2024年の情報セキュリティ動向

藤堂 伸勝 ●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

正規ツールを使用して長期間の潜在をもくろんだ高度なサイバー攻撃が見つかった。また、複数の法執行機関による共同捜査でランサムウエア攻撃グループを摘発するも、ランサムウエア被害が続いた。

■セキュリティインシデントの報告件数

2024年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4万7677件（2023年は6万5669件）であった（資料4-1-1）[1]。インシデントの内訳は、2023年と比べて「スキャン」「ウェブサイト改ざん」「マルウエアサイト」の割合が減少し、「フィッシングサイト」の割合が増加した（資料4-1-2）。

■個人ユーザーを対象とした攻撃

個人を狙ったサイバー攻撃は、心理的な隙を巧みに突いた詐欺的手口を用いる。代表的な手口として、実在するサービスのメールやSMSを装って偽サイトに誘導するフィッシング、偽の警告画面に表示されたサポート窓口に電話させるサポート詐欺などが挙げられる。これらの攻撃は、主に金銭などの個人の資産を窃取することを目的としており、2024年も継続して被害が確認されている。

●フィッシングによる被害

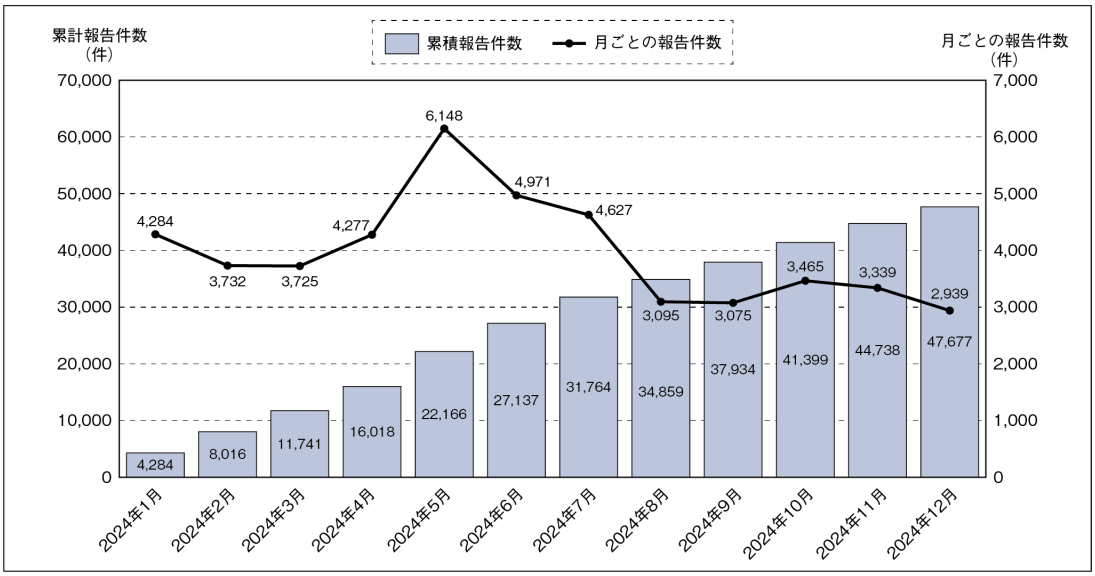
2024年は、2023年に引き続き不正送金やクレジットカード情報の詐取を目的としたフィッシングが多く見られた。3〜4月の転居シーズンには、電力会社やガス会社、水道局をかたった未納料金の支払いを求めるフィッシングの報告が増加した[2]。お中元や夏季休暇の時期を迎える7月には、配送を装ったフィッシングが急増した[3]。8月には、2次元コードから偽サイトへ誘導するフィッシングの報告が増加した[4]。

フィッシング対策協議会は「消費者への影響が大きいと考えられるフィッシング情報」をウェブサイトで発信し、注意喚起を行っている。近年のフィッシングメールやフィッシングサイトは非常に精巧に作られており見分けることは困難であるため、よく利用するオンラインサービスについては、あらかじめブックマークしたURLまたはダウンロードした正規のアプリからアクセスすることをユーザーに推奨している[5]。また、事業者側の対策としてはDMARCの導入などを挙げている[6]。

●サポート詐欺による被害

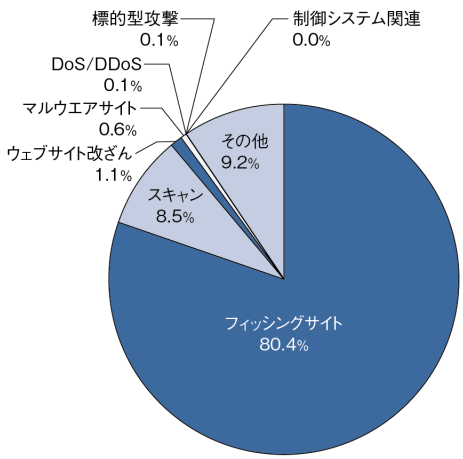
2024年は、サポート詐欺による被害も多く確認された。情報処理推進機構（IPA）のレポートによれば、4月に828件の相談が寄せられ、過去最高の月次報告数を記録した。以前はアダルト動画などから偽警告画面に誘導する手口が主流であったが、2023〜2024年ごろから手口が多様化し、サポート詐欺の被害を伝えるニュースや記事

資料4-1-1　インシデント報告件数の推移（2024年1～12月）



出所：JPCERT/CC、「インシデント報告対応レポート」を基に筆者作成

資料4-1-2　インシデント報告件数のカテゴリー別内訳（2024年1～12月）



項目	件数	割合	
フィッシングサイト	18,819件（－2,147件）	80.4%（＋7.4%）	↗
スキャン	1,993件（－3,096件）	8.5%（－9.2%）	↘
ウェブサイト改ざん	246件（　－623件）	1.1%（－1.9%）	↘
マルウエアサイト	151件（　－242件）	0.6%（－0.8%）	↘
DoS/DDoS	18件（　　－3件）	0.1%（±0.0%）	→
標的型攻撃	14件（　　＋4件）	0.1%（＋0.1%）	↗
制御システム関連	0件（　　－1件）	0.0%（±0.0%）	→
その他	2,160件（　＋774件）	9.2%（＋4.4%）	↗

※（）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」を基に筆者作成

の広告、「開く」「次へ」などのリンクボタンに偽装された広告、検索サイトの検索連動型広告枠に出てくる偽リンクなどからの誘導が確認されている[7]。

警察庁は「シャットダウンしないように」などの偽警告画面があっても指示に従う必要はなく、その画面を閉じて最寄りの警察署に通報・相談するように広報している[8]。

■法人や組織を対象とした攻撃

2024年は2023年に引き続き、脆弱（ぜいじゃく）性を突いた攻撃やランサムウエア攻撃が確認された。また、生成AIの目覚ましい進化に伴うリスクも懸念されるが、2024年はITに精通していない人が生成AIでランサムウエアプログラムを作成した事例の報告があった[9]。

生成AIの利活用に伴うリスクについては、デジタル庁が2024年6月に対策ガイドブックを公開している[10]。リスクや対策に関する議論はまだ発展途上にあり、今後、実践的なフレームワークやチェックリストなどの拡充が期待されている。

●ネットワーク機器などの脆弱性を悪用した攻撃

2024年は2023年に引き続き、ネットワーク機器などの脆弱性を悪用する攻撃事例が国内外で見られた。代表的な事例として、2024年1月に公表された「Ivanti製VPN製品の脆弱性」が挙げられる[11]。これは、典型的なゼロデイ脆弱性である。メーカーからの脆弱性情報公開時点ではセキュリティパッチがなく、暫定的な回避策でしか対策できない状況だった。そこで、パッチが公開されるまでの間に、第三者から脆弱性の詳細分析や脆弱性を実証するコード（Proof of Concept：PoC）が公表されたが、こうした情報が悪用のハードルを下げ攻撃が拡大した可能性は否定できない。また、攻撃者が当該機器のログを削除していて、周辺の機器のログ調査で初めて攻撃を確認できたケースもあった。

この他にも、ファイアウオールやネットワークインフラを構成するソフトウエアアプライアンス製品の脆弱性の悪用が見られた[12]。これらの製品は組織ネットワークとインターネットの接続点に置かれ、境界防御の要となっている。新たに公表される脆弱性に即応できるように有効なライセンスを維持するとともに、公表される脆弱性情報を速やかにキャッチアップできる体制が肝要である。

●正規のツールを用いて長期的・断続的に内部侵入する攻撃

2024年の注目される攻撃事例としては、Living off the Land戦術（侵入したシステムに標準で存在する正規ツールを利用する攻撃手法）を用いた「Operation Blotless攻撃キャンペーン」が挙げられる。JPCERT/CCでは、本件について6月に注意喚起を発行した[13]。この攻撃では、攻撃者は組織ネットワーク内に長期間にわたって潜在し、次の段階の攻撃に備えて偵察活動や認証情報の窃取をしていたと考えられ「個人情報漏えい」や「システム停止」などの目立つ実害が顕在化しない点にも特徴があった。

正規ツールは組織内の通常業務でも頻繁に利用され、セキュリティ対策や監視の対象になっていないことが多い。攻撃者はそれを逆手に取って、長期的な攻撃活動を目立たないように拡大する手段としている。正規ツールを利用した攻撃を検知できるように、保存するログの種類や項目、保存期間、検証サイクルなどを見直すことが重要である。

●放置されている既知の脆弱性による攻撃

2024年に発覚した特徴的な事例として、放置されていた「EC-CUBEの脆弱性」への攻撃を挙げたい。この攻撃は、2021年に報告された「WaterPamola攻撃キャンペーン」によるもので、3年が経過した2024年に至ってもその攻撃がなお続いていたと考えられる[14]。ECサイトは、その開発や運用段階でセキュリティの考慮が十分になされず、その上でカスタマイズされて運用されることがある。そのような場合は、脆弱性対応が困難な状態に陥り、そのまま放置されることもある。

Water Pamolaの攻撃は、このようなECサイトにありがちな特徴を攻撃者によく観察され狙われたものと言えそうだ。

「独自の機能が修正パッチと競合しないか」「独自の機能自体に脆弱性が潜んでいないか」「業務プロセスにも脆弱なポイントが潜んでいないか」にも目を向けた定期的なレビューが重要である。

●ランサムウエア攻撃

2024年のランサムウエア動向として、EUの欧州刑事警察機構（Europol）や警視庁を含む複数の法執行機関による共同捜査「オペレーション・クロノス」が挙げられる。この捜査により、法執行機関はランサムウエア攻撃グループ「LockBit」の活動に用いられたプラットフォームを制御下に置き、保存されていた被害組織の詳細や窃取されたデータ、暗号資産口座などを押収している。さらに、押収したデータの中から過去に身代金を支払った被害組織のデータを発見しており、身代金の支払いに応じたとしても攻撃者がデータを削除する保証がないことを示した点や、暗号化されたデータの復号ツールを開発した点も成果として挙げている[15]。

しかし、こうした取り組みにもかかわらず、ランサムウエアを用いる攻撃グループはいまだに多数存在し、活動を続けている。このような攻撃グループでは、グループの解散やメンバーの入れ替え、グループ名の変更なども多く、実態を捉えにくい。昨今では、データを暗号化せずに機微情報を窃取して脅迫するグループや、インターネット上に公開されているデータを窃取したと見せかけて偽の攻撃を主張するグループなども存在する。いずれも攻撃者が身代金を要求する点が共通するが、脅迫手段はさまざまで、必ずしもデータの暗号化だけが脅迫の材料ではなくなっている。ランサムウエア攻撃グループに対抗するためにも、被害組織やセキュリティ専門機関、公的機関による密な情報共有が求められる。

法人や組織が関連する、多数の顧客に影響が及んだ2024年の被害事例を2例説明する。

1例目は、業務委託を受けて複数の組織のデータを預かる企業がランサムウエア攻撃によって被害を受けた事例である。同社からの報告によると、組織内部への侵入口としてVPNが狙われ、社内の端末やサーバーがランサムウエアに感染した[16]。同社は、国内の自治体や企業などから委託を受けており、ランサムウエア攻撃によって委託元のデータが侵害を受けた。それにより、複数の委託元組織に影響が及び、各組織からの被害報告が相次いだ。

グループ企業や海外拠点であれば、自組織の統制を効かせて、求めるセキュリティ対策を講じることも可能であるが、業務委託先にそれを強制することは難しい。委託業務契約を締結するとすぐに変更することが難しくなるため、契約前にセキュリティ対策と運用体制を十分に確認することが重要になる。さらに、セキュリティ対策とセキュリティ管理体制を義務付け、必要に応じて監査できる旨を契約に盛り込んでおくことも重要である。

2例目は、多くのユーザーが利用するアプリケーションサービスを提供する企業がランサムウエア攻撃による被害を受けた事例である。この攻撃によって、グループ会社を含む複数のサーバーに障害が発生し、出版製造・物流システムが停止するとともに顧客や従業員などの個人情報約26.2万件が漏えいした。悪質な情報拡散行為による二次被害も発生した。本事案は2024年6月に発生したが、段階的な復旧は同年8月、完全復旧は同年11月にまで及び、長期間の業務影響が生じた。これにより、売上高で約77億円、営業利益で約47億円を失い、調査や復旧などのために約

24億円の特別損失が発生する見通しとなった[17]。この事例は、ランサムウエア攻撃で大きな損失を被った事例として、国内で大きく報じられた。

ランサムウエアによるインシデントが発生した場合、発生する損害はシステムの修復費用だけではない。システム停止などによる業務の中断が長期化した場合は、その間に得るはずであった利益を喪失する。システム復旧に向けて、本来不要であった人件費・固定費の発生に加え、人的リソースも消費される。被害に遭った顧客への損害もサポートする必要がある。さらに、株価の下落、風評被害やブランドイメージの低下など、被害額の算定が難しい損害も伴う[18]。

このように、被害時に考慮しなければならない点は多く、被害発生を想定して準備しておかないと通常業務に戻ることがますます難しくなる。アクセス制限や権限の最小化、脆弱性管理といった基本的な対策と、万が一の感染に備えたバックアップ取得方法と復旧手順の検証、業務継続計画の策定、緊急時における株主や顧客との信頼関係の構築が重要である。

JPCERT/CCでは、2024年3月からインシデント対応に関する相談やインシデントに関する情報を、被害組織からだけでなく調査を支援するセキュリティベンダーやシステム運用会社からも提供していただけるように、窓口を拡大している[19]。攻撃者の脅迫を受けた場合は、安易に交渉や身代金支払いには応じず、JPCERT/CCが公開しているウェブページ[20]や上記受付窓口を活用し、その他の専門機関にも相談しながら対応していただきたい。

■対策

上述した攻撃に対しては、次のような複数の対策が推奨されている。

1つめの対策は、ASM（Attack Surface Management）である。ASMは、外部から把握できる情報を用いて自組織のIT資産を発見・管理する手法として注目されている[21]。これをうまく活用することで、放置された脆弱性や組織が把握していない未管理の機器、意図しない情報の公開や設定ミスを発見でき、攻撃者の侵入経路となり得るポイントを押さえることができる。

2つめの対策は、脆弱性有無の調査やパッチ適用などを速やかに実施できる運用体制を整備することである。たとえ迅速な抜本的対処が難しい場合にも、攻撃されるリスクを認識し、運用において監視を強化するなどの対策が望まれる。

3つめの対策は、侵入後に発生するネットワーク内部での横断的侵害への対策を行うことである。権限の最小化やEDR（Endpoint Detection and Response）の導入など、侵入後の攻撃者の横断的侵害を制限する対策を検討することで、ゼロデイ攻撃に備えることができる。

4つめの対策は、システムの設計段階からセキュリティを考慮する「セキュリティ・バイ・デザイン」を取り入れることである[22]。攻撃者に狙われやすいシステム上・運用上の弱点を事前に検討して対応することで脆弱性の発見や保守性の向上が見込め、結果的にセキュリティにかかるトータルコストを抑えることができる。

組織に降りかかるセキュリティリスクを低減し安定した成長を固めるためにも、これらの対策への真摯な取り組みを期待したい。

1. JPCERT/CC、「インシデント報告対応レポート」 https://www.jpcert.or.jp/ir/report.html
2. フィッシング対策協議会、「月次報告書：2024/04 フィッシング報告状況」 https://www.antiphishing.jp/report/monthly/202404.html
3. フィッシング対策協議会、「月次報告書：2024/07 フィッシン

グ報告状況」
https://www.antiphishing.jp/report/monthly/202407.html

4. フィッシング対策協議会、「緊急情報：QRコードから誘導するフィッシング」、2024年8月28日
https://www.antiphishing.jp/news/alert/qr_20240828.html
5. 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2024年度版」
https://www.antiphishing.jp/report/consumer_antiphishing_guideline_2024.pdf
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. IPA、「サポート詐欺レポート」
https://www.ipa.go.jp/security/anshin/measures/supportscam_report.html
8. 警察庁、「サポート詐欺対策」
https://www.npa.go.jp/bureau/cyber/countermeasures/support-fraud.html
9. トレンドマイクロ、「生成AIでランサムウェアを作成した容疑者の摘発事例を考察」、2024年5月29日
https://www.trendmicro.com/ja_jp/jp-security/24/e/breaking-securitynews-20240529-02.html
10. デジタル庁、「テキスト生成AI利活用におけるリスクへの対策ガイドブック（α版）」テキスト生成AI利活用におけるリスクへの対策ガイドブック（α版）、2024年6月10日
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/c1959599-efad-472e-a640-97ae67617219/fe843dc6/20240610_resources_generalitve-ai-guidebook_01.pdf
11. JPCERT/CC、「Ivanti Connect SecureおよびIvanti Policy Secureの脆弱性（CVE-2023-46805およびCVE-2024-21887）に関する注意喚起」、2024年1月11日
https://www.jpcert.or.jp/at/2024/at240002.html
12. JPCERT/CC、「Fortinet製FortiManagerにおける重要な機能に対する認証の欠如の脆弱性（CVE-2024-47575）等に関する注意喚起」、2024年10月24日
https://www.jpcert.or.jp/at/2024/at240020.html
13. JPCERT/CC、「Operation Blotless攻撃キャンペーンに関する注意喚起」、2024年6月25日
https://www.jpcert.or.jp/at/2024/at240013.html
14. JPCERT/CC、「EC-CUBEのクロスサイトスクリプティングの脆弱性（CVE-2021-20717）に関する注意喚起」、2021年5月10日
https://www.jpcert.or.jp/at/2021/at210022.html
15. NCA, "International investigation disrupts the world´s most harmful cyber crime group," 20 Feb. 2024
https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group
16. イセトー、「不正アクセスによる個人情報漏えいに関するお詫びとご報告」、2024年10月4日
https://www.iseto.co.jp/news/news_202410.html
17. KADOKAWA、「Earning Results 2025年3月期第2四半期決算」、2024年11月7日
https://ssl4.eir-parts.net/doc/9468/ir_material_for_fiscal_ym10/166643/00.pdf
18. 日本ネットワークセキュリティ協会、「インシデント損害額調査レポート第2版」、2023年2月9日
https://www.jnsa.org/result/incidentdamage/data/2024-1.pdf
19. JPCERT/CC、「インシデント相談・情報提供（被害組織／保守・調査ベンダー向け）」
https://www.jpcert.or.jp/ir/consult.html
20. 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
21. 経済産業省、「ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」、2023年5月29日
https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf
22. デジタル庁、「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」、2024年1月31日
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf

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～2025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