IPA NEWS vol.66 5月号

「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 今、専門家が注目する“脅威”はこれだ！

情報セキュリティ10大脅威2024

- セキュリティのすゝめ 15〈不注意による情報漏えいへの対策〉
  うっかりミスによる情報漏えい
  4つの要因と効果的な対策
- IPAの最新情報をまとめてお届け！
  Hot & New Topics

SBテクノロジー株式会社
サービス統括
セキュリティ&テクノロジー本部
プリンシパル
セキュリティリサーチャー
辻伸弘さん（右）

IPA
セキュリティセンター
対処調整部
脆弱性対策グループ
主幹
篠塚耕一さん（左）

特集

今、専門家が注目する“脅威”はこれだ！

情報セキュリティ10大脅威2024

セキュリティインシデントが増加する中、IPAの発表した「情報セキュリティ10大脅威2024」が話題となっています。今回は組織向けの10大脅威に焦点を当て、上位3つの脅威の概要や傾向、対策について、IPA職員と選考メンバーが詳しく解説します。組織の経営者層やセキュリティ担当者のみならず、情報を扱う人なら知っておきたい内容です。

選考メンバーは200名以上。現場の実態や時代を反映

セキュリティ対策の普及・啓発を目的として、IPAが2006年から公開している「情報セキュリティ10大脅威」。「組織」「個人」別にランキング形式を採用してきましたが、今年1月公開の2024年版からは個人向けの順位を撤廃しました。IPAセキュリティセンター主幹の篠塚耕一さんは、「下位だから安心というわけでなく、いずれの脅威も警戒していただきたいと考え、個人向けは五十音順の表記としたのです」と説明します。組織・個人向けともに選考方法は、前年に発生したセキュリティ事故や攻撃の状況などを基にIPAが脅威候補を選定し、そこからセキュリティ分野の研究者や企業の実務担当者などから成る10大脅威選考会で投票して決定します。開始当初約30名だった選考メンバーは年々拡大し、現在は200名以上。「それだけ多くの知見が反映され、現場の実態や時代の変化に即した投票結果になっているというわけです」と篠塚さん。

2016年から選考メンバーを務める、SBテクノロジー株式会社のプリンシパルセキュリティリサーチャー・辻伸弘さんは、投票に当たって「ニュートラルな判断」を心掛けているといいます。「インシデント動向や被害に遭った企業の対応など、リサーチデータの定量分析に加えて、危険性の評価が世間的に適切かどうかといった定性分析も行います。さらに、個人的に関心のある脅威はバイアス抜きに考えるなど、可能な限り客観的な視点で投票するよう努めています」

経営層が最新の脅威を知り、組織全体で対策を共有

2024年版の組織向け10大脅威は図表1の通りです。篠塚さんは、「前年と順位の変動はあるものの、顔ぶれは同じでした。特に1～3位の脅威は引き続き警戒が必要です」と指摘します。この上位3つの脅威について個別に見ていきましょう。

■ ランサムウェアによる被害

ランサムウェアとはコンピュータウイルスの一種で、パソコンやサーバーが感染するとデータが暗号化されます。攻撃者は復旧と引

図表1　情報セキュリティ10大脅威 2024「組織」向けの脅威の順位

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目

き換えに金銭要求の脅迫をするのです。「近年では攻撃者が暗号化の前に情報を窃取し、金銭を払わなければ『窃取した情報を公開する』『感染したことを関係者に連絡する』『DDoS攻撃でサーバーに負荷をかける』と脅すなど、多重脅迫もみられます。また、最近では窃取した情報の公開のみの脅迫も少し目立ってきています。ランサムウェアの感染により事業停止や取引先からの信用失墜を招くことも少なくありません」と辻さんはいいます。

メールの添付ファイルや本文中のリンクを開くことで感染するケースのほか、OSやアプリケーションの脆弱性を悪用したり、認証を突破することで不正にアクセスするなどして感染させる手口も確認されています。「金銭目当ての攻撃者が増えており、ウイルス開発、脆弱性の探索、脅迫の実行など分業化・専業化が進み、攻撃者の裾野が広がっていると感じます。“運が悪ければ被害に遭う”というより、隙があると“いつかは被害に遭う順番が回ってくる”というくらい、いまやこの脅威は誰にとっても無縁ではないと考えたほうがいいでしょう」と辻さん。実際、被害に遭う企業・団体等の過半数を中小企業が占めるなど、規模に関係なく、誰もが攻撃を受ける可能性があります（図表2）。

対策としては、不審なメールはできるだけユーザーに届かないようにフィルタをかけ、届いてしまったり開いてしまったりしても遮断、ないしは早期に検知するしくみを導入する。そして、脆弱性の対応も怠らず、有事に備えた適切なバックアップ運用、インシデント対応計画の策定を行うなどが挙げられます。

■ サプライチェーンの弱点を悪用した攻撃

辻さんによると、攻撃の対象となるサプライチェーン（SC）は、①開発会社の環境が汚染されソフトウェアにウイルスなどが仕込まれる「ソフトウェアSC」、②ネットワーク監視事業者を踏み台に、その顧客が被害に遭うなどの「サービスSC」、③子会社や海外支社などを踏み台に、関連会社が被害に遭うといった「ビジネスSC」等があります。

攻撃を受けた場合、情報漏えいや信用失墜といった被害が生じるだけでなく、自組織が足掛かりとなって取引相手に損害を与える可能性もあります。その結果、取引停止や損害賠償請求といった事態にまで発展することもあるのです。「最近ではユーザーや開発者など個人を介して、無関係のSCが連鎖的に被害に遭う事例もあり、いっそうの注意が必要です」と辻さん。また、ニューノーマルで働き方が多様化し、組織の管理が行き届きにくくなったこともリスク拡大の一因といえるでしょう。「情報管理の徹底、信頼できる取引先・サービスの選定、ソフトウェアやネットワークの脆弱性の確認といった対策を講じつつ、被害に遭った場合の対応をあらかじめ策定しておくことをお勧めします」

いまやランサムウェア攻撃と無縁ではいられない時代

■ 内部不正による情報漏えい等の被害

従業員や退職者など組織の関係者が機密情報を持ち出すほか、自宅など社外で作業するために情報を持ち出して漏えいさせるといったケースがこれに当たります。

「内部不正をする人は、①バレると思っていない、②不正が悪いことだと思っていない、③死なばもろともと考えている、という3タイプに分かれます。③はさておき、①と②は抑止できるはずです。不正の『動機』『機会』『正当化』という3要件をなくすため、情報管理ポリシーの作成や内部不正者への懲戒規定の整備を進めることが肝心です」と辻さん。具体的には、アクセスログの取得、ファイル持ち出し制御ソフトの導入、情報モラルを高める従業員教育などが考えられます。「従業員がスマートフォンを充電するために会社のパソコンにつないだら、情報システム部門か

ら『何かしましたか』と連絡するのも一手です。充電は不正ではありませんが、システムが監視下にあることをそれとなく知らせ、不正の抑止力とするわけです」

また、ランクインこそしていませんが、今後注目されるのが「生成AIを活用した脅威」です。「AIでIT部門の社員の声色を生成し、認証情報を聞き出して内部に入り込んできたという事例もあります。機密情報や金銭に関係する電話は相手が本人かどうか確認するよう、しっかりとしたフローをつくり、それに則って電話をかけ直したり同席者に代わってもらうなどして確認しましょう。同時に、そうした確認をいとわず、当たり前とする風土づくりも必要です。そのためにも経営層が最新の脅威を知り、対策を指揮してほしいと思います」

できることから素早く、着実に取り組むことが大切

「いずれの脅威にも共通するのは、“基本の対策”が重要ということ」と辻さんは強調します。まずは組織の情報資産の把握から始めましょう。使用しているOSやソフトウェアの種類やバージョンを確認し、インターネットに公開しているサービスについてはその必要性や管理・認証の妥当性を検証します。そこで運用上必要がないと判断されるものであれば、停止。必要であれば必要なアクセス元に制限をするなどを検討しましょう。「情報セキュリティは情報管理という土台の上に成り立つもの。外部から自社の状況を眺めて、どこに脆弱性があるか、攻撃者ならばどこを狙うかを洗い出し、そこを補強することが第一です」と辻さん。事業継続に必要な情報を絞り込み、それがどんな脅威にさらされているかを明らかにすることで、必要な対策がみえてくるというわけです。

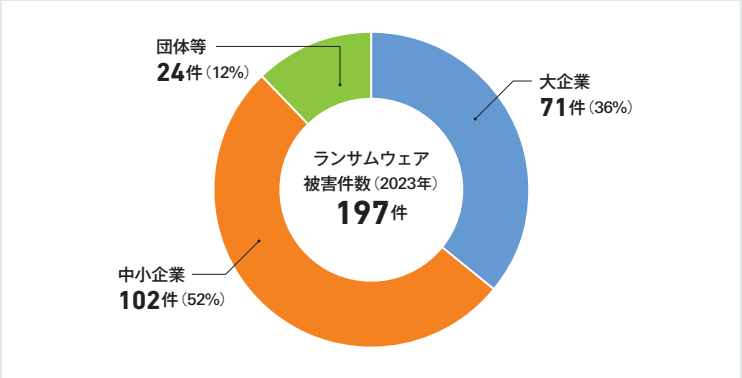
こうした作業を自社で行うのが難しい場合はベンダーの活用も一案ですが、丸投げはNG。「自分たちの資産は自分たちの責任で守る、そのためにベンダーの手を借りるのだという主体性を持った姿勢が重要です」

情報管理の土台を整えたら、セキュリティ対策の基本を徹底しましょう。繰り返しになりますが、セキュリティ対策の基本とは、不審なメールはできるだけユーザーに届かないようにフィルタをかける、届いてしまったり開いてしまったりしても遮断、ないしは早期に検知するしくみを導入する、そして有事に備えた適切なバックアップ運用やインシデント対応計画の策定を行うなどです。脅威の数だけ対処すると手間もコストもかさみます。まずは自分たちが守りたいものはどこにある何かを明確にしてください。そうすれば、その守りたいものがどういった経路の脅威にさらされているかがわかり、効率的かつ有効な対策が何かが見えてくるはずです。「セキュリティは『複雑』『お金ばかりかかる』などと敬遠されがちですが、脅威のしくみを知れば打つべき手が見えてきます。そこで必ずしも大金を投じる必要はありません。できることから素早く、着実に取り組むことが何より大切です」と辻さんは説きます。

また、篠塚さんは「組織・個人の別や順位にとらわれず、自社の立場や環境を踏まえて優先度を付け、対応してほしい」と注意を促します。10大脅威の解説書には、脅威の概要や事例、対策が盛り込まれており、ぜひ一読してほしいと篠塚さん。「企業研修はもちろん、学校での情報教育でも役立つ内容ですので、さまざまなシーンで活用いただければと思います」

基本の対策を徹底することで、攻撃に対するバリア強化を図る！

図表2　ランサムウェア被害の企業・団体等の規模別報告件数



※図中の割合は小数点第1位以下を四捨五入しているため、総計が必ずしも100にならない。
出典：警察庁「令和5年におけるサイバー空間をめぐる脅威の情勢等について」（2024年3月14日）

● **情報セキュリティ10大脅威 2024「個人」向けの脅威を解説したウェブ限定記事はこちら**
https://www.ipa.go.jp/about/ipanews/ipanews202405.html#specialissue_weblimited
● **情報セキュリティ10大脅威 2024「解説書」はこちら**
https://www.ipa.go.jp/security/10threats/nq6ept000000g22h-att/kaisetsu_2024.pdf

怖いのは外部からのサイバー攻撃だけではない！

うっかりミスによる情報漏えい 4つの要因と効果的な対策

社会的信用の失墜や巨額損失のリスクも

情報セキュリティの脅威の多くは外部の攻撃者によるものですが、従業員や業務委託先など身内のミスが起点となることもあります。いわゆる「不注意による情報漏えい」で、「情報セキュリティ10大脅威2024（以下、10大脅威）」組織編では6位となっています。今年の10大脅威の解説書で示す事例に合わせて不注意による情報漏えいの原因3つを解説します。

①メールの誤送信……アドレスの打ち間違い、BCCに入れるべきアドレスをCCに入れてしまう、添付するファイルを間違えるなど、意図しない相手へ情報を送ってしまう。

②機密情報が保存された媒体の紛失……機密情報が保存されたUSBメモリやパソコン、社用スマホ、紙媒体などを社外に持ち出し、紛失してしまう。

③設定ミスによる情報漏えい……ウェブサービスを立ち上げたときの設定ミスで、ユーザーの個人情報が誰でも見られるようになってしまう。

こうしたうっかりミスが顧客やユーザーの不信を買い、売上減少や取引停止といった事態になることがあります。従業員が対応に追われることで事業停止や人件費増大のリスクも生じます。また、漏えいした個人情報が標的型攻撃やだましの手口に悪用されて二次被害を引き起こすこともあり、情報管理の甘さが社会的信用の失墜や事業停止につながることも懸念されます。

対策の第一歩はセキュリティ規程の整備

不注意による情報漏えいの要因としては、次の4つが挙げられます。

①組織規定および情報を取り扱うプロセスの不備……機密情報を外部に持ち出してはいけないとルールで定めていない。持ち出しを許す場合、その際の確認手順や作業時の確認手順が整備されていない。

②情報を扱う人の情報リテラシーが低い……組織のルールが定められていても、従業員の情報リテラシーが低く、ルールが守られていない。

③情報を扱う際の本人の状況……組織のルールが確立され、個人の情報リテラシーが高くても、体調不良や多忙といった状況次第で注意力が散漫になり、漏えい事故を生んでしまう。

④不注意を想定した悪意ある第三者の存在……メールの誤送信を想定して偽のメールアドレス（ドッペルゲンガードメイン）を準備したり、新規ウェブサービスの設定不備を突いたりと、情報詐取を図る第三者がいる。

これらを踏まえ、セキュリティ対策を徹底することが重要です。「中小企業の情報セキュリティ対策ガイドライン」も参考に、左図のようなセキュリティ規程の整備から始めましょう。

情報セキュリティ関連規程（サンプル）の概要

	名称	ルールの概要・対象
1	組織的対策	情報セキュリティのための管理体制の構築や点検、情報共有など。
2	人的対策	取締役および従業員の責務や教育、人材育成など。
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。
4	アクセス制御および認証	情報資産に対するアクセス制御方針や認証。
5	物理的対策	セキュリティを保つべきオフィス、部屋および施設などの領域設定や領域内での注意事項など。
6	IT機器利用	IT機器やソフトウェアの利用など。
7	IT基盤運用管理	サーバーやネットワークなどのITインフラ。
8	システム開発および保守	独自に開発および保守を行う情報システム。
9	委託管理	業務委託にあたっての選定や契約、評価。
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。
11	テレワークにおける対策	テレワークで使用する機器やネットワーク、勤務中の注意事項など。

※「中小企業の情報セキュリティ対策ガイドライン第3.1版」をもとに作成

＋ 対策のポイント ＋

1. 組織規定および情報を取り扱うプロセスの整備
2. 社内教育などで情報を扱う人のリテラシーを向上
3. 従業員の注意力を維持するため、負荷状況に配慮
4. 悪意ある第三者に隙を見せない体制をつくる

● 「不注意による情報漏えい等の被害」の事例と、より具体的な対策はこちら
https://www.ipa.go.jp/about/ipanews/ipanews202405.html#security_weblimited

● 「中小企業の情報セキュリティ対策ガイドライン第3.1版」はこちら
https://www.ipa.go.jp/security/guide/sme/about.html

IPAの最新情報をまとめてお届け！

Hot & New Topics

DXに向けた「デジタルスキル標準」活用術の連載を開始

「デジタルスキル標準」は、経済産業省・IPAが2022年に策定したDX人材の確保・育成のための指針です。本指標はDXに求められるスキルやマインド、専門性などを明文化したもので、企業・組織が目指すDXの形に合わせて必要な人材像やスキルなどを洗い出すことができます。

今回開始した連載では、DXの原動力となる人材をどのように育成しているかに着目し、DXの取り組みの経緯やデジタルスキル標準の活用術について各企業にインタビューした内容を公開しています。

各社のDXに向けた試行錯誤の施策や独自の教育プログラムなど、DX推進の参考となる情報を発信していますので、ぜひご覧ください。

https://dx.ipa.go.jp/

株式会社
イトーキ様

トヨタ自動車
株式会社様

内部不正の手口や対策を解説する動画コンテンツを公開

近年、雇用の流動化や国家間の技術情報の競争激化などにより、深刻な内部不正の事案が顕在化しています。転職時に前職の権限を悪用して機密情報を持ち出し、それを国外で利用しようとしたり、元の職場の部下からパスワードを聞き出し情報を不正に取得したりするケースも確認されており、手口が巧妙化、悪質化しています。

本動画は、内部不正の手口や不正を起こさせないポイントのほか、自社の経営者や管理部門だけでなく関連会社や国内外の委託先なども含め、組織全体で実施すべき内部不正対策について解説しています。内部不正対策強化にお役立てください。

https://youtu.be/YVBHBIf23gA

「DX実践手引書 ITシステム構築編」改訂版を公開

本書はDX推進に向けたITシステムの構築を支援するガイドで、DXを実現するための考え方やDXに求められるITシステム・技術要素群の全体像などを示しています。

今回の改訂版では、この全体像の中の「データ活用基盤」に着目し、DX実践のためのデータ活用に関する項目を拡充しました。

国や組織、分野を横断したデータ連携を可能にする空間「データスペース」と「AI」に関する解説を加え、後者ではDXの実現に向けてAIシステムが効果的に機能するための環境整備の観点から、AIのセキュリティ・セーフティへの課題や、注目されるAIの機能とその具体例などについて紹介しています。

https://www.ipa.go.jp/digital/dx/dx-tebikisyo.html

● **本書で示すAIシステムの課題、検討事項の例**

AIシステムのセキュリティ・セーフティ面の課題例

- 倫理
- アルゴリズム
- バイアス
- AIセキュリティマネジメント
- サプライチェーン攻撃・漏えい・改ざんリスク
- 学習データ改ざん・汚染
- 個人情報・営業秘密漏えい
- 偽情報、誤情報

AIシステムの検討事項例

- 性能
- 説明性
- コンプライアンス
- 倫理性

Just Information

AIの安全性評価手法の検討などを行うIPAの新組織
「AIセーフティ・インスティテュート」を設立

ごあいさつ

AIセーフティ・
インスティテュート 所長
村上明子

AIセーフティ・インスティテュート（AISI）の初代所長を拝命いたしました、村上明子でございます。このたび、損害保険ジャパン株式会社のCDaO（Chief Data Officer）との兼務で日本初のAISIでの実務に携わることとなりました。

AISIは10府省庁と5政府系機関からなる政府横断的な組織で、安全・安心で信頼できるAIの実現に向けて、AIの安全性の評価手法の検討や規制の在り方を検討するための組織です。

規制というとブレーキのイメージを持たれることが多いのですが、安心してアクセルを踏む（AIの利活用を推進する）ためには必要なものと考えています。私はこれまでのキャリアの中で、AIの一分野である自然言語処理の研究、その研究内容を実務に活かすためのAIソフトウェア開発およびDX支援、そして、現職では自社のDXをけん引する立場を経験してきました。これらの経験を活かして、AIの安全性の評価やリスクに対する規制の在り方を検討し、皆様が安心してAIを活用できる社会の実現に貢献してまいりたいと思います。

AIの安全性については国際的にも関心が高まっていることから、先行してAISIを設立した英国や米国をはじめ、諸外国の関係機関とも連携しながら日本がグローバルな議論をリードしていけるよう取り組んでまいります。

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5年度・問19】

住宅地に設置してある飲料の自動販売機に組み込まれた通信機器と，遠隔で自動販売機を監視しているコンピュータが，ネットワークを介してデータを送受信することによって在庫管理を実現するような仕組みがある。このように，機械同士がネットワークを介して互いに情報をやり取りすることによって，自律的に高度な制御や動作を行う仕組みはどれか。

ア　MOT　　**イ**　MRP　　**ウ**　M2M　　**エ**　O2O

問2　マネジメント系【令和5年度・問39】

運用中のソフトウェアの仕様書がないので，ソースコードを解析してプログラムの仕様書を作成した。この手法を何というか。

ア　コードレビュー　　**イ**　デザインレビュー
ウ　リバースエンジニアリング　　**エ**　リファクタリング

問3　テクノロジ系【令和5年度・問61】

IoTシステムなどの設計，構築及び運用に際しての基本原則とされ，システムの企画，設計段階から情報セキュリティを確保するための方策を何と呼ぶか。

ア　セキュアブート　　**イ**　セキュリティバイデザイン
ウ　ユニバーサルデザイン　　**エ**　リブート

正解：問1 ウ　問2 ウ　問3 イ

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。
デジタル基盤の構築・提供、デジタル人材の育成、
サイバーセキュリティ対策の普及促進などの事業に取り組んでいます。

● 「IPA NEWS」最新号の公開をお知らせするメール配信サービスをご提供しています。お申込み、配信先の変更・配信停止につきましてはウェブページをご覧ください。

IPAニュース　検索

https://www.ipa.go.jp/about/ipanews/index.html

● 「IPA NEWS」アンケートはこちら

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

VEGETABLE OIL INK
リサイクル適性Ⓐ この印刷物は、印刷用の紙へリサイクルできます。
R70 古紙パルプ配合率70%再生紙を使用

独立行政法人情報処理推進機構
〒113-6591 東京都文京区本駒込二丁目28番8号　文京グリーンコートセンターオフィス
URL●https://www.ipa.go.jp/