マルウエア感染などにより不正な通信を行う端末を即時に隔離

情報セキュリティ事故の増加

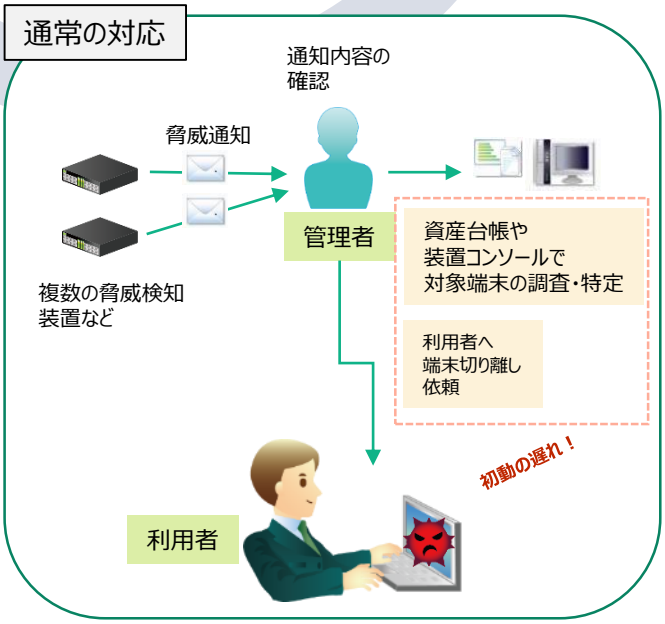
標的型攻撃やランサムウエアによる被害は近年の大きな脅威となっています。侵入の痕跡を隠しながら活動するマルウエアなど、手段が高度化しています。万が一の重大な被害を回避するには、異常な状態を早期に検知するのと同時に、初動対応を早く行えるよう準備することが非常に重要です。

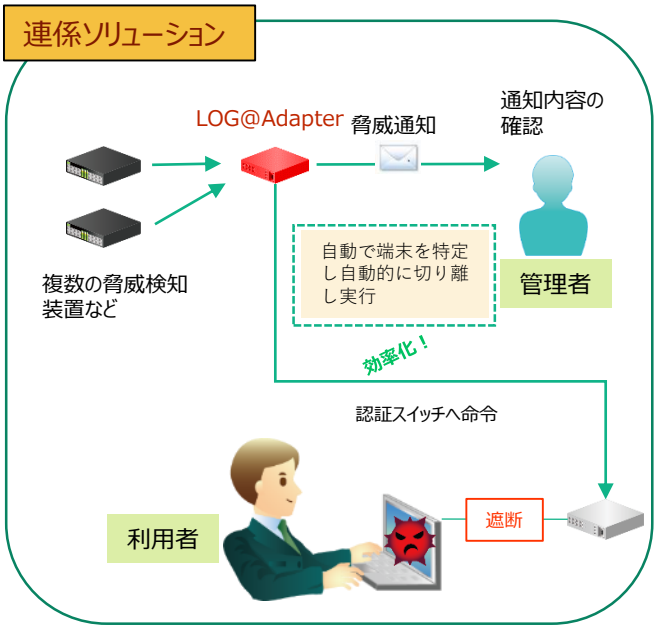
不正通信端末 遮断ソリューション

万が一、攻撃を受けた場合でも、自動的に端末をネットワークから隔離

インシデント対応における初動（脅威検知、端末特定、脅威遮断）を効率化します。

■ ソリューション概要
- 脅威検知装置から脅威を通知
- LOG@Adapterで解析し端末を特定
- 端末を自動的に遮断し、管理者に通知





エイチ・シー・ネットワークス株式会社

@Adapterシリーズによる接続端末の把握と自動通信遮断

▼ 概要

LOG@AdapterとAccount@Adapter+をIPSなどの脅威検知製品と組み合わせることで、マルウエアに感染した端末をネットワークから自動的に遮断します。

LOG@Adapterはネットワークに接続している端末の情報(※)を把握し、発生源の特定を容易にします。
また、Account@Adapter+はブラックリスト機能により感染端末のネットワーク再認証(再接続)を防止します。
IPSやファイアウォールなどの脅威検知機器が発する不正通信の検知情報など、あらかじめ指定したキーワードを含むsyslogをLOG@Adapterが受信したことを起点として、認証アカウントのブラックリスト登録と認証スイッチに対してのログアウトコマンド発行を自動で行います。
一般的に利用されているsyslogを使用するため、既存設備を生かしたさまざまな環境への適用が可能です。

※「RADIUSクライアント」、「接続ポート」、「認証アカウント」、「MACアドレス」、「IPアドレス」

さまざまな脅威を連携ソリューションで多層防御

▼ 脅威と対策の例

▼ 連係確認機器

IPS	DAMBALLA Checkpoint Fortigate® +FortiAnalyzer® PaloAlto® SecureSoft Sniper ONE
認証スイッチ	APRESIA® ALAXALA® Cisco® WLC
DHCP	Account@Adapter+ ISC-DHCP
ネットワークセンサー	VISUACT-X

注：本ソリューションのみですべての脅威を防御できるわけではありません

▼ ソリューション構成製品

認証ログを可視化するsyslog管理アプライアンス

LOG@Adapter ログ アダプター

●いつ・誰が・どのPCで・どのスイッチ&ポートから、接続しているか把握
●認証スイッチやIPSなどの不正通信検知装置Account@Adapter+と連係して、認証スイッチから不正通信端末をログアウト

ログ検索機能 / レポート機能 / ログアクション機能 / APRESIA、ALAXALA、Aruba QuOLA@Adapter 連係機能 / 端末遮断機能

アカウント管理を変えるこれからの認証アプライアンス

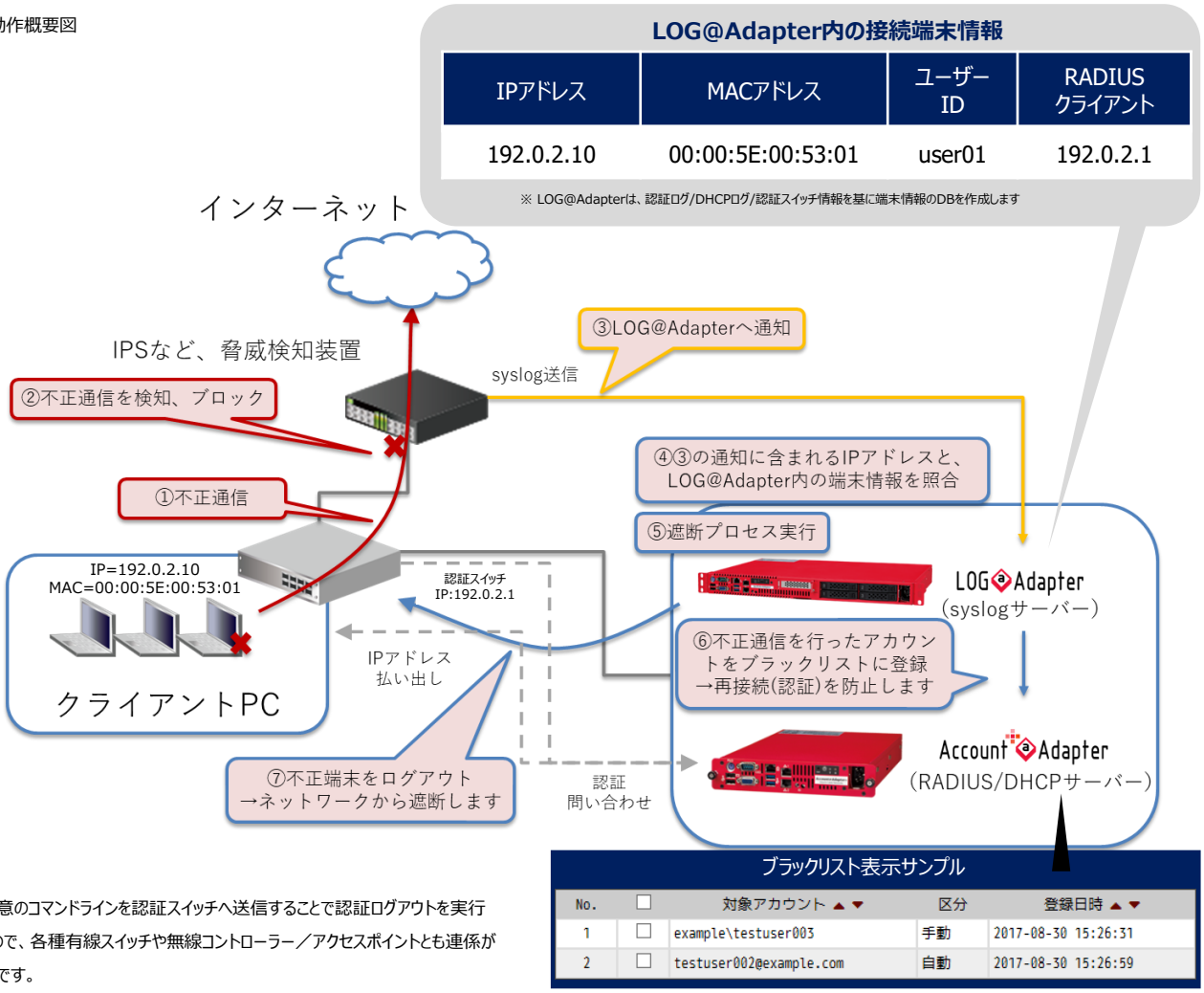
Account@Adapter アカウント アダプター プラス

●RADIUSサーバー／アカウント管理
●認証局　●アカウント申請ワークフロー
●DHCPサーバー　●ブラックリスト

RADIUSサーバー / LDAP/AD連係 / 認証局（CA） / 証明書ダウンロード / ID/端末申請ワークフロー
ゲストID自動発行 / MACアドレス収集 / DHCPサーバー / Shibboleth SP / UPKIクライアント証明書配付

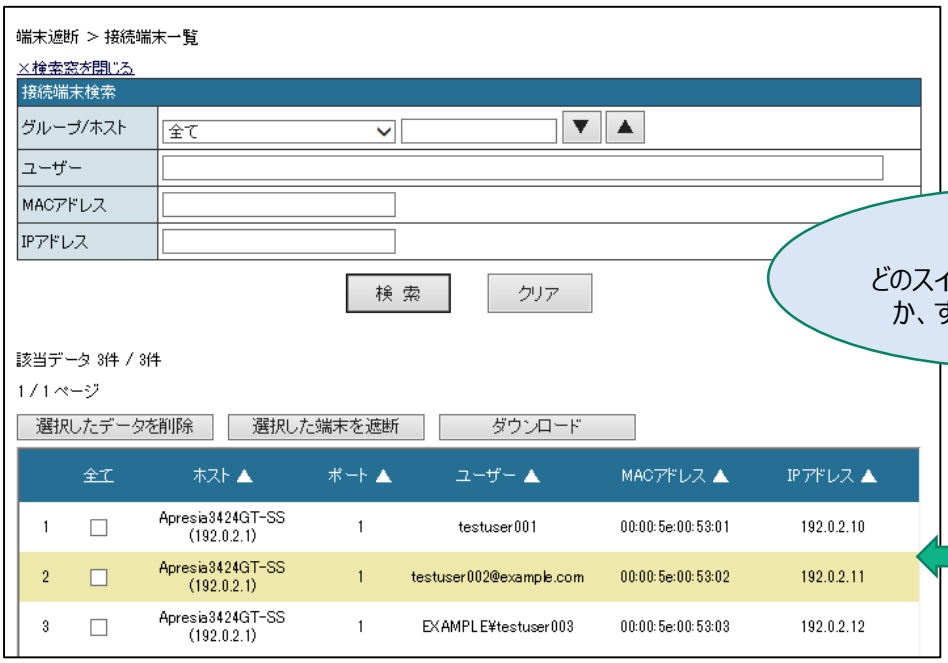
不正通信端末遮断ソリューション動作概要

▼ 動作概要図



※任意のコマンドラインを認証スイッチへ送信することで認証ログアウトを実行するので、各種有線スイッチや無線コントローラー／アクセスポイントとも連係が可能です。

▼ 接続端末一覧 画面（LOG@Adapter）



どの端末が
どのスイッチに接続されている
か、すぐに把握できます。

自動で端末情報
データベースを作成

多層防御連係シリーズ　外部脅威対策編

次世代ファイアウォール連係

■ ソリューション構成製品

多様化するサイバー攻撃から保護するUTM/次世代FWアプライアンス

サイバー攻撃によるセキュリティ被害は年々深刻化しており、侵害された場合の企業に与えるダメージも大きくなっています。
FortiGateアプライアンスは、導入規模に応じた幅広いラインアップでどの業務形態にも適用することができ、ウイルス対策、ランサムウエア対策、侵入検知・遮断、スパム対策、アプリケーション可視化、Webフィルタリングなどあらゆる攻撃に多彩なUTM機能で高度なセキュリティ脅威や標的型攻撃に対して業界最高の保護機能を提供します。

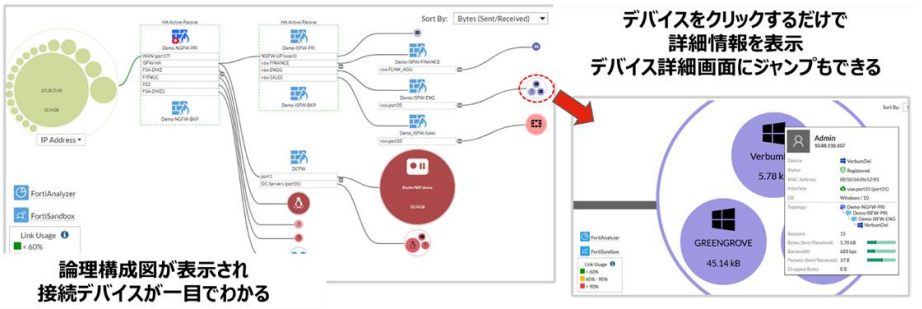
製品の特長

- ネットワーク全体の可視化(右図)
- 標的型攻撃対策の自動運用
- Security Fabric

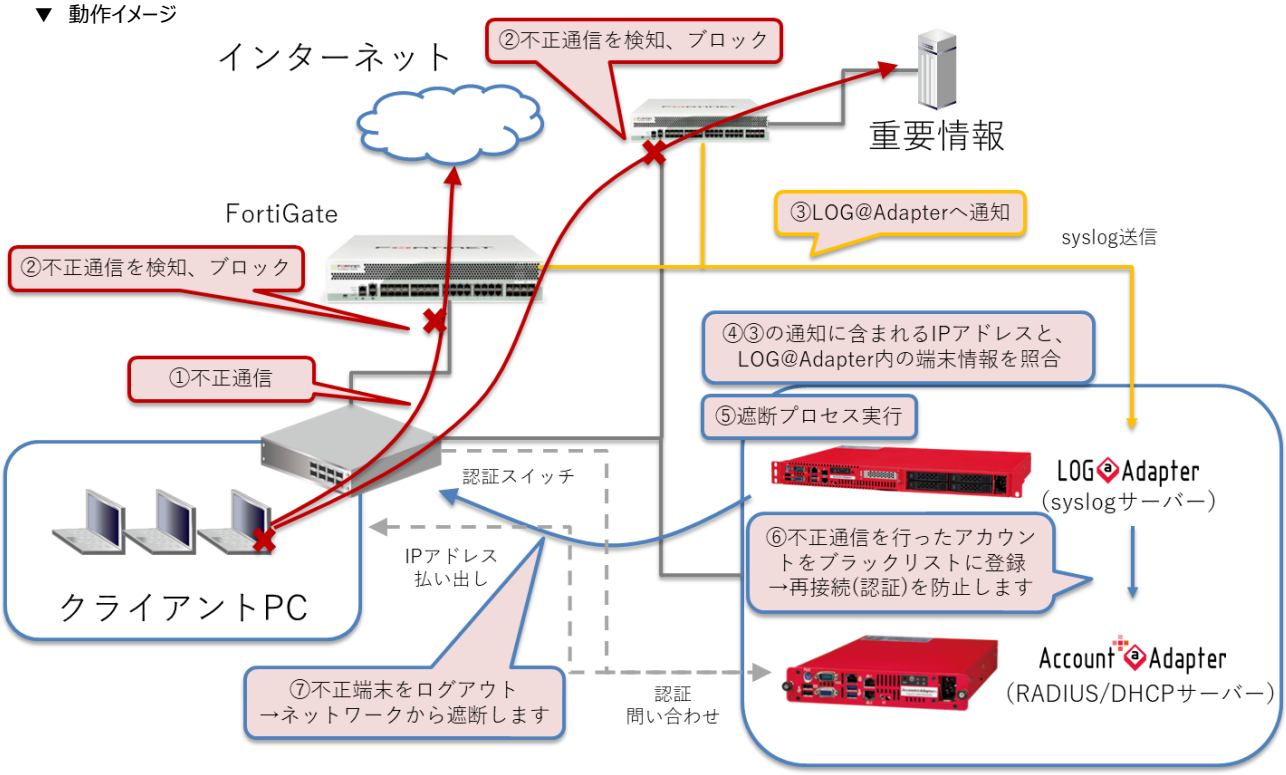
※弊社販売取扱製品

ネットワーク全体の可視化

- FortiViewで、ネットワークトラフィックをあらゆる角度から可視化
- ワンクリックで、送信元、送信先、アプリケーション種別、脅威、インターフェース、デバイス、ポリシー及び国別にトラフィックを表示できます。



▼ 動作イメージ



多層防御連係シリーズ　外部脅威対策編

次世代ファイアウォール連係

■ ソリューション構成製品

アプリケーション、ユーザー、コンテンツを独自の識別技術で可視化しサイバー攻撃に対抗する、次世代ファイアウォール

次世代ファイアウォールシリーズは、ポート番号ではなく利用しているアプリケーションの識別、IPアドレスではなくユーザー名でのトラフィック制御、リアルタイムに脅威を制御するコンテンツ識別、ハイパフォーマンスを実現するアーキテクチャ、さらには未知のマルウエア検知や振る舞い検知機能を搭載した市場をリードする次世代ファイアウォールです。

ネットワークロケーション	データセンター/クラウド	エンタープライズ境界	分散型エンタープライズ/BYOD
次世代ファイアウォール製品群	 アプライアンス: PA-200, PA-500, PA-30x0, PA-50x0, PA-70x0 仮想ソフトウェア: VM-Series VM-100,200,300,1000-HV		
サブスクリプションサービス	脅威防御		
	URLフィルタリング		
	Global Protect™		
	WildFire™		
管理システム	Panorama および M-100 アプライアンス		
OS	PAN-OS™		

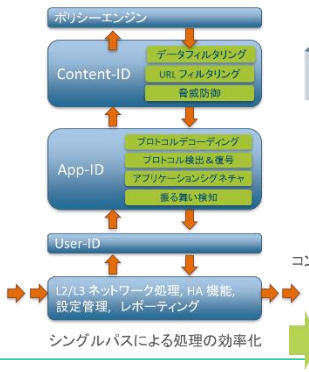
※弊社販売取扱製品

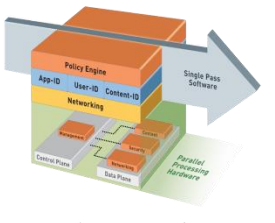
Palo Alto Networks, Inc.

次世代ファイアウォールのアプリケーション識別

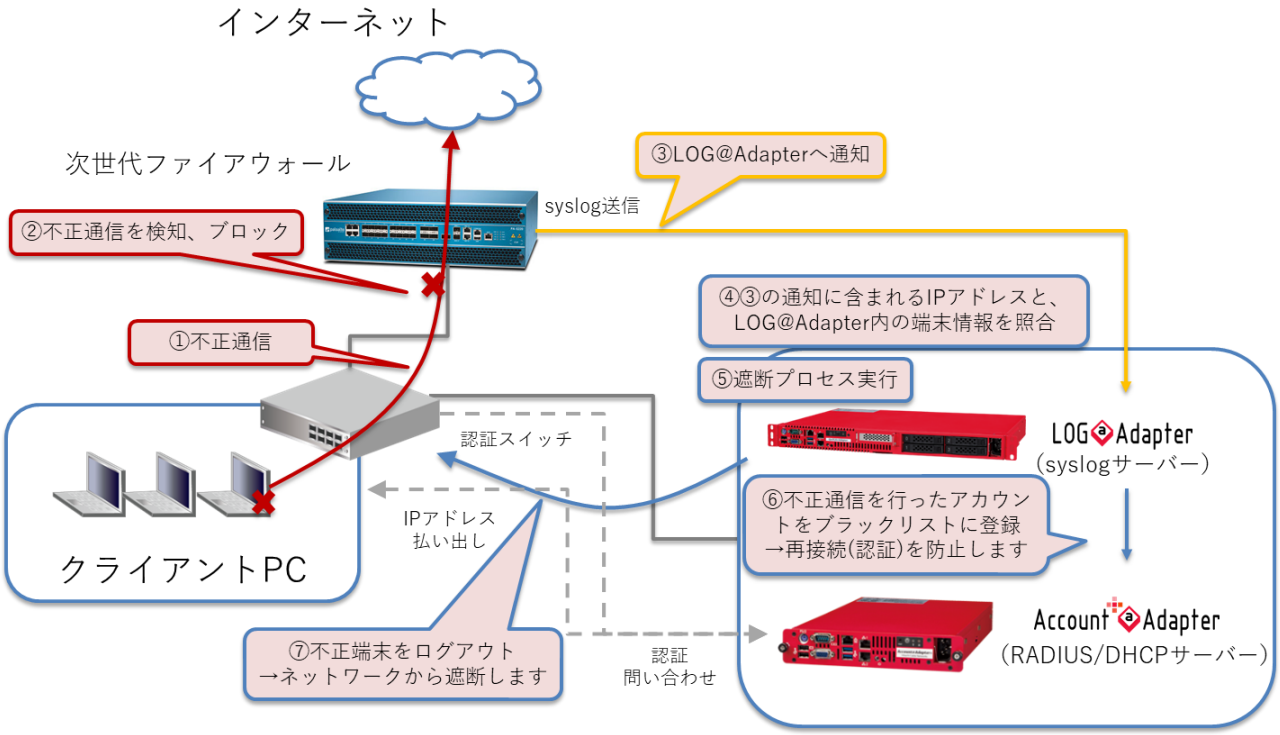
- 全トラフィックのアドレス、ポート、プロトコルの情報に加え、アプリケーション情報も自動的に取得し、識別します。
- SSLにも対応しています。（復号化してアプリケーション識別を行います。）
- ビジネス、インターネット、ネットワーキングと2,000種類以上のアプリケーションとプロトコルを幅広くサポートし、DB更新により毎週続々と対応数を拡大しています。
- お客さまの自社開発のアプリケーションにもリクエストベースで対応しています。
- その場でカスタムシグネチャを作成することも可能です。

◆ 次世代ファイアウォールのアーキテクチャ





▼ 動作イメージ



多層防御連係シリーズ　内部脅威対策編

ネットワークセンサー連係

■ ソリューション構成製品

アズビルセキュリティフライデー株式会社

ITシステムに侵入したサイバー攻撃を検知する ネットワークセンサ

VISUACT™ X　ビジュアクトエックス

発見することが困難なITシステム内部に侵入してしまった高度なサイバー攻撃の検知を独自のWindows解析技術で実現

高度標的型攻撃 攻撃シナリオ(*)

(*) IPA 独立行政法人情報処理推進機構セキュリティセンター「高度標的型攻撃」対策に向けたシステム設計ガイド

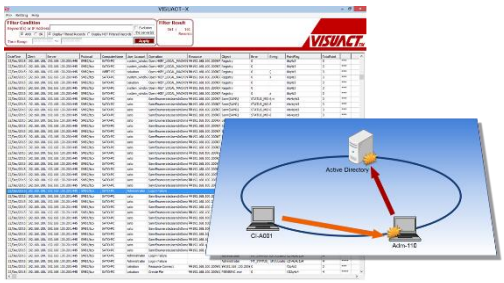
販売・提供元：アズビルセキュリティフライデー株式会社
※製品の詳細は直接お問い合わせください

膨大なネットワークアクセスの中からサイバー攻撃だけを検知します

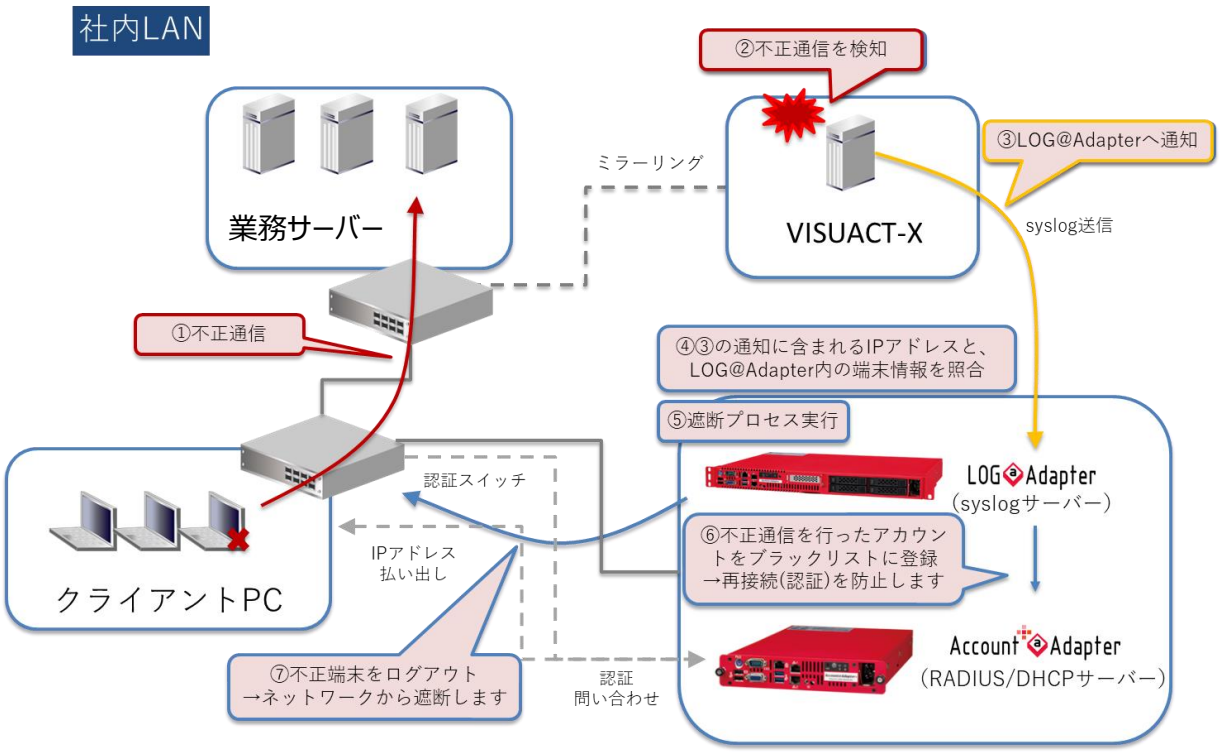
- 膨大なアクセスの中からサイバー攻撃だけを検知し通知します。
- インシデント発生時の事後調査に必要となる管理者レベルのアクセスログを出力します。

サイバー攻撃をリアルタイムに検知する新開発テクノロジー

- サイバー攻撃に利用されるWindows APIが実行された際のネットワークパケットを多面的に分析することでサイバー攻撃（未知の攻撃含む）を検知します。
- ネットワーク上の挙動を分析するため、攻撃者が改ざんできません。



▼ 動作イメージ



さまざまなシーンにフィットするAdapterシリーズ

■ Adapterシリーズ製品群

Account Adapter

VA版
VMware®

認証・アカウント管理・証明書発行・DHCP
統合アプライアンス

QuOLA Adapter

VA版
VMware®

マルチOS対応
検疫アプライアンス

LOG Adapter

ソフト版

syslogを一元管理する
認証ログ管理アプライアンス＆ソフトウエア

SSO Adapter

Windows®認証とネットワーク認証
シオングルサイオンソフトウエア

自社開発でお客さまのご要望に柔軟にお応えします！

■ メーカーサポート

■ ご提案から運用までご安心いただける体制を整えております

■ 自社開発製品

- 管理者、ユーザー共に使いやすいシステムの継続開発
- お客さまの要望に応じた柔軟な開発
- ソフトウエア不具合時の迅速な改修

■ 当社Adapterシリーズ主管システムエンジニアによるご協力

- デモなどの実施
- ご提案活動
- 既存環境からの移行、設計・導入・構築の支援、各種ご相談

■ 充実した保守体制

- 当社トータルサポートセンターによる迅速なQ&A対応
- 柔軟な保守体制

マルウエア感染などにより
不正な通信を行う端末を
即時に隔離

不正通信端末 遮断ソリューション

HCNET

HC Networks, Ltd.

エイチ・シー・ネットワークス株式会社

〒111-0053 東京都台東区浅草橋1-22-16 ヒューリック浅草橋ビル4 F

お問い合わせ： https://www.hcnet.co.jp/inquiry/

Printed in Japan ‘18-04