情報発信型ネットワーク・フォレンジックシステム「DynamicMSIESER」の紹介

Network Forensics System, DynamicMSIESER

山内 直*
Naoki Yamauchi

DynamicMSIESERは、いつ、誰が、どのような情報をネットワーク経由で通信したかの監査証跡（パケットデータ）を記録し、情報セキュリティ事故の原因を迅速に調査・追及できる、ネットワーク・フォレンジック製品である。ただ証跡を記録するだけでなく、ネットワーク経由での情報漏えいをいち早く検知し、通知する。これが「情報発信型ネットワーク・フォレンジックシステム」と冠する所以である。

DynamicMSIESER is a network forensics product that can record what information who when communicated by way of the network as an audit trail (packet data), and investigates and pursue the cause of the security incident promptly. However, evidence not only is recorded but also the information leakage by way of the network is promptly detected, and it notifies. This is a reason for the name of "Dynamic".

1. まえがき

刑事事件や交通事故が発生した際、事後の原因調査に役立つのは、「監視カメラ」であり、「ドライブレコーダ」である。これらの記録装置の必要性は社会的に十分認識されている。情報セキュリティ事故についても同様に、原因を調査するためには証跡データを記録しておくことが重要である。このような考え方を「フォレンジック」と言う。「標的型攻撃」に代表されるように、最近のサイバー攻撃は非常に多様化している。もちろん、情報漏えいに対する入口・出口対策は必要であるが、100％防止することは出来ない。そこで、情報漏えいが発生した事後対策としてのフォレンジックシステムの重要性が高まっている。

2. 「DynamicMSIESER」とは

「DynamicMSIESER」は、パケットキャプチャ方式のネットワーク・フォレンジックシステムである。LAN上を流れる全ての通信（パケット）データを取得し、記録する、言わば「ネットワーク監視カメラ」と言える。しかし、監視カメラとは異なり、生のパケットデータはそのままではどのような通信内容なのか確認することは出来ない。DynamicMSIESERは、パケットデータをリアルタイムで解析し、通信内容を復元する。復元された通信データは、各プロトコル（HTTP・SMTP・POP3・FTP）ごとにインデックス化され、容易に検索、閲覧することができる。

次に、DynamicMSIESERの特長について述べる。

2.1 簡単導入・簡単運用

DynamicMSIESERは、パケットキャプチャ方式のネットワーク・フォレンジック装置であるため、顧客の社内ネットワーク構成を変更することなく、ミラーリング設定したLANスイッチポートに接続するだけで導入することができる。システム構成もサーバ１台構成のアプライアンス製品であり、省スペース、省電力、安定稼働を図っている。DynamicMSIESERの導入構成を図１に示す。

2.2 高性能

DynamicMSIESERのサーバは、HP社製の高性能、省電力サーバであるHP Proriantシリーズを採用しており、随時新世代のサーバに対応している。１日当たりのキャプチャデータ量が1.4TB（高速モード）までパケットロス、セッション解析遅延なく安定稼働することができる。リアルタイム解析性能では、ネットワーク・フォレ

＊鎌倉事業部　ICTソリューション開発部

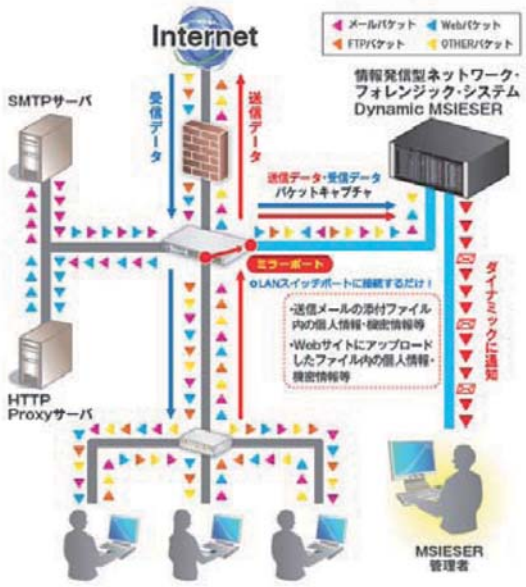

図１　DynamicMSIESER導入構成

ンジック業界では上位に位置づけられる（2014年12月当社調べ)。また、取得したパケットデータ及び解析結果データを長期間内部ディスク内に蓄積することが可能であり、数百TBのNASへ蓄積することもできる。

2.3　情報発信

DynamicMSIESERは様々な情報を管理者へ通知する。特長的な通知機能を以下に示す。

（1）送信ファイル検査機能

社内から外部へ、メールやWebアクセスで送信されるファイルに対して、個人情報、機密情報、特定情報等が含まれているかリアルタイムで検査し、管理者へメール通知する。本検査機能は、当社製品である個人情報ファイル検出ツール「すみずみ君」と同等の検索エンジンを用いており、競合製品と比較して非常に優位性がある。

（2）POST通知機能

Webアクセスでサイトに送信されたPOSTデータ、及び送信ファイル名を、定期的に管理者へメール通知する。送信データサイズの閾値を設定することにより、外部へ送信された不審なデータを検知することができる。

（3）マッチデータ通知機能

指定した検索条件にヒットした通信サマリと一覧を定期的に管理者へメール通知する。検索条件はインデックス化された情報及び全文検索キーワードを指定することができる。

3.　主なソリューション

3.1　アウトバウンド通信キャプチャ

アウトバウンド通信キャプチャとは社外ネットワーク向けのパケットのみを取得・解析する機能である。全てのパケットを取得・解析する場合、外部ネットワークから社内ネットワークへの通信がキャプチャデータの多くを占める(HTTP通信でダウンロードされるWEBページの内容など)。上記データは、情報セキュリティ上重要でない一般的な情報が多く含まれている。そのため、社内ネットワークから社外ネットワークへの通信（アウトバウンド通信）のみをキャプチャ・解析することにより、ストレージに保持するデータ量を削減することが可能である（図２参照)。

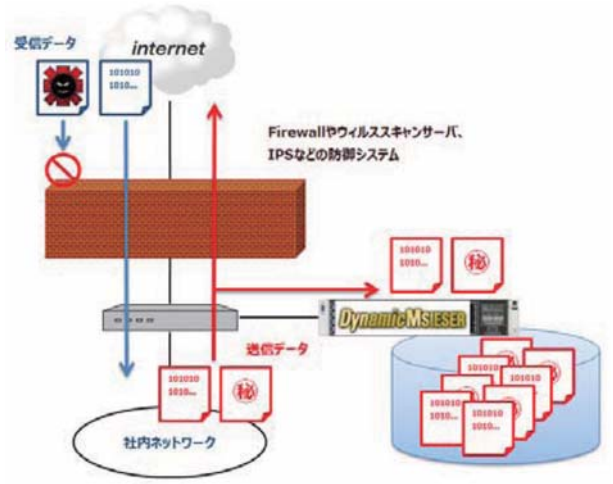

図２　アウトバウンド通信キャプチャ対応構成

3.2　復号化HTTPS通信解析

HTTPSを含むSSL暗号化通信による情報のやり取りは日々増加している。SSL暗号化通信は内容が秘匿されるためセキュアな一方、業務情報等の不正な外部送信があった場合に、被害状況の把握が困難になる。SSL復号化装置との連携により、暗号化された通信を解析することが可能である（図３参照)。

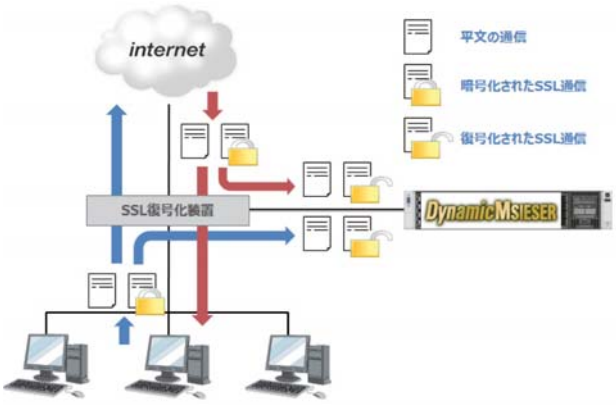

図３　HTTPS復号化対応構成

3.3　仮想化基盤

社内システムのクラウド化に対応して、仮想環境上でDynamic MSIESERを稼働させることができる。プライベートクラウドやIaaS上でDynamicMSIESERを稼働させることで、サーバの統合や仮想ネットワークのパケットキャプチャが可能である（図４参照）。

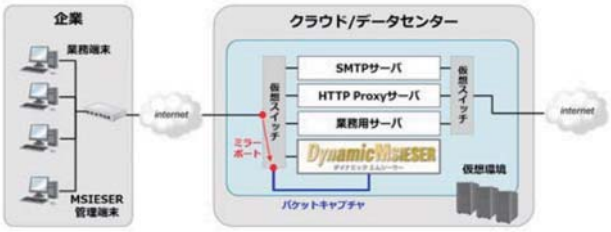

図４　クラウド対応構成

４．むすび

本稿では、情報発信型ネットワーク・フォレンジックシステム「DynamicMSIESER」について紹介した。当社では他にも情報セキュリティ関連の製品を提供している。詳細は当社ＨＰ（http://www.mss.co.jp）を参照されたい。

執筆者紹介

山内　直
2001年入社。2011年より現在のDynamicMSIESER関連業務に従事、現在に至る。

※「MSIESER」は三菱スペース・ソフトウエア株式会社の登録商標です。