【講演③】

サイバー脅威と官民連携～JC3 の取組

一般財団法人
日本サイバー犯罪対策センター業務執行理事
島根　悟

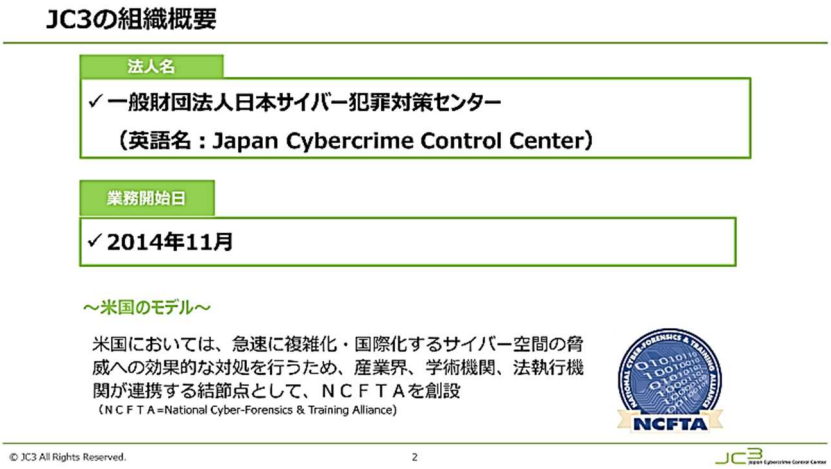
1　はじめに

本日は、「サイバー脅威と官民連携～JC3 の取組」というテーマでお話ししたい。主な内容としては、まず JC3 の組織概要の説明をし、続いて、官民連携について具体的なイメージを持っていただけるよう取組の例をお話ししたい。

様々なサイバー空間の脅威の中でも、経済的利得を目的に行われる犯罪に対する対策として、インターネットバンキングに係る不正送金事犯をメインに、クレジットカード不正利用の一手口としての不正トラベルについての取組、暗号資産に関連した取組について説明をし、その上で、官民連携の意義や今後の目標について、まとめの話をする。

2　JC3 の組織概要

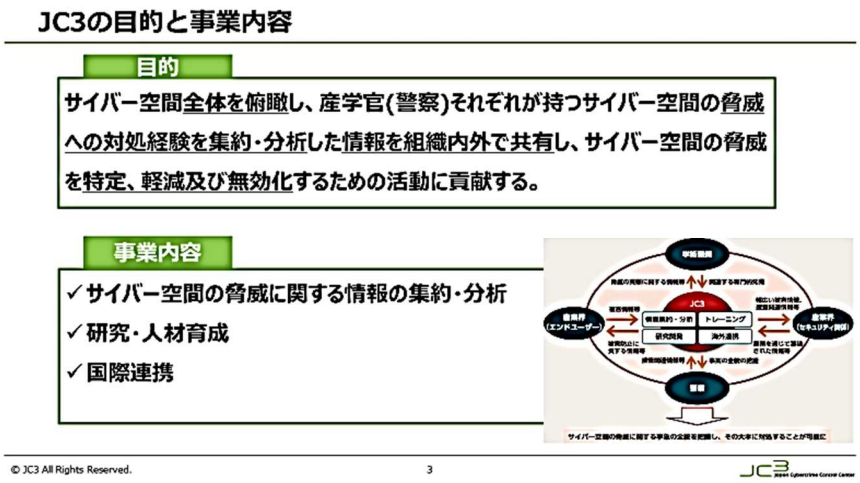
一般財団法人日本サイバー犯罪対策センター（JC3）は 2014 年 11 月に業務を開始した。米国に、産業界、学術機関、法執行機関が連携する結節点として NCFTA という組織があるが、その組織をモデルにして、日本においても同種の組織を創設する必要があるのではないかという議論を踏まえ、発足したという経緯がある（図１参照）。



〈図１　JC3 の組織概要〉

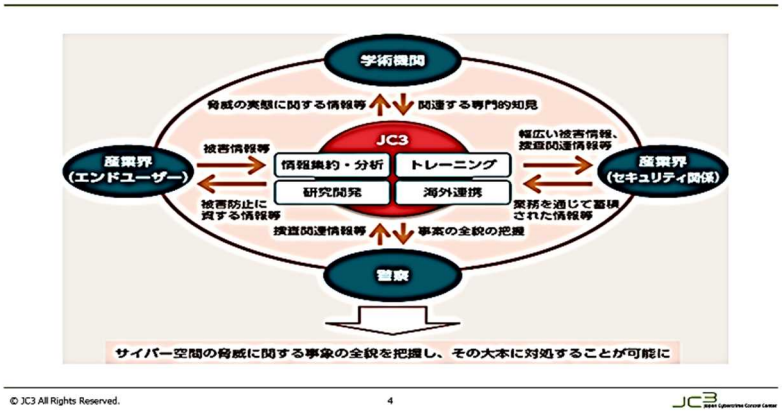
JC3 の目的としては、サイバー空間全体を俯瞰し、産学官（この官は主として警察であるが）、それぞれが持つサイバー空間の脅威への対処経験を集約・分析した情報を組織内外で共有し、サイバー空間の脅威を特定、軽減及び無効化するための活動に貢献することである。

事業内容としては、サイバー空間の脅威に関する情報の集約・分析、研究や人材育成、そして国際連携を柱としている(図２参照)。



〈図２　JC3 の目的と事業内容〉

産業界としては、直接被害に遭う可能性のあるエンドユーザーとしての立場の産業界とセキュリティ関係の産業界を包括するような形、法執行機関たる警察では、その権限を行使してサイバー犯罪やサイバー脅威の実態を明らかにする、そして、これらの「ハブ」としての役割を、JC3 としては果たしていきたいということで日々の活動を行っている(図３参照)。



〈図３　ハブとしての役割〉

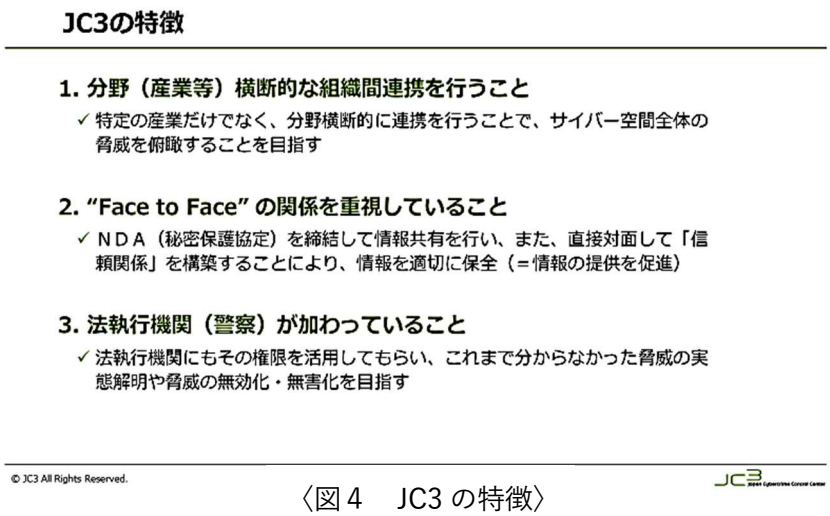
次に JC3 の特徴であるが、ここに３つに整理している（図４参照）。

１つは、分野横断的な組織間連携を行うことである。現在は、例えば金融、通信関係、交通関係等、それぞれの業種によって ISAC と呼ばれるサイバーセキュリティに関する情報交換を行う団体がある。JC3 においては、特定の産業だけでなく、分野横断的に連携を行うこ

とでサイバー空間全体の脅威を俯瞰することを目指している。

２つとして、サイバー空間の脅威、あるいはその被害ということで、各企業にとってはいろいろ秘密にわたるようなこともあるから、情報共有を行う上では、秘密保護協定を締結して秘匿性を担保する、また、直接対面して信頼関係を構築することで情報を適切に保全するなどして情報提供の促進を図っている。

そして３つめは、法執行機関としての警察が加わっていることで、法執行機関ならではの権限を活用していただき、脅威の実態解明、脅威の無効化・無害化を目指すということを、特徴として考えている。



〈図４　JC3 の特徴〉

主な活動領域としては、金融犯罪、E コマース関係への対策、様々な企業の情報流出についての対策をメインに、情報共有・分析を図っている。また、こうした対策の基盤となる活動として、マルウェアの解析、様々な脅威情報の活用、国際連携の推進、あるいは法執行機関に対してサイバー捜査能力の向上に貢献できるような研修を提供している。

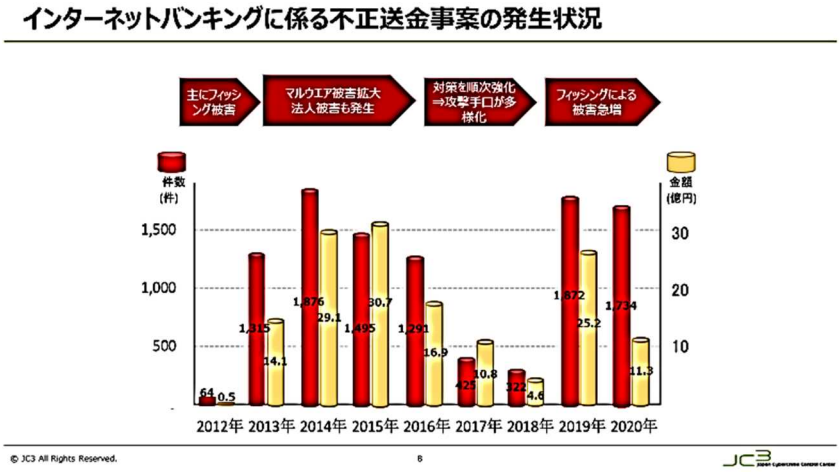
サイバー空間における攻撃者像ということで主として対象としているのは、基本的には経済的な利得を狙って行われるサイバー犯罪に重点を置いて活動をしている。

〈図５　JC3 の活動領域〉

3　インターネットバンキングに係る不正送金事案の発生状況

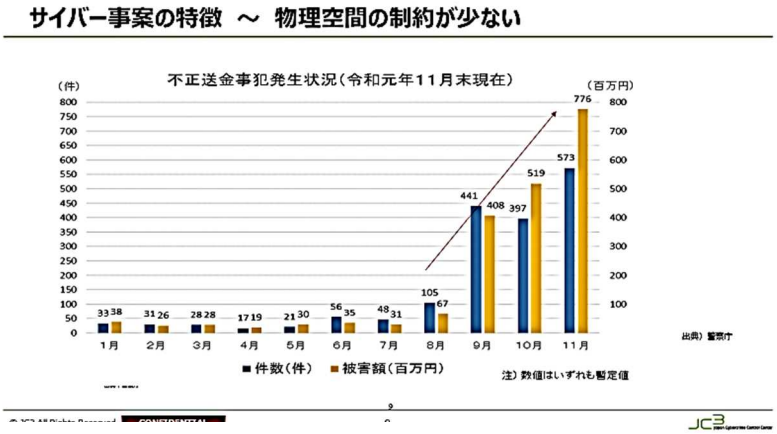
それでは、具体的な活動内容について御紹介する。まず、インターネットバンキングに係る不正送金事案が、サイバー犯罪の１つの典型的な例として取り上げられる。グラフに示しているように、2013 年頃から被害が発生してきて、2014 年、2015 年と、かなり大きな被害件数、被害金額になっていた（図６参照）。この当時は主に、バンキングマルウェアと呼ばれるマルウェアによる被害が拡大していった時期である。

金融機関の御努力あるいは警察の捜査等の取組があり、様々な対策を順次強化したということで、2017 年、2018 年辺りはかなり発生件数・被害金額が減少していた。かなり落ち着いてきたかなと思っていたところ、2019 年からフィッシングによる被害が急増した状況となっている。



〈図６インターネットバンキングに係る不正送金事案の発生状況〉

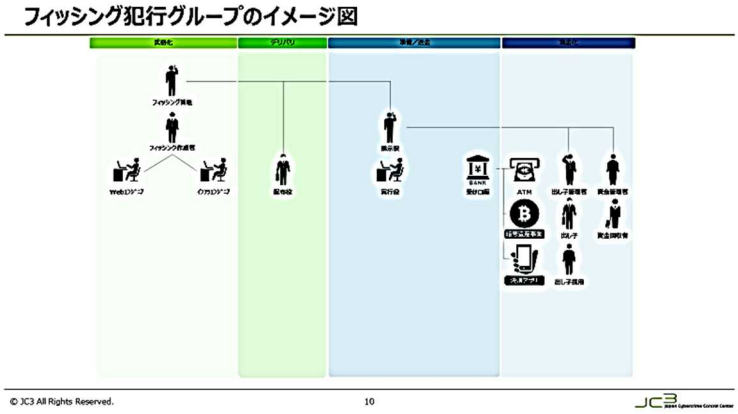
こうしたサイバー事案の特徴として、物理空間の制約が少ないことが挙げられる（図７参照）。2019 年の月別の発生件数を見てみると、前半は非常に少なかったが、9 月から急増する。このように短期間で発生が増減するというのは、物理的空間の制約が.少ないサイバー犯



〈図７　サイバー事案の特徴～物理空間の制約が少ない〉

罪の１つ

JC3 としては、会員と協力して、こうしたフィッシングの犯行グループの特性について検討し、必要な対策を考えている。フィッシングキットを作成する者、実際の犯行を指示して実行する者、そして犯人の用意した受け口座に不正送金して ATM 等から出金する者、このような犯行グループが考えられる。このようなグループに対してどのような対策が効果的なのかを検討している。

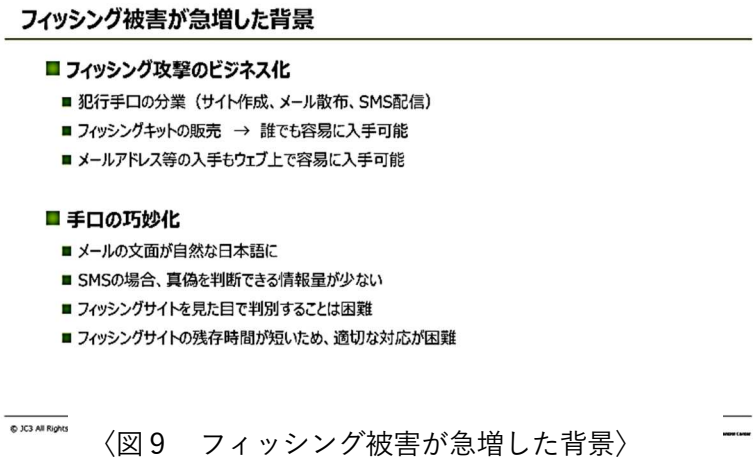


〈図８　フィッシング犯行グループのイメージ図〉

４　フィッシング被害が急増した背景

先ほど、フィッシング被害が急増したと申し上げたが、この背景には、攻撃のビジネス化、つまり犯行の手口が非常に分業化されていること、あるいはフィッシングキットが販売されていて、誰でも容易に入手可能になっていることなどが考えられる（図９参照）。

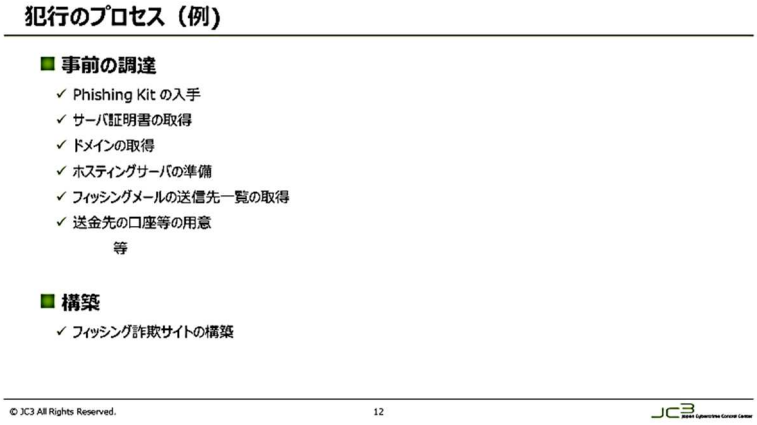
また、被害者の側からすると、受信したメールの文面が非常に自然で、違和感のない日本語であり、それがフィッシングサイトであるかどうかを見た目で判別することが非常に困難であること、また、フィッシングサイトの稼働している期間が非常に短く、適切な対応が困難であるという事情があると考えられる。



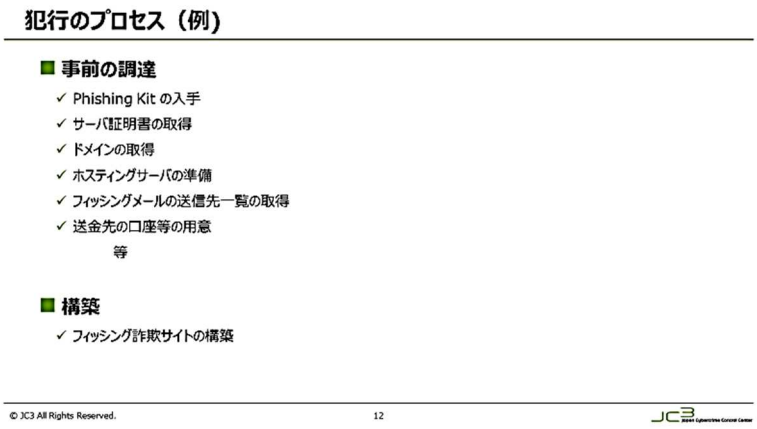
〈図９　フィッシング被害が急増した背景〉

犯行プロセスを例として示したが（図 10、11 参照）、サーバー証明書を取ったり、ドメイ

ンを取得したり、サーバーを準備したり、あるいは送金先の口座を用意する、フィッシング詐欺サイトを構築して電子メールあるいは SMS で誘導したりするというように、用意した口座へ送金し、現金を引き出し、それを集金するといった犯行の形態が考えられる。



〈図 10　犯行のプロセス(例) ①〉

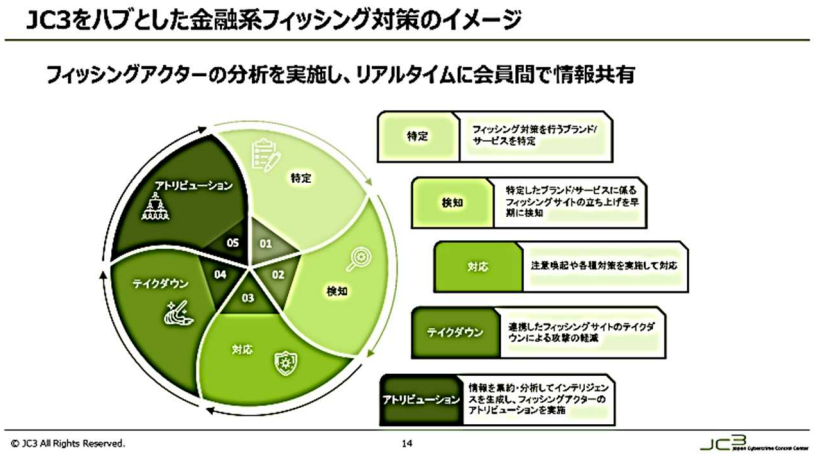


〈図 11　犯行のプロセス(例) ②〉

5　JC3 をハブとした金融系フィッシング対策のイメージ

JC3 においては、このような状況に対して、会員と協力して、ここに記載のようなイメージに基づいて対応を図っている（図 12 参照）。

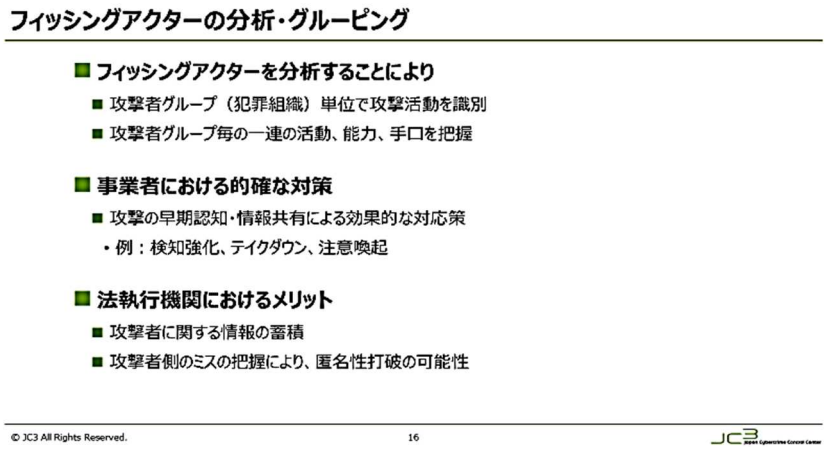
例えばフィッシングサイトといっても非常に多種多様で、様々な金融機関のものがあり、あるいは 1 つの金融機関でもどんどんサイトが変わるという状態である。JC3 ではこれらを分析しており、現在、こうしたアクターをグルーピングして分析するという活動に力を入れている（図 13 参照）。これにより、攻撃者グループの活動の時間帯や、どのような時期に活動しているか、あるいはその能力や規模はどの程度か、また、その具体的な手口といったものの把握に努めている。



〈図 12　JC3 をハブとした金融系フィッシング対策のイメージ〉

事業者からすれば、攻撃を早期に認知して情報共有による効果的な対応策が図られることを期待していると思う。例えば検知体制を強化するとか、フィッシングサイトを早い段階でテイクダウンしたり、あるいは一般の方に注意喚起したりするというようなことである。

また、法執行機関におけるメリットとしては、こうした攻撃者に関する情報を蓄積し、あるいは多くの情報を集めることで、攻撃者側の意図せぬミスを把握し、匿名性の打破についてもできる可能性がある。このような効果を期待しているところである。

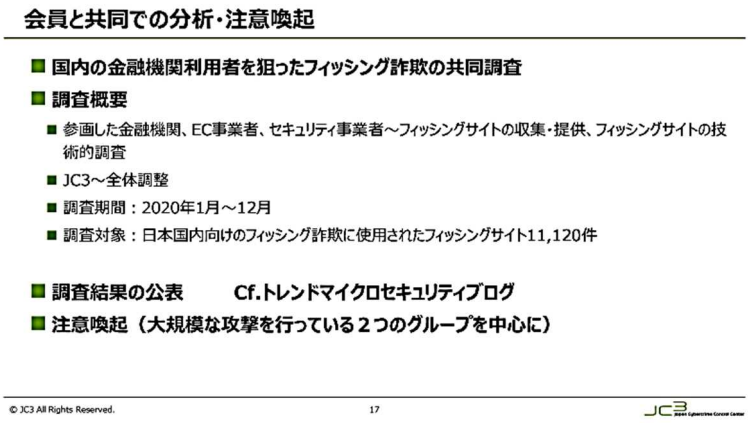


〈図 13　フィッシングアクターの分析・グルーピング〉

令和 2 年 1 年間をかけて、金融機関やセキュリティ事業者の方々の御協力をいただき、国内の金融機関利用者を狙ったフィッシング詐欺の共同調査もしている（図 14 参照）。トレンドマイクロ社のセキュリティブログ等でその調査結果を公表しているし、JC3 においても注意喚起をしているので、参照していただきたい。

これらのグルーピングでは、BP1、BP6 という符号を付けているが、これは Bank Phishing（バンクフィッシング）という意味で、グループごとに名称を付け、それらがどのような特

があって、どのようなところをターゲットにしているかなどについて分析をしている。

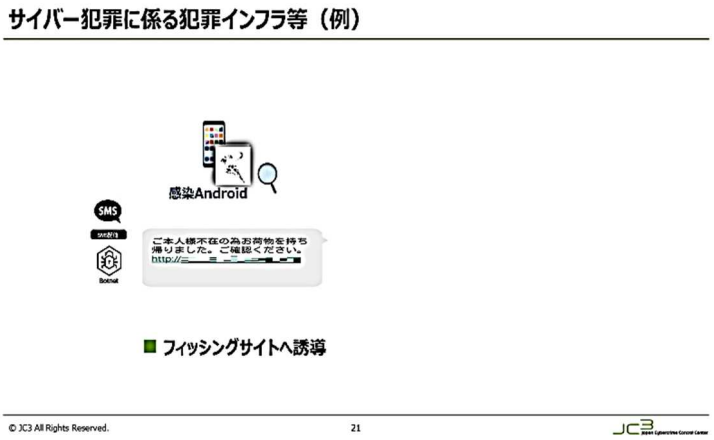


〈図 14　会員と共同での分析・注意喚起〉

6　サイバー犯罪に係る犯罪インフラ等

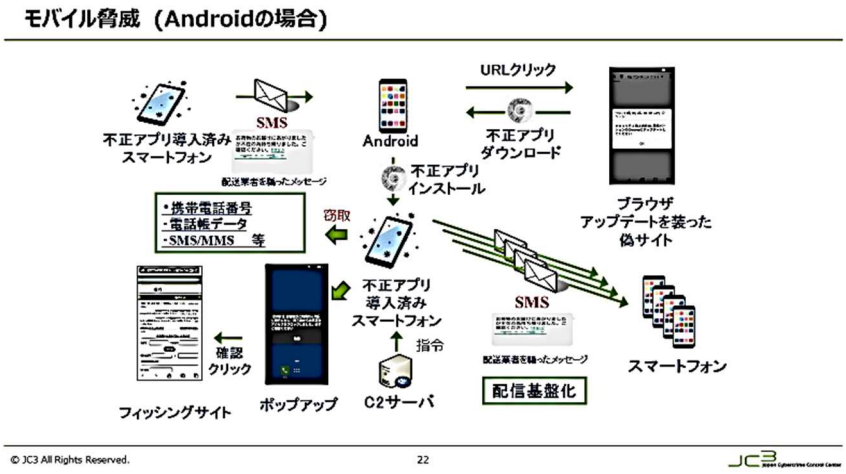
フィッシングを行うために、様々な犯罪インフラが使われているが、JC3 がもう 1 つ力を入れているのは、こうした犯罪インフラに対する対策を打つということである。こうした取組により、犯行をやりづらくさせるという効果が期待できるのではないかと考えている。

犯罪インフラの例として、簡単にフィッシングサイトを構築できるフィッシングキットが流通しており、JC3 の活動の過程でもそれらを発見している。また、フィッシングサイトへ誘導する偽の SMS の配信やプロキシサービス等が犯罪インフラとして用いられる場合も見受けられる(図 15 参照)。



〈図 15　サイバー犯罪に係る犯罪インフラ等（例)〉

SMS については、配送業者をかたったメッセージが非常に有名である。多くの人が被害に遭う状況があるので、具体的にどのように配信されて、それを受け取った人がどのように誘導されてしまうかを、分かりやすい動画の形で示し、注意喚起の実が上がるように対応している（図 16、17 参照）。

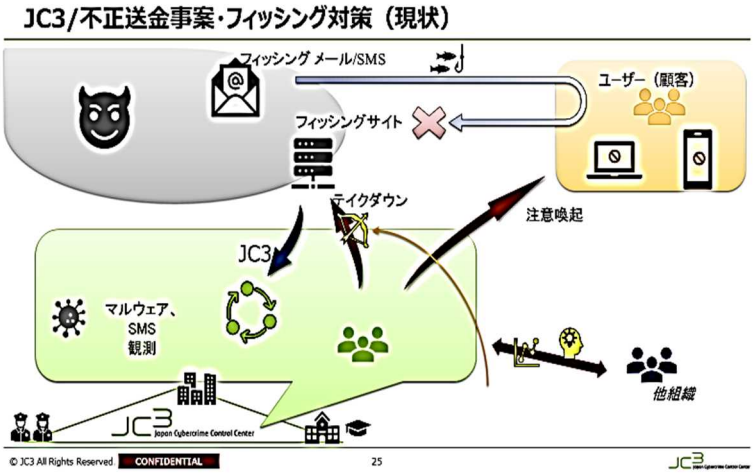


〈図 16 モバイル脅威（Android の場合）〉

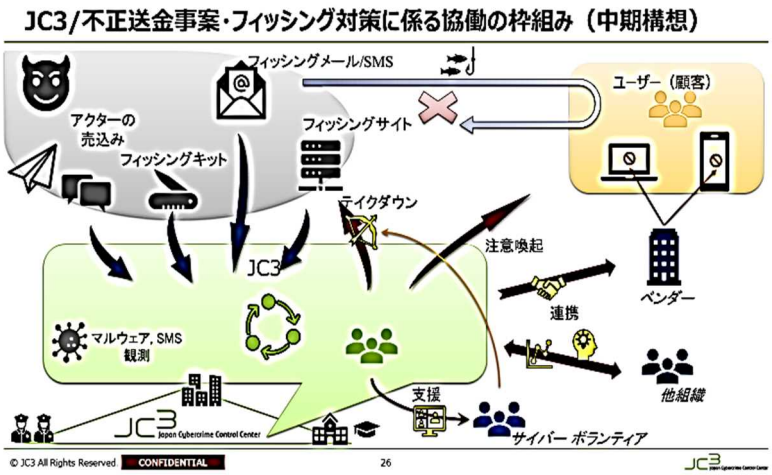
〈図 17 注意喚起〉

そのほかにも、マーケットではチャット等の形でやりとりするものがあったり、金を送る先の口座については金融機関の口座を買うというアプローチがあったりと、このような犯罪インフラが様々に使われる状況になっている。

JC3 では会員と共同して、ユーザーに対する注意喚起等を行っているが、被害はなかなか減らない。中期的には、例えば犯人側のフィッシングキットの売り込み状況等を少し調べてみるとか、あるいはベンダーにフィッシングメールや SMS についての警告をしていただくとか、あるいは非常にたくさん立ち上がるフィッシングサイトについて、例えばサイバーボランティアのような方々に協力をいただくというように、仲間を広げる形での連携、その上での対策ということに力を入れたいと考えている（図 18、19 参照）。



〈図 18　JC3/不正送金事案・フィッシング対策(現状)〉

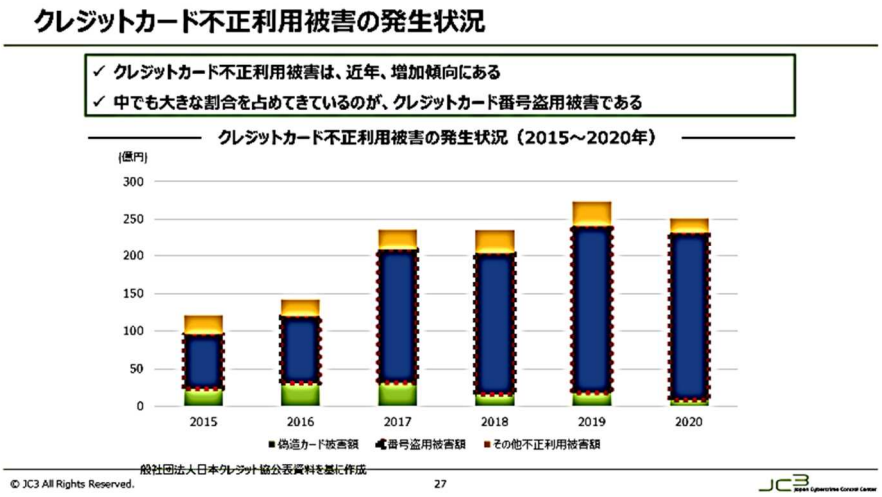


〈図 19　JC3/不正送金事案・フィッシング対策に係る協働の枠組み(中期構想)〉

7　クレジットカード不正利用被害の発生状況

続いての具体例として、クレジットカード不正利用の被害関係について説明する。近年、クレジットカードの不正利用の被害額が非常に大きくなっている（図 20 参照）。以前は偽造カードの被害が多かったが、近年はクレジットカード番号の盗用被害が非常に増えている。ちなみに、昨年（令和 2 年）の特殊詐欺の被害額が 285 億円であるのに対して、クレジットカードの不正利用被害額は 250 億円を超えている。これは財産被害として非常に大きな問題の 1 つと考えている。

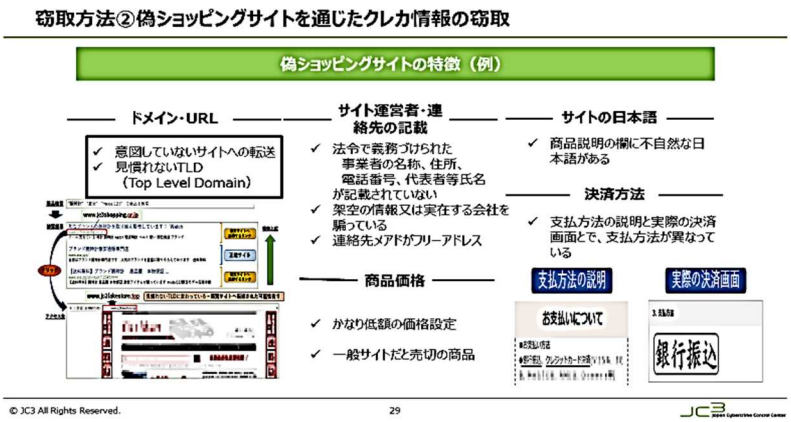
クレジットカード情報窃取の方法としては、カードの券面情報を直接目で見て窃取する場合もあるが、ユーザーがサイバー空間において、例えば、フィッシングページや偽ショッピングサイトでクレジットカードの情報を入力してしまう、あるいは偽の決済サイトでカード



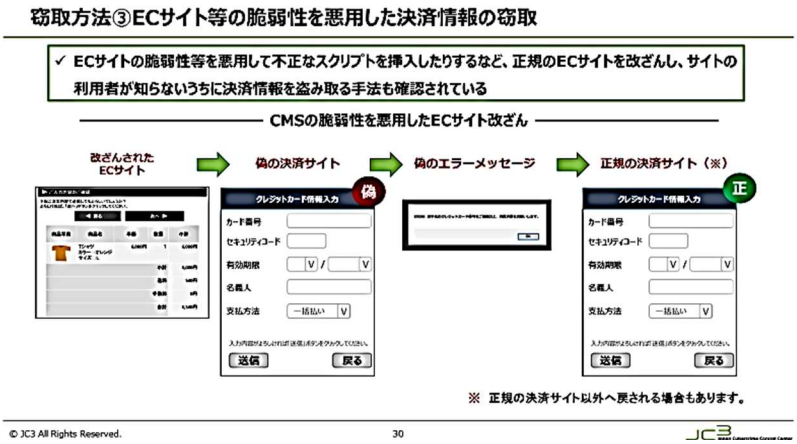
〈図 20　クレジットカード不正利用被害の発生状状況〉

情報を取られてしまうというように、様々な形でクレジットカード情報が取られてしまうケースがあることを把握している。また、こうしたクレジットカード情報が、いわゆるダークサイトと呼ばれるマーケットで販売されている状況も把握している（図 21、22、23 参照）。

〈図 21　窃取方法①フィッシングサイトを通じたクレジットカード情報の窃取〉

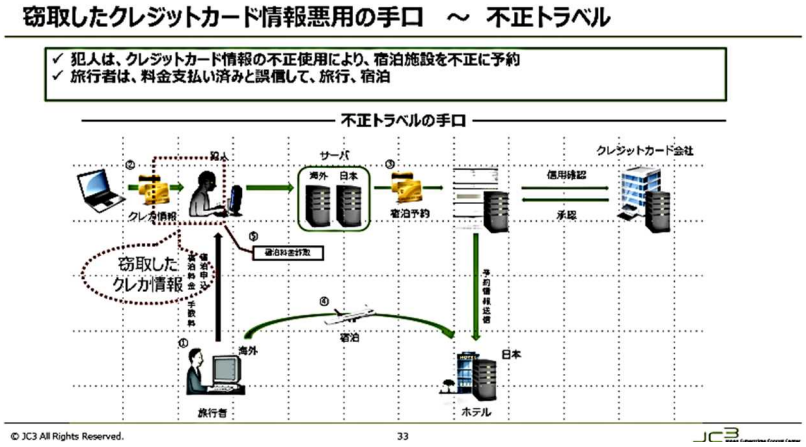


〈図 22　窃取方法②偽ショッピングサイトを通じたクレカ情報の窃取〉



〈図 23　窃取方法③EC サイト等の脆弱性を悪用した決済情報の窃取〉

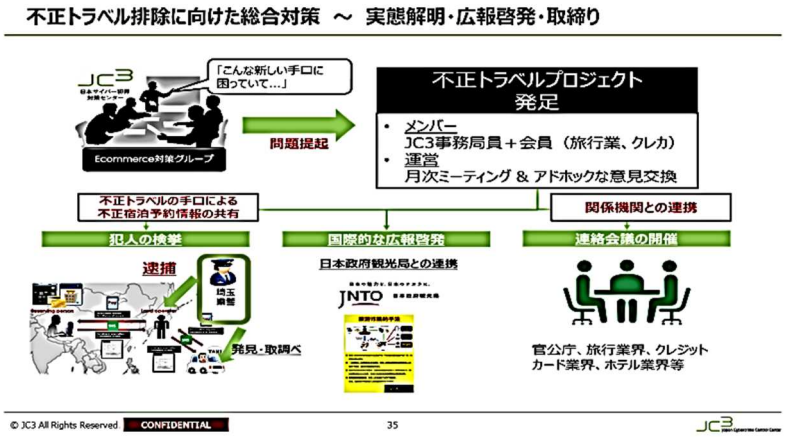
近年は、一般ユーザー、イシュアー、アクワイアラー、加盟店、決済代行会社（PSP）などクレジットカードの関係者が非常に増えてきて、どこに、どのような対策をすれば効果的なのかが非常に難しいところである。こうしたクレジットカード情報の悪用の１事例として、不正トラベルの手口を把握したが、これは窃取したクレジットカード情報を悪用して、旅行・宿泊の料金を騙し取るというものである（図 24 参照）。



〈図 24 窃取したクレジットカード情報悪用の手口～不正トラベル〉

国外の場合が多いが、通常の旅行代理店よりも安く航空券・ホテル等が予約できると宣伝して旅行者を募り、旅行させる。実際上、犯人側は情報を窃取した他人のクレジットカードで決済をしているので、旅行者から受け取る代金分が丸々もうけになるという状況になる。

JC3 では、会員企業からこのような手口が発生して困っているという話を聞き、プロジェクトの場を設けて情報共有、実態解明、広報啓発を行うとともに、警察において取締りをしていただくなど、総合的な対策を講じている（図 25 参照）。現在、コロナの影響でインバウンドが減少しているため顕著な被害は生じていないが、回復した際にはこのような犯罪が再び増えないか、現在、注視している状況である。



〈図 25 不正トラベル排除に向けた総合対策～実態解明・広報啓発・取締り〉

8　暗号資産に関連する違法行為

暗号資産については、最近マネロンの手段としていろいろ使われているのではないかという懸念が示されている（図 26 参照）。犯罪収益移転防止法に基づく「疑わしい取引の届出」の件数も近年増加しており、暗号資産の関係も最近注意を要することから、情報共有の場を設け、分析を行い、あるいは法執行機関向けのトレーニングをやっていきたいと考え、取組をある程度進め始めている（図 27、28 参照）。

〈図 26 暗号資産に関連する違法行為〉

区分	平成28年 件数	平成29年 件数	平成30年 件数	令和元年 件数	令和2年 件数
金融機関等	367,399	384,331	401,155	415,299	402,868
預金取扱機関	369,936	363,347	363,380	366,973	342,226
銀行等	354,346	346,595	346,014	344,523	319,812
信用金庫・信用協同組合	13,070	13,259	14,375	19,487	19,793
労働金庫	453	476	467	371	300
農林等	2,067	3,017	2,524	2,592	2,321
保険会社	2,310	2,382	2,671	2,976	2,635
金融商品取引業者	8,528	8,436	13,345	17,116	17,933
貸金業者	5,263	7,512	12,396	17,316	25,255
資金決済業者	530	1,782	1,801	3,013	6,036
暗号資産交換業者		669	7,096	5,996	8,023
商品先物取引業者	16	17	50	256	320
両替業者	627	490	649	712	252
電子債権記録機関	3	4	10	4	5
その他	177	192	167	137	179
ファイナンスリース事業者	214	109	222	270	123
クレジットカード事業者	13,436	15,448	15,114	24,691	29,138
宅地建物取引業者	8	7	8	6	7
宝石・貴金属等取扱事業者	27	146	952	217	63
郵便物受取サービス業者	6	2	6	4	2
電話受付代行業者	1	0	0	0	0
電話転送サービス事業者	0	0	0	5	1
合計	401,091	400,043	417,465	440,492	432,202

注：暗号資産交換業者の件数は、特定事業者に規定された平成29年4月以降の届出受理件数である。

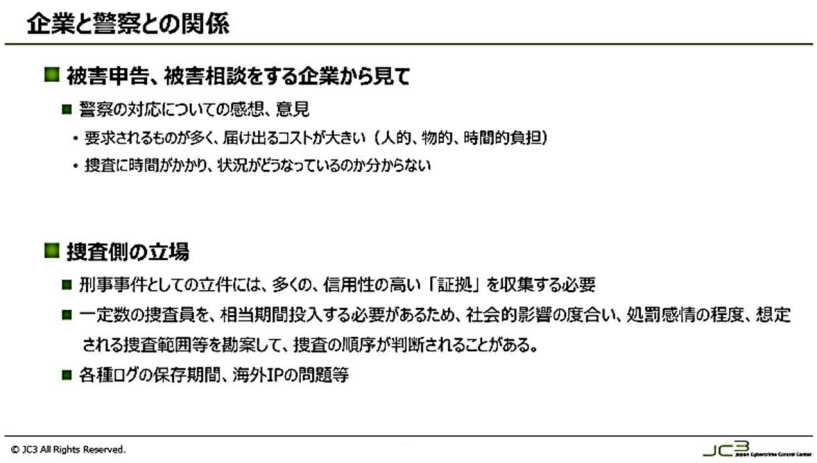
注）警察庁発表資料

〈図 27 暗号資産に関する現況〉

〈図 28 暗号資産関連の主な取組〉

9　企業と警察との関係

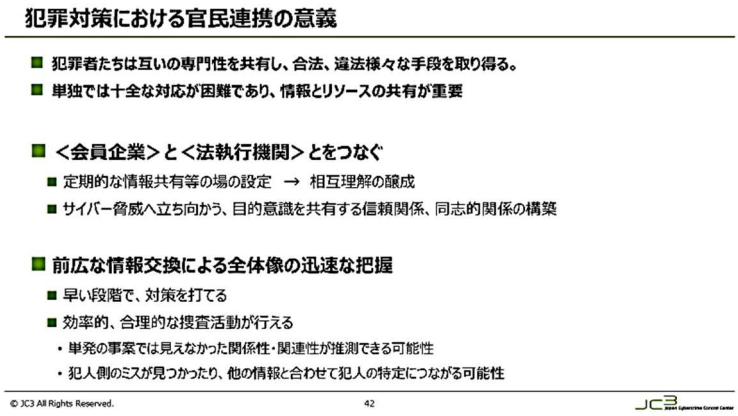
JC3 においては、企業と警察とのハブの役割を果たしていきたいと考えているが、被害に遭い被害申告をする企業の方の立場、そして捜査側の立場と、様々な意見、考え方がある。（図 29 参照）犯罪者たちは互いの専門性を共有して、合法なものも含め違法な手段もとり得るわけで、守る側単独での対応は困難であるから、官民連携の意義としていて、情報とリソースの共有が重要と考えている（図 30 参照）。



〈図 29 企業と警察との関係〉

そのような意味で、会員企業と法執行機関とをつなぐべく定期的な情報共有の場を設定していることにより、相互理解の醸成にもなるし、また、そのような機会を通じて、サイバー脅威へ立ち向かうこと、つまり犯罪者をしっかりと取り締まらなければいけないという目的意識を共有する信頼関係が構築できることを期待している。

また、前広な情報交換により事案の全体像が迅速に把握できれば、早い段階で効果的な対策が打てるし、効率的・合理的な捜査活動が行えるのではないかと考えている。



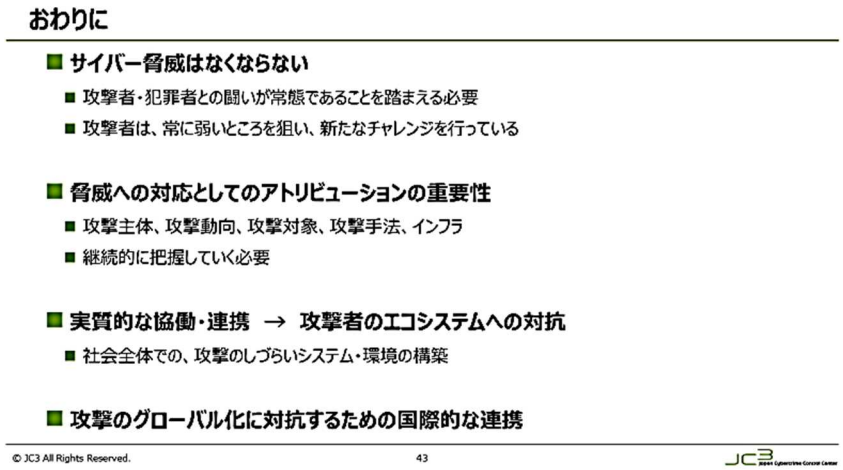
〈図 30 犯罪対策における官民連携の意義〉

10　おわりに

デジタル化が非常に進んだ結果、こうしたサイバー脅威は、残念ながらなくならないことから、これからは攻撃者・犯罪者との闘いが常態であることを踏まえる必要がある。犯人側は、常に弱いところを狙って、新たなチャレンジを仕掛けてくる。そうした手口や攻撃手法について継続的に把握していく必要があると考えている。

攻撃者のほうでは、先ほど申し上げたようなエコシステムができているので、守る私たちの側でも実質的な協働・連携を図り、社会全体で攻撃のしづらいシステム・環境を構築していく必要がある。

JC3 がモデルにしたアメリカの NCFTA のような官民連携組織も各国にできてきているので、攻撃のグローバル化に対抗するための国際的な連携を図っていきたいと考えている。皆様方それぞれの御協力が非常に貴重なものとなってくるので、JC3 の活動について御理解と御支援をいただければ幸いである。



〈図 31 おわりに〉