広　報　資　料
令和４年４月７日
警　　察　　庁

令和３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

１　情勢概況

デジタル化の進展等に伴い、サイバー空間の公共空間化が加速する中、ランサムウェアによる被害が拡大し、市民生活に大きな影響を及ぼす事案も確認されているほか、不正アクセスによる情報流出や、サイバー攻撃事案への国家レベルの関与も明らかとなるなど、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

○　ランサムウェアによる被害が拡大。国内の医療機関が標的となり、市民生活にまで重大な影響を及ぼす事案も確認。

○　Ｇ７各国の法執行機関等が参加する「ランサムウェアに関するＧ７高級実務者会合」が開催されるなど、世界各国において、ランサムウェア被害の防止に向けた諸対策が喫緊の課題。

○　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増加。大半が海外からのものであり、海外からの脅威が引き続き高まっている。

○　国内の政府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窃取された可能性のある事案が相次いで確認されたほか、サイバー攻撃事案の実態解明を推進する中で、国家レベルの関与が明らかとなった事例も確認。

３　警察における取組

○　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４月に警察庁にサイバー警察局、関東管区警察局にサイバー特別捜査隊を設置。

○　サイバー攻撃事案に関する各種捜査により、中国人民解放軍が我が国に対する各種情報収集を実行している可能性が高いことが判明。

○　サイバー攻撃集団「APT40」に関し、内閣サイバーセキュリティセンター（ＮＩＳＣ）と連携した事業者等に対する注意喚起等を実施。

○　東京オリンピック・パラリンピック競技大会について、官民が一体となったサイバー攻撃対策を実施。結果として、大会の運営に影響を及ぼすようなサイバー攻撃の発生はなかった。

別　添

令和３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

デジタル化の進展等に伴い、サイバー空間の公共空間化がさらに加速している。今やサイバー空間は社会経済活動の場として、例えば実空間における学校や公園や図書館といった広く国民に開かれ、利活用される公共施設に勝るとも劣らない機能と役割を担っている[*1]。

サイバー空間には、子供から高齢者まで幅広い世代が参画するようになっている一方で、新しいサービスや技術を悪用した犯罪が続々と発生し、その手口は悪質・巧妙化の一途をたどっている。国内では、キャッシュレス決済の普及等を背景として、令和３年中のサイバー犯罪の検挙件数が12,209件と過去最多を記録しているほか、ランサムウェアによる被害が拡大するとともに、不正アクセスによる情報流出や、国家を背景に持つサイバー攻撃集団によるサイバー攻撃が明らかになるなど、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。

令和３年中に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146件と、前年以降、右肩上がりで増加しており、その被害は、企業・団体等の規模やその業種等を問わず、広範に及んでいる。また、テレワーク等による外部から内部ネットワークへの接続が急増し、セキュリティ対策の一環としてＶＰＮ機器を導入する企業等が増加しているが、そのＶＰＮ機器のぜい弱性等から組織内部のネットワークに侵入し、ランサムウェアに感染させる手口が被害の多くを占めている。さらに、感染したシステム等の復旧までに２か月以上要した事例や、調査・復旧に5,000万円以上の費用を要した事例等の甚大な被害も確認されているほか、国内の医療機関において、電子カルテ等のシステムがランサムウェアに感染し、新規の診療受付や救急患者の受入れが一時停止する事態となるなど、重要インフラ事業者が標的となり、市民生活にまで重大な影響を及ぼす事案も確認されている。５月に発生した米国の石油パイプライン事業者を標的とした攻撃など、ランサムウェア攻撃は、世界各国において市民生活に重大な影響を及ぼしており、その対策には、緊密な国際連携が求められている。12月には、Ｇ７各国の法執行機関等が参加する「ランサムウェアに関するＧ７高級実務者会合」も開催されるなど、世界各国において、ランサムウェア被害の防止に向けた諸対策が喫緊の課題となっている。

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

---

*1　サイバーセキュリティ政策会議「実空間とサイバー空間とが融合したデジタル社会の安全・安心の確保」（令和３年12月）
（https://www.npa.go.jp/cybersecurity/CS.html）

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窃取された可能性のある事案が相次いで確認されたほか、サイバー攻撃事案の実態解明を推進する中で、国家レベルの関与が明らかとなった事例もあった。４月には、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。12月には、中国人民解放軍関係者と思われる人物からの指示を受け、日本製法人版ウイルス対策ソフトの年間使用権を不正に取得しようとした者を特定し、本件捜査により、中国人民解放軍が我が国に対する各種の情報収集を実行している可能性が高いことが判明した。このほか、７月には、英国・米国等がサイバー攻撃集団「APT40」について中国を非難する声明を発表し、我が国も、APT40は中国政府を背景に持つものである可能性が高いとの評価に基づく外務報道官談話を発表した。警察では、内閣サイバーセキュリティセンター（ＮＩＳＣ）と連携して、関係機関と連携した情報収集や対策等を進めていく旨を発表し、事業者等に対する注意喚起を実施するとともに、攻撃の対象となっていた企業に対して個別の情報提供を実施した。

さらに、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件数も増加の一途をたどっている。その内訳を分析したところ、アクセス件数の大半が海外からのものであることから、海外からのサイバー攻撃等に係る脅威が引き続き高まっていることが示唆されている。加えて、12月に公表された「Apache Log4j」のぜい弱性については、その公表直後から当該ぜい弱性を標的としたアクセスが急増した状況も確認されている。

このほか、７月から９月にかけて開催された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。）においては、官民が一体となった共同対処訓練や大会関係事業者等に対する注意喚起といったサイバー攻撃対策を実施するとともに、大会期間中の対応にも万全を期した。結果として、聖火リレーや開会式の動画配信を装った偽サイトとみられるウェブサイトの出現や、ＳＮＳ上における大会関係機関を標的としたサイバー攻撃の呼び掛け等が確認されたものの、大会の運営に影響を及ぼすようなサイバー攻撃の発生はなかった。

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は、その多くが、前年から継続している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。

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年の悪質なショッピングサイト等の通報件数は17,717件で、前年に比べて7,622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、インターネット利用が増えたほか、悪質なショッピングサイトの通報について、

関心が高まってきたことが要因と分析している[*2]。

また、令和３年に警察庁が実施した治安に関するアンケートにおいて、サイバー犯罪の被害に遭う危険性について「不安を感じる」又は「ある程度不安を感じる」との回答が79.4％に上るなど、国民が抱く不安感も高まっている。

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、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４月に警察庁にサイバー警察局、関東管区警察局にサイバー特別捜査隊を設置した。

警察では、引き続き警察庁と都道府県警察とが一体となった捜査・対策等に取り組むとともに、国際的な連携・共同捜査や官民連携をさらに推進し、サイバー空間に実空間と変わらぬ安全安心を確保すべく努めていく。

*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）」
(https://www.jc3.or.jp/threats/topics/article-431.html)

１　令和３年における脅威の動向

(1)　ランサムウェアの情勢と対策

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機器をはじめとする企業のネットワーク等のインフラのぜい弱性を狙って侵入するなど、特定の個人や企業・団体等を標的とした手口に変化している。

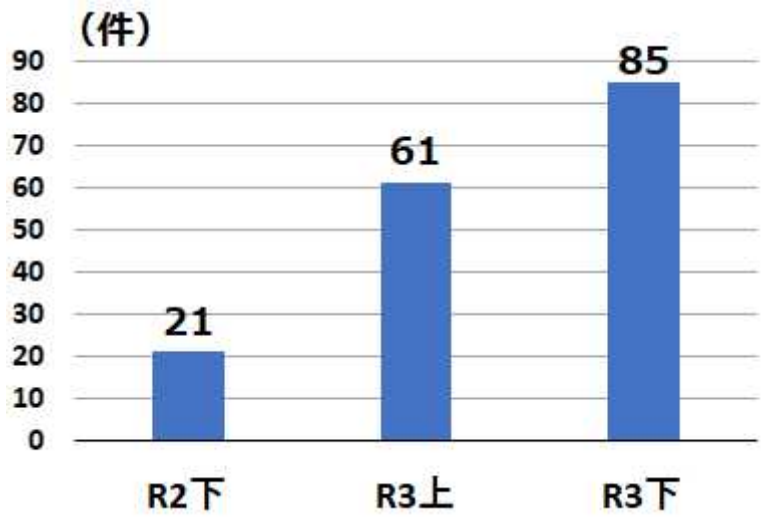
また、最近の事例では、データの暗号化のみならず、データを窃取した上、企業等に対し「対価を支払わなければ当該データを公開する」などと金銭を要求する二重恐喝（ダブルエクストーション）という手口が多くを占めている。

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年に都道府県警察から警察庁に報告のあった件数は146件（令和３年上半期61件、下半期85件）であり、前年下半期（21件）以降、右肩上がりで増加した。

【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

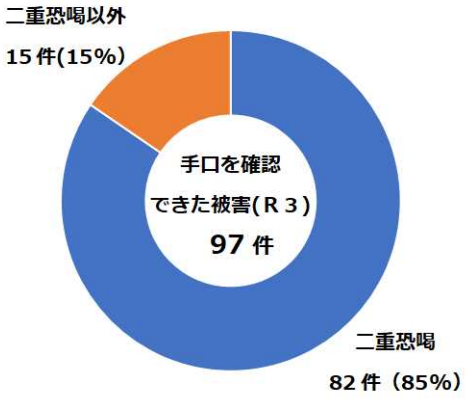
○　二重恐喝（ダブルエクストーション）による被害が多くを占める

被害件数（146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97件あり、このうち、二重恐喝の手口によるものは82件で85％を占めている。

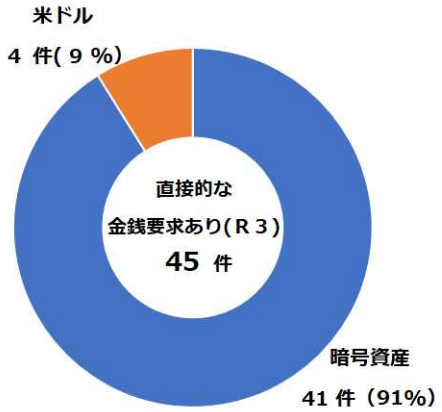
○　暗号資産による金銭の要求が多くを占める

被害件数（146件）のうち、直接的に金銭の要求があった被害は45件あり、このうち、暗号資産による支払いの要求は41件で91％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】



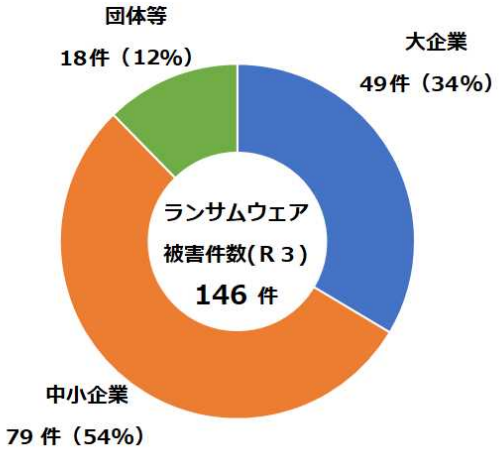
【図表３：要求された金銭支払い方法別報告件数】



○　企業・団体等の規模を問わず被害が発生

被害件数（146件）の内訳を被害企業・団体等の規模別[*3] にみると、大企業は49件、中小企業は79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】



*3　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

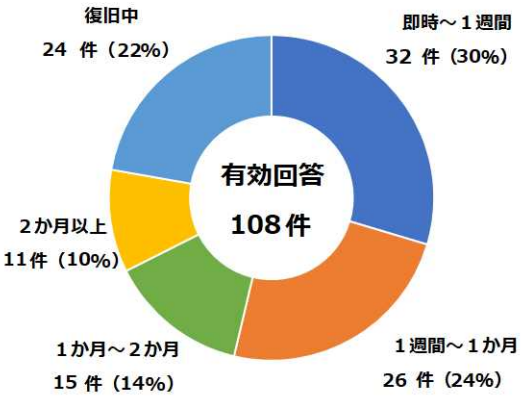
企業・団体等におけるランサムウェア被害の実態を把握するため、被害件数（146件）のランサムウェア被害に関し、被害企業・団体等にアンケート調査を実施したところ、集計期限までに123件の回答が得られたことから、その回答結果について分析を行った。

(ｱ)　復旧等に要した期間・費用

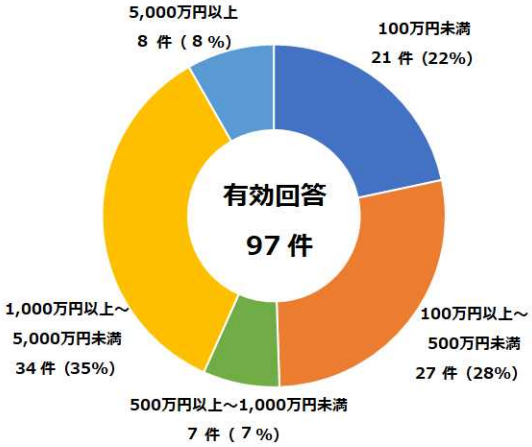
復旧に要した期間について質問したところ、108件の有効な回答があり、このうち、１週間以内に復旧したものが32件と最も多かったが、復旧に２か月以上要したものもあった。

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、97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42件で43％を占めている。

【図表５：復旧に要した期間】



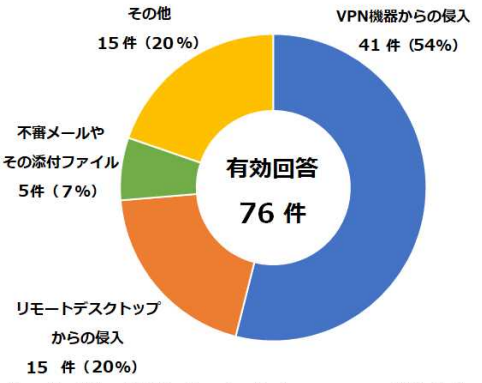
【図表６：調査・復旧費用の総額】



(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、76件の有効な回答があり、このうち、ＶＰＮ機器からの侵入が41件で54％、リモートデスクトップからの侵入が15件で20％を占めており、テレワークにも利用される機器等のぜい弱性や強度の弱い認証情報等を利用して侵入したと考えられるものが大半を占めている。

【図表７：感染経路】

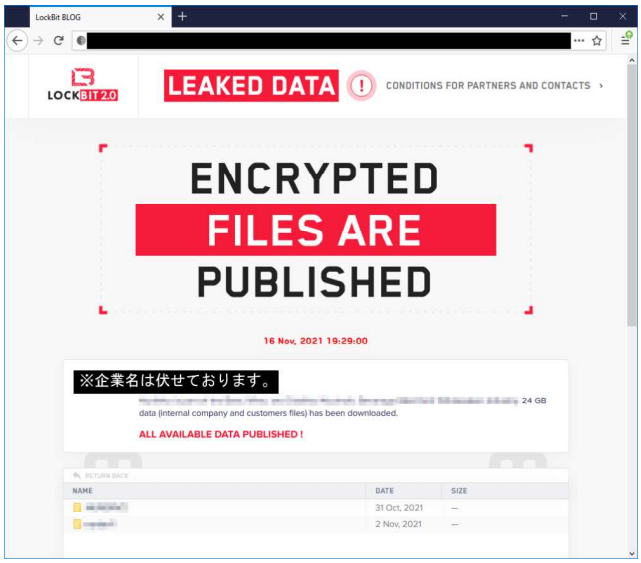


注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100にならない。

エ　ランサムウェアと関連するリークサイトの状況

警察では、ダークウェブ上のサイトを観測しており、令和３年において、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】



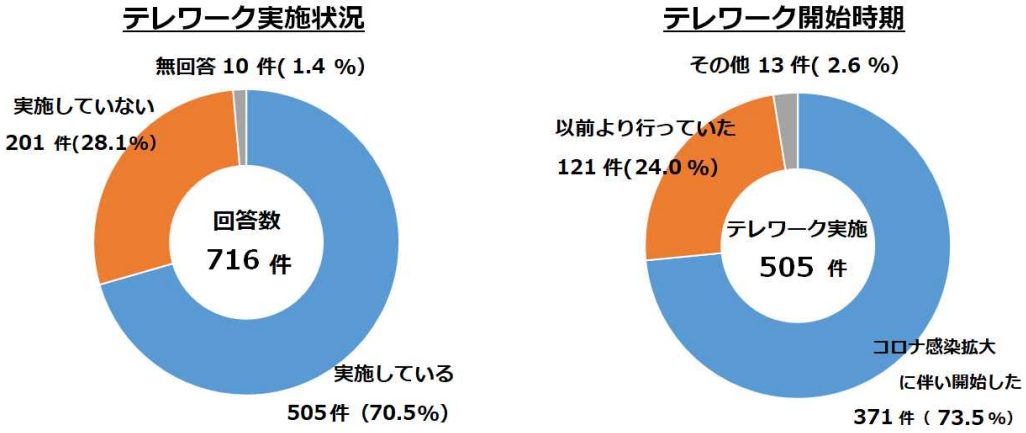
オ　サイバー犯罪被害に係る企業・団体等を対象としたアンケート調査[*4]

警察では、不正アクセス行為による被害防止のための広報啓発に資することを目的として、民間企業や行政機関等に対する「不正アクセス行為対策等の実態調査」を例年行っており、令和３年の調査では企業・団体等2,950件を無作為に抽出し、アンケート調査を実施したところ、716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)　テレワーク実施状況等

テレワークを実施していると回答した企業・団体等は全体（716件）の70.5％を占め、このうち、新型コロナウイルス感染症の拡大により、新たにテレワークを開始したと回答した企業・団体等が７割以上を占めている。

【図表９：テレワーク実施状況等】



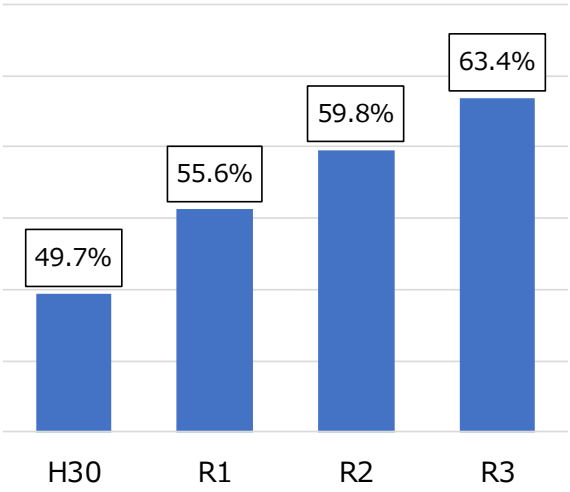
注　図中の割合は小数点第２位以下を四捨五入しているため、総計が必ずしも100にならない。

(ｲ)　外部から社内ネットワークへの接続率

テレワークの実施等により、業務上、外部から社内ネットワークへの接続を許可している企業・団体の割合は全体（716件）の63.4％を占めており、年々増加している。

*4　警察庁ウェブサイト「サイバー犯罪対策プロジェクト」
(https://www.npa.go.jp/cyber/research/index.html)

【図表10：外部から社内ネットワークへの接続率】



カ　ランサムウェアへの対策

(ｱ)　警察庁ウェブサイトにおける注意喚起

警察庁では、令和３年上半期に実施した国内のランサムウェア被害を受けた企業・団体等に対するアンケート調査の結果等を踏まえ、被害の未然防止対策等について、９月に警察庁ウェブサイトにおいて注意喚起を行った。

(ｲ)　損害保険会社と連携した対策の推進

警察では、被害の潜在化その他のランサムウェアを始めとするサイバー犯罪の温床となっている要素・環境の改善を図る観点から、一般社団法人日本損害保険協会等と連携して、サイバー犯罪に係る防犯対策に関する広報啓発活動を推進するとともに、警察への通報の促進に取り組んでいる。

(ｳ)　流出したＶＰＮ製品の認証情報に係る注意喚起

９月、テレワークの実施等の際に用いるＶＰＮ製品の認証に必要な情報がダークウェブ上のサイトに掲出されており、流出していることが確認された。警察庁では、ランサムウェア攻撃等への悪用を防止するため、流出した情報を分析し、当該情報の関係企業等に対し、都道府県警察を通じて注意喚起を行った。

(ｴ)　医療機関を標的としたランサムウェアへの対策

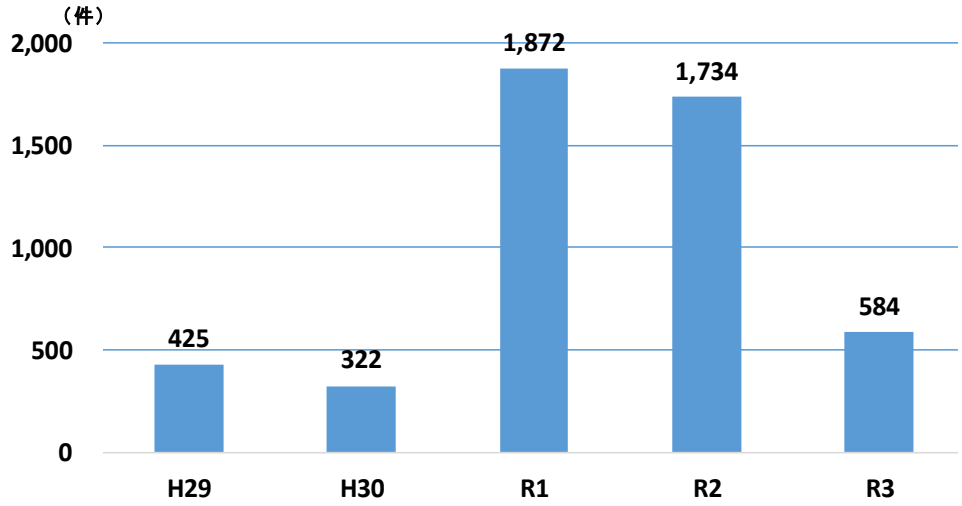
国内の医療機関において、電子カルテ等のシステムがランサムウェアに感染し、新規の診療受付や救急患者の受入れが一時停止する事態となるなど、医療機関を標的とするランサムウェア被害が発生している状況を受け、警察庁では、厚生労働省に情報提供を行うなど、関係機関と連携した被害防止対策に取り組んでいる。

(2)　フィッシング等に伴う不正送金・不正利用の情勢と対策

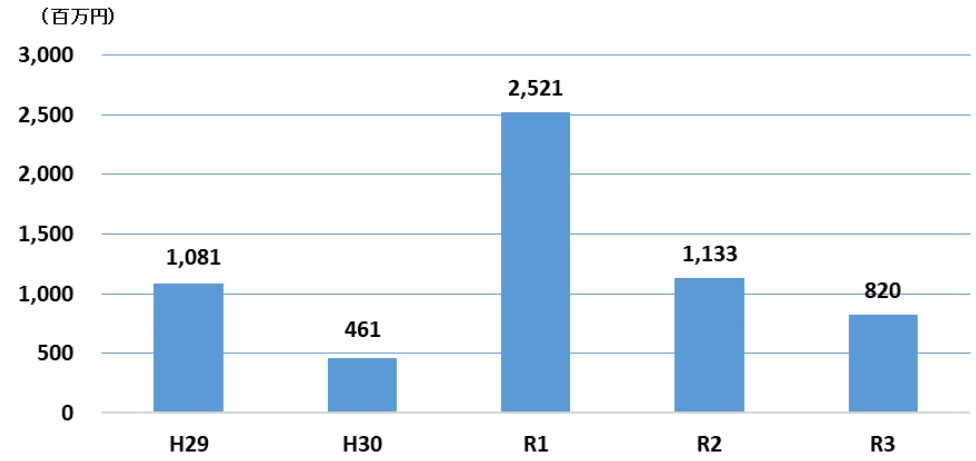
ア　インターネットバンキングに係る不正送金事犯の発生状況

令和３年中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、犯行手口等の関係機関との迅速な情報共有等の取組を進めたところ、発生件数584件、被害総額約８億2,000万円と、前年と比べて発生件数、被害額ともに減少した。

【図表11：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12：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】



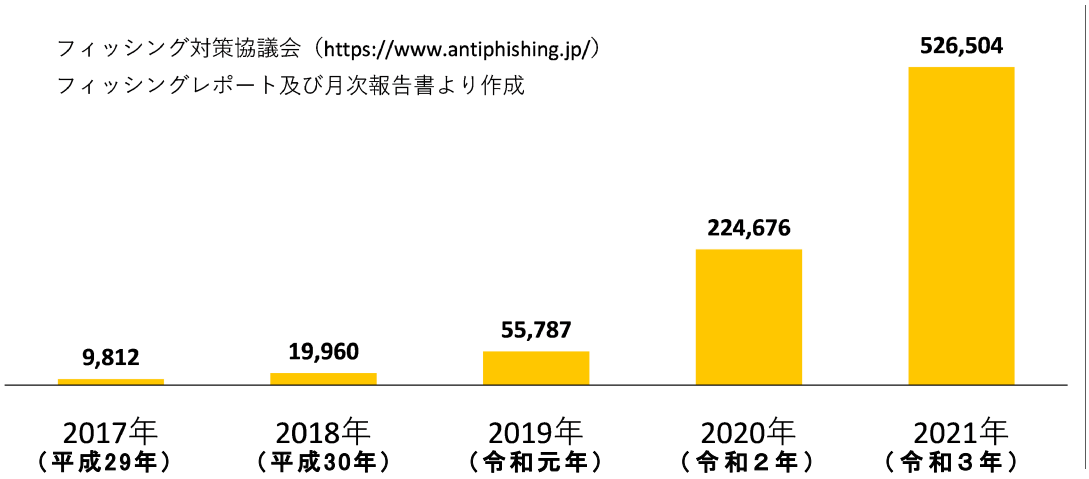
イ　フィッシング等に伴う被害の実態

インターネットバンキングに係る不正送金事犯は、令和元年に、ＳＭＳ等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が急増し、ＩＤ・パスワード、ワンタイムパスワード等が窃取され、金融機関のインターネットバンキングから不正送金される被害等が多発し、同年には、発生件数1,872件、被害額約25億2,100万円に達した。

こうした情勢を踏まえ、金融機関では、警察、ＪＣ３等と緊密に連携し、モニタリングの強化、利用者への注意喚起などといった諸対策を推進した結果、フィッシングを主な手口とするインターネットバンキングに係る不正送金事犯は、令和３年まで発生件数、被害額ともに減少した。

他方、フィッシング対策協議会によれば、令和３年のフィッシング報告件数は52万6,504件と、一貫して増加傾向にある[*5]ほか、ＪＣ３の分析結果[*6]によれば、令和３年に観測したフィッシングサイトは、銀行を装ったものの割合は少なく、インターネット通信販売サイト等のｅコマースや、通信事業者、クレジットカード事業者を装ったものが多くを占めている。

【図表13:フィッシング報告件数（ＪＣ３ウェブサイトより引用)】

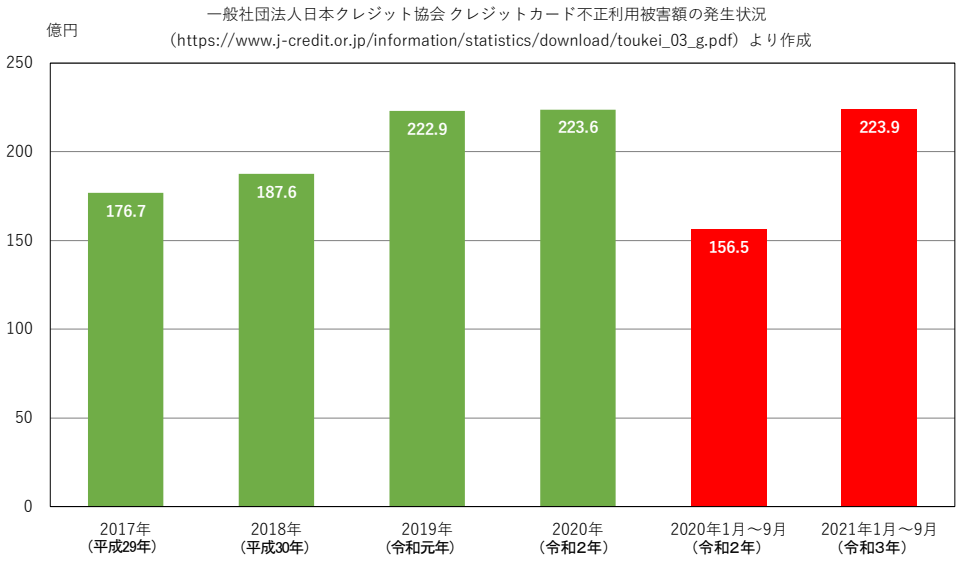


*5　フィッシング対策協議会ウェブサイト「2021/12 フィッシング報告状況」他
(https://www.antiphishing.jp/report/monthly/202112.html)

*6　ＪＣ３ウェブサイト「フィッシングターゲットの変遷」
(https://www.jc3.or.jp/threats/topics/article-430.html)

さらに、一般社団法人日本クレジット協会によれば、令和３年１月から９月までの間における番号盗用型のクレジットカード不正利用被害額は約223億9,000万円と、既に令和２年中の不正利用被害額を超えている[*7]。

【図表14:クレジットカード不正利用（番号盗用）被害額】



ＪＣ３では、クレジットカード不正利用が増加した要因の一つとして、クレジットカード情報を窃取するフィッシングサイトの存在を指摘しており、犯罪者らが、官民連携により対策が強化された金融機関から、ｅコマースやクレジットカード事業者にフィッシングの標的を移していることがうかがわれる。

ウ　警察の取組

○　不正送金組織の検挙等

・　不正送金組織の検挙

令和元年９月から令和２年２月にかけて連続発生した大手金融機関を対象とした不正送金事犯で、令和３年中に犯行指示役、送金先口座名義人、送金先口座からの現金引き出し役など、指定暴力団構成員等を含む男女29名を検挙した。

・　金融機関との連携強化

被害の未然防止に向けて、金融機関とサイバー犯罪防犯情報連絡会議を開催し、犯行手口を踏まえた情報共有を実施するなど連携強化を図った。

---

*7　一般社団法人日本クレジット協会ウェブサイト「2021年12月　クレジットカード不正利用被害の発生状況」
（https://www.j-credit.or.jp/information/statistics/download/toukei_03_g.pdf）

○　口座売買組織の検挙等

・　口座売買組織の検挙

令和元年12月に発生した不正送金事犯を端緒として、令和２年６月から令和３年10月までに、口座売買組織の犯行指示役、口座譲渡者等７名を検挙した。

・　犯行ツール対策

被害金融機関に対し、口座開設時の開設目的の確認や犯罪に利用された口座の凍結を依頼するなどの犯行ツール対策を行った。

○　メモアプリ提供事業者に対する対策強化の働きかけ及びメモアプリ利用に係る注意喚起

インターネットバンキングのＩＤやパスワード等を保存していたメモアプリが不正アクセスされて、インターネットバンキングに係る不正送金被害に遭うケースを確認したことから、同メモアプリ提供事業者に対し、被害防止対策を要請した結果、同事業者のウェブサイト等において注意喚起がなされた。

また、ＪＣ３と連携し、ＪＣ３のウェブサイト等においてメモアプリ利用に係る注意喚起を実施した。

○　関係団体と連携した金融機関に対する対策の要請

金融犯罪への対応を行う関係団体に対し、犯行手口や被害状況等に係る迅速な情報共有を行ったところ、関係団体から金融機関に対して、本人確認書類等の確認態勢の強化や顧客への注意喚起等の対策が要請された。

○　通信事業者を装ったフィッシングに関する注意喚起

通信事業者を装ったフィッシングＳＭＳにより、不正アプリをインストールさせ、ネットワーク暗証番号等を入力させる手口について、従来のＡｎｄｒｏｉｄ端末を対象としたものだけでなく、ｉＰｈｏｎｅを対象としたものも確認したとのＪＣ３からの情報提供を受け、ＪＣ３と連携し、ＳＮＳ等を活用して注意喚起を実施した。

(3) 東京大会のサイバー関連対策

サイバー攻撃が世界的規模で発生する中、平成30年（2018年）に開催された平昌（ピョンチャン）冬季オリンピック競技大会においては、大会の運営に直接的な影響はなかったものの、大会運営に用いられたシステムに対するサイバー攻撃が発生した。近年、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おり、東京大会においても、その妨害や情報窃取等を目的として、競技会場をはじめとする関係施設の管理者や重要インフラ事業者等を標的としたサイバー攻撃の発生が懸念されたことから、特段の注意を払う必要があった。実際に、聖火リレーや開会式の動画配信を装った偽サイトとみられるウェブサイトの出現、東京大会の名称を使用したマルウェアの作成、大会組織委員会のシステムからの流出ではないとみられるボランティア及びチケット購入者のＩＤ・パスワードの流出、ＳＮＳ上における大会関係機関を標的としたサイバー攻撃の呼び掛け等が確認されるなど、何らかの被害が発生する可能性が否定できない状況であった。

こうした情勢を踏まえ、警察では、大会組織委員会、競技会場を管理する事業者、重要サービス事業者等と連携して、サイバー攻撃による被害の未然防止に努めた。

事前対策として、東京大会の開催決定の直後から、競技会場を管理する事業者、重要サービス事業者等に対して、システムのセキュリティ対策状況の確認及び助言を実施したほか、競技会場を管理する事業者等と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実施するなどの官民が連携したサイバー攻撃対策を行った。また、重要サービス事業者、大会関連事業者等に対して、ＩＴ監視システムやサーバソフトウェアのぜい弱性を狙ったサイバー攻撃等に関する注意喚起等を実施した。

大会期間中には、大会関係機関等との緊密な連携の下、24時間体制での即応体制を整え、サイバー攻撃発生時の対応に万全を期した。

関係都道府県警察では、ＪＣ３からの偽ライブ配信サイトに誘導する国内の改ざんサイトを発見したとの情報提供に基づき、サイト管理者等に対して改善を要請するなどの対策を実施したほか、委嘱しているサイバー犯罪対策テクニカルアドバイザーの協力を得て、海外の政府機関のＷｅｂサイトにも改ざんページが蔵置されているのを発見し、警察庁を通じて海外の捜査機関へ情報提供した。

結果として、大会の運営に影響を及ぼすようなサイバー攻撃の発生はなかった。

(4) 主なサイバー攻撃事例と警察における取組

ア　サイバー攻撃事例

○　出入国在留管理庁が運用するシステムにおける不正プログラム検知

７月、出入国在留管理庁は、空港に設置された自動化ゲートの利用者

登録等を行うシステム（ＴＴＰシステム）において、５月に不正プログラムが検知されたと発表した。調査の結果、同システムの構成機器に関する情報が流出した可能性があるとしている。

○　サイバー攻撃集団「APT40」に関するパブリック・アトリビューション

７月、米国司法省は、航空、防衛、バイオ医薬品分野等に関する情報を標的として、米国、英国、ドイツを始めとした複数の国々にサイバー攻撃を行っていたとして、APT40の構成員である中国人４人を起訴したと発表した。標的とされた情報には、潜水艦及び自動運転車に関する機微な技術情報、感染症に関する研究情報等が含まれていたとしている。

また、英国、米国等は、APT40の背景に中国政府があると指摘し、中国を非難する声明を発表した。我が国も、APT40は中国政府を背景に持つものである可能性が高いと評価した上、悪意あるサイバー活動を断固非難するとともに、厳しく取り組んでいく旨の外務報道官談話を、英国、米国等と足並みをそろえて発表した。

○　大手電気機器メーカーに対する不正アクセス

11月、我が国の大手電気機器メーカーは同月に同社のネットワークに対する不正アクセスが発生し、ファイルサーバのデータの一部が不正に読み出されたことが判明したと発表した。調査の結果、当該不正アクセスは、同社の海外子会社のサーバを経由して実行され、対象のファイルサーバには、同社の社内情報、取引先の業務関連情報のほか、採用応募者の個人情報等の情報が含まれていたとしている。

イ　警察における取組

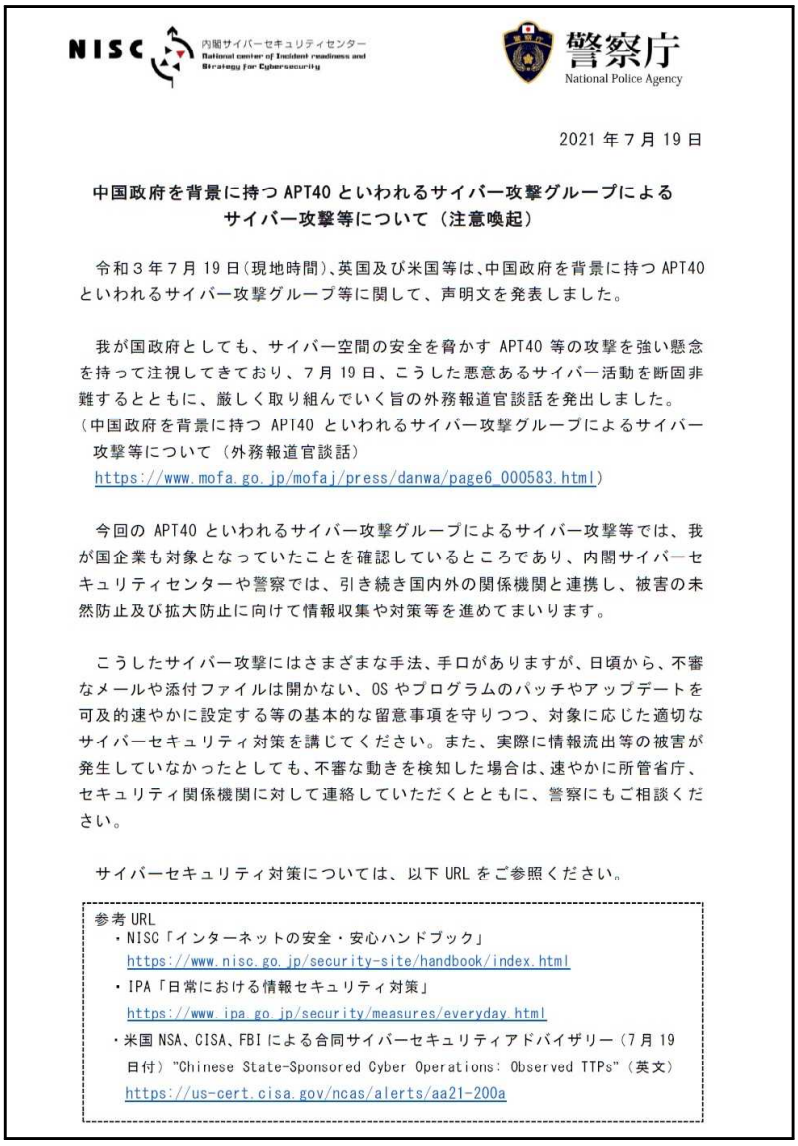
○　被害企業等に対する注意喚起

７月、警察庁及び内閣サイバーセキュリティセンター（ＮＩＳＣ）は、サイバー攻撃集団APT40によるサイバー攻撃に関して、引き続き国内外の関係機関と連携し、被害の未然防止及び拡大防止に向けて情報収集や対策等を進めていく旨を発表した。事業者等に対しては、適切なサイバーセキュリティ対策を講じることに加え、実際に情報流出等の被害が発生していなかったとしても、不審な動きを検知した場合は、速やかに所管省庁及びセキュリティ関係機関に連絡するとともに、警察にも相談するよう注意喚起した。

加えて、警察では、攻撃を認知後、速やかに攻撃の対象となっていた企業に対して、マルウェア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、被害拡大防止の措置を講じた[*8]。

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

【図表15:ＮＩＳＣとの連名による注意喚起文書】



NISC 内閣サイバーセキュリティセンター National center of Incident readiness and Strategy for Cybersecurity

警察庁 National Police Agency

2021 年７月 19 日

中国政府を背景に持つ APT40 といわれるサイバー攻撃グループによる サイバー攻撃等について（注意喚起）

令和３年７月 19 日（現地時間）、英国及び米国等は、中国政府を背景に持つ APT40 といわれるサイバー攻撃グループ等に関して、声明文を発表しました。

我が国政府としても、サイバー空間の安全を脅かす APT40 等の攻撃を強い懸念を持って注視してきており、７月 19 日、こうした悪意あるサイバー活動を断固非難するとともに、厳しく取り組んでいく旨の外務報道官談話を発出しました。
（中国政府を背景に持つ APT40 といわれるサイバー攻撃グループによるサイバー攻撃等について（外務報道官談話）
https://www.mofa.go.jp/mofaj/press/danwa/page6_000583.html）

今回の APT40 といわれるサイバー攻撃グループによるサイバー攻撃等では、我が国企業も対象となっていたことを確認しているところであり、内閣サイバーセキュリティセンターや警察では、引き続き国内外の関係機関と連携し、被害の未然防止及び拡大防止に向けて情報収集や対策等を進めてまいります。

こうしたサイバー攻撃にはさまざまな手法、手口がありますが、日頃から、不審なメールや添付ファイルは開かない、OS やプログラムのパッチやアップデートを可及的速やかに設定する等の基本的な留意事項を守りつつ、対象に応じた適切なサイバーセキュリティ対策を講じてください。また、実際に情報流出等の被害が発生していなかったとしても、不審な動きを検知した場合は、速やかに所管省庁、セキュリティ関係機関に対して連絡していただくとともに、警察にもご相談ください。

サイバーセキュリティ対策については、以下 URL をご参照ください。

参考 URL
・NISC「インターネットの安全・安心ハンドブック」
https://www.nisc.go.jp/security-site/handbook/index.html
・IPA「日常における情報セキュリティ対策」
https://www.ipa.go.jp/security/measures/everyday.html
・米国 NSA、CISA、FBI による合同サイバーセキュリティアドバイザリー（7 月 19 日付）"Chinese State-Sponsored Cyber Operations: Observed TTPs"（英文）
https://us-cert.cisa.gov/ncas/alerts/aa21-200a

○　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いる。令和３年にはマルウェアの感染拡大のためのインフラとして悪用されていた疑いのあるＩＰアドレスに関する注意喚起のほか、コンテンツ管理システムの一種であるMovable Type、ログの管理等で使用されるApache Log4j[*9] 等のぜい弱性に関する注意喚起等を実施し、重要インフラ事業者等のサイバー攻撃による被害の未然防止・拡大防止を図った。

○　詐欺未遂被疑者の逮捕状取得・指名手配

12月、警視庁公安部は、中国人民解放軍関係者と思われる人物から指示を受け、日本製の法人版ウイルス対策ソフトの年間使用権を不正に取得し

*9　Apache Log4jのぜい弱性を標的としたアクセスについては20頁、21頁参照。

ようと企て、平成28年11月、都内に所在するソフトウェア販売代理店に対して、架空の法人情報や実在しない担当者名等の虚偽の情報でライセンス契約を申し込んだとして、詐欺未遂容疑で中国籍の元留学生の男の逮捕状を取得し、指名手配した。

中国人民解放軍が関与している可能性の高いサイバー攻撃集団が、平成28年６月から12月にかけて行った、ＪＡＸＡ等に対するサイバー攻撃事件[*10]を捜査する過程で、本件犯行が浮上したものであり、本件捜査により、中国人民解放軍が、我が国に対する各種の情報収集を実行している可能性が高いことが判明した。

○　Ｃ２サーバ[*11] 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、不正に蔵置されたファイルにより動作している不正な機能を停止（テイクダウン）するようサーバを管理する事業者等に依頼するなどして、Ｃ２サーバの対策を継続的に実施している。この結果、令和３年には27件のＣ２サーバのテイクダウンを行った。

○　共同対処訓練の実施

重要インフラ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継続的に実施している。令和３年においても、電力事業者、自治体、金融機関等、幅広い分野の事業者等を対象として、模擬の標的型メールを使用した訓練、警察との連携を確認するための現場臨場訓練等を実施し、各事業者等のサイバー攻撃に対する対処能力の向上を図った。

---

*10　「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」９頁、10頁参照。

*11　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。

２　サイバー空間の脅威情勢

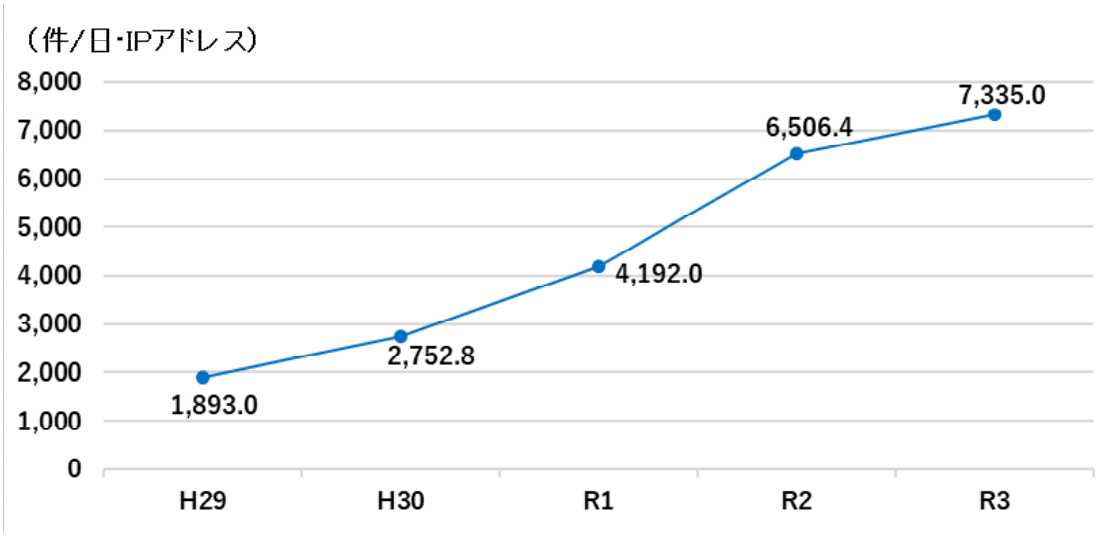
(1)　サイバー空間におけるぜい弱性探索行為等の観測状況

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[*12] 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7,335.0件と増加傾向にある。アクセス件数が増加傾向にあるのは、ＩｏＴ機器の普及により攻撃対象が増加していること、技術の進歩により攻撃手法が高度化していることなどが背景にあるものとみられる。

【図表16：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

○　海外を送信元とするアクセスの増加

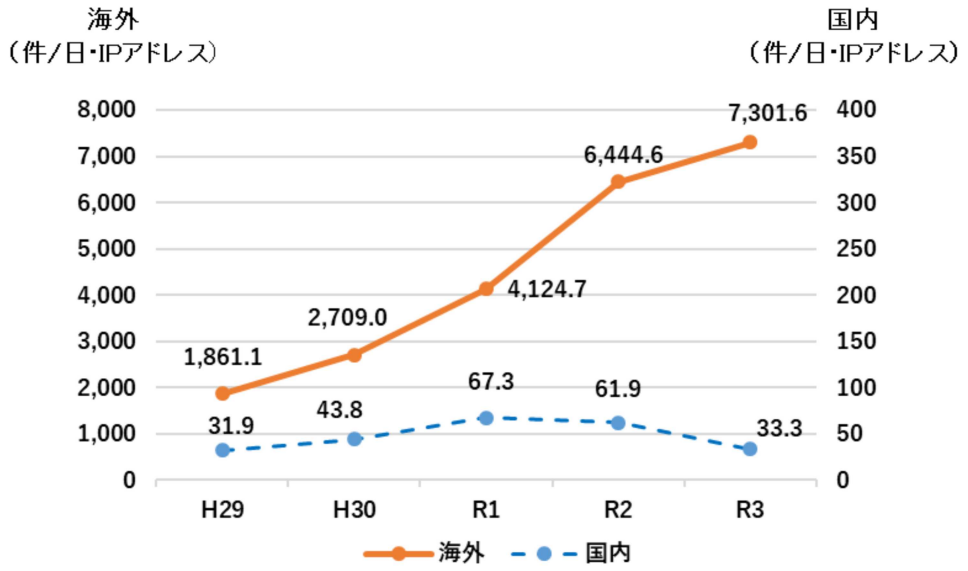
検知したアクセスの送信元の国・地域に着目すると、過去５年において、海外を送信元とするアクセス件数が全アクセス件数に対して、高い割合を占めている。

---

*12　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。

令和３年においては、国内を送信元とするアクセス件数は１日当たり33.3件で、前年の61.9件から減少する中、海外を送信元とするアクセス件数は7,301.6件で、前年の6,444.6件から大きく増加しており、海外からの脅威への対処がこれまでに引き続き重要となっている。

【図表17：検知したアクセスの送信元で比較した１日・１ＩＰアドレス当たり件数の推移】



○　国内を送信元とするＩｏＴ機器等のぜい弱性を狙ったアクセスの増加

令和３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257.3件で、前年（461.7件）よりも減少していることが確認されている。一方で、国内を送信元とするMiraiボットの特徴を有するアクセスに注目すると、令和２年には１日・１ＩＰアドレス当たり2.8件だったアクセス件数が令和３年には3.6件に増加している。国内を送信元とするアクセス件数の総数が前年と比較して減少している中、Miraiボットの特徴を有するアクセスはむしろ増加していることから、ぜい弱性を持つＩｏＴ機器等が国内に一定数存在し、Miraiボットに感染した後に他のＩｏＴ機器等に二次感染活動を行っている状況が継続していることがうかがえる。

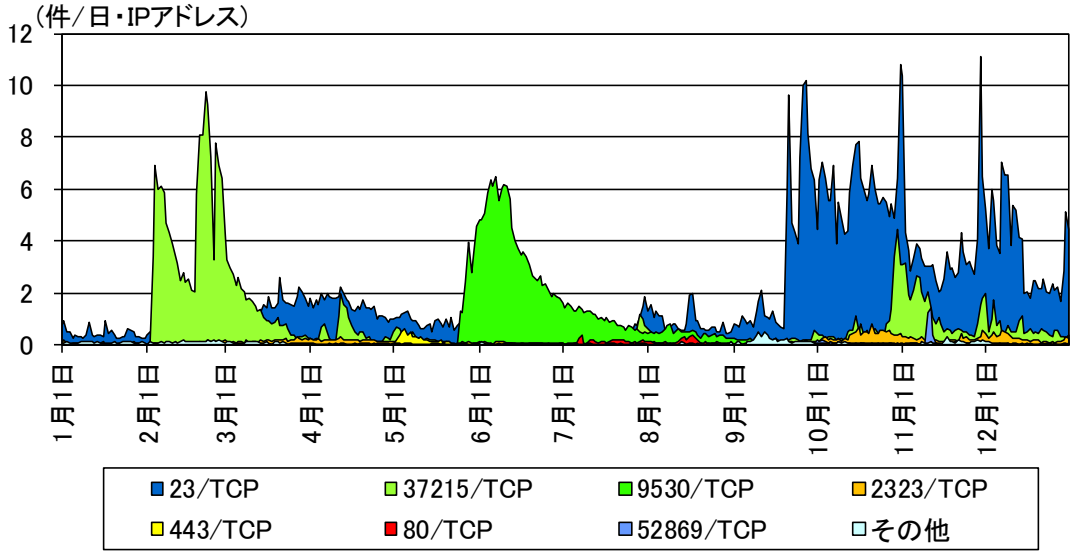
また、令和３年中の国内を送信元とするMiraiボットの特徴を有するアクセスの宛先ポート[*13]別の特徴は以下のとおりである。既知のぜい弱性を狙った探索行為が急増することがあり、国内のＩｏＴ機器等に対する脅威は依然として継続している。

---

*13　ＴＣＰ/ＩＰ通信（インターネット等で用いられているネットワーク上でデータを交換する際の取り決め）において、利用するサービスを識別するための番号であり、０から65535までが割り当てられている。

・　２月上旬から、海外製ルータ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とみられる宛先ポート37215/ＴＣＰに対するアクセスの増加を観測。
・　５月下旬から、海外製ビデオレコーダ等において遠隔から任意の操作が可能となるぜい弱性を探索したものとみられる宛先ポート9530/ＴＣＰに対するアクセスの増加を観測。
・　９月下旬から、ネットワーク機器等のぜい弱性を標的としたとみられる宛先ポート23/ＴＣＰに対するアクセスの増加を観測。

【図表18：Miraiボットの特徴を有する国内を送信元とするアクセス件数の推移（宛先ポート別）】

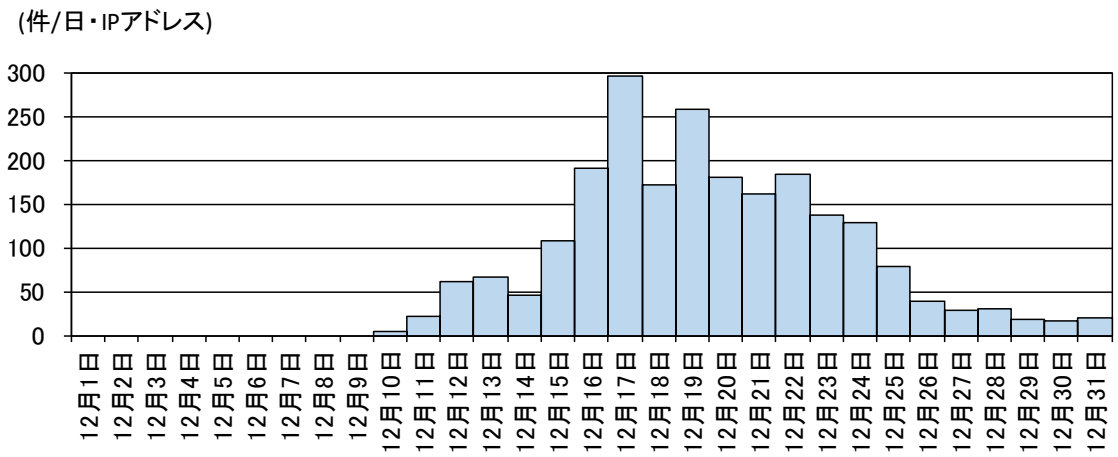


○　Javaライブラリ「Apache Log4j」のぜい弱性を標的としたアクセスの観測

Javaライブラリ「Apache Log4j」はApache Software Foundationがオープンソースで開発しているJava言語用のログ出力ライブラリであり、Java言語で開発された多数のソフトウェアにおいて、サーバのログの記録や管理に使用されている。12月10日に「Apache Log4j」のぜい弱性が公表されたことを契機とし、同ぜい弱性を標的としたアクセスの急増を観測した。

これは、「Apache Log4j」を使用してログの記録を行うソフトウェアに対して、遠隔の第三者が細工した文字列を送信し、その文字列がログに記録されることで、外部から第三者による任意の操作が可能となるぜい弱性を標的とした攻撃が行われたとみられる。

【図表19：Javaライブラリ「Apache Log4j」のぜい弱性を標的としたアクセス件数の推移（宛先ポート別）】

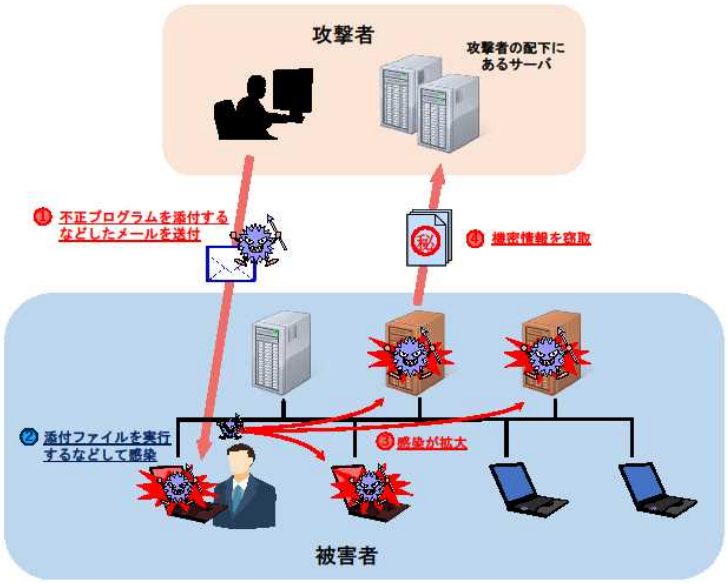


(2)　標的型メール攻撃

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４年１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）から提供を受けた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、これらの事業者等に対して情報共有を行っている。

【図表20：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には以下のようなものがあった。令和３年においても、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が送信されたほか、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始めとする不審なメールも送信されていることが確認されている。

①　機械部品関連の製造業者に対する標的型メール攻撃

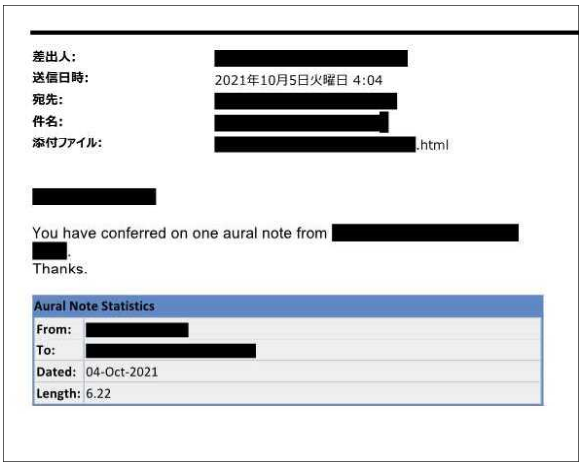
新ＩＤのお知らせと称して、不正プログラムが仕掛けられたファイルをダウンロードするよう誘導する標的型メールが機械部品関連の製造業者に送信された。

【図表21：メール文面】

② 半導体の製造業者に対する標的型メール攻撃

添付ファイルから偽のパスワード入力画面に遷移させ、業務で使用するアカウントのパスワードを入力するよう誘導する標的型メールが半導体の製造業者に送信された。

【図表22：メール文面】



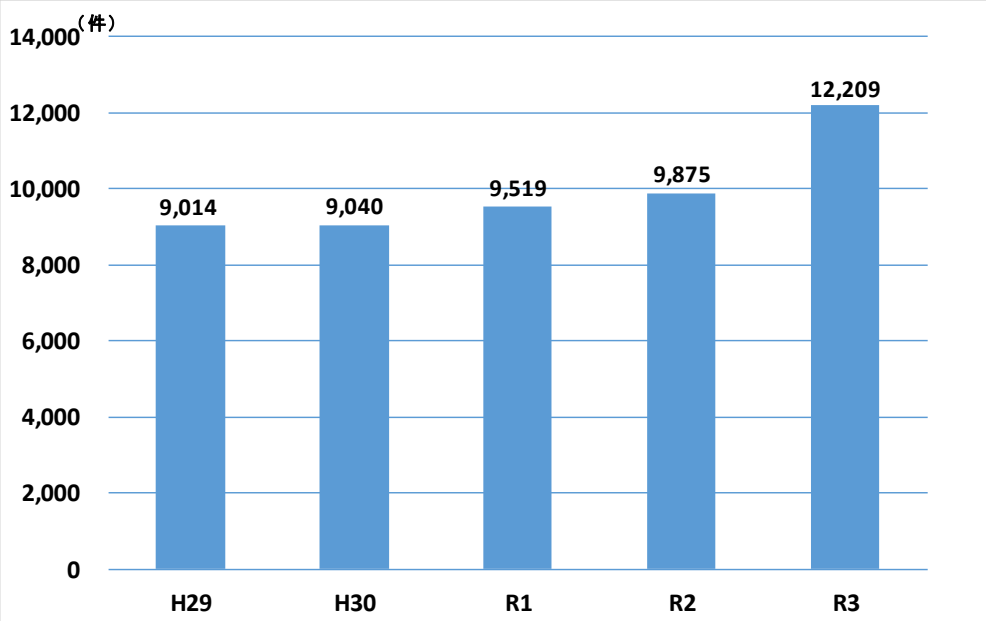
【図表23：遷移後の画面】

(3)　サイバー犯罪の現況

ア　サイバー犯罪の検挙件数

令和３年中における検挙件数は12,209件と、前年と比べて増加した。

【図表24：サイバー犯罪の検挙件数の推移】



イ　不正アクセス禁止法[*14] 違反

(ｱ)　検挙件数

令和３年中における不正アクセス禁止法違反の検挙件数は429件と、前年と比べて減少した。

(ｲ)　特徴

検挙件数のうち、398件が識別符号窃用型[*15] で全体の92.8％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、「利用権者のパスワードの設定・管理の甘さにつけ込んで入手」が153件と最も多く、全体の38.4％を占めており、次いで「フィッシングサイトにより入手」が70件で全体の17.6％を占めている。

---

*14　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。）

*15　不正アクセス行為は、他人の識別符号を無断で入力する「識別符号窃用型」と、アクセス制御機能による特定利用の制限を免れる情報（識別符号を除く）又は指令を入力する「セキュリティ・ホール攻撃型」に分類することができる。

○　被疑者が不正に利用したサービスは「オンラインゲーム・コミュニティサイト」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、「オンラインゲーム・コミュニティサイト」が144件と最も多く、全体の36.2％を占めており、次いで「インターネットバンキング」が96件で全体の24.1％を占めている。

ウ　コンピュータ・電磁的記録対象犯罪[*16]

(ｱ)　検挙件数

令和３年中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729件で、前年と比べて増加した。

(ｲ)　特徴

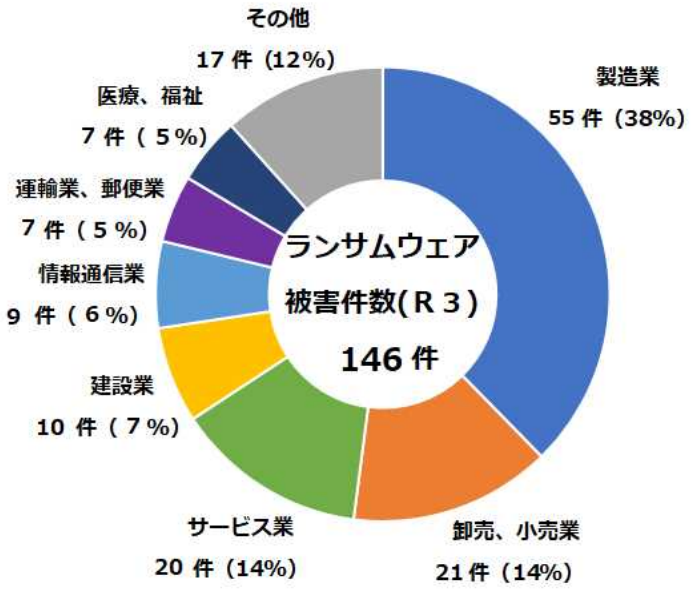
検挙件数のうち、電子計算機使用詐欺が692件と最も多く、全体の94.9％を占めている。

*16　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】

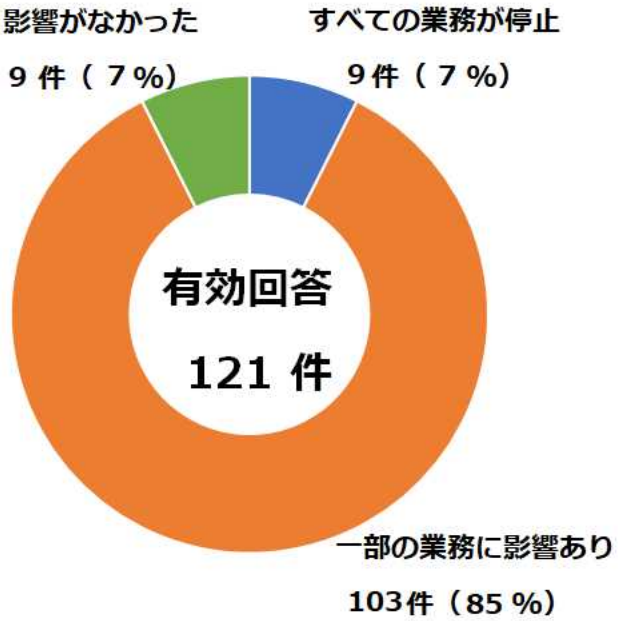
1　企業・団体等におけるランサムウェア被害及びその実態

(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



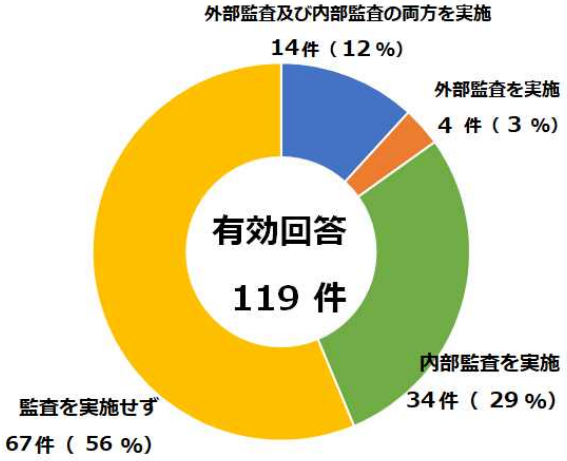
注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100%にならない。

(2)　ランサムウェア被害が業務に与えた影響



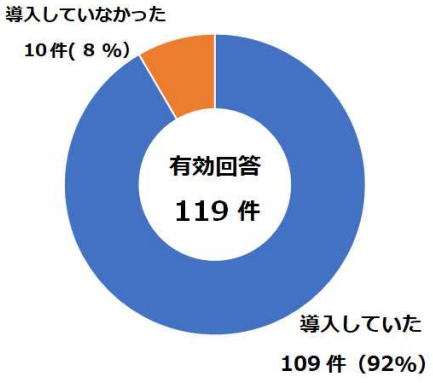
注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100%にならない。

(3)　被害企業・団体等の情報セキュリティ監査の実施状況

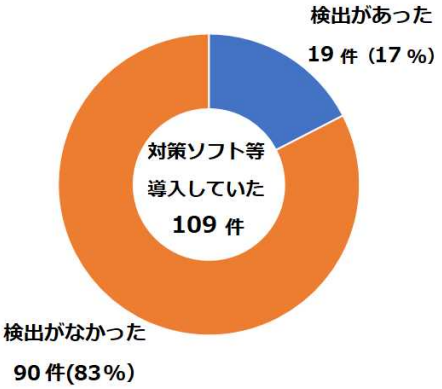


(4)　被害企業・団体等のウイルス対策ソフト等の導入・活用状況

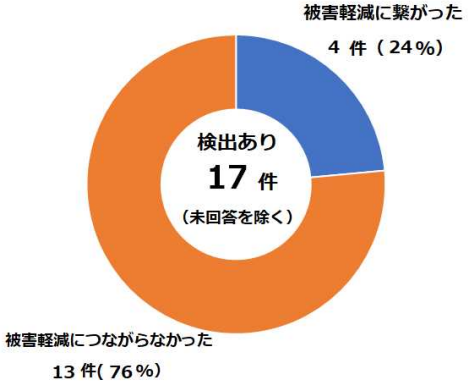
導入状況



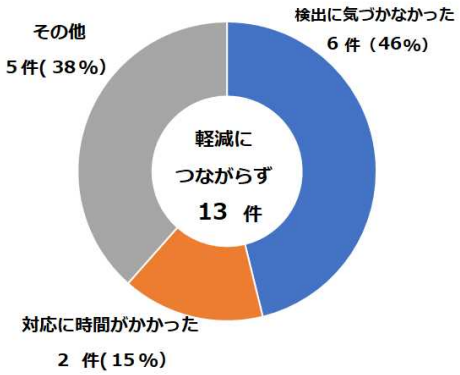
検出の有無



被害軽減効果

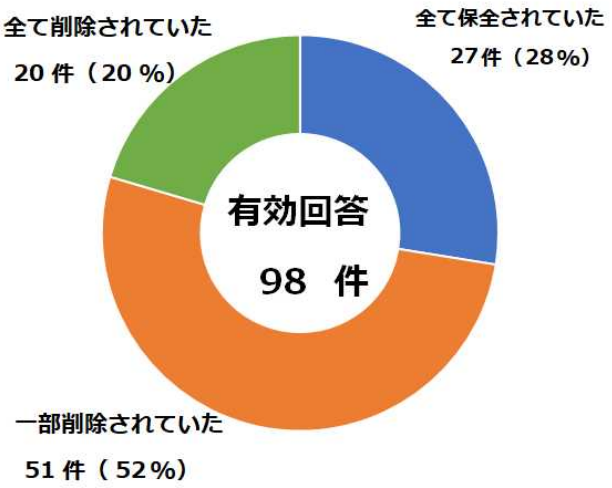


被害軽減に繋がらなかった理由



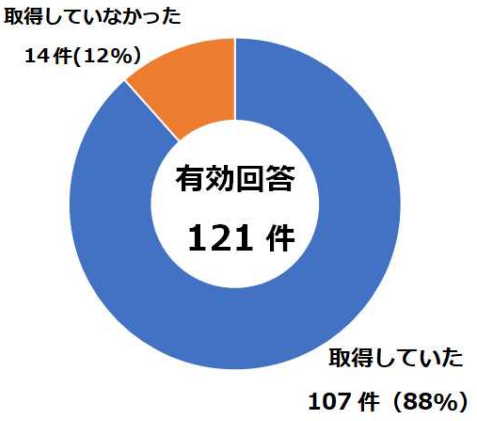
注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100にならない。

(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

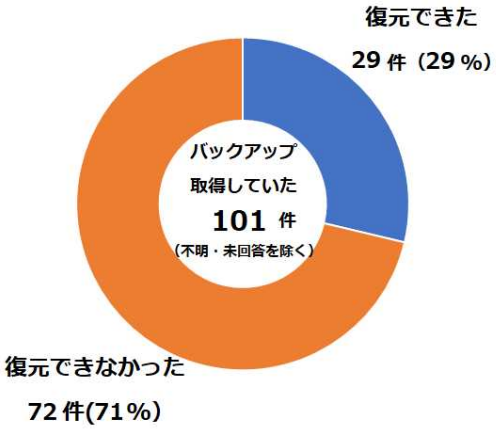


(6)　被害企業・団体等のバックアップの取得・活用状況

バックアップ取得の有無

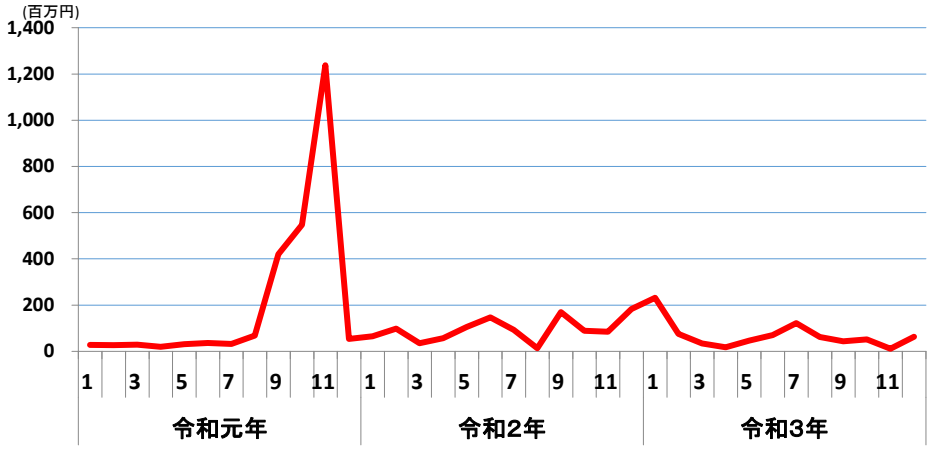


復元結果

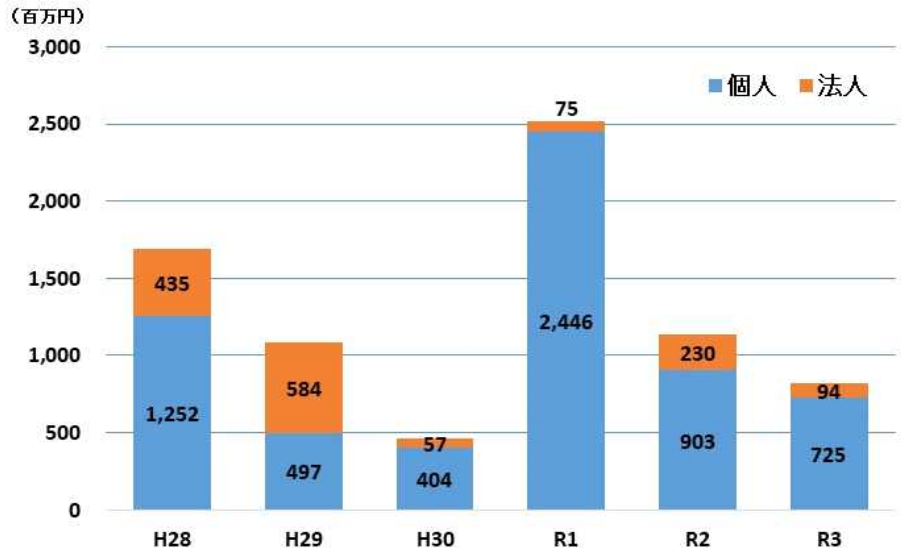


2　インターネットバンキングに係る不正送金事犯の発生状況等

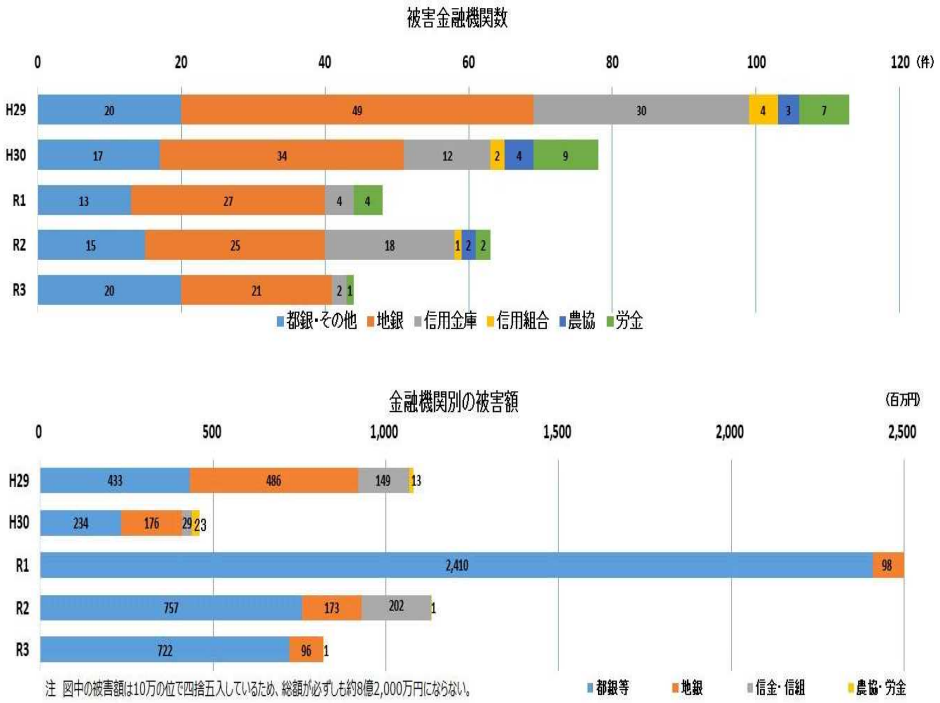
(1)　被害額の推移



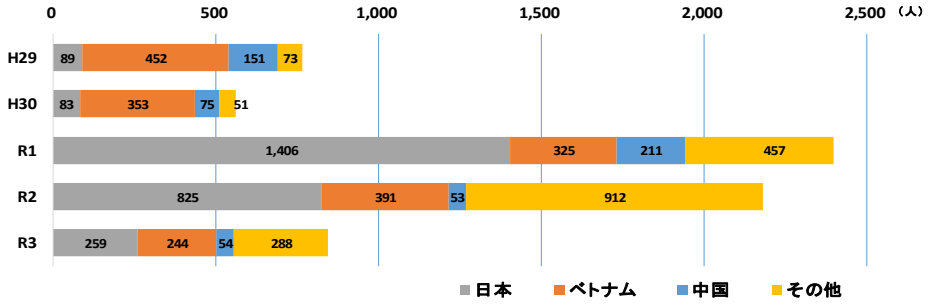
(2)　口座開設者別の被害状況



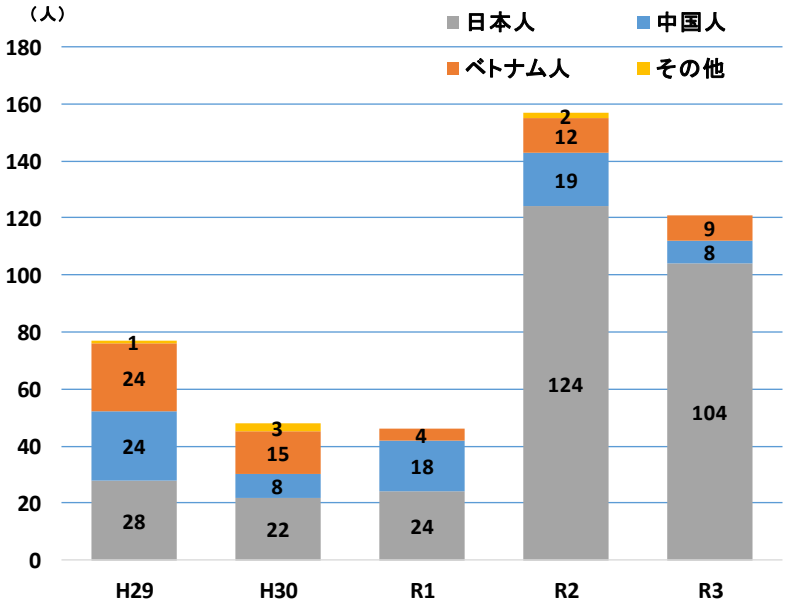
(3)　金融機関別の被害状況



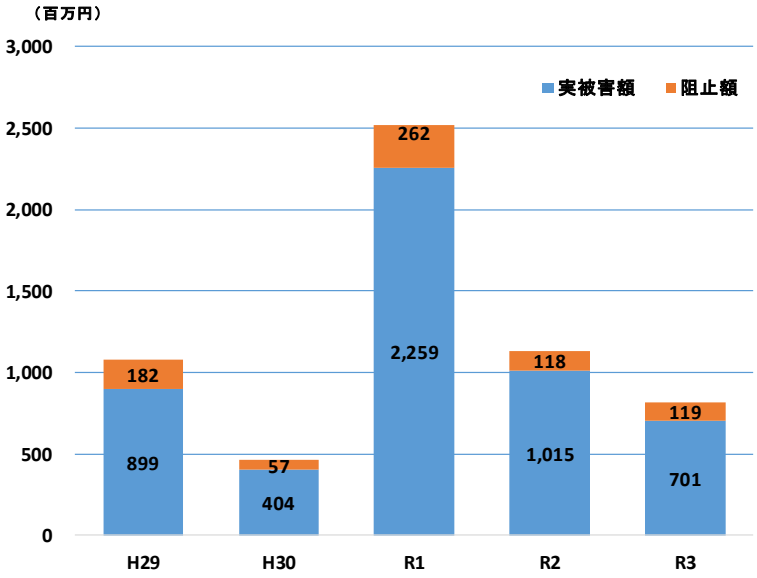
(4)　一次送金先口座名義人の国籍



(5)　国籍別の関連事件検挙状況

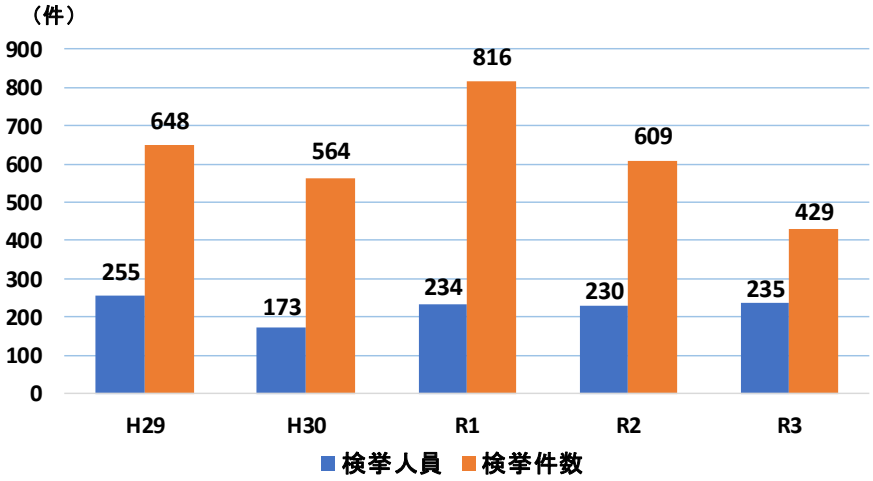


(6)　不正送金阻止状況

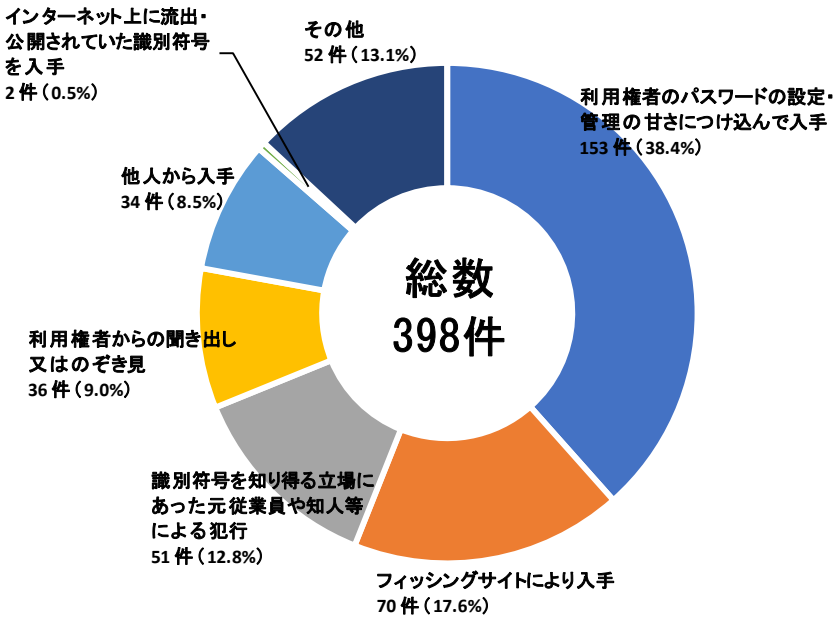


3　不正アクセス禁止法違反の検挙状況

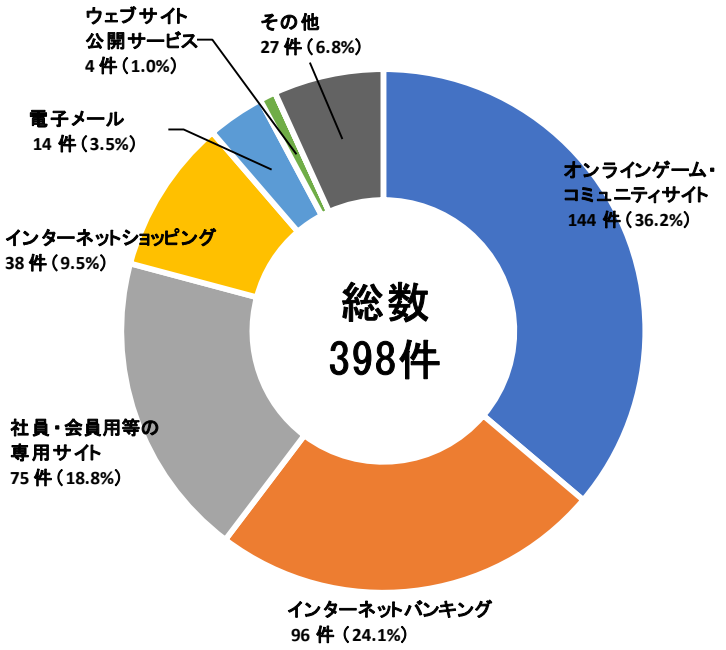
(1)　不正アクセス禁止法違反の検挙件数の推移



(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）

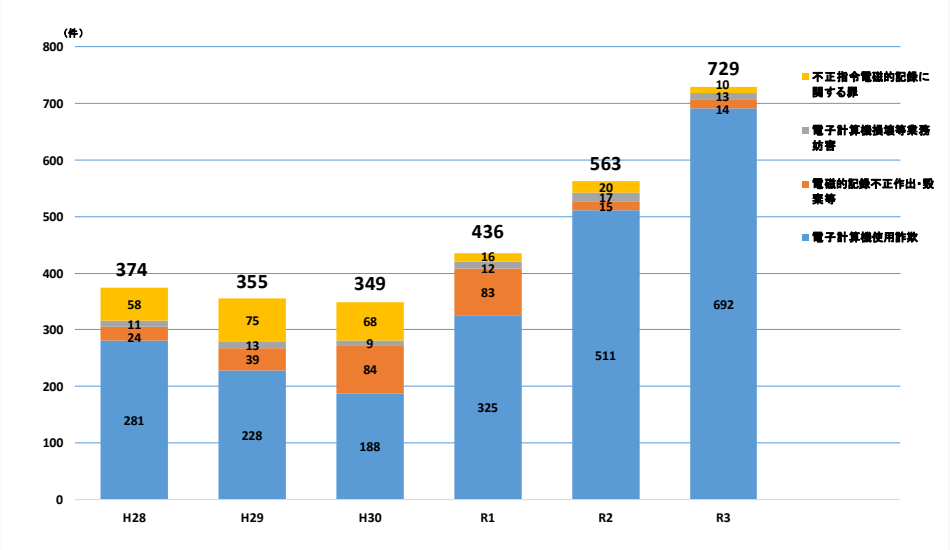


不正アクセス禁止法違反

○　会社員の男(42)は、平成31年２月、不正アクセス行為をする目的で、業務上知り得た顧客の証券口座のＩＤ・パスワードを自己の端末に保管し、同証券口座から自己が管理する銀行口座に不正に送金するなどした。令和３年３月、男を不正アクセス禁止法違反（識別符号保管）等で検挙した。

○　会社員の男（37）は、令和２年11月、知人女性の個人情報を収集する目的で、同女のＩＤ・パスワードを使用してメールアカウントに不正アクセスし、登録情報やメール内容を閲覧した。令和３年６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。

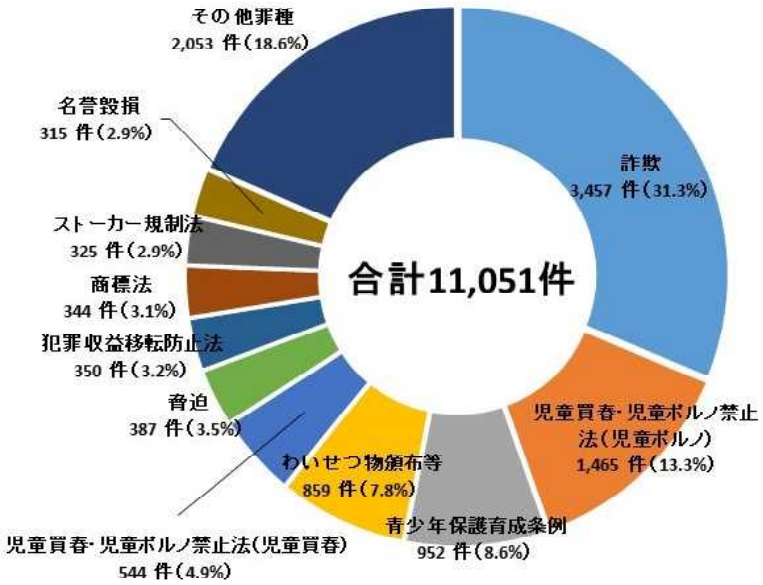
４　コンピュータ・電磁的記録対象犯罪の検挙状況



コンピュータ・電磁的記録対象犯罪

○　会社員の男（34）は、令和２年11月から12月にかけて、元勤務先のサーバに不正アクセスし、データを削除する不正なプログラムを蔵置して、誤って機能を有効化した従業員のパソコン等のデータを消去した。令和３年９月、男を電子計算機損壊等業務妨害等で検挙した。

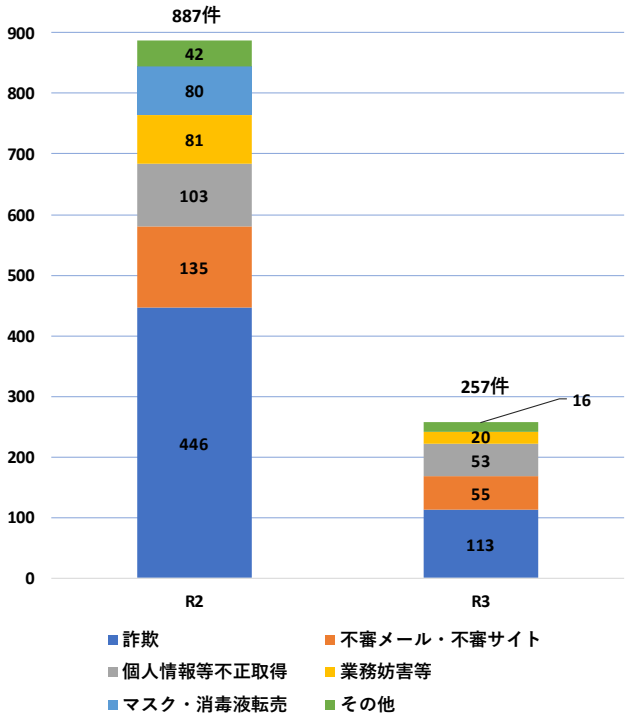
５　その他の検挙状況



詐欺

○　会社員の男（36）は、令和２年10月、オンラインで暗号資産を取り扱うための口座を第三者に利用させる目的で開設し、ログインに必要なＩＤ及びパスワードを有償で提供した。令和３年６月、男を詐欺等で検挙した。

６　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[*17]



*17　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、都道府県警察から警察庁に報告のあった件数。