

【サイバーセキュリティお助け隊 説明会資料】

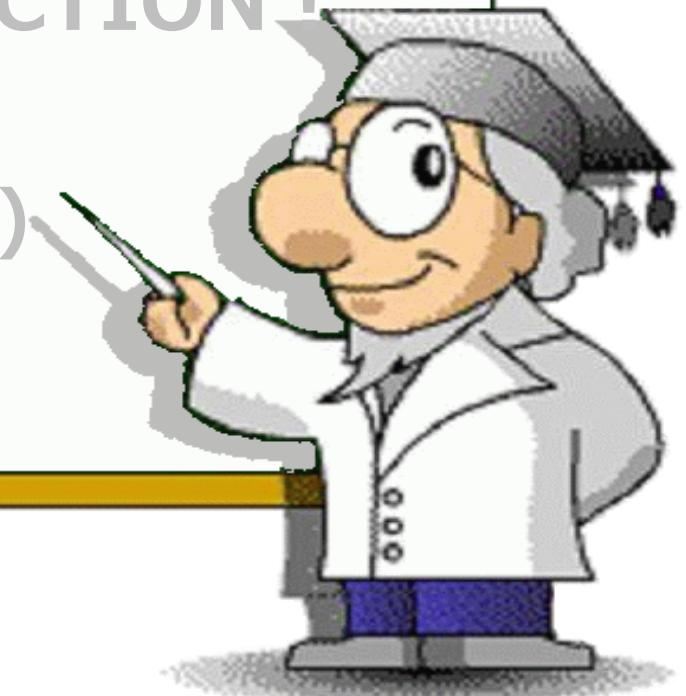
中小企業におけるサイバーセキュリティ対策普及 に向けた国等の支援事業について

令和2年9月

経済産業省 商務情報政策局 サイバーセキュリティ課
独立行政法人 情報処理推進機構 セキュリティセンター

目次

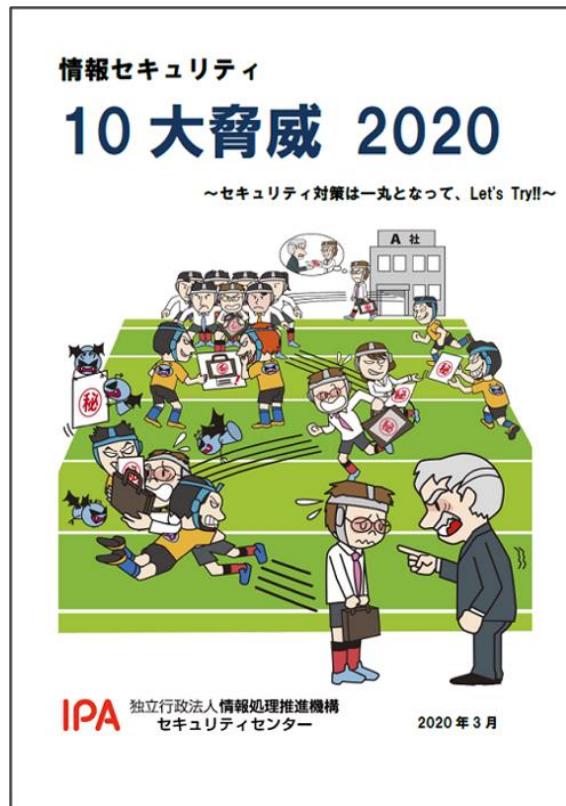
-
- 1. サイバーセキュリティを巡る状況
 - 2. 国等における主な取組みと中小企業
　　向けサイバーセキュリティ対策支援事業
 - 3. 始めましょう SECURITY ACTION !
 - 4. 参考情報
　　(IPAのツール・制度のご紹介)



情報セキュリティ10大脅威2020

<https://www.ipa.go.jp/security/vuln/10threats2020.html>

- ◆ IPAが2006年から毎年発行している資料
- ◆ 前年に発生したセキュリティ事故や攻撃の状況等から専門家等が選考したTOP10について解説



脅威に対して様々な立場の方が存在

立場ごとに注意すべき脅威も異なるはず

- 家庭等でパソコンやスマホを利用する人 「個人」
- 企業や政府機関などの組織
- 組織のシステム管理者や社員・職員 「組織」



「個人」と「組織」の2つの立場で
脅威を解説

情報セキュリティ10大脅威2020

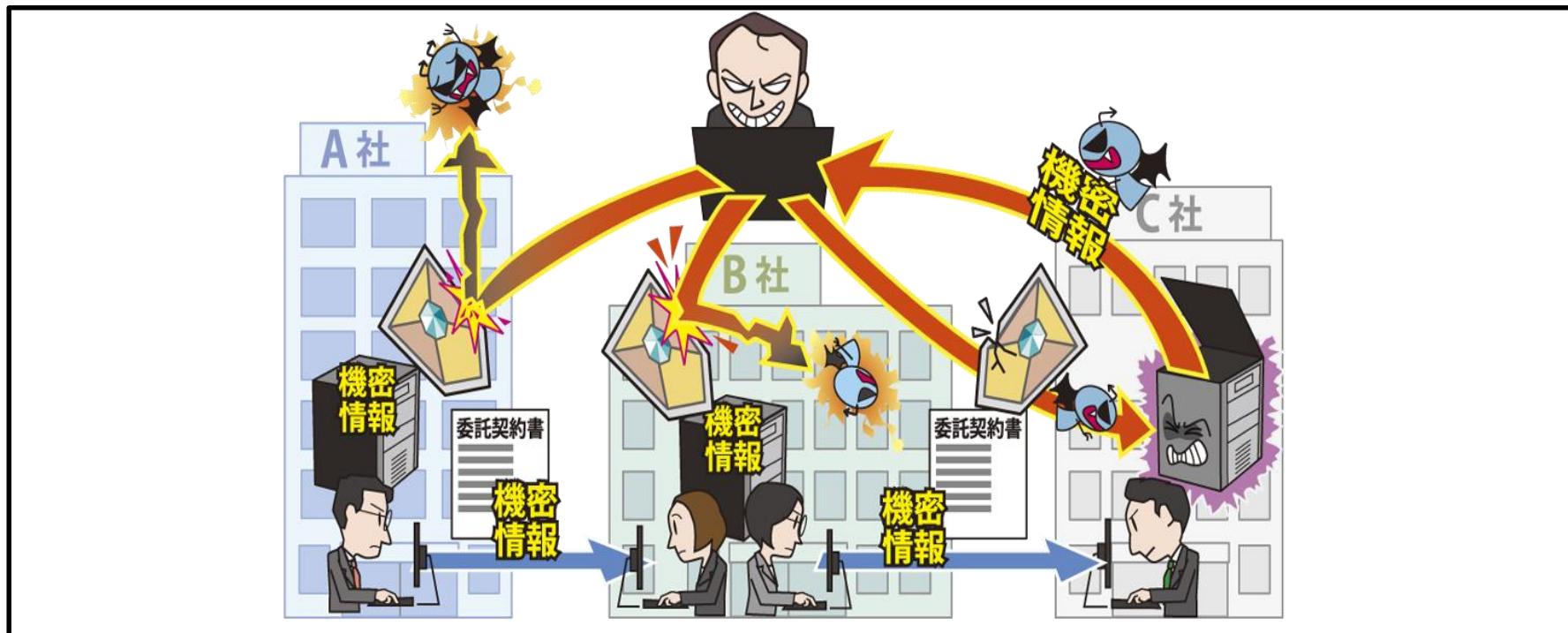
「個人」および「組織」向けの脅威の順位

昨年 順位	個人の脅威	順位	組織の脅威	昨年 順位
NEW	スマホ決済の不正利用	1位	標的型攻撃による機密情報の窃取	1位
2位	フィッシングによる個人情報の詐取	2位	内部不正による情報漏えい	5位
1位	クレジットカード情報の不正利用	3位	ビジネスメール詐欺による金銭被害	2位
7位	インターネットバンキングの不正利用	4位	サプライチェーンの弱点を悪用した攻撃	4位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	5位	ランサムウェアによる被害	3位
3位	不正アプリによるスマートフォン利用者への被害	6位	予期せぬIT基盤の障害に伴う業務停止	16位
5位	ネット上の誹謗・中傷・デマ	7位	不注意による情報漏えい	10位
8位	インターネット上のサービスへの不正ログイン	8位	インターネット上のサービスからの個人情報の窃取	7位
6位	偽警告によるインターネット詐欺	9位	IoT機器の不正利用	8位
12位	インターネット上のサービスからの個人情報の窃取	10位	サービス妨害攻撃によるサービスの停止	6位



【4位】サプライチェーンの弱点を悪用した攻撃

～業務委託先にも適切なセキュリティ管理を要求～



- 原材料や部品の調達、製造、在庫管理、物流、販売、業務委託先などの一連の商流（サプライチェーン）において、セキュリティ対策が甘い組織が攻撃の足がかりとして狙われる
- 一部業務を委託している外部委託先組織から情報が漏えい

【4位】サプライチェーンの弱点を悪用した攻撃

～業務委託先にも適切なセキュリティ管理を要求～

● 要因 サプライチェーンのセキュリティ対策不足

- サプライチェーンを適切に選定、管理していない
- 再委託先や再々委託先の管理は困難
 - 委託先組織の先に再委託先組織や再々委託先組織がある場合、その管理は委託先組織が行うため、委託元からのセキュリティ対策管理はさらに難しくなる



● 2019年の事例／傾向

■ 再委託先の開発環境への不正アクセス

(※1)

- ・再委託先のスポーツ関連企業が不正アクセスを受けた
- ・開発環境のサーバー内からデータが削除された
- ・開発環境のセキュリティ設定に不備
- ・削除されたデータは国体参加者データ等で、氏名、性別、生年月日等が含まれる
- ・データの流出や公開の事実は確認されていない

【出典】※1 国民体育大会参加者データおよび公認スポーツ指導者データの消失について

<https://www.japan-sports.or.jp/news/tabid92.html?itemid=4065>

【4位】サプライチェーンの弱点を悪用した攻撃

～業務委託先にも適切なセキュリティ管理を要求～

サイバー攻撃 供給網の穴

サイバー攻撃
供給網の穴

トヨタの取引先を脅迫



企業のサプライチェーン（供給網）を狙う二重の脅迫の手口
（出典：日本経済新聞朝刊）

「不正侵入してデータを盗む」「データを漏洩する」など、企業が抱えるリスクを踏まえて、攻撃者は「データを漏洩する」と「データを盗む」の二つの脅迫を行なった。データ漏洩は、主に内部情報漏洩（内部者による情報漏洩）や外部情報漏洩（外部者による情報漏洩）がある。内部情報漏洩は、内部者の個人的な問題で発生する場合もあるが、内部者の故意によるものが多い。外部情報漏洩は、組織外の人間によるもので、組織内にいる人物が組織外の人間に情報を漏洩する場合や、組織外の人間が組織内に入り込み情報を漏洩する場合がある。

（出典：日本経済新聞朝刊）

身代金要求→拒否で「機密公開」
防御甘い中小入り口

（出典：日本経済新聞朝刊）

企業のサプライチェーン（供給網）を狙う二重の脅迫の手口（出典：日本経済新聞朝刊）

（出典：日本経済新聞朝刊）

サイバー攻撃
供給網の穴

「次は取引停止」迫る大手

下請けを含めたセキュリティ対策が求められている
米国防総省は2018年以降、セキュリティ対策のできていない企業を新規不可に
取引先からの情報漏洩も自社の責任負担に
日本の防衛省も2018年以降、同条件の契約基準を実施
欧州連合(EU)は22年5月以降の新規取引で、下請けも含めたサイバーアクセス権を自動車メーカーに義務づける
日本や韓国、ロシアなど50以上の国と地域でも同様の規制が適用される見込み

中小、人・力不足で苦慮

車・防衛… 各国で規制強化

対策強要 下請法に抵触も
（出典：日本経済新聞朝刊）
（出典：日本経済新聞朝刊）
（出典：日本経済新聞朝刊）
（出典：日本経済新聞朝刊）

対策、海外で続々進化

世界の端末「健康診断」も

【出典】

サイバー攻撃 供給網の穴>(上) トヨタの取引先を脅迫
： 2020年9月15日 日本経済新聞 朝刊 17ページ

【出典】

サイバー攻撃 供給網の穴>(下)「次は取引停止」迫る大手
： 2020年9月16日 日本経済新聞 朝刊 16ページ

目次

-
- 1. サイバーセキュリティを巡る状況
 - 2. 国等における主な取組みと中小企業
向けサイバーセキュリティ対策支援事業
 - 3. 始めましょう SECURITY ACTION !
 - 4. 参考情報
(IPAのツール・制度のご紹介)



産業サイバーセキュリティ研究会とWGの設置による検討体制



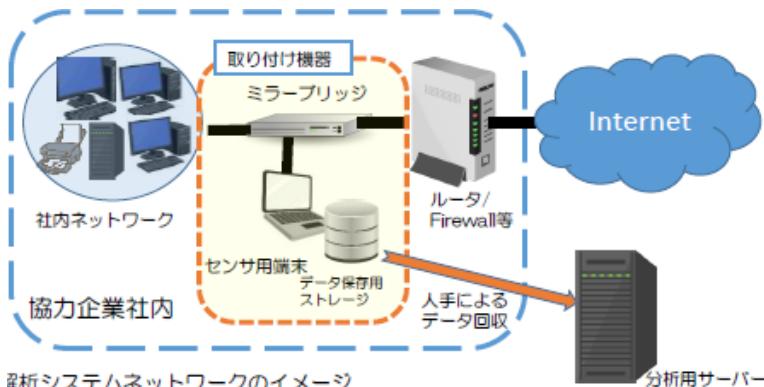
中小企業に対するサイバー攻撃の調査・分析結果（大阪商工会議所）

- 地域の中小企業も、例外なくサイバー攻撃の脅威にさらされている。

中小企業被害実態に関する調査

■調査内容

実証期間：平成30年9月～平成31年1月
実証内容：中小企業30社を対象に、ネットワーク上の通信データ等を一定期間収集。



■調査結果

- 調査した**30社全てでサイバー攻撃**を受けていたことを示す不審な通信が記録されていた。
- 少なくとも5社ではコンピューターウィルスに感染するなどして、**情報が外部に流出したおそれ**があることが分かった。

出典：大阪商工会議所「平成30年度中小企業に対するサイバー攻撃実情調査（報告）」共同研究実施者：神戸大学、東京海上日動火災保険（株）（2019年7月）

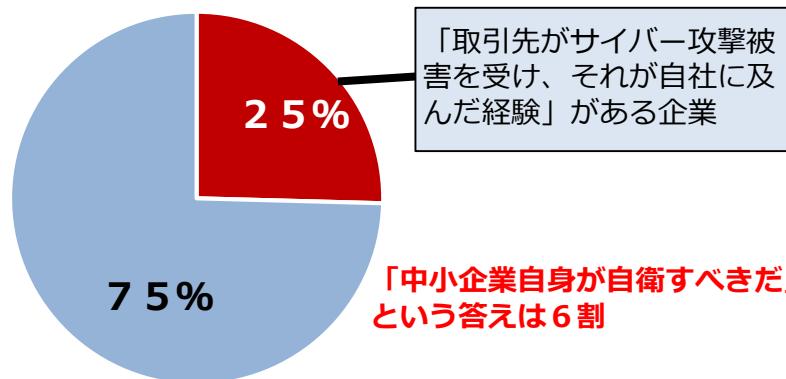
取引先経由の被害に関する調査

■調査内容

調査期間：平成31年2月～3月
調査内容：全国の従業員100人以上の企業を対象に、郵送、FAX、メール、Web、対面による依頼・回答

■調査結果

- 大企業・中堅企業118社に調査したところ、取引先がサイバー攻撃被害を受け、**影響が自社に及んだ経験**がある企業が30社あった（25%）



出典：大阪商工会議所「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」（2019年5月）

中小企業のセキュリティ対策自己宣言「SECURITY ACTION」

- 中小企業自らが、セキュリティ対策に取り組むことを自己宣言する制度（IPA）。
- IT導入補助金の申請において、「SECURITY ACTION」の宣言を必須要件化。
- **10万者を超える中小企業が宣言**（2020年7月末時点）。



情報セキュリティ
5か条に取り組む



情報セキュリティ自
社診断を実施し、基
本方針を策定

＜ご参考＞中小企業の情報セキュリティ対策ガイドライン

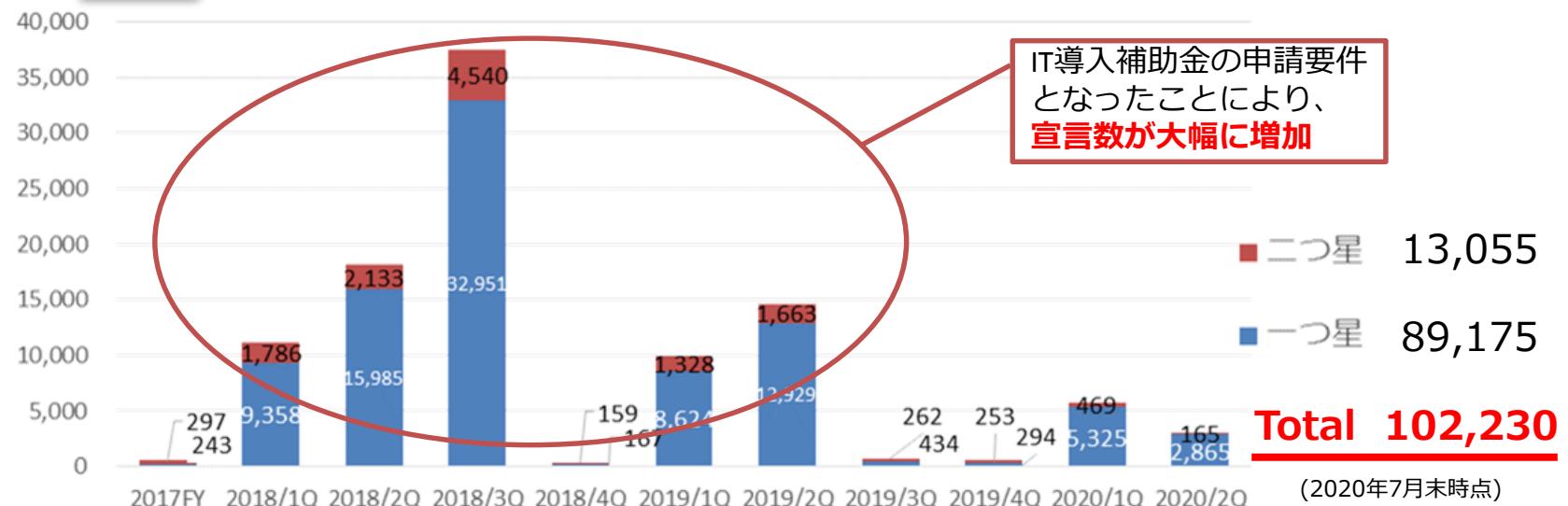


経営者向けの
解説

経営者が認識すべき3原
則と実施すべき重要7項
目を解説

実践者向けの
解説

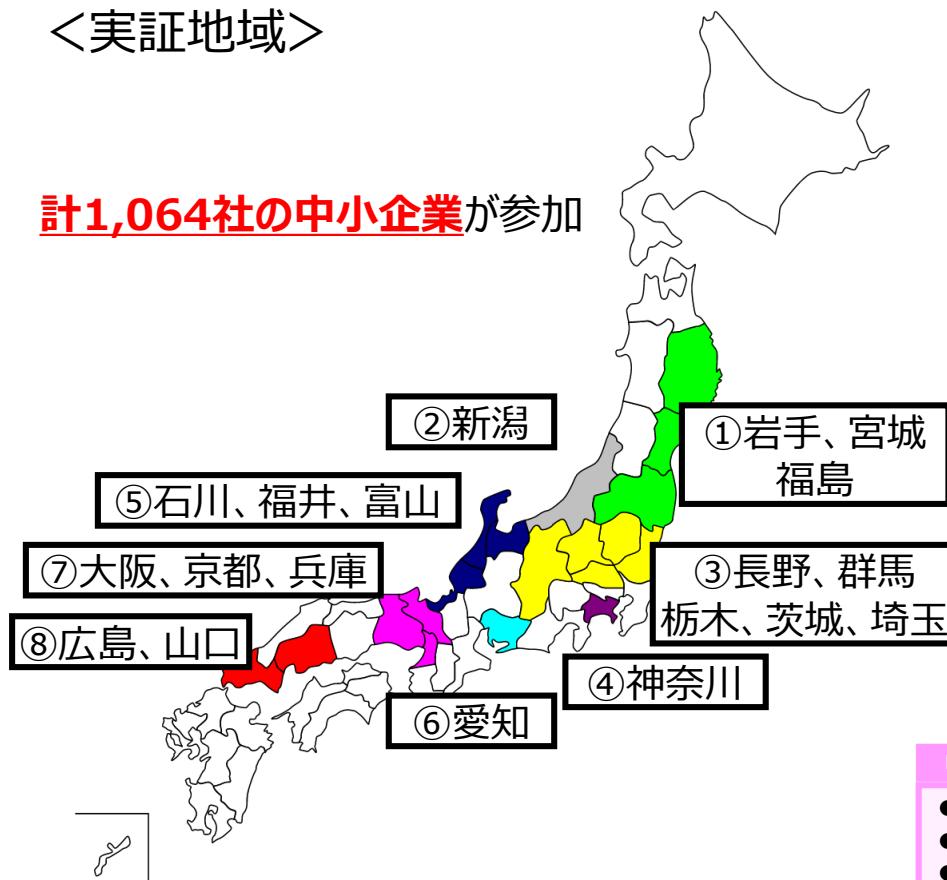
企業のレベルに合わせて段
階的にステップアップできる
ような構成で解説



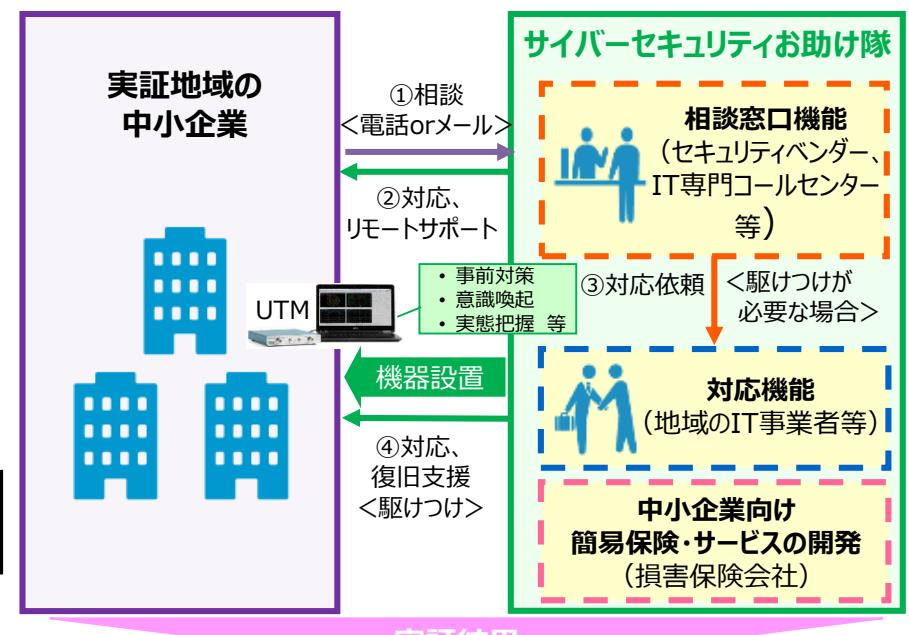
サイバーセキュリティお助け隊実証事業（2019年度の取組）

- 全国**8地域**において、中小企業のセキュリティ対策の促進や意識喚起、攻撃実態や対策ニーズの把握を行い、**民間による中小企業向けのセキュリティサービスの開発を目指し、実証事業を実施。**
- 2019年度の実施内容・成果について、IPAより報告書を公開。（2020年6月15日）

<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

(参考) サイバーセキュリティお助け隊コンソーシアムリスト

地域名	実施主体	実施体制	参加 中小企業数
宮城、岩手、福島	株式会社デジタルハーツ	損害保険ジャパン日本興亜株式会社 株式会社アライブ 地元関係団体多数	111
新潟	東日本電信電話株式会社	東京海上日動火災保険株式会社 東京海上日動リスクコンサルティング株式会社	148
長野、群馬、栃木、茨城、埼玉	富士ゼロックス株式会社	東京海上日動火災保険株式会社	112
神奈川	SOMPOリスクマネジメント 株式会社	損害保険ジャパン日本興亜株式会社 日本PCサービス株式会社 株式会社コムネットシステム 株式会社サイバーセキュリティクラウド 株式会社ラック 学校法人岩崎学園	150
石川、福井、富山	株式会社PFU	アイパブリッシング株式会社 損害保険ジャパン日本興亜株式会社 金沢支店 北陸先端技術大学院大学 PFU西日本株式会社	120
愛知	MS&ADインターリスク総研株式会社	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 NTTアドバンステクノロジ株式会社 綜合警備保障株式会社 デロイトトーマツサイバー合同会社	201
大阪、京都、兵庫	大阪商工会議所	東京海上日動火災保険株式会社 日本電気株式会社 キューアンドエー株式会社	112
広島、山口	株式会社日立製作所	損害保険ジャパン日本興亜株式会社 SOMPOリスクマネジメント株式会社 株式会社日立システムズ 広島県情報産業協会	110

計1,064社の
中小企業が参加

2019年度サイバーセキュリティお助け隊実証事業の結果

- 1,064社が参加した実証期間中に、全国8地域で**計910件のアラート**が発生。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に接続することで、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。

<実証参加の成果（参加中小企業のアンケート結果より）>

<https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html>

- ・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**。（大阪府・建設業）
- ・UTM導入時、当社に**専門知識が無いため、業者と話がかみ合わず、導入に手間取った**。（神奈川県・サービス業）
- ・参加することで、情報セキュリティ対策を実施していることを、外向けにアピールできるのが良い。（新潟県・電気通信工事業）
- ・総務担当がセキュリティを兼務していることもあり、**ワンパッケージでやってくれると非常に助かる**。（石川県・製造業）

2019年度実証事業の結果を踏まえた2020年度実証事業の取組

- 17件の応募があり、**15件を採択**。昨年度事業の結果を踏まえ、サービス内容のスリム化や導入・運用負荷を下げる検討を進めることで、**2021年度以降の民間でのサービス展開に繋げる**。

〈実証地域〉



2021年度以降
民間でのサービス展開

2019度実証で明らかになった実態・課題等

- 業種や規模を問わず内外に向けた不正通信等を数多く検知
- 地域特性、産業特性等の考慮が必要
- 無償の実証事業でも参加の必要性を感じない中小企業が多い
- 中小企業が自社のNW構成図を把握していないかたり人手不足により、機器設置に対応できないケースが多い
- 中小企業の多くはセキュリティ対策にコストを割けない

2020年度実証のポイント

- 全国で**15件**実施。（昨年度の8地域より拡大）
- 地域特性や産業特性等を考慮して進める
- セキュリティ対策への理解を促す意識啓発（継続）
- セキュリティサービスの導入・運用負荷を下げる方法の検討
- サービス内容のスリム化、事前対策等とのセットによるリスク低減方法の検討
- テレワークに留意した実証も実施（例 テレワーク環境での実態調査、テレワークにも対応した機器等）

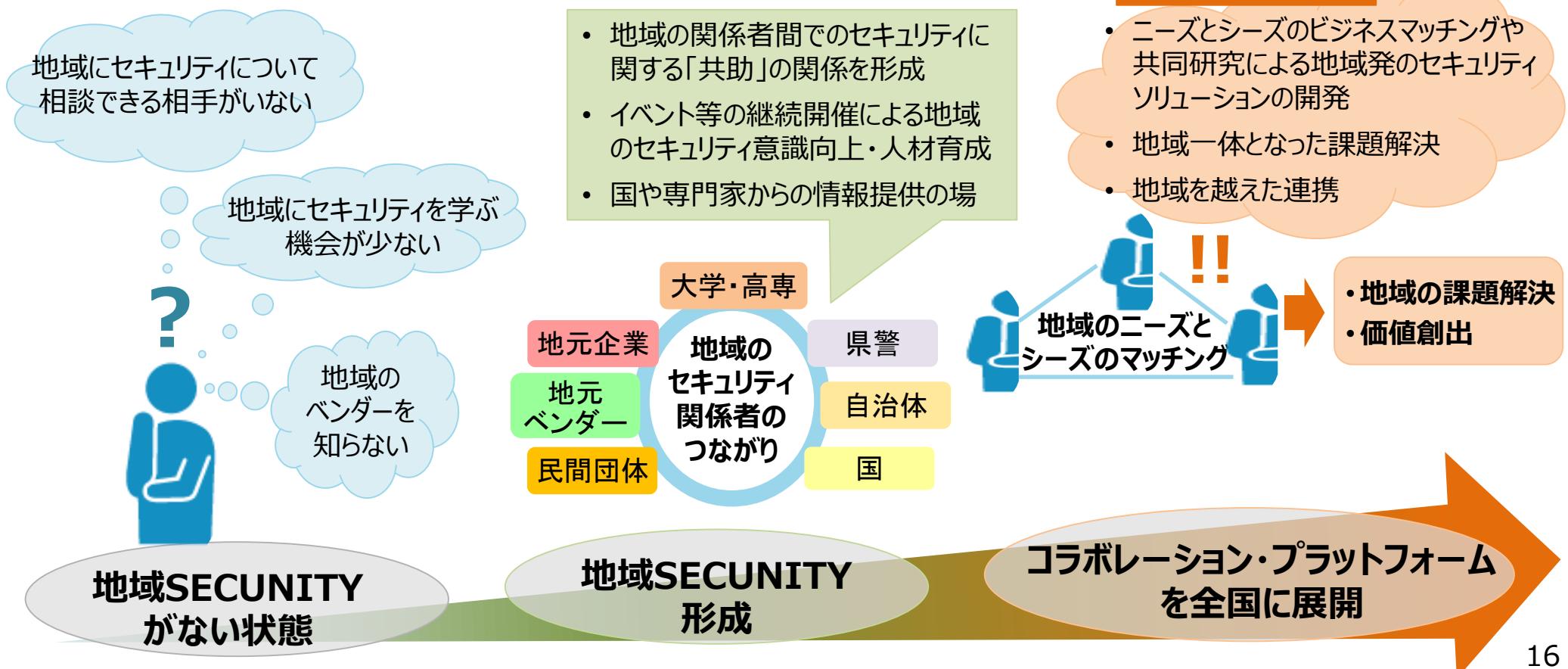
(参考) サイバーセキュリティお助け隊チームリスト (2020年度)

	対象 (地域／産業分野)	実施体制 ●：実施主体		対象 (地域／産業分野)	実施体制 ●：実施主体
①	北海道	●東日本電信電話株式会社 ・東京海上日動火災保険株式会社	⑩	香川県	●高松商工会議所 ・株式会社STNet ・西日本電信電話株式会社 ・キャノンマーケティングジャパン株式会社 ・損害保険ジャパン株式会社 ・東京海上日動火災保険株式会社
②	宮城県、山形県、秋田県、青森県	●東北インフォメーション・システムズ株式会社 ・ハイテックシステム株式会社 ・秋田システムマネージメント株式会社 ・あいおいニッセイ同和損害保険株式会社	⑪	福岡県を中心とした九州 6 県	●株式会社BCC ・日本電気株式会社 ・東京海上日動火災保険株式会社 ・NECフィールディング株式会社
③	岩手県	●富士ソフト株式会社 ・東京海上日動火災保険株式会社	⑫	熊本県	●西日本電信電話株式会社 熊本支店 ・株式会社くまなんピーシーネット ・東京海上日動火災保険株式会社 ・一般社団法人熊本県サイバーセキュリティ推進協議会
④	岩手県、宮城県、福島県	●株式会社デジタルハーツ ・損害保険ジャパン株式会社	⑬	沖縄県	●沖電グローバルシステムズ株式会社 ・株式会社セキュアイノベーション ・ファーストライディングテクノロジー株式会社 ・那覇商工会議所 ・沖縄電力株式会社 ・損害保険ジャパン株式会社
⑤	千葉県、埼玉県	●富士ゼロックス株式会社 ・東京海上日動火災保険株式会社	⑭	防衛・航空宇宙 産業	●株式会社PFU ・株式会社エヴァアビエーション ・富士通株式会社 ・ウェブルート株式会社 ・損害保険ジャパン株式会社
⑥	千葉県	●SOMPOリスクマネジメント株式会社 ・ちばぎんコンピューターサービス株式会社 ・株式会社千葉銀行 ・株式会社ラック ・損害保険ジャパン株式会社	⑮	自動車産業	●東京海上日動リスクコンサルティング株式会社 ・東京海上日動火災保険株式会社 ・エヌ・ティ・ティ・コミュニケーションズ株式会社 ・NTTコム ソリューションズ株式会社 ・NTTセキュリティ・ジャパン株式会社 ・ジェイズ・コミュニケーション株式会社
⑦	岐阜県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 ・中部電力株式会社 ・中部電力ミライズ株式会社 ・株式会社中電シーティーアイ ・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			
⑧	愛知県、岐阜県、三重県	●名古屋商工会議所 ・株式会社日立システムズ ・西日本電信電話株式会社 ・東京海上日動火災保険株式会社 ・損害保険ジャパン株式会社			
⑨	滋賀県、奈良県、和歌山県	●大阪商工会議所 ・日本電気株式会社 ・東京海上日動火災保険株式会社 ・キューアンドエー株式会社			

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>



各地域でのセキュリティコミュニティ形成に向けた取組状況

- コミュニティ形成に向けた取組を実施している地域が増えてきているが、更に取組を広める必要がある。

＜各地域の主な取組状況＞

サイバーセキュリティセミナー in 岩手、秋田、宮城、青森

(東北経産局、IPA、MISEC^{※1}、TiSA^{※2}、自治体他)

令和元年10月に岩手にて地方版コラボレーション・プラットフォーム第1弾を開催。その後、秋田、宮城、青森で順次開催し、セミナーと合わせ懇親会、個別相談会や名刺交換会等を実施



北海道地域情報セキュリティ連絡会（HAISL）

(北海道経産局、北海道総通局、北海道警察)

平成26年9月に発足し、年3回程度セミナー開催（計14回）



関東サイバーセキュリティセミナー

(関東経産局、関東総通局、

一般社団法人テレコムサービス協会 関東支部)

令和2年に東京で関東総通局と連携し、初開催し、セミナーと合わせ名刺交換会を実施



サイバーセキュリティセミナー広島・岡山

(中国経産局、中国総通局、広島県警、岡山県警)

平成31年2月に広島で、3月に岡山で初開催し、令和元年度も2月に岡山、広島で開催



関西サイバーセキュリティ・ネットワーク

(近畿経産局、近畿総通局、KIIS^{※3})

平成30年10月に発足し、人材育成、機運醸成等に取り組む



※1 MISEC…特定非営利活動法人みちのく情報セキュリティ推進機構

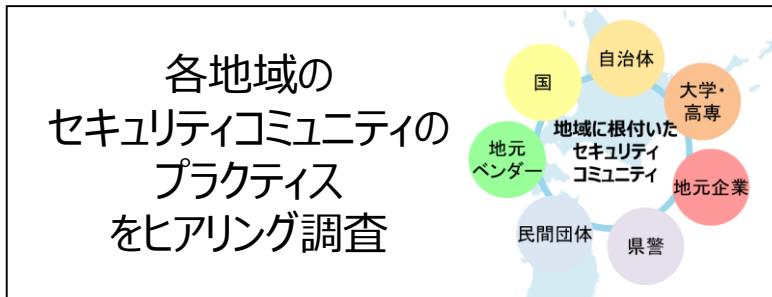
※2 TiSA…東北地域情報サービス産業懇談会

※3 KIIS…一般財団法人関西情報センター

地域に根付いたセキュリティコミュニティ形成促進に向けた令和2年度の取組

- 全国各地で地域に根付いたセキュリティコミュニティの形成を促進するために、「地域セキュリティコミュニティ形成促進のためのプラクティス集」の開発や、専門家派遣制度・団体等のリスト化を行う。

＜今年度の取組＞



インターネット等に掲載

「地域セキュリティ
コミュニティ
形成促進のための
プラクティス集」
を開発



※イメージ

専門家派遣
制度・団体等
をリスト化

各地域に専門家を
派遣可能な制度概要
及び
専門家・団体の
連絡先リスト

参照

新たにセキュリティコミュニティを形成する団体・
取組を拡充したいセキュリティコミュニティ等



令和2年度の取組状況

- 業界団体や専門家、各地方経産局等と連携し、各地域におけるセキュリティ関係者間での意見交換・情報共有等を実施。コミュニティ形成に向けた取組を全国で推進する。

<各地域のコミュニティ形成の促進に向けた支援例>

- 地域のキーパーソン発掘支援
- 地域のセキュリティに関する活動調査
- 地域のセキュリティに関する意識調査
- セキュリティ関連のイベント・演習開催支援
- 講師・専門家派遣
- 他地域のプラクティス集の共有 等



<目指す姿>

継続的に活動できるセキュリティ
コミュニティの形成を促進



先行事例：

<福井県：サイバーセキュリティフォーラム in 福井（8/3）>

- 福井県において、テレワーク時代にあった、サイバーセキュリティの取組機運向上及び域内関係者間のつながりを深めることを目的に実施。
- YouTubeLiveによるオンラインセミナーで148名(※)が参加し、地域の有識者による講演や、メディアが中心となった民間主体のセキュリティコミュニティ「メディアコンソーシアム」の立ち上げ等、県内の取組ピッチを実施。

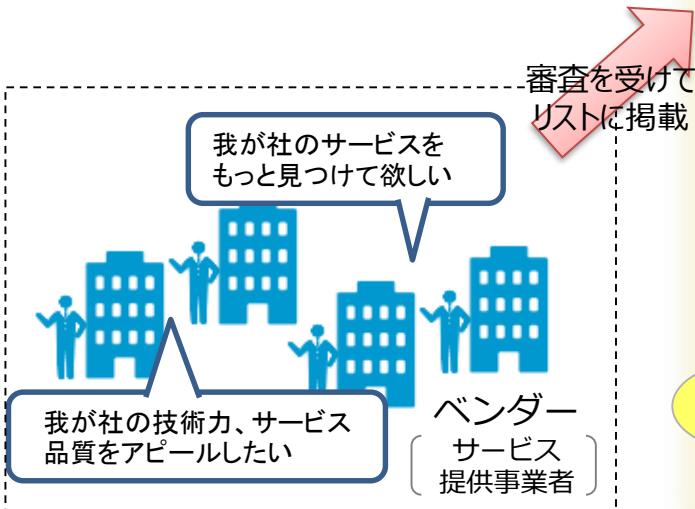
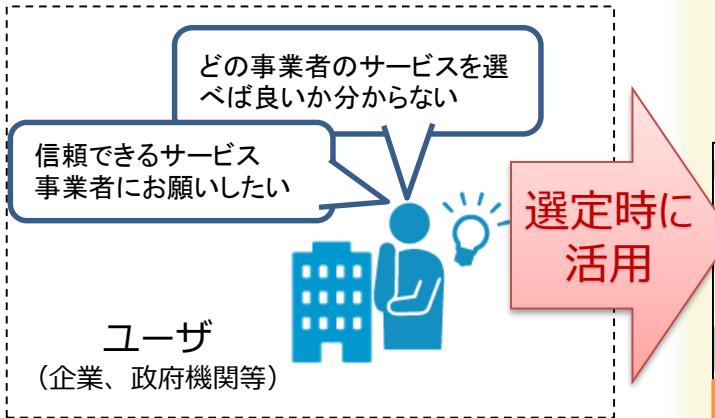


(※)YouTubeの
ユニーク視聴者数。

情報セキュリティサービス審査登録制度の概要

- 一定の技術・品質管理要件を定めた「情報セキュリティサービス基準」を策定し、基準に適合するサービスのリストを2018年6月よりIPAが公開。

<情報セキュリティサービスにおける課題>



○情報セキュリティサービス基準適合

サービスリスト (IPA)

審査登録機関による審査で基準を満たすと認められたサービスをリストとして公開

サービス名	登録年月日	リスト登録年月日	審査登録年月日
情報セキュリティ監査	2018年6月12日	2018年6月12日	2018年6月12日
脆弱性診断	2018年6月12日	2018年6月12日	2018年6月12日
デジタルフォレンジック	2018年6月12日	2018年6月12日	2018年6月12日
セキュリティ監視・運用	2018年6月12日	2018年6月12日	2018年6月12日

基準を満たした 192 サービスが掲載

- 情報セキュリティ監査 (54サービス)
- 脆弱性診断 (76サービス)
- デジタルフォレンジック (26サービス)
- セキュリティ監視・運用 (36サービス)

2020年7月現在

本制度を通じて 目指す社会

専門的知識を持たない
ユーザでも、自社に
最適かつ品質を備えた
サービスを選択できる

技術と品質を備えた
情報セキュリティサービスの
普及・発展

制度の普及・浸透

技術

品質

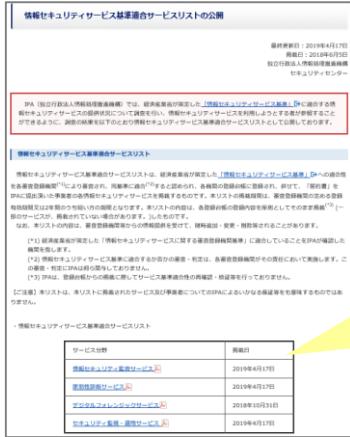
○情報セキュリティサービス基準 (METI)

上記 4 サービスに関して
技術要件・品質管理要件
を定めた基準

情報セキュリティサービス審査登録制度のご活用方法

● サービスをお探しの方

https://www.ipa.go.jp/security/it-service/service_list.html



サービス分野	掲載日
情報セキュリティ監査サービス	2020年6月11日
脆弱性診断サービス	2020年6月11日
デジタルフォレンジックサービス	2020年6月11日
セキュリティ監視・運用サービス	2020年6月11日



IPAのウェブサイトにて『情報セキュリティサービス基準適合サービスリスト』をご覧ください。（無料）

● 本制度に登録したいベンダーの方

<https://sss-erc.org/>



審査登録制度ウェブサイトにて、
登録の流れのご確認、申請書類のダウンロード等が可能です。

登録事業者は自社のウェブページ等に、
情報セキュリティサービス基準に適合することを示す
手段として「情報セキュリティサービスマーク」をお使
いいただけます！



Security Service Standard



※日本セキュリティ監査協会(JASA)は、情報セキュリティサービスに関する審査登録機関基準に適合していることをIPAが確認した機関です。

目次

-
- 1. サイバーセキュリティを巡る状況
 - 2. 国等における主な取組みと中小企業
　向けサイバーセキュリティ対策支援事業
 - 3. 始めましょう SECURITY ACTION !**
 - 4. 参考情報
(IPAのツール・制度のご紹介)



情報セキュリティ対策 よくある質問

- どこからどう始めたら良いか
 - まずは、基本的なセキュリティ対策から実施
 - 組織の実態に合わせ段階的に強化
- どこまで実施すれば良いか
 - 組織における改善点を把握し、対策の周知・実践
 - リスクを受容できるレベルまで実施



SECURITY ACTION の取組みから始める

SECURITY ACTION 制度概要

<https://www.ipa.go.jp/security/security-action/>



- 中小企業自らが情報セキュリティ対策に取組むことを自己宣言する制度
 - 「中小企業の情報セキュリティ対策ガイドライン」の実践をベースに2段階の取組み目標を用意



1段階目（一つ星）

「情報セキュリティ5か条」に取組むことを宣言



2段階目（二つ星）

「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たうえで、「情報セキュリティ基本方針」を定め、外部に公開したことを宣言

SECURITY ACTION 制度の特長

・情報セキュリティ対策への取組みの見える化

- ⌚ ロゴマークをウェブサイトに掲出したり、名刺やパンフレットに印刷することで自らの取組み姿勢をアピール



・顧客や取引先との信頼関係の構築

- ⌚ 既存顧客との関係性強化や、新規顧客の信頼獲得のきっかけに



・公的補助・民間の支援を受けやすく

- ⌚ SECURITY ACTIONを要件とする補助金の申請、普及賛同企業から提供される様々な支援策が利用可能

IT導入補助金2020 : <https://www.it-hojo.jp/>



SECURITY ACTION 一つ星



「情報セキュリティ 5か条」に取組むことを宣言

1. OSやソフトウェアは常に最新の状態にしよう！
2. ウィ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！

中小企業・小規模事業者の皆様へ

情報セキュリティ 5か条

ウチには秘密なんかないなあ…

いいえ、こんな情報があるはずですよ!

- 従業員のマイナンバー、住所、給与明細
- お客様や取引先の連絡先一覧
- 取引先ごとの仕切り額や取引実績
- 新製品の設計図などの開発情報
- 取引先から“取扱注意”として預かった情報

サイバー攻撃といっても、被害など知れているのでは?

漏れたら大変! こんなダメージが!

- 被害者への損害賠償などの支払い
- 取引停止、顧客流出
- ネットの遮断などによる業務効率のダウン
- 従業員の士気低下

情報セキュリティ対策と言っても、何をやれば良いのか分からぬ組織では、裏面の5か条を守るところから始めてみましょう。

裏面をご覧ください

SECURITY ACTION ニつ星



1. 「5分でできる！情報セキュリティ自社診断」で自社の状況を把握する
2. 情報セキュリティ基本方針を定め、外部に公開したことを宣言

中小企業・小規模事業者の皆様へ

新 5分でできる！
情報セキュリティ自社診断

最新動向への対応、できてますか？

脅威や攻撃の変化 IT環境の変化

標的型攻撃 ランサムウェア IoT機器 クラウド
パスワードリスト攻撃 スマートフォン

取り返しのつかないことになる前に
あなたの会社のセキュリティ状況を
「5分でできる！自社診断」でチェック！

+

情報セキュリティ基本方針の記載項目例

- 管理体制の整備
- 法令・ガイドライン等の順守
- セキュリティ対策の実施
- 繼続的改善

など

自社診断のための25項目

- 25項目の設問に答え、自社の情報セキュリティ対策の実施状況を把握

基本的対策 5項目

脆弱性対策、ウイルス対策、
パスワード強化など

従業員としての対策 13項目

標的型攻撃メール、電子メール、持ち出し、廃棄、ウェブ利用など

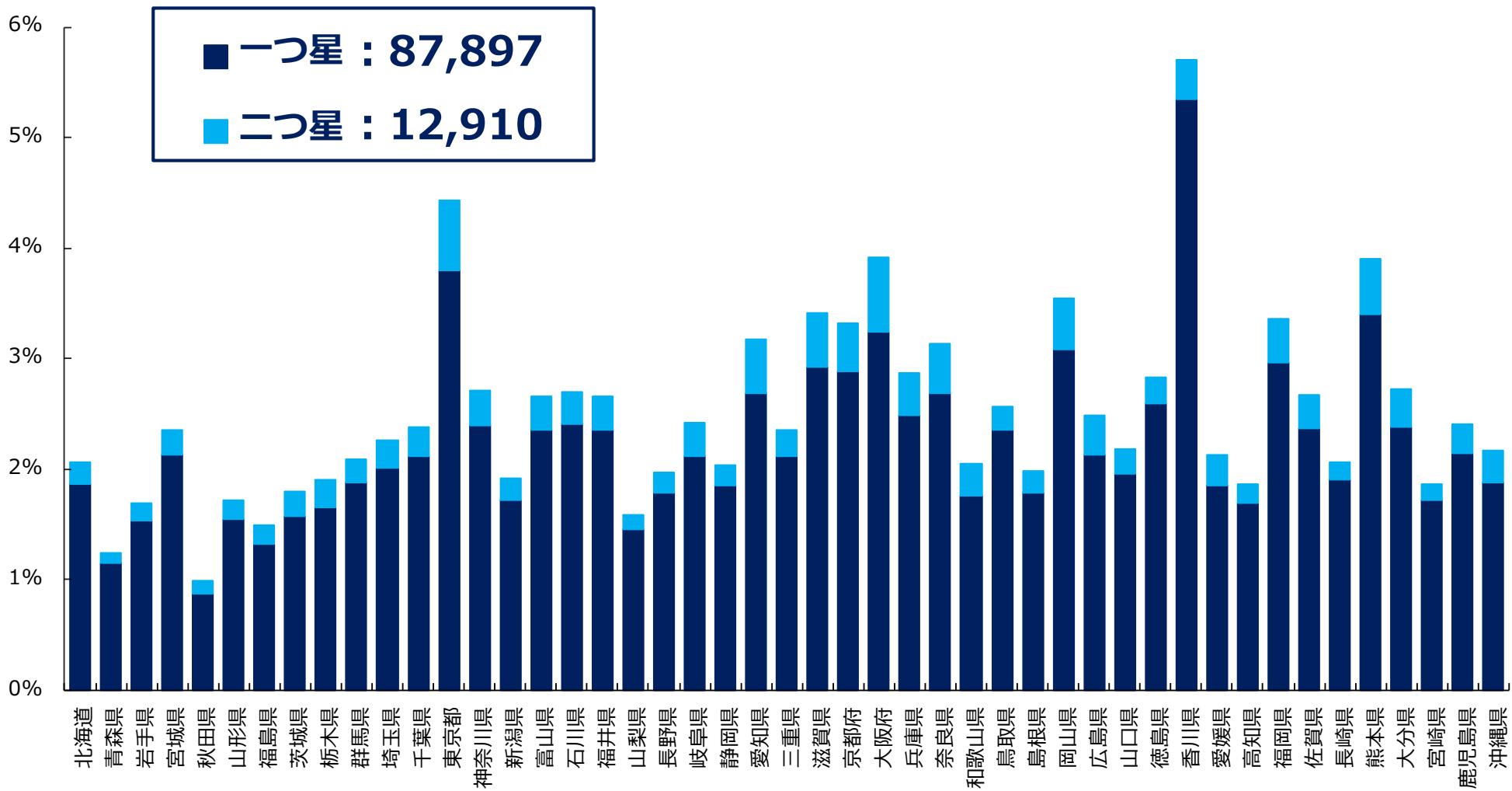
組織としての対策 7項目

守秘義務、インターネット利用、ルール化など

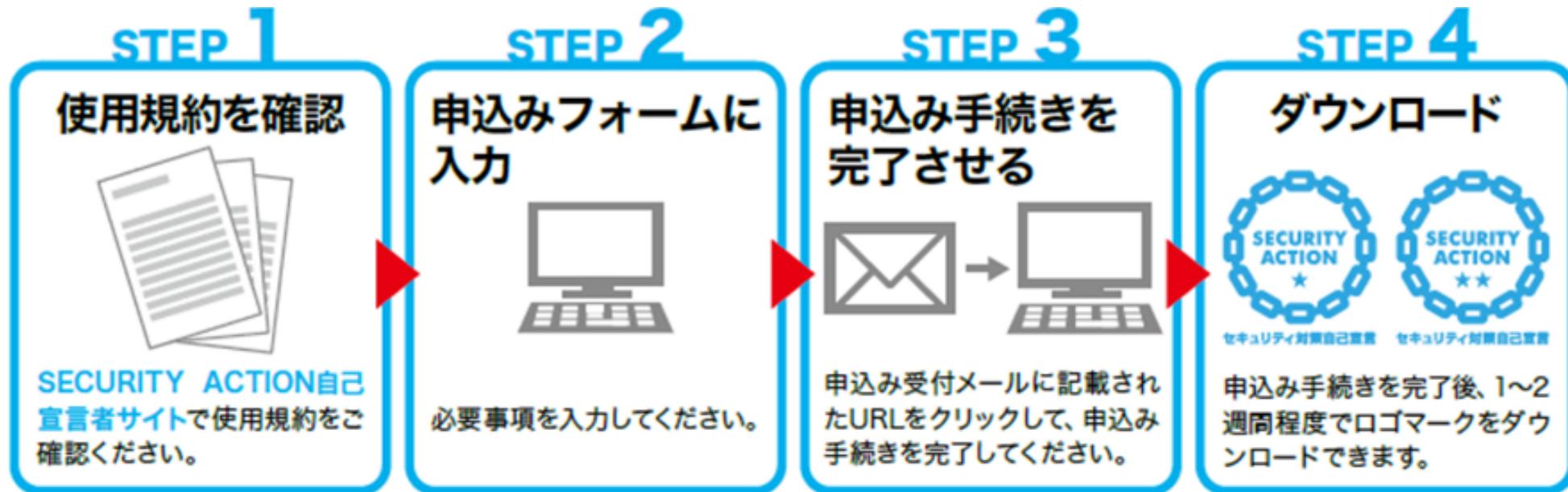
No	診断内容
1	パソコンやスマートフォンなど情報機器のOSやソフトウェアは常に最新の状態にしていますか？
2	パソコンやスマートフォンなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル ^{※1} は最新の状態にしていますか？
3	パスワードは複雑で長い「長く」「複雑な」パスワードを設定していますか？
4	重要情報 ^{※2} に対する適切なアクセス制限を行っていますか？
5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？
6	電子メールの添付ファイルや本文中のURLリンクを介したウイルス感染に気をつけていますか？
7	電子メールやFAXの宛先の送信ミスを防ぐ取り組みを実施していますか？
8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？
9	無線LANを安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？
10	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？
11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？
12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？
13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？
14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？
15	関係者以外の事務所への立ち入りを制限していますか？
16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？
17	事務所が無人になる時の施錠忘れ対策を実施していますか？
18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？
19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？
20	従業員にセキュリティに関する教育や注意喚起を行っていますか？
21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？
22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？
23	クラウドサービスやウェブサイトの運用などで利用する外部サービスは、安全・信頼性を把握して選定していますか？
24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？
25	情報セキュリティ対策（上記1～24など）をルール化し、従業員に明示していますか？

SECURITY ACTION申込状況

中小企業数比 (%) (2020年7月末現在)



SECURITY ACTION 申込手順



SECURITY ACTION自己宣言者サイト

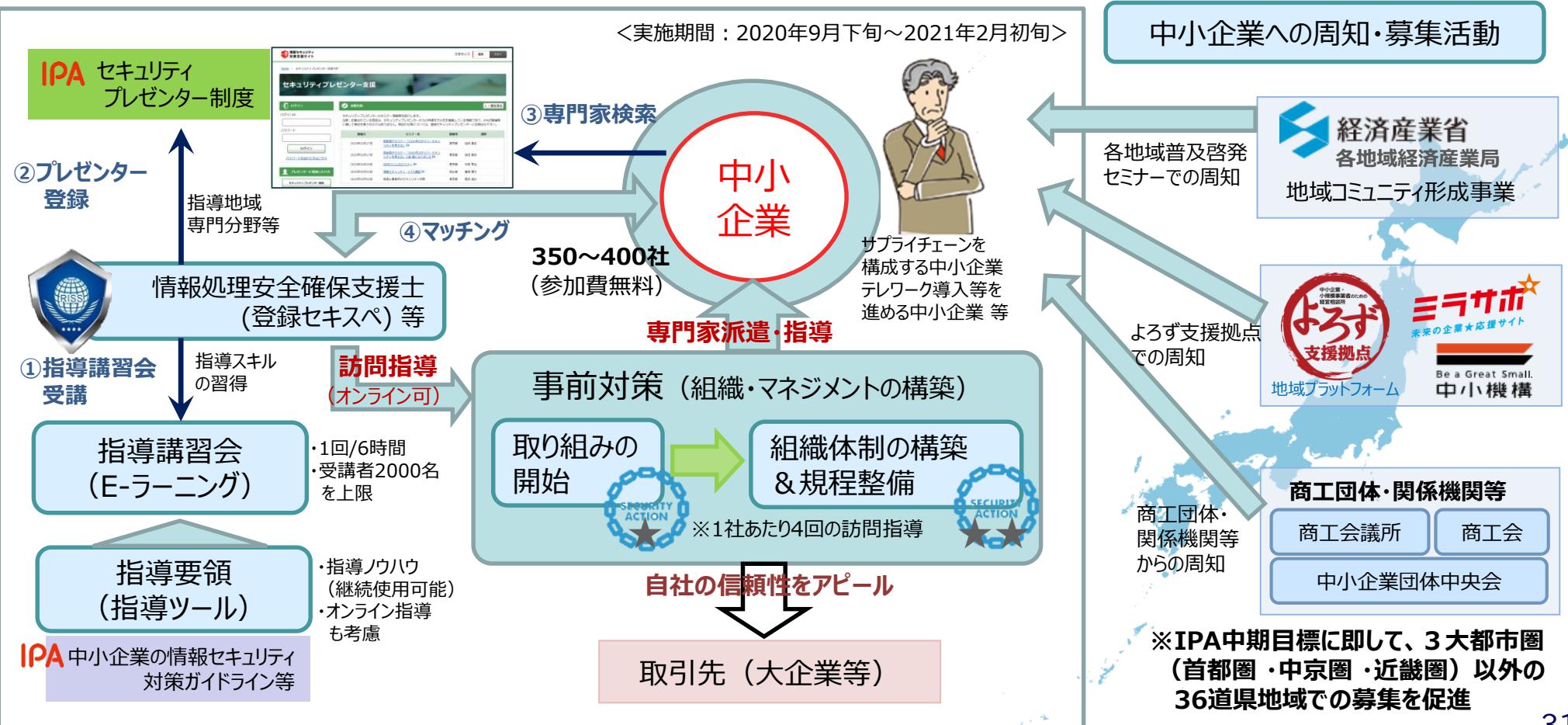
<https://security-shien.ipa.go.jp/security/entry/>





令和2年度 中小企業の情報セキュリティ マネジメント指導業務

- 中小企業向けに情報セキュリティに関するマネジメント体制の構築に向けた支援体制を構築し、**全国の中小企業400社を対象に専門家派遣を実施。**



情報セキュリティマネジメント指導業務 実施概要

専門家には、情報処理安全確保支援士（登録セキスペ）等を起用し、中小企業の現場に応じたリスクの洗い出しから、マネジメントに必要なセキュリティ基本方針や関連規定の策定に向けた支援を実施（1社あたり4回派遣、参加費無料）。

指導業務の進め方と成果物

指導希望企業の現状レベル



セキュリティ対策自己宣言



情報セキュリティ 5 か条



情報処理安全確保支援士

サイバーセキュリティ分野の国家資格で、サイバーセキュリティに関する実践的な知識・技能を有する専門人材

1

SECURITY ACTION の
二つ星宣言を行う



セキュリティ対策自己宣言

現状評価と
気づき



本事業の成果物



情報セキュリティ基本方針
/ 関連規程類

情報セキュリティ対策
実行計画書

2

現在の対策レベルと経営者の意向を把握し、
「中小企業の情報セキュリティ対策ガイドライン」を
活用して、具体的対策の実行計画を作成する

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/>



目次

-
- 1. サイバーセキュリティを巡る状況
 - 2. 国等における主な取組みと中小企業
　向けサイバーセキュリティ対策支援事業
 - 3. 始めましょう SECURITY ACTION !
 - 4. 参考情報
(IPAのツール・制度のご紹介)



情報セキュリティ対策支援サイト

<https://security-shien.ipa.go.jp/>



IPA

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



情報セキュリティ対策支援サイト

文字サイズ 標準 大きく
ログイン 利用者登録 お問い合わせ

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 一般/学生の方

このサイトでできること

情報セキュリティ対策支援サイトは、情報セキュリティ対策を「知りたい」「学びたい」「始めたい」「強化したい」方々と、それを後押しする方々の活動をサポートします。このサイトではそれぞれの役割（経営者、対策実践者、従業員、啓発者／教職員、一般／学生）にあわせて情報セキュリティ対策を進めることができます。

ご自身があなたの役割を上記のタブから選択して情報セキュリティ対策を始めましょう！

知りたい

情報セキュリティ診断
《入門編》5分でできる！情報セキュリティ自社診断
《基本編》情報セキュリティ対策ハンズマーク
《応用編》情報セキュリティ対策ハンズマークPLUS

診断に答えるだけで自社のセキュリティ対策状況を把握することができます。診断後は、診断結果に即した推奨資料や対策が確認できますので、今後の対策に必要な資料を探す必要はありません。

利用者登録をしていただくと、診断結果を保存することができ、過去5回の診断結果や他社、同業他社との比較を行うことができます。

学びたい

5分でできる！ポイント学習
自社診断の質問を1テーマ5分で学べる

情報セキュリティについてe-Learning形式で学習できるツールです。構成の日常の1コマを取り入れた親しみやすい学習テーマで、セキュリティに関する様々な事例を疑似体験しながら適切な対処法を学ぶことができます。また、利用者登録をして頂くと、学習の中断・再読みが可能、これまでの学習進捗状況を表形式で確認することができます。

始めたい

SA自己宣言者サイト
情報セキュリティ対策の取り組みを外部にアピールしよう

情報セキュリティ対策に取り組むことを自己宣言する方を支援するサイトです。本サイトでは、自己宣言の手続き、SECURITY ACTIONロゴマークダウンロード、SECURITY ACTION自己宣言企業の検索などが行えます。

検索

5分ができる！自社診断＆ポイント学習

- ・職場での日常を取り入れた親しみやすいシナリオで、セキュリティに関する様々な事例を疑似体験しながら正しい対処法を1テーマ5分で学べる
- ・学習テーマは自社診断の25の質問と連動



【確認テスト】No.9

Q1 ✕ 不正解

無線LANについて、不適切なのはどれでしょうか。

正答	回答	選択肢
		無線LANは、暗号化が施されているものを選ぶのはもちろん、暗号強度が高いものを選ぶ。
<input checked="" type="radio"/>		急ぎの仕事があったので、街中の無線LANを使って顧客とメールのやり取りを行った。
	<input checked="" type="radio"/>	無線LANに接続する時は、他人に見られないよう、ファイル共有機能をOFFにする。
		社内などで設置した無線LANは、暗号強度の高いものを設定し、パケット捕捉機能をOFFにする。

修了証

おめでとうございます！セイバーライフセキュリティ講座
受講者：小笠原一郎 氏
修了日：2024年4月1日

あなたは、上記テーマの全問題を解答したこと
を認めます。
今後とも、情報セキュリティ対策に積極的
に取り組みます。

株式会社セイバーライフセキュリティ
IPA認定講師

修了証も発行できます

セキュリティプレゼンター制度

- ・IPAのセキュリティ対策資料を活用して、中小企業等に対して普及啓発を行う人材を「セキュリティプレゼンター」として登録する制度
- ・活動地域などを条件にセキュリティ
プレゼンターを検索可能

セキュリティプレゼンター登録タイプ
は次の2種類

公開

「情報セキュリティ対策支援サイト」
で自身のプロフィール、活動等を掲載しPRすることができる。

コンテンツ
利用のみ

「情報セキュリティ対策支援サイト」
から、セキュリティ対策資料等をダウンロードすることができる。

セキュリティプレゼンター詳細		
<div style="background-color: #008000; color: white; padding: 5px; text-align: center;">ログイン</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">ログインID <input type="text"/></div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">パスワード <input type="password"/></div> <div style="background-color: #008000; color: white; padding: 5px; text-align: center;">ログイン</div> <div style="text-align: right; font-size: small;">パスワードを忘れた方はこちら</div>		
<div style="background-color: #008000; color: white; padding: 5px; text-align: center;">アカウントを申請したい方</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">セキュリティプレゼンター登録申請</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">セキュリティプレゼンター登録登録</div>		
性別	相性	名前
男(男性)	アイビー	美子 名(女性) エイコ
<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">活動場所</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">生年月</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">メールアドレス</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">専門機関</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">専門知識</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">市区町村/場所</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">ビル名など</div>		
<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">東京都、埼玉県、神奈川県、千葉県</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">ipa@ips.go.jp</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">113-0551</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">東京都</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">文京区本郷2-28-8</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">文京グリーンコートセンターオフィス</div>		



セキュリティプレゼンター



企業等

映像で知る情報セキュリティ

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



IPA

- ♦ 情報セキュリティに関する様々な脅威と対策を10分程度のドラマなどで分かりやすく解説した映像コンテンツ27タイトル。
- ♦ YouTube「IPAチャンネル」では27タイトルをいつでも視聴可能。主な映像はDVD-ROMでも提供中。

**IPA 独立行政法人
情報処理推進機構**

映像で知る情報セキュリティ

ドラマやデモンストレーションを通じて最新の脅威と対策を学びましょう！

映像約10分
研修に最適！

ウイルス・サイバー攻撃対策

そのメール本当に信頼してもいいですか？
～劇的型サイバー攻撃メールの手口と対策～
企業内の標的型攻撃メールの朝日を両方に、ウイルスが含まれている添付ファイルを開かせる手口を示し、その対策を説明します。

企業・組織(従業員向け) 約10分

見えざるサイバー攻撃
～標的型サイバー攻撃の組織的な対策～
標的型サイバー攻撃で組織的な対応ができるなかったケースの再現ドラマを通じて、標的型サイバー攻撃の組織的な対策のポイントを説明します。

企業・組織(システム管理者向け) 約13分

組織の情報資産を守れ！
～標的型サイバー攻撃に備えて経営者がなぜべき組織マネジメントのポイントを経営者の視点で説明します。

企業・組織(経営者・管理者向け) 約10分

デモで知る！標的型攻撃によるパソコン乗っ取りの脅威と対策
標的型攻撃によるパソコンの乗っ取りについて、その手口や脅威をデモを通して説明すると共に、被害に遭わなかったための対策を説明します。

企業・組織(約7分)

中小企業向け

あなたの会社のセキュリティドクター
～中小企業向け情報セキュリティ知識の基本～
中小企業の情報セキュリティ対策について、その必要性と今まで実践できる情報セキュリティ手法について、開拓ドクターの診断に見立ててわかりやすく説明します。

企業・組織(経営者・管理者向け) 約12分

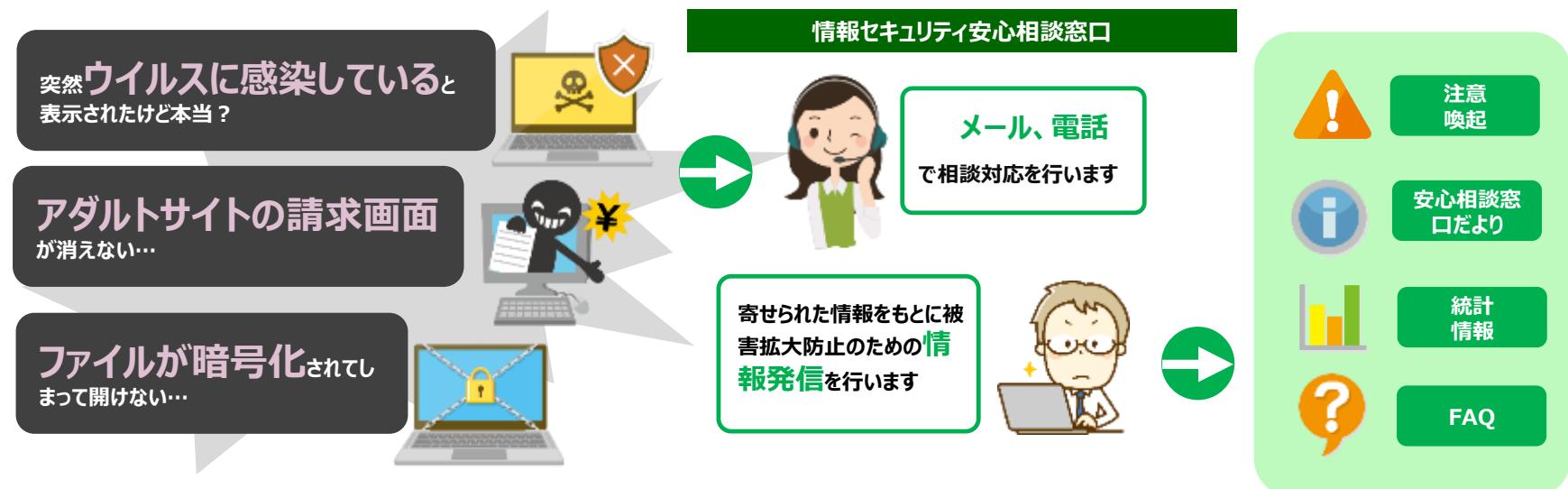
寸劇・ぶちあたる前に学べ！
あなたの職場の“あるある”セキュリティ事故・対策
寸劇その解説を通じて職場における情報セキュリティルールの暗黙文化の重要性などを学べます。

企業・組織(中小企業向け) [前編]約16分
[後編]約12分

IPA 映像 検索

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



IT利用者に求められるIT知識を 習得できる国家試験

IPA

ITパスポート試験

試験の特徴

- ・ITパスポートは、ITを利活用するすべての社会人・学生が備えておくべきITに関する基礎的な知識が証明できる国家試験です。

メリット

試験勉強を通じ、幅広い分野の基礎知識が取得可能！

- ・情報セキュリティや情報モラルに関する知識が身に付きます
- ・企業コンプライアンス・法令遵守に貢献する正しい知識が身に付きます
- ・経営戦略、財務など、経営全般に関する基礎知識が身に付きます
- ・業務に必要なITの基礎知識が身に付きます
- ・システム開発などIT管理に関する基礎知識が身に付きます

試験時間・出題形式

時間区分	試験時間	出題形式	出題数 解答数	基準点
午前	120分	四肢択一	100問	60点 (100点満点)

試験実施概要



・試験実施日

CBT方式で隨時実施中

CBTとは、コンピュータを利用して実施する試験方式のことです。

- ・インターネットにて受付

情報セキュリティマネジメント試験

試験の特徴

- ・IT利用者の情報セキュリティ対策に特化した国家試験です。
- ・社会人として必要な情報セキュリティの知識を体系的に習得できます。
- ・身近な事例をベースにした実践的な出題。

受験をお勧めする方

- ・業務で個人情報を扱う方
- ・業務部門・管理部門で情報管理を担当する方

試験時間・出題形式

時間区分	試験時間	出題形式	出題数 解答数	基準点
午前	90分	多肢選択式 (四肢択一)	50問 50問	60点 (100点満点)
午後	90分	多肢選択式	3問 3問	60点 (100点満点)

試験実施概要



・試験実施日

年2回実施（春期・秋期）

春期：4月第三日曜日

秋期：10月第三日曜日

- ・インターネット・郵便にて受付



新国家資格 「情報処理安全確保支援士」

IPA

通称：登録セキスペ
(登録情報セキュリティスペシャリスト)

サイバーセキュリティに関する実践的な
知識・技能を有する専門人材を育成・確保

①人材の質の担保

- ・「情報セキュリティスペシャリスト試験」をベースとした
新たな試験の合格者を登録
- ・継続的な講習受講義務により、最新の知識・技能を維持

②人材の見える化

- ・資格保持者のみ資格名称を使用
- ・登録簿の整備・登録情報の公開（希望しない者を除く）

③人材活用の安心感

- ・国家資格として厳格な秘密保持義務、信用失墜行為の禁止義務

企業における安全な情報システムの
企画・設計・開発・運用を支援、
サイバーセキュリティ対策の指導・助言を実施

情報処理安全確保支援士
試験受験

登録簿へ登録
(申請が必要)

登録情報の
公開

資格名称の
使用

講習受講

ご清聴ありがとうございました



経済産業省

IPA 独立行政法人
情報処理推進機構