経済産業省・
IPA（独立行政法人情報処理推進機構）

【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のご紹介

２０２０年９月

株式会社ＢＣＣ

目次

- 本実証事業について
- 本実証事業に対する弊社の取り組みについて
- ご提供する内容について
- ご参加頂ける企業様へ

本実証事業について

IPAサイバーセキュリティお助け隊事業の背景

中小企業の実情

●企業の危機意識が十分でない
●サプライチェーンに参加する地域の中小企業であっても、例外なくサイバー攻撃の脅威にさらされていることが明らかになった

昨年度の実証事業

令和元年度　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
・全国８地域（北海道、四国、九州除く）

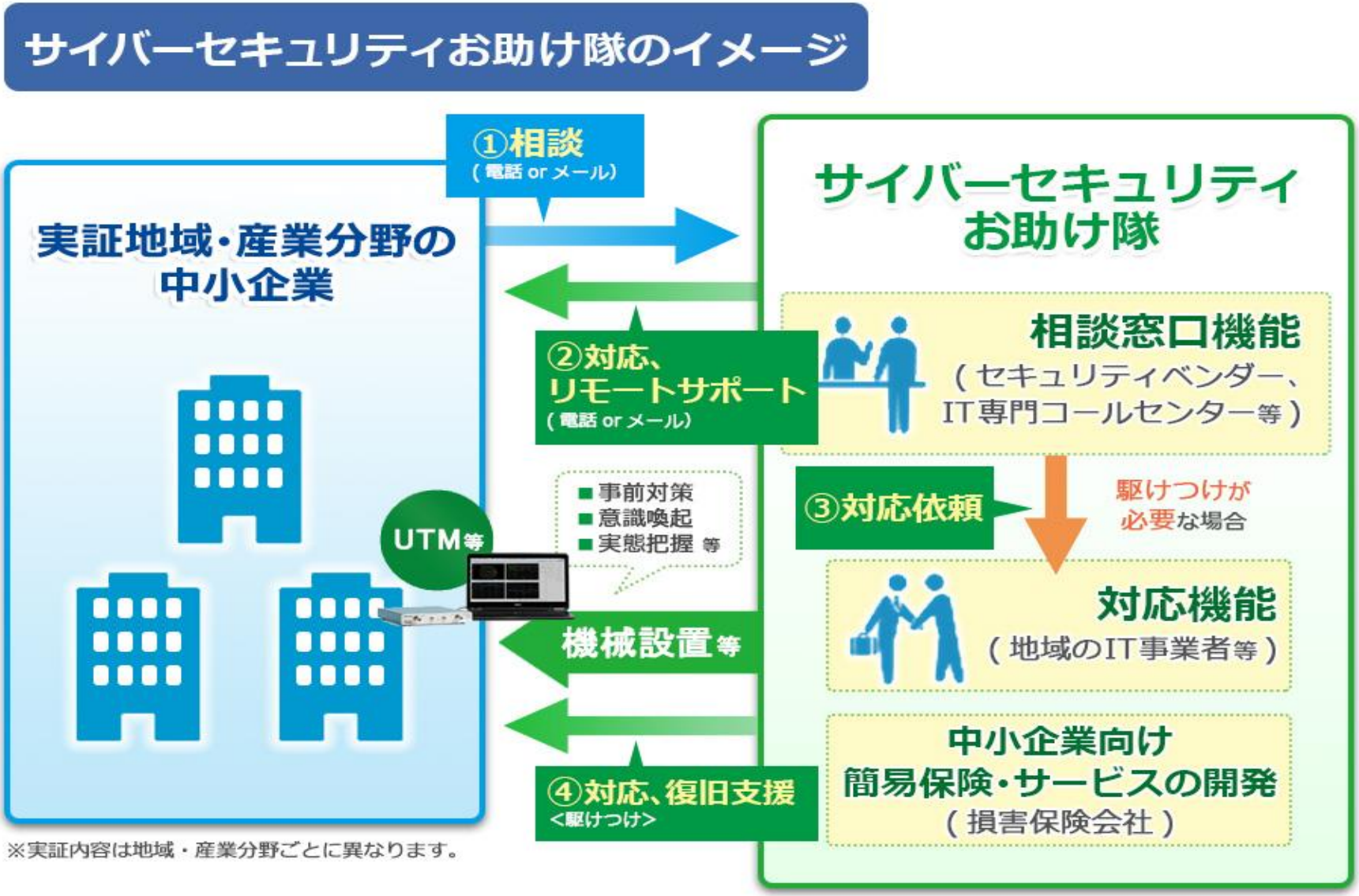
実証結果の課題

①地域特性、産業特性などの考慮が必要である
②人手不足による導入負荷を下げる必要がある
③事後対策だけでなく事前対策も必要である
④支援内容のスリム化によるコスト低減が必要である

今回の実証事業

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
・全国１５事業者（実施地域、規模も事業者が提案）
損害保険会社、ITベンダー、地元の団体などと連携して、中小企業の実態にあったセキュリティ対策を定着させていく

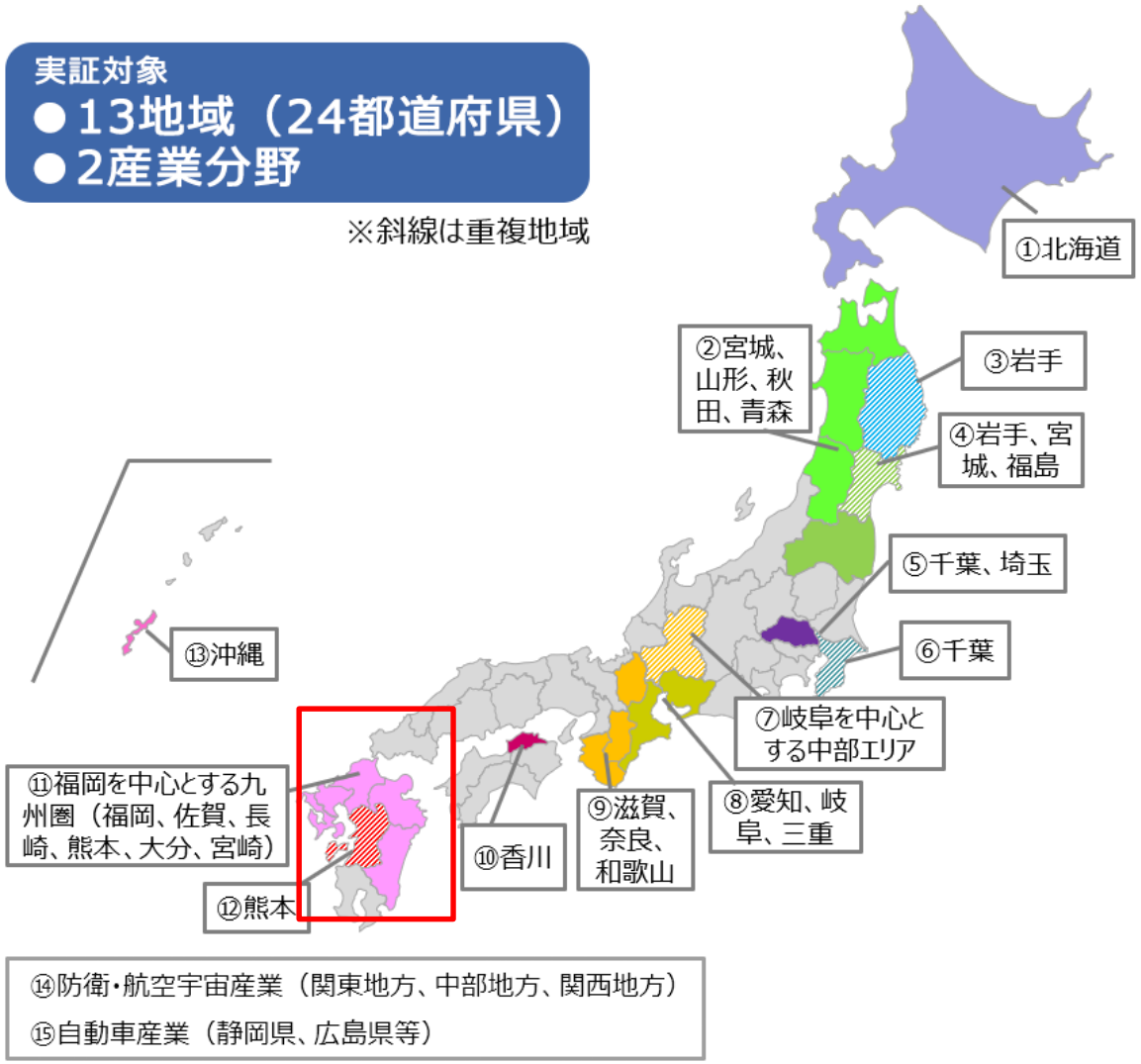
IPAサイバーセキュリティお助け隊事業イメージ



IPAサイバーセキュリティお助け隊事業実証対象

実証対象
- **13地域（24都道府県）**
- **2産業分野**

※斜線は重複地域

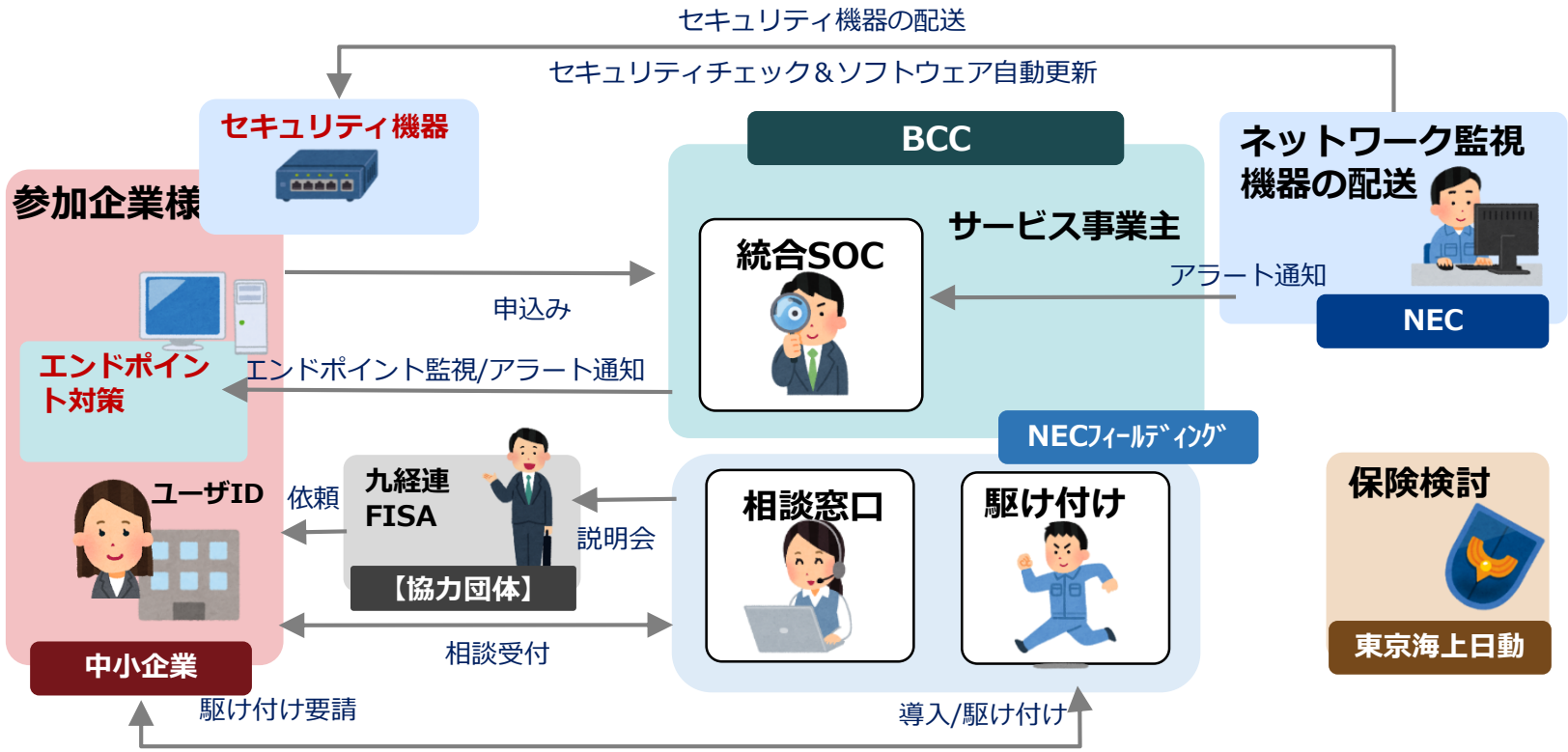


⑭防衛・航空宇宙産業（関東地方、中部地方、関西地方）
⑮自動車産業（静岡県、広島県等）

地域	実施主体
①北海道	東日本電信電話株式会社
②宮城、山形、秋田、青森	東北インフォメーション・システムズ株式会社
③岩手	富士ソフト株式会社
④岩手、宮城、福島	株式会社デジタルハーツ
⑤千葉、埼玉	富士ゼロックス株式会社
⑥千葉	SOMPOリスクマネジメント株式会社
⑦岐阜を中心とする中部エリア	MS&ADインターリスク総研株式会社
⑧愛知、岐阜、三重	名古屋商工会議所
⑨滋賀、奈良、和歌山	大阪商工会議所
⑩香川	高松商工会議所
⑪福岡を中心とする九州圏（福岡、佐賀、長崎、熊本、大分、宮崎）	株式会社BCC
⑫熊本	西日本電信電話株式会社 熊本支店
⑬沖縄	沖電グローバルシステムズ株式会社

産業分野	実施主体
⑭防衛・航空宇宙産業（関東地方、中部地方、関西地方）	株式会社PFU
⑮自動車産業（静岡県、広島県等）	東京海上日動リスクコンサルティング株式会社

今回の弊社事業体制



BCC
- サービス提供事業主
- エンドポイントとネットワークの統合SOC
- 参加企業管理

九経連・FISA
- 地域での参加企業募集支援

NECフィールディング
- 相談窓口
- 駆け付け

東京海上日動
- セキュリティ簡易保険の検討

NEC
- セキュリティ機器提供・配送
- ネットワーク監視
- 技術支援

実証事業参加へのお願い

中小企業のサイバーセキュリティ対策強化は、

我が国の重要な課題

テレワークへの
サイバー攻撃
増大

国の規定
ガイドライン

ガイドライン

取引先企業
からの
対策依頼

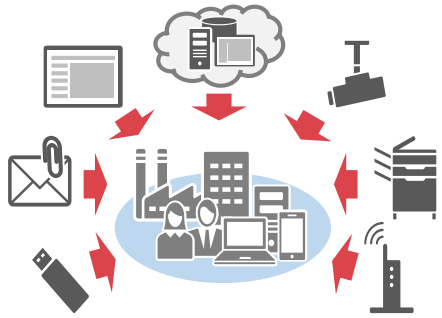
実証事業によるセキュリティ対策のお助け

本実証事業に対する
弊社の取り組みについて

セキュリティに関する世の中の状況

組織の重要情報や資産を脅かすセキュリティ上の脅威は日々増え続けており攻撃の手口も多様化、巧妙化

内閣サイバーセキュリティセンター（NISC）から「政府機関等の情報セキュリティ対策のための統一基準群」が改正



2．改定のコンセプト

（1）将来像を見据えたサイバーセキュリティ対策の体系の進化

・新たな防御技術の導入、システムによる自動化等により、サイバーセキュリティ対策を新たなレベルに進化させることができる時期に来ていると認識。

①エンドポイント検知による未知の不正プログラムの被害の未然防止／拡大防止

・未知の不正プログラムに対しては、従来のシグネチャ型の既知の不正プログラム検知方式では対応できず、境界監視により不正通信を検知した際はインシデント発生後とならざるを得ない。近年の技術進歩により、不正プログラムが動作する内部（端末等のエンドポイント）での挙動を検出することにより、インシデントの発生の未然防止や被害拡大防止の機能が向上してきている。

・このような機能の導入は、「監視」機能の高度化との視点でとらえることもできる。

出典：政府機関等の情報セキュリティ対策のための統一基準群の見直し（骨子）
https://www.nisc.go.jp/conference/cs/dai17/pdf/17shiryou03.pdf

1．将来像を見据えたサイバーセキュリティ対策の体系の進化

《主な内容》

✓ 端末、サーバにおける『未知の不正プログラムの検知／実行の防止の機能の導入』
⇒未知の不正プログラム対策を「侵入後の検知」から「感染の未然防止」へ、「境界監視」に加え「プログラムが動作する内部」へ進化

✓ ソフトウェア等の情報を自動的に収集する『IT資産管理ソフトウェアの導入』
⇒脆弱性の所在の効率的な把握を可能とし、ゼロデイ攻撃等のソフトウェアの脆弱性を狙った攻撃に迅速に対応

✓ 情報へのアクセス制御機能として、『デジタル著作権管理による方式』を導入
⇒万が一ファイルが外部に流出しても、オンプレミス※／クラウドを問わず記録された内容の漏洩を防止し、ダメージを無効化

※オンプレミス：[情報システムのハードウェアを自ら調達し主体的に管理する運用形態]

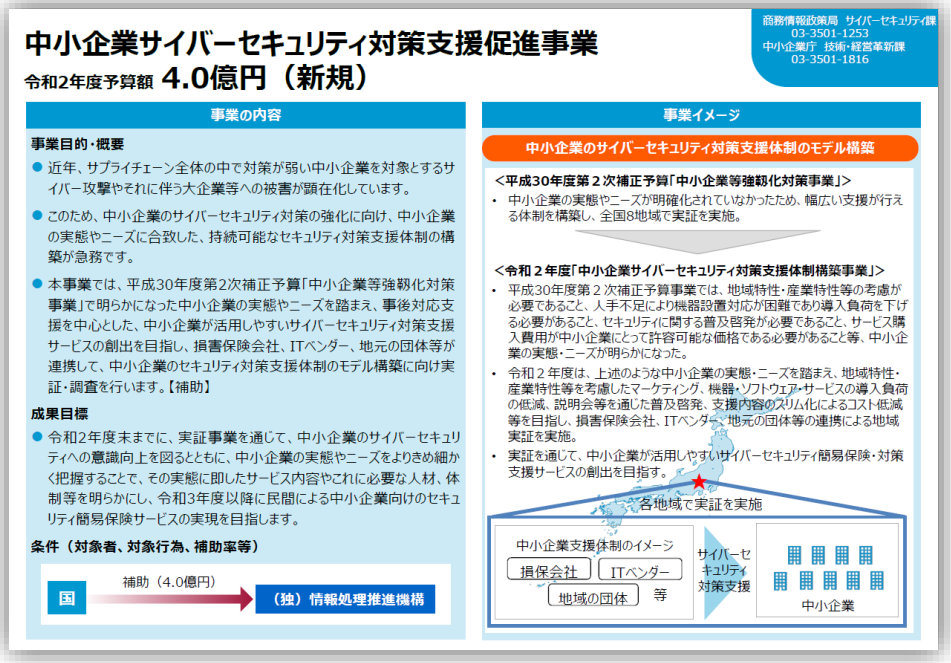
出典：NISC「政府機関等の情報セキュリティ対策のための統一基準群の見直し（案）」
https://www.nisc.go.jp/active/general/pdf/gaiyo2018.pdf

九州地区でもセキュリティ事故が発生、狙われるのは大企業だけではない

サイバーセキュリティお助け隊事業参加のポイント

九州地域の企業様が安心安全なICT環境が利用できるようになることを目的として参加企業様の現状のセキュリティレベルを把握し、IPAが定める一定の基準を満たしたセキュリティサービスを検討・構築することを目指します

1. セキュリティ診断と対策製品導入による現状のセキュリティレベルの把握
2. 参加企業様の負担を最小限としたサービスの導入と実運用にむけた運用検証
3. 利用しやすいセキュリティ保険の検証
4. 事故発生時の駆け付け作業のリモート対応について有効性を検証



中小企業サイバーセキュリティ対策支援促進事業

令和2年度予算額 4.0億円（新規）

商務情報政策局 サイバーセキュリティ課 03-3501-1253
中小企業庁 技術・経営革新課 03-3501-1816

事業の内容

事業目的・概要

- 近年、サプライチェーン全体の中で対策が弱い中小企業を対象とするサイバー攻撃やそれに伴う大企業等への被害が顕在化しています。
- このため、中小企業のサイバーセキュリティ対策の強化に向け、中小企業の実態やニーズに合致した、持続可能なセキュリティ対策支援体制の構築が急務です。
- 本事業では、平成30年度第2次補正予算「中小企業等強靭化対策事業」で明らかになった中小企業の実態やニーズを踏まえ、事後対応支援を中心とした、中小企業が活用しやすいサイバーセキュリティ対策支援サービスの創出を目指し、損害保険会社、ITベンダー、地元の団体等が連携して、中小企業のセキュリティ対策支援体制のモデル構築に向け実証・調査を行います。【補助】

成果目標

- 令和2年度末までに、実証事業を通じて、中小企業のサイバーセキュリティへの意識向上を図るとともに、中小企業の実態やニーズをよりきめ細かく把握することで、その実態に即したサービス内容やこれに必要な人材、体制等を明らかにし、令和3年度以降に民間による中小企業向けのセキュリティ簡易保険サービスの実現を目指します。

条件（対象者、対象行為、補助率等）

国 → 補助（4.0億円） → （独）情報処理推進機構

事業イメージ

中小企業のサイバーセキュリティ対策支援体制のモデル構築

<平成30年度第２次補正予算「中小企業等強靭化対策事業」>

- 中小企業の実態やニーズが明確化されていなかったため、幅広い支援が行える体制を構築し、全国8地域で実証を実施。

<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」>

- 平成30年度第２次補正予算事業では、地域特性・産業特性等の考慮が必要であること、人手不足により機器設置対応が困難であり導入負荷を下げる必要があること、セキュリティに関する普及啓発が必要であること、サービス購入費用が中小企業にとって許容可能な価格である必要があること等、中小企業の実態・ニーズが明らかになった。
- 令和２年度は、上述のような中小企業の実態・ニーズを踏まえ、地域特性・産業特性等を考慮したマーケティング、機器・ソフトウェア・サービスの導入負荷の低減、説明会等を通じた普及啓発、支援内容のスリム化によるコスト低減等を目指し、損害保険会社、ITベンダー、地元の団体等の連携による地域実証を実施。
- 実証を通じて、中小企業が活用しやすいサイバーセキュリティ簡易保険・対策支援サービスの創出を目指す。

各地域で実証を実施

中小企業支援体制のイメージ：損保会社／ITベンダー／地域の団体 等 → サイバーセキュリティ対策支援 → 中小企業

セキュリティに取り組むためのガイドラインの活用

中小企業の情報セキュリティガイドラインを意識したセキュリティ対策が重要。実証を通して、自社で賄いきれないセキュリティ対策を委託することで容易なレベルアップを図ります。

取組 1	情報セキュリティに関する組織全体の対応方針を定める
取組 2	情報セキュリティ対策のための予算や人材などを確保する
取組 3	必要と考えられる対策を検討させて実行を指示する
取組 4	情報セキュリティ対策に関する適宜の見直しを指示する
取組 5	緊急時の対応や復旧のための体制を整備する
取組 6	委託や外部サービス利用の際にはセキュリティに関する責任を明確にする
取組 7	情報セキュリティに関する最新動向を収集する

SECURITY ACTION二つ星取得条件

1	OSやソフトウェアは常に最新の状態にしよう！
2	ウイルス対策ソフトを導入しよう！
3	パスワードを強化しよう！
4	共有設定を見直そう！
5	脅威や攻撃の手口を知ろう！

「5分でできる！情報セキュリティ自社診断」で自社の状況把握

「情報セキュリティポリシー(基本方針)」を定め、外部公開

(ご参考)「一つ星」に必要なセキュリティ対策

「一つ星」は、中小企業が取り組むべき最低限のセキュリティ対策を対象としています。

- 宣言するためには、IPA発行の「情報セキュリティ５か条」に取り組むことが必要条件となります。

「情報セキュリティ５か条」

1	OSやソフトウェアは常に最新の状態にしよう！
2	ウイルス対策ソフトを導入しよう！
3	パスワードを強化しよう！
4	共有設定を見直そう！
5	脅威や攻撃の手口を知ろう！

画像引用元：IPA「SECURITY ACTION セキュリティ対策自己宣言」https://www.ipa.go.jp/security/security-action/

(ご参考)「二つ星」に必要なセキュリティ対策

「二つ星」は、自社状況を把握し、セキュリティポリシーを策定・公開した企業を対象としています

- 宣言するためには、IPA発行の「5分でできる！情報セキュリティ自社診断」で自社の状況を把握し、その上で「情報セキュリティポリシー(基本方針)」を定め、外部に公開することが必要条件となります。

1. 「5分でできる！情報セキュリティ自社診断」で自社の状況把握
2. 「情報セキュリティポリシー(基本方針)」を定め、外部公開

画像引用元：IPA「SECURITY ACTION セキュリティ対策自己宣言」https://www.ipa.go.jp/security/security-action/

九州地区でのサービス開始前最適プロセスの確立

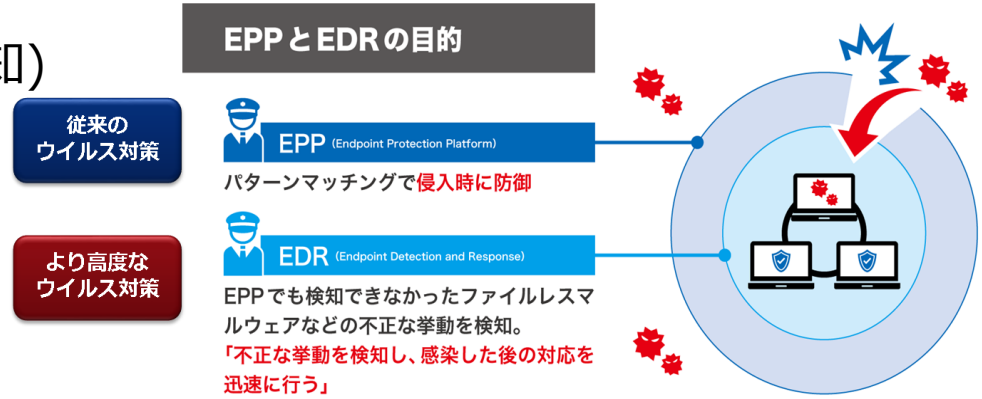
九州内企業様に導入検証を行い、実運用上の課題と解決方法について精査

サービス提供に必要なスキーム・プロセスの検証
（検知レベルに合わせたセキュリティ監視の有効性検証）

- マルウエアなどの不正な挙動を検知するEDR(未知のウイルス検知)が有効だが・・

エンドユーザ単独で運用することは難しい

マネージドセキュリティサービス(MSS)と合わせて使うのが一般的



- エンドユーザ・地域SOC事業者・先端分析技術を有するMSSの組み合わせと、役割分担の有効性を検証

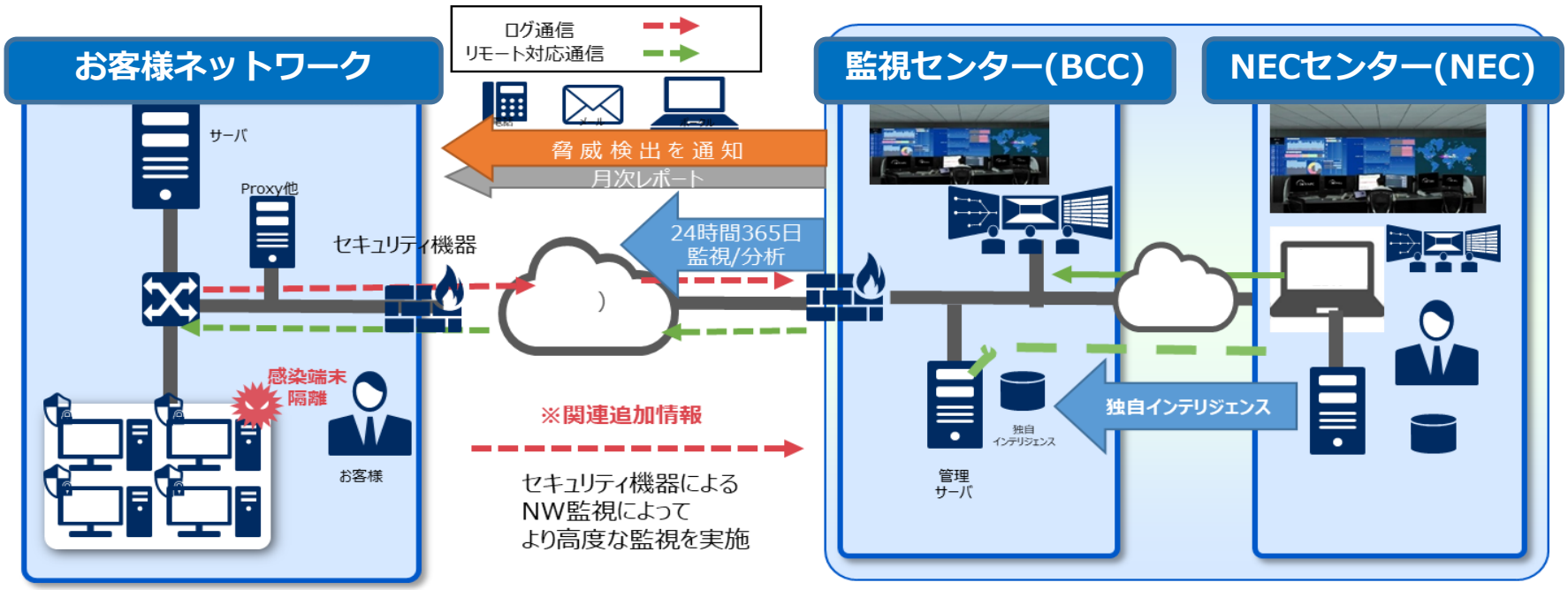
地域企業様、NECと連携し、最適な運用スキームの有効性を検証

地域企業様向けセキュリティサービス実現に向けた検証環境

パソコン向けウイルス対策に着目し、実績のある既設サービスを組み合わせ、地域企業連携型サービスを導入

多段階のセキュリティ運用監視で安全な端末向けセキュリティをご提供

- 信頼性の追求　　国産製品を採用
- 低コスト化と安全性の追求　　地域パートナー企業様と連携したスキームの構築
- ユーザーの負荷低減の追求　　端末監視とネットワーク監視を組み合わせたサービス



ご提供する内容について

ご提供する内容

『簡易セキュリティ診断』と『ツール・UTM（統合脅威管理）』の大きく分けて二つがございます。

申し込み

簡易セキュリティ診断

ツール・UTM導入

実証

そのままご利用

セキュリティ状況のチェックを行います

サービスを導入しセキュリティ監視を行います

サービス導入前に実施する簡易セキュリティ診断について ご紹介いたします

申し込み

簡易セキュリティ診断

ツール・UTM導入

実証

そのままご利用

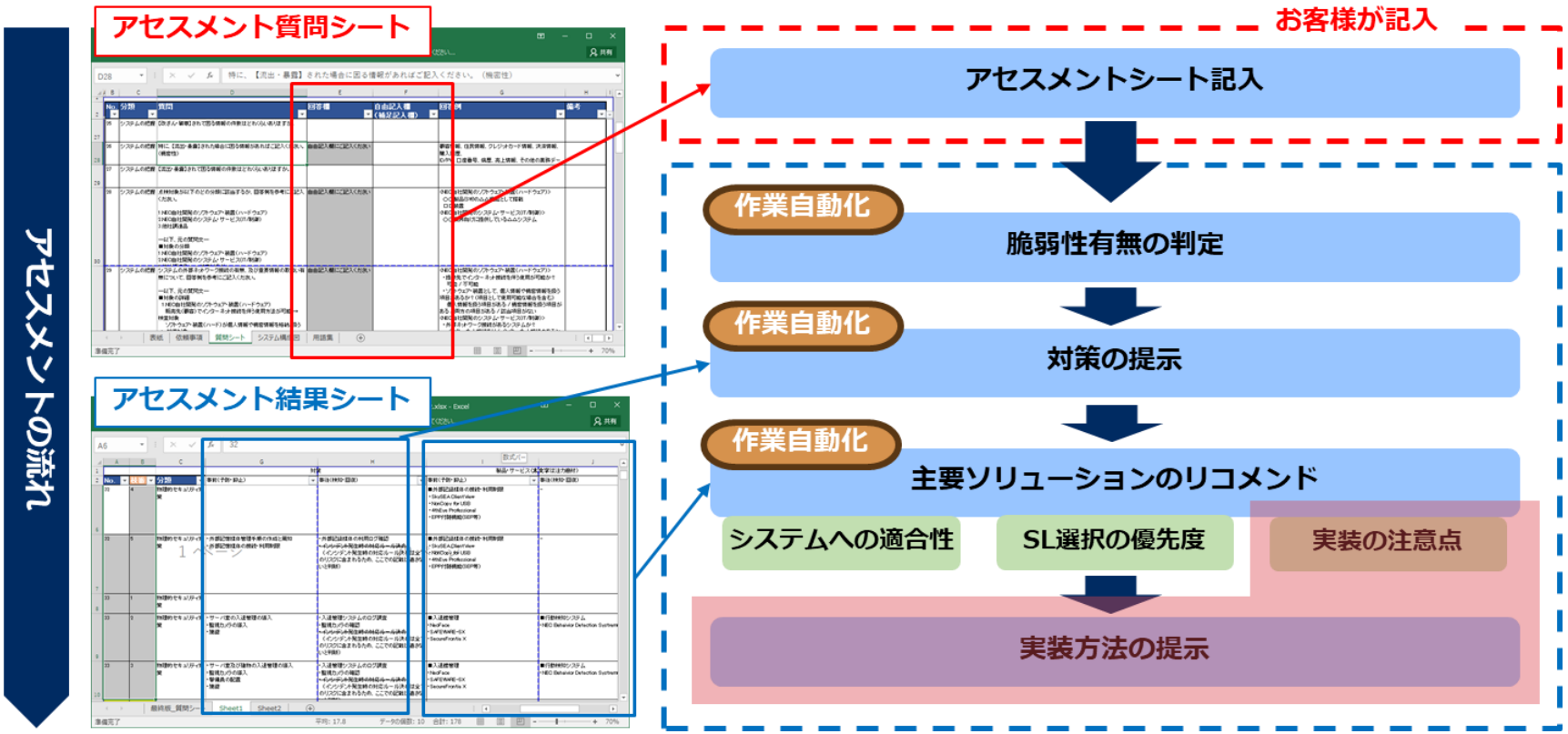
セキュリティ状況の
チェックを行います

サービスを導入し
セキュリティ監視を
行います

簡易セキュリティ診断

簡単なアンケート(アセスメントシート)にご回答頂くだけで、現状のセキュリティレベルを確認できます。

- SECURITY ACTIONに照らし合わせて現状のセキュリティレベルを確認・診断します



サービスとしてご提供するツール・ＵＴＭ（統合脅威管理）についてご紹介いたします

申し込み

簡易セキュリティ診断

ツール・UTM導入

実証

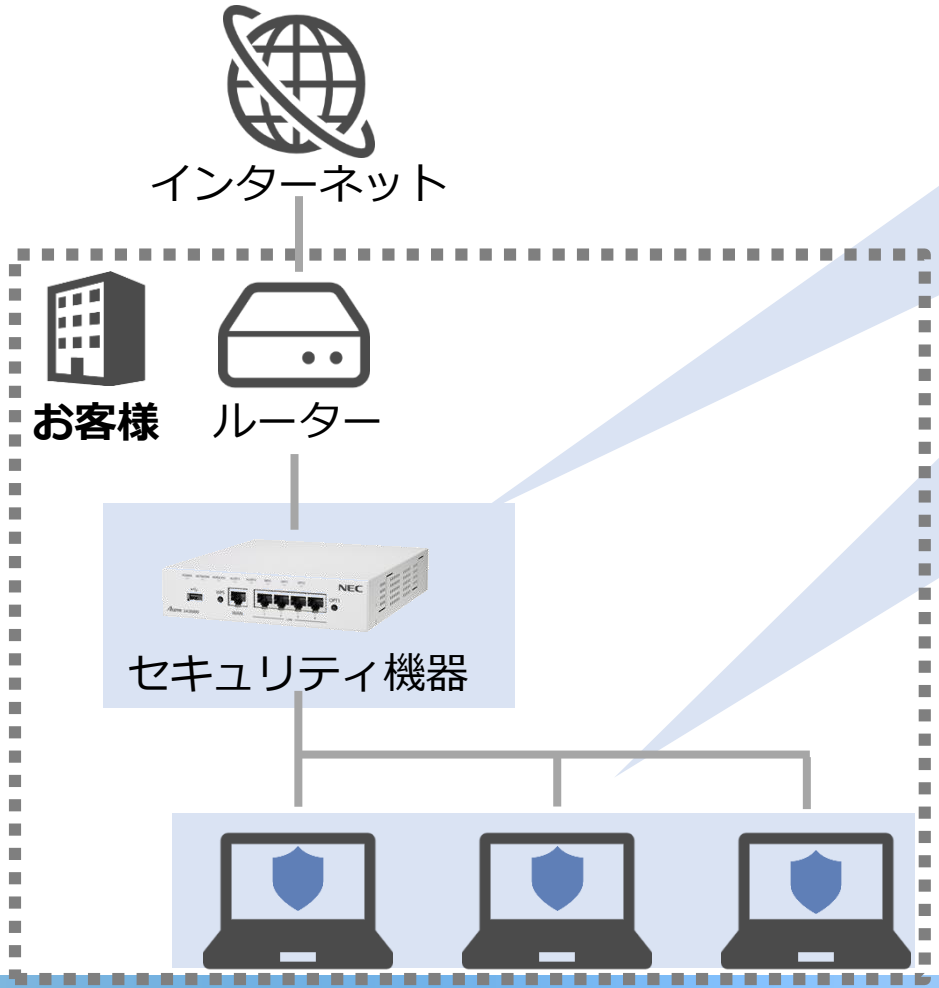
そのままご利用

セキュリティ状況の
チェックを行います

サービスを導入し
セキュリティ監視を
行います

サービス概要

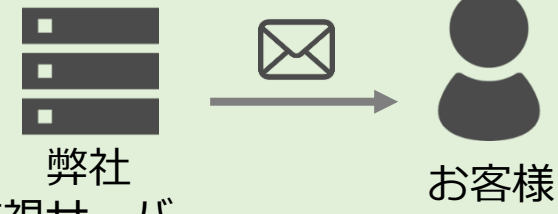
２種類の製品をご導入頂き、２段構えのセキュリティ環境を実現。攻撃を検知した際にはお客様へ迅速に連携します。



①通信を監視する製品
（サイバーセキュリティ
見守りサービス）

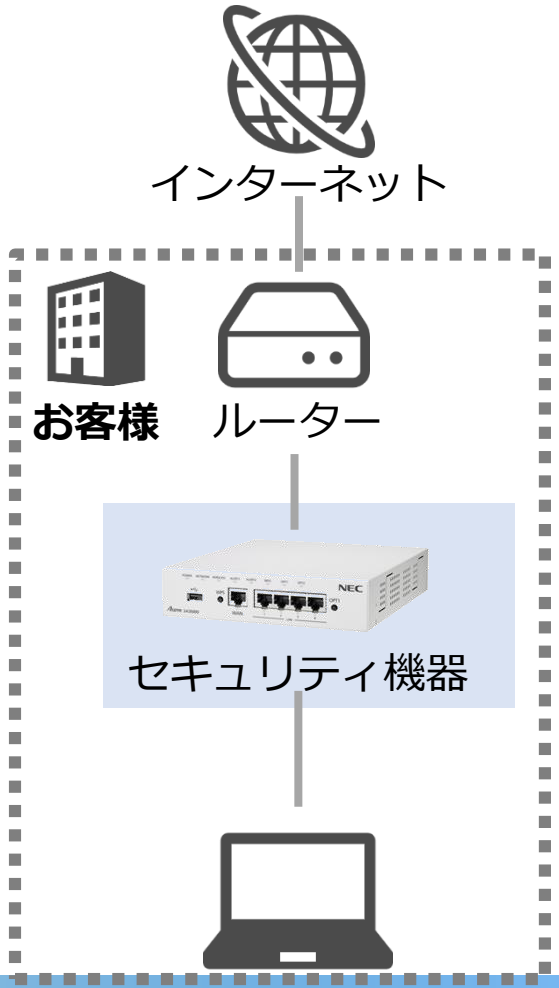
②PC向けウイルス対策製品
(エンドポイント
監視サービスType-Y)

攻撃を検知した際にはメールにて
お客様へご連絡



①通信を監視する製品（サイバーセキュリティ見守りサービス）

通信を監視して適宜遮断することで、外部からの攻撃を防ぐことに加えて端末のウイルス感染リスクも低減



必要十分なセキュリティ対策機能

社内ネットワークの通信を監視する上で必要な機能をまとめてご提供

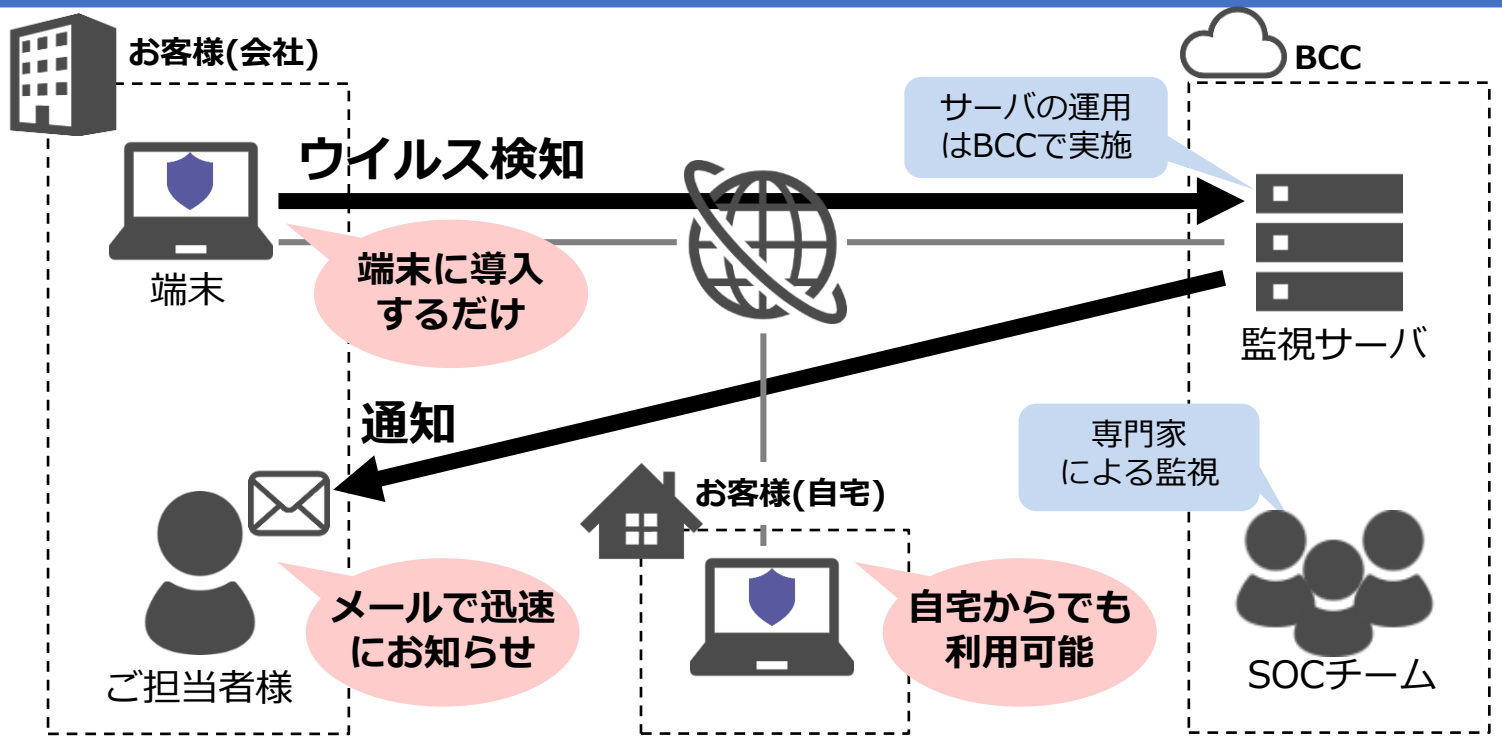
- Webページからのダウンロードや不審メールの添付ファイルのウイルスを無害化する機能
- 危険なWebサイト(ウイルス配布・詐欺)へのアクセスを防ぐ機能
- 外部からの不正侵入を防ぐ機能

簡単導入

基本設定後社内ネットワークに繋ぐだけでご利用可能

②PC向けウイルス対策製品 (エンドポイント監視サービス Type-Y)

高度なセキュリティ対策をお手軽に！！
PC・サーバ向けのマネージドセキュリティサービス



信頼と実績のあるエージェント

約74万クライアントの導入実績がある検知エンジンを採用した**純国産セキュリティ製品**
『NEC ActSecureχ』を利用

BCCによる運用・監視

サイバーセキュリティの国家資格を保有した
メンバーが運用を実施。
九州を中心に豊富な導入実績あり。

実証事業にご参加頂くメリット①

自社セキュリティ環境の現状を把握し、２段構えの防御＋監視サービスにより着実なレベルアップを実現できます。

現状把握

簡易セキュリティ診断

自社のセキュリティ対策の強みと弱みを見える化
どのようにセキュリティ対策を進めれば良いかがわかる

防御（２段構え）

① 通信を監視する製品（サイバーセキュリティ見守りサービス）

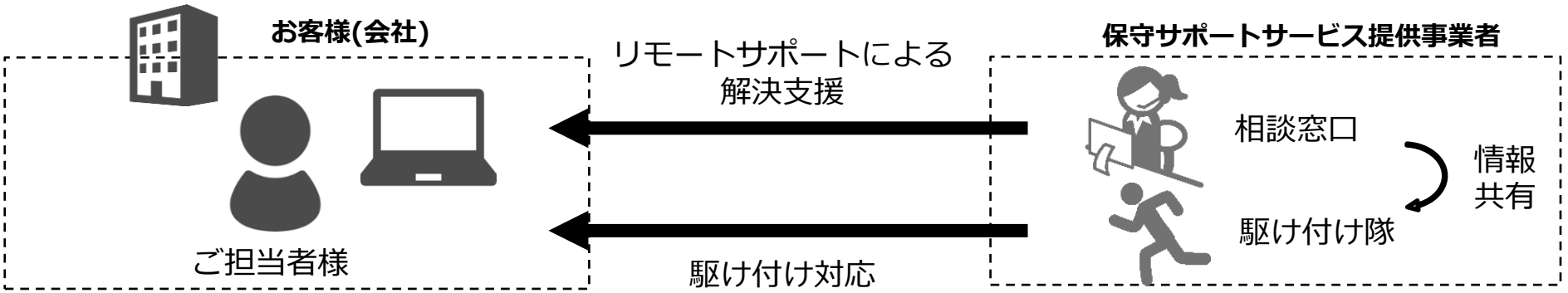
通信を監視し外部からの攻撃を防御
社内からの危険サイトへのアクセスも遮断し安心

② PC向けウイルス対策製品（エンドポイント監視サービス Type-Y）

ＰＣのふるまいを監視してウイルスを検知
約74万クライアントの導入実績がある検知エンジンを採用

実証事業にご参加頂くメリット②

検知内容への対処や問題発生時も安心！相談窓口や緊急時の駆け付け支援により手厚くサポートいたします。



相談窓口

お客様相談窓口

セキュリティ脅威に対し、メール、電話等でリモートから解決のご支援を行います。

駆け付け

駆け付け支援

遠隔からのリモート支援による解決が難しい場合は、現地への駆けつけ対応を行います。

ご参加頂ける企業様へ

検証事業のスケジュールと作業内容

簡易セキュリティ診断・構築・運用の各フェーズにおいて、参加企業様の作業負荷を最小限で実施します

	お客様作業	
セキュリティ診断	● **アセスメントシートの記入**	● 診断の分析
ツール・UTM導入	● **ツールのインストール** ● **UTMの設置**	● リモート監視 ● システム構築設定 ● 設置トラブル時の受付 ● リモート対応 ● 駆け付け
実証	● **検知時の対処** ● リモートセキュリティ監視 ● 検知時の通報	● セキュリティ評価 ● アンケート結果の分析 ● 結果報告 ● リモート対応 ● 駆け付け

① 申し込み

『実証参加申込書』と『5分でできる！情報セキュリティ自社診断』のご記入・ご提出をお願いします。

スケジュール

日時	概要
9/8(月)～ （※企業数上限に達し次第締め切り）	以下資料をご記入、ご提出いただく ・実証参加申込書 ・５分でできる！情報セキュリティ自社診断

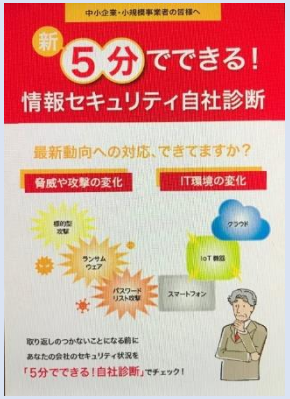
お客様にご実施頂く作業

『実証参加申込書』のご記入

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　実証事業参加申込書

FAX	092-521-4458	メール	ipa_otasukepj@bcc-net.co.jp		
郵送	〒810-0022 福岡市中央区薬院4－5－17 BCC 薬院ビル お助け隊事業担当				
会社名		業種		社員	人
所在地		〒			
窓口担当者	氏名		TEL		
	部署役職		メルアド		
代表者	代表者役職： 代表者名　： 会社印 事業参加を申込お場合押印必須。				
参加条件等	上記①～⑭を了承し申込みます。☐←チェックをお願いします。		実証対象端末台数		台

25項目からなる『5分でできる！情報セキュリティ自社診断』の実施



[出典] https://www.ipa.go.jp/files/000055848.pdf

② 簡易セキュリティ診断

お客様のセキュリティ状況についてお伺いする『簡単なアンケート（アセスメントシート）』をご記入、実証開始前に送付をお願いします。

スケジュール

日時	概要
9/23(水)～9/30(水)	アセスメントシート（Excelファイル）をメールにて送付
	アセスメントシートにご記入頂き、メールで返送いただく
（※報告会前後を想定）	アセスメントシートを基にセキュリティ診断を実施し、結果をお客様へ送付。

お客様にご実施頂く作業

アセスメントシートのご記入

③ ツール・ＵＴＭ導入

製品の導入作業にご協力をお願いします。

スケジュール

日時	概要
９/２３(水)～９/３０(水) (※申込順で順次実施)	・宅配便にてセキュリティ機器をお届け ・メールにてPC用のインストーラーをお届け
	・お客様にてセキュリティ機器を設置 ・お客様にて各PCへインストール
１０/１(火)～ (※申込順で順次実施)	・実証スタート

お客様にご実施頂く作業

※いずれの作業も手順書をご用意しております

セキュリティ機器の設置

PCへのインストール

問題解決へのご協力
(※問題発生時のみ)

④ 実証

ウイルス検知時のみ、ウイルス駆除のご協力をお願いします。

スケジュール

日時	概要
10/1(火)～12/31(木)	実証期間 （※準備ができた企業様から順次スタート）

お客様にご実施頂く作業

※手順書をご用意しております

検知への対処
（※検知時のみ）

問題解決へのご協力
（※問題発生時のみ）

実証完了後

実証期間後も作業無しでそのままご利用いただけます（有償）
商用利用をされない場合は以下作業をお願いします

スケジュール（※商用利用（有償）をしない場合）

日時	概要
（※報告会にて実施予定）	実証事業報告会にて商用利用するかご意向を確認
～1/31(日)	セキュリティ機器返送キットをお客様に宅配便にて送付
	・お客様にてセキュリティ機器を取り外し、返送キットに入れて宅配便にて発送 ・お客様にてＰＣ内のツールをアンインストール

お客様にご実施頂く作業（※商用利用（有償）をしない場合）

※いずれの作業も手順書をご用意しております

セキュリティ機器の
取り外し・返送

PCから
アンインストール

問題解決へのご協力
（※問題発生時のみ）

ご了承事項

以下事項についてご了承のほどよろしくお願いします。
その他詳細については実証参加申込書をご参照ください。

障害発生時の対応について

お客様ご協力のもと問題解決に全力を尽くしますが、万が一解決できない場合、実証前の状況に戻す方法をご案内させて頂く場合がございます。

検知時のお客様作業について

PCのウイルス感染等が疑われる場合に、お客様にウイルス駆除をはじめとした対処作業にご協力頂く場合がございます。

参加募集既定数に達した場合について

参加申し込み数が既定の50社に達した場合、ご参加いただけない場合がございます。