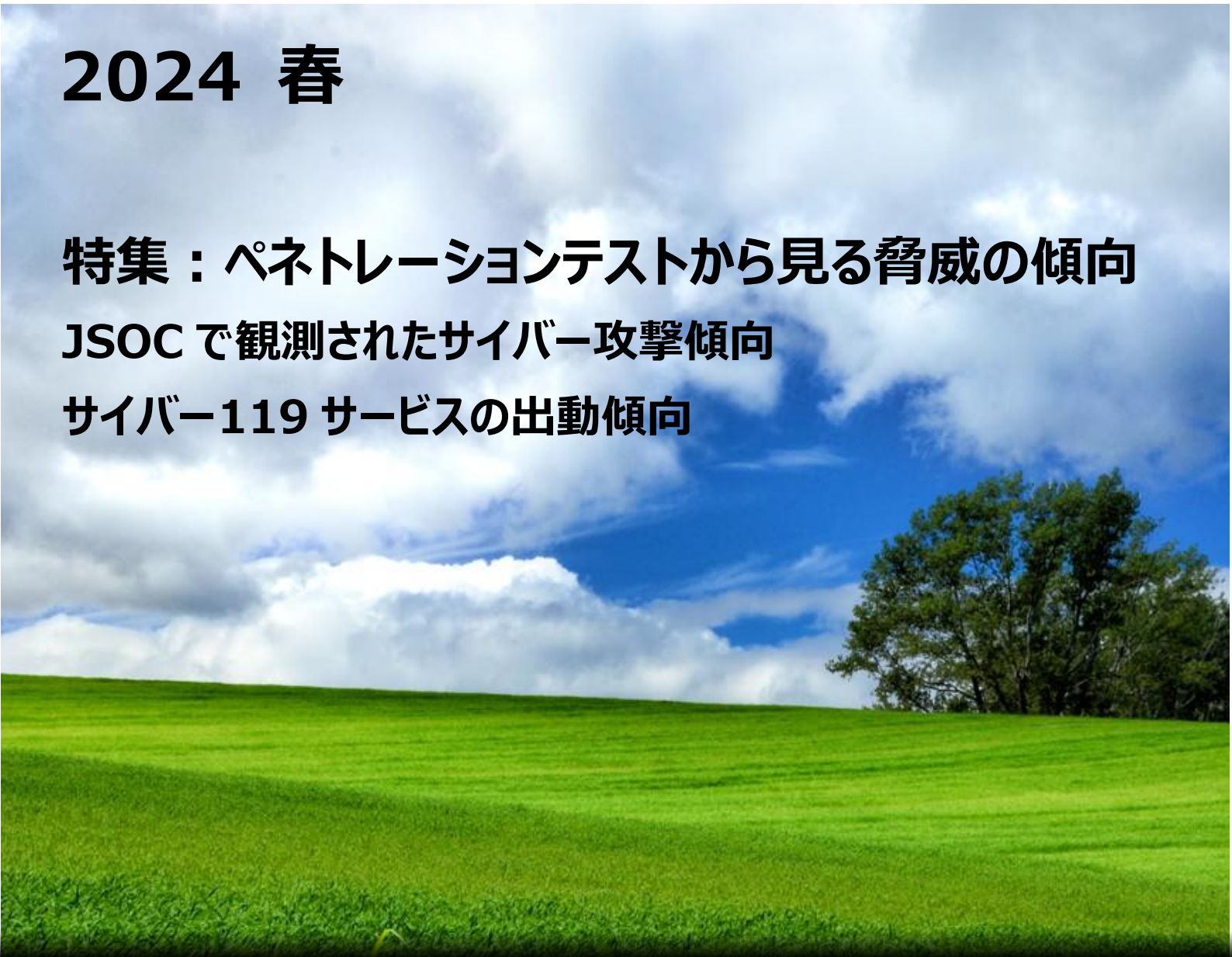
LAC SECURITY INSIGHT

第 8 号

2024 春



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

JAPAN SECURITY OPERATION CENTER

CYBER EMERGENCY CENTER

2024 年 5 月
株式会社ラック

LAC SECURITY INSIGHT

第 8 号／2024 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サービス部において、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
技術統括部 副統括部長
内田 法道

サイバー119で出動したインシデント傾向

2024年1月～3月の出動傾向

当該期間では、マルウェア関連による被害の相談が30%、およびサーバ不正侵入による被害の相談が47%であり、両者で全体の77%を占めています。マルウェア関連による被害の相談は前四半期（2023 年 10 月から 12 月）および前年同期（2023 年 1 月から 3 月）と同様の傾向ですが、サーバ不正侵入による被害は前四半期（35%）および前年同期（40%）と比較して増加しています。一方で、内部不正による被害の相談が7%であり、前四半期（12%）および前年同期12%）と比較して減少しています。

マルウェア関連の被害では、依然としてランサムウェア関連による被害が前四半期（14%）および前年同期（15%）と同様に15%と高い割合を占めており、不正侵入の経路としてはリモート接続機器の脆弱性が引き続き悪用されています。特に 1 月に公開された Ivanti社製品の脆弱性[1]を悪用する攻撃の相談が多く寄せられています。

サーバ不正侵入関連の被害では、ID不正利用の被害が全体の25%と、前四半期（12%）および前年同期（15%）と比較して高い割合を占めています。特にクラウドサービスの管理アカウントが不正利用される事例が多く、多要素認証の未導入や古い管理アカウントの管理不備などが要因と考えられます。

[1] CVE-2023-46805 および CVE-2024-21887（https://www.jpcert.or.jp/at/2024/at240002.html）

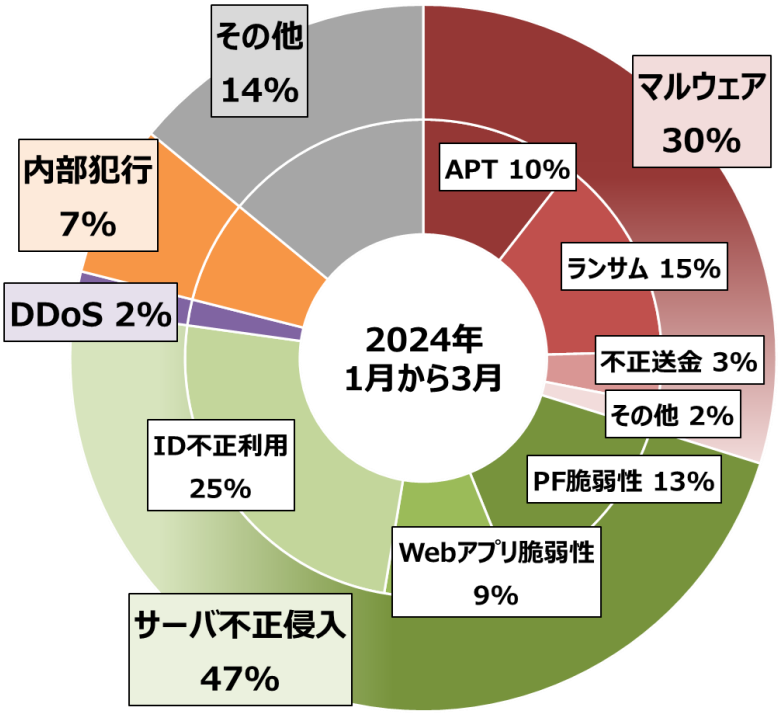


図 1　2024 年 1 月から 3 月の出動インシデントの内訳

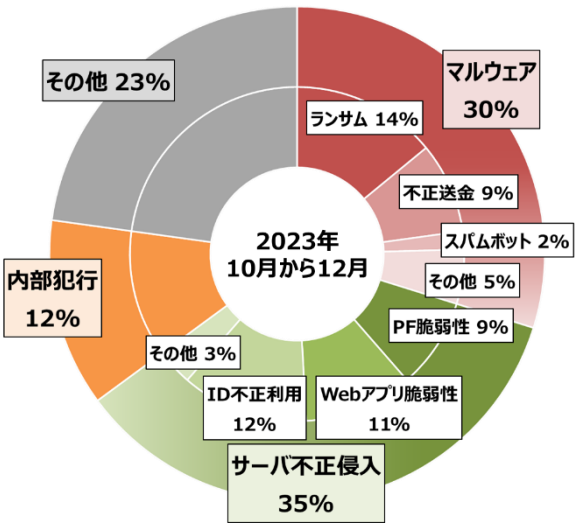


図 2 前四半期（2023 年 10 月から 12 月）

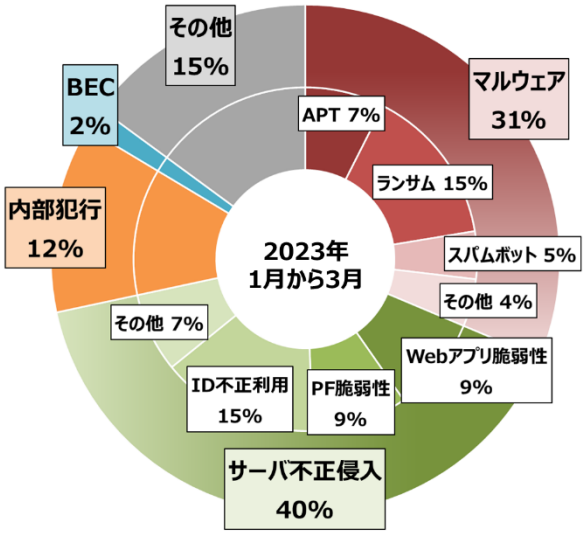


図 3 前年同期（2023 年 1 月から 3 月）

【Ivanti 社製品の脆弱性を悪用した攻撃】

近年、SSL-VPN 機器は企業の内部ネットワークへの侵入口として、攻撃者にとって主要なターゲットとなっています。侵入の手口として、SSL-VPN 機器の脆弱性が利用されるケースが多く、SSL-VPN 機器の脆弱性情報が公開される前に悪用されたケースも報告されています。また、脆弱性情報の公表後および当該脆弱性を実証するコードの公開後に攻撃が増加する傾向も報告されています。

2024 年1月10日（現地時間）に海外のセキュリティベンダーから Ivanti 社製品の脆弱性（CVE-2023-46805 および CVE-2024-21887）を悪用する攻撃事例が公開され、1 月 16 日に、Ivanti 社から当該脆弱性の侵害有無を確認する整合性チェックツールが公開されました。複数の組織が整合性チェックツールを実行した結果、脆弱性が悪用され侵害されていたことを確認しており、当該脆弱性が公表される前もしくはその前後で被害を受けていたと考えられます。

当該脆弱性を悪用されることによって、SSL-VPN 機器に WebShell が作成され、機器内に保存されていたネットワーク情報などの設定情報やアカウント情報が盗み出される可能性があります。これらの侵害は目立たない形で行われており、Ivanti 社製品を利用する組織側で脆弱性情報をキャッチしIvanti 社製品を意識的に監視していないと、侵害されていることに気付けない可能性があります。実際にサイバー119 に相談いただいた組織は、脆弱性情報の公表を受けて整合性チェックツールを実行した結果、侵害の可能性を認知したものでした。Ivanti 社製品を使用しており、まだアップデートや侵害有無を確認するツールを実行していない場合は、既に侵害されている可能性を考慮して、Ivanti 社が提供する最新の情報を確認の上で、侵害有無を調査することを推奨します。

2024 年 4 月には、Palo Alto Networks 社製品の重大な脆弱性が公表[2]され、その脆弱性を悪用した攻撃が増加しています。実際に被害を受けた組織の存在も確認されていますので、当該製品を利用されている場合は、メーカーから公開されている侵害痕跡方法の実施、対応を迅速に行うことを推奨します。

このように SSL-VPN 機器の脆弱性は攻撃者に常に狙われているため、日頃から使用している製品の脆弱性情報を収集し、素早くアップデートや回避策の適用を行える運用の構築および継続が重要です。また、脆弱性情報が公開された直後は、回避策をさらに回避するような細工がなされた攻撃方法が新たに発生するなど、状況が変化する可能性があるため、回避策による対策を実施した場合はアップデートするまで継続的に情報を収集する必要があります。自組織での運用が難しい場合は、脆弱性情報収集・管理ツールやマネージドサービスの活用も検討ください。

[2] CVE-2024-3400 （https://www.lac.co.jp/lacwatch/alert/20240415_003818.html）

【クラウドサービスの ID 不正利用】

当該期間にはID不正利用による被害に関する相談を多くいただきました。ご相談の大半はクラウド環境のアカウントの不正利用でした。特に、AWSやAzureなどのクラウドサービスの管理アカウントが不正利用される事例とMicrosoft365やメールサービスのアカウント情報が不正利用される事例が多く見受けられました。

クラウドサービスの管理アカウントが不正利用された際の被害としては、クラウドサーバ上のデータ削除や漏えい、暗号資産のマイニングや踏み台用の新たなサーバの作成などが考えられます。また、開発やテスト段階で作成されたアカウントが残っていたため悪用される事例も確認されています。それらのアカウントは、正規な運用で管理されておらず、脆弱なパスワードが使用されていたり、必要以上の権限が与えられていたりするなどアカウント管理に不備があることが多く、不正利用の被害を受けやすい傾向にあります。

アカウントに関しては、不要なアカウントがないか棚卸しをした上で、必要なアカウントに必要最低限の権限のみを付与する運用が大切です。また、アカウント管理のベストプラクティスを公開しているクラウドサービス提供企業[3]もあるので、運用規則を策定する上で参考になります。

メールサービスのアカウントが不正利用された際の被害としては、メールでやり取りしている情報の漏えいだけでなく、不正利用されたアカウントになりすまして関係者へメールが送付されるなどの二次被害の可能性も考えられます。さらに、メールアドレスをひもづけている他のサービスのアカウントの侵害（パスワードの再設定を行って不正利用）につながる可能性もあります。

被害の要因の多くは、アカウントの認証方法としてパスワード認証のみを利用している点でした。サービスで提供されている多要素認証を利用することで、万が一ID/PWが漏えいまたは推測された場合でも、アカウントを守れる可能性が高くなるため、多要素認証の利用を検討ください。

---

[3] Amazon Web Services, Inc. :
https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html
Microsoft Corporation :
https://learn.microsoft.com/ja-jp/azure/security/fundamentals/identity-management-best-practices
Google LCC :
https://cloud.google.com/architecture/identity/best-practices-for-planning?hl=ja

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

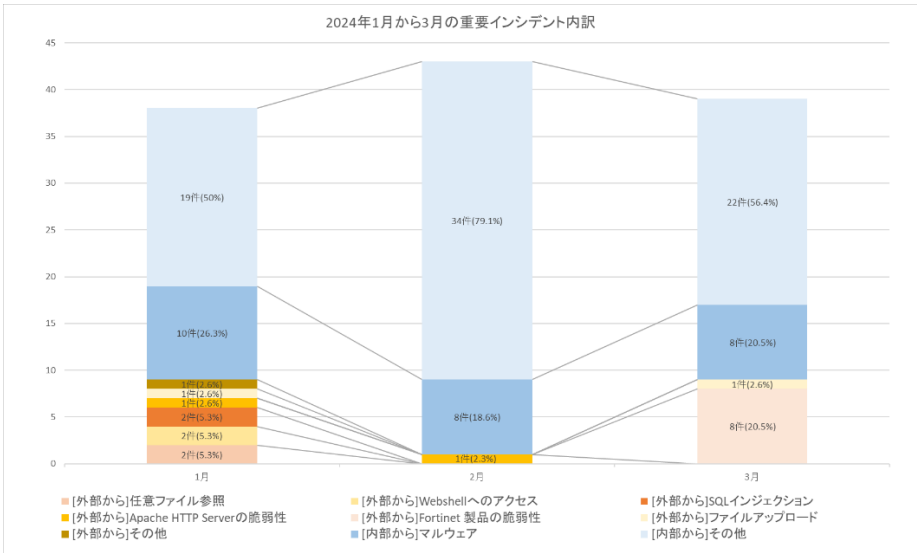
2024 年1月から3月に発生した重要インシデント(検知件数の多寡を問わず攻撃の成功を確認もしくは被害が発生している可能性が高いと判断されるセキュリティインシデント)の合計件数は 120件でした。内訳はインターネットからの攻撃によるインシデントが19件(16%)、ネットワーク内部からの通信によるインシデントが 101 件(84%)であり、前四半期と比較していずれも増加しました。図４に2024年1月から3月の重要インシデントの内訳を示します。

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

Fortinet社製品に存在する脆弱性(CVE-2024-21762)を狙った攻撃通信を検知しました。そのほかには、WebShellへのアクセスを試みる通信を検知し、JSOCによる調査の結果、サーバ上にWebShell と考えられるファイルが設置されている事例がありました。

2) ネットワーク内部から発生した重要インシデント

Stealcをはじめとするマルウェアの感染に起因する重要インシデントが多く発生しました。また、不審なあて先に対する通信を多数検知しており、Ivanti社製品の脆弱性(CVE-2023-46805、CVE-2024-21887、CVE-2024-21893)を狙った攻撃通信による影響の可能性があります。



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 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
ownCloud 社製品に存在する脆弱性(CVE-2023-49103)を狙った攻撃	ownCloud 社製品に存在する脆弱性(CVE-2023-49103)を狙った攻撃通信を多数検知しました。	1 月上旬～
Atlassian 社製品に存在する脆弱性(CVE-2023-22527)を狙った攻撃の増加	Atlassian 社製品に存在する脆弱性(CVE-2023-22527)を狙った攻撃通信を多数検知しました。	1 月 25 日 ～1 月 29 日
185.224.128.10(オランダ)からの攻撃通信の増加	不審ファイルを取得および実行させるための攻撃通信を多数検知しました。	2 月 8 日 ～2 月 13 日 および 2 月 16 日 ～2 月 19 日
198.46.192.12(アメリカ)からの攻撃通信の増加	3 月 22 日から 3 月 31 日にかけて、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 22 日 ～3 月 31 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

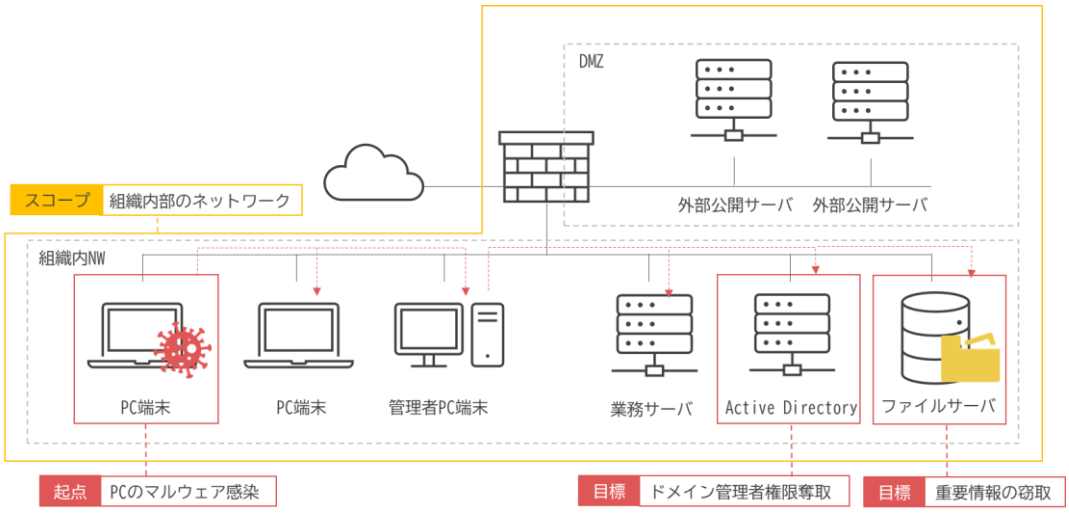


図 5　一般的な高度標的型攻撃（APT 攻撃）の攻撃シナリオ

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。言い換えれば、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」が反映されたものでもあるといえます。

2023 年度における攻撃シナリオの傾向

2023 年 4 月から 2024 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　クラウド環境、特に Microsoft Entra ID 環境が対象
- 起点　リモートワーク用の「持ち出し PC」が起点
- 目標　重要情報の社外への持ち出し可否に着目

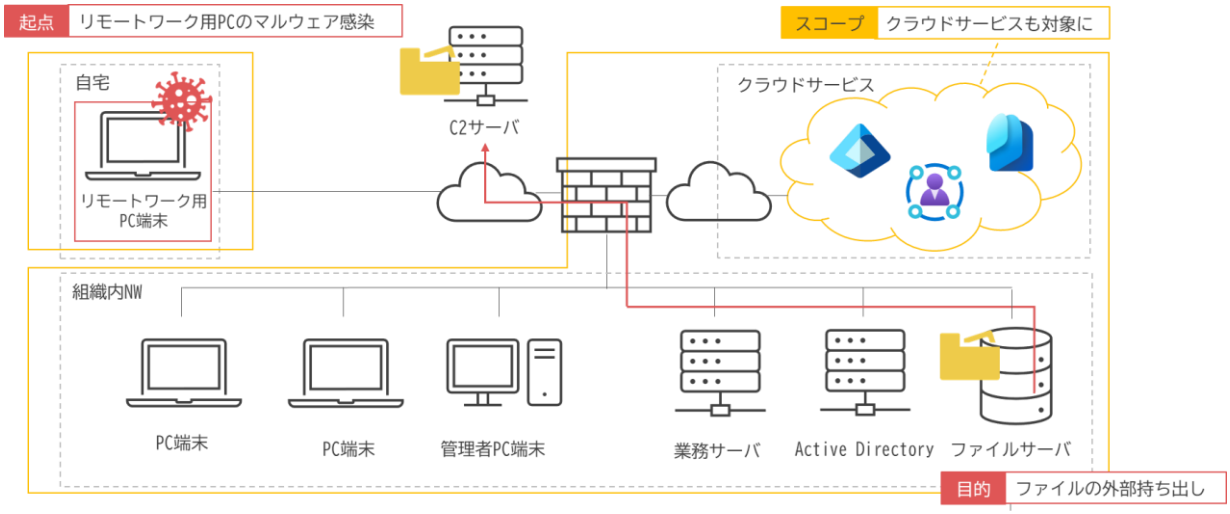


図 6　2023 年度における攻撃シナリオの傾向

クラウド環境、特に Microsoft Entra ID 環境を対象とするテスト

業務で使用しているクラウドサービスをペネトレーションテストのスコープに含めて実施するケースが、2022年度から引き続き多くを占めています。クラウドサービスと一口にいっても、メールの送受信やファイルの保管・共有などの特定の機能を利用することを目的としてSaaSのサービスを利用するケースや、業務システムをクラウド上に構築するために PaaS、IaaS のサービスを利用するケースなど、さまざまな利用の形態があります。特に2023年度は、多くの組織で利用されている IDaaSの 1 つであるMicrosoft

Entra ID（旧 Azure AD）環境をスコープとする組織が多く見られました。

Microsoft Entra IDはMicrosoft社が提供するクラウド型のID・アカウント管理サービスであり、Microsoft 365 や Microsoft Azure などの各種クラウドサービスを運用する環境で使用されます。つまり、従来のオンプレミスの業務環境では Active Directory を使ってアカウントや端末の管理をしていたものが、各種クラウドサービスを運用する環境では、Microsoft Entra IDに置き換えられるという位置づけです。

リモートワークの定着に伴い、クラウド環境はもはや情報システムの一部となっており、それらのクラウド環境の ID・アカウント管理を行うMicrosoft Entra ID環境におけるセキュリティ上の問題点の有無を確認することは、組織の情報セキュリティにとって非常に重要といえます。

リモートワーク用「持ち出し PC」のマルウェア感染

リモートワークの定着に伴い、クラウドサービスをペネトレーションテストのスコープに含めることに加え、リモートワークで社外に持ち出して使用する用途のいわゆる「持ち出し PC」をテストの起点として選択する組織が増加しています。持ち出し PC がマルウェアに感染した場合、社内で使用している PC がマルウェアに感染した際とは異なる状況が発生することが想定されるためです。具体的には、マルウェアに感染したことを CSIRT などのセキュリティ担当者が検知する仕組みや手順、他の社内システムに与える影響の違いなどが想定されます。

また、社外に持ち出せるPCは紛失や盗難のリスクがより高いことから、PC自体の運用でも社内で使用しているPCとは異なる運用を行うケースが考えられますが、その運用でもセキュリティ上の問題点が検出される場合があります。

内部不正による重要情報の社外への持ち出し

業務環境の多様化に伴い、社内の重要情報の外部への持ち出し対策を重要視する企業が増加しています。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、各種クラウドサービスなどさまざまなものが想定されます。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。これは、「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いう理論です。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、内部不正の対策に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

2023 年 4 月から 2024 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を以下の表に示します。

表 2　2023 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）[4]	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	Defense Evasion （防衛機構の回避）	・ 実行ファイルの実行制限の回避 ・ マルウェアの検知回避
3	Privilege Escalation （権限昇格）	・ フォルダのアクセス制御不備 ・ タスクスケジューラに登録されている実行ファイルのアクセス制御不備
4	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
5	Collection （収集）	・ ファイルサーバのアクセス制御不備 ・ 所定のファイルサーバ以外にファイル共有が有効な端末が存在

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、特筆すべき事項を以下に記載します。

[4] 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

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悪用する方法もありますが、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。

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、2023 年度の特徴的な検出の傾向として、Windows の共有フォルダ機能を使用して社内ネットワークで共有されているフォルダ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、重要なサーバからの情報窃取のような目的の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を閲覧可能な場合は、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。

Active Directory 環境における脆弱なパスワードの利用

先述した Microsoft Entra ID 環境では、ユーザの認証に二要素認証を使用するように設定できるため、認証を不正に突破するための問題点がペネトレーションテストで見つかることは少ないといえます。一方で、Microsoft Entra ID環境とオンプレミスのActive Directory環境を併用しており、Microsoft Entra ID 環境側ではセキュリティ上の問題点が検出されなかったものの、Active Directory 環境側では脆弱なパスワードに関連する問題点が検出されたケースがたびたび見受けられます。

Active Directory環境におけるドメインアカウントで脆弱なパスワードを使用しているケースについて、具体的なケースとしては、文字数が少なく単純なものや、組織に関するキーワードが含まれているもの、アカウント名とパスワードが同一の文字列であるものなどが挙げられます。このようなパスワードを使用しているアカウントでは、パスワード推測によるログイン試行、またはすでに侵入に成功した端末から入手したパスワードハッシュ値の解析などの方法でパスワードを容易に特定可能です。

脆弱なパスワードが利用されているのは一般ユーザ権限のドメインアカウントに限りません。これまでに実施したペネトレーションテストでは、ドメイン管理者アカウントでも脆弱なパスワードを使用しており、パスワード推測によるログイン試行のみでドメイン管理者権限の奪取に成功したケースも少なくありません。万が一ドメイン管理者アカウントの認証情報が攻撃者に悪用された場合には、ドメインネットワークの全権限を掌握されてしまう恐れがあります。

脆弱なパスワードが使用される原因の一つとして、Active Directoryのパスワードポリシーの設定が挙げられます。パスワードポリシーにおいて、長さや複雑さに関する要件を定めていない場合、組織のユーザが短く単純なパスワードを設定可能な状態となります。

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年度では、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 攻撃は世界最大級のサイバーセキュリティカンファレンスにて近年取り上げられた手法であり、実際にこの攻撃手法による被害が複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ます。以降にて、RBCD 攻撃の手法や対策について解説します。

リソースベースの制約付き委任（RBCD）とは

リソースベースの制約付き委任とは、ドメインコントローラーのバージョンが Windows Server 2012 以上である Active Directory 環境において、コンピュータが特定のサービスにアクセスする権限を別のコンピュータに「委任」する機能を指します。具体的には、委任元のコンピュータアカウントの権限でのみアクセス可能なサービスに対して、別のコンピュータアカウントの権限でもアクセスが可能となるように、別のコンピュータアカウントに権限を「委任」する行為を指します。リソースベースの制約付き委任は以下の2点の前提がそろった場合に実施可能です。

(1) 委任元のコンピュータアカウントにて特定のサービスにアクセス可能である
(2) ドメインユーザアカウントにて、委任元のコンピュータアカウントに委任先のコンピュータアカウントを委任先として登録する権限を行使できる

委任元のコンピュータアカウントに委任先のコンピュータアカウントが委任先として登録されると、委任先のコンピュータアカウントでも対象のサービスの Kerberos チケットを要求、取得することが可能になります。これは、委任先のコンピュータアカウントで特定のサービスにアクセス可能となることを意味します。これがリソースベースの制約付き委任（RBCD）です。

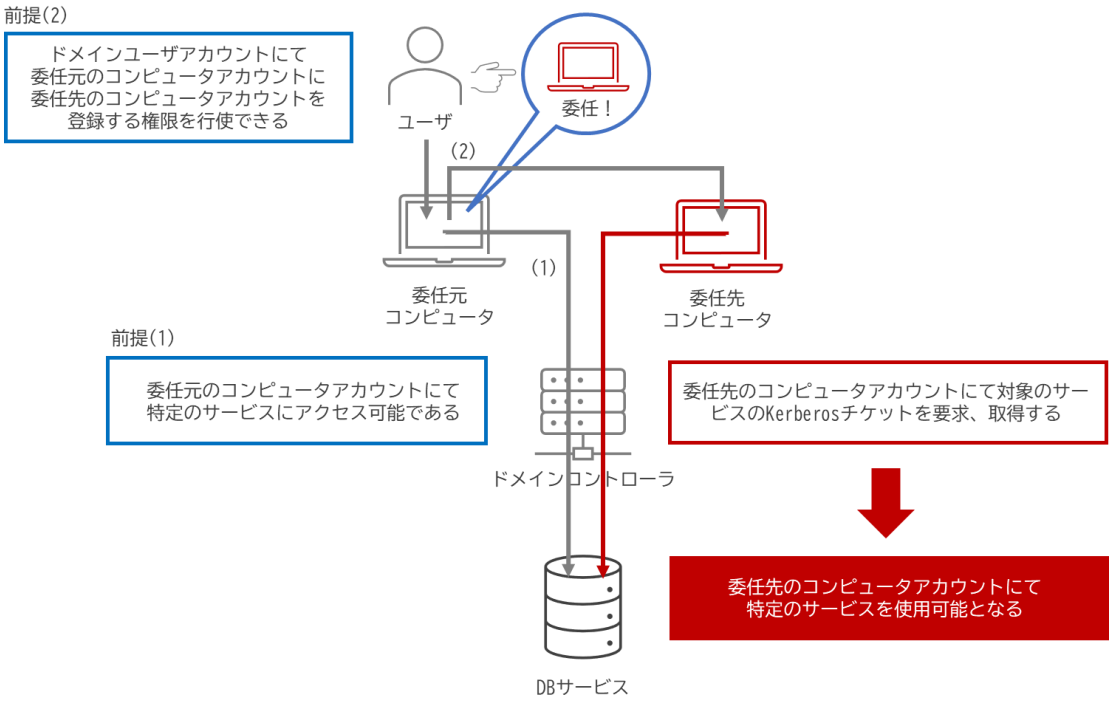


図 7　制約付き委任（RBCD）

RBCD 攻撃が成功可能となる条件

上記のリソースベースの制約付き委任を攻撃に悪用したものが RBCD 攻撃です。攻撃者視点では、以下の前提を満たせれば、委任元のコンピュータアカウントでアクセス可能なサービスに対して、委任先のコンピュータアカウントとしてアクセスすること、つまり横断的侵害が可能となります。

(1) 特定のサービスにアクセス可能である委任元のコンピュータアカウントを特定すること
(2) 委任元のコンピュータアカウントに委任先のコンピュータアカウントを委任先として登録する権限を持つドメインユーザアカウントの権限を奪取すること
(3) 委任先のコンピュータアカウントのパスワードのハッシュ値を入手すること

「条件(3)委任先のコンピュータアカウントのパスワードのハッシュ値を入手すること」は、委任先のコンピュータアカウントにて悪用したいサービスの Kerberos チケットを要求、取得するために必要な条件です。パスワードのハッシュ値を入手するためには、例えば攻撃者が侵入したシステム内部で、任意のコンピュータの管理者権限を奪取する方法があります。既存のコンピュータの管理者権限を奪取できれば、攻撃者はそのコンピュータを乗っ取って悪用したいサービスの Kerberos チケットを要求、取得し、サービスにアクセスできます。言い換えれば、委任元のコンピュータアカウントの権限でサービスにアクセスする横断的侵害が成立します。

コンピュータアカウントの新規作成によるパスワードのハッシュ値の入手

任意のコンピュータの管理者権限を奪取する方法以外で、パスワードのハッシュ値を入手する方法として挙げられるのが、ドメインユーザアカウントの権限を用いて新規にコンピュータアカウントを作成する方法です。

上記の前提(1)または前提(2)を満たしている状態では、少なくとも攻撃者は侵入したシステム内部ですでに何らかのドメインユーザアカウントを行使可能である状況が想定されます。このドメインユーザアカウントに新規のコンピュータアカウントを作成する権限が与えられている場合、攻撃者は侵入したシステム内部でコンピュータアカウントを新しく作成できます。自身で作成したコンピュータアカウントは自由に悪用できるため、任意のコンピュータの管理者権限を奪取してパスワードのハッシュ値を入手する工程が不要になります。

ドメインユーザアカウントによる新規のコンピュータアカウントの作成可否および作成可能な数は、Active Directory の機能で設定が可能です。デフォルトでは「10（＝10 アカウントまで作成可能）」が設定されており、ペネトレーションテストを実施した多くの組織においてデフォルト設定のまま運用されている状況が見受けられました。

つまり攻撃者視点では、行使できるドメインユーザアカウントがコンピュータアカウントを新規に作成する権限を持っている場合は、(1)委任元のコンピュータアカウントを特定し、(2)委任元のコンピュータアカウントに委任先のコンピュータアカウントを登録できるドメインユーザアカウントの権限を奪取すれば、攻撃者自身が作成したコンピュータアカウントを委任先として登録することで、そのコンピュータアカウントで悪用したいサービスの Kerberos チケットを要求、取得し、サービスにアクセスできるようになります。

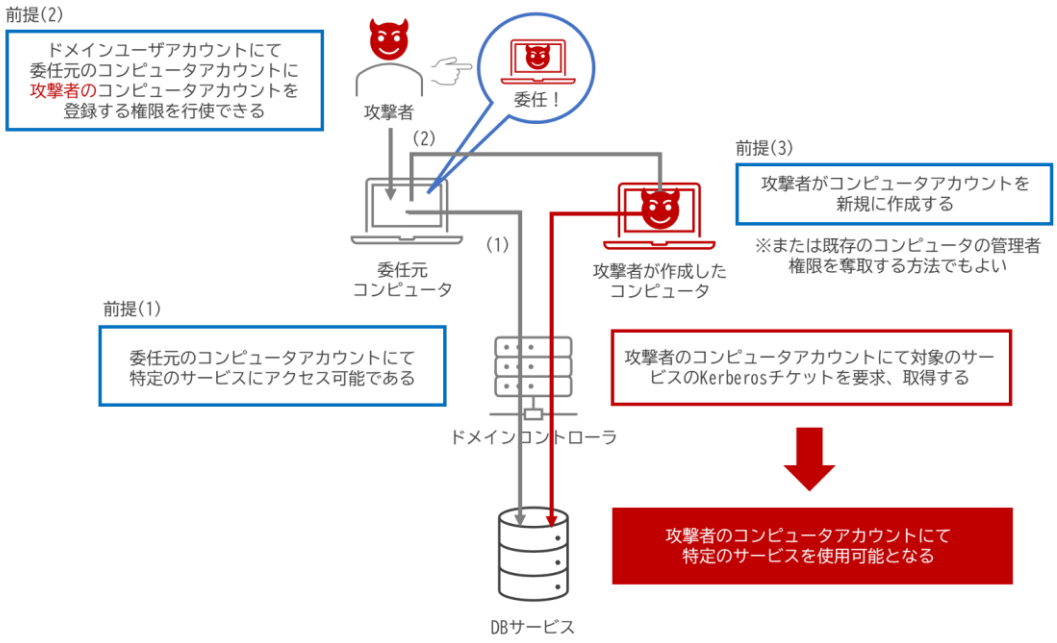


図 8　RBCD 攻撃による横断的侵害

ユーザアカウント権限の適切な運用が肝要

RBCD 攻撃では、ドメインユーザアカウントにおける以下の2つの権限を悪用します。そのため、これらの権限について適切な運用が行われることが肝要です。

(1) 委任元のコンピュータアカウントに委任先のコンピュータアカウントの登録が可能な権限
任意のコンピュータアカウントに対して、委任先のコンピュータアカウントの登録が可能であるドメインユーザアカウントを調査し、委任先の登録について適切な権限設定がされているか確認します。コンピュータアカウントにおいて、本来権限の必要ない一般権限のドメインアカウントに委任先の登録が可能な権限が付与されているなど、意図していない権限設定になっている場合は最小権限の原則にのっとり、権限を削除することを推奨します。

(2) コンピュータアカウント作成の権限
業務要件にもよりますが、可能であれば一般権限のドメインアカウントでは、コンピュータアカウントの作成ができないように制限することが望ましいです。一般権限のドメインアカウントでのコンピュータアカウントの作成を制限する場合、新規にコンピュータアカウントを作成する際には、システム管理者にて専用のアカウントを用いて作成する運用が想定されます。

参考（RBCD 攻撃および対策に関する詳細情報）：
ラック・セキュリティごった煮ブログ「Active Directory に対する RBCD 攻撃の対策の話」
https://devblog.lac.co.jp/entry/20240117

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： 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、定期的に棚卸しを行うことを推奨します。

- Active Directory のパスワードポリシーの強化： ドメインアカウントについて、グループポリシーの「最低限必要なパスワードの長さ」および「複雑さの要件を満たす必要があるパスワード」の設定を強化した上で、脆弱なパスワードを使用しているアカウントはパスワードを複雑性が高いものに変更してください。

- 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。

- 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。

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/B2MRNVF

【memo】

【memo】

【memo】

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
sales@lac.co.jp