情報漏洩を契機とした攻撃者探査システムの提案

池上 祐太　　山内 利宏

岡山大学大学院自然科学研究科
700-8530 岡山県岡山市北区津島中 3-1-1
ikegami@swlab.cs.okayama-u.ac.jp, yamauchi@cs.okayama-u.ac.jp

あらまし 機密情報の漏洩を防止する研究は比較的多いものの，機密情報を狙う攻撃者を特定する研究はあまりない．攻撃者を特定することで，攻撃の抑制，新しい攻撃への対策，および攻撃者の告発を実施できる．そこで，機密情報の漏洩を契機として攻撃者を特定するシステムを提案する．提案システムでは，計算機内において機密情報を追跡し，機密情報が外部へ送信される場合にダミーデータと入れ替え，機密情報の漏洩を防止する．また，ダミーデータには，ダミーデータを操作している計算機の情報を指定した計算機に送信するプログラムを埋め込む．このプログラムが動作することで，攻撃者の情報を取得し，攻撃者を特定する．

Proposal of Attacker Investigation System Triggered Information Leakage

Yuta Ikegami　　Toshihiro Yamauchi

Graduate School of Natural Science and Technology, Okayama University
3-1-1, Tsushima-naka, Kita-ku, Okayama, 700-8530, JAPAN

Abstract There are many researches which prevent classified information leakage. However, there are few researches which specify attacker who steals classified information. By specifying attackers, control of attacks, countermeasures for new attacks, and prosecuting attackers can be carried out. This paper proposes attacker investigation system focusing on classified information leakage. This system traces classified information in a computer and substitute dummy data for classified information, which is sent to the outside the computer. Therefore, we can prevent classified information leakage. In addition, the program, which is embedded in the dummy data, transmits information of an attacker's computer, to a specified computer for investigation. By executing this program, we can acquire attacker's information.

1　はじめに

近年，機密情報を狙うサイバー攻撃が問題となっている [1]．サイバー攻撃の手口は，巧妙化しており，計算機への侵入を完全に防ぐことは困難である．これに伴い，計算機への侵入後の対策として，機密情報の漏洩を防止する研究が存在する [2],[3],[4]．しかし，機密情報を狙う攻撃者を特定する研究は，あまりない．攻撃者を特定することで，攻撃の抑制，新しい攻撃への対策，および攻撃者の告発を実施できる．攻撃者を特定するサービスや製品として，Cloud strike [5] や Junos WebApp Secure [6] が存在する．これらのサービスや製品は，マルウェアの解析や膨大な量の攻撃者のデータベースが必

要である．攻撃者を調査する手法として，攻撃者と思われる人物の計算機にスパイウェアを送りこみ，攻撃者の情報を取得する事例がある [7]．しかし，法律上，日本では能動的にスパイウェアを送り込むことはできない．

そこで，本稿では，これらの問題へ対処するため，機密情報の漏洩を契機として攻撃者を特定するシステムを提案し，提案システムの Linux を対象とした実現方式と評価について述べる．提案システムでは，計算機内において，機密情報として登録したファイル (以降，機密情報) を追跡し，機密情報が外部へ送信される場合にダミーデータと入れ替える．これにより，機密情報の漏洩を防止できる．また，ダミーデータには，ダミーデータを操作している計算機の情報を指定した計算機に送信するプログラム (以降，探査プログラム) を埋め込む．攻撃者の計算機上で，探査プログラムが動作することにより送信された情報を確認することで，攻撃者の情報を取得できる．提案システムは，どのようなダミーデータにでも入れ替えることができるため，利用者の目的に応じて取得できる情報を変更できる．

2 関連研究と問題点

2.1 マルウェアの解析や攻撃の痕跡から攻撃者を特定する手法

Cloudstrike [5] は，マルウェアの解析や攻撃の被害を受けた計算機を調査することで，攻撃者を特定するサービスを提供する．マルウェアを解析することで，マルウェアの使用言語，マルウェアの通信先のサーバ，およびマルウェアの通信情報などから攻撃者を探査できる．また，攻撃の被害を受けた計算機の調査により攻撃の特徴を見つけ，攻撃者を探査する．

2.2 攻撃者のデバイス情報を元に攻撃を検知する手法

Junos WebApp Secure [6] は，Web サイトや Web アプリケーションに対する攻撃を検知するアプライアンス製品である．Junos WebApp Secure は，入力フォームに対する不正なコードの挿入を検知した場合，攻撃者にトークンを送信する．このトークンは，永続的に攻撃者の計算機内に保存され，トークンを確認することで，同じ攻撃者からの攻撃を検知できる．また，攻撃者の情報として，ブラウザのバージョン，ブラウザのアドオン，IP アドレス，およびタイムゾーンなど約 200 種類の情報を取得する．これらの情報を利用することで，攻撃者を探査できる．

2.3 ダミーデータをサーバ上に設置し，攻撃を検知する研究

文献 [8] では，ファイルサーバ上に，攻撃者の興味を引くようなダミーデータ (passwords.txt など) を設置し，ダミーデータが操作されると，攻撃されていると検知する．

2.4 既存研究の問題点

これまでに述べた既存の研究には，以下のいずれかの問題が存在する．

(問題 1) 機密情報の漏洩を防止できない

(問題 2) 攻撃に使用されたマルウェアが必要

(問題 3) 攻撃者の特定に期間がかかる

(問題 4) 攻撃者を探査不可能

文献 [5] は，攻撃を受けた後に攻撃者を特定するため，機密情報が漏洩している (問題 1)．同様に，文献 [8] は，ダミーデータの検知のみを行うため，機密情報の漏洩を防止できない．

文献 [5] は，マルウェアの解析や攻撃を受けた計算機を調査することで，攻撃者を特定する．攻撃者の特定において，攻撃者が使用したマルウェアの解析は有効である．しかし，攻撃者が使用したマルウェアを入手できない場合，攻撃者の特定は難しい (問題 2)．また，攻撃者を特定する手掛かりを調査するため，通常のマルウェアの解析や攻撃の調査よりも時間がかかる (問題 3)．

文献 [6] は，200 種類もの攻撃者の情報を取得し，攻撃者を特定する．しかし，取得できる情報は，攻撃を行う計算機の情報であるため，攻撃者が第 3 者の計算機を踏み台にして攻撃を行う場合などは，攻撃者を特定できない (問題 4)．同様に，文献 [8] は，攻撃の検知のみにとどまっており，攻撃者の特定まで至っていない．

3　情報漏洩を契機とした攻撃者探査システムの設計

3.1　提案システムの要件

2 章で述べた問題を解決するシステムを提案する．(問題 1) への対処では，計算機内の機密情報を監視する．監視する機密情報の外部への送信を漏れなく検知することが有効である．

(問題 2)，(問題 3)，および (問題 4) への対処では，直接，攻撃者の計算機上で探査プログラムを実行させることが有効である．しかし，能動的に探査プログラムを攻撃者の計算機に送り込むことは，法律上できない．このため，攻撃者自身に探査プログラムを取得させ，実行させる必要がある．

各問題への対処から，提案システムの実現における要件は以下のようになる．

(要件 1) 計算機内の機密情報を漏れなく追跡

(要件 2) 攻撃者の計算機上で攻撃者自身が探査プログラムを実行

3.2　基本的な考え方

提案システムの目的は，計算機外部への機密情報の漏洩を防ぎ，攻撃者の計算機上で探査プログラムを実行させ，攻撃者の情報を取得することである．情報の漏洩は，プログラムの実行状態であるプロセスが機密情報にアクセスし，計算機外部へ機密情報を伝達することによって起こる．プロセスが情報を伝達する経路には，ファイル操作，プロセス間通信，および子プロセスの生成がある．上記の処理には，必ず OS が関与しているため，これらの処理のシステムコールを監視することで機密情報を漏れなく追跡できる．

攻撃者の計算機上で探査プログラムを実行させるには，攻撃者の計算機に探査プログラムを配置する必要がある．攻撃者の計算機に探査プログラムを配置するには，攻撃者が窃取を試みる機密情報と探査プログラムを入れ替えることで，実現できる可能性が高くなる．機密情報と探査プログラムの入れ替えは，計算機外部への機密情報の送信を検知し，機密情報の送信前に行う．機密情報と探査プログラムを入れ替えることにより，攻撃者に探査プログラムを送信できる．情報を外部へ送信するには，必ず OS が関与しているため，この処理のシステムコールを監視することで，機密情報が外部に送信される前に機密情報と探査プログラムを入れ替えることができる．

攻撃者の情報を取得するために，攻撃者に探査プログラムを実行させる必要がある．しかし，探査プログラムをそのまま配置すると，簡単に攻撃者に探査プログラムと検知される．そこで，攻撃者に探査プログラムと検知されにくくする必要がある．攻撃者に探査プログラムと検知されにくくするには，攻撃者が窃取しようとした機密情報であるかのようなダミーデータに探査プログラムを埋め込むことが効果的である．これにより，攻撃者はダミーデータの窃取を機密情報の窃取と勘違いし，ダミーデータを開き，探査プログラムを実行する可能性が高まる．

3.3　提案システムが対象とする攻撃

提案システムが対象とする攻撃は，攻撃者が不正アクセスにより直接計算機を操作する場合とマルウェアによる場合である．また，文献 [11] を参考に，想定する攻撃手順を以下に述べる．

(1) 攻撃者 (マルウェア) が計算機内に侵入

(2) 目的の機密情報を収集

(3) 収集した機密情報を圧縮

(4) 外部の計算機へ圧縮した機密情報を送信

攻撃者は，収集した機密情報を圧縮し，外部へ送信することが多い．しかし，機密情報を圧縮せず送信する可能性もある．このため，提案システムは，機密情報を圧縮する場合と圧縮しない場合の両方に対応する．

3.4　提案システムの課題

3.2 節より，提案システムの課題は以下のようになる．

(課題 1) 機密情報の操作に関係するシステムコールのフック

(課題 2) 機密情報とダミーデータを入れ替える処理の実現

(課題 3) 機密情報と誤認するようなダミーデータの作成

(要件 1) は，機密情報の操作に関係するシステムコールをフックすることで，実現できる (課題 1)．フック後，提案システムにおいて機密情報を追跡し，本来のシステムコール処理を呼び出し，システムコール処理を再開させる．

(要件 2) は，機密情報が外部へ送信される際に使用されるシステムコールをフックし，機密情報と探査プログラムを埋め込んだダミーデータを入れ替えることで実現できる (課題 2)．また，ダミーデータのファイル名やファイルサイズを機密情報のファイル名やファイルサイズに合わせることで，攻撃者自身に探査プログラムを実行させる可能性を高めることができる (課題 3)．攻撃者の視点から考察すると，情報の窃取に成功し，窃取した情報のファイル名やファイルサイズが攻撃対象の計算機内の機密情報と一致している場合，ダミーデータを機密情報と判断する可能性が高い．

3.5 提案システムの構成

提案システムは，3.4 節で述べた課題へ対処する．提案システムの全体像を図 1 に示す．提案システムは，以下の機能と機構により実現する．

- 機密情報の拡散追跡機能
- ダミーデータ入れ替え機構

機密情報の拡散追跡機能は，文献 [2] の方式を利用する．機密情報の拡散追跡機能は，プロセスが発行したシステムコールをフックし，プロセスが機密情報を読み込んだ場合，その内容を他のプロセスやファイルなどに伝える可能性があるため，それらのプロセスやファイルを機密情報として登録し，追跡する．機密情報の拡散追跡機能の詳細は，3.6 節で説明する．

ダミーデータ入れ替え機構は，機密情報の拡散追跡機能から呼ばれ，機密情報が外部へ送信される前に，機密情報とダミーデータを入れ替える．ダミーデータ入れ替え機構の詳細は，3.7 節で述べる．

3.6 機密情報の拡散追跡機能

機密情報の拡散追跡機能とは，機密情報が拡散していく様子を追跡することで，機密情報が持つ可能性のある資源を把握し，機密情報が計

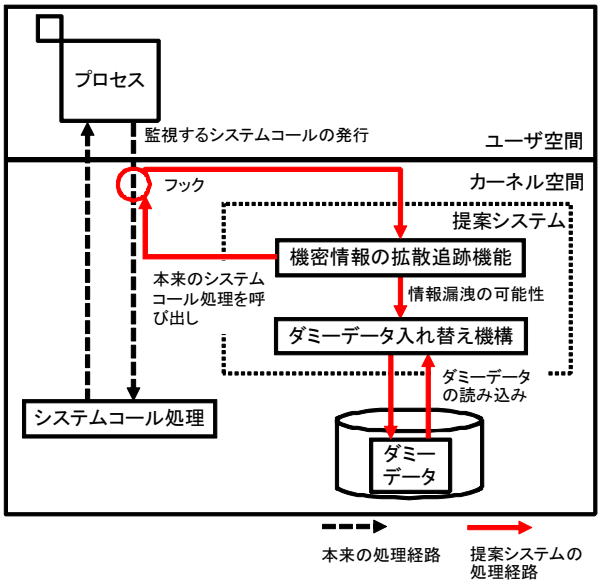

図 1 提案システムの全体像

算機外へ漏洩する際，それを検知する機能である．機密情報の拡散は，ファイル形式で存在する機密情報をプロセスが読み込み，さらに他のプロセスやファイルなどへ，その内容を伝えることで行われる．プロセスが情報を拡散する経路を以下に示す．

(1) ファイル操作

(2) プロセス間通信

(3) 子プロセスの生成

機密情報が拡散するファイル操作として，ファイル内容を読み込みとファイルへの書き出しがある．読み込み元が機密情報を有するファイルの場合，プロセスを監視対象とする必要がある．また，監視対象のプロセスがファイルに情報を書き出した場合，機密情報が書き出された可能性があるため，書き出し先のファイルを管理対象ファイルとする必要がある．

管理対象プロセスは，プロセス間通信により，他のプロセスに情報を伝達できる，このため，ソケット，共有メモリ，パイプ，およびメッセージキューによるプロセス間通信を監視する．送信元プロセスが管理対象であるとき，送信を仲介する通信用資源と受信プロセスを管理対象とする必要がある．

子プロセスの生成時に，子プロセスが親プロセスの資源を引き継ぐ機能がある場合 (UNIX における fork 処理など) には，この機能を通してプロセス間で情報が拡散する．したがって，親プロセスが管理対象プロセスであるときは，子プロセスも管理対象プロセスとする必要がある．

これらの処理を監視し，機密情報の拡散を追跡する (課題 1 への対処)．

3.7 ダミーデータ入れ替え機構

ダミーデータ入れ替え機構は，機密情報が外部へ送信されようとしている場合に機密情報の拡散追跡機能から呼び出され，機密情報とダミーデータを入れ替える (課題 2 への対処)．これにより，機密情報の漏洩を防ぐと同時に，ダミーデータを攻撃者に送信できる．

ダミーデータ入れ替え機構の処理手順を以下で説明する．

(1) 機密情報のファイルサイズを取得

(2) ダミーデータを読み込み，ファイルサイズを取得

(3) (1) と (2) のファイルサイズを比較

(4) 機密情報のファイルサイズの方が大きい場合，機密情報のバッファにダミーデータのバッファを上書きし，機密情報のファイルサイズまでパディング

(5) 機密情報のファイルサイズの方が小さい場合，機密情報のバッファとダミーデータのバッファを入れ替え

機密情報とダミーデータのファイルサイズが異なる場合，攻撃者が機密情報の送信前と送信後でファイルサイズを比較することで，ダミーデータと入れ替わっていることを検知できる．このため，ダミーデータのファイルサイズを機密情報のファイルサイズに合わせることで，対処できる (課題 3 への対処)．機密情報のファイルサイズがダミーデータのファイルサイズより大きい場合，機密情報が読み込まれたバッファにダミーデータの内容を書き込み，機密情報のファイルサイズまでパディングする．バッファは，監視するシステムコールの引数から取得できる．

なお，機密情報のファイルサイズがダミーデータのファイルサイズより小さい場合，探査プログラムの内容を機密情報のファイルサイズ内に書き込むことができず，探査プログラムが正常に動作しない．そこで，ダミーデータのファイルサイズまでバッファを拡張し，ダミーデータの内容を書き込む．このため，機密情報のファイルサイズにダミーデータのファイルサイズを一致させることができない問題がある．

3.8 探査プログラムについて

ダミーデータには，操作されると攻撃者の情報を取得するプログラム (探査プログラム) を埋め込む．ダミーデータには，どのようなプログラムでも埋め込むことができるため，利用者が取得したい情報に応じて変更できる．本稿で作成した探査プログラムが取得する攻撃者の情報を以下に示す．

(1) 攻撃者が使用する計算機の IP アドレス

(2) 攻撃者が使用する計算機の MAC アドレス

(3) 攻撃者が使用する計算機の使用言語

(4) 攻撃者が使用する計算機のタイムゾーン

(5) 攻撃者が使用する計算機のベンダ，製品名，および製造番号

攻撃者が使用する計算機の IP アドレスを取得することで，攻撃者が使用するネットワーク環境を探査できる．

MAC アドレスは，NIC (Network Interface Card) に割り当てられる固有の番号であるため，攻撃者の使用する計算機の特定に効果的である．しかし，攻撃者が MAC アドレスを変更している場合，他の MAC アドレスと重複する可能性があるため，攻撃者の特定まで至らない可能性がある．

使用言語とタイムゾーンの取得は，攻撃者が活動の拠点とする国や現在の所在地の特定に効果的である．

攻撃者が使用する計算機のベンダ，製品名，および製造番号の情報は，計算機に割り当てられる固有の番号であり，攻撃者の特定に効果的である．

探査プログラムの実行方法は，攻撃者の OS や操作方法が GUI か CUI かで異なる．例えば，ダミーデータに Windows 上でのみ動作する探査プログラムを埋め込むとする．しかし，攻撃者の計算機が Windows 以外の OS を使用していた場合，探査プログラムは正常に動作しない．また，GUI で実行する場合，ダミーデータをクリックし，開かせることで，探査プログラムを実行できる．しかし，Windows の場合，拡張子によってファイルを識別する．このため，ダミーデータの拡張子を exe ファイルのような実行ファイルの拡張子に変更する必要がある．また，攻撃者が Linux のターミナルのような CUI で計算機を操作する場合，探査プログラムを攻撃者の計算機で実行させるには，コマンドを入力させる必要がある．CUI で探査プログラムを実行させる方法は，今後の課題である．

3.9 期待される効果

期待される効果を以下に示す．

(1) 攻撃者の情報を利用者の目的に応じて取得

(2) 機密情報の漏洩の防止

ダミーデータに埋め込んだ探査プログラムが動作することで，攻撃者の情報を取得できる．提案システムは，どのような探査プログラムでもダミーデータとして機密情報と入れ替えることができる．このため，利用者の目的に応じて探査プログラムの変更や改変をすることで，幅広く攻撃者の情報を取得でき，攻撃者を探査できる．

提案システムは，機密情報の外部への送信を漏れなく検知し，ダミーデータと入れ替える．このため，攻撃者が探査プログラムを検知した場合や探査プログラムが正常に動作しない場合でも，機密情報の漏洩は，確実に防止できる．

4 実装と評価

4.1 実装内容

ダミーデータ入れ替え機構を Linux 3.4.9 上にプロトタイプとして実装した．ダミーデータ入れ替え機構は，LKM (Loadable Kernel Module) として実現し，OS の再構築をすることなく機密情報の拡散追跡機能と連携できる．機密情報の拡散追跡機能とダミーデータ入れ替え機構の連携は未完成のため，今後の課題である．4.2 節では，ダミーデータ入れ替え機構にファイル操作のみを追跡する機能を追加し，評価した．

4.2 評価目的と評価内容

評価目的と評価内容について以下に示す．

提案システムが導入された計算機内で，機密情報を外部のアップロード用計算機に送信するプログラムを実行させ，以下の 2 点を確認する．

(1) 機密情報の漏洩の防止

(2) 攻撃者の計算機の情報の取得

提案システムの導入により，攻撃者が窃取しようとする機密情報とダミーデータが入れ替わり，機密情報の漏洩を防ぐことを確認する．また，攻撃者の計算機上で，ダミーデータに埋め込んだ探査プログラムが動作し，攻撃者の情報を取得できることを確認する．提案システムが動作する環境を表 1，攻撃者の計算機の環境を表 2 に示す．本評価では，攻撃者の OS は Windows であると想定しているため，Windows 上で動作する探査プログラムを作成し，使用した．ただし，今回作成した探査プログラムは，Windows 上で動作する実行ファイル (exe ファイル) であるため，ダミーデータのファイル名が機密情報のファイル名のままでは，実行ファイルとして認識されない．このため，攻撃者の計算機上で，ダミーデータのファイル名の拡張子を exe に変更した．拡張子の問題への対処は，今後の課題である．探査プログラムは，3.8 節で示した情報を取得する．本評価で使用した探査プログラムの動作について以下に示す．

(1) 指定した計算機とコネクションを確立

(2) 攻撃者の計算機の情報の取得

(3) 指定した計算機に攻撃者の情報を送信

IP アドレス，MAC アドレス，計算機のベンダ，製品名，および製造番号は，system 関数を

表 1 提案システムが動作する環境

CPU	Intel Core i7-3770 (3.40 GHz)
メモリ	4.0 GB
カーネル	Linux 3.4.9

表 2　攻撃者の計算機の環境

OS	Windows Vista (32 bit)
IP アドレス	172.21.48.231
MAC アドレス	00:50:56:C0:10:08
使用言語	英語
タイムゾーン	サモア標準時
計算機のベンダ	Dell Inc.
計算機の製品名	OptiPlex 755
計算機の製造番号	1YC7KBX

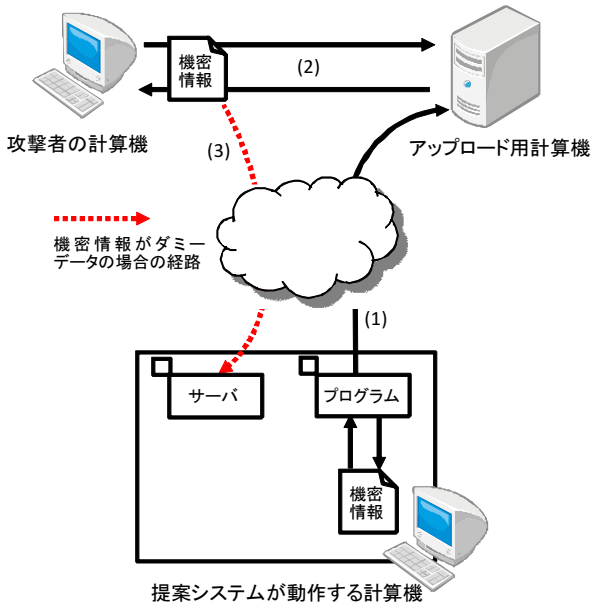

図 2　実験の概要図

使用し，cmd.exe にコマンドを実行させて取得する．攻撃者の計算機の使用言語は，上記のコマンドの実行結果から取得できる．計算機のタイムゾーンは，strftime() 関数を使用し，取得する．

4.3　計算機外部へ機密情報を送信するプログラムによる実験

4.3.1　実験手順

実験の概要図を図 2 に示し，以下で実験手順を示す．

(1) 提案システムが動作する計算機上で，機密情報を外部のアップロード用計算機へ送信するプログラムを動作

表 3　機密情報と探査プログラムのサイズ

	ファイル名	ファイルサイズ (bytes)
機密情報	secret_file	102.400
探査プログラム	investigate.exe	53,003

(2) 攻撃者の計算機から外部のアップロード用計算機にアクセスし，機密情報を攻撃者の計算機に移動

(3) 攻撃者の計算機上で機密情報を開く

上記の攻撃手順は，3.3 節で示した攻撃手順において，攻撃者が機密情報を圧縮せず，計算機の外部へ送信する手順である．本評価では，探査プログラムが取得した情報を受信する計算機は，提案システムが動作する計算機に，サーバとして動作させ，受信した．また，評価で使用した機密情報と探査プログラムのサイズを表 3 に示す．

4.3.2　実験結果

攻撃者の計算機上で，取得したファイルのサイズと名前は，表 3 の機密情報と一致した．取得した機密情報の拡張子を exe に変更して開くと，指定したサーバで攻撃者の情報を受信した．受信した攻撃者の情報は，表 2 の情報と一致した．上記の実験結果から，提案システムの導入により，機密情報の漏洩の防止と機密情報とダミーデータが入れ替わり，攻撃者の情報を取得できたことを確認した．

4.4　残された課題

提案システムの残された課題を以下に示す．

(1) 効果的な探査プログラムの実行方法

現在は，攻撃者がダミーデータを開くことで，ダミーデータに埋め込んだ探査プログラムが動作し，攻撃者の情報を取得する．この手法では，攻撃者に探査プログラムを確実に実行させることはできない．このため，探査プログラムを効果的に実行させる手法を提案する必要がある．

(2) 探査プログラムのマルチプラットフォームでの動作

現在の探査プログラムは，マルチプラットフォームでの動作に対応していない．攻撃者が使

用する OS 上で，正常に探査プログラムを動作させるために，探査プログラムをマルチプラットフォームに対応する必要がある．

(3) カーネルレベルや仮想計算機モニタで動作するマルウェアへの対処

提案システムは，カーネルの改変や LKM で実現しているため，文献 [9],[10] のようなカーネルレベルや仮想計算機モニタで動作するマルウェアから攻撃できるため，対処する必要がある．

5 おわりに

機密情報の漏洩を契機として攻撃者を特定するシステムを提案した．提案システムは，機密情報の操作に関係するシステムコールをフックすることで，計算機内において機密情報を追跡し，機密情報が外部へ送信される場合にダミーデータと入れ替える．これにより，機密情報の漏洩を防止できる．入れ替えたダミーデータには，ダミーデータを操作している計算機の情報を指定した計算機に送信する探査プログラムを埋め込む．探査プログラムが攻撃者の計算機上で動作することで，攻撃者の情報を取得し，攻撃者を特定する．

評価では，提案システムが動作する計算機上で，機密情報を外部へ送信するプログラムを動作させる実験をした．実験結果は，提案システムの導入により，機密情報の漏洩を防ぎ，攻撃者の情報を取得できたことを確認した．

今後は，4.4 節で述べた課題を解決し，実際にマルウェアを動作させた評価や提案システムのオーバヘッドを評価する．

参考文献

[1] “2013 DATA BREACH INVESTIGATIONS REPORT, ”http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

[2] 田端 利宏，箱守 聰，大橋 慶，植村 晋一郎，横山 和俊，谷口 秀夫，“機密情報の拡散追跡機能による情報漏えいの防止機構”，情報処理学会論文誌，vol.50，no.9，pp.2088–2102，2009.

[3] David Yu Zhu, Jaeyeon Jung, Dawn Song, Tadayoshi Kohno, David Wetherall, “TaintEraser: Protecting Sensitive Data Leaks Using Application-Level Taint Tracking, ”ACM SIGOPS Operating Systems Review, vol.45, no.1, pp.142–154, 2011.

[4] Simon Liu, Rick Kuhn, “Data Loss Prevention, ”IT Professional, vol.12, no.2, pp.10–13, 2010.

[5] “Crowdstrike, ”http://www.crowdstrike.com/index.html

[6] “Junos WebApp Secure, ” http://www.juniper.net/us/en/local/pdf/datasheets/1000401-en.pdf

[7] “CYBER ESPIONAGE Against Georgian Government (Georbot Botnet), ”http://dea.gov.ge/uploads/CERT%20DOCS/Cyber%20Espionage.pdf

[8] Jim Yuill, Mike Zappe, Dorothy Denning, Fred Feer, “Honeyfiles: deceptive files for intrusion detection, ”Proc. Fifth Annual IEEE Information Assurance Workshop, pp.116–122, 2004.

[9] Ryan Riley, Xuxian Jiang, Dongyan Xu, “Multi-Aspect Profiling of Kernel Rootkit Behavior, ”Proc. 4th ACM European conference on Computer systems (EuroSys’09), pp.47–60, 2009.

[10] Samuel T. King, Peter M. Chen, Yi-Min Wang, Chad Verbowski, Helen J. Wang, Jacob R. Lorch, “SubVirt: Implementing malware with virtual machines, ” Proc. 2006 IEEE Symposium on Security and Privacy(SP’06), pp.314–327, 2006.

[11] “標的型サイバー攻撃の事例分析と対策レポート, ”http://www.ipa.go.jp/files/000014188.pdf