2025 年 10 月　第 271 号

Grant Thornton

太陽グラントソントン

エグゼクティブ・ニュース

バックナンバー
はこちらから

テーマ：サイバー空間を巡る脅威情勢と警察の取り組み

執筆者：警察庁　サイバー警察局　サイバー企画課長　阿久津 正好 氏

要　旨　（以下の要旨は 2 分 50 秒でお読み頂けます。）

今年（2025 年）9 月に発生した、ランサムウェア（身代金要求ウイルス）感染によるシステム障害から、大手飲料メーカーでは工場の稼働停止などの被害が発生しました。こうした情勢下、10 月に内閣総理大臣に就任された高市早苗氏は、その著作（日本を守る 強く豊かに）で「サイバーセキュリティ対策の強化を急げ！」と論じています。

最近のサイバー空間（データや情報が電子的にやり取りされる仮想空間）を巡る脅威に対し、警察当局はどう対応しているのか、以下、警察庁の阿久津正好サイバー企画課長に解説して頂きます。

サイバー攻撃は、「システム破壊・機能停止」、「妨害・信用失墜」、「情報窃取」等の目的で行われるが、近年、特に企業経営上のリスクとなっているのは「金銭獲得」の目的で行われるランサムウェアである。警察庁の調査では、ランサムウェアの被害は、企業規模、業種を問わず幅広く被害が発生している。その復旧には「1 か月以上」が 3 割、費用で「1,000 万円以上」が 4 割強あり、年を追うごとに高額化している。感染経路では、VPN（仮想プライベートネットワーク）機器からの侵入が 6 割で、その 4 割強はソフトウェアを最新の状態に更新していたにも関わらず発生している。バックアップがある場合も、一緒に暗号化されてしまうことが多く実際に復元できた割合は 2 割に留まる。

また、フィッシング（偽サイトに誘導し、金銭を詐取）によるサイバー犯罪も急増している。例えばインターネットバンキングを通じた不正送金被害額は、4 年前比 8 倍近くに上る（2024 年 86.9 億円）。

こうしたサイバー犯罪に対し適切に対処すべく、警察庁では 2022 年にサイバー警察局を設置し、47 都道府県警察のサイバー捜査を調整する体制を整えた。特にランサムウェアに対しては、国際共同捜査による被疑者の検挙を推進しており、この間、警察庁ではランサムウェアにより暗号化されたファイルの復号ツールの開発に成功している。

サイバー被害の防止に向けた官民連携を推進すべく都道府県警察ごとに「サイバーテロ対策協議会」等を設置している。他方、サイバー攻撃に対しては「未然防止の徹底」に加え「発生前提の拡大防止策」の推進も必要だ。官民連携に関しては、2014 年設置の「（一財）日本サイバー犯罪対策センター」に大手、中小企業合わせ 106 社が会員となっている。最近では、フィッシング対策防止のため、警察庁と金融庁の連名で、金融機関に対し対策の強化を要請している。

一方、国レベルでは基幹インフラ事業者にサイバー攻撃が行われた場合の政府への報告義務を定めた「サイバー対処能力防止法」が成立した（今年 5 月）。このような動きを見据え、警察でも網羅的なメニューを掲げた「サイバー人材確保・育成方針」を策定（同 3 月）し、加えて、警察官としての採用も見据えつつサイバー防犯ボランティアとの連携にも努めている。

サイバー空間は、道路などの実空間と同じ「公共空間」である。警察は検挙・抑止を通じ、その安全・安心の確保に向け全力で対応して参りたい。

「太陽グラントソントン エグゼクティブ・ニュース」バックナンバーはこちらから⇒https://www.grantthornton.jp/insight/
本ニュースレターに関するご意見・ご要望をお待ちしております。Tel: 03-6438-9395　e-mail: mc@jp.gt.com
太陽グラントソントン マーケティングコミュニケーションズ 宛

テーマ：サイバー空間を巡る脅威情勢と警察の取り組み

警察庁　サイバー警察局　サイバー企画課長　阿久津 正好

1. はじめに

今年（2025 年）9 月にシステム障害が発生した大手飲料メーカーにおいては、工場の稼働停止や出荷の停止に追い込まれたとされており、また、復旧には数か月の時間が掛かり、そのため億円単位の費用が掛かるとも報じられている。

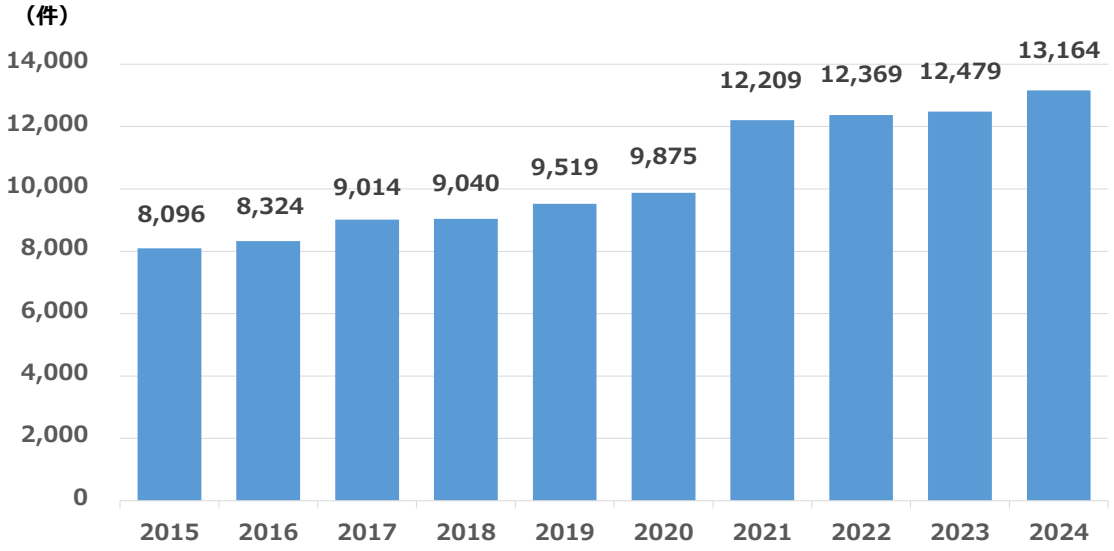
今回の被害は、ランサムウェア（身代金要求型ウイルス）の感染でシステム障害が発生したと同社から発表されている。このような被害は、企業活動に大きな影響を与えるが、こうしたサイバー空間（データや情報が電子的にやり取りされる仮想空間）をめぐる脅威が大きく拡大している。

以下、こうしたサイバー空間をめぐる脅威情勢と警察の取組について論じたい。

2. サイバー空間を巡る脅威情勢～特にランサムウェアの影響

サイバー犯罪は、どのくらいの規模で行われているのだろうか？これについて警察庁が発表している「サイバー空間をめぐる脅威の情勢等」によると、その検挙件数が一貫して右肩上がりである。コロナ禍の 2021 年には 1 万件を突破し、昨年（2024 年）には 13,164 件と過去最高となっている（図 1）。

（図 1）サイバー犯罪の検挙件数



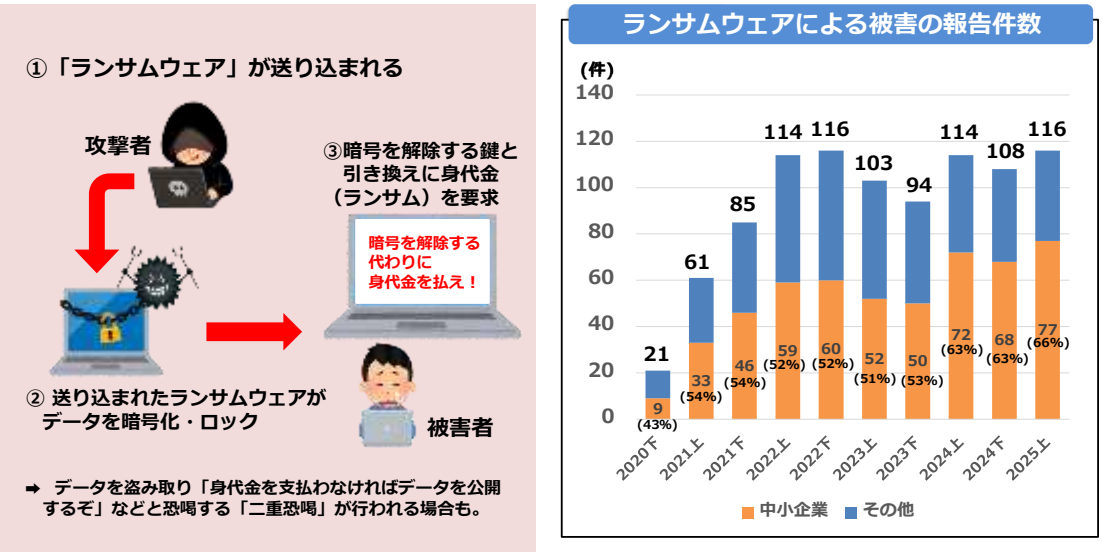
出典：警察庁「サイバー空間をめぐる脅威の情勢等について」

サイバー攻撃の主な目的・手口は大きく 4 つに分けられる。一つ目は「システム破壊・機能停止目的」のサイバーテロ攻撃、2 つ目は「妨害・信用失墜目的」で行われる、大量のデータ送付などでウェブの閲覧等を妨害する DDoS(ディードス)攻撃のようなサイバー攻撃、3 つ目は「金銭獲得目的」のランサムウェアのようなサイバー攻撃、最後に「情報窃取目的」のサイバーエスピオナージ（窃取）である。

この中で特に厄介なのがランサムウェアである。これは送り込まれたウイルスでデータを暗号化・ロックし、解除する代わりに身代金（ランサム）を要求するものであり「身代金を払わなければデータを公開する」と要求する、二重恐喝が行われる場合が多い。

最近では、半年で約 100 件ほどの被害が出ており、中小企業が過半数を占め、その割合は増加傾向にある（図 2）

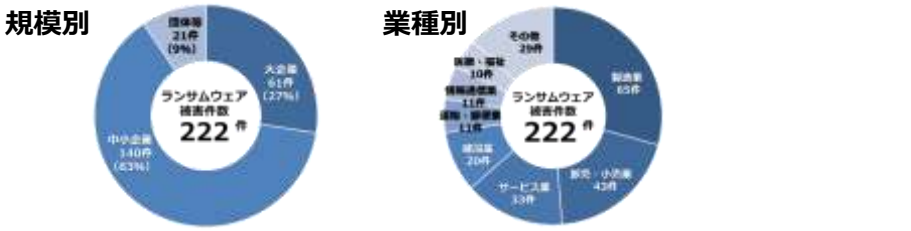
（図 2）高度なサイバー攻撃　～ランサムウェア～



出典：警察庁「サイバー空間をめぐる脅威の情勢等について」を元に作成

ランサムウェアの被害状況を見ると、企業規模、業種を問わず幅広く被害が発生していることが分かる。ちなみに、昨年（2024 年）に報告があった 222 件中、大企業が 61 件（27%）、中小企業が 140 件（63%）で、業種では、製造業 65 件、卸・小売業 43 件、サービス業 33 件などとなっている。注目すべきは、サプライチェーンを通じて、想定を超える範囲で被害が発生していることだ。一昨年（2023 年）には、愛知の港湾施設で、コンテナターミナルシステムの感染から、コンテナの搬出入作業が 3 日間停止に追い込まれる事態が発生している（図 3）。

（図 3）ランサムウェアによるサプライチェーンリスク

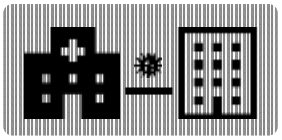


企業規模・業種を問わず、幅広く被害が発生

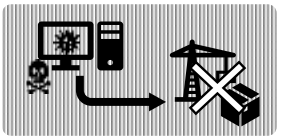
（主な被害事例）

出典：警察庁「令和６年におけるサイバー空間をめぐる脅威の情勢等について」

感染したシステムだけでなく、
被害への対応のため、全システムを停止
（米・石油パイプライン 2021）



取引業者のシステムを経由し、
内部に侵入され、感染
（大阪・医療機関　2022）

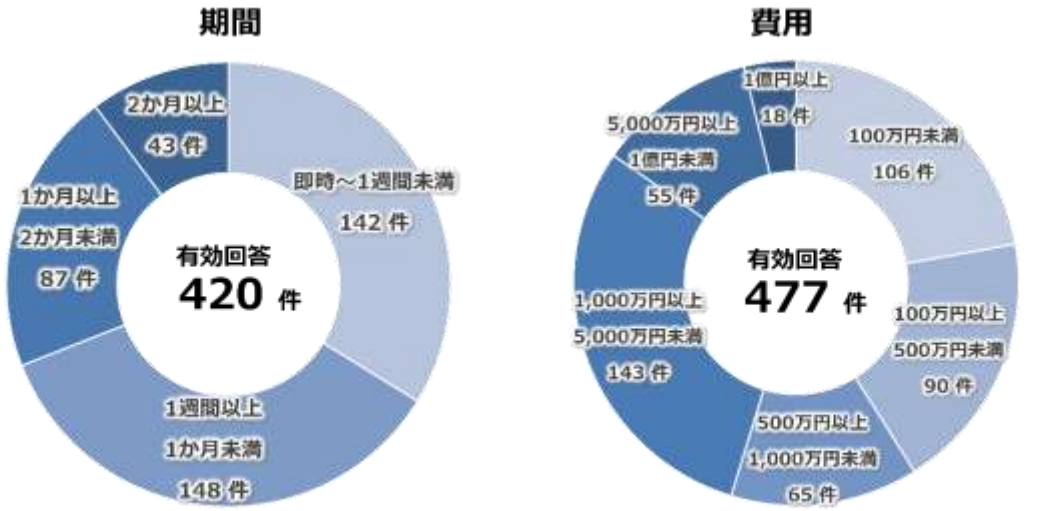


コンテナターミナルシステムが感染し、
コンテナ搬出入作業が３日間停止
（愛知・港湾施設　2023）

サプライチェーンリスクにより、想定を超える範囲で被害が発生

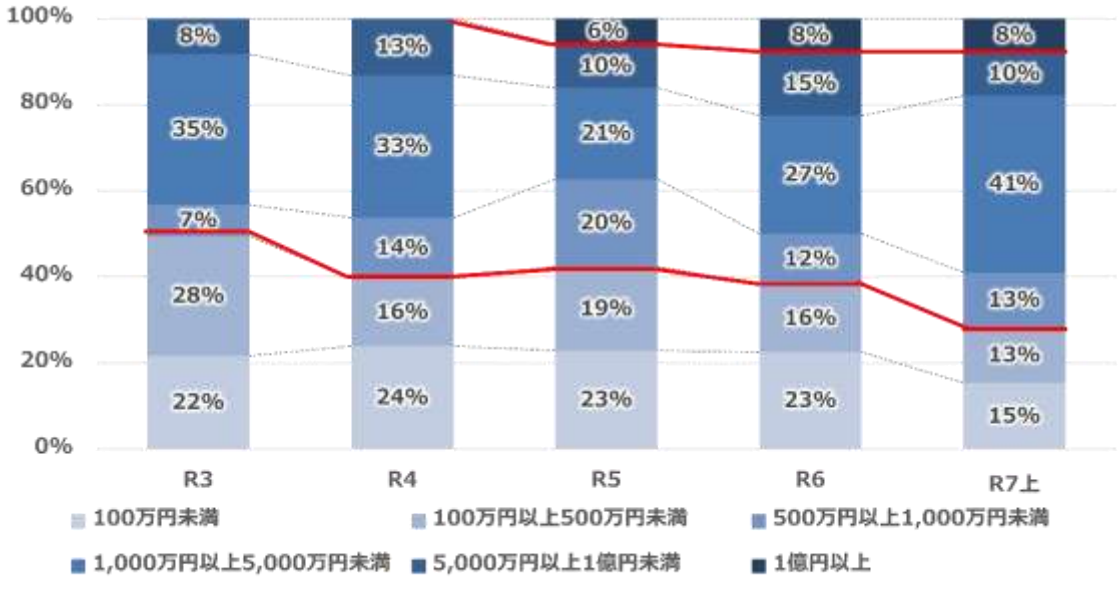
それでは、この被害に対し調査・復旧に要した期間と費用はどの位だったのだろうか。期間を見ると「即時から 1 週間未満」と比較的短期に復旧した例もある（420 件中 142 件）が、「1 か月以上」も 3 割を超えている（同 130 件）。費用を見ると「100 万円未満」が 2 割ほど（477 件中 106 件）であるが、「1,000 万円以上」が合計で 4 割強（216 件）と大きな費用が発生している（図 4）。これらには逸失利益は含まれていない。また、調査・復旧に要した費用の割合は、年を追うごとに高額化しており（1 億円以上の被害：2022 年ゼロ→23 年 6%→24 年 8%）、被害が深刻化していることがうかがえる（図 5）。

（図 4）調査・復旧に要した期間・費用



出典：警察庁「ランサムウェア等被害に関する実態調査」（R３～R７上）を元に作成

（図 5）ランサムウェア被害の調査・復旧に要した費用の推移

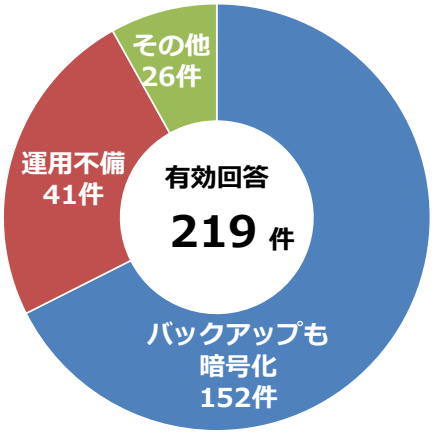


出典：警察庁「ランサムウェア等被害に関する実態調査」（R３～R７上）を元に作成

また、ランサムウェアの感染経路では、VPN（仮想プライベートネットワーク）機器からの侵入が 6 割と多く、感染の 4 割強は最新のセキュリティパッチ（プログラム）を適用しているにも関わらず感染している。こうした感染に対し、大半はバックアップ体制を整えているものの、実際に感染した場合に全て復元できた組織は 2 割に留まっている。

復元できなかった理由としては、復元するための運用に不備があった（回答 219 件中 41 件）ことのほか、暗号化していたバックアップも暗号化された（同 152 件）との回答も多く、適切な対策が浸透していないという状況がうかがわれる（図 6）。

（図 6）バックアップから復元できなかった理由

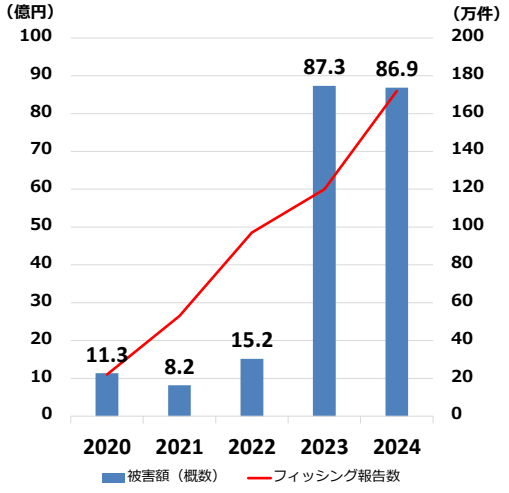


出典：警察庁「サイバー空間をめぐる脅威の情勢等について」（R5～R7上）より作成

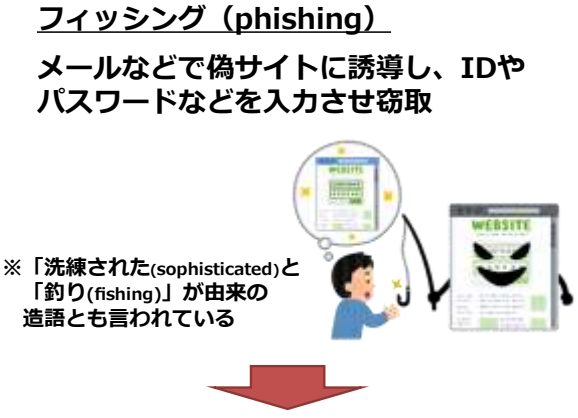
さらに、国家を背景とするサイバー攻撃も認められ、交流のある人物を詐称しての情報窃取など、システムの脆弱性のみならず、人間の脆弱性を悪用する事例も見られる。

加えて、フィッシング（偽サイトに誘導しパスワードなどを入力させ金銭を窃取）によるサイバー犯罪も急増しており、例えばインターネットバンキング不正送金の被害額は 4 年前と比較して 8 倍近くに上っている（2020 年 11.3 億円→24 年 86.9 億円＜図 7＞）。

（図 7）フィッシングを入口としたサイバー犯罪 ～インターネットバンキング不正送金～



出典：警察庁「サイバー空間をめぐる脅威の情勢等について」



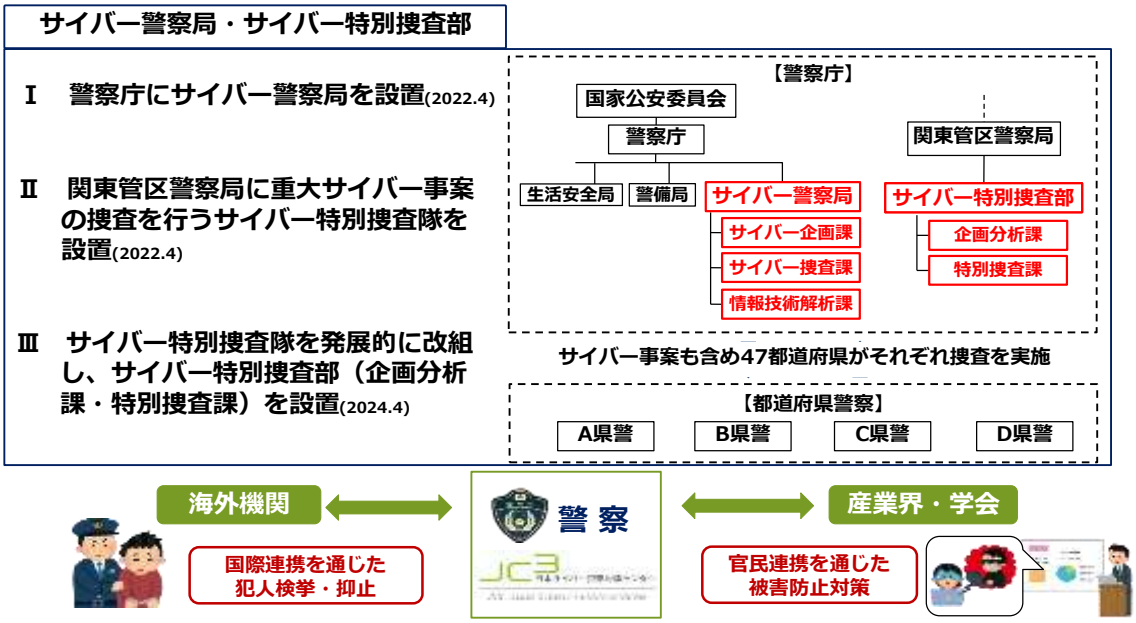
中には銀行員を装うボイスフイッシングや、メールを使って偽サイトに誘導するフィッシングもある。警察庁では未然防止に向けて手口を公開しているが、例えば、対策が不十分な状態の自社販売サイトでクレジットカードを不正利用された場合には、不正利用分の売上はカード会社から支払われず、損害となり得ることにも留意する必要がある。

このほか、AI を悪用したランサムウェアやフィッシングサイト作成に係る被疑者についても不正アクセス禁止法違反等で検挙している。

3. 警察の取り組み

こうしたサイバー空間の脅威に対処すべく、警察庁は大規模な組織改編を実施した。具体的には、2022 年 4 月、サイバー企画課、サイバー捜査課、情報技術解析課から成るサイバー警察局を設置し、47 都道府県警察のサイバー捜査を調整する体制を整えた。また、国の捜査機関として新たにサイバー特別捜査隊（現：サイバー特別捜査部）を設置し、国際共同捜査を推進するなど、国際連携を通じた犯人検挙・抑止と、官民連携を通じた被害防止対策を推進している（図 8）。

（図 8）警察庁サイバー警察局・サイバー特別捜査部の設置



特に、ランサムウェアに対しては、国際共同捜査による被疑者の検挙を推進している。サイバー警察局・サイバー特別捜査部は「ユーロポール」（EU の専門機関でハーグ所在。情報交換による加盟国の警察を支援）や米国 FBI を含む外国捜査機関との相互協力により、被疑者の逮捕や犯罪インフラの閉鎖などを行っている。

このような国際協力の取り組みの中で、警察庁ではランサムウェアにより暗号化されたファイルの復号を成し遂げている。具体的には、サイバー特別捜査部の技術力を駆使し、暗号化されたファイルを復号するツールの開発に成功している。例えば「Phobos」と呼ばれるランサムウェアについては、暗号化されたデータを復元できる可能性があり、警察庁のホームページからダウンロード可能である。

さらに、国際共同捜査により、海外被疑者と国内被疑者で共謀してフィッシング詐欺を行った事件について、インドネシア国家警察と連携して同国人被疑者を逮捕した事例もある（2022 年～23 年）。

加えて、国家による情報窃取型サイバー攻撃や暗号資産窃取型サイバー攻撃についても、米国 FBI などと連名で注意喚起を行った事例もある。

4. 官民連携

サイバー被害防止のため官民連携で、都道府県警察ごとに管内の重要インフラ事業者等をメンバーとする「サイバーテロ対策協議会」を設置するなどしており、サイバー被害事例から抽出される教訓は、政府広報でも閲覧できる（例：動画「ランサムウェア対策の基本」＜図 9＞）。

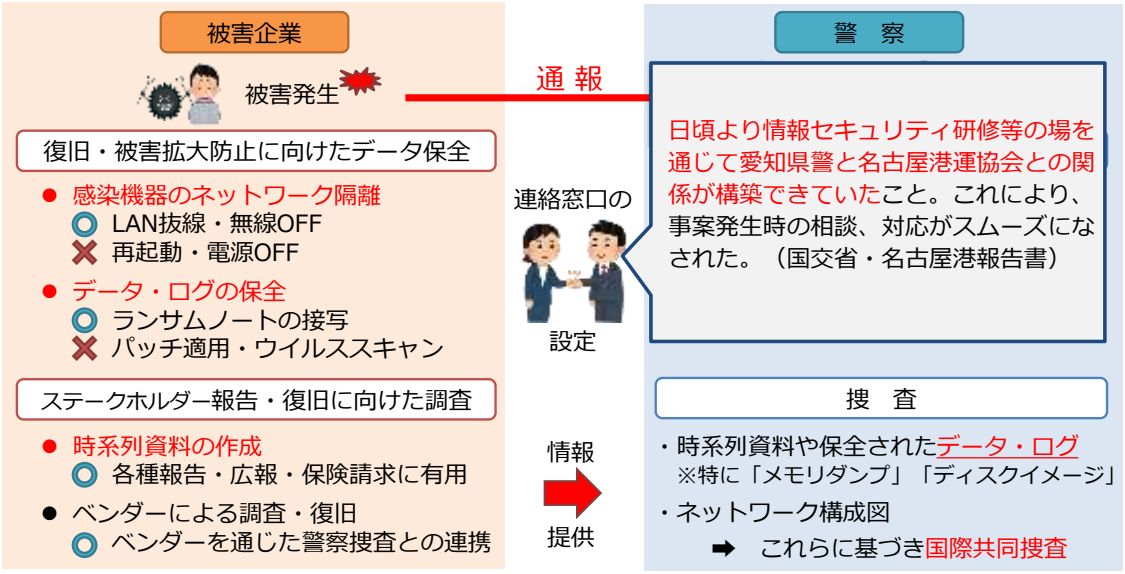
（図 9）被害事例から抽出される教訓

出典：当該医療機関に係る「情報セキュリティインシデント調査委員会報告書」を元に作成

ただし、すべてのサイバー攻撃を防ぎきることは困難であることから、今後は、「未然防止の徹底」に加え「発生前提の拡大防止対策」を推進していくことが必要である（図 10）。具体的には、被害に遭うことを想定した「業務継続計画（BCP）」を策定し、オフラインを含む複数のバックアップを取得するとともに、バックアップからの復元訓練を実施することなどが必要となってくる。また、この場合、BCP に事案発生時における警察との窓口設定と通報・捜査協力について規定することが適切と考えられ、このような警察捜査における証拠保全と復旧に向けた調査におけるデータ保全は、実は、相互補完的で親和性がある（図 11）。

（図 10）「未然防止対策の徹底」から「発生前提の拡大防止対策の推進」へ

（図 11）復旧に向けた調査と警察捜査の親和性



なお、2014 年に設置された「（一財）日本サイバー犯罪対策センター」には捜査関係情報を含む情報が提供されており、警察との連携のハブとなっている。現在、メガバンクや大手証券会社等のみならず中小企業も含め 106 社が会員となっており、官民連携の実が挙げられている（図 12）。

（図 12）（一財）日本サイバー犯罪対策センターを軸とした官民連携

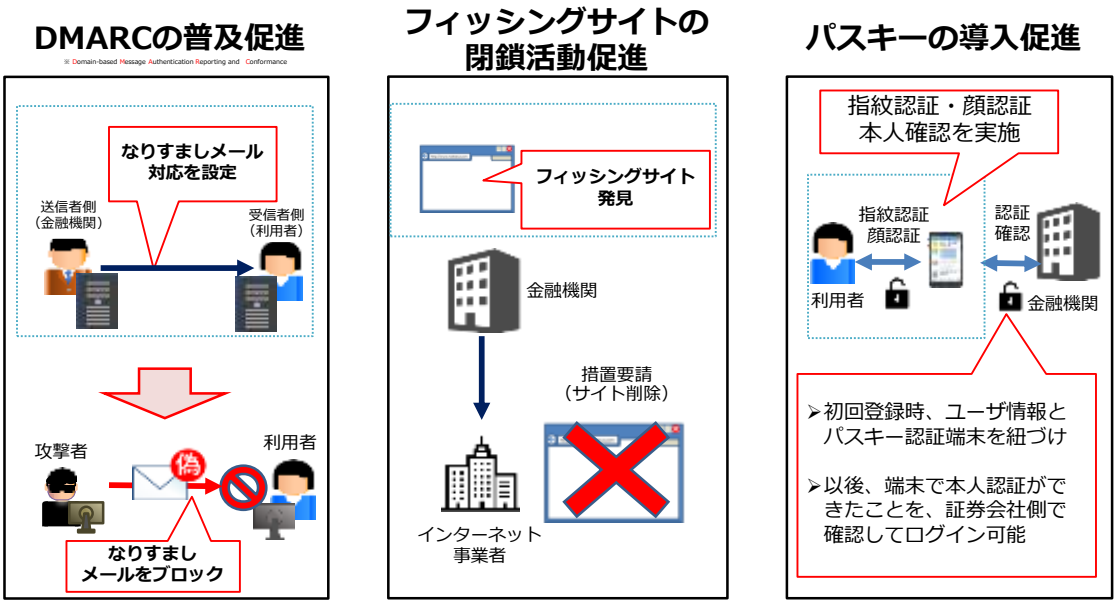
- （一財）日本サイバー犯罪対策センター（JC3）は、**産業界、学術機関、法執行機関等、それぞれが持つサイバー空間の脅威への対処経験を集約・分析し、その結果を共有**することで、サイバー空間全体を俯瞰し、サイバー犯罪等のサイバー空間の脅威の大本を特定・軽減・無効化することを目指す非営利団体として、2014年11月業務開始。

- 産学官の連携の枠組として、インターネットを利用した金融犯罪事案、標的型攻撃等による情報窃取事案、詐欺等のeコマースに対する脅威等、サイバー空間における様々な脅威に対処すべく、情報共有や手口分析、マルウェアの解析、脅威情報の収集・活用、国際連携等、様々なアプローチを通じて、安全かつ安心してインターネットを利用できる環境の構築に貢献。

出典：日本サイバー犯罪対策センター

このほか、警察庁では今年（2025 年）7 月に金融庁と連名で、金融機関が自ら、当該金融機関を騙ったフィッシングサイトを発見し、その削除要請を行うなどのフィッシング対策を推進することを要請している（図 13）。

（図 13）金融機関に対するフィッシング対策の要請（金融庁連名・本年 7 月）



出典：警察庁「サイバー空間をめぐる脅威の情勢等について」

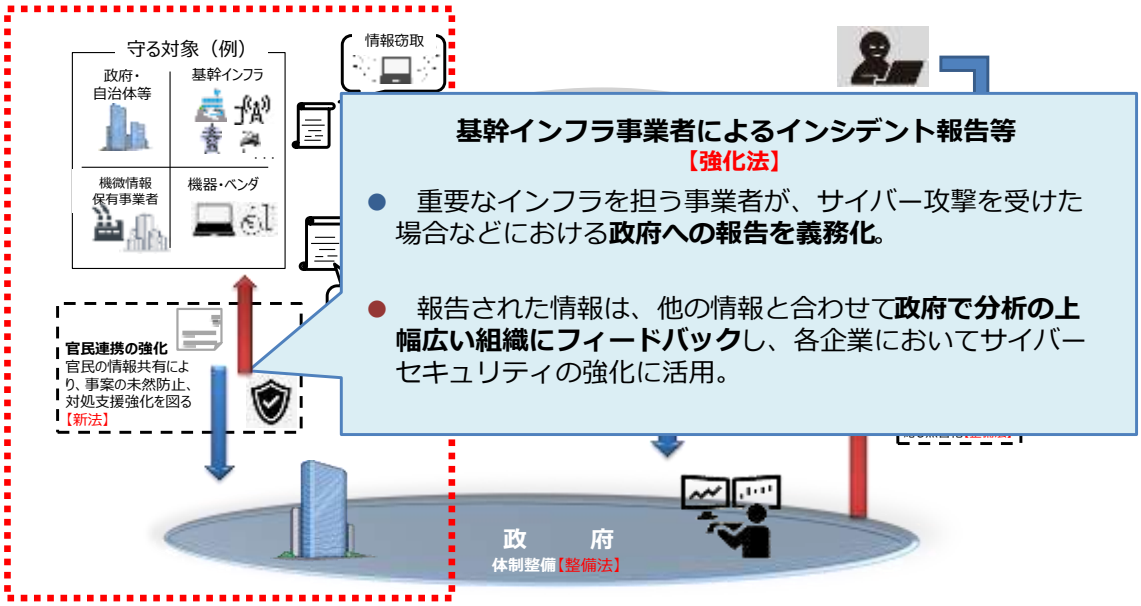
5. 今後の課題

前述のように、警察庁では 2022 年にサイバー警察局を設置し、昨年（2024 年）4 月にはサイバー特別捜査「隊」をサイバー特別捜査「部」に発展的に改組した。

今年 5 月には、基幹インフラ事業者にサイバー攻撃を受けた場合における政府への報告の義務化等を定めた「サイバー対処能力強化法」が成立したほか、同時に整備された「サイバー対処能力強化法整備法」により「警察官職務執行法」が改正され、警

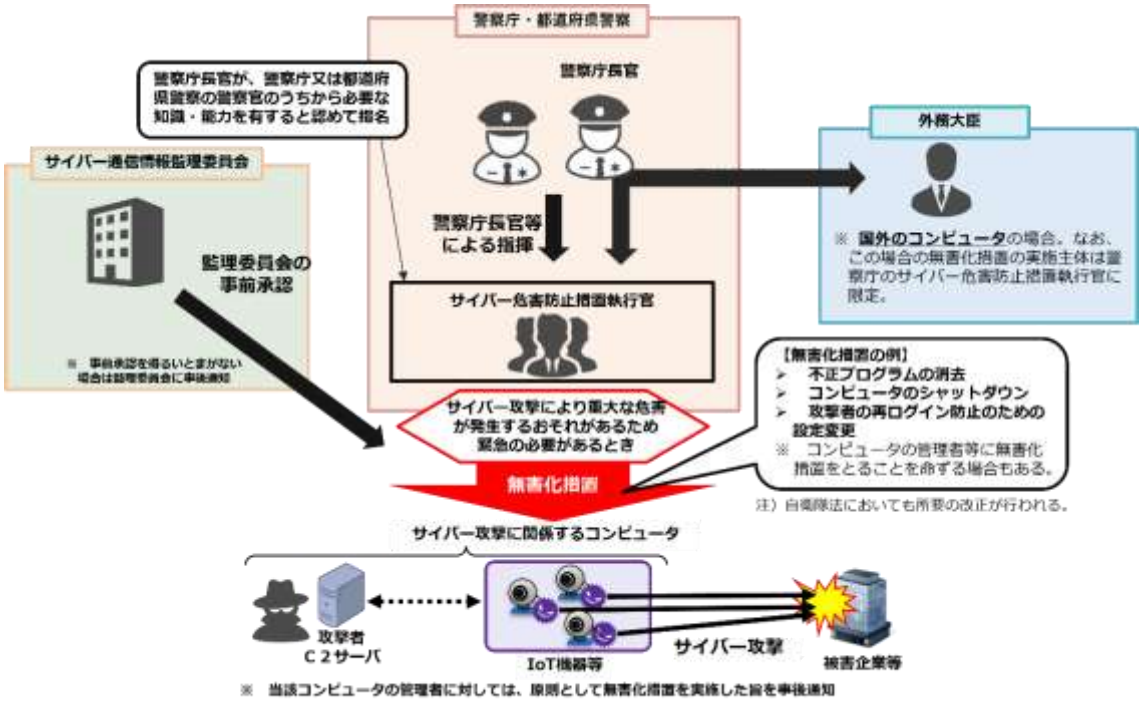
察・自衛隊が不正プログラムを消去するなどのアクセス・無害化措置を講ずることが可能となった（図 14、15）。今年（2025 年）4 月にサイバー特別捜査部に設置された特別対処課を中心に当該アクセス・無害化措置を講ずることが想定される。

（図 14）サイバー対処能力強化法・同整備法の全体イメージ



出典：内閣官房サイバー安全保障体制整備準備室「サイバー対処能力強化法案及び同整備法案について」を元に作成

（図 15）改正警察官職務執行法に基づく「アクセス・無害化」の概要

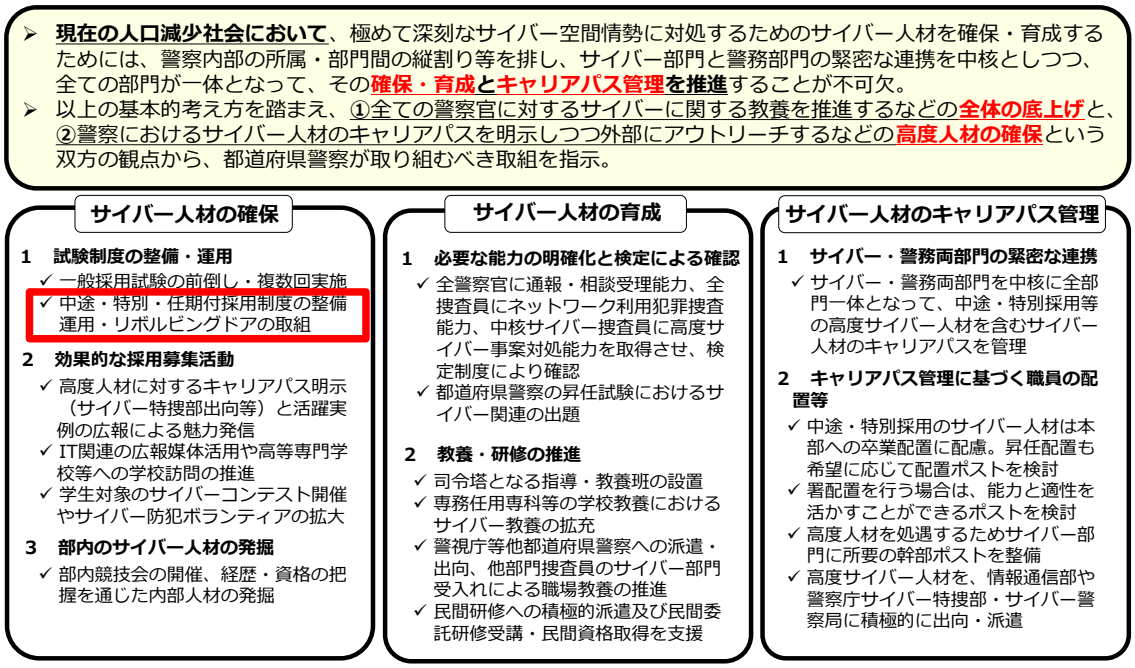


出典：警察庁「サイバー空間をめぐる脅威の情勢等について」

6. 人材育成

警察においては、サイバー人材の確保・育成にも力を入れている。今年（2025 年）3 月には、新たに「サイバー人材確保・育成方針」を制定した。具体的には、中途採用等を含む網羅的なメニューを規定しており、これにより、全国警察においてサイバー人材の確保・育成やキャリアパスの管理などを推進している。実際、中途採用のサイバー特別捜査官（警視正）がサイバー特別捜査部の特別捜査課長として活躍しているほか、官民人事交流でサイバー分析官を幹部警察官（警視正）として採用している（図 16）。

（図 16）「サイバー人材確保・育成方針」の制定（本年 3 月）



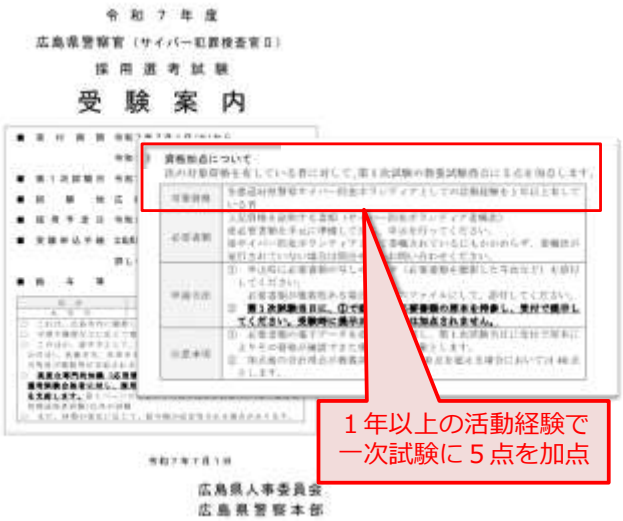
出典：警察庁「サイバー空間をめぐる脅威の情勢等について」

加えて、サイバー防犯ボランティアとの連携も図っており、このボランティア活動に従事した経験者を警察官採用選考において加点事由として評価する県警察も現れている（図 17）。

（図 17）サイバー防犯ボランティア活動の促進に向けた取組

【山口県警】
警察ボランティアに対する活動証明書の発行

【広島県警】
サイバー防犯ボランティア活動経験者に対する採用加点



7. おわりに

サイバー空間は、実空間と同様の「公共空間」である。道路と同様の「公共空間」である以上、警察は、検挙と抑止を通じて、その安全・安心を確保する責務を有する。引き続き、警察として全力で対応して参りたい。

以上

執筆者紹介

阿久津 正好（あくつ まさよし）1973 年 埼玉県出身
警察庁 サイバー警察局 サイバー企画課長

＜学歴・職歴＞
1996 年　東京大学法学部 卒業
1996 年　警察庁 入庁
2008 年　在ドイツ日本国大使館 一等書記官
2017 年　刑事局刑事企画課 刑事指導課長
2020 年　長官官房参事官（国際・サイバーセキュリティ対策調整担当）
2022 年　サイバー警察局 サイバー捜査課長
2023 年　山口県警 本部長
2024 年　現職