LAC SECURITY INSIGHT

第 17 号

2026 夏

特集：OAST が捉える脆弱性のサイン
～ランダムなサブドメインに見える通信の正体～

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 8 月
株式会社ラック

LAC SECURITY INSIGHT

第 17 号／2026 夏

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4月～6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 30%、サーバの不正侵入による被害の相談が 29%であり、両者で全体の59%を占めています。この割合は、前四半期（2026年1月から3月）62%、前年同期（2025 年 4 月から 6 月）66%と比較して、やや減少しています。

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 15%を占めています。前四半期（11%）および前年同期（15%）とほぼ同水準で推移しており、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。当該期間では、SSL-VPN 機器の脆弱性を悪用した侵入は減少していましたが、パスワードのみの単一認証やテストアカウントの放置などにより、正規アカウントが悪用された事例が多く確認されており、攻撃者グループの侵入方法の変化、多様化が伺えます。

侵入後の被害としては、ファイルサーバや共有フォルダの暗号化に加え、ESXi などの仮想化基盤が暗号化される事案も複数確認されました。仮想化基盤上に Active Directory、ファイルサーバやバックアップサーバが集約されている場合、基盤側の侵害・暗号化により複数システムが同時に利用不能となり、調査・復旧の難易度が高まるため、対策の内容や優先度の見直しを推奨します。

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 15%を占めました。前四半期（21%）と比較すると減少したものの、前年同期（11%）を上回っており、ID 不正利用による被害は引き続き主要な相談類型の一つとなっています。

当該期間では、クラウドサービスの認証情報が不正利用される事例が複数確認されています。ログイン時に多要素認証を適用している場合でも、API キーやサービスアカウントなど、通常の対話型ログインとは異なる認証情報は多要素認証の対象外となる場合があります。これらの認証情報が適切に管理・監視されていない場合、不正アクセスや不正操作につながる可能性があるため、発行済み認証情報の棚卸し、権限の見直し、利用状況の監視を継続的に行うことが重要です。

当該期間では、「その他」に分類される相談が 28%となり、前四半期（22%）および前年同期（15%）から増加しました。要因としては、サポート詐欺の被害相談の増加が挙げられます。サポート

詐欺は、業種や組織規模を問わず幅広い組織から相談が寄せられており、遠隔操作ツールの導入や不正送金などの金銭被害に発展する事案も確認されています。

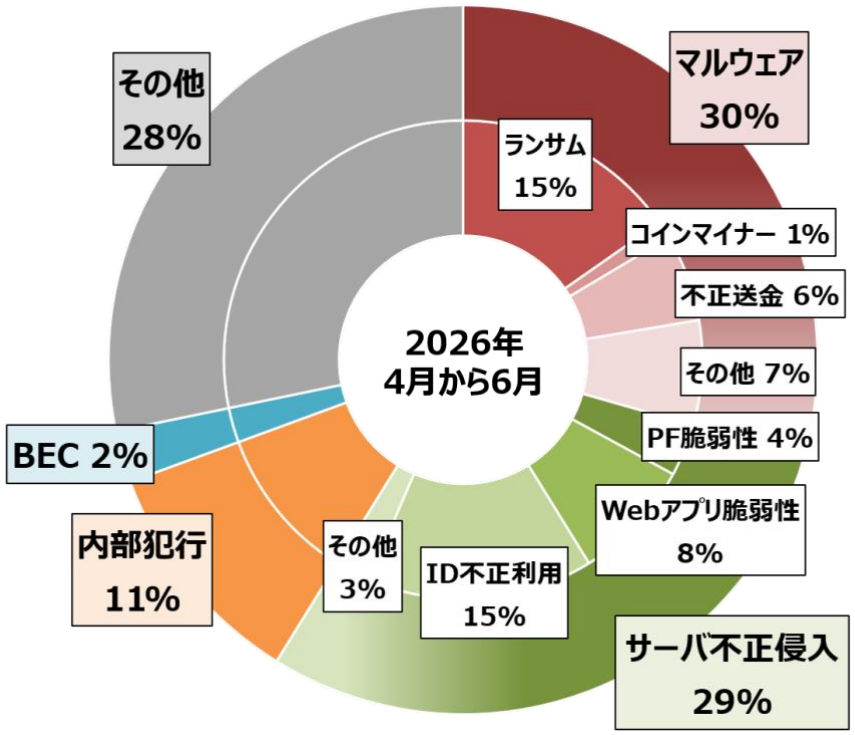

図 1 2026 年 4 月から 6 月の出動インシデントの内訳

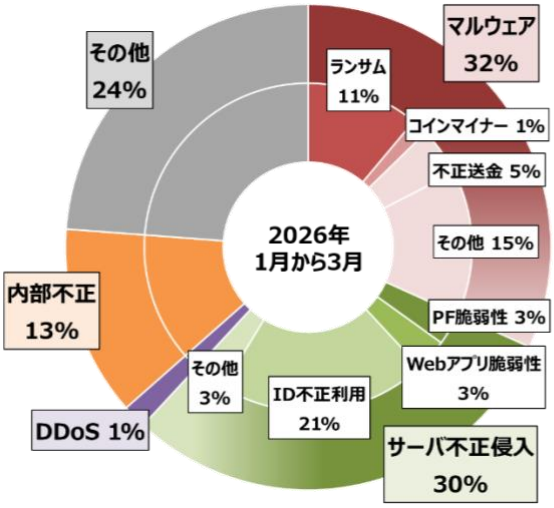

図 2 前四半期（2026 年 1 月から 3 月）

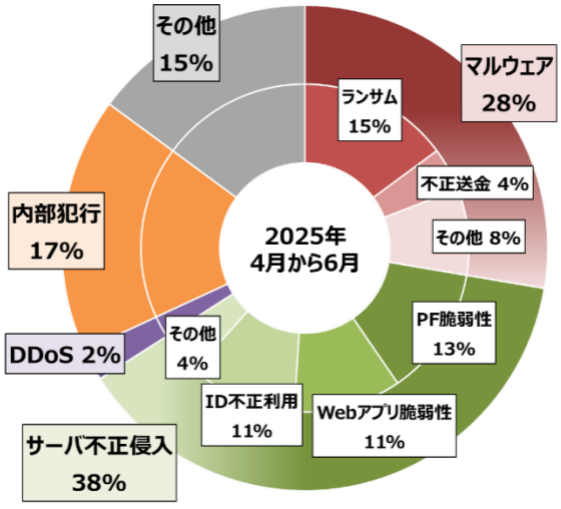

図 3 前年同期（2025 年 4 月から 6 月）

下表は、当該期間（2026 年 4 月～6 月）、前四半期（2026 年 1 月～3 月）および前年同期（2025 年 4 月～6 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 33%となり、前四半期（25%）および前年同期（30%）から増加しており、引き続き高い割合を占めています。また、製造業も 21%となり、前四半期（17%）および前年同期（13%）から増加しています。また、当該期間では「サービス業（他に分類されないもの）」が上位 5 業種に含まれました。ただし、当該期間は上位 2 業種への相談が比較的集中していましたが、確認した相談内容からは、特定の業種を狙った事象は確認されませんでした。その他にも多種多様な業種の組織から相談が寄せられており、幅広い業種で被害が発生している傾向に変化はありません。

順位	当該期間（2026 年 4 月から 6 月）		前四半期（2026 年 1 月から 3 月）		前年同期（2025 年 4 月から 6 月）	
1	情報通信業	33%	情報通信業	25%	情報通信業	30%
2	製造業	21%	製造業	17%	金融業，保険業	17%
3	卸売業，小売業	7%	卸売業，小売業	11%	製造業	13%
4	サービス業（他に分類されないもの）	7%	金融業，保険業	11%	卸売業，小売業	13%
5	学術研究，専門・技術サービス業	7%	学術研究，専門・技術サービス業	8%	学術研究，専門・技術サービス業	9%

表 1 上位 5 業種の相談件数割合

【ランサムウェアによる仮想化基盤への被害】

当該期間のランサムウェア被害では、個別の端末やファイルサーバだけでなく、ESXi などの仮想化基盤が影響を受ける事案が複数確認されています。仮想化基盤上には、Active Directory、ファイルサーバ、業務システムなど、組織の業務継続に不可欠な複数のサーバが集約されている場合があります。そのため、仮想化基盤が侵害・暗号化されると、単一のサーバの被害にとどまらず、複数の仮想サーバが同時に利用不能となり、業務への影響が広範囲に及ぶ可能性があります。

また、仮想サーバのディスクイメージが暗号化された場合、当該サーバ上で攻撃者が行った操作を確認することも困難になります。通常、侵害調査では OS 上のイベントログ、認証ログ、プロセス実行履歴、ファイル操作履歴などを確認します。しかし、仮想マシンを構成する仮想ディスクごと暗号化されていると、これらのログや設定ファイルを取得できず、侵害経路、被害範囲、情報漏えいの有無の判断が困難になります。

さらに、バックアップサーバをバックアップ対象と同一の仮想化基盤で構築している運用も散見されます。この構成では、ランサムウェア被害時にバックアップサーバも同時に影響を受け、本来復旧手段として機能すべきバックアップが利用できなくなる可能性があります。

ランサムウェアの標的として仮想化基盤が狙われている可能性を踏まえ、基盤側のセキュリティ対策を強化する必要があります。具体的な対策は以下の通りです。

- 管理画面へのアクセス制限（インターネットおよび不要なネットワークからの直接アクセス遮断）
- 管理者アカウントの棚卸しと多要素認証の適用
- 不要な SSH や管理サービスの停止
- ハイパーバイザおよび管理コンポーネントの継続的な更新
- 仮想化基盤側のログ取得と外部保管

加えてバックアップは、被害環境と同一の認証基盤や同一の仮想化基盤に依存しない形で保管し、オフライン保管やイミュータブルストレージの活用、定期的な復元試験を通じて、被害時にも確実かつ迅速に復旧できる状態を維持することが求められます。

【サポート詐欺被害の企業環境への影響拡大】

当該期間では、サポート詐欺や偽警告を契機とした遠隔操作被害に関する相談が引き続き複数寄せられています。サポート詐欺とは、Web サイト閲覧中にウイルス感染やシステム異常を装った警告画面を表示し、記載された電話番号に連絡させ、遠隔操作ツールの導入を促すとともに、サポート費用などの名目で金銭を要求する攻撃手法です。

従来のサポート詐欺では、金銭窃取を行うためにウイルス駆除費用や長期的なセキュリティサポート費用として電子マネーでの送金や振り込みを求める事例が多くありましたが、近年のサポート詐欺では、単純な費用請求にとどまらない攻撃手法がとられていることを観測しています。当該期間に確認した複数の事例では、攻撃者から以下のような質問を受けるケースがありました。

- 警告画面が出ている PC は私物 PC か社用 PC か
- 会社の銀行口座を扱っている PC が存在しないか
- 会社用のアカウントで通販サイトにログインすることはあるか

また、これらの事案では、PC に限らずスマートフォンにも遠隔操作アプリを導入するように攻撃者が促してくることを確認しています。これらの事例は、サポート詐欺の攻撃者グループの狙いが、個人からの金銭窃取にとどまらず、企業の資産や情報に接点を持つ端末・アカウントへと変化している可能性を示しています。

企業・団体の環境でサポート詐欺が発生した場合、被害は利用者個人の金銭被害にとどまらず、組織の情報漏えいリスクとして評価すべき事案に発展します。遠隔操作された端末に業務データや個人情報が保存されていた場合や、クラウド同期フォルダ、メール、業務システム等へアクセス可能な状態であった場合には、攻撃者が端末を経由して組織の情報へアクセスできた可能性があります。

サポート詐欺の注意喚起が盛んに行われている中でも被害がなくならないことから、対策としては、利用者への注意喚起だけでなく、利用者個人の判断に依存しない体制や仕組みづくりが重要です。被害を最小限にするために、偽警告が表示された場合の社内相談先を明確にすること、業務端末での遠隔操作ツールの利用を制御すること、ブラウザに保存された認証情報やクラウド同期フォルダの利用状況を管理すること、業務データの私用端末への持ち出しを適切に管理することを検討ください。

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 4 月から 6 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 247 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 4 件（1.6%）、ネットワーク内部からの通信によるインシデントが 243 件（98.4%）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

WordPress プラグインの脆弱性や ProFTPD の脆弱性の悪用、不審なファイルアップロードの試みによるインシデントが発生しました。そのほかには前四半期に引き続き、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。図 4 に 2026 年 4 月から 6 月の重要インシデントの内訳を示します。

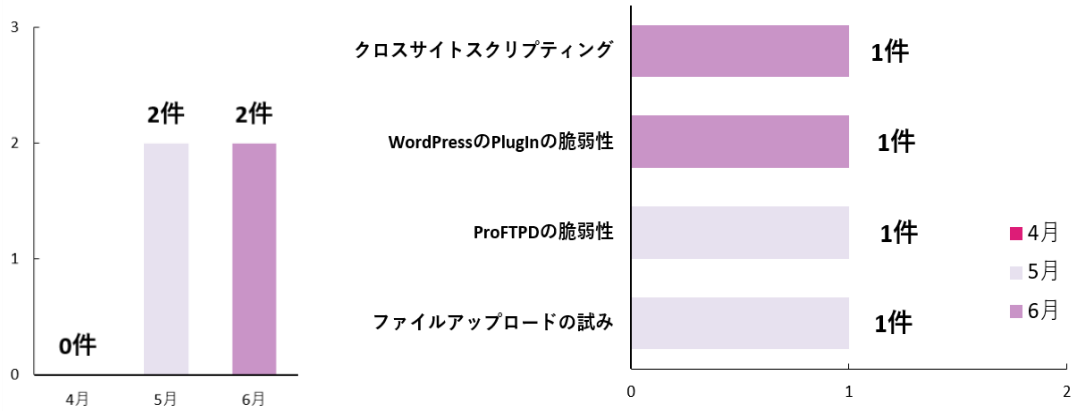

図 4 [外部から] 2026 年 4 月から 6 月の重要インシデントの内訳（月別・種類別）

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く発生しました。発生したマルウェア感染インシデントでは、macOS を標的とする情報窃取マルウェアの一種である AMOS Stealer や、ブラウザに保存された機微情報の窃取を行う Arechclient2 に感染したことに起因する通信を検知しました。マルウェア以外に分類している重要インシデントについては、監視対象ホストから外部に対する不審な通信や不審なドメイン名の名前解決の通信を検知したことによるインシデントが発生しました。図 5 に 2026 年 4 月から 6 月の重要インシデントの内訳を示します。

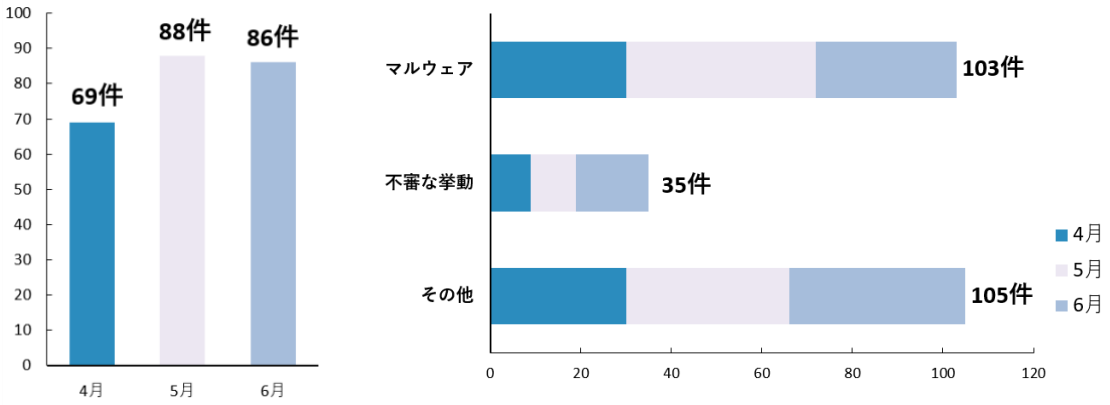

図 5 [内部から] 2026 年 4 月から 6 月の重要インシデントの内訳（月別・種類別）

EDR 製品の検知による重要インシデントは 34 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 4 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 30 件でした。これらのインシデントのうち特徴的なものは、USB メモリを介したマルウェア感染です。USB メモリは利便性が高い一方で、感染の媒体となる恐れがあります。対策としては、信頼できない USB メモリを使用しないことや、使用前にウイルススキャンを実施することなどが挙げられます。そのほかにも、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インシデントも発生しました。図 6 にＮＷ監視（IPS/IDS 他）、端末監視それぞれで検知したインシデント種類別の内訳を示します。

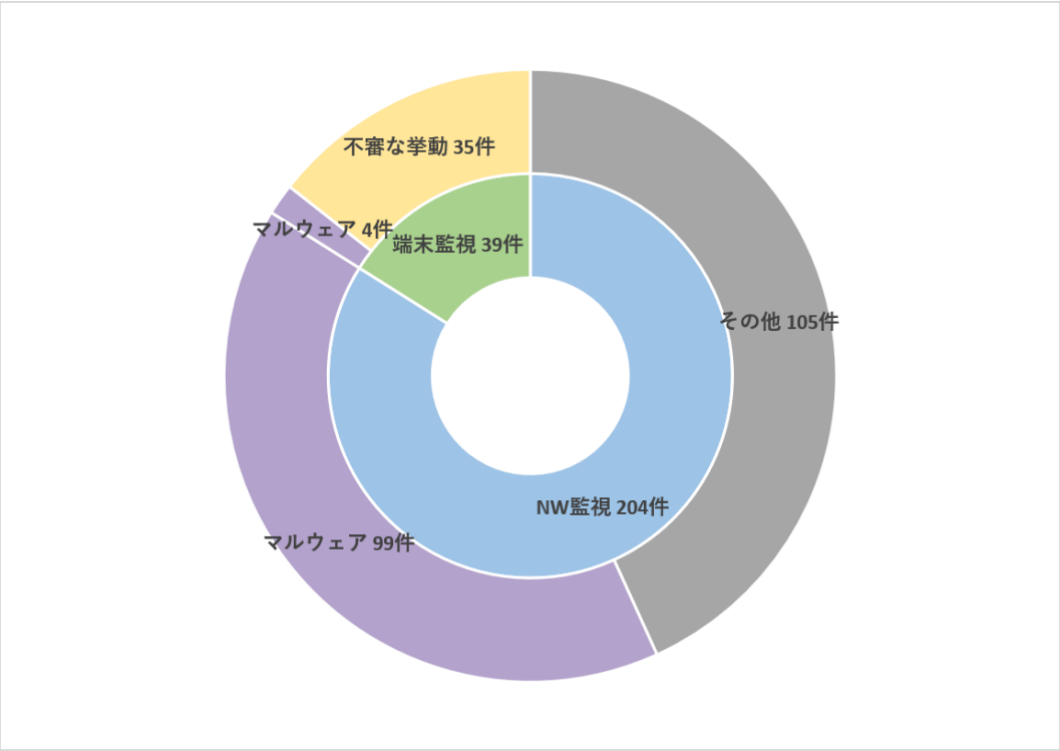

図 6 [内部から] 監視形態ごとのインシデント種類別内訳

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
Joomla!の脆弱性（CVE-2026-48908）を狙った攻撃	脆弱性を悪用し、不審な zip ファイルのアップロードを試みる通信を多数検知しました。	6 月 21 日～
NGINX の脆弱性（CVE-2026-42945）を狙った攻撃	脆弱性を悪用し、特殊文字を含む GET リクエストを多数検知しました。	5 月 14 日～
157.245.109.139（インド）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。	5 月 4 日～ 5 月 6 日
TFTP サーバへの設定ファイルを参照する攻撃	短期間に集中して特定の送信元から TFTP サーバへの設定ファイル参照を多数検知しました。	6 月 6 日

特集：OAST が捉える脆弱性のサイン

～ランダムなサブドメインに見える通信の正体～

攻撃者は、稼働しているサービスに存在する脆弱性を様々な手法で探索しており、JSOC は日々その変化を観測しています。その中でも JSOC 全体の検知傾向として、オープンソースの脆弱性診断ツールなどを用いた脆弱性スキャン通信を多数確認しています。また、脆弱性が悪用された可能性のある通信を検知したことを契機として、複数のお客様において重要インシデントとして対応した事例も発生しています。本特集においては、日々の観測の中で見えてきた傾向として、近年攻撃者にも積極的に採用されている「OAST（Out-of-Band Application Security Testing）」と呼ばれる脆弱性検査手法について、検知傾向とともにご紹介します。

OAST による脆弱性の検査の仕組み

OAST（Out-of-Band Application Security Testing）は、検査対象に外部通信を発生させるテスト用入力を与え、その外部通信の有無を観測することで、脆弱性の存在を確認する手法です。図 7 に OAST による検査フローを示します。

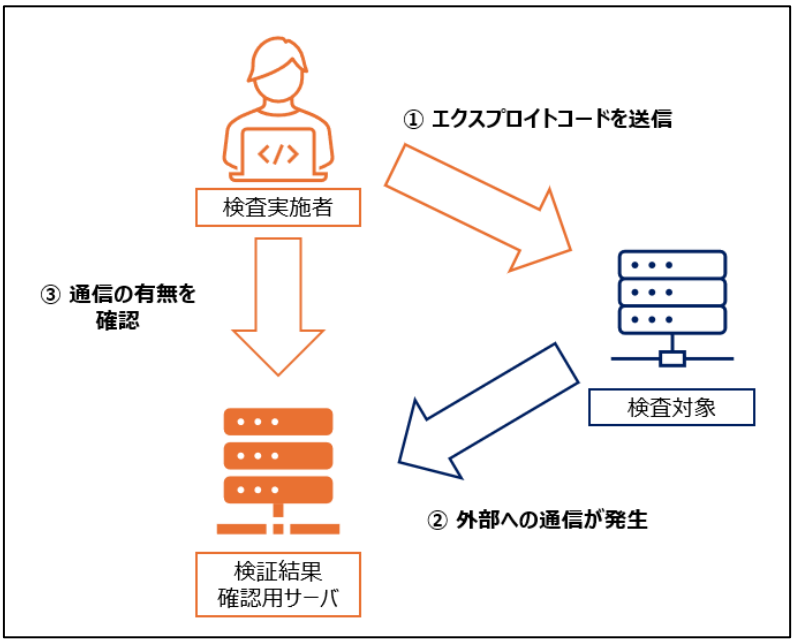

図 7 OAST の検査フロー

OAST では、初めに検査実施者が外部通信を受け取ることができる検査結果確認用の外部サーバを準備します。そのうえで、脆弱性を利用するためのエクスプロイトコードの中に、外部サーバへ通信を発生させるためのペイロードを含めて、検査対象に送信します（図 7 ①）。検査対象に脆弱性が存在する場合、その処理の中でペイロードが実行され、外部への通信が発生します（図 7 ②）。検査実施者は、この通信の有無を確認することで、脆弱性の有無を判定します（図 7 ③）。

ここでいうエクスプロイトコードとは、検査対象の脆弱性を利用して特定の動作を引き起こすための入力や処理内容を指します。ペイロードとは、その中に含まれる実際に実行させたい内容であり、OAST では外部サーバへの通信を発生させる処理がこれにあたります。

このような OAST による脆弱性検査は、検査対象の応答に変化が現れない脆弱性の調査に有効です。例えば、OS コマンドインジェクションやサーバーサイド・リクエスト・フォージェリなどの脆弱性は、与えた入力が内部で処理され、結果が検査実施者に見えないことがあります。このような脆弱性に対しても、OAST を利用して外部通信を発生させる処理を実行させ、その通信発生の有無を検査結果確認用のサーバにおいて確認することで脆弱性の検査が可能です。

図 8 に実際の OAST による検査例を示します。

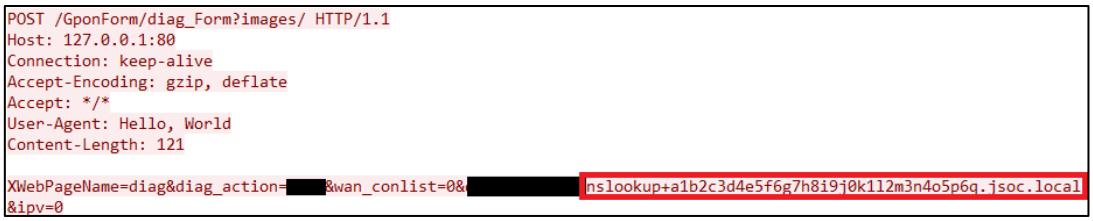

図 8 OAST による検査例（エクスプロイトコードの送信）

図 8 では、「a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6q.jsoc.local の名前解決を行う」というペイロードを含んだエクスプロイトコードを送信しています。その後、検査対象が脆弱かどうかを、名前解決通信のログの有無で判断します。

図 9 に、検査対象に脆弱性が存在する場合の名前解決通信ログを示します。

図 9 OAST による検査例（DNS ログによる検査結果の確認）

このようなフローによって、検査対象のサービスからの直接の応答に依存せずに検査を実施できます。また、OAST は効率よく様々なサービスの脆弱性検査を行えることも利点です。OAST を利用した多くのテスト手法においては、検査したい脆弱性ごとに識別子となるサブドメインを与えることで、効率的に検査結果を管理することが可能です。脆弱性診断ツールにおいても有償・無償を問わず OAST をサポートしているものが多く、ツールによっては検査用のインフラやコンソールを提供しているものもあります。一例を図 10 に示します。

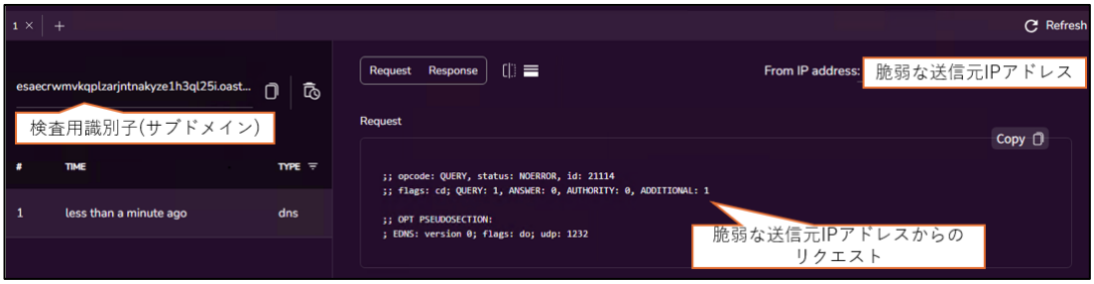

図 10 OAST をサポートするツールの利用例

OAST を用いた攻撃の事例

OAST は脆弱性検査手法であり、その手法を簡単に利用するためのツールも多く公開されていますが、その利便性から攻撃者にも悪用されています。JSOC においても 2022 年頃から悪用を観測し始め、現在でも多数の脆弱性を狙った攻撃において、OAST を用いる傾向がみられています。

図 11 および図 12 に、OAST を用いた攻撃通信例を示します。

図 11 React Server Component の脆弱性（CVE-2025-55182）を狙う攻撃通信例

図 12 ProFTPD の脆弱性（CVE-2026-42167）を狙う攻撃通信例

攻撃者が発生させた図 11 や図 12 のような攻撃通信が脆弱なサービスに到達することで、脆弱なサービスから d6gm...pjuo[.]oast[.]site や d15...877[.]oast[.]pro に関する外部への通信が発生します。攻撃者は、脆弱なサービスから発生させた通信が外部サーバに到達したかどうかを確認することで、脆弱なサービスを認知し、更なる攻撃への足掛かりに利用します。

以下に JSOC で観測している OAST に利用されるドメインの例を記載します。

- XXXX..XXXX.oast[.]pro
- XXXX..XXXX.oast[.]me
- XXXX..XXXX.oast[.]fun
- XXXX..XXXX.oast[.]live
- XXXX..XXXX.oast[.]site
- XXXX..XXXX.oast[.]online
- XXXX..XXXX.dnslog[.]cn
- XXXX..XXXX.i-sh.detectors-testing[.]com
- XXXX..XXXX.interactsh[.]com

補足：OAST に類似した誤検知の例

OAST が疑われる通信は、JSOC による観測より、以下のようなシナリオで発生する場合もあります。発生原因について調査を行う際は事例の 1 つとして参考にしていただければ幸いです。

- Access ログの閲覧中に、ログに含まれていたドメインを誤ってクリックしてしまうケース
- チャットツールやエディタがドメインを解釈し、名前解決通信を発生させてしまうケース
- 外部から内部への攻撃通信に含まれるドメイン名などについて、自動で名前解決を行うネットワーク機器が経路上に存在するケース

ネットワーク内部から OAST を疑う通信を検知した時は

OAST を疑うような通信を内部ネットワークから検知した場合でも、あくまで外部からのテスト通信が内部のサービスに到達したことと、対応する外部通信をサービスから発生させることができる可能性があることを示すのみであり、直ちに重大な侵害が発生していることを断定するものではありません。しかしながら、このような通信が発生した際には、ネットワーク内に残存した何らかの脆弱性が利用された可能性を考慮して、発生原因を調査することが必要です。

ネットワーク内部から発生した OAST 通信の宛先ドメイン等をもとに、検知した送信元ホストで稼働しているサービスのログを調査し、OAST 通信の発生源となった外部からの攻撃通信の有無を調査いただくことを推奨いたします。

なお、発生した OAST 通信の送信元ホストが DNS サーバである等、内部からの通信を中継する機能を有している場合においては、そのログをもとに OAST 通信の発生元を確認した上で後続の調査を実施することが重要です。

【memo】

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/WMQBTKQ

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/