# 日本を標的としたサイバー攻撃：2020 年の概観と 2021 年への予測

株式会社テリロジーワークス

# Contents

# イントロダクション

2020 年は新型コロナウイルス感染症の年でした。パンデミックが全世界に広がり、日々の感染者数の増加が国境通過や往来の制限、都市のロックダウン等を引き起こす中で、我々は仕事の面でも私生活の面でも、「新しい生活様式」の導入を迫られました。

今年一年を通して、多くの企業や個人がその「新しい生活様式」に順応しようと努力していた一方、サイバー犯罪者はその状況を利用し、できるだけ多くの利益を上げるために、悪意ある活動を行っていました。

一般的に、サイバー犯罪者がその標的を選ぶ際に重要視するのは、その標的がどの程度攻撃に対して脆弱かであり、特定の国や企業を特別に標的に選ぶことはありません。一方で、政府等の組織によって支援されていると考えられている APT（Advanced Persistent Threat）グループは、その目的の達成のために特定の国や産業を選んで攻撃をすることが知られています。例えば、ロシアやイランの APT グループは、米国や英国に所在する組織を狙うことが多く、中国や北朝鮮のグループは東アジア地域諸国を標的にすることが多い、などです。しかし、このことは、例えば中国のグループが EU 諸国を標的にせず、イランのグループが東アジアを標的にしないという事を保証するものではありません。

これらの攻撃について公開されている情報から判断すると、日本並びに日本企業はそれらグループによって真っ先に狙われる標的というわけではありません。しかしながら、オリンピック・パラリンピックが 2020 年に開催される予定だったこともあり、今年は日本企業が従来よりも様々なサイバー攻撃の標的になるだろうと予想されていました。

オリンピックは昨今の情勢により、幸か不幸か 2021 年に延期になりました。しかしそのことは、攻撃者の準備期間がその分だけ長くなるという事を意味しています。従って、2021 年夏までに行われるであろう、APT グループやサイバー犯罪者を始めとした、様々な脅威アクターによる攻撃に、日本全体で備えなければなりません。

このホワイトペーパーは、2020 年現在における日本を取り巻くサイバー脅威の現状を概観し、その傾向の解説を示した上で、2021 年に向けての予測を行うことを目的としています。

# COVID-19 関連のフィッシング、詐欺

## 2020 年 概観

新型コロナウイルス（COVID-19）は、ビジネス活動や私生活での行動を含め、多くの面での変化を我々にもたらしました。例えばビジネス領域においては、リモートでの面談やテレビ会議、テレワーク等が大規模に導入されましたが、多くの場合それは事前準備の少ない中短時間で行われざるを得ませんでした。また、ウイルスについての情報や対処法が不透明な中、人々は不安に苛まれ、できるだけ多くの情報を集めようとしました。

これらの急速な変化とそれに伴う精神的な不安が、サイバー犯罪者に付け入る隙を与えました。彼らは、新型コロナウイルスやテレワーク関連の情報が記載されたファイルやリンクを含むメールをスパム的に拡散し、それらを不安に思う人々を攻撃対象としたのです。

サイバー犯罪者が、その時盛んに議論されている話題を悪用してフィッシングや詐欺行為を働くことは非常によくあることです。彼らはその話題を利用して、メール受信者の感情を揺さぶり正常な判断力を失わせようとします。そして彼らの望む行動、例えば個人情報の入力やマクロ付ドキュメントの開封などをメール受信者に行わせ、目的を達成します。2020年で最も議論された話題は勿論新型コロナウイルスでしょうから、それに伴って関連するフィッシングが増加したことは不思議ではありません。

これらの攻撃の恐ろしい点は、高度なスキルを持った脅威アクターだけでなく、あまり経験のない者でもこれらの攻撃を比較的に実行することが可能であるということです。例えば、フィッシングを行うためのツールセットなどは、GitHub 等に「教育目的」でアップロードされている他、在野にはそれらと同等以上の機能を持つだろうフィッシングキットが、大体 10 ドルから 100 ドルで売買されています。

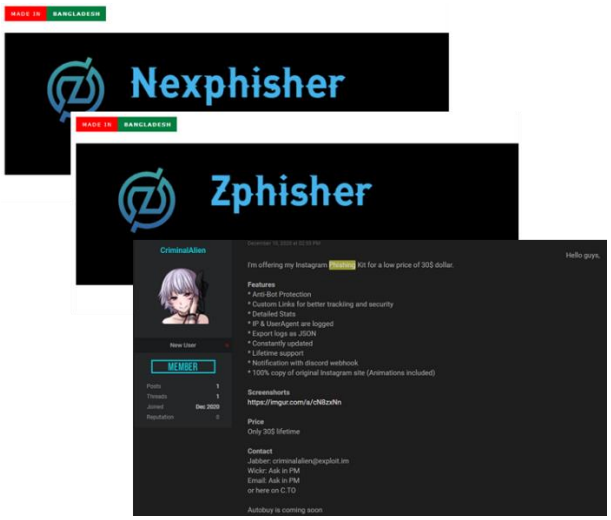



*図1 フィッシングキットが売買されているフォーラム*

勿論、高度な脅威アクターはその技術を活かし、より判別しにくいフィッシングメールやランディングページを作成します。下の画像の例は Amazon に扮したフィッシングメールですが、日本におけるフィッシングメール対策でよく言われるような漢字や文法の間違いなどは無く、それらの視点からでは非常に分かりづらいものとなっています。


amazon.co.jp プライム

Amazon お客様

Amazon に登録いただいたお客様に、Amazon アカウントの情報更新をお届けします。
残念ながら、Amazon のアカウントを更新できませんでした。
今回は、カードが期限切れになってるか、請求先住所が変更されたなど、さまざまな理由でカードの情報を更新できませんでした。

アカウント情報の一部が誤っている故に、お客様のアカウントを維持するため Amazon アカウントの 情報を確認する必要があります。下からアカウントをログインし、情報を更新してください。
**Amazon ログイン**

**なお、24時間以内にご確認がない場合、誠に申し訳ございません、お客様の安全の為、アカウントの利用制限をさせていただきますので、予めご了承ください。**

アカウントに登録のEメールアドレスにアクセスできない場合
お問い合わせ： Amazonカスタマーサービス。

お知らせ:

- パスワードは誰にも教えないでください。
- 個人情報と関係がなく、推測しにくいパスワードを作成してください。大文字と小文字、数字、および記号を必ず使用してください。
- オンラインアカウントごとに、異なるパスワードを使用してください。

どうぞよろしくお願いいたします。
Amazon

*図2 一見で見分けのつかないフィッシングメール*

新型コロナウイルス関連の話題がサイバー犯罪者によってどの程度用いられているのか、新規取得されたドメイン数から見てみましょう。図 3 は、各月に新規登録された、“covid”

という文字列を含むドメインのうち、悪意があると判断されたドメインの数を示しています[1]。サイバー犯罪者達はこれらのドメインを用いて、新型コロナウイルス関連の情報、例えば感染予防策や保障、ワクチン等のコンテンツをホストし、人々を引き寄せようとしていたと考えられます。

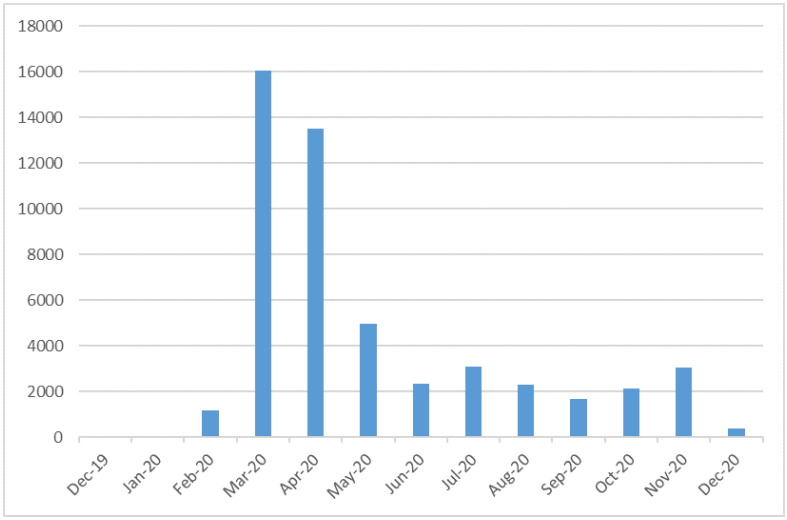



*図3 "covid"という語を含む、悪意のある新規作成ドメイン数*

数字の増減を見ると、新型コロナウイルスの感染が全世界に広がるにつれて、新規作成されたドメイン数が増加していき、多くの先進諸国で大規模なロックダウンが開始された 3 月から 4 月にそのピークを迎えたことがわかります。このグラフを見ると、それ以降の新規作成ペースは落ち着いているかのように見えますが、例えば 11 月から 12 月初旬においても、一日約 100 件の悪意あるドメインが新規作成されています。

コロナウイルス関連のフィッシングを行っているのはサイバー犯罪者だけではありません。今年 2 月後半から 3 月中旬にかけて、Mustang Panda[2]と呼ばれる APT グループが、台湾並びにベトナムに対するフィッシングキャンペーンを行いましたが、そこで「餌」となる情報として用いられたのは新型コロナウイルス関連の情報でした。また、APT41[3]や

[1] DomainTools Iris のデータより作成

[2] Mustang Panda は中国の APT グループ。

[3] APT41 は中国の APT グループであり、戦略的情報や知的財産の窃取活動並びに金銭目的の活動も行う。

APT28[1]といったグループも同様の攻撃を行っていることが確認されています[1] [2]。

新型コロナウイルス関連の話題が全世界的であることもあり、ここまでは世界的な動向についての話が殆どでした。そこでここからは、その中でも日本在住者を標的とした新型コロナウイルス関連の攻撃を取り上げ、我々がどのような状況に置かれているかを少し見てみましょう。

下記のグラフは、”kyufu”あるいは”kyuhu”という語句を含む、悪意ある新規作成ドメインの月別作成数を表したものです。上記の語句によるフィルターをかけることで、お察しの通り、日本政府によって 5 月後半から 10 月中旬まで支給された「特定定額給付金」を利用した悪意あるドメインを検知しています。

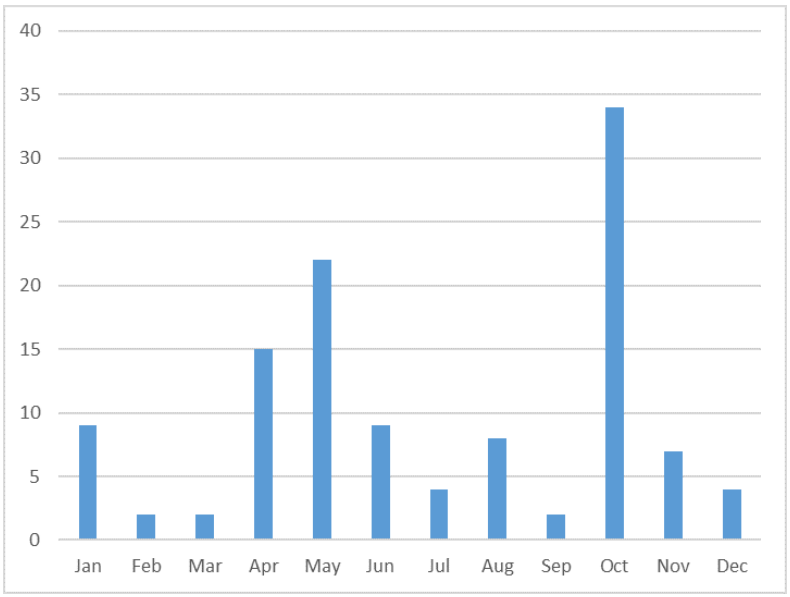



*図4 "kyufu" もしくは "kyuhu" という語を含む、悪意ある新規作成ドメイン数*

グラフを見ると分かる通り、大きなスパイクが 5 月と 10 月に存在しています。5 月のものは給付金の開始時期と、10 月のものは終了時期と、それぞれ一致していることがわかります。更に 10 月には、追加の給付金があるとの噂と、それを悪用して個人情報や口座情報等を入力させるようなフィッシングキャンペーンに対する注意喚起が複数発表されています[3], [4]。10 月のほうが 5 月よりも新規作成されたドメイン数が多い理由の一つは、上記のフィッシングキャンペーンであると考えられます。

[1] APT28 はロシアの APT グループであり、ロシアの情報機関 GRU の第 85 Main Special Service Center が関与していると考えられている。

### 2021 年予測

- シンプルで安価かつ強力な手段として、フィッシングは来年も数多くの脅威アクターによって用いられる。
- 新型コロナウイルスのワクチンについての声明が日本政府によって発表され、広く流布されるに従い、それを利用したフィッシングキャンペーンも増えると予想される。
- 2021 年に議論されるだろう主要なニュースやその他トピック等も、フィッシングの「餌」として用いられる。
- それらトピックの具体例としては、オリンピック・パラリンピック関連や、国境や移動等の制限撤廃、コロナウイルスの抗体検査（PCR 検査等）などが挙げられる。

## 医療機関・研究機関等への脅威

### 2020 年 概観

新型コロナウイルスが猛威を奮った今年、APT グループの多くが関連情報を窃取しようと医療機関や関連組織への攻撃を繰り返したことが、FireEye, Malwarebytes, CrowdStrike や他のサイバーセキュリティ企業によって観測、報告されています。

例えば FireEye によって報告された、年明けすぐの 1 月 6 日から APT32[1]によって行われた攻撃では、当該グループが中国政府の応急管理部並びに武漢の行政機関に対してスピアフィッシングを行い、内部ネットワークに侵入して新型コロナウイルス関連の情報を得ようとしたとのことです。また 2 月初めには、Patchwork によって同様の作戦が中国政府機関に対して行われています[2] [5]。

上記のように、年初のサイバー攻撃は主に新型コロナウイルスの性質や、他国政府によって隠されているかもしれない情報を窃取するために行われていました。しかしその後、この傾向は、コロナウイルスのワクチン製造に向けたスパイ活動に変化します。

[1] APT32 はベトナムの APT グループ。

[2] Patchwork はインドの APT グループ。

8 月には、米国保健福祉省が声明を発表し、イラン・中国並びにロシアの APT グループが、米国に拠点を置く製薬会社並びに新型コロナウイルスワクチンの研究開発・製造に携わる機関を対象にした攻撃を行っていると述べました[6]。

11 月終わりには、北朝鮮の APT グループが英国の製薬会社であるアストラゼネカのシステムに侵入を試みたというニュースも発表されています[7]。アストラゼネカも、新型コロナウイルスワクチンの研究を積極的に行っている企業の一つです。

さらに、IBM が 12 月に出したレポートでは、輸送に冷却が必要な新型コロナウイルスワクチンの、その冷却サプライチェーンに対するスピアフィッシングを 9 月から観測していたとのことです。

日本の製薬会社等もこの例にもれず、APT グループの標的となっています。米国や英国のように、特定の企業を対象にした重大なインシデントが一般に報道された訳ではありませんが、CrowdStrike が 10 月に発表したところによると、中国の APT グループが、日本の製薬会社や研究機関を標的にフィッシング攻撃を行っているという事です[8]。

以上のように、本年は新型コロナウイルス関連の情報をめぐり、政府の支援を受けた APT グループがその獲得に向けて積極的に攻撃を行ったことが観測されました。

### 2021 年 予測

- ワクチンの開発が進むにつれ、その情報を欲する APT グループを始めとした脅威アクターが、日本の医療機関・研究機関や関係する組織を標的に攻撃を行うことが予想される。
- 攻撃者が内部ネットワークへのアクセスを得る方法としては、フィッシングが今後も最も使われる手法であることが予想される。
- APT グループを始めとした政府の支援を受けた脅威アクターが、偽旗作戦としてランサムウェア攻撃を行う傾向がわずかに見られ、来年にはそのような攻撃が増える可能性がある。

## オリンピック関連

### 2020 年 概観

新型コロナウイルスの影響で 2021 年夏に延期された東京オリンピック・パラリンピックですが、それによってオリンピックの重要度が引き下がった訳ではありません。日本政府

と国際オリンピック委員会が参加選手や来場者、国民の安全をいかに確保するかを議論する中、サイバー犯罪者たちはいかにイベントを彼らの目的に利用するかを考えています。

過去数回に渡って、APT グループ・金銭目的のハッカーやサイバー犯罪者・またハクティビストらがオリンピックを攻撃の標的にし、情報の窃取やサービス停止、脅迫活動やフィッシング、政治的声明の拡散など、様々な活動をサイバー空間で行って来ました。その流れから言えば、東京オリンピックもまた攻撃の標的になるのは当然と言えるでしょう。

実際に、攻撃の前段階と考えられるサイバー空間での偵察行為が今年 10 月に観測されています。英国サイバーセキュリティセンター（NCSC）の発表では、APT28 と関連があると見られるロシアの情報機関 GRU によって、東京オリンピック・パラリンピックのネットワークインフラに対してスキャニング等の偵察行為が行われたとのことです[9]。APT28 は 2018 年の平昌オリンピックにおいて、大規模なサイバー攻撃をオリンピック関係者並びにネットワークインフラに対して行ったグループであると考えられています。具体的に行われた攻撃は、オリンピック関係者を狙ったスピアフィッシングキャンペーンや内部ネットワークへの侵入、そして「Olympic Destroyer」と呼ばれるマルウェアを用いた PC の破壊などです。この APT28 によるオリンピックへの攻撃は、ロシア選手団内でのドーピング問題と、それに伴い世界反ドーピング機構と国際オリンピック委員会によって行われたロシア代表選手のオリンピックへの参加禁止措置への抗議活動の一環であるとの見方が支配的です。2020・2021 年の東京オリンピックにおいてもその措置は継続しており、APT28 が 2021 年のオリンピックに対する攻撃の準備を行っている可能性は高いでしょう。10 月の観測はそれを裏付けるものです。

また、前回の 2018 年平昌オリンピックは北朝鮮にも狙われていました。オリンピック開催の数ヶ月前から、北朝鮮の APT グループの一つである Lazarus Group[1]は韓国に対し大規模なフィッシングキャンペーンを展開しています。この場合の北朝鮮側の動機は、おそらく地政学的なものであると考えられています。従って 2021 年東京オリンピックの場合も、地政学的動機で他国の APT グループに標的にされ得るという事を考慮する必要があるでしょう。

しかしながら、オリンピックをその標的にしようとするのは政府の支援を受けた APT グループだけではありません。ハクティビストや金銭目的のサイバー犯罪者なども、その機会を利用しようと試みるでしょう。ハクティビストに関しては、現在観測されている彼らの

[1] Lazarus Group は北朝鮮に支援されていると考えられているハッカー集団

行動の中に、オリンピックに関連する動きがいくつか見られます。例えば **#BoycottTokyo2020** という Twitter 上のハッシュタグは、その字の如く東京オリンピックをボイコットすることを推奨し、その運動を加速するために用いられています。ボイコットの理由としては福島第一原発事故絡みや、今回の新型コロナウイルスの話題などが挙げられています。この運動は有名な Anonymous の一部にも支持されており、彼らが過去に日本に対して行った「作戦」のハッシュタグ、例えば#OpKillingBay, #OpNuke, #OpGreenRights などとともに拡散されています。下の画像はそういった Twitter 上の投稿の一例です。また金銭目的のサイバー犯罪者についても、フィッシングや詐欺行為に旬の話題を取り込む彼らの習性を鑑みると、オリンピックに向けて更に活動を活性化させると考えられるでしょう。

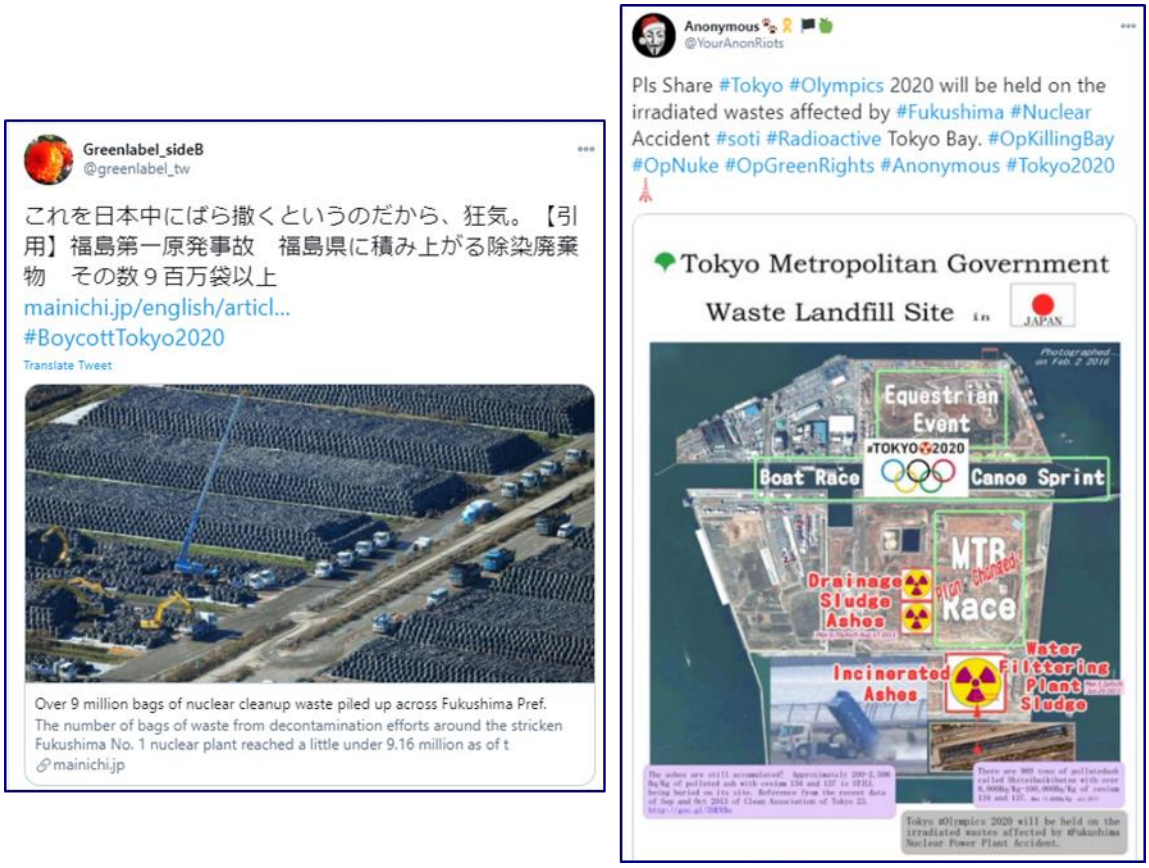



*図5 "#BoycottTokyo2020"ハッシュタグを用いて投稿をするアカウントの例*

### 2021 年 予測

- 2021 年に開催される東京オリンピック・パラリンピックは様々な種類の脅威アクターによって攻撃の標的となることが予想される。
- ロシア選手団へのオリンピック参加禁止措置が解除されていない現状、APT28 を始めとしたロシア系 APT グループがオリンピックのネットワークインフラ等に対する攻撃を行うことが考えられる。また、来年の地政学的動向によっては北朝鮮や中国の APT グループも、オリンピックへの攻撃に加わる可能性がある。
- アクティビストやハクティビスト等も、オリンピックという世界の注目が集まる機会を利用して、彼らの主張を広めようとすることが予想される。
- サイバー犯罪者やハクティビストらによって、SNS が彼らの活動に使用される可能性が高い。また、彼らの活動が APT グループ等によって偽旗として用いられ、さらにそれを利用したフェイク・ニュースキャンペーンなどが行われる可能性がある。

## 重要社会インフラ企業への攻撃

### 2020 年 概観

前節ではオリンピックへの攻撃を論じましたが、オリンピックへの攻撃はオリンピックのインフラ本体にのみ行われるわけではなく、それを取り巻くサプライチェーンや重要社会インフラにまで波及しうるということを言及しておくべきでしょう。オリンピックによって特定の部分に防御のリソースを割いたがために、リソースが薄くなったその他の部分にサイバー犯罪者等が攻撃を仕掛けるということも十分考えられます。

特に、重要社会インフラ企業は政府の支援を受けた APT グループから、金銭目的のサイバー犯罪者、さらにはハクティビストまで、様々な脅威アクターによって狙われる可能性があります。

2020 年に、IPA 配下のサイバーレスキュー隊(J-CRAT)が公開したレポートによると、2019 年 12 月から少なくとも 2020 年 8 月までの期間、APT10[1]が日本の政府機関を中心にフィッ

[1] APT10 (Cicada とも)は中国に支援されていると考えられているハッカー集団であり、日本企業を主な標的としてきた。

シングキャンペーンを行っていたことが報告されています[10], [11]。また、シマンテックが 11 月に明らかにした所によると、同グループが様々な業界の日本企業に対して、2019 年 10 月中旬から少なくとも 2020 年 10 月初旬まで、断続的に情報の窃取を目的としたフィッシング攻撃を行っていたということです[12]。

サービスを継続的に提供しなければならない重要社会インフラ企業にとって、最も考慮すべき攻撃の一つは DDoS 攻撃でしょう。今年 2 月の、Amazon が史上最高の 2.3Tbps ものDDoS 攻撃を観測したという報告や[13]、8 月のニュージーランド証券取引所に対するDDoS 攻撃と、それによる数日間のサービス停止から考えて、洗練された脅威アクターの実行する DDoS 攻撃は更に洗練されていると考えられます。

また、日本においても、その様な重要社会インフラ企業への攻撃の前準備である、または悪用されると考えうるインシデントが複数観測されています。

11 月には、イベント管理サービス等を提供する Peatix の顧客情報が不正アクセスにより流出するというインシデントが発生しました[14]。この件で最大約 677 万件の氏名、メールアドレスや SSHA 方式で保存されたパスワードなどが窃取され、その大部分が Dark Web 等で閲覧可能となっています。サイバー犯罪者はこのような流出データ等を用いて標的の企業への攻撃を準備することが多いと言われています。この流出の多くが日本人の情報であったこともあり、今回の流出の情報がさらなる被害を生む端緒になる可能性があるでしょう。

また、これも 11 月ですが、日本の原子力規制委員会がサイバー攻撃を受け、比較的機密度の低い情報が外部の侵入者によって閲覧されたという報道がありました[15]。機密情報へのアクセスはなかったということですが、それでも 1200 人あまりの電子メールや業務ファイルは、サイバー犯罪者がスピアフィッシングのための情報源としては余りあるものです。

以上のデータ流出も含め、2020 年日本では例年以上の数のデータ流出事件が発生しました。それらの流出の一部は、更なる攻撃のための下準備とでも言うべきものであった可能性があります。従って、事件によって流出したデータの持ち主のみならず、その関連企業なども十分に注意を行う必要があるでしょう。

## 2021 年 予測

- 日本において発生した多大な量のデータ流出事件が、主に日本人や日本企業を標的にした更なる攻撃に用いられる可能性が高い。また重要度やミッションクリテ

ィカル性のために、大企業や重要社会インフラ企業が標的となり、流出情報を悪用したスピアフィッシング行為などが行われることが予想される。

- 高度な DDoS 攻撃やランサムウェアなど、今年大規模に用いられた攻撃が今後も継続すると考えられる。そしてその攻撃の性質により、可用性が求められている重要社会インフラ企業は格好の標的になる可能性がある。また、それらの一見金銭目的に思われるサイバー攻撃が、APT グループ等によって偽旗作戦として行われる可能性がある。
- DDoS 攻撃に関しては、高度な能力を持つアクターからハクティビスト等の比較的洗練されていないアクターまで、様々な脅威アクターがサービス中断を引き起こす手段として用いることが予想される。
- オリンピックシーズンにおいては、通常よりもネットワークトラフィック量が増加することが考えられる。従って、ISP やデータセンター、クラウドサービス単位を対象にした大規模な DDoS 攻撃が行われた場合、その増加したトラフィック量も相まって想定以上のパケットを処理する必要が生じる。そのような状況がサイバー犯罪者やハクティビストに利用される可能性がある。

# ランサムウェア

## 2020 年 概観

ランサムウェア攻撃は、今年最も注目を浴びたサイバー攻撃と言えるでしょう。ランサムウェアを使用する脅威アクターは新しい戦術や恐喝手段を開発し、また効率的な組織構造を取ることで、より一層企業や組織を脅かすようになっています。

今年行われたランサムウェア攻撃は、かなりの部分が脆弱な RDP サーバもしくは VPN サーバから始まっています。CVE-2019-11510（Pulse Secure 社 VPN の脆弱性）や CVE-2018-13379（Fortinet 社 VPN の脆弱性）に脆弱な VPN サーバ、更に適切な設定がなされず、誰でもアクセスできてしまう RDP サーバ等が主な標的となっているようです。この様な侵入経路が広く使われる背景には、新型コロナウイルスに伴うテレワークのあまりにも急速な普及が、企業の IT 部門に十分な準備を行う時間を与えなかったことも原因があるでしょう。

更に、ランサムウェアオペレータは、被害者へ身代金を払わせるために新たな恐喝手段を編み出しました。以前取られていた、データを暗号化して人質に取る方法に加え、現在では多くのランサムウェアオペレータがデータ暗号化以前にデータを盗み出し、身代金を払わなければ窃取した情報を一般に公開すると脅す方法を同時に行うようになってきています。すなわち、現在のランサムウェア攻撃は可用性・完全性だけでなく機密性をも脅かし、ランサムウェアへの感染はデータ流出インシデントをも意味するようになりつつあるということです。このデータ暗号化とデータ窃取を同時に行う手法は”Double-Extortion Scheme”（二重恐喝)と呼ばれています。このスキームは Maze と呼ばれるランサムウェアを運営する脅威アクターによって 2019 年 11 月に最初に用いられ[16]、現在では計 20 以上のランサムウェアによって使用されています。

今年に入って、世界的な大企業を含む数多くの企業がランサムウェアの被害に苦しんでいることは、明らかになっている被害状況を見てもわかります。以前と比較しても、ランサムウェア攻撃の数、並びにその洗練度はかなり向上していると言って良いでしょう。2020 年に入り、Revil, Maze, DoppelPaymer, Conti や Egregor などのランサムウェアグループが「アフィリエイト」を募集し、他の脅威アクターと協力して一連の攻撃を行っている為だと考えられます。「アフィリエイト」はランサムウェア攻撃において、主に企業ネットワークの偵察、その企業の内部ネットワークへの侵入及び横展開を行います。ランサムウェアグループは開発したランサムウェアを「アフィリエイト」に貸与し、「アフィリエイト」は企業から支払われた身代金のうち 6〜7 割を手に入れます。そして残りの身代金とランサムウェアの貸与に対する費用が、ランサムウェアグループに渡るというわけです。以上の構造によって、ランサムウェアグループは実際に手間のかかるサイバー攻撃を行うことなく効率的に資金を回収でき、「アフィリエイト」は最新のランサムウェアを用いた攻撃の実行や関連する技術サポートを受けることができます。さらに、この変化によりサイバー犯罪者間の競争原理や分業性による効率化・技術の先鋭化、攻撃者の増加による標的の多彩化の効果も生じました。それが、今年に数多くのランサムウェア攻撃が発生し、大企業さえもその被害を受けた理由の一つでしょう。

また、ランサムウェアグループの中には、政府と協力関係を築いているものもいます。例えば、Maze ランサムウェアのオペレータにはロシア政府との繋がりが示唆されているようです。ランサムウェアグループが APT グループと同様に標的を選定し、機密情報を盗み出すために特定の企業を攻撃するというシナリオが存在しうるという事を認識しておく事は、攻撃を予見し、防御に役立てる観点から有用でしょう。

また、明らかになっている限りでも、日本企業の日本、もしくは海外の拠点がランサムウェア攻撃を受けた例がいくつか見られます[17], [18]。被害を一般に公開していない企業も数多くあると思われ、ランサムウェアの増加という世界的な傾向は、日本にも波及していると言えるでしょう。以下は明らかになっている日本におけるランサムウェア攻撃の例です。

- 2020 年 6 月 – Snake ランサムウェアの亜種である Ekans ランサムウェアにより、ホンダの日本、米国、EU 拠点が攻撃を受ける。
- 2020 年 8 月 – RansomEXX ランサムウェアにより、コニカミノルタが攻撃を受ける。この攻撃により、会社のサービスが約一週間停止。
- 2020 年 8 月 – Maze ランサムウェアがキャノン USA 関連のインフラを攻撃。
- 2020 年 11 月 – Ragnar Locker ランサムウェアがカプコンを攻撃。この攻撃により、日本、米国、カナダのネットワークから計 1TB の情報が窃取され、その後公開された。

公表されている被害以外にも、多くのランサムウェア攻撃が日本企業並びにその海外拠点を襲いました。2020 年には、上で言及されているランサムウェアグループに加えて、少なくとも DoppelPaymer、 Egregor、Conti、Revil ランサムウェアグループ、もしくはその「アフィリエイト」が日本企業を攻撃したことがわかっています。標的の企業が医療機関、エネルギー、小売、建設、製造など多岐に渡ることから、サイバー犯罪者がどの業界をランサムウェア攻撃の標的に選ぶかを予測することは非常に難しくなっていると言っていいでしょう。

また、我々が今年観測した、日本企業を標的にしたランサムウェア攻撃の例を見ると、殆どの企業に対する攻撃は海外拠点のネットワークへの侵入から始まっている事がわかります。日本企業について、ダークウェブ上においても 2020 年初頭から RDP 等を通じたネットワークへのアクセス権を売買する投稿が見られ、同年後半にはユーザ認証情報や任意コード実行の脆弱性等のやり取りも見られました。2020 年に起きた日本における企業へのランサムウェア攻撃の事例の分析、並びにダークウェブ上でのサイバー犯罪者の動向から鑑みるに、被害を受けた日本企業の多くは、海外拠点の持つ RDP や VPN サーバの脆弱性を突いた攻撃によりネットワークへ侵入され、結果攻撃を受けたと思われます。従って、ランサムウェア攻撃による被害を防ぐためには、まず組織内のネットワークを調査し、その中に存在している RDP・VPN 製品に対してパッチ等が正しく適応され、既知の脆弱性に必要な対処が行われていることを確認することが重要でしょう。

### 2021 年 予測

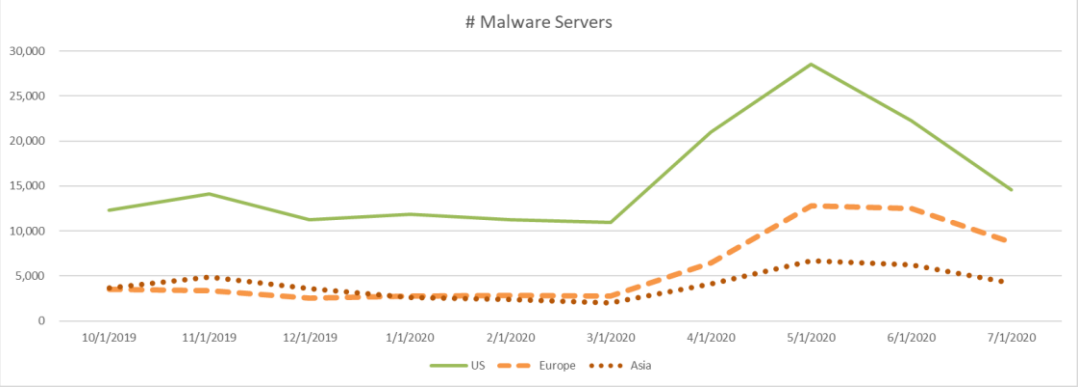
- 2020 年を通じて、ランサムウェア攻撃が大きな利潤を効率的に生むことが数多くの脅威アクターに知られたため、2021 年にもランサムウェア攻撃は増加を続けることが予想される。
- 金銭目的のサイバー犯罪者は特定の国や地域、産業に拘らず、脆弱なネットワークを察知して攻撃を行う。従って、業種・大小問わず、全ての企業が標的となる可能性がある。
- APT グループによる情報窃取活動の一環として、ランサムウェア攻撃が行われる兆候が見られ、その傾向は 2021 年も継続すると思われる。特に重要社会インフラ企業やそのサプライチェーンについては、ランサムウェアについて追加の注意が必要となる。
- “Double-Extortion”（二重恐喝）がより数多くのランサムウェアグループによって用いられることが予想される。
- 今年見られた日本企業に対するランサムウェア攻撃は、殆ど RDP もしくは VPN 機器の脆弱性に基づく攻撃であり、その傾向は 2021 年にも継続すると考えられる。従って、該当する機器に対するパッチの適用などを適切に行う必要がある。

## マルウェア

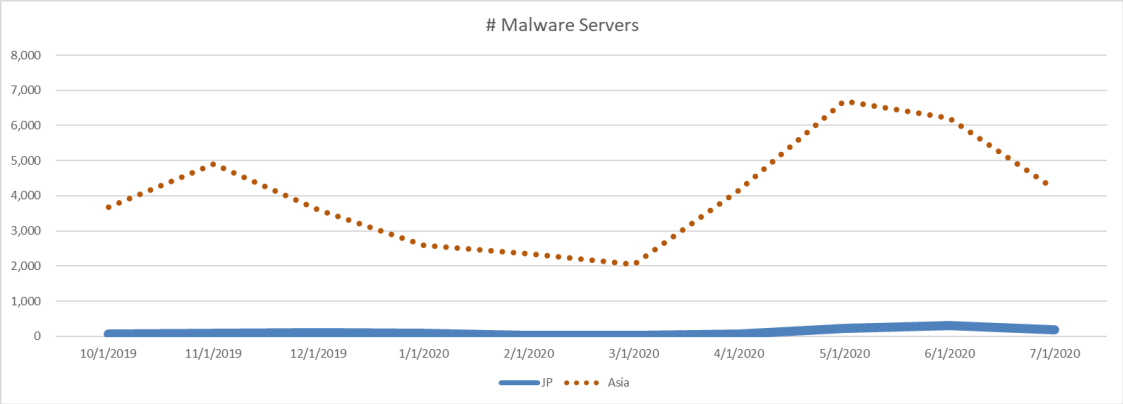
### 2020 年 概観

2020 年はランサムウェアが話題を席巻したとは言え、その他のマルウェアがその勢いを緩めた訳ではありません。次の図は、サイバー犯罪者らによってフィッシングサイトやマルウェア拡散に用いられているネットワークインフラの数を、米国、アジア、EU の地域別に示したグラフです[1]。これを見ると、アジア地域のネットワークインフラは米国、EU 地域のものに比べて悪意ある目的で使われる数が少ないという事がわかります。

[1] BitSight の情報を元に作成




下の図は、アジアと日本の比較です。日本はアジアの中でも最もその様なインフラの少ない国であることがグラフからわかります。




しかし、この事は日本がマルウェア等の被害に会いにくい環境である事を示している訳ではありません。2020 年上半期において、日本を対象としたマルウェア攻撃は 2019 年上半期比 20%増加しています[19]。特に、今年最も猛威を奮ったマルウェアは Emotet と TrickBot でしょう[20]。

Emotet は 2014 年に発見されたマルウェアで、元々は口座情報等を窃取するためのトロイの木馬でした。しかしアップデートを繰り返す中で機能を拡張し、現在では主に追加のマルウェアのローダーやバックドアとして用いられています。

この Emotet ですが、2020 の 2 月まで大規模なフィッシングキャンペーンを展開した後、数カ月に渡って活動を停止しました。日本においても同様に、2019 年 10 月から 2020 年 2 月までの活動の後、7 月中旬まで活動を停止していましたが、近年はその活動が再活発化しています[21]。

もう一つの脅威である TrickBot は 2016 年に、こちらも情報窃取型のトロイの木馬として観測されました。このマルウェアは特に、Ryuk ランサムウェア並びにその後継ランサムウェア Conti のローダーとして用いられていることが知られています。Conti は“Double-Extortion”（二重恐喝）を用いるランサムウェアグループであり、2020 年を通じて精力的に活動を行っていました。さらに、TrickBot と Emotet はお互いがお互いをインストールしようとすることが知られています。

今年 10 月、米 Microsoft とそのパートナー組織らによって、TrickBot が主に C2 として用いているネットワークインフラをテイクダウンする作戦が実行されました。Microsoft はその約一週間後、最大 94%のインフラを成功裏に停止させたというレポートを発表しました。しかしその直後から、複数の CTI 企業や組織によって、TrickBot の活動が未だ継続していること、ネットワークインフラがその数を新たに増やしていることなどが報告されています。また 12 月には、英国において企業インフラを用いた大規模な TrickBot のフィッシングキャンペーンが報告されました。これらのことから、TrickBot は Microsoft 等の作戦にもかかわらず、未だ健在であることが伺えます[22]。

またマルウェア配布の面では、2020 年に起きた多くのデータ流出により入手した情報を、2021 年以降サイバー犯罪者が活用する公算は高いと言えます。ダークウェブ上に公開された氏名やメールアドレス、所属組織等の情報がスパムやフィッシングキャンペーンに用いられ、結果データ流出の被害者が新たなマルウェアを感染させるための標的となる可能性が高いため、該当の組織並びに個人は十分に警戒する必要があるでしょう。

## 2021 年 予測

- 世界的な潮流に対応して、日本もマルウェア攻撃の数が増加し続けることが予想される。しかし、マルウェア拡散等に用いられるインフラとしては、日本以外の地域がよく用いられ、日本におけるそのようなインフラ数は大きく変化しないと考えられる。
- オリンピック関連企業、並びに重要社会インフラ企業等の標的に対して、フィッシング等によるマルウェア攻撃が増加すると考えられる。その結果として、マルウェア被害企業に対して情報窃取活動やランサムウェア攻撃が行われる可能性がある。

# 「日本におけるサイバーリスク 2021」リスクアセスメント

以下の表は、2020 年のサイバー攻撃関連の状況やトレンドの評価に基づいて算定した、日本における 2021 年の各サイバー脅威のリスクアセスメントです。

| サイバー脅威 | 妥当性 | 影響度 |
|---|---|---|
| **COVID-19 関連のフィッシング、詐欺** | | |
| 政府支援の APT グループ |  |  |
| 金銭目的のサイバー犯罪者 |  |  |
| ハクティビスト |  |  |
| **医療機関・研究機関等への脅威** | | |
| 政府支援の APT グループ |  |  |
| 金銭目的のサイバー犯罪者 |  |  |
| ハクティビスト |  |  |
| **オリンピック関連** | | |
| 政府支援の APT グループ |  |  |
| 金銭目的のサイバー犯罪者 |  |  |
| ハクティビスト |  |  |
| **重要社会インフラ企業への攻撃** | | |
| 政府支援の APT グループ |  |  |
| 金銭目的のサイバー犯罪者 |  |  |
| ハクティビスト |  |  |
| **ランサムウェア** | | |
| 政府支援の APT グループ |  |  |
| 金銭目的のサイバー犯罪者 |  |  |
| ハクティビスト |  |  |
| **マルウェア** | | |
| 政府支援の APT グループ |  |  |
| 金銭目的のサイバー犯罪者 |  |  |
| ハクティビスト |  |  |

## リスクアセスメント方法論

妥当性

| | |
|---|---|
| *高*  | 日本、日本企業並びに日本企業の海外拠点に対して、その種のサイバー攻撃が行われる公算が高い。世界的、もしくは特定地域においてその種の攻撃が流行しており、またその攻撃が起こる前提条件が満たされている。サーフェスウェブ、ダークウェブ等において、特定の標的に対するその攻撃の準備が行われていることが確認できる。 |
| *中*  | 日本、日本企業並びに日本企業の海外拠点に対して、その種のサイバー攻撃が行われる可能性がある程度存在する。世界的、もしくは特定地域においてその種の攻撃が流行しており、またその攻撃が起こる前提条件が満たされている。サーフェスウェブ、ダークウェブ等において、標的への言及無くその攻撃の準備が行われている兆候が見受けられる。 |
| *低*  | 日本、日本企業並びに日本企業の海外拠点に対して、その種のサイバー攻撃が行われる可能性がある程度存在する。世界的、もしくは特定地域においてその種の攻撃が流行しており、またその攻撃が起こる前提条件が満たされている。しかしサーフェスウェブ、ダークウェブ等においてその攻撃が行われる兆候は見受けられない。 |

影響度

| | |
|---|---|
| *高*  | その種のサイバー攻撃が成功した場合、以下の一つ以上の影響を受ける。<br>● その組織の主要な活動が一日以上停止する。<br>● 攻撃の結果、その組織の顧客や業務請負先との契約遵守が不可能になる、または法令、規則等に違反する結果となる。<br>● その攻撃が広く一般に周知され、その組織の評判を損なう。<br>● 組織の財務状況に多大な影響を及ぼす。 |
| *中*  | その種のサイバー攻撃が成功した場合、以下の一つ以上の影響を受ける。<br>● その組織の主要な活動が最大一日停止する。<br>● 攻撃の結果、その組織の顧客や業務請負先との契約遵守、法令、規則等の遵守が困難になる。<br>● その攻撃が一部に周知され、その組織の評判を損なう。<br>● 組織の財務状況に軽微な影響を及ぼす。 |
| *低*  | その種のサイバー攻撃が成功した場合でも、<br>● その組織の主要な活動は影響を受けず、停止されない。<br>● 攻撃によって、その組織の顧客や業務請負先との契約遵守、法令、規則等の遵守に影響が及ばない。<br>● その攻撃が一般に論じられず、結果組織の評判の損失が最低限に抑えられる。<br>● 組織の財務状況に影響がない。 |

# 参考文献


1. This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html
2. Accenture SITREP. Cybersecurity risks related to COVID-19 https://www.accenture.com/_acnmedia/PDF-124/Accenture-SITREP-COVID-19-20200428-V8-Final-Edit.pdf
3. 武田総務大臣閣議後記者会見の概要 https://www.soumu.go.jp/menu_news/kaiken/01koho01_02000957.html
4. [更新] 特別定額給付金に関する通知を装うフィッシング (2020/10/19) https://www.antiphishing.jp/news/alert/kyufukin_20201019.html
5. APTs and COVID-19: How advanced persistent threats use the coronavirus as a lure. Malwarebytes Threat Intelligence. April 2020 https://resources.malwarebytes.com/files/2020/04/200407-MWB-COVID-White-Paper_Final.pdf
6. COVID-19 Cyber Threats (Update) https://www.aha.org/system/files/media/file/2020/08/hc3-threat-brief-tlp-white-covid-19-cyber-threats-update-8-13-20.pdf
7. Exclusive: Suspected North Korean hackers targeted COVID vaccine maker AstraZeneca – sources https://jp.reuters.com/article/us-healthcare-coronavirus-astrazeneca-no/exclusive-suspected-north-korean-hackers-targeted-covid-vaccine-maker-astrazeneca-sources-idUSKBN2871A2
8. Cyberattacks on coronavirus vaccine projects confirmed in Japan https://mainichi.jp/english/articles/20201019/p2g/00m/0na/075000c
9. UK exposes series of Russian cyber-attacks against Olympic and Paralympic Games https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games
10. サイバーレスキュー隊（J-CRAT） 活動状況 https://www.ipa.go.jp/files/000083013.pdf
11. サイバーレスキュー隊(J-CRAT)活動状況　[2020 年度上半期] https://www.ipa.go.jp/files/000086892.pdf
12. Japan-Linked Organizations Targeted in Long-Running and Sophisticated Attack Campaign https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage
13. AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/
14. 弊社が運営する「Peatix（https://peatix.com/）」へのの不正アクセス事象に関するお詫びとお知らせ https://announcement.peatix.com/20201117_ja.pdf
15. 【独自】原子力規制委にサイバー攻撃、機密情報を不正閲覧か https://www.yomiuri.co.jp/national/20201126-OYT1T50335/
16. Ransomware Evolved: Double Extortion https://research.checkpoint.com/2020/ransomware-evolved-double-extortion/

17. The State of Ransomware in 2020 https://www.blackfog.com/the-state-of-ransomware-in-2020/
18. The biggest hacks, data breaches of 2020 https://www.zdnet.com/article/the-biggest-hacks-data-breaches-of-2020/
19. MID-YEAR UPDATE: Cyber threat intelligence for navigating the new business normal https://www.sonicwall.com/resources/2020-cyber-threat-report-mid-year-update-pdf
20. October 2020's Most Wanted Malware: Trickbot and Emotet Trojans Are Driving Spike in Ransomware Attacks https://blog.checkpoint.com/2020/11/06/october-2020s-most-wanted-malware-trickbot-and-emotet-trojans-are-driving-spike-in-ransomware-attacks/
21. マルウェア Emotet の感染に繋がるメールの配布活動の再開について (追加情報) https://www.jpcert.or.jp/newsflash/2020072001.html
22. Massive Subway UK phishing attack is pushing TrickBot malware https://www.bleepingcomputer.com/news/security/massive-subway-uk-phishing-attack-is-pushing-trickbot-malware/