

「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。



特集

かしこい中小企業はもう始めている!! “守るが勝ち”の セキュリティ対策!

- データで読むITの今・未来
標的に「例外」はない! 中小企業を狙うサイバー攻撃
- セキュリティのすゝめ 10〈取引先や経営層を装う詐欺の手口と対策〉
巧妙な手口に注意! 「ビジネスメール詐欺」
- IPAの最新情報をまとめてお届け!
Hot & New Topics

株式会社 DankSoft
代表取締役 CEO
星野晃一郎さん

IPA
セキュリティセンター
企画部
中小企業支援グループ
鈴木浩之さん

特集

かしこい中小企業はもう始めている!!

“守るが勝ち”のセキュリティ対策!

サイバー攻撃のリスクが高まる昨今、中小企業のセキュリティ対策は大きな課題です。被害を受ければ自社ばかりか、サプライチェーンにも悪影響を及ぼします。今回の特集では、IPAが提供する中小企業向けのセキュリティ対策コンテンツに着目。これらを活用している株式会社 DankSoft の代表取締役 CEO・星野晃一郎さんにお話をうかがいます。

ランサムウェア攻撃の被害の約半数は中小企業

サイバー攻撃の魔の手は大企業のみならず、中小企業にも迫っています。警察庁の調査によると、2022年の上半期、深刻な被害をもたらすランサムウェア攻撃の被害の約半数は中小企業でした^{*}。被害を受けると復旧に時間も費用もかかるうえ、サプライチェーンへの悪影響や取引先からの信用低下といったデメリットも招きます。「事業規模が小さいから狙われる心配はない」と他人事にせず、どの企業もしっかり対策を行うことが重要です。

平時の備えとして活用したいのが、IPAが提供する「SECURITY ACTION」です。セキュリティ対策に取り組んでいることを事業者が

自己宣言する制度で、中小企業におけるセキュリティの具体的方策を示した「中小企業情報セキュリティガイドライン」の実践をベースに、2段階の取り組み目標を示しています。1段階目(一つ星)は「情報セキュリティ5か条」に取り組むことを宣言。2段階目(二つ星)は「5分のできる! 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します。IPA セキュリティセンターの鈴木浩之さんは「セキュリティ対策に悩む中小企業の皆さんに、まずは意識を高めていただくためのツールです。各種補助金などの申請要件に含まれていることもあり、自己宣言数は20万件を突破しまし

た」と説明します。

株式会社 DankSoft (東京・千代田区)も宣言した企業の1社。ウェブサイトのコンサルティング・制作・構築などを手掛ける1983年創業のIT企業です。同社では学童クラブやNPOなど中小組織のデジタルデバインド(格差)の解消やペーパーレス化を支援。副次的効果として、事務処理の効率化、働きやすさの実現、コミュニティの活性化といったメリットも生み出しています。

同社の代表取締役CEOである星野晃一郎さんは「顧客に金融機関が含まれることもあり、当社では早くから自社のセキュリティ対策に意欲的に取り組んできました」と語ります。2006年にプライバシーマークを取得するとともに、ペー

図表 「5分のできる! 情報セキュリティ自社診断」(全25問のうちから一部抜粋)

診断項目	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	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
	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
従業員としての対策	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?	4	2	0	-1
	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?	4	2	0	-1
	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?	4	2	0	-1
	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?	4	2	0	-1
組織としての対策	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?	4	2	0	-1
	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?	4	2	0	-1
	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?	4	2	0	-1
	クラウドサービスやウェブサイトの運用等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?	4	2	0	-1

「5分のできる! 情報セキュリティ自社診断」はこちらから。
<https://www.ipa.go.jp/security/keihatsu/sme/guideline/5minutes.html>

パーレス化を推進。2008年ごろからクラウドへの移行を進め、段階的にFAXやプリンタもオフィスからなくし、現在はウェブ会議やテレワークのインフラを含めた高度なデジタル環境を構築しています。

同社のセキュリティ対策は、不正アクセス防御、ユーザ認証、マルウェアのリアルタイム検出、データのバックアップ、デバイスの情報保護、定期的なチェックによる情報漏えい対策など実にさまざま。2019年にSECURITY ACTION(一つ星)を宣言していますが、「二つ星でも遜色のない充実ぶりです」と鈴木さんは述べます。

セキュリティ対策は経営の根幹に関わる

DankSoftの取り組みで特に目を引くのが、セキュリティ関連の社外向け申請業務を、新人や社歴の浅い人に任せていることです。

「セキュリティ対策を嫌でも理解できますし、周りもサポートするので組織全体のリテラシーの底上げにもつながります」と星野社長。

また、同社では自治体やNPOからの依頼でセキュリティ対策のセミナーを行う際、冒頭でIPAの「5分のできる! 情報セキュリティ自社診断」を実施しているそうです。「セミナー参加団体の中には10点台のところもあります。担当の方はショックを受けますが、現状を知ることによって『このままでは危ない』と気づきが得られるのです」と星野社長は語ります。

デジタル化で社会が便利になると同様、企業でも多くのメリットを享受できると星野社長。例えば DankSoft ではデジタル環境を整備したことで、社員の要望に応える柔軟な就労体制を敷くことができました。現在、26名の社員全員が全国各地で在宅ワークをして

現状を知ることによって「このままでは危ない」と気づきが得られる

おり、育児・介護と仕事を両立しているそうです。こうした働きやすい環境が評価され、「東京ライフ・ワーク・バランス認定企業」(2017年)などに選ばれているほか、取引先や金融機関からの信頼醸成にも役立っています。「とはいえ、国や警察が人々を守る実社会と違って、インターネットは危険と隣り合わせです。デジタル技術が浸透すればするほど、セキュリティを表裏一体で高めないとはいけません。それは企業にとって経営の根幹に関わるテーマであることを、特に中小企業の経営者は認識すべきです」と星野社長。同社は今後も各地でセキュリティ対策セミナーを行うほか、脆弱性対策や多要素認証など自社の対策をさらに強化し、SECURITY ACTIONの2つ星の宣言も取り組むとしています。

また、同社では「インターネットにより良いものをのせていく^{*}」をテーマに掲げています。この言葉には、安心や安全、快適さを追求する目的にインターネットを使いたい、それも多くの企業で協調していきたい——そんな星野社長の強い思いが表れています。このテーマを実現するためにも、経営者は若い世代を頼りにしてほしいと星野社長。「若者はデジタルリテラシーが高いので、彼らの能力を最大限に生かすためにも、経営者は彼らから学ぶ感覚でデジタルデバインドを解消してみても。できることからステップを踏んでいきましょう。明るい未来が待っています」

最後に、鈴木さんはこうエールを送ります。「セキュリティは家の戸締まりと同じで、普段から気をつけることが重要です。中小企業はSECURITY ACTIONの宣言後も、中小企業情報セキュリティガイドラインなどで対策を高度化しましょう」

^{*} https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf



標的に「例外」はない！ 中小企業を狙うサイバー攻撃

企業や組織を狙うサイバー攻撃。
業種や事業規模を問わず、どの中小企業でも
その標的になるリスクがあります。

調査対象企業数：1,117社
調査期間：2020年10月～2020年12月

令和2年度中小企業サイバーセキュリティ対策支援体制構築事業 成果報告書(全体版)
https://www.ipa.go.jp/security/fy2020/reports/sme/otasuketai_houkoku.html

FACT 1

社内システムへの侵入などを
試みる不審なアクセスを
検知した件数

18万1,536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

FACT 3

サイバー攻撃による
想定被害額が

5,000万円

を超える案件も確認

2021年度 中小企業における情報セキュリティ対策に関する実態調査(事例集)
<https://www.ipa.go.jp/files/000098149.pdf>

CASE 1

東京都 建設業
従業員数：21～50名

標的型攻撃メールによる被害を受けた。初動対応できたが、取引先にも同様のメールをばらまくことになってしまった。

CASE 2

東京都 卸売業・小売業
従業員数：101～300名

メールアドレスとパスワードの漏えい被害に遭った。漏えいしたメールアドレスから取引先に向け大量のメールが送りつけられ、メールが不通になる被害に発展した。

CASE 3

大阪府 卸売業・小売業
従業員数：5名以下

自社のECサイトに不正アクセスの痕跡があり、対処のため1週間程度一部の機能が制限され、利益にマイナスが生じた。

近年、企業や組織を狙ったサイバー攻撃が激化し、その手口も多様化しています。IPAが2020年に行った実態調査では、中小企業約1,100社で18万件以上の不審なアクセスを確認しました。業種や事業規模にかかわらず、どの企業も攻撃

の対象となるリスクがあります。また、サイバー攻撃によって多大な金銭的損失や、顧客・取引先への二次被害に発展するケースも珍しくありません。サイバーリスクを自分ごととして捉え、できる対策からしっかり行っていくことが重要です。

顧客や取引先を攻撃の被害から守るためにも
自社のセキュリティ対策強化を！

セキュリティのすゝめ

10

Theme

取引先や経営層を装う詐欺の手口と対策

国内外で被害が多発。億単位の損害の事例も…

巧妙な手口に注意！ 「ビジネスメール詐欺」

❗ 攻撃者は入念に準備して なりすましている

ビジネスメール詐欺(Business E-mail Compromise:BEC)とは、攻撃者が偽の電子メールを企業・組織に送りつけて従業員をだまし、攻撃者の用意した口座へ送金させる詐欺の手口です。パターンは2種に大別できます。

ひとつは、攻撃者が取引先になりすまして口座情報を差し替えた偽の請求書を送りつけ、振り込みをさせようとするもの。海外の企業と取引引きしている企業で多く見られます。

もうひとつは、攻撃者が企業の経営者や幹部になりすまして従業員にメールを送り、攻撃者が用意した口座へ送金させるものです。

財務・経理部門の担当者に対して、「秘密の案件で相談がある」などと経営層からの問い合わせを装う手口が確認されています。

どのパターンも、いかにも本人(取引

先や経営者等)のようになりすます巧妙さが特徴です。特に取引先へのなりすましは、攻撃者が正規メールのやりとりを事前に盗み見て、取引や請求に関する情報を入手している可能性があります。

被害を受ける企業・組織が後を絶たず、中には巨額の損失を被った事例もあります。国内では、取引先関係者を騙った人物から仕入れ代金の送金を促すメールを受け取った日用品販売会社が約1億円を払い込んだほか、電子機器メーカーの海外子会社が虚偽の送金指示に騙されて約5億円を流出させています。

海外では、韓国の航空関連企業が、取引先担当者になりすました攻撃者から送付された口座変更の偽メールに従い、約16億ウォンを送金した事例が報告されています。米国では、自治体が消防車の販売担当者を騙った攻撃者に約120万ドルを送金した例があります(後に資金が発見され返還)。

❗ 偽口座へ送金してしまったら すぐ銀行や警察に連絡

まずは従業員にこうした詐欺の手口があることを認識してもらうこと。その上で、以下の対策が望めます。

① **普段と異なるメールに注意する**：いつもと違う言い回しや表現の誤りがあれば要注意。不審なメールは社内情報共有することも重要です。

② **電信送金に関する社内規程の整備**：振込先や決済手段の急な変更が発生したら、電話やFAXなどメール以外の方法で取引先へ確認しましょう。複数の担当者によるチェック、電子署名付きメールの活用も有効です。

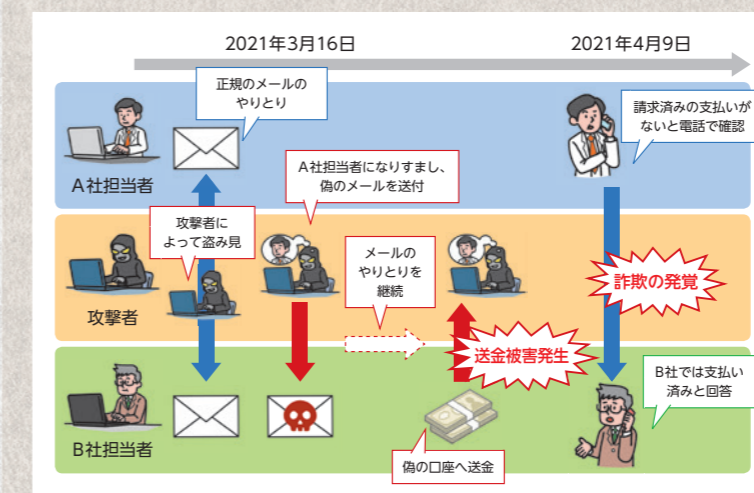
③ **ウイルス・不正アクセス対策**：メールを盗み見られないよう、基本の対策を万全に。セキュリティソフトを導入して最新の状態にする、メールアカウントに複雑なパスワードを設定する、メールシステムでの多要素認証、アクセス制限の導入などがあります。

偽の口座へ送金してしまったら、早急に銀行や警察に連絡しましょう。その際、攻撃者のメールやログなどを提出できれば状況の把握に役立ちます。

+ 対策のポイント +

- 1 こうした詐欺があることを従業員が認識する。
- 2 普段と違う言い回しや表現の誤りがあれば注意。
- 3 振込先等の急な変更は、電話などで取引先に確認。
- 4 ウイルス・不正アクセス対策の基本を徹底する。

攻撃のイメージ図



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

地域のDXプロジェクトを支援する「地域DX推進ラボ」が始動

「地域DX推進ラボ」は、地域の課題解決や競争優位性の確立に資するDXの取り組みを選定・支援する事業です。デジタルの活用で地域の社会課題解決や地域格差の是正を目指す「デジタル田園都市国家構想」の政策のひとつで、本事業では、各地域の公的機関、企業、学校、市民などによって構成される組合・団体等からそれぞれの地域で目指すDXのプロジェクトを募集しています。

地域DX推進ラボとして選定された地域は、プロジェクトの実現・発展に向けたメンター派遣や、他地域との交流・ビジネスマッチングの機会提供などの支援を受けることができます。第一弾選定地域は2023年3月に発表予定です。



<https://www.ipa.go.jp/kc/dx-local.html>

●「地域DX推進ラボ」公募要領

公募期間	2022年11月30日(水)～ (第一弾は2023年2月3日(金)までに応募された地域から選定)
募集対象	各地域の公的機関、企業、学校、市民等によって構成される組合・団体等(自治体の参加を必須とする)
応募手順	地域DX推進ラボウェブページから応募書類をダウンロードし、「実施計画書」「実施体制」を提出
審査手順	審査対象組織が属する地域を管轄する経済産業局と連携して書類による一次審査を行った後、申請者へのヒアリングを実施し、経済産業省とIPAが選定地域を決定します

●「地域DX推進ラボ」に選定された地域が受けられる支援

- 「地域DX推進ラボ」マークの使用権付与
- ポータルサイト、ラポイベント等による広報
- 地域のプロジェクト・企業等の実現・発展に資するメンターの派遣
- 他地域との交流機会の創出
- 中堅・中小企業等のDX優良事例を紹介する「DXセレクション」への推薦資格付与

DX推進のための人材確保・育成の指針「デジタルスキル標準」を策定

経済産業省・IPAが策定した「デジタルスキル標準(DSS)」は、DX時代のすべてのビジネスパーソンが身につけるべきスキルを示す「DXリテラシー標準(DSS-L)」と、DXの取り組みをリードする専門人材の役割およびその役割に必要なスキルを示す「DX推進スキル標準(DSS-P)」の2つで構成しています。

後者は昨年12月に策定したもので、このスキル標準ではDX推進の中心的な役割を担う人材類型を5つに分類。類型ごとの「ロール(役割)」と、そのロールに求められるスキルを定義しています。

デジタルスキル標準は、特定の産業や職種によらない共通的な指標として、個人の学び直しや企業における人材の育成・確保に活用いただけます。



<https://www.ipa.go.jp/jinzai/skill-standard/dss/>

●デジタルスキル標準の全体図

デジタルスキル標準

DXリテラシー標準

以下の指針と各指針において学習が期待される項目(学習項目例)を定義。
 ●DXに関するリテラシーとして身につけるべき知識の学習の指針
 ●個人が自身の行動を振り返るための指針および組織・企業が構成員に求める意識・姿勢・行動を検討する指針

DX推進スキル標準

DX推進に必要な5つの「人材類型」(ビジネスアーキテクト、デザイナー、データサイエンティスト、ソフトウェアエンジニア、サイバーセキュリティ)および類型ごとのロール、そのロールに求められるスキルを定義。

情報処理安全確保支援士試験などの出題構成等を変更

DXの進展などによってセキュリティ人材やIT人材に求められる役割の重要性と多様性が高まっていることを受け、IPAでは、「情報処理安全確保支援士試験(SC)」と「エンベデッドシステムスペシャリスト試験(ES)」の午後試験等を変更しました。

SCでは、セキュリティ人材の育成・確保の加速を目的に、これまで二分していた午後試験を統合。試験時間を60分短縮し、受験者の時間的な負担を軽減します。ESでは、これまで他の高度試験区分で出題していた組込みシステム分野の上流工程の要素を同試験に集約。技術面に加えてビジネスの視点でIoTソリューションを設計・開発するスキルを評価します。これらの変更は、2023年10月の試験から適用されます。



https://www.jitec.ipa.go.jp/1_00topic/topic_20221220.html

●試験の概要

情報処理安全確保支援士試験(SC)
 サイバーセキュリティに関する高度な知識・技能を問う試験。合格者は所定の登録手続きによって国家資格「情報処理安全確保支援士(登録セキスベ)」の資格保持者になることができます。
エンベデッドシステムスペシャリスト試験(ES)
 IoTを含む組込みシステムに関する高度な知識・技能を問う試験。あらゆるモノがつながるIoT時代に欠かせない組込みエンジニアに求められる専門的なスキルを評価します。

情報処理安全確保支援士試験の変更内容

【変更前】	午前 I	午前 II	午後 I	午後 II
試験時間	50分	40分	90分	120分
出題形式	多肢選択式(四肢択一)	多肢選択式(四肢択一)	記述式	記述式
出題数	30問	25問	3問	2問
解答数	30問	25問	2問	1問
配点(合計)	3.4点/問(100点)*	4点/問(100点)	50点/問(100点)	100点/問(100点)

【変更後】	午前 I	午前 II	午後
試験時間	50分	40分	150分
出題形式	多肢選択式(四肢択一)	多肢選択式(四肢択一)	記述式
出題数	30問	25問	4問
解答数	30問	25問	2問
配点(合計)	3.4点/問(100点)*	4点/問(100点)	50点/問(100点)

*午前 I 試験の得点の上限は100点とする。

Just Information

第18回IPA「ひろげよう情報モラル・セキュリティコンクール」2022受賞作品発表！

「ひろげよう情報モラル・セキュリティコンクール」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小中高生・高専生から募集し、表彰するものです。今年度は4コマ漫画、標語、ポスターなど全国から計6万1,962点の作品が集まりました。今回は、偽のセキュリティ警告から有償サポートなどに誘導するだましの手口(サポート詐欺)への注意を呼びかける作品のほか、インターネット上のコミュニケーションにおける相手への気づかひや、情報の真偽を判断することの大切さを伝える作品が最優秀作品に選ばれました。

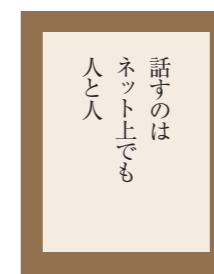
最優秀賞

【4コマ漫画部門】



「それは買」
 沖縄県 沖縄市立沖繩東中学校 2年
 安慶田 ひよりさん

【標語部門】



「話すのはネット上でも人々」
 北海道 北海道帯広柏葉高等学校 2年
 小沼 裕詞郎さん

【ポスター部門】



「情報はまず、分別から。」
 青森県 弘前大学教育学部附属中学校 2年
 橋本 和香さん



そのほかの受賞作品はこちらからご覧いただけます。 <https://www.ipa.go.jp/security/event/hyogo/>



令和5年10月から
消費税インボイス制度が始まります。

消費税
インボイス
制度

登録を予定されている事業者の方へ
登録申請はお早めに!

※制度開始時にインボイス発行事業者となるためには、原則として、**令和5年3月31日までに**登録申請を行う必要があります。

登録申請手続は、

かんたん・便利♪

e-Tax 
をご利用ください!!



「e-Taxソフト(WEB版)」を
ご利用いただくと、質問に回答
していくことで申請が可能です。



e-Taxで申請した場合、電子データ
で登録通知の受領が可能です。



個人事業者の方はスマートフォン
からでもe-Taxで申請できます。

※e-Taxのご利用には事前にマイナンバーカードの取得が必要です。

説明会を開催中

税務署での説明会や
オンラインでの
説明会をご案内しております。

説明会ページへ



制度について詳しくお知りになりたい方は、
国税庁ホームページ(<https://www.nta.go.jp>)の
「インボイス制度特設サイト」をご覧ください。

特設サイトへ



特設サイトでは

- ① 制度の解説動画
- ② AIを活用したチャットボット
- ③ 軽減・インボイスコールセンター
などをご案内しております

IPAとは

独立行政法人情報処理推進機構(IPA)は、経済産業省所管の政策実施機関です。
IT社会の課題解決や産業の発展につながる指針を示し、情報セキュリティ対策・DXの普及促進や、
優れたIT人材を育成するための活動に取り組んでいます。

- 「IPA NEWS」定期送付のお申込み、送付先の変更、
送付停止は、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 spd-ipanews@ipa.go.jp



- 「IPA NEWS」アンケートはこちら

- 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。
誌面に掲載しているQRコードは、cookieによりアクセス状況、
簡易位置情報を取得します。制作の参考情報とするため、
これらを外部に公表することはありません。