広　報　資　料
令和４年９月15日
警　　察　　庁

令和４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

サイバー空間が量的に拡大・質的に進化するとともに、実空間との融合が進み、あらゆる国民、企業等にとって、サイバー空間は「公共空間」として、より一層の重みを持つようになっている。

一方で、国内においてランサムウェアによる感染被害が多発し、事業活動の停止・遅延等、社会経済活動に多大な影響を及ぼしているほか、サイバー攻撃や不正アクセスによる情報流出の相次ぐ発生など、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感染被害により、国内の自動車関連企業、半導体関連企業等のサプライチェーン全体が影響を受ける事案が発生したほか、個人情報・機密情報の流出、新規患者の受入れ停止、サービス障害等の事態が発生した。

○　複数の事業者に対して不正アクセスが行われ、情報流出の可能性がある事案を確認した。

○　警察庁が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は継続して高水準に推移している。大部分が海外を送信元とするものであり、海外からの脅威が引き続き高まっている。

３　警察における取組

○　サイバー事案への対処能力の強化、諸外国と連携した脅威への対処等を推進する観点から、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。

○　ランサムウェアによる被害の発生やサイバー攻撃事案のリスクの高まりを踏まえ、複数回にわたって、内閣サイバーセキュリティセンター（ＮＩＳＣ）等との連名による注意喚起を実施した。

○　Emotetの新たな感染手口について解析を行い、警察庁ウェブサイトにおいて注意喚起を実施した。

○　キャッシュレス決済サービスの不正利用防止を図るため、関係事業者と協議。関係事業者において、認証対策の強化や送金可能金額の引下げ等の対策が実施された。

別　添

令和４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

デジタル化の進展等に伴い、サイバー空間が量的に拡大・質的に進化するとともに、実空間との融合が進み、あらゆる国民、企業等にとって、サイバー空間は「公共空間」として、より一層の重みを持つようになっている。また、デジタルトランスフォーメーション（DX）の進展や中小企業を含めたサプライチェーンの拡大等、サイバー空間の「公共空間化」の加速は、国民生活や社会経済活動に様々な恩恵をもたらしている。

一方、国内においてもランサムウェアによる感染被害が多発し、事業活動の停止・遅延等、社会経済活動に多大な影響を及ぼしているほか、サイバー攻撃や不正アクセスによる情報流出の相次ぐ発生、Emotetの新たな感染手口の出現等、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４年上半期中に警察庁に報告されたランサムウェアによる被害件数は114件と、令和２年下半期以降、右肩上がりで増加し、その被害は、企業・団体等の規模やその業種を問わず、広範に及んでいる。サプライチェーンの中でセキュリティのぜい弱な部分が狙われ、サプライチェーン全体が影響を受ける事案がみられ、国内においては、自動車関連企業や半導体関連企業、産業機器関連企業においてランサムウェア感染被害が発生し、生産・販売活動の停止等を余儀なくされた。このほか、医療・福祉、運輸、建設、小売等の様々な企業・団体等がランサムウェアに感染し、個人情報・機密情報の流出、新規患者の受入れ停止、サービス障害、金銭被害等の事態が発生した。また、国内企業の海外子会社においてもランサムウェア感染被害が発生しており、一部企業では内部データの流出が確認されるなど、社会経済活動のみならず、国家安全保障にも大きな影響が生じ得る状況となっている。

国外においても、石油・港湾関連施設や運送会社、航空関連企業等に対するランサムウェア攻撃によって、燃料の供給停止や航空機の運行停止等の事態が生じ、市民生活や社会経済活動に多大な影響を及ぼすなど、ランサムウェアが世界的に猛威を奮っている状況にあるほか、ウクライナ情勢をはじめ、国際情勢が変化する中で、政府機関や重要インフラ分野の関連企業・施設等に対するサイバー攻撃も頻発しており、これらの攻撃には、国家の関与が疑われるものがみられるなど、こうした脅威についても注視していかなければならない。

警察庁では、ランサムウェアによる被害の発生やサイバー攻撃事案のリスクの高まりを受け、内閣官房内閣サイバーセキュリティセンター（ＮＩＳＣ）や関係省庁との合同により、複数回にわたって、重要インフラ事業者等をはじめとする企業・団体等に対して注意喚起を行った。

そのほか、Emotetの感染被害も相次いでおり、更なる感染被害の拡大も懸念さ

れるところ、警察では、Emotetの解析を継続して実施しており、４月にはショートカットファイルを用いた新たな感染手口について、６月にはウェブブラウザに保存されたクレジットカード番号等の情報を外部に送信する新機能について、それぞれ警察庁ウェブサイトを通じて注意喚起を実施した。

インターネットバンキングに係る不正送金事犯については、令和２年以降、発生件数、被害額ともに減少傾向が続いているが、フィッシング対策協議会によれば、令和４年上半期のフィッシング報告件数は前年同期と比較して倍増しており、クレジットカード事業者、通信事業者を装ったものが多くを占めている。

また、警察庁が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継続して高水準で推移している。これらのアクセスの大半は海外を送信元とするものであり、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と認められる。さらに、検知したアクセスの宛先ポートに着目すると、ポート番号1024以上のポートへのアクセスが大部分を占めており、これらのアクセスの多くがぜい弱性を有するＩｏＴ機器の探索やＩｏＴ機器に対するサイバー攻撃を目的とするためのものであるとみられる。

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、警察では、令和４年４月、警察庁にサイバー警察局を、関東管区警察局にサイバー特別捜査隊を新設し、警察庁と都道府県警察とが一体となった捜査、実態解明等に取り組むとともに、捜査・解析能力の高度化や事業者等と連携した被害防止対策の立案・実施等の取組を推進している。引き続き、これらの取組を強力に推進し、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。

1　令和４年上半期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。

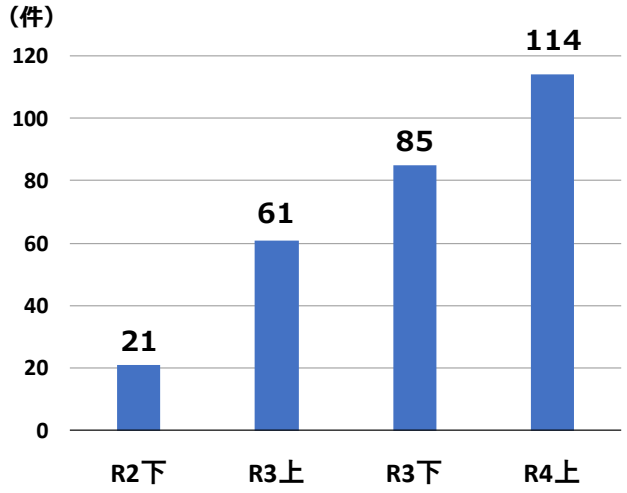
従来は、暗号化したデータを復元する対価として企業等に金銭を要求していたが、最近では、データの暗号化のみならず、データを窃取した上で「対価を支払わなければ当該データを公開する」などとして金銭を要求する二重恐喝（ダブルエクストーション）という手口や、ＶＰＮ機器をはじめとするネットワーク等のインフラのぜい弱性を狙って侵入する手口が多くみられる。

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４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114件であり、令和２年下半期以降、右肩上がりで増加している。

【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

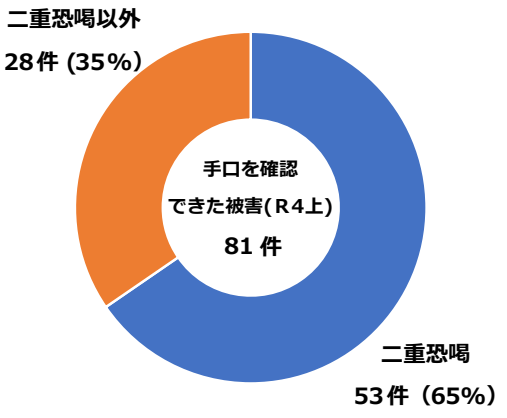
○　二重恐喝（ダブルエクストーション）による被害が多くを占める

被害（114件）のうち、警察として手口を確認できたものは81件あり、このうち、二重恐喝の手口によるものは53件で65％を占めている。

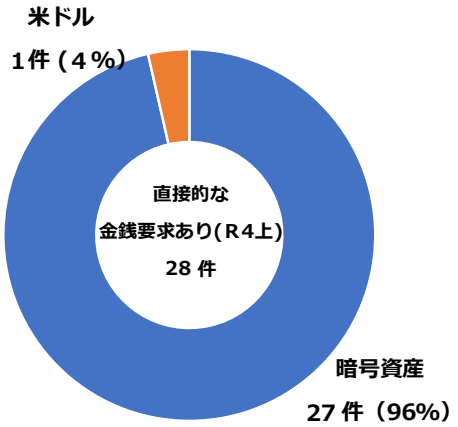
○　暗号資産による金銭の要求が多くを占める

被害（114件）のうち、直接的な金銭の要求を確認できたものは28件あり、このうち、暗号資産による支払いの要求があったものは27件で96％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】



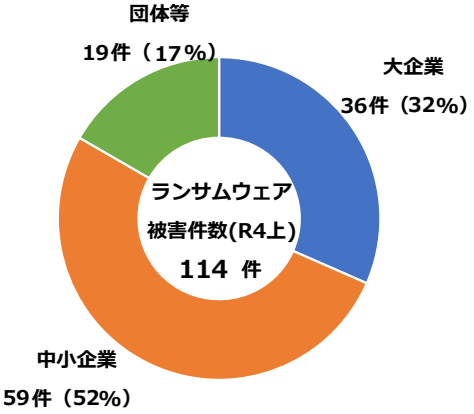
【図表３：要求された金銭支払い方法別報告件数】



(ｳ)　被害企業・団体等の規模

被害（114件）の内訳を企業・団体等の規模別[*1] にみると、大企業は36件、中小企業は59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企業・団体等の規模別報告件数】



注　図中の割合は小数第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。

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（114件）のあった企業・団体等にアンケート調査を実施したところ、57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

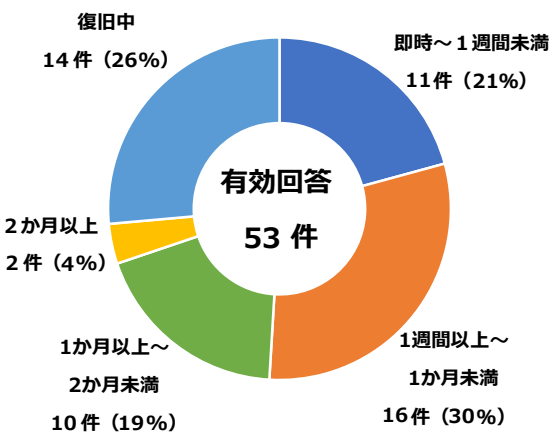
復旧に要した期間について質問したところ、53件の有効な回答があり、このうち、復旧までに１か月以上を要したものが12件あった。

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、49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27件で55%を占めている。

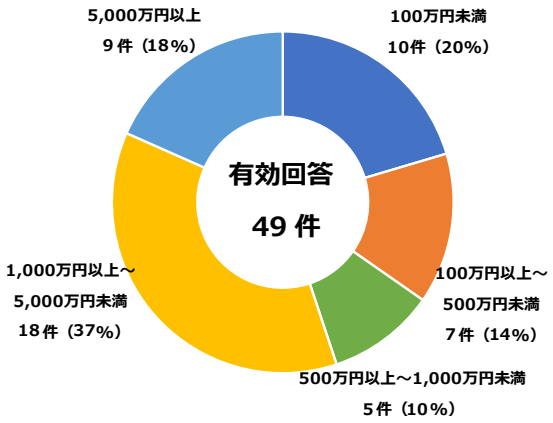
---

*1　中小企業基本法第２条第１項に基づき分類

【図表５：復旧に要した期間】



【図表６：調査・復旧費用の総額】

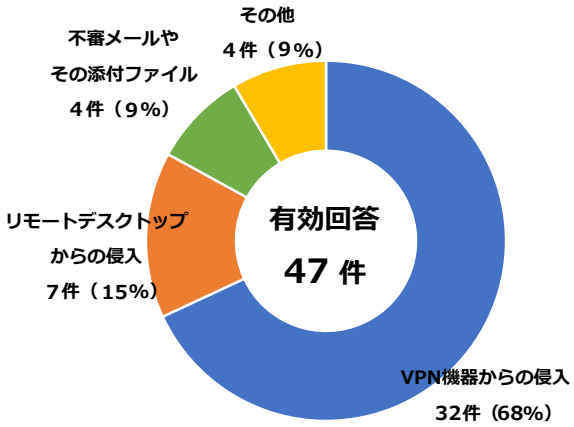


注　図中の割合は小数第１位以下を四捨五入しているため、総計が必ずしも100にならない。

(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、47件の有効な回答があり、このうち、ＶＰＮ機器からの侵入が32件で68%、リモートデスクトップからの侵入が７件で15%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83%と大半を占めている。

【図表７：感染経路】



注　図中の割合は小数第１位以下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

令和４年上半期においても、ランサムウェアによって流出した情報等が掲載されているダークウェブ上のリークサイトに、日本国内の事業者等の情報が掲載されていたことを確認した。掲載された情報には、財務情報や関係者、顧客等の情報が含まれていた。

【図表８：ダークウェブ上のリークサイト例】

オ　警察の取組

○　中小企業や医療機関等を対象としたランサムウェアへの対策

国内の中小企業や医療機関において、ランサムウェアの被害により製造・販売・サービス等の停止、電子カルテ等の閲覧障害による新規患者の受入れ停止等の事態が生じた。

そのため、商工会・商工会議所等の経済団体とその傘下の事業者や病院協会とその傘下の病院等とネットワーク等を構築し、手口の情報共有や注意喚起を実施したほか、テレビ、ラジオ、オンデマンド配信、警察主催のセキュリティセミナーの開催等のあらゆる機会・媒体の活用、各都道府県警察が関係機関・団体等と構築する協議会等の参画組織を通じた情報発信等による積極的な広報啓発を実施し、セキュリティ強化等の被害防止対策の実施を促した。

○　関係省庁等との連名による注意喚起の実施

ランサムウェアによる被害の発生やサイバー攻撃事案のリスクの高まりを踏まえ、内閣官房内閣サイバーセキュリティセンター（ＮＩＳＣ）や関係省庁との合同により、重要インフラ事業者等をはじめとする企業、団体等に対して、具体的なセキュリティ対策の実施項目を挙げながら、サイバーセキュリティ対策を強化するよう注意喚起を行った。

【図表９：ＮＩＳＣ、関係省庁との連名による注意喚起文書】

令和４年３月１日
経済産業省
金融庁
総務省
厚生労働省
国土交通省
警察庁
内閣官房内閣サイバーセキュリティセンター

サイバーセキュリティ対策の強化について（注意喚起）

昨今の情勢を踏まえるとサイバー攻撃事案のリスクは高まっていると考えられます。本日、国内の自動車部品メーカーから被害にあった旨の発表がなされたところです。

政府機関や重要インフラ事業者をはじめとする各企業・団体等においては、組織幹部のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、以下に掲げる対策を講じることにより、対策の強化に努めていただきますようお願いいたします。

また、中小企業、取引先等、サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロールできるよう、適切なセキュリティ対策を実施するようお願いいたします。

さらに、国外拠点等についても、国内の重要システム等へのサイバー攻撃の足掛かりになることがありますので、国内のシステム等と同様に具体的な支援・指示等によりセキュリティ対策を実施するようお願いいたします。

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、早期対処のために速やかに所管省庁、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。

１．リスク低減のための措置
○パスワードが単純でないかの確認、アクセス権限の確認・多要素認証の利用・不要なアカウントの削除等により、本人認証を強化する。
○IoT 機器を含む情報資産の保有状況を把握する。特に VPN 装置やゲートウェイ等、インターネットとの接続を制御する装置の脆弱性は、攻撃に悪用されることが多いことから、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。
○メールの添付ファイルを不用意に開かない、URL を不用意にクリックしない、連絡・相談を迅速に行うこと等について、組織内に周知する。
２．インシデントの早期検知
○サーバ等における各種ログを確認する。
○通信の監視・分析やアクセスコントロールを再点検する。
３．インシデント発生時の適切な対処・回復
○データ消失等に備えて、データのバックアップの実施及び復旧手順を確認する。
○インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、対外応答や社内連絡体制等を準備する。

(2) 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

○　複数の化学企業におけるマルウェア感染

１月、化学工業関連企業は、自社で運用するサーバに不正アクセスが行われ、サーバ内に保存した情報の一部が外部に流出した可能性があると発表した。これに関連し、同社のグループ企業においても管理するサーバに不正アクセスが行われ、サーバ内に保存した情報が外部に流出した可能性があることを発表した。

○　大手システム事業者等に対する不正アクセス

５月、大手システム事業者及びグループ会社は、一部の通信制御装置に対して、ぜい弱性を悪用した不正アクセスが行われていたことを確認したと発表した。これにより、当該通信制御装置を通過した通信パケット等を窃取された可能性があるとしている。

イ　警察における取組

○　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４年上半期には特定の情報通信機器のぜい弱性に関して全国に注意喚起を実施したほか、海外の関係機関・団体等からサイバー攻撃等に関する情報を入手した場合は個別に注意喚起を行うなど、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。

○　Ｃ２サーバのテイクダウン

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Ｃ２サーバとして機能している国内のサーバを把握し、Ｃ２サーバとしての不正な機能を停止（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の対策を継続的に実施している。令和４年上半期では、３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

サイバー攻撃事案の発生を想定した重要インフラ事業者等との共同対処訓練を継続的に実施している。令和４年上半期においても、自治体、電力事業者、金融機関等の幅広い分野の事業者等を対象とした、標的型メールを題材とした訓練や警察との連携を確認するための現場臨場訓練等の実践的な訓練を実施し、警察との連携強化や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。

○　Emotetの解析と注意喚起の実施

電子メールの添付ファイルを主な感染経路とする不正プログラムEmotetは令和３年11月頃から活動を再開し、令和４年２月頃から再び被害が多くなった。警察庁では、変化し続けるEmotetを継続的に解析しており、

令和４年４月にはショートカットファイルを用いた新たな感染手口について、６月にはウェブブラウザ「Google Chrome」に保存されたクレジットカード番号等の情報を外部に送信するという新機能について、それぞれ警察庁ウェブサイトにおいて注意喚起を行った。

【図表10：Emotetの新たな手口に係る注意喚起文書】

令和４年４月28日
警　　察　　庁

マルウェアEmotetの新たな手口に係る注意喚起について

警察庁では、国内においてEmotetの攻撃によるものとみられる被害を確認しております。Emotetは、主にメールを感染経路としたマルウェア（不正プログラム）です。メールソフトに登録されている連絡先から知り合いのメールアドレスを盗んで使うなどして、本人作成のメールであると信じ込ませ、不審に思わず開封してしまいそうなメールの返信を装うなど巧妙化が進んでいます。感染すると、情報を盗まれる、ランサムウェア等の他のマルウェアにも感染するといった被害に遭うおそれがあります。

これまでは、添付ファイルのマクロを有効化した場合にEmotetに感染させる手口等が確認されていました。これに加えて本年４月下旬以降、ショートカットファイル（LNKファイル）を添付し、これをダブルクリックなどで開いた場合にEmotetに感染させる手口が新たに確認されています。

不用意にメールの添付ファイルを開かないようにするなど、マルウェアに感染しないように注意してください。

【関連サイト】

○　春の大型連休に向けて実施いただきたい対策について（注意喚起）
https://www.npa.go.jp/cybersecurity/pdf/20220425press.pdf

○　警察庁（@police）Emotetの解析結果について
https://www.npa.go.jp/cyberpolice/important/2020/202012111.html

○　マルウェアEmotetに係る注意喚起について
https://www.npa.go.jp/cyber/pdf/R040204_emotet.pdf

【図表11：Emotetの解析結果】

Emotetの解析結果について

2022年6月9日
警察庁

新機能の確認（2022年6月9日）

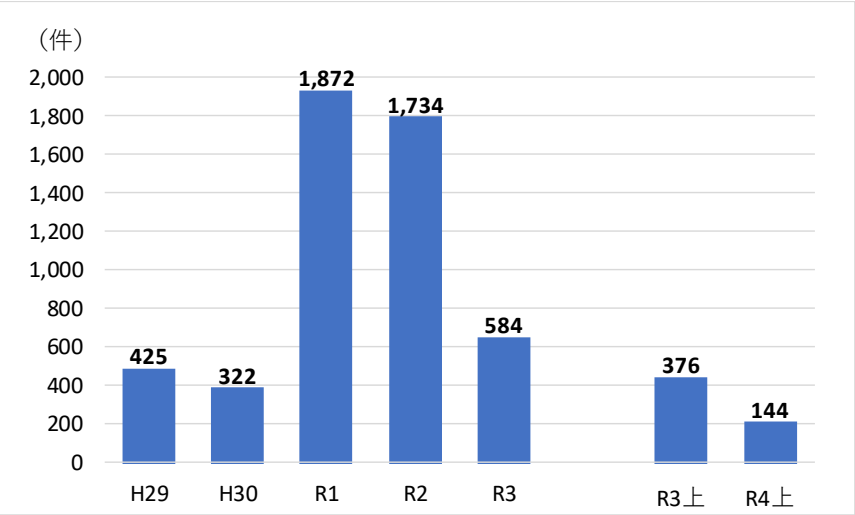
ウェブブラウザ「Google Chrome」に保存されたクレジットカード番号や名義人氏名、カード有効期限を盗み、外部に送信する機能が追加されたことを確認しました。Google Chromeでは個人情報を暗号化して安全に保存していますが、Emotetの新機能は暗号データを元に戻すための鍵も同時に盗み出すため、Emotetに感染すると、お使いのクレジットカード情報が第三者に知られるおそれがあります。

(3)　フィッシング等に伴う不正送金・不正利用の情勢と対策

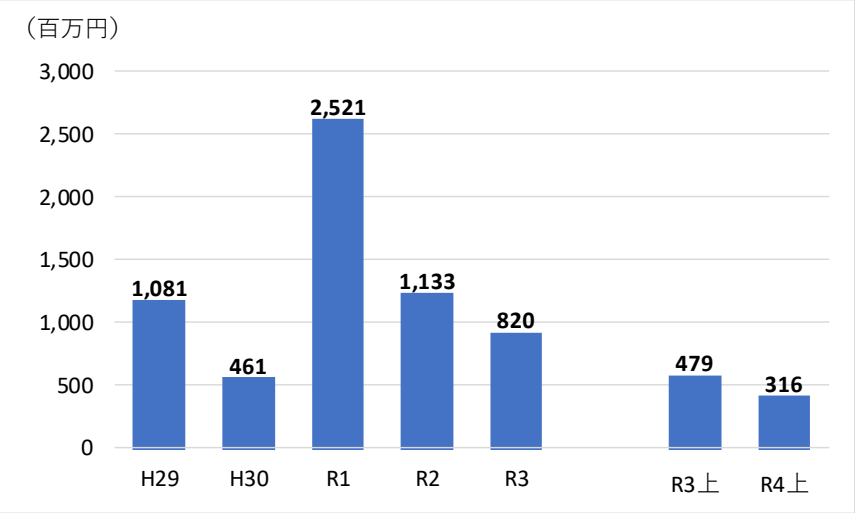
ア　インターネットバンキングに係る不正送金事犯の発生状況

令和４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144件、被害総額約3億1,571万円で、前年同期と比べて発生件数、被害額ともに減少した。

【図表12：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13：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

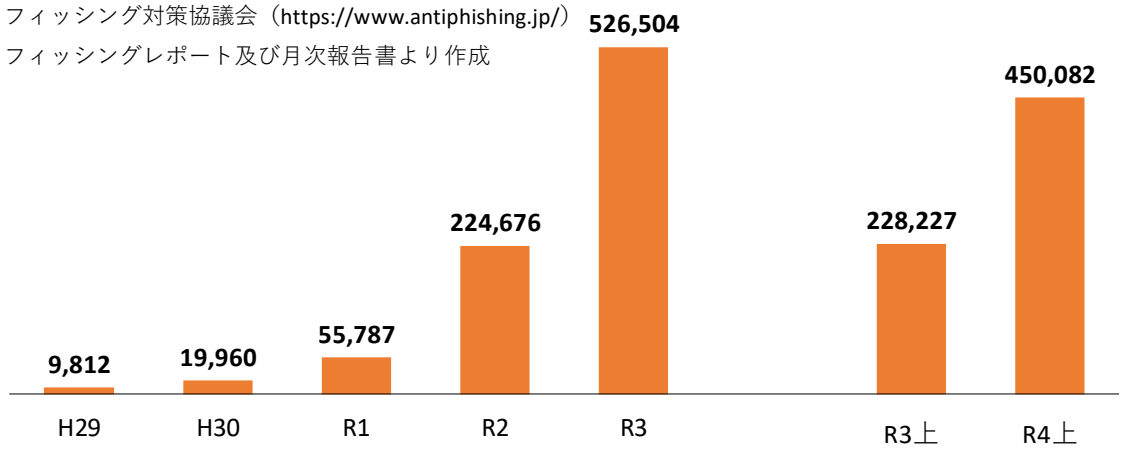
インターネットバンキングに係る不正送金事犯は、令和元年に、ＳＭＳ等を用いて金融機関を装ったフィッシングサイトへ誘導する手口が急増し、ＩＤ・パスワード、ワンタイムパスワード等が窃取され、金融機関のインターネットバンキングから不正送金される被害等が多発し、同年には、発生件数1,872件、被害総額約25億2,100万円に達した。

こうした情勢を踏まえ、金融機関、ＪＣ３等と緊密に連携の上で被害防止対策について協議した結果、金融機関において、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が推進され、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２年以降、件数、被害額ともに減少している。

他方、フィッシング対策協議会によれば、令和４年上半期のフィッシング報告件数は45万82件（前年同期比＋22万1,855件）で、銀行を装ったものの割合は少なく、クレジットカード事業者、通信事業者を装ったものが多いとされており、フィッシング報告件数は右肩上がりで増加している。

【図表14：フィッシング報告件数の推移】



ウ　警察の取組

○　不正送金事犯に係る被疑者の検挙

令和３年５月に発生した不正送金事犯に関し、令和４年１月、口座名義人がメモアプリに保存していた口座情報を利用して不正送金に関与した指示役を不正アクセス禁止法違反及び電子計算機使用詐欺で検挙した。

○　キャッシュレス決済サービス不正利用事犯に係る被疑者の検挙

令和４年４月に発生したフィッシングに係るキャッシュレス決済サービスの不正利用事犯に関し、同年６月、他人名義のキャッシュレス決済用画像を利用して商品を騙し取った不正利用事件に関与した買い子役を詐欺で検挙した。

○　金融機関等との連携強化

金融庁及び一般社団法人全国銀行協会等に対して、インターネットバンキングの不正送金に係る被害状況等を提供することにより、被害防止対策に取り組んでいる。

○　ＳＭＳを悪用したフィッシング対策

ショートメッセージサービス（ＳＭＳ）によってフィッシングサイトへ誘導する手口であるスミッシングによる被害を防止するため、大手携帯電話事業者及びＪＣ３と協議を行った。その結果、ＪＣ３から提供される情報を活用してフィッシングサイトへ誘導するＳＭＳの受信を自動で拒否する機能が、令和４年３月から当該大手携帯電話事業者により提供されるよ

うになった。

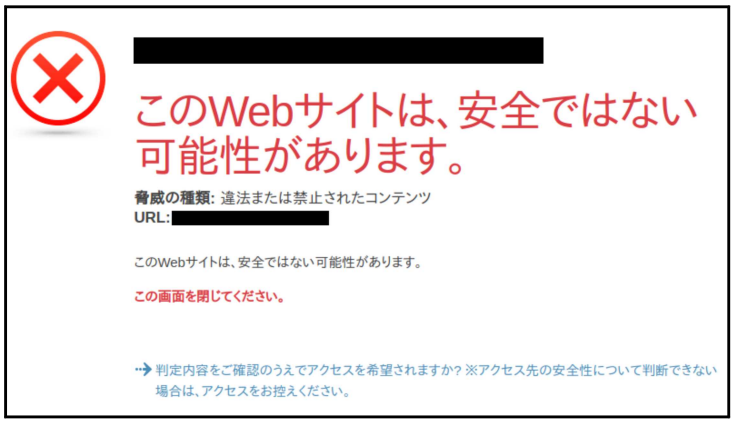
○　キャッシュレス決済サービスの不正利用防止対策

フィッシングに係るキャッシュレス決済サービスの不正利用防止を図るため、関係事業者と協議したところ、当該事業者において、令和４年４月から、オートチャージ設定に係る認証対策が、令和４年５月から、送金可能金額の引下げ等の不正利用対策が、それぞれ実施されるようになった。

○　フィッシングサイトの閲覧防止対策

都道府県警察が把握したフィッシングサイトに係るＵＲＬ情報等を警察庁において集約し、ウイルス対策ソフト事業者等に提供することにより、ウイルス対策ソフトの機能による警告表示がされるなど、フィッシングサイトの閲覧を防止する対策を実施している。

【図表15：警告表示の例[*2]】



*2　図表15については、複製・転載により使用することを禁じる。

２　サイバー空間の脅威情勢

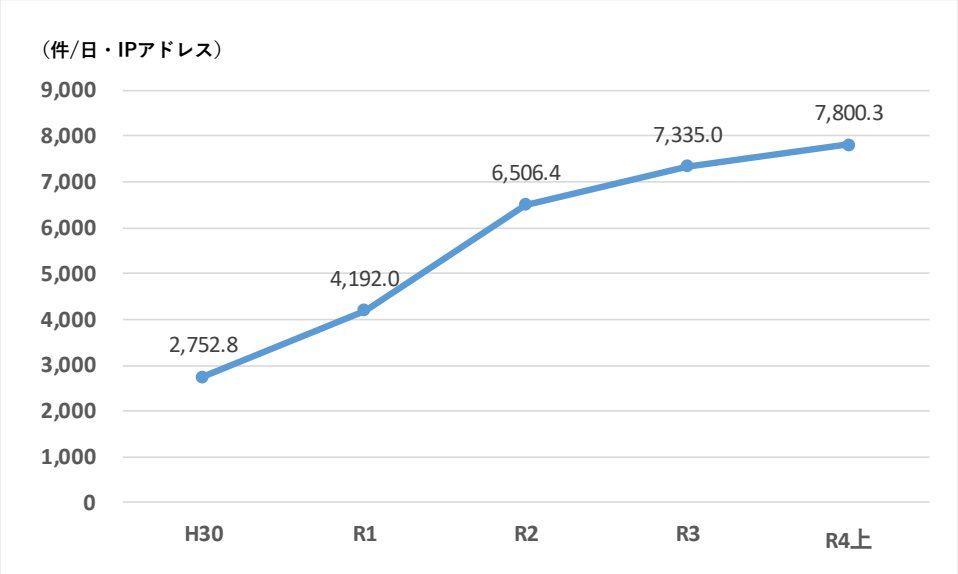
(1)　サイバー空間におけるぜい弱性探索行為等の観測状況

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ので、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。送られてくるのは不特定多数のＩＰアドレスに対して無差別に送信される通信パケットであり、これら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等を観測し、ぜい弱性を悪用した攻撃、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４年上半期にセンサー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7,800.3件と、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、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】

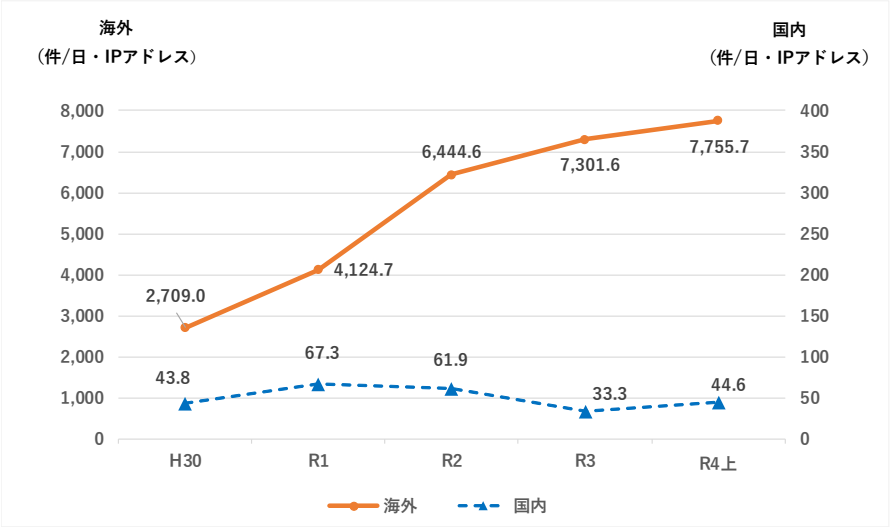


イ　特徴的な観測

○　海外を送信元とするアクセスが高水準で推移

検知したアクセスの送信元の国・地域に着目すると、近年、海外の送信元が高い割合を占めている。

【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】

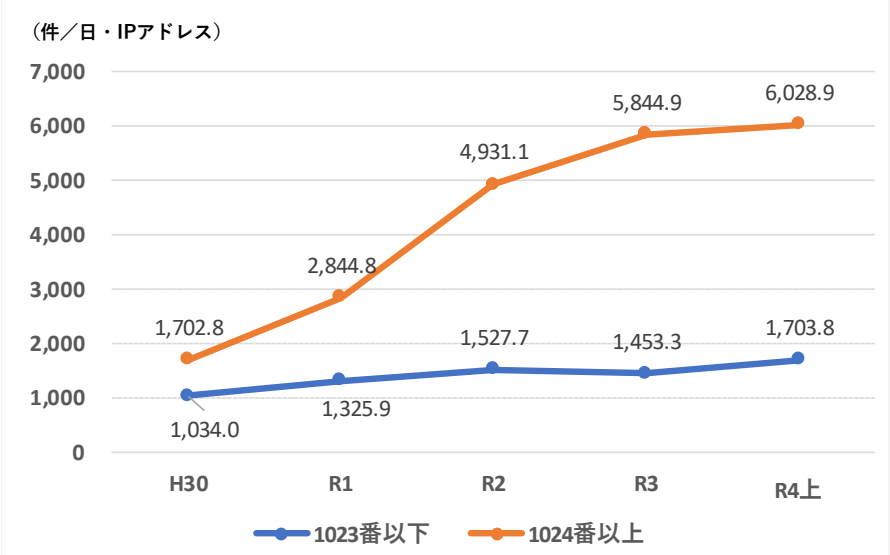


令和４年上半期においても、国内を送信元とするアクセスが１日・１ＩＰアドレス当たり44.6件であるのに対して、海外を送信元とするアクセスが7,755.7件と大部分を占めており、海外からの脅威への対処が引き続き重要となっている。

○　ＩｏＴ機器を対象としたぜい弱性探索行為等

検知したアクセスの宛先ポートに着目すると、ポート番号1024以上のポートへのアクセスが大部分を占めており、全体のアクセス件数が高水準で推移する要因となっている。

【図表18：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】



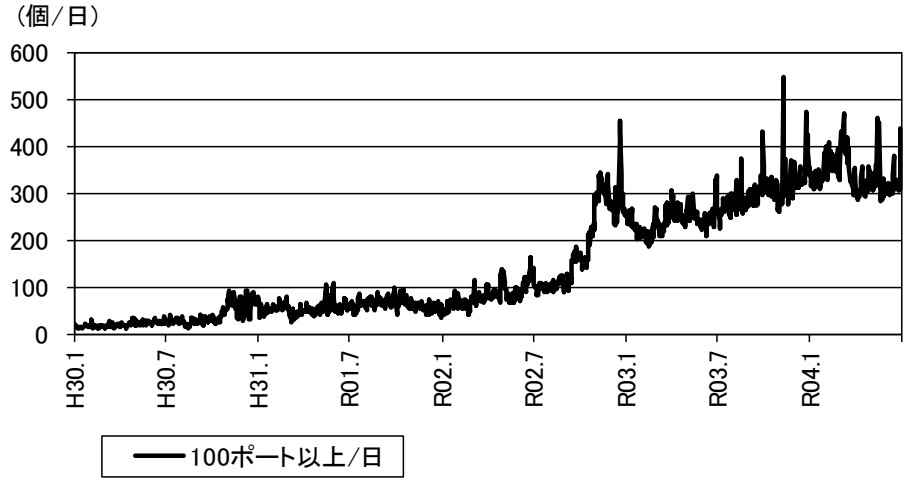
ポート番号1024以上は、主としてＩｏＴ機器が標準設定で使用するポート番号であることから、これらのアクセスの多くがぜい弱性を有するＩｏＴ機器の探索やＩｏＴ機器に対するサイバー攻撃を目的とするためのものであるとみられる。

また、Miraiボットの特徴を有するアクセスを継続して検知していることもあり、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状況である。

○　単一の送信元から広範な宛先ポートへのアクセスの増加

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。令和４年上半期において、１日当たり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アドレス数は341.8個で、前年同期の242.5個と比較して99.3個（41%）増加した。

【図表19：１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】



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アドレス数の増加の背景としては、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、それらのぜい弱性の有無を網羅的かつ短期的に把握しようとする者が増加していることや、ボットネットを利用することで広範な探索が行われていることなどがあると考えられる。把握したぜい弱性等の情報を悪用された場合は、短期間に広範囲の攻撃が行われるなどといった被害の発生が懸念される。

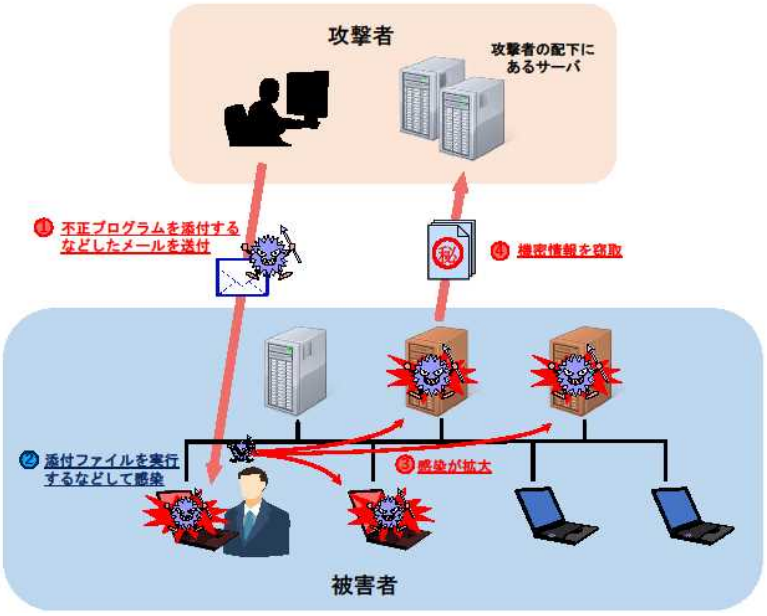
そのため、機器のぜい弱性対策として、OS等を最新のものにアップデートする、パスワードを使い回さないなど、一般的なセキュリティ対策を確実に行うことが重要である。

(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

警察及び先端技術を有するなど情報窃取の標的となるおそれのある全国約8,400の事業者等（令和４年６月末現在）から構成されるサイバーインテリジェンス情報共有ネットワーク（以下「ＣＣＩネットワーク」という。）の枠組みを通じて、事業者等から提供される標的型メール攻撃をはじめとする情報窃取を企図したとみられるサイバー攻撃に関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、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、当該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

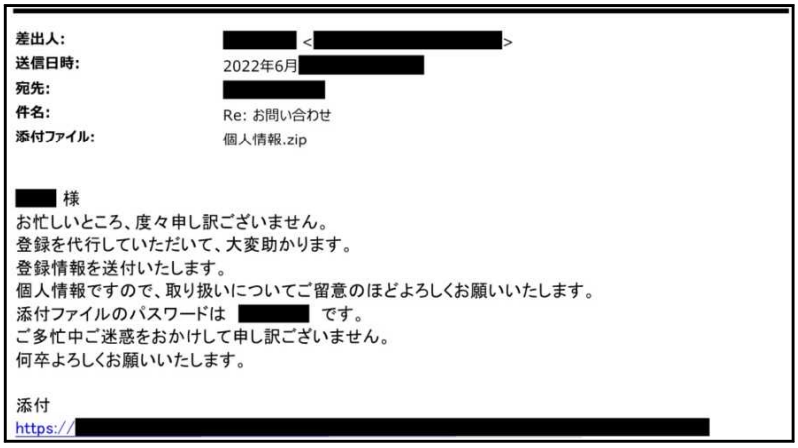
ＣＣＩネットワークを通じて事業者等から情報提供を受けた標的型メール攻撃には以下のようなものがあった。

なお、令和４年上半期においても、事業者等に対して、業務に関連した精巧な内容の標的型メールが確認されたほか、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はじめとする不審なメールも確認されている。

○　シンクタンクに対する標的型メール攻撃

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。

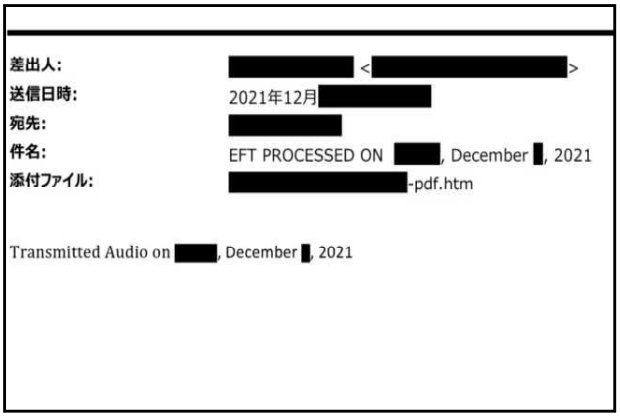
【図表21：メール文面】



○　医薬品メーカーに対する攻撃

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医薬品メーカーに送信された。

【図表22：メール文面】



【図表23：遷移後の画面】

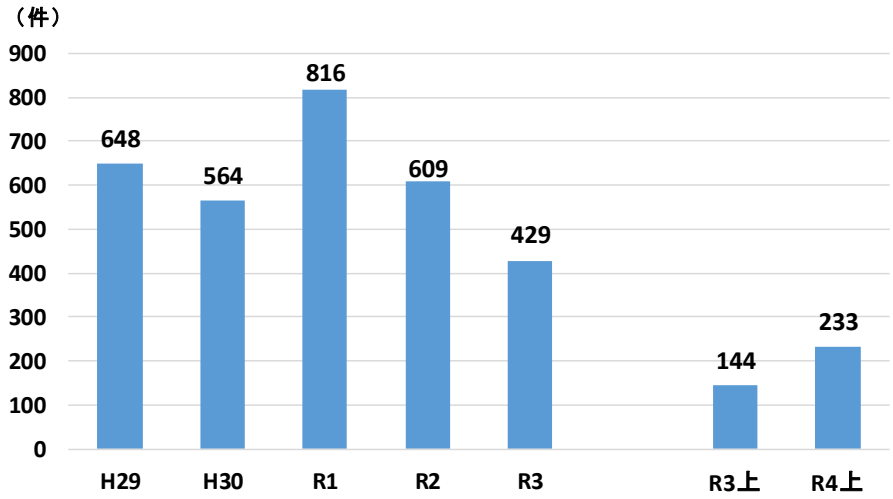
(3)　主なサイバー犯罪の現況

ア　不正アクセス禁止法[*3]違反

(ｱ)　検挙件数

令和４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233件と、前年同期と比べて89件増加した。

【図表24：不正アクセス禁止法違反の検挙件数の推移】



(ｲ)　特徴

検挙件数のうち、217件が識別符号窃用型[*4]で全体の93.1％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100件と最も多く、全体の46.1％を占めており、次いで「他人から入手」が22件で全体の10.1％を占めている。

○　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

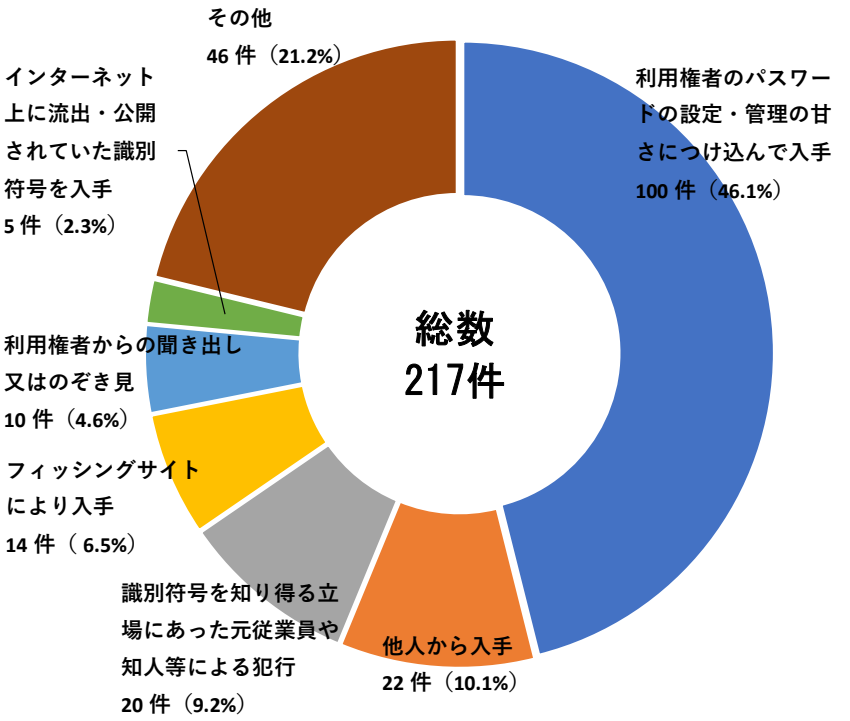
識別符号窃用型の不正アクセス行為に係る被疑者が不正に利用したサービスは、「オンラインゲーム・コミュニティサイト」が113件と最も多く、全体の52.1％を占めており、次いで「社員・会員用等の専用サイト」が51件で全体の23.5％を占めている。

---

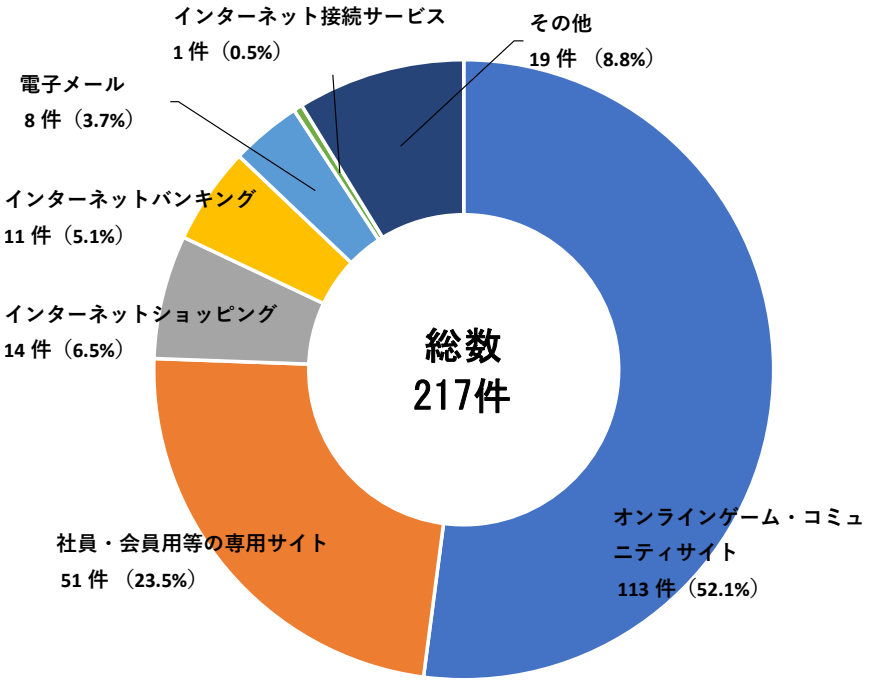
*3　不正アクセス行為の禁止等に関する法律（「不正アクセス行為・他人の識別符号を不正に取得する行為・不正アクセス行為を助長する行為・他人の識別符号を不正に保管する行為・識別符号の入力を不正に要求する行為」の５つの違反行為が定められている。）

*4　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。

【図表25：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】



【図表26：不正に利用されたサービス別検挙件数（識別符号窃用型）】



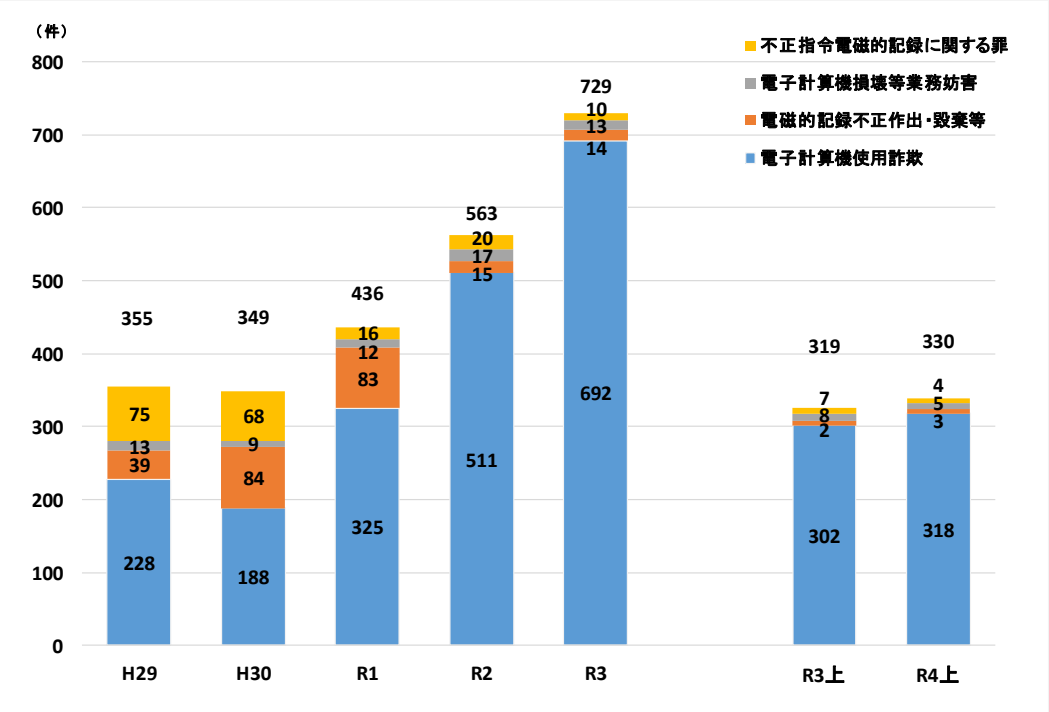
注　図中の割合は小数第２位以下を四捨五入しているため、総計が必ずしも100にならない。

イ　コンピュータ・電磁的記録対象犯罪[*5]

(ｱ)　検挙件数

令和４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330件で、前年同期と比べて11件増加した。

【図表27：コンピュータ・電磁的記録対象犯罪の検挙件数の推移】



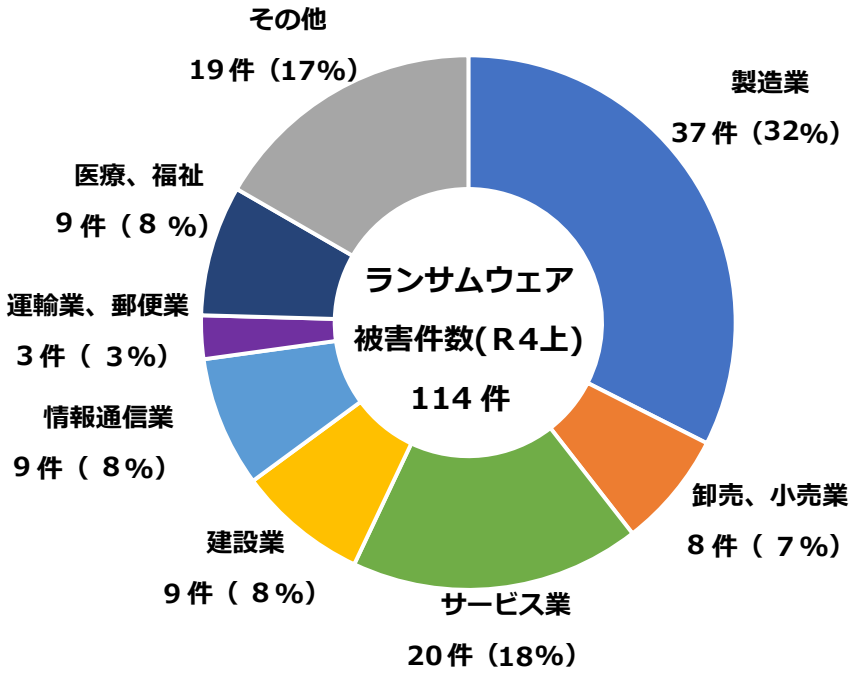
(ｲ)　特徴

検挙件数のうち、電子計算機使用詐欺が318件と最も多く、全体の96.4％を占めている。

*5　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

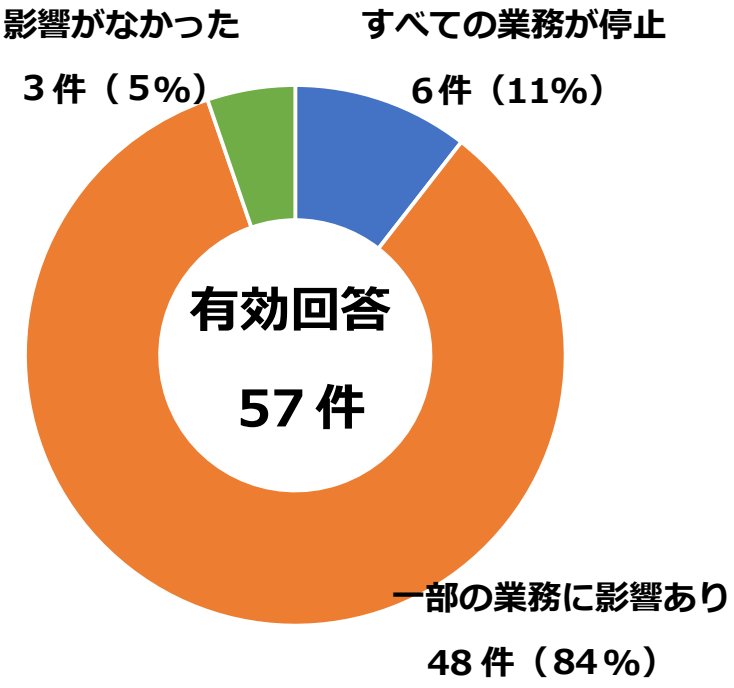
1　企業・団体等におけるランサムウェア被害及びその実態

(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

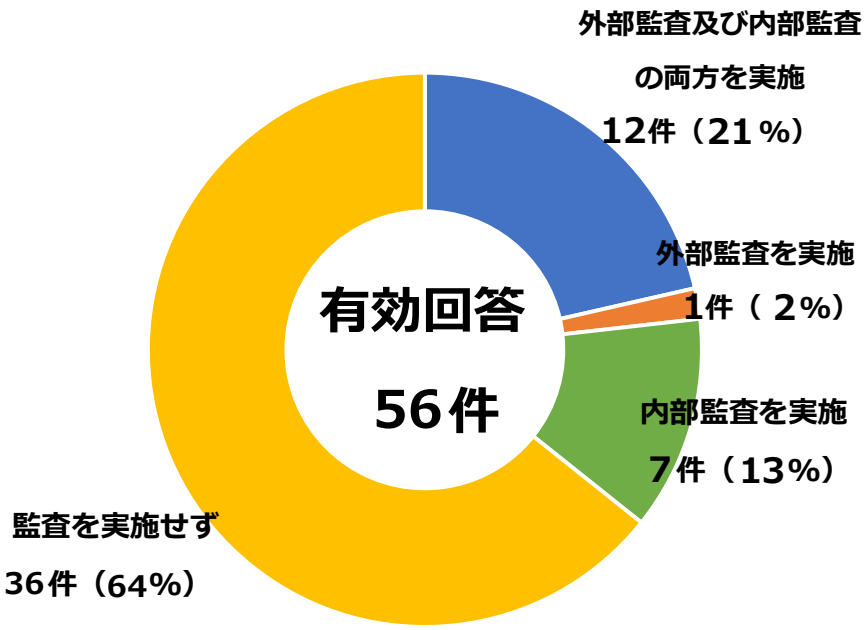


注　図中の割合は小数第１位以下を四捨五入しているため、総計が必ずしも100にならない。

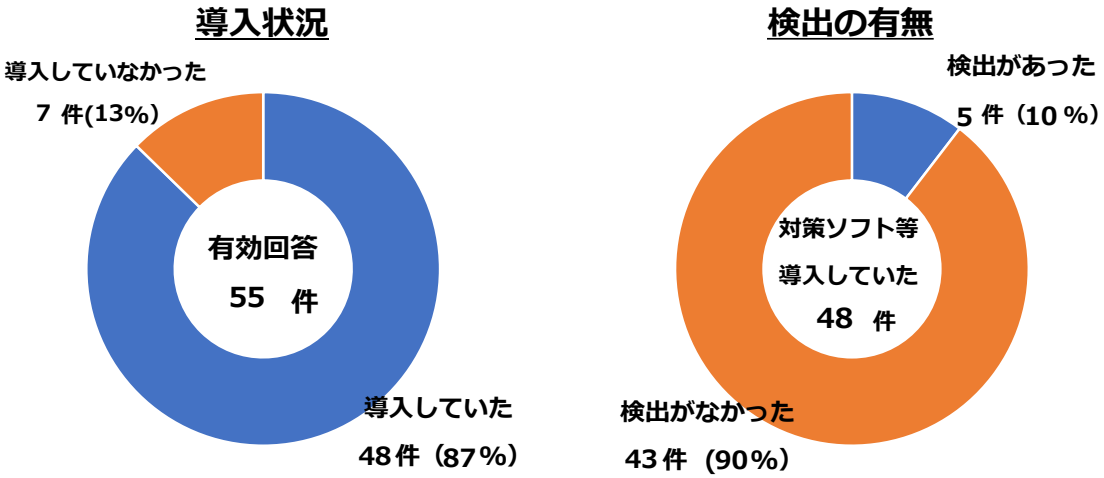
(2)　ランサムウェア被害が業務に与えた影響



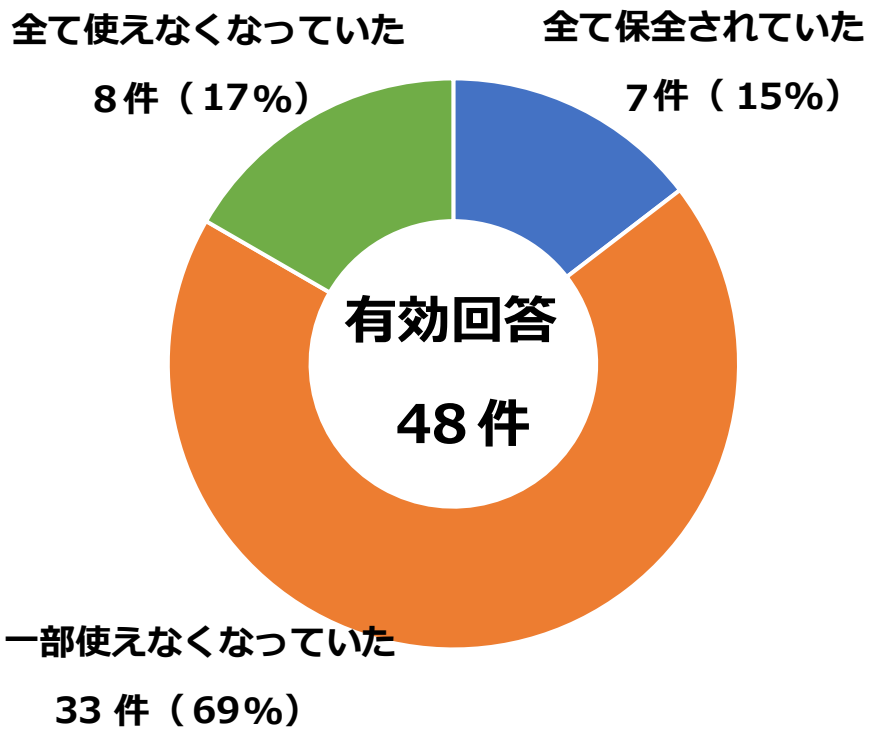
(3)　被害企業・団体等の情報セキュリティ監査の実施状況



(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

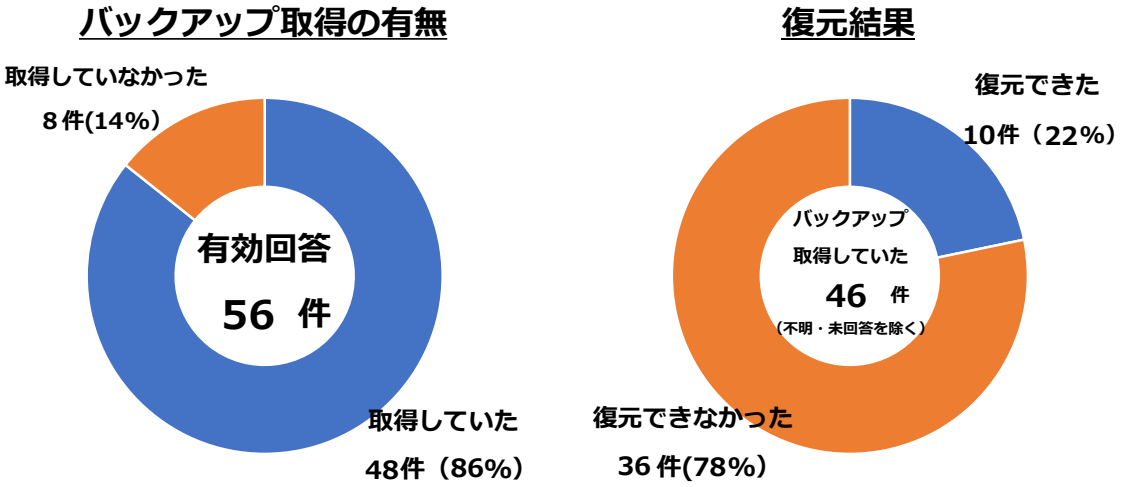


(5)　ランサムウェア被害における被害企業・団体等のログの保全状況



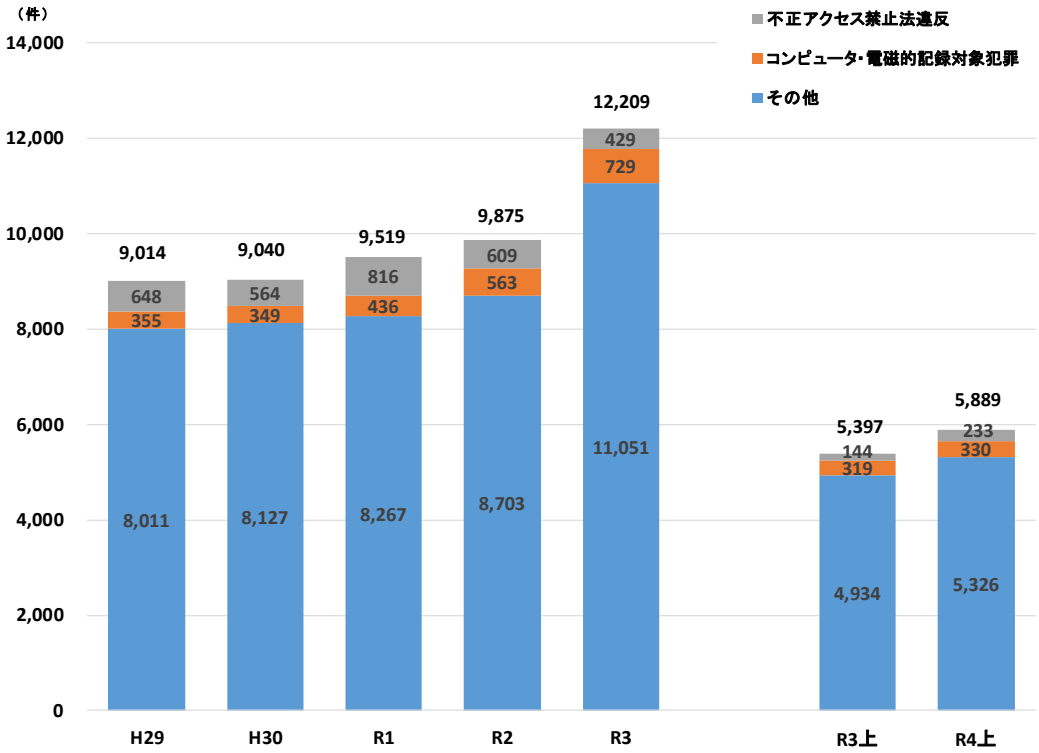
注　図中の割合は小数第１位以下を四捨五入しているため、総計が必ずしも100にならない。

(6)　被害企業・団体等のバックアップの取得・活用状況

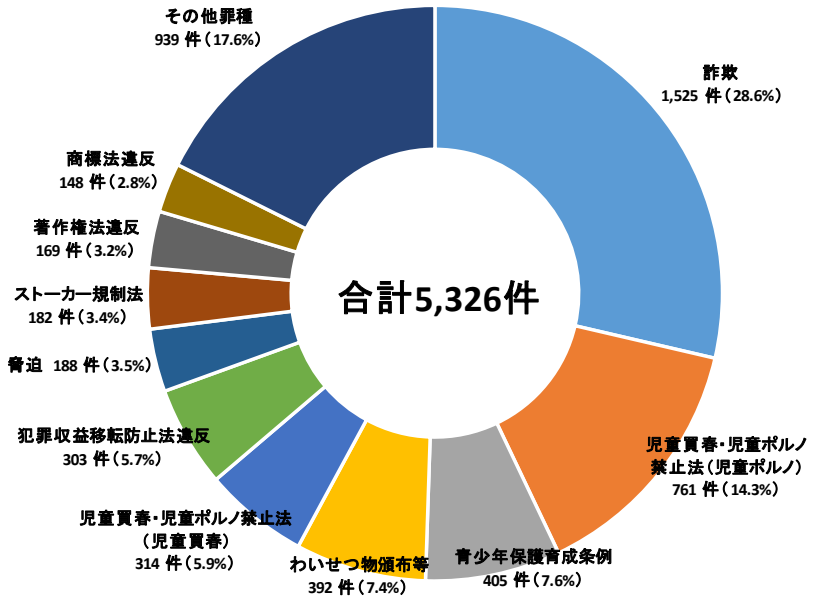


2　サイバー犯罪[*1]の検挙状況

(1)　サイバー犯罪の検挙件数の推移



(2)　その他の検挙状況[*2]



注　図中の割合は小数第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。

---

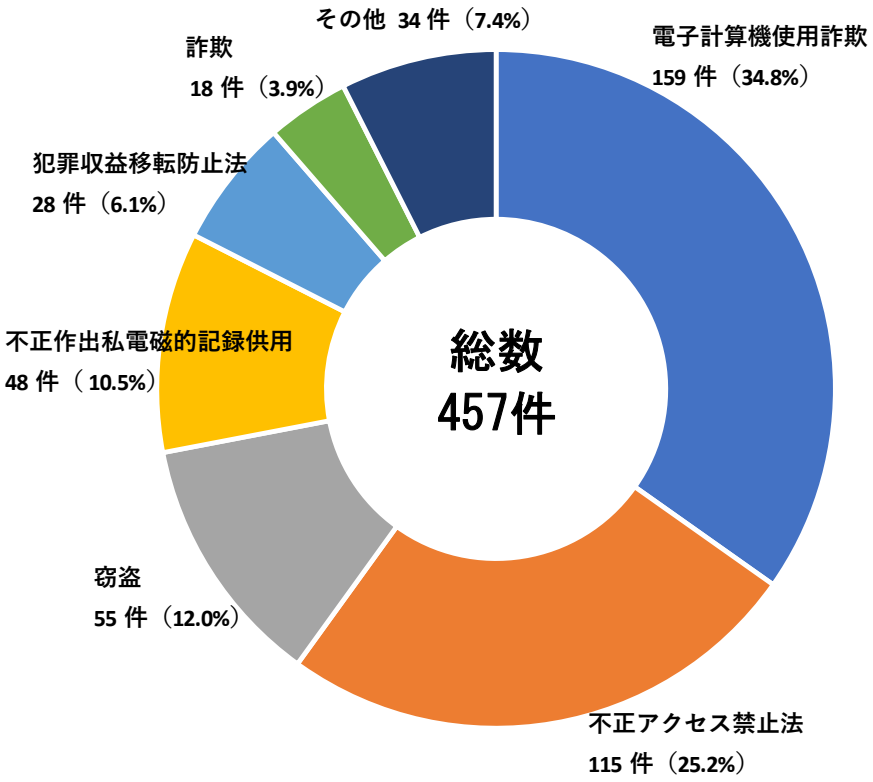
*1　サイバー犯罪とは、不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪、その他犯罪の実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪。

*2　その他の検挙状況は、サイバー犯罪の検挙状況から不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪の検挙を除いたもの。

参考　２

サイバー事案の検挙状況

警察法の一部を改正する法律（令和４年法律第６号）施行後の令和４年４月から６月までのサイバー事案[*1]の検挙状況



注　図中の割合は小数第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。

電子計算機使用詐欺

○　令和４年５月、不正に入手した他人名義のクレジットカード情報を宿泊予約サイトに入力して宿泊の予約をし、宿泊代金の支払いを免れた派遣社員の男（49）を、電子計算機使用詐欺で検挙した。

不正アクセス禁止法違反等

○　令和４年４月、元勤務先のサーバに不正アクセスし、保存されていたデータを消去した無職の女（31）を、不正アクセス禁止法違反及び電子計算機損壊等業務妨害で検挙した。

---

*1　サイバー事案とは、サイバーセキュリティが害されることその他情報技術を用いた不正な行為により生ずる個人の生命、身体及び財産並びに公共の安全と秩序を害し、又は害するおそれのある事案をいう。