WithSecure™ Elements EPP for Linux

2023年3月

ウィズセキュア株式会社

ご挨拶

平素は弊社製品をご愛顧いただき誠にありがとうございます。

また弊社Linux製品にご興味を持っていただき、重ねて御礼申し上げます。

弊社、ウィズセキュア株式会社では20数年以上前からLinux対応のセキュリティ製品に力を入れており、国内でも多くのお客様にてご利用いただいております。

Linux創始者のLinus Torvalds氏がフィンランドのヘルシンキ生まれで弊社の創業メンバーとも親しくされていたことも関係して、弊社ではLinux 対応製品の開発・提供を継続して行っております。

このたびはオンプレミスタイプからクラウドタイプへの製品ライン移行に伴いまして、本資料にてクラウド管理タイプの製品「WithSecure™ Elements EPP for Servers (以下 EPP Linux) 」をご案内いたします。

WITH secure

目次

- ご挨拶
- 国内でのLinuxの利用状況
- Linux のセキュリティ対策
- WithSecure の Linux 対応製品ラインナップの紹介
- EPP Linux と Linux Security64の比較表
- EPP Linuxの機能紹介
  - ✓ 基本機能
  - ✓ 動作環境
  - ✓ クローズド環境での利用
  - ✓ 自動アップデート
  - ✓ Elements Portalへの統合
  - ✓ 価格・ライセンス情報
  - ✓ 各種問い合わせ先
- LS64からEPP Linux へのマイグレーション
- Appendix: WithSecure™ Elements アーキテクチャ

WITH secure

国内でのLinuxの利用状況

- 日本においてもLinuxマーケットは、オープンソースソフトウェアへの需要の高まりにより年々拡大しています。特にLinuxベースのオペレーティングシステムを採用する企業や公共団体が増加しており、日本のビジネス市場においては、Linuxが重要な位置を占めています。
- 一部の企業ではLinuxを含むオープンソースソフトウェアを採用することで、ライセンス料の削減や自由度の高いカスタマイズなどの利点を享受しています。
- 日本国内の大手IT企業もLinuxを活用したソリューションを提供する等、Linuxの利用に積極的に取り組んでいます。
- 日本のLinuxマーケットは今後も拡大が見込まれており、特にIoT、ビッグデータ、AIなどの分野での需要の高まりにより、Linuxベースのソフトウェアやプラットフォームがますます重要になっていくことが予想されています。
- 金融・公共分野や大企業での基幹システムにおいてもLinuxの利用が増えており、弊社のLinux Securityもこの分野を中心に多数導入していただいております。

Linuxのセキュリテイ対策

- Linux は Windows などの他のオペレーティングシステムに比べて、マルウェアに感染する可能性が低いとされていますが、感染する可能性はゼロではありません。
- インターネットに接続されたサーバー環境では、攻撃者がシステムに侵入し、悪意のあるプログラムを実行することもあります。
- Linux の利用ユーザーが増えるに連れて、攻撃者が Linux を標的とした攻撃を行うというような事例も増えています。
- Windows 環境でしか動作しないマルウエアは Linux 環境には感染しませんが、ファイルサーバ等の Linux システムを経由して Windows 環境への感染を拡げる危険があります。
- Linux 環境であってもウイルス対策ソフトウェアを導入されるケースが増えており、特に金融・公共分野では必須となってきております。例えば国際クレジット産業向けのデータセキュリティ基準である PCI-DSS においても Linux を含むすべてのオペレーティングシステムについてウイルス対策ソフトウェアの利用が要件化されております。

WithSecure の Linux 対応製品

WithSecure では以下の Linux 対応製品を提供しています。
本資料では主として WithSecure™ Elements EPP for Linux（略称：EPP Linux）をご紹介いたします。

- EPP Linux（クラウド型アンチウイルス製品）
- Linux Security 64（オンプレミス型アンチウイルス製品）
- Policy Manager（オンプレミス製品の集中管理ソフト）
- Atlant（ICAP 等で他製品と連携し、連携先へマルウェアスキャン機能を提供）
- Web サイトライセンス（公開サーバ上で Linux Security 64 を利用するためのライセンス）

EPP LinuxとLinux Security64の比較表

機能	機能の概要	EPP Linux	Linux Security 64
マルウェア・スパイウェア防御	パターンファイルによる既知のマルウェア、スパイウェア防御	●	●
セキュリティクラウド	WithSecure™ Security Cloud の利用による未知の脅威の検知	●	●
マニュアルスキャン	コマンドによるスキャンの実行	●	●
スケジュールスキャン	スケジュールによる定期スキャン	●	●
完全性検査	登録したファイルに対してファイルの改竄を検出	●	●
スタンドアロン対応	集中管理せずスタンドアロンでの運用		●
製品自体の自動更新	自動的に製品のバージョンアップやモジュールの自動更新	●	●
製品バージョンの固定化	自動バージョンアップせずバージョンを固定（特定バージョンのみ）		●
非インターネット環境	非インターネット環境での利用について（完全クローズド環境）		●
非インターネット環境	非インターネット環境での利用について（プロキシ経由）	●	●
EDR 連携	WithSecure™ Elements EDRとの連携	●	
集中管理	集中管理の方法	クラウドの管理ポータル	管理サーバ
集中管理端末	集中管理に必要な端末	標準ブラウザ	管理コンソール
集中管理（階層管理）	クラウドの管理ポータルにての階層での集中管理	●	

WITH secure

WithSecure™ Elements EPP for Linux の機能紹介

WITH secure

EPP Linux - 基本機能

- ウイルス・スパイウェア対策
  高性能スキャンエンジンにより、リアルタイム、マニュアル、スケジュールでのウイルス、スパイウェアスキャン機能。

- セキュリティクラウド
  　未知のファイルに対する評価を WithSecure™ Security Cloud のデータベースを利用して行う機能（ORSP）。
- 完全性検査による改ざん防止
  保護対象のファイルに対して、ハッシュ値等を取得しリアルタイムで変更を監視、ブロックの設定を行うことでシステムファイルを改ざんの脅威から保護。
- 集中管理
  Elements Security Center から複数台のサーバを一括管理が可能。
  （Windows混在環境も一括管理可能。）
- 自動更新
  ウイルス定義ファイルやマスターエージェントも自動で最新のものに更新。

EPP Linux - 動作環境

ハードウェアスペック
- CPU: x86-64 compatible CPU
- メモリー: 2GB
- HDD: 3GB以上（20GB以上を推奨）

対応プラットフォーム
- AlmaLinux 8、AlmaLinux 9
- Amazon Linux 2
- CentOS 7 (7.3 or newer)、CentOS Stream 8
- Debian 10、Debian 11
- Oracle Linux 7 (7.3 or newer)、Oracle Linux 8
- RHEL 7 (7.3 or newer)、RHEL 8、RHEL 9
- SUSE Linux Enterprise Server 12 (Service Pack 1 or newer)
- SUSE Linux Enterprise Server 15 (Service Pack 1 or newer)
- Ubuntu 18.04、Ubuntu 20.04、Ubuntu 22.04
- MIRACLE LINUX 8、MIRACLE LINUX 9（特定パートナー経由でのサポート）

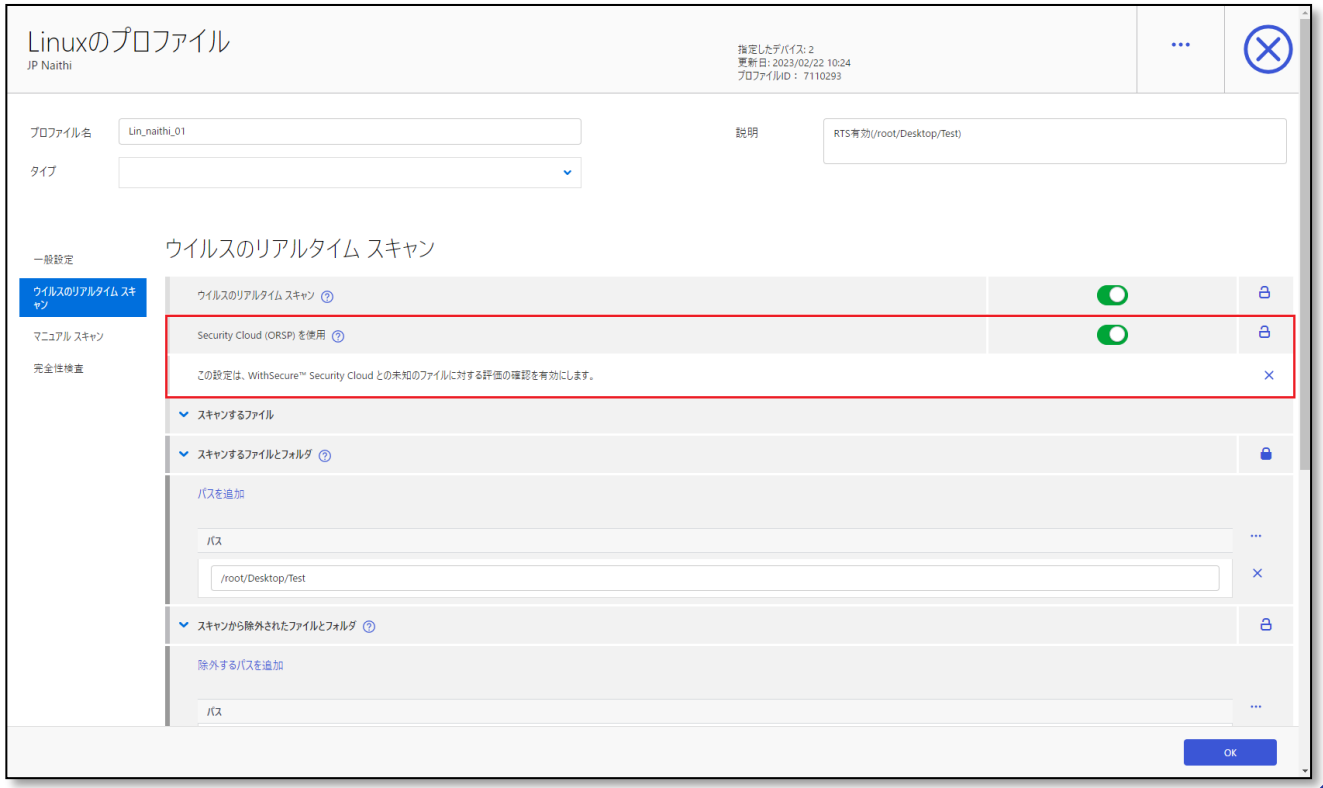
※　上記は2023年3月1日現在。最新の動作環境はリリースノートを参照して下さい。

※　OSのサポート終了後は、そのOS上でのご利用はサポート外の扱いとなります。

W / T H
secure

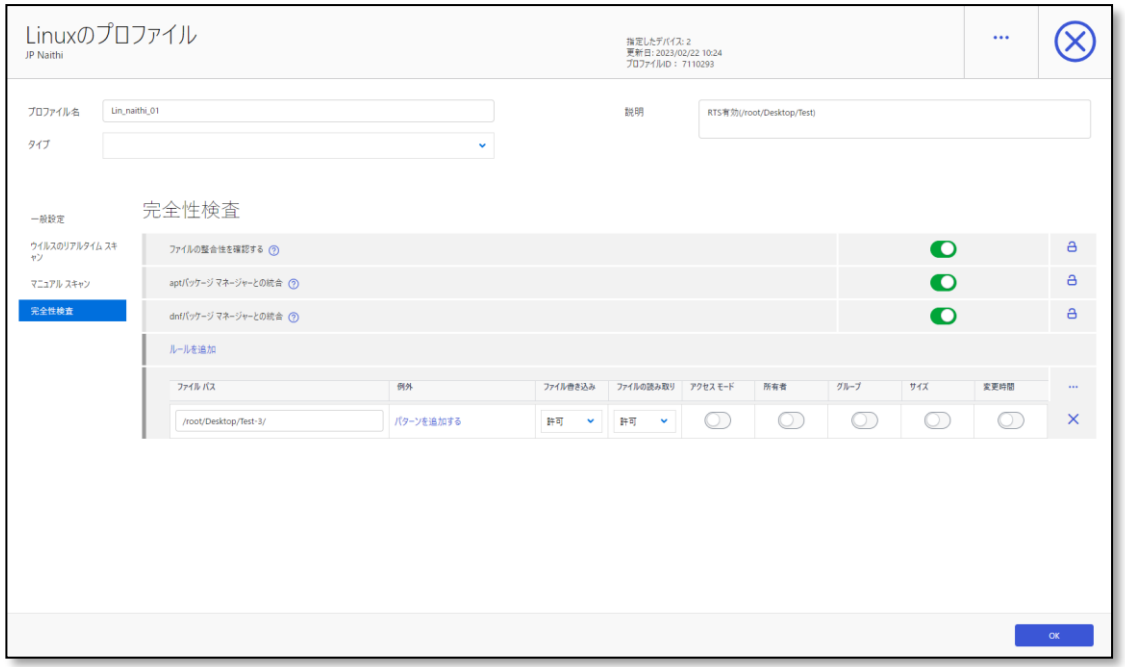
EPP Linux - セキュリティクラウド

- クラウドベースのオブジェクト評価サービスプラットフォーム（ORSP）は、未知のファイルに対する評価をWithSecure™ Security Cloud のデータベースを利用して行う機能です。
- リアルタイムスキャンの設定ではデフォルト有効になっています。



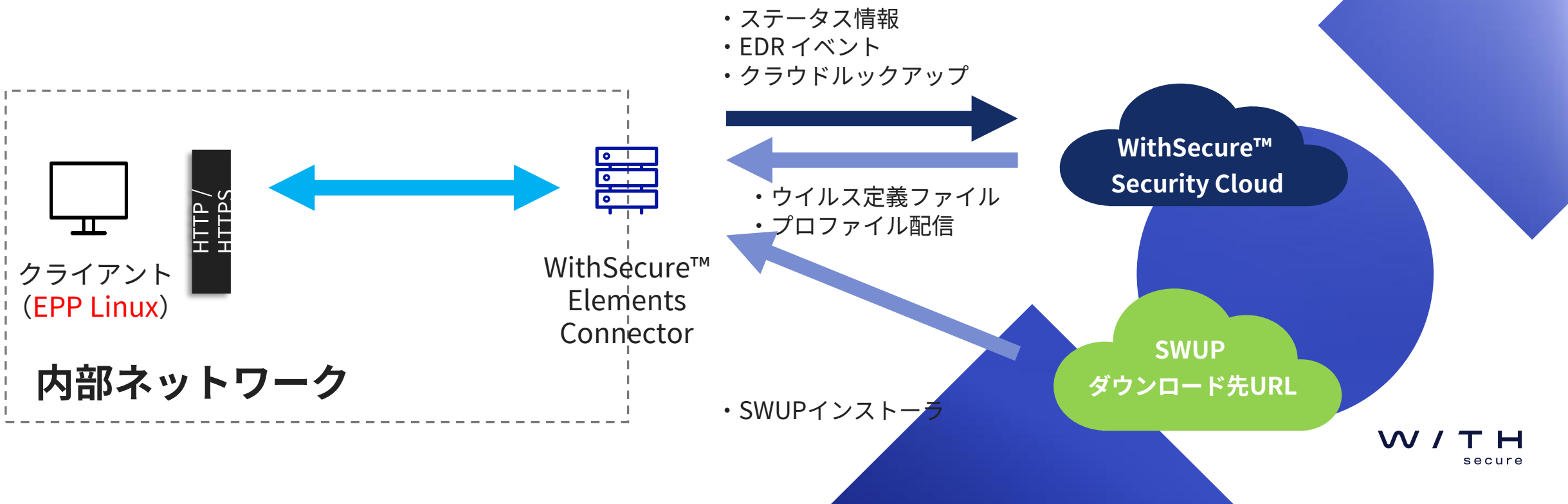
EPP Linux - 完全性検査

- 「完全性検査」はシステムを不正な変更から保護します。この機能は既知の構成 (正常で問題がないシステムの状態) に基づいて、システムの安全性を確認します。保護したいファイルのベースラインを作成して、すべてのユーザに対してファイルの変更を阻止することができます。また、新しいファイルが対象ディレクトリ内に作成された場合は、ベースラインを更新しない限り完全性検査の対象とはなりません。
- デフォルトプロファイルでは、完全性検査の設定自体は有効になってますが、対象のファイルパスが設定されておらず、ベースラインが作成されていないので機能しません。ベースラインを設定してからご利用下さい。



EPP Linux - クローズド環境での利用

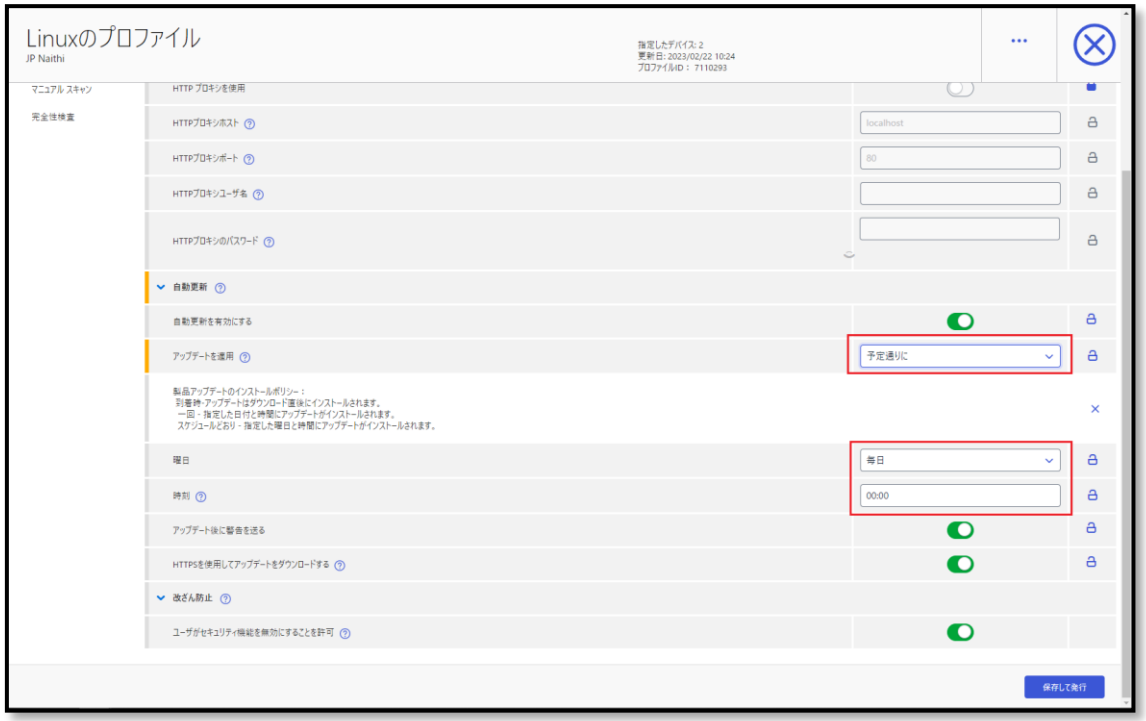
- EPP Linux は専用プロキシ製品（Elements Connector：無償）を使用してクローズド環境で利用することがでいます。Elements Connector だけをインターネットへ接続すれば、EPP Linux 搭載サーバを直接インターネットに接続できないクローズド環境内でもご利用可能です。
- 完全なクローズド環境でのご利用が必要な場合には、LinuxSecurity64とPolicyManager（集中管理サーバー）をご利用下さい。（2027年末のサポート終了時点までご利用可能です）



EPP Linux - 自動アップデート

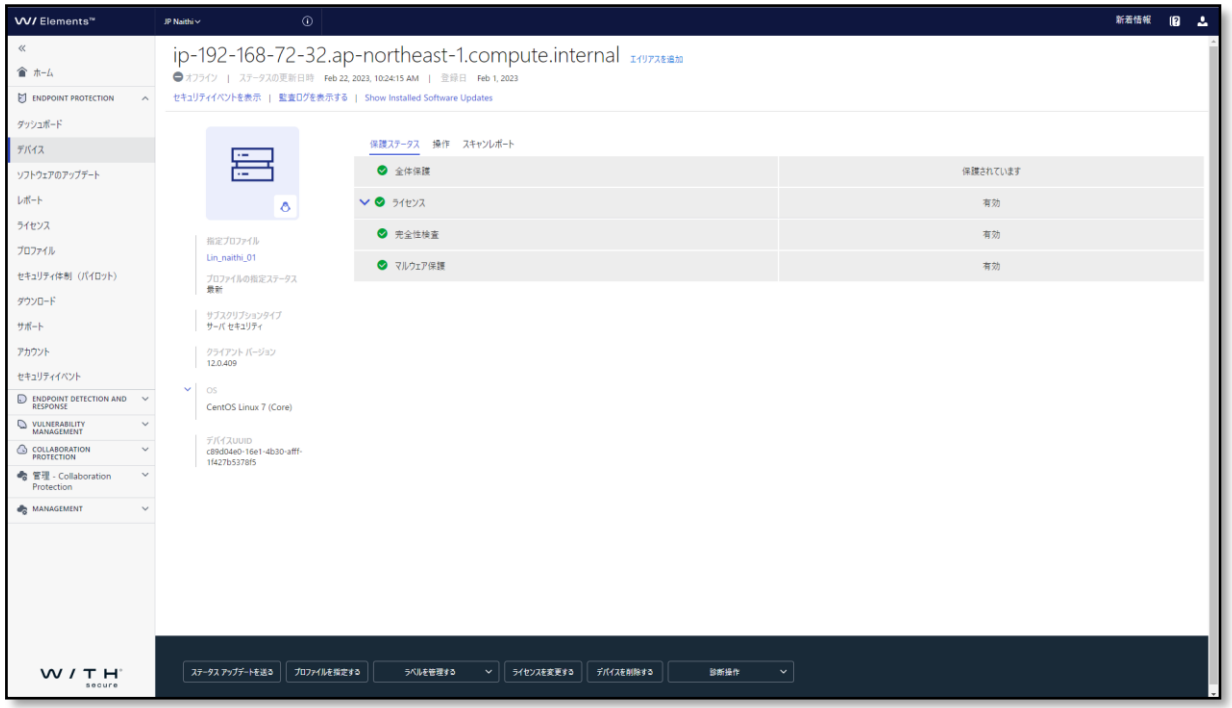
- EPP Linux は製品自体も自動で更新されますので、管理者によるバージョンアップやパッチ適用を手動で行う必要はありません。
- 製品自体の更新はプロファイルから適用のタイミングを設定することが可能です。設定では「受信時に」、「1回」、「予定通りに」を選択でき、例えば下記のように「予定通りに」を選択すると曜日及び時間を指定できます。

※パターンファイル更新/適用のタイミングについてはダウンロード後即時適用となり、本設定で変更することはできません。



EPP Linux – Elements ポータルへの統合

- EPP Linux は管理サーバーを必要とせずに Elements ポータルから管理することができます。また、他の Elements 製品（EDR、VULNERABILITーY MANAGEMENT、COLLABORATION PROTECTION）についても同一ポータル上から一元管理することが可能です。
- Elements ポータルのデバイスタブから製品のステータスを確認することができます。
- 製品の設定は、Elements ポータル上のプロファイル、及びコマンドラインで変更することが可能です。



EPP Linux - 価格・ライセンス情報

製 品	購入型番	標準単価 (税別)
Elements EPP for Linux 新規1年間 (1-24)	FCXOSN1NVXAQQ	49,090 円
Elements EPP for Linux 新規1年間 (25-99)	FCXOSN1NVXBQQ	38,180円
Elements EPP for Linux 新規1年間(100-499)	FCXOSN1NVXCQQ	27,270円
Elements EPP for Linux 新規1年間 (500-999)	FCXOSN1NVXDQQ	16,360円

- 新規・更新ともに同単価となります
- 教育機関のユーザー様は 50 %、公共機のユーザー様は 15 % のディスカウントが適用されます。
- 2年～5年までの複数年一括でライセンス購入いただくと、単年毎の購入よりもディスカウントされての提供となります。

WITH secure

EPP Linux - 各種問い合わせ先

- Elements Security Center 管理者ガイド
  https://www.withsecure.com/content/dam/with-secure/ja/support-news/support-resource/windows/WithSecure™%20Elements%20Security%20CenterGuide.pdf
- EPP Linuxオンラインマニュアル
  https://help.f-secure.com/product.html#business/linux-protection/latest/ja/concept_BA55FDB13ABA44A8B16E9421713
  latest-ja
- サポートリクエストフォーム（下記リンク先フォームよりサポート受付）
  https://www.withsecure.com/jp-ja/support/contact-support/email-support?m=support-request-thank-you
- 営業窓口
  japan@withsecure.com

LS64からEPP Linuxへのマイグレーション

WITH secure

LS64からEPP Linuxへのマイグレーション

- LinuxSecurity64からEPP Linuxへのマイグレーションについては、製品のアンインストール/インストールにて入れ替えを行ってください。（現時点でマイグレーションツールのようなものはございません。製品のアンインストール/インストール手順については、下記URLをご参照下さい。）

LinuxSecuity64のアンインストール

https://help.f-secure.com/product.html#business/linux-security-64/latest/ja/task_2A64F1654288495483B72115B60245EE-latest-ja

Linux Protectonのインストール

https://help.f-secure.com/product.html#business/linux-protection/latest/ja/task_7C893CC525EF4BA5B7B4477FDE23E40F-latest-ja

Appendix

WithSecure™ Elements アーキテクチャ

WithSecure™ Elements

WithSecure™ Elementsは統一されたエージェントと管理ポータルにより、EPP, EDR, 脆弱性管理、M365クラウドプロテクションを統合するアーキテクチャです。

マルチプラットフォームの対応のEPP(Endpoint Protection)、EDR(Endpoint Detection and Response)、VM(Vulnerability Management : 脆弱性管理)が同一のエージェントにて提供され、統合された管理ポータル(セキュリティセンタ)にて管理可能です。

ウィズセキュア クラウドサービス全体図

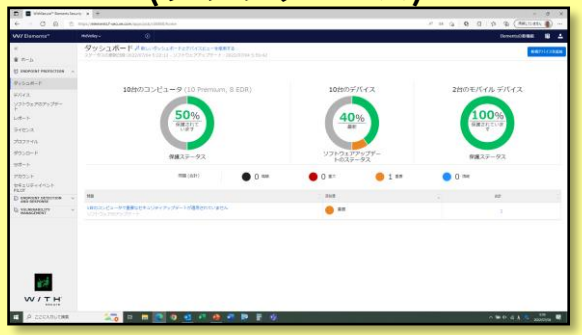
専用管理サーバー導入不要

どこからでも
アクセス

管理者

クラウド

Elements Security Center
(ブラウザベース)



自動更新(OSによって、機能が異なります)
パターンファイル、プロファイル、ソフトウェアバージョンアップ、セキュリティパッチ

- Windows
- macOS
- Android
- iOS

- Windows Server
- Linux

社内LAN

- Windows
- macOS
- Android
- iOS

支社/海外

マルチプラットフォーム対応

多拠点も一元管理

WITH secure


WITH
secure