情報漏洩を契機とした攻撃者探査システムの提案

2013年10月21日

池上 祐太　山内 利宏

岡山大学　大学院自然科学研究科

はじめに

機密情報を狙うサイバー攻撃が問題

⇒ 侵入後の対策として，機密情報の漏洩を防止する研究が盛んに実施

しかし，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可能

既存の攻撃者を特定する研究は，機密情報の漏洩を防止できない，攻撃者の特定まで時間がかかる等の問題が存在

▼

機密情報の漏洩を契機とした攻撃者を特定するシステムを提案

機密情報の漏洩の防止と攻撃者の情報を取得できたことを確認

関連研究

(研究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

(A) マルウェアの使用言語，通信先のサーバ，および通信情報などから攻撃者を探査

(B) 攻撃を受けた計算機の調査から攻撃者の特徴を発見

(研究2) 攻撃者のデバイス情報を元に攻撃者を検知する手法

(A) Webアプリケーションに対して不正なコードの挿入を検知し，不正なコードを挿入した攻撃者にトークンを送信

(B) 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

(研究3) ダミーデータをサーバ上に設置し攻撃を検知する手法

(A) ファイルサーバ上に，攻撃者が興味を引くようなダミーデータを設置 (password.txt など)

(B) ダミーデータが操作された場合，攻撃されていると検知

※ (研究1): 文献[5] 2011 ～ (研究2): 文献[6] 2013 (研究3): 文献[8] 2004

既存研究の問題点

(問題1) 機密情報の漏洩を防止できない

- 研究 1，3 は，攻撃を受けた後に攻撃者を特定するため，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

- 研究 1 は，攻撃者が使用したマルウェアを入手できない場合，攻撃者を特定することが難しい

(問題3) 攻撃者の特定に時間がかかる

- 研究 1 は，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時間がかかる

(問題4) 攻撃者を探査できない

- 研究 2 は，取得できる情報が攻撃を行う計算機の情報であるため，第3者の計算機を踏み台としている場合は特定できない
- 研究 3 は，攻撃の検知のみであり，攻撃者を特定できない

提案システムの要件

(問題1) 機密情報の漏洩を防止できない
対処として…計算機の機密情報を監視することで，機密情報の外部への送信を漏れなく検知可能

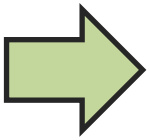
(問題2) 攻撃に使用されたマルウェアが必要
(問題3) 攻撃者の特定に時間がかかる
(問題4) 攻撃者を探査できない
対処として…直接，攻撃者の計算機上で攻撃者の情報を取得するプログラム (探査プログラム) を実行

(要件1) 計算機内の機密情報を漏れなく追跡すること
(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

基本的な考え方

(要件1) 計算機内の機密情報を漏れなく追跡すること

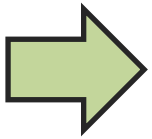
情報の漏洩は，プロセスが機密情報にアクセスし，計算機外部へ機密情報を伝達するによって発生



上記の処理にかかわる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可能

(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

攻撃者の計算機上に探査プログラムを配置する必要がある



攻撃者が摂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，実現の可能性が高まる

しかし，攻撃者に探査プログラムと検知される可能性がある

対処として…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有効

提案システムが対象とする攻撃

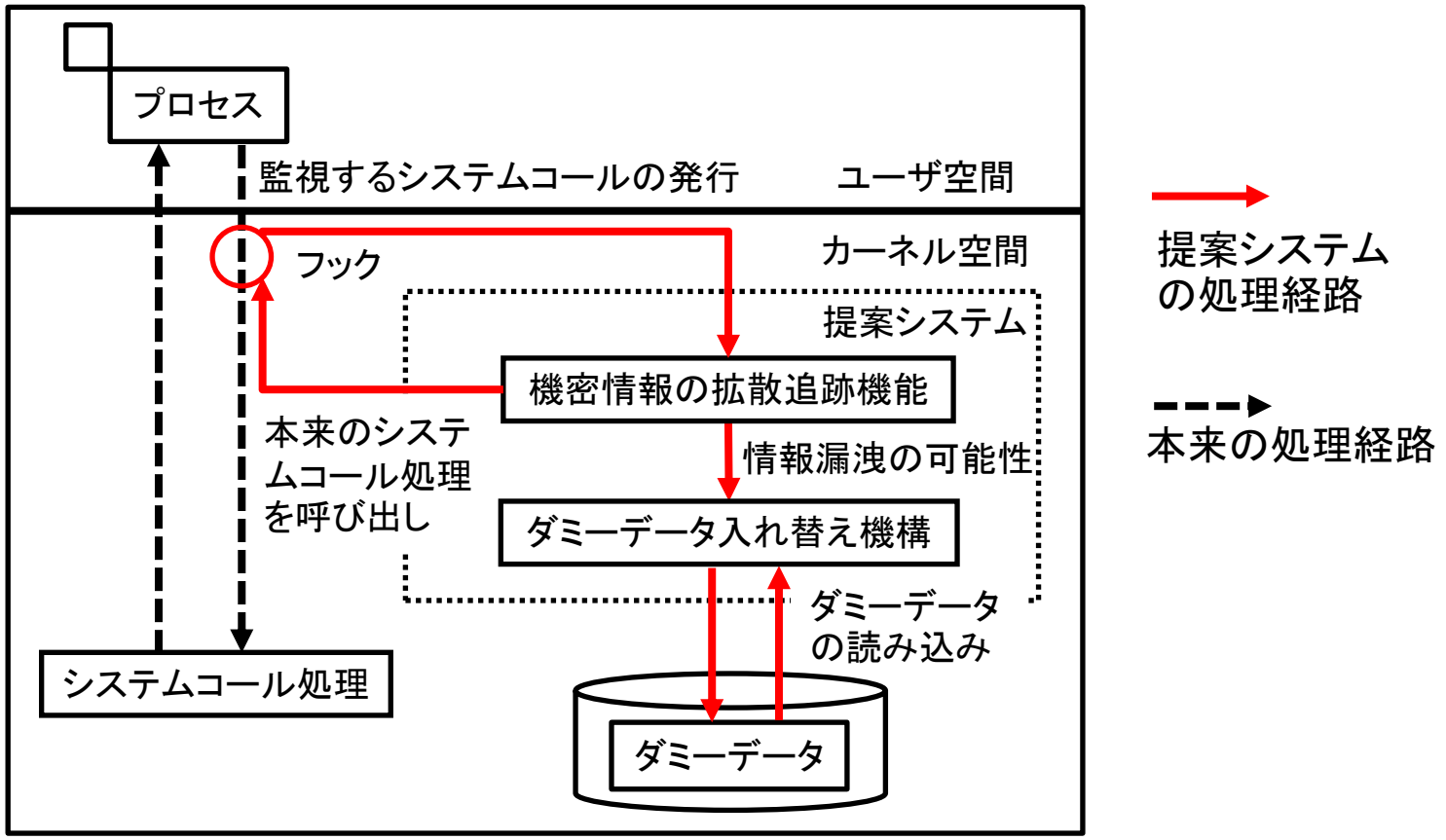
(1) 不正アクセスにより直接計算機を操作する攻撃
(2) マルウェアによる攻撃

■ 攻撃手順

(1) 攻撃者 (or 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

機密情報を圧縮せず外部へ送信する場合にも対応

提案システムの構成



(機密情報の拡散追跡機能)
　文献[2] の方式を利用

(ダミーデータ入れ替え機構)
　機密情報の拡散追跡機能から呼び出し

機密情報の拡散追跡機能

計算機内の機密情報の拡散を追跡し，機密情報の外部への漏洩を検知する機能

■ 計算機内における機密情報の拡散

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，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

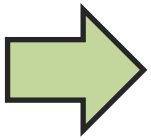
■ 監視する処理

(1) ファイル操作
(2) プロセス間通信
(3) 子プロセスの生成

上記の処理を監視し，機密情報の拡散を追跡可能

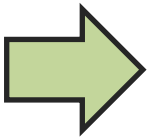
ダミーデータ入れ替え機構

機密情報が外部へ送信されようとしている場合，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



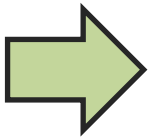
(1) 機密情報の漏洩の防止
(2) ダミーデータを攻撃者に送信可能

ダミーデータのファイル名とファイルサイズを機密情報のファイル名とファイルサイズに合わせる



攻撃者にダミーデータと気づきにくくさせる

機密情報のファイルサイズが探査プログラム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すべて書き込めない



探査プログラムのファイルサイズでダミーデータを作成

探査プログラムについて

操作されると攻撃者の情報を取得するプログラム

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可能

■ 探査プログラムが取得する攻撃者の情報

(1) IPアドレス
(2) MACアドレス
(3) 計算機のベンダ
(4) 製品名
(5) 製造番号

■ 探査プログラムの実行方法の問題点

(1) 攻撃者の OS の種類による実行の問題

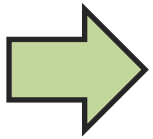
(例) Windows ○　Linux ×

(2) 操作方法が GUI か CUI による問題

(例) GUI: クリックで実行　CUI: コマンド入力で実行

実装

ダミーデータ入れ替え機構は，LKM (Loadable Kernel Module) として実現



OS の再構築なく機密情報の拡散追跡機能と連携可能

現在，機密情報の拡散追跡機能との連携は未完成である

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

評価

■ 目的

(1) 機密情報の漏洩の防止すること

(2) 攻撃者の計算機の情報を取得すること

■ 評価内容

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

(1) 攻撃者の計算機の OS は，Windows であると想定

(2) 探査プログラムは実行ファイル (exe形式) として作成

■ 探査プログラムの動作

(1) 指定した計算機とコネクションを確立

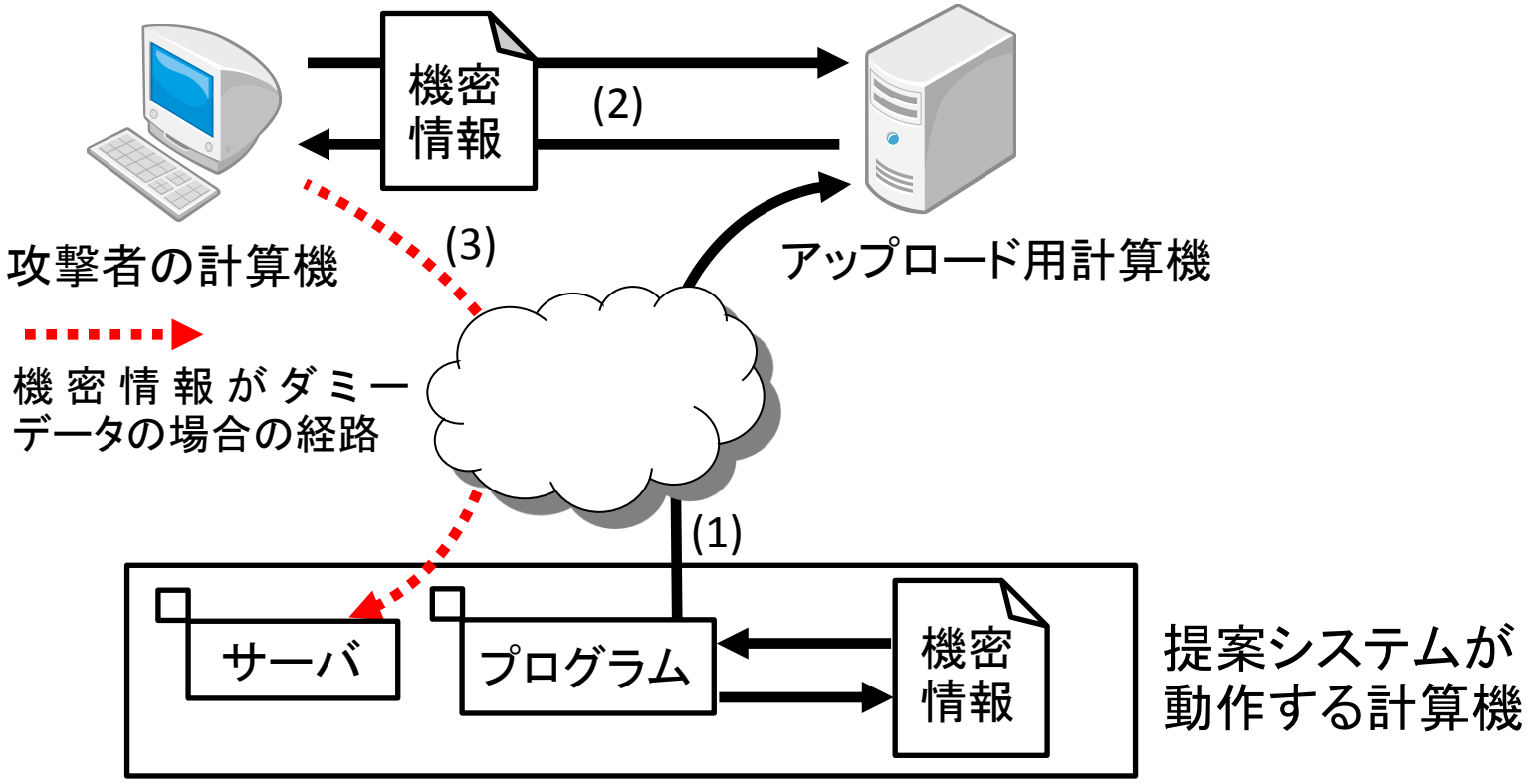
(2) 攻撃者の情報を取得

(3) コネクションを確立した計算機に攻撃者の情報を送信

■ 提案システムが動作する環境

CPU	Intel Core i7-3700 (3.40 GHz)
メモリ	4.0 GB
カーネル	Linux 3.4.9

実験



(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
(2) 攻撃者の計算機から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へ移動
(3) 攻撃者の計算機上で機密情報を開く

実験結果

■ ダミーデータについて

攻撃者の計算機上で取得したダミーデータは，攻撃対象の計算機上の機密情報のファイル名とファイルサイズと一致

	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
ダミーデータ	secret_file	102,400

■ 攻撃者の情報の取得について

取得した機密情報の拡張子を exe に変更 (secret_file.exe) して開く

探査プログラムがコネクションを確立させた計算機上で攻撃者の情報を受信

機密情報の漏洩の防止と攻撃者の情報を取得できたことを確認

まとめ

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

(1) 機密情報の拡散追跡機能

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，計算機内の機密情報を追跡

(2) ダミーデータ入れ替え機構

(A) 機密情報が外部へ送信させ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

(B) ダミーデータに埋め込んだ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

(3) 評価

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

⇒ 機密情報の漏洩の防止と攻撃者の情報の取得を確認

(4) 今後の課題

効果的な探査プログラムの実行方法