Future Vuls

クラウド型脆弱性管理サービス

公開サーバの自己確認ガイド

未適用の修正とサポート切れを確かめる

2026年11月

830件

10月1日～16日のわずか半月で報告された、
不正アクセスによる個人データの漏えい等

今年度（4月～）の報告総数の約4割を、半月で占める異常事態です。
修正プログラムの適用など基本的な対策で、防げる被害は少なくありません。

出典：個人情報保護委員会「最近の不正アクセスによる個人データの漏えい等の傾向」（2026年10月28日）。
割合は2026年4月1日～10月16日の累計2,094件に対するもの。委員会へ直接報告された速報値で、委託元・委託先の双方が報告している場合を含む。
金融業・電気通信業等の委任先省庁経由の報告、行政機関等からの報告は含まない。

Copyright 2026 by Future Corporation. Public

FutureVuls

このガイドで確かめること

特別なツールは不要。サーバ標準のコマンドだけで、2つの「穴」を確かめます

01 未適用のセキュリティ修正

公開されている修正プログラムのうち、
まだ適用していないものはないか

02 サポート切れのソフトウェア

修正がもう提供されない、または近く
提供されなくなるものを使っていないか

想定する読者

管理者権限でサーバに入れる担当者向け。
共用レンタルサーバ等は対象外（後述）

所要時間の目安

1台15〜30分（初回は1時間程度）。未適用が多ければ Critical／Important から照合します

安全について

コマンドは状態を見るだけ。
入っているソフトは変わりません
（Linuxは最新の更新情報の一覧を取り込みます）

時間がないときは、外部公開サーバについて STEP 3（未適用の修正）と STEP 5（サポート切れ）だけでも先に確認してください。

Copyright 2026 by Future Corporation. Public

FutureVuls

5つのステップで進めます

外部公開サーバから始め、悪用が確認されたものを最優先にします

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5
対象サーバを決める	**OSとバージョン確認**	**未適用の修正を確認**	**悪用確認済みを優先**	**サポート切れを確認**
外部公開サーバから始める	何が動いているかを把握する	OS標準機能で一覧を出す	公的機関の一覧から自社製品を拾う	修正が出ないものを洗い出す

すべてを同時に直す必要はありません。STEP 4で「実際に攻撃に使われているもの」を見極め、そこから手を付けるのが近道です。
コマンドのコピーと結果の記入には、付属の記入シート（Excel）を使います。つまずいたら「うまくいかないとき」のページへ。

Copyright 2026 by Future Corporation. Public

FutureVuls

先に知っておきたい用語

手順の中で出てくる5つの言葉です。ここだけ押さえれば、あとは読み進められます

CVE番号

脆弱性ごとに付く世界共通の通し番号。
例：CVE-2026-12345。ベンダー情報や公的機関の一覧は、この番号で引きます

アドバイザリ

OSベンダーが出す修正のお知らせ。RHSA-〇〇（Red Hat）、USN-〇〇（Ubuntu）など。1件に複数のCVEが含まれます

バックポート

新しい版の修正だけを、バージョン番号を変えずに古い版へ取り込むこと。番号が古くても直っている場合があります

KEV

米国CISAがまとめる「実際に悪用が確認された脆弱性」の一覧。載っていれば優先度を一段上げます

サポート切れ（EOL）

ベンダーが修正の提供をやめた状態。新しい脆弱性が見つかっても直らないため、確認コマンドには何も出ません

確認コマンドの多くは管理者権限（Linuxは sudo、Windowsは管理者として起動したPowerShell）で実行します。
どれも状態を表示するだけで、入っているソフトは変わりません（Linuxでは最新の更新情報の一覧をサーバ内に取り込みます）。
重要度はベンダーが付ける深刻さの段階で、高い順に Critical（緊急）、Important（重要）、Moderate（警告。Amazon Linuxでは Medium と表示）、Low（注意）です。

Copyright 2026 by Future Corporation. Public

対象サーバを決める

攻撃者が最初に狙う、インターネットから直接届くサーバから始めます

Webサーバ、メールサーバ、外部向けAPIのサーバなどが該当します。次のような一覧を作ると、後のステップが楽になります。

ホスト名	役割	OS	外部公開	担当者
web01	会社Webサイト	（STEP 2で記入）	あり	○○
mail01	メール	（STEP 2で記入）	あり	○○
api01	外部向けAPI	（STEP 2で記入）	あり	○○

まずは外部公開サーバの5〜10台から。
全台を一度にやろうとしないことが、続けるコツです。

```
# あわせて：待ち受けているポートを見る
sudo ss -tulpn                          # Linux（TCP/UDP）
Get-NetTCPConnection -State Listen      # Windows（TCP）
Get-NetUDPEndpoint                      # Windows（UDP）
```

管理画面・RDP（3389）・SSH（22）・データベースが外部に開いていないかも確認します。上のコマンドはサーバ側の待ち受けを見るもので、外部から実際に届くかは、ファイアウォールやクラウドのセキュリティグループの設定で確かめてください。

Copyright 2026 by Future Corporation. Public

OSとバージョンを確認する

FutureVuls

各サーバで、OSと主なソフトウェアのバージョンを控えます

Linux（共通）

```
# OSの種類とバージョン
cat /etc/os-release
# カーネルのバージョン
uname -r
```

Windows Server（PowerShell）

```
# OSの名称・バージョン
Get-CimInstance Win32_OperatingSystem |
  Select-Object Caption, Version, BuildNumber
```

例：PHPのバージョン

```
# コマンド用のPHPの版
php -v
# パッケージとして入っているPHP
rpm -qa | grep -i php      # RHEL系
dpkg -l | grep -i php      # Ubuntu/Debian
```

ここがポイント

「php -v」では表示されるのに、パッケージの一覧に出てこない場合は、ソースから独自に導入された可能性があります。STEP 3の方法では確認できないため、導入した担当者や構築ベンダーに更新方法を確認してください。なお php -v はコマンド用のPHPです。Webサーバが使うPHP（php-fpm など）と版が違うことがあるので、パッケージ一覧とあわせて確認します。

Copyright 2026 by Future Corporation. Public

控えておくソフトウェアの例

公開している機能のソフト名と版を控えます。STEP 4で一覧を探す手がかりになります

種類	代表的なソフト
Webサーバ	Apache（httpd）、nginx、Tomcat、IIS
プログラムの実行環境	PHP、Java、Node.js
データベース	MySQL、MariaDB、PostgreSQL、SQL Server
メール	Postfix、Exim、Dovecot
CMS・業務アプリ	WordPress、Jenkins、GitLab、Confluence
ファイル共有・リモート接続	Samba、OpenSSH、リモートデスクトップ

何が動いているかを見るコマンド

```
# Linux：動いているサービスの一覧
systemctl list-units --type=service --state=running
# RHEL系：主なソフトの版
rpm -qa | grep -iE 'httpd|nginx|tomcat|php|mysql|mariadb|postgres|postfix|exim|samba'
# Ubuntu／Debian：主なソフトの版（Apacheは apache2）
dpkg -l | grep -iE 'apache2|nginx|tomcat|php|mysql|mariadb|postgres|postfix|exim|samba'
# Windows：インストール済みソフトの一覧
Get-ItemProperty HKLM:¥Software¥Microsoft¥Windows¥
  CurrentVersion¥Uninstall¥* | Select-Object DisplayName, DisplayVersion
```

WordPressやJenkinsなどは管理画面にも版が表示されます。分からないものは、構築ベンダーにソフトと版の一覧をもらうのが確実です。
Windowsのコマンドは1行につなげて入力します。PDFからコピーすると記号（¥）が正しく入力されないため、記入シートの「コマンド一覧」からコピーするか、手で入力してください。

Copyright 2026 by Future Corporation. Public

未適用のセキュリティ修正を確認する

FutureVuls

OSに備わる機能で、未適用のセキュリティ修正を一覧にします

OS	コマンド
RHEL系	`sudo dnf updateinfo list --security`
Amazon Linux 2023	`sudo dnf updateinfo list --security` `sudo dnf updateinfo list --security --releasever=latest  # 新リリース分も`
Amazon Linux 2 2026年6月30日 サポート終了済み	`sudo yum updateinfo list security`
Ubuntu／Debian	`sudo apt update` `apt list --upgradable 2>/dev/null`
SUSE Linux Enterprise	`sudo zypper list-patches --category security`
Windows Server	`$s = (New-Object -ComObject Microsoft.Update.Session).CreateUpdateSearcher()` `$s.Search("IsInstalled=0 and IsHidden=0").Updates | Select-Object Title`

RHEL系：Red Hat Enterprise Linux、Rocky Linux、AlmaLinux、Oracle Linux。「apt update」はパッケージ情報の取得のみで、更新は行いません。Ubuntu／Debianは、セキュリティ修正が通常の更新に置き換わって表示されることがあるため、表示された全件を対象にします。Windowsは既定の更新元（WSUS配下ならWSUS）を検索するため、WSUSやインターネットへの到達が必要です。WSUSで未承認の更新は表示されず、ドライバなどセキュリティ以外の更新も混ざります。表示まで数分かかることがあります。

Copyright 2026 by Future Corporation. Public

出力の見方と注意点

FutureVuls

何も表示されなければ未適用なし。ただし「空＝安全」とは限らない場合があります

RHEL系・Amazon Linux

1行ごとに「アドバイザリ番号」「重要度」「修正版のパッケージ」が並びます。sudo dnf updateinfo --security で、重要度ごとの件数も出ます

Ubuntu／Debian

表示された行すべてが、更新の必要なパッケージです。重要度とCVE番号は表示されないため、全件を重要として扱います

Windows Server

表示された更新（KB番号）が未適用分。重要度とCVE番号は表示されません。定例の更新は毎月第2火曜日（日本時間は翌水曜日）

注意：「何も表示されない」が安全とは限らない場合

- サポート切れのOS（CentOS 7、Pro未契約のUbuntu 20.04等）：修正自体が出ない（STEP 5）
- RHELのサブスクリプション未登録、社内ミラーが古い：更新情報を取得できない
- Amazon Linux 2023：既定でリリースが固定。--releasever=latest を付けて再確認
- Rocky Linux・AlmaLinux など：修正パッケージより後に重要度の情報が付くことがある。sudo dnf check-update に更新が出ていないかも確認
- Windows（WSUS配下）：WSUSで未承認の更新は表示されない
- Remi などサードパーティ製（RHEL系）：セキュリティの分類が付かず表示されないことがある
- 再起動待ち：新しいカーネル等を入れても、再起動までは古い版が動いている

特定の脆弱性が直っているか（バックポート対策）

```
# RHEL系：そのCVEを直す未適用の修正があるか
sudo dnf updateinfo list --cve CVE-XXXX-XXXXX
#   （Amazon Linux 2023 は --releasever=latest を追加）
# RHEL系：適用済みかを変更履歴で確認
rpm -q --changelog パッケージ名 | grep CVE-XXXX-XXXXX
# Ubuntu／Debian：入っている版の変更履歴で確認
zgrep CVE-XXXX-XXXXX /usr/share/doc/パッケージ名/changelog*
```

件数の数え方は「うまくいかないとき」のページへ。変更履歴にCVE番号があれば修正済みの強い手がかりですが、見つからなくても未修正とは限りません。
履歴ファイルが無いときや迷うときは、ベンダーのCVEページを確認してください。

Copyright 2026 by Future Corporation. Public

STEP 4

悪用が確認されているものを優先する

FutureVuls

公的機関が「悪用確認済み」とした脆弱性から、自社に関係するものを拾うのが近道です

公的機関の一覧を見る（製品名で絞り込む） → 自社の製品を拾う（STEP 2の記録から） → 修正が入っているか確認する（STEP 3） → **入っていなければ最優先で対応**

CISA「KEVカタログ」

米国CISAが公開する、悪用が確認された脆弱性の一覧。CSVをダウンロードし、ベンダー（vendorProject）・製品（product）の列で絞り込めます

cisa.gov/known-exploited-vulnerabilities-catalog

JPCERT/CC「注意喚起」

国内で特に注意が必要な脆弱性を、製品名と対策つきで公表しています。直近数か月分に目を通すのが目安です

jpcert.or.jp/at/

IPA「重要なセキュリティ情報」

広く使われるソフトウェアの、緊急性の高い脆弱性を製品名でまとめています

ipa.go.jp/security/security-alert/

具体的な探し方は次のページ。STEP 3で出た修正からCVE番号を調べて照らし合わせる方法は、その次のページです。

Copyright 2026 by Future Corporation. Public

実践：KEVの一覧から自社のソフトを探す

OS名ではなく、中で動くソフトの名前（PHP、Apacheなど）で探すのがコツです

1 CSVをダウンロード

KEVカタログのページの「CSV」から。記入シートの「コマンド一覧」に直リンクがあります

2 Excelで開く

「データ」→「テキストまたはCSVから」で開くと文字化けしにくくなります

3 ソフト名で絞り込む

vendorProject列とproduct列で「テキストフィルター」→「指定の値を含む」。表記が揺れるため「php」「apache」「tomcat」など短い語で

4 新しい順に並べる

dateAdded列を降順に。2回目以降は前回確認した日より後の追加分だけ見れば十分です

作例：PHPを使っている場合

「php」で絞ると10件。phpMyAdminなど別の製品も混ざるので、自社で使う製品だけ残します。数年前のCVEは、サポート中の版を使っていれば通常は修正済みです。

まず確認するのは、10月26日に追加された CVE-2026-109618／109619（通称 PHP2Shell）。修正が入っているかを、STEP 3の変更履歴コマンドで確かめます。

件数の多いものは「最新の更新」で判断

Microsoft／Windows は173件、Linux／Kernel は32件。1件ずつは追いません。ただしサポート中のOSに限ります（STEP 5で確認）。

Windows：STEP 3のコマンドで何も表示されなければ最新の累積更新が入っており、それより前の掲載分は修正済み（Exchange・SQL Serverなどは別に更新）

Linuxカーネル：STEP 3でカーネルの更新が出ず、再起動も済んでいれば問題なし

knownRansomwareCampaignUse列が「Known」のもの（361件）は、ランサムウェアでの悪用も確認済み。最優先の中でも先に対応します。件数は2026年11月4日時点のCSVによる。

Copyright 2026 by Future Corporation. Public

OS別：修正からCVE番号を調べる

STEP 3で出た修正に、どの脆弱性（CVE）が含まれるかを調べる方法です

OS	STEP 3で分かること	CVE番号の調べ方
RHEL系・Amazon Linux	アドバイザリ番号（RHSA／RLSA／ALSA／ALAS）と重要度	`sudo dnf updateinfo info アドバイザリ番号` 表示にCVE番号の一覧が含まれます。Amazon Linux 2023 は末尾に --releasever=latest を付けます（付けないと何も出ません）。Amazon Linux 2 は yum updateinfo info
SUSE Linux Enterprise	パッチ名と重要度	`sudo zypper list-patches --cve` パッチごとにCVE番号が表示されます
Ubuntu	更新が必要なパッケージ名と版のみ（重要度・CVEは出ない）	`ubuntu.com/security/notices` パッケージ名で検索し、Ubuntuの修正情報（USN）に載るCVE番号を確認
Debian	パッケージ名と版のみ（重要度・CVEは出ない）	`security-tracker.debian.org/tracker/` パッケージ名で検索し、修正済みの版とCVE番号を確認
Windows Server	更新のタイトルとKB番号のみ（重要度・CVEは出ない）	`msrc.microsoft.com/update-guide` KB番号で検索し、その更新で直るCVE番号と深刻度を確認

重要度が表示されないOS（Ubuntu／Debian／Windows）は、記入シートの「うちCritical／Important」欄に、表示された更新の件数をそのまま記入してください。迷ったら重要として扱うのが安全側です。

Copyright 2026 by Future Corporation. Public

サポート切れを確認する

FutureVuls

「未適用なし」は安全の証明ではありません。修正がもう出ていないだけの可能性があります

近年サポートが終了した・終了が近い主な例

OS・ソフトウェア	サポート（2026年11月確認）
CentOS 7 ／ RHEL 7	2024年6月 終了
Amazon Linux 2	2026年6月30日 終了済み
Windows Server 2012 / R2	2023年10月 終了（有償ESUも2026年10月終了）
Windows Server 2016	2027年1月12日 終了予定（有償ESUあり）
Ubuntu 20.04 LTS	2025年5月 標準終了（Proで延長）
Ubuntu 22.04 LTS	2027年5月 標準終了予定
Debian 11	2026年8月 終了（LTS含む）
Debian 12	2026年7月 通常終了（LTSは2028年6月）
PHP 8.1 ／ 8.2	2025年12月 終了 ／ 2026年12月 終了予定
MySQL 8.0	2026年4月 終了

※日付は必ず各ベンダーの公式情報で最新のものを確認してください（横断的にはendoflife.dateが便利）。
12か月以内に終了するもの（Windows Server 2016、PHP 8.2、Ubuntu 22.04など）も移行計画の対象です。

見落としやすい「実質的なサポート切れ」

アプリケーションが使うライブラリ（npm、PyPI、Composerなど）には、終了宣言がないまま開発が止まっているものが少なくありません。

CVEベースの脆弱性スキャナは「既知の脆弱性がない」限り何も報告しないため、公式情報だけでは見つかりません。

→ フューチャーのOSS「uzomuzo-oss」で確認できます（後述）

Copyright 2026 by Future Corporation. Public

結果の読み方と対応の優先順位

「悪用確認済み × 外部公開」から手を付けると、限られた時間で効果が出ます

優先度	確認結果	対応の目安
最優先	悪用確認済みの脆弱性が、外部公開サーバに該当	できるだけ早く修正を適用。難しければ回避策や外部からのアクセス制限を検討
高	サポート切れのOS・ソフトウェアが外部公開サーバで稼働	移行計画を立て、移行までは外部からの露出を減らす
優先	外部公開サーバで Critical／Important が未適用、またはサポート終了まで12か月以内。社内サーバで悪用確認済みの脆弱性が該当	次の計画メンテナンスを待たずに適用を検討。社内サーバも、侵入後の横展開に使われるため後回しにしない
計画	上記以外（社内向けサーバの Moderate 以下の修正など）	定期メンテナンスで計画的に適用

Copyright 2026 by Future Corporation. Public

点検チェックリスト（見本）

記入用のExcelファイルを別途ご用意しています。ここでは、どんな項目を確認するかの見本です

実施日：　　年　　月　　日　　担当：　　対象サーバ（ホスト名）：　　役割：

☐	STEP	確認すること	結果・メモ（記入）
☐	**STEP 1**	外部公開か（Web／メール／API／VPN等）	外部公開：あり ・ なし
☐	**STEP 1**	待ち受けポート（TCP/UDP）とFW・クラウドの公開設定を確認した	不要な公開：あり ・ なし
☐	**STEP 2**	OSの種類とバージョンを控えた	OS：
☐	**STEP 2**	主なソフト（Web・DB・メール等）の版と導入方法を控えた	
☐	**STEP 3**	未適用のセキュリティ修正を一覧にした（重要度が出ないOSは全件を重要扱い）	件数：　　件（うちCritical／Important：　　件）
☐	**STEP 3**	「空」の場合、STEP 3の注意点（7つのケース）に当てはまらないか確かめた	
☐	**STEP 4**	KEV／JPCERT／IPAの一覧から自社製品を拾い、修正の有無を確認した	悪用確認済み：あり ・ なし
☐	**STEP 5**	OS・ソフトウェアのサポート期限を確認した	終了済み ・ 12か月以内 ・ 問題なし
☐	**判定**	PRIORITYの表で優先度を決めた	最優先 ・ 高 ・ 優先 ・ 計画
☐	**対応**	対応内容と予定日を決め、担当者を割り当てた	予定日：　　／　　担当：

付属のExcel「点検チェックリスト」シートは1台につき1シート。結果はプルダウンで選び、終わったら「サーバー覧」に転記します。

Copyright 2026 by Future Corporation. Public

FutureVuls

サーバ別 記入シート（見本）

付属のExcel「サーバー一覧」シートと同じ項目です。Excelでは優先度が自動で判定されます

ホスト名	役割	外部公開	OS・バージョン（STEP 2）	未適用件数（STEP 3）	Critical／Important	悪用確認済み（STEP 4）	サポート切れ（STEP 5）	優先度	対応予定・担当
web01	会社Webサイト	あり				あり ・ なし			

優先度の目安：悪用確認済み×外部公開＝最優先／サポート切れ×外部公開＝高／外部公開でCritical・Important未適用、外部公開でサポート終了12か月以内、社内で悪用確認済み＝優先／それ以外＝計画。1行目はグレーの記入例です。

Copyright 2026 by Future Corporation. Public

うまくいかないとき

よくあるつまずきと対処です。多くはこのページで解決できます

こんなとき	考えられる原因と対処
「権限がありません」「Permission denied」と出る	管理者権限が必要です。Linuxはコマンドの先頭に sudo、Windowsは PowerShell を右クリック→「管理者として実行」。「Failed to download metadata … Permission denied」もこの例です（AWS上のRHELなど）
「dnf: command not found」と出る	古いOS（CentOS 7、RHEL 7、Amazon Linux 2）は dnf の代わりに yum を使います（yum updateinfo list security）。いずれもサポート終了済みです（STEP 5）
RHELで「not registered」などと出る	サブスクリプション未登録で、更新情報が取れていません。登録状況を契約窓口や構築ベンダーに確認してください
apt や dnf がエラーになる・止まる	サーバがインターネット（または社内ミラー）につながっていない可能性があります。プロキシ設定などをネットワーク担当に確認します
Windowsのコマンドが終わらない・エラーになる	更新サーバへの接続を待っています。10分ほど待っても終わらなければ、「Windows Update」の画面で更新の有無を確認する方法でも構いません
件数を数えたい（出力が多い）	RHEL系は sudo dnf updateinfo --security で重要度ごとの件数が出ます（Amazon Linux 2023 は --releasever=latest を追加、Amazon Linux 2 は sudo yum updateinfo）。SUSEは一覧の最後の行に件数。Ubuntu／Debianは apt list --upgradable 2>/dev/null | grep -c / で更新が必要なパッケージ数が出ます（パッケージの行にだけ含まれる「/」を数えるので、言語設定に関係なく数えられます）
どのサーバが外部公開か分からない	ファイアウォールやクラウドの設定画面、構築時の構成図で確認します。なければ構築ベンダーに一覧を依頼してください
修正を当ててよいか判断できない	業務への影響を確認のうえ、社内の手順で適用します。判断に迷うときは、OS・製品のベンダーや保守契約先に相談してください

本ガイドは無償公開の資料のため、個別の技術的なご質問にはお答えしていません。お使いのOS・製品のベンダーや、保守契約先にご相談ください。

Copyright 2026 by Future Corporation. Public

続けるための月1回の見直し

FutureVuls

一度きりで終わらせず、月1回の見直しを続けます（サーバ5台程度なら15分ほど）

01

タイミング

毎月第2火曜日の翌日（日本時間の水曜日）に出る定例更新の後。カレンダーに予定を入れておくと続きます

02

新しく載ったものを見る

KEVのCSVを dateAdded 順にし、前回確認日より後の追加分だけ確認。JPCERT/CC・IPAの新着もあわせて

03

コマンドを再実行

STEP 3のコマンドで未適用の件数を確かめ、記入シートの「サーバ一覧」を更新

04

期限を見直す

「サポート期限」シートで、12か月以内に入ったものを移行計画に加える

記入シートの「使い方」に、KEVを前回確認した日を書いておく欄があります。
サーバや担当者が増えて手作業がつらくなったら、無償のVulsでの自動化や、FutureVulsでの一元管理も選択肢になります。

Copyright 2026 by Future Corporation. Public

このガイドで確認できないこと

見えない範囲を知っておくことも、点検の大事な一部です

独自に導入したソフトウェア

ソースから導入したものはパッケージ管理の外にあり、STEP 3では見えません

導入した担当者や構築ベンダーに更新方法を確認

CMS・アプリのライブラリ

WordPressのプラグインや、アプリが使うライブラリはOS標準コマンドの対象外です

既知の脆弱性はVuls、保守状況はuzomuzo-ossで確認

VPN装置・ネットワーク機器

ランサムウェア被害の侵入経路の約6割はVPN機器です（警察庁、2025年上半期）。この手順では確認できません

各ベンダーの脆弱性情報を直接確認。管理画面は外部に出さない

すでに侵入されていないか

このガイドは、既知の修正漏れという「入り口」を確認するものです

侵害の疑いがあればJPCERT/CCや専門事業者に相談

設定不備や認証の弱さ（管理画面・RDP・SSHの公開、推測しやすいパスワード、多要素認証なし）も、修正の適用とは別の「入り口」です。
STEP 1で開いているポートを確認し、不要な公開を閉じてください。

このほか、コンテナの中身、RDSなどのマネージドサービス、共用レンタルサーバも対象外です。事業者からの通知や管理画面で、利用中のバージョンとサポート状況を確認してください。

Copyright 2026 by Future Corporation. Public

FutureVuls

確認を続ける・広げるためのOSS

フューチャーは脆弱性対応の底上げのため、2つのツールを無償で公開しています

Vuls（バルス）

脆弱性の確認を自動化する

何ができるか	エージェント不要で、インストール済みソフトと脆弱性情報を照合して一覧化
対象	Linux、FreeBSD、コンテナ、WordPress、言語ライブラリ、ネットワーク機器
ガイドとの関係	STEP 2〜4を自動で定期実行できる

github.com/future-architect/vuls

uzomuzo-oss （有象無象オーエスエス）

保守が止まったライブラリを見つける

何ができるか	保守状況を複数の指標で評価し、7段階に分類
対象	アプリが使うライブラリ（npm、PyPI、Maven、Cargo、Go、NuGet、RubyGems、Packagist）。GitHub Actions のワークフローにも対応
ガイドとの関係	STEP 5で見つからない「実質的なサポート切れ」を補う

github.com/future-architect/uzomuzo-oss

Copyright 2026 by Future Corporation. Public

FutureVuls

「既知の脆弱性ゼロ」でも、安全とは限らない

実稼働環境の約1万6千パッケージのうち、約半数にライフサイクル上のリスクがありました

48%

ライフサイクル上のリスクがあった割合。CVEベースの脆弱性スキャナでは検出対象外になりやすいリスク

```
# 1つのライブラリを確認
uzomuzo scan pkg:npm/express@4.18.2
# 依存ライブラリをまとめて確認
trivy fs . --format cyclonedx | uzomuzo scan --sbom -
```

分類	意味と対応の目安
Active	保守が続いている。対応不要
Legacy-Safe	更新はないが既知の問題なし。受容か固定
Stalled	保守が低下・凍結。監視し移行を計画
EOL-Scheduled	終了日が予告済み。期日までに移行
EOL-Confirmed	公式に終了・非推奨。すぐに移行
EOL-Effective	宣言はないが実質終了。移行
Review Needed	自動判定不可。個別に確認

出典：フューチャー調べ。FIRST VulnCon 2026（2026年4月）で発表。uzomuzo-oss は Vuls の作者・神戸康多が開発し、Apache License 2.0 で公開。

Copyright 2026 by Future Corporation. Public

FutureVuls

OSSを、組織の運用にのせるとき

2つのOSSを基盤に、企業での継続運用に必要な機能を加え提供しているのがFutureVuls です

FutureVuls （クラウドサービス）が加えるもの

一元管理

多数のサーバやコンテナ、ライブラリの状況を一つの画面で把握

優先度づけ

悪用状況などの情報をもとに、対応すべきものを絞り込む

対応の記録

担当者の割り当てや対応状況を残し、報告や監査に使える形に

保守状況の評価

uzomuzo-oss の手法で、実質的なサポート切れのOSSを検知

Vuls 脆弱性の検知エンジン（無償）

uzomuzo OSS Dependency Lifecycle Management OSSの保守状況の評価（無償）

OSSで十分な場面も多くあります。サーバや担当者が増え、記録や報告が必要になったときの選択肢の一つとしてご検討ください（www.vuls.biz）。

Copyright 2026 by Future Corporation. Public

ご自由にご活用ください

このガイドは、サイバー攻撃が相次ぐ状況を受けて、
FutureVuls チーム（フューチャー株式会社）が作成・公開しています。

OSS Vuls github.com/future-architect/vuls

uzomuzo-oss github.com/future-architect/uzomuzo-oss

FutureVuls www.vuls.biz

本ガイドは2026年11月時点の情報に基づきます。コマンドの実行や修正の適用は、各社の判断と社内の手順のもとで行ってください。
本ガイドは無償公開の資料のため、個別の技術的なご質問にはお答えしていません。お使いのOS・製品のベンダーや、保守契約先にご相談ください。

Copyright 2026 by Future Corporation. Public