広　報　資　料
令和４年２月10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（速報版）

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年度に警察庁にサイバー警察局を設置すること等を盛り込んだ警察法改正案を国会に提出。

○　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。

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（速報版）

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12,275件（暫定値）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、右肩上がりで増加を続けており、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

---

*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）

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。

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。

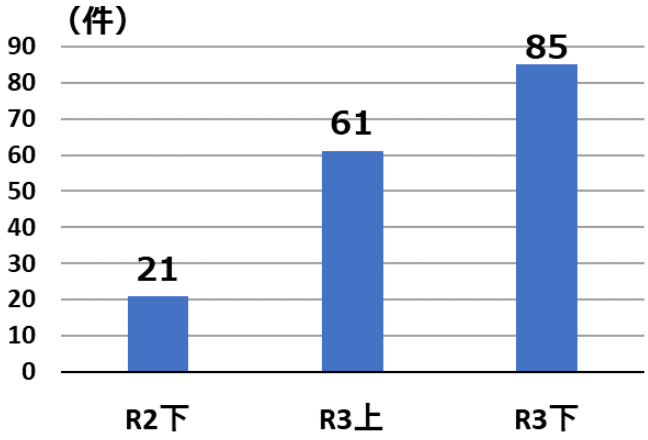
このように、引き続きサイバー空間における脅威が極めて深刻である中、サイバー事案への対処能力を強化し、諸外国と連携した脅威への対処を推進するなどの観点から、令和４年度に警察庁にサイバー警察局を設置すること等を盛り込んだ警察法の一部を改正する法律案を国会に提出した。

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。

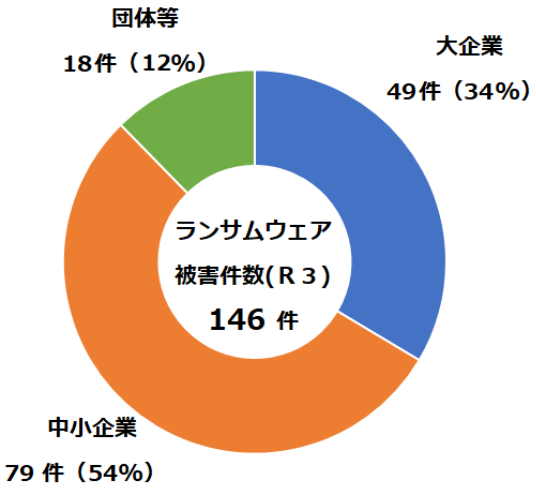
1　ランサムウェアに係る統計

(1) ランサムウェア被害の状況

【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[*2] の推移】



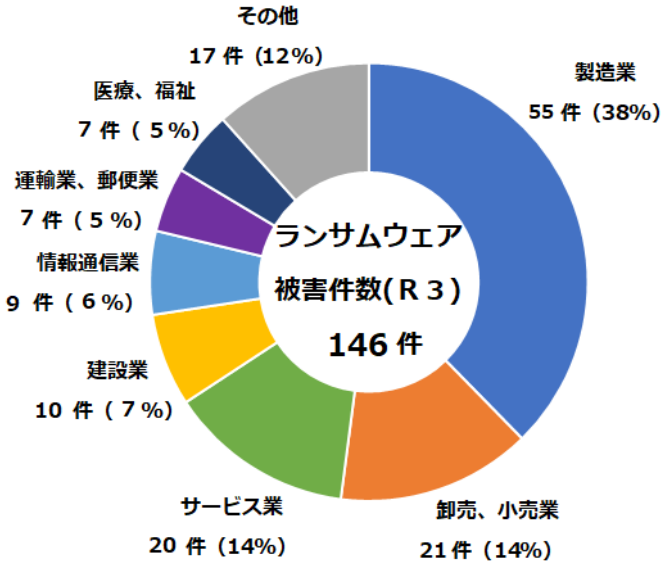
【図表２：被害企業・団体等の規模別[*3] 報告件数（令和３年）】



*2　各期間中に都道府県警察が認知したランサムウェア被害について、都道府県警察から警察庁へ報告があった件数。

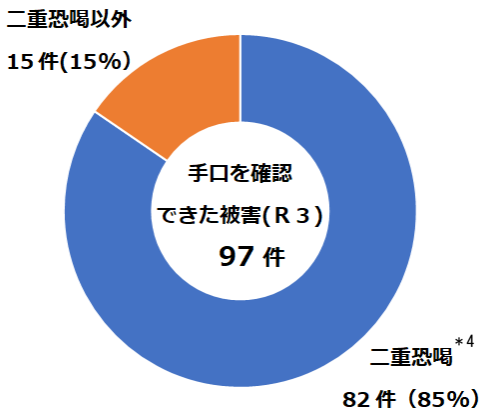
*3　中小企業基本法第２条第１項に基づき分類。

【図表３：被害企業・団体等の業種別報告件数（令和３年）】

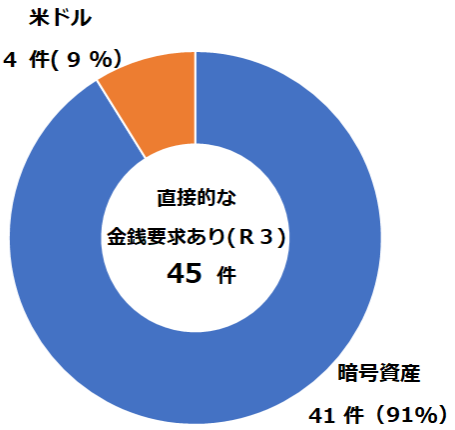


注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100にならない。

【図表４：ランサムウェアの手口別報告件数（令和３年）】



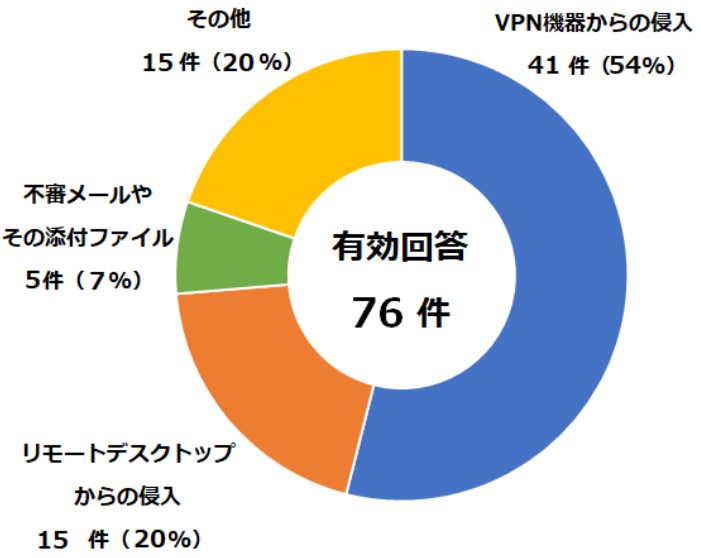
【図表５：要求された金銭支払い方法別報告件数（令和３年）】



*4　データを暗号化し、復号のための金銭を要求することに加え、データを窃取した上、「対価を支払わなければ当該データを公開する」などと更に金銭を要求する手口。

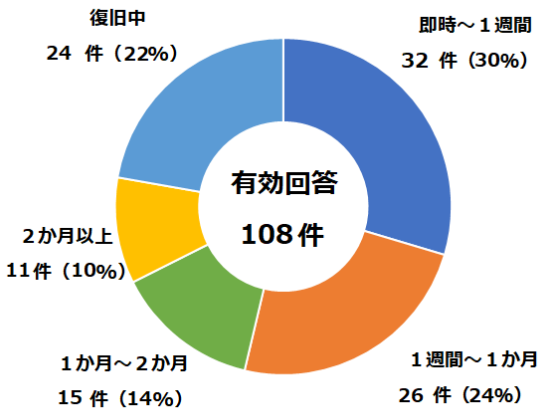
(2) 被害企業・団体等へのアンケート調査[*5] 結果

【図表６：ランサムウェアの感染経路】

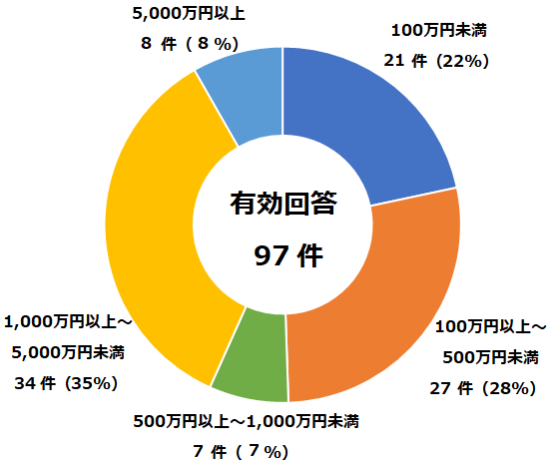


注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100にならない。

【図表７：被害からの復旧に要した期間】



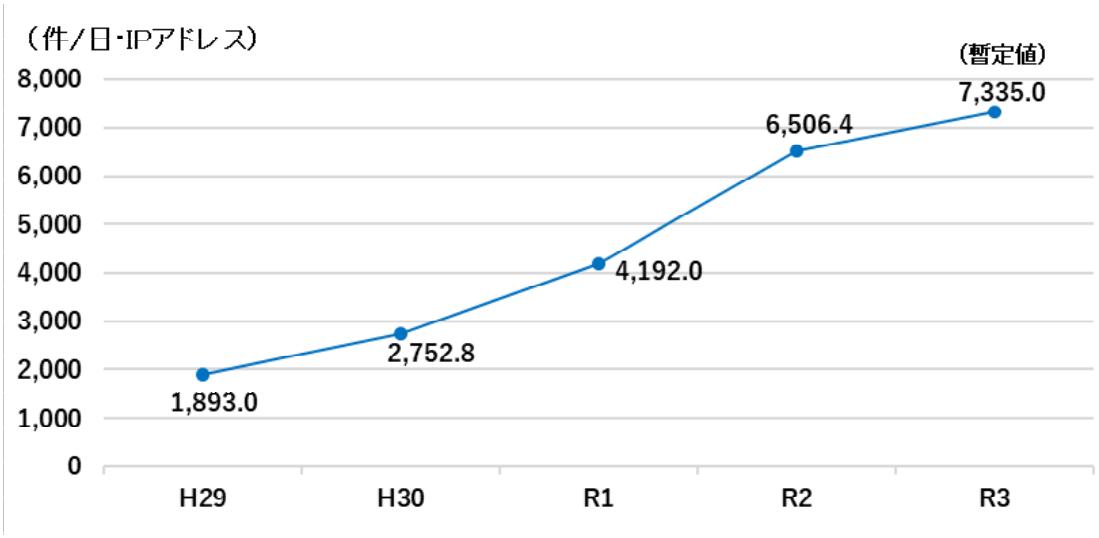
【図表８：被害の調査・復旧に要した総額】



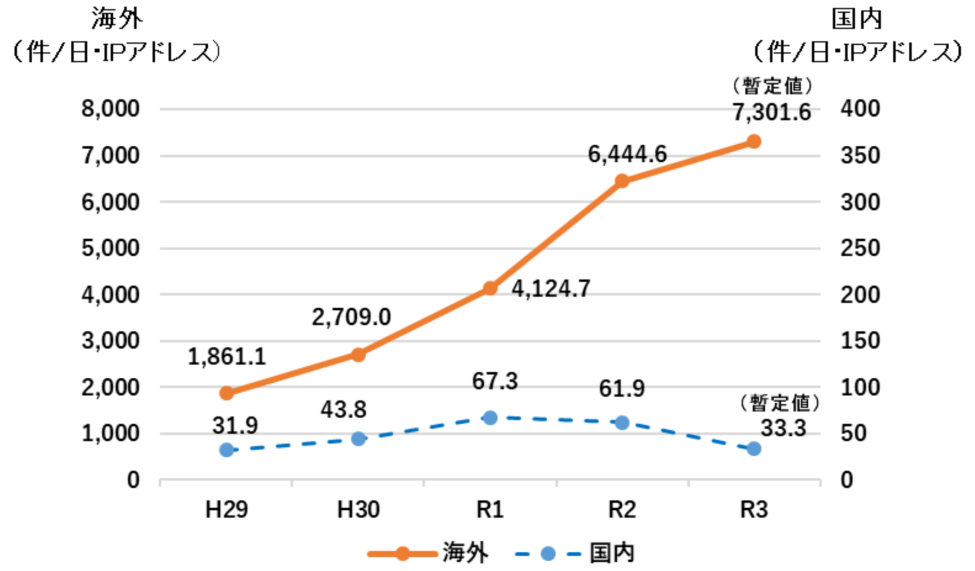
*5　令和３年中に都道府県警察から警察庁に報告があったランサムウェア被害（146件）について、被害企業・団体等に対して警察が実施したアンケート調査。

２　サイバー空間におけるぜい弱性探索行為等の観測状況[*6]

【図表９：センサーにおいて検知したアクセス件数の推移】



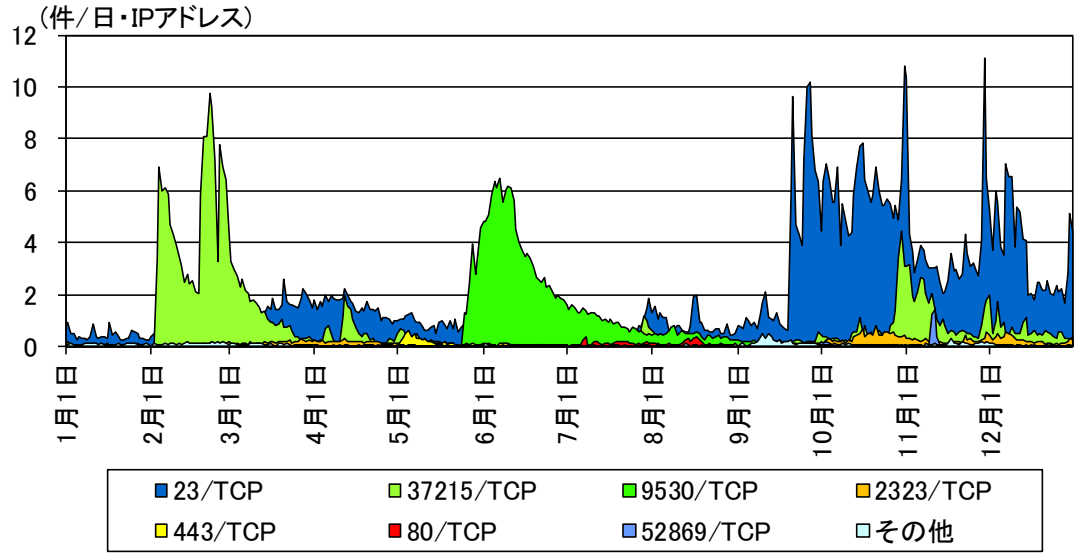
【図表10：検知したアクセスの送信元で比較した１日・１ＩＰアドレス当たり件数の推移】



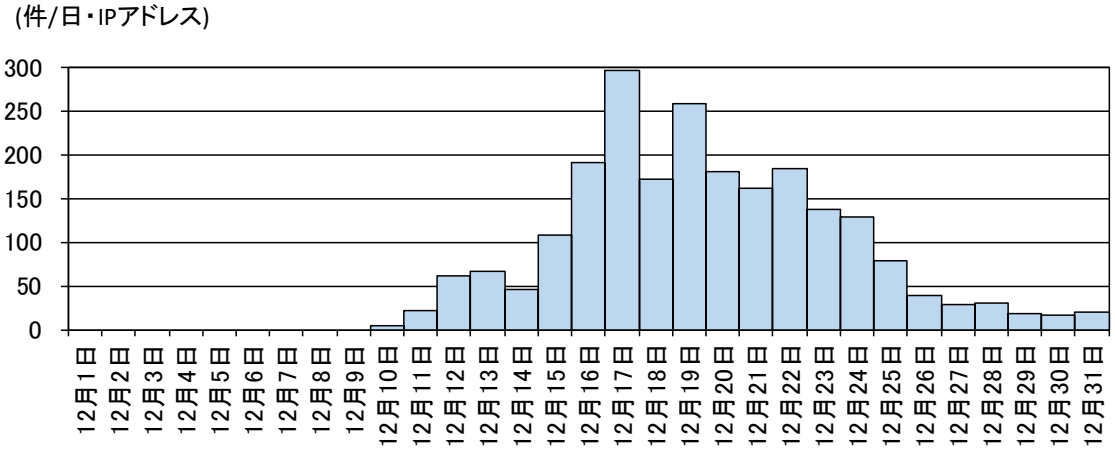
---

*6　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。

【図表11：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）[*7] 】



【図表12：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[*8] 】

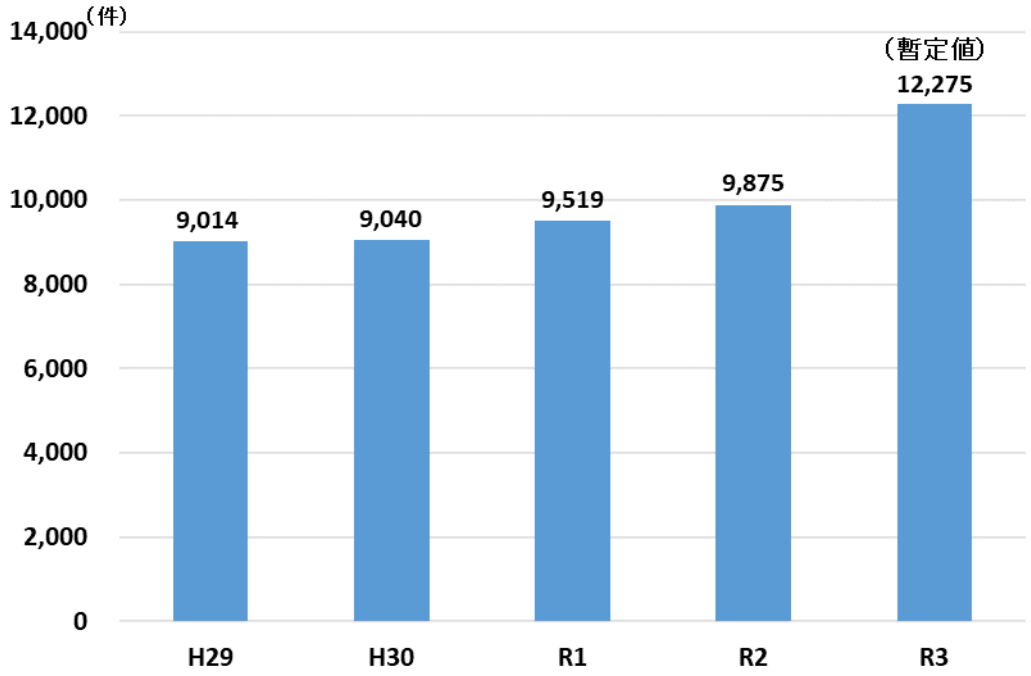


*7　「Mirai」とは、ＩｏＴ機器等に感染しＤｏＳ攻撃等を行う不正プログラムの一種。

*8　「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。12月10日にぜい弱性が公表された。

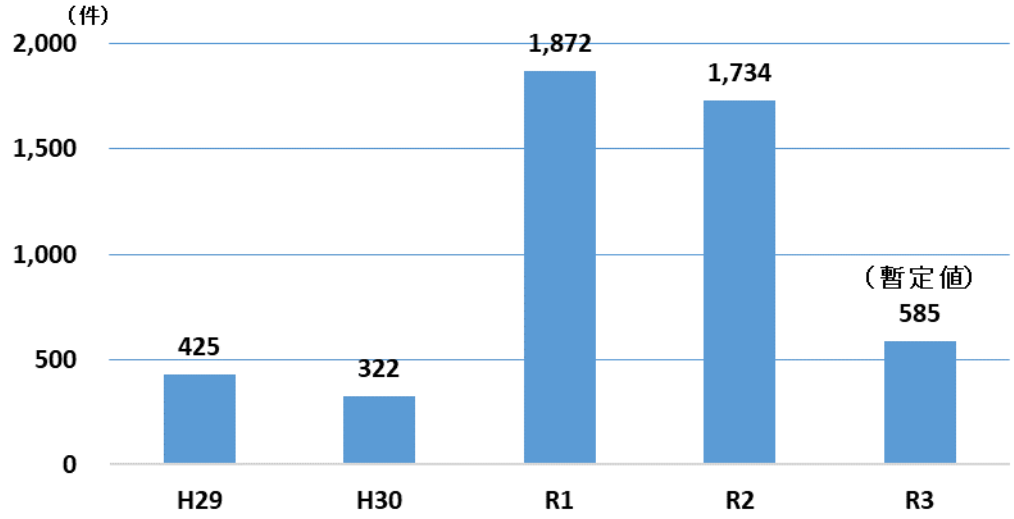
３　サイバー犯罪に係る統計

【図表13：サイバー犯罪の検挙件数の推移】



４　不正送金事犯に係る統計

【図表14：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15：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】