平成２３年１２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の策定について

警察庁において開催された平成22年度総合セキュリティ対策会議では、不正アクセス行為[*1]に係る情報を収集・共有して不正アクセス行為に係る実態を詳細かつ正確に把握するとともに、不正アクセス行為に係る実態の把握を踏まえて問題点を抽出し、不正アクセス防止対策の官民の役割分担や連携施策を検討することが必要であるとの提言がなされた。これを受け、社会全体としての不正アクセス防止対策の推進に当たって必要となる施策に関して、現状の課題や改善方策について官民の意見を集約するため、平成23年６月30日、警察庁、総務省及び経済産業省は、民間事業者等と共同で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。）を設置した。

この度、官民ボードに設置された４つのワーキング・グループ（以下「ＷＧ」という。）の議論を経て、「不正アクセス防止対策に関する行動計画」（以下「行動計画」という。）を策定したところであるが、次は行動計画の策定に当たって行われた検討の内容等を記述したものである。

記

１　不正アクセスをめぐる状況

(1)　不正アクセス事犯の発生状況

平成22年中における不正アクセス事犯の認知件数は1,885件（前年比-910件）、検挙件数は1,601件（前年比-933件）であり、検挙件数は減少したものの、検挙事件数で見ると104件（前年比+9件）と、平成12年の不正アクセス行為の禁止等に関する法律（平成11年法律第128号。以下「不正アクセス禁止法」という。）施行後最多となっている。

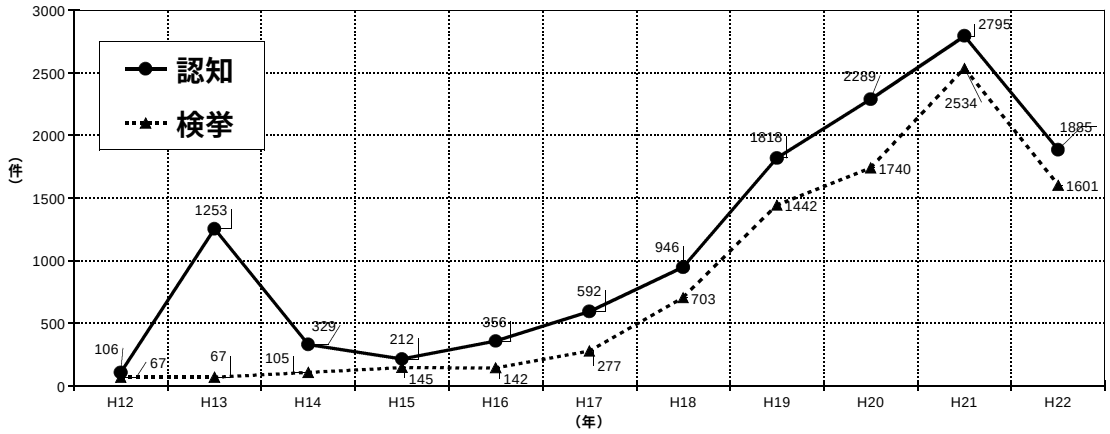
不正アクセス事犯の手口は識別符号を「フィッシングにより入手」したものが1,411件であり、平成21年に引き続き手口種別中では最も多く、全体の88%を占めている。また、不正アクセス事犯の動機は「不正に金を得るため」が1,455件であり、動機種別の全体の91%を占めている。

不正アクセス禁止法施行当初は、ハッカーと呼ばれる者が自己の知名度

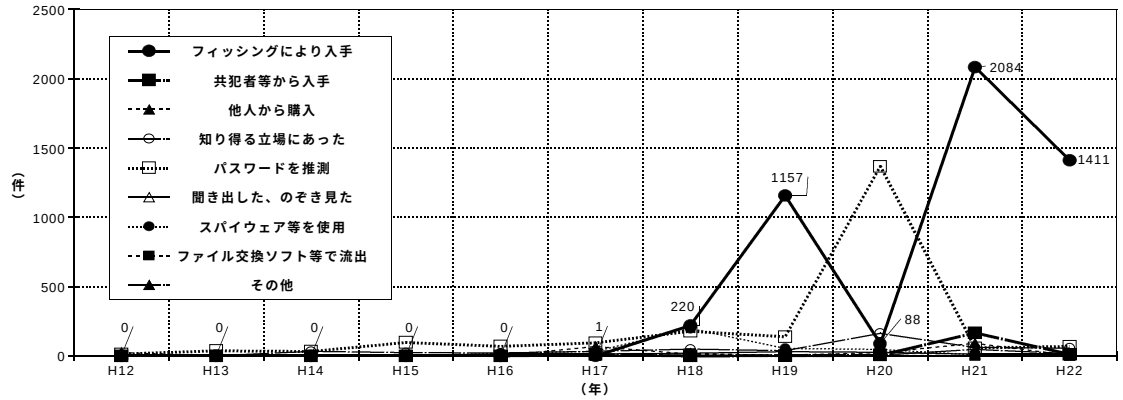
＊１　不正アクセス行為　他人のＩＤ・パスワードを悪用したり、コンピュータ・プログラムの不備をつくことにより、本来アクセスする権限のないコンピュータ（サーバ）を利用する行為をいう。

を高めたり、技術の高さを他人に誇示したりするなど、不正アクセス行為そのものを動機とした、好奇心によるものも散見されたが、現在では、銀行預金の送金やクレジットカード決済を始め金融機関等がインターネットを利用したサービスを開始したことなどを背景に、不正に金を得ることを動機としたものが急増している。平成23年４月以降、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送金し、ＡＴＭで現金を引き出すという手口が急増し、多額の被害が発生しているところである。

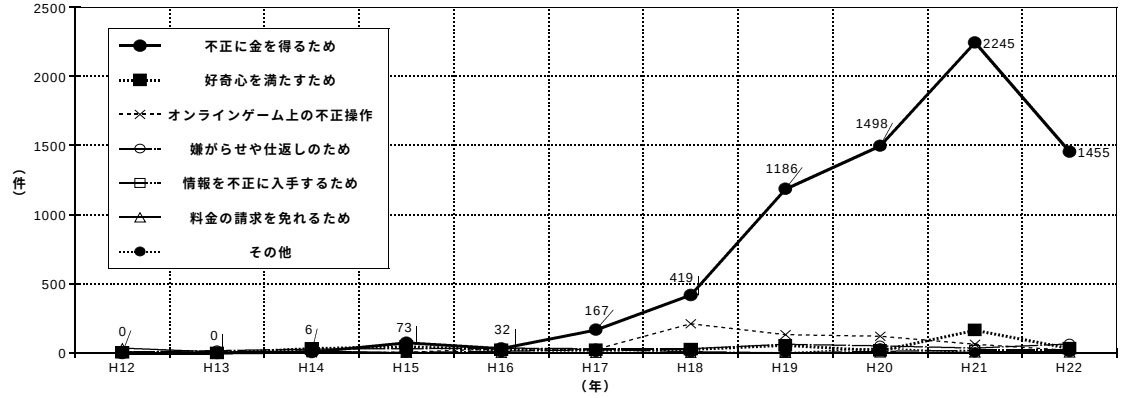
不正アクセス事犯の認知・検挙件数の推移



不正アクセス事犯の手口の推移



不正アクセス事犯の動機の推移



(2)　アクセス制御機能に関する技術の研究開発状況

国家公安委員会、総務大臣及び経済産業大臣は毎年、不正アクセス禁止法第７条１項の規定に基づき、アクセス制御機能に関する技術の研究開発状況について公表している。平成23年３月に公表した研究開発状況は次のとおりである。

実施主体	対象技術	研究開発内容
日本電気(株) 奈良先端科学技術大学院大学 (株)ＫＤＤＩ研究所 パナソニック電工(株) (株)クルウィット (財)日本データ通信協会 （(独)情報処理通信機構（ＮＩＣＴ）からの委託）	侵入検知技術	インターネットにおけるトレースバック技術に関する研究開発
(株)エヌ・ティ・ティ・データ （ＮＩＣＴからの委託）	その他認証技術	持続的な安全性を持つ暗号・電子署名アルゴリズム技術に関する研究開発～安全な暗号技術を利用し続けるための暗号利用フレームワーク～
(株)日立製作所 神戸大学 福井大学 （ＮＩＣＴからの委託）	その他認証技術	次世代ハッシュ関数の研究開発
富士通(株) （ＮＩＣＴからの委託）	その他認証技術	適切な暗号技術を選択可能とするための新しい暗号等技術の評価手法～暗号の技術的評価に関する研究開発～
(株)ラック (財)九州先端科学技術研究所 (株)セキュアウェア (株)セキュアブレイン (株)クリプト ジャパンデータコム(株)	その他認証技術	インシデント分析の広域化・高速化技術に関する研究開発

ＫＤＤＩ(株) （ＮＩＣＴからの委託）		
ＮＩＣＴ	侵入検知技術	ネットワークセキュリティ技術の研究開発
(株)日立製作所 ＫＤＤＩ(株)	その他認証技術等	マルウェア対策ユーザサポートシステムの研究開発
(独)産業技術総合研究所（ＡＩＳＴ） （経済産業省からの委託）	その他認証技術等	証明可能な安全性をもつキャンセラブル・バイオメトリクス認証技術の構築とそれを利用した個人認証インフラストラクチャ実現に向けた研究開発
(株)日立製作所 （経済産業省からの委託）	その他認証技術	生体認証サービスにおける情報漏えい対策（キャンセラブル・バイオメトリクス）の研究開発
(株)グローバルワイズ	侵入検知技術	同一ネットワーク上の端末情報収集技術
(株)ニーモニックセキュリティ	その他認証技術	認証権限分散技術
佐賀大学	ネットワーク	利用者認証システム
信州大学	サーバ、通信情報、データ	・ＰＫＩ処理を高速に実行するアクセラレータ ・各個人のその人らしさの認証
神奈川大学	ネットワーク	パケットフィルタの最適化
北海道大学	データ、その他	ＰＤＦファイルの作成時刻保証
国士舘大学	通信情報、その他	クラウドの脆弱性検証
奈良先端科学技術大学院大学	ネットワーク、通信情報	ＤｏＳ攻撃の攻撃者追跡
岩手大学	サーバ	コンピュータ・ウイルスの解析手法
東北工業大学	ネットワーク、サーバ、クライアント	データリンク層における低コストな通信制御

九州大学	ネットワーク、サーバ、クライアント、通信情報、データ	暗号及び暗号プロトコル技術、コンピュータシステムセキュリティ技術等
シスメックスＲＡ(株)	通信情報	IPsec暗号化
(株)アクアシステムズ	通信情報	データベースのアクセス監査及びログ保管
ＫＤＤＩ(株)	サーバ	ウェブサイト改ざん検知システム
メトロ(株)	クライアント	・ハードディスク暗号化、ＯＳ起動前ログイン認証 ・メディア暗号化、デバイス制御
三菱電機(株)	データ、サーバ	・ファイルの暗号化、ハードディスクの逐次暗号化 ・ウェブシステムのSaaS型診断サービス
ログイット(株)	通信情報	Ｅメールのアーカイブでの監査認証
(株)日立ソリューションズ	サーバ、通信情報、データ	ファイルサーバの暗号化、アクセス制御、ログ取得
(株)シー・エス・イー	ネットワーク、サーバ、クライアント	マトリクス認証による本人認証システム
(株)インテリジェントウェイブ	クライアント、データ、その他	パソコンからの情報漏えい防止ソフトウェア

2　官民ボードの開催状況について

(1)　開催状況

官民ボードには、行動計画の策定を円滑に実施するため、次のＷＧが設置された。

○　行動計画策定ＷＧ

○　実態把握方策ＷＧ

○　普及啓発方策ＷＧ（平成23年９月29日の第２回官民ボード全体会議で情報セキュリティ講習方策ＷＧから名称変更）

○　不正アクセス行為対応方策ＷＧ

ＷＧでの検討に当たっては、まず行動計画策定ＷＧにおいて、実態把握方策ＷＧ、普及啓発ＷＧ及び不正アクセス行為対応方策ＷＧの各ＷＧで検討すべき事項、検討スケジュール等について方針を示し、各ＷＧでは、それに基づき個別の検討を行った。そして、その検討結果を行動計画策定ＷＧに報告し、行動計画策定ＷＧにおいて当該検討結果を確認し、全体調整を図った上で、全体会議において全会一致の原則に基づき審議を行い、最終的に行動計画を取りまとめた。

○　官民ボード全体会議

開催日	検討事項
第１回 平成23年６月30日（木）	・「不正アクセス防止対策に関する官民意見集約委員会設置要綱」の検討 ・　官民ボードの運営の在り方について検討 ・「ワーキング・グループの設置、任務及び運営について」の検討 ・今後の官民ボードの進め方について検討
第２回 平成23年９月29日（木）	・官民ボード構成員等の追加について検討 ・情報セキュリティ講習方策ＷＧを普及啓発方策ＷＧに名称変更することについて検討 ・「不正アクセス行為の防止対策に関する行動計画」（骨子）の検討
第３回 平成23年12月22日（木）	・「不正アクセス防止対策に関する行動計画」の検討 ・ワーキング・グループの構成の改編について検討 ・今後の官民ボードの開催スケジュールについて検討

○　行動計画策定ＷＧ

開催日	検討事項
第１回	・行動計画策定に当たっての検討事項の関連性に

平成23年７月６日（水）	ついて検討 ・過去に他の官民会議で策定された行動計画について紹介 ・行動計画骨子案の構成について検討 ・行動計画策定ＷＧ構成員の作業分担について検討
第２回 平成23年７月20日（水）	・行動計画策定ＷＧ構成員の作業分担の確定 ・各ＷＧ（実態把握方策ＷＧ、情報セキュリティ講習方策ＷＧ及び不正アクセス行為対応方策ＷＧ）第１回会合での検討状況について議論
第３回 平成23年９月２日（金）	・各ＷＧ第２回会合での検討状況について議論 ・行動計画策定のイメージについて検討
第４回 平成23年９月15日（木）	・行動計画骨子案の前文概略部分について検討 ・各ＷＧで議論した行動計画骨子案を取りまとめ、検討
第５回 平成23年10月13日（木）	・第２回全体会議で決定した行動計画骨子を元に行動計画を策定するに当たっての作業方針等を検討
第６回 平成23年11月９日（水）	・フィッシング対策の必要性について説明 ・各ＷＧにおける行動計画策定に向けた検討状況について議論 ・行動計画の取りまとめについて議論
第７回 平成23年12月５日（月）	・各ＷＧで議論した行動計画案を取りまとめ、検討 ・行動計画策定後のスケジュールについて検討 ・行動計画策定後のＷＧ改編について検討

○　実態把握方策ＷＧ

開催日	検討事項
第１回 平成23年７月８日（金）	・行動計画策定について説明 ・ＷＧ構成員による不正アクセスの実態説明

第２回 平成23年８月５日（金）	・ＷＧ構成員による不正アクセスの実態説明 ・不正アクセス発生時の届出等について検討
第３回 平成23年９月９日（金）	・行動計画策定ＷＧにおいて出された実態把握方策ＷＧに対する意見について検討 ・不正アクセス行為の実態把握方法について検討
第４回 平成23年10月21日（木）	・不正アクセスの届出方法について検討 ・不正アクセスを検出するための対策について検討 ・相談対応マニュアルについて検討 ・各機関の統計・リポートの作成について検討
第５回 平成23年11月８日（火）	・フィッシング対策の必要性について説明 ・不正アクセス発生時の通報要領について検討 ・不正アクセス行為の適正な認知について検討 ・不正アクセス行為認知時の対応方針の明確化について検討
第６回 平成23年11月15日（火）	・不正アクセスの量的把握について検討 ・不正アクセスの情報共有について検討 ・行動計画及び行動計画の策定についての記載内容について修正・検討
第７回 平成23年11月25日（金）	・届出受理機関におけるマニュアル作成について検討 ・行動計画及び行動計画の策定についての記載内容について最終検討

○　普及啓発方策ＷＧ

開催日	検討事項
第１回 平成23年７月14日（木）	・行動計画策定について説明 ・各機関における情報セキュリティ講習の現状について説明

	・情報セキュリティ講習の在り方について検討
第２回 平成23年７月26日（火）	・ＩＰＡによる中小企業向け普及啓発活動について説明 ・普及啓発対象の選定について検討
第３回 平成23年９月６日（火）	・行動計画策定ＷＧにおいて出された情報セキュリティ講習方策ＷＧに対する意見について検討 ・学校における情報セキュリティ教育について説明 ・普及啓発のための基盤について検討 ・対象別普及啓発方策について検討
第４回 平成23年10月21日（金）	・行動計画作成担当の割り振りについて検討 ・普及啓発のためのポータルサイトの作成について検討 ・あらゆる対象に対する普及啓発活動について検討
第５回 平成23年11月１日（火）	・フィッシング対策の必要性について説明 ・ＩＰＡを中心としたポータルサイトの構築について検討 ・塾業界等と連携した普及啓発について検討 ・広く一般に普及啓発するための活動について検討 ・不正アクセス行為の被害に遭った際の対応方法等の周知活動について検討
第６回 平成23年11月18日（金）	・企業経営者に対する普及啓発活動について検討 ・中小企業に対する普及啓発活動について検討 ・行動計画及び行動計画の策定についての記載内容について修正・検討
第７回 平成23年11月25日（金）	・官公庁・地方公共団体に対する普及啓発方策について検討 ・行動計画及び行動計画の策定についての記載内容について最終検討

○　不正アクセス行為対応方策ＷＧ

開催日	検討事項
第１回 平成23年７月８日（金）	・行動計画策定について説明 ・フィッシングについて検討
第２回 平成23年７月28日（金）	・フィッシングについて検討 ・ＳＱＬインジェクションについて検討 ・その他の不正アクセスに関する危険な行為について検討
第３回 平成23年９月１日（木）	・ブルートフォース攻撃及び不正アクセス助長行為の規制の在り方について検討 ・ＳＱＬインジェクションについて検討 ・ブルートフォース・辞書攻撃について検討 ・その他不正アクセス行為に関する危険な行為について検討
第４回 平成23年10月21日（金）	・フィッシングの現状について説明 ・識別符号の不正取得全般について検討 ・行動計画作成担当の割り振りについて検討
第５回 平成23年11月４日（金）	・フィッシングサイトの閉鎖等の取組について検討 ・新たなフィッシング対策の在り方について検討 ・アクセス管理者[*2]による不正ログイン対策について検討
第６回 平成23年11月22日（火）	・アクセス管理者による不正ログイン対策について検討 ・ＩＤ・パスワードの不正流通への対策の強化について検討 ・行動計画及び行動計画の策定についての記載内容について修正・検討

＊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。

第７回 平成23年11月28日（月）	・パスワードの発行・再発行に関する適切な手順について検討 ・ＩＤ・パスワードの使い回し対策について検討 ・行動計画及び行動計画の策定についての記載内容について最終検討

(2)　官民ボード構成員

官民ボードの各ＷＧに参加している構成員については次表のとおりである。

ＷＧ名称	構成員（順不同）
行動計画策定ＷＧ	伊藤忠テクノソリューションズ(株)、(株)シマンテック、日本ヒューレット・パッカード(株)、日本マイクロソフト(株)、ヤフー(株)、(独)情報処理推進機構（ＩＰＡ）、(特)日本データセンター協会、(社)テレコムサービス協会
実態把握方策ＷＧ	(株)ラック、セコムトラストシステムズ(株)、日本アイ・ビー・エム(株)、日本電気(株)、フィッシング対策協議会、ＩＰＡ ［官民ボード第２回全体会議以降の追加構成員］ (株)エヌ・ティ・ティ・データ、ＳＣＳＫ(株)
普及啓発方策ＷＧ	トレンドマイクロ(株)、チェック・ポイント・ソフトウェア・テクノロジーズ(株)、(株)ジェーシービー、ＩＰＡ、（一社）日本オンラインゲーム協会
不正アクセス行為対応方策ＷＧ	マカフィー(株)、(株)日立製作所、日本セキュリティオペレーション事業者協会（ISOG-J)、ＡＩＳＴ、（一社）JPCERTコーディネーションセンター（JPCERT/CC)、ＮＩＣＴ、(社)電気通信事業者協会、(社)日本インターネットプロバイダー協会、(社)日本ケーブルテレビ連盟、ＩＰＡ ［官民ボード第２回全体会議以降の追加構成員］ (社)日本情報システム・ユーザー協会（ＪＵＡＳ)、 (一社)情報サービス産業協会（ＪＩＳＡ）
オブザーバ	内閣官房情報セキュリティセンター（ＮＩＳＣ） ［官民ボード第２回全体会議以降の追加オブザーバ］ 消費者庁

事務局	警察庁、総務省、経済産業省

3　行動計画の策定について

(1)　実態把握方策

ア　不正アクセス行為の発生件数の把握（量的把握）

(ｱ)　多面的把握

・　警察庁、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の集約分析

取組主体：警察庁、ＩＰＡ、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。

①　現状

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、検挙数やそれぞれの組織で把握する不正アクセス行為の発生件数等の統計情報をそれぞれ公表している。

これらの統計情報を比較することにより、国内の不正アクセス行為の発生傾向等を読み取ることは可能である。

一方、これらの統計情報は、それぞれの組織で独自に集計した数値であることから、日本国内全体の実態を把握できるとは必ずしもいえない。

②　取組の趣旨

不正アクセス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

＊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。

把握することを目標とする。

③　配意事項

現在の各組織の公表する不正アクセス状況の把握については、その件数の単位や分類等は各組織が独自の考え方に基づいて行っているものであり、現在公開されている各組織の統計情報をそのまま足し合わせても、有意な統計情報とはならない。

このため、リポートのベースとなる不正アクセス行為の件数の単位や分類等の考え方についての共通化に向けた検討を行う。また、継続的に今後新たに発生する不正アクセス行為を量的に把握するため、その件数の単位や分類等の考え方について議論できる枠組みについても検討を行う。

(ｲ)　警察の統計による把握

・　通報指針策定による通報の促進

取組主体：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など、事務処理の効率化を図る。

①　現状

現在、発生件数を始めとする不正アクセス行為に関する情報は、警察やＩＰＡ、JPCERT/CCで集約分析されている。しかし、各機関の設置・活動の目的が様々であるため、収集する情報の傾向もおのずと異なる。よって、各機関の情報を単純に合算しても、不正アクセス行為の量的把握が可能となるものではない。また、一部の企業等においては不正アクセス行為を受けても「信用が低下する」等を理由に連絡しないケースがあるなど、その量的把握は難しい状況にある。

②　取組の趣旨

不正アクセス行為を受けた際に企業が通報の要否を判断する通報指針を策定することで、その判断過程を定型化し、不正アクセス行為が正しく警察に通報される社会的枠組みを構築する。策定後は指針の社会的周知を図るとともに通報の目的、必要性等に対する理解を深めるよう企業

に働き掛けることにより、社会全体で不正アクセス行為の実態を把握する。

③　配意事項

社会全体で、不正アクセス行為の通報が積極的に行われるよう、多くの企業等の理解を得るようにする。通報内容については、被害拡大の防止その他の事情により公表の必要性が高いと認められる場合を除き、原則非公表とする。指針の策定に際しては、即時通報事案を限定するなど通報業務の負担軽減に配慮する。インターネット等に係る教養の充実、装備資機材の計画的配備等を通じ、警察組織全体の不正アクセス事案に対する対処能力の向上を図る。

イ　不正アクセス行為の手口の把握（質的把握）

(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

・　サイバー攻撃や脆弱性を検出するためのツールの紹介

取組主体：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。

①　現状

不正アクセス行為は、被害者(企業等)からの申告を元に発生件数や手口が把握されている。ところが多くの企業等では費用面の制約から、「セキュリティソフトの導入」、「データを解析できる技術力要員の確保」、「外部のセキュリティ監視サービスの活用」といったセキュリティ対策が不十分であり、不正アクセス行為を見逃している場合が多い。また、初期段階の不正アクセス行為が見逃されてしまうことにより、攻撃者がしだいに不正アクセス手段をエスカレーションさせ、悪質かつ大規模なサイバー犯罪に発展する可能性が指摘されている。

②　取組の趣旨

現状の問題を解決するためには、不正アクセス行為の検知に役立つソフトウェアの一覧を紹介し、それらのソフトウェアを活用する利点、実際に不正アクセス行為を発見するノウハウ等を同時に例示することが必要である。また、企業のＩＴ管理者の認知度を上げるために、これらの情報をポータルサイト上で、利用者に分かりやすく分類整理して提供することが必要である。

③　配意事項

セキュリティ監視ツールの紹介に当たっては、無償若しくは利用者の費用負担が少ない不正アクセス検知に有効なツールを対象とする。また、特定のツールや企業の宣伝、あるいは営業妨害行為にならないように配慮する。さらに、幅広い利用者が各々のＩＴ技術レベルに応じて選択できるよう可能な限り複数のツールを紹介する。

悪意のある人に利用されかねないツール(脆弱性診断ツール等)や、不適切な動作・通信を行うツール、情報漏えいを誘発するツール、ウイルス対策ソフトで検知される類いのツールは推奨しないよう、特に配慮する。また、紹介するツールのリストは、定期的に見直しを行うことが必要である。

(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

取組主体：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。

①　現状

警察、ＩＰＡ、JPCERT/CC等の不正アクセス届出等受理機関は、受理した情報の利用目的に合わせて独自のルールで不正アクセス行為の届出を受け付けており、不受理の判断もそれぞれ異なる。例えば、

・　警察は、違法行為を行った被疑者の検挙を目的として被害者からの通報等を受け付け、違法行為が確認できない場合は被害に遭わないための防犯指導を行っている。
・　ＩＰＡは、「コンピュータ不正アクセス対策基準」（平成８年通商産業省告示第362号。以下「不正アクセス対策基準」という。）に該当する行為について被害の有無に関係なく届出を受け付け、毎月統計情報を公表するとともに、注意喚起を発信している。客観的に不正アクセス行為を受けていると判断できない場合は、相談レベルで対応している。
・　JPCERT/CCは、不正アクセス行為や不正プログラム感染等に悪用されているウェブサイト等について、被害者の問題を解決し被害の拡大を防止するため、報告や攻撃の停止、サイト閉鎖等に関する対応調整依頼を受け付けている。

また、不正アクセス行為や被害のカテゴライズもそれぞれの受理機関独自のルールであるため、集約して統計データを作成することへの障害となっている。

② 取組の趣旨

現状の問題を解決するためには、それぞれの受理機関が現在行っている作業手順について、カテゴリ、用語、判断基準等整合できる部分を整合し、目的によって異なる部分をお互いに認識し、届出者に対して適切な対応ができるマニュアルを作成することが有効である。

③ 配意事項

マニュアルの検討に当たっては、受理機関の受付担当者ごとに判断が異ならないように、なるべくチェックリストや定量的な判断基準を示すよう心掛ける。

また、マニュアルの中で届出事項を示す場合には、大口の届出者に当たる民間事業者やその委託を受けたサイバー犯罪警戒防止事業者等の意見を参考にして検討する。

(ｳ) 不正アクセス行為リポートの作成・公表

・　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

取組主体：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。

① 現状

不正アクセス行為の手口に関する情報については、届出等受理機関がそれぞれの目的に合わせて収集しており、内容、形式や用語についても統一されていない。

また、情報の発信の頻度は、発信主体によって隔週から年一度と様々であり、内容についての技術的な難度も多様となっている。そのため、実務者が必要とするときに十分な情報を的確に把握できる状態であるとはいえない。

② 取組の趣旨

実務者が活用できる情報を発信するためには、届出等受理機関が定期的な情報交換及び共有を実施できる体制を構築し、維持・運用することが必要である。

この体制によって共有された情報は、発信する情報の範囲や難度に応じた形式及び期間の設定に有効であり、用語の統一についても期待できる。

③ 配意事項

共有する情報の内容には、他の届出等受理機関と共有することが難しい項目が多く含まれており、それをもって、共有をしないという判断に偏らないよう、具体的かつ技術的な解決策を持って形式を策定するよう配慮が必要である。

情報発信の在り方については、どの届出等受理機関がどういった難度や範囲及び時期に情報を発信しているか把握するようにある程度の配慮が必要である。

(2) 普及啓発方策

ア 普及啓発内容の斉一化

(ｱ) ポータルサイトの充実

取組主体：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。

① 現状

現在は、それぞれの団体・企業等が独自にポータルサイトを開設しており、内容も自らの業務に関わる部分の情報のみの場合が多い。そこにアクセスすれば全ての情報セキュリティ関連情報にアクセスできるような網羅的なポータルサイトが存在しないため、利用者は、自分が必要とする情報が掲載されているポータルサイトを自ら検索して探さなければならず、使いやすさの低下を招いている。

ポータルサイトによっては、メンテナンスされず放置されているようなサイトもあり、掲載されている情報が必ずしも最新のデータに基づいていない場合がある。

② 取組の趣旨

現状の問題を解決するためには、情報セキュリティに関するポータルサイトから、利用者が必要とする情報を容易にアクセスすることができるようにすることが必要である。また、情報処理の促進に関する法律（昭和45年法律第90号）に基づき情報処理の高度化の推進を目的として設置された独立行政法人であるＩＰＡは、これまで企業等への情報セキュリティ対策の活動を多く手掛けていること、一般利用者向けの情報セキュリティ対策も手掛けていることなどから、官民意見集約委員会の取組を集約する立場として適任である。

③ 配意事項

「官民ボード・ポータルサイト」（仮称）の運営に当たっては、偽の情報を掲載している団体・企業等が参入しないよう配意する。また、「官民ボード・ポータルサイト」（仮称）に掲載された情報が古く、信頼できないものになることを防ぐため、適切に更新が行われるよう配意する。加えて、公的性質を有するＩＰＡの認知度を向上させることなどにより、ＩＰＡによる「官民ボード・ポータルサイト」（仮称）が信頼の置けるサイトであることをインターネット利用者に認識させ、当該ポータルサイトの利用が促進されるよう配意する。

(ｲ) 既存資料の相互利用

取組主体：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。

① 現状

官民を含め、各組織・企業から、情報セキュリティの普及啓発に関する様々な資料が作成され、それぞれのルートを通じて配布されている。しかし、相互の情報共有がなされていないため、互いにどのような資料が存在するかさえ、把握できていない。このため、各組織・企業は、他者が作成した資料を適切なユーザに紹介できないばかりか、類似の資料を作成してしまう可能性もある。

各組織・企業で個々に作成された情報セキュリティの普及啓発に関する資料は、有効活用が十分には図られていないのが現状である。

② 取組の趣旨

各組織・企業が個別に作成・保有している情報セキュリティの普及啓発に関する資料の相互利用を推進することで、自組織・企業で保有していない資料についてもユーザに提供することが可能になり、また、他者が既に作成済みの類似資料の重複作成も回避できる。

また、相互利用可能となった資料については「官民ボード・ポータルサイト」（仮称）からの一元提供を推進することで、ユーザの利便性を向上する。

③ 配意事項

「官民ボード・ポータルサイト」（仮称）のリンク等に民間事業者を加える場合に、どのような組織や企業であれば安心して紹介できるか、また製品紹介と啓発資料の切り分けをどのようにすべきか、「官民ボード・ポータルサイト」（仮称）を運営するＩＰＡが主体となって基準を作成しておく必要がある。さらに、官民を含めた各組織・企業間での資料の一部引用、一般ユーザでの資料の一部引用等について、利用に関する制限事項等のすり合わせが必要である。

また、運用時には、コンテンツ作成元の継続的なアップデートが必要である。

イ　有機的かつ重層的な普及啓発

(ｱ)　生徒・学生・保護者・教育機関を対象とした普及啓発

取組主体：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。

①　現状

生徒・学生・保護者・教育機関向けの体験教室や講演等は、例えば、学校と警察が連携して実施している講演会等や、総務省と文部科学省を中心として実施されているe－ネットキャラバン等が数多く行われているが、情報セキュリティに関する事項は多く取り扱われていない。また、情報セキュリティに特化した周知啓発活動については、一部の情報セキュリティ関連事業者による夏休み情報セキュリティ教室が行われているが、取組としては余り多くはない。

講習以外の関連した現在の活動としては、ＩＰＡ主催の「ＩＰＡ情報セキュリティ標語・ポスターコンクール」や日本オンラインゲーム協会とその加盟各社による、不正アクセス対策のためのワンタイムパスワードの導入・ワンタイムパスワード利用促進の周知啓発活動等が挙げられるが、更に活動を活発化させることが望まれている。

②　取組の趣旨

生徒・学生等は携帯電話等を利用してソーシャル・ネットワーキング・サービス（ＳＮＳ）やオンラインゲームに多く触れているが、セキュリティ意識や知識の低さから、不正アクセス行為の被害を受けたり、逆

に安易に不正アクセス行為に及んだりしていることがある。生徒・学生等に対する情報セキュリティの普及啓発の重要性は高いことから、生徒・学生等の興味を引く題材を利用した取組を推進していく。

また、生徒・学生等に効率的に普及啓発するため、情報セキュリティに特化した新たな取組を実施していくことと併せて、学校関係者等からの依頼による講演会等で情報セキュリティに関するチラシ等の配布を検討するなど既存の全般的な取組の中に情報セキュリティの項目を盛り込むことを推進する。

③　配意事項

カリキュラムが多い教育現場において、新たに情報セキュリティの周知啓発活動に時間や工数を割く理解を得られるか、配意しなければならない。ポスター等で訴求する方法については、例えば、生徒・学生の興味を引くオンラインゲームをテーマにした内容は、周知という観点でも事件数を減らすという意味でも有効であると考えられる。本業と関係が薄い内容を掲示することについて、学校関係者等の理解を得る必要がある。

(ｲ)　一般利用者（高齢者等を含む。）を対象とした普及啓発

取組主体：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。

①　現状

パソコンの習熟度には個人により差がある。会社員等パソコンを利用する機会の多い利用者においては習熟度が高い一方で、パソコンを利用する機会が少なく、習熟度が相対的に低い利用者もいる。

また、情報セキュリティ対策を適切なレベルで行えていない現状がある。セキュリティソフトを例として挙げた場合、ＩＰＡの調べによると、

セキュリティソフトの利用者のうち、10%強がパターンファイル・更新ファイルを更新していない状況となっている（2008年度第１回情報セキュリティに関する脅威に対する意識調査報告書）。加えて、不正プログラムの感染等により、インターネットバンキングのＩＤ・パスワードを詐取するケースもあるため、セキュリティソフトの適切な更新が行われていないと、利用者が危険にさらされることもある。現に、不正プログラムの感染やフィッシング等により、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が相次いでおり、平成23年11月24日現在の警察庁調べによると、平成23年３月末以降、56金融機関で未遂も含め160口座が被害を受け、不正送金被害総額は約３億円に上る。また、ボットに感染した場合、自宅のパソコンが攻撃者の踏み台として利用される場合があり、被害者ではなく加害者にもなり得ることが想定される。

② 取組の趣旨

パソコンの習熟度が低い利用者は情報セキュリティ対策のレベルも十分でなく、また、家庭内において多くの時間を過ごす専業主婦や高齢者等に対しては、各組織・企業が実施している情報セキュリティに関する普及啓発活動もリーチしづらいという問題がある。これら情報セキュリティに関心が薄い一般利用者に対して訴求力のある対策を実施するため、可能な限り簡潔で広域に普及できる方法を用いる必要がある。

③ 配意事項

インターネット初心者に対する普及啓発には、分かりやすい言葉を使った資料を作成したり、高齢者に対しては、字を大きく記載した読みやすい資料を作成したりするなど、アクセシビリティに配意する。また、情報セキュリティに興味がない人の関心を引くため、動画を活用することも検討する。

(ｳ) 企業経営者を対象とした普及啓発

取組主体：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。

① 現状

企業の経営陣が、自社で保有する情報の価値を正しく認識し、リスク管理の一環として情報セキュリティ対策を推進することは、今や企業の経営課題の一つと認識されている。企業経営者や情報セキュリティ担当役員、管理者向けに実施された各種アンケートの結果でも、主要なリスクの中で最も重視するものとして「サイバー攻撃」等が挙げられている。しかしながら、セキュリティを十分に考慮した上で、しっかりとしたセキュリティ・システムを構築していると思われる比較的規模の大きい企業から知財情報や個人情報が漏えいするという事件が絶えない。上記のような実情を考慮した上で、企業経営者向けの普及啓発を改めて考える必要が生じている。

② 取組の趣旨

情報セキュリティ対策が企業経営者の責務であるという意識が希薄な経営者がいまだにいる現状を踏まえ、企業経営者に対して情報セキュリティ・インシデント発生時の被害実態や対策方法についての普及啓発に努め、企業において適正な情報セキュリティ対策が講じられるよう働き掛けていく必要がある。

③ 配意事項

企業経営者に対しては、情報セキュリティ対策が経営上のリスク管理の一環として事業リスクと同列に扱うべき問題であることを認識していただくよう配意することを第一とする。その後に、リスク管理に必要な考え方である、「ベースライン：必要最低限の事項とレベルを決める」、「ポリシーベース：客観的かつ論理的な根拠に基づいて環境整備を行う」、「ライフサイクル：定期的なチェック及び必要に応じて見直しを実行する」を理解して実践してもらうよう配意する。

また、リスク管理には然るべき資金と労力を継続的に投資することが必要であり、セキュリティ対策もその例外とはなり得ないという現実を理解して対策を講じてもらうよう配意することも必要である。

＊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。

(エ) 中小企業を対象とした普及啓発

取組主体：経済産業省、ＩＰＡ、情報セキュリティ関連事業者等

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。

① 現状

中小企業では、情報セキュリティに対するリスクの認識が少ないため、ＩＰＡでは、中小企業向けに、「５分でできる！自社診断パンフレット」等を作成した。これは、情報資産の洗い出し、リスク分析、セキュリティポリシーの策定等、本来の情報セキュリティマネジメント手法では実施が難しい中小企業に対して、入門レベルとして最初に取り組むべき情報セキュリティ対策の自社診断シートである。また、「中小企業のためのクラウドサービス安全利用の手引き」を公表するなど、新しい取組も行っている。さらに、経済産業省では、中小企業向けの情報セキュリティ指導者育成セミナーを全国で開催し、人材の育成を図っている。

しかし、中小企業への浸透はまだまだ難しく、様々なチャネルを通じたアプローチが必要とされている。

② 取組の趣旨

中小企業では、人的・金銭的なリソースの不足から情報セキュリティ対策が後回しにされることがあり、コストを低く抑えた導入しやすい情報セキュリティ対策を推進し、セキュリティ意識を向上させていく必要があるため、ＩＰＡが中小企業向けに作成している自社診断シートや手引き等を踏まえた対策を推進するとともに、一般セミナー等においても情報セキュリティ対策の内容を盛り込むことで、セキュリティ意識向上の機会を提供していく。

③ 配意事項

全国の様々な企業規模、業種にわたる中小企業に、情報セキュリティを浸透させるためには、関係各機関や民間の協力の下に、あらゆる機会を捉えて普及啓発を推進することが必要である。また、多様な中小企業のそれぞれに応じた様々な資料の提供に配意する。情報ネットワークインフラを利用する一員として、最低限の情報セキュリティ対策は講じなければならないという自覚を醸成する。

(オ) 官公庁・地方公共団体を対象とした普及啓発

取組主体：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。

① 現状

- 各府省は、府省内の情報セキュリティ関係規程に基づき、情報セキュリティ教育資料を用いるなどして、職員に対し、教育・意識啓発に関する活動を実施している。また、職員の情報セキュリティ対策の実施状況を年１回点検し、当該活動等の評価を実施している。

  ＮＩＳＣは、「政府機関の情報セキュリティ対策のための統一管理基準」（平成23年４月21日情報セキュリティ政策会議決定。以下「統一管理基準」という。）等を策定するほか、情報セキュリティ教育資料のひな形を作成するなどし、各府省の取組を支援している。また、各府省庁は、電子政府利用促進週間、情報セキュリティ月間等の機会を捉え、直近の事故・事例を踏まえた意識啓発を行っている。
- 地方公共団体は、総合行政ネットワーク内の情報セキュリティに関する取組事例や情報セキュリティに関する解説を活用するなどして、情報セキュリティ対策水準向上のための普及・啓発活動を実施している。

② 取組の趣旨

各府省における情報セキュリティ対策については、ＮＩＳＣが策定した統一管理基準等に基づいて実施されており、また、地方公共団体についても総合行政ネットワークを通じて様々な取組が行われていることから、既存の取組を検証・改善しながら一層の推進に努める。

③ 配意事項

公的機関の保有する情報の重要性を認識し、全ての国の機関・地方の機関が取組に含まれるよう配意する。

研修内容の形骸化を避けるため、具体的な事例を踏まえつつ、研修内容の更新を行っていく。

情報の取扱いの意思決定及び組織内のセキュリティ対策に責任を持つ管理者向けの教育にも配意する。

(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

取組主体：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。

① 現状

警察においては、警察安全相談等を通じて、不正アクセス行為の被害の相談等を受け付けている。

ＩＰＡにおいては、不正アクセス対策基準に基づき、不正アクセス行

為の被害届出を受け付けており、情報セキュリティ安心相談窓口では不正アクセス行為に関わる相談に応じている。

JPCERT/CCにおいては、インシデント対応支援組織として、フィッシングサイトや不正プログラム配布サイトの閉鎖、不正アクセス行為の攻撃元に対する連絡、対処要請等の対応依頼や相談を受け付け、国内外の関係機関等の協力を得つつ、問題となっているサイトの閉鎖や攻撃の停止等の調整に当たっている。

しかしながら、相談・届出の窓口が十分に認知されていないことに加え、不正アクセス行為に関する一般的な相談や不正アクセス罪等での事件化のための相談等の異なる状況において何を相談者等が準備しておくべきかが認知されていない状況にある。このような状況は、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などの理由とともに、不正アクセス行為が潜在化する原因となっている。

② 取組の趣旨

不正アクセス行為の適正な実態把握のため、不正アクセス行為の被害者等が漏れなく適切な相談・届出窓口に相談・届出を行うことが不可欠である。この場合において、被害等の相談に必要となる情報と犯罪捜査のために必要な情報は異なっていることから、状況に応じた窓口・必要な情報等の周知を図り、円滑な相談・届出が行われるよう努めることが必要である。

③ 配意事項

相談・届出担当者等は、各相談・届出窓口が扱う概要等を十分に理解し、必要に応じ、適切な窓口への円滑な引継ぎができるよう努める。また、各窓口での相談・届出の範囲等のホームページ掲載に当たっては、分かりやすい説明となるよう工夫する。相談・届出等の際に必要な情報の周知に当たっては、当該情報の内容にぶれがないよう留意する。

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各機関は、相談者等からの相談等に適切に対応できるよう、担当者の教育を推進する。

ウ 最新の技術動向を踏まえた的確な情報提供

取組主体：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。

① 現状

スマートフォンやタブレット型端末の爆発的な増加、各種ＳＮＳ等の普及は、幅広い層のユーザが、今までにない高度な端末を通じて、プライバシーを含む多くの情報を交換する環境を生み出している。こうした環境は、利便性の向上をもたらす一方、コンピュータの知識やネットワーク上のリスクと安全性の確認に関して知識が低い、高齢者層や若年層を含む利用者が増大することによるリスクも伴っている。

スマートフォンについては、平成22年後半にスマートフォン向け不正プログラムが実際に発見されるなど、今後、攻撃者の悪意に基づくサイバー攻撃への加担や、個人情報・組織の重要情報の漏えいといった、攻撃・犯罪の道具として悪用される可能性を秘めている。総務省では「スマートフォン・クラウドセキュリティ研究会」を開催し、携帯電話事業者や端末製造事業者、関係事業者団体等が利用者に対して啓発すべき内容や伝達手段について、平成23年12月、中間報告を取りまとめたところである。

② 取組の趣旨

新しい技術、新しいサービスには、新しい情報セキュリティ上の問題があるが、市場発展期においては、それらの問題が表面化していない場合もあるため、利用者に対しては、新しい技術やサービスにおいては解決されていない情報セキュリティの問題があるということの理解を深め、リスク回避のための普及啓発活動を実施していく必要がある。

③ 配意事項

危険性を極端にあおることは避けながらも、関連事業者（通信事業者、端末製造事業者、サービス提供事業者等）に協力を求めながら幅広いユーザ層へ届くように広報啓発活動を推進する。

官民ボードのポータルサイトにおいて適切な問合せ窓口への案内方法を検討する。

(3) 不正アクセス行為対応方策

ア フィッシング対策の推進

(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

取組主体：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。

① 現状

フィッシングや、フィッシングによって詐取されたＩＤ・パスワードを用いた金銭的被害が依然として発生しており、その手口も高度化しつつある。他方で、その実態は不明な部分が多く、サービス利用者が気付かないうちに被害に遭っていることもある。

② 取組の趣旨

現状の問題を解決するためには、フィッシングの発生を早期に認知するとともに、認知したフィッシングに対し、フィッシングサイトの閉鎖等の取組を速やかに実施することが必要である。また、フィッシングは、詐称された事業者（ブランドの所有者）、事業者の顧客（サービス利用者）、詐称のために悪用されたサイト（フィッシングサイト）に係るサーバ運営者といった複数の関係者が存在し、それぞれにおいてフィッシング対策の取組が必要となることから、関係機関の連携が必要である。

③ 配意事項

フィッシングを事件化する場合、捜査に必要な証拠保全措置を行いつつ、被害の発生及び拡大を防止するためにフィッシングサイト閉鎖等も行う必要があることから、関係機関の適切な連携により、これらの措置が両立できるよう配意する。

(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

取組主体：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。

① 現状

フィッシング対策として、フィッシング対策協議会による注意喚起、JPCERT/CCによるフィッシングサイトの閉鎖の調整等の活動が行われており、各事業者においても個別にフィッシング対策として技術的な対応を行っている。また、警察においては、フィッシング行為の後に発生した不正アクセス行為や不正アクセス行為による金銭的被害等を認知した段階で取締りを開始している。しかしながら、閉鎖の調整や取締りは後手の対応となっており、フィッシング行為による被害を未然に防止できない状況が続いている。

② 取組の趣旨

フィッシング対策としては、フィッシングサイトの閉鎖等、既に行われたフィッシングによる被害を防止するための取組と並行して、利用者への啓発や技術的な対応策等の推進及びフィッシング行為による被害を未然に防止するための新たなフィッシング対策の在り方を検討することが必要である。

③ 配意事項

技術的対応策については、利便性の低下に伴うサービス利用者の減少等、その対応策の実施によって発生する副作用に配意する。また、法規制化の検討に当たっては、一般国民の自由な活動の阻害や民間サービスの萎縮を生じさせるおそれがないかを慎重に見極めるとともに、その規制に基づく捜査の際には、誤った逮捕者が出ないよう、慎重な捜査を推進する必要がある。

イ　不正ログイン対策の推進

(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

取組主体：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。

①　現状

近年、不正アクセス行為の手口として連続自動入力試行攻撃が認知されており、一度の攻撃で相当程度高い頻度でアクセス制御機能を突破していることが確認されている状況にある。

しかしながら、アクセス管理者から警察に対する通報が十分になされていないことから、このような攻撃についての警察の情報把握が十分ではなく、取締りも進んでいない状況にある。

②　取組の趣旨

連続自動入力試行攻撃を抑止するためには、警察による取締りが行われることが必要である。また、捜査活動を通じて、当該攻撃に用いられるＩＤ・パスワードのデータの不正流通の実態を把握することが期待できる。

③　配意事項

・　アクセス管理者からの通報の促進については、３(1)ア(ｲ)の「通報指針策定による通報の促進」の取組による。

・　警察が取締りを行うに当たっては、把握した情報を分析した上で対象事件や捜査手法の選定を行い、効率的かつ効果的な取締りを行うよう配意する。

・　警察の捜査活動によってアクセス管理者の企業活動に過剰な負担をかけないように配意する。

(ｲ)　ＩＤ・パスワードのリストの不正流通への対策の強化

取組主体：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。

①　現状

近年、利用者によるＩＤ・パスワードの使い回しを背景に、ある企業から流出したＩＤ・パスワードのリストが他の企業への不正アクセス行為のために収集・蓄積されているものとみられているが、その実態は適切に把握されているとは言い難い状況にある。また、ＩＤ・パスワードの使い回しの危険性が利用者に周知され、その対策が取られているとは言い難い状況にある。

②　取組の趣旨

識別符号リストの不正流通の防止を図ることにより、不正ログインが減少することが期待できる。

③　配意事項

利用者への注意喚起や啓発に当たっては、利用者の取組が実効性のあるものとなるように配意する。

また、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に当たっては、セキュリティレベルを高めることなどを目的とした民間事業者等による正当な取組が阻害されないように配意する。

(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

取組主体：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

① 現状

金融機関等、特に高いセキュリティが求められるウェブサイトでは乱数表やワンタイムパスワード等の導入が進む一方で、利用者規模の小さい金融機関や一般の民間のウェブサイトでは導入が進んでいない現状がある。また、不正ログイン対策の技術方式として、乱数表とワンタイムパスワード以外に何があるかについて、十分に知られているとは言い難い状況にある。

さらに、安易なパスワードを許してしまったり、パスワードリマインダが脆弱(ぜいじゃく)で容易に他人のパスワードを変更できてしまったりするなど、パスワードの発行・再発行に係る手続の設計が不適切なウェブサイトが散見されているが、こうしたウェブサイトの仕様上の問題はこれまで余り議論されておらず、放置されている現状がある。

② 取組の趣旨

アクセス管理者が執り得る不正ログイン対策措置について洗い出して整理することで、様々なアクセス管理者の業態や必要性に応じた不正ログイン対策措置の実施が期待できる。

③ 配意事項

- 対策技術の効果については、実態を踏まえた検証と評価が必要である（例えば、乱数表の有無による被害件数の差から定量的な評価を試みるなど）。
- 対策技術の導入には一定のコストを要するほか利用者の利便性を低下させるなどの副作用があること、企業の活動内容は多様であることなどから、企業の活動内容に見合った不正ログイン対策の水準を画一的に示すことは容易でなく、また、国際水準や他の基準との整合性の観点から、安易に画一的な水準を示すべきではない点に配意する。

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

(ｱ)　「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

取組主体：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

①　現状

ＩＰＡとJPCERT/CCは、平成16年から、脆弱性取扱基準に基づき、主に国内のソフトウェア製品やウェブサイトに関する脆弱性情報の届出を受け付け、ソフトウェア製品開発者やウェブサイト運営者に対して脆弱性の解消を働き掛ける活動を行っている。しかし、潜在的な脆弱性はまだ多く存在すると考えられ、攻撃者が発見するよりも前に、ソフトウェア製品開発者やウェブサイト運営者が事前に脆弱性を把握し対策を行うことが必要である。

＊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。

② 取組の趣旨

脆弱性対策ホームページを作成し、関係省庁のサイトでリンクを張るなど紹介を行うことで、脆弱性取扱基準に基づく脆弱性対策の取組の認知度が上がり、当該取組が更に活性化することが期待できる。

③ 配意事項

現に運用している他人のウェブサイトの脆弱性を発見する場合、手法によってはその発見行為が不正アクセス行為となるおそれがあることから、脆弱性の発見行為は、情報セキュリティ早期警戒パートナーシップガイドライン*7等を十分理解の上、法律に反しない範囲で行う必要があることを周知する必要がある。

(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。）

取組主体：アクセス管理者

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。

① 現状

情報システムの脆弱性を低減するための様々な取組が行われてきており、一定の効果を挙げているものの、システムの脆弱性を完全になくすことは困難である。また、既存のファイアウォールや侵入検知システム、侵入防止システム等、システムの入口で攻撃を防ぐ「境界防御」の仕組みは、ＵＳＢメモリによるシステム内部からの不正プログラム感染や、特定の個人をターゲットとした標的型攻撃への対策としては効果が薄

＊7 脆弱性関連情報の適切な流通により、コンピュータウイルス、不正アクセス等による被害発生を抑制するために、関係者及び関係業界と協調して国内におけるソフトウェア等の脆弱性関連情報を適切に扱うための指針をいう。

い。さらに、新種や亜種を含めた不正プログラムの発生頻度にウイルス対策ソフトのシグネチャ（パターンファイル）の更新が追い付かず、シグネチャベースの対策にも一定の限界がある。

② 取組の趣旨

セキュリティ・ホール攻撃対策にはシステムの脆弱性の把握及び解消が基本ではあるものの、脆弱性を完全になくすことは困難であることから、セキュリティ・ホール攻撃が行われることを前提とし、その上で被害の発生及び拡大を防止するための取組が必要である。

③ 配意事項

ＵＲＬやＩＰアドレスのレピュテーションの利用に際しては、偽陽性（正当な通信を不正と判断）や偽陰性（不正な通信を正当と判断）をゼロにはできない点に配意する。

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

取組主体：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。

① 現状

昨今、大手先端企業等に対し、機密情報の窃取等を目的としたサイバー攻撃が行われているなど不正アクセス行為等の手法が高度化・複雑化してきている。これらの攻撃手法の中には、企業秘密に関する事項等が

含まれていることもあることから、他社への情報共有が進んでいない。

このため、経済産業省においては、重要インフラ等に利用されている機器の製造業者等を中心にサイバー情報共有イニシアティブを発足させ、情報共有が円滑になされるような体制の検討を開始した。

また、警察庁においては、先端技術を有する全国の事業者等とのネットワークを構築し、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、これを事業者等に提供して注意喚起等を実施している。

② 取組の趣旨

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とで、同様の手法による不正アクセス行為等の未然防止や被害拡大を防ぐ。これらの情報共有を円滑にするためには、対策に有効となる共有すべき情報の内容や範囲等の情報共有ルール等を整備し、対応能力の向上を図る必要がある。

③ 配意事項

- 不正アクセス行為等の手法の中には、個社に関する情報が含まれることがあるため、当該個社情報の匿名化に配慮した上で、情報共有する必要がある。
- 発生した不正アクセス行為等の情報を迅速に、共有できる体制を検討する必要がある。

4 参考資料

- 参考資料１　不正アクセス防止対策に関する行動計画
- 参考資料２　不正アクセス行為の禁止等に関する法律
- 参考資料３　ソフトウェア等脆弱性関連情報取扱基準
- 参考資料４　情報システム安全対策指針
- 参考資料５　コンピュータ不正アクセス対策基準

参考資料１　不正アクセス防止対策に関する行動計画

平成２３年１２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。

参考資料２ 不正アクセス行為の禁止等に関する法律

不正アクセス行為の禁止等に関する法律

〔平成十一年八月十三日号外法律第百二十八号〕

〔総理・法務・通商産業・郵政大臣署名〕

〔沿革〕

不正アクセス行為の禁止等に関する法律をここに公布する。

不正アクセス行為の禁止等に関する法律

（目的）

第一条　この法律は、不正アクセス行為を禁止するとともに、これについての罰則及びその再発防止のための都道府県公安委員会による援助措置等を定めることにより、電気通信回線を通じて行われる電子計算機に係る犯罪の防止及びアクセス制御機能により実現される電気通信に関する秩序の維持を図り、もって高度情報通信社会の健全な発展に寄与することを目的とする。

（定義）

第二条　この法律において「アクセス管理者」とは、電気通信回線に接続している電子計算機（以下「特定電子計算機」という。）の利用（当該電気通信回線を通じて行うものに限る。以下「特定利用」という。）につき当該特定電子計算機の動作を管理する者をいう。

２　この法律において「識別符号」とは、特定電子計算機の特定利用をすることについて当該特定利用に係るアクセス管理者の許諾を得た者（以下「利用権者」という。）及び当該アクセス管理者（以下この項において「利用権者等」という。）に、当該アクセス管理者において当該利用権者等を他の利用権者等と区別して識別することができるように付される符号であって、次のいずれかに該当するもの又は次のいずれかに該当する符号とその他の符号を組み合わせたものをいう。

一　当該アクセス管理者によってその内容をみだりに第三者に知らせてはならないものとされている符号

二　当該利用権者等の身体の全部若しくは一部の影像又は音声を用いて当該アクセス管理者が定める方法により作成される符号

三　当該利用権者等の署名を用いて当該アクセス管理者が定める方法により作成される符号

３　この法律において「アクセス制御機能」とは、特定電子計算機の特定利用を自動的に制御するために当該特定利用に係るアクセス管理者によって当該特定電子計算機又は当該特定電子計算機に電気通信回線を介して接続された他の特定電子計算機に付加されている機能であって、当該特定利用をしようとする者により当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号（識別符号を用いて当該アクセス管理者の定める方法により作成される符号と当該識別符号の一部を組み合わせた符号を含む。次条第二項第一号及び第二号において同じ。）であることを確認して、当該特定利用の制限の全部又は一部を解除するものをいう。

（不正アクセス行為の禁止）

第三条　何人も、不正アクセス行為をしてはならない。

２　前項に規定する不正アクセス行為とは、次の各号の一に該当する行為をいう。

一　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）

二　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。）

三　電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為

（不正アクセス行為を助長する行為の禁止）

第四条　何人も、アクセス制御機能に係る他人の識別符号を、その識別符号がどの特定電子計算機の特定利用に係るものであるかを明らかにして、又はこれを知っている者の求めに応じて、当該アクセス制御機能に係るアクセス管理者及び当該識別符号に係る利用権者以外の者に提供してはならない。ただし、当該アクセス管理者がする場合又は当該アクセス管理者若しくは当該利用権者の承諾を得てする場合は、この限りでない。

（アクセス管理者による防御措置）

第五条　アクセス制御機能を特定電子計算機に付加したアクセス管理者は、当該アクセス制御機能に係る識別符号又はこれを当該アクセス制御機能により確認するために用いる符号の適正な管理に努めるとともに、常に当該アクセス制御機能の有効性を検証し、必要があると認めるときは速やかにその機能の高度化その他当該特定電子計算機を不正アクセス行為から防御するため必要な措置を講ずるよう努めるものとする。

（都道府県公安委員会による援助等）

第六条　都道府県公安委員会（道警察本部の所在地を包括する方面（警察法（昭和二十九年法律第百六十二号）第五十一条第一項本文に規定する方面をいう。以下この項において同じ。）を除く方面にあっては、方面公安委員会。以下この条において同じ。）は、不正アクセス行為が行われたと認められる場合において、当該不正アクセス行為に係る特定電子計算機に係るアクセス管理者から、その再発を防止するため、当該不正アクセス行為が行われた際の当該特定電子計算機の作動状況及び管理状況その他の参考となるべき事項に関する書類その他の物件を添えて、援助を受けたい旨の申出があり、その申出を相当と認めるときは、当該アクセス管理者に対し、当該不正アクセス行為の手口又はこれが行われた原因に応じ当該特定電子計算機を不正アクセス行為から防御するため必要な応急の措置が的確に講じられるよう、必要な資料の提供、助言、指導その他の援助を行うものとする。

２　都道府県公安委員会は、前項の規定による援助を行うため必要な事例分析（当該援助に係る不正アクセス行為の手口、それが行われた原因等に関する技術的な調査及び分析を行うことをいう。次項において同じ。）の実施の事務の全部又は一部を国家公安委員会規則で定める者に委託することができる。

３　前項の規定により都道府県公安委員会が委託した事例分析の実施の事務に従事した者は、その実施に関して知り得た秘密を漏らしてはならない。

４　前三項に定めるもののほか、第一項の規定による援助に関し必要な事項は、国家公安委員会規則で定める。

第七条　国家公安委員会、総務大臣及び経済産業大臣は、アクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に資するため、毎年少なくとも一回、不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況を公表するものとする。

２　前項に定めるもののほか、国は、アクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に関する啓発及び知識の普及に努めなければならない。

（罰則）

第八条　次の各号の一に該当する者は、一年以下の懲役又は五十万円以下の罰金に処する。

一　第三条第一項の規定に違反した者

二　第六条第三項の規定に違反した者

第九条　第四条の規定に違反した者は、三十万円以下の罰金に処する。

附　則

この法律は、公布の日から起算して六月を経過した日から施行する。ただし、第六条及び第八条第二号の規定は、公布の日から起算して一年を超えない範囲内において政令で定める日から施行する。

〔平成一一年一一月政令三七四号により、平成一二・七・一から施行〕

〔平成一一年一二月二二日法律第一六〇号抄〕

（処分、申請等に関する経過措置）

第千三百一条　中央省庁等改革関係法及びこの法律（以下「改革関係法等」と総称する。）の施行前に法令の規定により従前の国の機関がした免許、許可、認可、承認、指定その他の処分又は通知その他の行為は、法令に別段の定めがあるもののほか、改革関係法等の施行後は、改革関係法等の施行後の法令の相当規定に基づいて、相当の国の機関がした免許、許可、認可、承認、指定その他の

処分又は通知その他の行為とみなす。

2　改革関係法等の施行の際現に法令の規定により従前の国の機関に対してされている申請、届出その他の行為は、法令に別段の定めがあるもののほか、改革関係法等の施行後は、改革関係法等の施行後の法令の相当規定に基づいて、相当の国の機関に対してされた申請、届出その他の行為とみなす。

3　改革関係法等の施行前に法令の規定により従前の国の機関に対し報告、届出、提出その他の手続をしなければならないとされている事項で、改革関係法等の施行の日前にその手続がされていないものについては、法令に別段の定めがあるもののほか、改革関係法等の施行後は、これを、改革関係法等の施行後の法令の相当規定により相当の国の機関に対して報告、届出、提出その他の手続をしなければならないとされた事項についてその手続がされていないものとみなして、改革関係法等の施行後の法令の規定を適用する。

（従前の例による処分等に関する経過措置）

第千三百二条　なお従前の例によることとする法令の規定により、従前の国の機関がすべき免許、許可、認可、承認、指定その他の処分若しくは通知その他の行為又は従前の国の機関に対してすべき申請、届出その他の行為については、法令に別段の定めがあるもののほか、改革関係法等の施行後は、改革関係法等の施行後の法令の規定に基づくその任務及び所掌事務の区分に応じ、それぞれ、相当の国の機関がすべきものとし、又は相当の国の機関に対してすべきものとする。

（罰則に関する経過措置）

第千三百三条　改革関係法等の施行前にした行為に対する罰則の適用については、なお従前の例による。

（政令への委任）

第千三百四十四条　第七十一条から第七十六条まで及び第千三百一条から前条まで並びに中央省庁等改革関係法に定めるもののほか、改革関係法等の施行に関し必要な経過措置（罰則に関する経過措置を含む。）は、政令で定める。

附　則〔平成一一年一二月二二日法律第一六〇号抄〕

（施行期日）

第一条　この法律（第二条及び第三条を除く。）は、平成十三年一月六日から施行する。ただし、次の各号に掲げる規定は、当該各号に定める日から施行する。

一　〔前略〕第千三百四十四条の規定　公布の日

二　〔略〕

附　則〔平成二三年六月二四日法律第七四号抄〕

（施行期日）

第一条　この法律は、公布の日から起算して二十日を経過した日から施行する。ただし、次の各号に掲げる規定は、当該各号に定める日から施行する。

一　〔略〕

二　第六条の規定　サイバー犯罪に関する条約が日本国について効力を生ずる日

三～五　〔略〕

〔経過措置〕

第七条　第六条の規定による改正後の不正アクセス行為の禁止等に関する法律第八条第二項の規定は、附則第一条第二号に掲げる規定の施行の日以後に日本国について効力を生ずる条約により日本国外において犯したときであっても罰すべきものとされている罪に限り、適用する。

第八条　施行日前にした行為に対する罰則の適用については、なお従前の例による。

○経済産業省告示第二百三十五号

ソフトウエア等脆弱性関連情報取扱基準を次のように定めたので、告示する。

平成十六年七月七日

経済産業大臣　中川　昭一

ソフトウエア等脆弱性関連情報取扱基準

Ⅰ．主旨

本基準は、ソフトウエア等に係る脆弱性関連情報等の取扱いにおいて関係者に推奨する行為を定めることにより、脆弱性関連情報の適切な流通及び対策の促進を図り、コンピュータウイルス、コンピュータ不正アクセス等によって不特定多数の者に対して引き起こされる被害を予防し、もって高度情報通信ネットワークの安全性の確保に資することを目的とする。

Ⅱ．用語の定義

本基準で用いられる用語の定義は、以下のとおりとする。

１．脆弱性

ソフトウエア等において、コンピュータウイルス、コンピュータ不正アクセス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所。ウェブアプリケーションにあっては、ウェブサイト運営者がアクセス制御機能により保護すべき情報等に誰もがアクセスできるような、安全性が欠如している状態を含む。

２．脆弱性関連情報

脆弱性に関する情報であって、以下に掲げる類型のいずれかに該当するもの。

（１）脆弱性情報

脆弱性の性質及び特徴を示す情報。

（２）検証方法

脆弱性が存在することを調べる方法。

（３）攻撃方法

脆弱性を悪用するプログラム、コマンド又はデータ及びそれらの使用方法。

３．対策方法

脆弱性によって生じる問題を解決又は回避するための方法であって、以下に掲げる類型のいずれかに該当するもの。

（１）回避方法

脆弱性を修正することなく、それが原因となって生じる被害を回避するための方法。

（２）修正方法

脆弱性を修正する方法。

４．ソフトウエア製品

ソフトウエア又はそれを組み込んだハードウエアであって、汎用性を有する製品。

５．ウェブアプリケーション

インターネット上のウェブサイトで稼働する固有のシステム。

６．コンピュータウイルス

コンピュータウイルス対策基準（平成７年通商産業省告示第４２９号）における「コンピュータウイルス」をいう。

７．コンピュータ不正アクセス

不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）における「不正アクセス行為」をいう。

Ⅲ．本基準における関係者の定義

本基準における関係者の定義は、以下のとおりとする。

１．発見者

脆弱性関連情報を発見又は取得した者。

２．受付機関

発見者が脆弱性関連情報を届け出るための機関。

３．調整機関

脆弱性関連情報に関して、製品開発者への連絡及び公表等に係る調整を行う機関。

４．製品開発者

ソフトウエア製品の開発等を行う者であって、以下のいずれかに該当する者。

（１）ソフトウエア製品を開発した者。

（２）（１）に掲げる者のほか、ソフトウエア製品の開発、加工、輸入又は販売に関する形態その他の事情からみて、当該ソフトウエア製品の実質的な開発者と認められる者。

５．ウェブサイト運営者

ウェブサイトを運営する者。

Ⅳ．本基準の適用範囲

本基準は、以下に掲げるものの脆弱性であって、その脆弱性に起因する被害が不特定多数の者に影響を及ぼし得るものに適用する。

１．日本国内で利用されているソフトウエア製品

（ソフトウエア製品において通信プロトコル等の仕様を実装した部分を含む。）

２．主に日本国内からのアクセスが想定されているウェブサイトで稼働するウェブアプリケーション

Ⅴ．対象がソフトウエア製品である場合の脆弱性関連情報取扱基準

一．発見者が製品開発者ではない、又は、発見者が製品開発者であり発見若しくは取得した脆弱性関連情報の影響範囲が自社のソフトウエア製品に限らない場合

対象がソフトウエア製品であり、かつ、発見者が製品開発者ではない、又は、発見者が製品開発者であり発見若しくは取得した脆弱性関連情報の影響範囲が自社のソフトウエア製品に限らない場合における脆弱性関連情報の取扱いの流れを以下に示す。

（ｉ）発見者は、脆弱性関連情報を受付機関に届け出る。

（ii）受付機関は、届出を受理した場合、一定の場合を除き、調整機関に当該脆弱性関連情報を通知する。

（iii）調整機関は、受付機関から通知された脆弱性関連情報を、製品開発者に速やかに通知するとともに、当該製品開発者が開発等を行ったソフトウエア製品における当該脆弱性の有無及びその新規性の検証結果について、当該製品開発者に報告を求める。

（iv）調整機関は、当該脆弱性情報の公表日を定める。

（ｖ）当該製品開発者は、当該脆弱性情報の公表日までに、対策方法を作成するよう努める。

（vi）受付機関及び調整機関は、当該脆弱性情報の公表日に、当該脆弱性情報、その日までに得られた製品開発者による当該脆弱性の有無及びその新規性の検証結果並びに当該脆弱性に関する対策方法、取組みの状況等を含む対応状況について、インターネット等を通じて公表する。

関係者における詳細な行動基準を以下に定める。

１．発見者基準

（１）発見者（自ら開発等を行ったソフトウエア製品に影響範囲が限られると認められる脆弱性関連情報を発見又は取得した製品開発者を除く。）は、発見又は取得した脆弱性関連情報を経済産業大臣が別に指定する受付機関に届け出ること。ただし、当該製品開発者に対し同じ内容を届け出ることを妨げない。

（２）発見者は、以下の点を明示した上で脆弱性関連情報を届け出ること。

①発見者の氏名、連絡先等の情報及びその取扱い

②脆弱性を有する製品の名称等

③当該脆弱性関連情報

（３）違法な方法により脆弱性関連情報を発見又は取得しないこと。

（４）発見者は、当該脆弱性情報が受付機関及び調整機関から公表されるまでの間、当該脆弱性関連情報を第三者に漏えいしないよう適切に管理すること。ただし、当該脆弱性関連情報を正当な理由により第三者に開示する場合､あらかじめ受付機関に問い合わせをすること。

２．受付機関基準

（１）受付機関は、１．（１）による届出が１．（２）で定めた届出事項を満たしているか否かを判断し、満たすと判断した場合、これを受理したものとし、当該発見者に対しその旨を

速やかに通知すること。また、届出を不受理とした場合、当該発見者に対しその旨及びその理由を速やかに通知すること。

（２）受付機関は、届出を受理したときは、速やかに、経済産業大臣が別に指定する調整機関に対し当該脆弱性関連情報を通知すること。ただし、当該脆弱性関連情報が以下に該当すると認められる場合、当該届出に係る処理を取りやめることができる。この場合においては、当該発見者にその旨及びその理由を通知すること。

①受付機関が既知の脆弱性関連情報であると確認した場合

②受付機関が調整機関から既知の脆弱性関連情報である旨の通知を受けた場合

③受付機関が脆弱性関連情報に該当しないと確認した場合

④受付機関が調整機関から脆弱性関連情報に該当しない旨の通知を受けた場合

⑤受付機関が違法な方法により発見又は取得されたおそれがあると認めた場合

（３）受付機関は、届出を受理した後においても、対策上必要と認められる場合、当該脆弱性関連情報について、当該発見者に問い合わせをすること。また、発見者からの問い合わせに対しては、調整機関と協議した上で、適切な情報を提供すること。その際、発見者の本人確認に留意すること。

（４）受付機関は、氏名、連絡先等の発見者を特定し得る情報を適切に管理し、当該発見者の同

意がない場合は他者（調整機関及び製品開発者を含む。）に開示しないこと。

（５）受付機関は、当該脆弱性情報が公表されるまでの間、当該脆弱性関連情報を第三者に漏えいしないよう適切に管理すること。ただし、対策上必要と認められる場合、当該脆弱性関連情報の適切な管理を前提として、第三者に分析を依頼することができる。

（６）受付機関は、対策方法が作成されてからそれが公表されるまでの間であって、当該脆弱性関連情報が、国民の日常生活に必要不可欠なサービスを提供するための基盤となる設備に重大な影響を与えるおそれがあると認められる場合、調整機関及び当該製品開発者と協議をした上で、政府機関等に当該脆弱性関連情報及び対策方法をあらかじめ通知することができる。その際、当該発見者に対して、その旨を事前に通知すること。

（７）受付機関は、調整機関が当該脆弱性情報を公表した場合には、その公表時期に合わせて当該脆弱性情報及び調整機関から当該脆弱性情報の通知を受けた製品開発者から報告された当該製品開発者の当該脆弱性に関する対策方法、取組みの状況等を含む対応状況（以下「対応状況」という。）を公表するとともに、当該発見者に対しその旨を通知すること。

（８）受付機関は、脆弱性に起因する被害の予防に資するため、脆弱性関連情報の届出状況等を公表すること。

３．調整機関基準

（１）調整機関は、脆弱性関連情報を製品開発者に適切に通知するために必要な製品開発者の名簿（以下「名簿」という。）を作成すること。その際、製品開発者と調整の上、当該製品開発者が調整機関との連絡をとるために設置した窓口を名簿に記載すること。

（２）調整機関は、受付機関から脆弱性関連情報の通知を受けた場合には、その内容に照らして当該脆弱性関連情報を通知すべき製品開発者を名簿から特定し、速やかに通知するとともに、当該製品開発者に対し、当該製品開発者のソフトウエア製品における当該脆弱性の有無及びその新規性を検証（以下「脆弱性検証」という。）しその結果を報告するよう求めること。また、名簿に記載のない製品開発者の中から新たに通知すべき者を特定した場合には、それを名簿に加えた上で、同様に通知を行い、脆弱性検証の結果を報告するよう求めること。

（３）調整機関は、製品開発者から脆弱性検証の結果報告を聴取し、その結果を踏まえつつ、対策方法の作成及び海外の調整機関との調整に要する期間、当該脆弱性情報の流出するリスク等の要素を考慮した上で、当該脆弱性情報を公表すべき日（以下「脆弱性情報公表日」という。）を定めるとともに、当該脆弱性情報公表日を受付機関及び当該製品開発者に通知すること。また、通知を行ったいずれの製品開発者からも脆弱性検証の結果報告が得られなかった場合には、国内外における脆弱性情報の取扱事例、海外の調整機関との調整に

要する期間、当該脆弱性情報の流出するリスク等の要素を考慮した上で、脆弱性情報公表日を独自に定め、同様に、受付機関及び当該製品開発者に通知すること。

（４）調整機関は、製品開発者から脆弱性情報公表日を変更したい旨の申し出を受けた場合、当該製品開発者から意見を聴取した上で、当該脆弱性情報公表日を変更することができる。脆弱性情報公表日を変更した場合、新たに定めた脆弱性情報公表日を受付機関及び当該脆弱性情報に関して通知を行った製品開発者に対し通知すること。

（５）調整機関は、通知を行った製品開発者に対して、脆弱性情報公表日までに当該製品開発者の対応状況を報告するよう求めること。

（６）調整機関は、脆弱性情報公表日に、当該脆弱性情報並びにその日までに得られた製品開発者による脆弱性検証の結果及び対応状況について、インターネット等を通じて公表すること。なお、通知を行った製品開発者が調整機関に脆弱性検証の結果及び対応状況のいずれか又は双方を報告しない場合、当該製品開発者の名称とともに、それらについて報告がない旨を公表することができる。

（７）調整機関は、脆弱性情報公表日までに通知を行ったすべての製品開発者から既知の脆弱性情報である旨の通知を受けた場合、その公表を取りやめることができる。公表を取りやめた場合、受付機関にその旨を通知すること。

（８）調整機関は、脆弱性情報公表日までに通知を行ったすべての製品開発者から脆弱性による影響がない旨の脆弱性検証の結果報告を受けた場合、受付機関から通知された情報は脆弱性関連情報には該当しないものと判断し、その公表を取りやめることができる。公表を取りやめた場合、受付機関にその旨を通知すること。

（９）調整機関は、脆弱性情報公表日までの間、当該脆弱性関連情報を第三者に漏えいしないよう適切に管理すること。ただし、対策上必要と認められる場合、当該脆弱性関連情報の適切な管理を前提として、第三者に分析を依頼し又は通知することができる。

４．製品開発者基準

（１）製品開発者は、調整機関と調整の上、調整機関と連絡をとるための窓口を設置し、調整機関に通知すること。

（２）製品開発者は、調整機関から通知された脆弱性関連情報に関して、遅滞なく脆弱性検証を行い、その結果を調整機関に報告すること。

（３）製品開発者は、当該脆弱性が他社のソフトウエア製品に含まれることが推定される場合には、その旨及びその理由を調整機関に通知すること。

（４）製品開発者は、脆弱性情報公表日までの間、当該脆弱性関連情報を第三者に漏えいしないよう適切に管理すること。

（５）製品開発者は、脆弱性情報公表日までに、対応状況を受付機関及び調整機関に報告するとともに、対策方法を作成するよう努めること。

（６）製品開発者は、対策方法を作成した場合、受付機関及び調整機関に報告し、脆弱性情報公表日以降、自らもそれを利用者に周知すること。

二．発見者が製品開発者であり、発見又は取得した脆弱性関連情報の影響範囲が自社のソフトウエア製品に限られる場合

対象がソフトウエア製品であり、かつ、発見者が製品開発者であり、発見又は取得した脆弱性関連情報の影響範囲が自社のソフトウエア製品に限られる場合における関係者の行動基準を以下に定める。

（１）製品開発者は、自ら開発等を行ったソフトウエア製品に影響が限られると認められる脆弱性関連情報を発見又は取得した場合、対策方法を作成し、当該脆弱性関連情報及び対策方法を受付機関及び調整機関に通知すること。

（２）受付機関及び調整機関は、（１）による通知を受けたときは、当該脆弱性情報及び対策方法をインターネット等を通じて公表すること。ただし、調整機関はそれらを公表すべき日について、当該製品開発者から意見を聴取した上で定めること。

Ⅵ．対象がウェブアプリケーションである場合の脆弱性関連情報取扱基準

対象がウェブアプリケーションである場合における脆弱性関連情報の取扱いの流れを以下に示す。

（ⅰ）発見者は、脆弱性関連情報を受付機関に届け出る。

（ⅱ）受付機関は、届出を受理した場合、一定の場合を除き、当該ウェブサイト運営者に当該脆弱性関連情報を通知する。

（ⅲ）当該ウェブサイト運営者は、受付機関から通知された脆弱性関連情報を検証し、必要に応じて当該脆弱性を修正する。

関係者における詳細な行動基準を以下に定める。

１．発見者基準

（１）発見者（自ら運営するウェブサイトのウェブアプリケーションについての脆弱性関連情報を発見又は取得したウェブサイト運営者を除く。）は、発見又は取得した脆弱性関連情報を経済産業大臣が別に指定する受付機関に届け出ること。ただし、当該ウェブサイト運営者に対し同じ内容を届け出ることを妨げない。

（２）発見者は、以下の点を明示した上で脆弱性関連情報を届け出ること。

①発見者の氏名、連絡先等の情報及びその取扱い

②脆弱性を有するウェブアプリケーションを稼働しているウェブサイトの名称等

③当該脆弱性関連情報

（３）違法な方法により脆弱性関連情報を発見又は取得しないこと。

（４）発見者は、当該脆弱性が修正されるまでの間、当該脆弱性関連情報を第三者に漏えいしないよう適切に管理すること。ただし、当該脆弱性関連情報を正当な理由により第三者に開示する場合、あらかじめ受付機関に問い合わせをすること。

２．受付機関基準

（１）受付機関は、１．（１）による届出が１．（２）で定めた届出事項を満たしているか否かを判断し、満たすと判断した場合、これを受理したものとし、当該発見者に対しその旨を速やかに通知すること。また、届出を不受理とした場合、当該発見者に対しその旨及びその理由を速やかに通知すること。

（２）受付機関は、届出を受理したときは、速やかに、当該ウェブサイト運営者に対し当該脆弱性関連情報を通知すること。ただし、当該脆弱性関連情報が以下に該当する場合、当該届出に係る処理を取りやめることができる。この場合においては、当該発見者にその旨及びその理由を通知すること。

①受付機関が既知の脆弱性関連情報であると確認した場合

②受付機関がウェブサイト運営者から既知の脆弱性である旨の通知を受けた場合

③受付機関が脆弱性関連情報に該当しないと確認した場合

④受付機関がウェブサイト運営者から脆弱性関連情報に該当しない旨の通知を受けた場合
⑤受付機関が違法な方法により発見又は取得されたおそれがあると認めた場合

（３）受付機関は、届出を受理した後においても、対策上必要と認められる場合、当該脆弱性関連情報について、当該発見者に問い合わせをすること。また、発見者からの問い合わせに対しては、当該ウェブサイト運営者と協議し、適切な情報を提供すること。その際、発見者の本人確認に留意すること。

（４）受付機関は、氏名、連絡先等の発見者を特定し得る情報を適切に管理し、当該発見者の同意がない場合は他者（ウェブサイト運営者を含む。）に開示しないこと。

（５）受付機関は、当該脆弱性関連情報を第三者に漏えいしないよう適切に管理すること。ただし、対策上必要と認められる場合、当該脆弱性関連情報の適切な管理を前提として、第三者にその分析を依頼することができる。

（６）受付機関は、当該ウェブサイト運営者から当該脆弱性を修正した旨の通知があったときは、それを速やかに発見者に通知すること。

（７）受付機関は、脆弱性に起因する被害の予防に資するため、脆弱性関連情報の届出状況等を公表すること。

３．ウェブサイト運営者基準

（１）ウェブサイト運営者は、受付機関から通知された脆弱性関連情報に関して、その内容を検証し、必要に応じて当該脆弱性を修正すること。

（２）ウェブサイト運営者は、当該脆弱性関連情報に関して検証した結果又は当該脆弱性を修正した旨を速やかに受付機関に通知すること。

（３）ウェブサイト運営者は、当該脆弱性が修正されるまでの間、当該脆弱性関連情報を第三者に漏えいしないよう適切に管理すること。

（４）ウェブサイト運営者は、当該脆弱性に起因する個人情報の漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生回避等の観点から、可能な限り事実関係等を公表するなど必要な対策をとること。

附則

この基準は、平成１６年７月８日から、施行する。

○経済産業省告示第二百二十三号

平成十六年経済産業省告示第二百三十五号（ソフトウェア等脆弱性関連情報取扱基準）に基づき、経済産業大臣が別に指定する受付機関及び経済産業大臣が別に指定する調整機関を次のように定め、平成二十一年六月二十五日から施行する。

なお、平成十六年経済産業省告示第二百三十六号は、平成二十一年六月二十四日限り廃止する。

平成二十一年六月二十五日

経済産業大臣臨時代理　国務大臣　甘利　明

一、経済産業大臣が別に指定する受付機関について

1．名称　　独立行政法人情報処理推進機構

2．主たる所在地　　東京都文京区本駒込二丁目二十八番八号

二、経済産業大臣が別に指定する調整機関について

1．名称　　一般社団法人ＪＰＣＥＲＴコーディネーションセンター

2．主たる所在地　　東京都千代田区神田錦町三丁目十七番地

参考資料４ 情報システム安全対策指針

平成９年９月 18 日制定（国家公安委員会告示第９号）

平成 11 年 11 月 22 日一部改正（国家公安委員会告示第 19 号）

情報システム安全対策指針

＜目次＞

第１編　総則

１　目的

本指針は、情報システムの関係者に対し、情報システムに係る犯罪、不正行為、個人情報の漏えい、災害等による被害を未然に防止し、又は最小限に抑えるために講ずべき対策及び犯罪発生時における警察との連携を確保するための措置を示すことにより、国民生活の安全を確保し、情報社会における秩序を維持することを目的とする。

２　定義

(1)　情報システム　コンピュータ・システムを中心とする情報処理及び通信に係るシステム（人的組織を含む。）をいう。

(2)　ネットワーク　通信のために用いられる装置及び回線をいう。

(3)　ホスト等　クライアント・サーバ・システムにおけるサーバ及びクライアント、メインフレーム・システムにおけるホスト・コンピュータ及び端末並びにネットワークの接続を制御するコンピュータをいう。

(4)　個人情報　個人に関する情報であって、特定の個人を識別することができるものをいう。

(5)　セキュリティ　犯罪、不正行為、災害若しくは事故による被害を受けること又は情報システムが犯罪若しくは不正行為の用に供されることが防止されている状態をいう。

(6)　管理者　情報システムの設置及び運営に関し責任及び権限を有する者をいう。

(7)　ユーザ　情報システムにより提供されるサービスを利用するためにアクセスする権限を有する者をいう。

(8)　統括セキュリティ責任者　情報システムのセキュリティに関し責任及び権限を有する者をいう。

(9)　監査責任者　監査に関し責任及び権限を有する者をいう。

(10) 危機管理責任者　危機に対する対応に関し責任及び権限を有する者をいう。

(11) 危機管理オペレータ　危機の状況を記録するとともに、危機管理責任者の指示を受け、具体的な対処を行う者をいう。

(12) アクセス　コンピュータ・システムを利用できる状態とすること又はその内部に電子的に存在する情報を取り扱うことをいう。

(13) 不正アクセス　不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）第３条第２項に規定する不正アクセス行為その他の不正な

手段によりユーザ以外の者が行うアクセス又はユーザが行う権限外のアクセスをいう。

(14) 危機　情報システムに被害が生じ、又は生ずるおそれがある状態をいう。

(15) 攻撃　コンピュータ・システムのセキュリティを侵害することを目的として故意に行われるアクセスをいう。

3　対策の策定

(1)　モデル・システム

本指針は、企業会計システム、顧客管理システムその他の次に掲げる要件を満たす情報システムをモデルとして、情報システムのセキュリティを確保するために必要と考えられる項目を列挙している。

ア　ホスト等を回線により相互に接続したネットワーク・システムであること。

イ　当該情報システムの管理者がユーザを管理することができるものであること。

ウ　破壊、改ざん又は漏えいによる影響が小さくない情報を処理するものであること。

エ　当該情報システムが運用停止することにより受ける影響が小さくない業務を処理するものであ ること。

(2)　対策の策定方法

管理者は、対象とする情報システムについて、リスク分析に基づきセキュリティ方針を立て、当該方針に沿って本指針の示す項目から必要なものを選択するとともに、必要に応じ追加を行い、対策を策定する必要がある。特に、社会的に重要な基盤を形成している情報システムについては、サイバーテロのリスクについても考慮する必要がある。

(3)　他の基準の活用

対策の策定に当たっては、別表に掲げる他省により示された基準も活用することが重要である。

第２編　情報システムについて講ずべき安全対策

インターネット等開放的なネットワークとの接続の状況の有無にかかわらず、すべての情報システムについて講ずべき安全対策は、次のとおりである。

I　管理者が講ずべき対策

第１章　ネットワーク

管理者は、ネットワークに係る不正アクセス、他者のユーザＩＤを不正に利用したなりすまし等を防止するため、次に掲げる項目について対策を講ずること。

1　監視

(1)　ログ

ア　ログを取得すること。ログの内容は、少なくともアクセスした者を特定可能なものであるこ と。

イ　ログ自体のセキュリティを確保すること。

ウ　ログを定期的に監査すること。

エ　ログは、次回の監査まで保管すること。

(2)　不正アクセス検出機能

不正アクセスが行われた場合に、これを検出し、危機管理責任者に知らせる機能を設けること。

(3)　その他

ア　ネットワーク及びホスト等の状態を監視する機能を設けること。

イ　端末を利用したアクセスについて当該端末を特定する機能を設けること。

ウ　異状がある場合に、ネットワーク及びホスト等の機能を停止させることができる機能を設けること。

2　パスワード

パスワードにより認証を行うネットワークについては、次の対策を講ずること。

(1)　ユーザには、必ずパスワードを設定させ、その秘匿に努めさせること。

(2)　他者が容易に推測できる語句等をパスワードとして設定しないようユーザを指導し、又は設定を拒否する機能をシステムに設けること。

(3)　パスワードを適切な期間ごとに変更するようユーザを指導し、又は変更を促す機能をシステムに設けること。

(4)　パスワードの再入力の回数を制限するなど、他者によるパスワードの推測を困難にするための措置を講ずること。

(5)　ユーザがパスワードを忘れたときなどに、パスワードを通知する場合に備え、本人確認の方法等について手続を定めておくこと。

(6)　パスワード・ファイルの暗号化等の措置を講ずるなど、パスワードの秘匿に努めること。

３　ネットワーク・アクセス

(1)　ログインに際し、識別及び認証を行うこと。

(2)　認証の手段については、当該情報システムに求められるセキュリティに応じ選択すること。

(3)　前回のログインの日時を確認できる機能を設けること。

４　ユーザＩＤ管理

(1)　退職、異動、長期出張、長期留学等により、不要となり、又は長期間使用されないユーザＩＤについては、廃止等の措置を講ずること。

(2)　長期間ログインが無いユーザに対して、文書等によりその旨を通知すること。

(3)　ユーザから要求があったときは、当該ユーザによる使用状況を開示すること。

５　暗号化

(1)　通信を行うときは、必要に応じデータ等を暗号化すること。

(2)　暗号鍵の保管を適切に行うこと。特に、ユーザの暗号鍵を集中的に管理する場合は、その保管の適正を図ること。

６　データ交換

(1)　データ交換に先立ち、意図する通信相手であることを確認するため、認証を行うこと。

(2)　デジタル署名等によりデータの完全性の確認を行うこと。

(3)　データが送信されたこと、受信されたこと等を証明し、これらの否認を防止できる機能を設けること。

(4)　(1)から(3)までを暗号を利用して行う場合であって、ユーザの暗号鍵を集中的に管理するときは、その保管の適正を図ること。

７　災害等対策

災害、事故等による回線の途絶を避けるため、必要に応じ回線の二重化を図ること。

第２章　ホスト等

管理者は、ホスト等に係る不正アクセス、他者のユーザＩＤを不正に利用したなりすまし等を防止するため、次に掲げる項目について対策を講ずること。

1　監視

(1)　ログ

ア　ログを取得すること。ログの内容は、少なくともアクセスした者を特定可能なものであること。

イ　ログ自体のセキュリティを確保すること。

ウ　ログを定期的に監査すること。

エ　ログは、次回の監査まで保管すること。

(2)　不正アクセス検出機能

不正アクセスが行われた場合に、これを検出し、危機管理責任者に知らせる機能を設けること。

2　パスワード

パスワードにより認証を行うホスト等については、次の対策を講ずること。

(1)　ユーザには、必ずパスワードを設定させ、その秘匿に努めさせること。

(2)　他者が容易に推測できる語句等をパスワードとして設定しないようユーザを指導し、又は設定を拒否する機能をシステムに設けること。

(3)　パスワードを適切な期間ごとに変更するようユーザを指導し、又は変更を促す機能をシステムに設けること。

(4)　パスワードの再入力の回数を制限するなど、他者によるパスワードの推測を困難にするための措置を講ずること。

(5)　ユーザがパスワードを忘れたときなどに、パスワードを通知する場合に備え、本人確認の方法等について手続を定めておくこと。

(6)　パスワード・ファイルの暗号化等の措置を講ずるなど、パスワードの秘匿に努めること。

3　ホスト等へのアクセス

(1)　ログインに際し、識別及び認証を行うこと。

(2)　認証の手段については、当該情報システムに求められるセキュリティに応じ選択すること。

(3)　前回のログインの日時を確認できる機能を設けること。

4　アクセス制御

セキュリティ方針に応じ、ホスト等へのアクセス制御のほか、データベースのデータ、ファイル等ごとにアクセス制御を行うこと。

5　オペレーティング・システム

アクセス制御機能等セキュリティを確保するために必要となる機能を有するオペレーティング・システムを選択すること。

6　セキュリティ・ホール

(1)　専用のソフトウェア等を用いて、セキュリティ・ホールのチェックを行うこと。

(2)　セキュリティ・ホールが発見されたときは、それを無くすために必要な措置を講ずること。

7　暗号化

(1)　データを保管する際は、必要に応じデータ等を暗号化すること。

(2)　暗号鍵の保管を適切に行うこと。特に、ユーザの暗号鍵を集中的に管理する場合は、その保管の適正を図ること。

8　ホスト等の管理

(1)　各装置を容易に取り外し、取り付け、又は持ち運ぶことができないよう措置を講ずること。

(2)　ディスプレイは、表示された情報を利用者以外の者に直接に又は容易に見られないように設置すること。

9　災害等対策

(1)　必要に応じ、装置を二重化し、代替運転機能を設けるなどの措置を講ずること。

(2)　自動回復機能を設けること。

第３章　施設

管理者は、ホスト・コンピュータ等コンピュータ・システムを構成する重要な装置を設置する施設を部外者の侵入、災害等から保護するため、次に掲げる項目について対策を講ずること。

1　資格及び身分証明書等

(1)　資格

ア　施設立入資格（以下「資格」という。）を設けること。

イ　資格は、必要最小限の者に対して、有効期間を限って与えること。

ウ　資格は、個人に対して与えること。

エ　資格の付与に際しては、立入りが可能な施設の範囲及び立入りの目的を

特定すること。

(2)　身分証明書等

ア　資格を与えた者には、次の事項が記録された身分証明用の文書、ＩＣカード等（以下「身分証明書等」という。）を交付すること。

(ｱ)　資格の有効期間

(ｲ)　立入りが可能な施設の範囲及び立入りの目的

(ｳ)　顔写真等の個人識別情報

イ　身分証明書等は、偽造等の困難な材質のものとすること。また、身分証明書等の原紙等が流出することのないよう厳重な管理を行うこと。

ウ　資格を与えた者が、身分証明書等を紛失し、又はき損したときは、直ちに統括セキュリティ責任者に届け出させること。

エ　ウの届出があったときは、直ちに当該身分証明書等を無効とすること。

２　入退管理等

(1)　入退管理

ア　施設への立入りを許可するに当たっては、身分証明書等により、その都度資格を確認すること。

イ　施設への立入りを許可する期間を限定すること。

ウ　立ち入る者の氏名、許可の有効期間、立入りが可能な施設の範囲、立入りの目的等、施設立入許可（以下「許可」という。）に関する記録を作成し、保存すること。

エ　許可を与えた者には、記章等の施設立入票を貸与し、見やすい位置に着用させること。

オ　施設立入票については、１(2)イからエまでに準じ対策を講ずること。

カ　建物、コンピュータ室等の出入口において、資格及び許可の有無をチェックすること。

キ　施設に物資を搬出入するときは、その都度、当該物資、運搬用具等をチェックすること。

ク　物資の搬出入に際しては、担当者の氏名、物資の名称、数量、搬出入の日時等の記録を作成し、保存すること。

ケ　警備員を配置し、入退管理に当たらせること。

(2)　防犯設備等

ア　敷地の出入口の数を制限し、資格の確認等を行うための施設を設けること。

イ　敷地内に侵入センサ、防犯カメラ等を設置するなど、侵入の発見及び抑止のための措置を講ずること。

ウ　建物、コンピュータ本体又は周辺機器が設置されている部屋、電源室、空調室、ＭＤＦ（主配線盤）室、ＩＤＦ（中間配線盤）室、データ保管室等の出入口及び開口部には、侵入センサを設置するなど、侵入の発見及び抑止のための措置を講ずること。

エ　警備員に施設内外の巡回に当たらせること。

３　災害等対策

(1)　施設の立地に当たっては、可能な限り自然災害の少ない場所を選定すること。

(2)　建物については、耐震構造とするとともに、防火構造とすること。

(3)　各種設備については、地震による移動、転倒及び震動防止の措置を講ずること。

(4)　内装については、不燃材料を使用するなど、防火措置を講ずること。

(5)　電源設備については、停電に対する措置を講ずること。

(6)　空気調和装置については、防火措置及び防水措置を講ずること。水冷式空気調和装置を使用する場合は、断水に対する措置を講ずること。

第４章　攻撃等認知時における措置等

管理者は、犯罪発生時における警察との連携を確保し、危機に対して的確に対応するとともに、セキュリティを確保するため、次に掲げる項目について対策を講ずること。

１　攻撃等認知時における措置

(1)　ユーザ等に対し、攻撃、事故その他情報システムのセキュリティを侵害する行為又は事態（以下「攻撃等」という。）を認知したときは、直ちに危機管理責任者に報告することを義務付けること。

(2)　攻撃を受けた対象、不正アクセス検出の結果、ログイン時のログ等、その後の監査又は調査に必要な情報を、攻撃等を認知した時点の状態で保存すること。

(3)　警察機関等への通報が必要なときは、直ちに通報すること（(4)に掲げる措置を除く。）。

(4)　攻撃が不正アクセス行為の禁止等に関する法律第３条第２項に規定する不正アクセス行為であり、同法に規定する都道府県公安委員会による援助が必要なときは、援助を受けたい旨の申出をすること。

(5)　警察機関等の調査等が終了し、復旧を行うに当たっては、作業の経過を記録すること。

2　組織体制

(1)　責任及び権限の明確化のため、次に掲げる体制をとること。

ア　通常の体制

専任の統括セキュリティ責任者及び監査責任者を置くこと。

イ　危機管理体制

専任の危機管理責任者及び危機管理オペレータを置くこと。

(2)　(1)ア及びイの責任者等のほか、責任及び権限の明確化のため、必要に応じ、その他の責任者等を置くこと。

3　情報システムの開発、運用及び保守

(1)　開発

ア　開発に従事する者以外の者に、基礎データ等の情報が漏えいすることを防止する措置を講ずること。

イ　システム設計等に関し、ドキュメントを作成すること。

ウ　運用及び保守のためのマニュアルを作成すること。

エ　運用のためのマニュアルには、危機の範囲及び危機に対する対応を定めること。

(2)　運用

ア　マニュアルに基づいて行うこと。

イ　運用記録を取ること。

(3)　保守

ア　マニュアルに基づいて行うこと。

イ　保守記録を取ること。

4　データ管理

(1)　重要なデータを記録している記録物が不要となったときは、データの消去、記憶媒体の破砕等アクセスが不可能となるような措置を講じた後、当該記録物を直ちに廃棄すること。

(2)　重要なデータを記録している記録物については、保管場所の入退管理、データの暗号化等の措置を講ずること。

(3)　フロッピー・ディスク等の容易に取り外すことができる記憶媒体については、必要に応じ、データの暗号化、物理的な書込み禁止の措置等所要の措置を講ずること。

5　バックアップ

(1)　バックアップは、定期的に、かつ、可能な限り頻繁に行うこと。
(2)　バックアップ・ファイルは、適切な保存方法、保存期間等を定め、原本と異なる場所に保管すること。

6　監査
(1)　監査は、情報システムの安全性、信頼性及び保全性並びに犯罪予防の観点から行うこと。
(2)　監査の方法を定めて、マニュアルを作成すること。
(3)　計画的かつ定期的に行うこと。ただし、重大な事故が発生し、又は発生するおそれがあると認められるときは、その都度行うこと。
(4)　監査報告書を作成すること。
(5)　統括セキュリティ責任者は、監査結果に基づき、速やかに所要の措置をとること。

7　教育及び訓練
(1)　危機発生時の措置について、マニュアルを作成してユーザに配布するとともに、定期的に訓練を行うこと。
(2)　危機が社会に与える影響の大きさ等をユーザに理解させること等により、モラルの向上を図ること。
(3)　ユーザによる対策の実施状況を監視し、十分な措置が講じられていない場合は指導を行うこと。

第５章　個人情報保護

管理者は、情報システムにおいて処理される個人情報を保護するため、次に掲げる項目について対策を講ずること。

1　個人情報の収集等
(1)　個人情報の収集は、あらかじめ収集の目的を明確に定め、その目的を達成するために必要な範囲内で、適法かつ公正な手段によって行うこと。
(2)　本人以外からの個人情報の収集は、本人の権利利益が不当に侵害されるおそれのない場合に限って行うこと。
(3)　個人情報は、収集の目的に必要な範囲内で正確かつ最新の状態に保つこと。
(4)　個人情報の収集の目的及び範囲は、原則として、公開すること。

2　個人情報の利用及び提供

(1)　個人情報の利用及び提供は、原則として、収集の目的の範囲内で行うこと。
(2)　収集の目的の範囲を超える個人情報の利用及び提供は、原則として、本人の同意がある場合又は法律の規定による場合に限って行うこと。

3　自己情報の開示等
(1)　本人から自己の個人情報の開示を求められたときは、原則として、これに応じること。
(2)　本人から自己の個人情報の訂正、追加又は消去を求められたときは、その内容を確認の上、原則としてこれに応じること。

II　ユーザが講ずべき対策
1　パスワードの管理
パスワードにより認証を行うコンピュータ・システムを利用する場合は、次のことに留意すること。
(1)　メモを残さないなど、パスワードの秘匿に努めること。
(2)　次のような、他者が容易に推測できる語句等をパスワードとして使用しないこと。
ア　短いもの又は単純なもの
イ　辞書に記載されているもの
ウ　家族の名前、生年月日等、ユーザ自身に関係するもの
エ　過去に使用したもの
(3)　適切な期間ごとにパスワードを変更すること。

2　暗号化
(1)　通信を行うときは、経済取引にかかわる情報等の重要なデータ等を暗号化すること。
(2)　暗号鍵の保管を適切に行うこと。

3　データ交換
(1)　データ交換に先立ち、意図する通信相手であることを確認するため、認証を行うこと。
(2)　デジタル署名等によりデータの完全性の確認を行うこと。

4　端末等の管理
(1)　端末から離れるときは、次に掲げる措置のいずれかを講ずること。

ア　電源を切る。（電源キーを使用している場合は、電源キーを抜く。）
イ　ログアウトする。
ウ　パスワード付きスクリーン・セーバを使用する。
(2)　ディスプレイに表示された情報を、直接に又は容易に他者に見られないよう留意すること。
(3)　ユーザＩＤの不正な利用を発見するため、前回のログインの日時を確認すること。

5　身分証明書等の管理
身分証明書等を交付された場合は、次のことに留意すること。
(1)　身分証明書等を厳重に管理し、紛失しないこと。
(2)　身分証明書等を他者に貸与しないこと。
(3)　身分証明書等を紛失したときは、直ちに統括セキュリティ責任者に届け出ること。

6　攻撃等認知時における措置
(1)　攻撃等を認知したときは、危機管理責任者に報告すること。
(2)　攻撃を受けた対象、不正アクセス検出の結果、ログイン時のログ等、その後の監査又は調査に必要な情報を、攻撃等を認知した時点の状態で保存すること。

7　データ管理
(1)　重要なデータを記録している記録物が不要となったときは、データの消去、記憶媒体の破砕等アクセスが不可能となるような措置を講じた後、当該記録物を直ちに廃棄すること。
(2)　重要なデータを保存するときは、データを暗号化すること。
(3)　フロッピー・ディスク等の容易に取り外すことのできる記憶媒体については、必要に応じ、データの暗号化、物理的な書込み禁止の措置等所要の措置を講ずること。
(4)　携帯端末等については、重要なデータを内蔵の記憶装置に保存することを避け、やむを得ず保存する場合は、データの暗号化等の措置を講ずること。

8　バックアップ
(1)　バックアップは、定期的に、かつ、可能な限り頻繁に行うこと。
(2)　バックアップ・ファイルは、適切な保存方法、保存期間等を定め、原本

と異なる場所に保管すること。

III　コンピュータ・ウイルスに関し管理者及びユーザが講ずべき対策

1　システムの使用開始時に講ずべき措置

ホスト等を起動させるときは、始めにワクチン・プログラムを用いるなどして、コンピュータ・ウイルスのチェックを行うこと。

2　新たに入手したプログラムを使用するときに講ずべき措置

(1)　出所不明のプログラムの使用自粛

フリーウェア、シェアウェア等のうち、出所が不明のプログラムは、コンピュータ・ウイルスに感染しているおそれがあるため、可能な限り使用しないこと。

(2)　コンピュータ・ウイルスのチェック

新たに入手したプログラムを使用するときは、あらかじめ、ワクチン・プログラムを用いるなどして、少なくとも次の点を調べることにより、コンピュータ・ウイルスのチェックを行うこと。また、チェックを行った結果、陽性とされたもの及び陽性の疑いのあるものについては使用しないこと。

なお、オの点を調べるときは、端末等をネットワークから切り離して行うこと。

ア　ファイル（隠しファイルを含む。以下同じ。）に内容の不明なもの又は不必要なものが無いか。

イ　ファイルの作成日時又は変更日時が異常でないか。

ウ　ファイル・サイズが異常な値のファイルが無いか。

エ　ファイル名に拡張子を付加するオペレーティング・システムを使用している場合に、予定されていない拡張子を付加されたファイルが無いか。

オ　プログラムの各種機能を作動させることにより不正な命令が機能しないか。

3　システム使用中に講ずべき措置

(1)　コンピュータ・ウイルスのチェック

ワクチン・プログラムを用いるなどして、少なくとも次の点を調べることにより、コンピュータ・ウイルスのチェックを行うこと。

なお、新たにファイルを入手したときは、ワクチン・プログラムによるチェックを行うこと。

ア　ファイルの作成日時又は更新日時が異常でないか。

イ　ファイル・サイズが異常な値になっていないか。

ウ　ファイルの内容に変化が無いか。
エ　余計なファイルが増えていないか。
オ　存在しているはずのファイルが無くなっていないか。
カ　余計なプログラムが主記憶装置に常駐していないか。

(2)　作動状況の監視

ホスト等の作動状況を監視し、次のような異状が現れた場合は、ワクチン・プログラムを用いるなどしてチェックを行うこと。

ア　アクセスすることが想定されない装置にアクセスする。
イ　記憶媒体へのアクセス時間が異常に長い。
ウ　利用可能な記憶領域が通常より少ない。
エ　記憶媒体の未使用領域が急激に小さくなる。
オ　異常なメッセージが出る。
カ　誤入力が多い。

4　コンピュータ・ウイルス発見時に講ずべき措置

(1)　ネットワークからの切離し

使用中の端末等をネットワークから切り離すこと。

(2)　コンピュータ・ウイルスの除去等

ワクチン・プログラムを用いるなどして、コンピュータ・ウイルスを除去し、又はその機能を停止させること。

(3)　ファイルの修復

ファイルの破壊又は改ざんが行われたときは、あらかじめ作成されたマニュアルに基づき、修復ツール等を用いて修復すること。

(4)　再起動

再起動は、システム・ファイルのバックアップ・ファイルにより行うこと。

(5)　危機管理責任者への報告

速やかに危機管理責任者に報告すること。

(6)　ユーザへの通知

危機管理責任者は、ユーザに対し、とるべき措置を速やかに通知すること。

5　その他

(1)　アクセス制御等

コンピュータ・ウイルスによるファイルの破壊又は改ざんを防止するため、必要に応じ、アクセス制御等の措置を講ずること。

(2)　バックアップ

ア　システム・ファイルのバックアップ・ファイルを作成し、保存すること。

イ　バックアップに当たっては、ワクチン・プログラムを用いるなどしてチェックを行うこと。

(3)　ワクチン・プログラムの更新等

ア　新種のコンピュータ・ウイルスに対応するため、必要に応じ、ワクチン・プログラムを更新すること。

イ　ワクチン・プログラムを用いるときは、適切な条件設定を行うこと。

(4)　教育

管理者は、コンピュータ・ウイルス対策に関するマニュアルを作成してユーザに配布するとともに、マニュアルの内容をよく理解させておくこと。

第３編　開放的なネットワークに接続する情報システムについて追加的に講ずべき安全対策

情報システムのうち、インターネット等開放的なネットワークに接続するものについて、第２編に示した安全対策に加え、不正アクセス、コンピュータ・ウイルスの侵入等の防止の観点から講ずべき安全対策は、次のとおりである。

なお、開放的なネットワークに接続する情報システムについては、第２編に示した安全対策についても、不正アクセス、コンピュータ・ウイルスの侵入等のリスクの増加を考慮する必要がある。

Ⅰ　管理者が講ずべき対策

第１章　ネットワーク

管理者は、開放的なネットワークを介した不正アクセス、コンピュータ・ウイルスの侵入等を防止するため、次に掲げる項目について対策を講ずること。

１　接続等

(1)　開放的なネットワークとの接続は、必要最小限の機能、回線及びホスト等に限定すること。

(2)　開放的なネットワークと接続するときは、当該開放的なネットワークからの保有する情報への不正アクセスを防止する機能を設け、すべての通信を制御すること。

(3)　(2)をファイアーウォール等を利用して行う場合は、適切な条件設定を行うこと。

(4)　(2)をコンピュータ・システムを利用して行う場合は、セキュリティ・ホールに関する措置を講ずるなど当該システムのセキュリティを確保すること。

(5)　ネットワークの構成等に関する重要な情報は、真に必要な場合を除き公

開しないこと。

２　監視

回線の負荷状況等を監視する機能を設けること。

３　切離し

異状が発見された場合等必要がある場合は、接続された開放的なネットワークを切り離すことができるようにすること。

第２章　攻撃等認知時における措置等

管理者は、犯罪発生時における警察との連携を確保し、危機に対して的確に対応するとともに、セキュリティを確保するため、次に掲げる項目について対策を講ずること。

１　攻撃等認知時における措置

(1)　攻撃等を認知したときは、関係機関等と協力して被害の状況を把握すること。

(2)　関係機関等と協力して被害の拡大を防止するための措置を講ずること。

(3)　攻撃の分析及び原因の究明を行い、関係機関等と協力して再発防止のための措置を講ずること。

２　ユーザの限定

開放的なネットワークを介してアクセスできるユーザは、可能な限り限定すること。

３　情報収集

(1)　開放的なネットワークを介してなされる不正アクセス等に関する情報について平素から収集すること。

(2)　収集した情報については、必要に応じユーザに提供すること。

４　教育

情報システムの安全対策が適当でない場合は、他者のユーザＩＤを不正に利用したなりすまし等を助長することとなり、その結果、開放的なネットワークに接続される他の情報システム等に被害を与える危険性があることをユーザに十分認識させること。

II　コンピュータ・ウイルスに関し管理者及びユーザが講ずべき対策

1　新たに入手したプログラムを使用するときに講ずべき措置

送信元が不明のプログラムは、コンピュータ・ウイルスに感染しているおそれがあるため、使用しないこと。

2　システム使用中に講ずべき措置

開放的なネットワークを介して、電子メール（添付ファイルを含む。）の受信又はファイルのダウンロードを行ったときは、ワクチン・プログラムによるチェックを行うこと。転送するときは、事前にチェックを行うこと。

別表（第１編の３(3)関係）
他省により示された基準
「コンピュータウイルス対策基準」（平成７年７月７日付け通商産業省告示第４２９号）
「情報システム安全対策基準」（平成７年８月２９日付け通商産業省告示第５１８号）
「コンピュータ不正アクセス対策基準」（平成８年８月８日付け通商産業省告示第３６２号）
「情報通信ネットワーク安全・信頼性基準」（昭和６２年２月１４日付け郵政省告示第７３号）

参考資料５ コンピュータ不正アクセス対策基準

コンピュータ不正アクセス対策基準

平成８年８月８日（通商産業省告示第３６２号）（制定）
平成９年９月２４日（通商産業省告示第５３４号）（改定）
平成１２年１２月２８日（通商産業省告示第９５０号）（最終改定）

コンピュータ不正アクセス対策基準を次のように定め、平成８年８月８日から施行する。

Ⅰ．主旨

本基準は、コンピュータ不正アクセスによる被害の予防、発見及び復旧並びに拡大及び再発防止について、企業等の組織及び個人が実行すべき対策をとりまとめたものである。

Ⅱ．用語の定義

本基準で用いられる用語の定義は、以下のとおりである。

１．コンピュータ不正アクセス（以下「不正アクセス」とする。）

システムを利用する者が、その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うこと。

２．ソフトウェア

システムプログラム、アプリケーションプログラム、ユーティリティプログラム等のプログラム及びそれに付随するデータ

３．コンピュータ

ネットワークに接続され得るコンピュータであり、ルータ、交換機等の通信用コンピュータ及びその他専用コンピュータを含むもの。

４．ネットワーク

通信回線及び通信機器の複合体

５．システム

コンピュータ及びネットワークの複合体

６．ファイル

記憶装置又は記録媒体上に記録されているプログラム、データ等

７．機器

ハードウェア、通信回線又は通信機器

８．バックアップ

プログラム、データ等と同一の内容を別の媒体に記録すること。

9．保守機能

システムを正常な状態に維持するための機能

III．構成

本基準は、システムユーザ基準、システム管理者基準、ネットワークサービス事業者基準及びハードウェア・ソフトウェア供給者基準からなり、その構成及び内容は以下のとおりである。

1．システムユーザ基準

システムを利用する者（以下「システムユーザ」とする。）が実施すべき対策についてまとめたもの。

（1）パスワード及びユーザID管理（9項目）

システムユーザ自身が使用するパスワード及びユーザIDを管理する際に実施すべき対策についてまとめたもの。

（2）情報管理（7項目）

システムユーザ自身が利用する情報を管理する際に実施すべき対策についてまとめたもの。

（3）コンピュータ管理（6項目）

システムユーザ自身が利用するコンピュータを利用及び管理する際に実施すべき対策についてまとめたもの。

（4）事後対応（2項目）

システムの異常及び不正アクセスをシステムユーザが発見した場合の対応についてまとめたもの。

（5）教育及び情報収集（2項目）

セキュリティ対策に関する教育及び情報の収集についてまとめたもの。

（6）監査（1項目）

不正アクセス対策を適切に実施するための監査についてまとめたもの。

2．システム管理者基準

システムユーザの管理並びにシステム及びその構成要素の導入、維持、保守等の管理を行う者（以下「システム管理者」とする。）が、実施すべき対策についてまとめたもの。

（1）管理体制の整備（7項目）

システム及びその構成要素を管理するための体制を整備する際に実施すべき対策についてまとめたもの。

(2) システムユーザ管理 (10項目)

システムユーザをシステム管理者が管理する際に実施すべき対策についてまとめたもの。

(3) 情報管理 (8項目)

システム全体の情報をシステム管理者が管理する際に実施すべき対策についてまとめたもの。

(4) 設備管理 (18項目)

ハードウェア、ソフトウェア、通信回線及び通信機器並びにそれらの複合体をシステム管理者が管理する際に実施すべき対策についてまとめたもの。

(5) 履歴管理 (4項目)

システムの動作履歴、使用記録等をシステム管理者が記録、分析及び保存する際に実施すべき対策についてまとめたもの。

(6) 事後対応 (6項目)

システム全体の異常及び不正アクセスをシステム管理者が発見した場合並びにシステムユーザからの発見の連絡を受けた場合の対応についてまとめたもの。

(7) 情報収集及び教育 (4項目)

セキュリティ対策に関する情報の収集及びその活用方法並びにシステムユーザへの教育についてまとめたもの。

(8) 監査 (1項目)

不正アクセス対策を適切に実施するための監査についてまとめたもの。

3．ネットワークサービス事業者基準

ネットワークを利用して、情報サービス及びネットワーク接続サービスを提供する事業者 (以下「ネットワークサービス事業者」とする。) が実施すべき対策についてまとめたもの。

(1) 管理体制の整備 (2項目)

ネットワークサービスを行うための体制を整備する際に実施すべき対策についてまとめたもの。

(2) ネットワークサービスユーザ管理 (7項目)

ネットワークサービスユーザをネットワークサービス事業者が管理する際に実施すべき対策についてまとめたもの。

(3) 情報管理 (3項目)

ネットワークサービスユーザ及び事業者自身の情報を管理する際に実施すべき対策についてまとめたもの。

(4) 設備管理 (5項目)

ネットワークサービスに係る機器をネットワークサービス事業者が管理する際に実施すべき対策についてまとめたもの。

(5) 事後対応 (6項目)

ネットワークサービスに係るシステムの異常及び不正アクセスをネットワークサービス事業者が発見した場合並びに発見の連絡を受けた場合の対応についてまとめたもの。

(6) 情報収集及び教育 (3項目)

セキュリティ対策に関する情報の収集及びその活用方法並びにネットワークサービスユーザへの教育についてまとめたもの。

(7) 監査 (1項目)

不正アクセス対策を適切に実施するための監査についてまとめたもの。

4. ハードウェア・ソフトウェア供給者基準

ハードウェア及びソフトウェア製品の開発、製造、販売等を行う者 (以下「ハードウェア・ソフトウェア供給者」とする。) が、実施すべき対策についてまとめたもの。

(1) 管理体制の整備 (2項目)

ハードウェア及びソフトウェアを供給するための体制について実施すべき対策をまとめたもの。

(2) 設備管理 (2項目)

ハードウェア及びソフトウェア製品の開発及び製造に係る機器をハードウェア・ソフトウェア供給者が管理する際に実施すべき対策についてまとめたもの。

(3) 開発管理 (7項目)

ハードウェア及びソフトウェア製品をハードウェア・ソフトウェア供給者が開発及び製造する際に実施すべき対策についてまとめたもの。

(4) 販売管理 (4項目)

ハードウェア及びソフトウェア製品をハードウェア・ソフトウェア供給者が販売等を行う場合に実施すべき対策についてまとめたもの。

(5) 事後対応 (6項目)

開発システムの異常及び不正アクセスをハードウェア・ソフトウェア供給者が発見した場合の対応についてまとめたもの。

(6) 情報収集及び教育 (2項目)

セキュリティ対策に関する情報の収集及びその活用方法並びに製品のユーザに対する教育についてまとめたもの。

(7) 監査 (1項目)

不正アクセス対策を適切に実施するための監査についてまとめたもの。

Ⅳ. 個人ユーザが留意する点

本基準は企業等の組織及び個人を対象としているが、構成の便宜上、組織を対象とした記述となっているため、個人ユーザは以下の項目について留意することにより、不正アクセスからの被害を　防止することができる。

1. 不正アクセスによる被害の予防について

「Ⅴ 1. システムユーザ基準」の「(1) パスワード及びユーザID管理」、「(2) 情報管理」、「(3) コンピュータ管理」の中の必要な項目

2. 不正アクセスによる被害の発見、復旧、拡大及び再発防止について

「Ⅴ　2. システム管理者基準」の「(6) 事後対応」

Ⅴ. 基準項目

1. システムユーザ基準

(1) パスワード及びユーザID管理

1.ユーザIDは、複数のシステムユーザで利用しないこと。
2.ユーザIDは、パスワードを必ず設定すること。
3.複数のユーザIDを持っている場合は、それぞれ異なるパスワードを設定すること。
4.悪いパスワードは、設定しないこと。
5.パスワードは、随時変更すること。
6.パスワードは、紙媒体等に記述しておかないこと。
7.パスワードを入力する場合は、他人に見られないようにすること。
8.他人のパスワードを知った場合は、速やかにシステム管理者に通知すること。
9.ユーザIDを利用しなくなった場合は、速やかにシステム管理者に届け出ること。

(2) 情報管理

1.重要な情報は、パスワード、暗号化等の対策を図ること。
2.重要な情報を送信する場合は相手先を限定し、宛先を十分に確認すること。
3.ファイルの属性は、内容の重要度に応じたアクセス権限を必ず設定すること。
4.コンピュータ及び通信機器を維持、保守するために必要なファイルは、盗用、改ざん、削除等されないように厳重に管理すること。
5.重要な情報を記録した紙、磁気媒体等は、安全な場所に保管すること。
6.重要な情報を記録した紙、磁気媒体等を廃棄する場合は、内容が漏えいしない方法で行うこと。
7.ファイルのバックアップを随時行い、その磁気媒体等を安全な場所に保管すること。

(3) コンピュータ管理

1.コンピュータ、通信機器及びソフトウェアの導入、更新、撤去等を行う場合は、システム管理者の指導の下で行うこと。
2.コンピュータを管理するために与えられた最上位の権限（以下「特権」とする。）によるコンピュータの利用は、必要最小限にすること。
3.特権によりコンピュータを利用する場合は、コンピュータ、場所、期間等を限定すること。
4.コンピュータが無断で利用された形跡がないか、利用履歴等を随時確認すること。
5.コンピュータを入力待ち状態で放置しないこと。
6.パスワードの入力を省略する機能は、システム管理者の指導の下で使用すること。

(4) 事後対応

1.システムの異常を発見した場合は、速やかにシステム管理者に連絡し、指示に従うこと。
2.不正アクセスを発見した場合は、速やかにシステム管理者に連絡し、指示に従うこと。

(5) 教育及び情報収集

1.システム管理者からセキュリティ対策に関する教育を随時受けること。
2.セキュリティ対策に関する情報を入手した場合は、システム管理者に随時提供すること。

(6) 監査

1.システムユーザが行う不正アクセス対策の実効性を高めるため、システム監査の報告を受け、必要な措置を講ずること。

2．システム管理者基準

(1) 管理体制の整備

1.システムのセキュリティ方針を確立し、周知･徹底すること。
2.システムの管理体制、管理手順を確立し、周知･徹底すること。
3.緊急時の連絡体制及び復旧手順を確立し、周知･徹底すること。
4.システム管理の業務上知り得た情報の秘密を守ること。
5.システム管理者の権限は、業務を遂行する上で必要最小限にすること。
6.システム管理者は2人以上かつ必要最小限の管理者で、その業務は定期的に交代すること。
7.システム管理者の資格を喪失した者の権限は、速やかに停止すること。

(2) システムユーザ管理

1.システムユーザの登録は、必要な機器に限定し、システムユーザの権限を必要最小限に設定すること。
2.ネットワークを介して外部からアクセスできるユーザIDは、必要最小限にすること。
3.ユーザIDは、個人単位に割り当て、パスワードを必ず設定すること。
4.長期間利用していないユーザIDは、速やかに停止すること。
5.ユーザIDの廃止等の届出があった場合は、速やかに登録を抹消すること。
6.パスワードは、当該システムユーザ以外に知らせないこと。
7.パスワードのチェックを随時行い、悪いパスワードは、速やかに変更させること。
8.パスワードが当該システムユーザ以外に知られた場合又はその疑いのある場合は、速やかに変更させること。
9.特権を付与する場合は、当該システムユーザの技術的能力等を考慮すること。
10.必要としなくなったシステムユーザの特権は、速やかに停止すること。

(3) 情報管理

1.通信経路上の情報は、漏えいを防止する仕組みを確立すること。
2.通信経路上で情報の盗聴及び漏えいが行われても、内容が解析できない機密保持機能を用いること。
3.通信経路上で情報の改ざんが行われても、検出できるような改ざん検知機能を用いること。
4.システム関連のファイルは、システムユーザがアクセスできないように管理すること。
5.重要な情報は、削除、改ざん、漏えい等による被害が少なくなるように分散化すること。
6.重要な情報を記録した紙、磁気媒体等は、安全な場所に保管すること。
7.重要な情報を記録した紙、磁気媒体等を廃棄する場合は、内容が漏えいしない方法で行うこと。
8.ファイルのバックアップを随時行い、その磁気媒体等を安全な方法で保管すること。

(4) 設備管理

1.すべての機器及びソフトウェアの管理者を明確にすること。
2.重要な情報が格納されているか又は重要な処理を行う機器は、許可を与えられた者以外立ち入れない場所に設置し、厳重に管理すること。
3.移動可能な機器は、盗難防止策を行うこと。
4.システム構成を常に把握しておくこと。
5.機器及びソフトウェアを導入する場合は、セキュリティ機能がセキュリティ方針に適合していることをあらかじめ確認してから行うこと。
6.機器及びソフトウェアの設定情報がシステムに適合していることを随時確認すること。
7.機器及びソフトウェアは、供給者の連絡先及び更新情報が明確なものを利用すること。
8.セキュリティ上の問題点が解決済みの機器及びソフトウェアを利用すること。
9.外部と接続する機器は、十分なアクセス制御機能を有したものを利用すること。
10.システム構成の変更を行う前に、セキュリティ上の問題が生じないことを確認すること。
11.ネットワークを介して外部からアクセスできる通信経路及びコンピュータは、必要最小限にすること。
12.ネットワークを介して外部からシステム管理を行う場合は、認証機能、暗号機能及びアクセス制御機能を設定すること。
13.長期間利用しない機器は、システムに接続しないこと。
14.機器及びソフトウェアの廃棄、返却、譲渡等を行う場合は、情報の漏えいを防ぐ対策を行うこと。
15.ソフトウェア及びシステムファイルの改ざんが生じていないことを随時確認すること。
16.システムが提供するパスワード強化機能は最大限に活用すること。
17.ネットワークの負荷状況を監視すること。
18.システムの利用形態等に応じて、ネットワークを分離すること。

(5) 履歴管理

1.システムのセキュリティ方針に基づいたシステムの動作履歴、使用記録等を記録すること。
2.システムの動作履歴、使用記録等を記録する場合は、改ざん、削除、破壊及び漏えいの防止措置を施すこと。
3.記録したシステムの動作履歴、使用記録等を随時分析すること。
4.記録したシステムの動作履歴、使用記録等は、安全な方法で一定期間保管すること。

(6) 事後対応

1.異常の連絡を受けた場合又は異常を発見した場合は、速やかに原因を追究すること。
2.不正アクセスであることが判明した場合は、関係者と協調して被害の状況を把握すること。
3.関係者と協調して不正アクセス被害の拡大を防止するための処置を行うこと。
4.事前に確立した復旧手順を遂行し、関係者と協調して不正アクセス被害の復旧に努めること。
5.不正アクセス被害の原因を分析し、関係者と協調して再発防止策を行うこと。
6.不正アクセス被害の拡大及び再発を防止するため、必要な情報を経済産業大臣が別に指定する者に届け出ること。

(7) 情報収集及び教育

1.セキュリティ対策に関する情報を随時収集すること。
2.収集した情報を分析し、重要な情報については速やかに対応すること。
3.システムユーザがセキュリティ対策を行う場合に必要な情報を提供すること。
4.システムユーザに、セキュリティ教育を随時実施すること。

(8) 監査

1.システム管理者が行う不正アクセス対策の実効性を高めるため、システム監査の報告を受け、必要な措置を講ずること。

3．ネットワークサービス事業者基準

(1) 管理体制の整備

1.ネットワークサービス事業者の要員の業務範囲を明確にすること。
2.不正アクセスを発見したときの連絡体制及び復旧手順を確立し、周知･徹底すること。

(2) ネットワークサービスユーザ管理

1.ネットワークサービス事業者及びネットワークサービスユーザの責任範囲を明確にすること。
2.ネットワークサービス事業者が提供できるセキュリティサービスを明示すること。
3.ネットワークサービスユーザとの連絡体制を複数確立し、周知･徹底すること。
4.不正アクセスを行ったネットワークサービスユーザに対するサービスを制限できる仕組みを確立すること。
5.ネットワークサービスユーザから要求があった場合、本人の利用情報等を開示すること。
6.ネットワークサービスユーザへの不正アクセスを監視できる仕組みを確立すること。
7.ネットワークサービスユーザの利用情報等を記録できる仕組みを確立すること。

(3) 情報管理

1.ネットワークサービスユーザの情報は、厳重に管理すること。
2.ネットワークサービスユーザの情報を公開する場合は、本人の了解を得ること。
3.ネットワーク構成等の重要な情報は、公開しないこと。

⑷ 設備管理

1.ネットワークサービスに係る機器は、許可を与えられた者以外立ち入れない場所に設置し、厳重に管理すること。
2.ネットワークサービスに係る機器の管理が常に可能な仕組みを確立すること。
3.ネットワークサービスに係る機器を遠隔管理する通信回線は、複数確保すること。
4.ネットワークサービスユーザにサービスを提供するネットワークは、他の業務のネットワークと分離すること。
5.特定のサービスに関する情報は、そのサービスに関連した機器に限定して流すこと。

⑸ 事後対応

1.異常の連絡を受けた場合又は異常を発見した場合は、速やかに原因を追究すること。
2.不正アクセスであることが判明した場合は、関係者と協調して被害の状況を把握すること。
3.関係者と協調して不正アクセス被害の拡大を防止するための処置を行うこと。
4.事前に確立した復旧手順を遂行し、関係者と協調して不正アクセス被害の復旧に努めること。
5.不正アクセス被害の原因を分析し、関係者と協調して再発防止策を行うこと。
6.不正アクセス被害の拡大及び再発を防止するため、必要な情報を経済産業大臣が別に指定する者に届け出ること。

⑹ 情報収集及び教育

1.セキュリティ対策に関する情報を随時収集すること。
2.ネットワークサービスユーザがセキュリティ対策を行う場合に必要な情報を提供すること。
3.ネットワークのセキュリティ上の問題及びその対策に関する十分な情報を提供し、必要に応じてその情報を活用するための教育をすること。

⑺ 監査

1.ネットワークサービス事業者が行う不正アクセス対策の実効性を高めるため、システム監査の報告を受け、必要な措置を講ずること。

4．ハードウェア･ソフトウェア供給者基準

⑴ 管理体制の整備

1.ハードウェア･ソフトウェア供給者の要員の業務範囲を明確にすること。
2.不正アクセスを発見したときの連絡体制及び復旧手順を確立し、周知･徹底すること。

⑵ 設備管理

1.開発業務に係る機器は、許可を与えられた者以外立ち入れない場所に設置し、厳重に管理すること。
2.開発業務に係るネットワークは、他の業務のネットワークと分離すること。

⑶ 開発管理

1.製品のセキュリティ機能の実装に関する方針を明確にすること。
2.製品は、機密保持機能、認証機能、改ざん検知機能等のセキュリティ機能を設けること。
3.製品のネットワークに係る機能は、セキュリティ上の重要な情報の解析を防ぐ機能を組み込むこと。
4.製品の保守に係る機能は、利用する者を限定する機能を組み込むこと。
5.セキュリティの設定を行わないと製品が利用できない機能を設けること。

6.製品の開発に使用したデバッグ機能等は、出荷前に削除しておくこと。
7.製品のセキュリティ機能が仕様どおり動作するか検査すること。

(4) 販売管理

1.製品は、流通段階における改ざん等を防止するための措置を施すこと。
2.製品は、利用上の制限事項及び推奨事項を明示の上、販売等を行うこと。
3.製品は、供給者の連絡先を明示しておくこと。
4.製品にセキュリティ上の問題が発見された場合は、製品のユーザ及び関係者に情報を通知するとともに、問題を解決するための適切な処置を行うこと。

(5) 事後対応

1.製品開発システムにおける異常を発見した場合は、速やかに原因を追究すること。
2.不正アクセスであることが判明した場合は、関係者と協調して被害の状況を把握すること。
3.関係者と協調して不正アクセス被害の拡大を防止するための処置を行うこと。
4.事前に確立した復旧手順を遂行し、関係者と協調して不正アクセス被害の復旧に努めること。
5.不正アクセス被害の原因を分析し、関係者と協調して再発防止策を行うこと。
6.不正アクセス被害の拡大及び再発を防止するため、必要な情報を経済産業大臣が別に指定する者に届け出ること。

(6) 情報収集及び教育

1.製品のセキュリティ対策に関する情報を随時収集し、その情報を製品の開発に生かすこと。
2.製品の販売を通じてセキュリティ対策の情報を提供し、必要に応じて教育を行うこと。

(7) 監査

1.ハードウェア・ソフトウェア供給者が行う不正アクセス対策の実効性を高めるため、システム監査の報告を受け、必要な措置を講ずること。

VI. 留意事項

1.本基準は、システムの構成及び利用形態、取り扱う情報等に則して活用すること。
2.ネットワークサービス事業者基準及びハードウェア・ソフトウェア供給者基準は、各事業者特有の観点からまとめた基準であることから、各事業の機器の導入等にあたっては、システム管理者基準も併せて活用すること。
3.コンピュータウイルス対策の実施については、「コンピュータウイルス対策基準」(平成7年7月7日付　通産省告示第429号)を活用すること。
4.システム自体の安全対策の実施については、「情報システム安全対策基準」(平成7年8月29日付　通産省告示第518号)を活用すること。
5.システム監査の実施については、「システム監査基準」(平成8年1月30日付　通産省公報)を活用すること。
6.ソフトウェア管理の実施については、「ソフトウェア管理ガイドライン」(平成7年11月15日付通産省公報)を活用すること。
7.コンピュータウイルス、不正アクセス、災害等の対策としては、警察庁からも「情報システム安全対策指針」(平成9年 国家公安委員会 告示 第9 号)が発表されており、本基準と併せて活用することにより、情報システムのセキュリィテイを高めることができる。

- 関連告示

平成8年通商産業省告示第３６２号（コンピュータ不正アクセス対策基準を定める件）に基づき、経済産業大臣が別に指定する者を次のように定める。

なお、平成１２年通商産業省告示第９４９号（コンピュータ不正アクセス対策基準に基づく経済産業省大臣が別に指定する者）は廃止する。

平成１６年1月5日　経済産業大臣　中川　昭一

１．名称　　独立行政法人情報処理推進機構
２．主たる所在地　　東京都文京区本駒込二丁目二十八番八号

不正アクセス防止対策に関する官民意見集約委員会　関係者

（民間）

浅沼　靖人	ＳＣＳＫ株式会社
池田　和生	株式会社エヌ・ティ・ティ・データ
石井　茂	独立行政法人情報処理推進機構（ＩＰＡ）
石戸谷　雅	社団法人テレコムサービス協会
泉原　克人	一般社団法人日本オンラインゲーム協会
稲葉　直宏	ヤフー株式会社
井上　大介	独立行政法人情報通信研究機構（ＮＩＣＴ）
岩井　博樹	株式会社ラック
上原　宏	日本ヒューレット・パッカード株式会社
宇佐美　茂男	日本ヒューレット・パッカード株式会社
卯城　大士	チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
宇野　誠	マカフィー株式会社
榎本　司	日本ヒューレット・パッカード株式会社
岡野　大良	伊藤忠テクノソリューションズ株式会社
奥天　陽司	株式会社ラック
片山　建	日本マイクロソフト株式会社
加藤　雅彦	日本セキュリティオペレーション事業者協議会（ISOG-J）
加賀谷　伸一郎	独立行政法人情報処理推進機構（ＩＰＡ）
川口　洋司	一般社団法人日本オンラインゲーム協会
川嶋　一宏	株式会社日立製作所
神林　彰	社団法人日本情報システム・ユーザー協会（ＪＵＡＳ） （会員　富士ゼロックス株式会社）
木村　孝	社団法人日本インターネットプロバイダー協会
木邑　実	独立行政法人情報処理推進機構（ＩＰＡ）
久保　啓司	フィッシング対策協議会
桑子　博行	社団法人テレコムサービス協会
講武　洋次郎	株式会社ジェーシービー
小屋　晋吾	トレンドマイクロ株式会社
齋藤　直樹	株式会社ジェーシービー
齋藤　広晃	ＳＣＳＫ株式会社
坂本　晋也	セコムトラストシステムズ株式会社
佐藤　正実	ＳＣＳＫ株式会社
佐藤　元彦	伊藤忠テクノソリューションズ株式会社
佐藤　慶浩	日本ヒューレット・パッカード株式会社
澤田　英繁	株式会社エヌ・ティ・ティ・データ
三瓶　徹	社団法人電気通信事業者協会
塩野　周一	マカフィー株式会社

瀬古　敏智	フィッシング対策協議会
外村　慶	株式会社シマンテック
高木　浩光	独立行政法人産業技術総合研究所（ＡＩＳＴ）
高橋　誠	一般社団法人日本オンラインゲーム協会
高橋　正和	日本マイクロソフト株式会社
高橋　幸雄	独立行政法人情報通信研究機構（ＮＩＣＴ）
瀧本　正人	伊藤忠テクノソリューションズ株式会社
武智　洋	日本セキュリティオペレーション事業者協議会（ISOG-J）
立道　豊典	日本電気株式会社
谷川　哲司	日本電気株式会社
谷口　浩一	日本アイ・ビー・エム株式会社
丹京　真一	日本セキュリティオペレーション事業者協議会（ISOG-J）
徳田　敏文	日本アイ・ビー・エム株式会社
外所　宏章	トレンドマイクロ株式会社
中島　寛	社団法人日本ケーブルテレビ連盟
西本　逸郎	株式会社ラック
二宮　温子	株式会社シマンテック
沼田　文彦	独立行政法人情報通信研究機構（ＮＩＣＴ）
野澤　篤史	株式会社日立製作所
萩原　健太	トレンドマイクロ株式会社
萩原　和典	株式会社エヌ・ティ・ティ・データ
早貸　淳子	フィッシング対策協議会
平林　純一	独立行政法人情報処理推進機構（ＩＰＡ）
藤川　春久	特定非営利活動法人日本データセンター協会
古岡　宏理	ＳＣＳＫ株式会社
堀越　朝久	日本電気株式会社
松本　泰	特定非営利活動法人日本データセンター協会
真鍋　敬士	一般社団法人ＪＰＣＥＲＴコーディネーションセンター(JPCERT/CC)
溝口　紀子	チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
水戸　和	特定非営利活動法人日本データセンター協会
宮田　康	株式会社ラック
明神　浩	社団法人テレコムサービス協会
村上　智	株式会社シマンテック
望月　貴仁	ヤフー株式会社
本橋　裕次	マカフィー株式会社
守屋　英一	日本アイ・ビー・エム株式会社
矢橋　康雄	社団法人電気通信事業者協会
山岡　正輝	エヌ・ティ・ティ・データ株式会社
油井　秀人	一般社団法人情報サービス産業協会（ＪＩＳＡ） （会員　富士通エフ・アイ・ピー株式会社）
吉田　奨	ヤフー株式会社

米澤　一樹	株式会社シマンテック
渡邊　創	独立行政法人産業技術総合研究所（ＡＩＳＴ）
渡辺　貴仁	独立行政法人情報処理推進機構（ＩＰＡ）

（事務局）

四方　光	警察庁生活安全局情報技術犯罪対策課　課長
岸田　憲夫	警察庁生活安全局情報技術犯罪対策課　情報技術犯罪捜査指導室長
大橋　一夫	警察庁生活安全局情報技術犯罪対策課　理事官
米田　茂雄	警察庁生活安全局情報技術犯罪対策課　理事官（平成23年８月まで）
蔵原　智行	警察庁生活安全局情報技術犯罪対策課　課長補佐
田川　顕	警察庁生活安全局情報技術犯罪対策課　課長補佐
内野　雅則	警察庁生活安全局情報技術犯罪対策課　課長補佐（平成23年８月まで）
人見　友章	警察庁生活安全局情報技術犯罪対策課　専門官
丸山　篤	警察庁生活安全局情報技術犯罪対策課　係長
入江　雄大	警察庁生活安全局情報技術犯罪対策課　係長
廣瀬　陽一	警察庁生活安全局情報技術犯罪対策課　係長
田中　純人	警察庁生活安全局情報技術犯罪対策課　主任
佐藤　健治	総務省情報流通政策局情報セキュリティ対策室　室長
中野　正康	総務省情報流通政策局情報セキュリティ対策室　室長（平成23年７月まで）
武馬　慎	総務省情報流通行政局情報セキュリティ対策室　課長補佐
中谷　純之	総務省情報流通行政局情報セキュリティ対策室　課長補佐
長瀬　貴志	総務省情報流通行政局情報セキュリティ対策室　課長補佐
牧野　知子	総務省情報流通行政局情報セキュリティ対策室　係長
波間　広輔	総務省情報流通行政局情報セキュリティ対策室
江口　純一	経済産業省商務情報政策局情報セキュリティ政策室　室長
山田　安秀	経済産業省商務情報政策局情報セキュリティ政策室　室長（平成23年７月まで）
乃田　昌幸	経済産業省商務情報政策局情報セキュリティ政策室　課長補佐
林　　弘毅	経済産業省商務情報政策局情報セキュリティ政策室　課長補佐（平成23年８月まで）
枝川　慶彦	経済産業省商務情報政策局情報セキュリティ政策室　係長

（オブザーバ）

高田　充人	内閣官房情報セキュリティセンター（ＮＩＳＣ）　参事官（平成23年７月まで）
伊貝　耕	内閣官房情報セキュリティセンター（ＮＩＳＣ）　参事官補佐
木原　栄治	内閣官房情報セキュリティセンター（ＮＩＳＣ）　参事官補佐
佐藤　朝哉	内閣官房情報セキュリティセンター（ＮＩＳＣ）　主査
松元　泰裕	消費者庁消費者政策課　政策調査員

（敬称略）