別紙

サイバーセキュリティお助け隊

実証参加企業事例集

この事例集は、「令和２年度中小企業サイバーセキュリティ対策支援体制構築事業（サイバーセキュリティお助け隊事業）」に参加した企業のうち、７社へヒヤリングを行い、実証参加企業が実施した実証内容、制度・施策に関する意見、これまでの取組みと今後についてまとめたものです。

事例掲載企業一覧

	地域	業種	従業員数	資本金
A 社	愛知県	卸売業	101～200 名	1 億円以下
B 社	広島県	製造業	201-300 名	1 億円以下
C 社	福島県	卸売業・小売業	6 名	600 万円
D 社	埼玉県	製造業	16 名	1,000 万円
E 社	千葉県	製造業	10 名強	3,000 万円
F 社	岩手県	製造業	201 名～300 名	5,000 万円
G 社	長野県	製造業	21～50 名	3,000 万円以下

A 社　愛知県		
業種	卸売業	＜サマリ＞ 取引先からの要請に応えるために必要なセキュリティ対策について、お助け隊事業のサービスを活用し、継続的なセキュリティ対策の向上を推進している。セキュリティ課題を明確にしつつ、今後 3 か年計画をたてて更なるセキュリティ推進を検討している。
従業員数	101～ 200 名	
資本金	1 億円以下	
セキュリティ対策に関する取引先からの要求	有	
過去に経験したインシデント	無	
SECURITY ACTION の宣言・活用状況	二つ星	
■参加動機		
実証事業への参加動機、期待	昨年度に引き続いてお助け隊事業に参加。今年度は、従業員のセキュリティ意識向上、組織のセキュリティ対策の高度化を期待した。	
■今回の実証事業で実施した対策と結果		
実施した対策（サービス内容）及び結果（監視、駆けつけ有無、診断結果等）	◆EDR アラートは発生したが、インシデントには至らなかった。アラートは、サポート切れしたソフトウェアであり、社内で削除することを徹底した。 ◆標的型攻撃メール クリック率は約 4%で低い方であった。クリックした従業員でも、総務に対応を確認する等、開いた後でも社内ルールに則り適切に対応するケースが見られた。 ◆簡易セキュリティ診断 スコアは高い方に位置している。診断結果を踏まえ、セキュリティの対応方針等について検討を行った。	
■得られた効果		
サービス活用のポイントと組織において得られた効果	今回の実証事業では標的型攻撃メール訓練では、メール送信のみの対応であったが、自主的に、事前学習、事後学習を計画し、お助け隊事業に相談した上で自社にて教育研修を準備・実施した。 EDR 設置の検知では、インシデントまではいかないがアラートが上がったことから、サポート切れ製品についてはアンインストールするなど、セキュリティ対策で欠けていた対応について改善した。 今回の実証事業の結果を踏まえて、さらに社内セキュリティ対策推進のための材料とするなどお助け隊事業の製品・サービス利用について自社内で位置づけを決めて積極的に実証事業に参加した。 現状のネットワーク構成が複雑で管理しきれていないため、ネットワーク調査や整備については引き続き今後の課題としている。	

■今後のセキュリティ対策	
実証を通じて得られた結果を踏まえた、今後のセキュリティ対策推進の考え方や計画	IPA の情報セキュリティマネジメント指導業務も利用しており、サプライチェーンの上流への対応を行うため、引き続き、セキュリティ対策の推進を進めている。 今後 3 か年計画を立て、教育メニューとして標的型攻撃メール訓練を組み込んだ。EDR についても、必要性を認識し導入検討したいという要望があった。 UTM の設置について、ネットワーク構成の整理など自社の課題を克服した後、費用対効果を考慮して設置を検討している。 セキュリティ事業者と対応を検討できる人材は必要であるが、セキュリティ対策そのものは外部の信頼できる事業者を活用するなどの方針を決め、今後の施策を進めている。

B 社　広島県		
業種	製造業	＜サマリ＞ 取引先からの要求としてセキュリティ対策が始まり、現実的な事業継続上のビジネスリスクとして認識された。実証により、客観的評価、業界における位置づけを把握でき、経営層の巻き込みについて効果が得られた。さらに、今後の社内セキュリティ施策の推進に活かしていきたい。
従業員数	201-300 名	
資本金	１億円以下	
セキュリティ対策に関する取引先からの要求	要求は始まりつつあり、セキュリティの専任担当者を配置するように求められている。	
過去に経験したインシデント	生産や取引先への影響レベルでは発生していないが、社内的な損害（標的型攻撃を受けたり、情報漏洩等）は多少発生した。専門家までは依頼していないため、本来の被害には気づけていないという可能性もゼロではない。	
SECURITY ACTION の宣言・活用状況	無	
■参加動機		
実証事業への参加動機、期待	・自社セキュリティリスクを第 3 者的な視点から可視化できる。 ・同業他社と比較した、自社の取り組み状況が把握でき、経営層へ課題認識を持ってもらうために効果的に活用したい。	
■今回の実証事業で実施した対策と結果		
実施した対策（サービス内容）及び結果（監視、駆けつけ有無、診断結果等）	◆問診：求められている合格ラインに対して、マネジメント面・技術面の双方で合格ラインに達しておらず、同業と比較しても、取り組みが遅れていることが明らかになり、どのカテゴリを対策すべきかが明らかになった。 ◆外部診断：総合ランクは A だが、一部項目が A ではないため、詳細レポートを確認し、対応を検討したい。 ◆内部診断：具体的な脆弱性が数件見つかったため、委託先に対して確認を行い対応を検討する。 ◆マルウェア対策診断：exe ファイルの実行が可能となっている実態が明らかになったが、部門によっては生産に活用しているケースがあり、IT 部門として強制できていない。今後検討したい。 ◆不正通信監視：インシデント発生無し。不正なプログラムを 2 件ブロック、不正な URL（Web 広告や詐欺サイト）へのアクセスを 300 件程度ブロックされていた。	

■得られた効果	
サービス活用のポイントと組織において得られた効果	セキュリティ対策の必要性は認識しているが、予算化がしにくいのが実情である。今回の結果から必要性は改めて認識できたため、UTM を含むセキュリティソリューションに関して、自社のシステム構成に合わせて、効果が最も上げられる対策を限られた予算内で実行していきたい。 問診、各種診断について：今後取引先からもセキュリティ対策に対する要求が高まる状況の中で、今回のような診断によって、自社の対策状況が第 3 者的に可視化され、自身がどのようにアクションしていくかについては、非常に有益と感じている。一方で診断については、対策ではないため、我々中小企業にとっては、予算化するのにハードルが高いのが実情であり中々取り組むことが難しかった。 今回の実証を通して、実施することの重要性は再認識できたため、簡易診断として年 10 万円以下(Basic レベル)であれば、取り組めると思う。 不正通信監視について：必要性は理解しているが、評価がしにくい。セキュリティ対策は「何か起きた時にやっていた良かった。」と感じる一方で、「何も起きなかったときはこの投資に意味があるのか」と感じられるため、担当者としては必要と認識しても、経営者目線だと生産の利益にはなりにくいが、コストになるという考えになってしまう。今回のように各種診断を通じて第 3 者的に意見を頂き、また同業の対応状況が見えることで、経営層へのアプローチもやりやすくなると感じている。
■今後のセキュリティ対策	
実証を通じて得られた結果を踏まえた、今後のセキュリティ対策推進の考え方や計画	今回の営みは非常に有益であった。今回の個社別レポートは内容を確認し、経営層にも上げ、自社にとって効果的な対策から予算化して取り組んでいきたい。事業経営上の課題として認識されたことにより、経営層の巻き込みという観点で前進した。

C 社　福島県		
業種	卸売業・小売業	＜サマリ＞ 過去にセキュリティインシデントがあり、セキュリティ対策について、何をどこまで実施すべきかがわからなかったが、お助け隊事業において製品・サービスを導入することで知識を深め、今後の対策について一歩を踏み出すことができた。
従業員数	6 名	
資本金	600 万円	
セキュリティ対策に関する取引先からの要求	不明	
過去に経験したインシデント	有	
SECURITY ACTION の宣言・活用状況	無	
■参加動機		
実証事業への参加動機、期待	過去にサイバー攻撃を受けており、どのような対策をすべきか検討するために、製品の性能や効果等を確認するため。	
■今回の実証事業で実施した対策と結果		
実施した対策（サービス内容）及び結果（監視、駆けつけ有無、診断結果等）	◆EDR：ランサムウェアの発見と駆除　２件、マルウェアの発見と駆除　２件、PUA の発見と駆除　１件 ◆標的型攻撃メール訓練：開封検知　１件 ◆WEB 診断：特になし	
■得られた効果		
サービス活用のポイントと組織において得られた効果	従来のアンチウイルスソフトと比較し、EDR が高性能だと実感できた。ただし、アラートの際の表示内容が専門的であり、高性能な製品は自社での運用が困難であると感じた。後にその運用も任せられるということを知り安心できた。実際に製品を利用できたことは、セキュリティ対策を検討する上で良いきっかけとなった。	
■今後のセキュリティ対策		
実証を通じて得られた結果を踏まえた、今後のセキュリティ対策推進の考え方や計画	お助け隊事業で利用した中小企業向け EDR については、正式サービス化を前提に導入を検討している。また、現状 PC 等の資産管理やネットワークの構成管理を行っていないので、社内の資産管理の運用ルール等も併せて検討する。 セキュリティ計画はまだ明確ではないが、まず製品導入・運用を行ってみて、気づきがあれば今後の計画に採り込んでいく予定である。	

D 社　埼玉県		
業種	製造業	<サマリ> 情報セキュリティ規定の明確化及び詳細化したものを明文化するステップについて、実証を通じて明確にできた。セキュリティ対策に一歩が踏み出せた。
従業員数	16 名	
資本金	1,000 万円	
セキュリティ対策に関する取引先からの要求	無	
過去に経験したインシデント	無	
SECURITY ACTION の宣言・活用状況	無	
■参加動機		
実証事業への参加動機、期待	情報セキュリティ規定の明確化及び詳細化したものを明文化するステップを明確化できる事を期待した。	
■今回の実証事業で実施した対策と結果		
実施した対策（サービス内容）及び結果（監視、駆けつけ有無、診断結果等）	◆セキュリティ対策の可視化： セキュリティ対策の診断結果のスコアは高めであったが、全体的な視点が欠けていることが明らかになった。	
■得られた効果		
サービス活用のポイントと組織において得られた効果	情報セキュリティ規定の明確化及び詳細化したものを明文化するにあたり、何をどんなステップで実現するかを実証を通じて確認できた。	
■今後のセキュリティ対策		
実証を通じて得られた結果を踏まえた、今後のセキュリティ対策推進の考え方や計画	情報セキュリティ規程により、従業員への理解を深め、リテラシーの向上を図って行きたい。対外的にも、どういったセキュリティ対策を実施しているかが、アピールになることが分かった。具体的な対策は、今後セキュリティ専門家と相談して、検討を進めていきたい。	

E 社　千葉県		
業種	製造業	＜サマリ＞ セキュリティ対策の意識は高く、お助け隊事業の提供する製品・サービスを複数体験し、自社の対策に反映できた。また、対外的にセキュリティ対策していることをアピールすることも必要と認識できた。
従業員数	10 名強	
資本金	3000 万円	
セキュリティ対策に関する取引先からの要求	無	
過去に経験したインシデント	無	
SECURITY ACTION の宣言・活用状況	無	
■参加動機		
実証事業への参加動機、期待	情報セキュリティ対策の必要性を認識していたところ、当事業参加の打診があり、外部の目で点検してもらう良いタイミングと捉えて参加した。社内でも進めていたセキュリティ対策を確認したいという要望があった。	
■今回の実証事業で実施した対策と結果		
実施した対策（サービス内容）及び結果（監視、駆けつけ有無、診断結果等）	◆UTM 監視：不審メールの侵入などは発生していないことを確認した。インシデント発生時の駆けつけ支援も行っておらず、特に問題ないことを確認した。 ◆専門家によるヒアリングと自社診断：セキュリティリスクの存在を認識できた。5 分でできる診断でのスコアは比較的高めであった。 ◆訓練メール：通常通り不審メールとして開かずに削除できた。	
■得られた効果		
サービス活用のポイントと組織において得られた効果	SA 二つ星宣言により、ロゴマークを名刺・会社案内に使用することを決めた。専門家による外部支援の必要性を認識し、専門家派遣事業を申請して二つ星宣言に取り組むこととなった。	
■今後のセキュリティ対策		
実証を通じて得られた結果を踏まえた、今後のセキュリティ対策推進の考え方や計画	情報セキュリティ管理担当者設置、情報セキュリティ規程策定、等の体制を整備する。セキュリティ製品を導入する上でも、体制作りから、目標を明確にして取り組んでいきたい。	

F 社　岩手県		
業種	製造業	＜サマリ＞ 取引先からの要求もあり、以前からセキュリティ対策を実施しているが、自社の対策やリスクの評価ができていなかったため、お助け隊事業を利用した。 実証を通じ、セキュリティリスクと対策状況が把握・評価でき、今後のセキュリティ対策として実施すべき事項を明確にできた。
従業員数	201 名- 300 名	
資本金	5,000 万円	
セキュリティ対策に関する取引先からの要求	商品の出荷先データを取引先から受領する場合、ネットワークセキュリティや個人情報保護体制の整備状況等の調査がある。	
過去に経験したインシデント	無	
SECURITY ACTION の宣言・活用状況	一つ星宣言済み。　今後、二つ星の宣言に関しても前向きに検討する。	
■参加動機		
実証事業への参加動機、期待	自社でセキュリティ対策状況を把握できず、どこまで対策するのが適切か判断が難しかったため、実証事業に参加し客観的な対策状況の評価やリスク評価を行うことを希望した。クライアント PC に対しては、インターネット及びメールに対するセキュリティを施しているが、実際の攻撃やリスクがわからない状況だったので、ネットワーク監視を行うこととした。	
■今回の実証事業で実施した対策と結果		
実施した対策（サービス内容）及び結果（監視、駆けつけ有無、診断結果等）	◆簡易セキュリティ診断 ・診断スコアは、参加企業において平均的であった。 ◆ネットワーク監視 ・不審な IP アドレスからサーバへの偵察行為（不正侵入が行われる前の情報収集の疑い）があった。対策として、ルータのファイアウォール機能で、アクセスをブロックした。 ・社内のクライアント端末から、アドウェアに感染していると考えられる通信を確認。不審な URL へのアクセスが行われる可能性があった。対策として、古い端末だったため、端末の入替を行った。 ・インシデント通報は 2 件（緊急性は無し）、駆け付け回数は 0 件であった。	
■得られた効果		
サービス活用のポイントと組織において得られた効果	お助け隊事業を通じて、自社のセキュリティの対策状況を理解し、簡易診断結果から必要となる対策について検討することができた。 ネットワーク上の端末管理について、今後強化していく必要性を認識できた。	

■今後のセキュリティ対策	
実証を通じて得られた結果を踏まえた、今後のセキュリティ対策推進の考え方や計画	ネットワークに接続する端末の状態を把握し、最新の状態に更新するため、管理部門で集中管理する体制が必要と感じた。また、実証事業を通じて、外部からの侵入に対する継続的な監視体制も必要と考える。 現時点では、具体的なツール導入に向けて検討を進めている訳ではないが、価格次第では、今回の実証で設置した監視センサー、及びインシデント疑いの際の通報サービスの継続利用を検討したい。

G 社　長野県		
業種	製造業	＜サマリ＞ 緊急対処が必要な脅威レベルではないが、業務上好ましくないアプリが導入されていることが想定され、パソアコンの脆弱性も可視化できたことから、社内への現実的な啓発活動に繋げ、今後は具体的な計画も検討していきたい。
従業員数	21-50 名	
資本金	3,000 万円以下	
セキュリティ対策に関する取引先からの要求	無	
過去に経験したインシデント	無	
SECURITY ACTION の宣言・活用状況	無	
■参加動機		
実証事業への参加動機、期待	「長野県テクノ財団」からの広報活動がきっかけで参加した。 セキュリティ対策状況が十分に可視化できていなかったため、セキュリティ課題と、必要な対応（規定の整備、仕組み、体制、知識等）が検討できることを期待した。	
■今回の実証事業で実施した対策と結果		
実施した対策（サービス内容）及び結果（監視、駆けつけ有無、診断結果等）	◆意識調査アンケート：回答 ◆セキュリティ対策整備状況診断：診断済 ◆パソコンの脅威検知：業務上好ましくないアプリの導入状況が把握できた。 ◆パソコンの脆弱性監視：パソコン上の脆弱性が把握できた。 ◆工場の IT 機器見える化：OA 系とネットワークが分離できていることが確認できた。	
■得られた効果		
サービス活用のポイントと組織において得られた効果	・導入済みのウイルス対策ソフトでは検知できないマルウェア（100 件程度）と危険度が把握でき、グレーゾーンのマルウェアもあると認識を新たにすることができた。また、グレーゾーンとはいえ、マルウェアが社内パソコンに侵入した事実を認識できた。 ・感染行為が想定された。（フリーソフトダウンロード時など） ・OS のアップデートの停滞状況の見える化ができた。 ・社内 IT 管理の課題が可視化できた。	
■今後のセキュリティ対策		
実証を通じて得られた結果を踏まえた、今後のセキュリティ対策推進の考え方や計画	・実証結果により、不十分なセキュリティ対策を認識でき、今後の方向性を検討することができた。 ・実証から判明したセキュリティ課題について、社員向けに現実味のある啓発を行うことで、よりセキュリティ対策を推進していきたい。	