〈製品/ハードウェア〉

不正侵入防御/ワーム感染防止システム「S@FEGUARD IP」,「WormGuard IP」シリーズ

Intrusion Prevention/Anti-Worm System “S@FEGUARD IP”, “WormGuard IP” Series

鈴木洋司* Yoji Suzuki　十文字昌夫** Masao Jumonji　飯島明夫* Akio Iijima　西　敏通* Toshimichi Nishi

要　旨

増え続けるネットワークへの新たな脅威と脆弱性，これらに即座に対応するには，従来のセキュリティ対策だけでは十分とはいえません。たとえば，従来の不正侵入検知システム（IDS）による運用では，新しい攻撃を検出できない，誤検知が多い，運用管理コストがかかるといった課題がありました。「S@FEGUARD IP」および「WormGuard IP」は，攻撃者やワームが不正アクセスの前に行う偵察行為をもとに攻撃を検知，攻撃者を確実に特定し，既知・未知を問わず不正アクセス，ワームの自動防御・抑制を行うため，従来の運用課題を解決することができます。

本稿では，「S@FEGUARD IP」,「WormGuard IP」が持つ特長および機能について説明します。

The conventional network security measures are not enough to cope with the new threat and vulnerability which continue increasing. For example, the conventional IDS (Intrusion Detection System) has the problems that it is unable to detect new attack, has much incorrect detection, and requires a large amount of management cost. “S@FEGUARD IP” and “WormGuard IP” detect attacks based on the information of reconnaissance which attackers and worms perform before attack. Since they can identify attackers and worms correctly, and block known and unknown attacks automatically, it is possible to solve the conventional management problems.

This paper describes the features and functions of “S@FEGUARD IP” and “WormGuard IP”.

1. まえがき

近年，クラッカーおよびウイルス，ワームの技術はますます高度化しています。また，その種類も多様であり，毎日のように新しい攻撃手法が生まれています。

一般的には，これらの攻撃を認識するためには，その攻撃パターンをあらかじめ保持している情報と照らし合わせる「シグネチャ分析」，あるいは異常なセッション情報から攻撃を判別する「アノマリー分析」を用いる必要があります。

これらはいずれも有効な検知方法ですが，基本的には既知の攻撃しか認識することができず，未知の攻撃に対しては無防備であるといえます。また，新しい攻撃に対応し，誤検知を軽減するためには，シグネチャ情報（攻撃パターンのデータベース）の更新・調整作業が必須であり，運用コスト増大の要因となっていました。

これに対し「S@FEGUARD IP」および「WormGuard IP」は，シグネチャ情報が不要であり，「Active Response」と呼ばれる技術を用いて，未知の攻撃に対する防御（2003年に大きな被害をもたらしたBlaster.wormについても，正しくブロックした実績があります），誤検知の排除を実現することができました。以下では，この技術を用いた製品の動作概要と機能について紹介します。

2. S@FEGUARD IPの構成と機能

2.1　S@FEGUARD IPの構成

運用の際には，ネットワークパケットをリアルタイムに監視する「S@FEGUARD IP本体」,および本体を管理し,不正アクセスの状況,ワームの感染状況をグラフィカルに表示して運用者を支援するツール「Site Manager」を使用します。

（1）S@FEGUARD IP本体

監視対象ネットワークのパケット情報をスイッチのミラーリングポート経由などで取得して，パケットの分析，およびアクセスに対する処理（攻撃の検知，ブロックなど）を行います。スパン型ネットワークをモニタするための監視用インタフェース，攻撃者に対し偽装応答を送出するための偽装応答出力用インタフェース，および「Site Manager」と接続するための管理用インタフェースを持っています。監視用インタフェースには，IPアドレスを割り振る必要がなく，ステルスモードで動作しますので，本製品が設置さ

＊ IPネットワーク事業部
IP Networks Division

＊＊ NECマグナスコミュニケーションズ 第二技術部
NEC Magnus Communications, Ltd.

れていることを外部の攻撃者に知られることはありません。なお，本体のハードウェアにはExpress5800シリーズを採用しており，標準版のIP100と，冗長化されたネットワークの監視に対応した高機能版のIP200を用意しています。

(2) Site Manager

「S@FEGUARD IP」の管理コンソール用ツールです。ユーザのPCにインストールして使用します（Windows，Solaris，Linuxに対応しています)。

「Site Manager」を用いて「S@FEGUARD IP本体」にアクセスすることにより，「S@FEGUARD IP本体」が取得した情報の解析，および設定の変更を行うことができます。なお，「Site Manager」と「S@FEGUARD IP本体」間の通信は暗号化されており，第三者への管理情報の漏えいを防ぐことができます。

「S@FEGUARD IP本体」，および「Site Manager」の一般的なネットワーク構成は，図1のようになります。

2.2 S@FEGUARD IPの機能

(1) ActiveResponse技術による攻撃の検知，防御機能

「S@FEGUARD IP」が，攻撃者からの不正アクセスを検知し，ブロックするまでの動作を，図2を用いて説明します。

1）攻撃者からの潜在的な通信を監視します。外部から入ってくるトラヒックをモニタし，攻撃者からのポートスキャンなどの偵察行為を常時監視しています。

2)「S@FEGUARD IP」が作成した偽装のIPアドレス，ポートに対してアクセスがあった場合，その通信を偵察行為とみなし，攻撃者が探している情報に類似した偽装情報を作成し，応答します。攻撃者からは，正常な通信との区別はできません。

3）偽装情報に対して攻撃者が攻撃行為を仕掛けてきた場合，「S@FEGUARD IP」は攻撃者からの通信を「ブロック対象」と認識します。以降は，攻撃者から監視対象ネットワークに対する通信は，すべてブロックされます。

なお，通信のブロックは，攻撃者もしくは監視対象の端末に対してTCPのRSTパケットを送信し，TCPセッションを切断することにより実現しています。セッションを確立しないUDP通信については，ファイアウォールと連携し，通信を遮断することができます。

(2) 管理機能

「S@FEGUARD IP」は，以下の管理機能を持っており，すべて「Site Manager」を使用して運用することができます。

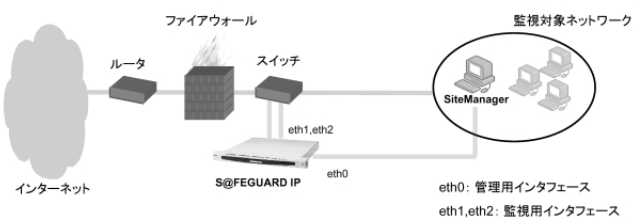


図1 一般的なネットワーク構成
Fig.1 Network components of S@FEGUARD IP solution.

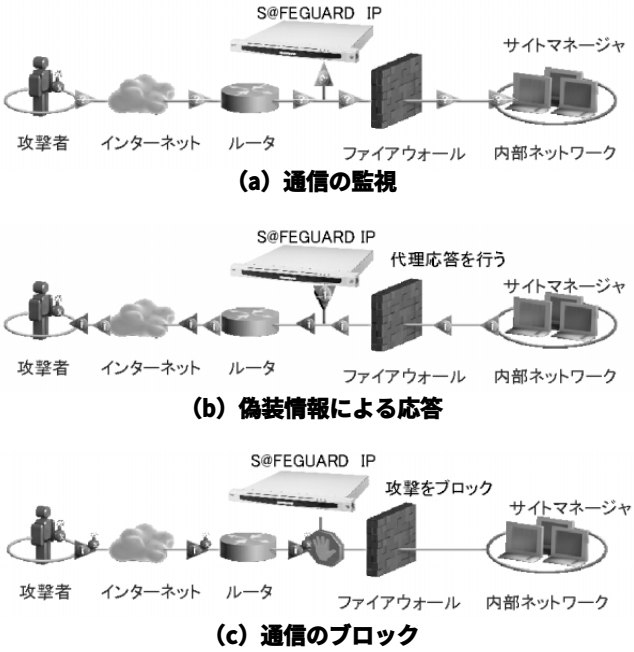


図2 ActiveResponseによる攻撃の検知，防御動作
Fig.2 ActiveResponse technology.

1）アラート表示，イベント分析，レポート出力機能

攻撃者の偵察行為，虚偽情報に対する攻撃，攻撃者からの通信のブロックなどのイベントをアラートとして画面に表示したり，運用者にE-mailで通知したりすることができます。これらのイベント情報は蓄積されており，パケット情報の解析，時系列での通信履歴，攻撃者の位置情報の表示など，様々な角度から分析を行うことも可能です。また，レポート機能も充実しており，用途や報告する相手のレベルに応じて，様々なレポートを出力することが可能です。出力形式も，PDF，HTML，およびオリジナルの形式をサポートしています。

図3に，攻撃者の位置情報，アラートを示す画面，イベント表示画面，レポート出力画面の例を示します。

2）ポリシー設定機能

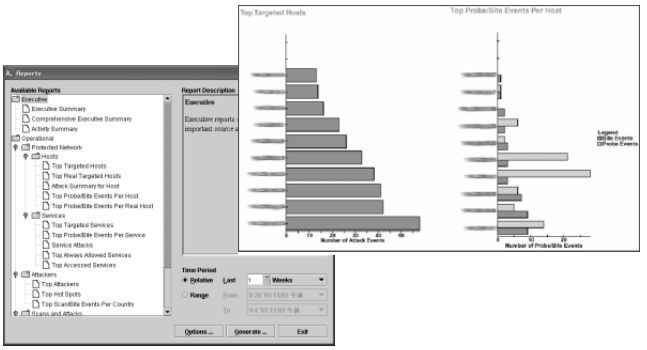
「Site Manager」から許可されたユーザが，許可された場所（IPアドレスで制御）から「S@FEGUARD IP」のあらゆる設定と操作を行うことができます。攻撃検知の条件設定はチューニング可能であり，ネットワークや外部の環境に応じて，「S@FEGUARD IP」の設定を詳細に調整することが可能です。また，「Site Manager」を使用するユーザごとに，アクセスできる機能を制限することもできます。

3. WormGuard IPの構成と機能

3.1 WormGuard IPの構成

「S@FEGUARD IP」と同様に，ネットワークパケットをリアルタイムに取得・分析・応答する「WormGuard IP」本体，また本体を管理し不正アクセスの状況，ワームの感染状況を表示して運用者を支援するツール，「WormScout

（a）位置情報，アラート表示，イベント表示画面例



（b）レポート出力画面例

図3　Site Managerの画面例
Fig.3　Screen shots of Site Manager.

Console」から構成されます。

（1）WormGuard IP本体

監視対象ネットワークの双方向パケット情報をスイッチのミラーリングポート経由などで取得して，パケットの分析，およびアクセスに対する処理（攻撃の検知，ブロックなど）を行います。スパン型ネットワークをモニタするための監視用インタフェース，攻撃者に対し偽装応答を送出するための偽装応答出力用インタフェース，および「WormScout Console」と接続するための管理用インタフェースを持っています。本体のハードウェアにはExpress5800シリーズを採用しており，標準版のIP100と，設置するネットワークの冗長化に対応しハードディスクや電源も冗長化した高機能版のIP200を用意しています。

（2）WormScout Console

「WormGuard IP」の管理コンソール用ツールです。お客様のPCなどにインストールして使用します（Windows，Solaris，Linuxに対応しています）。

「WormScout Console」を用いて「WormGuard IP」本体が取得した情報の表示・解析，および設定の変更を行うことができます。

「WormGuard IP」本体，および「WormScout Console」の一般的なネットワーク構成は，図4のようになります。

3.2　WormGuard IPの機能

ActiveResponse技術による攻撃の検知，防御機能など

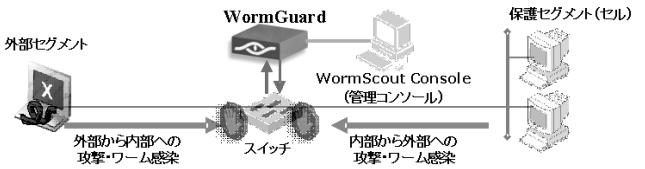


図4　一般的なネットワーク構成
Fig.4　Network components of WormGuard IP solution.

「WormGuard IP」も「S@FEGUARD IP」と同じ技術を用いています。ここでは「WormGuard IP」固有の機能・技術について説明します。

（1）ポートブロック機能

感染元IPアドレスからの通信をすべて遮断（ソースブロック）するのではなく，攻撃に利用しているポートのみブロックし，業務への影響を最小限にすることができます。また設定により一定回数のポートブロック後にソースブロックに移行させることも可能です。

（2）Worm Slowdown技術

偽装情報へのアクセスを保持し，感染端末からの通信がすぐに次のターゲットに移らないようにすることで，ワーム感染スピードを抑制する機能です。実際にはWindowサイズ0のパケットを用いてコネクションを維持することでネットワークへの負荷も最小としています。

（3）Management Serverによる運用

複数台設置された「WormGuard IP」をManagement Server（攻撃情報集約DB）経由で接続することで，複数の「WormGuard IP」間の連携，および集中管理を行うことができます。管理コンソールには，「Enterprise Manager」を使用します。

1）Enterprise Lockdown機能

「Management Server」で管理されているすべての「WormGuard IP」でワーム感染端末の情報を共有することができます（図5：Enterprise Lockdown機能）。

ある「WormGuard IP」で検知した感染端末情報をEnterprise Lockdownとして「Management Server」へ通

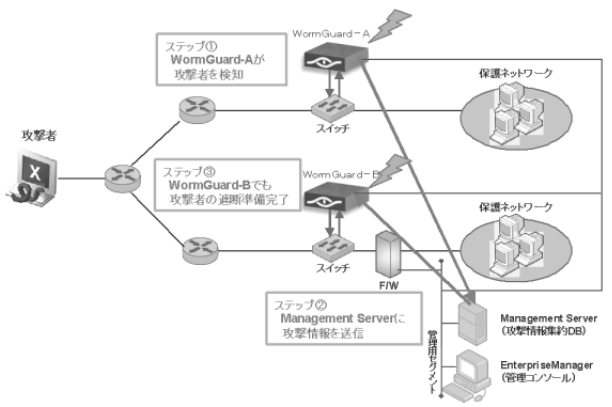


図5　Enterprise Lockdown機能
Fig.5　Enterprise Lockdown feature.

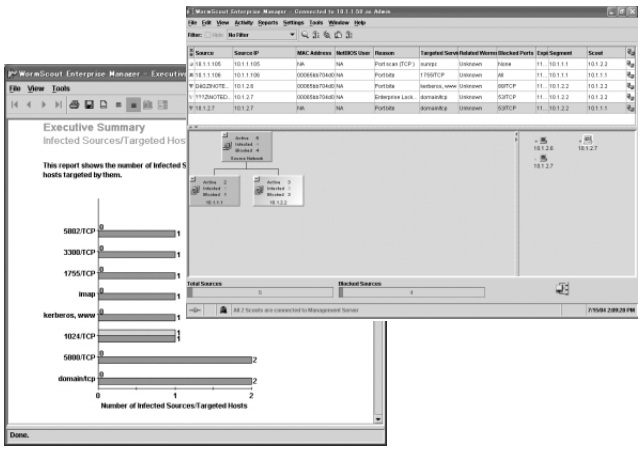


図6　イベント，レポート画面例
Fig.6　Screen shots of Enterprise Manager.

知します（ステップ①）。「Management Server」は他の「WormGuard IP」に攻撃情報を送信し（ステップ②）情報共有することで，他の「WormGuard IP」でも当該感染端末からの通信遮断準備をします（ステップ③）。その後攻撃を検知すると，偽装情報へのアクセスを待つことなく瞬時に感染を阻止することが可能となります。

2）複数「WormGuard IP」の集中管理

「Enterprise Manager」から複数の「WormGuard IP」を一元管理することが可能です。管理者は1台のコンソールから複数の「WormGuard IP」を設定することができます。

また各「WormGuard IP」が検出したイベント情報を「Management Server」が集約することで，攻撃者やワーム感染端末の特定を集中的に行うことが可能で，様々なレポートも各「WormGuard IP」からの情報をもとに作成されます（図6：イベント，レポート画面例）。

4. S@FEGUARD，WormGuardの組合せ構成

図7に示すように，「S@FEGUARD IP」と「WormGuard IP」を組み合わせることにより，VPN/RAS，モバイルユーザ経由による内部不正アクセス，ワーム感染対策（WormGuard），インターネットからの不正アクセス対策（S@FEGUARD IP）を実現することができ，隅々まで行き届いた不正アクセス対策ソリューションを提供することが可能です。

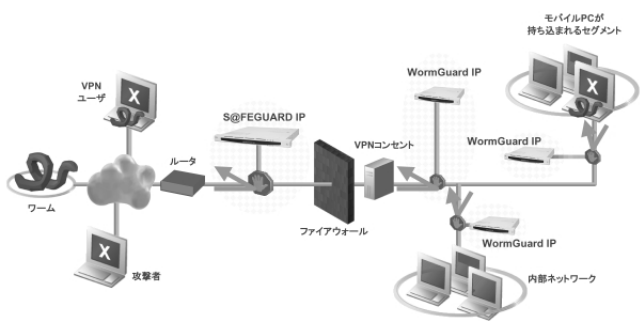


図7　組合せ構成
Fig.7　Network components including S@FEGUARD and WormGuard.

5. むすび

ネットワークのブロードバンド化，ユビキタス化が進むにつれて，ネットワークに対する新たな脅威と脆弱性はますます増えていくものと予想されます。そのような環境のなかで，既知・未知を問わず不正アクセス，ワームの自動防御・抑制を行うことが可能な「S@FEGUARD IP」および「WormGuard IP」は，お客様に対してより安全なネットワークの構築，運用コストの削減といった効果をもたらすものと期待されます。

今後は，他のセキュリティ製品との連携性を高め，お客様にとって最適なセキュリティソリューションを提供することができるよう，製品開発を進めていく所存です。

＊「Active Response」技術は，ForeScout Technologies社の特許技術です。
＊その他本稿に記載した会社名，製品名は，各社の商標または登録商標です。

筆者紹介

Yoji Suzuki
鈴木　洋司（すずき　ようじ）　2003年，NEC入社。現在，ブロードバンドネットワーク事業本部IPネットワーク事業部勤務。

Masao Jumonji
十文字昌夫（じゅうもんじまさお）　1986年，NEC入社。現在，NECマグナスコミュニケーションズ 第二技術部エキスパート。

Akio Iijima
飯島　明夫（いいじま　あきお）　1983年，NEC入社。現在，ブロードバンドネットワーク事業本部IPネットワーク事業部グループマネージャー。電子情報通信学会会員。

Toshimichi Nishi
西　敏通（にし　としみち）　1990年，NEC入社。現在，ブロードバンドネットワーク事業本部IPネットワーク事業部エキスパート。