Vol.2013-CSEC-62 No.53
Vol.2013-SPT-6 No.53
2013/7/19

組織内ネットワークにおける標的型攻撃の検知方式

山田正弘† 森永正信† 海野由紀† 鳥居悟† 武仲正彦†

近年，標的型攻撃と呼ばれるサイバー攻撃による被害が急激に増加しており，効果的な検知技術の実現が急務である．標的型攻撃では，標的組織のネットワーク内部における内部攻撃の方法が明らかになっておらず，加えて，新たに開発された新種や，既知の攻撃ツールがカスタマイズされた亜種の攻撃ツールが利用されるため，攻撃ツール毎に特徴を定義する従来の検知技術では検知できない．このような背景から，本論文では，攻撃ツールの種類に関わらず，標的型攻撃を検知できる技術の実現を目指し，組織内ネットワークにおける内部攻撃の方法を調査，分析し，その結果に基づく内部攻撃の検知方式を提案する．具体的には，第一に，実際に著名な RAT，および組織内ネットワークでの攻撃に利用される Pass-the-hash 攻撃に関連するツールを調査，分析した．この結果から，攻撃ツールによって発生する通信は通常業務に偽装され，攻撃との判別が難しいことと，一方で，内部攻撃は RAT の機能と SMB 管理ツールの連携によって行われることを明らかにした．第二に，分析結果に基づいて内部攻撃を検知する方式を設計して評価を行い，調査した限りで，新種や亜種の攻撃ツールを利用する場合にも，提案方式が標的型攻撃における内部攻撃を検知できることを確認した．

A Detection Method against Activities of Targeted Attack on The Internal Network

Masahiro Yamada† Masanobu Morinaga† Yuki Unno†
Satoru Torii† Masahiko Takenaka†

The recent increase of incidents caused by targeted attacks has realization of countermeasures against them imperative. Since attackers use self-developed tools or customized tools for targeted attacks, traditional signature-based detection doesn't work against them. In addition, activities of targeted attack on the internal network are not clear. In this paper, first, we analyze the tools used in the actual incidents, and reveal the attacking methods and their features of activities on the internal network. As a result, attackers use SMB-based remote administration tools in combination with RAT. Second, we propose a detection method based on the features. Our experiments indicate that, the proposed method can detect activities of targeted attack on the internal network, despite self-developed or customized tools.

1. はじめに

近年，標的型攻撃と呼ばれる，特定組織の機密情報を標的としたサイバー攻撃による被害の急増が問題となっている [1]．標的型攻撃は，標的組織のネットワーク内部に侵入した後，ネットワーク内部での攻撃 (以下，内部攻撃) を繰り返しつつ，長期間に渡って機密情報を窃取し続け，徐々に被害が拡大する特徴がある．被害の発覚まで平均 416 日を要し，40 台程度のホストが不正侵入されることが報告されている [2][3]．このため，内部攻撃を検知する技術の開発が急務である．

文献[2]によれば，標的型攻撃では，標的組織内のホストをリモート制御するために RAT (Remote Access Trojan)，また，内部攻撃において Pass-the-hash 攻撃に関連するツールが利用される．しかし，これらのツールに共通する動作や機能，また，それらを組み合わせる攻撃方法や特徴は明らかでない．さらに，文献[3]によれば，これらのツールは攻撃者によって新たに開発され，または既存のツールがカスタマイズされて攻撃に利用される．このため，既知の攻撃ツールのファイルや通信データの定義を利用する，従来の検知技術 [4][5][6]では攻撃が検知できない．

このような背景から，本研究では，標的型攻撃を検知する技術の実現を目的とし，標的型攻撃における組織内ネットワークでの攻撃方法の調査と分析を行い，さらに，分析結果に基づく検知方式を提案する．より具体的には，第一に，実際に標的型攻撃で利用された実績のある RAT，および内部攻撃に利用されたツールを調査し，それらを組み合わせた攻撃方法や特徴を明確にする．第二に，この特徴に基づいて通信を解析し，標的型攻撃における内部攻撃を検知する方式を設計する．加えて，提案方式を実装し，新種または既知の攻撃ツールの亜種を利用する場合でも，内部攻撃が検知できることを評価する．

以下，2 節では，標的型攻撃を検知するための課題を整理する．3 節で，RAT 等の標的型攻撃に利用されるツールを調査し，それらの組み合わせによる，組織内ネットワークにおける内部攻撃の方法や特徴を明らかにする．4 節で，内部攻撃の特徴に基づいて，攻撃を検知する方式を提案した後，5 節で，提案方式を評価する．6 節では，関連研究を概説し，7 節で本論文の結論をまとめる．

† 株式会社富士通研究所
FUJITSU LABORATORIES LTD.

Vol.2013-CSEC-62 No.53
Vol.2013-SPT-6 No.53
2013/7/19

2. 標的型攻撃検知の課題

前述のように，標的型攻撃では，攻撃者が新たに開発した新種のツール，またはカスタマイズされた既知のツール(以下，亜種)が利用される．一方で，従来の攻撃検知技術は既知の攻撃ツールの定義に基づいて攻撃を検知する．例えば，従来のネットワークベースの検知技術 [4][5]では，攻撃ツール毎に固有の通信データをリストとして保持している．ネットワークを流れる通信データとリストの比較により攻撃ツールを検知する．攻撃ツールの定義に基づく従来の技術では，定義されていない新種のツールは検知することができない．加えて，既知の攻撃ツールであっても，カスタマイズされ，通信データやファイル等が定義と異なる亜種は検知できない．

以上から，新種や亜種の攻撃ツールを利用する場合にも，攻撃を検知する方式が必要である．本研究では，標的型攻撃における内部攻撃で，攻撃ツールに依らず，攻撃者が利用する攻撃方法の特徴に着目する．このために，内部攻撃に利用されるツールに共通の機能や，それらを利用する攻撃方法と，攻撃の際に必ず現れる特徴を明確にする必要がある．

3. 内部攻撃方法の調査と特徴の分析

本節では，標的型攻撃で利用される RAT や Pass-the-hash 攻撃ツールを調査，分析し，それらの組み合わせによる，組織内ネットワークでの内部攻撃の方法や特徴を明確にする．以下，それぞれのツールの分析結果を整理した後に，内部攻撃の方法や特徴を説明する．

3.1 RAT

一般に，標的型攻撃では RAT が利用される．RAT はサーバとクライアントから構成され，RAT クライアントから RAT サーバが動作するホストに対して，ネットワークを介して，リアルタイムに様々な操作を行う (以下，リモート制御)ツールである．本研究では，主要な RAT を収集して動作させ，それらの機能を分析した．中でも，Poison Ivy は亜種や類似の RAT を含め，2012 年の国内標的型攻撃事例の約 5 割で利用された報告がある [7].

これらの RAT を分析した結果，共通する代表的な動作や機能を表 1 にまとめる．まず，RAT に共通する動作として，リモート制御の通信コネクションは RAT サーバから RAT クライアントに向けて構築され，攻撃者が設定したポート番号で暗号通信が行われる．このため，RAT の通信は，一般的な HTTPS の Web アクセスに偽装された場合に，検知が難しい．

また，共通する機能として，ユーザのキー操作情報やスクリーンショット，Web カメラによる撮影，マイクによる録音等の情報奪取に関する多数の機能がある．加えて，感染ホストのファイルやプロセス，レジストリ，サービス等の情報も参照，制御する機能がある．これらの機能によって，攻撃者が感染ホストの状況を把握し，状況に応じて攻撃を隠蔽し続けることを可能にしていると推測される．さらに，ファイルのアップロードや，コマンド，プログラムを実行する機能があり，新たに攻撃ツールをアップロードして実行することで，RAT の遠隔操作と他の攻撃手法を組み合わせることが出来る．

表 1　RAT の機能調査結果
Table 1 Result of analysis of RAT

RAT	A	B	C	D
通信開始時の接続元	サーバ	サーバ	サーバ	サーバ
通信プロトコル	独自	独自	独自	独自
通信コネクション維持	あり	あり	あり	あり
通信暗号化	あり	あり	あり	あり
通信 TCP ポート番号	任意	任意	任意	任意
ファイルのダウンロードアップロード	可	可	可	可
任意のコマンド/プログラムの実行	CLI/GUI	GUI/CLI	CLI	CLI
レジストリ参照/編集	可	可	可	可
サービス参照/開始/停止	可	可	可	可
プロセス参照/kill	可	可	可	可
インストールされているアプリ参照/削除	可	可	可	可
アクティブポート参照	可	可	可	可
OS シャットダウン/再起動	不可	可	不可	不可
キーロガー	可	可	可	可
スクリーンショット	可	可	可	可
Web カメラ撮影	可	可	可	可
マイク録音	可	可	可	可

RAT に共通する機能は，時々刻々と変化する感染ホストや組織内ネットワークの状況に応じて，攻撃者がリアルタイムに情報を取得して，検知されずに攻撃を行い続けることに特化している．このようなリアルタイムな遠隔制御を行うため，RAT は，攻撃者からの指令を随時受け付けて実行できるように，一度構築した TCP コネクションを維持し続けるという特徴がある．このため，一般的な HTTP や HTTPS の Web アクセスと比較して，コネクションの継続時間が長いという特徴がある．

3.2 Pass-the-hash 攻撃ツール

標的型攻撃では，内部攻撃において Pass-the-hash 攻撃 [8] が応用されることが知られている [2]. Pass-the-hash 攻撃は，Windows が管理するログインパスワードのハッシュ値 (以下，パスワードハッシュ)を奪取し，パスワードハッシュを

利用して，権限昇格や他のホストへネットワーク経由で侵入する攻撃手法である．パスワードハッシュは，ローカルホストやドメインへのログオン，その他の Windows 標準のサービスにおける認証で利用される．これらの認証手続きでは，パスワードハッシュを使用してチャレンジ・レスポンスの計算を行う．このため，攻撃者が，奪取したパスワードハッシュから平文のパスワードを解析する必要が無い[9].

本研究では，主要な Pass-the-hash 攻撃ツールを収集して動作させ，これらに共通する機能を分析した．分析結果を表 2 に示す.

表 2　Pass-the-hash 攻撃ツールの分析結果
Table 2 Result of analysis of Pass-the-hash tools

攻撃ツール	パスワードハッシュ奪取	カレントユーザの権限昇格	ネットワーク経由で侵入
(1)	lsass.exe	可	不可
(2)	lsass.exe	可	不可
(3)	lsass.exe	可	不可
(4)	SAM	不可	不可
(5)	SAM	不可	不可
(6)	SAM	不可	不可

表 2 にあげた Pass-the-hash 攻撃ツールは，Windows が管理する SAM (Security Account Manager)データベース，または，lsass.exe (LSASS: Local Security Authority Subsystem Service)というプロセスからパスワードハッシュを奪取する．SAM データベースには，全ローカルユーザのパスワードハッシュが格納されており，lsass.exe には，ログイン中のユーザのパスワードハッシュが格納されている．表 2 には，各ツールの動作から推定されるハッシュ値奪取手法を記している．

一部の Pass-the-hash 攻撃ツールでは，lsass.exe が管理するカレントユーザのパスワードハッシュを，より権限の高いユーザのパスワードハッシュに書き換えることで，権限昇格を行う機能を有する．

また，表から，Pass-the-hash 攻撃ツールはパスワードハッシュの奪取やカレントユーザの権限昇格に特化しており，他のホストへ侵入する機能がないことが分かる．よって，奪取したパスワードハッシュを用いてネットワーク経由で侵入する場合には，他のツールを併用せざるを得ない．

3.3 侵入時の通信プロトコル

奪取したパスワードハッシュが認証に利用できるのは，Windows 標準のサービスである，SMB (Server Message Block)を利用するリモート管理や，RDP (Remote Desktop Protocol)を利用するリモートデスクトップである．これらのサービスに関するツールとして，SMB のリモート管理では，Microsoft 社が無償で配布する PsExec 等の SMB 管理ツール，リモートデスクトップでは Windows に標準搭載のリモートデスクトップクライアントがあげられる．奪取したパスワードハッシュを用いて，これらのツールを利用することで，攻撃者は侵入したホスト上で任意のコマンドやプログラムを実行可能である．

侵入の候補となる SMB と RDP について，標的型攻撃の内部攻撃において，通常業務との判別と制約の 2 点の観点から整理する．まず，通常業務との判別の観点として，SMB と RDP は共に，通常業務で頻繁に利用されるツールである．このため，いずれのプロトコルにおいても，これらの通信のみで，攻撃と通常業務を判別することは困難であり，攻撃の隠蔽に適している．また，RDP はリモートデスクトップ等，アクセスしたホストに対する制御で利用される．一方で，SMB は Windows のネットワークログオンやファイル共有，ネットワーク上のホスト探索等，多数の Windows 標準機能で利用され，用途が多岐に渡るプロトコルである．このため，RDP と比較して，サーバとクライアントの関係がより複雑であり，SMB での操作内容を解析しない限り，管理者やユーザが攻撃を感知することが難しい．

また，プロトコルの制約の観点として，SMB では，アクセスを受けるホストが一度に許容するセッション数に制限がない．一方で，RDP は許容セッション数に制限があるため，侵入によって，正規ユーザの既存セッションが切断され，正規ユーザが攻撃を感知できる可能性がある．

以上の観点から，SMB が内部攻撃に適したプロトコルであるといえる．よって，本研究では，SMB プロトコルを利用した内部攻撃に着目する．SMB において，リモート制御を特定するためには，前述の通り，SMB 通信の操作内容を解析する必要がある．

3.4 内部攻撃方法

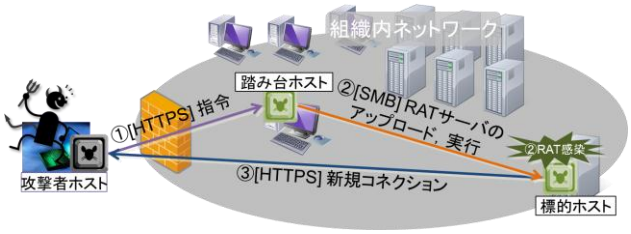

図 1 内部攻撃方法
Figure 1 Method of internal attack

前小節までの内容を整理すると，内部攻撃の攻撃手順は図 1 に示す通りである．まず，攻撃者は，標的組織内の RAT 感染ホスト (踏み台ホスト)で Pass-the-hash 攻撃により，パスワードハッシュを奪取する．次に，奪取したパスワードハッシュを用いて，踏み台ホストから別の内部ホスト(標的ホスト)に侵入して，RAT サーバを実行し，標的ホストを RAT 感染させる．これにより，攻撃者は，新たに標的

ホストをリモート制御することが可能になる．このような内部攻撃を繰り返すことで，攻撃者は感染を拡大し，より多くの機密情報の入手を試みる．

内部攻撃において，標的ホストへの侵入し RAT 感染させる段階は，前節で述べたように，RAT のコマンド実行機能と SMB 管理ツールの組み合わせによって行われると推定できる．この段階において，攻撃者ホストと踏み台ホスト間の RAT 通信と SMB 管理ツールによるリモート管理通信，標的ホストと攻撃者ホスト間の新規の RAT 通信は，図 1 に示すように，攻撃者ホストと踏み台ホスト，標的ホスト間で連動して発生する．

加えて，3.1 で述べたように，RAT 通信は組織外のホストとの通信であり，プロトコルや通信の内容は RAT の種類によって異なるが，コネクションの継続時間が長いという特徴がある．また，パスワードハッシュを用いた SMB での侵入は，通常の SMB のリモート管理通信のシーケンスで行われる．

4. 内部攻撃の検知方式

本節では，内部攻撃において，踏み台ホストでパスワードハッシュが奪取された後の，標的ホストへの侵入，および RAT 感染させる段階の通信を検知する方式を提案する．具体的には，この段階において，攻撃者ホスト，踏み台ホスト，標的ホストの間の一連の通信が順に連動して発生する，通信シーケンスを検出することで，正常な通信に紛れた攻撃を検知する．

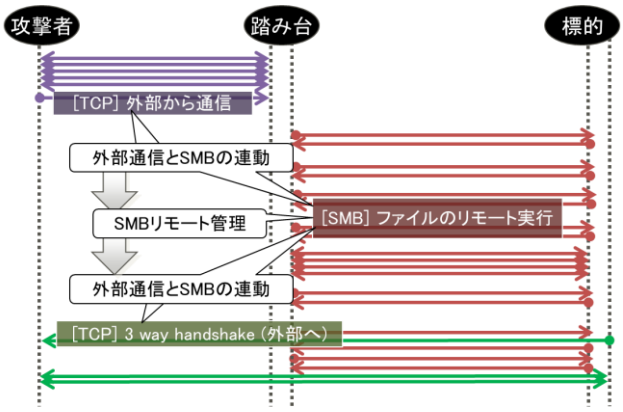

図 2　内部攻撃の通信シーケンス概要
Figure 2 Outline of communication sequence of internal attack

内部攻撃における通信シーケンスの概要を図 2 に示す．本方式は，まず，組織内ネットワークを監視し，SMB リモート管理通信の特徴に該当する通信を抽出する．SMB リモート管理通信が抽出された場合，その直前に発生した外部からの通信で，通信の宛先と SMB リモート管理通信の発信元が一致し，かつ RAT 通信の特徴を満たす通信を候補として抽出する．RAT 通信の特徴は，前節で述べたように，組織内から外部向けに構築された TCP コネクション上の通信であり，かつコネクションの継続時間が長いことである．また，SMB リモート管理通信において，標的ホストに送り込んだファイルがリモート実行された直後に，組織内から外部向けに新たな TCP コネクション構築の通信があれば，候補として抽出する．

このように，SMB リモート管理通信とその前後の RAT 通信の候補を抽出し，それらの通信の送信元と送信先が一致し，一連の通信が 3 ホスト間で連動して発生している場合に内部攻撃として検知する．

5. 評価

本節では，提案方式が新種や亜種の攻撃ツールを利用する場合にも，内部攻撃を検知できることを評価する．以下，評価のために構築した評価環境について説明した後に，評価結果を説明する．

5.1 評価環境

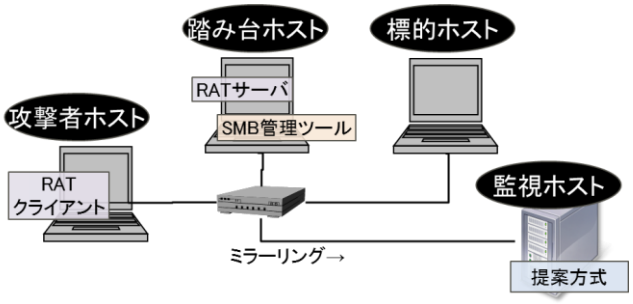

図 3　評価環境
Figure 3 Evaluation environment

評価のために，提案方式のプロトタイプを実装し，図 3 に示すように，プロトタイプが動作する監視ホスト，および攻撃者ホスト，踏み台ホスト，標的ホストが 1 台のスイッチで接続されるネットワークを構築した．攻撃者ホスト，および踏み台ホスト，標的ホストは Windows XP SP3 で構成した．この内，踏み台ホスト，標的ホストでは Windows のファイアウォール機能で，ファイル共有による SMB 通信を許可するよう設定した．監視ホストは CentOS 5.8 で構成し，スイッチの機能により，全ホスト間の通信をミラーリングによって取得し，提案方式による解析を行うよう設定した．

5.2 評価結果

評価では，評価環境に置いて，RAT と SMB 管理ツールを利用して内部攻撃を再現し，提案方式で検知できることを検証する．検証に際し，攻撃者が新たに開発した新種や，既知のツールをカスタマイズした亜種を利用する攻撃の検知を確認するため，既存の Anti Virus ソフトウェア，および，既存のネットワーク侵入検知ツールのどちらでも定義されていない RAT を新種として利用する．また，これらの既存技術で定義されている，既知の RAT を独自にカスタマ

イズした RAT を亜種として利用する．

より具体的に，既知の RAT として，2 節で調査，分析した 4 種類に加えて，新たに入手した 2 種類の既知の RAT と，1 種類の新種の RAT を利用する．加えて，既知の RAT の内，1 種類に関して，RAT サーバファイルを専用のツールによって加工し，通信データを SSL 暗号化ツールによって暗号化した亜種を利用する．

なお，新種の RAT の配布開始時期は 2012 年 10 月である．加えて，評価を行った 2013 年 2 月 1 日の時点で，本評価で使用した既存の Anti Virus ソフトウェア，および，既存のネットワーク侵入検知技ツールでは，亜種の RAT と新種の RAT を利用する内部攻撃が検知されないことを確認している．

また，SMB 管理ツールとして，Microsoft 社が無償で配布している PsExec 2.44，および Power Admin LLC 社が無償で配布している PAExec 1.9 を利用する．

表 3　検知結果
Table 3 Detection result

SMB 管理ツール			PsExec	PAExec
RAT	既知	A	○	○
		B	○	○
		C	○	○
		D	○	○
		E	○	○
		F	○	○
	亜種	G	○	○
	新種	H	○	○

攻撃を再現した際の提案方式の検知結果を表 3 に示す．表から，既知の攻撃，および新種の攻撃のいずれにおいても，RAT と SMB 管理ツールの組み合わせによらず，内部攻撃を検知できていることが分かる．このことから，調査した限りで，新種や亜種の攻撃ツールを利用する場合にも，提案方式が内部攻撃を検知できると言える．

6. 関連研究

既存技術として，攻撃の通信シーケンス，もしくは正常シーケンスを定義しておき，監視対象トラフィックのシーケンスと比較することで攻撃や異常を解析する技術が提案されている．攻撃シーケンスを定義するプロトコル解析としては，Bot 感染時における，攻撃者ホストと感染ホスト間の通信シーケンスを定義することで Bot を検知する技術[10][11]が提案されている．文献[10][11]のように，Bot 感染のシーケンスを定義する場合，定義されたシーケンスに従う Bot や RAT を検知することができる．しかし，感染時における RAT の通信シーケンスは RAT の種類毎に異なり，定義に従わないシーケンスで通信する RAT であれば検知することができない．

一方，正常シーケンスを定義する検知技術 [12]では，定義された正常シーケンスに従わない通信を異常として検知できる．しかし，標的型攻撃における内部攻撃のように，正常な操作を組み合わせて，通常業務の通信に紛れるような攻撃では，異常として検知することが困難である．

これらの他に，解析対象トラフィックのコネクション毎の流量，IP アドレスやポート番号，プロトコルの分布などを特徴量として，特徴量の変化や類似性を解析する技術が提案されている [13][14]．より具体的に，文献[13]では，大規模な DoS 攻撃や DDoS 攻撃，または，ワームのように，トラフィックの特徴量が通常運用のパターンと大きく異なる攻撃を効果的に検知できる技術が提案されている．一方で，通常運用時のトラフィックの特徴と統計的に変化のない今日の Bot，RAT は検知できない．

また，文献[14]では，従来の Bot のように，複数の感染ホストと指令サーバ間で同一の指令と実行結果がやり取りされる場合に，IP アドレスやペイロードの類似性を解析し検知する技術が提案されている．しかし，標的型攻撃の RAT 通信で頻繁に利用される HTTPS 等の暗号通信では，複数の通信内容の類似性は解析できない．

7. おわりに

本論文では，標的型攻撃を効果的に検知する技術の実現に向けて，標的型攻撃における組織内ネットワークでの内部攻撃の方法を調査，分析した．この結果，RAT の通信と SMB リモート管理通信が攻撃者ホストと踏み台ホスト，標的ホストの間で連動して発生するという特徴を明らかにした．さらに，この特徴に基づいて，内部攻撃を検知する方式を提案した．提案方式のプロトタイプを用いた本論文の評価では，調査した限りで，既存の Anti Virus ソフトウェアやネットワーク侵入検知技術で検知できない，新種や亜種の攻撃ツールを利用する場合にも，業務通信に紛れた内部攻撃を検知できることを確認した．

今後，提案方式の検知精度向上に向けて，提案方式における誤検知，および検知漏れに関して，それぞれ評価を行い，方式の改善を検討する予定である．加えて，実装した提案方式のプロトタイプの処理性能に関する評価を行い，改善を検討する予定である．

参考文献

1) C. Tankard: Advanced Persistent Threat and How to Monitor and Deter Them, Network Security, vol.2011, issue.8, pp.16-19 (2011)
2) MANDIANT: M-Trends An Evolving Threat, White Paper (2012)
3) MANDIANT: M-Trends The Advanced Persistent Threat, White Paper (2010)
4) M.Roesch: Snort – Lightweight Intrusion Detection for Network, Proceedings of The 13th USENIX Conference on System Administration, pp.229-238 (1999)
5) V. Paxon: Bro: A System for Detecting Network Intruders in

Real-Time, Computer Networks: The International Journal of Computer and Telecommunications Networking, vol.31, no. 23-25, pp.2435-2463 (1999)
6) K. Ilgun, R. A. Kemmerer, P. A. Porras: State Transition Analysis: A Rule-Based Intrusion Detection Approach, IEEE Transactions on Software Engineering, vol.21, pp.181-199 (1995)
7) Trend Micro: 2012 年国内における持続的標的型攻撃の分析, White Paper (2013)
8) SANS Institute: Pass-the-hash Attacks: Tools and Mitigation, Technical Report (2010)
9) SANS Institute: Why Crack When You Can Pass the Hash?, Technical Report (2009)
10) G. Gu, P. Porras, V. Yegneswaran, M. Fong, W. Lee: BotHunter: Detecting Malware Infection Through IDS-driven Dialog Correlation, Proceedings of 16th USENIX Security Symposium, pp.167-182 (2007)
11) R. Sekar, A. Gupta, J. Frullo, A. Tiwari, H. Yang, S. Zhou: Specification-based Anomaly Detection: A New Approach for Detecting Network Intrusions, Proceedings of the 9th ACM Conference on Computer and Communications Security, pp.265-274 (2002)
12) S. Yun Lim, A. Jones: Network Anomaly Detection System: The State of Art of Network Behaviour Analysis, Proceedings of The 2008 International Conference on Convergence and Hybrid Information Technology, pp.459-465 (2008)
13) 榊原祐之, 北澤繁樹, 大野一広, 藤井誠司: 定点観測による不正アクセス分析システム, 情報処理学会研究報告 コンピュータセキュリティ, (2006)
14) T. Yen, M. K. Reiter: Traffic Aggregation for Malware Detection, Proceedings of The 5th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pp.207-227 (2008)