Vol.2017-DPS-170 No.16
Vol.2017-CSEC-76 No.16
2017/3/2

文書ファイルを用いた攻撃者情報収集システムの提案

新穂隼人[†1]　佐々木良一[†1]

概要：近年，機密情報を狙った攻撃が問題化している．攻撃手法の一つとして，特定の組織や個人に対して情報窃取等を目的として行う標的型攻撃がある．中でもメールを用いて行う標的型メール攻撃は急激に増加している．機密情報漏洩等のインシデントが発生した際に，インシデントの被害把握や攻撃者を特定するために，攻撃に使用されたマルウェアやコンピュータの通信ログの解析を行うことがある．しかし，これらの解析には時間を要することや解析を行ったとしても十分な情報を得られない場合があり，攻撃者を特定することは困難である．攻撃者を特定することにより，攻撃者を告発することができるだけでなく，攻撃者が新たな攻撃を行うことを防ぐための抑止力となる．攻撃者を特定するために，攻撃者が使用しているコンピュータの情報を取得することが有効な手法として挙げられる．そこで，本研究では，文書ファイルを用いて攻撃者の情報を収集するシステムを提案する．提案システムは，Microsoft Office で使用されるファイルを対象として，VBA(Visual Basic for Applications)を用いる方法と VSTO(Visual Studio Tools for Office)を用いる方法である．提案システムの有効性を示すための実験を通じた考察から VSTO を用いた提案システムがより有効的に本研究の目的を達成できることを確認した．

キーワード：サイバー攻撃，標的型メール攻撃，機密情報，攻撃者情報収集

Proposal of attacker information collection system using document file

HAYATO NIIBO[†1]　RYOICHI SASAKI[†1]

1. はじめに

近年，機密情報を狙った攻撃が問題化している．攻撃手法の一つとして，特定の組織や個人に対して情報窃取等を目的として行う標的型攻撃がある．中でもメールを用いて行う標的型メール攻撃は急激に増加している[1].

機密情報漏洩等のインシデントが発生した際に，インシデントの被害把握や攻撃者の特定のために，攻撃に使用されたマルウェアやコンピュータの通信ログの解析を行うことがある．しかし，これらの解析には時間を要することや解析によって十分な情報を得られない場合があり，攻撃者を特定することは困難である．

攻撃者を特定することにより，攻撃者を告発することができる．また，攻撃者の特定が可能であることを示すことにより，新たな攻撃の発生を防ぐための抑止力になる[2]. これらのことから，攻撃者を特定することは有用であると言える．

攻撃者を特定するために，攻撃者が使用しているコンピュータの情報を収集することが有効な手法として挙げられる．文献[3]では，機密情報が外部へ送信される際に，機密情報とコンピュータの情報を収集するプログラムを埋め込んだダミーデータを入れ替える．このダミーデータを攻撃者が操作することで，攻撃者の情報を収集するシステムを提案している．しかし，この提案システムでは，ダミーデータは実行ファイルの形式になるため，ダミーデータのファイルタイプを調査することにより，窃取したものが機密情報ではないと判断することが可能である．このことから，攻撃者は窃取したものが目的の機密情報ではないことを検知し，ダミーデータを操作しない可能性が高い．つまり，文献[3]の提案システムでは，攻撃者の情報を収集することは困難である．

そこで，本研究では，この問題へ対処するため，文書ファイルの体裁を保ったまま攻撃者の情報を収集するシステムを提案する．提案システムでは，Microsoft Office で使用されるファイルを対象として，VBA(Visual Basic for Applications)を用いて実装する方法と，VSTO(Visual Studio Tools for Office)を用いて実装する方法を示し，評価を行う．

2. 関連研究

2.1 関連研究の概要

攻撃者を特定するために，攻撃者の情報を収集する研究として，前述した文献[3]が挙げられる．文献[3]で提案しているシステムは，主に以下の機能から構成される．

- 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では，機密情報の拡散を追跡し，機密情報が外部へ送信されようとする際に，検知を行う．文献[3]の提案システムでは，文献[4]の方式を利用して機密情報の拡散追跡機能を実現する．

ダミーデータ入れ替え機構では，機密情報の拡散追跡機能で追跡していた機密情報が外部へ送信されようとする際

†1 東京電機大学
Tokyo Denki University

に，機密情報とダミーデータを入れ替える．この機構により，攻撃者にはダミーデータが送信されるため，機密情報の漏洩を防止する．

文献[3]において，攻撃者の情報を収集する方法は，ダミーデータ入れ替え機構によって入れ替えるダミーデータに，攻撃者の情報を収集するプログラムを埋め込み，攻撃者がダミーデータを操作することにより，攻撃者の情報を収集する．

2.2 関連研究の問題点

文献[3]の問題点として，次の 2 つが挙げられる．

- 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がある．
- ダミーデータのファイル形式は実行ファイルの形式となる．

ダミーデータ入れ替え機構において，ファイルサイズの違いから攻撃者に気が付かれることを防止するため，ダミーデータのファイルサイズを外部に送信されようとしている機密情報のファイルサイズに合わせる処理を行う．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も大きい場合，機密情報が読み込まれたバッファにダミーデータを書き込み，機密情報のファイルサイズと一致するまでパディングする．このため，機密情報のファイルサイズと一致する．しかし，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も小さい場合，機密情報が読み込まれたバッファにダミーデータをすべて書き込むことができないため，ダミーデータのファイルサイズまでバッファを拡張してダミーデータを書き込む．このため，機密情報のファイルサイズと一致しない．

文献[3]において，攻撃者の情報を収集するプログラムは，GUI で実行する場合，攻撃者自身がダミーデータをクリックし，開くことで実行する．また，Windows 環境で実行する場合，ダミーデータの拡張子を exe 等の実行ファイルの拡張子に設定する必要がある．これらのことから，ダミーデータは実行ファイルの形式となっており，ファイルタイプを調査することで，攻撃者は窃取したものが目的の機密情報ではないことを検知し，ダミーデータを操作しない可能性が高い．

3. 提案手法

3.1 提案手法の概要

本研究では，関連研究の問題点を解決するため，文書ファイルの体裁を保ったまま攻撃者情報を収集するシステムを提案する．文書ファイルを用いることにより，攻撃者の情報を収集するプログラムとのファイルサイズの違いを考慮する必要がなくなる．また，文書ファイルの体裁を保っているため，ファイルタイプを調査することによって検知されてしまうことはない．

提案システムが動作する環境は，Microsoft Office と.NET Framework がインストールされた Windows 環境とする．対象とする文書ファイルは，Microsoft Office Word，Excel，PowerPoint で使用されるファイルとする．

Office で使用される文書ファイルにおいてプログラムを実行する方法は，VBA と呼ばれるマクロ言語を用いて，文書ファイルにマクロ機能として実装する方法と，VSTO と呼ばれる Office アプリケーションやドキュメントを拡張する機能を用いて，任意のプログラムを実装する方法がある．VSTO では， C#(Microsoft Visual C#)や VB(Microsoft Visual Basic)を用いて実装することが可能である．

本研究では，この 2 つの方法を用いて，VBA を用いた攻撃者情報収集システムと VSTO を用いた攻撃者情報収集システムを提案する．

3.2 提案システムの基本構成

提案システムでは，基本的に以下の機能を実装する．

- 文書ファイルの所有者を判定する機能
- コンピュータの情報を収集する機能

文書ファイルの所有者を判定する機能では，文書ファイルが開かれたコンピュータが正しい所有者であるかを判定する．提案システムでは，判定する方式として，IP アドレスを用いた認証を行う．正しい所有者のみ通信可能な領域に認証サーバを設置し，認証サーバと正常に通信できた場合，正しい所有者と判定する．

コンピュータの情報を収集する機能では，文書ファイルの所有者を判定する機能で正しい所有者ではないと判定した場合，文書ファイルが開かれたコンピュータの情報を収集する．

3.3 提案システムで収集する攻撃者情報

提案システムでは，攻撃者を特定するために，様々な情報を収集する．表 1 に提案システムで収集する攻撃者の情報を示す．

基本的な情報として収集するコンピュータ名やユーザ名，ソフトウェアの情報として収集する OS の登録者名を，SNS(Social Networking Service)で調査することにより，攻撃者の SNS アカウントを発見できる可能性がある．また，タイムゾーンや言語設定から攻撃者がどの地域に所在しているのかを特定できる．

ハードウェアの情報として収集する情報はコンピュータに設定されている固有の情報であるため，攻撃者が使用したコンピュータを特定できる．

ネットワークの情報として収集するプロバイダーから提供されている IP アドレスから，攻撃者が文書ファイルを開いた時点でどこからインターネットに接続していたのかを特定できる．

表 1　収集する攻撃者の情報
Table 1　Information on attackers to collect

収集する情報の種類	収集する情報
基本的な情報	コンピュータ名
	ユーザ名
	タイムゾーン
	言語設定
ハードウェアの情報	シリアル番号
	プロダクト番号
	メーカー名
	モデル名
	UUID
ソフトウェアの情報	OS 名
	OS のバージョン
	OS のアーキテクチャ
	OS のシリアル番号
	OS の登録者名
ネットワークの情報	インターフェース名
	インターフェースの説明
	インターフェースの種類
	MAC アドレス
	IPv4 アドレス
	IPv6 アドレス
	プロバイダーから提供されている IP アドレス

3.4 VBA を用いた攻撃者情報収集システムの提案（提案手法 1）

提案手法 1 では，VBA を用いてプログラムを文書ファイルにマクロとして実装する．VBA とは，Microsoft Office で使用されるマクロ言語で，VBA を用いることで，Office アプリケーションを拡張することが可能である．また，VBA は VB から派生した言語であるため，VB と同様な記述が可能である．

VBA を用いる際の特徴として，実装したプログラムは文書ファイルの一部として保存される．このため，文書ファイル単体でプログラムの実行が可能である．また，他のコンピュータ上でも実行することが可能である．しかし，Microsoft Office の既定の設定では，マクロのセキュリティ設定[5]が，「警告を表示してすべてのマクロを無効にする」に設定されているため，攻撃者が自らの意思でマクロを実行しなければプログラムは実行しない．

3.4.1 提案手法 1 の動作

図 1 に提案手法 1 の動作フローを示す．

① 攻撃者がマルウェア等を用いて企業等のコンピュータに侵入する．
② 機密情報を含んだ文書ファイルを窃取する．
③ 攻撃者が，窃取した文書ファイルを対応する Office アプリケーションで開く．
④ 攻撃者がマクロを実行することにより，文書ファイルに保存されているプログラムが実行される．
⑤ プログラムが実行されると，企業等にある認証サーバに HTTP，もしくは，HTTPS の GET リクエストを行う．認証サーバは企業等の内部ネットワークからのみ通信可能なため，攻撃者が外部のネットワークで文書ファイルを開いた場合，認証が失敗となり，文書ファイルの正しい所有者ではないと判定する．
⑥ 文書ファイルが開かれたコンピュータの情報を収集する．収集した情報は，情報ごとにパラメータを設定し，HTTP，もしくは，HTTPS の POST リクエストを用いて，認証サーバに送信する．

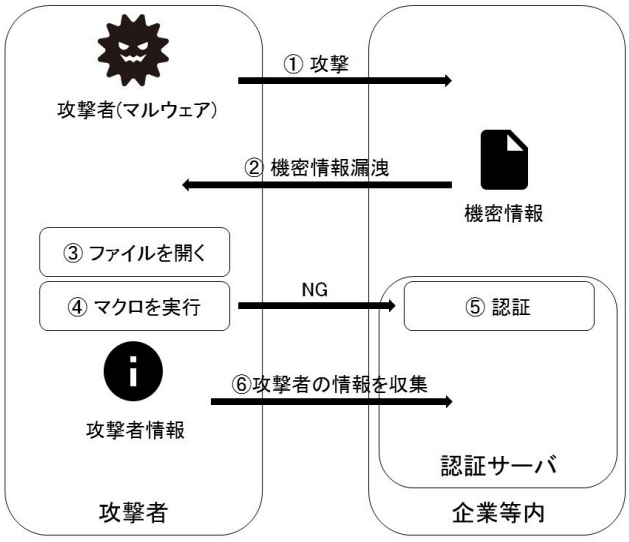

図 1　提案手法 1 の動作フロー
Figure 1　Operational flow of proposed method 1

3.5 VSTO を用いた攻撃者情報収集システムの提案（提案手法 2）

提案手法 2 では，VSTO を用いてプログラムを Microsoft Office のアドインとして実装する．VSTO とは，Microsoft Visual Studio を用いて Office アプリケーションやドキュメントを拡張する機能で，C#や VB を用いて実装することが可能である．

VSTO を用いる際の特徴として，.NET Framework を用いた実装を行うことが容易である．また，C#や VB を用いることが可能なため，VBA では実現が困難な複雑な処理を実現することができる．しかし，実装したプログラムは文書ファイルとは別にアドインとして保存される．このため，プログラムを実行するためには，アドインがコンピュータにインストールされている必要がある．また，アドインだけでなく，.NET Framework と VSTO Runtime(Visual Studio Tools for Office Runtime)[5]もコンピュータにインストールされている必要がある．

3.5.1 機密情報の漏洩防止機能

提案手法 2 では，3.2 節で述べた機能に加えて，機密情報の漏洩防止機能を実装する．

文書ファイルの内容を保存するアプリケーション(文書サーバ)を実装し，認証サーバ内に設置する．文書ファイルの内容は，文書ファイル自体には保持せず，文書サーバに保存する．実装するプログラムに，文書ファイルの内容を管理する機能を実装し，文書ファイルの閲覧や編集を行う際に，文章サーバから対応する文書ファイルの内容を取得する．この機能を実装することにより，アドインがない場合，ファイルの内容について一切の情報を取得できないため，機密情報の漏洩防止機能として動作する．

文書ファイルの内容を管理するために，以下の機能を実装する．

- 文書ファイルを，文書サーバに保存する機能(保存処理)
- Office アプリケーションの終了時，もしくは，文書ファイルを閉じる際に，文書ファイルから内容を削除する機能(終了処理)
- 対応する文書ファイルの内容を，文書サーバから取得する機能(内容取得処理)

保存処理では，文書ファイルが Office アプリケーションによって保存された際に，文書ファイルの内容を文書サーバに保存する．また，このとき，文書サーバに一度も保存したことがない文書ファイルの場合，文書ファイルと文書ファイルの内容を対応付けるために，ドキュメント ID を作成する．ドキュメント ID は，保存する文書ファイルの名前，保存日時，0 から 65535 までのランダムな数値を連結した文字列を，SHA-256(Secure Hash Algorithm 256-bit)を用いてハッシュ化することで作成する．作成したドキュメント ID は文書ファイルに保存する．

終了処理では，文書サーバに保存している文書ファイルの内容を文書ファイルから削除する．内容が削除された文書ファイルには，保存処理で作成されたドキュメント ID のみが保存されており，このファイルを認証用ファイルとする．

内容取得処理では，認証用ファイルを用いて，対応する文書ファイルの内容を文書サーバから取得する．

3.5.2 文書サーバの構成

提案手法 2 で実装する機密情報の漏洩防止機能で用いる文書サーバには，文書ファイルを再構築するために必要な情報を保存する．以下に文書サーバに保存する情報を示す．

- ファイル名
- アプリケーション名
- ドキュメント ID
- 文書ファイルの内容と構造

ファイル名とアプリケーション名には，文書ファイルの名前と文書ファイルに対応するアプリケーション名を保存する．提案システムでは，Microsoft Word，Excel，PowerPoint で使用されるファイルを対象としているため，「Word」，「Excel」，「PowerPoint」のいずれかを保存する．

ドキュメント ID には，文書ファイルと文書ファイルの内容を対応付けるために作成した ID を保存する．ドキュメント ID は，3.5.1 項で述べた文書ファイルの内容を管理する機能で作成される．

文書ファイルの内容と構造には，XML で表現した文書ファイルの内容と構造を保存する．Microsoft Office 2007 以降の文書ファイルでは，Office Open XML[6]と呼ばれる XML ベースのファイル形式が採用されているため，文書ファイルを XML で表現することは容易である．しかし，ファイル形式が Office Open XML ではない文書ファイルは，バイナリファイル形式[7]が採用されているため，XML で表現することができない．このため，機密情報の漏洩防止機能を適用できる文書ファイルは，Microsoft Office 2007 以降の文書ファイルに限定される．

3.5.3 提案手法 2 の動作

図 2 に提案手法 2 の動作フローを示す．ここで示す動作フローでは，攻撃者が使用しているコンピュータに，提案手法 2 で実装したアドインと VSTO Runtime がインストールされているとする．

① 攻撃者がマルウェア等を用いて企業等のコンピュータに侵入する．
② 機密情報の漏洩防止機能にて作成された認証用ファイルを窃取する．
③ 攻撃者が，窃取した認証用ファイルを対応する Office アプリケーションで開くことにより，
④ プログラムが実行される．
⑤ プログラムが実行されると，認証サーバに HTTP，も

しくは，HTTPS の GET リクエストを行う．認証サーバは企業等の内部ネットワークからのみ通信可能なため，攻撃者が外部のネットワークで文書ファイルを開いた場合，認証が失敗となり，文書ファイルの正しい所有者ではないと判定する．

⑥ 文書ファイルが開かれたコンピュータの情報を収集する．収集した情報は，情報ごとにパラメータを設定し，HTTP，もしくは，HTTPS の POST リクエストを用いて，認証サーバに送信する．

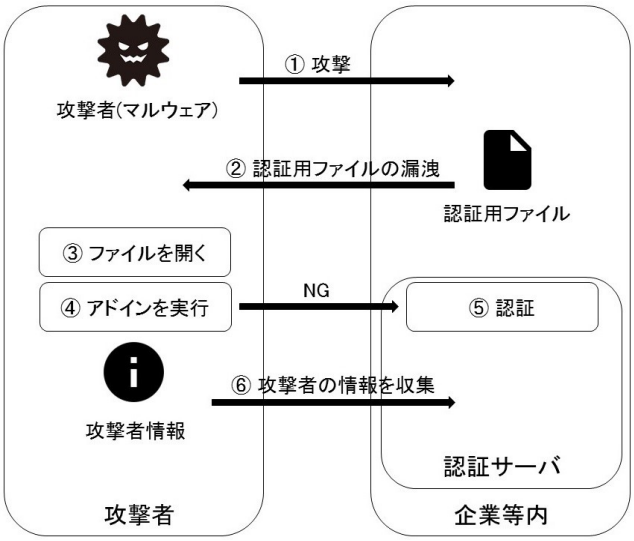

図 2 提案手法 1 の動作フロー
Figure 2 Operational flow of proposed method 2

3.6 収集した情報の蓄積

提案システムでは，提案手法 1，提案手法 2 で収集した情報を蓄積するため，収集した情報を項目毎にデータベースに保存するアプリケーション(アクセスログサーバ)を実装し，認証サーバ内に設置する．認証サーバは正しい所有者のみ通信できる領域に設置するが，アクセスログサーバは，収集した情報の送信のみ正しい所有者以外からも通信が可能な設定を行う．

アクセスログサーバは, HTTP, もしくは, HTTPS の POST リクエストによって送信された情報を受け取る．収集した情報は，それぞれパラメータに設定されているため，パラメータごとにデータベースに保存することで蓄積する．

4. 実験と考察

4.1 実験の概要

実験では，提案システムの有効性を示すため，Microsoft Office Word で使用されるファイルを対象として実装を行い，以下のことを確認する．

- 提案システムにより, 攻撃者に気が付かれることなく，攻撃者の情報を収集できる(実験 1)
- 提案手法 1 で実装したマクロを組み込んだ文書ファイルと提案手法 2 で実装したアドインがアンチウイルスソフトによって検知されない(実験 2)

実験 1 では，被験者を攻撃者とみなして行う．実験で使用する文書ファイルは被験者に配布する．被験者に実験で使用する文書ファイルを使用してもらい，被験者に気が付かれることなく，被験者のコンピュータの情報を収集できることを確認する．

実験 2 では，3.1 節で述べた，提案システムが動作する環境を作成し，アンチウイルスソフトを導入する．作成した環境において，実験 1 を行い，アンチウイルスソフトによって検知されないことを確認する．

4.2 実験 1

実験 1 では，提案システムにより，攻撃者に気が付かれることなく，攻撃者の情報を収集できることを確認する．実験後，被験者にアンケートを行い，コンピュータの情報を収集されていたことに気が付いたか確認する．

また，実験 1 では，提案手法 1 のシステムと提案手法 2 のシステムを同時に確認する．このため，提案手法 1 で実装したマクロに，提案手法 2 で実装したアドインをダウンロードする機能を追加し，実験で使用する文書ファイルに組み込む．

被験者は，筆者と同じ研究室に所属する学生とする．また，被験者の予備知識の有無や程度によって実験結果に差が生じるかを確認するため，グループ分けを行う．表 2 に各グループの概要を示す．まず，予備知識の有無でグループを分けるため，学部 3 年生のグループ(グループ A)と学部 4 年生，修士 1 年生，修士 2 年生のグループ(グループ B)に分ける．さらに，グループ B から，本研究の内容を把握しているグループ(グループ B1)と把握していないグループ(グループ B2)に分ける．

表 2 各グループの概要
Table 2 Outline of each group

グループ名	概要
グループ A	学部 3 年生 (本研究の内容を把握していない)
グループ B1	学部 4 年生，院生 (本研究の内容を把握している)
グループ B2	学部 4 年生，院生 (本研究の内容を詳しく把握していない)

Vol.2017-DPS-170 No.16
Vol.2017-CSEC-76 No.16
2017/3/2

4.2.1 実験 1 の手順

実験 1 は，被験者に実験の内容を説明せず行うため，実験の内容を説明する代わりに,「コンピュータの環境情報調査」と称した調査の協力を依頼した．また，実験で使用する文書ファイルは，調査の回答用紙として配布した．図 3 に配布した文書ファイルの一部を示す．配布した文書ファイルの下部にある「送信プログラムのダウンロード」ボタンを押下することにより，マクロが実行され，被験者のコンピュータの情報を収集する．また，送信プログラムと称した，提案手法 2 で実装したアドインのインストーラがダウンロードされる．このインストーラを使用することにより，実装したアドインと VSTO Runtime がインストールされる．被験者には,「送信プログラムのダウンロード」ボタンを押下し，ダウンロードされた送信プログラムをインストール，配布した文書ファイルを開き直すことによって回答内容が送信されると説明を行い，この手順を実施するように指示した．

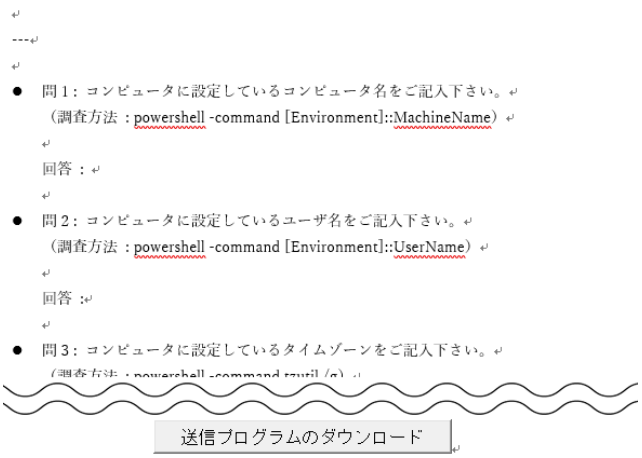

図 3　配布した文書ファイルの一部
Figure 3　A part of the distributed document file

図 4 に実験 1 の手順を示す．

① 被験者が，配布された文書ファイルを開く．
② 被験者が,「送信プログラムのダウンロード」ボタンを押下することにより，マクロが実行され，
③ 被験者のコンピュータの情報を収集する．
④ 被験者のコンピュータに，送信プログラムと称した，提案手法 2 で実装したアドインのインストーラがダウンロードされる．
⑤ 被験者が，インストーラを実行し，アドインと VSTO Runtime をインストールする．
⑥ 再度，配布された文書ファイルを開くことにより，
⑦ アドインが実行され，
⑧ 被験者のコンピュータの情報を収集する．
⑨ 被験者に，実験後のアンケート URL が送信される．

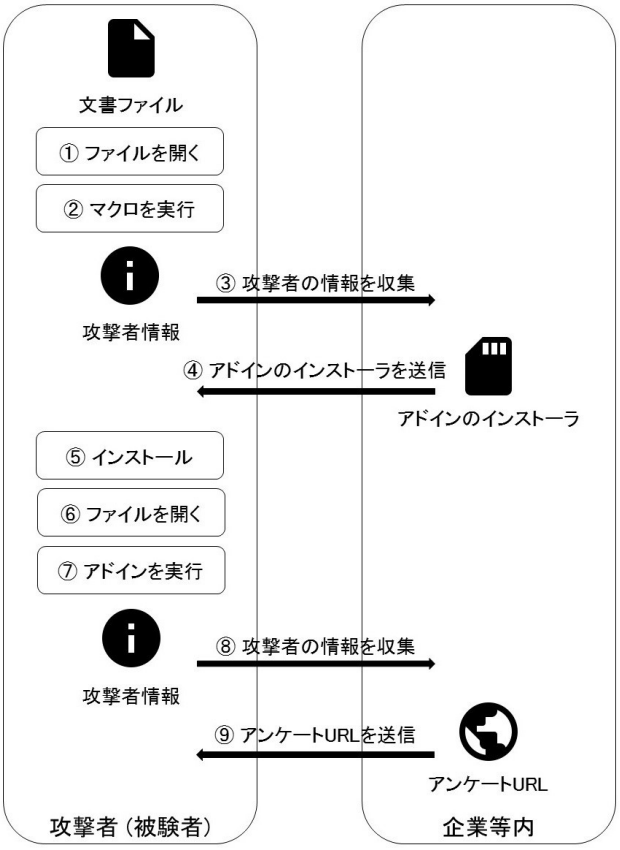

図 4　実験 1 の手順
Figure 4　Procedure of Experiment 1

4.3 実験 2

実験 2 では，提案手法 1 で実装したマクロを組み込んだ文書ファイルと提案手法 2 で実装したアドインがアンチウイルスソフトによって検知されないことを確認する．表 3 に実験 2 で作成する環境の情報を示す．実験環境にて実験 1 を行い，文書ファイルやアドインが，アンチウイルスソフトによって脅威判定や警告等された場合に，検知されたと判断する．

表 3　実験環境
Table 3　Experiment environment

OS	Windows 7 Professional SP1 (x64)
ライブラリ	.NET Framework 4.5.2
Microsoft Office	Microsoft Office 2013
アンチウイルスソフト	カスペルスキー セキュリティ 2017
	ウイルスバスター クラウド
	ノートンセキュリティ
	Microsoft Security Essentials

4.4 実験結果

実験 1 では，21 名の学生から協力を得られた．21 名のうち，21 名が提案手法 1 で実装したマクロを実行し，20 名が提案手法 2 で実装したアドインをインストール，実行した．

表 4 に実験後のアンケート結果を示す．アンケート結果から，どちらの提案手法においても，本研究の内容を把握しているグループ B1 の結果が 14%と低く，予備知識の有無にかかわらず，情報収集処理に気が付かない可能性が高いと言える．

表 4　実験後のアンケート結果
Table 4　Questionnaire result after experiment

提案手法 1	
設問	回答
コンピュータの情報を収集されていたことに気が付いた	グループ A : 0% (0/7)
	グループ B1:14% (1/7)
	グループ B2: 0% (0/7)
提案手法 2	
設問	回答
コンピュータの情報を収集されていたことに気が付いた	グループ A : 0% (0/7)
	グループ B1:14% (1/7)
	グループ B2: 0% (0/6)

表 5 に実験 2 の結果を示す．

表 5　実験 2 の結果
Table 5　Result of Experiment 2

提案手法 1	
アンチウイルスソフト	結果
カスペルスキー セキュリティ 2017	検知
ウイルスバスター クラウド	検知せず
ノートンセキュリティ	検知せず
Microsoft Security Essentials	検知せず
提案手法 2	
アンチウイルスソフト	結果
カスペルスキー セキュリティ 2017	検知せず
ウイルスバスター クラウド	検知せず
ノートンセキュリティ	検知
Microsoft Security Essentials	検知せず

4.5 考察

実験 1 の結果から，どちらの提案手法も気が付かれる可能性が低く，攻撃者に気が付かれることなく攻撃者の情報を収集することが可能であると考えられる．また，本研究の内容を把握しているグループ B1 においても 14%と低いことから，予備知識の有無や程度に関わらず，有効な手法であると考えられる．

実験 2 では，どちらの提案手法も，異なる 1 つのアンチウイルスソフトによって検知された．提案手法 1 で実装したマクロは，「カスペルスキー セキュリティ 2017」によって，「Trojan-Downloader.Script.Generic」と判定された．これは，実験 1 を行うにあたり，提案手法 2 で実装したアドインをダウンロードする機能を追加していたためだと考えられる．このため，該当部分の機能を削除することで検知されなくなると考えられる．提案手法 2 で実装したアドインは，「ノートンセキュリティ」のダウンロードインサイト機能[8]によって，アドインのインストーラが警告された．実装したアドイン自体は，いずれのアンチウイルスソフトにおいても検知されていないため，アドインのインストール方法を変更することで対応できると考えられる．

これらのことから，攻撃者の情報を収集する点や，アンチウイルスソフトへの対応においては，提案手法 1 と提案手法 2 に差はなく，どちらの提案手法も完全ではないが有効性が高いと考えられる．一方で，提案手法 2 では機密情報の漏洩防止機能を実装しており，この点では，提案手法 1 より優位であると考えらえる．また，提案手法 2 において，攻撃者が機密情報を窃取するためには，文書サーバから文書ファイルの内容を取得するアドインが必要であり，機密情報を窃取したい攻撃者に対しては，攻撃者の情報を収集するプログラム実行へ誘導し易いと考えられる．このため，提案手法 2 の方が提案手法 1 よりも優位であると考えられる．

5. おわりに

本研究では，文書ファイルの体裁を保ったまま攻撃者の情報を収集するシステムを提案し，VBA を用いた攻撃者情報収集システムと VSTO を用いた攻撃者情報収集システムの 2 つを示した．提案システムの有効性を示すため，被験者に気が付かれることなく情報収集処理を実行できることを確認する実験を行った．また，提案手法 1 で実装したマクロを含む文書ファイルと提案手法 2 で実装したアドインが，アンチウイルスソフトによって検知されないことを確認する実験を行った．実験結果から，攻撃者の情報を収集する点や，アンチウイルスソフトへの対応において提案手法 1 と提案手法 2 に差はなく，どちらの提案手法も有効であると考えた．また，機密情報の漏洩防止が可能な点やプログラム実行への誘導し易さから，提案手法 2 の方が提案手法 1 よりも有効な手法であり，優位であると考えた．

なお，本研究の提案手法では，コンピュータ上で，不正者とはいえ使用者が意図していない動作をすることから，実フィールドでの実施に当たっては，法的観点からの検討が必要である．

Vol.2017-DPS-170 No.16
Vol.2017-CSEC-76 No.16
2017/3/2

参考文献

[1] 警察庁，”平成 27 年におけるサイバー空間をめぐる驚異の情勢について”, http://www.npa.go.jp/kanbou/cybersecurity/H27_jousei.pdf (参照 2016-12-28)
[2] FireEye，”ファイア・アイ、2016 年セキュリティ動向予測を発表”, https://www.fireeye.jp/company/press-releases/2015/fireeye-publis
[3] 池上祐太，山内利宏，”情報漏洩を契機とした攻撃者探査システムの提案”，コンピュータセキュリティシンポジウム 2013(CSS2013)論文集，Vol.2013，No.4，pp.17-24
[4] 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
[5] Microsoft, “Visual Studio Tools for Office Runtime の概要”, https://msdn.microsoft.com/ja-jp/library/bb608603.aspx (参照 2017-12-28)
[6] Microsoft，”Office (2007) Open XML ファイル形式の概要”, https://msdn.microsoft.com/ja-jp/library/aa338205(v=office.12).aspx (参照 2016-12-28)
[7] Microsoft，” Office バイナリ ファイル形式の理解”, https://msdn.microsoft.com/ja-jp/library/office/gg615407(v=office.14).aspx (参照 2016-12-28)
[8] Symantec，”ダウンロードインサイト機能について”, https://support.symantec.com/ja_JP/article.TECH171776.html (参照 2017-12-28)