JP AAWG JAPAN ANTI-ABUSE WORKING GROUP

脆弱性急増時代のリスク管理 ― 業界はどう立ち向かうか

株式会社クオリティア

平野美賢

目次

- 自己紹介
- 注意事項
- 脆弱性を取り巻く現状
  - 脆弱性の公開件数、2026年は"爆増“
  - 脆弱性急増の背景 ― AIによる自動化
  - NVD（脆弱性データベース）の現状
- 皆さんに聞きたいこと

JPAAWG

自己紹介

- モデレータ：平野美賢（株式会社クオリティア）
  - Role: 社内システム管理・ISMS委員、JPAAWGプログラム委員
  - 好きな技術：CI/CD、AWS
  - 趣味：ミュージカル・宝塚観劇

- ノートテイカー：石本裕也（株式会社クオリティア）
  - Role: Webメールサービス 開発者
  - 趣味：レトロゲーム

注意事項

- 本セッションは “Open Round Table” です
  - **対等なポジション**
    - 上座・下座はなく、全員が同じ目線で発言できる。
  - **双方向の対話**
    - 主催者が一方的に話すレクチャー形式ではなく、参加者同士の相互理解やアイデア創出を目的とする。
  - **他者の意見を尊重する**
    - 自身の意見を自由に発言してよいですが、他人の意見に耳を傾けましょう。
- 宣伝はおやめください
- 録画、録音はおやめください



脆弱性を取り巻く現状

JPAAWG

脆弱性の公開件数、2026年は"爆増"

- 2021年：20,161件
- 2022年：25,059件
- 2023年：28,961件
- 2024年：40,077件
- 2025年：48,244件
- 2026年：72,812件（※9月末時点ですでに2025年の1.5倍超）
- 2026年 1日平均267件（2025年は132件）

※ 出典
2021～2024年：CVE Program Metrics
2025年：日経クロステック
2026年（9月末時点累計・1日平均）：jgamblin/monthlyCVEStats（GitHub）
https://github.com/jgamblin/monthlyCVEStats

JPAAWG

脆弱性急増の背景 ― AIによる自動化

- AIによる脆弱性発見の自動化が進んでいる
- 専門家が数週間かけて発見 → AIツールが数時間～数分で発見・エクスプロイト化
- Claude Mythos（Anthropic）など高性能モデルが相次いで登場
- 公開CVEのエクスプロイトコードをAIが10～15分・約1ドルで生成可能（CSA, 2026）
- PoC公開済みの脆弱性への攻撃の88%が公開後48時間以内に発生（CrowdStrike, 2026年8月）
- 月間公開件数：2026年1月5,045件 → 8月10,740件（約2倍）（Google GTIG）

※ 出典
CSA「Collapsing Exploit Window」／CrowdStrike 2026 Threat Hunting Report／Google GTIG

NVD（脆弱性データベース）の現状

- CVE → NVD分析 → CISA KEV という3段階構造が機能不全に
- NISTが2026年4月に方針転換：全CVEの15～20%のみ詳細分析
- CVSSスコアがつかない脆弱性が大量発生
- 「スコアを見て優先順位を決める」アプローチが通用しなくなりつつある
- 平均パッチ適用時間（MTTR）：重大脆弱性で43日（Verizon 2026 DBIR）攻撃側の速度に対して防御側は追いついていない
- 一方、AI発見の脆弱性のうち実際に悪用されたのは1.3%（VulnCheck, 2026年上半期）件数増加の大半は「実際には悪用されていない」

※ 出典
NIST NVD / Verizon 2026 DBIR / VulnCheck KEV Research



皆さんに聞きたいこと

皆さんに聞きたいこと

- AIツールが数時間～数分で発見・エクスプロイト化している中、現場の対応はどう変わっているか？
- CVSSスコアが使いにくくなっている中で、脆弱性の優先順位付けをどう行っているか？
- AIを防御側に活用している事例はあるか？
- 業界全体で連携・情報共有できることはあるか？