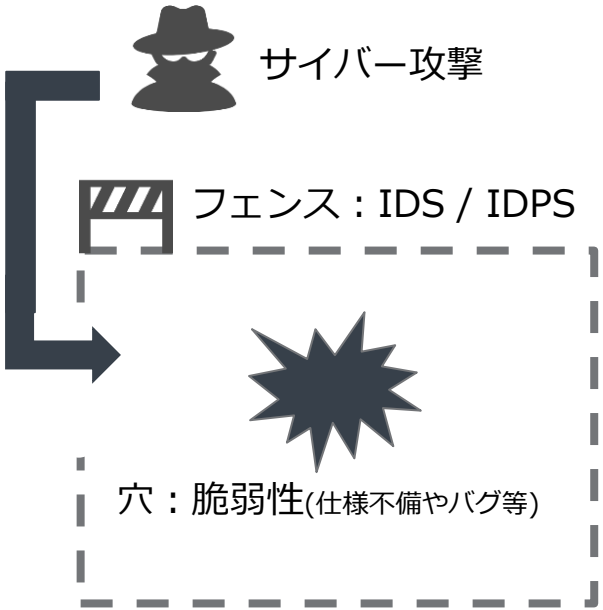
Linux を無停止でアップデート！
Linux ライブパッチサービス

cybertrust

ライブパッチとは？

セキュリティ対策の1丁目1番地はOSのアップデート

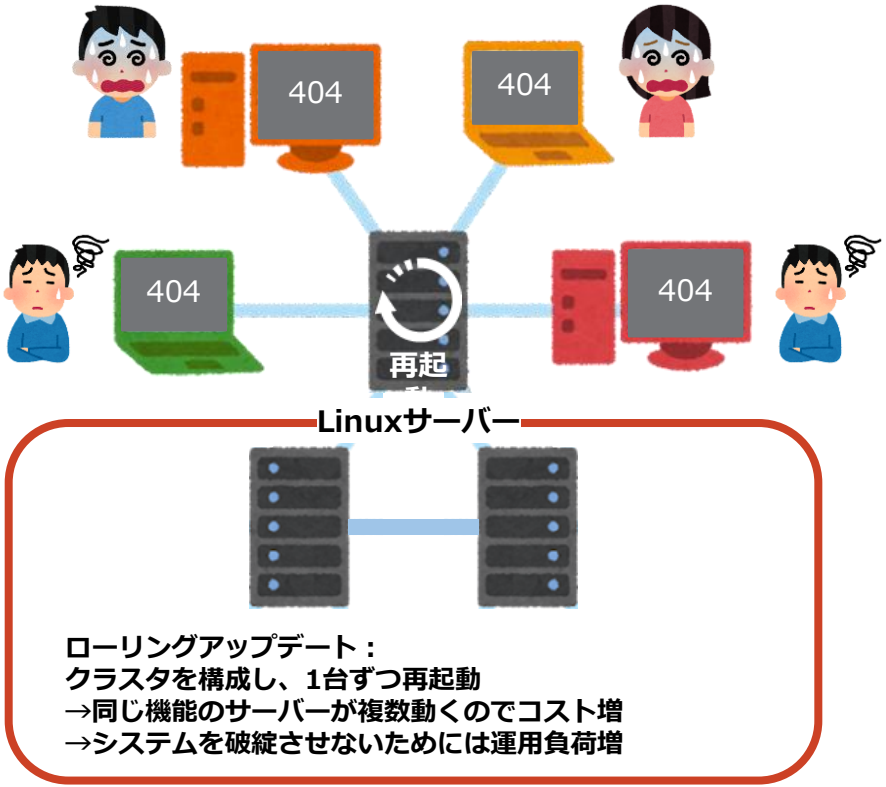


サイバー攻撃はOSの脆弱性を悪用して実行される

1. OSの脆弱性を利用して管理者権限を奪取
2. マルウェアなどをインストール
3. 機密情報などの窃盗、ネットワーク経由で他のマシンへ被害を拡大(これにも脆弱性を悪用)

IDPSなどでネットワーク経由の侵入を防いでも
攻撃手法は日々進化しているため、根本となる
脆弱性を塞いでおくことが最も重要

OSアップデートは再起動を伴うため頻繁な実施が難しい

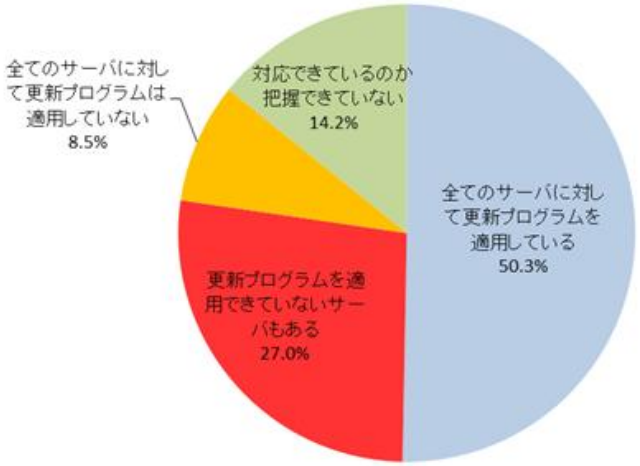


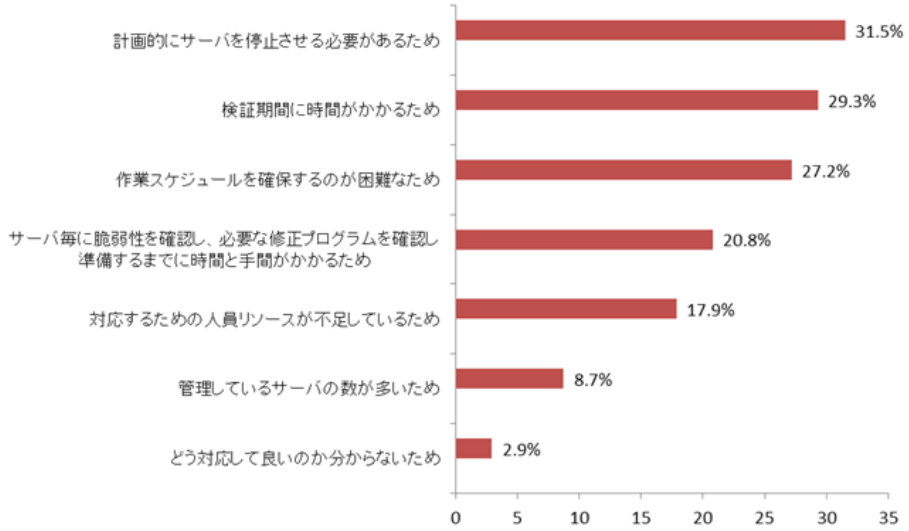
サーバーが再起動するとシステムが止まる

- OSの更新時には再起動が必要
  ※Kernelの更新時など
- 再起動はシステムダウン直結するため
  システム利用者全員に影響
  (サイト閲覧、Web会議、決済処理 …)
- クラスタ構成など回避方法もあるが
  完全無停止を目指すと運用の複雑化や
  コスト増など負担が大きい

OS再起動を伴うアップデートで膨大なコストが発生

- 企業における**脆弱性対応は半数が不完全**。主な理由は「**時間がかかる**」
- **8割以上**の企業がアップデート適用までに**1週間以上**必要
- 最も多い「**時間のかかる**」要因は「**サーバーの停止**」
- 事前調査や検証、スケジュール調整にも**多くのコストが必要**





企業におけるサーバ脆弱性対策に関する実態調査 | トレンドマイクロ

Linuxライブパッチで OSの再起動を回避する

cybertrust

KLP (kernel live patch)

KernelをOS再起動なしで修正可能に

脆弱性が発見された場合
迅速なセキュリティ修正が必要

セキュリティ

システム
稼働率

OS再起動はシステムが
止まるので極力避けたい

Linux 4.0以降のカーネルから利用可能

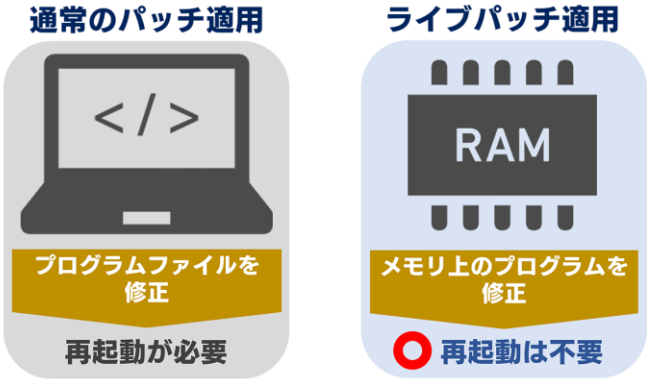
Linuxライブパッチサービス

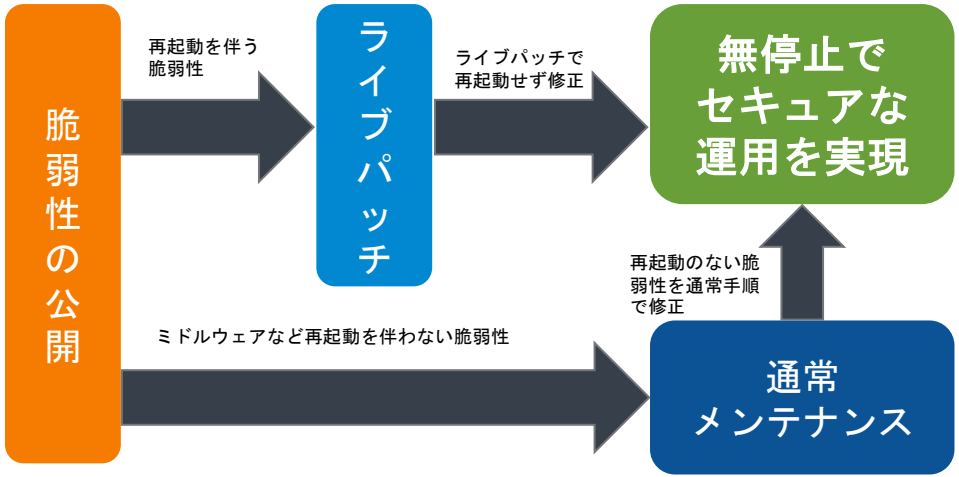
cybertrust

OS再起動を行わずに脆弱性を塞ぎ、セキュリティとコストのトレードオフを解決！

- 対応が必要な脆弱性を監視
- 必要なパッチを自動適用
- OS無停止の運用を実現
- 様々LinuxOSに対応
- 再起動不要で切り戻し可能
- 共有ライブラリにも対応

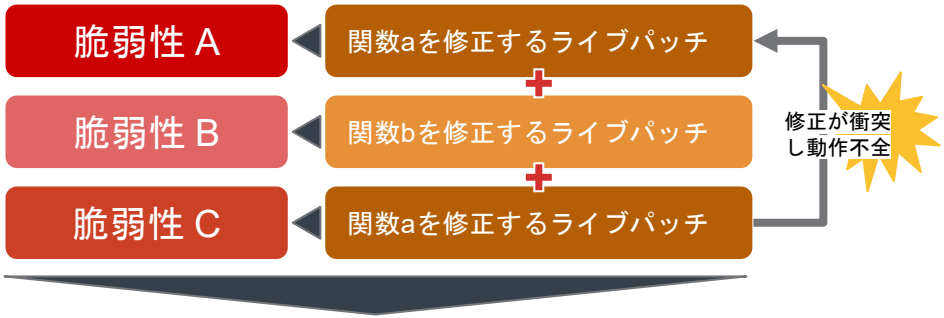
OSのコア機能はアップデート時再起動が必要





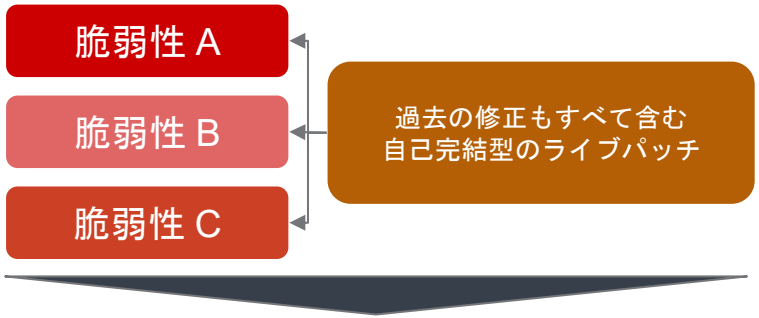
他社製品と比べ安定かつ長期間の無停止を実現

一般的なライブパッチ
(テンポラリパッチング方式)



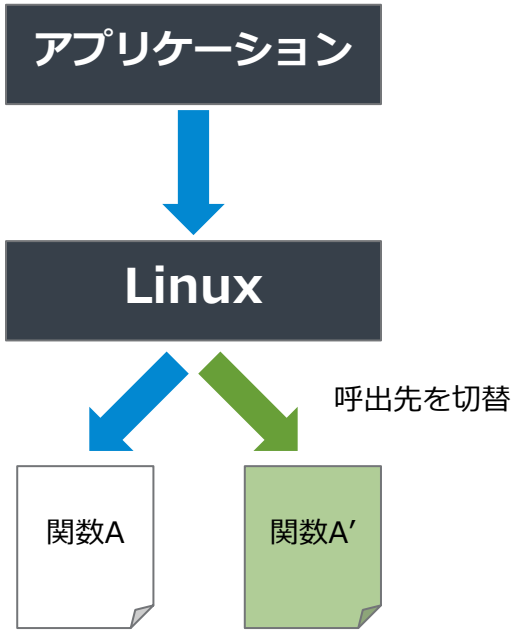
ライブパッチが蓄積されメモリ空間を
圧迫することで**定期的な再起動が必要**

Linux ライブパッチサービス
(パーシステントパッチング方式)



修正の衝突やメモリ圧迫が発生せず
長期的な無停止の運用を実現

再起動せずにOSアップデートする仕組み=ライブパッチ”



OSの再起動をせずに、関数レベルで修正されたプログラムに切替が可能
＝ライブパッチ

再起動が必要になるKernelアップデートを再起動無しで実施する仕組み

- Linuxライブパッチはプログラムを実行したまま修正を適用する仕組み
- 修正したプログラムをメモリに展開し呼出されたときに切替
- Kernelの脆弱性を修正しつつ、通常必要となる再起動をスキップできる。

KLPを実際に運用するための課題

cybertrust

1. ライブパッチは自分で用意する必要がある

KLPは**”ライブパッチを適用できるKernel機能”**なので適用するライブパッチは自分でビルドする必要がある
→技術要求が高く、稼働中のシステムに影響が出ないようにテストや検証も複雑になる。
→一部のディストリビューションではライブパッチを提供している(ただし仕様はまちまち)

2. メモリリソースを消費する

ライブパッチはメモリ上に展開されるため、**余分にリソースを消費する。**
→数個のライブパッチ適用であれば問題ないが、修正を積み重ねると動作に影響する
→2023年にCVE(脆弱性方法データベース)に登録されたKernel関係の脆弱性は既に200件以上

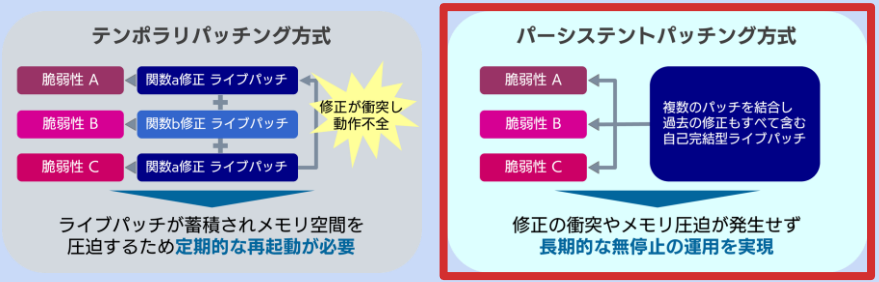
3. KLP単体はシステム運用全体をカバーする技術ではない

複数台のLinuxが存在する大規模環境ではライブパッチを**どう管理して適用するかが課題**になる
　例：マルチクラウド環境、システム内に複数種類/複数verのLinuxが混在

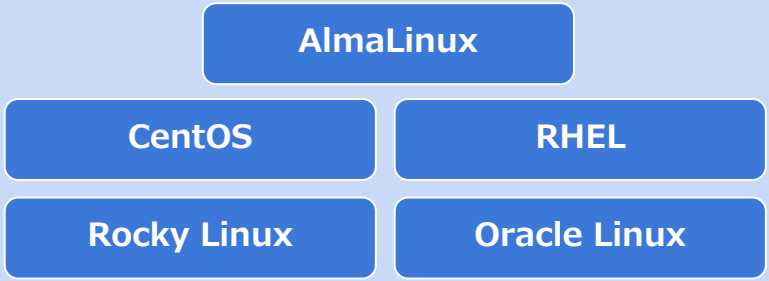
サイバートラストが提供する
ライブパッチサービスで課題を解消

サイバートラストのライブパッチサービス

最適化されたライブパッチセット



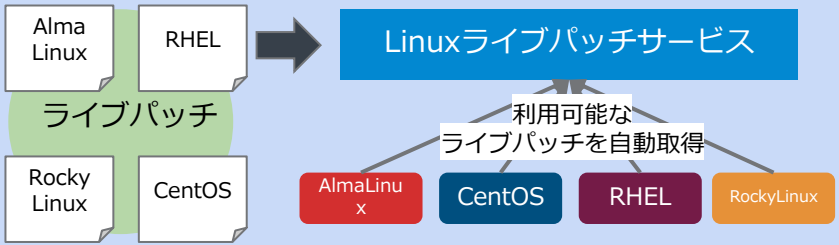
様々なLinuxで利用可能



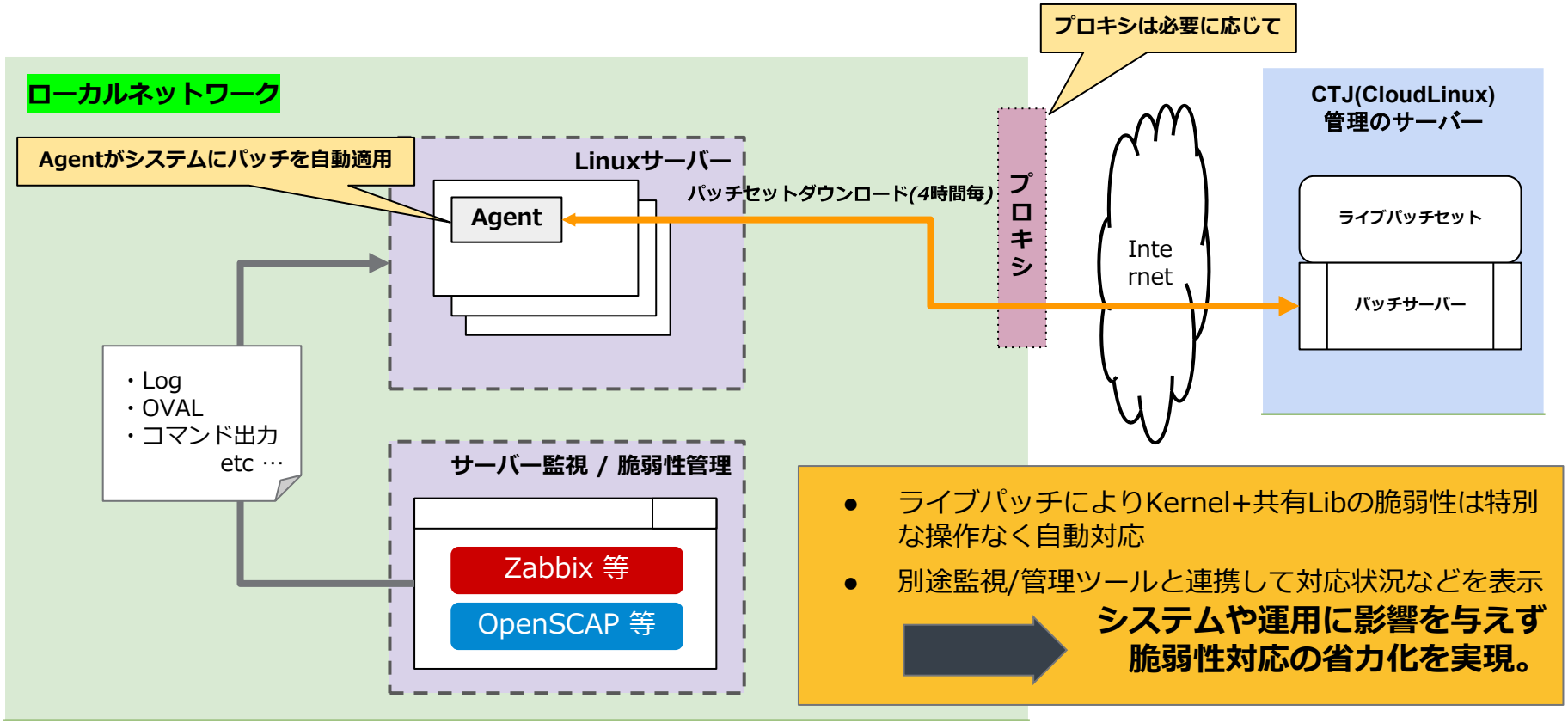
Kernel 以外も無停止アップデート

脆弱性が発見された際の影響が大きい
共有ライブパッチにもライブパッチを提供

パッチセットの管理が容易



ユースケース：脆弱性対応の省力化



- ライブパッチによりKernel+共有Libの脆弱性は特別な操作なく自動対応
- 別途監視/管理ツールと連携して対応状況などを表示

システムや運用に影響を与えず脆弱性対応の省力化を実現。

サービスメニュー

メニュー	金額価格	提供内容
Linux ライブパッチ サービス	**Open Price**	● Kernel, OpenSSL, glibc向けライブパッチ ● ライブパッチ管理用エージェント ● テクニカルサポート

他社ライブパッチサービスとの比較

比較項目	某社	Linux ライブパッチサービス
対応Linux Distro	RHEL	複数種類のOSに対応
Kernel	Yes	Yes
対象範囲	kernel	kernel + & critical userspace (glibc & openssl)
パッチセットの有効期限	6ヶ月	実質無制限
API対応の有無	No	Yes
ロールバック時の再起動	必要	不要

Linuxライブパッチサービス
クイックリファレンス

クイックリファレンス①

エージェントのインストール

```
# curl -s -L https://kernelcare.com/installer | bash
```

または

```
# wget -qq -O - https://kernelcare.com/installer | bash
```

ライセンスキーの登録

```
# kcarectl --register <KEY>
```

クイックリファレンス②

Kernelに対するライブパッチの手動適用

```
# kcarectl --update
```

パッチが適用されているかどうかを確認する

```
# kcarectl --info
```

適用されたパッチに関する詳細を確認する

```
# kcarectl --patch-info
```

すべてのパッチを削除

```
# kcarectl --unload
```

クイックリファレンス③

共有ライブラリ用ライブパッチの手動適用

```
# kcarectl --lib-update
```

ライブパッチが適用されているかどうかを確認する

```
# kcarectl --lib-info
```

適用されたライブパッチに関する詳細を確認する

```
# kcarectl --lib-patch-info
```

共有ライブパッチ用ライブパッチの削除

```
# kcarectl --lib-unload
```

クイックリファレンス④

cybertrust

共有ライブラリ用ライブパッチの自動適用

```
# libcare-cron init
```

共有ライブラリへのライブパッチ自動適用は事前に設定が必要です
※Kernelへのライブパッチはデフォルトで自動適用

上記コマンドががうまく動作しない場合は一度プロセスを手動再起動して設定してください

```
# systemctl stop libcare.socket          ※共有ライブラリ用ライブパッチのソケット停止
# systemctl stop libcare.service         ※共有ライブラリ用ライブパッチのサービス停止
# kcarectl --disable-libcare             ※ライブパッチのサービス無効化
# kcarectl --enable-libcare              ※ライブパッチのサービス再有効化
# libcare-cron init                      ※共有ライブラリ用ライブパッチの自動起動設定
# systemctl start libcare.socket         ※共有ライブラリ用ライブパッチのソケット起動
# systemctl start libcare.service        ※共有ライブラリ用ライブパッチのサービス起動
```

AlmaLinux 8.7 の場合の手順

クイックリファレンス⑤

ライブパッチが適用されたKernelバージョンの確認

```
# kcarectl --uname
```

ライセンスキーの登録解除

```
# kcarectl --unregister
```

関連情報

cybertrust

Linuxライブパッチサービス 製品ページ

Linuxライブパッチサービス セミナー情報(試用版有)

cybertrust

すべてのヒト、モノ、コトに 信頼を

留意事項

本資料に記載されている会社名、製品名、サービス名は、当社または各社、各団体の商標もしくは登録商標です。
その他本資料に記載されているイラスト・ロゴ・写真・動画・ソフトウェア等は、当社または第三者が有する知的財産権やその他の権利により守られております。
お客様は、当社が著作権を有するコンテンツについて、特に定めた場合を除き、複製、改変、頒布などをすることはできません。
本資料に記載されている情報は予告なしに変更されることがあります。また、時間の経過などにより記載内容が不正確となる場合がありますが、当社は、当該情報を更新する義務を負うものではありません。