平成１６年３月４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１５年１月１日から平成１５年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

警察庁、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ﾍﾟｰｼﾞ　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15年中の不正アクセス禁止法違反事件の検挙状況等について

平成15年中に全国の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。

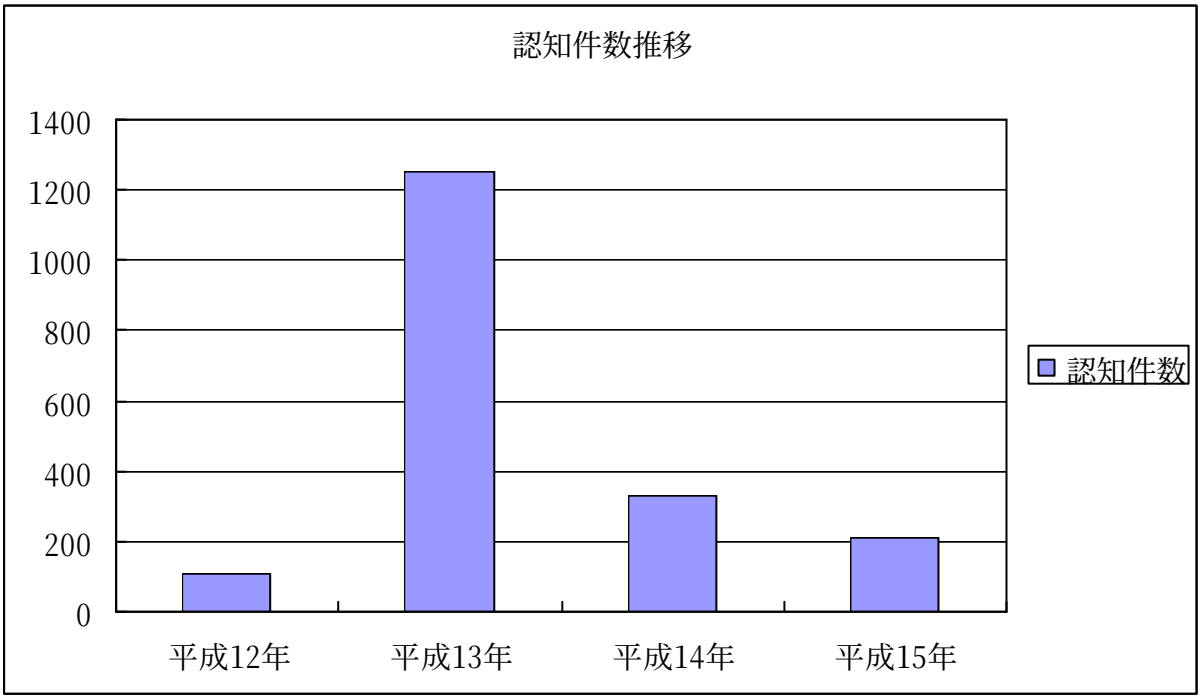
なお、本文中平成12年の数字は、不正アクセス禁止法の施行日である平成12年２月13日から平成12年12月31日までの間のものである。

１　不正アクセス行為の発生状況及びその特徴

(1) 認知件数（注１）（注２）

平成15年中の不正アクセス行為の認知件数は212件で、前年と比べ、117件減少した。

なお、平成13年の不正アクセス行為の多発は、ホームページ書き換えプログラム（コンピュータ・ワーム）によるものである。



	平成12年	平成13年	平成14年	平成15年
認　知　件　数	106	1,253	329	212
海外からのアクセス	25	448	13	35
国内からのアクセス	73	258	286	158
アクセス元不明	8	547	30	19

(2) 被害に係る特定電子計算機（注３）のアクセス管理者（注４）

被害に係る特定電子計算機のアクセス管理者を見ると、プロバイダが98件と最も多く、次いで一般企業の76件となっている。

被害に係る特定電子計算機のアクセス管理者	平成12年	平成13年	平成14年	平成15年
プロバイダ	59	182	243	98
一般企業	25	429	62	76
大学、研究機関等	8	101	3	16
その他	14	139	21	22
うち行政機関	-	-	12	3
不明	0	402	0	0
計	106	1,253	329	212

※　「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、大学、高等学校等の学校機関及びその附置機関を含む。

「その他」の「うち行政機関」には、国の行政機関、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。

なお、平成12年及び13年は「その他」の内訳の集計をしていない。

(3) 認知の端緒

認知の端緒としては、警察職員によるサイバーパトロールや被疑者の取調べ等の警察活動が100件と最も多く、次いで利用権者（注５）からの届出が78件、発見者からの通報が19件、アクセス管理者からの届出が12件の順となっている。

認知の端緒	平成12年	平成13年	平成14年	平成15年
アクセス管理者からの届出	30	168	47	12
利用権者からの届出	23	118	92	78
警察活動	35	930	185	100
発見者からの通報	7	21	0	19
その他	11	16	5	3
計	106	1,253	329	212

(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、ホームページの改ざんが49件で最も多く、次いで電子メールの盗み見等の情報の不正入手が48件であり、他にインターネット・オークションに関する不正操作（他人になりすましての入札、販売代金の取得等）が40件、オンラインゲームの不正操作が29件、判明したID・パスワードの販売が16件、インターネットの利用が６件等であった。

2　不正アクセス禁止法違反事件の検挙状況

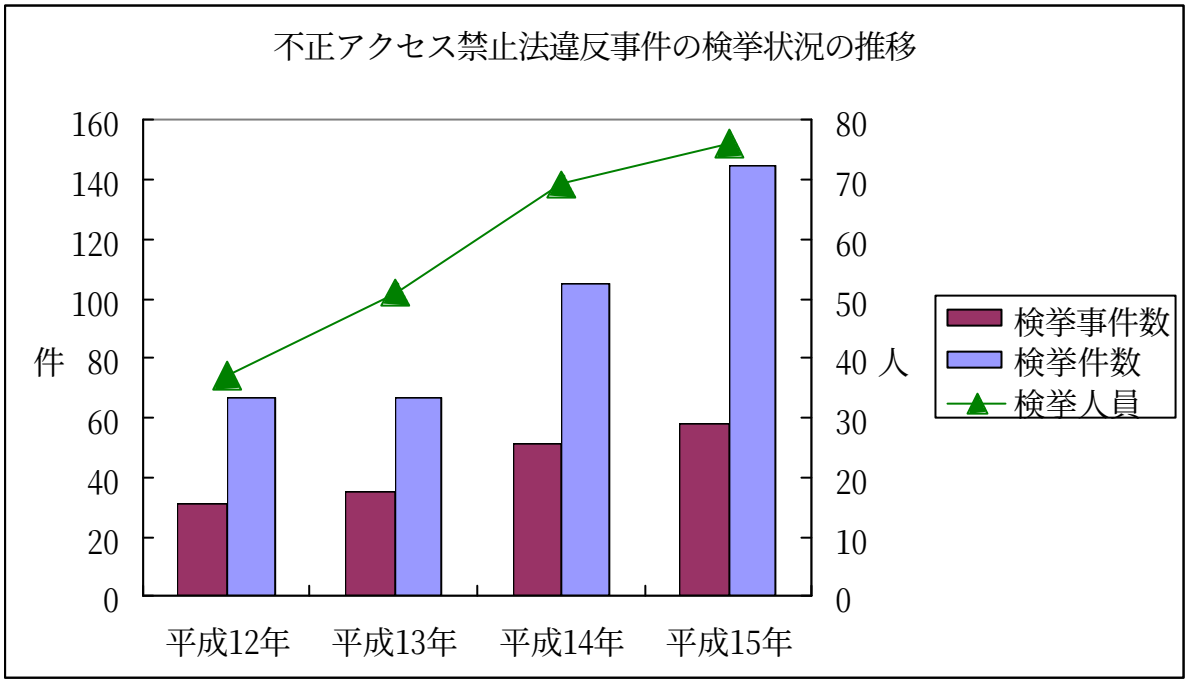
不正アクセス禁止法違反の検挙事件数（注６）は58事件（145件)、検挙人員は76人で、前年と比べ検挙事件数は７事件（40件）増加し、検挙人員は７人増加した。その内訳は、不正アクセス行為が58事件(143件)、76人であり、不正アクセス助長行為は２事件(２件)、２人であった。

検挙事件のほとんど（56事件、141件）は識別符号窃用型（注７）であり、利用権者のパスワードの設定・管理の甘さにつけ込んで入手したものが最も多かった。

不正アクセス行為により利用されたサービスとしては､オンラインゲーム・サービス、電子メール・サービス、インターネット・オークション・サービス等がみられた。

このほか、２事件（２件）がセキュリティ・ホール攻撃型（注８）であった。

なお、検挙人員76人中60人が成人であり、16人が少年であった。



		平成12年	平成13年	平成14年	平成15年
不正アクセス行為	検挙事件数	30	35	51	58
	検挙件数	62	66	102	143
	検挙人員	34	51	68	76
不正アクセス助長行為	検挙事件数	4	1	2	2
	検挙件数	5	1	3	2
	検挙人員	5	1	3	2
計	検挙事件数	31 (重複3)	35 (重複1)	51 (重複2)	58 (重複2)
	検挙件数	67	67	105	145
	検挙人員	37 (重複2)	51 (重複1)	69 (重複2)	76 (重複2)

3　検挙事例

1	企業の業務用電子メールの盗み見に係る不正アクセス禁止法違反及び電子掲示板を利用した名誉毀損事件

会社員の男（45）が、勤務先の商社を解雇させられたことを恨み、嫌がらせをする目的で、平成14年６月から９月までの間、同商社の社員７人が業務で使用する電子メール用のＩＤとパスワードを使用し、メールサーバに不正アクセスして電子メールの内容を盗み見した上で、無料のインターネット電子掲示板に、商社の事業に関する内容虚偽の文言を投稿掲示した。平成15年１月、不正アクセス禁止法違反及び名誉毀損罪で検挙した（奈良）。

2	ゲームアイテムの換金を目的にオンラインゲームの識別符号を窃用した不正アクセス禁止法違反事件

自営業の男（21）が、知人の女性がオンラインゲームの世界で持つゲームアイテム（ゲーム上で利用する仮想の道具等）を無断で換金する目的で、オンラインゲームのリマインダ機能（注９）によりパスワードを入手して、平成14年９月から11月までの間、女性が使用するＩＤ及びパスワードを窃用してサーバに不正アクセスし、女性になりすまして他人にアイテムを譲渡して現金に換金した。15年２月、不正アクセス禁止法違反で検挙した（警視庁）。

3	インターネット・バンキング利用の不正送金に係る不正アクセス禁止法違反、私電磁的記録不正作出・同供用及び電子計算機使用詐欺事件

無職の男（35）が、他人の口座から金を不正に得る目的で、平成14年９月、銀行のインターネット・バンキング用の認証サーバに、あらかじめキーロガー（注10）を用いて収集していた口座開設者５人のＩＤ及びパスワードを使用して不正アクセスし、うち１名の口座から、他の銀行に開設していた架空名義の口座へ送金操作を行い、現金自動預払機から、同口座の現金1,600万円を引き出して窃取した。15年３月、不正アクセス禁止法違反、私電磁的記録不正作出・同供用罪、電子計算機使用詐欺罪でこの男を検挙するとともに、現金の引出操作をした会社員の男（27）を組織的犯罪処罰法違反（犯罪収益隠匿）で検挙した（警視庁）。

4	インターネット・オークションに係る識別符号の販売を目的とした不正アクセス禁止法違反事件

無職の男（40）が、他人が使用するインターネット・オークション用のＩＤ及びパスワードを第三者に提供して不正に金を得る目的で、平成14年９月から11月までの間、多数のＩＤに対してパスワードを推測して入力する操作を行い、合致した15件のＩＤ及びパスワードにより、インターネット・オークション・サービスのサーバに不正アクセスした。15年５月、不正アクセス禁止法違反で検挙した（京都）。

5	リマインダ機能を利用して入手したパスワード使用による出会い系サイトに係る不正アクセス禁止法違反事件

会社員の男（31）が、平成14年11月、リマインダ機能を利用して出会い系サイトの女性会員のパスワードを入手し認証サーバに不正アクセスし、女性会員の自己紹介欄に自己のホームページのアドレスを登録した。女性会員の自己紹介欄を見た男性らに、男の開設したホームページを女性のものと信じ閲覧させることで、当該ホームページに貼り付けた出会い系サイトのバナー広告による収入を得ていたもの。
平成15年５月、不正アクセス禁止法違反で検挙した（京都）。

6	セキュリティ・ホール攻撃によりホームページを改ざんした不正アクセス禁止法違反事件

高校生（15）が、自己の技量を試し、愉快感を味わう目的で、平成14年11月から15年４月までの間、Ｗｅｂサーバのホームページ管理プログラムに存在するセキュリティ・ホールを攻撃する手法等により、約23カ国・地域の140のＷｅｂサーバに不正アクセスしてホームページを改ざんした。15年６月、不正アクセス禁止法違反で検挙した（警視庁）。

7	インターネット・オークションの識別符号を窃用した不正アクセス禁止法違反及び詐欺事件

自営業の男（32）ら男女６人が、インターネット・オークションを利用して金をだまし取る目的で、平成14年５月から11月までの間、他人が使用するオークション・サービス用ＩＤ164個のパスワードを推測して不正アクセスした上、当該ＩＤを使用して架空のオークション出品操作を行い、偽名で開設した口座に現金を振り込ませる手口で約390名から総額約1,200万円をだまし取った。平成15年７月までに、不正アクセス禁止法違反、詐欺罪、組織的犯罪処罰法違反（隠匿・収受）等で６人を検挙した（茨城、広島）。

8	ホームページ管理用ＩＤの窃用による不正アクセス禁止法違反、電子計算機損壊等業務妨害及び脅迫事件

会社経営の男（37）が、元取引先への恨みから、平成15年５月、元取引先のホームページ管理用のＩＤ及びパスワードを使用してＷｅｂサーバに不正アクセスし、ホームページのファイルデータを削除して業務を妨害したほか、元取引先の経営者にあてて脅迫の電子メールを送信した。15年７月、不正アクセス禁止法違反、電子計算機損壊等業務妨害罪及び脅迫罪で検挙した（千葉）。

9	電子掲示板の投稿を契機としたインターネット・オークションのＩＤ窃用による多人数の不正アクセス禁止法違反事件

インターネットの電子掲示板に、あるインターネット・オークション利用者のパスワードを推測するヒントが投稿掲示されたことから、掲示を閲覧した多数の者がパスワードを推測し、好奇心等から、平成15年１月、それぞれが同ＩＤ及びパスワードを使用してオークションサービスのサーバに不正アクセスした。15年７月から10月までに、不正アクセス禁止法違反で会社員（36）、学生（21）、少年（19）ら10人を検挙した（京都、北海道、秋田、山形、埼玉、兵庫）。

10	セキュリティ・ホール攻撃によりホームページを改ざん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

派遣社員の少年（17）が、自己の技量試し等を目的に、平成14年９月、東京都内の私立高校及びコンピュータサービス会社が公開していたホームページをそれぞれ改ざんしたほか、15年７月、京都市内の病院が管理するＷｅｂサーバに対して、セキュリティ・ホールを攻撃して不正アクセスし、同サーバで公開されていたホームページを改ざんした。15年10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罪で検挙した（警視庁）。

4　検挙事件の特徴

(1) 犯行の手口

検挙した不正アクセス行為のほとんど（56事件（141件））が識別符号窃用型であったが、当該識別符号（ＩＤ及びパスワード）の入手方法については、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（ＩＤ等から容易に推測されるパスワードが利用されていたもの等）が前年に引き続き最も多く、26事件（77件）であった。次いで元従業員等の、立場上識別符号を知りうる立場にあった者によるものが15事件（23件）、盗み見・盗み聞き等により利用権者から直接入手したものが３事件（３件）、

リマインダ機能における質問への安易な回答が設定されていたものが２事件（21件）、利用権者になりすましてアクセス管理者から入手したものが２事件（２件）、何者かにより識別符号がインターネット上に公開されていたものが１事件（４件）であった。

また、プログラムの脆弱性を利用したホームページの改ざんのように、セキュリティの脆弱性を突くセキュリティ・ホール攻撃型も引き続きみられたほか、キーロガーを使用して識別符号を入手するなど、高度なコンピュータ技術を悪用したものもあった。

(2) 被疑者

元交際相手や元従業員等顔見知りの者による犯行は26事件（35件）（うち１事件は被疑者２名のうち１名が利用権者と顔見知りで１名が利用権者と他人。）、全くの他人による犯行は20事件（98件）であり、実際には会ったことがないネットワーク上のみの知り合いによる犯行は12事件（12件）であった。

また、検挙した被疑者の年齢は、20代が26人と最も多く、次いで30代が24人、10代が16人、40代が９人、50代が１人の順となっており、20代以下が過半数を占めた。最年少の者は14歳であり、最年長の者は50歳であった。

(3) 犯行の動機

不正アクセス行為の動機としては、嫌がらせや仕返しのためが最も多く、元交際相手や元勤務先等に対するもののほか、気を紛らわすための無差別な嫌がらせも含め22事件（30件）であった。次いで好奇心を満たし又は自己の技量を試すためが18事件（47件）、不正に金を得るためが11事件（73件）、オンラインゲームで不正操作を行うためが５事件（５件）、メールを盗み見るためが２事件（５件）、料金請求を免れるためと自分のＩＤにはない機能を利用したかったためがそれぞれ１事件（１件）の順となっている（重複計上あり）。

前年と比べると、嫌がらせや仕返しのためが３事件（１件）、好奇心を満たし又は技量試しのためが４事件（14件）それぞれ増加し、特に不正に金を得るためが急増し９事件（67件）増であった。

(4) 利用されたサービス

識別符号窃用型の不正アクセス行為で検挙した56事件（141件）において、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別にみると、オンラインゲーム・サービスが13事件（13件）と最も多く、次いで電子メール・サービスが11事件（17件）、インターネット・オークション・サービスが10事件（61件）、ホームページ公開サービスが10事件（11件）、掲示板等会員専用サイトの閲覧が６事件（29件）、インターネット接続サービスが３事件（３件）、インターネット・バンキングが１事件（５件）等となっている。

(5) その他

不正アクセス禁止法違反のほか、他の罪についても検挙した事件は、19事件であった。

	事件数
私電磁的記録不正作出・同供用	4
電子計算機損壊等業務妨害	4
電子計算機使用詐欺	3
脅迫	2
詐欺	2
電気通信事業法	2
有印私文書偽造・同行使	1
わいせつ図画販売目的所持	1
名誉毀損	1
窃盗	1
恐喝	1
覚せい剤取締法違反	1
麻薬及び向精神薬取締法違反	1
児童買春・児童ポルノ禁止法違反	1
組織犯罪処罰法違反	1

注　重複計上あり。

5　都道府県公安委員会による援助措置

都道府県公安委員会は、不正アクセス行為を受けたアクセス管理者からの申出への対応として、不正アクセス禁止法第６条の援助規定に基づくアクセス管理者に対する助言・指導を５件（北海道１、宮城１、愛知２、佐賀１）実施した。

6　防御上の留意事項

(1) 利用権者の講ずべき措置等

ア　パスワードの適切な設定・管理

識別符号窃用型の不正アクセス行為で検挙した56事件（141件）中、26事件（77件）では、パスワードがＩＤから容易に推測できるもの（例えば、ＩＤが「abcd1234」に対して、パスワードが「abcd」や「1234」）等であったことから、利用権者においては、そのような行為を防ぐため、他人による推測が難しいパスワードを設定する必要がある。

また、15事件（23件）が、かつて当該パスワードを利用していた者や、利用権者のパスワードをのぞき見ることができた者の犯行であり、アクセス管理者及び利用権者がパスワードの設定・管理を適切に行っていなかったことが問題点として挙げられる。利用権者等においては、パスワードを定期的に変更するなど、パスワードを適切に設定・管理する必要がある。

イ　リマインダ機能の適切な設定

リマインダ機能を悪用して、アクセス管理者からパスワードを入手する手口が引き続きみられた。アクセス管理者及び利用権者においては、パスワード再発行時に必要となる情報（質問に対する回答）について、他人による推測が困難となるような仕組み及び内容とする必要がある。

ウ　不特定多数の人が利用できる端末を利用する際の注意

インターネット・カフェ等のパソコン端末に、キーロガーを仕掛け、インターネット・バンキングのＩＤやパスワードを入手する手口がみられたことから、不特定多数の人が利用できるような端末では、口座番号やクレジットカード番号を始め、個人情報等の入力を伴うサービスの利用については、出来るだけ避ける必要がある。

(2) アクセス管理者の講ずべき措置等

ア　セキュリティ・ホールに関する対策

セキュリティ・ホール攻撃型の不正アクセス行為事犯は、一旦発生すれば被害が大きくなる危険があることから、セキュリティ水準の維持・向上が不可欠であり、特にサーバの管理者等はインターネット上等で公表される最新のセキュリティ情報を定期的に確認し、使用しているオペレーティング・システム又はアプリケーション・プログラムにセキュリティ・ホールが発見されたことを知ったときは、速やかに修正プログラムをインストールするなど既に判明しているセキュリティ・ホールを解消するための措置等を講じる必要がある。

イ　不特定多数の人が利用できる端末の適切な管理

インターネット・カフェ等の不特定多数の人が利用できる端末の管理者及び運営者は、個人情報等の入力については十分注意を払うよう利用者に注意喚起を行うとともに、リカバリーソフト（コンピュータ内の情報を利用前の状態に戻すソフト）の導入、不必要な履歴の削除、利用者によるプログラムのインストール制限等を実施することが必要である。

ウ　その他

アクセス管理者は、サーバを適切に管理するだけでなく、利用権者に対して識別符号の適切な設定・管理について注意喚起を行うほか、容易に推測されるおそれのあるパスワードを設定できないようにする仕組みを活用するなど、不正アクセス行為を防止するために必要な措置を講ずる必要がある。

(参考)

注１　認知

ここで認知とは、被害の届出を受理をした場合のほか、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としている。

注２　件数

件数とは、被疑者が行った犯罪構成要件に該当する行為の数をいう。

なお、不正アクセス行為の件数の計上については、一つのアクセス制御機能に対する一つの手口による侵害行為が１回あったことをもって１件としている。ただし、被疑者が異なる場合（共犯を除く。）はそれぞれ１件として計上し、短期間に一つのアクセス制御機能に対して同一手口による侵害が連続的に行われ、実質上１回の行為とみなしうる場合は包括して１件としている。

注３　特定電子計算機

特定電子計算機とは、電気通信回線に接続している電子計算機をいう。

注４　アクセス管理者

アクセス管理者とは、ネットワークに接続しているコンピュータ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店主が、それぞれアクセス管理者である。

注５　利用権者

利用権者とは、ネットワークに接続されたコンピュータをネットワークを通じて利用することについて、当該コンピュータ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６　事件数

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も１事件と数える。

注７　識別符号窃用型

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。

例えば、他人のインターネット・オークション用のＩＤ及びパスワードを使用して、当該インターネット・オークションを利用する行為が該当する。

注８　セキュリティ・ホール攻撃型

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。

注９　リマインダ機能

利用権者がパスワードを忘れてしまった時に、アクセス管理者が何らかの方法で本人確認を行った上でパスワードを再発行する機能をいう。本人確認の方法としては、サービス利用のための登録時に、本人が決めた情報を登録しておき、パスワードの再発行時にその情報を利用権者に入力させるもの（例えば、「出身小学校は？」等の質問に対して、あらかじめ登録しておいた情報を答えとして入力すると、パスワードが再発行される）等がある。

注10　キーロガー

インストールしたパソコン端末において、キーボードでどの文字を打鍵したかを記録するプログラムをいう。

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　独立行政法人情報処理推進機構(ＩＰＡ)（平成16年1月5日より情報処理振興事業協会から改組)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１５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被害届出件数は407件（昨年：619件）であった（注２）。平成１５年は侵入やアクセス形跡、メール不正中継などの届出が減少した一方、ワームに関する届出が若干増加した。

以下に、種々の切り口で分類した結果を示す。各々の件数には未遂(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分類に該当するものがあるため、それぞれの項目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。重複があるため、届出件数とは異なり総計は510件（昨年：790件）となる。なお、この件数には、ワームに関する届出は含まれていない。

ア 侵入行為に関して

侵入行為に係わる攻撃等の届出は313件（昨年：671件）あった。

(ｱ) 侵入の事前調査行為

システム情報の調査、稼動サービスの調査、アカウント名の調査等である。

110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など、侵入のための行為である。

110件の届出があり、これらのうち実際に侵入を受けたものは64件である。

パスワード推測：4件

ソフトウェアのバグを利用した攻撃：55件

システムの設定内容を利用した攻撃：19件

(ｳ) 不正行為の実行及び目的達成後の行為

実際に侵入を受けた64件について、その後行われた種々の行為である。１件の侵入で種々の行為が行われているため重複がある。

ファイル等の改ざん、破壊等：38件

プログラムの作成(インストール)、システムファイルの改ざん、トロイの木馬などの埋め込み等：25件

資源利用（ファイル、CPU使用)：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：13件

裏口の作成：2件

証拠の隠滅：7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もしくは低下させる攻撃である。15件（昨年：22件）の届出があった。

過負荷を与える攻撃：8件

例外処理を利用した攻撃：2件

spamメール：5件

ウ　その他

その他には、ソーシャルエンジニアリングや、サービスの外部からの利用が含まれ、57件（昨年：97件）の届出があった。

メール中継に関するもの：11件

そのうちメール中継に実際に利用されたもの：9件

メールアドレス(ドメイン)の詐称：18件

その他：28件

(2)　ワーム別の分類

ワームの種類による分類である。ワームに関する届出は、実際にワームに感染した届出5件、ワームには感染しなかった届出39件、合計44件であった。主なワームの届出件数は以下の通りである。

W32/MSBlaster：15件（うち感染：2件）

CodeRed：12件（うち感染：0件）

W32/Welchia：10件（うち感染：2件）

W32/SQLSlammer：6件（うち感染：1件）

その他（Nimdaなど）：6件（うち感染：0件）

(3) 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。

実際に侵入を受けた64件（昨年：106件）、ワームに感染した5件（昨年6件）、メール中継に係わる問題(弱点)のあった9件（昨年：16件）などの計92件（昨年：151件）を分類すると以下のようになる。

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)が原因となった被害が最も多くなり、古いバージョンの利用やパッチ・必要なプラグインなどの未導入が原因となった被害を上回った。

ID、パスワード管理の不備によると思われるもの：6件

古いバージョンの利用やパッチ・必要なプラグインなどの未導入によるもの：22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：28件

不明：37件

(4) 電算機分類

攻撃や被害の対象となった機器による分類である。

WWWサーバー：43件

メールサーバー：12件

DNSサーバー：1件
FTPサーバー：3件
ファイアウォール：2件
ルータ：6件
Proxyサーバー：1件
その他のサーバー・不明：19件
クライアント：302件

(5) 被害内容分類

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届出件数は126件（昨年：225件）である。

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

メール中継に利用された：9件
サーバーダウン：4件
不正アカウント作成：2件
WWW書き換え：15件
パスワードファイル盗用：4件
サービス低下：9件
オープンプロキシ：1件
ファイルの書き換え：43件
その他：61件

(6) 対策情報

(3)の被害原因分類にもあるように、基本的な(既知の)対策をとっていなかったために被害にあってしまったものが多くなっている。下記ページなどを参照し、今一度状況確認・対処されたい。

「セキュリティ対策セルフチェックシート」
http://www.ipa.go.jp/security/ciadr/checksheet.html
「コンピュータ不正アクセス被害防止対策集」
http://www.ipa.go.jp/security/ciadr/cm01.html

ウイルス対策を含むセキュリティ関係の情報・対策などについては、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/index.html

(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）ここにあげた件数は、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ような数値ではない。

２　JPCERT コーディネーションセンター（JPCERT/CC）に届出があった不正アクセス関連行為の状況について

平成１５年１月１日から１２月３１日の間にJPCERT/CCに届出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および件数

届出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 3,457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 3,224件の報告があった。

[1/1-3/31: 645件、4/1-6/30: 1005件、7/1-9/30: 968件、10/1-12/31: 606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26件の報告があった。

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

ウ　電子メールの送信ヘッダを詐称したメールの配送

電子メールの送信ヘッダを詐称した電子メールの配送について 23件の報告があった。

[1/1-3/31: 6件、4/1-6/30: 6件、7/1-9/30: 7件、10/1-12/31: 4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 24件の報告があった。

[1/1-3/31: 11件、4/1-6/30: 5件、7/1-9/30: 7件、10/1-12/31: 1件]

オ　サーバプログラムの不正中継

電子メール配送プログラムへの電子メールの中継を目的としたアクセス等について 8件の報告があった。

[1/1-3/31: 2件、4/1-6/30: 4件、7/1-9/30: 2件、10/1-12/31: 0件]

カ　その他

コンピュータウィルス、SPAM メールの受信等について 165件の報告があった。
[1/1-3/31: 40件、4/1-6/30: 51件、7/1-9/30: 37件、10/1-12/31: 37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)。

ア 注意喚起

[新規]

TCP 139番ポートへのスキャンの増加に関する注意喚起
Windows RPC の脆弱性を使用するワームに関する注意喚起
135番ポートへのスキャンの増加に関する注意喚起
新たな sendmail の脆弱性に関する注意喚起
Microsoft IIS 5.0 の脆弱性に関する注意喚起
sendmail の脆弱性に関する注意喚起
UDP 1434番ポートへのスキャンの増加に関する注意喚起

イ 活動概要(届出状況等の公表)

発行日:2004-01-21 [2003年10月1日 ～ 2003年12月31日]
発行日:2003-10-17 [2003年7月1日 ～ 2003年9月30日]
発行日:2003-07-17 [2003年4月1日 ～ 2003年6月30日]
発行日:2003-04-17 [2003年1月1日 ～ 2003年3月31日]

ウ 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] 248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。

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のいずれかに係るアクセス制御機能の研究開発に関してとりまとめたものである。具体的には、独立行政法人等による研究や国からの委託研究及び国からの補助事業により実施している研究である。

実施テーマは以下のとおりであり、その研究開発の概要は、別添１のとおりである。

暗号アプリケーションプログラムインターフェース基盤技術に関する研究開発
出所不明のパケット流出を許さないセキュアな情報通信ネットワークに関する研究開発
次世代証拠基盤技術に関する研究開発
情報セキュリティ高度化のためのデータ保護技術に関する研究開発
相互接続時のセキュリティポリシの管理技術に関する研究開発
属性認証を用いたサービスの相互接続技術に関する研究開発
大規模ネットワークセキュリティの確保に向けた研究開発
インターネットアプリケーションのセキュリティ脆弱性に関する研究
ネットワーク侵入検出システム IDA(Intrusion Detection Agent System)の研究開発
アクセス制御機構を有するセキュア WebDAV の開発

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１５年１１月１９日から１２月１９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。その間の応募者は次のとおりであり、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。

RSA セキュリティ株式会社
インターネットセキュリティシステムズ株式会社
株式会社エイシーエス
株式会社 SAP（エス・エイ・ピー）
エヌ・ティ・ティ アイティ株式会社
株式会社 NTT データ
株式会社グローバルフレンドシップ
シーア・インサイト・セキュリティ株式会社
株式会社シーフォーテクノロジー
ジャパン･インフォメーション・テクノロジー株式会社
株式会社セキュアプロバイダ

株式会社ソフテック
大日本印刷株式会社
株式会社ディ・アイ・ディ
株式会社ドリームウェア
日本サイバーサイン株式会社
日本電気株式会社
日本電気システム建設株式会社
ネットエージェント株式会社
株式会社ネットコム
松下電工株式会社
三菱スペース・ソフトウェア株式会社
三菱電機株式会社

(2) 調査

警察庁が平成１５年９月に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、次のとおりであり、それぞれの研究開発の概要は、別添３のとおりである。

アンケート調査は、平成１５年８月１日から平成 15 年８月３１日までの間にインターネット上において検索を行った結果、

・ 現にアクセス制御機能等の情報セキュリティに係る研究開発を実施している旨表示のあった企業・大学

及び

・ 平成１４年１０月１日から平成１５年９月３０日までの間の情報セキュリティに関連する展示会（出展企業５０社以上）に出展する旨表示のあった企業

の中から無作為に抽出した５００団体を対象に実施した。

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）大学

茨城大学
東京電機大学

イ）企業

ELNIS テクノロジーズ株式会社
sonicWALL,Inc　日本オフィス
アナログ・テック株式会社
アルプスシステムインテグレーション株式会社
インタネットセキュリティシステムズ株式会社
株式会社アークン

株式会社アクセンス・テクノロジー
株式会社アニモ
株式会社エイチ・エム・アイ
株式会社コムワース
株式会社セキュアプロバイダ
株式会社ソフテック
株式会社ディアイティ
株式会社ディー・ディー・エス
株式会社ドリームウェア
株式会社パンプキンハウス
株式会社ハンモック
株式会社富士通インフォソフトテクノロジ
株式会社富士通ソーシアルサイエンスラボラトリ
株式会社富士通ビー・エス・シー
株式会社プロトンソフトボード事業部
株式会社ホライズン・デジタル・エンタープライズ
株式会社ライトウェル　LAM 事業部
株式会社ルートレック・ネットワーク
公共情報システム株式会社
ジェイズ・コミュニケーション
セイコープレシジョン株式会社
セキュアコンピューティングジャパン株式会社
ソフォス株式会社
ソラン株式会社
日本電気株式会社第一ソリューション営業事業本部 PID システム営業部
トップレイヤーネットワークスジャパン株式会社
日本エフ・セキュア株式会社
日本キャンドル株式会社
日本サイバーサイン株式会社
ネクサンティス株式会社
富士通関西中部ネットテック株式会社
三菱スペース・ソフトウェア株式会社
矢崎総業株式会社
リコーシステム開発株式会社
ワールドアクセル株式会社

（別添１）

対象技術　侵入検知技術

テーマ名　情報通信危機管理基盤技術の研究開発

開発年度　平成１２年度～１７年度

実施主体　独立行政法人通信総合研究所

背景、目的

我が国の電子政府構想の根幹を揺るがし、我が国経済の将来を背負う電子商取引などを危機的状況に陥れる不正アクセスやサイバーテロに対処するため、ネットワーク上に生じた異変を的確に検出・分析し、対策を提示する先端的要素技術を研究開発する。

研究開発状況（概要）

今後極めて大きな市場が見込める電子商取引等のIT市場の発展を阻害する恐れのある不正アクセスやサイバーテロを未然に防止するため、平成12年度に、総務省通信総合研究所（現独立行政法人通信総合研究所）に、不正アクセス模擬実験装置等を備えたネットワークセキュリティ施設、危機管理用安全対策施設、検証実験用テストフィールド、の3つからなる情報通信危機管理研究施設を整備し、不正アクセス行為やサイバーテロを検証・再現し、対策に関する研究開発を開始した。平成13年度にはこれらの施設を拡充し、不正アクセスを記録・検証する方法、サービス不能攻撃への対処方法、不正アクセス模擬実験装置を実ネットワークに接続し検証する方法、及び電磁波漏洩対策等の研究開発に着手した。

平成14年度には、攻撃に対して自動的にシステム構成切替え被害を最小限にとどめる抗脆弱性クラスタ技術、侵入検知機能とアクセス制御機能との広域連携によるネットワーク保全装置等に、平成15年度には、利用状況やセキュリティポリシにあわせて自動設定可能なアクセス制御装置、持ち込み機器への自動検査及び自動アクセス制御機構等の研究開発に着手した。

詳細の入手方法（関連部署名及びその連絡先）

独立行政法人通信総合研究所　情報通信部門　非常時通信グループ　大野浩之

電話　042-327-5542

将来の方向性

ナショナルセキュリティーや国民経済・生活に対する大きな脅威となっている「サイバーテロ」や大規模不正アクセスに対抗する国家レベルのネットワーク危機管理技術の研究、標準化等を行い、現実のサイバーテロや情報戦争に対応できる技術の獲得を目指す。

対象技術　その他の認証技術

テーマ名　暗号アプリケーションプログラムインターフェース基盤技術に関する研究開発

開発年度　平成 13 年度～平成 15 年度

実施主体　日本電気株式会社（通信・放送機構(TAO)からの委託）

背景、目的

政府・自治体、各企業における申請業務、調達・購買業務の電子化が数年内に本格化する動きにあり、電子文書の真正性や機密性を確保する電子署名技術、暗号化技術の重要性は日々増している。電子政府や電子商取引などのアプリケーションにはプラットフォームフリーの JAVA が採用され始めており、電子文書交換のための標準フォーマットについても XML が定着しつつある。しかしながら、署名･暗号化ライブラリとのインターフェース（暗号 API）は未だ標準化に至らず、各々のアプリケーションが個別に対応しているため、互換性を損なっているのが現状である。

また、XML 文書に対して暗号化を施した文書の格納フォーマット（以下「XML 暗号文書フォーマット」という。）もアプリケーション毎に個別に定義しているため、XML 暗号文書の相互運用性も確保できない。

そこで、電子政府システムや電子商取引システムなどへの適用を想定して XML 暗号文書フォーマットを策定し、JAVA 実行環境における XML 署名・暗号化のための API を実現するとともに電子署名、暗号化処理を実現するアーキテクチャの構築を目的とする研究開発を実施する。

研究開発状況（概要）

・平成 13 年度から以下の研究開発を実施中。

（１） XML 文書に対する署名・暗号インターフェース

（２） Web クライアントのブリッジ機能

・平成 15 年度末に上記研究開発完了予定。

詳細の入手方法（関連部署名及びその連絡先）

通信・放送機構（http://www.shiba.tao.go.jp/）

将来の方向性

上記セキュリティ技術を確保し、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　その他の認証技術

テーマ名　出所不明のパケット流出を許さないセキュアな情報通信ネットワークに関する研究開発

開発年度　平成 13 年度～平成 15 年度

実施主体　株式会社東芝（通信・放送機構（TAO）からの委託）

背景、目的

電子投票など、サーバに多数のコネクションが集中するケースでは、Dos（Denial of Service）攻撃等のサイバー攻撃によってサービスが致命的なダメージを受ける危険性がある。そのため、サーバ自体にコネクションを張る前の段階で、不正な通信を排除することが求められる。

また、不正な通信と正しい通信を判別するためには、利用者認証と機器認証を組み合わせるなどの方法によって、より厳密な認証を実現することが望まれる。

これらの技術の実現によって、不正な通信をより早期に発見、遮断し、ネットワークの不正利用防止と重要システムの保護を可能とする研究開発を実施する。

研究開発状況（概要）

・　平成 13 年度から以下の研究開発を実施中。

（１）　ネットワーク層における段階的な利用者・機器認証を行うプロトコル

（２）　上記プロトコルを用いたポリシベースの各種管理技術

・　平成 15 年度末に上記研究開発完了予定。

詳細の入手方法（関連部署名及びその連絡先）

通信・放送機構（http://www.shiba.tao.go.jp/）

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　その他認証技術

テーマ名　次世代証拠基盤技術に関する研究開発

開発年度　平成 13 年度～平成 15 年度

実施主体　株式会社日立製作所（通信・放送機構（TAO）からの委託）

背景、目的

電子政府の実現には、電子文書の証拠性が必須であるが、電子文書の証拠性確保は電子署名などの暗号技術に依存しており、20～30 年以上の期間にわたって証拠性を確保しない限り、これらの電子文書は補助的にしか扱うことはできない。

また、電子文書の保存のみならずネットワーク上の様々な行為などの証拠性の確保も電子文書の証拠性を長期維持する基盤技術の表現の研究として実施する必要がある。本研究では、以上に対応する技術開発を実施する。

研究開発状況(概要)

- 平成 13 年度から以下の研究開発を実施中。

（１） 電子文書の証拠性を長期にわたって維持する技術

（２） 証拠性保証基盤システム

（３） 証拠性保証システムにおけるネットワークモデル

（４） ヒューマンインターフェース

- 平成 15 年度末までに上記研究開発完了

詳細の入手方法（関連部署名及びその連絡先）

通信・放送機構（http://www.shiba.tao.go.jp/）

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　侵入探知技術

テーマ名　情報セキュリティ高度化のためのデータ保護技術に関する研究開発

開発年度　平成 13 年度～平成 15 年度

実施主体　日本電気株式会社、東京工業高等専門学校、株式会社富士総合研究所、
リコーシステム開発株式会社、東京工業大学、エヌ・ティ・ティ・
コミニュケーションズ株式会社（平成 13 年度まで三菱電機株式会社も参加）
（通信・放送機構（TAO）からの委託）

背景、目的

ネットワーク上の資源は、ネットワーク機器やサーバ・クライアント装置などのハードウェア、ハードウェア上で様々なサービスをネットワーク利用者に提供するアプリケーションなどのソフトウェア、そして利用者のユーザデータに大別できる。ハードウェアとソフトウェアはサイバー攻撃により破壊を受けても入れ替えることで修復することが可能であるが、人間の知的生産の結果であり各ユーザにとって最も重要な資産であるユーザデータは、バックアップがない限り再生することは不可能である。

さらに次世代インターネットプロトコルである Ipv6 では、ユーザは特別の知識なしに情報機器等をネットワークに接続し、その利便性を享受できる反面、グローバルネットワークアドレスの使用により LAN 内に置かれたユーザデータに対するサイバー攻撃の危険性が増加すると考えられる。

以上により、ネットワーク上の存在するユーザデータをどのように守るかが重要な課題となりつつあることから、サイバー攻撃に対して耐性を持つネットワークとして、保存装置等の周辺機器が OS の管理から独立して動作することでデータに対する不正アクセスの防止、データの保存、復旧を図るためのアーキテクチャを研究・開発し、さらにこのアーキテクチャを保存装置以外の周辺機器に応用し、セキュリティ面で高機能な外部装置を開発することを目的とする。

研究開発状況（概要）

- 平成 13 年度から以下の研究開発を実施中。
  （１） データ保護機能を有する電子保存技術
  （２） データ保護機能を有する分散環境自動構築技術
- 平成 15 年度末までに上記研究開発完了予定

詳細の入手方法（関連部署名及びその連絡先）

通信・放送機構（http://www.shiba.tao.go.jp/）

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　その他の認証技術

テーマ名　相互接続時のセキュリティポリシの管理技術に関する研究開発

開発年度　平成 13 年度～平成 15 年度

実施主体　富士通株式会社、九州大学、株式会社富士通プライムソフトテクノロジ
（通信・放送機構（TAO）からの委託）

背景、目的

電子政府や電子商取引など、異なるネットワークのインターネット相互接続ニーズが高まる中、相互接続におけるセキュリティレベルの一貫性の確保が大きな問題として認識されている。この問題への対応として特定のサイトで集中的にセキュリティ管理を行う方法があるが、このような方法は非常に上に大きな負荷の集中を招きやすく、スケーラビリティの問題が指摘されている。また将来的には、パソコンだけでなくすべての携帯電話や PDA（Personal Digital Assistants）などが P2P(Peer to Peer)型のネットワークを構成する可能性もある。このような莫大な数のネットワークの相互接続と将来的な分散ネットワーク環境を念頭に、集中管理型ではなく自律分散型でネットワーク相互間のアクセス制御を実現し、セキュリティレベルの一貫性を確保するセキュリティ管理システムの開発を実施する。

研究開発状況（概要）

- 平成 13 年度から以下の研究開発を実施中。
  （１） 相互接続時のセキュリティポリシ管理技術
  （２） 標準化活動と普及促進

詳細の入手方法（関連部署名及びその連絡先）

通信・放送機構（http://www.shiba.tao.go.jp/）

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　その他の認証技術

テーマ名　属性認証を用いたサービスの相互接続技術に関する研究開発

開発年度　平成 13 年度～平成 15 年度

実施主体　株式会社日立製作所（通信・放送機構（TAO）からの委託）

背景、目的

電子政府、商行為、組織内業務など、将来的には非常に多くの分野で各種の電子申請、取引行為が実施されるものと思われる。このとき、特定の資格を持った人の申請機能や特定の会員・組織に属する人に限ったアクセス制御機能が必要になるが、本研究では、単独のサービス内に閉じた申請ではなく、複数の独立したサービスが連携を取ることによって新たなサービスを提供するという、サービスの相互接続を前提とした電子申請に対応した技術開発を実施する。

研究開発状況（概要）

- 平成 13 年度から以下の研究開発を実施中。
  - （1） 資格証明機能の拡張技術
  - （2） アプリケーション利用時の制御技術
- 平成 15 年度末に上記研究開発完了予定

詳細の入手方法（関連部署名及びその連絡先）

通信・放送機構（http://www.shiba.tao.go.jp/）

将来の方向性

上記セキュリティ技術を確立し、高度情報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　侵入探知技術

テーマ名　大規模ネットワークセキュリティの確保に向けた研究開発

開発年度　平成 14 年度～平成 16 年度

実施主体　松下電工株式会社、工学院大学、安川情報システム株式会社、
NTT アドバンステクノロジ株式会社（通信・放送機構（TAO）からの委託）

背景、目的

最近の不正アクセス数増加等、システム運用・管理に対する脅威が増加するなかで、より安全性・信頼性の高い大規模ネットワークシステムを構築するために、セキュリティの確保が不可欠であり、セキュリティ侵害への対処方法や再発防止などの対策を行うことを可能にするセキュリティ運用の仕組みの研究開発が求められている。

そこで、分散化・階層化された様々なネットワーク機器等の情報（稼動状況、通信のやりとりを記録したデータ、アクセスログ等）の集中的な管理と不正データの発信源調査を基盤とする総合的なセキュリティ運用の仕組みについて研究開発を行う。

研究開発状況（概要）

- 平成 14 年度より以下の研究開発を実施中。

（1） 様々な機器のログを集中的に管理するための仕組みの研究開発

（2） 送信元 IP アドレスを偽装したデータから真の発信元を探査するための発信源探査技術の研究開発

- 平成 16 年度末に開発終了予定。

詳細の入手方法（関連部署名及びその連絡先）

通信・放送機構（http://www.shiba.tao.go.jp/）

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	その他の認証技術
テーマ名	インターネットアプリケーションのセキュリティ脆弱性に関する研究
開発年度	平成１２年度から
実施主体	独立行政法人 産業技術総合研究所 グリッド研究センター

背景、目的

電子政府、電子自治体、ネットバンキング、電子商取引などの様々なサービスが、Web アプリケーションとして構築される動きが急激に拡大しつつある。しかし、Web アプリケーションのアクセス制御機能は、統一された安全規格があるわけでなく、各サイトで個別にその都度設計・実装が行われており、その安全性は、システムの発注者が仕様書に安全基準を正しく盛り込めるか、あるいは受注者が自主的に正しい設計・実装を行うかにかかっている。我々のこれまでの調査で、なりすましアクセスを許してしまう欠陥のあるサイトが実際に数多く運用に供されていた事実が判明している。

こうしたアクセス制御機能の欠陥（セキュリティ脆弱性）の問題は、発注仕様書の作成、システムの開発、納品物の検収に携わる各現場の技術者が、安全なアクセス制御に関する正しい知識を持つ他に解決の道はない。この研究は、実運用サイトに存在した欠陥の原因を分析し、正しい設計・実装のための技術情報を事例に基づいて公表することで、同じ欠陥が繰り返し生産される事態を防止することを目的とする。

研究開発状況（概要）

平成 15 年度の成果：

SSL による暗号化で情報保護をうたっている代表的サイトのうち、cookie を用いたアクセス制御方式を採用している国内の 22 サイトを調査し、アクセス制御用 cookie の非 secure モードでの発行を原因とする欠陥（パケット盗聴によるセッションハイジャック攻撃を許し、その結果として、サイトに登録されている個人情報等の漏えいを招く欠陥）のあるサイトが 20 か所に及ぶことを明らかにした。この問題の原因と解決方法をテクニカルレポートにまとめて出版した。これを受け、経済産業省からこの問題について周知徹底を図るよう関係団体に要請する通知がなされた。

これまでの研究で培ってきた欠陥検査の手法を基に、アクセス制御機能の欠陥を機械的に検出する脆弱性診断ソフトウェアを考案し、特許出願した。

平成 14 年度の成果：

秘密情報を含まない cookie に頼ったアクセス制御方式の欠陥について調査し、国内の 5 つのサイトにおいて、のべ 4 百万～5 百万人分ほどと推定される個人情報が、パスワードなしに誰でもいつでも閲覧可能な状態にあったことを指摘した。これらの事例を基に、この欠陥の原理と解決策を解説する文書を公表した。

政府認証基盤（GPKI）及び地方公共団体組織認証基盤（LGPKI）において、通信路の信頼の

起点となるはずのルート証明書及びそのフィンガープリント（真正性確認情報）が、信頼できない通信路によって配布されており、誤った安全確認手段を国民に習慣づけてしまう危険性があることを指摘した。

平成 13 年度の成果：

クロスサイトスクリプティング脆弱性について調査し、国内の大手サイト 8 か所において個人情報が漏洩する可能性があり、うち 3 サイトではクレジットカード番号も盗まれ得る状態であることを指摘した。また、プライバシーマーク及びオンラインマークの取得事業者から無作為に抽出した 50 サイトと、銀行 22 サイトのうち、約 8 割に同脆弱性が残存していることを確認した。後に、経済産業省からこの問題について周知徹底を図るよう関係団体に要請する通知がなされた。

平成 12 年度の成果：

国内 18 か所の Web メールサービスのうち 7 ヶ所に、URL に含まれるセッション ID が漏洩することが原因でメールの内容を盗み見られる欠陥があることを指摘し、事例に基づく原因の解説を公表したところ、「REFERER 問題」として広く知られることとなり、他のサービスにおいても同様の欠陥が自発的に修正されることとなった。

現在の研究状況：

これまでに発見、分析してきた欠陥パターンを体系化し、安全な Web アプリケーションの構築のために必要な開発手法の整理を進めている。

詳細の入手方法

これまでに公開した論文、資料等は下記の URL より入手できる。

http://SecureIT.gtrc.aist.go.jp/

将来の方向性

Web アプリケーションを含むシステムの発注仕様書で安全基準を指定するのに利用できる、実効的な欠陥防止対策リストの作成。

対象技術　アクセス制御技術

テーマ名　「アクセス制御機構を有するセキュア WebDAV の開発」

開発年度　平成１５年度

実施主体　株式会社 SRA 先端技術研究所（独立行政法人情報処理推進機構(IPA)からの委託）

背景、目的

インターネット上で、遠隔地から協同で文書を作成するための技術である WebDAV は、Web の通信プロトコル標準である HTTP を拡張する技術であり、既に多様なシステムに実装され稼動している。シンプルで特定のサーバーや OS に依存しない仕様であることから、昨今注目されている技術である。

しかしながら、WebDAV の基本仕様にはセキュリティの概念が含まれていない。また、文書ファイルの読込、更新、消去等の操作に関し、許可/不許可などのアクセス制御も提供されていない。これを解消する拡張仕様である WebDAV ACL 機能についても、実装例は少なく、このため、電子政府等、厳密な管理下で文書を取り扱う際に WebDAV を用いるにはそのセキュリティ機能は不足していると言える状況である。

本開発では、ｓWebDAV にロール（役割）ベースのアクセス制御（Role Base Access Control，RBAC）機能を付加することを目的とし、WebDAV プロトコルの一部拡張をはかり、サーバーソフトウェア及びクライアントソフトウェアへの実装を行う。

研究開発状況（概要）

RBAC 及び WebDAV に関する調査検討に基づいて、アーキテクチャ設計、システムの各機能の開発及び実装を行う。2003 年末現在開発を継続中であり、2004 年 3 月の開発完了を予定している。対象のシステムには以下の機能が含まれる。

（１）拡張 WebDAV サーバー

Linux 上で稼動する。WebDAV RBAC クライアントに資源へのアクセス機能を提供する。従来の WebDAV サーバー機能に RBAC 機能を追加するため、RBAC サーバー（後述）と通信可能な Web サーバー（Apache）の拡張モジュールとして実装する。

（２）RBAC サーバー

Linux 上で動作する。拡張 WebdAV サーバーからの資源のアクセス権についての問合せに答えることで、アクセス権に関する管理を行い、その整合性を保つ。

（３）RBAC データベース

Linux 上で動作する。RBAC に関するユーザ、ロール、資源のアクセス権に関するデータを管理する。RBAC サーバーのためのバックエンドデータベースとなる。

（４）WebDAV RBAC クライアント

主に Windows 環境及び Mac OS X 環境で動作する。ユーザ認証及び資源へのアクセスの許諾をサーバーと連携して行う機能を持つ。

（５）WebDAV RBAC 管理ツール

ユーザ、ロールの登録・削除等、資源を管理する者に必要なインタフェース機能をを提供する。

詳細の入手方法

開発完了後 2004 年 5 月に IPA ホームページに関連報告書を掲載する予定。プログラムについても同時期より公開する予定。

将来の方向性

運用マニュアル等と組み合わせて提示し、政府・民間企業におけるセキュアな WebDAV 機能の利用を促進させる。また、W3C、IETF における WebDAV 標準化活動への積極的貢献を図る。更に、オープンソース化をはかり、デファクトとしての利用を目指す。

（別添２）

企業名（及び略称）	RSAセキュリティ株式会社
代表者氏名	山野　修
所在地（郵便番号及び住所）	〒100-0005 千代田区丸の内1-3-1東京銀行協会ビルヂング13F
関連部署名及び電話番号	マーケティング統括本部　03-5222-5240
ＵＲＬ	http://www.rsasecurity.co.jp

対象技術	技術開発状況
その他認証技術 (1985年米国)	【時刻によって変化するパスワードを生成するアルゴリズムとその認証方法】 一定間隔(通常一分)で変化する乱数を、その時点での時刻と秘匿されている番号から一定のアルゴリズムで生成し表示するカード型のデバイスを、認証を希望する利用者側に配備し、利用者は認証希望時にその時表示されている乱数をパスワードとして認証側に送付する。認証側、例えば一般のアプリケーションは送付されたパスワードを別途設置された認証装置に転送して認証の代行を依頼し、その回答により認証の可否を決定する。認証装置は、パスワード受信時の時刻と予め登録されている当該利用者の秘密番号から利用者デバイスと同じアルゴリズムで乱数を生成し、送付されたパスワードの妥当性（一致）を検証し結果を回答する。利用者デバイスと認証装置間の時計の差を補償するため、認証装置では、前回認証時までの累積時間差を記憶し乱数生成時に時刻を調整したり、許容できる範囲の複数の時刻について乱数を生成し、いずれかとの一致を確認して認証を許可するなどの処理を行う。

企業名（及び略称）	RSAセキュリティ株式会社
代表者氏名	山野　修
所在地（郵便番号及び住所）	〒100-0005 千代田区丸の内1-3-1東京銀行協会ビルヂング13F
関連部署名及び電話番号	マーケティング統括本部　03-5222-5240
ＵＲＬ	http://www.rsasecurity.co.jp

対象技術	技術開発状況
その他認証技術 （1997年）	Ｗｅｂアクセス管理技術 ■認証管理 アクセス管理対象のWebリソースにアクセスするユーザを認証。認証方法としてパスワード、X509v3証明書、ワンタイムパスワード等を使用可能。 ■シングル・サイン・オン 一度認証成功したユーザには、認証トークンを発行。認証トークン有効期間内であれば、ユーザは再度認証することなくWebリソースにアクセス可能。またSAML対応により、異なるネットワークドメインのWebサーバへのシングル・サイン・オンにも対応。 ■ルールに基づくアクセス制御 ユーザID、所属グループ、その他任意のユーザ属性に基づいてアクセスルールを定義。ルールに合致したユーザのみWebリソースへのアクセスを許可。

企業名（及び略称）	インターネット セキュリティ システムズ株式会社（ISS）
代表者氏名	林　界宏
所在地（郵便番号及び住所）	〒141-0021　東京都品川区上大崎三丁目1番1号 JR東急目黒ビル
関連部署名及び電話番号	マーケティング部　03－5740－4072
ＵＲＬ	http://www.isskk.co.jp/product/proventia/g_series.html

対象技術	技術開発状況
侵入検知技術 （1997年）	不正侵入防御システム（IPS）は、パケットを分析し、不正アクセス・攻撃・ワームなどを検知し、自動防御を行う。分析は、プロトコル分析／パターンマッチング分析／ビヘイビア分析の組み合わせで行われる。セキュリティの研究機関では、セキュリティホールの発見及びそれに対する攻撃やワームのロジックを自社で研究し、その情報をシステムに反映している。 不正侵入防御システムには、防御ネットワーク型とホスト型（サーバ型とクライアント型）がある。ネットワーク型は、ゲートウェイ、ワームなどの被害を局限化するために、セグメント毎に設置、セキュリティパッチが適用不可能は重要サーバ群の前に設置する。ホスト型は、重要なサーバやクライアントPCなどにインストールし、そのホストに対する不正な兆候をリアルタイムに検出し、防御する。

企業名（及び略称）	株式会社エイシーエス
代表者氏名	大河　克好
所在地（郵便番号及び住所）	〒211-0005　神奈川県川崎市中原区新丸子町９１５－１５ フコク生命ビル４階
関連部署名及び電話番号	044-722-0602
ＵＲＬ	http://www.acs-co.co.jp/

対象技術	技術開発状況
その他認証技術 （2003年）	双方向ワンタイムID・ワンタイムパスワード認証技術 従来の認証システムでは固定のIDと固定のパスワードによるクライアントの認証が一般に行われてきた。これに対し本認証技術では認証の度にパスワードだけでなくIDも変更して認証を行う。これにより経路上では一過性のIDとパスワードしか流れないため盗聴などされても再利用、推測ができずなりすましを防止する。またIDも一過性のものであるため個人を特定することができない。さらにクライアントのみでなくサーバの認証も行うためサーバのなりすましも防止する。 この技術は既に製品化されており、当製品は世界初のワンタイムIDによる認証製品である。 [国際特許出願済み：相互認証方法及び装置並びにこれに用いるワンタイムIDの生成方法、認証方法、認証システム、サーバ、クライアント及びプログラム]

企業名（及び略称）	株式会社 ＳＡＰ （ｴｽ･ｴｲ･ﾋﾟｰ）
代表者氏名	代表取締役 山縣日出人
所在地（郵便番号及び住所）	〒744-0011 山口県下松市大字西豊井１６６３番地
関連部署名及び電話番号	0833-41-9030
ＵＲＬ	http://www.joho-yamaguchi.or.jp/sap/

対象技術	技術開発状況
その他認証技術 （平成15年）	多重変換技術〔国際特許申請中〕（送受信側双方のメールアドレスを当社のサーバ内で多重に変換する）により企業等から変換されたメールアドレスが漏洩しても第三者が使用出来ないため漏洩後の二次被害（迷惑メールやスパムメール、メールアドレスの転売等）の防止に役立つもので、結果として不正アクセス対策に有効。

企業名（及び略称）	エヌ・ティ・ティ　アイティ株式会社
代表者氏名	橋田 幸雄
所在地（郵便番号及び住所）	〒231-0032横浜市中区不老町2-9-1　関内ﾜｲｽﾞﾋﾞﾙ
関連部署名及び電話番号	映像ｺﾐｭﾆｹｰｼｮﾝ事業部　045-651-7514
ＵＲＬ	http://www.ntt-it.co.jp/

対象技術	技術開発状況
その他の認証技術 (2003年)	日本語テキスト検索エンジンを用いた組織内部から外部への電子的情報漏洩防止技術 インターネット上の様々な情報の検索や、社内の電子化された文書の検索のために、日本語フルテキスト検索エンジンInfoBee3がある。基本的な機能は、ユーザが入力したテキストキーワードをもとに、事前処理で作成された検索対象情報のインデックスファイルから 該当するものを抽出するものであるが、これを、組織内部から外部へ、例えばメールなどによって電子的に伝送しようとする場合において、漏洩防止すべき対象となる情報のチェックに用いる。漏洩防止対象となる単位が文書ファイル等である場合は、そのファイル等にアクセス制御を施せばよいが、ファイル等の内容をコピー、もしくは、閲覧することによる手入力で複製された場合、これを電子的に組織外部へ、意図的な場合であれ意図的でない場合であれ、伝送することを防止することはできない。 本技術は、組織内部から外部へ伝送しようとする電子的情報を検索キーワードと看做し、これを予め設定しておいた、防止すべき情報をもとに作成したインデックスファイルを対象に検索し、該当する検索結果が得られた場合、当該伝送を行おうとするユーザに警告を与えることや伝送そのものに強制的禁止措置を与えて、情報漏洩を防止しようとするものである。 関連ホームページ　http://bee.ntt-it.co.jp/index.html

企業名（及び略称）	株式会社エヌ・ティ・ティ・データ
代表者氏名	浜口　友一
所在地（郵便番号及び住所）	〒135-6033　東京都江東区豊洲三丁目三番三号
関連部署名及び電話番号	公共ﾋﾞｼﾞﾈｽ事業本部ﾅｼｮﾅﾙｾｷｭﾘﾃｨﾋﾞｼﾞﾈｽﾕﾆｯﾄ 第一営業担当（担当　藤本）TEL 03-3504-2261
ＵＲＬ	http://www.nttdata.co.jp/

対象技術	技術開発状況
侵入検知技術 H12～H15	【パケット追跡技術】 近年の不正アクセスの手口はますます巧妙になる一方である。攻撃者は、一般的なアクセス追跡手法を掻い潜り、自らの安全を確保するため、不正アクセスをする際には自己を示すアドレス情報を改竄し、詐称していることが多い。しかし、当社が開発した「パケット追跡技術」を用いることで、アドレス情報を使用せずにパケットの特徴的な部分を利用して攻撃者を追跡することが可能である。また、不正アクセス等のネットワーク犯罪の抑止にも効果が期待できる。 【主な技術】 ・IPアドレスを詐称したサイバー攻撃に対して発信元を追跡する技術 ・プライバシーを遵守した発信元の追跡技術 ・リアルタイムに追跡を実施し、NW地図上で可視化する技術

企業名（及び略称）	株式会社エヌ・ティ・ティ・データ
代表者氏名	浜口　友一
所在地（郵便番号及び住所）	〒135-6033　東京都江東区豊洲三丁目三番三号
関連部署名及び電話番号	公共営業推進部　03-3507-4409
ＵＲＬ	http://www.nttdata.co.jp/

対象技術	技術開発状況
侵入検知技術 （平成15年度）	NSA(米国家安全保障局)が開発､GPLライセンスで公開しているSELinux(Security-Enhanced Linux)に下記の拡張を施した。 (1)　カーネル内に実装されたアクセス制御機構(AVC)で複数の「状態」を保持するようにした。 (2)　アクセスポリシーの構文を拡張し、前項で追加した「状態」に基づく処理および状態の遷移を行うイベントを記述できるようにした。（もともとの構文に対しては上位互換性を保持している） (3)　カーネルの「状態」を取得するためのAPIを実装した。 上記拡張により、不正アクセスを受けた場合それをトリガーとして、OS自体が自動的にファイル等システムへのリソースを強化（制限）したり､あるいは提供しているWebコンテンツの範囲を制限できることをプロトタイプシステムにより実証した。 本取組みはOSのセキュリティ強化の一端であるが、アクセスポリシー違反をトリガーとした侵入検知や検知後の対応へ応用が可能である。

企業名（及び略称）	グローバルフレンドシップ株式会社
代表者氏名	保倉　豊
所在地（郵便番号及び住所）	〒160-0004/東京都新宿区四谷４－１３ワークスナカノ２F
関連部署名及び電話番号	代表取締役/０３－５３６６－５４９０
ＵＲＬ	http://www.gfi.co.jp/

対象技術	技術開発状況
その他認証技術	当社では、人類の叡智ともいえる「情報資産をシェアする」つまり、「割符」の概念をデジタル情報に適用できるよう技術開発を進め、自社開発・国産の秘密分散をベースとしたモジュールを世界で最初（1999年9月自社調査）に商用リリースすることができました。「割符」の役割、つまり１、割符を開示することで本人とみなす（認証）２、割符を統合することで原本情報を復元する（原本性・秘匿性）３、当事者同士の合意確認（アクセスコントロール）を、ひとつの基礎技術基盤で対処しています。現在当社は、電子割符を活用しISMS取得の活動を行っております。すでに当社財務会計資料は、電子割符によって運用しておりますが、2004年は、CEOとCFOの了承の下、両当事者の管理する電子割符を開示し、原本情報へのアクセスを制御する。という明確なポリシーの情報資産運用管理システムへの発展も予定です。

企業名（及び略称）	シーア・インサイト・セキュリティ株式会社
代表者氏名	向井　徹
所在地（郵便番号及び住所）	〒108-0073 東京都港区三田3-1-4 中島ビル4F
関連部署名及び電話番号	技術開発部門　03-3451-3335
ＵＲＬ	http://www.seerinsight.co.jp/

対象技術	技術開発状況
侵入検知技術	開発年度　平成14年～平成15年度 ・「ログ情報のリアルタイム監視による侵入検知及び、ログ情報の保護・解析・保管の管理業務とセキュリティ監査を容易にするためのシステム」 情報システムネットワーク全般から発生するログ情報をリアルタイムで監視し、異常検知を行うと共に、ログ情報に対する改竄・削除などの不正行為を防止し、一元管理するための技術を実用化した。本システムは、情報システムネットワークのシステム障害やセキュリティ事故防止、原因究明・再発防止対策を効率的・経済的に実現するものである。また、「情報セキュリティ監査」に必要不可欠となる時刻証明・原本性証明を伴う、「監査ログ」の取得と保管を容易にしたシステムである。
その他認証技術	・「情報システムネットワークへのクライアントPCの接続と個人認証を管理するためのシステム」 クライアントPCからの情報漏えいや正規ユーザの目的外利用を防止する事を目的に、PCの接続管理と個人認証及び、クライアントPCのログ情報（PC利用履歴、業務履歴）の取得～管理を可能にするシステムを開発した。

企業名（及び略称）	株式会社シーフォーテクノロジー
代表者氏名	三住　光男
所在地（郵便番号及び住所）	〒141-0021　東京都品川区上大崎2-13-17目黒東急ビル5階
関連部署名及び電話番号	セキュリティインテグレーション部　03-5447-2551
ＵＲＬ	http://c4t.jp

対象技術	技術開発状況
その他認証技術 開発年：2003年	データをn個の分散情報に符号化し、そのうちk個集めれば元のデータに復元できる(k,n)又は(k,L,n)閾値秘密分散法を用いた認証技術。 従来の認証方式では公開鍵暗号技術を用いるため非常に処理が重く、低スペックな端末上での実現が困難であった。しかし本認証技術では共通鍵暗号レベルの計算力しか必要としないため、さまざま状況での利用が可能である。またパラメータLを導入することにより、データから分散情報へ符号化する際にサイズの最適化が行える。 <相互認証> C/S間で、分散情報を交換することによりワンタイムパスワード形式の相互認証を実現する。この際、通信系路上で分散情報を盗聴した第三者による再利用が発生しても否認することが可能である。<回数制限>事前にC/S双方に複数の分散情報を割り当てることで、認証回数を制限することが可能である。 <合意認証>各エンティティに複数の分散情報を割り当てることで、詳細なアクセスレベル設定が可能な合意認証が実現できる。

企業名（及び略称）	ジャパン・インフォメーション・テクノロジー株式会社（JIT）
代表者氏名	石崎　利和
所在地（郵便番号及び住所）	〒101-0051　東京都千代田区神田神保町3-10-3　松晃ビル５F
関連部署名及び電話番号	03-3511-8971　　info@jit-g.co.jp
ＵＲＬ	http://www.jit-g.co.jp

対象技術	技術開発状況
その他認証技術 開発年 2000年1月～ 2004年12月 合計4年	eCipherGate（イーサイファーゲート） １．対象 ・　大切な顧客、消費者の安全を考える会社むけ ・　ハッカーから貴方の会社を守りたい愛社精神あふれる方むけ ・　インターネットを利用する会社むけ ２．特徴 ・　データベースに対するファイアウォール ・　データベースのセキュリティ ・　利用方法はODBC、JDBCと同じミドルウェア ・　データベースに格納する情報を自動的に暗号化復号化 ・　導入コストは暗号関数の1/3 ３．機能 ・　暗号化、復号化＝データベースの情報を自動的に暗号化、復号化 ・　利用者権限機能＝情報利用者権限を柔軟に設定 ・　検知機能＝不正なアクセスを管理者へ通知 ・　データベース移行＝既存のDBを暗号DBへ変換 ４．動作環境 ・　対象OS ＝ Solaris、AIX、HP/UX、Linux、Windows ・　対象DB ＝ Oracle、DB2、SQL Server、PostgreSQL

企業名（及び略称）	株式会社セキュアプロバイダ
代表者氏名	小川　秀治
所在地（郵便番号及び住所）	〒101-0063 東京都千代田区神田淡路町2-19-1ロイヤルお茶の水205
関連部署名及び電話番号	営業企画部　03-5298-2374
ＵＲＬ	

対象技術	技術開発状況
その他認証技術	◇PassLogic方式によるワンタイムパスワード認証技術 （開発年：1997年） 利用者からのユーザID入力をトリガーとし、利用者のブラウザにＮｘＭの数字が表示された乱数表（チャレンジコード）を送付する。利用者は乱数表から、利用者自身が設定した「抜き出し位置」にある数字を抽出・「変換法則」で変換してパスワード（レスポンスコード）を作成する。特殊な機器を使用せず、ワンタイムパスワードを採用することができる。特許取得済み。 ◇シームレスサインオン （開発年：2002年） 複数サービスのパスワードを統合化し、さらにワンタイムパスワード化を図る認証技術。サービス毎に異なるセキュリティ設定を管理するキーボックスサーバと、認証及びアクセスコントロールを行う認証管理サーバから構成される。パスワード漏洩、パスワード利用不能攻撃、パスワードハッキングなど、パスワードに関するセキュリティリスクに対応することが可能。PCT国際特許出願済み。

企業名（及び略称）	株式会社ソフテック
代表者氏名	加藤　努
所在地（郵便番号及び住所）	〒154-0004　東京都世田谷区太子堂1-12-39 三軒茶屋堀商ビル
関連部署名及び電話番号	技術統括部　03-3412-6008
ＵＲＬ	http://www.softek.co.jp/

対象技術	技術開発状況
その他認証技術 平成14年 ～平成15年	政府が推進するe-Japan重点計画における行政手続きの電子化、インターネットバンキングなどの電子商取引サイトは、Webブラウザからインターネット経由でログインするシステムが多数存在する。しかし実際には、Webアプリケーションにおけるセッション管理機能に潜在的な欠陥を持つシステムが多く、これを悪用した攻撃により個人情報の漏洩や偽の申請・注文などが発生する危険が常に伴う。 こうした被害を未然に防ぐためには、Webアプリケーションにおける欠陥に対する開発・検収段階での事前検査が不可欠である。代表的な検査方法はツールによる検査であるが、現状、セッション管理機能に対する欠陥の検査ツールは存在せず、コストが発生するセキュリティ監査業者が行う検査サービスに委託するしかないことから、十分な検査が行われずに潜在的な欠陥を抱えたまま運用が行われる問題が存在する。 当社では、独立行政法人産業技術研究所グリッド研究センターセキュアプログラミングチーム長の高木浩光氏と共同研究を行い、情報処理振興事業協会の2002年度電子政府情報セキュリティ技術開発事業の1つとして採択された「アクセス制御機構の機能不全を検出・検証するシステム」の成果を製品化（製品名：「WebProbe」）し、2003年12月1日に販売を開始した。 「WebProbe」はログイン（ユーザ認証）機能を伴うWebアプリケーションにおけるセッション管理の欠陥の検査ツールであり、これまで技術的なスキルや手作業による緻密な作業を必要としたセッション管理の欠陥に対する検査を簡単な操作で実現可能にした。

企業名（及び略称）	大日本印刷株式会社
代表者氏名	矢野　義博
所在地（郵便番号及び住所）	〒162-8475　東京都新宿区榎町７番地
関連部署名及び電話番号	アプリケーション開発部　03-3513-2740
ＵＲＬ	http:// www.dnp.co.jp/bf

対象技術	技術開発状況
その他認証技術 開発年：H15年	１．ICカードを用いた802.1×認証（EAP-TLS方式） ICカード内に秘密鍵と電子証明書を格納し、無線LANシステムにおけるセキュリティと利便性の向上を実現。 ２．ICカードを用いたファイル及びフォルダ暗号化 ICカード内に格納された暗号鍵（AES方式）を用いて、暗号及び復号を行う技術。暗号化したフォルダは、ICカード内の暗号鍵を自動判別し、当該フォルダへのアクセス制御も実現。 ３．ICカードを用いた利用制限 ICカードを用いた端末のログイン制御を行う技術。 ４．アプリケーション起動制御 端末におけるソフトウェアの起動を制御する技術。登録されたアプリケーションのみを起動許可します。

企業名（及び略称）	株式会社ディ・アイ・ディ
代表者氏名	林　守澤
所在地（郵便番号及び住所）	〒106-0041　東京都港区麻布台3-3-12WITビル4階
関連部署名及び電話番号	(03)5573-4372
ＵＲＬ	http://www.did2121.com　製品の説明は http://www.did2121.com/network/tracking.htm

対象技術	技術開発状況
侵入探知技術	製作年度-2001年(2003年3月、最新バージョン) Stealth Trackingは“ウェブ基盤の侵入者追跡システム”として中間経由地(Proxy Server)を利用し偽装IPにアクセスする不法侵入者のリアル IPとMACアドレスをリアルタイムに追跡することで、インターネットからの不法侵入者に対する対応方案を提示する。ファイアウォールやIDSなどが設置されていたとしてもネットワークの構造上、80番ポートは常に開放されるため、ここからの侵入に対しては限界があったが、Stealth Trackingは、このようなセキュリティの死角を完全に防御するソルーションとして、大韓民国情報通信部優認証印であるITマークと韓国毎日経済新聞のデジタル技術大賞を獲得した製品である。 特徴及び長所 - クライアントエージェントによる侵入者のReal IPの追跡 : 独自に開発したエージェントロボットによる侵入者のリアルIPアドレスやMACアドレスをリアルタイムに追跡 - 偽装IPアドレスを利用した侵入者の追跡 : Proxyを利用した位置情報の隠匿に対しても実際の侵入者のIPアドレスやMACアドレスを追跡 - パフォーマンスの向上 : ネットワークを通じ入ってくる 全体 パケットに対する点検でなく、特定の攻撃パターンだけを探知、追跡することでパフォーマンス向上 - 不法侵入者の自動分類 : 偽装IPアドレスユーザー及び頻繁なエラーメッセージの発生者に対する自動分類で不法行為者の情報をDB化 - 既存のインターネットサービスとの相互連動 : 別途のインターネットサービスの内容変更なしに、エージェント挿入で Stealth機能を提供 多様なプラットフォームとの相互連動 : Window, Linux, Unix基盤による多様なウェブサーバ(IIS, Apache など)と相互連動 主要供給所 - 大韓民国国家情報院 - 大韓民国 大検察庁 コンピューター捜査課 - 大韓民国警察庁保安課/ソウル地方警察庁サイバー犯罪センター - 大韓民国 国軍合同調査団 - 大韓民国 ホンミョン大学 - 大韓民国 機務司令部 インターネット取引、ポータル会社など

企業名（及び略称）	株式会社ドリームウェア
代表者氏名	田中　光一
所在地（郵便番号及び住所）	〒160-0023 東京都新宿区西新宿8-14-24 西新宿KFビル7F
関連部署名及び電話番号	
ＵＲＬ	http://www.logsaver.jp/

対象技術	技術開発状況
その他認証技術	【背景・目的】 不正アクセス行為の手口は巧妙になる一方で、さらに内部使用者による不正行為も問題視されている。そこで、完全に不正アクセスを防御する事は不可能だということを前提に、今までになかったAfterセキュリティに焦点を。具体的にはログファイル管理に着目した。 【適用技術】 既存にはないPacketWriting方式を適用する事により、発生するログファイル（ログデータ）を、リアルタイムでCD-Rへ記録する事を可能とした。これにより保全性のあるログファイルを管理する事が可能となる。また、その保全性のあるログデータを分析する事により、初めて完全な分析結果を得ることができると考える。

企業名（及び略称）	日本サイバーサイン株式会社
代表者氏名	茶位　利昭
所在地（郵便番号及び住所）	〒105-0003　東京都港区西新橋3-5-8 渡瀬ビル2F
関連部署名及び電話番号	開発部　03-5733-3131
ＵＲＬ	http://www.cybersign.co.jp

対象技術	技術開発状況
その他認証技術	オンラインサイン照合技術を利用した、バイオメトリクス個人認証システムを開発・販売しています。 これは、予め登録されている手書きサインと、新たに描かれた手書きサインとを比較して、登録者本人のサインか否かを照合判定する技術です。サイン照合はネットワーク上のサイン認証サーバ（C-SIGNサーバ）または、ローカルPC上で行われます。照合はサインの形状と、ペンの動きの両方を評価しますが、照合に用いるサインデータは、サインを描く時のペンの動きや筆圧を表す時系列データですので、サインの形のみを評価するのではなく、他人が真似することは困難です。 サイン認証は、使用者の意思が必要なバイオメトリクス認証です、逆に考えると、認証を正しく行ったと言うことで、使用者の意思の確認が可能です。今後この意味が重要になると思います。

企業名（及び略称）	日本電気株式会社
代表者氏名	中村　悦也
所在地（郵便番号及び住所）	〒108-8001　東京都港区芝五丁目７－１
関連部署名及び電話番号	インターネットソフトウェア事業部 セキュリティG 03-3456-6436
ＵＲＬ	http://www.nec.co.jp/press/ja/0305/2003.html http://www.sw.nec.co.jp/solution/network/sec/fire_wall.html http://www.sw.nec.co.jp/middle/caras-vs/ http://www.sw.nec.co.jp/middle/WebSAM/products/GetAccess/ http://www.sw.nec.co.jp/middle/WebSAM/products/IceWall/ http://www.sw.nec.co.jp/middle/WebSAM/products/VLANaccess/vaclt_tokutyou.html

対象技術	技術開発状況
その他認証技術	・ファイアウォール技術に関しまして以下の技術開発状況でございます。 1)CheckPoint社のファイアウォールをエンジンとしてNECのIAサーバをベースとしたFWアプライアンスExpress5800/FWの技術。運用面ではノード管理ツールのESMPRO、可用性を高めるFW二重化技術（2000～）。 2) ステートフルインスペクション，DoS対策機能，ホストIDSなどの機能をNECのIAサーバに実装した独自ファイアウォールアプライアンスExpress5800/SG300a開発の技術（2002～）。 ・侵入検知技術に関しましては以下の技術開発状況でございます。 1) Internet Security Systems(ISS)社セキュリティ監視ツールRealSecureを利用してセキュリティ監視システムを構築するサービス技術（2001～）およびNECのIAサーバに実装した侵入検知アプライアンスExpress5800/RS300a開発の技術（2002～）。 2) サーバに対する振る舞いを監視して、規定外の動作を不正侵入とみなす、未知侵入検知技術（2003～）。 ・その他の認証技術に関しましては以下の技術開発状況でございます。 1) 企業内で公開鍵基盤システムを実現するための 証明書発行局(CA)・登録審査局(RA)の機能を提供するPKIサーバ/Carassuit開発の技術（1999～） 2) GetAccess，IceWallを利用したシングルサインオン開発･構築技術（2001～） 3)ソリトン社のSmartOnとICカード等のトークンを使った情報漏えい対策のデスクトップ認証技術

企業名（及び略称）	日本電気システム建設株式会社
代表者氏名	代表取締役社長　馬場　征彦
所在地（郵便番号及び住所）	〒140-8620　東京都品川区東品川1-39-9
関連部署名及び電話番号	ネットワーク事業本部サービスソリューション事業部 サービス開発部　03-5463-7302
ＵＲＬ	http://www.nesic.co.jp/iplocks/

対象技術	技術開発状況
その他認証技術 2002年開発 2003年機能追加	IPLocks-DSASはデータベースのセキュリティ製品です。 弊社は米国IPLocks社が開発したIPLocks-DSASをアプライアンス販売、カスタマイズ、技術サポート、保守を行います。 本製品は、情報漏えい監視、ユーザー権限の監視、表構造の監視、データ正常性の監視、脆弱性診断といった監視／評価をエージェント・プログラムを用いずIPLocks-DSASをネットワークに接続するだけで実現します。管理、設定はWeb画面より行い、監視項目の設定は簡単な操作だけで設定可能で、すぐに運用が開始できます。運用はアラートをメールで受信し、どのような異常かを確認できます。レポートマネージャーからもアラートを確認できます。 本製品はアプライアンス販売の為、導入に際し面倒なインストール作業等はありません。

企業名（及び略称）	ネットエージェント株式会社
代表者氏名	杉浦　隆幸
所在地（郵便番号及び住所）	東京都墨田区錦糸３－５－８ソアビル７Ｆ
関連部署名及び電話番号	技術室（03-5619-1243）
ＵＲＬ	http://www.netagent.co.jp/

対象技術	技術開発状況
侵入検知技術 (平成12年～平成15年)	ネットワーク傍受および証拠保全技術 ネットワークを流れる通信を全て傍受し傍受した通信の中からサーバ等に侵入されたかを検知し名簿などの重要情報や秘密情報の流出を内容により自動判断できる。侵入者による被害を検知記録できるシステム。 メールや掲示板書き込み、ｗｅｂメール等のデータの内容を判断して、麻薬取引などの違法行為を通信内容から判断し検知することが可能。 傍受する対象をメールアドレスや、ＩＰアドレス、認証ＩＤなどにより絞ることにより、傍受対象者以外のデータを記録しないことが可能。 低いパケットロス率を実現しているため、メールの添付ファイルなどの再現性に優れている。 記録データの電子署名により記録の改竄を防止できる。 関連URL（ http://www.packetblackhole.com/ ）

企業名（及び略称）	株式会社ネットコム
代表者氏名	三部　哲雄
所在地（郵便番号及び住所）	〒213-0012　神奈川県川崎市高津区坂戸3-2-1　KSP西4階418
関連部署名及び電話番号	経営企画部　　陳　海波　　張　書明　　044-813-3868
ＵＲＬ	http://www.netcome.co.jp/

対象技術	技術開発状況
侵入検知技術	E-mail改ざん防止技術「E-mail　Guard」 Mailからの情報漏えい・改ざんなどが増加する現在、E-mailで取引される重要機密を改ざんされるのを抑え、被害を最小限度に抑える。 1.E-mailのファイルまで全て暗号化・認証・電子署名を行うことで、万が一侵入されてもファイルが解読されるのを防ぐ。 2.また、受信時に認証等を確認することでファイルに改ざんが加えられているかどうかを判断できる。 今回使用している基礎技術はカオス理論暗号の最先端Cobra暗号であり、操作に関しても38種のメーラに対応している。また、公開鍵の自動登録、自動送付、自動管理も可能にしており、鍵の書き換えも可能である。 また、携帯電話にも組み込み利用可能。

企業名（及び略称）	松下電工株式会社
代表者氏名	畑中　浩一
所在地（郵便番号及び住所）	〒571-8686　大阪府門真市大字門真１０４８
関連部署名及び電話番号	新事業企画室　ネットワークセキュリティ事業推進グループ 06-6906-6384
ＵＲＬ	http://www.nais-netcocoon.com

対象技術	技術開発状況
その他認証技術等 2003年	米国Ecutel Systems社のモバイルVPNソフトウェア「Viatores」をベースに，ICカードとディレクトリサービスとを連携させた認証技術。運用の容易さと利便性とを両立させ，アプリサーバへの経路で認証と暗号通信を可能にする。 【処理手順】 ①ICカードにネットワーク情報，認証情報を格納　②ICカードを挿入，PIN入力で起動し，決められた認証サーバへ接続　③ディレクトリサービス連携して認証，その後すべての通信を暗号化 【特 長】 ①情報を個人認証・暗号通信・アクセス制御でトリプルガード ②IPレベルでアクセス制御（フィルタリング）が可能 ③セキュリティレベルの異なるネットワークを仮想的に分離可能 すでに、京都府宇治市のネットワークに納入済み。

企業名（及び略称）	三菱スペース・ソフトウエア株式会社
代表者氏名	三宅　道昭
所在地（郵便番号及び住所）	〒105-6132　東京都港区浜松町2-4-1 （世界貿易センタービル32階）
関連部署名及び電話番号	事業推進部　03-3435-4737
ＵＲＬ	http://www.mss.co.jp/

対象技術	技術開発状況
その他 (ネットワーク通信パケット記録・解析技術) 開発年：2002年	計算機に対する不正アクセス(外部からの攻撃、内部からの情報漏えい等)の可能性に対する捜査と証拠を示すことをComputer Forensicといい、これを可能にするシステムをForensic Systemといいます。不正アクセスのうち、ネットワークを経由して行われるものについて、ネットワーク上の通信の全てを記録し、不正アクセスの証拠を示すためのシステムを開発しました。従来のログベースでの記録では十分な証拠性を示すことができませんでしたが、本システムによれば、十分な証拠を示すことが可能になります。具体的には、IPに準拠するネットワーク通信パケットを記録し、プロトコル種別に分類・解析・復元することを基本機能とし、以下の用途への技術応用されている。いわゆるフォレンジック（証拠保管）サーバ技術を開発した。 (1) SMTP、POP3、HTTP、FTP　記録・解析 (2) (1)項記載プロトコル含むTCP/IPプロトコルの記録・保存 (3) SMTP（メール）に特化した通信記録・解析（メールを利用した通信傍受法対応） (4) SMTP（メール）の通信経路情報の記録・解析による迷惑メール等対策技術応用 記録した通信パケット・データを他のパケット解析ソフトウェアを利用した解析分離可能

企業名（及び略称）	三菱電機株式会社
代表者氏名	執行役社長　野間口　有
所在地（郵便番号及び住所）	〒100-8310　東京都千代田区丸の内２－２－３
関連部署名及び電話番号	社会情報システム事業部　セキュリティシステム部 03-3218-2339
ＵＲＬ	http://www.mitsubishielectric.co.jp/ids

対象技術	技術開発状況
侵入検知技術 (1999年～)	不正アクセスを検知し、ルータ制御などによる防御を行うネットワーク型の侵入検知システム（IDS）を製品開発しています。 技術開発項目は以下のとおりです。 ・専用OSファームウェアによる侵入検知ボード ・侵入検知ボードによる不正検出、異常検出 ・独自の基本ソフトウェアによる分析エンジン ・シグネチャの更新をリモートで行うエージェント機能 ・ギガビットネットワーク対応 ・攻撃パケットを自動的にフィルタリングする機能 ・攻撃パケットをおとり装置へ誘導する機能 ・攻撃パケットの発信元を追跡する機能

（別添３）
【大学】

大学名	茨城大学
所在地（郵便番号及び住所）	〒316-8511 日立市中成沢町4-12-1
関連部署名及び電話番号	工学部黒澤研究室　0294-38-5135
ＵＲＬ	http://crypt.cis.ibaraki.ac.jp/omac/omac.html

対象技術	技術開発状況
認証	メッセージ認証コードを利用すると送信したメッセージ、あるいは大切に保存してあるデータの改ざん、偽造を防ぐことができます。任意の長さのメッセージに対応できる従来の方式は、鍵が3つ必要でした。これに対し提案するOMACは鍵が1つで済みます。また、その安全性も数学的に証明されています。提案方式は、米国政府（NIST）が推奨方式にするつもりであるとアナウンスしています。 詳しくはNISTのホームページhttp://csrc.nist.gov/CryptoToolkit/modes/を見て下さい。

企業名（及び略称）	東京電機大学
所在地（郵便番号及び住所）	〒270-1382 千葉県印西市武西学園台2-1200
関連部署名及び電話番号	情報環境学部　0476-46-8442
ＵＲＬ	http://www.dendai.ac.jp

対象技術	技術開発状況
暗号技術	鍵を公開するマスターキーシステムは乱数サーバを用いて、認証つき通信を行います。正しい鍵の所有者間のみが成立するので、なりすまし攻撃、中間一致攻撃が排除できます。秘密分散を用いると、鍵の不正使用が検出できます。この方式をOS内部の命令にも適用すれば、原理的にはウィルスやワームも検出でき、その活動も制圧出来ます。この方式は他の方式を排除しません（併用できます）。

企業名（及び略称）	東京電機大学
所在地（郵便番号及び住所）	〒270-1382 千葉県印西市武西学園台2-1200
関連部署名及び電話番号	情報環境学部　0476-46-8442
ＵＲＬ	http://www.dendai.ac.jp

対象技術	技術開発状況
暗号技術	ネットワークセキュリティ環境構築に関わる製品・システムの情報（メーカ、製品名、機能など）をWEBで提供する。

【企業】

企業名（及び略称）	ELNISテクノロジーズ株式会社
所在地（郵便番号及び住所）	〒101-0024 千代田区神田和泉町1
関連部署名及び電話番号	営業部　03-5821-5914
ＵＲＬ	http://www.elnis.com

対象技術	技術開発状況
ネットワークセキュリティ	CyberGuard Firewallは、専用OS上で動作させることで、ファイアウォールの土台から保護し、安全性を高めたファイアウォール。

企業名（及び略称）	ELNISテクノロジーズ株式会社
所在地（郵便番号及び住所）	〒101-0024 千代田区神田和泉町1
関連部署名及び電話番号	営業部　03-5821-5914
ＵＲＬ	http://www.elnis.com

対象技術	技術開発状況
ネットワークセキュリティ	ELNIS Security Wallは、Stonesoft社のファイアウォールソフトウェアStoneGateを高性能サーバにプリインストールしたアプライアンス形式として提供する。運用開始までに煩雑な手間が不要で、ハードウェア故障時のオンサイト交換復旧サービスも提供。購入後すぐに信頼性のあるネットワークが構築できる。新しい分散アーキテクチャを採用することで従来にない高い信頼性を実現したのがELNIS Security Wall。ファイアウォール機能を「ファイアウォールエンジン」「マネジメントサーバ」「ログサーバ」の3つの独立した部分に分割することで、それぞれの処理機能をコンパクト化し、高い処理能力と信頼性を実現している。

企業名（及び略称）	ELNISテクノロジーズ株式会社
代表者氏名	鈴木　伸秀
所在地（郵便番号及び住所）	〒101-0024 千代田区神田和泉町1
関連部署名及び電話番号	営業部　03-5821-5914
ＵＲＬ	http://www.elnis.com

対象技術	技術開発状況
ネットワークセキュリティ	個人レベルでは利用の徹底が難しかったパーソナルファイアウォールを、組織レベルで管理･徹底できるため、統一されたセキュリティポリシーの下で、企業の全PCのセキュリティを確保することができる。

企業名（及び略称）	ELNISテクノロジーズ株式会社
代表者氏名	鈴木　伸秀
所在地（郵便番号及び住所）	〒101-0024 千代田区神田和泉町1
関連部署名及び電話番号	営業部　03-5821-5914
ＵＲＬ　http://www.elnis.com	

対象技術	技術開発状況
セキュリティマネジメント	セキュリティフライデー社のVISUACT(TM)とSymantec Intruder Alert3.5.1Jを連携させることで、Windowsネットワーク環境下において、従来不可能だった不審なアクセス行為の即時検出と、詳細な証跡管理ができるようにした。内部ネットワークにおける不正行為の抑制、情報漏洩の未然防止に効果的。

企業名（及び略称）	ELNISテクノロジーズ株式会社
所在地（郵便番号及び住所）	〒101-0024 千代田区神田和泉町1
関連部署名及び電話番号	営業部　03-5821-5914
ＵＲＬ　http://www.elnis.com	

対象技術	技術開発状況
セキュリティサービス関連	当社の認証システムコンサルティングは、実績をベースに、ネットワークから見たシステムを情報セキュリティ管理システム(ISMS)を表裏一体化したISMSの確立、メンテナンス、改ざんのセキュリティ管理サイクルの構築支援と、認証取得を支援する。

企業名（及び略称）	ELNISテクノロジーズ株式会社
所在地（郵便番号及び住所）	〒101-0024 千代田区神田和泉町1
関連部署名及び電話番号	営業部　03-5821-5914
ＵＲＬ　http://www.elnis.com	

対象技術	技術開発状況
セキュリティサービス関連	検査対象のマシン上でダウンロードした検査プログラムを実行、生成された検査結果を、指定のメール窓口まで返信。数日後、この検査結果に対する詳細レポートを提出する。

企業名（及び略称）	sonicWALL,Inc　日本オフィス
所在地（郵便番号及び住所）	〒107-0052 港区赤坂1-8-6　赤坂HKNビル7F
関連部署名及び電話番号	03-5573-4701(代)
URL	http://www.sonicwall.co.jp/
対象技術	技術開発状況
ネットワークセキュリティ	今後より高度化されるインターネットをサポートすべく2003年度よりハードウェア・プラットフォームの一新を行ない、より高機能なトータル・セキュリティ・アプライアンスを市場に導入予定。

企業名（及び略称）	アナログ・テック株式会社
所在地（郵便番号及び住所）	〒102-0074 千代田区九段南2-3-10
関連部署名及び電話番号	IT営業部　03-3265-2801
URL	http://www.analogtech.co.jp
対象技術	技術開発状況
ネットワークセキュリティ	USB Keyを用いてPC内のフォルダ／ファイルを暗号化できる。PKI方式により暗号化したファイルへのアクセス権を簡単に付与／削除ができる。また、各ドライブ(FD、CD-R、リムーバブルディスク)をロックして使用不可にできる。Webサイトにアクセスする際に必要とするユーザID、ログインパスワードをUSB Keyに格納する。

企業名（及び略称）	アルプスシステムインテグレーション株式会社
所在地（郵便番号及び住所）	〒145-0067 大田区雪谷大塚町1-7
関連部署名及び電話番号	システム商品部　03-5499-8045
URL	http://www.alsi.co.jp
対象技術	技術開発状況
ネットワークセキュリティ	日本語を中心に世界のURL約1700万ページを40のカテゴリーに分類してサーバ（GATEWAY）上でフィルタリングするURLフィルタリングソフトを開発構築し規制データベースを提供するサービスを行なっている。

企業名（及び略称）　　インターネットセキュリティシステムズ株式会社	
所在地（郵便番号及び住所）〒141-0021 品川区上大崎3-1-1　JR東急目黒ビル	
関連部署名及び電話番号　　マーケティング部　03-5740-4072	
URL　http://www.isskk.co.jp	
対象技術	技術開発状況
不正侵入対策	Real Secure、Network Sensorはソフトウェアの分野においては世界で44%、日本で68%のマーケットシェアを持っている製品。その機能はITセキュリティ業界最大のセキュリティ調査機関であるX-Forceのナレッジをベースとする。最高1.2Gまでのトラフィックを不正侵入から防御することが可能。

企業名（及び略称）　　インターネットセキュリティシステムズ株式会社	
所在地（郵便番号及び住所）〒141-0021 品川区上大崎3-1-1　JR東急目黒ビル	
関連部署名及び電話番号　　マーケティング部　03-5740-4072	
URL　http://www.isskk.co.jp	
対象技術	技術開発状況
セキュリティサービス関連	世界6ヵ所で展開しているセキュリティオペレーションセンターの情報を統合しインターネット上で発生している事象を全世界レベルで監視し、それらの情報と弊社X-Forceの脆弱点の情報をもとに、FWとIDSの監視、防御サービスを提供。

企業名（及び略称）　　株式会社アークン	
所在地（郵便番号及び住所）〒101-0041 千代田区神田須田町2-17-3　神田I.N.ビル6F	
関連部署名及び電話番号　　プロダクト事業本部　03-5294-6065	
URL　http://www.ahkun.jp	
対象技術	技術開発状況
ウイルス対策ツール	キーロガー、RATなどのハッカーツールやスパイウェア、アドウェアなどの不正プログラムを包括的に検知、駆除するツール「ペストパトロール」はすでに製品化されているがWindows PC上でのみ動作する。各種のサーバ、ゲートウェイ上で動作させるための開発を進めている。また他のアプリケーションとの連携をするための開発kitの開発も進めている。

企業名（及び略称）	株式会社アクセンス・テクノロジー
所在地（郵便番号及び住所）	〒162-0825 東京都新宿区神楽坂6-38　神楽坂中島ビル
関連部署名及び電話番号	03-5206-7740
URL	http://accense.com

対象技術	技術開発状況
ネットワークセキュリティ	RADIUSは、ネットワーク利用者の認証とアカウンティングを一元的に行なうプロトコルで近年ダイヤルアップ以外の接続サービス、例えば無線LANなどにおいても広く利用されるようになったプロトコルです。アクセンス・テクノロジーの「fullflex」シリーズはインターネット標準RFCに基づいて開発したRADIUSサーバソフトウェアであり、実績・品質・サポートすべての面で高い信頼性を実現している。

企業名（及び略称）	株式会社アニモ
所在地（郵便番号及び住所）	〒231-0015 横浜市中区尾上町2-27　朝日生命横浜関内ビル
関連部署名及び電話番号	VSS営業部　045-663-8640
URL	http://www.animo.co.jp

対象技術	技術開発状況
認証	音声による本人認証を実現した音声認証・識別エンジンです。本製品は、フリーワード方式を提供しています。10秒程度の発話により、認証・識別を行なう、電話サービス等での自然な会話の中で本人確認を実現可能、言語非依存などの特徴をもつ。

企業名（及び略称）	株式会社エイチ・エム・アイ
所在地（郵便番号及び住所）	〒550-0014 大阪市西区北堀江1-5-2　四ツ橋興産ビル11F
関連部署名及び電話番号	営業部　06-6110-2552
URL	http://www.hmi-jp.com

対象技術	技術開発状況
認証	真性乱数生成器を内蔵したUSBトークンを利用したユーザ認証及びファイル暗号ソフトウェア。PCの起動制御、USBトークンの抜き差しによるPCのロック、ファイル、フォルダ毎の暗号化、デバイス制御、ログ管理等クライアントPCのセキュリティ機能がある。

企業名（及び略称）　　株式会社コムワース	
所在地（郵便番号及び住所）〒143-0026 大田区西馬込2-35-7	
関連部署名及び電話番号　　通信機器営業部　03-3777-0888	
URL　http://www.comworth.co.jp	
対象技術	技術開発状況
セキュリティマネジメント	ネットワーク上に流れる全パケットをHDDにて取得可能。1 Gbps（全二重）におけるラインレートキャプチャ（64Byte）に対応可能となるため大容量のキャプチャバッファを持ったプロトコルアナライザとしても使用可能。

企業名（及び略称）　　株式会社セキュアプロバイダ	
所在地（郵便番号及び住所）〒101-0063 千代田区淡路町2-19-1　ロイヤルお茶の水205	
関連部署名及び電話番号　　営業企画部　03-5298-2374	
URL　http://www.s-provider.co.jp/	
対象技術	技術開発状況
認証	利用者側に特別なソフトウェアやハードウェアが不要。標準的な認証プロトコルである「RADIUS」に対応しているので、ソフトウェア開発が不要です。イントラネット・エクストラネット、またインターネットカフェや出張先など、いろんな環境からでも安心して利用できるように高度なセキュリティを実現。特に、特許技術（一部申請中）により、パスワード漏洩、パスワード利用不能攻撃パスワードハッキングなど、パスワードに関するセキュリティリスクに対応することが可能。

企業名（及び略称）　　株式会社セキュアプロバイダ	
所在地（郵便番号及び住所）〒101-0063 千代田区淡路町2-19-1　ロイヤルお茶の水205	
関連部署名及び電話番号　　営業企画部　03-5298-2374	
URL　http://www.s-provider.co.jp/	
対象技術	技術開発状況
認証	IPアドレスレベルでアクセス制限することが可能な遮断型のファイアウォール。ユーザ名とIPアドレスおよび使用中のポートを結びつけることが可能なため、対応するモジュールを外部wwwに導入することでwwwサーバに対して、クッキーを用いることなく詳細なアクセスコントロールが可能であり「個人認証→IPアドレス認証」としてシングルサインを実現することも可能。

企業名（及び略称）　株式会社ソフテック	
所在地（郵便番号及び住所）〒154-0004 世田谷区太子堂1-12-39　三軒茶屋堀商ビル5F	
関連部署名及び電話番号　営業部　03-3412-6008	
URL　http://www.softek.co.jp/	
対象技術	技術開発状況
セキュリティサービス関連	アクセス制御機構の機能不全を検出・検証するシステム（webのセッションIDの欠陥を自動検出、検証するシステム）。本ツールにはIPAセキュリティセンターの「情報セキュリティ関連の調査･開発に関する公募」で採択された技術開発テーマの研究開発結果をシステム化した製品である。本ツールのアーキテクチャはシンプルでユーザと監査の対象となるwebサイトとの間にてプロキシとして動作し､ユーザがアクセスした際の通信内容を分析することで「アクセス制御周りの欠陥の推定／検査を行なう」監査ツールに位置付けられる。

企業名（及び略称）　株式会社ディアイティ	
所在地（郵便番号及び住所）〒136-0075 東京都江東区新砂1-6-35　Nビル東陽町5階	
関連部署名及び電話番号　製品事業本部マーケティングユニット　03-5634-7651	
URL　http://www.dit.co.jp	
対象技術	技術開発状況
認証	強固なPKIを容易に構築・管理するソリューション。

企業名（及び略称）　株式会社ディアイティ	
所在地（郵便番号及び住所）〒136-0075 東京都江東区新砂1-6-35　Nビル東陽町5階	
関連部署名及び電話番号　製品事業本部マーケティングユニット　03-5634-7651	
URL　http://www.dit.co.jp	
対象技術	技術開発状況
ネットワークセキュリティ	セキュアシェルにより、VPN相当の認証、鍵管理、暗号処理するアプライアンスサーバとクライアントソフトウェアのソリューション。クライアントの操作をより簡単にし、使いやすくなっている。アプリケーションレイヤで動作するため､WindowsOSのアップデートや通信環境の変化に影響を受けない高い可用性を持つソリューション。

企業名（及び略称）	株式会社ディアイティ
所在地（郵便番号及び住所）	〒136-0075 東京都江東区新砂1-6-35　Nビル東陽町5階
関連部署名及び電話番号	製品事業本部マーケティングユニット　03-5634-7651
URL　http://www.dit.co.jp	
対象技術	技術開発状況
ネットワークセキュリティ	Webサーバーの前に設置し、リバースプロキシとして動作します。http及びhttpsの通信を文字列単位でチェックし、正常な通信のみをWebサーバーへ通します。・Webサービスの不正操作、パラメータの不正操作 ・cookie値の不正な操作、クロスサイトスクリプティング Webインフラストラクチャの脆弱性、バッファオーバフロー攻撃、データベースへの攻撃などの脅威から防御するサーバソリューション。

企業名（及び略称）	株式会社ディアイティ
所在地（郵便番号及び住所）	〒136-0075 東京都江東区新砂1-6-35　Nビル東陽町5階
関連部署名及び電話番号	製品事業本部マーケティングユニット　03-5634-7651
URL　http://www.dit.co.jp	
対象技術	技術開発状況
ネットワークセキュリティ	セキュアシェル（SecSH）サーバ／クライアント ソフトウェアの商用版。ワンタイムパスワード、PKIによるサーバ認証、ユーザ認証などを可能にする。暗号、認証のライブライを内部に持ち、動的リンクされるライブラリの脆弱性の影響を受けない。

企業名（及び略称）	株式会社ディアイティ
所在地（郵便番号及び住所）	〒136-0075 東京都江東区新砂1-6-35　Nビル東陽町5階
関連部署名及び電話番号	製品事業本部マーケティングユニット　03-5634-7651
URL　http://www.dit.co.jp	
対象技術	技術開発状況
不正侵入対策	DDSは管理下にあるネットワークに対する攻撃をIDSで検知し、自動でハニーポットに誘い込み閉じ込めることができる。DDSはSymantec ManHunt、Symantec DecoyServer、アプリケーションスイッチ、DDSモジュールよりなるソリューション。

企業名（及び略称）	株式会社ディアイティ
所在地（郵便番号及び住所）	〒136-0075 東京都江東区新砂1-6-35　Nビル東陽町5階
関連部署名及び電話番号	製品事業本部マーケティングユニット　03-5634-7651
URL　http://www.dit.co.jp	
対象技術	技術開発状況
セキュリティマネジメント	現在、世の中に出ている脆弱性検査スキャナの多くは、DNSサーバやルータなどの既製品を対象とした、いわゆる“ネットワーク”レベルの検査スキャナである。昨今流行しているクロスサイトスクリプティング脆弱性やSQLインジェクションといった攻撃は、アプリケーションレベルで行われるため、従来のネットワークスキャナでは検出することは難しい。Kavado社のWebアプリケーションスキャナであるScanDoはWebアプリケーションの構造を隅々まで詳しく調査した上で、アプリケーションレベルで起こり得る様々な脆弱性を検査する。

企業名（及び略称）	株式会社ディアイティ
所在地（郵便番号及び住所）	〒136-0075 東京都江東区新砂1-6-35　Nビル東陽町5階
関連部署名及び電話番号	製品事業本部マーケティングユニット　03-5634-7651
URL　http://www.dit.co.jp	
対象技術	技術開発状況
セキュリティマネジメント	エージェント型のシステム構成の管理ツール。ESMはポリシーに基づくセキュリティ管理を企業規模で行うためのソリューションを提供します。システムのセキュリティを維持・管理するために、アクセス制御やパスワード、パッチの適用、ユーザアカウント管理、バックアップ、レジストリ、各種パラメータに関するルールを取り決めて運用していく必要があります。マルチプラットフォーム環境におけるポリシーの保守状況を効率よく自動的に監査することが可能になります。DMSや個人情報保護コンプライアンスプログラム等と併用可能。

企業名（及び略称）	株式会社ディー・ディー・エス
所在地（郵便番号及び住所）	〒454-0012 名古屋市中川区尾頭橋4丁目13番7号-2F
関連部署名及び電話番号	営業課　052-323-3011
URL　http://www.dds.co.jp	
対象技術	技術開発状況
認証	指紋認証装置。以前からの方式とは全く違う方式の採用により処理能力の劣るマイコンでも簡単に動く装置を開発。これにより携帯電話をはじめPDAなどセキュリティを必要とする機器の組み込みが容易となった。

企業名（及び略称）　株式会社ドリームウェア	
所在地（郵便番号及び住所）〒160-0023 新宿区西新宿8-14-24　西新宿KFビル7F	
関連部署名及び電話番号　03-5337-3301	
URL　http://www.dreamware.jp/	
対象技術	技術開発状況
不正侵入対策	各種ネットワーク接続機器より発生するログデータを記録･管理するためのバックアップ装置。情報セキュリティを考える上でログファイルの管理は欠かせない。発生するログデータをリアルタイムで書換可能なメディア（CD-R）へ記録するため、第三者により改ざん、削除される心配がない、信頼性の高いログファイルを保存することが可能。また、独自の圧縮技術により、1枚のCD-Rに大量のログデータを記録できる。

企業名（及び略称）　株式会社パンプキンハウス	
所在地（郵便番号及び住所）〒102-0083 千代田区麹町5丁目5番地　共立麹町ビル1F	
関連部署名及び電話番号　営業部　03-3511-3580	
URL　http://www.pumpkin.co.jp	
対象技術	技術開発状況
暗号技術	あらゆる種類のデータを自動的に暗号化。暗号化されたデータの階層やグループによる共有化。鍵の一元管理などの特徴を持つ。

企業名（及び略称）　株式会社ハンモック	
所在地（郵便番号及び住所）〒169-0075 新宿区高田馬場2-14-5　サンエスビル4F	
関連部署名及び電話番号　製品開発部　03-5287-5661	
URL　http://www.hammock.jp/	
対象技術	技術開発状況
セキュリティマネジメント	企業内でインターネット利用が進むにつれ、私的利用や有害サイトへのアクセスはもちろんのこと、その結果によるトラフィックの増加などの新たな問題を生じている。SurtWatcherは従業員のインターネットアクセスを監視、分析し、最適なアクセス管理を実現するツールである。SurtWatcherの特徴：・インターネットアクセスのログ監視、分析に特化・部署ごとの監視、分析が可能・簡単な操作と多彩な機能の両立を実現・プロクシー／ファイアウォールなどの設定変更が不要。

企業名（及び略称）	株式会社富士通インフォソフトテクノロジ
所在地（郵便番号及び住所）	〒422-8572 静岡市南町18-1　サウスポット静岡12F
関連部署名及び電話番号	インターネットビジネス部　054-203-0225
URL	http://www.ist.fujitsu.com/

対象技術	技術開発状況
セキュリティマネジメント	チェックポイント社の小型ファイアウォール機器であるS-boxをリモートで管理するサービス。

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
所在地（郵便番号及び住所）	〒211-0063 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	人事総務部　044-739-1511(代)
URL	http://www.ssl.fujitsu.com/products/network/netproducts/safemng/index.html

対象技術	技術開発状況
セキュリティマネジメント	「Safe Manager」は、ウィルス検知および駆除ソフトの最新のウィルスパターン定義ファイルへの更新、セキュリティパッチへの対応、ウィルススキャンの定期的な実施など、社内パソコンのウィルス対策実施状況が一目で把握でき、対応が遅れているパソコン利用者には、メールで対応を促すなど、セキュリティ管理者に負担をかけることなく、ウィルス対策を素早く、確実に全社に徹底することができる。さらに、各々のパソコンへのソフトウェアのインストール状況など、資産管理が容易に行なえるため、セキュリティの管理対象を明確に把握できる。

企業名（及び略称）	株式会社富士通ビー・エス・シー
所在地（郵便番号及び住所）	〒141-8581 品川区大崎1-11-2　ゲートシティ大崎イーストタワー11F
関連部署名及び電話番号	ソリューション営業本部第二ソリューション営業統括部 第三ソリューション営業部　03-5740-3231
URL	http://www.bsc.fujitsu.com/

対象技術	技術開発状況
暗号技術	基本的にはファイル暗号を行なうクライアントアプリケーションである。特徴：自動暗号；対象のフォルダドライブ、ネットワークドライブに保存されたファイルを自動的に暗号化、復号できる　圧縮暗号；複数のファイルやフォルダを1つの圧縮された暗号ファイルにできる。

企業名（及び略称）　株式会社プロトン	
所在地（郵便番号及び住所）〒169-0073 新宿区百人町1-22-17	
関連部署名及び電話番号　ソフトボード事業部　営業部営業課　03-5337-6430	
URL　http://www.proton.co.jp	
対象技術	技術開発状況
セキュリティマネジメント	小規模サイトのログファイルからサービスプロバイダのような大きなサイズのログファイルまで高速に処理可能なwebアクセス分析ツール。

企業名（及び略称）　株式会社ホライズン･デジタル･エンタープライズ	
所在地（郵便番号及び住所）〒150-0047 渋谷区神山町16-2	
関連部署名及び電話番号　マーケティング部　03-5738-5410	
URL　http://www.hde.co.jp/	
対象技術	技術開発状況
ウイルス対策ツール	HDE Anti-Virusはウィルスの侵入を防ぐための製品。サーバ内のチェックをゲートウェイとしてのチェックの2種類の検査ラインがある。HDE Mail Filterは内部から外部への情報漏洩をメールのゲートウェイで監視し、防ぐ製品。スパムメールのフィルターも可能。

企業名（及び略称）　株式会社ライトウェル	
所在地（郵便番号及び住所）〒110-0005 台東区上野1-20-10　上野風月堂本店ビル7F	
関連部署名及び電話番号　LAM事業部営業グループ　03-5817-3242	
URL　http://www.itLAM.com	
対象技術	技術開発状況
セキュリティマネジメント	クライアントPCのインベントリ及びプロセス情報を日々把握することにより、OS、アプリケーション等のパッチレベルでのバージョンチェック、またウィルス対策ソフトの稼動及び更新チェックを行なうことにより、外部からの脅威に対する対策に効果を発揮する。特徴としては詳細なインベントリ情報の自動取得はもとより、クライアントへのインストール作業を必要とせず、また非常勤のため、導入／展開が容易でクライアントPC及びネットワークへの負荷が少ない点が上げられる。

企業名（及び略称）	株式会社ライトウェル
所在地（郵便番号及び住所）	〒110-0005 台東区上野1-20-10　上野風月堂本店ビル7F
関連部署名及び電話番号	LAM事業部営業グループ　03-5817-3242
ＵＲＬ	http://www.itLAM.com

対象技術	技術開発状況
セキュリティマネジメント	クライアントPCの詳細なログ及び操作画面を取得することにより、機密情報漏洩、監査対策、また「いつ、どこで、誰が」を特定できるので内部犯罪抑止に効果を発揮します。また、同時に個人のモラル意識の向上を促進し、生産性向上にも効果的です。特徴としては導入／展開が容易でクライアントPC及びネットワークへの負荷が少ない点、また異常検知時にメールを管理者に送信する機能等がある。

企業名（及び略称）	株式会社ライトウェル
所在地（郵便番号及び住所）	〒110-0005 台東区上野1-20-10　上野風月堂本店ビル7F
関連部署名及び電話番号	LAM事業部営業グループ　03-5817-3242
ＵＲＬ	http://www.itLAM.com

対象技術	技術開発状況
セキュリティマネジメント	クライアントソースに対する中央集中管理、及び各クライアントでのファイル単位の詳細な権限管理、PKIを使用した暗号化による情報漏洩防止が行なる。特徴としては、指紋、ICカード、IDkeyを使用することによる確実な個人認証、またネットワークに対する未登録PCの接続検知、登録PC盗難時の接続検知を行なうことにより内部犯罪抑止に効果を発揮する。

企業名（及び略称）	株式会社ルートレック・ネットワークス
所在地（郵便番号及び住所）	〒213-0011 川崎市高津区久本3-5-7　ニッセイ新溝ノ口ビル5F
関連部署名及び電話番号	044-829-4361
ＵＲＬ	http://www.routrek.co.jp

対象技術	技術開発状況
ネットワークセキュリティ	Rute Spikeはリモートネットワークのファイアウォールの内側など、直接IPによる接続ができない環境にあるホストやルータへのアクセスを提供するVPN製品。

企業名（及び略称）	株式会社ルートレック･ネットワーク
所在地（郵便番号及び住所）	〒213-0011 川崎市高津区久本3-5-7　ニッセイ新溝ノ口ビル5F
関連部署名及び電話番号	044-829-4361
URL	http://www.routrek.co.jp
対象技術	技術開発状況
ネットワークセキュリティ	Rute Spikeはリモートネットワークのファイアウォールの内側など、直接IPによる接続ができない環境にあるホストやルータへのアクセスを提供するVPN製品。

企業名（及び略称）	公共情報システム株式会社
所在地（郵便番号及び住所）	〒103-0004 中央区東日本橋2-15-5　モリビル
関連部署名及び電話番号	第2システム部　03-5820-9891
URL	http://www.pims.co.jp
対象技術	技術開発状況
認証	指紋だけでOSにロゴオンできる。スクリーンセーバの解除が指紋によってのみ可能にできるため離席時の不正使用を防止できる。各種アプリケーションのID／パスワードを指紋に置換えることができる。

企業名（及び略称）	ジェイズ・コミュニケーション株式会社
所在地（郵便番号及び住所）	〒103-0025 中央区日本橋茅場町1-11-2　フジビル16
関連部署名及び電話番号	セキュリティソリューション営業部　03-5623-0363
URL	http://www.jscom.co.jp
対象技術	技術開発状況
セキュリティサービス関連	clearsneft社にて（メーカ）販売：ソフトウェアに対しPCサーバとパックにして提供予定。

企業名（及び略称）　　セイコープレシジョン株式会社	
所在地（郵便番号及び住所）〒275-8558 習志野市茜浜1-1-1	
関連部署名及び電話番号　　システム事業部企画部商品企画課　03-5620-6824	
URL　http://www.seiko-p.co.jp	
対象技術	技術開発状況
認証	電子データ（文書、画像等）に対し、時刻情報を含む電子証明書を発行し、そのデータの存在時刻と改ざんのないことの証明をする。

企業名（及び略称）　　セキュアコンピューティングジャパン株式会社	
所在地（郵便番号及び住所）〒105-0001 東京都港区虎ノ門2-2-1　JTビル15階	
関連部署名及び電話番号　　営業部　03-5114-8224（代）	
URL　http://www.securecomputing.co.jp	
対象技術	技術開発状況
認証	ワンタイムパスワードソリューションとして、RSA社とともに二大代表製品として発売以来、企業を中心としたユーザに幅広く受け入れられている。特に日本では製薬業界、米国では金融業界に多くの導入実績を誇る。近年のアプリケーションのWeb・ネットワーク化に伴い、Webアクセスコントロール機能を強化し、認証用のPKI機能も装備したSafe Word Premier Accessを平成13年秋より発売している。また、併せて主要なWebアプリケーションやVPN装置に簡単にワンタイムパスワードソリューションを提供できる製品群を計画している。

企業名（及び略称）　　セキュアコンピューティングジャパン株式会社	
所在地（郵便番号及び住所）〒105-0001 東京都港区虎ノ門2-2-1　JTビル15階	
関連部署名及び電話番号　　営業部　03-5114-8224（代）	
URL　http://www.securecomputing.co.jp	
対象技術	技術開発状況
ネットワークセキュリティ	現在市場に出回っているファイアウォールの多くとは異なり、完全なアプリケーションゲートウェイ方式を採用しているため、アプリケーション（Webやメールなど）のセキュリティホールを突く攻撃にも有効に対処できる。米国特許技術のType Enforcementを採用し、自身にセキュリティホールを発生させない仕組みになっており、CERTやBug Traqでも発売以来、指摘されたセキュリティホールが無いという実績を誇る。ルーツは米国の国防プロジェクトに有り、そのため米国の政府機関や軍で幅広い導入実績を持っている。特に米空軍では制式ファイアウォールに指定されている。

企業名（及び略称）	セキュアコンピューティングジャパン株式会社
所在地（郵便番号及び住所）	〒105-0001 東京都港区虎ノ門2-2-1　JTビル15階
関連部署名及び電話番号	営業部　03-5114-8224（代）
ＵＲＬ	http://www.securecomputing.co.jp

対象技術	技術開発状況
ネットワークセキュリティ	世界初の商用URLフィルタリングツールとして発売されて以来、教育機関・大企業を中心に幅広くユーザを獲得している。現在のバージョンの最大の特徴は、主要なWebキャッシュサーバやファイアウォールにプラグインの形式でインストールされるOn-Box方式であり、これによってネットワークの接続速度を落とすことなくURLフィルタリングの導入を行うことができる。フィルタリングは専任の要員によって日々更新されるコントロールリストによって行われ、30のカテゴリ別に時間・曜日・任意のグループ毎に異なったフィルタリング環境を提供できる。

企業名（及び略称）	ソフォス株式会社
所在地（郵便番号及び住所）	〒231-0062 中横浜市中区桜木町1-1-8　日石横浜ビル15F
関連部署名及び電話番号	045-227-1800
ＵＲＬ	http://www.sophos.co.jp

対象技術	技術開発状況
ウイルス対策ツール	サーバー・クライアントのウィルス検出・駆除の統合ソリューション。マルチプラットフォーム対応なので混在したネットワーク環境に最適。ソフォス独自の技術（特許取得済）でウィルス検索が最適化されており、システム負荷を最小限に保ちながらセキュリティを保持することが可能。

企業名（及び略称）	ソフォス株式会社
所在地（郵便番号及び住所）	〒231-0062 中横浜市中区桜木町1-1-8　日石横浜ビル15F
関連部署名及び電話番号	045-227-1800
ＵＲＬ	http://www.sophos.co.jp

対象技術	技術開発状況
ウイルス対策ツール	スパム対策・ウィルス対策を一つで実施できるメール管理ソリューション。多様なツールを使用してセキュリティポリシーを簡単に策定・管理することも可能。

企業名（及び略称）	ソフォス株式会社
所在地（郵便番号及び住所）	〒231-0062 中横浜市中区桜木町1-1-8　日石横浜ビル15F
関連部署名及び電話番号	045-227-1800
ＵＲＬ	http://www.sophos.co.jp
対象技術	技術開発状況
ウイルス対策ツール	SMTPゲートウェイ、メールサーバーを通過する電子メール送受信のウィルス対策。添付ファイル（ZIP等一般的な圧縮ユーティリティで圧縮されたファイル含む）のウィルス検索も可能。ウィルス発見時には管理者、送受信者に警告メッセージを送信。ウィルス定義ファイルのアップデートも簡単。

企業名（及び略称）	ソラン株式会社
所在地（郵便番号及び住所）	〒108-8368 港区三田3-11-24
関連部署名及び電話番号	セキュリティ事業部　03-5427-5584
ＵＲＬ	http://www.sorun.co.jp
対象技術	技術開発状況
認証	電子印鑑は現在抱えている課題（個人認証）を補完すると共に電子化への加速を推進するツールとして、また市場の趨勢である認証の統合化を捉えた統合認証機能を持ったシステム。実際の印鑑にICチップを内蔵した電子印鑑はビジネス上の照査、承認、決済と言った業務をネットを通して実現し、ペーパーレスの効果をもたらす。PKIより利便性が高く、パスワードよりはるかに安全で実感を伴うシステム、それが電子印鑑である。

企業名（及び略称）	日本電気株式会社
所在地（郵便番号及び住所）	〒108-8001 港区芝5-7-1
関連部署名及び電話番号	第一ソリューション営業事業本部PIDシステム営業部　03-3798-2940
ＵＲＬ	http://www.sw.nec.co.jp/pid/
対象技術	技術開発状況
認証	ID番号の入力等で、指紋のみの入力で個人認証が可能。パソコンに接続するユニットなどの製品がある。

企業名（及び略称）	トップレイヤーネットワークスジャパン株式会社
所在地（郵便番号及び住所）	〒102-0094 千代田区紀尾井町3-32　紀尾井町WITHビル2F
関連部署名及び電話番号	マーケティング　03-3511-1202
ＵＲＬ	http://www.toplayer.co.jp
対象技術	技術開発状況
認証	内部ネットワークのエッジもしくはその周辺に配置され未認証ユーザからのトラフィックを監視。認証ツールと連携して正当なユーザからの接続のみ許可を行なうネットワーク機器。接続されたユーザに関しては、通信ログの記録を行なう。有線・無線・ブロードバンド等、接続の形式に関係なくユーザのアクセスコントロールを一元化することが可能。

企業名（及び略称）	トップレイヤーネットワークスジャパン株式会社
所在地（郵便番号及び住所）	〒102-0094 千代田区紀尾井町3-32　紀尾井町WITHビル2F
関連部署名及び電話番号	マーケティング　03-3511-1202
ＵＲＬ	http://www.toplayer.co.jp
対象技術	技術開発状況
不正侵入対策	http、ftp、ICMPを使用した攻撃及びDOS攻撃をリアルタイムに検知して遮断。ステルス・モードでの導入が可能であり専用OS／ハードのため、機器自体の可能性と堅牢性が優れている。

企業名（及び略称）	日本エフ・セキュア株式会社
所在地（郵便番号及び住所）	〒210-0005 川崎市川崎区東田町8　パレール三井ビル20F
関連部署名及び電話番号	営業部　044-230-2223
ＵＲＬ	http://www.f-secure.co.jp
対象技術	技術開発状況
ウイルス対策ツール	緊急ウィルス情報の発信、新規ウィルスに対する最速の対応、安定稼動、かつ最高の検知率、ローカルスタッフによる手厚いサポートを特徴とする。

企業名（及び略称）	日本キャンドル株式会社
所在地（郵便番号及び住所）	〒100-0014 千代田区永田町2-14-3　赤坂東急ビル9F
関連部署名及び電話番号	マーケティング部　03-3595-7200
ＵＲＬ	http://www.candle.co.jp
対象技術	技術開発状況
暗号技術	IBM社のミドルウェアであるWebsphere MQのメッセージデータの暗号化及びアクセスの認証を制御できる。暗号化はRSAの公開鍵方式を採用。

企業名（及び略称）	日本サイバーサイン株式会社
所在地（郵便番号及び住所）	〒105-0003 港区西新橋3-5-8　渡瀬ビル2F
関連部署名及び電話番号	営業部　03-5733-3131
ＵＲＬ	http://www.cybersign.co.jp
対象技術	技術開発状況
認証	サイン認証によりコンピュータルーム等、機密性の高い部屋への入室をコントロールするシステムです。入口でサインをして予め登録されているサインと認証されればドアが開きます。ネットワーク対応により複数の出入口がコントロールも可能です。誰が何時入室、退室したのかのログ管理も可能です。

企業名（及び略称）	日本サイバーサイン株式会社
所在地（郵便番号及び住所）	〒105-0003 港区西新橋3-5-8　渡瀬ビル2F
関連部署名及び電話番号	営業部　03-5733-3131
ＵＲＬ	http://www.cybersign.co.jp
対象技術	技術開発状況
認証	PCの起動時にサイン認証を行ない、正しく認証された時のみWindowsにログオンできるというWindowsのログオン時の認証プログラム。サインの認証はログオンするパソコン内で行なうことも、ネットワーク上のサイン認証サーバで行なうことも可能。

企業名（及び略称）	日本サイバーサイン株式会社
所在地（郵便番号及び住所）	〒105-0003 港区西新橋3-5-8　渡瀬ビル2F
関連部署名及び電話番号	営業部　03-5733-3131
ＵＲＬ	http://www.cybersign.co.jp

対象技術	技術開発状況
認証	社内ネットワークとインターネット等の外部のネットワークとの境界に設置することにより外部から社内ネットワークへの接続者も認証する装置。外部からアクセスする者はサイン認証システムで認証された場合のみ社内へのアクセスが許可される。

企業名（及び略称）	日本サイバーサイン株式会社
所在地（郵便番号及び住所）	〒105-0003 港区西新橋3-5-8　渡瀬ビル2F
関連部署名及び電話番号	営業部　03-5733-3131
ＵＲＬ	http://www.cybersign.co.jp

対象技術	技術開発状況
認証	Windows-CE（Pocket-PC）のパワーオン時の使用者確認のソフト。Pocket-PCの電源を入れた時にサイン入力をさせ、予め登録してあるサインと照合して正しく認証された時のみPocket-PCが使用可能になる。正しく認証されない場合は電源が自動的に切断される。Pocket-PCなどキーボードの無い端末では起動時のセキュリティ確保のためのパスワード入力がスマートにできないがサイン認証を使うことで素早くスマートにログオンすることができるようになる。

企業名（及び略称）	日本サイバーサイン株式会社
所在地（郵便番号及び住所）	〒105-0003 港区西新橋3-5-8　渡瀬ビル2F
関連部署名及び電話番号	営業部　03-5733-3131
ＵＲＬ	http://www.cybersign.co.jp

対象技術	技術開発状況
認証	手書きのサインで個人認証を行なうためのソフトウェアをアプリケーション等に組込むための開発ツールキット。この開発ツールを利用するには日本サイバーサイン社とのパートナー契約が必要。

企業名（及び略称）	日本サイバーサイン株式会社
所在地（郵便番号及び住所）	〒105-0003 港区西新橋3-5-8　渡瀬ビル2F
関連部署名及び電話番号	営業部　03-5733-3131
URL	http://www.cybersign.co.jp
対象技術	技術開発状況
認証	手書きのサインで個人認証を行なうサービスを提供するサーバプログラム。開発者はこの製品に付く開発ツールキットを利用することによって自社のアプリケーションにサイン認証プログラムを組込むことができる。この製品を利用するには日本サイバーサイン社とのパートナー契約が必要。

企業名（及び略称）	ネクサンティス株式会社
所在地（郵便番号及び住所）	〒106-0031 東京都港区西麻布4-3-11　泉西麻布ビル4F
関連部署名及び電話番号	インターネット・エンタプライズ・ソリューション事業部 03-3409-7501
URL	http://www.nexantis.co.jp
対象技術	技術開発状況
暗号技術	ICカードを使って、PCに保存されているファイルやフォルダを暗号化することで、情報の不正な持ち出しやノートPC紛失などによるデータの漏洩、改竄等を防ぐ。ファイルやフォルダを暗号化するための暗号鍵やパスワードをPCから切り離してセキュリティ強固なICカードに格納するため、カード所有者以外がPCを使用しても暗号化された情報を解読することができない。万一、不正ユーザが正当ユーザのカードを入手しても、誤ったパスワードを続けて3回入力するとカードがブロックされ使用不能になる。

企業名（及び略称）	ネクサンティス株式会社
所在地（郵便番号及び住所）	〒106-0031 東京都港区西麻布4-3-11　泉西麻布ビル4F
関連部署名及び電話番号	インターネット・エンタプライズ・ソリューション事業部 03-3409-7501
URL	http://www.nexantis.co.jp
対象技術	技術開発状況
認証	AccessMasterは、ユーザー認証、アクセスコントロール、シングルサインオン、アイデンティティマネジメント、PKIマネジメントの機能をひとつのプラットフォームで提供する、エンタープライズ統合セキュリティソリューション。メインフレームからWebサーバーまで、あらゆるアプリに対してのアクセスコントロールとシングルサインオンを実現。同時に、アイデンティティマネジメント機能により、各アプリケーションのユーザーアカウント登録や変更・削除の作業をAccessMasterコンソールで集約して管理できる。

企業名（及び略称）	ネクサンティス株式会社
所在地（郵便番号及び住所）	〒106-0031 東京都港区西麻布4-3-11　泉西麻布ビル4F
関連部署名及び電話番号	インターネット・エンタプライズ・ソリューション事業部 03-3409-7501
URL	http://www.nexantis.co.jp

対象技術	技術開発状況
認証	PortalXpert（ポータルエキスパート）は、インターネット・イントラネットWebサーバーに対するアクセスコントロールとシングルサインオン機能を提供する認証サーバ。リバースプロシキアーキテクチャーの採用により、Webリソースへのエージェント追加が不要であり、プラグアンドプレイで容易に展開可能なソリューション。パスワード又はX.509証明書によるユーザー認証後、ユーザー毎にパーソナライズされたウェルカムページを表示する。負荷分散と高可用性機能がプラグインされており、B2B、B2E及びB2Cでも利用可能な信頼性と拡張性が提供されている。

企業名（及び略称）	ネクサンティス株式会社
所在地（郵便番号及び住所）	〒106-0031 東京都港区西麻布4-3-11　泉西麻布ビル4F
関連部署名及び電話番号	インターネット・エンタプライズ・ソリューション事業部 03-3409-7501
URL	http://www.nexantis.co.jp

対象技術	技術開発状況
認証	利用するアプリケーションが増えると、ログイン情報（IDとパスワード）も同数必要になるため、ユーザは、全てのIDとパスワードを同一にしたり、机回りにメモをとるなどして間に合わせることが多くなる。ICカードに保管したあらゆるアプリケーションのIDとパスワードが、各アプリケーションのログイン時に自動伝送されるため、ユーザは唯一ICカードのPINコードを入力するだけでよく、ログイン情報を管理・入手する手間から開放される上、セキュリティポリシーの徹底をも実現することができる。

企業名（及び略称）	ネクサンティス株式会社
所在地（郵便番号及び住所）	〒106-0031 東京都港区西麻布4-3-11　泉西麻布ビル4F
関連部署名及び電話番号	インターネット・エンタプライズ・ソリューション事業部 03-3409-7501
URL	http://www.nexantis.co.jp

対象技術	技術開発状況
認証	PCのユーザ認証をICカードやiKey(R)、指紋認証システムで行なうことにより、正当なユーザ以外のWindowsドメインへのログインを退け、PC内のあらゆる情報への不正アクセスを防ぐことができる。ICカードをセットし、正しいPINｺｰﾄﾞを入力するとWindowsにログインする。

企業名（及び略称）	ネクサンティス株式会社
所在地（郵便番号及び住所）	〒106-0031 東京都港区西麻布4-3-11　泉西麻布ビル4F
関連部署名及び電話番号	インターネット・エンタプライズ・ソリューション事業部 03-3409-7501
URL	http://www.nexantis.co.jp

対象技術	技術開発状況
認証	ICカードに保存した証明書や個人鍵でユーザ認証を行なうことにより、送信者を証明できる電子署名付きEメール、及び、意図した受信者のみが複号･解読可能な暗号化メッセージの作成（S/MIME）、セキュアWebアクセス（SSL3）、VPN、Windows2000／XPへのスマートログオンを実現することができる。秘密鍵の生成や暗号処理の演算全てをPCから切り離し、セキュリティ強固なICカード内で実現するため、PKIに基づく高度なセキュリティが物理的に可能になった。

企業名（及び略称）	ネクサンティス株式会社
所在地（郵便番号及び住所）	〒106-0031 東京都港区西麻布4-3-11　泉西麻布ビル4F
関連部署名及び電話番号	インターネット・エンタプライズ・ソリューション事業部 03-3409-7501
URL	http://www.nexantis.co.jp

対象技術	技術開発状況
認証	ICカードリーダ・ライタ端末は、ICカード内の情報の読取り、及び、ICカードへの情報の書き込みを行う装置で、PCに直接（シリアルポートやUSBポート、PCMCIAを経由）して使用するタイプと、リーダー・ライタのみで独立して使用するタイプとがあります。Nexantisでは、あらゆるご要望にお答えできるよう各種ICカードリーダー・ライタ端末を取り揃えている。

企業名（及び略称）	ネクサンティス株式会社
所在地（郵便番号及び住所）	〒106-0031 東京都港区西麻布4-3-11　泉西麻布ビル4F
関連部署名及び電話番号	インターネット・エンタプライズ・ソリューション事業部 03-3409-7501
URL	http://www.nexantis.co.jp

対象技術	技術開発状況
セキュリティマネジメント	自動インベント機能により､インベントリモジュールのインストール、監査を完全に一元化、監査のスケジュール・処理の自動化。

企業名（及び略称）	ネクサンティス株式会社
所在地（郵便番号及び住所）	〒106-0031 東京都港区西麻布4-3-11　泉西麻布ビル4F
関連部署名及び電話番号	インターネット・エンタプライズ・ソリューション事業部 03-3409-7501
URL	http://www.nexantis.co.jp

対象技術	技術開発状況
セキュリティサービス関連	SecureScanは、ネットワークの脆弱性（セキュリティホール）を検査する、第3世代のネットワークセキュリティスキャナー。IPアドレスをもつ全てのネットワーク機器（サーバ等）に対して擬似攻撃により脆弱性を発見し、修正方法を含めたレポートを出力。脆弱性検査により、クラッカーからの攻撃を未然防止する。

企業名（及び略称）	富士通関西中部ネットテック株式会社
所在地（郵便番号及び住所）	〒540-0001 中央区城見2-2-53　大阪東京海上ビル
関連部署名及び電話番号	総務部　06-6949-0561(代)
URL	http://www.kcn.fujitsu.com

対象技術	技術開発状況
認証	サーバ群に対するアカウント情報やアクセス制御情報を管理。人事データを連携するため、組織変更にも柔軟に対応などの特徴がある。

企業名（及び略称）	富士通関西中部ネットテック株式会社
所在地（郵便番号及び住所）	〒540-0001 中央区城見2-2-53　大阪東京海上ビル
関連部署名及び電話番号	総務部　06-6949-0561(代)
URL	http://www.kcn.fujitsu.com

対象技術	技術開発状況
セキュリティサービス関連	セキュアシステムの診断・企画から設計・構築・運用までスペシャリストがトータルにサポートする各種サービスご提供。セキュリティ診断、セキュリティポリシー策定支援、不正アクセス、情報漏洩対策、ウィルスチェック、URLフィルタリング機構構築、セキュリティ管理サポート、セキュリティ／ウィルス情報提供、セキュリティ教育など。

企業名（及び略称）	三菱スペース・ソフトウェア株式会社
所在地（郵便番号及び住所）	〒105-6137 港区浜松町2-4-1
関連部署名及び電話番号	技術推進部
ＵＲＬ	http://www.mss.co.jp
対象技術	技術開発状況
セキュリティマネジメント	MSIESERはネットワーク上を流れるメール、Webなどのパケット情報を記録し、解析する装置。メールの内容、Webサイトのアクセス状況、掲示板への書き込み内容などを記録・監視できる。このためネットワークの私的利用の監視や情報漏洩を抑止することができる。また内部・外部からの不正アクセスを監視することもできる。

企業名（及び略称）	矢崎総業株式会社
所在地（郵便番号及び住所）	
関連部署名及び電話番号	車載システム開発センター第４システム技術開発部　055-965-3355
ＵＲＬ	http://www.yazaki-group.com
対象技術	技術開発状況
暗号技術	PC内のファイルの暗号化、PC本体の利用制限（PCロック機能）。アプリケーションソフトのコピー防止を目的としたハードウェアプロテクトキー。コピー防止の他に起動回数制限やインストールの試用期間対応やネットワーク対応といった様々なアプリケーションに対応可能。

企業名（及び略称）	リコーシステム開発株式会社
所在地（郵便番号及び住所）	〒104-0054 中央区勝どき3-12-1　フォアフロントタワー
関連部署名及び電話番号	ソリューション開発事業部セキュリティビジネスグループ 03-5560-8921
ＵＲＬ	http://www.rsk-tokyo.co.jp
対象技術	技術開発状況
暗号技術	PKIを用いたセキュア文書交換システム。アプリケーションフレームワークとして提供し、既存業務システムに容易にファイル交換セキュリティ（アクセス制御、電子署名／検証、原本性確保）を提供。

企業名（及び略称）	リコーシステム開発株式会社
所在地（郵便番号及び住所）	〒104-0054 中央区勝どき3-12-1　フォアフロントタワー
関連部署名及び電話番号	ソリューション開発事業部セキュリティビジネスグループ 03-5560-8921
ＵＲＬ	http://www.rsk-tokyo.co.jp

対象技術	技術開発状況
暗号技術	PKIを用いたセキュア文書交換システム。アプリケーションフレームワークとして提供し、既存業務システムに容易にファイル交換セキュリティ（アクセス制御、電子署名／検証、原本性確保）を提供。

企業名（及び略称）	ワールドアクセル株式会社
所在地（郵便番号及び住所）	〒105-0013 港区浜松町1-2-12
関連部署名及び電話番号	オペレーション部　03-5402-6731
ＵＲＬ	http://www.worldaxle.com

対象技術	技術開発状況
ネットワークセキュリティ	個人ユーザー向けNATによるグローバルアドレスとプライベートアドレスの変換により不正アクセスを防ぐ。