BASIC
Confertas Office

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
2023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。

BASIC Confertas Office

■マイナポイント事務局かたる詐欺メールに注意！「2万ポイントが失効します」と偽サイトに誘導

2023年3月31日

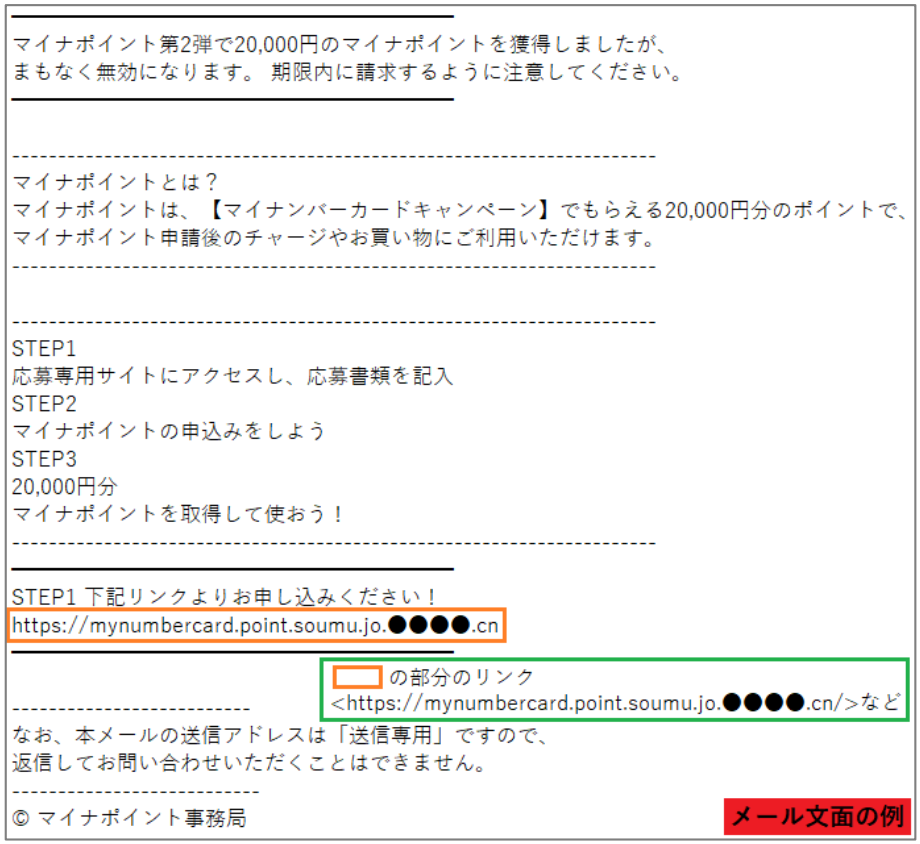
・「マイナポイント事務局」をかたる偽メールを確認したとして、フィッシング対策協議会が3月31日に注意喚起した。マイナポイントの申し込みをしなければ獲得したポイントが失効するなどとして偽サイトに誘導し、個人情報を盗み取ろうとするという。

・メールの件名は「【マイナンバーカード】マイナポイント第2弾で獲得した20,000円ポイントはまもなく失効します」など。文中のリンクから偽サイトに誘導する。

・偽サイトでは、メールアドレスや氏名、住所、クレジットカード情報などの入力を求められるという。なお、総務省は「総務省や市区町村の職員、その関係者が金融機関の口座番号、口座の暗証番号、資産の情報などを伺うことはない」と注意喚起している。

・フィッシング対策協議会はJPCERT/CCにサイト閉鎖に向けた調査を依頼しているという。マイナポイントの申請期限については、河野太郎デジタル大臣が9月末までに延長する方針を発表している。

申請期限が現在は5月末であることもあり、今後被害が拡大してしまう可能性があります。個人情報を扱う際はより一層、冷静な姿勢や対応が必要です。


マイナポイント第2弾で20,000円のマイナポイントを獲得しましたが、
まもなく無効になります。 期限内に請求するように注意してください。

マイナポイントとは？
マイナポイントは、【マイナンバーカードキャンペーン】でもらえる20,000円分のポイントで、
マイナポイント申請後のチャージやお買い物にご利用いただけます。

STEP1
応募専用サイトにアクセスし、応募書類を記入
STEP2
マイナポイントの申込みをしよう
STEP3
20,000円分
マイナポイントを取得して使おう！

STEP1 下記リンクよりお申し込みください！
https://mynumbercard.point.soumu.jo.●●●●.cn

の部分のリンク
<https://mynumbercard.point.soumu.jo.●●●●.cn/>など

なお、本メールの送信アドレスは「送信専用」ですので、
返信してお問い合わせいただくことはできません。

© マイナポイント事務局

メール文面の例

■画像：偽メールの文面（フィッシング対策協議会）

■出典：ITmedia NEWS
https://www.itmedia.co.jp/news/articles/2303/31/news205.html

■2022年 日本人のサイバー犯罪被害総額 1千億円超 最多遭遇犯罪はフィッシング

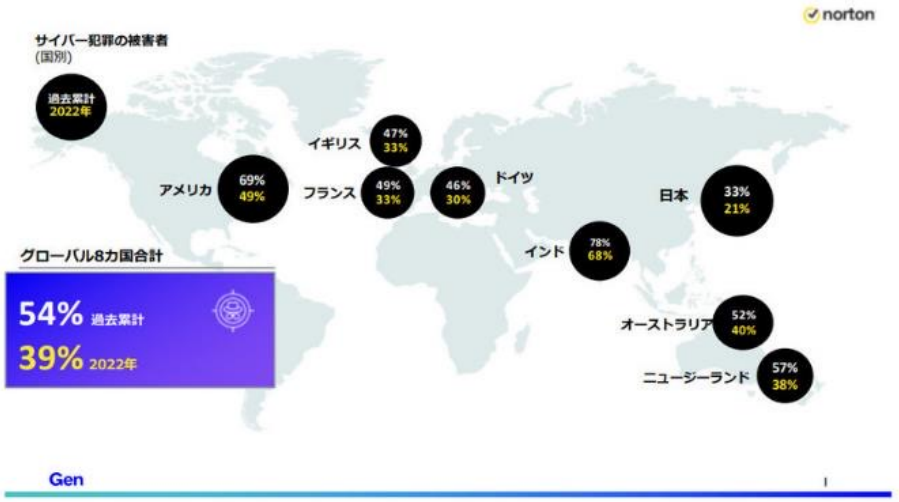
2023年4月6日

・株式会社ノートンライフロックは世界8カ国、8,000人以上の消費者を対象にオンライン調査をした、グローバル調査「ノートン サイバーセーフティ インサイトレポート 2023」の結果を発表した。

・調査対象の日本の成人1,005人の33%が「何らかの形でサイバー犯罪の被害に遭ったことがある」と回答し、21%が「2022年にサイバー犯罪に遭ったことがある」と回答している。

・日本の成人が経験したサイバー犯罪の中で、最も多かったのは「フィッシング詐欺」（20%）で、「コンピュータやモバイル機器のウイルス感染」（16%）、「恐喝メール詐欺」（14%）、「モバイル/SMS詐欺」（13%）と続いた。

・個人情報が流出したきっかけでは、「フィッシングメール」が42%、以下「SNSアプリやウェブサイト」（37%）、「フィッシングテキスト」（28%）、「第三者運営のウェブサイト」（22%）と続いた。



■画像：サイバー犯罪の被害者（ノートン）

あらゆる方法でフィッシング詐欺にあう可能性があります。少しでも怪しいと思ったら、個人情報を入力したりするのはやめて、周りの人やセキュリティの専門家へ相談してみましょう。

■出典：Yahoo!ニュース ScanNetSecurity
https://news.yahoo.co.jp/articles/aaba0189f0b3022f714438b6d71b9f0d489abbb9

■「Google Chrome」の更新失敗を装って、マルウェアを実行させようとする手口に注意！

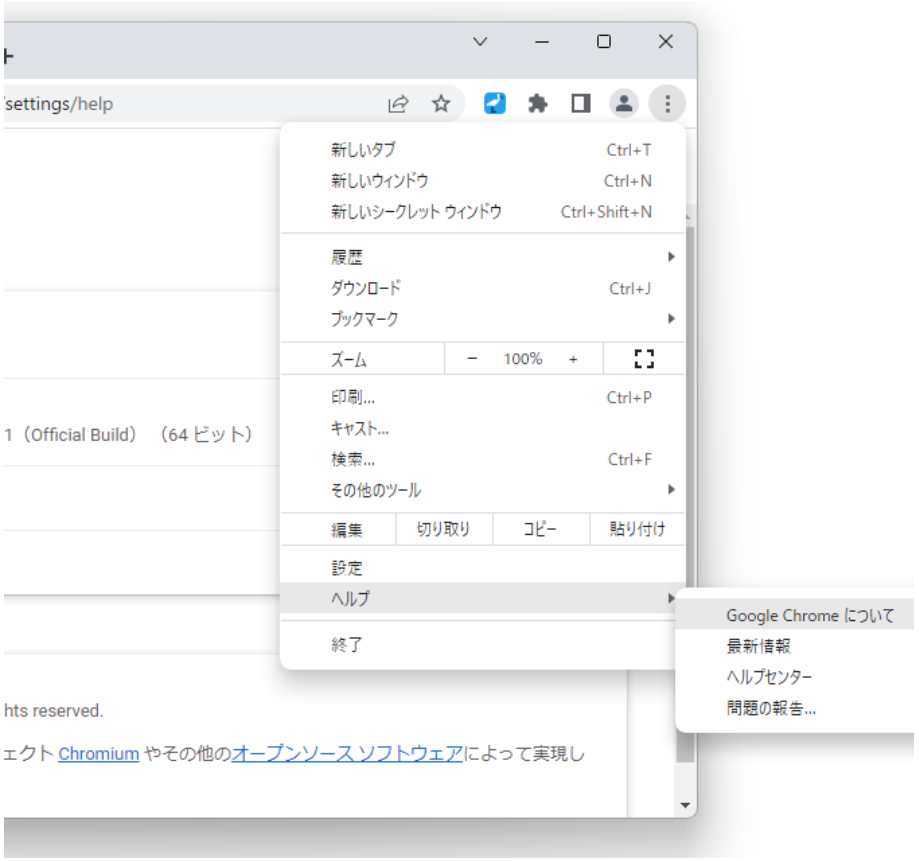
2023年4月19日

・2022年11月頃より、正規のWebサイトを改竄して「Google Chrome」のエラー画面を装った偽のWebページを表示し、そこからマルウェアを配布する攻撃キャンペーンが観測されているとのこと。

・手動でのアップデートを促す偽のエラー画面に従ってダウンロードしたZIPファイルを展開し、実行ファイルを起動してしまうと、PCで暗号通貨モネロ（XMR）の採掘（マイニング）が行われる。

・「Chrome」には自動更新機能が搭載されており、基本的にユーザーがなにか特別なことを行う必要はない。手動で更新する場合も、画面右上のアイコン（縦に3つの点）からバージョン情報画面（chrome://settings/help）へアクセスするだけ。（右図参照）

万が一「Chrome」の更新に失敗する場合は、公式サイトから正規のインストーラーを入手して実行するなどして、常にインストールやダウンロードをする場合は正規ルートからのアクセス・実行を意識しましょう。



■画像：Chromeのバージョン情報画面へのアクセス手順

■出典：Yahoo!ニュース　Impress Watch
https://news.yahoo.co.jp/articles/b5f04f5cb49c1c7a36f3af257a91e6124c844390

■横浜など地方議会にシステム障害　９０以上、サイバー攻撃で

2023年４月13日

・横浜市や広島市、滋賀県など全国９０以上の地方議会の情報システムがサイバー攻撃を受け、インターネット議会中継や議事録検索などのサービスを停止したことが１３日、横浜市などへの取材で分かった。

・システムの運営を担う名古屋市のＩＴ企業のサーバーが、攻撃によって障害を起こした。個人情報の流出は確認していないとしている。

・障害を起こした地方議会の情報システムは、名古屋市のフューチャーインが運営。フューチャーインによると、４月９日に外部からネットを通じ、サーバーに大量のアクセスがあった。

・このようにWebサイトなどのサーバーが処理できないほどの大量のアクセス要求を多数の端末から一斉に送りつけることで、サービス停止に追い込むサーバー攻撃をDDoS(ディードス)攻撃といいます。

■画像：停止した横浜市会のサイト画面

事業にとって、このようなDDoS攻撃も近年増えています。対策が必要と感じる場合は、すぐにセキュリティ担当者へ相談してみましょう。

■出典：東京新聞
https://www.tokyo-np.co.jp/article/243934?rct=national

BASIC Confertas Office

■全日空システム障害 原因は「データベースに負荷」サイバー攻撃、データ流出なし

2023年4月7日

・4/3に全日空の国内線システムの不具合により遅れや欠航が相次いだ問題で全日空は、データベースに負荷がかかりシステムが停止したことが原因であると明らかにしました。

・搭乗手続きなどを行う国内線のシステムの不具合で55便が欠航するなど、およそ2万7000人に影響が出ました。

・国内線の旅客システムは2つのデータベースを同期して運用していますが、予期せぬエラーで片方のデータベースがフリーズ。その影響でデータベースに負荷がかかりシステムが停止したことで、航空券の予約や販売、搭乗手続きができなくなったということです。サイバー攻撃やデータの外部流出はないとしています。

・全日空は、データ処理の方法を変更するなどし、再発防止につとめるとしています。

こちらはサイバー攻撃によるものではないとのことですが、外部からの攻撃だけでなく、社内の情報資産の運用・管理方法も定期的に見直していく必要があるかもしれませんね。

■画像：例
■出典：Yahoo!ニュース　日テレNEWS
https://news.yahoo.co.jp/articles/55c27fe401eb66e099a1a977dd28e563660c6015

■中小企業も使える技術情報管理の自己チェックリスト 経済産業省が公開

2023年4月3日

・技術情報管理自己チェックリストとは、経済産業省によると、技術情報管理認証制度の基準をもとに、事業者が情報セキュリティ対策の状況を自ら確認し、必要な対策を把握するためのツールです。中小企業などが共同研究を進める上で欠かせない技術情報流出防止策を考えるうえで役に立つと説明しています。

・以下のような企業での活用を想定しており、中小企業や情報セキュリティの専属担当者がいない事業者でも利用できます。

- ●これまで情報セキュリティ対策に取り組んだ経験のない事業者が対策を始めるに当たって、まず取り組むべきことを把握したい
- ●これまで情報セキュリティ対策に取り組んできた事業者がこれまでの取組を振り返り、不足が無いかを確認したい

・経済産業省の公式サイトからファイルをダウンロードし、自社の対応状況を確認しながら各チェック項目を選択すると採点され、取り組みが進んでいる対策分野、遅れている対策分野がレーダーチャートで表示されます。

社内の情報管理方法を客観視できるいい機会かもしれません。結果を元にセキュリティ担当者とお話してみましょう。

■画像：経済産業省HP　自己チェックリスト（採点結果の例）
■出典：ツギノジダイ　https://smbiz.asahi.com/article/14876018

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。