不正アクセス行為の発生状況

第 1 平成25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25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25年中の不正アクセス行為の認知件数^{注1}は2,951件で、前年と比べ、1,700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 21年	平成 22年	平成 23年	平成 24年	平成 25年
認知件数		2,795	1,885	889	1,251	2,951
	海外からのアクセス	40	57	110	122	289
	国内からのアクセス	2,673	1,755	678	987	2,474
	アクセス元不明	82	73	101	142	188

(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、事業者から約80万件の「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。

当該不正アクセス行為の状況については別添参照。

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、余罪として新たな不正アクセス行為の事実を確認した場合、報道を踏まえて事業者等に不正アクセス行為の事実を確認した場合、その他関係資料により不正アクセス行為の事実を確認すること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)」として記載した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被害の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を確認すること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) 被害を受けた特定電子計算機のアクセス管理者^{注3}

被害を受けた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（2,893件）、次いで行政機関（24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 21年	平成 22年	平成 23年	平成 24年	平成 25年
一般企業		466	457	762	1,163	2,893
プロバイダ		2,321	1,405	115	22	9
大学、研究機関等		4	2	1	12	9
その他		4	21	11	54	40
	うち行政機関	3	13	6	52	24
	計	2,795	1,885	889	1,251	2,951

※ 「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、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が最も多く（1,208件）、次いで利用権者^{注4}からの届出によるもの（929件）、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（781件）、発見者からの通報によるもの（20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 21年	平成 22年	平成 23年	平成 24年	平成 25年
アクセス管理者からの届出		21	66	121	80	1,208
利用権者からの届出		487	314	680	892	929
警察活動		2,277	1,488	75	270	781
発見者からの通報		7	9	7	5	20
その他		3	8	6	4	13
	計	2,795	1,885	889	1,251	2,951

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、インターネットバンキングの不正送金が最も多く（1,325件）、次いでインターネットショッピングの不正購入（911件）、オンラインゲーム、コミュニティサイトの不正操作（379件）、ホームページの改ざん・消去（107件）、情報の不正入手（92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）（36件）、不正ファイルの蔵置（20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24年	平成25年
インターネットバンキングの不正送金		95	1,325
インターネットショッピングの不正購入		223	911
オンラインゲーム、コミュニティサイトの不正操作		662	379
ホームページの改ざん・消去		42	107
情報の不正入手		99	92
インターネット・オークションの不正操作		29	36
不正ファイルの蔵置		1	20
その他		100	81

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25年中における不正アクセス禁止法違反の検挙件数は980件、検挙人員は147人と、前年と比べ、検挙件数は437件増加し、検挙人員は7人減少した。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968件、144人、識別符号提供行為^{注5}に係るものがそれぞれ7件、7人、識別符号の取得行為^{注6}が2件、1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1件、1人であった。

表2-1 検挙件数等の推移

区分		年次	平成 21年	平成 22年	平成 23年	平成 24年	平成 25年
不正アクセス 行為	検挙件数		2,532	1,598	242	533	968
	検挙事件数 ^{注9}		95	103	101	133	142
	検挙人員		114	123	110	151	144
識別符号 提供（助長）行為	検挙件数		2	3	6	4	7
	検挙事件数		1	3	6	4	7
	検挙人員		1	4	6	4	7
識別符号 取得行為	検挙件数					2	2
	検挙事件数					2	1
	検挙人員					2	1
識別符号 保管行為	検挙件数					2	2
	検挙事件数					2	2
	検挙人員					2	2
フィッシング 行為	検挙件数					2	1
	検挙事件数					1	1
	検挙人員					1	1
計	検挙件数 （件）		2,534	1,601	248	543	980
	検挙事件数 （事件）		95 （重複1）	104 （重複2）	103 （重複4）	136 （重複6）	145 （重複8）
	検挙人員 （人）		114 （重複1）	125 （重複2）	114 （重複2）	154 （重複6）	147 （重複8）

※（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。平成24年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。

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。平成24年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により新設された罪。

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。平成24年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により新設された罪。

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965件であり、セキュリティ・ホール攻撃型^{注11}は3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 21年	平成 22年	平成 23年	平成 24年	平成 25年
識別符号窃用型	検挙件数	2,529	1,597	241	532	965
	検挙事件数	94	102	100	133	139
セキュリティ・ ホール攻撃型	検挙件数	3	1	1	1	3
	検挙事件数	1	1	1	1	3
計	検挙件数 (件)	2,532	1,598	242	533	968
	検挙事件数 (事件)	95	103	101	133 (重複1)	142

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、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が最も多く（767件）、次いで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（64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（56件）、共犯者等から入手したもの（35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（25件）、フィッシングサイトにより入手したもの（9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24年	平成25年
識別符号窃用型		532	965
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	767
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		229	64
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	56
共犯者等から入手したもの		22	35
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		29	25
フィッシングサイトにより入手したもの		18	9
他人から購入したもの		0	7
その他		11	2
セキュリティ・ホール攻撃型		1	3

(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（103人）、次いで交友関係のない他人によるもの（72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（44人）が最も多く、30歳代（37人）、20歳代（30人）、40歳代（27人）、50歳代（8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21年	平成22年	平成23年	平成24年	平成25年
10歳代（人）	31	29	51	64	44
20歳代	33	39	30	34	30
30歳代	35	35	19	21	37
40歳代	13	17	10	28	27
50歳代	2	5	2	6	8
60歳代	0	0	2	1	1
計	114	125	114	154	147

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、不正に経済的利益を得るためが最も多く（706件）、次いで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（77件）、嫌がらせや仕返しのため（56件）、顧客データの収集等情報を不正に入手するため（53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24年	平成25年
不正に経済的利益を得るため		79	706
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		219	77
嫌がらせや仕返しのため		100	56
顧客データの収集等情報を不正に入手するため		38	53
好奇心を満たすため		85	46
料金の請求を免れるため		10	25
その他		2	5
計		533	968

(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（965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、インターネットショッピングが最も多く（728件）、次いでオンラインゲーム、コミュニティサイト（138件）、電子メール（48件）、会員専用・社員用内部サイト（24件）、インターネットバンキング（7件）、ホームページ公開サービス（6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24年	平成25年
識別符号窃用型（件）		532	965
インターネットショッピング		28	728
オンラインゲーム、コミュニティサイト		318	138
電子メール		44	48
会員専用・社員用内部サイト		98	24
インターネットバンキング		31	7
ホームページ公開サービス		8	6
インターネット・オークション		5	5
その他		0	9

4 都道府県公安委員会による援助措置

平成25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16年	平成17年	平成18年	平成19年	平成20年	平成21年	平成22年	平成23年	平成24年	平成25年
援助措置		3	4	3	0	1	0	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と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。さらに、金融機関等が提供するワンタイムパスワード^{注13}等の個人認証方法を積極的に利用する。

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多発していることから、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多発していることから、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。金融機関等が提供するセキュリティ対策ソフトを積極的に利用する。

(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

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利用時に使用できないこととなる。

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とっては、ワンタイムパスワード等により個人認証を強化するなどの対策を講ずる。

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) 自称契約社員の男（42）は、平成24年6月から8月までの間、元勤務先の不動産仲介販売会社の会社情報が掲載されていた大手不動産情報サイト2社のサーバに不正アクセスを行い、同サーバに記録されていたデータを改変して損壊し、同社の業務を妨害した。平成25年1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（埼玉）。
- (2) 会社員の男（36）は、平成24年11月、少年（16）が利用しているブログサイトの管理者を装い、ブログサイトのパスワードを入力して返信するよう求める電子メールを少年の携帯電話に送り、少年にパスワードを返信させて識別符号を不正取得した。平成25年2月、不正アクセス禁止法違反で検挙した（香川）。
- (3) 無職の少年（15）は、平成25年2月、匿名化ソフト「T o r」で発信元を特定困難にさせた上で、他人の識別符号を入力して、レンタルサーバ会社のサーバに不正アクセスし、サーバ内に保存されている他人のパスワードやメールアドレスを変更した。平成25年4月、不正アクセス禁止法違反及び私電磁的記録不正作出で検挙した（京都）。
- (4) 自営業の男（36）は、平成24年4月、携帯電話販売店において、陳列中の携帯電話機を使用し、携帯音声通信事業者のサーバに不正アクセスした上、オンラインゲームサイトで使用できる仮想通貨の購入手続を行い、携帯電話販売店に料金を

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。

課金させて支払いを免れた。平成25年7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（愛知・三重）。

- (5) パチンコ店員の少年（18）は、平成25年2月、大手ゲーム会社になりすまし、同社の利用権者に対し、抽選に応募するために識別符号を入力してログインする必要がある旨の記載とともに識別符号の入力欄等を設け、同社の登録商標であるロゴを掲示したフィッシングサイトをレンタルサーバ会社のサーバ内に設置した。平成25年10月、不正アクセス禁止法及び商標法違反で検挙した（静岡）。

別添

「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の状況

約80万件の「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のうち、「約〇件」など概数により報告されたものを除いた604,153件の状況は次のとおり。

1 アクセス元

海外からのアクセス	67,295
国内からのアクセス	437,959
アクセス元不明	98,899
計	604,153

2 被害を受けた特定電子計算機のアクセス管理者

一般企業	604,000
プロバイダ	153
計	604,153

3 警察が把握した経緯

アクセス管理者からの届出	600,750
発見者からの通報	3,272
その他	131
計	604,153

4 不正アクセス行為後の行為（※）

情報の不正入手	283,119
インターネットショッピングの不正購入	4,084
不明	316,950
計	604,153

（※） 各欄の件数は、「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の被害を受けた事業者から、当該不正アクセス行為の後に行われた可能性のある行為として報告を受けたものである。

(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、個人ユーザー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、防止策を公表している。

1. 不正アクセスに関する届出状況

（平成25年1月1日から12月31日の間に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。）

コンピュータ不正アクセスに関する届出件数は168件（平成24年：121件）であった。（注2）

平成25年は同24年と比べて、47件（約39%）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件の届出で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。総計は373件（平成24年：255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、届出件数とは一致しない。

ア 侵入行為に関して

侵入行為に係る攻撃等の届出は243件（平成24年：201件）あった。

(7) 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。

5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。

(i) 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。

124 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 88 件。

【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：24 件

パスワード推測：14 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 114 件の届出があった。

【主な内容】

ファイル等の改ざん、破壊等：82 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：11 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：7 件

裏口（バックドア）の作成：5 件

証拠の隠滅（ログの消去等）：1 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止める、若しくは低下させたりする攻撃。36 件（平成 24 年：10 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、94 件（平成 24 年：44 件）の届出があった。

【主な内容】

正規ユーザへのなりすまし：80 件

メールアドレス詐称：8 件

メールの不正中継：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。

168 件の届出中、実際に被害に遭った計 158 件（平成 24 年：105 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】

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：27件

ID、パスワード管理の不備によると思われるもの：12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：6件

DoS 攻撃・その他によるもの：28件

原因不明：85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（被害の有無は問わない。）。

【主な対象】

WWW サーバ：103件

メールサーバ：34件

クライアント：16件

その他のサーバ：7件

不明：7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

168件の届出を被害内容で分類した205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。機器に対する実被害があった件数は195件（昨年：117件）。

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：75件

踏み台として悪用：50件

サービス低下：22件

オンラインサービスの不正利用：19件

データの窃取や盗み見：12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

2013 年は、過去にウェブサイト改ざんが流行した 2010 年、2012 年の約 2 倍に上る 75 件のウェブサイト改ざんに関する被害届出があった。

2013 年のウェブサイト改ざんの急増の理由には、過去（2010 年、2012 年）にウェブサイト改ざんが流行した際のいわゆる「ガンブラー」の手口と、ウェブサーバー上のソフトウェアなどの脆弱性を悪用する、簡単な FTP パスワードなどを推測して改ざんを行う、といった複数の手口を組み合わせたことによる手口の巧妙化が挙げられる。

届出内容を見ると、改ざんされたサイトの多くは、セキュリティ対策の不十分なパソコンで閲覧するとウイルスに感染するように細工されており、閲覧者のパソコンをウイルスに感染させることがウェブ改ざんの主な目的であったと言える。サイト管理者が対策を行うことはもちろんだが、一般利用者も、万が一改ざんされたページを閲覧してしまってもウイルスに感染しないように、十分なセキュリティ対策を行う必要がある。

手口は巧妙化しているものの、基本的な対策は以下のとおり従来から変わらない。なお、ウェブサイト管理者は、システム管理者向け対策のみならず、ウェブサイト更新用のパソコン上での対策も必要である。

システム管理者向け対策

- ・ OS、CMS などのアップデートを行い、サーバーの脆弱性を解消する
- ・ 複雑なパスワードにする、アカウントを共有しないなど、アカウント管理を見直す
- ・ アクセス元 IP アドレスによる接続制限などによりウェブサイトを更新できる場所を限定する
- ・ ウイルス感染を防止するためウェブサイト更新専用パソコンの導入を検討する

パソコン上での対策

- ・ OS、各種プログラム（Java、Flash Player、Adobe Reader）のアップデートを行い、パソコンの脆弱性を解消する
- ・ セキュリティソフトを使用する

(参照 URL)

【システム管理者向け参考情報】

「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/>

「ウェブサイトが改ざんされないように対策を！」(2013年6月の「呼びかけ」)

<http://www.ipa.go.jp/security/txt/2013/06outline.html>

「IPA メールニュース」

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

【個人ユーザ向け参考情報】

「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/>

「ウェブサイト改ざんの増加に関する一般利用者(ウェブ閲覧者)向け注意喚起」

<http://www.ipa.go.jp/security/topics/alert20130626.html>

※ウイルス対策を含むセキュリティ関係の情報・対策等

「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 が受理した件数であり、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 25 年 1 月 1 日から 12 月 31 日の間に 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 29,746 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 27,845 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、その他の不審なアクセス等、システムのアクセス権において影響を生じないか、無視できるアクセスについて 11,227 件の報告があった。
[1/1-3/31: 2,379 件、4/1-6/30:4,629 件、7/1-9/30:2,659 件、10/1-12/31: 1,560 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 7,409 件の報告があった。
[1/1-3/31: 1,184 件、4/1-6/30: 1,847 件、7/1-9/30:2,774 件、10/1-12/31: 1,604 件]

（3） マルウェアサイト

閲覧することで PC がマルウェ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ェアを公開しているサイトについて 945 件の報告があった。
[1/1-3/31: 181 件、4/1-6/30: 379 件、7/1-9/30:156 件、10/1-12/31: 229 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 127 件の報告があった。

[1/1-3/31:36 件、4/1-6/30:71 件、7/1-9/30:12 件、10/1-12/31:8 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 1,831 件の報告があった。

[1/1-3/31: 474 件、4/1-6/30: 287 件、7/1-9/30: 469 件、10/1-12/31:601 件]

(6) その他

コンピュータウイルス、SPAM メールを受信等について 6,306 件の報告があった。

[1/1-3/31:1,435 件、4/1-6/30:1,872 件、7/1-9/30:2,214 件、10/1-12/31:785 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.jpccert.or.jp/>参照。)

(1) 注意喚起

[新規]

2013 年 1 月	2013 年 1 月 Microsoft セキュリティ情報 (緊急 2 件含) に関する注意喚起 Adobe Reader 及び Acrobat の脆弱性 (APSB13-02) に関する注意喚起 Adobe Flash Player の脆弱性 (APSB13-01) に関する注意喚起 Oracle Java SE のクリティカルパッチアップデートに関する注意喚起 Microsoft Internet Explorer の脆弱性 (MS13-008) に関する注意喚起 Portable SDK for UPnP の脆弱性に関する注意喚起
2013 年 2 月	2013 年 2 月 Oracle Java SE のクリティカルパッチアップデートに関する注意喚起

	<p>Adobe Flash Player の脆弱性 (APSB13-04) に関する注意喚起</p> <p>Adobe Flash Player の脆弱性 (APSB13-05) に関する注意喚起</p> <p>2013年2月 Microsoft セキュリティ情報 (緊急 5件含) に関する注意喚起</p> <p>2013年2月 Oracle Java SE のクリティカルパッチアップデート (定例) に関する注意喚起</p> <p>Adobe Reader 及び Acrobat の脆弱性 (APSB13-07) に関する注意喚起</p> <p>Adobe Flash Player の脆弱性 (APSB13-08) に関する注意喚起</p>
2013年3月	<p>2013年3月 Oracle Java SE のクリティカルパッチアップデートに関する注意喚起</p> <p>Adobe Flash Player の脆弱性 (APSB13-09) に関する注意喚起</p> <p>2013年3月 Microsoft セキュリティ情報 (緊急 4件含) に関する注意喚起</p> <p>ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2013-2266) に関する注意喚起</p>
2013年4月	<p>旧バージョンの Parallels Plesk Panel の利用に関する注意喚起</p> <p>Adobe Flash Player の脆弱性 (APSB13-11) に関する注意喚起</p> <p>2013年4月 Microsoft セキュリティ情報 (緊急 2件含) に関する注意喚起</p> <p>2013年4月 Oracle Java SE のクリティカルパッチアップデート (定例) に関する注意喚起</p> <p>DNS の再帰的な問い合わせを使った DDoS 攻撃に関する注意喚起</p>
2013年5月	<p>Adobe Flash Player の脆弱性 (APSB13-14) に関する注意喚起</p> <p>Adobe Reader 及び Acrobat の脆弱性 (APSB13-15) に関する注意喚起</p> <p>2013年5月 Microsoft セキュリティ情報 (緊急 2件含) に関する注意喚起</p>
2013年6月	<p>ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2013-3919) に関する注意喚起</p> <p>Web サイト改ざんに関する注意喚起</p> <p>Adobe Flash Player の脆弱性 (APSB13-16) に関する注意喚起</p> <p>2013年6月 Microsoft セキュリティ情報 (緊急 1件含) に関する注意喚起</p> <p>2013年6月 Oracle Java SE のクリティカルパッチアップデート (定例) に関する注意喚起</p>

2013年7月	Adobe Flash Player の脆弱性 (APSB13-17) に関する注意喚起 2013年7月 Microsoft セキュリティ情報 (緊急 6件含) に関する注意喚起 Apache Struts の脆弱性 (S2-016) に関する注意喚起 ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2013-4854) に関する注意喚起
2013年8月	2013年8月 Microsoft セキュリティ情報 (緊急 3件含) に関する注意喚起
2013年9月	SIP サーバの不正利用に関する注意喚起 Adobe Reader 及び Acrobat の脆弱性 (APSB13-22) に関する注意喚起 Adobe Flash Player の脆弱性 (APSB13-21) に関する注意喚起 2013年9月 Microsoft セキュリティ情報 (緊急 4件含) に関する注意喚起 2013年9月 Microsoft Internet Explorer の未修正の脆弱性に関する注意喚起
2013年10月	Adobe Reader 及び Acrobat の脆弱性 (APSB13-25) に関する注意喚起 2013年10月 Microsoft セキュリティ情報 (緊急 4件含) に関する注意喚起 2013年10月 Oracle Java SE のクリティカルパッチアップデート (定例) に関する注意喚起
2013年11月	2013年11月 Microsoft Graphics Component の未修正の脆弱性に関する注意喚起 2013年11月 Microsoft セキュリティ情報 (緊急 3件含) に関する注意喚起 Adobe Flash Player の脆弱性 (APSB13-26) に関する注意喚起
2013年12月	Adobe Flash Player の脆弱性 (APSB13-28) に関する注意喚起 2013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

(2) 活動概要 (報告状況等の公表)

発行日：2014-01-16 [2013年10月1日～2012年12月31日]

発行日：2013-10-10 [2013年7月1日～2012年9月30日]

発行日：2013-07-11 [2013年4月1日～2012年6月30日]

発行日：2013-04-15 [2013年1月1日～2012年3月31日]

(3) JPCERT/CC レポート

[発行件数] 51 件

[取り扱ったセキュリティ関連情報数] 209 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。