脆弱性
対応
勉強会

初めてのSCAP

CVE, CWE, CPEなどはどこから来たのか

hogehuga

2025-09-14

はじめに

はじめに & アジェンダ

この資料で説明すること

- SCAPとは何か
- なぜSCAPは生まれたのか、何なのか
- SCAPを構成する主要な要素たち（全部ではない）

本日のゴール

- 「CVEとかCWEとか色々あるね」という状態から、「こういう目的でCVEやCWEなどが作られたのか！」という理解を得る

1. SCAPとは

1.1. SCAPとは？（全体像）

- SCAPを一言でいうと：
  - 「情報システムのセキュリティ設定や脆弱性評価を自動化するための共通言語・フレームワーク」です
- SCAPが解決すること：
  - 手動での脆弱性チェックは手間と時間がかかる
  - ツールごとに結果の形式がバラバラで比較しづらい
  - 脆弱性の深刻度や種類を共通の基準で評価したい
- 重要なポイント：
  - SCAPは「単一のツール」ではなく、「CVE」や「CPE」など、複数の異なる標準を組み合わせて使う「仕組み」です

1.2. SCAPの歴史

- 誕生のきっかけ：
  - 2002年、米国で成立したFISMA（連邦情報セキュリティ管理法）という法律が、連邦政府機関の情報セキュリティ管理を義務付けました
- NISTによる開発：
  - この法律の要求を満たすため、NIST（米国国立標準技術研究所）が脆弱性管理の自動化標準としてSCAPを開発しました
- 管理団体の分化：
  - 当初はNISTが全てを管理していましたが、セキュリティ情報の多様化と国際的な普及のため、専門団体が各標準を管理する体制に移行しました
- SCAPの進化：
  - 時代に合わせて更新され、現在はSCAP 1.3が最新版

年表（当勉強会作成）

バージョン	公開年	主な変更点	技術的特徴
FISMA	2002	連邦情報セキュリティ管理法	2002/12に成立し、SCAPが出るまで手動管理
v1.0	2008	初版、FISMA対応のための自動化基盤	XMLベース、CVE/CPE/OVAL/XCCDFを統合
v1.1	2011	仕様整理と拡張	XCCDF/OVALの表現力向上、相互運用性を改善
v1.2	2012	国際標準との整合性強化	ISO/IEC標準とリンク、構成管理や資産管理の連携を意識
v2.0	2016	構成要素のモジュール化を導入	複数仕様を"コンポーネント"として整理
v2.1	2017	改定版、実装上の不整合を解消	API利用を想定した改良、v3への橋渡し
v3.0	2018	大幅刷新、モジュール化を本格化	各仕様を独立コンポーネント化、クラウド対応強化
v3.1	2020	改良版、クラウド/コンテナ利用に最適化	コンテナや仮想化基盤利用を強化
v4.0	2024	モダン化、JSON形式へ刷新	JSONベースに移行、クラウドモバイル対応

1.3. 管理団体の分化

SCAPを構成する要素は、それぞれの専門家が管理しています。

要素名	管理団体・機関	役割
CVE	MITRE Corporation -> CVE Foundation	脆弱性の識別子を管理
CWE	MITRE Corporation (with CVE Community)	ソフトウェアの弱点を分類・整理
CPE	MITRE Corporation (part of NVD)	IT製品の命名規則を管理
CVSS	FIRST	脆弱性の深刻度をスコアリング
SWID	ISO/IEC	ソフトウェアの識別子を管理
XCCDF/OVAL	MITRE Corporation (transferred to CISecurity)	設定評価の記述言語を管理

もともとはMITREが中心でしたが、現在はNISTがSCAPの枠組み全体を統括し、各コンポーネントは国際的な普及と専門性向上のため、別々の団体が管理しています。

2. 最新のSCAP

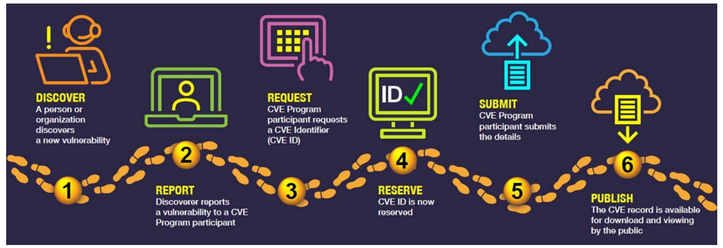
2.1. SCAP 1.3の構成要素（全体像）

- SCAP 1.3が目指すこと：
  - 脆弱性だけでなく、ソフトウェア資産管理やセキュリティ設定評価まで、より広範なセキュリティ管理を自動化すること。
- **主要な**構成要素：
  - ID・識別子： CVE, CWE, CPE
  - 評価記述言語： XCCDF, OVAL, OCIL
  - 評価結果の報告： ARF
  - その他： CVSS, SWID Tags
    - 「XCCDFで設定評価のルールを記述」し、「OVALでシステムを検査」し、「見つかった脆弱性をCVEで識別」し、「その深刻度をCVSSで評価」する、という流れになります。

2.2. CVE（Common Vulnerabilities and Exposures）

- 概要：
  - 既知の脆弱性に対して、世界共通のユニークなIDを付与するリストです。
- どう登録される？：
  - 世界中の「CNA（CVE Numbering Authority）」と呼ばれる組織（ベンダー、研究機関など）が脆弱性を発見・公開し、CVE番号を申請・登録します。
- 例：
  - CVE-2021-44228
    - 通称「Log4j脆弱性」として知られる、インターネット全体に大きな影響を与えた脆弱性です。

補足：CVE登録プロセス



from https://www.cve.org/About/Process

1.	Discover（発見）	脆弱性を発見する（発見者）
2.	Report（報告）	発見者が CVEプログラムパートナー に脆弱性を報告
3.	Request（割当要求）	CVEプログラムパートナーはCVE-IDを割当
4.	Reserve（予約）	CVE-IDが予約済み状態となる
5.	Submit（提出）	CVEプログラムパートナーが詳細を提出する
6.	Publish（公開）	担当のCNAによってリストに公開される

CVE Program Parrtner：CVEプログラム全体の協力者（CNAより広範囲）

CNA(CVE numbering Authority)：CVEプログラムパートナーの実務を担う

2.3. CWE（Common Weakness Enumeration）

- 概要：
  - ソフトウェアの設計やコーディングに潜む「弱点（Weakness）」を分類したものです。
- CVEとの違い：
  - CVEは「何が危険か（個別の脆弱性）」
  - CWEは「なぜ危険か（脆弱性の原因となる弱点の種類）」
- 例：
  - CWE-89：「不適切なSQLクエリの組み立て」 -> SQLインジェクションにつながる弱点。

2.4. CPE (Common Platform Enumeration)

CPE：Common Platform Enumeration

- 概要：
  - オペレーティングシステム、アプリケーション、ハードウェアなどのIT製品を識別するための統一された命名規則です。
- どう使われる？：
  - CVE情報と紐づけて、「どの製品の、どのバージョンに脆弱性が存在するか」を正確に特定するために使われます。
- 例：
  - cpe:/o:microsoft:windows_server_2016
  - cpe:/a:apache:http_server:2.4.54

2.5. CVSS (Common Vulnerability Scoring System)

- 概要：
  - 脆弱性の深刻度を客観的な指標で評価するための採点システムです。
- どう算出される？:
  - 脆弱性の悪用可能性（攻撃ベクトル、複雑性など）、影響範囲（機密性、完全性、可用性）など、複数の要素に基づいてスコアを算出します。
- 例：
  - スコア：0.0〜10.0
    - 9.8 (Critical): 深刻度が非常に高い。Log4jの脆弱性などが該当します。
    - 6.3 (Medium): 中程度の深刻度。

2.6. OVAL（Open Vulnerability and Assessment Language）

- 概要：
  - システムの脆弱性や設定を評価するための、コンピュータが解釈可能な言語です。
- 役割：
  - 「このバージョンのWindowsは、特定のレジストリ設定がこうなっているか？」といったチェックをXML形式で記述します。

2.7. SWID Tags（Software Identification Tags）

- 概要：
  - ソフトウェアのインストール状況やライセンス情報（GPLやApache License等）などを識別するための標準タグです。
- 役割：
  - 資産管理ツールが、PCにインストールされているソフトウェアを正確に特定し、脆弱性情報を照合するのに役立ちます。
- 補足：
  - SBOM（Software Bill of Material）の記述形式として利用されます。
  - 対象に含まれるソフトウェアやライブラリなどの名前やバージョン、ライセンスなどを記載します。

3. まとめ

3 まとめ

SCAPは、情報セキュリティ管理を自動化・標準化するための共通言語です。

- CVEやCWEなど、それぞれの専門家が管理する複数の標準をNISTがフレームワークとして統合しています。
- SCAPを利用することで、脆弱性管理やセキュリティ設定の効率的な運用が可能になります。

よく使うフレームワークや仕組みは、気になったときに調べてみると役に立つことがあります。

X. Appendix

Appendix

- CVE
  - MITRE Corporation https://www.cve.org/
    - 登録プロセス https://www.cve.org/About/Process
- CWE
  - MITRE Corporation https://cwe.mitre.org/
- CPE
  - NIST https://nvd.nist.gov/products/cpe

- CVSS
  - FIRST https://www.first.org/cvss/
  - 脆弱性対応勉強会
    https://github.com/hogehuga/vulnRespStudyGroup/tree/master/document/annou
    - 当勉強会でのCVSS v4の解説
- SWID
  - ISO/IEC https://www.iso.org/standard/66528.html
  - NIST https://csrc.nist.rip/projects/software-identification-swid/
- XCCDF
  - NIST https://nvd.nist.gov/ncp/repository
- OVAL
  - CISecurity https://oval.cisecurity.org/

- SCAP
  - NIST https://csrc.nist.gov/projects/security-content-automation-protocol
  - IPA https://www.ipa.go.jp/security/vuln/scap/scap.html
    - ここから、CVEやCPEなどの日本語解説にもリンクしている（が古い）