THE NEW VALUE FRONTIER
KYOCERA

SecureOWL

Trend Micro Deep Security（クラウドサーバセキュリティ）

Windows Server 2008サポート終了後のセキュリティリスクへの対策ソリューション

https://www.kccs.co.jp/secureowl/solution/external/deep_security/

Windows Server 2008のサポートが2020年1月14日に終了！
新しいOSへの移行準備は出来ていますか？

サポート終了するとセキュリティリスクが高まります

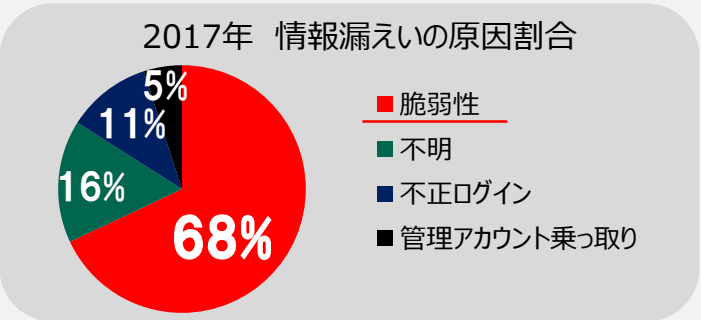
サポートが終了したOSに対しては、マイクロソフトから更新プログラムが提供されなくなります。
新たに脆弱性が発見された場合、その**脆弱性を利用した攻撃からサーバを保護することが出来なくなります。**

■脆弱性とは

プログラムの不具合や設計上のミス等によるセキュリティ上の欠陥のことで、受けるべきでない指示を受けてしまい、意図しない動作を実行してしまうもの。

脆弱性を突いた攻撃は、近年のサーバへの侵入で最も使用されている手法（右図参照）。

サーバに侵入されてしまうことで情報漏洩やWeb改ざん等の被害につながる。



●2017年1月から3月までに報道された事例をトレンドマイクロで独自に整理

脆弱性対策が保護されないことで、恒久的に脆弱性を攻撃されるリスクを伴ったまま
サーバを使用することになってしまいます。
そのため一刻も早いOSの移行が必須となります。

しかし、OSの移行を行いにくいのも事実…

時間が足りない

OSを移行する際の検証に時間がかかり、サポート終了までに移行が間に合わない。

現在のOSでしか使用できない業務アプリケーション

Windows Server 2008でしか動作しない業務アプリケーションがある。

コストを割けない

OS移行に割くための費用が準備できていない。

Trend Micro Deep Securityなら
Windows Server 2008上での脆弱性保護を
2023年5月23日までサポートいたします。

Trend Micro Deep Securityによる脆弱性保護

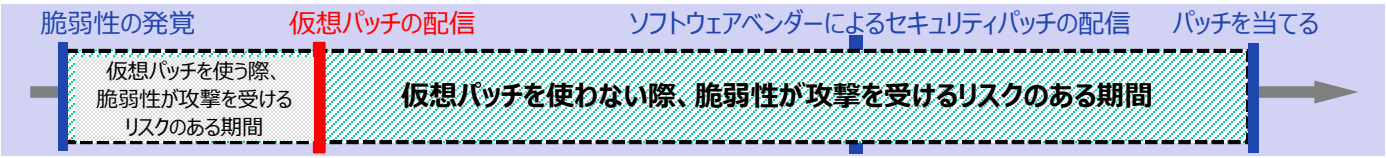
Deep Securityは、「仮想パッチ」で脆弱性を狙う攻撃から自動でサーバを保護可能

※脆弱性を狙う攻撃をIPSルールでブロックすることによってあたかもパッチが当たっている状態にすることを「仮想パッチ」といいます。

◎脆弱性を狙った攻撃をネットワークレベルでブロックする仮想パッチを使って、脆弱性保護が可能。

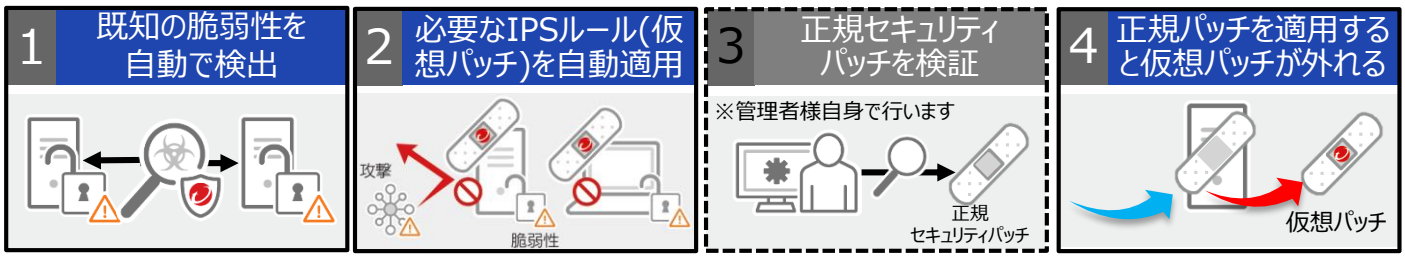
仮想パッチのメリット①

○仮想パッチは、ソフトウェアベンダーが配信する正規のセキュリティパッチと違い、OSのコードレベルでの修正が不要です。
そのため、正規のセキュリティパッチよりも短い期間で配信することが可能で、脆弱性が攻撃を受けるリスクのある期間を大幅に短縮することが出来ます。



仮想パッチのメリット②

○推奨設定検索を実施していただくことによって、Deep Securityが保護しているサーバ内の既知の脆弱性を自動で発見し、それに対応する仮想パッチを自動で適用することが出来ます。
これによってサーバ管理者様の脆弱性管理にかかる負担を大幅に軽減することができます。



※サポート終了に伴い、正規パッチがリリースされない場合は、仮想パッチは適用されたままとなります。

KCCSならではの柔軟なDeep Securityプロフェッショナルサービス

経験豊富なセキュリティエンジニアがお客様環境や要件に合わせ設計～本番作業をワンストップでご提供。
ご要望に合わせ、サーバ移行までの継続的な運用支援のご提案などトータルソリューションのご提案も可能です。

【標準プロフェッショナルサービス】

1 要件定義・サイジング	2 導入ポリシー設計	3 作業準備・作業実施	4 動作確認	5 図書作成・完成図書納品
お客様の環境、および要件をヒアリングし導入製品や、導入範囲を策定します。	お客様にヒアリングシートを記載いただきます。また、適用ポリシーを決定しパラメータ設計を実施します。	作成済みの設計書をベースにお客様環境に事前調査および導入作業を実施します。	導入後に機能が正常に動作することを確認します。	パラメータ設計書の更新および動作確認シートを作成し、納品します。

KYOCERA
京セラ コミュニケーションシステム株式会社
KCCSカスタマーサポートセンター
フリーコール　0120-911-901
携帯電話・PHS・IP電話など　050-2018-1827
受付時間　平日9:00 ～ 17:00
（17:00以降のお問い合わせは自動応答になります。）
KCCSホームページ　http://www.kccs.co.jp/
E-mail：kccs-support@kccs.co.jp

2018年12月現在