サイバーセキュリティレポート

2026.06

NTT セキュリティ・ジャパン株式会社
プロフェッショナルサービス部 OSINT モニタリングチーム

目次

【1 ページサマリー】

当レポートでは 2026 年 6 月中に生じた様々な情報セキュリティに関する事件、事象、またそれらを取り巻く環境の変化の中から特に重要と考えられるトピック 3 点を選び、まとめたものである。各トピックの要旨は以下のとおりである。

第 1 章『FortiBleed の教訓: 認証への大規模攻撃』

- 2026 年 6 月、Fortinet 製品に関連する大規模な認証情報漏洩事案（通称「FortiBleed」）が発覚した。その影響は世界 194 か国に及び、公的機関も注意喚起を発出する深刻なインシデントとなっている。
- 攻撃手法は新規脆弱性の悪用ではなく、過去のインシデントやインフォスティーラー由来の既知の認証情報を悪用し、自動化ツールを用いて 24 時間体制で認証試行を繰り返すというものであった。
- 企業は、認証情報管理や多要素認証（MFA）の導入をはじめとする基本的なセキュリティ対策が適切に実施されているかを継続的に点検・改善する必要がある。

第 2 章『オフィスへの来訪者: オンラインで終わらないサイバー攻撃』

- ランサムウェアを使わず、IT サポート担当者を装った高度なソーシャルエンジニアリングによって機密データを窃取し、その公開を盾に金銭を要求する攻撃者グループ「UNC3753」の活動が報告された。
- 遠隔からの侵入に失敗した場合は、攻撃者が実際にオフィスを訪問し、端末に直接アクセスした上で、USB メモリ等の外部記憶媒体を使用してデータを持ち出す手口も確認されており、FBI も警告を発している。
- 本事例はサイバー攻撃がオンライン上だけで完結しないことを示している。技術的対策のみでは十分に防御できない状況が生じつつある点に留意し、組織においてはセキュリティ対策の包括的な見直しが求められる。

第 3 章『BOD 26-04 が示すリスクベース脆弱性対応への転換』

- CISA は 6 月 10 日に BOD 26-04 を発令し、脆弱性対応について、資産の公開状況や既知の悪用状況、攻撃の自動化可能性、技術的影響という 4 つの要素を踏まえリスクを評価し、その結果に応じて定められた期限内に是正措置を講じることを義務付けた。
- 近年は脆弱性の増加に加え、AI の活用による攻撃の自動化と高速化が進み、脆弱性公開から攻撃までの時間も急速に短縮している。そのため、限られたリソースの中で、どの脆弱性へ優先的に対応すべきかを判断することが運用上の課題となっている。
- BOD 26-04 は、従来の網羅的な対応から、リスクに応じて対応内容や対応期限を定める運用へと転換し、限られたリソースを効率的に活用するためのリスクベースの意思決定を実現することを目的としている。

1. FortiBleed の教訓: 認証への大規模攻撃

1.1. 概要

2026 年 6 月、FortiGate をはじめとする、Fortinet 社製品に関連した認証情報が大規模に漏洩していることが明らかになった。本事案は「FortiBleed」と命名され、影響は世界中に及んでいる。米国の CISA(サイバーセキュリティ・インフラストラクチャセキュリティ庁)や日本の JPCERT コーディネーションセンター(JPCERT/CC)といった公的機関も注意喚起を発出しており、現在も侵害は進行中とみられる[1, 2]。

1.2. FortiGate とは

FortiGate は、米 Fortinet 社が提供するネットワークファイアウォール製品であり、世界市場において 50%以上のシェアを占める[3]。従来のファイアウォール機能や VPN 機能に加え、アンチウイルス、Web フィルタリング、侵入防御システム（IPS）など複数のセキュリティ機能を統合した UTM（統合脅威管理）製品として[4]広く利用されている。

1.3. FortiBleed について

【事案の概要】

本事案が明るみに出る契機となったのは、セキュリティ研究者の Volodymyr "Bob" Diachenko 氏が、インターネット上で公開状態となっていたサーバーを発見し、そこに保存されていた、大量の Fortinet 機器関連の認証情報を確認したことであった。6 月 13 日に、同氏がこの事を自身の SNS を通じて報告すると、複数のセキュリティ企業も相次いで調査結果を公表した。

今回発見された認証情報は、攻撃者自身が実際に検証したものとみられ、その中に有効なユーザー名とパスワードが含まれていることを、セキュリティ関係者たちも確認している。

なお、「FortiBleed」は脆弱性の名称ではなく、Fortinet 製品を標的として大量の認証情報を収集・検証し、不正アクセスを試みる大規模な攻撃キャンペーンを指すものであり、サイバーセキュリティ企業の SOCRadar が名付けた。

---

[1] 出典: JPCERT/CC『Fortinet 製品に関連する認証情報の漏えいに関する注意喚起』
https://www.jpcert.or.jp/at/2026/at260019.html

[2] 出典: CISA『CISA Urges Hardening Fortinet Devices After Reports of Credential Exposure』
https://www.cisa.gov/news-events/alerts/2026/06/18/cisa-urges-hardening-fortinet-devices-after-reports-credential-exposure

[3] 出典: Fortinet『次世代ファイアウォール（NGFW）』
https://www.fortinet.com/jp/products/next-generation-firewall

[4] 出典: 株式会社 日立ソリューションズ『FortiGate』
https://www.hitachi-solutions.co.jp/fortinet/function/fortigate/

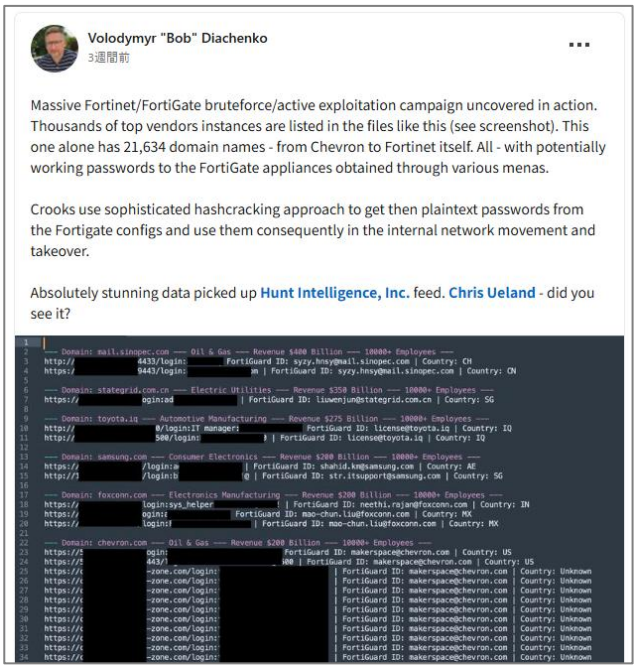

図 1 Volodymyr "Bob" Diachenko 氏による投稿(抜粋)[5]

【攻撃者】

SOCRadar は、FortiBleed で使用されているツールやインフラ構成、標的の選定などに見られる特徴から、攻撃者がロシア語圏のグループである可能性が高いと分析している[6]。また、FortiBleed の攻撃者とランサムウェアグループ「INC」および「Lynx」（Lynx は INC から派生した可能性あり）の関連性も指摘している。この根拠として同社は、FortiBleed 関連インフラの管理者が INC と Lynx 両方のランサムウェア身代金交渉サイトにアクセスして被害者とやりとりを行っていたことなどを挙げている[7]。INC／Lynx は 2023 年頃から、北米および欧州を中心に、医療、教育、政府、製造業などの組織を標的として活動している。

今回、公開状態となっていた FortiBleed 関連サーバーからは、防衛産業に属するとみられる VPN 認証情報も発見されていることから、攻撃者の目的が金銭的利益にとどまらない可能性も指摘されている。

【被害規模】

侵害された機器は 86,644 台にのぼり、8 万件以上の IP アドレスおよび 2 万件以上のドメインが特定されている。影響は 194 か国に及んでおり、特にインドと米国で被害の約 3 分の 1 を占めている。また、被害組織には売上高 10 億ドルを超える大企業や、多数の政府機関も含まれる。

[5] 出典: LinkedIn『Volodymyr "Bob" Diachenko : Fortinet FortiGate Bruteforce Campaign Exposed』 https://www.linkedin.com/posts/vdyachenko_massive-fortinetfortigate-bruteforceactive-activity-7471222472193830913-YBDi

[6] 出典: SOCRadar『FortiBleed Breach How 80,000+ Corporate Firewalls Were Quietly Compromised』 https://socradar.io/blog/fortibleed-fortinet-firewalls-compromised/

[7] 出典: SOCRadar『Is FortiBleed Linked to INC and Lynx Ransomware? All You Need to Know』 https://socradar.io/blog/fortibleed-inc-lynx-ransomware-link/

【攻撃手法】

攻撃は以下のような流れで行われた。

Step1: 認証情報の収集

攻撃者は、過去の Fortinet 関連インシデント(認証回避の脆弱性等により発生)で流出したり、インフォスティーラー（情報窃取型マルウェア）によって窃取されたりした認証情報を収集した。

Step2: 自動化された認証試行キャンペーン

攻撃者は、FortiGate 機器へのログインを自動化し、多数の送信元から 24 時間体制で認証情報の検証を行った。これにより、約 32 万台の FortiGate に対し、11 億回を超えるログインを試したとされている[8]。

SOCRadar 社の調査によると、多くの被害組織では当該機器のデフォルトのアカウント名や初期パスワードが変更されていなかった。また、Fortinet 社は、多要素認証（MFA）が導入されていない機器が攻撃対象となったと推測している[9]。

一方で、本事案では非常に複雑なパスワードも多数漏洩していた(図 2)。たとえ強固なパスワードが使用されていたとしても、攻撃者が既知の認証情報を用いる場合、パスワードの複雑性のみでは十分な防御とはならない。自社の認証情報が漏洩していた場合に備えれば、MFA は不正ログイン対策として極めて重要である。

```
--- Domain: [redacted].com.ar --- Industrial Equipment --- Revenue $50 Million --- 201-500 Employees ---
https://[redacted]:8443/login:[redacted]:21151Amc951**- | FortiGuard ID: [redacted].com.ar | Country: AR
https://[redacted]:8443/login:[redacted]21151Amc951**- | FortiGuard ID: [redacted].com.ar | Country: AR
https://[redacted]:8443/login:[redacted]:21151Amc951**- | FortiGuard ID: [redacted]com.ar | Country: AR
https://[redacted]:8443/login:[redacted]:21151Amc951**- | FortiGuard ID: [redacted].com.ar | Country: AR
https://[redacted]:8443/login:[redacted]:21151Amc951**- | FortiGuard ID: [redacted].com.ar | Country: AR
https://[redacted]:8443/login:[redacted]:21151Amc951**- | FortiGuard ID: [redacted].com.ar | Country: AR
https://[redacted]:8443/login:[redacted]:21151Amc951**- | FortiGuard ID: [redacted].com.ar | Country: AR
https://[redacted]:8443/login:[redacted]:21151Amc951**- | FortiGuard ID: [redacted].com.ar | Country: AR
https://[redacted]:8443/login:[redacted]:wAkbzodKo7L6D4f7ABKBJFNXDCgBJ@#a | FortiGuard ID: [redacted].com.ar | Country: AR
https://[redacted]:8443/login:[redacted]:wAkbzodKo7L6D4f7ABKBJFNXDCgBJ@#a | FortiGuard ID: [redacted].com.ar | Country: AR
https://[redacted]:8443/login:[redacted]:EnmoSuto#20 | FortiGuard ID: [redacted].com.ar | Country: AR
https://[redacted]:8443/login:[redacted]:wAkbzodKo7L6D4f7ABKBJFNXDCgBJ@#a | FortiGuard ID: [redacted].com.ar | Country: AR
```

図 2 侵害された認証情報の中に含まれていた複雑なパスワードの例 [8]

Step3: 暗号化されたパスワードの解析

アクセス成功後、攻撃者は Fortinet 機器の構成ファイルをエクスポートし、そこに含まれる暗号化されたパスワードを抽出した。この際、多くの機器で古い暗号化アルゴリズムが使われており、パスワードの解読に対して非常に脆弱な状態であったとされている[10]。Fortinet 社は 2025 年初頭に、より安全な暗号化アルゴリズムである PBKDF2 を導入したが、この方式はファームウェアを更新するだけでは有効とならず、管理者が再度ログインする必要があった。そのため、多くの機器で、攻撃者にとって解析が容易な古い形式のまま、パスワードが保存されていた。

---

[8] 出典: HudsonRock『FortiBleed: 75,000 Fortinet Firewalls Compromised: Global Enterprises Exposed – Claim Your Ethical Disclosure』
https://www.hudsonrock.com/blog/fortibleed-75000-fortinet-firewalls-compromised-global-enterprises-exposed-claim-your-ethical-disclosure

[9] 出典: Fortinet『Analysis of Reported Credential Compromise of FortiGate Devices』
https://www.fortinet.com/blog/psirt-blogs/analysis-of-reported-credential-compromise-of-fortigate-devices

[10] 出典: DoublePulsar『FortiBleed — 75k Fortinet firewalls have admin passwords cracked』
https://doublepulsar.com/fortibleed-75k-fortinet-firewalls-have-admin-passwords-cracked-60299faa65f8

Step4: パッシブ・ハーベスティング（受動的な認証情報収集）

攻撃者は侵害した FortiGate を単なる侵入経路として利用するだけでなく、同デバイスを経由する通信を傍受し、通信に含まれる認証情報を収集していた。

認証情報は傍受の時点では暗号化されているが、45 基の GPU クラスタ(多数の GPU サーバーを連携させて大量の計算を高速に実行する環境)を使用して解読していた。

1.4. まとめ

FortiBleed においては FortiGate が主な標的となったが、攻撃者は Sophos 製品[11]や Microsoft SQL Server (MSSQL)に対しても同様の攻撃を実行していることから、あらゆる公開システムが標的となり得るといえる。

本事案は、認証情報の管理や MFA の導入など、基本的なセキュリティ対策の重要性を改めて示した事例である。インターネットに公開しているシステムにおいては、ID・パスワードのみに依存した認証は突破されることを前提に、組織は、セキュリティ対策が適切に実施されているかを定期的に点検し、改善していくことが必要である。

[11] 出典: Sophos『Advisory: Fortinet “FortiBleed” Credential Exposure and Sophos VPN Bruteforcing Campaign』 https://www.sophos.com/en-us/security-advisories/fortinet-fortibleed-credential-exposure-and-sophos-vpn-bruteforcing-campaign

2. オフィスへの来訪者: オンラインで終わらないサイバー攻撃

2.1. 概要

6 月 6 日、Google の脅威インテリジェンス部門である Mandiant は、攻撃グループ「UNC3753」による、米国の法律事務所・金融機関・専門サービス企業を標的とした大規模なデータ窃取・恐喝キャンペーンを報告した[12]。本キャンペーンでは、電話やリモートツールを用いた侵入だけでなく、対面での接触により物理的に侵入を試みる事例も確認されている。

2.2. UNC3753 について

UNC3753 は 2022 年 3 月に活動を開始した金銭目的のグループであり [12]、ロシアを拠点とする可能性が指摘されている [13]。主な標的は米国の法律事務所等である。

同グループは「Silent Ransom Group (SRG)」とも呼ばれており [12]、この呼称は攻撃手法の特徴を端的に示している。活動当初は標的組織のファイル(データ)を暗号化するランサムウェアを使用していたが、現在はファイルを一切暗号化せず、システムを停止させることもない。機密データのみを静か(Silent)に窃取し、これらを自ら運営する暴露サイト上で公開すると脅して身代金の支払いを迫る手法へと移行している。活動開始から現在に至るまで逮捕者は出ておらず、サーバー等の攻撃インフラの摘発も行われていない [13]。

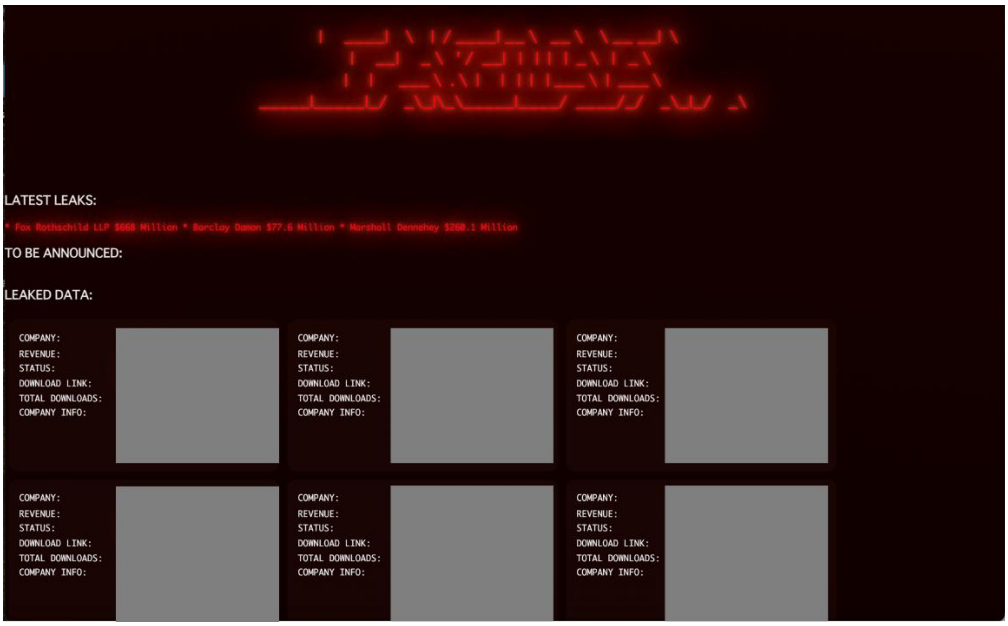

図 3 UNC3753 の暴露サイト

[12] 出典: Google Cloud『Seeking Counsel: Ongoing Targeted Campaign Against US Law Firms』
https://cloud.google.com/blog/topics/threat-intelligence/targeted-campaign-us-law-firms?hl=en

[13] 出典: Halcyon『THREAT ACTOR Silent』
https://www.halcyon.ai/threat-group/silent

2.3. 攻撃の全体像

活動開始からしばらくの間、当グループが用いていた手法は、「サブスクリプションの更新通知」を装ったメールを標的組織の従業員に送信し、メールに記載していた電話番号へ連絡させるという、比較的単純なものであった [12]。それが最近では電話やリモートツールを組み合わせた、より高度なソーシャルエンジニアリングへと発展している。

【遠隔からの攻撃手順】

- **STEP1: 偽のメールで警戒心を植え付ける**
  攻撃者はまず、請求書を装った無害なメールを送りつける [12]。このメールには悪意あるリンクや添付ファイルは含まれていない。目的は、身に覚えのない内容のメールを受信した従業員のセキュリティ上の懸念を高め、この後に仕掛ける偽の電話に対して疑いを抱かせないよう準備することである。
- **STEP2: IT サポートを装った電話(ビッシング: 電話で相手を騙し、システム操作や情報提供をさせる手口)**
  IT サポート担当者を騙る攻撃者が従業員(STEP1 で送付していたメールの受信者)に電話をかける。メールへの対応やデータ移行等における支援を口実にし、従業員の信頼を獲得したうえで、リモートアクセスや画面共有を可能とするツールをインストールするよう誘導する。Zoom や Microsoft Teams、Quick Assist といった、通常業務でも広く使われている正規のツールを悪用するため、従業員から疑念を抱かれにくい。同グループは英語を母国語とするスタッフによるコールセンターを組織的に運営しているとみられており [13]、言語的・地理的な距離を感じさせることなく標的組織の IT 担当者になりすましている。
- **STEP3: 機密データの探索と窃取**
  従業員の端末へのアクセスが確立されると、攻撃者は契約書・個人情報・財務記録・税務書類など、組織内の機密性の高いデータを探索・収集し、窃取する。ある事例では、標的となった従業員の OneDrive フォルダから 1.7 ギガバイトのデータが攻撃者の Google ドライブアカウントに送信された後、さらに仮想デスクトップ環境を経由して 14.4 ギガバイトもの追加データが窃取されるという被害が確認されている。
- **STEP4: 脅迫メールの送付**
  データ窃取の完了からわずか 30 分以内に、身代金獲得に向け、被害組織に対して恐喝メールを送付する。文中では、「3 日以内に連絡がなければ、従業員・取引先・顧客に直接通知し、暴露サイトでデータを公開する」と脅迫するだけでなく、規制当局から多額の罰金を科されたり、顧客から訴訟を起こされたりするリスクにも言及。さらには本件が組織の存続を危うくするとまで述べる、極めて攻撃的な内容である。

```
Subject: [Victim Name] has lost confidential data of their clients. Very Important!

Hello,

We have to inform you that we got access to the [Victim Name] corporation's database and took a very large dataset. We have been in your network for weeks in multiple systems , aiming for proprietary and confidential files, and were able to obtain what We were looking for as well as the data of many clients. <mentions the general nature of the stolen documents>. This is not a joke or a scam.

This is a real problem that puts the existence of your firm in danger and to prove it We have attached screenshots that are confirming the possession of the files.

Reply to Our email and We will show you the complete file tree and actual files.
```

【訳】
件名：[被害組織名]は顧客の機密データを漏えいさせた。非常に重要！

こんにちは。
[被害組織名]のデータベースへのアクセスに成功し、極めて大量のデータセットを取得したことを通知する。我々は、数週間にわたり、あなた方のネットワーク内にある複数のシステムに侵入し、専有情報および機密ファイルを狙って活動していた。その結果、目的としていた情報に加え、多数の顧客データも入手できた(※窃取した文書の概要がここに記載されている)。これは冗談でも詐欺でもない。

これはあなた方の組織の存続を危険にさらす深刻な問題だ。その証拠として、我々が当該ファイルを保有していることを示すスクリーンショットを添付する。
このメールへ返信すれば、完全なファイルツリーおよび実際のファイルを見せてあげよう。

図 4 UNC3753 の恐喝メールの例(一部)[12]

【攻撃に要する時間】

Mandiant のレポートによれば、従業員への最初の接触から、機密データを窃取して恐喝メールを送付するまでの工程が 1 営業日以内に完結した攻撃事例が多数確認されている他、データがわずか 1 時間以内に窃取された事例もあった[12]。

2.4. 攻撃の拡張: 対面での接触を伴う侵入

電話やリモートツールを用いた遠隔からの侵入が失敗した場合、当該グループは標的組織に対して対面での接触を試みる[12]。この手法は、IT エンジニアや技術サポートスタッフを名乗る人物が実際に標的組織のオフィスを訪問するというもの[14]。フィッシングメールの影響への対処を理由に、端末の確認やバックアップが必要であるなどと従業員に伝え、その場で端末にアクセスし、USB メモリ等の外部記憶媒体を使ってデータを持ち出す事例が確認されている。5 月 26 日には、FBI もこの手口について警告を発した。

なお、UNC3753 の拠点とは異なる国で標的組織へのオフィスに出向くことができる背景として、同グループがギグワーカー(インターネットを通じて短期・単発の業務を請け負う個人労働者)を活用している可能性があることが、セキュリティ研究者たちから指摘されており、オフィス訪問者自身が、犯罪に加担していることを認識していないケースもあるとみられる[15]。

2.5. まとめ

本事例は、サイバー攻撃がもはやオンライン上だけで完結するものではないことを示している。言語や地理的な距離といった制約を越えて実行される攻撃は、現実世界にまで影響を及ぼしており、技術的対策のみでは十分に防御できない状況が生じつつある。ログやエンドポイントの監視等の技術的な防御が高度化する一方で、オフィス等の施設へのアクセス制御は依然として人的手続きへの依存が大きい。このような防御上のギャップを突き、攻撃者が物理的な侵入といった追加的手段を取る可能性にも留意する必要がある。以上を踏まえ、組織においてはセキュリティ対策の包括的な見直しが求められる。

[14] 出典: FBI FLASH『Silent Ransom Group Impersonating IT Personnel through Social Engineering』 https://www.ic3.gov/CSA/2026/260526.pdf

[15] 出典: CyberScoop『FBI warns US-based law firms to be on the lookout for cybercrime group that steals data in person』 https://cyberscoop.com/fbi-warning-silent-ransom-group-law-firms/

3. BOD 26-04 が示すリスクベース脆弱性対応への転換

3.1. 概要

2026 年 6 月 10 日、CISA（米サイバーセキュリティ・インフラセキュリティ庁）は運用指令「BOD 26-04」を発出した。本指令は、米国連邦機関に対し、脆弱性対応においてリスクに基づき優先順位と是正期限を決定し、その期限内に是正措置を講じることを義務付けるものである。これまで広く利用されてきたCVSSスコアを中心とした網羅的な脆弱性対応とは異なり、資産の公開状況、既知の悪用状況、攻撃の自動化可能性、技術的影響という 4 つの要素を踏まえてリスクを動的に評価することを義務付けている[16]。

3.2. リスクベースの脆弱性管理への転換

【CVSS による脆弱性管理の課題】

これまで CVSS (Common Vulnerability Scoring System：共通脆弱性評価システム)は、「脆弱性の深刻度を評価するための国際的な指標」として広く利用され、継続的に改良されてきた。だが、近年は脆弱性の増加に加え、AI の活用による攻撃の自動化と高速化が進み、脆弱性公開から実際の悪用までの期間が急速に短縮している。そのため、限られたリソースの中で対応の優先順位を適切に決定することが、組織にとって重要な課題となっている。

【SSVC による評価】

このような課題に対して、リスクベースの意思決定を実現するための枠組みとして提唱されているのが、SSVC（Stakeholder-Specific Vulnerability Categorization）である[17]。
SSVC ではステークホルダー（脆弱性対応に関する意思決定を行う主体）として、脆弱性への対応を実施する組織（Deployer）、製品やサービスを提供する組織（Supplier）、脆弱性情報の共有や調整を担う組織（Coordinator）を定義しており、各ステークホルダーが、それぞれの立場や責任に応じて脆弱性対応の優先順位を決定する。

ステークホルダ	対象
デプロイヤー	脆弱性の対応としてパッチ適用を実施する組織
サプライヤー	製品開発ベンダとしてパッチを提供する組織
コーディネーター	脆弱性情報を統制する組織

図 5　SSVC におけるステークホルダーの分類(情報処理推進機構 [IPA]の資料より) [18]

[16] 出典：CISA『BOD 26-04: Prioritizing Security Updates Based on Risk』
https://www.cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk

[17] 出典：Carnegie Mellon University Software Engineering Institute CERT Coordination Center (CERT/CC)『What is SSVC?』
https://certcc.github.io/SSVC/tutorials/ssvc_overview/

[18] 出典：独立行政法人情報処理推進機構（IPA）『脆弱性対応におけるリスク評価手法のまとめ ver1.1』
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/f55m8k0000003v30-att/f55m8k0000003v94.pdf

3.3. BOD26-04 の運用モデル

【BOD 26-04】

BOD 26-04 は、SSVC のリスクベースの脆弱性評価・意思決定の考え方を踏まえ、CISA が米国連邦機関向けの運用に適した形で制度化した指令である。連邦機関全体で迅速かつ一貫した意思決定が行えるよう、評価項目を標準化し、評価結果に応じた対応期限を明確に定義している。

【評価方法】

SSVC が、ステークホルダーごとの意思決定を支援する汎用的なフレームワークとして、複数の評価要素を決定木形式で組み合わせて対応方針を導き出すのに対し、BOD 26-04 は、連邦機関における運用を前提として評価方法を大幅に簡素化している。

例えば、SSVC の運用主体（Deployer）向け意思決定モデルでは、公開状況（Exposure）を 3 段階、悪用状況（Exploitation）を 3 段階、攻撃の自動化可能性（Automatable）を 2 段階、影響（Human Impact）を 4 段階で評価することにより、3×3×2×4 の組み合わせ（72 通り）の意思決定が行われる。

これに対し、BOD 26-04 では、SSVC のリスクベースの意思決定の考え方を踏まえつつ、「資産の公開状況（Asset Exposure）」「既知の悪用状況（KEV Status）」「攻撃の自動化可能性（Exploit Automation）」「技術的影響（Technical Impact）」の 4 要素をそれぞれ 2 段階で評価し、16 通り（2×2×2×2）の分類によって対応期限を決定する。

これは、連邦機関における実運用を前提として、複雑な分岐による詳細な評価よりも、迅速かつ一貫した意思決定を重視した設計であると考えられる。

No.	資産の公開状況	脆弱性の既知の悪用	攻撃の自動化可能性	技術的影響	対応期限
1	公開	有	有	完全な制御が可能	3 日以内＋フォレンジック・トリアージ
2	公開	有	有	部分的な制御が可能	3 日以内
3	公開	有	無	完全な制御が可能	3 日以内＋フォレンジック・トリアージ
4	公開	有	無	部分的な制御が可能	14 日以内
5	公開	無	有	完全な制御が可能	3 日以内
6	公開	無	有	部分的な制御が可能	14 日以内
7	公開	無	無	完全な制御が可能	14 日以内
8	公開	無	無	部分的な制御が可能	60 日以内
9	非公開	有	有	完全な制御が可能	3 日以内＋フォレンジック・トリアージ
10	非公開	有	有	部分的な制御が可能	14 日以内
11	非公開	有	無	完全な制御が可能	14 日以内
12	非公開	有	無	部分的な制御が可能	14 日以内
13	非公開	無	有	完全な制御が可能	60 日以内
14	非公開	無	有	部分的な制御が可能	60 日以内
15	非公開	無	無	完全な制御が可能	次回システム更新時に対応
16	非公開	無	無	部分的な制御が可能	次回システム更新時に対応

図 6 BOD 26-04 における評価要素と対応期限 [16]

【高リスク時の追加対応】

BOD 26-04 は、対応期限の設定に加え、一部の高リスク事案に対する追加対応も定めている。具体的には、侵害の可能性があると判断した場合には、「フォレンジック・トリアージ（侵害の有無の確認等）」を実施し、システムやネットワーク基盤への影響や侵害の有無を確認する。この段階で侵害が確認された場合には、インシデント対応へ移行する[19]。

3.4. まとめ

BOD 26-04 は、SSVC のリスクベースの意思決定の考え方を、連邦機関向けの実運用に適した形で具体化した取り組みといえる。4 つの評価要素を用いたシンプルな評価モデルと明確な対応期限を組み合わせることで、迅速な脆弱性対応の優先順位付けを支援している。脆弱性の増加や攻撃の自動化が進む今日において、このようなリスクベースの運用モデルは、連邦機関に限らず多くの組織にとって有効な示唆を与えるものと考えられる。

以上

[19] 出典：CISA『BOD 26-04: Implementation Guidance for Prioritizing Security Updates Based on Risk』 https://www.cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk

免責事項

本記事の内容は、正確であることに最善を尽くしておりますが、内容を保証するものではなく、本記事の利用に起因して発生したいかなる損害、損失についても補償しませんのでご留意ください。記事内に誤植や内容の誤り、その他ご指摘等、お問い合わせ事項がある場合は、お手数ですが下記までご連絡ください。

[お問い合わせ先]
NTT セキュリティ・ジャパン株式会社
プロフェッショナルサービス部 OSINT モニタリングチーム
メールアドレス: nsj-ps-osintmonitoring@security.ntt