

デジタル庁GSSへの不正アクセスが示したこと

VPN機器の既知脆弱性を自社で点検する手順

株式会社DnD / 2026年10月11日

この記事の要点

- CVSSで「Medium」に分類された既知の脆弱性でも、パッチが当たっていなければ実際の侵入に使われる。
- VPN機器のパッチ管理は「誰の担当かが曖昧」になりやすく、テレワーク導入後に保守が放置されているケースがある。
- 検知から公表まで78日かかった背景には「異常なアクセスを検知できる仕組み」の有無がある。

公式発表の経緯（デジタル庁、2026年9月11日）

- 2026年6月25日：保守運用担当者のアカウントによる大量のファイルアクセスを検知。

2. 2026年7月9日：VPN機器の既知の脆弱性（CVSSでMedium）を悪用した侵入と判明。アカウント停止・通信遮断。
3. 2026年7月15日：個人情報保護委員会へ報告。
4. 2026年9月11日：公表（検知から78日）。

漏えいした可能性がある情報：氏名・メールアドレス・電話番号・住所など、約24.6万件。マイナンバー・金融機関口座情報・年金番号は含まれない。VPN機器の製品名・脆弱性識別番号は非公表。

自社で確認できる7項目

#	確認すること	答えられないときの論点
1	自社でVPN機器・UTM・セキュリティアプライアンスを使っているか	機器の存在自体が把握されていない
2	機器のメーカー・製品名・ファームウェアバージョンが分かるか	パッチ情報と照合できない
3	最後にファームウェアを更新したのはいつか	既知の脆弱性が残ったままの可能性
4	パッチ適用の担当者が今もいるか	誰も対応できない状態になっている
5	メーカーのセキュリティ通知が届く設定になっているか	新しい脆弱性の情報を受け取れない
6	VPN接続のログイン成功・失敗の記録を確認できるか	不審なアクセスに気づけない
7	管理用アカウントは担当者ごとに分かれているか	侵害範囲の特定が難しくなる

対策の考え方

すぐ始められること：機器台帳の作成

機器名・バージョン・保守担当者・最終更新日を1枚のスプレッドシートにまとめる。定期的にメーカーの公開ページと照合する習慣を作る。

段階的に整えること：ログの定期確認

多くの機器はアクセスログを記録している。月1回、心当たりのないIPアドレスや時間帯のアクセスがないか確認する。

中長期で検討できること：ゼロトラスト型への移行

VPN機器はインターネット公開された入口であるため、脆弱性発見時に標的になりやすい構造がある。「内側は安全」という前提を置かないゼロトラスト型のアクセス設計も選択肢のひとつ。現状把握から段階的に検討できる。

「担当者が分からない機器がある」「最後にパッチを当てたのがいつか分からない」という段階からご相談いただけます。

<https://dnd-inc.jp/contact.html>

株式会社DnD — DX/AX（AIによる業務変革）パートナー