令和７年度第３回ＳＥＤＩＯユーザー会

中小企業の情報セキュリティ対策

IPAセキュリティプレゼンター
資格ソムリエ®・デジタル士業®
はやし総合支援事務所　代表　林雄次

講師略歴

【林雄次】1980年生まれ、東京都足立区出身。
筑波大学附属高校卒業後、社会福祉を志し、淑徳大学にて社会福祉を学び社会福祉士の資格を取得。

卒業後はＩＴを通じて多くの方に役立つべく、ＩＴ関連企業で１０００社以上の中小企業の業務改善に従事し、業務・システムに精通。副業として『はやし総合支援事務所』開業、兼業２年を経て独立。

社労士、中小企業診断士、行政書士、情報処理安全確保支援士等として企業向け支援を行いつつ、保有資格・検定は【660】を超え、「資格ソムリエ」「デジタル士業」として各メディアで活躍中。

全国社会保険労務士会連合会　情報セキュリティ部会委員
東京都社会保険労務士会　デジタル・ＩＴ化推進特別委員　広報委員
独立行政法人　情報処理推進機構（IPA）セキュリティプレゼンター
日本パラリンピック委員会　情報・科学スタッフ
経産省:認定情報処理推進機関、中小企業庁:認定経営革新等支援機関、デジタル庁:デジタル推進委員

著書：『かけ合わせとつながりで稼ぐ 資格のかけ算大全』（実務教育出版）
『ITストラテジスト 究極の合格ルール』（オーム社）
『社労士事務所のDXマニュアル』（中央経済社）
『行政書士・社労士・中小企業診断士 副業開業カタログ』（中央経済社）
『資格が教えてくれたこと　400の資格をもつ社労士がみつけた学び方・活かし方・選び方』（日本法令）他多数

保有資格

中小企業診断士、社会保険労務士、行政書士、社会福祉士、情報処理安全確保支援士、マンション管理士、管理業務主任者、宅地建物取引士、賃貸不動産経営管理士、キャリアコンサルタント、国内旅行業務取扱管理者、経営士、防災士、防災管理者、甲種防火管理者、相続診断士、統計調査士、システム監査技術者、ITストラテジスト、プロジェクトマネージャ、ITサービスマネージャ、情報セキュリティスペシャリスト、ネットワークスペシャリスト、データベーススペシャリスト、ソフトウェア開発技術者、基本情報技術者、情報セキュリティマネジメント、ITパスポート、初級システムアドミニストレータ、kintone認定 カイゼンマネジメントエキスパート、kintone認定 アプリデザインスペシャリスト、kintone認定 アソシエイト、.com Master ADVANCE、.com Master BASIC、パソコン整備士検定2級、パソコン整備士検定3級、コンピュータサービス技能評価試験 情報セキュリティ部門、DXアドバイザー検定 スペシャリスト、スマートフォン整備士検定3級、スマートフォン・モバイル実務検定、モバイル技術基礎検定、ワイヤレスIoTプランナー検定、G検定、AI検定、AI・IoT基礎検定、WEBライター検定3級、ドローン検定2級、ドローン検定3級、ドローン検定4級、インターネット ルール＆マナー検定、P検（ICTプロフィシエンシー検定）5級、パソコン能力評価試験パソコン・ネット操作部門4級、タイピング技能検定3級、タイピング技能検定4級、タイピング技能検定5級、タイピング技能検定6級、タイピング技能検定7級、タイピング技能検定8級、Microsoft Office Specialist Expert (Office 2019)、Microsoft Office Specialist Word 2019 Expert、Microsoft Office Specialist Excel 2019 Expert、Microsoft Office Specialist Associate (Office 2019)、Microsoft Office Specialist Word 2019、Microsoft Office Specialist Excel 2019、Microsoft Office Specialist PowerPoint 2019、健康経営アドバイザー、第一種衛生管理者、ビジネスマネジャー検定、ワークルール検定中級、ワークルール検定初級、人的資本経営検定BASIC、人事評価者検定初級、CSR検定4級、感染対策アドバイザー検定、緊急時避難誘導員、防災コンシェルジュ、eco検定、eco検SEEKER、CDA、心理相談員、メンタルヘルス・マネジメント検定Ⅱ種、メンタルヘルス・マネジメント検定Ⅲ種、メンタルケア心理士、メンタルケアカウンセラー、マスターケアストレスカウンセラー、青少年ケアストレスカウンセラー、高齢者ケアストレスカウンセラー、企業中間管理職ケアストレスカウンセラー、ケアストレスカウンセラー、こころ検定2級、こころ検定3級、こころ検定4級、心理カウンセリングスペシャリスト、メンタルヘルス・スペシャリスト、メンタルトレーニングスペシャリスト、キャリアカウンセリングスペシャリスト、コミュニケーションスキルスペシャリスト、マインドフルネスコンサルタント、アンガーバランスマネジメント、心理＆WEBカラーセラピスト、チャイルドコーチングマイスター、エニアコミュニケーション心理学アンバサダー、ナッジアドバイザー、ビジネスモデル鑑定士、販売士検定2級、販売士検定3級、統計検定3級、統計検定4級、マーケティング検定3級、実践マーケティング力検定3級、ネットマーケティング検定、SNSマーケティング検定、webマーケティングマスター、ブランド・マネージャー3級、ニーズマネジメント検定、プレゼンテーション検定準2級、プレゼンテーション検定3級、プレゼンテーション検定準3級、SNSリスクマネジメント検定、初級SNSエキスパート検定、クラファン検定、通販エキスパート検定2級、通販エキスパート検定3級、通販エキスパート検定カスタマー・セントリシティ、ファイナンシャル・プランナー（AFP）、ファイナンシャル・プランニング技能士2級、会計ソフト実務能力検定Ⅰ級、日商簿記検定2級、日商簿記検定3級、日商簿記検定初級、日商簿記検定原価計算初級、こどものお金先生検定3級、銀行業務検定CBT サステナブル経営サポート、銀行業務検定CBT DXサポート、生命保険協会一般課程、金融リテラシー検定、知的財産管理技能士2級、ビジネス実務法務検定2級、ビジネス実務法務検定3級、ビジネス実務与信管理検定3級、ビジネス著作権検定初級、ビジネスコンプライアンス検定、ビジネス事務検定、ビジネス文書検定2級、ビジネス文書検定3級、ビジネス・キャリア検定試験3級経営戦略スペシャリスト、ビジネス・キャリア検定試験3級マーケティングスペシャリスト、ビジネス・キャリア検定試験3級営業スペシャリスト、ビジネス・キャリア検定試験3級経営情報システムスペシャリスト、ビジネスメール実務検定3級、事務スペシャリスト、テレワーク検定、リモート実務検定3級、コンタクトセンター検定、在宅ワークスペシャリスト、QC検定4級、お客様対応専門員（CAP）、秘書検定2級、秘書検定3級、サービス接遇検定2級、サービス接遇検定3級、ホスピタリティ接遇検定、医療ホスピタリティ接遇検定、福祉ホスピタリティ接遇検定、おもてなし学検定Ⅰ級、おもてなし学検定2級、おもてなし学検定3級、ほめ達検定2級、ほめ達検定3級、営業力強化検定、判断力検定初級、人間力徳育検定中級、人間力徳育検定初級、社会人コンプライアンス検定、社会人ホスピタリティ検定［実践］、社会人ホスピタリティ検定［基本］、社会人常識マナー検定2級、社会人常識マナー検定3級、社会人常識マナー検定 Japan Basic、マナーインストラクター、マナー・プロトコール検定3級、実用マナー検定準3級、ビジネス実務マナー技能検定3級、ビジネスマナーWEB検定、ソーシャルマナー3級、和文化マナー検定3級、きもの文化検定4級、令和のマナー検定、就活マナーWEB検定、異性間コミュニケーションアンバサダー、人間関係のストレス解消検定、礼法道アンバサダー、コミュニケーション検定初級、ハラスメントWEB検定、ニュース時事能力検定2級、ニュース時事能力検定準2級、ニュース時事能力検定3級、ニュース時事能力検定4級、日本語検定2級、日本語検定3級、日本語検定4級、日本漢字能力検定3級、日本漢字能力検定4級、日本漢字能力検定5級、四字熟語検定Ⅰ級、四字熟語検定準Ⅰ級、四字熟語検定2級、四字熟語検定3級、四字熟語検定4級、敬語力検定準Ⅰ級、敬語力検定2級、敬語力検定3級、敬語力検定4級、略語検定Ⅰ級、略語検定準Ⅰ級、略語検定2級、略語検定3級、ことわざ検定4級、ことわざ検定5級、英検3級、英検4級、みんなの外国語検定ブロンズ、理科検定3級、理科検定4級、理科検定5級、賃貸不動産メンテナンス主任者、普通自動車第一種運転免許、原動機付自転車免許、安全運転能力検定3級、安全運転能力検定4級、乙種1類危険物取扱者、乙種2類危険物取扱者、乙種3類危険物取扱者、乙種4類危険物取扱者、乙種5類危険物取扱者、乙種6類危険物取扱者、丙種危険物取扱者、第二級陸上特殊無線技士、第三級陸上特殊無線技士、第二級海上特殊無線技士、第三級海上特殊無線技士、第三級アマチュア無線技士、第四級アマチュア無線技士、測量士補、潜水士、PADIアドバンスオープンウォーターダイバー、PADIディープダイバー、PADIオープンウォーターダイバー、PADIドルフィンスキンダイバー、PADI AWAREサンゴ礁の保護、PADIデジタルアンダーウォーターフォトグラファー、サービス介助士、防災介助士、認知症介助士、スマート介護士初級、終活ガイド2級、終活ガイド3級、終活ライフコーディネーター、ジェロントロジー・マイスター、ジェロントロジー検定、ウェルエイジングBasic、福祉住環境コーディネーター2級、福祉住環境コーディネーター3級、健康介護コンシェルジュ、共生社会コミュニケーション検定、ケア・コミュニケーション検定、ユニバーサルマナー検定3級、おひとりさま検定、キッズコーチ検定3級、予防医療検定、予防医療アンバサダー、上級救命技能、スポーツ医学検定2級、スポーツ医学検定3級、スポーツ医学検定初級、ピンクリボン検定入門コース、グリーンリボン検定、リンパケア検定2級、口腔ケアアンバサダー、歯みがき検定マイスター、歯みがき検定Ⅰ級、歯みがき検定2級、歯みがき検定3級、メディカルハーブ検定、メディカルハーブコーディネーター、ハーブ＆ライフコーディネーター、ハーブ＆ライフ検定、アロマ＆ケアスペシャリスト、アロマテラピー検定Ⅰ級、アロマテラピー検定2級、環境カオリスタ検定、ナチュラルビューティスタイリスト検定、スローライフマイスター検定、ラジオ体操指導員、日本健康マスター検定エキスパート、日本健康マスター検定ベーシック、健康管理検定2級、健康管理検定3級、空気環境アドバイザー、食生活アドバイザー3級、食育栄養コンサルタント、食育イノベーター、食品衛生責任者、食品表示検定試験初級、食育フードテック検定、食の検定3級、食の検定4級、良食検定、イートライトサポーター、栄養検定3級、栄養検定4級、薬膳漢方マイスター、薬膳・漢方検定、漢方マニア検定、アレルギースペシャリスト、腸活腸育ライフアンバサダー、温活検定3級、入浴検定、高齢者入浴アドバイザー、睡眠健康指導士、睡眠検定Ⅰ級、睡眠検定2級、睡眠検定3級、睡眠検定入門、睡眠コンサルタント、ダイエット検定Ⅰ級、ダイエット検定2級、筋肉のこと知ってますか検定3級、筋トレスペシャリスト、整体＆セラピースペシャリスト、骨格診断アドバイザー検定3級、姿勢診断士5級、色彩検定2級、色彩検定3級、色彩検定UC級、色彩士検定4級、カラーマスターデジタル検定ゴールドクラス、パーソナルカラー実務検定3級、美術検定4級、日本化粧品検定3級、化粧品成分検定3級、コスメマイスター、コスメマイスター・ライト、スキンケアマイスター、スキンケアスペシャリスト、メンズメイク検定3級、整理収納アドバイザー2級、デジタル整理アドバイザー2級、ライフオーガナイザー2級、片付け収納スペシャリスト、クリンネスト3級、お掃除プロフェッショナル、掃除能力検定2級、掃除能力検定3級、掃除能力検定4級、掃除能力検定5級、洗濯検定上級、洗濯検定中級、洗濯検定初級、ガーデニングコンシェルジュ、うつわ検定ホームユースうつわマスター、箸ソムリエベーシック、レザーソムリエBasic、靴磨き知識検定、スニーカー検定3級、ふろしき＆手ぬぐいマスター検定、道化文字☆モジスト、ペット看護＆セラピーエキスパート、生物分類技能検定4級、いぬ検定初級、ねこ検定初級、サウナ・スパプロフェッショナル、サウナ・スパ健康アドバイザー、サウナエキスパート、サウナ・スパ健康士、ウィスキング for ビギナーズ、温泉健康指導士、温泉ソムリエマスター、温泉ソムリエ、銭湯検定4級、日本の宿おもてなし検定2級、日本の宿おもてなし検定3級、山の知識WEB検定ゴールドコース、山の知識WEB検定シルバーコース、山の知識WEB検定ブロンズコース、初級バーベキューインストラクター、晴れ男・晴れ女検定、日本城郭検定オンライン入門級、夜景観光士検定3級、世界遺産検定2級、世界遺産検定3級、世界遺産検定4級、無人島サバイバル検定、船の文化検定初級、文化浴入門検定、全国道の駅検定、東京シティガイド検定、東商ねりマニア検定上級、東商ねりマニア検定初級、名古屋観光検定上級、名古屋観光検定初級、京都検定3級、福岡検定初級、軽井沢WEB検定3級、検定「お伊勢さん」初級、エイサー検定Ⅰ級、エイサー検定2級、エイサー検定3級、渋沢栄一検定初級、土方歳三・箱館戦争検定、ハワイスペシャリスト検定中級、ハワイスペシャリスト検定初級、J.S.A.ワインエキスパート、J.S.A.ワイン検定シルバークラス、J.S.A.ワイン検定ブロンズクラス、J.S.A.SAKE検定、ANSAソムリエ、ワイン品質鑑定士、ワインマイスター、ワイン検定3級、ワイン検定4級、ワイン検定5級、ワインナビゲーター、オーガニックワインアンバサダー、モルドバ アグリ＆ラダチーニ ワインマスター、日本酒スペシャリスト、日本酒検定3級、日本酒検定4級、日本酒検定5級、日本酒ナビゲーター、焼酎検定3級、焼酎検定4級、焼酎検定5級、ウイスキー検定2級、ウイスキー検定3級、カクテル検定3級、カクテルマイスター、日本ビール検定3級、日本茶検定Ⅰ級、日本茶検定2級、日本茶検定3級、日本茶スペシャリスト、茶道文化検定3級、茶道文化検定4級、紅茶アナリスト、紅茶検定初級、コーヒースペシャリスト、料飲サービス検定、スポーツフードスペシャリスト、機能性フード検定、介護食コンサルタント、発酵検定、さしすせそ調味料検定、料理検定2級、料理検定3級、菓子検定2級、菓子検定3級、家庭料理検定4級、家庭料理検定5級、野菜マエストロ検定（野菜アンバサダー）、野菜＆果物コンシェルジュ、チョコレート検定中級、チョコレート検定初級、プレチョコレート検定、チーズソムリエ、チーズ検定、すし検定、パンシェルジュ検定初級、カレーパン検定（カレーパンタジスタ）、日本ラーメン検定初級（ラーメニスト）、おにぎり検定（オニギリスト）、焼き鳥検定（焼き鳥アンバサダー）、唐揚検定（カラアゲニスト）、串カツ検定（串カツマイスター）、フライドポテト・アンバサダー検定シルバー、フライドポテト・アンバサダー検定ブロンズ、あんこ検定、タマリエ検定「一ツ星タマリエ」、レモン検定、さば検定、だしソムリエ初級、昆布検定、風水＆パワーストーンコンサルタント、パタゴティタン・マヨルム検定、実用技能しか犬定、謎解き能力検定7級、フォトマスター検定3級、学び直し＆独学アンバサダー検定、集中力検定、ゾーン検定、聖書検定3級、聖書検定4級、聖書検定5級、神社検定参級、神社検定初級、葬送儀礼マナー検定2級、仏教葬祭アドバイザー、日本仏教検定2級、日本仏教検定3級、僧侶（法名：釋覚論）

著書等

ブクログ：　https://booklog.jp/users/yujihys

情報セキュリティ10大脅威　2025

[組織編]

IPA Better Life with IT

「情報セキュリティ10大脅威」とは？

- 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
- TOP 10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

10大脅威の特徴

脅威に対して様々な立場の方が存在

立場ごとに注意すべき脅威も異なるはず

- 家庭等で PC やスマホを利用する人 「個人」

- 企業や政府機関等の組織
- 組織のシステム管理者や社員・職員 「組織」

「個人」と「組織」の２つの立場で脅威を解説

情報セキュリティ10大脅威 2025

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

情報セキュリティ10大脅威 2025

IPA

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃		年連続8回目
4	内部不正による情報漏えい等		回目
5	機密情報等を狙った標的		
6	リモートワーク等の環境や		
7	地政学的リスクに起因する		
8	分散型サービス妨害攻撃（DDoS		6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

自組織により強く関係する脅威から対策する
ことが重要

情報セキュリティ10大脅威 2026

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	ランサム攻撃による被害	2016年	11年連続11回目
2	サプライチェーンや委託先を狙った攻撃	2019年	8年連続8回目
3	AIの利用をめぐるサイバーリスク	2026年	初選出
4	システムの脆弱性を悪用した攻撃	2016年	6年連続9回目
5	機密情報を狙った標的型攻撃	2016年	11年連続11回目
6	地政学的リスクに起因するサイバー攻撃（情報戦を含む）	2025年	2年連続2回目
7	内部不正による情報漏えい等	2016年	11年連続11回目
8	リモートワーク等の環境や仕組みを狙った攻撃	2021年	6年連続6回目
9	DDoS攻撃（分散型サービス妨害攻撃）	2016年	2年連続7回目
10	ビジネスメール詐欺	2018年	9年連続9回目

情報セキュリティ対策の基本

- 多数の脅威があるが「攻撃の糸口」は似通っている
- 基本的な対策の重要性は長年変わらない
- 下記の**「情報セキュリティ対策の基本」を常に意識することが重要**

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消して脆弱性を悪用した攻撃によるリスクを低減する
マルウェアに感染	セキュリティソフトの利用	攻撃を検知してブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取による情報漏えい等のリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導(罠にはめる)	脅威・手口を知る	手口から重要視するべき対策を理解する

情報セキュリティ対策の基本＋α

- 昨今はクラウドサービスの利用も一般的になってきている
- クラウドサービスを利用を想定した＋α の対策を行い、備える必要がある

備える対象	情報セキュリティ対策の基本＋α	目的
クラウドの選定	選定前の事前調査	クラウドサービスのガイドラインに沿った運営をしている業者やそのサービスを選定する
インシデント全般	責任範囲の明確化(理解)	クラウドサービスを契約する際は、インシデント発生時に誰(どの組織)がどこまでインシデント対応する責任があるのかを明確化(理解)する
クラウドの停止	代替案の準備	業務が停止しないように代替策を準備する
クラウドの仕様変更	設定の見直し	更新情報は常に確認し、仕様変更により意図せず変更された設定を適切な設定に修正する(設定不備により発生する情報漏えいや攻撃を防止する)

「組織」向け脅威の解説

- ここからは脅威毎に解説します
- 組織により強く関係する脅威から確認しましょう
- **各脅威の対策の紹介では前項の「情報セキュリティ対策の基本」は実施していることを前提とし、記載には含めていません**

【1位】ランサム攻撃による被害

- ランサムウェアに感染させ、端末ロックや PC やサーバーのデータ窃取、暗号化を行い、業務継続困難な状態にする
- 攻撃者は複数の脅迫を組み合わせて、被害組織が金銭の支払いを検討せざるを得ない状況を作り出そうとする
- RaaS（Ransomware as a Service）という、サービスとして開発・提供されたランサムウェアによる攻撃もある
- ランサムウェアを用いない金銭要求を行う攻撃として、「ノーウェアランサム」による攻撃や、DDoS 攻撃を仕掛けると脅迫するランサムDDoS 攻撃も確認されている

【出典】 令和６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（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf

【1位】ランサム攻撃による被害

- **攻撃手口**

・ランサムウェアに感染させて金銭を要求

- **脆弱性を悪用しネットワークから感染させる**
  - ソフトウェアの脆弱性を悪用し
    PC やサーバーをランサムウェアに感染させる

- **不正アクセスによりネットワークから感染させる**
  - 意図せず公開されているポート(リモートデスクトップ等)を
    利用した不正アクセスからマルウェアに感染させる

【1位】ランサム攻撃による被害

IPA

- **攻撃手口**

・ランサムウェアに感染させて金銭を要求

- **Web サイトやメールから感染させる**
  - ランサムウェアをダウンロードさせるように Web サイトの脆弱性を悪用して改ざんし、閲覧した際に感染させる
  - 不正な添付ファイルを開かせて感染させる
  - 悪意のあるリンクをメール本文中に仕込み開くよう誘導し、感染させる

【1位】ランサム攻撃による被害

- **2024年の事例/傾向①**
  - **ランサムウェア感染による被害と二次被害**
    - 2024年6月、KADOKAWA が ランサムウェア攻撃を含む大規模なサイバー攻撃にあった
    - フィッシング攻撃等により従業員のアカウント情報が窃取され、社内ネットワークに侵入されたことが原因と推測
    - 複数のサービスが停止したほか、約25万4,000人分の個人情報や企業情報の漏えいが判明した
    - 攻撃組織が公開したとされる情報が、SNS 等を通じて拡散された

【出典】 ランサムウェア攻撃による情報漏洩に関するお知らせ（株式会社KADOKAWA）
https://group.kadokawa.co.jp/information/media-download/1356/d3f77b589c58d083/
漏洩情報の拡散行為に対する措置ならびに刑事告訴等について（株式会社KADOKAWA）
https://www.kadokawa.co.jp/topics/12010/

【1位】ランサム攻撃による被害

- **2024年の事例/傾向②**
  - **ノーウェアランサムによる攻撃事例**
    - 2024年10月、国立遺伝学研究所の生命情報・DDBJセンターがデータ窃取の脅迫を受けたと情報・システム研究機構が公表した
    - 国際ハッカー集団「CyberVolk」の犯行声明では、DDBJのデータ 5%を公開し、1万ドルを支払わなければ残り95%も公開するとSNS上で脅迫した。
    - 調査によってシステムへの不正侵入やデータ消失等は確認されず、窃取したとされるデータも公開データであった。

【出典】 国際塩基配列データベース「DDBJ」に対するサイバー脅迫に関するご報告（生命情報・DDBJセンター）
https://www.ddbj.nig.ac.jp/news/ja/2024-10-22

【1位】ランサム攻撃による被害

- **2024年の事例/傾向③**
  - **RaaS が利用された国内事例**
    - 2024年6月、ヒロケイが RaaS の一種である「Phobos」を用いた攻撃を受けていたことを公表
    - 原因は、サーバーの脆弱性および VPN ルーターの設定不備で、攻撃者がこれを悪用し社内ネットワークに侵入後、複数のサーバーに対してデータの暗号化を行った
    - この攻撃で、情報の漏えいや二次被害は確認されていない

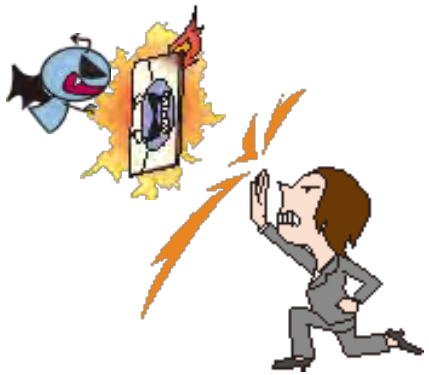
【出典】 弊社内ネットワークへの外部からの不正アクセス被害の発生について（第一報）（株式会社ヒロケイ）
https://www.hirokei.co.jp/news/646/
弊社内ネットワークへの外部からの不正アクセス被害の発生について（第二報）（株式会社ヒロケイ）
https://www.hirokei.co.jp/news/649/
弊社内ネットワークへの外部からの不正アクセス被害の発生について（第三報）（株式会社ヒロケイ）
https://www.hirokei.co.jp/news/668/

【1位】ランサム攻撃による被害

- **対策**
  - **組織(経営者層)**

【組織としての体制確立】

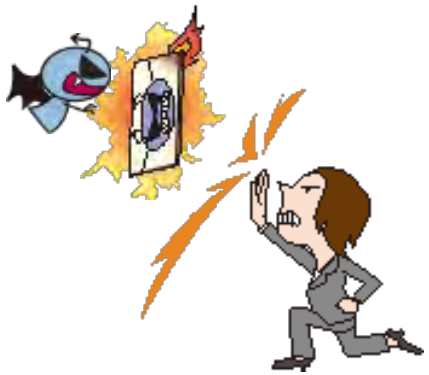
- インシデント対応体制を整備し、対応する
  - CISO を配置する
  - CSIRT を構築する
  - 報告フォーマットは決めておく
  - 有事の際の対応フローを確立、社員へ通知する
  - 対応フロー通りに実施できるか訓練をする
  - 外部の協力依頼先を用意する
  - 社内規則の整備や予算確保をする



【1位】ランサム攻撃による被害

- **対策**
  - **組織(システム管理者、従業員)**

【被害の予防／被害に備えた対策】



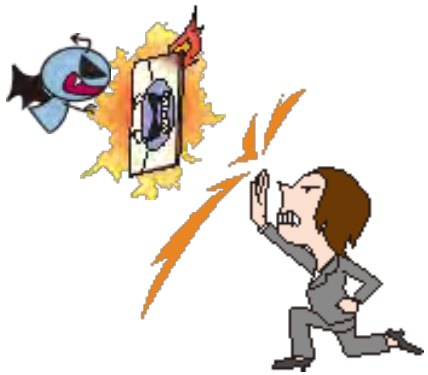
- インシデント対応体制を整備し、対応する
- 添付ファイル開封や、メールや SMS のリンク、URL のクリックを安易にしない
- 多要素認証の設定を有効にする
- 提供元が不明のソフトウェアを実行しない
- サーバーや PC、ネットワークに適切なセキュリティ対策を行う
- 共有サーバー等へのアクセス権の最小化と管理の強化
- 公開サーバーへの不正アクセス対策
- 適切なバックアップ運用(取得、保管、復旧訓練)を行う
  - バックアップ自体の暗号化対策として、WORM（Write Once Read Many）機能等も有効である。

【1位】ランサム攻撃による被害

- **対策**
  - **組織(システム管理者、従業員)**

【被害を受けた後の対応】

- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等
- インシデント対応体制を整備し、対応する
- 適切なバックアップ運用(復旧作業)を行う
- 復号ツール※1の活用



【出典】 ※1 The No More Ransom Project(No More Ransomプロジェクト)
https://www.nomoreransom.org/

【1位】ランサム攻撃による被害

- **身代金の支払いと復旧業者の選定について**
  - 原則、身代金を支払わずに復旧を行う
  - 支払いに応じてもデータの復元や情報の流出を防げるとは限らない
  - 対応を依頼した業者が攻撃者との裏取引で身代金を支払うことで復旧した場合、事実上、自組織が攻撃者に資金提供をしたとみなされるおそれもある
  - 対応を依頼する業者の選定※1にも注意が必要
  - データの復旧に関しては、復号ツールの活用についても検討すると良い

【出典】 ※1 データ被害時のベンダー選定チェックシート Ver.1.0(特定非営利活動法人デジタル・フォレンジック研究会)
https://digitalforensic.jp/home/act/products/higai-checksheet/

【2位】サプライチェーンや委託先を狙った攻撃

- 調達から販売、業務委託等一連の商流において、セキュリティ対策が甘い組織が攻撃の足掛かりとして攻撃される
- ソフトウェア開発のライフサイクルに関与するモノや人の繋がりである「ソフトウェアサプライチェーン」を悪用して攻撃される
- 取引先や業務を委託している外部組織から情報漏えいする

【2位】サプライチェーンや委託先を狙った攻撃

IPA

- **攻撃手口**

・取引先や委託先が保有する機密情報を狙う

- セキュリティが脆弱な取引先や委託先、国内外の子会社等を攻撃し、標的組織の機密情報を狙う

・ソフトウェア開発元や MSP※1 等を攻撃し、標的組織を攻撃するための足掛かりとする

- ソフトウェアやサービスを改ざんしてマルウェアを仕込み、インストールやサービス利用の際に顧客にマルウェアを感染させる等

※1 MSP（マネージドサービスプロバイダー／企業システムの運用・監視等を請け負う事業者）

【2位】サプライチェーンや委託先を狙った攻撃

- **2024年の事例/傾向①**
  - **業務委託先業者からの顧客情報漏えい**
    - 2024年5月、イセトーは VPN 経由の不正アクセスを受け、端末やサーバー等がランサムウェア攻撃を受けたと公表した
    - 2024年6月、攻撃者が窃取したとされる情報のダウンロード用 URL が攻撃者グループのリークサイトに掲載された
    - 自治体だけでも約 50 万件以上の個人情報が漏えいした
    - 業務委託元より損害賠償請求の予定も報告された

【出典】 不正アクセスによる個人情報漏えいに関するお詫びとご報告（株式会社イセトー）
https://www.iseto.co.jp/news/news_202410.html
報道発表資料「委託業者のランサムウェア被害に伴う個人情報漏えい事案」に係る市民への対応について（豊田市）
https://www.city.toyota.aichi.jp/pressrelease/1060027/1060257.html
印刷業務委託先のランサムウェア被害について（第3報）（徳島県）
https://www.pref.tokushima.lg.jp/ippannokata/kurashi/zeikin/7242743/
委託業者におけるコンピューターウイルス感染について（和歌山市）
https://www.city.wakayama.wakayama.jp/kurashi/zeikin/1001083/1058780.html
委託業者におけるコンピューターウイルス感染について（最終報）（愛媛県）
https://www.pref.ehime.jp/page/85357.html

【2位】サプライチェーンや委託先を狙った攻撃

- **2024年の事例/傾向②**
  - **委託先への攻撃に起因するサービス停止**
    - 2024年9月、関通はサイバー攻撃により、サーバーがランサムウェアに感染したことを公表した
    - 入出庫関連のシステムが停止し、生産・出荷業務の一部が一時停止となった
    - 影響を受けた業務委託元の多数の組織からも出荷の遅延や一時停止等も公表された
    - 原因は悪意のある第三者による不正アクセス
    - 個人情報の漏えいは確認されなかった

【出典】 【第1報】当社におけるサイバー攻撃によるシステムの停止事案発生のお知らせ（株式会社関通）
https://www.kantsu.com/news/6573/
【第3報】当社におけるサイバー攻撃によるシステムの停止事案発生のお知らせ（株式会社関通）
https://www.kantsu.com/news/6615/
個人情報漏洩の可能性に関する確報（株式会社関通）
https://www.kantsu.com/news/6628/

【2位】サプライチェーンや委託先を狙った攻撃

- **2024年の事例/傾向③**
  - **ソフトウェアサプライチェーンの悪用**
    - 2024年3月、Linux 環境で広く利用されている「XZ Utils」という可逆圧縮ツールに悪意のあるコードが仕込まれたことが確認された
    - この悪意あるコードは共同開発者によって挿入された
    - 特定の条件下でリモートからシステム全体へ不正アクセスできるおそれがあった

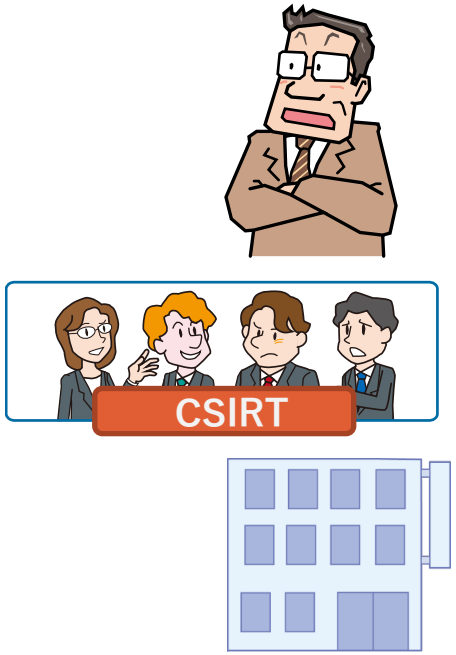
【出典】 XZ Utilsに悪意のあるコードが挿入された問題（CVE-2024-3094）について（JPCERT/CC）
https://www.jpcert.or.jp/newsflash/2024040101.html
Urgent security alert for Fedora Linux 40 and Fedora Rawhide users（Red Hat）
https://www.redhat.com/en/blog/urgent-security-alert-fedora-40-and-rawhide-users

【2位】サプライチェーンや委託先を狙った攻撃

- **対策**
  - **組織(経営者層)**

【被害の予防／被害に備えた対策】

- インシデント対応体制を整備し、対応する
  - CISO を配置する
  - CSIRT を構築する
  - 報告フォーマットは決めておく
  - 有事の際の対応フローを確立、社員へ通知する
  - 対応フロー通りに実施できるか訓練をする
  - 外部の協力依頼先を用意する
  - 社内規則の整備や予算確保をする



【2位】サプライチェーンや委託先を狙った攻撃

- **対策**
  - **組織(自組織で実施)**

【被害の予防／被害に備えた対策】

- 情報管理規則の徹底
- セキュリティ評価サービス(SRS)を用いた自組織のセキュリティ対策状況の把握
- 信頼できる委託先、取引先、サービスの選定
- 契約内容の確認
- 委託先組織の管理
- 納品物の検証(ソフトウェアの把握や管理※1 、脆弱性対策の実施等)
- サーバーや PC、ネットワークの適切なセキュリティ対策

【出典】 ※1 サイバー攻撃への備えを！「SBOM」（ソフトウェア部品構成表）を活用してソフトウェアの脆弱性を管理する具体的手法についての改訂手引を策定しました（経済産業省）
https://www.meti.go.jp/press/2024/08/20240829001/20240829001.html