

5. IPAの脆弱性対策支援ツール等紹介

脆弱性対策情報データベース JVN iPedia

<https://jvndb.jvn.jp/>

- 国内外30,000件以上の製品の脆弱性情報を日本語で提供
- 日付、ベンダ、製品、キーワード等で検索可能
- CVSSに基づく深刻度（CVSS基本値）も記載

最終更新日: 2018/09/15

JVN iPedia 脆弱性対策情報データベース

JVNDB-2018-001412

Oracle Java Micro Edition の Java ME SDK における Installer に関する脆弱性概要

Oracle Java Micro Edition の Java ME SDK には、Installer に関する処理に不備があるため、機密性、完全性、および可用性に影響のある脆弱性が存在します。

CVSS による深刻度 (CVSS とは?)

CVSS v3 による深刻度
基本値: **7.8 (重要)** [NVD値]

- 攻撃元区分: ローカル
- 攻撃条件の複雑さ: 低
- 攻撃に必要な特権レベル: 不要
- 利用者の関与: 要
- 影響の想定範囲: 変更なし
- 機密性への影響(C): 高
- 完全性への影響(I): 高
- 可用性への影響(A): 高

CVSS v2 による深刻度
基本値: 4.4 (警告) [NVD値]

- 攻撃元区分: ローカル
- 攻撃条件の複雑さ: 中
- 攻撃前の認証要否: 不要
- 機密性への影響(C): 部分的
- 完全性への影響(I): 部分的
- 可用性への影響(A): 部分的

JVN

HOME

JVNとは

脆弱性レポートの

脆弱性レポート

VN-JP

VN-JP (連絡不能)

VN-VU

TA

TRnotes

JVN iPedia

脆弱性対策情報データ

検索

JVN iPediaとは

使い方

MyJVN

JVNS/JRSS

ベンダ情報一覧

必要な情報の効率的な収集②

■ MyJVN バージョンチェッカ

<https://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html>

- PCにインストールされているソフトウェア製品のバージョンが最新のものか、簡単な操作で確認可能

ソフトウェア製品名 ▲	チェック結果 ▲(X○一順)	結果詳細 ▲
<input checked="" type="checkbox"/> Adobe Flash Player (Plug-in)	× 最新のバージョンではありません	表示
<input checked="" type="checkbox"/> Google Chrome	× 最新のバージョンではありません	表示
<input checked="" type="checkbox"/> JRE	× 最新のバージョンではありません	表示
<input checked="" type="checkbox"/> Adobe Reader	○ 最新のバージョンです	表示
<input checked="" type="checkbox"/> Becky! Internet Mail	○ 最新のバージョンです	表示
<input checked="" type="checkbox"/> Lhaplus	○ 最新のバージョンです	表示
<input checked="" type="checkbox"/> Mozilla Firefox	○ 最新のバージョンです	表示
<input checked="" type="checkbox"/> Adobe Shockwave Player	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> iTunes	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> LibreOffice	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> Lunascape	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> Mozilla Thunderbird	— インストールされていないか、対象外のバージョンです	

Adobe Flash Player (Plug-in) バージョン情報詳細
あなたのPCに現在インストールされているアプリケーションの判定結果は以下の通りです

[判定]	[インストールバージョン]	[最新バージョン]
×	32.0.0.114	32.0.0.142(WOW64) (2019/02/12時点)

バージョンアップ方法は下記のURLを参照ください。
<https://jvndb.jvn.jp/apis/myjvn/vcchecklist.html#cpid233>

- Adobe Reader、JRE、Google Chrome等、多く利用されている12種類のソフトウェア製品についてチェック可能

■ icat for JSON

<https://www.ipa.go.jp/security/vuln/icat.html>

- HTMLタグを埋め込むことで、IPAが発信する「重要なセキュリティ情報」を自社のイントラにリアルタイムに表示

- 「重要なセキュリティ情報」は、インターネット利用者に広く影響を及ぼす危険なセキュリティ上の問題が対象
- Microsoft、Adobe、Oracle製品など、企業内でも利用度の高い製品について多く発信

重要なセキュリティ情報とは

<https://www.ipa.go.jp/security/security-alert/about.html>

icat for JSON
cyber alert system

更新日:2019年02月27日 IPAセキュリティセンター:重要なセキュリティ情報

2019年02月27日 「ナブラーク」における汎用データフォーマット機能における XML 外部実体参照 (XXE) の脆弱性について (JVN#56542712)

2019年02月26日 Drupal の脆弱性対策について (CVE-2019-6340)

2019年02月22日 Adobe Acrobat および Reader の脆弱性対策について (APSB19-13) (CVE-2019-7815)

2019年02月13日 Microsoft 製品の脆弱性対策について (2019年2月)

2019年02月13日 Adobe

■ サーバ用オープンソースソフトウェアに関する製品情報およびセキュリティ情報

https://www.ipa.go.jp/security/vuln/oss/sw_security_info.html

-広く利用されているオープンソースソフトウェアのバージョン情報やセキュリティ情報を掲載

-対象ソフトウェア

Apache Struts, ISC BIND, Joomla!, OpenSSL, WordPress 等

3.ソフトウェア製品のセキュリティ情報

オープンソースソフトウェアとして提供されている、以下のサーバ用ソフトウェア製品について製品開発者情報および、セキュリティに関する情報を掲載、更新（週1回程度）しています。

Apache HTTP Server	Apache Struts	Apache Tomcat	ISC Bind	Joomla!Japan	OpenSSL	WordPress (日本語)
------------------------------------	-------------------------------	-------------------------------	--------------------------	------------------------------	-------------------------	---------------------------------

■ 本日説明した内容相当の動画をYouTubeでも公開しています

https://www.youtube.com/playlist?list=PLi57U_f9scIKfSpnABcnhcOHXJ5XZHEuv

The screenshot shows a YouTube channel page for 'IPA Channel' with 6 videos. The main video is 'CVSSを活用し情報漏洩を防ごう' (Using CVSS to Prevent Information Leakage) with 10,187 views. The playlist includes:

- 1. CVSS活用し情報漏洩を防ごう (6:52)
- 2. CVSS解説 2章 ~「基本評価基準」で脆弱性の技術的な特性を評価しよう~ (13:51)
- 3. CVSS解説 3章 ~「現状評価基準」で脆弱性を取り巻く状況进行评估しよう~ (7:06)
- 4. CVSS解説 4章 ~「環境評価基準」でシステムに求められるセキュリティ要求度とその~ (8:11)
- 5. CVSS解説 5章 ~3つの評価結果を基にして脆弱性の深刻度を数値化してみよう~ (5:31)
- 6. CVSS解説 (統合版) (41:15)

他にもIPAではセキュリティに関する映像コンテンツを公開しています

<https://www.ipa.go.jp/security/videos/list.html>

情報収集先例

■ IPA : 重要なセキュリティ情報

<https://www.ipa.go.jp/security/security-alert/index.html>

Microsoft 製品の脆弱性対策について(2024年1月)

公開日：2024年1月10日
最終更新日：2024年1月10日

注釈： 追記すべき情報がある場合には、その都度このページを更新する予定です。

概要

2024年1月10日（日本時間）に Microsoft 製品に関する脆弱性の修正プログラムが公表されています。これらの脆弱性を悪用された場合、アプリケーションプログラムが異常終了したり、攻撃者によってパソコンを制御されたりして、様々な被害が発生するおそれがあります。

攻撃が行われた場合の影響が大きいため、早急に修正プログラムを適用して下さい。

対策

1.脆弱性の解消 - 修正プログラムの適用

Microsoft 社から提供されている修正プログラムを適用して下さい。
Windows Update の利用方法については以下のサイトを参照してください。

[Windows Update の利用手順 - Windows 11 の場合](#)

[Windows Update の利用手順 - Windows 10 の場合](#)

参考情報

[2024年1月のセキュリティ更新プログラム\(月例\)](#)

[セキュリティ更新プログラムガイド](#)

注釈：閲覧には利用規約への同意が必要な場合があります。

[サイバーセキュリティ注意喚起サービス「icat for JSON」](#)

- IPAが公表する注意喚起情報
 - マイクロソフト・オラクル・アドビ製品等利用者が多く存在するソフトウェアの脆弱性対策情報を掲載
 - 悪用有無を「緊急」「注意」で確認可能
- 緊急

注意
- 下記サービス・ツールでも入手可能
 - サイバーセキュリティ注意喚起サービス「icat for JSON」
 - Twitter 「ICATalerts」 等

■ JVN (Japan Vulnerability Notes)

<https://jvn.jp/>

The screenshot shows the JVN Japan Vulnerability Notes website. At the top, there is a navigation bar with the JVN logo and the text "Japan Vulnerability Notes". Below the navigation bar, there is a blue banner with the text "共通脆弱性評価システムCVSS v2評価の掲載終了のお知らせ (2024-03-08)". The main content area is titled "新着リスト" (New List) and contains a table of vulnerability entries. Each entry includes a JVN ID, a description of the vulnerability, and the date and time of the report.

JVN ID	Vulnerability Description	Date/Time
JVN#48443978:	a-blog cms におけるディレクトリトラバーサルの脆弱性	[2024/03/08 12:00]
JVNVU#91793178:	Chirp Systems製Chirp Accessにおけるハードコードされた認証情報の使用の脆弱性	[2024/03/08 10:00]
JVN#54451757:	SKYSEA Client View における複数の脆弱性	[2024/03/07 15:30]
JVNVU#95852116:	オムロン製マシンオートメーションコントローラ/NXシリーズにおけるパストラバーサルの脆弱性	[2024/03/07 13:00]
JVN#34328023:	富士フイルムビジネスイノベーション製プリンターにおけるクロスサイトリクエストフォージェリの脆弱性	[2024/03/06 16:30]
JVN#82749078:	ブラザー製 Web Based Management を実装しているプリンターやスキャナーにおける複数の脆弱性	[2024/03/06 16:30]
JVNVU#96911165:	Nice製Linear eMerge E3-Seriesにおける複数の脆弱性	[2024/03/06 13:00]
JVNVU#91126191:	Santesoft製Sante FFT Imagingにおける境界外書き込みの脆弱性	[2024/03/06 13:00]
JVN#52919306:	スマートフォンアプリ「東横INN公式アプリ」におけるサーバ証明書の検証不備の脆弱性	[2024/03/06 12:00]
JVNVU#90228926:	Integration Objects製OPC UA Server Toolkitにおけるログ出力内容の不適切な無害化の脆弱性	[2024/03/06 09:30]
JVNVU#95474666:	Delta Electronics製CNCSoft-Bにおけるスタックベースのバッファオーバーフローの脆弱性	[2024/03/01 10:00]
JVNVU#94598176:	MicroDicom製DICOM viewerにおける複数の脆弱性	[2024/03/01 10:00]
JVN#35928117:	RevoWorks 製品における保護メカニズムの不具合の脆弱性	[2024/02/29 14:00]
JVN#77203800:	OET-213H-BTS1 における不適切な初期設定	[2024/02/29 14:00]
JVN#78084105:	OpenPNE 用プラグイン opTimelinePlugin におけるクロスサイトスクリプティングの脆弱性	[2024/02/29 12:00]

- JPCERT/CC、IPAが運営する「脆弱性対策情報ポータルサイト」
- 「情報セキュリティ早期警戒パートナーシップ」制度に基づいて報告され調整された脆弱性対策情報を掲載
- CERT/CC など海外の調整機関と連携した脆弱性対策情報を掲載

■ JPCERT/CC 注意喚起③

<https://www.jpccert.or.jp/at/2024.html>

Ivanti Connect SecureおよびIvanti Policy Secureの脆弱性（CVE-2023-46805およびCVE-2024-21887）に関する注意喚起

最終更新: 2024-02-29

X ポスト メール

JPCERT-AT-2024-0002
JPCERT/CC
2024-01-11（公開）
2024-02-29（更新）

I. 概要

2024年1月10日（現地時間）、IvantiはIvanti Connect Secure（旧: Pulse Connect Secure）およびIvanti Policy Secureゲートウェイにおける脆弱性に関するアドバイザリを公開しました。認証バイパスの脆弱性（CVE-2023-46805）とコマンドインジェクションの脆弱性（CVE-2024-21887）が対象で、脆弱性が組み合わされて悪用されると、遠隔の第三者が認証不要で任意のコマンドを実行する可能性があります。

Ivantiは本脆弱性を悪用する攻撃を確認しており、JPCERT/CCは本脆弱性を悪用したとみられる攻撃が国内組織に対しても行われた可能性があることを確認しています。また、1月16日に本脆弱性を実証するコード（Proof-of-Concept）が公開されて以降、本脆弱性を悪用するさまざまな攻撃が発生しています。本脆弱性の影響を受ける製品を利用している場合、後述「III. 対策」以降に記載の情報およびIvantiが提供する最新の情報を確認の上、回避策の適用や侵害有無を確認する調査などを推奨します。

- JPCERT/CCが公表する注意喚起情報
- 深刻且つ影響範囲の広い脆弱性などに関する情報を掲載
- 情報システムや制御システムに関わる端末やネットワークの構築・運用管理業務、組織内CSIRT業務、セキュリティ関連業務などに関与する担当者、技術者、研究者等が対象
- 官公庁系を含めて国内で広く参照されている

■ 警察庁：@police セキュリティポータル

<https://www.npa.go.jp/bureau/cyber/koho/detect.html>

Javaライブラリ「Apache Log4j」の脆弱性（CVE-2021-44228）を標的とした攻撃の観測について

2021年12月14日

概要

- Javaでログ出力に使われるライブラリ「Apache Log4j」の脆弱性（CVE-2021-44228）に関する情報が、The Apache Software Foundationから公表されています。
- 12月10日以降、当該脆弱性を標的とした攻撃を観測しています。

「Apache Log4j」の脆弱性に対する攻撃の観測状況（グラフ）

- 警察庁が公表する注意喚起情報
- 全国の警察施設のインターネット接続点に設置されたセンサーで観測したアクセス状況などを掲載
- 攻撃の事前準備として行われるサーバの稼働状況確認や脆弱性の有無の確認、脆弱性を悪用したコマンドの試行情報などを掲載

■ 米国 : CISA (Cybersecurity and Infrastructure Security Agency)

<https://www.cisa.gov/>



- アメリカの行政機関のひとつであり、米国土安全保障省の外局
- 制御システム向け勧告（ICS advisory）等を掲載
- 2023年2月24日にUS-CERTとICS-CERTが廃止となり、CISAに統合

■ NVD(National Vulnerability Database)

<https://nvd.nist.gov/>

The screenshot shows the NVD website interface. At the top, it says 'NATIONAL VULNERABILITY DATABASE' and 'NVD'. Below that, there's a green button labeled 'VULNERABILITIES'. The main content is for 'CVE-2020-0768 Detail'. Under 'Current Description', it states: 'A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0823, CVE-2020-0825, CVE-2020-0826, CVE-2020-0827, CVE-2020-0828, CVE-2020-0829, CVE-2020-0830, CVE-2020-0831, CVE-2020-0832, CVE-2020-0833, CVE-2020-0848.' Below the description, it says 'Source: MITRE' and has a link '+View Analysis Description'. At the bottom, there's a 'Severity' section with tabs for 'CVSS Version 3.x' and 'CVSS Version 2.0'. Under 'CVSS 3.x Severity and Metrics:', it shows an NVD icon, 'NIST: NVD', and 'Base Score: 7.5 HIGH'. The 'Vector' is 'CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H'.

- 米国標準技術研究所（NIST）が運営
- CVEで管理されている
- DB検索機能、統計機能を備える
- 約22万件の脆弱性対策情報を登録（2024年2月時点）
- JVN iPediaの情報元の1つ

■ Vulnerability Notes Database

<https://www.kb.cert.org/vuls/>

The screenshot shows the homepage of the Vulnerability Notes Database. At the top, there is a red header with the Carnegie Mellon University logo and a search bar. Below the header, the text 'Software Engineering Institute' and 'CERT Coordination Center' is displayed. A navigation menu includes 'Home', 'Notes', 'Search', 'Report a Vulnerability', and 'Provide a Vendor Statement'. The main content area features the title 'Vulnerability Notes Database' and a paragraph explaining the database's purpose. To the right, there is a circular logo for CERT. Below the logo, a text block describes the database's operation. At the bottom left, a section titled 'Recently Published Vulnerabilities' lists a specific vulnerability: 'VU#660597: Periscope BuySpeed is vulnerable to stored cross-site scripting' dated 'APRIL 06, 2020'.

- カーネギーメロン大学のソフトウェア工学研究所CERT/CCが運営
- CSIRTとして収集・発見した脆弱性情報を公開
- DB検索機能を備え、公開日やCVSS情報などで並び替えも可能
- 世界で初めてCERT/CCが設置された

■ 定例アップデート提供

- マイクロソフト （毎月第2火曜日 更新）

<https://msrc.microsoft.com/blog/categories/japan-security-team/>

- オラクル （年4回 1月,4月,7月,10月）

<https://www.oracle.com/security-alerts/>

■ クライアント系

- アドビ （Adobe Reader など）

<https://helpx.adobe.com/jp/security.html>

- Mozilla （Firefox/Thunderbird など）

<https://www.mozilla.org/en-US/security/advisories/>

- Google(Google Chrome)

<https://chromereleases.googleblog.com/>

- アップル

<https://support.apple.com/ja-jp/HT201222>

■ サーバ、ネットワーク製品系

- シスコ – セキュリティアドバイザー

<https://tools.cisco.com/security/center/publicationListing.x>

- 日立 – セキュリティ情報

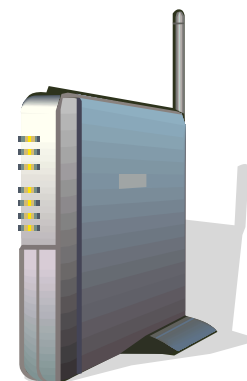
<http://www.hitachi.co.jp/hirt/security/index.html>

- IBM – Security Intelligence

<https://www.ibm.com/blogs/security/jp-ja/>

- Red Hat

<https://rhn.redhat.com/>



■ オープンソース系

■ Apache Foundation

- Apache HTTP Server

https://httpd.apache.org/security/vulnerabilities_24.html

- Apache Tomcat

<http://tomcat.apache.org/security.html>

- Apache Struts

<https://cwiki.apache.org/confluence/display/WW/Security+Bulletins>

■ ISC (Internet Systems Consortium)

- BIND

<https://kb.isc.org/docs/aa-00913>

■ OpenSSL

<https://www.openssl.org/news/vulnerabilities.html>

■ WordPress

<https://wordpress.org/news/category/security/>

■ 国内ニュースメディア

- ITmedia エンタープライズ セキュリティ

<http://www.itmedia.co.jp/enterprise/subtop/security/index.html>

- 日経XTECH セキュリティ

<https://tech.nikkeibp.co.jp/theme/security/>

■ 海外ニュースメディア

- ComputerWorld Security (米国中心)

<http://www.computerworld.com/category/security/>

- The Register Security (英国・欧州中心)

<https://www.theregister.com/security/>



■ Exploit Database

<https://www.exploit-db.com/>

The screenshot shows the Exploit Database website interface. At the top, there are filters for 'Verified' and 'Has App', and buttons for 'Filters' and 'Reset All'. Below the filters, there is a 'Show' dropdown set to '15' and a search box. The main content is a table of exploits with columns for Date, D, A, V, Title, Type, Platform, and Author. The table lists various exploits such as 'Hide My WP < 6.2.9 - Unauthenticated SQLi', 'Akaunting < 3.1.3 - RCE', and 'Ladder v0.0.21 - Server-side request forgery (SSRF)'. At the bottom, it indicates 'Showing 1 to 15 of 45,901 entries' and has pagination controls.

Date	D	A	V	Title	Type	Platform	Author
2024-03-10	↓	×		Hide My WP < 6.2.9 - Unauthenticated SQLi	WebApps	PHP	Xenofon Vassilakopoulos
2024-03-10	↓	×		Akaunting < 3.1.3 - RCE	WebApps	PHP	u32i
2024-03-10	↓	×		Ladder v0.0.21 - Server-side request forgery (SSRF)	WebApps	Go	@_chebuya
2024-03-10	↓	×		DataCube3 v1.0 - Unrestricted file upload 'RCE'	WebApps	PHP	Samy Younsi - NS Labs
2024-03-10	↓	×		Numbas < v7.3 - Remote Code Execution	WebApps	NodeJS	Matheus Alexandre
2024-03-10	↓	×		TP-Link TL-WR740N - Buffer Overflow 'DOS'	WebApps	Hardware	Anish Feroz
2024-03-06	↓	×		GLiNet - Router Authentication Bypass	WebApps	Hardware	Daniele Linguaglossa
2024-03-06	↓	×		elFinder Web file manager Version - 2.1.53 Remote Command Execution	WebApps	PHP	tmsrwr
2024-03-06	↓	×		CSZ CMS Version 1.3.0 - Authenticated Remote Command Execution	WebApps	PHP	tmsrwr
2024-03-06	↓	×		CVE-2023-50071 - Multiple SQL Injection	WebApps	PHP	Geraldo Alcantara
2024-03-06	↓	×		Lot Reservation Management System - Unauthenticated File Disclosure	WebApps	PHP	Elijah Mandila Syoyi
2024-03-06	↓	×		Lot Reservation Management System - Unauthenticated File Upload and Remote Code Execution	WebApps	PHP	Elijah Mandila Syoyi
2024-03-05	↓	×		kk Star Ratings < 5.4.6 - Rating Tampering via Race Condition	WebApps	PHP	Mohammad Reza Omrani
2024-03-05	↓	×		Neontext Wordpress Plugin - Stored XSS	WebApps	PHP	Eren Car
2024-03-05	↓	×		Solar-Log 200 PM+ 3.6.0 Build 99 - 15.10.2019 - Stored XSS	WebApps	Hardware	Vincent McRae, Mesut Cetin

- Offensive Securityが運営する脆弱性の攻撃コード（exploit）の有無を確認できるデータベース
- ペネトレーションテスターや研究者向け

■ Metasploit

<https://www.metasploit.com/>

metasploit®

The world's most used penetration testing framework


Knowledge is power, especially when it's shared. A collaboration between the open source community and Rapid7, Metasploit helps security teams do more than just verify vulnerabilities, manage security assessments, and improve security awareness; it empowers and arms defenders to always stay one step (or two) ahead of the game.

★ Star 15,445

Get Metasploit

OPEN SOURCE	COMMERCIAL SUPPORT
Metasploit Framework	Metasploit Pro
Download	Free Trial
Latest	Latest

[Compare Features >](#)
[View More Projects >](#)

Latest Metasploit Modules  [View All Modules >](#)

TITLE	DATE	AUTHOR
Land #11500, Add more checks to cisco_directory_traversal module	Mar 01, 2019	bcoles
Land #11461, Update manageengine_deviceexpert_traversal.th	Mar 01, 2019	wrchen-7

- Rapid7が運営する脆弱性の攻撃コード（exploits）をモジュールとして提供しているデータベース
- ペネトレーションテスターや研究者向け

脅威・動向に関する情報

意図せずインターネット上に晒されている機器があるかも？

■ SHODAN

<https://www.shodan.io/>

Shodan Developers Book View All...

SHODAN [Search Bar] Explore Developer Pricing Enterprise Access New to Shodan? Login or Register

The search engine for

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started

- Explore the Internet of Things**
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.
- See the Big Picture**
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!
- Monitor Network Security**
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.
- Get a Competitive Advantage**
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

56% of Fortune 100 **1,000+ Universities**

Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

Analyze the Internet in Seconds

Shodan has servers located around the world that crawl the Internet 24/7 to provide the latest Internet intelligence. Who buys Smart TVs? Which countries are building the most wind farms?

- インターネットにつながっているコンピュータ機器の検索エンジン
- サーバ、制御機器、オフィス機器など、5億台以上の情報を格納
- 認証が弱い機器や古いバージョンのまま運用している機器など、セキュリティに問題がある機器も見つけることが可能
- 攻撃者は、攻撃の侵入口となり得る脆弱な機器を探すのに当サイトを使っていると言われている

脆弱性対策は日々の情報収集と
タイムリーな対策が重要です。
自組織にとって危険な脆弱性を
放置しないよう、
適切な対応を行いましょう。



セミナーに対する質問等について

本セミナーに対するアンケートの回答にご協力をお願いいたします。

「<https://info.ipa.go.jp/form/pub/survey/isec-seminar>」
受付期限：2023年3月31日までとなっております

本セミナーに関する質問等は
以下メールアドレスにご連絡ください。

「isec-labsemi-scap@ipa.go.jp」



IPA