攻撃空間の探索範囲を拡大する FTP ハニーポットの設計

八木　毅　　秋山 満昭　　青木 一史　　針生 剛男

NTT セキュアプラットフォーム研究所
180-8585 東京都武蔵野市緑町 3-9-11
yagi.takeshi@lab.ntt.co.jp

あらまし 正規Webサイトを悪用してユーザ端末をマルウェアに感染させる攻撃が脅威となっている．この攻撃では，正規Webサイトが改ざんされ，当該サイトにアクセスしたユーザ端末が，マルウェアに感染させるために攻撃者が用意した悪性Webサイトに誘導される．さらに,マルウェアに感染したユーザ端末からFTPアカウント情報が攻撃者により不正に入手され，当該ユーザのWebサイトコンテンツが攻撃者に改ざんされる．この際の通信やコンテンツを分析すれば，新たな悪性Webサイト情報等を発見して対策を講じることができる．そこで本稿では，おとりのFTPアカウントにより，監視下にあるWebサイトの改ざんを誘発して改ざんの特徴を分析する，FTPハニーポットを設計，実装し，観測した情報を分析した結果を報告する．

Design of an FTP Honeypot for Expanding the Search Scope in Attack Space

Takeshi Yagi　　Mitsuaki Akiyama　　Kazufumi Aoki　　Takeo Hariu

NTT Secure Platform Laboratories
3-9-11 Midori-cho, Murashino-shi, Tokyo 180-8585, JAPAN
yagi.takeshi@lab.ntt.co.jp

Abstract Recently, with the widespread of the web, malware has been spreading via malicious websites. In many cases, the malicious websites are constructed by falsifying legitimate websites. A user, who accesses the falsified website, is redirected to an attacker's website and is forced to download malware. Additionally, the attacker steals the user's FTP account information stored on the computer infected by the malware. Furthermore, the attacker tries to falsify the user's website as a legitimate website administrator using the stolen FTP account information. To detect and prevent such an attack, it is necessary to reveal its characteristics, especially the method to falsify user websites. In this research, we proposed an FTP honeypot which analyzes the characteristics by triggering off falsification to our monitored website using decoy FTP account information.

1　はじめに

近年, 企業や個人の Web サイトにおいてコンテンツが改ざんされるインシデントが多発している[1]．この改ざんにより，正規の Web サイトのコンテンツの一部に自動転送コードが挿入される. 改ざんされた Web サイトを閲覧したユーザのアクセスは，ユーザの意図とは無関係に, 攻撃者が用意した悪性 Web サイトへ転送される．悪性 Web サイトには，Web ブラウザやプラグインのぜい弱性を標的とする攻撃コードが設置されており，ユーザは閲覧するだけでマルウェアに感染する．この際感染するマルウェアの一部は，FTP アカウン

ト情報を漏えいする機能を保有している[2]. このため, 感染端末上に Web サイト管理者用の FTP アカウント情報が記憶されている場合は，その情報が攻撃者に漏えいしてしまい，新たな Web サイト改ざんを引き起こす[3]. このように, Web サイト改ざんと FTP アカウント情報漏えいを引き起こす一連の攻撃では，Web サイト改ざんとマルウェア感染が繰り返されることで，被害が拡大する仕組みとなっている.

2 マルウェア感染手法

近年，Windows OS の基本機能としてパーソナルファイアウォールが適用されたことや，NAT 環境下でのインターネット利用の普及により，外部ネットワークから直接 Windows OS のぜい弱性を攻撃するネットワーク経由の感染が減少してきた．一方で，Web ブラウザやプラグインのぜい弱性が継続的に多数発見されており，攻撃者としては，Web 経由の方がユーザをマルウェアに感染させることができる状況になっている．このため，マルウェアの感染経路の主流は Web 経由への転換しつつある.

Web 経由のマルウェア感染活動の典型例を図 1 に示す. ぜい弱な Web ブラウザやプラグインを使用しているユーザは，攻撃者が用意した改ざんコンテンツを閲覧した際に，攻撃コードやマルウェアが配置された悪性 Web サイトに誘導され，マルウェアに感染する. マルウェアに感染した端末に Web サイト管理用の FTP アカウント情報が記憶されている場合，FTP アカウント情報は攻撃者に漏えいする．攻撃者は，Web サイト管理者としてユーザの FTP サーバにログインしてコンテンツを改ざんする. Web サイトでは FTP サーバ上に配置されたコンテンツが表示されるため，それ以降，この FTP サーバとシンクしている Web サイトは，別の閲覧ユーザを悪性 Web サイトへ誘導するために使用される.

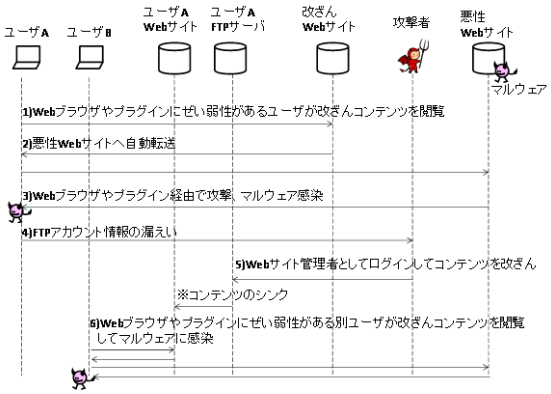

図 1 Web 経由のマルウェア感染

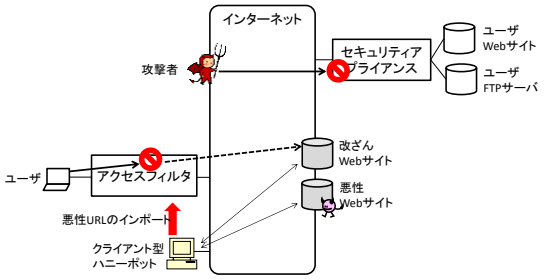

図 2 従来の対策手法

3 従来の対策手法

この攻撃を防御するために, 従来では, Web サイトの改ざんを検知して制御するサーバ側の対策手法と, ユーザから改ざん Web サイトや悪性 Web サイトへのアクセスをフィルタするユーザ側の対策手法が検討されている.

前者に関しては, SQL インジェクション[4]など異常な HTTP リクエストメッセージを用いたコンテンツ改ざんを検知する intrusion detection system や intrusion prevention system および web application firewall[5]などの，セキュリティアプライアンスでの対処が検討されている.

一方，後者に関しては，悪性 Web サイトへの誘導やマルウェア感染を検知する仕組みを搭載したクライアント型ハニーポット[6]で Web サイトを巡回する手法が検討されている．この手法では，クライアント型ハニーポットで不特定多数の Web サイトへアクセス

することで，改ざん Web サイトや悪性 Web サイトの URL を特定する．なお，アクセスした Web サイトのコンテンツを分析することで，マルウェア検体の収集に加え，ユーザのマルウェア感染の原因となる改ざんコンテンツも特定できる．特定された URL はブラックリスト化され，アクセスフィルタを実施する際にフィルタ対象とされる，

4　従来の対策手法における課題

Web 経由のマルウェア感染活動は，Web サイトの改ざんと，ユーザのマルウェア感染の両者が起点となっている．このため，サーバ側での対策とユーザ側での対策の両者を考慮した検討が必要となる．

セキュリティアプライアンスは，異常なアクセスを検知する．このため，不正入手した FTP アカウント情報を悪用して Web サイト管理者として正規な手順でコンテンツを変更する攻撃者は検知できない．一方，クライアント型ハニーポットは， Web サイトの改ざん結果および改ざん Web サイトへのアクセス後の発生事象は確認できるが，Web サイトで発生したコンテンツ改ざんの経緯を把握できない．このようなセキュリティアプライアンスとクライアント型ハニーポットの課題を考慮すると，サーバ側での対策とユーザ側での対策の両者を実現するためには，以下の課題があると考えられる．

サーバ側での対策という視点では，従来の対策手法では，図 3 に示すように，クライアント型ハニーポットで既に改ざんされた Web サイトを検知できるが，FTP アカウント情報を悪用したコンテンツ改ざんは防御できない．なお，Web サイトが改ざんされる際，正規 Web サイトの.htaccess が不正に制御されて Web サイトを閲覧したユーザを悪性 Web サイトに誘導するなど，クライアント型ハニーポットでの観測のみでは観測できない不正制御が含まれる場合がある[7]．改ざん時に使

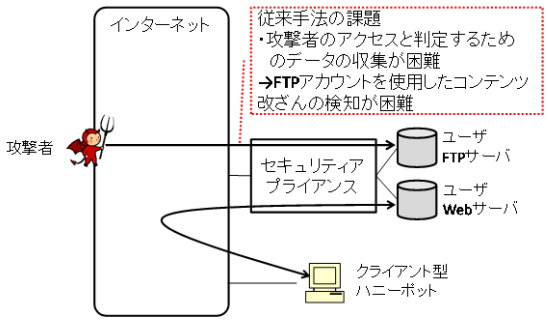

図 3　従来手法の課題

用される攻撃者の IP アドレスや，改ざん時にアップロードされるコンテンツなどを観測できれば，観測結果をセキュリティアプライアンスでの攻撃検知に反映することで，Web サイトの改ざんを防止できる．

ユーザ側での対策という視点では，従来の対策手法では，Web サイトが改ざんされてからクライアント型ハニーポットが改ざんを検知するまでの期間，マルウェア感染活動は検知できない．なお，既存の全 URL を短期間で検査するクライアント型ハニーポットを用意することは物理リソース面から非現実的である．このため，本課題は，効率的に検査対象の URL を決定するという課題と同義である．効率的な検査方法としては，既知の改ざん Web サイトや悪性 Web サイトの URL の近傍を検査する手法[8]が検討されている．未知の改ざん Web サイトや悪性 Web サイトを特定できれば，既存の手法を用いて効率的に検査対象の URL を決定できる．

5　FTP ハニーポットの設計

本稿では，クライアント型ハニーポットで収集したマルウェア検体を，おとりの FTP アカウント情報を記憶させた開環境型マルウェア動的解析機能[9]で動作させるとともに，おとりの FTP サーバで攻撃者からのアクセスを収集する FTP ハニーポットを提案する．FTP ハニーポットへのアクセス元から攻撃者の IP アドレスを特定するとともに，FTP ハニー

ポットにアップロードされる情報から，改ざん時に発生する事象を観測する．さらに，FTP ハニーポットにアップロードされたコンテンツをクライアント型ハニーポットで検査することで，未知の改ざん Web サイトや悪性 Web サイトの特定を試行する．

5.1 構成

FTP ハニーポットは，クライアント型ハニーポットと，インターネットに接続した環境でマルウェアを動的解析する開環境型マルウェア動的解析機能と，おとり FTP サーバと，おとり Web サーバおよび，各機能を管理するマネージャで構成される．

FTP ハニーポットにおけるクライアント型ハニーポットとして，Marionette[10]を適用する．Marionette は，図 4 に示すように，ぜい弱性個所の監視等による正確な攻撃検知や，ダウンロードしたプログラムの動的隔離により，安全性を確保しつつ実ブラウザを利用した検査を実施する，高対話型のクライアント型ハニーポットである．さらに，マルチプロセス化や複数 OS 上での分散配置等を実現しており，多数 URL を短時間で検査できる．Marionette を用いることで，マルウェア検体の収集に加え，マルウェア感染を引き起こす改ざん Web サイトや悪性 Web サイトを特定する．

また，開環境型マルウェア動的解析機能としては，Botnet Watcher[11]を適用する．Botnet Watcher は，マルウェア検体を感染させた内部端末に対して，ゲートキーパーが内部端末から正規 Web サイト等へのアクセスに対して疑似応答を返信しつつ，攻撃者との通信をインターネットへ転送する機能を保有している．これにより，マルウェア検体が送受信する通信の特徴や感染端末の挙動を安全に解析する．各内部端末には複数の FTP クライアントソフトウェアをインストールしておくとともに，各マルウェア検体の解析毎にランダムに生成した FTP アカウント情報を設定し，マルウェア検体がおとり FTP アカウント情報を外部へ送信する動作を管理下で実行する．具体的には，マルウェア検体を動作させた際に，FTP クライアントソフトウェアと FTP アカウント情報に関するレジストリアクセスとファイルアクセスを監視し，FTP アカウント情報の漏えいを確認する．

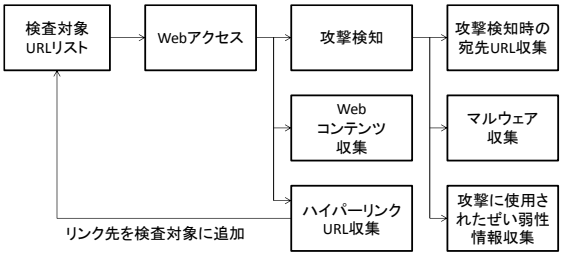

図 4 Marionette のワークフロー

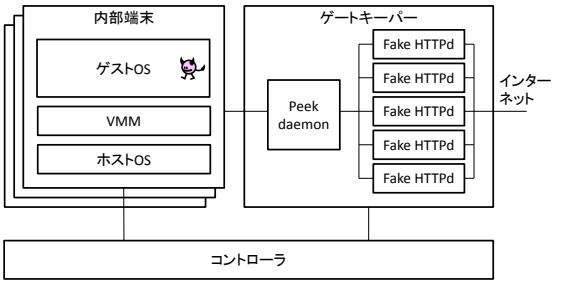

図 5 Botnet Watcher 概要

おとり FTP サーバでは，予め記憶していたおとり FTP アカウント情報を用いてログインしたユーザに対して，ユーザディレクトリを割り当てるとともに，FTP アクセスや HTTP アクセスのログをセッション毎に記録する．この際，FTP アクセスに関しては，セッション毎に改ざん差分を記録する．また，おとり FTP サーバと，インターネットに接続した Web サーバとをシンクさせ，おとり Web サイトを構築する．ただし，一般ユーザがおとり Web サイトを閲覧してマルウェアに感染する事態を回避するために，おとり Web サイトにアクセス可能なユーザを制限する．

マネージャは，おとり FTP アカウント毎のログを管理する．具体的には，おとり FTP アカウント毎に，漏えいさせる際に使用したマルウェア検体の情報と，おとり FTP サーバへ

の FTP アクセスと HTTP アクセスのログをセッション毎に記録する．

5.2　攻撃収集方法

FTP ハニーポットでは, 図 6 に示すように, 改ざん時に攻撃者が使用する IP アドレスや, 攻撃者が改ざん Web サイトを制御する際の挙動および，改ざんコンテンツに記述された他の改ざん Web サイトや悪性 Web サイトの情報を収集する．

Marionette は，過去に改ざんが観測されたインターネットサービスプロバイダが提供する Web サイトや，公開されている悪性 Web サイトリスト Malware Domain List (MDL) [12] から，マルウェア検体を収集する．マネージャは，Marionette が収集したマルウェア検体を Botnet Watcher の内部端末へ投入する．この際，マネージャは，おとり FTP アカウント情報を内部端末に設定するとともに，おとり FTP アカウント情報とマルウェア検体情報を関連付けて管理する．Botnet Watcher は，マルウェア検体を動作させ，おとり FTP アカウント情報の漏えいを発生させる．マネージャは, 定期的におとり FTP サーバやおとり Web サーバからログを収集し，FTP アカウント情報毎に分割して管理する．さらに，コンテンツが改ざんされた可能性があるおとり Web サイトに関しては，Marionette で検査し，結果をおとり FTP アカウント情報と関連付けて管理する．

おとり FTP サーバやおとり Web サーバのログから, 攻撃者が改ざん時に使用する IP アドレスや攻撃者の振る舞い情報が収集できる．さらに，Marionette による改ざん Web サイト検査により，改ざんコンテンツに記述された他の改ざん Web サイトや悪性 Web サイトの情報を収集できる．

6　FTP ハニーポットの評価

サーバ側の対策手法の課題に関しては，FTP ハニーポットにより，改ざん時に発生するサーバ上での事象を観測できれば，観測結果から Web サイトの改ざんを検知するための情報を抽出できる可能性がある．特に攻撃者の IP アドレスに関しては, フィルタリング等に活用できる．一方，ユーザ側の対策手法の課題に関しては, FTP ハニーポットにより，未知の改ざん Web サイトや悪性 Web サイトを特定できれば，既存の手法を用いて効率的に検査対象の URL を決定できる．

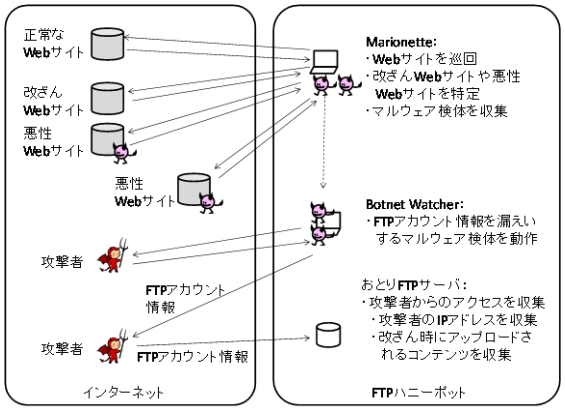

図 6　攻撃収集方法

そこで本稿では，FTP ハニーポットを実装し, 攻撃者が改ざんに使用する IP アドレス数を調査した．さらに，FTP ハニーポットで収集した改ざんコンテンツを Marionette で検査した際に抽出した URL と，公開ブラックリスト MDL に掲載されていた URL の発見時間を比較評価した．なお，本評価では 2012 年 4 月 1 日から 2012 年 8 月 22 日までの期間で収集した情報を用いている．

6.1　攻撃者が使用した IP アドレスの評価結果

おとり FTP アカウント情報を漏えいさせるために Marionette で収集したマルウェア検体数と, 攻撃者が使用した IP アドレス数および, 改ざんアクセス数の時系列累積グラフを図 7 に示す．

本評価では，継続的に一定数のマルウェア検体を収集し，各検体を用いて FTP アカウント情報の漏えいを試行できた．その結果，従

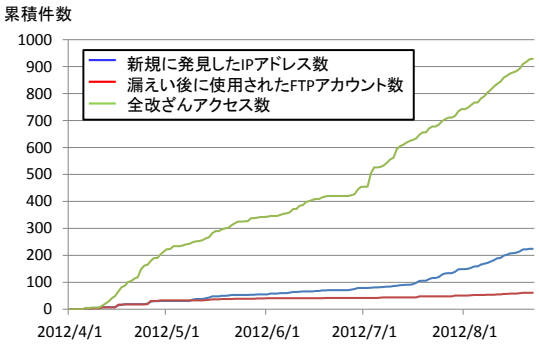

図 7 収集情報

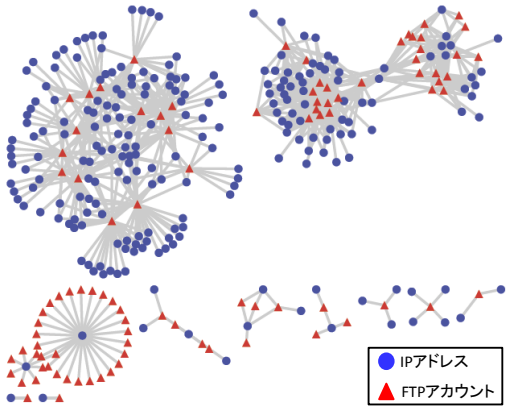

図 8 FTP アカウントと IP アドレスの関係

来の手法では収集できない攻撃者の IP アドレスを 200IP アドレス以上，改ざんアクセスを 900 アクセス以上収集できた．なお，攻撃者からおとり FTP サーバへのアクセスを確認したところ，ログイン認証時に失敗する事象が発生していなかった．このことから，攻撃者は，ブルートフォース攻撃ではなく，漏えいした FTP アカウント情報を用いておとり FTP サーバにアクセスしていることが確認できた．また，漏えいさせた FTP アカウント数と比較して，収集した IP アドレス数は倍以上の数となっている．これは，攻撃者が同一の FTP アカウント情報を用いて複数の IP アドレスからおとり FTP サーバへアクセスしていることを示している．図 8 は，おとり FTP サーバへのアクセスに利用された FTP アカウントとアクセス元の IP アドレスの関係を示している．FTP アカウントと IP アドレスは複数のクラスタに分割できる．これは，FTP アカウント情報を入手した攻撃者が複数の bot を用いておとり FTP サーバへアクセスしていることを示している．

このように，FTP ハニーポットを用いることで，従来の手法では特定できない，攻撃者が改ざんの際に使用している IP アドレスや，改ざんコンテンツを収集できる．この IP アドレスからユーザの Web サイトへのアクセスを監視することで，攻撃者が改ざんコンテンツをアップロードするアクセスを検知できる可能性がある．また，Web サイトにアップロードされるコンテンツに対して FTP ハニーポットで収集した改ざんコンテンツとの一致性を確認することで，攻撃者による Web サイトの改ざんを検知できる可能性がある．

表 1 特定時間の比較

	MDL 掲載件数	差異があった件数	提案方式での発見日	MDL 掲載日
URL	2	1	4/23	4/25
FQDN	28	2	4/23	4/25
			5/24	5/23

表 2 改ざんコンテンツを Marionette で検査した際に発生した外部アクセス

	件数
検査対象 URL	60
外部アクセスが発生した検査対象 URL	50
外部アクセスの宛先 URL	65
iframe タグが挿入されていた宛先 URL	48

6.2 改ざんコンテンツに記載された URL の評価結果

FTP ハニーポットで収集した改ざんコンテンツを保有する Web サイトを Marionette で検査した際に抽出した 796URL と 150FQDN に関して，公開ブラックリストである MDL への掲載状況を調査した．掲載されていた場合の日時情報において日単位の差異があった場

合の比較を表 1 に示す.

本調査が示すように，URL に関しては，攻撃者が改ざんコンテンツに記載していたが MDL に掲載されていない最新の URL を 794 件収集できた．一方，MDL に掲載されていた URL や FQDN に関しては，MDL への掲載日と同等の時期に FTP ハニーポットで観測できた．このため，FTP ハニーポットを用いることで，最新の悪性 URL 情報を収集できると考えられる．

本評価では，MDL に未掲載の URL を多数収集した．この URL には，MDL に掲載前の悪性 URL が含まれていると考えられる．そこで，2012 年 8 月 21 日に FTP ハニーポットで収集した URL を Marionette で検査した結果を分析したところ，表 2 に示すように，インターネットへのリダイレクトアクセスが 50 件発生し，内 48 件のアクセス先において iframe タグが挿入されていた．また，リダイレクトアクセスの内 38 件は国外の Web サイトへのリダイレクトだったが，リダイレクト先でリンク切れ状態が発生していた. さらに，リダイレクト先の URL を解析したところ，blackhole という exploit kit が使用された形跡を多数確認できた．このため，リダイレクト先の URL が，今後攻撃者が使用を開始する悪性 Web サイトである可能性が高いと考えられる．

このように，FTP ハニーポットを用いることで，未知の改ざん Web サイトや悪性 Web サイトを特定できる．これらの URL や，改ざんコンテンツの文字列は，セキュリティアプライアンスでの攻撃検知に利用できる．FTP ハニーポットの情報を用いてユーザから Web サイトへのアクセスを監査することで，ユーザをマルウェア感染から保護できる可能性を高めることができる．

6.3 考察

Web 経由のマルウェア感染において，改ざん Web サイトや悪性 Web サイトの動作は，

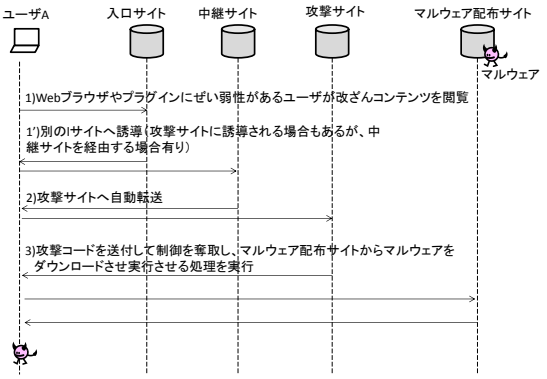

図 9 改ざん Web サイトや悪性 Web サイトの動作

入口サイトや中継サイトと，攻撃サイトおよびマルウェア配布サイトに分類できる．入口サイトや中継サイトは，アクセスしたユーザを攻撃サイトへリダイレクトさせる．攻撃サイトは，ユーザに対してマルウェア配布サイトからマルウェアをダウンロードさせて実行させる攻撃コードを送信する. Marionette は，図 9 に示すような, 改ざん Web サイトにアクセスした後のリダイレクト関係を分析できる．表 2 に示すように，FTP ハニーポットでは，iframe タグの挿入が多数確認されるなど，多くの入口サイトや中継サイトを特定できた．このため，Marionette を用いることで，一回の改ざんから，複数の中継サイトや攻撃サイトおよびマルウェア配布サイトも発見できると考えられえる．また，攻撃者が悪性 Web サイト URL の近傍に悪性 Web サイトを多数構築するという報告がある[12]．このため，FTP ハニーポットで収集した URL の近傍を Marionette で検査することで，未知の改ざん Web サイトや悪性 Web サイトを発見できる可能性がある．

FTP アカウント情報を不正入手した攻撃者は，このアカウント情報を用いてアクセスできる FTP サーバを最大限活用すると考えられる．このため，長期間おとり FTP サーバにアップロードされるコンテンツを分析することで，有効な情報を継続的に収集できると考えられる．また，攻撃者が改ざん後の Web サイ

トを確認する可能性を考慮すると，本来おとり Web サイトへのアクセスは可能な限り制限しないことが望ましい．しかし，一般ユーザがおとり Web サイトにアクセスした場合，マルウェアに感染する可能性があるため，おとり Web サイトへのアクセスは Marionette での検査時に発生する通信のみに限定している．このように，長期間の観測と，安全性を維持しつつ攻撃者とおとり Web サイトの通信を最大限許容する通信制御の実現は，今後の課題ではあるが，FTP ハニーポットの有効性を高める効果が期待できる．

7 おわりに

本稿では，おとりの FTP アカウント情報により，監視下にある Web サイトの改ざんを誘発して改ざんの特徴を分析する，FTP ハニーポットを提案した．

FTP ハニーポットでは，クライアント型ハニーポット Marionette で収集したマルウェア検体を，おとりの FTP アカウント情報を記憶させた開環境型マルウェア動的解析機能 Botnet Watcher で動作させるとともに，おとりの FTP サーバで攻撃者からのアクセスを収集する．FTP ハニーポットを用いた実態調査では，従来の手法では収集できない，攻撃者が使用する IP アドレスや，ユーザを悪性 Web サイトへ誘導するための改ざんコンテンツなどを継続的に収集できた．これらの情報は，Web サイトの改ざんを防止するサーバ側の対策手法と，ユーザから改ざん Web サイトや悪性 Web サイトへのアクセスを防止するユーザ側の対策手法に活用できると考えられる．

FTP ハニーポットを用いることで，ユーザを Web 経由のマルウェア感染から保護できる確率を高めることができる．今後の課題としては，長期間の観測と，安全性を維持しつつ攻撃者とおとり Web サイトの通信を最大限許容する通信制御の実現が挙げられる．

参考文献

[1] サイバークリーンセンター，“ホームページからの感染を防ぐために，” https://www.ccc.go.jp/detail/web/ index.html

[2] JPCERT/CC，“FTP アカウント情報を盗むマルウェアに関する注意喚起，” http://www.jpcert.or.jp/at/2010/ at100005.txt

[3] 独立行政法人情報処理推進機構，“Gumblar 攻撃に対する技術の現状と課題，” http://www.ipa.go.jp/security/fy22 /reports/tech1-tg/a_07.html

[4] C.Anle，“Advanced SQL Injection In SQL Server Applications,” An NGSSoftware Insight Security Research (NISR) Publication, 2002.

[5] The Web Application Security Consortium，“Web Application Firewall Evaluation Criteria，” http://projects.webappsec.org/ Web-Application-Firewall-Evaluation-Criteria

[6] The Honeynet PROJECT，“Capture-HPC Client Honeypot/ Honeyclient，” https://projects.honeynet.org/capture-hpc/

[7] LAC，“Gumblar（ガンブラ―）ウィルスによる新たなホームページ改ざん被害を確認，” http://www.lac.co.jp/info/alert /alert20100303.html

[8] M.Akiyama, T. Yagi and M.Itoh, “Searching Structural Neighborhood of Malicious URLs to Improve Blacklisting,” IEEE/IPSJ International Symposium on Applications and the Internet (SAINT) 2011, Jul, 2011.

[9] Anubis, “Anubis – analyzing unknown binaries,” http://anubis.iseclab.org/

[10] M.Akiyama, K.Aoki, Y.Kawakoya, M.Iwamura and M.Itoh, “Design and Implementation of High Interaction Client Honeypot for Drive-by-download Attacks,” IEICE TRANS.COMMUN., VOL.E93-B, NO5, pp1131-1139, May, 2010.

[11] 青木一史，川古谷裕平，岩村誠，伊藤光恭，“半透過性仮想インターネットによるマルウェアの動的解析，”マルウェア対策研究人材育成ワークショップ 2009，2009 年 10 月

[12] MalwareGroup.com, “malwaregroup,” http://www.malware group.com/