異常トラフィック監視システム

～ ワーム／ボット型ウィルスの被害拡散防止を目指し ～

土屋　和英　　八木　勇
三浦　卓彦　　宮崎　衛

映像・音声・データを融合したトリプルプレーサービスの導入などネットワークを取り巻く環境は大きく変化し，よりネットワークの重要性が増している。一方で，ネットワークを悪用したセキュリティ事件も続発しており，ネットワークセキュリティの取り組みが不可欠となってきている。

ネットワークセキュリティを確保するうえでFirewallやIDS（侵入検知システム）だけでは不十分であり，特に企業や組織の内部ネットワークにおいては，内部LANの回線／機器に悪影響を与える異常トラフィックの監視が必要である。

本稿では，当社が開発した異常トラフィック監視システムSecure Traffic Probe™*1) の機能や効果について紹介する。あわせて情報漏えい対策システムCWAT®*2) やネットワークの遮断・帯域制御装置SecApPlat™*3) と連携した内部リスク対策ソリューションについて紹介する。

より重要性が増すネットワーク

近年，VoIPの導入やWebを利用したビジネスモデルの普及，モバイルやRAS接続を活用したワークスタイルの定着等ネットワークは高度化・複雑化し，社会基盤としての重要性が高まっている。従来のネットワークは基幹系や情報系など，それぞれに専用のネットワークが敷設され，接続範囲も限定されていた。しかし，現在のネットワークではLAN/WAN接続やVoIP等の通信データの乗り入れ等ネットワークの規模や利用方法が大きく変化している。また，ネットワーク設計当初では想定していなかったさまざまなアプリケーション（P2PソフトやChatソフト）の出現により，IPネットワーク網に通信トラフィックが集中し，障害発生時の原因切分けがより複雑となっている。一方で，ネットワークの停止は即大きな営業損失となってしまう。このように，企業や組織はより重要性の高まるネットワークを安定的に運用することが求められている。

後を絶たないウィルスによる被害の現状

ネットワークを安定的に運用する上で，情報セキュリティは大きな課題となる。ここでは，情報セキュリティの各種脅威の中からネットワークに深刻なダメージを与えるワーム／ボット型ウィルスの被害の現状について紹介する。

ワーム／ボット型ウィルスの被害としては，2003年1月のSQLスラマーウィルスによる韓国でのインターネット接続障害や2003年8月のMSブラスタの大流行などが挙げられる。これらのウィルスはネットワークに過負荷をかけ，サービスを停止（サービス妨害攻撃）するウィルスであった。さらに最近ではP2PソフトのWinnyを悪用したワーム型ウィルスによる情報漏えいやトロイの木馬型ウィルスを利用した大手カード会社からの情報漏えい事件など，情報漏えいを目的としたウィルスによる被害が増えている。以下の事件はウィルス感染に起因する情報漏えい事件と考えられている。

【ウィルス感染に起因する事件例】

- 2004年3月　ウィルス感染した私用PCから捜査書類が漏えい
- 2005年4月　ウィルス感染端末から発電所検査情報が漏えい
- 2005年6月　ウィルス感染端末から小学生の児童名簿が漏えい
- 2005年6月　不正プログラム使用によりクレジットカード情報が漏えい

TIPS【ボット型ウィルス】

情報資産の破壊／悪用を目的とした悪質なプログラムで，外部からの命令（操作）に従って破壊活動を行うウィルス。従来はトロイの木馬型ウィルスに分類されていたが，2002年の初観測以降，年々脅威が増しており，昨年は1万台以上の感染が確認された。攻撃者はボットウィルスに感染したパソコンを外部から操作することができ，ウィルスに感染した被害者が加害者となってしまう危険性がある。

ウィルスへの対応としては，利用者の教育とアンチウィルスシステムやFirewall･IDSの導入が有効であると考えられていた。現在，国内団体のアンチウィルスシステム導入率はほぼ100%といわれている。Firewallの導入率も50%を超え，既に必要最低限の対策は実施されているものと考えられる。しかし，ウィルス感染に起因するセキュリティ事件（事案とも言う）は後を絶たず，ワーム／ボット型ウィルスによる大きな事件の報道も多い。これはアンチウィルスシステムやFirewallを導入したとしても，パターンファイルの更新漏れやFirewallの設定不備等でウィルスに感染する危険性が残っており，前記の対策だけでは完全にウィルス被害を防ぐことができないことを示している。

ネットワーク管理者の課題

ネットワーク管理者は，重要性が高まるネットワークをさまざまな脅威から守り，安定的に運用することが求められ，その責任と職務範囲はより大きなものとなっている。ネットワークを適切に管理するために，現在のネットワークの状態を正確に把握し，適正に利用されていることを監視する必要がある。また，ネットワーク帯域を圧迫するトラフィックやネットワーク機器に悪影響を及ぼす異常を検知・抑制する必要もある。

一方，通信トラフィックは日々変化し，IP網に通信トラフィックが集中する現在のネットワークにおいては，ネットワークの状況を正確に把握することさえ難しい状況である。さらに，日々新しいウィルスが発生しており，その原因の特定や対処方法が複雑化している。ワーム型ウィルスが網内に侵入すると，たった一台の感染端末によってネットワーク全体が数時間に渡りダウンし，莫大な復旧コストが必要となるケースもある。最近では，ワーム／ボット型ウィルスによる情報漏えい事件も続出しており，顧客情報を漏えいした企業や組織は損害賠償だけでなく，社会的な信用失墜を招く事態となっている。

ネットワーク管理者にとって，ネットワークの帯域や機器に悪影響を与えるトラフィックやウィルス感染端末のトラフィックといった異常なトラフィックへの監視と対応が不可欠となってきている。

Secure Traffic Probe™の概要

Secure Traffic Probe™は沖電気独自のネットワークトラフィック分析技術を活用したセキュリティシステムであり，2004年11月から販売を行っている。Secure Traffic Probe™は既存ネットワークに接続するだけで，日本語による簡易な操作でワーム対策とトラフィック監視が可能な商品である。現在Ver2.0がリリースされ，CWAT®やSecApPlat™との連携や取得情報の拡充，操作性の向上等，ネットワーク管理者の実務に合わせた，負荷軽減の機能が拡張されている。

Secure Traffic Probe™はトラフィックを観測するプローブ装置と管理・表示を行うマネージャ装置から構成され，ネットワーク管理者は自身の端末からブラウザで容易に操作・設定を行うことができる。プローブ装置は100Mbit/sまでを監視するスタンダードモデルと1Gbit/sの高速回線を監視するハイエンドモデルをラインナップしている。また，1台のマネージャ装置で最大8台までのプローブ装置を管理することができる。Secure Traffic Probe™の構成と画面イメージを**図1**に示す。

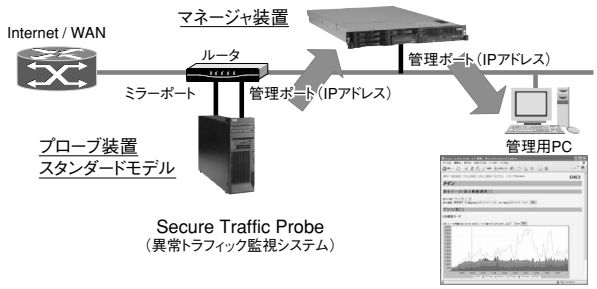

図1　Secure Traffic Probe™の構成と画面

Secure Traffic Probe™の機能

Secure Traffic Probe™の特長的な機能を3つ紹介する。

（1）アプリケーション別のトラフィック計測機能

Secure Traffic Probe™は既存ネットワークの構成に変更を加えることなくアダプティブに設置することができ，ユーザのネットワークの利用状況をアプリケーション別に把握することができる。このとき利用状況の画面に表示するアプリケーションはXMLで定義することができる。マネージャ装置を設置することにより，遠隔地や複数サイトのネットワーク利用状況をリモートから一元的かつリアルタイムに監視することも可能である。

（2）異常トラフィック検出機能

Secure Traffic Probe™はネットワーク資源に著しい負荷を与えるトラフィックとワーム型ウィルスの感染活動の2種類の異常なトラフィックを検出することが可能である。次に説明するアクション機能を用いることで，異常の検出と同時に，ネットワーク感染型ワームの拡散を防止することができる。

ワーム型ウィルスの感染活動の検知はウィルスパターンを利用しない沖電気独自のトラフィック分析技術を用いているため，既存のアンチウィルスシステムと異なり，パターンファイルの更新が不要で，未知のワーム型ウィルスにも有効である。

Secure Traffic Probe™は異常を検出すると，その内容をデータベースに格納するとともに，分析に必要なトラフィック情報を取得する。Secure Traffic Probe™ Ver2.0では，検知した異常を一覧で確認することができ，分析に必要なトラフィック情報を効率的に保存するスナップショット機能も有している。

(3) アクション機能

Secure Traffic Probe™は異常を検知すると，メール通知，SNMP TRAP，特定コマンド実行，外部システム連携等のアクションを行うことができる。連携可能な外部システムとしてはCWAT®を始め，SecApPlat™やルータがある。このアクション機能により対処や通知を自動で行うことができる。そのため，ネットワーク管理者は常時モニタを監視する必要がなく，管理者の負荷を軽減することができる。

この他にVLAN単位での監視機能や蓄積したデータをファイル出力するExport機能，他の機材で観測したデータを本装置で利用するためのImport機能なども有している。

Secure Traffic Probe™の効果

Secure Traffic Probe™導入の効果を紹介する。

Secure Traffic Probe™はネットワークトラフィック分析技術を用いてワーム型ウィルスの感染活動を検知している。そのため，従来のワーム対策では防ぎきれないワーム型ウィルスにも対処できる。パターンファイルの配布が間に合わないワーム型ウィルスや，持ち出したノートPC等ワクチンの更新漏れPCの対策として有効である。また，ネットワーク負荷や利用状況を表示する機能を活用することで，ネットワーク資源の有効利用とネットワークコストの適正化が図れる。

Secure Traffic Probe™ / CWAT®/SecApPlat™連携

Secure Traffic Probe™を中核に，CWAT®やSecApPlat™と連携を図り，異常トラフィック監視に基づく内部リスク対策ソリューションを展開している。本ソリューションは企業や組織の内部ネットワークをネットワークレイヤとシステムレイヤから保護し，ワーム感染被害や情報漏えいを抑止・予防する。Secure Traffic Probe™/CWAT®/SecApPlat™連携時の動作概要を**図2**に示す。異常トラフィックの検知からLANの遮断までは，検知内容によって，

① CWAT OPDCを活用した端末のシャットダウンやメール送信の停止等の端末への対処

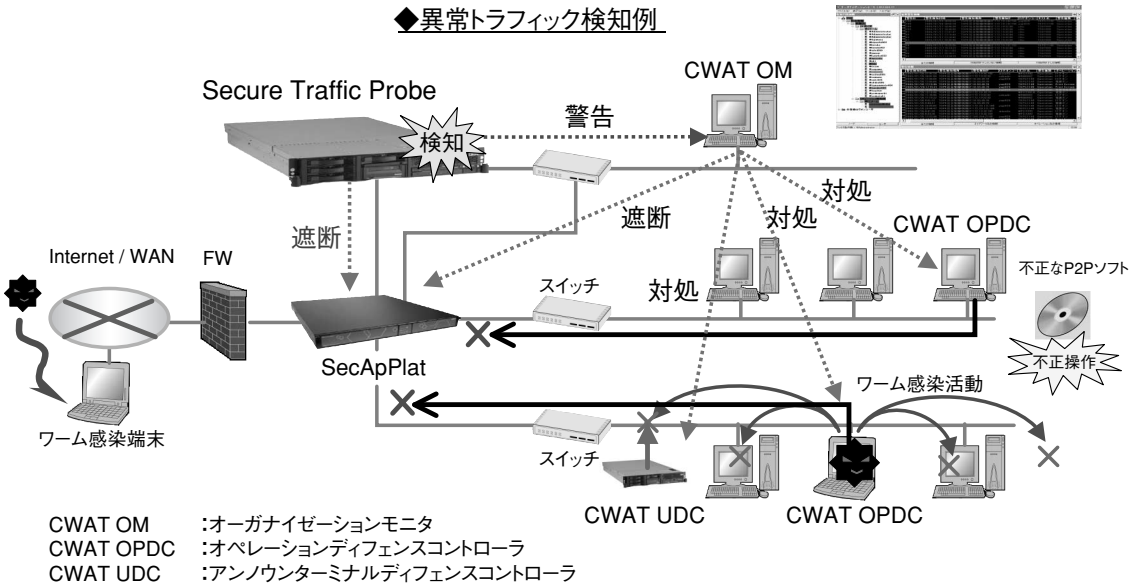

図2 Secure Traffic Probe™/CWAT®/SecApPlat™連携時の動作概要

② CWAT UDCを活用したワーム感染端末の通信遮断
③ SecApPlat™を活用したワーム感染端末の外部／他セグメントへの通信遮断
などのセキュリティポリシーを適用することが可能である。

Secure Traffic Probe™の導入活用事例

Secure Traffic Probe™の導入事例とその効果について紹介する。本事例では数千台のパソコン・サーバが設置されている事業所のWAN接続点にSecure Traffic Probe™を設置し，約9ヶ月に渡り異常トラフィックの監視を行った。その際，2つの効果を確認することができた。

(1) ワーム型ウィルス検知

パッチ未適用のサーバ機がワーム型ウィルスに感染し，大量の通信トラフィックを発生させ，事業所のネットワークがダウンする事象が発生した。この時，Secure Traffic Probe™はウィルス感染端末からの異常な通信を検知し，ネットワーク管理者にアラートを発した。通知を受けたネットワーク管理者はアラート内に記録された端末情報から対処を行った。これは，本製品により早急な対処とそれによる営業損失の低減・復旧コストの削減が図れた事例である。本事例のトラフィック状況を**図3**に示す。特定のアプリケーションのトラフィックのみでネットワーク帯域が占有されていることが確認できる。

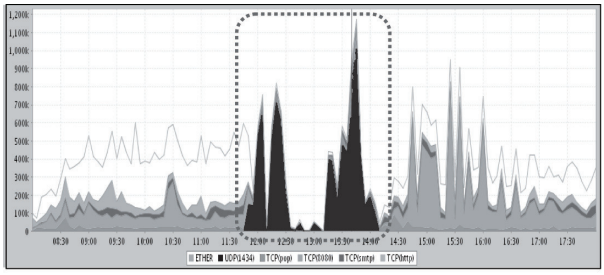

図3　ワーム型ウィルス検知時のトラフィック状況

(2) 不正トラフィックの監視

利用者の一人が自身の作業用PCに暗号化ソフトをインストールし，外部のネットワークとデータ通信を実施し，ネットワーク資源を不正に消費している事象が発生した。Secure Traffic Probe™はネットワーク帯域のしきい値を超える通信を検知し，ネットワーク管理者にアラートを発した。これは，本製品により帯域占有端末と不正なアプリケーションの通信を確認できた事例である。帯域占有端末検知時のトラフィック状況を**図4**に示す。特定のアプリケーションのトラフィックが急激に増加していることが確認できる。

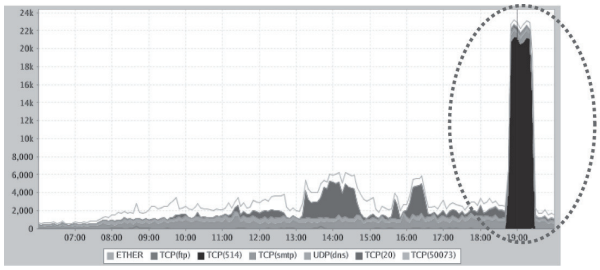

図4　帯域占有端末検知時のトラフィック状況

ま と め

Secure Traffic Probe™は既存ネットワークに接続するだけで，日本語による簡易な操作でワーム対策とトラフィック監視が可能な製品である。今後は分析機能の強化や運用管理系機能の拡充を行い，ネットワーク管理者の課題解決により有効な製品へと機能を拡張する予定である。本製品の開発・提供を通じ，ネットワークソリューションの沖電気として，安心・安全なe社会®の構築と社会の発展に寄与したいと考える。 ◆◆

●筆者紹介

土屋和英：Kazuhide Tsuchiya. システムソリューションカンパニー 社会情報ソリューション本部 SE第一部 第四チーム
八木勇：Isamu Yagi. システムソリューションカンパニー 社会情報ソリューション本部 SE第一部 第四チーム チームマネージャ
三浦卓彦：Takuhiko Miura. システムソリューションカンパニー 社会情報ソリューション本部 SE第一部 第四チーム
宮崎衛：Mamoru Miyazaki. システムソリューションカンパニー 社会情報ソリューション本部 SE第一部 第四チーム