PRESS RELEASE

ノートン 広報部

2021 年 12 月 9 日

1 ヶ月に世界全体で平均約 3 億件のサイバー攻撃をブロック！
日本で急増！「テクニカルサポート詐欺」の増加が顕著に
サイバー犯罪傾向振り返りレポート 2021
2022 年のサイバー犯罪予測 3 選も

株式会社ノートンライフロック（本社：東京都港区赤坂）は、「ノートン」ブランドのセキュリティ製品で検知したサイバー攻撃のデータを元に、2021 年のサイバー犯罪トレンドの振り返り及び、2022 年のサイバー犯罪トレンド予測を発表いたしました。

【サマリー】2021 年サイバー犯罪の傾向（世界全体）

・世界全体で、ノートンは 1 ヶ月に平均約 3 億件のサイバー攻撃をブロック（1 月～10 月）。特に 2021 年 10 月は 3 億 5,000 件を突破し、前年同月比 151%の攻撃を確認。

・偽サイト等に個人情報を入力させ、盗みとる「フィッシング詐欺」が増加傾向に。2021 年 10 月には世界全体で、前年同月比 278%を記録。日本では「2 回目の特別給付金特設サイト」といったような、コロナ禍に乗じた不正行為も引き続き確認された。

・パソコンが危険な状態にある等のエラーメッセージを出すことで恐怖心を煽り、偽の IT サポートに電話をするよう促す、「テクニカルサポート詐欺」の増加が顕著に。日本は検知件数が主要国[*1]で最多であった。

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

【サマリー】2022 年以降のサイバー犯罪の予測 TOP3 選（世界全体）

・仮想通貨を狙うサイバー犯罪

・人工知能（AI）や機械学習を活用したサイバー犯罪

・コロナのもたらしたデジタルシフトに便乗するサイバー犯罪

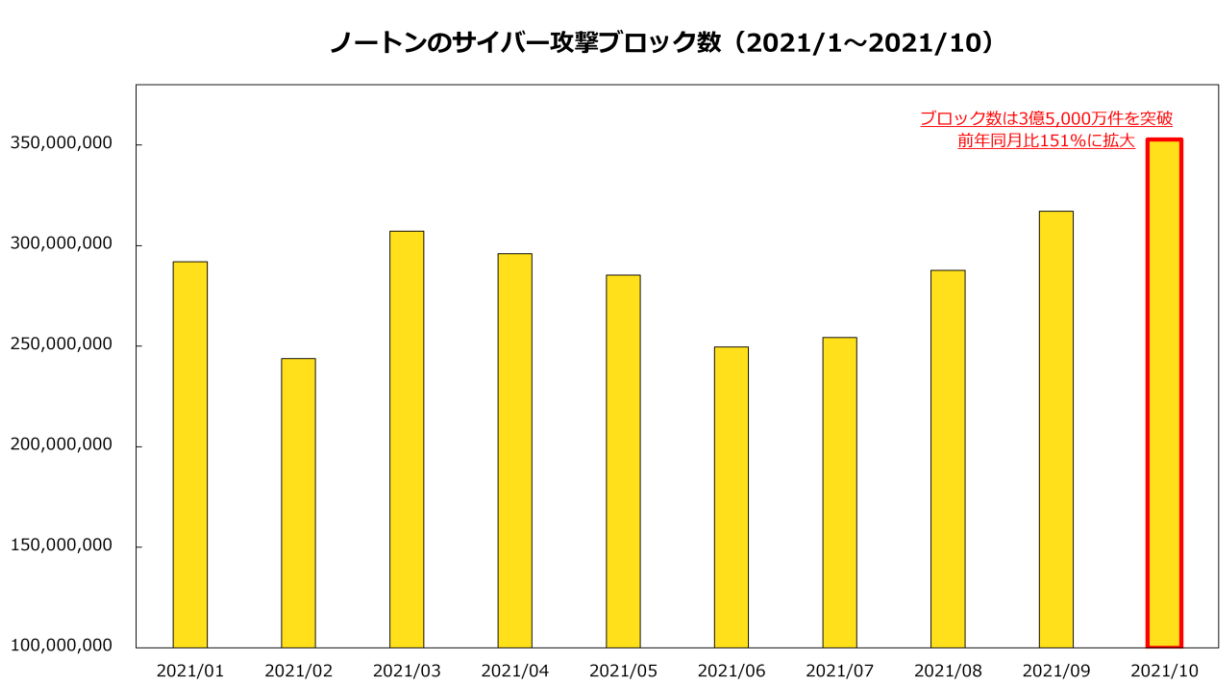
2021 年サイバー犯罪の傾向(世界全体)

・世界全体で、ノートンは 1 ヶ月に平均約 3 億件のサイバー攻撃をブロック（2021 年 1 月～10 月）

ノートンでは、世界全体で、1 ヶ月に平均約 3 億件以上のサイバー攻撃をブロックしました（2021 年 1 月～10 月）。特に 2021 年 10 月は 3 億 5,000 件を突破し、前年同月比 151%の脅威が確認されました（2020 年 10 月：198,786,313 件）。

この背景には、コロナ禍での生活の変化があると考えられます。在宅時間の増加により、インターネット・トラフィックが前年比 500%以上を記録する[*2]等、急速なデジタルシフトが進みました。あわせて、ネットショッピングの利用割合も増加[*2]傾向にあり、慣れない中で利用している人も多いことが想定されます。そのため、オンラインサービスに慣れていない消費者をターゲットとしたサイバー犯罪が増加したと考えられます。

*2 総務省：令和 3 年 情報通信白書（https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/n2100000.pdf）



・偽サイト等に個人情報を入力させ、盗みとる「フィッシング詐欺」が増加傾向に。2021 年 10 月には世界全体で、前年同月比 278%を記録。日本では「2 回目の特別給付金特設サイト」といったような、コロナ禍に乗じた内容も 2020 年から引き続き確認された。

2021 年、ノートンは世界全体で、1 ヶ月に平均約 420 万件のフィッシング詐欺を検知しました（2021 年 1～10 月）。検知されたフィッシング詐欺の数は、2021 年 10 月には昨年同月比 278%を記録しており、増加傾向にあります（2020 年 10 月: 1,322,700 件、2021 年 10 月: 4,352,273 件）。日本では、2021 年 7～9 月の 3 ヶ月間で、5,385,537 件のフィッシング詐欺が確認されおり、主要国別[*1]ではアメリカに継ぎ 2 番目に多い結果となりました（アメリカ：5,703,065 件）。

今年も昨年に引き続き、世界的に、コロナ禍に乗じた詐欺が見受けられました。世界中でワクチン摂取が開始した年だったため、ワクチン予約に関するフィッシング詐欺や、給付金・税金の還付等に関するフィッシング詐欺が確認されました。中には総務省を装い「2 回目の特別給付金特設サイト」をかたるサイト[*3]も見られました。今後も給付金等が出る際には、乗じた詐欺が発生する可能性が高く、引き続き注意が必要です。詐欺等による個人情報漏洩を防ぐためには、リンクをクリックする前に、メールアドレスや URL に違和感がないかを確認する他、危険サイトを検知するセキュリティソフトを利用する等の対策が重要です。

*3 フィッシング対策協議会：特別定額給付金に関する通知を装うフィッシング
（https://www.antiphishing.jp/news/alert/kyufukin_20210824.html）

・パソコンが危険な状態にある等のエラーメッセージを出すことで恐怖心を煽り、偽の IT サポートに電話をするよう促す、「テクニカルサポート詐欺」の増加が顕著に。日本は検知件数が主要国[*1]で最多。

テクニカルサポート詐欺は、ウェブ上のポップアップ通知等で、「パソコンがウイルス感染等で危険な状態にあり、すぐにサポートに連絡する必要がある」などの偽のエラーメッセージを出し、通知にある番号に電話を促す詐欺です。電話をすると、詐欺師が遠隔サポートを申し出、修理とセキュリティ使用料として費用を請求します。2021 年 7～9 月の 3 ヶ月間、日本だけで 950 万件以上のテクニカルサポート詐欺が、ノートンによって検知されました。主要国別[*1]では一番多い件数で、2 番目に多いアメリカとは約 800 万件の差がありました。

コロナ禍でリモートワークが求められたものの、日本においては馴染みが薄かったことにより、他国よりもターゲットになりやすく、件数が増えたことが考えられます。詐欺に引っかかってしまい、デバイス、ネットワーク、個人情報のセキュリティ対策をしていなかった場合、金銭的な被害に遭う可能性があります。アフターコロナにおいても、リモートワークが一般化していく可能性があるため、今のうちにセキュリティ環境を整える必要があります。

2022 年以降のサイバー犯罪トレンド予測 3 選（世界全体）

・仮想通貨を狙うサイバー犯罪

2021 年は、仮想通貨事業を手掛ける企業が続々と NASDAQ 上場を果たしました。メジャーになっていくにつれ、仮想通貨を使い始める人は増える可能性があります。初心者はサイバー犯罪のターゲットになりやすい可能性があり、注意が必要です。

2021 年 11 月には NASDAQ 上場企業から、全顧客の 1/3 に相当する 700 万人の顧客データが流出しました。今後、盗まれたメールアドレスや氏名を悪用したサイバー犯罪が発生する可能性があります。

・人工知能（AI）や機械学習を活用したサイバー犯罪

音声や映像データから特定の人のフェイク音声・映像を生成する「ディープフェイク」という技術が、近年では犯罪に活用され始めています。社員になりすまし、偽の音声で電話をして会社のお金を引き出すことに成功した事例もあり、今後技術がより発展し、よりクリアな音声を生成できるようになった際には、本物との区別がさらに難しくなるため、ディープフェイクを利用した犯罪が増える可能性があります。

また、機械学習を応用して、漏洩している個人情報のデータからプロファイリングをし、「詐欺に引っかかりやすい人」を割り出し、「ターゲットリスト」を作ることが、サイバー犯罪者の常套手段になりつつあります。合わせて、ターゲットが利用しているオンラインサービスを割り出し、適したサイバー犯罪手法を推察するなど、データを活用した効率的な詐欺手段が出てきており、今後も増えることが予想されます。

・コロナのもたらしたデジタルシフトに便乗するサイバー犯罪

2021 年のトレンドにもあったように、コロナ禍に乗じたサイバー犯罪は、コロナ禍での生活変容に合わせ、今後も継続していくことが予測されます。今後、GoTo キャンペーンの再開時や、デジタルのワクチンパスポートが本格的に始動する際には、それらに乗じた詐欺が発生する可能性があるため、注意する必要があります。

また、コロナ禍がもたらしたデジタルシフトにより、身分証を始め、個人情報をオンラインでやり取りする機会が増えました。例えば EU は 2030 年までに加盟国の国民の 80%がデジタル身分証（eID）を利用することを目標としています。日本でもデジタル庁が設立された頃により、マイナンバーカード機能のスマートフォンへの搭載他、今後も本人確認のデジタル化等が進むことが予測されます。オンラインでの個人情報のやり取りが増えるため、流出対策等が必要です。

●ノートンライフロック について

ノートンライフロック社(NASDAQ：NLOK(日本法人：(株)ノートンライフロック))は、消費者向けサイバーセーフティのグローバルリーダーです。人々がデジタルライフを安全に暮らせるように守り、後押しします。複雑に繋がる世界において、私たちは消費者の信頼できる味方です。私たちがサイバーセーフティをどのように変革しているかについて詳しくは、www.NortonLifeLock.com をご覧ください。