第124回スクエアfreeセミナー

ニューノーマルなLinuxサーバ・パッチ管理

Linuxサーバの脆弱性対応はライブパッチの時代へ
KernelCareは運用自動化をサポートします

KernelCare

***1800*社以上で採用、*50*万台以上のサーバが使用**

リブート無しでカーネルパッチを適用

CentOSサポートも継続

株式会社*OPEN*スクエア

その悩み、KernelCareで解決

“サーバの再起動無しで、カーネルの脆弱性パッチを適用したい”を実現

1 ダウンタイムを大幅削減します

パフォーマンスへの影響やダウンタイムなしに、稼動中の（またはステージング）サーバーにパッチを適用

ユーザに対するサービス提供停止が無くなります

パッチ適用によるアプリケーションの停止が不要
ユーザに継続してサービスを提供することでユーザ満足度を向上

2 重要なパッチの見逃しは無くなります

迅速に最新のセキュリティパッチ情報を発見、専用のパッチを作成
エージェントが4時間ごとに新しいパッチをチェック

セキュリティ問題を回避します

Linuxカーネルには、常に全てのセキュリティ・パッチが適用されるため既知の脆弱性は無し

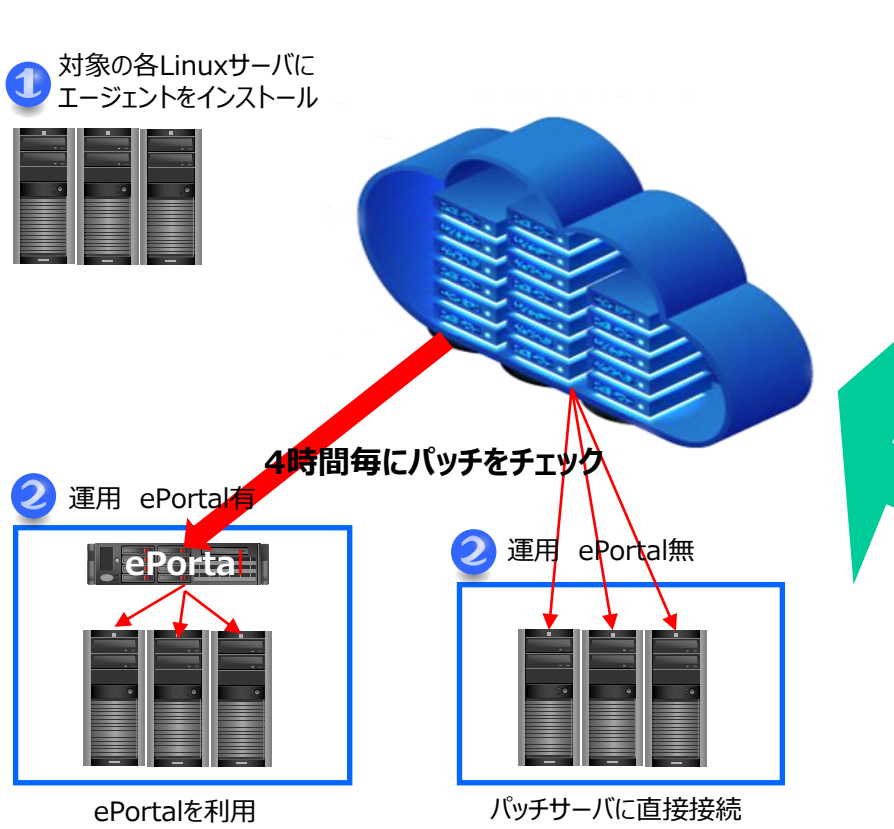
3 簡単な操作でリブート無しにパッチを適用

インストールに数分、アップデートにナノ秒、ロールバック機能付きで全ての作業がリブートなしで完結

サーバの運用コストを削減できます

自動的なパッチ適用により、運用チームを深夜、週末に現地で実施するメンテナンス作業から解放

KernelCareの動作



Up Load

Watch

KernelCare

◇ステップ1　脆弱性情報の監視
KernelCareセキュリティチームが常時、全ての Linux 脆弱性リストを監視。

◇ステップ2　パッチの作成
サポート対象のカーネルに影響する脆弱性を感知すると、直ちに脆弱性パッチ（KernelCareパッチ）を作成。

◇ステップ3　パッチのアップロード
KernelCareパッチは、バイナリ形式でコンパイルされ、クラウド上のKernelCareパッチサーバにアップロード。

KernelCareライブパッチの仕組み

カーネルメモリを割当て、そこに新しく安全なコードをロードします。

「安全」な状態にある全てのプロセスを一時的にフリーズします。

オリジナルの機能を変更して新しい安全なコードが実行されるようにします。

フリーズされた全てのプロセスを解除して、処理を再開します。

ありがとうございました。

ニューノーマル時代ではサイバー攻撃に対する更なるセキュリティ対策が求められます。
KernelCareでLinuxカーネルのセキュリティ・パッチ適用時のサーバ・リブートが不要になります。これにより、リモートワークでのパッチの適用、取消が可能になり、脆弱性対策を先延ばしにする必要がなくなります。
KernelCareの評価版も御用意しておりますので、評価ご希望の方は当社までご連絡ください。

OPENスクエア社はICTを利用して働き方改革を支援して参ります。

＜お問い合せ先＞

株式会社OPENスクエア

営業担当

E-Mail： sales_os@opensquare.co.jp
TEL： 03-6413-1840

資料をご覧頂き、ありがとうございました。

製品紹介URL：https://www.gdep-sol.co.jp/products/cloud/kernelcare.html

製品日本語マニュアル：https://docs.kernelcare.com/jp/installation/

END