NTTグループのセキュリティビジネスを支えるマルウェア対策用セキュリティインテリジェンス

針生 剛男 †1 /横山 恵一 †2 /畑田 充弘 †3
矢田 健 †1 /八木 毅 †1 /秋山 満昭 †1
幾世 知範 †1 /高田 雄太 †1 /千葉 大紀
田中 恭之

NTTセキュアプラットフォーム研究所 †1
NTTコムセキュリティ †2
NTTコミュニケーションズ †3

マルウェア（悪意あるソフトウェア）に起因したサイバー攻撃が世界各地で社会問題化しています．本稿では，グローバル統合セキュリティサービスWideAngleを支えるセキュリティインテリジェンス技術について紹介します．

サイバー攻撃の社会問題化

近年，サイバー攻撃により，さまざまな社会問題が発生しています．特にマルウェア感染に伴う被害は甚大で，国家レベルの情報漏洩を引き起こしています． PCがマルウェアに感染する例を**図1**に示します．Webブラウザやプラグインに脆弱性があるPCは，攻撃者が用意した自動転送用コンテンツが配置された入口・中継サイトにアクセスすると，攻撃コードが配置された攻撃サイトに自動転送され，攻撃コードの受信によって，マルウェアをダウンロードして感染してしまいます．これら一連の悪性サイトへのアクセスによってマルウェアに感染してしまったPCは，攻撃者が用意した指令

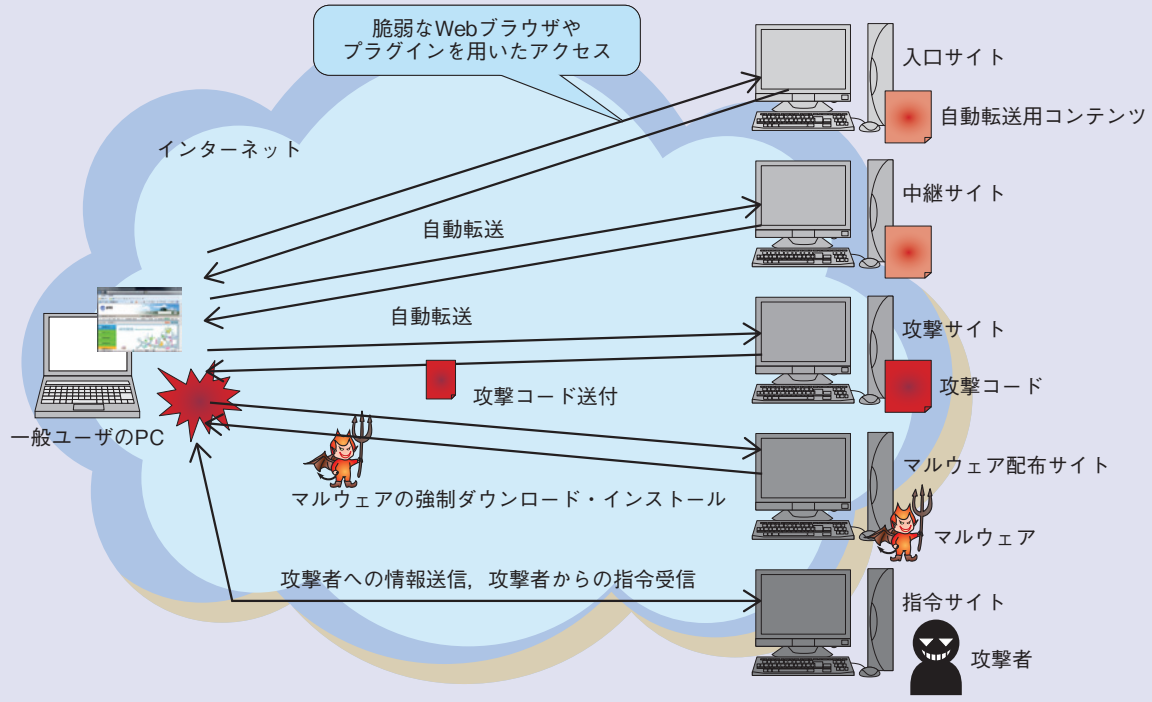


図1　マルウェア感染攻撃

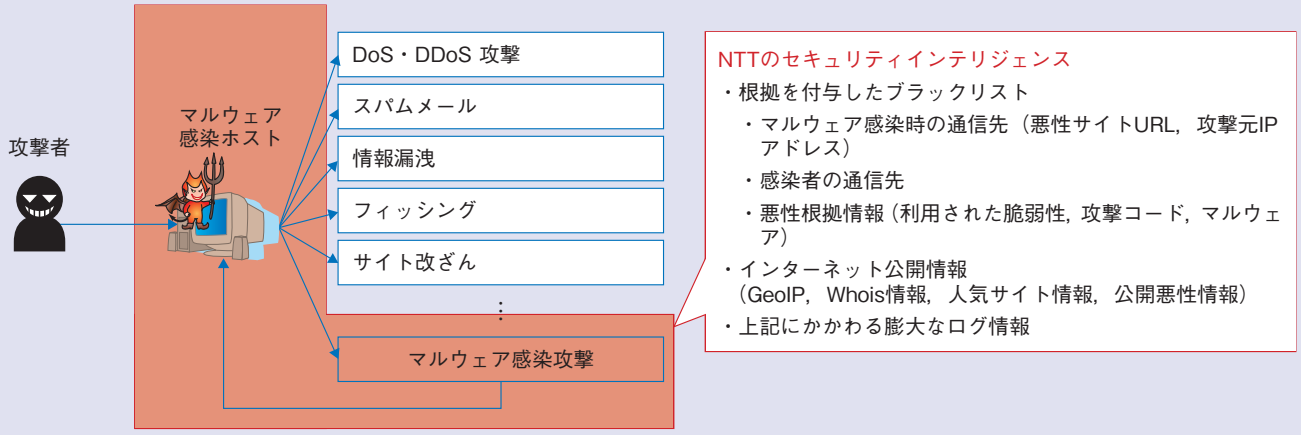


図2　NTTのセキュリティインテリジェンス

サイトとの間で情報の送受信を実施してしまい，情報漏洩などが発生してしまいます．

NTT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きました[(1)]．具体的には，攻撃を継続的に収集して解析することで，最新のマルウェア感染の特徴を正確かつ効率的に特定する技術を創出してきました．しかし，昨今では，非常に短いサイクルで新たなタイプの攻撃やマルウェアが出現し，攻撃も複雑化が進んでいるため，各技術単体では対策につながるサービスを創出することが困難でした．

そこで，過去の研究開発や攻撃観測から得た経験的知識から，マルウェア感染時から感染後までに発生する攻撃や通信のデータを横断的に解析して得られる，マルウェア感染に関連する通信先などの悪性情報（セキュリティインテリジェンス）の重要性にたどり着き，世界に先駆けて，インテリジェンス創出技術の研究開発に着手しました[(2)]．

さらに，グローバルセキュリティビジネスで世界を牽引するNTTコミュニケーションズと連携し，セキュリティインテリジェンスをマネージドセキュリティサービス“WideAngle”[(3)]へビジネス展開しました．

NTTのセキュリティインテリジェンス

一般的なセキュリティインテリジェンスは，サイバー攻撃防御用の情報を示します．例えば，DDoS（Distributed Denial of Service）攻撃やスパムメールの発信元となっているIPアドレスや，攻撃者がマルウェアを操作するために設置している指令（C&C: Command and Control）サーバや情報漏洩先のIPアドレス，フィッシングサイトや改ざんされたWebサイトのURLなどが挙げられます．

さまざまなサイバー攻撃の発信元は，マルウェアに感染して攻撃者に乗っ取られたPCやサーバです．このため，サイバー攻撃を根本的に解決するためには，マルウェア感染対策用のセキュリティインテリジェンスが非常に重要となります．また，セキュリティインテリジェンスをビジネスへ展開するためには，悪性と判断した根拠情報や使用用途に関する情報を明示する必要があります．

NTT研究所のセキュリティインテリジェンスは，**図2**に示すように，マルウェア感染時の通信先や感染者の通信先にかかわるIPアドレスやURLなどの情報で構成されています．各情報へは，独自のおとりシステム（ハニーポット）技術やマルウェア動的解析技術で特定した根拠情報を付与しています．また，各技術を連携させ，他社では収集できない悪性サイトURLを特定します．さらに，収集した悪性サイトURLを解析し，未知の悪性サイトURLを特定します．

■ハニーポット

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，マルウェア感染の際に利用された脆弱性の情報を根拠情報として特定するとともに，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．

私たちは，マルウェア感染活動の動

向に応じたハニーポットを研究開発しています．現在は，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ブラウザやプラグインの脆弱性を悪用する攻撃に対応するハニークライアントを研究開発しています．今回は，インテリジェンス創出の中核を担うハニークライアントを紹介します．

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，私たちは，安全な高対話型ハニークライアントの開発に成功しています．また，低対話型は，収集できる情報に制限があるといわれていますが，情報収集力を改善した低対話型ハニークライアントの開発にも成功しています．ハニークライアントを用いることで，マルウェア感染を検知し，アクセスするとマルウェアに感染する悪性サイトのURLを特定できます．例えば，このURLへのアクセスを禁止することで，ユーザをマルウェア感染から守ることができます．

■マルウェア動的解析

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．さらに，マルウェア感染によって発生する通信を解析し，追加のマルウェアを取得する際の通信先サーバや，攻撃者が設置した指令サーバなどを発見することで，マルウェア感染の被害を抑制するために有効となる情報を特定します．

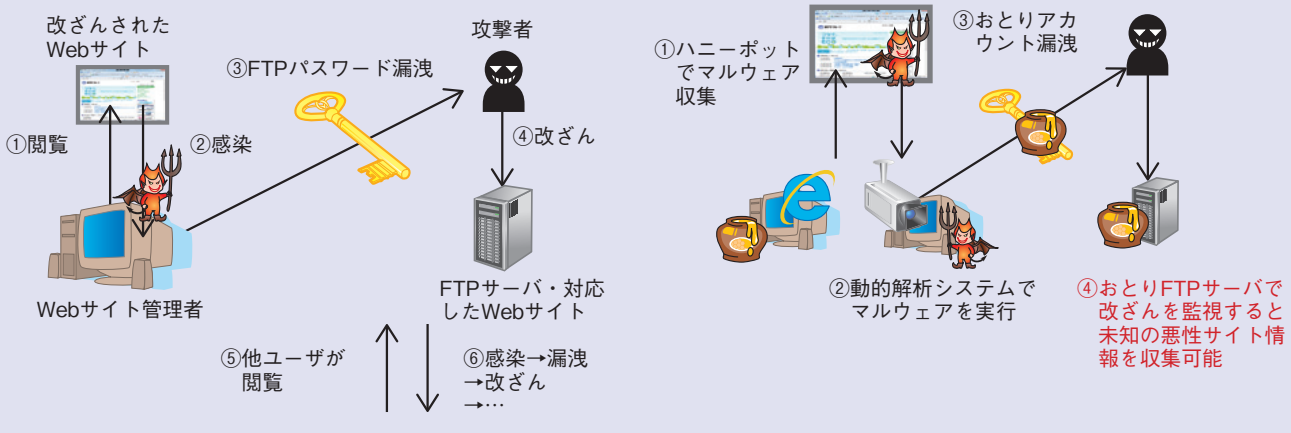
マルウェアの解析には，マルウェアを実際に動作させて挙動を明らかにする動的解析と，マルウェアのプログラムコードを読み解く静的解析があります．今回は，動的解析を紹介します．

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．また，両環境でデバッガを使用することで，マルウェアの挙動を詳細に監視できます．さらに，テイント解析技術と呼ばれる，システム内でやり取りされるデータの流れを追跡する技術を用いることで，悪性な挙動を引き起こすデータの送信元を，攻撃者が用意した指令サーバとして特定できます．例えば，追加のマルウェアを取得する際の通信先サーバや指令サーバにアクセスしているPCを特定することで，マルウェアに感染しているPCを発見できます．

■ハニートークン

ハニーポットで収集したマルウェアを動的解析する際に，解析環境におとりのWebサイト管理者アカウント情報を配置しておくことで，管理下で攻撃者におとりのWebサイトを改ざんさせることができます．これにより，最新の攻撃情報を収集できます．

前述のとおり，近年では，悪性サイトを閲覧したユーザがマルウェアに感染する攻撃が最大の脅威となっています．この攻撃で感染させるマルウェアの一部は，各種アカウント情報を収集して外部へ送信する機能を持っています．このため，**図3**に示すように，感



(a)　PCに対する典型的な攻撃　　(b)　ハニートークンを用いた独自観測技術

図3　ハニートークン

染したPCにWebサイト管理者アカウント情報が記録されている場合は，その情報が攻撃者に漏洩し，そのWebサイトは攻撃者に改ざんされてさらなる攻撃に悪用されてしまいます．

ハニートークンとは，おとりの情報全般を示します．Webサイトのコンテンツは FTPサーバにて管理されることが多いため，ハニートークンとしておとりのFTPアカウント情報を用意します．攻撃者は，別途用意するおとりのFTPサーバに対してハニートークンの情報を用いてログインし，コンテンツを改ざんします．この改ざんコンテンツをハニーポットで検査することで，攻撃者が用意した最新の攻撃に関するセキュリティインテリジェンスを収集できます．

本技術をまとめた論文[4]は，世界トップレベル国際会議にて日本人として10年ぶりに採録されるなど，世界で高く評価されています．

■悪性サイト近傍探索

攻撃者は，セキュリティインテリジェンスによって攻撃が防御されないように，多くの悪性サイトを構築します．この際，多くのコストを費やすことはできないため，追加コストが不要なかたちで悪性サイトを構築します．私たちは，その動きを先読みし，攻撃者が用意する可能性が高いWeb空間を探索し，悪性サイトを発見します．

この探索技術では，**図4**に示すように，既知の悪性サイトURLと同一のプライベートドメインに存在するURL群において，既知の悪性サイトURLと同一のパス構造を持つURLを抽出し，ハニーポットで検査します．既知の悪性サイトURLを管理する攻撃者は，このようなURLをコスト負担なく生成できるため，この探索技術によって攻撃者がセキュリティインテリジェンス回避のために用意した悪性サイトURLを発見することができます．

本技術をまとめた論文[5]は，メジャーな国際会議で論文賞を受賞するなど，世界で認められています．

セキュリティインテリジェンスのグローバルビジネス展開

NTT研究所で創出したハニーポットや解析技術およびセキュリティインテリジェンスは，NTTコミュニケーションズのサービスに活用されています．**図5**に示すように，NTTコミュニケーションズは，研究所の技術やセキュリティインテリジェンスと既存製品とを組み合わせて運用することで，NTTコミュニケーションズ独自のセキュリティインテリジェンスを創出しています．

セキュリティインテリジェンスをビジネスに展開する場合，ログを監査するサービスや，ユーザのアクセスをフィルタリングするサービス，ユーザのWebサイトを監査するサービスなどが考えられます．NTTコミュニケーションズのマネージドセキュリティ

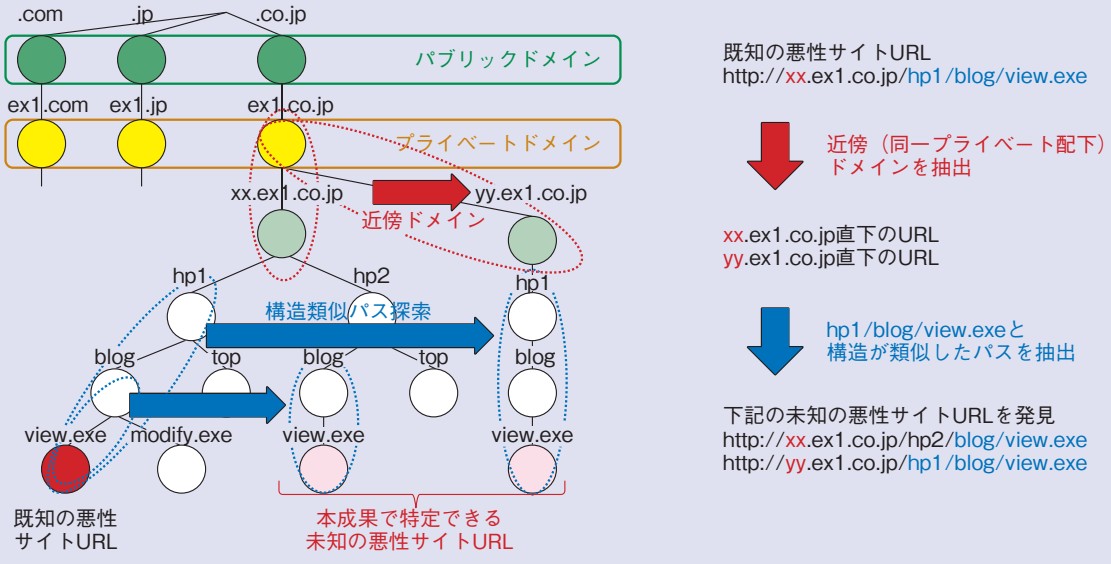


図4　悪性サイト近傍探索

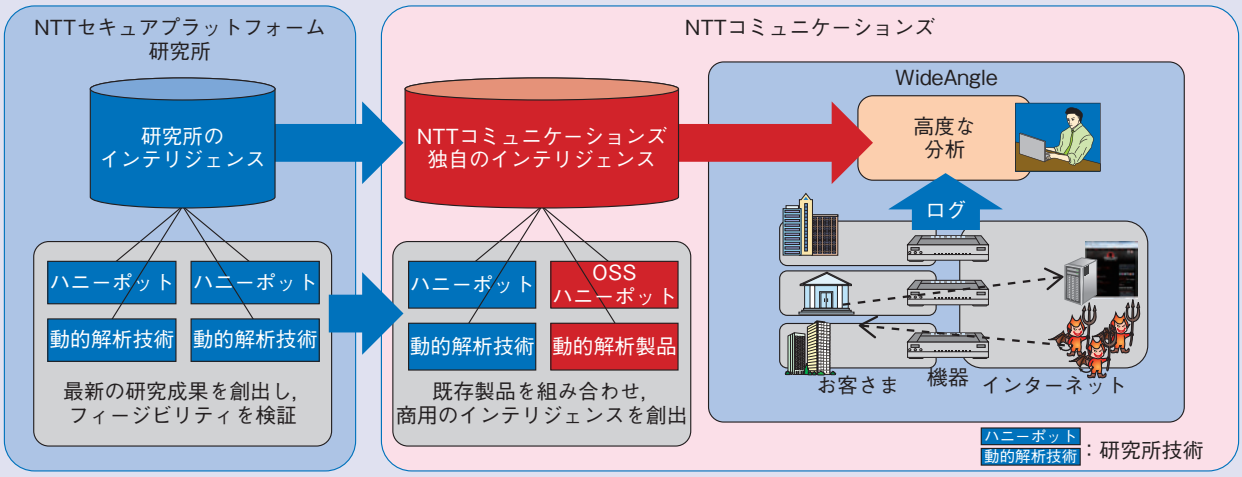


図5　グローバルビジネス展開

サービスでは，2013年2月から，セキュリティインテリジェンスをログ監査サービスに活用しています．このサービスでは，高度な自動相関分析によるセキュリティリスクの検知や脅威レベルの自動評価を実施する際に，セキュリティインテリジェンスを活用しています．これにより，さまざまなICT機器から収集される通信履歴など膨大なセキュリティ情報を自動で相関分析し，高度かつ迅速な対応を実現しています．

現在，マネージドセキュリティサービスは“WideAngle”というブランド名で，世界14カ国900名以上の専門家によるセキュリティ提供体制のもと，24時間365日の高度なセキュリティ監視を行うことで，ユーザに対してグローバルシームレスで統合的なセキュリティ対策を実現しています．

今後の展開

今後は，グローバルビジネスにおける競争力を向上できる，世界トップレベル技術のプロトタイピングを進めながら，技術のビジネス展開を図っていく予定です．

■参考文献

⑴ 伊藤・針生・谷本・岩村・八木・川古谷・青木・秋山・中山：“マルウェア対策技術，”NTT技術ジャーナル，Vol.22，No.3，pp.40-44，2010.
⑵ 針生・秋山・青木・八木・岩村・倉上：“進化するマルウェア等によるサイバー攻撃の検知・解析・対策技術，”NTT技術ジャーナル，Vol.24，No.8，pp.13-17，2012.
⑶ https://www.ntt.com/wideangle_security/
⑷ M. Akiyama，T. Yagi，K. Aoki，T. Hariu，and Y. Kadobayashi：“Active Credential Leakage for Observing Web-Based Attack Cycle，”Proc. of RAID2013，Vol.8145，pp.223-243，Rodney Bay，St.Lusia，Oct. 2013.
⑸ M. Akiyama，T. Yagi，and M. Itoh：“Searching Structural Neighborhood of Malicious URLs to Improve Blacklisting，”SAINT2011，pp.1-10，Munich，Germany，July 2011.

（上段後列左から）秋山 満昭/ 千葉 大紀/ 幾世 知範/ 高田 雄太
（上段前列左から）八木 毅/ 針生 剛男/ 矢田 健
（下段左から）畑田 充弘/ 横山 恵一/ 田中 恭之

NTTセキュアプラットフォーム研究所とNTTコミュニケーションズ，およびNTTコムセキュリティは，今後もセキュリティ技術の研究開発やビジネス化を通じて，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セキュアプラットフォーム研究所
サイバーセキュリティプロジェクト
TEL　0422-59-3892
FAX　0422-59-3844
E-mail　yagi.takeshi@lab.ntt.co.jp