情報セキュリティ大学院大学殿 セグメント・プロテクタ導入事例

鈴木　友泰　　濱田　恒生
濱　隆二

近年，ネットワークによりさまざまな情報サービスが提供され，ITの利便性と自由度が高まる一方で，そのITの社会基盤を脅かす不正な攻撃は後を絶たない。その攻撃の形態は，単一のコンピュータから不正な攻撃を仕掛けるプログラムがネットワークを経由して増殖するものから，複数のコンピュータから一斉に組織的な攻撃を仕掛けるものまでさまざまである。前者はワームと呼ばれるウィルスである。後者はワームより攻撃が高度化したボットネットと呼ばれるウィルスであり，現在その被害は急増している。いずれもネットワークの特性を悪用するウィルスの一種であり，その対策は，各方面で研究されている。

情報セキュリティ大学院大学殿は，2004年に，沖電気工業株式会社（以下，沖電気）からの委託により，沖テクノクリエーションが開発したワーム対策ソリューション「セグメント・プロテクタ」を学内ネットワークに設置し，イントラネットワークのセキュリティ強化の研究を実施した。

本稿では，セグメント・プロテクタを導入した背景，システムの概要，システムの特長，システムの機能，導入の効果を紹介する。

導入の背景

情報セキュリティ大学院大学殿は，2004年に情報セキュリティを専門の分野として横浜市に開学した大学院である。ITの利便性と自由度を維持しつつ，安全・安心の社会基盤を構築するという理念で，セキュリティに関する技術研究と管理・運営，情報システム監査，情報法制，社会制度，情報モラルなどの体系化と人材育成を実施している。

沖テクノクリエーションは，ワームの感染拡大を未然に防止するワーム対策ソリューション「セグメント・プロテクタ」を開発した。既存種，新種に関わらず，ワームの自己増殖活動（ワームがネットワーク上の感染対象を見つけ出すためのトラフィックの挙動）を検出し，感染端末のトラフィックを隔離することで，感染拡大を防止することができる。

セキュリティ分野を専門に研究する情報セキュリティ大学院大学殿は，ワーム対策のツールとして，セグメント・プロテクタの有効性を評価し，ワームなどの不正アクセスを研究するために，沖電気からの委託研究を実施した。そのために，セグメント・プロテクタを大学内に設置した。

システムの概要

セグメント･プロテクタは，ワームの感染拡大を未然に防止するワーム対策ソリューションである。既存種，新種に関わらず，ワームの自己増殖活動を検出し，感染端末のトラフィックを隔離することで，感染拡大を防止することができる。

セグメント･プロテクタは，4種類のコンポーネントで構成し，各コンポーネントを相互に連携することで，ワームに感染した端末のトラフィック（ワーム･トラフィック）を隔離する。**図1**にシステムの構成を示す。

●Engine（専用ハードウェア）

透過的にイーサネット・フレームを転送する専用ハードウェアである。イントラネットワークの既存VLANあるいはポートVLANに所属する各部門間あるいは各フロア間に仮想的な防壁を作成できる。この仮想的な防壁をプロテクションセグメントと呼ぶ。プロテクションセグメントは，最大64個を作成でき，そのうちの1つを隔離セグメントとして設定する。隔離セグメントに転送するワーム・トラフィックを廃棄することで，ワームに感染した端末の隔離を実現する。

●Manager（PCサーバ）

最大10台のEngineを管理するソフトウェアである。管理者は，Web画面を操作することで，ワーム検出状態やモニタグラフによる統計情報の監視を実行する。

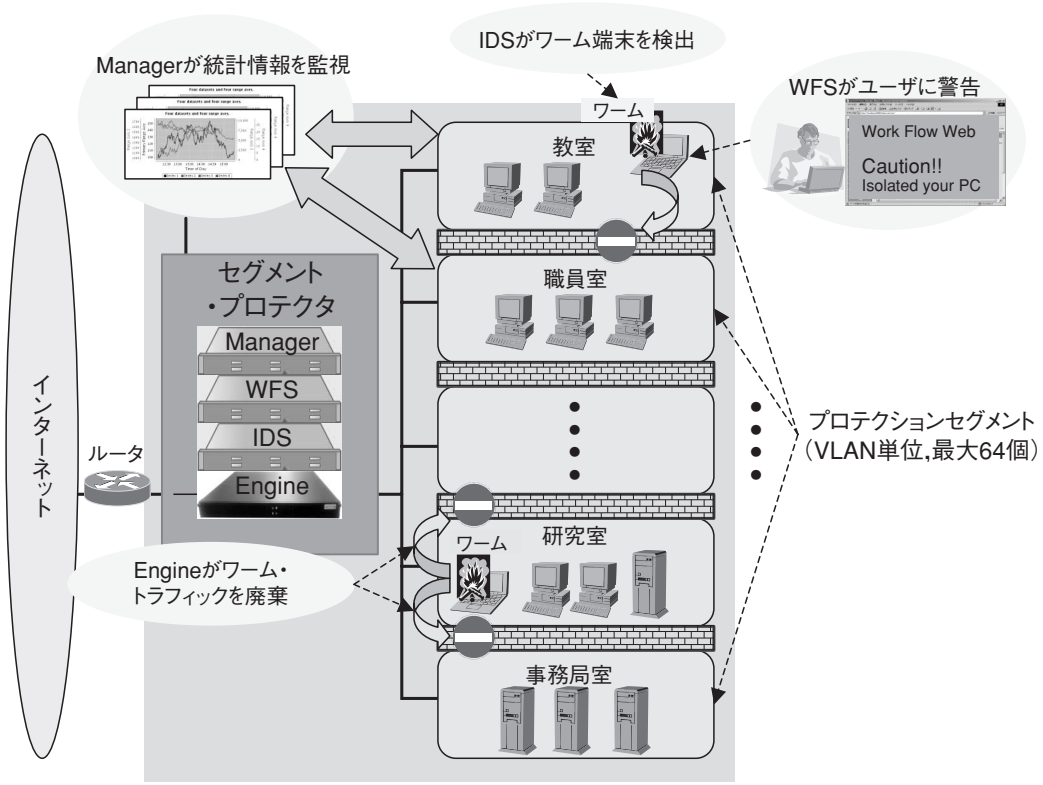

図1　システム構成

●IDS：Intrusion Detection System（PCサーバ）

Engineから複製されたトラフィックを受信し，その挙動を解析することで，ワームの自己増殖活動を検出する。

●WFS：Work Flow Server（PCサーバ）

隔離された端末を利用するユーザーへ感染を通知するために，警告Web画面を強制的に表示する。

システムの特長

セグメント・プロテクタは，大きく3つの特長を持つ。

（1）ワーム感染拡大を防止

ユーザーのうっかりミスで，ワームに感染した端末が学内に持ち込まれ感染が拡大するなど，ウィルス対策ソフトの導入だけではワームの自己増殖活動を完全に防止することができない。これは，ウィルス対策ソフトが，基本的にパターンマッチングを用いた仕組みによりワーム感染を検出するため，新種のワームには，パターンが更新されるまで，無力であることに起因する。

セグメント･プロテクタは，既存種，新種に関わらずワームの自己増殖活動を検出し，感染端末のトラフィックを自動的に隔離する。さらに，**図1**に示すように，学内ネットワークの既存VLANあるいはポートVLANに対応づけて，各フロア間に仮想的な防壁を作り出し，感染した端末が存在するフロアから，他のフロアへの感染拡大を防止することができる。

（2）導入が容易

一般に，新しいネットワーク・セキュリティ製品を導入するためには，既存ネットワークのコンフィグレーションの変更や端末に専用の対策ソフトウェアをインストールする必要があり，導入に手間がかかってしまう。

セグメント･プロテクタは，端末に専用の対策ソフトウェアをインストールする必要がなく，防衛するネットワークへ専用ハードウェア（Engine）とPCサーバ（Manager，IDS，WFS）を接続するだけで利用できる。また，既存のネットワークトポロジやセキュリティポリシーを変更することなく，容易に既存のネットワークに設置できる。さらに，最小構成でも1,000台以上の端末を監視することができ，端末1台当りの導入コストを劇的に低減できる。

(3) 効率よくトラフィックを転送

DoS攻撃や不正アクセスなどの異常トラフィックにより，業務のトラフィックが悪影響を受ける場合がある。また，ブリッジ型のネットワーク・セキュリティ製品の導入は，ネットワークの転送能力を劣化させ，ネットミーティング中に音声が途切れるなど，アプリケーションの運用の障害になることがある。

セグメント･プロテクタは，QoS制御機能を搭載しており，プロテクションセグメントで分割した部門あるいはフロアごとの利用帯域や特定アプリケーションごとのQoSを制御できるために，リアルタイム性の高い音声や映像トラフィックを劣化させることなく，スムーズに転送できる。

システムの機能

セグメント・プロテクタの機能のうち，情報セキュリティ大学院大学殿で主に利用した，ワーム感染端末の検出・隔離を実施するための検疫機能と，トラフィックの収集・評価を実施するためのトラフィック分析機能を紹介する。

(1) 検疫機能

図2にセグメント・プロテクタの4要素（Engine，Manager，IDS，WFS）が連携し，感染端末を隔離する動作の概要を示す。

① IDSでワームの自己増殖活動を検出
② Managerにワーム検出を通知
③ Managerは，感染端末の隔離を指示し，Engineが感染端末を隔離セグメントへ移転
④ ユーザーが感染端末のブラウザを起動，WFSは警告Web画面を送信し，ブラウザに表示
⑤ ユーザーは，WFSに配備したワーム除去ソフトウェアや，許可された特定サーバへアクセスし，復旧作業を実施

以上の動作によりワームの感染拡大を最小限に防止することができる。

(2) トラフィック分析機能

図3にトラフィック分析機能の概要を示す。トラフィック分析機能は，レポートによるトラフィック分析と，Snort*1) によるトラフィック分析の大きく2通りがある。

① レポートによるトラフィック分析

レポートは，Engineから定期的に収集し蓄積したパケット統計情報に基づき，時間・日・週・月を単位とし

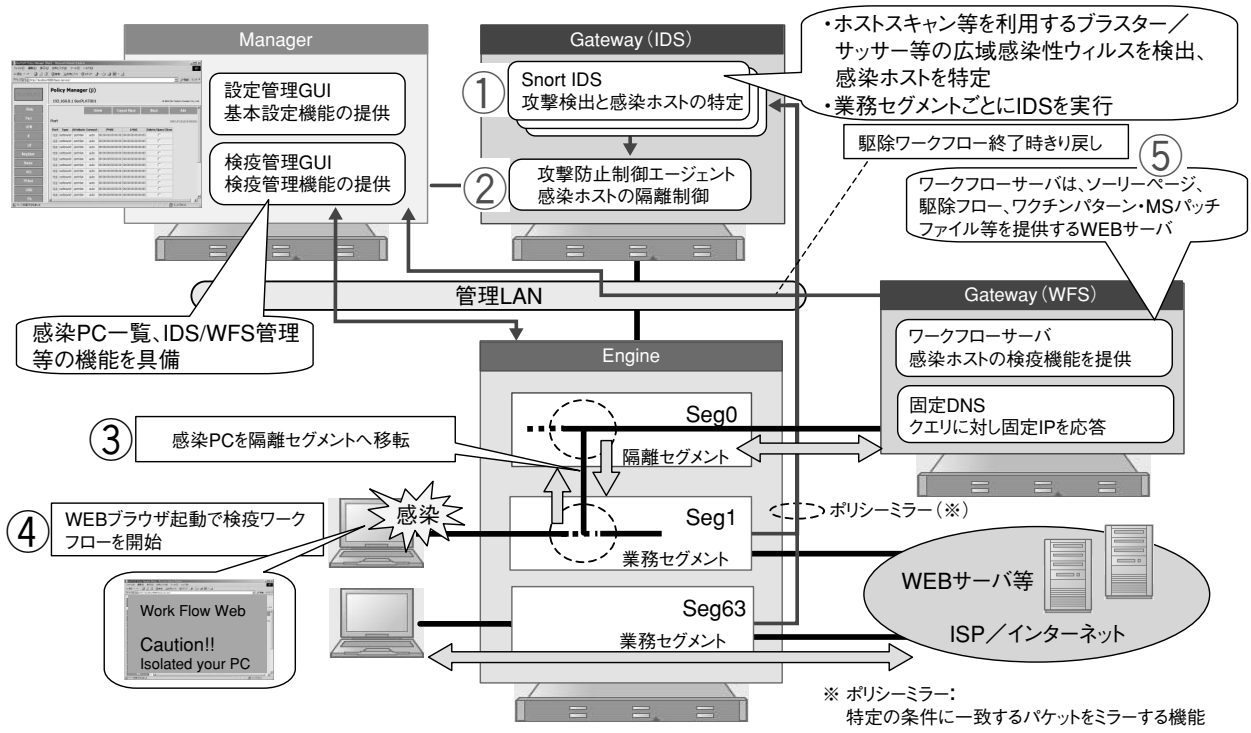

図2　検疫機能（動作概要）

*1)Snortとは，米国のMartin Roesch氏によって開発されたフリーのIDS(Intrusion Detection System：侵入検知システム)ソフトウェア。

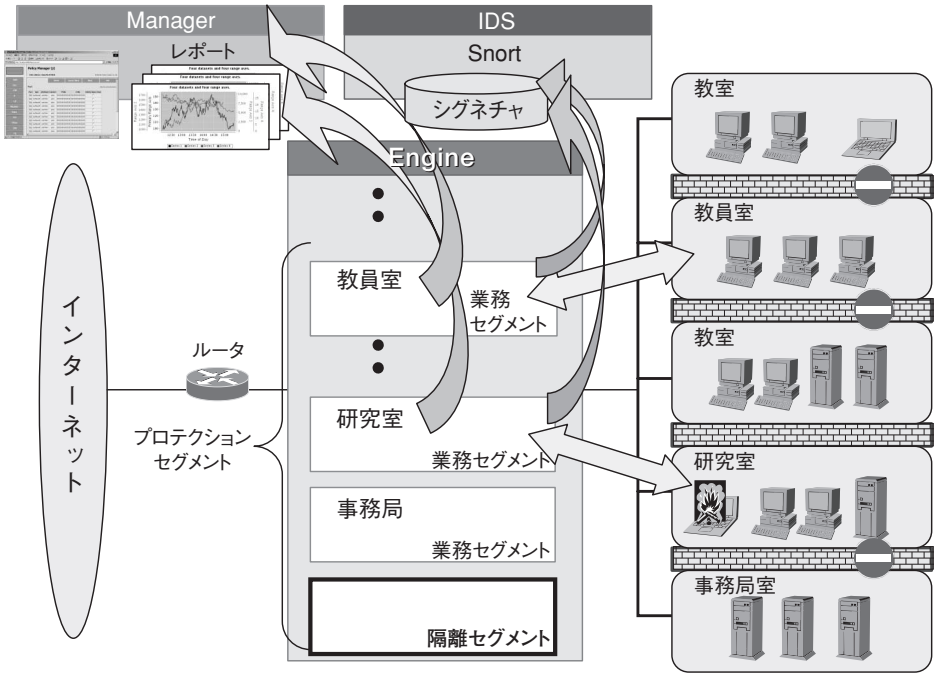

図3　トラフィック分析機能

て，トラフィックの状況をグラフィカルに表示し，通知する機能である。管理者は，Webブラウザまたはメールに添付したPDFファイルを見ることでトラフィックの異常を分析できる。

② Snortによるトラフィック分析

IDSは，不正アクセスを監視するためのソフトウェアとしてSnortを搭載する。このSnortのシグネチャ*2) を操作し，ログを分析することで学内ネットワークの不正トラフィックの状態を的確に分析できる。

導入の効果

セグメント・プロテクタを情報セキュリティ大学院大学殿に導入することで，大きく3つの効果を得た。

- 実網で，ワームがネットワークを経由して感染を拡大させるときの予兆となるホストスキャン動作をセグメント・プロテクタが検知できることを確認した。
- 研究で収集したトラフィックの情報を，セキュリティポリシーの策定に活用できた。
- ユーザーアクセス権と統合されたセグメント管理によるネットワークのユーザービリティの向上と，イントラネットのセキュリティ強化に有効であることを確認した。

あ と が き

2005年度，情報セキュリティ大学院大学殿と沖電気は，不正アクセスの検知手法の共同研究を実施している。セグメント・プロテクタは，同研究のために，継続して学内ネットワークで利用される。 ◆◆

■参考文献

1）鈴木友泰，吉田守男，濱田恒生，青木裕樹：セキュリティ・アプライアンス・プラットフォーム，沖テクニカルレビュー202号，Vol.72 No.2，pp.50–55，2005年
2）濱田恒生，鈴木友泰，芝修吾，濱隆二：ネットワーク・セキュリティ・ソリューション，沖テクニカルレビュー205号，Vol.73 No.1，pp.26–31，2006年
3）宗吉隆行，小柳和子（情報セキュリティ大学院大），相場信夫（沖電気）：ユーザアクセス権と統合されたセグメント管理によるネットワークのユーザビリティの向上，電子情報通信学会2005ソサイエティ大会，B-6-49

●筆者紹介

鈴木友泰：Tomoyasu Suzuki. 株式会社沖テクノクリエーション システム開発部
濱田恒生：Tsuneo Hamada. 株式会社沖テクノクリエーション システム開発部
濱隆二：Ryuji Hama. 株式会社沖テクノクリエーション システム開発部

*2) シグネチャとは，IDSが不正アクセスのパターンを判別するためのデータの集合体であり，その多くはデータベースの形態をとる。