不正アクセス行為の発生状況

第１　平成26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26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26年中の不正アクセス行為の認知件数[注1]は3,545件で、前年と比べ、594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22年	平成23年	平成24年	平成25年	平成26年
認知件数		1,885	889	1,251	2,951	3,545
	海外からのアクセス（※）	57	110	122	289	298
	国内からのアクセス（※）	1,755	678	987	2,474	2,469
	アクセス元不明	73	101	142	188	778

※　被害に遭ったコンピュータへの直近のアクセス元を示すものであるが、不正アクセス行為は複数のコンピュータを経由して行われることもあることから、必ずしも不正アクセス行為を行った者のアクセス元を示すものではなく、海外から国内のコンピュータを経由して不正アクセスしたような場合にも「国内からのアクセス」に分類される。

（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]の報告受理状況

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」によるログイン行為が報告され、そのうち「約○件」など概数により報告されたものを除いた629,632件の攻撃対象となったサービスは次のとおりであった。

攻撃対象となったサービス	ログイン件数
オンラインゲーム・コミュニティサイト	59,463
インターネットショッピング	21,235
インターネットバンキング	109
その他	548,825
合計	629,632

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。

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・パスワードを入力する攻撃をいう。なお、同攻撃については、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。

(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（3,468件）、次いで「大学、研究機関等」（56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24年	平成25年	平成26年
一般企業	1,163	2,893	3,468
大学、研究機関等	12	9	56
プロバイダ	22	9	16
その他	54	40	5
うち行政機関	52	24	3
計	1,251	2,951	3,545

※「大学、研究機関等」には、高等学校等の学校機関を含む。
「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。
「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（1,848件）、次いで利用権者[注4]からの届出によるもの（1,337件）、発見者からの通報によるもの（238件）、警察職員による特定電子計算機のアクセスログ解析等の警察活動によるもの（119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22年	平成23年	平成24年	平成25年	平成26年
アクセス管理者からの届出	66	121	80	1,208	1,848
利用権者からの届出	314	680	892	929	1,337
発見者からの通報	9	7	5	20	238
警察活動	1,488	75	270	781	119
その他	8	6	4	13	3
計	1,885	889	1,251	2,951	3,545

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（1,944件）、次いで「他人へのなりすまし」（1,009件）、「インターネットショッピングの不正購入」（209件）、「情報の不正入手」（177件）、「オンラインゲーム、コミュニティサイトの不正操作」(130件)、「ホームページの改ざん・消去」(40件)、「インターネット・オークションの不正操作」（13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25年	平成26年
インターネットバンキングの不正送金	1,325	1,944
他人へのなりすまし	26	1,009
インターネットショッピングの不正購入	911	209
情報の不正入手	92	177
オンラインゲーム、コミュニティサイトの不正操作	379	130
ホームページの改ざん・消去	107	40
インターネット・オークションの不正操作	36	13
不正ファイルの蔵置	20	1
その他	55	22

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26年中における不正アクセス禁止法違反の検挙件数は364件、検挙人員は170人と、前年と比べ、検挙件数は616件減少し、検挙人員は23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338件、150人、「識別符号の取得行為[注5]」が16件、15人、「識別符号の保管行為[注6]」が２件、２人、「フィッシング行為[注7]」が８件、６人であった。

表２－１　検挙件数等の推移

区分＼年次		平成22年	平成23年	平成24年	平成25年	平成26年
不正アクセス行為	検挙件数	1,598	242	533	968	338
	検挙事件数[注8]	103	101	133	142	141
	検挙人員	123	110	151	144	150
識別符号提供（助長）行為	検挙件数	3	6	4	7	0
	検挙事件数	3	6	4	7	0
	検挙人員	4	6	4	7	0
識別符号取得行為	検挙件数			2	2	16
	検挙事件数			2	1	5
	検挙人員			2	1	15
識別符号保管行為	検挙件数			2	2	2
	検挙事件数			2	2	2
	検挙人員			2	2	2
フィッシング行為	検挙件数			2	1	8
	検挙事件数			1	1	6
	検挙人員			1	1	6
計	検挙件数（件）	1,601	248	543	980	364
	検挙事件数（事件）	104 (重複2)	103 (重複4)	136 (重複6)	145 (重複8)	150 (重複4)
	検挙人員（人）	125 (重複2)	114 (重複2)	154 (重複6)	147 (重複8)	170 (重複3)

※　１事件で複数の区分にわたる行為を検挙した場合及び１人を複数の区分にわたる行為で検挙した場合は、それぞれの区分に重複して計上。

注5　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6　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7　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8　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9]」が336件であり、「セキュリティ・ホール攻撃型[注10]」は２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22年	平成23年	平成24年	平成25年	平成26年
識別符号窃用型	検挙件数	1,597	241	532	965	336
	検挙事件数	102	100	133	139	140
セキュリティ・ホール攻撃型	検挙件数	1	1	1	3	2
	検挙事件数	1	1	1	3	2
計	検挙件数（件）	1,598	242	533	968	338
	検挙事件数（事件）	103	101	133（重複1）	142	141（重複1）

※　１事件で複数の区分にわたる行為を検挙した場合は、それぞれの区分に重複して計上。

３　検挙事件の特徴

(1)　被疑者の年齢

不正アクセス禁止法違反に係る被疑者の年齢は、「14～19歳」（49人）が最も多く、「30～39歳」（45人）、「20～29歳代」（43人）、「40～49歳」（25人）、「50～59歳」（５人）及び「60歳以上」（３人）の順となっている。

なお、最年少の者は14歳[注11]、最年長の者は70歳であった。

表３－１　年代別被疑者数の推移

区分＼年次	平成22年	平成23年	平成24年	平成25年	平成26年
14～19歳（人）	29	51	64	44	49
20～29歳	39	30	34	30	43
30～39歳	35	19	21	37	45
40～49歳	17	10	28	27	25
50～59歳	5	2	6	8	5
60歳以上	0	2	1	1	3
計	125	114	154	147	170

注9　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。

注11　平成26年中、不正アクセス禁止法違反で補導された14歳未満の触法少年は８名であった（犯罪統計による集計）。

(2)　被疑者と利用権者の関係

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、交友関係のない他人によるものが最も多く（76人）、次いで元交際相手や元従業員等の顔見知りの者によるもの（75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。

(3)　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（84件）、次いで「フィッシングサイトにより入手したもの」（71件）となっている。また、「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」（53件）、「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」（47件）等も依然として発生している。

表３－２　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25年	平成26年
識別符号窃用型		965	336
	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	767	84
	フィッシングサイトにより入手したもの	9	71
	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	53
	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	47
	インターネット上に流出・公開されていた識別符号を入手したもの	9	34
	他人から入手したもの	33	25
	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	25	6
	その他	2	16
セキュリティ・ホール攻撃型		3	2

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。

(4)　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、「顧客データの収集等情報を不正に入手するため」が最も多く（139件）、次いで「不正に経済的利益を得るため」（86件）、「嫌がらせや仕返しのため」（54件）、「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」（41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25年	平成26年
顧客データの収集等情報を不正に入手するため	53	139
不正に経済的利益を得るため	706	86
嫌がらせや仕返しのため	56	54
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	41
好奇心を満たすため	46	15
料金の請求を免れるため	25	2
その他	5	1
計	968	338

(5)　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（336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（69件）、次いで「社員用等の内部サイト」（65件）、「インターネットショッピング」（44件）、「電子メール」（30件）、「インターネットバンキング」（20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25年	平成26年
識別符号窃用型　（件）		965	336
	オンラインゲーム、コミュニティサイト	138	69
	社員用等の内部サイト	15	65
	インターネットショッピング	728	44
	電子メール	48	30
	インターネットバンキング	7	20
	インターネット・オークション	5	15
	インターネット接続サービス	0	11
	ホームページ公開サービス	6	7
	その他	18	75

４　都道府県公安委員会による援助措置

平成26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	平成26年
援助措置	4	3	0	1	0	0	0	0	0	0

５　検挙事例

(1)　中国人の男（24）らは、平成25年６月、他人の識別符号を入力して大手通販サイトのサーバに不正アクセスし、他人に付与されたポイントを電子マネーに交換して財産上不法の利益を得た。同年12月及び26年1月、不正アクセス禁止法違反（識別符号の保管行為、不正アクセス行為）及び電子計算機使用詐欺で逮捕した（岐阜、兵庫）。

(2)　中国人の男（34）らは、中継サーバ事業を営む者であるが、25年10月、不正に取得した他人の識別符号により日本のインターネットサービスプロバイダのサーバに不正アクセスした。26年２月、不正アクセス禁止法違反（不正アクセス行為）で逮捕した（警視庁、埼玉）。

(3)　無職の男（29）は、26年２月、インターネットバンキングの識別符号の入力を求めるフィッシングサイトを開設し、他人の識別符号を不正に取得するとともに、取得した識別符号によりインターネットバンキングに不正アクセスし、他人の口座から不正に送金した。同年７月までに、不正アクセス禁止法違反（識別符号の取得行為、不正アクセス行為）及び電子計算機使用詐欺等で検挙した（警視庁、愛媛）。

(4)　無職の男（29）は、26年５月、インターネット上に流出していた他人の識別符号を多数入力して大手通販サイト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ＩＤを変更するとともに、他人になりすまして大手通販サイトでゲーム等の商品を購入した。同年９月、不正アクセス禁止法違反（不正アクセス行為）及び私電磁的記録不正作出・同供用で逮捕した（千葉）。

(5)　中学生の少年（14）らは、26年３月、無料コミュニケーションアプリのサイトを模したフィッシングサイトを開設するとともに同アプリの利用者の識別符号を不正に取得した。同年11月までに不正アクセス禁止法違反（フィッシング行為、識別符号の取得行為）で検挙した（埼玉）。

第２　防御上の留意事項

１　利用権者の講ずべき措置

(1)　パスワードの適切な設定・管理

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、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ずる。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。

(2)　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。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。

(3)　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及びワンタイムパスワード等の個人認証方法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

(1)　フィッシング及び不正プログラム等への対策

フィッシングや不正プログラム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等により個人認証を強化するなどの対策を講ずる。

(2)　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、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、必要に応じて定期的にパスワードの変更を促す仕組みを構築するなどの措置を講ずる。

(3)　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。

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。

(4)　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。

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。

（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

平成 26 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）が対象である。

コンピュータ不正アクセスに関する届出件数は 120 件（平成 25 年：168 件）であった。（注２）

平成 26 年は同 25 年と比べて、48 件（約 28%）減少した。

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、「なりすまし」及び「侵入」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。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総計は 192 件（平成 25 年：373 件）となる。

ア　侵入行為に関して

侵入行為に係る攻撃等の届出は 126 件（平成 25 年：243 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。

２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。

82 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 16 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：15 件

パスワード推測：９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 42 件の届出があった。

【主な内容】

ファイル等の改ざん、破壊等：20 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：13 件

裏口（バックドア）の作成：４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：１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不可若しくは低下させたりする攻撃である。23 件（平成 25 年：36 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、43 件（平成 25 年：94 件）の届出があった。

【主な内容】

正規ユーザへのなりすまし：33 件

ソーシャルエンジニアリング：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。

120 件の届出中、実際に被害に遭った計 102 件（平成 25 年：158 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」が多く、パスワードの使い回しやフィッシング、初期値のままでの利用など、アカウント所有者のパスワード管理の隙を狙った攻撃が多いと推測される。また、原因が不明なケースは依然として多くなっており、手口の巧妙化により原因の特定に至らない事例が多いと推測される。

【主な要因】

DoS 攻撃：18 件

ID、パスワード管理の不備によると思われるもの：17 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：11 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：10 件

原因不明：35 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：32 件
メールサーバ：23 件
その他のサーバ：５件
FTP サーバ：３件
不明：36 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

120 件の届出を被害内容で分類した 151 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 133 件（昨年：195 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】

踏み台として悪用：38 件
サービス低下：22 件
オンラインサービスの不正利用：21 件
ホームページ改ざん：15 件
データの窃取や盗み見：11 件
※１件の届出で複数の項目に該当するものがある。

(5) 対策情報

2013 年には届出のなかったパスワードリスト攻撃による被害の届出が 2014 年は 4 件あった。 報道された情報によるとパスワードリスト攻撃が原因と考えられる不正ログイン被害は、2013 年より継続的に発生しており、2014 年も収束の兆しが見られなかった。

また、パスワードリスト攻撃と同様に継続的に発生しているのが、メールアカウントの不正使用による、スパムメール送信の踏み台とされてしまう被害だ。 2013 年は 27 件、2014 年は 20 件の届出があった。ほとんどの被害でメールアカウント不正使用の原因は特定されていないが、当該アカウントのパスワード変更により被害の再発を防げたことから、推測が容易なパスワードの利用、パスワードの使い回し、フィッシングサイトへの入力等が原因であったと考えられる。

パスワードリスト攻撃の被害、スパムメール送信の踏み台となる被害、いずれも、ウェブサイト改ざん被害のようにサーバの脆弱性が起因するものではないため、サーバの脆弱性を解消していても被害を防ぐことはできないた

め、以下のような対策が必要となる。

システム管理者向け対策
- ログイン通知やログイン履歴の機能を設ける
- 外部からメールサーバへ接続する際にはアカウント情報以外の認証情報を必要とする

など、不正ログインを早急に検知できるような機能追加を検討することが推奨される。

ユーザの対策
- パスワードの使いまわしをしない
- 二段階認証などのセキュリティオプションを積極的に採用する

など、適切なアカウント管理とリスクへの対策を実施することが推奨される。

下記ページ等を参照し、今一度状況確認・対処されたい。

【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/

「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/

「パスワードリスト攻撃による不正ログイン防止に向けた呼びかけ」
https://www.ipa.go.jp/about/press/20140917.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、下記ページを参照のこと。
「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 26 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 20,284 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 18, 783 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 8,870 件の報告があった。
[1/1-3/31: 1,719 件、4/1-6/30:1,611 件、7/1-9/30:1,948 件、10/1-12/31: 3,592 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 4,373 件の報告があった。
[1/1-3/31: 1,501 件、4/1-6/30: 1,123 件、7/1-9/30: 968 件、10/1-12/31: 781 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 988 件の報告があった。
[1/1-3/31: 211 件、4/1-6/30: 194 件、7/1-9/30: 271 件、10/1-12/31: 312 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 143 件の報告があった。
[1/1-3/31: 23 件、4/1-6/30: 88 件、7/1-9/30: 18 件、10/1-12/31: 14 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 1,889 件の報告があった。
[1/1-3/31: 557 件、4/1-6/30: 509 件、7/1-9/30: 417 件、10/1-12/31: 406 件]

（６） 制御システム関連

インターネット経由で攻撃が可能な制御システム等について 9 件の報告があった。
[1/1-3/31: 0 件、4/1-6/30: 0 件、7/1-9/30: 6 件、10/1-12/31: 3 件]

（７） 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 2,511 件の報告があった。
[1/1-3/31: 518 件、4/1-6/30: 735 件、7/1-9/30: 760 件、10/1-12/31: 498 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]

2014 年 1 月	2014 年 1 月 Microsoft セキュリティ情報に関する注意喚起 Adobe Flash Player の脆弱性 (APSB14-02) に関する注意喚起 Adobe Reader 及び Acrobat の脆弱性 (APSB14-01) に関する注意喚起 2014 年 1 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 ntpd の monlist 機能を使った DDoS 攻撃に関する注意喚起
2014 年 2 月	Adobe Flash Player の脆弱性 (APSB14-04) に関する注意喚起 Apache Commons FileUpload および Apache Tomcat の脆弱性に関する注意喚起 2014 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 2014 年 2 月 Microsoft Internet Explorer の未修正の脆弱性に関する注意喚起 Adobe Flash Player の脆弱性（APSB14-07）に関する注意喚起
2014 年 3 月	2014 年 3 月 Microsoft セキュリティ情報（緊急 2 件含）に関する注意喚起 2014 年 3 月 Microsoft Word の未修正の脆弱性に関する注意喚起
2014 年 4 月	OpenSSL の脆弱性に関する注意喚起 2014 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 Adobe Flash Player の脆弱性（APSB14-09）に関する注意喚起 DNS キャッシュポイズニング攻撃に関する注意喚起 2014 年 4 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 2014 年 4 月 Microsoft Internet Explorer の未修正の脆弱性に関する注意喚起 Adobe Flash Player の脆弱性（APSB14-13）に関する注意喚起
2014 年 5 月	マイクロソフト セキュリティ情報(MS14-021)に関する注意喚起 Adobe Reader および Acrobat の脆弱性（APSB14-15）に関する注意喚起 Adobe Flash Player の脆弱性（APSB14-14）に関する注意喚起 2014 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 旧バージョンの Movable Type の利用に関する注意喚起
2014 年 6 月	Adobe Flash Player の脆弱性（APSB14-16）に関する注意喚起 2014 年 6 月 Microsoft セキュリティ情報（緊急 2 件含）に関する注意喚起 ISC BIND 9 サービス運用妨害の脆弱性（CVE-2014-3859）に関する注意喚起
2014 年 7 月	Adobe Flash Player の脆弱性（APSB14-17）に関する注意喚起 2014 年 7 月 Microsoft セキュリティ情報（緊急 2 件含）に関する注意喚起 2014 年 7 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
2014 年 8 月	Adobe Reader および Acrobat の脆弱性（APSB14-19）に関する注意喚起 Adobe Flash Player の脆弱性（APSB14-18）に関する注意喚起 2014 年 8 月 Microsoft セキュリティ情報（緊急 2 件含）に関する注意喚起
2014 年 9 月	Adobe Flash Player の脆弱性（APSB14-21）に関する注意喚起 2014 年 9 月 Microsoft セキュリティ情報（緊急 1 件含）に

	関する注意喚起 Adobe Reader および Acrobat の脆弱性（APSB14-20）に関する注意喚起 GNU bash の脆弱性に関する注意喚起
2014 年 10 月	TCP 10000 番ポートへのスキャンの増加に関する注意喚起 2014 年 10 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 Adobe Flash Player の脆弱性（APSB14-22）に関する注意喚起 2014 年 10 月 Microsoft セキュリティ情報（緊急 3 件含）に関する注意喚起 Drupal の脆弱性に関する注意喚起 2014 年 10 月 Microsoft OLE の未修正の脆弱性に関する注意喚起
2014 年 11 月	登録情報の不正書き換えによるドメイン名ハイジャックに関する注意喚起 Adobe Flash Player の脆弱性（APSB14-24）に関する注意喚起 2014 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 2014 年 11 月一太郎シリーズの脆弱性に関する注意喚起 2014 年 11 月 Kerberos KDC の脆弱性に関する注意喚起 Adobe Flash Player の脆弱性（APSB14-26）に関する注意喚起
2014 年 12 月	ISC BIND 9 サービス運用妨害の脆弱性（CVE-2014-8500）に関する注意喚起 Adobe Reader および Acrobat の脆弱性（APSB14-28）に関する注意喚起 Adobe Flash Player の脆弱性（APSB14-27）に関する注意喚起 2014 年 12 月 Microsoft セキュリティ情報（緊急 3 件含）に関する注意喚起 TCP 8080 番ポートへのスキャンの増加に関する注意喚起 Active Directory のドメイン管理者アカウントの不正使用に関する注意喚起

（２） 活動概要（報告状況等の公表）

発行日：2015-01-14 [2014 年 10 月 1 日～ 2014 年 12 月 31 日]
発行日：2014-10-09 [2014 年 7 月 1 日 ～ 2014 年 9 月 30 日]
発行日：2014-07-10 [2014 年 4 月 1 日 ～ 2014 年 6 月 30 日]
発行日：2014-04-15 [2014 年 1 月 1 日 ～ 2014 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]254 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。