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

川北 将　島 成佳

要 旨

サイバー攻撃手法や犯行声明などの脅威情報は、ソーシャルメディアやディープウェブを通じて流通しますが、情報量の爆発やセキュリティアナリストの人員不足からそうした情報を早急に察知することが難しく、攻撃被害の備えに遅れが生じる課題があります。本稿では、金融工学で用いられるテクニカル分析手法によって脅威トレンドがピークに達する兆候をつかみ、同時に、ディープラーニングを活用してサイバー攻撃の全体像を分析する自動化されたプロアクティブな攻撃予防技術について紹介します。

KeyWords　サイバーセキュリティ／オープンソースインテリジェンス／脅威情報／ソーシャルメディア／ディープウェブ／STIX／TAXII

1. はじめに

昨今、サイバー攻撃による被害が世界各国で発生しており社会問題となっています。しばしば標的となる重要インフラ、政府機関及び民間企業を滞りなく運営するには、各組織を守るセキュリティアナリストが常日頃からサイバー攻撃の予兆となる膨大な脅威情報を収集・分析し、事案発生が予期される場合に即応する体制が必要です。

組織内で利用するソフトウェア・ハードウェアに新たな脆弱性が発見された場合、パッチの適用や通信遮断などの適切な対処をせずに放置するとその脆弱性を用いたサイバー攻撃を受けて、組織内だけでなく顧客や無関係の組織まで機密情報の窃取やマルウェア感染などの被害が発生する恐れがあります。例えば、2017年5月中旬に世界的な被害をもたらした身代金型ランサムウェア「WannaCry」はOSの脆弱性を突く攻撃ツール「EternalBlue」によって拡散しました。

サイバー脅威をもたらす攻撃者は、ソーシャルメディアや闇マーケットなどから攻撃ツール及び未公開脆弱性の情報を得て、組織的にサイバー攻撃を実行します。また、サイバー攻撃を請け負うサービスが台頭しており、DDoSを代行するBooterやStresser、及び、被害者のファイルを人質に取る身代金型ランサムウェアを広く散布して、被害者から金銭が支払われた場合に依頼者へ収益の一部を分配するRaaS（Ransomware as a Service）がその代表例です。このようなサービスは、一連の攻撃行動が自動化されていることや攻撃にかかるコストの少ないことが特徴です。

一方、防護側では以下の理由から100%人手によるサイバー脅威の分析はもはや限界となっています。

- インダストリー4.0の到来により守るべき対象の機器がITだけでなくOTへも拡大したこと[1)]。
- サイバー犯罪の検挙件数や相談件数が年々増加していること[2)]。
- 脅威情報の拡散するソーシャルメディアの情報流通量は2005年から2014年までの9年間でおよそ9倍に拡大したこと[3)]。
- セキュリティ技術者の不足が叫ばれていますが、システムの構築に関する幅広い知識を必要とすることから一朝一夕に人材を育成できないこと[4)]。

このような背景から効率的なサイバー脅威の分析手段が、社会において求められています。

本稿では、第2章においてNECの提案するOSINT（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情報分析手法について説明し、第3章において評価実

験について述べ、最後に本稿全体をまとめます。

2. OSINT（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情報分析

NECでは、サイバー脅威の分析を**図1**にある5つのフェーズで自動化を図ります。本章ではそれぞれのフェーズにおける要素技術について述べます。

2.1 Data Collection

リサーチを目的として、インターネット上に存在する300万以上のソーシャルメディア、ブログ、アンダーグラウンドサイトなどから脅威情報を常時収集・蓄積しています。世界各地のデータセンターを転々とする悪質サイトを攻撃者コミュニティの検知によって追跡し、自律的に収集対象を拡大しています。また、通常の検索エンジンでは探索できないディープウェブ[5]上に存在するサイトも収集します。

2.2 Prediction

2015年9月中旬、一定の条件下にあるルータを介して感染拡大するマルウェアを確認しました。同年9月中旬から下旬にかけて、このルータを狙ったサイバー攻撃が頻繁に発生しました[6]。

IPアドレスあたりの攻撃発生件数及びソーシャルメディアTwitterに投稿された当該攻撃に関する発言数の推移を1日ごとに表したグラフが**図2**です。攻撃の行われた全期間にわたって重回帰分析を行った結果，両者に相関があるとは言えませんでした。しかし、9月15日正午付近の攻撃発生件数と投稿数の最初のピークのみに着目すると高い相関があり、連動性が見られました。投稿数が急騰する兆候をできるだけ早くとらえることで、攻撃発生の兆候もまたとらえられます。

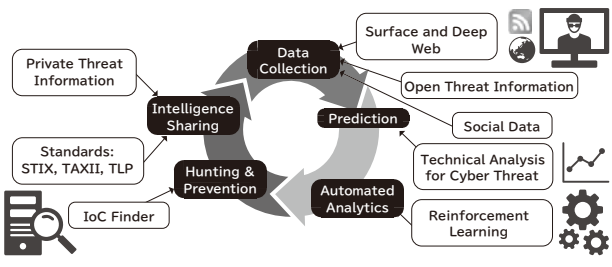


図1　自動化されたサイバー脅威分析の流れ

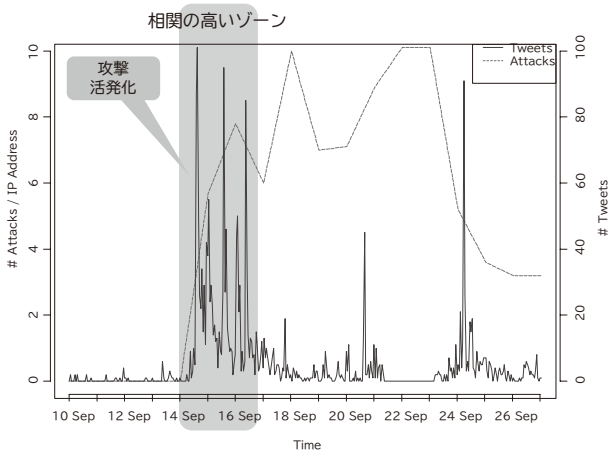


図2　ルータを狙った攻撃の回数とソーシャルメディアでの言及数

金融業界において投資業務に携わるトレーダーは数多くの銘柄からこれから急騰する銘柄を誰よりも早く予測し、安値で買い、高値で売る業務によって利益を得ています。

一方、セキュリティアナリストは脅威情報の動きから今後流行する脆弱性攻撃やマルウェアの到来をいち早く予測し、サイバー攻撃への備えを事前に行うことで被害に遭う可能性のある期間を最小限に抑えたいと考えています。

トレーダーとセキュリティアナリストは、対象が異なるだけで未来のトレンドを予測したいという点では同じ目的を持っていることが分かります。

金融業界では銘柄の値動きを予測する手段の1つとして、過去から現在までの値動きの推移から将来の値動きを予測するテクニカル分析が用いられています。目的と同じくするサイバー脅威の予測においても、このテクニカル分析手法を適用可能と考えました。

テクニカル分析は、トレンド系とオシレーター系の2種類に大別されます。トレンド系の指標は中長期的な傾向をとらえる目的に適しているEMA（Exponential Moving Average）などが、一方、オシレーター系の指標は短期的な傾向をとらえる目的に適しているHistorical VolatilityやRSI（Relative Strength index）が知られています。また、これら双方の特性を持つ中間的な指標として短期・長期の移動平均線から相場の周期と売買のタイミングをとらえるMACD（Moving Average Convergence Divergence）があります。サイバー脅威のトレンド分析においては、特にMACD法

が有効であることを明らかにしました。

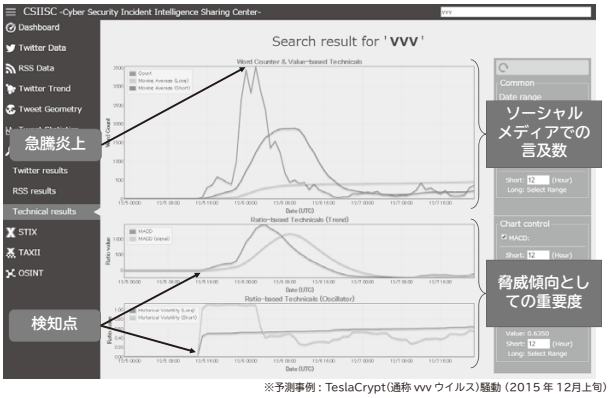
図3に示すように脅威情報に含まれる特徴的な語を、MACD法をベースとする独自アルゴリズムによって分析し、重大な事案につながる度合いを算出します。**図4**に示す重要度ランキングとして出力し、脅威の予兆をとらえた結果としてセキュリティアナリストへ気付きの機会を与えるとともに次工程の全体像分析の材料とします。

2.3 Automated Analytics

熟練したセキュリティアナリストによるサイバー脅威の全体像分析のノウハウを既存の分析結果や端末の操作履歴から学習し、新たな端緒が発見されたとき、その知見を活用して脅威の全貌を暴き出す技術をディープラーニングの活用によって開発しました（**図5**）。

脅威とは、ただちに被害を及ぼすものではないため、将来的に自組織の被害につながるか否かの判断は組織のシステム構成やワークフロー、分析者の見解、情報元の信頼性によって異なります。また、脅威情報は膨大であるため、単純な情報の紐づけでは数万もの悪性IPアドレスなどの要素が列挙され、そのままセキュリティ対策へ利用すると過剰な防護によって通常業務に影響をもたらす可能性があります。

過去の分析事例からサイバー被害をどのような手順で分析したかを学習し、新たな脅威を検出した際にその学習結



※予測事例：TeslaCrypt（通称 vvv ウイルス）騒動（2015 年 12月上旬）

図3　MACD法ベースの独自アルゴリズムによる脅威情報のトレンド分析例

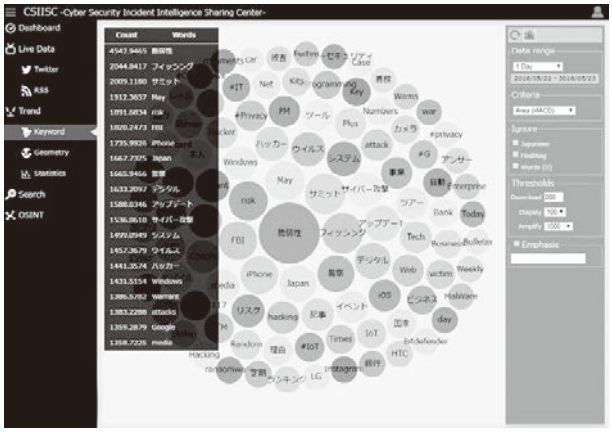


図4　脅威予測結果のランキング表示

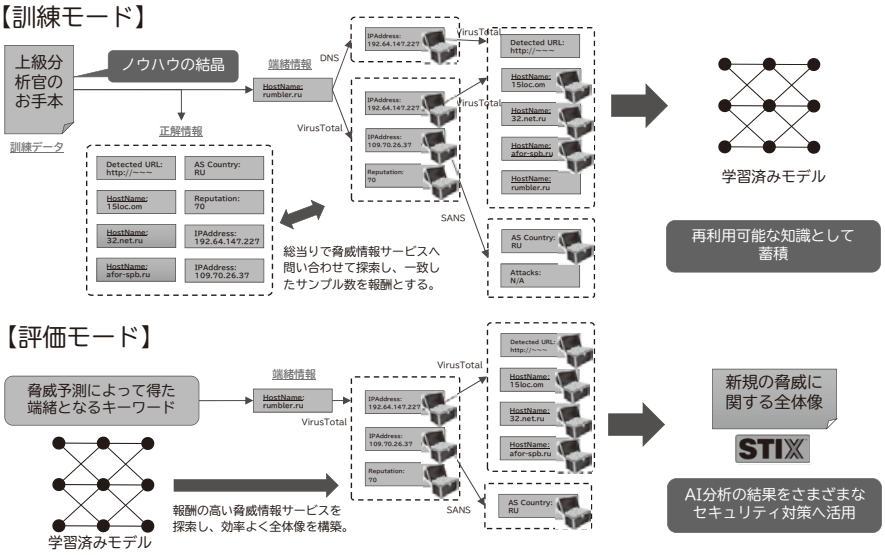


図5　ディープラーニングの活用によるサイバー脅威の全体像分析

果に基づいて機械的に分析することで、組織固有の基準かつ適切な分量での脅威の全体像分析を可能にします。

2.4 Hunting & Prevention

電子メールなどを介して、特定の組織を狙う標的型攻撃へ対抗する方法論として「脅威ハンティング」の重要性が高まっています。

例えば、エンドポイントにおいては、アンチウイルスソフトの提供するパターンファイルによってマルウェアの存在を検出しますが、パターンファイルの配付やそれによる検出動作が完了するまでの期間にマルウェアによる被害が発生する場合があります。特に標的型攻撃においては、標的組織の用いるアンチウイルスソフトによる検知を回避するなどの悪質な細工を施したマルウェアを用いる場合があり、被害に遭いやすい状況です。

脅威ハンティングでは脅威情報から分析した予兆を仮説としたシステム全体の検査を行い、被害の有無やリスクの度合いを検証します。自動化によって、例えば、サイバー攻撃グループが犯行声明を出した直後（パターンファイル配付前）に、被害に遭っていないか、将来の攻撃可能性はあるのかといったプロアクティブなセキュリティ対策が可能となります。

2.5 Intelligence Sharing

脅威分析の結果を標準化団体OASISで策定されたオープンな脅威情報構造化記述形式STIX[*1]によって蓄積します。ここからファイアウォールやIDSなどの設定変更に必要な情報を生成し、サイバー攻撃の発信源を遮断するなどのセキュリティ対策を実施します。

また、同団体による検知指標情報自動交換手順TAXII[*2]を用いて他部門・他組織・他国と脅威分析結果の共有を可能にします。他からの知見を自組織のセキュリティ対策へ役立てるなど、協力関係の構築を行います。

NECでは、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」に加入し、サイバーセキュリティ事業において技術・人材に加えてインテリジェンスも強化しました[7)]。

表　サイバー脅威の速報率

年月	早期検出	脅威の総数	速報率
2015年7月	66	128	51.6%
2015年8月	47	78	60.3%
2015年9月	34	60	56.7%
2015年10月	30	59	50.8%
2015年11月	30	62	48.4%
2015年12月	40	58	69.0%
平均			**56.1%**

3. 評価実験

2015年7月から12月までにソーシャルメディアへ投稿された発言からサイバー脅威への言及数を、1時間おきに計測しました。言及数の推移から、MACD法ベースの独自アルゴリズムによって急騰を検出した日時を求めました。また、公的機関、マスメディア、ベンダーによるサイバー脅威に関する最速の記事公開日時を調査しました。その結果、独自アルゴリズムが平均56.1%早くサイバー脅威を検出できました（**表**）。

4. むすび

拡大するサイバー攻撃とその背景にあるソーシャルメディアやディープウェブを通じた脅威情報の流通について述べ、ソーシャルメディア上のサイバーインシデントに関する投稿数の最初のピークが関連する攻撃の発生数のそれと連動している点に着目し、金融工学におけるテクニカル分析手法によって被害をもたらす可能性の高い脅威情報を抽出する手法を提案しました。また、公的機関などによる発表よりも平均56.1%早く検出したことを評価実験によって示しました。

本手法を導入することにより、膨大な脅威情報から攻撃の予兆をとらえ、迅速かつ的確な対処を行うことで、被害に遭う可能性のある期間を短縮することが可能となります。

今後も、サイバー攻撃による被害を受ける前に予防的措置を実施する脅威ハンティングを推進し、安全・安心で効率的

[*1] Structured Threat Information eXpression。サイバー攻撃を特徴付ける事象などを取り込んだサイバー攻撃活動に関連する項目を記述するための技術仕様　http://stix.mitre.org/
[*2] Trusted Automated eXchange of Indicator Information。サイバー攻撃活動に関連する脅威情報を交換するための技術仕様　http://taxii.mitre.org/

な社会インフラの実現へ向けた研究活動を継続します。

*Twitterは、Twitter,Incの登録商標または商標です。
*その他記述された社名、製品名などは、該当する各社の商標または登録商標です。

参考文献

1) ドイツ連邦教育科学研究技術省：The new High-Tech Strategy
https://www.bmbf.de/pub/HTS_Broschuere_eng.pdf
2) 警視庁：平成25年度中のサイバー犯罪の検挙状況等について
http://www.npa.go.jp/cyber/statics/h25/pdf01-2.pdf
3) 総務省：情報通信白書平成27年版，2015.7
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h27/index.html
4) 独立行政法人情報処理推進機構：「情報セキュリティ人材の育成に関する基礎調査」報告書について
https://www.ipa.go.jp/security/fy23/reports/jinzai/
5) Bergman, Michael K ：The Deep Web: Surfacing Hidden Value, The Journal of Electronic Publishing. 7 (1). doi:10.3998/3336451.0007.104., 2001.8
6) 警察庁：インターネット観測結果等(平成27年9月期)
https://www.npa.go.jp/cyberpolice/detect/pdf/20151028_1_2.pdf
7) 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，2017.3.15
http://jpn.nec.com/press/201703/20170315_01.html

執筆者プロフィール

川北 将
セキュリティ研究所
主任

島 成佳
セキュリティ研究所
主任研究員

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

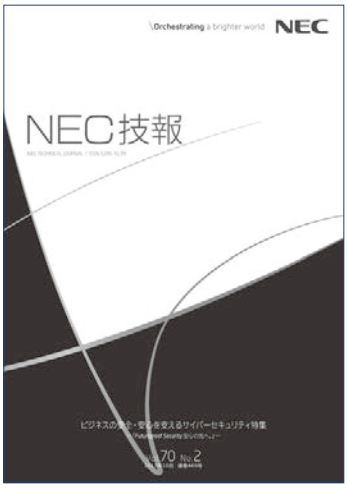
◇ 特集論文

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