FUJITSU

FUJITSU Software
システムウォーカー　セキュリティ　コントロール
Systemwalker Security Control V1

サイバー攻撃への対処負荷の軽減と確実な運用を実現

正規の業務に紛れて巧妙に企業システムへの侵入を図るサイバー攻撃への対策には、速やかな検知と初動対処により被害を抑えることが重要です。
Systemwalker Security Controlは、検知製品と当社での運用実践知を組み合わせ、サイバー攻撃に対して迅速な対処を実現します。

サイバー攻撃対策を当社実践知で支援

高度化・巧妙化するサイバー攻撃に対し、侵入を前提に、プログラムの動作特性を監視し悪意のあるコードを判定する検知製品の採用が始まっています。しかし、検出される「疑わしい挙動」のアラートを理解し、適切な切り分けと対処を行うためには、専門的な知識の習得と経験の蓄積が不可欠でした。
Systemwalker Security Controlは、検知製品と連携し当社運用での実践知を組み合わせ、アラートの切り分け・対処から再発防止対策まで、迅速なサイバー攻撃対策を支援します。

検知製品と容易に連携

Systemwalker Security Controlは、ネットワーク通信やPCプログラムの挙動を監視する最新の検知製品群と連携します。有力な検知製品との継続的な連携により、新たなセキュリティ脅威にも対抗していきます。

実績にもとづく最新の運用知見を継続的に提供

検知製品での新たな検知内容への対応や、当社社内実践に基づいた最新の実践知は「運用シナリオ」として、製品購入後も提供* します。

セキュリティ運用の標準化による対処品質の向上

お客様のICT基盤は、複数の拠点や様々なスキルの人員で運用されています。次々と登場する攻撃手口に対し、人手による切り分けと対処では、スキルのばらつきやヒューマンエラーによる運用リスクが発生します。攻撃手口に対応した適切な対応フローを標準化することで、対処品質を向上できます。

* 別途契約が必要です。

図1 実践知によるｻｲﾊﾞｰ攻撃対策運用

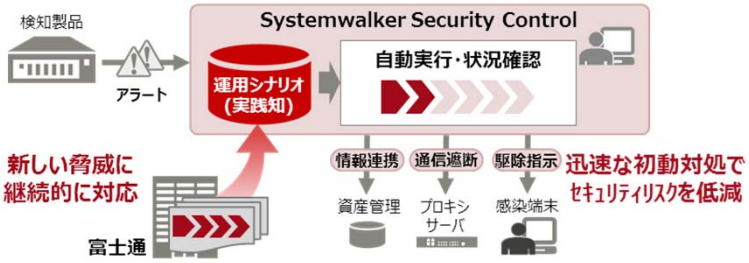


図2 対応フロー

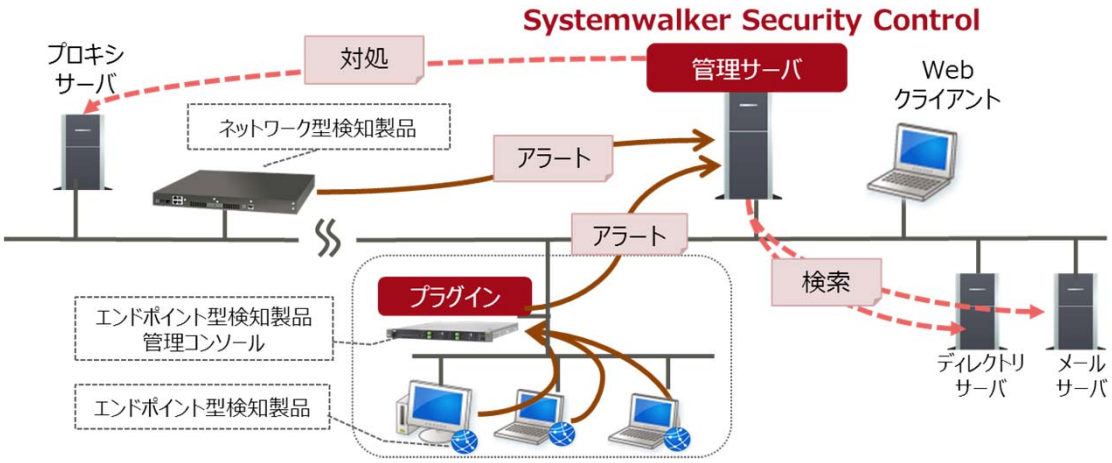
- ✓ オープン中のインシデントの全体状況を表示
- ✓ 対処完了の目標日時が迫ったインシデントを抽出
- ✓ 対処状況を見える化し、対処の実施をナビゲート

迅速な初動対応によるリスクの低減

検知製品からの大量のアラートを監視し、リスクレベルを判定。対処が必要なアラートに対し、ネットワーク通信の遮断など迅速に初動対処を開始することができます。
ユーザ情報、PC/サーバの構成情報等と組み合わせることで、感染端末の特定、さらに、特定した感染端末の利用者や管理者には、アラートに応じた対処方法を、速やかに指示することが可能です。
侵入したマルウェアが放置される時間とともに、リスクが増大します。攻撃者の活動開始までに初動対処を行うことで、情報漏洩や感染拡大のリスク、対処コストを低減します。

図3 初動対応時間の削減

システム概要図



入口・出口対策への適用

ネットワーク型検知製品との組み合わせにより、ネットワーク上を流れる通信データを監視し、マルウェアの検知と対処が行えます。導入する検知製品により、Webサーバや電子メール、不審ファイルやボット攻撃に関する通信が、監視できるようになります。

業務保護対策への適用

エンドポイント型検知製品との組み合わせにより、PC上のプログラムの振る舞いを監視し、マルウェアの検知と対処が行えます。従来のパターン型対策製品では検知できないマルウェアに対し、挙動監視による検知ができるようになります。

商品体系

FUJITSU Software Systemwalker Security Control V1

- Systemwalker Security Control メディアパック (64bit) *1
- Systemwalker Security Control プロセッサライセンス *2

*1： メディアパックは、インストール用媒体商品です。別途、必要なライセンスをご購入ください。
*2： 本商品では、管理サーバのプロセッサ数分(マルチコアプロセッサ搭載サーバの場合はコア数)に応じたライセンスが必要です。
なお、本ライセンスには、「1年間24時間サポート」がバンドルされています。

動作環境

種類/用途	動作OS	
管理サーバ	Microsoft® Windows Server® 2012 R2 (64-bit) / Microsoft® Windows Server® 2012 (64-bit)	
プラグイン	【FFR Enterprise Management Console用】 Microsoft® Windows Server® 2012 (64-bit) Microsoft® Windows Server® 2008 R2 (64-bit) / Microsoft® Windows Server® 2008 (64-bit) / Microsoft® Windows Server® 2008	
Webコンソール	Windows® Internet Explorer® 9 / Windows® Internet Explorer® 10 / Windows® Internet Explorer® 11	
連携製品	**検知**	【エンドポイント型検知製品】 FFR yarai [株式会社ＦＦＲＩ社製] 【ネットワーク型検知製品】 ・FireEye NX Series / FireEye EX Series [ファイア・アイ株式会社製] ・チェック・ポイント アプライアンス [チェック・ポイント・ソフトウェア・テクノロジーズ株式会社製] (Anti-Bot Software Blade、Threat Emulation Software Blade)
	対処	【プロキシサーバ】 Squid 2.6 / Squid 3.1 [フリーソフトウェア]
	ユーザ情報	Microsoft® Active Directory 2012 / Microsoft® Active Directory 2008
	メール宛先情報	Microsoft® Exchange Server 2013 / Microsoft® Exchange Server 2010

製品・サービスについてのお問い合わせは

富士通コンタクトライン
0120-933-200
受付時間 9:00～17:30（土・日・祝日・年末年始を除く）
富士通株式会社 〒105-7123 東京都港区東新橋1-5-2 汐留シティセンター
http://www.fujitsu.com/jp/software/systemwalker/securitycontrol/