2023年の情報セキュリティ動向

世古 裕紀 ●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

2023年は、SSL-VPN製品やオンラインストレージの構築に用いられる製品で新たに見つかった脆弱性を悪用した攻撃に加えて、社会インフラを狙う深刻なランサムウエア攻撃が目立った。

■セキュリティインシデントの報告件数

2023年の1月から12月までに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6万5669件（2022年は5万8389件）であった（資料4-1-1）。インシデントの内訳は「ウェブサイト改ざん」や「マルウエアサイト」の報告が大幅に減少するなど、2022年から大きく変化した（資料4-1-2）。

■個人ユーザーを対象とした攻撃

●フィッシングサイトへ誘導するメッセージ

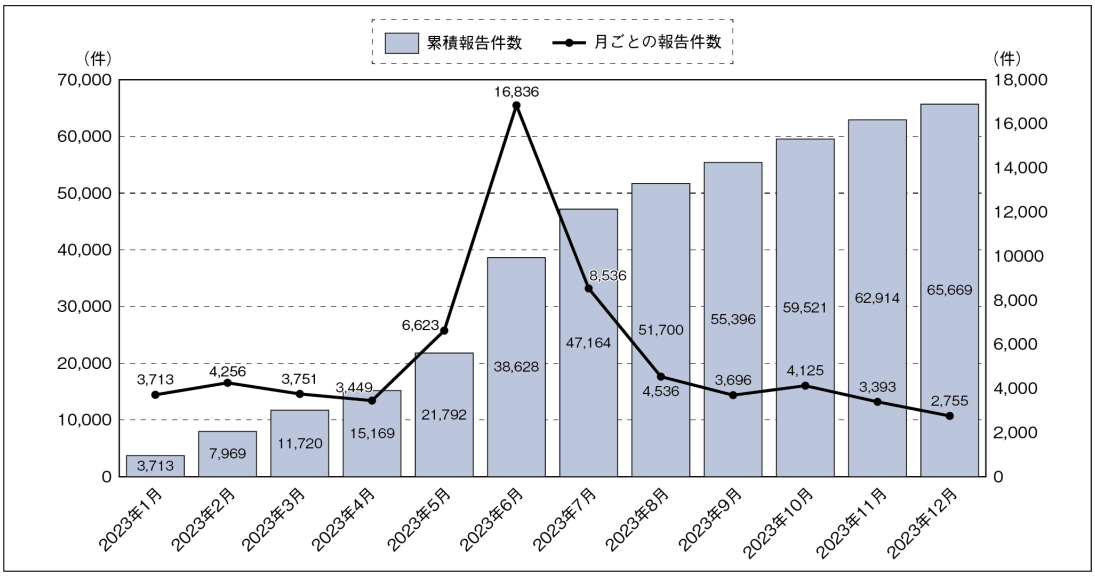
2022年に引き続き、2023年も多くの利用者を擁するサービスを装ったメールやSMSで送り付けられたメッセージが多数報告された。ユーザーがメッセージ内に記載されたリンクを開くと攻撃者が用意した偽サイトへ誘導され、この偽サイトで認証情報（IDやパスワード）をはじめとする個人情報を入力させて、それを窃取するというものである。Android搭載スマートフォンでアクセスした場合は、不正なアプリケーション（マルウエア等）のインストールサイトへ誘導されることもある。

2022年までと同様、銀行やクレジットカード会社など金融関連のウェブサイトを装ったものの割合が多かった。特殊なケースとして、2023年10月にはURLのアルファベットが罫線で囲まれた飾り文字などが含まれたメッセージ[1]、同年11月にはIPアドレスを8進数や16進数などで表記してフィルター回避を試みていると推測されるURLを用いたメッセージ[2]が確認されている。さらにJPCERT/CCでは、フィッシングサイト経由で窃取した認証情報を悪用して、ドメインを不正に別のレジストラーに移管する事案を2023年7月に確認したとして、情報を公開している[3]。

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といった、基本的な行動の徹底が求められる[4]。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[5]。

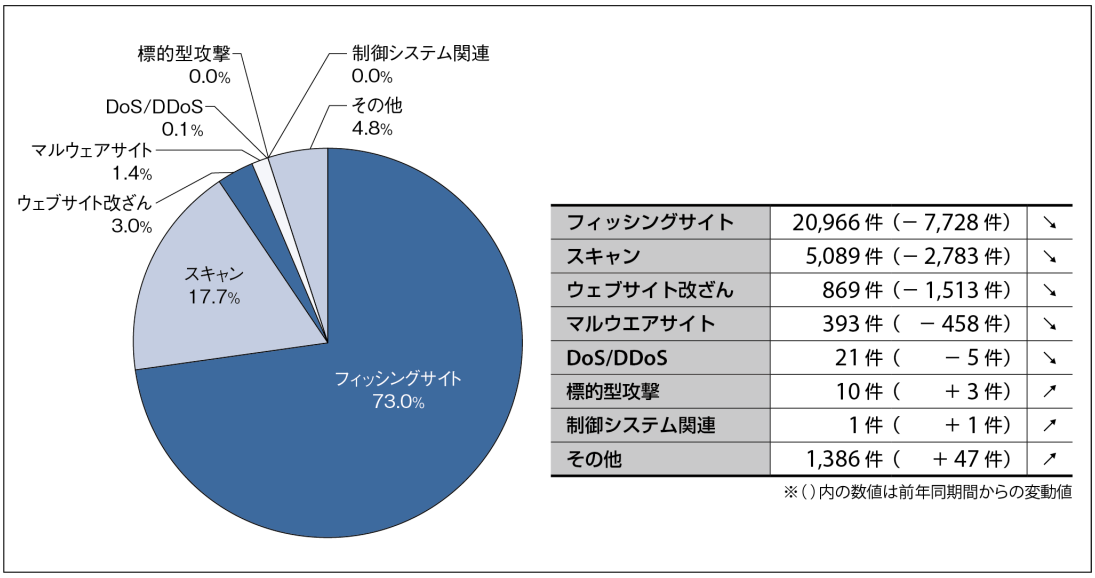
フィッシング対策は、ユーザーが警戒するだけではなく事業者側の対策も重要である。フィッシング対策協議会ではDMARCの導入を推奨しており、DMARC検証と迷惑メールフィルターを併用することで、なりすましメールの多くを検知できることを確認している[6]。メール・セキュリティ・ベンダーのTwoFiveが2023年1月から5月にかけて行った調査によると、日経225の企業におけるDMARC導入率は62.2％と、1年で12.4ポイン

資料4-1-1　インシデント報告件数の推移（2023年）



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（2023年）



フィッシングサイト	20,966件（－7,728件）	↘
スキャン	5,089件（－2,783件）	↘
ウェブサイト改ざん	869件（－1,513件）	↘
マルウエアサイト	393件（　－458件）	↘
DoS/DDoS	21件（　　－5件）	↘
標的型攻撃	10件（　　＋3件）	↗
制御システム関連	1件（　　＋1件）	↗
その他	1,386件（　＋47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

ト増加しており、国内でも着実に浸透していることがうかがえる[7]。

■法人や組織を対象とした攻撃

●マルウエア「Emotet」の動向

2020年に世界的に攻撃活動が報告されたマルウエアであるEmotetは、感染したパソコンから窃

取した情報に基づいて実在する組織や人物になりすましてメールを発信し、そのメールに添付されたWordファイルやExcelファイルのマクロ機能によってメールの受信者のパソコンを感染させるもので、他のマルウエ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、機能拡充を繰り返しながら感染を広げていた。2022年11月以降、しばらく活動が沈静化していたが、2023年3月に再び活動が確認された。その際の攻撃では、メールに添付されたZIP形式の圧縮ファイルを展開すると500MBを超えるWordファイルになるという、これまでにない特徴を有していた。これは、展開後のサイズを大きくすることによってアンチウイルス製品などに検知されないようにしていると考えられる。加えて、Microsoft OneNote形式のファイルを添付するメールも確認されている[8]。

Emotetに感染すると、感染したパソコンから取引先や顧客のメールアドレス、過去のメールの内容などが窃取され、それらを利用して外部の組織に大量の不審メールが送信される。さらに、ダウンロードされる他のマルウエアにパソコンを感染させられる恐れもある。感染や被害の拡大を防ぐためにも、改めて適切な対策や対処ができているかの確認や点検を推奨する。

●SSL-VPN機能の脆弱性を悪用した攻撃の事例

ネットワーク製品のSSL-VPN機能に内在する脆弱性の公表や悪用も、2022年に引き続き見られた。

2023年3月、アレイ・ネットワークスのArray AGシリーズにおけるリモートコード実行の脆弱性（CVE-2023-28461）が公表された。2022年4月にも同製品におけるコマンドインジェクションの脆弱性（CVE-2022-42897）が公表されているが、2022年5月以降、これらの脆弱性を悪用する標的型サイバー攻撃が断続的に確認されている。攻撃は国内のみならず海外拠点も標的となっているため、JPCERT/CCでは自組織の海外拠点における対策や侵害の有無を調査するように推奨している[9]。

新型コロナウイルスの感染拡大以降、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く、そこが攻撃者の狙い目になっていると想像できる。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。

●NetScalerの脆弱性を悪用した攻撃の事例

2023年7月、シトリックス・システムズの「NetScaler ADC」および「NetScaler Gateway」（旧名：Citrix ADCおよびCitrix Gateway）におけるリモートコード実行の脆弱性（CVE-2023-3519）[10]、同年10月は同製品における情報漏えいの脆弱性（CVE-2023-4966）が公表された[11]。いずれの脆弱性に関しても悪用する攻撃を確認したとして、シトリックスが対策を呼びかけている。

●Cisco IOS XEの脆弱性を悪用した攻撃の事例

2022年10月、シスコシステムズのソフトウエア「Cisco IOS XE」のWeb UI機能における脆弱性（CVE-2023-20198、CVE-2023-20273）が公表された[12]。同社の調査によると、攻撃者はCVE-2023-20198を悪用してシステムに侵入し、最上位の特権レベルのコマンドを発行して新たなローカルユーザーを作成する。その後、CVE-2023-20273を悪用し、作成したローカルユーザーの権限をルートに昇格させ、インプラントをファイルシステムに書き込んだとのことである。JPCERT/CCでは本脆弱性を悪用した攻撃による被害を確認しており、侵害の有無の調査と対

策の実施を呼びかけている。

●Proselfの脆弱性を悪用した攻撃の事例

2023年8月、ノースグリッドのオンラインストレージ構築製品「Proself」における認証不備の脆弱性（CVE-2023-39415）、およびOSコマンドインジェクションの脆弱性（CVE-2023-39416）が公表された[13]。同年11月には、同製品のXML外部実体参照（XXE）の脆弱性（CVE-2023-45727）も公表された[14]。いずれの脆弱性に関しても悪用する攻撃を確認したとして、ノースグリッドは侵害の有無の調査や対策の実施を呼びかけている。

Proself以外にも、オンラインストレージ関連製品を狙った攻撃が継続して発生している。メールに代わるデータ授受の手段としてこのような製品を利用したサービスが昨今主流になっているが、製品ベンダーや外部専門機関からの脆弱性・脅威情報の収集、ログを基にした侵害の調査や迅速な脆弱性対策の適用といった対応が円滑に行えるように、平時から備えておくことが重要である。

■社会・インターネット基盤に影響する攻撃

●ランサムウエア攻撃の動向

多くのランサムウエア被害も、2022年に引き続き確認された。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。従来は、メールやウェブサイトによって配布されるばらまき型が主流であったが、近年はSSL-VPNなどのネットワーク機器やリモートデスクトップを介して外部から組織内部のネットワークに侵入し攻撃を行う、侵入型の割合が高まっている。2020年から2021年ごろは、過去に漏えいしたネットワーク機器やリモートデスクトップの認証情報が、イニシャルアクセスブローカーと呼ばれる違法な販売者によって他の攻撃グループに流通したり、公開情報として拡散したりして、悪用される事案が多発していた。攻撃の準備段階の手間が減ったことで、新たな攻撃グループの増加につながったとみられる。2022年以降は、過去の認証情報漏えいに起因しているとは明確に判断できない事案が増えつつある。新たに見つかった機器の脆弱性の悪用や、パスワードを総当たりで試行することによって認証突破を試みるブルートフォース攻撃の可能性が疑われる。

身代金が支払われないとシステムの可用性を取り戻せないだけでなく、窃取した情報も暴露すると脅す「二重の脅迫」の手法も多く見られる。セキュリティ対策がおろそかになりがちなグループ企業や海外拠点などが狙われるケースが多く、グループ全体での対策が必須である。

最近のランサムウエアを使った攻撃は、侵入後、数十時間から数日以内に、迅速に行われることが多い。潜伏期間が短く、ラテラルムーブメントや外部との通信が少ないため、攻撃を検知するチャンスが少ない。ランサムウエアの実行自体はアンチウイルス製品で検知できることが多いが、あっという間に暗号化されるため、それに気付いた頃にはすでに手遅れとなってしまう。さらに、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。

また、近年はRaaSとして攻撃者の分業化が進んでいる。ランサムウエアの開発者と攻撃者が異なるなど役割が細分化されており、実態が捉えにくいだけでなく、犯罪スキームとして効率的に攻撃が行わ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エア名を変更して活動を再開する攻撃集団もある。多様化し変化も速いので、個々のランサムウエアに特化した

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の徹底が必要である。バックアップの取得方法の検討および復旧手順の定期確認などの、万一の感染への備えも重要である。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応じず、専門機関に相談していただきたい。

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形式で記載した文書を用意しているので、活用していただきたい[15]。

●ランサムウエア攻撃による社会的影響

2023年7月、NUTS（名古屋港統一ターミナルシステム）がランサムウエア攻撃を受けた。この攻撃によって名古屋港の全ターミナルが稼働停止を余儀なくされ、復旧までの丸2日以上、搬出入作業が滞った。名古屋港は総取扱貨物量が国内一の港[16]であるため、当該事案の社会的影響は大きなものであった。

●ランダムサブドメイン攻撃の被害発生

2023年上半期、世界中でランダムサブドメイン攻撃（DNS水責め攻撃）の報告が散発的に確認され、日本国内においても多数の組織で同攻撃によると考えられる被害が確認された。ランダムサブドメイン攻撃はDDoS攻撃手法の一つであり、攻撃対象の権威DNSサーバーに対して、実在しないサブドメインを含むDNS問い合わせを大量に送り付ける攻撃である。キャッシュが存在しないためすべての問い合わせが権威DNSサーバーに送られることになり、アクセス不能の状態に陥れることを狙っているとされる。攻撃を行っているアクターやその目的は判然としないが、今後も警戒が必要である。

1. フィッシング対策協議会、「緊急情報：URLに飾り文字などが含まれたフィッシング（2023/10/17）」 https://www.antiphishing.jp/news/alert/decourl_20231017.html
2. フィッシング対策協議会、「緊急情報：URLに特殊なIPアドレス表記を用いたフィッシング（2023/11/14）」 https://www.antiphishing.jp/news/alert/ipurl_20231114.html
3. JPCERT/CC、「フィッシングサイト経由の認証情報窃取とドメイン名ハイジャック事件」、2023年10月25日 https://blogs.jpcert.or.jp/ja/2023/10/domain-hijacking.html
4. フィッシング対策協議会、「利用者向けフィッシング詐欺対策ガイドライン2023年度版」、2023年6月1日 https://www.antiphishing.jp/report/consumer_antiphishing_guideline_2023.pdf
5. JPCERT/CC、「STOP! パスワード使い回し!」 https://www.jpcert.or.jp/pr/stop-password.html
6. フィッシング対策協議会、「なりすまし送信メール対策について」 https://www.antiphishing.jp/enterprise/domain_authentication.html
7. TwoFive、「TwoFive、なりすましメール対策実態調査の最新結果を発表」、2023年5月18日 https://www.twofive25.com/news/20230518_dmarc_report.html
8. JPCERT/CC、「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. JPCERT/CC、「Array Networks Array AGシリーズの脆弱性を悪用する複数の標的型サイバー攻撃活動に関する注意喚起」 https://www.jpcert.or.jp/at/2023/at230020.html
10. JPCERT/CC、「Citrix ADCおよびCitrix Gatewayの脆弱性（CVE-2023-3519）に関する注意喚起」 https://www.jpcert.or.jp/at/2023/at230013.html
11. JPCERT/CC、「Citrix ADCおよびCitrix Gatewayの脆弱性（CVE-2023-4966）に関する注意喚起」 https://www.jpcert.or.jp/at/2023/at230026.html
12. JPCERT/CC、「Cisco IOS XEのWeb UIの脆弱性（CVE-2023-20198）に関する注意喚起」 https://www.jpcert.or.jp/at/2023/at230025.html
13. JPCERT/CC、「Proselfの認証バイパスおよびリモートコード実行の脆弱性に関する注意喚起」 https://www.jpcert.or.jp/at/2023/at230014.html
14. JPCERT/CC、「ProselfのXML外部実体参照（XXE）に関する脆弱性を悪用する攻撃の注意喚起」 https://www.jpcert.or.jp/at/2023/at230022.html
15. JPCERT/CC、「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

16. 名古屋港管理組合、「名古屋港の実力」
https://www.port-of-nagoya.jp/shokai/kohoshiryo/1001907/1001909.html

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～2024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