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2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。

■ウェブサイトがドメインをランサムウェア配布サイトに乗っ取られる被害

2021年2月1日

・プログラミング言語Perlに関する情報を1997年以来提供している「Perl.com」のドメインが何者かに乗っ取られたことが明らかになった。

・当該ドメイン「perl.com」がランサムウェアを配布するサイトと同一のIPアドレスにホストされていることが確認されており、アクセスしないように注意が呼びかけられている。

・ランサムウェアとは、感染するとパソコンやサーバ内のデータを暗号化されてしまい、その解除と引き換えに金銭を要求するタイプのウイルスの一種。感染すると、あらゆるデータが使えなくなってしまう。

■画像：GIGAZINE

アクセスしたサイトがもし乗っ取られていると、ウイルスに感染してしまう可能性があります。見極めが困難であることから、防ぐのが難しい手口と言えます。感染の確率を下げるには、PC内のソフトウェアやブラウザのバージョンをアップデートすると共に、ウイルスソフトやゲートウェイの対策を複合的に強化しましょう。

■出典： GIGAZINE
https://gigazine.net/news/20210201-perl-domain-stolen/

サイバー攻撃最新事例

■「就職希望です！」「研究成果を見て！」 ―就職希望者を装って企業が狙われる、巧妙な“攻撃”手口

2021年2月4日

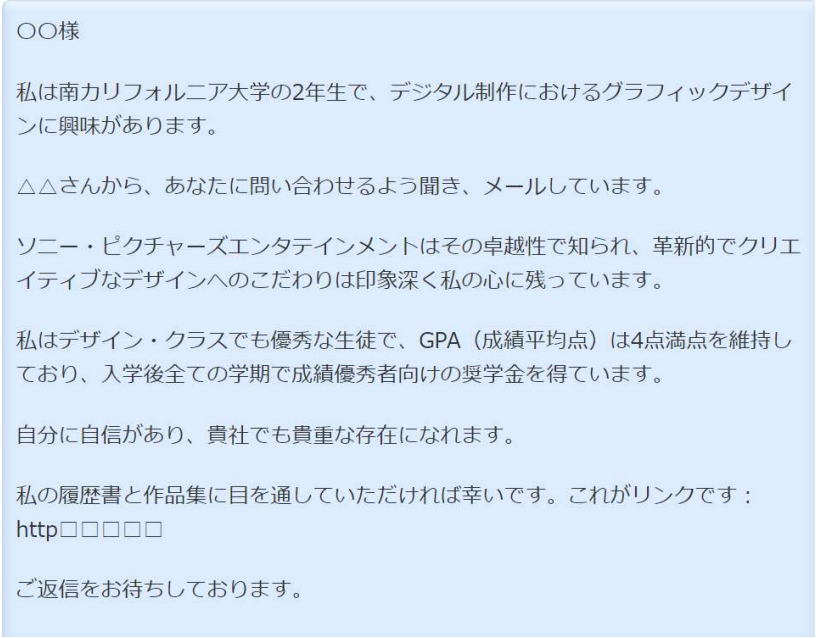
・攻撃者たちは日々、詐欺メールをクリックさせるために巧妙な工夫を凝らしてきている。

・そのひとつが、企業に対して、就職希望者を偽って詐欺メールを送り付けるパターンだ。

・「履歴書」や「研究成果」などと偽って、企業の採用担当者に添付ファイルをクリックさせようとしたりする手口が見つかっている。

・中には、北朝鮮のハッカー集団の可能性が高いと見られる詐欺メールも届いている。

採用活動を行っている企業にこのようなメールが届くと、採用担当者も騙されてしまう危険性が高い手口です。添付ファイルや文中のリンクには十分注意するとともに、ウイルスメールをブロックする対策を強化しましょう。



〇〇様

私は南カリフォルニア大学の2年生で、デジタル制作におけるグラフィックデザインに興味があります。

△△さんから、あなたに問い合わせるよう聞き、メールしています。

ソニー・ピクチャーズエンタテインメントはその卓越性で知られ、革新的でクリエイティブなデザインへのこだわりは印象深く私の心に残っています。

私はデザイン・クラスでも優秀な生徒で、GPA（成績平均点）は4点満点を維持しており、入学後全ての学期で成績優秀者向けの奨学金を得ています。

自分に自信があり、貴社でも貴重な存在になれます。

私の履歴書と作品集に目を通していただければ幸いです。これがリンクです：
http□□□□□

ご返信をお待ちしております。

■画像：企業に実際に送られた就職希望者を装った詐欺メールの例
（ITmediaビジネスONLINE）

■出典：ITmediaビジネスONLINE
https://www.itmedia.co.jp/business/articles/2102/04/news016.html

■クラウド会計のfreee、個人情報約3000件が閲覧可能な状態に。―Salesforce製品の設定ミス

2021年2月10日

・クラウド会計ソフトを提供するfreeeは2月10日、メールアドレスなど2898件の個人情報が外部から閲覧可能な状態になっていたと発表した。

・問い合わせの管理に使っていたCRM（顧客関係管理）ツール「Salesforce」の権限設定に不備があり、第三者がアクセスできる状態になっていたという。

・Salesforceの設定ミスに起因する情報漏えいを巡っては、20年12月にPayPayが約2000万件の加盟店情報、楽天が148万件以上の個人情報に流出の可能性があると発表。内閣サイバーセキュリティセンターが注意を呼び掛けていた。

■画像：freeeによるプレスリリース（freee）

社内で利用しているシステムの設定不備によって、情報漏えいの恐れが発生することもあります。最近ではテレワーク化なども進んでいることから、クラウドサービスの利用も広がっています。設定の不備などが内容に、ベンダー側に相談を投げかけながら、運用の際には十分に注意しましょう。

■出典：ITmedia NEWS
https://www.itmedia.co.jp/news/articles/2102/10/news135.html

サイバー攻撃最新事例

■最も“なりすまし”が多かったのはMicrosoft、楽天も6位にランクイン。2020年フィッシング攻撃Top20

2021年2月10日

・セキュリティ企業であるVade Secure社による、フィッシング詐欺の攻撃数をランキングしたレポート「Phishers‘ Favorites（フィッシャーズ・フェイバリット）」の2020年1年が発表された。

・このレポートによると、世界76か国に渡る調査結果として、探知したフィッシング攻撃のなりすましとして最も多かったのが、Microsoftを装った手口だったとのこと。

・Microsoftフィッシングメールの多くは、Microsoftになりすますのではなく、別のブランドになりすまして攻撃を仕掛けてくるという。Microsoft 365フィッシングページへのリンクを仕込み、Microsoftブランドに対するユーザーの信頼を悪用するものだ。

・また、日本企業である楽天も初めて6位にランクインしている。

順位	2019年からの変動	ブランド・サービス名	カテゴリー	ユニークフィッシングURL数
1	➡	Microsoft	クラウド	39,621
2	⬆ 2	Facebook	ソーシャルメディア	14,876
3	⬇ 1	PayPal	金融サービス	11,841
4	⬆ 4	Chase	金融サービス	8,832
5	⬆ 28	eBay	eコマース／ロジスティクス	6,918
6	–	楽天	eコマース／ロジスティクス	6,452
7	⬇ 4	Netflix	クラウド	6,417
8	⬆ 2	Amazon	eコマース／ロジスティクス	6,063
9	⬆ 5	WhatsApp	ソーシャルメディア	5,322
10	⬇ 1	DHL	eコマース／ロジスティクス	4,403
11	–	Credit Agricole	金融サービス	4,317
12	⬆ 6	Wells Fargo	金融サービス	4,265
13	⬆ 3	Adobe	クラウド	4,171
14	⬇ 9	Bank of America	金融サービス	4,042
15	⬆ 2	Google	クラウド	3,317
16	⬆ 8	Comcast	インターネット／通信事業	3,297
17	⬇ 11	Apple	クラウド	3,131
18	⬆ 22	La Banque Postale	金融サービス	2,932
19	⬆ 9	LinkedIn	ソーシャルメディア	2,548
20	⬇ 8	Dropbox	クラウド	2,427

■画像：2020年のフィッシング攻撃のランキング（Vade Secure社）

フィッシングの手口はどんどん増えており、巧妙化も増しています。詐欺メール対策・サイトアクセス制御などを強化しましょう。

■出典：Security NEXT
https://www.security-next.com/122558

■ゲーム会社がサイバー攻撃を受け、ランサムウェア感染

2021月2月21日

・話題のゲームソフト『サイバーパンク2077』を開発した「CD PROJEKT RED」が2月8日にサイバー攻撃に遭っていたことが判明した。

・同社の日本支社によると、「何者かが内部ネットワークに不正なアクセスを働き、「CD PROJEKT RED」キャピタルグループに属する一部のデータを奪取し、身代金要求のテキストを残していた。」と発表している。

・その後、奪取された「CD PROJEKT RED」のソースコードが、ハッカーによりオークションサイトに出品されているのが発見された。

・同社は、2017年にも複数ファイルをハッキングされ、ハッカーから「身代金」を要求されている。

■画像：『サイバーパンク2077』キービジュアル

企業がファイルを盗まれ、ランサムウェアによって暗号化されるだけでなく、盗まれた情報がダークウェブ（闇サイト）のオークションで出品されていたという事例です。基本的にすべての企業は業務にかかわる機密情報を持っているはずですので、十分にランサムウェア感染には注意しましょう。

■出典：ニコニコニュース
https://news.nicovideo.jp/watch/nw8974239

サイバー攻撃最新事例

■石垣食品子会社、カード情報流出の恐れ。２２４人分、通販サイトへ不正アクセス

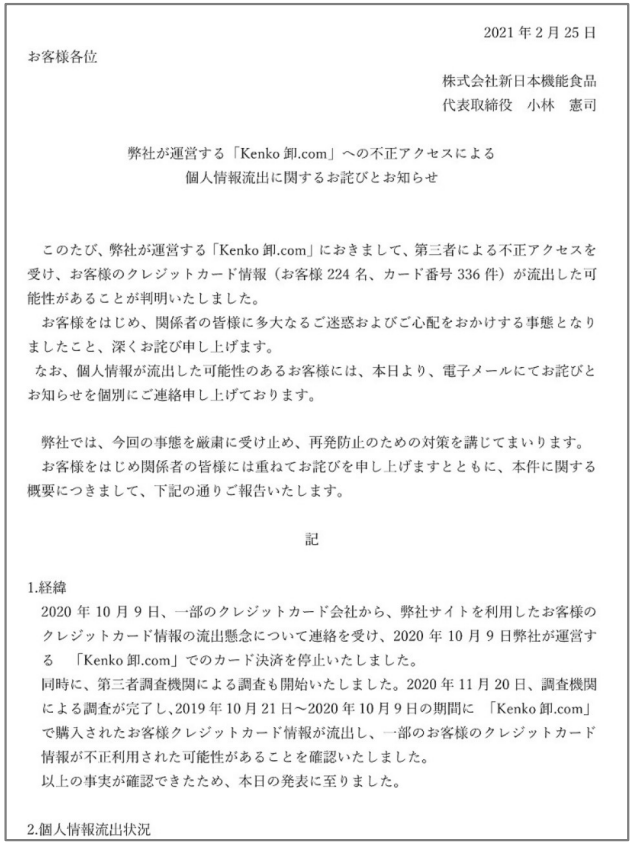
2021年1月26日

・石垣食品は２５日、子会社の新日本機能食品（岡山市）が運営する通信販売サイト「Kenko卸.com」が不正アクセスを受け、顧客２２４人分のクレジットカード情報が流出し、一部で不正利用された恐れがあると発表した。

・ウェブサイトのシステムの一部脆弱性を突かれたことが原因としている。

・流出した恐れがあるのは、２０１９年１０月２１日から２０年１０月９日までの間、このサイトでカード決済をした顧客のカード番号や名義人氏名、有効期限、セキュリティコード。

自社のウェブサイトのシステムに脆弱性が残っていて対策をしていないと、不正アクセスとして攻撃の対象になることがあります。顧客情報の漏えいを起こさぬよう、個人情報を扱うウェブサイトを運営する際は、セキュリティ対策をきちんと施しましょう。



2021 年 2 月 25 日

お客様各位

株式会社新日本機能食品
代表取締役　小林　憲司

弊社が運営する「Kenko 卸.com」への不正アクセスによる
個人情報流出に関するお詫びとお知らせ

このたび、弊社が運営する「Kenko 卸.com」におきまして、第三者による不正アクセスを受け、お客様のクレジットカード情報（お客様 224 名、カード番号 336 件）が流出した可能性があることが判明いたしました。
お客様をはじめ、関係者の皆様に多大なるご迷惑およびご心配をおかけする事態となりましたこと、深くお詫び申し上げます。
なお、個人情報が流出した可能性のあるお客様には、本日より、電子メールにてお詫びとお知らせを個別にご連絡申し上げております。

弊社では、今回の事態を厳粛に受け止め、再発防止のための対策を講じてまいります。
お客様をはじめ関係者の皆様には重ねてお詫びを申し上げますとともに、本件に関する概要につきまして、下記の通りご報告いたします。

記

1.経緯
2020 年 10 月 9 日、一部のクレジットカード会社から、弊社サイトを利用したお客様のクレジットカード情報の流出懸念について連絡を受け、2020 年 10 月 9 日弊社が運営する 「Kenko 卸.com」でのカード決済を停止いたしました。
同時に、第三者調査機関による調査も開始いたしました。2020 年 11 月 20 日、調査機関による調査が完了し、2019 年 10 月 21 日～2020 年 10 月 9 日の期間に 「Kenko 卸.com」で購入されたお客様クレジットカード情報が流出し、一部のお客様のクレジットカード情報が不正利用された可能性があることを確認いたしました。
以上の事実が確認できたため、本日の発表に至りました。

2.個人情報流出状況

■画像：株式会社新日本機能食品による発表

■出典：JIJI.COM
https://www.jiji.com/jc/article?k=2021022500645&g=eco
https://www1.kenko064.com/user_data/important-notice

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。