Monthly Topics 2026.08

・AI の時代に即した NVD の在り方：NIST がRFIを公開

・AI Agent による継続的な攻撃

CSIRT トレーニングセンター

① AI の時代に即した NVD の在り方：NIST がRFIを公開

AI 時代の NVD のあり方：NIST が RFI (Request for Information) を公開

出典：NIST／Federal Register (2026/08/12) | IoT OT Security News (2026/08/14)

RFI（情報提供依頼）の概要

公開	2026年8月12日 Federal Register
目的	意見を NVD の今後の設計・運用方針に反映。 **スケーラビリティ・自動化・相互運用性・透明性・有用性** の向上
募集対象	研究者・セキュリティ専門家・ ソフトウェアベンダー・政府機関など
募集分野	7分野（次ページ）

2026/10/13

意見募集期限（NIST）

背景：脆弱性情報の急増・複雑化と NVD の現状

263%

CVE 提出件数の増加（2020→2025年）

+1/3

2026年 Q1 も前年同期比で約1/3増

→「公開 CVE を人間が順次補完する」従来モデルではスケールしない

すでに始まった転換：リスクベース優先処理（ 2026年4月～NIST）

• **KEV 掲載 CVE**	受領後1営業日以内の enrichment が目標
• **連邦政府利用ソフトの CVE**	優先的に分析
• **Critical Software の CVE**	優先的に分析
– **それ以外の CVE**	Lowest Priority：登録はされるが追加分析は後回しの場合も

① AI の時代に即した NVD の在り方：NIST がRFIを公開

AI による NVD の再設計：継続的・文脈依存・自動化へ

RFI の目的：NVD のスケーラビリティ・自動化・相互運用性・透明性・有用性の向上

従来
定期・静的

定期的なスキャン → CVSS 等で優先順位付け → 手作業による修正

将来
Continuous / Contextual / Automated

継続的な情報取得 — 自動分析 — 組織・資産の状況を踏まえたリスク評価 — 修正 — 継続監視

NIST が RFI で意見を求めている7分野

1 脆弱性管理プロセス
どこを AI で自動化し、
どこを人間がレビューすべきか

2 脆弱性情報の配信
情報をより迅速・正確に届ける方法

3 リスク評価・優先順位付け
CVSS だけでなく実環境や
脅威情報をどう考慮するか

4 修正・展開・監視
AI による自動修正を
どこまで許容するか

5 脆弱性データ・標準
CVE・CPE・CVSS・
機械可読データをどう改善するか

6 開発プロセス
AI を開発ライフサイクルへ
どう組み込むか

7 将来の NVD
今後5年間のNVDの
役割そのものを再設計

💡
CVE 番号・製品名・CVSS だけで AI 時代の優先順位付けに十分か ―
NIST 自身が問い直している

関連する取り組み： NIST・Linux Foundation・Chainguard

AI 時代の脆弱性管理を、それぞれ異なるレイヤーで支える 3つの動き

Athena

Chainguard（2026年6月 発足）

- AI 等が発見した未公開の脆弱性を集約・検証し、公開前に修正版と防御策を準備（Find → Fix → Shield）
- CVE 化されない脆弱性は OSV レコードとして配信し、スキャナの空白を埋める
- 提出された脆弱性の 42% が Critical/High、86% がネットワークから到達可能（自己申告値）

40,000+ findings / 2,000+ パッチ

Akrites

Linux Foundation（2026/06/25 発表）

- OSS 全体で利用できる共有 SIRT。報告の集約・重複排除・検証・修正・協調的開示を業界横断で担う
- メンテナー不在の重要 OSS では ”Maintainer of Last Resort” として修正を支援
- AWS・Google・Microsoft/GitHub・Anthropic・OpenAI など20社超が創設参加

2026年9月 本格稼働予定

V-etalon

NIST

- AI を利用して脆弱性情報の enrichment（深刻度・影響製品の付与）を支援
- NIST 自身が開発に着手。NVD 近代化の実装側の動き

開発中

競合ではなく役割分担

Athena（発見→修正→公開前防御）→ Akrites（メンテナー調整→協調的開示）→ NVD / CVE / OSV（識別・標準化・流通・リスク評価）

② AI Agent の脅威

AI Agent による継続的な攻撃：失敗しても新たなツールを生成

出典：IoT OT Security News (2026/08/14)

AI エージェントは固定されたマルウェアや単一のエクスプロイトに依存しない。攻撃が失敗すると新しいスクリプトやツールを作成し、別の経路を試す。防御側が特定のファイルや通信をブロックしても停止せず、次の手段へ移行する。

2026年7月の事例では約17,600件のアクションが確認され、その多くは失敗していた。それでも試行回数と適応力によって攻撃は成立する。端末に固定的な痕跡を残さず活動を継続できる点が、従来の「永続化」と異なる。

事例のタイムライン（ 2026年7月）

- 侵入：自己ホスト型 JFrog Artifactory の未知の欠陥を発見・悪用
- 連携：複数エージェント間で情報を共有する仕組みを構築
- 遮断→再構築：通信経路を遮断されると別の経路を再構築
- 到達：Hugging Face の本番インフラへ約2日半、活動を継続

🏭 サプライチェーンへの拡大

実在組織へ接触し、悪意あるパッケージをPyPI に公開

15台のシステムでダウンロード・実行された事例も

⚠️ 何が新しいのか

失敗しても停止せず、新しいツールを生成し続ける

ブロックされた経路を捨てて別経路を再構築

固定的な痕跡（ファイル・タスク）に依存しない

② 防御側への示唆

ファイル検知から「行動の追跡」へ

AI Agents Don't Stop When Malware Fails — IoT OT Security News (2026/08/14)

🚫 不十分になる対策

- ハッシュ値・特定ファイルの検知だけの防御
- 単一の悪性ファイル・通信のブロック
- 端末上の痕跡に依存した永続化の検出
- 修正できない技術的負債の放置

⚔️

✅ 必要になる対策

- 一連の不審な行動パターンの追跡
- アカウント・権限・接続先・操作の可視化
- 即座に権限を取り消せる体制・承認フロー
- AI エージェントの操作ログ取得

従来型マルウェア vs AI エージェント

比較軸	従来型マルウェア	AI エージェント
攻撃手段	固定されたツール・単一経路	失敗すると新ツール生成・別経路
永続化	端末上の変更・タスクに残る	固定的な痕跡を残さず継続
対策の軸	ファイル・シグネチャ検知	挙動監視・権限管理・迅速な更新

参照記事一覧

1. AI の時代に即した NVD の在り方：NIST が有識者の意見を求め始めた
   iototsecnews.jp 2026/08/14
2. RFI: Modernizing the National Vulnerability Database in the Age of AI（意見募集期限 2026/10/13）
   nist.gov / Federal Register 2026/08/12
3. NIST Updates NVD Operations to Address Record CVE Growth
   nist.gov 2026/04
4. Linux Foundation and Industry Leaders Launch Akrites（20社超が創設参加）
   linuxfoundation.org / akrites.org 2026/06/25
5. Exclusive: Linux Foundation's Akrites to Go Live in September
   infosecurity-magazine.com 2026/08/19
6. Athena: Chainguard announces an industry coalition ／ Expanding Athena
   chainguard.dev 2026/06〜07
7. AI Agent による継続的な攻撃：マルウェアの試行に失敗しても新たな悪意のツールを生成する
   iototsecnews.jp 2026/08/14