2022年の情報セキュリティ動向

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

2022年は、2021年にテイクダウンされたマルウエアのEmotetが復活し、以前を上回る猛威を振るった。さらに、SSL-VPN製品の脆弱性を利用した攻撃とサプライチェーン攻撃も頻発した。

■セキュリティインシデントの報告件数

2022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5万8389件（2021年は4万3161件）であった（資料4-1-1）[1]。このうち「スキャン」の報告は2021年と比較して大幅に増加している（資料4-1-2）。全体に占める割合では、2021年と同様に国内ブランドを装ったフィッシングサイトが最も多かった。

■個人ユーザーを対象とした攻撃

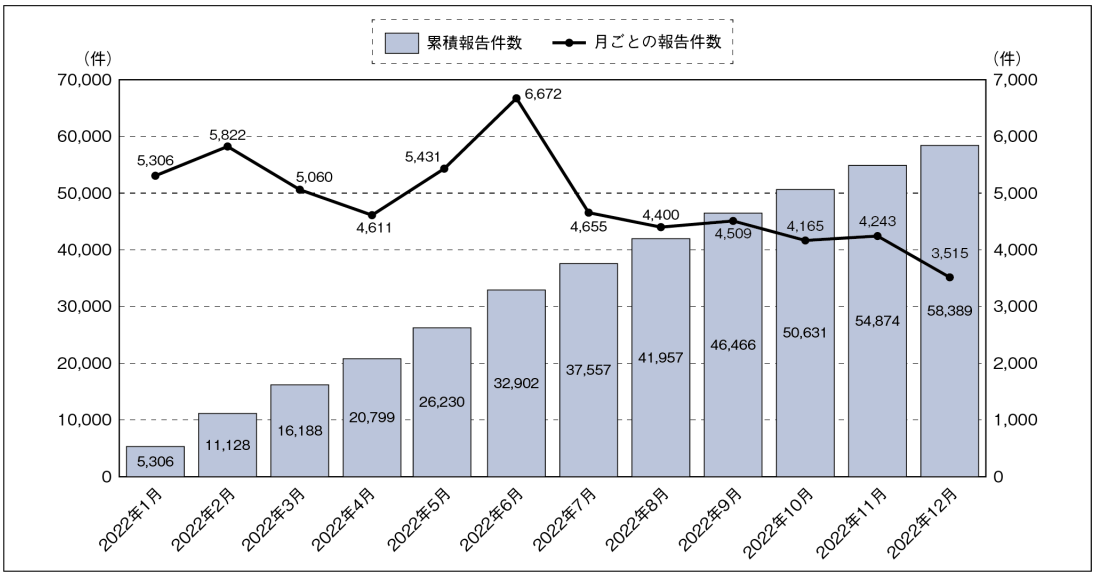
●偽サイトへ誘導するメッセージ

2022年も、2021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、それを詐取するというものである。Androidスマートフォンの利用者は、不正なアプリケーション（マルウエア等）をインストールするように誘導されることもある。

2022年6～9月にクレジットカードの利用確認を装うフィッシング[2]が、8～10月に国税庁を模した偽サイトへ誘導するフィッシング[3]が、8～9月にメールに記載されたGoogle翻訳の正規URLをクリックするとそのURLからECサイトやクレジットカードブランドなどをかたるウェブサイトへ誘導されるフィッシング[4]が確認された。この、Google翻訳の正規URLを利用したフィッシングの場合にはURLフィルターで警告が出ないため、注意が必要である。

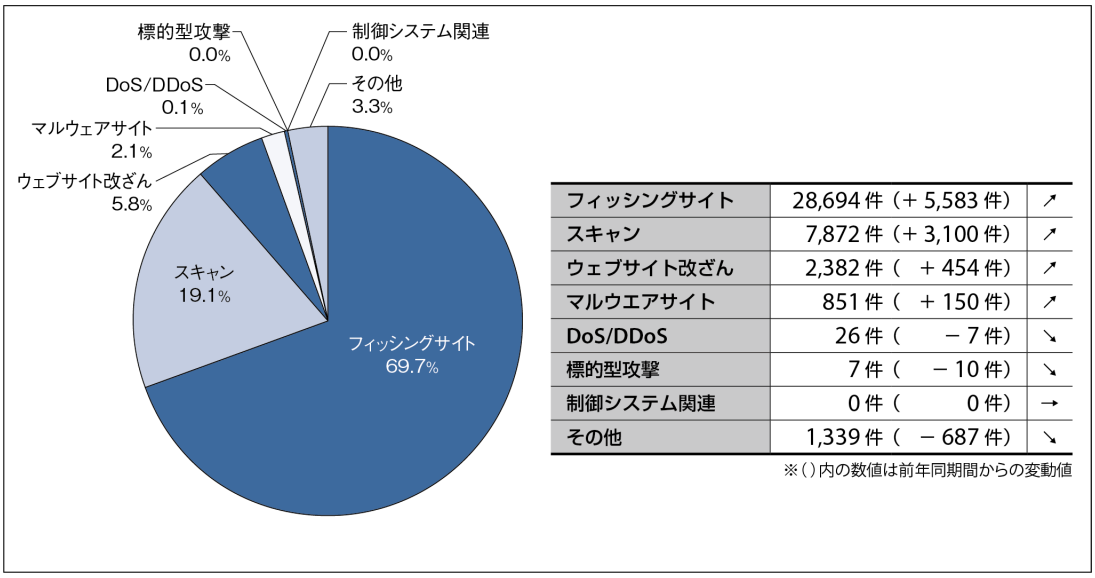
フィッシングメール対策はユーザー側の警戒だけではなく、フィッシングメールか否かをユーザー（メールサービス側）が検出しやすくするための事業者側（ドメインホルダー）の対応も重要であるが、現時点ではそれが不十分であると言わざるを得ない。特に、差出人メールアドレスを詐称するなりすまし送信メールのケースでは、送信ドメイン認証技術の一つであるDMARC（Domain-based Message Authentication, Reporting, and Conformance）が有効である。DMARCは、正規のサーバーから送信されたかを検証するSPF（Sender Policy Framework）と電子署名でメールを検証するDKIM（DomainKeys Identified Mail）の結果を使って検証する技術であるが、現時点では普及率は高くない。フィッシング対策協議会ではDMARC

資料4-1-1　インシデント報告件数の推移（2022年1～12月）



出所：JPCERT/CC、「インシデント報告対応レポート」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ー別内訳（2022年1～12月）



フィッシングサイト	28,694件（＋5,583件）	↗
スキャン	7,872件（＋3,100件）	↗
ウェブサイト改ざん	2,382件（　＋454件）	↗
マルウエアサイト	851件（　＋150件）	↗
DoS/DDoS	26件（　－7件）	↘
標的型攻撃	7件（　－10件）	↘
制御システム関連	0件（　0件）	→
その他	1,339件（　－687件）	↘

※（）内の数値は前年同期間からの変動値

出所：JPCERT/CC、「インシデント報告対応レポート」を基に作成

の導入を推奨しており、DMARC検証と迷惑メールフィルターを併用することで、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[5]。また、同協議会では、事業者向けの「フィッシング対策ガイドライン」を毎年改訂しており、対策の重要性を説いている[6]。

■法人や組織を対象とした攻撃

●Emotetの動向

マルウエアのEmotetは、2020年に世界的に感染が拡大した。Emotetに感染すると実在する組織や人物になりすましたメールが発信される。このメールにはWordファイルやExcelファイルが添付されていて、これらのファイルに組み込まれたマクロによってメールの受信者を感染させる。さらに、他のマルウエアをダウンロードして感染させるダウンローダーとしての機能も有する。

攻撃集団はEmotetの機能拡充を繰り返しながら感染を拡大させたが、2021年1月にEmotetをコントロールしていたC2サーバーが法執行機関によって差し押さえられ、Emotetのテイクダウンが成功した[7]。Emotetを使用していた攻撃集団のメンバーの一部も逮捕され、Emotetに感染した端末は法執行機関が管理するC2サーバーとのみ通信を行うようになった。その後、感染した端末上のEmotetも2021年4月に停止する機能が加えられ、無害化されたファイルに自動的に更新された。

しかし、2021年11月にEmotetをコントロールする新しいC2サーバーとマルウエアサンプルが確認され、感染再開が日本を含む世界各国で確認された。2022年2月からはEmotetの感染が急速に拡大した[8]。具体的には、感染拡大を試みるスパムメール送信に悪用される可能性のあるEmotetに感染した端末が利用している国内ドメイン（.jp）のメールアドレスの数が、2020年の感染ピーク時の約5倍を超す水準まで急増した。2022年4月には、ショートカットファイル（LNKファイル）あるいはそれを含むパスワード付きZIPファイルを添付したメールが新たに観測された。これは、WordやExcelのマクロやコンテンツ有効化を必要としない方法での感染を目的とした手法の変化である可能性がある。

Emotetに感染すると、取引先や顧客の連絡先とメールの内容が窃取され外部に送信されたり、外部の組織に大量の不正なメールが送信されたり、ダウンロードされる他のマルウエアに感染したりする恐れがある。

●脆弱なSSL-VPN製品に対する攻撃の事例

2021年に引き続き、SSL-VPN機能に内在する脆弱性の公表や悪用が複数のネットワーク製品において見られた。

2021年7月、ソニックウォール製の「SonicWall Secure Mobile Access（SMA）100シリーズ」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た[9]。2021年12月には、同製品の脆弱性（CVE-2021-20038）が公表された[10]。その後、2022年1月にこの脆弱性を悪用する通信が観測されている。さらに、窃取された認証情報を利用して侵入された事例も見られた。

2021年9月、多数のフォーティネット製ForiOS SSL-VPNから認証情報を攻撃者が窃取し、それを公開した[11]。2022年12月には、同製品のヒープベースのバッファオーバーフローの脆弱性[12]とこれを悪用する攻撃が確認されていることを同社が公表した。ほかにも、上記のソニックウォール製品と同様に、公表された認証情報を利用して侵入された事例が見られた。

SSL-VPN製品の大半が、リセラーやSIer経由で販売／導入されており、日本法人や日本総代理店は直接ユーザーに販売／サポートをしていない。そのため、脆弱性などの重要な情報が製造事業者からユーザーに伝わるルートがないことが多い。SIerがシステムを引き渡した後の保守契約がない、あるいは保守契約があってもハードウエアトラブル等の対応が主たる作業内容で、脆弱性の修正対応が明示的に契約に含まれていないケースも多い。こうした商流の下では、脆弱性情報が

ユーザーに届かない、あるいは修正対応がなされない。このような現状を打破するには、個別の運用保守契約の変更／追加や、そもそも誰がどのように費用的負担をするのか、といった検討をしなければならない[13]。

●F5 BIG-IPの脆弱性を利用した攻撃の事例

2022年5月に、F5 BIG-IPの脆弱性（CVE-2022-1388）を悪用した日本の組織に対する攻撃活動があった[14]。この事案ではBIG-IP内のデータが漏えいするなどの被害が確認された。この攻撃は、攻撃グループであるBlackTechの活動と関連しているものと推測している。

●サプライチェーン攻撃

2022年も、サプライチェーン攻撃によるランサムウエア被害が確認された。サプライチェーン攻撃は大きく分けて、ソフトウエアサプライチェーン攻撃、サービスサプライチェーン攻撃、ビジネスサプライチェーン攻撃の3種類に分類できる[15]。

ソフトウエアサプライチェーン攻撃は、ソフトウエアの製造や提供の工程を侵害し、ソフトウエアそのものやアップデートプログラムなどに不正コードを混入させて、標的組織に侵入する攻撃を指す。サービスサプライチェーン攻撃は、マネージド・サービス・プロバイダー（MSP）などのサービス事業者を侵害し、サービスを通じて顧客に被害を及ぼす攻撃を指す。ビジネスサプライチェーン攻撃は、標的組織の取引先やグループ会社などパートナー企業への攻撃により、当該企業の事業活動に支障が生じたり、標的組織が提供した重要な情報が流出してしまったり、当該企業を踏み台に自社が攻撃されたりする可能性のある攻撃を指す。

2022年5月には、MSP事業者が警戒する必要があるという警告を「ファイブアイズ（Five Eyes）」と総称される英国とオーストラリア、カナダ、ニュージーランド、米国から成る諜報同盟が発信した[16]。

■社会・インターネット基盤に影響する攻撃

●ゼロデイ脆弱性を突かれた攻撃

2022年は、ゼロデイ脆弱性を突いた攻撃が2021年よりも多く見られた。2021年12月に発見されたApache Log4j 2の脆弱性（CVE-2021-44228）[17]や2022年3月に発見されたSpring Frameworkの脆弱性（CVE-2022-22965）[18]、2022年9月に発見されたMicrosoft Exchange Serverの脆弱性（CVE-2022-41040およびCVE-2022-41082）[19]などがゼロデイ脆弱性として挙げられる。

●ランサムウエア攻撃の動向

2021年に引き続き、多くのランサムウエア被害も確認された。ランサムウエア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エアを指す。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侵入型の割合が高まっている。

2022年に見られた組織内部への侵入の手口には、イニシャル・アクセス・ブローカーのリスト[20]を利用する、脆弱なSSL-VPN製品を狙う、外部から接続可能なリモート・デスクトップ・サービスの認証を突破するなどがあり、侵入手口が多様化している。

2022年は、ランサムウエアのLockBitが猛威を振るい、日本国内でも被害があった。2022年6月、バグ報奨金プログラムやZcash支払いなど

を含む新機能が導入されたLockBit 3.0がリリースされた[21]。LockBitによる攻撃では、侵入後、数十時間から数日以内に暗号化やデータ窃取が行われる場合が多い。侵入後の潜在期間が短く、ラテラルムーブメントや外部との通信が少ないことから、検知が難しい。そのため、ランサムウエアの挙動をアンチウイルス製品で検知できていたとしても、その時点ではすでに暗号化されてしまっている。また、バックアップデータを削除される、ないし暗号化されるケースもある。

これまで、JPCERT/CCは多数の脆弱性に関する注意喚起や、イニシャル・アクセス・ブローカーによって認証情報が漏えいした際や脆弱なままになっている対象機器を発見した際に対する通知作業を進めてきた。しかし、残念ながら修正されていない機器が稼働を続け、その後、標的型サイバー攻撃や侵入型ランサムウエア攻撃被害を受けるケースが後を絶たない。また、上記の通知オペレーションと並行して、SSL-VPN製品の流通経路上の現状についてヒアリングなども行ってきた。

JPCERT/CCでは、企業や組織の内部ネットワークに攻撃者が侵入した後、情報窃取やランサムウエアを用いたファイルの暗号化などを行う攻撃の被害に遭った場合の対応のポイントや留意点などを、FAQ形式で記載したものを用意している[22]。ぜひご活用いただきたい。

●ランサムウエア攻撃による社会的影響

2022年2月、トヨタ自動車のサプライヤーである小島プレス工業が攻撃を受け[23]、トヨタ自動車は国内の工場をすべて停止することになった。そのため、同社は数日間自動車生産を停止せざるを得ない状況となり、約1万3000台の生産スケジュールを遅らせることとなった。

2022年7月、カナダ・オンタリオ州にあるセント・メアリーズ市がLockBitの攻撃を受けた[24]。この攻撃で同市は、盗んだ公共事業などに関する文書を公開すると脅迫された。同年11月に、オンタリオ州警察が本攻撃に関与した疑いのあるロシアとカナダの二重国籍者を逮捕している。

2022年下期には、国内で医療機関を狙ったランサムウエ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、緊急以外の手術や外来診療の一時停止で通常診療ができない状況となるなど、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可能性だけでなく、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ることから、適切な脆弱性管理の重要性が示唆される。

1. インシデント報告対応レポート
   https://www.jpcert.or.jp/ir/report.html
2. クレジットカードの利用確認を装うフィッシング（2022/06/24）
   https://www.antiphishing.jp/news/alert/creditcard_20220624.html
3. 2022/08 フィッシング報告状況
   https://www.antiphishing.jp/report/monthly/202208.html
4. Google 翻訳の正規URLから誘導されるフィッシング（2022/08/09）
   https://www.antiphishing.jp/news/alert/googletranslate_20220809.html
5. なりすまし送信メール対策について
   https://www.antiphishing.jp/enterprise/domain_authentication.html
6. フィッシング対策ガイドライン2022年度版
   https://www.antiphishing.jp/report/antiphishing_guideline_2022.pdf
7. World´s most dangerous malware EMOTET disrupted through global action
   https://www.europol.europa.eu/media-press/newsroom/news/world's-most-dangerous-malware-emotet-disrupted-through-global-action
8. マルウェアEmotetの感染再拡大に関する注意喚起

https://www.jpcert.or.jp/at/2022/at220006.html
9. SonicWall SMA100 シリーズの複数の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2022/at220004.html
10. Urgent Security Notice: Critical Risk to Unpatched End-of-Life SRA & SMA 8.x Remote Access Devices
https://www.sonicwall.com/support/product-notification/urgent-security-notice-critical-risk-to-unpatched-end-of-life-sra-sma-8-x-remote-access-devices/210713105333210/
11. 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
12. FortiOS のヒープベースのバッファーオーバーフローの脆弱性（CVE-2022-42475）に関する注意喚起
https://www.jpcert.or.jp/at/2022/at220032.html
13. なぜ、SSL-VPN 製品の脆弱性は放置されるのか～“サプライチェーン”攻撃という言葉の陰で見過ごされている攻撃原因について～
https://blogs.jpcert.or.jp/ja/2022/07/ssl-vpn.html
14. 攻撃グループ BlackTech による F5 BIG-IP の脆弱性（CVE-2022-1388）を悪用した攻撃
https://blogs.jpcert.or.jp/ja/2022/09/bigip-exploit.html
15. サプライチェーン攻撃とは？～攻撃の起点別に手法と事例を解説～
https://www.trendmicro.com/ja_jp/jp-security/22/j/securitytrend-20221024-03.html
16. Protecting Against Cyber Threats to Managed Service Providers and their Customers
https://www.cisa.gov/uscert/ncas/alerts/aa22-131a
17. Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210050.html
18. Spring Framework の任意のコード実行の脆弱性（CVE-2022-22965）について
https://www.jpcert.or.jp/newsflash/2022040101.html
19. 2022 年 10 月マイクロソフトセキュリティ更新プログラムに関する注意喚起
https://www.jpcert.or.jp/at/2022/at220028.html
20. 漏えいした SSL-VPN 製品の認証情報リストやダークウェブで販売されているリスト等のこと。
21. LockBit 3.0 introduces the first ransomware bug bounty program
https://www.bleepingcomputer.com/news/security/lockbit-30-introduces-the-first-ransomware-bug-bounty-program/
22. 侵入型ランサムウェア攻撃を受けたら読む FAQ
https://www.jpcert.or.jp/magazine/security/ransom-faq.html
23. ウィルス感染被害によるシステム停止事案発生のお知らせ
https://www.kojima-tns.co.jp/wp-content/uploads/2022/08/ウィルス感染被害によるシステム停止事案発生のお知らせ-2.pdf
24. A small Canadian town is being extorted by a global ransomware gang
https://www.theverge.com/2022/7/22/23274372/st-marys-canada-lockbit-ransomware-cyber-incident

インターネット白書 ARCHIVES

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～2023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的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