経済産業省

IPA 独立行政法人 情報処理推進機構

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

独立行政法人情報処理推進機構（IPA）
セキュリティセンター
企画部 中小企業支援グループ
横山　尚人

独立行政法人 情報処理推進機構（IPA）とは

- 経済産業省の政策実施機関として：

情報セキュリティ対策を実現

- ウイルス・不正アクセス等の**情報受付**
- 情報セキュリティ対策の**普及啓発**
- 標的型サイバー攻撃情報の**共有・初動対応**

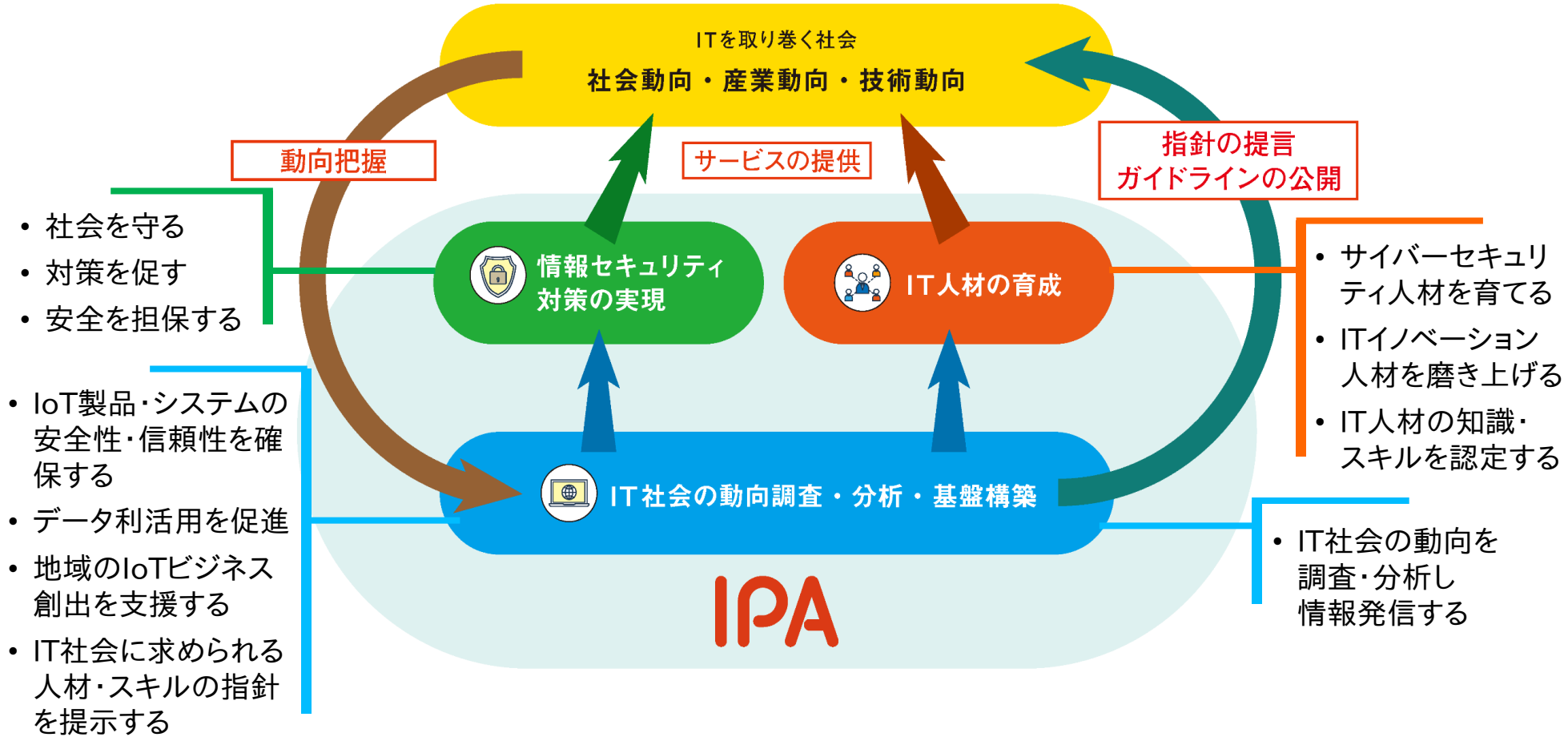
IT人材を育成

- 国家試験「**情報処理技術者試験**」実施・国家資格「**情報処理安全確保支援士**」認定
- **イノベーション人材**の育成・発掘の取組
- 産業サイバーセキュリティ対策を担う**中核人材**育成

IT社会の動向を調査・分析し基盤構築

- **先端技術情報**の収集・調査分析
- 各種**指針**の策定・**ガイドライン**の公開
- IT利活用のための**基盤構築**

IPAの役割：日本企業のDXを支援するために



１．はじめに
～情報セキュリティ10大脅威などから

２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．サイバーセキュリティ支援施策
～地域、経営、人材

4．はじめましょう、サイバーセキュリティ
～「SECURITY ACTION」と
「中小企業の情報セキュリティ対策ガイドライン」

5．参考情報
（IPAのツール・制度のご紹介）

情報セキュリティ10大脅威 2021

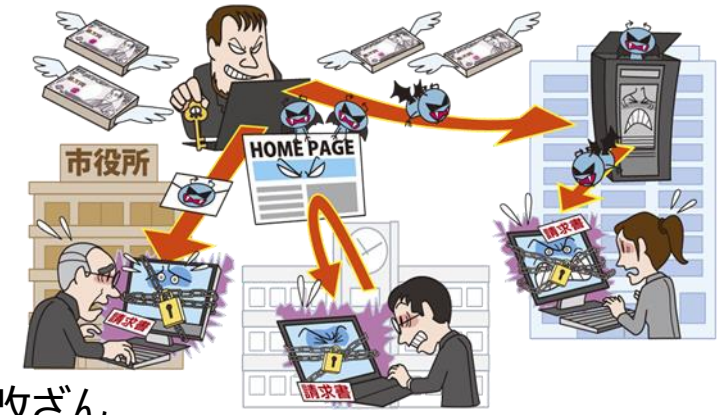
昨年順位	個　人	順 位	組　織	昨年順位
→ 1位	スマホ決済の不正利用	**1位**	**ランサムウェアによる被害**	5位 ↗
→ 2位	フィッシングによる個人情報の詐取	**2位**	**標的型攻撃による情報流出**	1位 ↘
↗ 7位	ネット上の誹謗・中傷・デマ	**3位**	**テレワーク等のニューノーマルな働き方を狙った攻撃**	NEW —
↗ 7位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	**4位**	**サプライチェーンの弱点を悪用した攻撃**	4位 →
↘ 3位	クレジットカード情報の不正利用	**5位**	ビジネスメール詐欺による金銭被害	3位 ↘
↘ 3位	インターネットバンキングの不正利用	**6位**	内部不正による情報漏えい	2位 ↘
↗ 10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**	予期せぬIT基盤の障害に伴う業務停止	6位 ↘
↗ 9位	偽警告によるインターネット詐欺	**8位**	インターネット上のサービスへの不正ログイン	16位 ↗
↘ 6位	不正アプリによるスマートフォン利用者への被害	**9位**	不注意による情報漏えい等の被害	7位 ↘
↘ 8位	インターネット上のサービスへの不正ログイン	**10位**	脆弱性情報等の公開に伴う悪用増加	14位 ↗

<出典：(独)情報処理推進機構(IPA)、202011.27.>

【１位】ランサムウェアによる被害

～ランサムウェアに感染しないための対策と感染時の対処を知る～

- **ランサムウェアとは**
  - 「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語。
  - 感染したパソコンのデータを暗号化するなど使用不可能にし、その**解除と引き換えに金銭を要求**する。

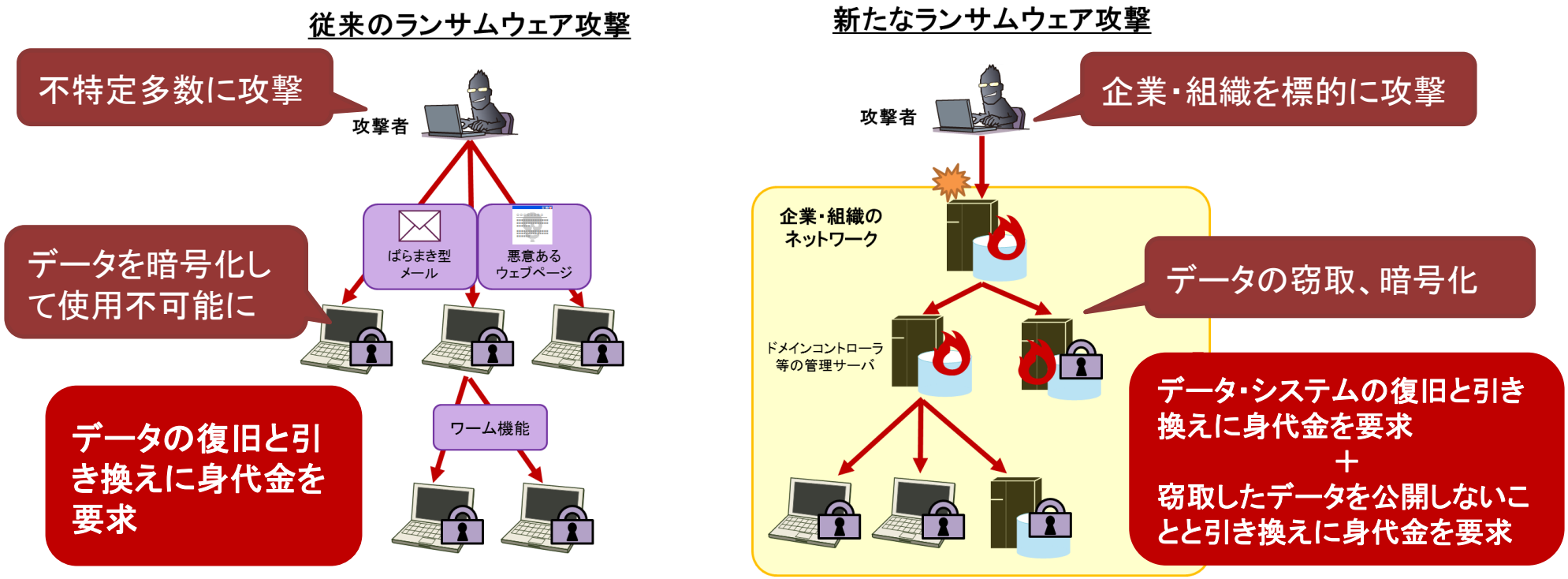


- 攻撃の手口
  - メールを利用した手口
    - ・不正な添付ファイルを開かせる
  - ウェブサイトを利用した手口
    - ・ランサムウェアをダウンロードさせるように ウェブサイトを改ざん
  - 脆弱性を悪用した手口
    - ・OSの脆弱性を悪用しウイルスを実行（感染させる）
  - 不正アクセスによる手口
    - ・サーバーに不正アクセスした攻撃者がウイルスを実行（感染させる）

ランサムウェアの手口の変化（二重の脅迫）

2020年12月18日経済産業省公開資料

- **新たな（標的型）ランサムウェア攻撃（二重の脅迫）とは**
  - ターゲットとなる企業・組織内のネットワークへ侵入し、パソコン等の端末やサーバ上のデータを窃取した後に一斉に暗号化してシステムを使用不可能にし、脅迫をするサイバー攻撃。
  - システムの**復旧に対する金銭要求**に加えて、窃取した**データを公開しない見返りの金銭要求**も行うので、**二重の脅迫**と恐れられる。窃取された情報に顧客の情報や機微情報を含む可能性がある場合には、被害組織は**より困難な判断を迫られること**になる。



【2位】標的型攻撃による機密情報の窃取
～引き続き行われる標的型攻撃、様々な仕掛けで発見を遅らせる～

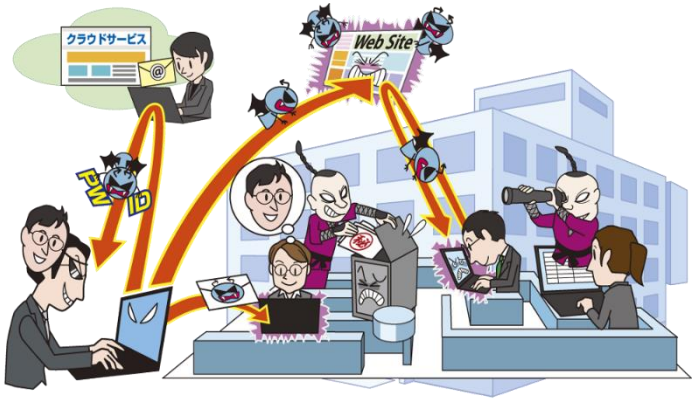
- メール等によりPCをウイルスに感染させ組織内部へ潜入
- 長期にわたって侵害範囲を徐々に広げる
- 組織の機密情報を窃取

● 攻撃手口

10大脅威2020より

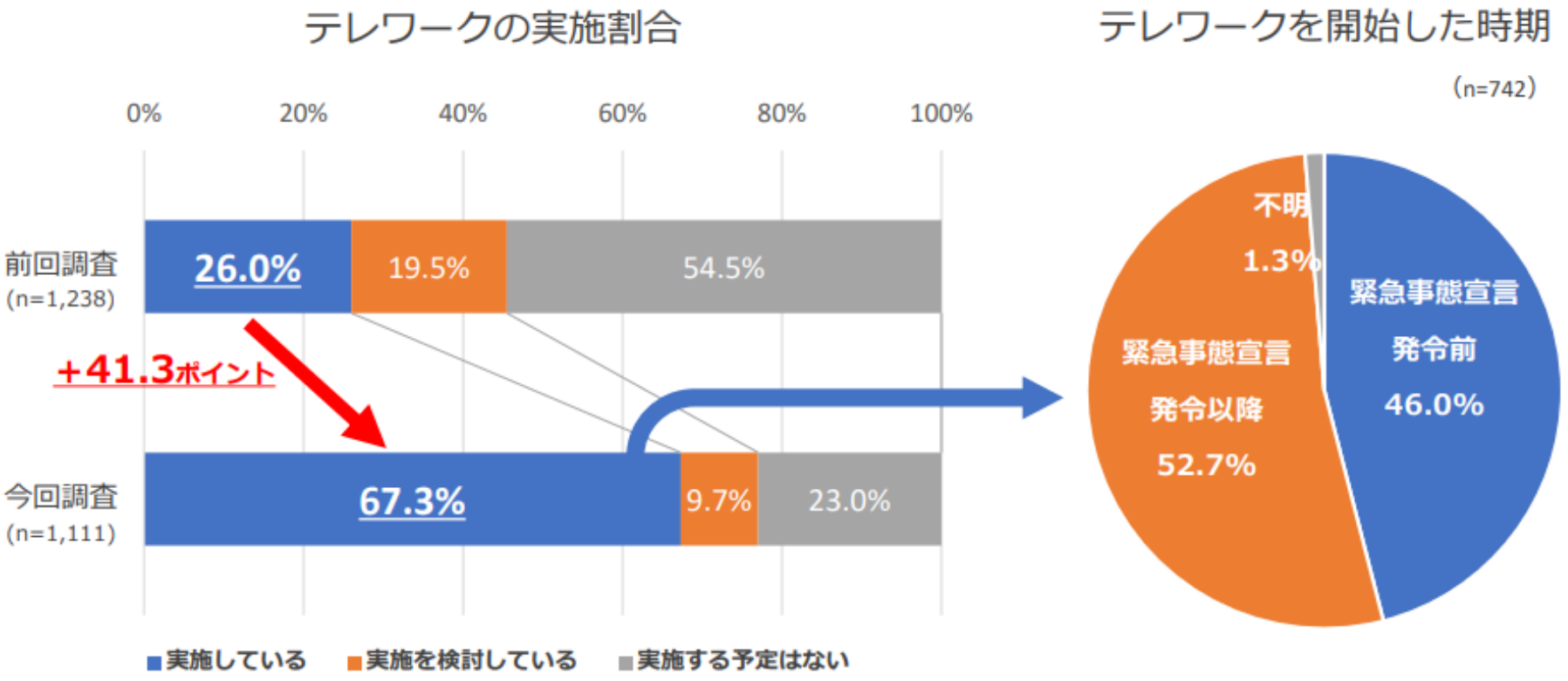
メールやウェブサイトからウイルスに感染させる

- メールを利用した手口（標的型攻撃メール）
  - 不正な添付ファイルを開かせる
  - 不正なウェブサイトへのリンクをクリックさせる
- ウェブサイトを利用した手口
  - 標的組織がよく利用するウェブサイトを調査し、このサイトを閲覧するとウイルスに感染するように改ざん（水飲み場型攻撃）
- 不正アクセスによる手口
  - 組織が利用するクラウドサービスへ不正にログイン
  - 社内システムへ正規の経路を悪用し不正にアクセス
  - 社内システムへウイルスを感染させる



【3位】テレワーク等のニューノーマルな働き方を狙った攻撃

- 急速に進むテレワーク
  - 新型コロナウイルス感染症(COVID-19)の影響により、ICTを用いて自宅でも業務が行えるような環境を整えて、従業員等を出社させずに事業継続を図る動きが急速に進んでいる



※前回調査：「会員企業の防災対策に関するアンケート　付帯調査　新型コロナウイルス感染症への対応について」（公表：2020年4月8日）
調査期間：2020年3月13日～31日　／　回答企業：東商会員企業1,333社（13,297件にFAX・メールにて調査票を送付し依頼）　／　回答率：10.0%

【出典】東京商工会議所「テレワークの実施状況に関する緊急アンケート」調査結果（2020年6月17日）

【3位】テレワーク等のニューノーマルな働き方を狙った攻撃

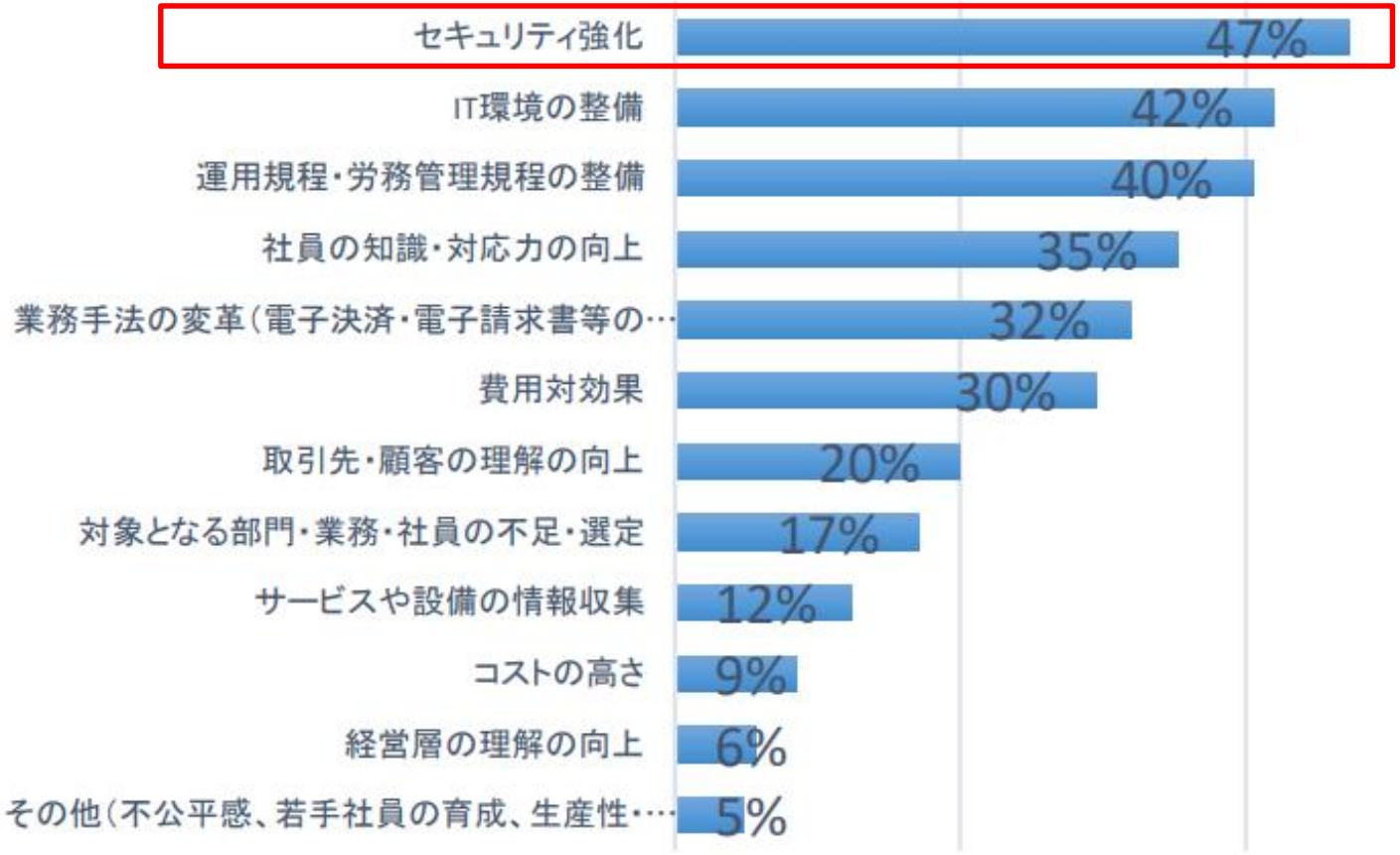
- テレワークとは
  - ICT（情報通信技術）を活用した、場所や時間にとらわれない柔軟な働き方のこと
    - 「tele ＝ 離れた所」と「work ＝ 働く」をあわせた造語
  - テレワークの形態

形態	特徴
在宅勤務	自宅を就業場所とする働き方
モバイルワーク	移動中（交通機関の車内など）や顧客先、カフェなどを就業場所とする働き方
サテライトオフィス勤務	所属するオフィス以外の他のオフィスや遠隔勤務用の施設を就業場所とする働き方

- テレワーク環境を構築するシステムの方式
  - 会社PCの持ち帰り：会社で使用しているPCを社外に持ち出して業務を実施
  - クラウド型アプリ方式：オフィス内外からクラウド型アプリにアクセス
  - リモートデスクトップ方式：遠隔でデスクトップを操作
  - 仮想デスクトップ方式：個人に割り当てた仮想デスクトップを操作

【3位】テレワーク等のニューノーマルな働き方を狙った攻撃

- テレワークの導入後の課題
  - テレワーク導入後の継続課題は、「セキュリティ強化」（47%）、「IT環境の整備」（42%）、「運用規程・労務管理規程の整備」（40%）など



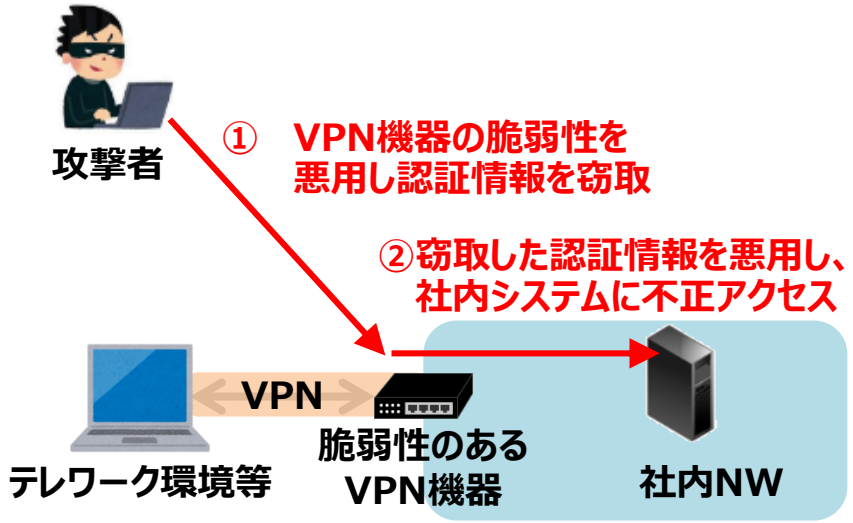
【出典】大阪商工会議所「中小企業のテレワークについての緊急アンケート調査」結果について（2020年6月19日）

ネットワーク貫通型：VPN機器の脆弱性を悪用したネットワークへの侵入

2020年12月18日経済産業省公開資料より

- **VPN（バーチャル プライベート ネットワーク）機器の脆弱性**が相次いで報告され、そうした脆弱性を**悪用するコードが公開**されるなど深刻な状況が発生。**攻撃者はこうした脆弱性を通じて直接的に社内ネットワークへ侵入**し、攻撃を展開。
- 2020年8月、Pulse Secure製VPN機器の脆弱性が悪用され、**国内外900以上の事業者からVPNの認証情報が流出**。2020年11月、Fortinet製品の**VPN機能の脆弱性の影響を受ける約5万台の機器に関する情報が公開。 認証情報等が悪用されることで容易に侵入されるおそれ。**
- **どちらのケースも既に悪用されている可能性**があるため、**機器のアップデートや多要素認証の導入といった事前対策**に加え、事後的措置として**侵害有無の確認や、パスワード変更等の対応**が必要。

VPN機器に対する不正アクセス



Pulse Secure製VPN機器の脆弱性

2019年4月	脆弱性情報公開
2019年8月	脆弱性の悪用を狙ったとみられるスキャンを確認
2019年9月	脆弱性を悪用したとみられる攻撃を確認
2020年8月	国内外900社（国内は38社）の認証情報が公開

Fortinet製FortiOSの脆弱性

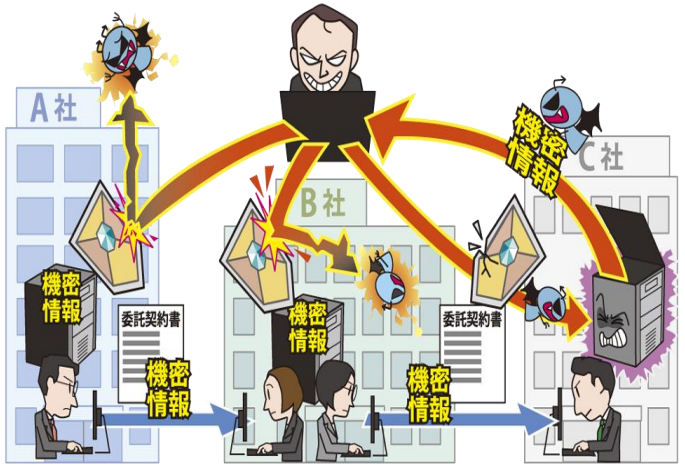
2019年5月	脆弱性情報公開
2019年8月頃	脆弱性の詳細情報公開、悪用やスキャン開始
2020年11月	脆弱性の影響を受ける約5万台の機器情報が公開 IPアドレス、ユーザーアカウント名、平文パスワード等

https://www.jpcert.or.jp/newsflash/2020112701.html
https://www.jpcert.or.jp/at/2019/at190033.html

【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

- 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



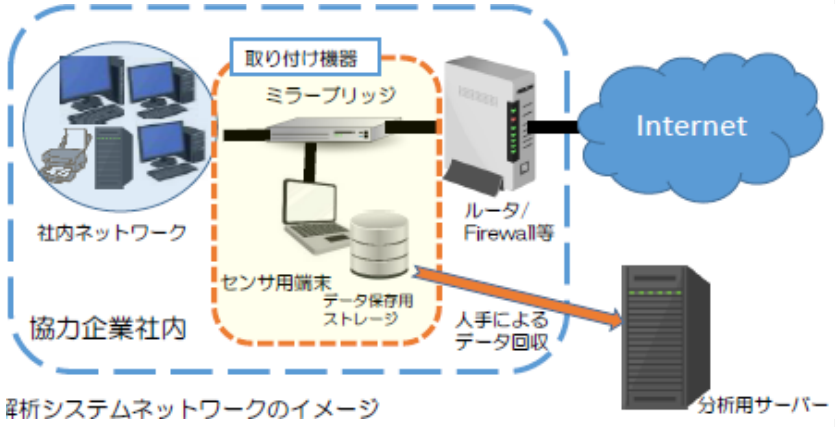
中小企業に対するサイバー攻撃の調査・分析結果（大阪商工会議所）

- 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。



解析システムネットワークのイメージ

■ 調査結果（中間報告）

- 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イ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。

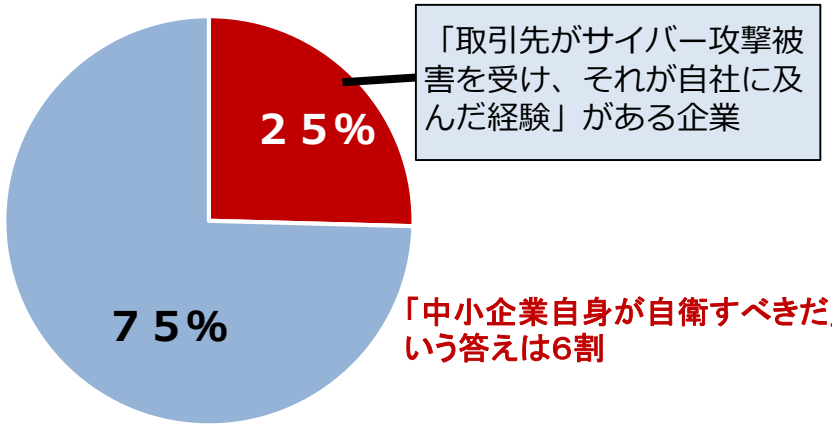
取引先経由の被害に関する調査

■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（中間報告）

- 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）

<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）>

令和元年度の取組：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**5,000万円**近くなる事案も。

＜駆け付け支援件数＞

対応種別	総数	内容	発生件数
インシデント対応	128件	**電話及びリモートによるインシデント対応※**	**110件**
		訪問によるインシデント対応	**18件**

※電話及びリモートによるインシデント対応には、訪問によるインシデント対応の一次対応を含む。

＜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としか接続できないプリンタを使用するために、**マルウェア対策ソフト未導入のWindows XP端末を使用**し感染。

・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**される。

・私物iPhoneにインストールされたアプリが、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**。

・感染により連絡先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

・**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。

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

「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」

2020年12月18日
経済産業省公開資料

●サイバー攻撃は規模や烈度の増大とともに多様化する傾向にあり、実務者がこれまでの取組を継続するだけでは対応困難になっている。
●アップデート等の基本的な対策の徹底とともに、**改めて経営者のリーダーシップが必要に**。

① 攻撃は格段に高度化し、被害の形態も様々な関係者を巻き込む複雑なものになり、技術的な対策だけではなく関係者との調整や事業継続等の判断が必要に。改めて経営者がリーダーシップを。

② ランサムウェア攻撃による被害への対応は企業の信頼に直結。経営者でなければ判断できない問題。

●「二重の脅迫※」によって、顧客等の情報を露出させることになるリスクに直面。日常的業務の見直しを含む事前対策から情報露出に対応する事後対応まで、経営者でなければ対応の判断が困難。
●金銭支払いは犯罪組織への資金提供とみなされ、制裁を受ける可能性のあるコンプライアンスの問題。

③ 海外拠点とのシステム統合を進める際、サイバーセキュリティを踏まえたグローバルガバナンスの確立を。

●国・地域によってインターネット環境やIT産業の状況、データ管理に係るルール等が異なっており、海外拠点とのシステム統合を通じてセキュリティ上の脆弱性を持ち込んでしまう可能性も。
●拠点のある国・地域の環境をしっかりと評価し、リスクに対応したセグメンテーション等を施したシステム・アーキテクチャの導入や拠点間の情報共有ルールの整備等、グローバルガバナンスの確立が必要。

④ 基本行動指針（高密度な情報共有、機微技術情報の流出懸念時の報告、適切な場合の公表）**の徹底を。**

※攻撃者が、被攻撃企業が保有するデータ等を暗号化して事業妨害をするだけではなく、暗号化する前にあらかじめデータを窃取しておいて支払いに応じない場合には当該データを公開することで、被攻撃企業を金銭の支払いに応じざるをえない状況に追い込む攻撃形態。

経済産業省「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起（2020年12月18日）」https://www.meti.go.jp/press/2020/12/20201218008/20201218008.html

取引先等のサイバー攻撃による自社への影響

- 委託先がサイバー攻撃をうけることにより、懸念される自社への影響は？

1

委託先に預けた機密情報が**漏えい**する。

2

委託先システム、生産設備停止に伴い、**納期が遅れる**。

3

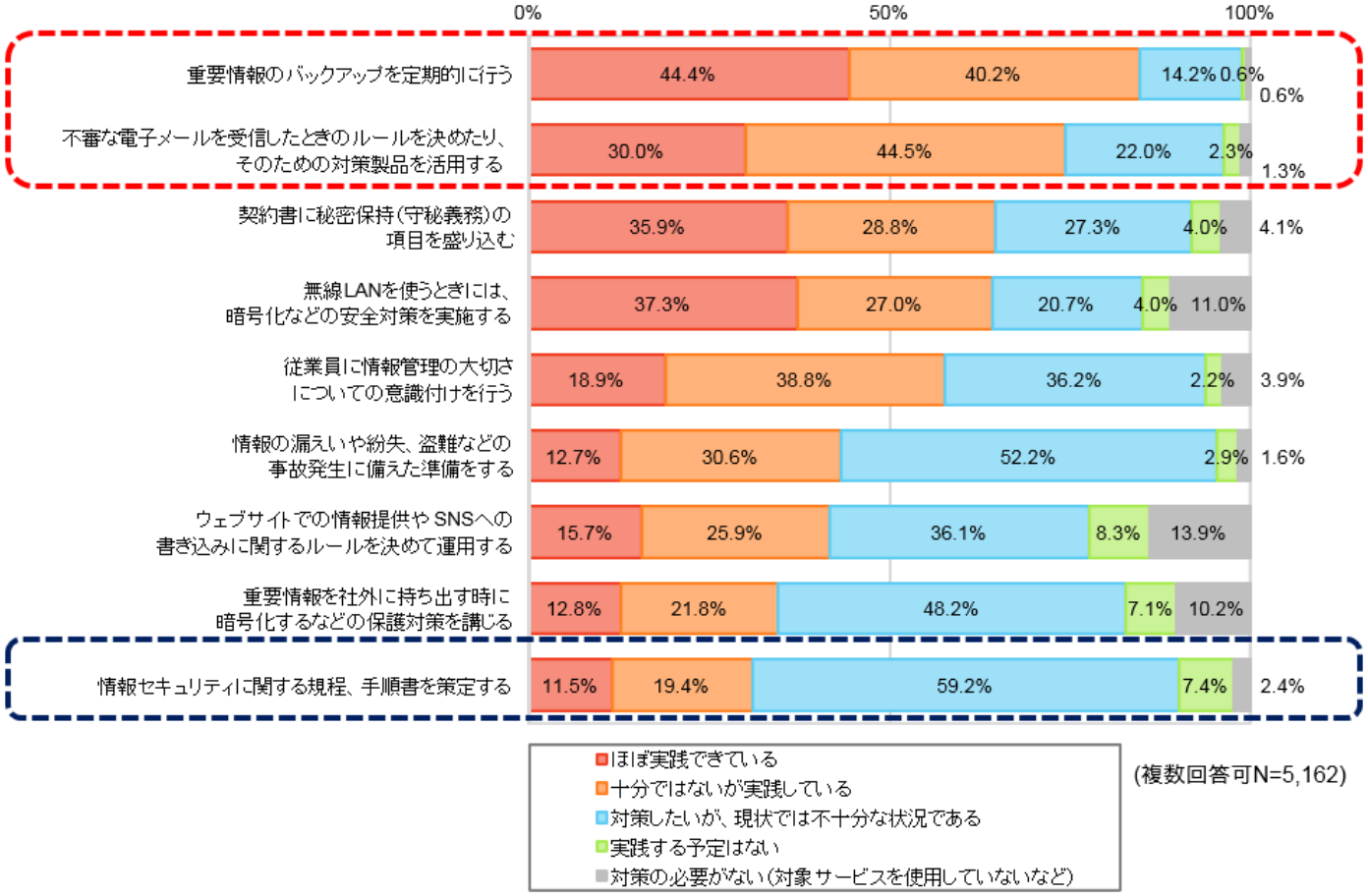
委託先から納入されたプログラムに、**不正コードが混入**している。

4

機器等のメンテナンスのために委託先が持ち込んだPC等から**マルウェア感染**する。

中小企業における対策の状況
～具体的な取組み状況

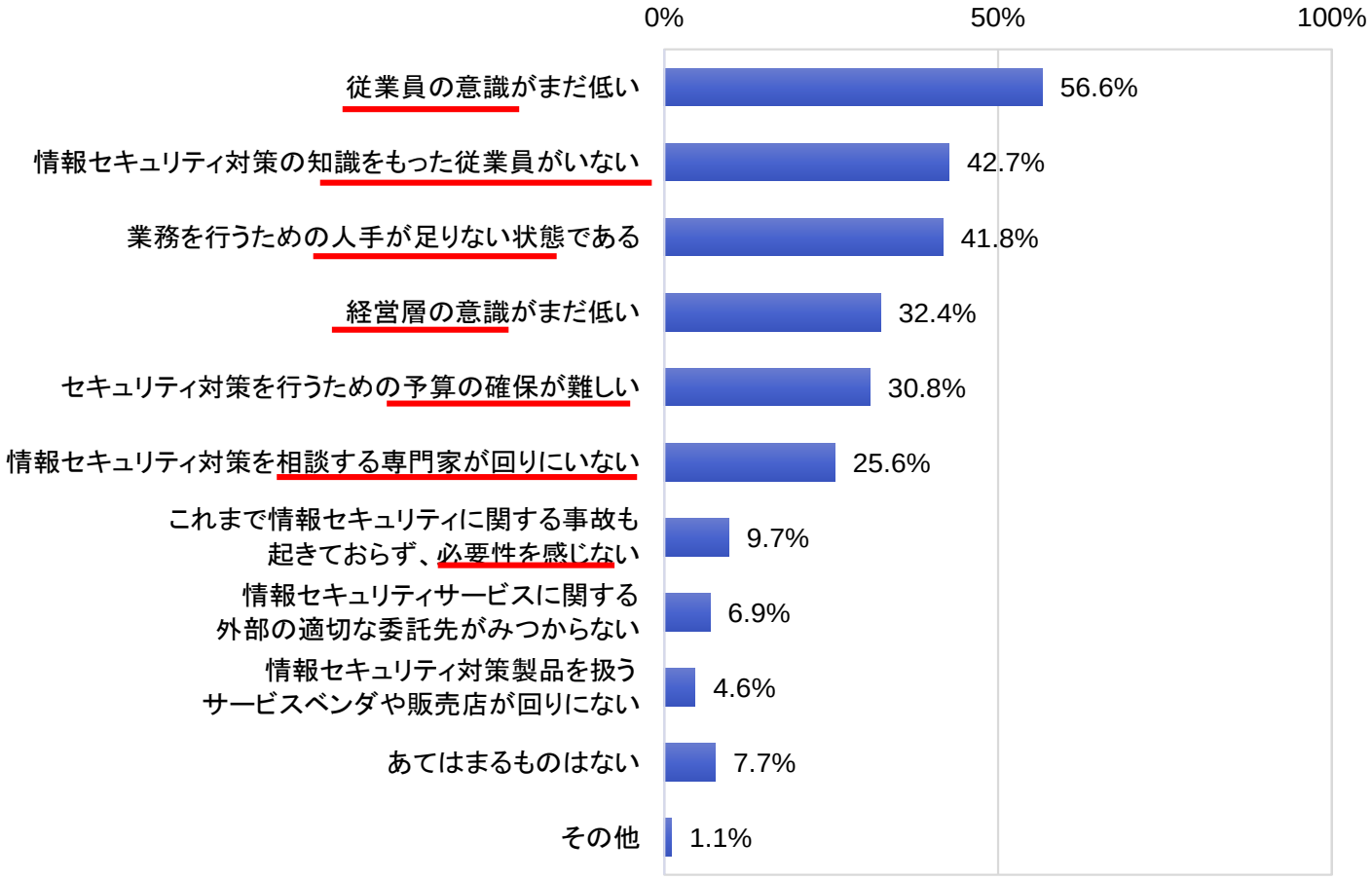
- 「重要情報のバックアップを定期的に行う」が 84.6%と最も高く、次いで「不審な電子メールを受信時のルール、対策製品活用」が74.5%
- 一方、「情報セキュリティに関する規定、手順書策定」は30.9%止まり



出典：IPA「2018年度SECURITY ACTION宣言事業者における情報セキュリティ対策の実態調査」 https://www.ipa.go.jp/files/000072383.pdf

中小企業における対策の状況
情報セキュリティ対策を進める上での課題点

- 「従業員の意識がまだ低い」が最も高く**56.6%**
- 「情報セキュリティ対策の知識をもった従業員がいない」が**42.7%** 、「業務を行うための人手が足りない状態である」が**41.8%**



出典：IPA「2018年度SECURITY ACTION宣言事業者における情報セキュリティ対策の実態調査」 https://www.ipa.go.jp/files/000072383.pdf

１．はじめに
～情報セキュリティ10大脅威などから

２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．サイバーセキュリティ支援施策
～地域、経営、人材

４．はじめましょう、サイバーセキュリティ
～「SECURITY ACTION」と
「中小企業の情報セキュリティ対策ガイドライン」

５．参考情報
（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

産業サイバーセキュリティ研究会

第１回：平成29年12月27日　開催
第２回：平成30年　5月30日　開催
　アクションプラン（４つの柱）を提示
第３回：平成31年　4月19日　開催
　アクションプランを加速化する３つの指針を提示
第４回：令和2年　　4月17日　開催（電話開催）
　産業界へのメッセージを発信
第５回：令和2年　　6月30日　開催
　サイバーセキュリティ強化運動の展開

構成員

※2020年4月開催時点

- 泉澤　清次　三菱重工業株式会社取締役社長
- 遠藤　信博　日本経済団体連合会サイバーセキュリティ委員長、日本電気株式会社取締役会長等
- 大林　剛郎　日本情報ｼｽﾃﾑ･ﾕｰｻﾞｰ協会会長、株式会社大林組代表取締役会長
- 櫻田　謙悟　経済同友会代表幹事、ＳＯＭＰＯホールディングスグループＣＥＯ取締役　代表執行役社長
- 篠原　弘道　日本電信電話株式会社取締役会長
- 中西　宏明　株式会社日立製作所取締役会長
- 船橋　洋一　アジア・パシフィック・イニシアティブ理事長
- 村井　純(座長)慶應義塾大学教授
- 渡辺　佳英　日本商工会議所特別顧問、大崎電気工業株式会社取締役会長

オブザーバー

NISC、警察庁、金融庁、総務省、外務省、文部科学省、厚生労働省、農林水産省、国土交通省、防衛省

WG１（制度･技術･標準化）

第１回　平成30年2月7日
第２回　平成30年3月29日
第３回　平成30年8月3日
第４回　平成30年12月25日
第５回　平成31年4月4日
第６回　令和２年3月（書面開催）

１．サプライチェーン強化パッケージ

WG２（経営･人材･国際）

第１回　平成30年3月16日
第２回　平成30年5月22日
第３回　平成30年11月9日
第４回　平成31年3月29日
第５回　令和　2年1月15日
第６回　令和　2年8月25日

２．経営強化パッケージ
３．人材育成・活躍促進パッケージ

WG３（サイバーセキュリティビジネス化）

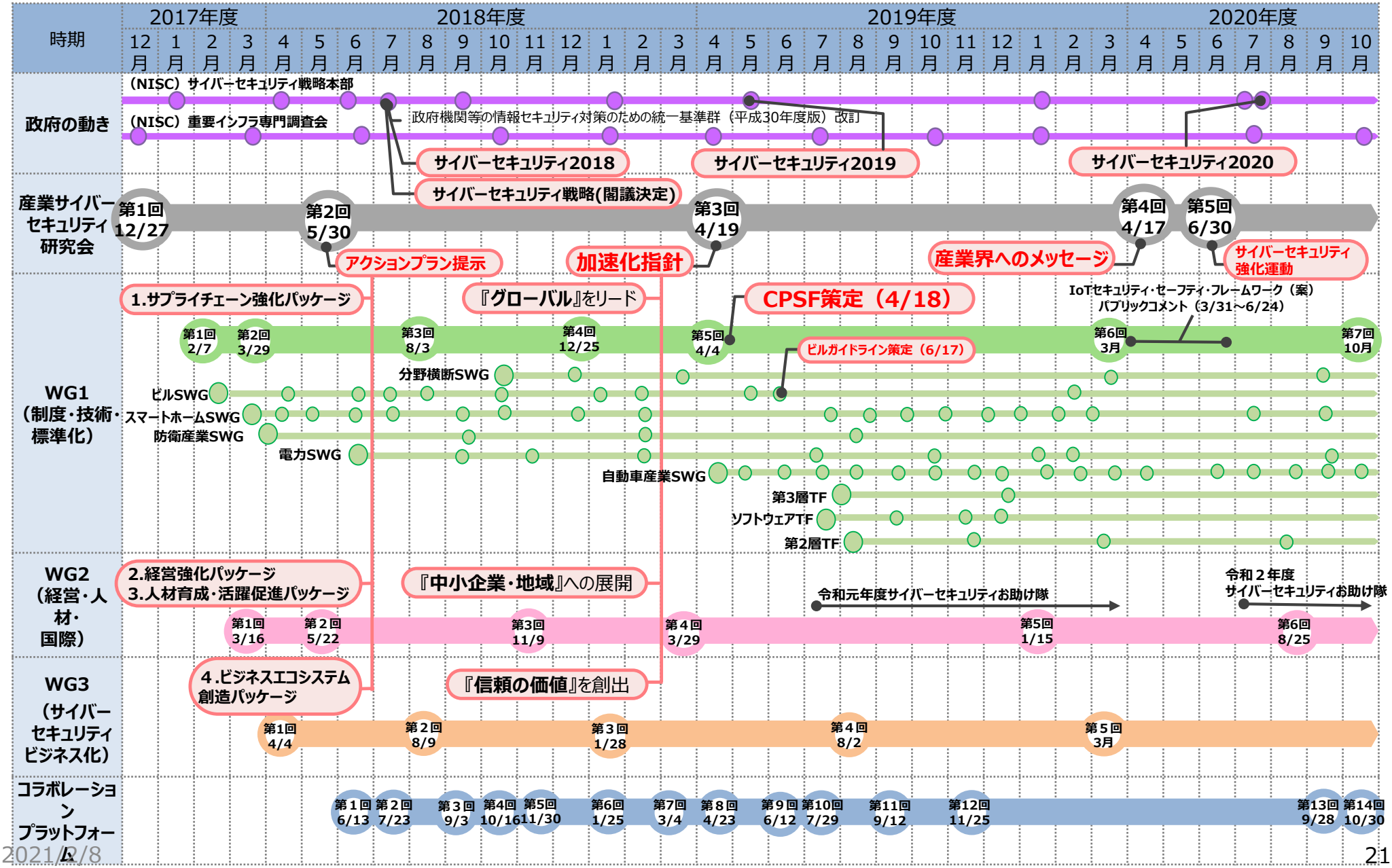
第１回　平成30年4月4日
第２回　平成30年8月9日
第３回　平成31年1月28日
第４回　令和元年8月2日
第５回　令和2年3月(書面開催)

４．ビジネスエコシステム創造パッケージ

産業サイバーセキュリティの加速化指針

１．『グローバル』をリードする
２．『信頼の価値』を創出する~Proven in Japan~
３．『中小企業・地域』まで展開する

産業サイバーセキュリティ研究会関連会議の活動状況



１．はじめに
～情報セキュリティ10大脅威などから

２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．サイバーセキュリティ支援施策
～地域、経営、人材

４．はじめましょう、サイバーセキュリティ
～「SECURITY ACTION」と
「中小企業の情報セキュリティ対策ガイドライン」

５．参考情報
（IPAのツール・制度のご紹介）

中小企業における現場対応の徹底支援

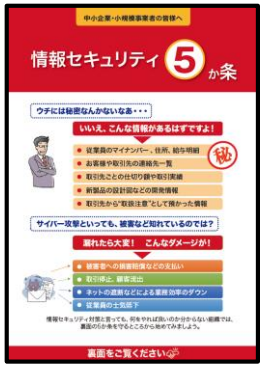
～事前の備えから、インシデントが発生してしまった後の対応・復旧支援まで

- セキュリティ対策を始めるに当たって何をやればいいのかわからない、そういった悩みをもつ中小企業に対し、まずは意識を持つ為、セキュリティ対策自己宣言「**SECURITY ACTION**」の取り組み。
- インシデントが発生してしまったが対処方法がわからない、この様な中小企業の事後対応を支援し、また簡易保険の実現を目指し、「**サイバーセキュリティお助け隊**」による支援体制等を実証

主に事前支援（防御等）

SECURITY ACTION

- セキュリティ対策に取り組むことを事業者が自己宣言する制度



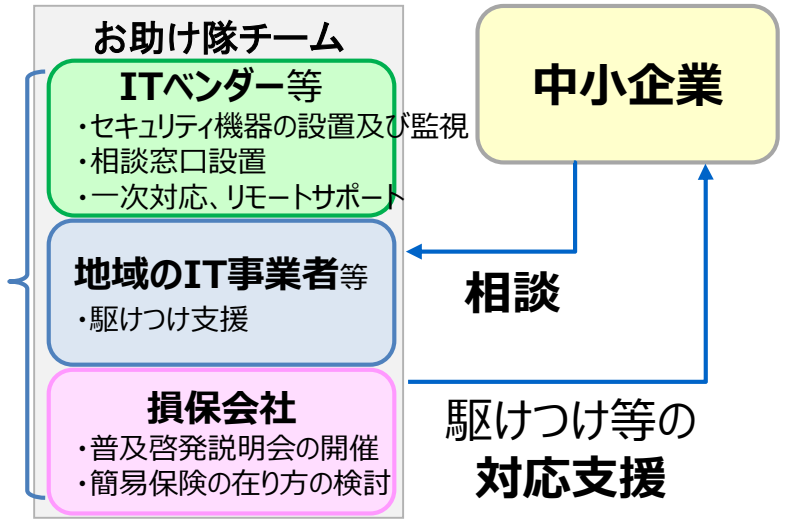
中小企業の情報セキュリティ対策ガイドライン

- (1)経営者が認識し実施すべき指針、(2)社内において対策を実践する際の手順や手法をまとめたガイドライン
- **情報セキュリティ規程の作成**に活用

主に事後支援（検知、対応、復旧等）

サイバーセキュリティお助け隊

- 中小企業がサイバー攻撃等で困った時の**相談窓口、駆けつけ支援体制**構築等を実証



中小企業の情報セキュリティ対策ガイドライン

- これからセキュリティ対策に取り組む企業向けの対策や、ある程度対策の進んでいる企業向けの対策の提示など、**企業のレベルに合わせてステップアップ**できるように構成。

ガイドライン本体

経営者向けの解説

サイバーセキュリティ経営ガイドラインの内容を中小企業向けに整理し、**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

実践者が具体的にセキュリティ対策を実施していくための方法を、**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

Step1 まず始める

最低限実施すべき
セキュリティ対策の5か条

Step2 現状を知り改善する

簡易的な
セキュリティ対策の25項目

Step3 本格的に取り組む

セキュリティポリシーを策定し、
組織的な対策の取り組み

Step4 改善を続ける

第三者認証(ISMS)の取得を
目指した取り組み

こちらより無料ダウンロード可能です
https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html

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。
- **11万社を超える中小企業が宣言**（2021年1月末時点）。

★ 一つ星

情報セキュリティ5か条に取り組む企業

① OS・ソフトウェアの最新化
（パッチ適用、バージョンアップ）
② ウイルス対策ソフトの導入
③ 強固なパスワード設定
④ データ等は必要最低限の人のみに共有
⑤ 攻撃の手口の把握

★★ 二つ星

情報セキュリティ自社診断により自社の状況を把握し、セキュリティポリシーを策定する企業

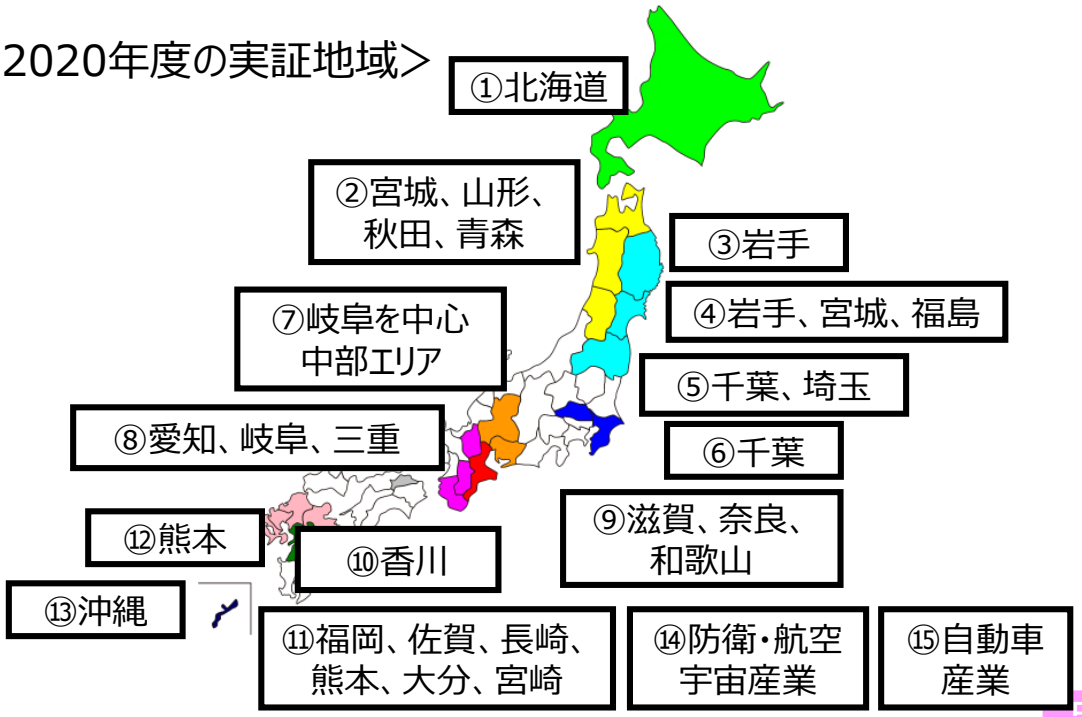
25の診断項目により
自社の対策状況を把握

セキュリティポリシー
策定のためのひな形も提供

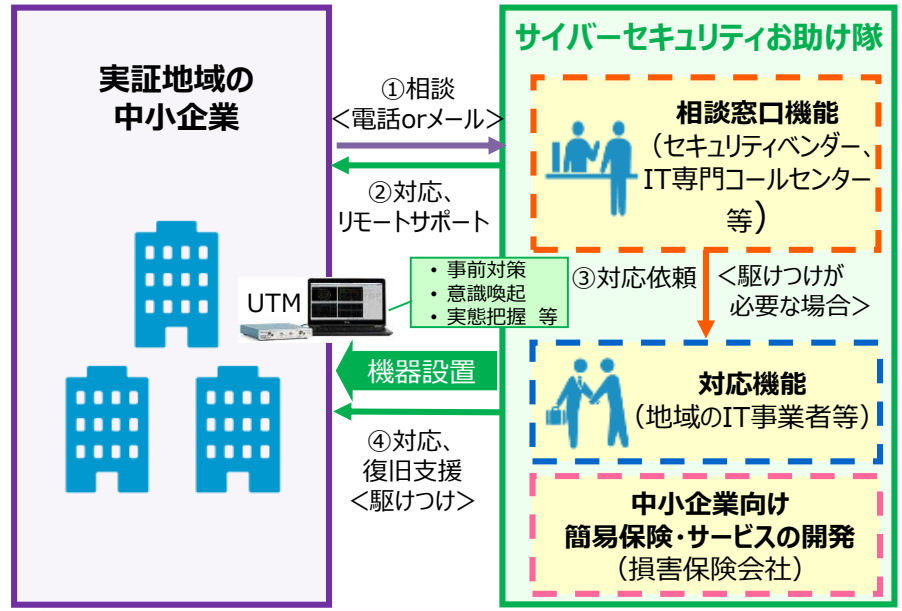
サイバーセキュリティお助け隊実証事業(2020年度)

- 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（全国で**15件**実施）。
- 本事業により、中小企業の事前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簡易保険サービスの実現を目指す**。

<2020年度の実証地域>



<実証のイメージ>



実証結果

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

（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）
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
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
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
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
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
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
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

	対象 （地域／産業分野）	実施体制 ●：実施主体
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
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
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
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
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
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

実証事業から民間サービスへの移行状況と普及促進のための支援策

- 2019年度実証事業後に、民間サービスが開発されたり、実証終了後も継続的なサービス展開が図られたりと、**お助け隊サービスの民間への移行**が進みつつある。
- **お助け隊サービスをブランド化**し、審査体制を構築すること等により、民間でのサービス展開を支援していく。

実証事業から民間サービスへの移行状況

- 実証事業後の2020年4月、**「サイバーセキュリティお助け隊サービス」を商用化。**

（大阪商工会議所）

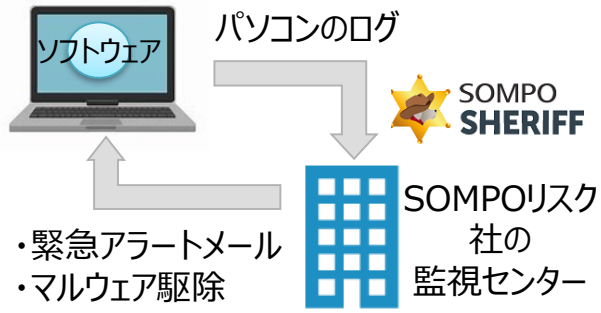
実証を通じて中小企業にとって必要な機能・サービスを精査することで、安価なサービスを実現。

（商工会議所会員月6,600円（年79,200円）
非会員月8,250円（年99,000円））

- 実証事業での経験やノウハウを元に、2019年12月に**新サービスを提供開始。**

（SOMPOリスクマネジメント）

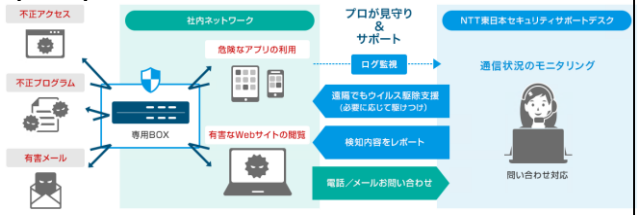
<サービスのイメージ>



- 参加中小企業**148社の内、約4割の61社が有償サービスへ移行。**※2020年2月17日時点

（NTT東日本）

(参考)同社の提供する「おまかせサイバーみまもり」



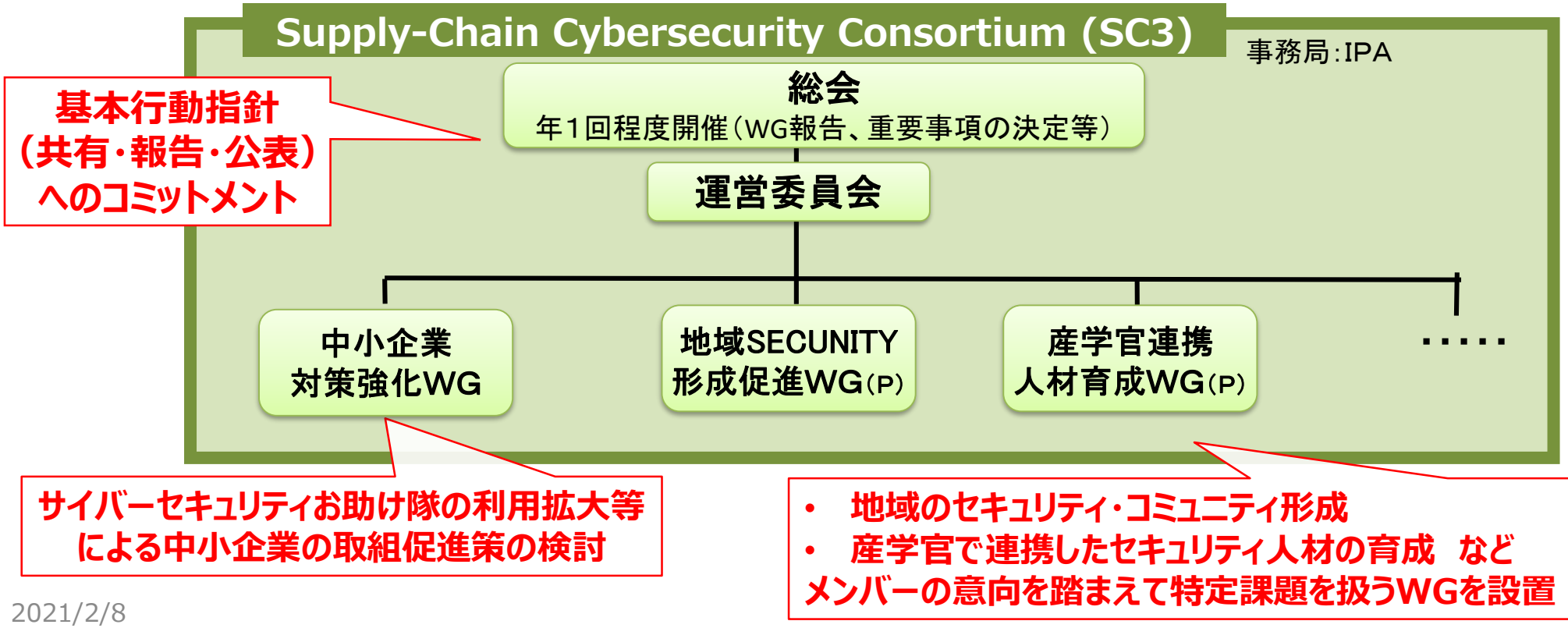
実証事業の取組（説明会や標的型メール攻撃の訓練、機器設置による脅威の可視化等）により、約4割の中小企業が民間サービスへの移行を希望。

お助け隊サービスのブランド化・審査体制構築へ

お助け隊サービス基準を策定し、**一定の基準を満たすサービスに「サイバーセキュリティお助け隊」の商標を付与するスキームを構築**することで、**民間でのサービス展開を支援**。

サイバーセキュリティ強化運動の全体像（コンソーシアムのイメージ）

- **趣旨：**大企業と中小企業がともにサイバーセキュリティ対策を推進するためのコンソーシアムを立ち上げ、「基本行動指針※」の実践と中小企業・地域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を産業界全体の活動として展開していく。
  ※サイバー攻撃事案発生時における、「共有、報告、公表」によるリスクマネジメントの徹底。
- **参加者:** 経済団体（経団連、日本商工会議所、経済同友会）、業種別業界団体　等
- **設立日:** 2020年11月1日（**設立総会：2020年11月19日**）
- **活動:** 特定の課題についてWGを設置し、具体的アクションを展開。



地域に根付いたセキュリティ・コミュニティ（地域SECUNITY）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SECUNITY」と命名。
- まずは各地域で地域SECUNITY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SECUNITY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

大学・高専
地元企業
県警
地元ベンダー
地域のセキュリティ関係者のつながり
自治体
民間団体
国

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

!!

地域のニーズとシーズのマッチング

- **地域の課題解決**
- **価値創出**

地域SECUNITYがない状態

地域SECUNITY形成

コラボレーション・プラットフォームを全国に展開

令和２年度の取組状況

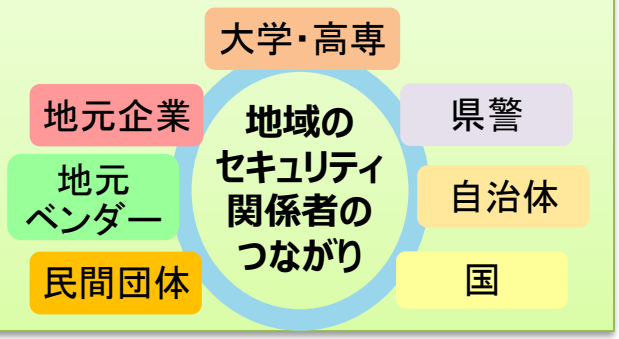
● 業界団体や専門家、各地方経産局等と連携し、各地域におけるセキュリティ関係者間での意見交換・情報共有等を実施。コミュニティ形成に向けた取組を全国で推進する。

＜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。

コミュニティ形成に必要な取組

- 全国各地で地域に根差したセキュリティコミュニティの形成を推進するために、以下の取組を実施中。

①セキュリティコミュニティを形成するための**モデル及びプラクティスの共有**

- 新たにコミュニティを形成する際にアプローチ先として想定される関係機関（自治体、商工団体、県警、大学 等）をリスト化。
- 他地域でのコミュニティの取組を参考にできるよう、各コミュニティのプラクティスを共通のフォーマットでとりまとめ、横展開。
- 課題なども共有することで、ソリューションを有するプレイヤーとの更なる連携を促進。

＜イメージ＞

②各地域に駆けつけ可能な専門家や、専門家派遣制度等の**情報・問合せ先リストの作成・共有**

- 連携できる可能性のある専門家やイベント（例．JNSA全国横断セミナー）、活用可能な制度（例．IPAセキュリティプレゼンター制度）等の情報・問合せ先リストを作成・共有。

＜イメージ＞

活用可能な制度

組織名	担当部署	連絡先
IPA セキュリティプレゼンター	××課	XX-XXXX
IPA 講師派遣制度	○○課	XX-XXXX

セキュリティ専門家

組織名	氏名	連絡先	専門等
JUAS	○○	XX-XXXX	経営層向け
JPCERT	△△	XX-XXXX	最新攻撃事例

国立高専機構と産・官との連携促進・具体化

- METI、IPA、JPCERT及び業界団体が国立高専機構と連携し、高専生の専攻（セキュリティ、IT、その他（機械、電気等））に応じた教育コンテンツの提供や講師の派遣等、産学官連携の具体化を推進中。

（赤字＝前回WGからのアップデート）

使用できるインフラ
- 演習設備
- 同時中継
  (全国高専間で配信可)
- 仮想空間

国立高専卒業生 約1万人/年の内訳	コンテンツ開発・授業の提供（パワーポイント、ビデオ等）	セキュリティ合宿に関する協力
セキュリティスキルレベル	**パターン①：90分程度** ・高専教員がコンテンツを使って講義 又は 企業等の方が講義 (拠点校から全国各校に同時配信も可) **パターン②：15分程度** 授業冒頭や隙間時間でビデオ放映	**高度セキュリティ合宿**（1泊2日） 年2回程度開催（インシデント対応演習等）参加者：35名程度 **KOSENセキュリティコンテスト**（１泊2日） 年1回程度開催（CTF）参加者：130名程度 ※開催期間中の一部の時間を利用して、一線で活躍するホワイトハッカーから講義を実施可能。
約１％ トップガンの学生 → 主に**セキュリティ企業**に就職	※トップガンの学生は、全国各校、各学科に散らばっているため、通常の授業時間で集合する機会がない。  ゲーム形式教材のイメージ	・**高専機構がJNSAに講師派遣を依頼できる体制を構築。** ・**METIがセキュリティ専門官を高度セキュリティ合宿に講師として派遣。**  開催の様子@石川高専
約20% 情報系学科の学生 → 主に**IT企業**に就職	・**JNSAのゲーム形式教材を石川高専と連携してアプリ化。** ※JNSA：NPO日本ネットワークセキュリティ協会 ・**JNSAがオンライン授業環境を利用した現場第一線講師による最新事例授業の開催検討中** ※一度に数十校を対象に同時開催可能。JNSAで実施中の岡山理科大学遠隔授業内容を最新事例中心に発展・展開。 ・**高専機構が四国地域企業のIPA ICSCoE修了生に講師派遣を依頼できる体制を構築。** ・**日立製作所が一関高専生向けに出前授業、インターンシップを実施し、出前授業は全国各校に配信。**	・**JNSAとSECCONビギナーズを石川高専と苫小牧高専で開催。** ・**JNSAがCTFビギナーズfor高専生@木更津高専に講師を派遣。** ・**IPAが高度セキュリティ合宿に講師を派遣し、App Goat（脆弱性体験学習ツール）の講習会を開催。** ・**METIがセキュリティ専門官を高知高専に派遣し、出前授業を実施。**
約80% 非情報系学科の学生 → 主に**ユーザー企業**に就職	・**CRICが高専機構と連携し、業界別（例．機械、電気、建築等）ビデオ教材（20分程度）を作成。** ※CRIC：一般社団法人サイバーリスク情報センター	※セキュリティ合宿のような機会は特段なし。  AppGoat講習の様子
KOSEN 国立高等専門学校機構 国立高専教員	・**JNSAが教員向けのセキュリティ基礎講座の実施を検討中。** ※神奈川県での高校教員向けセキュリティ基礎講座の実績を展開。	・**IPAが教員向けにAppGoat講習会を開催。** ・**JPCERT/CCが情報担当教員向け研修に講師を派遣。** ・**教員がIPAのセキュリティキャンプ全国大会を見学。** ・**高専機構が、教師向け合宿の機会に、METIにセキュリティ専門官の講師派遣を依頼できる体制を構築。**

１．はじめに
～情報セキュリティ10大脅威などから

２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．サイバーセキュリティ支援施策
～地域、経営、人材

４．はじめましょう、サイバーセキュリティ
～「SECURITY ACTION」と
「中小企業の情報セキュリティ対策ガイドライン」

５．参考情報
（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

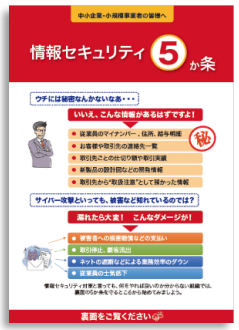
- **どこからどう始めたら良いか？**
  - まずは、基本的なセキュリティ対策から実施
  - 組織の実態に合わせ段階的に強化
- **どこまで実施すれば良いか？**
  - 組織における改善点を把握し、対策の周知・実践
  - リスクを受容できるレベルまで実施

SECURITY ACTION の取組みから始める

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。
- **１１万者を超える中小企業が宣言**（2020年12月末時点）。

★一つ星



１段階目（一つ星）

- **情報セキュリティ５か条に取り組む**

【情報セキュリテイ５か条】

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

SECURITY ACTION 制度のメリット

- リモートワーク環境の整備やサイバーセキュリティ対策などを支援するIT導入の**補助金申請の要件**
  - IT導入補助金
  - 東京都サイバーセキュリティ対策促進助成金
  - 堺市テレワーク導入支援補助金
  - 秋田県リモートワーク環境整備支援事業費補助金
- 普及賛同企業による**サイバー保険の保険料割引**が適用
- 情報セキュリティ対策への取組の見える化

★★二つ星

2段階目（二つ星）

- **情報セキュリティ自社診断を実施**
- **基本方針を策定**

3大都市圏	63,990
36道県	48,389
Total	112,379

(2020年12月末時点)

SECUITY ACTION 公式サイト

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

- SECURITY ACTIONの制度紹介や申込(宣言)、セキュリティ対策推進に役立つ情報･ツールを提供

ロゴマークの使用申込(宣言)

SECURITY ACTION　公式　検索

SECURITY ACTION 申込手順

STEP 1 使用規約を確認

SECURITY ACTION自己宣言者サイトで使用規約をご確認ください。

STEP 2 申込みフォームに入力

必要事項を入力してください。

STEP 3 申込み手続きを完了させる

申込み受付メールに記載されたURLをクリックして、申込み手続きを完了してください。

STEP 4 ダウンロード

申込み手続きを完了後、1～2週間程度でロゴマークをダウンロードできます。

SECURITY ACTION自己宣言者サイト

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

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/

企業＝経営者は何をやらなければならないのか

認識すべき「３原則」

経営者は、以下の３原則を認識し、対策を進める

原則１　情報セキュリティ対策は経営者のリーダーシップで進める

・経営者は情報セキュリティ対策の重要性を認識する　・自らリーダーシップを発揮して対策の実施を主導する

⇒ **要するに、社長自ら、「我が社は情報セキュリティ対策を実施します！」と社内外に表明すること。**

原則２　委託先の情報セキュリティ対策まで考慮する

・必要に応じて委託先が実施している情報セキュリティ対策も確認し、不十分な場合は対処する

⇒ **要するに、情報セキュリティ対策について、自社だけでなく、仕事をお願いしている相手先もよく確認しましょう！ということ。**

原則３　関係者とは常に情報セキュリティに関するコミュニケーションをとる

・情報セキュリティに関する取組方針を常日頃より関係者に伝えておく
⇒ サイバー攻撃によるウイルス感染や情報漏えいなどが発生した際、説明責任を果たすことができ、信頼関係を維持することが可能

⇒ **要するに、なにか事件が起きた時、慌てずしっかり「社長としての説明責任」が果たせるように、日頃から状況把握しておきましょう！ということ。**

企業＝経営者は何をやらなければならないのか

実行すべき「重要7項目の取組」

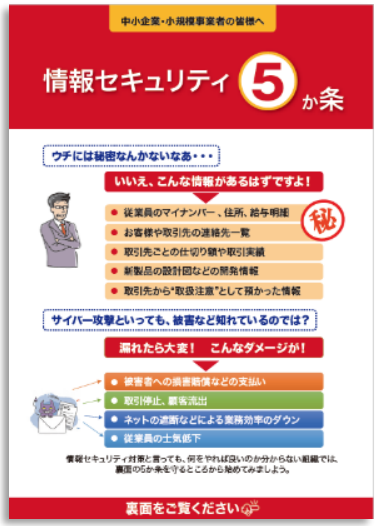
経営者は以下の７項目を自ら実践する、あるいは、情報セキュリティ対策の責任者・担当者に　指示し、**確実に実行**する

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

中小企業の情報セキュリティ対策ガイドライン

・できるところから始めて段階的にステップアップ

Step1
できるところから始める



情報セキュリティ 5 か条

Step2
組織的な取り組みを開始

5分でできる！
情報セキュリティ自社診断

Step3
本格的に取り組む

情報セキュリティ関連規程

Step4
より強固にするための方策

- 情報収集と共有
- ウェブサイトの情報セキュリティ
- クラウドサービスの情報セキュリティ
- 情報セキュリティサービスの活用
- 技術的対作例と活用
- 詳細リスク分析の実施方法

より強固にするため方策

SECURITY ACTION
★一つ星を宣言
セキュリティ対策自己宣言

SECURITY ACTION
★★二つ星を宣言
セキュリティ対策自己宣言

自社の取り組み目標に応じた
SECURITY ACTION を宣言！

情報セキュリティ対策の更なる強化に活用

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

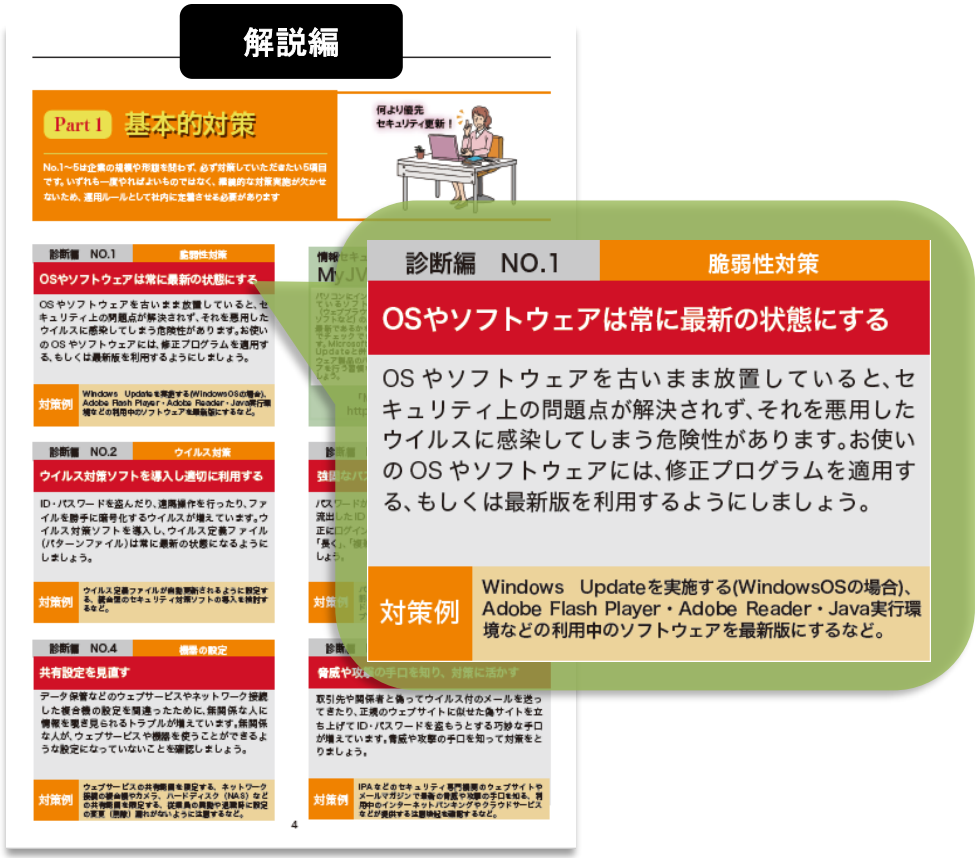
守秘義務、インターネット利用、ルール化など

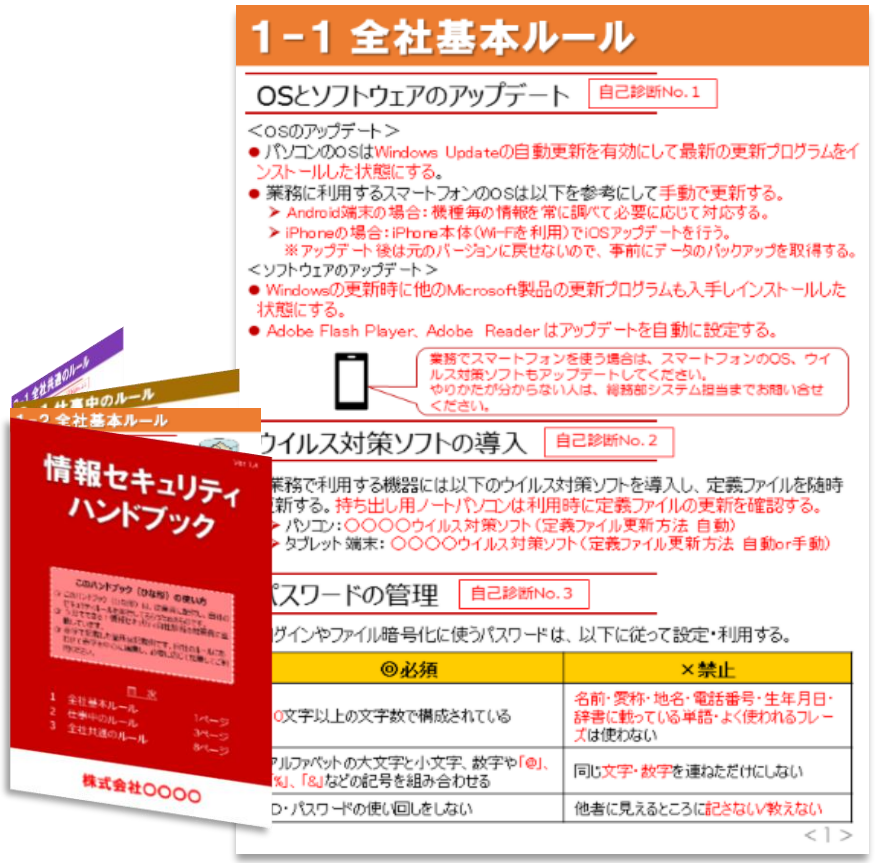
No		診断内容
基本的対策	1	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？
	4	重要情報※2 に対する適切なアクセス制限を行っていますか？
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？
従業員としての対策	6	電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？
	7	電子メールや FAX 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？
組織としての対策	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？

組織的に取り組む

対策の決定と周知

- 自社診断で問題があった項目は、「解説編」を参考に対策を決定
- 付録「情報セキュリティハンドブック（ひな形）」を編集して社内周知





管理体制構築・情報セキュリティ予算化

- 情報セキュリティ対策推進の管理体制を決定

【表５】情報セキュリティ管理のための役割と責任分担（例）

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者です。情報セキュリティ対策などの決定権限を有するとともに、全責任を負います。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者です。各部門における情報セキュリティ対策の実施などの責任と権限を有します。
システム管理者	情報セキュリティ対策のためのシステム管理を行います。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施します。
点検責任者	情報セキュリティ対策が適切に実施されているか点検します。

【表６】緊急時対応体制の役割と責任（例）

役職名	役割と責任
情報セキュリティ責任者	事故の影響を判断し、対応について意思決定する。
情報セキュリティ部門責任者	対応責任者の判断・意思決定に基づき適切な処置を行う。事故の原因を調べて情報セキュリティ責任者に報告する。
事故・異常を発見した従業員	事故や異常の内容を情報セキュリティ部門責任者に報告する。

- 利用、検討している情報システムを把握
- 情報セキュリティ対策の予算も確保

情報セキュリティ規程の作成①

・対応すべきリスクの特定

経営者が避けたい重大事故から、対応すべきリスクを特定

外部状況：法律や規制、情報セキュリティ事故の傾向、取引先からの情報セキュリティに関する要求事項など

内部状況：経営・情報セキュリティ方針、管理体制、情報システムの利用状況など

・対策の決定

リスクが大きなものを優先して対策を実施

いつ事故が起きてもおかしくない
事故が起きると大きな被害になる

リスクが**小さなものは許容**する

事故が起きる可能性が小さい
発生しても被害が軽微である

情報セキュリティ規程の作成②

・規程の作成：付録「情報セキュリティ関連規程（サンプル）」を活用

	名称	概要
1	組織的対策	情報セキュリティ管理体制の構築や点検、情報共有などのルールを定めます。
2	人的対策	取締役及び従業員の責務や教育、人材育成などのルールを定めます。
3	情報資産管理	情報資産の管理や持ち出し方法、バックアップ、破棄などのルールを定めます。
4	アクセス制御及び認証	情報資産に対するアクセス制御方針や認証のルールを定めます。
5	物理的対策	セキュリティ領域の設定や領域内での注意事項などのルールを定めます。
6	IT 機器利用	IT 機器やソフトウェアの利用などのルールを定めます。
7	IT 基盤運用管理	サーバーやネットワーク等のIT インフラに関するルールを定めます。
8	システムの開発及び保守	独自に開発及び保守を行う情報システムに関するルールを定めます。
9	委託管理	業務委託にあたっての選定や契約、評価のルールを定めます。業務委託契約書の機密保持に関する条項例と委託先チェックリストのサンプルが付属します。
10	情報セキュリティインシデント対応ならびに事業継続管理	情報セキュリティに関する事故対応や事業継続管理などのルールを定めます。
11	個人番号及び特定個人情報の取り扱い	マイナンバーの取り扱いに関するルールを定めます。

より強固にするための方策

- **情報収集と共有**
  情報セキュリティに関する情報収集の方法と情報共有の枠組み
- **ウェブサイトの情報セキュリティ**
  ウェブサイトを安全に構築し、運用するためのポイント
- **クラウドサービスの情報セキュリティ**
  クラウドサービスを安全に利用するためのポイント
- **セキュリティサービス例と活用**
  情報セキュリティに関する外部サービス
- **技術的対策例と活用**
  ITを活用する際の技術的対策
- **詳細リスク分析の実施方法**
  付録「リスク分析シート」を活用した詳細リスク分析の実施方法

１．はじめに
～情報セキュリティ10大脅威などから

２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．サイバーセキュリティ支援施策
～地域、経営、人材

４．はじめましょう、サイバーセキュリティ
～「SECURITY ACTION」と
「中小企業の情報セキュリティ対策ガイドライン」

５．参考情報
（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/

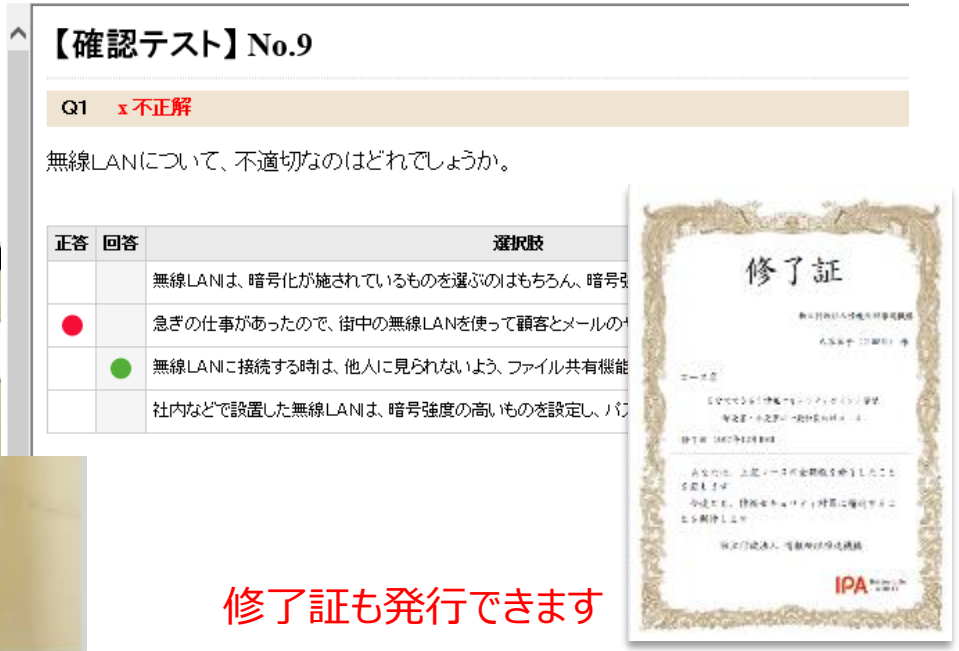
情報セキュリティ対策を「始めたい」「強化したい」「学びたい」中小企業の方々をサポートするポータルサイト

- 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　検索

情報セキュリティ対策支援サイト
5分でできる！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



修了証も発行できます

セキュリティプレゼンターの検索

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

映像で知る情報セキュリティ

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

- 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　映像　**検索**

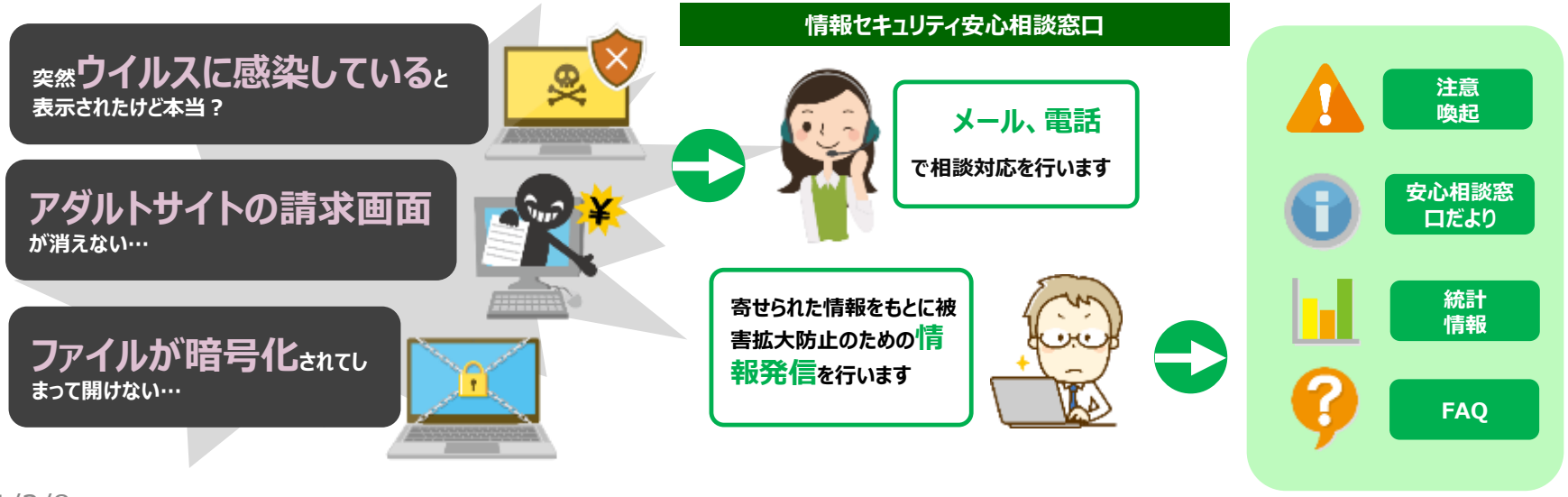
情報セキュリティ安心相談窓口

・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

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　IPA安心相談　検索



テレワークを行う際の
セキュリティ上の注意事項

テレワーク勤務者に向けたセキュリティ上の注意事項を公開
https://www.ipa.go.jp/security/announce/telework.html

- テレワークを行う際のセキュリティ上の注意事項
- テレワークから職場に戻る際のセキュリティ上の注意事項

情報セキュリティ

テレワークを行う際のセキュリティ上の注意事項

掲載日：2020年 4月 21日
更新日：2020年 9月 14日
独立行政法人情報処理推進機構
セキュリティセンター

1. はじめに

新型コロナウイルス感染症(COVID-19)の影響により、ICTを用いて自宅でも業務が行えるような環境を整えて、社員等を出社させずに事業継続を図る動きが急速に進んでいます。このような環境で働くテレワーク勤務者に向けたセキュリティ上の注意事項をご案内します。

テレワークには様々な利用環境があります。代表的なのは、自宅のパソコン等を用いてリモートデスクトップや仮想デスクトップで社内での業務用端末と同じ利用環境（テレワーク環境）を実現する方法です。

一方でそのような本格的な環境が提供されていない状況で自宅勤務を実施されている場合もあると思います。このページでは、そのような場合における注意事項も説明します。

2. テレワークを行う際のセキュリティ上の注意事項

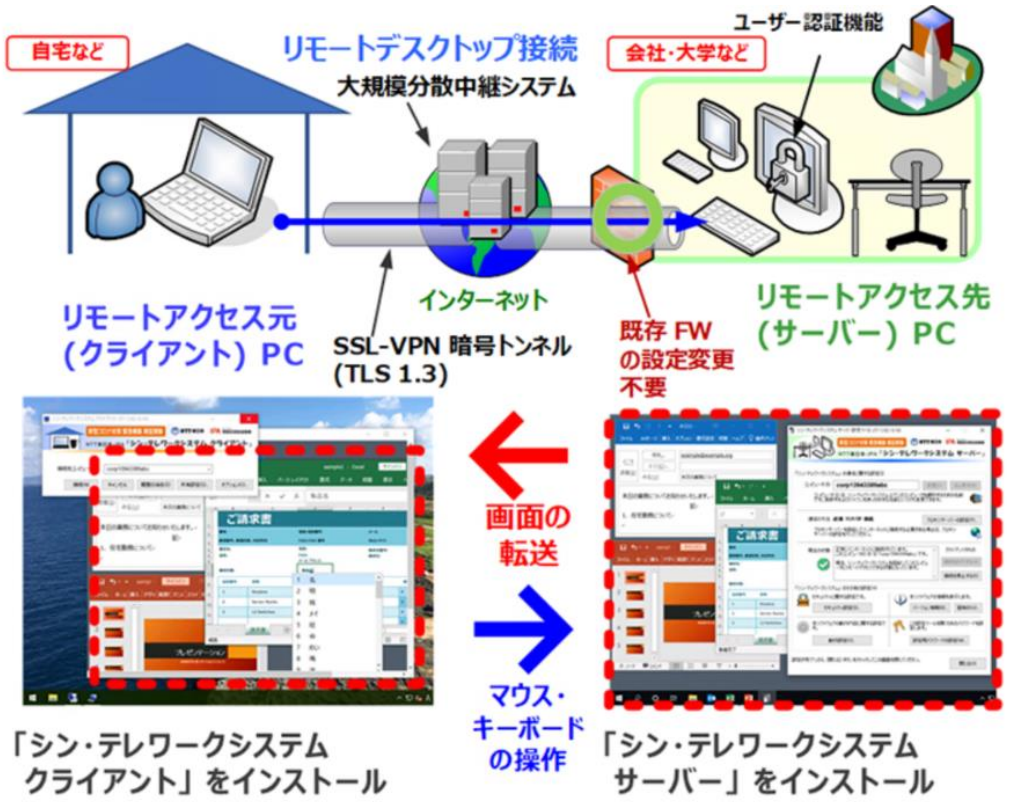
（1）所属する組織や企業からテレワーク環境が提供されている場合

- テレワーク勤務者の方は、お使いのテレワーク環境に関して所属先が定めた規程やルールをよく理解し、それに従ってください。
- 不明な点等がある場合は自分で判断せず、まずは所属先のシステム管理者等に相談をしてください。
- 規程やルールとあわせて、お使いのパソコン等に対して<日常における情報セキュリティ対策>を実施してください。

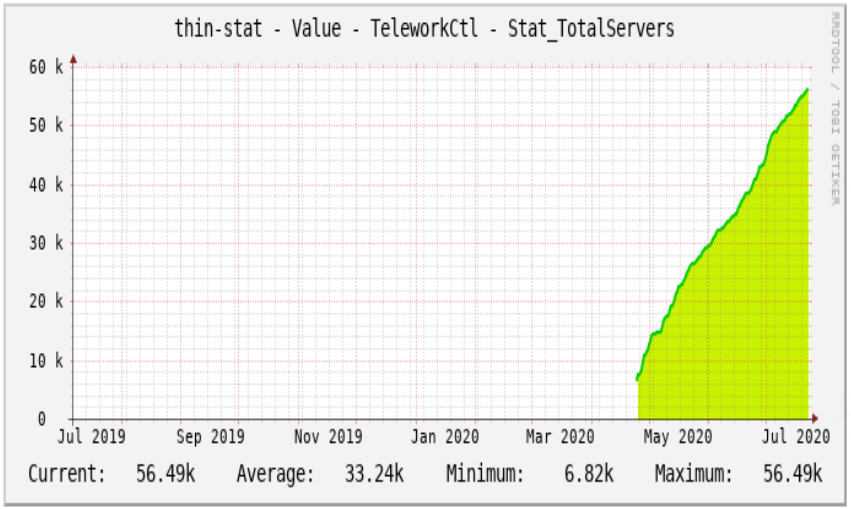
情報セキュリティ
- 脆弱性対策情報
- 届出・相談・情報提供
- 特集コンテンツ
- 情報セキュリティ啓発
- 情報セキュリティ対策
  - 情報セキュリティ対策のキホン
  - 日常における情報セキュリティ対策
  - 長期休暇における情報セキュリティ対策
  - テレワークを行う際のセキュリティ上の注意事項
  - Web会議サービスを使用する際のセキュリティ上の注意事項
  - ウイルス対策
  - 不正アクセス対策
  - 脆弱性対策
  - 標的型サイバー攻撃対策
  - IoT

（参考）シン・テレワークシステム

- 2020年4月21日、IPA産業サイバーセキュリティセンター サイバー技術研究室は、NTT東日本と連携し、緊急事態下においてテレワークを直ちに必要とされる方々のため、多くの方々が迅速かつ簡単に利用できるシンクライアント型SSL-VPNリモートデスクトップシステムを緊急構築し無償提供。
- 公開３か月で5.5万ユーザーが利用（2020/7/21時点）。現在は約12.8万ユーザーに増加。
- 現在もユーザーからの様々な要望を受けて機能強化を継続中。



NTT 東日本 - IPA「シン・テレワークシステム」
直近 1 年間のユーザー総数 (インストール・起動済の職場側 PC の台数) の推移



出典：https://www.ipa.go.jp/about/press/20200421.html
https://telework.cyber.ipa.go.jp/stat/

IT利用者に求められるIT知識を習得できる国家試験

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

試験時間	出題形式	出題数 解答数	基準点	
			総合評価	分野別評価
120分	四肢択一	100問 100問	600点 (1,000点満点)	300点 (1,000点満点)

試験実施概要

・試験実施日

CBT方式で随時実施中

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。

受験を特にお勧めする方

・業務で個人情報を取り扱う方
・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

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

CBT方式で上期、下期に実施

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

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）

- 講習受講
- 資格名称の使用
- 登録情報の公開

ご清聴ありがとうございました