生活様式の変化等に伴うサイバー空間の新たな脅威に対処するための官民連携の更なる推進

令和２年度サイバーセキュリティ政策会議　報告書

サイバーセキュリティ政策会議

はしがき

近年めざましい発展を遂げている情報通信ネットワーク、とりわけインターネットは、国民生活の利便性を向上させるにとどまらず、社会経済活動の根幹を支える重大なシステムとして機能するに至っている。その一方で、サイバー犯罪やサイバー攻撃の多発等が大きな社会問題となるなど、サイバー空間の脅威に対する国民の不安は急速に高まっており、官民が連携して効果的な対策を検討・実施する必要性が高まっている。

こうした状況に適切に対処するため、平成 13 年度には、官民連携したサイバー犯罪捜査及び被害防止対策によりサイバー空間の安全安心を確保することを目的に、サイバー空間の脅威への対処に向けた産業界等と警察との連携の在り方について有識者等による検討を行うため、警察庁生活安全局長主催の私的懇談会である「総合セキュリティ対策会議」が設置された。サイバーセキュリティに関するより幅広いテーマを取り扱うため、平成 29 年度には、「総合セキュリティ対策会議」は、警察庁長官官房サイバーセキュリティ・情報化審議官の私的懇談会として「サイバーセキュリティ政策会議」に改組され、サイバーセキュリティに関する有識者にとどまらず、電気通信事業、コンテンツ事業等の各種事業に関する知見を有する方々、さらには、法曹界、教育界、防犯団体など、幅広い分野の有識者を交えて、活発な意見交換を行ってきた。

これまでの意見交換の結果は、平成 13 年度以降、毎年度、報告書として取りまとめられるとともに、その報告書の内容を踏まえ、様々な施策が取りまとめられ、実施されてきた。例えば、平成 18 年のインターネット・ホットラインセンターの運営開始、平成 20 年のファイル共有ソフトを悪用した著作権侵害対策協議会の発足、平成 21 年の児童ポルノ流通防止協議会の発足、平成 24 年の不正アクセス禁止法の改正、平成 26 年の一般財団法人日本サイバー犯罪対策センター（JC3）の創設、平成 29 年の青少年ネット利用環境整備協議会の設立等の取組が挙げられる。

令和２年度のサイバーセキュリティ政策会議は、「生活様式の変化等に伴うサイバー空間の新たな脅威に対処するための官民連携の更なる推進」をテーマに選定した。新型コロナウイルスの感染拡大を受けた「新しい生活様式」の定着やこれに伴い加速するデジタル化推進の動きにより、我々の社会経済活動に急激な変化が生じている。また、デジタル社会の実現に向けた政府全体の取組により、今後、サイバー空間は、地域や老若男女問わず、全国民が参画し、重要な社会経済活動を営む、これまで以上に重要かつ公共性の高い場へと変貌を遂げていくものと考えられる。こうしたサイバー空間における大きな変革の動きの中で国民の安全・安心を守っていくためには、サイバーセキュリティ確保のための具体的対策はもちろんのこと、サイバーセキュリティの在り方そのものを大局的見地から検討することが必要であることから、本会議で

は、今後のサイバーセキュリティに求められる新たな基本理念や警察をはじめとする関係機関・団体等が緊密に連携しながら取り組むべき今後の取組の方向性について検討を行った。

各委員には、それぞれが属する企業・組織における知見を背景としつつも、中立的な立場で議論に参加していただき、本報告書に議論の結果を取りまとめた。本報告書が、警察にとどまらず政府全体・社会全体のサイバーセキュリティの検討や方針策定に活かされ、全ての国民が安心して参画できるサイバー空間の実現の一助となれば幸いである。

令和３年３月

サイバーセキュリティ政策会議委員長

前田雅英

目　次

はじめに

新型コロナウイルスの感染拡大を受けた「新しい生活様式」の定着やこれに伴い加速するデジタル化推進の動きにより、我々の社会経済活動に急激な変化が生じている。実空間において対面で行うことを前提としていた我々の活動は、人やモノとの接触を可能な限り避けるべく、テレワークの積極的な実施やキャッシュレス決済サービスの普及を含む取引のオンライン化により、サイバー空間を通じて非対面・非接触で行われるものに大きく変容している。

また、政府は、「デジタル社会の実現に向けた改革の基本方針」（令和２年 12 月 25 日閣議決定）において、デジタル社会の目指すビジョンとして「デジタルの活用により、一人ひとりのニーズに合ったサービスを選ぶことができ、多様な幸せが実現できる社会」を掲げ、このような社会を目指すことは、「誰一人取り残さない、人に優しいデジタル化」を進めるということにつながるとしており、今後、サイバー空間は、地域や老若男女問わず、全国民が参画し、重要な社会経済活動を営む、これまで以上に重要かつ公共性の高い場へと変貌を遂げていくものと考えられる。

他方で、令和２年９月に警察庁が実施したアンケート調査によると、回答者の75.3%がサイバー犯罪に不安を感じると回答するなど、依然として、大多数の国民がサイバー空間に対する不安を感じている。また、個人レベルではサイバーセキュリティに対する意識や知識に大きなギャップが存在するのが実情である。

こうした中で国民の安全・安心を守っていくためには、官民を挙げたサイバーセキュリティの確保のための具体的な対策はもちろんのこと、サイバーセキュリティの在り方そのものを大局的な見地から検討することが必要である。

そこで、令和２年度サイバーセキュリティ政策会議では、「生活様式の変化等に伴うサイバー空間の新たな脅威に対処するための官民連携の更なる推進」をテーマとして幅広く検討を行うこととし、令和２年 10 月以降、５回の会合を開き、専門家からヒアリングを行うなど、様々な意見を聴取しながら議論を重ねてきたところである。

本報告書は、今後のサイバーセキュリティに求められる新たな基本理念や警察をはじめとする関係機関・団体等が緊密に連携しながら取り組むべき今後の取組の方向性について、本会議における議論の結果を取りまとめたものである。

第Ⅰ部　総論

第１章　生活様式の変化等に伴うサイバー空間の新たな脅威

１．コロナ禍が顕在化させるサイバー空間の新たな脅威

新型コロナウイルス感染症の感染拡大に伴う社会経済活動の変容は、サイバー空間の新たな脅威を顕在化させており、既に深刻な被害が発生しているものもあることから、官民が連携した対策が急務となっている。

(1)　キャッシュレス決済サービスの不正利用をめぐる被害の急増

令和２年９月、国内の複数のキャッシュレス決済サービスにおいて、金融機関に開設された口座情報が不正に入手・連携され、不正なチャージが行われる事案が大きな社会問題となった。

図表１は、キャッシュレス決済サービスの不正振替のイメージを示したものである。犯行の手口としては、被疑者が被害者の口座情報等を不正に入手し、被害者になりすましてキャッシュレス決済サービスのアカウントを開設し、被害者の銀行口座と当該アカウントを連携させ、不正なチャージが行われたものであり、口座振替サービスを利用していない高齢者が被害者となった事例も明らかになっている。

日本のキャッシュレス化は、海外と比べて遅れていると指摘されており、政府は、令和元年に 26.8%であったキャッシュレス決済比率を、令和７年までに４割程度とすることを目標に掲げている[1]。

図表１：キャッシュレス決済サービスの不正振替のイメージ

[1] 「成長戦略フォローアップ」（令和２年７月 17 日閣議決定）

一般に、キャッシュレス決済サービスにおいては、アカウントの乗っ取り、アカウントと銀行口座の不正な連携、クレジットカードの不正な登録、不正なアカウントの作成等の不正利用が確認されており、事業者ごとに不正利用の防止対策が講じられているが、安全性と利便性のバランスをとる必要があるほか、事業者だけでは対処が難しい課題もあり、官民が連携した取組の強化が求められている。

(2) テレワークの脆弱性等を狙ったサイバー攻撃

コロナ禍により急速にテレワークが普及しているが、テレワークには、例えば、Windows に標準装備されているリモートデスクトップとよばれる機能が活用されている。リモートデスクトップ機能により、外部から職場のパソコンに接続し、ファイルの編集やアプリケーションの起動が可能となるが、機能が攻撃者に悪用されれば、情報流出等の深刻な被害につながることとなる。例えば、令和２年、悪用されれば機器の乗っ取りにもつながる深刻な脆弱性が発見されたが、この脆弱性については、既にマイクロソフト社から対策プログラムが配布されるなどしている。このように、サイバーセキュリティに携わる民間事業者等において、こうした脆弱性を発見し、必要な対策を講じる取組が日々続けられている。

急速なテレワークの普及により、家庭用のネットワークから、場合によっては家族共有の家庭用端末を使って、事業所の機器やネットワークに接続することが一般的に行われるようになった。職場とは異なり、各家庭では、個人のリテラシーレベルにかかわらず各自で対策をとる必要があるところ、既に対策が存在する脆弱性であっても、必要な対策がとられずにそれが攻撃者に悪用されれば、深刻な被害につながるおそれがある。

また、テレワークには、外部からのマルウェア（不正プログラム）等の持込みというリスクが存在し、防衛関連企業において、在宅勤務時に社有パソコンを外部ネットワークに接続した際にマルウェアに感染し、社内ネットワークに持ち込んだ事案が確認されている。

さらに、テレワークの拡大により、セキュリティ事案に対応する組織であるCSIRT[2]などの体制が脆弱となり、事案への即応が遅れるのではないかとの懸念も存在する。

[2] Computer Security Incident Response Team の略

２．犯行手口等の悪質化と被害の深刻化

コロナ禍の前より確認されていたフィッシングやマルウェア攻撃についても、その犯行手口等は悪質化しており、その被害も深刻化している実態があることから、官民が連携した対策が急務となっている。

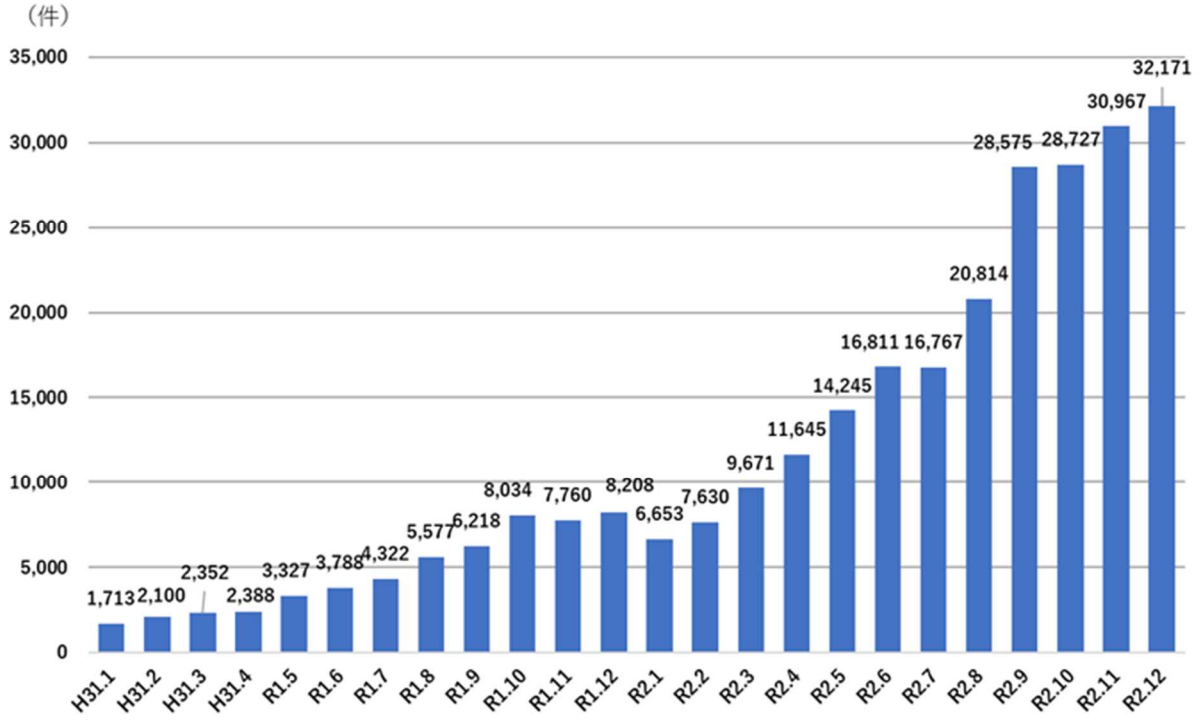
(1)　フィッシング被害の急増と手口の巧妙化

フィッシングは、不正送金事犯のほか、SNS（ソーシャル・ネットワーキング・サービス）のアカウント乗っ取りなど、様々な犯行に悪用されており、フィッシングやフィッシングで窃取した個人情報を悪用したサイバー犯罪が急増している。

図表２は、フィッシング対策協議会に寄せられたフィッシング報告件数の推移を示しており、令和２年に入り急増し、過去最高を更新し続けている[3]。

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、令和元年に被害が急増し、令和２年の年間被害は、発生件数 1,734 件（前年：1,872 件）、被害額約 11 億 3,300 万円（前年：約 25 億 2,100 万円）と前年に比べて被害額は大幅に減少したものの、発生件数はやや減少したにとどまり、引き続き高水準で推移している[4]。

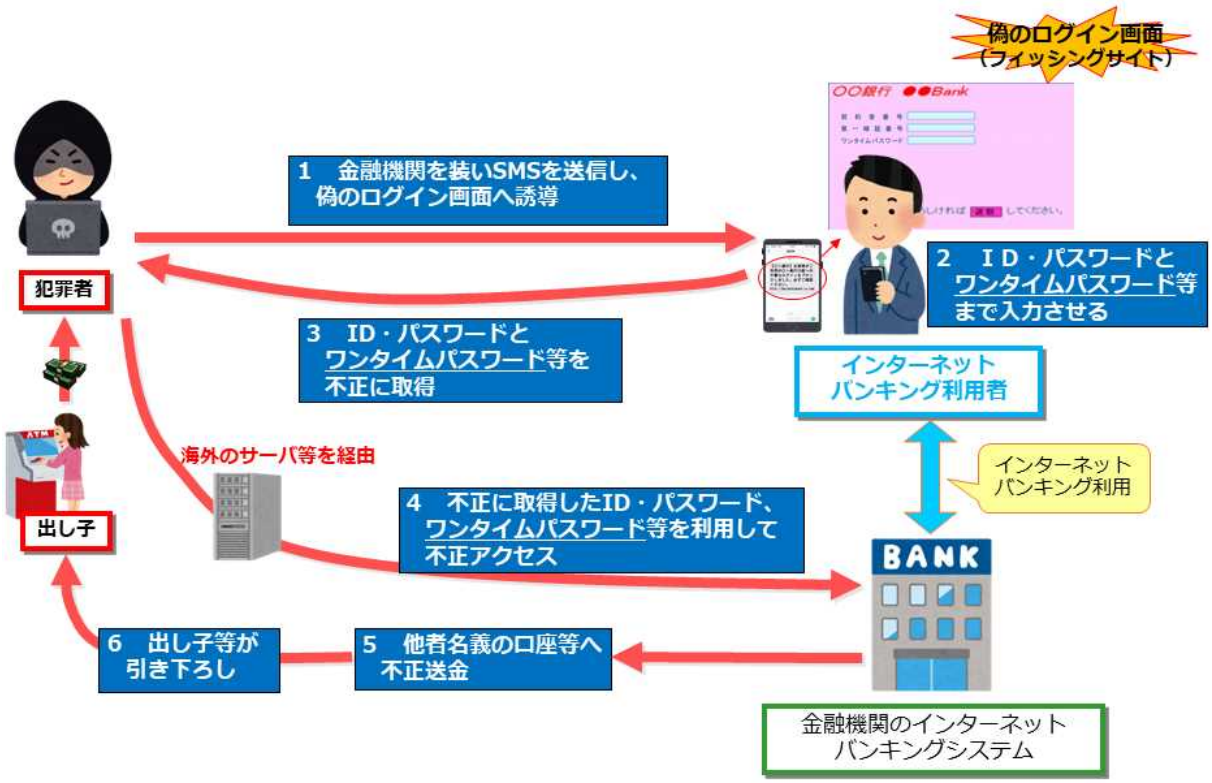
図表２：フィッシング報告件数



[3] フィッシング対策協議会の統計に基づいて作成

[4] 警察庁の統計による。

図表３：スミッシングによる手口のイメージ



不正送金の被害の多くは、ショートメッセージや電子メールを用いて、金融機関を装ったフィッシングサイトへ誘導する手口によるものと見られており、こうした手口の多くが、ソーシャルエンジニアリングとよばれる手法を用いている。ソーシャルエンジニアリングとは、ネットワークに侵入するために必要となるパスワード等の重要な情報を、マルウェア等の情報通信技術を使用せずに盗み出す方法であり、その多くは人間の心理的な隙や行動のミスにつけ込むものである。

従来のフィッシングは、電子メールにより誘導される手口が一般的であったが、図表３のとおり、昨今のフィッシング被害多発の要因の一つとして、ショートメッセージにより誘導する手口であるスミッシング（SMSとphishingを組み合わせた造語）が確認されるようになっている。

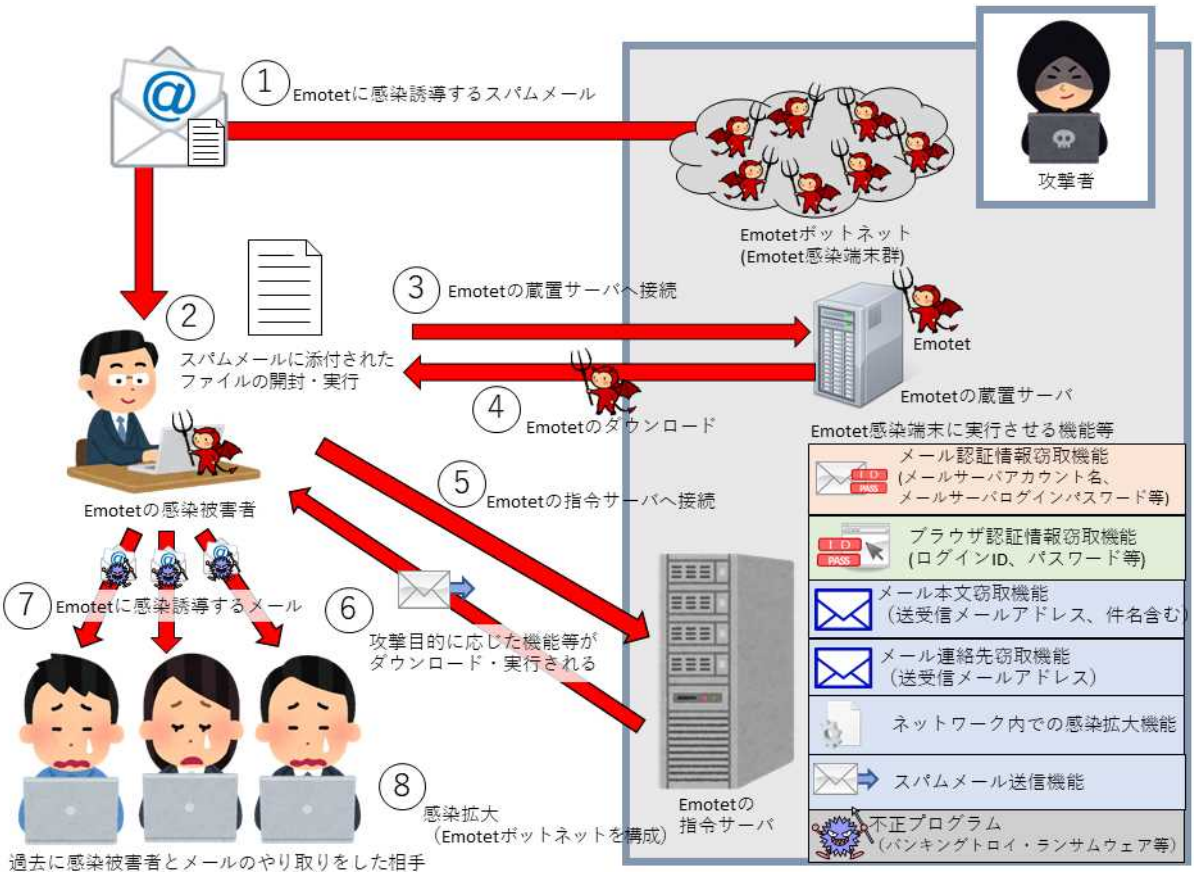
(2)　悪質化するマルウェア攻撃

ア　ソーシャルエンジニアリングの手法の利用

ソーシャルエンジニアリングは、フィッシングや標的型攻撃等の手口に多く見られる手法であるが、最近では、マルウェア攻撃においてもソーシャルエンジニアリングの手法が用いられるようになっている。

Emotet は、主にメールの添付ファイルを感染経路としたマルウェアであり、平成 26 年に最初の被害が確認されて以来、サイバー空間の犯罪インフラとして、世界中でサイバー犯罪・サイバー攻撃に悪用されてきた。

図表４：Emotet 動作概要



図表４は、警察庁が Emotet を解析し、動作概要をまとめたものである。Emotet は、過去にやり取りしたメールへの返信を装ったメールを送信し、添付ファイルの開封を促すことが判明している。具体的には、Emotet に感染したパソコンからメールアカウント、パスワード、メール本文等の情報を窃取し、これらの情報を悪用して、感染拡大を目的としたメールを送信する[5]。

このように、Emotet は、過去にやり取りしたメールへの返信を装ったメールを送信し、添付ファイルの開封を促すなど、ソーシャルエンジニアリングの手法を利用しており、Emotet への感染被害による情報窃取が、他者に対する新たな攻撃メールの材料とされる悪循環が発生しているおそれがある。

また、Emotet は、インターネットバンキングに係る不正送金事犯にも悪用されている可能性があり、端末に感染した Emotet が、Zloader とよばれるインターネットバンキングの情報を窃取するためのマルウェアを端末にダウンロードし、ID・パスワードを窃取したと疑われる事案が確認されている。

世界中で大きな被害をもたらした Emotet は、令和３年１月、オランダ、ドイツ、米国、英国、フランス、リトアニア、カナダ及びウクライナの当局等の

[5] 警察庁の発表による。

連携により、そのボットネット[6]が破壊され、我が国においても、海外の当局から国内の Emotet 感染端末に関して情報提供を受け、インターネットプロバイダを通じて、当該端末の利用者に注意喚起を行うこととしている。

Emotet 以外にも、類似の手口のマルウェアが確認されており、今後もこうしたソーシャルエンジニアリングの手法を利用したマルウェアの動向に警戒が必要である。

イ　ランサムウェア攻撃

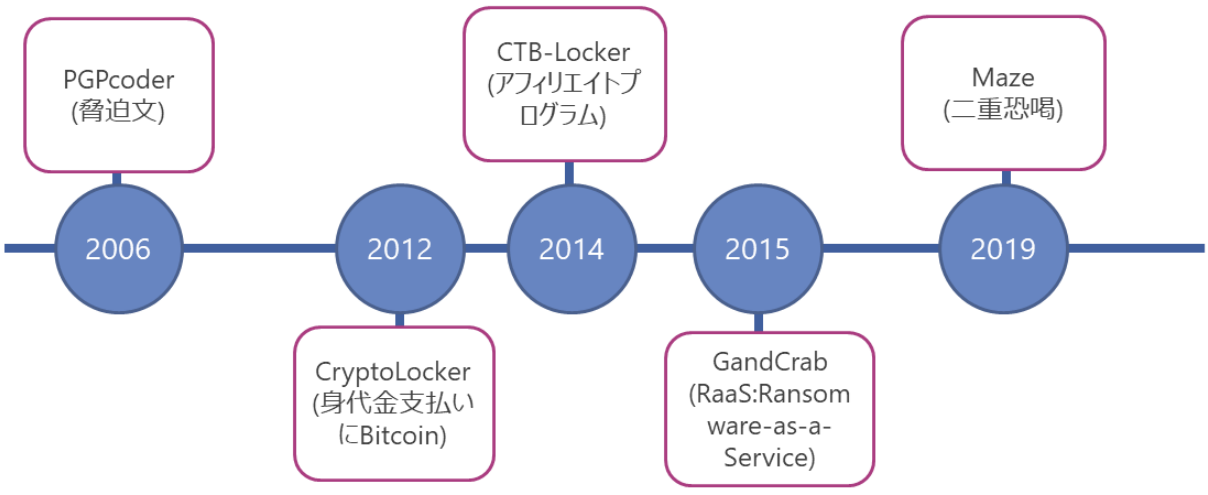
ランサムウェア（ransomware）とは、ransom（身代金）と software（ソフトウェア）を組み合わせて作られた名称であり、マルウェアの一種である。このマルウェアに感染すると、パソコン内に保存しているデータを勝手に暗号化して使えない状態にされ[7]、その制限を解除するための身代金を要求される。

令和元年 11 月以降、企業などを標的にしたランサムウェア被害が国内外で相次いでいる。従来のランサムウェアは、不特定多数の利用者を狙ってランサムウェアに感染するファイルが添付された電子メールを送付するといった手口が一般的であったが、現在では、特定の個人や組織を狙った手口にシフトし、企業のネットワーク等のインフラを狙うようになっている。

図表５は、ランサムウェアの悪質化と模倣の歴史をまとめたものである[8]。

ランサムウェアは平成 18 年頃から存在し、PGPCoder とよばれるランサムウェアが、その例であるといわれており、パソコンのデスクトップ画像を変更し

図表５：ランサムウェアの悪質化と模倣の歴史



[6] マルウェアに感染したコンピュータ（以下「感染端末」という。）と多数の感染端末に指令を送信する C&C（Command and Control）サーバから構成されるネットワーク

[7] 感染した端末の中のファイルが暗号化されるのみではなく、その端末と接続された別のストレージも暗号化される場合がある。

[8] 株式会社 NTT データの新井悠氏の作成による。

て、脅迫文を表示させ、利用者に読むよう指示する手口が使われたが、この手口は、現在のランサムウェアでも踏襲されている。

その６年後に登場した CryptoLocker とよばれるランサムウェアは、身代金の支払いに暗号資産（仮想通貨）であるビットコインを要求し、暗号資産が身代金の取扱いに悪用される事例を作った。ビットコインが悪用された理由は、一つは、送金プロセスの中で、当事者の身元を匿名化できる性質を利用し、受取主である犯行グループの身元特定を困難にするためである。もう一つは、ビットコインが社会で普及し、より身代金の回収が容易になったためと考えられる。これ以後、ランサムウェアでは暗号資産を要求する手口が模倣されるようになった。

平成 26 年には、CTB-Locker とよばれるランサムウェアが登場し、ランサムウェアの生成技術がなくても、アフィリエイトプログラムへの参加により、誰でも収益を上げることが可能になった。アフィリエイトとは、ランサムウェアの生成や実行の基盤を提供して、実行役の参加者を募集する仕組みのことをいう。参加者はこのプログラムに参加して、実行基盤からランサムウェアをダウンロードし、被害者に送りつけてマルウェアに感染させ、身代金の支払いに応じさせた場合には、その実行役には身代金の７～８割程度を分配し、CTB-Locker の提供元には身代金の２～３割程度が入る仕組みになっている。これにより、実行役は、ランサムウェアに関する IT の詳細な知識がなくても、例えばメールで相手方をマルウェアに感染させることによって、収益を上げることができるようになった。

平成 27 年には、GandCrab とよばれるランサムウェアが登場し、感染パソコンの一覧や暗号化ファイルの数などの進捗状況を一元管理できるようになり、実行役の管理コストが効率化された。こうした仕組みは RaaS（Ransomware-as-a-Service）とよばれているが、RaaS の特徴として、アフィリエイトと同様、このシステムの提供元が身代金の２～３割程度を徴収する仕組みになっており、ランサムウェアの実行行為を可視化することにより、ゲーム性を高め、実行役を攻撃に加担、熱中しやすいように仕向けている。

令和元年には、Maze を名乗るサイバー犯罪グループによって二重恐喝（ダブルエクストーション）とよばれる手口が登場した。従来型のランサムウェアは、暗号化されたファイルの復号鍵や復号ソフトの購入を強要していたが、現在主流となっている二重恐喝は、ファイルを暗号化する前に盗み出したファイルをランサムウェアグループ自らが運営する暴露サイトを通じて漏出させると脅迫して、このための支払いも暗号化の復号の身代金に加えて要求する手口であ

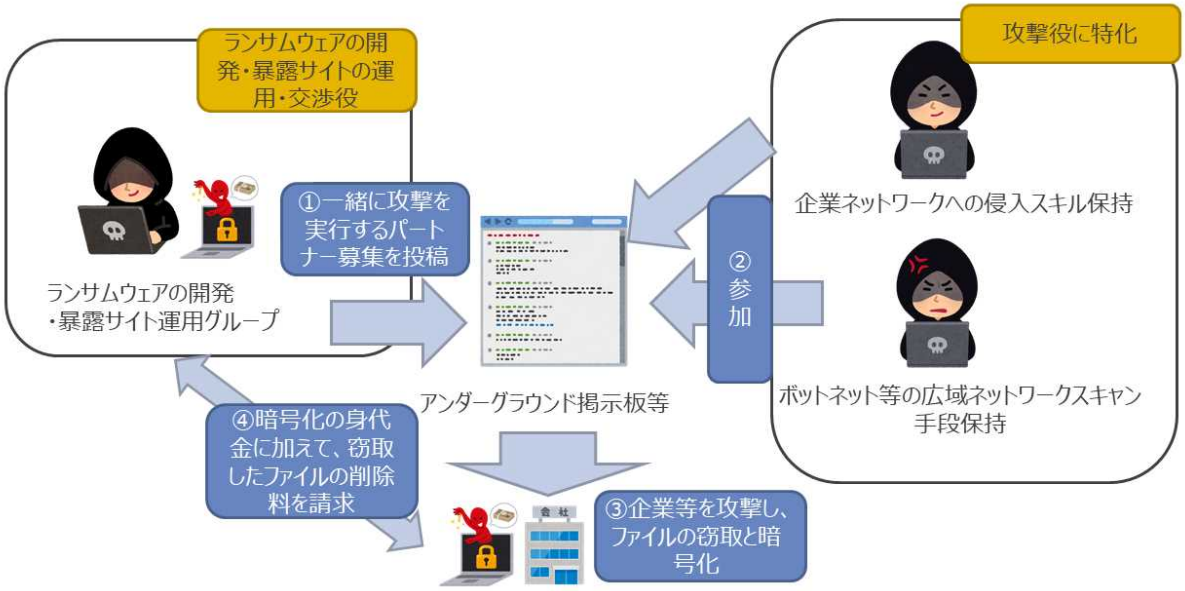
る。図表６は、二重恐喝の時系列推移を示したものであり、同年 11 月から企業の被害が相次いでいることが確認されている[9]。

図表６：二重恐喝の時系列推移

日時	事案
令和元年 11 月	Maze を名乗るサイバー犯罪グループが米国の人材派遣大手に侵入。日本円にして約２億５千万円の身代金を要求するも応じなかったため、盗み出した情報を漏洩。
令和元年 12 月	Maze を名乗るサイバー犯罪グループが二重恐喝に応じなかった企業の情報を漏洩する暴露サイトを立ち上げた。
令和元年 12 月	Maze の手段を模倣し、別のグループが二重恐喝に応じなかった企業の情報を漏洩。これ以降、二重恐喝の手法が常套手段に。
令和２年２月	国内の総合重機大手の海外子会社が CLOP というグループによるランサムウェア攻撃を受けた上、同グループの運営するサイトから内部情報を漏洩された。
令和２年４月	英国の両替会社大手が REvil ランサムウェアの攻撃を受け、復旧のために日本円にして約２億円を支払った。
令和２年５月	米国の大手法律事務所が REvil ランサムウェアの攻撃を受け、有名歌手らの情報を含む情報が漏洩された。
令和２年６月	米国の大学がランサムウェアの被害を受け、復旧のために日本円にして約１億円を支払った。
令和２年７月	国内の金型メーカーがランサムウェアの被害に遭い、情報漏洩が発生。
令和２年８月	政府の登録検定機関がランサムウェアの被害に遭い、情報漏洩が発生。
令和２年８月	国内の大手精密機器メーカーの米国販売会社がランサムウェアの被害に遭い、情報漏洩が発生。
令和２年９月	国内の中堅ゼネコンがランサムウェアの被害に遭い、情報漏洩が発生。
令和２年 10 月	国内の製薬メーカーの台湾現地法人がランサムウェアの被害に遭い、情報漏洩が発生。
令和２年 11 月	国内のゲームソフトメーカーがランサムウェアの被害に遭い、情報漏洩が発生。

[9] 警察庁及び株式会社 NTT データの新井悠氏の調査に基づく。

図表７：最近のランサムウェアグループの生態



図表７は、最近のランサムウェアグループの生態を示したものであり[10]、アンダーグラウンドの掲示板において実行役を募集したり、技術を競うコンテストを実施したりしていることが確認されている。犯罪集団は、こうした取組により実行役を募集し、より優秀な技術を持った人材を集め、自らの活動を活発化させようとしているものと考えられる。

このように、複数の犯罪集団がランサムウェアや犯行手口、実行役を集める取組を相互に模倣することにより、総体的にランサムウェア攻撃が悪質化している実態がある。

ウ　IoT マルウェアの爆発的感染

今後、第５世代移動通信システム（5G）の進展により、IoT（Internet of Things）機器の更なる普及が見込まれるところであるが、IoT 機器もサイバー空間の脅威にさらされている。

その予兆は平成 27 年まで遡る。横浜国立大学では同年から IoT 向けのハニーポット[11]を継続的に運用し、不審なアクセスの観測とマルウェアの捕獲・詳細分析を行っている。同大学の観測によれば、同年４～７月の３か月で、約 15 万台、約 360 種類の感染した IoT 機器が観測された。また、国立研究開発法人情報通信研究機構（NICT[12]）において、ダークネットにおけるリモートアクセ

[10] 株式会社 NTT データの新井悠氏の作成による。
[11] 脆弱な機器を模したおとりシステム。攻撃を受けつつ観測を行うことで不審なアクセスの観測、マルウェアの収集が可能。
[12] National Institute of Information and Communications Technology の略

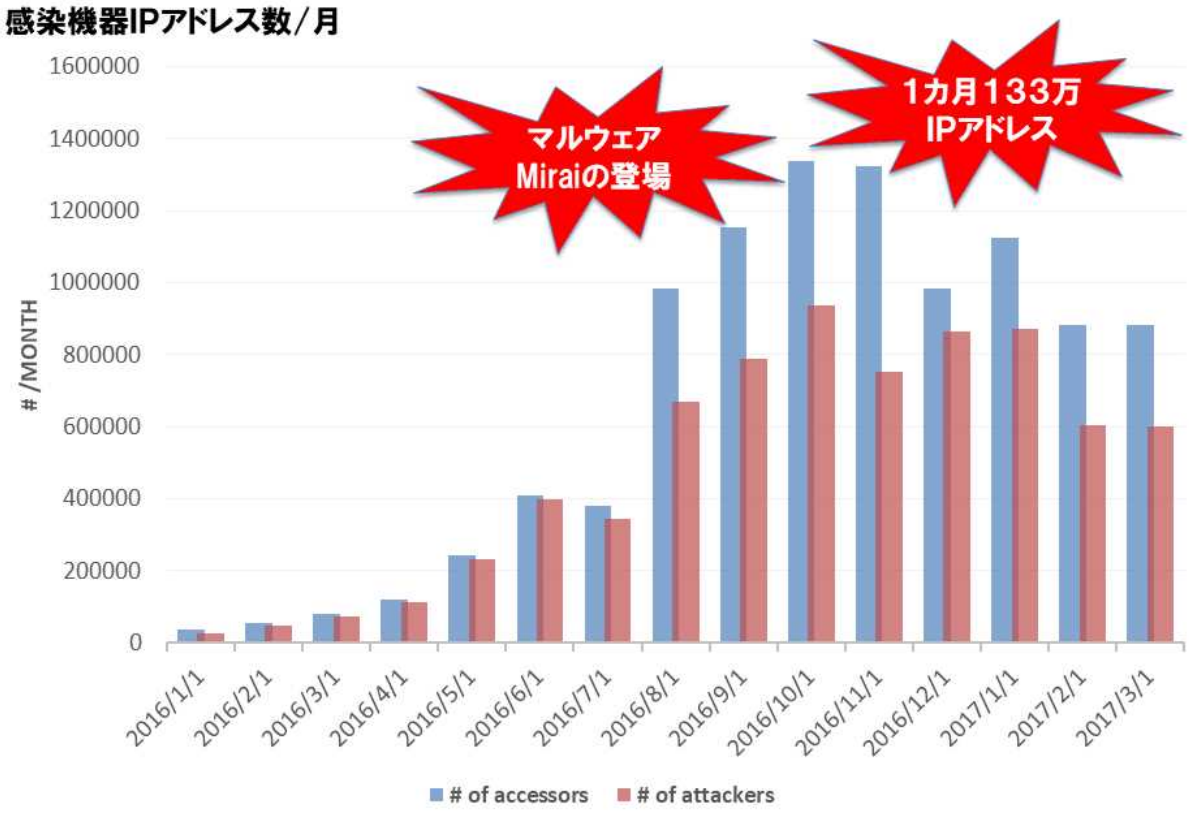
スサービスへの攻撃を観測したところ、同年から攻撃が急増したことが判明した。

平成 28 年には、Mirai とよばれる IoT マルウェアの爆発的感染が観測された。図表８は、同年１月から翌平成 29 年３月までの横浜国立大学における観測結果を示したものである[13]。

このように、平成 28 年 10 月と 11 月は、１か月で約 130 万 IP アドレスからの攻撃を観測した。また、Mirai は、218 の国や地域からの攻撃が観測され、特にアジアと南米の感染が多いなど、世界的な感染が認められた。Mirai の爆発的感染は、世界中の何十万台もの IoT 機器が実際に乗っ取り可能であり、乗っ取った機器を悪用した攻撃が実社会に多大な影響を与える規模の攻撃を起こし得ることを世界中に示す結果となった。このマルウェアのソースコードが一般に流通していることもあり、現在に至るまで、Mirai が次々と攻撃に悪用される事態につながっている。

これを裏付けるように、警察庁における観測においても、平成 28 年８月以降、Mirai ボットの探索行為によるものとみられるアクセス件数が増加し、現

図表８：横浜国立大学における観測結果（平成 28 年１月～平成 29 年３月）



[13] 横浜国立大学の吉岡克成准教授の作成による。

状においても、令和２年のMiraiボットの特徴を有するアクセス件数は１日・１IPアドレス当たり461.7件で、一定数継続的に観測されている[14]。

Miraiによる攻撃の最近の傾向の一つとして、攻撃の高度化が挙げられる。初期のMiraiは、基本的には機器を再起動するとマルウェアが消えたが、最近は持続感染型のIoTマルウェアが増えてきている。これにより、マルウェアが組織のネットワークに侵入したのちに長期の活動が容易になるなど、Miraiによる脅威は深刻さを増している。

３．国家の関与が疑われるサイバー攻撃被害の深刻化

サイバー攻撃の中には、国家が犯罪集団を支援するなど、国家の関与が疑われるものがあり、その被害やリスクが深刻化している。

例えば、令和２年５月、米国は、中国と関連のあるサイバー攻撃集団が、新型コロナウイルス感染症関連情報の不正取得を試みていたとして、中国に対し悪意ある活動を中止するよう求めた。

また、同年７月、米国、英国及びカナダは、新型コロナウイルス感染症に関連する研究及びワクチン開発に関連して、APT29（Cozy Bear, The Dukes）[15]とよばれるサイバー攻撃集団が研究情報及び知的財産を窃取しようとしているとして、注意喚起を行った。APT29は、ロシアの諜報機関に属する集団であることが確実視されており、政府機関、医療機関等を標的としてサイバー攻撃を行っているとされる。

さらに、同年12月、米国の大手ITインフラ管理ソフトウェア会社の顧客に密かにサイバー攻撃が仕掛けられ、同社のソフトウェアを利用していた米国の政府機関のメールがサイバー攻撃集団に傍受された可能性が判明したが、この攻撃について、FBI[16]等の米国の政府機関は、ロシアによるものとしている。

このように、国家の関与が疑われるサイバー攻撃の被害が深刻化しており、諸外国との連携強化はもちろんのこと、官民が連携した対策が急務となっている。

---

[14] 警察庁の発表による。

[15] ロシアの国家的関与が疑われているサイバー攻撃集団。APT攻撃（Advanced Persistent Threat：高度で持続的な脅威）とよばれるサイバー攻撃を実行する集団は世界中で確認されており、セキュリティベンダー等が命名した名称で一般に呼称されている。APT攻撃を実行するサイバー攻撃集団には国家の関与が疑われるものが多く存在する。

[16] Federal Bureau of Investigation（米国司法省連邦捜査局）の略

第２章　今後のサイバーセキュリティに求められる新たな基本理念

１．新たな基本理念：公共空間としての安全性確保

コロナ禍による社会経済活動の変容は、サイバー空間の新たな脅威を顕在化させ、令和２年に大きな社会問題となったキャッシュレス決済サービスの不正振替のように深刻な被害が生じているものもある。また、コロナ禍の前より確認されていたフィッシングやマルウェア攻撃の犯行手口等は悪質化し、国家の関与が疑われるサイバー攻撃の被害も深刻化しており、サイバー空間の安全確保は、国民にとって喫緊の課題となっている。

デジタル社会の実現について、政府は、そのビジョンとして「デジタルの活用により、一人ひとりのニーズに合ったサービスを選ぶことができ、多様な幸せが実現できる社会」を掲げ、このような社会を目指すことは、「誰一人取り残さない、人に優しいデジタル化」を進めるということにつながるとしており、今後、サイバー空間は、地域や老若男女問わず、全国民が参画し、重要な社会経済活動を営む、これまで以上に重要かつ公共性の高い場へと変貌を遂げていくものと考えられる。また、政府は、デジタル社会を形成するための基本原則に「安全・安心」を掲げ、「デジタルで生涯安全・安心に暮らせる社会を構築すること、サイバーセキュリティ対策で安全性を強化すること、デジタル技術の善用、個人情報の保護、不正利用の防止を進めること等により、デジタル利用の不安を低減し、安全・安心なデジタル社会を目指す」としている[17]。

このように、サイバー空間が、重要な社会経済活動を営む公共空間[18]へと変貌を遂げつつある一方で、令和２年９月に警察庁が実施したアンケート調査[19]によると、回答者の 75.3%がサイバー犯罪に不安を感じると回答するなど、サイバー空間に対する国民の不安感は払拭されていない状況にある。

こうした目下の厳しい脅威情勢や今後の我が国に到来するデジタル社会の実現に適切に対処していくためには、サイバー空間に、公共空間として実空間と変わらぬ安全・安心が確保されることが必要である。すなわち、全国民が、心置きなくデ

---

[17] 「デジタル社会の実現に向けた改革の基本方針」（令和２年 12 月 25 日閣議決定）

[18] サイバー空間を「コンピュータ（端末）、これらをつないだネットワークから構成され、情報の交換、蓄積ができる空間」として考えると、サイバー空間の構成要素は、民間が管理、運営していることとなる。このように私有財産の集積として構成されるサイバー空間を「公共空間」と表現することには議論があろうが、昨今のデジタル化の進展等により、サイバー空間は、公共空間としての役割を果たすことが求められるようになってきていることを踏まえ、本報告書においては「公共空間」と表現することとしている。

[19] 全国の 15 歳以上の男女１万人を対象に、年代別・性別・都道府県別の回答者数の割合が平成 27 年国勢調査の結果に準じたものとなるようインターネットを通じて実施したもの。

ジタル社会におけるあらゆる活動に参画し、個々の能力を創造的かつ最大限に発揮するとともに、生活の利便性向上や個性豊かで活力に満ちた地域社会の実現を通じて、ゆとりと豊かさを実感できるようになることが求められており、こうした誰もが安心して参画できる空間を実現するため、今後のサイバーセキュリティにおける新たな基本理念に、「公共空間としての安全性確保」を据えることが必要である。

２.「公共空間としての安全性確保」の実現に必要な２つの観点

新たな基本理念である「公共空間としての安全性確保」を実現するためには、次の２つの観点から検討を行うことが必要である。

(1) 犯罪対策と安全保障を一体として捉えた包括的対策の必要性

サイバー犯罪やサイバー攻撃への対策について、警察では、違法行為に対する捜査を推進するとともに、被害を受けたコンピュータや使用されたマルウェアを解析し、その結果や犯罪捜査の過程で得た情報等を総合的に分析するなどして、攻撃者及び手口に関する実態解明を進めている。また、各国治安情報機関との情報交換を行うとともに、国際刑事警察機構（ICPO[20]）を通じるなどして、外国捜査機関との間で国際捜査協力を積極的に推進している。

他方で、令和２年７月には、米国、英国及びカナダにより、APT29 とよばれるサイバー攻撃集団による新型コロナウイルス感染症関連のサイバー攻撃に関する注意喚起が行われたほか、同年 12 月、サイバー攻撃集団により米国政府のメールが傍受された可能性が指摘されるなど、世界中で国家の関与が疑われるサイバー攻撃の被害が深刻化している。

こうした厳しい情勢の下、サイバー空間に、公共空間としての安全性を確保するためには、犯罪対策の観点からだけでは十分なアプローチが難しく、警察においても国家安全保障の観点からのアプローチを強化する必要に迫られている。また、こうした国家の関与は一見して明らかなものではなく、高度な分析を通じて明らかとなるものであり、警察においては、犯罪対策と安全保障を一体として捉え、包括的な対策を講じていくことが求められている。

(2) サイバーセキュリティを担う各主体による地道な活動の積み重ねの重要性

新型コロナウイルス感染症の感染拡大により、国民一人一人に新たな生活様式が求められるようになるなど、個人レベルでの公衆衛生の実践が、社会にとっていかに重要なものであるかを再認識することとなった。サイバー空間においても、実空間の公衆衛生に対応するサイバー・ハイジーン（Cyber Hygiene）とよばれる考え方があり、例えば、ソフトウェアに適切にパッチが適用されているかを

[20] International Criminal Police Organization の略

確認する、定期的にデータのバックアップを取得するといった基本的な行動に平時から取り組むことをいう。欧州ネットワーク・情報セキュリティ機関（ENISA[21]）では、サイバー・ハイジーンを、個人の公衆衛生にならい、組織のネットワーク環境が最適な状態を維持できるよう、単純な日常業務、良好な習慣及び定期的な確認を組織的に行うことと定義し、これにより、被害や被害拡大を最小限に抑えることができるとしている[22]。

社会において、サイバーセキュリティを担う取組主体は多岐にわたる。サイバー空間を構築している各種インフラ事業者、多様なサービスを提供する事業者、専門的な研究・教育を担う学術研究機関、サイバー犯罪やサイバー攻撃の取締り、抑止等に取り組む警察など、産学官の各主体がそれぞれの強みを活かして対策に取り組んでいる。また、サイバー空間に参加する各個人も、その脅威から自らを守るための主体的な取組が求められるという意味では、サイバーセキュリティを担う重要な取組主体である。

サイバーセキュリティは、こうした様々な取組主体による地道な活動の積み重ねから構築されるものであり、サイバー空間に、公共空間としての安全性を確保するためには、各主体がサイバー・ハイジーンを実践することが重要である。

[21] European Network and Information Security Agency の略
[22] ENISA「Review of Cyber Hygiene practices」（平成 29 年２月７日公表）

第Ⅱ部　各論

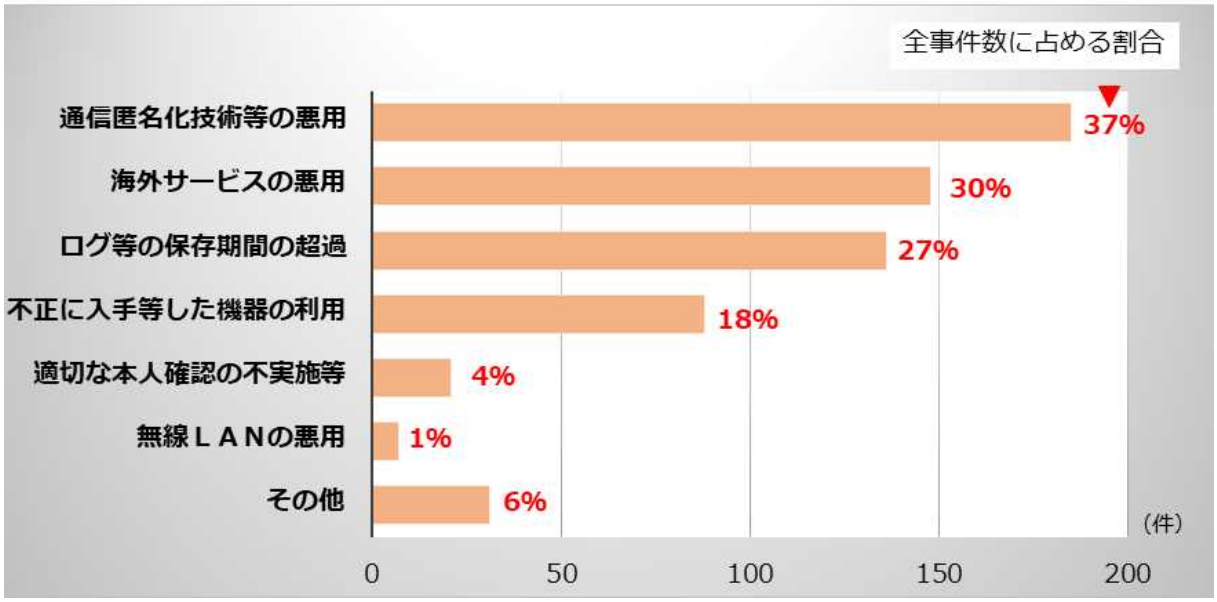
第１章　犯行主体の特定を通じた犯罪対策・安全保障

１．課題

警察における実空間の治安改善に向けた取組については、刑法犯認知件数が減少傾向にあり、重要犯罪が検挙されるなど、一定の成果を上げてきた一方で、サイバー空間の脅威情勢は依然として厳しく、令和２年９月に警察庁が実施したアンケート調査においても、回答者の 75.3％がサイバー犯罪に不安を感じると回答している。このように、国民はサイバー空間に安全・安心がもたらされることを期待しており、犯行主体の特定を通じてサイバー犯罪やサイバー攻撃の取締り等を行う警察は、我が国のサイバーセキュリティの確保において、極めて重要な役割を担っている。

しかしながら、サイバー空間における犯行主体の事後追跡には、依然として困難がつきまとう。図表９は、警察庁においてサイバー犯罪捜査における事後追跡上の課題を調査した結果の分析であり[23]、通信匿名化技術等の悪用、海外サービスの悪

図表９：サイバー犯罪捜査における事後追跡上の課題



[23] 昨年６月、警察庁から都道府県警察に対して実態調査を実施し、令和元年中に認知した各都道府県警察本部のサイバー犯罪対策担当課が管理しているサイバー犯罪事件であって、事後追跡上の課題となったものについて分析を行ったもの。

用[24]、ログ等の保存期間の超過、不正に入手等した機器の利用、適切な本人確認の不実施等が課題として判明している。

こうしたサイバー犯罪捜査における一般的な課題に加えて、インターネットバンキングに係る不正送金事犯や暗号資産をめぐる事件など、警察による取締りが特に期待される重大なサイバー犯罪事件は、大規模な犯罪組織による敢行が推認されており、犯行組織の実態解明の観点から高度な分析が必要となる。また、サイバー空間においては、国家と個人が同じ土俵で活動を行うこととなり、特に国家を背景としたサイバー攻撃等に対しては、その抑止等を公的機関の責務・役割として全うすることが求められる。こうした課題に対するアプローチとして、犯行主体やその手口、目的を特定する活動（アトリビューション）も必要不可欠である。

昨今、サイバー空間をめぐる脅威の特徴として、攻撃者の優位性や抑止の困難性ばかりが強調され、こうした認識の下、現状の対策においては、被害者側のリテラシー不足が殊更に課題として取り上げられ、どうしても犯行主体への対策の観点が欠けてしまう傾向にある。参加主体の更なる拡大が予想される今後のサイバー空間に、実空間と同様の法の支配を実現するため、あらためて法治国家として犯罪の行為者に帰責する健全な社会認識の必要性が確認されるとともに、警察における犯人の事後追跡可能性の向上やアトリビューションの強化・活用に取り組むことが必要である。

２．会議における主な意見

(1)　会議では、事後追跡可能性の向上に関して、次のような意見があった。

- 事後追跡可能性について警察としてどこまでできるのかを整理することが必要ではないか。
- 事後追跡の課題の中には国民の理解が必要なものもあることから、犯罪捜査の障害となっている事項について、国民が見える形で議論を進めていくことが必要ではないか。
- SMS 認証代行業が犯罪の温床となっており、これへの対策を講じるべきではないか。
- SMS 認証代行を通じた不正なアカウント作成やProxyGate[25]等犯罪者を幇助する技術への対応が必要ではないか。

---

[24] 犯人が海外のサービスを犯行に悪用していた場合、外国捜査機関等に協力を求め、国際捜査を行うが、一般に国際照会に数か月以上の期間を要したり、有益な回答が得られなかったりする場合があり、犯人の特定が困難となる。

[25] プロキシサービスの一種。有料ソフトウェアのライセンス認証の回避を騙るソフトウェア

・　捜査において、いかなるログが必要か、それはどこに照会すればよいか等について、事業者と連携した上で必要な資料化をして現場で活用できるようにするとともに、新たな犯罪の形態・手口が出た場合は、それに応じて逐次更新するなどして、捜査の合理化・効率化を図るべきではないか。

(2)　会議では、アトリビューションの強化に関して、次のような意見があった。

・　米国の国際政治学者であるトマス・リッドらは、アトリビューションのシステマティックなモデルにおいて、犯行主体の特定と動機の解明に取り組む戦略的分析（strategic）、犯行主体の属性の解明に取り組む作戦術的分析（operational）及び技術的な側面に取り組む戦術的分析（tactical）の３層の連携を提唱しているが[26]、このうち、戦略的分析と戦術的分析を結び付ける作戦術的分析を担う人材を国として育成していくことが必要ではないか。また、政府において作戦術的分析を担う人材の育成を強化するため、数年ごとに、大学院、政府機関、民間企業と勤務先を変えていくキャリアパスを構築すべきではないか。

・　リバースエンジニアリング[27]等高度な技術を必要とするアトリビューションを実施できる技術者を官民で育成していく必要があるのではないか。

・　犯人グループの上位層の検挙に向けて、攻撃グループに関する情報収集・分析、都道府県警察への共有等の体制を強化すべきではないか。

・　犯行主体の特定に資する新たな捜査手法についても検討を進めていくべきではないか。

・　アトリビューションの強化のため、国内外の関係機関との連携を深めることが必要ではないか。

・　我が国として、米国、イギリス、オーストラリア、インドといった国々との連携が重要ではないか。

・　海外捜査機関と双方向的かつリアルタイムな情報共有等を能動的に実現していくことが重要ではないか。

等のダウンロード時に、改変されたProxyGateプログラムが同時にダウンロードされ、不正アクセス等の踏み台として悪用される事例が多数確認されている。

[26] トマス・リッド、ベン・ブキャナン（土屋大洋訳）「サイバー攻撃を行うのは誰か」『戦略研究』第18号、平成28年５月、59～98頁

[27] ソフトウェアやハードウェアなどを解析・分解し、その仕組みや仕様、目的、要素技術などを明らかにすること

(3)　会議では、アトリビューションの活用に関して、次のような意見があった。

- 健全な法治国家として行為者に帰責する健全な風潮を醸成するためにも、アトリビューションを強化するだけではなく、その成果を広報啓発や被害防止に積極的に活用することを検討すべきではないか。
- 警察や各企業が連携してアトリビューションを行い、被疑者の検挙や犯罪被害の未然防止に活用していくことが重要ではないか。
- 様々な犯罪が複合的に敢行される、又は、組織的に敢行されるサイバー犯罪やサイバー攻撃に対しては、その手口、被害実態を全体的に把握することにより、犯罪グループの実態を解明し、取締りや対策へ活用することが必要ではないか。

３．今後の取組の方向性

今後のサイバー空間において、法治国家として犯罪の行為者に帰責する健全な社会認識の必要性が再確認され、警察における犯人の事後追跡可能性の向上やアトリビューションの強化・活用を図るため、次の取組が必要である。

(1)　事後追跡可能性の向上

ア　犯罪インフラを提供する悪質事業者の摘発強化

サイバー空間における警察の事後追跡を困難にし、犯罪行為を容易にする、いわば犯罪インフラを提供する悪質な事業者の存在が確認されている。

例えば、次の事例①は、SMS 認証代行の検挙事例である。SMS 認証代行とは、通信当事者以外の第三者が、SMS 認証[28]に用いる携帯電話番号や当該認証に係る認証コードを当該通信当事者に提供する行為のことをいう。

【事例①】

埼玉県警察は、IP 電話アプリの電話番号取得時に必要となる SMS 認証に用いる携帯電話番号や当該認証に係る認証コードを提供した無職の男を、令和２年７月に私電磁的記録不正作出・同供用で検挙した。

本件では、本人確認が行われていない SMS 機能付きデータ SIM が犯行に用いられ、契約者情報による被疑者の特定ができなかったが、別の捜査過程で被疑者の特定に至ったもの。

捜査の過程において、この男は、携帯電話番号や認証コードを提供するため、約 100 枚ものデータ SIM を悪用しており、これにより取得された電話番号の一

[28] SMS（ショート・メッセージ・サービス）を利用して顧客等の携帯電話に認証コードを送信し、当該コードを使用した認証を行う方式

部が、IP 電話アプリを用いて特殊詐欺に悪用されていたことが明らかになっている。

SMS 認証は、ID・パスワードによる認証と併用することにより、認証の安全性を高める方法として広く使用されており[29]、SMS 認証代行は、それ自体がサイバー空間における本人確認の信頼性を貶める悪質な行為であり、特殊詐欺等に必要な犯行ツールを提供する犯罪インフラにもなっている。

また、次の事例②は、中継サーバを運営する事業者の検挙事例である。

【事例②】

茨城県警察は、電気通信事業法（昭和 59 年法律第 86 号）に基づく届出をせずに中継サーバを運営した中国籍の女を、令和元年５月に同法違反（無届営業）で検挙した。この事件で使用された中継サーバは、不正送金に悪用されていたほか、解析の結果、不正に入手したとみられる１億件以上の他人の ID・パスワードや複数の未知の攻撃プログラムが保管されていたことが判明した。

各種サービスにおけるセキュリティ対策の一環として、海外からのアクセスを遮断する取組があるが、こうしたアクセス制限の回避を目的で日本に設置された中継サーバが利用されるケースが確認されている。中継サーバ事業者が運営するサービスの中には、ログをあえて残さないなど、犯罪インフラと化しているものがある。

このように、犯罪インフラを業として提供する事業者が後を絶たず、サイバー犯罪を容易にしている実態を踏まえ、警察においては、官民の情報を活用しながら、こうした悪質な事業者の摘発を強化していくべきである。

イ　捜査の合理化・効率化に向けた取組

事後追跡可能性を確保するためには、各事業者のシステムから得られる事後追跡可能な情報等を踏まえつつ、現場のニーズを踏まえた地道な取組が必要である。例えば、捜査において、いかなるログが必要か、それはどこに照会すればよいのか等といった現場のニーズを踏まえ、官民が連携して資料化に取り組み、現場で活用できるようにするとともに、新たな犯罪の形態、手口が出た場合には、それに応じて逐次更新する等の取組が必要である。捜査の合理化・効率化に向けて、こうした地道な取組を不断に続けていくべきである。

(2)　アトリビューションの強化と戦略的な活用

サイバー空間の脅威の軽減・無効化を図るためには、各主体が連携してアトリビューションを行い、着実に対策を進めることが重要であるが、現状では、警察

[29] 30～32 頁参照

や民間事業者は、現象面への対応に追われ、中長期的な対策を十分に進めることができていない。

こうした現状を打破し、我が国のアトリビューションのレベルを引き上げ、その成果を活用した抑止・検挙・広報啓発を強力に展開するため、警察が総力を結集してアトリビューション体制の充実強化を図るとともに、警察が有する権限の効果的な活用や犯行主体の特定に資する新たな捜査手法についても研究を進めていくべきである。

また、アトリビューションの強化に向け、関係省庁や一般財団法人日本サイバー犯罪対策センター（JC3[30]）との連携を強化するとともに、複数国の当局等によりEmotetのボットネットに対する共同オペレーションが実施されたように[31]、海外捜査機関との連携を個別具体のオペレーションのレベルで強化することを含め、国際連携のより一層の推進を図るべきである。

さらに、今後のサイバー空間において、犯罪の行為者に帰責する健全な社会認識の必要性が再確認されるよう、アトリビューションによって判明した犯行手口や犯罪者の動向等の情報を、国民に積極的に発信していくべきである。

[30] Japan Cybercrime Control Centerの略。我が国における新たな産学官連携の枠組みとして、平成25年度総合セキュリティ対策会議における議論を経て設立され、平成26年から業務を開始した。JC3においては、産学官の情報や知見を集約・分析し、その結果等を還元することで、脅威の大本を特定し、これを軽減及び無効化することにより、以後の事案発生の防止を図ることとしている。警察では、捜査関連情報等をJC3において共有し、産学におけるサイバーセキュリティに関する取組に貢献するとともに、JC3において共有された情報を警察活動に迅速・的確に活用している。

[31] ６、７頁参照

第２章　健全なサイバー空間の実現に向けた各主体による取組

１．課題

社会において、サイバーセキュリティを担う取組主体は多岐にわたる。サイバー空間を構築している各種インフラ事業者、多様なサービスを提供する事業者、専門的な研究・教育を担う学術研究機関、サイバー犯罪やサイバー攻撃の取締り、抑止等に取り組む警察など、産学官の各主体はもちろん、サイバー空間に参加する各個人も、その脅威から自らを守るための主体的な取組が求められる重要な取組主体である。

サイバーセキュリティは、こうした様々な取組主体による地道な活動の蓄積から構築されるものであり、サイバー空間に、公共空間としての安全性を確保するためには、各主体がサイバー・ハイジーン[32]を実践し、健全なサイバー空間を実現することが重要である。

しかしながら、健全なサイバー空間の実現には、取組主体ごとに多くの課題が残る。産学官の各主体においては、連携の必要性や重要性については、既に共通認識となっているものの、実効性のある体制の構築や全国的な活動の充実が課題である。また、各個人においては、厳しい脅威情勢の下、サイバー空間に対する不安感が未だに払拭されていない状況にありながら、個人レベルでの具体的な対策は十分に行われておらず、サイバー空間の脅威から自らを守るリテラシーの普及が必要である。こうした課題を解決するため、各主体に求められる具体的取組やこれを促すための警察の関与・支援の在り方について検討する必要がある。

２．会議における主な意見

(1)　会議では、サイバーセキュリティを担う取組主体である事業者や個人に求められる取組に関して、次のような意見があった。

- 犯罪者は常に新しい攻撃手法を考えてくるため、サービスを提供する事業者等としては、「不正利用は起こる」と考えて、常に攻撃から守る対策を導入し、備える必要があるのではないか。
- キャッシュレス決済サービスの不正振替対策について、アカウント開設時の本人確認だけでなく、取引時確認についてもリスクベース・アプローチで実施することが必要ではないか。

[32] 14、15 頁参照

・　フィンガープリンティング[33]の活用等、事後追跡性を向上させるために事業者において取り得る方法の検討・働きかけをすることが必要ではないか。
・　ソフトウェアのアップデート、二経路認証の活用等基本的な対策をユーザ側に促すことが必要ではないか。
・　ユーザ側において怪しいメールを開かない、怪しいサイトに情報を入力しないといった基本的対策を行うことが重要ではないか。
・　フィッシング詐欺対策では、自らの専門的な知識や経験、技能を社会貢献のために無償又は無償に近い形で活動を行っている技術者が数多く存在しており、こうした活動を後押しする取組が必要ではないか。

(2)　会議では、警察の公的機関としての関与・支援の在り方に関して、次のような意見があった。
・　捜査その他の警察活動に支障の生じない形で、時宜を得た情報発信を行っていくべきではないか。
・　警察は、刑事訴訟法（昭和 23 年法律第 131 号）第 47 条との関係から、捜査情報を活用した情報発信に慎重になる傾向があるが、判例を踏まえると、サイバーセキュリティの確保を目的とする情報発信について、もっと積極的に行ってよいのではないか。
・　組織犯罪として敢行されるサイバー犯罪や国家の関与が疑われるサイバー攻撃の実態を効果的に発信するなど、サイバー空間の利用者にも攻撃者のイメージを持たせ、一般国民と危機感を共有すべきではないか。
・　ランサムウェアについて、インシデント発生時の対応ガイドラインを警察において取りまとめるとともに、被害企業の相談窓口の整備を進め、啓発していくことが必要ではないか。
・　技術的なセキュリティ対策は、サイバー空間の具体の脅威に応じて講じ得る対策が変わる一方で、一般利用者がサイバー空間を利用する際に注意すべき事項は、「アクセスする前に、立ち止まって何が起こるかを考えること」と普遍的であり、この点を広く啓発していくことが重要ではないか。
・　マルウェアの存在だけではなく、それを作った人、使っている人がいるということも意識させることが必要ではないか。
・　IoT マルウェアが重要インフラを攻撃対象としているといった事実を、統計とともに広く関係者に周知することで、問題の深刻さを伝えていくことが必要ではないか。
・　SNS と連携した国民の意識調査を実施してみてはどうか。

[33] サービスにアクセスしてくる端末の特徴を割り出し、個々の端末を識別する技術

・　同じメッセージ、ロゴマーク、ブランドカラーを使い続けるなど、啓発活動の認知度を高める工夫が必要ではないか。
・　消費者や中小企業に対するリテラシーの普及が必要ではないか。
・　学校教育のオンライン化によって友人の間で気軽に相談できなくなり、不審メール等もつい信頼してしまうといった話もあることから、社会経済活動のオンライン化も踏まえた対策を検討すべきではないか。
・　ランサムウェア攻撃の実行犯募集の取組のように、青少年がサイバー犯罪に手を染めることのないよう啓発活動を充実させていくことが必要ではないか。
・　サイバーセキュリティの実効性のある体制構築や全国的な活動の充実には、全国に存在し、企業の大多数を占める中小企業へのアプローチが必要ではないか。
・　現場レベルで施策を実行できる体制を持ち、業種にとらわれず事業者全体に働きかけることができる都道府県警察の特色を活かす方策を検討すべきではないか。
・　各都道府県警察のサイバーセキュリティに関する連携組織について、グッドプラクティスを共有するとともに、活動に協力する研究者等の確保や共同事業の実施を促進すべきではないか。
・　産学官連携を強化するためには、警察や民間事業者から、学術機関の研究に必要な実データを提供することが必要ではないか。
・　産学官連携の一環として行う情報共有について、情報の提供先ごとに情報提供の必要性や情報管理の安全性を吟味した上で情報の提供範囲を定めることが必要ではないか。
・　防御の効率という観点からすれば、攻撃者側の使っている情報を官民で情報共有する方途の可能性についても検討できないか。

３．今後の取組の方向性

健全なサイバー空間の実現に向けた各主体におけるサイバー・ハイジーンの実践を促すため、各主体に求められる具体的取組や警察の公的機関としての関与・支援として、次の取組が必要である。

(1)　事業者や個人における取組の促進

ア　キャッシュレス決済サービスの不正振替事案を踏まえた対応

令和２年に大きな社会問題となったキャッシュレス決済サービスの不正振替事案は、銀行口座とキャッシュレス決済サービスのアカウントを連携させ、当該アカウントから口座振替を可能とするシステムが悪用されたものである。今般の事案を踏まえ、金融庁においては、銀行と資金移動業者等に対して、不

正防止策の実施[34]、補償方針の策定・実施及び利用者相談に真摯に対応するための態勢整備を要請した。

当該要請を踏まえ、一般社団法人全国銀行協会と一般社団法人日本資金決済業協会は、被害の速やかな補償も含め、本事案に対応するための業界指針を策定・公表した[35]。また、金融庁においても、当該要請に係る事項等を監督上の評価項目に盛り込むため、監督指針等を改正した。

こうした一連の対応を踏まえ、今後とも、関係事業者において利用者保護の観点から適切な対応が講じられるよう働きかけていくとともに、官民が連携して被害抑止に取り組んでいくべきである。

イ　リスクベース・アプローチに基づく民間事業者の自主的な取組の促進

キャッシュレス決済サービスのように、サイバー空間では、複数のサービスを連携させることにより利用者に新たな価値を提供するものが増えてきており、この場合には、法規制により求められている最低限の安全確保措置だけでは十分ではない場合も考えられる。

こうしたサービスを提供する民間事業者は、マネー・ローンダリング及びテロ資金供与対策におけるリスクベース・アプローチ[36]にならい、それぞれ連携して、自らが提供しているサービスに係るリスクを適切に評価し、必要な自主規制やモニタリング等の措置を検討・実施することが期待されており、官民が連携してこうした取組が促進されるよう働きかけていくべきである。

ウ　国民一般に対する基本的なリテラシーの普及

サイバー・ハイジーンの重要性を踏まえ、国民一般がサイバー空間の脅威に対して正しく危機意識を持つことができるよう、サイバー空間に参加する際の基本的なリテラシーやサイバー空間の脅威について、官民が連携して広報啓発を進めていくべきである。

---

[34] 金融庁が、銀行と資金移動業者等に求めた不正防止策は、具体的に次のとおりである。
① 相手方の認証方式を含めたリスクの検証、役割・責任の明確化
② リスクに見合った適切な認証方式の導入（銀行による認証の強化、資金移動業者による本人確認の強化等の実施）
③ 口座振替契約時の預金者への通知
④ 既存の口座振替契約の中に不正に締結されたものが残っている可能性を踏まえた不正防止策の実施
⑤ 不正が疑われる取引の適切なモニタリング

[35] 一般社団法人全国銀行協会「資金移動業者等との口座連携に関するガイドライン」（令和２年 11 月 30 日策定）、一般社団法人日本資金決済業協会「銀行口座との連携における不正防止に関するガイドライン」（資金移動業：令和２年 12 月３日策定、前払式支払手段：令和３年１月 28 日策定）

[36] 金融機関等が、自らのマネロン・テロ資金供与リスクを特定・評価し、これを実効的に低減するため、当該リスクに見合った対策を講ずること

エ　プロボノ活動の支援

プロボノ活動とは、ボランティア活動の一種で、ボランティア活動の中でも特に、普段は専門家として稼働している人が、その専門スキルや経験を活かして行うものをいう。サイバー空間には、自らの専門的な知識や経験、技能を活かして社会貢献のために無償又は無償に近い形で活動を行っている技術者が数多く存在する。こうした技術者のプロボノ活動を支援するための取組を、官民が連携して推進していくべきである。

(2)　公的機関としての関与・支援

ア　警察による情報発信の強化

サイバー犯罪やサイバー攻撃の実態把握については、官民で様々な取組が行われているが、警察では、捜査活動により犯罪の全体像を解明する中で、その具体的な方法・手口を把握し、各種システム・事業の脆弱性やリスクを知り得る場合がある。犯罪に悪用されるリスクの高いインフラ、技術など、警察捜査の過程で判明した情報を官民で情報共有することについては、サイバーセキュリティの確保の観点から高い公益性が認められるところであり、警察として積極的に情報発信を行うとともに、民間事業者に対して積極的な働きかけをしていくべきである。こうした取組により、国民一般に攻撃者のイメージを持たせ、適切に危機感を共有するとともに、行為者に帰責する健全な社会認識を醸成していくことが期待できる。

また、サイバー空間の特色として、物理空間の制約がなく、短期間、短時間で攻撃が行われ、被害が一気に拡大する傾向があるため、早期の注意喚起が予防策として有効である。警察では、被害相談の形で被害の初期段階の情報を把握できる場合があることから、被害相談の情報を活用し、時宜を得た情報発信を行う方策を検討していくべきである。

なお、警察が情報発信をしていく上で課題となるのが、刑事訴訟法第 47 条との関係をどのように整理するかである。同条は、その本文において、「訴訟に関する書類は、公判の開廷前には、これを公にしてはならない」と定め、そのただし書において、「公益上の必要その他の事由があって、相当と認められる場合は、この限りでない」と定めている。刑事司法手続の一翼を担う警察では、その取扱いに関して慎重な対応が期されてきたところであるが、判例を踏まえると、サイバーセキュリティの確保の観点から高い公益性が認められる情報発信について、関係者の名誉、プライバシーの侵害や捜査、公判への悪影響などの弊害がないかが適切に確認されており、かつ、発信した情報が適切に取り扱われる環境が整っていると認められる場合においては、警察による捜査関連情

報の発信も許容されるものと考えられる[37]。

イ　子供や高齢者を対象とした安全教育の拡充

総務省の調査によれば､インターネット利用者の割合が全体の 89.8%と９割に迫っており、特に６～12 歳及び 60 歳以上の年齢層での利用割合が大きく伸びている[38]。このように、デジタル化の進展に伴い、サイバー空間の参加主体は拡大を続けており、特に利用者が大きく増加している子供や高齢者に対する啓発活動を充実させていく必要がある。子供や高齢者に対する啓発活動について、特殊詐欺の被害防止や交通安全を目的とする啓発活動においては、様々な創意工夫を凝らした取組が行われている。サイバー空間におけるリテラシーの普及についても、こうした取組を参考にしながら、学校教育の場や地域のコミュニティの場など、あらゆる機会を通じてリテラシー普及を推進することにより、子供や高齢者に対する安全教育を充実させていくべきである。

ウ　都道府県警察の体制を活用した地方の中小企業に対する支援

我が国全体でのサイバーセキュリティ確保のためには、全国に存在し、企業の大多数を占める中小企業へのアプローチが特に重要である。サプライチェーンリスクの観点等から経済界等様々な主体においても対応が取られはじめているが、全国一帯をカバーし、特定の方向性を示した場合、現場レベルにおいて当該施策を実行できる体制を持ち、業種にとらわれず事業者全体に働きかけることができる都道府県警察の特色を活かす方策を検討すべきである。

具体的には、既に各都道府県警察においては、サイバーセキュリティに関する協議会等の連携組織が立ち上がり、情報共有等が図られているが、その実効性を高めるために、警察庁から各都道府県警察に対してグッドプラクティスを共有するとともに、都道府県警察においては、活動に協力するセキュリティ研究者等の確保や共同事業の実施といった取組等が考えられる。

---

[37] 最決平成 16 年５月 25 日民集第 58 巻５号 1135 頁は、刑事訴訟法第 47 条について、「同条本文が「訴訟に関する書類」を公にすることを原則として禁止しているのは、それが公にされることにより、被告人、被疑者及び関係者の名誉、プライバシーが侵害されたり、公序良俗が害されることになったり、又は捜査、刑事裁判が不当な影響を受けたりするなどの弊害が発生するのを防止することを目的とするものであること、同条ただし書が、公益上の必要その他の事由があって、相当と認められる場合における例外的な開示を認めていることにかんがみると、同条ただし書の規定による「訴訟に関する書類」を公にすることを相当と認めることができるか否かの判断は、当該「訴訟に関する書類」を公にする目的、必要性の有無、程度、公にすることによる被告人、被疑者及び関係者の名誉、プライバシーの侵害等の上記の弊害発生のおそれの有無等諸般の事情を総合的に考慮してされるべきものであり、当該「訴訟に関する書類」を保管する者の合理的な裁量にゆだねられているものと解すべきである」と判示している。

[38] 総務省「通信利用動向調査」（令和２年５月 29 日公表）

また、中小企業に対して様々な主体がそれぞれの強みを活かして支援を進めることは重要である一方、リソースが限定的な中小企業においては、多数の取組に参画する、あるいは多数の取組の中から参画する取組を選択するといったことは重い負担となり、結果的にサイバーセキュリティ対策に支障を生じるおそれがある。中小企業へのアプローチに際しては、各主体間の連携を図り、中小企業の負担軽減に配慮すべきである。

エ　産学官における円滑な情報共有の促進

産学官の円滑な情報共有は、産学官連携の実効性の担保に必要不可欠であるが、産学官の組織間における情報共有に関して、共有する情報の範囲や情報管理の在り方について明確な取り決めがなく、円滑な情報共有の支障となっている。こうした課題に、平成 25 年度総合セキュリティ対策会議における議論を経て設立された JC3 では、秘密保持契約（NDA[39]）を締結し、直接対面して信頼関係を構築することで、適切に情報を保全し、情報の共有と実効的な協働を行っている。

また、フィッシングをはじめとするサイバー空間の脅威に対する防御を効率化するためには、攻撃者側の情報を官民で情報共有することが有効であるが[40]、捜査関連情報等のセンシティブな情報の取扱いに関しては、刑事訴訟法等の関係法令に照らして慎重な検討が必要になる。

産学官の円滑な情報共有を更に促進するため、情報を共有する組織の選定方法、情報が共有される組織に求められる情報管理体制や捜査関連情報等のセンシティブな情報の取扱いについて論点整理を行い、具体的な方策やルールの整備を検討していくべきである。

[39] Non-Disclosure Agreement の略
[40] 35、36 頁参照

第３章　安全性確保に向けた取組の実効性を担保する基盤・観点

１．課題

第１章や第２章で取り上げた取組を実効性のあるものとしていくためには、併せて検討すべき基盤や観点があるが、概してこうしたものへの対策の必要性は見落とされがちである。

まず、サイバー空間の基盤となるプラットフォームへの対策である。サイバー空間で提供されるサービスについて脅威が確認された場合、当該サービスだけに着目しがちであるが、実効的な安全対策を講じるためには、当該サービスだけではなく、プラットフォームにも着目することが重要である。例えば、キャッシュレス決済サービスの不正利用について、当該サービスは、クレジットカード、電子マネー、デビットカード、スマートフォン等を使った支払いにより、現金を使用せずに支払いができるサービスであるが、当該サービスだけで完結する仕組みではなく、スマートフォン等のプラットフォームの利用を前提としているものである。こうしたプラットフォームにおける最も重要な課題の一つが、本人確認の信頼性の確保であり、その在り方について具体的な検討が必要である。

見落とされがちな要素や観点は他にもある。例えば、サイバー空間は、サイバー空間と実空間との対比において、ブラックボックス化した仮想空間としてイメージされることが多いが、その実態は、通信機器、通信チャンネル及び記憶装置から構成されており、こうしたハードウェアの防護も重要な課題である。こうした見落としがちな要素・観点を洗い出し、必要な対策を検討することが必要である。

また、ソーシャルエンジニアリングへの対応についても検討が必要である。フィッシングやマルウェア攻撃の手口には、サービスやプラットフォームの脆弱性を狙ったものばかりではなく、ソーシャルエンジニアリングの手法を利用したものも多く存在し[41]、利用者のリテラシー向上に向けた様々な啓発活動が官民で行われているが、技術的なアプローチからも講じ得る対策がないか検討が必要である。

２．会議における主な意見

(1)　会議では、サイバー空間のプラットフォームにおける本人確認の信頼性を確保する観点から、次のような意見があった。

- SMS 機能付きデータ SIM の本人確認を徹底する必要があるのではないか。
- SMS 認証代行を通じた不正なアカウント作成への対応が必要ではないか。

[41] ５～７頁参照

・　電子署名の方式も当事者型から立会人型に移行する中で、必ずしも本人確認ができないという課題についても議論が必要ではないか。

・　S/MIME 等偽装を阻むための暗号技術を普及させる取組が必要ではないか。

(2)　会議では、安全性の確保において見落としがちな要素・観点に関して、次のような意見があった。

・　海底ケーブルの陸揚げ局、端局装置等サイバー空間を支える実空間上の構成要素の物理的防護やサプライチェーン対策が必要ではないか。

・　ドメイン名や DNS サーバの管理が不十分な場合、意図と異なるサイトに誘導され被害に遭うおそれもあり、事業者にこれらの適切な管理を促すことが必要ではないか。

(3)　会議では、ソーシャルエンジニアリングへの対応に関して、次のような意見があった。

・　昨今のフィッシング被害が多発している要因の一つとして、ショートメッセージにより誘導する手口が確認されている。こうした手口を一般利用者が見破るのは極めて困難であり、効果的な被害防止を行うためには、一般利用者にショートメッセージが届く前に検知し、遮断することが必要ではないか。

３．今後の取組の方向性

第１章や第２章で取り上げた取組に実効性を担保するためには、次の取組が必要である。

(1)　サイバー空間を構成するプラットフォームの信頼性確保

○　SMS 機能付きデータ SIM 契約時の本人確認の徹底

実空間と異なり、サイバー空間においては、通信の相手方を視認等により直接確認することができないため、重要な通信を行う際には、本人確認の信頼性が確保されていることが重要である。これを確認する手段として、現在も、知識認証とよばれ、通信の相手方が ID・パスワード等の正しい知識を有していることを確認する手法が広く用いられているが、この手法には、フィッシング等により ID・パスワード等を窃取することで容易に他者に偽装できるという課題が存在する。

SMS 認証は、こうした知識認証の弱点を補うために、知識認証と併用して認証の安全性を高める手段として広く採用されている認証方法であり、ショートメッセージで利用者の携帯電話に認証コードを送信し、携帯電話を所有している当該利用者が当該認証コードを入力することにより認証を行う。SMS は、携帯電話に標準装備されている機能であり容易に利用できるほか、安全性に関しても、ショートメッセージが回線番号に紐づいて送信されるものであるため、

ショートメッセージを確認できる者は携帯電話を現に所持している者に限られ、他者による偽装は困難となるという利点があることから、広く普及が進んでいる。

しかしながら、SMS 認証はあくまでも電話番号に対応した携帯電話を所持していることのみを保証するものであり、当該携帯電話を所持している者の身元を保証するものではない。よって、携帯電話の契約時に厳格な本人確認がなされていなければ、第三者を騙ることが可能であり、SMS 認証が信頼性のある本人確認の方法足り得るには、携帯電話を契約する際に公的身分証を用いた本人確認が徹底されていることが前提となっている。

この点、携帯電話の契約時の本人確認義務は、携帯電話不正利用防止法[42]において携帯音声通信役務を提供する場合に限定されており、音声通信機能を有さないデータ SIM 契約は、SMS 機能を有するものについても本人確認の義務付けの対象外となっている。

SMS 機能付きデータ SIM 契約時の本人確認について、NTT ドコモ、KDDI、ソフトバンク及び楽天モバイルの４社は、音声 SIM 契約時と同一の本人確認を実施している一方で、仮想移動体通信事業者（MVNO[43]）が本人確認を実施せずに契約したデータ SIM が犯行に悪用された事例が確認されており[44]、IT 関連業界も、SMS を用いた二経路認証[45]の抜け道になるとして、SMS 機能付きデータ SIM の本人確認の徹底を強く求めている[46]。こうした状況を踏まえ、令和３年１月、一般社団法人テレコムサービス協会 MVNO 委員会は、同委員会加盟の MVNO の自主的な取組として、SMS 機能付きデータ SIM 契約時の本人確認について、音声 SIM 契約時と同一の本人確認を実施する方針を申し合わせた。

このように、SMS 認証は、その安全性と簡便性から、ID・パスワード等の知識認証を補強する認証方法として広く使用され、サイバー空間において欠かすことができないプラットフォームの一部となっている。デジタル化の更なる進展には、その基盤となる認証方法の信頼性を担保することが必要不可欠であ

---

42 携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律（平成 17 年法律第 31 号）

43 Mobile Virtual Network Operator の略。自ら無線局を開設・運用せずに移動通信サービスを提供する電気通信事業者

44 19 頁事例①参照

45 インターネットバンキング等において、コンピュータ（第一経路）で振り込み等の取引データを作成した後、スマートフォン等（第二経路）で承認を行うことで取引を成立させる認証方式

46 一般社団法人日本 IT 団体連盟「2021 年度（令和３年度）政策要望：デジタル庁創設に望む」（令和３年１月７日公表）

り、MVNO においても SMS 機能付きデータ SIM 契約時の本人確認が徹底されるべきである。

(2) 見落としがちな要素・観点への対応

ア 通信インフラのセキュリティ強化

通信インフラのセキュリティについて、マルウェア対策などソフト面のセキュリティばかりが注目されがちであるが、例えば、通信ケーブルを物理的に切断することにより、通信を遮断することが可能である。我が国の国際通信は、海底ケーブルに依存しており、海底ケーブルを物理的に切断されれば、たちまち我が国の国際通信に大きな支障を及ぼすことになる。

海底ケーブルのネットワークと陸上ネットワークとの中継局である陸揚げ局は、国内・国際通信ネットワーク上の重要な拠点である。太平洋・インド洋海域は、アジア諸国間や、アジアと米国間を結ぶ国際回線が 40 以上敷設されている世界的にも海底ケーブルが高密度に集中する海域でもあり、アジア諸国や米国、オーストラリア等と日本を結ぶ拠点となっている。

このように、通信インフラのセキュリティ強化に当たっては、陸揚げ局等の重要防護施設の警備など、ハードウェア面からの対策についても民間事業者等と連携して取り組んでいくべきである。

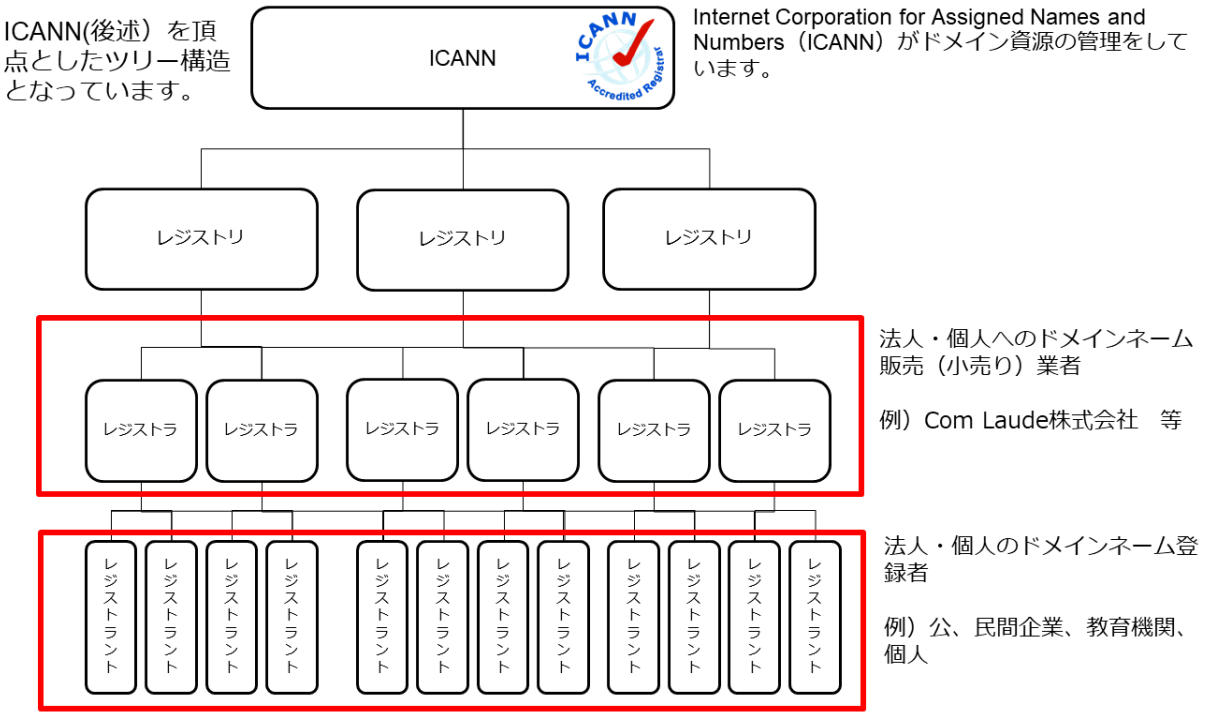
イ サプライチェーンリスクへの対応

ハードウェア対策が求められるもう一つの課題は、サプライチェーンリスクである。米国の治安情報機関等において、通信機器メーカーが製品の製造段階でサイバーセキュリティを脅かす細工をすることや配送途中で製品を抜き取った上で当該製品に細工をすることが技術的に可能であり、こうしたサプライチェーンリスクへの対応の必要性が指摘されている。我が国においても、官民が連携してサプライチェーンリスクを洗い出し、必要な対策を講じていくべきである。

ウ ドメイン名や DNS サーバのセキュリティ強化

ドメイン名とは、ウェブサイトにアクセスする際に必要となる文字列であり、サイバー空間にアクセスするための手段である。ドメイン名は末尾から数えた場所でレベル分けをしており、例えば、ドメイン名が「npa.go.jp」であれば、「jp」はトップレベルドメイン、「go」は第２レベルドメイン、「npa」は第３レベルドメインとなる。

図表 10：ドメインの分配構造



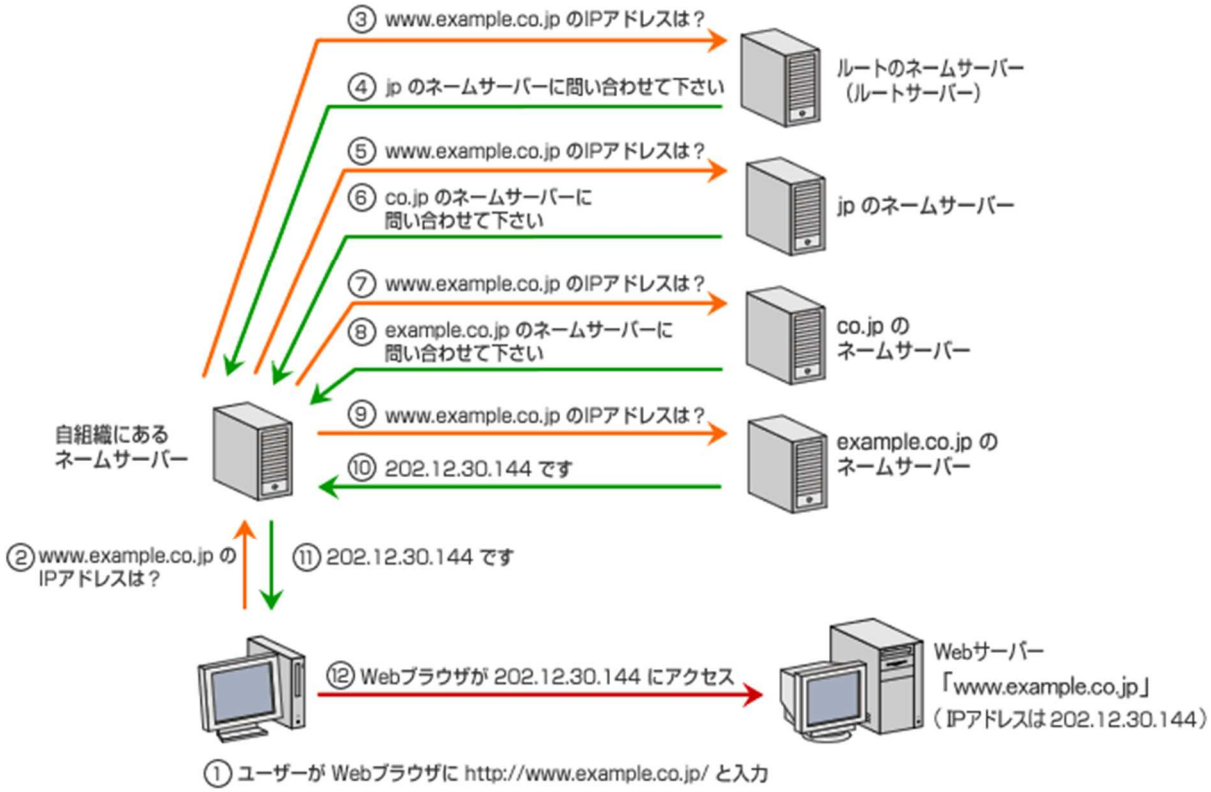
図表 10 は、ドメインの分配構造を示したものである[47]。一番上の ICANN[48]において、ドメインに関するルールメイキングが行われている。その下に、ICANN の認定を受けたレジストリがあり、１つのトップレベルドメインに対して、１つのレジストリが独占的にドメインの分配する権限が与えられている。例えば、「.com」であれば米国のベリサイン社、「.jp」であれば株式会社日本レジストリサービス（JPRS[49]）がレジストリとして認定を受けている。レジストリの下に、レジストラがあり、同じく ICANN の認定を受けた小売業者が、レジストリからドメイン名を仕入れて、登録者に販売する仕組みになっている。一番下の法人・個人のドメイン名の登録者をレジストラントといい、ドメイン名を取得して、ウェブサイトを展開したり、電子メールを使用することなどが可能となる。

ドメイン名を使ってインターネット上でやりとりを行うためには、これをコンピュータ同士が通信するために必要な IP アドレスに変換しなければならない。このドメイン名と IP アドレスを対応させる仕組みが DNS[50]である。

---

[47] コムラウデ株式会社の村上嘉隆氏の作成による。
[48] Internet Corporation for Assigned Names and Numbers の略
[49] Japan Registry Services の略
[50] Domain Name System の略

図表 11：名前解決の流れ



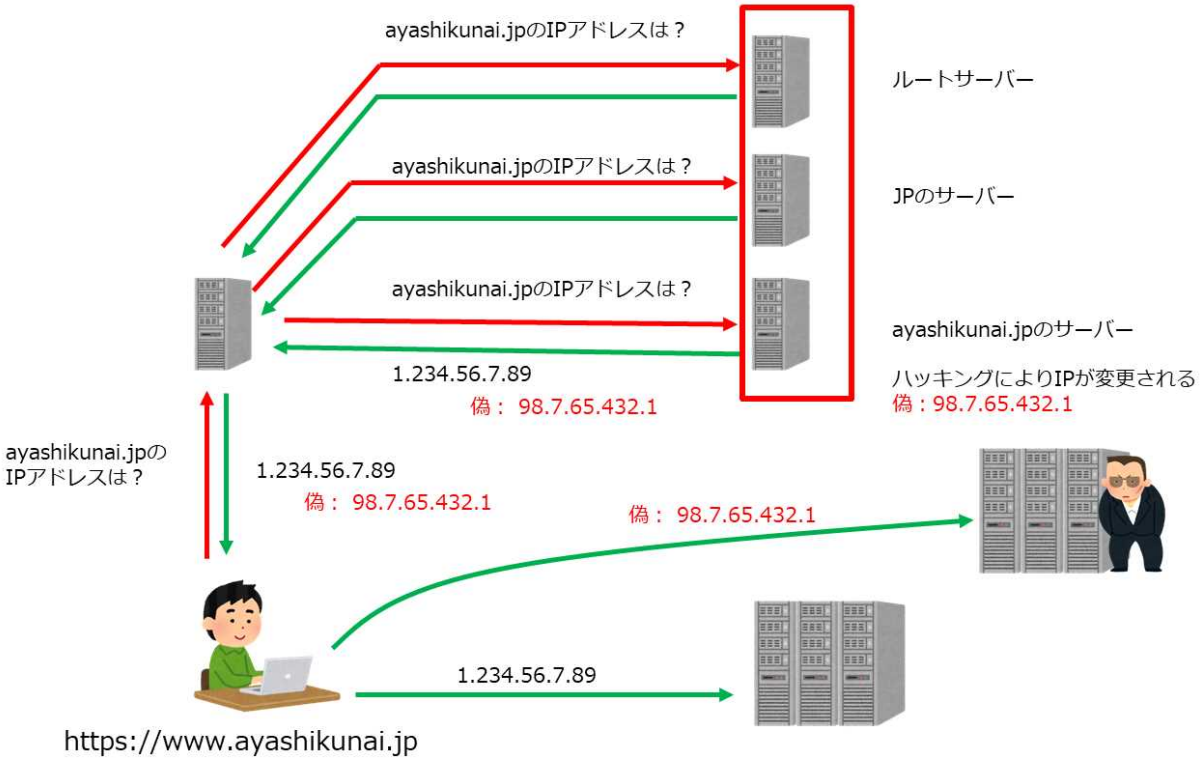
DNS サーバを使って、あるドメイン名からそれに対応する IP アドレスを引き出すことを名前解決という。図表 11 は、一般社団法人日本ネットワークインフォメーションセンター（JPNIC[51]）が名前解決について説明したものであり、ユーザが「www.example.co.jp」のウェブサイトにアクセスしようとした場合に、実際にどのようにして名前解決が行われるかを示している[52]。

この名前解決の仕組みを悪用し、DNS サーバのハッキングにより、利用者を全く別のウェブサイトにアクセスさせる事例が確認されている。図表 12 は、DNS サーバがハッキングされた場合に、どのように名前解決が行われ、全く別のウェブサイトにアクセスすることになるかを示したものである[53]。

この DNS サーバのハッキングが、利用者をフィッシングサイトに誘導させたり、個人情報を漏洩させたりするための一手段となっている。また、類似のドメイン名を用いて偽サイトを作成し、利用者に偽サイトへのアクセスを促す事

[51] Japan Network Information Center の略
[52] JPNIC「ドメイン名のしくみ」JPNIC ウェブサイト https://www.nic.ad.jp/ja/dom/system.html（令和３年２月 24 日閲覧）
[53] コムラウデ株式会社の村上嘉隆氏の作成による。

図表 12：名前解決の流れ（DNS サーバがハッキングされた場合）



例も確認されており、これも同様に、フィッシングサイトへの誘導等の一手段となっている。

こうしたドメイン名の登録・管理が、サイバーセキュリティに及ぼす影響は大きく、ドメイン名や DNS サーバの管理が不十分な場合、利用者が意図と異なるサイトに誘導され被害に遭うおそれがあることから、事業者において適切に管理されるよう働きかけていくべきである。

(3) ソーシャルエンジニアリングに対応するための技術的措置

○ フィッシングサイトに誘導するショートメッセージの遮断

フィッシングは、インターネットバンキングに係る不正送金事犯をはじめとして様々なサイバー犯罪に悪用されているが、昨今のフィッシング被害多発の要因の一つとして、スミッシングが手口として確認されている[54]。一般利用者にとって、スミッシングを見破るのは困難であり、効果的に被害を防止するためには、ショートメッセージ送信元のなりすまし防止対策はもちろんのこと、一般利用者にこうしたショートメッセージが届く前に検知し、遮断するための仕組みが構築されることが必要である。

[54] 5 頁参照

スミッシング被害を防止するため、警察として、フィッシングサイトに誘導するショートメッセージの遮断に向けて関係事業者において必要な対策等が講じられるよう働きかけを行うとともに、関係事業者の取組に必要となる捜査関連情報等の提供の在り方についても検討を進めていくべきである[55]。

[55] 28 頁参照

おわりに

以上のように、令和２年度サイバーセキュリティ政策会議では、「生活様式の変化等に伴うサイバー空間の新たな脅威に対処するための官民連携の更なる推進」をテーマとして幅広く検討を行い、本報告書を取りまとめた。

本報告書では、まず、コロナ禍がもたらした社会経済活動の変容等により、キャッシュレス決済サービスの不正利用、フィッシングやマルウェア攻撃の悪質化や国家の関与が疑われるサイバー攻撃への対策が急務となっていることを確認した。

こうした新たな脅威に対処していくため、今後のサイバーセキュリティに求められる「公共空間としての安全性確保の重要性」を新たな基本理念として据えるとともに、当該理念を実現するための観点として「犯罪対策と安全保障を一体として捉えた包括的対策の必要性」及び「全国民が安心して参画できる空間の実現に向けた各主体による取組の必要性」の２つを提示し、国民が、デジタル社会におけるあらゆる活動に参画し、生活の利便性向上や、個性豊かで活力に満ちた地域社会の実現を通じて、ゆとりと豊かさを実感できるようにするためには、サイバー空間においても、実空間と同水準の安全性の実現を目指していくべきことを明確にした。

これを受けた取組について、「犯行主体の特定を通じた犯罪対策・安全保障」、「健全なサイバー空間の実現に向けた各主体による取組」及び「安全性確保に向けた取組の実効性を担保する基盤・観点」という３つの論点に整理した上で、今後の方向性を示したところであり、今後、更に検討を加速化させていく必要がある。

今後のデジタル社会の到来は、全ての国民に多くの恩恵をもたらすことが期待されているが、その前提としてサイバーセキュリティの確保が必要不可欠である。警察には、今まで以上の困難が予想される難題に、迅速に取り組んでいくことが求められている。こうした国民の高い期待に応えていくためには、警察において柔軟な発想で新たな取組を模索し続けていくことはもとより、政府全体の力を結集するための施策に安全・安心の観点から積極的・主体的に参画していくこと、そして何より、官民の連携をより一層強化し、社会全体でサイバーセキュリティの確保に取り組む体制を構築することが重要である。

本報告書が、警察にとどまらず政府全体・社会全体のサイバーセキュリティの検討や方針策定に活かされ、全国民が安心して参画できるサイバー空間を実現するとともに、来たるデジタル社会において、全ての国民に多くの恩恵がもたらされることを強く期待するものである。

令和２年度サイバーセキュリティ政策会議委員名簿

◎委員長

前田　雅英	東京都立大学 法学部 客員教授

○委員

新井　悠	(株)NTTデータ 技術革新統括本部システム技術本部情報セキュリティ推進室 エグゼクティブセキュリティアナリスト
大久保隆夫	情報セキュリティ大学院大学 情報セキュリティ研究科 研究科長・教授
片山　建	日本マイクロソフト(株) 政策渉外・法務本部 デジタル政策部長
桑子　博行	違法情報等対応連絡会 主査
佐川　英美	Zホールディングス(株) GCTSO部 常務執行役員付参事/ ヤフー(株) 政策企画部 参事
佐々木良一	東京電機大学 研究推進社会連携センター 顧問・客員教授
沢田登志子	(一社)ECネットワーク 理事
島根　悟	(一財)日本サイバー犯罪対策センター 業務執行理事
神部　永志	セコムトラストシステムズ(株) 常務執行役員
土屋　大洋	慶應義塾大学 総合政策学部長・教授
寺田　真敏	(株)日立製作所 HIRT チーフコーディネーションデザイナ
林　憲明	フィッシング対策協議会 運営委員
藤原　靜雄	中央大学 法科大学院 教授
星　周一郎	東京都立大学 法学部長・教授
宮下　正彦	TMI総合法律事務所 弁護士

計 16人（敬称略・50音順）

【オブザーバー】

内閣官房(NISC)、金融庁、総務省、法務省、経済産業省