

「IPA NEWS」はIPAの日々の活動をわかりやすくご紹介する広報誌です。



- データで読むITの今・未来
中小企業約1,100社に18万件超の不審なアクセス！
- セキュリティのすゝめ 01〈ランサムウェアの手口と対策〉
事業継続までも脅かすランサムウェアの脅威
- IPAの最新情報をまとめてお届け！
Hot & New Topics
- 目指せ！ 情報処理のエキスパート!!
国家試験に挑戦！ ～ITパスポート試験編～

中小企業の強い味方

サイバーセキュリティ お助け隊サービス始動!

IPA
セキュリティセンター 企画部
中小企業支援グループ
研究員 小野 慎一郎さん(左)

IPA
セキュリティセンター 企画部
中小企業支援グループ
寺江 晴菜さん(中央)

IPA
セキュリティセンター 企画部
中小企業支援グループ
主幹 赤木 伸悟さん(右)

大手企業のみならず、中小企業でもサイバー攻撃の脅威が高まっています。対策が後手に回ると、サプライチェーン全体に甚大な被害が及ぶことも想定されます。今こそ活用したい「サイバーセキュリティお助け隊サービス」と、その審査登録制度についてIPAの担当者に聞きました。

対策ソフトだけでは脅威を防ぎきれない

大手企業がサイバー攻撃に遭ったというニュースがたびたび報じられますが、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ことをご存じでしょうか。

大阪商工会議所が中小企業30社を対象に調査(2018~2019年)したところ、全社がサイバー攻撃を受け、少なくとも5社で情報が外部に流出した恐れがあるとわかりました。また、同所の大企業・中堅企業118社への調査(2019年)では、取引先が受けたサイバー攻撃の影響が自社に及んだという企業が25%に上っています。

製造から販売までのサプライチェーン(商流)のデジタル化が進

む昨今では、わずか1ヶ所のセキュリティの綻びが全体に悪影響を及ぼしかねません。IPAが毎年発表している「情報セキュリティ10大脅威」組織編でも、「サプライチェーンの弱点を悪用した攻撃」が2019年から3年連続で4位にランクインしています。中小企業のセキュリティ強化は自社にとってだけでなく、サプライチェーン全体としても急務なのです。

とはいえ、中小企業では人材・体制・資金に限りがあります。そこで中小企業の実態を把握してセキュリティ強化を支援する仕組みを構築するため、経済産業省とIPAはITベンダーや地域団体、損害保険会社と連携し、「サイバーセキュリティお助け隊実証事業」を2年にわ

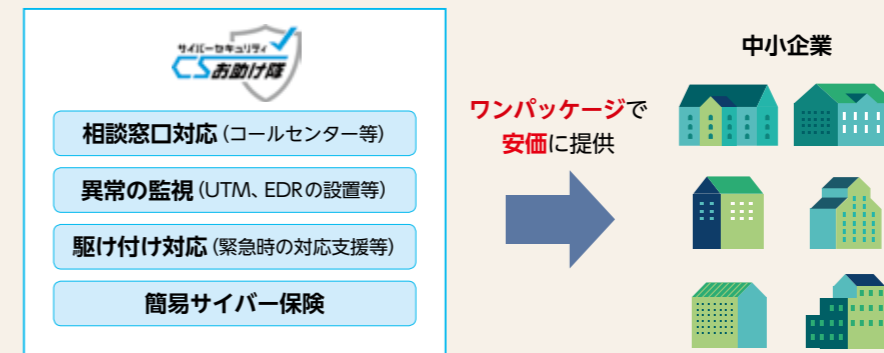
たって実施しました。

2019年度の実証事業は、全国8地域で中小企業1,064社が参加。「重大なインシデントの可能性があると判断し対処した件数は128件に上りました。中には対処を怠った場合の被害想定額が5,000万円近くになるケースもありました」とIPAセキュリティセンターの赤木伸悟さんは明かします。

15の地域・産業分野で1,117社が参加した2020年度の実証事業でも、ほとんどの中小企業がサイバー攻撃の危険にさらされている実態が浮き彫りになりました。

実証事業に参加した企業の9割はウイルス対策ソフト(以下、対策ソフト)を導入しています。しかし、それだけではセキュリティ対策は不

図表 「サイバーセキュリティお助け隊サービス」で提供するサービス内容



● 第1回登録サービスリスト

サービス名	事業者名
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
防検サイバー	MS & ADインターリスク総研株式会社
PCセキュリティみまもりパック	株式会社PFU
EDR運用監視サービス「ミハルとモモル」	株式会社デジタルハーツ
SOMPO SHERIFF(標準プラン)	SOMPOリスクマネジメント株式会社

十分だとIPAセキュリティセンターの小野慎一郎さんは指摘します。「対策ソフトは既知のウイルスをもとにしたパターンマッチングで検知します。そのため、特定企業を狙った標的型攻撃ではウイルスを検知しきれないことがあるのです。また、ファイルを暗号化・圧縮された場合も、一般的な対策ソフトではウイルスを捕捉できません」

事実、2020年度の実証事業でも先述と同様に被害想定額が高額に及ぶ攻撃を受けた企業があり、同社でも対策ソフトは導入していました。にもかかわらず、ウイルスの侵入を許してしまったわけです。

実証事業では、ネットワークを統合的に一括監視するUTM、端末やサーバーなどエンドポイントの侵害を検知して対応するEDRを導入している企業もありました。しかし、社内にIT人材がいないため十分使いこなせていないケースがあったと小野さんは言います。「たとえるなら、UTMはマンションのエントランスに設置されているオートロック、EDRは個々の部屋

の鍵のようなものです。ネットワーク各所のわずかな隙を狙う不正プログラムが横行している実態を考えると、UTMやEDRをしっかり活用することもセキュリティ対策の要となります」

対策の見える化も実現。取引先への信頼性向上に

そこで頼りになるのが、「サイバーセキュリティお助け隊サービス」(以下、お助け隊サービス)です。「これは、相談窓口やUTM等の機器の設置による異常の監視、緊急時対応、簡易サイバー保険など、中小企業のセキュリティ強化に不可欠なサービスを安価にワンパッケージで提供するものです」とIPAセキュリティセンターの寺江晴菜さんは説明します(図表)。

実証事業で得られた知見に、サプライチェーンにおけるセキュリティ強化の業界横断的な枠組みである「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)での検討も加えて、中小企業向けのセキュリティサービスが満

たすべきサービス基準を策定。その基準を満たすサービスにIPAが「サイバーセキュリティお助け隊サービスマーク」の使用を許諾することで普及の促進を図ります。

図表にある通り、2021年3月の第1回審査では5つのサービスが登録され、「サイバーセキュリティお助け隊サービスマーク」付きのサービスとして展開が始まっています。安価かつ効果的な中小企業向けセキュリティ対策支援サービスとしてある種のお墨付きが与えられた形で提供されるということで、画期的なものといえるでしょう。

「中小企業にとっては相談できる専門家が身近にできるだけでなく、お助け隊サービスの採用・導入が自社の対策の見える化も実現するので、取引先に対する信頼性向上に大きくつながるはず」と寺江さん。

日頃からセキュリティ対策自己宣言制度「SECURITY ACTION」や「中小企業の情報セキュリティ対策ガイドライン」といった制度やコンテンツを活用した基本的な対策を講じることがまず重要ですが、その上で「専門的なツールをどう使えばよいのか」「何かおかしい動きがある」といった場合の備えとして、お助け隊サービスを活用したいものです。

「DXの推進が叫ばれていますが、イノベーションや業務効率化は万全のセキュリティ対策があってこそ。攻めと守りの両輪が大事です」と赤木さん。「セキュリティ対策をコストではなく、取引先へのアピールや将来への投資ととらえて、お助け隊サービスの活用をぜひご検討ください。それがサプライチェーン全体のセキュリティ強化にもつながるのです」と展望を語ってくれました。

セキュリティ強化に不可欠なサービスをワンパッケージで



中小企業約1,100社に 18万件超の不審なアクセス!

サイバーセキュリティお助け隊実証事業で判明!
地域の中小企業もサイバー攻撃の脅威にさらされています。

(参考資料) サイバーセキュリティお助け隊(令和2年度中小企業向けサイバーセキュリティ対策支援体制構築事業)の報告書
https://www.ipa.go.jp/security/fy2020/reports/sme/otasuketai_houkoku.html

サイバーセキュリティお助け隊実証事業概要(令和2年度中小企業向けサイバーセキュリティ対策支援体制構築事業)

対象	全国13地域(24道県)と合わせて以下の2産業を実証対象とした。 ・防衛・航空宇宙産業(関東・中部・関西地方) ・自動車産業(静岡県・広島県等)
参加企業	上記に該当する中小企業1,117社
参加企業の属性	・業種は製造業(24.1%)、卸売業・小売業(13.6%)、サービス業(10.2%)など多種多様 ・従業員数規模は1,000人未満の企業が中心。各割合は1~5人(24.3%)、21~50人(20.2%)、201~300人(3.1%)など
UTM設置数	746
EDR設置数	437
実証期間	2020年10月~2020年12月

FACT 1

社内システムへの侵入等を試みる
不審なアクセスを検知した件数

181,536件

FACT 2

ランサムウェアやトロイの木馬などの
ウイルスを検知し、無害化した件数

1,345件

CASE 1

従業員がダウンロードしたフリーソフトから社内の端末がウイルス感染。感染した端末から攻撃者サーバーへの不正通信が1ヶ月の間に**4,126件**検知された。

CASE 2

ウイルスが仕込まれていると思われる報告書を添付した、なりすましメールが同じ企業宛てに**3日間にわたって**送付されていた。

CASE 3

実証期間内で同一企業へのランサムウェアの攻撃を**129件**検知した。

業種や事業規模を問わずサイバー攻撃や不審なアクセスなどの脅威に晒されていることがわかり、中には攻撃者が狙った企業に対して集中的に攻撃を仕掛けているといったケースも見られました。また、ウイルス対策ソフトの導入といった既存対策だけでは攻撃を防ぎきれていない実態も明らかとなりました。

「うちは狙われない」はキケンです。
リスクに備え、速やかな対策をとみましょう!

01

Theme

知っていますか?

事業継続までも脅かす ランサムウェアの脅威

❗ 米国パイプラインなど 社会インフラも被害

今年5月、アメリカのパイプラインがサイバー攻撃を受け、一時操業停止に追い込まれたことが世界的なニュースになりました。ここで使われたのが、ランサムウェア(Ransomware)というコンピュータウイルスです。

国内では昨年11月にゲームメーカーのカプコンが被害を受けたことを発表し、注目を集めました。ランサムウェアに悩まされる企業は後を絶たず、「情報セキュリティ10大脅威2021」の組織編でも1位にランクインしており、業種や企業規模にかかわらず、すべての組織において厳重な警戒が必要な脅威です。

❗ データを“人質”にして 身代金を要求する

ランサムウェアという名称は「Ransom

(身代金)」と「Software(ソフトウェア)」を組み合わせたものです。パソコンやサーバーが感染すると保存データが暗号化され、その復旧と引き換えに身代金が要求されるのです。

感染経路の多くはメールやウェブサイトです。メールの添付ファイルや本文中のリンクを開かせる、攻撃者が用意したウェブサイトを開いた際にブラウザの脆弱性を悪用するといった手口が横行しています。対策には、メールの添付ファイルやリンクを安易に開かない、OSやソフトウェアを常に最新の状態にする、データのバックアップを取っておくなどが有効です。

❗ 新たなランサムウェア攻撃 の手口と対策は?

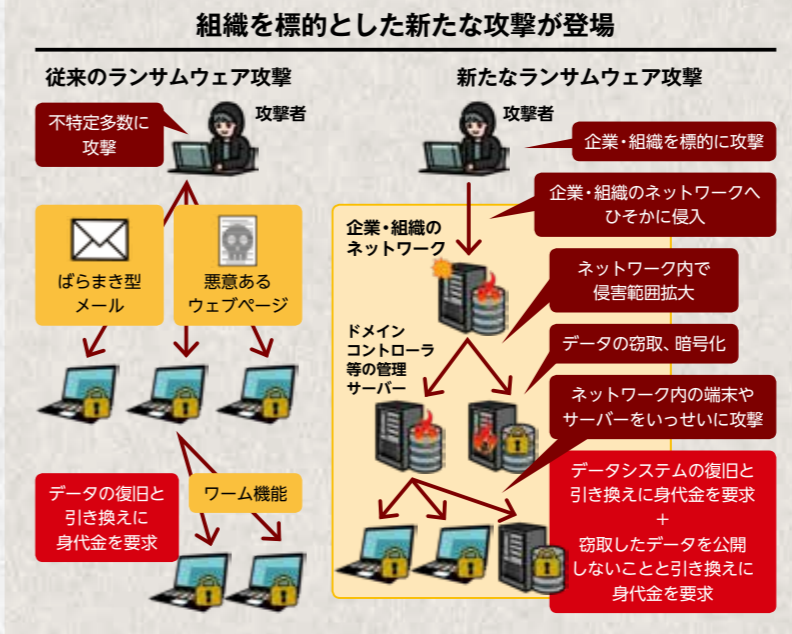
最近では、組織のネットワークに侵入してパソコンやサーバーを感染させる「人手によるランサムウェア攻撃」

や、暗号化する前にデータを窃取し、そのデータを公開しないことを条件に金銭を払わせる「二重の脅迫」といった新たな手口も見られます。この攻撃によって組織のパソコンやサーバー等が数千、数万台規模で暗号化されたり、数テラバイトものデータが窃取されたりする恐れがあり、実際にデータが暴露されたケースも報告されています。身代金を支払ってもデータが復旧されたり、攻撃者がデータを約束通り破棄したりする保証はなく、事業継続にまで影響を及ぼすこともある深刻な脅威です。

ネットワークへの侵入手口として、VPN装置やリモートデスクトップの設定不備の悪用やVPN装置の脆弱性の悪用、メールの添付ファイルなどが確認されています。それらへの対策としては、インターネットからアクセス可能なサーバー等は最小限にし、適切なアクセス制御や認証を行うなどが挙げられます。また、基本的な対策に加え、システムの再構築を含めた復旧計画を事前に策定しておくことも重要です。着実に多層的な防御を講じて、ランサムウェア攻撃の脅威から身を守りましょう。

+ 「脅威」の特徴と対策 +

- 1 近年有数の重大な脅威。企業や社会に深刻な影響
- 2 データの暗号化と暴露という「二重の脅迫」も
- 3 金銭を支払ってもデータ復旧の保証はない
- 4 確実かつ多層的なセキュリティ対策が重要



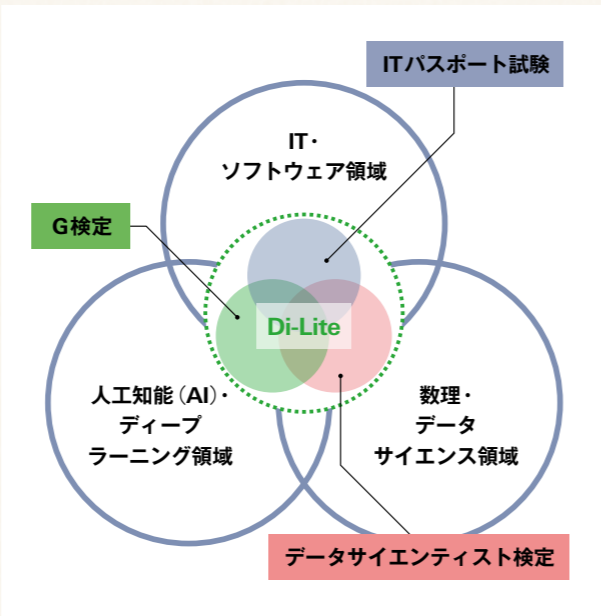
もっと詳しく知りたい方は… <https://www.ipa.go.jp/security/announce/2020-ransom.html>

「デジタルリテラシー協議会」を設立

DSS（一般社団法人データサイエンティスト協会）、JDLA（一般社団法人日本ディープラーニング協会）、IPAは3団体共同にて「デジタルリテラシー協議会」を設立しました。当協議会では、DX時代のビジネスパーソンに求められるデジタルリテラシー※を「Di-Lite（ディーライト）」と定義し、各団体が実施する「ITパスポート試験」、「データサイエンティスト検定リテラシーレベル」、「G検定」のシラバスにも反映することで、その普及促進を行います。また、Di-Liteをはじめとするデジタルリテラシー・スキル習得の促進のため、デジタルに関連して習得すべきスキルや知識・マインドを全体像として表した「デジタルリテラシー・スキルフレームワーク」を併せて公開しました。

※IT・データサイエンス・AIを使うための基礎的なスキル・知識・マインド
<https://www.ipa.go.jp/about/press/20210420.html>

● デジタルリテラシー Di-Liteと検定・試験の位置づけ



「ひろげよう情報モラル・セキュリティコンクール」作品募集

6月より「ひろげよう情報モラル・セキュリティコンクール」の作品募集を開始しました。

本コンクールは、情報モラル・情報セキュリティの大切さを伝える作品を全国の児童・生徒から募集し、表彰するものです。標語やポスター、4コマ漫画などの作品制作を通じて、子どもたちが情報モラルや情報セキュリティについて考え、意識を高めていくことを目的としています。

ウイルス対策やパスワードの管理、安全なSNSの使い方など、インターネットやデバイスを利用するうえで必要な対策やモラルなどをテーマにした作品を9月17日（金）まで受け付け、教育関係者や有識者の審査によって受賞作品を決定します。各受賞作品の公表は12月頃を予定しています。

<https://www.ipa.go.jp/security/event/hyogo/>

● 第17回IPA「ひろげよう情報モラル・セキュリティコンクール」2021 募集概要

◆ 募集部門

標語部門、ポスター部門、4コマ漫画部門、書写（硬筆）、活動事例

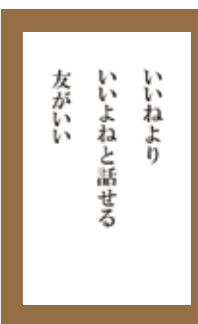
◆ テーマ

情報モラルおよび情報セキュリティ
 〈キーワードの例〉ウイルス、パスワード、アップデート、なりすまし、フィッシング、不正アプリ、フリーWi-Fi、不正なアップロード/ダウンロードなど

◆ 応募締切

2021年9月17日（金）【当日必着】

2020年度受賞作品 （標語部門）



諫早市立西諫早中学校 1年 石橋 蘭さん

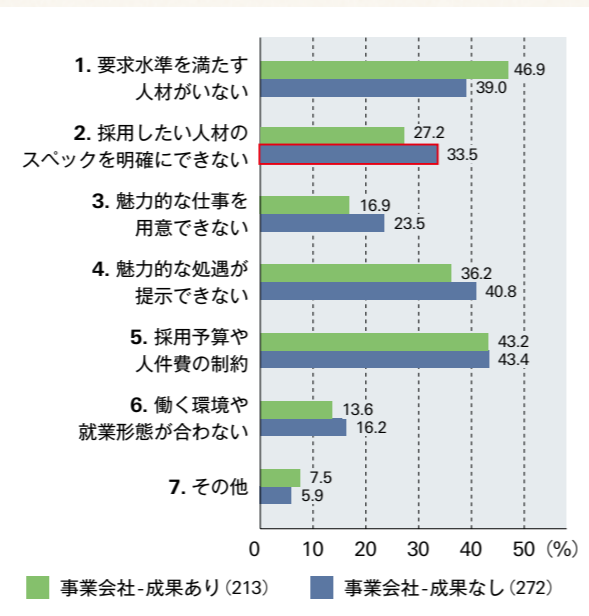


「デジタル時代のスキル変革等に関する調査報告書」を公開

第4次産業革命の実現にはデジタル技術の活用だけでなく、その推進基盤となる「人や組織のマネジメントのあり方」の変革も重要です。本調査ではその観点からIT人材のスキル変革の促進要因や阻害要因などを分析しました。調査の結果、「DXで成果が出ない企業では人材不足を訴えてはいるものの、デジタル化戦略やそれに必要な人材要件が明確になっていない」「人材市場において自身のスキルレベルが分からないIT人材の割合は3割以上に上る」といったことなどがわかりました。今回の調査では、このほか先端領域への転換に関して人材を5つに分類した「転換タイプ」の分析なども行っており、これらの結果は、企業での人材育成や採用、処遇制度の改善などに役立っていただけます。

<https://www.ipa.go.jp/ikc/reports/20210422.html>

● IT人材を新たに採用する阻害要因（複数回答）



Just Information

「IPA Channel」おすすめ映像コンテンツ

IPA公式YouTubeチャンネル「IPA Channel」に公開している、今注目のおすすめ映像をご紹介します！

手口検証動画シリーズ

つい引かかる!? よくある「だましの手口」と対処法を解説

「宅配業者を装った不在通知の偽SMSの手口」、「iPhoneのカレンダーに不審な書き込みを行う手口」など、最近、IPAに相談が多く寄せられているだましの手口を検証した映像シリーズ。パソコンやスマートフォンでどのようにだましの手口が使われるのか、手口の流れと被害の回避方法を学べます。（2021年5月時点で7つの手口を公開中。）



ネット接続製品の安全な選定・利用ガイド

“なんとなく”で選ぶと危険！ ネット接続製品の選び方・使い方のポイントを解説

スマート家電やゲーム機といったネットワークに接続する製品には、サイバー攻撃による不正利用や情報漏えい、破損などのリスクが潜んでいます。セキュリティに考慮した製品を見極めるポイントや、被害に遭わないために行うべき基本的なセキュリティ対策などを解説しています。



映像で知る情報セキュリティ

検索

「IPA Channel」チャンネル登録はこちら
<https://www.youtube.com/user/ipajp>



目指せ！情報処理のエキスパート！！

国家試験に挑戦！ ～ITパスポート試験編～

ITパスポート試験(iパス)は、IT社会で働くすべての社会人が備えておくべきITに関する基礎的な知識が証明できる国家試験です。

問1 ストラテジ系【令和3年度・問4】

エンタープライズサーチの説明として、最も適切なものはどれか。

- ア 企業内の様々なシステムに蓄積されている定型又は非定型なデータを、一元的に検索するための仕組み
- イ 自然言語処理を実現するための基礎データとなる、電子化された大量の例文データベース
- ウ 写真や書類などを光学的に読み取り、デジタルデータ化するための画像入力装置
- エ 情報システムや業務プロセスの現状を把握し、あるべき企業の姿とのギャップを埋めるための目標を設定し、全体最適化を図ること

問2 マネジメント系【令和3年度・問52】

自社の情報システムに関して、BCP(事業継続計画)に基づいて、マネジメントの視点から行う活動a～dのうち、適切なものだけを全て挙げたものはどれか。

- a 重要データのバックアップを定期的に取り得する。
 - b 非常時用の発電機と燃料を確保する。
 - c 複数の通信網を確保する。
 - d 復旧手順の訓練を実施する。
- ア a, b, c イ a, b, c, d ウ a, d エ b, c, d

問3 テクノロジ系【令和3年度・問58】

サーバールームへの共連れによる不正入室を防ぐ物理的セキュリティ対策の例として、適切なものはどれか。

- ア サークル型のセキュリティゲートを設置する。
- イ サーバの入ったラックを施錠する。
- ウ サーバルーム内にいる間は入室証を着用するルールとする。
- エ サーバルームの入り口に入退室管理簿を置いて記録させる。

正解：問1ア 問2イ 問3ウ

IPAの事業領域

情報セキュリティ対策の実現

- 社会を守る
- 対策を促す
- 安全を担保する

IT人材の育成

- サイバーセキュリティ人材を育てる
- ITイノベーション人材を磨き上げる
- IT人材の知識・スキルを認定する

IT社会の動向調査・分析・基盤構築

- IT社会の動向調査・分析、情報発信
- IoT製品・システムの安全性・信頼性を確保する
- 地域における取り組みの支援
- データ利活用を促進する
- スキル変革の推進

「IPA NEWS」定期送付のお申込み、送付先の変更は、
下記のメールアドレスにご連絡くださいますようお願い致します。
メール pr-inq@ipa.go.jp

IPAのSNS公式アカウント、メールニュースの配信登録はこちら

   <https://www.ipa.go.jp/>

本誌に記載の製品名、サービス名などは、IPAまたは各社の商標もしくは登録商標です。

 独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan

