社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2008－CSEC－42（46）
2008 / 7 / 25

IPマーキングによる不正活動ホストの広報機能の開発

松木 隆宏† 松岡 正明† 寺田 真敏‡ 鬼頭 哲郎‡ 仲小路 博史‡

†(株) ラック サイバーリスク総合研究所
〒105-7111 東京都港区東新橋 1-5-2 汐留シティセンター 11 階

‡(株) 日立製作所 システム開発研究所
〒212-8567 神奈川県川崎市幸区鹿島田 890

あらまし 近年，P2P ファイル交換ソフトウェア環境を悪用したマルウェアなどにより，個人あるいは組織の機密情報が流出する事象が続発し，社会へ悪影響を与えている．本稿では，P2P ファイル交換ソフトウェア環境において，マルウェアによる感染ノードの活動や利用者の誤った操作によって，ノードから機密情報が流出する問題に対し，意図しないファイルの流出を検出した場合にホストが送信するパケットに符号を付与し，不正な活動をしていることを近傍ネットワークに広報する機能を提案する．また，提案方式を実装したプロトタイプシステムについて報告する．
キーワード P2P，情報漏えい，広報機能

Development of publicity function of the illegitimate activity host by the IP marking

Takahiro Matsuki† Masaaki Matsuoka† Masato Terada‡ Tetsuro Kito‡
Hirofumi Nakakoji‡

†Little eArth Corporation Co., Ltd
1-5-2 Higashi-Shinbashi, Minato,Tokyo, 105-7111 Japan.

‡System Development Lab. Hitachi Ltd.
890 Kashimada, Saiwai-ku, Kawasaki, Kanagawa, 212-8567 Japan

Abstract Recently, there are many problems regarding the P2P file exchange environment on the Internet. The need to reconsider the current P2P file exchange environment for information leak. In this paper, we propose notification function of illegal activities of host. That is a part of the Information part of Sharing Architecture for P2P File Exchange Environment we showed. And we show prototype system.
Keyword P2P, Information leakage, Notification

1 はじめに

近年，P2P ファイル交換ソフトウェア環境を悪用したマルウェアなどにより，個人あるいは組織の機密情報が流出する事象が続発し，社会へ悪影響を与えている．著者らはこのような問題への包括的な対策として，情報流通対策アーキテクチャを提案した [1].

本稿では，マルウェアや利用者の誤った操作によって機密情報が流出する問題に対し，情報流通対策アーキテクチャの一部として提案した「不正活動ホストの広報機能」の実現手法の検

討結果と，検討結果に基づき実装したプロトタイプについて報告する．

なお，不正活動ホストの広報機能の目的は，機密情報の流出を検出した際に当該ホストの送信するパケットに発生事象を識別する符号を付与し，近傍のホストやネットワーク機器に不正な活動をしている旨を広報することで，近傍のホストやネットワーク機器と連携して通信を遮断するなどの対処を実現可能にすることにある．

2 不正活動ホストの広報機能

本章では，不正活動ホストの広報機能の背景と概要について述べる．

報告されている個人／機密情報の漏えい問題の多くは，表面化しにくい事象であること，問題が発生した後の対処にあたっては，近傍のネットワーク装置や事業者と協調して解決した方が良い場合がある．本機能の目的は，利用者ホストから，近傍のネットワークにインシデント発生あるいは，発生の可能性を通知することにより，ネットワーク側で情報流出に伴う拡散抑止につなげることにある．本機能の実現にあたっては，次のような事象を捉えた場合，ホストが送信する TCP/IP パケットに「ホストが不審あるいは不正な活動をしている」ことを表す事象フラグを格納する．

1. 個人／機密情報ファイルが P2P ファイル交換ネットワークに対してアップロードされるのを検知した場合
2. 暴露型ウイルス感染を検知した場合

上述の広報対象となる事象を検出したときの動作概要を図 1 に示す．広報対象となる事象の検出は，情報流通対策アーキテクチャの一部としてそれぞれ独立した上位機能として実装し，本稿で提案する「不正活動ホストの広報機能」は，それらの上位機能から利用可能なインターフェイスを提供する．このような機能分割を図ることにより，前述の事象以外に広報すべき事象が発生した場合でも，その事象を検出する上位機能を追加することで，広報機能の拡張が可能となる．

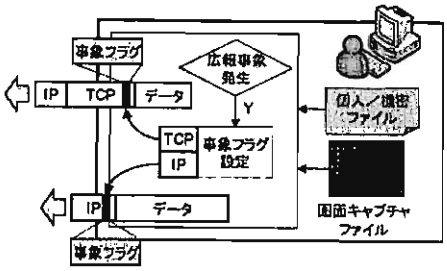

図 1: 不正活動ホストの広報機能

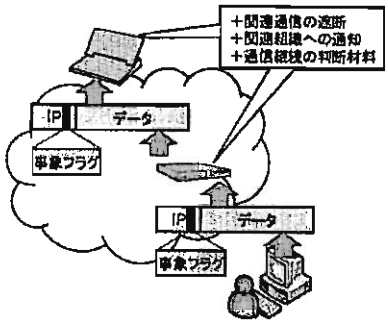

図 2: 不正活動ホストの通知の受信

また，このような「ホストが不審あるいは不正な活動をしている」ことを表す事象フラグを格納した TCP/IP パケットを送信することにより，受信した中継装置やホストは，関連する通信を遮断する，関連する組織に通知する，あるいは他の信頼できる装置に TCP/IP パケットを転送するなどの対処が可能となる (図 2)．さらに，事象フラグには，発生の事象によって異なる値を付与し，広報することでネットワーク側との対策連携の選択肢が増えると考えている．以降，TCP/IP パケットに事象フラグを格納する本提案手法を IP マーキングとする．

3 IP マーキングの開発方針

本章では，IP マーキングの開発方針について述べる．

3.1 事象とパケットの紐付け

現在広く利用されている「Winny」や「Share」などのP2Pファイル交換ソフトウェアでは，匿名性，機密性を高めるためプロトコルに暗号や分散処理が組み込まれており，ペイロードの内容を確認するには暗号の復号や分割されたデータの結合が必要である．そのため，暴露型ウイルスによるファイルアクセスとP2Pネットワークへのパケット送出を紐付けて，個人/機密情報を流出させるパケットのみにIPマーキングを行うことは困難である．「Winny」や「Share」においては，リバースエンジニアリング技術等によってプロトコルや暗号の解析がなされているが，今後新たなP2Pファイル交換ソフトウェアが利用されるようになった場合，その解析には高い解析技術と多くの時間が必要と推測される．

本稿で提案するIPマーキングでは，不正な活動の検出を上位機能に委ねることで，パケットの解析，ファイルと送出パケットの紐付けを行わずに，2章で述べた2つの事象を検出後に送出されるパケットにマークを付与する．これにより，新たなP2Pファイル交換ソフトウェアが登場しても汎用的に対応できる．また，情報流出や暴露型ウイルスへの感染のみに限らず，ボット等のマルウェアによる不正な動作の広報にも応用可能となる．

3.2 IP マーキング対象パケット

上位機能によってホストの不正な活動が検出された際にIPマーキングの対象とするパケットは以下の2通り考えられる．

1. P2Pファイル交換ソフトウェアが送出するパケットのみ
2. ホストから送出される全てのパケット

中継装置においてP2Pファイル交換ソフトウェアによるパケットのみを遮断するにはP2Pファイル交換ソフトウェアが送出するパケットのみに対するマーキングで十分と考えられる．しかし，IPマーキングの目的は不正な活動の広報であるため，時間軸，範囲軸の2つの側面からも，より多くのホストやネットワーク機器にマーク付きパケットを送信することが望ましいと考え，ホストから送出される全てのパケットにマークを付与する．

3.3 事象フラグ格納箇所

事象フラグの格納箇所はTCP/IPパケットのIPヘッダまたはTCPヘッダが考えられる．より多くのパケットにマーキングを行うにはIPヘッダへの格納が適している．そのため，本稿ではIPヘッダ(IPv4)に事象フラグを格納する．さらに，IPヘッダの中で事象フラグを格納するフィールドとして，表1に示す3つのフィールドが利用可能である．

表1: 事象フラグ格納フィールドの検討

フィールド	最大情報量	拡張性
TOS(Type Of Service)	8 bit	なし
Flags	1 bit	なし
IP Option	40 byte	あり

- TOSフィールドは8ビットの領域がある．Diff-Serv(RFC2474[2])のQoSに利用される．RFCにおいて全てのビットの使用目的が定義されており，未使用領域はない．
- Flagsフィールドは，最下位1ビットが未使用の予約領域であるが，RFC791[3]で必ず0と定義されている．利用したとしても1ビットの情報しか格納できない．
- IP Optionフィールドは，最大40バイトの領域を利用可能である．独自のIP Optionフォーマットを定義し可変長データを格納することができるため，拡張性がある．

3つのフィールドのうち，RFCに違反することなく，格納可能な情報量が最も多いIP Optionフィールドを事象フラグの格納先とした．なお，IPヘッダではなくTCPヘッダへの格納する場合は，TCPオプションが候補として考えられる．

4 設計と実装

本章では，3章で述べた開発方針に基づいたIPマーキングの設計とプロトタイプ実装について述べる．プロトタイプは，Windows XP Professional SP2 (32bit版) [1]を動作環境として開発した．

4.1 事象フラグの設計

IP Optionフィールドに独自のIP Optionとして格納する事象フラグの設計について述べる．

IP Optionフィールドの構造を図3に示す．

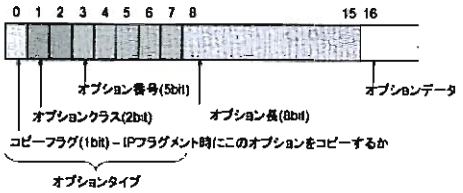

図3: IP Optionフィールドの構造

4.1.1 オプションタイプ

先頭の1バイトでオプションタイプであり，フラグメント時にオプションをコピーするかどうかを示すコピーフラグ(1bit)，オプションの種類を示すオプションクラス(2bit)とオプションを識別するためのオプション番号(5bit)から構成される．既存のIP Optionで使用されているオプションタイプの値は，IANAに管理されている[4]．本稿で定義したオプションタイプを表2に示す．

表2: オプションタイプ

	値
コピーフラグ	1
オプションクラス	0
オプション番号	25

[1]商品名称等に関する表示
Windows XPはMicrosoft Corporationの米国およびその他の国における登録商標または商標です．

不正な活動を広報するというIPマーキングの性質からコピーフラグの値は，1が望ましいと考える．オプションクラスは，0～3の値を取ることができるが，1および3は予約済みであり，既存のIP Optionでは，0または2が利用されている．1および3を利用した場合，不正なIP Optionとしてパケット中継装置やファイアウォールでパケットがフィルタリングされる可能性が考えられたため，パケットの制御に関するIP Optionで主に利用される0を採用した．オプション番号は，0～31の値で一般的に未使用なものとして，25を選択した．これは，RFC4782[5]で定義されているQuick-Startという実験的なプロトコルと重複するが，Quick-Startは，コピーフラグが0と定義されているため，本稿で定義したオプションタイプとは異なる．

4.1.2 オプションデータ

オプション長を3バイト固定とした．オプションタイプフィールドとオプション長フィールドがそれぞれ1バイトであるため，オプションデータには1バイトの情報を格納できる．ここに事象の種類を識別する情報の格納を想定しているが，詳細は未定義である．

4.2 実装方式

アプリケーションを変更することなく，前述の事象フラグを格納するIP Optionフィールドを IP ヘッダに追加するには，ホストのパケット送出をフックしてIPパケットにデータを追加する必要がある．実装方式の要件としては以下の項目が挙げられる．

1. ホストから送出される全てのパケットにIP Optionフィールドが付加できること
2. 安全であり安定であること

パケット送出フックの実装方式には，表5に示す5つの方式が考えられる．

DLL InjectionおよびLayered Service Providerはユーザモードでのフック手法である．これら

表 3: パケット送出フック手法

	mode
DLLinjection(IAThook,wrapperDLL)	user
LSP(Layered Service Provider)	user
ipfilter driver	kernel
TDI driver	kernel
NDIS driver	kernel

の手法は，Windows socket API をフックすることでアプリケーションレベルで送受信データを取得，改変できるため様々な応用が可能である．DLL Injection を用いて P2P ファイル交換ソフトウェアを介した情報流出を防止する研究もなされている [6]．しかしながら，実装にあたって各アプリケーションがロードする DLL や利用する Win32API を調査/解析する必要がある．一部の アプリケーションでは，これらの手法によって動作を監視，変更されることを防ぐために API フックができないように耐解析機能を備えているものがある．P2P ファイル交換ソフトウェアでもこのような耐解析機能を備えているものが存在する．今後新たに開発される P2P ファイル交換ソフトウェアにも耐解析機能が備えられる可能性が高く，リバースエンジニアリングによる解析が必要と考えられる．

また，近年では一部の暴露型ウイルスやマルウェアもこれらの手法を用いてパケット送出をフックし，悪意のある動作をするものも存在するため，これらによってフックが上書きされ，無効化される危険性もある．以上の理由から，ユーザモードでのフック手法は，要件 1 および要件 2 の両方を完全に満たすことができない．

一方，ipfilter driver, TDI driver, NDIS driver は，いずれもカーネルモードでのフックであり，パーソナルファイアウォール等のセキュリティソフトウェアの実装にも使用される方式である [7][8]．ユーザモードでのフック手法のようにアプリケーション個別の実装を解析することなく，ホストから送出される全ての IP パケットのヘッダを変更することができる．カーネルモードで動作するマルウェア，rootkit も存在するが，ユーザモードと比較してフック無効化の危険度が低いと考える．以上の理由から，ユーザモードでのフック手法よりも要件 1 と要件 2 を満たすことができると判断し，プロトタイプは，3 つのカーネルモードでのフックで最も低いレイヤで動作する NDIS driver での実装を採用した．

5 パケットの到達性の検証

本章では，IP マーキングを施したパケットの到達性についてプロトタイプ実装を用いた検証結果を述べる．

5.1 検証目的

IP マーキングを施したパケットは受信側ホストに正常に処理されない可能性や経路上の中継装置によって，IP Option フィールドが書き換えられたり，パケットそのものが破棄される可能性も考えられる．

そこで，パケット到達性の検証では，IP マーキングにより発生しうる事象を明らかにすることを目的とした．任意のプロトコルとポート番号を使用する TCP/IP パケットのみに IP マーキングを施すテストプログラムを作成し，これを用いて，最も一般的なインターネットアクセスである HTTP にのみ IP マーキングを行い，数カ所の Web サイトにアクセスを試みた．

5.2 検証結果

検証の結果を表 4 に示す．

表 4: マーキングパケットでの Web 閲覧

URL	閲覧可否
http://www.google.co.jp/	可
http://www.yahoo.co.jp/	可
http://www.microsoft.co.jp/	不可
http://www.soumu.go.jp/	不可
http://www.wikipedia.org/	可
http://www.kernel.org/	可
http://www.hitachi.co.jp/	不可
http://www.lac.co.jp/	不可

www.hitachi.co.jp へのアクセスでは，SYN に対する SYN+ACK を受信できなかった．原因が経路上にあるのか，受信ホストにあるのかを判別するため，tracert をマーキングありの場合となしの場合で実行し，比較を行った．その結果，マーキングを行った場合，最後の 1 hop で到達不能となっていることが分かった．このことから，マーク付きパケットが IPS 等によって遮断されたか受信ホストに正常に処理されなかったと考えられる．www.soumu.go.jp, www.lac.co.jp も同じく，SYN+ACK を受信できなかった．これらのサイトは，マーキングなしでも tracert で対象ホストに到達できなかったが，マーキングありの場合もマーキングなしの場合と同じ中継装置まで到達可能であった．

www.microsoft.co.jp は，TCP コネクションは正常に確立され HTTP 通信が正常に行われた．しかし，http://www.microsoft.com/japan にリダイレクトされた後，HTTP GET の応答が得られなかったため，パケットが経路上で遮断されている可能性が考えられる．

以上の例から，正常に通信が行えない原因は，受信側のホストやネットワーク機器によるものと経路上の中継装置によるものの両方が存在すると考えられる．マーキングを行っても正常に通信できるように IP Option を変更することが課題として挙げられる．

6 おわりに

本稿では，情報流通対策アーキテクチャの一部として提案した「不正活動ホストの広報機能」の実現手法として，ホストの送出するパケットの IP ヘッダに IP Option として事象フラグを格納する IP マーキング方式を提案し，プロトタイプシステムを実装した．プロトタイプを用いた検証の結果，IP マーキングを施したパケットの到達性に課題が存在することがわかった．

今後の課題としては，IP マーキングを施したパケットの到達性の改善のほか，事象フラグのオプションデータのフォーマットを定義し，情報漏えいやマルウェアへの感染など，ユーザの意図しない不適切な動作がコンピュータ内で行われた場合に，周囲のネットワークにそれを広報できるように情報流通対策アーキテクチャの上位機能との具体的な相互連携が挙げられる．

謝辞

本研究は総務省から受託した「ネットワークを通じた情報流出の検知及び漏出情報の自動流通停止のための技術開発」の成果の一部です．本研究を進めるにあたって有益な助言と協力を頂いた関係者各位に深く感謝致します．

参考文献

[1] 寺田真敏，鬼頭哲郎，仲小路博史，松木隆宏，松岡正明：P2P ファイル交換ソフトウェア環境における情報流通対策アーキテクチャの検討

[2] RFC : Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
http://www.ietf.org/rfc/rfc2474.txt

[3] RFC : RFC791 - INTERNET PROTOCOL
http://www.ietf.org/rfc/rfc791.txt

[4] IANA : IP OPTION NUMBERS
http://www.iana.org/assignments/ip-parameters

[5] RFC : RFC4782 - Quick-Start for TCP and IP
http://www.ietf.org/rfc/rfc.txt

[6] 安藤類央，外山英夫，門林雄基：DLL injection を用いた P 2 P ソフトウエアの情報漏洩の追跡と防止，第 130 回 DPS 研究会・第 36 回 CSEC 研究会合同研究会

[7] TDIFW project
http://tdifw.sourceforge.net/

[8] NDIS Developer's Reference
http://www.ndis.com/