HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.45

株式会社 日立システムズ

Human * IT

Hitachi Systems security Jounral VOL.45

TABLE OF CONTENTS

●はじめに

本文書は、株式会社日立システムズ の公開資料です。バックナンバーは以下の Web サイトで確認できます。
https://www.hitachi-systems.com/report/specialist/index.html

ハイブリッド戦争の観点から考える
ディスインフォメーションの驚異とその対策

小原 凡司 インタビュー

取材・文＝斉藤健一

インターネットがインフラとして社会に浸透するのに伴い、サイバー・セキュリティが扱う領域は、従来の IT システムや情報資産の安全確保から、企業の経営戦略や国家の安全保障までをも包含することとなった。

サイバー攻撃というと、インターネットを通じた情報窃取やシステム破壊などをイメージすることが多い。しかし、インターネット上で情報操作を行ない、国家の意思決定プロセスなどに影響を与えることも新たなサイバー脅威として認識されるようになってきた。

情報操作は、ディスインフォメーション（虚偽の情報）の流布によって行なわれる。今回は笹川平和財団の小原凡司氏に、情報戦の観点からディスインフォメーションについて話を伺った。

なお、インタビューは本年 2 月初旬に行なわれた。そのため、2 月下旬に始まったロシアによるウクライナへの軍事侵攻について、具体的な言及はしていない。

ハイブリッド戦争とディスインフォメーション

インタビューの冒頭では、安全保障の専門家である小原氏がディスインフォメーションの研究を始めた経緯について、その前提となる部分から順を追って説明していただいた。

まずは、現代の軍事戦略である「ハイブリッド戦争」について。これは、2013 年ロシアのゲラシモフ参謀総長が論文の中で提唱した概念で、この論文はゲラシモフ・ドクトリンとも呼ばれている。21 世紀の戦争では、軍事衝突に至る前の、有事とも平時ともつかない「グレーゾーン」での展開が重要となるとともに、戦争の手段も軍事的なものに限らず、非軍事的なものが多用されるとしたものだ。

グレーゾーンでは、サイバー攻撃をはじめ、「ディスインフォメーション・キャンペーン」も盛んに行なわれるという。

ここでいうディスインフォメーションとは、社

●小原凡司（おはら・ぼんじ）

1985 年 防衛大学校卒業、1998 年 筑波大学大学院（地域研究修士）修了（修士）。1985 年に海上自衛隊入隊後、回転翼操縦士として勤務。2003 年～ 2006 年 駐中国防衛駐在官。2006 年防衛省海上幕僚監部情報班長、2009 年第 21 航空隊司令、2011 年 IHS Jane's アナリスト兼ビジネス・デベロップメント・マネージャーを経て、2013 年に東京財団、2017 年 6 月より笹川平和財団上席研究員。単著・共著による著作も多数あり。最新刊は森本敏 元防衛大臣らと共同で執筆・編集にあたった「台湾有事のシナリオ」（ミネルヴァ書房刊）。

会や公益への攻撃を目的とした害意ある情報を指す。ディスインフォメーション・キャンペーン自体は以前から使われてきた手法だが、近年では特に SNS などの発展により、より高度で、かつ効果的なキャンペーンが展開されるようになってきたという。

こうしたディスインフォメーション・キャンペーンを用いたサイバー攻撃に積極的なのが、ロシアと中国だ。2016 年の米国大統領選でのロシアの介入工作や、2016 年・2020 年の台湾総統選での中国の介入工作などが具体例として挙げられる。特に中国では、人の認知領域を新たな戦場空間として捉え、AI や量子コンピューティング技術などを取り入れた「智能化」への発展を加速させている。

ディスインフォメーション・キャンペーンによる選挙介入や世論操作は、国家の意思決定への攻撃であり、安全保障上の観点から看過できない問題だ。そこで、小原氏は防御の観点からディスインフォメーションの対抗策の研究をはじめたのだという。

ディスインフォメーションの特徴と事例

小原氏にディスインフォメーション・キャンペーンの特徴について伺った。キャンペーンの目的は、社会を混乱させ、対立させ、衝突させることにある。したがって、効果を高めるには虚偽の情報を流すだけではなく、社会の不安をあおるような状況を作り出すことも重要だという。例えば、物資の不足を招く海上・航空の封鎖や、電気・水道といったライフラインの供給停止などが挙げられる。また、キャンペーンは、外国政府やその協力者からのプロパガンダという形をとることが多い。しかし、内部からの不満や怒りの声といった形の時の方が、人々の混乱の度合いが増し、暴動へと発展しやすくなると言われている。

2014 年のクリミア危機での事例を紹介する。きっかけはディスインフォメーションだったという。ウクライナで起きた民主化運動（マイダン革命）により親ロシア派のヤヌコーヴィチ大統領が失脚、ロシアへ亡命することとなった。広場では市民が活気づいていたが、その中に親ロシア派、もしくはロシアから送り込まれた人間が「民主義的なデモから武装蜂起になった」とその場から英語で発信した。これを欧米のメディアが「クリミア半島で暴動が起こり始めた」と報じることとなる。そして、ロシアはこれを介入の口実にしたのだという。

そのような暴動は実際には起きておらず、結果として欧米は偽情報に踊らされることとなった。これには、ウクライナに対する欧米の関心の低さという当時の認識も関係していたと小原氏は分析する。ただし、現在のウクライナ情勢では NATO などがサイバー・セキュリティやディスインフォメーション対策の分野で支援を表明しており、2014 年の時と比べて状況は改善されているという。

次に台湾の事例だ。厳密にいえば、中国が主体であるという明確な根拠はないとされている。いくつか例を挙げると、総統選挙戦で報じられた蔡英文氏の学歴詐称疑惑や民進党政権のコロナ禍対策への批判、コロナワクチンの安全性を疑問視するもの、マスクと同じ原材料で生産される紙製品の不足といったものなどがある。

また、キャンペーンでは、必ずしも親中派に有利な情報だけを流すというわけではない。台湾政府への不満をあおるような情報を流す一方で、反中派を怒らせるような情報も流したり、反中派のデモの中に人を送り込み、デモを暴徒化させ、新中派・反中派、どちらにも与しない市民が反中派に嫌悪感を抱くように仕向けたりするのだという。

ただし、台湾の場合は、ディスインフォメーションを監視する機関やファクトチェックを行なう組織を設立し、ディスインフォメーションをいちはやく検知し、正しい情報をすぐに発信する対策を講じているという。また、メディアリテラシー教育にも力をいれており、ディスインフォメーションが社会の中で大きな影響を与えることはないとされている（ディスインフォメーション対策の詳細は後述）。

日本における
ディスインフォメーション対策

続いて、日本におけるディスインフォメーション対策について尋ねた。小原氏は、欧米やアジア

各国と比較して、わが国の対策は進んでいないと現状を語る。その背景には、日本語の特殊性が外国からの攻撃を阻んできたことも関係しているという。日本語は文法が難しく、文章のささいな間違いであっても違和感を覚え、日本人によるものではないと気づくことができる。

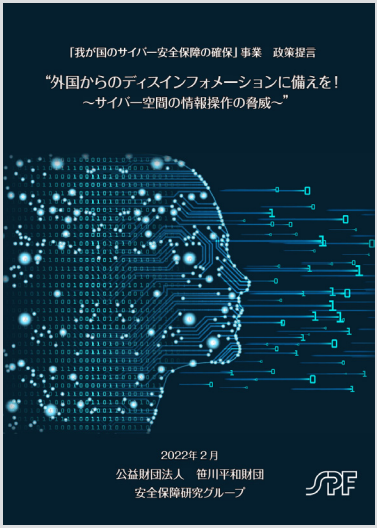
この言語の特性により、これまで、ディスインフォメーションの実質的な被害は抑えられてきたという。しかし、AI 技術の発展などにより、日本語の文書生成・機械翻訳のレベルは格段に上がっており、日本人が書くものと遜色がなくなりつつある。そのため、具体的なディスインフォメーション対策が、いま求められている。

笹川平和財団による政策提言

そのような中、笹川平和財団による「外国からのディスインフォメーションに備えを！〜サイバー空間の情報操作の脅威〜」という政策提言が発表された※。2019 年に発足した国内有識者による研究会がとりまとめたものだという。

この提言では、ディスインフォメーションを新たなサイバー脅威として捉え、各国での事案を調査・分析するとともに、その対策についても、共通の指標を定めて国ごとの比較を行なっている。比較の対象は、米国・英国・EU・シンガポール・台湾・日本などだ。また、提言の中で示されている対策の指標は以下のとおり。

- **ディスインフォメーションによる干渉を検知、モニタリングする機関や制度はあるか？**
- **選挙などの民主主義プロセスについて干渉があったか否か調査し処罰する法律があるか？**
- **選挙インフラが重要インフラに指定されているか？**
- **選挙干渉行為に対し国家としてサイバー攻撃による反撃、防御を行なうことができるか？**
- **選挙干渉などに関連しプラットフォーマーを規制する法律があるか？**
- **ディスインフォメーション対策としてメディアリテラシー教育を行なっているか？**
- **行政府による／行政府から独立したファクトチェック機関があるか？**



笹川平和財団による政策提言「外国からのディスインフォメーションに備えを！〜サイバー空間の情報操作の脅威〜」

これらの指標に照らし合わせると、日本がクリアしているのは「行政府から独立したファクトチェック機関がある」という項目だけであり、比較対象国の中で最も対策が遅れていることが分かる。これらの事実を踏まえ、下記の提言は対策指針のクリアを促すものとなっている。なお、本稿では紙幅の都合から、各項目の詳述は割愛させていただく。興味のある方は発表された提言の内容を参照いただきたい。

- **ディスインフォメーション対策を行なう情報収集センターの設置**
- **選挙インフラを重要インフラに指定**
- **情報操作型サイバー攻撃に対する積極的サイバー防御（Active Cyber Defense：ACD）実施体制の整備**
- **政府とプラットフォーマーによる協同規制の取**

※「外国からのディスインフォメーションに備えを！ 〜サイバー空間の情報操作の脅威〜」
政策提言本文 ：https://www.spf.org/global-data/user172/cyber_security_2021_web1.pdf
要旨　　：https://www.spf.org/global-data/user172/cyber_security_2021_abstract_web.pdf

り組みと行動規制の策定の推進
・メディアリテラシー教育環境の拡充

ディスインフォメーション検知に資するシステムの研究と今後の活動について

当社では小原氏に監修いただき、ディスインフォメーション検知システムの開発を進めている。残念ながら詳細をお伝えすることはできないが、小原氏の言葉をお借りして、その意義について簡単に触れておきたい。

小原氏によれば、SNS などで展開されるディスインフォメーション・キャンペーンではネットワークにハブとなる存在がいて、そこを起点に情報が拡散される特徴があるという。そうした特徴からキャンペーンを見つけ出すのがシステムの基本的な設計思想だ。ただし、システムはあくまでも検知を支援するものであり、情報の真偽は人間が判断することとなる。

こうしたシステムにより早期にディスインフォメーション・キャンペーンが発見できれば、ファクトチェック機関による調査や政府機関による正しい情報の発信などに役立つはずだと小原氏は語る。

最後に、今後の活動について伺った。小原氏はグレーゾーンの脅威への対処を研究テーマに据えており、現在は、米国・東欧・台湾のシンクタンクなどと、ディスインフォメーション対策の分野で共同研究を進めている。安全保障の研究なので、いかに戦争を回避するかという視座が重要なのだという。

また、ハイブリッド戦争という観点から見ると、サイバー・セキュリティの各分野の連携や統合の必要性も感じているそうだ。例えば、ディスインフォメーションに対処する部署を作ったとしても、それがサイバー・セキュリティの部署と分離されていたのでは意味がない。同様に、サイバー・セキュリティの部門が、衛星ネットワークや重要インフラを管理する部門と分離されていたとしたら、それも意味がなくなってしまう。こうした連携や統合のための仕組み作りについて大きな関心を持っているという。

昨今、国際ニュースを見聞きする中で、ディスインフォメーションに関連する話題が増えているように感じる。例えば、新疆ウイグル地区での人権侵害を否定する中国政府の主張や、ウクライナ国内で親ロシア派住民の安全が脅かされているというロシア政府の主張などだ。前者は、国際社会の批判をかわす中国政府の意図が見られるし、後者は、ウクライナ侵攻を正当化するための大義名分として使われている。

ディスインフォメーション対策の制定が求められている日本にあって、小原氏の研究は大変に有用だと感じた。引き続き、今後の動向に注目していきたい。

中国による情報操作戦の戦略・技術・手順を明らかにする

チェ・チャン（Che Chang）シルビア・イエ（Silvia Yeh）

Team T5 脅威インテリジェンスチーム インタビュー

取材・文＝斉藤健一　協力＝エル・ケンタロウ

今回は台湾のセキュリティ企業、TeamT5 のチェ・チャン（Che Chang）氏とシルビア・イエ（Silvia Yeh）氏に話を伺った。サイバー脅威インテリジェンスのアナリストとして活躍する両氏は、活動の一環として国家主導による情報操作（InfoOps）を調査しており、その結果を CODE BLUE や SANS Cyber Threat Intelligence Summit といった国際会議の場で発表している。調査は長期間継続され、その結果もアップデートされていることから、発表では回を重ねるごとに新たな洞察が加えられている。

本稿では、2021 年 10 月に CODE BLUE で発表された「クリップ中毒：動画を使った中国の情報操作戦と脅威インテリジェンスに関する研究」について、彼らのインタビュー（2022 年 1 月下順に実施）を交えながら、プレゼンテーションの内容を紹介する。

ソーシャルメディアの武器化が情報戦の新たな潮流に

2016 年の米国大統領選では、ロシアを背景に持つ主体（Actor）がソーシャルメディアを武器化して情報戦を展開し、大きな話題となった。

以前から APT に関する調査を行なってきた TeamT5 の脅威インテリジェンスチームも、こうした情報戦の変化による影響をつぶさに感じ取ってきた。2018 年頃から中国を背景に持つ主体が、ソーシャルメディアを通じて自国が意図する情報を拡散し、他国の人々に対して影響を及ぼそうとする情報戦を展開するようになってきたというのだ。加えて、近年では動画コンテンツを活用したより大規模なものへと進化しているとも語る。

「公然の主体」の発信を「隠密の主体」が拡散する

講演では、動画コンテンツ全盛時代における中国の情報戦を自国民向け・海外（主に英語圏）向けに分けて言及しているが、本稿では主に海外向けの情報戦に絞って紹介したい。

情報戦を展開する主体は、公然の主体（Overt Actor）と隠密の主体（Covert Actor）に分けられるという。前者は中国政府とのつながりが明白な存在で、国営メディアや各国の中国大使館などを指す。一方、後者は中国政府とのつながりが直接的には見えない存在だ。政府に雇われたマーケティング企業やオピニオンリーダー、さらには外国人ユーチューバーなどが含まれるという。

情報戦の流れは以下のとおりだ。まず、国営メディアがニュースやプロパガンダを発信する。この時点では有害な「偽情報」とは言いがたく、あくまでも誤解を招くような「誤情報」の範ちゅうなのだという。TeamT5 の両氏はこうした情報を「ミスインフォメーション（Misinformation）」と呼んでいる。

国営メディアから発信された情報は、オピニオンリーダーや海外ユーチューバー、さらには AI やボットによって自動生成されたコンテンツを通じ、歪められた偽情報として拡散されることとなる。彼らはこうした情報を「ディスインフォメーション（Disinformation）」と呼んでいる。

新疆ウイグル地区と香港の 2 つの事例

講演では「#StopXinjangRumours（新疆ウイグ

ル地区の噂を止める）」と「#PatriotGoverningHong Kong（愛国者統治の香港）」という 2 つのディスインフォメーション・キャンペーンの事例が紹介された。

まずは、新疆ウイグル地区の事例から。情報戦は YouTube、Facebook、Twitter、TickTok といったプラットフォームを横断する形で展開される。少なくとも 20 の YouTube チャンネルで 180 本以上の動画が上記のハッシュタグ付きで投稿されていた。動画は新疆ウイグル地区での日常を紹介し、人権侵害は西側諸国によるねつ造だと非難するものが多い。中には数万ものチャンネル登録者数を持つ外国籍のユーチューバーによる動画もある。

そして、これらの動画を紹介する投稿がボットによって大量に生成され、ソーシャルメディア上にばらまかれる。投稿の多くは英語だが、中には日本語で発信するボットアカウントも存在する。また、新疆ウイグル地区に関するハッシュタグに加えて「＃母の日」といった一般的なタグを付けて、より一層の拡散を狙うこともあるという。

続いて香港の事例を紹介する。こちらも先の事例と同様、複数のプラットフォームを横断する形で展開される。経緯は以下のとおり。人民日報、新華社など国営メディアや親中派メディアが相次ぎソーシャルメディアで公式アカウントを開設。「愛国者治港（PatriotGoverningHongKong）」を掲げ、民主派の排除を目的に選挙候補者を親中派に限る改革を支持するキャンペーンを展開した。すると、これに同調するオピニオンリーダーがハッシュタグ付きで発言、呼応するかのように大量のボットアカウントも現れた。その数は YouTube チャンネルで 5000 以上、Facebook、Twitter それぞれのアカウントでも 5000 以上に及ぶという。ボットアカウントは、国営メディアの社説を切り取り、自動読み上げ（Text To Speech）で音声化した動画を次々と投稿した。

TeamT5 の両氏によれば「専制主義国家の中国は、民主主義国家でソーシャルメディアがどのように使われているのか、非常によく研究している」と語る。「例えば、ここ数年の例を見ても、人の興味を惹く動画の作り方や、ハッシュタグの使い方など、情報戦をより効率的に、より効力を発揮するものに進化させようとする努力を怠らない」と中国の情報戦の進化を強調した。

情報戦調査の現状

プレゼンテーションから、ソーシャルメディアを用いた中国の情報戦はボットによる自動化が進んでいることが分かった。ならば、調査の自動化

●チェ・チャン（Che Chang）

TeamT5 サイバー脅威インテリジェンスチームのアナリストであり、TeamT5 のインフォメーション・オペレーション・ホワイトペーパーの共同執筆者。研究テーマは、アンダーグラウンドの市場調査や国家主導の情報操作（InfoOps）が中心。SANS Cyber Threat Intelligence Summit 2021、CODE BLUE 2020、2020 年 4 月 vGCTF disinfo workshop、2019 Cybersec in Taiwan などのスピーカーも務める。

●シルビア・イェ（Silvia Yeh）

TeamT5 サイバー脅威インテリジェンスチームのアナリスト。研究テーマは APT、OSINT、中国のサイバー政策、情報操作など。SANS Cyber Threat Intelligence Summit 2021、CODE BLUE 2020 などの国際会議で発表を行なっている。

は進んでいるのだろうか。この点について尋ねてみると、意外にも「調査は手動だ」との答えが返ってきた。「Twitter、Facebook、Weibo など複数のソーシャルメディアを横断的にクローリングして、アカウント間の関連性を可視化するような統合ツールを作るのは困難だから」というのがその理由だ。TeamT5 では、現在 3 ～ 4 名の人員で調査を継続している。国営メディアの動向を注視したり、疑わしいハッシュタグやボットがないか、常にネットワークを監視したりしているのだという。また、自動化の取り組みを進めるには、プラットフォーム企業の協力が不可欠だとも語る。TeamT5 は香港の事例の調査において、香港在住の親中派議員自身のものとされるソーシャルメディア・アカウントが、実はバングラデシュなどの海外から投稿されていたことを突き止めている。この事実はソーシャルメディアの透明性レポート（Transparency Report）から、ロケーション情報などのメタ情報が得られたからこそたどり着けたのだという。

ソーシャルメディアの透明性を保つために

プレゼンテーションの事例で紹介したハッシュタグ・アカウント・投稿などはすでに削除されており、現在では見ることはできない。Twitter や Facebook などのプラットフォーム企業が、ソーシャルメディアの透明性を保つために、ファクトチェックや有害コンテンツの削除といった作業を独自で行なっているためだ。もちろん、これは評価に値するが、情報戦の終結を意味するものではない。あくまで表層的な部分の変化と捉えるべきだろう。

プラットフォーム企業のこうした取り組みについて、TeamT5 の両氏に意見を求めたところ、彼らはファクトチェックの難しさを挙げた。「ボットによって大量に生成される有害コンテンツに対して、現状ではプラットフォーム企業のコンテンツ管理チームが対応しきれていない」と指摘する。「特に動画コンテンツに含まれるディスインフォメーションを機械的に識別するソリューションが確立されていないことに加え、英語・中国語・日本語など各国の言語に精通した人材を用意する必要がある」ことも要因だと語る。また、現状を踏まえると、「プラットフォーム企業と第三者である研究者や組織とのコラボレーションがファクトチェックの課題解決につながる」と力説する。

台湾にはいくつかのファクトチェック組織があり、2020 年の台湾総統選挙の時期には、報道機関などとも連携して活動していたそうだ。TeamT5 も短期間ではあるものの選挙期間中に他組織と共同で活動したという。具体的には、疑わしいアカウントが情報戦に関わっていないか、背景に何があるかなど、OSINT（公然情報によるインテリジェンス）から調査・分析を行なったそうだ。

情報戦による脅威と今後の抱負

新疆ウイグル地区で人権侵害が行なわれていることも、香港で民主派が弾圧されていることも、西側諸国の一員である日本では、当然のこととして報道されている。それゆえ、中国による情報戦が現地や海外でどれほどの影響をもたらしているのか、想像の及ばない部分が大きい。TeamT5 の両氏に情報戦の影響について尋ねた。彼らは、情報戦の成果や影響を定量化して語ることはできないとしながらも、その影響は大きく 2 つあると語った。

1 つは「ボットにより自動生成されたコンテンツが溢れてしまい、他の主張を掲げるコンテンツが埋もれてしまう」という点だ。これによって視聴者側に嫌気がさして動画コンテンツ離れが起こったり、先述のようにソーシャルメディアのコンテンツ管理チームが忙殺されたりすることが考えられ、ひいてはニュースの信頼性低下にもつながる懸念があるという。

もう 1 つは、「オピニオンリーダーやボットによる過激なコメントに触発されて、一部の人の言動が攻撃的になる」という点だ。人はソーシャルメディアから潜在的に多くの影響を受けており、エンゲージメントだけを見ていればよいというものではない。それが情報戦の脅威でもあると TeamT5 では考えている。

また、今後の調査対象を尋ねてみると、「COVID-19（新型コロナウイルス）の起源について調べるつもりだ」と語ってくれた。COVID-19 に関して言えば、武漢起源説を否定し米国を批判するスイス人研究者のことを中国のメディアが盛

んに喧伝していた時期がある。その報道は各国の中国大使館によって翻訳され世界中に拡散した。ところが昨年末に、この人物は実在せず、顔写真も CG で作られたものだと判明した。上記の情報拡散の流れは、TeamT5 が講演で紹介した中国の情報戦の手法と一致している。今後の調査でどのようなことが判明するのか、世界がその結果に注目しているはずだ。

最後に余談だが、昨年秋、驚くべきことに TeamT5 自身がディスインフォメーションによる誹謗中傷の対象となる事案が発生した。経緯などは同社 Web サイトのニュースリリースに記載されているので、本稿では詳細は割愛する※。情報戦を仕掛けてきた主体は不明としながらも、TeamT5 がこれまで調査を進めてきた主体と手法などが似通っているという。このことは、TeamT5 の調査の正しさを示すものではないかと筆者は考えている。情報戦の主体は TeamT5 の存在を認識しており、目障りだと警告してきたと受け取れるだろう。攻撃は軽微なものであったので、TeamT5 氏の両氏も「先方からのあいさつが来た」という認識を持っているのだという。こうした事情を知ると、ますます彼らの動向から目が離せなくなると思うのだが。読者の皆さんはいかだだろうか。

※ **「当社に関する偽情報の流布及び誹謗中傷への対応について」**
https://teamt5.org/jp/posts/clarification-on-malicious-disinformation-targeting-teamt5/

台湾の国際セキュリティ・カンファンスにオンラインで参加

HITCON2021 レポート

文＝樋田拓也

2021 年 11 月 26 日・27 日の 2 日間、台湾・台北で HITCON2021 が開催された。COVID-19 の感染状況を考慮し、国立研究機関の中央研究院を会場とした対面開催（国内向け）と、オンライン配信（国内・海外向け）を組み合わせたハイブリッド形式で行なわれた。初日の開幕式には台湾の蔡英文総統も出席したという。これは対中関係が緊迫化している台湾におけるサイバーセキュリティへの関心の高まりを示すものだろう。

HITCON の Web サイトには「技術の側面から見れば正邪の区別はない。ハッカーという言葉は、プロフェッショナルのスキルと挑戦することへの勇気を指す」というスローガンが掲げられている。chr00t セキュリティグループによって始められたこのセキュリティ・カンファレンスには、セキュリティやハッキングに興味を持つ人たちが一堂に会し、技術情報のみならず、ハッカー精神をも共有することで、交流を深めてきた。

本稿では、HITCON2021（2 日目）にオンラインで参加した筆者が、聴講して興味を持った講演を簡単に紹介する（2022 年 2 月上旬執筆）。

未承認の Exchange - 標的型エスピオナージから世界的なサイバー・パンデミックへ -

An Unauthorized Exchange - From Targeted Espionage to a Global Cyber Pandemic

VOLEXITY 社／スティーブン・アデール（Steven Adair）氏

VOLEXITY 社は、デジタル・フォレンジックとインシデントレスポンスに特化した企業で、フォレンジックソフトウェアの販売も行なっている。

本セッションでは、2021 年 3 月にパッチが公開された「Microsoft Exchange Server」のぜい弱性に関して、国家が関与したとされる攻撃を調査した際に得られた情報や知見が発表された。VOLEXITY 社では、パッチ公開以前の 2021 年 1 月には、このぜい弱性を突いた IoC（Indicators of Compromise：侵害の痕跡）を確認していたそうで、メモリフォレンジック、ファイルアーティファクト（pagefile、$MFT、event logs、registry、hive 他）などから調査を実施していたとのこと。

その後、2 例目となるインシデントが確認された際は、1 例目の調査で取得した IoC を用いて感染の痕跡を確認し、調査を進めることができたため、迅速に対応できたのだそうだ。

このぜい弱性を悪用した攻撃では、Web シェルを設置するものだけではなく、ビットコインのマイニングやランサムウェアを使用する攻撃もあったという。

ゼロデイ攻撃では、その痕跡が確認された時点においては、ベンダーからの情報も少なく、対応策も分からない。攻撃者の情報や IoC などの情報収集にも苦労することが多い。ただ、講演での事例のように、初期の調査段階で得られた IoC 情報をいち早く活用することができれば、その後の調査や攻撃の検知にも役立てることができる。日々の情報収集の大切さを改めて感じさせられる内容だった。

なお、VOLEXITY 社のブログにて発表内容の一部が公開されているので、興味のある方はそちらもご覧いただきたい。

- **ブログ記事：Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities**
  https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

デジタル ID カードのセキュリティ分析に関する経験の共有と提言
數位身分識別證的安全分析經驗分享與建議

国立台湾大学／シチョウ・シャ（Shi-Cho Cha）氏

スマートカードの規格や分析方法をはじめ、チップ付きパスポートと関連するセキュリティプロトコルなどが紹介され、その分析に必要な方法論やアイデアなども披露された。

講演では、オープンソースで実装された「JMRTD」が紹介されていた。「JMRTD」は、国際民間航空機関（ICAO）によって指定された機械可読旅行文書（MRTD）規格の オープンソースで、Java で実装されており、多くの国の電子パスポート（e パスポート）で採用されているそうだ。

なお、MRTD の規格は、ICAO Doc 9303 で定義されている。

また、台湾の国民身分証の eID カードに関しても、Common Criteria の基準や、公開データ領域、暗号化データ領域などに含まれる情報も紹介されるなど、さまざまな規格の情報が共有されることとなった。

- **JMRTD: An Open-Source Java Implementation of Machine Readable Travel Documents**
  https://jmrtd.org/
- **ICAO Doc 9303**
  https://www.icao.int/publications/pages/publication.aspx?docnum=9303
- **講演スライド**
  https://hitcon.org/2021/agenda/8aedb710-ac21-4f0d-96b9-0a4837c2af1b/%E6%95%B8%E4%BD%8D%E8%BA%AB%E5%88%86%E8%AD%98%E5%88%A5%E8%AD%89%E7%9A%84%E5%AE%89%E5%85%A8%E5%88%86%E6%9E%90%E7%B6%93%E9%A9%97%E5%88%86%E4%BA%AB%E8%88%87%E5%BB%BA%E8%AD%B0.pdf

Winnti がやってくる - 訴追後の進化
Winnti is Coming - Evolution after Prosecution

Team T5 ／アラゴーン・ツェン（Aragorn Tseng）氏、チャールズ・リー（Charles Li）氏
ピーター・シュウ（Peter Syu）氏、トム・ライ（Tom Lai）氏

APT41、別名 Winnti（TeamT5 による呼称）は、中国に背景を持つ攻撃主体であり、2020 年には米国 FBI によって起訴されている。講演では、起訴後も活動を続けている Winnti に関して、攻撃の対象や手法とった技術情報の詳細が発表された。

2021 年、Winnti は各国の通信企業・主要医療機関・政府・重要インフラを攻撃対象としていることが、Team T5 の調査によって判明している。攻撃に使われる技術や手法は進化しており、リサーチャーが追跡して検知することを困難にしているという。

講演では、Winnti が攻撃に使用するぜい弱性、対象ネットワークへの侵入手法、設置するバックドアなど一連の流れが解説された。また、ログによる侵入痕跡の調査もあわせて紹介されている。

他にも、マルウェアがメモリフォレンジックを回避するための手法や、CDN を用いて C2 インフラの IP アドレスを秘匿する方法など、攻撃キャンペーン全体にわたる詳細な情報が惜しみなく提供された。

発表資料には IoC も公開されており、Winti の TTPs（戦術・技術・手順）を知りたい人には非常に参考になる発表であった。

- **講演スライド**
  https://hitcon.org/2021/agenda/1abeaad2-5152-4468-91ac-d50a39dd7834/Winnti%20is%20Coming%20-%20Evolution%20after%20Prosecution.pdf

空挺の危機：クラウドをめぐる二転三転の攻防
空降危機：雲端攻防二三事

ボイク・スー（Boik Su）氏、ダンジ・リン（Dange Lin）氏

講演はクラウド全盛期における情報セキュリティの問題点をレッドチームの視点から探っていく。導入部分では、クラウドサービスの責任共有モデルや CSA（Cloud Security Alliance）を紹介するとともに、クラウドにおける脅威を、3 つのカテゴリー「1. ID 境界」「2. ネットワーク境界」「3. ホストされているアプリケーション（サービス）」に分け解説した。中盤では、この脅威に沿って代表的な 3 つのクラウドサービス、AWS、Azure、GCP（Google Cloud Platform）での事例を交えながら攻撃手法の分析が行なわれた。

また、後半では、認証情報の窃取（Credentials Harvest）、横方向展開（Lateral Movement）、権限昇格（Privilege Escalation）などの攻撃手法がグラフィカルに紹介されていた。

リモートワークが進む中で、クラウドサービスを利用する機会が多くなっているが、CSA などのベストプラクティスを参考に、脅威に対して適切に対応する必要性があることを改めて感じた。

・講演スライド
https://hitcon.org/2021/agenda/d90156b6-1714-4162-804a-3f9a951c213b/%E7%A9%BA%E9%99%8D%E5%8D%B1%E6%A9%9F%EF%BC%9A%E9%9B%B2%E7%AB%AF%E6%94%BB%E9%98%B2%E4%BA%8C%E4%B8%89%E4%BA%8B.pdf

全体のまとめ

HITCON の YouTube チャンネルでは講演の動画も公開されている。講演の詳細を知りたい方や、HITCON の雰囲気を知りたい方などは、是非ともご覧いただきたい。

筆者は、過去に、現地でのトレーニングを受講したことがあるが、その経験からすると、セキュリティカンファレンスは現地で参加してこそ、その楽しさがあると感じている。

ここ数年、オンラインでさまざまなカンファレンスが開催されているが、現地参加できないもどかしさがある。おそらく皆さんも同じ気持ちを抱いているのではないだろうか。

来年度、COVID-19 が沈静化し、国際的な往来が復活した時には、再び台湾を訪問し多くの方々と交流したいと願っている。

・HITCON の YouTube チャンネル
https://hitcon.org/2021/agenda/d90156b6-1714-4162-804a-3f9a951c213b/%E7%A9%BA%E9%99%8D%E5%8D%B1%E6%A9%9F%EF
https://www.youtube.com/channel/UCjW91GWKraCfWuKLGonq1vw

Human * IT

人と IT のチカラで、驚きと感動のサービスを。

Hitachi Systems Security Journal VOL.45

株式会社 日立システムズ
本社 〒141-8672 東京都品川区大崎 1-2-1