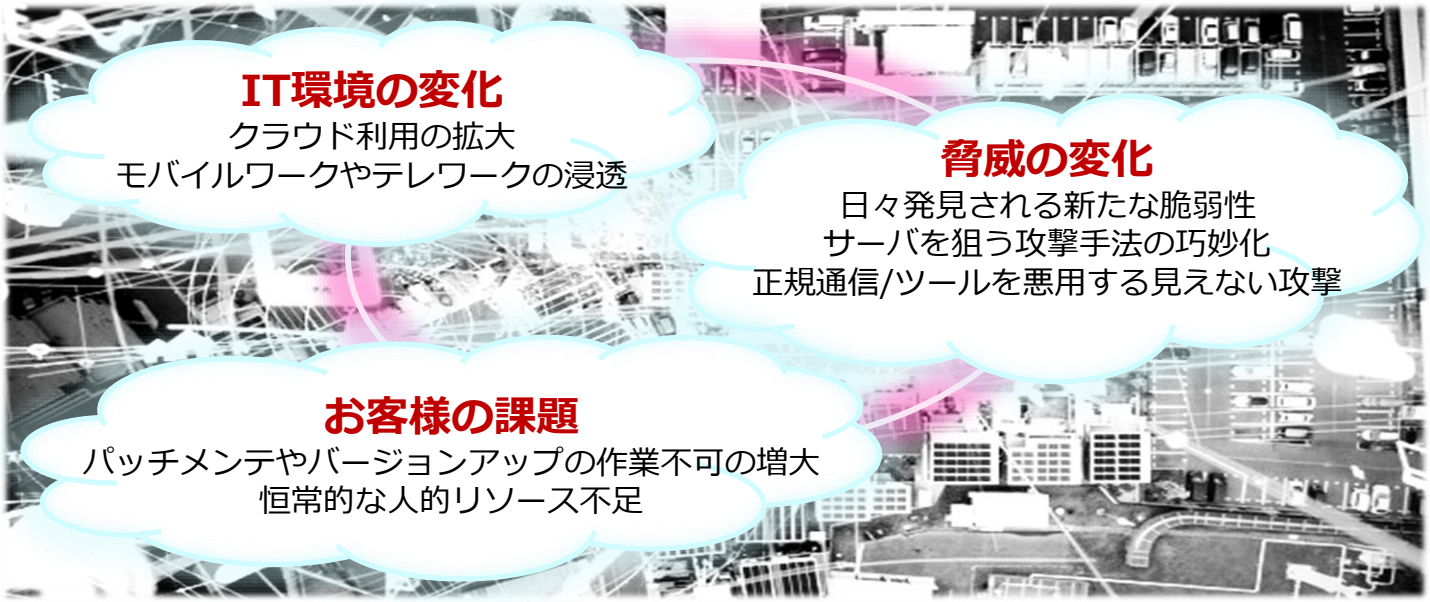
サーバセキュリティ
SaaS型へ切り替えませんか？



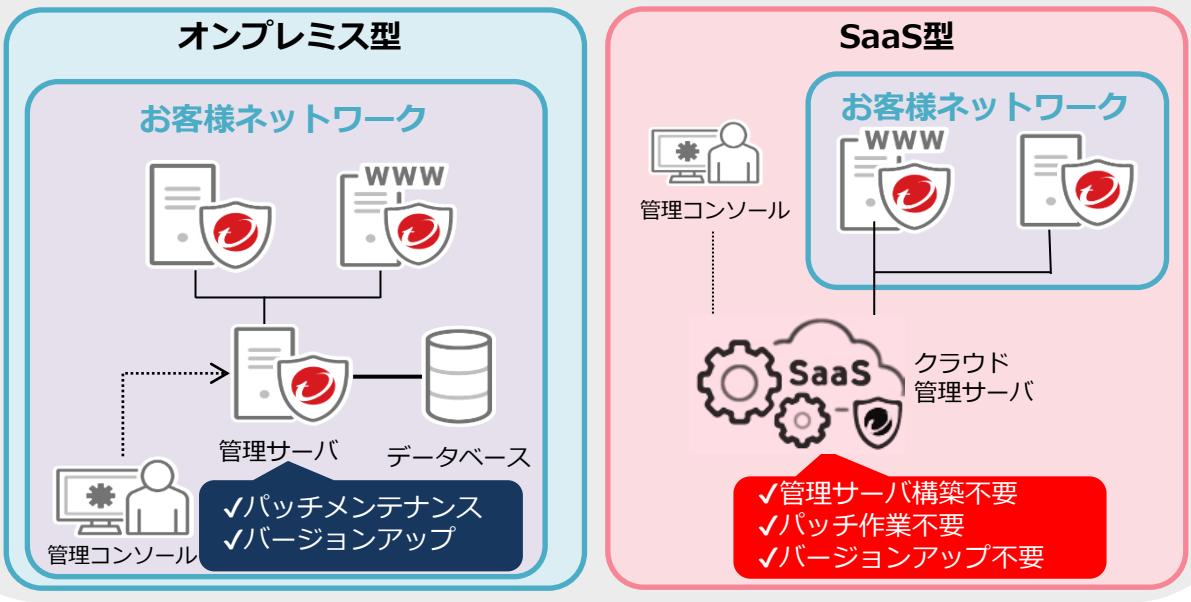
IT環境の変化
クラウド利用の拡大
モバイルワークやテレワークの浸透

脅威の変化
日々発見される新たな脆弱性
サーバを狙う攻撃手法の巧妙化
正規通信/ツールを悪用する見えない攻撃

お客様の課題
パッチメンテやバージョンアップの作業不可の増大
恒常的な人的リソース不足

解決のカギは・・ **“自動化”** **“クラウド管理”** ➡ **SaaS**

オンプレミス型とSaaS型の違い



SaaS型に移行することのメリットは？

メリット① クラウド管理サーバの利用でコスト削減

- ✓ 社内に管理サーバの構築は不要
- ✓ 初期導入費用とバージョンアップ作業費用の削減

メリット② 運用の自動化による作業負荷の軽減

- ✓ 自動アップデート+自動バージョンアップ+自動パッチ適用
- ✓ バグの修正は自動的に即日対応が可能

※全てのバグに即日対応できるわけではありません。

メリット③ 常に最新の状態で脅威対策が可能

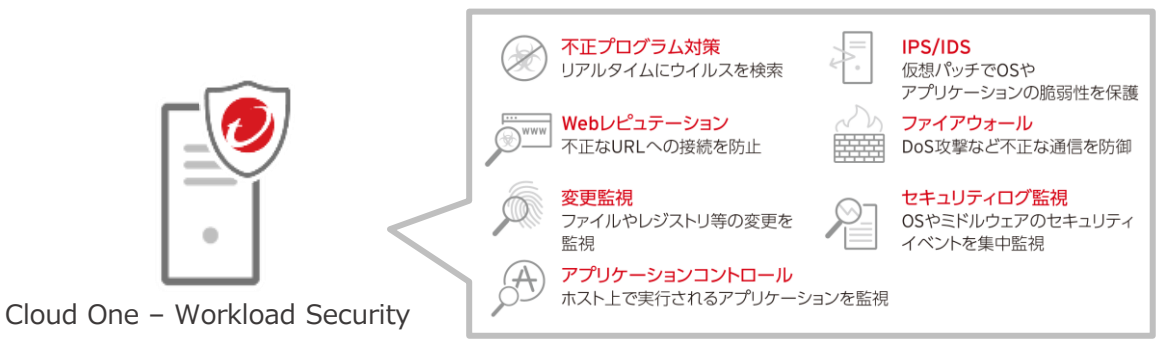
- ✓ 新機能の実装があった場合、自動的に追加することが可能
- ✓ 日々変化するサーバへの脅威に対応

自動化＋クラウド管理でセキュリティ担当者が“楽になる”

オススメのSaaS型サーバセキュリティ

Cloud One – Workload Security

- ■サーバセキュリティに必要な複数の機能を１つの保護モジュール実装
- ■攻撃手口の主流である「サーバに存在する脆弱性を突いた攻撃」にも対応
- ■Deep SecurityのSaaS版なので管理サーバの構築は不要



仮想パッチ（IPS/IDS）とは

脆弱性を狙う攻撃コードを、IPS/IDSルールでブロック。
脆弱性に対して**仮想的に**パッチが当たっている状態にします。