2017サイバー攻撃最新動向 NEC Cyber Threat Intelligence活用モデル

磯田 弘司　角丸 貴洋

要 旨

近年のサイバー攻撃は、マルウェア単体だけでなくターゲットのシステムにある管理ツールを巧みに悪用して検知を回避するなど、従来のセキュリティ対策だけでは防御が難しくなっています。進化し続ける攻撃手法に対抗するため、サイバー攻撃手法分析などのCyber Threat Intelligence（CTI）の活用が注目を集めています。本稿では、CTIを活用して得られた最近のサイバー攻撃手法について紹介します。

KeyWords

サイバー攻撃対策／Cyber Threat Intelligence／マルウェア／ランサムウェア

1. はじめに

NECは、2017年3月、米国国土安全保障省（DHS）が推進する、官民でサイバー攻撃の脅威情報を迅速に共有する枠組み「Automated Indicator Sharing（AIS）」に加入し、サイバーセキュリティ事業において技術・人材と並び重要な情報（CTI）を強化しています[1)]。CTIは、脅威となる要素の相互関係、メカニズム、指標などの分析に基づき、さまざまな脅威への対処すべき判断基準を提供、セキュリティ対策の強化と運用コスト削減を目指します。

2. CTIを活用したサイバー攻撃に対する防御強化

2.1 日本の企業・組織を狙う「URSNIF/DreamBot」

2016年6月頃から、バンキングマルウェアの「URSNIF」に感染させるさまざまな日本語のスパムメールが配布されています。受信者が添付ファイルを開くと不正サイトから不正コードがダウンロードされ、機密情報などが盗まれる可能性があります。警察庁・警視庁・一般財団法人 日本サイバー犯罪対策センター（JC3）から頻繁に注意喚起が出ており、被害も発生し続けています。**図1**は、2017年1月から6月末まで特定組織に送信されたスパムメールの情報を、ピボット分析した一例です。

ピボット分析は、点在する個々の事象を収集整理し、相関関係を面でとらえて防御策の検討に利用します。図1の場合、攻撃者のドメインやIPアドレスなどが、時期により3つのパターンで実行されていたことが判明しました。

これを世界地図に表したのが**図2**です。

更に、攻撃者が使用するIPアドレスの範囲、使い回す周期などを洗い出し、防御体制を整えることができます。NECではさまざまな情報ソースから最新のサイバー攻撃

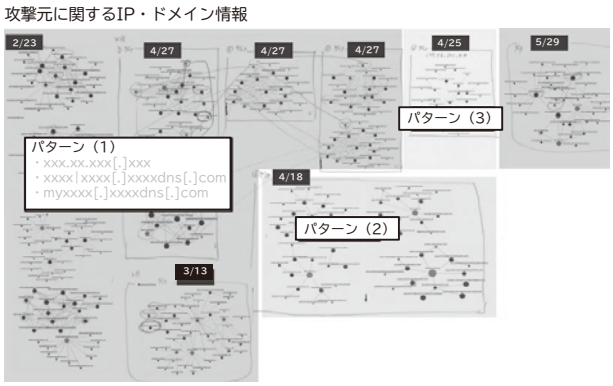


図1　攻撃元の分析結果1

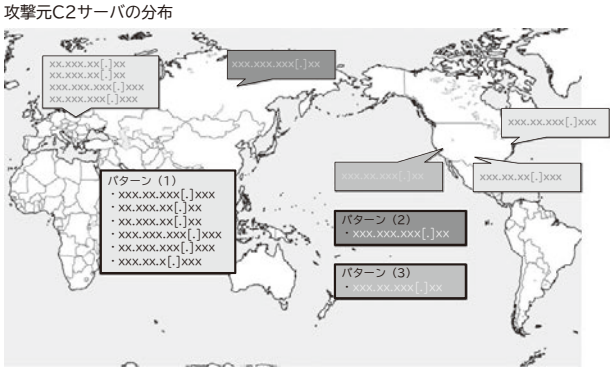


図2　攻撃元の分析結果2

図3　NEC Cyber Threat Map

情報を収集・分析して**図3**のように見える化し、セキュリティ対策の基盤として活用しています。

2.2 PowerShellを使うマルウェアが増加、どう防ぐか

最近、実行ファイルを直接使用しないファイルレスマルウェアの脅威が、よくメディアに取り上げられるようになりました。しかし、これは新しい脅威の概念ではありません。例えば、2001年の「Code Red」や2003年の「SQL Slammer」は、メモリ上でのみ動作し、ディスク上には何も書き込みませんでした。IoTマルウェアの「Mirai」や、最近の米国国家安全保障局（NSA）から流出したバックドアの「DoublePulsar」も同様で、ディスク上に痕跡を残しません。攻撃対象のシステムに実装されているWindowsの標準機能WMI[2]や、PowerShell[3]をリモートから悪用し、攻撃で使うファイルは最小限に抑えて、目的達成後は不正ファイルやログを消去します。本稿の作成時点では、以下の特徴が明らかになっています。事案については、JPCERT/CCで紹介されています[4]。

・不正なPowerShellが実行されてもログが残らない
・OSを再起動すると不正コードの痕跡も残らない
・メモリ上に直接読み込まれるので検知が難しい
・HTTPS通信で実行されるとネットワーク検知が困難
・攻撃手法の特定や発見が難しい

現在、「PowerShellを使った攻撃の検知は難しい」と思い込まれている企業・組織があります。Windows7に実装されているPowerShell 2.0の場合は、起動・終了程度しか記録できませんでしたが、5.0にアップデートしロギングを有効にすることにより、実行されたPowerShellコマンドやスクリプトなど攻撃者の行動を記録できます。また、Windowsの「Module Logging」や[5]、WindowsのSysmonを使うことでPowerShellなどのログを出力して可視化できます。既存の環境を生かしつつ、どのような運用設計でセキュリティ強度を向上させられるか、日々発生するさまざまな脅威を検証しつつ、より精度の高いIntelligenceを生成することにより、「セキュアな運用」に活用できます。

2.3「WannaCry」の脅威、脆弱性対策だけで防御できない

2017年5月12日（米国時間）、英国の医療機関や世界各国の企業・組織で「WannaCry」ランサムウェア（別名：WannaCrypt、WannaCryptor、Wcryなど）による被害が発生しました[6]（**表**）。

各種メディアなどでは、「MS17-010」のセキュリティパッチを適用することで被害が防げると報道されてきました。NECでは速やかに当該検体を入手して検証、その結果「WannaCry」にはWindowsのファイル共有プロトコルSMBv1の脆弱性を悪用して拡散するワーム機能とランサムウェアの機能が別々に機能することが判明、「MS17-010」を適用後もランサムウェア対策は必須であ

表　「WannaCry」ランサムウェアによる被害発生のTime Line

2016年9月	MicrosoftがSMBv1の使用停止を推奨
2017年1月	US-CERTがSMBv1の無効化を提唱
3月14日	Microsoftが「MS17-010」をリリース
4月14日	Shadow Brokersが攻撃ツールEternalBlueを公開
4月25日	DropboxのURLを悪用したWannaCryが発生
5月12日	**WannaCryによるサイバー攻撃が世界各国で発生**
5月14日	IPAがWannaCryの就業前対応について注意喚起
5月23日	Symantecは北朝鮮関与の可能性について発表

図4　「MS17-010」を適用したWindows 10で感染

ることを、NECグループ内のCSIRT担当者やSEに検証結果を展開しました（**図4**）。

2.4 破壊型ランサムウェアPetyaの脅威、真の目的

2017年6月27日（現地時間）、欧州各国を中心に、再びランサムウェア感染被害（NotPetya、PetrWrap、GoldenEyeなど）が確認され、多くの企業・組織で深刻な被害が発生しました[7)]。

2017年6月28日時点での被害状況は以下となります。

・ウクライナ：政府機関、企業、銀行は約3分の1、国内PCの10台に1台が感染、チェルノブイリ原発の放射線計測システムで障害
・ロシア：国営石油会社、中堅石油会社
・デンマーク：海運事業者大手
・米国：製薬会社大手、菓子メーカー大手

感染経路は、次のとおりです。

・ウクライナの企業で使われている会計ソフト「MeDoc」
・Microsoft Officeの脆弱性（CVE-2017-0199）の悪用
・ウクライナの主要サイトを改ざんした水飲み場型攻撃

2016年に発生した「Petya」ランサムウェアのコードが一部使われていますが、Windows上のすべてのファイル情報を管理するMFT（Master File Table）を暗号化した鍵を破棄して復旧不可にしたため、「NotPetya」と呼ばれています。感染拡大には、「WannaCry」と同様、ハッキングツールの「EternalBlue」やWindowsの正規ツールPsExec、WMIコマンドが使われています。「WannaCry」はSMBv1の脆弱性を悪用して外部ネットワークに感染拡大しますが、「Petya」はターゲット組織内部に感染拡大を図ります。当該攻撃には以下の特徴があります。

・ファイルは暗号化後のファイルで上書きされる
・暗号に使われた Salsa20の鍵が破棄され復旧不可
・ランサムウェアの常套手段である「Tor」は未使用
・連絡先はブロックされたメールアドレスのみ
・管理者情報を搾取、Mimikatzの類似ツールを使用
・ウクライナ憲法記念日の前日に攻撃が発生
・2016年の「Petya」とは異なり復号できない

前述の事実関係から、身代金搾取が目的ではなく、国家レベルでの破壊活動が推察されます。2017年5月にウクライナで発生した「Xdata」というランサムウェアは、今回と同様、ウクライナで普及している会計ソフトMeDocのアップデート機能を悪用し、認証情報を盗むMimiktzツールなどで多くの被害が発生しています。また、2015年12月と2016年12月にはウクライナでサイバー攻撃により大規模停電が発生しました。これはBlackEnergy APTという攻撃者グループによるものと、ロシアのKaspersky社が報告しています[8)]。その後、ウクライナの親ロシア派が「新国家」宣言し、米海軍がウクライナ軍と共同訓練を行うなど、軍事的緊張が続いています。CTIは技術面だけでなく、国際情勢や攻撃の動機となる背景を考察することも重要です。

2.5 日本の組織を執拗に狙うBRONZE BUTLER

「BRONZE BUTLER」（別名：Tick）は、セキュリティベンダーのDELL SecureWorksが命名した攻撃グループで、高い技術力を使って日本の特定組織の機密情報を執拗に狙います。いったん侵入を許すと、数年にわたって繰り返しサイバースパイ活動を行います[8)]。

・攻撃目的
　日本企業の「技術情報、知財情報」
・攻撃対象
　重要インフラと関連企業が標的
・標的型攻撃メール
　メールの不正な添付ファイルで感染
　季節の挨拶メールを偽装した標的型メール
　水飲み場型攻撃

参考情報:
Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.1;+Trident/4.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET4.0E)

データ分析ツールのSplunkによるログ解析の一例:
host=ISC_Proxy UserAgent="Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; SV1)" ¦ eval MalType = if(match(URL,".*¥.(gif¦asp¦jpg)$"),"Daserf", MalType)

図5　調査時のログ解析の一例

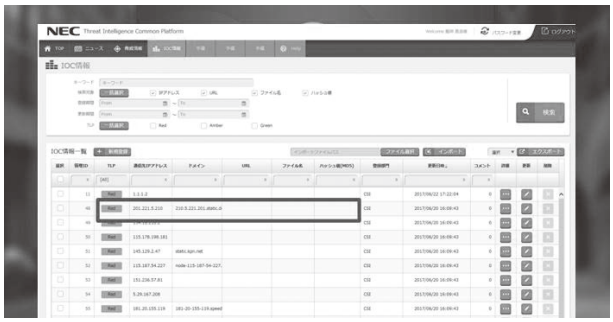


図6　NEC Cyber Threat Intelligence画面イメージ

・遠隔操作で使用するRAT（Remote Access Tool、Remote Administration Tool）
Daserf、Datper、xxmmなど

Symantecは当該攻撃を「Tick」と命名し、10年以上前から活動していると報告しています。

当該攻撃では、50MB以上のごみデータが含まれ、既存のセキュリティアプライアンス製品で検証されずにすり抜ける可能性があります。SecureWorksの下記分析を参考に、ある特定組織のログ情報を調べた結果、4台の端末が感染、更にそれらから数十台の水平展開された感染が見つかりましたが、早期であったため大事には至りませんでした。

図5は、調査時のログ解析の一例です。

3. まとめ

NECでは、CTIを活用してお客様を支援すべく、さまざまなIntelligenceの強化を図っています。マルウェアなどの攻撃の指標となる脅威情報は、構造化して表現する言語STIX（Structured Threat Information eXpression）[9]をベースにデータを生成します。データは人が見る脅威情報と、各種セキュリティ製品・サービスに設定して自動防御するための脅威情報（不正なドメイン、IPアドレス、ハッシュ値など）があり、これらを日々検証して精度を高めています（**図6**）。

システムの自動化やAIの活用による分析能力の向上を進めていますが、教師データを実装するには人間による適切に解析した結果と判断が不可欠です。また、進化し続けているサイバー攻撃手法に対しては、継続的な対策強化の実施が重要です。

参考文献

1) NECプレスリリース：NEC、米国国土安全保障省が推進する官民でサイバー脅威情報を共有する枠組み「AIS」に加入，2017.3
http://jpn.nec.com/press/201703/20170315_01.html
2) Microsoft：WMI の FAQ
https://technet.microsoft.com/ja-jp/scriptcenter/ff576025.aspx
3) Microsoft：Windows PowerShell でのスクリプティング
https://technet.microsoft.com/ja-jp/scriptcenter/powershell.aspx
4) JPCERT/CC：PowerSploitを悪用して感染するマルウエア，2017.2
https://www.jpcert.or.jp/magazine/acreport-ChChes_ps1.html
5) IPA：世界中で感染が拡大中のランサムウェアに悪用されているMicrosoft製品の脆弱性対策について，2017.5
https://www.ipa.go.jp/security/ciadr/vul/20170514-ransomware.html
6) IPA：感染が拡大中のランサムウェアの対策について，2017.6
https://www.ipa.go.jp/security/ciadr/vul/20170628-ransomware.html
7) From BlackEnergy to ExPetr，2017.6
https://securelist.com/from-blackenergy-to-expetr/78937/
8) 日本企業を狙う高度なサイバー攻撃の全貌– BRONZE BUTLER，2017.6
https://www.secureworks.jp/resources/rp-bronze-butler
9) STIX（脅威情報構造化記述形式）
https://www.oasis-open.org/committees/cti/

執筆者プロフィール

磯田 弘司

サイバーセキュリティ戦略本部
セキュリティ技術センター
シニアエキスパート

角丸 貴洋

CISSP
サイバーセキュリティ戦略本部
セキュリティ技術センター
主任

NEC 技報のご案内

NEC 技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報（日本語）　NEC Technical Journal（英語）

Vol.70 No.2　ビジネスの安全・安心を支えるサイバーセキュリティ特集
～Futureproof Security　安心の先へ。～

ビジネスの安全・安心を支えるサイバーセキュリティ特集によせて
増大するサイバー犯罪の根源的な解決へ～“産学官”のオールジャパンで立ち向かう第三者機関の姿とは？～
サイバーセキュリティを取り巻く社会動向とNECの取り組み

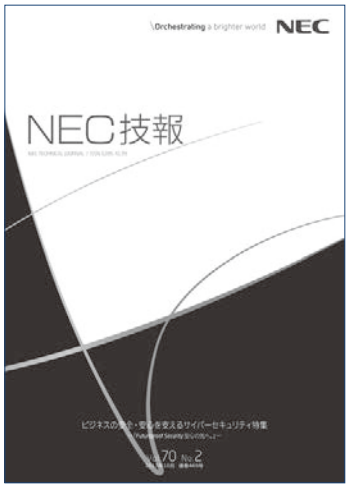
◇ 特集論文

社会の動向とNECの取り組み
重要インフラに対するサイバー攻撃の実態と分析
2017 サイバー攻撃最新動向 NEC Cyber Threat Intelligence活用モデル
サイバーセキュリティ対策の社内事例

サイバーセキュリティソリューション
複雑化 / 高度化するサイバー脅威に対抗するSOCとセキュリティ監視サービス
攻撃被害を極小化するためのインシデント対応支援ソリューション
サイバー演習によるインシデントハンドリング能力の強化
セキュリティ統合管理・対処ソリューション「NEC Cyber Security Platform」
クラウド型ファイル暗号化サービス －ActSecureクラウドセキュアファイルサービス－
セキュリティLCMサービス
EMMを活用したセキュアなモバイルワークソリューション
IoT 時代の経営を支援するサイバーセキュリティコンサルティング

サイバーセキュリティへのAI技術の活用
AI（人工知能）を活用した未知のサイバー攻撃対策
採るべき対策の「なぜ？」に答えるAIの可能性
オープンソースインテリジェンスを活用したサイバー脅威の検出と自動分析
犯罪捜査支援のためのサイバー・フィジカル統合分析技術

お客様に安全・安心を届けるための社内の取り組み
安全・安心な製品・サービスをご提供するための取り組み ～セキュア開発・運用～
サイバーセキュリティ人材のタレントマネジメント



Vol.70 No.2
（2017年10月）

特集TOP