HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.30

株式会社 日立システムズ

Human * IT

Hitachi Systems security Journal VOL.30

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

産官学の連携でサイバー脅威に対抗

一般財団法人

日本サイバー犯罪対策センター（JC3）

島根 悟（理事）間仁田 裕美（経済・金融犯罪対策チームリーダー）

インタビュー

バンキングマルウェア・ビジネスメール詐欺・ランサムウェアなど、攻撃者が繰り出す新たな手法はとどまることを知らない。対抗策の鍵となるのはサイバー犯罪に関する情報やノウハウの共有といった防御側の連携だろう。一般財団法人日本サイバー犯罪対策センター（JC3）は産官学が連携する機関であり、サイバー脅威に対処する活動を続けている。組織の概要と 3 月に予定される JC3 フォーラムについて話を伺った。

取材・文・撮影＝斉藤健一

JC3 設立の経緯と海外組織との連携

斉藤（以下 K ）：一般財団法人日本サイバー犯罪対策センター（JC3：Japan CyberCrime Control Center）の組織と 3 月に行なわれるフォーラムについて、島根さん（理事）と間仁田さん（経済・金融対策チームリーダー）にお話しを伺います。よろしくお願いします。

島根（以下 S ）・間仁田（以下 M ）：よろしくお願いします。

K JC3 は 2014 年 11 月に業務を開始しましたが、まず、組織設立の経緯を教えてください。

S 日本版 NCFTA（National Cyber-Forensics & Training Alliance）として設立されました。NCFTA とは米国の非営利団体で、法執行機関・民間企業・学術機関を構成員としてサイバー犯罪に関する情報の集約や分析、海外を含めた捜査機関の職員に対するトレーニングなどを実施しています。日本においても同様に、産官学が連携しサイバー空間全体を俯瞰した上で、犯罪などの脅威を特定し、軽減・無効化する取組みを推進する組織として JC3 が設立されました。

K 2014 年 11 月といえば、サイバーセキュリティ基本法の成立とほぼ同時期です。前年の秋には 2020 年の東京五輪の開催が決定しました。政府がサイバーセキュリティに力を入れはじめた時期と符合することがよく分かりますね。次に活動内容に関する質問です。NCFTA をはじめとする海外組織との連携をより具体的に教えてください。

M 前述の NCFTA の他、英国の CDA（Cyber Defense Alliance）とも提携しています。両組織とは定期的にビデオ会議を開催し、サイバー犯罪の情勢や手口の変遷といった分野で情報共有を行なっています。海外で起きた犯罪事例が時間差で日本に入ってくるケースもありますから、その手口を知ることは日本のサイバー犯罪対策に有効だと考えています。また、APWG（Anti Phishing Working Group：フィッシング対策ワーキンググループ）という国際機関とも、偽ショッピングサイトに関する情報交換をしています。日本においても最近、偽ショッピングサイトの被害が広がってきました。

●島根 悟（しまね・さとる）写真右

1984 年　警察庁入庁
2007 年　警察庁長官官房参事官（企画担当）
2010 年　警察庁長官官房国家公安委員会会務官
2011 年　警察庁刑事局刑事企画課長
2013 年　静岡県警察本部長
2014 年　警察庁長官官房審議官（生活安全局担当）
2015 年　神奈川県警察本部長
2017 年　警視庁副総監
2018 年　辞職
2018 年　JC3 理事

●間仁田 裕美（まにた・ゆみ）写真左

2001 年　警察庁入庁
2004 年　警察庁生活安全局情報技術犯罪対策課企画法令係長
2006 年　警察庁情報通信局通信施設課施設第一係長
2008 年　内閣官房情報通信技術（IT）担当室主幹
2010 年　警察庁警備局警備企画課課長補佐（サイバーセキュリティ）
2013 年　警察庁生活安全局情報技術犯罪対策課課長補佐（対策防犯）
2014 年　オランダ国家警察ハイテク犯罪特別捜査隊
2015 年　警察庁生活安全局情報技術犯罪対策課課長補佐（対策防犯・国際）
2016 年　JC3

K 国際連携で得た情報は、どのような形で活かされているのでしょうか。

M NCFTA とは契約で、情報をシェアできる範囲を決めており、その範囲内で活用しています。情報については会員企業にシェアしたり、Web サイトの注意喚起などに役立てたりしています。

会員企業のメリットとは

K 会員企業になるとどのようなメリットがあるの

でしょうか。

S 会員には正会員と賛助会員があります。また、警察などの法執行機関や学術機関は賛同組織という位置付けとなります。警察を始め会員企業は定期的に会合を持ち情報共有を行なっています。興味を持つテーマは会員企業によってさまざまですが、不正送金・e コマース・情報流出対策・脅威情報活用などのグループでの活動のほか、会員向けワークショップも開催されています。

K JC3 の Web サイトでは、ワークショップの要旨が公開されており、興味深く拝見させていただきました。この中で CTQ という語句があったのですが、何を意味するものなのでしょうか。

M CTQ とは Catch Threat Quickly の略です。標的型攻撃の犯罪者グループの特徴・手口などをまとめた Wikipedia 方式のデータベースです。会員企業と連携することによって、情報流出を狙うような標的型攻撃の情報を共有するものになります。

K 会員企業が得られる情報は、公開情報にはない貴重なものと考えてよいですか。

M 会員企業・組織が持っている情報に加えて、警察から提供される情報（例えばインターネットバンキングに係る不正送金の情報）が、JC3 というプラットフォームに集約されています。また、これらの情報を JC3 のアナリストが横断的に分析し、付加価値をつけた情報が共有されていると思います。

K セキュリティ企業などが脅威インテリジェンスとして情報を販売することもありますが、そういった情報と同等なのでしょうか。

M 一般に商品として提供される脅威情報は、なるべく多くの人が欲しがる情報を集めて提供されていると思います。JC3 はそれぞれの会員企業のニーズを聞いて、それに応じた情報を提供するように努めています。

K 俗っぽい質問で恐縮です。正会員になった場合に発生する費用とセキュリティ企業から脅威インテリジェンスを購入する費用を比較することはできますか。

M JC3 に加入する理由は企業それぞれにあるとは思いますが、いわゆる脅威インテリジェンスのサービス提供を受けるような感覚で入会しているところは多くないと考えます。もちろん脅威情報の収集も目的の 1 つですが、それ以上に皆で対策を講じていきたいという思いで、警察や個別の企業だけでは実現できない、同じ志をもった人とアクションしたいと考えて参加されている企業が多いと思います。

K ありがとうございます。話題を変えて Web サイトで提供されている情報についてお聞きしたいと思います。注意喚起として「不正送金等の犯罪被害につながるメール」などが公開されています。さまざまな事例がまとめて紹介されており興味を持ちました。これはどのように収集されているのでしょうか。例えば JPCERT/CC にはマルウェアの検体を受け付ける窓口がありますが、JC3 でも同様にユーザーからの通報を受け付ける窓口があるのでしょうか。

M 収集方法は異なります。犯罪被害につながるメールについては、主に犯罪者が使っているフレームワークを分析して、日本のユーザー向けにどのようなメールを配信しているかを探っています。

K JC3 には専任のアナリストがいらっしゃるのでしょうか。それとも会員企業からそういったスキルを持った人財が派遣されているのでしょうか。

S 主に後者です。

JC3 が開発するトレーニングコース

K JC3 でサイバー脅威に対処するためのトレーニングやそれに類するプログラムなどを開発されているのでしょうか。

S 現在トライアルの位置付けで、法執行機関向け、具体的には警察向けのトレーニングコースを実施し、受講者の感想なども聞きながら開発を進めているものがあります。

K それは興味深いですね。トレーニングコースを受講する方は各都道府県警の方ですか。差し支えなければ、受講者の IT に関する知識レベルなどについて教えてください。

S 全国 47 都道府県ありますから、職員のサイバー犯罪捜査のレベルも異なります。東京などの大都

市では発生する事件や相談の数も多いので、概して捜査に携わっている人数も多く、経験も豊富です。また、都道府県警によっては民間企業でバリバリと活躍してきた人を採用することもあります。都道府県それぞれで体制や事情は異なりますが、JC3 としては、能力向上を図るお手伝いをしていきたいと考えています。

K 受講者の方からの感想はいかがでしたか。

S 実践的なノウハウを学ぶことができたといった声は聞いています。

K 実践的ということは、トレーニングは具体的な事件の捜査を進めるような形になっているということですね。

S そのとおりです。サイバー捜査に携わってきた人が、自分が経験してきた事案をベースにしています。現場の警察官からすれば、なるほどと納得できるものになっていると思います。

JC3 が注目する今後のサイバー犯罪動向

K 続きまして JC3 が注目しているサイバー犯罪について伺いたいと思います。会員企業の中に bitFlyer がありました。昨年はコインチェックの NEM 流出事件が起こるなど、仮想通貨については社会全体が注目しています。この分野の研究などは進められているのですか。

S 仮想通貨交換業の登録制度ができるなど、仮想通貨は国として法的な位置付けを持ったものになりました。不正送金に仮想通貨が使われるケースもありますから、今後は会員企業とともにこの方面に関心を向けていかなくてはならないと考えています。

K 日本のセキュリティ業界のトピックには 2020 年の東京五輪があります。懸念されている事柄の 1 つに IoT 機器に対するサイバー攻撃があります。こちらはどのようにお考えでしょうか。

M JC3 では PC を対象にしたマルウェアの監視・対策だけではなく、スマートフォンを対象にした不正なプログラム、そして IoT 機器に対するマルウェアについても定期的に監視・解析を行なっています。IoT 機器を対象にしたマルウェアについては、特に DDoS 攻撃に使われることが分かってきています。DDoS がどういった組織に向けられているかといった情報もあわせて収集しています。

3 月 28 日にフォーラムが開催

K 最後に 3 月に開催されるフォーラムについてお聞きします。すでにアナウンスされているのでしょうか（編注：インタビューが行なわれたのは 2019 年 2 月 14 日）。

S 専用ページが昨日公開となりました※ 1。

K 一般の方も参加できるということですが、どういった趣旨になりますか

S JC3 から見たサイバー空間の脅威に関するトピックを一般の方に提示し、それぞれの登壇者の方からご講演いただきます。最後は私の方から JC3 の活動を紹介します。

K 登壇者も決定されているのでしょうか。

S 今年の基調講演は、三菱 UFJ さまが専任の CISO を設置されたということで、この任に就く亀田氏から経営とサイバーセキュリティの関係について講演をお願いしています。また、第二部にあたる形として、東京五輪を間近に控えて、オリンピック・パラリンピック大会組織委員会の CISO である坂氏が講演を行ないます。組織委員会によるサイバーセキュリティの取り組みを語っていただけると思います。さらに放送事業者のフジテレビさまから、また多数の外国人観光客が来日することを考慮し、旅行会社の JTB さまにもお願いし、インバウンド関連の話題でご講演いただこうと考えています。そのほかの方にもお願いしておりますので、全体が分かる専用ページを見ていただきたいと存じます。

K 仕事柄、サイバーセキュリティを技術的な視点から見ることは多いのですが、今回のフォーラムでは、さまざまな業種の方がそれぞれ異なった視点で講演を行ないます。なかなか得がたい機会だと思いますので期待しています。本日はありがとうございました。

※ 1 **JC3 Forum 2019** https://www.jc3.or.jp/activity-report/forum2019.html

AV Tokyo で開催されたインテリジェンスを競う CTF

チャレンジ Open xINT CTF

文＝日立システムズ CTF チーム K

Open xINT CTF とは

こんにちは。日立システムズ CTF チームの K です。2018 年 11 月 3 日に開催された、Open xINT CTF にチャレンジしてきましたので、ここに報告します。

Open xINT CTF は、コンピューターセキュリティに関する日本最大級のコミュニティーカンファレンスである AVTokyo 内のイベントの 1 つで、2016 年から開始され今回で 3 回目の開催となっています。運営を担当する pinja は DEFCON の Intel CTF に出場するために結成されたチームです。

通常の CTF では、マルウェアを解析したり、ソフトウェアのぜい弱性を探したり、コンピューターを攻撃したりしますが、Open xINT CTF は異なります。名前の INT が示すとおり、Intelligence（インテリジェンス：諜報活動）の能力を競うもので、Osint（オシント：Open Source INTelligence： 公開情報を活用したインテリジェン）、Humint（ヒューミント：人間を媒介としたインテリジェンス）といった手法を駆使して解答を導き出します。

Open xINT CTF は個人戦です。結果を先に報告すると、筆者は 1100 点を獲得し 10 位に終わりました。PC を持たず飛び入りでの参加だったので、いま一歩という結果も当然かもしれません。

ちなみに 2018 年の問題は、OSINT（Webint） 手法を用いて解く問題が多かったため、スマートフォンだけでも対応できたと思います（レスポンスヘッダを見る必要がある「HIMA 300」を除く）。

画像からバスの位置情報を特定

ここでは数ある問題の中から BUS 500 を紹介したいと思います。当日、この問題を最初に解いたのは筆者でした。調査状況を再現するために、すべてスマートフォンで取得したスクリーンショットを使用します。なお、これらのスクリーンショットは当日取得したものではありません。

BUS 500 は、バスが停車している地点を探す問題です（図 1 右）。問題には、「Nxx.xx Exxx.xx」で解答するとありましたので、バスが停車している位置の緯度経度で解答する必要があります。

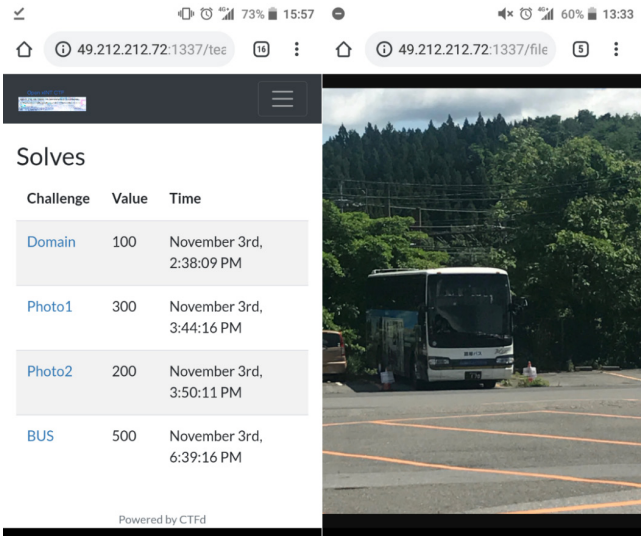

図 1 画像からバスの位置情報を特定する

・ステップ 1：バスの特定

まず、バスの種別を特定することが第一ステップと考えました。問題画像を見ると、解像度が低く「XX バス」と特定不能な 2 文字が見受けられます。筆者は、例えば「日立バス」のように、特定の観光地のバス名が記載されているものと推測し、思いつくかぎり、Google 画像検索を行ないました（その後、この推測は誤りであることが分かります）。会場でチャレンジしている多くの参加者も同様に考え、Google 画像検索を行なっているようでした。

筆者は、この「XX バス」について 30 分ほど調査しましたが、該当するバスを特定することができませんでした。そこで方針を変更し、画像から特定可能なヒントであるナンバープレート「170」をキーに検索を試みることにしました。とはいえ、ナンバープレート「170」だけでは、情報の絞り込みが難しいと考え、画像の背景に山らしき画像が確認できることから、山間部走行しているバスであると想定し、検索ワードを「バス 山 170」に設定しました。その結果、このバスは「かたしなエクスプレス」であると特定することができました（図 2 左）。また、前述した「XX バス」の箇所は、検索よって得られた画像より、「路線バス」ということが判明し、当初の推測が大きな思い込みであったことが分かりました。

図 2 バスの種別が特定できた

・ステップ 2：地点の特定

バスの種別を特定できましたので、問題の地点の特定を行ないます。まずは「かたしなエクスプレス」の路線表を調査しました（図 2 右）。問題画像からは、どこかの大きな駐車場のような場所であると推定できますので、路線表中の大きな停留所のいずれかではないかと推測しました。怪しいのは当然、始発駅の「東武日光駅」と終着駅である「鎌田」です。これらを Google ストリートビューで確認したところ、「東武日光駅」は開けた町であり「山」らしくない、「鎌田」は停留所が問題画像ほど大きくないという理由から、筆者はこれらの場所が正解ではないと判断しました。

次に、路線の停留所の中にドライブインなどのような広い場所がないか、Google ストリートビューなどを利用して確認してみましたが、近しい結果を得ることはできませんでした。これまでの調査の結果、解答が得られなかったことから、筆者はもう一度問題画像を見直すことにしました。すると、バスの後方、山の前方に、電線のようなものが写っていることが確認できました。しかし、電線にしては、数が多く、また複雑であり、林間部を通っているように見受けられました。そのため、私は電車の送電線ではないかとの推測にいたりました。

そこで、再度、Google Map を用いて、「東武日光駅」から「鎌田」の経路を確認すると、電車が通っているのは、「東武日光駅」だけであることが分かりました。加えて、もう一度、東武日光駅の周辺を、Google Map（衛星画像）で確認すると、直近に大きな駐車スペースがあり（図 3 左）、ストリートビューで確認したところ（図 3 右）、問題画像の箇所に酷似していことも分かりました。この結果、解答の位置座標「N36.74, 139.62」を特定する

ことができました。

なお、公開されている WriteUp によると、「東武日光駅」の位置情報で正解との情報ありますが、これは解答位置情報のフォーマットが、「Nxx.xx Exxx.xx」と少数 2 ケタまでであり、約 1111m の誤差を許容しているためだと考えられます。仮に解答が少数 3 ケタまでであった場合、約許容される誤差は 111m となるため、「東武日光駅」近辺の位置情報では、不十分であり、今回の紹介したように駐車スペースまで特定する必要があった可能性があります。

図 3 位置情報を特定できた

チャレンジを終えて

今回は、Open xINT CTF から、BUS 500 の問題について紹介させていただきました。この問題はは、画像から OSINT（Webint）を駆使して位置を特定するものでしたが、その手法などは、サイバー犯罪に係るリサーチなどにおいても、一般的に利用されているものであり、このような手法を実践形式で経験することができる Open xINT CTF は、非常に有用であると考えられます。

運営チームは、2019 年開催予定の AV Tokyo の Call For X（企画募集）にも応募するといっています。その時は皆さんも “PC を持参して ”、参加してみてはいかがでしょうか。

Hitachi Systems Security Journal VOL.30

Human * IT

人と IT のチカラで、驚きと感動のサービスを。

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