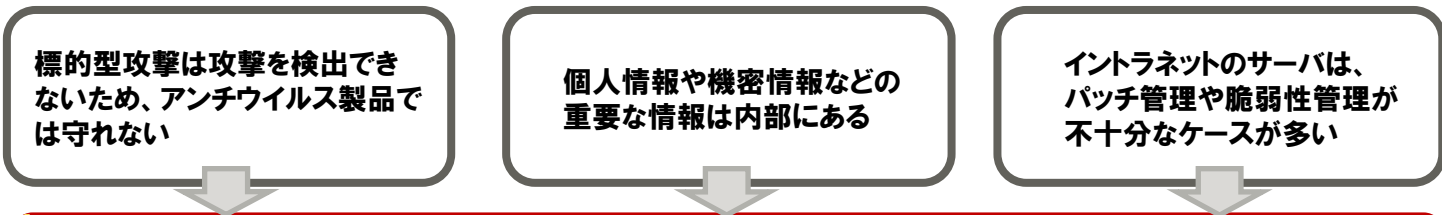


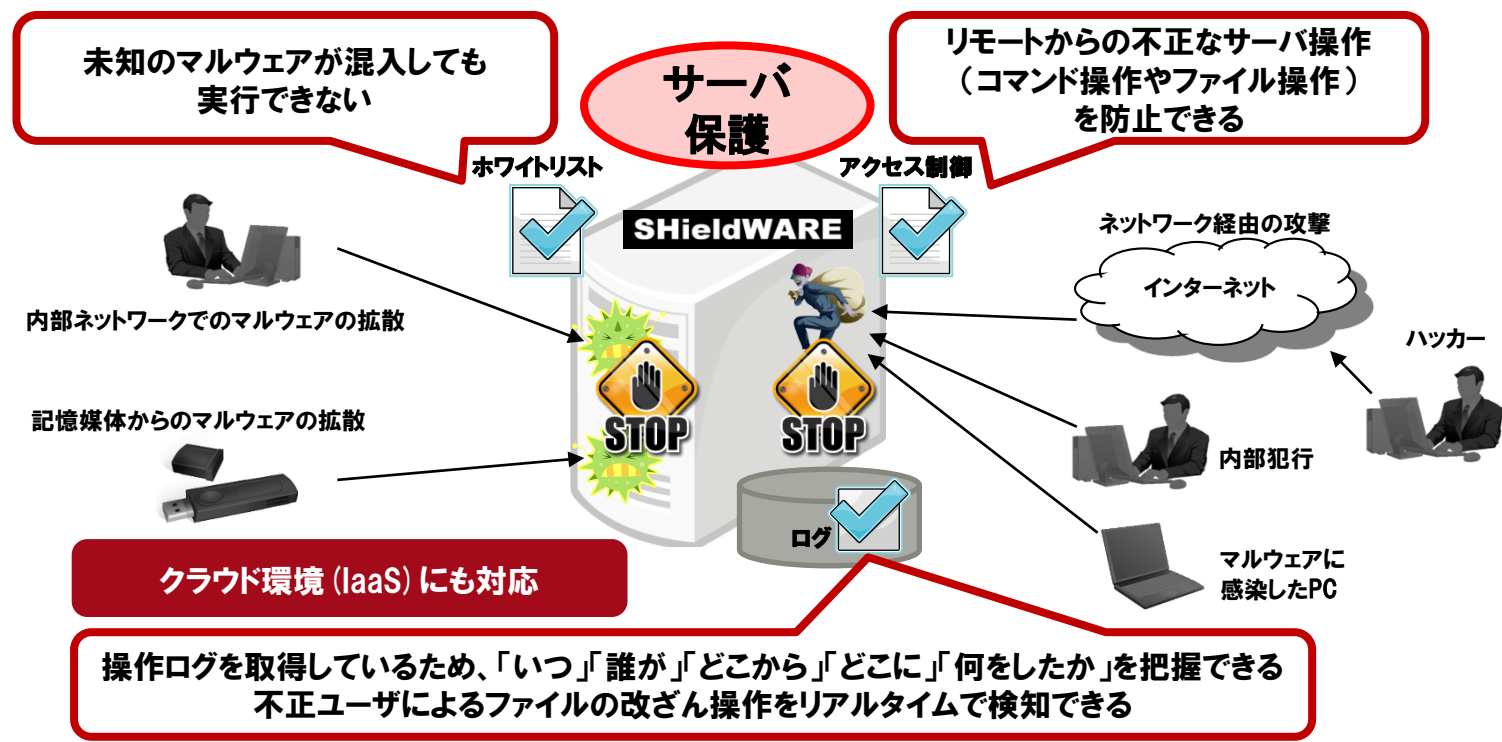
SHieldWARE(シールドウェア) 社内の重要サーバを標的型攻撃から守る

特定の組織・人を標的とし、機密情報を詐取することを目的としたサイバー攻撃は増加の一途を辿っています。複数の対策を適切に組み合わせる多層防御の一環として、内部ネットワークにあるサーバの堅牢化が重要視されています。



内部ネットワークに存在する重要サーバも攻撃を受ける対象となる

対策ソリューションの概要



製品価格

品名		ライセンス数	標準価格 (円)	対象OS	対応OS
メディアバック	メディアバック	-	10,000	マルチ	-
統合管理サーバ	統合管理サーバ (標準版) 用 ライセンス	1	480,000	Linux	RHEL 6.3 ~ 6.10 7.1 ~ 7.6
	統合管理サーバ (暗号化DB版) 用 ライセンス	1	1,500,000	Linux	
	統合管理サーバ (大規模DB版) 用 ライセンス	1	1,980,000	Linux	
仮想コンピュータ用	仮想コンピュータ用 ライセンス	1	280,000	マルチ	RHEL 6.3 ~ 6.10 7.1 ~ 7.6
物理コンピュータ用	1-2CPUサーバ用 ライセンス	1	380,000	マルチ	Microsoft Windows Server 2008 ~ 2016 Oracle Solaris 11 ~ 11.4
	1-8CPUサーバ用 ライセンス	1	640,000	マルチ	
	CPU数無制限サーバ用 ライセンス	1	980,000	マルチ	

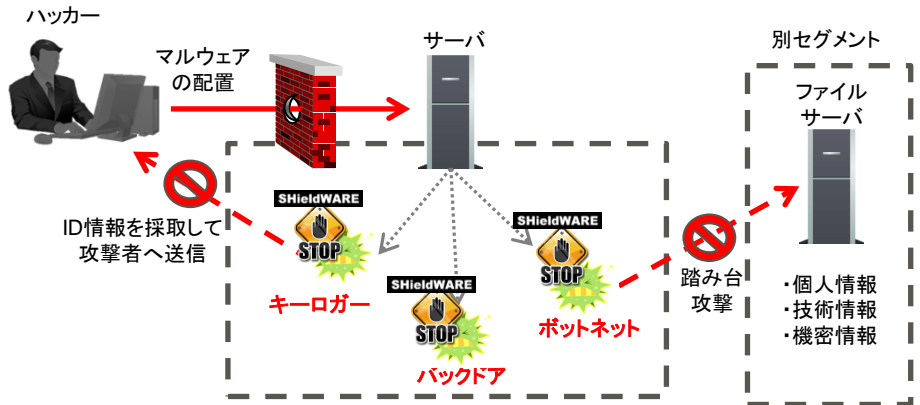
ホワイトリストによるプログラム実行制御

POINT

導入効果

マルウェアが配置されても、実行できないため、情報採取が行われたり、踏み台サーバとして利用されることを防ぐことができます。

- ・キーロガーツールを利用したID情報の奪取を防止できます。
- ・ポットネット等を利用した別サーバへの攻撃を防止できます。
- ・バックドアを利用したハッカーの容易なアクセスを防止できます。



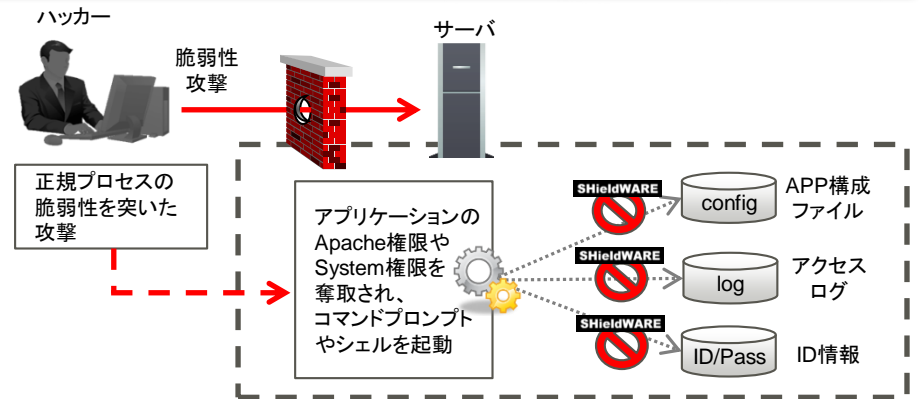
アクセス制御

POINT

導入効果

Root/Administrator/system権限などの特権を奪取されても、重要なファイルの改ざんや、不正コマンド操作を防ぐことができます。

- ・不正操作の痕跡削除(ログの改ざん等)を防止できます。
- ・アプリケーションのコンフィグファイルやID情報などの改ざんを防止できます。
- ・不正ユーザからのコマンド操作(ID追加や設定変更等)を防止できます。



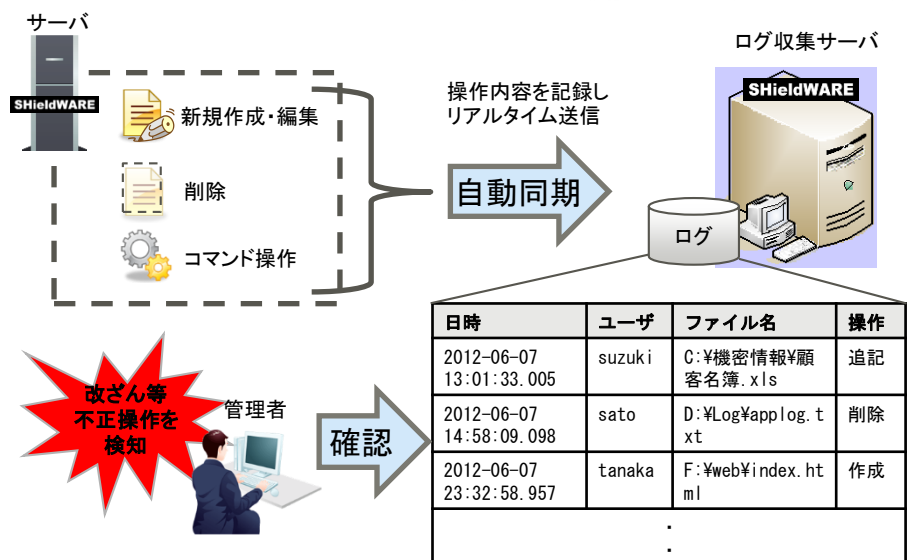
不正操作検知 (監査証跡)

POINT

導入効果

OSレベルでは取得できない詳細ログ(サーバの操作履歴など)をリアルタイムに取得できるため、ファイル改ざん等不正操作をすぐに検知できます。

- ・PCI DSS やNISC 統一基準で求められる要件に対応できるレベルの証跡を取得できます。
- ・不正操作のみを抽出することで、攻撃を早期発見できます。
- ・特権へと昇格する前のユーザ情報も取得できるため、詳細な原因究明を行うことができます。



※記載の会社名、商品名は、各社の商標または登録商標です。
 ※記載された情報は、予告なく変更することがあります。
 ※記載の内容は、2019年8月現在のものです。

お問い合わせ先
 株式会社富士通ソーシャルサイエンスラボラトリ(富士通SSL)
 お問い合わせ総合窓口
 〒211-0063 川崎市中原区小杉町1-403武蔵小杉タワープレイス
 E-mail : ssl-info@cs.jp.fujitsu.com
 当社ホームページ <http://www.fujitsu.com/jp/group/ssl/>