PRESS RELEASE

ノートン 広報部

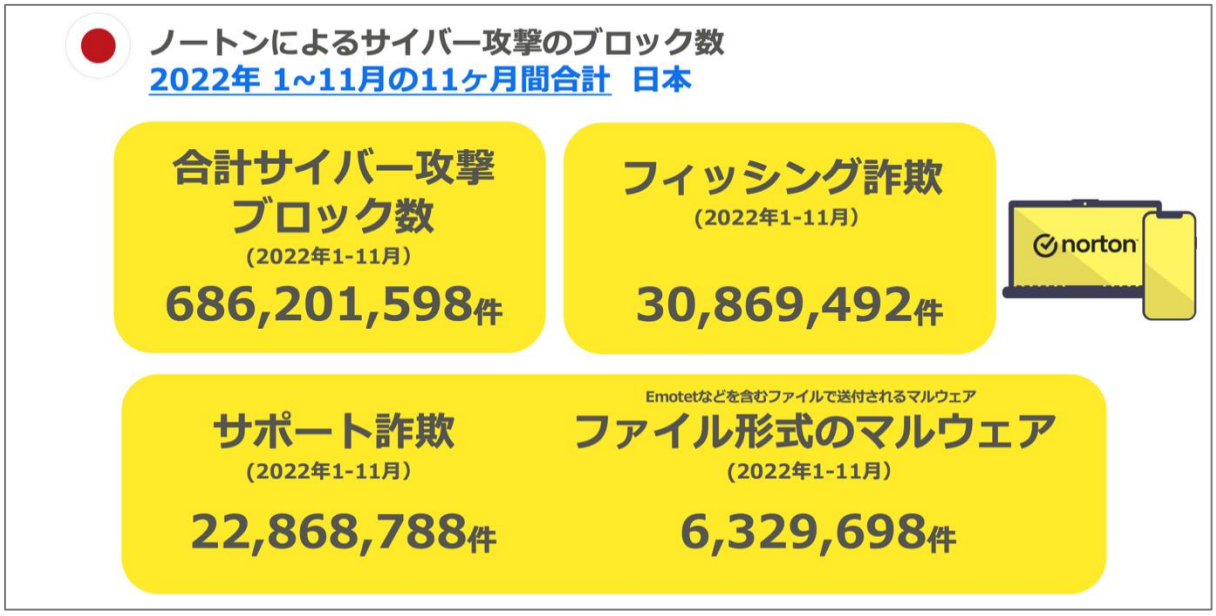
2022 年 12 月 20 日

2022 年 1-11 月 ノートン サイバー攻撃ブロック数レポート

約 6 億 8,620 万件の日本の消費者を狙ったサイバー攻撃を阻止

2022 年の消費者を狙ったサイバー攻撃の傾向、及び 2023 年以降の予想も発表

消費者向けセキュリティブランド「ノートン™」は、2022 年 1-11 月に日本でブロックしたサイバー攻撃数を公表いたします。さらに、「2022 年に日本の消費者の情報・金銭を狙ったサイバー攻撃の傾向 5 選」と「2023 年以降の予想 4 選」を発表いたします。



2022 年 1-11 月に、日本でノートンがブロックした合計のサイバー攻撃数は、約 6 億 8,620 万件(686,201,598 件)です。そのうち、フィッシング詐欺は合計約 3,087 万件(30,869,492 件)、サポート詐欺は約 2,287 万件(22,868,788 件)、Emotet などのようにファイルで送付されるマルウェアは約 633 万件(6,329,698 件)でした。

本レポートは、セキュリティソフト「ノートン」によりブロックしたサイバー攻撃を数値化したものです。レポートには下記が含まれます。

■2022 年 4-11 月各月に、日本にてブロックしたサイバー攻撃の数

■2022 年 1-11 月、日本でフィッシング詐欺に悪用されたブランド/企業ランキング

■2022 年に日本の消費者の情報・金銭を狙ったサイバー攻撃の傾向 5 選

■消費者をターゲットにしたサイバー犯罪 今後の予想 4 選

●2022 年 4 月~11 月各月のサイバー攻撃ブロック数 (日本)

2022 年 4-11 月に日本では、月々平均約 6,077 万件(60,765,412 件)のサイバー攻撃がブロックされ、そのうちファイル形式のマルウェアは、月々平均約 51 万件(513,723 件)、フィッシング詐欺は月々平均約 318 万件(3,184,673 件)、サポート詐欺は月々平均約 169 万件(1,689,540 件)ブロックされました。フィッシング詐欺は、5 月以降は各月 300 万件以上をブロックしました。サポート詐欺に関しては、5 月に 500 万件以上、6 月に 400 万件近くブロックしており、多くの日本人がネットサーフィン時にサポート詐欺サイトに遭遇したことが確認されています。

ノートンによるサイバー攻撃のブロック数(2022年4~11月)日本

【日本】ノートンによるサイバー攻撃のブロック数	4月	5月	6月	7月	8月	9月	10月	11月
合計サイバー攻撃ブロック数(月)	61,647,420	67,116,952	60,415,294	58,920,029	58,995,586	58,374,942	56,137,181	64,515,891
1日平均 *1ヶ月間の1日毎のブロック数から割り出した平均値	670,081	2,165,063	2,013,843	1,900,646	1,903,083	1,945,831	1,810,877	2,150,530
ファイル形式のマルウェア	754,955	478,600	586,969	475,595	517,130	483,791	414,926	397,815
フィッシング詐欺	1,946,156	3,408,860	3,074,749	3,340,053	3,784,656	3,328,847	3,448,964	3,145,099
サポート詐欺	128,567	5,202,135	3,870,097	933,632	1,221,695	1,101,110	717,830	341,255

norton *2022年4月より前に関しては、日本の月々の数字はお出ししておりません。前ページ5-11月の合計は含んでおります。 4

*月々のブロック数は、2022 年 4 月分以降のみお出ししております。

*日本以外での国々でのブロック数、比較、グラフなど詳細に関しましては、PR 事務局へお問合せください。

●2022 年 1 月~11 月 最もブロックされたフィッシング詐欺(日本)

【日本でフィッシング詐欺に悪用されたブランド/企業ランキング】

	フィッシング詐欺に悪用されたブランドランキング 上位10位 (日本) 2022年1-11月の11ヶ月間
1位	ヤフー
2位	インスタグラム
3位	サポート詐欺・偽セキュリティ通知
4位	エクセル ファイルのダウンロードサイト(Emotet関連含む)
5位	イオンカード
6位	楽天
7位	三井住友銀行
8位	JCBカード
9位	アマゾン
10位	えきねっと（JR東日本）

***日本のノートンユーザーのデバイスでブロックされたフィッシング詐欺に基づいたランキング**

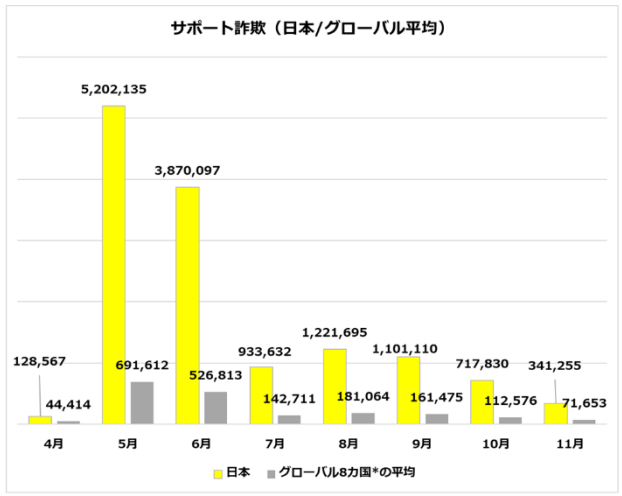
2022 年 1-11 月に日本では、多くのフィッシング詐欺が確認されましたが、表は、その中でも最も多かったフィッシング詐欺を「悪用されたブランド・企業」ごとにまとめ、ランキングにしたものです。サポート詐欺やエモテットに関連するサイト(マルウェア感染するエクセルファイルをダウンロードさせるサイト)に加え、大手検索サイト、SNS、クレジットカードブランドや通販サイトなどがランクインしました。通販サイトや新幹線予約サイトなどに関しては、クレジットカード情報を含む個人情報の詐取および不正購入を目的としていることが想定されます。

●2022 年に日本の消費者の情報・金銭を狙ったサイバー攻撃の傾向 5 選

2022 年の消費者をターゲットとしたサイバー犯罪は、日本人が関心がありそうな企業等を装い、手の込んだ偽ページ・アプリを作成、さらには、デジタル広告の出稿や公式アプリストアへの掲載を行うなど、大胆かつ詐欺を行うまでのプロセスに手間をかけている印象でした。

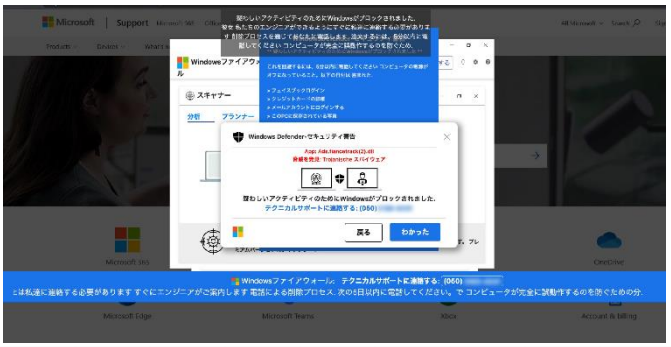
■【傾向 1】日本の消費者をターゲットとする「サポート詐欺」が増加。

2022 年 1 月～11 月に、ノートンが日本でブロックしたサポート詐欺の件数は、約 2,287 万件とフィッシング詐欺のブロック件数(約 3,087 万件)と大きく変わらない件数でした。月ごとのブロック数(2022 年 4 月~11 月）においては、日本でのブロック件数が、主要 8 カ国[*1] と比較し圧倒的に多く、ノートンユーザーが 1 番多いアメリカと比較しても、桁が 1 つ違う月もありました。2021 年頃は、各言語に翻訳された同様のサポート詐欺ページが世界中で確認されましたが、より多くの日本人が、詐欺の電話番号へ電話をしてきたためか、日本を集中的にターゲットとし詐欺行為を強化した可能性があります。



*主要8カ国：日本、オーストラリア、フランス、ドイツ、インド、ニュージーランド、イギリス、アメリカ

*表/グローバル平均について：日米はノートンのユーザー数が多い一方、日米ほど多くない国もあるため、グローバルの平均値が日本と比較し低く/高く見える場合があります。



サポート詐欺	日本	オーストラリア	フランス	ドイツ	インド	ニュージーランド	イギリス	アメリカ
4月	128,567	4,222	15,854	5,677	314	1,674	10,978	188,027
5月	5,202,135	19,623	15,230	15,385	1,211	3,062	21,603	254,643
6月	3,870,097	17,184	4,868	10,159	761	2,524	13,540	295,374
7月	933,632	7,356	4,363	6,774	337	2,309	4,379	182,537
8月	1,221,695	5,746	4,426	8,023	390	2,487	4,828	200,915
9月	1,101,110	4,548	4,678	10,763	790	2,524	5,060	162,324
10月	717,830	5,594	7,406	14,761	351	1,217	6,015	147,434
11月	341,255	26,542	8,420	24,162	1,532	1,444	11,316	158,554

*1 日本、オーストラリア、フランス、ドイツ、インド、ニュージーランド、イギリス、アメリカ

*サポート詐欺実験映像 https://youtu.be/ByKbEoMCuac

■【傾向 2】日本の消費者をターゲットとする「ロマンス詐欺」が多く確認され、逮捕事例も。

2021 年に、アメリカでは年間で過去最高の被害額 5 億 4700 万ドル(約 601 億 7000 万円[*2])を記録し、日本でも相談件数が増加していると報告[*3] があったロマンス詐欺ですが、2022 年も引き続き確認され、ロマンス詐欺師が国内で逮捕される事案も発生しました。

以前は、海外駐在をしていて一時的に今お金に困っている(例:口座からお金が引き出せない）や日本へ送った荷物の関税費用を一時負担してほしいなどが金銭要求の主な手口でしたが、近年は「仮想通貨を詳しいから教えてあげるよ」と丁寧に投資を教えるフリをし詐欺サイトへ誘導する手口や、「海外にいてスマホを壊してしまって連絡ができなくなるからスマホの購入代金を送ってほしい」とギフトコードを 10 万円分ほど依頼する手口(貯蓄が多くない若年層ターゲットの可能性）が確認されています。さらには「宇宙ステーションにいて地球に帰る費用を出してほしい」という手口まで、常に詐欺手法をアップデートしていることが伺えます。

ノートンでは、2021 年 12 月-2022 年 1 月に架空の人物の SNS アカウントを作り実験をした結果、11 人以上のロマンス詐欺師から連絡を 1 ヶ月半で受けましたが、その後も多数の詐欺師からアプローチを受けました。*実験に関する詳細については、PR 事務局までお問いわせください。

*2 https://bit.ly/3FzOaXh https://bit.ly/3Puaoye *3 https://www.kokusen.go.jp/news/data/n-20220303_2.html

■【傾向 3】テンプレートを使いまわしたような、同じ手法の SMS 詐欺(ショートメールのフィッシング詐欺・スミッシング）が確認される。

テンプレートを使いまわしたような詐欺 SMS が、2022 年はたびたび確認されました。携帯キャリア会社各社や、国税庁などをかたり「未払金がある」との警告ポップアップメッセージが表示され、「支払い期限」としてページ上にはページを開いた日付が表示され、ギフトコードによる支払いを求めます。

こちらのタイプの SMS は、Android スマホで開いた場合と iPhone で開いた場合で誘導先が異なり、Android スマホの場合は、偽アプリをダウンロードさせるパターンも確認されています。

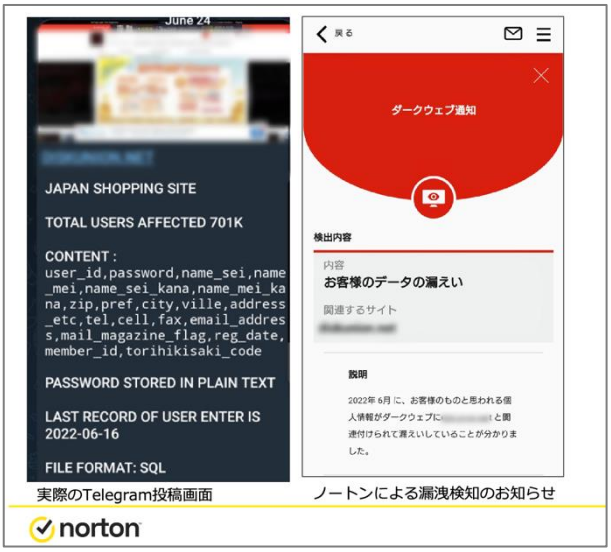
■【傾向 4】偽サイトがデジタル広告を利用することで、ウェブの検索結果で、正規サイトより上位に表示されるケースや、偽アプリが正規ストアで公開される事案が発生。

2022 年は、たびたび偽サイトが広告出稿(リスティング広告）をしていることにより、ネットの検索結果で、正規サイトよりも上に表示されるケースが確認されました。身近な家電の公式サイトや、新幹線の切符を購入する「えきねっと」の偽サイトが確認されており、「えきねっと」においては2022年10 月に一度確認されていましたが、再度 2022 年 12 月上旬にも検索結果の最上位に表示されました。帰省ラッシュの年末年始の新幹線予約を 1 ヶ月前の 11 月末~12 月上旬に行う消費者が多いことを想定し、このタイミングを狙い再掲載した可能性があります。新幹線の切符を不正購入をされた被害なども SNS 等で多数報告されています。また、2022 年は偽アプリが公式アプリストアに掲載された事案も確認されています。「公式アプリストアに掲載されていれば安心だ」と思う消費者の心理を突く狙いがあると思われます。

*実際の詐欺サイトのイメージです。悪用されたブランド・企業は無関係です。

■【傾向 5】企業等による情報漏洩。USB 等の紛失やメールの誤送信から、サイバー攻撃まで幅広いきっかけで情報漏洩が懸念される事案が発生。ダークウェブへの漏洩を調査したケースや、SNS のテレグラムに漏洩した情報が無料で公開された件も。

2022 年は、サイバー攻撃だけではなく、個人情報を含む USB メモリー紛失[*4]や類似した偽ドメイン(ドッペルゲンガードメイン）にメールを誤送信[*5] するなどのミスによる情報漏洩疑惑の事案がありました。



情報漏洩をした可能性があることから、ダークウェブを調査したケースなどもありました。また、実際に SNS の Telegram(テレグラム）で企業から漏洩した日本人の個人情報が公開されていることも確認されています。(ノートンでは、こちらの漏洩に個人情報が含まれていたユーザーに対してダークウェブモニタリング機能により漏洩通知をアプリ等でお送りしました。）最近では、漏洩した個人情報をダークウェブで取引するだけではなく、テレグラムなどで一部無料公開しているケースが確認されています。

*4 https://bit.ly/3FXHxj2　*5 https://bit.ly/3uUoGPy

●消費者をターゲットにしたサイバー犯罪 今後の予想 4 選

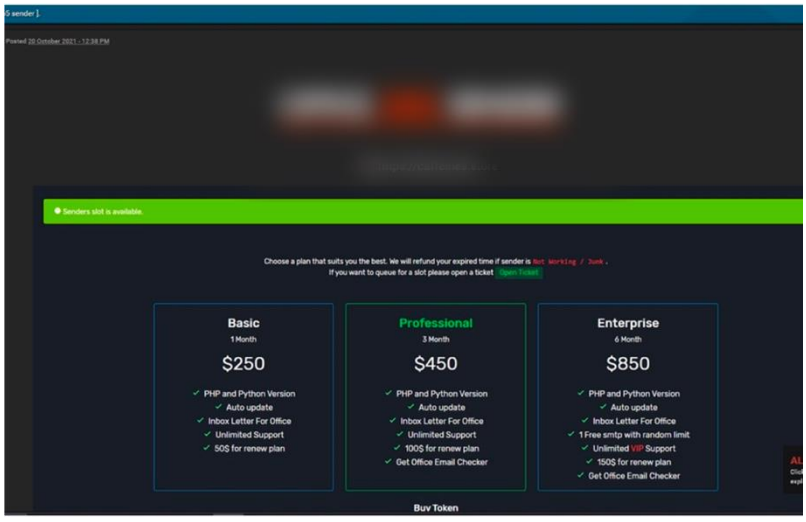
■【予想 1】オンライン上のサイバー犯罪や情報漏洩と、オフラインの犯罪行為を掛け合わせた犯罪が増える可能性。

2022 年 7 月に、日本在住の会社経営者の男性が知らない間に携帯電話を解約され、電話番号を詐取・悪用され、さらにはインターネットバンキングから約 1 千万円を、知らない別口座に不正に振り込まれる事案が発生しました。男性を名乗る人物が携帯ショップへ来店し、本人確認書類として運転免許証を提示し解約をした上で、電話番号を他のキャリアに変更する手続きを行ったとのことです。インターネットバンキングに関しては、高額出金のため、銀行から確認の電話をしたようですが、既に電話番号は詐欺師に渡っていたため、被害者本人へは確認の連絡が届かなかったとのこと。[*6] この事案に関しては、調査の結果、フィッシング詐欺やパスワードの使い回しなどが原因として疑われるようですが、身分証や個人情報などは企業等から漏洩してダークウェブ等で取引されるケースもあります。

このようなオンラインのサイバー犯罪・情報漏洩に加え、日本国内の店頭に来店し不正に携帯電話の解約手続きを行うなどのオフラインの犯罪を組み合わせた手口は巧妙で、今後も注意が必要です。パスワードを推測されづらいものにし、使い回しをせず、フィッシング詐欺をブロックするセキュリティ機能や、漏洩を知らせるダークウェブモニタリング機能などを活用し、悪用される前にカードやログイン情報を変えるなど対処が必要です。また身分証の画像をアップロードする先のサイトが偽サイトではないか、SNS やホームページなどに自身の情報を載せすぎていないかなど日常で注意を払うようにしましょう。

*6 https://bit.ly/3j11zQp

■【予想 2】サイバー攻撃を容易にするサブスクサービスを犯罪者が活用することで、フィッシング詐欺などサイバー攻撃が増加する可能性。



サイバー犯罪者間では、ダークウェブ上で、サイバー犯罪のマニュアルやトレーニングが売買されている他、ランサムウェア攻撃を容易にするランサムウェアの提供サービス(RaaS：ランサムウェアアズアサービス)やフィッシング詐欺を行うことを容易にするフィッシングのサービス（PhaaS：フィッシング・アズ・ア・サービス）があります。フィッシングのサービス(PhaaS)は、フィッシング詐欺のキットの用意や、リダイレクトするページの管理などフィッシング詐欺を行う上で必要な機能を包括的に提供するサブスクリプションサービスですが、かつてはダークウェブのフォーラム上で推薦や紹介を受けなければ利用できませんでした。

しかし、2022 年 10 月ごろに見つかった新プラットフォームの「Caffeine(カフェイン）」は、サブスク費用さえ払えば誰でも利用ができ、英語以外の一部言語にも対応をしているため、フィッシング詐欺を容易に誰でも始めることができ、今後このようなサービスを活用することでサイバー攻撃が増えることが懸念されます。

■**【予想3】AI画像メーカーやディープフェイク（偽映像や音声作成）ツールなど、最新のテクノロジーを駆使することで、2023年以降もロマンス詐欺が増加する可能性。**
2022年後半に日本のSNS上でもAIの画像メーカーが話題になりましたが、画像の内容を伝えるだけで、それに合致するイメージ画像を作成してくれるAIツールは、ロマンス詐欺にも悪用される可能性があります。偽の音声や合成映像を簡単に作れるツールも誕生していますが、以前からロマンス詐欺師はディープフェイク映像や、SNSに投稿されている自撮りの配信映像などを詐欺の連絡に悪用していたため、今後も最新のツールを駆使して、容易に新たな架空の人物のSNSアカウントを作っては捕まる前に消すことを繰り返す可能性があります。ロマンス詐欺師の詐欺行為にかかる手間やハードルがテクノロジーにより軽減され、より巧妙かつ効率的になることが考えられます。

■**【予想 4】2023 年新たにオープンする話題の映画テーマパークや、話題のスポーツイベントに乗じた詐欺が登場する可能性。**
2023 年に、日本では人気映画のテーマパークが夏にオープンを予定しており、世界では「ラグビーワールドカップ 2023」が 9-10 月に開催されますが、人々が情報を求めてネット上で検索するような人気イベントに乗じたフィッシング詐欺等を行うのがサイバー犯罪者の常習手口です。サッカーのワールドカップや人気ネット番組をかたる偽サイトなども 2022 年では確認されているため、2023 年もイベントごとに乗じた詐欺に注意が必要です。「(他では売り切れている）チケットを買えます」や「映像が見れます」「グッズを買えます」などをかたる偽サイトが登場する可能性があります。

■**【その他】**
・**旅行**が 2023 年以降はさらに増えるため、旅行予約関係の偽サイト等にあらためて注意が必要です。
・**マイナンバー**を利用する機会が増えますが、漏洩には注意しましょう。マイナンバーの入力やカードの写真を求めるサイトは、偽物ではないかをよく確認してから情報を提供しましょう。(漏洩を通知してくれるダークウェブモニタリング機能の利用も有効です。）
・**物価上昇**に伴い、「**節約**や**投資**をしよう」と考える消費者をターゲットとした詐欺サイトや DM などでの勧誘には注意しましょう。
・2022 年に引き続き、**ウェブ検索結果の最上位に偽サイトが表示されたり、公式アプリに偽アプリが掲載**される可能性もあるため注意が必要です。

●ノートン製品情報

■パソコン、スマホをオールインワンで守るセキュリティソフト

ノートン™ 360：https://jp.norton.com/360

ノートン 360 は、パソコン、スマホ、タブレットなどのデバイスと Wi-Fi 通信等をオールインワンで守るセキュリティソフトです。詐欺サイトやウイルスなどサイバー攻撃の脅威を検知し、防御する他、インターネット利用時に通信内容を盗み見されないように暗号化する VPN 機能を搭載。その他お子様を守るための保護者機能、個人情報流出を検知するダークウェブ モニタリング機能、パスワードを安全に管理するパスワードマネージャー機能など、消費者の皆様が、より快適かつ安全にインターネットを利用できるようになる機能を多数搭載しています。

*ノートン 360 スタンダード版には、保護者機能とダークウェブモニタリング機能の搭載なし。

■個人情報の流出を検知し、メールとアプリで通知、被害時に 365 日電話でサポート！

ノートン™ ID アドバイザー：https://japan.norton.com/dwm/
ノートン 公式ストア：https://nr.tn/3iuW3li

流出した個人情報は、ダークウェブにて売買され、不正利用される可能性があります。ノートンはインターネットをパトロールし、お客様の個人情報が流出した場合、メールとアプリでお知らせします。また、SNS アカウントの乗っ取り、フィード内の危険なリンクや不適切コンテンツを警告します。個人情報の不正利用被害にあった場合は、365 日復旧支援スペシャリスト(日本拠点）がトラブル解決をサポートします。関連機関と三者通話を行い、サポートさせていただく場合もございます。

*対象 SNS 等、機能の詳細は HP をご確認ください。

●ノートンについて

ノートンは、サイバーセーフティのブランドである、Norton、Avast、LifeLock、Avira、AVG、ReputationDefender、CCleaner を通じて、デジタル化が進んだ世界においてもサイバー犯罪などの危険を心配せず、自由にデジタルを使いこなせる環境、「デジタルフリーダム」の実現に力を注ぐグローバル企業「ジェン デジタル社（NASDAQ：GEN)」の主要サイバーセーフティブランドです。人々が安全に、プライバシーが保たれ、自信を持ってデジタルライフを送ることができるよう、これからの時代もサポートしてまいります。ジェン デジタルは、サイバーセキュリティ(インターネット利用の保護)、プライバシー保護、個人情報対策の分野で受賞歴のある製品とサービスを、150 カ国以上の 5 億人以上のユーザーに提供しています。詳しくは、Norton.com と GenDigital.com をご覧ください。