別紙１

不正アクセス行為の発生状況

第１　平成24年中の不正アクセス禁止法違反事件の認知・検挙状況等について

平成24年中に都道府県警察から警察庁に報告のあった不正アクセス行為を対象とした。

１　不正アクセス行為の認知状況

(1)　認知件数

平成24年中の不正アクセス行為の認知件数[注1]は1,251件で、前年と比べ、362件増加した。

表１－１　不正アクセス行為の認知件数の推移

区分＼年次		平成20年	平成21年	平成22年	平成23年	平成24年
認知件数		2,289	2,795	1,885	889	1,251
	海外からのアクセス	214	40	57	110	122
	国内からのアクセス	1,993	2,673	1,755	678	987
	アクセス元不明	82	82	73	101	142

(参考)「連続自動入力プログラムによる不正ログイン攻撃[注2]」による不正アクセス行為

不正アクセス行為については、表１－１の記載とは別に、一部の事業者から都道府県警察が新たに提供を受けることとした資料により、平成24年５月以降、114,013件の「連続自動入力プログラムによる不正ログイン攻撃」による不正アクセス行為が報告された。

注1　ここでいう認知件数とは、不正アクセス被害の届出を受理した場合のほか、余罪として確認した場合、報道を踏まえて確認した場合、援助の申出を受理した場合、その他関係資料により不正アクセス行為の事実確認ができた場合において、被疑者が行った構成要件に該当する行為の数をいう。なお、本文「(参考)」として記載の連続自動入力プログラムによる不正ログイン攻撃については、ＩＤ・パスワードの正規利用権者に対する確認を行っていないことから、従来の認知件数と同様の不正アクセス行為の事実確認ができた場合とまではいえず、別に記載した。

注2　連続自動入力プログラムによる不正ログイン攻撃とは、インターネット利用者の多くが複数サイトで同一のＩＤ・パスワードを使い回ししている状況に目を付け、不正取得した他人のＩＤ・パスワードのリストを悪用して、連続自動入力プログラムを用いてＩＤ・パスワードを入力し、不正アクセス行為を敢行する手口の攻撃をいう。

(2)　被害に係る特定電子計算機のアクセス管理者[注3]

被害に係る特定電子計算機のアクセス管理者をみると、一般企業が最も多く（1,163件）、次いで行政機関（52件）となっている。

表１－２　被害を受けた特定電子計算機のアクセス管理者の推移

区分＼年次	平成20年	平成21年	平成22年	平成23年	平成24年
一般企業	685	466	457	762	1,163
プロバイダ	1,589	2,321	1,405	115	22
大学、研究機関等	5	4	2	1	12
その他	10	4	21	11	54
うち行政機関	6	3	13	6	52
不明	0	0	0	0	0
計	2,289	2,795	1,885	889	1,251

※　「プロバイダ」とは、インターネットに接続する機能を提供する電気通信事業者をいう。
「大学、研究機関等」には、高等学校等の学校機関を含む。
「その他」の「うち行政機関」には、独立行政法人、特殊法人、地方公共団体及びこれらの附属機関を含む。

(3)　認知の端緒

認知の端緒としては、利用権者[注4]からの届出によるものが最も多く（892件）、次いで警察職員による被疑者の取調べ等の警察活動によるもの（270件）、被害を受けた特定電子計算機のアクセス管理者からの届出によるもの（80件）、発見者からの通報によるもの（５件）の順となっている。

表１－３　認知の端緒の推移

区分＼年次	平成20年	平成21年	平成22年	平成23年	平成24年
利用権者からの届出	656	487	314	680	892
警察活動	1,567	2,277	1,488	75	270
アクセス管理者からの届出	60	21	66	121	80
発見者からの通報	4	7	9	7	5
その他	2	3	8	6	4
計	2,289	2,795	1,885	889	1,251

注3　特定電子計算機とは、ネットワークに接続されたコンピュータをいい、アクセス管理者とは、特定電子計算機を誰に利用させるかを決定する者をいう。例えば、インターネットへの接続や電子メールの受信についてはプロバイダが、インターネットショッピング用のホームページの閲覧についてはその経営者が、それぞれアクセス管理者となる。

注4　利用権者とは、特定電子計算機をネットワークを通じて利用することについて、当該特定電子計算機のアクセス管理者の許諾を得た者をいう。例えば、プロバイダからインターネット接続サービスを受けることを認められた会員や企業からＬＡＮを利用することを認められた社員が該当する。

(4)　不正アクセス行為後の行為

不正アクセス行為後の行為としては、オンラインゲーム、コミュニティサイトの不正操作（他人のアイテムの不正取得等）が最も多く（662件)、次いでインターネットショッピングの不正購入（223件)、情報の不正入手（99件)、インターネットバンキングの不正送金（95件)、ホームページの改ざん・消去（42件)、インターネット・オークションの不正操作（他人になりすましての出品・落札）(29件)、不正ファイルの蔵置（１件）の順となっている。

表１－４　不正アクセス行為後の行為の内訳

区分＼年次	平成23年	平成24年
オンラインゲーム、コミュニティサイトの不正操作	358	662
インターネットショッピングの不正購入	172	223
情報の不正入手	74	99
インターネットバンキングの不正送金	188	95
ホームページの改ざん・消去	28	42
インターネット・オークションの不正操作	22	29
不正ファイルの蔵置	4	1
その他	43	100

２　不正アクセス禁止法違反事件の検挙状況

(1)　検挙件数等

平成24年中における不正アクセス禁止法違反の検挙件数は543件、検挙人員は154人と、前年と比べ、検挙件数は295件増加し、検挙人員は40人増加した。その内訳をみると、不正アクセス行為に係るものがそれぞれ533件、151人、識別符号提供行為[注5]に係るものがそれぞれ４件、４人であったほか、平成24年５月１日に施行された不正アクセス行為の禁止等に関する法律の一部を改正する法律（平成24年法律第12号）により新設された罪については、識別符号の取得行為[注6]が２件、２人、識別符号の保管行為[注7]が２件、２人、フィッシング行為[注8]が２件、１人であった。

表２－１　検挙件数等の推移

区分＼年次		平成20年	平成21年	平成22年	平成23年	平成24年
不正アクセス行為	検挙件数	1,737	2,532	1,598	242	533
	検挙事件数[注9]	101	95	103	101	133
	検挙人員	135	114	123	110	151
識別符号提供（助長）行為	検挙件数	3	2	3	6	4
	検挙事件数	3	1	3	6	4
	検挙人員	3	1	4	6	4
識別符号取得行為	検挙件数					2
	検挙事件数					2
	検挙人員					2
識別符号保管行為	検挙件数					2
	検挙事件数					2
	検挙人員					2
フィッシング行為	検挙件数					2
	検挙事件数					1
	検挙人員					1
計	検挙件数（件）	1,740	2,534	1,601	248	543
	検挙事件数（事件）	101（重複3）	95（重複1）	104（重複2）	103（重複4）	136（重複6）
	検挙人員（人）	137（重複1）	114（重複1）	125（重複2）	114（重複2）	154（重複6）

※　（重複）とは、各行為の重複を示す。

注5　他人の識別符号をアクセス管理者や利用権者に無断で第三者に提供する行為をいう。

注6　不正アクセスの目的で他人の識別符号を取得する行為をいう。

注7　不正アクセスの目的で他人の識別符号を保管する行為をいう。

注8　アクセス管理者になりすまし、当該アクセス制御機能にかかる識別符号の入力を求める行為をいう。いわゆるフィッシングサイトを公衆が閲覧できる状態に置く行為等。

注9　事件数とは、事件単位ごとに計上した数であり、一連の捜査で複数の件数の犯罪を検挙した場合は１事件と数える。

(2)　不正アクセス行為の態様

検挙件数を不正アクセス行為の態様別にみると、識別符号窃用型[注10]が532件であり、セキュリティ・ホール攻撃型[注11]は１件であった。

表２－２　不正アクセス行為の態様の推移

区分＼年次		平成20年	平成21年	平成22年	平成23年	平成24年
識別符号窃用型	検挙件数	1,736	2,529	1,597	241	532
	検挙事件数	100	94	102	100	133
セキュリティ・ホール攻撃型	検挙件数	1	3	1	1	1
	検挙事件数	1	1	1	1	1
計	検挙件数（件）	1,737	2,532	1,598	242	533
	検挙事件数（事件）	101	95	103	101	133（重複1）

３　検挙事件の特徴

(1)　不正アクセス行為の手口

検挙した不正アクセス禁止法違反に係る不正アクセス行為の手口についてみると、言葉巧みに利用権者から聞き出した又はのぞき見たものが最も多く（229件）、次いで利用権者のパスワードの設定・管理の甘さにつけ込んだもの（122件）となっている。また、識別符号を知り得る立場にあった元従業員や知人等によるもの（101件）、スパイウェア等のプログラムを使用して識別符号を入手したもの（29件）、共犯者等から入手したもの（22件）、フィッシングサイトにより入手したもの（18件）等も依然として発生している。

注10　アクセス制御されているサーバに、ネットワークを通じて、他人の識別符号を入力して不正に利用する行為（不正アクセス禁止法第２条第４項第１号に該当する行為）をいう。

注11　アクセス制御されているサーバに、ネットワークを通じて情報（他人の識別符号を入力する場合を除く。）や指令を入力して不正に利用する行為（不正アクセス禁止法第２条第４項第２号又は第３号に該当する行為）をいう。例えば、セキュリティの脆弱性を突いて操作指令を与えるなどの手法による不正アクセス行為が該当する。

表３－１　不正アクセス行為に係る犯行の手口の内訳

区分＼年次		平成23年	平成24年
識別符号窃用型		241	532
	言葉巧みに利用権者から聞き出した又はのぞき見たもの	29	229
	利用権者のパスワードの設定・管理の甘さにつけ込んだもの	59	122
	識別符号を知り得る立場にあった元従業員や知人等によるもの	52	101
	スパイウェア[注12]等のプログラムを使用して識別符号を入手したもの	1	29
	共犯者等から入手したもの	38	22
	フィッシングサイトにより入手したもの	59	18
	他人から購入したもの	0	0
	ファイル交換ソフトや暴露ウイルスで流出した識別符号を含む情報を利用したもの	0	0
	その他	3	11
セキュリティ・ホール攻撃型		1	1

(2)　被疑者

不正アクセス禁止法違反に係る被疑者と識別符号を窃用された利用権者の関係についてみると、元交際相手や元従業員等の顔見知りの者によるものが最も多く（75人）、次いで交友関係のない他人によるもの（60人）、ネットワーク上の知り合いによるもの（19人）となっている。

また、被疑者の年齢についてみると、10歳代（64人）が最も多く、20歳代（34人）、40歳代（28人）、30歳代（21人）、50歳代（６人）及び60歳代（１人）の順となっている。

なお、最年少の者は14歳、最年長の者は65歳であった。

表３－２　年代別被疑者数の推移

区分＼年次	平成20年	平成21年	平成22年	平成23年	平成24年
10歳代　（人）	48	31	29	51	64
20歳代	42	33	39	30	34
30歳代	35	35	35	19	21
40歳代	11	13	17	10	28
50歳代	1	2	5	2	6
60歳代	0	0	0	2	1
計	137	114	125	114	154

注12　パソコン内のファイル又はキーボードの入力情報、表示画面の情報等を取り出して、漏えいさせる機能を持つプログラムをいう。

(3)　不正アクセス行為の動機

不正アクセス行為の動機としては、オンラインゲームやコミュニティサイトで不正操作を行うためが最も多く（219件）、次いで嫌がらせや仕返しのため（100件）、好奇心を満たすため（85件）、不正に経済的利益を得るため（79件）の順となっている。

表３－３　不正アクセス行為の動機の内訳

区分＼年次	平成23年	平成24年
オンラインゲームやコミュニティサイトで不正操作を行うため	39	219
嫌がらせや仕返しのため	58	100
好奇心を満たすため	32	85
不正に経済的利益を得るため	97	79
顧客データの収集等情報を不正に入手するため	15	38
料金の請求を免れるため	0	10
その他	1	2
計	242	533

(4)　利用されたサービス

検挙した不正アクセス禁止法違反に係る識別符号窃用型の不正アクセス行為（532件）について、当該識別符号を入力することにより利用されたサービスをみると、オンラインゲーム、コミュニティサイトが最も多く（318件）、次いで会員専用・社員用内部サイト（98件）、電子メール（44件）、インターネットバンキング（31件）、インターネットショッピング（28件）、ホームページ公開サービス（８件）、インターネット・オークション（５件）の順となっている。

表３－４　利用されたサービスの内訳

区分＼年次		平成23年	平成24年
識別符号窃用型　（件）		241	532
	オンラインゲーム、コミュニティサイト	83	318
	会員専用・社員用内部サイト	16	98
	電子メール	23	44
	インターネットバンキング	14	31
	インターネットショッピング	87	28
	ホームページ公開サービス	5	8
	インターネット・オークション	4	5
	その他	9	0

4　都道府県公安委員会による援助措置

平成24年中、不正アクセス禁止法第９条の規定に基づき、都道府県公安委員会がアクセス管理者に対して行った助言・指導はなかった。

表４－１　都道府県公安委員会の援助措置実施件数の推移

区分＼年次	平成20年	平成21年	平成22年	平成23年	平成24年
援助措置	1	0	0	0	0

5　防御上の留意事項

(1)　利用権者の講ずべき措置

ア　フィッシングに対する注意

電子メールにより、本物のウェブサイトに酷似したフィッシングサイトに誘導したり、添付されたファイルを開かせたりして、ＩＤ・パスワードやクレジットカード情報を不正に取得する事案が多発していることから、発信元に心当たりのない電子メールに注意する。また、金融機関等が電子メールで口座番号や暗証番号、個人情報を問い合わせることはなく、これらの情報の入力を求める電子メールはフィッシングメールであると考えられることから、情報を入力しない。

イ　パスワードの適切な設定・管理

言葉巧みに聞き出したＩＤ・パスワードによる不正アクセス行為、利用権者のパスワードの設定の甘さにつけ込んだ不正アクセス行為、知人等による不正アクセス行為が発生していることから、パスワードを設定する場合には、ＩＤと全く同じパスワードやＩＤの一部を使ったパスワード等、パスワードの推測が容易なものは避ける､複数のサイトで同じパスワードを使用しないなどの対策を講じる。また、パスワードを他人に教えない、パスワードを定期的に変更するなど自己のパスワードを適切に管理する。

ウ　不正プログラムに対する注意

コンピュータに不正プログラムを感染させ、他人のＩＤ・パスワードを不正に取得する事案が発生していることから、信頼できない電子メールに添付されたファイルを不用意に開いたり、信頼できないウェブサイト上に蔵置されたファイルをダウンロードしたりしない。また、不特定多数が利用するコンピュータでは重要な情報を入力しない。さらに、コンピュータ・ウイルス対策等の不正プログラム対策（ウイルス対策ソフトの利用のほか、オペレーティングシステムやウイルス対策ソフトを含む各種ソフトウェアのアップデート等）を適切に講ずる。

(2)　アクセス管理者等の講ずべき措置

ア　フィッシング等への対策

フィッシング等により不正に取得したＩＤ・パスワードを使用した不正アクセス行為が多発していることから、インターネットショッピング、オンラインゲーム、インターネットバンキング等のサービスを提供する事業者にあっては、ワンタイムパスワード[注13]等により個人認証を強化するなどの対策を講ずる。

注13　インターネット銀行等における認証用のパスワードであって、認証の度にそれを構成する文字列が変わるものをいう。これを導入することにより、識別符号を盗まれても次回の利用時に使用できないこととなる。

イ　パスワードの適切な設定・運用体制の構築

利用権者のパスワードの設定の甘さにつけ込んだ不正アクセス行為が多発していることから、アクセス管理者は、容易に推測されるパスワードを設定できないようにする、定期的にパスワードの変更を促す仕組みを構築する、複数のサイトで同じパスワードを使用することの危険性を周知するなどの措置を講ずる。

ウ　ＩＤ・パスワードの適切な管理

ＩＤ・パスワードを知り得る立場にあった元従業員による不正アクセス行為も引き続き発生していることから、従業員が退職した時や特定電子計算機を利用する立場でなくなった時には、当該従業員に割り当てていたＩＤを削除したり、パスワードを変更したりするなど識別符号の適切な管理を徹底する。

エ　セキュリティ・ホール攻撃への対応

セキュリティ・ホール攻撃の一つであるＳＱＬインジェクション攻撃[注14]を受け、クレジットカード番号等の個人情報が流出する事案や、Ｗｅｂサーバの脆弱性に対する攻撃を受け、ホームページが改ざんされる事案が発生していることから、アクセス管理者は、プログラムを点検してセキュリティ上の脆弱性を解消するとともに、攻撃の兆候を即座に検知するための侵入検知システム等を導入し、セキュリティ・ホール攻撃に対する監視体制を強化する。

６　検挙事例

１	**サーバのセキュリティ・ホールを攻撃して不正アクセスを行い、記録されていた複数のＩＤ・パスワードを入手するとともに、これらをインターネット上の掲示板に投稿して他人に提供した不正アクセス禁止法違反事件**

無職の少年（15）は、平成24年５月、無料ホームページサービスを提供するサーバのセキュリティ・ホールを攻撃して不正アクセスし、同サーバ内に記録されていた複数の会員のＩＤ・パスワードを不正に入手した上で、これらをハッカー仲間らが使用する掲示板上に投稿して他人に提供した。平成24年６月、不正アクセス禁止法違反で検挙した（京都）。

２	**他人が契約した無線ＬＡＮを無断利用してインターネットに接続し、他人になりすましてメールサーバに不正アクセスした上で、嫌がらせメールを送信した不正アクセス禁止法違反事件**

高校生の少年（17）は、平成23年10月、通学路付近の複数の無線ＬＡＮ電波を無断利用してインターネットに接続のうえ、同級生が使用するメールアカウント用のＩＤ・パスワードを使用してメールサーバに不正アクセスした上で、同人に嫌がらせメールを送信した。平成24年７月、不正アクセス禁止法違反等で検挙した（警視庁）。

３	**大手チケット販売サイトに他人のＩＤ・パスワードを使用して不正アクセスを行い、大量の観劇チケット等を不正に購入して換金した不正アクセス禁止法違反及び電子計算機使用詐欺事件**

注14 ＳＱＬというプログラム言語を用いて、企業等が個人情報を管理するデータベースを外部から不正に操作する行為をいう。

無職の男（42）らは、平成24年１月から９月までの間、他人のＩＤからそのパスワードを推測して大手チケット販売サイトに不正アクセスを行い、利用権者があらかじめ登録していたクレジットカード情報を使用して観劇チケット等を大量に不正購入した上、チケットショップでこれを換金した。平成24年10月、不正アクセス禁止法違反及び電子計算機使用詐欺で検挙した（広島）。

４	**大手コミュニティサイトのフィッシングサイトを海外サーバ上に構築し、複数の利用権者からＩＤ・パスワードを不正に取得した不正アクセス禁止法違反事件**

中学生の少年（14）は、平成24年５月、大手コミュニティサイトのログイン画面に酷似したフィッシングサイトを海外のサーバに開設した上、自己が開設するブログに同フィッシングサイトに誘引する書き込みを投稿して、他人のＩＤ・パスワードを不正に要求した。平成24年12月、不正アクセス禁止法違反で検挙した（熊本）。

５	**元勤務先のサーバに不正アクセスを行い、同サーバ内のブログデータを消去して同社の業務を妨害した不正アクセス禁止法違反及び電子計算機損壊等業務妨害事件**

風俗店従業員の男（22）は、平成24年３月、元勤務先のホームページ管理用サーバに管理者用のＩＤ・パスワードを入力して不正アクセスを行い、同サーバに記憶・蔵置されていたブログデータを消去し、同社の業務を妨害した。平成24年６月、不正アクセス禁止法違反及び電子計算機損壊等業務妨害で検挙した（愛知）。

（参考）　不正アクセス関連行為の関係団体への届出状況について

○　独立行政法人情報処理推進機構（IPA）に届出のあったコンピュータ不正アクセスの届出状況について

IPA では、不正アクセス被害の実態を把握し、その防止に関する啓発を行うため、情報産業、企業の情報部門、個人ユーザ等から、広くコンピュータ不正アクセスの被害情報の届出を受け付け、その被害状況、防止策を定期的に公表している。

１．<u>不正アクセスに関する届け出状況</u>
（平成24年中にIPAに届出のあったコンピュータ不正アクセス（注１）が対象）

平成 24 年中のコンピュータ不正アクセスに関する届出件数は 121 件（平成 23 年：103 件）であった。（注２）
平成 24 年は同 23 年と比べて、18 件（約 17%）増加した。
届出のうち実際に被害があったケースにおける被害内容の分類では、「侵入」及び「なりすまし」による被害届出が多く寄せられた。
以下に、種々の切り口で分類した結果を示す。
※個々の件数には未遂（実際の被害はなかったもの）も含まれる。
※また、１件の届出にて複数の項目に該当するものがあるため、それぞれの分類での総計件数はこの数字に必ずしも一致しない。

(1) 手口別分類
意図的に行う攻撃行為による分類である。総計は 255 件（平成 23 年：180 件）あった。
※１件の届出について複数の攻撃行為を受けている場合もあるため、届出件数とは一致せず

ア　不正アクセスによる侵入行為
侵入行為に係る攻撃等の届出は 201 件（平成 23 年：145 件）あった。
(ｱ) 侵入の事前調査行為
システム情報の調査、稼働サービスの調査、アカウント名の調査等である。
６件の届出があり、ポートやセキュリティホールを探索するものであった。
(ｲ) 権限取得行為（侵入行為）

パスワード推測やソフトウェアのバグ等いわゆるセキュリティホールを利用した攻撃やシステムの設定内容を利用した攻撃等侵入のための行為である。

99 件の届出があり、これらのうち実際に侵入につながったものは 47 件である。

【主な内容】

ソフトウェアのぜい弱性やバグを利用した攻撃：14 件

パスワード推測：11 件

(ｳ) 不正行為の実行及び目的達成後の行為

侵入その他、何らかの原因により不正行為を実行されたことについては 96 件の届出があった。

【主な内容】

ファイル等の改ざん、破壊等：41 件

プログラムの作成・設置（インストール）、トロイの木馬等の埋め込み等：21 件

裏口（バックドア）の作成：10 件

踏み台とされて他のサイトへのアクセスに利用された：９件

資源利用（ファイル、CPU 使用）：３件

証拠の隠滅（ログの消去等）：３件

イ　サービス妨害攻撃

過負荷を与えたり、例外処理を利用してサービスを不可若しくは低下させたりする攻撃である。10 件（平成 23 年：７件）の届出があった。

ウ　その他

その他にはメール不正中継やメールアドレス詐称、正規ユーザになりすましてのサービスの不正利用、ソーシャルエンジニアリング等が含まれ、44 件（平成 23 年：28 件）の届出があった。

【主な内容】

正規ユーザへのなりすまし：41 件

メールの不正中継：１件

ディレクトリ・トラバーサル：１件

(2) 原因別分類

不正アクセスを許した問題点／弱点による分類である。

121 件の届出中、実際に被害に遭った計 105 件（平成 23 年：75 件）を分類

すると次のようになる。

被害原因として「ID、パスワード管理不備」や「古いバージョン使用、パッチ未導入等」が多くなっているなど、基本的なセキュリティ対策がなされていないサイトが狙われていると推測される。また、原因が不明なケースがますます多くなっており、手口が巧妙化するとともに原因究明が困難な事例が多いことが推測される。

【主な要因】

ID、パスワード管理の不備によると思われるもの：18 件

古いバージョンの利用や、パッチ・必要なプラグイン等の未導入によるもの：15 件

DoS 攻撃・その他によるもの：９件

設定の不備（セキュリティ上問題のあるデフォルト設定を含む。）によるもの：７件

原因不明：56 件

(3) 電算機分類

不正アクセス行為の対象となった機器による分類である（被害の有無は問わない。）。

【主な対象】

WWW サーバ：64 件

メールサーバ：14 件

クライアント：５件

その他のサーバ：５件

不明：26 件

※１件の届出で複数の項目に該当するものがある。

(4) 被害内容分類

121 件の届出を被害内容で分類した 133 件中、実際に被害に遭ったケースにおける被害内容による分類である。機器に対する実被害があった件数は 117 件（昨年：81 件）である。

なお、対処に係る工数やサービスの一時停止、代替機の準備等に関する被害は除外している。

【主な被害内容】

ホームページ改ざん：38 件

踏み台として悪用：25 件

オンラインサービスの不正利用：20 件

サービス低下：13 件

データの窃取や盗み見：８件
※１件の届出で複数の項目に該当するものがある。

２．対策情報

平成 23 年は CMS（Content Management System）のぜい弱性を悪用したウェブサイト改ざんの届出が増加したが、平成 24 年はそれに加えてサーバ管理ツールのぜい弱性を悪用したウェブサイト改ざんが多かったといえる。また、被害原因の多くが不明であったことから、こうした改ざんを行うための攻撃手口の巧妙化がうかがえる。その他では、なりすましによってオンラインゲーム等のサービスを勝手に使われて金銭被害が出たケースや、メールアカウントを窃取されて迷惑メール送信に悪用されていた被害も目立っていたといえる。主に原因不明なケースが多く見受けられたが、基本的なセキュリティ対策を実施していれば、被害を免れていたと思われるケースが多く見受けられる。システム管理者は次の点を確認して総合的に対策を行うことが望まれる。

- ID やパスワードの厳重な管理及び設定
- ぜい弱性の解消（修正プログラム適用不可の場合は、運用による回避策も含む。）
- ルータやファイアウォール等の設定やアクセス制御設定
- こまめなログのチェック

また、個人ユーザにおいても同様に次の点に注意することが望まれる。

- Windows Update や Office Update 等､OS やアプリケーションソフトのアップデート
- パスワードの設定と管理（複雑化、定期的に変更、安易に他人に教えない等）
- ルータやパーソナルファイアウォールの活用
- 無線 LAN の暗号化設定確認（WEP は使用せず、できる限り WPA2 を使用する。）

（参照）
【システム管理者向け】
「icat」サイバーセキュリティ注意喚起サービス
http://www.ipa.go.jp/security/vuln/icat.html
「情報セキュリティに関する啓発資料」
http://www.ipa.go.jp/security/fy18/reports/contents/
「脆弱性対策のチェックポイント」

http://www.ipa.go.jp/security/vuln/20050623_websecurity.html

「安全なウェブサイトの作り方　改訂第 6 版」

http://www.ipa.go.jp/security/vuln/websecurity.html

「JVN (Japan Vulnerability Notes)」　※脆弱性対策情報ポータルサイト

http://jvn.jp/

「SQL インジェクション攻撃に関する注意喚起」

http://www.ipa.go.jp/security/vuln/documents/2008/200805_SQLinjection.html

「古いソフトウェア製品を利用しているウェブサイトへの注意喚起」

http://www.ipa.go.jp/security/vuln/documents/2009/200903_update.html

「ウェブサイト管理者へ：ウェブサイト改ざんに関する注意喚起」

http://www.ipa.go.jp/security/topics/20091224.html

「IPA メールニュース」

http://www.ipa.go.jp/about/mail/

【個人ユーザ向け】

「ここからセキュリティ」情報セキュリティ・ポータルサイト

http://www.ipa.go.jp/security/kokokara/

「IPA セキュリティセンター・個人ユーザ向けページ」

http://www.ipa.go.jp/security/personal/

「Microsoft セキュリティセンター」（日本マイクロソフト社）

http://www.microsoft.com/ja-jp/security/default.aspx

「MyJVN」（セキュリティ設定チェッカ、バージョンチェッカ）

http://jvndb.jvn.jp/apis/myjvn/

「国内のインターネットバンキングで不正アクセスが相次いでいる問題について」

http://www.ipa.go.jp/security/topics/alert20110803.html

ウイルス対策を含むセキュリティ関係の情報・対策等については、下記ページを参照。

「IPA セキュリティセンタートップページ」

http://www.ipa.go.jp/security/

注１　コンピュータ不正アクセス

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。

注２　ここに挙げた件数は、コンピュータ不正アクセスの届出を IPA が受理した件であり、不正アクセスやアタック等に関して実際の発生件数や被害件数を直接類推できるような数値ではない。

○　一般社団法人 JPCERT コーディネーションセンター（以下、JPCERT/CC）に報告（調整対応依頼）があった不正アクセス関連行為の状況について

JPCERT/CC は、国内の情報セキュリティインシデントの被害低減を目的として、広く一般から不正アクセス関連行為を含むコンピュータセキュリティインシデントに関する調整対応依頼を受け付けている。

１．　不正アクセス関連行為の特徴および件数

（平成 24 年中に JPCERT/CC に報告（調整対応依頼）のあったコンピュータ不正アクセスが対象）

報告（調整対応依頼）のあった不正アクセス関連行為(注１)に係わる報告件数(注２)は 17,265 件であった。この報告を元にしたインシデント件数（注３）は 16,926 件であり、インシデントをカテゴリ別に分類すると以下の通りである。

（１）　プローブ、スキャン、その他不審なアクセスに関する報告

防御に成功したアタックや、コンピュータ／サービス／弱点の探査を意図したアクセス等、システムのアクセス権において特に問題のなかったもの（影響を生じないか又は無視できるアクセス）について 10,289 件の報告があった。

[1/1-3/31: 1,823 件、4/1-6/30:2,281 件、7/1-9/30:3,391 件、10/1-12/31: 2,794 件]

（２）　システムへの侵入

管理者権限の盗用が認められる場合やワーム等を含め、システムへの侵入について 1,814 件の報告があった。

[1/1-3/31: 142 件、4/1-6/30: 139 件、7/1-9/30:796 件、10/1-12/31: 737 件]

（３）　マルウエアサイト

閲覧することで PC がマルウエアに感染してしまう攻撃用サイトや攻撃に使用するマルウエアを公開しているサイトについて 786 件の報告があった。

[1/1-3/31: 162 件、4/1-6/30: 209 件、7/1-9/30:202 件、10/1-12/31: 213 件]

（４）　ネットワークやコンピュータの運用を妨害しようとする攻撃

大量のパケットや予期しないデータの送信によって、サイトのネットワークやホストのサービス運用を妨害しようとするアクセスについて 36 件の報告があった。

[1/1-3/31:7 件、4/1-6/30:11 件、7/1-9/30:12 件、10/1-12/31:6 件]

（５） Web 偽装事案(phishing)

Web のフォームなどから入力された口座番号やキャッシュカードの暗証番号といった個人情報を盗み取る Web 偽装事案について 1,324 件の報告があった。

[1/1-3/31: 324 件、4/1-6/30: 367 件、7/1-9/30: 273 件、10/1-12/31:360 件]

（６） その他

コンピュータウイルス、SPAM メールの受信等について 2,677 件の報告があった。

[1/1-3/31:77 件、4/1-6/30:825 件、7/1-9/30:592 件、10/1-12/31:1,183 件]

２．防御に関する啓発および対策措置の普及

JPCERT/CC は、日本国内のインターネット利用者に対して、不正アクセス関連行為を防止するための予防措置や、発生した場合の緊急措置などに関する情報を提供し、不正アクセス関連行為への認識の向上や適切な対策を促進するため、以下の文書を公開している(詳細は http://www.jpcert.or.jp/参照。)

（１） 注意喚起

[新規]

2012 年 1 月	Microsoft .NET Framework の複数の脆弱性に関する注意喚起 Adobe Reader 及び Acrobat の脆弱性に関する注意喚起 2012 年 1 月 Microsoft セキュリティ情報（緊急 1 件含）に関する注意喚起
2012 年 2 月	PHP 5.3.9 の脆弱性に関する注意喚起 Adobe Flash Player の脆弱性に関する注意喚起 2012 年 2 月 Microsoft セキュリティ情報（緊急 4 件含）に関する注意喚起
2012 年 3 月	Adobe Flash Player の脆弱性に関する注意喚起 DNS 設定を書き換えるマルウエア（DNS Changer）感染に関する注意喚起 2012 年 3 月 Microsoft セキュリティ情報（緊急 1 件含）に関する注意喚起 2012 年 2 月公開の Java SE の脆弱性を狙う攻撃に関する注意喚起 Adobe Flash Player の脆弱性に関する注意喚起

2012 年 4 月	Adobe Reader 及び Acrobat の脆弱性に関する注意喚起 2012 年 4 月 Microsoft セキュリティ情報（緊急 4 件含）に関する注意喚起
2012 年 5 月	Adobe Flash Player の脆弱性（APSB12-09）に関する注意喚起 2012 年 5 月 Microsoft セキュリティ情報（緊急 3 件含）に関する注意喚起 PHP の脆弱性に関する注意喚起 ロジテック社製ブロードバンドルータの脆弱性に関する注意喚起
2012 年 6 月	ISC BIND 9 サービス運用妨害の脆弱性に関する注意喚起 Adobe Flash Player の脆弱性（APSB12-14）に関する注意喚起 2012 年 6 月 Microsoft セキュリティ情報（緊急 3 件含）に関する注意喚起 2012 年 6 月 Java SE の脆弱性を狙う攻撃に関する注意喚起
2012 年 7 月	2012 年 7 月 Microsoft セキュリティ情報（緊急 3 件含）に関する注意喚起
2012 年 8 月	2012 年 8 月 Microsoft セキュリティ情報（緊急 5 件含）に関する注意喚起 Adobe Flash Player の脆弱性（APSB12-18）に関する注意喚起 Adobe Reader 及び Acrobat の脆弱性（APSB12-16）に関する注意喚起 Adobe Flash Player の脆弱性（APSB12-19）に関する注意喚起 MS-CHAP v2 の認証情報漏えいの問題に関する注意喚起
2012 年 9 月	2012 年 8 月 Java SE の脆弱性に関する注意喚起 ISC BIND 9 サービス運用妨害の脆弱性（CVE-2012-4244）に関する注意喚起 2012 年 9 月 Microsoft Internet Explorer の未修正の脆弱性に関する注意喚起
2012 年 10 月	Adobe Flash Player の脆弱性（APSB12-22）に関する注意喚起 ISC BIND 9 サービス運用妨害の脆弱性（CVE-2012-5166）に関する注意喚起 2012 年 10 月 Microsoft セキュリティ情報（緊急 1 件含）に関する注意喚起
2012 年 11 月	Adobe Flash Player の脆弱性（APSB12-24）に関する注意喚起 2012 年 11 月 Microsoft セキュリティ情報（緊急 4 件含）に関する注意喚起 2012 年 10 月公開の Java SE の脆弱性を狙う攻撃に関する注意喚起

2012 年 12 月	2012 年 12 月 Microsoft セキュリティ情報（緊急 5 件含）に関する注意喚起 Adobe Flash Player の脆弱性 (APSB12-27) に関する注意喚起

（２） 活動概要（報告状況等の公表）

発行日：2013-01-17 [2012 年 10 月 1 日～ 2012 年 12 月 31 日]
発行日：2012-10-10 [2012 年 7 月 1 日 ～ 2012 年 9 月 30 日]
発行日：2012-07-12 [2012 年 4 月 1 日 ～ 2012 年 6 月 30 日]
発行日：2012-04-12 [2012 年 1 月 1 日 ～ 2012 年 3 月 31 日]

（３） JPCERT/CC レポート

[発行件数] 50 件
[取り扱ったセキュリティ関連情報数] 276 件

注１ 不正アクセス関連行為とは、コンピュータやネットワークのセキュリティを侵害する人為的な行為で、意図的(または、偶発的) に発生する全ての事象が対象になる。

注２ ここにあげた件数は、JPCERT/CC が受け付けた報告の件数である。実際のアタックの発生件数や、被害件数を類推できるような数値ではない。また類型ごとの実際の発生比率を示すものでもない。一定以上の期間に渡るアクセスの要約レポートも含まれるため、アクセスの回数と報告件数も一般に対応しない。報告元には、国内外のサイトが含まれる。

注３ 「インシデント件数」は、各報告に含まれるインシデント件数の合計を示す。ただし、１つのインシデントに関して複数件の報告がよせられた場合は、１件のインシデントとして扱う。