



経済産業省
九州経済産業局

令和3年度中小企業サイバーセキュリティ対策促進事業
(九州地域における地域SECURITY形成促進事業)

中小企業向けサイバーセキュリティ対策強化 に向けた支援策のご紹介

2021年9月

経済産業省 九州経済産業局

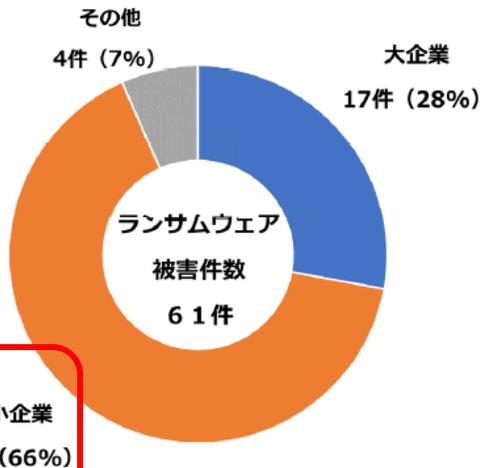
デジタル経済室

中小企業へのサイバー攻撃の被害状況

令和3年度上半期におけるランサムウェアの脅威 (令和3年9月9日発表警察庁調査)

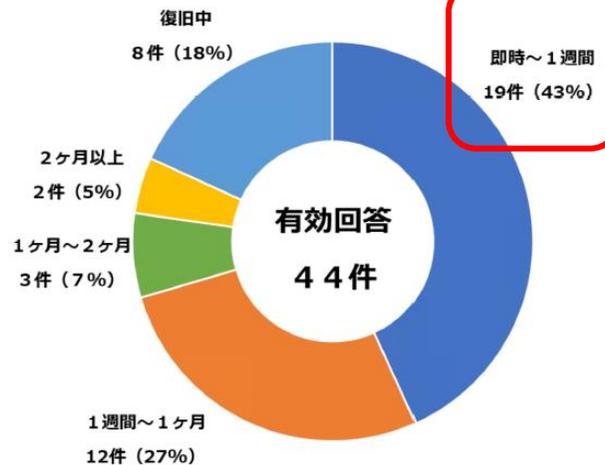
- ランサムウェア：感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価として金銭を要求する不正プログラム。
- 都道府県警察から報告のあった件数は61件。前年下半期（21件）と比べて**大幅に増加**。
被害件数の66%が中小企業。調査・復旧費用は**1000万円以上**要したものが多数。

ランサムウェア被害の被害企業団体等の規模別報告件数



注 図中の割合は小数点第1位以下を四捨五入しているため、総計が必ずしも100にならない。

復旧に要した期間



調査・復旧費用の総額

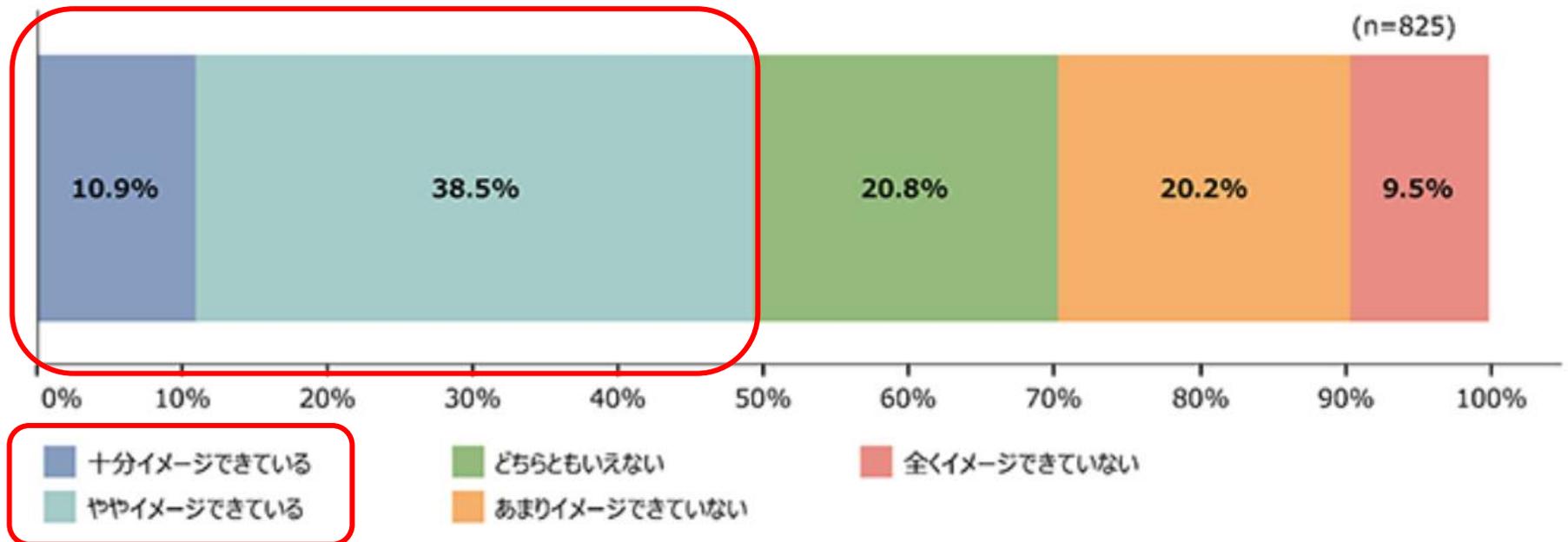


注 図中の割合は小数点第1位以下を四捨五入しているため、総計が必ずしも100にならない。

中小企業へのサイバー攻撃の被害状況（2021年度版中小企業白書）

- 情報セキュリティの問題は、自社の信用トラブルにも発展する恐れがある中、サイバー攻撃によって自社が被る被害についてイメージできている中小企業は、半数に満たない。

中小企業におけるサイバー攻撃の被害イメージに関する認識状況

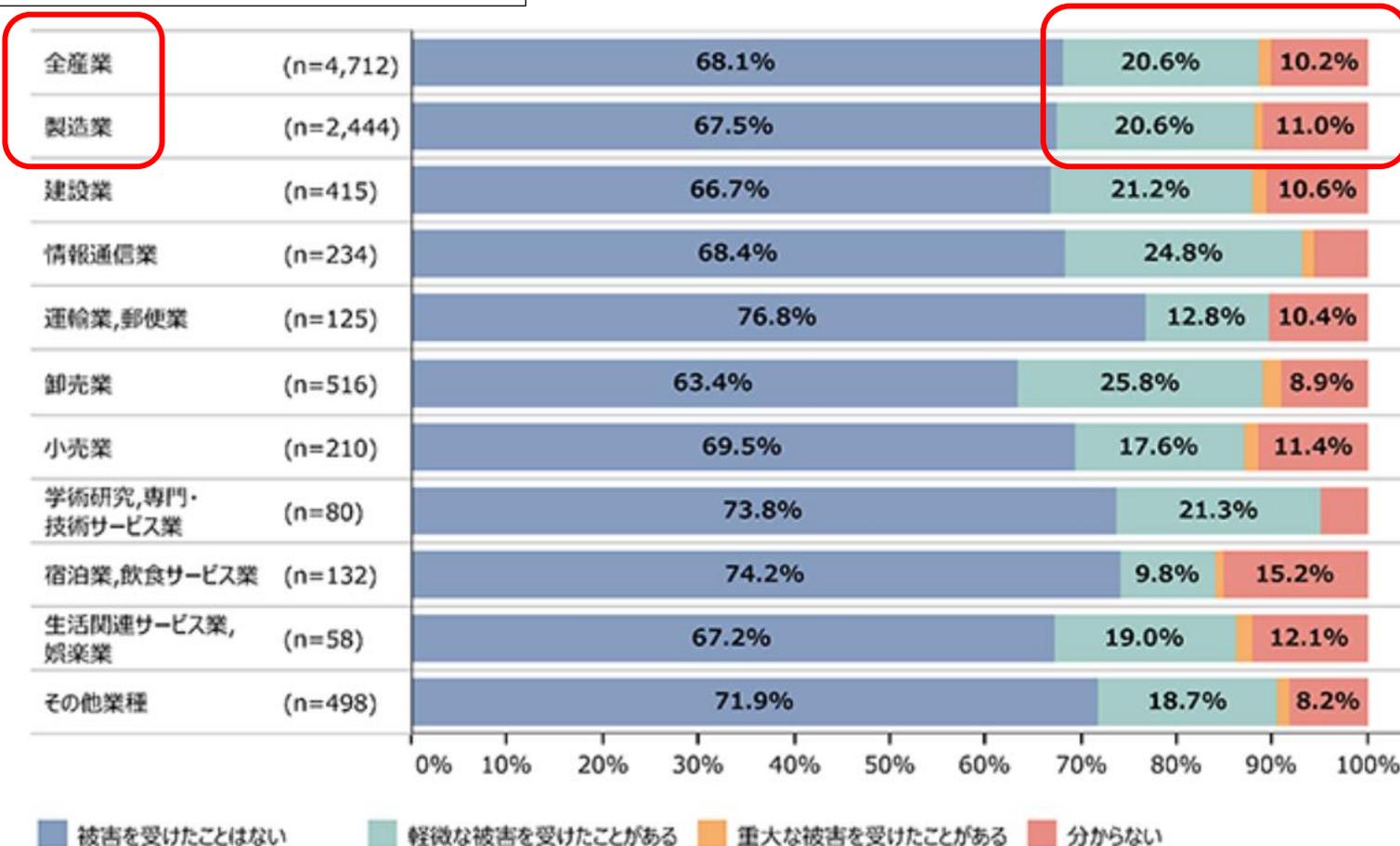


資料：（独）情報処理推進機構「情報セキュリティ白書2020」

中小企業へのサイバー攻撃の被害状況（2021年度版中小企業白書）

- 全体の2割以上の企業が何らかの被害を受けている。
- 被害状況は「分からない」と回答している企業も一定数存在。潜在的な被害も示唆される。

サイバー攻撃の被害状況（業種別）



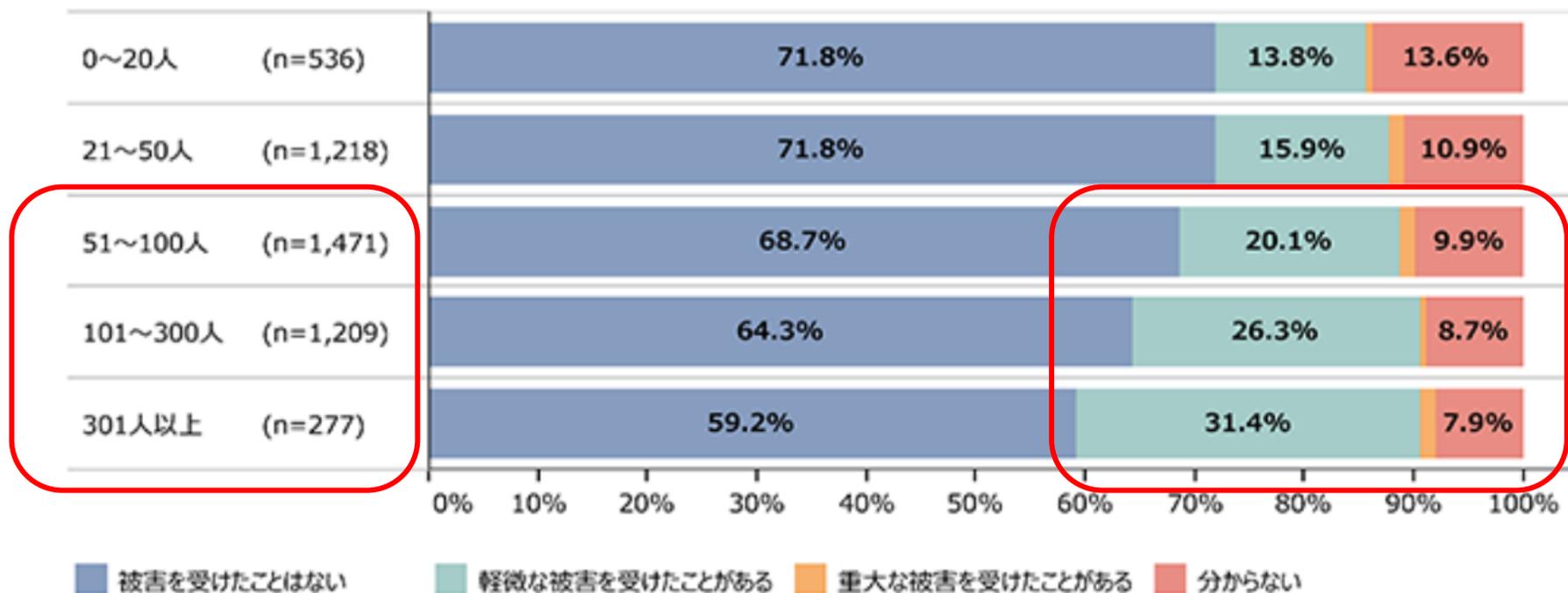
資料：（株）野村総合研究所「中小企業のデジタル化に関する調査」

（注）「全産業」では、業種不明の企業は除外して集計している。

中小企業へのサイバー攻撃の被害状況（2021年度版中小企業白書）

- 従業員数が多い企業ほど、サイバー攻撃を受けている割合が高い傾向。
- 51人以上の企業では3割程が被害を受けている。

サイバー攻撃の被害状況（従業員規模別）

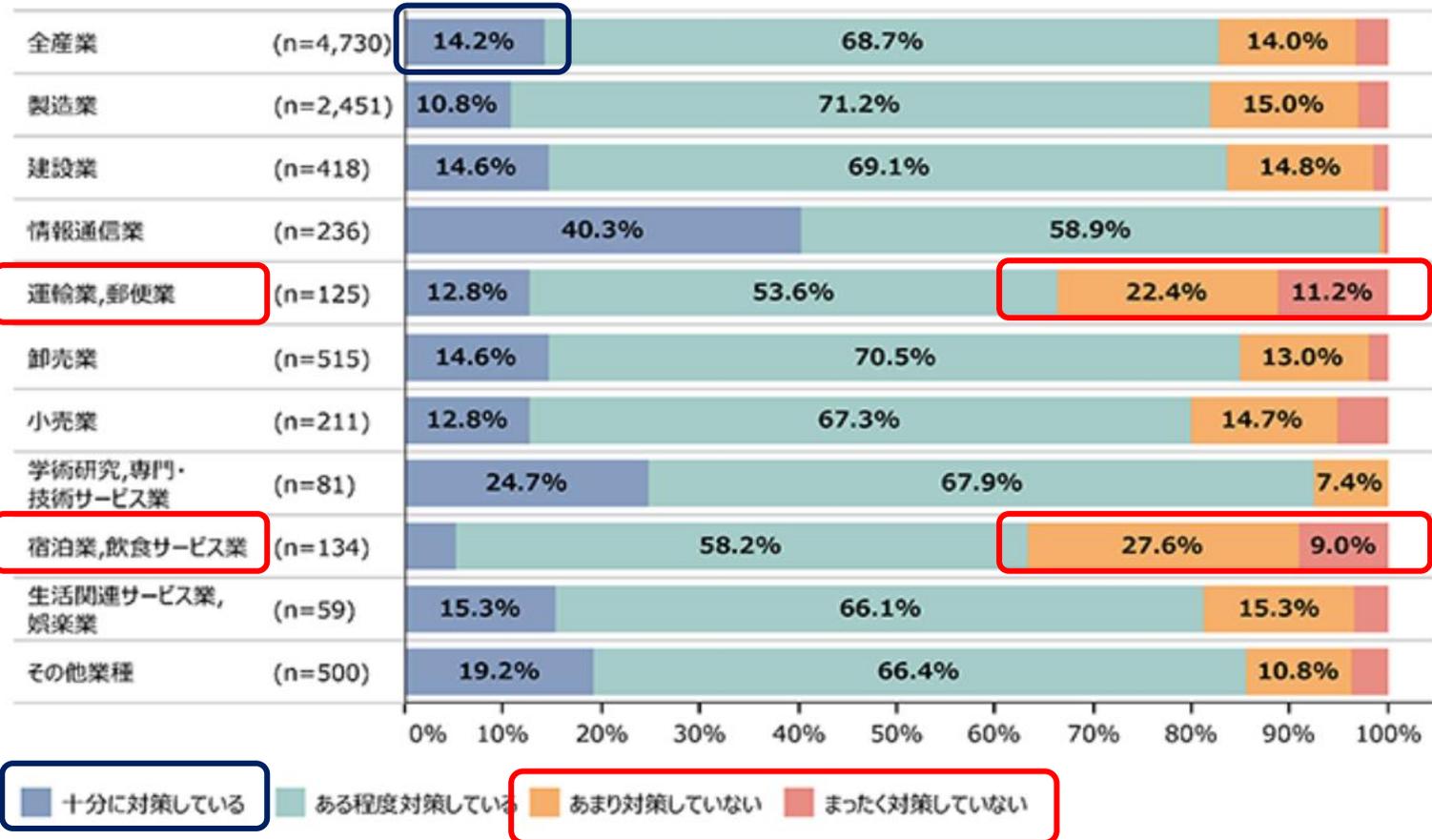


資料：（株）野村総合研究所「中小企業のデジタル化に関する調査」

セキュリティ対策の状況（2021年度版中小企業白書）

- 「十分に対策している」企業は全体の14.2%にとどまる。
- （P.4で）被害を受けた割合が低かった「運輸業,郵便業」や「宿泊業,飲食サービス業」では、サイバー攻撃による被害が懸念される状況。

情報セキュリティ対策の状況（業種別）

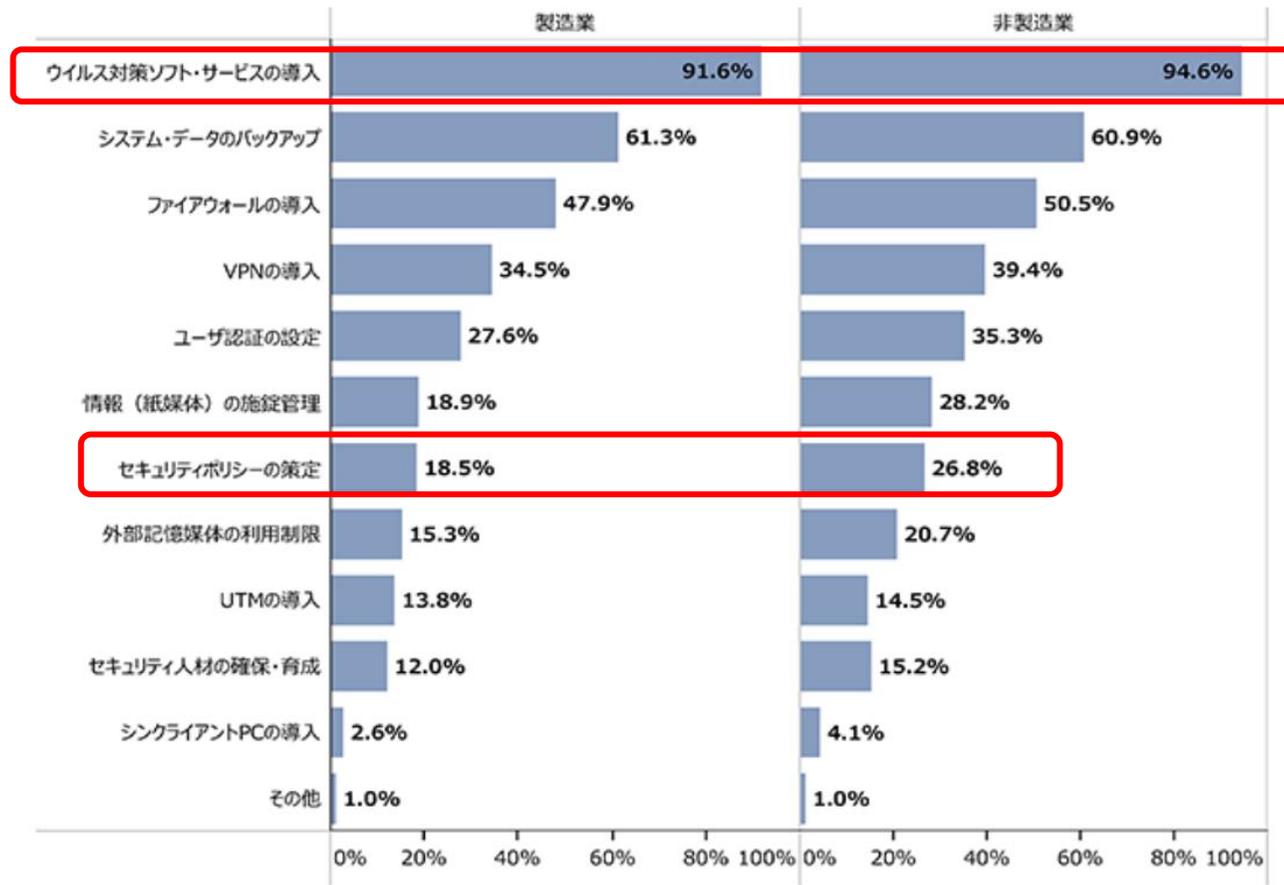


資料：（株）野村総合研究所「中小企業のデジタル化に関する調査」
 (注)「全産業」では、業種不明の企業は除外して集計している。

セキュリティ対策の状況（2021年度版中小企業白書）

- 「セキュリティポリシーの策定」は、資金をかけずに取り組むことができるが、2割程度にとどまる。
- 「社内の検討・推進体制が整わない」や「セキュリティ対策を実施できる人材がない」という課題を挙げる割合が最も多く、情報セキュリティ対策の体制面が追いついていないことが示唆される。

情報セキュリティ対策の内容（製造業・非製造業別）

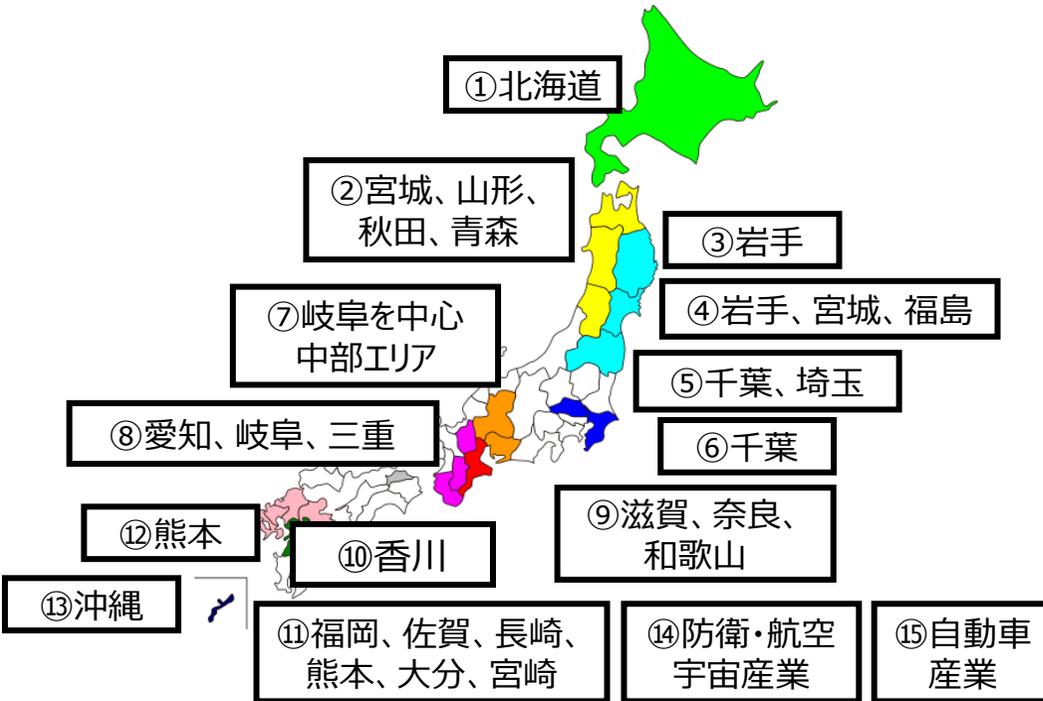


資料：（株）野村総合研究所「中小企業のデジタル化に関する調査」
(注)1.回答数(n)は以下のとおり。製造業：n=2,377、非製造業：n=2,224。
2.複数回答のため合計が100%とならない。

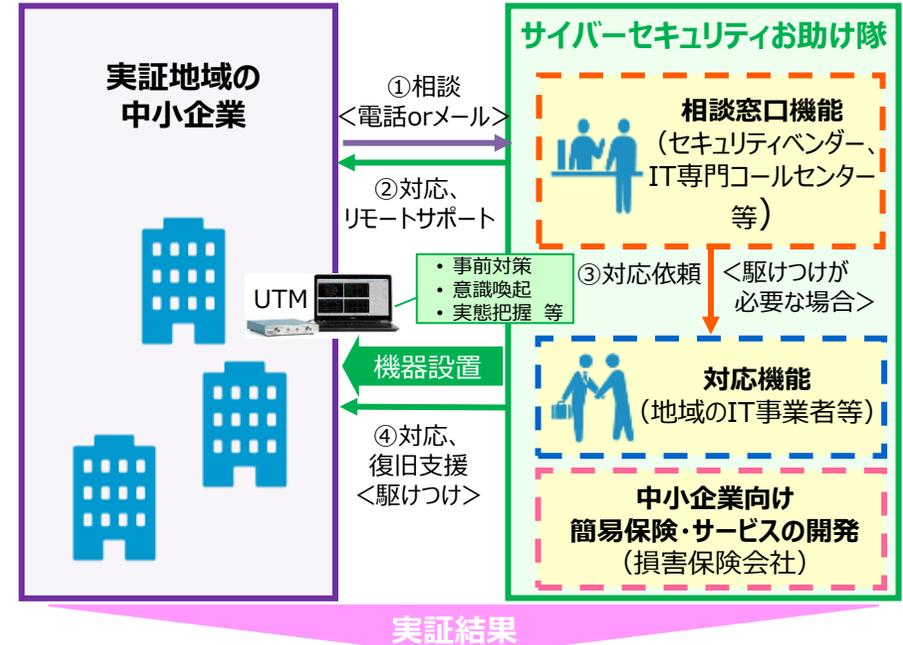
サイバーセキュリティお助け隊実証事業(2019-2020年度)

- 地域の団体、セキュリティ企業、保険会社がコンソーシアムを組み、中小企業向けのセキュリティ対策支援の仕組みの構築を目的とした実証事業を実施（2019年度15件、2020年度8件）。
- 2年間にわたる実証事業を通して、サイバーセキュリティに関する中小企業の実態を把握。2021年度より簡易サイバー保険を含むサイバーセキュリティお助け隊の民間自走化を促進すべく、お助け隊サービス基準を策定し、同基準を満たすサービスの審査登録制度の運営を開始。

<2020年度の実証地域>



<実証のイメージ>



中小企業 側

- 自社の攻撃実態等への気付き
- セキュリティ事前対策の促進
- 事後対応への意識向上 等

保険会社、セキュリティベンダー 側

- 中小企業のセキュリティ対策状況の把握
- 中小企業の被害実態の把握
- 中小企業が求めるサービスの把握 等

※2019年度実証地域（全8地域、1064社の中小企業が参加）：

①宮城、岩手、福島②新潟③長野、群馬、栃木、茨城、埼玉④神奈川⑤石川、富山、福井⑥愛知⑦大阪、京都、兵庫⑧広島、山口

サイバーセキュリティお助け隊実証事業の結果（2019年度）

- 1,064社が参加した実証期間中に、重大なインシデントの可能性ありと判断し、**対処を行った件数は128件**。対処を怠った場合の**被害想定額が5000万円**近くなる事案も。
- 実証参加前後の中小企業の意識変化や、お助け隊サービスに求められる機能等が明らかになった。

<駆け付け支援の対象となった特徴的な対応事例>

古いOSの使用

- ・Windows XPでしか動作しないソフトウェア利用のために、**マルウェア対策ソフト未導入のWindows XP端末を使用**。
- ・社内プリンタ使用のために、社内LANに接続したことで、意図せずにインターネット接続状態になり、マルウェアに感染。
- ・検知・駆除できていなかった場合の**想定被害額は5,500万円**。

私物端末の利用

- ・社員の**私物iPhoneが会社のWi-Fiに無断で接続**されていたことが判明。
- ・私物iPhoneは、過去にマルウェアやランサムウェアの配布に利用されている攻撃者のサーバーと通信していた。
- ・検知・駆除できていなかった場合の**想定被害額は4,925万円**。

ホテルWi-Fiの利用

- ・社員が**出張先ホテルのWi-Fi環境**でなりすましメールを受信し、添付されたマルウェアを実行したことで**Emotetに感染**。
- ・感染により悪性PowerShellコマンドが実行され、アドレス情報が抜き取られた後、**当該企業になりすまして、取引先等のアドレス宛に悪性メールが送信**された。

サプライチェーン攻撃

- ・実証参加企業でマルウェア添付メールを集中検知。
- ・**取引先のメールサーバーがハックされてメールアドレスが漏えい**し、それらのアドレスからマルウェア添付メールが送付されていた。
- ・メールは賞与支払い、請求書支払い等を装うなりすましメールであり、**サプライチェーンを通じた標的型攻撃**であった。

サイバーセキュリティお助け隊実証事業の結果（2020年度）

- 1,117社が参加した実証期間中に、セキュリティ機器による検知、および脆弱性診断等の結果に基づき、計293件のインシデント対応ほか技術的支援を実施。
- コロナ禍において、できる限りリモートでの対応を実施。
- また、2020年度に新たな取組として実施した産業別実証では、業界内での仕組み作りを求める声等があった。

<リモート対応事例>

お助け隊EDRサービスを導入した企業において、**不正プログラム「ブラウザハイジャッカー」をEDRで検知**、駆除方法を案内したが自力で対応出来なかったため、お助け隊が**リモート支援により駆除を実施**した。

UTMサービスを導入した企業において、**マルウェアへの感染の疑いがある通信をUTMで検知**。フルスキャンの結果、**Hacktool及びトロイの木馬、計6件のマルウェアを発見したため、お助け隊でリモート駆除を実施**。

<産業別実証での気づき>

自動車産業

- 外部診断の結果、実証参加企業全体のセキュリティ管理レベルの平均は、**製造業の平均と比べ比較的高かった**。
- 取引先からの要請は高まっているが、セキュリティ対策を行う上でのリソースが全般的に不足。**業界内での人材プールを共有できる仕組み**等の整備が課題。
- **同業他社の状況**を知ることができると、投資判断における経営者への動機付けになる。

防衛・航空宇宙産業

- セルフアセスメント（情報セキュリティ整備状況診断）を実施したところ、今後業界として求められるであろう**レベルに到達していた企業は10%** ※
- **防衛・航空宇宙産業という名目で特別な対策を要求された企業は38%**。要求された対策の中にはアクセス権に関するものもある一方で、セルフアセスメントでは、**秘密情報へのアクセス管理について約半数の企業が実施できていない**と回答。

※CMMC Level 1の17項目全てを達成しているか否かで判定

- 産業別実証事業は、「自動車産業の中小企業サプライヤーを対象とした実証」と、「防衛・航空宇宙産業に関わる中小企業及び今後防衛・航空宇宙産業に参入を検討する中小企業を対象とした実証」を実施。

サイバーセキュリティ対策の強化に向けた支援策 ～①地域SECURITY～

地域に根付いたセキュリティ・コミュニティ（地域SECURITY）の形成促進

- 地域の民間企業、行政機関、教育機関、関係団体等が、セキュリティについて語り合い、「共助」の関係を築くコミュニティ活動を、「地域SECURITY」と命名。
- まずは各地域で地域SECURITYの形成を促進し、将来的には、地域のニーズとシーズのマッチングによる課題解決・付加価値創出の場（コラボレーション・プラットフォーム）へと発展することを目指す。

<地域SECURITYのコンセプト>

地域にセキュリティについて相談できる相手がいない

地域にセキュリティを学ぶ機会が少ない

地域のベンダーを知らない

- 地域の関係者間でのセキュリティに関する「共助」の関係を形成
- イベント等の継続開催による地域のセキュリティ意識向上・人材育成
- 国や専門家からの情報提供の場

将来目指す姿

- ニーズとシーズのビジネスマッチングや共同研究による地域発のセキュリティソリューションの開発
- 地域一体となった課題解決
- 地域を越えた連携



地域SECURITY
がない状態

地域SECURITY
形成

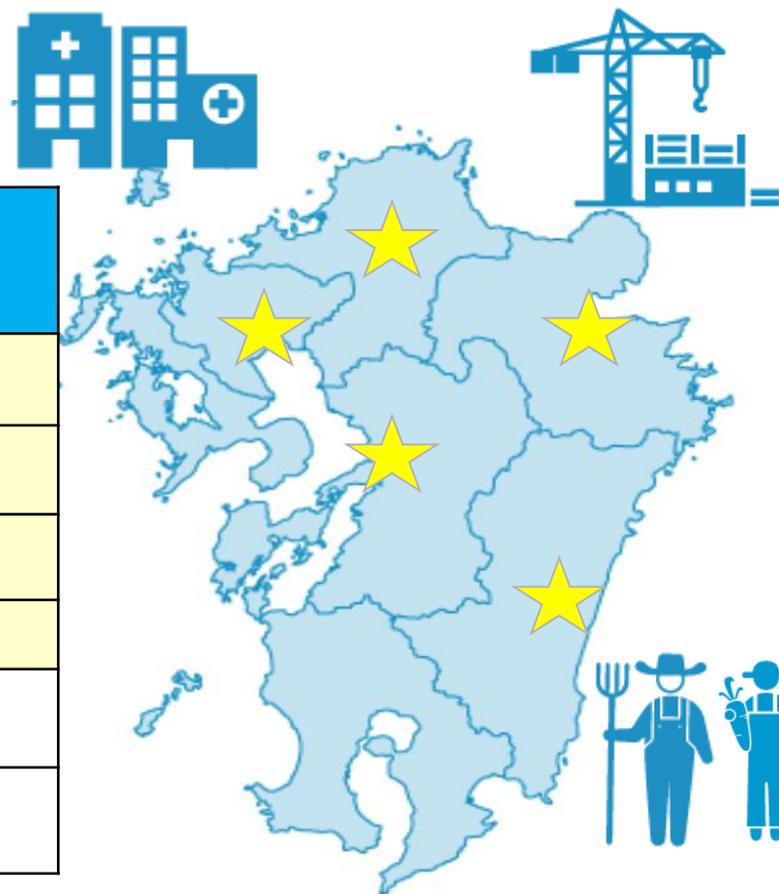
コラボレーション・プラットフォーム
を全国に展開

九州での「地域SECURITY」展開予定

- 業種ごとの特徴を踏まえたセキュリティ対策やビジネスリスク対応ができるよう、業種別にセミナーを実施。
- 地域企業からの事例紹介や対策のご紹介を通じ、普及啓発と地域でのコミュニティ形成を推進。
- 情報共有、人材育成が継続的に地域で行えるよう、コミュニティ活動を通じた九州地域全体でのセキュリティ対策強化を目指す。

【セミナーの開催予定(原則オンライン開催)】

対象	中心となる業種・ビジネス	開催時期(予定)
福岡県	①機械・金属関連分野	9月28日開催
	②海外ビジネス関連	10月28日開催
佐賀県	医療・薬局関連分野	11月22日開催
大分県	宇宙産業関連分野	11月10日開催
熊本県	農業関連分野	令和4年1月下旬頃
宮崎県	林業関連分野	令和4年2月上旬頃



サイバーセキュリティ対策の強化に向けた支援策 ～②サイバーセキュリティお助け隊ブランド～

サイバーセキュリティお助け隊ブランドの使用開始

- 実証事業で得られた知見に基づき、中小企業向けのセキュリティサービス（お助け隊サービス）が満たすべき基準を整理、パブコメを経て2月末にIPAより公開。
- 2021年3月に第1回審査を行い、4月15日にお助け隊マークが付与された民間サービスが「サイバーセキュリティお助け隊サービス※」として登録され、市場に展開。

※中小企業のサイバーセキュリティ対策支援サービスに不可欠な各種サービス内容（相談窓口、システムの異常の監視、緊急時の対応支援、簡易サイバー保険など）の基準を満たした民間による支援サービス事業

2019年度
(実証1年目)

2020年度
(実証2年目)

2021年度以降
(民間で自走)



攻撃実態の把握

ニーズを踏まえたサービスのスリム化

地域特性・産業特性の考慮

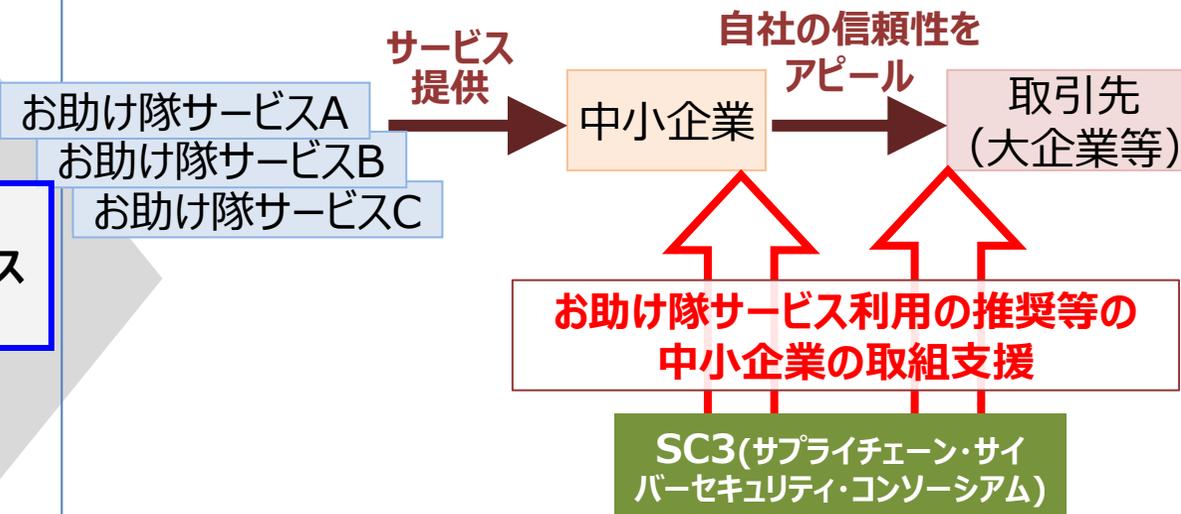
実証事業：
中小企業が利用しやすい安価なセキュリティサービスの開発

意識啓発

事前対策とのセットによるリスク低減

導入・運用負荷を下げる方法の検討

お助け隊サービス審査登録制度：
一定の基準を満たすサービスにお助け隊の商標利用権を付与。



→SC3（業種別業界団体が参加）で利用推奨を行うことで、より多くの中小企業がお助け隊サービスを活用し、万が一の際に早急に正しい対処が行える状態を目指す。

サイバーセキュリティお助け隊サービス 登録リスト

- 全国各地域の中小企業の皆様にとって選択・利用可能な「サイバーセキュリティお助け隊サービス」
第1回登録サービスリスト（5件）

【第1回登録サービスリスト】

	サービス名	事業者名	対象地域
1	商工会議所サイバーセキュリティお助け隊サービス	大阪商工会議所	近畿エリア、名古屋・東京・神奈川の都心部 ※近畿地方に本社を置く企業
2	防検サイバー	MS & AD インターリスク 総研株式会社	全国
3	PCセキュリティみまもりパック	株式会社 P F U	全国
4	EDR運用監視サービス 「ミハルとマモル」	株式会社デジタルハーツ	全国
5	SOMPO SHERIFF (標準プラン)	SOMPO リスク マネジメント株式会社	全国

【サイバーセキュリティお助け隊サービス概要はこちら】

<https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html> 16

(参考) 「サイバーセキュリティお助け隊サービス基準」の概要

- 【コンセプト】中小企業に対するサイバー攻撃への対処として**不可欠なサービス**を**効果的かつ安価に、確実に**提供する。
- 第1回審査(3月)において出た論点を踏まえ、第2回中小企業対策強化WGにおいて、基準改定や基準解釈の目安となるガイドの作成等の方針を議論。「v1.1版」として公開した基準の概要は以下のとおり。

主な要件	概要
相談窓口	お助け隊サービスの導入・運用に関するユーザーからの各種 相談を受け付ける窓口を一元的に設置／案内
異常の監視の仕組み	次のいずれかを含む異常監視サービスを提供すること ・ユーザーのネットワークを24時間見守り、攻撃を検知・通知する仕組み（UTM等のツールと異常監視サービスから構成） （ネットワーク括監視型の場合） ・ユーザーの端末（PCやサーバ）を24時間見守り、攻撃を検知・通知する仕組み（EDR等のツールと異常監視サービスから構成） （端末監視型の場合）
緊急時の対応支援	ユーザーと合意したサービス規約等に基づき、ユーザーから要請された場合、ユーザーの指定する場所に 技術者を派遣することにより、緊急時の対応支援を行うこと （リモートによる対応支援が可能な場合には、リモートによる対応支援も可とする。）
中小企業でも導入・運用できる簡単さ	IT・セキュリティの 専門知識のないユーザーでも導入・運用できるような工夫 が凝らされていること
簡易サイバー保険	インシデント対応時に突発的に発生する各種コストを補償する サイバー保険が付帯 されていること なお、当該保険は初動対応（駆付け支援等）の費用を補償するものであること
上記機能のワンパッケージ提供	原則として、これら機能をユーザーが個別に契約することなく 一元的に契約可能 であること （例外的に個別契約とする場合にも、ユーザーにおいて手続上の煩雑さを伴わないよう工夫が凝らされていること）
中小企業でも導入・維持できる価格等	・ ネットワーク括監視型の場合：月額1万円以下 （税抜き） ・ 端末監視型の場合：端末1台あたり月額2,000円以下 （税抜き） これらの仕組みを合わせて提供する場合には、この和（ 月額1万円に端末1台あたり月額2,000円を加えた価格 （税抜き））に相当する価格を超えない価格であること。端末1台から契約可能であること。 ・最低契約年数は2年以内 ・初期費用、契約年数等の契約にかかる条件をサービス規約等に記載するとともに、口頭又は書面によりユーザに分かりやすく説明すること
中小企業向けセキュリティ事業の実績	お助け隊実証事業に参加していたこと又は類似のサービスを 中小企業向けに提供・運用した実績 があること
情報共有	お助け隊サービス事業者間の 情報共有（少なくともアラートの統計情報の提供） に応じること
事業継続性	要員の確保、品質管理等の社内プロセス整備、企業としての安定した財政基盤、経理処理能力等
更新	2年毎に更新審査 を受けること

サイバーセキュリティ対策の強化に向けた支援策 ～③対策ガイドライン、相談窓口～

中小企業の情報セキュリティ対策ガイドライン

入門から本格的対策までこれ一冊！

- ・情報を安全に管理するための具体的な手順
- ・企業が認識すべき「3原則」
- ・企業がやらなければならない「重要7項目の取組」
- ・ウェブサイトの運用・クラウドサービス安全利用の手引き



<https://www.ipa.go.jp/security/keihatsu/sme/guideline/>





情報セキュリティ対策を「始めたい」「強化したい」「学びたい」中小企業の方々をサポートするポータルサイト

- ・5分でできる！自社診断
&ポイント学習
- ・セキュリティプレゼンター支援
- ・SECURITY ACTION
自己宣言者サイト



The screenshot shows the homepage of the Information Security Support Site. At the top, there is a navigation bar with the site name and a search bar. Below the navigation bar, there are several tabs for different user roles: 'このサイトについて', 'サービス一覧', '旧TOP画面', '経営者の方', '対策実践者の方', '従業員の方', '啓発者/教職員の方', and '一般/学生の方'. The main content area is titled 'このサイトでできること' and lists three main features: 1. '情報セキュリティ診断' (Information Security Diagnosis) with a sub-section '知りたい' (I want to know), 2. '5分でできる！ポイント学習' (5-minute! Point Learning) with a sub-section '学びたい' (I want to learn), and 3. 'SA自己宣言者サイト' (SA Self-Declaration Site) with a sub-section '始めたい' (I want to start). Each feature is accompanied by a brief description and a small icon.

情報セキュリティ安心相談窓口

- ・ウイルスや不正アクセスに関する相談にアドバイスを提供
- ・相談内容から判明したトラブルの傾向、手口、対策に関する情報を公開

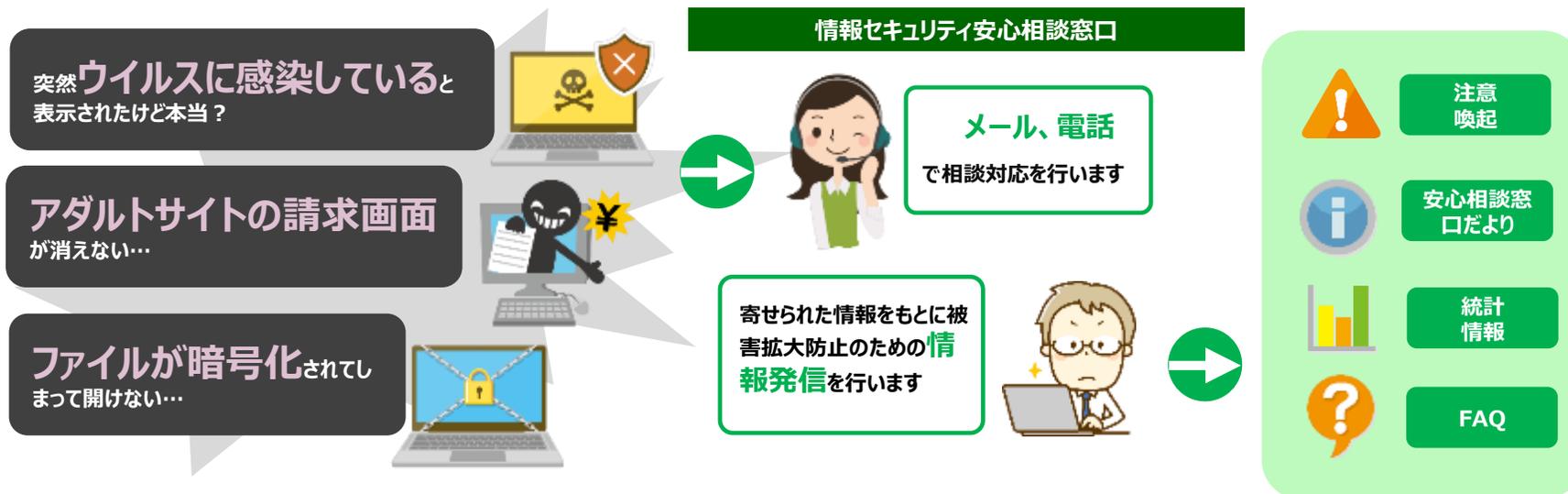
 **03-5978-7509**

電話 平日 10:00-12:00、13:30-17:00

 **anshin@ipa.go.jp**
メール



ポータル



様々な支援策は用意しておりますが…
概略はこちらにもまとめております！

経済産業省
九州経済産業局



デジタル関連施策 のご紹介

九州経済産業局（情報政策課）では、「九州IoTコミュニティ（※）」活動の一環として、デジタル関連施策（補助金公募情報、イベント情報）を月3回程度、メルマガ配信しております。本資料で掲載している施策の最新情報をお届けしますので、配信ご希望の方は下記URL（もしくは二次元コード）よりお申し込みください。
<https://www.kyushu.meti.go.jp/seisaku/jyoho/kyushu-iot.html>

※九州IoTコミュニティ
Society 5.0の実現に向けて、IoT等の導入を促進するため平成29年7月に設立したネットワーク。ユーザーとベンダーの出会いの場や、人材育成の機会等を提供。

【お問い合わせ先】

九州経済産業局 デジタル経済室

TEL：092-482-5552

E-mail：kyushu-iot@meti.go.jp

■九州経済産業局HPに掲載■
補助金、イベント情報、サイバーセキュリティ対策等、月2回程度更新しながら配信中！

<https://www.kyushu.meti.go.jp/seisaku/jyoho/kyushu-iot.html>



九州経済産業局
バーチャル職員
九州 あおい