広　報　資　料
令和５年３月16日
警　　察　　庁

令和４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　概要

サイバー空間は、全国民が参加し、重要な社会経済活動が営まれる公共空間へと変貌を遂げ、実空間とサイバー空間が融合した社会の到来が現実となりつつある。本資料は、令和４年中におけるサイバー空間の脅威の情勢を示す指標、事例等を紹介するものである。

２　情勢概況

ランサムウェアの感染被害が拡大するとともに、我が国の暗号資産関連事業者、学術関係者等を標的としたサイバー攻撃が明らかになり、また、インターネットバンキングに係る不正送金被害が下半期に急増するなど、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。

３　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が拡大する中、サプライチェーン全体の事業活動や地域の医療提供体制に影響を及ぼす事例が確認された。

○　政府機関や国内企業等の運営するウェブサイトが一時閲覧不能になる事案が発生し、親ロシアのハッカーが犯行をほのめかす声明を発表した。

○　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で推移している。

４　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。

○　北朝鮮当局の下部組織「ラザルス」によるものとみられるサイバー攻撃に対し、金融庁及び内閣サイバーセキュリティセンター（ＮＩＳＣ）と連名で注意喚起を実施した。

○　国内の学術関係者、シンクタンク研究員等に対して、一定の共通する手口で不正プログラムを実行させ、情報窃取を試みるサイバー攻撃が多数確認されたことを受け、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案の急増を受け、金融庁と連携し、一般社団法人全国銀行協会等に対して、フィッシング対策の強化を要請した。

別　添

令和４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

サイバー空間は、地域や老若男女を問わず、全国民が参加し、重要な社会経済活動が営まれる公共空間へと変貌を遂げ、金融、航空、鉄道、医療等といった国民生活や社会経済活動を支える基盤となる機能から、警察や防衛といった治安や安全保障に関わる国家機能に至るまで、あらゆる場面で実空間とサイバー空間が融合した社会の到来が現実となりつつある。

他方で、政治、経済、軍事及び技術をめぐる国家間の競争の顕在化を含む国際社会の変化、情報通信技術の進歩や、複雑な社会経済活動の相互依存関係の深化が進むなど、サイバー空間を取り巻く不確実性は絶えず、変容し、増大している。

こうした中、国内において被害が拡大を続けるランサムウェアの感染被害では、サプライチェーン全体の事業活動や地域の医療提供体制に影響を及ぼす事例が確認されるとともに、我が国の暗号資産関連事業者を標的としたサイバー攻撃や、学術関係者・シンクタンク研究員等を標的としたサイバー攻撃が明らかになり、また、フィッシング報告件数が増加する中でインターネットバンキングに係る不正送金被害が一時的に急増するなど、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４年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230件（前年比で57.5％増加）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び、国内の自動車関連企業では生産・販売活動等の停止等を余儀なくされ、医療機関においては、電子カルテシステムに障害が発生し、手術の延期や外来診療及び救急外来の受け入れが一時停止するなど、これら社会インフラの機能の停止や低下により、国民生活及び社会経済活動に多大な影響が生じた。加えて、その感染経路に着目すると、過去に報告されたＶＰＮ機器のぜい弱性等がランサムウェアの感染経路となる事例が依然として多くを占めており、ひとたび感染すると、被害は当該組織に限られないことから、サプライチェーンに関わる事業者へ感染が拡大する事例も確認された。また、感染したシステム等の復旧までに２か月以上を要した事例や、調査・復旧のために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。

警察庁では、こうした情勢を受け、政府機関や重要インフラ事業者のみならず、広く産業界において適切なサイバーセキュリティ対策が講じられるよう、累次にわたり関係府省庁と連携して注意喚起を実施したほか、都道府県警察では、商工会・商工会議所等の経済団体等との連携を推進し、手口の情報共有や注意喚起を実施した。

我が国の特定の事業者や学術関係者等を標的としたサイバー攻撃も発生している。北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループ

が用いる手口と同様のサイバー攻撃が、我が国の暗号資産交換業者に対してもなされており、数年来、我が国の関係事業者もこのサイバー攻撃グループによるサイバー攻撃の標的となっていることが強く推察される状況となった。また、近年、国内の学術関係者、シンクタンク研究員等に対して、一定の共通する手口で不正プログラムを実行させ、情報窃取を試みるサイバー攻撃が多数確認された。こうしたサイバー攻撃に関して、警察庁では、関係省庁と連携して、サイバー攻撃の具体的な手口等を公表し、注意喚起を実施した。

また、ウクライナ情勢をはじめ、国際情勢が緊迫する中で、海外の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後を絶たず、これらの攻撃には国家を背景とするサイバー攻撃グループの関与が疑われるものがみられる。国内においては、「e-Gov」等の政府機関等が運営する複数のウェブサイトが一時的に閲覧できなくなる事案が発生し、時期を同じくして、「Killnet」等の親ロシア派のハッカー集団が犯行をほのめかす声明を発表していることが確認された。

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たが、令和４年下半期に急増し、令和４年は発生件数が1,136件、被害総額は約15億円と、いずれも３年ぶりに前年比増加となった（それぞれ前年比で94.5％、85.2％増加）。その被害の多くがフィッシングによるものとみられており、金融機関を装ったフィッシングサイトへ誘導する電子メールが多数確認されている。また、フィッシング対策協議会によれば、令和４年中のフィッシング報告件数は96万8,832件（前年比で84.0％増加）と、右肩上がりで増加している。

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、１日１ＩＰアドレス当たり7,707.9件と、継続して高水準で推移している。これらのアクセスのほとんどが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。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月に新設した警察庁サイバー警察局及び関東管区警察局サイバー特別捜査隊が中心となり、国内外の多様な主体と協力しつつ、警察庁と都道府県警察とが一体となった捜査・実態解明に取り組むとともに、関係省庁、民間事業者等と連携した効果的な被害防止対策を推進し、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るところである。

1　令和４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（金銭又は暗号資産）を要求する不正プログラムである。

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」などと対価を要求する二重恐喝（ダブルエクストーション）の手口が多くを占める。

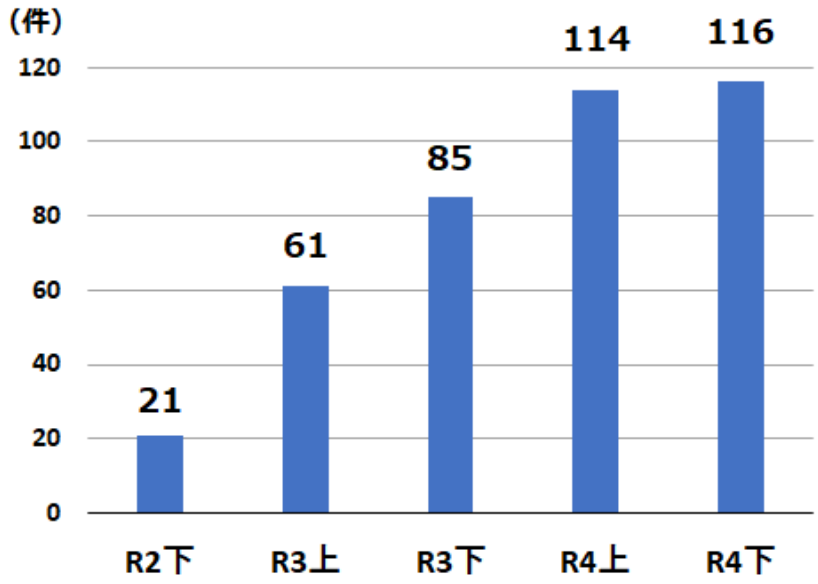
また、感染経路は、令和３年に引き続き、インターネットに公開されたＶＰＮ機器等のぜい弱性や強度の弱い認証情報等を悪用し、組織のネットワークに侵入した上でランサムウェアに感染させる手口が多くみられた。

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年に都道府県警察から警察庁に報告のあった件数は230件であり、令和２年下半期以降、右肩上がりでの増加となった。

【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

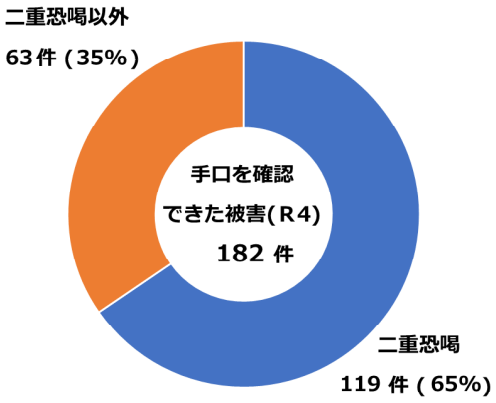
被害（230件）のうち、警察として手口を確認できたものは182件あり、このうち、二重恐喝の手口によるものは119件で65％を占めた。

○　暗号資産による対価の要求が多くを占める

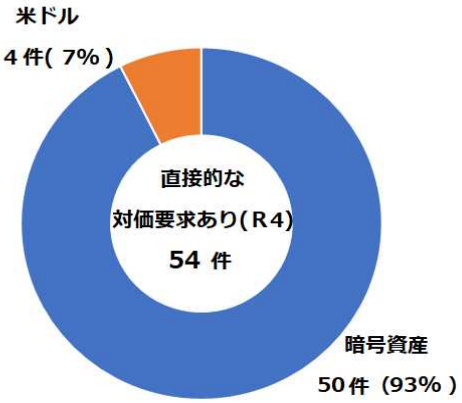
被害（230件）のうち、直接的な対価の要求を確認できたものは54件

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50件で93％を占めた。

【図表２：ランサムウェア被害の手口別報告件数】



【図表３：要求された対価支払い方法別報告件数】

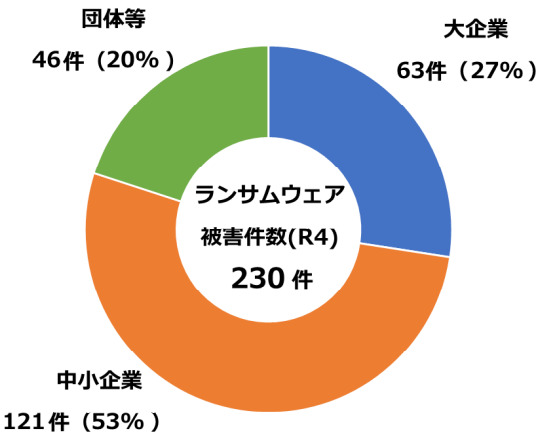


(ｳ)　被害企業・団体等の規模

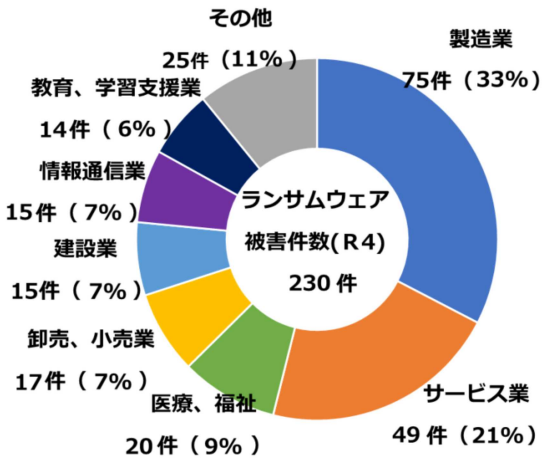
被害（230件）の内訳を企業・団体等の規模別[*1]にみると、大企業は63件、中小企業は121件であり、その規模を問わず、被害が発生した。

また、業種別[*2]にみると、製造業は75件、サービス業は49件、医療、福祉は20件となるほか、その業種を問わず、被害が発生した。

【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】



【図表５：ランサムウェア被害の企業・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。

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（230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、140

---

*1　中小企業基本法第２条第１項に基づき分類

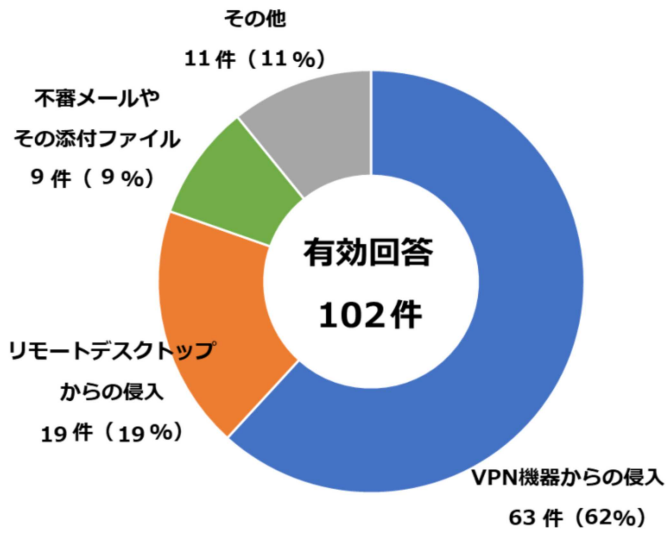
*2　日本標準産業分類に基づき分類

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)　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、102件の有効な回答があり、このうち、ＶＰＮ機器からの侵入が63件で62%、リモートデスクトップからの侵入が19件で19%を占め、テレワーク等に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81%と大半を占めた。

【図表６：感染経路】



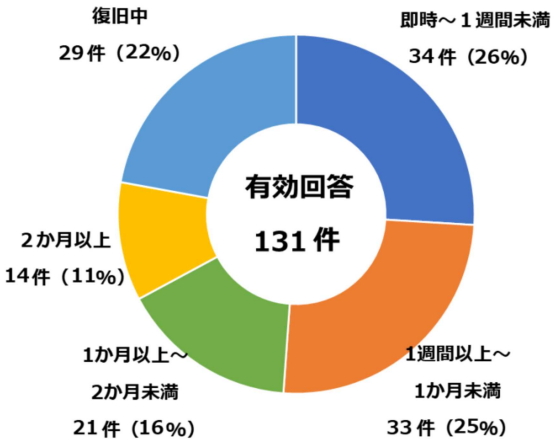
注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100にならない。

(ｲ)　復旧等に要した期間・費用

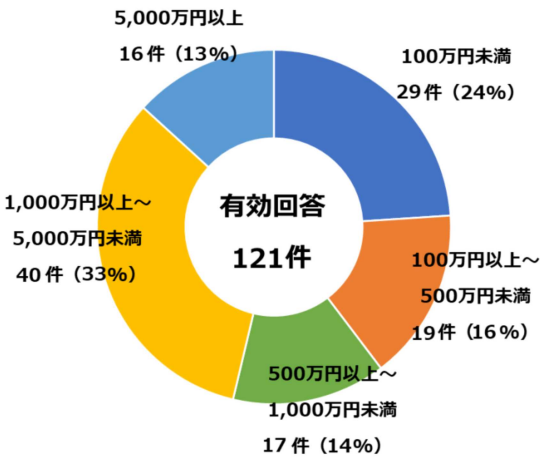
復旧に要した期間について質問したところ、131件の有効な回答があり、このうち、復旧までに１か月以上を要したものが35件あった。

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、121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56件で46%を占めた。

【図表７：復旧に要した期間】



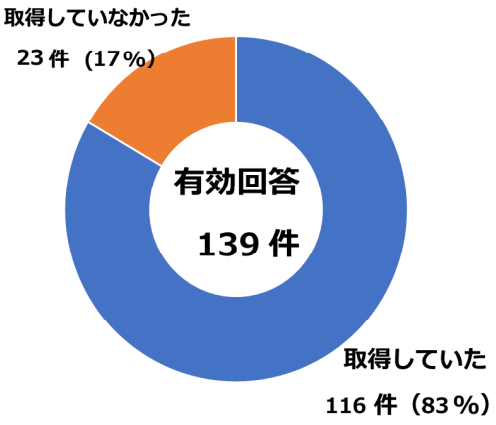
【図表８：調査・復旧費用の総額】



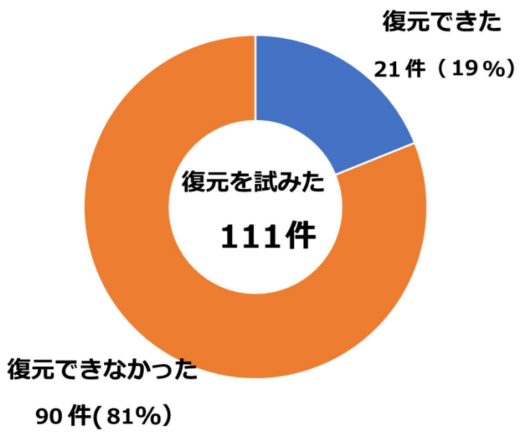
(ｳ)　バックアップの取得・活用状況

被害に遭ったシステム又は機器のバックアップの取得状況について質問したところ、139件の有効な回答があり、このうち、取得していたものが116件で83％を占めた。また、取得していたバックアップから復元を試みた111件の回答のうち、バックアップから被害直前の水準まで復旧出来なかったものは90件で81％であった。

【図表９：バックアップ取得の有無】



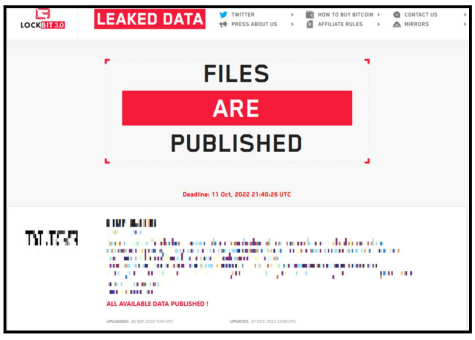
【図表10：バックアップからの復元結果】

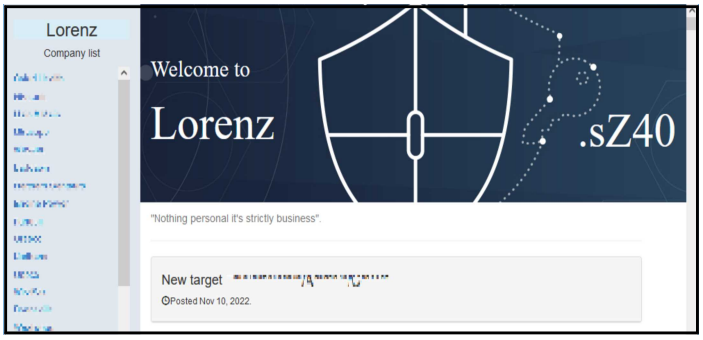


エ　ランサムウェアと関連するリークサイトの状況

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、製品に関する情報、ユーザーＩＤ、パスワード等が含まれていた。

【図表11：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会員である事業者

や、多数の病院等が加入する医療団体との連携を推進し、手口の情報共有や注意喚起を実施した。

　このほか、テレビ、ラジオ、ウェブサイト、セキュリティセミナー等の様々な媒体・機会を活用するほか、各都道府県警察が関係機関・団体等と構築する協議会等を通じた情報発信を行うなど積極的な広報啓発を実施した。

○　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、累次にわたり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12：ＮＩＳＣ、関係省庁との連名による注意喚起文書】

令和４年 12 月 20 日
経済産業省
総務省
警察庁
内閣官房内閣サイバーセキュリティセンター

年末年始休暇において実施いただきたい対策について（注意喚起）

サイバー攻撃被害のリスクの高まりを踏まえ、本年８月には、関係府省庁の連名にて「夏季の長期休暇において実施いただきたい対策について（注意喚起）」を発出しましたが、その後も、ランサムウェアによるサイバー攻撃被害が国内外の様々な企業・団体等で続き、国民生活に影響が出る事例も発生しました。また、エモテットと呼ばれるマルウェアへの感染を狙う攻撃メールについては、本年１１月に活動再開とその新たな手口（【参考】内※１，２，３を参照）を確認しており、感染や被害の拡大が懸念される状況にあります。

さらに、本年９月には、日本の政府機関や企業のホームページ等を標的としたDDoS攻撃と思われるサービス不能攻撃により、業務継続に影響のある事案も発生したほか、国家等が背景にあると考えられる攻撃者による暗号資産取引事業者等を狙ったサイバー攻撃や、一定の集団によるものとみられる学術関係者等を標的としたサイバー攻撃も明らかとなり、国民の誰もがサイバー攻撃の懸念に直面することとなっています。

このように依然として厳しい情勢の下での長期休暇においては、休暇中の隙を突いたセキュリティインシデント発生の懸念が高まるとともに、長期休暇後に電子メールの確認の量が増えることで偽装のチェックなどがおろそかになるといった感染リスクの高まりが予想されます。さらに、長期休暇中は、通常と異なる体制等により、対応に遅延が生じたり、予期しない事象が生じたりすることが懸念されます。

こうした長期休暇がサイバーセキュリティに与えるリスクを考慮し、別紙の対策を参考に、適切な管理策によるサイバーセキュリティの確保について、サプライチェーンも含めてご検討をお願いいたします。

あわせて、不審な動き等を検知した場合は、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ご連絡いただくとともに、警察にもご相談ください。

(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。

○　複数のウェブサイトの閲覧障害

９月、「e-Gov」等の政府機関や国内企業等の運営するウェブサイトが一時閲覧不能になる事案が発生し、時期を同じくして、親ロシアのハッカー集団とされる「Killnet」等が犯行をほのめかす声明を発表したことが確認された。

「Killnet」は、ロシアによるウクライナ侵略等に対する我が国の対応に反対する旨の声明を発表したものの、ロシア政府との関係については否定した。

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年中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年中においても、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。令和４年中では、596回の共同対処訓練を行った。

○　ラザルスと呼称されるサイバー攻撃グループに関する注意喚起の実施

北朝鮮当局の下部組織とされる「ラザルス」と呼称されるサイバー攻撃グループが、数年来、国内の暗号資産関係事業者を標的としたサイバー攻撃を行っていると強く推察される状況にあることが、関係都道府県警察やサイバー特別捜査隊の捜査等によって判明した。

「ラザルス」によるものとみられる暗号資産の窃取を目的としたサイバー攻撃は今後も継続されると考えられるところ、最近は暗号資産取引の多様化により、暗号資産取引が事業者だけでなく、個人間でも行われているため、個人も標的とされるおそれがある。こうしたことから、暗号資産取引に関わる個人や事業者がこうした組織的なサイバー攻撃が行われているという認識を持ち、サイバーセキュリティの強化に取り組むよう、警察庁は令和４年10月14日、金融庁及びＮＩＳＣとの連名で注意喚起を発表した。

【図表13：注意喚起の一部】

令和4年 10 月 14 日
金　　融　　庁
警　　察　　庁
内閣サイバーセキュリティセンター

北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループによる暗号資産関連事業者等を標的としたサイバー攻撃について（注意喚起）

北朝鮮当局の下部組織とされる、ラザルスと呼称されるサイバー攻撃グループについては、国連安全保障理事会北朝鮮制裁委員会専門家パネルが本年 10 月7日に公表した安全保障理事会決議に基づく対北朝鮮措置に関する中間報告書が、ラザルスと呼称されるものを含む北朝鮮のサイバー攻撃グループが、引き続き暗号資産関連企業及び取引所等を標的にしていると指摘しているところです。また、米国では本年4月 18 日、連邦捜査局（FBI）、サイバーセキュリティ・インフラセキュリティ庁（CISA）及び財務省の連名で、ラザルスと呼称されるサイバー攻撃グループの手口や対応策等の公表を行うなど、これまでに累次の注意喚起が行われている状況にあります。同様の攻撃が我が国の暗号資産交換業者に対してもなされており、数年来、我が国の関係事業者もこのサイバー攻撃グループによるサイバー攻撃の標的となっていることが強く推察される状況にあります。

このサイバー攻撃グループは、

- 標的企業の幹部を装ったフィッシング・メールを従業員に送る
- 虚偽のアカウントを用いた SNS を通じて、取引を装って標的企業の従業員に接近する

などにより、マルウェアをダウンロードさせ、そのマルウェアを足がかりにして被害者のネットワークへアクセスする、いわゆるソーシャルエンジニアリングを手口として使うことが確認されています。その他様々な手段を利用して標的に関連するコンピュータネットワークを侵害し、暗号資産の不正な窃取に関与してきているとされ、今後もこのような暗号資産の窃取を目的としたサイバー攻撃を継続するものと考えられます。

○　学術関係者・シンクタンク研究員等を標的としたサイバー攻撃に対する注意喚起

近年、日本国内の学術関係者、シンクタンク研究員等に対し、講演依頼や取材依頼等を装ったメールをやりとりする中で不正なプログラムを実行させ、当該人物のメールやコンピュータ内のファイルの内容を盗み見るサイバー攻撃が多数確認されている。

こうしたサイバー攻撃のうち、一定の共通点を有する事案を確認し、情報窃取被害の発生が深く懸念されることに鑑み、11月30日にＮＩＳＣと連名で広く手口を公表し、注意喚起を行った。

【図表14：注意喚起の一部】

令和4年 11 月 30 日
警察庁サイバー警察局
内閣サイバーセキュリティセンター

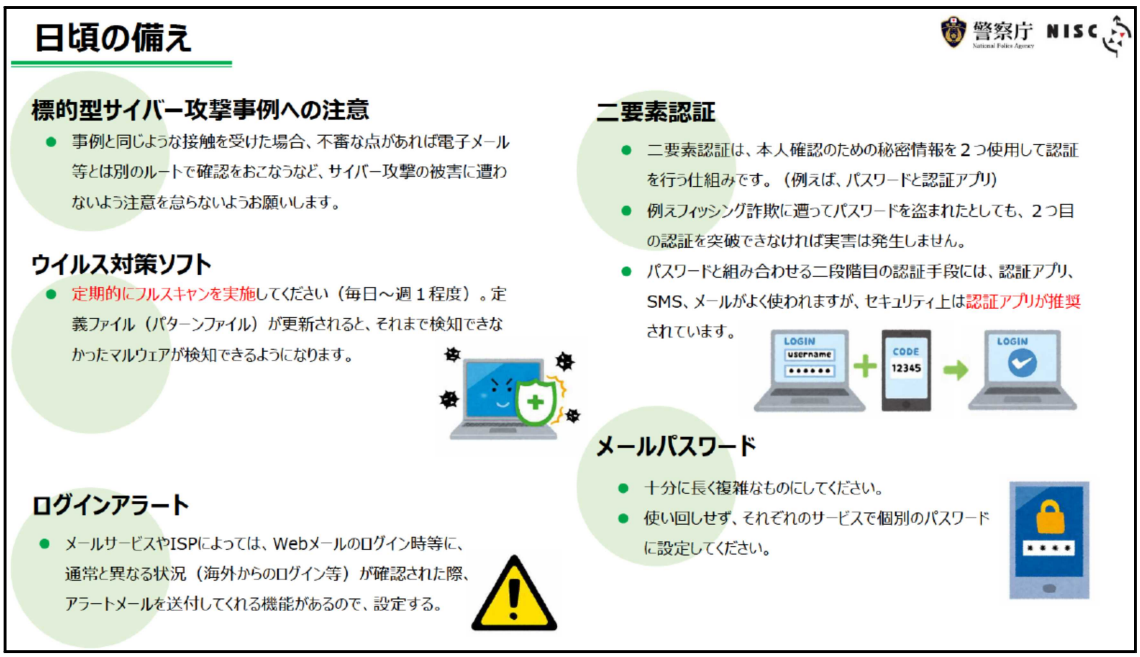
学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について（注意喚起）

近年、日本国内の学術関係者、シンクタンク研究員、報道関係者等に対し、講演依頼や取材依頼等を装ったメールをやりとりする中で不正なプログラム(マルウェア)を実行させ、当該人物のやりとりするメールやコンピュータ内のファイルの内容の窃取を試みるサイバー攻撃が多数確認されています。

このサイバー攻撃に共通する特徴は以下のとおりです。

（1） 手口

- 実在する組織の社員・職員をかたり、イベントの講師、講演、取材等の依頼メールや資料・原稿等の紹介メールが送られてくる。
- 日程や内容の調整に関するやりとりのメールの中で、資料や依頼内容と称したURLリンクが本文に記載されたり、資料・原稿等という名目のファイルが添付されたりする。当該URLをクリックしたり添付ファイルを開いたりすると、マルウェアに感染する。



○　Emotetの注意喚起の実施

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４年７月中旬頃から活動を停止していたが、令和４年11月、警察庁において、添付ファイルを指定されたフォルダにコピーするよう指示を行い、マクロを実行可能とさせEmotetに感染させるメールを複数確認するなど、国内において活動が再開したとみられる事象を確認した。これを受けて、警察庁ウェブサイトにおいて注意喚起を実施した。

【図表15：Emotetの活動再開に関する注意喚起】

令和４年11月４日
警　　察　　庁

マルウェアEmotetの活動再開に関する注意喚起について

マルウェアEmotetは、令和４年７月中旬頃から活動を停止していましたが、今般、警察庁では、Emotetメールを複数確認するなど、国内において活動が再開したとみられる事象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。

今回の手口では、添付ファイルを指定されたフォルダにコピーするよう指示を行い、マクロを実行可能とさせEmotetに感染させるといった特徴があります。

なお、これまで、添付ファイルのマクロを有効化した場合に、Emotetに感染させる手口や、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。

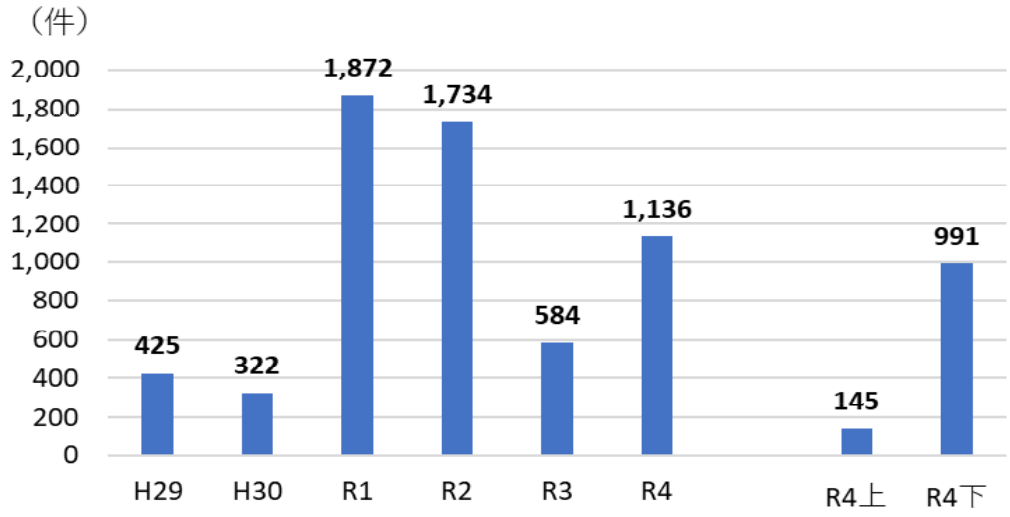
不用意にメールの添付ファイルを開かないようにするなど、マルウェアに感染しないように注意してください。

(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

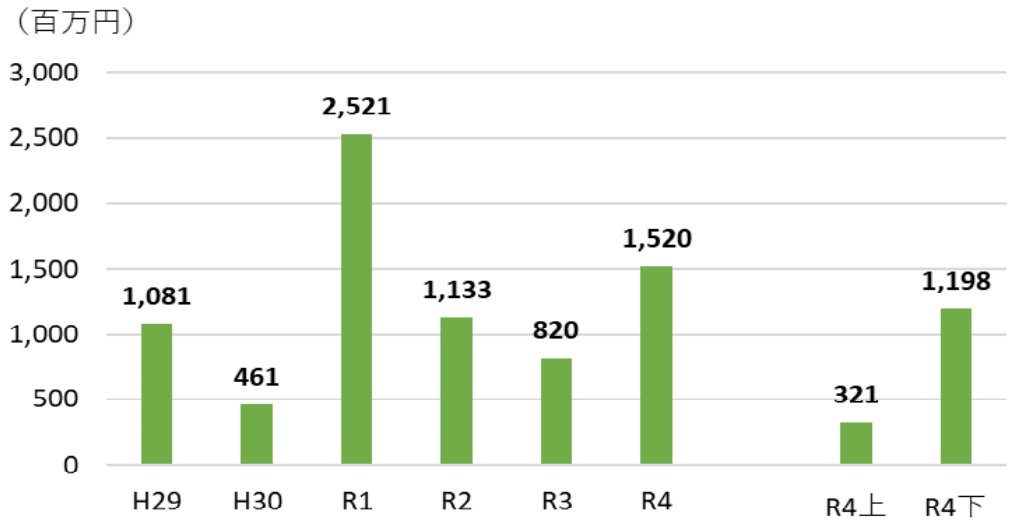
ア　インターネットバンキングに係る不正送金事犯の発生状況

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、８月下旬から９月にかけて急増し、発生件数1,136件、被害総額約15億1,950万円で、前年と比べて発生件数、被害額ともに増加した。

【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】



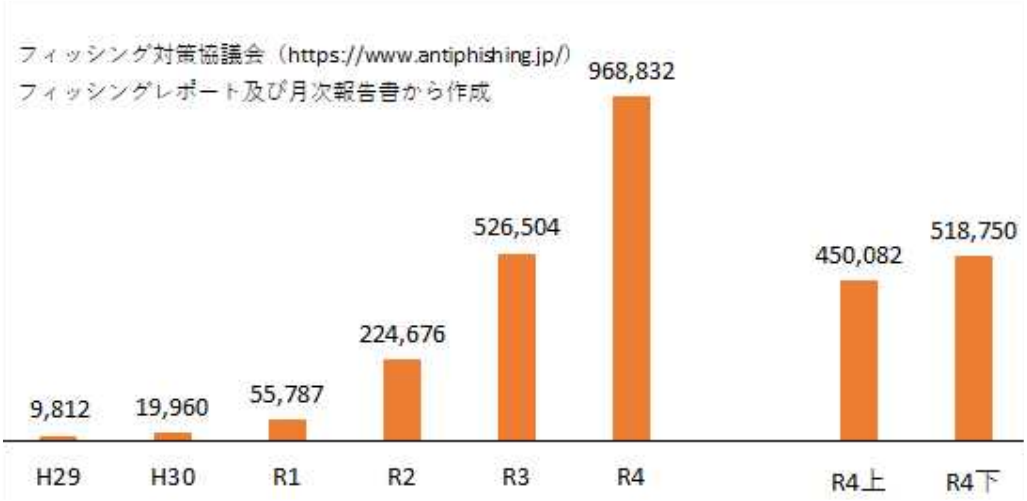
イ　フィッシング等に伴う被害の実態

令和４年８月下旬から９月にかけて急増した被害の多くはフィッシングによるものとみられ、銀行を装ったフィッシングサイト（偽のログインサイト）へ誘導するメールを多数確認した。

また、フィッシング対策協議会によれば、令和４年のフィッシング報告件数は96万8,832件（前年比＋44万2,328件）で、右肩上がりで増加となり、フ

ィッシングで騙られた企業は、クレジットカード事業者、ＥＣ事業者を装ったものが多くを占めた。

【図表18：フィッシング報告件数の推移】



ウ　警察の取組

○　金融機関等との連携強化

警察庁において、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。

○　フィッシング対策強化の要請等

令和４年８月下旬から９月にかけて、フィッシングによるものとみられるインターネットバンキングに係る不正送金被害が急増した。これを受け、警察庁において、令和４年９月に、ＪＣ３と連携し、メールやショートメッセージサービス（ＳＭＳ）に記載されたリンクからアクセスしたサイトにＩＤ・パスワード等を入力しないよう注意喚起を実施するとともに、金融庁と連携し、一般社団法人全国銀行協会等に対して、送信ドメイン認証技術（ＤＭＡＲＣ等）導入等のフィッシング対策の強化を要請した。

○　ＳＭＳを悪用したフィッシング対策

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、フィッシングサイトに誘導するＳＭＳを利用者が受信すること自体を阻止する仕組みの構築に向けた大手携帯電話事業者等による検討に参画した。その結果、大手携帯電話事業者３社において、それぞれ令和４年３月、同年６月、令和５年２月にフィッシングサイトに誘導するＳＭＳの受信を自動で拒否する機能が提供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

警察庁において、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等、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。

○　関係機関と連携した不審なＳＭＳ等に係る注意喚起の実施

令和４年８月以降、国税の納付を求める旨や、差押えの執行を予告する旨のショートメッセージやメールが多数確認されたことから、令和４年９月に、警察庁及び都道府県警察において、国税庁と連携して、フィッシングサイトの閲覧防止に関する広報啓発を実施した。

また、令和４年10月に、警察庁及び金融庁のロゴを使用したフィッシングサイトを認知したことから、それぞれのウェブサイトにおいて注意喚起を実施した。

○　ＪＣ３と連携した検挙

会社員の男（49）は、令和３年12月、宿泊予約サイトにおいて、不正に入手した他人名義のクレジットカード情報を入力して宿泊予約を行い、代金の支払いを免れて不正宿泊を行った。ＪＣ３から情報提供を受け、令和４年５月、男を電子計算機使用詐欺で検挙した。

２　サイバー空間の脅威情勢

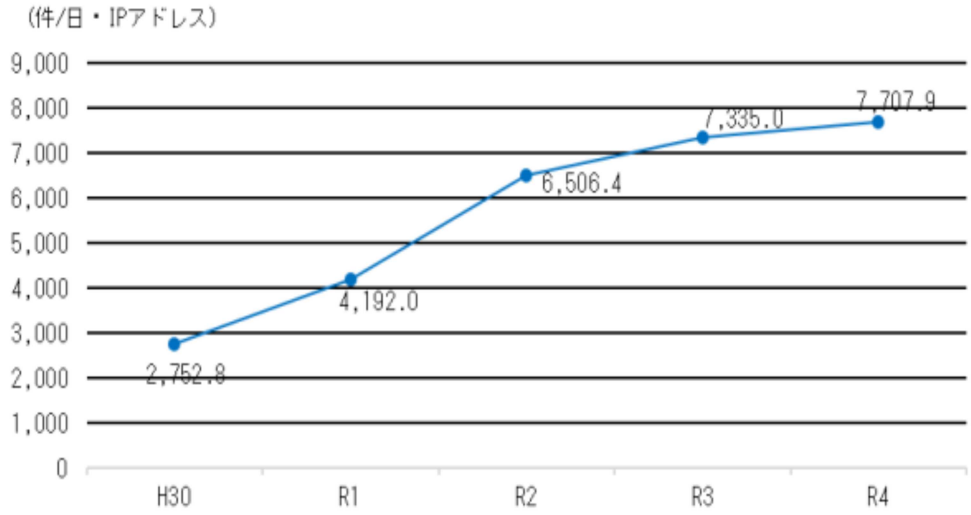
(1)　サイバー空間におけるぜい弱性探索行為等の観測状況

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7,707.9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19：センサーにおいて検知したアクセス件数の推移】

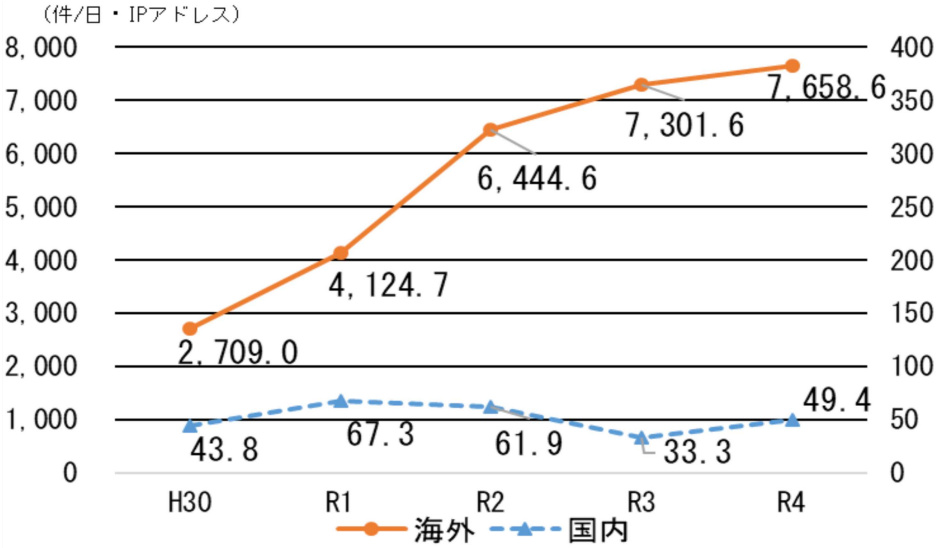


イ　特徴的な観測

○　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、海外の送信元が高い割合を占めている。

【図表20：検知したアクセスの送信元で比較した１日・１ＩＰアドレス当たりの件数の推移】

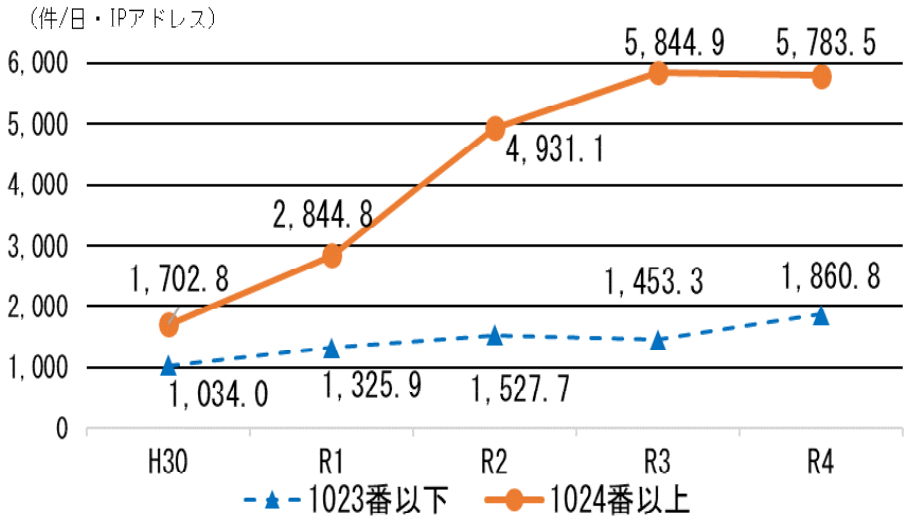


令和４年においても、国内を送信元とするアクセスが１日・１ＩＰアドレス当たり49.4件であるのに対して、海外を送信元とするアクセスが7,658.6件と大部分を占めており、海外からの脅威への対処が引き続き重要となっている。

○　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多数を占めており、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21：検知したアクセスの宛先ポートで比較した１日・１ＩＰアドレス当たりの件数の推移】

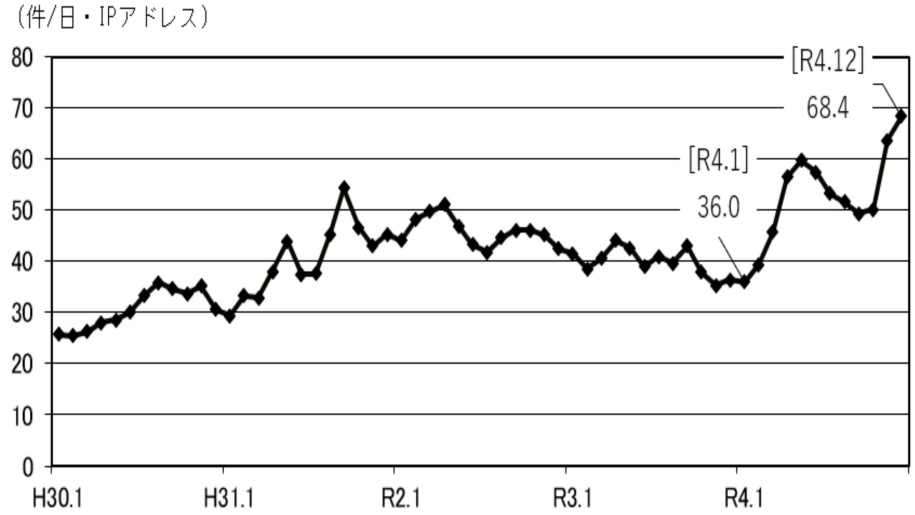


ＩｏＴ機器では標準設定として1024番以上のポート番号を使用しているものが多く、これらのアクセスの多くがぜい弱性を有するＩｏＴ機器の探索やＩｏＴ機器に対するサイバー攻撃を目的とするためのものであるとみられる。

○　リモートデスクトップサービス[*3]を対象としたアクセスの観測

平成30年から令和４年にかけて、リモートデスクトップサービスが標準で使用するポート3389/ＴＣＰに対するアクセスが、緩やかな増加傾向にある。特に令和４年の12月には、同年１月と比較しておよそ２倍のアクセスが観測された。

【図表22：リモートデスクトップサービスで使用される宛先ポート3389/ＴＣＰに対するアクセス件数の推移】



アクセスを詳細に確認すると、当該サービスの稼働状況を調べることが目的と思われるアクセスが増加しており、令和４年は過去最高の件数を観測した。そのほか、推測されやすいＩＤやパスワードが設定されていないかを確認するためのアクセスも観測されるなど、攻撃の対象となるリスクは増加している。

テレワークが社会的に浸透し、リモートデスクトップサービスを利用する機会が増えている。このサービスの利用に当たっては、一定時間内のログイン試行回数の制限等の適切な設定、推測されにくいＩＤやパスワードへの変更、多要素認証等の対策を講じることが必要である。

*3 ネットワークで接続された他のコンピュータのデスクトップ環境を操作する機能。

(2)　標的型メール攻撃

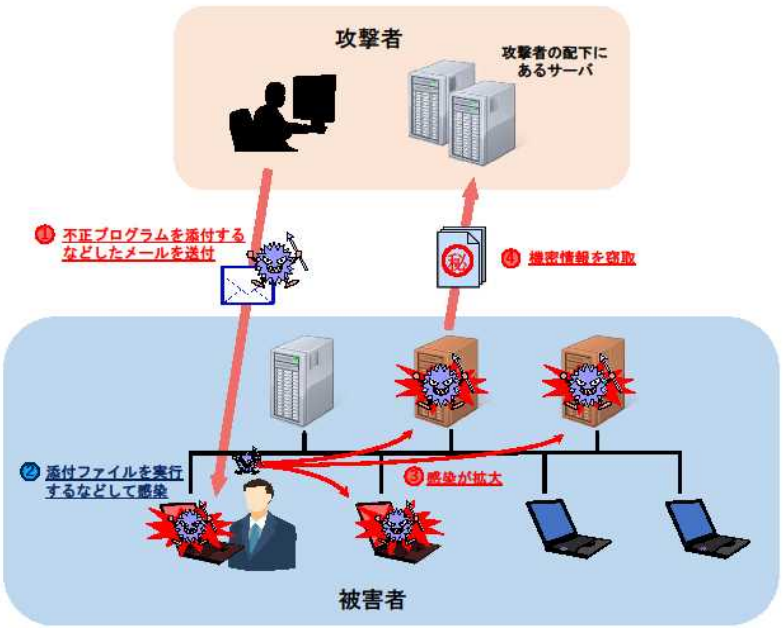
ア　傾向

令和４年中に、全国警察で把握した事例について、様々な種類の不正プログラムが標的型メールに添付されていたことが確認されている。手口としては、実在する人物になりすましてメールを送りつけ、何度かメールのやり取りを行うことで信用させ、ファイル名として興味を惹くキーワードを盛り込んだ不正プログラムのファイルを実行させるものが確認されている。

イ　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8,500の事業者等（令和４年12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23：標的型メール攻撃による情報窃取の例】



ウ　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年中においても、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た。

○　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。

○　医薬品メーカに対する攻撃

　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に送信された。

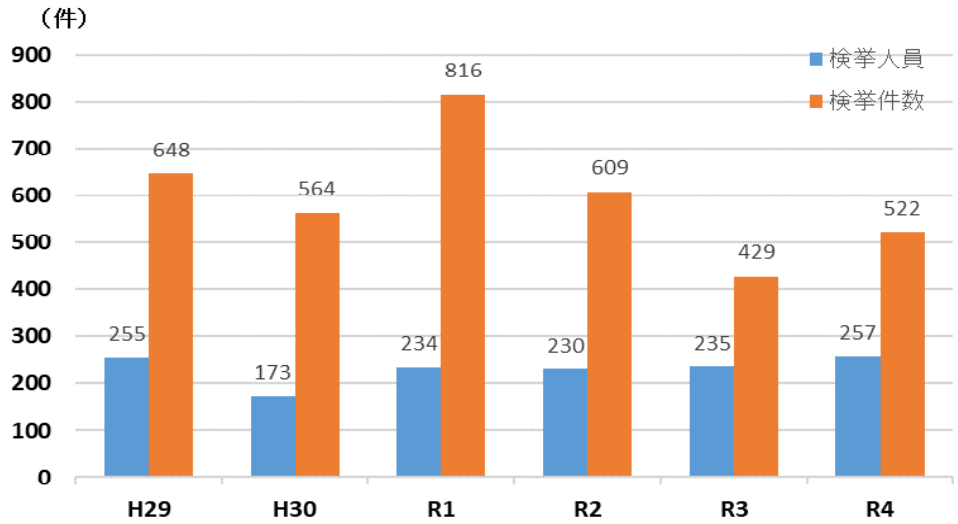
(3)　主なサイバー事案の検挙状況

ア　不正アクセス禁止法[*4]違反

(ｱ)　検挙件数

令和４年中における不正アクセス禁止法違反の検挙件数は522件と、前年同期と比べて93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、482件が識別符号窃用型[*5]で全体の92.3％を占めた

○　「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230件と最も多く、全体の47.7％を占めており、次いで「識別符号を知り得る立場にあった元従業員や知人等による犯行」が41件で全体の8.5％を占めた

○　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」が最多であった。

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233件と最

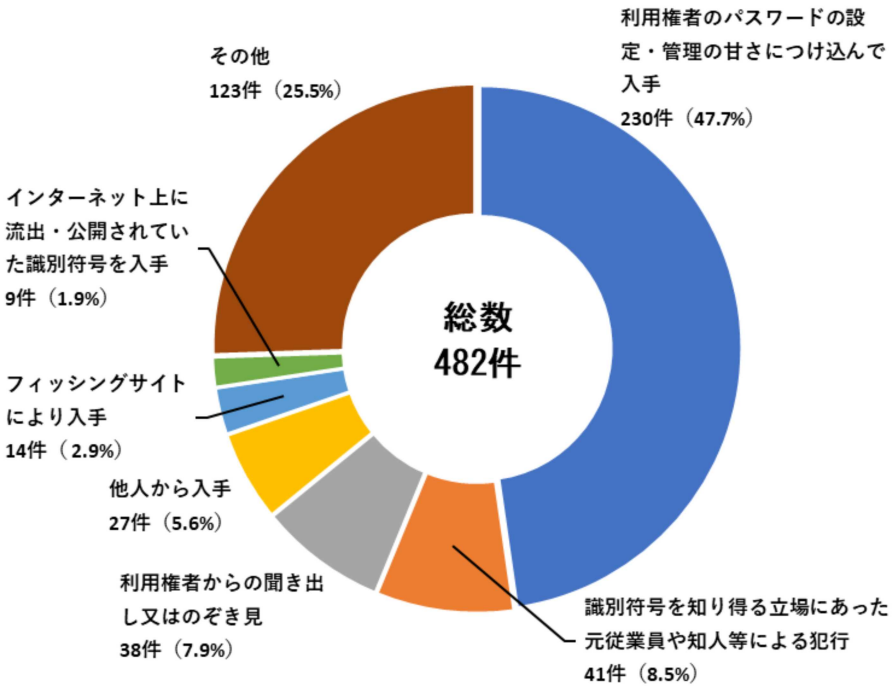
---

*4　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。）

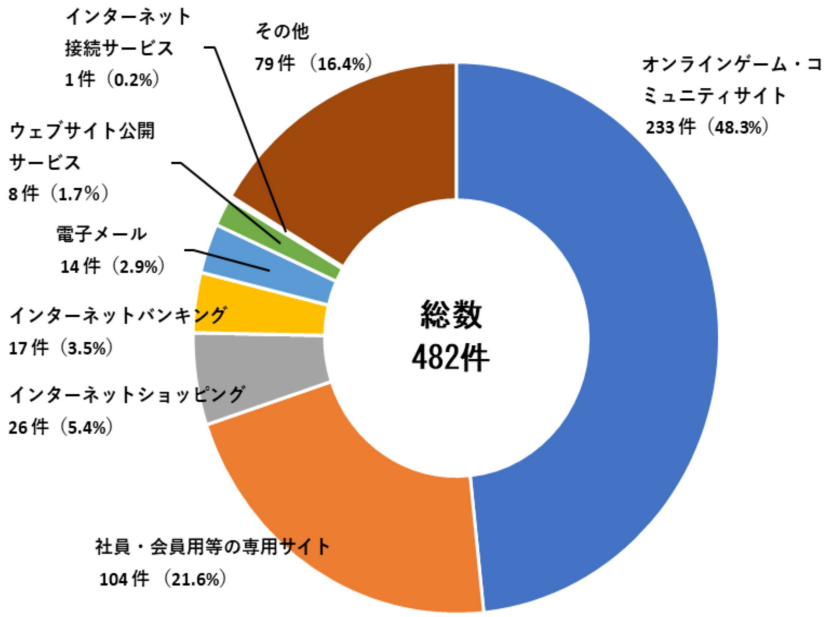
*5　不正アクセス行為は、他人の識別符号を無断で入力する「識別符号窃用型」と、アクセス制御機能による特定利用の制限を免れる情報（識別符号を除く）又は指令を入力する「セキュリティ・ホール攻撃型」に分類することができる。

も多く、全体の48.3%を占めており、次いで「社員・会員用等の専用サイト」が104件で全体の21.6%を占めた。

【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）】

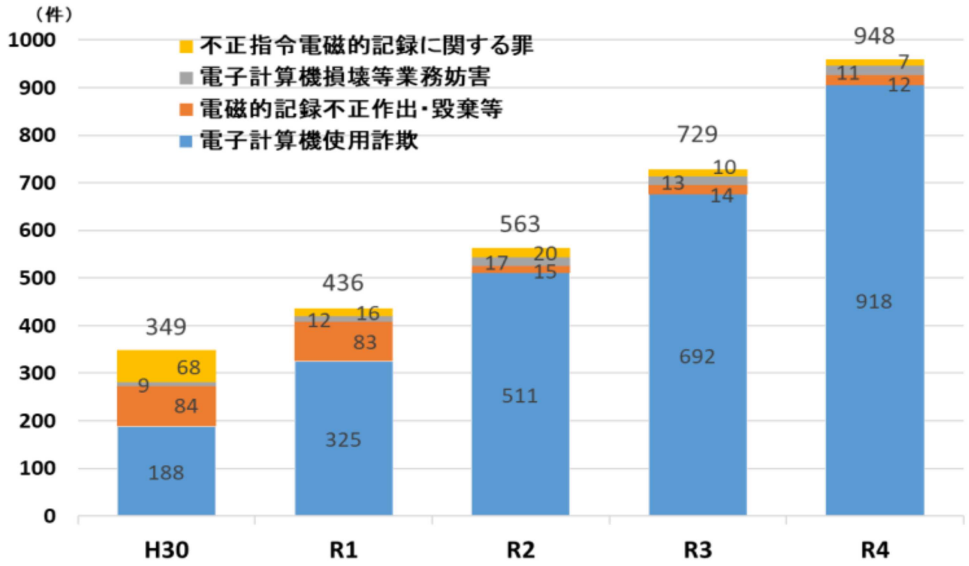


イ　コンピュータ・電磁的記録対象犯罪[*6]

(ｱ)　検挙件数

令和４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948件で、前年同期と比べて219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】



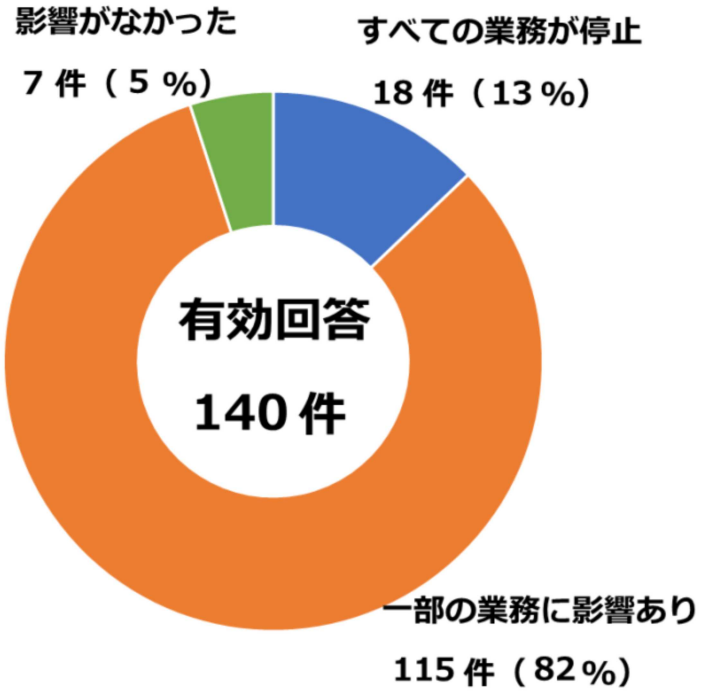
(ｲ)　特徴

検挙件数のうち、電子計算機使用詐欺が918件と最も多く、全体の96.8％を占めた。

*6　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

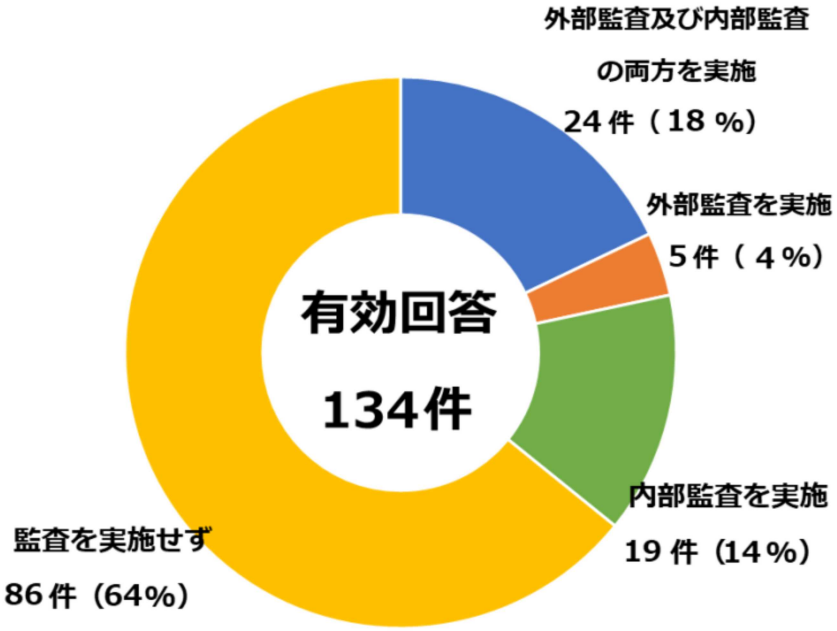
1　企業・団体等におけるランサムウェア被害及びその実態

(1)　ランサムウェア被害が業務に与えた影響



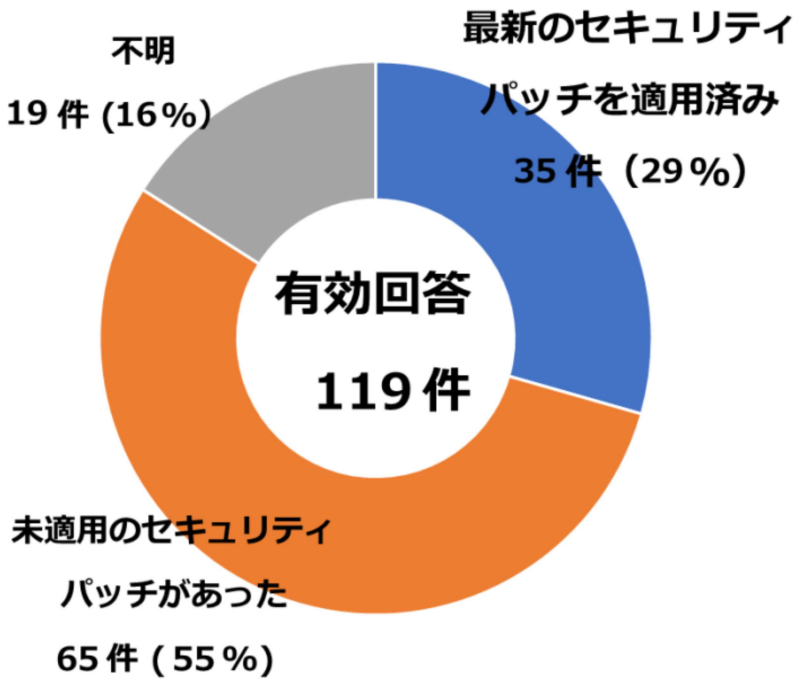
注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100にならない。

(2)　被害企業・団体等の情報セキュリティ監査の実施状況

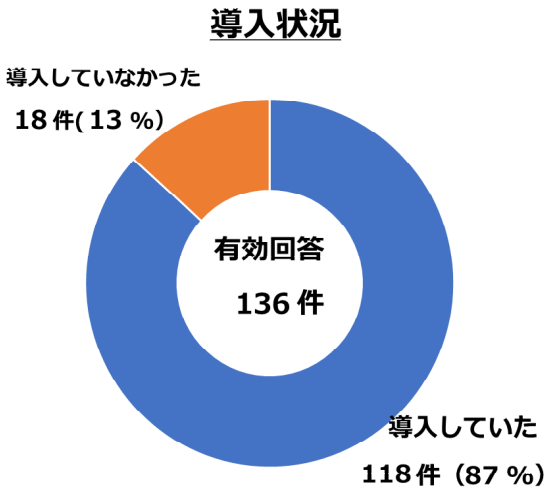


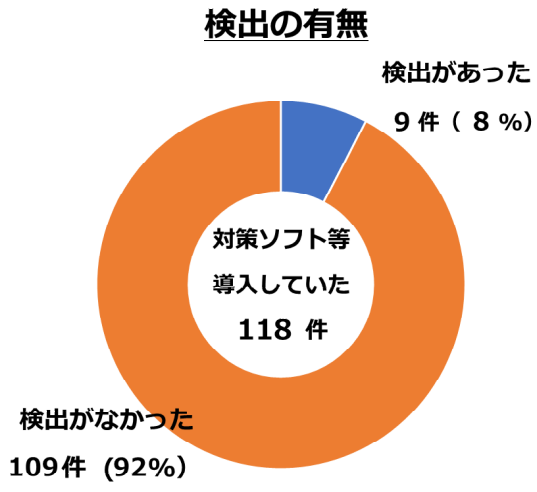
注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100にならない。

(3) 侵入経路とされる機器のセキュリティパッチの適用状況

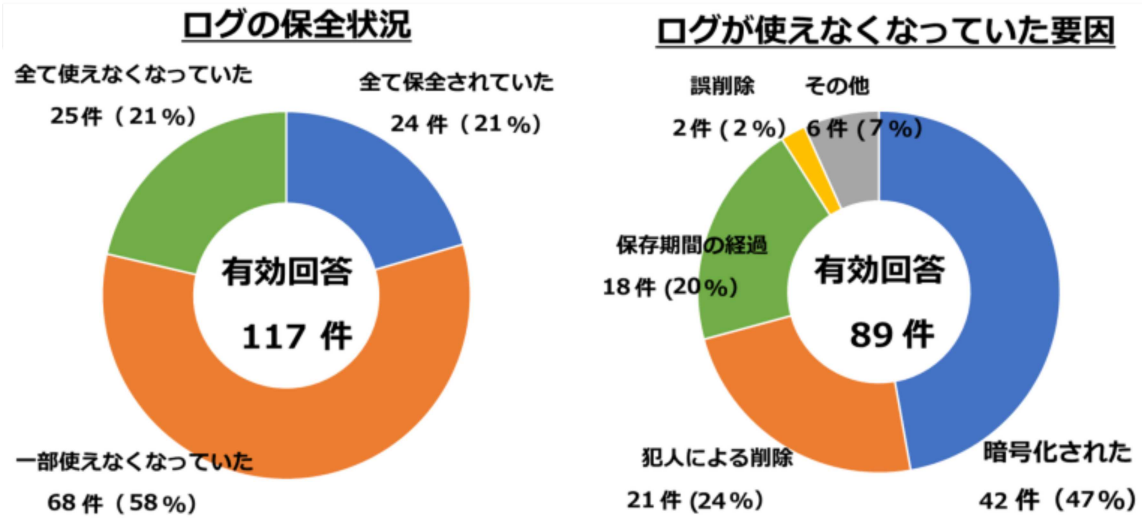


(4) 被害企業・団体等のウイルス対策ソフト等の導入・活用状況

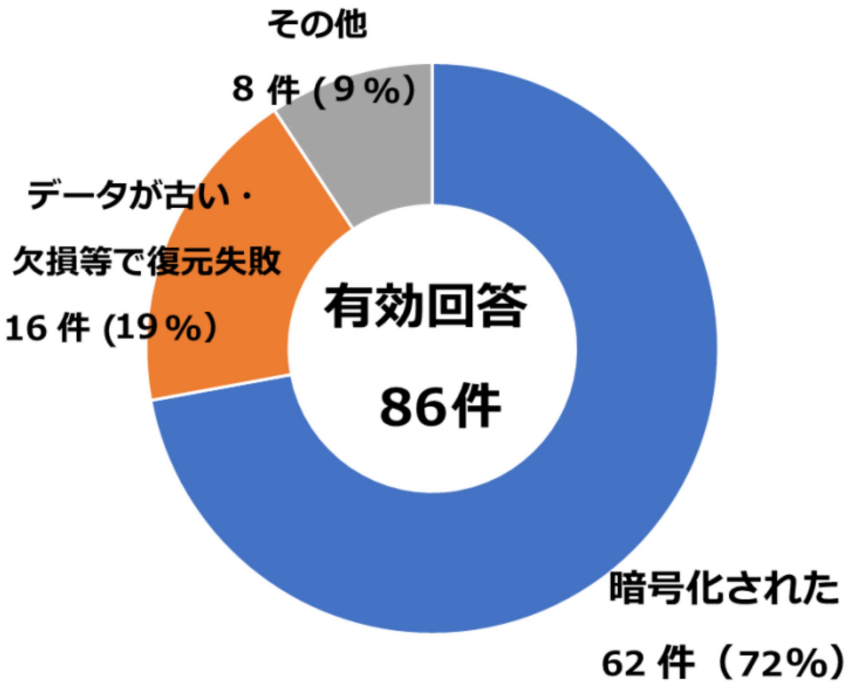




(5)　ランサムウェア被害における被害企業・団体等のログの保全状況

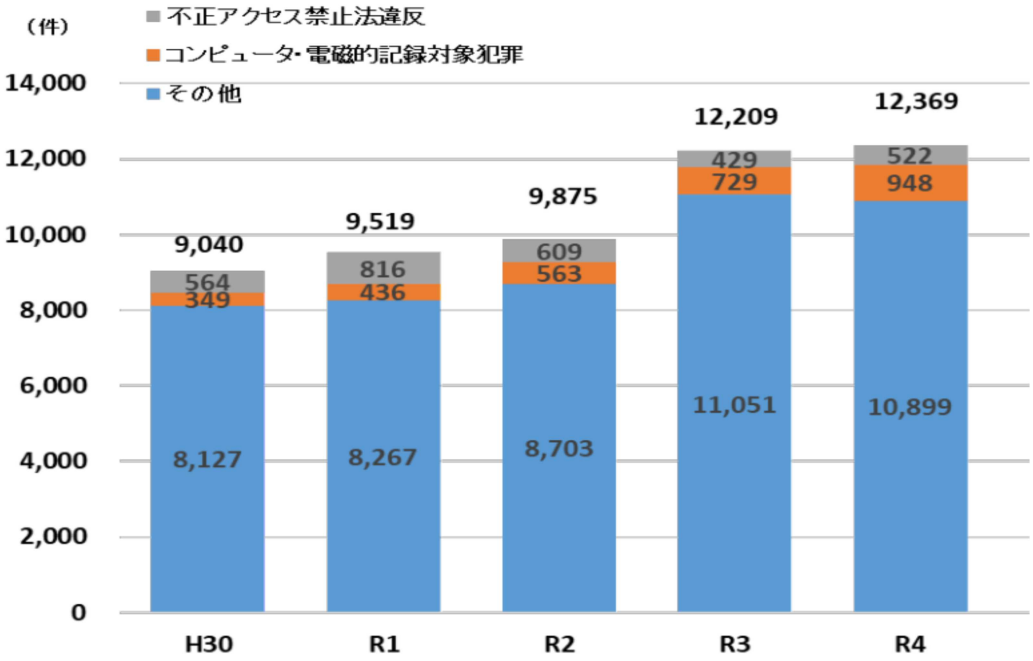


(6)　被害企業・団体のバックアップを利用して復元できなかった理由

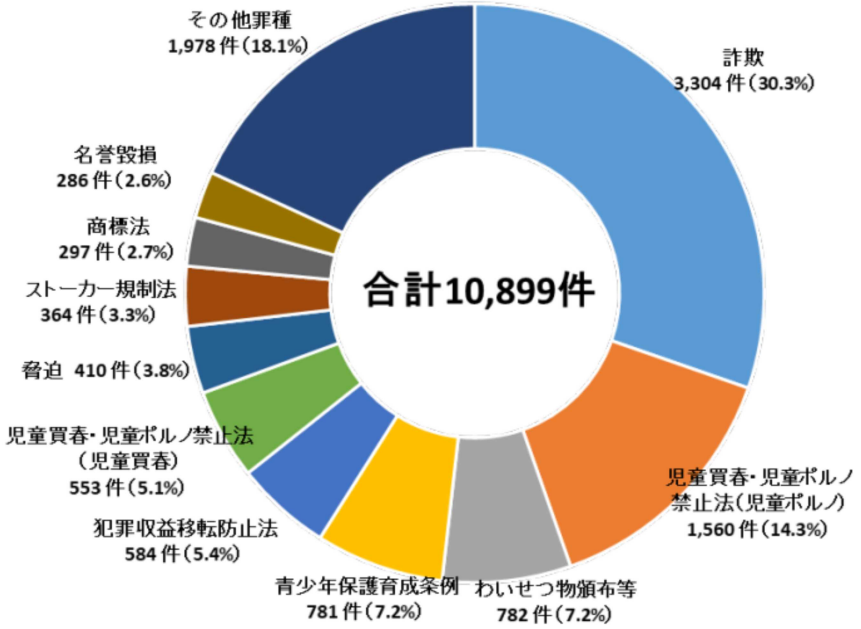


2　サイバー犯罪[*1]の検挙状況

(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]



---

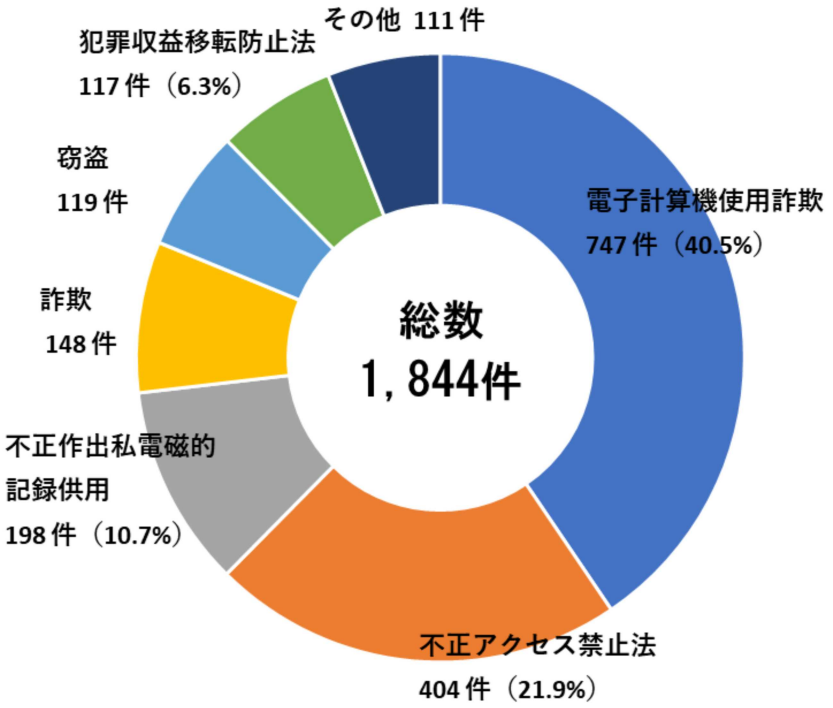
*1　サイバー犯罪とは、不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪、その他犯罪の実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪。

*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12月までのサイバー事案[*1]の検挙状況



電子計算機使用詐欺等

○　会社役員の男（29）らは、令和３年７月、架空の名義でスマートフォン決済アプリのアカウントを開設し、翌月の返済を条件に必要な金額がすぐにチャージされる同アプリの仕組みを悪用して電子マネーをだまし取った上、自身が経営する店舗で架空の商品代行決済を行った。令和４年７月、男ほか３名を電子計算機使用詐欺等で検挙した。

不正アクセス禁止法違反等

○　飲食店従業員の男（49）は、令和３年12月から令和４年１月にかけて、元勤務先である法人が管理するＶＰＮ機器に不正アクセスした上で、同法人が管理するサーバに不正アクセスし、サーバ内のアクセス権限の設定を変更した。令和４年10月、男を不正アクセス禁止法違反等で検挙した。

---

*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。