

2021年の情報セキュリティ動向

土居 毅彦 ●一般社団法人JPCERT コーディネーションセンター 早期警戒グループ 脅威アナリスト

東京オリンピック・パラリンピックは、目立ったサイバー攻撃もなく平穩に開催された。一方で、Emotetのテイクダウンと活動再開、国内外で社会インフラを狙う深刻なランサムウェア攻撃が確認された。

■セキュリティインシデントの報告件数

2021年1～12月にJPCERTコーディネーションセンター（JPCERT/CC）に報告されたコンピューターセキュリティインシデント（以下、インシデント）の件数は4万4231件で、昨年の4万3823件と同水準であった（資料4-1-1）。内訳においては「DoS/DDoS」が大幅に減少した（資料4-1-2）。フィッシングサイト、特に国内ブランドを装ったものが多い状況は昨年と同様である。

■個人ユーザーを対象とした攻撃

●偽サイトへ誘導するメッセージ

2021年も昨年に引き続き、多数の利用者を擁するサービスを装ってメールやSMSでメッセージを送り付け、フィッシングサイトへ誘導する攻撃が多数報告された。ユーザーがメッセージ内に記載されたリンクを開くと攻撃者が用意した偽サイトへ誘導され、この偽サイトで登録情報（IDやパスワード）をはじめ、その他の個人情報を入力させて、それを窃取するというものである。

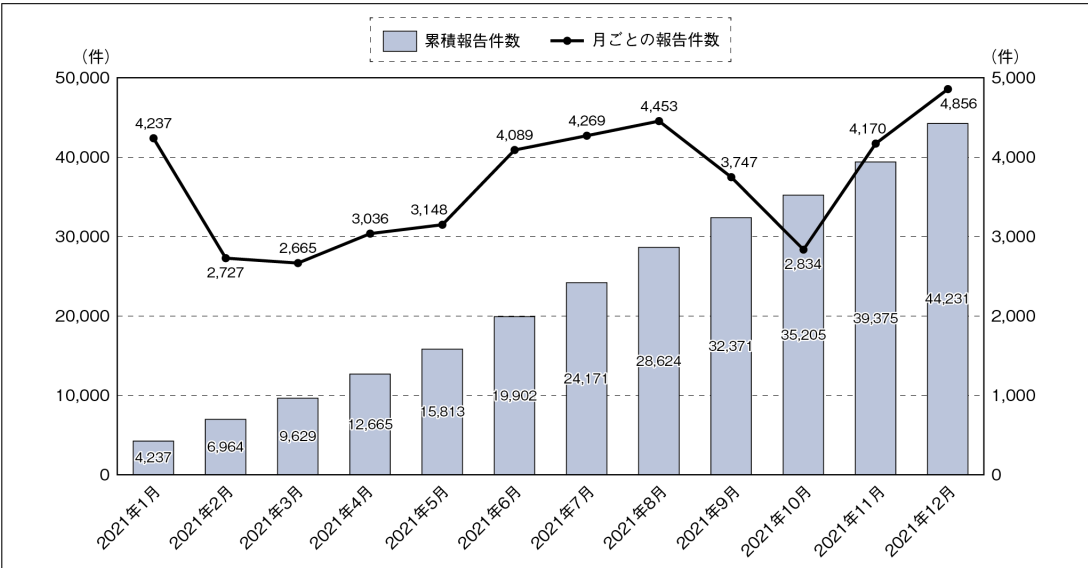
2021年8月には、ねんきんネット、特別定額給付金の申請サイト、コロナワクチンナビを模した偽サイトへ誘導するフィッシングが確認され¹、10月から11月にかけては、これまでかたられなかったコンビニエンスストアや旅行予約サイト、

保険会社、電子マネーサービスを模した偽サイトが確認された²。さらに、フィッシングに分類してはいないが、7月から8月にかけて、無料のスポーツ動画配信サービスを装うウェブサイトなどから有料サービスへの登録を誘導するケースも確認されている³。

これらは、新型コロナウイルス感染症（COVID-19）への不安感や東京オリンピック・パラリンピック競技大会への関心に乗じた攻撃である。ユーザーには、正規のアプリやブックマークした正規のURLからサービスへログインして情報を確認するなどの基本的な行動の徹底が求められている。加えて、被害時に備えてパスワードの使い回しを避けることも重要である⁴。

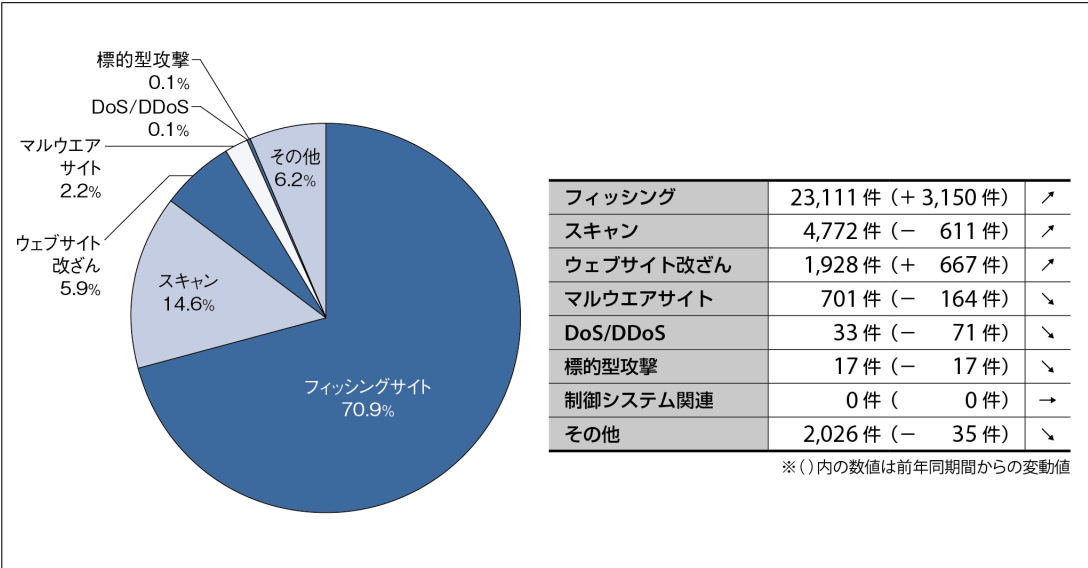
フィッシングメール対策では、ユーザー側の警戒だけでなく事業者側の対応も重要である。フィッシング対策協議会ではDMARCの導入を推奨しており、DMARC検証と迷惑メールフィルターの併用で多くのなりすましメールを検出できることを確認している。日本ブルーフォンプointが2021年2月に行った調査では、日経225企業の25%しかDMARC認証を導入しておらず、普及率は高いとはいえない⁵。組織においては、ドメインは企業のブランドと等しいことを認識し、なりすましメールの排除を検討することが望まれる。

資料 4-1-1 インシデント報告件数の推移（2021 年 1～12 月）



出所：JPCERT/CC、「インシデント報告対応レポート」(<https://www.jpcert.or.jp/ir/report.html>) を基に作成

資料 4-1-2 インシデント報告件数のカテゴリ別内訳（2021 年 1～12 月）



出所：JPCERT/CC、「インシデント報告対応レポート」(<https://www.jpcert.or.jp/ir/report.html>) を基に作成

■法人や組織を対象とした攻撃

●マルウェア「Emotet」の動向

2020年に世界的に攻撃活動が観測されたマルウェア「Emotet」は、実在する組織や人物にな

りすまして発信されたメールに添付された Word ファイルのマクロ機能によって感染させるもので、他のマルウェアに感染させるダウンローダーとしての機能も有するなど、機能拡充を繰り返

ながら感染を広げていた。

2021年1月、EUROPOL（欧州刑事警察機構）によるEmotetのテイクダウンが報じられた⁶。テイクダウン直後に感染端末内のEmotetを自動的に無害化する措置が取られ、4月には自動停止機能によってプロセスが削除されたことで、感染拡大が沈静化した。

国内では2021年2月に、総務省と警察庁、ICT-ISACが連名で「マルウェアに感染している機器の利用者に対する注意喚起の実施」を発表した⁷。これにより、インターネットサービスプロバイダー各社と連携し、Emotetに感染した端末を利用している組織に対して通知が行われた⁸。

2021年11月、Emotetに感染させようとする攻撃メールが再度観測された⁹。同年1月までの特徴に加え、Excelファイルが添付されたメールも確認されている。2019年と2020年の経験を踏まえて、組織内の注意喚起を行うことや感染時のインシデントに対応することが期待される。

●脆弱なSSL-VPN製品に対する攻撃の事例

昨年に引き続き、複数のネットワーク製品においてSSL-VPN機能に内在する脆弱性の公表や悪用があった。

2021年2月、米ソニックウォールのSMA100シリーズの脆弱性（CVE-2021-20016）が公表された¹⁰。同社は同年1月に、この脆弱性が悪用されていることを公表していた¹¹。7月には、同製品から窃取した認証情報を用いた攻撃キャンペーンについて注意喚起が行われている¹²。JPCERT/CCでも8月に、同製品からユーザーアカウント情報を窃取しようとする通信を確認したケースについてユーザーに通知し、対策を依頼した。9月には、SMA100シリーズの他の脆弱性（CVE-2021-20034）も公表されている¹³。

2021年9月、米フォーティネットはFortigate

から窃取された利用者の認証情報を攻撃者が公開したと明らかにした¹⁴。当該情報は、Fortigateで稼働するFortiOSの既知の脆弱性（CVE-2018-13379）を悪用して窃取されたとみられている。

COVID-19の感染拡大以降、テレワークの推進に当たりSSL-VPN製品を導入または利用拡大した組織が多いと想像できる。他のネットワーク機器同様、速やかな脆弱性対応がサイバー攻撃を防ぐために必要である。認証情報が公開されている機器があることも踏まえ、脆弱性対応時には認証情報のリセットも忘れずに行うことを推奨する。

■社会・インターネット基盤に影響する攻撃

●東京オリパラ開催に伴うサイバー攻撃

内閣サイバーセキュリティセンター（NISC）が公開した「東京オリンピック・パラリンピック競技大会におけるサイバーセキュリティ対策（結果報告）等」では、2021年7～9月に開催された東京オリンピック・パラリンピック競技大会に関連して「大会運営に影響を与えるようなサイバー攻撃は確認されなかった」としている¹⁵。確認されたのは、サイバー攻撃に関するSNS上の書き込みや不正な動画配信サイトのみであった。サイバーセキュリティ対処調整センターおよび同センターの情報共有プラットフォーム（JISP）が適切に運用され、関係者が協力して効果的な監視活動ができたことが功を奏したと考えられる。

●ランサムウェア攻撃の動向

ランサムウェア被害も、昨年に引き続き多数確認された¹⁶。ランサムウェアとは、ファイルを暗号化したり画面をロックしたりするなどして、パソコンやサーバーに保存されているファイルを利用できない状態にし、復旧と引き換えに金銭を要

求するマルウェアを指す。近年は、メールによって配付されるばらまき型だけでなく、組織内部に侵入して配備される標的型の割合が高まっている。なお、組織内部への侵入に当たっては脆弱なSSL-VPN製品が狙われるケースが増加している。

情報を窃取して、身代金が支払われないと暴露すると脅す「二重の脅迫」の手法も多く見られる。脆弱性管理を含むセキュリティ対策が疎かになりがちで、グループ企業や海外拠点などが狙われることが多く、グループ全体での網羅的な脆弱性情報の管理および対応が必須である。

最初に組織内に侵入するために、サプライチェーンを通じて埋め込まれた脆弱性が悪用された事例もあった。2021年7月、米カセヤのRMM製品であるKaseya VSAの脆弱性(CVE-2021-30116)が悪用され、同製品のオンプレミス版を利用するユーザーの環境が侵害された結果、ランサムウェアの感染被害が一挙に広がった¹⁷。本事例は、ユーザーに多くのMSP事業者が含まれており、各MSPサービスを利用するエンドユーザーがランサムウェアに感染するサプライチェーン攻撃となっている。

ランサムウェアを使った攻撃は、侵入後、数十時間から数日以内に暗号化やデータ窃取が迅速に行われることが多い。正規のプログラムを使用して侵害範囲を拡大させる場合もあり、検知することが困難なことも多い。バックアップデータが削除されたり暗号化されたりするケースもある。

さまざまな攻撃グループが暗躍しており、企業規模や業種を問わず被害が発生している。近年はRaaSとして分業化が進んでおり、ランサムウェアの開発者と攻撃者が異なるケースをはじめ役割が細分化されており、実態が捉えにくいだけではなく犯罪スキームとして効率的に運用されるようになっている。活動休止宣言後、攻撃グループ名やランサムウェア名を変更して活動再開するケー

スもあるため、個々のランサムウェアに特化した対策よりも、脆弱性管理などの基本的なセキュリティ対策を徹底する必要がある。これには、バックアップ取得方法の検討および復旧手順の定期確認といった準備が重要となる。被害を受けた場合には、安易に攻撃者との交渉や身代金支払いに依らず、専門機関に相談していただきたい。

●ランサムウェア攻撃による社会的影響

2021年5月、米国の石油パイプライン企業であるコロニアル・パイプラインがランサムウェア攻撃を受けた¹⁸。同社は約1週間にわたり操業の停止に追い込まれ、社会的に大きな影響を及ぼした。例えば、同社は米国東海岸における燃料供給の約45%を担っていたため、燃料不足を懸念した多くの消費者がガソリンスタンドに詰めかける事態となり、在庫切れやガソリン価格の上昇を招いた。事態を受け、米運輸省の連邦自動車運輸安全局(FMCSA)は18の州で緊急事態を宣言し、燃料輸送に関わるドライバーの長時間労働の緩和など、安定供給に向けた施策を取った¹⁹。ジョージア州がガソリン税を一時撤廃するなど影響を受けた他の州も対策を取り、消費者負担の軽減を図った。この攻撃は攻撃グループのダークサイド(DarkSide)によるものとされ、コロニアル・パイプラインは身代金として440万ドルを支払ったことが報道されている。この事例は、社会インフラを混乱させ高額の身代金が支払われたサイバー攻撃として、日本でも大きく報じられた。

2021年6月に、厚生労働省は「医療機関を標的としたランサムウェアによるサイバー攻撃について(注意喚起)」を公開した²⁰。国内外で医療機関を狙ったランサムウェア攻撃が発生していることを指摘し、ランサムウェアへの基本的な対応方法や平時の備えなどを掲載している。11月には、デジタル・フォレンジック研究会の「医療」分科

1 会と医療ISACが連携して「医療機関向けランサムウェア対応ガイドンス」を公開した²¹。前述の厚生労働省の資料を踏まえた、ランサムウェア対応の検討ポイントがまとめられている。

2 2021年下期には、国内でも医療機関を狙ったランサムウェア攻撃が確認されている。被害組織では電子カルテが使えなくなり、新規患者の受け

入れを一部停止するなど医療活動への影響が発生した。医療機関へのサイバー攻撃は、患者などの機微な情報が窃取されるだけではなく、時に人命に関わるインシデントに発展する可能性もあり、社会的影響が大きい。SSL-VPN製品が侵入経路となっているケースが多く見られ、適切な脆弱性管理の重要性が示唆される。

1. フィッシング対策協議会、「2021/08 フィッシング報告状況」
<https://www.antiphishing.jp/report/monthly/202108.html>
2. フィッシング対策協議会、「2021/10 フィッシング報告状況」
<https://www.antiphishing.jp/report/monthly/202110.html>
フィッシング対策協議会、「2021/11 フィッシング報告状況」
<https://www.antiphishing.jp/report/monthly/202111.html>
3. フィッシング対策協議会、「2021/07 フィッシング報告状況」
<https://www.antiphishing.jp/report/monthly/202107.html>
4. JPCERT/CC、「STOP! パスワード使い回し!」
<https://www.jpccert.or.jp/pr/stop-password.html>
5. ブルーポイント、「ブルーポイントの調査により日経225企業の75%および日本政府が「なりすましメール詐欺」に有効な対策ができていないことが判明」
https://www.proofpoint.com/jp/newsroom/press-releases/nikkei225_DMARC_analysis_2021
6. EUROPOL, "World's most dangerous malware EMOTET disrupted through global action"
<https://www.europol.europa.eu/newsroom/news/world-s-most-dangerous-malware-emetet-disrupted-through-global-action>
7. 総務省、「マルウェアに感染している機器の利用者に対する注意喚起の実施」
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00095.html
8. NOTICE、「Emotet への対応」
<https://notice.go.jp/emotet/>
9. 情報処理推進機構、「Emotet の攻撃活動再開について (2021 年 11 月 16 日追記)」
<https://www.ipa.go.jp/security/announce/20191202.html>
10. JPCERT/CC、「SonicWall 製 SMA100 シリーズの脆弱性 (CVE-2021-20016) に関する注意喚起」
<https://www.jpccert.or.jp/at/2021/at210006.html>
11. SonicWall, "SonicWall Publishes Additional SMA 100 Series 10.x and 9.x Firmware Upgrades"
<https://www.sonicswall.com/blog/2021/01/security-notice-update-on-sma-100-series-product-investigation/>
12. SonicWall, "Urgent Security Notice: Critical Risk to Unpatched End-of-Life SRA & SMA 8.x Remote Access Devices"
<https://www.sonicswall.com/support/product-notification/urgent-security-notice-critical-risk-to-unpatched-end-of-life-sra-sma-8-x-remote-access-devices/>
13. JPCERT/CC、「SonicWall 製の SMA100 シリーズの脆弱性 (CVE-2021-20034) に関する注意喚起」
<https://www.jpccert.or.jp/at/2021/at210042.html>
14. フォーティネット、「悪意のあるアクターがFortiGate SSL-VPN の認証情報を公開」
<https://www.fortinet.com/jp/blog/psirt-blogs/malicious-actor-discloses-fortigate-ssl-vpn-credentials>
15. NISC, 「東京オリンピック・パラリンピック競技大会におけるサイバーセキュリティ対策 (結果報告) 等について」
<https://www.nisc.go.jp/conference/cs/dai31/pdf/31shiryou04.pdf>
16. 警察庁、「令和3年上半期におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_kami_cyber_jousei.pdf
17. Kaseya, "Updates Regarding VSA Security Incident"
<https://www.kaseya.com/potential-attack-on-kaseya-vsa/cisa-cisa-fbi-guidance-for-msp-and-their-customers-affected-by-the-kaseya-vsa-supply-chain-ransomware-attack>
18. CISA, "DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks"
<https://us-cert.cisa.gov/ncas/alerts/aa21-131a>
19. FMCSA, "ESC-SSC-WSC - Regional Emergency Declaration 2021-002 - 05-09-2021"
<https://www.fmcsa.dot.gov/emergency/esc-ssc-wsc-regional-emergency-declaration-2021-002-05-09-2021>
20. 厚生労働省、「医療機関を標的としたランサムウェアによるサイバー攻撃について (注意喚起)」
<https://www.mhlw.go.jp/hourei/doc/tsuchi/T210630U010.pdf>
21. デジタル・フォレンジック研究会、「「医療機関向けランサムウェア対応検討ガイドンス」の公開」
<https://digitalforensic.jp/2021/11/25/medhi-18-gl/>



1996, 1997, 1998, 1999, 2000, ...

[インターネット白書ARCHIVES] ご利用上の注意

このファイルは、株式会社インプレスR&Dおよび株式会社インプレスが1996年～2022年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書 ARCHIVES」として以下のウェブサイトで公開しているものです。

<https://IWParchives.jp/>

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容(技術解説、データ、URL、名称など)は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者(執筆者、写真・図の作成者、編集部など)が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&Dおよび株式会社インプレスと著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接のおよび間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先

インプレス・サステナブルラボ

✉ iwp-info@impress.co.jp