広　報　資　料
令和３年９月９日
警　　察　　庁

令和３年上半期におけるサイバー空間をめぐる脅威の情勢等について

１　情勢概況

サイバー空間が重要な社会経済活動を営む重要かつ公共性の高い場へと変貌を遂げつつある中、ランサムウェアによる被害が大幅に増加しているほか、サイバー攻撃が多数発生するなど、サイバー空間における脅威は極めて深刻な情勢が続いている。

２　サイバー空間の脅威情勢

○　国内外で、ランサムウェアによる攻撃が多発。
- 二重恐喝（ダブルエクストーション）の攻撃手口の拡散や産業制御システムに影響を及ぼしうるマルウェアを確認。
- 被害企業へのアンケート結果によると、国内における被害も深刻化の傾向。

○　サイバー攻撃による情報流出事案が引き続き多発。国内の政府機関や研究機関等で被害が発生。

○　警察庁が国内で検知したサイバー空間における探索行為等とみられるアクセスの件数は引き続き高い水準。

○　インターネットバンキングに係る不正送金事犯は、発生件数が減少したものの、被害額は微減にとどまり引き続き高い水準。

３　警察における取組

○　宇宙航空研究開発機構（ＪＡＸＡ）等に対するサイバー攻撃事案について、事件捜査等を通じたアトリビューションにより、国家レベルの関与を解明。

○　犯罪インフラ化するＳＭＳ認証代行に関し、総務省と連携して業界団体へ本人確認の強化を要請。

○　重要インフラ事業者等とサイバー攻撃の発生を想定した共同対処訓練を実施したほか、サイバー攻撃事案で使用されたＣ２サーバのテイクダウン（機能停止）を実施。

○　ＪＣ３と連携し、国内の金融機関等やワクチン接種予約を装ったフィッシングについて、注意喚起を実施。

別　添

令和３年上半期におけるサイバー空間をめぐる脅威の情勢等

新型コロナウイルス感染症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。このような中、政府は「誰一人取り残さない、人に優しいデジタル化」の実現を目指してデジタル改革を強力に推進しており、今後、サイバー空間は、全国民が参画し、重要な社会経済活動を営む、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[*1]。

その一方、国内の企業・団体等に対するランサムウェアによる被害が大幅に増加しているほか、我が国の政府機関、研究機関等に対するサイバー攻撃が多数発生するなど、令和３年上半期におけるサイバー空間をめぐる脅威は、極めて深刻な情勢が続いている。

ランサムウェアによる攻撃については、国内外で二重恐喝（ダブルエクストーション）の攻撃手口の拡散や産業制御システムに影響を及ぼしうるマルウェアも引き続き確認されている。警察庁に報告された国内のランサムウェアによる被害件数は、前年下半期と比較して大幅に増加している。被害企業・団体等に対して警察が実施したアンケート調査の結果によると、被害の発覚後システム等の復旧までに相当の期間・費用を要している実態が認められるなど、その被害が深刻化している状況がうかがわれる。国外においても、５月に米国の石油パイプライン事業者最大手のシステムがランサムウェアに感染し、同社が運営する全てのパイプラインの操業が停止するなど、市民生活や広範な産業活動に影響を及ぼす事案等も発生している。

このほか、サイバー攻撃により情報が窃取される事案も引き続き多発している。国内においても政府機関や研究機関等が外部からの不正アクセスを受け、職員の個人情報等が流出した可能性がある事案が相次いで確認されたほか、警察庁が国内で検知した、サイバー攻撃の対象をインターネット上で探索する行為等とみられるアクセスの件数についても、継続して高水準で推移している。

また、警察では、４月、宇宙航空研究開発機構（ＪＡＸＡ）をはじめとする国内企業等へのサイバー攻撃を実行した集団の背景に、中国人民解放軍第61419部隊が関与している可能性が高いと結論付けるに至った。本事案を通じて、警察では、独自の実態解明や外国治安情報機関との緊密な連携により、サイバー攻撃への国

---

*1　サイバーセキュリティ政策会議「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３年３月）
（https://www.npa.go.jp/cybersecurity/CS.html）

家レベルの関与を明らかにするとともに、警察の全国ネットワークを駆使し、迅速な被害の未然・拡大防止を図った。

2020年東京オリンピック・パラリンピック競技大会（以下「東京大会」という。）については、その円滑な進行を確保するため、大会関係機関等と協力し、東京大会を標的としたサイバー攻撃に関する情報の収集・分析、事案発生を想定した共同対処訓練、未知の不正プログラム等に関する注意喚起といった対策を実施した。また、東京大会の期間中には、事案発生時に即応できるよう、24時間体制でサイバー攻撃対策を実施した。

インターネットバンキングに係る不正送金事犯の発生件数・被害額は、ともに前年同期と比較して減少したものの、被害額の減少幅は小さく、引き続き大きな被害が発生している。これらの被害の多くは、金融機関や宅配業者を装ったＳＭＳや電子メールを用いてフィッシングサイトへ誘導する手口によるものと考えられるが、インターネット上に情報を保存するメモアプリ等が不正アクセスされ、保存していたパスワード等の情報を窃取されたと思われるケースも確認されている。

新型コロナウイルス感染症に直接関連するサイバー犯罪が疑われる事案としては、都道府県警察から警察庁に報告のあった件数は減少したものの、悪質なショッピングサイト等の通報件数は増加している。一般財団法人日本サイバー犯罪対策センター（Japan Cybercrime Control Center。以下「ＪＣ３」という。）が一般社団法人セーファーインターネット協会を通じて把握した令和３年上半期の悪質なショッピングサイト等の通報件数は6,535件で、前年同期と比べて1,516件増加しており、ＪＣ３は新型コロナウイルス感染症の影響もあり、インターネットの利用が増えたことが要因であると分析している[*2]。

このほか、サービス利用時の本人確認として広く用いられているＳＭＳ認証を不正に代行する「ＳＭＳ認証代行[*3]」が確認されているが、これは、サイバー空間における本人確認の手段として広く用いられるＳＭＳ認証の信頼性を貶める悪質な行為であるとともに、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。

このように、引き続きサイバー空間における脅威が極めて深刻である中、警察庁では、サイバー事案への対処能力を強化し、諸外国と連携した脅威への対処を推進するなどの観点から、令和４年度に警察庁にサイバー局を設置するとともに、一定のサイバー事案について直接捜査を行うサイバー隊を設置する組織改正を検討している。

---

*2　ＪＣ３ウェブサイト「悪質なショッピングサイト等に関する統計情報（2021年上半期）」（https://www.jc3.or.jp/threats/topics/article-377.html）

*3　通信当事者以外の第三者が、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当該通信当事者に提供する行為

警察においては、組織の総合力を一層発揮するとともに、関係事業者や国内外の関係機関等と緊密に連携し、サイバー空間の脅威に対する厳正な取締りや実態解明、これらにより判明した事項を活用した被害の未然・拡大防止対策を強力に推進することにより、これまで以上にサイバー空間の安全安心の確保に努めていく。

1　令和３年上半期における脅威の動向

(1)　ランサムウェアの情勢

ア　概要

ランサムウェアとは、感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価として金銭を要求する不正プログラムである。

従来のランサムウェアは、不特定多数の利用者を狙って電子メールを送信するといった手口が一般的であったが、現在では、ＶＰＮ機器からの侵入等、特定の個人や企業・団体等を標的とした手口に変化しており、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。

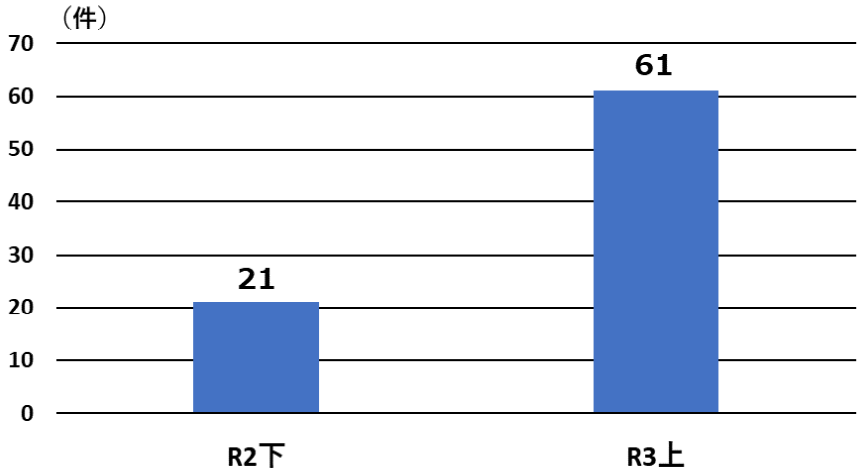
また、最近の事例では、データの暗号化のみならず、データを窃取した上、企業等に対し「対価を支払わなければ当該データを公開する」などと金銭を要求する二重恐喝（ダブルエクストーション）という手口が認められるようになっている。

イ　企業・団体等におけるランサムウェア被害

(ｱ)　被害件数

企業・団体等におけるランサムウェア被害として、令和３年上半期に都道府県警察から警察庁に報告のあった件数は61件であり、前年下半期（21件）と比べて大幅に増加した。

【図表１：企業・団体等におけるランサムウェア被害の報告件数の推移】



(ｲ)　特徴

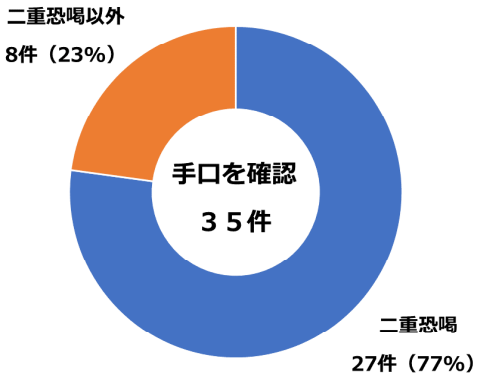
○　二重恐喝（ダブルエクストーション）による被害が多くを占める

被害件数（61件）のうち、警察として金銭の要求手口を確認できた被害は35件あり、このうち、二重恐喝の手口によるものは27件で全体の77％を占めている。

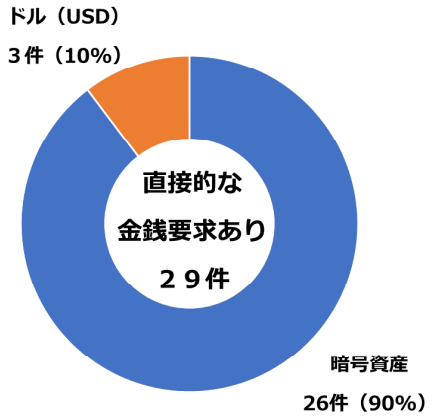
○　暗号資産による金銭の要求が多くを占める

被害件数（61件）のうち、直接的に金銭の要求があった被害は29件あり、このうち、暗号資産による支払いの要求は26件で全体の90％を占めている。

【図表２：ランサムウェア被害の手口別報告件数】



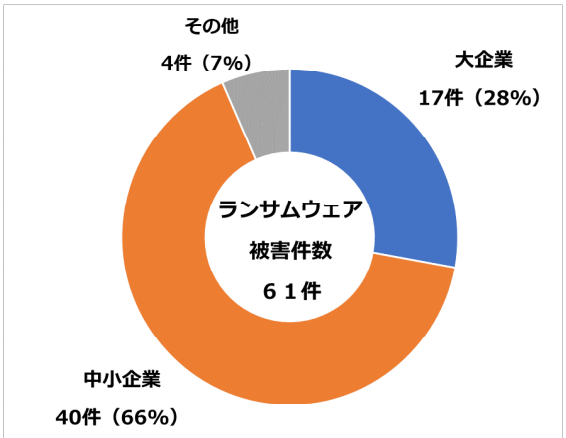
【図表３：要求された金銭支払い方法別報告件数】



○　企業・団体等の規模を問わず被害が発生

被害件数（61件）の内訳を被害企業・団体等の規模別[*4]にみると、大企業は17件、中小企業は40件であり、その規模を問わず、被害が発生している。

【図表４：ランサムウェア被害の被害企業・団体等の規模別報告件数】



注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100にならない。

*4　中小企業基本法第２条第１項に基づき分類

ウ　企業・団体等におけるランサムウェア被害の実態

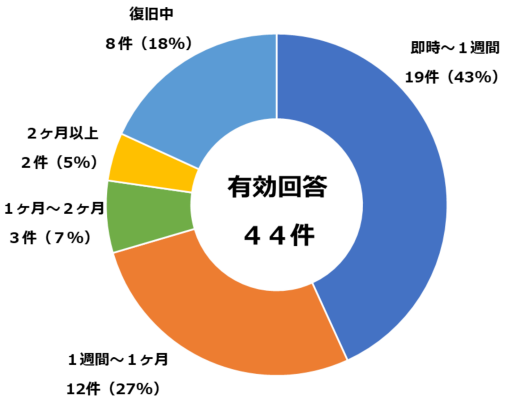
企業・団体等におけるランサムウェア被害の実態を把握するため、被害件数（61件）のランサムウェア被害に関し、被害企業・団体等にアンケート調査を実施したところ、令和３年８月末までに50件の回答が得られたことから、その回答結果について分析を行った。

(ｱ)　復旧等に要した期間・費用

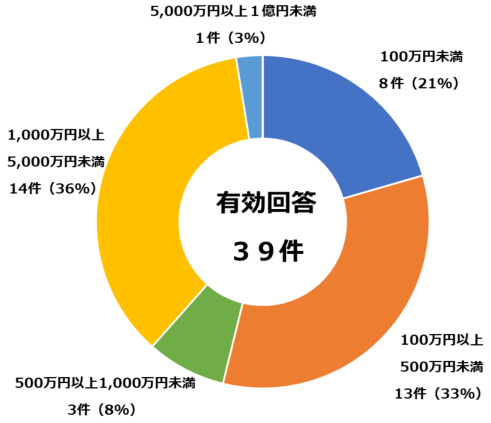
復旧に要した期間について質問したところ、44件の有効な回答があり、このうち、１週間以内に復旧したものが19件と最も多かったが、復旧に２か月以上要したものもあった。

また、ランサムウェア被害に関連して要した調査・復旧費用の総額について質問したところ、39件の有効な回答があり、このうち、1,000万円以上の費用を要したものが15件で、全体の39%を占めている。

【図表５：復旧に要した期間】



【図表６：調査・復旧費用の総額】

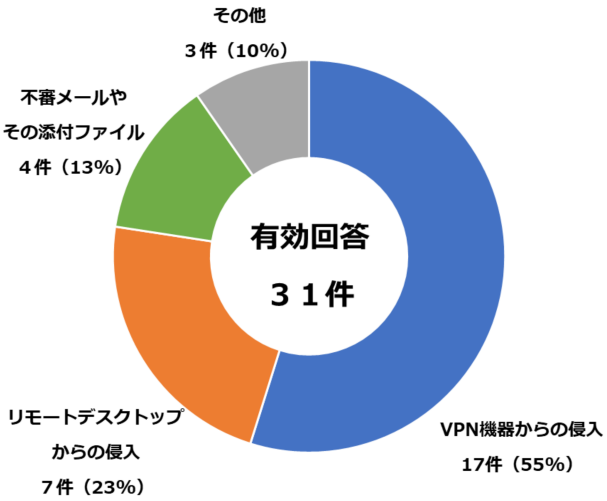


注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100にならない。

(ｲ)　感染経路

ランサムウェアの感染経路について質問したところ、31件の有効な回答があり、このうち、ＶＰＮ機器からの侵入が17件で全体の55%を占め、次いで、リモートデスクトップからの侵入が７件で全体の23%を占めており、テレワーク等の普及を利用して侵入したと考えられるものが全体の８割近くを占めている。

【図表７：感染経路】



注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100にならない。

エ　ランサムウェアの分析

警察では、ダークウェブ上のサイトを分析しており、令和３年上半期において、ランサムウェアによって流出した情報等を掲載しているリークサイトに、日本国内の事業者等の情報が掲載されたことを確認した。掲載されている情報には、財務情報や関係者、消費者等の情報が含まれ、会社の評判を落とすなどといった記載がある。

【図表８：ダークウェブ上のリークサイト例】

(2) 新型コロナウイルス感染症に関連するサイバー犯罪が疑われる事案

新型コロナウイルス感染症に関連するサイバー犯罪が疑われる事案として、令和３年６月までに都道府県警察から警察庁に報告のあった件数は109件であった。その内訳としては、詐欺が59件で全体の54.1％と最も多く、次いで不審メール・不審サイトが24件で全体の22.0％を占めている。

令和２年上半期の件数は608件であり、前年同期と比べて499件の減少となった。

(3) 主な事例

○　国内の事例

・　海洋研究開発機構に対する不正アクセス

３月、国立研究開発法人海洋研究開発機構は、同機構の基幹ネットワークシステムに対する不正アクセスが行われていたことを発表した。当該不正アクセスにより、同機構の職員等の名前、職員番号、アカウント、メールアドレス等が窃取された。

・　内閣府職員等が使用するファイル共有ストレージに対する不正アクセス

４月、内閣府は、内閣府、内閣官房、復興庁及び個人情報保護委員会の職員が使用するファイル共有ストレージが不正アクセスを受けていたことを公表した。当該不正アクセスにより、不正アクセスを受けたファイルに含まれていた231名分の個人情報が流出した可能性がある。

・　原子力規制委員会ネットワークシステムに対する不正アクセス

５月、原子力規制庁は、原子力規制委員会に対する不正アクセス事案に関する中間報告を発表した。同報告では、原子力規制委員会ネットワークシステムに対する不正アクセスにより、職員及び請負業者の認証情報を含むデータが窃取されたとしている。また、攻撃者は、窃取した職員及び請負業者の認証情報を悪用し、システム内に侵入したなどとしている。

・　プロジェクト情報共有ツールに対する不正アクセス

５月、我が国の大手ＩＴベンダーは、関係者と情報共有を行うためのプロジェクト情報共有ツールが不正アクセスを受け、当該ツールに保存されていた情報の一部が窃取されたことを発表した。窃取された情報には、我が国の政府機関等が提供した情報が含まれていたほか、官民の参加したサイバーセキュリティに関する情報共有訓練に関する情報が含まれていた。

・　異性紹介サービス等を提供する事業者に対する不正アクセス

５月、異性紹介サービス等を提供する事業者は、当該サービスに係るサーバが不正アクセスされたと発表した。当該不正アクセスにより、同社顧客の年齢確認審査書類合計約171万件の運転免許証、健康保険証、パスポート等の画像データが流出した可能性があるとしている。

○　国外の事例

・　米国司法省による北朝鮮ハッカーの起訴

２月、米国司法省は、過去のサイバー攻撃事案に関与したとして、サイバー攻撃集団「Lazarus」に所属する北朝鮮ハッカー３名を起訴したと発表した。起訴内容には、2014年の米国ソニー・ピクチャーズ・エンターテインメントに対するシステム破壊を伴うサイバー攻撃、2015年から2019年にかけて実行されたバングラデシュ中央銀行等に対する金銭窃取を目的としたサイバー攻撃、2017年に世界各国の政府機関、病院、銀行、企業等に被害を発生させたランサムウェア「Wannacry」を用いたサイバー攻撃等が含まれている。

・　SolarWinds社製ソフトウェアのぜい弱性を利用したサイバー攻撃等に対する制裁

４月、米国は、同国の大手ソフトウェア開発企業SolarWinds社製ソフトウェアのぜい弱性を利用したサイバー攻撃等に関連して、対ロシア制裁を発動する大統領令を発出した。外交官10名の追放、32の団体・個人への制裁対象追加等の措置が発動された。また、当該サイバー攻撃は、ロシア対外情報庁（ＳＶＲ）を背景とするサイバー攻撃集団「APT29」が実行したと断定している。

・　米国石油パイプラインの操業停止

５月、米国石油パイプライン事業者最大手のコロニアル・パイプラインのシステムがランサムウェアに感染したことにより、同社が管理する全てのパイプラインの操業が停止した。これを受けて、米国政府は、当該攻撃がロシアのハッカー集団「DarkSide」によるものであると断定した上、サイバーセキュリティ強化のための大統領令を発出した。

(4)　警察における取組

○　警察のアトリビューションにより国家レベルの関与を明らかにしたサイバー攻撃事案

・　レンタルサーバ不正契約事件被疑者の検挙

中国共産党員の男（30代）は、平成28年９月から平成29年４月までの間、合計５回にわたり、住所、氏名等の情報を偽って日本のレンタルサーバの契約に必要な会員登録を行った。警視庁公安部は、令和３年４月、同男を私電磁的記録不正作出罪・同供用罪で検挙した。

・　一連のサイバー攻撃に関与した背景組織の特定

本事件の捜査を通じ、警察では、同男が不正に契約したレンタルサーバが宇宙航空研究開発機構（ＪＡＸＡ）等に対するサイバー攻撃に悪用されたことを把握するとともに、同攻撃の実態解明の過程で、同一の攻撃者が関与している可能性が高いサイバー攻撃が約200の国内企業等に対して実行されたことを把握した。

本事件被疑者・関係者の供述をはじめ数多くの証拠を積み上げた結果、これらのサイバー攻撃がTickと呼ばれるサイバー攻撃集団によって実行されたものであり、このTickの背景組織として山東省青島市を拠点とする中国人民解放軍第61419部隊が関与している可能性が高いと結論付けるに至った。

・　被害企業等に対する注意喚起

警察では、これらのサイバー攻撃を認知後、被害企業等に対し、速やかに不正プログラムへの感染可能性や有効な対応策について個別に情報提供を実施した[*5]。

また、一連のサイバー攻撃は、日本製ソフトウェアのぜい弱性が悪用されたゼロデイ攻撃[*6]であったことから、このソフトウェアの開発企業と協力し、ぜい弱性の存在と有効な対応策について広く周知した。

○　スマートフォン決済サービスを利用した不正振替事犯に係る対策

・　スマートフォン決済サービスを利用した不正振替事犯の検挙

令和２年９月に確認された、スマートフォン決済サービスと不正に入手した銀行口座情報を連携して、不正な振替（チャージ）を行い、商品を購入した事犯について、令和３年６月までに、男女８人を詐欺等で検挙した。

・　関係団体に対する要請等

事業者が提供するスマートフォン決済サービスに関して、同社と業務提携する金融機関に開設された口座情報を不正に入手・連携し、不正な振替（チャージ）を行う手口等について、金融庁及び関係団体に対して情報提供するとともに、金融機関及びスマートフォン決済サービス提供事業者における不正防止対策の強化を要請するなど、スマートフォン決済サービスを利用した不正振替事犯に係る対策を実施した。

○　犯罪インフラ化するＳＭＳ認証代行に係る対策

・　ＳＭＳ認証代行の検挙

専門学校生の男は、令和元年９月、ＩＰ電話アプリのアカウント作成に必要な電話番号及びＳＭＳ認証コードを他人に譲渡し、アカウントを不正に作出させ、利用者本人の情報が登録されていないアプリを利用可能にした。令和２年７月、男を私電磁的記録不正作出・同供用で検挙した。

・　関係団体に対する要請等

サービス利用時の本人確認として広く用いられているＳＭＳ認証を不

---

*5　令和３年４月時点、これら被害企業等において情報流出等の被害は確認されていない。

*6　ＯＳやアプリケーションのぜい弱性に対応するパッチがソフトウェアの開発企業等から提供される前に、そのぜい弱性を悪用して行われる攻撃の総称

正に代行し、第三者に不正にアカウントを取得させる事例が確認されたことから、総務省と連携して、一般社団法人テレコムサービス協会ＭＶＮＯ委員会に対し、契約時の確実な本人確認を要請した。同要請を受け、加盟事業者の自主的な取組として、ＳＭＳ機能付きデータ通信契約に係る本人確認実施が申し合わされた。また、警察庁では、都道府県警察に対し、ＳＭＳ認証代行を含む犯罪インフラに関し、法令に違反する悪質事業者に対する取締りの強化を指示した。

○　重要インフラ事業者等に対する注意喚起

重要インフラ事業者、東京大会関連事業者等に対してサイバー攻撃に関する注意喚起を継続的に実施しており、ＩＴ監視システムのぜい弱性を狙ったサイバー攻撃に関する注意喚起、サーバソフトウェアのぜい弱性を狙ったサイバー攻撃に関する注意喚起等を実施した。

○　共同対処訓練の実施

重要インフラ事業者、東京大会関連事業者等とのサイバー攻撃の発生を想定した共同対処訓練を実施した。会場制御システムに対するサイバー攻撃を想定した共同対処訓練を公益財団法人東京オリンピック・パラリンピック競技大会組織委員会や競技会場を管理する事業者と実施するなど、開催を間近に控えた東京大会に向けて、サイバー攻撃対策についての詰めの調整・確認を進め、大会の安全・円滑な開催に万全を期した。

○　Ｃ２サーバ[*7] のテイクダウン

サイバー攻撃事案で使用された不正プログラムの解析等を通じて把握した国内のＣ２サーバについて、サーバを管理する事業者等に働きかけ、不正に蔵置されたファイルを削除するなどのＣ２サーバのテイクダウン（機能停止）を行うよう依頼するなどして、Ｃ２サーバの対策を継続的に実施している。この結果、22件のＣ２サーバのテイクダウンを行った。

○　マルウェアに感染している機器の利用者に対する注意喚起

海外の捜査当局から警察庁に対し、国内のEmotetに感染している機器に関する情報提供があったことから、総務省等と連携し、当該情報をインターネットサービスプロバイダ（ＩＳＰ）に提供し、ＩＳＰにおいて機器の利用者に対する注意喚起を実施した。

○　偽の特別定額給付金の申請サイトに誘導するメールに関する注意喚起

前年に引き続き、総務省を装って特別定額給付金に関するメールを送信し、偽の特別定額給付金の申請サイトに誘導する手口を確認したことから、ＪＣ３と連携し、ＪＣ３のウェブサイト等において注意喚起を実施した。

---

*7　Command and Control server（指令制御サーバ）の略。Ｃ＆Ｃサーバと省略する場合もある。制御の中心として、不正プログラムに感染した端末に指令を送り動作させるなどするサーバのこと。

○　金融機関等を装ったフィッシングの攻撃者グループの手口分析

ＪＣ３と連携し、国内の金融機関等を装ったフィッシングについて分析を行い、その特徴から攻撃者グループを分類、それら攻撃者グループによるフィッシングの手口について、ＪＣ３のウェブサイト等において注意喚起を実施した。

○　新型コロナワクチンの接種予約を装うフィッシングに関する注意喚起

新型コロナワクチンの接種予約を装うＳＭＳにより、フィッシングサイトへ誘導したり、不正プログラムに感染させたりする手口について、ＪＣ３と連携し、ＪＣ３のウェブサイト等において注意喚起を実施した。

２　サイバー空間の脅威情勢

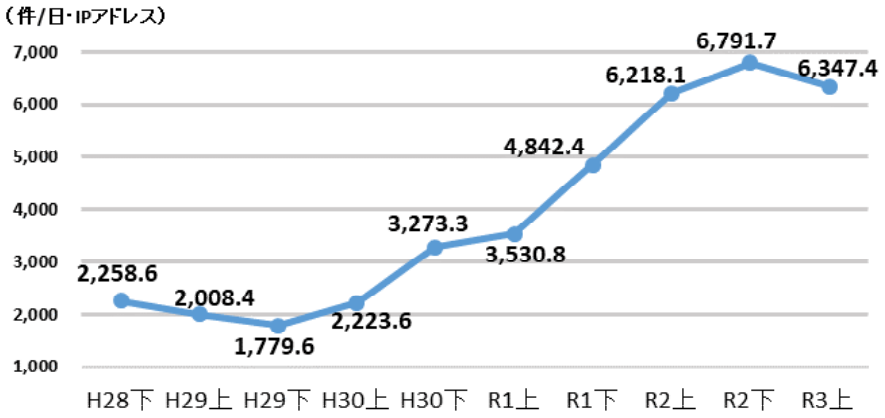
(1)　サイバー空間におけるぜい弱性探索行為等の観測状況

ア　センサーにおいて検知したアクセスの概況

警察庁では、インターネット上にセンサーを設置し、当該センサーに対して送られてくる通信パケット[*8] を収集している。このセンサーは、外部に対して何らサービスを提供していないため、本来であれば外部から通信パケットが送られてくることはないが、攻撃者が攻撃対象を探索する場合等に、不特定多数のＩＰアドレスに対して無差別に送信される通信パケットを観測することができる。この通信パケットを分析することで、インターネットに接続された各種機器のぜい弱性の探索行為やそれらを悪用した攻撃、不正プログラムに感染したコンピュータの動向等、インターネット上で発生している各種事象を把握することができる。

令和３年上半期に本システムにおいて検知したアクセス件数は、１日・１ＩＰアドレス当たり6,347.4件と令和２年上半期から継続して高水準で推移している。アクセス件数が継続して高い水準にあるのは、ＩｏＴ機器の普及により攻撃対象が増加していること、テレワークが普及する中テレワーク環境で使われるＶＰＮ製品やＷｅｂ会議サービス等のぜい弱性が公開され、それを攻撃者が悪用していることなどが背景にあるものとみられる。

【図表９：センサーにおいて検知したアクセス件数の推移】



イ　特徴的な観測

○　単一の送信元からの広範な宛先ポートへのアクセスが高い水準で推移

検知したアクセスの宛先ポート[*9] に着目すると、ポート番号1024以上

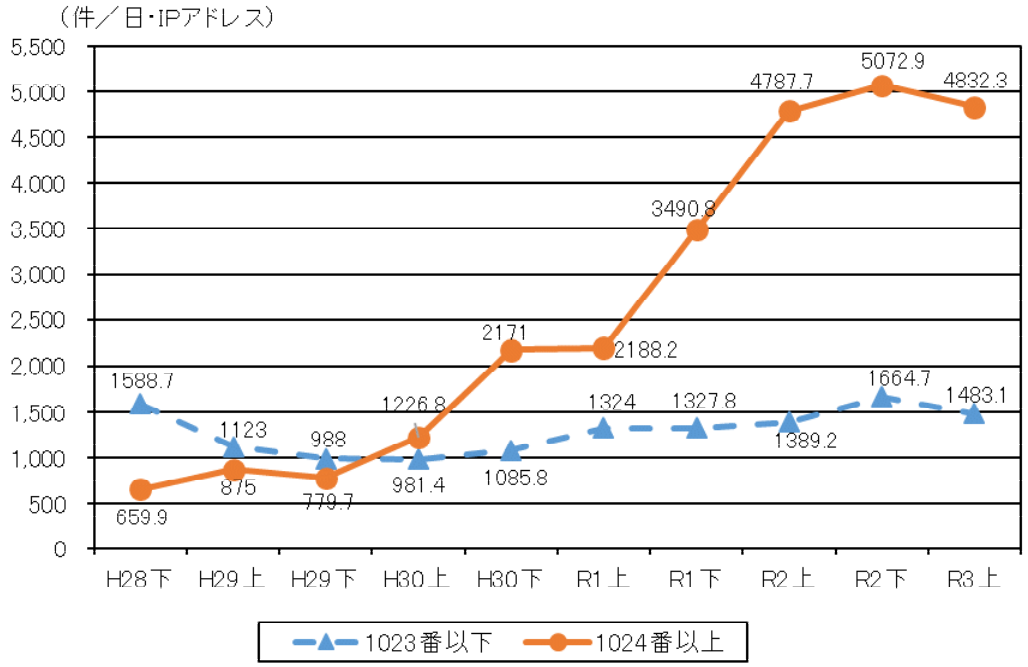
---

*8　ネットワークを通して送信される際に分割されるデータのかたまりのことであり、各パケットには、送信先や送信元のＩＰアドレス等の情報が付加されている。

*9　ＴＣＰ・ＵＤＰ/ＩＰ通信において、通信を行うコンピュータが、利用するサービスを識別するためのインターフェースのこと。０から65535までの番号が割り当てられている。

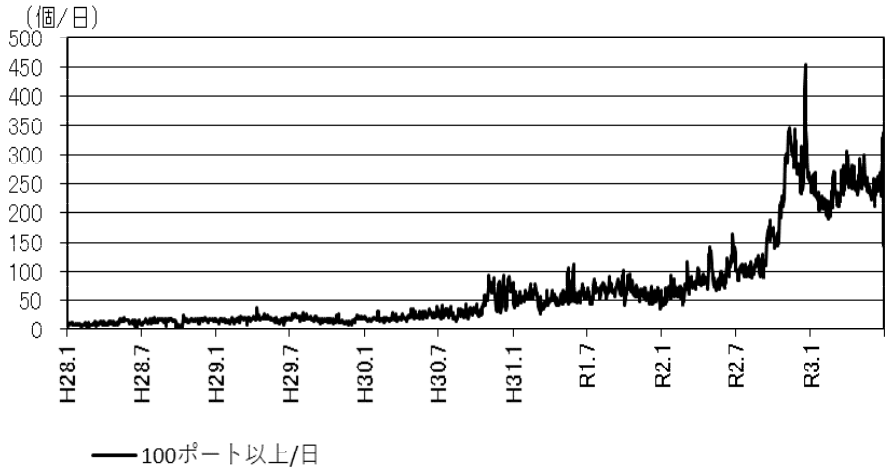
のポートへのアクセス件数が高い水準で推移しており、全体のアクセス件数が高い水準で推移する要因となっている。1024以上のポートは、主としてＩｏＴ機器が標準設定で使用するポート番号であることから、多くがＩｏＴ機器に対するサイバー攻撃やぜい弱性を有するＩｏＴ機器の探索行為であるとみられる。

【図表10：検知したアクセスの宛先ポートで比較した１日・１ＩＰアドレス当たり件数の推移】



また、単一の送信元からの広範な宛先ポートに対するアクセスは、近年増加傾向にある。１日に100個以上の宛先ポートに対してアクセスを行った送信元ＩＰアドレス数の推移は、平成28年から30年上半期にかけて同水準で推移していたが、30年下半期から増加傾向となり、令和２年下半期に急増し、令和３年上半期は高い水準で推移した。

【図表11：１日に100個以上の宛先ポートに対してアクセスした送信元ＩＰアドレス数の推移】



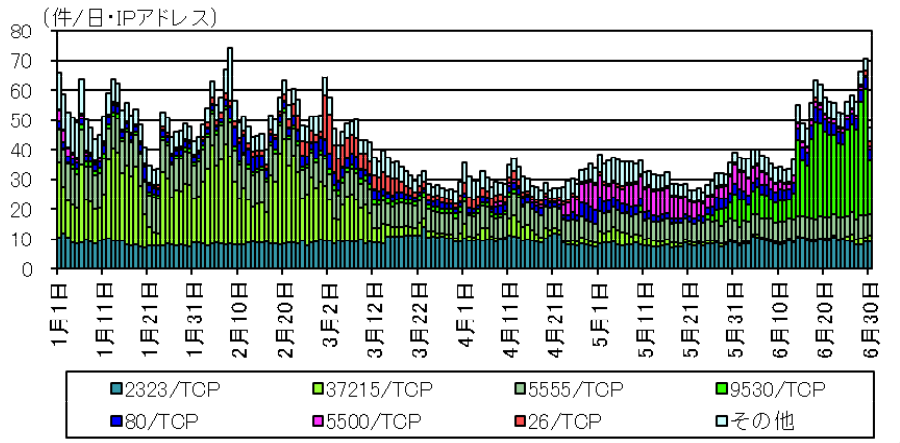
令和３年上半期における広範な宛先ポートに対してアクセスする送信元ＩＰアドレス数は、１日当たり242.5個で、前年同期の82.2個と比較して、160.3個（195.0%）増加した。

送信元ＩＰアドレス数の増加の背景には、インターネットに接続されている機器やそれらが行っているサービス、さらに、そのぜい弱性の有無を網羅的かつ短期間に把握しようとする組織等が増加していることや攻撃者がボットネットを利用することで手軽な探索が可能になっていることなどがあると考えられる。把握した情報を悪用された場合は、前触れなく様々な攻撃が行われたり、短期間に広範囲の攻撃を行われたりするなどの被害が懸念される。

○　ＩｏＴ機器等のぜい弱性を狙ったアクセスの観測

令和３年上半期の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230.7件で、前年同期の547.7件と比較して、317.0件減少しているものの、Miraiが大流行した平成28年以降、一定数継続的に観測している。観測したアクセスを宛先ポート別に見ると、３月中旬まで、宛先ポート37215/ＴＣＰに対するアクセスを観測したが、これは、海外製ルータ等に使われる宛先ポートであり、遠隔から任意のコードが実行可能となるぜい弱性を悪用し、不正プログラムの感染拡大を狙ったものと考えられる。また、５月下旬から、宛先ポート9530/ＴＣＰに対するアクセスの増加を確認したが、これは、海外製ビデオレコーダ等に使われる宛先ポートであり、遠隔から接続可能となるバックドアのぜい弱性を悪用し、不正プログラムの感染拡大を狙ったものと考えられる。

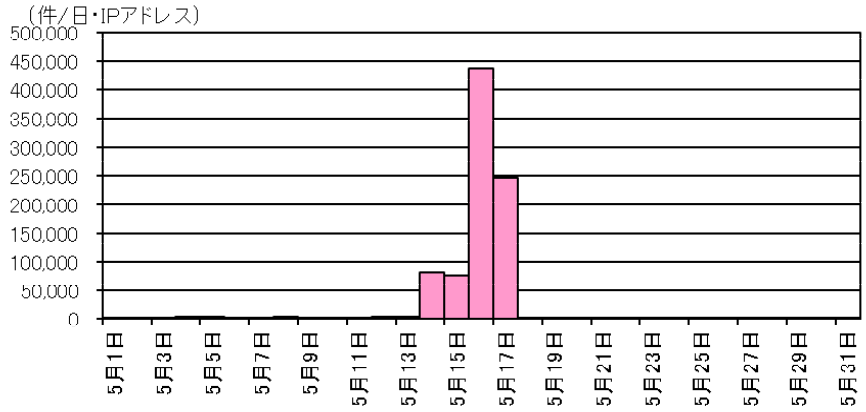
【図表12：Miraiボットの特徴を有するアクセス件数の推移（23/ＴＣＰを除く宛先ポート別）】



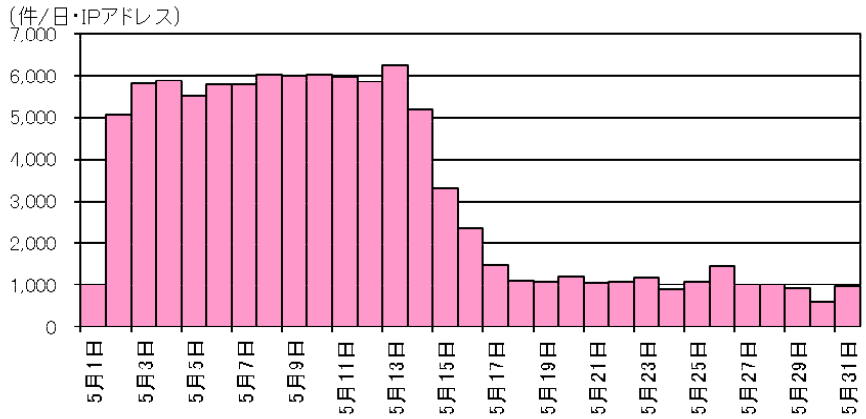
○　リモートデスクトップサービスを標的とした広範な宛先ポートに対するアクセスの観測

リモートデスクトップサービス(Microsoft Windowsの遠隔操作に利用)は、職場等に設置されたコンピュータのデスクトップ環境を、別の場所に設置されたコンピュータから閲覧・操作などできるサービスであり、テレワーク等で利用されている。５月中旬、リモートデスクトップサービスを標的とした特定の地域からのアクセスの急増を観測した。５月上旬には、同地域からの広範な宛先ポートに対するアクセスの増加を観測しており、この探索行為で把握した情報を使用し、５月中旬の短期間に、リモートデスクトップサービスを標的とした攻撃が行われたとみられる。

【図表13：特定の地域の送信元ＩＰアドレスからのリモートデスクトップサービスを標的としたアクセス件数の推移】



【図表14：特定の地域の送信元ＩＰアドレスからの広範な宛先ポートに対するアクセス件数の推移】

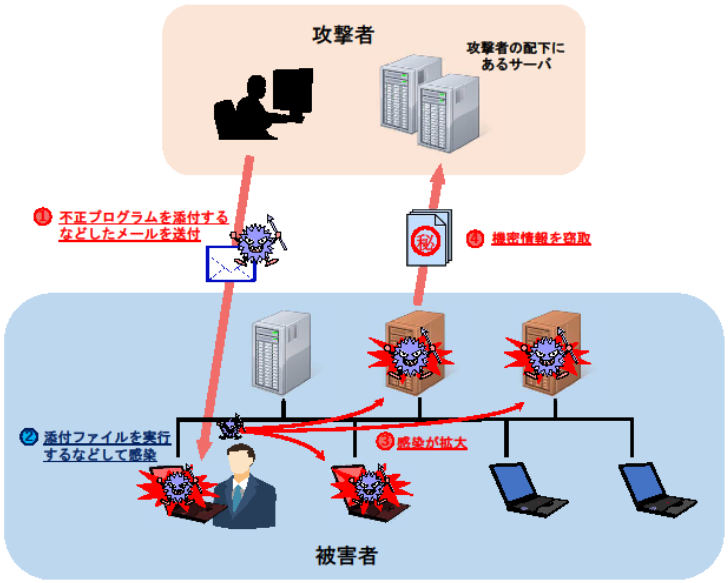


(2)　標的型メール攻撃

ア　サイバーインテリジェンス情報共有ネットワーク

警察と先端技術を有する全国約8,200の事業者等（令和３年７月現在）との間で、情報窃取を企図したとみられるサイバー攻撃に関する情報共有を行う枠組みであるサイバーインテリジェンス情報共有ネットワークを構築しており、このネットワークを通じて事業者等から提供された標的型メール攻撃[*10]をはじめとする各種情報を集約するとともに、これらの情報を総合的に分析して、事業者等に対し、分析結果に基づく注意喚起を行っている。また、内閣サイバーセキュリティセンター（ＮＩＳＣ）と連携し、政府機関に対する標的型メール攻撃の分析結果についても情報を共有している。

【図表15：標的型メール攻撃による情報窃取の例】



イ　事例

サイバーインテリジェンス情報共有ネットワークを通じて事業者等から情報提供を受けた標的型メール攻撃等には以下のようなものがあった。

令和３年上半期においても、事業者等に対して、業務に関連させた精巧な内容の標的型メール攻撃が実行された。このほか、パスワード等の窃取を企図したとみられるフィッシングメールをはじめとする不審なメールも

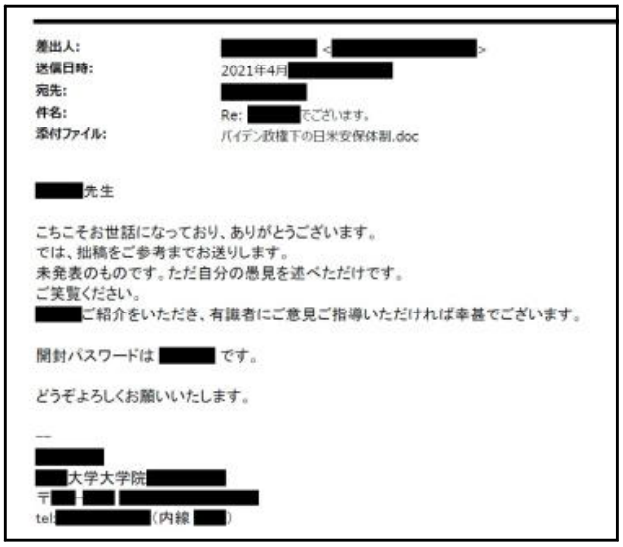
---

*10　警察庁では、業務に関連した正当なものであるかのように装った電子メールを送信し、添付ファイルやリンク先からダウンロードされるファイルを介して受信者のコンピュータを不正プログラムに感染させるものであって、市販のウイルス対策ソフトでは検知できないものを「標的型メール攻撃」として集計している。

事業者に送信されていたことが確認されている。

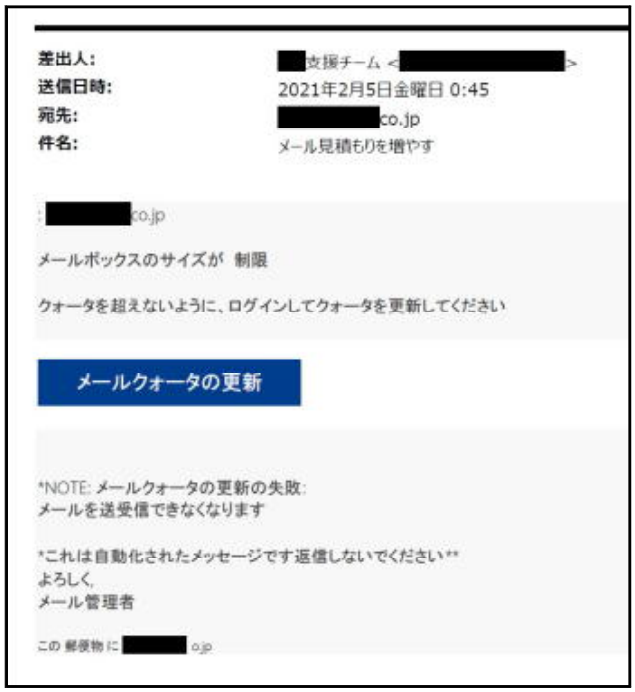
① シンクタンクに対する標的型メール攻撃

大学の研究者をかたり、「バイデン政権下の日米安保体制」と題して、不正プログラムが仕掛けられた添付ファイルを開くよう誘導する標的型メールがシンクタンクに送信された。



② 半導体関連の製造業者に送信された不審なメール

メールボックスのクォータ（割り当てられた容量）の更新と称して、リンク先からログインしてパスワード等を入力するよう誘導する不審なメールが半導体関連の製造業者に送付された。



③　機械部品関連の製造業者に送信された不審なメール

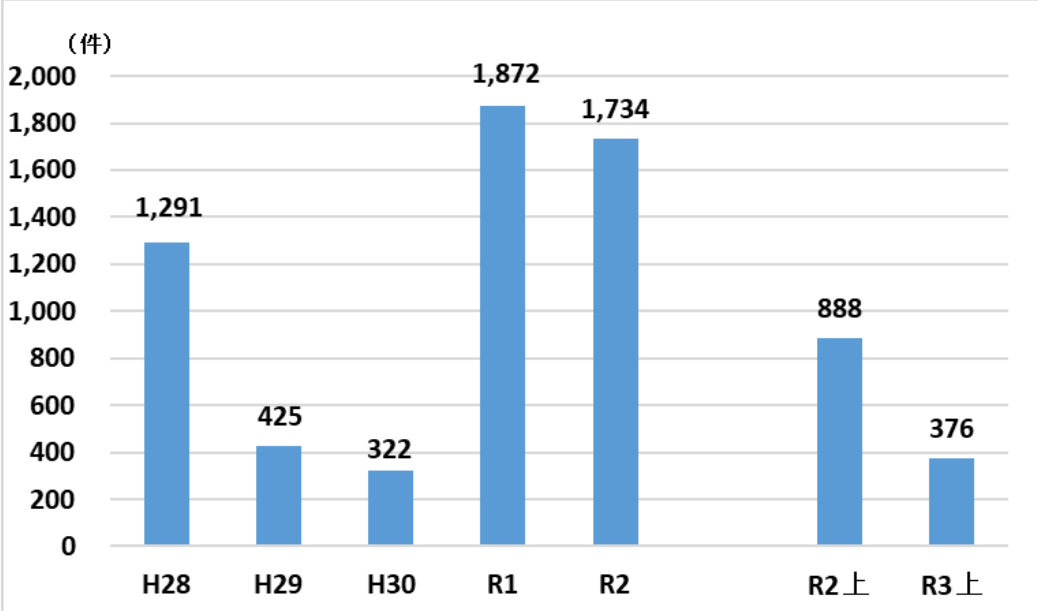
支払い依頼の確認と称して、リンク先から資料をダウンロードするよう誘導する不審なメールが機械部品関連の製造業者に送信された。

(3)　インターネットバンキングに係る不正送金事犯の発生状況等

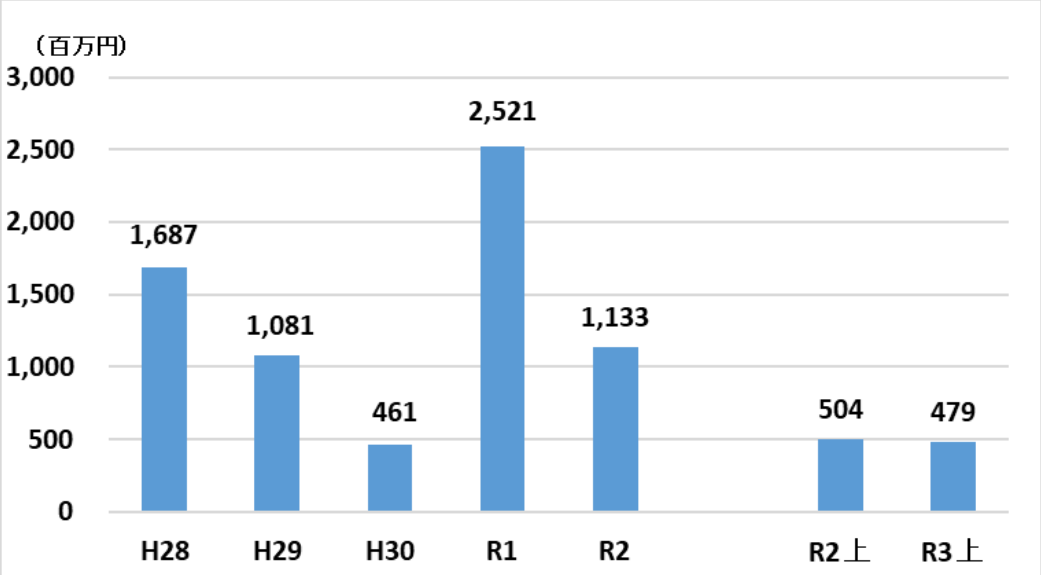
ア　概況

令和３年上半期におけるインターネットバンキングに係る不正送金事犯による被害は、発生件数376件、被害総額約４億7,900万円で前年同期と比べて発生件数、被害額ともに減少した。

【図表16：インターネットバンキングに係る不正送金事犯の発生件数の推移】



【図表17：インターネットバンキングに係る不正送金事犯の被害額の推移】



イ　特徴

・　令和３年上半期は、前年同期と比べて、発生件数は減少したものの、被害額はやや減少にとどまっており、その被害の多くは、前年から継続しているＳＭＳ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考えられる。

・　フィッシングサイトへの誘導には、金融機関を装ったＳＭＳ等のほか、宅配事業者からの荷物の配達連絡を装ったＳＭＳによって、金融機関を装ったフィッシングサイトへ誘導するものも確認されている。

・　インターネット上に情報を保存するメモアプリ等にネットバンキングのＩＤ、パスワード等を保存していたところ、同アプリ等が不正アクセスされ、保存していた情報を用いてネットバンキングに不正アクセスされ、不正送金されたと思われるケースが確認されている。

・　一次送金先として把握した574口座のうち、名義人の国籍はベトナムが40.4％と最も多く、次いで日本が26.0％、中国が5.4％であった。従来の手口である預貯金口座への不正送金のほか、暗号資産の購入や、プリペイドカードへのチャージ等の手口が確認されている。

ウ　警察における取組

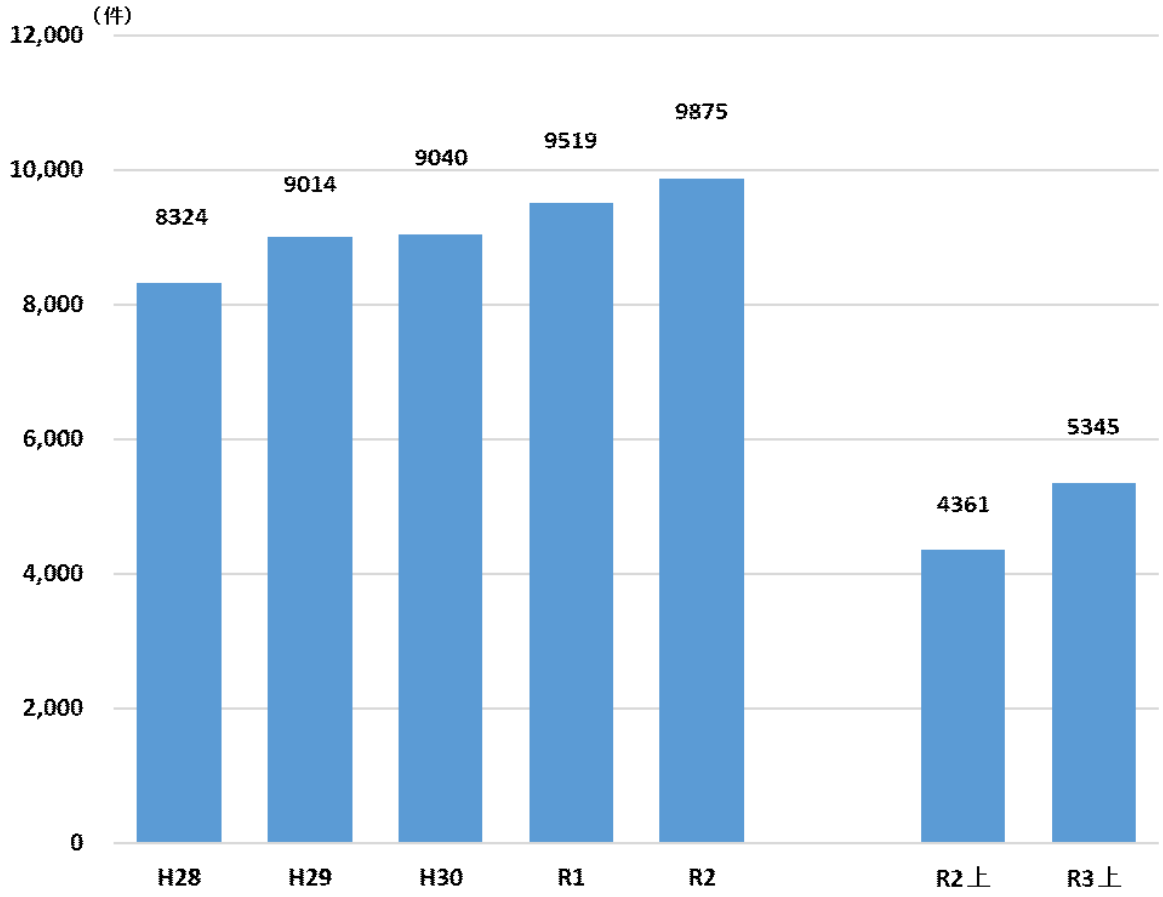
インターネットバンキングに係る不正送金事犯による被害が集中している金融機関に対して、モニタリングの強化、認証手続に係るセキュリティ強化、利用者への注意喚起の強化等の重点的な働きかけを行った。

(4)　サイバー犯罪の検挙状況

ア　サイバー犯罪の検挙件数

サイバー犯罪の検挙件数は増加傾向にあり、令和３年上半期における検挙件数は5,345件と、前年同期と比べて増加した。

【図表18：サイバー犯罪の検挙件数の推移】



イ　不正アクセス禁止法[*11] 違反

(ｱ)　検挙件数

令和３年上半期における不正アクセス禁止法違反の検挙件数は146件と、前年同期と比べて減少した。

(ｲ)　特徴

検挙件数のうち、123件が識別符号窃用型[*12] で全体の84.2%を占めている。

○　「利用権者のパスワードの設定・管理の甘さにつけ込んで入手」が最多

識別符号窃用型の不正アクセス行為に係る手口では、「利用権者のパ

---

*11　不正アクセス行為の禁止等に関する法律（「不正アクセス行為・他人の識別符号を不正に取得する行為・不正アクセス行為を助長する行為・他人の識別符号を不正に保管する行為・識別符号の入力を不正に要求する行為」の５つの違反行為が定められている。）

*12　アクセス制御されているサーバに、ネットワークを通じて、他人の識別符号を入力して不正に利用する行為

スワードの設定・管理の甘さにつけ込んで入手」が38件と最も多く、全体の30.9％を占めており、次いで「他人から入手」が22件で全体の17.9％を占めている。

○　被疑者が不正に利用したサービスは「社員・会員用等の専用サイト」が最多

識別符号窃用型の不正アクセス行為に係る被疑者が不正に利用したサービスは、「社員・会員用等の専用サイト」が33件と最も多く、全体の26.8％を占めており、次いで「オンラインゲーム・コミュニティサイト」が32件で全体の26.0％を占めている。

ウ　コンピュータ・電磁的記録対象犯罪[*13]

(ｱ)　検挙件数

令和３年上半期におけるコンピュータ・電磁的記録対象犯罪の検挙件数は317件で、前年同期と比べて増加した。

(ｲ)　特徴

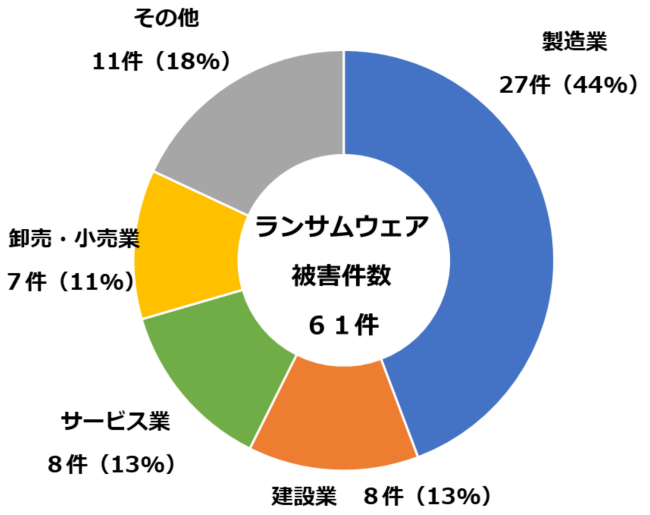
検挙件数のうち、電子計算機使用詐欺が300件と最も多く、全体の94.6％を占めている。

*13　刑法に規定されているコンピュータ又は電磁的記録を対象とした犯罪

【　参考　】

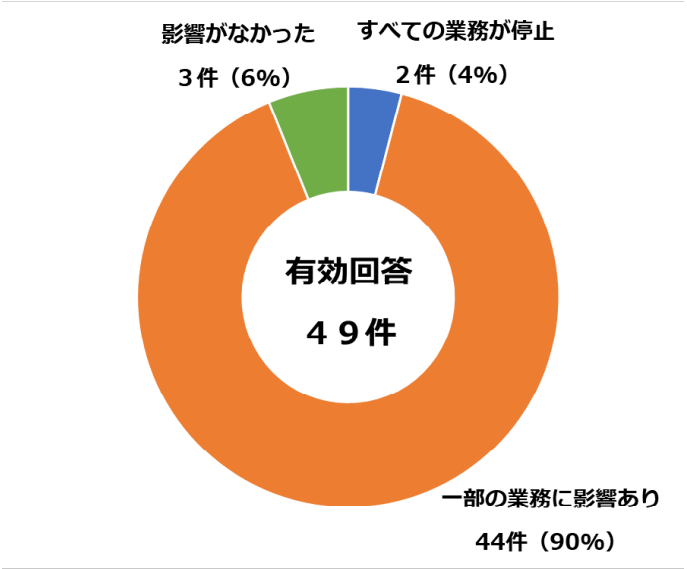
１　企業・団体等におけるランサムウェア被害及びその実態

(1)　ランサムウェア被害の被害企業・団体等の業種別報告件数

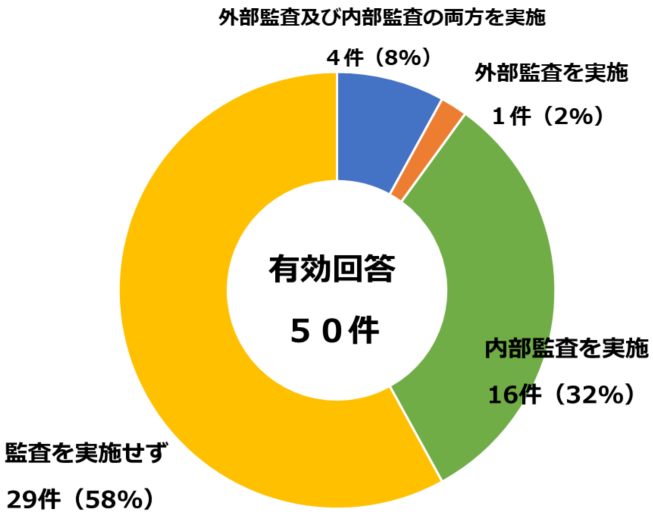


注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100にならない。

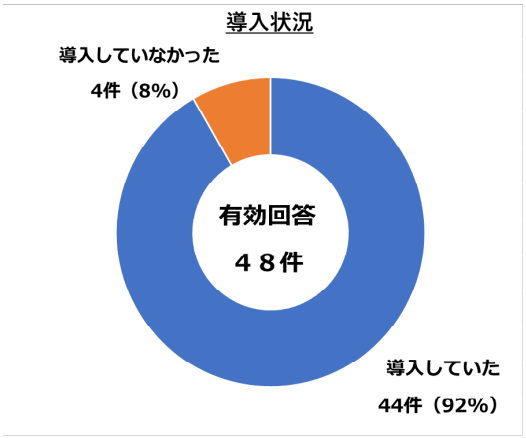
(2)　ランサムウェア被害が業務に与えた影響

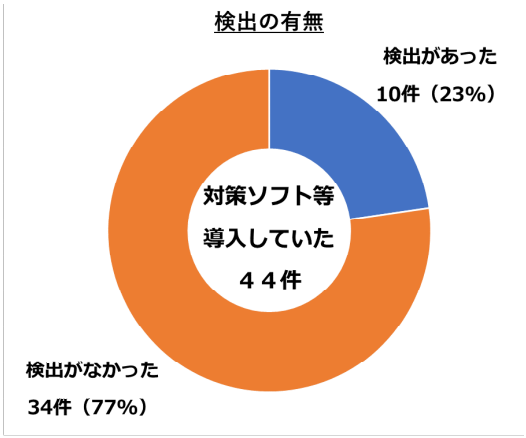


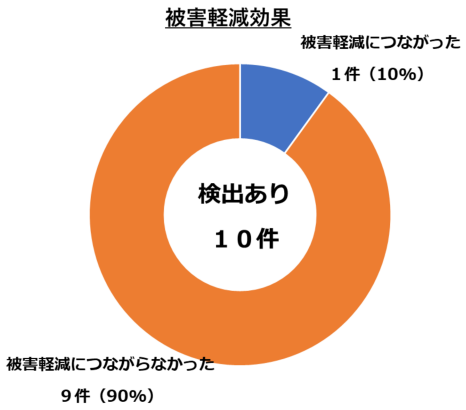
(3)　被害企業・団体等の情報セキュリティ監査の実施状況

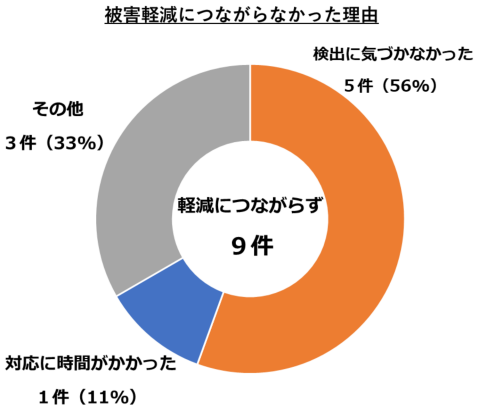


(4)　被害企業・団体等のウイルス対策ソフト等の導入・活用状況

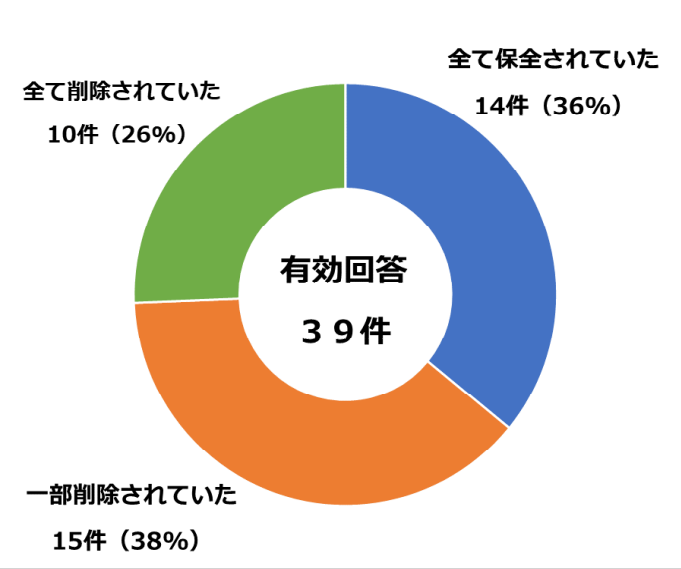




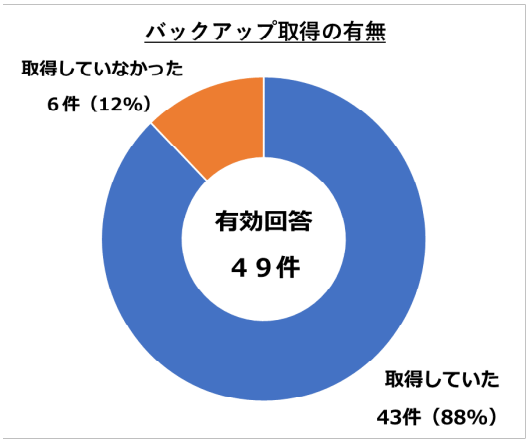


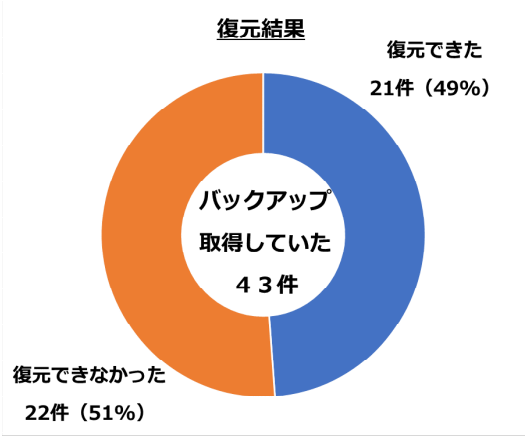


(5)　ランサムウェア被害における被害企業・団体等のログの保全状況



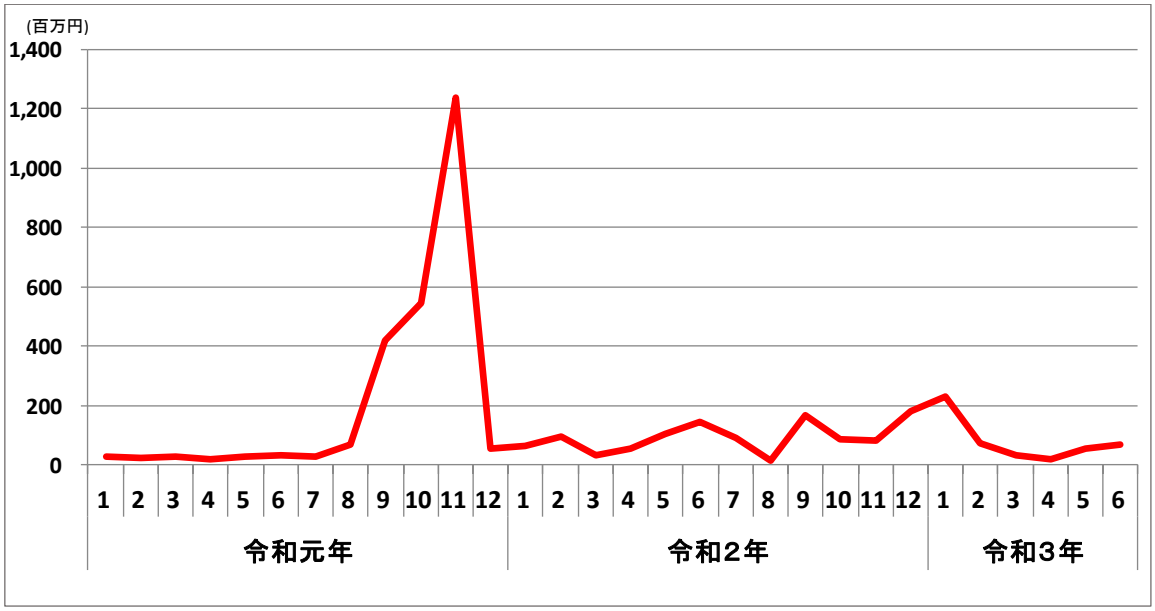
(6)　被害企業・団体等のバックアップの取得・活用状況



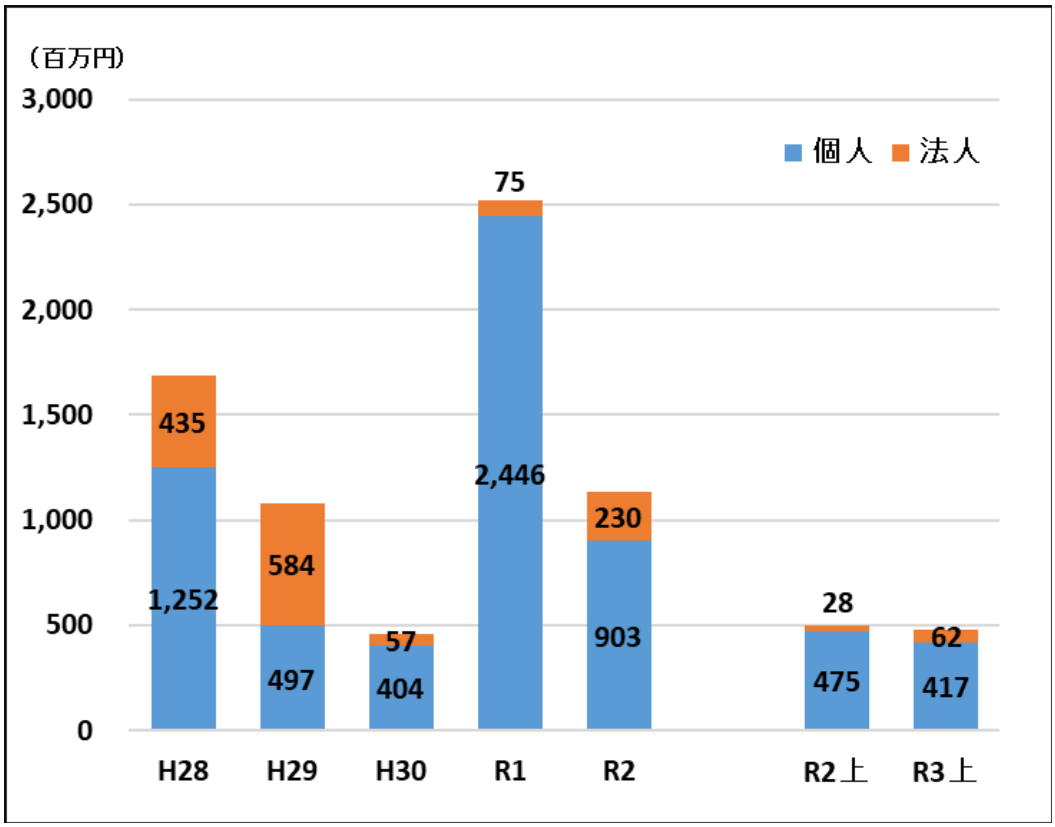


２　インターネットバンキングに係る不正送金事犯の発生状況等

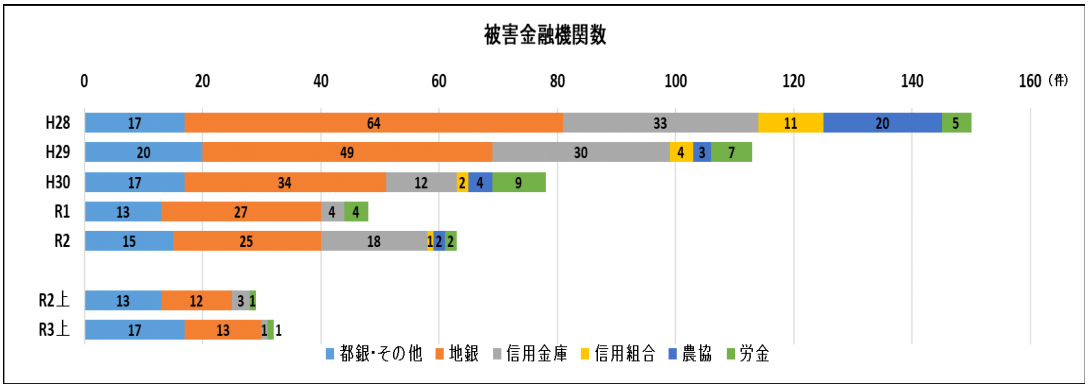
(1)　被害額の推移

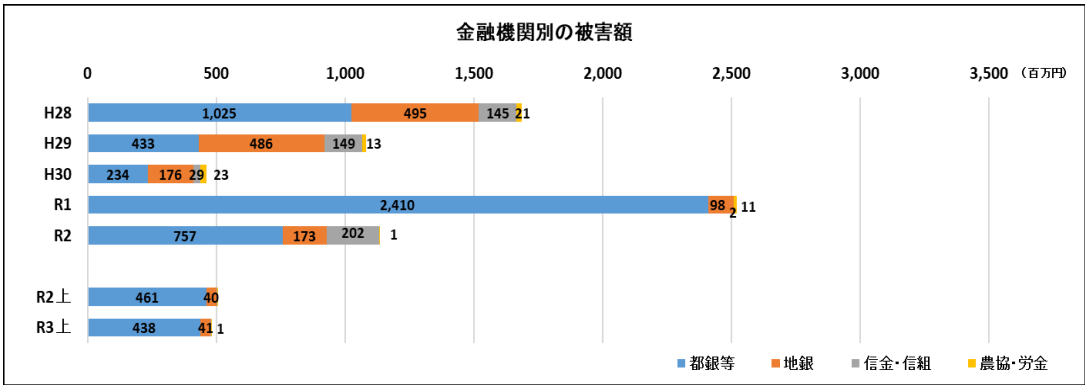


(2)　口座開設者別の被害状況

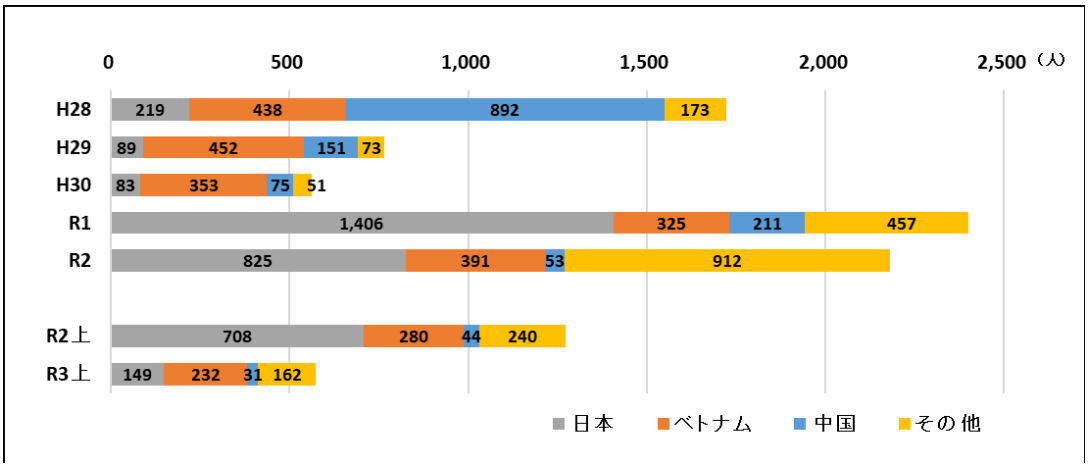


(3)　金融機関別の被害状況

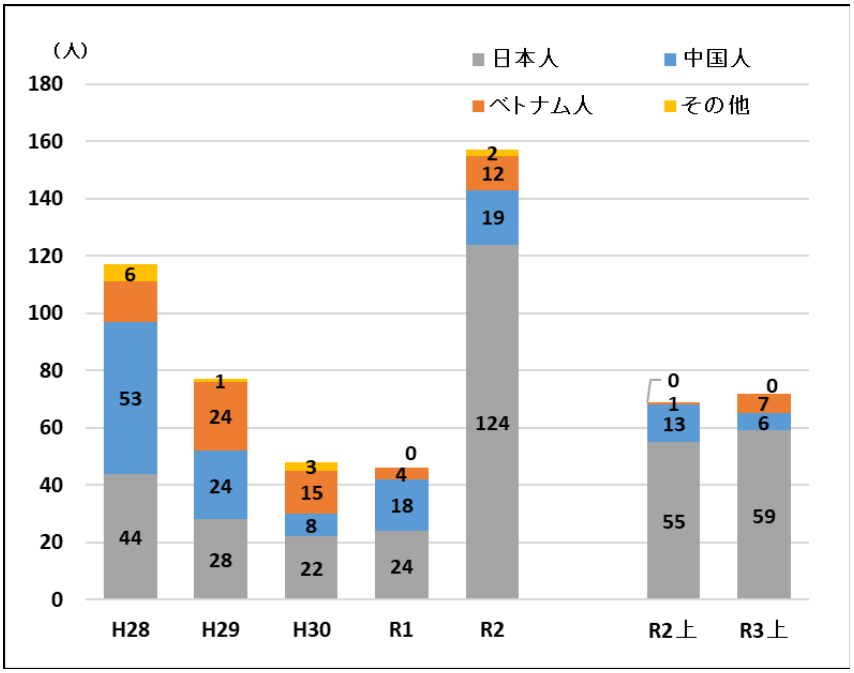




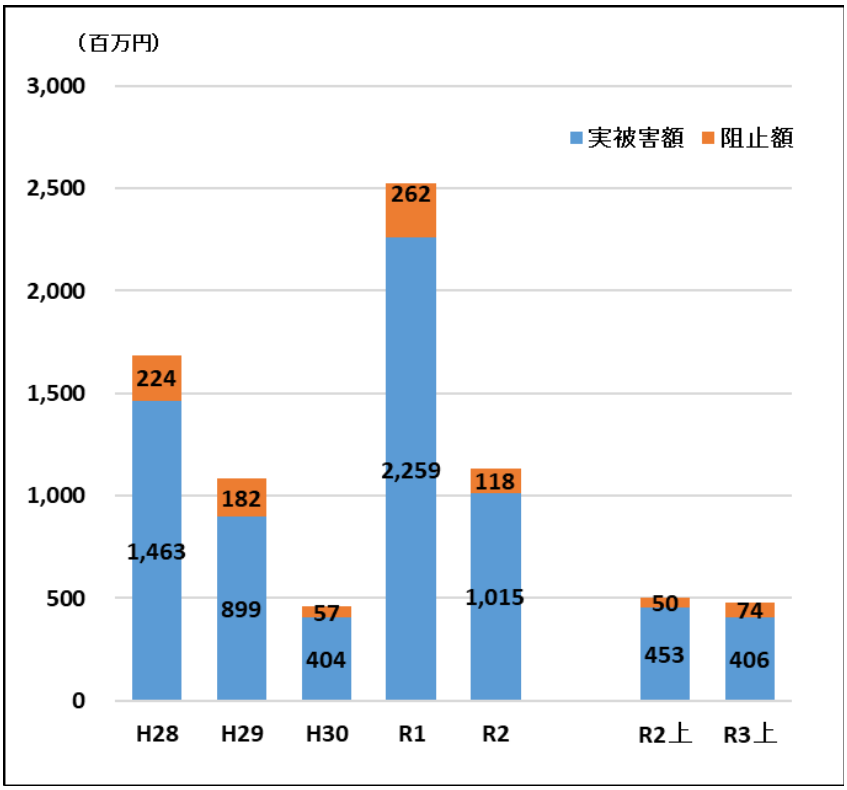
(4)　一次送金先口座名義人の国籍



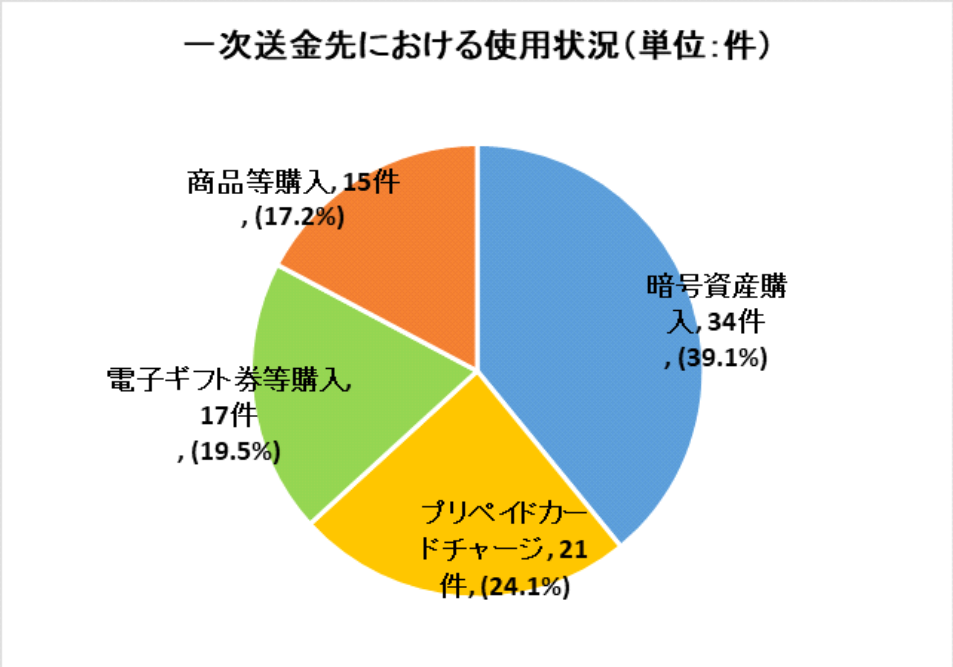
(5)　国籍別の関連事件検挙状況

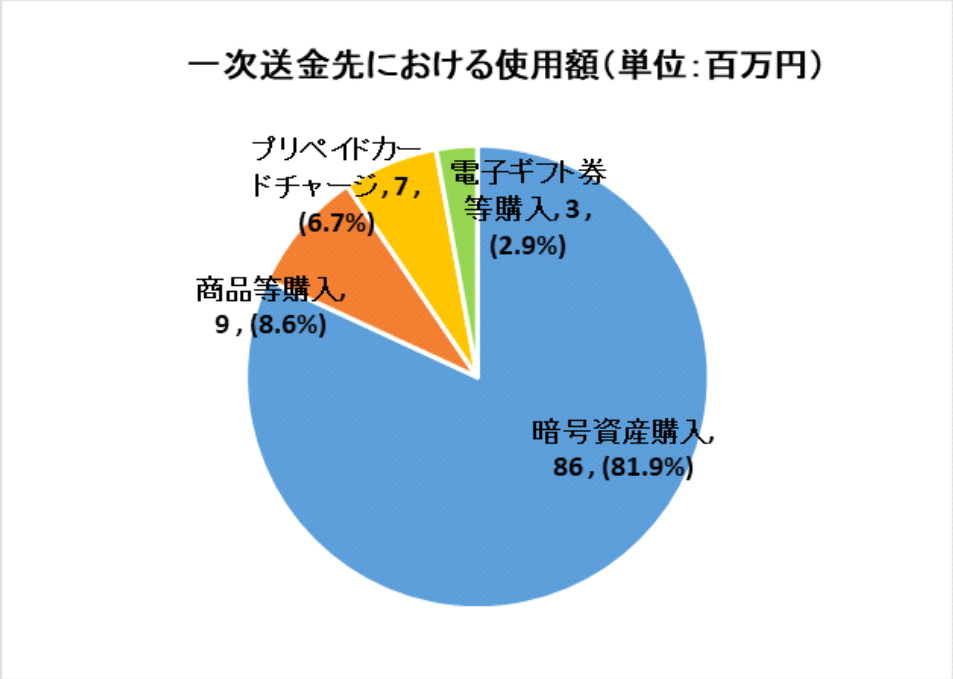


(6)　不正送金阻止状況



(7)　一次送金先における被害金の使用状況*





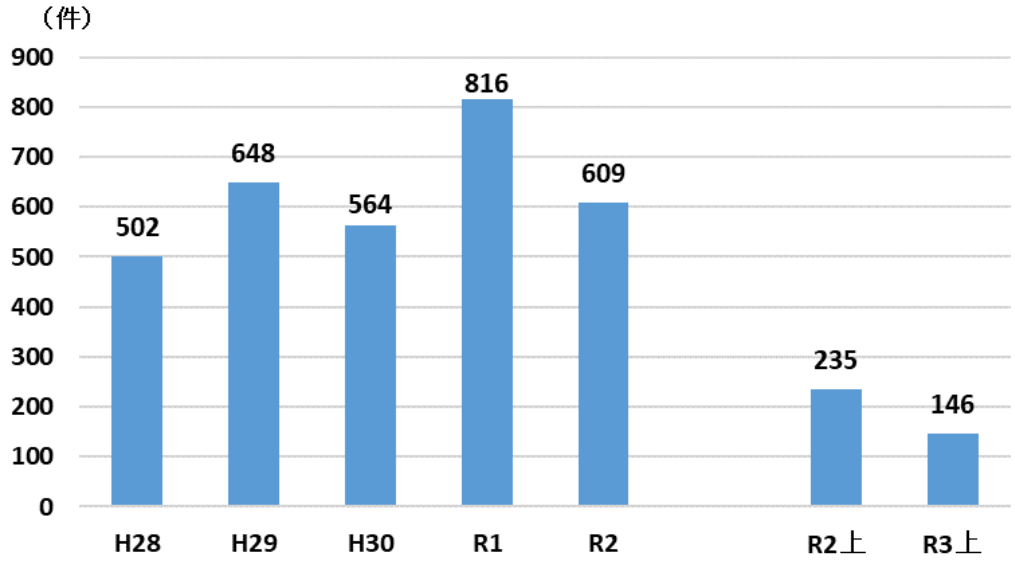
(8)　不正送金被害に係る口座名義人のセキュリティ対策実施状況

	利用していた		利用していない		不　明		合　計
ワンタイムパスワード（個人口座）	195	53.3%	109	29.8%	62	16.9%	366
電子証明書（法人口座）	1	10.0%	5	50.0%	4	40.0%	10

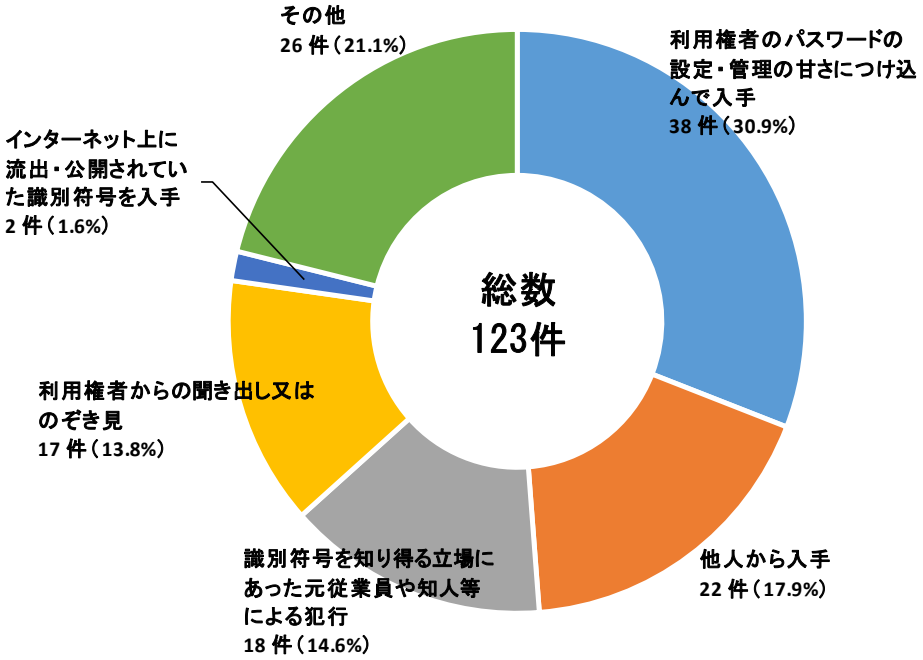
＊　警察において確認できた一次送金先における被害金の使用状況（出金・二次送金等を除く）

3　不正アクセス禁止法違反の検挙状況

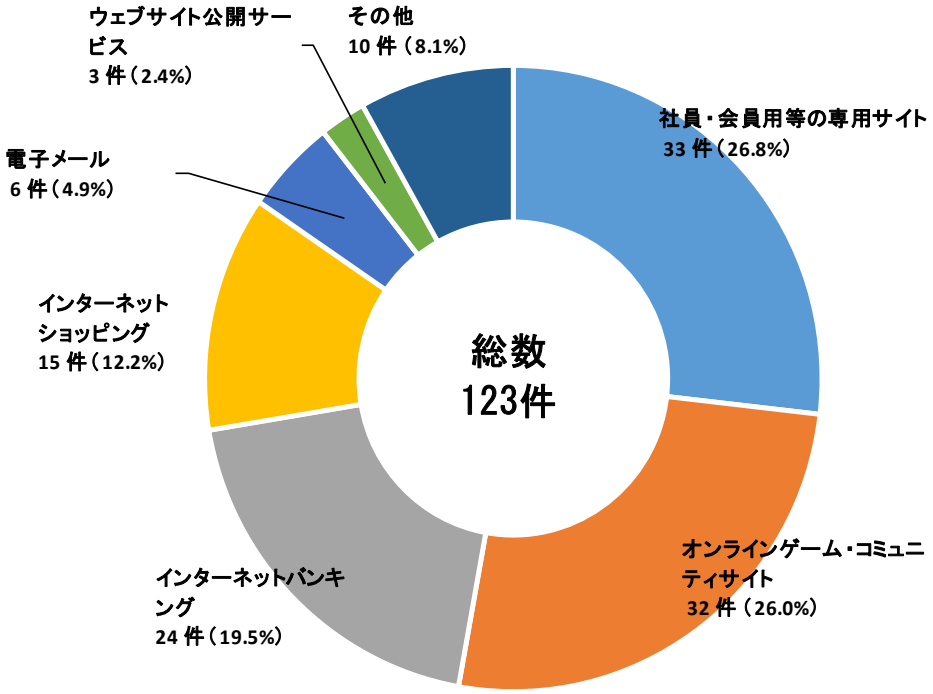
(1)　不正アクセス禁止法違反の検挙件数の推移



(2)　不正アクセス行為（識別符号窃用型）に係る手口別検挙件数



(3)　不正に利用されたサービス別検挙件数（識別符号窃用型）

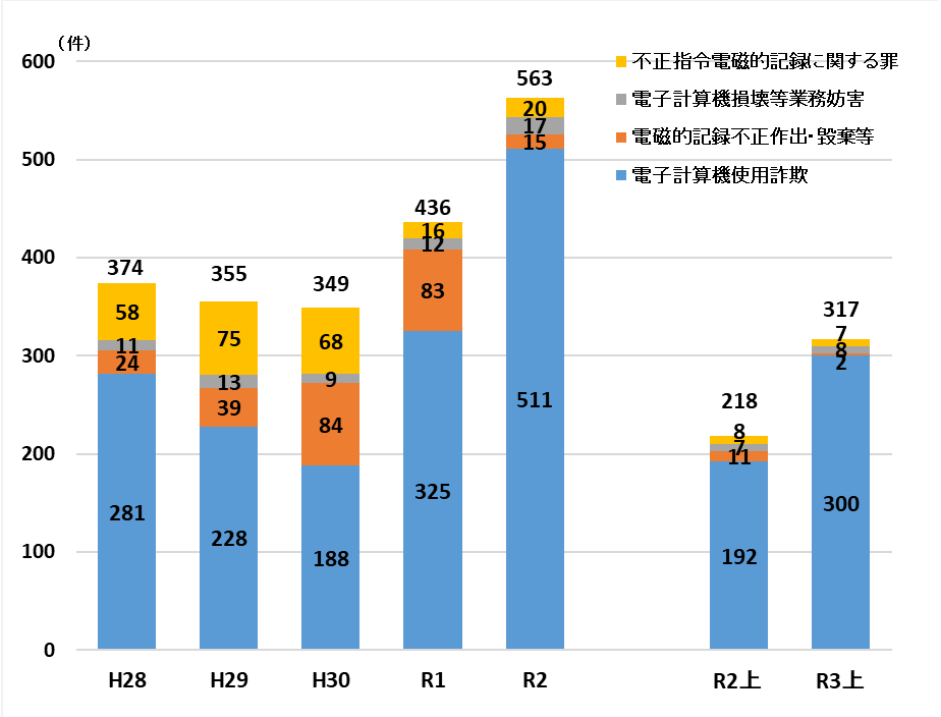


不正アクセス禁止法違反

○　会社員の女（21）は、令和２年４月、他人のＩＤ・パスワードを使用して、電気通信事業者が提供するキャリア決済サービスに不正にアクセスし、インターネット通販サイトにおいてスニーカー等を同キャリア決済により注文し窃取した。令和３年１月、女を不正アクセス禁止法違反（不正アクセス行為）及び私電磁的記録不正作出・同供用、窃盗で検挙した。

○　無職の男（23）は、令和３年１月、元交際相手のＩＤ・パスワードを使用して元交際相手が利用するＳＮＳに不正アクセスし、元交際相手になりすまして投稿等を行った。同年３月、男を不正アクセス禁止法違反（不正アクセス行為）で検挙した。

４　コンピュータ・電磁的記録対象犯罪の検挙状況



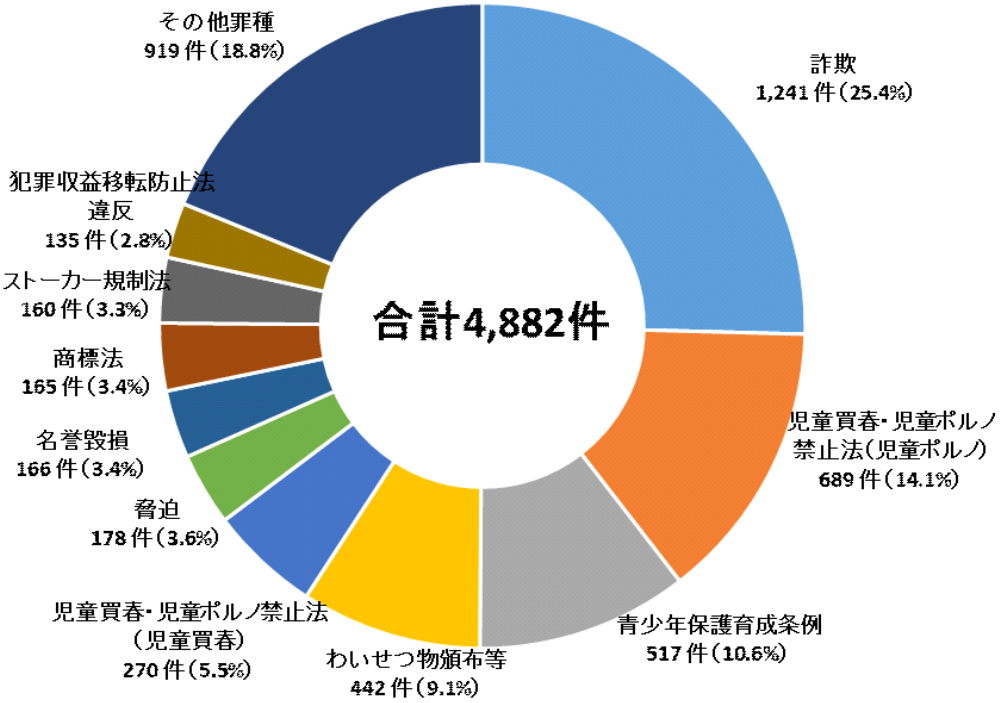
コンピュータ・電磁的記録対象犯罪

○　専門学校生の男（24）は、令和２年７月、男が管理するスマートフォン決済サービスに他人名義の銀行口座情報を連携させ、同口座から電子マネーを不正にチャージした。令和３年３月、男を私電磁的記録不正作出・同供用、電子計算機使用詐欺で検挙した。

○　会社員の男（51）は、令和２年８月、被害女性の位置情報等を盗み取る目的で、同人の使用する携帯電話機に位置情報等を送信させるなどの指令を与える遠隔操作アプリを導入したが、設定が未完了であったため、その目的を遂げなかった。令和３年３月、男を不正指令電磁的記録供用未遂で検挙した。

○　自営業の男（42）は、令和２年10月、被害男性のウェブサイトを改ざんするため、同ウェブサイトが開設されたサーバコンピュータに正当な権限を持たない者のアクセスを可能にする不正なプログラムを蔵置した。令和３年５月、男を不正指令電磁的記録供用等で検挙した。

５　その他の検挙状況



詐欺

○　無職の男（39）は、令和２年６月、芸能人が直筆したサイン色紙でないのに、直筆サイン色紙である旨の虚偽の内容の出品情報をフリマアプリに掲載し、誤信した落札者から落札代金を詐取した。令和３年２月、男を詐欺で検挙した。

不正競争防止法違反

○　無職の男（23）は、令和２年４月、家庭用ゲーム機のセーブデータの改ざんや複製等を防止するために施している技術的制限手段を無効化し、改ざん等したゲームソフトのセーブデータを顧客に提供して、不正競争を行った。令和３年２月、男を不正競争防止法違反で検挙した。