中小企業における
サイバーセキュリティ対策と
普及に向けた取組みについて

2021/10/27

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　副部長
兼　中小企業支援グループ　グループリーダー
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**

目次

- サイバーセキュリティを巡る状況と対策の必要性

- 具体的な対策～どこからどう始めるか？
  - SECURITY ACTION、中小企業の情報セキュリティ対策ガイドライン
  - サイバーセキュリティお助け隊サービス

- 産業界・地域と連携した対策普及の取組み ～ サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）

- 参考情報

情報セキュリティ10大脅威

- 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IPAが脅威候補を選出
- セキュリティ専門家や企業のシステム担当等から構成される「10大脅威選考会」が投票
- TOP10入りした脅威を「10大脅威」として脅威の概要、被害事例、対策方法等を解説

情報セキュリティ10大脅威
https://www.ipa.go.jp/security/vuln/10threats2021.html

情報セキュリティ10大脅威 2021 脅威ランキング

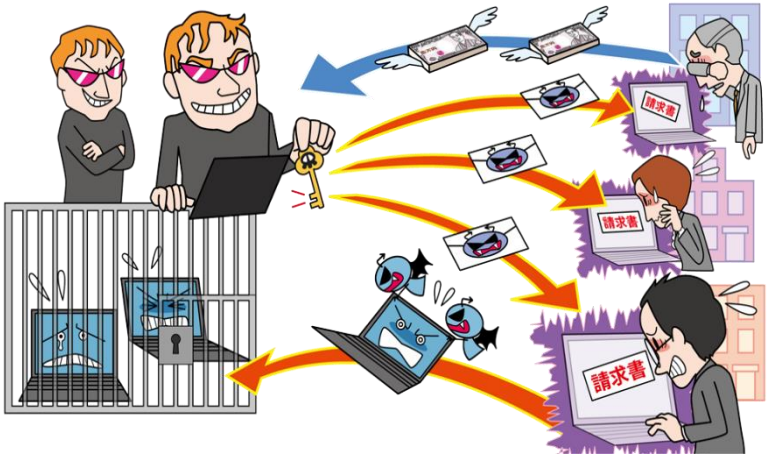
「個人」向け脅威	順位	「組織」向け脅威
スマホ決済の不正利用	1	ランサムウェアによる被害
フィッシングによる個人情報等の詐取	2	標的型攻撃による機密情報の窃取
ネット上の誹謗・中傷・デマ	3	テレワーク等の ニューノーマルな働き方を狙った攻撃
メールやSMS等を使った脅迫・詐欺の手口 による金銭要求	4	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	5	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	6	内部不正による情報漏えい
インターネット上のサービスからの 個人情報の窃取	7	予期せぬIT基盤の障害に伴う業務停止
偽警告によるインターネ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

3年間の情報セキュリティ10大脅威から見える動向

- 「**ランサムウェア**による被害」は手口の悪質化により**１位**に上昇
- コロナ禍を契機として**テレワーク等**の新しい働き方の拡大。それを狙った攻撃への懸念から３位にランクイン。
- 2019年から継続して**「サプライチェーンの弱点を悪用した攻撃」が4位**にランクイン。
- 標的型攻撃、ビジネスメール詐欺、内部不正が引き続き上位

順位	10大脅威2019	10大脅威2020	10大脅威2021
1	標的型攻撃による被害	標的型攻撃による機密情報の窃取	ランサムウェアによる被害
2	ビジネスメール詐欺による被害	内部不正による情報漏えい	標的型攻撃による機密情報の窃取
3	ランサムウェアによる被害	ビジネスメール詐欺による 金銭被害	テレワーク等のニューノーマルな働き方を狙った攻撃
4	**サプライチェーンの弱点を悪用した攻撃の高まり**	**サプライチェーンの弱点を悪用した攻撃の高まり**	**サプライチェーンの弱点を悪用した攻撃**
5	内部不正による情報漏えい	ランサムウェアによる被害	ビジネスメール詐欺による金銭被害
6	サービス妨害攻撃によるサービスの停止	予期せぬIT基盤の障害に伴う業務停止	内部不正による情報漏えい
7	インターネットサービスからの個人情報の窃取	不注意による情報漏えい	予期せぬIT基盤の障害に伴う業務停止
8	IoT機器の脆弱性の顕在化	インターネット上のサービスからの個人情報の窃取	インターネット上のサービスへの不正ログイン
9	脆弱性対策情報の公開に伴う悪用増加	IoT機器の不正利用	不注意による情報漏えい等の被害
10	不注意による情報漏えい	サービス妨害攻撃によるサービスの停止	脆弱性対策情報の公開に伴う悪用増加

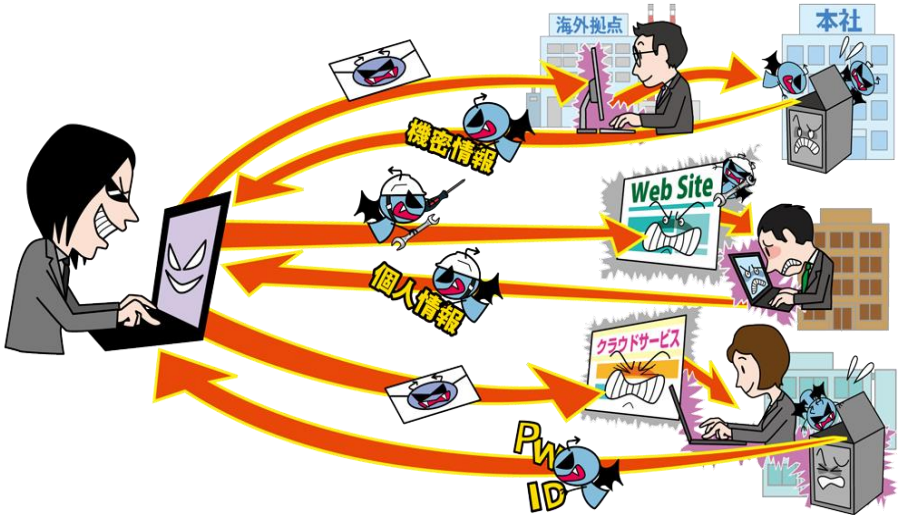
【1位】ランサムウェアによる被害
～組織を狙ったランサムウェアの攻撃が増加～



- PC等に保存されているファイルを暗号化され使用不可に
- 復旧と引き換えに金銭を要求される
- 情報を窃取しそれを公開すると脅迫するケースも
- 今年度上半期では、**被害企業の66%が中小企業**との報告も（警察庁「令和３年上半期におけるサイバー空間をめぐる脅威の情勢等について」より https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_kami_cyber_jousei.pdf）

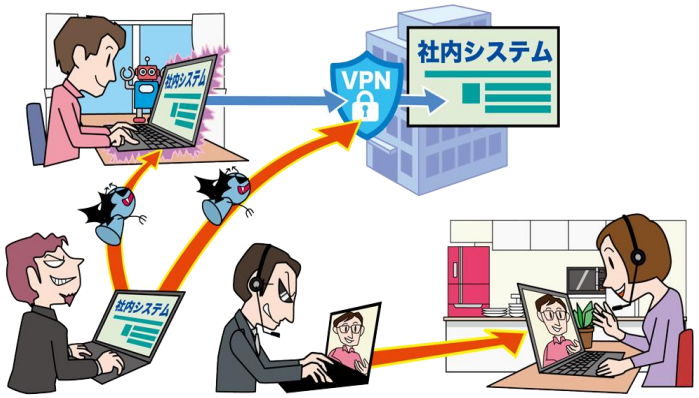
【2位】標的型攻撃による機密情報の窃取

～新型コロナウイルスの影響に便乗した標的型攻撃メールを観測～



- メール等を利用し特定組織のPCをウイルスに感染させる
- 組織内部に潜入し長期にわたり侵害範囲を徐々に広げる
- 組織の機密情報窃取やシステムの破壊を行う
- 攻撃手口
  - メールやウェブサイトからウイルスに感染させる
  - 不正アクセスして認証情報を窃取
  - 社内システムへ侵入しウイルスを感染させる

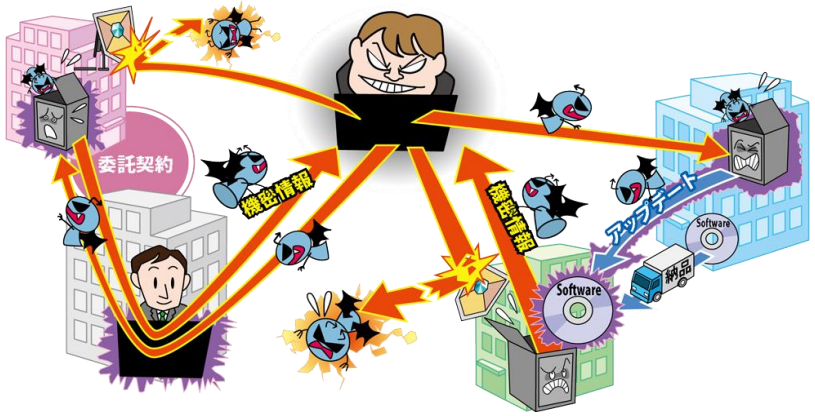
【3位】テレワーク等のニューノーマルな働き方を狙った攻撃
～テレワーク環境を意識した対策を～



- 2020年はコロナ禍の影響によりテレワークへの移行が増加
- ウェブ会議サービスやVPNの本格的な活用の始まりに伴い、それらを狙った攻撃が発生
- ウェブ会議ののぞき見やテレワーク用PCのウイルス感染のおそれ
- 攻撃手口/発生要因：テレワーク環境や管理体制の不備
  - テレワーク用ソフトの脆弱性を悪用した不正アクセス
  - 急なテレワーク移行による管理体制の不備
  - 私物PCや自宅ネットワークの利用　※私物PCからの情報漏えいのおそれ

【4位】サプライチェーンの弱点を悪用した攻撃

～自組織の対策だけでは不十分？広がるサプライチェーンを悪用した攻撃被害～



- 原材料や部品の調達、製造、在庫管理、物流、販売、業務委託先等の一連の商流（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
- 取引先や一部業務を委託している外部組織から情報漏えい
- 攻撃手口：サプライチェーンの中でセキュリティが脆弱な組織を狙う
  - 標的組織の取引先や委託先を攻撃し、それらが保有する標的組織の機密情報を狙う
  - ソフトウェア開発元等を攻撃し、標的を攻撃するための足掛かりとする
    - ソフトウェアのアップデートにウイルスを仕込み、アップデートを適用した利用者にウイルスを感染させる等

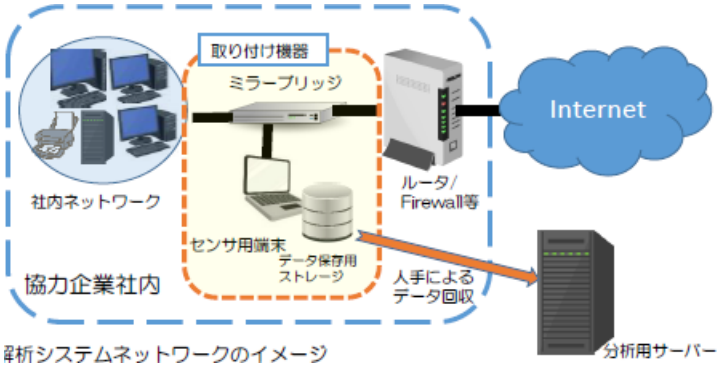
中小企業に対するサイバー攻撃の調査・分析結果（大阪商工会議所）

- 「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）」から、**地域の中小企業も、例外なくサイバー攻撃の脅威に晒されている**ことが明らかに。

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

- 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。

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）

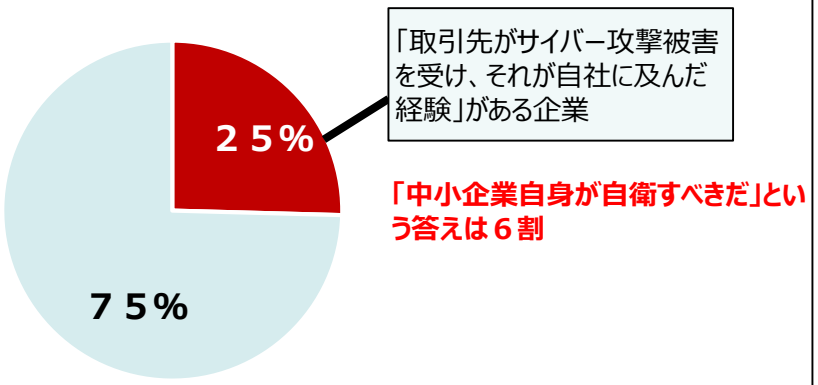
取引先経由の被害に関する調査

■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%**）



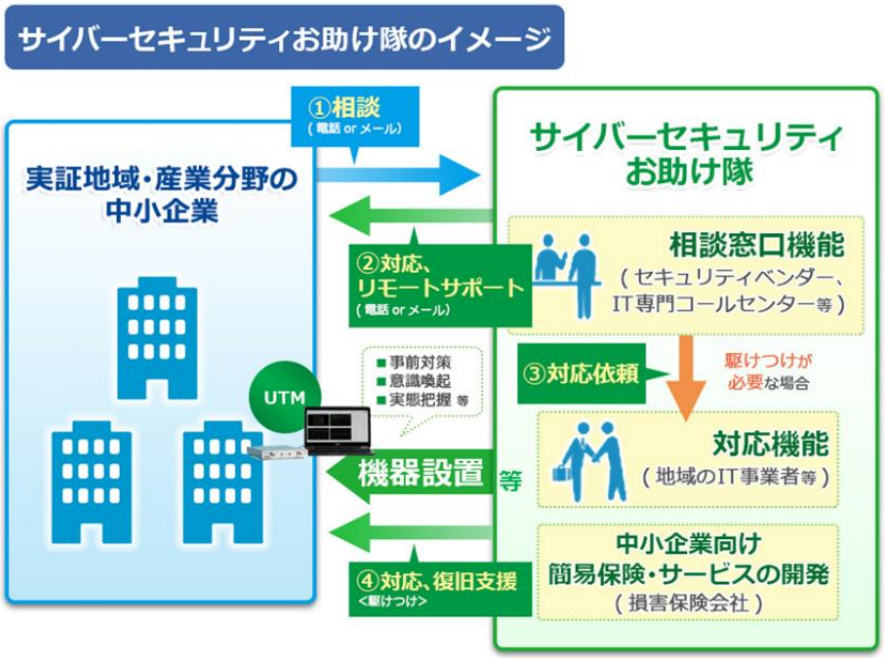
「中小企業自身が自衛すべきだ」という答えは６割

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）

サイバーセキュリティお助け隊実証事業で得られた結果

中小企業の被害実態等を把握することで、**中小企業向け事後サービスに必要な人材スキルやサービス内容等を明らか**にし、**中小企業の支援機能を低コストで構築**するために実証事業を実施（2019年度、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を構築。
- **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、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を把握。



- 2019年度には**全国8地域**で中小企業**1,064社**が参加。
- 2020年度には**15の地域・産業分野**で中小企業**1,117社**が参加。

サイバーセキュリティお助け隊

2019年度実証事業における対応事例

- 実証期間中に、重大なインシデントの懸念・可能性ありと判断し、**対処・支援を行った件数**は**128件**。対処を怠った場合の**被害想定額**が**約5000万円**となる事案も。
- 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。

経済産業省　昨今の産業を巡るサイバーセキュリティ
https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html

サイバーセキュリティお助け隊
2020年度実証事業における対応事例

- 新型コロナウイルス感染症拡大の影響もあり、**リモートにより管理可能なサービスの提供**が多く行われ、インシデント発生に際しても**概ねリモートによる支援対応**を実施。

＜2020年度実証事業における具体的な対応事例＞

事例１	UTMサービスを導入した企業において、同一ホストにて断続的に**要注意検知が発生していることが確認**されたため、お助け隊事業者が駆けつけ支援を実施。対象の**マルウェアと判定されたプログラム**は、インターネットからダウンロードしたフリーソフトであったことが判明、**駆除を実施**。
事例２	UTMサービスを導入した企業において、PCの「ウィルス対策ソフト」を導入済みであったものの、**「不正なIPアドレスへの通信」が成立していることが確認**されたため、緊急度「高」のアラートを発報、支援を実施。 接続元端末をLANから分離した上、**ウイルス対策ソフトでのフルスキャンを実施した結果、何も検知されなかった**ものの、もし被害に至っていた場合の**被害試算額**は**54,760,000円**にも。
事例３	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**、リモート支援により駆除を実施。該当端末(PC)をLANから分離した上でフルスキャンを実施した結果、**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駆除を実施。**

情報セキュリティ対策はなぜ必要？

- IT活用がビジネスに利益をもたらす一方で、サイバー攻撃や従業員の不注意などによる損害が多発
- 大企業だけではなく、中小企業もサイバー攻撃のターゲットになっている
- 取引先攻撃への踏み台にされる懸念
- 近年増加しているサイバー攻撃は金銭窃取などを目的としていることが多く日々巧妙化、複雑化、悪質化
- 組織の損害を未然に防ぐために、今や情報セキュリティ対策は必須

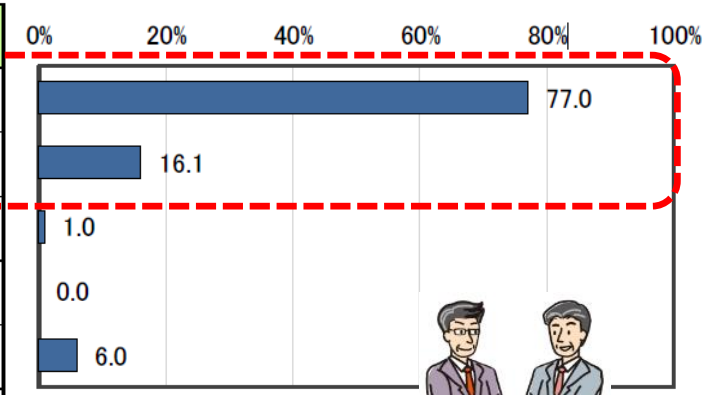
顧客や取引先はどう考えているか？

- デジタル化が進む今の社会、顧客や取引先の情報セキュリティに対する要求、期待は確実に高まっている

IPA「ITサプライチェーン における情報セキュリティの責任範囲に関する調査」から
＜以下の情報セキュリティ要求事項に関し、業務委託契約において、**委託先の責任を明確にしたいと思う度合**について、当てはまるものをお選びください。(それぞれひとつずつ)＞

a.秘密保持

選択肢	%	N
1　強くそう思う	77.0	321
2　ややそう思う	16.1	67
3　あまりそう思わない	1.0	4
4　全くそう思わない	0.0	0
5　分からない・無回答	6.0	25
計	100	417



責任や義務はあるのか？

- 個人情報保護法では委託先の監督が求められている
- 顧客や取引先から見て自社が委託先に該当する場合は、「監督」される立場にある

「個人情報保護法」
(委託先の監督)
第22条 個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、**委託を受けた者に対する必要かつ適切な監督を行わなければならない。**

「個人情報の保護に関する法律についてのガイドライン(通則編)」
次の(1)から(3)までに掲げる必要かつ適切な措置を講じなければならない
(1)適切な委託先の選定
(2)委託契約の締結
(3)委託先における個人データ取扱状況の把握

目次

- サイバーセキュリティを巡る状況と対策の必要性
- 具体的な対策～どこからどう始めるか？
  - SECURITY ACTION、中小企業の情報セキュリティ対策ガイドライン
  - サイバーセキュリティお助け隊サービス
- 産業界・地域と連携した対策普及の取組み ～ サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）
- 参考情報

どこからどう始めてどこまですれば？

- 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

サイバーセキュリティお助け隊サービスの活用

目次

- サイバーセキュリティを巡る状況と対策の必要性
- 具体的な対策～どこからどう始めるか？
  - SECURITY ACTION、中小企業の情報セキュリティ対策ガイドライン
  - サイバーセキュリティお助け隊サービス
- 産業界・地域と連携した対策普及の取組み ～ サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）
- 参考情報

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）

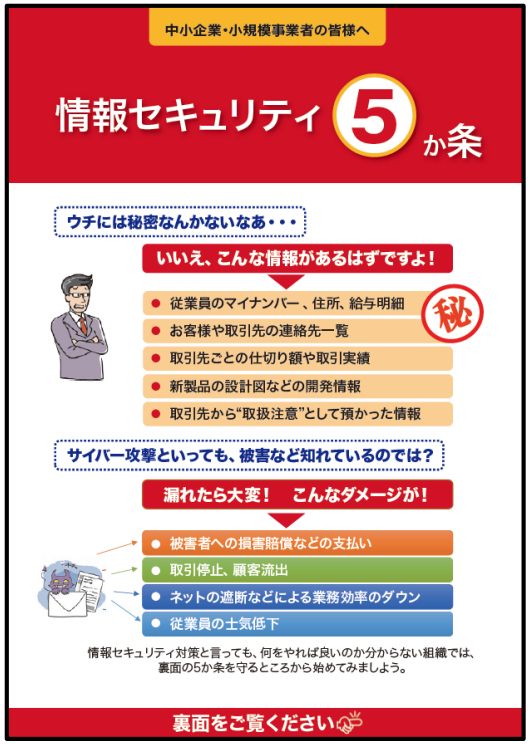
「5分でできる！情報セキュリティ自社診断」で自社の状況を把握したうえで、「情報セキュリティ基本方針」を定め、外部に公開したことを宣言

SECURITY ACTION 一つ星

セキュリティ対策自己宣言

「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！



SECURITY ACTION 二つ星

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

＋

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
- 継続的改善　　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

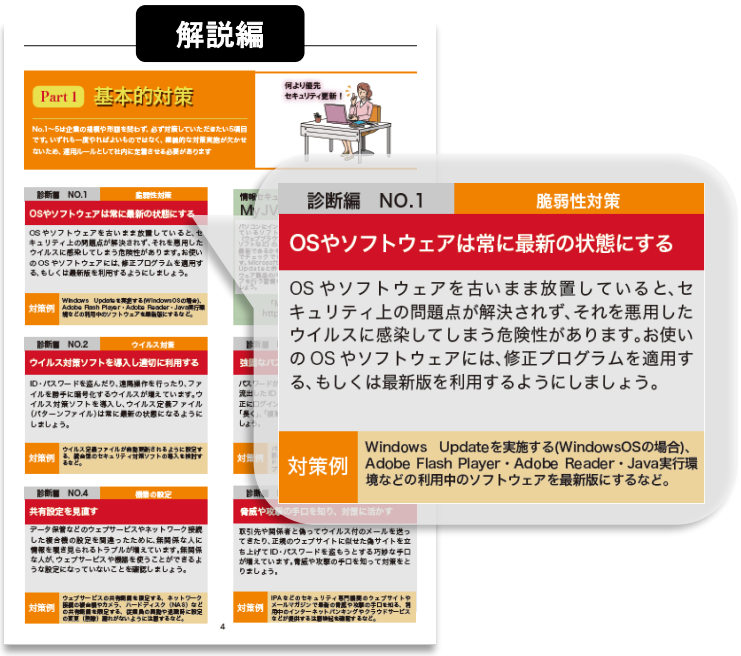
組織としての対策 7項目

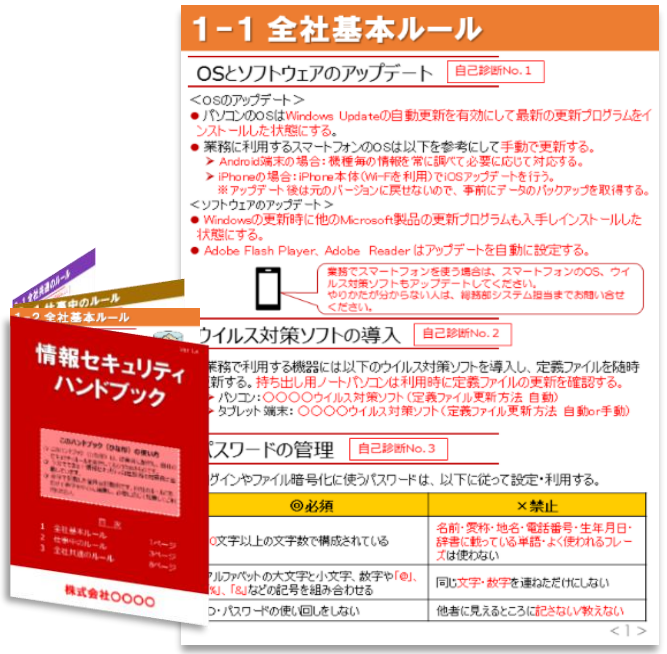
守秘義務、インターネット利用、
ルール化など

	No	診断内容	チェック			
			実施している	一部実施している	実施していない	わからない
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？	4	2	0	-1
	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？	4	2	0	-1
	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	2	0	-1
	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？	4	2	0	-1
	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 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				
	14	離席時にパソコン画面の覗き見や				
	15	関係者以外の事務所への立ち入り				
	16	退社時にノートパソコンや備品を				
	17	事務所が無人になる時の施錠忘れ				
	18	重要情報が記載された書類や重要 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 守らせていますか？				
	20	従業員にセキュリティに関する教				
	21	個人所有の情報機器を業務で利用				
	22	重要情報の授受を伴う取引先との				
	23	クラウドサービスやウェブサイト 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 等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？				

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





情報処理推進機構

SECURITY ACTION 申込手順

IPA

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/

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

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

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

実行すべき「重要7項目の取組」

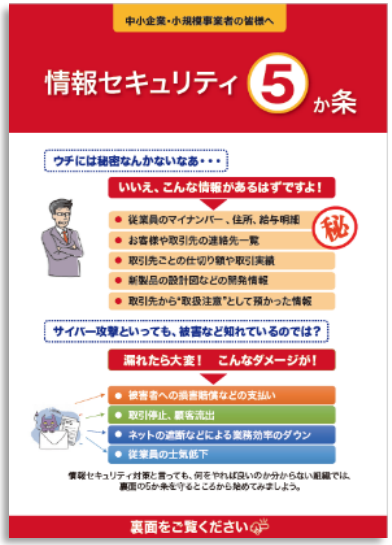
- 経営者は以下の**７項目**を**自ら実践**する、あるいは
- 情報セキュリティ対策の責任者・担当者に指示し、確実に実行する

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

具体的な対策実践に向けた構成

- **できるところ**から始めて段階的に**ステップアップ**

Step1	Step2	Step3	Step4
できるところから始める	組織的な取り組みを開始	本格的に取り組む	より強固にするための方策



情報セキュリティ５か条

５分でできる！
情報セキュリティ自社診断

情報セキュリティ関連規程

- 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

SECURITY ACTION ★★二つ星を宣言

目次

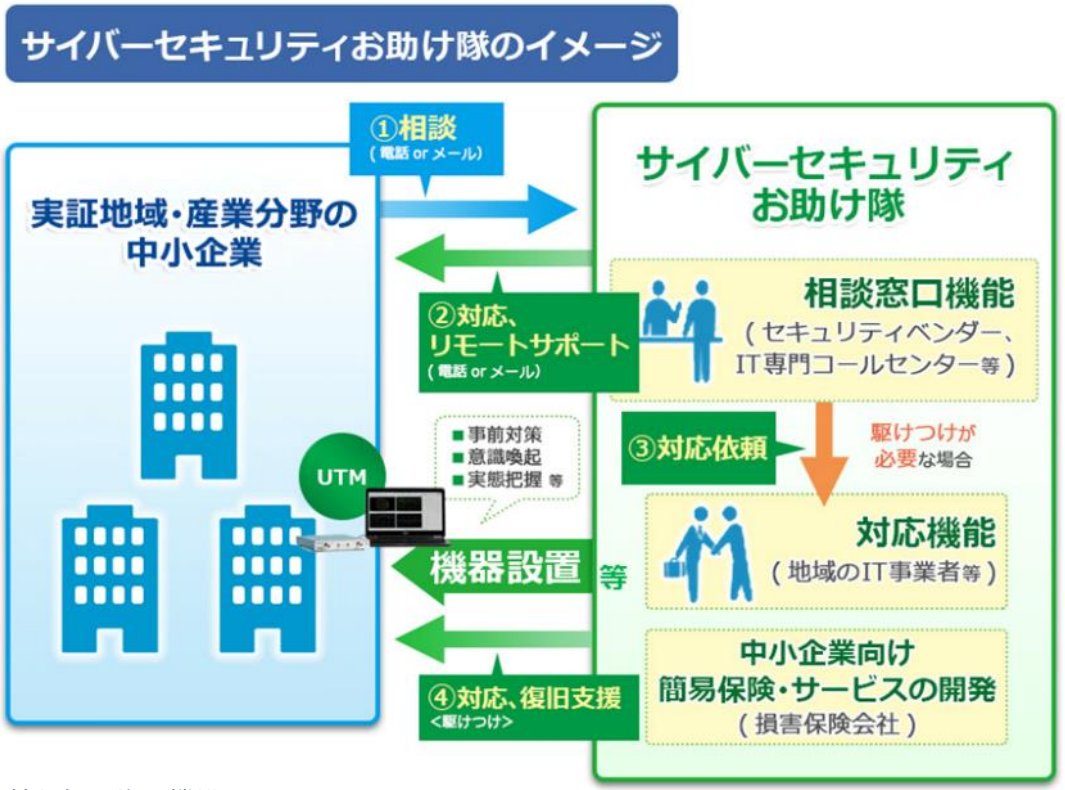
- サイバーセキュリティを巡る状況と対策の必要性
- 具体的な対策～どこからどう始めるか？
  - SECURITY ACTION、中小企業の情報セキュリティ対策ガイドライン
  - サイバーセキュリティお助け隊サービス
- 産業界・地域と連携した対策普及の取組み ～ サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）
- 参考情報

サイバーセキュリティお助け隊実証事業（再掲）

中小企業の被害実態等を把握することで、**中小企業向け事後サービスに必要な人材スキルやサービス内容等を明らか**にし、**中小企業の支援機能を低コストで構築**するために実証事業を実施（2019年度、2020年度）

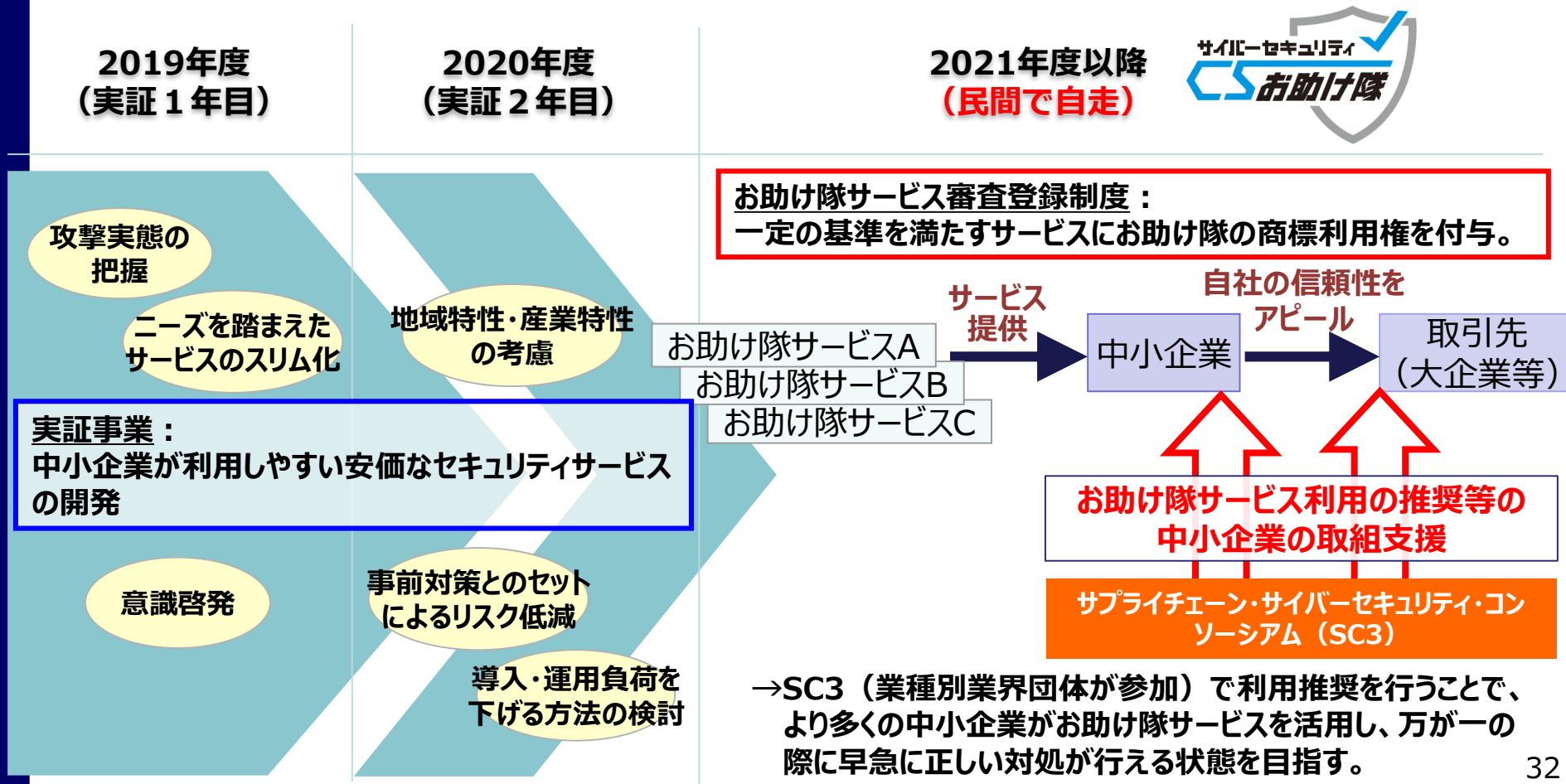
- 地域の団体、セキュリティ企業、保険会社がコンソーシアムを組み、中小企業向けのセキュリティ対策支援の仕組みを構築。
- **民間による中小企業向けのセキュリティ簡易保険サービスの実現**を目指し、中小企業の事前対策の促進や意識喚起、攻撃実態や対策ニーズを把握。

- 2019年度には**全国8地域**で中小企業**1,064社**が参加。
- 2020年度には**15の地域・産業分野**で中小企業**1,117社**が参加。



実証事業から民間サービスへの移行・普及に向けたステップ

2年間の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**をサプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）中小企業対策強化WGにて議論・整理、パブコメを経て２月末にIPAより公開。



→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制度　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　提供する中小企業向けセキュリティサービスを**「お助け隊サービス」**として登録・公表。
- 第1回審査(3月)において新たに出た論点を踏まえ、中小企業対策強化WGにおいて、サービス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。**7月に改定版を公表**。
- 今後も中小企業対策強化WGにおいて継続的に制度の在り方を検討するとともに、**SC3を通じて普及を促進**。

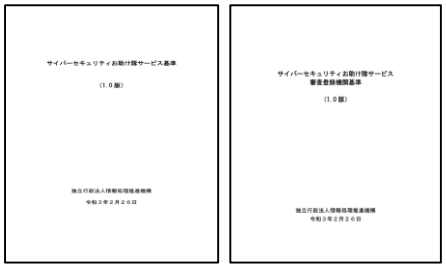
サイバーセキュリティお助け隊サービスマーク

「サイバーセキュリティお助け隊サービス基準」の主な内容

主な要件	概要
相談窓口	ユーザーからの**相談を受け付ける窓口**を設置／案内
異常の監視の仕組み	ネットワーク及び／又は端末を**24時間見守る仕組み**を提供
緊急時の対応支援	インシデント発生などの**緊急時には駆け付け支援**
中小企業でも導入・運用できる簡単さ	**専門知識がなくても導入・運用できるような工夫**
簡易サイバー保険	突発的に発生する駆付け費用等を補償する**サイバー保険**
中小企業でも導入・維持できる価格	・ネットワーク一括監視型：**月額１万円以下（税抜き）** ・端末監視型：**月額2,000円以下／台（税抜き）** ・併用型：**これらの和に相当する価格を超えないこと** ※端末1台から契約可能であることが条件

相談窓口、緊急時の対応支援、簡易サイバー保険などを**ワンパッケージで提供**

本サービスを採用することを通じて、取引先企業に対する**自社の信頼性のアピール**に



①サービス基準　②審査登録機関基準

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）**
- 今年度内、2回の審査を通じて登録サービスの拡充を図る（10月に第2回審査受付を実施、現在審査中）

【第1回登録サービスリスト】

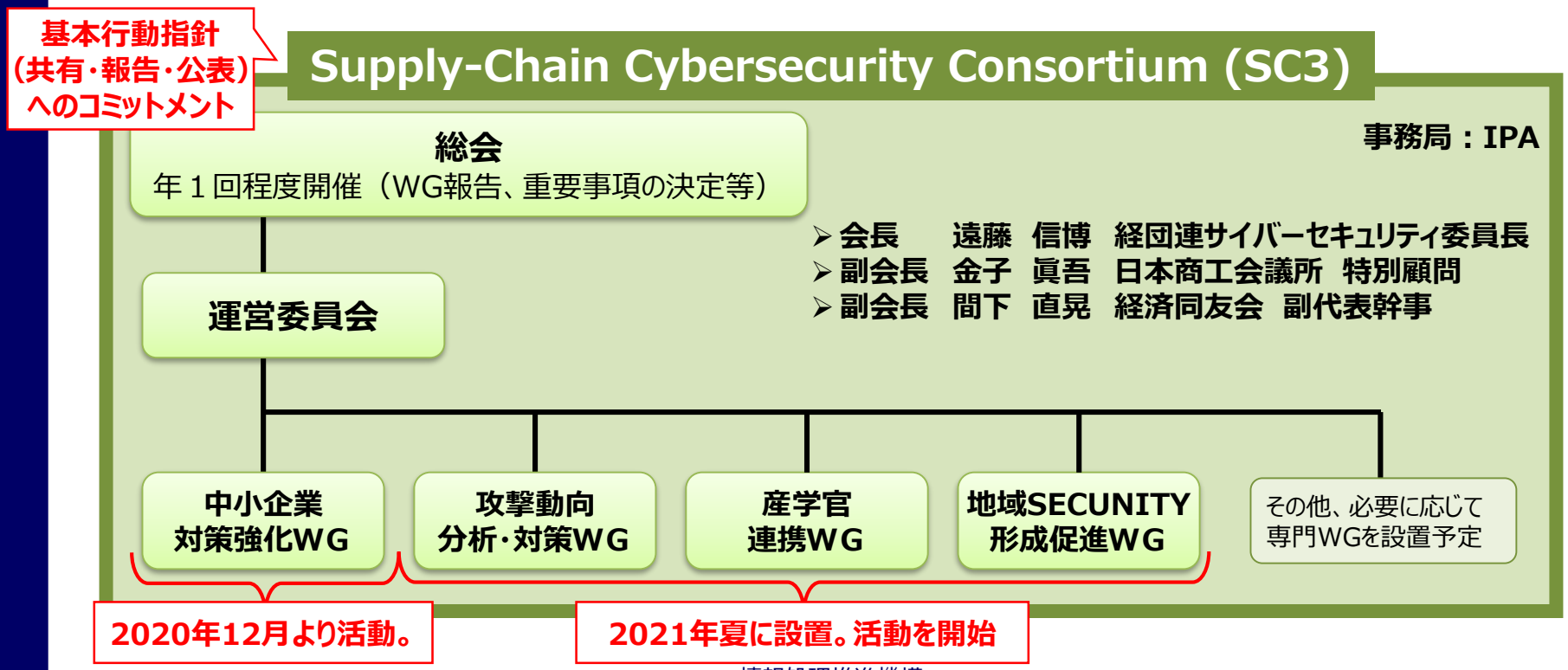
	サービス名	事業者名	対象地域
1	**商工会議所サイバーセキュリティお助け隊サービス**	大阪商工会議所	近畿エリア、名古屋・東京・神奈川の都心部 ※近畿地方に本社を置く企業
2	**防検サイバー**	ＭＳ＆ＡＤインターリスク総研株式会社	全国
3	**PCセキュリティみまもりパック**	株式会社ＰＦＵ	全国
4	**EDR運用監視サービス「ミハルとマモル」**	株式会社デジタルハーツ	全国
5	**SOMPO SHERIFF（標準プラン）**	ＳＯＭＰＯリスクマネジメント株式会社	全国

目次

- サイバーセキュリティを巡る状況と対策の必要性
- 具体的な対策～どこからどう始めるか？
  - SECURITY ACTION、中小企業の情報セキュリティ対策ガイドライン
  - サイバーセキュリティお助け隊サービス
- 産業界・地域と連携した対策普及の取組み ～ サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）
- 参考情報

サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）

- **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、業種別業界団体　等（2021年9月末時点で172会員）
- **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。



（参考）コンソーシアムの構成員

- 経済三団体（経団連、日本商工会議所、経済同友会）から役員が出ているほか、幅広い業界団体・個社が参加。（2021年9月末時点、93団体含む172会員）

役員
- 会　長　：一般社団法人 日本経済団体連合会　サイバーセキュリティ委員長　遠藤信博氏
- 副会長：日本商工会議所　特別顧問　金子眞吾氏　、　公益社団法人経済同友会　副代表幹事　間下直晃氏

団体会員リスト

特定非営利活動法人 日本ネットワークセキュリティ協会
一般社団法人 コンピュータソフトウェア協会
一般社団法人 日本金型工業会
鋳型ロール会
一般社団法人 日本陸用内燃機関協会
一般社団法人 日本機械工業連合会
石油連盟
特定非営利活動法人 ITコーディネータ協会
一般社団法人 日本電子回路工業会
一般社団法人 全国地方銀行協会
一般社団法人 日本自動車工業会
日本商工会議所
一般社団法人 中小企業診断協会
一般財団法人 日本自動車査定協会
一般社団法人 日本鋳鍛鋼会
日本筆記具工業会
一般社団法人 日本ボディファッション協会
日本化学繊維協会
一般社団法人 日本金属熱処理工業会
静岡県ソフトウェア事業協同組合
一般社団法人 日本化学工業協会
一般社団法人 情報サービス産業協会
一般社団法人 全日本文具協会
一般社団法人 日本ガス協会
特定非営利活動法人 映像産業振興機構
全国商工会連合会
全国社会保険労務士会連合会
日本ドキュメントサービス協同組合連合会
一般社団法人 日本風力発電協会
日本小売業協会
電気事業連合会
一般社団法人 日本医療機器産業連合会
一般社団法人 日本航空宇宙工業会
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
独立行政法人 中小企業基盤整備機構
一般社団法人 日本広告業協会
一般社団法人 情報処理安全確保支援士会
一般社団法人 日本電機工業会
一般社団法人 日本印刷産業連合会
一般社団法人 日本自動車部品工業会
一般社団法人 日本鉄鋼連盟
一般社団法人 ビジネス機会・情報システム産業協会
一般社団法人 太陽光発電協会
一般社団法人 日本中古自動車販売協会連合会
特定非営利活動法人 日本セキュリティ監査協会
一般社団法人 電子情報技術産業協会
一般社団法人 日本情報システム・ユーザー協会
一般社団法人 鹿児島県サイバーセキュリティ協議会
一般社団法人 日本工業炉協会
一般社団法人 日本経済団体連合会
一般社団法人 沖縄県情報産業協会
全日本フレキソ製版工業組合
一般社団法人 九州経済連合会
一般社団法人 日本金属プレス工業協会
産業横断サイバーセキュリティ検討会
一般財団法人 関西情報センター
一般社団法人 日本防衛装備工業会
四国ＩＴ協同組合
特定非営利活動法人 山梨ＩＣＴ＆コンタクト支援センター
一般社団法人 保健医療福祉情報システム工業会
せんい強化セメント板協会
一般社団法人 日本自動車機械器具工業会
一般社団法人 全国信用金庫協会
全国カレンダー出版協同組合連合会
一般社団法人 第二地方銀行協会
一般社団法人 日本損害保険協会
一般財団法人 デジタルコンテンツ協会
宮城県サイバーセキュリティ協議会
一般社団法人 中国経済連合会
一般社団法人 日本スポーツ用品工業協会
一般社団法人 日本オンラインゲーム協会
一般社団法人 長崎県情報産業協会
一般社団法人 日本レコード協会
一般社団法人 情報通信ネットワーク産業協会(CIAJ)
公益社団法人 経済同友会
一般社団法人 日本ボランタリーチェーン協会
公益社団法人 日本訪問販売協会
公益社団法人 日本マーケティング協会
一般財団法人 沖縄ITイノベーション戦略センター
公益社団法人 福岡貿易会
大阪商工会議所
公益財団法人 ハイパーネットワーク社会研究所
公益社団法人 関西経済連合会
一般社団法人 組込みシステム技術協会
一般社団法人 オープンガバメント・コンソーシアム
特定非営利活動法人 日本情報技術取引所
全国中小企業団体中央会
日本税理士会連合会
東部大阪経営者協会
一般社団法人 日本医療機器ネットワーク協会
独立行政法人　国立高等専門学校機構
一般社団法人　日本スマートフォンセキュリティ協会
一般社団法人　日本建設機械工業会

SC3　中小企業対策強化WG

- **趣旨**：中小企業のサイバーセキュリティ対策強化のために、**現状の課題**や官民が**取り組むべき施策**や方向性について幅広く検討。**取組検討**のためのセッションと、会員への**情報共有**のためのセッションの２種類のセッションを開催。
- 中小企業関係団体、業種別業界団体等が一堂に会し議論

- **本WGにおいて今後取扱う議題：**

◆ **業界別のセキュリティ対策取組共有**

- 各業種別業界団体より、サプライチェーンセキュリティ関連の取組を共有いただき、各業界で抱える課題や今後の方向性について業種間共有を図る。

◆ **SECURITY ACTION制度の次の展開**

- 「SECURITY ACTION制度について発注元企業のニーズも含むご意見をいただきながら、今後の展開について検討を行う。

◆ **発注元企業として取り組むべき課題の整理**

- 中小企業に対する取組の強化に加え、発注元となる企業として取り組むべき課題について整理。

SC3　その他のWG

攻撃動向分析・対策WG

- **目的：**サイバー攻撃が日々高度化・巧妙化していく中で、**ユーザー企業の経営層**が認識すべきサイバー**攻撃に関する動向**やセキュリティ**対策**・インシデント**対応**上の**留意点を産業横断的に発信**することでサプライチェーン全体のセキュリティ対策の底上げを図る。
- **活動内容：**ユーザー企業の経営層が、**ビジネス・経営の観点**から認識・留意すべきサイバーセキュリティ関連動向や事例に基づくインシデント対応ポイント等を取り纏め、ウェビナー、レポート、メルマガ等でSC3会員向けに情報を配信。

産学官連携WG

- **目的：産学官連携**による**セキュリティ人材の育成・活躍推進**、学術機関におけるセキュリティ対策の強化などサプライチェーンにおけるサイバーセキュリティの強化のために産学官が連携して実施すべき取組について検討・推進する。
- **活動内容：産学官が情報・意見交換**を行う場として、サプライチェーンにおけるサイバーセキュリティの強化のために産学官が連携して実施すべき取組について包括的に検討・推進する。まずは取組が先行している**セキュリティ人材の育成・活躍**（特に取組が先行する高等専門学校と産業界の連携による人材育成）について先行して議論を開始し、状況に応じて取組を拡大。

地域SECUNITY形成促進WG

- **目的：**各地域で形成が進みつつある**地域のセキュリティ・コミュニティ（地域SECUNITY）の取組をさらに推進**するため、**地域間の情報共有**や、**共通課題の解決**に向けた取組を検討・推進する。
- **活動内容：**各地域SECUNITYの担当者等を対象として、各地域における活動にあたって必要となる**情報の共有**、**ベストプラクティス**の展開、**共通課題**に対する解決策の検討などを目的としたワークショップやセミナー等を企画・開催する。また、共通課題に対する解決策の検討にあたっては、必要に応じて支援機関、業界・経済団体等を募り、　有効な取組の検討等を行う。

ご参考：サイバーセキュリティお助け隊サービス　関連URL

- **サイバーセキュリティお助け隊サービス**

  https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html
- **2019年度　サイバーセキュリティお助け隊実証事業**

  https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index2019.html
- **2019年度　サイバーセキュリティお助け隊実証事業　成果報告書**

  https://www.ipa.go.jp/security/fy2019/reports/sme/otasuketai_houkoku.html
- **2020年度　サイバーセキュリティお助け隊実証事業**

  https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index2020.html
- **プレス発表 「サイバーセキュリティお助け隊サービス」に5つのサービスを登録（2021年4月15日）**

  https://www.ipa.go.jp/about/press/20210415.html
- **サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）**

  https://www.ipa.go.jp/security/keihatsu/sme/sc3/index.html

目次

- サイバーセキュリティを巡る状況と対策の必要性
- 具体的な対策～どこからどう始めるか？
  - SECURITY ACTION、中小企業の情報セキュリティ対策ガイドライン
  - サイバーセキュリティお助け隊サービス
- 産業界・地域と連携した対策普及の取組み ～ サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）
- 参考情報

情報セキュリティ対策支援サイト

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

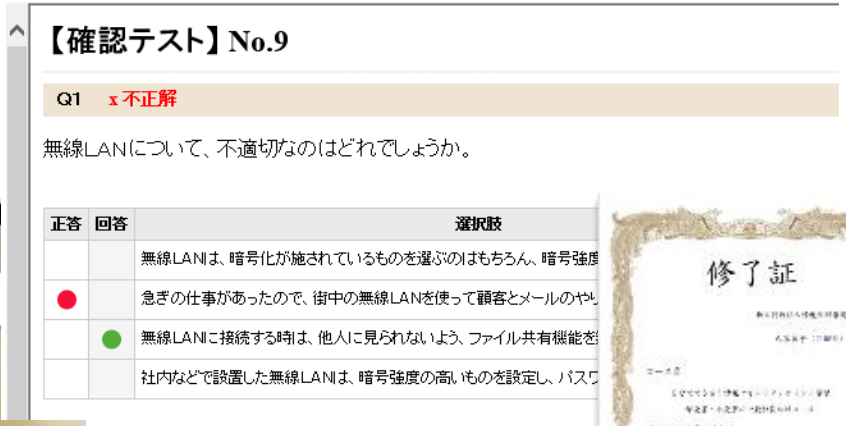
情報セキュリティ対策を「**始めたい**」「**強化したい**」
「**学びたい**」中小企業の方々をサポートするポータルサイト

- 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

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

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

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

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

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」

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**

ご清聴
ありがとうございました。