LAC SECURITY INSIGHT

第 16 号

2026 春

特集：プラットフォーム診断員から見る脅威の動向

JSOC で観測されたサイバー攻撃傾向

サイバー119 サービスの出動傾向

JSOC JAPAN SECURITY OPERATION CENTER

CYBER EMERGENCY CENTER

DiaForce

2026 年 6 月
株式会社ラック

LAC SECURITY INSIGHT

第 16 号／2026 春

目　　次

はじめに

本レポートは、ラックの中でもサイバー攻撃の脅威に対して最前線で対応している JSOC およびサイバー救急センター、そして攻撃者が利用するサイバー攻撃手法も活用してお客様のシステムへ侵入テストを行うデジタルペンテスト部において、分析・調査・侵入テストを実施する中で得た、最近の脅威の傾向や特徴を、セキュリティ専門家が「洞察」としてまとめたものです。

日々発生している実際の攻撃やインシデントに根ざしており、また日本の企業や団体を狙った脅威を中心にまとめているため、日本の企業や団体のサイバーセキュリティ担当者が、自組織が直面しているサイバー攻撃や脅威を把握できる内容です。

サイバー攻撃の傾向の変化は年々早く強くなっており、セキュリティ対策も継続的に見直して対応していく必要があり、またそのスピードが求められます。本レポートが、皆さまの継続的なセキュリティ対策の改善に役立てていただけることを願っております。

株式会社ラック
技術サービス本部 副本部長
内田 法道

サイバー119で出動したインシデント傾向

2026年1月～3月の出動傾向

当該期間では、マルウェアによる被害の相談が 32%、およびサーバの不正利用による被害の相談が30%であり、両者で全体の62%を占めています。この割合は、前四半期（2025年10月から12月）75%、前年同期（2025年1月から3月）87%より減少しています。

マルウェア関連の被害では、ランサムウェアによる被害が全体の 11%を占めています。前四半期（16%）および前年同期（31%）と比較して大幅に減少しましたが、マルウェア関連被害の中では引き続き最も高い割合です。侵入経路としては、SSL-VPN 機器が悪用されるケースが継続して確認されています。侵入後は社内ネットワークへ展開され、Web システムや基幹システムを中心に暗号化被害を受ける傾向が見受けられます。

サーバ不正侵入の被害では、ID 不正利用による被害が全体の 21%を占め、前四半期（15%）から増加しています。一方、前年同期（22%）と同水準で推移しており、被害が継続しています。特にクラウドサービスのアカウント情報が不正利用される事例が多数報告されており、当該期間では、フィッシングサイトへ誘導された従業員が認証情報を入力してしまう事例を複数確認しています。こうした傾向は、SaaS に限らず、クラウド基盤（IaaS/PaaS）を利用する環境でも、アカウント侵害が重要なリスクとなることを示しています。そのため、クラウド環境では従来のネットワーク境界に加え、アカウントが重要なセキュリティ境界となります。開発から運用までの各フェーズにおいて、適切なアカウント管理や強固な認証方式の選定が重要です。

当該期間では、内部不正による被害の相談が 13%となり、前四半期（4%）および前年同期（9%）と比較して増加しています。USB デバイスやオンラインストレージサービスを悪用した機密情報の持ち出し、機密情報を表示した画面をスマートフォンで撮影して持ち出すなどの相談が寄せられました。対策としては、従業員に対するセキュリティ教育やガバナンス研修の実施、ならびにセキュリティポリシーの整備・周知といったガバナンス面の対策が必要です。併せて、DLP などのセキュリティ製品を導入し、機密情報の持ち出しを防止または検知できる仕組みを整備することが重要です。

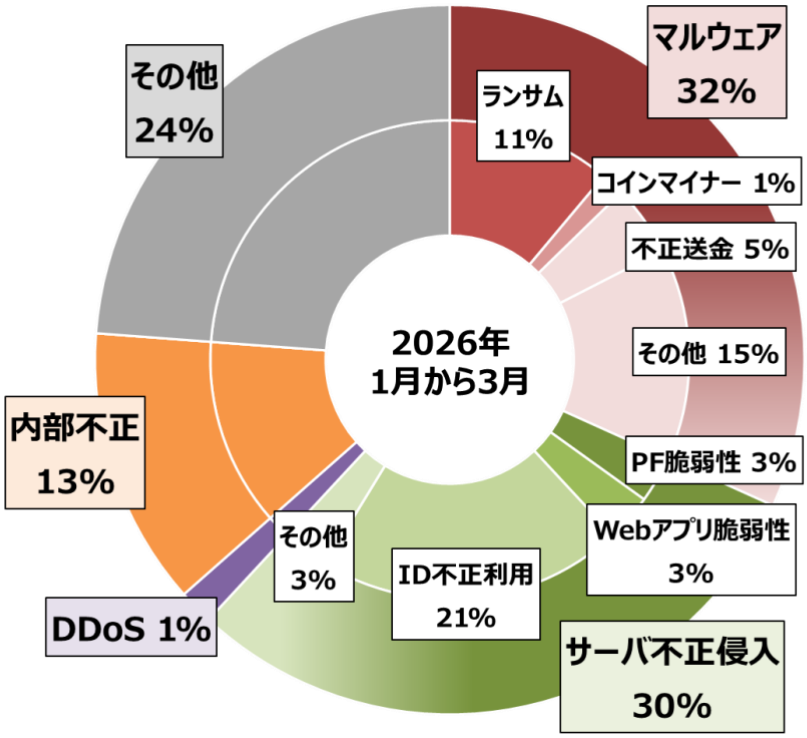

図 1 2026 年 1 月から 3 月の出動インシデントの内訳

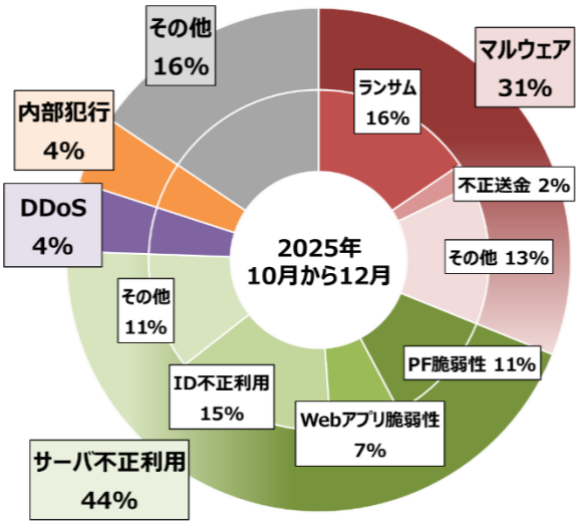

図 2 前四半期（2025 年 10 月から 12 月）

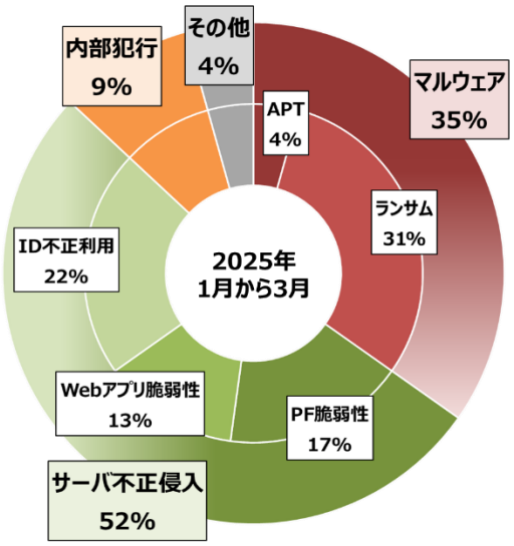

図 3 前年同期（2025 年 1 月から 3 月）

下表は、当該期間（2026 年 1 月～3 月）、前四半期（2025 年 10 月～12 月）および前年同期（2025 年 1 月～3 月）の各期間における相談件数の割合を業種別に集計し、上位 5 業種の推移を示したものです。

情報通信業は当該期間において 25%となり、前四半期（28%）からは低下しているものの、前年同期（25%）と同水準で推移しており、引き続き高い割合を占めています。また、当該期間の上位業種は、前四半期に上位であった「教育，学習支援業」および前年同期に上位であった「不動産業，物品賃貸業」が上位 5 業種から外れており、上位業種の構成に一部入れ替わりが見られます。さらに、上位 5 業種の割合合計は当該期間において 72%となり、前四半期（72%）とは同水準である一方、前年同期（84%）を下回っています。これらの結果から、相談が発生する業種が特定の業種に固定されず、より広範な業種へ分散している可能性が示唆されます。

順位	当該期間 (2026 年 1 月から 3 月)		前四半期 (2025 年 10 月から 12 月)		前年同期 (2025 年 1 月から 3 月)	
1	情報通信業	25%	情報通信業	28%	製造業	28%
2	製造業	17%	製造業	15%	情報通信業	25%
3	卸売業，小売業	11%	金融業，保険業	12%	学術研究，専門・技術サービス業	14%
4	金融業，保険業	11%	卸売業，小売業	9%	卸売業，小売業	11%
5	学術研究，専門・技術サービス業	8%	教育，学習支援業	8%	不動産業，物品賃貸業	6%

表 1 上位 5 業種の相談件数割合

【偽の Zip インストーラーのインストール被害】

当該期間では、人気の圧縮・解凍ソフト「7-Zip」を装った偽のインストーラーをインストールしてしまう事案が報告されています。攻撃者は、正規サイトに類似したドメイン「7zip.com」で偽の Web サイトを用意し、検索エンジンの検索結果で上位に表示させることで、利用者を偽サイトへ誘導する手口を用いています。偽インストーラーの実行後、表面上は正規のソフトウェアがインストールされたように見えるため、利用者がマルウェア感染に気付きにくい点が特徴です。

偽インストーラーにより感染するマルウェアでは、感染端末を通信の中継点（プロキシ）として悪用する挙動が確認されています。攻撃者は感染端末を経由して通信を行うことで発信元を隠蔽し、不正な活動を実施することが可能となります。その結果、他システムへの不正アクセスなどが感染端末から行われたように見えるため、脅威検知システムの回避を目的としていると考えられます。加えて、不正通信の踏み台として自組織の IP アドレスが利用された場合、当該アドレスのブラックリスト登録やインシデント調査対象となるなど、二次的な業務影響が生じる可能性があります。

また、端末の OS 情報やハードウェア構成などのデバイス構成情報を外部サーバへ送信する機能も確認されています。感染端末内のファイルを探索して外部へ送信する機能は確認されていませんが、収集された構成情報が端末の特定や、より高度な攻撃の準備情報として悪用される可能性があります。

対策としては、インターネット経由でソフトウェアを導入する場合は、公式サイトからのみダウンロードする運用を徹底する必要があります。検索結果で上位に表示される Web サイトであっても、アクセス先の URL が正規ドメインであることを事前に確認することが求められます。組織としては、承認済みソフトウェア以外のインストールを制限する仕組み[1]（アプリケーション制御など）を併用することが有効です。また、EDR（Endpoint Detection and Response）[2]を導入し、異常なプロセス実行や不審な通信を早期に検知できる運用体制を整えることが重要です。さらに、可能な場合はデジタル署名やハッシュ値などにより、取得したインストーラーの真正性を確認することも有効です。

---

[1] Ivanti Endpoint Manager : https://www.ivanti.com/ja/products/endpoint-manager
LANSCOPE Endpoint Manager : https://www.lanscope.jp/endpoint-manager/

[2] CrowdStrike : https://www.crowdstrike.com/ja-jp/platform/endpoint-security/
Microsoft Defender for Endpoint : https://www.microsoft.com/ja-jp/security/business/endpoint-security/microsoft-defender-endpoint

【フィッシングメールの巧妙化】

フィッシングメールによるマルウェア感染や認証情報の漏えいに関する相談が多く寄せられています。従来は不自然な日本語表現や粗いデザインなどから判別できるケースも多く見られましたが、近年は AI を活用した自然な文章や、実在する企業のロゴ・署名を精巧に模倣したデザインを用いる事例が増加しています。通信事業者、金融機関やクラウドサービスなど日常的に利用されるサービスを装うケースに加え、人事異動の辞令や給与制度の改定案内など、年度替わりや人事異動といった季節的な慣行に沿った内容のメールが送付される事例も確認されています。これらは受信者の警戒心を低下させ、内容を疑いにくくする意図があるものと考えられます。

フィッシングメール内のリンクをクリックした場合、正規サイトと判別しにくい偽サイトへ誘導され、ID やパスワードなどの認証情報の入力を求められます。近年は、ワンタイムパスワード（OTP）をリアルタイムで中継する「リバースプロキシ型」の攻撃手法も確認されており、多要素認証（MFA）を設定している場合でも突破されるケースが発生しています。また、従来確認されている手口として、メール本文中に記載されたリンク先の Web サイトから不審な実行ファイルをダウンロードさせ、遠隔操作マルウェア（RAT）の感染を狙う事例も確認されています。RAT に感染した場合、攻撃者が端末を任意に操作可能な状態となるため、認証情報の窃取にとどまらず、組織内ネットワーク全体の侵害へと発展する可能性があります。

フィッシングメールによる被害を防止するための技術的対策としては、送信ドメイン認証（SPF、DKIM、DMARC）[3]の導入が挙げられます。送信ドメイン認証を適切に設定・運用し、なりすましメールを検知して受信を拒否することで、送信元を偽装したフィッシングメールが従業員に到達するリスクを低減できます。加えて、本文中の URL リンクや添付ファイルを自動的に分析するアンチスパム・ウイルスツール[4]の導入も有効です。従業員が操作を行う前に不審な URL リンクや添付ファイルを検知・遮断することで、インシデントの発生を未然に防止します。さらに、不審サイトへのアクセス防止を目的とした Web フィルタリングの実施や、端末への EDR 導入により不審な挙動を検知・遮断することも有効です。

また、ワンタイムパスワードを中継することで多要素認証の突破を狙うリバースプロキシ型攻撃への対策としては、FIDO/WebAuthn 認証や PKI（公開鍵基盤）ベースの認証など、フィッシング耐性を持つ

---

[3] フィッシング対策協議会「送信ドメイン認証技術導入マニュアル 第 3.1 版」
https://www.dekyo.or.jp/soudan/data/anti_spam/meiwakumanual3/manual_3rd_edition.pdf

[4] Microsoft「Microsoft Defender for Office 365 安全な添付ファイル（Safe Attachments）機能」
https://learn.microsoft.com/ja-jp/defender-office-365/safe-attachments-about
デジタルアーツ「m-FILTER」
https://www.iij.ad.jp/svcsol/partner/solution/daj.html

多要素認証[5]の導入が有効です。これらの認証方式では、アクセス先 Web サイトの真正性確認や利用者本人の検証が行われるため、攻撃者による認証情報の窃取とそれに伴う不正ログインの抑止が期待できます。

技術的対策に加えて、従業員がフィッシングメールを受信した場合に適切に対処できるよう、人的・組織的対策を強化することも重要です。従業員向けのセキュリティ教育には、リンクを安易にクリックしないこと、添付ファイルを安易に実行しないことなど、フィッシングメールに対する基本的な行動指針を盛り込む必要があります。加えて、標的型攻撃メール訓練を実施し、受信時の対応や報告手順を実践させることで、セキュリティ意識および初動対応力の向上を図ることが有効です。

[5] Okta FastPass : https://help.okta.com/oie/ja-jp/content/topics/identity-engine/devices/fp/fp-main.htm

JSOC で観測したサイバー攻撃傾向

重要インシデントのトピックス

2026 年 1 月から 3 月に発生した重要インシデント（検知件数の多寡を問わず攻撃の成功を確認もしくは被害が発生している可能性が高いと判断されるセキュリティインシデント）の合計件数は 230 件でした。内訳はインターネットからの攻撃によるインシデントが 9 件（4.0%）、ネットワーク内部からの通信によるインシデントが 221 件（96.0%）であり、ネットワーク内部からの通信によるインシデントは前四半期と比較して増加しました。

1）インターネットからの攻撃により発生した重要インシデント

Palo Alto Networks 社製品に存在するクロスサイトスクリプティングの脆弱性（CVE-2025-0133）を狙った攻撃によるインシデントが発生しました。そのほかには SQL インジェクションやクロスサイトスクリプティングによる重要インシデントが発生しました。図 4 に 2026 年 1 月から 3 月の重要インシデントの内訳を示します。

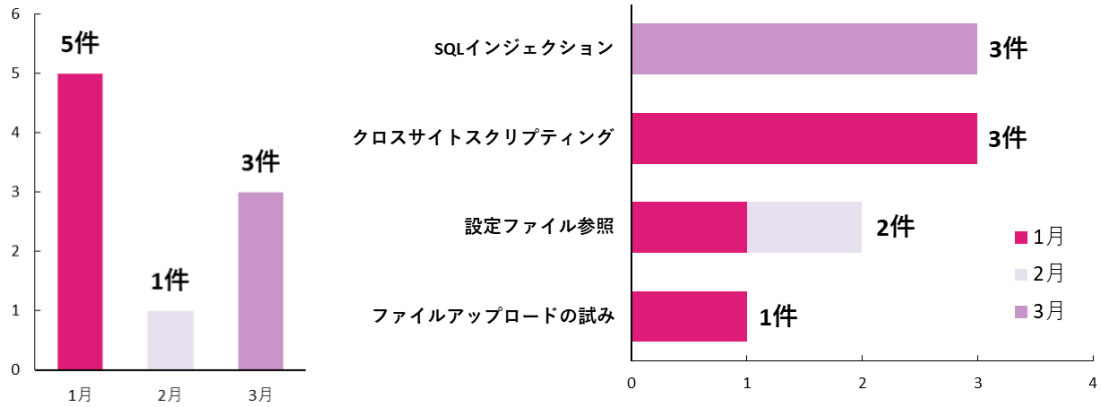

図 4 [外部から] 2026 年 1 月から 3 月の重要インシデントの内訳（月別・種類別）

2) ネットワーク内部から発生した重要インシデント

マルウェア感染に起因する重要インシデントが多数発生しました。これらのインシデントでは、ユーザ情報の窃取を目的とした悪意のあるプラグインのダウンロードに伴う通信が多く検知されました。こうしたインシデントを防ぐためには、プラグイン導入の必要性を十分に検討したうえで、導入時点の評価やレビューを確認することが重要です。さらに、提供元の信頼性を確認し、インストール後も利用中のプラグインに関する情報を定期的に収集することが求められます。必要に応じて、プラグインの利用を制御する措置の導入もご検討ください。 また、攻撃者に改ざんされた Axios の npm パッケージのインストール、Amaday に関連する通信、NetSupport RAT を利用した通信、不審な名前解決の検知に起因する重要インシデントも確認されました。図 5 に、2026 年 1 月から 3 月に発生した重要インシデントの内訳を示します。

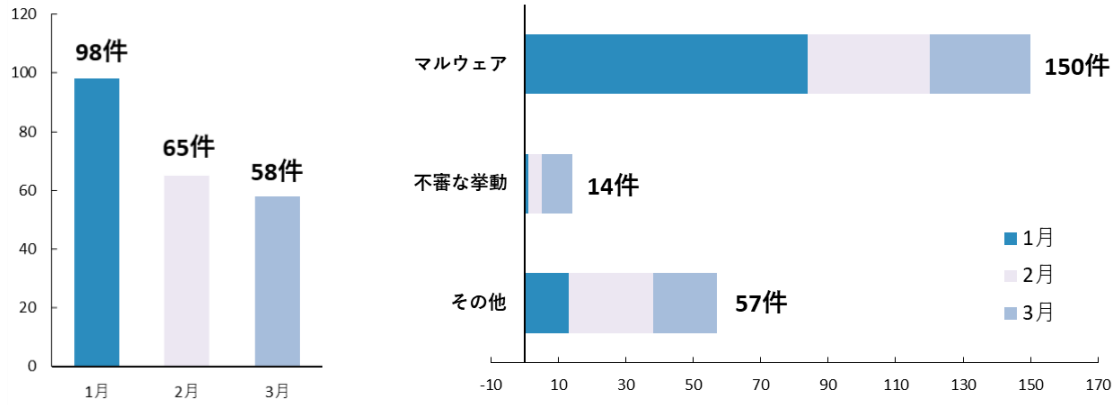

図 5 [内部から] 2026 年 1 月から 3 月の重要インシデントの内訳（月別・種類別）

EDR 製品の検知による重要インシデントは 32 件発生しました。マルウェア感染につながる挙動を検知したことによるインシデントが 18 件、攻撃者によって行われた可能性のある不審な挙動を検知したことによるインシデントが 14 件でした。これらのインシデントのうち特徴的なものは、インストーラーに偽装した不審なファイルの実行によるものと考えます。対策として、公式サイトからのダウンロードを遵守する、ファイルの署名や発行元を確認するなどが挙げられます。そのほかには、公式のセキュリティアドバイザリやセキュリティニュースを定期的に確認し、インシデント情報をいち早く把握できる体制を整えることも重要です。

注意が必要な通信

注意が必要な通信や、大きな被害には発展していないものの検知件数が多い攻撃通信を、下表で紹介します。

表 2 注意が必要な通信について

概要	JSOC の検知内容	検知時期
SQL インジェクションの脆弱性を狙った攻撃	多数の IP アドレスから SQL インジェクションの脆弱性を狙った攻撃を検知しました。	1 月 30 日～
DNS 再帰問い合わせ可能なホストを探査する目的の通信	多数の IP アドレスから DNS Amplification 攻撃を試みる通信を検知しました。	2 月 3 日～ 2 月 28 日 3 月 25 日～
107.172.22.3（アメリカ）からの攻撃通信	脆弱性スキャナを悪用した攻撃通信を多数検知しました。	3 月 24 日～ 3 月 25 日

特集：プラットフォーム診断員から見る脅威の動向

昨今のニュース等で、VPN 機器の侵害を起因とした被害や、攻撃影響がサプライチェーン全体に波及した事例を耳にすることが多くなってきました。

どちらも以前から報じられている攻撃手法やリスクであり、今もなお組織における主要なサイバーリスクとして挙げられるものです。実際に、IPA が毎年公表する「情報セキュリティ 10 大脅威 2026 組織編」でも、VPN 機器の侵害を起因とした被害は「システムの脆弱性を悪用した攻撃」や「リモートワーク等の環境や仕組みを狙った攻撃」として、攻撃影響がサプライチェーン全体に波及した事例は「サプライチェーンや委託先を狙った攻撃」として継続的に取り上げられています[6]。

本特集では、プラットフォーム診断員の観点から上記事例をひもとき、システムで攻撃者に狙われやすいポイントをプラットフォーム診断の問題点検出傾向を示しながら考察します。

昨今の攻撃事例

- VPN 機器の侵害を起因とした事例

企業において、VPN は必要不可欠な技術として広く普及しています。複数拠点を抱える企業における拠点間接続や、テレワーク等による社外から社内システムへの接続、外部ベンダーによるシステム保守のための接続など、用途は多岐にわたります。VPN 機器は社外から内部ネットワークへの接続点となり、常にインターネットに面していることから、侵害された場合に組織への影響が大きく、攻撃者から狙われやすい機器です。

VPN 機器に残存する脆弱性や認証設定の不備が侵入経路として悪用されて、重要なサーバが侵害された結果、業務停止に至ったケースは弊社サイバー救急センターでも数多く相談を受けています。また、プラットフォーム診断の対象に VPN 機器を指定されるお客様も増加傾向にあります。

[6] 情報セキュリティ 10 大脅威 2026 – IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/10threats/10threats2026.html

● 攻撃影響がサプライチェーン全体に波及した事例

サプライチェーンは、製品の原材料調達から製造、在庫管理、配送、顧客への販売に至る一連のビジネスプロセスを指します。多くの企業では、委託先や協力会社など複数企業と密接に連携して事業を運営しているため、サプライチェーン上の企業が攻撃を受けた場合、影響はその企業だけにとどまらず、サプライチェーン全体に甚大な被害をもたらすリスクがあります。

実際、委託先のシステムがランサムウェア攻撃を受けたことにより、そのシステムを使用していた委託元企業の一部業務およびそれに伴う製造から販売までのプロセスを停止したケースや、サプライチェーン上の企業が侵害されたことにより関連企業との共有システム経由で侵害が広がったケースは、各種報道で目にしている通りです。また、弊社プラットフォーム診断で、グループ企業や委託先のサーバ・ネットワーク機器などをまとめて診断対象とするご相談が増えてきています。

VPN 機器を狙った攻撃およびサプライチェーン上の脆弱な箇所を狙った攻撃で、共通して注視すべき観点は主に以下の４つです。

- ✓ アクセス制御の設定不備
  設定不備等により、本来一部の従業員のみがアクセスすべき機能を不正に操作されることで、システム情報やその他機密情報取得や情報改ざんの被害に発展する可能性
- ✓ 脆弱な認証方法／パスワードの利用
  システムの認証で、機器認証などを含む強固な二要素認証を利用していない、パスワードによる認証を利用しており強固なパスワードの設定を強制していない、などのために攻撃者に認証を突破され正規ユーザとしてシステムを操作される可能性
- ✓ 古いバージョンのシステム／ソフトウェアの利用
  古いバージョンのシステムやソフトウェアのまま、アップデートせずに利用していたため、残存していた既知の脆弱性を悪用され、情報取得や任意のコード実行等の被害に発展する可能性
- ✓ 脆弱な暗号方式の利用
  ユーザがシステムにアクセスする際の通信で利用する際に、安全な暗号方式を利用していないため、通信の傍受や解読が可能となり、機密情報取得や情報改ざんの被害に発展する可能性

これらのポイントは、プラットフォーム診断でも特によく検出される問題点です。ラックのプラットフォーム診断で検出される問題点の傾向について紹介しますので、上記ポイント以外も含めて、セキュリティ事故に発展する前にシステムに潜むリスクの対処に活用いただけると幸甚です。

プラットフォーム診断における問題点検出傾向

プラットフォーム診断ではインターネット上の悪意のある第三者による攻撃を想定脅威としたリモート診断と、マルウェア感染や内部不正などによる内部ネットワークに対する攻撃を想定脅威としたオンサイト診断に大別されます。弊社が 2025 年に実施したプラットフォーム診断結果に関して、対応が必要な問題点の検出数上位 10 件を、リモート診断とオンサイト診断[7]の順にそれぞれ表 3、表 4 に示します。

表 3 リモート診断において多く検出された「対応が必要」と定める問題点上位 10 件
（2025 年 1 月-2025 年 12 月）

順位	対応が必要な問題点
1	サービスへのパスワード認証を試行可能
2	管理用 Web コンソールにおいてパスワード認証を試行可能
3	HTTP サービスの Web コンテンツにおいてパスワード認証を試行可能
4	暗号化されていない資格情報を受け入れるリモート管理サービスの検出（FTP）
5	POP3 サービスにおいてパスワード認証を試行可能
6	WordPress の REST API にユーザ列挙の脆弱性
7	jQuery 3.0 より前のバージョンに XSS の脆弱性
8	ファイアウォールによるアクセス制御を回避可能
9	HTTP サービスにおけるシステム情報の取得
10	SMTP サービスの VRFY コマンドを利用したユーザ情報の取得

リモート診断では、特定サービスに対するパスワード認証の試行が可能である点やファイアウォールのアクセス制御を回避できる点など、アクセス制御の不備が多数検出されました。実際にサイバー攻撃に発展するようなケースで考えると、アクセス制御に不備のある VPN 機器の管理者用コンソールの認証画面から認証を突破されシステム改ざんや情報窃取に至るケースや、VPN 機器を経由して内部ネットワークの侵入に至るケースが考えられます。

また、パスワード認証を試行可能な問題点が残存している環境では、脆弱なパスワードを設定可能だった場合に、パスワードを推測されて攻撃者に認証を突破される可能性が考えられます。対策として、NIST SP 800-63 などのパスワード要件に関する推奨事項に従い運用することで認証突破の可能性を

[7] プラットフォーム診断 - 株式会社ラック
https://www.lac.co.jp/consulting/platform.html

低減することが可能です[8]。NIST SP 800-63 は、直近では 2025 年に最新版が公開されたように時代の変遷と共に重視すべき内容が再考されるため、それに伴った継続的な運用見直しを実施していくことが重要です。

表 4 オンサイト診断において多く検出された「対応が必要」と定める問題点上位 10 件（2025 年 1 月-2025 年 12 月）

順位	対応が必要な問題点
1	サービスへのパスワード認証を試行可能
2	管理用 Web コンソールにおいてパスワード認証を試行可能
3	HTTP サービスの Web コンテンツにおいてパスワード認証を試行可能
4	SNMP サービスにおいて読み込み/書き込み可能なコミュニティ名が推測可能
5	セキュリティサポートの終了したソフトウェアの利用
6	暗号化されていない資格情報を受け入れるリモート管理サービスの検出（FTP）
7	SMB/NetBIOS サービスの Null セッションを利用したユーザ一覧の取得
8	Proxy を認証なしに利用可能
9	SMB/NetBIOS サービスの Null セッションを利用した資源共有名の一覧情報の取得
10	ファイアウォールによるアクセス制御を回避可能

オンサイト診断では、リモート診断で検出された問題点に加えて、特に、情報取得可能な問題点、Proxy を認証なしに利用可能な、アクセス制御の不備に関する問題点や、システムのセキュリティサポートが終了したソフトウェアの問題点が多数検出されました。実際にサイバー攻撃に発展するようなケースで考えると、内部侵入に成功した攻撃者が取得した情報を利用してその他システムへの侵入を試行するケースや、セキュリティサポートが終了した機器に対して既知の脆弱性の悪用を試行し攻撃拡大を図るケースが想定されます。

ラックで実施した、サプライチェーン上の企業へのプラットフォーム診断（リモート／オンサイト）でも、同様の問題点が検出されています。委託先管理の対策として、これらの問題への対応状況をチェックリストベースで確認している企業は多いと思いますが、可能であれば、プラットフォーム診断を含む脆弱性診断の実施状況と対応状況も詳細を確認することをお勧めします。また、経済産業省が、サプライチェーンの強化に向けた評価制度を進めているため、それらも活用してサプライチェーンの強靭化に取り組む必要があります。

[8] NIST SP 800-63 Digital Identity Guidelines - NIST
https://pages.nist.gov/800-63-4/

閉域環境でも免れないサイバー攻撃のリスク

事例に取り上げたインターネットに面したシステムおよびサプライチェーン上にあるシステムの他にも、企業が運用するシステムの中には、インターネットへ接続しない閉域環境のシステムもあります。

ラックのプラットフォーム診断では、検出された問題点を基にセキュリティ事故に発展する可能性の有無を評価します。下図は、2025 年に実施したリモート診断およびオンサイト診断で、そのような問題点が 1 つ以上検出されたシステム数の割合を示しています。

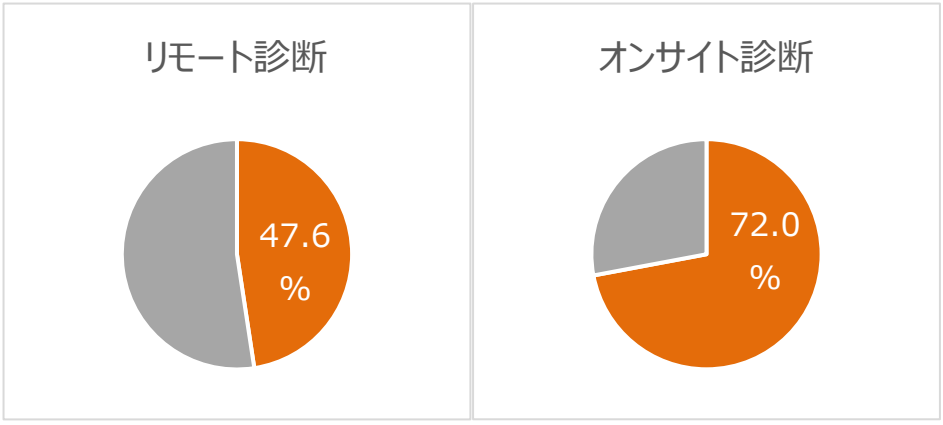

図 6 セキュリティ事故に発展する問題点が 1 つ以上検出されたシステム数の割合
（リモート診断/オンサイト診断）

リモート診断では、47.6%のシステムでセキュリティ事故に発展する問題点が検出されているのに対して、オンサイト診断では、72.0%という結果になりました。傾向として、インターネット公開を想定しているシステムについて、リモートからの攻撃を想定しセキュリティ対策に積極的に取り組んでいることが考えられます。

一方で、閉域環境では、それ自身を理由として相対的にセキュリティ対策の優先度が低くなっているケースも見受けられます。しかし、閉域環境に持ち込んだ端末にマルウェアが潜んでいることに気づかないまま接続し、セキュリティ対策が不十分だったためにマルウェアによる被害があっという間に広がったという事例もあります。そのため、閉域環境に存在するシステムでも、外部公開システムと同様にアクセス制御やネットワーク分離、脆弱性診断の実施等セキュリティ対策に取り組むことが重要です。

なお、閉域だと思っていた環境に、インターネットに面した機器が存在していたというケースもありますので、閉域環境ではシステム構成やインターネット接続の有無の確認も重要なポイントとなります。

最後に

昨今の攻撃事例では、VPN 機器を起点とした攻撃や、一企業または一拠点の侵害を起点としたサプライチェーン全体に波及した攻撃が注目されています。弊社で実施したプラットフォーム診断の中でも、特に初めて診断を実施するお客様では、「プラットフォーム診断における問題点検出傾向」で示した問題点が多く検出される傾向にありますので、表 3 および表 4 を参考にセキュリティ対策を見直していただくことを推奨します。また、サイバー攻撃による被害を低減するためにも、自組織の抱える情報資産にリスクが内在するかどうかに関しては、机上のリスクアセスメントとともに、脆弱性診断も活用して継続的に机上および実査を通じてリスクを可視化し対処し続けることが重要です。また、委託先への脆弱性診断実施状況のヒアリングや、予算とコストに応じてサプライチェーン上の複数システムを統括した脆弱性診断を検討することも有効な手段と言えます。

アンケートのお願い

今後のよりよい記事づくりの参考とさせていただくため、以下の URL または QR コードから、アンケートに回答いただけると幸甚です。忌憚のないご意見・ご感想をお寄せください。

https://jp.surveymonkey.com/r/JS58WFL

株式会社ラック
〒102-0093
東京都千代田区平河町 2-16-1
平河町森タワー
https://www.lac.co.jp/