サイバー事案の
被害の潜在化防止に向けた検討会
報告書　2023

令和5年3月
警察庁サイバー警察局

「サイバー事案の被害の潜在化防止に向けた検討会」報告書

目　次

はじめに

サイバーパンク小説の嚆矢とされる「ニューロマンサー」において「電脳世界（サイバースペース）」の概念が描かれてから、40 年近くが経過しようとしている。一昔前までは遠い夢物語のように感じていたが、ここ最近のメタバース等をめぐる動向は、映画や小説の中で描かれる「電脳世界」の住人として過ごす未来の到来を予感させるには、十分なもののように思う。

かように近年のデジタル化の進展は著しいものがある。

コンビニの支払いはスマホ一つで完結し、レストランや飲み会の予約、会議の開催はオンラインで行われることが浸透しつつある。我々が普段意識することのないバックエンドでは、クラウドサービスが広く利用され、様々なシステムにＡＩ技術が採用されてきており、これまで人間が膨大なリソースや時間を費やしても実現が困難であったものなどが手軽に利用できるようになりつつある。

サイバー空間は、量的に拡大し質的に深化するとともに、実空間との融合が進み、「公共空間」としての外縁を着実にそして驚くべき速さで広げている。同時に、ひとたびサイバー事案が発生すると、社会経済活動に多大な影響を及ぼしかねないことは周知のとおりである。インターネットで検索すれば、毎日のようにサイバー事案のニュースが目に飛び込んでくる。ランサムウェア感染被害の件数は右肩上がりで増加し、個人情報・機密情報の流出やインターネットバンキングに係る不正送金等のサイバー事案の例は枚挙にいとまがない。

様々な主体が参画し、公共空間化が進むサイバー空間においては、各主体の関係が複雑に絡み合い、一部の被害が予想外の形で広範囲に波及する危険がある。これに的確に対処するためには、犯人を検挙して犯行の制圧を迅速に行い、また、被害拡大の阻止と被害の未然防止により、可能な限り「潜在的な被害者」を現実の被害者にしないようにすることが重要である。この点、警察が有する犯罪を捜査する機能と犯罪を予防する機能に対する国民の期待・要請は大きい。

警察においては、従来、被害の届出により実態把握のための情報を収集していたが、被害者が刑事処分を望むとは限らず、被害に遭ったことへの引け目や被害者に対する社会的評価の悪化（レピュテーションリスク）の懸念から被害申告をためらうなど、現実の被害が潜在化している状況がうかがわれる。また、サイバー空間においては匿名性が悪用され、サイバー事案の中には国家の関与が疑われるものもあるなど、犯行が組織化され手法が洗練されてきていることから、被害自体の認知や事件捜査が一層困難なものになってきている。このことから、個々の事案から得られる情報が断片的なものにとどまるとしても、それらを幅広く集め、総合的に分析・検討することで実態を把握し、取締りと対策を効果的に進める必要がある。

こうした観点から、警察への通報・相談をより一層促進し、被害者等からの情報を広範に収集する必要があるが、そのためには、警察の情報収集能力を強化するとともに、被害者の被害拡大防止や被害回復に貢献することや、犯罪手口や未然防止対策に関する情報を社会に速やかに還元するなどの活動を充実させ、それにより、被害の通報・相談が自ずと行われる社会的な気運を醸成していくことが重要である。その前提として、警察においても、通報・相談に係る負担を軽減することや、通報・相談に対して適切に対応する必要があることは言うまでもない。

そうしたところ、サイバー警察局が令和４年４月に警察庁に設置された。実に 28 年振りの局の新設である。サイバー空間に山積する課題に対し、関係機関等との連携強化を含め、一元的かつ強力に対処する体制が備わることとなった。もちろん、対策を進める中で被害の潜在化防止もその射程の一つである。

そこで、警察庁では、サイバー事案に関する被害の潜在化の防止を目的として、関係機関等と連携した情報共有や被害者が自発的に通報・相談しやすい環境の整備等に関して、効果的な方策を多様な観点から議論するため、「サイバー事案の被害の潜在化防止に向けた検討会」を令和４年 12 月から令和５年３月までに計３回開催し、各分野の有識者による幅広い視座からの議論を重ねてきた。

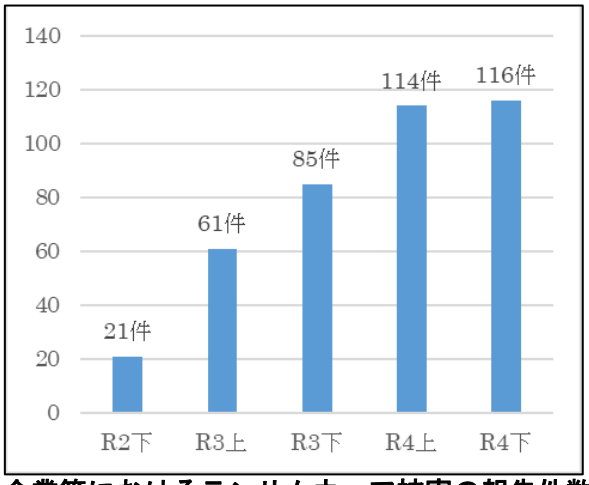
本報告書はその結果を取りまとめたものである。

１　サイバー空間における情勢認識

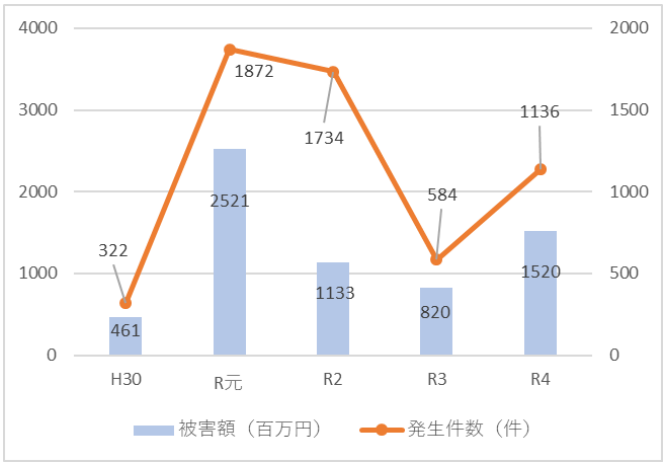
サイバー空間の情勢は、ランサムウェアによる被害が広範に及んでいるほか、国家を背景に持つ集団によるサイバー攻撃も確認されているなど、極めて深刻な情勢が続いている。

令和５年２月に警察庁が公表した「令和４年の犯罪情勢」によると、令和４年中に警察庁に報告されたランサムウェアによる被害件数は 230 件と、前年比で 57.5%増加し、ＶＰＮ機器やリモートデスクトップ等のテレワークにも利用される機器等のぜい弱性を狙われたケースが大半を占めている。その被害は企業・団体等の規模やその業種を問わず広範に及んでおり、一時的に業務停止に陥る事態も発生している。

また、インターネットバンキングに係る不正送金事犯について、令和４年は発生件数が 1,136 件、被害総額は約 15 億円と、いずれも３年ぶりに前年比増加となった（それぞれ前年比で 94.5%、85.4%増加。）。その被害の多くがフィッシングによるものとみられており、金融機関を装ったフィッシングサイト（偽のログインサイト）へ誘導する電子メールが多数確認されている。



企業等におけるランサムウェア被害の報告件数



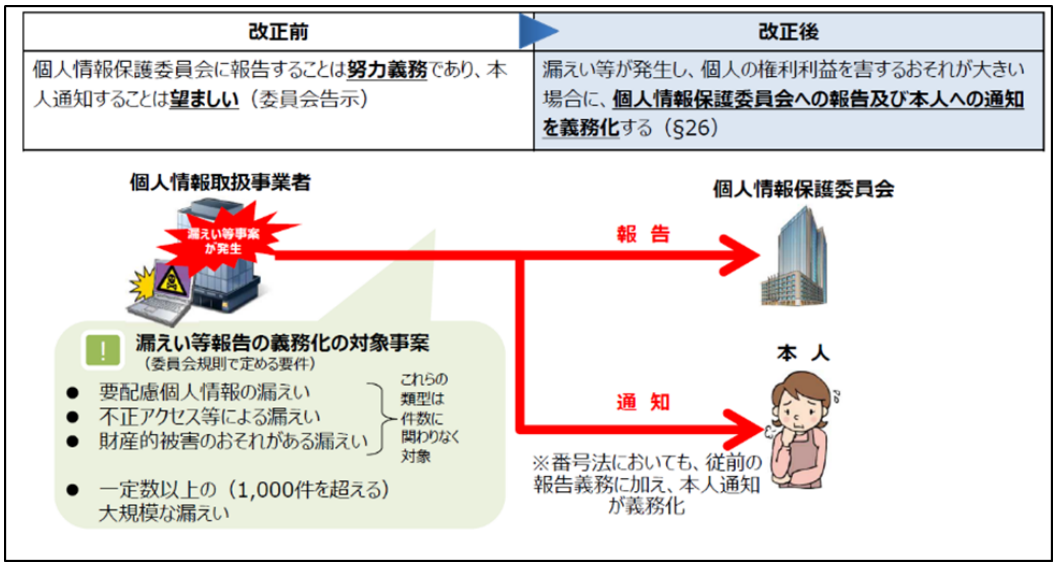
インターネットバンキングに係る不正送金事犯

さらに、特に深刻な被害等が及んでいる分野に焦点を当てると、概ね次のとおりである。

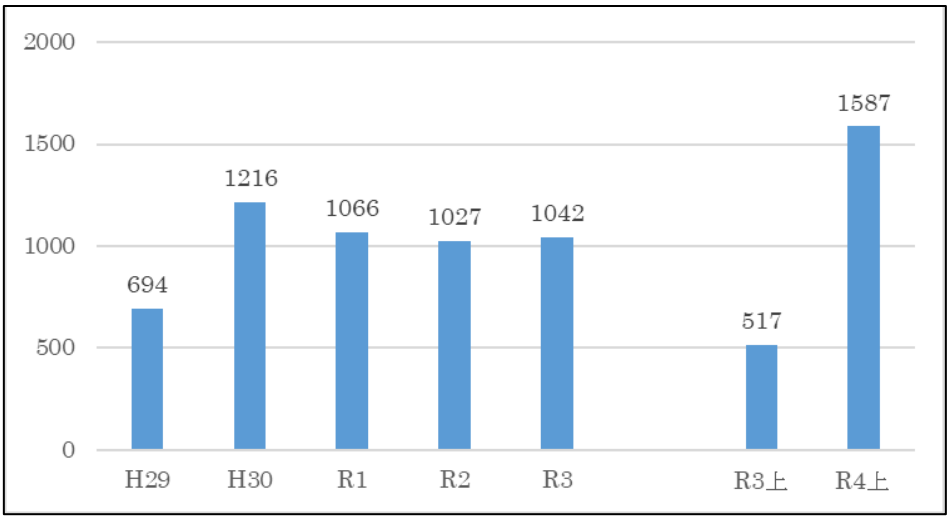
１．１　個人情報の漏えい等の被害

令和２年に改正された個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）の令和４年４月の全面施行により、従前、努力義務であった個人情報の漏えい等事案の発生時における個人情報保護委員会への報告について、一定の要件を満たすものに係る同委員会への報告及び本人への通知が義務化された。これに伴い、令和４年度上半期に個人情報保護委員会に報告された個人データの漏えい等事案は、1,587 件と前年度同期の報告件数（517 件）と比較して件数が増加しており、このうち、不正アクセス等による漏えい事案については、報告件数全体に占める割合こそ大きくないものの、１件当たり

の漏えいの規模が 1,000 人を超えるものが多く確認されるなど、深刻な被害が生じている状況である。



漏えい等報告の義務化

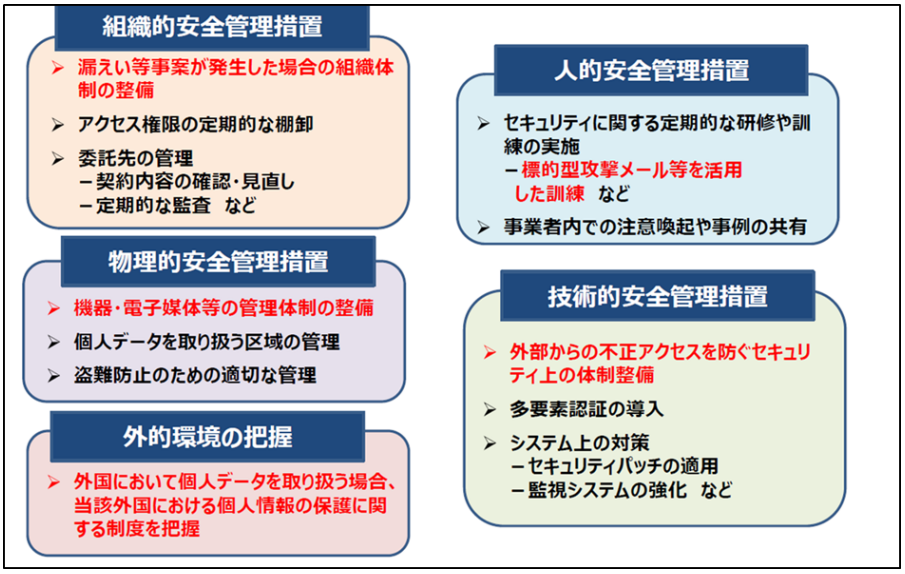


漏えい等事案に関する報告の受付件数

個人データの取扱いに当たっては、個人情報保護法において、個人情報取扱事業者は「個人データの安全管理のために必要かつ適切な措置を講じなければならない」と定められており、具体的に講じるべき措置として、「組織的安全管理措置」、「人的安全管理措置」、「物理的安全管理措置」、「技術的安全管理措置」、「外的環境の把握」が「個人情報の保護に関する法律についてのガイドライン（通則編）」において示されている。個人情報保護委員会では、個人情報等の取扱いに関する監視・監督を行う中で、漏えい等事案の報告を受けた場合には、事実関係及び再発防止策の確認等を行い、必要に応じて指導等を行っている。

また、「個人情報の保護に関する基本方針」（平成 16 年４月２日閣議決定、令和４年４月１日一部変更）において、「サイバーセキュリティ対策の観点から、個人情報保護委員会は、

各主体が取り扱う保有個人データや個人データの外部からの不正アクセスやランサムウェア等のサイバー攻撃等による漏えい等の未然防止や被害の拡大防止等のリスクの低減、漏えい等事態への適切かつ迅速な対応を図るため、ＮＩＳＣ等の関係省庁等及びサイバーセキュリティ関係機関と緊密に連携する」と定められている。これを踏まえ、令和４年 12 月に開催された「個人情報保護法サイバーセキュリティ連携会議」において、各省庁・機関が持つ報告等の枠組みを活用して双方の報告等制度の更なる促進を図ることの重要性について認識が共有された。

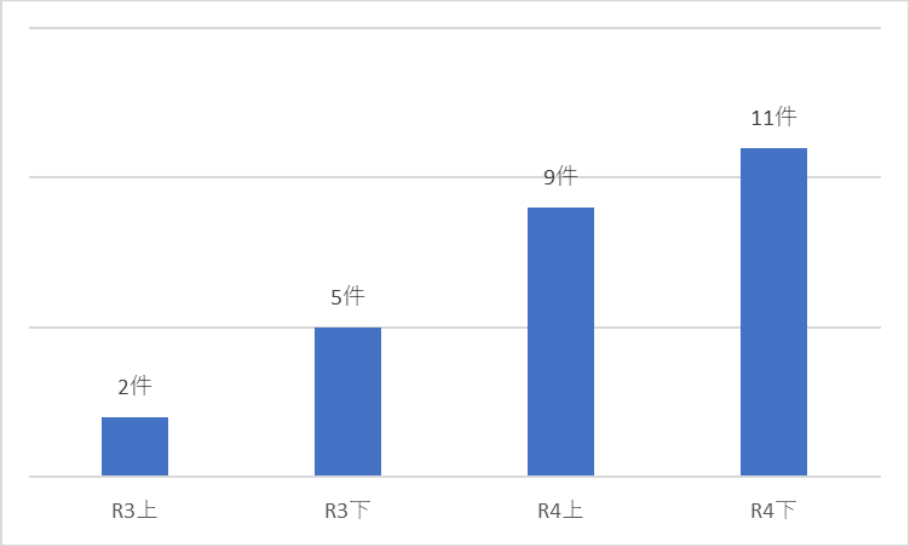


安全管理措置

１．２　医療分野におけるサイバー事案被害

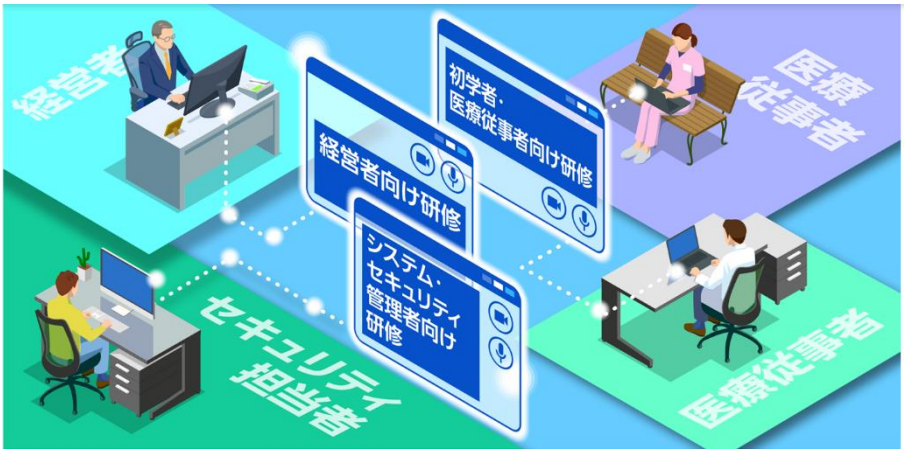
本検討会における警察庁の発表によると、警察庁に報告された医療・福祉分野におけるランサムウェアによる被害件数は増加傾向にあり、データが暗号化されることによって電子カルテシステムが使用不能となり、新規外来患者の受け入れを停止するなどの被害が生じている。

具体の事例について、厚生労働省の発表によると、令和４年 10 月、大阪府立病院機構の大阪急性期・総合医療センターにおいて、センター内の調理を委託していた給食事業者のシステムを経由してランサムウェアに感染する被害が生じた。これにより、同センターでは新規外来患者の受入れを一時停止するとともに、緊急性が高くない入院患者の一度自宅退院、周辺病院への転院を進めることとなった。結果的に患者の生命等への影響はなかったものの、地域医療に深刻な影響が生じた。



医療・福祉分野におけるランサムウェア被害件数

厚生労働省においては、こうした状況を踏まえ、「医療情報システムの安全管理に関するガイドライン」の改定を進めるとともに、ぜい弱性が指摘されている機器・ソフトウェアの確実なアップデートの働きかけ、医療分野におけるサイバーセキュリティに関する情報共有体制（ISAC）の構築等に向けた取組等のほか、厚生労働省委託事業において、「医療機関向けセキュリティ教育支援ポータルサイト(MIST:Medical Information Security Training)」等による医療機関向けサイバーセキュリティ対策研修の充実や被害発生時の初動対応の支援（駆けつけ機能の確保）等により、医療情報システムのサイバーセキュリティの強化を推進している。

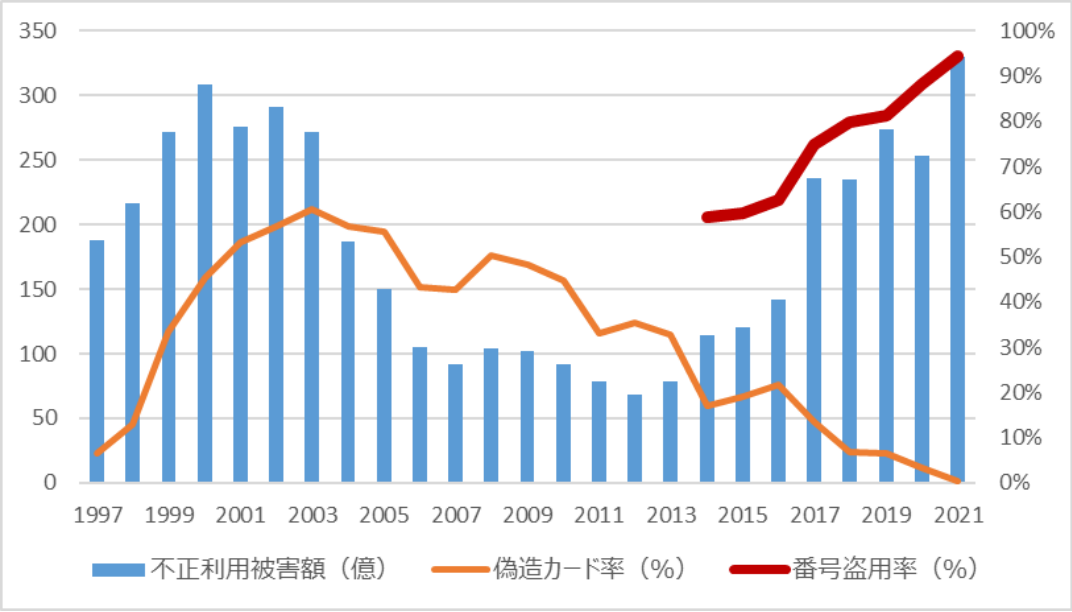


医療機関向けセキュリティ教育支援ポータルサイト（MIST）のイメージ

１．３　クレジットカード決済におけるサイバー事案被害

社会のデジタル化・新型コロナウイルス感染症の被害拡大を受けた巣ごもり需要の拡大等により、令和３年のＥＣの市場規模は約 21 兆円にまで拡大し、これに伴いＥＣサイトでの非対面取引における主要な決済手段としてクレジットカードが利用される機会が増加している。民間最終消費支出に占めるキャッシュレス決済比率は令和３年には 32.5%に達し、クレジットカードの取引はそのうち約９割を占めているところ、今後も引き続き増加すると見込まれている。

一方で、ＥＣ加盟店やクレジットカードの決済代行会社等が標的となったサイバー事案だけでなく、消費者が標的となったフィッシング被害により、令和３年にはクレジットカードの不正利用被害額は約 330 億円と過去最高となっている。このうち、クレジットカードの番号盗用の割合が約 94%を占め、非対面取引でクレジットカード番号等を窃取したなりすましによる不正利用が主要な要因となっている。これらの不正利用の対象となっているクレジットカード番号等は、関係事業者からの漏えいだけでなく、クレジットカード決済処理の仕組みを悪用しクレジットカード番号等を割り出すクレジットマスター、ＳＭＳ等を通じて利用者からクレジット情報等をだまし取るフィッシングにより詐取されているとみられている。また、クレジットカード決済機能の分化により多様な主体がクレジットカード決済網に関与しているため、ＥＣ加盟店、ＥＣシステム提供者、決済代行業者、消費者等、多様な主体に対するサイバー攻撃のリスクが存在している。

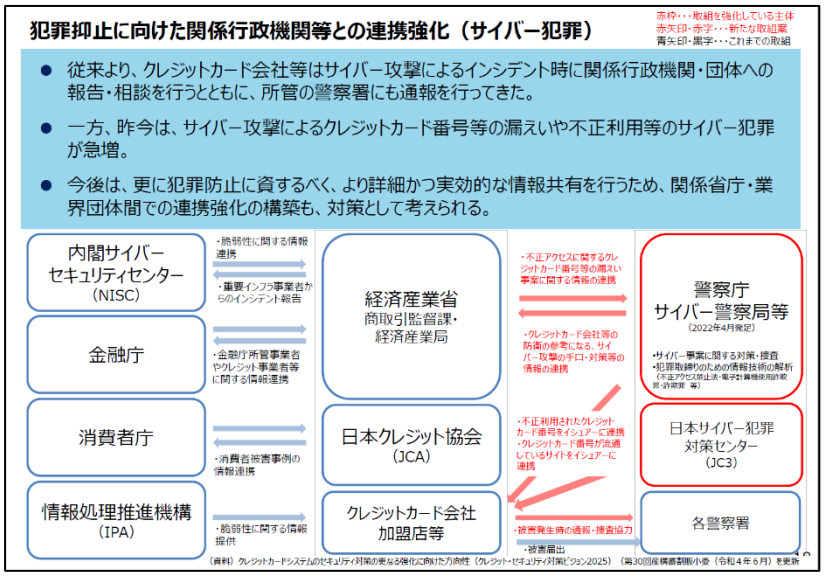


国内発行クレジットカードにおける年間不正利用被害額

（出典：日本クレジット協会（令和４年３月））

経済産業省においては、クレジットカード決済システムの信頼性を確保すべく、割賦販売法（昭和 36 年法律第 159 号）に基づくクレジットカード番号等の適切管理や加盟店での不正利用防止を義務付けている。

特に非対面取引での安全・安心なクレジットカード決済を確保するため、令和４年８月に有識者会議「クレジットカード決済システムのセキュリティ対策強化検討会」を立ち上げ（警察庁はオブザーバ参加）、①　クレジットカード番号等を安全に管理する（漏えい防止）、②クレジットカード番号等を不正に利用させない（不正利用防止）、③　クレジットの安全・安心な利用に関する周知・犯罪の抑止、の３本柱に沿って、当該検討会での議論を踏まえ、クレジットカード決済システムのセキュリティ対策強化に向けた具体的な取組と今後の課題について、令和５年１月に報告書を取りまとめている。



経済産業省における警察等との連携強化

（出典：第４回「クレジットカード決済システムのセキュリティ対策強化検討会」資料から抜粋）

今後、デジタル化の更なる進展により新たなサービスが次々と生み出され、社会に展開されていくと予想されることに伴い、複数のデジタルサービスの連携の間隙を突いた犯罪や、技術革新の恩恵を攻撃側が悪用する犯罪等の発生が懸念される。また、クラウドサービスの利用拡大、産業分野でのＡＩやＩｏＴ機器の利用拡大等により、サイバー事案が経済社会活動等に与える影響も、より広範により重篤に及ぶようになり、被害が発生した際の影響を予見したり、発生原因を特定したりすることが困難になると懸念される。

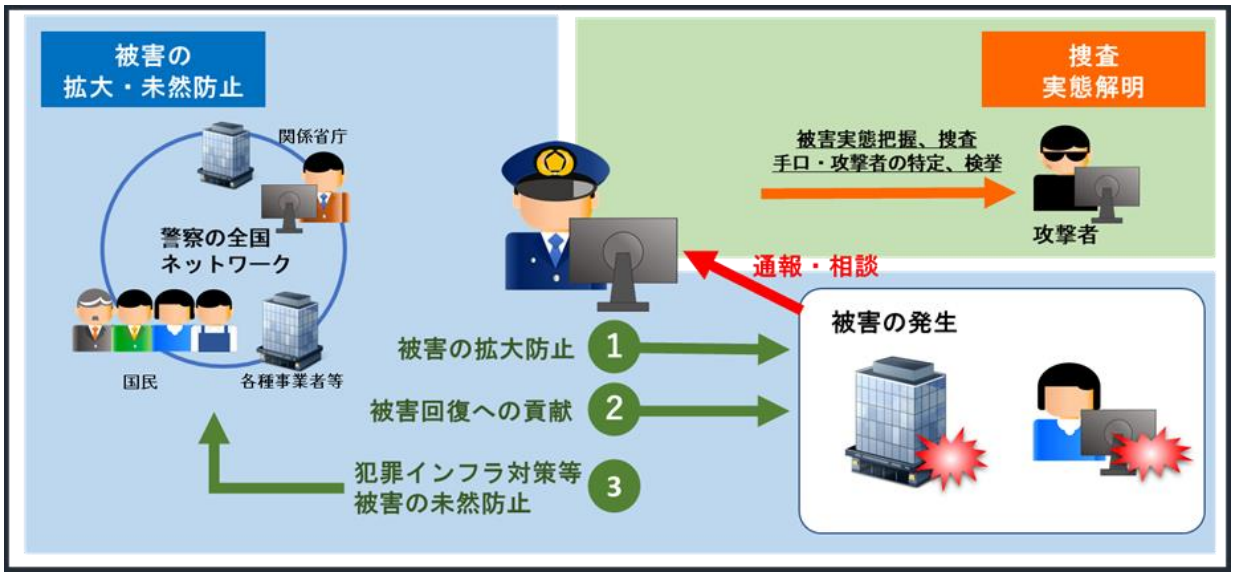
サイバー空間の脅威は、今後、より一層深刻なものになっていくことが予想される。

２　被害の潜在化

２．１　通報・相談の重要性

１で述べた深刻化する情勢においてもなお、サイバー空間の安全・安心を確保するためには、サイバー事案が発生した場合に、被疑者の検挙に向けた捜査を行うことに加え被害者や被害企業等における被害の拡大防止や被害回復、社会全体の被害の未然防止対策を推進することが必要不可欠である。

こうした観点から、警察では、サイバー事案を把握した場合は、捜査のみならず攻撃者・犯行手口等の実態解明や被害防止対策・未然防止対策等、様々な取組を行っている。



サイバー事案発生時における警察の取組概要

被害の未然防止対策については、例えば、令和４年８月下旬から９月にかけてインターネットバンキングに係る不正送金被害が急増した際には、警察庁において、通報・相談により把握した情報を基に不正送金被害の手口等を分析し、令和４年９月に警察庁ウェブサイトにおいて注意喚起を行っている。また、同月、金融庁と連携し、業界団体等を通じて金融機関に対しフィッシング対策の強化を要請している。

また、サイバー攻撃を受けたコンピュータやサイバー攻撃に使用された不正プログラムの解析結果や犯罪捜査の過程で得た情報等を総合的に分析し、攻撃者及び手口に関する実態解明に努めているところ、これらの情報等は、サイバー攻撃の攻撃者を公表し、非難することでサイバー攻撃を抑止する、いわゆるパブリック・アトリビューション等にも活用されている。令和４年 10 月には、金融庁、内閣サイバーセキュリティセンターと連名で、北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループによる暗号資産関連事業者等を標的としたサイバー攻撃について、具体的な攻撃の手口、リスク低減のための対処例を示すなどの注意喚起を行っているほか、12 月には、我が国として同グループを外国為

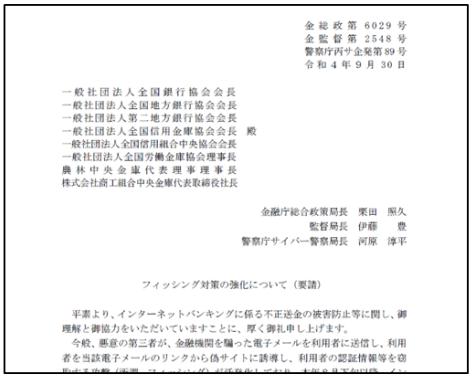
替及び外国貿易法（昭和 24 年法律第 228 号）に基づく資産凍結等の対象として指定している。

さらに、サイバー攻撃の攻撃者等を特定するに至らず、パブリック・アトリビューションを実施できない事案についても、事業者等からの通報・相談を基に捜査・実態解明を実施し、関係省庁と連携して広く手口や対策方法を公表し、注意喚起を行うことで、被害の未然防止・拡大防止を図っている。例えば、令和４年 11 月 30 日には、内閣サイバーセキュリティセンターと連名で、学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について、注意喚起文を発出している。

① 警察庁においてネットバンクの不正送金事案に係る通報の増加を把握
- ８月中　　：被害件数　70件、被害額　２億1,300万円
- ９月15日まで：被害件数　184件、被害額　１億6,900万円（いずれも９月15日現在の暫定値）

② 金融庁、関係団体、被害金融機関と被害状況を共有し、拡大防止対策等を推進
- 警察庁ウェブサイトにおいて注意喚起を実施　（令和４年９月22日）
- 金融庁と連名で関係団体にフィッシング対策の強化を要請（令和４年９月30日）

③ 被害件数、被害額ともに減少（令和４年10月28日現在の暫定値）
被害件数：８月（77件）　→　９月（384件）　→　10月（81件）
被害金額：８月（２.３億円）　→　９月（３.３億円）　→　10月（１.１億円）


金総政第 6029 号
金監督第 2548 号
警察庁丙サ企発第 89 号
令和４年９月 30 日

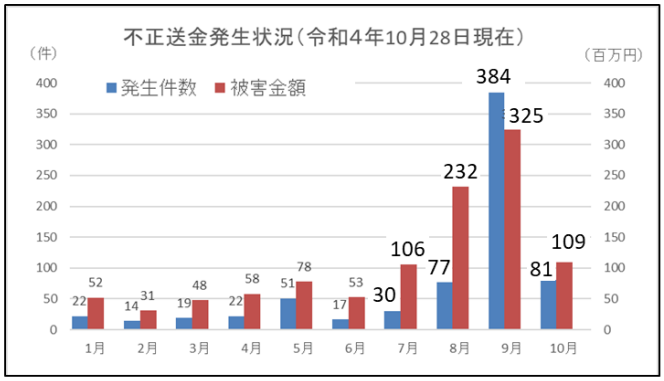
一般社団法人全国銀行協会会長
一般社団法人全国地方銀行協会会長
一般社団法人第二地方銀行協会会長
一般社団法人全国信用金庫協会会長　殿
一般社団法人全国信用組合中央協会会長
一般社団法人全国労働金庫協会理事長
農林中央金庫代表理事理事長
株式会社商工組合中央金庫代表取締役社長

金融庁総合政策局長　栗田　照久
監督局長　伊藤　豊
警察庁サイバー警察局長　河原　淳平

フィッシング対策の強化について（要請）

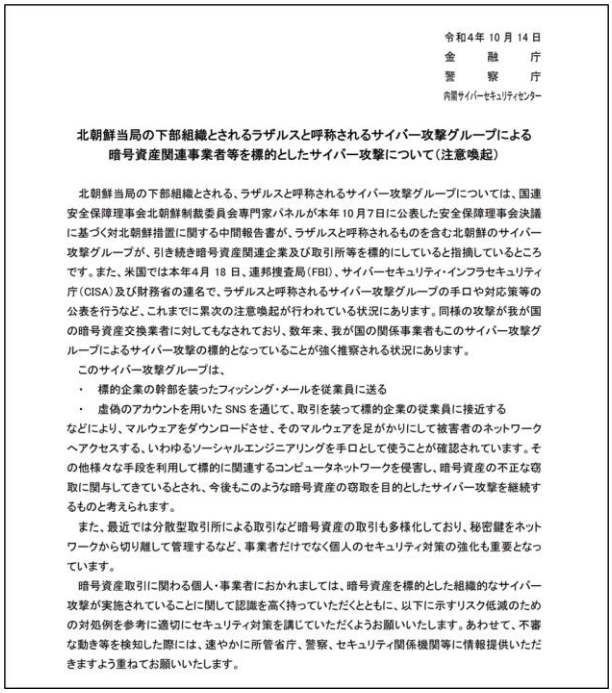
平素より、インターネットバンキングに係る不正送金の被害防止等に関し、御理解と御協力をいただいていますことに、厚く御礼申し上げます。
今般、悪意の第三者が、金融機関を騙った電子メールを利用者に送信し、利用者を当該電子メールのリンクから偽サイトに誘導し、利用者の認証情報等を窃

【フィッシング対策の強化要請】



【被害件数、被害額の減少】（警察庁作成）

ネットバンクの不正送金事案に関する注意喚起等



令和4年 10 月 14 日
金　融　庁
警　察　庁
内閣サイバーセキュリティセンター

北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループによる暗号資産関連事業者等を標的としたサイバー攻撃について（注意喚起）

北朝鮮当局の下部組織とされる、ラザルスと呼称されるサイバー攻撃グループについては、国連安全保障理事会北朝鮮制裁委員会専門家パネルが本年 10 月7日に公表した安全保障理事会決議に基づく対北朝鮮措置に関する中間報告書が、ラザルスと呼称されるものを含む北朝鮮のサイバー攻撃グループが、引き続き暗号資産関連企業及び取引所等を標的にしていると指摘しているところです。また、米国では本年4月 18 日、連邦捜査局（FBI）、サイバーセキュリティ・インフラセキュリティ庁（CISA）及び財務省の連名で、ラザルスと呼称されるサイバー攻撃グループの手口や対応策等の公表を行うなど、これまでに累次の注意喚起が行われている状況にあります。同様の攻撃が我が国の暗号資産交換業者に対してもなされており、数年来、我が国の関係事業者もこのサイバー攻撃グループによるサイバー攻撃の標的となっていることが強く推察される状況にあります。

このサイバー攻撃グループは、

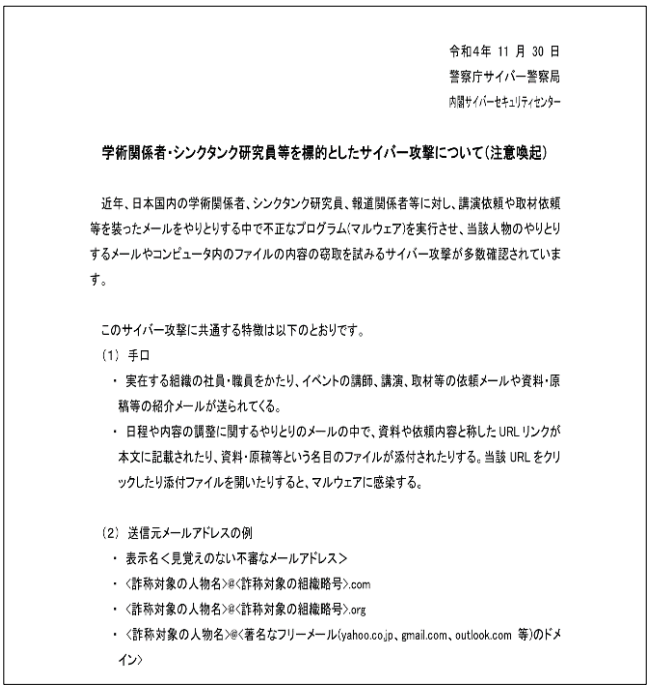
・　標的企業の幹部を装ったフィッシング・メールを従業員に送る
・　虚偽のアカウントを用いた SNS を通じて、取引を装って標的企業の従業員に接近する

などにより、マルウェアをダウンロードさせ、そのマルウェアを足がかりにして被害者のネットワークへアクセスする、いわゆるソーシャルエンジニアリングを手口として使うことが確認されています。その他様々な手段を利用して標的に関連するコンピュータネットワークを侵害し、暗号資産の不正な窃取に関与してきているとされ、今後もこのような暗号資産の窃取を目的としたサイバー攻撃を継続するものと考えられます。

また、最近では分散型取引所による取引など暗号資産の取引も多様化しており、秘密鍵をネットワークから切り離して管理するなど、事業者だけでなく個人のセキュリティ対策の強化も重要となっています。

暗号資産取引に関わる個人・事業者におかれましては、暗号資産を標的とした組織的なサイバー攻撃が実施されていることに関して認識を高く持っていただくとともに、以下に示すリスク低減のための対処例を参考に適切にセキュリティ対策を講じていただくようお願いいたします。あわせて、不審な動き等を検知した際には、速やかに所管省庁、警察、セキュリティ関係機関等に情報提供いただきますよう重ねてお願いいたします。

パブリック・アトリビューション



令和4年 11 月 30 日
警察庁サイバー警察局
内閣サイバーセキュリティセンター

学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について（注意喚起）

近年、日本国内の学術関係者、シンクタンク研究員、報道関係者等に対し、講演依頼や取材依頼等を装ったメールをやりとりする中で不正なプログラム（マルウェア）を実行させ、当該人物のやりとりするメールやコンピュータ内のファイルの内容の窃取を試みるサイバー攻撃が多数確認されています。

このサイバー攻撃に共通する特徴は以下のとおりです。

（1） 手口

・ 実在する組織の社員・職員をかたり、イベントの講師、講演、取材等の依頼メールや資料・原稿等の紹介メールが送られてくる。
・ 日程や内容の調整に関するやりとりのメールの中で、資料や依頼内容と称した URL リンクが本文に記載されたり、資料・原稿等という名目のファイルが添付されたりする。当該 URL をクリックしたり添付ファイルを開いたりすると、マルウェアに感染する。

（2） 送信元メールアドレスの例

・ 表示名く見覚えのない不審なメールアドレス＞
・ ＜詐称対象の人物名＞@＜詐称対象の組織略号＞.com
・ ＜詐称対象の人物名＞@＜詐称対象の組織略号＞.org
・ ＜詐称対象の人物名＞@＜著名なフリーメール（yahoo.co.jp、gmail.com、outlook.com 等）のドメイン＞

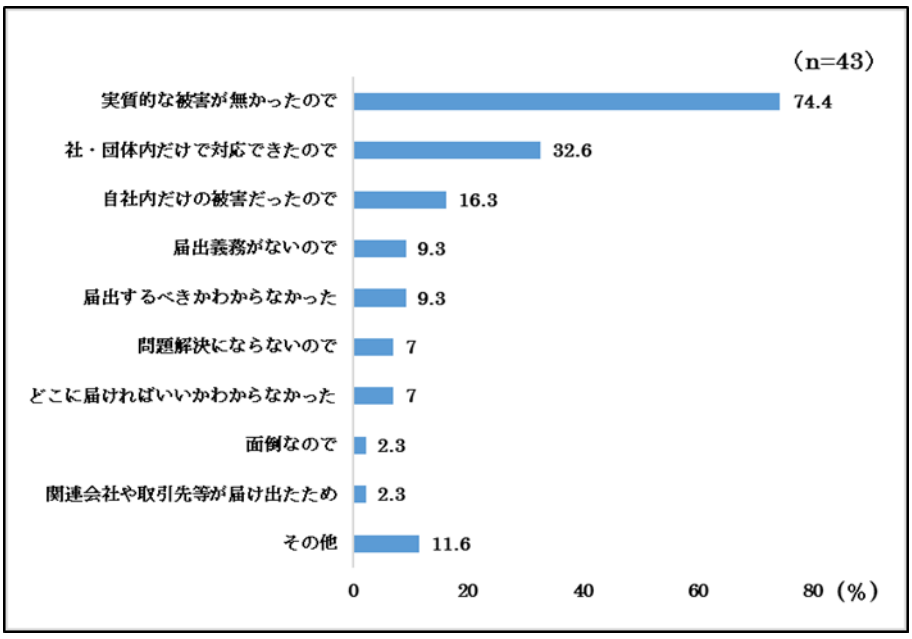
注意喚起文の一部

このように、警察では、サイバー事案の捜査のみならず、攻撃者・犯行手口等の実態解明、被害の拡大防止・未然防止対策に取り組んでいるところであるが、これらは主に国民・企業等からの通報・相談によって得られた情報を端緒として実施しているものであり、通報・相談が警察の活動において重要かつ代替できない役割を担っている。

２．２　被害の潜在化

ところが、サイバー事案においては、被害者側におけるレピュテーションリスクや、早期復旧に支障が及ぶことなどへの懸念、届出するべきなのか分からないなどの理由から、被害者からの通報・相談がためらわれる傾向があり、いわゆる「被害の潜在化」が課題となっている。

警察庁が令和４年に実施した「不正アクセス行為対策等の実態調査」において、過去１年間に不正アクセス等の被害に遭った行政機関や企業等に対して、届出先機関を調査したところ、「届け出なかった」が最も多く 43.9％を占めていた。また、このうち、届出を躊躇させる要因（複数回答）については、「実質的な被害が無かった」との回答が 74.4％、「社・団体内で対応できた」との回答が 32.6％であった。



届出を躊躇させる要因

通報・相談が適切に対応されていない要因には、

○　届出する必要があるかわからない

○　どこに届ければよいかわからない（通報すべき窓口がわからない）

など、犯罪の態様や通報・相談に関する情報不足によるものが見受けられるほか、ランサムウェアの被害者に対して警察が実施したアンケートにおいて、「復旧作業等に対応する中で、捜査協力としてどのような対応を求められるかわからない」、「被害に関する情報が外部に伝わってしまう懸念がある」等の捜査協力に関して不安がある旨の意見も見受けられた。

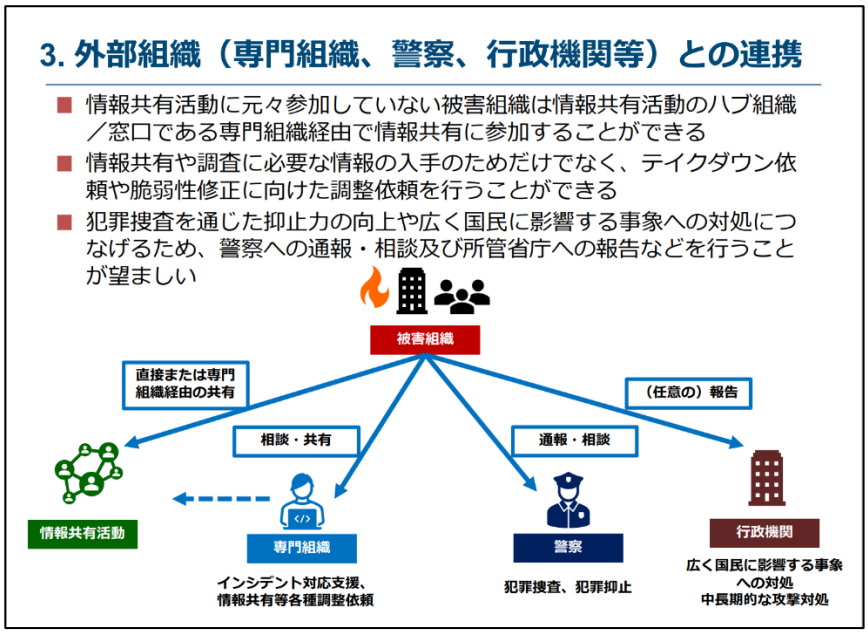
また、個人の被害者に目を向けると、高齢者や青少年が被害に遭った際に、そもそも被害に遭ったことを認識していないことや、犯罪に関する知識不足や家族に相談しにくい内容などにより、被害の通報・相談がなされていない状況がうかがわれる。

さらに、警察への通報・相談がなされた際、警察の受理体制の不足や対応者の知識不足等により、適切な対応・処理がなされていない状況も発生している。暗号資産やＮＦＴ（Non-Fungible Token；非代替性トークン）等のいわゆるデジタル資産をはじめとした新たな情報通信技術に関する知識不足・理解不足は、その一因であろう。

なお、被害の潜在化は、「サイバーセキュリティ戦略」（令和３年９月 28 日閣議決定）においても、「サイバー犯罪に関する警察への通報や公的機関への連絡の促進によって、サイバー犯罪の温床となっている要素・環境の改善を図る」とされているなど、警察のみならず政府・社会全体として取り組むべき課題とされている。

また、攻撃を受けた被害組織がサイバーセキュリティ関係組織と被害に係る情報を共有するための取組として、官民の多様な主体が連携する協議体である「サイバーセキュリティ協

議会」の運営委員会の下に、「サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会」を開催し、被害組織が被害情報を共有する際の実務上の参考となるガイダンス（サイバー攻撃被害に係る情報の共有・公表ガイダンス）が策定された。当該検討では、警察庁も事務局として参画しており、被害発生時における警察への通報・相談の必要性やその意義について活発な議論等が行われたところである。



「サイバー攻撃被害に係る情報の共有・公表 ガイダンス（案）の概要」から抜粋

（リンク先：https://www.nisc.go.jp/policy/group/kihon-2/pubcom-guidance2022.html）

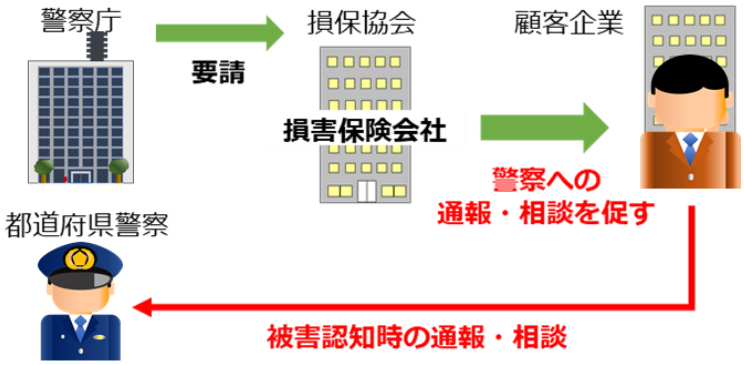
２．３　被害の潜在化に対する現状の取組

警察においては、２．２で述べた状況を踏まえ、これまでも被害の潜在化防止に向けた対策を講じてきたところである。

具体的には、サイバー事案の標的となるおそれのある重要インフラ事業者等で構成されるサイバーテロ対策協議会や、企業等との共同対処協定の枠組みを活用して、サイバー事案の脅威やサイバーセキュリティに関する情報共有を行うことにより、被害に関する警察への通報・相談を促進している。

また、警察庁では、一般社団法人日本損害保険協会等に対して、サイバー事案等により企業に生じた損害等を補償するサイバー保険を取り扱う損害保険会社等と都道府県警察との連携が図られるよう働きかけを行い、これを受け、都道府県警察では、サイバー保険を取り扱う損害保険会社との共同対処協定の締結、セミナーの開催等を通じて、被害発生時の警察への通報・相談を促進している。

サイバーテロ対策協議会



サイバー保険を取り扱う損害保険会社等との連携

しかしながら、１で述べたとおり、今後ともサイバー空間の脅威の情勢が深刻なものになっていくと予想されることを踏まえると、被害の潜在化防止に関する対策を強力に推進する必要がある。

３　被害の潜在化防止に向けた方策

２で述べた被害の潜在化を防止するためには、広く社会に対して警察への通報・相談の重要性、意義等のほか、被害発生時の被害拡大防止・被害回復等に関する助言等の被害企業等に裨益する事項を丁寧に周知する必要がある。

社会への周知に当たっては、既に整備された法的枠組みや関係省庁や企業等との情報共有や交換の枠組み等を活用することが一般に効率的かつ効果的であることは論をまたないであろう。

具体的には、個人情報の漏えい等が発生し、個人の権利利益を害するおそれが大きい場合は、個人情報保護委員会への報告等が義務化されており、また、重要インフラ事業者等については、各業法等により事業への障害を所管省庁へ報告することが義務付けられている。

こうした枠組みを活用するためには、所管省庁等と連携した取組を推進する必要があり、これについては３．１において検討する。

同時に、警察における通報・相談に関する環境整備を進める必要がある。これは、情報発信や広報啓発の観点、マニュアル整備や教育の実施等、警察側の対応を見直すものであり、その中には、警察の相談・受付対応者の意識改善といった論点を含むものである。

これについては、３．２において検討する。

３．１　関係機関等との連携強化

３．１．１　関係機関等との現状の取組・課題

⑴　関係省庁間の情報連携不足

事業所管省庁等では、それぞれの所掌事務に基づき、所管業界のサイバーセキュリティの確保に取り組んでいるが、従来から緊密な連携を行ってきた内閣官房内閣サイバーセキュリティセンター（ＮＩＳＣ）、総務省や金融庁等の一部の省庁等を除くと、現状、警察と事業所管省庁等との間のサイバー事案の被害に関する情報共有等は必ずしも十分とは言えない状況にある。

警察では様々なサイバー事案を捜査等する中で把握した犯行手口、犯罪情勢等の脅威情報を保有している。また、事業所管省庁等では、サイバー事案の被害が生じた場合に、法令や各業界のガイドライン等に基づき、所管企業等に報告を求めている場合があり、こうした報告等を基に所管企業等における個別具体的な被害状況や被害の傾向等の情報を保有している。

警察と所管省庁等において、それぞれが保有する情報の共有を更に促進し、捜査や被害防止対策等をより一層効果的に進める必要がある。また、特定の分野では、各企業等で犯罪被害を未然に防ぐため様々な情報を蓄積・分析し、不正とみられる行為を検知する仕組み等が

運用されているが、こうした取組を捜査等に活用できるよう、警察庁、業界団体と関係機関等の間で情報共有を進めることも検討すべきである。

これらに加え、被害発生時の警察への通報・相談や、所管省庁等に対する報告を、警察と所管省庁等の双方において促進することも必要である。

⑵ 複数にわたるサイバー事案の被害に関する報告窓口

サイバー事案の被害が生じた場合には、被害企業等は、警察への通報・相談のほか、法令やガイドライン等に基づき事業所管省庁等に対し報告する場合があることは、⑴においても述べたとおりである。ここで、事業所管省庁等に対する報告と、警察への通報・相談とは、それぞれ目的が異なるといった背景から、各機関で定める様式、報告事項等は統一化されておらず、報告先に応じた回答を個別に作成等する必要がある。また、社会的に反響が大きい事案であれば、それぞれの機関等からより詳細な又は補完的な情報の提供を求められることになることは想像に難くない。

こうした報告等のほか、被害企業等は、被害による影響範囲の調査、システムの復旧作業、顧客や取引先といった関係者に対する説明・謝罪等に忙殺されることになる。そうした状況を踏まえると、複数の関係機関等に対する個別の通報・相談等まで手が回らず、また、大きな負担を強いることになる。

このように、サイバー事案の被害に関する窓口が多岐にわたっていることや、報告様式・内容等が異なることも、警察への通報・相談を躊躇させる要因の一つになっていると考えられる。

３．１．２　関係機関等との連携に関する今後の取組

３．１．１で述べた課題に関する今後の取組について、以下に例示する。

⑴ 関係機関等との連携強化

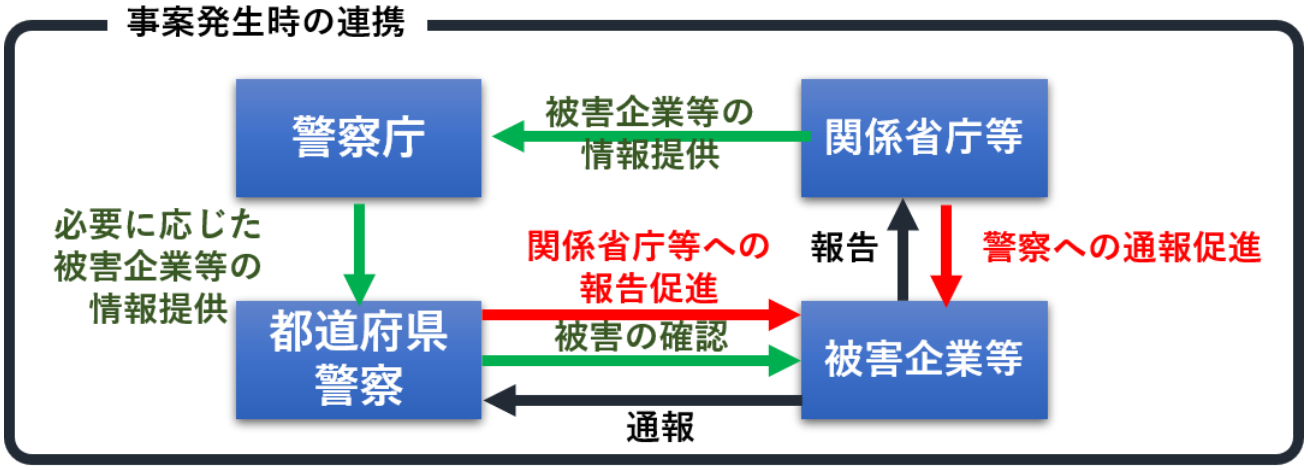
概括すると、事案発生時においては、可能な場合は関係省庁等から被害概要等を提供してもらうとともに、関係省庁等から被害企業等に警察への通報・相談を促進してもらうべきである。一方で、警察において事案を認知した場合は、所管行政を円滑に進めるためにも被害企業等に対し関係省庁等への報告の有無を確認し、報告していない場合は報告を促すべきである。

社会的な反響の大きい事案となりやすい分野を所管する省庁等として、例えば、ＮＩＳＣ、金融庁や総務省に加え、個人情報保護法を所管する個人情報保護委員会や、医療機関を所管する厚生労働省、大学等を所管する文部科学省、クレジットカード業界を所管する経済産業省等が挙げられる。

具体的には、個人情報保護委員会においては、個人情報漏えい等事案の報告を受けた場合に、被害企業等に対し警察への通報を促進することが望まれる。また、厚生労働省、文部科学省及び経済産業省においては、医療機関や大学、クレジットカード事業者等においてサイバー事案が発生した際に、被害組織に対し警察への通報を促進するとともに、情報の取扱い等に関する被害組織の意向に配慮しつつ、被害の概要を警察庁に提供することが望まれる。

また、こうした取組は、被害発生時に緊急に実施したとしても実効性を確保することが困難であることから、平素から相互に通報・相談又は報告の促進に関する広報啓発を推進することが求められる。

具体的には、ガイドライン等に盛り込んだり、講演等において説明したりすることが適当であろう。また、令和５年３月 24 日、警察庁サイバー警察局と個人情報保護委員会事務局との間で連携に関する覚書が締結されているところ、このように関係機関等との間で申し合わせを締結し、これを広報することなどにより、関係業界団体や国民に対しそれぞれの取組を可視化することも効果が大きいと考える。



事案発生時の関係機関等との連携

⑵　サイバー事案の被害に関する報告窓口の一元化

被害企業等の報告先が複数にわたる場合があることは、３．１．１⑵において述べたが、企業等がサイバー事案の被害に遭った場合の関係機関等への報告は、被害企業等の負担軽減や関係機関等における迅速な情報の把握・共有の観点から、ポータルサイトを設けるなど窓口を一元化（統一化）すべきである。警察庁においては、犯罪被害の拡大防止を強力に進めるため、省庁横断の統一窓口の創設に向けイニシアティブを強力に発揮することを期待する。

そして、より負担が少なくスタートしやすいことから、第一歩として、被害に遭った企業等が届け出る内容や様式について、関係機関等と連携し可能な限り統一化することから始めるべきである。

そのほか、例えば、インターネット上の誹謗中傷について警察による捜査等を望まずに削除のみを希望する被害者や、自社のウェブサイトを騙ったフィッシングサイトについて迅速なテイクダウンを求める企業等、通報・相談の内容によっては警察以外の窓口に相談することが適している場合もある。そうした通報・相談の内容に関し、関係機関等と連携して対策等に関する広報啓発を行うとともに、それぞれの所掌事務、特徴等を生かせる分野等を基に、効果的な役割分担となるよう検討を進め、あわせて、関係機関等の窓口や担当業務を都道府県警察のウェブサイト等において提示すべきである。

３．２　被害者が自発的に通報・相談しやすい環境整備

３．２．１　通報・相談しやすい環境整備に関する現状の取組・課題

⑴　被害者に対する情報発信の不足

通報・相談を行うに当たって必要な情報が不十分であることが、通報・相談を躊躇させる理由となっている状況がうかがえることは、２．２において述べたとおりである。

実際、都道府県警察のウェブサイトにおける情報発信の状況について調べたところ、「サイバー犯罪の具体例を示している」のが 30 警察、「通報・相談すべき具体的内容を示している」のが 23 警察、「通報・相談時に必要となる情報を示している」のが 10 警察、「よくある相談とその対応策を示している」のが 26 警察、「被害回復の手続を示している」のが４警察であるなど、全ての都道府県警察において情報発信を十分に実施できていないことが判明している（令和５年２月末時点）。

また、都道府県警察のウェブサイトからのサイバー相談受理状況は極めて低調であることも併せて判明しているところ、都道府県警察における通報・相談窓口は、必ずしも担当窓口や警察署の電話番号が明示的ではない状況である。都道府県警察のウェブサイトにおけるサイバー相談に関する窓口の設置状況について確認したところ、入力フォームか電子メールかの違いはあるものの、19 警察にのみ設置されている状況であり、残りの都道府県警察では、警察相談の枠組みで相談を受け付けている状況であった（令和５年２月末時点）。

⑵　被害者が相談しにくい事案の存在

３Ｇ回線のサービス終了や成人年齢の引き下げといったことを背景として、これまでインターネットやスマホに触れてこなかったなどの理由から情報リテラシーが比較的低い層における急速なスマートフォンの普及が見込まれる。こうしたことに加え、被害に遭った高齢者や青少年が家族等に相談しにくいなどの理由から、通報・相談が躊躇されることが懸念される。例えば、サポート詐欺であれば、被害者が犯罪と認識できずコンビニエンスストア等でギフトカードを購入し送金する事案が発生しているほか、フィッシング詐欺のように偽の

サイトと気付かずに銀行の口座番号やパスワードを入力し不正送金されてしまう事案が発生している。

また、令和４年 10 月末時点で外国人労働者数が過去最高を記録し、今後も来日する外国人の増加が見込まれることを踏まえ、「外国人材の受入れ・共生のための総合的対応策（令和４年度改訂）」（令和４年６月 14 日関係閣僚会議決定）に基づいて日本語が堪能ではない外国人に対する配慮を実施する観点や、「障害者基本計画（第５次）」（令和５年３月 14 日閣議決定）に基づく障害のある人への合理的配慮を提供する観点等からの対応を併せて行う必要がある。

こうした状況を踏まえると、高齢者、青少年、外国人、障害のある人等に対し、被害の拡大防止・未然防止等の観点から、どういった犯行手口があるのかを個別かつ丁寧に説明を行う必要があるほか、万が一だまされた場合における被害対策を講じる必要がある。

⑶　警察の適切な対応の不足

国民や企業等が警察に通報・相談した際に、警察において適切な対応が取られていない場合があるとの指摘がなされている。例えば、警察からの説明が不十分であり、「通報や相談をしても警察は捜査に消極的である」との印象を与える場合がある。また、通報・相談の対応をする警察職員によっては、デジタル資産をはじめとした新たな情報通信技術に関する知識不足・理解不足等により、被害者の窮状や切迫した状況等が理解できず適切な対応ができていない場合がある。

これまで述べてきた施策を推進し通報・相談が促進されたとしても、こうした対応が改善されない場合は、被害者の要望や希望に対する落差は大きくなり警察への信頼が失われ、かえって被害が潜在化してしまうおそれがある。

３．２．２　通報・相談しやすい環境整備に関する今後の取組

⑴　積極的な情報発信

３．２．１⑴で述べた課題を踏まえ、次のア及びイに掲げる情報発信に関する対策を講じるべきである。

ア　都道府県警察のウェブサイトのコンテンツの改善

通報・相談を促進するために、警察からの情報発信を強化する必要があるが、情報発信の強化に当たり基本的にはウェブサイトを活用すべきである。ＳＮＳの広報啓発における有用性は非常に高いものの、掲載できる情報量はウェブサイトに比して非常に限定的にならざるを得ない。高齢者に対しては、新聞やテレビ等のメディアがいまだに影響力を有しているが、こちらも掲載等のタイミングや内容について警察が主体的に、又は柔軟に実施できず、ウェ

ブサイトよりも劣っている面がある。情報発信を強化するに当たっては、まずは都道府県警察のウェブサイトのコンテンツを改善することから始め、ＳＮＳや新聞等は改善したウェブサイトへの呼び水として活用することが効果的であろう。

コンテンツの改善については、どういったものが犯罪として取り扱われるのか、被害の未然防止策や被害に遭った際の対処方法（被害の拡大防止策）等に加え、被害回復の手続や関係機関等の紹介といった通報・相談者の視点に立ったものに再構成する必要があるが、これは、３．２．２⑶の検討と併せて行うべきである。

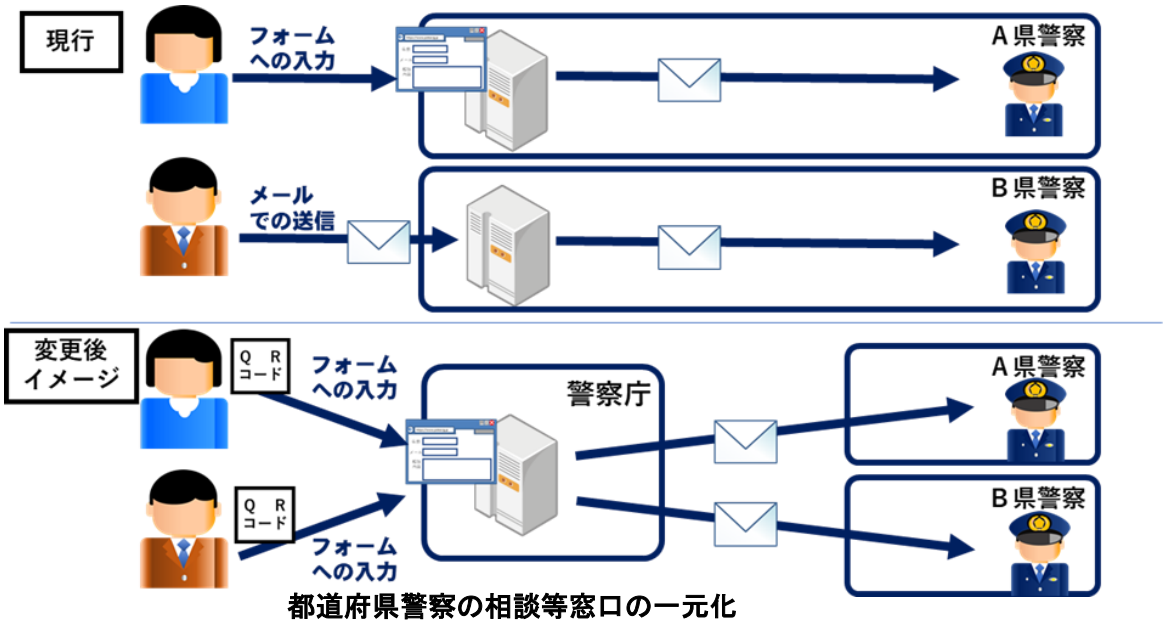
そして、通報・相談後の被害者の負担軽減や手続等の円滑化のため、警察の捜査ではどういったことをどういった流れで行うのか、通報・相談する際はどういった資料を用意する必要があるのか、といった内容をあらかじめ示すべきである。また、関係機関等の窓口や担当業務をウェブサイト等において提示すべきである（再掲）。

これらを実行に移す際には、警察庁においてウェブサイトのひな形を都道府県警察に示した上で、都道府県警察でこれを活用して情報発信することが、効率性、統一性等の観点から適当であろう。また、現状でも他の都道府県警察の参考となる情報発信を行っている都道府県警察もあることから、それぞれの特色を継続して活かせるよう、都道府県警察の裁量の余地を十分に残すように配慮すべきである。さらに、こうした独自の情報発信については、警察庁において適切に把握し、他の都道府県警察で使用できるように共有するといった好循環のサイクルを回すべきである。

イ　インターネット上の通報・相談窓口の統一化

３．１．２で述べたとおり、企業等がサイバー事案の被害に遭った場合の関係機関等への届出先は、通報・相談を行う企業等の負担軽減や関係機関等における迅速な情報の把握・共有の観点から、ポータルサイトにより統一されることが望ましい。しかし、こうした取組については、関係機関等との調整や所要の期間、予算等を要することから、関係機関等の相談窓口について相互に参照できるようにすると同時に、まずは警察庁においてインターネットから一元的かつ簡易に通報・相談できる窓口を整備するべきである。

この際、インターネットからの手続に苦手意識を持つ高齢者等もいることから、一元的に相談を受け付けるページにおいて、各都道府県警察の警察署の連絡先のリンクを掲載するなどの配慮を行うべきである。



都道府県警察の相談等窓口の一元化

⑵　高齢者や青少年等に対する広報啓発活動

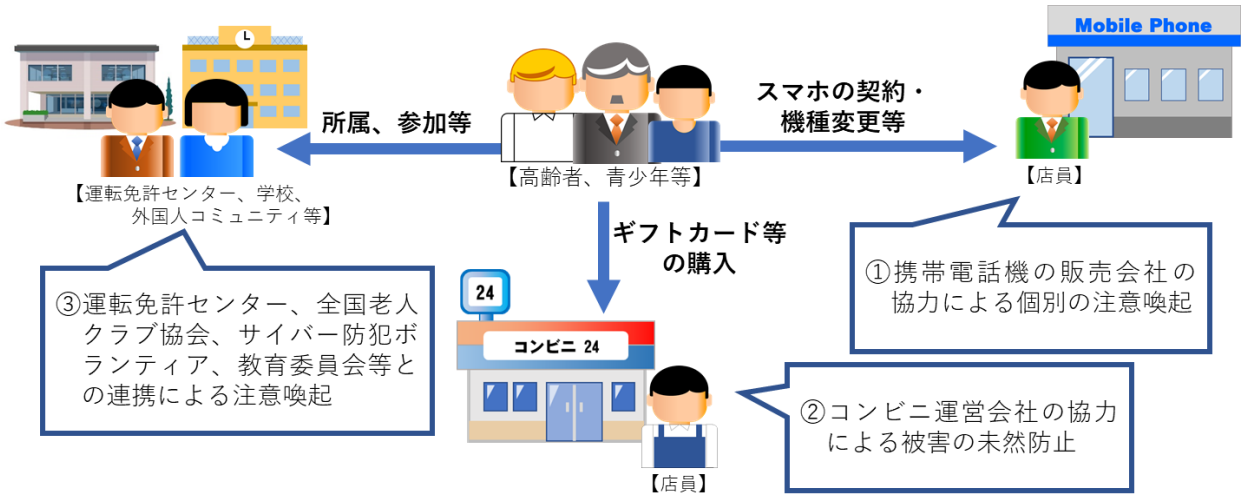
３．２．１⑵で述べた課題を踏まえ、主に３つの観点から、高齢者、青少年、外国人、障害のある人等に対する広報啓発を推進すべきである。

まず、携帯電話事業者や家電量販店の協力を得て、スマートフォンの新規契約時や機種変更時に、契約者に対する個別の注意喚起を行うべきである。特に、新規契約時は、契約者の多くは情報リテラシーが決して高いといえない状況である場合が多い反面、サイバー事案に巻き込まれかねないと認識している状況であり、犯罪の具体的な事例やその対策、被害に遭った場合の通報・相談先等を示すことにより、効果的な広報啓発を行うことが期待できる。この際、外国人や障害のある人の事情に配慮した形で実施することも必要である。

２点目として、コンビニにおける対策強化である。欺罔、脅迫等によりコンビニにおいてギフトカード等を購入させ、不正に送金させる手口が横行していることから、被害者が欺罔行為等により錯誤に陥りギフトカード等を購入することを思い立ったとしても、直前に思いとどまらせることができれば被害防止が可能となる。この点、コンビニの店員が被害防止に貢献している例が散見されることから、フランチャイズ事業者に対して、店長・オーナーへの注意喚起事項等を伝達してもらうよう協力依頼すべきである。

３点目として、対象者が集まる場所を活用し積極的に注意喚起すべきである。例えば、運転免許センターの待合室に設置されたデジタルサイネージ等を使用し注意喚起することや、全国老人クラブ連合会の協力により、老人クラブにおける注意喚起を実施するほか、青少年に対しては、特に初めてスマートフォンを持つ可能性が高い新入生を対象とし、学校におけるサイバー防犯ボランティア等による教育活動が効果的であると考えられる。また、外国人に対する広報啓発は、関係省庁等の協力を得つつ、外国人コミュニティに対して実施するべ

きである。さらに、高齢者の被害に係る届出先の案内等は消費生活センターで既に実施していることから、都道府県警察と都道府県の消費生活センターとの間で情報共有等の連携を進めるべきである。



高齢者や青少年等に対する広報啓発活動

⑶　警察における対応改善に向けた取組

通報・相談の促進を行う上で、最も重要な要素となるのが、警察署、交番等で対応する警察職員の対応改善である。これまで述べた諸施策を推進し、通報・相談が更に促進されたとしても、警察署等における対応がおろそかになっては、通報・相談者の失望はかえって大きくなり、警察への信頼は失墜し、通報・相談をする被害者・被害企業等が減少していくことが懸念される。ひいては、情報収集やその先にある捜査、対策等を的確に行うことが困難となることは想像に難くない。

警察における対応改善は、まずは通報・相談者の視点に立つことから始めるべきである。通報・相談者は、警察に何を望んでその門戸を叩いたのか、具体的には、

○　被疑者を厳罰に処すための検挙を望んでいるのか

○　被害回復を望んでいるのか

○　被害の拡大防止や今後の再発防止対策を望んでいるのか

○　サイバー空間の安全・安心の確保のため情報を役立ててもらうことを望んでいるのか

ということ（又はこれらの組み合わせであること）を的確に把握する必要がある。

特に、捜査を望む通報・相談者に対して、捜査に消極的であるとの誤解を与えることのないように対応することは、何よりも重要である。「捜査しても攻撃者まで辿り着くことが困難な見通しである」、「あなたはこの犯罪の被害者に当たらない」などと消極的な対応をされたとの事例等を聞くことがあるが、警察を拠り所として訪ねてきた被害者に対し、警察が消極的な対応をすることがあってはならない。仮に現実的に捜査が困難である見通しがあった

としても、被害者等に寄り添い、通報・相談者に適切な説明をして理解、納得を得ることが必要である。また、通報・相談によって得られる情報が、未然防止対策やアトリビューション等の警察の活動において非常に重要であるという観点からも、通報・相談者の声を丁寧に拾い上げることが警察に求められる。

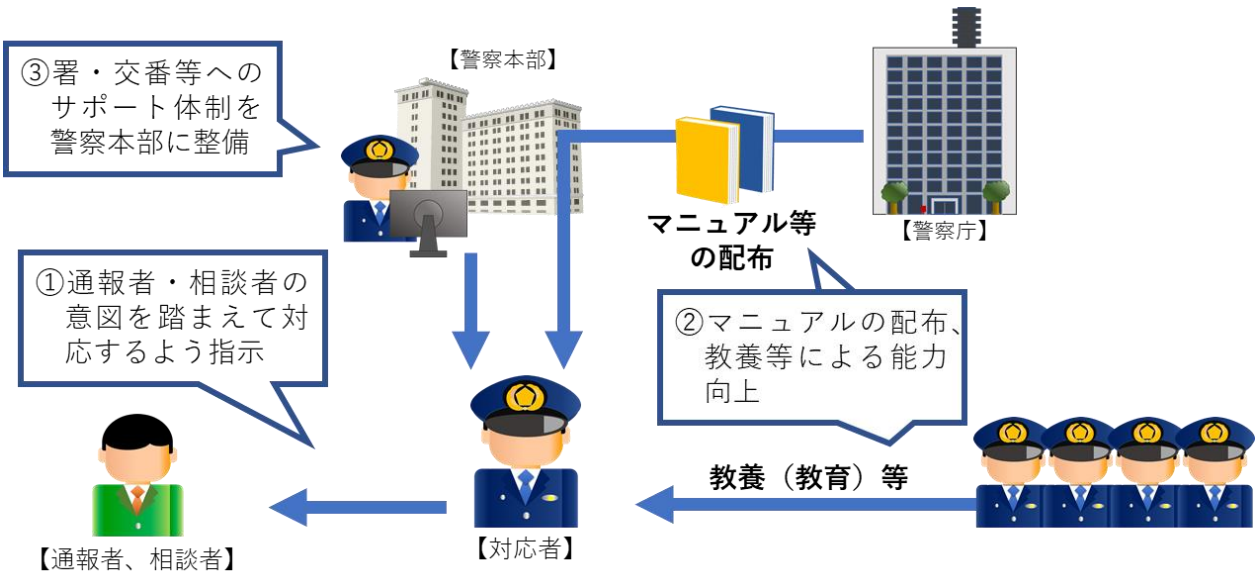
他方で、サイバー事案に限らず、警察が取り扱う事象は広範かつ複雑化しており、警察に期待する声も大きいという状況に対して、警察のリソースは有限である。そのような中で、通報・相談者に適切に対応するためには、警察職員の対応改善に加え、３．２．２⑴で述べた情報発信の強化等による業務負担の軽減に確実に取り組まなければ、第一線の現場が疲弊し、負の連鎖が発生してしまう。例えば、都道府県警察において消費生活センター等と的確に連携するなど、他機関と適切な役割分担を行い、警察のリソースを警察にしかできない業務に集中させるという観点も重要である。被害の潜在化防止は、都道府県警察の業務負担が過重なものとならないよう配意しつつ進めなければならない。

以上のことを踏まえ、警察庁から都道府県警察に対し、通報・相談にはどういった視点を持って対応すべきかを明確に示すべきである。

通報・相談者が何を望んでいるのかを丁寧に聴取しつつ、「どのように説明し対応するのか」、「どういった項目について聴取するのか」といった視点に関し、対応マニュアルを整備し、過不足なく丁寧な説明や聴取ができるように備えるべきである。この際、仮に通報・相談者が被害回復のみを望むために捜査協力が得にくい場合等も想定し、捜査や対策等に必要な情報を取得できるような内容を盛り込む必要がある。また、マニュアルの配布対象としては、サイバー事案担当者だけでなく、警察相談担当者や当直体制時に相談対応に当たる者とし、これらの者が当該マニュアルに沿って適切に聴取し、対応できるようなものとすべきである。

加えて、通報・相談対応する者に対する教育も定期的に実施すべきである。通報・相談対応者の意識向上・改善に加え、デジタル資産等についての理解も進める必要があり、情報リテラシーの向上の観点からも、適切な通報・相談対応ができるよう警察内部での教育を行う必要がある。

一方、通報・相談者が警察署や交番を訪問した際に、状況によっては対応できない場面も想定されることから、警察本部によるサポート体制を整備するべきである。例えば、佐賀県警察においては、警察本部と警察署をオンライン会議システムで繋ぎ、警察本部において警察署等のサポートをしており、こうした事例を参考にするべきである。



警察における対応改善に向けた取組

また、これらの取組を国民に理解してもらうため、積極的な広報啓発を行うべきである。これは、３．２．２⑴で述べた情報発信の一環で推進することが適当であろう。

おわりに

本検討会では、サイバー事案の被害者による警察への通報・相談が躊躇される課題を整理した上で、被害の潜在化の防止に向けた効果的な方策に関する議論を行った。被害の潜在化については、被害発生時にどのような主体に対してどのような対応を行うべきか、被害者の視点に立った対応が明確に示されていないという課題等があると考えられ、「関係省庁等と連携した通報・相談の促進」、「被害者が自発的に通報・相談しやすい環境の整備」の２つの観点から、警察において推進すべき取組を洗い出した。

デジタル化の進展に伴いサイバー事案による被害の影響が甚大化・広範化・複雑化し、自助的な取組のみでは対応することが困難な状況において、サイバー空間における安全・安心という公益を確保するためには、警察をはじめとした関係機関等、企業等、そして国民一人一人がそれぞれの立場で適切な対策を講じつつも、各主体の緊密な連携が必要となることには異論が少ないであろう。

本検討会では、被害者が通報・相談を行う際の様々な課題を解消するために、被害の拡大・未然防止に係る取組等を行う主体が連動して対処に当たる枠組みの整備、国民や企業等に呼びかける事項の明確化・情報発信強化等を具体的な方策として示したが、その中でも重要なことは、「通報したら被害回復の支援をしてもらえた」、「警察に相談したら、どういった対策が必要になるか教えてもらえた」というように、警察から目に見える結果を示し、被害者からの信頼を得ることである。

その点、警察においては個別事案の事件化を第一に対応してきた側面や、事務運営の効率を優先して、消極的と取られかねない対応をしてきたことも否定できない。犯人検挙は治安の維持に必要不可欠であり、引き続き強力に推進する必要があるが、一方で、被害者からの信頼を得るためには、被害者の視点に立ち、その負担の軽減に配意するとともに、事件化のみを指向した対応に終始することなく、事業復旧への支援、情報発信、窓口対応等の取組を充実させるべきである。また、これらの取組の進捗を適時に把握し、情勢等を踏まえ見直していくことが求められる。さらに、取組の結果として警察に寄せられることとなる情報を集約して総合的な分析や検討を進めるためのリソースを確保し、これらの情報の適正かつ効果的な活用を図っていくことも必要となる。

本報告書で述べた提案は警察のみで実行できるものではなく、関係機関や企業等と協力して乗り越えなければならない課題も存在するが、我が国のサイバーセキュリティに係る対処能力を高める上で避けては通ることのできないものである。提案した取組を実施する過程において新たな課題が生じることも考えられるが、被害者や被害企業等の声を丁寧に拾いつつ、関係機関等が一丸となり、安全・安心なサイバー空間の確保のために柔軟かつ的確に対応してもらいたい。我々としても、こうした取組を引き続き後押ししていく所存である。提案し

た取組が推進されることで、被害者が自ずと通報・相談するような風土が醸成され、安全・安心なサイバー空間が実現されることを強く期待している。