Vol.2013-DPS-154 No.19
Vol.2013-CSEC-60 No.19
2013/3/14

おとりを用いた標的型攻撃の検知手法について

北澤 繁樹† 桜井 鐘治†

近年，標的型攻撃が増えている．標的型攻撃とは，標的とする組織や個人を絞り込み，ソーシアルエンジニアリングによってユーザを巧みに騙してプログラムをダウンロード・実行させたり，未知の脆弱性を悪用したりといった手口で標的固有のマルウェアを組織内部の端末へ感染させることにより，機密情報の窃取などを行なうことを目的とした攻撃である．対策としては，これまで行われてきたような，侵入自体を防ぐための入口対策に加え，仮に入口対策が突破され，侵入されてしまった場合であっても情報漏洩の被害を防ぐための出口対策の強化が指摘されている．

本論文では，入口対策と出口対策の中間にあたる，標的内部の情報システムにおける攻撃者の活動を検知することを目的として，ファイルサーバ上に「おとり」となる，ファイルやフォルダを配置しておき，おとりへのアクセスを基に標的型攻撃を検知する方式を提案する．提案方式では，おとりへアクセスしたユーザの挙動が標的型攻撃における一連の事象と照らし合わせて，おとりへのアクセスが標的型攻撃によるものかどうかを判断する．これにより，重大な被害がでる前に，標的型攻撃への対策をとることができるようになる．

A Detection Technique of a Targeted Attack Using a Decoy

SHIGEKI KITAZAWA† SHOJI SAKURAI†

Recently, a targeted attack is increasing. The targeted attack is one that seeks to breach the security measures of a specific individual or organization. Usually the initial attack, conducted to gain access to a computer or network, is followed by a further exploit designed to cause harm or, more frequently, steal data. Countermeasures for the targeted attack are prevention of intrusions at entrance of network, and prevention of information leakage from network exit.

In this paper, we propose a countermeasure which uses decoys of file or folder on a fileserver. In our method, we decide whether the targeted attack is occurring or not, by user's illegal actions who accessed to the decoy. From this reason, we are able to take another countermeasure before serious damage comes out.

1. はじめに

近年，標的型攻撃（APT：Advanced Persistent Threat）が増えている．標的型攻撃とは，標的とする組織や個人を絞り込み，ソーシアルエンジニアリングによってユーザを巧みに騙してプログラムをダウンロード・実行させたり，未知の脆弱性を悪用したりといった手口で標的固有のマルウェアを組織内部の端末へ感染させることにより，機密情報の窃取やなどを行なうことを目的とした攻撃である．

標的型攻撃で用いられるマルウェアは，未知の脆弱性への攻撃や，ウイルス対策ソフトウェアによる検知を回避するよう，標的固有に作られているため，ウイルス対策ソフトウェアによって対策することは難しい．

文献[1]によれば，標的型攻撃（文献[1]では，“新しいタイプの攻撃”と呼んでいる）は，事例ごとに具体的な攻撃手法は異なるものの，大まかな攻撃の流れは，以下の 5 つの段階を経て行われるとしている．

第 0 段階：攻撃準備段階
標的に関する情報（社員のメールアドレスなどの情報）を収集する

第 1 段階：初期潜入段階
収集した情報を基に，メール等の手段を用いて標的内部の端末にマルウェアを潜入させる

第 2 段階：攻撃基盤構築段階
攻撃者の C&C（Command and Control）サーバとのバックドア通信路を確立する

第 3 段階：システム調査段階
確立したバックドアを用いて標的内部のシステム情報を収集する

第 4 段階：攻撃最終目的の遂行段階
目的としている情報へアクセスし窃取する

文献[1]では，上記を踏まえ，第 1 段階において，マルウェアが標的内部へ侵入することを防ぐ対策（入口対策と呼ぶ）に加え，第 2 段階において行われるマルウェアと攻撃者の C&C サーバとの通信や第 4 段階における情報の窃取を防ぐ対策（出口対策と呼ぶ）を行うことの重要性が述べられている．これは，標的型攻撃の攻撃者が，ウイルス対策ソフトウェアなどの入口対策をすり抜けて標的内部まで侵入してしまったとしても，その後にもたらされる情報漏洩などの被害を，出口対策によって防ぐことで対応するという考え方である．しかしながら，標的型攻撃では，マルウェアと攻撃者の C&C サーバとの通信に, HTTP や HTTPS など，一般的に組織内部からインターネットへの通信が許可されたプロトコルが用いられる．したがって，出口対策では，大量に発生している正規の通信の中から，標的型攻撃に関係した通信を抽出する必要があり，抽出の方法によ

† 三菱電機株式会社 情報技術総合研究所
Mitsubishi Electric Corporation, Information Technology R&D Center

Vol.2013-DPS-154 No.19
Vol.2013-CSEC-60 No.19
2013/3/14

っては，誤検知の多発や検知漏れが発生する．そのため，一口に出口対策を強化するといっても容易なことではない．

入口対策および出口対策は，それぞれ，攻撃者が標的内部へ侵入を試みた場合や標的内部から C&C サーバへ通信した場合を検知するものである．つまり，攻撃者が標的型攻撃の一連の流れにおいて，特定のアクションを起こした場合に検知もしくは防御するものである．したがって，攻撃者が標的内部に潜伏している期間，つまり，標的型攻撃の一連の流れにおける「第 3 段階：システム調査段階」でば，対策として「待ち」の状態となっているといえる．

標的型攻撃の一連の流れにおいて，「第 3 段階：システム調査段階」は，最も長期に渡るとされる．なぜなら，標的に侵入直後の攻撃者は標的内部のシステムに関する情報持っておらず，1 つ 1 つ情報を収集していく必要があるためである．加えて，目立つ動作を行うと，標的に気づかれる恐れがあるため，大量のパケットを送信する探査ツールなどによる端末の調査など，効率的な情報収集活動ができないことも長期化する一因であると考えられる．

そこで，我々は，標的型攻撃の第 3 段階において，攻撃者が標的内部のシステム情報を収集する際に探索を行う点に着目し，「おとり」を用いて標的型攻撃を検知する方式を提案する．

「おとり」としては，ファイルサーバ上のファイルやフォルダを用いる．攻撃者は，ファイルサーバにアクセスした際に，どれがおとりのファイルで，どれが正規のファイルであるか，見分けることができない．しかしながら，正規のユーザは，自分がアクセスすべきファイルについては分かるため，操作ミスなどを除けば，おとりのファイルにアクセスする可能性は少ない．おとりに関するこの特徴を利用して標的型攻撃を検知する．

本論文の構成は，次の通りである．まず，2 節で「おとり」を用いた攻撃検知に関する関連研究について触れ，3 節で提案方式について説明する．その後，4 節で提案方式に関する考察を行い，5 節で本論文をまとめる．

2. 関連研究

ファイルサーバ上で，ファイルをおとりとして使う既存の方式として，“honeyfiles”が文献[2]で提案されている．

honeyfiles では，例えば，“passwords.txt”のように，攻撃者の興味を引くような名前のおとりファイルを，NFS（Network File Server）上に設置しておき，ユーザがおとりファイルにアクセスした場合に検知する．

honeyfiles では，「悪意のあるユーザのみおとりにアクセスする」という前提に基づいて検知を行う．したがって，おとりファイルにアクセスしたユーザが，本当に悪意があるのか（マルウェアに感染し，なりすまされている場合も含む），または，設定ミスや操作ミスなどの人為的な要因によってアクセスしたのかについては関係なく，単におとりファイルへアクセスしたという事象を観測しただけで判別するため，誤検知が発生する可能性がある．端的な例としては，ファイル検索が挙げられる．あるフォルダ以下のファイルに対して検索をかけた場合，検索ツールは，検索対象のファイルが，おとりファイルであるか，または，正規のファイルかを区別せずにアクセスするため，誤検知が発生する．

そこで，本論文では，おとりファイルやおとりフォルダへのアクセスのみで検知を行うのではなく，おとりへのアクセスが発生したことをトリガとして，そのユーザの挙動を監視し，標的型攻撃に繋がるような不審な行動が他に観測されていた場合に検知する．

3. 提案方式

3.1 システム概要

本節では提案方式のシステム構成について述べる．図 1 に，提案方式のシステム環境を示す．図 1 において，標的型攻撃検知サーバが，提案方式を実装したサーバである．図 1 に示すように，標的型攻撃検知サーバは，ファイルサーバへアクセス可能な内部のサーバとして配置される．

ファイルサーバ上のファイルやフォルダは，認証サーバによる適切なユーザ認証に基づいたアクセス制御の設定がなされているものとする．したがって，アクセス権が無いユーザがフォルダやファイルにアクセスした場合には，アクセスが拒否されたログがログデータベースに記録される．この他，アクセスが許可された場合にもログが記録される．

図 2 に，標的型攻撃検知サーバの構成図を示す．標的型攻撃検知サーバには，大きく分けて，おとり生成管理機能と，ログ収集分析機能の 2 つの機能がある．おとり生成管理機能とログ収集分析機能は，それぞれ以下のデータベースを備えている．

おとり生成管理機能

- おとり情報データベース
  設置したおとりファイルやおとりフォルダのパスと設置したファイルサーバ名が格納されている．
- おとりデータベース
  おとりのベースとなるファイルやフォルダ（圧縮ファイル）が格納されている．

ログ収集分析機能

- ログデータベース
  ファイアウォール，プロキシ，メールサーバ，認証サーバ，ファイルサーバ，端末など，様々な機器から収集したログが格納されている．
- 挙動パターンデータペース
  標的型攻撃によって，内部ネットワークに攻撃者が侵入した場合に観測される事象のパターンが挙動パターンとして格納されている．

挙動パターンデータベースに格納されている，挙動パタ

ーンとしては，例えば，「同じ端末から複数の異なるユーザでの認証が行われている」，「特定のユーザアカウントによるファイルやフォルダへのアクセス拒否が普段よりも多く発生している」，「特定端末から不審な Web サイトへ頻繁にアクセスしている」，「端末を利用しているユーザが不審なメールを受信していた」などがある．

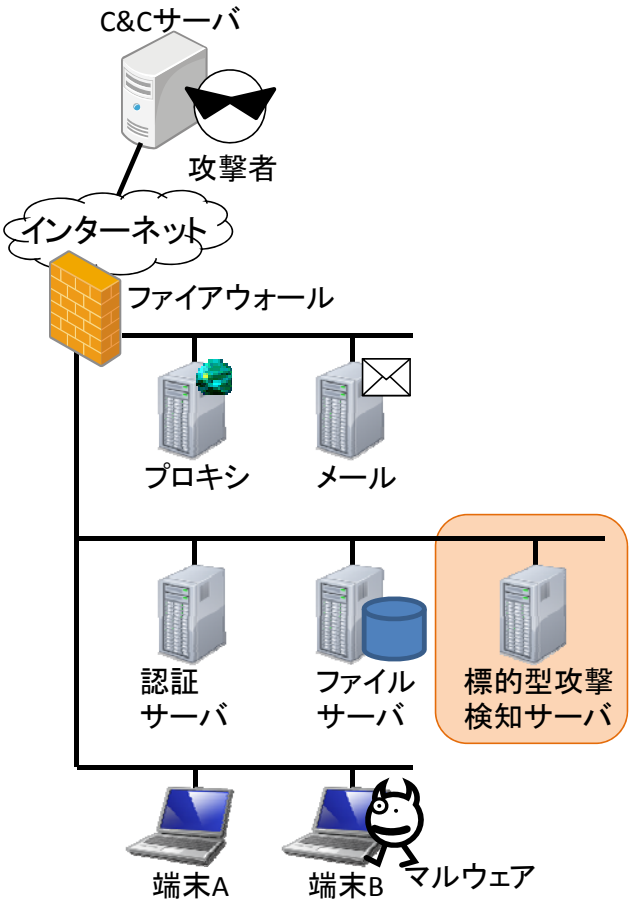

図 1 提案方式のシステム構成

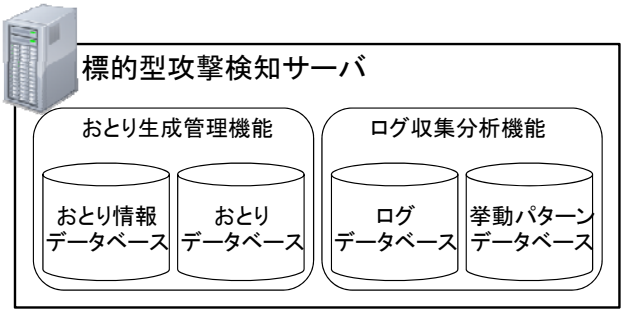

図 2 標的型攻撃検知サーバの構成図

3.2 動作の流れ

3.2.1 おとり生成手順

図 3 は，標的型攻撃検知サーバのおとり生成管理機能の動作を示すフローチャートである．なお，おとり作成は，定期的もしくはランダムな時間間隔で動作するものとする．

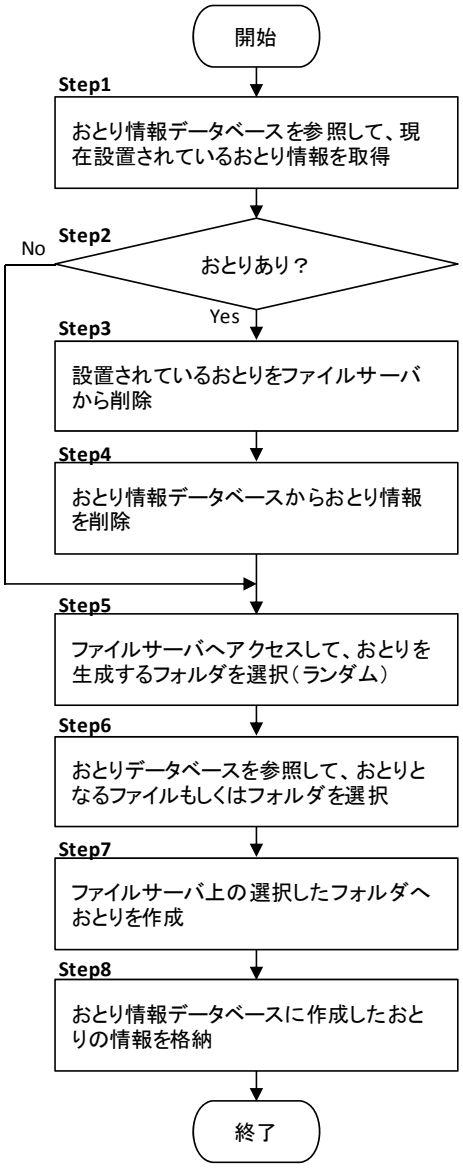

図 3 おとり作成動作のフローチャート

以下に，図 3 における各 Step について説明する．

Step 1 ：おとり情報データベースを参照して，ファイルサーバ上に設置されているおとり情報を取得する．

Step2 : 取得したおとりの設置パス上におとりがあった場合に Step3 へ進み，無かった場合には Step5 へ進む．

Step3 : 設置パス上に設置されていたおとりをファイルサーバから削除する．

Step4 : おとり情報データベースから，ファイルサーバから削除したおとりのおとり情報を削除する．

Step5 : ファイルサーバへアクセスして，おとりを作成する任意のフォルダをランダムに選択する．

Step6 : おとりデータベースを参照して，おとりとなるフォルダもしくはファイルをランダムに選択する．

Step7 : おとりを作成するフォルダへおとりを作成する．

Step8 : 最後に，作成したおとりのおとり情報を，おとり情

報データベースへ格納して，終了する．

なお，Step7 において，おとりのファイル名やフォルダ名は，攻撃者が興味を持ってアクセスしそうな名前にしておくことで，おとりによる侵入の検出率を上げることができる．

3.2.2 標的型攻撃検知手順

図 4 は，おとり生成管理機能によって生成されたおとりに対してアクセスが発生した場合の，ログ収集分析機能の動作を示すフローチャートである．

おとりへのアクセスの発生は，ファイルサーバから送られてくるアクセス制御のログを監視し，おとり情報データベースに格納されているおとり情報と一致するアクセス制御のログを受信した場合に，おとりへのアクセスが発生したと判断する．

以下に，図 4 における各 Step について説明する．

Step1：カウンタ X の値を 0 に初期化する．

Step2：挙動パターンデータベースから，挙動パターンを 1 つ読み込む．

Step3：挙動パターンの読み込みに成功した場合は Step4 へ進み，読み込みに失敗（全ての挙動パターンについて読み込みを完了）した場合には，Step7 へ進む．

Step4：アクセス制御のログから，おとりにアクセスしたユーザ及び端末を特定し，その情報を基に，ログデータベースを検索する．

Step5：ログデータベースを検索した結果，読み込んだ挙動パターンと一致する事象が発生していた場合は，Step6 へ進み，発生していなかった場合は，Step2 へ戻り，次の挙動パターンの読み込みの処理を行う．

Step6：カウンタ X に 1 を加算してから，Step2 へ戻り，次の挙動パターンの読み込みの処理を行う．

Step7：Step2～Step6 を繰り返し，全ての挙動パターンについて一致する事象の有無を確認した後に，カウンタ X の値が，予め決められている閾値以上だった場合は，Step8 へ進み，閾値以下であった場合は終了する．

Step8：カウンタ X の値が，予め決められている閾値以上だった場合，挙動パターンへの一致度が高いとして標的型攻撃発生と判定する．

なお，Step7 において，カウンタ X の値が閾値未満だった場合は，発生したおとりへのアクセスは，正規のユーザによる操作ミスや設定ミスなど無害なものであったと判定する．

Step5 において，挙動パターンに一致する事象の発生の有無を確認している．以下に，3.1 節で挙げた挙動パターンの例について，「挙動パターンに一致」と判断する際の判断方法について説明する．

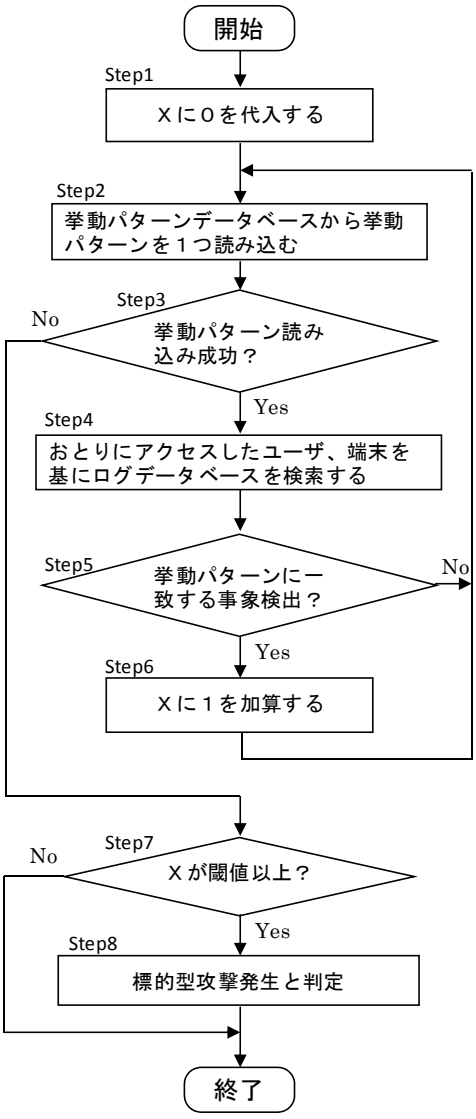

図 4 標的型攻撃検知動作のフローチャート

- 同じ端末から複数の異なるユーザでの認証が行われている
  - 認証サーバのログから，IP アドレスやホスト名で特定される同一端末とユーザの組み合わせが複数記録されているかについて確認する．なお，複数人で共有している端末等については，ホワイトリストで除外する．
- 特定のユーザアカウントによるファイルやフォルダへのアクセス拒否が普段よりも多く発生している
  - 普段ファイルやフォルダへのアクセス拒否のログが 1 ユーザ当たり発生する数を基に閾値を設定し，閾値以上のアクセス拒否が発生しているか確認する．
- 特定端末から不審な Web サイトへ頻繁にアクセスしている
  - 悪意のあるサイトの URL 一覧をブラックリストとして登録しておき，同じ端末から閾値以上ブ

ラックリストに記載されているURLにアクセスした形跡があるか確認する．

- 端末を利用しているユーザが不審なメールを受信していた
  - ブラックリストに，標的型メールで使われる頻度の多い単語を登録しておき，インターネットから送信されてきたメールの件名，本文，添付ファイル名などの文字情報と比較して一致するか確認する．

提案方式では，おとりへのアクセスの有無により，内部ネットワークへ攻撃者が侵入した疑いのあることを検出し，それをトリガとして，おとりへアクセスしたユーザや端末に関する挙動パターンに一致するかどうかで，おとりへのアクセスが標的型攻撃によるものかを判別しているため，標的型攻撃よる攻撃者の侵入を検知できる．

4. 考察

3 節では，提案方式に関するシステム概要と動作の流れについて説明した．動作の流れでは，以下の 2 つの手順について説明した．

- ファイルサーバ上におとりを生成する手順
- おとりを使って標的型攻撃を検知する手順

おとりを生成する手順で重要となるのは，攻撃者に，ファイルやフォルダがおとりであることを見破られないようにすることである．攻撃者が，ファイルサーバ上に保存されている目的のファイルやフォルダを探索する際に手掛かりにできる情報は限られており，せいぜい，名前や保存されているファイルパス程度である．後は，実際にファイルやフォルダにアクセスして，保存してある内容を見て確認するしか手段がない．3.2.1 節では，おとりのファイル名やフォルダ名を，攻撃者が興味を持ってアクセスしそうな名前にしておくことで，おとりによる侵入の検出率を上げることができることを述べた．しかしながら，通常，ファイルサーバ上のフォルダの中には，そのフォルダ名で関連付けられた類似のフォルダやファイルが格納されているため，別の角度から見れば，特に重要な機密と関係が無さそうに見えるフォルダの中に，いかにも機密情報が保存されていそうな名前のファイルやフォルダが保存されていた場合，逆に，おとりではないかと攻撃者に疑われてしまう可能性がある．

そこで，おとりを生成する場合に，おとりとなるファイルやフォルダの名前を，おとりを設置するフォルダに保存されている正規のファイルやフォルダの名前を基に，類義語辞書引いて，おとりの名前を決定することを考える．

例えば，「店舗一覧」という名前のフォルダには，「○○店」，「××店」といった類似した名前を持つフォルダやファイルが格納されていると推測される．この場合，おとりの名前としては，正規のファイルやフォルダに類似した，「□□店」とすることによって，ファイルサーバ内を探索している攻撃者に違和感を持たれない名前のおとりを設置できる．

また，おとりファイルの名前だけを変更するのではなく，おとりファイルが内部に格納している文字情報，画像情報や数値データなどのコンテンツについても，おとりファイルの名前から類推できる代表的なコンテンツに変更するようにしておくことによって，攻撃者に対してより，おとりを気づかれにくくすることができる．

この場合は，おとり生成管理機能は，単語に対応付けられる代表的なコンテンツを内部に格納しておき，おとりファイルの名前に含まれる単語に対応するコンテンツをも用いておとりを作成する．これにより，攻撃者に対して，おとりファイルやフォルダがおとりであることを，見分けにくくすることができる．

次に，標的型攻撃の検知手順について考察する．3.2.2 節で示した標的型攻撃検知動作のフローチャート（図 4）では，おとりへアクセスユーザの挙動が挙動パターンに一致するごとに，カウンタ X の値に 1 を加算していき，カウンタ X の値が閾値を超えた場合に，標的型攻撃の発生として検知している．

カウンタ X の値に 1 を加算していくということは，つまり，挙動パターンデータベース内に定義されている様々な挙動パターンを一律同じ重みで評価している．しかしながら，標的型攻撃が疑われる挙動には，普段からある程度の頻度で観測されるものから，稀にしか観測されないものまであると考えられる．そこで，それぞれの挙動パターンに対して，スコアを定義しておき，図 4 のフローチャートの Step5 において，ある挙動パターンに一致した場合に，その挙動パターンに対して定義されているスコアをカウンタ X に加算する．挙動パターンにスコアによる重み付けを行うことによって，おとりへのアクセスが標的型攻撃によるものか，より適切に判定することができるようになる．

また，特定端末から不審な Web サイトへ頻繁にアクセスしている場合のアクセス数や，端末を利用しているユーザが不審なメールを受信していた場合の，不審なメールにおける標的型メールで使われる頻度の多い単語の出現数を基にスコアを算出することによって動的なスコアを定義することができる．前者であれば，不審な Web サイトへ頻繁にアクセスしている事象が多く観測されている場合に，後者であれば，不審な度合いが高いメールをユーザが受信していた場合に，カウンタ X の値がより大きな値となる．動的なスコアを用いることにより，標的型攻撃で観測される特徴が顕著に表れている場合に，カウンタ X の値を大きくすることができるため，発生している事象に合わせて適切に標的型攻撃を検知可能である．

Vol.2013-DPS-154 No.19
Vol.2013-CSEC-60 No.19
2013/3/14

5. まとめ

本論文では，入口対策と出口対策の中間にあたる，標的内部の情報システムにおける攻撃者の活動を検知することを目的として，ファイルサーバ上に「おとり」となる，ファイルやフォルダを配置しておき，おとりへのアクセスを基に標的型攻撃を検知する方式を提案した．

提案方式では，おとりへアクセスしたユーザの挙動が標的型攻撃における一連の事象と照らし合わせて，おとりへのアクセスが標的型攻撃によるものかどうかを判断する．これにより，重大な被害がでる前に，標的型攻撃への対策をとることができるようになる．

今後は，有効性を示すため，提案方式を実装後，実環境において試使用することで評価する予定である．

参考文献

1) 独立行政法人情報処理推進機構(IPA):「新しいタイプの攻撃」の対策に向けた設計・運用ガイド（改訂第 2 版）, 2011. http://www.ipa.go.jp/security/vuln/documents/newattack.pdf

2) Yuill, J., Zappe, M., Denning, D. and Feer, F.: Honeyfiles: Deceptive Files for Intrusion Detection, Proceedings of the 2004 IEEE Workshop on Information Assurance, pp.116-122, 2004.