



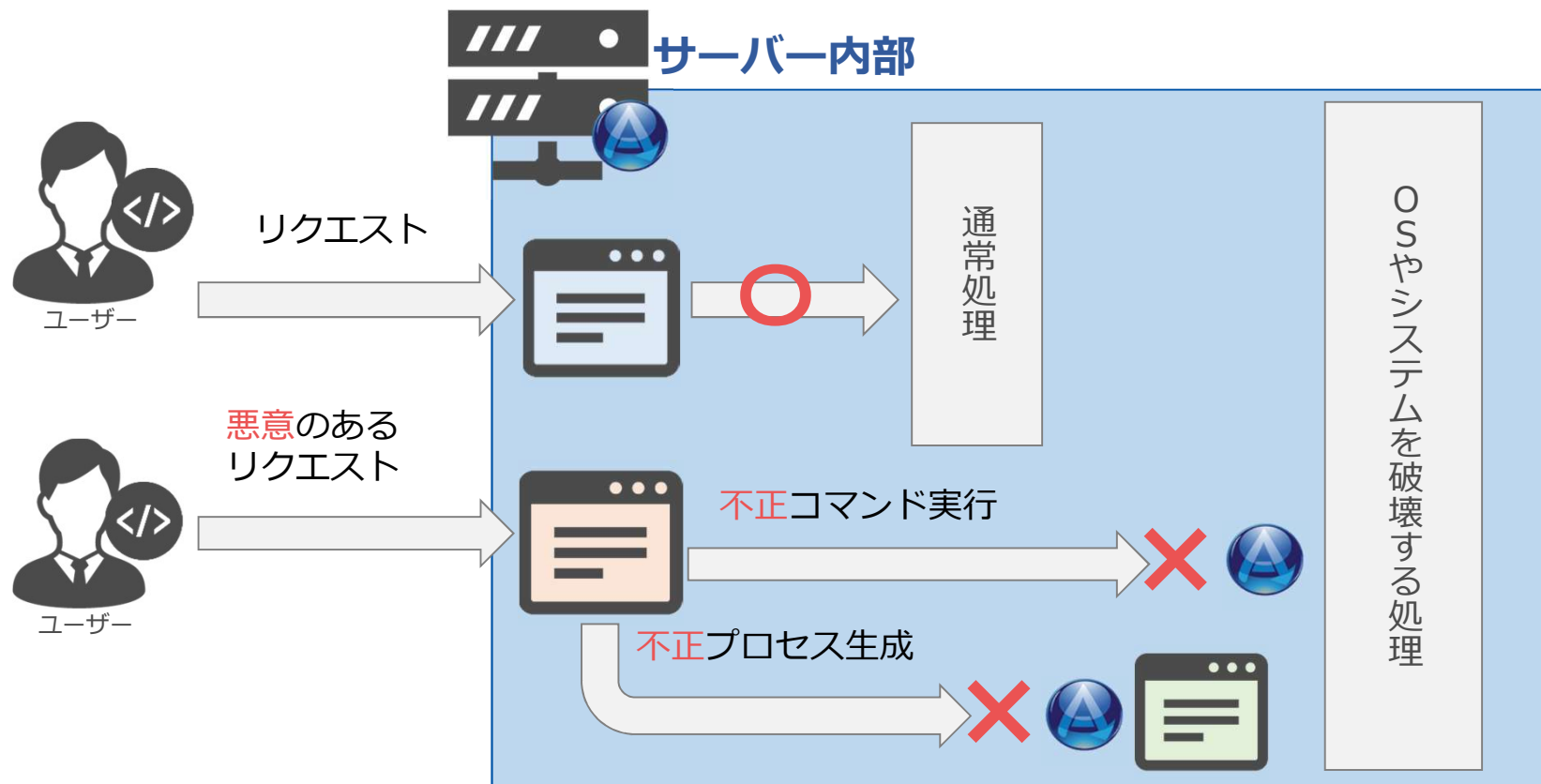
Blue Planet-works
Safety for the Connected World

Safety for the Connected World AppGuard Serverのご紹介

株式会社Blue Planet-works

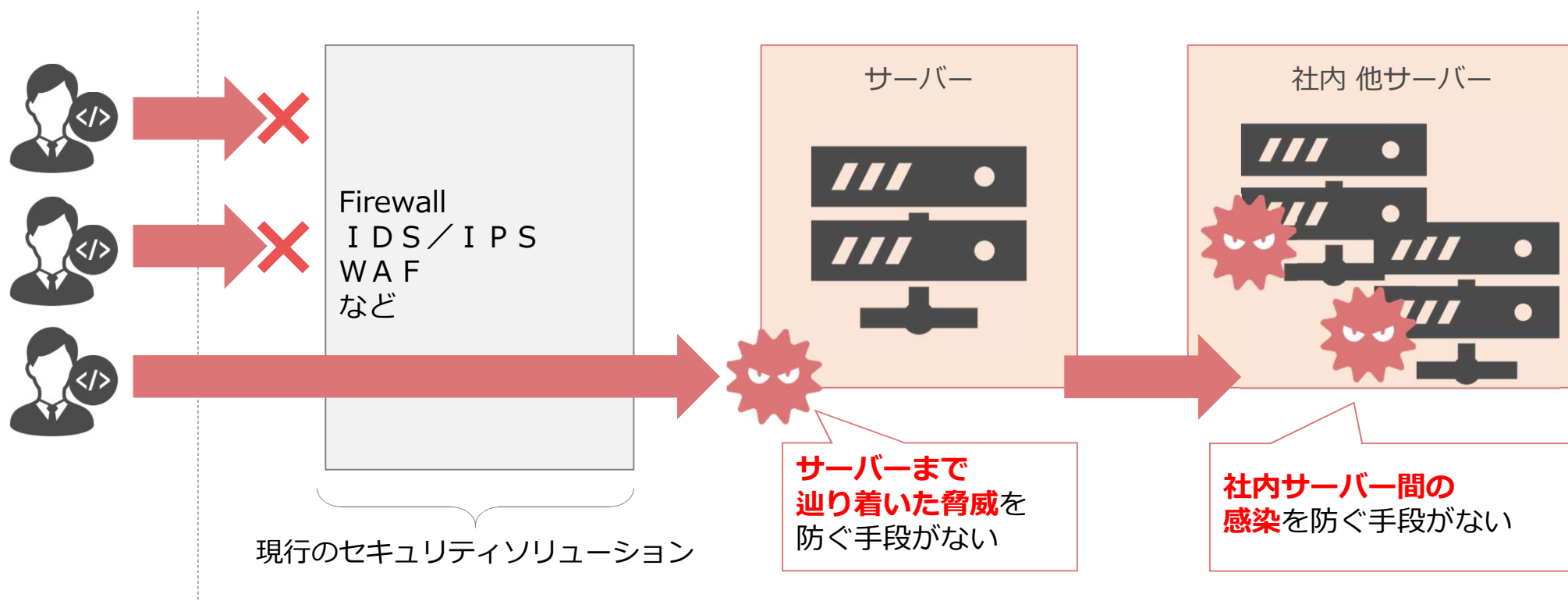
AppGuard Severによるソリューション

脆弱性に依存せずに**不正な動きを防止**する、従来のエンドポイントセキュリティとは異なる方式を実装。

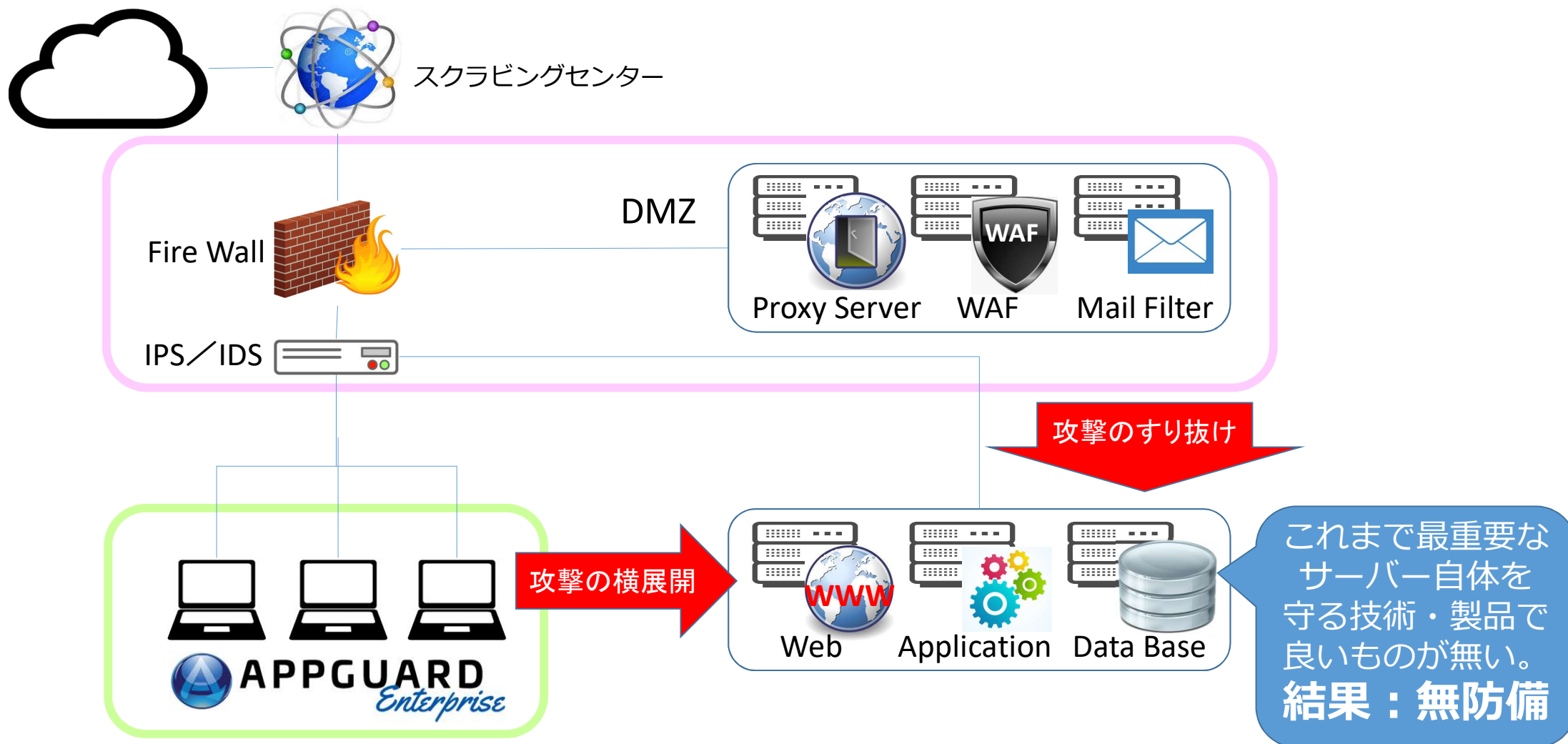


サーバーセキュリティの現仕組みと課題

現在使用されているのはサーバーに接続するまでのセキュリティソリューションのみ。
サーバー本体を守る有効な仕組み（エンドポイントセキュリティ）が存在しない。



サーバー自体のセキュリティ対策



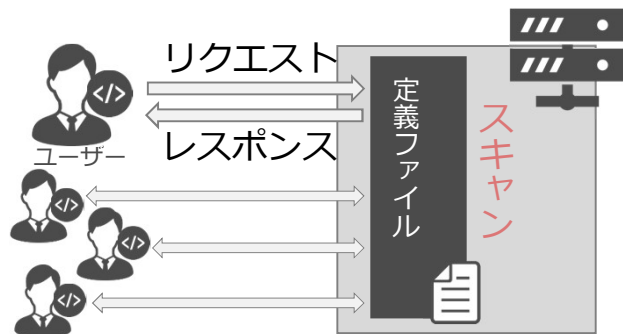
従来型エンドポイントセキュリティによるサーバ保護

リアルタイムスキャンによる処理の遅延や運用コスト等の観点から、サーバーに適したソリューションが存在しなかった。

従来のエンドポイントセキュリティソリューション

アンチウイルス製品

マルウェアの特徴が記録されたファイルを基にマルウェアを駆除する方式。

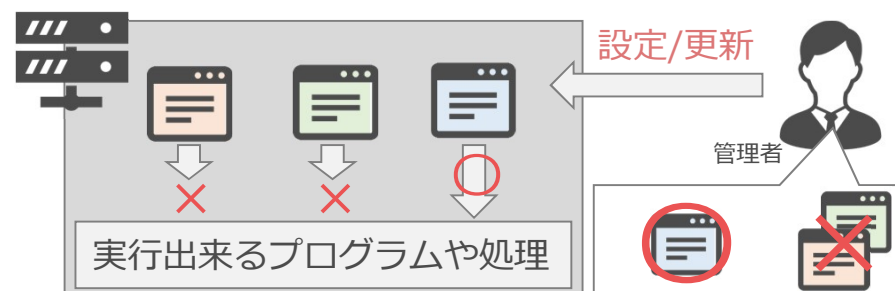


使用されない理由

- ファイルを利用しない“通信リクエスト”による攻撃がメインであり、**ファイルスキャンが効果的でない**。
- 複数人からの同時アクセスを受けることで**高負荷**になり**性能問題が発生する**。

ホワイトリスト型

動作を許可するアプリ・プロセスの一覧表を作成することで、悪意ある操作を行わせない。

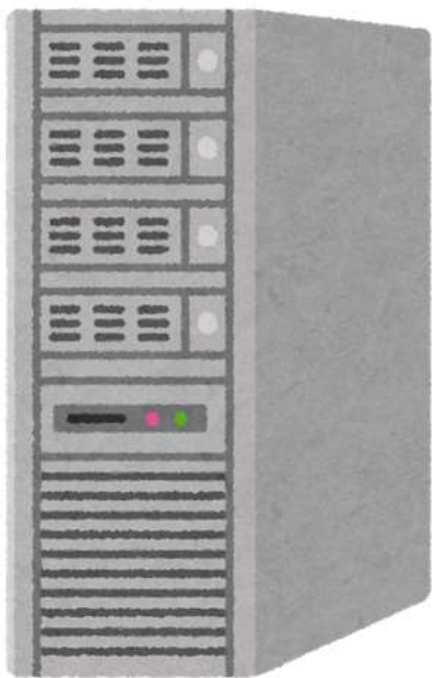


使用されない理由

- アプリや処理の追加・更新を行うたびにホワイトリストの更新が必要とされ、メンテナンスに**膨大な人的運用コスト**がかかる。
⇒アジャイル開発には不向き

サーバー専用ソリューションの要件

アプリケーションの要件とは別に、サーバーとして本来求められるモノが必要



軽量

リクエストおよび利用ユーザが多いサーバでは軽量であることが安定したサービスを継続するために必須

プロセス制御

ファイルからではなく、サーバへのリクエストによるプロセスの不正な行動や処理を制御することが必要

運用容易性

アジャイル開発によるアプリケーションの頻繁な更新、OS やミドルウェアへのパッチ適用時などもスムーズに行える運用の容易性が必要

APPGUARD SERVERの優位性

従来型のセキュリティでは実現不可能であったサーバーのエンドポイントセキュリティとして運用可能。

サーバーセキュリティの課題

サーバーまで辿り着いた脅威を防ぐ手段がない。

ファイルを利用しない通信リクエストによる攻撃がメインであり、ファイルスキャンが効果的でない。

複数人からの同時アクセスを受けることで高負荷になり性能問題が発生する。

ポリシーのメンテナンスに膨大な人的運用コストがかかる。

APPGUARD SERVERによるソリューション

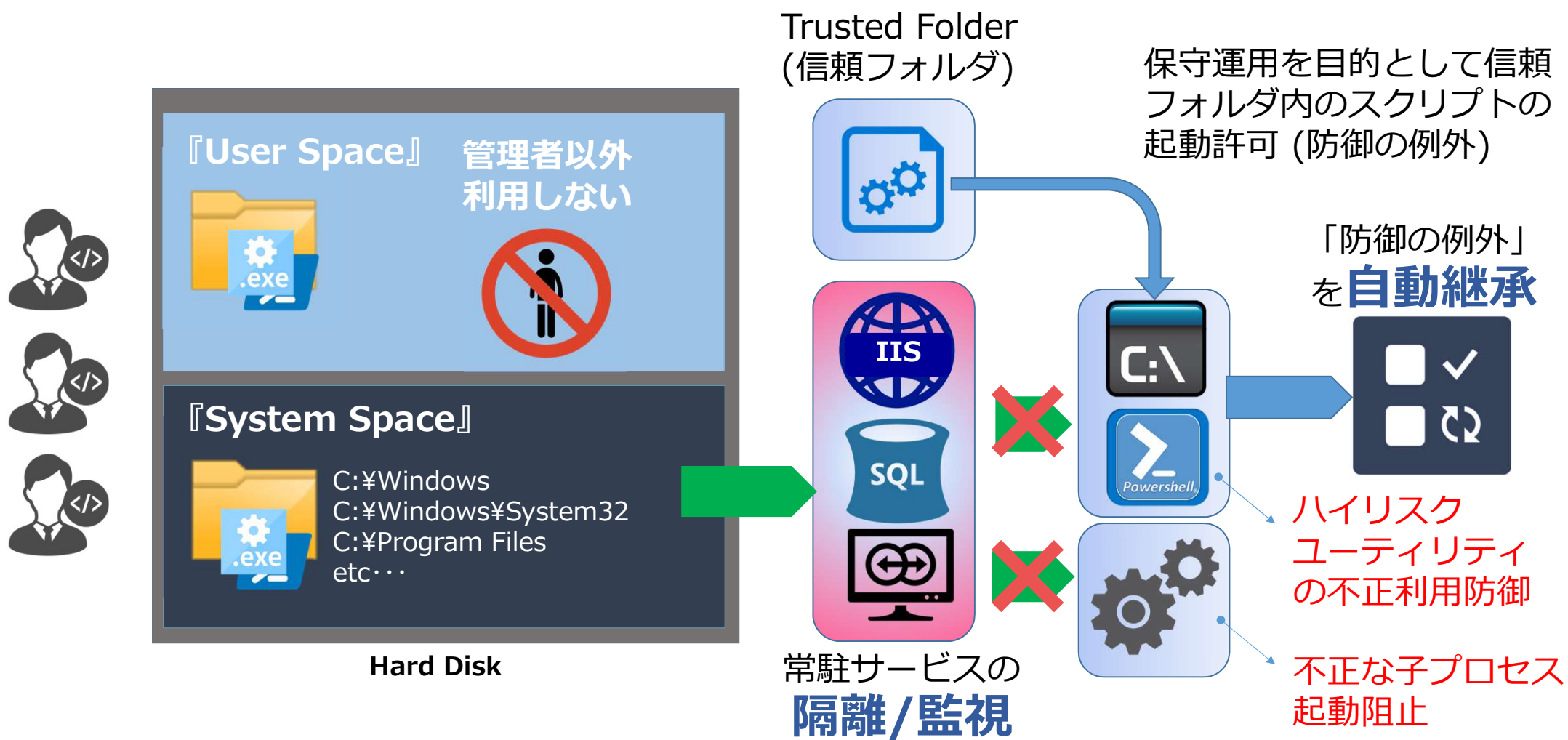
今まで空白だった**エンドポイントセキュリティ**を担保。サーバー自体の保護が可能。

適切なサービスを提供しながら、**攻撃者からの悪意のある処理を阻止**。

定義ファイルを用いないため**サーバーへの負荷は軽微**であり、**動作も軽快**。

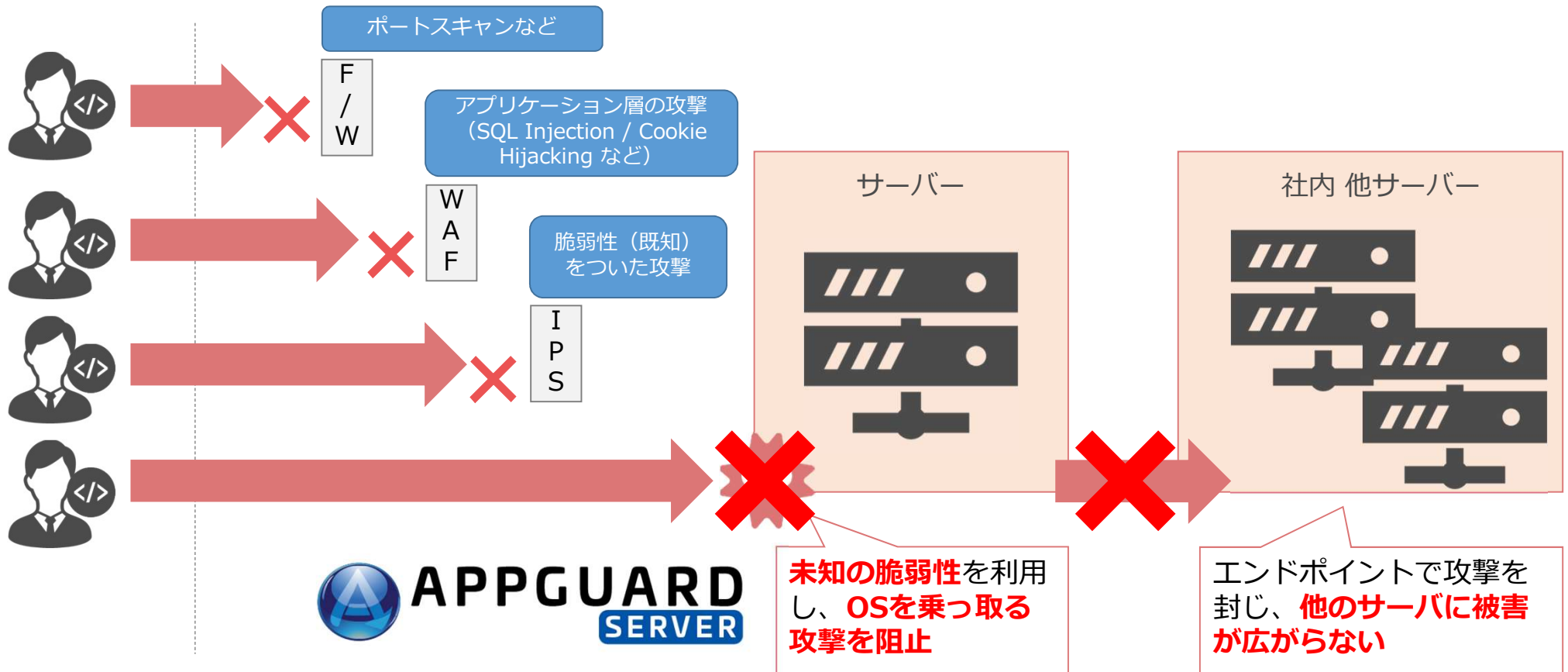
対象ミドルウェア毎に**ポリシーセットを用意**。また追加のポリシーを設定する場合も、**都度のポリシー更新は不要**。

AppGuard Serverの防衛技術



サーバの多層防御とAppGuard Serverの役割分担

AppGuard Server では、ネットワークセキュリティを通過した脅威からサーバの乗っ取り(ランサムウェアやスパイウェアによる攻撃およびそこから被害拡大)を防ぎます。



システム構成

