A Countermeasure Against Targeted Attacks Using Visual File Deception and Periodic Log Analysis.

Computer Security Symposium 2020
26 - 29 October 2020

視覚型欺瞞機構と定期ログ分析の併用による標的型攻撃対策

長谷川 翔†1　澤村 遼†1　北川 沢水†1
西川 弘毅†2　山本 匠†2　大木 哲史†1　西垣 正勝†1*

概要：攻撃者に対する内部対策の一つに攻撃者を騙すダミーの情報を配置する欺瞞機構の設置がある．欺瞞機構の設置によって起こる正規ユーザの利便性が低下する問題を低減する手法の先行研究が存在する．しかし，従来の手法では，欺瞞機構へのアクセスは正規ユーザと攻撃者のみを想定しており，正規プロセスが欺瞞機構へアクセスすると誤検知が発生してしまうなど汎用性において不十分な点があった．また，欺瞞機構と侵入検知の機構を同一のシステム上で行うため，システムそのものの乗っ取りに対して課題が残る．本論文では，フォルダアイコン画像の変更機能を用いた視覚型欺瞞機構と欺瞞機構へのアクセスログ等を用いた侵入検知システムを提案する．視覚型欺瞞機構を用いることで正規ユーザの利便性を保ったまま，攻撃を遅延させ，さらに侵入検知システムとして，視覚型欺瞞機構のログ等を基に侵入検知を行うことで，深刻な被害が出る前に攻撃者の侵入を検知することが可能となる．本提案手法は欺瞞機構と侵入検知システムを分けることで，提案システムそのものの乗っ取りに対しても耐性がある．また，正規プロセスが欺瞞機構へアクセスすることで発生する問題も解決した．

キーワード：欺瞞機構，侵入検知，標的型攻撃，ダミーファイル，ログ分析

A Countermeasure Against Targeted Attacks Using Visual File Deception and Periodic Log Analysis.

Kakeru Hasegawa†1　Ryo Sawamura †1　Takumi Kitagawa †1　Hiroki Nishikawa †2
Takumi Yamamoto†2　Ohki Tetsushi †1　Masakatsu Nishigaki †1*

Abstract: Deception is one of against attacker countermeasures. There is previous study on methods to reduce a problem of deterioration usability for authorized users. However, previous study assumes that only authorized users and attackers have access to deception, so it is not versatile enough. In addition, since deception and intrusion detection are performed on same system, there is a problem against hijacking of system itself. This paper proposes visual file deception based on changing folder icon and an intrusion detection using log of deception. Using visual file deception can be used to delay an attack while maintaining usability of authorized users. In addition, intrusion detection can detect an attacker's intrusion based on log before any serious damage is caused. By separating deception and intrusion detection, proposed method is resistant to hijacking of system itself. We also solved the problem that occurs when a legitimate process accesses a deception.

Keywords: Deception, Intrusion Detection, APT, Honneyfile, Log Analysis

1. はじめに

近年，サイバー攻撃の手法は多様化し，その脅威は増加し続けている．特に標的型攻撃と呼ばれる，特定の企業・団体等を標的とするサイバー攻撃は未知の脆弱性の利用やヒューマンエラーを誘うメールなど，より巧妙・多様で執拗になっている. ファイアウォール, ウィルス対策ソフト, IDS 等，従来の対策では内部への侵入を完全に防止することはもはや不可能という現状にある．そのため，攻撃者の侵入やマルウェアの感染等を前提とした防御対策が必要とされている．

その 1 つが欺瞞機構である．欺瞞機構とは，本物に見せかけたダミーのデータ（サーバ，端末，フォルダ，ファイル等）を配置し，攻撃者を欺く防御対策である．欺瞞機構は，万が一攻撃者がネットワークへ侵入したとしても，タールピット（攻撃者がダミーデータへのアクセスが強いられることによる攻撃進行の遅延，攻撃者の労力増加）あるいはハニーポット（ダミーデータへのアクセスをトリガとした侵入の検知，侵入者の行動把握）として機能し，被害の緩和が期待できる．一方，ダミーデータの設置は，正規ユーザの利便性低下を引き起こす. 攻撃者を欺くためには，正規かダミーかを判別するための手掛かりが存在してはならない．しかし，ダミーが精巧になるほど，その虚実の判別は正規ユーザにとっても難しいものとなる．正規ユーザによるダミーデータへのアクセスの増加は，利便性の低下だけでなく，侵入の誤検知にも直結する．

この問題を低減する手法として，文献[1]では，ユーザ端末（PC）のファイルシステムに対する欺瞞機構を対象とし

†1 静岡大学
Shizuoka University
†1 三菱電機株式会社
Mitsubishi Electric Corporation

* nisigaki@inf.shizuoka.ac.jp

て，正規ユーザによるファイル操作中はダミーファイルを非表示とする方法（以下，先行手法）を提案している．しかし，先行手法では，正規ユーザによるファイル操作の有無を「ファイルマネージャ（Windows Explorer）のウィンドウハンドルの有無」によって判断している．すなわち，先行手法はファイルマネージャが起動しユーザがウィンドウを開いている間のみダミーファイルを非表示化する．そのため，正規ユーザがファイル操作を行なっている間は欺瞞機構が働かず，無防備な状態となる．また，PC 内のファイルシステムの利用は正規ユーザと攻撃者のみを想定しており，正規プロセスが欺瞞機構へアクセスすると誤検知が発生してしまうなど汎用性において不十分な点があった．また，ユーザ端末（PC）の中に欺瞞機構を利用した侵入検知機能を PC 内に同一のシステム上で行うため，システム PC そのものの乗っ取りが起こると対処ができない．このように，先行手法には，利便性（誤検知）と安全性（検知漏れ）に対して課題が残る．

我々は，ユーザの端末 PC にダミーフォルダとダミーファイルを配置するタイプの欺瞞機構に焦点を当て，視覚型欺瞞化と定期ログ分析を併用した標的型攻撃対策を提案する．欺瞞化の対象は PC 内のユーザドキュメント（フォルダおよびファイル）であり，正規ユーザはファイルマネージャ（Windows Explorer）を用いて GUI 操作によってユーザドキュメントにアクセスすることを想定している．また，ファイルマネージャを介してのファイルアクセスの際には，意思確認のためのポップアップを表示して，ユーザの同意を求める．提案手法では，ダミーフォルダを識別するための視覚情報をアイコンに付与することにより，正規ユーザがファイル選択を行う際の GUI 操作が阻害されないよう配慮されている．提案手法では，侵入検知の機能を PC の後段に配備した別システムにより実装し，ファイルアクセスログを定期的に分析して侵入の痕跡を検査する．欺瞞機構がタールピットとして機能し，侵入者のファイル探索活動に要する時間を増大するため，定期ログ分析の実施タイミングについてはある程度余裕を持たせた周期を設定することができる．

以降の本論文の構成は次の通りである．まず，2 章では欺瞞機構に関連する先行研究を紹介する．3 章では提案手法を説明する．最後に 4 章でまとめと今後の課題について述べる．

2. 関連研究

2.1 実環境を対象とした欺瞞機構の要件

Yuill らは仮想環境のファイルサーバにダミーファイルを配置し，ダミーファイルへのアクセスが発生した際にアラートを発生させる仕組みを提案した[2]. Yuill らのダミーファイルは既存のファイルを変換して作る簡易的なものであった．

その後，より誘引効果の高いダミーファイルを作成する研究が多くなされた. Witham は実際のファイルのプロパティや設置環境のアクセス動向の統計を参考に，ダミーファイルを作成する手法を提案した[3]．Salem と Stolfo は，偽の個人情報や口座情報などから単語を抽出し，ダミー文書ファイルを作る手法を提案した[4]．Witham は自然言語処理を用いて一見もっともらしいダミー文書ファイルを作成する手法などを提案した[5]. Bowen らはユーザが利用する実環境にダミーファイルを手動で設置する手法を提案した[6]. Voris らは，欺瞞化対象のファイルシステムを調査し，フォルダを利用頻度や機能種別で分類し，効果的なダミーファイルの設置戦略を自動で決定する手法を提案した[7].

しかし，ユーザの実環境へのダミーファイルの配置は，正規ユーザのファイル選択を惑わせる要因となる．また，PC 内では，OS によって自動実行される正規プロセス（以下，OS プロセス）も多数稼動している．例えばアンチウィルスソフトが定期的に全ファイルをフルスキャンする場合，ダミーファイルの存在は，所要時間を肥大させる．すなわち，ユーザの実環境を対象とした欺瞞化は，正規ユーザおよび OS プロセスの利便性を低下させてしまう．更に，正規ユーザが誤ってダミーデータにアクセスしてしまった場合や，OS プロセスによるダミーデータのアクセスは，侵入誤検知の温床となる．この問題に対応するためには，データの虚実を判別するための手掛かりを正規ユーザと OS プロセスのみに伝える工夫が必要となる．

また，ユーザの実環境の欺瞞化を考えるにあたっては，欺瞞機構が「攻撃者の侵入」を前提とした防御策である点にも配慮する必要がある．このため，侵入者も当該環境を自由に操作し得る状況を想定しなければならない．すなわち，実環境内に配備された侵入検知機構は，侵入者によって解除され得る．侵入者は，実環境における正規ユーザの全操作を監視することも可能である．

以上より，ユーザの実環境を欺瞞化する方法を検討する際には，以下の要件に配慮する必要がある．

要件 1）正規ユーザならびに OS プロセスの利便性低下をできるだけ抑える．

要件 2）侵入検知機能については，欺瞞機構が配備されている実環境からできるだけ分離する．

要件 3）欺瞞機構の観測によって露見する「ダミーデータを特定するための手掛かり」をできるだけ小さくする．

2.2 正規ユーザの利便性を考慮した欺瞞機構

青池らは，「攻撃者は遠隔から CUI 操作によって標的 PC を操作する」という事実に基づき，正規ユーザによる GUI 操作時は PC の欺瞞化を解除するという手法（以下，先行手法）を提案している．ファイルマネージャ（Windows Explorer）が起動している間はダミーファイルを不可視にすることによって，正規ユーザの利便性を確保しながら攻撃者を欺く欺瞞機構を実現している[1].

しかし，単純に GUI 操作の有無を基準にするだけでは，PC 内で動作している正規の OS プロセス（例えばアンチウィルスソフト）がダミーファイルにアクセスしてしまう問題に対応できないという点で，要件 1 に対する課題が残る．また，侵入者が正規ユーザの利用中に行動する場合には無防備となる，正規ユーザの利用／非利用に応じて表示／非表示が変化するファイルはダミーファイルであると気付かれるという点で，要件 3 に対する課題が残る．更に，欺瞞機構の中に侵入検知機能が併設されているという点で，要件 2 に対する課題が残る．本稿では，上記の先行研究の個々の課題を緩和する方法を検討していく．

3. 提案手法

3.1 概要

3.1.1 システムモデル

提案手法は，ユーザの実環境を対象とした欺瞞機構である．組織内ネットワーク内のユーザ端末（PC）にダミーフォルダとダミーファイルを配置することによって，各 PC のファイルシステムを欺瞞化する．本稿では，PC の OS は Microsoft Windows を想定する．ユーザドキュメントの防御を目的とし，Documents フォルダ以下のファイルとフォルダが欺瞞化の対象である．

提案手法は，欺瞞機構，イベントログ機構，侵入検知機構によって構成される．欺瞞機構は，正規ユーザの PC のファイルシステムの欺瞞化によって，侵入者に対するターレルピットを実現する．イベントログ機構は，PC のシステム領域で稼働し，PC 内の各種アクティビティを記録する．侵入検知機構は，PC の後段に配備した別システムにより実装され，イベントログを定期的に分析して侵入の有無を検査する．

3.1.2 ユーザモデルと攻撃者モデル

正規ユーザは PC の GUI 型ファイルマネージャ（Windows Explorer）を用い，GUI 操作によって欺瞞化されたファイルシステムへアクセスすることを前提とする．コマンドプロンプトや PowerShell の利用自体は禁止されていないが，フォルダ選択およびファイル選択の操作は必ず Windows Explorer 上で実行することが正規ユーザに求められる．

攻撃者は何らかの方法で正規ユーザの PC に不正ログインし，遠隔から標的 PC を操作する．攻撃者が仮想デスクトップ環境（VDI）を用いて標的 PC を GUI 操作することも可能であるが，標的 PC の画面情報をリアルタイムで受信し続ける場合は，その通信挙動から侵入検知するという前提を置く．このため提案手法は，CUI 操作によって標的 PC のファイルシステムへアクセスする攻撃者を想定する．ただし，必要なタイミングで標的 PC のスクリーンショットを撮り，攻撃者端末側で標的 PC の画面（静止画）を視認することによって，通信量を抑えた形で簡易的に標的 PC の GUI 操作を実現しようと試みる攻撃者が現れ得ることについては，想定に含める．

図 1 フォルダアイコン

PC 内では多数の OS プロセスも稼働している．OS プロセスによる欺瞞化ファイルシステムへのアクセスは，CUI 操作となる．

攻撃者は何らかの方法で標的 PC 内の正規プロセス（ユーザプロセスあるいは OS プロセス）を乗っ取り，このプロセスを介して遠隔から標的 PC を操作することも可能である．この場合も不正ログインの場合と同様，攻撃者は CUI 操作によって標的 PC のファイルシステムへアクセスする形となる．

攻撃者は標的 PC 内に自動実行型マルウェアを設置することも可能である．自動実行型マルウェアによる欺瞞化ファイルシステムへのアクセスは，CUI 操作となる．

3.2 欺瞞機構

3.2.1 視覚型欺瞞化

提案手法は，ユーザ端末（PC）の Documents フォルダ以下にダミーファイルとダミーフォルダを配置する．正規ユーザの利便性に配慮し，Windows OS のフォルダアイコン変更機能を利用して，フォルダの虚実を判別するための視覚的情報をフォルダアイコンに付与する．フォルダアイコンの画像例を図 1 フォルダアイコンに示す．GUI 操作によってファイル選択を行う正規ユーザのみが両者を区別することができる．本稿ではこれを「視覚型欺瞞化」と呼ぶ．Windows OS においては，ファイルアイコンは拡張子と紐づいており，正規ファイルとダミーファイルを視覚的に区別させることはできない．このため，正規フォルダ内にはダミーファイルを配置せず，また，ダミーフォルダ内にはダミーファイルのみを配置する．

3.2.2 ファイルシステムの多重複製

提案手法は，Documents フォルダ以下のフォルダ構造を多重複製するという方法によって，ファイルシステム全体を欺瞞化する．多重度mの複製の結果，各正規フォルダから$m-1$個のダミーフォルダが生成される．$m=2$の場合の欺瞞化のイメージをに示す．フォルダアイコンは，正規フォルダとダミーフォルダが一目見て区別がつくように変更する（図 1 フォルダアイコン）．フォルダ名から正規フォルダかダミーフォルダか推測されないように，m個のフォルダ（1 個の正規フォルダと$m-1$個のダミーフォルダ）に対してランダムに通し番号を振り，正規フォルダ名に通し番号を付すことによってm個のフォルダ名を設定する．

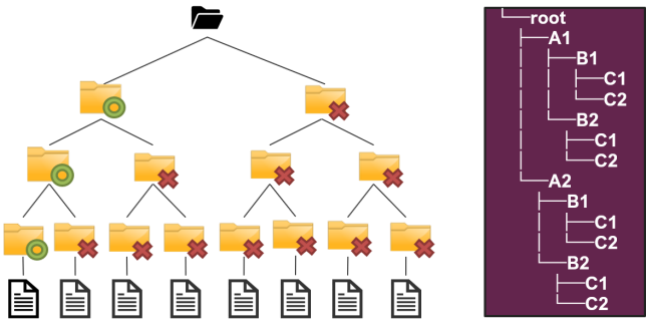

図 2 欺瞞化ファイルシステムの GUI イメージ（左）と CUI イメージ（右）

複製された各ダミーフォルダには，複製元の正規フォルダ内に含まれているすべてのファイルの複製が配置される．ダミーファイルの名前，属性，アイコンは正規ファイルと同じである．しかし，ダミーファイルの中身は正規の情報を含まず，例えば”This is dummy”という情報のみが記録されている．これにより，正規ユーザがフォルダアイコンを見誤ってダミーフォルダにアクセスしてしまったとしても，その中のダミーファイルを開いた時点で自身の誤りに気づくことができる．その一方で，侵入者もフォルダ内のファイルを 1 つ開けば，当該フォルダの虚実を知ることができる．すなわち，提案手法のタールピットの性能は，ダミーファイルの数ではなく，ダミーフォルダの数（複製の多重度m）に依存する．提案手法のタールピット性能を高めるには，多重度mを十分大きく設定する必要がある．

3.2.3 アイコン画像の識別困難化

Windows OS では，アイコン画像を変更したフォルダに関しては，フォルダのプロパティ情報にアイコン画像のファイルパスが記載される．そのため，攻撃者は CUI 操作によってプロパティ情報を参照し，ファイルパスからどのフォルダが正規でどれがダミーか推測することができてしまう可能性がある．この問題に対応するため，提案手法では，すべてのフォルダに対してそれぞれ個別のアイコン画像を用意する．ただし，攻撃者が行うことができるのは CUI 操作のみであり，アイコンを実際に視認することはできないため，フォルダごとに「ファイル名が異なるアイコン画像」を用意しさえすれば良く，絵柄自体は同じでも構わない．

提案手法では，PC の後段に設置された侵入検知機構によって，PC に対する侵入検知が実行される．すなわち，侵入検知機構がダミーフォルダを識別するための仕組みが必要となる1. そこで提案手法においては，正規アイコンかダミーアイコンかを示す情報を，フォルダアイコン画像名（フォルダアイコンのアイコン画像のファイル名）に埋め込む．

図 3 フォルダアイコン画像群

具体的には，欺瞞機構内のすべてのフォルダに対してそれぞれ乱数を割り当て，正規フォルダであれば “g_乱数”，ダミーフォルダであれば “d_乱数” という形で各フォルダの平文アイコン名を生成し，それぞれを AES によって暗号化した文字列に “.ico” の拡張子を連結したものを各フォルダのフォルダアイコン画像名とする．この例をに示す．侵入検知機構が暗号鍵を所持することで，侵入検知機構はフォルダアイコン画像名を復号してフォルダの虚実に関する情報を取得することができる．PC 内には暗号鍵が存在しないので，PC に侵入した攻撃者が当該情報を得ることはできない．

3.3 イベントログ機構

3.3.1 ファイルアクセスログ

欺瞞化されたファイルシステム内のすべてのフォルダおよびファイルへのアクセスを，アクセスログとして記録する．ログには，ファイルアクセスに関する一般的な情報（アクセスの発生時刻，ファイルにアクセスしたユーザ／プロセス，アクセスされたファイルのファイルパス，等）に加え，アクセスされたファイルが配置されているフォルダのファイルアイコン画像名も記録される．

3.3.2 ポップアップログ

侵入者は，ファイルマネージャ（Windows Explorer）を乗っ取り，ファイルマネージャの子プロセスとしてファイル操作を行うことにより，GUI 操作によるファイルアクセスを装うことが可能である．これに対処するために，提案手法では，ファイルマネージャを介してのファイルアクセス（アプリケーションプログラムによるドキュメントファイルのオープン）に対しては，意思確認のためのポップアップを表示して，ユーザの同意を求める．

CUI 操作の侵入者には回答ができないように，視認によってチャレンジ&レスポンスを実行するタイプのポップアップ2 を採用する．侵入者は GUI 操作を装うことができても，実際には画面を視認することはできない．このため，このポップアップに正しく反応することは困難である．

正規ユーザはポップアップを視認し，容易に正答可能である．ユーザにとっては，ファイル削除などの際に表示さ

1 提案手法では，正規フォルダの中に正規ファイルが，ダミーフォルダの中にダミーファイルが配置されるため，ダミーフォルダを識別できればダミーファイルも識別できる．

2 チャレンジ&レスポンス型のポップアップとしては，例えば，確認ボタンが表示される位置が毎回異なるようなポップアップが考えられる．また，画像選択型 CAPTCHA を採用することも可能である．これは，人間と機械を判別するための CAPTCHA を，GUI ユーザと CUI ユーザを判別する目的で利用することができるということを意味している．

れるポップアップと同じイメージである. PC を日頃から利用しているユーザは既にこのような意思確認には慣れていることから，ポップアップへの回答は正規ユーザにとって大きな負担にはならないと考える．また，複数ファイルへのアクセス（例：アーカイブソフトを用いてフォルダ内のすべてのファイルを圧縮）の際はまとめて一つのポップアップとして表示する等，正規ユーザの利便性を保つための配慮は可能な限り取り入れる．

イベントログ機構は，すべてのポップアップの回答を，ポップアップログとして記録する．

3.3.3 スクリーンショットログ

侵入者が，必要なタイミングで PC のスクリーンショットを撮影し，攻撃者端末側で標的 PC の画面（静止画）を視認することによって，視覚型欺瞞機構を回避する攻撃が考えられる．そのため，スクリーンショット要求があった場合は，毎回ポップアップを表示し，スクリーンショットが正規ユーザによって行われているものか意思を確認する．

イベントログ機構は，すべてのポップアップの回答を，スクリーンショットログとして記録する．なお，ポップアップに正しく反応できない場合は，スクリーンショットは許可されない．

3.4 侵入検知機構

3.4.1 定期ログ分析による侵入検知

侵入検知機構は，ファイルアクセスログ，ポップアップログ，スクリーンショットログを定期的に分析し，侵入者の痕跡を検査する．欺瞞機構がタールピットとして機能し，侵入者のファイル探索活動に要する時間が増大するため，侵入検知機構による定期ログ分析の実施タイミングについてはある程度余裕を持たせた周期を設定することができる．

侵入検知機構は，フォルダアイコン画像名を復号するための暗号鍵を所持しているため，フォルダアイコン画像名を復号することによって，アクセスされたファイルが正規ファイル（正規フォルダ内に配置されているファイル）であるかダミーファイル（ダミーフォルダ内に配置されているファイル）であるか判別できる．

ログ分析の結果，以下のいずれかの条件に当てはまった場合，侵入があったと判定し，アラートを発する．

- (ヒューマンエラー発生率以上の頻度で) ダミーファイルへのアクセスが合った場合.
- ポップアップに対する反応がない場合.
- (ヒューマンエラー発生率以上の頻度で) ポップアップへの誤答がある場合.

3.4.2 OS プロセスに関するホワイトリスト

OS によって自動実行される正規プロセス(OS プロセス)は，フォルダアイコンを視認して正規ファイルとダミーファイルを識別することはできず，ポップアップを視認してこれに回答することも不可能である. そこで提案手法では，OS プロセスを「特定のタイミングでドキュメントファイルにアクセスするプロセスか否か」,「特定のドキュメントファイルのみにアクセスするプロセスか否か」の 2 軸の観点で 4 種類に分類し，それぞれのホワイトリストを用意することによって，この問題に対処する．

具体的には, OS プロセスの中で「特定のタイミングでドキュメントファイルにアクセスする OS プロセス」を抽出し，個々のプロセス名とアクセスタイミングを「特定タイミング型 OS プロセス用ホワイトリスト」に登録する．同様に, OS プロセスの中で「特定のドキュメントファイルのみにアクセスする OS プロセス」を抽出し，個々のプロセス名とアクセス先ファイルパスを「特定ファイル型 OS プロセス用ホワイトリスト」に登録する．

2 つのホワイトリストは, 侵入検知機構にて保管される．定期ログ分析の時点でファイルアクセスログが検査される中で，いずれのホワイトリストからも外れたファイルアクセスを行ったプロセスが発見された場合に，アラートを発する. ただし,「任意のタイミングで任意のドキュメントファイルにアクセスする正規の OS プロセス」が存在した場合は, 誤検知が発生してしまう.（これについてはやむを得ないため受容する.）

この結果，攻撃者が「特定のタイミングでドキュメントファイルにアクセスする OS プロセス」を乗っ取って，欺瞞化ファイルシステムへのアクセスを試みた場合,「当該 OS プロセスの正規のタイミング」から外れたタイミングでファイルアクセスをした時点で，そのログから侵入が検知される．同様に，攻撃者が「特定のドキュメントファイルのみにアクセスする OS プロセス」を乗っ取って，欺瞞化ファイルシステムへのアクセスを試みた場合,「当該 OS プロセスの正規のアクセス先」以外のファイルにアクセスをした時点で，そのログから侵入が検知される.（「任意のタイミングで任意のドキュメントファイルにアクセスする OS プロセス」は，正規の OS プロセスであっても「侵入」として誤検知される．このため，攻撃者が「任意のタイミングで任意のドキュメントファイルにアクセスする OS プロセス」を乗っ取って，欺瞞化ファイルシステムへのアクセスを試みた場合も，そのファイルアクセスはすべて「侵入」として検知される.）

4. まとめと今後の課題

本論文では, フォルダアイコン変更機能を用いることで，正規ユーザの利便性を保った欺瞞機構，及び欺瞞機構へのアクセスログ等を用いたログ解析を行い，侵入検知を行う手法を提案し，コンセプトを明らかにした．

提案手法はフォルダアイコンを視認し正規フォルダとダミーフォルダとを判別出来るようにし，GUI を用いる正規ユーザの利便性を保ちつつ，攻撃者に対しては，タールピットとハニーポットとして機能し，被害の緩和が期待できる．侵入者の活動に要する時間を増大させた上で，定期

ログ分析を行い効果的な侵入検知ができる．標的型攻撃対策として欺瞞機構を用いた新たな提案を行った．本手法は標的型攻撃のみならず，多くの攻撃に対応できる効果的な内部対策となる．

本提案には妥当性の検討や誤検知の可能性の追究，それらについてのインパクトの検討，攻撃者への遅延効果の検証，利便性についての具体的な検証，検討や検証を行うべきことが残っている．また，リモートデスクトップ等でGUIが利用可能になった攻撃者に対しての対策が出来ていない等，課題が残っている．今後はこれら検討や検証，課題について取り組む．

参考文献

[1]青池優，神薗雅紀，衛藤将史，松本倫子，吉田紀彦，“欺瞞機構に伴う利便性低下を防止するためのおとりファイル非表示化，” コンピュータセキュリティシンポジウム 2019 論文集, pp.691-696, 2019

[2]Jim Yuill, Michael Zappe, Don Denning and Fred S. Feer, “Honeyfiles: deceptive files for intrusion detection,” in Information Assurance Workshop, Proc. the Fifth Annual IEEE SMC, pp.116–122, 2004

[3]Ben Whitham, “Automating the generation of fake documents to detect network intruders,” Int. J. of Cyber-Security Forensics, Vol.2, No.1, pp.103-118, 2013

[4] Malek Ben Salem, Salvatore J. Stoflo, "Decoy Document Deployment for Effective Masquerade Attack Detection," in Detection of Intrusions and Malware, and Vulnerability Assessment, LNCS, No.6739, Springer, pp35-54, 2011

[5]Ben Whitham, "Automating the Generation of Enticing Text Content for High-Interaction Honeyfiles," Proc. 50th Hawaii Int. Conf. on System Sciences, pp.6069-6078, 2017

[6]Brian M. Bowen, Shlomo Hershkop, Angelos D. Keromytis, and Salvatore J. Stolfo, "Baiting inside attackers using decoy documents," Proc. Inf. Conf on Security and Privacy in Communication Systems, Security and Privacy in Communication Networks, pp.51-70, 2009

[7]Jonathan Voris, Jill Jermyn, Angelos D. Keromytis, Salvatore J.Stolfo, "Bait and Snitch: Defending Computer Systems with Decoys," Proc. Cyber Infrastructure Protection Conference, 25 pages, 2013