることを UTM で検知
アラート発生	11 月 15 日【UTM 設置後 37 日】	12 月 17 日【UTM 設置後 149 日】
駆け付け日時	11 月 26 日【37 日後に駆け付け】	12 月 19 日【2 日後に駆け付け】
現認発生事象	・再現性なし ・他機器での発生なし	ウイルス対策ソフトでのスキャン結果 EMOTET を検知したことを確認
対処概要	(11 月 26 日) ・検知した端末の MAC アドレスと合致する PC が見つからないため、使用頻度の高い PC に対してウイルススキャン実施 ・Windows、ウイルス対策ソフトの最新化 (12 月 12 日) ・親族が経営する別会社端末がつながっていると連絡があり追加調査実施 ・端末の特定 ・Windows、AcrobatReader、ウイルス対策ソフトの最新化 ・被疑 SW(IobitUninstaller)のアンインストール ・ウイルススキャン実施	・感染ファイルを含むメールの駆除 ・他に有害なものが侵入していないか、プログラムフォルダ、タスクを確認 ・他 PC の点検を打診したが必要ないとの事で実施せず
対処結果	(11 月 26 日) ウイルス検出なし (12 月 12 日) 474 件のウイルスを検出し駆除	ウイルスを検出し駆除
検出マルウエア	(不明)	Ransom_HPLOCKY… JS_PAWXNIC.D Trojan.W97M.EMOTET… ADW_MYWEBSEA…
対処時間	210 分、225 分	90 分
保険対象適否	対象	対象

表 49

	⑦G社	⑧F社（⑥と同一社）
UTM 検知機能	IPS	IPS
アラート概要	マルウエア（Ghost rat）への感染の疑いがある通信を UTM で検知	マルウエア（Ghost rat）への感染の疑いがある通信を UTM で検知
アラート発生	12 月 27 日【UTM 設置後 16 日】	1 月 23 日【UTM 設置後 186 日】
駆け付け日時	12 月 27 日【当日に駆け付け】	1 月 23 日【当日に駆け付け】
現認発生事象	・再現性なし ・他機器での発生なし	・再現性なし ・他機器での発生なし
対処概要	・ネットワークからの切り離しを提案したが、システムを使用できないと困るということで、インターネットに接続できないよう DNS の設定を無効化 ・ウイルススキャン実施済みとのことであったが、パターンファイルを確認したところ 2016 年であった。パターンファイルをアップデートするとシステムが動かなくなる恐れがあるとのことで、アップデートは断念 ・以下を助言 ※HD を回収し、業者でウイルススキャンをすることは可能 ※Windows Update の実施、ウイルス対策ソフトの導入、有効化を強く推奨 ※個人 PC の社内 NW への接続しないこと ※USB の取り扱いを注意すること	・ネットワーク概要確認 ・対象 PC の用途、活用状況、インストールアプリケーションの確認 ・対象 PC のイベントログから、アラート発生時の起動アプリケーションを確認 ・送信先 IP を確認したところ、Google 関係の広告会社と思われる。 ・フルスキャンを再度(駆け付け前に顧客自身で実施し検出されず）。検出なし。
対処結果	ウイルス検出なし（2016 年のパターンファイルでのスキャン結果）	ウイルス検出なし【過検知】
検出マルウエア	―	―
対処時間	75 分	135 分
保険対象適否	対象	否

（参加企業側の駆け付け希望期限と本実証事業の駆け付け結果）

表 50

駆け付け希望期日	社数	本実証事業での実際の駆け付け実施までに要した日数
当日中	8 社	8 件中 3 件（38%）※最速で 3 時間半後
数日中	2 社	8 件中 3 件（38%）※1 日後 1 件、2 日後 1 件、3 日後 1 件
1 週間以内	1 社	
1 週間～	0 社	8 件中 2 件（25%）※11 日後 1 件、25 日後 1 件 主に参加企業側都合によりアポが決定

（ロ）お助け実働隊による駆け付け・初動対処に係る考察

○全体で 8 件（頭数 7 社）に対し計 10 回行った。うち 2 社は同一案件でそれぞれ 2 回ずつ駆け付け。1 社は別々の案件（AV、IPS）で同一企業に 2 回駆け付けた。

○8 件中 4 件が結果として保険対象となりうる案件である。他の 4 件はアラート発報段階では保険対象となりえるか否か微妙ではあったが、保険の適用条件などを見極めるため、また、お助け実働隊の駆け付け対処能力や作業内容を精査するためという政策的目的から駆け付けを適用した。

○過検知は 8 件中 4 件（50%：上記①、②、③、⑧）であり、簡易 UTM の精度向上が今後の課題である。これは「空振り」より「見逃し」を避けるという“安全寄り”の設計思想に基づいていること、人手を介さずに簡易 UTM が自動で判断する仕組みにしていることなどによるものである。(アクセス解析の通信の過検知等)

○8 件中 3 件（38%）で当日中にお助け実働隊の駆け付け実行。同 3 件が数日中に実行。約 7 割が数日中に実行できた。１週間以上かかっている事例は、緊急性が比較的低い案件や主に参加企業側の都合により、日数が経過したものである。このことから、お助け実働隊を主力とするサイバーセキュリティに係る地域支援体制構築という本実証事業の主要目的の一つは概ね実現できたものといえよう。

○所定インシデント駆け付けは、「当日中」を全て実現するのは困難であるものの、簡易 UTM が外部の悪性サイトとの通信を遮断していることもあり、現実的には数日以内の駆け付けを目標とすべきであろう。参加企業は総論としては「当日中」を望んでいる一方で、現実問題、当日中に駆け付けられて長時間立ち合う準備ができてない場合も少なくない。被疑端末を業務から速やかに外せないケースも少なくない。上記④の企業では、当日中に駆け付けたのものの、フルスキャンをすると夜遅くなってしまい、労務管理上、差し障りがあるため別日の再来を依頼された。この場合、お助け実働隊に支払う対価は１回分か２回分か、という問題が生じる。同企業に限らず、昨今の“働き方改革”や“生産性向上”の時流がオンサイトサポートの在り方にも少なからず影響を与えうる要素となりつつある。

○駆け付け先での初動対処に要した時間の平均は約 170 分。最短で 75 分、最長で 300 分。短時間で済んだケースは、インシデントの質、対応難易度という点などにおいて必ずしも低レベルであった為というわけではなく、対処のしようが無かった、対処を断られた、などによる場合も含まれている。一方で、長時間を要したケ

ースは、インシデントの原因や全体像がすぐには分からなかった、被疑端末が容易に特定できなかった、フルスキャンに長時間を要した、フルスキャン以前にウイルス対策ソフトの定義ファイルを先ず最新化する必要があった、などである。

○駆け付け先での初動対処は、インシデント内容や駆け付け先の環境等に大きく依存するので平均値（170 分）はあまり参考にすべきではない。しかし、本実証事業の駆け付け謝礼とした一律固定額 35,000 円は、内部で検討のうえ試行的に設定した時給 1 万円に照らせば概ね妥当な金額設定であったといえる。しかし、結果的に短時間で済んだ案件の“謝金のもらいすぎ”より、長時間かかった案件の“謝金の少なすぎ”の方が問題と捉えるなら、駆け付けの謝金（対価）は一定の最低保証額（固定額）に上乗せするかたちで時給制とする手法が望ましいだろう。

○お助け実働隊のスキルの格差も多少見られた。よって、どのお助け実働隊が駆け付けを行っても一律かつ同水準の作業ができるよう、作業の標準化が課題である。本実証事業で得られた知見をもとに、標準作業項目の再定義、現場チェックシート・実施報告書の改善などが必要である。

○2019 年 11 月頃から感染拡大がみられた「Emotet」に起因する駆け付けも 1 件発生（上記⑥）。本件は、メールのタイトル、添付されていたマクロ実行へ誘導するワードファイルなどの存在から、参加企業側で「Emotet」感染を認識しており、感染端末も明確であったことからスムーズに駆除作業が行われた。

○駆け付け先で簡易 UTM 検知の被疑端末（LAN 側 Mac アドレス）がどうしても見つからないという事例が 1 件あった（上記⑤）。後日、被疑端末が見つかったとの連絡があり再度駆け付けた。その端末は参加企業の資産ではなく、同参加企業の経営者の親族が経営する別法人（中小企業にはよくある話）の端末であった。同一 LAN 環境下にあり、簡易 UTM の監視対象に入っていた。本件については論点が 2 つある。一つ目は「シャドーIT（IoT 含む）」の問題。二つ目はユーザー企業所有端末以外の端末の問題。いずれも情報システム担当者が存在を把握していないような端末を商用化段階において保険対象（駆け付け対象）とするか否かという問題である。

○通常、保険には、告知義務等の“事前身体検査”があり、それと保険加入可否や保険料が連動している。シャドーIT や従業員等の個人所有端末をサービス上どう扱うかを早急に検討せねばならない。前者は、仮にシャドーであったとしても社

有である以上、保険対象にせざるを得ないが、後者は WiFi の普及などに鑑み、保険対象（駆け付け対象）にすると保険が破綻する可能性がある。業務フロー的にも複雑である。アラートを出すところまでは機械的に行われるが、アラートに記載された IP アドレスや Mac アドレスに基づき、先ずそれが社有物か私有物かの特定をし、前者であることを確認したうえでないと駆け付けができない。この確定作業をユーザー側が自力で出来るのかどうかという問題もある。DHCP 払出しの場合の該当 IP の端末特定も容易ではなかろうが、特定できた場合、個人所有端末のマルウエア感染は保険対象外とせざるを得ないだろう。

○ウイルス対策ソフトのバージョンが古かったので、お助け実働隊が最新の定義ファイルに更新しようとしたところ「製品管理システムが動かなくなっては困るので、更新しないでほしい」と言われたのでその意向に従い、更新せず、それゆえにマルウエア存否の確認もできないままクローズとせざるを得なかった例もある（上記⑦）。ある意味“中小企業によくあるケース”といえる。せめてもの初動対処として、当該 PC からインターネットに接続できないように DNS の設定を無効化した。

○ここで問題となるのが、サイバーセキュリティに係る意識・知識・対策が非常に低いレイヤーを商用化後のサービスの利用対象とすべきか否かという問題である。OS が古いまま（XP など）の場合や、ウイルス対策ソフトの更新が十分でない企業を顧客とした場合、駆け付け適用が多くなりすぎ（場合により、同じ企業に何度も駆け付けるケースも）、保険が破綻する可能性がある。政策的見地という意味ではボトムアップは必要であり支援対象（顧客対象）とすべきだが、商用化段階では事業のサステナビリティーも大切なことなので、一定の“事前身体検査”を行うか、行わないとすれば、それに代わるフィルターが必要となる。

○簡易 UTM 設置後、駆け付け案件が発生するまでの日数は、過検知 4 案件含む全 8 件ベースでは、平均値 66 日、中央値 38 日であり、最短 16 日、最長 186 日である。過検知案件を除く（結果的）保険対象案件だけで見ると、平均値 55 日、中央値 29 日であり、最短 16 日、最長 149 日である。これはサイバー攻撃の動向や実証実施前に潜んでいたマルウエア等の動き方などを推定するうえで有用なデータといえるが、保険設計とりわけ免責の内容や期間を決定するうえでも無視できない重要なデータである。

○商用化後のサービスの実施目的は、広く様々なレベルの中小企業の支援を行い、サ

プライチェーンを守る、というものである。かかる政策的意義からも、採算性が担保できる範囲内で“事前身体検査”の如きをサービス利用の条件として課さず、門戸を全方位的に開きたいところである。一方で、どの会社でも利用可能とする代わりに、先述の★★★メールを送信した場合、直ちに駆け付け適用とするのではなく、先ずユーザー企業にてフルスキャンをしてもらい、マルウエア検知がなかった場合（過検知）や、自力で駆除できた場合は駆け付け（保険）適用外とするなどのフィルタリング（“直前身体検査”）も必要となろう。しかし、隔離はできても駆除までは出来ないケースなどは、やはり駆け付け（保険）適用が相当といえよう。

（ハ）参加企業側は、所定サイバーインシデント駆け付け・初動対処をどう感じたか

○注目すべきは、参加企業はインシデントの症状にも予兆にも気付いていないケースが殆どであった点。「なんですかそれ？ホンマでっか？」という反応が多かった。

○上記８件の駆け付け先企業のうち１社（上記④）のみ「最近なんとなく PC の調子がおかしい」ことを理由に本実証事業に参加したが、実際にマルウエアが侵入しており、駆け付け対象案件にまで悪化していた事実には気付いていなかったという。それでも「最近、なんとなくおかしい」という気付きがあったことだけでも良い方であり、早期発見、早期解決につながり、被害が最小限で留められた。これはむしろ例外的ケースであり、最近のサイバーインシデントは足音無く侵入し、長期間の潜伏期間を経て、バックドアなどをしかけることが特徴であるため、「なんですか、それ？ホンマでっか？」の反応の中にこそ、簡易 UTM の効果と本実証事業の意義が見い出せた、といっても過言ではなかろう。「なんとなくおかしい」というのは、中小企業の気付きとしては看過できないものであり、サイバーセキュリティの潜在的需要もこうした「なんとなくおかしい」の中に存しているのかもしれない。

○参加企業側の感想は下記のとおり　表 51

・素早く対応して頂けた
・（過検知ではあったが）問題の可能性のある部分についてきちんと確認してもらえたので、ＨＵＢのスペックについて問題があることが分かった
・分かり易く話してくれて相談しやすかった
・問題があるＰＣを確定し対応できた
・トロイの木馬を発見し駆除することが出来た
・今までマルウエアが作動していても全く判らないという状況が改善された
・お助け実働隊にすぐ連絡を取り、最短で対処することが出来た
・急な依頼であったのにその日のうちに駆け付けて対応して頂けた

（ニ）お助け実働隊自身は、所定サイバーインシデント駆け付け・初動対処をどう感じたか

○お助け実働隊は初動対処を概ね遂行することはできたと自己認識している。

表52

事象が発生しているＰＣを特定できたか	
特定できた	4 件（66%）
特定できなかった（結果的には特定できた）	2 件（33%）

表53

現場での発生事象の把握・対処方法の特定はできたか		
全て（殆ど）のケースで発生事象把握と対処方法特定ができた	2	・事象発生時に被疑端末を操作していた人物は帰宅しており詳細は聞けなかったが、端末のログをもとに事象を把握し、対処方法を特定することができた。 ・検出エンジンの情報が足りない。 ・誤検知と判断できるまでの時間がかかった。
多くのケースで発生事象の把握と対処方法の特定ができたが、一部のケースで容易に把握・特定できなかった	1	
多くのケースで発生事象把握と対処方法特定が容易にできず、一部のケースで容易に把握・特定できた	1	
全て（殆ど）のケースで発生事象把握と対処方法特定ができなかった	1	

表54

参加企業は駆け付け・初動対処の趣旨・内容・結果を理解したと思うか		
全て（殆ど）のユーザーは初動対処の趣旨・内容・結果を理解したと思われる	3	・中小企業の担当者はＩＴ知識が高くないケースが多い。平易な言葉で伝えることを意識して取り組んだ。 ・訪問前に電話にて事前説明を行い、現地でのヒアリングと趣旨説明をすることで問題なく理解いただけた。 ・UTM の動作を理解しきれていない
多くのユーザーは初動対処の趣旨・内容・結果を理解したと思われるが、一部のユーザーは理解していないと思われる	2	
多くのユーザーは初動対処の趣旨・内容・結果を理解していないと思われるが、一部のユーザーは理解したと思われる	0	
全て（殆ど）のユーザーは初動対処の趣旨・内容・結果を理解していないと思われる	0	

表55

初動対処の結果を教えて下さい		
全て（殆ど）のケースで相談窓口や仕様書の指示通りの初動対処（マルウエアの有無にかかわらず）ができた	2	・駆け付けた時には担当者が対策の一部を既に実施していたため、仕様書の内容を少し変更して初動対処を行った。 ・被疑端末以外の端末のチェックを打診したところ業務に支障が出るとのことで断られた。
多くのケースで相談窓口や仕様書の指示通りの初動対処（マルウエアの有無にかかわらず）ができたが、一部のケースではできなかった（適切ではなかったのでしなかった場合を含む）	1	
多くのケースで相談窓口や仕様書の指示通りの初動対処（マルウエアの有無にかかわらず）ができなかったが（適切ではなかったのでしなかった場合を含む）、一部のケースではできた	1	
全て（殆ど）のケースで、相談窓口や仕様書の指示通りの初動対処（マルウエアの有無にかかわらず）ができなかった	1	

（6）マス・メディアでの報道状況

下記のとおりマス・メディアによる報道があった（把握できているもののみ）ほか、ネットニュース等でもいくつか紹介された。

表 56

事業開始時（7 月 3 日プレス発表）	事業実施中
○新聞 ・日本経済新聞…7 月 4 日 ・産経新聞……7 月 4 日 ・大阪日日新聞…7 月 5 日 ・日刊工業新聞…7 月 17 日 ・日経産業新聞…8 月 21 日 ○テレビ ・ＮＨＫ……7 月 8 日（ニュース）	○新聞 ・日本経済新聞…9 月 26 日（特集） ○テレビ ・ＮＨＫ……11 月 15 日（「かんさい熱視線」30 分番組のうちの 10 分程度） ・ＮＨＫ……11 月 27 日（「おはよう日本」特集として＜全国放送＞） ※IPA の紹介もあり

（7）実証事業の総括

○本実証事業を進めるにあたり、中小企業のセキュリティの実態を調査するだけでなく、サービス利用者にとって、セキュリティ対策の有力な手段となる機器の「導入の手軽さ」、「運用の手軽さ」を実現することを追求した。加えて、必要かつ十分なサービスを実現しつつ、利用しやすい価格を実現するための運用の効率化の試みも併せて行った。

○簡易 UTM の設置に関しては、設定をゼロにすることにより、約 7 割の企業で UTM を自力で設置できた。とはいえ、3 割は自力では設置できなかったというのも事実である。また、「ネットワークのどの箇所に設置すればよいかわからなかった」というアンケート結果から伺えるが、設置をできた企業においても、必ずしも適切な箇所に設置されていなかった可能性もある。たとえば、攻撃の検知がゼロである 26 社（23%）のうち、何社かが配下に端末がない箇所に簡易 UTM が設置されていた可能性が考えられる。こういった不適切な箇所に接続された UTM を検出できるような機能追加が必要である。

○本実証事業参加 112 社中 74 社（66%）で何らかの外部からの攻撃を検知し防御していたにも関わらず、その効果が利用者に十分に伝わっていなかった。攻撃の検知・防御状況は、ポータルサイトで確認できるようにはなっていたが、ポータルを参照したとしても、データの参照方法や、その意味するところが理解しづらかったものと考えられる。また、アラートの通知については、実証を通して通知レベルの調整を行い、通知自体は適切に行えるようになったと考えるが、通知文を見ただけでは、次のアクションをどうすればよいかがわからないという意見も多く、通知文や通知方法の見直しが必要である。

○準備したシステム（簡易 UTM、簡易 SOC）を使って 100 を超える拠点での実証を行うのは NEC にとっても今回が初めてであったが、中小企業のセキュリティ実態を表す様々なデータと、サービス提供者としての様々な知見を得ることができた。この知見については、商用化の実現に最大限に活用し、更なるサービス改善を行っていく。

○また、相談窓口での対応については、日頃から既存業務として IT のコールセンター業務を担うキューアンドエーにおいても、本実証事業ならではの特徴的な対応や固有の専門知識が必要なケースが少なくなく、商用化に向けての良き予行演習となった。

○簡易的な保険の検討については、8 件という本実証事業の「駆け付け」実施件数と最長でも 7 か月という実証期間は、保険発動要件やその基準、免責、保険料・保険金の額などを検討するうえで、ややサンプル数が少なく、商用化に向けた制度設計はなんとかできたものの、商用化後も引き続きデータや知見の収集を継続し、中期的に軌道修正を続けていかねばならないことと考えられる。

○本実証事業の機会を提供して下さった経済産業省、IPA および本実証事業にご協力いただいた参加企業、お助け実働隊地域 IT 事業者各位に対し、深く感謝の意を表したい。

６．実証結果をふまえた検討

（１）実証の成果

①本実施体制が得た成果（ここでは総括のみ。得られた知見等の詳細は上記各項目参照）

（イ）本実施体制の構築・信頼関係強化・商用化に向けた役割分担策定と利害調整を行えたこと

○本実証事業の応募検討から終了までの約１年間、本実施体制４者による打ち合わせを東京、大阪で数十回行い、実証と商用化に向けた信頼関係を強化できた。

○東京海上日動や NEC は、これまで地方都市の中小企業に直接リーチする機会が殆どなかったが、本実証事業により、現場の中小企業に直に接する機会を得、その課題解決に向けた気付きや知見を得ることができ、大阪商工会議所は非営利団体ゆえにこれまで殆ど経験したことのない民間ビジネスの商品開発プロセスに関与する機会を得、民間的発想に基づきサービスの販売を行ううえでの知見を多数得た。

（ロ）お助け実働隊を核とする地域支援体制を構築し、商用化段階でも概ね参加頂けそうな信頼関係の構築･法的関係の整理･業務フロー･仕様などの確立ができたこと

○実際の民民の関係性の中で、募集・商談・契約・受発注・役務提供・報告・請求・支払・検証など一連の業務フローを回し、商用化の基盤を築くことができた。

○本実証事業での委託契約先 11 者のうち少なくとも 9 者は商用化後も参加の意向を示しており、商用化サービスに早期に移行できる体制を整えることができた。

（ハ）実稼働中の様々な業種の京阪神中小企業 112 社への最新のサイバー攻撃を観測・考察したこと

○長いところで半年以上の通信監視により得られたログ情報は膨大なものであり、サイバー攻撃の最新トレンドを統計的に把握・分析することができた。

（ニ）京阪神中小企業のサイバーセキュリティ実施状況とニーズに係る情報を収集・考察したこと

○数回におよぶアンケート調査により、京阪神の中小企業におけるセキュリティ実施状況とニーズに係る大まかなベクトルを見い出すことができた。

○実地訪問ヒアリング、UTM 設置支援や所定サイバーインシデント駆け付けへの立ち合い、相談窓口に寄せられた質問や意見などにより、リアリティーに満ちた“現場の声”や、各社各様の“一筋縄ではいかない背景事情”を見聞することができた。

（ホ）簡易 UTM、簡易 SOC、相談窓口の現状と改善すべき点に係る情報を収集・考察したこと

○上記（ハ）（ニ）にて得られた情報をもとに、サービスを構成する各役務提供と簡

易 UTM につき、各論レベルで改善に係る議論を深耕させることができた。

（ヘ）簡易的な保険の組成と発動要件等の策定に必要となる情報を収集・考察したこと

○上記（ハ）（ニ）（ホ）にて得られた情報をもとに、中小企業に寄り添い、その意識と行動の変容を後押しする、これまで我が国に存在しなかった新たな簡易的な保険実現に向けた、エビデンス・ベイストの検討を行うことができたこと。

（ト）上記（イ）～（ヘ）を通じ、中小企業でも導入可能な安価・簡便なサイバーセキュリティお助けサービス（仮称）の商用化に向けた検討を行い、具体的な商用化案を策定できたこと

○「日本の中小企業ならびにサプライチェーンを守る」「サイバーセキュリティにより事業継続力と企業価値を高めることをお手伝いする」というビジョンを掲げ、「安価かつ簡便な」「パッケージ化されたサイバーセキュリティお助け隊サービス」構築という目標に向かって、商用化をふまえた実証を行い、随時軌道修正なども行ってきたため、実証終了後速やかに商用化に移行できる具体案の取りまとめと各組織内での意思決定を進めることができた。

②参加企業が得たと考えられる成果

（イ）本実証事業に参加して良かったと思う点

表 57

お助け隊実証に参加し良かった点	最終アンケ n=105 ※複数回答あり	備考
社員のサイバーセキュリティ意識・知識が向上した	(21%) 22	・IPA セキュリティアクション診断を受講し二つ星宣言準備中／情報セキュリティ５か条の周知 ・危機感を持つようになった／攻撃は常にあるという意識を徹底できた ・事象があって初めて社員に啓発することが出来た／セキュリティへの重要性が伝わった ・怪しいメールへの警戒感が高まった／必要事項以外は使用しないように徹底 ・勉強会を開催しレポートを作成した／セキュリティの勉強会のテーマとして UTM を紹介した ・役員を含め必要を感じるきっかけとなった ・第三者に評価してもらうことが良かった
自社へのサイバー攻撃動向が把握できた	(21%) 22	・アラート通知が実際にあり、他人事ではないとの意識につながった ・アラート通知にて動向が確認できた／メール通知での把握ができた ・規模に関係なく何らかの攻撃があると分かった／攻撃があるらしいと大雑把には分かった ・攻撃内容が解った／攻撃の有無実態を把握できるようになった ・重篤なマルウエア感染は自社では把握することが出来なかったと思う ・サイバー攻撃は無かったことが分かった（３）
自社のサイバーセキュリティやネットワーク環境を把握・改善することができた	(18%) 19	・UTM を含む新ネットワークを構築中 ・ウイルス対策ソフトの無い PC にウイルス対策ソフトをインストールした ・ネットワーク設定の問題点の把握ができた／問題があるＰＣを確定し対応できた ・マニュアル作成中 ・メインＨＵＢのスペックに問題があることが分かった（交換予定）
自社へのサイバー攻撃・情報流出等が防げた	(17%) 18	・トロイの木馬を発見し駆除することが出来た／メール攻撃が無くなった ・不正アクセスを防いだ形跡があった／不正アクセスに対するアラートを受信 ・外部からのポートスキャン等を見つけることが出来た ・週１回程度何らかの攻撃が有ることが分かった ・セキュリティソフト未検知案件も UTM で防止できた ・今までマルウエアが作動していても全く判らないという状況が改善された
自社の社会的信用が向上した	(6%) 6	・実証を機に SECURITY ACTION に登録 ・自社がこのような対策を行っていることを HP 更新や名刺更新時にアピールする予定 ・小企業で対策を行っていることを評価されている
その他	(22%) 23	・UTM の機能とセキュリティ対策の理解ができた（２）／導入しても業務に支障がないと感じた ・ＵＴＭ導入のきっかけになった／UTM を検討していたので情報となった ・安心感があった（３）／何かあったとしても気付くことが出来る安心感を得られた ・サイバー攻撃の内容を把握することができた／サイバー攻撃を意識するようになった ・「脆弱性を検知した」ということでパスワードを見直すきっかけになった ・セキュリティ情報の取得に時間がさけないので重要な情報をもらえるので助かった ・他社からのセキュリティ状況の問合せで「UTM 入れてます」といえたこと ・色々なサイバー犯罪等から守る物が有るのだなと再確認した ・「Emotet」をいち早くメールにて知ることができた 【否定的評価】 ・メリット、効果が分からない（実感できない）（４）／攻撃は無かった
良かったと思う点は無い	(17%) 18	・効果があったかどうかはよく分からなかった、見えない（６） ・具体的な問題が発生しなかった（３） ・アンチウイルス対策ソフトで十分（２） ・サムライファクトリーを誤検知／誤検知が何度かあり調査に複数の人員を使い、結果、何とも無かった ・ネット環境が不備になったため実証途中で取り外した ・良かったところもあったのではないかと思うが内容の理解不足で実感できなかった

○「自社へのサイバー攻撃・情報流出等が防げた」は 17%とやや少ない。簡易 UTM ならではの「お守り」「見守り」の効果実感が乏しい表れであろう。簡易 UTM により守られていたがために「攻撃→被害→実害」のプロセスが見えなくなってしまい、攻撃や防御の実態に対し、逆に警戒心が低下してしまったのかもしれない。

○「自社のサイバーセキュリティやネットワーク環境を把握・改善することができた」は 18%と比較的多く、成果の一つである。簡易 UTM を自力で能動的に設置したことを通じて、又はお助け実働隊による設置支援の際に間近で見たり説明を受けたりすることを通じて、自社のネットワーク環境を改めて把握したり、改善する機会となったことによるものと考えられる。

○「自社へのサイバー攻撃動向が把握できた」は 21%あり、「サイバー攻撃の見える化（把握）」という本実証事業の主要目的の一つは概ね達成できたといえるが、もう少し多くあってほしかった。アラート通知メール（「内→外」の悪性通信等のお知らせ）、参加企業閲覧用サービスポータル（3 か月分のログ情報や他社比較）に加え、11 月分より月次レポート（「外→内」の攻撃。ポートスキャン含む）を開始したが、もう少し早く始めていれば更に効果実感が高まったものと考えられる。

○「その他」が 22%と一番多いのが特徴である。肯定的意見と否定的意見が混在しており、前者のほうが多いものの「効果が目に見えるかたちで実感できない」という意見に集約できる。これは、簡易 UTM が守ってくれた結果なのか、実際に攻撃自体が無く簡易 UTM の意味がそもそも無かったのか、参加企業自身よく解らない、という意味であろう。このレイヤーへの訴求が商用化の成否を分けるといっても過言ではなく、効果実感のアピールが課題である。

○「良かったと思う点はない」も 17%もあり大変残念である。理由は上記とほぼ同じく「効果が目に見えるかたちで実感できない」「よく分からない」が多く、過検知に対する不満も挙げられている。アンチウイルスソフトで十分との声もある。セキュリティ意識が高い企業による「期待外れ」との評価と、意識が低い企業による関心の無さに由来する低い評価が混在している点が特徴である。

○「自社の社会的信用が向上した」も 6%あり、数は少ないものの、参加を機に SECURITY ACTION 宣言をした企業、他社との間で本実証事業や簡易 UTM のことが話題に上るなどして実証への参加を評価されたケースなどもあった。

（ロ）アラート通知メール記載の対処の実施

表 58

アラート通知メール記載の対処は実施したか	最終アンケ n=105	備考
はい	（全体の34%） 35	・被疑端末のウイルス対策ソフトによるスキャン・・・・・・・・・・・・・・9 ・被疑端末のウイルス対策ソフトによるスキャン（ウイルス検出されず）・・1 ・被疑端末のウイルス対策ソフトによるスキャン（ウイルス検出され駆除）・2 ・ウイルス対策ソフトの被疑端末への導入とスキャン（ウイルス検出され駆除）・・1 ・ＯＳのクリアインストール・・・・・・・・・・・・・・・・・・・・・・・・1 ・被疑端末に入っていた問題のソフトの特定と削除・・・・・・・・・・・・・1 ・セキュリティソフトのアップデート・・・・・・・・・・・・・・・・・・・2 ・Windows アップデート・・・・・・・・・・・・・・・・・・・・・・・・・1 ・ブラウザアップデート・・・・・・・・・・・・・・・・・・・・・・・・・1 ・お助け実働隊に駆け付けてもらい最短で対処出来た・・・・・・・・・・・・1 ・攻撃してきたとされるサイトの調査・・・・・・・・・・・・・・・・・・・1 ・調査を行い対応が必要かどうかを切り分け・・・・・・・・・・・・・・・・1 ・接続の確認・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・2 ・パスワード変更・・・・・・・・・・・・・・・・・・・・・・・・・・・・1 ・相談窓口に相談・確認・・・・・・・・・・・・・・・・・・・・・・・・・7
いいえ	（全体の24%） 25	【対処の必要性が分からない（ない）ため】・・・・・・・・・・・・・・１１ ・具体的被害が確認されなかった、大問題ではなかった、危険度 LOW だから（3） ・通知メールの内容だけでは本当に対処が必要なのか判断がつかなかったため（2） ・相談窓口から対応の必要がないとの回答があったため（2） ・原因が明らかなため（UTM オフライン、こちらの接続ミスなど）（2） ・既に対策済みであり新たに対処する必要がないと判断したため ・ＵＴＭで外部からのアクセスを遮断できているため 【対処の方法が分からない（対処のしようがない）ため】・・・・・・・8 ・何をすればよいか分からない・対処方法がよく分からない（中間４、最終２） ・「不審通信をブロックしました」と書かれているが対処のしようがないので困った 【過検知・誤検知だったため】・・・・・・・・・・・・・・・・・・・・・・5 ・Windows Update の処理がアラートとして検知されたため ・アラート自体がミス発信だったため ・社内ネットワーク調査作業時の操作がアラート通知されたため ・忍者ツールズを CrossSiteScript と過検知した為　（中間２） 【記載内容自体が理解できないため】・・・・・・・・・・・・・・・・・・4 ・アラート内容の意味がよく分からない（中間３、最終１）

○能動的、具体的な改善を実践した企業は 34%とあまり多くない。実施しない理由は、リテラシーにより異なっているが、大別すると以下のとおり。(a)「アラートの意味が分からない（言葉レベルで）」、(b)「何をどうすればいいか分からない（具体的対処法の記載が不十分）」、(c)「対処する意味が分からない・無い（過検知である、原因が明白で対処の必要性がない）」。（a）（b）は、実証事業途中で記載内容を具体化する改善をしたが依然として改善の余地は残っている。対処実施組に多いのはアンチウイルスソフトによるスキャンなどであり、実際にマルウエアを駆除したケースもあり、本実証事業の付随的効果の一つといえる。

（ハ）成果の代表的ケース

表 59

会社	実証の効果
A 社 大阪府大阪市 建設業	①アラート通知が実際にあり、他人事ではないとの意識につながった。 ②月次レポートについては、脅威の大まかな内容が分かった。（アラートだけだとよく分からないことも多いため） ※漠然とどこかの UTM 等を勧められることに比べれば、事業意図や対応内容がはっきりしており、事業の信用度が高いので有料化後も利用を前向きに検討する。
B 社 大阪府大阪市 サービス業	①UTM がウイルス検知したとのアラートメールに基づき、ウイルス対策ソフトでフルスキャン実施。ウイルスを駆除した。 ②社員向けに勉強会を開催しレポートを作成した。 ※セキュリティレベル向上のため有料化後もサービス利用を検討したい。
C 社 大阪府大阪市 サービス業	①これまではアンチウイルスソフトのみだったが、UTM 設置により、「通信の見える化」ができ、安心感があった。 ②取引先の大手電機メーカーから毎年セキュリティ関係のヒアリングがあるが、今年は「UTM 設置」と堂々と回答できる。
D 社 大阪府箕面市 製造業	①「駆け付け」の結果、社員の WiFi 利用（接続）のリスクを認識。 社長と相談し、これらを分離することにした。 ②本実証事業を通じて大商から情報提供を受けた「IPA　中小企業の情報セキュリティマネジメント指導業務」に申し込み、支援（研修）を受けることに。これにより、情報セキュリティ診断等による潜在的リスクの洗い出し、診断結果から重点領域を可視化した対策の決定、基本方針の策定を行うことができ、「Do」のフェイズに進むことができた。
E 社 大阪府茨木市 サービス業	①UTM でウイルスが検知され、相談窓口に相談した結果、駆け付けをして頂いた。急な依頼であったのにその日のうちに駆け付けて対応頂き、ウイルスを検出・駆除してもらえた。 ②重篤なマルウエア感染は自社では把握することが出来なかったと思う。 ③メールでも非常に丁寧かつ役立つ情報を頂くことができた。
F 社 大阪府豊中市 製造業	①かつて標的型攻撃メール／ビジネスメール詐欺などを受けたことがあるが、実証期間中はサイバー被害がなかった。 ②お助け隊実証を機に、SECURITY ACTION１つ星を宣言。社員に情報セキュリティ５か条の周知をしている。現在、２つ星宣言に向けてマニュアルを作成中。 ※相談窓口にも的確な対応を頂いたので、有料化後も利用したい。
G 社 兵庫県明石市 サービス業	①セキュリティの勉強会のテーマとして UTM を紹介できた。
H 社 京都府京田辺市 製造業	①ネットワークの問題点が把握できた。 ※価格が安価なので利用を検討したい。

（ニ）実証に参加しての満足度

表 60

お助け隊実証に満足しましたか	最終アンケ n=105	備考	
はい	（53%）56	【攻撃を防御してくれた】 ・脆弱性を検知し防いでもらえた／ウイルス攻撃を防げた（２）／実際に不審な通信を検知しブロックできた ・アラートが来るので防御出来ていることが実感できた ・重篤なマルウエア感染に際し早急なアラートがあり対応できたため	【対応が良かった】 ・相談窓口の対応が丁寧、的確、敏速（５） ・Emotet が弊社に届いた時の対応がベンダー企業とは比べものにならないくらい早かった ・ベンダーにお願いすると対応の観点が“商売”に根差してしまうが、実証ではそこが感じられなかった
		【攻撃の実態が分かった】 ・現状や実際の発生事案を把握することができた（３） ・現状、自社セキュリティに大きな問題が無いことが分かった／重篤なサイバー攻撃が今のところないことを確認できた ・サイバー攻撃を受けているのが分かった／自社への攻撃が視覚化され初めて確認できた／WiFi 接続しているスマホの通信に対し脅威を検出する時があった／導入前には見えていなかった脅威が見つかった	【便利だった】 ・ＵＴＭの設置のみでサービスを利用できる点が良かった ・ログが見やすかった 【UTMを知った・UTM導入のきっかけになった】 ・ＵＴＭを実証で試しに導入することができた／UTM を知るきっかけになった／UTM の扱い方が分かった ・元々UTM を設置していたが設置のみでカスタマイズ対応していなかった
		【安心感があった】 ・UTM 設置で安心感が得られた（４） ・アラート等はなかったが一連のサポート体制の優位性には満足 ・今回インシデントは無かったが監視してもらえる環境は心強い ・不審な動きがあれば連絡下さる安心感 ・有事の際に電話、メール相談、駆け付けしてもらえる安心感（３） ・ポータルサイトでチェックできるサポートの安心感 ・大商が中心に展開されている安心感	【意識・知識が高まった】 ・社員の知識・意識向上、最新セキュリティ情報入手（５） ・セキュリティに関して知らないことが多くあったことに気付いた ・講習会での学びも良かった ・流行情報の展開が有効だった 【改善につながった】 ・これを機会に社員でネットワークの使い方を見直しました ・セキュリティレベルの向上 【対外的信用の向上につながる】 ・取引先からの情報セキュリティ調査にもよい回答ができる ・信用力の向上に寄与
いいえ	（5%）5	・誤報が何度かあり、詳細調査に多数の人員を使い、結果、何とも無かった ・実感がない ・ネット環境が不備になったため実証途中で取り外した／ネット接続が切れるのであまり使えなかった／期間が短くほぼ利用できなかった	
どちらともいえない	（40%）42	【効果が分からなかった】 ・効果が有った（守られている）のか無かったのか分からない、見えない、判断できない、実感がない（１４）	【サポート体制が良くなかった、内容が理解できなかった】 ・管理サイトの情報が分かりづらい ・攻撃や初動対処法などが、頂いた案内では分からなかった。 ・ＵＴＭの内容をよく理解できておらず満足感が分からない（２）
		【攻撃、被害、問題がなかった】 ・サイバー攻撃、被害、問題がなかった（不明である）ので実感がない（７） ・どの程度リスクがあったか実感できない（２）	【ネット環境等への悪影響があった】 ・ＰＣが使用不能になるときがあった／ネットスピード遅延 【その他】 ・継続を検討しているが費用によっては他社を選定する可能性あり ・各種情報をデータ出力出来ないのが残念 ・ネットワーク不具合で参加の時間が短く判断しかねる（２）
		【過検知・誤検知が多かった】 ・アラート通知はあったが対象 PC フルスキャン実施のみで結果が分からなかった ・誤検知、過検知があった（２）	
（無回答）	（2%）2		

（ホ）簡易 UTM による防御

○上記（イ）のとおり、「自社へのサイバー攻撃・情報流出等が防げた」という主観レベルの効果はさほど高くはなかったが、ＩＰＳやアンチウイルスの機能により、外部 C&C サーバーとの悪性通信をブロックし、情報流出等がブロックされた企業が 88 社（約２万件）あった。（詳細は先述）

（ヘ）お助け実働隊による所定サイバーインシデント駆け付け・初動対処

○過検知を除く少なくとも３社、駆け付けを行い、マルウエアの駆除を行うことで被害の実害化を防いだ。（詳細は先述）

○付随的効果として、お助け実働隊による駆け付けを受け、社員の意識変容が見られた企業もあった。

③お助け実働隊が得たと考えられる成果

（イ）地域におけるサイバーセキュリティ産業（とりわけ中小の）の振興

○京阪神を含め地方ではサイバーセキュリティのマーケットが未成熟であり、産業としても十分育っていない。中小のサイバーセキュリティ事業者や情報処理安全確保支援士は“活躍の場”が少ないため、スキルや実績も向上しにくい。

○こうした状況をふまえ、本実証事業では、極めて限定的とはいえ、大阪商工会議所が 11 者の地域 IT 事業者と請負契約を締結し、本実証事業の実施それ自体が“需要開拓型”の試みとなるような事業スキームにて実施した。また経済産業省・IPA の当意即妙な命名による「サイバーセキュリティお助け隊」という、分かり易く親しみのあるネーミングを付与することでモチベーションを高めて頂くアレンジとした。

○その結果、頭数 10 者のお助け実働隊に対し、のべ 37 件（35 社）の簡易 UTM 設置支援、のべ 8 件（10 回）の所定サイバーインシデント駆け付けの発注を行うこととなった。お助け実働隊の各地域 IT 事業者にとっては、京阪神エリアにおける新しいサイバーセキュリティ地域支援体制の構築とその商用化への実証という公共目的にご協力頂くことを通じて、中長期的には各事業者のスキルアップ、ネットワーク構築、潜在的顧客との接点獲得、売上向上などの点で一定の収穫を得て頂くことができたものと思われる。それは 10 者のうち 9 者が商用化後もお助け実働隊として参加する意向を示していることからも読み取れる。

④関係者以外に及んだと考えられる成果

（イ）事業説明会によるもの

○第１回、第２回、第３回の事業説明会の受講者は、参加企業より非参加企業の方が多かった。これら参加企業以外の企業にも、本実証事業の実施を機に、「サイバーセキュリティお助け隊」実証の途中経過や最終結果を含むサイバーセキュリティ最新動向の情報収集、意識啓発、講師との交流などの機会が得られた。これは本実証事業の付随効果、波及効果といえよう。

表 61

	第１回（事業案内）	第２回（中間報告）	第３回（成果報告）
参加企業以外	**35 社（51%）**	**101 社（87%）**	**55 社（70%）**
参加企業	34 社	15 社	24 社

○参加企業以外の事業説明会のアンケート回答は以下のようなもの。

表 62

	第１回（事業案内）	第２回（中間報告）	第３回（成果報告）
とても役に立った	12 社	50 社	24 社
やや役に立った	11 社	33 社	19 社
第２回	・IPA の「5 分でできるポイント学習での社員教育」を利用してみたい（大阪府：卸売業） ・中小企業だからこそやらなければならないことがあると感じた（大阪府：卸売業） ・何より大切なことはセキュリティ意識を持つこと（大阪府：製造業） ・攻撃されているのに気づかないということが怖くなった。対策を見直したい（大阪府：サービス業） ・今回、役員を連れてきてよかった（大阪府：製造業） ・思った以上に深刻な状況であることが分かった。簡単な対策でも大切だと思った（大阪府：製造業） ・社員教育の必要性を理解できた（兵庫県：サービス業）		
第３回	・個人情報保護運用のヒントになった（大阪府：サービス業） ・初動の対策を講じたい（大阪府：建設業） ・セキュリティの考え方として本質的に何が大切か理解できた（大阪府：サービス業） ・攻撃者の考えを知ることは守る側の対策に役立つ（大阪府：サービス業） ・トップマネジメントの判断の必要性が分かった（大阪府：製造業） ・カードの有効期限や出生地等の今まで見落としていたことを知ることができた（奈良県：通信業）		

（ロ）マス・メディアの報道によるもの

○本実証事業については、新聞やテレビでも複数回取り上げられたことから、これらを見た少なからぬ中小企業において、本実証事業はもとより、中小企業におけるサイバー攻撃の深刻さやセキュリティの必要性などにつき幾分かの関心は高まったものと考えられる。ＮＨＫ報道を見て本実証事業やその商用化サービスの予定内容について電話等で問い合わせをしてきた中小企業が数社あった。

（２）実証結果をふまえた中小企業が利用しやすいサービスの商用化案

①商用化サービスの必要性・趣旨、本実施体制の存在理由、目指すべきサービスの概要・特徴

（イ）参加企業の生の声をふまえて

表 63

商用化サービスを利用するか	最終アンケ n=105	備考	
利用したい	(11%) 12	【金額面】 ・非常に安価で利用しやすいと感じた／費用がそこまで高額でない ・これまで費用面で断念してきたが本サービスは金額的に採用可 【必要性がある】 ・実際に週１回程度ではあるが攻撃を防げているため ・今回の実証において UTM で検知したアクセスがあった為 ・現状、弊社でセキュリティ被害にあった場合、社内対応が不可能 ・一瞬で信用を失うこと、対応に時間と労力を取られるような状況の未然防止	【機能・サービス内容・利便性】 ・社内システム規模拡大に伴い機器ごとの個別対策実施が煩雑になるため入口での一括対策が必要と感じられるため ・社内で手薄なセキュリティ対策ができる。 ・駆け付け対応を含む一次対応の方策があるだけ助かります。 ・何かあった時に相談できる ・実証に参加し安心感があった
利用する方向で検討するので、実証 UTM は春まで残置したい	(34%) 36	【金額面・費用対効果】 ・６千円という価格の安さ（７） ・業者の UTM レンタルサービスを利用するとコストが３倍位かかる ・５千円程度なら利用する／年一括５万円（税込）なら利用する ・クライアント数に対しては利用料が比較的安価と思うから／安価にここまでのサービスを提供して頂けるなら安心／費用対効果を考えると導入メリットが大きいと思う／経費が低くすむのであれば使い勝手が良いので継続利用したい／元々他社ＵＴＭをリースで導入しているが、こちらの方が月額費用は安くなりサポートもして頂けるので安心。 【必要性がある】 ・攻撃に対する脅威、セキュリティ向上、安心安全のため（16） ・今後ネットショップ開業予定のためセキュリティをしっかりさせたい ・本業に専念したい	【機能・サービス内容・利便性】 ・リスクの程度は不明だがブロックが働いたことは確かなので ・Emotet メールが弊社に届いた時の対応スピードが早かった為。 ・相談窓口のスピードが速い点と決着までに対応して頂けたこと ・初期設定さえできればあまり手がかからない為 ・普段のネットワーク利用時にはＵＴＭを殆ど意識することがない点 ・機能自体も自動でアップデートが行われる点が運用しやすい。 ・有事の際に専門家に相談できる安心感 ・事業意図や対応内容がはっきりしており、事業の信用度が高い ・やはり大阪商工会議所が事業実施主体となって頂ける安心感 ・“商売”が感じられなかった為 【検討すべき点】 ・他社ＵＴＭと比較したい ・社内稟議さえ通れば導入したい
利用しない	(37%) 39	【金額面】 ・利用料金が高い、予算がない（８） 【効果が分からなかった、問題がなかった】 ・効果が有ったのか無かったのか分からない（５） ・攻撃や問題がなかった（４） 【必要性がない】 ・必要性がない、現在のシステムで対応できている（５） ・ウイルス対策ソフト等で十分（２） ・NW見直し等の際に再検討するが現在は不要（2）	【機能・サービス・利便性】 ・煩雑すぎる ・各種情報のエクスポート機能がないため ・誤報が多く詳細調査に労力を使い報告後の回答が遅く迷惑に感じた ・設置段階でネット不備になりその解決策が見当たらず取り外した（２） ・サポート体制や管理画面等の見やすさから他社 UTM 採用を決めた ・接続が遅くなるなどの弊害があった
分からない	(16%) 17	・現場としては継続したい。社長がＰＣのＡＶとパックになっていればよいと言っている ・弊社ベンダーの SE と協議する時間が必要	
（無回答）	(1%)1		

（ロ）サービス商用化の必要性・趣旨【Why？Who？When？】

○アンケートのⅠ（専門人材の不足）、Ⅱ（僅少な予算）、Ⅲ（UTM 普及の鈍さ）、Ⅳ（SECURITY ACTION の不浸透）、Ⅴ（取引先からの要望）、Ⅵ（価格、機能、使い勝手へのニーズ）、Ⅶ（相談や駆け付けへのニーズ）、Ⅷ（サイバー攻撃・被害の多さ）などに鑑み、実証を実証だけで終わらせることは出来ないとの結論に達し、実証結果に基づき改善を加え、商用化に移行する必要があると決断するに至った。

○中小企業向けのサイバーセキュリティ市場はまだまだ未成熟であり、サプライヤー側もなかなかリスクテイクしてまで事業化を進める（低価格化などを含め）ことができない状況である。そこで、大阪商工会議所が、政策的事業の一つとして、NEC、東京海上日動、キューアンドエー、NEC ネクサソリューションズなど各分野のリーディングカンパニー、そして地域で機動的に活躍している地場の IT 事業者などとタッグを組み、先取的に完全オリジナルの試行的サービスを提供し、市場開拓の先鞭をつける必要があると考える。幸運なことに、商用化に先立つフィージビリティーや支援体制構築を本実証事業にて行うことができたため、先行投資や研究開発経費の売価転嫁も最小限で済むうえ、事業を展開するうえで一定の助走が出来ている（各社の本実証事業担当者が残存、初期顧客として参加企業の一部が有料化後もサービス利用継続の意向を示している）状態に在る。

（ハ）目指すべきこと、目指すべきサービス【Where？Whom？】

○ビジョン

「日本の中小企業ならびにサプライチェーンをサイバー攻撃から守る」

「中小企業がサイバーセキュリティにより事業継続力と企業価値を高めることを支援する」

○目標

「安価かつ簡便な、パッケージ化されたサイバーセキュリティお助け隊サービス（仮称）」を販売し、３年で採算ベースに乗るようにする。（３年間は事業継続をすることを申し合わせ済）

○顧客ターゲット

・あらゆる業種・業態の中小企業（製造業 300 人以下、卸・サービス業 100 人以下、小売・飲食業 50 人以下）および小規模事業者（法人、個人を問わない）
・UTM 未設事業者および UTM 既設事業者
・サイバーセキュリティの意識・知識・対策が中～下位層にある事業者

○訴求キーワード

「総合性」……保険もついているワンストップ性、パッケージ性

「公的イメージ」……販売主体が大阪商工会議所。利潤目的でなく政策実現が目的

「安価」……月額 6,600 円（年額 79,200 円）。初期費用ゼロ。

「簡便」……簡易 UTM の導入・運用が簡便。

「事前＆事後対応」……後者に力点を置く

「会社の価値を高める」…本サービスの利用が第三者認証に近いような“取引先を安心させる”要素になるようブランディングを推進

「ＢＣＰ対応商材」……事後対応力の向上に資するもの

「付随教育機能も充実」…各種セミナーへの優先案内、最新セキュリティ情報の提供、SECURITY ACTION の宣言支援

②座組・商流・サービス概要

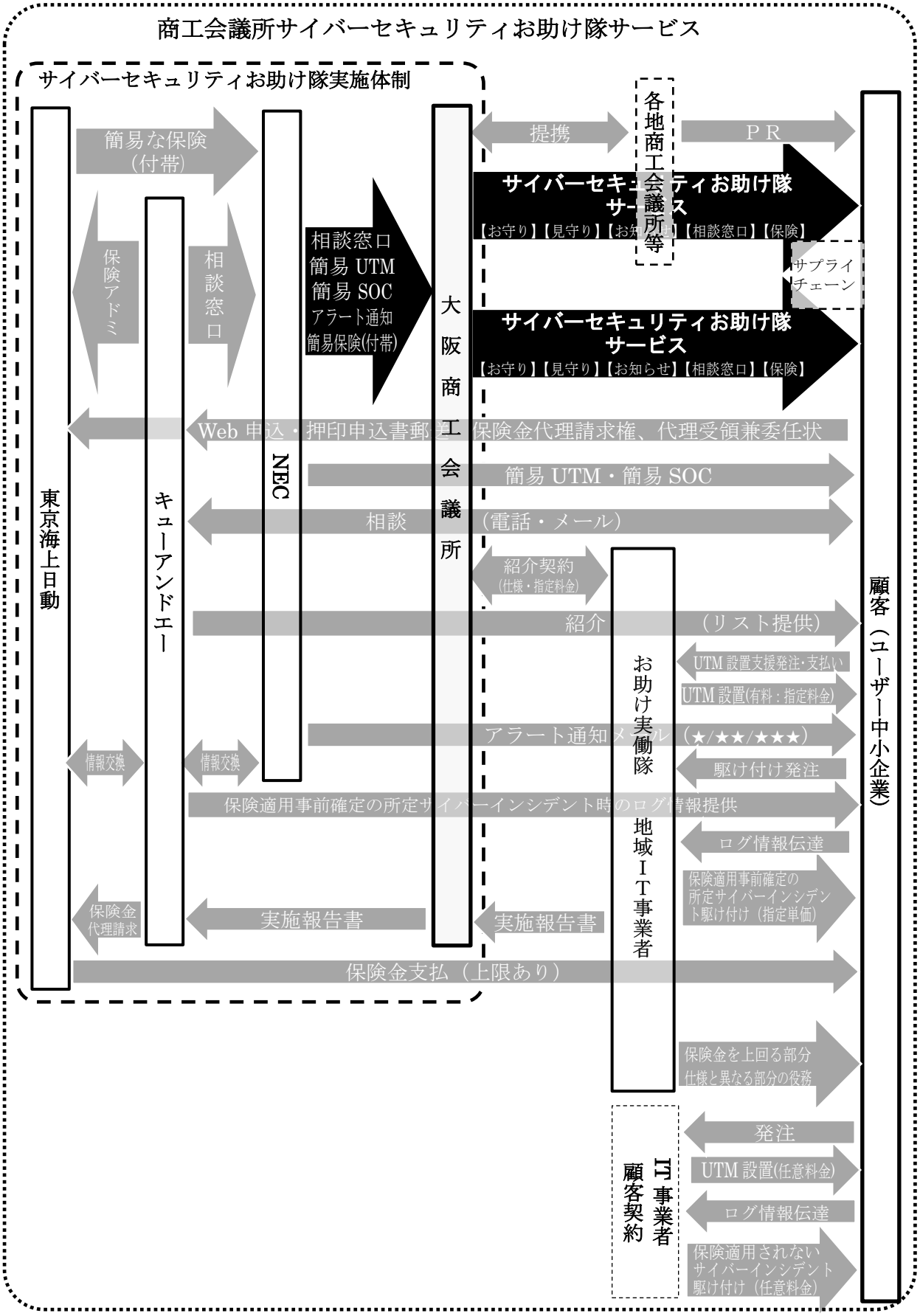
（イ）サービス提供主体【Who？】

○大阪商工会議所がサービス提供主体となり、サイバーセキュリティサービス（「お守り」「見守り」「お知らせ」「相談窓口」「保険」）を一体的に NEC から仕入れ、サービス一式を提供する。

○本実施体制が（一定の採算性を前提としつつも）自社の利潤のみを追求するのではなく、「サイバー攻撃から日本の中小企業とサプライチェーンを守る」という公共性の高い志のもとに本実証事業および商用化に携わってきている所以であり、この点にこそ本サービスと本実施体制の存在理由がある。

（ロ）座組・商流・サービス概要【What？How？】

図 14



③商用化段階でのお助け実働隊【駆け付け】

（イ）本実証事業からの変更点

○簡易 UTM 設置は、本実証事業では無料としたが、商用化段階では、持続的事業実施の観点から顧客負担（発注者、支払者は顧客）とする予定。顧客は大阪商工会議所が提供するリスト掲載のお助け実働隊に発注する場合は、対価は大阪商工会議所が予め定めた額（実証事業と同じ）となる。これにより、顧客は安心して発注することができる。

（ロ）お助け実働隊に求めるべきスキルセットとスキルレベル

○情報システムおよびサイバーセキュリティに係る高度な知識

・マルウエア、不審なアプリケーション等の最新情報を有しているレベル
・主要なアプリケーション等の脆弱性に関する最新情報を有しているレベル
・ウイルス対策ソフトの名称やバージョンの最新情報を有しているレベル

○初訪問する“情報システム担当者のいない中小企業”において初動対処できるコミュニケーション力

・感染経路確認のため、被疑端末の所有者に重要アラート検知時刻帯周辺で実施した操作等（被疑 URL へのアクセスを意図的に実施したか否かなど）を聴き出すことのできるレベル
・ウイルス対策ソフトのアップデートやフルスキャンを（自身がやるのではなく）ユーザー側に説明しつつユーザー自身に実施させることのできるレベル。また、それをユーザーが今後も適切かつ定期的に行う必要性を理解し実践にむけた意識変容を後押しすることができるレベル。
・OS クリアインストールのメリットとデメリットを平易かつ過不足なく説明でき、その場で決裁権ある人物からその了承を得られるレベル

○インシデント発生時の状況把握力、証拠の収集・分析力

・初訪問する“情報システム担当者のいない中小企業”で、ネットワーク構成図を概ね書けるレベル
・不審なアプリケーションを特定できるレベル
・IP アドレス、MAC アドレスのベンダーコード、通信が発生した時間帯から被疑端末を特定できるレベル
・イベントログ等から不審な通信と通信先を特定できるレベル

○こうしたスキルを有する人物や会社を探すのは容易ではないが、一つの目安とし

て、実証でもそのスキルの高さが明らかとなった情報処理安全確保支援士を有力な候補とし、サイバーセキュリティ地域支援体制を整備していきたい。

④商用化段階での簡易 UTM【お守り】

（イ）設置マニュアル改善

○実証中の問い合わせ内容やアンケート結果をもとに、設置マニュアルの改善を行う。それにより、企業自身の設置コスト削減や、サービス運用コスト削減（問合せ件数、問い合わせ対応に掛かる時間）の削減を図る。

（ロ）デフォルト設定の見直し

○実証中に有効化した電子メールの添付ファイルのアンチウイルススキャン機能は、商用化時には、事前設定で有効とし、ユーザーに提供を行うようにする。それにより、ユーザーは設置直後から電子メールの添付ファイルのアンチウイルススキャン機能が有効となり、より安全になる。

（ハ）正しく設置されているかの確認方法の提供

○UTM を設置しても、設置位置が誤っており、監視対象に含まれていない端末がサイバー攻撃を受ける可能性がある。実証事業では 1 台でも対象となっていれば問題ないとしたが、商用化では、保険の対象範囲にも影響するため、どの端末が監視対象になっているかユーザーも把握できる手段の提供を検討していく。

⑤商用化段階での簡易 SOC【見守り】

（イ）セキュリティ検知基準の平準化

○ユーザーにて UTM のセキュリティ設定を変更された場合、適切に監視できなくなる可能性がある。そのため、ユーザーが設定できる項目は最低限のみ公開し、セキュリティ設定については、監視運用者しか変更できないようにする。

（ロ）ポータルサイトのログイン方法の変更

○UTM での検知防御実績をポータルサイトに掲載しても、ユーザーが閲覧しなければ意味がない。実証で見えた中小企業の実態を基に、ポータルログイン時の認証に使用する端末がない場合や、IT リテラシーが低い場合でもログインできるよう、手段を用意する。

⑥商用化段階での相談窓口【寄り添い】

（イ）回答時間の短縮と回答期限の明確化

○実証では問い合わせに対する回答までに時間がかかり、催促を頂くケースがあった。即答できない事象はNECへエスカレーションをする事で回答を行ったが、エスカレーション時の情報不足や事象によっては確認に時間を要するケースもあった。今回実証で得た事例をナレッジ化することで回答時間の短縮を図り、且つ回答に要する日数を明確にすることで窓口に対する CS 向上に繋げる必要がある。

（ロ）リモート対応活用

○今回実証では、サポート時に「忙しい」「自身で対応する」というような理由でリモートサポートによる活用事例が少ない結果となった。商用化においては、正しい状態でのウイルススキャンが実施されているか、ユーザーの申告内容が正しいものかなど内容の詳細確認や迅速な対応のため、トラブル対応やインシデント対応に対して、積極的にリモート提案を行い、ユーザーの負担軽減に繋げる。

（ハ）分かりやすさ・伝わりやすさ・聞きやすさ

○中小企業の中にはICT・セキュリティのリテラシーが高くない方もいるため、トラブル状況を正確に伝えられない可能性がある。その場合でも、窓口では少ない情報から発生状況を正確に把握し、「専門用語」を使わず、できるだけ噛み砕いた言葉で説明やサポートを行い、企業担当者へのストレスをかけない窓口対応を目指す。

（ニ）よろず相談

○今回実証ではUTM設置やインシデント対応に関する相談だけではなく、PCの一般的な操作方法やトラブルなどについても相談を頂いた。操作方法については簡単なアドバイスまでを実施。トラブルの場合はサイバーインシデントとの関連性を見極め、状態により製造者やプロバイダへ誘導を行った。専属のサポート契約がなく、どこに問い合わせをして言いか分からない中小企業ユーザーに対しては、相談ができる窓口があることで不安を取り除く役割を担える。

⑦商用化段階でのアラート通知【お知らせ】

（イ）アラート精度の向上

○UTM検知した内容に関して、UTMだけではセキュリティインシデントの問題を特定できないケースがある。エンドポイントセキュリティと組み合わせセキュリティインシデントの問題特定を検討していく。

○アラート通知メールが大量に届くと、ユーザーがメールを開封すらしなくなる恐れがあるため、重要度に応じてアラート通知する／しないを検討にしていく。

（ロ）月次レポートの送付

○インターネットから社内 LAN への不審な通信の防御状況について、ポータルサイトに表示しているが、ユーザーが確認する必要がある。そのため、ユーザーがポータルを確認しなくても、自社への攻撃状況を把握できるように、月次レポートで防御実績を送付する。

⑧商用化段階での保険設計【補償】

（イ）中小企業が利用しやすいサイバーに関する保険の仮説

○前述のとおり、中小企業においては、重大インシデントに対して損害賠償責任、フォレンジック費用等を幅広く補償する一般的なサイバーリスクに関する保険の普及率が未だ低い状況である。これは、中小企業にサイバーリスクに対する意識の低さや保険料水準の高さが要因であると言われている。

○そのため、中小企業向けには段階的に保険の必要性を訴求していくことが必要と考え、まずはインシデントへの対処を促す簡易的な補償を提供し、次に一般的なサイバーリスクに関する保険のニーズを高めていくことが必要との仮説に至った。

○あわせて、簡易的な保険を任意加入とすると、一般的なサイバーリスク保険同様に普及が難しくなることが予想されることから、任意加入ではなくお助け隊サービスの導入企業全社に提供する必要があるとの仮説を立てた。

○本証事業では、上記仮説に基づいて中小企業の利用しやすいサイバーリスクに関する保険のあり方を、以下のステップに分けて、その妥当性を検証することとした。

■ステップ１：参加企業全社に対し、インシデント発生時に 5 万円程度の補償を提供し、簡易処置・診断を提供することで、サイバー攻撃に対する初動対処の重要性を理解させ、万が一の際の被害について考えさせるという“行動変容”を促す。→保険機能として、参加企業間で薄く広くリスク分担する仕組み（補償）を構築する。

■ステップ２：ステップ１の簡易処置・診断を通じて「重大事案」の発生を早期に検知し、真に対応が必要な場合に本格的な対処（フォレンジック等）へとつなげる仕組みを構築。本格的な対処には数百万円から数千万円の費用負担が必要となり、加えて賠償リスク（サプライチェーンへの影響）の懸念も早期に顕在化することから、各自がオプション（任意）

でも保険に加入し、簡易的な保険だけでは対応できない対処費用や損害賠償責任に備えられる仕組みを構築する。→既存の中小企業向けサイバーリスクを補償する保険へ誘導する。

＜仮説検証の具体的な手順＞

表 64

	ステップ 1		ステップ 2
	実証事業中（全員補償）	実用化以降（全員加入保険）	実証中・実用化以降（任意加入保険）
提供方法	サイバーセキュリティサービスパッケージ導入企業全社に対し、実証予算の中から補償を提供	サイバーセキュリティサービスパッケージ導入企業全社に対し、保険を全員付保して補償を提供（保険料はサービス利用料に包含）	・相談窓口での任意保険への誘導（全員加入保険による企業の**"行動変容"**により任意保険へのアクセス向上） ・サイバーセキュリティサービスパッケージ導入企業向けに割安な団体保険を構築し加入促進
補償内容	提供した簡易UTMによる検知や相談・リモートサポートでの判定により、5万程度の対策費用を実費で支払い	同左	・不正アクセスの「おそれ」の段階からの外部調査依頼費用 ・不正アクセス確定後の状況に応じて、通常の損害賠償、データ等復旧費用・情報システム復旧費用、再発防止費用などを支払
効果	従来放置されてきた不正アクセス等に対して、検査を行い対処をするという**"行動変容"**につながる	同左	・早期段階での十分な調査費補償による被害の拡散防止、事業活動の早期再開により事業やサプライチェーンも維持 ・再発防止費用等により将来的な被害の防止にも効果
保険（補償）の使い方	判定に基づき、中小企業の**"行動変容"**のために保険（補償）を提供	同左	加入企業の受けた被害（講じた対策）に対して、実際に支出した費用に対して保険（補償）を提供

（ロ）仮説に対する実証を通じた気付き（保険の在り方に関する考察）

（簡易的な保険の検証）

○今回の参加企業においては、簡易 UTM の設置や簡易 SOC 機能を実際に提供することで、中小企業にとっては従来目に見えなかったサイバー攻撃が見える化され、何ら

かの対処が必要であることを一定程度認知させることができた。

○サイバー攻撃を認知し駆け付けによる対処（フルスキャンなどの初期対応）がスムーズに行われるようになり、従来であれば放置されていた可能性のあるマルウエア感染に対して何らかの対処をするという行動が確認された。実際に、駆け付けによる初期対応によりウイルス駆除等がなされ、その後の被害拡大防止に繋がったケースも確認できた。

○上記の事実から考えると、お助け隊に簡易的な保険を自動的に組み込むことで、中小企業は自社のリスクを認識し、何らかの対処に動くという“行動変容”が見られるなど、中小企業のリスクの軽減に繋がる効果があったものと考える。

（上乗せ保険の検証）

○一方で、上記駆け付けによる初期対応だけでは、根本的な問題が解決しないケースも想定される。その際、中小企業には更に難易度の高い対応が求められることになり、上乗せ保険が必要となる。今回の参加企業へのヒアリングでも、お助け隊（簡易的な保険）で対応できる範囲と、上乗せ保険で対応できる範囲につき説明（以下、図表参照。）した際には、上乗せ保険のニーズも一定程度確認することができた。但し、これは中小企業であっても相当数のサイバー攻撃を受けている事実を個別に説明したことで、リスクを具体的に認識し、上乗せ保険の必要性を認識したことによるものと推測される。

○加えて、今回の実証で上乗せ保険について、どこまでの補償を中小企業が求めているのかという検証にまでは至っていない。サイバーインシデントは、自動車事故や自然災害事故と比べ、その被害が顕在化しにくく、上乗せ保険で備える必要性を感じている中小企業は少ない。例えば、マルウエア感染が発生したとしても、フォレンジックなどの調査を行わずに、PC の買い替えだけで済ませばよいと考える中小企業も多いのが実態である。したがって、お助け隊の UTM 等で見える化されるサイバー攻撃やウイルスの感染を放置するとどのような被害に繋がるかという事例を中小企業に具体的に示した上での、更なるニーズ把握が必要となる。

○今回の実証では、実際に大きな被害が発生した事案や、フォレンジックなどの外部調査費用、データ復旧費用がどの程度かかるのかを把握できるような事案が発生しなかった。今後は、他地域の実証事業における事例も含めて、このような事例をより多く集約して示すことで、中小企業に対して上乗せ保険の必要性をより高めると

ともに、中小企業にとって必要な補償額の基準等が明らかになることが望ましい。

表 65

起こりうる事象（代表事例）	お助け隊を導入していた場合	被害事例	上乗せの保険で出来る事
・不正なプログラム（ウィルス等）の送付などの攻撃	UTMにより攻撃をブロック	被害無し （ウィルスなどの感染の恐れも無し。）	（お助け隊で対応完了）
	UTMで不正アクセス検知。（アラート★3） IT事業者が駆けつけ、初期対応を実施（フルスキャンなどによりハードディスク上のファイルと実行中のプログラムをチェックし、確認出来たウィルスを可能な範囲で除去。）	被害無し （ウィルスなどの感染も除去。）	（お助け隊で対応完了）
		被害無し （ウィルスなどの感染の恐れが残っている。）	【費用】 IT事業者の駆けつけによる初期対応でウィルスの除去や感染源の特定などが出来なかった場合の追加費用を補償。
		社内のネットワークの稼働が停止	【費用】 稼働停止の原因の調査と、原因に対する復旧費用の補償。
		社内データが消失	【費用】 データが消去した場合の復元等の費用の補償。
		社内の顧客情報データが流出	【費用/賠償】 データが流出した顧客に対する見舞金、プライバシーの侵害による賠償請求を補償。
		自社になりすまし、取引先にウィルスなどを送付し、取引先のデータを消失。	【賠償】 取引先のデータ消失による損害賠償責任や、データを復元するための費用に対する損害賠償責任を補償。
		端末の乗っ取りにより、取引先を攻撃し、取引先のネットワークを切断。	【賠償】 ネットワークの切断に伴う損害賠償責任を補償。

（ハ）今後の保険制度運用で想定される課題

○本実証事業で得られたデータは、期間や対象企業が非常に限定されたものであり、そのデータ内容についても一般的な中小企業のデータと比較すると、偏りがある可能性が否定できず、安定的な制度運用に際してはより多くのデータ収集体制の構築が不可欠である。

○簡易 UTM の検知を保険発動要件とした簡易的な保険の提供を検討するにあたってはより多くのデータ収集が不可欠であるが、UTM の機能がメーカー（機種毎）毎に異なる場合など、それぞれ異なるリソースから収集されたデータを集約して 1 つの保険データとして活用することについては、データの前提条件が異なる可能性があり、その妥当性を検証する必要がある。

○サイバー攻撃は日々進化し、それにあわせて UTM の機能も継続的に改善されることなるが、その場合、保険の発動要件が定期的に変動するという事象が発生し、保険商品設計が複雑になる可能性がある。

○UTM において過検知などが多く発生した場合、本来不必要な事案に対し駆け付け（補

償）を提供することになるため、UTM の機能の一定の安定性が確認できた上での補償の提供が望ましい。

○中小企業が加入しやすい保険料水準を安定的に提供するには、中小企業が自ら、ウイルス対策ソフトの更新など最低限の対策を日常的に実施することや事前のリスク診断、最新のサイバーリスク対策に関する情報収集を適時適切に行っていくことが望ましい。

（ニ）現状の商用化に向けた保険の形

○簡易的な保険（全員加入型）

全員加入型の簡易的な保険については、以下の内容で検討を進めている。

・中小企業が設置している UTM で不正アクセス等の発生やそのおそれを検知。
・検知後に大阪商工会議所が紹介する IT 事業者が訪問のうえ初動対処等を行う。
・上記駆け付け対応にかかる費用につき 5 万円を限度に保険金でお支払いする。

簡易的な保険の設計にあたっては上述の通りデータが少ないため、広く販売をした際に保険金の支払いが増え、保険制度が破綻する可能性がある。そのため、1 回の駆け付けあたりの保険金上限（5 万円）を設けるなど、安定的に保険を提供できるような工夫が必要である。

また、駆け付け対応では一時的な処置に留まるため、サイバーインシデントの原因特定や情報が漏えいした際の費用補償については、別途上乗せ保険に加入頂く必要があると考えている。

○上乗せ保険（任意加入型）

上乗せの保険にあたっては、東京海上日動が提供している主に以下を補償するサイバーリスクに関する保険の提供を予定している。

① 【賠償】サイバー・情報漏えい事故
サイバー攻撃などに起因して法律上の損害賠償責任を負担することによって被る損害

② 【費用】サイバー・情報漏えい事故対応費用
セキュリティトラブルへの対応やサイバー・情報漏えい事故に起因する訴訟対応を行うために負担するサイバー・情報漏えい事故対応費用

⑨その他（価格・販売方法等）

（イ）料金体系は簡素に

○IT 業界の商品・サービスの料金体系は一般的に非常に複雑であり料金改定も少なくない。料金表が存在していない場合も多く透明感もない。中小企業には専任の情シスがいない場合も多く、内容と価格を精査する余裕がなく相場感も乏しいため、料金体系は簡素さと明朗さが求められる。

○一方で大阪商工会議所は営利団体ではないため営業上のリスクは冒せないため、サービス料金は前払いとする必要がある。

○所定インシデント駆け付け・初動対処に係る料金は、保険上限金額（5 万円）までは、保険により補償されるが、上回った分（時間的、作業内容的に）は、顧客とお助け実働隊との二者間の契約関係となり、見積額や作業内容、作業方法などを（その場で又は後日に）提示し顧客自身が（その場で又は後日に）発注の有無を決めることとした。このときのコミュニケーショントラブル防止のため、現場での作業チェックシート等の改善を行いつつある。

（ロ）「買い取り（資産の譲渡）」でなく「リース（役務の提供）」としハードルを下げる

○UTM は一般的に買い取りが多いが、買い取りだと初期費用が高くなり、中小企業にはハードルが高い。また、日進月歩の著しいセキュリティ機器を一定の頻度で買い替えることは、その判断の難易度やコストなどの面から考えても、中小企業では難しいことだろう。よって本実施体制では、簡易 UTM はリースとし「初期費用ゼロ」を訴求することとした。

（ハ）契約期間はできるだけ短く

○UTM に限らず IT に係る機器やサービスについては、その契約期間が長い（例えば５年や７年などもある）ことが、中小企業の“最初の第一歩”の阻害要素の一つとなっている。そこで、本実施体制では、商用化にあたっては、出来るだけ短い契約期間を設定する予定（例えば１年）である。これはサービスを提供する側にとっては長期的な収益計画を立てづらくする要素ともなるが、ユーザーファースト、中小企業フレンドリーという意味では、短い契約期間は必須といえよう。

（ニ）簡易 UTM 設置は受益者負担

○本実証事業ではお助け実働隊による設置支援は無料とできたが、設置支援率が

31%であったことをふまえると、商用化段階では、サービス提供主体である大阪商工会議所は負担できないので、受益者負担（オプション）とする。なお、1社でも多く自力設置ができるよう「設置マニュアル」の記載改善を進める。

○オプション有料制とする以上、その価額が事前確定している必要がある。実証の実施結果をふまえ、実証と同一の 15,000 円（交通費込・税別）とする予定。

（ホ）サービス提供価格

○本実証事業の参加企業へのヒアリング結果から、商用化後のサービス提供価格として約7割が「月額 3,000 円未満」を希望し、9割が「月額 6,000 円未満」を希望するなど非常にシビアな反応である。参加企業が比較的サイバーセキュリティ意識の高い企業であることを勘案すると、意識の低い中小企業も含めて市場開拓し、採算ベースで商用化を持続させていくことは、まさに“茨の道”ともいえる。

○事業の持続性と中小企業のニーズである「安価」の両方を斟酌すると、全て込みで月額6千円～8千円程度に設定することになろう。総合的視点から、実証前および実証中に理想として想定した月額5千円は実現できそうにない。

⑩集客

（イ）概要

○サイバー攻撃は益々巧妙化と増加の一途を辿ることが予想されるため、商用化に向け、歩みを止めるわけにはいかない。下記のような手法で集客に努め、持続的に事業を展開し日本の中小企業とサプライチェーンを守っていかねばならない。

（ロ）ＷＨＯＬＥ　ＳＡＬＥ的手法を通じて

○サプライチェーン頂点に位置する大企業に結節点になって頂く

(a) 取引条件化（独占禁止法及び下請法の優越的地位濫用に抵触するおそれあり）
(b) 推奨（可能性はあり）
(c) 個別紹介して頂き個別案内（やや効率悪いが堅実な手法）
(d) 案内させて頂く機会の提供（取引先が集まる調達方針説明会やセミナーで）
(e) 案内して頂く（チラシ配布・配架）
(f) 案内して頂く（適宜口頭で）

○実証中に、サプライチェーンの頂点に位置すると考えられる大企業を対象に、取引先等へのサイバーセキュリティの関与・ガバナンスの状況や、商用化後のサー

ビス普及に向けたご協力の可能性についてヒアリングを行ったところ、概ね下記のような回答であった。

表 66

サプライチェーンの頂点に位置する大企業へのヒアリング結果（2019 年 10～11 月）		
企業	取引先等へのサイバーセキュリティの関与等	サイバーセキュリティお助け隊商用化への協力申し出状況
大手鉄道	・グループ会社のうちコストがかけられないところは最低 HP、個人情報管理のみ指導。AV ソフト程度が殆ど。 ・契約等で規定しているのではなく口頭依頼レベル。「中小企業としてココまでやっているのだから許してよ」とエキスキューズできる程度。	・大商のお助け隊サービスは素晴らしい。特に簡易補償が喜ばれるだろう。IT 部門としては推奨したい。 ・グループ会社で、ニーズアンケート、サービス概要チラシを配布。 ・調達先が集まる説明会、グループ会社の情シスが集まる会での説明機会を準備する。
大手化学	・優越的地位の濫用については、既存取引先に教育や監査を行うことまでは問題ないが、取引条件化はＮＧ。	・購買先を紹介することはできる。 ・調達方針説明会の場での説明機会付与は可。
大手食品	・主要取引先に専用 PC を配布。 ・取引先に今後採り得る対応は、アンケート回答くらい。特定のソフトや機器の利用などは盛り込めない	・年１回調達方針の機会を付与できるかどうか調達部門に聞いておく。
大手家電	・周りの大企業が取り組み始めれば当社も動きやすい。	・下請法の関係で、お助け隊サービスを取引先に薦めたり、紹介することはできない。
大手重工	・サイバーセキュリティ対策を取引の要件とするのは違法になるが、ウイルス付きの図面などを送ってきたら即取引停止するといった警告を発するのは有効	・取引先に働きかけるのは下請法がネック。経産省に対し、サイバーセキュリティに関しては同法の適用を緩和するか、どこまで許されるのかガイドライン等で示してもらうよう要望してもらえないか。

大手機械	・社内システムは本社が、調達に関しては調達本部が担当している。 ・情報セキュリティのチェックシート記入を依頼。80 点以上は約 3 割。 ・取引条件にセキュリティ要件を入れてしまうと取引できない会社ばかりになってしまうのが実情。	・お助け隊サービスの「月額数千円」は興味深い。取引先に案内をすることは可能だが強制はできない。 ・誰がお金を払うかの議論になってしまう。調達先での導入コストは結局、当社への売価に転嫁され、結局弊社が間接的に負担することになるかも。

○中堅企業（大企業１次取引先等）に結節点になって頂く

大企業の１次取引先のサイバーセキュリティはほぼ整備されていると考えられるが、その取引先以降の中小企業はまだサイバー対策を進める余地があると考えられる。

○経営コンサルタントや各部門専門家、士業会などに結節点になって頂く

中小企業診断士、社会保険労務士、税理士、弁理士等の士業に、コンサルテーションの一環としてサイバーセキュリティを取り込んで頂くとともに、本サービスの普及も付随的に依頼。

○情報処理安全確保支援士、IT コーディネーター等に旗振り役になって頂く。

（ハ）ＲＥＴＡＩＬ　ＳＡＬＥ的手法を通じて

○中小企業への直販（竹槍戦法の一本釣りは出来ない）

○テレマーケティング

○大阪商工会議所の通常の広報媒体

（ニ）ＡＬＬＩＡＮＣＥを通じて

○各地商工会議所と提携し、一定のキックバックを前提に普及・個別紹介を依頼

○日本商工会議所との連携

○地域金融機関（信金・地銀）などと提携し、一定のキックバックを前提に融資先等への普及、個別案内、個別紹介などを依頼。単なる周知依頼の方が現実的。

○IT ベンダーに卸す、もしくは何らかの形での連携（場合によりライバル関係）

（ホ）ＰＵＢＬＩＣ　ＲＥＬＡＴＩＯＮを通じて

○公式Ｗｅｂサイト（これが一番基本となる）

○公式Ｗｅｂサイト以外のＷｅｂを使った広報（コスト、手法、費用対効果が課題）
○セミナー（大阪商工会議所主催のプロバーの販促セミナー、啓発セミナー、他団体主催のサイバーセキュリティセミナーで説明機会を設けて頂くなど）
○展示会・商談会への出展（コストが課題）
○プレス発表
○広告（コストが課題）

（へ）国の支援の必要性

○国全体のサプライチェーンのサイバーセキュリティを強化する観点から、一刻も早く、「サイバーセキュリティお助け隊」事業を全国展開する必要があるが、本実証事業を商用化（有料化）するとしても、継続希望の企業は極めて限定的であり、その理由として「必要性（意識）」と「価格」が依然大きな障壁となっていることが分かった。

○ビジネスベースで、安価かつ簡便なサービスを継続的に供給するうえでは、相当数のユーザー確保が求められることから、引き続き国の支援が必要である。よって、「サイバーセキュリティお助け隊」をはじめ同種の民間サービスを普及させるために、国による、より積極的な普及拡大支援を求めたい。なお、本件については、本実証事業に付随して 2019 年 12 月 27 日付で下記のとおり国に建議した。

図 15

（参考）「中小企業のサイバーセキュリティ対策強化に関する意見」
（2019 年 12 月 27 日　大阪商工会議所　建議）

１．　中小企業サイバーセキュリティ対策支援促進事業の予算確保
今年度の地域実証事業の空白地域(北海道、首都圏、四国、九州)を確実に埋めるなど、重要インフラや重要産業のサプライチェーンを守る支援体制モデルの早期構築と今年度実証事業の民間事業化を進めるために、必要かつ十分な予算措置を講じられたい

２．　サイバーセキュリティお助け隊等民間サービスの普及拡大支援
サイバーセキュリティお助け隊はじめ同種の民間サービスを普及させるために、以下のような制度改善をされたい

（a）SECURITY ACTION 三つ星の新設と宣言要件への組み込み

宣言要件に「お助け隊サービス等の利用」を設定されたい

(b)「サイバーセキュリティ経営ガイドライン」への組み込み

同ガイドライン指示９「サプライチェーン全体の対策」における「望ましいこと」の事例として、「お助け隊サービス等の利用」を追加されたい

(c) IT 導入補助金の加点要件へ追加

申請書を審査する際、「お助け隊サービス等の利用」を加点要件として追加されたい

(d)「サイバーセキュリティお助け隊」の商標登録とブランド化

「サイバーセキュリティお助け隊」を IPA 等にて商標登録し、実証実施事業者に通常使用権を許諾され、分かり易い統一ブランド化による普及を推進されたい

(e) 民間事業化されたサービス利用者への補助金

事業化されたサービスを利用する中小企業に対し、利用料の一部を補助されたい

(f) 独占禁止法及び下請法の規制との関係明確化

サプライチェーンを守るために大企業が取引先の中小企業に対し、事業化されたサービスの利用を促すにあたって、独占禁止法及び下請法に抵触しない範囲を明確化されたい

（3）サイバーセキュリティお助け隊アドバイザーによるコメント

大阪大学　情報セキュリティ本部兼大学院情報科学研究科　教授
サイバーセキュリティお助け隊（京阪神）アドバイザー
コメント

情報漏えいインシデントに対する備えとして、昨今の企業組織はそのリスクを事前に十分検討しておくことが一般的になりつつある。しかし、どれだけの被害規模を想定し、準備すべきかを検討することはそれほど容易なことではない。しかも、専門的な外部機関に託すことは費用面を含めてそれなりの話になることも多く、たとえ外部に託す余裕があったとしても相談側において十分な経験や知識が必要となることも多い。

今回の実証事業は、特に中小企業を考慮して開発された UTM を利用し、実際の業務内に導入した上での評価を行うなど現実的な状況を想定しており、非常に有用性かつ価値の高い取り組みであると評価できる。

私として指摘しておきたい点を以下の通りである。

大きな点は肯定的な意見と否定的な意見が大きく分かれていることにある。肯定的に取られた側においてはコスト面においても導入のしやすさや、セキュリティの視える化という点で組織としてのセキュリティに対する「意識付け」に大きな意味をもたらしたことにある。特に、自組織がもし漏えい事件を起こしてしまったことを想定するならばその信用喪失に対する脅威や想定を越えた非常時における事業継続性についても改めて再認識された点であり、これは本取り組みの成果の１つとして積極的に評価したい。

一方、実攻撃がそもそも無かった、あるいは視えなかったという組織においてはその必要性を感じ取れなかったという意見もあり、導入意義やコスト面の説明に対して納得がいかないという現実を浮き彫りにしたことは現実に対して大きな示唆を与えている。

この問題はここだけの話ではなく、実はセキュリティ全体における大きな課題であり、そもそもセキュリティ投資は見えないもの、必ずしもリターンされないものへの投資の価値を今後どう伝えていくべきかも本事業における次なる課題として考えていく必要があるだろう。

以上