Spectrum Technology

V1.0 2026/11/6

Linux 内部セキュリティ診断ツール

～脆弱性のない、安定した運用を支援します～



rkhunter



スペクトラム・テクノロジー株式会社

https://spectrum-tech.co.jp

sales1@spectrum-tech.co.jp

all rights reserved 2026 spectrum technology co.

Spectrum Technology

Linux　内部セキュリティ診断

1. 目的
   - 外部からの脆弱性診断では見つかりにくい、内部に潜んでいる、ウイルス、マルウエア、osの脆弱性、不備などを診断するツールについて紹介します。
   - 今回は、ubuntu22.04で検証しました。
2. 各ツール紹介
   ① ClamAV（ウイルス・マルウェアのパターンマッチング）
   - 既知のファイルの検出

   ② rkhunter / chkrootkit（ルートキットの検出）
   - システムの深い改ざん・潜伏チェック

   ③ Lynis（セキュリティ監査・脆弱性診断）
   - 設定ミスやセキュリティホール対策

利用にあたっては、各自でリスクを判断して、実施してください。インストール後のトラブルについては、弊社は責任を負いかねます。

サイバー攻撃対策としての「AIを活用した中小企業向け脆弱性診断・自動管理ツール」の販売中です。Ubuntuで動作します。是非利用ください。

all rights reserved 2026 spectrum technology co.

3.ClamAV

A) 概要

- Linuxでは、代表的なオープンソースのアンチウイルスソフトです。ウイルス、トロイの木馬、バックドアなどの既知のパターンファイル（定義ファイル）と一致するファイルをスキャンして検出します。
- https://docs.clamav.net/

B) インストール

- sudo apt install clamav clamav-daemon

C) 動作

- sudo freshclam
- sudo clamscan -r -i --remove=yes
- -l /var/log/clamav/fullscan.log　ログに結果を残す場合はこちらをつける
- 約数時間：フォルダなど、インストール内容による。

D) 結果

- 出力例

```
----------- SCAN SUMMARY -----------
Known viruses: 8654321
Engine version: 0.103.8
Scanned files: 1250
Infected files: 0
Data scanned: 45.20 MB
Data read: 38.10 MB (ratio 1.19:1)
Time: 8.421 sec (0 m 8 s)
```

all rights reserved 2026 spectrum technology co.

4. rootkit

A) 概要

- OSの奥深く（カーネルやシステムコマンドの改ざん、隠しプロセスなど）に潜伏する「ルートキット」を検知するためのツールです。通常のアンチウイルスでは見つかりにくいシステムファイルの不正書き換えを発見できます
- https://www.rkhunter.dev/

B) インストール

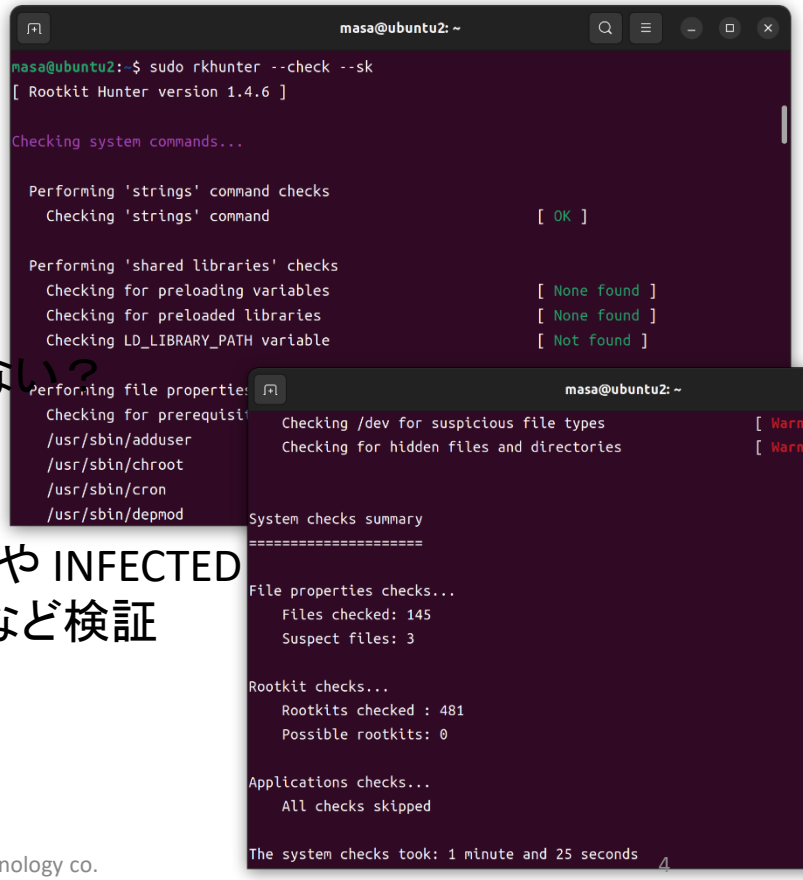
- sudo apt-get install -y chkrootkit rkhunter

C) 動作

- sudo chkrootkit
- sudo rkhunter --check --sk
- sudo rkhunter --update　更新がうまくいかない？
- 約20分位

D) 結果

- Suspect, possible rootkitの数と、WARNING や INFECTED
- 詳細は、ログでチェックし、該当のファイルなど検証



all rights reserved 2026 spectrum technology co.

5. lynis

A) 概要

- マルウェアそのものを駆除するというよりは、OS自体の設定不備、不要なサービスの稼働、パーミッションの甘さなどを総合的に診断し、侵入リスクを減らすための監査ツールです
- https://cisofy.com/lynis/

B) インストール

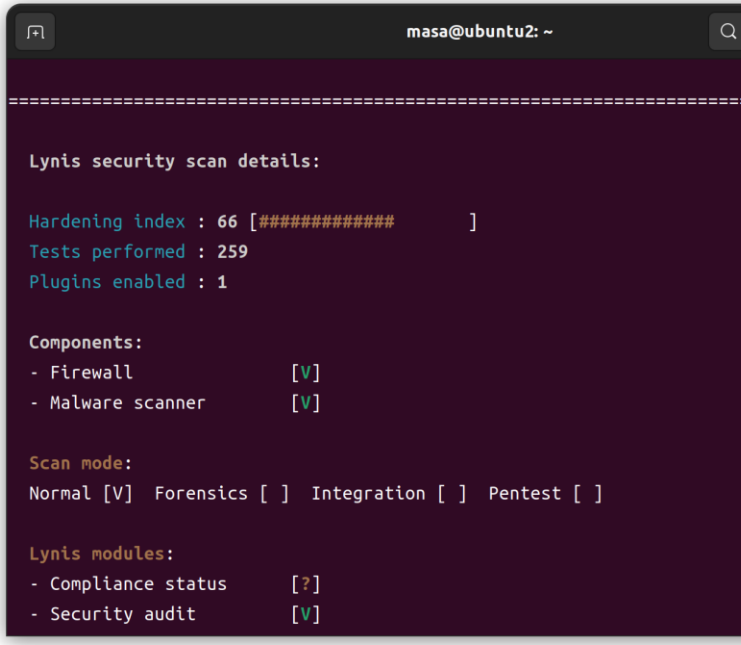
- sudo apt install lynis

C) 動作

- sudo lynis audit system
- 5分位

D) 結果

- warnig,suggestionが出ていなければok
- 総合点数；hardening indexは、66（65以上はok)



all rights reserved 2026 spectrum technology co.

6. その他

- 不審なプロセス・自動起動設定の確認
  - ps aux --sort=-%cpu | head -n 10
  - 大量にcpu消費してなければok
  - crontab -l
  - 不明の更新がないこと
- 不正な外部通信（C2サーバー通信）の特定
  - sudo ss -tulpn
  - 変なip addr,portなどがないことを確認、一杯でます
- ログの解析（不正アクセスの履歴）
  - sudo lastb -n 20 ログイン失敗

all rights reserved 2026 spectrum technology co.