マルウェア対策技術

NTT情報流通プラットフォーム研究所では，マルウェア（悪意あるソフトウェア）感染によりユーザのPCやサーバがボット（不正に操作されるコンピュータ）として悪用される問題の解決に向けて，マルウェア対策技術の研究開発を行っています．この技術では，感染活動を検知してマルウェアを収集し，感染経路やマルウェアを解析して対策を講じることで，マルウェアの脅威からネットワークを保護します．

伊藤 光恭（いとう みつたか）/針生 剛男（はりう たけお）/谷本 直人（たにもと なおと）
岩村 誠（いわむら まこと）/八木 毅（やぎ たけし）/川古谷 裕平（かわこや ゆうへい）
青木 一史（あおき かずふみ）/秋山 満昭（あきやま みつあき）/中山 心太（なかやま しんた）
NTT情報流通プラットフォーム研究所

インターネットにおける サイバー攻撃の撲滅に向けて

近年，インターネット上のPCやサーバをコンピュータウイルスに代表されるようなマルウェアに感染させて個人情報を不正に取得するなどのサイバー攻撃が急増しています．さらに，マルウェアを用いて他のユーザのPCやサーバをボット化し，新たな攻撃の攻撃元として悪用する攻撃も継続しています．

マルウェア感染活動は日々複雑化しています．感染活動には，OS（Windows）の脆弱性に加え，サーバ上のWebアプリケーションやPCのWebブラウザなどの脆弱性も悪用されるため，感染の検知や感染経路の特定が非常に困難です．さらに，マルウェア自体も多様化しています．別のマルウェアをダウンロードする機能しか具備していないダウンローダの存在や，マルウェアの亜種の増加は，マルウェアの解析を一層困難にしています．

NTT情報流通プラットフォーム研究所では，感染活動を検知してマルウェアを収集し，感染経路やマルウェアを解析する技術の研究開発に取り組んでいます．これらの技術により，マルウェア感染の特徴情報を正確かつ効率的に特定することで，マルウェアによる被害を抑制し，安心・安全なネットワークの実現を目指しています．

マルウェア対策技術の概要

マルウェア対策技術は，**図1**に示す3つの軸で構成されています．今回は，マルウェア感染活動検知・収集に関する技術と，マルウェア解析に関する技術を紹介します．

■マルウェア感染活動検知・収集

おとりシステムであるハニーポットを用いて攻撃を受け，マルウェアを収集します．さらに，ハニーポットへの通信を解析し，マルウェア感染を防御するために有効となる情報を特定します．

一般的にハニーポットは，脆弱なシステムを模擬して安全に最低限の情報を入手する低対話型と，脆弱性を持つ実システムを利用して多くの情報を収集する高対話型に分類されます．高対話型は，マルウェアに感染するリスクが課題といわれていますが，NTT情報流通プラットフォーム研究所では，安全な高対話型ハニーポットの開発に成功しています．現在は，OS（Windows）の脆弱性を悪用する攻撃に対応するハニーポットと，Webアプリケーションの脆弱性を悪用する攻撃に対応するWebサーバ型ハニーポットと，Webブラウザの脆弱性を悪用する攻撃に対応するWebクライアント型ハニーポットを研究開発しています．

■マルウェア解析

ハニーポットで収集したマルウェアを解析し，機能を詳細に調査することで潜在的な脅威を解明します．マルウェアの解析には，マルウェアを実際に動作させて挙動を分析する動的解析と，マルウェアのプログラムコードを分析する静的解析があります．

マルウェアの動的解析には，完全に隔離された環境でマルウェアを動作させる閉環境型と，インターネットに接続できる環境でマルウェアを動作させる開環境型があります．さらに，両環境でデバッガ*を使用することによりマルウェアの挙動を詳細に監視できます．動的解析で得られたマルウェアの通信パターンは，マルウェア感染者の有無を確認する場合などに利用できます．

マルウェアの静的解析では，逆アセンブル等の技術によりマルウェアが保有する全機能を解明します．この際，プログラムの類似度に応じてマルウェアを複数のグループに分類し，各グ

＊デバッガ：プログラムのバグの発見や修正を支援するソフトウェア．

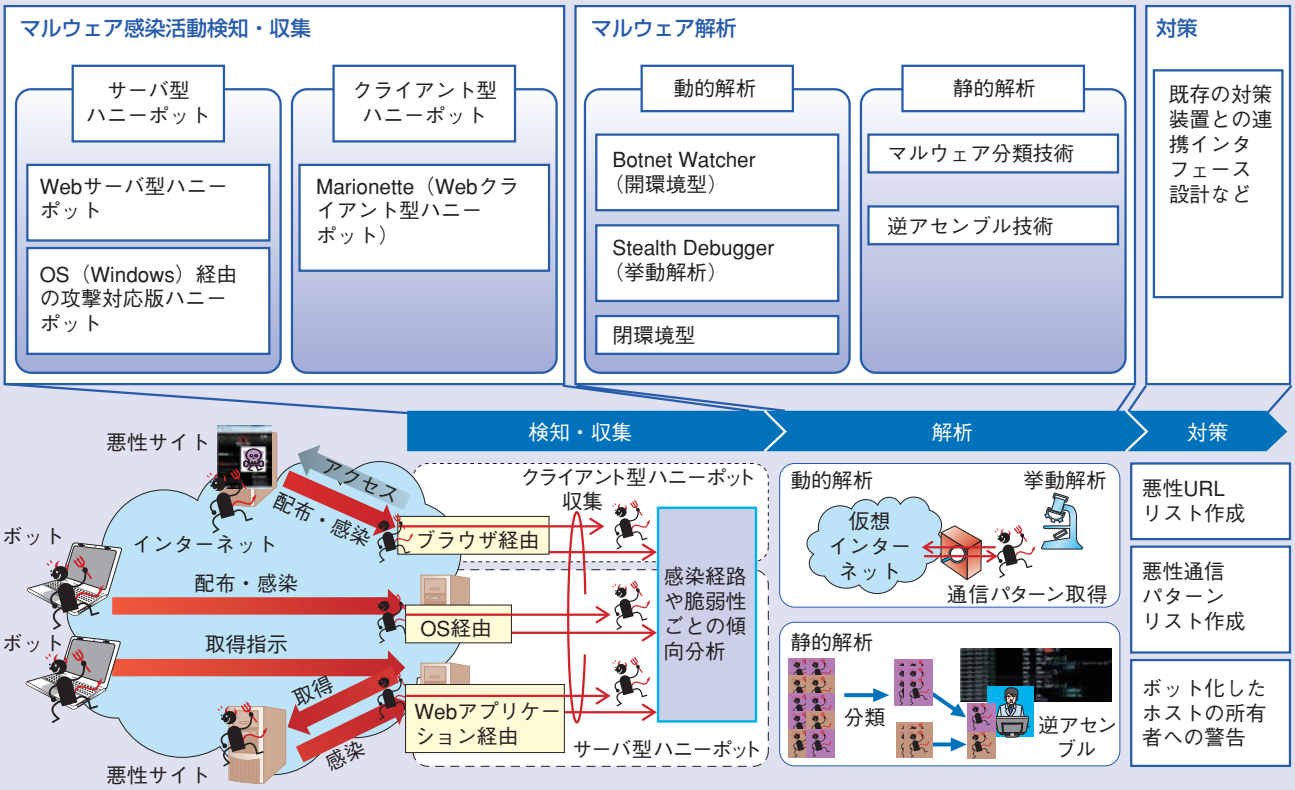

図1　マルウェア対策技術の概要

ループの代表的なマルウェアを分析することで効率化を図ります．

次に各技術の一例を紹介します．

Webサーバ型ハニーポット

ブログの普及にみられるように，Webアプリケーションはさまざまなサービスの基盤となっています．これに伴い，Webアプリケーションの脆弱性を標的とした攻撃コードの送付が急増しています．これにより，攻撃者は，Webサイト上の情報の改ざんや不正入手，さらにはWebサイトをマルウェアに感染させます．現在，これらの攻撃を防御するために，Webアプリケーションファイアウォールやログ監査が適用されています．しかし，Webサイトの構成に合わせて設定項目をカスタマイズしつつ，検知漏れや誤検知に対応する必要があり，運用コストが課題となっています．そこでNTT情報流通プラットフォーム研究所では，Webサイトへの攻撃を収集し，対策に活用可能な情報を自動的に特定する，高対話型のWebサーバ型ハニーポット（Webハニーポット）を研究開発しています．

Webハニーポットは，脆弱なWebアプリケーションを通常の手順で容易にインストール可能な構造を備えています．さらに，マルウェア感染などのリスクに対して安全性を確保するために，攻撃コードの実行状況を監視し，実行完了を検知した後，Webハニーポットを攻撃コード受信前の状態に戻します．これにより，インターネットからのマルウェアダウンロードなど，攻撃コードが引き起こした一連の動作に関する情報を安全かつ自動的に収集します．さらに，収集した情報を基にWebハニーポットへの通信を閉環境で再現し，情報の改ざんやマルウェア感染などの有害な状態の直接的な原因となっ

ている通信を正確に特定します．例えば，マルウェア感染を検知した場合は，悪用されたWebアプリケーションの脆弱性や，マルウェアをダウンロードする際に宛先に指定したマルウェアダウンロードサイトのURL等を特定できます．これにより，Webアプリケーションの新たな脆弱性の発見，および開発者や利用者への注意喚起が実現できます．さらに，顧客のWebサイトからこのURLへの通信をフィルタすることで，顧客のWebサイトをマルウェア感染の脅威から保護できます．なお，Webハニーポットで収集した情報を集中的に監視することで，安全性を効率的に管理できます（**図2**）．

Webクライアント型ハニーポット

Webブラウザやプラグインの脆弱性が多数発見され続けており，その脆弱性を標的とした攻撃が増加しています．脆弱性を持つWebブラウザは，攻撃コードが埋め込まれた悪性Webサイトを閲覧するだけでマルウェアに感染してしまいます．NTT情報流通プラットフォーム研究所が開発した「Marionette」は，悪性Webサイトを発見し，対策につなげるための詳細情報を収集する高対話型のWebクライアント型ハニーポットです．

Marionetteは高対話型ハニーポットの課題である安全性の確保のために，脆弱性個所の監視による正確な攻撃検知機能と，ダウンロードしたプログラムの動的隔離機能を備えています．加えて，並列分散処理の実行管理機能を実現しており，膨大な数のWebサイトから悪性Webサイトを高速に発見できます．

さらに，Marionetteはリンク情報を収集する機能を備えています．これは，悪性Webサイトへ自動転送するコードが一般Webサイトに埋め込まれる事例が急増しており，被害Webサイトを特定する必要があるためです．これらのWebサイト間のリンク構造は，踏み台となるサイトを経由して最終的に悪性Webサイトのコンテンツを自動的に読み込ませる構造になっており，これはマルウェア配布ネットワークと呼ばれています．Marionetteはこのような悪性Webサイトのネットワーク構造を抽出する機能を持っています．

これまでの調査から，攻撃コードが埋め込まれた悪性Webサイトは多数の踏み台サイトから参照されていること

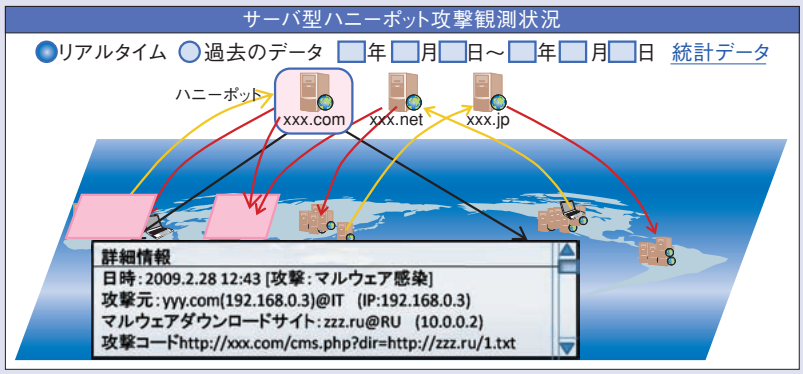

図2　Webハニーポットを用いたマルウェア感染活動の監視画面例

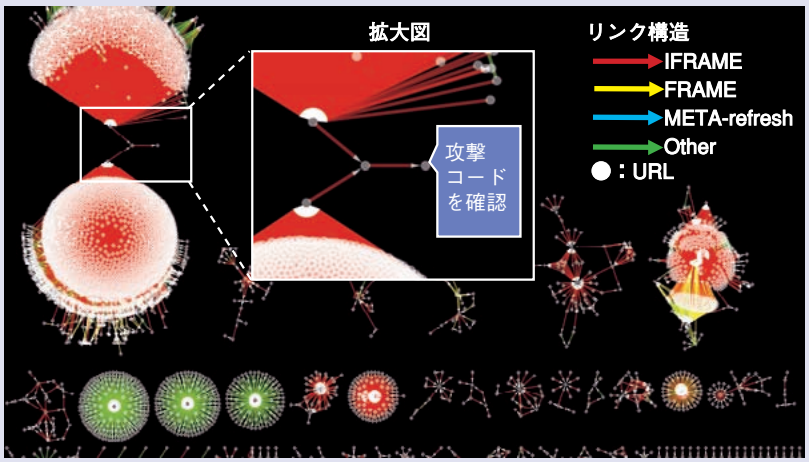

図3　Webブラウザを標的とするマルウェア配布ネットワークの可視化例

が判明しました（**図3**）．Marionetteで取得した情報を利用することで，例えば改ざんされて踏み台となっているサイトには“サイトの運用者に対する通知”と“コンテンツ修正依頼”，攻撃コードが配置されているサイトには“フィルタリング”や“サーバの停止”など被害に応じた対策が可能になります．

マルウェア動的解析技術

マルウェアの動的解析は，完全に隔離された環境で実施する閉環境型と，インターネットに接続できる環境で実施する開環境型とに大別できます．最近では，ボットやダウンローダといった，インターネットとの通信により脅威が顕在化するマルウェアが増えており，開環境型での解析が必要不可欠となっています．一方で，開環境型では，インターネットと接続した環境でマルウェアを動作させるので，安全性を保ちながら，いかにして解析を実現するかが課題となります．

また，マルウェアの詳細な分析を行う際に，デバッガを用いることがありますが，最近のマルウェアは巧妙につくられており，デバッガで解析されていることを検出すると正常に作動しなくなるものが存在します．

ここでは，開環境で動的解析を安全に行うための仕組みであるBotnet Watcherと，仮想マシンにデバッグ機能を持たせ，マルウェアによるデバッガ検出の回避を実現したStealth Debuggerについて説明します．

Botnet Watcherは，マルウェアから外部への通信を一度終端させ，ペイロードの検査を行います．検査の結果，ボットとC&C（Command and Control）サーバ間の通信や，他のマルウェアをダウンロードするための通信であった場合には，その通信をインターネットに転送します．また，インターネットに悪影響を及ぼすスパムメール送信やDDoS（Distributed Denial of Service）攻撃といった通信は，仮想インターネットで擬似的な応答を返し安全性を保ちます．Botnet Watcherを用いることで，マルウェアが送受信する通信の特徴をとらえることができます（**図4**）．

Stealth Debuggerは，仮想マシンを利用して，マルウェア実行環境の外側からデバッグ機能を提供します．一般的なデバッガは，CPUやOSのデバッグ支援機構を使用するため，マルウェアに検知されやすくなっていました．Stealth Debuggerでは，仮想マシンを利用し，マルウェアの実行環境とは別の仮想マシン上でデバッグを行います．また，従来のデバッグ支援機構に依存せずに動作します．Stealth Debuggerを用いることで，解析を妨害するマルウェアを容易に解析でき，マルウェアの機能解明を迅速に行えます．

マルウェア静的解析技術

近年のマルウェア数は増加の一途を辿り，それらすべてに対策を打つことはおろか，対策の優先度を決めることさえ難しくなっています．NTT情報流通プラットフォーム研究所ではこうした状況をかんがみ，マルウェアの全容解明を目的としてマルウェアの分類技術を中心としたマルウェア静的解析技術の研究に取り組んでいます．マルウェアの分類技術では，マルウェアのプログラムコードに着目することで，マルウェア間の類似度を算出します．これにより，マルウェアが潜在的に備える機能を踏まえた分類が可能になります．一方，昨今のマルウェアの多くは難読化ツールにより，元のプログラム

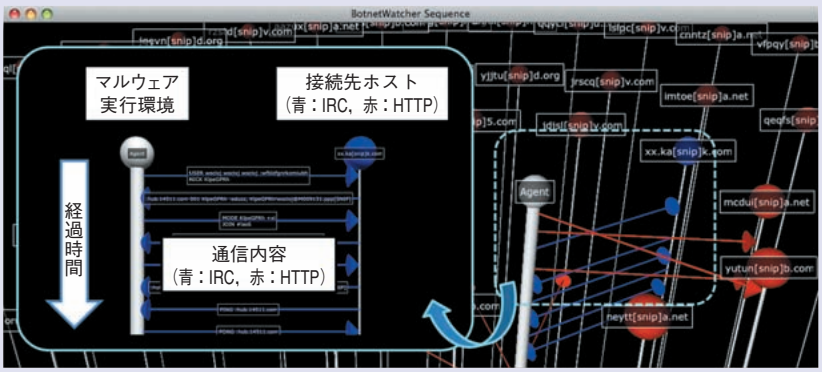

図4　マルウェアのインターネットにおける活動の可視化例

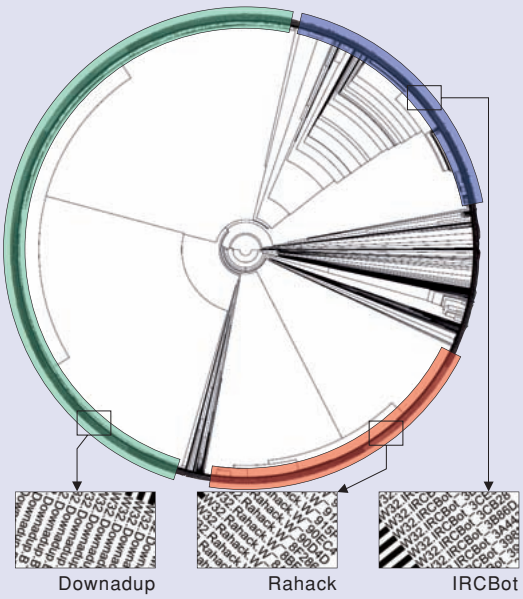

図 5　3 232検体の分類結果

コードが隠蔽されています．また，マルウェアのシンボル情報等を入手することも困難なため，機械語命令とデータが入り混じったバイナリ列の逆アセンブルが難しいといった問題もあります．そこでNTT情報流通プラットフォーム研究所では，これらの課題を踏まえ，新たに次の3つのマルウェア解析手法を開発し，それらを組み合わせたマルウェア分類システムを構築しました．

① 動的生成コードを抽出するアンパッキング手法

② 確率モデルに基づきもっともらしい逆アセンブル結果を算出する手法

③ 機械語命令系列の最長部分一致列を効率的に算出する手法

このシステムを利用し，我々が収集した3 232検体をクラスタリングした結果を**図 5** に示します．円周上には3 232検体の名称が並んでいます．大きい半径の弧でつながっているほど似ており，中心に近い弧でつながっているほど類似度が低いことを意味します．この分類結果では約50％をDownadup，約25％をRahack，約20％をIRCBotが占めていました．つまり今回の分類対象に関しては，すべてを解析せずとも，わずか数種類の検体を解析するだけで，マルウェアの機能の大半を把握できることが分かりました．

マルウェアの脅威の排除

NTTのマルウェア対策技術では，アクセスすべきではないURLを，既存のフィルタリング装置へ入力できる形式で特定できます．さらに，マルウェアの通信や機能の特徴に基づき，感染ユーザを高い精度で特定できます．現在は，特定した情報に応じた対策技術の具体化に取り組んでいます．

今後の展開

今後は，プロトタイプを用いてさまざまな検証実験を行っていくとともに，対策技術の具体化に取り組む予定です．

（後列左から）青木　一史/ 秋山　満昭/
八木　　毅/ 川古谷　裕平/
中山　心太
（前列左から）岩村　　誠/ 針生　剛男/
伊藤　光恭/ 谷本　直人

NTT情報流通プラットフォーム研究所では，今後もICTセキュリティ技術の研究開発を通じて，安心・安全なネットワークの実現を目指します．

◆問い合わせ先
NTT情報流通プラットフォーム研究所
セキュアコミュニケーション基盤プロジェクト
TEL　0422-59-3757
FAX　0422-59-5607
E-mail　itoh.mitsutaka@lab.ntt.co.jp