KernelCare

IoTの脆弱性対策って難しそう…

実はカンタン

KernelCareのススメ

GDEPソリューションズ株式会社

営業・マーケティング本部　川口明男

企業情報

GDEPソリューションズ株式会社

[代表取締役]　長﨑 敦司　　[設立年月日]　2016年1月16日

[資本金]　6,000万円

[事業概要]　**GPUプラットフォーム事業**
クラウドインフラ事業

[主要株主]　プロメテック・ソフトウェア株式会社

株式会社構造計画研究所　株式会社サイコム

[所在地]　東京都文京区本郷三丁目34番3号

TEL：03-5802-7050　FAX：03-5842-4123

[URL]　http://www.gdep-sol.co.jp　e-mail：info@gdep-sol.co.jp

NVIDIA 社
Elite Partner 認定企業

3年連続
DGXシリーズ販売実績 No.1

設立背景
GPUコンピューティングの黎明期に、用途開拓・市場創出を狙い、
2010年に設立されたG-DEP（日本GPUコンピューティング組合）が
母体となり、更に事業を発展させるべく、2016年株式会社化

GPUコンピューティングのパイオニア

KernelCare

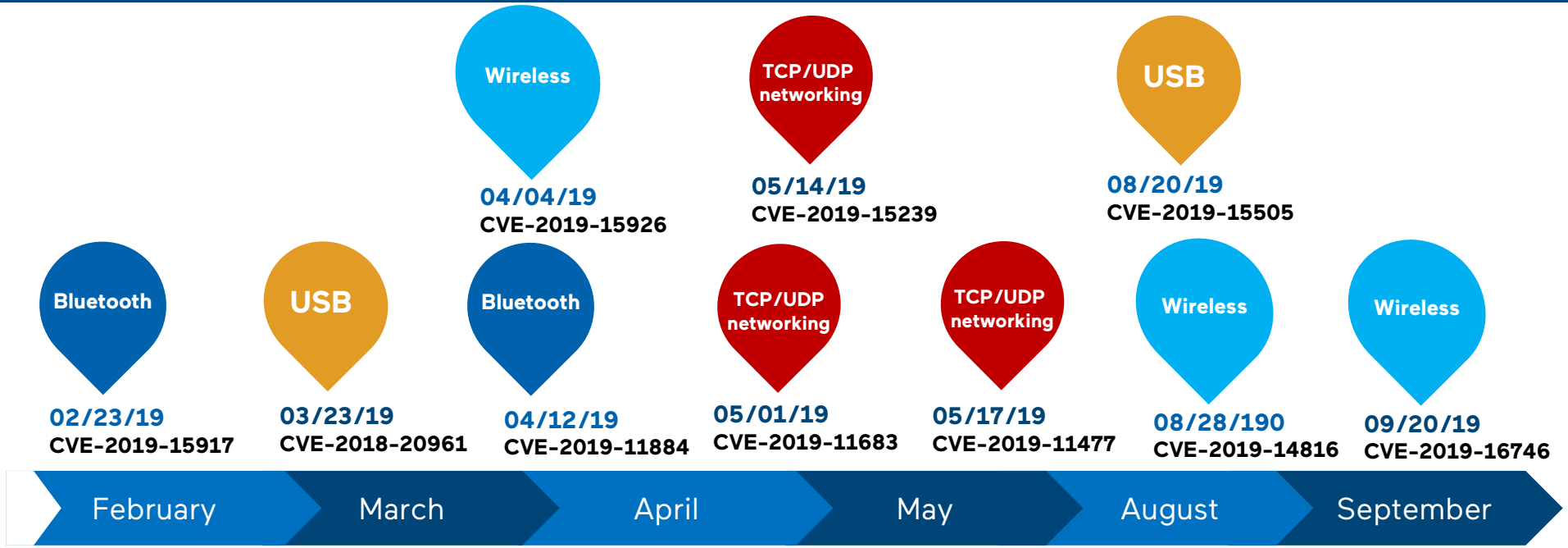
IoT のセキュリティ確保は、とても大変

調査対象企業の 61% が、IoT デバイスまで遡る必要があるセキュリティインシデントに遭遇

** "IoT Cybersecurity Readiness Report" by Trustwave and Osterman Research, 2018*

急増！　IoT に影響する CVE

KernelCare

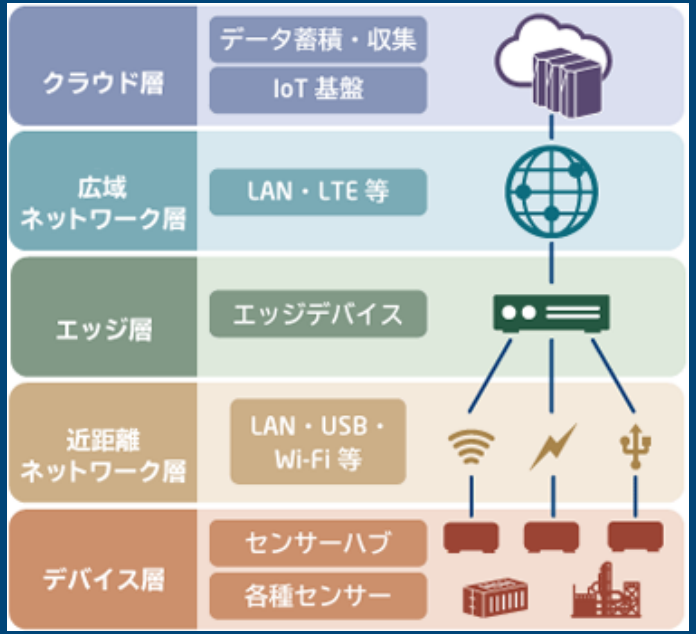


様々な出入口・経路でリスクにさらされている

KernelCare

IoT は常にリスクにさらされている

エッジ・デバイス層からエンタープライズ層まで
様々なモノがインターネットに接続されている



絶対的に安全性が必要なもの？

システムのコアである Linux カーネル

Linuxカーネル？

IoT デバイス OS の多くは

Embedded Linux

（組込みLinux）

CPUは ARM

IoT → IoST

Linux カーネルを**最新状態**に
することで、**脆弱性回避**は可能

でも…

考慮すべきことが山積

- パッチの見落としは避けたい
  タイムリーに適用したい

- IoT 機器をリブートできない
  → サービス停止期間ができるから

- どうやってパッチを配布するの

- 上位層に影響ないの

……

KernelCare

カーネルライブパッチ
KernelCare（カーネルケア）

60万台以上のLinux

2000社での利用実績

KernelCare

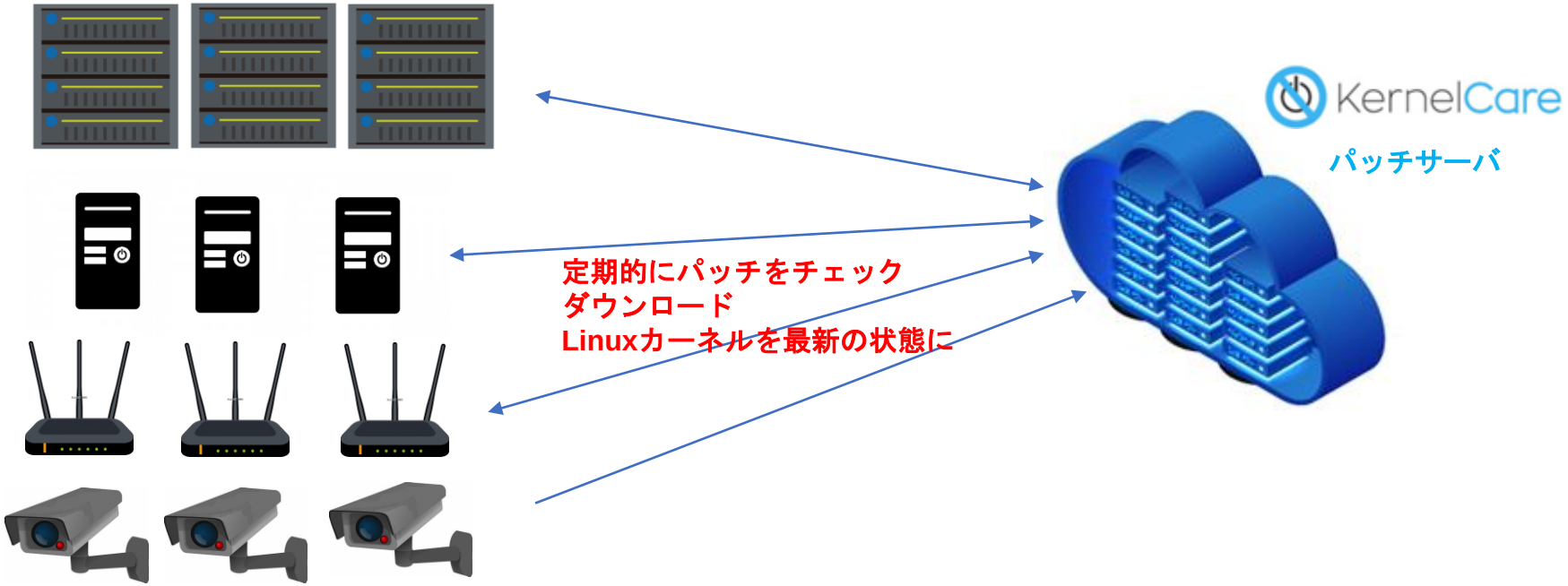
KernelCare は、IoT システムをセキュアに保つ

- Linux カーネルの脆弱性情報を常に監視
- 脆弱性発見次第パッチを作成しリリース
- 多くのディストリビューションをサポート
- パッチを 自動で適用

しかもリブートは不要で、お手頃価格！

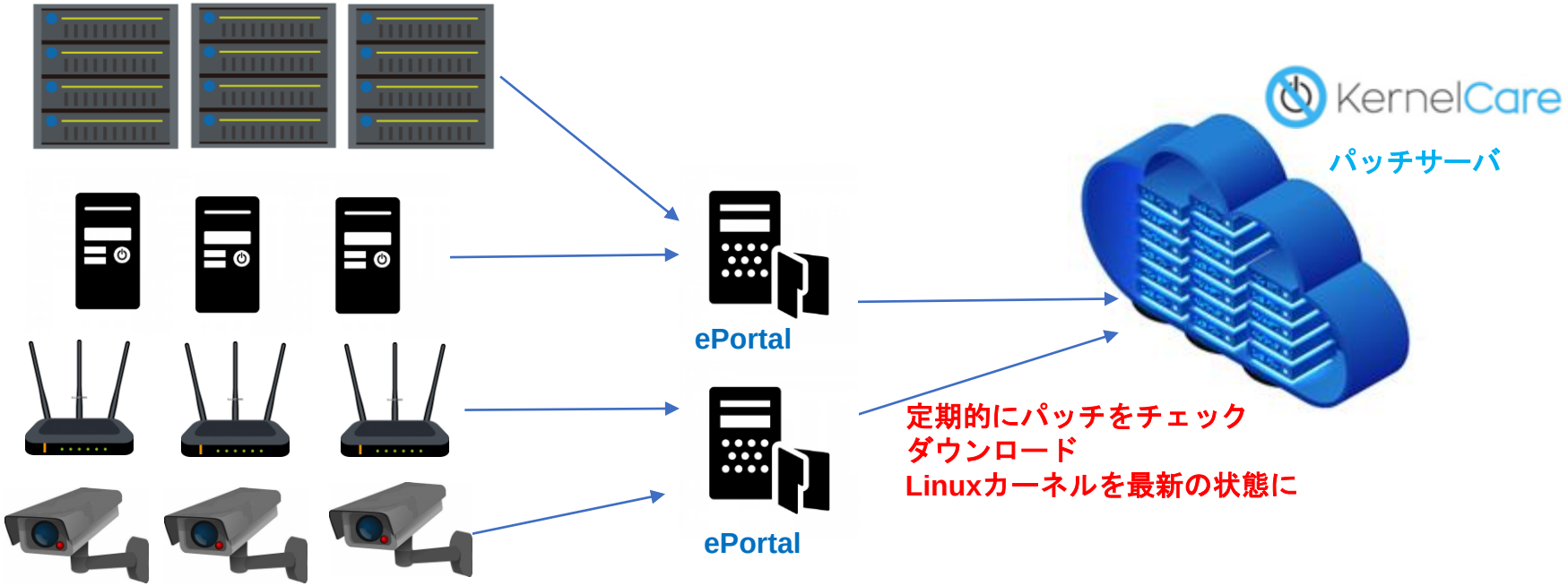
KernelCare の導入方法

各エッジ、デバイス、サーバ に KernelCare エージェント
クラウド上の KernelCare パッチサーバにアクセス



KernelCare の導入方法（企業内）

各エッジ、デバイス、サーバ に KernelCare エージェント
KernelCare パッチのレポジトリ ePortal を社内に構築



KernelCare

KernelCare価格情報

お手頃価格の保険のようなものです

月額 600円～ （台数によります）

OEMは別途、お問合せ下さい。

※上記は１Linuxマシン当たりの価格です。年間サブスクリプションとなっております。

※ 日本語によるテクニカルサポート（E-mail）が含まれております。

※為替変動や経済・社会情勢、その他により、上記価格は変更される場合があります。

KernelCare

もっとセキュアに！ KernelCare+

(カーネルケアプラス)

カーネルの脆弱性パッチに加えて、

glibc、OpenSSLのパッチも自動適用！

もちろんリブートも不要

KernelCare からの有償アップグレードも可能

KernelCare

KernelCare＋ 価格情報

KernelCare からの
アップグレードも可能

月額 1,200円～ （台数によります）

OEMは別途、お問合せ下さい。

※上記は１Linuxマシン当たりの価格です。年間サブスクリプションとなっております。

※ 日本語によるテクニカルサポート（E-mail）が含まれております。

※為替変動や経済・社会情勢、その他により、上記価格は変更される場合があります。

耳寄りな話

Project LenixからAlmaLinuxが誕生！

CentOS に代わるOSの開発をコミュニティが計画

コード名 Project Lenix

CloudLinux社（KernelCare開発元）は、Project Lenixを

コミットし、2021年第1四半期に AlmaLinux という

名称で、ディストリビューションを発表予定

KernelCare

THANK YOU!

QUESTIONS?

ご購入、その他ご相談は

株式会社 OPENスクエア

参考スライド

KernelCare

IoTへのサイバー攻撃（ほんの一部）

2016: ホスティングプロバイダーOVHへの攻撃は、約150,000台のデバイスを参加させたボットネットを使用して、被害者のサーバに1秒あたり1テラバイトのデータを送信

2017: **犯罪グループはカジノからデータを盗むために水槽をハッキングしました**

2018: 何十億もの接続デバイスを脅かす「Bluetoothの脆弱性」が出現したハッカーがワイヤレス攻撃を開始してIoTデバイスを完全に制御できるようになる可能性が示唆

2018: ハッカーはフォーラムでスクリプトを交換して、脆弱なIoTデバイスをインターネットでスキャンし、脆弱な資格情報をダンプして、最終的に本格的な DDoS 攻撃を開始

2019: IoTデバイスを攻撃する大規模な Mirai 型の攻撃

他システムとの統合

- 構成管理ツール

  Puppet、Ansible、Chefとの統合
- 脆弱性スキャナ

  Nessus、Qualys、Rapid 7との統合、レポート
- 脆弱性管理ツール

  Tenableとの統合

ライブパッチの KernelCare が唯一のソリューション

- 自動

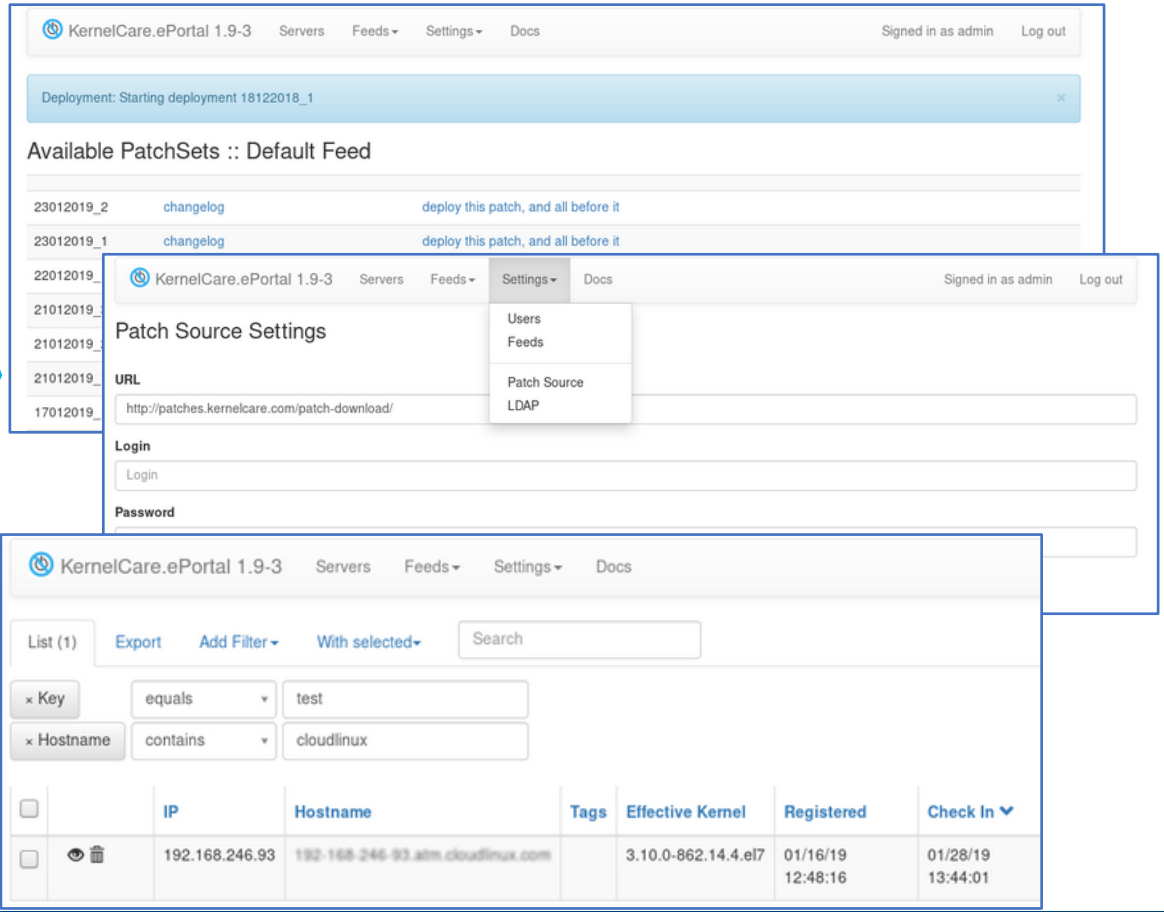
  パッチの適用漏れなし
- リブート不要

  サービスを止める必要なし
- 小さいパッチサイズ
- 多くのディストリビューションをサポート
- ARM をサポートする唯一のベンダー

ePortal：大規模システムに対応

パッチ配布制御のための大規模システム向けリポジトリツール

ファイアウォールの内側、インターネットに直接接続されていない Linux にパッチをフィード



KernelCare

IoT の脆弱性対策には KernelCare

カーネルの動作が不安定・不具合がある

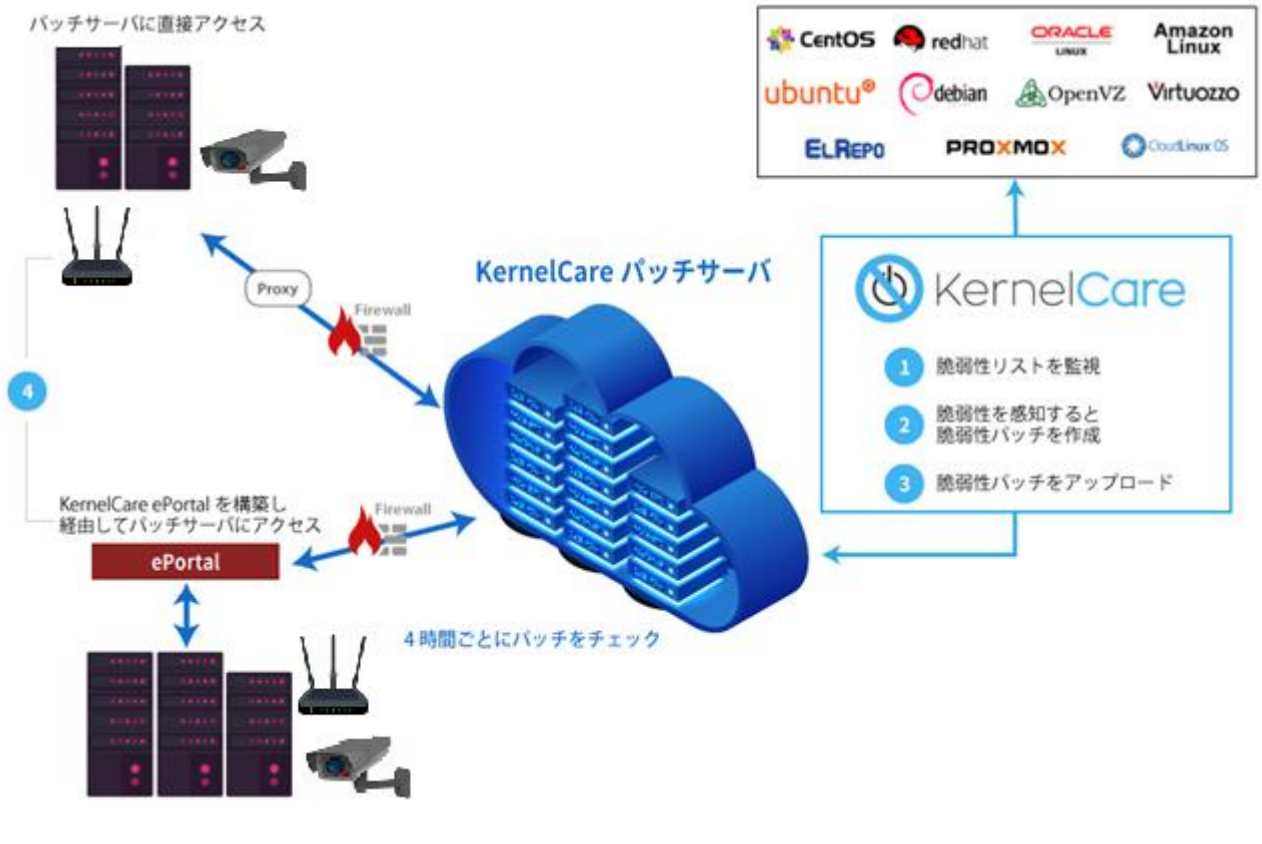
➔ システム全体に影響が及ぶ

➔ でも、今すぐには止められない

お手上げ状態を回避しましょう

運用も簡単。安価に導入。

KernelCare の全体の仕組み



◇ステップ1　KernelCareセキュリティチームが常時、Linux 脆弱性リストを監視

◇ステップ2　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　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

◇ステップ4　KernelCare稼働開始

4-1：各 Linux からパッチサーバにアクセスし、該当パッチを取得

4-2 ：ローカルに Web ベースの管理サイト ePortal を構築し、ePortal が、パッチサーバにアクセスして該当パッチを取得・適用
各 Linux は、ePortal にアクセスして、該当パッチを取得・適用

KernelCare

どうしてリブート不要なの？
どうやって動作中のカーネルにパッチ適用？

カーネルメモリを割り当て、そこに新しく安全なコードをロードします

「安全」な状態にあるすべてのプロセスを一時的にフリーズさせます

オリジナルの機能を変更して、新しくて、安全なコードへとジャンプし、古い（脆弱な）コードが実行されないようにします

すべてのプロセスの凍結を解除して再開します