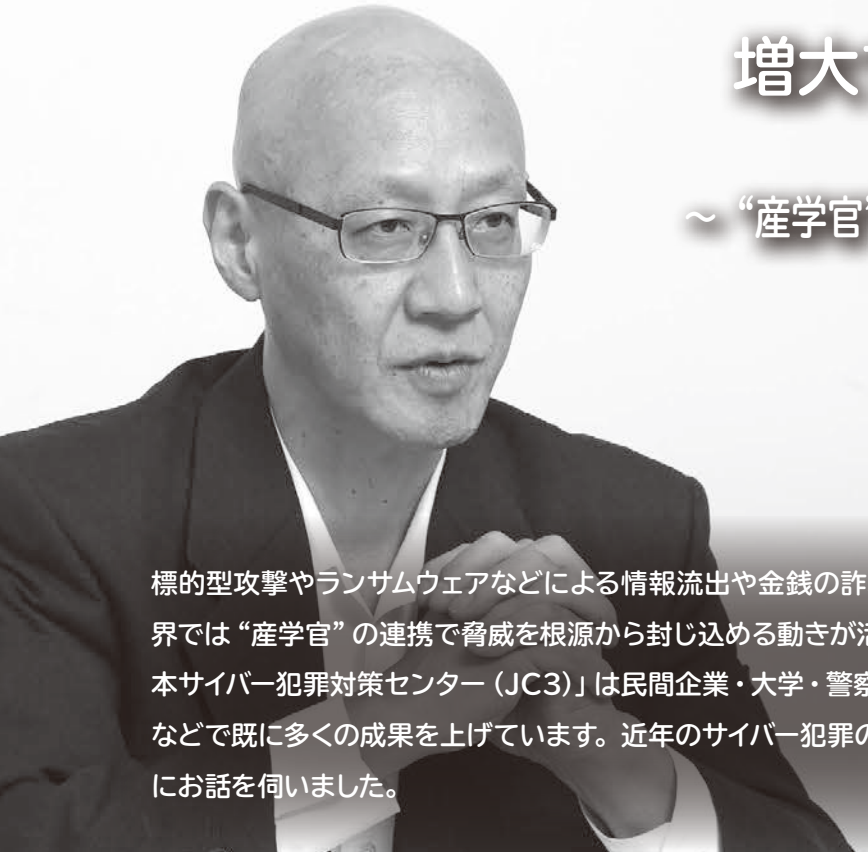


増大するサイバー犯罪の根源的な解決へ

～“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？～

標的型攻撃やランサムウェアなどによる情報流出や金銭の詐取といったサイバー犯罪が後を絶たないなか、世界では“産学官”の連携で脅威を根源から封じ込める動きが活発化しています。2014年11月に始動した「日本サイバー犯罪対策センター（JC3）」は民間企業・大学・警察庁の参画で設立された組織で、犯罪集団の摘発などで既に多くの成果を上げています。近年のサイバー犯罪の傾向とJC3の取り組みについて、理事の坂明氏にお話を伺いました。

坂 明　氏

日本サイバー犯罪対策センター（JC3）
理事

1981年、警察庁に入庁。目黒警察署長、通商産業省（現、経済産業省）通商政策局中南米室長、兵庫県警察本部長、国土交通省大臣官房審議官（自動車局担当）などを務めたほか、生活安全局セキュリティシステム対策室長、情報技術犯罪対策課長として勤務し、サイバー犯罪対策に従事。2002年にはハーバード大学国際問題研究所（WCFIA）客員研究員としてサイバーテロの研究に従事し、2008年から2年間は慶應義塾大学大学院政策・メディア研究科教授。2014年11月より日本サイバー犯罪対策センター理事。原子力規制委員会核セキュリティに関する検討会委員、東京オリンピック・パラリンピック競技大会組織委員会チーフ・インフォメーション・セキュリティ・オフィサー（CISO）なども務めている。

サイバー犯罪の最近の動向とは？

――サイバー攻撃の被害が世界各国で増加するとともに、犯罪事案が増えています。近年の傾向として、どのような脅威が出現しているのでしょうか。

依然として多いのが標的型攻撃です。警察庁が発表した2016年上半期のデータを見ると、多くの人を対象とした「ばらまき型攻撃」以上に、ピンポイントでターゲットを狙う本格的な標的型攻撃が増えています。重要インフラ事業者を狙ったマルウェア「Daserf（ダザーフ）」がその典型で、感染させたPCから長期間にわたって重要な情報を搾取するなど、手口が非常に巧妙化しています。ランサムウェアについても、ファイルを人質にユーザーを脅迫して金銭をだまし取る以外に、ネットワーク経由で自己増殖し、システムを破壊するなどの新しい脅威が増えはじめました。

経営者や取引先になりすまして、企業内の財務会計担当者に偽の送金指示などを行う「BEC（Business E-mail Compromise:ビジネスメール詐欺）」も増加しています。ネットワークカメラやデジタルビデオレコーダといったIoTデバイスを主なターゲットとした「Mirai」、クローズドネットワーク環境から情報を移動させるために利用される

USBメモリ内の機密情報を盗み出す「USB情報窃取」といった手口も確認されています。

――あらゆる企業や個人が脅威にさらされる時代となったわけですね。

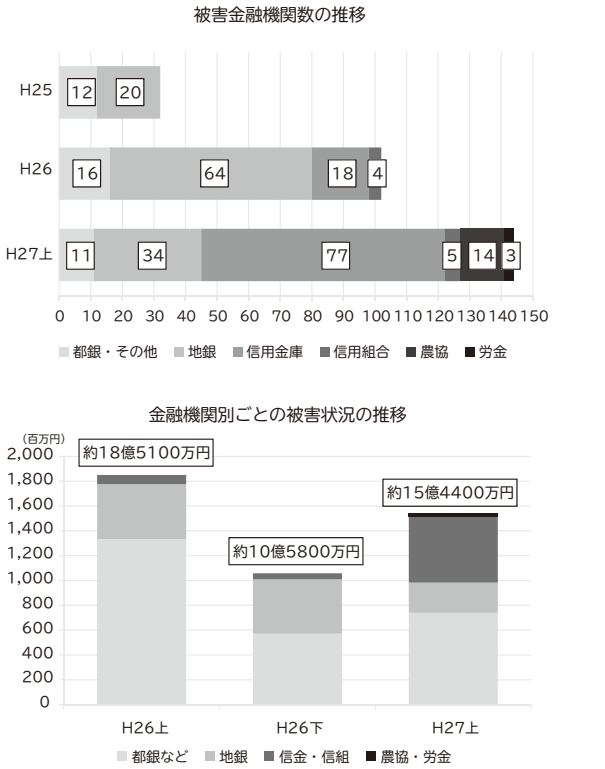
攻撃者は常に“一番弱いと判断した”対象を狙ってきます。金融業界なら、以前は都市銀行や地方銀行がターゲットとされていましたが、それらのセキュリティ対策が強固になると、今度は信用金庫や信用組合、農協、労金などの中小金融機関をターゲットにしてきます。特に中堅中小企業の場合、サプライチェーンのなかで大企業に侵入するための踏み台として利用される可能性がありますから、規模や業種に関係なくセキュリティへの防御をおろそかにすることはできません。

――標的型メール攻撃の件数も増えているようですね。

警察庁が2016年中にサイバーインテリジェント情報共有ネットワークで把握した数だけでも、標的型メール攻撃の件数は4,046件と前年より218件増加しています。一般の方や企業などからの相談件数も13万件を越えるなど、過去最大を記録しました。インターネットバンキングにかかわる不正送金は、被害総額は減少傾向にあるものの、攻撃者は常に新たな手法を用いさまざまな分野で弱いターゲットを狙ってきております。**図1**は平成27年上半期の被害状況ですが、ここから分かるように幅広い金融機関がターゲットとなっており、現在はいずれの種類の金融機関であってもその中で弱いところが狙われる、という状況ですし、更にビットコイン口座を狙うなどの新たな動きもあります。

――脅威が増大するなか、国や企業はどのような対策と心構えが必要なのでしょうか。

サイバー犯罪はある意味、グローバルなビジネスとして成立しています。分業化も進んでおり、マルウェアを開発する人、マルウェア攻撃の指示を出す人、実際にマルウェアをばらまく人、そのためのサーバを提供する人、不正送金を要求する人、不正口座を用意する人、現金を引き出す“出し子”など、多くの犯罪者が国境をまたぎながら有機的につながっています。こうした犯罪を防ぐには、攻撃者の行動プロセスとなっている「サイバー・キル・チェーン」をどこかで断ち切ることが重要です。



出典：警察庁「平成27年上半期のインターネットバンキングに係る不正送金事犯の発生状況等について」2015年9月3日

図1　攻撃対象の推移

現時点では、日本で最も多く検挙されるのは出し子グループです。出し子はさまざまな犯罪のインフラの1つですから、そこから不正送金の指示にまで遡ることも決して不可能ではありません。しかし、より重要なのはサイバー・キル・チェーンの全体を俯瞰しながら先制的・包括的な対応を行い、犯罪者集団を根本的に無効化していくことにあります。そのため米国では1997年にFBIなどの法執行機関、民間企業、学術機関が連携した「NCFTA（National Cyber-Forensics & Training Alliance）」という組織が設立され、サイバー犯罪にかかわる情報の集積・分析、国際的な捜査連携などでサイバー犯罪に対処していく取り組みが行われています。

産官学それぞれの強みを生かす橋渡し役として

――そのNCFTAをモデルに設立されたのが、坂様が常

勤理事を務めておられる「日本サイバー犯罪対策センター（JC3:Japan Cybercrime Control Center）」なのですね。

おっしゃるとおりです。JC3は「日本版NCFTA」の創設に向けた政府の情報セキュリティ政策会議での検討と閣議決定を経て、サイバー空間の脅威に“産学官”の垣根を越えた連携体制で対応すべく2014年11月に設立されました。民間企業、警察庁、学術研究機関といったさまざまな組織が参画しており、互いの信頼関係と秘密保持契約の下で、それぞれの情報や知識・経験、ノウハウを共有し、脅威の実態解明や犯罪者の特定・追跡を行い、脅威の除去に向けた活動を展開しています。また、人材育成や海外の関係機関との国際連携なども事業の大きな柱となっています。

――JC3は“産官学”の参加者に対して、どのような役割を果たしているのでしょうか。

産業界、法執行機関、学術研究機関、それぞれの強みを生かすための橋渡し役といったところでしょうか。これまで各企業が単独でサイバー攻撃と戦ってきた際の経験や実績を持ち寄り、学術研究機関が分析や研究成果の知見を加え、更に法執行機関の捜査権限を生かした強制力で攻撃者を叩く。そういったコラボレーションのハブとしての役割を果たしています（**図2**）。

――JC3がモデルとした米国NCFTAは、既にかなりの成果を上げているようですね。

もう20年近くの歴史を誇る団体ですから、積み上げてきた実績も大きいですね。昨年だけでも検挙したサイバーセキュリティ事案数が300件以上と聞いています。JC3はNCFTAとも協力関係にあり、コンセプトや組織運営でも多くの部分でNCFTAの手法を学ばせていただいています。例えばNCFTAには4つの基本ポリシーがあります。

“One team, one goal”
（1つのチームで同じゴールをめざそう）
“Face to Face”
（直接会って話し合おう）
“Industry First”
（民間企業を第一に考えよう）
“Focus on what you can share and are comfortable sharing”
（共有できる情報、共有しても支障のない情報にフォーカスしよう）

というものです。

JC3も基本的に同じポリシーで活動を進めており、参加者が互いに強い信頼関係を築きながら、情報を共有し合い、1つのチームとしてサイバー犯罪に立ち向かっています。

ただしNCFTAとは少し異なる特長もあります。例えば、NCFTAにはFBIをはじめとする連邦政府や国外の15以上の法執行機関が参加しています。これに対し、JC3には全国の警察組織をとりまとめる警察庁のメンバーが、事務所内に常駐体制を敷いています。そのため、全国一斉の捜査・摘発では足並みを揃えた行動が非常に取りやすいのです。また、NCFTAに参加する企業の多くは、サイバー攻撃の対象となる可能性が高いため、積極的にはメンバーシップを公表していません。しかしJC3はホームページでもご覧いただけるように、参加企業や協賛団体をオープンに公表しています。それぞれの企業が強固なセキュリティ対策を実践し、互いに協調しながらサイバー犯罪に一丸となって立ち向かおうという気概の現れだと思います。

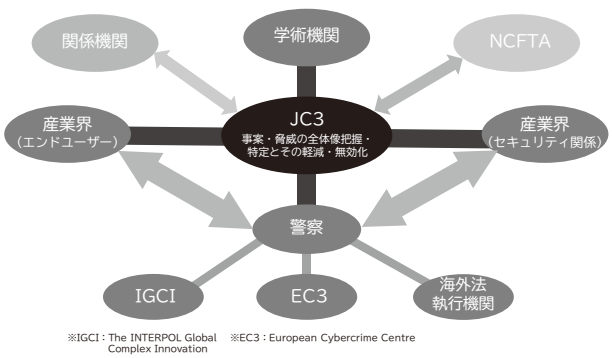


図2　JC3における情報・知見の共有スキーム

サイバー犯罪のテイクダウンに協力

――メディアなどにも掲載されているように、JC3もNCFTA同様に、サイバー犯罪の摘発で数々の成果を上げていますね。

まだ設立3年弱ですので、数的には決して多くありませんが、犯罪者の検挙や犯罪組織のインフラのテイクダウン

（壊滅）、注意喚起活動などで実績を上げています。例えば2015年11月には、10都道府県の警察と協力して違法アダルトサイトの管理者ら13人を逮捕しました。ここでJC3は、違法性のあるアダルトサイトをインターネット上から探し出すソフトを茨城県警と共同開発し、約2,000サイトを抽出することで海外にあるサーバも含めた管理者の特定に協力したわけです。違法サイトは閲覧したPCがウイルス感染する恐れがありますし、海外サーバはサイバー犯罪の隠れみのとして悪用されているため、決して野放しにはできません。

また、ネットバンキングの不正送金や振り込め詐欺などに悪用されている、不正口座についても、JC3と埼玉県警が合同でサイバーパトロールを行い、不正な口座売買に絡む約500件の書き込みを発見したのを端緒に、2016年10月に12人を摘発しています。このうち7人は、口座売買の誘引や預金通帳などの譲り受け・譲り渡しの疑いで逮捕されました。

――まさにサイバー・キル・チェーンを断ち切る成果を上げているわけですね。

こうした犯罪の摘発と並行して、改ざんサイトの無害化にも取り組んでいます。発端はJC3と会員企業の調査により、ランサムウェアや不正送金ウイルスなどによる被害が攻撃ツール「RIG-EK*」によって拡大していることを把握したことでした。改ざんサイトを閲覧したユーザーはRIG-EKが設置されたサイトへと誘導され、不正送金などの犯罪被害に遭う恐れがあります（**図3**）。これは「水飲み場型攻撃」と呼ばれるものです。そこで各都道府県の警察と協力し、Webサイトの管理者にサイトの修復や再発防止などのセキュリティ指導を実施していただく一方、RIG-EKによる攻撃の全容解明を図っているところです。

注意喚起活動としては、JC3における分析や会員企業から寄せられた脅威情報を基に、サイバー犯罪の被害が懸念される緊急度の高い情報をホームページで公開しています。最近では仮想通貨取引所などのサイトがマルウェア「DreamBot」の標的となる恐れがあること、USB情報窃取の手口が確認されたことなどを迅速にアナウンスし、

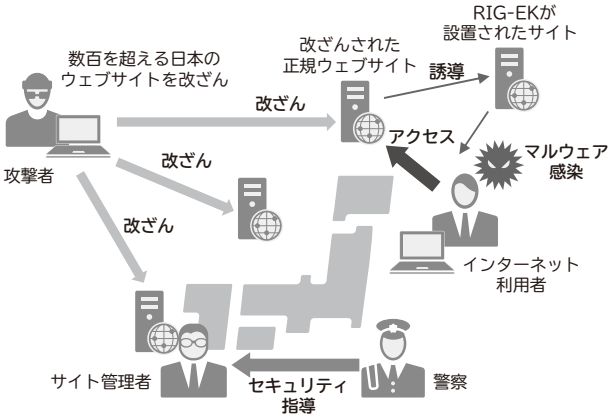


図3　改ざんサイト無害化の取り組み

被害拡大の抑止に貢献しています。

JC3の取り組みが犯罪抑止に貢献

――サイバー犯罪の摘発に至るまでには、どんなご苦労があるのでしょうか。

複雑な要素が絡み合うサイバー犯罪の摘発には、想像以上に多くの時間と手間がかかります。例えば、ランサムウェアや不正送金ウイルスを送りこむことを目的とした水飲み場攻撃として、あるサイトが改ざんされていることを発見したとしましょう。このケースで、改ざんサイトの管理者に「あなたのサイトが狙われています」「すぐに修復してください」と通知しても、表面的には改ざんの痕跡が残らない形に見えますから「何も変化は起こっていない」とか「本当だとしても、どう対処していいのか分からない」といった反応が多く、ただちに対策を取ってもらうのが非常に難しいのです。

不正口座売買の取り締まりでも、相手にこちらの動きを悟られないよう、全国一斉での摘発が必要です。そのため犯罪者を特定するための調査、ログなどの証拠収集と確保、民間企業であるプロバイダや回線事業者への協力要請、更に摘発する各都道府県警の足並みを揃えたり、海外にサーバがある場合は国際的な法執行機関との事前連携

* EK（Exploit Kit）とは、アクセスした端末が保有する脆弱性に合わせ、端末にマルウェアを感染させることができるよう、さまざまなプログラムをパッケージ化した攻撃ツール。RIG-EKはその1つ。

を取ったりすることも必要です。こうして関係者間の調整をしっかり行わなければ効果的な摘発が行えないため、どうしてもテイクダウンに至るまでには一定の時間がかかってしまいます。

――とはいえ、ここ数年のサイバー犯罪被害状況を見ると、JC3の発足以降、そうした地道な努力が着実に実を結んでいるように感じます。例えば、警察庁が発表した2017年3月の報告では、インターネットバンキングの不正送金事犯は発生件数・被害額とも減少していますし、不正アクセス行為の認知状況も前年に引き続き減少。それに対し検挙件数は502件、検挙人員200人と、過去最高になったと記されています。JC3の取り組みが大きな影響を与えているのではないでしょうか。

ありがとうございます。もちろんそれはJC3単独の力ではなく、民間企業の方々が熱心に先進的なセキュリティ対策に取り組んでこられた成果であり、サイバー犯罪を決して許さない警察の断固たる姿勢、そして各国捜査機関との連携によるシナジーだと解釈しています。例えば、最近の国際的事例として有名なのがサイバー犯罪インフラ「Avalanche」のテイクダウン作戦です。世界各国の警察機関やセキュリティベンダーなどの協力によって、2016年末に攻撃指令サーバなどに利用されていたネットワークの解体に成功したこの作戦では、日本においても、関係機関と共有した情報を基に、警察庁をはじめ多くの方々がユーザーへの注意喚起などを実施して、マルウェアの駆除などに積極的に取り組みました。さまざまな犯罪に利用されるボットネットへの対応は大きな課題となっており、こうした取り組みが日本発でもできるとうれしいと思いますし、JC3がこれに貢献できれば幸いと思っております。

――サイバー犯罪との戦いは今後も続いていくと思います。JC3の活動をこれからどのように発展させていきたいとお考えでしょうか。

手口をますます高度化していく攻撃者に対抗するには、信頼関係に基づいてともに脅威の大本を無力化していくための協働が欠かせません。JC3では産学官連携が実体を伴った形で広がりつつあり、これまでセキュリティ関係企業や金融機関、eコマース関係企業などの方々にご協力をいただいておりますが、今後も脅威の実態に合わせて、製造や、流通、商社などの分野をはじめ、業種・業界の枠を越えた信頼できる仲間を募り、脅威の実態を共有することが大切だと考えています。また、グローバルという点では、NCFTAのみならず英国のCDA（Cyber Defense Alliance）といった各国の第三者機関や、インターポール（国際刑事警察機構）やユーロポール（欧州警察機関）といった捜査機関とも一層連携を深めながら、グローバルなサイバー犯罪に立ち向かってきたいと思います。

――今後のご活躍に期待しています。本日はありがとうございました。

---

*本稿は2017年7月の取材をもとに作成したものです。

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

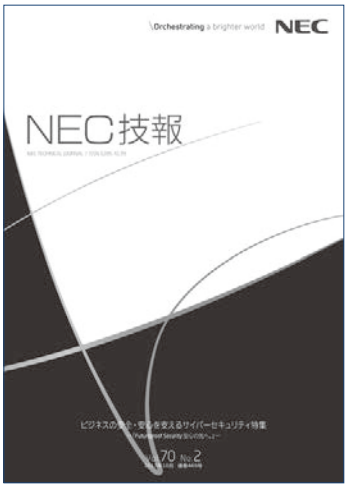
◇ 特集論文

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