2025 年 11 月 25 日

報道関係各位

GMO サイバーセキュリティ by イエラエ株式会社

GMO サイバーセキュリティ by イエラエ、2025 年第 3 四半期の「GMO サイバー攻撃ネット de 診断 ASM 脅威レポート」発表

～ランサムウェア感染要因となる VPN や RDP 公開が高リスク脅威にランクイン、IT 資産の棚卸し・状態可視化の重要性が浮き彫りに～

GMO インターネットグループでサイバー攻撃対策事業を展開する GMO サイバーセキュリティ by イエラエ株式会社（代表取締役 CEO：牧田 誠、以下 GMO サイバーセキュリティ by イエラエ）は、外部公開 IT 資産を自動で棚卸し・可視化する ASM（Attack Surface Management、以下 ASM）ツール「GMO サイバー攻撃ネット de 診断 ASM」での脅威検知の結果を分析し、2025 年 第 3 四半期（7 月～9 月）の 脅威検知ランキングを発表しました。本調査は、期間中に「GMO サイバー攻撃ネット de 診断 ASM」で検知した約 57 万件のデータを集計・分析しています (※1)。

(※1)　調査結果のパーセンテージは、小数点以下第一位を四捨五入した数値です。

【レポートの趣旨と総評】

「GMO サイバー攻撃ネット de 診断 ASM」では、IT 資産に影響あたえる脅威を 5 段階のリスクレベルで評価しており、脅威が検知された場合は、検知内容とリスクレベル、対策方針を利用者へ通知しています。「GMO サイバー攻撃ネット de 診断 ASM 脅威レポート」は、検知した脅威の内容を統計分析し、企業や団体における IT 資産の棚卸しや定期的なセキュリティ対策に役立ててもらうことを目的で発表しています。

GMO サイバーセキュリティ by イエラエにとって、初めての統計調査となる今期の脅威レポートでは、「サポートの終了したソフトウェアの利用」や「既知の脆弱性が存在するソフトウェアの利用」といった IT 資産管理の不備が、脅威カテゴリの上位にランクインしました。脆弱性は公開されてから 1 カ月以内に悪用されるリスクが高いといった調査 (※2)もあり、脆弱性が残存するソフトウェアを利用することは高いリスク

と言えます。加えて、近年猛威をふるうランサムウェア(※3)攻撃の感染につながるVPN(※4)機器やリモートデスクトップ（RDP）(※5)のアクセス制御不備がランクインしました。本レポートの結果は、企業のIT管理者に対し、システム運用やバージョン管理の継続的な改善を強く求めるものとなりました。

(※2)　Mandiant（2024年10月）,「Mandiant How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trend」

(※3)　ランサムウェアは、感染したシステムのデータを暗号化し、被害者に対してデータの復元と引き換えに身代金を要求することを目的とした悪意あるソフトウェアのこと。

(※4)　インターネットとデバイス間を仮想的な専用線でつなぎ、安全にデータ通信を行う技術

(※5)　手元のコンピュータからネットワークで接続された他のコンピュータを操作する技術

■ 2025年 第3四半期 集計対象の脅威数

- 集計対象件数：**571,493件**　（集計対象期間：2025年7月1日～9月30日）

【調査結果の主なトピック】

■高リスクの脅威検知数1位は「既知の脆弱性が存在するソフトウェアの利用」

2025年 第3四半期は、お客様のシステム環境から、サイバー攻撃に悪用される恐れのある脅威を35,609件検知しました。高リスクとして検知された脅威カテゴリの上位は以下の通りです。

1位「既知の脆弱性が存在するソフトウェアの利用」
2位「バージョン管理の不備（サポート終了のソフトウェア利用）」
3位「アクセス制御・暗号化・認証不備」

外部公開IT資産で「既知の脆弱性が存在するソフトウェアの利用」をしている状態は、サイバー犯罪者に攻撃方法を公開しているといっても過言ではなく、サイバー攻撃を受ける危険性が極めて高い状態です。また、「バージョン管理の不備（サポート終了のソフトウェア利用）」は、新たな脆弱性が発見されても修正対応されることはなく、脆弱性が発見された時の対策が困難になることから、常時適切なバージョンへ更新しておくことが求められます。

サイバー攻撃対策の第一歩は、所有するIT資産に脆弱性があるか、バージョンは最新化など状態を含めた棚卸しを行うことから始まります。その次に、悪用のされやすさから対策の優先順位を決定していきます。今回のレポート結果からは、定期的に外部公開IT資産を自動で棚卸し・可視化するASMの重要性が再確認される結果となりました。しかしながら、多種多様なソフトウェアを利用するシステム環境においてIT資産を適切に管理することは一筋縄ではいきません。全社で統一したASMツールを活用することは解決策のひとつとなります。

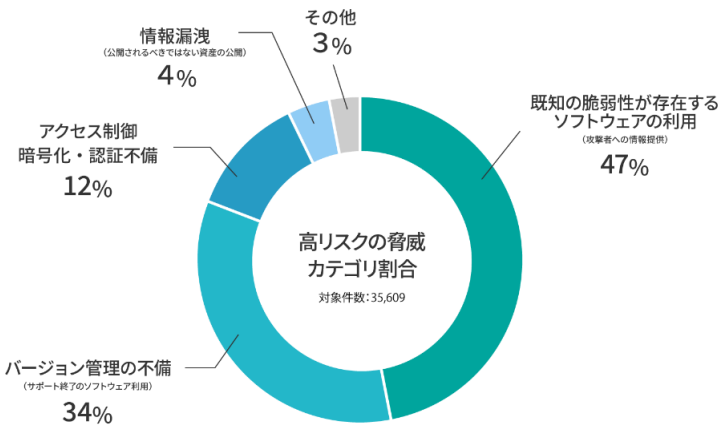

図1:高リスクの脅威カテゴリ割合

■ランサムウェア感染要因となる VPN 公開は「アクセス制御」カテゴリで 7 位

「アクセス制御・暗号化・認証不備」カテゴリの高リスク脅威は 4,426 件検出しました。本脅威カテゴリでは、 1 位は「FTP プロトコルでの平文通信」でした。FTP は多くのレンタルサーバで提供されている機能ですが、平文通信が有効化されていると、機密情報の漏洩や通信内容の改ざん（MITM 攻撃）の被害にあう可能性があります。また、本カテゴリでは、近年猛威をふるうランサムウェア攻撃の感染につながる VPN 機器やリモートデスクトップ（RDP）のアクセス制御不備がランクインしました。警察庁の調査 (※6) によると、ランサムウェアは VPN や RDP からの侵入が 8 割以上を占めており、攻撃の常套手段となっています。VPN・RDP がインターネット上で公開されている場合は、適切なセキュリティ対策を行うことが必須です。IT 資産が意図せず公開されていないか、設定不備がないか、企業は定期的に確認することが求められます。

(※6) 警察庁（2025 年 9 月），「令和 7 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」

順位	脅威項目
1 位	FTP プロトコルでの平文通信
2 位	管理用パスワード認証ページへアクセス可能(WordPress)
3 位	MySQL プロトコルが有効
4 位	脆弱なSSL/TLSプロトコルのサポート
5 位	平文通信 (HTTP) による認証情報の送信
6 位	管理画面にアクセス可能(phpmyadmin)
7 位	VPN プロトコル(PPTP)が有効
8 位	リモートデスクトッププロトコル(RDP)が有効
9 位	Telnet プロトコルが有効
10 位	SMB プロトコルが有効

表 1: 「アクセス制御・暗号化・認証不備」カテゴリで検知した高リスク脅威ランキング

■「バージョン管理の不備」の脅威のうち 10 個にひとつが「WordPress」の脆弱性

サポート終了のソフトウェア利用など「バージョン管理の不備」があった高リスクの脅威検知数は 12,184 件でした。中でも、WordPress のバージョン管理の不備は 1,071 件と検知数全体の 9%でした。日本語サイトの 83%が WordPress を利用しているという調査(※7)もあり、日本での利用率は非常に高いことが分かります。「また、多種多様なソフトウェアが利用されている中で、一つのソフトウェアに関連する脅威が約 1 割を占める状態は注視すべき事項です。

WordPress は活用しやすいという特徴の一方で、テンプレートやプラグイン(※8)が豊富にあり、それぞれのソフトウェアが独立しています。そのため、適切に管理・更新をしないとセキュリティリスクが残存する可能性があります。実際、脆弱性が残存した WordPress のテンプレートやプラグインを利用していたために改ざん・迷惑メール送信・情報流出の被害を被った事例は、毎年報告されています。被害を防ぐためにも、自社のウェブサイトのソフトウェアの状態を定期的に棚卸しを行い、アップデートを実施することが不可欠です。アップデートがすぐにできない場合でも、暫定的な対策として仮想パッチの設置などの防御策を講じることが求められます。

(※7)　W3Techs（2025 年 11 月），「Distribution of content management systems among websites that use Japanese as content language」

(※8)　アプリケーションに機能を追加・拡張するためのソフトウェアのこと。ブラウザの拡張機能としてよく使われる。

順位	脅威項目
1 位	Contact Form 7 (WordPressプラグイン)
2 位	Elementor Pro (WordPressプラグイン)
3 位	Elementor Website Builder More Than Just a Page Builder(WordPressプラグイン)
4 位	Travel Tour (WordPressテーマ)
5 位	NewsMag (WordPressテーマ)

表 2:「バージョン管理の不備」カテゴリで検知した WordPress 関連の高リスク脅威ランキング

【「GMO サイバー攻撃 ネット de 診断 ASM」開発担当者のコメント】

■プロダクトサービス事業部　副部長　診断エンジン開発者 大西 和貴

今回の結果からは、企業の IT 資産管理の重要性があらためて浮き彫りになりました。脆弱性の存在やサポート終了ソフトウェアの利用は、“見えないまま放置されるリスク”の代表例です。

私たちは、ASM（Attack Surface Management）を通じて、お客様が自社の IT 資産の現状を正しく把握し、どの対策を優先すべきかを具体的に判断できる環境を提供しています。

サイバー攻撃の多くは『見えていなかった資産』から始まります。継続的な可視化と迅速な対応が、今後ますます求められると考えています。

【「GMO サイバー攻撃 ネット de 診断 ASM」について】

(https://product.gmo-cybersecurity.com/net-de-shindan/lp_enterprise/)

「GMO サイバー攻撃ネット de 診断 ASM」は、簡単かつ直感的に使用が可能なセキュリティプラットフォームです。国産 ASM ツールとして培ってきた「IT 資産の棚卸しとリスク可視化」の強みを活かしながらも、ASM ツールの枠にとどまらず「複雑化するセキュリティ運用をシンプルにし、“何から対策すべきか”を可視化する」というビジョンの実現を目指しています。セキュリティ知識を問わず、お客様が最も優先すべき対策を一目で把握できるよう導きます。

【GMO サイバーセキュリティ by イエラエについて】

(https://gmo-cybersecurity.com/)

GMO サイバーセキュリティ by イエラエは、国内最大規模のホワイトハッカーで組織されたサイバーセキュリティのプロフェッショナルカンパニーです。会社理念である「人を助ける信念を守るチカラに変えて

いく」ために今後も最先端の技術と実践的な教育を通じて、日本のサイバーセキュリティの強化に貢献していきます。また、「世界一のホワイトハッカーの技術力を身近に」を目指して、各種脆弱性診断、ペネトレーションテスト、セキュリティコンサルタント、SOC サービス、フォレンジック調査まで包括的にサイバーセキュリティ対策サービスをご提供します。

以上

【報道関係お問い合わせ先】

●GMO サイバーセキュリティ by イエラエ株式会社
マーケティング部　広報担当　伊礼・棚田
TEL：03-6276-6045
E-mail：pr@gmo-cybersecurity.com

●GMO インターネットグループ株式会社
グループ広報部　PR チーム　田部井
TEL：03-5456-2695
お問い合わせ：https://group.gmo/contact/press-inquiries/

【GMO サイバーセキュリティ by イエラエ株式会社】（URL：https://gmo-cybersecurity.com/）

会　社　名	GMO サイバーセキュリティ by イエラエ株式会社
所　在　地	東京都渋谷区桜丘町 26 番 1 号　セルリアンタワー
代　表　者	代表取締役 CEO　牧田　誠
事 業 内 容	■Web アプリ及びスマホアプリ脆弱性診断 ■ペネトレーションテスト ■不正利用（チート）診断　■IoT 脆弱性診断　■自動車脆弱性診断 ■フォレンジック調査　■CSIRT 支援　■クラウドセキュリティ診断 ■クラウドセキュリティ・アドバイザリー
資　本　金	1 億円

【GMO インターネットグループ株式会社】（URL：https://group.gmo/）

会　社　名	GMO インターネットグループ株式会社　（東証プライム市場　証券コード：9449）
所　在　地	東京都渋谷区桜丘町 26 番 1 号　セルリアンタワー
代　表　者	代表取締役グループ代表　熊谷　正寿
事 業 内 容	持株会社（グループ経営機能） ■グループの事業内容 インターネットインフラ事業 インターネットセキュリティ事業 インターネット広告・メディア事業 インターネット金融事業 暗号資産事業
資　本　金	50 億円