LAC SECURITY INSIGHT

第 12 号

特集：ペネトレーションテストから見る脅威の傾向

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

2025 年 6 月
株式会社ラック

LAC SECURITY INSIGHT

第 12 号／2025 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
コンサルティング統括部長
内田 法道

サイバー119で出動したインシデント傾向

2025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 35%、およびサーバ不正侵入による被害の相談が52%であり、両者で全体の87%を占めています。この割合は前四半期（2024年10月から12月）の73%、および前年同期（2024年1月から3月）の77%と比較して増加傾向にあります。

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 31%を占めており、前四半期（16%）および前年同期（15%）と比較して高い割合となっています。引き続き不正侵入の経路として SSL-VPN が悪用されています。VPN アカウントの認証情報が攻撃者に悪用される原因が判明しない場合もありますが、多要素認証（MFA）を有効にしていない、容易に推測可能なパスワードを使用している、SSL-VPN機器のOSバージョンに含まれる脆弱性に対処していない、などが原因として考えられます。

サーバ不正侵入の被害では、プラットフォームの脆弱性に起因する被害が全体の 17%を占めており、前四半期（5%）および前年同期（13%）と比較して増加しています。特に、Ivanti 社製品の重大な脆弱性（CVE-2025-0282 および CVE-2025-0283）を狙った攻撃が増加しており、製品メーカーから重大なセキュリティアップデートが公開された際には早急なパッチ適用や侵入痕跡の確認が重要です。

前四半期（3%）および前年同期（7%）と比較して増加しているカテゴリは内部犯行であり、当該期間では全体の 9%を占めました。従業員が社内ポリシーで禁止されているにもかかわらず、個人のメールアドレス宛てにファイルを送付する方法や私用 PC を社内に持ち込んで作業をするといった方法でデータの持ち出しが疑われる相談が寄せられました。対策としては、従業員に対する情報セキュリティ教育やモラル教育の強化が必要であるほか、セキュリティポリシーや運用による対策だけでなく、システム的に情報を持ち出せない、および持ち出しても参照できないような仕組みを導入することも有効です。

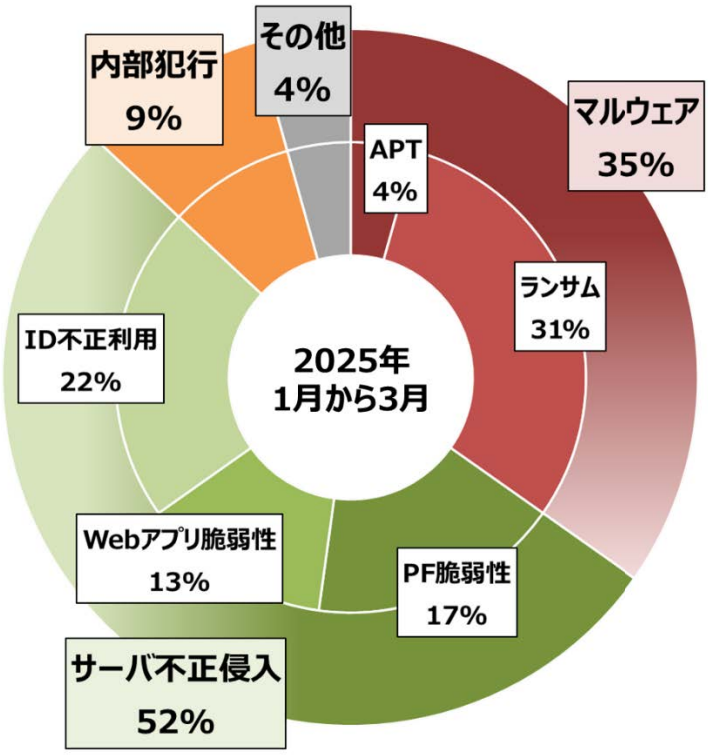

図 1　2025 年 1 月から 3 月の出動インシデントの内訳

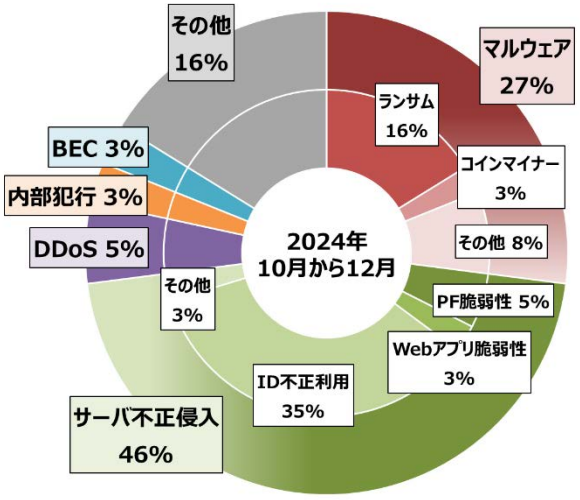

図 2　前四半期（2024 年 10 月から 12 月）

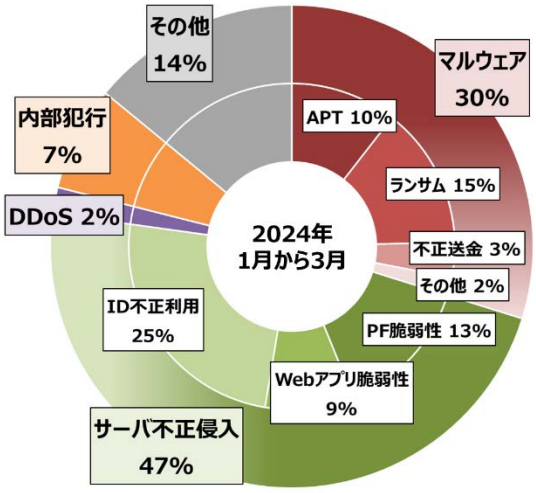

図 3　前年同期（2024 年 1 月から 3 月）

【SSL-VPN 機器の脆弱性とその対策について】

2025 年 1 月 8 日（現地時間）に、Ivanti 社製品の重大な脆弱性（CVE-2025-0282 および CVE-2025-0283）が公表されました [1]。当該脆弱性を悪用した攻撃者は、Ivanti 社製品上で認証情報を収集することが報告されており、VPN セッション情報やセッションクッキー、API キー、証明書、VPN 接続に利用した資格情報などが窃取される可能性があります [2]。当該脆弱性による侵害の有無については、Ivanti 社から提供されている整合性チェックツールを利用して確認できます。脆弱性情報が公開されてから対策するまでに、しばらく期間があいてしまった場合には、念のため整合性チェックツールを利用して確認することを推奨します。

また、2025 年 1 月 10 日（現地時間）には、Fortinet 社製品の脆弱性（CVE-2024-55591）を悪用した攻撃の観測が公開され、2025 年 2 月 11 日には CVE-2025-24472 も攻撃に悪用されていることが追加で公開されました [3]。これらの脆弱性を悪用した攻撃者は、管理者アカウントの作成、設定変更、ログの窃取・改ざん、定期的に実行されるアカウント作成ジョブの追加、VPN アカウントの追加（VPN 機能が有効な場合）、および他機器への横展開などを行っている可能性があります [4]。仮に侵害されていた場合、パッチを適用したとしても攻撃者が作成したアカウントが残存している可能性があります。Fortinet 社製品を利用している場合には、パッチ適用に加えて、管理アクセスの制限、管理者アカウントや VPN アカウントの棚卸し、自動化設定有無などが設計通りに正しく設定され、不審な設定がないことを確認することを推奨します。なお、Fortinet 社製品の FortiGate では、FortiOS 7.6.3 以降、全てのモデルで SSL-VPN 機能が利用できなくなりました [5]。

近年では、SSL-VPN 機器の脆弱性が悪用されるケースが絶えず、迅速にパッチを適用した場合でも、ゼロデイ攻撃により脆弱性情報が公開される前に侵害されているケースが報告されています。利用製品の脆弱性情報を収集し、迅速なアップデートや回避策を適用する運用の構築および継続がとても重要で

---

[1] Ivanti Connect Secure などにおける脆弱性（CVE-2025-0282）に関する注意喚起
https://www.jpcert.or.jp/at/2025/at250001.html

[2] Ivanti Connect Secure VPN Targeted in New Zero-Day Exploitation
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day

[3] Authentication bypass in Node.js websocket module and CSF requests
https://fortiguard.fortinet.com/psirt/FG-IR-24-535

[4] New Ransomware Operator Exploits Fortinet Vulnerability Duo
https://www.forescout.com/blog/new-ransomware-operator-exploits-fortinet-vulnerability-duo/

[5] SSL VPN tunnel mode no longer supported
https://docs.fortinet.com/document/fortigate/7.6.3/fortios-release-notes/173430/ssl-vpn-tunnel-mode-no-longer-supported

す。一方で、SASE（Secure Access Service Edge）製品（例：Prisma Access[6]、Netskope[7]）への切り替えなど、オンプレミスの製品が提供する SSL-VPN 機能を利用せずに、クラウドサービスが提供するリモートアクセスサービスへの変更も、今後のセキュリティ強化策の一案として検討する必要があると考えます。

【ランサムウェアによる被害への備え】

当該期間には、ランサムウェアによる被害に関する多くの相談を受けました。数台規模の被害もあれば、複数拠点のサーバや PC のデータが暗号化される大規模な被害事例も多く見受けられました。ランサムウェア被害発生時には、被害拡大防止や復旧、再発防止、対外発表などの対応により多大な負荷がかかります。組織は、被害に遭わないための対策だけでなく、被害に遭った場合に備えた事前準備を行うことも重要です。

ランサムウェア被害発生時に組織が気にする点の 1 つとして、情報漏えいの有無が挙げられます。例えば被害を受けたサーバに個人情報が含まれていた場合には、個人情報保護法に基づく対応（個人情報保護委員会への報告、本人への通知等）が必要です。しかしながら、サーバ内のデータが暗号化されているため、被害サーバにどのようなデータが格納されていたのかの特定に時間がかかる場合があります。被害に遭わないことが最善ですが、被害に遭った際にインシデント対応を迅速に進めるためにも、日頃から個人情報や機密情報などの重要情報をどこに格納しているか情報資産を定期的に棚卸ししておき、ランサムウェア被害に遭わない場所に保存しておくことを推奨します。

また、調査をした結果、具体的にどのファイルが漏えいしたのか特定することが困難な事例も多く見られます。一般的に、ファイアウォールのトラフィックログやファイルサーバのアクセスログ、資産管理ソフトのログなどが情報漏えいの有無や対象ファイルの特定に有用です。しかし、ログを取得していない、侵害時期のログが消失している、ログを保管していたサーバが暗号化されてしまいログを閲覧できない状態にある、などの理由により十分な調査が実施できないことがあります。

このような状況を防ぐために、ログの保管期間や保管場所を見直すことを推奨します。具体的には、取得したログは社内ネットワークとは異なるネットワーク環境に保管する、またはデータが一度書き込まれると

---

[6] Prisma® Access（Palo Alto Networks）～包括的なクラウド配信型セキュリティプラットフォーム～
https://www.lac.co.jp/solution_product/prismaaccess.html

[7] Netskope（ネットスコープ）
https://www.lac.co.jp/solution_product/netskope.html

変更や削除ができない特性を持つイミュータブルストレージ（例：Rubrik[8]、AWS S3 Object Lock[9]）に保管し、データの改ざんや不正アクセスから保護するなどの対策が有効です。なお、ログだけでなく、サーバのバックアップデータもイミュータブルストレージへ保管することで、暗号化の被害を防ぎ、復旧作業の負担を軽減することが期待できます。被害に遭う前に、データやログの保管について見直すことを推奨します。

[8] Rubrik Security Cloud
https://www.rubrik.com/ja/products

[9] S3 Object Lock を使用したオブジェクトのロック
https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/object-lock.html

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

2025 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、358 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 22 件（6.15%）、ネットワーク内部からの通信によるインシデントが 336 件（93.85%）であり、インターネットからの攻撃によるインシデント、ネットワーク内部からの通信によるインシデントともに、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

攻撃者により WebShell がサーバに設置されていることを確認したインシデントが、複数回発生しました。いずれも、攻撃者による WebShell へのアクセスを試みる通信を検知したため追加調査したところ、当該 WebShell がサーバに設置されていることを確認したものになります。対象のインシデントにおいては、当該 WebShell を悪用して、さらなる不審ファイルのアップロードを試みる通信も検知しており、攻撃者による侵害の拡大の可能性がありました。

このような事例もあるため、WebShell などの悪質なファイルの設置を確認した場合は、当該ファイルを削除するだけではなく、設置された WebShell を起点にさらなる侵害を受けているリスクがあるため、サーバ全体の侵害有無のためのフォレンジック調査、安全なバックアップからのコンテンツの復元等の対応が重要となります。

Web サービス系以外の攻撃のトピックとしては、DDoS 攻撃の可能性があるインシデントを検知しました。図 4 に、2025 年 1 月から 3 月の重要インシデントの内訳を示します。

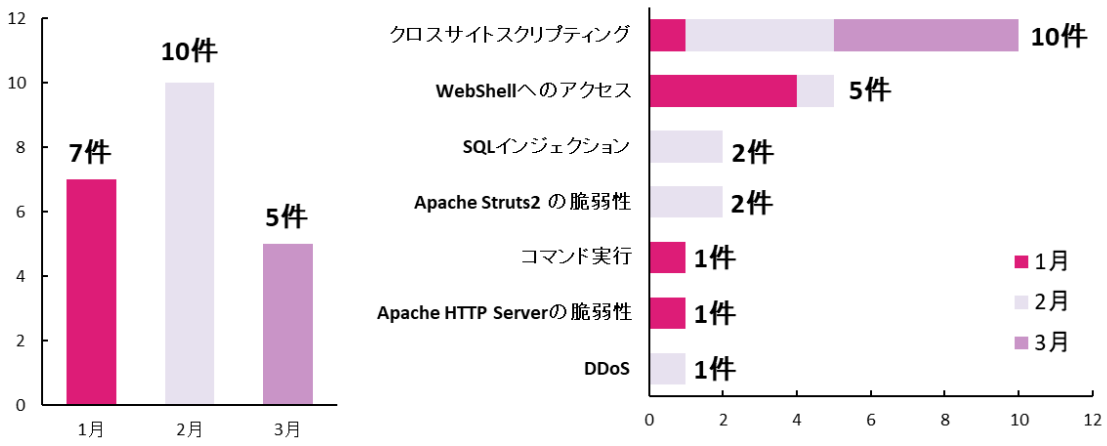

図 4　[外部から] 2025 年 1 月から 3 月の重要インシデントの内訳（月別・種類別）

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が、その多くは一部のお客様で継続している不審な通信によるものでした。発生したマルウェア感染インシデントでは、ブラウザに保存された機微情報の窃取を行う Arechclient2 や、メディア機器を対象に感染例が報告されている Vo1d に感染したことに起因する通信を検知したものになります。

マルウェア以外の重要インシデントのトピックとしては、監視対象ホストにて内部ネットワークの探索や不審なコマンド実行を検知したインシデントが発生しました。図 5 に、2025 年 1 月から 3 月の重要インシデントの内訳を示します。

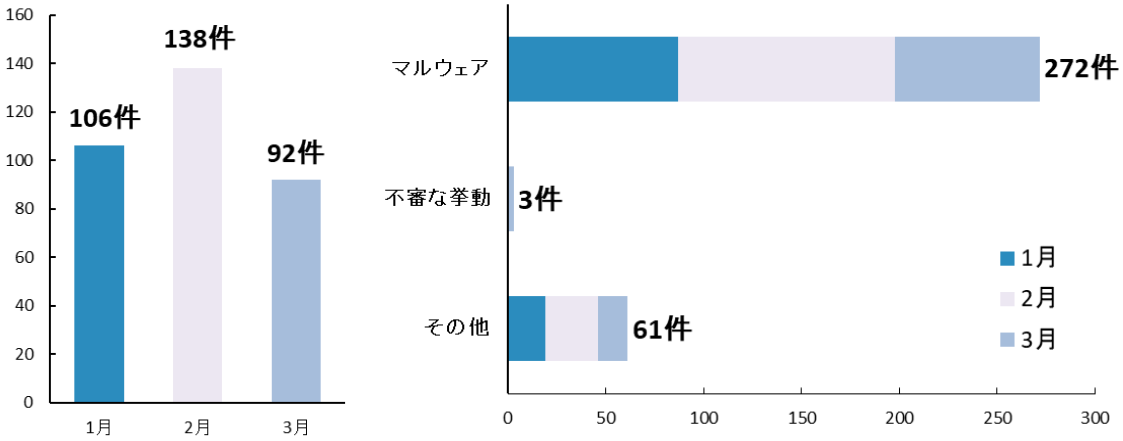

図 5　[内部から] 2025 年 1 月から 3 月の重要インシデントの内訳（月別・種類別）

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 1　注意が必要な通信について

概要	JSOC の検知内容	検知時期
192.3.1.169（アメリカ）からの通信	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。	1 月中旬～ 3 月中旬
46.19.139.130（スイス）からの通信	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。	2 月上旬～ 3 月下旬
Palo Alto Networks 社製品の脆弱性（CVE-2025-0108）を狙った攻撃	Palo Alto Networks 社製品に存在する脆弱性（CVE-2025-0108）を狙った攻撃通信を多数検知しました。	2 月 17 日～
Next.js の脆弱性（CVE-2025-29927）を狙った攻撃	Next.js に存在する脆弱性（CVE-2025-29927）を狙った攻撃通信を多数検知しました。	3 月 26 日～

特集：ペネトレーションテストから見る脅威の傾向

攻撃シナリオの傾向

ペネトレーションテスト（侵入テスト）は「対象のシステムに対して疑似的な攻撃を行い、攻撃者の目的が達成されるかを実証する」ことで、認識することが難しい潜在的な脅威を洗い出すテストです。疑似的な攻撃を行う上で欠かせないのが、攻撃の内容を定義する「攻撃シナリオ」です。組織が業務で利用している情報システムを調査対象とする、ラックの「情報システムペネトレーションテストサービス」では、「攻撃シナリオ」は「スコープ」、「起点」、「目標」の 3 つの要素から構成されます。例えば、一般的な高度標的型攻撃（APT 攻撃）の攻撃内容をこの攻撃シナリオの要素に当てはめると、以下になります。

- スコープ（＝テストの対象範囲）　：組織内部のネットワーク全体
- 起点　（＝テストの開始地点）　：従業員が業務で使用している PC 端末のマルウェア感染
- 目標　（＝テストのゴール）　：ドメイン管理者権限の奪取および重要情報の窃取

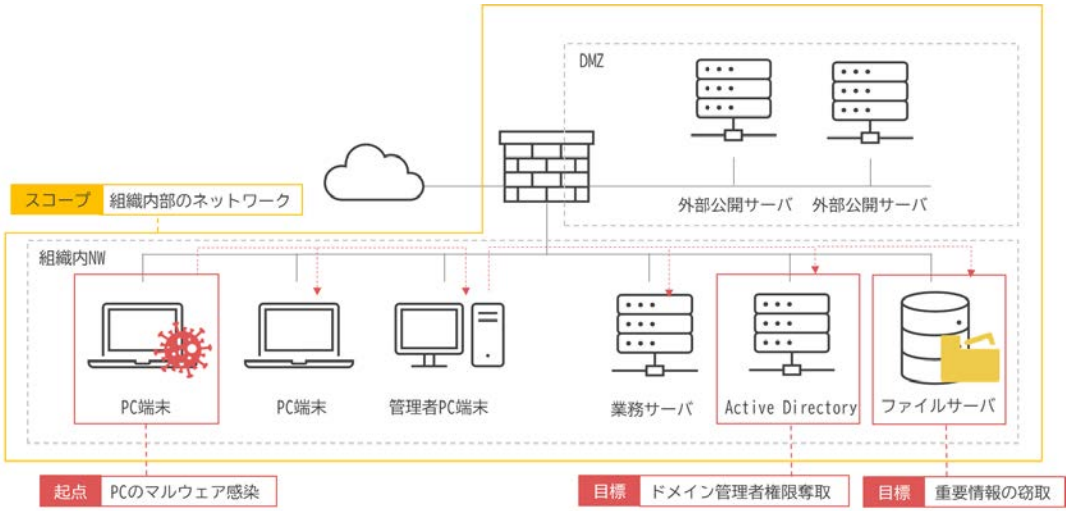

図 6　一般的な高度標的型攻撃（APT 攻撃）の攻撃シナリオ

攻撃シナリオの検討にはセキュリティ脅威のような組織外の動向に関する要素と、システム環境といった組織内の要素といった両方の視点が必要となるため、お客様とラックとで協力してお客様ごとに個別の攻撃シナリオを作成します。攻撃シナリオは、組織の情報システム環境において想定されるセキュリティ脅威

が反映されたものであり、お客様の情報システムにおける「守りたいもの」が反映されたものとなります。

2024 年度における攻撃シナリオの傾向

2024 年 4 月から 2025 年 3 月までの間にラックがお客様に対して実施したペネトレーションテストで用いた攻撃シナリオの傾向として、以下が挙げられます。

- スコープ：クラウド上の独自システムを対象とするケースが増加
- 起点　：インターネット外部からの攻撃を起点とするテストの実施
- 目標　：クラウド上の重要情報の社外への持ち出し可否に着目

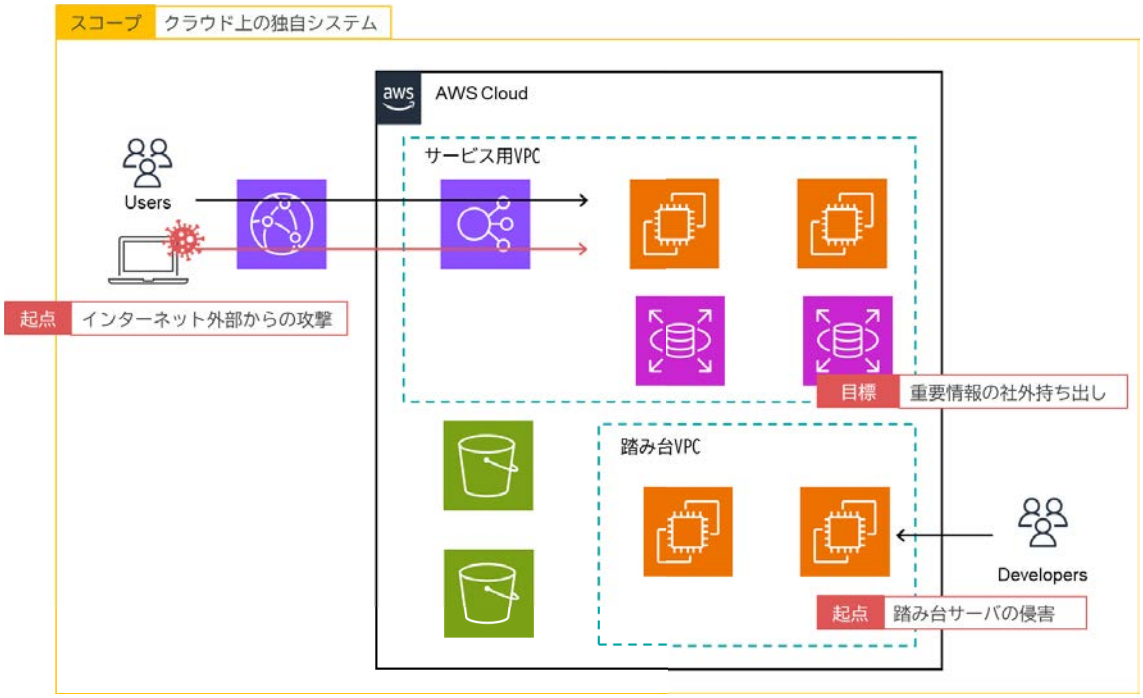

図 7　2024 年度における攻撃シナリオの傾向

クラウド上に構築された独自システムを対象とするテスト

ペネトレーションテストのサービス開始以降、社内ネットワークのようないわゆる OA 環境と呼ばれるシステムを対象としてテストを実施するケースが多くを占めてきましたが、2024 年度では OA 環境以外のシステムを対象とするケースも徐々に増えてきました。社内向けの業務システムのようなものもあれば、エンドユーザ向けにサービスを提供する用途の外部向け Web システムを対象とするケースも複数ありました。

こういったシステムはクラウド上に構築されることが多く、OA 環境で部分的にクラウドサービスを利用しているようなケースも含め、クラウド環境がペネトレーションテストのスコープに含まれるケースは、2023 年度

から増加傾向にあります。

インターネット外部からの攻撃を起点に

外部向け Web システムを対象とするペネトレーションテストを実施する場合、従来では踏み台サーバなどのネットワーク内部の端末が侵害されたことを想定したシナリオでの調査が一般的でした。2024 年度では内部の端末が侵害された想定のシナリオと合わせて、インターネット外部からの攻撃を想定したシナリオでのペネトレーションテストを実施するケースが徐々に増加しています。

Web システムのような公開システムに対するインターネット外部からのセキュリティ評価としては脆弱性診断が一般的でしたが、近年では脆弱性診断と合わせて侵入可否や侵入後の侵害活動の可否に焦点を当てたペネトレーションテストを合わせて実施する取り組みが広がりつつあります。

インターネット外部からの攻撃を想定したシナリオでは、OSINT（Open Source Intelligence：インターネット上などに一般公開されている情報を収集・分析し、インテリジェンスとして活用する手法）をペネトレーションテストと組み合わせる方法を採用すると効果的です。通常の脆弱性診断などではお客様から指定いただいた対象に対してセキュリティホールの有無を調査する方法が一般的ですが、OSINT を組み合わせることで、攻撃者視点でシステムがインターネットからどのように見えているか、どのホスト・サービスが攻撃対象として有用かという攻撃対象の選定部分も含めた調査が可能になります。

クラウド上の重要情報の社外への持ち出し

攻撃シナリオの目標にあたる部分では、「重要情報の社外への持ち出し」を重要視される企業が引き続き多く見られます。OA 環境からの情報持ち出しの経路はメールや USB メモリなどの可搬記憶媒体、各種 SaaS などさまざまなものが存在しますが、クラウド上に構築されたシステムでは、従来の経路に加えてクラウド特有の持ち出し経路が存在する場合があります。

また、社内の重要情報の外部への持ち出しは、組織内部に侵入した攻撃者だけではなく、悪意のある内部不正者によっても行われることがポイントです。

内部不正が発生する要因として、「動機」、「機会」、「正当化」からなる不正のトライアングルという概念があります。この理論では、「動機」、「機会」、「正当化」の 3 つの要素がそろった時に内部不正が発生するとされます。ペネトレーションテストを実施することで、この 3 つの要素のうち、情報を外部に持ち出す「機会」がシステム上に存在するかどうかを把握できるため、内部不正の対策としても活用することが可能です。

テストで検出した問題点の傾向

2024 年 4 月から 2025 年 3 月までの間にラックがお客様に対して実施したペネトレーションテストで多く検出されたセキュリティ上の問題点 Top5 を以下の表に示します。

表 2　2024 年度に多く検出されたセキュリティ上の問題点の一覧

順位	Tactics（戦術）[10]	検出されたセキュリティ上の問題点の例
1	Credential Access （認証情報へのアクセス）	・ 認証情報が記載されたファイルの存在 ・ 脆弱なパスワードの利用
2	Privilege Escalation （権限昇格）	・ アカウントやロールへの過剰な権限の付与 ・ フォルダのアクセス制御不備
3	Lateral Movement （横展開）	・ 推奨されていないコンピュータアカウント作成の設定 ・ 低権限アカウントにローカル管理者権限が付与された端末が存在
4	Command and Control （コマンド＆コントロール）	・ インターネットから端末の遠隔操作が可能
5	Defense Evasion （防衛機構の回避）	・ PowerShell バージョン 2 が実行可能 ・ マルウェアの検知回避

例年に引き続き、「Credential Access（認証情報へのアクセス）」に関連する問題点を多く検出しています。このことは、テストにおいて攻撃シナリオを遂行する中で、何らかの方法でドメインアカウントなどの認証情報を入手し、入手した認証情報を使用して他の端末やサーバへの横断的侵害を進めるパターンが多いことを示します。多く検出されたセキュリティ上の問題点に関して、特筆すべきトピックを 5 点紹介します。

① パスワードの運用に関する問題点

ペネトレーションテストにおいてパスワードの運用に関する問題点が多く検出される傾向は、ラックが情報システムペネトレーションテストの提供を開始した 2015 年から常に変わらず、またお客様の組織の規模や業種などを問わず、同様の傾向が見受けられます。実際のサイバー攻撃において、組織のネットワーク内部に侵入した攻撃者が他の端末やサーバへ横断的侵害を進めていく際には、端末やサーバの脆弱性を

[10] MITRE ATT&CK®（https://attack.mitre.org/）の Tactics（https://attack.mitre.org/tactics/enterprise/）をもとに問題点を分類

悪用する方法もありますが、脆弱なパスワード設定や共通アカウントの利用といったパスワードの運用に関する問題点を悪用する方法が一般的です。攻撃者の視点では、正規のアカウントを用いて操作を行うことで、攻撃行為が検知されにくくなるなどの利点があるためと考えられます。

② 認証情報が記載されたファイルの存在

マルウェア感染により攻撃者が遠隔操作の確立に成功したことを想定した PC や、組織で利用しているファイルサーバ上に、認証情報が記載されたファイルが存在しているケースが引き続き多く見られました。また、2024 年度の特徴的な検出の傾向として、PC だけではなく踏み台サーバのような業務で使用するサーバ上にも、認証情報が記載されたファイルが存在しているケースも複数確認しています。

こういった認証情報は重要な情報が保存されているサーバへの横断的侵害への足掛かりとなり、重要なサーバから情報を窃取するという攻撃者の目的達成に大きく寄与します。また、認証情報が記載されたファイルと合わせてネットワーク構成が記載されたファイルなども閲覧可能な場合には、それらの情報を突き合わせてバックアップサーバの存在を把握し、より上位の権限を奪取した後にバックアップサーバへアクセスするような攻撃活動にもつながります。

③ 過剰な権限の付与による権限昇格

Privilege Escalation（権限昇格）に関するセキュリティ上の問題点について、2023 年度までは Windows OS におけるローカル権限昇格の脆弱性やフォルダのアクセス不備によるものが多く見られましたが、2024 年度ではアカウントやロールへの過剰な権限の付与によるものが多く見られました。要因として、クラウド上に構築されたシステムをテスト対象とすることが増えたことで、クラウド上のリソースへのアクセス管理に不備があるケースが多く検出されるようになったことが挙げられます。

具体的な例の 1 つとしては、各種のクラウドサービスにおける IAM（Identity and Access Management）でのアクセス管理の不備が挙げられます。複数のサービスを統合して使用することによるアクセス管理の複雑化や、業務効率の優先などの要因で、本来の操作に必要な権限を超えた広範な権限がアカウントやロールに付与されており、その設定を悪用することで権限昇格につながるケースが複数見られました。より高位の権限に昇格することで、システムでの侵入範囲拡大に悪用される恐れがあります。

また、クラウド環境に限らず、オンプレミス環境とクラウド環境との連携部分の設定を悪用する権限昇格の問題点も検出されています。具体的には、オンプレミス環境の Active Directory とクラウド環境の Entra ID が連携しており、AD のドメインユーザが Entra ID の特権を持つ環境を確認しました。このような環境では、AD のドメイン管理者権限が奪取された場合、芋づる式に EntraID の特権も奪取されてしまいます。

④ インターネットからの端末の遠隔操作

2024 年度では Command and Control（C2）サーバに関するセキュリティ上の問題点が初めて上位に入りました。この問題点は、業務で使用する PC がマルウェアに感染するなどした場合、マルウェア感染した端末と攻撃者が管理する C2 サーバとの間で通信を確立することができ、インターネット外部からの PC の遠隔操作や情報の外部への持ち出しへの悪用につながるものです。とはいえ、OA 環境で PC をインターネットに接続して使用するケースではこの問題点の根本的な対策は難しく、不正な通信先への通信の検知や情報持ち出しの検知などの多層防御が対策として求められます。

このようなセキュリティ上の問題点は OA 環境だけでなく、クラウド上に構築されたシステムでも同様に検出されます。特にインターネットに公開せず、インターネットとの接続を行わないことを想定したシステムであっても注意が必要です。クラウド上での運用のために特定のドメインや IP のみ外部への通信を許可しているような対策をしているシステムであっても、システムの構築に利用しているクラウドサービスと同種のサービスを用いて構築した「調査用の疑似 C2 サーバ」との通信の確立および情報の持ち出しに成功するケースが複数ありました。このようなケースは、本来インターネットとの接続を想定していないシステムにおいて、外部への情報の持ち出しが可能となるため、注意が必要であるといえます。

⑤ コンピュータアカウント作成の設定に起因する横断的侵害

2023 年度に引き続き、推奨されていないコンピュータアカウント作成の設定に起因するセキュリティ上の問題点を多く検出しました。この問題点は対象システム内部での横断的侵害につながるものであり、Resource-based Constrained Delegation（リソースベースの制約付き委任、以下、「RBCD」）攻撃という手法を用いることで検出されています。RBCD 攻撃は実際にこの手法による被害が多数発生していることで、セキュリティ技術者から注目が集まっている攻撃手法であり、ペネトレーションテストにおいてもこの手法で他端末の遠隔操作などにつながるケースが多く見られます。RBCD 攻撃の手法や対策については LAC Security Insight 第 8 号で解説しましたので、そちらも参照ください。

傾向から見る対策の勘所

ペネトレーションテストで検出されるセキュリティ上の問題点は、組織にとっての潜在的な脅威であることが多く、あらかじめ対策をしておくことが困難な側面もあります。しかし、他組織におけるペネトレーションテストで検出された問題点を自組織に当てはめて、自組織で対策ができているかを検討することは有用であると考えます。

以下に示すようなセキュリティ対策の実施状況について、今一度ご確認いただくことを推奨します。

- 認証情報や機密情報が記載されたファイルの管理：PC やサーバ上の認証情報や機密情報を含む不要なファイルは削除してください。保管が必要な場合は閲覧時のパスワード設定などにより閲覧できる人を制限してください。認証情報や機密情報が記載されたファイルについては、定期的に棚卸しするなどの方法で管理を行うことを推奨します。

- 最小権限の付与：アカウントやロールに対して、業務要件に即した必要最低限の権限のみを付与してください。付与した権限については定期的にレビューし、不要な権限を削除することを推奨します。必要に応じて、IAM の設定を自動で監視し、異常を検出するようなツールを活用することも有用です。

- ネットワーク監視と不正通信の検知：インターネットからの端末の遠隔操作の対策としては、業務上必要な通信先に限定することが挙げられますが、外部との通信を完全に限定および遮断することは多くの場合困難です。そのため、不正な通信をリアルタイムで監視し、検知する体制を整えることが望ましいです。

- 特権アカウントの保護：最小権限の原則において、コンピュータアカウントの新規作成や委任先の登録といった権限を付与する特権アカウントの保護が重要です。上記のパスワードポリシーの強化に加え、特権アカウントが不正に利用されていないか、監視を強化することも対策として有効です。

- コンピュータアカウントの保護：先述の通り、コンピュータアカウントの新規作成を制限したとしても、攻撃者は既存のコンピュータアカウントを奪取することで RBCD 攻撃が可能です。RBCD 攻撃に限らず、端末に最新のセキュリティ更新プログラムを適用する、Credential Guard を有効にするなどの対策でパスワードのハッシュ値を窃取されるリスクの低減に努めてください。

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/ZQDWB9Y

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/