2021.3.24

サイバーセキュリティニュース ＜2020 No.004＞

サイバーセキュリティお助け隊事業（岐阜県を中心とする中部エリア）～実証事業の総括と今後の展望～

【要旨】
■ 大企業に比べサイバーセキュリティ対策が脆弱な中小企業の対策強化のため、経済産業省および独立行政法人情報処理推進機構（IPA）は昨年度に引き続き実証事業を実施した。
■ 弊社は、中小企業の実態把握と「地域の重要インフラ企業を核とした中小企業向けサイバーセキュリティ普及モデル」の実効性を検証するため、中部電力グループとの協業により中部エリアで実証を行った。
■ 本稿では、参加した中小企業のサイバーセキュリティ対策の実態と、実証したモデルの今後の展望について解説する。

１．実証事業の背景・目的

（１）2019 年度事業

2019 年 1 月に公表された「情報セキュリティ 10 大脅威 2019」において、「サプライチェーンの弱点を悪用した攻撃の高まり」が初めて 4 位にランクインし、サプライチェーンを構成する中小企業においてもサイバーセキュリティ対策の必要性が改めて認識されたこともあり、2019 年度に全国 8 地域でサイバーセキュリティお助け隊実証事業が行われた。

2019 年度事業では、弊社は愛知県において約 200 社を対象に実証を行った。特に①セキュリティに関する普及啓発が必要であること、②セキュリティ機器・サービス設置の導入負荷を減らす必要があること、③中小企業にとって許容可能な価格帯のサービスが必要であること、等が確認された。

また、中小企業はサイバーセキュリティ対策に投入できるリソースが不足しており、対策に着手していても「防御」までのケースが多く、「検知」や「対応」に必要な体制整備・人財育成等へ経営資源を投入できていない実態が見られた。

実証に参加した事業者に実施したアンケートやヒアリングの結果からは、「信頼できるサービスやベンダーを活用したセキュリティ体制構築が重要であり、価格はどちらかと言えば安い方が良いが、“ただ安ければ良い”というものではない」という意向が確認できた。

（２）2020 年度事業

弊社は 2019 年度事業での気づきを踏まえ、2020 年度は、

① 積極的に取り組む意欲のある企業 50 社に限定して、参加を募り、
② 中小企業の経営層と対話可能な地場の重要インフラ企業との協業により、
③ また、地域コミュニティとの連携強化により
④ 「実証終了後もサービスが継続利用されること」、「持続可能で全国に横展開可能なモデルを構築すること」が可能

との仮説を持ち、実証を計画・実行した。 経済産業省および IPA は、前年度よりも実証事業の規模を拡大し、全国 15 か所（13 地域と 2 業種）で実施された。

弊社は本実証事業を「岐阜県を中心とする中部エリア」において受注し、二つのコンセプトの実証を行った。

① 地域の重要インフラ企業を核とした中小企業向けサイバーセキュリティ普及モデルの構築

② 地域コミュニティとの連携による全国展開可能なサイバーセキュリティ支援体制モデルの構築

中小企業と幅広く関わりがあり、持続的で不可欠なサービスを提供している地域の中核企業・重要インフラ企業は、幅広い支援を行うリソースがあり、中小企業との密接な結びつきを可能とする基盤を備えている。ここにサイバーセキュリティの観点も加え、中小企業に幅広いセーフティネットを提供するモデルを構築することが可能と考えた。

また、大企業を中心とした取引先等を含めたサプライチェーンのサイバーセキュリティ対策の重要性を訴えることで、サプライチェーンリスクの対策促進も行うことを目指した。

更に地域サイバーセキュリティコミュニティは、地域によって成熟度は異なるものの、全国各地で支援体制を活性化させる動きが始まっている。この連携は、他地域における展開・実現の可能性が高いモデルと実証することを目指したものである。

２．実施体制と実証メニュー

（１）実施体制

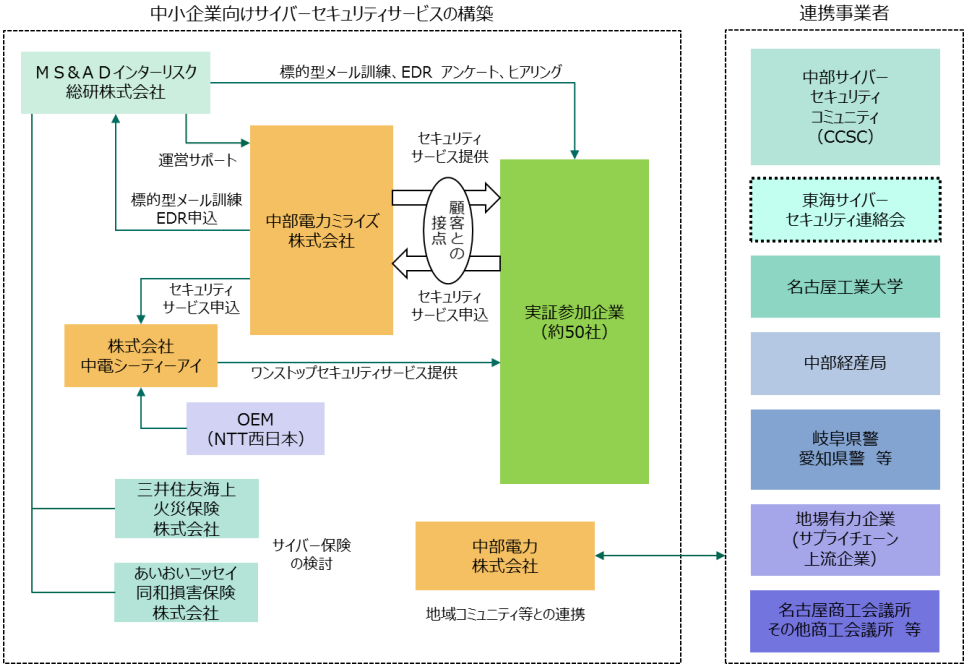
弊社は、説明会開催や集客管理など運営全般含めた全体調整に加え、標的型メール訓練や EDR[1] 提供といった個別セキュリティサービスの提供を担った。

中部地域のサイバーセキュリティ団体等との強力な結びつきを持つ中部電力株式会社は、関係団体やグループ会社との調整を担った。

電力販売事業を行う中部電力ミライズ株式会社は、接点のある大手企業のサプライチェーンや経営層との関係が深い中小企業に対して集客、簡易セキュリティ診断、セキュリティ対策の必要性の訴求など、参加企業の接点となる対応部分を中心に担った。

株式会社中電シーティーアイは、西日本電信電話株式会社（NTT 西日本）より OEM 提供を受けたセキュリティ商材の提供を行った。

MS&AD インシュアランスグループの保険事業会社 2 社（三井住友海上火災保険株式会社、あいおいニッセイ同和損害保険株式会社）は、中小企業に最適なサイバー保険及び付随サービスの検討を行った。



【図１】実施体制とスキーム

[1] Endpoint Detection and Response（パソコン等のエンドポイントでの検出と対応）

（２）実証メニューとスケジュール

実証メニューは以下・表１のスケジュールで行った。2020 年度事業は 2019 年度事業よりも実証期間が短く、募集期間や成果報告書などの取りまとめ期間を除くと実質 4 か月程度の期間となった。

参加企業向けメニューである「①簡易セキュリティ診断」「②標的型メール訓練」「③ワンストップセキュリティサービス」「④EDR（エンドポイント監視サービス）」を実証参加企業へ順次提供した。

このような多重の支援体制を作ることで、①アセスメント、②教育、③防御、④検知、⑤初動対応までカバーすることができる体制を構築し、有事の際の報告や被害最小化に活用することができ、発注元や取引先にとっても安心できるサービスとなることを目指した。

実施内容	9月	10月	11月	12月	1月
説明会の開催	←	→			
簡易セキュリティ診断	←			→	
標的型メール訓練	←				→
ワンストップセキュリティサービス	←				→
ＥＤＲ	←				→
事後アンケートの実施				←	→
事後ヒアリングの実施				←	→
成果報告会の開催					← →

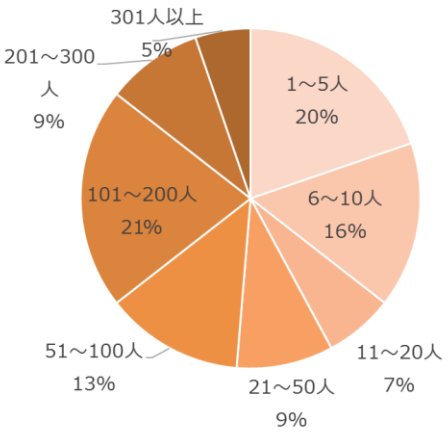
【表１】実証メニューとスケジュール

３．実証結果

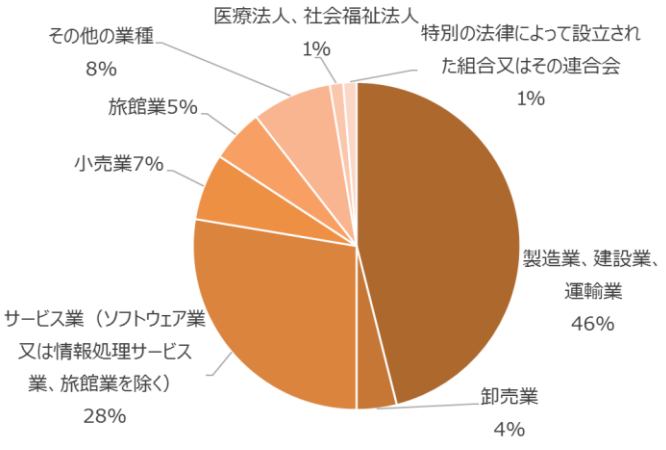
（１）参加企業属性

中部電力ミライズ株式会社を中心に実証参加企業を募集し、参加企業数は７６社となった。

中小企業の中でも従業員規模１００名以下が半数以上を占め、業種は「製造業・建設業・運輸業」が最も多く、次いで「サービス業」が多かった。



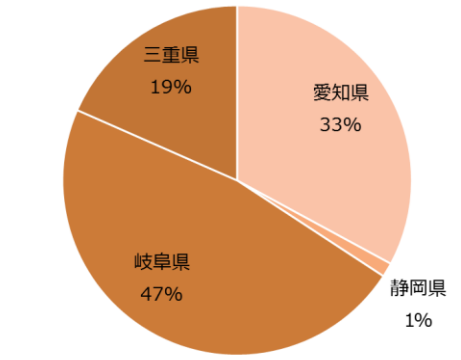
【図２】参加企業の従業員規模（Ｎ＝７６）



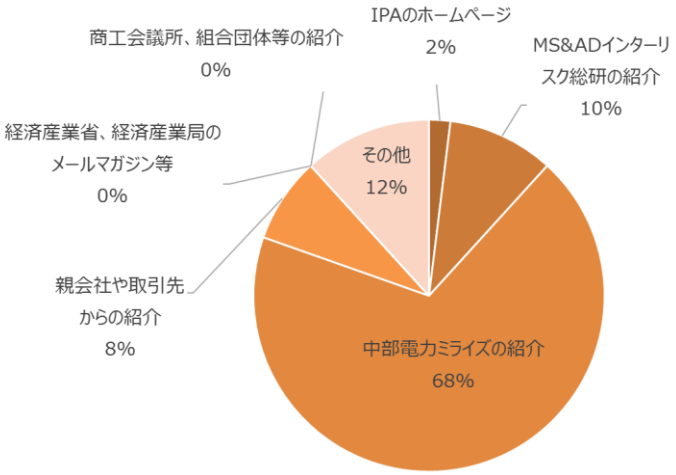
【図３】参加企業の業種分類（Ｎ＝７６）

所在地別では、岐阜県が最も多く、次いで愛知県・三重県・静岡県と続いた。

中部電力ミライズが中心となって集客を行ったため、本実証事業を知ったきっかけとして、中部電力ミライズの紹介を挙げた企業が７割近くとなった。



【図４】参加企業の所在地（Ｎ＝７６）



【図５】本事業を知ったきっかけ（Ｎ＝５１）

（２）簡易セキュリティ診断

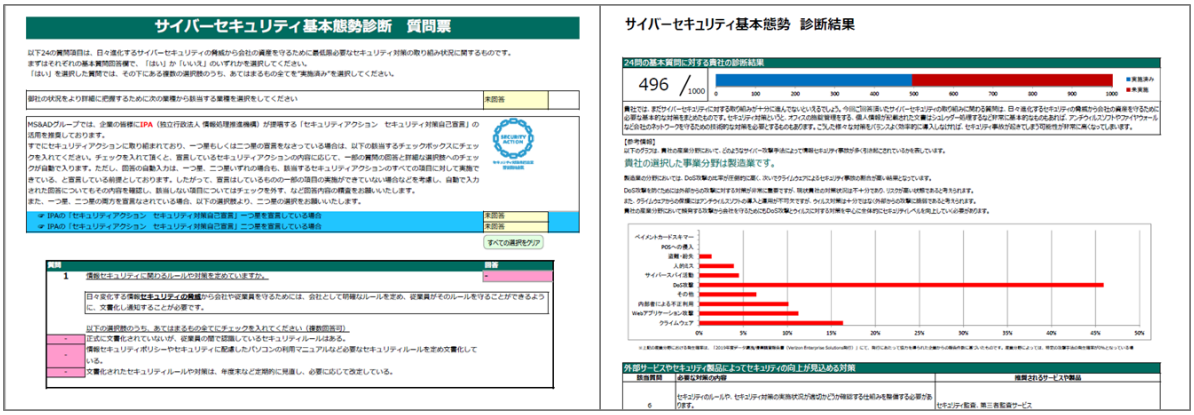
2019 年度事業で得られたデータを活用し、IPA の「5 分でできるセキュリティ自社診断」などの項目を反映させ、ベライゾンジャパン合同会社と共同開発した簡易セキュリティ診断ツールを活用した。本簡易セキュリティ診断を実施し、中小企業の実態を把握をするとともに自社の強み・弱みを明らかにする振り返りとして活用した。参加企業からは、網羅的に自社の取り組み状況を見直すきっかけとなり、自社の取り組み状況の振り返りに活用できたとの声が多かった。

500 点以上の高得点となった企業は全体の 15%程度にとどまり、無償版のアンチウイルスソフト等の導入に留まっている企業は多いことが把握できた。

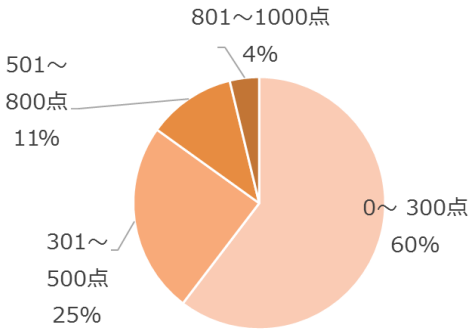
なお、本簡易セキュリティ診断は保険事業会社 2 社のホームページにて簡易版を公開している。

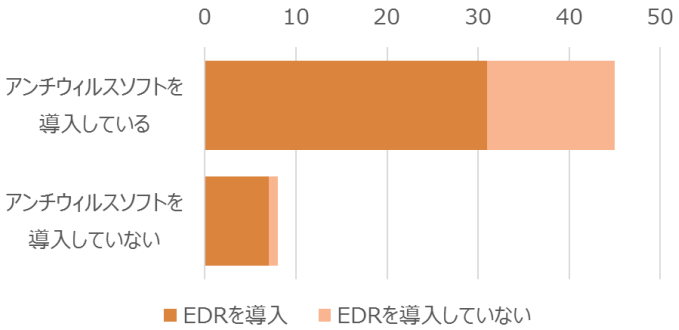
【三井住友海上】https://www.ms-ins.com/business/indemnity/pd-protector/diagnosis.html

【あいおいニッセイ同和損害保険】https://www.ad-cyber.com/diagnosis/index.html



【図６】簡易セキュリティ診断　質問票とレポートイメージ





【図７】簡易セキュリティ診断得点分布（Ｎ＝５３）　【図８】アンチウイルスソフト導入状況（Ｎ＝５３）

（３）標的型メール訓練

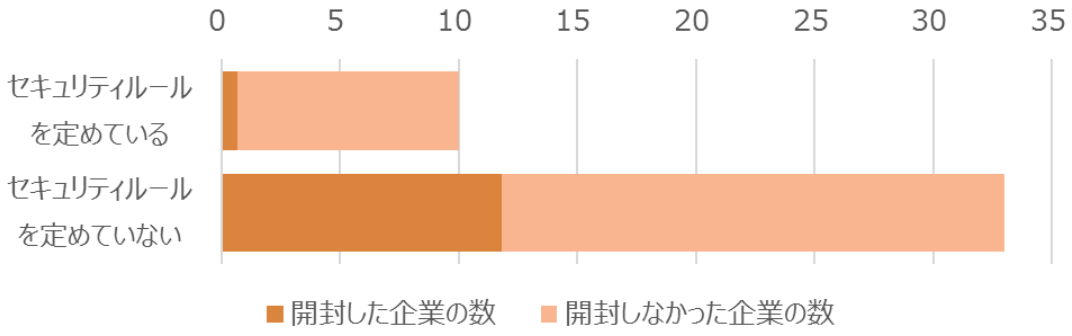
弊社の標的型メール訓練サービスを提供し、従業員のセキュリティ意識向上を図るとともに、開封率や教育状況などの実態を把握した。標的型メール訓練については、中小企業においても関心は高く、また結果に対する対策への意欲もあり、継続した実施を求める声が多かった。標的型メール訓練サービスとは、標的型攻撃を模した「訓練メール」を参加企業の従業員に送信し、その対応を個々に評価し、適切な対応が行えるよう教育機会を提供するものである。

主な実証結果は次のとおり。

・1 社における従業員（送信先）最大数の企業は「761 名」、開封者は 13 名で、メール開封率は 2%
・一方で、従業員（送信先）数「126 名」という比較的大きな会社において、メール開封率 12%
・従業員（送信先）数 10 名以上の企業で開封者 0 人の企業は 2 社のみ
・従業員（送信先）数 50 名以上の企業になると開封者 0 人の企業は 0 社

項目	開封率（企業数ベース）	開封率（送信数ベース）	備考
メール開封率（URL クリック率）	29%	7%	全社
	15%	7%	送信先 10 名以上
	5%	3%	送信先 100 名以上

【表２】訓練メール送信数別　開封率平均（５１社）



【図９】「電子メールの取扱に関わるセキュリティルールの有無」との関係（Ｎ＝５３）

図９のように、セキュリティルールを定めている企業では開封率は低いに傾向にあるが、どの企業でも誰かが不審メールを開封する可能性があり、開封率をゼロにするのは難しいことが改めてわかった。不審メールを開封しないことも大切だが、開封してしまったあとの対処が重要であり、その気づきを与えてくれるのが本訓練である。なお、弊社の標的型メール訓練サービスには、気付きを与えるだけでなく、気付きを即学びの機会にする仕組みが組み込まれている。（本稿末尾参照）

（４）ワンストップセキュリティサービス

中部電力グループ内の連携により、ワンストップセキュリティサービス（コールセンター、UTM 機器設置、駆けつけ対応までワンストップで提供できる体制を構築）を導入・運用する実証を行った。導入までに時間がかかり、実態の調査としての攻撃件数などの把握には課題が残ったが、サービス展開に必要な情報は収集することができた。

防御・検知だけでなく、初動対応までカバーすることで被害を最小化することと、有事の際の報告に活用することができ、本サービス導入企業だけでなく発注元や取引先にとっても安心できるサービスとなることを目指した。

本サービス自体は既に市場で提供されており、本サービスの OEM 提供を受けて中電シーティーアイが新たなセキュリティサービスとして提供できるかについて実証した。

弊社や中部電力ミライズは本サービスを参加企業へ案内し、申込受付や申込必要情報の聴取等の役割を担った。

本実証事業で 50 台（48 社）に新規導入し、提供オペレーションの検証やデータ収集を行った。

実証を通じて得られたデータとデータから読み取れる主なポイントは次のとおり。（表３）

- C&C[2] コールバックを UTM 設置によりブロックした。11 月～12 月の本通信は 1 企業において発生したもので、WindowsXP 端末により発生。当該端末を買い替えたことにより、以後検知せず。1 月は別企業でも発生。
- IPS（侵入防御システム）にて、防御が必要な通信を多数検知した。中小企業においても、標的となることが再確認できた。
- スパムメール対策は最も数多く検知された。無数に飛び交うメールは危険なものが多く、中小企業でもサイバー攻撃による被害を受けるきっかけとなり得ることを示している。
- ランサムウェアのブロックは 1 企業において発生した。UTM によりブロックされたことで、感染被害を防いだ。
- コールセンター対応は、C&C コールバックと UTM 機器の通信障害に関するものが主たる対応となった。
- 実証期間が短いこともあり、現地への駆けつけが必要なインシデントは発生しなかった。

2　Command and Control の略称。マルウェアに感染した PC をネットワーク経由で操作し、情報の収集や攻撃の命令を出すサーバー。

分類	件数				特記事項
	10 月	11 月	12 月	1 月	
導入数	11	28	44	50	累計
脅威イベント	243	10,342	135,186	174,356	2021 年 1 月末時点
C&C コールバック	0	3,500	626	42	
IPS（侵入防御システム）	13	2,594	24,260	51,792	
Web レピュテーション	2	30	149	180	
ウイルス/不正プログラム	2	12	19	30	
スパムメール対策	226	4,172	110,132	122,312	
ボットネット	0	0	0	0	
ランサムウェア	0	34	0	0	
不審オブジェクト	0	0	0	0	
仮想アナライザ	0	0	0	0	
機械学習型検索	0	0	0	0	
お客様通報	3	26	5	7	
現地駆けつけ	0	0	0	0	

【表３】UTM 検知状況とコールセンター等の活用状況

（５）EDR（エンドポイント監視サービス）

弊社が提供する脅威の検知・対応に重点をおいたエンドポイント監視サービス（防検サイバー：本稿末尾参照）により、ネットワーク一括監視型の UTM だけでなく、端末監視型のエンドポイント監視サービス（EDR）も導入することで多層防御によるセキュリティ強化を参加企業に提供した。EDR については導入がシンプルで、実施決定企業へのスピーディーな展開ができた。

EDR の導入に適している企業は、既に UTM など一定のセキュリティを導入している、または本実証で UTM を導入するものの、在宅勤務の増加や PC の社外持ち出しなどがあることから境界防御の限界を感じている企業である。

本サービスは、本実証事業における導入を「試用期間」と位置づけて、課題を洗い出し、また、実証期間と並行して初動対応・駆けつけサービスも含むサービスとして整備、2020 年 12 月に本サービスを正式にリリースした。

本実証事業で 50 社に新規導入し、提供オペレーションの検証やデータ収集を行った。実証を通じて得られたデータとデータから読み取れる主なポイントは次のとおり。なお、防検サイバーは導入から 1 ヵ月間は AI の学習期間としており、検知はするものの過検知が多くなる傾向があるため、アラートを送信しない仕様となっている。

- 導入から 1 ヵ月間は、過検知はあるものの、サポートが終了したメンテナンスされないソフトウェア（プラグイン）の振る舞いを検知するなどし、ユーザへの有効な注意喚起になった。
- コールセンター利用は個別アラートの内容や脅威レベルに関する問い合わせが多かった。
- 実証期間が短いこともあり、駆けつけが必要なインシデントは発生しなかった。

分類		件数				特記事項
		10 月	11 月	12 月	1 月	
導入数		8	29	50	50	累計
脅威イベント		235	3,613	4,173	2,702	2021 年 1 月末時点
	不審なプロセス起動	15	42	40	25	
	不審な通信	4	0	36	0	
	不審なファイル生成	0	0	4	2	
	不審なコマンド実行	201	3,571	3,995	2,640	
	不審な API 実行	15	0	97	34	
	不審なツール実行	0	0	0	0	
	不審なファイル操作	0	0	0	0	
	不審なレジストリ登録	0	0	0	0	
	不審なファイル読み込み	0	0	0	0	
	不審な常駐プログラム登録	0	0	1	4	
お客様通報		0	0	48	73	
現地駆けつけ		0	0	0	0	

【表４】EDR 検知状況とコールセンター等の活用状況

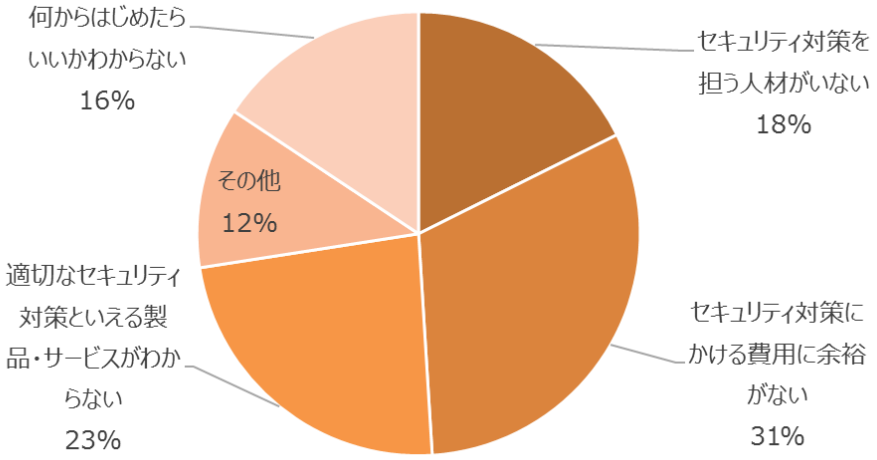
４． 実証事業の総括と今後の展望

（１）アンケートとヒアリング

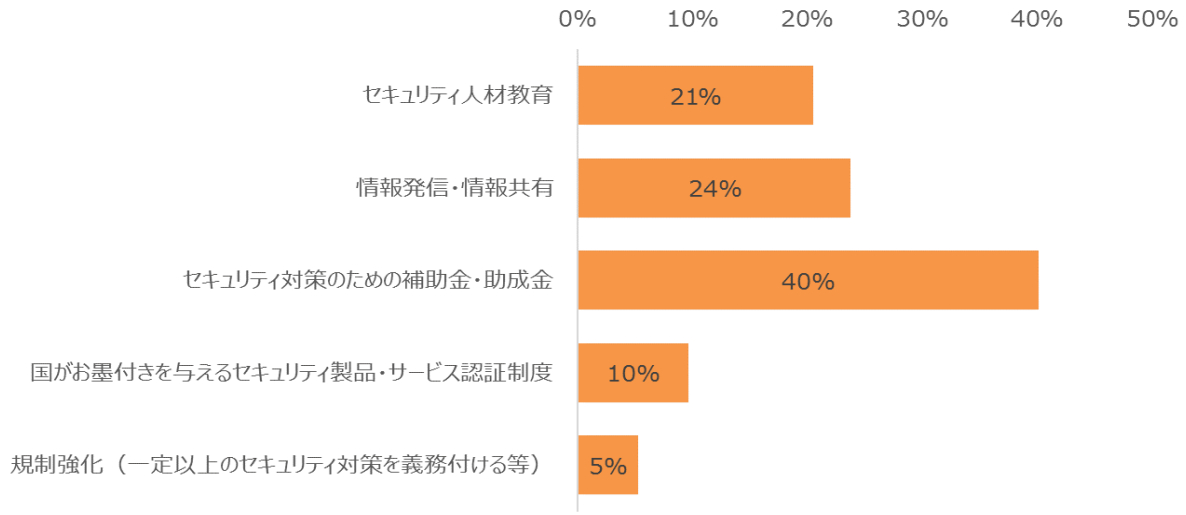
中小企業の実態調査のため、アンケートやヒアリングを実施した。図１０はアンケートの項目一つである「サイバーセキュリティ対策を進める上での課題」についての回答結果である。

最も多いのは「セキュリティ対策にかける費用に余裕がない」が 31%

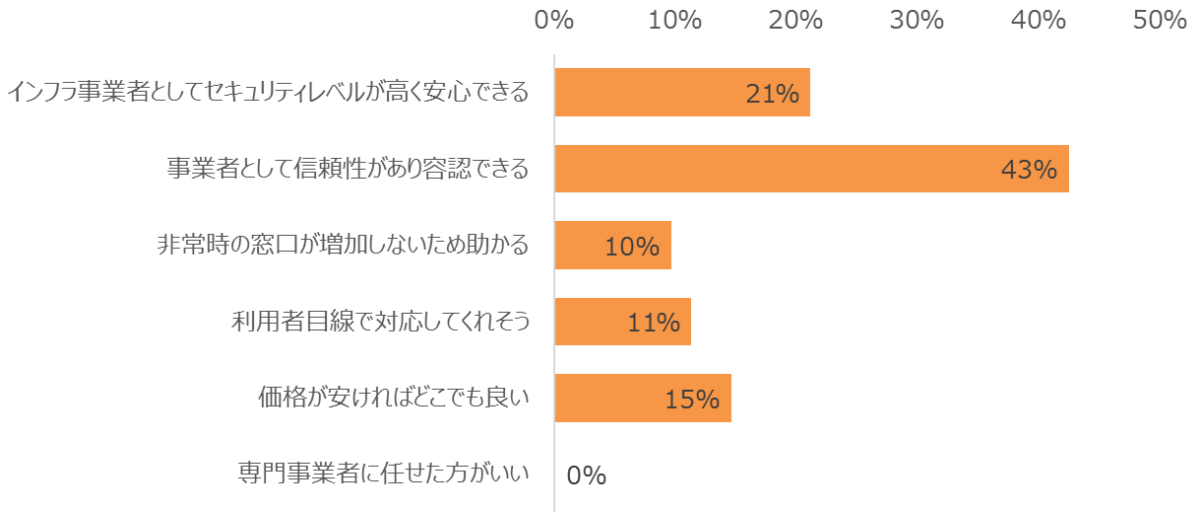
次いで「適切なセキュリティ対策と言える製品・サービスがわからない」が 23%、「セキュリティ対策を担う人材がいない」が 18%となっている。これらの 3 つの課題が全体の 7 割超を占めている。



【図１０】サイバーセキュリティ対策を進める上での課題（Ｎ＝５１）



【図１１】今後のサイバーセキュリティ対策を進めるために国に望む政策（Ｎ＝９２、複数選択）



【図１２】電力会社がこれらのサービスを提供することについて（Ｎ＝６１、複数選択）

これは本実証事業に参加した企業のみならず、多くの中小企業に当てはまる課題と考えられる。

中小企業におけるサイバーセキュリティの課題を集約すればこれらの 3 点のいずれかに行きつく一方、中小企業のサイバーセキュリティ対策への関心度、理解度、社内体制などを踏まえれば、実際の対策状況は千差万別である。

中小企業からは、国に望む政策として、これらの 3 つの課題を解消するための支援を強く要望する声が表れている（図１１）。また、本実証事業のコンセプトである「地域の重要インフラ企業を核とした中小企業向けサイバーセキュリティ普及モデル」が広く受け入れられる可能性を示している（図１２）。これらの結果から、中小企業にとって信頼できる事業者によって提供される、運用・管理サービスが付帯された、コスト面で許容できる範囲のサービスを望む声が多いことがわかる。無償のセキュリティ対策ソフトやこうした実証事業において無償で活用できる機会を得ることはとても重要との声があった。

それだけコスト面、及びそのコストを捻出するための経営層の理解などに制約があることがわかる。この点についても、中小企業の経営層に直接コンタクトできる企業からの推薦や提案があることが効果的であることも見て取れた。また、自社のやり方が正しいのか、全体を俯瞰してコンサルティングす

るサービスを望む声もあった。

更に潜在的な課題として、2019 年度事業でも見られた「無関心層の存在」が挙げられる。実証事業に参加していない膨大な数の企業の中には「サイバーセキュリティ対策には一切関心がない」という企業が少なからずあることは、実証事業への参加を募る活動においても把握できている。こうした無関心層には、国等からの情報発信やサプライチェーン上流からの取り組み強化によって、まずは関心を持ってもらうことから始めるアプローチが必要と考える。

（2）総括と今後の展望

実証後に実施したアンケートやヒアリングの結果から、「サービス提供者への信頼や安心感」が得られたという声も多く、電力会社グループとの協業モデルが受け入れられ、今回の仮説が成り立つことを確認することができた。

一方、個々のサービスに関しては、「現地支援を行うリソースが必要」や「（UTM や EDR 等のセキュリティサービスにおける）レポートのわかりやすさ向上が必要」等の指摘があり、今後サービスレベルを向上させる余地を認識するとともに、具体的な改善策の検討を既に関係者で進めている。

また、実証を通して、中小企業の抱える課題が、下記 3 点に概ね集約されることが改めて確認された。

① コスト負担（セキュリティ対策にかける費用に余裕がない）
② 製品・サービスの選定（自社の実態に即した適切な製品・サービスがわからない）
③ 人材確保（セキュリティ対策を担う人材がいない）

我々が今回の実証事業で構築した「保険会社グループと地場の重要インフラ企業との協業によるサイバーセキュリティサービス提供」モデルは、

①中小企業でも納得感のある価格帯で（コスト面）
②経産省サイバーセキュリティお助け隊サービスも見越した（適切な製品・サービス面）
③管理サービス付きサイバーセキュリティサービス（人材面）

を、中小企業経営者と接点が多く、信頼関係を構築している重要インフラ企業が提供していくことにより、上記の中小企業が抱える課題を解消し、中小企業のサイバーセキュリティレベルを引き上げる持続可能なモデルになり得ることが確認できた。

現状では、中小企業のサイバーセキュリティ対策（サイバー保険への加入を含む）はまだ道半ばである。だからこそ「安心と安全を提供する」損害保険会社グループとして、今回の実証で大きな役割を担った中電グループのような地域インフラ企業（中核企業）や、地域コミュニティと連携し、サイバー保険の提供にとどまらない役割を果たしていくことの重要性を再認識した。

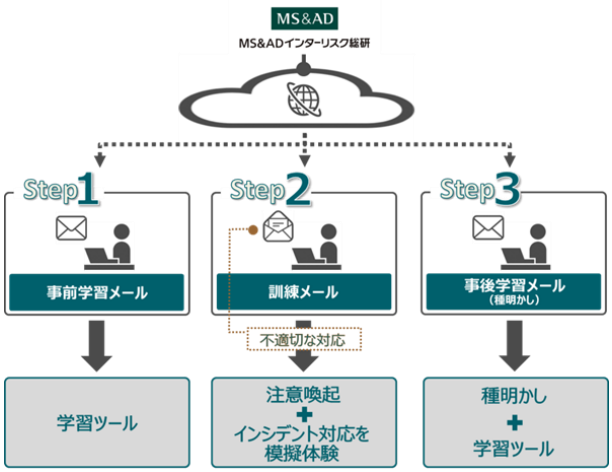
今後は中小企業へのサイバーセキュリティ対策の普及を図るため、本モデルをブラッシュアップし、全国への横展開を目指すとともに、本事業を通じて組成された「サイバーセキュリティお助け隊サービス」制度の活用も含め、引き続き国や関係機関等の支援をいただきつつ、取り組みを強化していく。

本稿が、中小企業におけるサイバーリスク実態と直面している課題の把握、およびセキュリティ強化けた取組の一助となれば幸いである。

ＭＳ＆ＡＤインターリスク総研株式会社
新領域開発部 サイバーリスク室
上席コンサルタント　槇　健介

ＭＳ＆ＡＤインターリスク総研株式会社では、標的型攻撃を巧妙に模した「訓練メール」を訓練参加者に送信し、その対応を個々人に評価する「標的型メール訓練サービス」を提供しています。

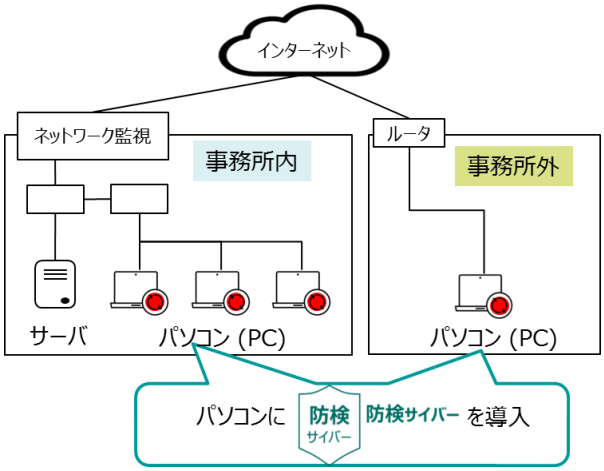
本サービスは、行動経済学の代表的な考え方である「ナッジ」を活用することで、「学び」のモチベーションを上げることを志向するとともに、訓練結果報告書に基づいて従業員個々人の不審なメールに対するリスク感度や学習の深度に応じたフォローアップを行うことができます。



【学習コンテンツのイメージ】

また、弊社では、脅威の侵入を素早く検知し、被害を最小限に止める次世代エンドポイントセキュリティ「EDR」 と、24 時間 365 日の監視がパッケージとなったセキュリティサービス「防検サイバー」を提供しています。

本サービスは PC に EDR ソフトを導入し、インターネットを経由して AI やセキュリティアナリストが監視を行います。その為、自宅や外出先でもセキュリティ監視に影響はなく、テレワークを行う企業に適したサービスとなっています。



ＭＳ＆ＡＤインターリスク総研株式会社は、ＭＳ＆ＡＤインシュアランス グループのリスク関連サービス事業会社として、リスクマネジメントに関するコンサルティングおよび広範な分野での調査研究を行っています。
サイバーリスク・情報セキュリティに関するコンサルティング・セミナー等を実施しております。
コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問合せ先、またはあいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
ＭＳ＆ＡＤインターリスク総研株式会社
新領域開発部　サイバーリスク室
千代田区神田淡路町2-105 TEL:03-5296-8961／FAX:03-5296-8941
https://www.irric.co.jp/