不正アクセス防止対策に関する行動計画

緊迫化するサイバー犯罪情勢

社会経済活動におけるインターネットの利用が拡大し、最早インターネットは国民生活や社会経済活動にとって不可欠なものとなっている。

インターネットバンキング用のID・パスワードを不正に取得し、インターネットバンキングに不正アクセスして、他人名義の銀行口座へ不正送金する事案や機密情報の窃取等を目的とする企業等への標的型メール攻撃等が相次いで発生

官民ボードの設置

警察庁、総務省、経済産業省、サーバ・コンピュータ製造事業者、OSソフト製造事業者、ウイルス対策ソフト開発事業者、コンピュータ・セキュリティ監査事業者、コンピュータ・セキュリティ関連団体、通信事業者関連団体、研究所等

行動計画の策定

官民が一体となって、不正アクセス行為に関する実態情報を共有し、不正アクセス防止対策として講ずべき措置について意見集約を行い、その結果を公表して社会全体で実行してもらう。

潜在化する不正アクセスの実態を適正に把握

- ○ 不正アクセス行為を受けた際の通報の活発化（3頁）
- ○ 届出取扱作業のマニュアル化（4頁）　等

不正アクセスの実態や対策の普及啓発による態勢整備

- ○ 「官民ボード・ポータルサイト」（仮称）の構築（5頁）
- ○ 一般利用者向けの標語作成（7頁）
- ○ 最新の技術動向を踏まえた的確な情報提供（9頁）　等

不正アクセスの対抗策を官民で研究・実施

- ○ フィッシング行為の法規制化の検討（10頁）
- ○ ID・パスワードの不正取得行為や提供行為の法規制化の検討（11頁）
- ○ セキュリティ・ホール攻撃対策等技術的なセキュリティ対策の推進（12頁）　等

達 成 目 標

不正アクセス行為の防止に関し、不正アクセス行為の発生件数等の実態を適正に把握した上で、効果的な普及啓発活動や的確な取締り・防御措置の実施を通じて、不正アクセス行為の発生件数の減少を図る。

平 成 2 3 年 1 2 月

官民意見集約委員会

不正アクセス防止対策に関する行動計画

1　行動計画の策定の趣旨

近年、社会経済活動におけるインターネットの利用が拡大し、最早インターネットは国民生活や社会経済活動にとって不可欠なものとなっているが、その健全な持続的発展の前提としては、インターネット利用における安全・安心の確保が図られなければならない。

しかしながら、インターネットバンキング用のＩＤ・パスワードを不正に取得し、インターネットバンキングに不正アクセスして、他人名義の銀行口座へ不正送金する事案や機密情報の窃取等を目的とする企業等への標的型メール攻撃等が相次いでいるなど、サイバー犯罪等をめぐる情勢は厳しさを増している。

このような情勢においては、官民が一体となって、不正アクセス行為[*1]に関する実態情報を共有し、不正アクセス防止対策として講ずべき措置について意見集約を行い、その結果を公表して社会全体で実行してもらうことが重要である。

（正確かつ適切な実態把握）

不正アクセス行為は、アクセス管理者[*2]が当該行為による被害を自ら確認する方法が分かりにくいことや、金銭的な被害が発生しない場合には届出の必要性を感じないことなどから、潜在化しやすい性質がある。この結果、不正アクセス行為の正確な発生実態が認知されないため、社会全体の適正な危機意識の共有が図られていない状況

---

*1　他人のＩＤ・パスワードを悪用したり、コンピュータ・プログラムの不備をつくことにより、本来アクセスする権限のないコンピュータ（サーバ）を利用する行為をいう。

*2　電気通信回線に接続している電子計算機の利用について、当該電子計算機の動作を管理する者をいう。

となっている。今後は、社会全体で危機意識を共有するため、不正アクセス行為に係る実態を正確かつ適切に把握するための取組を実施していく必要がある。

（効果的な普及啓発）

また、社会全体の適正な危機意識の共有がなされていない状況においては、不正アクセス行為の防止に関する施策を円滑に実施することは困難であることから、社会全体で適正な危機意識を共有することによって、社会全体が一致協力して十分な施策を実施できるよう環境整備を図る必要がある。そのためには、正確かつ適切に把握された不正アクセス行為の実態情報を社会の各層に対してあらゆる機会を活用して重層的に伝達する取組が重要である。すなわち、斉一的な普及啓発活動を行うための基盤を整備するとともに、普及啓発の対象に見合った活動を行う。加えて、日進月歩の情報通信技術の動向に社会全体が追い付いていけるよう、タイムリーな情報提供を推進する。

（不正アクセス行為を防止する対抗策）

その上で、不正アクセス行為をより直接的に防止できる各種の対抗策を研究し、速やかに実施していくことが重要である。すなわち、情報セキュリティ技術に関する知見を有する者が集まって共同研究し、合理的かつ効果的な対抗策、中でも、不正アクセス行為に係る新たな手口への対抗策やアクセス管理者による防御措置の具体的向上方策を社会全体に対して具体的に示していく必要がある。

2　社会全体として取り組むべき施策

(1)　適正な実態把握のために必要な施策

不正アクセス行為の潜在化を防ぐためには、不正アクセス行為の実態を適正に把握する必要があることから、

○　不正アクセス行為の発生件数の把握（量的把握）

○　不正アクセス行為の手口の把握（質的把握）

の両面から実態を捉えるため、次の取組を推進する。

ア　不正アクセス行為の発生件数の把握

不正アクセス行為の増減や発信地域を把握するため、認知・通報件数等の集約を行う。

(ｱ)　多面的把握

警察、独立行政法人情報処理推進機構（ＩＰＡ)、サイバー犯罪警戒防止事業者[*3]等が保有する不正アクセス行為についての情報を集約分析することにより、不正アクセス行為の発生件数を推測・把握する。

・　警察庁、ＩＰＡ、サイバー犯罪警戒防止事業者等が保有する不正アクセス行為についての情報の集約分析【警察庁、ＩＰＡ、JPCERTコーディネーションセンター（JPCERT/CC)、サイバー犯罪警戒防止事業者等】

不正アクセス防止対策を進めるに当たって、まずは実際に国内で発生している不正アクセス行為の状況を把握することが必要である。不正アクセス行為の国内の発生状況を全体として量的に把握し、その傾向や分類を把握することが望まれる。

警察庁、ＩＰＡ、JPCERT/CC、サイバー犯罪警戒防止事業者等の不正アクセス行為に対応する組織は、それぞれ把握する発生件数を公表しているが、これら各組織の統計情報を取りまとめ、集約することにより、日本国内で発生している不正アクセス行為の実態把握を可能とすることを目標とする。

(ｲ)　警察の統計による把握

不正アクセス行為認知時における警察への通報を促進し、認知件数によって不正アクセス行為の発生件数をより正確に把握する。

・　通報指針策定による通報の促進【警察庁】

不正アクセス行為の量的把握を正確に行うため、不正アクセス行為を受けた際の警察への通報の要否を客観的に判断する通報指針を策定するとともに、企業等に当該指針の周知及び通報の要請を行い、通報の活発化を図る。また、通報時における管轄警察署等と企業間の通報要領の確認や不正アクセス行為の通報を受けた際の処理手順を示す対応マニュアルを作成する

---

*3　委託を受けて、インターネットに接続されたサーバ等に対する不正アクセスやサイバー攻撃の発生を警戒し、防止する事業を行う者をいう。

など、事務処理の効率化を図る。

イ　不正アクセス行為の手口の把握

不正アクセス行為の手口を把握するため、同行為の態様、被害状況等の分析を行う。

(ｱ)　ウェブサイトの管理者その他アクセス管理者による不正アクセス行為の適正な認知

アクセス管理者に対し、不正アクセス行為の事実を簡易に確認するツールの活用を促し、不正アクセス行為の認知件数を高めるための改善を行う。

・　サイバー攻撃や脆弱性を検出するためのツールの紹介【ＩＰＡ、JPCERT/CC、サイバー犯罪警戒防止事業者】

不正アクセス行為の内容を正確に把握するため、情報セキュリティ対策に十分な投資ができない企業等を対象に、費用面の負担を心配せずに導入可能なセキュリティ監視ツールを選定し、紹介する活動を展開する。具体的には、サーバアクセスログの分析、不正プログラム感染調査、ネットワーク通信監視、改ざん検知、脆弱性確認、ネットワークパケットの取得等に関して、ツールを活用する利点・不正アクセス行為の発見方法等を紹介する。また、これらの分野で利用可能なツールのうち、価格・有効性・導入難易度等の観点から公開することが公益につながると判断したものを参考情報として紹介する。

(ｲ)　対応マニュアルによる不正アクセス行為認知時の対応方針の明確化

警察、ＩＰＡ、JPCERT/CC等の届出等受理機関は、不正アクセス行為の届出等受理時における対応方針・手順を共有し、お互いの対応手順を明確化する。

・　警察庁、ＩＰＡ、JPCERT/CC等の届出等受理機関における対応方針・手順の共有【警察庁、ＩＰＡ、JPCERT/CC】

警察、ＩＰＡ、JPCERT/CC等の不正アクセス届出等受理機関は、それぞれの受理機関が現在行っている作業手順を整理し、不正アクセス行為や被害のカテゴリを統一し、その上で、受理機関の間で届出取扱作業の方針・手順を共有し、マニュアル化する。

また、自部門では届出として受理しないが、他の受理機関で受理できる可

能性がある場合の紹介手順や、不正アクセス行為と判断するのに必要な情報や証拠についても対応マニュアルに記載する。

(ｳ) 不正アクセス行為リポートの作成・公表

届出等受理機関は、それぞれが受理した不正アクセス行為の内容を分析し手口を把握するとともに、時々の傾向等について他の機関と定期的に情報交換を行い、届出者固有の情報を匿名化した上で、リポートを作成・公表する。

・ 警察庁、ＩＰＡ、JPCERT/CC等の届出等受理機関における情報交換、リポートの作成・公表【警察庁、ＩＰＡ、JPCERT/CC】

警察庁、ＩＰＡ、JPCERT/CC等の届出等受理機関は、それぞれが受理した不正アクセス行為の内容を分析し、手口を把握するとともに、時々の傾向等について他の機関と定期的に情報交換を実施できる体制の構築を目指す。また、届出者固有の情報を匿名化した上で、実務者が活用できる情報発信の在り方について検討する。

(2) 効果的な普及啓発のために必要な施策

適正に把握された実態に基づき、社会の各層に対して効果的な普及啓発活動を重層的に行うことにより、社会全体の適正な危機意識の共有を図り、不正アクセス行為に対する十分な施策が実施できるよう環境整備を行う必要がある。適正な危機意識の共有に資する効果的な普及啓発活動のため、次の取組を推進する。

ア 普及啓発内容の斉一化

普及啓発の対象に見合った的確な内容で活動を行うため、ＩＰＡや総務省の情報セキュリティの普及啓発に係るポータルサイトの充実、既存の情報セキュリティの普及啓発のための資料の相互利用等を図る。

(ｱ) ポータルサイトの充実【警察庁、総務省、経済産業省、ＩＰＡ、情報セキュリティ関連事業者等】

ポータルサイトを構築するに当たり、統一的なリンクを作成することで連携し、どこのポータルサイトにアクセスしていても、利用者が必要としている情報を保有しているポータルサイトに簡単に到達できるようなサイト構築を目指す。さらに、「不正アクセス防止対策に関する官民意見集約委員会」（以下「官

民ボード」という。）としては、ＩＰＡを中心に、政府機関を始めとした既存のポータルサイトを統括する「官民ボード・ポータルサイト」（仮称）を構築し、官民ボードの取組を集約することを検討する。

(ｲ) 既存資料の相互利用【警察庁、総務省、経済産業省、ＩＰＡ、日本オンラインゲーム協会、情報セキュリティ関連事業者等】

各組織・企業の情報セキュリティの普及啓発に関する資料の情報共有・提供を図ることとする。第一段階として、各組織・企業間の情報共有を図り、どのような資料が存在しているかの相互理解を得る。次に、一般ユーザ向けに、「官民ボード・ポータルサイト」（仮称）を設けて、啓発資料を分類し、より進んだ提供を図ることとする。

イ　有機的かつ重層的な普及啓発

警察庁、総務省、経済産業省等の政府機関、ＩＰＡを始めとした情報セキュリティ関連事業者・団体等は、「情報セキュリティ2011」（平成23年７月８日情報セキュリティ政策会議決定）等に沿って有機的に連携しながら、成長の過程にある子どもやその保護者、インターネット利用者、企業経営者等のあらゆる啓発対象に対し、学校教育活動、企業内研修、情報セキュリティ講習会等のあらゆる機会を通じて一人一人の啓発対象が情報セキュリティについて重層的に学ぶことができるよう、有機的かつ重層的な普及啓発活動を推進する。また、その際には、不正アクセス行為の適正な実態把握に資するよう、不正アクセス行為の被害に遭った場合の対応方法等についても周知活動を推進する。

(ｱ) 生徒・学生・保護者・教育機関を対象とした普及啓発【警察庁、総務省、経済産業省、ＩＰＡ、日本オンラインゲーム協会、情報セキュリティ関連事業者等】

体験教室やターゲットを絞ったレクチャー等を増やすことが必要であることから、情報セキュリティ講習を引き続き推進するほか、例えば、情報通信技術関連イベントや学校関係者等からの依頼による講演会等を活用し、オンラインゲームにおける不正アクセス行為等情報セキュリティについて普及啓発活動を行うことを検討する。また、民間企業で取り組んでいる夏休み情報セキュリテ

ィ教室等、講師派遣型情報セキュリティ講座等の活動を広げることを検討する。加えて、対象者の目に多く触れる場所で訴求させる必要があることから、学校や塾等の教育現場にポスター等を貼り、意識を高めることに努める。

(ｲ) 一般利用者（高齢者等を含む。）を対象とした普及啓発【警察庁、総務省、経済産業省、ＩＰＡ、日本オンラインゲーム協会、情報セキュリティ関連事業者等】

・ インターネットを利用する際に、一般利用者にとって最低限必要となる対策の定義を行う（例：セキュリティソフトの導入、ＯＳのアップデート、パッチの適用等）。

・ パソコンの情報セキュリティ対策に不慣れな利用者の方にも広く周知を行うため、最低限必要となる対策方法について標語の作成を行う。

・ ポータルサイト、政府広報、各種セミナー等、多くの一般利用者に情報の提供が可能な普及チャネルを活用して標語の周知を行う。

(ｳ) 企業経営者を対象とした普及啓発【経済産業省、ＩＰＡ、情報セキュリティ関連事業者等】

情報セキュリティ対策が経営者の責務であることを改めて認識させることを前提に、

・ 適正な情報セキュリティ対策の実施、運用等を踏まえたセキュリティ面でのコーポレート・ガバナンス確立のために、企業経営陣が行うべき役割と、その効果について普及・促進を図る。

・ 企業における情報セキュリティ・インシデント[*4]発生時の被害実態を認識させ、その事前・事後の対策について、周知を図る。

・ 企業における情報セキュリティ対策の努力義務に関しては、関係省庁が取りまとめた各種ガイドライン等の活用を積極的に促すものとする。

(ｴ) 中小企業を対象とした普及啓発【経済産業省、ＩＰＡ、情報セキュリティ関

---

*4 情報セキュリティの脅威となる事案や情報セキュリティに関連する事故等をいう。

連事業者等】

中小企業関係団体等と連携して、それぞれが開催するセミナーや会議において、短時間であっても情報セキュリティの意識付け等の啓発活動を織り込むことや、それぞれのウェブサイトへの掲載協力を進めるなど、裾野の広い普及活動を展開する。あわせて、中小企業向け指導者育成セミナーを引き続き実施する。

また、より深く対策等を学んでもらうための情報セキュリティセミナーを各組織が開催できるように、講師派遣等の協力関係を進める。

中小企業が無理なく理解し実施できる情報セキュリティに関する様々なコンテンツを用意する必要がある。

(ｵ) 官公庁・地方公共団体を対象とした普及啓発【警察庁、総務省、経済産業省】

政府機関に対する脆弱性情報等に関する注意喚起の発出、政府職員に対する標的型メール攻撃対応訓練、ウェブサイトを通じた情報セキュリティに関する情報の地方公共団体への提供、政府機関であることが保証されるドメイン名の利用等、実効性のある既存の取組を推進するとともに、標的型サイバー攻撃の多発等の情勢の変化に臨機応変に対応できるよう、既存の取組の検証・改善を図るための協力を行う。また、省庁間、地方公共団体間の連携の強化を図る。

組織内における高度情報セキュリティ人材の効果的な育成のため、人事ローテーション等を考慮した適切な時期及び形式で研修を実施する。

(ｶ) 不正アクセス行為の被害に遭った場合の対応方法等の周知活動【警察庁、ＩＰＡ、JPCERT/CC】

・ 不正アクセス行為に関する相談・届出窓口を開設している警察、ＩＰＡ及びJPCERT/CCのホームページ等で、当該窓口で対応する相談・届出の概要、範囲、必要な情報を掲載するとともに、範囲外の相談・届出に対応する他の窓口の紹介を行い、相談者の意図に沿った届出が推進されるようにする。

・ 情報セキュリティに関する講習等の場を通じ、各相談・届出窓口やこれら窓口で扱う相談・届出の概要等について周知するとともに、企業の販促チャネル等でも周知を図れるよう、働き掛けを行う。また、関係省庁・団体等と連携し、企業等、特に、企業経営者等に対する警察等への相談・届

出に関する情報発信の在り方について検討する。

・　企業等が不正アクセス行為の被害の相談・届出等をする場合に必要となる事項が分かりやすくまとめられた資料の作成について検討する。

・　警察本部及び警察署の相談担当者等に対し、相談等対応能力の向上と不正アクセス相談の対応マニュアルの周知徹底を図る。

ウ　最新の技術動向を踏まえた的確な情報提供

スマートフォン等の情報端末やソーシャル・ネットワーキング・サービス（ＳＮＳ）等の最新の情報通信技術を悪用した犯罪等の身近な脅威について、警察庁、総務省、経済産業省等の政府機関、ＩＰＡ、JPCERT/CCを始めとした情報セキュリティ関連事業者・団体等は、事例等の情報提供に向けた取組を推進する。

・　最新の技術動向を踏まえた的確な情報提供【警察庁、総務省、経済産業省、ＩＰＡ、日本オンラインゲーム協会、情報セキュリティ関連事業者等】

スマートフォンやＳＮＳ等の新しい技術やサービスの利用に当たっては、利用者自身がそれぞれ情報セキュリティ対策を講じることが必要との前提を啓発した上で、各種端末、サービスを利用する幅広いユーザに対し認識が望まれる各種リスクと正しい内容を啓発する。

伝達手段としては、

・　「官民ボード・ポータルサイト」（仮称）で記載

・　製品サービスの紹介サイトやドキュメントに記載

・　製品・サービス契約時の案内

・　利用時における警告

等を想定する。

(3)　不正アクセス行為等への対処のために必要な施策

把握された実態を踏まえた危機意識の共有による環境の整備を図った上で、的確な取締りの強化とアクセス管理者等による防御措置等の促進の両面から不正アクセス行為等に対処するため、次の取組を推進する。

ア　フィッシング対策の推進

不正アクセス行為の手段となるフィッシングに対処するため、JPCERT/CCによるフィッシングサイトの閉鎖等の取組を推進するとともに、利用者への啓発、技術的な対応策及び法規制化の検討を含め、新たなフィッシング対策の在り方について検討する。

(ｱ) JPCERT/CCによるフィッシングサイトの閉鎖等の取組の推進【警察庁、総務省、経済産業省、JPCERT/CC、フィッシング対策協議会】

フィッシングサイトを認知した場合には速やかに閉鎖等の取組を進め、被害の発生及び拡大の防止に努める。そのためにはフィッシングメールやフィッシングサイトの早期発見が重要であることから、フィッシングに係る届出の手続を整理するとともに、関係機関の連携を強化する体制を検討する。また、閉鎖等の取組を適切に行うため、正当な活動とフィッシングとの切り分けについて関係機関で検討し、共通の見解を維持するよう努める。

(ｲ) 利用者への啓発、技術的な対応策及び法規制化の検討を含めた新たなフィッシング対策の在り方の検討【警察庁、総務省、経済産業省、JPCERT/CC、フィッシング対策協議会、アクセス管理者、情報セキュリティ関連事業者】

フィッシング行為についての注意喚起等フィッシング行為に係る利用者への広報啓発や、フィッシングサイトの閲覧を防止する技術、フィッシングで入手した情報を用いた不正ログインを防止する認証技術等フィッシング行為を防止する技術的対応策の推進に努める。また、フィッシング行為による金銭的被害等が発生する前の段階で取締りを行うことができるよう、フィッシング行為の法規制化の検討を行う。

イ　不正ログイン対策の推進

自動入力プログラムを用いたＩＤ・パスワードの連続入力による不正アクセス行為の取締り及びＩＤ・パスワードのリストの不正流通への対策を強化する。また、パスワードの適切な発行・再発行、乱数表やワンタイムパスワード等の導入等、アクセス管理者による不正ログイン対策の取組を推進する。

(ｱ) 自動入力プログラムを用いたＩＤ・パスワードの連続入力による不正アクセス行為の取締りの強化【警察庁】

不正に取得したＩＤ・パスワードのデータを連続自動入力プログラムを用いて様々なウェブサイトに試行入力して不正アクセス行為を敢行する攻撃（以下「連続自動入力試行攻撃」という。）について、アクセス管理者から警察に対する通報を促し警察における情報の把握を強化した上で、把握した情報に基づいて当該攻撃に対する取締りを強化する。また、捜査活動を通じて、ＩＤ・パスワードのリストの不正流通の実態把握に努める。

(ｲ) ＩＤ・パスワードのリストの不正流通への対策の強化【警察庁、総務省、経済産業省、アクセス管理者】

警察庁は、連続自動入力試行攻撃による不正アクセス行為の取締りの強化を通じて、ＩＤ・パスワードのリストの不正流通の実態を把握するとともに、不正流通に係る違法行為の取締りを強化する。関係省庁は、他人のＩＤ・パスワードの不正取得行為や提供行為の法規制化の検討を行う。アクセス管理者は、平素からＩＤ・パスワードの使い回しの問題に関する利用者への注意喚起や啓発に努めるとともに、ＩＤ・パスワードの流出事案が発生した場合は、利用者に対して速やかに周知を行うよう努める。

(ｳ) 不正ログイン対策技術の導入等、アクセス管理者による不正ログイン対策の取組の推進【警察庁、総務省、経済産業省、ＩＰＡ、アクセス管理者】

不正ログイン対策が適切に推進されるよう、ＩＰＡ及び関係省庁において次のような資料を作成する。アクセス管理者は、これらの資料等を参考に、適切な不正ログイン対策の実施に努める。

- 技術力を持たないアクセス管理者でもふさわしいセキュリティ水準の不正ログイン対策を把握できるような、乱数表、ワンタイムパスワードその他の不正ログイン対策の技術方式を国際水準等を踏まえて洗い出し、企業の活動内容ごとに、それに見合う不正ログイン対策のセキュリティ水準を整理した参考資料
- パスワードの発行・再発行に関する適切な手順の設計を整理した参考資料

ウ セキュリティ・ホール攻撃対策等アクセス管理者による技術的なセキュリティ対策の推進

「ソフトウェア等脆弱性関連情報取扱基準」（平成16年経済産業省告示第235号。以下「脆弱性取扱基準」という。）に基づくＩＰＡやJPCERT/CCを通じたソフトウェア製品及びウェブサイトのセキュリティ・ホール攻撃対策の取組等、アクセス管理者による技術的なセキュリティ対策の取組を推進する。

(ｱ) 脆弱性取扱基準に基づくＩＰＡやJPCERT/CCを通じたソフトウェア製品及びウェブサイトのセキュリティ・ホール攻撃対策の取組【警察庁、総務省、経済産業省、ＩＰＡ、JPCERT/CC】

ＩＰＡは、次の点に配意した脆弱性対策ホームページを作成し、関係省庁は、それぞれのサイトでリンクを張り紹介するなどして、脆弱性取扱基準に基づく更なる取組の推進を図る。

- ソフトウェア製品開発者やウェブサイト運営者に対し、より速やかに脆弱性対策が実施されるようその重要性及び脆弱性取扱基準に基づく届出制度を分かりやすく解説
- 情報セキュリティ研究者に対し、より多くの研究者による脆弱性発見活動及び届出がなされるよう届出の意義を説明
- 企業や一般利用者に対し、より速やかに既知の脆弱性への対応が行われるよう脆弱性対策情報を公表しているＪＶＮ[*5]（Japan Vulnerability Notes）サイトやJVN iPedia[*6]サイトを紹介

(ｲ) セキュリティ・ホール攻撃対策等アクセス管理者による技術的なセキュリティ対策の取組の推進（脆弱性取扱基準に基づく取組を除く。）【アクセス管理者】

---

*5　日本で使用されているソフトウェア等の脆弱性関連情報とその対策情報を提供している脆弱性対策情報ポータルサイトをいう。JPCERT/CCとＩＰＡが共同で運営している。

*6　国内で利用されるソフトウェア等の製品の脆弱性対策情報を中心に収集・蓄積する脆弱性対策情報データベースをいう。ＪＶＮに掲載される脆弱性対策情報以外の脆弱性対策情報についても公開対象としている。

既存の情報セキュリティ対策を着実に実施するとともに、不正アクセス行為やそれにつながる情報セキュリティ・インシデントの発生を前提とした情報システムの設計と運用を実施する。具体的には、既存の境界防御の仕組みに加え、情報システム内部に不正プログラムや攻撃者が侵入した場合に、それらを早期に検知・対処するための仕組みや、情報システム内部から外部への情報漏えいを防ぐため、不審な外部への通信の検出・防止を行う対策を検討する。

エ　不正アクセス行為に関する情報共有体制の整備による対応能力の向上

不正アクセス行為の未然防止と同行為による被害の拡大の防止のため、不正アクセス行為の手法やこれを防ぐための対策方法等に関する情報を共有するためのルール等の整備を通じて情報共有体制を整備し、対応能力の向上を図る。

・　不正アクセス行為の情報共有ルール等の整備を通じた情報共有体制の整備による対応能力の向上【警察庁、経済産業省、ＩＰＡ、JPCERT/CC、サイバー犯罪警戒防止事業者】

経済産業省は、サイバー情報共有イニシアティブ（J-CSIP）を順次拡大し、不正アクセス行為等の手法やこれに対する対策方法に関する情報の共有を促進する。このため、不正アクセス行為等に対する未然防止と被害拡大の防止に有効となる情報について、個社情報を匿名化した上で、共有すべき情報の内容やその範囲等、情報を共有するためのルール等を整備し、円滑に情報共有が行われる体制を整備する。また、ＩＰＡは、ここから得られた情報を一般化した上で、ＩＴユーザ全般へ注意喚起を行う。こうした取組により、不正アクセス行為等に対する対応能力の向上を図る。

あわせて、警察庁は、先端技術を有する全国の事業者等とのネットワークを順次拡大し、不正アクセス行為等のサイバー攻撃に関する情報を総合的に分析し、事業者等に提供して注意喚起等を実施する。

(4)　施策の効果検証

(1)から(3)に掲げた施策について、社会情勢の変化に応じて、適時適切に施策の効果を検証し、必要に応じ、見直し等所要の改善を図る。

3　達成目標

不正アクセス行為の防止に関し、不正アクセス行為の発生件数等の実態を適正に把握した上で、効果的な普及啓発活動や的確な取締り・防御措置の実施を通じて、不正アクセス行為の発生件数の減少を図る。