身を守るには
知ることから！

情報セキュリティ被害の最新事例
2025年3月版

【大切なお願い】
会社を守るため、社長様、幹部様、従業員様、
パソコンやスマホを利用する**皆さまに回覧ください。**
自分事で実態を知ることが対策の第一歩です。

【この冊子の活用の仕方】
この冊子では、セキュリティの最新情報を月刊で
お伝えしています。被害事例を**自社に置き換えて、**
対策と意識向上にお役立てください。

BASIC Confertas Office

■ランサムウェア「Medusa」の被害が世界で拡大 二重の恐喝、重要インフラに300件超の被害

2025年3月24日

・米連邦捜査局（FBI）などが、ランサムウェア「Medusa」に関する注意喚起を発表。既に300件以上の被害が報告されており、主に医療・教育・製造などの重要インフラが標的となっている。

・Medusaは、RaaS型のランサムウェアで、開発者が攻撃実行をアフィリエイトに委ねる形で拡散。フィッシングやソフトウェアの脆弱性を悪用して企業内に侵入し、内部ネットワークをスキャン、情報を窃取・暗号化する。

・Medusaは二重の恐喝モデルを採用しており、データの暗号化と同時に「支払わなければ公開する」と脅迫。身代金支払いの猶予は48時間で、金額は10万ドルから1500万ドルに及ぶこともある。

■画像：ZDNETの記事ページ

■出典： https://japan.zdnet.com/article/35230852/

ランサムウェアの手口は年々進化しており、特にRaaSモデルの普及により誰でも高度な攻撃を仕掛けられる時代に突入しています。最新の脅威情報の収集と迅速な対応体制の整備が不可欠です。

BASIC
Confertas Office

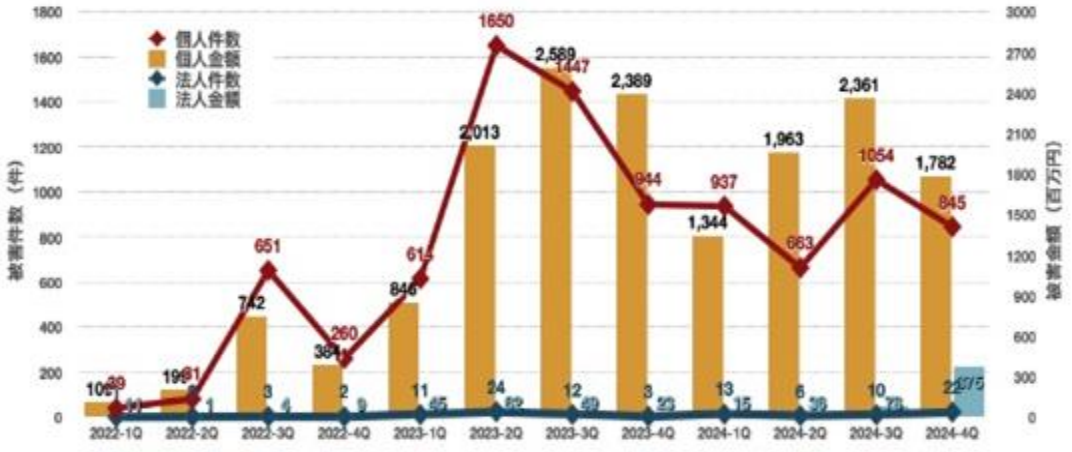
■法人の不正送金被害額が急増　約21.5億円で前四半期比4.5倍に

2025年3月31日

・全国銀行協会によると、2024年10～12月期のオンラインバンキングにおける不正送金被害額は約21億5700万円に上り、法人における被害額が前四半期比で約4.5倍と大幅に増加した。

・調査は全国189行を対象に実施。被害件数は867件と、前四半期の1064件から約18.5%減少。被害額も前期比で約11.6%減となったが、法人に関しては深刻な増加傾向が見られた。

法人の被害は22件ながら、被害額は約3億7500万円に達し、1件あたりの平均被害額は約1700万円と極めて高額。



法人を標的とした手口が巧妙化・大型化しています。被害が発生すれば経営への影響も甚大です。特に送金業務に関わるシステムやフローの見直し、そして社員のセキュリティ教育を徹底しましょう。

■画像：不正送金被害の推移

■出典：https://www.security-next.com/168720

BASIC Confertas Office

■ファーストリテイリングで情報流出の可能性 委託先の設定ミスが原因、従業員・取引先の個人情報が対象に

2025年3月19日

・ファーストリテイリング（ユニクロ・ジーユー運営）は、外部からの不正アクセスにより、従業員および取引先従業員の個人情報が流出した可能性があることを公表した。

・情報流出の可能性があるのは、2018年1月～2021年5月に取引があった事業者の従業員の氏名、電話番号、メールアドレス。また、2023年4月～2024年9月に店舗に在籍していた従業員、2018年5月～2023年9月に本部に在籍していた従業員も対象となる。

・本部従業員については、氏名・従業員番号・メールアドレスに加え、所属部署や電話番号など業務に関する情報も流出したおそれがある。

■画像：ファーストリテイリングのホームページ

■出典：
https://www.fastretailing.com/jp/group/news/2503181100.html

今回の事案は、委託先の設定変更に起因するものであり、自社だけでなく外部パートナーを含めたセキュリティ体制の強化が求められています。自社内外を含めたリスク管理体制の見直しを行いましょう。

BASIC Confertas Office

■Apple IDに関する偽メールに注意 急増するフィッシング詐欺、偽サイトで情報搾取

2025年3月5日

Appleユーザーを標的としたフィッシング攻撃が増加しているとして、フィッシング対策協議会が注意喚起を発表。「Apple IDの支払い情報更新」や「サブスクリプション期限切れ」などを装った偽メールで、ユーザーを不安にさせ偽サイトへ誘導する手口が確認されている。

・フィッシングメールには、「Appleよりご注文に関する重要なお知らせ」「Apple からの領収書です」など、少なくとも9種類の件名が用いられ、巧妙にユーザーの行動を促している。

・誘導先の偽サイトでは、Apple IDのメールアドレス、パスワード、電話番号、さらにはクレジットカード情報までを詐取するよう設計されていた。

■画像：Appleのホームページ

■出典:https://www.antiphishing.jp/news/alert/apple_20250305.html

フィッシング攻撃は年々巧妙化しており、誰もがターゲットになり得ます。「自分は大丈夫」と思わず、日頃からのセキュリティ意識が重要です。

■徳島県教委のメールサーバが悪用され約140万件の迷惑メール送信

2025年3月13日

・徳島県は、県教育委員会が利用するメールサーバを経由して約140万件の迷惑メールが送信されたと発表。迷惑メールが送信されたのは、2月22日15時50分から2月27日22時30分頃までの間でこのうち約137万件は実在しないメールアドレス宛だった。

・送信元として使われたのは、実在しないメールアドレス4件と、実在するメールアドレス1件。メールの件名は日本語ではなく、内容から明らかに迷惑メールと判断できるものだったという。

・原因は調査中だが、メールサーバのメンテナンス時に、サービス提供業者の設定および動作確認が不十分だった可能性があるとの報告を受けている。

■画像：徳島県のホームページ

■出典：https://www.security-next.com/168116

メールサーバの設定不備や確認不足は、第三者による悪用リスクを高めます。万が一の被害拡大を防ぐためにも、メンテナンス後の十分な動作確認を徹底しましょう。

BASIC Confertas Office

■「北海道じゃらん」関連サイトがサイバー攻撃被害 最大10万人超の個人情報が流出の可能性も

2025年3月21日

・リクルートが発行する旅行情報誌「北海道じゃらん」の関連サイトがサイバー攻撃を受け、最大10万4000人分の会員情報が流出した可能性があるとして、調査が進められている。

・攻撃は3月19日8時ごろに検知され、アンケートやスタンプラリー参加のために登録された会員情報が対象。流出の可能性があるのは、氏名、性別、生年月日、住所、電話番号、メールアドレス、ニックネーム、ハッシュ化されたパスワードなど。

・現在、当該サイトの機能は停止されており、原因や被害範囲についての調査が継続中。同時に、「北海道じゃらん」になりすましたフィッシングメールの存在も確認されており、利用者に対し、不審なメール内のリンクを開かないよう注意が呼びかけられている。

■画像：リクルートのホームページ

■出典：https://www.security-next.com/168415

近年、個人情報を保有するサイトは標的となりやすくなっています。不正アクセスの早期検知体制の構築、脆弱性の定期的な点検、パスワード管理の強化、通信の暗号化など多層的なセキュリティ対策が不可欠です。

情報セキュリティ対策は、実績豊富で信頼できる企業をお選びください。

最近は、ランサムウェアや情報漏えいなど、経営に関わるサイバー攻撃の被害も増加し、ひとつの社会問題となっています。私たちは、「サイバー攻撃の脅威からお客様を守りたい」そして、「今後もお客様と一緒に永く成長していきたい」と強く思っています。

情報セキュリティは、社内ネットワークに関わる重要な部分であり、信頼できる会社と付き合うことが大切です。私たちは、お客様に正確な情報と知識、安心の技術サポートを提供できる体制を整えていますので、ぜひご安心ください。