経済産業省

サプライチェーン全体のサイバーセキュリティ強化に向けた取組について

経済産業省
サイバーセキュリティ・情報化審議官
江口　純一

１．サプライチェーンを通じた攻撃

(独)情報処理推進機構：情報セキュリティ10大脅威 2020

昨年順位	個　人	順　位	組　織	昨年順位
ランク外	スマホ決済の不正利用 NEW	1位	標的型攻撃による情報流出	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（規則は遵守）	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 ↘

<出典：(独)情報処理推進機構(IPA)、2020.1.29.>

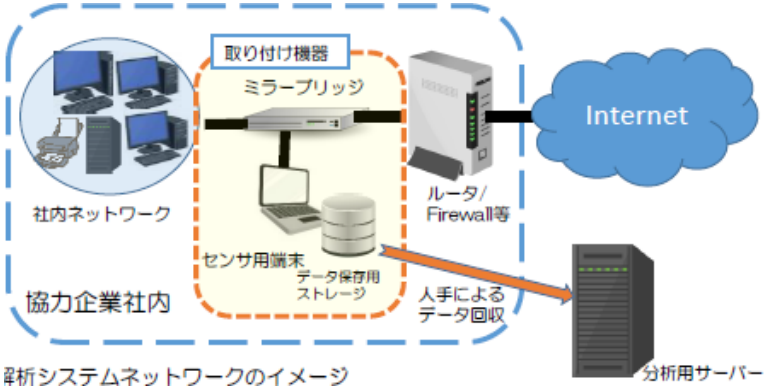
中小企業に対するサイバー攻撃の調査･分析結果（大阪商工会議所）

- 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。

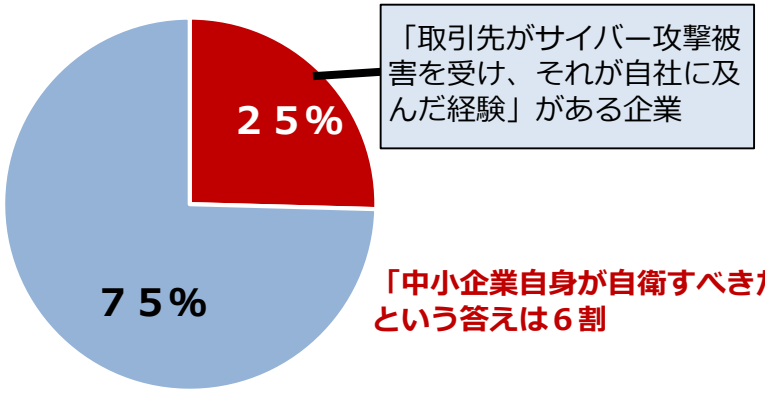
取引先経由の被害に関する調査

■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%**）



「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）

<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。

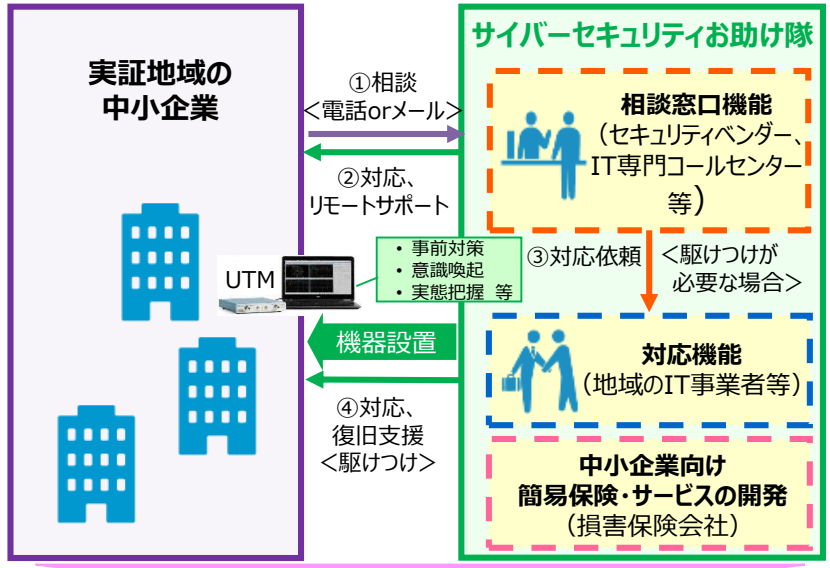
２．経済産業省・IPAの
サイバーセキュリティ政策

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

（参考）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。

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

＜実証参加の成果（参加中小企業のアンケート結果より）＞

- 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）

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）

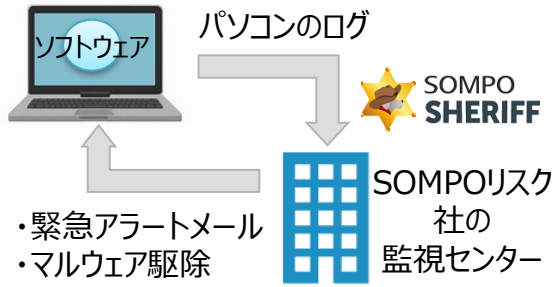
実証を通じて中小企業にとって必要な機能・サービスを精査することで、安価なサービスを実現。

（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、**<u>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</u>**することで、**<u>民間でのサービス展開を支援</u>**。

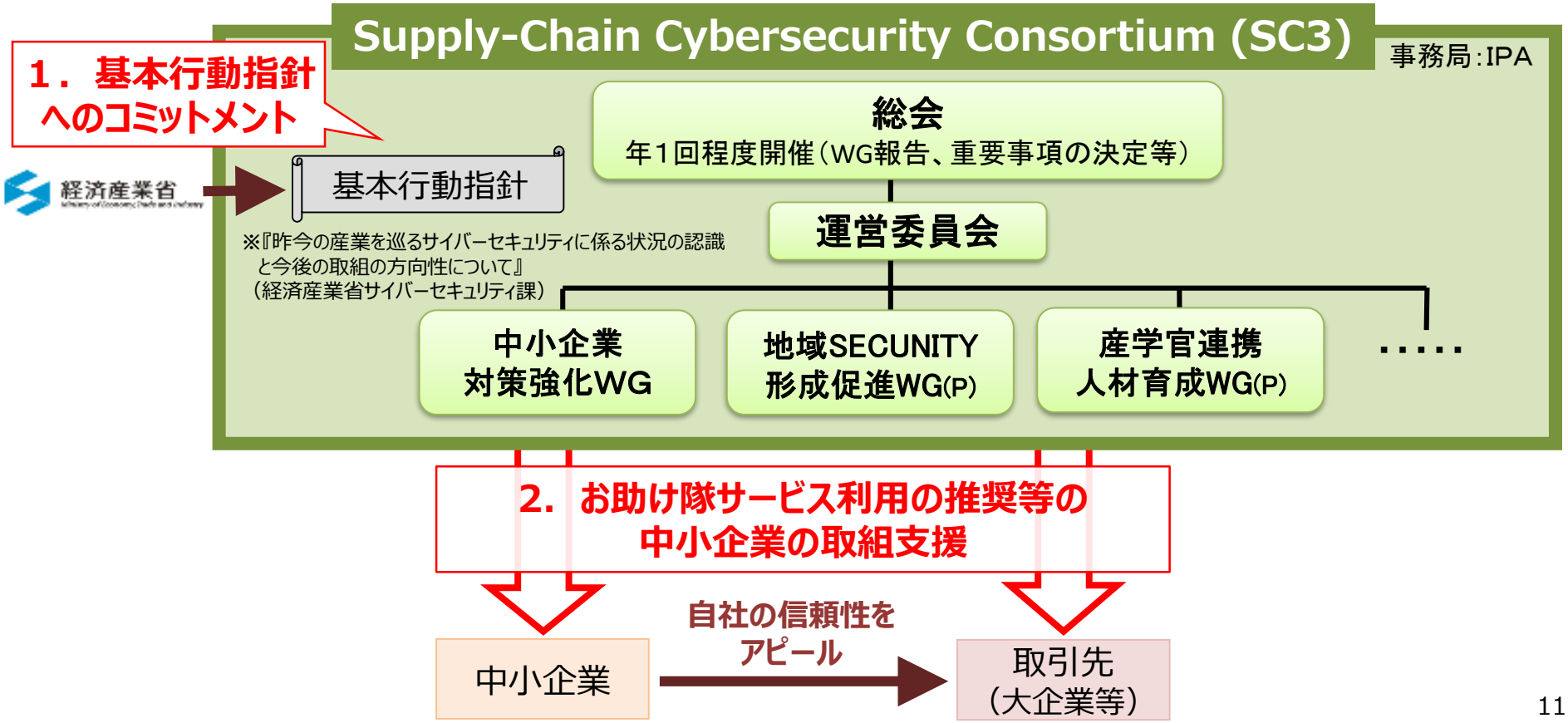
産業界を挙げた
サプライチェーン全体のサイバーセキュリティ強化運動の展開へ

１．企業のリスクマネジメント強化のための基本行動指針の設定（2020年６月12日）

共有（Share）	報告（Report）	公表（Announcement）
①サプライチェーン共有主体間での高密度な情報共有 ☞ NDA関連情報が目安	②機微技術情報の流出懸念時の経産省への報告 ☞ 輸出管理対象技術が目安	③適切な場合の公表 ☞ 被害企業内での取締役会への報告事項(①の対象外のもの)が目安

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。



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。
- **１０万社を超える中小企業が宣言**（2020年10月末時点）。

★ 一つ星

SECURITY ACTION ★

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

SECURITY ACTION ★★

セキュリティ対策自己宣言

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

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/

3. 参考資料

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

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　映像　**検索**

情報セキュリティ安心相談窓口

IPA

・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

電話　03-5978-7509
平日　10：00-12：00、13：30-17：00

メール　anshin@ipa.go.jp

ポータル　IPA安心相談　検索

相談窓口・注意喚起情報

2020年12月18日公開資料

● 内閣サイバーセキュリティセンター（NISC)

注意喚起情報	URL：https://twitter.com/nisc_forecast
ランサムウェアによるサイバー攻撃について（2020.11.26）	URL：https://www.nisc.go.jp/active/infra/pdf/ransomware20201126.pdf

● （独）情報処理推進機構（IPA）

■一般的な情報セキュリティ（主にウイルスや不正アクセス）に関する技術的な相談

情報セキュリティ安心相談窓口	URL：https://www.ipa.go.jp/security/anshin/index.html 電話：03-5978-7509

■標的型サイバー攻撃を受けた際の相談（専門的知見を有する相談員が対応）

J-CRAT／標的型サイバー攻撃特別相談窓口	URL：https://www.ipa.go.jp/security/tokubetsu/index.html 電話：03-5978-7599

セキュリティ関連情報サイト	URL：https://www.ipa.go.jp/security/index.html
ランサムウェアに関する注意喚起	URL：https://www.ipa.go.jp/security/announce/2020-ransom.html

● （一社）JPCERTコーディネーションセンター（JPCERT/CC）

■インシデントに関する対応依頼

インシデント対応依頼	URL：https://www.jpcert.or.jp/form/

注意喚起情報	URL：https://www.jpcert.or.jp/at/2020.html
マルウェアEmotetへの対応FAQ	URL：https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html