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4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。

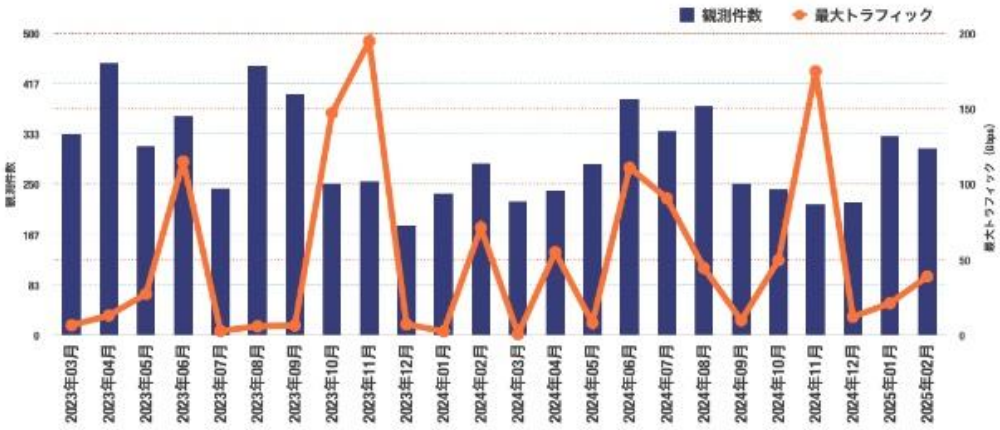
■DDoS攻撃は“量より頻度”の時代へ　IIJ観測レポートに見る最新動向

2025年4月2日

・インターネットイニシアティブ（IIJ）は、2025年2月に同社が観測したDDoS攻撃のレポートを公表。

・攻撃件数は309件で、前月の329件から減少したものの、2カ月連続で300件超えと依然高水準。1日平均攻撃数は11.0件と、前月（10.6件）より増加。2月25日には1日で30件のDDoS攻撃を観測。

・最大規模の攻撃では、398万pps、38.8Gbpsのトラフィックが発生（UDPフラッド等の複合攻撃）。最長の攻撃はNTPを悪用したUDP増幅攻撃で、38分間・最大5.4Gbpsのトラフィックを記録。



■画像：IIJが観測したDDoS攻撃の推移

■出典：https://www.security-next.com/168788

DDoS攻撃は単発の大規模攻撃から、頻度の高い中小規模の攻撃へとシフトしています。攻撃数の減少に安心せず、常時発生するリスクを前提にしたセキュリティ体制の整備が重要です。

■ANAを装うフィッシング詐欺が急増　偽サイトに要注意

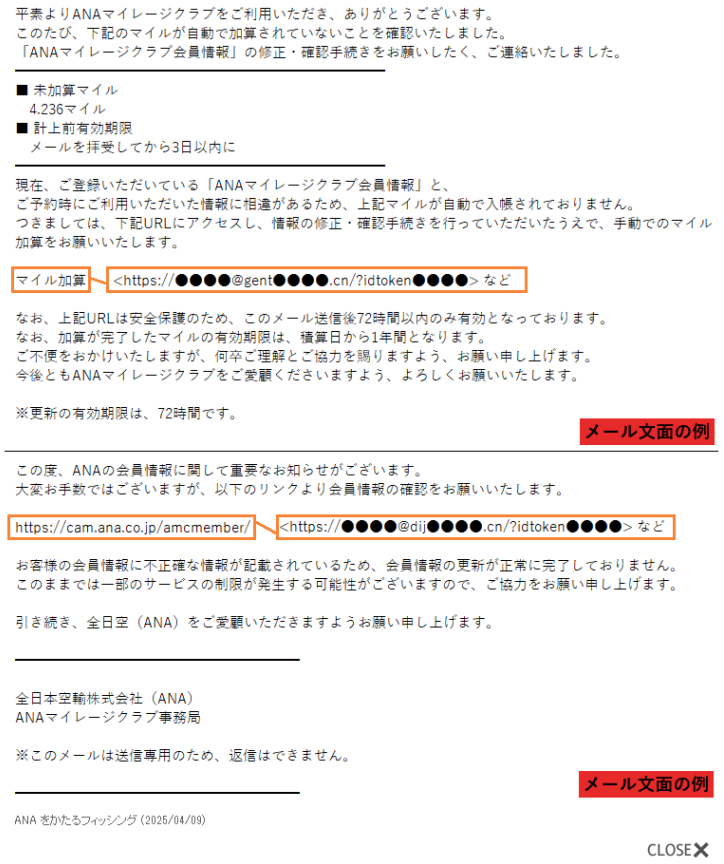
2025年4月9日

・2025年4月9日、ANAをかたるフィッシング詐欺の報告が増加しており、JPCERT/CCが該当サイトの閉鎖に向けた調査を進めている。

・これらのサイトは本物の画面を模倣しており、判別が困難なため、ログインは正規アプリやブックマークから行うことが推奨される。

・不審なメールやサイトを発見した場合は、フィッシング対策協議会（info@antiphishing.jp）への報告が求められている。

近年のフィッシング詐欺は、実在の企業サイトを巧妙に模倣し、見分けがつきにくくなっています。今回のような事例では、メールやSMS内のリンクからアクセスせず、公式アプリや正規のブックマークを使用してログインする習慣を徹底することが重要です。



平素よりANAマイレージクラブをご利用いただき、ありがとうございます。
このたび、下記のマイルが自動で加算されていないことを確認いたしました。
「ANAマイレージクラブ会員情報」の修正・確認手続きをお願いしたく、ご連絡いたしました。

■ 未加算マイル
4,236マイル
■ 計上前有効期限
メールを拝受してから3日以内に

現在、ご登録いただいている「ANAマイレージクラブ会員情報」と、
ご予約時にご利用いただいた情報に相違があるため、上記マイルが自動で入帳されておりません。
つきましては、下記URLにアクセスし、情報の修正・確認手続きを行っていただいたうえで、手動でのマイル加算をお願いいたします。

マイル加算　<https://●●●●@gent●●●●.cn/?idtoken●●●●> など

なお、上記URLは安全保護のため、このメール送信後72時間以内のみ有効となっております。
なお、加算が完了したマイルの有効期限は、積算日から1年間となります。
ご不便をおかけいたしますが、何卒ご理解とご協力を賜りますよう、お願い申し上げます。
今後ともANAマイレージクラブをご愛顧くださいますよう、よろしくお願いいたします。

※更新の有効期限は、72時間です。

メール文面の例

この度、ANAの会員情報に関して重要なお知らせがございます。
大変お手数ではございますが、以下のリンクより会員情報の確認をお願いいたします。

https://cam.ana.co.jp/amcmember/　<https://●●●●@dij●●●●.cn/?idtoken●●●●> など

お客様の会員情報に不正確な情報が記載されているため、会員情報の更新が正常に完了しておりません。
このままでは一部のサービスの制限が発生する可能性がございますので、ご協力をお願い申し上げます。

引き続き、全日空（ANA）をご愛顧いただきますようお願い申し上げます。

全日本空輸株式会社（ANA）
ANAマイレージクラブ事務局

※このメールは送信専用のため、返信はできません。

メール文面の例

ANA をかたるフィッシング (2025/04/09)

CLOSE✕

■画像：メール・SMSの文面例

■出典：https://www.antiphishing.jp/news/alert/ana_20250409.html

■元スタッフが不正アクセス　東急スポーツシステムの予約システムで内部不正が発覚

2025年4月15日

・東急スポーツシステム株式会社は、運営する「アトリオドゥーエ Next たまプラーザ」のレッスン予約システムにおいて、業務委託スタッフによる不正アクセスがあったことを4月15日に発表。

・事案は3月17日にクラブ外での予約キャンセルが発生し、調査の結果、退社後も他者のアカウントを不正利用していたことが判明。

・当該アカウントは、アルバイト期間中に他者から入手したもので、退社後も継続的に不正アクセスしていた。スマートフォンの履歴などから顧客情報の持ち出しは確認されていない。

・再発防止策として、委託先との再協議、研修強化、監督体制の強化、システム監視とパスワード更新の徹底、対策の効果検証を実施する方針。

■画像：東急スポーツシステム株式会社のホームページ

■出典：
https://scan.netsecurity.ne.jp/article/2025/04/30/52775.html

この事案は、内部関係者によるアカウント不正利用というインサイダーリスクが現実化した典型例です。外部攻撃だけでなく、元従業員や委託スタッフのアクセス権限管理や情報モラル教育の重要性を再認識する必要があります。

■サンエイ、サイバー攻撃でランサム被害　取引先情報流出の懸念

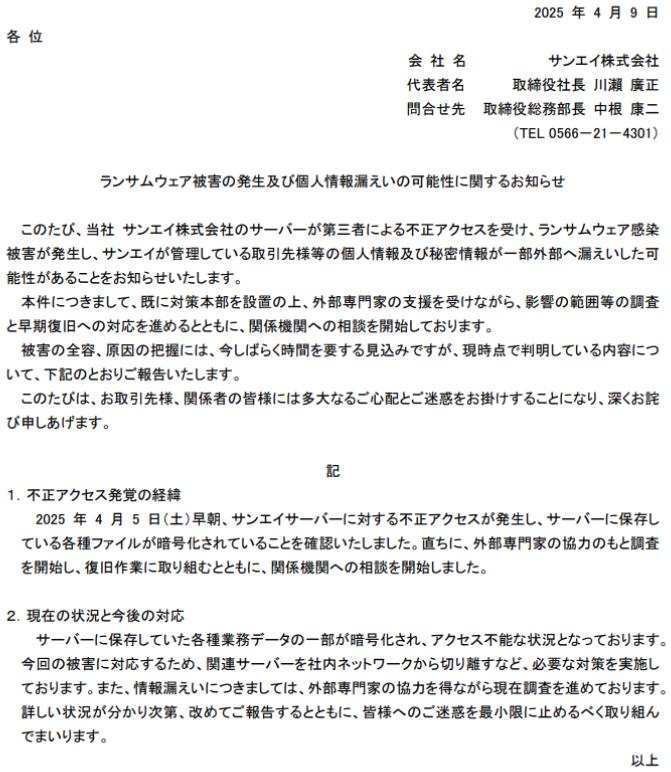
2025年4月24日

・建設や物流事業を手がけるサンエイがサイバー攻撃を受け、情報流出の可能性があるとして調査を進めている。

・攻撃は4月5日早朝に確認され、同社サーバがランサムウェアに感染。保存されていたファイルが暗号化される被害が発生した。

・流出の可能性がある情報には、取引先の個人情報や機密情報の一部が含まれる。現在、サーバは社内ネットワークから隔離されており、外部専門家の協力のもと、情報流出の有無や被害範囲の特定、復旧作業が進められている。

近年、ランサムウェアの手口は巧妙化しており、RaaSモデルの台頭により、技術的な知識が乏しい攻撃者でも深刻な被害を引き起こすケースが増えています。最新の脅威動向を常に把握するとともに、初動対応を含めたインシデントレスポンス体制の整備が急務です。



2025 年 4 月 9 日

各 位

会 社 名　サンエイ株式会社
代表者名　取締役社長 川瀬 廣正
問合せ先　取締役総務部長 中根 康二
（TEL 0566－21－4301）

ランサムウェア被害の発生及び個人情報漏えいの可能性に関するお知らせ

このたび、当社 サンエイ株式会社のサーバーが第三者による不正アクセスを受け、ランサムウェア感染被害が発生し、サンエイが管理している取引先様等の個人情報及び秘密情報が一部外部へ漏えいした可能性があることをお知らせいたします。

本件につきまして、既に対策本部を設置の上、外部専門家の支援を受けながら、影響の範囲等の調査と早期復旧への対応を進めるとともに、関係機関への相談を開始しております。

被害の全容、原因の把握には、今しばらく時間を要する見込みですが、現時点で判明している内容について、下記のとおりご報告いたします。

このたびは、お取引先様、関係者の皆様には多大なるご心配とご迷惑をお掛けすることになり、深くお詫び申しあげます。

記

1. 不正アクセス発覚の経緯

2025 年 4 月 5 日（土）早朝、サンエイサーバーに対する不正アクセスが発生し、サーバーに保存している各種ファイルが暗号化されていることを確認いたしました。直ちに、外部専門家の協力のもと調査を開始し、復旧作業に取り組むとともに、関係機関への相談を開始しました。

2. 現在の状況と今後の対応

サーバーに保存していた各種業務データの一部が暗号化され、アクセス不能な状況となっております。今回の被害に対応するため、関連サーバーを社内ネットワークから切り離すなど、必要な対策を実施しております。また、情報漏えいにつきましては、外部専門家の協力を得ながら現在調査を進めております。詳しい状況が分かり次第、改めてご報告するとともに、皆様へのご迷惑を最小限に止めるべく取り組んでまいります。

以上

■画像：サンエイ株式会社のホームページ上のお知らせ

■出典： https://www.san-ei-kk.co.jp/index.html

■従業員がサポート詐欺被害、顧客情報など約800件流出か 住友林業クレスト

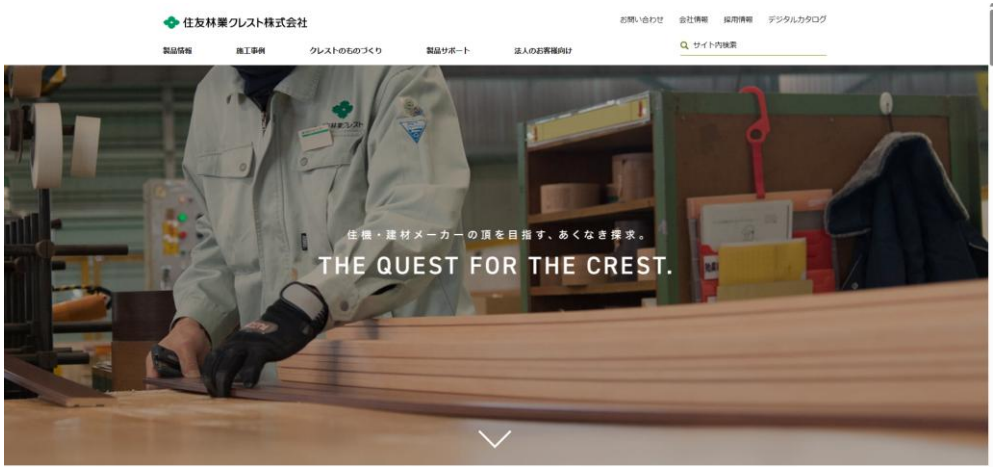
2025年4月28日

・住友林業クレストは、従業員がサポート詐欺の被害に遭い、顧客や従業員の個人情報が流出した可能性があると4月28日に発表。

・3月24日、サポート業務を担当する従業員が業務用PC使用中に詐欺サイトへ誘導され、遠隔操作ソフトをインストール。

・不正に気付き、端末をネットワークから遮断したが、PC内部の情報が外部に流出した可能性がある。流出の恐れがある情報は、顧客の氏名約500件、従業員の顔写真、携帯番号約300件、図面・見積書など。

・現在、外部協力のもとで被害状況の調査を継続中。関係機関への報告とともに、情報流出の可能性がある関係者への連絡を進めている。



■画像：住友林業クレスト株式会社のホームページ

■出典：https://www.sumirin-crest.co.jp/

この事例は業務用端末を狙ったサポート詐欺による人的ミスを起点とする情報漏洩リスクの事例です。従業員一人の誤操作が企業全体の機密情報漏洩につながる可能性があるので、人的エラーを前提とした多層的な防御体制を整備することが、今後ますます重要になります。

■保険見直し本舗グループ、ランサムウェア被害で最大510万件の個人情報流出の可能性

2025年4月30日

・保険見直し本舗グループは、2月16日に確認されたランサムウェア攻撃により、最大で約510万件の個人情報が漏えいした恐れがあると4月30日に発表した。

・対象情報には、保険契約者や相談者、協業先から受託した顧客の氏名、住所、電話番号、保険契約情報などが含まれるが、マイナンバーや銀行口座、クレジットカード情報は含まれていない。

・被害確認後はサーバをネットワークから隔離し、外部専門家の協力で調査、復旧を進行中。実際の情報流出や公開は確認されていないが、漏えいの可能性がある顧客には個別連絡を実施。

・現在も外部専門家と連携しながら再発防止策を講じ、営業を段階的に再開している。

■画像：保険見直し本舗のホームページ

■出典：https://mhompo.co.jp/

今回の事案は、ランサムウェアの深刻な影響と、情報資産管理の脆弱性を浮き彫りにしました。特に、保険業界のように個人情報を大量に扱う事業者にとって、「暗号化された＝流出していない」とは限らないというリスク認識が必要です。

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。