SECURITY ADVISORY REPORT

主要ソフトウェア脆弱性報告書

2026年11月 統合更新 — 言語ランタイム／基盤／インシデント／AI／生活者向け／法規制

報告日：2026年11月8日 — 第26版（Web v98統合更新）

対象読者: システム運用・開発・セキュリティ担当者/第7章は一般利用者・家族向け

統合集計・長期推移を先に確認し、各製品の章へ。CVE件数とインシデント報告件数は別です。全CVE・全歴史記述を再検証したものではありません。

第26版（2026年11月7日・51ページ）を起点に差分更新。基準18:00 JST。全過去記述・全CVEの提供元再検証ではありません。

目次

統合集計・長期推移 — Webと同じデータ 3
0. まず読む1ページ — 今回確認したこと 6
1. 全体一覧・対応優先度 7
2. 言語ランタイム 11
3. サーバー・基盤・機器 18
4. インシデント — 公式情報の再確認と統計 28
5. AIコーディングエージェントのリスク 36
6. セキュリティ特化 Agent Skills — 公式リポジトリの使い方 38
7. 生活者向け — 家族・従業員に配れる注意点 39
8. 法規制・補償・補助金 43
9. 結びに 44
10. 主要な情報源・留意事項・版履歴 49
注目CVE — 指定10件（第26版のNVD記録を継承） 5

統合集計・長期推移 — Webと同じデータ

基準日時：2026年11月9日14:15:00 JST（2026-11-09T05:15:00Z）。公開対象：2026年10月10日14:15:00〜11月9日14:15:00 JST、端点を含む直近30日。

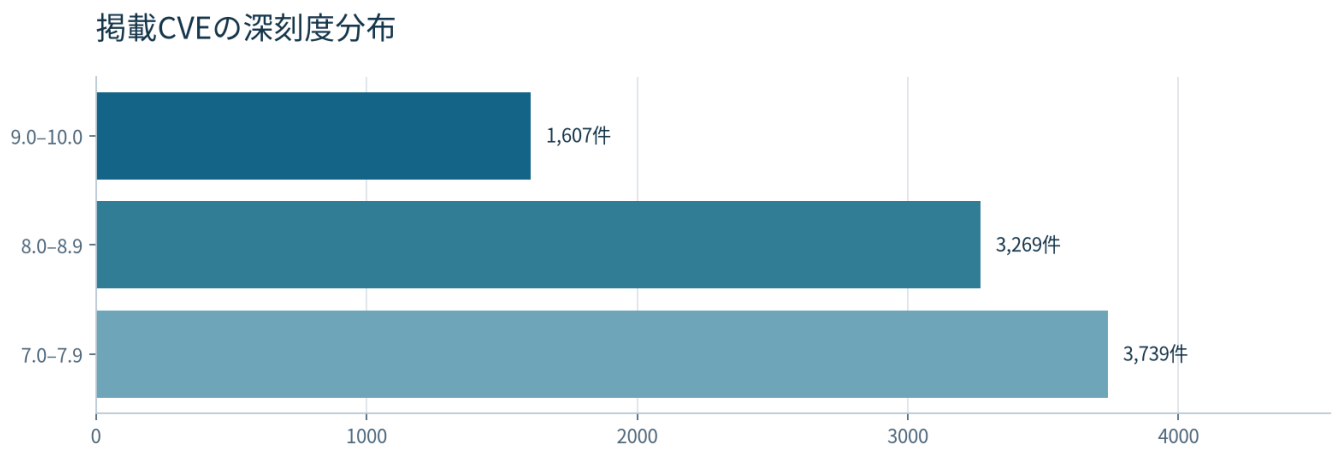
NVD取得：2026-11-09T05:29:57.864Z 〜 2026-11-09T05:33:05.453Z（UTC）。KEV取得：2026-11-09T05:25:36.091Z。公開基準・実取得・情報源の更新時刻は異なります。全ページの総数・連続offset・重複・期間を検査しましたが、APIは歴史時点のトランザクションスナップショットではありません。

対象CVE	うち9.0以上	対象内KEV	PPC速報報告
8,615件	1,607件	17件	2,094報告件（4月〜10月16日・第21版継承）

Rejected除外。CVE番号1個を1件。CVSS v3.0／3.1／4.0全評価の最大値7以上、9以上は内数。全17,584件＝掲載8,615＋未採点938＋Rejected652＋7未満7,379。版・評価元は混在。修正参照あり924件／不明・未確認7,691件、全件一覧の提供元独立精査0件。

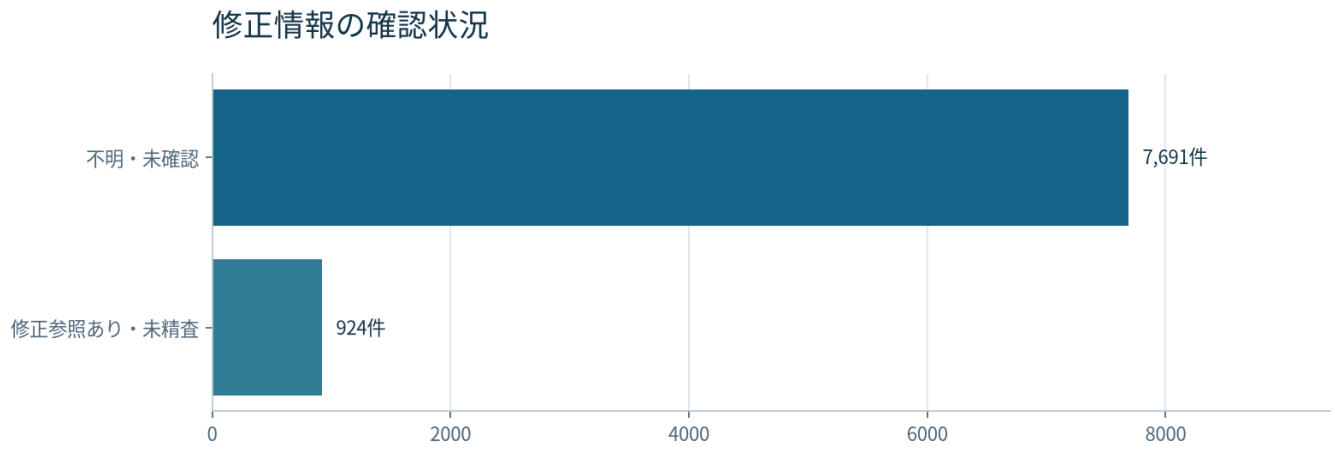
共通dataset ID：27a4aa4f95e61fa5dd5b7aa61bf015b4f39823b5db42b1a33f2e3cf7a4353c04
行データID：aifrontier-c867dac5565b2d45e0dc

> 月次は2024年1月〜2026年11月の35か月、UTC暦月。総CVEはRejected除外、KEVは現行カタログdateAdded月。11月は途中集計の白丸（総CVE3,427／KEV追加3）。高深刻度35月は未取得nullで、0ではなく図から省略。



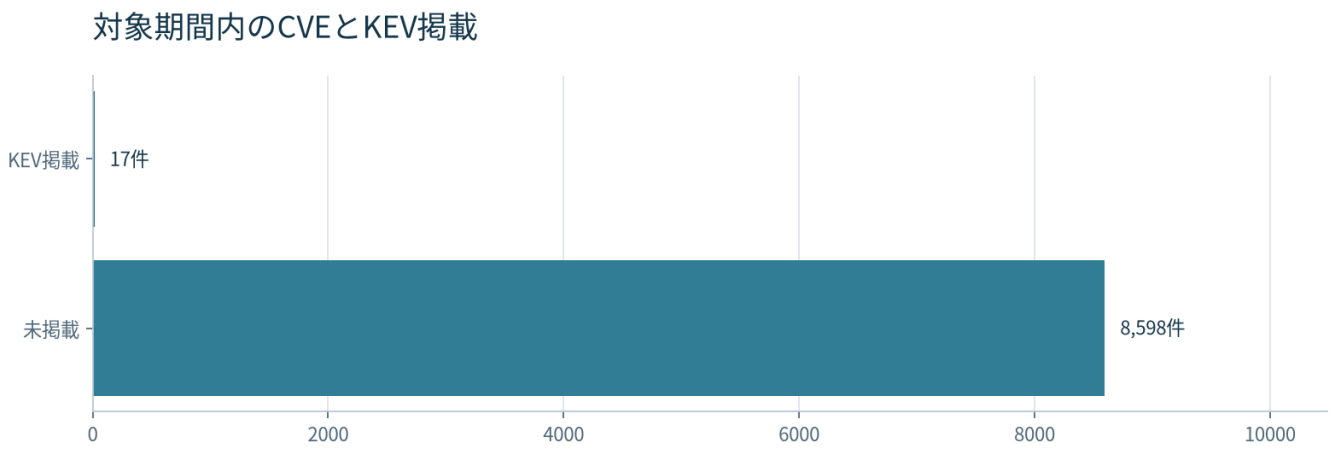
CVSS v3.0/3.1/4.0の掲載最大値。異なる版・評価元が混在。2026年10月10日14:15 JST基準。

Web・PDF共通画像。基準・期間・途中月・欠測は本章の定義を参照。



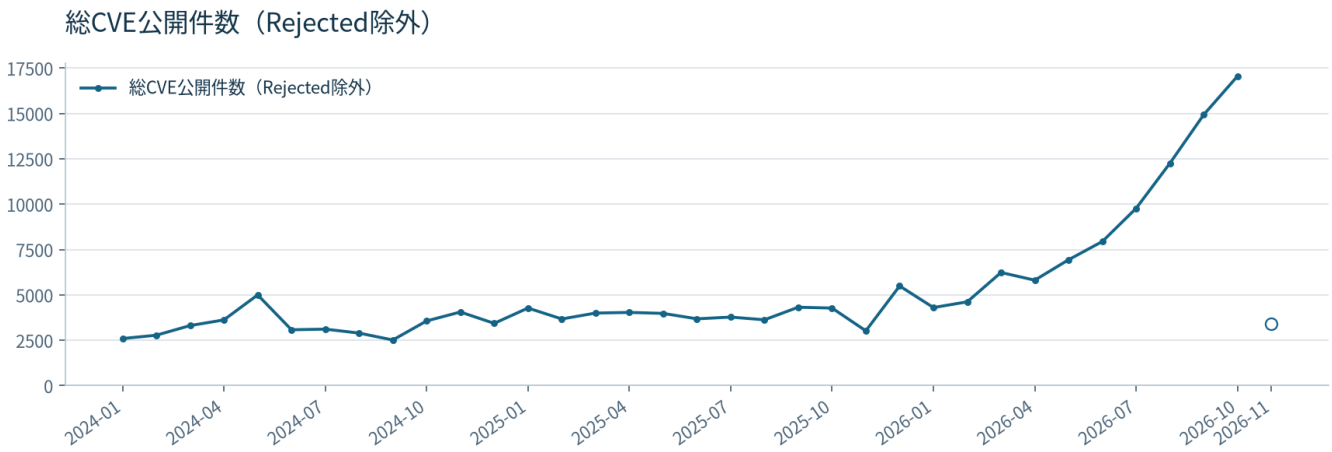
Patchタグの機械分類。修正版の提供・自社への適用を保証しません。2026年10月10日14:15 JST基準。

Web・PDF共通画像。基準・期間・途中月・欠測は本章の定義を参照。



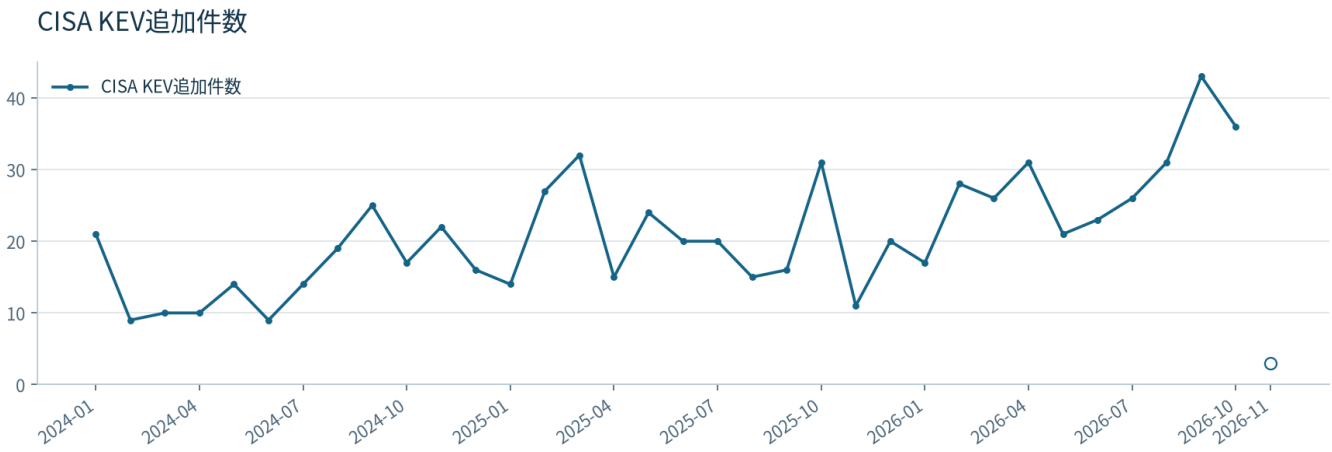
2026年10月10日14:15〜11月9日14:15 JST公開CVE。KEV未掲載は悪用なしを意味しません。

Web・PDF共通画像。基準・期間・途中月・欠測は本章の定義を参照。



UTC暦月・2024-01〜2026-11。11月は白丸の途中集計。高深刻度35月は欠測（0ではない）。

Web・PDF共通画像。基準・期間・途中月・欠測は本章の定義を参照。



UTC暦月・2024-01〜2026-11。11月は白丸の途中集計。高深刻度35月は欠測（0ではない）。

Web・PDF共通画像。基準・期間・途中月・欠測は本章の定義を参照。

注目CVE ― 指定10件（第26版のNVD記録を継承）

本節は第26版（2026年11月7日取得）のNVD記録をそのまま掲載した継承節です。本版で10件を再取得していないため、vulnStatus・CVSS・参照は11月7日時点の値です。窓内のCVEは本版の一覧・グラフ・CSVにも反映されています（窓内/窓外の判定のみ本版の窓で再計算）。

CVE	NVD公開日	NVD status（11/7）	CVSS最大	対象	窓内/窓外	一覧反映
CVE-2026-39430	2026-11-04	Received	9.8	HP Poly EagleEye Cube USB（1.3.1-001267）	窓内	掲載
CVE-2026-43499	2026-05-21	Modified	7.8	Linuxカーネル rtmutex（GhostLock）	窓外（一覧対象外）	対象外
CVE-2026-109469	2026-11-06	Awaiting Analysis	10.0	Microsoft Entra Device Registration	窓内	掲載
CVE-2026-74759	2026-11-01	Awaiting Analysis	9.8	Google::Auth（Perl）0.12	窓内	掲載
CVE-2026-122193	2026-11-06	Received	9.9	AWS Trusted Remote Execution（REX）SSMドキュメント	窓内	掲載
CVE-2026-98432	2026-10-15	Awaiting Analysis	9.8	Linuxカーネル（ipv4）	窓内	掲載
CVE-2026-19868	2026-11-06	Undergoing Analysis	7.5	SonicWall SonicOS SSLVPN	窓内	掲載
CVE-2026-123957	2026-11-07	Deferred	9.9	TOTOLINK CA300-PoE 6.2c.884	窓内	掲載
CVE-2026-113615	2026-11-06	Deferred	9.8	WordPress GS JWT Authentication（〜1.0.0）	窓内	掲載
CVE-2026-124040	2026-11-06	Deferred	9.2	CivetWeb 〜1.16（USE_HTTP2）	窓内	掲載

> NVDのstatusはNVD側の処理状態で、危険度や修正状況の判定ではありません。「Awaiting Analysis」「Received」を「危険」「安全」と読み替えません。CVSS v2のみの評価は本報告の集計対象外（未評価扱い）です。各CVEの技術的説明は第26版の個別メモを継承します。

0. まず読む1ページ — 今回確認したこと

> **第26版の検証範囲：**本日の更新は統合集計・グラフ・CVE一覧の再生成、11月8〜9日に一次情報で確認できた事象（金融庁、CISA KEV追加、Chrome、Brotli波及の機器側告知）の追記に限定します。各ソフトウェア章の既存記述と「注目CVE」10件のNVD記録は第26版からの継承です。旧版内の「本日」「今回」は当時の調査を指します。

第20版の全対象を本日再検証したものではありません。公式原文の再確認で変更・留保が必要な点を優先しました。新規公表日が確認できないものを11月2日の新着とは扱いません。

節・対象	第21版の公式確認と留保
2.1 PHP	公式アーカイブは8.5.12／8.4.27／8.3.36／8.2.35とWindows -1再ビルドを案内。115560の後続修正版は本文未掲載。session.upload_progress.enabled=0の暫定案を維持。
2.2 Node.js / Brotli	Node修正版26.12.1／24.22.1／22.23.4、Brotli CVE-2026-111497を再確認。Brotli上流1.2.1のSECURITY節も確認。Bun1.4.4はBrotliを修正対象に列挙するが、当該CVEとの対応・同梱版は未確認。
2.3 Python	3.15.2／3.14.10／3.13.18／3.12.16／3.11.18で115557（CA不信頼化）・114583（tarfile）を確認。後3系列はソースのみ。旧19445/19553個別勧告は未再確認。
2.4 Ruby	Onigmo4件は4.0.9／3.4.12／3.3.13に全修正。攻撃者由来の正規表現コンパイルが条件。resolvは0.7.2、Ruby3.3は0.3.2。
2.5 Oracle Java	114820は10/30 Rev2の組み込み製品追加を確認。最新Javaまたは公式緩和、製品別PADを参照。全JDKディストリビューションの現行版は今回未検証。
3.1 BIND	94300のGSS-TSIG再送条件、CVSS3.1 8.1、9.20.30／9.21.27／9.20.30-S1、既知回避策なし・ISCはactive exploitを認識していない旨を確認。他3件の個別本文は本日未再確認。
3.2 Linux	Ubuntu98432 generic 26.10／26.04／24.04／22.04はVulnerable work in progress。併記バージョンを配布済み修正版と読まない。AlmaLinuxのPwnEscapeとZDI-CAN-33367の本番修正版は前版記載と一致。ZDIは公式でCVE未採番。
3.4 GitLab / Tomcat	GitLab証明書対応7系列・Runner19.5.1・スキップ版を再確認。GitLab告知の絶対公開日は未確認。Tomcat11.0.27／10.1.61／9.0.123とHTTP/2・JNDIRealmを確認。103119は11系本文で確認し他系列へ無条件適用しない。
3.5 LiteLLM	原文再取得で1.107.0、公開管理キー未失効→Agent Platform→GitHub owner tokenという第20版の確定調査を再確認。今回の抽出回答に混入した1.17.0／1.17.1やGitHub token直接公開説は不採用。改善計画は完了3項目と進行中・予定を分け、11月・12月・2027年1月期限を実施済みとしない。署名・Trusted Publishingだけでは組織owner侵害を防げない。

3.13の再確認とAI追補は該当章を参照。GMOの累計情報提供は735件（11/2 18:00）へ更新。人数・事故数ではありません。

1. 全体一覧・対応優先度

> **第26版の検証範囲：**本日の更新は統合集計・グラフ・CVE一覧の再生成、11月8〜9日に一次情報で確認できた事象（金融庁、CISA KEV追加、Chrome、Brotli波及の機器側告知）の追記に限定します。各ソフトウェア章の既存記述と「注目CVE」10件のNVD記録は第26版からの継承です。旧版内の「本日」「今回」は当時の調査を指します。

第20版ソフトウェア調査の確認範囲は2.1〜2.5、3.1・3.2・3.4・3.5、3.11のLinux行、7.10のPython欄。これ以外の要約、第19版新着欄、旧悪用/KEV記載は第19版からの継承・今回個別再検証なし。更新した対処は該当詳細節の根拠リンク参照。

対象	名称 / CVE・深刻度	要点	対処	優先	期限目安	章
PHP	php2shell CVE-2026-109618 / 109619 9.2×2	未認証RCE。公表4日前から悪用、10/26 CISA KEV。Windows版は同梱Brotliも修正し再ビルド	8.5.12 / 8.4.27 / 8.3.36 / 8.2.35(Win版は再ビルド版)	緊急	即日	2.1
Brotli 同梱ソフト	HTTP2Shell(Node2Shell)CVE-2026-111497 9.2	Google Brotliデコーダーの境界外書き込み → RCEの恐れ。Node.js・Bun・Python・Envoy・Istio・PHP(Win)・PAN-OS・**VMware VCF**に波及。**10/27 CISA KEV追加**	Node 26.12.1／24.22.1／22.23.4。Bun1.4.4はセキュリティ修正あり、当該CVEとの対応は未確認。各同梱製品は個別勧告参照。	緊急	即日〜2日	2.2
Python	CVE-2026-19445 9.2 / 19553 / eMudhra証明書	侵害中間CAのsslブロック115557、tarfile 114583を公式確認。旧ssl19445/19553の個別記載は継承・未再検証。	3.15.2 / 3.14.10 / 3.13.18 / 3.12.16 / 3.11.18。前2者以外はソースのみ。注意喚起冒頭でpip26.2.2 / certifi2026.10.19 / uv0.13.6。既存venvも別確認。	高	今週	2.3
Ruby	Onigmo修正 / resolv CVE-2026-80212/80213	GitLab RCE 4件の根本原因(正規表現エンジン)を修正。resolvはDoS・検証迂回	4.0.9 / 3.4.12 / 3.3.13、resolv 0.7.2 (GitLab本体のOnigmo由来RCEは「GitLab」行(緊急)を参照)	中	2週間	2.4
Oracle Java	CVE-2026-91403 / CVE-2026-114820、CVSS 3.1 9.1	中間CA不信頼化と後続ルートCA削除を区別。10/30にDB/AHF/OPatch/SPMS追加。	91403のCPU426に加え114820のCPU427等を確認。8u511-b33と25.0.5.0.3+1の10/24ノート、後者baseline表に11/17/21の.0.3+1も掲載。	高	今週	2.5
jackson-databind	CVE-2026-110879 9.8 (開発元)	Java の JSON ライブラリ。総称型・配列の中の型が検証されず、任意クラス生成 → 条件次第でRCE	2.18.12 / 2.21.8 / 2.22.4 / 3.1.8 / 3.2.4	高	今週	2.6
ISC BIND 9	CVE-2026-94300 8.1 ほか3件	GSS-TSIGのメモリ破壊 → 停止・RCEの恐れ。回避策なし	9.20.30 / 9.21.27	高	今週	3.1

Linuxカーネル	PwnEscape 9.3 / Infinity Core / KSMBD 9.0×2 / ZDI-CAN-33367 / TCP UAF CVE-2026-98432 9.8	TCPはIPv4 TCP全般、Red Hat Critical/9.8・未認証RCEの可能性。研究実証と実悪用を区別。Infinity Core/KSMBD等は継承・未再検証。	3.2のAlmaLinux本番修正版を確認し再起動。TCPの部分緩和は完全防止不可。Ubuntu generic対象系列は修正作業中。MPTCP使用有無だけで対象外としない。	緊急/高	即日〜2日 / 今週	3.2
Apple	iOS / iPadOS 27.2 ほか (10/26)	iOSで160件超、全製品で329件の修正。macOS Gatekeeper回避 CVE-2026-112512 も	iOS / iPadOS / macOS 27.2 等	高	今週	3.3
GitLab	CVE-2026-110264 / 97229 10.0×2 ほか	細工した正規表現で未認証RCE(根本はRuby Onigmo)	証明書対応 CE/EE:19.5.3/19.4.5/19.3.7/19.2.10/19.1.10/19.0.11/18.11.14。Runner19.5.1、AI Gateway別更新。19.5.2/19.4.4はスキップ。 公開日未確認。旧KEV/Alpine記載は未再検証（3.4）。	緊急	即日〜2日	3.4
Apache Tomcat	8件(CVE-2026-101356 等)	HTTP/2混線・非GSSAPI SASL JNDIRealm fail-open。AJP103119は11系で確認、他系列へ無条件適用しない。	11.0.27 / 10.1.61 / 9.0.123	高	今週	3.4
LiteLLM	サプライチェーン攻撃 (10/21)/ CVE-2026-42208・42271(KEV)	1.107.0に情報窃取マルウェア混入	1.107.0環境は再構築・資格情報失効。1.106.2固定は旧暫定案。新cosign鍵署名を確認。別Enterprise GHSAは修正版未確認（3.5）。	緊急	即日	3.5
Wasmtime	CVE-2026-115889 / 115893 9.9×2	悪意あるWasmモジュールでサンドボックス脱出(1件はARM64限定、2020年から存在)	36.0.19 / 48.0.7 / 49.0.4 / 50.0.0+再ビルド	高	今週	3.6
GoAhead	CVE-2026-115881 / 115884 ほか計11件(うち3件 重大)	機器組み込みWebサーバー。失効した証明書を受理、特定条件で任意パスワードでログイン可	6.1.1(機器はメーカーのファーム更新待ち)	中	2週間	3.7
Oracle EBS	CVE-2026-101767 9.8	未認証SQLi → OSコマンド実行(12.2.3〜12.2.15)	2026年10月CPU	緊急	即日〜2日	3.9
NGINX	CVE-2026-42530(major)	HTTP/3 の解放後利用 → 停止・RCEの恐れ(1.31.0〜1.31.1)	1.31.2以上(現行は1.31.7 / 1.30.6)	高	今週	3.9
TeamViewer	CVE-2026-92372 ほか(TV-2026-1011)	Linux/macOS版の画面デコーダー境界外書き込み → RCE	15.83以上	高	今週	3.9
Chrome	62 CVE + 追加修正52件	Anthropicの研究モデルが攻撃チェーンを実証(62件)。10/28にさらに52件(重大4・高46・中2)を修正	Chrome 156.0.8078.73以上	高	今週	3.9 / 3.11
UEFI(EDK II)	CVE-2026-97631 9.5	PXEネットワークブート中の細工ICMPでOS起動前にコード実行。16年前から存在	BIOS更新待ち/不要ならPXE無効	中	更新提供次第	3.9

Tailscale	Tailworm報告(未修正・CVE未採番)	SSHポート転送許可時に横展開・root化の恐れ(研究者報告)	SSHルールを1対1に、ポート転送無効化	中	2週間	3.8
その他	Windows Shell・Citrix・Arista(KEV)、Microsoft eMudhra G3削除、Cloudflare Workers AI、AWS SAM CLI、LibreSSL ocspcheck、VMware ESX・Adobe Commerce(KEV追加分)、LocalStack ほか	悪用確認済み・個別アドバイザリ・事業者側の事案	各修正版(LibreSSLは未公開。ESX・CommerceはKEV) (内訳により異なる(VMware ESX・Adobe Commerce はKEV入り、LibreSSLは修正版未公開))	中	2週間	3.8〜3.9
Cisco Secure Firewall(ASA/FTD)	CVE-2026-76418 8.6 (KEV)	リモートアクセスSSL VPNのロジック誤り(tunnel groupで2次認証を設定時)。未認証の遠隔から細工リクエストで**装置が再起動(DoS)**。10/28公開、**10/29 CISA KEV追加**(Ciscoが悪用を確認済みと表明)	10/28公開の修正を適用。VPNの公開範囲を最小化	高	今週	3.11
GitLab(追加)	CVE-2026-97229 10.0 (KEV)	10/29 CISA KEV追加。Alpine Linuxが10/20〜21に自社GitLabインスタンスへの悪用未遂(ワーカー8回クラッシュ)を確認・公表、念のためインスタンスを再構築	証明書対応 CE/EE:19.5.3/19.4.5/19.3.7/19.2.10/19.1.10/19.0.11/18.11.14。Runner19.5.1、AI Gateway別更新。19.5.2/19.4.4はスキップ。 公開日未確認。旧KEV/Alpine記載は未再検証（3.4）。	高	即日	3.4 / 3.11
Teltonikaルーター	CVE-2026-82104(重大)	RutOS 7.22〜7.24.2 / TswOS 1.9〜1.10。HTTPS経由で**未認証のセキュリティチェック回避 → コマンド実行の恐れ**。RUT/RUTX/RUTM/RUTC/TAP/CAP等の全機種が対象(10/30 Teltonika公式開示)	RutOS 7.24.3 / TswOS 1.10.1 へ更新	高	今週	3.12
Cloudflare /cdn-cgi/image/	XSS連鎖(研究者実証・CVE未採番)	SVG無害化のすり抜け+キャッシュ経由でCSP除去+リダイレクト連鎖。**利用サイトのドメイン上でスクリプト実行**の恐れ(Cloudflareは全サイトの約24%の前面)	画像配信元のヘッダー素通しを見直し、nosniff (CVE番号・公式修正は本書時点で未確認、ヘッダー設定の見直しを推奨)	中	継続対応	3.11
phpMyAdmin	5.2.3対象、研究者単独報告10件(CVE未採番)	WebAuthn 2FA回避ほか。9件中8件は要ログイン。**公式PMASA未発行**	管理画面を公開しない、setup/フォルダ削除 (公式PMASA・CVE番号は本書時点で未確認、速報として扱う)	中	2週間	3.10
GMO事案	お名前.com デスクトップクラウド侵害	不正アクセス事案。懸賞金サイト累計情報提供735件（11/2 18:00）。被害者数ではない。	利用者: 端末点検・パスワード変更・MFA (個別対応(第4章参照)。パッチ適用ではなく端末点検・MFA)	—	—	4.1
AIエージェント	AGENTS.md / CLAUDE.md による乗っ取り / **Claude Code偽装拡張機能**	ダウンロードフォルダに置かれた指示ファイルでCodex等が悪性パッケージを導入(実害観測)。Open VSX上の偽装 `anthropic.claude-code`がSSHバックドアを設置	起動場所の制限・設定点検・拡張機能の出所確認	中	2週間	5

Telegram(Android)	通話経由の端末乗っ取り連鎖	受話するだけで起動する脆弱性を含む3件の連鎖で**端末を完全乗っ取り**(メッセージ・マイク・カメラ)。12.10.2以前が対象	Telegram を 12.10.4 以上へ更新 (全利用者に影響しうる)	高	今週	3.12
Ivanti Connect Secure	CVE-2026-111357 8.8 / CVE-2026-118527 4.3(KEV)	既知の認証バイパス(CVE-2026-104935)と組み合わせ**未認証root権限RCE**に悪用。脅威アクター「UTA0576」が認証情報窃取・ADメタデータ収集等を実施。10/30 CISA KEV追加	22.8R2.6 / 25.1.1.3 へ更新	緊急	即日	3.13
WordPress Core	CVE-2026-119977 8.1	公式7.1.4で更新中RCE・複数XSS・CA対応を確認。旧18,500試行は本日未確認。	7.1.4へ更新。旧系列バックポートは進行中、全系列完了とはしない。	緊急	即日	3.13
Canonical LXD	CVE-2026-112816 10.0	HTTPSリスナーの証明書検証不備。細工した証明書チェーンで**任意の信頼済みクライアントになりすまし**、クラスタとVMへ完全アクセス。MicroCloudも対象	4.0.15 / 5.0.11 / 5.21.9 / 6.10.1 へ更新	緊急	即日〜2日	3.13
ClickHouse Server	CVE-2026-116366 9.5	特定条件下で未認証RCEの恐れ。Cloud/BYOCは公式適用済み。実悪用状況は本日未確認。	26.10.3.7 / 26.9.27.3 / 26.8.36.3 / 26.3.62.3 へ更新	高	今週	3.13
Agent Skills	公式セキュリティスキル7種	Cloudflare・Anthropic・OpenAI・NVIDIA・Google・Alibaba の公式リポジトリ	導入前検査・隔離環境で使用 (活用推奨(第6章参照)。脆弱性そのものではない)	—	継続	6
ServiceNow AI Platform	CVE-2026-103093	管理者ロールを持つ認証済みユーザーが、Rhino JavaScriptサンドボックスの制限を回避しホストOS上で任意コード実行。ServiceNowが修正を配備、ホスト型インスタンスは適用済み。悪用報告なし	自己ホスト・パートナー提供インスタンスは最新パッチ(Yokohama P13 HF4a等)を確認・適用	中	2週間	3.12
全社・家族	—	第7章の周知、パスキー移行、JPCERT/CCのIOCとログ突合	継続的な周知・移行・突合	継続	月次	7

共通する所見(3点)

- **1つの部品の欠陥が多数の製品に波及。** Brotli(Node.js・Bun・Python・Envoy・PHP・PAN-OS)、Onigmo(Ruby → GitLab)、eMudhra証明書(Java・Python・Node.js)。**自社のコードを書き換えていなくても当事者になる**ため、ランタイム・同梱ライブラリ・コンテナの棚卸しが要。
- **悪用までの時間が短い。** php2shellは公表4日前から悪用試行、LiteLLMのSQLiは公開36時間後に実攻撃。AI支援で発見・攻撃とも高速化している(Apple更新でAnthropic・OpenAIが計7件の謝辞、ChromeではAnthropicの研究モデルが62件を発見、UEFI・jackson-databindの欠陥もAnthropic等の発見)。**防御側も公式のAIセキュリティスキルを使う段階**(第6章)。
- **「人が確認する」前提の防御が崩れている。** AIエージェントの乗っ取り、ClickFix、サポート詐欺など、利用者の操作・信頼を悪用する手口が主流。技術対策と同時に周知(第7章)が必要。

恒常的にやること

- **ランタイム・同梱ライブラリ・コンテナの棚卸し(SBOM)** — 部品1つの欠陥が多数の製品に波及する月だった。
- **CISA KEV・JPCERT/CC を優先順位の基準に**し、「公表日=攻撃開始日」と考えない(悪用は公表前から始まることがある)。
- パッチ適用と同時に**侵害痕跡の確認**、認証情報の最小権限化・短命化。
- AIエージェントの**指示ファイル・設定ファイルを資産管理**の対象に。

深刻度は各ベンダー表記(CVSS 4.0 / 3.1 混在)。行間の厳密な比較には使えない。

2. 言語ランタイム

第26版の検証範囲：本日の更新は統合集計・グラフ・CVE一覧の再生成、11月8〜9日に一次情報で確認できた事象（金融庁、CISA KEV追加、Chrome、Brotli波及の機器側告知）の追記に限定します。各ソフトウェア章の既存記述と「注目CVE」10件のNVD記録は第26版からの継承です。旧版内の「本日」「今回」は当時の調査を指します。

2.1 PHP — 「php2shell」CVE-2026-109618 / 109619 9.2 ×2 悪用中

11月2日再確認・PHP：公式アーカイブは8.5.12／8.4.27／8.3.36／8.2.35とWindows -1再ビルドを案内。115560の後続修正版は本文未掲載。session.upload_progress.enabled=0の暫定案を維持。
https://www.php.net/archive/2026.php

第20版調査差分（2026-11-01）: 第19版の悪用時刻・KEV・全GHSA・暫定操作は再検証していない。識別子: CVE-2026-109618 / CVE-2026-109619。確認範囲: Web要求を扱うPHPで未認証RCEの可能性。mod_phpはアプリコードより前の実証あり。 対処: 8.5.12 / 8.4.27 / 8.3.36 / 8.2.35。EOL向け最小ソースバックポートとLTSベンダー修正は別確認。 悪用状況: 今回悪用時刻・PHPのKEV追加は再検証せず。 未確認: 全GHSA本文 / 実悪用・KEV日付。根拠: 公式資料1

第20版調査差分（2026-11-01）: 識別子: CVE-2026-111497。確認範囲: cURLで自動HTTP応答展開を有効にした場合に同梱Brotliへ到達。 対処: 8.5.12-1 / 8.4.27-1 / 8.3.36-1 / 8.2.35-1、Brotli 1.2.1。runtime版は不変。 悪用状況: Brotli全体の実悪用はCISAで別確認。Windows PHP個別の悪用は未確認。 根拠: 公式資料1 / 公式資料2

第20版調査差分（2026-11-01）: 識別子: CVE-2026-115560。確認範囲: 特殊なserialize handlerの実行時切替とupload progress有効が条件のRCE経路。 対処: 公式10/23はsession.upload_progress.enabled=0と次の通常版で勧告予定。後続修正版は未確認。 悪用状況: 未確認。 未確認: 後続修正版。根拠: 公式資料1

項目	内容
内容	**109618**: memory_limit 超過時の中断が初期化途中に入り、未初期化メモリを解放 → RCE。**109619**: fatal error 後に解放済みの内部状態が残り、同じワーカーの次のリクエストで使われる → RCE。どちらも**認証不要・アプリのコードより前の1リクエストで発火**。
影響	8.5.12 / 8.4.27 / 8.3.36 / 8.2.35 未満、EOLの8.1以下。PHP-FPM・mod_php(最も危険)・php-cgi・FrankenPHP・LiteSpeed。**WordPress等のCMSを更新してもPHP本体は直らない。**
悪用	10/17(公表4日前)にAWSのハニーポットで悪用試行を検知。公表後は数時間で数百万件規模(Cloudflare)。10/26 **CISA KEV追加**。JPCERT/CC注意喚起 JPCERT-AT-2026-0033。
対処	**8.5.12 / 8.4.27 / 8.3.36 / 8.2.35 へ更新**(ディストリ・LTSベンダーのパッケージで可)。更新できない・8.1以前は**修正までオフライン化**(CISA・CERT-EU)。更新済みでも**10/17以降の侵害痕跡**(Webシェル・不審プロセス・設定変更、PHPワーカーがシェルを起動する挙動)を調査。
暫定緩和 (代替にならない)	109618: memory_limit=-1(php_admin_value)、post_max_size 縮小、プロキシでリクエストサイズ制限。 109619: session.upload_progress.enabled=0 で全ワーカー再起動。

Windows版PHPの公式再ビルド: 8.5.12-1 / 8.4.27-1 / 8.3.36-1 / 8.2.35-1、Brotli 1.2.1。runtime版は不変。 cURLで自動HTTP応答展開を有効にした場合に同梱Brotliへ到達。 第19版のGuzzle等の個別到達条件・回避操作は今回個別再検証なし。

CVE-2026-115560: 特殊なserialize handlerの実行時切替とupload progress有効が条件のRCE経路。 公式10/23はsession.upload_progress.enabled=0と次の通常版で勧告予定。後続修正版は未確認。 実悪用は今回未確認。未修正と現在断定しない。

2.2 Brotli — 「HTTP2Shell(Node2Shell)」CVE-2026-111497 9.2

> **11月2日再確認・Node.js / Brotli：**Node修正版26.12.1／24.22.1／22.23.4、Brotli CVE-2026-111497を再確認。Brotli上流1.2.1のSECURITY節も確認。Bun1.4.4はBrotliを修正対象に列挙するが、当該CVEとの対応・同梱版は未確認。
> https://nodejs.org/en/blog/vulnerability/october-2026-security-releases

> 第20版調査差分（2026-11-01）: 旧Express/body-parser・EOL系列は今回個別再検証なし。識別子: CVE-2026-111497 / CVE-2026-105482 / CVE-2026-105483 / CVE-2026-106069 / CVE-2026-106072 / CVE-2026-106074 / CVE-2026-106071 / CVE-2026-106073。確認範囲: Brotli入力でメモリ破壊・漏えい・RCE可能性。ほかDNS/TLS検証、snapshot乱数再利用、権限モデル。 対処: 26.12.1 / 24.22.1 / 22.23.4。各項目の影響系列は原文で異なる。 悪用状況: Brotliの実悪用はCISA。各Node経路の実悪用は未確認。 未確認: Express/body-parserの到達条件 / 全EOL系列。根拠: 公式資料1

> 第20版調査差分（2026-11-01）: 旧KEV期限・各同梱製品の個別版は未再検証。全同梱製品の実悪用と一般化しない。識別子: CVE-2026-111497。確認範囲: デコーダー境界外書き込み、RCE可能性。 対処: 上流v1.2.1のSECURITY節で修正確認。悪用状況: CISA 10/27告知がevidence of active exploitationとしてKEV追加。 未確認: 対応期限 / Python brotli/brotlicffi・Envoy/Istio/PAN-OS/VCF個別版。根拠: 公式資料1 / 公式資料2

> 第20版調査差分（2026-11-01）: 確認範囲: 1.4.4のSecurity節にBrotliを含む広範な修正列挙。 対処: 1.4.4一般修正は確認。当該Brotli CVEとの対応・同梱版は未確認。 悪用状況: 未確認。 未確認: CVE対応 / 公開日 / 同梱Brotli版。根拠: 公式資料1

Google の Brotli 展開ライブラリ(1.0.3〜1.2.0)の境界外書き込み。攻撃者が送るBrotli圧縮データを展開するだけでクラッシュ・メモリ漏えい・**コード実行の恐れ**。OpenAIが発見、上流修正は2月にコミット済みだったがリリースは10/21。10/22に公開PoC。**10/27に CISA が KEV に追加**(悪用の証拠に基づく。米連邦機関の対応期限 11/10)— 第13版の「悪用報告・KEV掲載なし」を訂正。

同梱・利用している製品	修正版	注意点
Node.js 26 / 24 / 22	26.12.1 / 24.22.1 / 22.23.4	Express 5・body-parser 2.x は `Content-Encoding: br` の本文を自動展開(express.json()だけで到達)。fetch()の応答も経路。25・23・20以下はEOLで修正なし → 22/24へ
Bun	1.4.4一般セキュリティ修正は確認。当該Brotli CVE対応・同梱版は未確認。	bun build --compile の単一実行ファイルも再ビルド
Brotli本体 / Python **brotli** / brotlicffi	1.0.10・1.1.1・1.2.1 / 1.2.1 / 1.2.1.0	venv・コンテナごとに更新
Envoy / **Istio**	1.40.0・1.39.3・1.38.6・1.37.8 / 1.29.9・1.30.6・1.31.2	修正までBrotli展開フィルターを無効化
PHP(Windows版)	10/26以降の再ビルド版	2.1の注記参照
VMware Cloud Foundation	VMSA-2026-0008.1(10/27公開・10/28更新)	Broadcomが**Critical(CVSSv3 7.5〜9.8)**と評価。SDDC Manager でRCEの恐れ(9.1.1系は9.8、旧系列も対象と報道)。回避策あり — 版別の修正・手順はVMSAで確認
Palo Alto PAN-OS	各ホットフィックス	PA-Series / VM-Series の **11.2.4以降**で、**Brotli検査とTLS復号の両方を有効**にしている場合のみ影響。管理インターフェース、11.1・10.2系は影響なし。回避策としてBrotliエンコーディング無効化のCLI設定、検知用の脅威シグネチャも提供。詳細はPalo Alto公式アドバイザリで確認

- **ランタイム更新が唯一の根本対処**(Node.jsはワークアラウンドを案内せず)。`node -v` / `bun --version` で全サーバー・CI・コンテナを棚卸し。

- **コンテナは作り直す。** `node:24.22.0-alpine` 等のピン留めタグは再ビルドしても脆弱なまま。
- 暫定: リバースプロキシ/WAFで `Content-Encoding: br` を含むリクエストを拒否(fetch応答側は防げない)。Cloudflareは10/25に検知ルール(既定Log)を追加。
- GitHub上の出所不明の「PoC」「スキャナ」はマルウェア混入の恐れ — 隔離環境でのみ。
- 同じNode.jsリリースでTLSホスト名検証バイパス等High 3件を含む計10件も修正(外部通信の多いランタイム・CIを優先)。

2.3 Python — ssl の2件と eMudhra 証明書問題

> **11月2日再確認・Python：**3.15.2／3.14.10／3.13.18／3.12.16／3.11.18で115557（CA不信頼化）・114583（tarfile）を確認。後3系列はソースのみ。旧19445/19553個別勧告は未再確認。
> https://blog.python.org/2026/10/python-3152-31410-31318-31216-31118/

> 第20版調査差分（2026-11-01）: 識別子: CVE-2026-115557 / CVE-2026-114583。確認範囲: 侵害CA中間鍵のsslブロック。tarfile.tar_filterで展開先置換リンク拒否。http.cookiejar負version拒否も含む。 対処: 3.15.2 / 3.14.10 / 3.13.18 / 3.12.16 / 3.11.18。前2者以外はソースのみ。 悪用状況: 取得した公式本文では実悪用を確認せず。 未確認: 旧19445/19553個別勧告 / 他系列個別公開日。根拠: 公式資料1 / 公式資料2 / 公式資料3

> 第20版調査差分（2026-11-01）: 確認範囲: pipのvendor CAとOSストア、更新済みsslブロックの違いに注意。 対処: 注意喚起冒頭でpip26.2.2 / certifi2026.10.19 / uv0.13.6。既存venvも別確認。 悪用状況: 今回具体的実悪用は未確認。 未確認: 長い会話全件 / 更新日時。根拠: 公式資料1

問題	内容	対処
CVE-2026-19445 9.2 CVE-2026-19553 7.6	SNIコールバックでSSLContextの解放後利用(未認証でクラッシュ等)/ wrap_bio() で server_hostname を渡さないと証明書検証が無言で省略	3.10.22 / 3.11.17 / 3.12.15 / 3.13.16 / 3.14.8 以上
eMudhra中間CA鍵の漏えい(2.5と同じ問題)	侵害CA中間鍵のsslブロック。tarfile.tar_filterで展開先置換リンク拒否。http.cookiejar負version拒否も含む。 CVE-2026-115557のリリース反映を公式発表で確認。CVE-2026-114583（tarfile）とhttp.cookiejarの修正も含む。3.14.10個別ページの公開日は10/25。他系列・ブログの公開日は別確認。	3.15.2 / 3.14.10 / 3.13.18 / 3.12.16 / 3.11.18。前2者以外はソースのみ。注意喚起冒頭でpip26.2.2 / certifi2026.10.19 / uv0.13.6。既存venvも別確認。

第19版からの継承・今回個別再検証なし：旧ssl CVE-2026-19445 / 19553の説明・修正版。今回確認した緊急版とは区別する。

注意: 既存venv内のpip・certifiは別途確認する。旧版のpip vendor CAとOSストアに関する注意を、更新済みsslの侵害中間証明書ブロック導入後にも無条件適用しない。 pipのvendor CAとOSストア、更新済みsslブロックの違いに注意。

2.4 Ruby — Onigmo(正規表現エンジン)修正と resolv gem

> **11月2日再確認・Ruby：**Onigmo4件は4.0.9／3.4.12／3.3.13に全修正。攻撃者由来の正規表現コンパイルが条件。resolvは0.7.2、Ruby3.3は0.3.2。
> https://www.ruby-lang.org/en/news/2026/10/23/regexp-fixes-for-gitlab-cves/

> 第20版調査差分（2026-11-01）: 識別子: CVE-2026-89078 / CVE-2026-93577 / CVE-2026-97229 / CVE-2026-110264。確認範囲: 攻撃者入力の正規表現コンパイル時のメモリ破壊。開発者固定の正規表現だけなら非該当と公式説明。 対処: 全修正Ruby4.0.9 / 3.4.12 / 3.3.13。4.0系列の初回修正はCVEごとに異なる。 悪用状況: GitLabでRCE転用可能との公式説明。実悪用の独立確認はしていない。 根拠: 公式資料1

> 第20版調査差分（2026-11-01）: 通常のOS resolver接続とgem経由を区別。依存gem経由も確認する。識別子: CVE-2026-80212 / CVE-2026-80213。確認範囲: gem経由DNSでメモリ枯渇/ホスト名検証迂回。普通のOS resolver接続とは別。 対処: 0.7.2、Ruby3.3は0.3.2。0.4.0–0.7.1および0.3.1以前が影響。 悪用状況: 未確認。 根拠: 公式資料1

問題	内容	対処
Onigmo のバグ (GitLab の CVE-2026-89078 / 93577 / 97229 / 110264 の根本原因)	攻撃者が渡した文字列を正規表現としてコンパイルするアプリで二重解放・整数オーバーフロー → RCEに転用可能(GitLabで実証)。**Regexp.timeout やパターン長制限では防げない。** Ruby側はCVEを採番していないため、スキャナではGitLab側のCVEで追跡	**Ruby 4.0.9 / 3.4.12 / 3.3.13**(10/23)。不可なら信頼できない入力から Regexp.new 等をしない
resolv gem `CVE-2026-80212` / `80213`	悪意あるDNS応答でメモリ枯渇(DoS)/ ホスト名検証の迂回(SSRF対策のすり抜け)。Resolv・resolv-replace を使う場合のみ(通常のNet::HTTP等は非該当)	resolv 0.7.2(3.3系は0.3.2)

2.5 Oracle Java SE — CVE-2026-91403 9.1(定例外アラート)

> **11月2日再確認・Oracle Java：**114820は10/30 Rev2の組み込み製品追加を確認。最新Javaまたは公式緩和、製品別PADを参照。全JDKディストリビューションの現行版は今回未検証。
> https://www.oracle.com/security-alerts/alert-cve-2026-114820.html

> 第20版調査差分（2026-11-01）: 114820は10/24初版、10/30 Rev2でDB/AHF/OPatch/SPMSを追加。識別子: CVE-2026-91403 / CVE-2026-114820。確認範囲: 91403は中間CA不信頼化、114820は関連ルートCA削除。後者10/30改訂でDB/AHF/OPatch/SPMS追加。 対処: 91403のCPU426に加え114820のCPU427等を確認。8u511-b33と25.0.5.0.3+1の10/24ノート、後者baseline表に11/17/21の.0.3+1も掲載。 悪用状況: 公式取得本文では実悪用有無未確認。CVSS3.1は9.1。 未確認: 全JDKディストリ / 27系列後続修正版 / PAD内部。根拠: 公式資料1 / 公式資料2 / 公式資料3 / 公式資料4 / 公式資料5

Javaのコード欠陥ではなく、**認証局 eMudhra の中間CA証明書8枚の秘密鍵が漏えい**し、JDK同梱の信頼ストアがそれを信頼してしまう問題。偽証明書によるTLSなりすまし・署名付きJARの検証すり抜けが起こりうる。GraalVM、各OpenJDKディストリ、Node.js・PythonのCAバンドルにも同じ対応が入った。

- 最新のJava更新を確認する。CVE-2026-91403のCPU426（中間CA不信頼化）だけでなく、後続CVE-2026-114820のCPU427等（関連ルートCA削除）を別に確認。91403のCPU426に加え114820のCPU427等を確認。8u511-b33と25.0.5.0.3+1の10/24ノート、後者baseline表に11/17/21の.0.3+1も掲載。 アプリ同梱JRE・コンテナも対象。全JDKディストリと27系列後続修正版は未確認。
- 更新できない場合(Oracle公式): cacertsをバックアップし、該当ルート4件を削除して再起動。eMudhra系の正規証明書を使う接続先はTLSが失敗しうるので事前確認。

```
keytool -delete -cacerts -alias "emsignrootcag1 [jdk]"
keytool -delete -cacerts -alias "emsignrootcag2 [jdk]"
keytool -delete -cacerts -alias "emsigneccrootcag3 [jdk]"
keytool -delete -cacerts -alias "comodoaaaca [jdk]"     # JDK 8 は -keystore $JDK_HOME/jre/lib/security/cacerts
```

新 Microsoft も同じ問題で eMudhra G3 ルート証明書を Windows の信頼リストから削除(MSRC 10月ブログ)。Windows上でeMudhra系の証明書を使う接続先・署名は失敗しうる。

2.6 jackson-databind — CVE-2026-110879(型検証のすり抜け)

> 第19版からの継承・今回個別再検証なし。以下の版番号・悪用状況・件数・日付を今回の現時点確認済みと解釈しない。

Java で最も広く使われるJSONライブラリ。**クラス名で型を指定させる構成**(@JsonTypeInfo(use=CLASS)、default typing)で、外側の型だけ検証し**総称型の引数・配列の要素の型を検証していなかった**(6月の CVE-2026-54512 の修正漏れ)。攻撃者が送ったJSONで任意のクラスを生成でき、Spring がある環境ではコマンド実行まで実証。開発元評価 9.8(Amazon Linuxは8.1)。発見者にAnthropicが含まれる。

影響範囲	修正版
com.fasterxml 2.10.0〜2.18.11 / 2.19.0〜2.21.7 / 2.22.0〜2.22.3	**2.18.12 / 2.21.8 / 2.22.4**
tools.jackson 3.0.0〜3.1.7 / 3.2.0〜3.2.3	**3.1.8 / 3.2.4**

- **Spring Data Redis の RedisSerializer.json() / GenericJackson2JsonRedisSerializer、Spring Security の旧Jackson 2モジュール**は既定でこの経路を使う — キャッシュ・セッションに他者が書き込めるなら優先。
- 確認: `mvn dependency:tree -Dincludes=com.fasterxml.jackson.core:jackson-databind` / Gradle `dependencyInsight --dependency jackson-databind`。フレームワークのBOM経由の版も確認。
- 更新できない場合(開発元): 信頼できないデータにクラス名ポリモーフィズムを使わない、許可する型を狭める、キャッシュ・セッションへの書き込みを制限。

2026年11月6日 追加確認（指定資料）

OpenSSH on musl libc — CVE-2026-123158（確認済み）

musl libc は2012年のコミット b3c4cc12 で、crypt() の失敗時に NULL ではなく「*」を返す設計にした。sha512crypt は DoS 対策で鍵長を256バイトに制限しており（KEY_MAX 256）、257バイト以上のパスワードでは crypt() が失敗して「*」を返す。OpenSSH は2016年（CVE-2016-6210 の対策）から、実在しない／ハッシュを持たないユーザーでも他アカウントのsaltでハッシュ計算を行うため、shadow の「*」と計算結果の「*」が一致し得る。結果として、パスワードログインを禁止したアカウント（root、鍵専用ユーザー、AlpineのAWS/Azureイメージ既定ユーザー等）が、257文字以上の任意パスワードで認証通過する。NVDは「OpenSSH 10.6p2 未満、musl libc かつ PAM 無効」と記載し、CVSS v3.1 8.1（AV:N/AC:H/PR:N/UI:N）、CWE-394。修正は commit 4353fdc（pick_salt の修正で、指摘されたバグの4行上）。

実務判断：Alpineコンテナで sshd を動かし、PasswordAuthentication を有効にしている構成は影響対象。PAM を使う構成、パスワード認証を無効化した鍵のみの構成は当該経路に乗らない。root を「*」でロックし鍵運用している構成は、まさにこの経路の前提に合致するため、OpenSSH 10.6p2 以降への更新を優先する。NVD status は Received（2026-11-06時点）。https://github.com/openssh/openssh-portable/commit/4353fdc43ef646c43a8dda7025cc1a898caf1482sshhole.com（研究者解説）

OpenSSL 3.4 / 3.6 のEOL（提供元公称）

OpenSSL 3.4 は2024年10月22日リリースの通常版で、当時の方針（非LTSは2年）により**2026年10月22日にEOL**。3.6 は2025年10月1日リリースで、現行方針（非LTSは13か月）により**2026年11月1日にEOL**。いずれも公開セキュリティ修正の提供が終了する。**EOLは「直ちに脆弱」という意味ではなく、今後判明する脆弱性に対する修正が公**

開されないという意味。最新は 4.1（2027年11月23日まで）、LTSは 3.5（2030年4月8日まで）。Extended support は LTS のみが対象で、3.4/3.6 は対象外（個別相談は可能と記載）。https://openssl-library.org/post/2026-11-01-eol34-36/

PHP OOM 関連（CVE-2026-109618／109619／115560）（提供元公表・第三者検証）

PHP は OOM 時に longjmp() でリクエスト処理を中断するが、一部コンテキストでこの経路のメモリ状態が初期化されない（CWE-416）。CVE-2026-109618 は CVSS v3.1 9.8／v4.0 9.2、NVD status は Analyzed。CVE-2026-115560 は NVD 未登録（totalResults=0）だが、Cloudflare の WAF changelog が 109618／109619／115560 の3件をまとめて参照している。**NVD未登録＝脆弱性なし、ではない**。

2026年11月7日 追加確認（指定2資料）

CVE-2026-98432 のUbuntuリリース別ステータス（提供元：Ubuntu Security）

Ubuntu の CVE ページは、linux パッケージについて次の状態を示しています（2026-11-07取得）。「Vulnerable work in progress」は**修正作業中**を意味し、悪用の確認でも「安全」でもありません。併記されるバージョンは作業中・修正済みの対象版であり、配布済みの修正版と読み替えないでください。

Ubuntuリリース	linux の状態	表記バージョン
26.10（stonking）	修正済み	7.3.0-10.10
26.04 LTS（resolute）	作業中（Vulnerable work in progress）	7.0.0-43.43
24.04 LTS（noble）	作業中	6.8.0-149.149
22.04 LTS（jammy）	作業中	5.15.0-203.213
20.04 LTS（focal）	作業中	（バージョン表記なし）
18.04 LTS（bionic）	作業中	（バージョン表記なし）
16.04 LTS（xenial）	作業中	4.4.0-293.327
14.04 LTS（trusty）	対象外（Not affected）	—

派生カーネルでは、linux-aws・linux-gcp・linux-oracle・linux-raspi の 26.10 が **7.3.0-1004.4 で修正済み**、linux-realtime・linux-riscv の 26.10 が 7.3.0-10.10.1 で修正済みです。一方 linux-azure の 26.10 は同じ 7.3.0-1004.4 という表記で「作業中」とされており、**パッケージごとに状態は異なります**。24.04／22.04 の各フレーバーは概ね作業中で、20.04 以前はバージョン表記のない「Vulnerable」が多数を占めます。linux-hwe 系は多くが Not in release で、18.04 は「Ignored end of standard support」等の表記があります。14.04 の「Not affected」は当該カーネルが影響を受けないという意味で、サポート期間の長短とは別です。

実務の読み方：修正済みと明示されたリリース／パッケージは、提示された版以降へ更新する対象です。作業中のリリースは、提供元が修正版を公開するまで待つ間、当該経路（外部からのTCP接続とSYN再送が重なる状況）の露出を下げる運用が考えられますが、提供元が個別の緩和策を提示しているわけではありません。**本報告は提供元の指示を超えた独自の運用手順を断定しません。**https://ubuntu.com/security/CVE-2026-98432

> Ubuntuページの取得内容には優先度（priority）表記と影響サブシステムの説明文を確認できませんでした。NVD側のCWEは未割当、CVSS v3.1は9.8（AV:N/AC:L/PR:N/UI:N）です。

GhostLock（CVE-2026-43499）を使った実端末LPEの公開

2026年11月、BlackBerry KEYone **BBB100-2**（Android 8.1.0、kernel 3.18.71-perf-gc924168、build ABS154、security patch 2019-03-05）に対する**ローカル権限昇格**の実装が公開されました。GhostLock（CVE-2026-43499）をカーネル書き込みプリミティブとして用い、adb shell が取れる状態から root を得るものです。bootloader unlock やファームウェア書き換えは不要とされています。

原理（要約）：3.18系の futex_requeue は FUTEX_CMP_REQUEUE_PI 経路で rt_mutex_start_proxy_lock() を呼び、デッドロック検査が -EDEADLK を返すと remove_waiter() に進みます。この版の remove_waiter() は待機側で

はなく実行者（current）の状態を操作し、さらに -EDEADLK 経路では requeue_futex() が省略されるため、待機タスクの pi_blocked_on が自スタック上の rt_mutex_waiter を指したまま残ります。その後、所有者側の remove_waiter() がこの古い waiter を辿り、waiter->lock に置いた偽ロックを経由して rt_mutex の pi_tree 操作（rb_erase）を任意アドレスへの8バイト書き込みに転用します。公開実装はこの書き込みで `security_hook_heads.capable` のリストを空にし、全プロセスの capable() を 0 にして setuid(0) を通します。

性質と限界：capable フックの無効化は**グローバルかつ一時的**で、他プロセスの権限検査も同時に緩むため、1〜2分程度で再起動に至ると説明されています。再起動で復旧します。同リポジトリは bootloader unlock はできないと明記しており（RPMB／TrustZone側の記録が正で、KEY2向けの kibo は KEYone に適用できない）、root 取得と unlock は別問題です。

なぜ重要か：CVE-2026-43499 自体は2026年5月公開のカーネルUAFで、CVSS v3.1 7.8（AV:L）のローカル前提です。しかし**実端末で完結するLPEチェーンとして公開された**ことで、Android 8.1／3.18カーネルのようなEOL端末における「adb が有効な端末は物理接触から root まで到達し得る」ことが具体化しました。CISA KEV には掲載されていません（2026-11-07時点）。**KEV未掲載は悪用がないことを意味しません。**

防御側の示唆：EOLのAndroid端末では、USBデバッグ（adb）を無効化し、端末を物理的に管理する以外の根本策がありません。ベンダー修正が見込めない端末は、業務データの保存先・認証端末としての利用を見直す対象です。

> **掲載方針：**本報告は公開されたPoCの存在と原理の要約までを扱い、攻撃コードのビルド手順・アドレス値・オフセット・実行手順は掲載しません。他者端末や他人の管理下の機器への適用は、日本法（不正アクセス行為の禁止等に関する法律、電子計算機損壊等業務妨害罪等）および各国法で違法となり得ます。検証は自身が所有・管理する機器に限られます。https://github.com/giannoccarol/root-key1

3. サーバー・基盤・機器

第26版の検証範囲：本日の更新は統合集計・グラフ・CVE一覧の再生成、11月8〜9日に一次情報で確認できた事象（金融庁、CISA KEV追加、Chrome、Brotli波及の機器側告知）の追記に限定します。各ソフトウェア章の既存記述と「注目CVE」10件のNVD記録は第26版からの継承です。旧版内の「本日」「今回」は当時の調査を指します。

3.1 ISC BIND 9 — CVE-2026-94300 8.1 ほか同時開示3件

11月2日再確認・BIND：94300のGSS-TSIG再送条件、CVSS3.1 8.1、9.20.30／9.21.27／9.20.30-S1、既知回避策なし・ISCはactive exploitを認識していない旨を確認。他3件の個別本文は本日未再確認。
https://kb.isc.org/docs/cve-2026-94300

第20版調査差分（2026-11-01）: ISCの悪用認識と世界的非悪用の保証を区別。旧公開PoC情報は未確認。識別子: CVE-2026-94300 / CVE-2026-19630 / CVE-2026-96888 / CVE-2026-97313。確認範囲: GSS-TSIG再送によるメモリ破壊/RCE可能性8.1。再帰資源枯渇、redirect+strict QNAME、複数RPZのDoSは各7.5。 対処: 9.20.30 / 9.21.27 / 9.20.30-S1。各個別公式は既知回避策なし。 悪用状況: ISCはいずれもactive exploitsを認識していないと記載。世界的非悪用の保証ではない。 未確認: 公開PoCの正否。根拠: 公式資料1 / 公式資料2 / 公式資料3 / 公式資料4 / 公式資料5

項目	内容
内容	GSS-TSIG(AD連携の動的DNS更新等)の署名付きメッセージのリプレイでメモリ破壊 → 停止、条件次第でRCE。同時にDoS系3件(CVE-2026-19630 / 96888 / 97313、各7.5)。
影響	9.11.0以降のほぼ全版(9.18系などEOLには修正なし)。悪用は未確認だが公開PoCの情報あり。
対処	**9.20.30 / 9.21.27**(S1は9.20.30-S1)で4件まとめて修正。**ワークアラウンドなし**(ISC・JPRS)。GSS-TSIG未使用でも全環境で更新。更新後 named -v → 再起動まで確認。

3.2 Linuxカーネル — 4系統をまとめて「修正カーネル+再起動」

11月2日再確認・Linux：Ubuntu98432 generic 26.10／26.04／24.04／22.04はVulnerable work in progress。併記バージョンを配布済み修正版と読まない。AlmaLinuxのPwnEscapeとZDI-CAN-33367の本番修正版は前版記載と一致。ZDIは公式でCVE未採番。
https://ubuntu.com/security/CVE-2026-98432

第20版調査差分（2026-11-01）: Red Hatの現行評価はCritical/9.8。評価変更日時は未確認。識別子: CVE-2026-98432。確認範囲: Red Hat Critical/9.8、未認証遠隔からタイミング競合によるRCE可能性。公式影響説明はMPTCP限定ではない。対処: Red HatがIPオプションを含む通信の部分フィルター緩和を案内、完全防止不可。Ubuntu generic linuxは26.10/26.04/24.04/22.04でVulnerable work in progress。 悪用状況: 研究実証と実悪用は区別。今回実悪用/KEVは未確認。 未確認: 上流mboxはAnubis / 全RHEL errata / 全Ubuntu flavor / 上流修正版一覧 / 評価変更日時。根拠: 公式資料1 / 公式資料2 / 公式資料3

第20版調査差分（2026-11-01）: 識別子: CVE-2026-99999。確認範囲: PwnEscape VM→hostメモリ漏えい/停止/root実証。ローカル経路も公式言及。 対処: 本番:8=4.18.0-553.177.1.el8_10、9=5.14.0-687.59.1.el9_8、10=6.12.0-211.67.1.el10_2。 悪用状況: 研究実証は確認、実悪用は未確認。 根拠: 公式資料1

第20版調査差分（2026-11-01）: 識別子: ZDI-CAN-33367。確認範囲: ローカル非特権からread-onlyファイルのpage cache改ざん、権限昇格。 対処: 10/28本番:8=4.18.0-553.178.1.el8_10、9=5.14.0-687.60.1.el9_8、10=6.12.0-211.69.1.el10_2。悪用状況: 公開PoCを公式が言及。実悪用は未確認。CVEは取得した公式で未採番。 未確認: 上流現状 / 他ディストリ。根拠: 公式資料1

名称	内容	状況・対処

PwnEscape CVE-2026-99999 9.3	ゲストVMが送るチェックサム情報をホストが信じ、IPv4ヘッダを上書き → ホストのメモリ漏えい・全VM停止・**ホストでroot実行**(実証)。約18年前から存在	本番:8=4.18.0-553.177.1.el8_10、9=5.14.0-687.59.1.el9_8、10=6.12.0-211.67.1.el10_2。 研究実証と実悪用は区別。元の仮想化ホスト優先方針を継承。
Infinity Core(6件)	Timer・Signal・MM・Futex・Scheduler・SLAB の解放後利用等。**公開エクスプロイトあり**。権限昇格・コンテナ脱獄・Android	修正カーネル。更新まで信頼できないローカルユーザー・CIジョブ・マルチテナントコンテナを動かさない
ZDI-CAN-33367(skb_zerocopy) 7.8	ローカル権限昇格。**動くPoC**でAlmaLinux 8/9/10、Debian 12/13、Ubuntu 24.04/26.04 のroot取得を確認	10/28本番:8=4.18.0-553.178.1.el8_10、9=5.14.0-687.60.1.el9_8、10=6.12.0-211.69.1.el10_2。 CVEは取得した公式で未採番。上流現状・他ディストリは未確認。 【第19版の過去時点・暫定策（今回再検証なし）】上流修正は未マージ(10/26時点)。暫定: user.max_user_namespaces=0、IPsec不使用なら esp4/esp6 ブロック。KernelCare等のライブパッチあり
KSMBD(ZDI-CAN-33774 / 33549) 9.0 ×2	カーネル内蔵SMBサーバーの認証前の範囲外読み取り/SMB Directのバッファ超過	KSMBDを使っていなければモジュール無効化(RHEL既定は非搭載、Samba利用は対象外)。使うなら445/tcpを外部公開しない
TCP UAF CVE-2026-98432 9.8	Red Hat Critical/9.8、未認証遠隔からタイミング競合によるRCE可能性。公式影響説明はMPTCP限定ではない。 【第19版の研究実証・評価履歴等（今回個別再検証なし）】IPv4 TCPの接続確立処理で、保留中リクエストのIPオプション(Record Route/Timestamp)をコピーせず新ソケットに渡すレース ― 再送SYNと競合するCPUが解放済みメモリを読む。 Anthropicが10/27、Claudeに「初期プロンプトのみ」で書かせたエクスプロイトが、MPTCP(マルチパスTCP)リスナーを持つサーバーに対し無認証リモートでroot権限のコマンド実行に成功したと公表 (カーネルアドレス漏えいまで48分、コード実行到達までさらに5分)。カーネル開発チーム評価9.8。 Red Hatは当初5.9〜8.1(Moderate〜High)と評価していたが、10/30付RHSB-2026-016で「未認証の遠隔攻撃者がこの競合状態を悪用してリモートコード実行を達成しうる」としてCritical(最高)へ評価を引き上げ 、単なるDoSではなくRCEとして扱うことを明言。IPv6は対象外(コピーする実装のため)。悪用は本書時点で未確認(CISA KEV未掲載)	Red HatがIPオプションを含む通信の部分フィルター緩和を案内、完全防止不可。Ubuntu generic linuxは26.10/26.04/24.04/22.04でVulnerable work in progress。MPTCP無効化だけを完全対処としない。全RHEL errata・Ubuntu flavor・上流修正版一覧は今回未確認。第19版にある自前ビルド版や他ディストリ配布済み判定を今回確認済みとして使わない。

3.2確認範囲: TCPの旧研究実証・評価変更日時・IPv6・KEV、Infinity Core / KSMBDおよび他ディストリの旧記載は第19版からの継承・今回個別再検証なし。MPTCP対象の実験結果と、公式のIPv4 TCP全般という影響説明を混同しない。

第19版のZDI報告当時の『パッチなし』という説明を現行対処へ一括適用しない。AlmaLinuxのZDI-CAN-33367は10/28本番配布を確認。上流状態・他のZDI案件は今回未確認。

3.3 Apple — iOS / iPadOS / macOS 27.2 ほか一斉更新(10/26)

> 第19版からの継承・今回個別再検証なし。以下の版番号・悪用状況・件数・日付を今回の現時点確認済みと解釈しない。

項目	内容
規模	iOS / iPadOS 27.2 で**160件超**(WebKit 30件超、カーネル約15件)。同日の macOS・watchOS・tvOS・visionOS・Safari 27.2 を合わせ**329件**の固有脆弱性(9to5Mac集計)。
主な修正	Apple Intelligence 経由で遠隔からデータにアクセスされうる問題、「メールを非公開」で本当のアドレスが漏れる問題など。脱獄研究者(Calif / Stefan Esser氏)が報告した6件も修正。発見者としてAnthropicが3件、OpenAIが4件で謝辞に掲載。
注目	**macOS Gatekeeper 回避 CVE-2026-112512**(パス処理の欠陥で、どのアプリでも安全確認をすり抜けうる。研究者がゼロデイとして公表)— macOS 27.2 / Sequoia 15.8.2 / Tahoe 26.7.2 で修正(NVD)。**WebKit**: Webページを開くだけでコードが実行されうる欠陥(PC Watch報道)— iPhone・Mac を最新へ。
悪用	Appleは今回の修正について**悪用の確認を表明していない**(10/29時点)。
対処	**全端末を27.2へ**(設定 → 一般 → ソフトウェアアップデート)。27へ上げられない旧機種向けの更新は Apple のセキュリティアップデート一覧で対象機種と版を確認。MDM管理端末は配信を前倒し。

3.4 GitLab と Apache Tomcat

> **11月2日再確認・GitLab / Tomcat：**GitLab証明書対応7系列・Runner19.5.1・スキップ版を再確認。GitLab告知の絶対公開日は未確認。Tomcat11.0.27／10.1.61／9.0.123とHTTP/2・JNDIRealmを確認。103119は11系本文で確認し他系列へ無条件適用しない。
> https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-5-3-released/

> 第20版調査差分（2026-11-01）: 追加証明書対応111943。公開日未確認、新着日を推定しない。旧97229個別・KEV/Alpineは未再検証。識別子: CVE-2026-110264 / CVE-2026-111943。確認範囲: 110264は未認証RCE可能性10.0。111943は侵害中間CAの不信頼化。 対処: 証明書対応CE/EE:19.5.3/19.4.5/19.3.7/19.2.10/19.1.10/19.0.11/18.11.14。Runner19.5.1、AI Gateway別更新。19.5.2/19.4.4はスキップ。 悪用状況: 旧KEV/Alpine事案は今回未確認。 未確認: 19.5.3公開日 / 97229個別原文 / KEV/Alpine。根拠: 公式資料1 / 公式資料2

> 第20版調査差分（2026-11-01）: 識別子: CVE-2026-101356 / CVE-2026-101296 / CVE-2026-103119。確認範囲: HTTP/2混線、非GSSAPI SASL JNDIRealm認証fail-open。AJP103119は11.0.0-M25–26を確認。 対処: 11.0.27 / 10.1.61 / 9.0.123。103119は11.0.27節で確認、他系列に無条件適用しない。 悪用状況: 未確認。 未確認: 全系列非該当の保証 / 実悪用。根拠: 公式資料1 / 公式資料2 / 公式資料3

製品	主な脆弱性	対処
GitLab	CVE-2026-110264・97229(10.0): CI設定等の細工した正規表現で**未認証RCE**(根本原因はRuby Onigmo、2.4)。ほか SAML+LDAP自動リンクでのアカウント乗っ取り(8.2)、OAuth discoveryのキャッシュポイズニング(7.5)	証明書対応 CE/EE:19.5.3/19.4.5/19.3.7/19.2.10/19.1.10/19.0.11/18.11.14。Runner19.5.1、AI Gateway別更新。19.5.2/19.4.4はスキップ。 【第19版のRCE対応版（証明書対応の完了条件ではない）】19.5.1 / 19.4.3 / 19.3.6 / 19.2.9。公開インスタンスはIP制限・VPN化
Tomcat	HTTP/2混線 CVE-2026-101356、非GSSAPI SASLのJNDIRealm認証fail-open CVE-2026-101296。CVE-2026-103119のAJP混線は11.0.0-M25–11.0.26で確認。10.1/9へ無条件適用しない。旧『8件』を全系列共通の件数としない（旧参照: JVNVU93110597）。	**11.0.27 / 10.1.61 / 9.0.123**。HTTP/2公開・AJP連携・LDAP認証の構成を優先

3.5 LiteLLM — リリース基盤侵害による汚染パッケージ(10/21)

> **11月2日再確認・LiteLLM：**原文再取得で1.107.0、公開管理キー未失効→Agent Platform→GitHub owner tokenという第20版の確定調査を再確認。今回の抽出回答に混入した1.17.0／1.17.1やGitHub token直接公開説は不採用。改善計画は完了3項目と進行中・予定を分け、11月・12月・2027年1月期限を実施済みとしない。署名・Trusted Publishingだけでは組織owner侵害を防げない。
> https://docs.litellm.ai/blog/security-changes-after-oct-21-2026

> 第20版調査差分（2026-11-01）: 確定調査公開10/23 21:00 UTC。10/31〜11/1の新規事件とはしない。識別子: litellm==1.107.0。確認範囲: 不正PyPI/コンテナが資格情報窃取・RCEツール。初動のログ由来説は公式確定調査で訂正。対処: 再構築・資格情報失効。旧1.106.2固定は初動暫定案。10/23cosign鍵変更、10/24から新鍵署名版、10/30verified更新。 悪用状況: 公式が悪性配布を確認。PyPI11:39:51–13:23、DockerHub11:46:56–14:20、GHCR11:46:56–13:51まで（10/21 UTC）。 未確認: 全脆弱性の現行推奨版。根拠: 公式資料1 / 公式資料2

> 第20版調査差分（2026-11-01）: 供給網事故とは別件。CVE/CVSS数値・公開日時・影響版・修正版を補完しない。識別子: GHSA-w4c7-34wj-hqm8。確認範囲: 未認証でローカルファイル読み取り・外部送信、master/provider key漏えい、条件次第root Python実行。無ライセンスOSSは非該当。 対処: 修正版は未確認。公式部分緩和:callback系キー拒否/除去、egress allowlist、VPN等。 悪用状況: 実悪用未確認。供給網事故とは別。 未確認: CVE / CVSS数値 / 絶対公開日時 / 影響版 / 修正版。根拠: 公式資料1

AIゲートウェイLiteLLMのPyPI版1.107.0と不正コンテナに資格情報窃取・RCEツールが混入。公式確定調査の侵入経路は、公開リポジトリに残った未失効のAgent Platform管理キー → Agent Platform API → GitHub組織所有者トークン。旧『内部LiteLLMのログから最初のトークンを取得』説は初動仮説であり訂正する。 公式が悪性配布を確認。PyPI11:39:51–13:23、DockerHub11:46:56–14:20、GHCR11:46:56–13:51まで（10/21 UTC）。

- `pip show litellm` で 1.107.0 なら**侵害済みとみなす**(ただし影響環境でPythonを起動すると再発火するため、除去前にpip等を実行しない)。`litellm.dev` への通信をログで検索。
- 汚染環境の再構築と資格情報の失効・ローテーションを行う。旧litellm==1.106.2固定は初動の暫定指示であり、現行の安全性や全脆弱性修正の保証ではない。10/23にcosign鍵変更、10/24から新鍵署名版、10/30にverified情報更新。署名鍵の世代を確認し、旧キーで署名が有効なことだけで安全判定しない。新キー指紋・全脆弱性の現行推奨版はこのJSONからは確定しない。
- **認証情報を全面ローテーション**(LiteLLM内の全プロバイダAPIキー・マスター/仮想キー、DBパスワード、IAMロール、SSH鍵、AIツールのトークン、環境変数のシークレット)。
- 第19版からの継承・今回個別再検証なし（旧CVE個別勧告・KEV）：別件で本体の重大脆弱性(`CVE-2026-42208` 未認証SQLi、`42271` RCE・KEV掲載)も。外部公開インスタンスは最新版・公開範囲最小化。

3.6 Wasmtime — サンドボックス脱出 CVE-2026-115889 / 115893 9.9 ×2

> 第19版からの継承・今回個別再検証なし。以下の版番号・悪用状況・件数・日付を今回の現時点確認済みと解釈しない。

WebAssemblyランタイム Wasmtime(Fastly Compute・Spin等に組み込み)の既定コンパイラ Cranelift の誤コンパイル。**攻撃者のWasmモジュールをコンパイルさせるとサンドボックスを脱出**できる。115889は全アーキテクチャ、115893は**ARM64のみ・2020年から存在**。悪用報告なし・KEV未掲載。

使用中の版	対応
36.0.19未満(24.x LTS含む)	36.0.19、または 48.0.7 / 49.0.4 / 50.0.0 へ
37.0.0〜47.x(37〜42系は修正なし)	48.0.7 / 49.0.4 / 50.0.0 へ移行
48.0.0〜48.0.6 / 49.0.0〜49.0.3	48.0.7 / 49.0.4 へ(ARM64側が未修正)

- **組み込みアプリは再ビルド必須**(CLI更新では直らない)。`cargo tree -i wasmtime`、`cargo audit`。事前コンパイル済み `.cwasm` も再生成。
- 4月に別件で36.0.7 / 42.0.2 / 43.0.1へ上げたホストも115893は未修正。**Dependabotは115893を警告しない可能性**。更新まで第三者のWasmモジュールを実行しない。

3.7 GoAhead(Embedthis)— 組み込みWebサーバー 6.1.1 で11件修正

> 第19版からの継承・今回個別再検証なし。以下の版番号・悪用状況・件数・日付を今回の現時点確認済みと解釈しない。

GoAhead はルーター・プリンター・IP電話など**機器の管理画面**に広く組み込まれる小型Webサーバー(開発元は「数億台」に搭載と説明)。6.1.1 は8月に機器メーカーへ先行提供され、10月に一般公開された。11件のアドバイザリのうち3件が重大。

問題	内容
`CVE-2026-115881`	OpenSSLを使う構成で、クライアント証明書認証(mTLS)の**失効リスト(CRL)を確認せず、失効済みの証明書を受け入れる**。影響 3.4.5〜6.1.0
`CVE-2026-115884`	旧来のLibreSSL経路で同種の問題
ログイン回避	6.1.0以降の既定フォームログインで、Blowfishパスワードハッシュ使用時に**認証を回避**できる問題
Mbed TLS	DH鍵交換の弱さ(CVE未採番)

- **機器メーカー・自社製品で組み込んでいる場合:** 6.1.1 へ更新し、既存セッションを破棄して再起動、**Blowfishのパスワードをすべて再設定**。
- **機器の利用者:** メーカーのファームウェア更新を待って適用。**管理画面をインターネットに公開しない**、初期パスワードを変える(第7章のルーター対策と同じ)。
- 状況: 研究者(FoxIO)がPoCを公開、悪用の報告はなし、CVEはNVD未登録(10/28時点)。HP・Canon・Siemens・D-Link等の製品が影響を受けうるとの報道があるが、**各社の確認は取れていない**。

3.8 その他の個別アドバイザリ・悪用確認済み脆弱性

> 第19版からの継承・今回個別再検証なし。以下の版番号・悪用状況・件数・日付を今回の現時点確認済みと解釈しない。

対象	内容	対処
Windows Shell `CVE-2026-96951`	Mark of the Web 回避。ゼロデイ悪用(KEV)	10/13月例パッチ
Citrix NetScaler `CVE-2026-88771` / `88772`	9.5のRCEほか。Webシェル設置に悪用(CISA警告)	Citrix修正版
Arista VeloCloud Orchestrator `CVE-2026-114625`	SQLインジェクション。10/23 KEV追加	修正版
Tailscale SSH「Tailworm」 (研究者報告、CVE・修正なし)	SSHでポート転送を許可していると、1台の侵害から他サーバーのroot取得・横展開の恐れ。第三者再現なし、Tailscaleは調査中(公告未掲載)	SSHルールを1対1に絞る、ポート転送無効化、Tailnet Lock・node key期限を有効化
AWS SAM CLI `CVE-2026-115414`	Terraformフック利用時のコマンドインジェクション	1.166.2
Microsoft Authenticator(Android) `CVE-2026-80097`	悪意あるアプリが職場アカウントのトークンを取得しうる(8.6)	6.2606.4246 以降

Microsoft Teams	外部からの初回チャットにAIのフィッシング検知を導入予定(11〜12月、MC1519866)	外部アクセス設定の見直しは引き続き必要
LibreSSL CVE-2026-118374	**ocspcheck**コマンド(ライブラリ本体のlibssl/libcryptoではない)が、悪意あるOCSP応答者からの応答でメモリを枯渇させうる。4.4.0以下が対象。評価はGitHub Advisory「High」、CVSSベクタ計算では5.9(中)と情報源により差あり。悪用報告なし	本書時点で**修正版は未公開**。ocspcheckを自動実行するパイプラインは信頼できるOCSP応答者のみに絞る、または一時停止

3.9 第14版での追加(10/27〜29)

> 第19版からの継承・今回個別再検証なし。以下の版番号・悪用状況・件数・日付を今回の現時点確認済みと解釈しない。

対象	内容	対処
Oracle E-Business Suite CVE-2026-101767 9.8	TCFサーブレット(/OA_HTML/AppsTCFServer)の**未認証SQLインジェクション**。既定のURLファイアウォールを通過し、OSコマンド実行へつながる(Horizon3.ai)。12.2.3〜12.2.15。悪用報告なし	**2026年10月CPU**を適用。EBSをインターネットに公開しない
NGINX CVE-2026-42530(major)	HTTP/3(QUIC)モジュールのQPACK処理で解放後利用。**認証不要**でワーカー停止、条件次第でコード実行。1.31.0〜1.31.1のみ。なお nginx.org では以後も 1.31.7 / 1.30.6 までに中程度の修正が続く	**現行の 1.31.7 / 1.30.6 以上**へ。暫定: HTTP/3 を無効化
TeamViewer(TV-2026-1011) CVE-2026-92372 ほか	Linux/macOS版 Full Client の画面デコーダー境界外書き込み → 接続先から**RCE**。同時に macOS の権限昇格、整数オーバーフローも修正。別公告で IPC のアクセス制御不備(TV-2026-1010/1012)	**15.83 以上**。悪用は未確認
Google Chrome	Anthropic(10/27)の未公開研究モデルが、V8 → サンドボックス脱出までの**1クリック攻撃チェーン**を実験環境で構築。報告分は Google が **62 CVE(高・重大、うち13件はサンドボックス脱出)**として採番。**10/28には別の安定版更新(156.0.8078.73/.74)で52件(重大4件)を追加修正**(3.11)	**Chrome 156.0.8078.73 以上**。Edge等のChromium系も更新
UEFI(TianoCore EDK II) CVE-2026-97631 9.5	PXE(ネットワークブート)ドライバーが ICMP エラーを504バイト固定領域にコピーする際のバッファ超過。**ブート中に同じネットワークから1パケット**で起動停止、特定ビルド向けに作り込めば**Secure Boot前にコード実行**。2010年から存在。AMI・Insyde・Phoenix・Project Mu の基盤コード。悪用報告なし・KEV未掲載	EDK II は修正を main に統合済みだが**安定版未リリース**(10/28時点)。**サーバー各社のBIOS/UEFI更新を待って適用**、PXE不要なら無効化、ブート用ネットワークを分離。RHEL・SUSE・Debian の edk2 パッケージ(仮想マシン用)も未修正
Microsoft(eMudhra)	認証局 eMudhra の鍵漏えい(2.5)を受け、**eMudhra G3 ルート証明書を Windows の信頼リストから削除**	eMudhra系証明書の利用先は証明書の切り替えを
Cloudflare Workers AI(GLM-5.3)	8/27〜9/9、68万トークン超の長いプロンプトへの応答**155件に他の利用者のリクエスト内容が混入**。設定ミスと推論エンジン SGLang の不具合の組み合わせ。意図的な悪用の証拠なし、他モデルは影響なし(10/27公表)	Cloudflare側で修正済み。**SGLang を自前運用する組織は v0.5.22 以上**へ、KVキャッシュ容量とコンテキスト長の整合を確認

3.10 phpMyAdmin 5.2.3 — 未確認の脆弱性報告(研究者単独発表、CVE・PMASA未採番)

> 第19版からの継承・今回個別再検証なし。以下の版番号・悪用状況・件数・日付を今回の現時点確認済みと解釈しない。

> **信頼性の注意:** 以下はGitHubユーザー「abraxas」が2026年10月12日に公開した計10件の報告(1件のみ星9、他は星0)に基づく。**phpMyAdmin公式のセキュリティ情報(PMASA)・CVE番号は本書時点で一切存在しない**。第三者による再現・公式の反応も確認できていない。本書の著者が phpMyAdmin 5.2.3 のソースコード(WebAuthn処理・setup/validate.php)を独

自に確認したところ、2件については報告内容と矛盾しない挙動を確認したが、残りは報告者の説明のみに基づく。**9件中8件は、攻撃する前に正規の認証済みアカウントでのログインを必要とする**(残り1件のSSRFも、旧式のsetup/フォルダが削除されずに残っている場合に限られ、公式Dockerイメージ等では通常該当しない)。

内容(報告者の主張)	深刻度(報告者)	前提条件
WebAuthn 2段階認証の回避	高 8.1	要ログイン。著者による独自コード確認で、署名(signature)をCOSE鍵で検証していない疑いを確認
#1 認証プラグイン経由SQLi	高 8.1	要ログイン
#2 isSuperUserの判定残存	中 6.3	要ログイン
#3 CSRF起点のSQLi	高 8.1	要ログイン(CSRF経由)
#4 Designer機能のJSON経由SQLi	高 8.1	要ログイン
#5 central columns機能のSQLi	高 8.1	要ログイン
#6 LOAD DATA経由SQLi	中 6.5	要ログイン
#7 config/set 経由の2段階認証解除	高 8.1	要ログイン
#8 setup/validate.php の SSRF	高 7.2	著者確認: 当該ファイルは未認証で到達可能。ただし**旧式のsetupフォルダが残存している場合のみ**
#9 Designer機能の格納型XSS	高 8.0	要ログイン

対処の目安: phpMyAdminの管理アカウントを限定し外部公開しない(通常推奨される運用のまま)。setup/フォルダが残っている環境は削除。公式のPMASA発行・CVE採番を継続して確認する。

3.11 第16版での追加(10/29午後)

第20版調査差分（2026-11-01）: この追補はLinux TCP行のみ。他行は継承・個別再検証なし。識別子: CVE-2026-98432。確認範囲: Red Hat Critical/9.8、未認証遠隔からタイミング競合によるRCE可能性。公式影響説明はMPTCP限定ではない。対処: Red HatがIPオプションを含む通信の部分フィルター緩和を案内、完全防止不可。Ubuntu generic linuxは26.10/26.04/24.04/22.04でVulnerable work in progress。 悪用状況: 研究実証と実悪用は区別。今回実悪用/KEVは未確認。 未確認: 上流mboxはAnubis / 全RHEL errata / 全Ubuntu flavor / 上流修正版一覧 / 評価変更日時。根拠: 公式資料1 / 公式資料2 / 公式資料3

対象	内容	対処
Google Chrome CVE-2026-118306 / 118331 / 118348 / 118344 ほか	安定版 156.0.8078.73/.74(Windows/Mac)、.73(Linux)で**52件**を修正: 重大4件(FileSystemのメモリ破壊・FileAPI/Skiaの入力検証不備・Layoutの解放後利用)+高46+中2。うち CVE-2026-118320(V8のメモリ破壊)は高。報告者はAnthropic(Xinyang Ge+Claude)・OpenAI Codex Securityほか。詳細は一部非公開	「Chromeについて」から**156.0.8078.73以上**へ。Edge等のChromium系も更新
Cisco Secure Firewall(ASA/FTD) CVE-2026-76418 8.6	リモートアクセスSSL VPNのロジック誤り(tunnel groupで2次認証を設定している場合)。未認証の遠隔から細工リクエストで**装置が再起動しDoS**(CVSS 3.1 8.6、機密性・完全性への影響なし)。10/28公開。**10/29 CISA KEV追加**(Ciscoは今月初めに悪用を把握したと説明、攻撃者・被害組織数は非公表)	Ciscoアドバイザリ(cisco-sa-asaftd-tunnel-dos-s6mgkb75)で該当版を確認し修正。VPNの公開範囲を最小化
VMware ESX CVE-2026-41709(KEV)	不十分なログ出力 — 悪意ある管理者が証跡を残さず操作できてしまう。10/28 **CISA KEV追加**(対応期限 11/11)。深刻度は高くないが、実害(監査証跡の消失)を重視した掲載。**cybersecuritynews.comが悪用継続を報道(10/30)**	BroadcomのVMSA/パッチを確認・適用。ESXホストの管理者権限を棚卸し

Adobe Commerce / Magento CVE-2026-48356(KEV)	危険な種類のファイルの無制限アップロード。10/27 **CISA KEV追加**(期限 11/10)	Adobeのセキュリティ情報で該当版と修正を確認(管理画面を持つECサイト)
Linuxカーネル(TCP) CVE-2026-98432 9.8(開発元)	IPv4のSYN応答経路で**解放後利用**: 再送SYNとの競合で、TCPオプション(ireq_opt/inet_opt)の解放が読み取りと競合する。開発元kernel.orgのCVSS 3.1は9.8。**3.2で詳細更新(Anthropicのroot権限奪取実証、Ubuntu/RHEL修正状況)。**導入から長期間存在	3.2の公式調査差分参照。IPオプション通信の部分緩和は完全防止ではない。上流修正版一覧は今回未確認、製品別修正と再起動を確認。
Cloudflare /cdn-cgi/image/ (XSS連鎖、CVE未採番)	Searchlight Cyber(10/28)が実証した連鎖: ①SVG無害化ツール(svg-hush/xml-rs)が名前空間の属性値を無害化せず通す ②Chromiumのキャッシュ動作(`no-cache="Content-Security-Policy"`)で**CSPヘッダーを消す** ③/cdn-cgi/access/logout のリダイレクトで画像取得元の制限をすり抜ける → **利用サイトのドメイン上でスクリプト実行**。Cloudflareは全Webサイトの約24%の前面にある。Netlify Image CDN・S3/GCSの署名付きURLでも同種の成立性。**CVE未採番、公式の修正発表は本書時点で未確認**	画像配信元から Cache-Control 等のヘッダーを素通しさせない、`X-Content-Type-Options: nosniff`、画像取得先の許可範囲を見直す、オープンリダイレクトを閉じる
LocalStack CVE-2025-65200(参考)	開発用AWSエミュレータ。CloudFormationデプロイUIの未エスケープ出力による反射型XSS → Lambda機能で**ローカルコンテナでのコマンド実行へ格上げ**(研究者が2025年10月報告・12月公開)。対象UI自体は2025年10月に削除済み。**2025年の事件で、新規の悪用報告は確認できていない**。CVE番号がその後公開されたため今回確認	LocalStackを最新へ。開発ツールでも、localhostで動くサービスは**「ローカルでのコード実行」と同じ危険度**で扱う

3.12 第18版での追加(10/30)

> 第19版からの継承・今回個別再検証なし。以下の版番号・悪用状況・件数・日付を今回の現時点確認済みと解釈しない。

対象	内容	対処
Teltonikaルーター CVE-2026-82104(重大)	RutOS 7.22〜7.24.2・TswOS 1.9〜1.10を実行する産業用ルーター(RUT/RUTX/RUTM/RUTC/ATRM/TAP/CAP/OXA/DAP/TRB/OTD/EBG/SWM/TSWの全モデル)。HTTPSポート経由で**未認証のまま検査を回避し、任意コマンドを実行しうる**。Teltonika自身が10/30に開示(自社発見・公式対応)。悪用報告なし	**RutOS 7.24.3 / TswOS 1.10.1** へ更新。管理画面(443/tcp等)をインターネットに公開しない
Telegram(Android) 連鎖(CVE未採番)	NebuSec(10/29開示)。Telegram Androidアプリの脆弱性と、他2件のバグ(うち1件はAndroidの権限昇格)を**音声通話1本**で連鎖させ、着信に応答するだけで端末を完全乗っ取り(メッセージ・マイク・カメラ)。影響はバージョン8.6.2〜12.10.3(2022年3月〜2026年9月相当)の全範囲。ARM64実機で実証済み	**Telegram を 12.10.4 以上**へ更新(9月下旬リリース済み。未更新の端末が広く残存と推定)
Open VSX「Claude Code」偽装拡張機能	OpenSourceMalwareが発見。`anthropic.claude-code` バージョン2.1.313として配布された改ざん版が、起動時(Claude未使用でも)に動作しSSH公開鍵(`svc-telemetry`)を`~/.ssh/authorized_keys`へ追加、134.209.82.225への**リバースSSHトンネルで永続アクセス**を確立(macOS LaunchAgent・Linux cron・Windowsタスクで永続化)。Anthropic公式Marketplace配信自体の侵害は確認されていない	拡張機能の出所をOpen VSXでなく**公式(Anthropic/Microsoft Marketplace)で確認**。`authorized_keys`に`svc-telemetry`がないか点検、該当すれば隔離・認証情報ローテーション。詳細は5章参照
ServiceNow AI Platform CVE-2026-103093	管理者ロールを持つ認証済みユーザーが、Rhino JavaScriptサンドボックスの制限を回避しホストOS上で任意コード実行。ServiceNowが修正を配備、ホスト型インスタンスは適用済み。悪用報告なし	自己ホスト・パートナー提供インスタンスは最新パッチ(Yokohama P13 HF4a等)を確認・適用

本章の詳細な出典はURLは第10章「情報源」に掲載。

3.13 第19版での追加(10/31)

11月2日再確認・WordPress：7.1.4公式原文を今回取得。更新中のRCE、複数XSS、eMudhra対応を確認。4.7までの対象系列へのバックポートは進行中と記載。全旧系列完了としない。公式リリース本文には119977の識別子・18,500試行の数値がなく、後者は今回未確認。
https://wordpress.org/news/2026/10/wordpress-7-1-4/

11月2日再確認・ClickHouse：116366は26.3.62.3-lts／26.8.36.3-lts／26.9.27.3-stable／26.10.3.7-stable。Cloud/BYOC適用済みを確認。公式本文に具体発動条件・実悪用有無の確定説明はなく、旧「悪用報告なし」は最新保証としない。
https://clickhouse.com/docs/whats-new/security-changelog

11月2日再確認・Canonical LXD / MicroCloud：API到達と信頼済み公開証明書を用いる認証迂回条件を確認。LXD6.10.1／5.21.9／5.0.11／4.0.15、MicroCloud2.1.5／3.4.1、表のリリース日は10/29。
https://discourse.ubuntu.com/t/security-advisory-critical-vulnerability-found-in-canonical-lxd-and-microcloud/90557

11月2日再確認・Ivanti：Ivantiブログで限定的実悪用と更新・ICT推奨を確認。カナダ当局は104935、111357、118527のKEV掲載と25.1.1.3／25.1.3.1／22.8R2.6未満の対象を記載。ベンダー個別勧告の系列別対応表は未確認。
https://www.cyber.gc.ca/en/alerts-advisories/ivanti-security-advisory-av26-1035

11月1日の追確認：Canonical LXD/MicroCloudの公式は証明書連鎖の検証不備とLXD 4.0.15／5.0.11／5.21.9／6.10.1、MicroCloud 2.1.5／3.4.1の修正を確認。ClickHouse公式はCVE-2026-116366と26.3.62.3／26.8.36.3／26.9.27.3／26.10.3.7の修正、Cloud/BYOC修正適用を説明。Ivantiはカナダ当局の10月30日更新で2件のKEV追加を確認しましたが、ベンダーページの本文は取得できませんでした。WordPressの旧記載は今回公式本文を取得できず、再確認待ちです。
Canonical ／ ClickHouse ／ カナダ当局

第19版からの継承・今回個別再検証なし。以下の版番号・悪用状況・件数・日付を今回の現時点確認済みと解釈しない。

対象	内容	対処
Ivanti Connect Secure CVE-2026-111357 8.8 / CVE-2026-118527 4.3 (KEV)	既存の認証バイパス(CVE-2026-104935、CVSS 8.6)と組み合わせることで、**未認証の遠隔攻撃者がroot権限のコード実行まで到達可能**な連鎖を構成。Volexityが脅威アクター「**UTA0576**」による実悪用を確認・報告 — 認証情報窃取、Active Directoryメタデータの収集などの活動を観測。10/30 CISA KEVに追加	**22.8R2.6 / 25.1.1.3** 以上へ即時更新。侵害指標(IOC)に基づくフォレンジック調査を推奨(Volexityアドバイザリ参照)
WordPress Core CVE-2026-119977 8.1	コアの完全パッケージ更新処理中に生じる**競合状態(レースコンディション)**。更新ファイルの展開先ディレクトリ名が予測可能な時間帯に、未認証の攻撃者がアクセスし任意コード実行に至りうる。10/28リリースのWordPress 7.1.4で修正(他22件の脆弱性も同時修正)。**攻撃の成立条件(タイミング窓)は狭いが、Wordfenceは公開直後から短時間で1万8千件超の悪用試行を観測**したと報告 — 影響範囲の広さ(WordPressは全Webサイトの4割超で稼働)から注意喚起	**7.1.4**(各旧系統は対応するメンテナンス版)へ直ちに更新。自動更新を有効化
Canonical LXD CVE-2026-112816 10.0	HTTPSリスナーにおける**証明書検証の不備**。細工したTLS証明書チェーンを提示することで、攻撃者が任意の信頼済みクライアントとして認証されうる — LXDクラスタ・仮想マシンへの完全アクセスに直結しうるためCVSS満点。MicroCloud経由の構成も対象	**4.0.15 / 5.0.11 / 5.21.9 / 6.10.1** 以上へ更新。信頼済みクライアント証明書の棚卸しも推奨
ClickHouse Server CVE-2026-116366 9.5	整数オーバーフローに起因し、**特定条件下で未認証の遠隔コード実行**に至る恐れ(ClickHouse公式セキュリティ changelog で確認)。発動の具体的な条件は詳細非公開。本書時点で実悪用の報告なし	**26.10.3.7 / 26.9.27.3 / 26.8.36.3 / 26.3.62.3** 以上(各系統の最新安定版)へ更新

Progress WS_FTP Server CVE-2026-84295 10.0	不適切な認証処理により、**未認証の攻撃者が管理者権限の認証情報を窃取**しうる(Censysアドバイザリで確認)。過去にMOVEit等同種の企業向けファイル転送製品が大規模侵害の起点となった前例があり注意	ベンダーの修正パッチを確認・適用。管理画面のインターネット直接公開を避ける
WordPressプラグイン群(複数)	Gravity Forms(CVE-2026-103039 9.8、PHPオブジェクト注入・未認証、導入1,100万サイト超)、WooCommerce PDF Invoice(CVE-2026-109220、同種)ほか、同時期に複数のWordPressプラグインでPHPオブジェクト注入・権限昇格系の脆弱性が報告されている。個別の悪用確認は本書時点でなし	該当プラグインの利用有無を確認し、提供元の修正版へ更新。不要なプラグインは無効化・削除

本節で検討したが見送った項目: Chrome Mac版サンドボックス回避(CVE-2026-106378、3.9既出のChrome更新に包含)、TeamViewer整数オーバーフロー(CVE-2026-111585、3.9既出)、Arista VeloCloud Orchestrator SQLi(CVE-2026-114625、3.8既出・KEV対応中)、各種ニッチなIoT/ライブラリ脆弱性(新規の大規模悪用キャンペーンとの関連は本書時点で確認できず)。

2026年11月6日 追加確認（指定資料）

Windows Paint — CVE-2026-83844（MSRC一次情報）

MSRC は2026年10月13日公開。境界外読み取り（out-of-bounds read）により、未認証の攻撃者がネットワーク経由でコード実行可能。CVSS v3.1 **8.1**（AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H）、重要度 Important、Exploitability は「Exploitation Less Likely」、公開時点で「Exploited: No」。MSRCのFAQは「細工したパケットを影響サービスへ送る」と記載し、**0クリック／ファイルを開く経路と断定していない**。二次報道では修正版の表記が 11.2605.91.0 → 11.2609.401.0 と揺れ、Store配布版（11.2605.81.0）に関する管理者報告があるが、MSRC取得ページに修正バージョン表は確認できなかった。Copilot関与などの推測は採用しない。https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83844Cyber Security News（二次）

Barracuda Email Security Gateway — CVE-2026-116606／CVE-2026-111560（提供元公称）

Barracuda は2026年11月2日付で2件を公表。CVE-2026-116606 は事前認証の認可バイパス（ESGのみ、CVSS 9.3、認証不要だが**管理UIへの到達が必要**と2026-11-05に表現を修正）。CVE-2026-111560 はコマンドインジェクション（ESG/ADC/BMA/WCC/WAF/WSG、CVSS 8.6、管理者権限が必要）。連鎖によりroot到達。修正はESG 9.4.0.030以降。watchTowrが2026-11-05に実演を公表し、検出ツールを公開（エクスプロイトは未公開）。両CVEとも2026-11-06時点でCISA KEV未掲載、実攻撃の報告なし。https://trust.barracuda.com/security/pre-authentication-authorization-bypass-command-injectionThe Hacker News（二次）

Cloudflare WAF 2026-11-03 リリース（提供元公称）

PHP OOM 系（CVE-2026-109618／109619／115560）向けルール式の反復改善。Free Ruleset と Managed Ruleset の #2／#3 はいずれも Block→Block（検知更新）。Managed Ruleset に「phpMyAdmin - Authentication Bypass」を新規検知として **Disabled** で追加。PHP CTF の報告に基づく改善と記載。

https://developers.cloudflare.com/changelog/post/2026-11-03-waf-release/

4. インシデント ― 公式情報の再確認と統計

> **第26版の検証範囲：**本日の更新は統合集計・グラフ・CVE一覧の再生成、11月8〜9日に一次情報で確認できた事象（金融庁、CISA KEV追加、Chrome、Brotli波及の機器側告知）の追記に限定します。各ソフトウェア章の既存記述と「注目CVE」10件のNVD記録は第26版からの継承です。旧版内の「本日」「今回」は当時の調査を指します。

27件は指標数であり一意事故数ではありません。人数・画像・口座・報告件・資産額を合算しません。一意事故総数はnull。第20版からの継承と11月2日の本文再確認を列で区別します。公表日は取得日ではありません。

指標	値と単位	公表日	位置付け・今回確認	重複・解釈
GMO 影響の可能性があるサーバー	26,739 サーバー	2026-10-22	影響可能性／第20版から継承・本日個別再確認なし	人数・口座数・漏えいレコード数・一意事故数ではない
GMO 懸賞金サイトへの累計情報提供	735 情報提供件	2026-11-02	累計情報提供／今回の公式本文で再確認（画像内詳細などは別注記）	被害者・事故・漏えいレコードとは別。日別累計を合算しない
GMO 国内外70超の証券・FX会社に関する記述	未確認・単一集計なし	2026-10-24	留保付き採用／第20版から継承・本日個別再確認なし	70超は被害者数でも全社で不正操作確認済みという集計でもない
タイムズカー 基本情報の外部送信痕跡	6,628,007 アカウント情報件	2026-10-23	外部送信痕跡確認／今回の公式本文で再確認（画像内詳細などは別注記）	画像・属性情報・タイムズクラブ情報との重複あり。合算して人数を作らない
タイムズカー 暗号化本人確認画像の外部送信痕跡	1,464,800 画像データ件	2026-10-23	暗号化データ外部送信痕跡確認／今回の公式本文で再確認（画像内詳細などは別注記）	基本情報の対象アカウントに関する部分集合。画像閲覧・復号成功の確認ではない
タイムズカー 暗号化本人確認画像へのアクセスのみ	891,602 画像データ件	2026-10-23	アクセス痕跡・外部送信痕跡なし／今回の公式本文で再確認（画像内詳細などは別注記）	表④とは別区分だが、基本情報と重複。外部流出確定数に含めない
タイムズクラブ 連携サービスID	135,436 識別情報件	2026-10-23	外部送信痕跡確認／第20版から継承・本日個別再確認なし	同一アカウント・人物の他属性と重複し得る
タイムズクラブカード番号	19,510 識別情報件	2026-10-23	外部送信痕跡確認／今回の公式本文で再確認（画像内詳細などは別注記）	同一アカウント・人物の他属性と重複し得る
タイムズクラブ クレジットカード番号下4桁	28 識別情報件	2026-10-23	外部送信痕跡確認／第20版から継承・本日個別再確認なし	同一アカウント・人物の他属性と重複し得る
日本交通 漏えいした可能性のある対象者区分	未確認・単一集計なし	2026-10-30	漏えい可能性／本文の可能性・範囲を再確認。componentsの画像内概数は第20版調査から継承。	区分間の重複排除が確認できず、一意人数合計は非採用
ニチレイ 漏えい確認個人情報の表内件数合計	53,866 個人情報件	2026-09-18	漏えい確認／今回の公式本文で再確認（画像内詳細などは別注記）	表のレコード件数合計。ユニーク人数や全国事故数ではない
デジタル庁GSS 漏えいした可能性のある個人情報	246,000 個人情報件（約）	2026-09-12	漏えい可能性／今回の公式本文で再確認（画像内詳細などは別注記）	18.9万件と5.7万件。氏名・メール・電話などの属性別数は同一対象の重複で合算禁止。行政機関等の報告はPPC本系列の対象外
デジタル庁 Studio 事案の対象範囲表	未確認・単一集計なし	2026-10-22	漏えい可能性・精査中／今回の公式本文で再確認（画像内詳細などは別注記）	フォーム・アカウント間で人物重複があり得る。GSSとは別事案。全国事故数に合算しない

アサヒ 漏えいのおそれがある個人情報の表内概数合計	2,289,000 個人情報件（概数合計）	2026-07-17	漏えいのおそれ／今回の公式本文で再確認（画像内詳細などは別注記）	確認済み個人情報と重複あり。両者合算禁止。ユニーク人数ではない
アサヒ 漏えい確認個人情報の表内合計	115,513 個人情報件	2026-02-18	漏えい確認／第20版から継承・本日個別再確認なし	従業員5117件はおそれ側にも含まれると公式注記。取引先についても7/17おそれ表との重複排除を推定しない
HISタイ法人 流出した可能性のあるパスポート情報等	627 人（最大）	2026-10-07	流出可能性／今回の公式本文で再確認（画像内詳細などは別注記）	627人は対象者であり、事故数・レコード数ではない
Binance 盗難トークン資産の概算額	6,300,000,000 米ドル（約）	2026-10-30	調査継続中の当事者推計／第20版から継承・本日個別再確認なし	資産盗難額であり顧客の確定損失・被害人数ではない
Binance 被害対象資産の補填率	95 パーセント（約）	2026-11-01	進捗・当事者発表／今回の公式本文で再確認（画像内詳細などは別注記）	被害者の95%に返金ではない。対象資産量の補填進捗
Binance事件に対するFBIの帰属判断	未確認・単一集計なし	日付未確認	公式確認／第20版から継承・本日個別再確認なし	金額推計や技術原因とは別の判断
Polymarket 流出資金	2,700,000 米ドル	日付未確認	公式返金方針・進捗／今回の公式本文で再確認（画像内詳細などは別注記）	流出270万と停止関連120万を区別。総額390万に再加算しない
Polymarket 停止関連損失への返金	1,200,000 米ドル	日付未確認	公式返金方針・進捗／今回の公式本文で再確認（画像内詳細などは別注記）	流出270万と停止関連120万を区別。総額390万に再加算しない
Polymarket 返金総額	3,900,000 米ドル	日付未確認	公式返金方針・進捗／今回の公式本文で再確認（画像内詳細などは別注記）	流出270万と停止関連120万を区別。総額390万に再加算しない
Polymarket 返金済み対象ウォレット割合	95 パーセント	日付未確認	返金進捗／今回の公式本文で再確認（画像内詳細などは別注記）	対象ウォレット割合。ユニーク人数・資産補填率ではない
Polymarket 710ウォレットという旧記述	未確認・単一集計なし	2026-10-29	公式集計としては不採用／第20版から継承・本日個別再確認なし	ウォレット数を人数に換算しない
PPC 不正アクセスによる漏えい等の延べ本人数	260,000,000 延べ人（約）	2026-10-28	速報・おそれ含む／今回の公式本文で再確認（画像内詳細などは別注記）	同一事象について委託先・委託元双方が報告する場合がある。各事案や延べ人数と加算禁止。一意事故数ではない。
PPC 月別速報報告件数の表内合計	2,094 報告件	2026-10-28	速報／今回の公式本文で再確認（画像内詳細などは別注記）	同一事象について委託先・委託元双方が報告する場合がある。各事案や延べ人数と加算禁止。一意事故数ではない。
旧版の昨年度確定値 1256件	未確認・単一集計なし	日付未確認	未確認・不採用／第20版から継承・本日個別再確認なし	比較母集団と期間が未検証

統計の出典・期間・今回の確認範囲

PPC 不正アクセス漏えい等の月別速報報告件数：2026-04〜2026-10-16／個人情報取扱事業者からPPCへ直接報告された、不正アクセスによる個人データ漏えい等の速報受付月別報告件数。委任先省庁経由（金融業・電気通信業等）と行政機関等を除外。実漏えいとおそれを含む。／7か月の数値・対象と重複注記を本日原文再確認。

https://www.ppc.go.jp/files/pdf/261028_sankoushiryou-2.pdf

金融庁 証券口座の不正アクセス件数：2025-01〜2026-09／各証券会社等から報告された発生日ベースの暫定値。不正取引件数は不正アクセス件数のうち不正取引まで行われた件数。／公式ランディングの対象期間と10/9更新を再確認。全点数表は第20版継承。

https://www.fsa.go.jp/ordinary/chuui/chuui_phishing/20261009.pdf

金融庁 証券口座の不正取引件数：2025-01〜2026-09／各証券会社等から報告された発生日ベースの暫定値。不正取引件数は不正アクセス件数のうち不正取引まで行われた件数。／公式ランディングの対象期間と10/9更新を再確認。全点数表は第20版継承。

https://www.fsa.go.jp/ordinary/chuui/chuui_phishing/20261009.pdf

警察庁 ランサムウェア被害報告件数・年次：2021〜2025／企業・団体等のランサムウェア被害の警察への報告件数。ノーウェアランサムは別系列。／既存数表を継承。正誤表の対象は特殊詐欺図表10でありランサム図ではないことを本日確認。

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf

警察庁 ランサムウェア被害報告件数・半期：2020-H2〜2026-H1／企業・団体等のランサムウェア被害報告件数。2020年下半期からの統計。／既存数表を継承。正誤表の対象は特殊詐欺図表10でありランサム図ではないことを本日確認。

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R8kami/R08_kami_cyber_jousei.pdf

警察庁 ノーウェアランサム被害報告件数・年次：2023〜2025／暗号化せず窃取情報の公開等で対価を要求するノーウェアランサムの被害報告。2023上半期から集計。／既存数表を継承。正誤表の対象は特殊詐欺図表10でありランサム図ではないことを本日確認。

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf

事案別出典と区分別補足

- GMO 影響の可能性があるサーバー：https://group.gmo/info/alert/20261022/
- GMO 懸賞金サイトへの累計情報提供：https://group.gmo/info/alert/2026102902/
- GMO 国内外70超の証券・FX会社に関する記述：https://group.gmo/info/alert/20261024/
- タイムズカー 基本情報の外部送信痕跡：https://share.timescar.jp/news/2026/1023/1825.html
- タイムズカー 暗号化本人確認画像の外部送信痕跡：https://share.timescar.jp/news/2026/1023/1825.html
- タイムズカー 暗号化本人確認画像へのアクセスのみ：https://share.timescar.jp/news/2026/1023/1825.html
- タイムズクラブ 連携サービスID：https://share.timescar.jp/news/2026/1023/1825.html
- タイムズクラブカード番号：https://share.timescar.jp/news/2026/1023/1825.html
- タイムズクラブ クレジットカード番号下4桁：https://share.timescar.jp/news/2026/1023/1825.html
- 日本交通 漏えいした可能性のある対象者区分：https://nihon-kotsu-hire.jp/news/261030/
- ニチレイ 漏えい確認個人情報の表内件数合計：https://www.nichirei.co.jp/news/2026/524.html
- デジタル庁GSS 漏えいした可能性のある個人情報：https://www.digital.go.jp/press/5fc99139-a4e2-4b7b-8b0c-d475e926143f
- デジタル庁 Studio事案の対象範囲表：https://www.digital.go.jp/press/a0a8f66c-b32d-4695-9372-bcd5d4280f22
- アサヒ 漏えいのおそれがある個人情報の表内概数合計：https://www.asahigroup-holdings.com/newsroom/detail/20260717-0101.html
- アサヒ 漏えい確認個人情報の表内合計：https://www.asahigroup-holdings.com/newsroom/detail/20260218-0101.html
- HISタイ法人 流出した可能性のあるパスポート情報等：https://www.his.co.jp/assets/20261007.pdf
- Binance 盗難トークン資産の概算額：https://www.binance.com/en/support/announcement/detail/d3306d9dca5243548c813b605e1d1751
- Binance 被害対象資産の補填率：https://www.binance.com/en/support/announcement/detail/73911fb819b240f88b88256bdd318eda

- Binance事件に対するFBIの帰属判断：https://www.fbi.gov/investigate/cyber/alerts/2026/north-korea-responsible-for-6-billion-binance-attack
- Polymarket 流出資金：https://status.polymarket.com/cmvvek1i90eme14ruga1z6tuj
- Polymarket 停止関連損失への返金：https://status.polymarket.com/cmvvek1i90eme14ruga1z6tuj
- Polymarket 返金総額：https://status.polymarket.com/cmvvek1i90eme14ruga1z6tuj
- Polymarket 返金済み対象ウォレット割合：https://status.polymarket.com/cmvvek1i90eme14ruga1z6tuj
- Polymarket 710ウォレットという旧記述：https://www.cnbc.com/2026/10/29/polymarket-reports-outage-on-international-exchange-halts-trading.html
- PPC 不正アクセスによる漏えい等の延べ本人数：https://www.ppc.go.jp/files/pdf/261028_sankoushiryou-2.pdf
- PPC 月別速報報告件数の表内合計：https://www.ppc.go.jp/files/pdf/261028_sankoushiryou-2.pdf
- 旧版の昨年度確定値1256件：公式根拠未確認

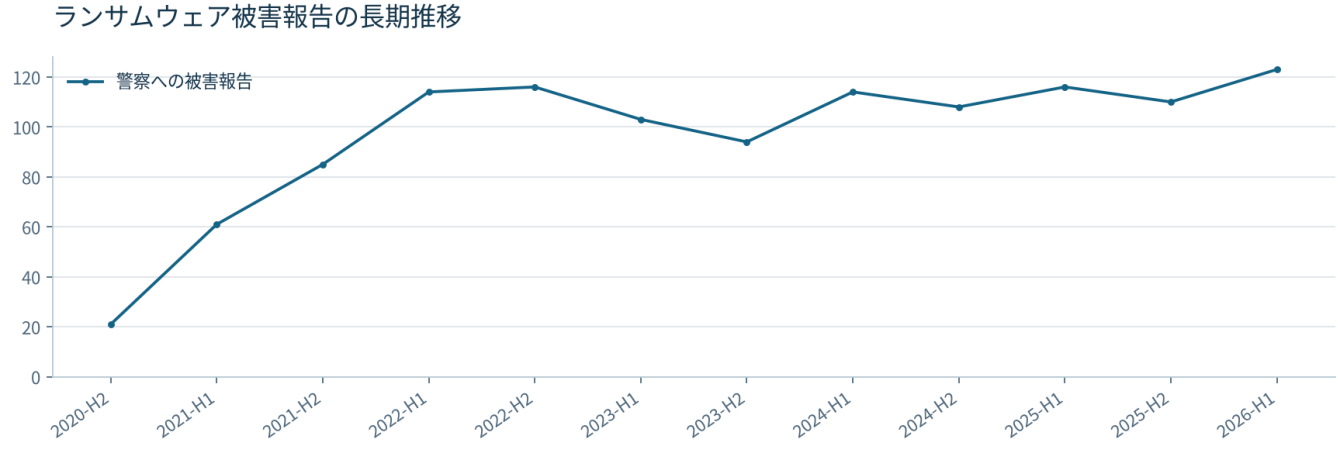
日本交通 漏えいした可能性のある対象者区分：ハイヤーのお客様 13,100、乗務員・職員 60,100、採用応募者 107,900、従業員家族 37,700、取引先担当者 2,100、事故等の相手方 72,000。区分間重複の排除なし。合算して一意人数にしません。

ニチレイ 漏えい確認個人情報の表内件数合計：配送先 3,308、取引先役職員 6,849、従業員・家族・求職者 43,709。区分間重複の排除なし。合算して一意人数にしません。

デジタル庁 Studio事案の対象範囲表：一般意見 最大8,833、採用問合せ 最大250、接種証明書アプリ 最大3,661、着ぐるみ借用 最大117、参加関連 最大462、Studioアカウント 記載件数35。区分間重複の排除なし。合算して一意人数にしません。

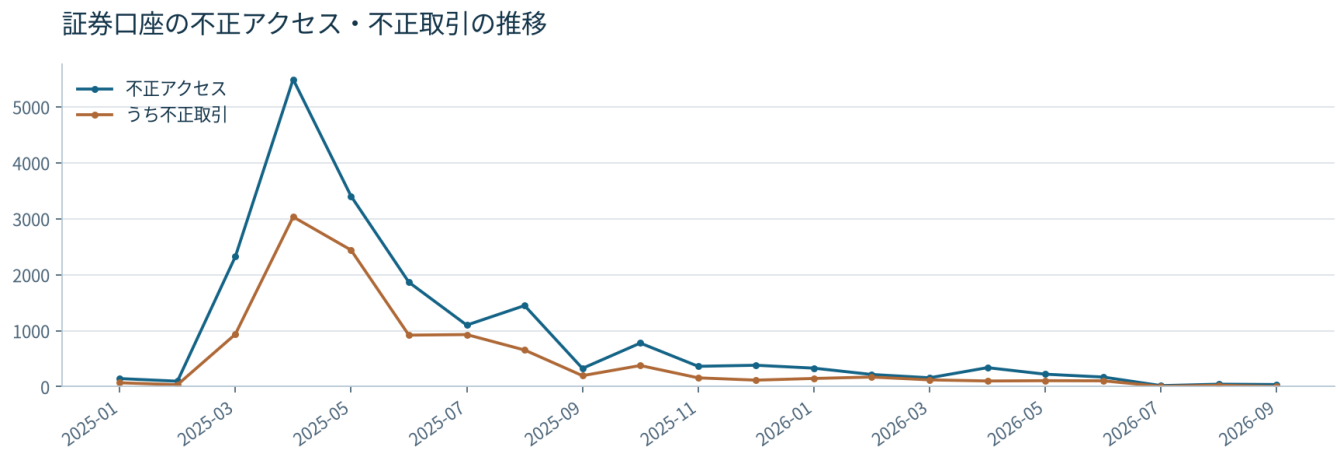
アサヒ 漏えいのおそれがある個人情報の表内概数合計：お客様相談室 1,525,000、慶弔対応先 117,000、従業員 107,000、従業員家族 162,000、取引先等 378,000。区分間重複の排除なし。合算して一意人数にしません。

> ニチレイの一括抽出回答は原文と不一致だったため不採用。原文の9/18第7報・3,308＋6,849＋43,709＝53,866個人情報件を使用。警察庁の正誤表は特殊詐欺の図表10が対象。過去ランサム数表の全点再検証とはしません。



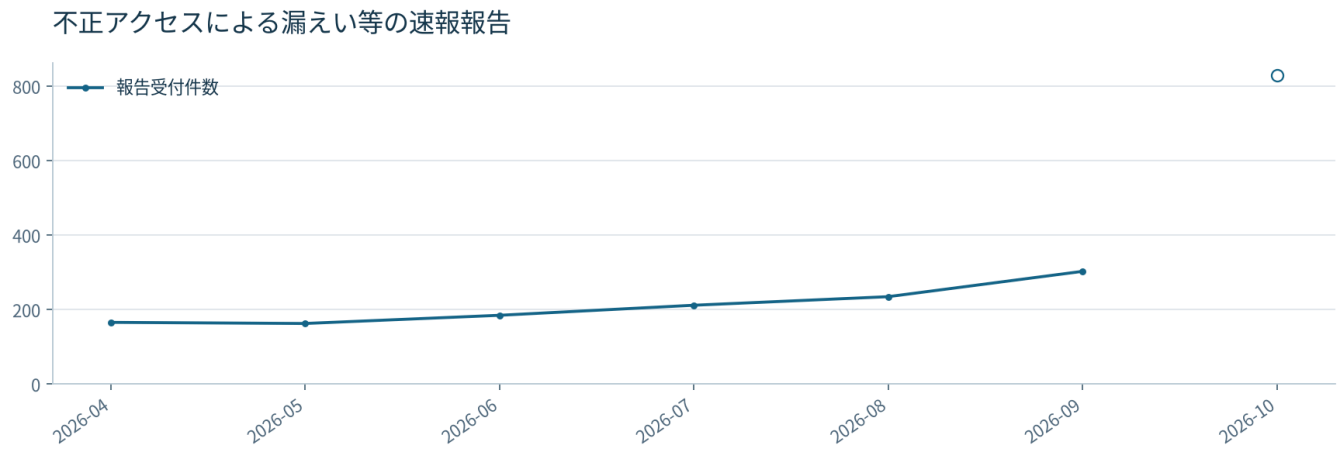
警察庁・半期別。ノーウェアランサムとは別系列。全国の実発生総数ではない。

Web・PDF共通画像。期間・指標・継承範囲は本章参照。



金融庁・発生日ベース暫定値。不正取引はアクセスの内数。因果効果は未判定。

Web・PDF共通画像。期間・指標・継承範囲は本章参照。



個人情報保護委員会。2026年10月は16日までの部分集計。事故発生月・一意事故数ではない。

Web・PDF共通画像。期間・指標・継承範囲は本章参照。

2026年11月7日〜8日の新規確認（第26版）

本節は、前版（11月7日20:00基準）以降に**提供元の一次情報**で確認できた事象のみを掲載します。確認できなかった論点は「未確認」と明記し、推測で補いません。

1. 金融庁「現下の情勢を踏まえた金融機関利用者へのお願い」（2026年11月6日）

金融庁は11月6日、顧客向けサービス・業務システムへの不正アクセスと顧客情報の漏洩が相次いでいることを踏まえ、金融機関利用者向けの注意喚起を公表しました。同日、サイバーセキュリティに関する関係閣僚会議が**「サイバーセキュリティ緊急対策パッケージ」**を決定したことが本文に明記されています。利用者への具体的な依頼は、メール内リンクを安易にクリックしないこと、パスワードの使い回しをしないこと、**フィッシング耐性のある多要素認証**の利用、身に覚えのない取引通知があった場合の金融機関への速やかな連絡、の4点です。

読み方：本件は新規の脆弱性（CVE）の公表ではなく、**漏洩済み情報を起点とした二次被害（なりすましメール・フィッシング）への注意喚起**です。当サイトのCVE集計には計上されません。10月9日公表の金融機関向け対策要請とあわせ、**9月以降の国内漏洩事案が利用者側の運用（MFA・連絡体制）に影響を及ぼしている**ことを示す一次情報として扱います。https://www.fsa.go.jp/news/r8/sonota/20261106/20261106.html

2. CISA KEV の新規追加（2026年11月7日以降、当日取得カタログ）

当日取得したKEVカタログに、dateAdded が 2026-11-07 以降の新規項目は**確認できませんでした**（取得カタログの最終更新は 2026-11-06T19:44:45.1797Z）。「追加がなかった」ことは「新たな悪用がない」ことを意味しま

せん。

3. Brotli（CVE-2026-111497）の機器側波及 ― Neat の告知（NEAT-SA-2026-11-02）

Google Brotli のデコーダに存在する境界外書き込み（CWE-787）は、Brotli 1.0.3〜1.2.0 が影響を受け、1.0.10／1.1.1／1.2.1 で修正されます。CISA は 2026年10月27日付で KEV に掲載しています。会議室端末ベンダーの Neat は11月2日付の告知で、NeatOS が Neat Browser（Neat Open Apps）とキャプティブポータル経由で当該ライブラリを使用していると説明し、**NeatOS 26.6.3 を11月21日までに段階配信**（11月7日開始）するとしています。CVSS は v4.0 9.2（Google評価）／v3.1 8.1（AC:H）、Neat 自身の評価は High です。

読み方：ライブラリ脆弱性が**組込み機器のファームウェア更新待ち**という形で運用負荷になる典型例です。Neat は「自社製品・顧客への悪用の証拠はない」としつつ、緩和として eMudhra 中間CA問題の修正を先行適用すること、キャプティブポータルを避けること、Neat Browser の利用を制限することを挙げています。**ベンダーの「悪用の証拠なし」は、KEV掲載（悪用の証拠あり）と矛盾するものではなく、対象範囲が異なる発言です。**

https://support.neat.no/article/security-advisory-november-2026-brotli-decoder-vulnerability-cve-2026-111497-affecting-neat-devices/

4. Google Chrome の更新（2026年11月3日 Stable／11月4日 Early Stable）

Chromium 公式ブログの2026年11月一覧で、11月3日付「Stable Channel Update for Desktop」、11月4日付「Early Stable Update for Desktop」の公開を確認しました。**本版では各記事本文を取得していないため、修正件数・CVE番号・深刻度は記載しません。**前版までに扱った Chrome の修正内容は継承です。

https://chromereleases.googleblog.com/2026/

5. 今回確認できなかった事項

- Microsoft 11月 Patch Tuesday の先行情報：MSRC の当月アドバイザリ本文を本版で取得できていません（11月の定例更新日は通常第2火曜で、本基準日時より後です）。件数・CVEは記載しません。
- Ivanti／Fortinet／Cisco／VMware／Citrix／SAP／Atlassian／WordPress主要プラグインの11月7〜8日付の新規告知：今回の検索で**当該日付の一次情報を特定できませんでした**。各章の記述は第26版以前の継承です。
- AIサービス・エージェント基盤の新規CVE、モデル配布物のサプライチェーン事案：11月7〜8日付の一次情報を確認できませんでした。プロンプトインジェクションの実害事例として引用できる新規の一次情報も得られていません。

> 本節の日付はすべて提供元ページの記載に基づきます。二次情報（報道・集約サイト）のみで確認した事項は掲載していません。

2026年11月8日〜9日の新規確認（第26版）

本節は、前版（11月7日20:00基準）以降に**提供元の一次情報**で確認できた事象のみを掲載します。確認できなかった論点は「未確認」と明記し、推測で補いません。

1. 金融庁「現下の情勢を踏まえた金融機関利用者へのお願い」（2026年11月6日）

金融庁は11月6日、顧客向けサービス・業務システムへの不正アクセスと顧客情報の漏洩が相次いでいることを踏まえ、金融機関利用者向けの注意喚起を公表しました。同日、サイバーセキュリティに関する関係閣僚会議が**「サイバーセキュリティ緊急対策パッケージ」**を決定したことが本文に明記されています。利用者への具体的な依頼は、メール内リンクを安易にクリックしないこと、パスワードの使い回しをしないこと、**フィッシング耐性のある多要素認証**の利用、身に覚えのない取引通知があった場合の金融機関への速やかな連絡、の4点です。

読み方：本件は新規の脆弱性（CVE）の公表ではなく、**漏洩済み情報を起点とした二次被害（なりすましメール・フィッシング）への注意喚起**です。当サイトのCVE集計には計上されません。10月9日公表の金融機関向け対策要請とあわせ、**9月以降の国内漏洩事案が利用者側の運用（MFA・連絡体制）に影響を及ぼしている**ことを示す一次情報として扱います。https://www.fsa.go.jp/news/r8/sonota/20261106/20261106.html

2. CISA KEV の新規追加（2026年11月7日以降、当日取得カタログ）

当日取得したKEVカタログに、dateAdded が 2026-11-07 以降の新規項目は**確認できませんでした**（取得カタログの最終更新は 2026-11-06T19:44:45.1797Z）。「追加がなかった」ことは「新たな悪用がない」ことを意味しません。

3. Brotli（CVE-2026-111497）の機器側波及 ― Neat の告知（NEAT-SA-2026-11-02）

Google Brotli のデコーダに存在する境界外書き込み（CWE-787）は、Brotli 1.0.3〜1.2.0 が影響を受け、1.0.10／1.1.1／1.2.1 で修正されます。CISA は 2026年10月27日付で KEV に掲載しています。会議室端末ベンダーの Neat は11月2日付の告知で、NeatOS が Neat Browser（Neat Open Apps）とキャプティブポータル経由で当該ライブラリを使用していると説明し、**NeatOS 26.6.3 を11月21日までに段階配信**（11月7日開始）するとしています。CVSS は v4.0 9.2（Google評価）／v3.1 8.1（AC:H）、Neat 自身の評価は High です。

読み方：ライブラリ脆弱性が**組込み機器のファームウェア更新待ち**という形で運用負荷になる典型例です。Neat は「自社製品・顧客への悪用の証拠はない」としつつ、緩和として eMudhra 中間CA問題の修正を先行適用すること、キャプティブポータルを避けること、Neat Browser の利用を制限することを挙げています。**ベンダーの「悪用の証拠なし」は、KEV掲載（悪用の証拠あり）と矛盾するものではなく、対象範囲が異なる発言です。**

https://support.neat.no/article/security-advisory-november-2026-brotli-decoder-vulnerability-cve-2026-111497-affecting-neat-devices/

4. Google Chrome の更新（2026年11月3日 Stable／11月4日 Early Stable）

Chromium 公式ブログの2026年11月一覧で、11月3日付「Stable Channel Update for Desktop」、11月4日付「Early Stable Update for Desktop」の公開を確認しました。**本版では各記事本文を取得していないため、修正件数・CVE番号・深刻度は記載しません。**前版までに扱った Chrome の修正内容は継承です。

https://chromereleases.googleblog.com/2026/

5. 今回確認できなかった事項

- Microsoft 11月 Patch Tuesday の先行情報：MSRC の当月アドバイザリ本文を本版で取得できていません（11月の定例更新日は通常第2火曜で、本基準日時より後です）。件数・CVEは記載しません。
- Ivanti／Fortinet／Cisco／VMware／Citrix／SAP／Atlassian／WordPress主要プラグインの11月8〜9日付の新規告知：今回の検索で**当該日付の一次情報を特定できませんでした**。各章の記述は第26版以前の継承です。
- AIサービス・エージェント基盤の新規CVE、モデル配布物のサプライチェーン事案：11月8〜9日付の一次情報を確認できませんでした。プロンプトインジェクションの実害事例として引用できる新規の一次情報も得られていません。

> 本節の日付はすべて提供元ページの記載に基づきます。二次情報（報道・集約サイト）のみで確認した事項は掲載していません。

2026年11月8日〜9日の新規確認（第26版）

本節は前版（11月8日18:00基準）以降に**提供元の一次情報**、または出典を明示できる二次情報で確認できた事象のみを掲載します。確認できなかった論点は「未確認」と明記します。

1. Microsoft 11月 Patch Tuesday ― 予告段階（基準日時点で未公開）

Microsoftの月次セキュリティ更新の定例日は**11月10日（第2火曜）**で、本基準日時（11月9日14:15 JST）より後です。基準日時点でMSRCの11月アドバイザリは公開されておらず、**件数・CVE番号・深刻度・悪用状況は一切記載しません。**公表後に判明した内容を先取りして書くことはしません。11月分の評価は次版以降で行います。

2. CISA KEV の新規追加（2026年11月8日以降、当日取得カタログ）

当日取得したKEVカタログ（2026.11.06、1,769件、最終更新 2026-11-06T19:44:45.1797Z）に、dateAdded が 2026-11-08 以降の新規項目は**確認できませんでした**。カタログの最終更新日が基準日より前であるため、**「追加が**

なかった」ことは「新たな悪用がない」ことを意味しません。

3. 警察庁と全国警察による合同捜査本部の設置（11月6日）― 二次情報

企業・組織へのサイバー攻撃による個人情報流出が相次いでいることを受け、警察庁が11月6日にサイバー特別捜査部と47都道府県警による合同捜査本部を設置した、と複数の報道が伝えています。**本版では警察庁の報道発表本文を取得できていないため、これは二次情報（報道）として扱い、事案の内容・被害規模・攻撃元についての断定は行いません。**10月9日・11月6日の金融庁の注意喚起、10月7日の個人情報保護委員会の注意喚起とあわせ、**国内の漏洩事案が捜査体制と利用者保護の両面に波及している**ことの傍証として位置づけます。

4. 今回確認できなかった事項（記載していない）

- Ivanti／Fortinet／Cisco／Apache／PHP／OpenSSL／Linuxカーネル／GitLab／Tomcat／VMware／Citrix／SAP／Atlassian／WordPress主要プラグイン／Chrome／Firefox／Adobe の11月8〜9日付の新規アドバイザリ：当該日付の一次情報を特定できませんでした。各章の記述は第25版以前の**継承**です。
- 国内企業の新規漏洩事案の一次公表：基準日時までの新規公表を確認できませんでした。
- AIサービス・エージェント基盤の新規CVE、プロンプトインジェクションの新規実害一次情報、モデル配布物のサプライチェーン事案：いずれも確認できませんでした。

> 本節の日付は提供元ページの記載、または報道日付に基づきます。二次情報のみの項目はその旨を明記しました。攻撃コードの再現手順・実アドレス値は掲載しません。

5. AIコーディングエージェントのリスク

> **第26版の検証範囲：**本日の更新は統合集計・グラフ・CVE一覧の再生成、11月8〜9日に一次情報で確認できた事象（金融庁、CISA KEV追加、Chrome、Brotli波及の機器側告知）の追記に限定します。各ソフトウェア章の既存記述と「注目CVE」10件のNVD記録は第26版からの継承です。旧版内の「本日」「今回」は当時の調査を指します。

> **11月2日再確認・AIエージェント防御：**OpenAI公式は外部入力の分類だけに頼らず、送信・操作側の制約で被害を限定する設計を説明。内部コーディングエージェントの監視は完了後30分以内の非同期であり、全危険操作を事前遮断する仕組みではない。偽陰性率は確定できないと明記。旧個別被害事例全件の裏取りではない。
> https://openai.com/index/designing-agents-to-resist-prompt-injection/

> 第19版からの継承・今回個別再検証なし。以下の説明・統計・制度施行日・金額等を今回確認済みとはしない。

5.1 ダウンロードフォルダの AGENTS.md / CLAUDE.md による乗っ取り(実害観測)

第19版からの継承・今回個別再検証なし。

Forever Security(10/22)が顧客PCで観測: OpenAI Codex が悪性npmパッケージ `function-color` を入れようとしたのを阻止し、指示元をたどると `~/Downloads` に置かれた**「開発ガイドライン」に偽装した AGENTS.md** だった。ブラウザ設定によっては、Webサイトはクリックなしでテキストファイルをダウンロードフォルダへ保存でき、OSの保護も働かない。

エージェント	実証された手口
Codex	`~/.codex/config.toml` にMCPサーバーを追記させ、承認・サンドボックスを外して実行(試験で9割超成功)。**以後どのフォルダで起動しても攻撃者のコマンドが走る**
Claude Code	研究者の実証: `.claude/settings.json` に `ANTHROPIC_BASE_URL` を書かせ、通信を迂回して**ログイントークンを窃取**(書き込み成功 約5割)

同社の観測では利用者の約半数がダウンロードフォルダでエージェントを動かしていた。研究者は「ベンダーが直せる欠陥ではなく仕様の組み合わせ」とし、**運用で防ぐ必要がある**(Windows・macOS・Linux共通)。

対策

1. **ダウンロードフォルダ・ホーム直下でエージェントを起動しない。** 空のフォルダか、git管理の自分のプロジェクトだけで起動。
2. 自分が書いていない AGENTS.md / CLAUDE.md は先に読む(clone直後のリポジトリも)。
3. 設定を点検: `~/.codex/config.toml` の覚えのない `[mcp_servers.*]`・`chatgpt_base_url`、`.claude/settings.json` の覚えのない `ANTHROPIC_BASE_URL`・プロキシ。
4. **承認とサンドボックスはオンのまま。** 外すよう求める指示は攻撃のサイン。
5. 見つけたら**トークンを失効・再発行**。function-color が入ったPCは侵害済み扱い(指示ファイルを消しても書き換えられた設定は残る)。
6. Chrome: 設定 → ダウンロード →「**ダウンロード前に各ファイルの保存場所を確認する**」をオン(Edgeも同様)。

5.2 指示ファイルが古いとエージェントはそれに従う(arXiv:2610.30571)

第19版からの継承・今回個別再検証なし。

指示ファイルと既存コードが矛盾する40プロジェクトで、Claude Code・Codex CLIは計320実行の**90.1%で古い指示ファイルに従った**(矛盾に気づいていても)。セキュリティ修正をエージェントに任せると、古い設計書どおりに設定を巻き戻す恐れがある。**指示ファイルを資産として棚卸し・レビューし、エージェントの変更はテスト・レビュー経由で取り込む。**

5.3 検索を「判定問題」にする DecisionRAG(arXiv:2610.35868、研究動向)

第19版からの継承・今回個別再検証なし。

リトリーバル(RAGの検索段階)を、トークンを生成せずに候補の分岐を1回の順伝播で判定する「決定モデル」で行う手法(10/26公開)。タスク固有の学習も1段目のリトリーバーも不要で、268万段落のコーパスでも1クエリ0.7〜1.8秒。密ベクトル検索+8Bリランカーの構成に対し、MultiDoc2Dial の R@1 で+13.8、Natural Questions の Hit@1 で+17.4。エージェントが知識・手順を探す速度と精度がさらに上がる方向で、防御側のナレッジ照会にも攻撃調査の高速化にも効く。脆弱性情報そのものではないため、動向としての記載にとどめる。

5.4 Open VSX の偽装「Claude Code」拡張機能 — SSHバックドア

第19版からの継承・今回個別再検証なし。

OpenSourceMalwareが発見・解析(10/30公表)。Open VSXで配布されていた `anthropic.claude-code` バージョン2.1.313は、正規の拡張機能バンドルの前に66行のJavaScriptローダーが挿入された改ざん版。**Claude Codeで会話を始めなくても、拡張機能が有効化された時点で悪性コードが動く。**解析対象はmacOS(Apple Silicon)だがLinux・Windows向けの分岐コードも確認された。

- 攻撃者のEd25519公開鍵(コメント `svc-telemetry`)を `~/.ssh/authorized_keys` に追加し、`134.209.82.225` へのリバースSSHトンネル(ローカル22番ポートへの転送)を確立。60秒間隔で再接続。
- 永続化: macOSは `com.apple.sysmond.plist`という名のLaunchAgent(Appleの正規コンポーネントではない)、Linuxは`@reboot` cron、Windowsはタスクスケジューラ(SYSTEM権限)またはスタートアップフォルダ。
- ホスト名・ユーザー名・OS・Gitメールアドレス・環境変数名(最大40件、値は含まず)を収集し134.209.82.225:8099へ平文HTTPで送信。
- **Anthropic公式のVisual Studio Marketplace配信自体が侵害された証拠はない** — 改ざん経路(サプライチェーンのどこで混入したか)は本書時点で未特定。

対策

1. `~/.ssh/authorized_keys` に `svc-telemetry` というコメントの鍵がないか確認。あれば削除し、侵害端末として扱う。
2. 該当プラットフォームのLaunchAgent・cron・タスクスケジューラの永続化痕跡(上記ファイル名)を点検・除去。
3. 拡張機能は**公式マーケットプレイス(Anthropic/Microsoft)から取得**し、Open VSX上の同名パッケージは出所を確認してから導入(6章「使うときのルール」と同じ考え方)。
4. 侵害が疑われる端末は認証情報を別端末からローテーション、ネットワークログでポート22・8099への不審な通信を確認。

6. セキュリティ特化 Agent Skills — 公式リポジトリの使い方

> **第26版の検証範囲：**本日の更新は統合集計・グラフ・CVE一覧の再生成、11月8〜9日に一次情報で確認できた事象（金融庁、CISA KEV追加、Chrome、Brotli波及の機器側告知）の追記に限定します。各ソフトウェア章の既存記述と「注目CVE」10件のNVD記録は第26版からの継承です。旧版内の「本日」「今回」は当時の調査を指します。

> 第19版からの継承・今回個別再検証なし。以下の説明・統計・制度施行日・金額等を今回確認済みとはしない。

Cloudflare・Anthropic・OpenAI・NVIDIA・Google・Alibaba が、AIエージェント(Claude Code・Codex・OpenCode 等)から使える**セキュリティ用のスキル・ツールを公式リポジトリで公開**している。本書の対処(依存ライブラリの棚卸し、PHPの版確認、自社コードの監査)をエージェントに手伝わせる際は、**このリストの公式版から取得**する。7件とも GitHub API で各社の公式組織アカウント配下であることを確認した(10/28)。

提供元 / リポジトリ	何をするか	本書での使いどころ	注意(公式の記載を含む)
Google `google/osv-scanner`	依存関係(11以上の言語・19種以上のロックファイル)とコンテナイメージをOSVデータベースと照合。ライセンス確認、修正版の提案	**まず最初に**: Brotli・jackson・LiteLLM 等が自分の依存に入っていないか。CIに常設	修正提案(fix)は信頼できないプロジェクトでパッケージマネージャのスクリプトを実行しうる
OpenAI `openai/php2shell-checker`	URLのヘッダ、またはサーバー上のPHP版から php2shell の影響可能性を判定(OK / POTENTIALLY VULNERABLE / UNKNOWN)。Codexにスキルとして導入可	2.1 PHP の版確認	**版数だけの判定**。ディストリのバックポートは見えない、ヘッダ非表示は UNKNOWN。自分の管理サイトにのみ使う
NVIDIA `NVIDIA/SkillSpector`	エージェント用スキルを**導入前に検査**(脆弱性・悪性パターン)。OpenCode・Pi拡張、MCP対応。NVIDIA Verified Skills の検査工程	**他のスキルを入れる前の関門**(本表のスキルも含む)	同社の調査では3万1,132件のスキルの**26.1%に脆弱性、5.2%に悪意の疑い**。LLM解析は設定したプロバイダへ内容を送る
Cloudflare `cloudflare/security-audit-skill`	エージェントを監査役にする6段階(偵察 → 網羅的な探索 → 別エージェントによる反証 → 構造化出力 → 独立検証 → 報告)	自社リポジトリの深い監査	結果に「要検証」が残る前提。人のレビュー必須、時間・トークン消費が大きい
Anthropic `anthropics/defending-code-reference-harness`	Claude Code 用 /threat-model・/vuln-scan・/triage・/patch、自律スキャン基盤、侵害の検知・対応スキル	脅威モデル → スキャン → 選別 → 修正案の一連の流れ	**保守されていない参照実装**。/patch・自律基盤はコードをビルド・実行するため隔離環境で(公式警告)
OpenAI `openai/codex-security`	Codexプラグイン・CLI・TypeScript SDK・GitHub Action。スキャン、検証、パッチ生成、脅威モデル、SARIF出力	CIでの継続スキャン、修正の検証	APIの利用料・送信範囲を事前に確認
Alibaba `alibaba/open-code-review`	Git差分をAIでレビューするCLI(決定的処理+エージェント)。OpenAI / Anthropic 互換APIで動く	PRごとのレビュー、修正の取り込み前チェック	誤検知を減らす設計で見逃し(Recall)は多め(公式)

使うときのルール(どのエージェントでも共通)

1. **取得元は公式組織のリポジトリだけ**(github.com/cloudflare・anthropics・openai・NVIDIA・google・alibaba)。同名のフォーク・「改良版」・SNSで回ってくるリンクは使わない。
2. **導入前に SkillSpector で検査**するか、SKILL.md と同梱スクリプトを自分で読む。
3. **隔離環境で動かす**(コンテナ・使い捨てVM、本番の認証情報なし)。ダウンロードフォルダ・ホーム直下では起動しない(5.1)。
4. **結果は人が確認**し、パッチはテストとレビューを通して取り込む(5.2: エージェントは古い指示に従いがち)。
5. **自分が権限を持つシステムだけ**を対象にする。導入したスキルは資産台帳に載せ、更新を追う。

スキル機能の有無はエージェントにより異なる。スキルを読み込めないエージェントでも、osv-scanner・codex-security・open-code-review のCLIは直接実行でき、SKILL.md は手順書として渡せる。ライセンス: Cloudflare は MIT、OpenAI・NVIDIA・Alibaba・Google は Apache-2.0、Anthropic は明示なし(GitHub表示)。

7. 生活者向け — 家族・従業員に配れる注意点

> **第26版の検証範囲：**本日の更新は統合集計・グラフ・CVE一覧の再生成、11月8〜9日に一次情報で確認できた事象（金融庁、CISA KEV追加、Chrome、Brotli波及の機器側告知）の追記に限定します。各ソフトウェア章の既存記述と「注目CVE」10件のNVD記録は第26版からの継承です。旧版内の「本日」「今回」は当時の調査を指します。

パスキーの公開鍵認証・ローカル認証・フィッシング耐性の仕組みは本日FIDOの説明を再確認しました。これだけであらゆるアカウント被害を防ぐと断定しません。Passkey Central

> 第19版からの継承・今回個別再検証なし。以下の説明・統計・制度施行日・金額等を今回確認済みとはしない。 7.10のPython欄のみ今回更新。

家族への一言(5か条)

1. **急がせるリンクは開かない** — 「未払い」「停止」「補償」「見舞金」「投票して」。公式アプリ・ブックマークから自分で確認。
2. **番号・コードは誰にも教えない** — 認証番号・PIN・パスワード。LINE・GMO・警察を名乗っても。
3. **画面の電話番号にはかけない、コマンドは貼り付けない**(サポート詐欺・ClickFix)。
4. **更新とバックアップを習慣に** — iPhone・Macは 27.2、Chromeは156.0.8078.73へ。
5. **大事なアカウントはパスキーに。**(面倒に感じたら7.3〜7.8を読んでみてください — 最初の10分だけです)

7.1 やってはいけないこと(PC・スマホ・アプリ)

第19版からの継承・今回個別再検証なし。

× やってはいけない	理由・正しい対応
Webページの指示で「Windowsキー+R」→貼り付け→Enter/ターミナルにコマンドを貼る	偽の「私はロボットではありません」画面で不正コマンドを実行させる**ClickFix**。正規サイトは求めない
「ウイルスに感染」画面の番号に電話/遠隔操作ソフトを入れる	サポート詐欺。Esc長押し → ブラウザ終了、無理なら再起動。入れてしまったらネットを切り、削除・パスワード変更。IPA 03-5978-7509
友だちから届いた「認証番号を教えて」「このURLでログイン」に応じる	友だちのアカウントが乗っ取られている。LINEの公式URLは `line.me` で終わる。送金依頼は電話で本人確認
SMSで届いたWhatsApp等の登録コードを他人に転送/他人のQRコードを読む	アカウント乗っ取り・端末の追加リンク(Signal等で会話を盗み見)
PayPay等のアカウントを売る・貸す	詐欺・資金洗浄に使われ、本人も捜査対象になりうる(規約違反)
アプリを公式ストア以外(SMSのリンク・APK)から入れる/「会議に参加するにはこのファイルを実行」に従う	情報窃取マルウェアの入口。Meetはブラウザだけで使える
同じパスワードの使い回し/サポート切れOS(Windows 10個人向けESUは2027/10/12まで)/普段から管理者で使う	1か所の漏えいで全部取られる。パスワード管理アプリ+パスキー、Windows 11移行、標準ユーザーで使う
話題の流出情報サイトを見に行く	閲覧者の情報が攻撃者に取られる(GMO事案で確認)
バックアップを常時接続の外付けディスクだけに取る	ランサムウェアは接続中のドライブも暗号化。普段は外す媒体か、版管理付きクラウドへ

7.2 やっておく設定

第19版からの継承・今回個別再検証なし。

対象	設定
全アプリ共通	OS・アプリの自動更新。「ログイン中の端末/リンク済みデバイス」を月1回確認し、知らないものはログアウト。画面ロック
LINE	パスワード・メールアドレスを登録、PC版を使わないなら「ログイン許可」オフ、PC/iPad版は生体認証ログイン
Signal / WhatsApp	Signal: PINと**登録ロック**。WhatsApp: **パスキー**と2段階認証
Zoom / Meet / Teams	パスコード・待機室(Zoom)、ホスト管理で参加承認(Meet)、組織外からの初回チャットは送信者確認 ―「ヘルプデスク」を名乗る遠隔操作の依頼に注意(Teams)
スマホ回線	携帯会社のSIM再発行・MNPにロック/暗証番号(SIMスワップ対策)。急に圏外になったら携帯会社へ
家庭用ルーター	初期パスワード変更・ファームウェア更新・サポート切れ機種は買い替え・外部からの管理機能はオフ(犯罪の「踏み台」=レジデンシャルプロキシ化の防止。GoAhead等の機器の脆弱性対策にもなる)

7.3 なぜパスキーなのか ―「使い回し84.3%」の現実

第19版からの継承・今回個別再検証なし。

トレンドマイクロの調査(2026年3月、Webサービス利用者1,034人)では、**84.3%が複数のWebサービスでパスワードを使い回し**、専用のパスワード管理アプリを使う人は17.7%だけ。使い回したパスワードが1か所で漏えると、その人が登録済みの**全サービスを順番にログインされる**(クレデンシャルスタッフィング)。GMO事案でもID・パスワードがそのまま攻撃に使われた。パスキーはこの根っこ ― **「共有する秘密の文字列」そのもの ― をなくす方式**で、偽サイトでは反応せず、鍵が漏れても使えないため、フィッシングに最も強い。

7.4 よくある誤解 ―「指紋・顔認証」と「パスキー」は別物

第19版からの継承・今回個別再検証なし。

「指紋(顔)認証を登録してあるから大丈夫」と答える人が多いが、それは別の層の話。**パスキーは、サイトごとに作られる暗号鍵(本体)。**指紋・顔・PINは、その鍵を端末の中で「解く」ための操作。鍵がなければ指紋だけではログインできず、逆に鍵があればPINだけでも使える。

よくある誤解	実際
指紋・顔を端末に登録すれば、それがパスキーになる	別。**サービス側でパスキーの作成(登録)が1回必要**。指紋はあくまで「鍵を解く」動作
指紋・顔の情報をサービス側に預ける	預けない。生体情報は端末の外に出ず、サービスが受け取るのは検証結果だけ
パスキー=生体認証のこと	鍵(パスキー)と解錠(指紋・顔・PIN)の組み合わせ。鍵は**サイトごとに別々**で、コピー・転用できない
SMSの認証コードと同じ仲間	違う。SMSは「送られてきた数字を打つ」方式で詐欺・転送に弱い。パスキーは打つ数字が存在しない

たとえるなら: **指紋は「鍵を回す指」、パスキーは「その家の鍵」**。鍵は訪問先(サイト)ごとに別のものを作り、自宅(端末)の鍵保管庫から持ち出せない。

7.5 「めんどくさい」は最初の10分だけ — 何から設定するか

第19版からの継承・今回個別再検証なし。

登録は、アカウントのセキュリティ設定で1回。以降は**指紋をかざす・顔を向けるだけ**で、パスワードの入力も生成も変更もなくなる(スマホ間の移動はQRコード+端末の承認)。「面倒の正体」は最初の10分で、以降はパスワードより楽になる。まず表の1行目だけでよい。

順	アカウント	設定の入口
1	Google / Apple / Microsoft	Googleは g.co/passkeys、AppleはiCloudキーチェーンを有効化、MicrosoftはWindows Helloを設定してから「パスキーを追加」
2	証券・銀行・カード・PayPay等	各サービスの「ログインとセキュリティ」(国内証券も対応が進む)
3	LINE・WhatsApp・SNS	WhatsAppは 設定 → アカウント → パスキー
4	通販・Yahoo! JAPAN ID	各サービスの案内

2台目の端末にも登録し、復旧用メール・電話番号を最新に。パスワード/SMSでのログインが残っていればそこが狙われる。他人から送られたQRでの承認はしない。共用端末には保存しない。

7.6 よくある不安への答え

第19版からの継承・今回個別再検証なし。

不安	答え
機種変更・故障でログインできなくなるのでは	iCloudキーチェーン・Googleパスワード マネージャー等に**暗号化して同期**され、新しい端末で復元する。機種変更前に「クラウドへの同期をオン」に。復旧用メール・電話番号も最新に
対応していないサイトがある	そこはパスワード管理アプリの**自動生成(長くて別々のパスワード)**に任せる。全サイトをパスキーにしなくても、**大事なものだけ**パスキーにすれば攻撃の入口は大幅に狭まる
家族と共用している端末では	共用端末にはパスキーを保存しない。本人の端末からQR+承認で通す
いま指紋でログインできているサイトは	それは「パスワードを端末が覚えている」だけのことが多い。ログイン画面に「パスキー」の案内が出ていれば作成し、出なければ7.5の順で対応済みのものから

7.7 データで見ると(2026年)

第19版からの継承・今回個別再検証なし。

- FIDOアライアンス(2026/5/7公表): パスキーの**認知は90%**(前年75%)、**利用中のパスキーは約50億**、企業の導入率68%。
- 同 Passkey Index 2026: 成功したサインインの**36%がパスキー**(前年26%)。
- 日本(トレンドマイクロ2026): 認知は91%まで広がった一方、利用率はまだ伸びしろが大きい。**「知っている」と「入れている」の差が、そのまま攻撃される差になっている**。

7.8 パスワードはなくなるか — FIDO2と今後

第19版からの継承・今回個別再検証なし。

パスキーの基盤は **FIDO2** = WebAuthn(ブラウザとサイトの間で鍵の登録・検証をするWeb API。W3C勧告として国際的なウェブ標準)+ CTAP(端末と認証器をつなぐプロトコル。現行のCTAP 2.3は2026年に公開され、現行の認証取得の基盤)。OS・ブラウザ・大手サービスは対応済みで、ログイン画面に「パスキーでログイン」が並ぶのはこのため。パスワードが完全に消えるまでには時間がかかる(対応していないサイト、復旧手続き、共用端末など)が、**方向は決まっている**。だから今日やることは、待つのではなく:

1. **使い回しをやめる**(パスワード管理アプリの自動生成へ)。
2. **大事なものからパスキーへ**(7.5の順)。
3. 残るパスワードは**サービスごとに別々**に。多要素認証があればあわせて入れる。

7.9 AIエージェントを使う人へ

第19版からの継承・今回個別再検証なし。

Codex・Claude Code 等は**ダウンロードフォルダ・ホームフォルダで起動しない**(作業ごとに空のフォルダを作る)。中身を見ていない AGENTS.md / CLAUDE.md があるフォルダで「おまかせ」実行をしない。承認・サンドボックスはオンのまま。Chromeの「ダウンロード前に保存場所を確認」をオン(詳細は第5章)。

7.10 開発者のPC ― 言語ランタイムを確認・更新する

この節はPythonの調査差分のみ反映。他言語・一般更新手順は第19版からの継承・今回個別再検証なし。

> 第20版調査差分（2026-11-01）: この節のPython欄・pyenv例のみ更新。他言語・一般手順は継承。識別子: CVE-2026-115557 / CVE-2026-114583。確認範囲: 侵害CA中間鍵のsslブロック。tarfile.tar_filterで展開先置換リンク拒否。http.cookiejar負version拒否も含む。 対処: 3.15.2 / 3.14.10 / 3.13.18 / 3.12.16 / 3.11.18。前2者以外はソースのみ。 悪用状況: 取得した公式本文では実悪用を確認せず。 未確認: 旧19445/19553個別勧告 / 他系列個別公開日。根拠: 公式資料1 / 公式資料2 / 公式資料3

サーバーだけでなく**手元のPCにも古い版が残る**。1台に複数の版があることが多いので全部洗い出し、入れたときと同じ方法で更新する。

言語	この版以上に	確認(Mac/Linux | Windows)
Node.js	26.12.1 / 24.22.1 / 22.23.4(Bun 1.4.4)	`which -a node | where.exe node`
Python	3.15.2 / 3.14.10 / 3.13.18 / 3.12.16 / 3.11.18。前2者以外はソースのみ。 注意喚起冒頭でpip26.2.2 / certifi2026.10.19 / uv0.13.6。既存venvも別確認。	`which -a python3 | py --list`
Ruby	4.0.9 / 3.4.12 / 3.3.13	`which -a ruby | where.exe ruby`
PHP	8.5.12 / 8.4.27 / 8.3.36 / 8.2.35(Windowsは再ビルド版)	`which -a php | where.exe php`
Perl	5.44.0 / 5.42.3	`which -a perl | where.exe perl`

```
# Mac (Homebrew)        brew update && brew outdated && brew upgrade
# Windows (winget)      winget upgrade --all
# Debian/Ubuntu         sudo apt update && sudo apt upgrade
# RHEL/Alma/Fedora      sudo dnf upgrade
# nvm / pyenv / mise    nvm install --lts / pyenv install 3.14.10 / mise upgrade
# パッケージも           npm outdated -g / python3 -m pip install -U pip certifi / gem outdated
```

Mac付属の /usr/bin の perl・ruby・python3、LinuxのOS付属Python・Perlは置き換えない(OS更新で直す)。ディストリ版は版番号が古いまま修正が入る(バックポート)ので各ディストリのセキュリティ情報で確認。Docker・venv・node_modules は作り直す。

7.11 万一のとき

第19版からの継承・今回個別再検証なし。

① ネットワークを切る ② 別の安全な端末からパスワード変更・全端末ログアウト ③ カード会社・銀行に連絡 ④ 画面や履歴を保存 ⑤ 相談: **警察 #9110/IPA 03-5978-7509/消費者ホットライン 188**。

8. 法規制・補償・補助金

> **第26版の検証範囲：**本日の更新は統合集計・グラフ・CVE一覧の再生成、11月8〜9日に一次情報で確認できた事象（金融庁、CISA KEV追加、Chrome、Brotli波及の機器側告知）の追記に限定します。各ソフトウェア章の既存記述と「注目CVE」10件のNVD記録は第26版からの継承です。旧版内の「本日」「今回」は当時の調査を指します。

> **11月1日の制度確認：**SCSは2026年度末頃の申請受付開始を目指す予定で、確定日ではありません。サイバー対処能力強化法は10月1日の官民連携等と、2027年秋予定の通信情報利用を区別します。旧版の罰則額・課徴金・補助金・海外制度の全記述を今回再検証したものではありません。
> 経済産業省 ／ 国家サイバー統括室

> 第19版からの継承・今回個別再検証なし。以下の説明・統計・制度施行日・金額等を今回確認済みとはしない。

一般情報の整理であり法的助言ではない。個別判断は専門家に確認のこと。

制度	要点	罰則・金額
サイバー対処能力強化法(能動的サイバー防御)	10/1から基幹インフラ事業者(15分野)にインシデント報告義務、資産届出は2027年3月まで。国の「アクセス・無害化措置」は独立機関の承認等を経て国が発動 ― GMOの要請で発動が決まるものではなく、適用は未定。委託先・機器供給元にも照会・協力が及びうる	報告せず是正命令にも違反 200万円以下の罰金 ほか
個人情報保護法	漏えい時は個人情報保護委員会へ速報(概ね3〜5日)・確報(30日、不正アクセスは60日)、本人通知。令和8年改正(7/17公布、施行は2028年頃)で**課徴金**創設・罰則強化。既知脆弱性の長期放置は安全管理措置義務違反と評価されうる	命令違反: 法人1億円以下の罰金
SCS評価制度(経産省)	取引先のセキュリティ対策を★3(自己評価+専門家確認)・★4(第三者評価)で可視化。申請受付は2026年度末頃から、評価ガイドは今秋公表予定。罰則はないが実質的な受注要件になりうる	―
EU CRA	EUで販売するデジタル製品の製造者に、9/11から悪用中の脆弱性・重大インシデントの報告義務(24時間で早期警告、72時間で通知)。主要義務は2027/12/11から	最大1,500万ユーロまたは世界売上の2.5%
EU NIS2 / 米 CIRCIA	NIS2: 18分野にリスク管理・報告義務。CIRCIA: 72時間報告・身代金支払い24時間報告の最終規則は審査中で**未発効**	NIS2: 1,000万ユーロ以上または2%以上

補償・保険の考え方

- 約款の免責があっても自主補償に踏み切る例が多い(GMO: 一律見舞金+無償化+実損補償+特別見舞金)。身代金の支払いは情報削除の保証にならない。
- サイバー保険は、**既知脆弱性の放置・多要素認証の未導入で支払い対象外**とする約款が増えている。更新時に条件を確認。

中小企業向けの支援(2026年度)

制度	内容・金額
デジタル化・AI導入補助金2026 セキュリティ対策推進枠	「お助け隊サービス」の利用料(最大2年分)。5万〜150万円、補助率1/2(小規模2/3)
東京都 サイバーセキュリティ対策促進助成金	EDR・UTM等。上限500万円、助成率1/2。第3回受付 2027/1/8〜15。SECURITY ACTION 二つ星とGビズIDプライムが必要
お助け隊(新類型)実証事業	SCS★3・★4取得を一貫支援(無料、2026年9月〜)

活用順の例: SECURITY ACTION 二つ星 → お助け隊導入(補助金) → 設備は東京都助成 → 年度末からSCS★3。

9. 結びに

> **第26版の検証範囲：**本日の更新は統合集計・グラフ・CVE一覧の再生成、11月8〜9日に一次情報で確認できた事象（金融庁、CISA KEV追加、Chrome、Brotli波及の機器側告知）の追記に限定します。各ソフトウェア章の既存記述と「注目CVE」10件のNVD記録は第26版からの継承です。旧版内の「本日」「今回」は当時の調査を指します。

本書で取り上げた脆弱性の多くに「AIによる発見」「AI支援の攻撃」が関わっている。しかし、攻撃者がAIを使う一方で、防御側もAIによる発見・調査・対応を進めている。問うべきは「AIが怖いか」ではなく、**どの入口から被害が起き、どの対策で減らせたか**である。

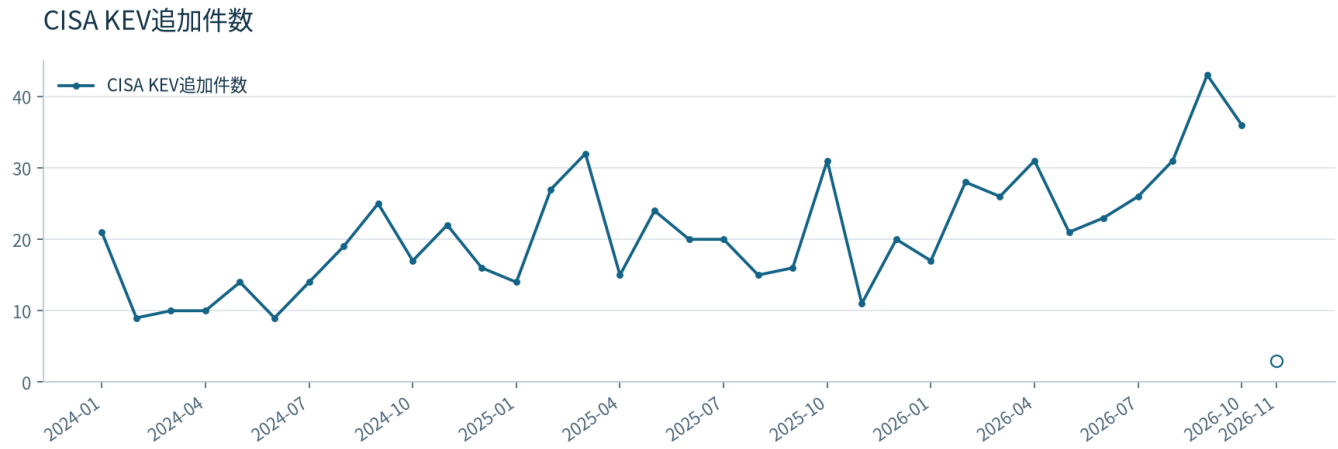
重なって見える背景 — 一つが原因とは限らない

被害の実体
現実に深刻な被害がある

公表の流れ
被害の公表が増え、早まっている

新たな手段
攻撃者がAIを使う事例が現れた

実害・公表・新技術への注目が重なっている。AI利用と被害の根本原因は分けて評価する。公表や発見の増加をそのまま悪化と断定しない。



UTC暦月・2024-01〜2026-11。11月は白丸の途中集計。高深刻度35月は欠測（0ではない）。

図：本版の共通集計画像。元データ・基準日時・指標定義は統合集計章とインシデント章を参照。AI公開やパスキー単独の因果効果を示すものではありません。

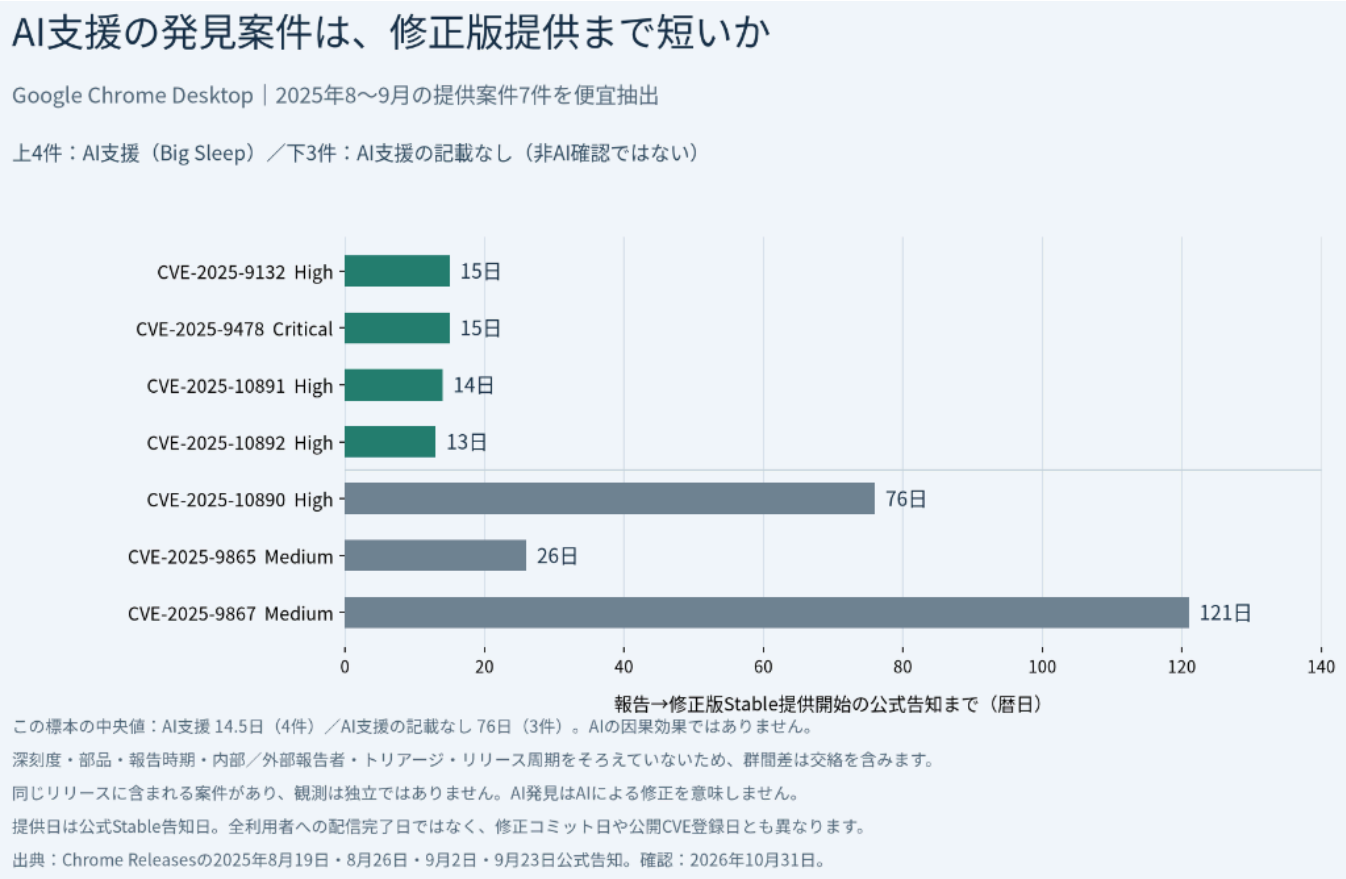


図: Google Chrome Desktopの2025年8〜9月の修正版提供案件7件を便宜抽出。報告→修正版Stable提供の公式告知までの暦日を比較すると、AI支援(Big Sleep)4件の中央値は14.5日、AI支援の記載なし3件の中央値は76日。標本が小さく交絡要因(深刻度・部品・報告時期・トリアージ)をそろえていないため、**AIの因果効果を示すものではない**。「AI支援の記載なし」は「非AI確認」を意味しない。出典:Chrome Releases公式告知(確認:2026年10月31日)。**【前版からの参考図・今回は7案件の個票を独立再検証していません】**

3つの提言

提言 01

「気をつけて」で済ませず、安全な初期設定を広げる

注意喚起だけに頼らず、認証・更新・復旧の手段をサービス側で使いやすく整える。利用者の見分けの負担も減らす。

提言 02

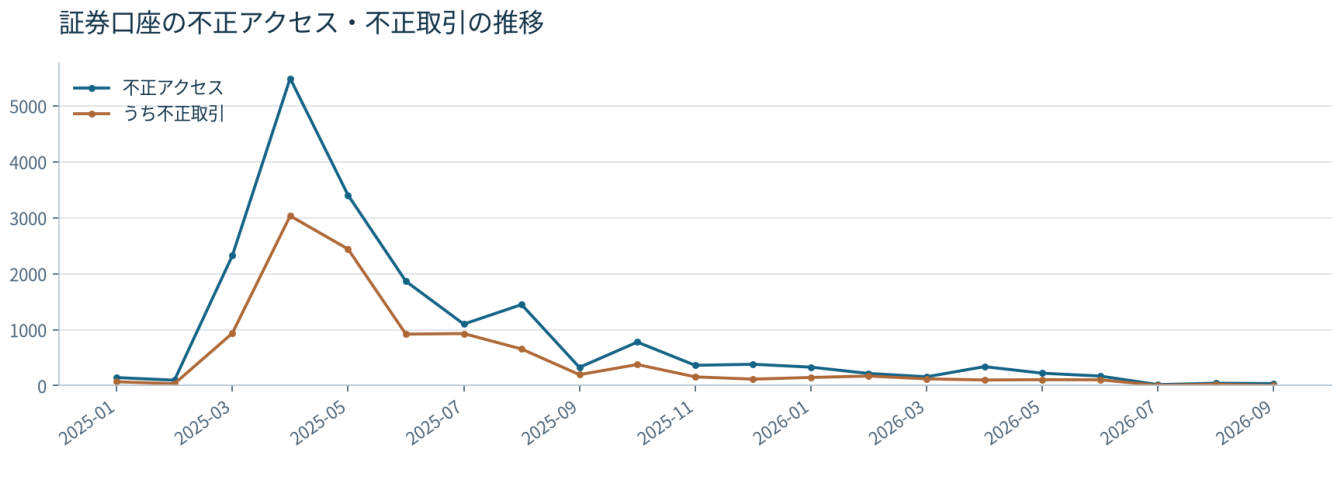
減った事例を、条件付きで共有する

証券口座の不正取引件数の大幅な減少を一例として共有。AIやパスキー単独の成果とは断定しない。

提言 03

物差しを、被害と回復へ変える

実損失・業務停止・復旧までの時間を重視。公表や発見の増加をそのまま悪化と評価しない。



図：本版の共通集計画像。元データ・基準日時・指標定義は統合集計章とインシデント章を参照。AI公開やパスキー単独の因果効果を示すものではありません。

締めの言葉

> 「危険を小さく語る必要はない。対処できる力まで小さく語らないことだ。」

> 「AIを犯人にするより、攻撃を成功させてしまう条件を減らそう。」

出典:警察庁 サイバー情勢／MM総研／Mandiant M-Trends 2026／金融庁 — 調査日 2026年10月31日

第21版からの変更点（第22版）

- データ基準を2026年11月4日10:30:00 JSTへ更新。NVD 17,864件を全件取得（Rejected 424、未採点 1,581、7未満 7,224を除外し8,635件）。9.0以上1,644件、対象内KEV 17件。
- 共通グラフ9点を新データで再生成し、Web（v94/images/security）と本文書assetsで同一バイトを使用。
- 「注目CVE」節を新設し、指定6件のNVDレコードを窓内・窓外を明記して掲載。窓外2件は一覧・グラフ・CSVに含めない。
- Web特設「フロンティアモデル動向」「意思決定モデル」を2026年11月4日付で追記更新（GPT-6.1 Terra、Claude Haiku 5.5、Gemini 4 Carbon、AA Decision Index、OpenAI Decisions API一般提供）。
- 第21版以前の各章は継承。全過去記述・全CVEの提供元再検証は実施していません。

第22版からの変更点（第23版）

- データ基準を2026年11月6日21:45:00 JSTへ更新。NVD 17,565件を全件取得（Rejected 661、未採点 1,124、7未満 7,151を除外し8,629件）。9.0以上1,622件、対象内KEV 16件。
- 共通グラフを新データで再生成し、Web（v95/images/security）と本文書assetsで同一バイトを使用（5点。インシデント系4点は第22版を継承）。
- 「注目CVE」節を指定12件に更新。窓内・窓外、NVD status、CVSS、CWE、出典を明記。CVE-2026-115560 はNVD未登録である事実を明記。
- 指定5資料（OpenSSH/musl、OpenSSL EOL、Windows Paint、Cloudflare WAF、Barracuda ESG）を該当章へ追記。
- Web v95：ホームの告知2件を色付きカードへ変更（日英）、3特設を更新。
- 第22版以前の各章は継承。全過去記述・全CVEの提供元再検証は実施していません。

第23版からの変更点（第24版）

- データ基準を2026年11月7日20:00:00 JSTへ更新。NVD 17,850件を全件取得（Rejected 678、未採点 950、7未満 7,409を除外し8,813件）。9.0以上1,676件、対象内KEV 17件。
- 共通グラフ9点を新データで再生成（データ駆動5点＋インシデント系4点）。Web（v96/images/security）と本文書assetsで同一バイトを使用しSHA-256を照合。
- 「注目CVE」節を指定10件に更新。窓内9件・窓外1件（CVE-2026-43499）を明記。CVE-2026-19868 は CISA KEV に 2026-11-06 付で掲載。
- 指定2資料（Ubuntu CVE-2026-98432 のリリース別状態、GhostLock を用いた BlackBerry KEYone のLPE公開）を第4章へ追記。攻撃コードの再現情報は掲載しない方針を明記。
- Web v96：3特設（最新LLM情報・意思決定モデル・AI秘書比較）を2026.11.07付で更新。ホームの告知カードはv95の状態を維持。
- 第26版以前の各章は継承。全過去記述・全CVEの提供元再検証は実施していません。

第24版からの変更点（第25版）

- データ基準を2026年11月8日18:00:00 JSTへ更新。NVD 17,673件を全件取得（Rejected 656、未採点 960、7未満 7,368を除外し8,689件）。9.0以上1,628件、対象内KEV 17件。
- 共通グラフ9点のうちデータ駆動5点を新データで再生成。Web（v97/images/security）と本文書assetsで同一バイトを使用しSHA-256を照合。インシデント系4点は第26版のまま継承。
- 第4章に「2026年11月7日〜8日の新規確認」を追加：金融庁の利用者向け注意喚起（11月6日）と緊急対策パッケージ、KEV新規追加（機械抽出）、Brotli CVE-2026-111497 の Neat 告知、Chrome の更新日付。確認できなかった事項も明記。
- 「注目CVE」節は第26版のNVD記録を継承（本版で10件を再取得していない旨を明記）。
- 攻撃コードの再現手順・アドレス値は引き続き不掲載。
- 第26版以前の各章は継承。全過去記述・全CVEの提供元再検証は実施していません。

第25版からの変更点（第26版）

- データ基準を2026年11月9日14:15:00 JSTへ更新。NVD 17,584件を全件取得（Rejected 652、未採点 938、7未満 7,379を除外し8,615件）。9.0以上1,607件、対象内KEV 17件。
- 共通グラフ9点のうちデータ駆動5点を新データで再生成。Web（v98/images/security）と本文書assetsで同一バイトを使用しSHA-256を照合。インシデント系4点は第26版のまま継承。
- 第4章に「2026年11月8日〜9日の新規確認」を追加：金融庁の利用者向け注意喚起（11月6日）と緊急対策パッケージ、KEV新規追加（機械抽出）、Brotli CVE-2026-111497 の Neat 告知、Chrome の更新日付。確認できなかった事項も明記。
- 「注目CVE」節は第26版のNVD記録を継承（本版で10件を再取得していない旨を明記）。
- 攻撃コードの再現手順・アドレス値は引き続き不掲載。
- 第26版以前の各章は継承。全過去記述・全CVEの提供元再検証は実施していません。

第25版からの変更点（第26版）

- データ基準を2026年11月9日14:15:00 JST（2026-11-09T05:15:00Z）へ更新。公開対象は2026年10月10日14:15〜11月9日14:15 JST。NVD全17,584件を取得し、Rejected 652・未採点 938・7.0未満 7,379を除いた**8,615件**を掲載（9.0以上 1,607件、対象内KEV 17件）。
- 統合集計章・CVE一覧・グラフ5点を新データで再生成。Web（v98/images/security）と本文書assetsは同一バイト（SHA-256照合）。

- 第4章に「2026年11月8日〜9日の新規確認」を追加：Microsoft 11月Patch Tuesdayは**予告段階（未公開）**として件数を書かず、KEV新規追加の機械抽出、警察庁の合同捜査本部設置（二次情報）を掲載。確認できなかった17製品・AI関連は明記。
- 注目CVE 10件は第25版（11月7日取得のNVD記録）を継承。
- Web v98では英語版のセキュリティページを日本語と同じ9章構成に再生成し、英語のセキュリティ情報センターを新設（別途、変更履歴に記載）。
- 攻撃コードの再現手順・アドレス値は引き続き不掲載。

10. 主要な情報源・留意事項・版履歴

> **第26版の検証範囲：**本日の更新は統合集計・グラフ・CVE一覧の再生成、11月8〜9日に一次情報で確認できた事象（金融庁、CISA KEV追加、Chrome、Brotli波及の機器側告知）の追記に限定します。各ソフトウェア章の既存記述と「注目CVE」10件のNVD記録は第26版からの継承です。旧版内の「本日」「今回」は当時の調査を指します。

第21版の追加調査根拠

- PHP：https://www.php.net/archive/2026.php
- Node.js / Brotli：https://nodejs.org/en/blog/vulnerability/october-2026-security-releases
- Python：https://blog.python.org/2026/10/python-3152-31410-31318-31216-31118/
- Ruby：https://www.ruby-lang.org/en/news/2026/10/23/regexp-fixes-for-gitlab-cves/
- Oracle Java：https://www.oracle.com/security-alerts/alert-cve-2026-114820.html
- BIND：https://kb.isc.org/docs/cve-2026-94300
- Linux：https://ubuntu.com/security/CVE-2026-98432
- GitLab / Tomcat：https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-5-3-released/
- LiteLLM：https://docs.litellm.ai/blog/security-changes-after-oct-21-2026
- Ivanti：https://www.cyber.gc.ca/en/alerts-advisories/ivanti-security-advisory-av26-1035
- Canonical LXD / MicroCloud：https://discourse.ubuntu.com/t/security-advisory-critical-vulnerability-found-in-canonical-lxd-and-microcloud/90557
- ClickHouse：https://clickhouse.com/docs/whats-new/security-changelog
- WordPress：https://wordpress.org/news/2026/10/wordpress-7-1-4/
- AIエージェント防御：https://openai.com/index/designing-agents-to-resist-prompt-injection/

2026年11月2日：第20版から差分更新。NVD全件取得・月次再集計、GMO735件、WordPress公式再確認、LiteLLM改善計画・AI防御設計追補。過去履歴の日付は変更していません。

> 本版の再調査範囲は調査記録を参照。以下の旧版出典・履歴は資料として保持し、全項目を11月1日に再検証済みという意味ではありません。

> 第20版調査差分の根拠は各対象h2ブロック内のリンクを参照。以下の旧出典台帳・第19版の留意事項・履歴は過去時点の記録として保持しており、古い修正状況やMPTCP限定等の留意事項は今回の本文差分を優先する。10/31〜11/1新規公開と絶対日時まで検証できた対象勧告は今回未確認。不在とは断定しない。 調査整理時刻は勧告の公開日時ではない。

一次情報(公的機関・ベンダー・当事者企業)を優先し、報道は補足に用いた。SNS・個人サイトは手がかりとしてのみ扱った。第13版の追加出典は同版第9章、第12版までの全出典は同版第18章を参照。

今回(第19版)追加

- Red Hat RHSB-2026-016(CVE-2026-98432をCriticalへ評価引き上げ、RCE確認) — https://access.redhat.com/security/vulnerabilities/RHSB-2026-016
- 情報通知サイト joho-todai.com「CVE-2026-98432」解説記事(Eric Dumazet氏の2行修正・Anthropic Xinyang Ge報告の経緯) — https://joho-todai.com/cve-2026-98432/
- CISA KEV(2026.10.30版: Ivanti Connect Secure CVE-2026-111357・118527追加) — https://www.cisa.gov/known-exploited-vulnerabilities-catalog / Volexity「Ivanti Connect Secure Exploitation by UTA0576」 — https://www.volexity.com/blog/
- NVD CVE-2026-111357 / CVE-2026-118527 / CVE-2026-104935 — https://nvd.nist.gov/vuln/detail/CVE-2026-111357
- WordPress 7.1.4 リリースノート(10/28) — https://wordpress.org/news/2026/10/wordpress-7-1-4/ / Wordfence「Active Exploitation Attempts of CVE-2026-119977」 — https://www.wordfence.com/blog/
- Canonical LXD Security Notice(CVE-2026-112816) — https://ubuntu.com/security/notices / NVD CVE-2026-112816 — https://nvd.nist.gov/vuln/detail/CVE-2026-112816
- ClickHouse公式セキュリティ changelog(CVE-2026-116366) — https://clickhouse.com/docs/en/whats-new/security-changelog

- Censys「Progress WS_FTP Server CVE-2026-84295」アドバイザリ — https://censys.com/blog/ / NVD CVE-2026-84295 — https://nvd.nist.gov/vuln/detail/CVE-2026-84295
- NVD CVE-2026-103039(Gravity Forms)・CVE-2026-109220(WooCommerce PDF Invoice) — https://nvd.nist.gov/vuln/detail/CVE-2026-103039
- GMO公式ニュース一覧(10/31時点、第17報の公開なしを確認) — https://internet.gmo/news/

今回(第19版)追加 — 4章インシデント続報

- パーク24公式「ニュースリリース」第5報(10/23、663万件・画像146万件確定) — https://www.park24.co.jp/news/2026/10/20261023-1.html / 第4報(10/16、本人確認書類の保有ルール変更を予告) — https://www.park24.co.jp/news/2026/10/20261016-1.html
- 日本交通「弊社システムへの不正アクセスに関するお知らせ(第6報)」(10/30、約29万人分・東京電力HDへの波及) — https://nihon-kotsu-hire.jp/news/261030/ / 日本経済新聞(内訳の詳細) — https://www.nikkei.com/article/DGXZQOUC30BHD0Q6A031C2000000/
- ニチレイ公式「当社グループでのシステム障害発生について(第7報)」(9/18、計5.4万件確定) — https://www.nichirei.co.jp/news/2026/524.html
- デジタル庁公式「Studio株式会社における不正アクセスによる個人情報の漏えいの可能性について」(10/22) — https://www.digital.go.jp/press/a0a8f66c-b32d-4695-9372-bcd5d4280f22 / GSS事案(9/11) — https://www.digital.go.jp/news/2026-0911-01
- アサヒグループホールディングス公式「漏えいのおそれがある個人情報(2026年7月17日時点)」(約229万件へ再整理) — https://www.asahigroup-holdings.com/newsroom/detail/20260717-0101.html
- HIS公式「子会社ファイルサーバへの不正アクセスによる個人情報流出の可能性に関するお詫びとお知らせ」(10/7、最大627名分) — https://www.his.co.jp/assets/20261007.pdf / ITmedia(検知から公表まで約10か月の経緯) — https://www.itmedia.co.jp/news/article/2610/07/2000002090/
- TRM Labs「North Korea Steals USD 6.36 Billion From Binance」(FBI断定の分析) — https://www.trmlabs.com/resources/blog/north-korea-steals-usd-6-36-billion-from-binance-in-the-largest-hack-in-history / The Guardian(90%補填・FBI声明) — https://www.theguardian.com/business/2026/nov/01/binance-losses-covered-hack-fbi-north-korea-cryptocurrency
- Reuters「Polymarket resumes trading after third-party security incident」(DebugBear起因) — https://www.reuters.com/business/polymarket-reports-major-outage-suspends-trading-actions-2026-10-29/ / Yahoo Finance(390万ドル返金・95%完了) — https://finance.yahoo.com/markets/crypto/articles/polymarket-sends-3-9m-back-181112258.html
- 時事通信「個人情報漏えい、2.6億人分」(10/30、木原官房長官会見・延べ2億6000万人分) — https://www.jiji.com/jc/article?k=2026103000493&g=pol / FNN(月次推移・緊急対策パッケージ) — https://www.fnn.jp/articles/-/1142867

前回(第18版)追加

- The Hacker News「Linux Kernel TCP Flaw With 9.8 CVSS Score」(10/30更新版、Anthropicのroot実証・配布版修正状況) — https://thehackernews.com/2026/10/linux-kernel-tcp-flaw-with-98-cvss.html / Anthropic公式ブログ「Discovering vulnerabilities with Claude」(10/27) — https://www.anthropic.com/research/discovering-vulnerabilities-with-claude
- Teltonika Networks Security Centre(CVE-2026-82104、10/30自社開示) — https://www.teltonika-networks.com/support/security-centre
- The Hacker News「Telegram Android Flaw Lets Attackers...」(10/29) — https://thehackernews.com/2026/10/telegram-android-flaw-lets-attackers.html
- OpenSourceMalware「Trojanized Claude Code Extension Plants Persistent SSH Backdoor」 — https://opensourcemalware.com/blog/trojanized-claude-code-extension-plants-persistent-ssh-backdoor / Cyber Security News — https://cybersecuritynews.com/malicious-claude-code-extension/
- The Hacker News「CISA Adds Actively Exploited GitLab RCE...」(10/30、CVE-2026-97229・76418のKEV追加) — https://thehackernews.com/2026/10/cisa-adds-actively-exploited-gitlab-rce.html
- NVD CVE-2026-103093(ServiceNow AI Platform) — https://nvd.nist.gov/vuln/detail/CVE-2026-103093 / securityonline.info CVE Watchtower — https://securityonline.info/cve-watchtower/cve-2026-103093/
- CISA KEV(2026.10.29版: GitLab・Cisco ASA/FTD追加) — https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- GMO 第16報(懸賞金サイト情報提供428件、定期公表開始) — https://internet.gmo/news/article/262/

前回(第16版)追加

- Chrome 156.0.8078.73/.74 リリースノート — https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_0562499947.html / Cyber Security News — https://cybersecuritynews.com/google-fixes-52-chrome-security-flaws/
- Cisco ASA/FTD アドバイザリ — https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-tunnel-dos-s6mgkb75 / Tenable CVE-2026-76418 — https://www.tenable.com/cve/CVE-2026-76418
- CISA KEV(2026.10.28版: ESX・Fragnesia・Commerce・Brotli・PHP) — https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Linux98432の旧評価・旧未掲載日付は履歴。第20版のRed Hat影響説明はIPv4 TCP全般であり、MPTCPの有無だけで対象外としません。第21版ではUbuntu generic 4系列のVulnerable work in progressを確認。併記版を修正版配布完了と読み替えません。実悪用・KEVは今回のカタログと個別注記を参照。
- Searchlight Cyber「Cache Me If You Can」 — https://www.slcyber.io/research/cache-me-if-you-can-xss-in-cloudflares-cdn-cgi-image / Cyber Security News — https://cybersecuritynews.com/cloudflare-xss-vulnerability/

- Dream「Chained php2shell exploit roots 25 servers」 — https://dreamgroup.com/blog/chained-php2shell-exploit-roots-25-servers / Cyber Security News — https://cybersecuritynews.com/php2shell-gained-root-access-on-25-servers/
- LocalStack CVE-2025-65200(研究者の技術メモ、2025年12月公開) — https://cyberroute.github.io/post/2025-12-11-localstack-hack/
- FIDO Alliance World Passkey Day 2026 — https://fidoalliance.org/fido-alliance-reports-accelerating-global-passkey-adoption-on-world-passkey-day-2026/ / Passkey Index 2026 — https://fidoalliance.org/passkey-index-2026/ / CTAP 2.3 — https://developers.yubico.com/CTAP/
- トレンドマイクロ「パスワード・パスキーの利用実態調査2026」 — https://www.trendmicro.com/ja_jp/about/newsroom/press-releases/2026/pr-20260324-01.html
- DecisionRAG(arXiv:2610.35868) — https://arxiv.org/abs/2610.35868

第15版追加

- GitHub abraxas氏のphpMyAdmin関連リポジトリ(10件、10/12公開) — https://github.com/abraxas-null?tab=repositories(例: PMA-5.2.3-WebAuthn-2FA) / phpMyAdmin公式セキュリティ情報一覧(PMASA、該当なしを確認) — https://www.phpmyadmin.net/security/
- LibreSSL ocspcheck GHSA-3v5r-5xmx-hw5g — https://github.com/advisories/GHSA-3v5r-5xmx-hw5g
- GMO 第15報(犯人特定の有力情報を提出、情報提供270件) — https://group.gmo/info/alert/20261029/

第14版追加

- CISA「Adds Two Known Exploited Vulnerabilities」(10/27、Brotli) — https://www.cisa.gov/news-events/alerts/2026/10/27/cisa-adds-two-known-exploited-vulnerabilities-catalog / Broadcom VMSA-2026-0008.1(サポートポータル アドバイザリ 39445)
- FasterXML GHSA-m8xf-2cr7-77ph — https://github.com/FasterXML/jackson-databind/security/advisories/GHSA-m8xf-2cr7-77ph
- Oracle Critical Patch Update October 2026 — https://www.oracle.com/security-alerts/cpuoct2026.html
- nginx security advisories — https://nginx.org/en/security_advisories.html / TeamViewer TV-2026-1011 — https://www.teamviewer.com/en-us/resources/trust-center/security-bulletins/tv-2026-1011/
- Anthropic「Discovering vulnerabilities with Claude」(10/27) — https://www.anthropic.com/research/discovering-vulnerabilities-with-claude
- TianoCore GHSA-99cj-7hg9-mp4m — https://github.com/tianocore/edk2/security/advisories/GHSA-99cj-7hg9-mp4m / The Hacker News(UEFI) — https://thehackernews.com/2026/10/critical-16-year-old-uefi-flaw-can-run.html
- NVD CVE-2026-112512 — https://nvd.nist.gov/vuln/detail/CVE-2026-112512 / Apple 一覧 — https://support.apple.com/en-us/100100 / PC Watch(WebKit、記事2151800)
- MSRC(eMudhra) — https://www.microsoft.com/en-us/msrc/blog/2026/10/microsoft-response-to-compromised-emudhra-certificate-authority-keys
- Cloudflare「Cross-request KV cache exposure」 — https://blog.cloudflare.com/kv-cache-exposure-remediation
- PHP CVE-2026-115560 — https://www.php.net/archive/2026.php#2026-10-23-1 / The Hacker News — https://thehackernews.com/2026/10/urgent-php-warns-of-another-unpatched.html
- GMO 第13報 — https://group.gmo/info/alert/20261028/ / 第14報 — https://group.gmo/info/alert/2026102802/
- Agent Skills: github.com/google/osv-scanner ・ openai/php2shell-checker ・ NVIDIA/SkillSpector ・ cloudflare/security-audit-skill ・ anthropics/defending-code-reference-harness ・ openai/codex-security ・ alibaba/open-code-review

主要な一次情報(抜粋)

- CISA「Critical Vulnerabilities in PHP Require Immediate Patching」 — https://www.cisa.gov/news-events/alerts/2026/10/21/critical-vulnerabilities-php-require-immediate-patching / CERT-EU 2026-018 — https://cert.europa.eu/publications/security-advisories/2026-018 / JPCERT-AT-2026-0033 — https://www.jpcert.or.jp/at/2026/at260033.html
- AWS Security Blog(php2shell 公表前の悪用) — https://aws.amazon.com/blogs/security/amazon-threat-intelligence-identifies-php2shell-exploitation-prior-to-public-disclosure-in-madpot/
- Node.js October 2026 Security Releases — https://nodejs.org/en/blog/vulnerability/october-2026-security-releases / Bun v1.4.4 — https://bun.com/blog/bun-v1.4.4 / GHSA-9v8h-qqgm-4m35 — https://github.com/advisories/GHSA-9v8h-qqgm-4m35
- Python eMudhra 注意喚起 — https://discuss.python.org/t/information-for-python-users-regarding-emudhra-emsign-ca-certificate-security-incident/109576
- Ruby「Regexp fixes for GitLab CVEs」 — https://www.ruby-lang.org/en/news/2026/10/23/regexp-fixes-for-gitlab-cves/ / resolv — https://www.ruby-lang.org/ja/news/2026/08/27/multiple-vulnerabilities-in-resolv/
- Oracle Security Alert CVE-2026-91403 — https://www.oracle.com/security-alerts/alert-cve-2026-91403.html / ops.java — https://ops.java/emudhra
- JPRS(BIND) — https://jprs.jp/tech/security/2026-10-22-bind9-cve-2026-94300.html / ISC — https://kb.isc.org/docs/cve-2026-94300
- AlmaLinux PwnEscape — https://almalinux.org/blog/2026-10-16-pwnescape-cve-2026-99999/ / Infinity Core — https://www.openwall.com/lists/oss-security/2026/10/16/36 / ZDI-CAN-33367 — https://almalinux.org/blog/2026-10-23-zdi-can-33367/ / The Hacker News(KSMBD) — https://thehackernews.com/2026/10/two-cvss-90-linux-ksmbd-rce-flaws.html
- GitLab 19.5.1 — https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-5-1-released/ / JVNVU93110597(Tomcat) — https://jvn.jp/vu/JVNVU93110597/index.html

- LiteLLM Security Incident — https://docs.litellm.ai/blog/security-incident-oct-21-2026 / GMO Flatt Security — https://blog.flatt.tech/entry/litellm_2nd_compromise
- Wasmtime GHSA-mghf-wjfp-p5xm — https://github.com/bytecodealliance/wasmtime/security/advisories/GHSA-mghf-wjfp-p5xm / The Hacker News — https://thehackernews.com/2026/10/two-critical-wasmtime-flaws-could-let.html
- Forever Security(AIエージェント乗っ取り) — https://forever.security/blog/hijacking-ai-agents-via-downloads-folder / arXiv:2610.30571 — https://arxiv.org/abs/2610.30571
- Tailworm — https://tailworm.com/ / Tailscale Security Bulletins — https://tailscale.com/security-bulletins
- JPCERT-AT-2026-0030(国内不正アクセス) — https://www.jpcert.or.jp/at/2026/at260030.html / GMO 10/24 — https://group.gmo/info/alert/20261024/
- パーク24 第5報 — https://share.timescar.jp/news/2026/1023/1825.html / HIS — https://www.his.co.jp/assets/20261007.pdf / サイボウズ Garoon — https://cs.cybozu.co.jp/2026/013781.html / ネオジャパン — https://www.neo.co.jp/news/20261022/
- 警察庁 情報流出の注意喚起 — https://www.npa.go.jp/bureau/cyber/koho/caution/caution20261000.html / 警視庁 ルーター — https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/notes/router.html / 警察庁 サポート詐欺 — https://www.npa.go.jp/bureau/cyber/countermeasures/support-fraud.html
- LINEヘルプ(乗っ取り・詐欺) — https://help.line.me/line/smartphone/sp?contentId=20000293&lang=ja / PayPay — https://paypay.ne.jp/notice/20261014/s-01/ / Passkey Central — https://www.passkeycentral.org/ja/introduction-to-passkeys/how-passkeys-work
- 国家サイバー統括室(強化法) — https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/setsumei.pdf / 個人情報保護委員会(改正法) — https://www.ppc.go.jp/files/pdf/260717_kaiseihounitsuite.pdf / 経産省 SCS — https://www.meti.go.jp/press/2025/03/20260327001/20260327001.html / 欧州委員会 CRA — https://commission.europa.eu/news-and-media/news/safer-and-more-secure-digital-products-2026-09-11_en
- 常時監視: CISA KEV — https://www.cisa.gov/known-exploited-vulnerabilities-catalog / JPCERT/CC — https://www.jpcert.or.jp/ / JVN — https://jvn.jp/

留意事項

- 第21版のCVE基準は2026年11月2日20:30 JST。本日の個別再確認は0章と追補に限定し、それ以外は第20版（11月1日）および第19版以前の記録を継承。悪用状況・修正版は適用前に提供元の最新情報を確認してください。
- GoAheadの影響を受ける機器メーカー名は報道段階で、各社の確認は取れていない。PAN-OSの修正ホットフィックス番号はPalo Alto公式アドバイザリで確認のこと。旧iPhone向け更新の版数は本書では確認できていない。
- GMOは第16報ページの11月2日18:00追記で累計情報提供735件を確認。第17報が存在しないとは断定しません。被害者・口座数へ換算しない。攻撃者側サイトは閲覧していません。
- Tailworm・phpMyAdmin等の旧研究者報告は本日個別未再確認。ZDI-CAN-33367はAlmaLinux公式で本番修正版とCVE未採番を再確認。Garoon等の旧推定を本日確認済みにはしません。
- VMware VCF の版別修正はBroadcomのVMSAで確認のこと(本書は概要のみ)。PC Watch報道のWebKit欠陥のCVE番号・対象版は本書では特定していない。PHP CVE-2026-115560 の影響版・修正版は未公表。UEFIの機器別の修正状況は各メーカーで確認。
- NGINX CVE-2026-42530 は個人のGitHubリポジトリを手がかりに、nginx.org の公式一覧で確認した。tracehound(取引追跡ツール)は脆弱性情報ではないため本文に含めていない。arXiv:2610.35868(DecisionRAG)は脆弱性情報ではないため5.3に研究動向として記載。Cloudflare /cdn-cgi/image/ の件は研究者の実証で、CVE番号・公式の修正発表は本書時点で未確認。LocalStack(CVE-2025-65200)は2025年の事件で、新規の悪用報告は確認できていない。
- Linux98432の旧評価・旧未掲載日付は履歴。第20版のRed Hat影響説明はIPv4 TCP全般であり、MPTCPの有無だけで対象外としません。第21版ではUbuntu generic 4系列のVulnerable work in progressを確認。併記版を修正版配布完了と読み替えません。実悪用・KEVは今回のカタログと個別注記を参照。
- 本版で参照した https://www.fsa.go.jp/common/about/research/20261030/20261030.html(t.co短縮URL経由)は、確認の結果「諸外国における金融制度の概要に関する調査」報告書の公表であり、**サイバーセキュリティとは無関係**と判明したため本文には反映していない。
- Teltonika CVE-2026-82104・ServiceNow CVE-2026-103093はいずれもベンダー自身の開示で、第三者による悪用報告は本書時点で確認できていない。Claude Code偽装拡張機能は、改ざんがどの経路で混入したか(サプライチェーンの具体的な侵害点)は本書時点で未特定。Telegram通話乗っ取り連鎖はNebuSec(研究者)による報告で、第三者再現・公式脆弱性情報(CVE)は確認できていない。
- 深刻度はベンダー表記(CVSS 4.0/3.1混在)。法規制の記述は一般情報で法的助言ではない。

第20版以前の版履歴（当時の記述を保存）：以下の確定・最新版等の表現は各版時点の記録です。第21版の検証結果を優先します。

版履歴: 第1版 10/25 → 第2〜10版 10/25〜26(各ランタイム・BIND・Linux・GitLab・Tomcat・LiteLLM・国内事案・生活者向け・法規制を順次追加)→ 第11版 10/27(58p)→ 第12版 10/27(63p、Wasmtime・AIエージェント乗っ取り)→ 第13版 10/28: 圧縮再構成(重複・経緯の記述を整理。iOS 27.2・GoAhead・PHP Windows版・PAN-OS・GMO第12報を追加)→ **第14版 10/29**: BrotliのKEV追加・VMware VCF、jackson-databind、Oracle EBS、NGINX、TeamViewer、Chrome 156、macOS Gatekeeper・WebKit、UEFI、Microsoft eMudhra、Cloudflare Workers AI、PHP 115560、GMO第13・14報、**第6章 Agent Skills を新設**→ **第15版 10/29深夜**: LibreSSL ocspcheck(CVE-2026-118374)を追加、**phpMyAdmin 5.2.3の未確認の脆弱性報告10件を新設(3.10、研究者単独発表・CVE未採番)**、GMO事案は第14報のまま変化なしを確認(当時)、第14版までの「新」表示を整理。→ **第16版 10/29午後**: Chrome 156.0.8078.73(52件)・Cisco ASA/FTD SSL VPN DoS(CVE-2026-76418)・VMware ESX/Adobe Commerce のKEV追加・Linux TCP UAF(CVE-2026-98432)・Cloudflare /cdn-cgi/image のXSS連鎖を追加、php2shell+Fragnesiaの25台root化事例(4.5)、DecisionRAG(5.3)、**第7章をパスキー特集に拡充(7.3〜7.8)**。→ **第17版 10/29 18時台**: **GMO事案を第15報へ更新**(犯人特定の有力情報を警察へ提出、懸賞金情報提供270件)。CISA KEV・LibreSSL修正版・phpMyAdmin公式発表は本書時点で変化なしを確認。→ **第18版 10/30**: **Linuxカーネル CVE-2026-98432 の深刻化**(AnthropicがClaudeでMPTCPサーバーのroot権限奪取を実証、3.2・3.11に反映、Ubuntu/RHEL修正未公開)、**Open VSXの偽装Claude Code拡張機能によるSSHバックドア**(5.4新設)、**Teltonikaルーター CVE-2026-82104**・**Telegram Android通話乗っ取り連鎖**(3.12新設)、ServiceNow AI Platform CVE-2026-103093、CISA KEVへGitLab(CVE-2026-97229)・Cisco ASA/FTD(CVE-2026-76418)追加確認、GMO事案を第16報へ更新(情報提供428件)。→ **第19版 10/31**: **Ivanti Connect Secureの3件連鎖攻撃**(CVE-2026-111357/118527、脅威アクターUTA0576による実悪用、10/30 CISA KEV追加)・**WordPress Core 7.1.4の競合状態RCE**(CVE-2026-119977、公開直後から悪用試行多数)・**Canonical LXD**(CVE-2026-112816、CVSS10.0)・**ClickHouse Server**(CVE-2026-116366、CVSS9.5)・**Progress WS_FTP Server**(CVE-2026-84295)を追加(3.13新設)。**Linuxカーネル CVE-2026-98432 はRed Hatが10/30、RHSB-2026-016でCriticalへ評価引き上げ**(RCE確認、3.2更新)。GMO事案は第16報のまま変化なしを10/31に直接確認。**4章を「国内インシデント」から「インシデント」に改称し、Binanceハッキング(史上最大63億ドル、FBI・TraderTraitor北朝鮮関与断定、4.6新設)・Polymarket資金盗難(DebugBear経由、約4億円、4.7新設)・日本の個人情報漏えい統計(延べ2億6000万人分、4.8新設)を追加。あわせて4.3の情報流出事案(タイムズカー・日本交通・ニチレイ・デジタル庁GSS・アサヒグループHD・HIS)を各社の最新発表に基づき更新**(タイムズカーは10/23第5報の確定件数、日本交通は10/30第6報で新規確定、デジタル庁は委託先Studio社の二次漏えいを追加、アサヒは7/17の対象拡大約229万件を反映)。

→ 第20版 2026/11/1：Web v92と統合集計（45ページ）。→ 第21版 2026/11/2：Web v93、基準20:30 JST、NVD全16,816件・高深刻度8,012件、GMO735件、公式調査差分と継承範囲を明示。

第22版の追加根拠

- NVD CVE API 2.0（公開日時窓・cveId指定） https://services.nvd.nist.gov/rest/json/cves/2.0
- CISA KEVカタログ https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json
- Wazuh CTI CVE-2026-98548 https://cti.wazuh.com/vulnerabilities/cves/CVE-2026-98548
- Wordfence CVE-2026-120534 https://www.wordfence.com/threat-intel/vulnerabilities/id/b8a7a925-2b9e-43bc-b649-c7ec518e063c
- WPScan CVE-2026-81648 https://wpscan.com/vulnerability/9b1490a0-1381-4d22-8086-f75aade4e898/
- F-Droid advisories CVE-2026-107053 https://github.com/FFG0d/fdroid-android-advisories
- OpenAI GPT-6.1 Terra / Decisions API、Anthropic Claude Haiku 5.5、Google Gemini料金、Reuters Gemini 4 Carbon（特設2ページ参照）

第26版の追加根拠

- NVD CVE API 2.0（公開日時窓・cveId指定） https://services.nvd.nist.gov/rest/json/cves/2.0
- CISA KEVカタログ https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json
- sshhole.com（OpenSSH/musl 解説） https://sshhole.com/
- OpenSSH commit 4353fdc https://github.com/openssh/openssh-portable/commit/4353fdc43ef646c43a8dda7025cc1a898caf1482
- OpenSSL EOL告知 https://openssl-library.org/post/2026-11-01-eol34-36/
- MSRC CVE-2026-83844 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83844
- Cloudflare WAF changelog https://developers.cloudflare.com/changelog/post/2026-11-03-waf-release/
- Barracuda セキュリティアドバイザリ https://trust.barracuda.com/security/pre-authentication-authorization-bypass-command-injection
- Artificial Analysis Decision Index https://artificialanalysis.ai/articles/artificial-analysis-decision-index
- Google Gemini Spark 発表 https://blog.google/intl/ja-jp/company-news/technology/next-evolution-gemini-app/

第26版の追加根拠

- NVD CVE API 2.0（公開日時窓・cveId指定） https://services.nvd.nist.gov/rest/json/cves/2.0
- CISA KEVカタログ https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json
- Ubuntu CVE-2026-98432 https://ubuntu.com/security/CVE-2026-98432
- GhostLock/KEYone 公開リポジトリ https://github.com/giannoccarol/root-key1
- Microsoft MSRC CVE-2026-109469 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-109469
- AWS セキュリティバルテン 2026-173 https://aws.amazon.com/security/security-bulletins/2026-173-aws/
- SonicWall PSIRT SNWLID-2026-0014 https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0014
- WPScan CVE-2026-113615 https://wpscan.com/vulnerability/40e0b8d1-8e13-4c4c-a09a-9ec07c578662/
- VulnCheck CivetWeb 勧告 https://www.vulncheck.com/advisories/civetweb-through-1.16-http-2-use-after-free-via-stale-pseudo-header-state
- VulDB CVE-2026-123957 https://vuldb.com/cve/CVE-2026-123957
- Poly CVE-2026-39430 研究メモ https://github.com/thackeraaron/polycom_research/blob/main/CVE-2026-39430_and_CVE-2026-39431.md

第26版の追加根拠

- 金融庁「現下の情勢を踏まえた金融機関利用者へのお願い」（令和8年11月6日） https://www.fsa.go.jp/news/r8/sonota/20261106/20261106.html
- CISA KEVカタログ（当日取得） https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json
- Neat NEAT-SA-2026-11-02（Brotli CVE-2026-111497） https://support.neat.no/article/security-advisory-november-2026-brotli-decoder-vulnerability-cve-2026-111497-affecting-neat-devices/
- Chromium Releases 2026年11月一覧 https://chromereleases.googleblog.com/2026/
- NVD CVE API 2.0（公開日時窓） https://services.nvd.nist.gov/rest/json/cves/2.0

> 本版で新たに確認したのは上記4件の一次情報です。MSRC・各ベンダーの当月告知は取得できておらず、記載していません。

第26版の追加根拠

- 金融庁「現下の情勢を踏まえた金融機関利用者へのお願い」（令和8年11月6日） https://www.fsa.go.jp/news/r8/sonota/20261106/20261106.html
- CISA KEVカタログ（当日取得） https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json
- Neat NEAT-SA-2026-11-02（Brotli CVE-2026-111497） https://support.neat.no/article/security-advisory-november-2026-brotli-decoder-vulnerability-cve-2026-111497-affecting-neat-devices/
- Chromium Releases 2026年11月一覧 https://chromereleases.googleblog.com/2026/
- NVD CVE API 2.0（公開日時窓） https://services.nvd.nist.gov/rest/json/cves/2.0

> 本版で新たに確認したのは上記4件の一次情報です。MSRC・各ベンダーの当月告知は取得できておらず、記載していません。

第26版の追加根拠

- CISA KEVカタログ（当日取得） https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json
- Microsoft Security Update Guide（11月分は基準日時点で未公開。定例日は11月10日） https://msrc.microsoft.com/update-guide/
- 警察庁 サイバー警察局 注意喚起（一次情報の本文は未取得） https://www.npa.go.jp/bureau/cyber/koho/caution.html
- 金融庁「現下の情勢を踏まえた金融機関利用者へのお願い」（11月6日、第25版で既報） https://www.fsa.go.jp/news/r8/sonota/20261106/20261106.html
- NVD CVE API 2.0（公開日時窓） https://services.nvd.nist.gov/rest/json/cves/2.0

> 警察庁の件は報道（二次情報）に基づき、一次情報の本文を取得していない旨を本文に明記しています。