身を守るには
知ることから！

社内回覧用

情報セキュリティ被害の最新事例
2021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。

サイバー攻撃最新事例

■「フィッシングメールにご注意ください」というフィッシングメールに注意！

2021年3月2日

・クレジットカード会社のアプラスを装うフィッシング攻撃が確認された。

・メール文中では、フィッシングメールの注意喚起を記載しつつ、偽サイトへ誘導し、偽サイトでは個人情報の入力をさせようとする。

【重要：注意喚起】アプラスを装ったフィッシングメールにご注意ください

アプラスを装ったフィッシングメールが当社のお客さまか否かを問わず不特定多数の方に配信され、電子メールに記載されたリンクから巧妙に偽のカード会員様向けサービス（NETstation*APLUS）に誘導し、カード情報などを入力させる手口が発生しています。
このたび、ご本人様のご利用かどうかを確認させていただきたいお取引がありましたので、誠に勝手ながら、カードのご利用を一部制限させていただき、ご連絡させていただきました。
つきましては、以下へアクセスの上、カードのご利用確認にご協力をお願い致します。
ご回答をいただけない場合、カードのご利用制限が継続されることもございますので、予めご了承ください。

■ご利用確認はこちら

偽メールには詐欺サイトへのURLが記載されています。

■注意事項

※本メールは送信専用です。
※本メールは「NETstation*APLUS」にメールアドレスをご登録いただいた方にお送りしています。
※変更後、48時間以内に発行する必要があり、期間中は使用できません。

■画像：フィッシングメール注意喚起を装うフィッシングメール（アプラス）

■画像：実際の詐欺サイトの例（アプラス）

偽メールから偽サイトへアクセスさせ、個人情報やクレジットカード番号などを入力させるフィッシングの手口は巧妙さを増しています。メールやサイトアクセスの防御を強めましょう。

■出典：アプラス
https://news.aplus.co.jp/notes/detail.html?id=10009688&category=&page=300

■楽天カードを装い、サービス障害復旧を騙るフィッシング手口に注意

2021年3月4日

・楽天カードをかたるフィッシングメールが確認されている。

・ECサイト「楽天市場」が障害から復旧したなどと偽ってフィッシングサイトへ誘導し、クレジットカード番号や個人情報を窃取しようとする。

・メールの件名は「【楽天市場】障害解消：複数サービスダウン復旧のお知らせ」など。「楽天市場の複数サービスダウンが回復しました」「ログインして、アカウントが利用可能かどうかを確認してください」などと書かれた本文で、偽サイトへ誘導する。

・誘導先は楽天のログインページに酷似した偽サイトで、会員IDやパスワード、クレジットカード番号、セキュリティコードなどの入力を求められる。

■画像：楽天を装う偽メールの例（ITmedia）

嘘の内容にリアル感があり、巧妙さを増しています。楽天は日本の利用者も多く、注意が必要です。メールブロックやサイトアクセス制御などのセキュリティ対策を強化しましょう。

■出典：ITmedia　NEWS
https://www.itmedia.co.jp/news/articles/2103/04/news138.html

サイバー攻撃最新事例

■ANAとJALの会員情報流出、予約システム会社にサイバー攻撃

2021年3月6日

・日本航空（JAL）は3月5日、約92万人分の会員情報が流出したと発表した。6日、全日本空輸（ANA）も、マイレージ会員の氏名など約100万人分の情報が流出したと発表した。

・JALやANAが所属する航空連合の一部加盟社が使っていた予約システム会社（スイスのSITA社）が、サイバー攻撃を受けたためである。

・JALやANAは同システムを使っていなかったが、この一部加盟社と共有していた情報が漏洩した。

・パスワードやパスポート番号、クレジットカード情報、住所、メールアドレスなどは流出していないという。

■画像：ロイター

自社の提携先や取引先、委託先などにも情報がある場合、情報を守るには自社だけなく、それらの会社にも働きかけ、協力していく必要があります。サプライチェーン全体でのセキュリティ対策を目指していきましょう。

■出典：REUTERS
https://jp.reuters.com/article/ana-jal-cyber-attack-idJPKCN2AY062

サイバー攻撃最新事例

■米中小企業など3万組織に攻撃、マイクロソフトの脆弱性を標的に。

2021年3月6日

・米国でマイクロソフトのメールシステムの脆弱性（セキュリティー上の欠陥）を突いたサイバー攻撃が広がっている。マイクロソフトによると中国系ハッカー集団「ハフニウム」が関与したとみられ、米政府も警鐘を鳴らしている。

・被害は米国の産業供給網（サプライチェーン）の基盤である中小企業など3万の組織に及ぶとの推計もある。

・標的となったのは、企業がメールや予定共有に利用するマイクロソフトのサーバー向けソフト「エクスチェンジ・サーバー」。中小企業や地方自治体、学校などで広く使われている。

・ハッカーは同ソフトの脆弱性を突いて「Webシェル」と呼ぶマルウエア（悪意のあるソフト）を作成。ソフトを遠隔操作し、組織のデータを盗み出す。

■画像：ロイター

中小企業など3万社に及ぶ大規模なサイバー攻撃が米国で発生しています。日本でも注意が必要です。脆弱性を残さないように、お使いの各種ソフトウェアは最新バージョンにアップデートしておきましょう。

■出典：日本経済新聞
https://www.nikkei.com/article/DGXZQOGN062GA0W1A300C2000000/

■サーバがランサム感染、受託先の情報流出の可能性 - ランドブレイン

2021月3月5日

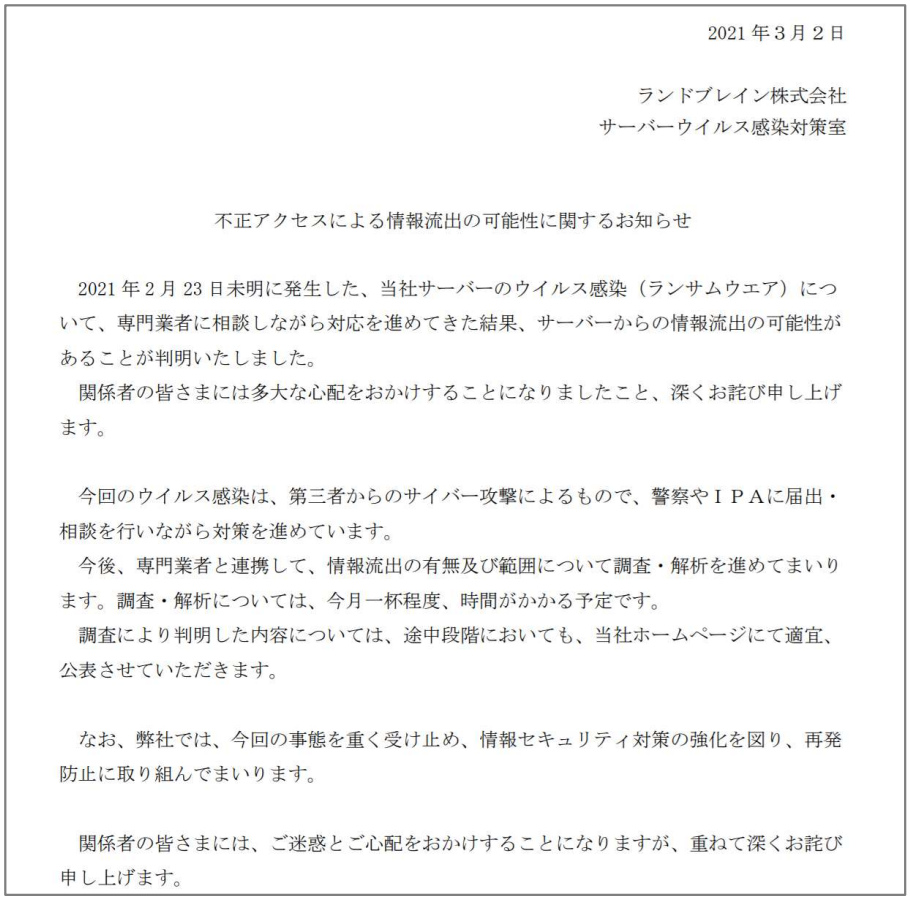
・復興支援や地方創生事業などを手がけるランドブレイン株式会社は、同社サーバがランサムウェアに感染し、外部に情報が流出した可能性があることを明らかにした。

・ランサムウェアとは、感染した端末内のデータを暗号化し、解除と引き換えに金銭を要求するマルウェアのこと。最近では、暗号化するだけでなく、情報を盗み取ることで脅迫を強める傾向にある。

・同社に委託していた北海道旭川市では、市営住宅の入居者情報が外部に流出した可能性があることを発表している。

・その他、大阪府岸和田市、千葉県芝山町、大阪府茨木市も同様の発表をしている。

自社の提携先や取引先、委託先などにも情報がある場合、情報を守るには自社だけなく、それらの会社にも働きかけ、協力していく必要があります。サプライチェーン全体でのセキュリティ対策を目指していきましょう。



2021 年 3 月 2 日

ランドブレイン株式会社
サーバーウイルス感染対策室

不正アクセスによる情報流出の可能性に関するお知らせ

2021 年 2 月 23 日未明に発生した、当社サーバーのウイルス感染（ランサムウエア）について、専門業者に相談しながら対応を進めてきた結果、サーバーからの情報流出の可能性があることが判明いたしました。
関係者の皆さまには多大な心配をおかけすることになりましたこと、深くお詫び申し上げます。

今回のウイルス感染は、第三者からのサイバー攻撃によるもので、警察やＩＰＡに届出・相談を行いながら対策を進めています。
今後、専門業者と連携して、情報流出の有無及び範囲について調査・解析を進めてまいります。調査・解析については、今月一杯程度、時間がかかる予定です。
調査により判明した内容については、途中段階においても、当社ホームページにて適宜、公表させていただきます。

なお、弊社では、今回の事態を重く受け止め、情報セキュリティ対策の強化を図り、再発防止に取り組んでまいります。

関係者の皆さまには、ご迷惑とご心配をおかけすることになりますが、重ねて深くお詫び申し上げます。

■画像：不正アクセスによる情報流出の可能性に関するお知らせ（ランドブレイン株式会社）

■出典：Security NEXT
https://www.security-next.com/123838

■LINEの個人情報、中国の開発委託先から閲覧可能に

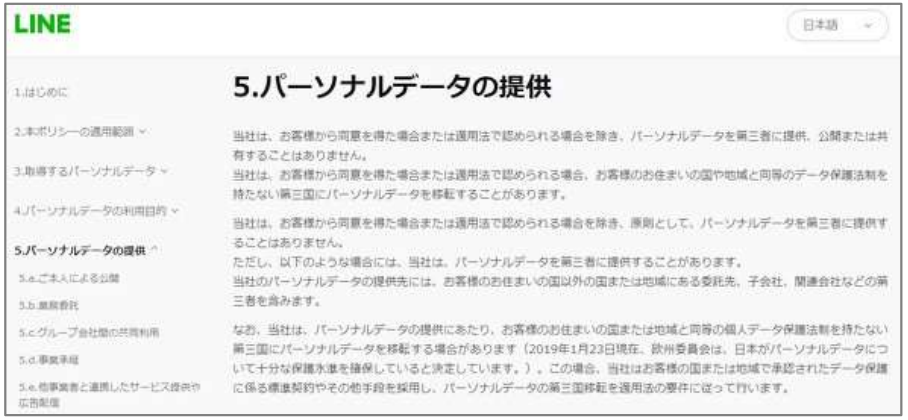
2021年3月17日

・LINEは3月17日、メッセージアプリ「LINE」を日本で使う人の個人情報などが、アプリのシステム開発を委託していた中国企業からアクセスできる状態だったと明らかにし、「利用者への説明が不十分だった」と謝罪した。既に閲覧できないように対策済みだという。

・中国企業に閲覧されたとみられるのは、日本のLINEアプリユーザーの暗号化された氏名、住所、メールアドレスなど。

・LINEは国際競争力を確保するため、海外企業に一部の作業を委託して開発スピードを上げているという。当該の中国企業は社内ツールやAI、LINEアプリ内の機能の開発を担っており、LINEは作業に必要な情報として、ユーザーの個人情報にアクセスできるようにしていた。

多くの日本人が利用しているLINE。これからは、「どこにどのような状態でデータを保管しているか」も、企業やサービスの信用に大きく関わってくることを認識して事業運営していきましょう。



■画像：LINEアプリでの情報の扱いについて、プライバシーポリシーには「お客さまから同意を得た場合または適用法で認められる場合を除き、パーソナルデータを第三者に提供、公開または共有することはありません」と記述があり、LINEはこの規定に基づいて情報を提供したとしている。

■出典：ITmedia NEWS
https://www.itmedia.co.jp/news/articles/2103/17/news127.html

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。