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
2024年9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

■ニチイHD、ランサムウェア被害で2.6万ファイル暗号化される 顧客の個人情報も

・医療・介護事業などを展開するニチイホールディングス（HD）は9月2日、ランサムウェア攻撃を受け、PC 計20台を経由して、約2万6000件のファイルが暗号化されたことが分かったと発表した。

・8月8日、子会社で介護事業を展開するニチイケアパレスのPC 1台がランサムウェアに感染していることが判明。その後、ニチイHDと子会社のニチイ学館で使っているPCでもデータ暗号化を確認した。

・同社の基幹システムやWebサイトへの被害は確認していない。また、現時点で外部への情報流出および二次被害も確認していないという。警察などと連携し、外部専門企業の協力を得ながら、原因究明や影響調査、復旧対応を進めているという。

サイバー攻撃を防御し、迅速に復旧するためには事前の準備が非常に重要です。自社のセキュリティ対策を改善していきましょう。

2024年9月3日

1．経緯

2024年8月8日（木）、当社子会社の株式会社ニチイケアパレスのPC1台がランサムウェアに感染していることを確認し、その後、当社および当社子会社の株式会社ニチイ学館で使用するPCにおいても電子データが暗号化されていることを確認しました。
※当社ホームページや基幹システムへの被害は確認されておりません。

2．被害の概要

外部の専門企業の協力のもと実施している調査において、現段階で、PC計20台を経由して、約2.6万件のファイルが暗号化・開封不可となっていることを確認しております。
また、前回公表以降の調査の結果、ランサムウェア感染により暗号化されたファイルに、お客様・関係企業等の担当者および当社の採用候補者・従業員・元従業員の個人情報が記載されたファイルが含まれていることが判明しました。対象者や個人情報の詳細は明らかになっていませんが、現時点の調査結果に則して、本日改めて個人情報保護委員会に報告しております。

なお、感染したPCについては社内ネットワークから切り離しており、また、外部への情報流出は確認されておりません。

3．暗号化された個人情報に関する当社対応

現時点で外部への情報流出および二次被害は確認されておりませんが、当社関係者になりすました不審メールやご連絡があるおそれがございます。専用のお問い合わせ窓口を設置いたしますので、不審なメール・連絡があった場合や、その他ご不安・ご心配を感じられた場合は、ご連絡ください。

■画像：ニュースリリースより

■出典:https://www.itmedia.co.jp/news/articles/2409/03/news129.html

■松竹、最大23万人分の個人情報漏洩の可能性と謝罪 物流システム通じサイバー攻撃の被害

2024年9月19日

・松竹は19日、サイバー攻撃により同社が運営する松竹ストアなどが業務委託している物流倉庫会社のシステムを通じて最大23万人分の個人情報漏洩の可能性が確認されたと発表した。

・現時点で漏洩した可能性のある個人情報の範囲については、「2024年9月12日（木）午前10時までに松竹ストア・松竹歌舞伎屋本舗楽天市場店で購入されたお客様の注文主様ならびにお届け先様（最大23万人分）の住所、氏名、電話番号、注文内容」とした上で「クレジットカード番号などの決済情報は倉業サービスのシステムでは保持しておりませんので、情報漏洩の可能性はございません」と強調した。

サイバー攻撃によって、流出する情報の範囲は計り知れません。個人情報を守れるよう、常にセキュリティの状態を確認しましょう。

■画像：松竹 （C）ORICON NewS inc.
■出典：https://news.livedoor.com/article/detail/27216842/

■不正アクセス被害 2 度 3 度の “リピーター” 企業も ～ 東京商工リサーチ アンケート結果

2024年9月5日

・株式会社東京商工リサーチは8月23日、「不正アクセスと情報セキュリティ対策に対するアンケート」調査の結果を発表した。

・同調査で、2020年以降で不正アクセスを受けたかを尋ねたところ5,735社から回答を得て、1回以上（「1回」および「2回」および「3回以上」の回答）不正アクセスを受けた企業は528社で約1割を占め、このうち2回以上（「2回」および「3回以上」の回答比率）不正アクセスを受けた企業は303社で、被害企業全体の半数を超えた。

・規模別では、1回以上受けた企業の比率は中小企業が8.7%に対し、大企業は13.8%で大企業が5.1ポイント高いことが判明した。大企業ほど大規模なシステムや大量データを保持しているため、不正アクセスの脅威に晒されやすいと推測している。

不正アクセスは 1 度だけでなく、何度でも被害に遭う可能性があります。被害を繰り返さないよう、被害を受けてからも、セキュリティを強化し続けましょう。

■画像：2020年以降に不正アクセスを受けた企業の割合（東商工調べ）

■出典：https://scan.netsecurity.ne.jp/article/2024/09/05/51584.html

BASIC Confertas Office

■農業協同組合(JAバンク)偽るフィッシング確認、注意を

2024年9月3日

・フィッシング対策協議会は9月2日、農業協同組合(JAバンク)を偽るフィッシングの報告を受けているとして、緊急情報を公開した。

・生体情報の利用登録によりログイン異常が発生し、振込およびATMの利用が一時停止されたといった内容のメールが送付され、リンク先はフィッシング詐欺サイトになっている。詐欺サイトでは、利用中の農業協同組合(JAバンク)の情報、ログインID、ログインパスワード、支店番号、科目、口座番号などの入力が求められる。

・2024年9月2日の時点で、フィッシングサイトは稼働している。フィッシング対策協議会は、フィッシングサイトやフィッシングメールを発見した際には同協議会まで報告してほしいと呼びかけている

フィッシングサイトは大抵、本物のサイトをコピーして作られているので人の目で判断するのは危険です。アクセスブロックを強化すると共に、日頃からブックマークや公式アプリを利用するように心がけましょう。

■画像：フィッシング対策協議会　Council of Anti-Phishing Japan｜ニュース｜緊急情報｜農業協同組合 (JAバンク) をかたるフィッシング (2024/09/02)

■出典：https://news.mynavi.jp/techplus/photo/article/20240903-3017786/images/001.jpg

■今年上半期のランサムウェア被害は114件 去年を上回るペースで増加　警察庁

2024年9月19日

・ランサムウェアの被害が今年6月までで114件に上っていたことが警察庁のまとめで分かった。

・前年の同時期の94件から増加し、国内の被害が拡大している。近年では「RaaS（Ransom as a Service）」と呼ばれるサイバー攻撃を代行するサービスも横行しており、セキュリティーが脆弱な企業などの重要なデータが狙われ続けている。また、復旧費用とは別にデータの公開をしない事を見返りに対価を要求する「二重恐喝」の手口も62件、確認されている。

・警察庁は引き続き「ネットワーク機器など脆弱性を放置することなく、常に対策を進めてほしい」と呼び掛けている。

■画像：テレ朝news

■出典：https://news.goo.ne.jp/article/tvasahinews/nation/tvasahinews-000372853.html

サイバー攻撃は常に進化しており、それに伴いセキュリティも進化させていく必要があります。自社のセキュリティを常に見直し、更新していきましょう。

■フィッシングの悪用URLが前月比2.2倍 - 過去最多を更新

・8月は前月に届かなかったものの、16万件を超えるフィッシングの報告が寄せられた。悪用されたURLの件数は、前月の2.2倍と急増し、過去最多を更新している。

・フィッシングサイトに悪用されたURLは8万5768件。前月の約2.2倍へと急増し、過去最多を更新そた。1日あたり約2766.7件のURLが見つかっている。大量にフィッシングメールをばらまく手口において、URLのサブドメインにランダムの文字列を用いるケースが目立ち、その影響でURL数が急増した。

・フィッシングサイトに悪用されたトップレベルドメインとしては、「.cn」が約46.9%でもっとも多く、「.com」が約35.6%、「.net」が約2.6%、「.top」が約2.4%で続いている。

ドメインの判別技術を用いた受信拒否をすり抜けてくるものもあります。対策しているからと安心せず、常に注意することが重要です。

2024年9月20日

■画像：フィッシング報告やURL件数の推移

■出典：https://www.security-next.com/162063

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。