平成２４年３月１５日
国家公安委員会
総　務　大　臣
経済産業大臣

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

１　趣旨

平成11年８月に成立した、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。）第７条第１項の規定に基づき、国家公安委員会、総務大臣及び経済産業大臣は、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。

参考：不正アクセス禁止法（抜粋）

第７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。

２　公表内容

○　不正アクセス行為の発生状況

平成23年１月１日から12月31日までの不正アクセス行為の発生状況を公表する。

○　アクセス制御機能に関する技術の研究開発の状況

国家公安委員会、総務省又は経済産業省のいずれかに係るアクセス制御機能の研究開発の状況、募集・調査した民間企業等におけるアクセス制御機能の研究開発の状況をそれぞれ公表する。

３　掲載先

○　国家公安委員会ホームページ　http://www.npsc.go.jp/

○　総務省ホームページ　http://www.soumu.go.jp/joho_tsusin/security/security.html

○　経済産業省ホームページ　http://www.meti.go.jp/policy/netsecurity/index.html

不正アクセス行為の発生状況

第１　平成23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23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23年中の不正アクセス行為の認知件数は889件で、前年と比べ、996件減少した。

※　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。

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19年	平成20年	平成21年	平成22年	平成23年
認知件数（件）	1,818	2,289	2,795	1,885	889
海外からのアクセス	79	214	40	57	110
国内からのアクセス	1,684	1,993	2,673	1,755	678
アクセス元不明	55	82	82	73	101

(2)　被害に係る特定電子計算機のアクセス管理者[注1]

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（762件）、次いでプロバイダ（115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19年	平成20年	平成21年	平成22年	平成23年
一般企業（件）	437	685	466	457	762
プロバイダ	1,372	1,589	2,321	1,405	115
大学、研究機関等	1	5	4	2	1
その他	8	10	4	21	11
うち行政機関	5	6	3	13	6
不明	0	0	0	0	0
計	1,818	2,289	2,795	1,885	889

※　「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。

注1　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。

(3) 認知の端緒

認知の端緒としては、利用権者[注2]からの届出によるものが最も多く（680件）、次いで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（121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（75件）、発見者からの通報によるもの（７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19年	平成20年	平成21年	平成22年	平成23年
利用権者からの届出　(件)	415	656	487	314	680
アクセス管理者からの届出	61	60	21	66	121
警察活動	1,326	1,567	2,277	1,488	75
発見者からの通報	2	4	7	9	7
その他	14	2	3	8	6
計	1,818	2,289	2,795	1,885	889

(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、オンラインゲームの不正操作（他人のアイテムの不正取得等）が最も多く（358件）、次いでインターネットバンキングの不正送金（188件）、インターネットショッピングの不正購入（172件）、情報の不正入手（個人情報の不正入手）（74件）、ホームページの改ざん・消去（28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等）（22件）、不正ファイルの蔵置（不正なプログラムやフィッシング[注3]用ホームページデータの蔵置）（４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22年	平成23年
オンラインゲームの不正操作　(件)	255	358
インターネットバンキングの不正送金	22	188
インターネットショッピングの不正購入	12	172
情報の不正入手	1,453	74
ホームページの改ざん・消去	45	28
インターネット・オークションの不正操作	10	22
不正ファイルの蔵置	40	4
その他	48	43

注2　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。

注3　金融機関を装って電子メールを送信するなどして、受信者が偽のウェブサイトにアクセスするよう仕向けたり、受信者に添付ファイルを開かせることにより、そこに個人の識別符号（ＩＤ・パスワード等）、クレジットカード番号等を入力させ、それらを不正に入手する行為をいう。

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23年中における不正アクセス禁止法違反の検挙件数は248件、検挙人員は114人と、前年と比べ、検挙件数は1,353件減少し、検挙人員は11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242件、110人、不正アクセス助長行為[注4]に係るものがそれぞれ６件、６人であった。

表２－１　検挙件数等の推移

区分＼年次		平成19年	平成20年	平成21年	平成22年	平成23年
不正アクセス行為	検挙件数	1,438	1,737	2,532	1,598	242
	検挙事件数[注5]	86	101	95	103	101
	検挙人員	126	135	114	123	110
不正アクセス助長行為	検挙件数	4	3	2	3	6
	検挙事件数	2	3	1	3	6
	検挙人員	4	3	1	4	6
計	検挙件数（件）	1,442	1,740	2,534	1,601	248
	検挙事件数（事件）	86 (重複2)	101 (重複3)	95 (重複1)	104 (重複2)	103 (重複4)
	検挙人員（人）	126 (重複4)	137 (重複1)	114 (重複1)	125 (重複2)	114 (重複2)

※　(重複)とは、不正アクセス行為と不正アクセス助長行為の重複を示す。

(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6]が241件であり、セキュリティ・ホール攻撃型[注7]は１件であった。

注4　他人の識別符号をどのコンピュータに対する識別符号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、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5　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。

注6　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３条第２項第１号に該当する行為）をいう。

注7　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３条第２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２－２　不正アクセス行為の態様の推移

区分＼年次		平成19年	平成20年	平成21年	平成22年	平成23年
識別符号窃用型	検挙件数	1,438	1,736	2,529	1,597	241
	検挙事件数	86	100	94	102	100
セキュリティ・ホール攻撃型	検挙件数	0	1	3	1	1
	検挙事件数	0	1	1	1	1
計	検挙件数（件）	1,438	1,737	2,532	1,598	242
	検挙事件数（事件）	86	101	95	103	101

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、フィッシングサイトを開設して識別符号を入手したもの（59件）及び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件）が最も多く、次いで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件）となっている。また、共犯者等から入手したもの（38件）、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件）等も依然として発生している。

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22年	平成23年
識別符号窃用型　(件)		1,597	241
	フィッシングサイトにより入手したもの	1,411	59
	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	70	59
	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	57	52
	共犯者等から入手したもの	12	38
	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	12	29
	スパイウェア[注8]等のプログラムを使用して識別符号を入手したもの	14	1
	他人から購入したもの	4	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	17	3
セキュリティ・ホール攻撃型		1	1

注8　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。

(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（54人）、次いで交友関係のない他人によるもの（34人）、ネットワーク上の知り合いによるもの（26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（51人）が最も多く、20歳代（30人）、30歳代（19人）、40歳代（10人）、50歳代（２人）及び60歳代（２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66歳であった。

表３－２　年代別被疑者数の推移

区分＼年次	平成19年	平成20年	平成21年	平成22年	平成23年
10歳代　(人)	39	48	31	29	51
20歳代	39	42	33	39	30
30歳代	34	35	35	35	19
40歳代	12	11	13	17	10
50歳代	2	1	2	5	2
60歳代	0	0	0	0	2
計	126	137	114	125	114

※　不正アクセス助長行為に係る被疑者を含む。

(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（97件）が最も多く、次いで嫌がらせや仕返しのため（58件）、オンラインゲームで不正操作を行うため（39件）、好奇心を満たすため（32件）、顧客データの収集等情報を不正に入手するため（15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22年	平成23年
不正に経済的利益を得るため　(件)	1,455	97
嫌がらせや仕返しのため	66	58
オンラインゲームで不正操作を行うため	19	39
好奇心を満たすため	33	32
顧客データの収集等情報を不正に入手するため	18	15
料金の請求を免れるため	4	0
その他	3	1
計	1,598	242

(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（241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（87件）、次いでオンラインゲーム（51件）、会員専用・社員用内部サイト（48件）、電子メール（23件）、インターネットバンキング（14件）、ホームページ公開サービス（５件）、インターネット・オークション（４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22年	平成23年
識別符号窃用型　(件)		1,597	241
	インターネットショッピング	16	87
	オンラインゲーム	71	51
	会員専用・社員用内部サイト	1,432	48
	電子メール	36	23
	インターネットバンキング	7	14
	ホームページ公開サービス	25	5
	インターネット・オークション	2	4
	その他	8	9

４　都道府県公安委員会による援助措置

平成23年中、不正アクセス禁止法第６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19年	平成20年	平成21年	平成22年	平成23年
援助措置　(件)	0	1	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

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9]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したり、定期的にパスワードの変更を促す仕組みを構築したり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　ＳＱＬインジェクション攻撃[注10]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を受け、クレジットカード番号等の個人情報が大量に流出す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、ＳＱＬインジェクション攻撃に対する監視体制を強化する。

注9　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。

注10　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。

6　検挙事例

1	フィッシングにより他人のＩＤ・パスワードやクレジットカード番号等を不正に入手し、インターネットショッピングにおいて商品をだまし取るなどした不正アクセス禁止法違反及び電子計算機使用詐欺等事件

中古品買取業の男（27）らは、平成21年９月から平成23年６月までの間、フィッシングにより他人のＩＤ・パスワードやクレジットカード番号等を入手し、クレジットカード会社のウェブサイトに不正アクセスを行い、インターネットショッピング等において合計約１億円相当の商品をだまし取るなどした。平成23年11月までに、不正アクセス禁止法違反及び電子計算機使用詐欺罪等で検挙した（静岡、茨城、千葉、熊本、広島）。

2	他人のＩＤからそのパスワードを類推してＳＮＳ[注11]サイトに不正アクセスを行い、女性会員になりすましてメッセージを送信した不正アクセス禁止法違反事件

派遣社員の男（28）は、平成23年８月、他人のＩＤからそのパスワードを類推してＳＮＳサイトに不正アクセスを行い､女性会員になりすましてメッセージを送信した。平成23年12月、不正アクセス禁止法違反で検挙した（高知）。

3	在職中に入手した他人のＩＤ・パスワードを使用してインターネットバンキングに不正アクセスを行い、現金を不正送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等事件

会社員の男（33）は、平成20年２月から４月までの間、在職中に入手した勤務先のインターネットバンキングのＩＤ・パスワードを使用して不正アクセスを行い、架空名義の健康保険証を使用して不正取得した銀行口座に不正送金した。平成23年３月、不正アクセス禁止法違反及び電子計算機使用詐欺等で検挙した（神奈川）。

4	パソコンに保存されていた他人のＩＤ・パスワードを使用してインターネットバンキングに不正アクセスを行い、現金を不正送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

通信販売業の男（46）は、平成22年８月、修理を頼まれたパソコンに保存されていた他人のインターネットバンキングのＩＤ・パスワードを使用して不正アクセスを行い、自己名義の銀行口座に不正送金した。平成23年８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（埼玉）。

注11 ソーシャルネットワーキングサービス（Social Networking Service）の略。登録したユーザのみが参加できるインターネット上のウェブサイトをいう。

５	言葉巧みに聞き出した元同僚のＩＤ・パスワードを使用して、以前に勤務していた会社の顧客情報システムに不正アクセスを行い、顧客情報を入手した不正アクセス禁止法違反事件

会社員の男（54）は、平成23年８月から９月までの間、言葉巧みに聞き出した元同僚のＩＤ・パスワードを使用して、以前に勤務していた会社の顧客情報システムに不正アクセスを行い、氏名、住所、注文内容等の顧客情報を入手した上、それを用いて顧客と契約した。平成23年11月、不正アクセス禁止法違反で検挙した（新潟）。

第２　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

１　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23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103件（平成22年：197件）であった。（注２）

平成23年は同22年と比べて、94件（約48%）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、「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。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180件（平成22年：365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145件（平成22年：309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。

１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。

68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28件である。

【主な内容】

パスワード推測：８件

ソフトウェアのぜい弱性やバグを利用した攻撃：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76件の届出があった。

【主な内容】

資源利用（ファイル、CPU使用）：21件

ファイル等の改ざん、破壊等：19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：16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：11件

証拠の隠滅（ログの消去等）：３件

裏口（バックドア）の作成：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。７件（平成22年：８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、28件（平成22年：48件）の届出があった。

【主な内容】

正規ユーザへのなりすまし：27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／弱点による分類である。

103件の届出中、実際に被害に遭った計75件（平成22年：123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：15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：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：11 件
DoS 攻撃・その他によるもの：５件
原因不明：32 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：47 件
メールサーバ：19 件
クライアント：１件
その他のサーバ：16 件
不明：14 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

103 件の届出を被害内容で分類した 109 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 81 件（昨年：140 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：27 件
オンラインサービスの不正利用：17 件
ホームページ改ざん：13 件
データの窃取や盗み見：８件
サービス低下：７件
ファイルの書換え：４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

平成 23 年は、いわゆる「ガンブラー」によるウェブサイト改ざんの被害が減少した反面、CMS（Contents Management System）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なケースだったことから、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、SSH で使用するポートへの攻撃で侵入（ID、パスワードの設定不備が主な原因）され、他のコンピュータを攻撃するための踏み台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。）

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】

「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 5 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

「ウェブサイトで利用されている DNS サーバの既知の脆弱性への注意喚起」
http://www.ipa.go.jp/security/vuln/documents/2009/200912_dns.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

【個人ユーザ向け】
「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/
「セーフティと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。

2　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

平成 23 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である。

(1) 不正アクセス関連行為の特徴及び件数

報告（調整対応依頼）のあった不正アクセス関連行為(注１)に係る報告件数(注２)は 7,722 件であった。

ア　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 4,580 件の報告があった。

[1/1-3/31: 919 件、4/1-6/30:958 件、7/1-9/30:1,079 件、10/1-12/31: 1,624 件]

イ　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 320 件の報告があった。

[1/1-3/31: 49 件、4/1-6/30: 34 件、7/1-9/30:73 件、10/1-12/31: 164 件]

ウ　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 789 件の報告があった。

[1/1-3/31: 352 件、4/1-6/30: 121 件、7/1-9/30:185 件、10/1-12/31: 131 件]

エ　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５件の報告があった。

[1/1-3/31:3 件、4/1-6/30:1 件、7/1-9/30:0 件、10/1-12/31:1 件]

オ　Web 偽装事案(phishing)

Web のフォーム等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 1,270 件の報告があった。

[1/1-3/31: 405 件、4/1-6/30: 325 件、7/1-9/30: 226 件、10/1-12/31:314 件]

カ　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 496 件の報告があった。

[1/1-3/31:155 件、4/1-6/30:123 件、7/1-9/30:113 件、10/1-12/31:105 件]

(2) 防御に関する啓発及び対策措置の普及

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等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、次の文書を公開している(詳細は http://www.jpcert.or.jp/参照)。

ア　注意喚起

[新規]

平成23年1月	Microsoft セキュリティ情報（緊急 1 件含む。）に関する注意喚起
平成23年2月	主に UNIX / Linux 系サーバを対象としたインターネット公開サーバのセキュリティ設定に関する注意喚起 Microsoft セキュリティ情報（緊急 3 件含む。）に関する注意喚起 Adobe Reader 及び Acrobat のぜい弱性に関する注意喚起 Adobe Flash Player のぜい弱性に関する注意喚起
平成23年3月	Microsoft セキュリティ情報（緊急 1 件含む。）に関する注意喚起 Adobe Flash Player 及び Adobe Reader / Acrobat のぜい弱性に関する注意喚起
平成23年4月	Microsoft セキュリティ情報（緊急 9 件含む。）に関する注意喚起 Adobe Flash Player のぜい弱性に関する注意喚起 Adobe Reader 及び Acrobat のぜい弱性に関する注意喚起 情報流出に伴う ID とパスワードの不正使用に関する注意喚起
平成23年5月	Microsoft セキュリティ情報（緊急 1 件含む。）に関する注意喚起 Adobe Flash Player のぜい弱性に関する注意喚起 ISC BIND 9 のぜい弱性を使用したサービス運用妨害攻撃に関する注意喚起
平成23年6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 Microsoft セキュリティ情報（緊急 9 件含む。）に関する注意喚起 Adobe Reader 及び Acrobat のぜい弱性に関する注意喚起 Adobe Flash Player のぜい弱性に関する注意喚起
平成23年7月	ISC BIND 9 サービス運用妨害のぜい弱性に関する注意喚起

	Microsoft セキュリティ情報（緊急 1 件含む。）に関する注意喚起
平成 23 年 8 月	Microsoft セキュリティ情報（緊急 2 件含む。）に関する注意喚起 Adobe Flash Player のぜい弱性に関する注意喚起 Apache HTTP Server のサービス運用妨害のぜい弱性に関する注意喚起
平成 23 年 9 月	Remote Desktop (RDP) が使用する 3389 番ポートへのスキャンに関する注意喚起 Adobe Reader 及び Acrobat のぜい弱性に関する注意喚起 Adobe Flash Player のぜい弱性に関する注意喚起
平成 23 年 10 月	Microsoft セキュリティ情報（緊急 2 件含む。）に関する注意喚起 標的型メール攻撃に関する注意喚起
平成 23 年 11 月	Microsoft セキュリティ情報（緊急 1 件含む。）に関する注意喚起 Adobe Flash Player のぜい弱性に関する注意喚起 ISC BIND 9 サービス運用妨害のぜい弱性に関する注意喚起
平成 23 年 12 月	Java SE を対象とした既知のぜい弱性を狙う攻撃に関する注意喚起 Microsoft セキュリティ情報（緊急 3 件含む。）に関する注意喚起 Adobe Reader 及び Acrobat のぜい弱性に関する注意喚起

イ　活動概要（報告状況等の公表）

発行日：2012-01-12 [平成 23 年 10 月 1 日～ 12 月 31 日]
発行日：2011-10-11 [平成 23 年 7 月 1 日 ～ 9 月 30 日]
発行日：2011-07-11 [平成 23 年 4 月 1 日 ～ 6 月 30 日]
発行日：2011-04-12 [平成 23 年 1 月 1 日 ～ 3 月 31 日]

ウ　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] 286 件

(3) 定点観測システム

インターネット定点観測システム（ISDAS）を運用することによってワームやウイルスの感染活動や弱点探索のためのスキャン等、セキュリティ上の脅威となるトラフィックの観測を行い、JPCERT/CC における分析や情報発信に活用しているほか、ウェブサイトにて観測情報を提供している（詳細は http://www.jpcert.or.jp/isdas/参照）。

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(又は偶発的) に発生する全ての事象が対象になる。

注２　ここに挙げた件数は、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。

３　ぜい弱性対策情報について

日本国内の製品開発者(ベンダ) 等の関連組織とのコーディネーションを行い、JVN (Japan Vulnerability Notes) にて公開したぜい弱性情報は 266 件であった(詳細は http://jvn.jp/参照)。
[1/1-3/31:68 件、4/1-6/30:64 件、7/1-9/30:55 件、10/1-12/31:79 件]

そのうち、平成 16 年７月の経済産業省告示「ソフトウェア等ぜい弱性関連情報取扱基準」に従って、JVN にて公開したぜい弱性情報は 114 件であった。
[1/1-3/31:24 件、4/1-6/30:26 件、7/1-9/30:29 件、10/1-12/31:35 件]

アクセス制御機能に関する技術の研究開発の状況

1　国で実施しているもの

総務省又は経済産業省が取り組むアクセス制御機能の研究開発に関して取りまとめたものであり、具体的には、独立行政法人自ら又は委託による研究、国からの委託又は補助による研究である。

実施テーマは次のとおりであり、その研究開発の概要は、別添１のとおりである。

マルウェア配布等危害サイト回避システム
ネットワークセキュリティ技術の研究開発
マルウェア対策ユーザサポートシステムの研究開発
情報家電など、非PC端末における未知脆弱性の自動検出技術に関する研究開発

2　民間企業等で研究を実施したもの

(1)　公募

警察庁、総務省及び経済産業省が平成23年12月２日から12月26日までの間にアクセス制御技術に関する研究開発状況の募集を行ったところ、応募者は次のとおりであった。それぞれの研究開発の概要は、別添２のとおりである。

なお、別添２の内容は当該企業から応募のあった内容をそのまま掲載している。

株式会社ネクストジェン
株式会社ICTストラテジー総合研究所
株式会社富士通ソーシアルサイエンスラボラトリ
エヌ・ティ・ティ・コミュニケーションズ株式会社
日本CA株式会社
情報セキュリティ大学院大学

(2)　調査

警察庁が平成23年10月から11月にかけて実施したアンケート調査に対し、アクセス制御技術に関する研究開発を実施しているとして回答のあった大学及び企業は次のとおりである。

ア　大学

国立大学法人九州工業大学
東京情報大学

イ　企業

株式会社エヌ・ティ・データ
株式会社ソリトンシステムズ
ヌリテレコム株式会社
株式会社シー・エス・イー

ファインアートテクノロジー
シスメックスＲＡ株式会社
ウォッチガード・テクノロジー・ジャパン株式会社
株式会社ＣＩＪ
日本信号株式会社
日本無線株式会社
富士通株式会社

また、それぞれの研究開発の概要は別添３のとおりである。

なお、別添３の内容は、アンケート調査の回答内容（研究開発のうち実用化しているもののみ）をそのまま掲載している。

アンケート調査は、次の条件により抽出した1,300団体を対象に実施した。

・大学
国公立・私立大学のうち、理工系学部又はこれに準ずるものを設置するもの

・企業
市販のデータベース（四季報・ＩＴ総覧等）に掲載された企業であって、業種分類が「情報・通信」、「サービス」、「電気機器」又は「金融」であるもの

(別添1)

対象技術　その他アクセス制御に関する技術
テーマ名　マルウェア配布等危害サイト回避システムの実証実験
開発年度　平成21年度～平成23年度
実施主体　エヌ・ティ・ティ・コミュニケーションズ株式会社（総務省からの委託）
背景、目的 近年、一般に広く利用される有名Webサイト改ざんによりWeb感染型マルウェアを埋め込まれることにより、多くの国民がマルウェア感染の脅威にさらされるようになった。 こうしたマルウェアへの対策として、ユーザは、セキュリティベンダから提供されるウイルス対策ソフトの導入及びアップデート、OSやアプリケーションのアップデートを行うことが有効であるが、インターネット利用ユーザの意識やスキルの不足により徹底されていないのが現状である。 社会全体としての情報セキュリティの向上を実現するためには、電気通信事業者によるネットワーク側での対策を行うことが効果的であり、マルウェアを配布するサイト等にアクセスすることによる感染を未然に防止するためのマルウェア配布等危害サイト回避システムが有効である。 本事業では、危害サイトへのユーザアクセスに対して、注意喚起を行うことにより、ユーザのマルウェア感染を未然に防ぐマルウェア配布等危害サイト回避システムの実証実験を行い、主に危害サイト評価情報データベースの構築とISPへの情報提供方法について検討する。
研究開発状況（概要） マルウェア配布等危害サイト回避システムは、危害サイト評価情報を基に、ISPの顧客である一般ユーザが危害サイトにアクセスするのを防止するものであり、危害サイト評価情報提供システム、トラヒック解析システム及び危害サイト注意喚起システムから構成される。 （１）危害サイト評価情報提供システム 正確性の高い危害サイト評価情報データベースを作成し、ISPに危害サイト評価情報を提供するシステムであり、以下のサブシステムから構成 ①　クローラシステム ②　マルウェア動的解析システム ③　サイト解析システム ④　スコアリング分析評価システム ⑤　危害サイト公開システム （２）トラヒック解析システム ISPのネットワークの一部のトラヒックをモニタリングし、シードリストを生成するシステム （３）危害サイト注意喚起システム 危害サイト評価情報提供システムから、危害サイト評価情報を受け取り、その情報を元に一般ユーザの危害サイトへのアクセス時に注意喚起を行うシステム

詳細の入手方法（関連部署名及びその連絡先）

総務省情報流通行政局情報流通振興課情報セキュリティ対策室

電話　03-5253-5749

将来の方向性

本事業を通じて、マルウェア配布等危害サイト回避システムに関する技術を確立し、実運用に向けての法律等の制度面の検討を行う。

対象技術　侵入検知技術

テーマ名　ネットワークセキュリティ技術の研究開発

開発年度　平成18年度～

実施主体　独立行政法人情報通信研究機構

背景、目的

　ネットワーク上におけるサイバー攻撃・不正通信等に耐えるとともに、それらを検知・排除するため、イベント（スキャン、侵入等）の収集・測定及びこれに基づく傾向分析･脅威分析を実時間で行い予兆分析を含めた対策手法の迅速な導出を行うインシデント対策技術の研究開発を行う。

　また，対策手法の導出に当たって，再現ネットワークの活用による検証、発信元追跡技術の研究開発を行う。さらに DoS(サービス不能)攻撃によるネットワーク障害への耐性を高めるための研究開発を行う。

研究開発状況（概要）

　これまでに研究開発･整備した広域に設置された観測点からのセキュリティログの分析手法､マルウェアの収集機構･収集したマルウェアの分析機構に関して、日本全国規模の観測網構築に向けた観測対象ネットワークの更なる拡充､より高度な観測アーキテクチャ・攻撃検出機構の開発、マルウェアの分析精度の高度化を行った。この結果をこれまでに構築したインシデント分析システムプロトタイプに反映し、実運用に向け開発を進めた。

　また、異なる機関に属する複数の観測点で収集したログから、その組織が有する情報を互いに開示することなく､共通の攻撃を解析する技術について更に高速化が可能なアルゴリズムを開発し、その有効性を検証した。本アルゴリズムを正規のユーザのプライバシーを保護しつつ発信元を追跡する技術に拡張した。攻撃ベクタの捕捉能力と解析能力の向上のため､仮想マシンモニタを用いて不正アクセス発生時点のメモリ、ディスク内容を捕捉する技術を開発し、逐次解析器による再現フローの自動化とデータ蓄積を実施した。また海外研究機関と連携し、ネットワークを流れるパケットの内容を自動分類し､パケットに含まれる攻撃ベクタを高精度で捕捉できる機械学習アルゴリズムの開発を進めた。

詳細の入手方法（関連部署名及びその連絡先）

独立行政法人情報通信研究機構　ネットワークセキュリティ研究所企画室
042-327-5774

将来の方向性

上記の研究開発を通じて､将来のネットワーク自身及びネットワーク上を流通する情報の安全性・信頼性の確保と、利用者にとって安全・安心な情報通信基盤の実現を目指す。

対象技術　不正プログラム対策技術

テーマ名　マルウェア対策ユーザサポートシステムの研究開発

開発年度　平成21年度～平成23年度

実施主体　株式会社日立製作所、KDDI株式会社
（情報通信研究機構（NICT）が実施する委託研究の委託先）

背景、目的

本研究開発では、ユーザパソコンに負荷がかかる実行コードの解析をnicter等の解析機能を有する外部のシステムが担うことにより、効率的なマルウェアの検出及び自動駆除の仕組みを実現することを目的とする。

ユーザにおけるマルウェア対策として一般的なものは、セキュリティベンダ等が提供しているシグネチャ（マルウェア検査パターン）に基づくアンチウィルスソフトである。

アンチウィルスソフトでは、シグネチャを採用しているため、既知のマルウェアに対しては十分対応できるが、未知のマルウェアや、一定期間感染行動等の挙動を見せないマルウェアの疑いのある怪しい実行コードに対しては、現状十分に対応できていない。

また、新しいマルウェアが現出した場合、セキュリティベンダ等が対応するパターンファイルを更新するまでに一定の時間を要するため、ユーザが必要なときに、必要なものをタイムリーに入手できるところまでには至っていない。

コード難読化やコード自己変貌化に代表されるように、昨今、マルウェアの高度化・巧妙化が進展する中で、上述のように未知のマルウェアや一定期間感染行動等の挙動を見せないマルウェアの疑いのある怪しい実行コードのように、アンチウィルスソフトによる対応では十分カバーし切れない領域が存在している。

セキュリティベンダ等による取組を補完しつつ、そのような未知のマルウェアも対応できるように、検体の解析に基づくマルウェア判定をベースとした駆除ツールを、実時間に近い形でユーザに提供していくことが必要になってきている。

研究開発状況（概要）

・平成21年度より以下の研究開発を実施中である。

（１）ユーザパソコンへの負荷をかけず、ホワイトリスト化等を用いた高能率探索手法を駆使し、実行コードがマルウェアかどうかをユーザサポートセンターで解析するとともに、マルウェアを駆除するツールを自動的に提供するフレームワーク

（２）ユーザのパソコン上で検査プログラムを実行してから、ユーザに対して駆除ツールが提供されるまでの一連の手続きが10分程度で完了するシステム

（３）上記のマルウェア検出から駆除までを実環境で有効に機能させるための実証実験

詳細の入手方法（関連部署名及びその連絡先）

独立行政法人情報通信研究機構　産学連携部門　委託研究推進室
（http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm）電話　042－327－6011

将来の方向性

上記セキュリティ技術を確立し、高度情報通信ネットワーク社会の安全性・信頼性の確保に資する。

対象技術　脆弱性対策技術

テーマ名　情報家電等、非PC端末における未知脆弱性の自動検出技術に関する研究開発

開発年度　平成22年度～平成24年度

実施主体　株式会社フォティーンフォティ技術研究所（経済産業省からの委託）

背景、目的

現在、情報技術の進歩や社会情勢の変化に伴い、情報セキュリティに係る脅威が急速に変化・拡大しており、経済活動全体の停滞や国民全体の生命・財産そのものに関わるリスクをもたらしかねない状況が生まれつつある。そこで「新世代情報セキュリティ研究開発事業」では、これまでの対症療法的な対策だけではなく、長期的な視点に立って、情報セキュリティ上の問題の根本的な解決を目指した研究開発を実施することを目指す。

本事業では、今後のインターネットにおいて重要な役割を占めることが予想される非PC端末において、外部脅威を誘発する主要因である「セキュリティぜい弱性」を自動検出するための技術を研究開発する。本技術により、製品出荷前に未知のセキュリティぜい弱性を効率的に検出・対処するスキームを開発現場で簡単に構築する事ができる。

研究開発状況（概要）

本事業により、開発する検査ツールにおいては、予測不能なデータを入力することで、セキュリティのぜい弱性を検査するファジングの手法を用いる。具体的な開発状況については、次のとおりである。

（１）ファジングベース開発（平成22年度実施）

①ファジング定義言語開発（平成22年度実施）

セキュリティ検査ツールで用いるファジング定義言語の設計を行った。

（２）ファジング開発・実装

①基本エンジン開発（平成22年度実施）

②エンジン群　追加開発（平成23・24年度実施予定）

①および②で未知ぜい弱性を検出するファジングエンジンの開発を行った。平成24年度も追加開発を行う。

（３）ファジングルール追加実装

①ベースルール開発（平成22年度実施）

②情報家電、モバイル端末、スマートメーター専用ルール開発（平成23・24年度実施予定）

ファジングルールを開発し対応プロトコルを追加した。平成23年度も追加開発を行う。

詳細の入手方法（関連部署名及びその連絡先）

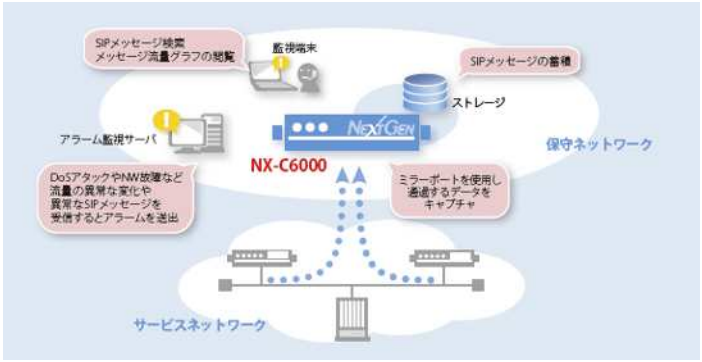
株式会社フォティーンフォティ技術研究所（http://www.fourteenforty.jp/）

鵜飼 裕司（Tel:03-6413-5177）

将来の方向性

　未知のセキュリティぜい弱性を発見する技術は世界的にも研究途上であり、主にセキュリティ研究者の一部が保持する特殊な技術となっているが、これら技術をツール化する事で、一般の開発現場で手軽にぜい弱性を発見する事が可能となる。

(別添2)

企業名（及び略称） 株式会社ネクストジェン	
代表者氏名 大西 新二	
所在地（郵便番号及び住所） 東京都千代田区麹町3-3-4 KDXビル9F	
関連部署名及び電話番号 ネットワークセキュリティ事業本部/03-3234-6855	
ＵＲＬ http://www.nextgen.co.jp/solution/security/	
対象技術	技術開発状況
・侵入検知・防御技術 開発年： 平成21年度～ 平成23年度	近年、悪意ある第三者が企業のIP-PBX(構内交換機)や個人宅内機器を乗っ取り、なりすましによる国際電話発信によって、高額な料金を請求される被害が発生しています。また、警察庁サイバーフォースのインターネット定点観測においてもシグネチャを用いた不正侵入などの検知では平成22年７月９日に「VoIP(Voice over IP)」が急増し、その後減少するも平成22年12月頃よりほぼ横ばいの推移を続けています。 このようなVoIPに関する脅威を解決するシステムとして、株式会社ネクストジェンではSIP(Session Initiation Protocol)に対応したネットワークフォレンジック技術および侵入検知技術を提供しています。SIPメッセージのヘッダ・パラメータを詳細解析し、規定に準拠しているか判断する他、メッセージ流量を監視し、IP電話システムの運用上の課題を解決するために必要な情報を集約します。本技術とネットワーク防御装置との連携により、健全なIP電話環境を社会に広めていくことに寄与できるものと考えます。 http://www.nextgen.co.jp/products/security/nx-c6000.html (製品概要) 

企業名（及び略称） 株式会社ネクストジェン	
代表者氏名　大西 新ニ	
所在地（郵便番号及び住所） 東京都千代田区麹町3-3-4 KDXビル9F	
関連部署名及び電話番号 ネットワークセキュリティ事業本部/03-3234-6855	
ＵＲＬ http://www.nextgen.co.jp/solution/security/	
対象技術	技術開発状況
・ぜい弱性対策技術 開発年： 平成21年度～ 平成23年度	＜概要＞ SIP(Session Initiation Protocol)を使用したVoIP(Voice over IP)システムに対し、ぜい弱性の洗い出しとリスク分析を実施し、対象システムの信頼性及び品質向上に貢献します。 ＜特徴＞ 実使用環境に即した疑似攻撃をVoIPシステムに対して実施し、盗聴、発着番号詐称などのセキュリティリスクや、DoS攻撃等によるシステムの停止に繋がるぜい弱性を洗い出します。擬似攻撃には、SIPプロトコルに特化した250万以上のメッセージを自動で生成し、容易かつ短期間にぜい弱性の問題を発見します。また、診断結果のリスク評価をCVSS (Common Vulnerability Scoring System)を用いて可視化し、運用におけるセキュリティポリシー策定をサポートします。

企業名（及び略称）　株式会社ICTストラテジー総合研究所	
代表者氏名　代表取締役　久保哲男	
所在地（郵便番号及び住所）　〒100-0005　東京都千代田区丸の内1-8-3	
関連部署名及び電話番号　本社　03-4530-0565	
ＵＲＬ　http://www.is-ri.co.jp	
対象技術	技術開発状況
・その他アクセス制御機能に関する技術 開発年： 平成22年度～ 平成23年度	・ネットショップやネットバンク等への初期登録や、毎回のログイン時に、予め登録してある固定電話・携帯電話から認証サーバに電話し発信者番号を通知することにより本人認証を行う技術 ・ＰＣやスマートフォンでの本人確認に対応 ・ＩＤ、パスワードを盗まれたとしても、電話端末を物理的に盗まれない限り、不正アクセスが不可能 ・ＰＣに特別なソフトを別途インストールする必要がなく、また全ての電話会社の全ての機種の電話端末で利用可能 ・ワンタイム・パスワードのようにトークンの配布・管理コスト不要 ・発信者番号は総務省令等にて、全電話会社が対策済

企業名（及び略称）：株式会社富士通ソーシアルサイエンスラボラトリ（富士通SSL）	
代表者氏名　　：花岡　和彦	
所在地（郵便番号及び住所）：211-0063　神奈川県川崎市中原区小杉町1-403 武蔵小杉タワープレイス	
関連部署名及び電話番号：セキュリティソリューション本部 ネットワークサーバセキュリティ部	
ＵＲＬ　http://www.ssl.fujitsu.com/	
対象技術	技術開発状況
・侵入検知・防御技術 ・ぜい弱性対策技術 ・インシデント分析技術 ・不正プログラム対策技術 ・その他アクセス制御機能に関する技術 開発年：平成15年	富士通SSLが開発した「SHieldWARE」は、サーバのアクセス制御を実現するソフトウェア製品です。 汎用ＯＳでシステム管理者が利用する「特権ＩＤ」の権限を最小化できます。管理者も含めた全てのユーザに対して強制アクセス制御を実施し、情報漏えいなどのリスクを低減できます。 また、サーバ上の操作ログをＯＳコマンドレベルまで詳細に記録でき、不正侵入の履歴からサーバアクセスログまで、ＩＴ全般統制に不可欠な監査証跡を確実に収集･管理することが可能です。

企業名（及び略称）　エヌ・ティ・ティ・コミュニケーションズ株式会社	
代表者氏名　代表取締役社長　有馬　彰	
所在地（郵便番号及び住所）　〒100-8019　東京都千代田区内幸町１丁目１番６号	
関連部署名及び電話番号　先端IPアーキテクチャセンタ　050-3812-4969	
ＵＲＬ　http://www.ntt.net/service/traffic.html	
対象技術	技術開発状況
・その他アクセス制御機能に関する技術 開発年：平成19年	1) 大規模ネットワークのトラフィックをxFLOWを使い、統括的に解析し、IPアドレス、アプリケーション別に可視化 2) トラフィックパターンシグネチャおよび通常トラフィック波形からの乖離レベルチェックによりDDoS攻撃等の異常トラフィックを検知 3) DDoS攻撃検知時に、ネットワーク機器を制御し、DDoS攻撃を効率的に軽減する技術開発

企業名（及び略称）日本CA株式会社	
代表者氏名	
所在地（郵便番号及び住所）東京都千代田区平河町2-7-9 JA共済ビル	
関連部署名及び電話番号　セキュリティ＆VSAソリューション事業部	
ＵＲＬ http://www.ca.com/jp/	
対象技術	技術開発状況
・高度認証技術	証明書技術を応用したソフトウェアトークンによる２要素認証を提供します。米国特許クリプトグラフィック・カモフラージュ技術＊1(US Patent No. 6,170,058)により、証明書で問題となるオフラインの総当たり攻撃による秘密鍵の解読を事実上不可能とする事が可能となり、従来ハードウェアで物理的に保護していた証明書をソフトウェアで安全に保護することができ、「証明書を持っている」および、秘密鍵を解くための「パスワードを知っている」の２要素認証を実現可能です。現在この技術を利用した製品を商用化済みで、さらに様々な認証形態に対応するための研究開発を進めている。 ＊1 クリプトグラフィック・カモフラージュ技術 通常の証明書におけるオフラインによる総当たり攻撃では、パスワードで保護されている証明書内の秘密鍵の特徴である「１で始まり１で終わる」（例：1E459FC479C3B41）という書式からパスワードおよび秘密鍵をクラッキングする。この技術は上記のように判読されるのを防ぐため、間違ったパスワードを利用しても１で始まり１で終わるように結果を偽装する。また利用したパスワードが正しいか否かは、サーバに問合せが必要となり、数回間違えるとロックされ、総当たり攻撃が不可能となる。

企業名（及び略称）　情報セキュリティ大学院大学	
代表者氏名　田中英彦 研究科長・教授	
所在地（郵便番号及び住所）　〒221-0835　神奈川県横浜市神奈川区鶴屋町2-14-1	
関連部署名及び電話番号　情報セキュリティ大学院大学事務局　045-311-7784	
ＵＲＬ　http://www.iisec.ac.jp/	
対象技術	技術開発状況
・侵入検知・防御技術 ・不正プログラム対策技術 ・その他アクセス制御機能に関する技術	1) TOMOYO Linux の研究開発 本研究では、アプリケーションが実行される状況に基づき、各アプリケーションが行おうとしている処理の内容を考慮することができるアクセス制御方式について検討している。提案方式は、TOMOYO LinuxとしてLinux上に実装され、公開されている。 2) アクセス制御ポリシー記述・管理方式の研究開発 本研究では、論理プログラムとしてアクセス制御規則を記述し、細粒度アクセス制御の課題であるポリシーの可読性や保守性を向上しながら、複数領域のポリシーを矛盾なく統合可能することで、情報システム全体のセキュリティを厳密なアクセス制御により強化するものである。本研究の成果に対しては、認可判定の妥当性と表現力の評価により、記述言語の有用性を実証済で現在1)を含む実際のＯＳへ実装中である。

（別添3）

【大学】

大学名	国立大学法人九州工業大学情報工学部飯塚キャンパス
所在地	〒820-8502 福岡県飯塚市川津680-4
関連部署／電話番号	0948-29-7500
ホームページのURL	http://www.iizuka.kyutech.ac.jp/
対象技術	技術の概要・特徴など
・その他アクセス制御に関する技術	高速パケット分類回路では、通常TCAMを使用している。しかし、TCAMは高価であり、消費電力も大きい。本製品は、汎用メモリと小型のFPGAのみを使用しているので、安価で低消費電力である。 本製品は、一般の消費者には販売せず、セキュリティ製品のベンダーに回路IPとして、提供する予定である。本研究は、文部科学省、地域イノベーション戦略支援プログラムの支援を受けている。

大学名	東京情報大学
所在地	〒265‐8501 千葉県千葉市若葉区御成台4‐1
関連部署／電話番号	庶務課／ 043-236-4603
ホームページのURL	http://www.tuis.ac.jp/
対象技術	技術の概要・特徴など
不正プログラム対策技術	現在のウイルスに対する対抗策は、各個人が所有するコンピュータ（以下「ノード」という。）に対し免疫を与えウイルスのまんえんを抑制している。これはネットワークの中からランダムにノードを選び免疫を与えている事になる（ランダム型）。バラバシ＝アルバートモデル（BAモデル）を用いたシミュレーションでは、この免疫配置手法ではネットワーク内部の８割ものノードに対し免疫を与えなければならないことが過去の研究から分かっている。 そのため平成14年にCohen らは、ネットワークの中からランダムにノードを選び、そのノードに隣接しているノード1つに免疫を与える手法（Cohen型）を提案し、２割程度の免疫数でウイルスのまんえんを抑制できることを実証した。 そこで、Cohen型を改良した手法の提案と、ASネットワーク（企業や学校などの団体を１ノードとした現実ネットワークデータ）を用いたシミュレーションでの効果の違い、またASに対する各免疫配置手法の効果の違いについての原因の解明を行った。 Cohen型では免疫を与えたノードのリンク数（ノード同士のつながり）がランダム型よりも多い特徴がある。これによりウイルスの拡散を最小限に留めることができ、ランダム型よりも効果的にウイルスのまんえんを抑制できる。これを応用し、Cohen型の改良として、ネットワークからある一つのノードを選び、そのノードに隣接している最もリンク数の高いノードに免疫を与える手法（Cohen改良型）でシミュレーションを行った。この結果、Cohen型よりもリンク数の多いノードに対し免疫を与えることができ、BAモデル、AS共にCohen型よりもCohen改良型のほうが効果的にウイルスのまんえんを抑制できた。

【企業】

企業名	株式会社エヌ・ティ・ティ・データ（略称NTTデータ）NTT DATA CORPORATION
所在地	〒135-6033 東京都江東区豊洲3-3-3 豊洲センタービル
関連部署／電話番号	TEL.03-5546-8202（代表）
ホームページのURL	http://www.nttdata.co.jp/index.html
対象技術	技術の概要・特徴など
・侵入検知・防御技術 ・ぜい弱性対策技術	■使いこなせるOSセキュリティ強化カーネル TOMOYO(R) Linux ＜商品概要＞ ・Linuxサーバ向けのセキュリティ強化カーネルであり、アクセス制御機能を強化することで、システムへの不正侵入を防止します。アクセス許可の学習機能により、セキュリティポリシー作成の労力を大幅に削減します。直感的なアクセス許可の指定が可能な構文により、使いこなせるセキュアなＯＳを実現します。 ＜用途・適用業務＞ ・アプリケーションレベルでのアクセス制御を行うシステム（Webサーバ、APサーバ、DBサーバ等）に存在する未知のセキュリティホールを攻撃してシステムに侵入されるという脅威に対する保険として利用します。 ＜メリット・効果＞ ・システム管理者が作成したポリシーに基づきファイルの読み書きやプログラムの実行を制限することで、セキュリティホールに起因する不正侵入に対する耐性を大幅に高めます。また、セキュリティ修正プログラムの適用頻度を減らすことができるようになるため、動作確認試験のための稼動を大幅に削減できます。 ・ポリシーを最初から作成できるため、管理者が許可したいことだけを許可できます。また、ポリシーの作成を支援する機能があり、管理者が許可したいことを実行するだけでポリシーを作成できます。ポリシーの構文は単純で誰でも理解して使いこなせます。必要に応じてログイン認証の強化や管理者業務の分担も実現できます。 ＜特徴＞ ・理解して使いこなせることを念頭に開発されているので、誰でも簡単に導入及び運用ができます。 　実際のシステムの振る舞いに沿ってポリシーを作成するため、自然な記述ができます。そして、ポリシーの内容は誰にでも理解できるため、不要なアクセス許可を確実に検出することができます。 　TOMOYO Linuxは学習機能によりポリシーを作成することができるため、Linuxディストリビュータが関与できない独自アプリケーションに対応することが得意です。

企業名	株式会社ソリトンシステムズ（Soliton Systems K.K.）
所在地	東京都新宿区新宿2-4-3
関連部署／電話番号	本社　03-5360-3811
ホームページのURL	http://www.soliton.co.jp/
対象技術	技術の概要・特徴など
・高度認証技術	■有線/無線LANはもちろん、VPN、ダイヤルアップも安全にLANは、企業に蓄積されたあらゆる情報への出入口です。誰もが無秩序に接続できる状態ではなく、決められた人、決められたPCだけが接続できるように鍵をかけておく必要があります。 NetAttest EPSにはLANへの接続時にユーザやPCを特定する認証サーバとしてIEEE802.1X等ネットワーク認証に必要な機能が詰め込まれています。LAN接続時に認証を行えば、正規のユーザの利便性を損ねずに不正なユーザやPCをシャットアウトできます。もちろんLANへの直接接続だけではなく、VPNやリモートアクセス接続など、ネットワークの入り口を1台で守る統合認証サーバとして活躍します。 ■利用可能なユーザ情報データベース ・ローカル NetAttest EPSに内蔵されたデータベースです。 ・Active Directory Active Directory に登録されたユーザを参照できます。主にMS-PEAP 認証で利用します。 ・LDAP X.500準拠のLDAPサーバに登録されたユーザ情報を参照し認証できます。主にPAPで利用します。 ・RADIUS RADIUSプロキシ機能により、受信した認証要求を他のRADIUSに転送し、認証できます。 ■本格的なプライベートCA 証明書の発行や運用に必要な各種機能を搭載しています。証明書の要求から、承認、発行、配付、更新などの一連のワークフローを提供し、証明書の運用・管理負荷を大幅に軽減します。 ■ワンタイム・パスワード 認証のたびに毎回違うパスワードを利用するワンタイム・パスワードが利用可能です。別途サーバを用意することなく、手軽に利用開始できます。PCでもスマートフォンでも端末を問わず高いセキュリティを確保します。VPN接続の認証に最適です。

企業名	ヌリテレコム株式会社
所在地	東京都千代田区麹町3-2-4
関連部署／電話番号	03-3512-2882
ホームページのURL	http://www.nuritelecom.co.jp/index.html
対象技術	技術の概要・特徴など
･不正プログラム対策技術	・USBストレージ、CD/DVD、SDメモリカード、FDの使用を禁止します。 ・社内で使用する外部記憶媒体を管理し、個人所有の外部記憶媒体の使用を禁止することができます。 ・一時的に使用可能にした後、自動的に使用禁止に戻すことができます。 ・管理者のための機能が充実しています。 ・各PCの設定変更や一括変更、一覧表示が行えます。 ・PCをグルーピングして管理することができます。 ・禁止対象外のユーザを設定することができます。 ・禁止設定を行っているPCでも、緊急時に管理者がデバイスを使用することができます。 ・アプリケーションの起動には管理者パスワードが必要です。コンソールの操作履歴が採取できます。 ・アンインストールやサービスの停止、使用禁止設定変更のためには管理者パスワードが必須です。

企業名	株式会社シー・エス・イー
所在地	〒150-0044東京都渋谷区円山町23-2 アレトゥーサ渋谷ビル
関連部署／電話番号	03-3463-5631 （代表）
ホームページのURL	http://www.cseltd.co.jp/
対象技術	技術の概要・特徴など
・高度認証技術	SECUREMATRIX（セキュアマトリクス）は、株式会社シー・エス・イーが開発した、認証デバイスを一切使わない本人認証システムです。人が頭の中に思い描くイメージからワンタイム・パスワードを生成する「マトリクス認証」方式を採用し、セキュリティ及び利便性の向上、コスト削減の全てを同時に実現します。 ＜マトリクス認証の仕組み＞ 「マトリクス認証」は、ユーザがあらかじめ設定した「位置」と「順番」（＝パスワードイメージ）を使って、マトリクス表（アクセスするたびにランダムに表示が変わる乱数表）から、その位置と順番に当てはまる数字を抜き出してワンタイム・パスワードとして認識させる認証方式です。パスワードは「ワンタイム（使い捨て） 」になるため、強固な認証を実現できます。

企業名	ファインアートテクノロジー
所在地	〒30072 台湾新竹市埔頂路18号8F
関連部署／電話番号	886-3-577-2211（代表）
ホームページのURL	http://www.fineart.com.tw/jp/
対象技術	技術の概要・特徴など
・不正プログラム対策技術	■X-FORT主要機能 ・コンピュータ周辺機器経由の情報漏えい防止 UFD、モバイルハードディスク、メモリカード等各種外部メモリデバイス及びCD/DVD-ROMドライブ、プリンタ、赤外線、Bluetooth等の書き出しルートを制御することができます。またハードプロテクションメカニズムを提供、ディスクによる起動やハードディスク接続によるデータの持ち出しを防止します。特に外部メモリデバイスに対し、禁止・リードオンリー・自動暗号化・管理者承認等多種のアクセスパターンを提供、情報セキュリティとユーザビリティを兼備した柔軟なツールです。 ・ネットワーク経由の情報漏えい防止 マイネットワークの利用を厳格に制御、電子メール、IMソフトウェア、P2Pソフトウェア、FTP、Webアップロード等の方法によるファイル転送、3G／3.5Gネットワークカード、無線ネットワークカード、ダイヤルアップネットワーク接続等行為等、完璧にネットワークルートの流出を制御します。 ・トータルなコンピュータ管理ツール 具有ソフトセキュリティ、リモートコントロール、ファイル転送、コンピュータ資産管理、Windows Update及びWSUS・Hotfix等コンピュータ管理機能を統合、また豊富な分析レポートを提供、コンピュータの状況を完全に把握することができます。 健全なシステム構成：データベース及びエクスポートログの定期バックアップカスタマイズが可能、事後調査のよりどころとすることができます。さらに自動バックアップ及びロードバランス機能を備えたclient-server構成、複数拠点を擁する大型企業に対しサーバ間の同期及び暗号ローミングメカニズム等多様なサーバ集中管理機能を提供します。 ・システムのセルフディフェンスメカニズム 作為的なデータの破壊や削除行為を回避します。クライアントへのサイレントインストールはユーザの操作にまったく影響を及ぼしません。

企業名	シスメックスＲＡ株式会社
所在地	本社　〒399-0702 長野県塩尻市広丘野村1850-3
関連部署／電話番号	TEL．0263-54-2251（代）
ホームページのURL	http://www.sysmex-ra.co.jp/
対象技術	技術の概要・特徴など
・ぜい弱性対策技術 ・高度認証技術	■IPsecによる強固なセキュリティ機能 　強力な暗号化と認証機能を持ったIPsecにてプロトコルやアプリケーションに関係なく転送される通信データ（TCP/UDPパケット）のセキュリティ機能を高めることができます。 ■簡単接続 　イーサネットインターフェースを2ポート装備し、通信機器とLANケーブルの間に中継器として挟み込むだけで通過する通信データは自動的に暗号化され送信先へと転送されます。 また、通信機器へは設定変更や特殊なアプリケーションをインストールする必要はなく、既存システムへの導入が迅速に行うことができます。 ■柔軟設定 　設定はPC上から専用ツール（NSSetup）にて行います。 認証キーの設定のみで完了する基本的な対向通信から、詳細なセキュリティポリシーの設定による経路別の動作指定といった応用的な用途まで幅広く柔軟に対応できます。 ■高速・安定動作 　専用ASICによるハードウェア処理により、最高90Mbps（AES、512byte/pkt双方向通信時のSmartbit値）の高速で安定した動作を実現しています。 ■NAT対応 　NAT-Traversal/UDP-Encapsulation によるNAT越えを実現できます。

企業名	ウォッチガード・テクノロジー・ジャパン株式会社
所在地	〒150-8512 東京都渋谷区桜丘町26-1 セルリアンタワー15階(本社は米国)
関連部署／電話番号	03-5456-7880
ホームページのURL	http://www.watchguard.co.jp/
対象技術	技術の概要・特徴など
・侵入検知・防御技術	■ XTM多機能ファイアウォール WatchGuard XTMネットワーク・セキュリティ・アプライアンスは、新しいクラスのパフォーマンス・ソリューションです。 高速スループットを大量のトラフィックに対応できる先進的なネットワーク機能と組み合わせ、手頃な価格で提供できます。 標準で柔軟な管理ツールがバンドルされているので、IT管理者は中央のコンソール、コマンドラインインタフェース、またはWebUIから一元的にセキュリティ管理を行うことが可能です。 WatchGuard XTMは、全部で16モデルです。 ・50ユーザから10,000ユーザ以上の環境まで、幅広いビジネスに対応しています。 ・Firewall、UTM機能をベースにレイヤ7のアプリケーション制御を実施できます。

企業名	株式会社ＣＩＪ
所在地	横浜市西区平沼1-2-24 横浜ＮＴビル
関連部署／電話番号	045-411-2571（市場開拓推進事業部市場開拓企画部）
ホームページのURL	http://bunshokanri.jp/
対象技術	技術の概要・特徴など
・その他アクセス制御に関する技術	Ofigoは文書管理システムと契約書管理システムをラインナップしたシリーズ製品 ■Ofigo文書管理 　Ofigo文書管理サーバへは、使いなれたブラウザでアクセスでき、登録も簡単な操作でドラッグ＆ドロップできるため「使いやすく、分かりやすい」４階層構造となっています。 その他 ・アクセス権限の設定で、重要ファイルへのアクセスを制限 ・Ofigo文書管理サーバへの全操作ログを保管 ・データは自動で暗号化。万が一の場合も情報漏えい防止 ・「確定署名」でファイルを改ざんから守る ことができます。 ■Ofigo契約書管理 　締結されている契約書の内容など都度総務に電話して聞かなくても、この契約書管理ソフトをインストールすれば自席のパソコンより確認ができます。 締結先、契約名、担当者など、各種の属性で検索できるので大量の契約書から該当する契約があるか？その内容は？などすぐさま確認することができます。 　契約の更新・メンテナンスなどに便利な、期限通知ができます。 　通知日と通知先を設定しておくことで、自動でメール通知が行われます。また、この設定は何個でも設定することが可能です。

企業名	日本信号株式会社（THE NIPPON SIGNAL CO.,LTD）
所在地	〒100-6513 東京都千代田区丸の内1-5-1 新丸の内ビルディング
関連部署／電話番号	03-3217-7200
ホームページのURL	http://www.signal.co.jp/
対象技術	技術の概要・特徴など
・侵入検知・防御技術	■目的 入室管理と連携し、物理資産の閲覧・貸出しの管理を行う。 ■機能概要 ・書類検知（常時） ・書類位置検索、表示 ・書類アクセス検知 ・書類持ち出し／貸出し管理 ・返却管理 ・不正アクセス管理 ■システム利用例 ・物理資産に積層ICタグを貼り付け、登録用リーダでサーバに登録する。 ・積層ICタグを貼り付けた物理資産を各書庫に設置し、積層ファイルリーダにより常時監視を行う。 ・書庫から書類を取り出す際には、各書庫の上に設置された認証用リーダに物理資産をかざし持ち出す。 ・認証せずに物理媒体を持ち出す等の不正があったときには警報装置が作動する。 ■システム構成及び導入規模の例 ・積層ICタグ１万5000枚 ・積層ファイルリーダ ・積層トレイリーダ ・管理サーバ ・情報端末必要数 ・警報装置必要数 ・入室管理システム別途用意

企業名	日本信号株式会社（THE NIPPON SIGNAL CO.,LTD）
所在地	〒100-6513 東京都千代田区丸の内1-5-1 新丸の内ビルディング
関連部署／電話番号	03-3217-7200
ホームページのURL	http://www.signal.co.jp/
対象技術	技術の概要・特徴など
その他アクセス制御に関する技術	■目的 　交通ICカードシステムの内部統制を実現するために、交通ICカード利用における一件明細の完全性保障と不正行為を防止する。 ■機能概要 ・接続するネットワークの正当性検証 ・運用者及び保守員の識別・認証 ・権限に応じたアクセス制御 ・データ保護 ・監査ログ取得 ■アクセス制御機能を実装した装置の例 ・自動券売機 ・自動精算機 ・自動改札機 ・駅係員端末 ・チャージ機

企業名	日本無線株式会社
所在地	〒167-8540東京都杉並区荻窪4-30-16藤澤ビルディング
関連部署／電話番号	03-6832-1721（代表）経営企画室／0422-45-9774
ホームページのURL	http://www.jrc.co.jp/jp/index.html
対象技術	技術の概要・特徴など
ぜい弱性対策技術	NDC-1434は、異なるイントラネットワーク間で、TCP/IPにより情報交換を行う場合のIPアドレス変換やセキュリティ問題を解決するゲートウェイ装置です。 ◆８組のクライアントーサーバ間のTCPコネクションデータを中継することが可能です。 ◆ネットワーク間の分離が可能となり、インターネットワーク間のセキュリティ機能を実現します。 ◆イントラネットワーク間のIPアドレス体系を完全に分離できます。

企業名	富士通株式会社
所在地	本店住所: 〒211-8588 神奈川県川崎市中原区上小田中4-1-1
関連部署／電話番号	044-777-1111
ホームページのURL	http://jp.fujitsu.com/
対象技術	技術の概要・特徴など
その他アクセス制御に関する技術	Interstage Application Server （インターステージアプリケーションサーバ）は、変化するビジネス環境を継続的に支える高信頼・高性能なアプリケーション実行基盤です。 富士通独自のスマートソフトウェアテクノロジー（注）と互換性保証及び標準技術への対応により、業務システムの安定稼動や、素早いシステム構築や柔軟なサーバ集約を実現します。