平成１７年２月２５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１６年１月１日から平成１６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16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16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認知状況

(1)　認知件数（注１）（注２）

平成16年中の不正アクセス行為の認知件数は356件で、前年と比べ、144件増加した。

なお、平成13年中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	平成16年
認知件数	106	1,253	329	212	356
海外からのアクセス	25	448	13	35	37
国内からのアクセス	73	258	286	158	303
アクセス元不明	8	547	30	19	16

(2)　被害に係る特定電子計算機のアクセス管理者（注３）

被害に係る特定電子計算機のアクセス管理者を見ると、一般企業が202件と最も多く、次いでプロバイダの126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	平成16年
プロバイダ	59	182	243	98	126
一般企業	25	429	62	76	202
大学、研究機関等	8	101	3	16	6
その他	14	139	21	22	22
うち行政機関	-	-	12	3	12
不明	0	402	0	0	0
計	106	1,253	329	212	356

※　「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及びその附置機関を含む。

「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。

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、利用権者（注４）からの届出が172件と最も多く、次いで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146件、被害に係る特定電子計算機のアクセス管理者からの届出が29件、発見者からの通報が７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	平成16年
アクセス管理者からの届出	30	168	47	12	29
利用権者からの届出	23	118	92	78	172
警察活動	35	930	185	100	146
発見者からの通報	7	21	0	19	7
その他	11	16	5	3	2
計	106	1,253	329	212	356

(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129件で最も多く、次いでインターネット・オークションに関する不正操作（他人になりすましての出品・入札等）が103件であり、他にホームページの改ざんが40件、電子メールの盗み見等の情報の不正入手が33件、不正ファイルの蔵置（不正ツールやフィッシング（注５）用ホームページデータの蔵置等）が11件、利用権者のパスワード変更が10件、データの消去等が９件、インターネット・バンキングの不正送金が７件等であった（重複計上あり）。

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65事件（142件）、検挙人員は88人で、前年と比べ検挙事件数は７事件増加（３件減少）し、検挙人員は12人増加した。すべての検挙が不正アクセス行為によるものであり、不正アクセス助長行為の検挙は無かった。

不正アクセス行為の態様については、識別符号窃用型（注７）が62事件（131件）であり、セキュリティ・ホール攻撃型（注８）が４事件（11件）であった。（うち１事件は、識別符号窃用型とセキュリティ・ホール攻撃型の両方の行為が行われた。）。

なお、検挙人員88人中62人が成人であり、26人が少年であった。

		平成12年	平成13年	平成14年	平成15年	平成16年
不正アクセス行為	検挙事件数	30	35	51	58	65
	検挙件数	62	66	102	143	142
	検挙人員	34	51	68	76	88
不正アクセス助長行為	検挙事件数	4	1	2	2	0
	検挙件数	5	1	3	2	0
	検挙人員	5	1	3	2	0
計	検挙事件数	31 (重複3)	35 (重複1)	51 (重複2)	58 (重複2)	65
	検挙件数	67	67	105	145	142
	検挙人員	37 (重複2)	51 (重複1)	69 (重複2)	76 (重複2)	88

3　検挙事例

1	**インターネット・オークションに係る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**

無職の男（31）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15年８月から16年１月までの間、他人が使用するオークション・サービス用ＩＤ12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等に現金を振り込ませる手口で、76人から総額約900万円をだまし取った。平成16年２月、不正アクセス禁止法違反、詐欺罪、私電磁的記録不正作出・同供用罪で検挙した（埼玉、山形、茨城、京都、岡山）。

2	**セキュリティ・ホール攻撃による個人情報ファイルの取得方法の公表に係る不正アクセス禁止法違反及び威力業務妨害事件**

公務員の男（40）が、社団法人が一般からの情報受付のために公開したホームページに係るセキュリティ・ホールを指摘する目的で、平成15年11月、公開のイベント会場において、セキュリティ・ホールを攻撃して同社団法人のＷｅｂサーバに不正アクセスし、処理情報を取得する手法を実演して、多数の参加者に公表した。16年２月、不正アクセス禁止法違反及び威力業務妨害で検挙した。さらに、16年３月、同手法をまねて同社団法人のＷｅｂサーバに不正アクセスしたイベント参加者の会社員ら３人を不正アクセス禁止法違反で検挙した（警視庁）。

3	**識別符号通知プログラムを使用して収集した識別符号の窃用によるオンラインゲームに係る不正アクセス禁止法違反事件**

コンピュータ保守管理作業員の男（20）が、オンラインゲームで使用するアイテムを他人から不正に取得する目的で、平成14年12月から15年７月までの間、ＩＤ及びパスワードを自動的に通知する自作のプログラムを電子掲示板等でその機能を隠して掲示及び配付し、同プログラムの使用者から収集したオンラインゲーム・サービスのＩＤ及びパスワードを窃用して不正アクセスし、当該オンラインゲーム・サービス利用者が保有していたアイテムを、不正に自己の保有となるよう移動させた。16年３月、不正アクセス禁止法違反で検挙した（北海道、埼玉、熊本）。

4	**電子メール等により言葉巧みにだまして入手した識別符号の窃用によるオンラインゲームに係る不正アクセス禁止法違反事件**

中学生（14）らが、オンラインゲームで使用するアイテムを他人から不正に取得す

る目的で、平成15年８月頃から11月までの間、電子メール等を利用して「アイテムを譲る」などと言葉巧みに持ちかけてだます方法で、他人が使用するオンラインゲーム・サービス用ＩＤ15個のパスワードを入手して不正アクセスした上、他人が保有するアイテムを不正に自己の保有となるよう移動させた。16年４月、不正アクセス禁止法違反で２人を検挙した（京都）。

5	電子メールアドレスの入手を目的とした不正アクセス禁止法違反及びいわゆる架空請求メールの送信による詐欺事件

出会い系サイト運営者の男（33）ら３人が共謀し、運営している出会い系サイトの宣伝・勧誘の電子メールを送信するための電子メールアドレスを入手する目的で、平成15年10月、他人が運営する出会い系サイトの会員管理用のパスワードを元従業員の男（29）から聞き出した上で、別の男（38)に作成させた電子メールアドレス等の自動抽出プログラムを使用して不正アクセスし、当該出会い系サイトの会員情報を入手した。また、プログラムを作成した男が単独で、いわゆる架空請求メールを送信し、他人名義の口座に振り込ませる手口で81人から約200万円をだまし取った。16年５月、不正アクセス禁止法違反で４人を検挙し、６月、不正アクセス禁止法違反及び詐欺で１人を検挙した（鹿児島）。

6	不正アクセスにより入手した電子メールアドレスに対して迷惑メールを送信した不正アクセス禁止法違反事件

無職の男（35）が、元勤務先の社長に対して嫌がらせをする目的で、平成16年４月から５月の間、元勤務先のメールサーバに、在職時に知り得た会社従業員の電子メールアドレス用のＩＤ及びパスワードを使用して不正アクセスし、同社の製品案内等の電子メールの受信希望者に係る電子メールアドレスのリストを発見したことから、約3,000人の電子メールアドレスにあてて、同社が送信したかのように装い、いわゆるコンピュータウイルス等を添付した電子メールを送信した。16年７月、不正アクセス禁止法違反で検挙した（愛知）。

7	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及び電子計算機使用詐欺事件

自営業の男（37）が、いわゆる出会い系サイトを通じて知り合った女性の口座から不正に金を得る目的で、平成16年６月から７月の間、信用金庫のインターネット・バンキング用の認証サーバに、女性のパソコンの設定を行った際に知り得た女性名義の口座のＩＤ及びパスワードを使用して不正アクセスし、インターネット上で購入した他人名義の口座へ575万円の送金操作を行い、同口座から現金を引き出した。16年９

月、不正アクセス禁止法違反及び電子計算機使用詐欺罪で検挙した（京都）。

8	他人になりすまして電子メールを送信した不正アクセス禁止法違反事件

アルバイトの男（26）が、元勤務先の会社経営者に対して嫌がらせをするため、同経営者の電子メールを盗み見る目的で、平成16年５月、リマインダ機能（注９）を利用してパスワードを入手した上で、不正アクセスして同経営者の電子メールの内容を盗み見た。さらに、同人からＩＤ及びパスワードを教示された知人の自営業の男（33）が、同様に不正アクセスし、同経営者になりすまして内容虚偽の電子メールを送信した。16年９月、不正アクセス禁止法違反で２人を検挙した（栃木）。

9	換金目的でオンラインゲームのアイテムを窃取した不正アクセス禁止法違反事件

無職少年（19）が、知人がオンラインゲームで使用するアイテムを不正に取得して換金する目的で、平成16年４月、オンラインゲームのサーバに、以前聞いていたＩＤ及びパスワードを使用して不正アクセスした上、更に別の知人のＩＤ及びパスワードを窃用した不正アクセスにより操作可能としたゲーム上のキャラクターを介して、多数のアイテムを他人に譲渡し、現金約29万円に換金した。16年９月、不正アクセス禁止法違反で検挙した（香川）。

10	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及び電子計算機使用詐欺事件

会社員の男（43）が、他人の口座から不正に金を得る目的で、平成16年６月から７月の間、銀行のインターネット・バンキング用の認証サーバに、あらかじめインターネット・カフェのパソコンに仕掛けていたキーロガー（注10）を用いて収集した口座開設者のＩＤ及びパスワードを使用して不正アクセスし、同口座開設者の口座からインターネット上で購入した他人名義の銀行口座へ約36万円の送金操作を行い、同口座から現金を引き出した。16年10月、不正アクセス禁止法違反及び電子計算機使用詐欺罪で検挙した（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多く（62事件（131件））が識別符号窃用型であった。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）が引き続き最も多く、31事件（65件）であった。次いで、立

場上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が13事件（21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が７事件（14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５事件（６件）等、特に高度な技術を有していない者でも行える形態が多かった。

しかし、プログラムの脆弱性を利用した情報の不正取得のように、セキュリティの脆弱性を突くセキュリティ・ホール攻撃型が４事件（11件）（うち、１事件は、識別符号窃用型とセキュリティ・ホール攻撃型の両方の行為が行われた。）であったほか、識別符号窃用型のうちキーロガー等のプログラムを使用して識別符号を入手したものが４事件（19件）と、高度なコンピュータ技術を悪用したものも増加した。

(2) 被疑者

アクセス管理者及び利用権者にとって、元交際相手や元従業員等顔見知りの者による犯行は29事件（49件）、面識のない他人による犯行は27事件（82件）であり、ネットワーク上のみの知り合いによる犯行は12事件（13件）であった（重複計上あり）。

また、被疑者の年齢は、10代が26人と最も多く、次いで30代が23人、20代が21人、40代が17人、50代が１人の順となっている。最年少の者は14歳であり、最年長の者は51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、元交際相手や元勤務先等に対する嫌がらせや仕返しのためが最も多く、23事件（35件）であった。次いで好奇心を満たすためが15事件（23件）、オンラインゲームで不正操作を行うためが10事件（31件）、不正に金を得るためが９事件（32件）、顧客データの収集など情報を不正に入手するためが５事件（12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１事件（５件）増加、好奇心を満たすためが３事件（24件）、不正に金を得るためが２事件（41件）それぞれ減少し、オンラインゲームで不正操作を行うためが５事件（26件）、情報を不正に入手するためが３事件（７件）それぞれ増加した。

(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62事件（131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見ると、オンラインゲームが23事件（47件）と最も多く、次いで電子メールが15事件（24件）、インターネット・オークションが７事件（34件）、ホームページ公開サービスが６事件（６件）、インターネット・バンキングが４事件（４件）等となっている（重複計上あり）。

(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、17事件であった。その内訳は次のとおり。

	事件数
電子計算機使用詐欺	5
詐欺	5
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	2
組織犯罪処罰法違反	2
脅迫	1
恐喝未遂	1
威力業務妨害	1
電気通信事業法違反	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３件（すべて愛知）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62事件（131件）中、28事件（61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」）や誕生日に関連する番号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、３事件（４件）が利用権者が書き出した又は口にしたパスワードを偶然に見聞きした者の犯行であり、７事件（14件）が利用権者からパスワードを言葉巧みに聞き出した、後ろからのぞき見た又は利用権者の周辺を探して見つけ出した者の犯行であるなど、アクセス管理者又は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、パスワードを不用意に教えない、また、パスワードを定期的に変更するなど、識別符号を適切に設定・管理する必要がある。

さらに、フィッシング事案による被害の増加が懸念されていることから、個人情報を聞き出そうとするメールに対し、不用意に回答しないよう注意する必要がある。

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、ＩＤやパスワード等を入手する手口が見られたことから、不特定多数の者が利用できる端末では、ＩＤやパスワードを始め、口座番号やクレジットカード番号等の個人情報の入力を伴うサービスをできるだけ利用しないようにする必要がある。

(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の発生が前年に比べて増加しており、また、この種の手口による事犯は、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向上・維持が必要である。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セキュリティ・ホールを解消するための措置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（注11）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の制限等の措置を講ずる必要がある。

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

認知とは、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としている。

注２ 件数

件数とは、犯罪構成要件に該当する行為を被疑者が行った数をいう。

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回の行為とみなし得る場合は包括して１件としている。

注３ 特定電子計算機のアクセス管理者

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である。

注４　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加入者や、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５　フィッシング

銀行等の企業からのメールを装い、メールの受信者に偽のホームページにアクセスするよう仕向け、そのページにおいて個人情報（クレジットカード番号、ＩＤ、パスワード等)を入力させるなどして当該情報を不正に入手するような行為をいう。その情報を元に金銭をだまし取る手口がフィッシング詐欺といわれる。

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。

例えば、ＩＤを不正に登録して使用する行為や、セキュリティの脆弱性をついて操作指令を与える等の手法による不正アクセス行為が該当する。

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、「ニックネーム

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、キーボードで打鍵した文字を記録するプログラムをいう。

注11　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16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594件（昨年：407件）であった（注２）。平成16年はアクセス形跡の届出が大幅に増加したが、実被害件数は減少した。

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557件（昨年：510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515件（昨年：313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。402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。63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43件である。

パスワード推測：23件

ソフトウェアのバグを利用した攻撃：12件

システムの設定内容を利用した攻撃：5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43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：24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：11件

資源利用（ファイル、CPU使用）：6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：5件

証拠の隠滅：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もしくは低下させたり

する攻撃である。10件（昨年：15件）の届出があった。
過負荷を与える攻撃：6件
例外処理を利用した攻撃：3件
spamメール：1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、33件（昨年：57件）の届出があった。
メール中継に関するもの：4件
そのうちメール中継に実際に利用されたもの：3件
メールアドレス(ドメイン)の詐称：11件
なりすまし：3件
オープンプロキシ：2件
その他：13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。

実際に侵入を受けた43件（昨年：64件）、メール中継に係わる問題(弱点)のあった3件（昨年：9件）などの計55件（昨年：92件）を分類すると以下のようになる。突出した件数となった被害原因は無く、様々なセキュリティ対策の不備が狙われていると推測される。

ID、パスワード管理の不備によると思われるもの：9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：11件
設定の不備(セキュリティ上問題のあるデフォルト設定を含む)によるもの：10件
不明：25件

(3) 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：21件
メールサーバー：6件
ファイアウォール：4件
ルータ：2件
Proxyサーバー：1件
その他のサーバー・不明：30件
クライアント：519件

(4) 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72件（昨年

：126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：4件
サーバーダウン：5件
不正アカウント作成：1件
WWW書き換え：15件
パスワードファイル盗用：3件
サービス低下：3件
オープンプロキシ：2件
ファイルの書き換え：21件
その他：31件

(5) 対策情報

(2)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い。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/

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（以下、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１６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5,217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4,974件の報告があった。
[1/1-3/31: 591件、4/1-6/30: 861件、7/1-9/30: 1658件、10/1-12/31: 1864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19件の報告があった。
[1/1-3/31: 2件、4/1-6/30: 14件、7/1-9/30: 2件、10/1-12/31: 1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30件の報告があった。
[1/1-3/31: 15件、4/1-6/30: 8件、7/1-9/30: 5件、10/1-12/31: 2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2件の報告があった。
[1/1-3/31: 2件、4/1-6/30: 0件、7/1-9/30: 0件、10/1-12/31: 0件]

オ　Web 偽装事案 (phishing)

Web のフォームなどから入力された口座番号やキャッシュカードの暗証番号といった個人情報を盗み取る Web 偽装事案について 30件の報告があった。
[1/1-3/31: 0件、4/1-6/30: 8件、7/1-9/30: 4件、10/1-12/31: 18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165件の報告があった。
[1/1-3/31: 38件、4/1-6/30: 31件、7/1-9/30: 15件、10/1-12/31: 19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]

phpBB の脆弱性を使って伝播するワームに関する注意喚起

libpng に複数の脆弱性

TCP プロトコルに潜在する信頼性の問題（更新)

Juniper JUNOS PFE の IPv6 処理にメモリリークの脆弱性

キーボード入力などを記録し外部に送信するプログラムに関する注意喚起

IEEE 802.11 DSSS 無線機器における DoS の脆弱性

Windows LSASS の脆弱性を使って伝播するワーム W32/Sasser

Windows に含まれる脆弱性に関する注意喚起

CISCO IOS における SNMP メッセージ処理の脆弱性

TCP プロトコルに潜在する信頼性の問題

Netsky.Q のサービス運用妨害攻撃に関する注意喚起

Microsoft ASN.1 Library の脆弱性に関する注意喚起

イ　活動概要（届出状況等の公表）

発行日：2005-01-25 [2004年10月1日～ 2004年12月31日]

発行日：2004-10-18 [2004年7月1日～ 2004年9月30日]

発行日：2004-07-16 [2004年4月1日～ 2004年6月30日]

発行日：2004-04-15 [2004年1月1日～ 2004年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] 302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、ワームの感染活動や弱点探索のためのスキャンなど、セキュリティ上の脅威となるトラフィクの観測を行い、セキュリティ予防情報を提供している（詳細はhttp://www.jpcert.or.jp/isdas/参照)。

(4) 脆弱性情報流通

日本国内の製品開発者（ベンダ）などの関連組織とのコーディネーションを行ない、JVN (JP Vendor Status Notes) にて公開した脆弱性情報は 30件であった（詳細はhttp://jvn.jp/参照)。

[1/1-3/31: 0件、4/1-6/30: 0件、7/1-9/30: 7件、10/1-12/31: 23件]

そのうち、平成１６年７月の経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」に従って、独立行政法人情報処理推進機構（IPA）に報告され、JVNにて公開した脆弱性情報は 11件であった。
[1/1-3/31：0件、4/1-6/30：0件、7/1-9/30：3件、10/1-12/31：8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。

情報通信危機管理基盤技術の研究開発
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
広域モニタリングシステムに関する基盤技術の研究開発
ネットワーク環境の脆弱性レベルをリアルタイムで定量評価し、情報流通をセキュアに運用するための意思決定システムの研究開発
モバイルセキュリティ基盤技術の研究開発
モバイル端末におけるセキュリティ保護技術に関する研究開発
ICカード等における認証のための高度な暗号技術に関する研究開発
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

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１６年１１月２６日から１２月２７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
大日本印刷株式会社
日本高信頼システム株式会社（JTS）
三菱電機株式会社

(2) 調査

警察庁が平成１６年１２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、次の条件により抽出した５００団体を対象に実施した。

- 国立・私立大学のうち理工系学部を設置するものから無作為に抽出
- 主なセキュリティ関連団体に所属する企業及び業種分類が「情報・通信」「サービス」「電気機器」「金融」である上場企業から無作為に抽出

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

広島大学

イ）企業

株式会社インテリジェントウェイブ
株式会社エス・エス・アイ・ジェイ
NECシステムテクノロジー株式会社
NECネクサソリューションズ株式会社
株式会社NTTドコモ
沖電気工業株式会社
コンピュータ・アソシエイツ株式会社
サイバーソリューション株式会社
サン・マイクロシステムズ株式会社
ジェイズ・コミュニケーション株式会社
シスコシステムズ株式会社
株式会社シマンテック
セキュアコンピューティングジャパン株式会社
セコムトラストネット株式会社
ソフトバンク･テクノロジー株式会社
株式会社タイテック
デジタルアーツ株式会社
トップレイヤーネットワークスジャパン株式会社
日本オラクル株式会社
日本ビジネスコンピュータ株式会社
株式会社日立情報システムズ
日立ソフトウェアエンジニアリング株式会社
ファルコンシステムコンサルティング株式会社
富士通関西中部ネットテック株式会社
富士通サポートアンドサービス株式会社
株式会社富士通ソーシアルサイエンスラボラトリ
富士通株式会社
株式会社ブリッジ･メタウェア
株式会社プロティビティジャパン
マカフィー株式会社
三菱スペース・ソフトウェア株式会社
横河電機株式会社
リコーテクノシステムズ株式会社

（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　独立行政法人情報通信研究機構

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：独立行政法人情報通信研究機構）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ー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。

平成16年には、不正アクセス模擬装置をネットワーク上で拡大する技術、広域に設置された観測点からセキュリティログを収集したり、大量のセキュリティログから効率的に、高精度にインシデントを分析する技術等に着手した。

詳細の入手方法（関連部署名及びその連絡先）

独立行政法人情報通信研究機構　情報通信部門　情報セキュリティ推進室　丹代　武

電話　042-327-5774

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　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（情報通信研究機構（ＮＩＣＴ）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）

独立行政法人情報通信研究機構　芝本部　研究開発推進部門委託研究推進室
（http://www2.nict.go.jp/ns/s802/itakukenkyu.htm）電話 03-3769-6810

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　侵入検知技術

テーマ名　広域モニタリングシステムに関する基盤技術の研究開発

開発年度　平成１６年度～平成１８年度

実施主体　横河電機株式会社，株式会社日立製作所，沖電気工業株式会社（情報通信研究機構（ＮＩＣＴ）からの委託）

背景、目的

近年のインターネットの急速な普及とブロードバンド化の進展は、利用者の裾野を急拡大するとともに、あらゆる社会経済活動の基盤を構成する不可欠な要素となり、電子商取引の発展や電子政府・電子自治体の実現など高度な利用を創成する土壌となっている。 一方で、このような情報通信ネットワークへの依存度の高まりは、その恩恵を十二分に享受している反面、情報通信ネットワークの機能不全や社会的混乱等を狙ったインシデントの発生や被害の拡大を助長させる一つの要因ともなっている。

さらに、利用者においては、最新のセキュリティパッチの適用等のセキュリティ対策が十分に講じられているとは必ずしも言えない状況である。このような利用者の意識不足がワーム感染の拡大に一層拍車をかける危険性が指摘されている。また、このような利用者が気付かない状態でワームに感染し、攻撃の踏み台となって大量の不要なパケットを送信するような事例が幾つも確認されているほか、このような事例が数多く積み重なることにより、ネットワークへの重大な支障や通信障害をきたすような大規模インシデントの発生に発展することも懸念される。

こうした中、本研究では、インターネット上の多地点で、トラフィックログ情報とセキュリティログ情報を収集して、その大規模情報を効率的に統合管理し、多地点・複数レイヤにまたがる分析を行うことで、広域ネットワークに影響を及ぼす異常なインシデントの早期発見を実現する基礎技術を確立する。また、異常が検出されてからの迅速な対応を促すために、セキュリティオペレーションおよびそのための情報交換を円滑にする基盤システムを開発する。

研究開発状況（概要）

・平成１６年度より以下の研究開発を実施中。
(1) 広域モニタリングシステムのプローブシステムの開発
(2) 広域モニタリングシステムのネットワーク装置情報収集方式の開発
(3) 広域モニタリングシステムで収集したデータの分析システムの開発
(4) 広域モニタリングシステムのオペレーション方式の開発

・平成１８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）

独立行政法人情報通信研究機構　研究開発推進部門委託研究推進室
（http://www2.nict.go.jp/ns/s802/itakukenkyu.htm）電話 03-3769-6810

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　ネットワーク環境の脆弱性レベルをリアルタイムで定量評価し、情報流通をセキュアに運用するための意志決定システムの研究開発

開発年度　平成１６年度～平成１８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、株式会社日立製作所、日本電気株式会社（情報通信研究機構（ＮＩＣＴ）からの委託）

背景、目的

e-Japan 重点計画-2003 において、『2006 年度までに、インターネット等におけるネットワークセキュリティの飛躍的向上を図るため、情報通信ネットワークの安全性及び信頼性の確保に必要となる総合的な研究開発を実施する』ことが目標として掲げられているように、ネットワーク利用の依存が高まる中でＶＰＮ等を利用して相互に接続する各サイト（イントラネット）間においても情報流通のセキュアな運用が求められている。ネットワーク相互接続のリスクは、接続相手の中で最もセキュリティレベルの低いサイトの影響を受けることであり、接続相手として安全であるか否かの判断は現状ではＩＳＭＳ認証の取得状況あるいはセキュリティポリシー作成やその監査結果が判断の基準となっており、接続相手のセキュリティレベルを定量的に且つ相互に確認できる仕組みがないことが課題となってくる。

本研究開発では、日々新たに発見されるソフトウェアのバグ等の脆弱性に対して、比較的短い時間間隔においてサイト内の端末の脆弱性の有無を自動で収集し、各サイトに設置されている侵入検知システム（ＩＤＳ）のアラート等の脅威情報と合わせて分析し、脆弱性レベルの定量的な評価を行う。また、各サイトの脆弱性レベル等を収集・管理し、複数のサイトをまたがった分析を行い、分析結果を各サイトへ配信する流通機構を確立し、各サイトの意思決定者が自サイトや接続相手サイトのセキュリティレベルを確認して、容易に適切なアクセス制御を実施できることで、自サイトへの被害を未然に防ぐ等、脅威を低減することが可能とする。

研究開発状況（概要）

・平成１６年度より以下の研究開発を実施中。
(1) ネットワークの脆弱性レベル・脅威レベルの数値化手法
(2) セキュリティ情報管理とネットワーク管理のための意思決定支援技術
(3) サイト間のアクセス制御技術
・平成１８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）

独立行政法人情報通信研究機構　芝本部　研究開発推進部門委託研究推進室
（http://www2.nict.go.jp/ns/s802/itakukenkyu.htm）電話 03-3769-6810

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　モバイルセキュリティ基盤技術の研究開発

開発年度　平成１６年度～平成１８年度

実施主体　株式会社日立製作所、株式会社エヌ・ティ・ティ・ドコモ、株式会社KDDI研究所、日本電気株式会社（情報通信研究機構（ＮＩＣＴ）からの委託）

背景、目的

近年、モバイルキャリア網内に閉じたサービスにとどまらず、インターネットを利用したモバイルサービスが増加し、特定のモバイル通信事業者のみからだけではなく、一般のサービス提供者からサービスを享受するシーンが増加している。

そのような状況の中、通信路の盗聴、IDの偽造・改ざん、不必要な情報漏洩等、インターネットを利用することによる不正行為の可能性が増加している。安心してサービスを提供・享受するためには、正確なユーザ（端末）認証および正確なサーバ認証が必須である。

複数のモバイル網や、インターネット網等の異種網間の不適切な接続により、網内、網間を流れるデータの偽造・改ざんが行われる可能性があり、そのようなモバイル環境特有のセキュア基盤の構築が必須と考えられる。また、携帯端末の処理速度、メモリ容量、通信速度、通信安定性等のモバイル特有の制約を解決するためにモバイル特有のセキュリティ方式の実現が必要であると考えられる。さらに、これらのセキュリティ対策は、各モバイル通信事業者が独自に取り組むのではなく、相互運用性が確保された共通的に利用され得るインフラとならなければならない。

このような中、本研究開発では、モバイルコマースにおいて共通的に利用可能で且つ安全なセキュリティ基盤を構築することを目的とする。

研究開発状況（概要）

・平成１６年度より以下の研究開発を実施中。
(1) モバイルセキュリティ技術（長期・短期属性認証技術）
(2) モバイルセキュリティ検証技術
(3) モバイルサービス代行技術
(4) モバイルコマースアプリケーション技術
・平成１８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）

独立行政法人情報通信研究機構　研究開発推進部門委託研究推進室
（http://www2.nict.go.jp/ns/s802/itakukenkyu.htm）電話 03-3769-6810

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　モバイル端末におけるセキュリティ保護技術に関する研究開発

開発年度　平成１６年度～平成１８年度

実施主体　株式会社　日立製作所（情報通信研究機構（ＮＩＣＴ）からの委託）

背景、目的

近年、モバイル端末を用いた電子マネーや二次元バーコードと組み合わせたモバイルチケット、更にe-コマースなどのモバイルサービスが急速に普及しつつある。このような状況において、モバイル端末の不正な解析による端末内部の情報取得・改ざんや、モバイル端末の盗難・紛失などによる第三者の不正利用等が、モバイル端末利用者にとって大きな脅威となってきている。

本研究開発は、１つのモバイル端末で、多種多様なサービスを低コストで安全に享受できる世界の実現を目指すものであり、その実現のためモバイル端末単体の耐タンパ性を保ち、更に認証情報を適切に組み合わせた複合認証技術を確立する。その結果、利用者が異なるレベルのセキュリティが必要な多種多様なサービスを安全かつ簡単に受けることができる。さらにこれらの研究成果の統合により、モバイル端末の安全性を確保する技術を確立し、その安全性を利用者に明示する仕組みを実現する。

研究開発状況（概要）

・平成１６年度より以下の研究開発を実施中。

(1) 耐タンパ技術に関する研究開発

(2) 複合認証システム技術に関する研究開発

(3) セキュアモバイル端末利用システムに関する研究開発

・平成１８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）

独立行政法人情報通信研究機構　研究開発推進部門委託研究推進室

（http://www2.nict.go.jp/ns/s802/itakukenkyu.htm）電話 03-3769-6810

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　ＩＣカード等における認証のための高度な暗号技術に関する研究開発

開発年度　平成１６年度～平成１８年度

実施主体　株式会社　日立製作所（情報通信研究機構（ＮＩＣＴ）からの委託）

背景、目的

ユビキタスネットワーク社会では、IT におけるPC やサーバのみならず、携帯電話やPDA(Personal Digital Assistance)などの携帯端末、クレジットカードや電子マネー機能を搭載したIC カード、そしてRFID (Radio Frequency IDentification)タグなど、多種多様な機器がネットワークを介して互いに情報をやり取りする。このような人・機器のネットワークによる繋がりは今後ますます緊密になり、それに伴い多様なサービス提供が可能になると想定される。

また、これらの小型電子機器の普及に伴って、通信における信頼性確保や、機器に格納されている情報保護の問題等が重要視されているが、一般的に小型電子機器では、コスト面や実装上の制約等の理由により、セキュリティ機能が省かれる場合が多く、通信内容の改ざんや秘匿すべき情報の漏洩防止などに十分な対処を実施できないことも少なくない。

こうした問題は、データの真正性検証、機器認証など、必要最低限の認証技術を実装することで回避できる。しかし、IC カードなどの小型電子機器で利用される認証技術においては、機能を実装するためのハードウェア回路規模やマイクロプロセッサのメモリ使用量などに対して厳しい要件が課される。さらに、外部からの微小な電力供給に依存して動作するRFID タグなどの電子タグでは、消費電力量についても制約がある。

従って、これからのユビキタスネットワーク社会におけるセキュリティ確保のため、小型電子機器での利用に適した、新たな認証技術の確立が急務であり、本研究開発においては、ユビキタスネットワーク社会で各種活用されるユビキタスネットワーク端末において、なりすまし等をはじめとした危険を未然に防ぐことのできる「認証技術」に関する研究開発を行う。

研究開発状況（概要）

- 平成１６年度より以下の研究開発を実施中。
  (1) 認証方式の設計技術
  (2) 認証方式の安全性評価技術
- 平成１８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）

独立行政法人情報通信研究機構　研究開発推進部門委託研究推進室
（http://www2.nict.go.jp/ns/s802/itakukenkyu.htm）電話 03-3769-6810

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　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16年度の成果：

近年普及が進みつつある「SSL-VPN」に分類されるアクセス制御製品について調査し、複数の製品において、15年度に公表したcookieの非secureモードでの発行を原因とする欠陥と同一の問題が存在する（SSLのクライアント認証を使用せずにユーザ名とパスワードでログインするモードを使用している場合に、セッションハイジャック攻撃を許してしまう）ことを発見した。この事実を、「ソフトウェア等脆弱性関連情報取扱基準」（平成16年経済産業省告示第235号）に基づき、届出機関である情報処理推進機構に届け出た。その結果、一部の製品はその欠陥が修正され、この事実は同機構より9月30日に公表された。

平成15年度の成果：

SSL暗号化による情報保護を約束していて、かつ、cookieに頼っ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、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）およ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およ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およ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（関連部署名及びその連絡先）

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://SecurIT.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。

（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）	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)	ユーザ情報やパスワードを記憶しておくサーバと、各ユーザが使用するPC上に配布されるクライアントより構成されるシングル・サイン・オン技術。ユーザが自分のPCから一度、ICカードやパスワード等で認証に成功すれば、あらかじめサーバに登録されたWebページや一般のアプリケーションにサイン・オンする際には、必要なユーザIDやパスワードが自動的にサーバからダウンロードされ所定のフィールドに埋め込まれる。ユーザがパスワードを記憶する必要な無いため、長く複雑なパスワードを設定することができセキュリティが高まる。またサーバが定期的にランダムなパスワードを生成しパスワードの更新を行うことも可能。初回認証時にICカード等を紛失した場合には、事前に登録された個人情報を正しく答えさせることにより、緊急パスワードが発行される。答えるべき個人情報の数はポリシーによって管理でき、パスワードを忘れた場合と、ICカードを紛失した場合など、場合によって必要な個人情報の数を設定する。また、許容される正解率もポリシーにより設定可能。サーバにもPCにもその個人情報は保存されず、暗号学的な乱数のみが保存され、一定の正解率になった場合にのみ、その解答が暗号学的に処理され緊急パスワードが発行される。

企業名（及び略称）	大日本印刷株式会社
代表者氏名	北島　義俊
所在地（郵便番号及び住所）	〒　　東京都新宿区市谷加賀町一丁目１番１号
関連部署名及び電話番号	ビジネスフォーム事業部　ビジネスソリューション開発本部 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
認証技術 開発年：H16年	１.Windowsスマートカードログオンとデスクトップセキュリティ製品の連携 Microsoft社のActiveDirectoryへのログオンを、従来のWindows用ID／パスワードから、ICカードに格納された公開鍵電子証明書を用いて、セキュリティレベルを向上（成りすまし防止等）させる機能です。Windowsスマートカードログオンとの連携機能を実装した「デスクトップセキュリティソフトウェアは、国内初となります。 ２．Windows2003サーバ用電子証明書大量発行API Microsoft社のWindwos2003サーバに無償添付されるMicrosoft-CAを用いて、PKCS#12ファイル形式で公開鍵電子証明書と秘密鍵を一括生成するものです。 ＊Microsoft-CAには、公開鍵電子証明書の一括生成機能がない為。 ３．端末認証機能 クライアントPCにおけるネットワーク型バックアップシステムにおいて、ログインしているクライアントPCが「ベース(=自分の通常利用するPC)」であるかどうかを識別・認証し、バックアップファイルのリストア先へのアクセス制御を行います。

企業名（及び略称）	日本高信頼システム株式会社（ＪＴＳ）
代表者氏名	澤田　栄浩
所在地（郵便番号及び住所）	〒112-0004　東京都文京区後楽2-3-25
関連部署名及び電話番号	03-3868-8921
ＵＲＬ	http://www.jtsl.co.jp

対象技術	技術開発状況
その他認証技術	企業ポリシーからシステムポリシーを作成し、システムポリシーをＯＳ（カーネル）に認識させることにより、たとえアプリケーションやＯＳのサービスプログラム（ftpやtelnetを含む）にセキュリティホールが存在しても脆弱性を対象とした攻撃からシステムを強固に守る強制アクセス制御技術。 システム内でSUID攻撃等を用いてシステム管理者特権を手に入れ、システムを思いのままにコントロールできるようになることを防ぐ、特権制御技術。 強制アクセス制御や特権制御を実現するために必要な機密ラベルを加工する権限を持つセキュリティ管理者の不正を抑制するために、認証を２人以上で構成させるDualLock技術。

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 (2004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)と、装置自信が防御を行うネットワーク型の侵入検知防御システム(IPS)を製品開発しています。 製品開発項目は以下のとおりです。 ・管理装置とセンサで構成するシステム ＜センサ＞ ・専用ボード搭載のアプライアンスでIDS、IPSをラインアップ ・駆動部であるHDDをICメモリ化することによる耐環境性、耐久性の向上 ＜管理装置＞ ・完全日本語対応GUIを搭載した専用ソフトウェアにより操作性のよい快適な動作を実現 ・複数コンソールの接続が可能であり、大規模ネットワークにも対応可能

（別添３）

【大学】

大学名	広島大学　情報メディア教育研究センター
所在地（郵便番号及び住所）	〒739-8511　東広島市鏡山1-4-2
関連部署名及び電話番号	情報化推進部情報企画グループ　082-424-5769
ＵＲＬ　http://www.media.hiroshima-u.ac.jp/	
対象技術	技術開発状況
ネットワーク	大学内等において認証付情報コンセント機能を手軽に提供する。本製品は広島大学が独自に研究・開発したPortGuardシステムのコンセプトを元に、（株）ネットスプリングにて開発した製品である。

【企業】

企業名（及び略称）	株式会社インテリジェントウェイブ
所在地（郵便番号及び住所）	〒135-0042　東京都江東区木場5-12-8　木場グリーンパークビル
関連部署名及び電話番号	セキュリティシステム事業部　03-5620-1051
ＵＲＬ	http://www.iwi.co.jp/

対象技術	技術開発状況
サーバ クライアント データ 施設	ＣＷＡＴはオーガナイゼーションモニタ（統合監視コンソール）、セグメントディフェンスコントローラ（ネットワーク監視）、アンノウンターミナルディフェンスコントローラ（未登録端末監視）、オペレーションディフェンスコントローラ（オペレーション監視）で構成された内部情報漏洩対策システムです。ＣＷＡＴは、ネットワーク情報を監視するだけではなく、外部に持ち出されるモバイルＰＣやクライアントＰＣでのＦＤ、ＣＤへの書き出し、外部接続バス経由での未登録端末の直接接続も監視できる機能を持っています。更に、操作員のポリシーに違反した挙動や、普段と著しく異なった挙動を監視することができます。

企業名（及び略称）	株式会社エス･エス･アイ・ジェイ
所在地（郵便番号及び住所）	〒105-0021　東京都港区東新橋二丁目2番8号
関連部署名及び電話番号	情報セキュリティ対策支援部　03-3432-1885
ＵＲＬ	http://www.ssij.co.jp/

対象技術	技術開発状況
ネットワーク サーバ サービス	QualysGuardおよびAppscanを使用した２種類の脆弱性検査サービス。 ① Ｎ-ＶＡＩＳネットワーク脆弱性検査サービス。Qualys社のQualysGuardによる検査を行ない、平易な日本語で記述された判り易い形式でのレポートを提出するサービス。 ② W-ＶＡＩＳ Webアプリケーション脆弱性検査サービス。ＳＡＮＣＴＵＭ社のAppscanとエンジニアによる検査結果から脆弱性のリスク分析と対処法の詳細説明など顧客向けにカスタマイズされたレポートを提出するサービス。

企業名（及び略称）	株式会社エス･エス･アイ・ジェイ
所在地（郵便番号及び住所）	105-0021　東京都港区東新橋二丁目2番8号
関連部署名及び電話番号	情報セキュリティ対策支援部　03-3432-1885
ＵＲＬ	http://www.ssij.co.jp/

対象技術	技術開発状況
サービス	Ｐマーク、ＩＳＭＳ適合性評価制度等の認証取得を目標として社員のモチベーションアップ等により企業全体のクオリティ向上を支援する。

企業名（及び略称）	株式会社エス･エス･アイ・ジェイ
所在地（郵便番号及び住所）	105-0021　東京都港区東新橋二丁目2番8号
関連部署名及び電話番号	情報セキュリティ対策支援部　03-3432-1885
ＵＲＬ	http://www.ssij.co.jp/

対象技術	技術開発状況
サービス	情報セキュリティ管理責任者、内部監査人教育およびユーザのリテラシー向上のための情報セキュリティに関する教育。

企業名（及び略称）	株式会社エス･エス･アイ・ジェイ
所在地（郵便番号及び住所）	105-0021　東京都港区東新橋二丁目2番8号
関連部署名及び電話番号	情報セキュリティ対策支援部　03-3432-1885
ＵＲＬ	http://www.ssij.co.jp/

対象技術	技術開発状況
サービス	経済産業省情報セキュリティ監査制度を基準にし、お客様に合わせたカスタマイズ監査。

企業名（及び略称）	ＮＥＣシステムテクノロジー株式会社
所在地（郵便番号及び住所）	〒211-8666　川崎市中原区下沼部1753 ＮＥＣ玉川ルネッサンスシテイ
関連部署名及び電話番号	企画部　044-435-5648
ＵＲＬ	http://www.necst.co.jp/

対象技術	技術開発状況
クライアント	・ USBメモリをPCの鍵として使う→PCに差し込まれているとき以外はPCがロックされる。 ・ USBメモリへファイルを格納すると地頭的に暗号化される→USBメモリを差し込んでいるPCではPCのハードディスクも暗号化可能。

企業名（及び略称）	ＮＥＣネクサソリューションズ株式会社
所在地（郵便番号及び住所）	〒108-8338　東京都港区三田1-4-28　三田国際ビル
関連部署名及び電話番号	セキュリティビジネスセンター　03-5730-5256
ＵＲＬ	http://www.nec-nexs.com/

対象技術	技術開発状況
サーバ サービス	Ｗｅｂアプリケーションのソースを提供いただき、脆弱性を検出するサービス。人的ミスやリソースに依存しないように、ソースをスキャンしてオブジェクトレベルに分離する解析補助ツールを開発した。対象はＡＳＰ、ＪＳＰ、ＪａｖａＳｃｒｉｐｔなどのスクリプト系と、ＶＢ、ＣｔｔなどのＣＯＭ系言語にも対応。

企業名（及び略称）	ＮＥＣネクサソリューションズ株式会社
所在地（郵便番号及び住所）	〒108-8338　東京都港区三田1-4-28　三田国際ビル
関連部署名及び電話番号	セキュリティビジネスセンター　03-5730-5256
ＵＲＬ	http://www.nec-nexs.com/

対象技術	技術開発状況
サーバ データ サービス	弊社データセンターとのハウジングユーザー向けセキュリティサービスとして提供されているサーバ防御用ソフトウェア。Ｗｉｎｄｏｗｓサーバ特にＷｅｂサーバの防御を目的とする機能は以下の４つ。 ・ ＷｅｂＡｌｅｒｔｅｒ・・・ＨＴＴＰ構文解析を行ない、不正アクセスを検知遮断。ＩＳＡＰＩフィルタ、ＩＳＡＰＩＥｘｔｅｎｓｉｏｎ技術。 ・ ＳｙｓｔｅｍＲｅｃｏｖｅｒ・・・コンテンツの改ざん検知と即時復旧。 ・ ＬｏｇＳｃａｎ・・・メールサーバとＷｅｂサーバのログを解析し、レポートを生成。 ・ ＰｅｒｍｉｓｓｉｏｎＣｏｌｌｅｃｔｏｒ・・・ＩＩＳのアクセス権やオブジェクトを監視。ミスオペレーションを即時通知。

企業名（及び略称）	株式会社ＮＴＴドコモ
所在地（郵便番号及び住所）	〒100-6150　東京都千代田区永田町2-11-1　山王パークタワー
関連部署名及び電話番号	03-5156-1111(代)
ＵＲＬ	http://www.nttdocomo.co.jp/

対象技術	技術開発状況
クライアント 通信情報	従来のＩＤ／パスワード認証に代わる公開鍵暗号基盤（ＰＫＩ）技術を使ったＦＯＭＡの電子認証サービス。ドコモから取得したユーザ証明書を利用することによりＦＯＭＡまたはＰＣとＦｉｒｓｔＰａｓｓ対応サイトとの相田でＳＳＬ相互認証を行う。ＦｉｒｓｔＰａｓｓにより、「なりすまし」などのセキュリティ被害に遭いにくくなり、さらに安全で信頼性のあるデータ通信が可能となる。

企業名（及び略称）　　沖電気工業株式会社	
所在地（郵便番号及び住所）〒105-8460　東京都港区虎ノ門1-7-12	
関連部署名及び電話番号　　03-3501-3111	
ＵＲＬ　http://www.oki.com/jp/	
対象技術	技術開発状況
ネットワーク サーバ クライアント	異常トラフィック監視システムはトラフィックの状況を監視するプローブ装置と、プローブ装置を管理するマネージャ装置から構成され、最大８台までのプローブ装置を配置することができます。（製品はアプライアンスにて提供）異常トラフィック監視システムには、アプケーション別のトラフィック計測機能、異常トラフィック検出機能、アクション機能があり、ネットワークトラフィックの統計画面から簡易な操作でトラフィック調査が行えるだけでなく、ネットワーク感染型ワームの感染活動を検出することが可能です。本製品はFast Ethernet対応のスタンダードモデルとGigabit Ethernet対応のハイエンドモデルを揃えました。

企業名（及び略称）　　沖電気工業株式会社	
所在地（郵便番号及び住所）〒105-8460　東京都港区虎ノ門1-7-12	
関連部署名及び電話番号　　03-3501-3111	
ＵＲＬ　http://www.oki.com/jp/	
対象技術	技術開発状況
サーバ 情報通信 その他	「eすぷりっと便」は企業内外を問わず、電子メールやCD-ROMなどのメディア形式で受け渡しされている個人情報・機密情報を紛失・盗難から守ります。情報は紛失や盗難が発生した場合、たとえ暗号化されていても情報流失と見なされます。「eすぷりっと便」は大事な情報を秘密分散法（電子割符）により、分割・暗号化し、異なる経路で相手に配送することで安全・確実な情報配送を実現します。

企業名（及び略称）　　沖電気工業株式会社	
所在地（郵便番号及び住所）〒105-8460　東京都港区虎ノ門1-7-12	
関連部署名及び電話番号　　03-3501-3111	
ＵＲＬ　http://www.oki.com/jp/	
対象技術	技術開発状況
クライアント 施設	アイリスパスは、目のアイリス（虹彩）模様が個人毎に異なることを利用して、個人を認証する装置です。虹彩模様は、生後２年程度で安定し、その後一生変わらないと言われていることと、非常に複雑な模様で形成されていることから、高精度な個人認証が可能です。情報セキュリティ向け認証装置であるアイリスパス-hは、ＰＣとＶＳＢで接続され、ＰＣやネットワークへのログオン時にアイリス認証を行う装置です。入退室管理向け認証装置であるアイリスパス-WGは、重要な施設への入退室をアイリス認証によって管理するシステムです。

企業名（及び略称）	コンピュータ・アソシエイツ株式会社
所在地（郵便番号及び住所）	〒163-0439　東京都新宿区西新宿2-1-1　新三井ビル39階
関連部署名及び電話番号	
ＵＲＬ	http://www.caj.co.jp/

対象技術	技術開発状況
ネットワーク サーバ データ	サーバ上のリソース（ファイルやプログラム等）に対するアクセス制御を実現する製品。役割に応じた適切なアクセス権限を設定（適切なユーザに適切な権限を与える）ことが可能。正常アクセスも含む追跡可能な監査ログを取得する。“だれが”、“いつ”、“どの端末から”、“何のツールを使って”、“どのリソースへ”といった４Ｗ１Ｈに基づいたログを出力。ログは誰も改ざんできない仕組みとなっている。

企業名（及び略称）	コンピュータ・アソシエイツ株式会社
所在地（郵便番号及び住所）	〒163-0439　東京都新宿区西新宿2-1-1　新三井ビル39階
関連部署名及び電話番号	
ＵＲＬ	http://www.caj.co.jp/

対象技術	技術開発状況
ネットワーク サーバ クライアント 通信情報	迷惑メール、情報漏洩、eメールに起因する法的責任、ウィルス、悪意あるコンテンツ・プログラム、不快なコンテンツなど、様々な脅威からＰＣを保護する統合コンテンツセキュリティソリューション。ビジネス主導型ポリシーエンジン、機密情報のフィルタリング、警告とアクションの自動化、ポリシーの一元管理、迷惑メールとＵＲＬアクセスに関する独自のルール作成など、コンテンツセキュリティに重要な機能を豊富に備えている。

企業名（及び略称）	コンピュータ・アソシエイツ株式会社
所在地（郵便番号及び住所）	〒163-0439　東京都新宿区西新宿2-1-1　新三井ビル39階
関連部署名及び電話番号	
ＵＲＬ	http://www.caj.co.jp/

対象技術	技術開発状況
サーバ クライアント	現アンチウィルスソフトだけでは防ぐことができない、スパイウェア、ハッカーツール、キーロガー、ＤｏＳといった攻撃／侵入を検知、対応をリアルタイムで実現します。

企業名（及び略称）　　コンピュータ・アソシエイツ株式会社	
所在地（郵便番号及び住所）〒163-0439　東京都新宿区西新宿2-1-1　新三井ビル39階	
関連部署名及び電話番号	
ＵＲＬ　http://www.caj.co.jp/	
対象技術	技術開発状況
	ＩＤＳ製品。包括的なネットワーク保護機能を提供し、被害を未然に防ぐプロアクティブな防御機能を装備。高性能でしかも使いやすい製品。広範なレベルの監視、侵入／攻撃の検知、不正なＵＲＬの検出、遮断、警告、ロギング、そして単一のソフトウェアでこれらのリアルタイム応答機能が利用可。

企業名（及び略称）　　コンピュータ・アソシエイツ株式会社	
所在地（郵便番号及び住所）〒163-0439　東京都新宿区西新宿2-1-1　新三井ビル39階	
関連部署名及び電話番号	
ＵＲＬ　http://www.caj.co.jp/	
対象技術	技術開発状況
その他	企業内の様々なＯＳ、セキュリティ製品から発生する情報を一元管理し、複数のイベントより問題の根源となるセキュリティインシデントを分析、また企業レベルでのリスク診断に役立てることができる。セキュリティ情報管理を実現する。セキュリティ業務にかかる現在のコストを削減しながら、様々なリスクに晒される可能性を最小限に低減できるようになる。

企業名（及び略称）　　コンピュータ・アソシエイツ株式会社	
所在地（郵便番号及び住所）〒163-0439　東京都新宿区西新宿2-1-1　新三井ビル39階	
関連部署名及び電話番号	
ＵＲＬ　http://www.caj.co.jp/	
対象技術	技術開発状況
ネットワーク サーバ クライアント	サーバ、クライアントＰＣ、グループウェア、ゲートウェイまでウィルスの脅威から保護するアンチウィルスソリューション。２つのウィルススキャニングエンジンでウィルスを完全ブロック。特に企業での利用を前提にして管理機能がすぐれており、運用や導入に大きなメリットとなる。

企業名（及び略称）　　サイバーソリューション株式会社	
所在地（郵便番号及び住所）	
関連部署名及び電話番号	
ＵＲＬ	
対象技術	技術開発状況
ネットワーク サーバ クライアント サービス	・ＩＤＣと監視。・ネットワーク(Ｇｌｏｂａｌ,Ｐｒｉｖａｔｅ),サーバの死活、状態監視と対応（ディスパッチレベル） ・ウィルス対応状況の監視と通知。・情報漏えい監視ツールの販売。

企業名（及び略称）　　サン・マイクロシステムズ株式会社	
所在地（郵便番号及び住所）〒158-8633　東京都世田谷区用賀4-10-1	
関連部署名及び電話番号　　e-japan営業開発本部　03-4232-2701	
ＵＲＬ　　http://jp.sun.com/	
対象技術	技術開発状況
ネットワーク サーバ クライアント 通信情報 データ	ＳｕｎＳｃｒｅｅｎ　Ｎｅｔは、アクセス制御や、認証、ネットデータの暗号化などを行う汎用的な全社向けファイアウォールシステムです。ＳｕｎＳｃｒｅｅｎ　Ｓｅｃｕｒｅ　Ｎｅｔには、ネットワークのアクセス制御を行うルールベースの動的なパケットフィルタリングエンジンと暗号化/認証エンジンがあります。暗号化/認証エンジンに公開鍵暗号化技術を統合することにより、安全な仮想プライベートネットワーク（ＶＰＮ）ゲートウェイを作成できます。

企業名（及び略称）　　サン・マイクロシステムズ株式会社	
所在地（郵便番号及び住所）〒158-8633　東京都世田谷区用賀4-10-1	
関連部署名及び電話番号　　e-japan営業開発本部　03-4232-2701	
ＵＲＬ　　http://jp.sun.com/	
対象技術	技術開発状況
ネットワーク サーバ クライアント 通信情報 データ	高レベルのプライバシー、追跡可能性の向上、セキュリティ違反リスクの軽減を実現し、政府関係機関、情報関係機関、およびセキュリティ関係機関での実績を持ち、金融、健康管理、小売などの業界で足場を固めたＴｒｕｓｔｅｄ　Ｓｏｌａｒｉｓ　Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ（ＯＳ）は、商用グレードのＯＳへのセキュリティの組み込みを実現します。Ｔｒｕｓｔｅｄ　Ｓｏｌａｒｉｓ　ＯＳを使用することによって、デスクトップユーザーからデータセンターのユーザーまでが、ネットワークのセキュリティリスクを軽減し、セキュリティの信頼性をさらに高めることができます。

企業名（及び略称）　　サン・マイクロシステムズ株式会社	
所在地（郵便番号及び住所）〒158-8633　東京都世田谷区用賀4-10-1	
関連部署名及び電話番号　　e-japan営業開発本部　03-4232-2701	
URL　http://jp.sun.com/	
対象技術	技術開発状況
ネットワーク サーバ クライアント 通信情報 データ	Ｓｏｌａｒｉｓ　10はエンタープライズを異なったレベルで保護できる。先進的なセキュリティ機能を備えています。このセキュリティ・システムは、外部からの悪意を持ったアタックや、内部からの不正なデータ・アクセスを防ぎます。再設計された暗号化フレームワークは、ハードウェアによる暗号化が可能な場合は自動的にそれを選択することで最適な暗号化メソドを選択し、柔軟な管理を実現します。Ｐｒｏｃｅｓｓ Ｒｉｇｈｔｓ　Ｍａｎａｇｅｍｅｎｔコンポーネントが、どのユーザをどのプロセスに対し、何時、どのような権限を与えるのか詳細な制御を可能にします。

企業名（及び略称）　　サン・マイクロシステムズ株式会社	
所在地（郵便番号及び住所）〒158-8633　東京都世田谷区用賀4-10-1	
関連部署名及び電話番号　　e-japan営業開発本部　03-4232-2701	
URL　http://jp.sun.com/	
対象技術	技術開発状況
サーバ 通信情報 データ	イントラネットとエクストラネットのアクセス制御が可能にする。オープン・スタンダード・ベースのアクセス・マネージャ。Ｓｕｎ　Ｊａｖａ　Ｓｙｓｔｅｍ　Ａｃｃｅｓｓ　Ｍａｎａｇｅｒは、企業の内側からもとより、B2B（ｂｕｓｉｎｅｓｓ－ｔｏ－ｂｕｓｉｎｅｓｓ）のバリュー・チェーン全体から、企業のＷｅｂアプリケーションへのアクセスを可能にするセキュリティ基盤です。オープンなスタンダード・ベースの認証機構とポリシー・ベースの承認を実現する、統合フレームワークを提供します。信頼性の高いネットワークをパートナー/納入先/顧客に提供し、リレーションシップを深めることで増収基盤を構築するだけでなくＳＳＯ（シングルサインオン：Ｓｉｎｇｌｅ　Ｓｉｇｎ－ｏｎ）を実現し、現代のニーズとこの先成長していくビジネス・ニーズに応えることが可能で、基本的なアイデンティティ情報とアプリケーション情報をセキュアに提供します。

企業名（及び略称）　　サン・マイクロシステムズ株式会社	
所在地（郵便番号及び住所）〒158-8633　東京都世田谷区用賀4-10-1	
関連部署名及び電話番号　　e-japan営業開発本部　03-4232-2701	
URL　http://jp.sun.com/	
対象技術	技術開発状況
サーバ 通信情報 データ	個人情報保護をはじめとして、エンタープライズレベルでの各種情報管理が求められる中、Ｓｕｎ　Ｊａｖａ　Ｓｙｓｔｅｍ　Ｉｄｅｎｔｉｔｙ　Ｍａｎａｇｅｒにより、既存のシステムに対するシステム変更を迫ることなく、高い安全性と運用性をもったアイデンティティ・マネジメントを行なうことが可能となります。

企業名（及び略称）	サン・マイクロシステムズ株式会社
所在地（郵便番号及び住所）	〒158-8633　東京都世田谷区用賀4-10-1
関連部署名及び電話番号	e-japan営業開発本部　03-4232-2701
URL	http://jp.sun.com/

対象技術	技術開発状況
ネットワーク サーバ 通信情報 データ	Ｓｕｎ　Ｃｒｙｐｔｏ　ＡｃｃｅｌｅｒａｔｏｒはＥコマース等で標準的に使用されるＳＳＬ　トランザクション処理を高速化するＰＣＩ拡張カードです。Ｓｕｎ　Ｃｒｙｐｔｏ　Ａｃｃｅｌｅｒａｔｏｒ１００００は、ＳＳＬ計算処理専用のコプロセッサとして動作し、ＳＳＬ処理をホストＣＰＵから切り離し（ＣＰＵオフロード）ホストＣＰＵの負荷を軽減します。

企業名（及び略称）	サン・マイクロシステムズ株式会社
所在地（郵便番号及び住所）	〒158-8633　東京都世田谷区用賀4-10-1
関連部署名及び電話番号	e-japan営業開発本部　03-4232-2701
URL	http://jp.sun.com/

対象技術	技術開発状況
ネットワーク サーバ 通信情報 データ	Ｓｕｎ　Ｆｉｒｅ　Ｂ10ｐ　ＳＳＬプロキシ・ブレードは、Ｓｕｎ　Ｆｉｒｅブレードプラットフォームの構成要素として、物理的にも機能的にもシームレスに統合されます。ＳＳＬオフローディングのためにカスタムＡＳＩＣとファームウェアで実装されたＳｕｎ　Ｆｉｒｅ　Ｂ10ｐ　ＳＳＬプロキシ・ブレードは、それぞれのサーバのホストＣＰＵによるＳＳＬ処理と比較して、最大１０倍のＳＳＬトランザクション処理能力を提供します。同時に、ホストＣＰＵのすべてのリソースを、本来のサービス提供に利用できるようになります。

企業名（及び略称）	サン・マイクロシステムズ株式会社
所在地（郵便番号及び住所）	〒158-8633　東京都世田谷区用賀4-10-1
関連部署名及び電話番号	e-japan営業開発本部　03-4232-2701
URL	http://jp.sun.com/

対象技術	技術開発状況
ネットワーク サーバ 通信情報 データ	Ｓｕｎ　Ｎ２０００　Ｓｅｒｉｅｓ　Ｓｅｃｕｒｅ　Ａｐｐｌｉｃａｔｉｏｎ　Ｓｗｉｔｃｈは、効率的なリソース運用/サービス統合/先進のコスト・パフォーマンスで、企業のセキュアなネットワーク・コンピューティング環境構築に伴うコストの複雑性を解消します。Ｓｕｎ　Ｎ２０００　Ｓｅｒｉｅｓ　Ｓｅｃｕｒｅ　Ａｐｐｌｉｃａｔｉｏｎ　Ｓｗｉｔｃｈには、ワイヤ・スピードＧｉｇａｂｉｔアプリケーション・スイッチ/チップ・レベルの組込みセキュリティ／リソースの動的な仮想化技術が統合されています。一つのシステムにこれら技術が統合されているので､既存サーバの負荷分散/ＳＳＬの高速化／帯域幅管理などを実現するために、アプライアンスなど独自機能を提供する高価なコンポーネントを必要とせず、大幅なＴＣＯ削減や分散型コンピューティング環境の管理を簡素化します。

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）	大阪市淀川区西中島5丁目5番15号
関連部署名及び電話番号	管理部　06-6309-7600
ＵＲＬ	http://www.jscom.co.jp/

対象技術	技術開発状況
サーバ クライアント サービス	外部より侵入するウィルスから企業ＬＡＮための包括的高速アンチウィルスゲートウェイサーバーであり、フィンランドのエフ・セキュア社からソフト提供を受け開発いたしました。

企業名（及び略称）	シスコシステムズ株式会社
所在地（郵便番号及び住所）	〒107-0052　東京都港区赤坂2-14-27　国際新赤坂ビル東館
関連部署名及び電話番号	アライアンス&テクノロジー　03-5549-6500
ＵＲＬ	http://www.cisco.com/jp/

対象技術	技術開発状況
ネットワーク サーバ	強固なエンタープライズクラスのネットワークセキュリティサービスを実現する。ファイアウォール、ＶＰＮ、侵入保護危機です。

企業名（及び略称）	シスコシステムズ株式会社
所在地（郵便番号及び住所）	〒107-0052　東京都港区赤坂2-14-27　国際新赤坂ビル東館
関連部署名及び電話番号	アライアンス&テクノロジー　03-5549-6500
ＵＲＬ	http://www.cisco.com/jp/

対象技術	技術開発状況
通信情報	リモートアクセスＶＰＮを実現するプラットフォームです。

企業名（及び略称）	シスコシステムズ株式会社
所在地（郵便番号及び住所）	〒107-0052　東京都港区赤坂2-14-27　国際新赤坂ビル東館
関連部署名及び電話番号	アライアンス&テクノロジー　03-5549-6500
URL	http://www.cisco.com/jp/

対象技術	技術開発状況
ネットワーク サーバ	ネットワーク全体に透過的な保護を提供可能で、ネットワークを通過する不正で悪意のある行為からネットワークを保護します。

企業名（及び略称）	シスコシステムズ株式会社
所在地（郵便番号及び住所）	〒107-0052　東京都港区赤坂2-14-27　国際新赤坂ビル東館
関連部署名及び電話番号	アライアンス&テクノロジー　03-5549-6500
URL	http://www.cisco.com/jp/

対象技術	技術開発状況
サーバ クライアント	CSAはエンドユーザーとも呼ばれるサーバおよびクライアントコンピュータに、侵入保護の機能を提供します。

企業名（及び略称）	株式会社シマンテック
所在地（郵便番号及び住所）	〒150-0031　東京都渋谷区桜丘町20-1　渋谷インフォスタワー　17階
関連部署名及び電話番号	法人営業事業部　03-5457-5330
URL	http://www.symantec.co.jp/

対象技術	技術開発状況
ネットワーク サーバ クライアント 通信情報	Symantec Enterprise firewallは独自のハイブリットアーキテクチャを採用しており、企業ネットワークを様々なネットワーク攻撃力で不正なアクセスから強固に、そしてプロアクティブに保護し、企業の情報資産の活用と保護を促進します。主な機能 ・ アプリケーションプロキシをそなえたフルインスペクションFW。 ・ プロキシセキュアドVPNによる安全性の高いIPSec VPNの提供。 ・ クラスター構成による冗長化と負荷分散が可能。 ・ Webベースの容易な管理。

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　　03-5114-8224(代)	
ＵＲＬ　http://www.securecomputing.com/	
対象技術	技術開発状況
サーバ	ワンタイムパスワードの草分け的存在であり、日本でも10年以上の間に渡る販売実績を持つ。独特の回数同期式と呼ばれる方式によって、時間同期式を採用している他社製品のユーザーが悩まされるような時間のずれがないのが、最大の特徴である。

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　　03-5114-8224(代)	
ＵＲＬ　http://www.securecomputing.com/	
対象技術	技術開発状況
ネットワーク	商用フィアウォールの草分け的存在であり､その一号機は平成7年の米国家安全保障局への納入実績を持つ。独自のType　ｅｎｆｏｒｃｅｍｏｎｔ　（ＳＥ　Ｌｉｎｕｘと同じ仕組み）と呼ばれる技術により、クラックが極めて困難なシステムを実現しており、発売以来、今だにクラックされた実績がない。またアプリケーションゲートウェイ方式をその最初のバージョンより採用しており、一般に「ファイアウォールで防げない」と言われる攻撃を防ぐのも特徴の一つである。

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　　03-5114-8224(代)	
ＵＲＬ　http://www.securecomputing.com/	
対象技術	技術開発状況
クライアント その他	ｗｅｂの適正な利用文化を組織に根付かせることを狙いにした製品であり､62のカテゴリ別に約600万のサイトの情報を格納したデータベースに基づいて業務上、必要であるか否かの判断を下し、アクセス禁止等の処置を行う。近年ではｗｅｂアクセスで感染するウィルスの出現や、いわゆるフィッシングなどの多発により業務の効率向上以外にもセキュリティという観点からも注目が高まっている。

企業名（及び略称）	セコムトラストネット株式会社
所在地（郵便番号及び住所）	〒150-0001　東京都渋谷区神宮前1-5-1 セコム本社ビル
関連部署名及び電話番号	事業推進部　03-5775-8661
ＵＲＬ	http://www.secomtrust.net/

対象技術	技術開発状況
クライアント データ 施設	入退室管理などのフィジカルセキュリティと、高度な認証技術によるサイバーセキュリティを１枚のＩＣカードで同時に実現するものであり、確実な本人認証により、内部情報漏洩対策にも効果を発揮している。

企業名（及び略称）	セコムトラストネット株式会社
所在地（郵便番号及び住所）	〒150-0001　東京都渋谷区神宮前1-5-1 セコム本社ビル
関連部署名及び電話番号	事業推進部　03-5775-8661
ＵＲＬ	http://www.secomtrust.net/

対象技術	技術開発状況
サーバ データ 施設	ユーザサイトに設置する小型データーセンター。高品質部材のメーカー等を中心に導入が進んでいる。

企業名（及び略称）	セコムトラストネット株式会社
所在地（郵便番号及び住所）	〒150-0001　東京都渋谷区神宮前1-5-1 セコム本社ビル
関連部署名及び電話番号	事業推進部　03-5775-8661
ＵＲＬ	http://www.secomtrust.net/

対象技術	技術開発状況
サービス	セコムのノウハウを結集した堅牢な設備面のセキュリティに加え、サイバーセキュリティまでをオールインワンで標準装備し、お客様のＩＴ環境にフィジカル＆サイバーの統合安全対策を提供。

企業名（及び略称）	セコムトラストネット株式会社
所在地（郵便番号及び住所）	〒150-0001　東京都渋谷区神宮前1-5-1 セコム本社ビル
関連部署名及び電話番号	事業推進部　03-5775-8661
ＵＲＬ	http://www.secomtrust.net/

対象技術	技術開発状況
サービス	お客様ネットワークに対する定期的なセキュリティ診断から監視、監視機器の運用までをオールインワンで提供するアウトソーシングサービス。お客様ネットワークに対する様々な不正アクセスを、セキュリティのプロが２４時間３６５日体制で見守り、緊急時には迅速な対応を実施する。

企業名（及び略称）	セコムトラストネット株式会社
所在地（郵便番号及び住所）	〒150-0001　東京都渋谷区神宮前1-5-1 セコム本社ビル
関連部署名及び電話番号	事業推進部　03-5775-8661
ＵＲＬ	http://www.secomtrust.net/

対象技術	技術開発状況
サービス	ウィルス対策のプロフェッショナルが２４時間３６５日体制でウィルスからの攻撃を監視し、お客様の大切なデータやプログラムをウィルスのリスクから守るマネージメントサービス。

企業名（及び略称）	セコムトラストネット株式会社
所在地（郵便番号及び住所）	〒150-0001　東京都渋谷区神宮前1-5-1 セコム本社ビル
関連部署名及び電話番号	事業推進部　03-5775-8661
ＵＲＬ	http://www.secomtrust.net/

対象技術	技術開発状況
サービス	Webサイトの脆弱性を検査する「セキュリティ診断」と、ＳＳＬ通信（暗号化通信）とWebサイトの運営事業体の実在性を証明する「Webサイト（ＳＳＬサーバ）用電子証明書」をパックでご提供するサービス。

企業名（及び略称）	セコムトラストネット株式会社
所在地（郵便番号及び住所）	〒150-0001　東京都渋谷区神宮前1-5-1 セコム本社ビル
関連部署名及び電話番号	事業推進部　03-5775-8661
ＵＲＬ	http://www.secomtrust.net/

対象技術	技術開発状況
サービス	ＳＳＬ通信（暗号化通信）とWebサイトが実在する企業・組織によって運営されていることを証明するWebサーバ用電子証明書発行サービス。

企業名（及び略称）	セコムトラストネット株式会社
所在地（郵便番号及び住所）	〒150-0001　東京都渋谷区神宮前1-5-1 セコム本社ビル
関連部署名及び電話番号	事業推進部　03-5775-8661
ＵＲＬ	http://www.secomtrust.net/

対象技術	技術開発状況
サービス	高度なセキュリティ対策と厳格な運用が実施され、高い信頼性の確保された認証局より、お客様が特定したいユーザ（社員や取引先の担当者など）に対して、インターネット上の身分証明書である「クライアント用電子証明書」を発行するサービス。

企業名（及び略称）	セコムトラストネット株式会社
所在地（郵便番号及び住所）	〒150-0001　東京都渋谷区神宮前1-5-1 セコム本社ビル
関連部署名及び電話番号	事業推進部　03-5775-8661
ＵＲＬ	http://www.secomtrust.net/

対象技術	技術開発状況
サービス	「電子署名及び認証業務に関する法律：平成１２年法律第１０２号」（「電子署名法」といいます）に基づく特定認証業務の認定を取得した電子証明書発行サービス。電子署名法における認証局設備、認証運用規定、証明書ポリシ等の基準をクリアしており、日本国籍を有し且つ日本国内に居住される個人の方に対して、電子証明書を発行。

企業名（及び略称）	セコムトラストネット株式会社
所在地（郵便番号及び住所）	〒150-0001　東京都渋谷区神宮前1-5-1 セコム本社ビル
関連部署名及び電話番号	事業推進部　03-5775-8661
ＵＲＬ	http://www.secomtrust.net/

対象技術	技術開発状況
サービス	お客様社内ネットワークへのＶＰＮアクセスを実現するアウトソーシングサービス。認証に「電子証明書」と「ＵＳＢトークン」を活用することで、強固なセキュリティを提供。

企業名（及び略称）	セコムトラストネット株式会社
所在地（郵便番号及び住所）	〒150-0001　東京都渋谷区神宮前1-5-1 セコム本社ビル
関連部署名及び電話番号	事業推進部　03-5775-8661
ＵＲＬ	http://www.secomtrust.net/

対象技術	技術開発状況
サービス	情報漏洩につながる様々なセキュリティ上の脆弱点を、ヒアリング、現地調査、またネットワーク診断などから分析。重要書類の不正持ち出し、システムへのアクセス制御、ネットワーク上の脆弱性などの対策が適切に講じられているか、セキュリティのプロであるセコムならではの診断を実施。お客様環境において最優先に取り組むべき対策事項をレポートにて提出する。

企業名（及び略称）	セコムトラストネット株式会社
所在地（郵便番号及び住所）	〒150-0001　東京都渋谷区神宮前1-5-1 セコム本社ビル
関連部署名及び電話番号	事業推進部　03-5775-8661
ＵＲＬ	http://www.secomtrust.net/

対象技術	技術開発状況
サービス	セキュリティ診断ツールを使用し、お客様のネットワークに対する脆弱性診断を行い、その結果をセキュリティ診断書で詳細にご報告。弊社からの、セキュリティ診断書及びアドバイスに従って、適切な対応を行なうことで、不正侵入等の脅威を軽減することが可能。

企業名（及び略称）	ソフトバンク･テクノロジー株式会社
所在地（郵便番号及び住所）	〒162-0812　東京都新宿区西五軒町13-1
関連部署名及び電話番号	ブロードバンド・ソリューション事業部　ＳＩ技術部　03-5206-3350
ＵＲＬ	http://www.tech.softbank.co.jp/

対象技術	技術開発状況
クライアント 通信情報 データ サービス	（独）情報通信研究機構が米国・日本において、３つの特許権を保持し、（株）カオスウェアが著作権を保持している世界最速のカオス理論を応用したランダムベクトル生成によるストリーム型暗号アルゴリズムであり、当社は本暗号アルゴリズムの安全性評価および論文発表、アプリケーションへの組み込み型ミドルウェアエンジン「ＶＳＣＡＴ」、ＳＤＫの共同研究開発を行なっています。

企業名（及び略称）	株式会社タイテック
所在地（郵便番号及び住所）	〒457-0071　愛知県名古屋市南区千竈通2丁目13番地1
関連部署名及び電話番号	総務部総務グループ　052-824-7373
ＵＲＬ	http://www.tietech.co.jp/

対象技術	技術開発状況
施設	施設出入口の開施錠権限者を認証する。

企業名（及び略称）	デジタルアーツ株式会社
所在地（郵便番号及び住所）	東京都港区北青山3-6-16 佐阿徳ビル
関連部署名及び電話番号	マーケティング部　03-5485-1330
ＵＲＬ	http://www.daj.co.jp/

対象技術	技術開発状況
その他	インターネットのページをアクセスできるものと、できないものとに分別するｗｅｂフィルタリングソフト。また書き込みやファイルアップロードの制限。あるいは書き込んだり書き込もうとした内容を確認することが可能であり、ｗｅｂ経由の情報漏洩対策が可能。

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	営業部　03-3511-1202
ＵＲＬ	http://www.TopLayer.co.jp/

対象技術	技術開発状況
ネットワーク サーバ	Ａｔｔａｃｋ　Ｍｉｔｉｇａｔｏｒ　ＩＰＳは、不正アクセスや、悪意のあるコンテンツ（ウィルスやワーム、トロイの木馬その他）及びＤｏＳ/ＤＤｏＳなどの量的な攻撃からネットワーク・レベルおよびアプリケーションレベルでの最適なサービスプロテクションを提供する。ＴｉｐＦｉｒｅＴＭＡＳＩＣとＴｏｐｉｎｓｐｅｃｔＴＭ詳細パケット分析アルゴリズムによるハイパフォーマンスなアプリケーション使用基準検査により、重要サーバに対する各種のサイバー攻撃を検知および遮断を行い、サーバに脆弱性が内包されている場合も不正侵入を未然に防ぐ。

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	営業部　03-3511-1202
ＵＲＬ	http://www.TopLayer.co.jp/

対象技術	技術開発状況
ネットワーク クライアント	Ｓｅｃｕｒｅ　Ｃｏｎｔｒｏｌｌｅｒは、ユーザ認証とｖＺＯＮＥ機能によるアクセス制御とポリシーベースのＱｏＳを提供。クオリティ株式会社および株式会社ＰＦＵが提供するソフトウェアとの組み合わせによりＳＰＣソリューション（ＰＣプロファイル認証および検疫）ネットワークを実現。ブリッジ型の機器であり、既存ネットワークの構成変更は不要である。

企業名（及び略称）	日本オラクル株式会社
所在地（郵便番号及び住所）	〒102-0094　東京都千代田区紀尾井町4-1 ニューオータニガーデンコート
関連部署名及び電話番号	マーケティング本部　03-5213-6666
ＵＲＬ	http://www.oracle.co.jp/

対象技術	技術開発状況
通信情報 データ	RDBMS内部に格納された機密性のある情報を保護するための各種機能があります。（一部オプション製品あり）

企業名（及び略称）	日本ビジネスコンピュータ株式会社
所在地（郵便番号及び住所）	〒144-8721　東京都大田区蒲田5-37-1 ニッセイアロマスクエア　15F
関連部署名及び電話番号	サービスマーケティング　ＳＣ&NW企画　03-5714-5144
ＵＲＬ	http://www.jbcc.co.jp/

対象技術	技術開発状況
サービス	ゲートウェイウィルス対策、ハードウェアレンタル、運用管理サービス、保守サービス、ログレポートサービス（全てをセットにしたお求めやすいセキュリティ・マネジメントサービスです。

企業名（及び略称）	株式会社日立情報システムズ
所在地（郵便番号及び住所）	〒150-8540　東京都渋谷区道玄坂1-16-5
関連部署名及び電話番号	社長室　広報・ＩＲグループ　03-3464-5073
ＵＲＬ	http://www.hitachijoho.com/

対象技術	技術開発状況
ネットワーク サーバ クライアント 通信情報 データ サービス	認証機能とアクセス制御機能を組み合わせた認証基盤ソフトウェア。 特徴： ・ Felica、PUPPY、認証トークン、ICカード等の認証媒体を使用し安全な認証を実現。 ・ VPN通信機能により盗聴や改ざんから通信内容を保護。 ・ グループアクセス制御による情報アクセス制御。

企業名（及び略称）	株式会社日立情報システムズ
所在地（郵便番号及び住所）	〒150-8540　東京都渋谷区道玄坂1-16-5
関連部署名及び電話番号	社長室　広報・ＩＲグループ　03-3464-5073
ＵＲＬ	http://www.hitachijoho.com/

対象技術	技術開発状況
通信情報 クライアント データ サービス	私的デジタル証明書の発行と証明書の管理を行う。 ・ 発行するデジタル証明書は企業内、庁内等で有効な私的証明書。 ・ 証明書の有効期限は自由に指定。 ・ 証明書紛失時の回復も可能。 ・ 認証局及び証明書のCPS作成は別サービス。

企業名（及び略称）	株式会社日立情報システムズ
所在地（郵便番号及び住所）	〒150-8540　東京都渋谷区道玄坂1-16-5
関連部署名及び電話番号	社長室　広報・ＩＲグループ　03-3464-5073
ＵＲＬ	http://www.hitachijoho.com/

対象技術	技術開発状況
サーバ 通信情報 データ その他 サービス	・イントラサーバのログイン情報であるUid及びPWの一元管理と各サーバが持つディレクトリへの反映を自動的に行う。認証基盤のソフトウェア。 特徴： ・ 市場にある各種ディレクトリと同期が可能。 ・ uID及びPWの変更等の内容がリアルタイムに各サーバのディレクトリへ反映。 ・ 既存のuID及びPW、PKIを適用した認証。

企業名（及び略称）	日立ソフトウェアエンジニアリング株式会社
所在地（郵便番号及び住所）	〒140-0002　東京都品川区東品川4-12-7
関連部署名及び電話番号	ソリューション企画本部　03-5780-2030
ＵＲＬ	http://hitachisoft.jp/

対象技術	技術開発状況
クライアント データ	秘文はクライアントＰＣからの情報漏洩防止を行ないます。基本的にはＰＣにインストールして活用します。そして更にサーバを組み合わせる事により、セキュリティの強度を上げますが、その際にネットワークにつながるＰＣの各アクセス権限を設定し、これをサーバで管理運用します。

企業名（及び略称）	ファルコンシステムコンサルティング株式会社
所在地（郵便番号及び住所）	〒101-0041　千代田区神田須田町2-2-2
関連部署名及び電話番号	マーケティング本部　03-5209-1411
ＵＲＬ	http://www.falconsc.com/

対象技術	技術開発状況
ネットワーク サーバ	Ｗｉｓｅ　Ｐｏｉｎｔの主な機能は独自方式の認証。Ｗｅｂアプリケーションに対するシングルサインオン、アクセスコントロール等の機能を持っております。特に認証方式についいぇは多種の認証方式（Ｊパスワード、マトリクスコード、イメージマトリクス、携帯電話ＩＤ認証）を持っております。

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　大阪市中央区城見2-2-53　大阪東京海上日動ビル
関連部署名及び電話番号	ソリューション統括部　06-6949-0561
ＵＲＬ	http://www.kcn.fujitsu.com/

対象技術	技術開発状況
データ	アクセスコントロールを実装する方法として、クライアントやサーバ、ゲートウェイなどに規制機能を持たせることが一般的であるが、本製品は、クライアント利用者に情報セキュリティポリシーを正しく理解させ、自発的なセキュリティ保全行動を促す事を目的として、以下のようなＰＤＳＡサイクルで運用されることを特徴とする。 ① 情報セキュリティポリシーの策定とリスク許容値の設定（Ｐｌａｎ） ② クライアントの日々の運用状態の監視と記録（Ｄｏ） ③ リスク許容値を超える利用者の抽出とポリシー理解度確認テストの実施（Ｃｈｅｃｋ） ④ 基準に満たない利用者の再教育、アクセス権制限など（Ａｃｔｉｏｎ） システム構成ＰｏｌｉｃｙＧｕａｒｄｉａｎサーバ：ＲｅｄＨａｔＬｉｎｕｘ9、クライアント：Ｗｉｎｄｏｕｗｓ2000/ＸＰ　ＩＥ6.0　ＳＰ2以上

企業名（及び略称）	富士通サポートアンドサービス株式会社
所在地（郵便番号及び住所）	
関連部署名及び電話番号	
ＵＲＬ	

対象技術	技術開発状況
サービス	クライアントサーバー型式のシステムで、サーバーでの一元管理を複数バイオ、マルチベンダー機能を取り入れたバイオ認証システム。さらに業務システムにタイミングフリーで読み込めるAPIをCXSから取り揃えています。

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）	〒211-6063　川崎市中原区小杉町1-403
関連部署名及び電話番号	
ＵＲＬ	http://www.ssl.fujitsu.com/

対象技術	技術開発状況
サーバ クライアント データ	ＰＣ/Ｓａｆｅシリーズは、富士通のセキュリティソリューション体系の中で、パソコンセキュリティを実施/管理する製品群です。 ・ ＳａｆｅＭａｎａｇｅｒ・・・パソコンのセキュリティ対策実施状況を一元管理。ウィルス感染対策。ハードウェア、ソフトウェアの資産管理。 ・ ＳａｆｅＢｏｏｔ・・・クラスタレベルでのハードディスクの暗号化、ＯＳ起動前のパスワード認証によるパソコンの情報漏えい防止。 ・ Ｓａｆｅディスク消去人・・・ハードディスク内容の完全消去により、廃棄したパソコンからの機密データ漏えい防止。 ・ ＳａｆｅＤｅｆｅｎｓｅＷｉｎＰＲＯ・・・パソコン機能制限/環境保護。ファイル/ドライブのアクセス制限。 ・ ＳａｆｅＩＰＷＡＴＣＨＥＲ・・・根とワーク不正接続や稼動状態監視。機器台帳管理。 ・ ＳａｆｅＳａｓｕｒｅＫｅｅｐｅｒ・・・サーバの機密制限による情報漏えい防止。 ・ ＳａｆｅＳＦ2000Ｂｉｏ・・・バイオメトリック認証。

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）〒211-6063　川崎市中原区小杉町1-403	
関連部署名及び電話番号	
URL　http://www.ssl.fujitsu.com/	
対象技術	技術開発状況
サービス	セキュア無線ＬＡＮ構築「基本」サービス（利用者認証とデータの暗号化で安全面に配慮した環境構築)無線ＬＡＮ運用環境構築サービス(不正なアクセスポイントの検知/排除）

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）〒211-6063　川崎市中原区小杉町1-403	
関連部署名及び電話番号	
URL　http://www.ssl.fujitsu.com/	
対象技術	技術開発状況
サービス	・ リモートアクセス、安全でクライアントの種別を問わないリモートアクセスを提供する。 ・ 認証強化、複数のワンタイムパスワード手段を提供し、認証を強化。

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）〒211-6063　川崎市中原区小杉町1-403	
関連部署名及び電話番号	
URL　http://www.ssl.fujitsu.com/	
対象技術	技術開発状況
サーバ データ サービス	ｗｅｂサーバ、ＤＮＳ、メールサーバなどのイントラ、インターネット上のサーバを対象とし、サーバ内にあるお客様の大切なデータを保護します。あらかじめ設定されたアクセスルートだけ許可するため、未知、既知や外部、内部を問わず不正な攻撃をＯＳレベルで遮断します。ＯＳ資源へのアクセスを詳細に記録します。また複雑なセキュリティ設定を簡易化し、マルチプラットフォームの複数のサーバを集中管理します。

企業名（及び略称）	富士通株式会社
所在地（郵便番号及び住所）	〒211-8588　神奈川県川崎市中原区上小田中4-1-1
関連部署名及び電話番号	サービスビジネス本部セキュリティサービス推進部　03-6424-6249
URL	http://segroup.fujitsu.com/secure/

対象技術	技術開発状況
ネットワーク サーバ クライアント 通信情報 データ	本製品はインターネット上でサービスを提供するwwwサーバやアプリケーションサーバのためにセキュリティを確保する製品です。ファイアーウォール機能およびアプリケーションゲートウェイ機能（HTTPアプリケーションゲートウェイ機能/OPアプリケーションケートウェイ機能）により不正アクセスの防止、通信データの保護、ユーザ認証、内部サーバの隠蔽等を含む強固なセキュリティソリューションを提供します。携帯端末(Iモード)からのアクセスについては、登録された端末のみアクセスを許可することで、セキュリティ強度を高める事も可能です。

企業名（及び略称）	富士通株式会社
所在地（郵便番号及び住所）	〒211-8588　神奈川県川崎市中原区上小田中4-1-1
関連部署名及び電話番号	サービスビジネス本部セキュリティサービス推進部　03-6424-6249
URL	http://segroup.fujitsu.com/secure/

対象技術	技術開発状況
ネットワーク	概要：ユーザ認証、課金情報を管理するRADIUSサーバ製品。 特徴： ・無線LAN認証(IEEE802.1ｘEAP)に対応。 ・EAP-MDG,EAP-TLS,EAP-TTLS,EAP-PEAPに対応。 ・認証DBひとつでLANとリモートアクセスユーザを集中管理。 ・リモートアクセスユーザへのIPアドレスの自動割当。 ・Radius-Proxyによる負荷分散 ・Webブラウザを利用した容易な環境設定が可能。 ・マルチベンダRadiusクライアント対応。

企業名（及び略称）	富士通株式会社
所在地（郵便番号及び住所）	〒211-8588　神奈川県川崎市中原区上小田中4-1-1
関連部署名及び電話番号	サービスビジネス本部セキュリティサービス推進部　03-6424-6249
URL	http://segroup.fujitsu.com/secure/

対象技術	技術開発状況
クライアント 通信情報 データ	画期的な暗号化・複合化　利用者は知識不要 ・　ＤＦ ・　パソコン内の重要なファイルを暗号化することで、個人情報などを保護します。 ・　暗号化対象のフォルダやドライブを設定する事によりその中に保存されるファイルを自動的に暗号化・複合化します。 ・　ハードディスク（システムドライブを除く）を丸ごと暗号化することも可能です。 ・　外部にファイルを持ち出すためにファイルを暗号化するため、メールやMOなどの外部記憶媒体を試用した受け渡しが安全に行えます。 ・　暗号化にファイルを圧縮するため、受け渡しするファイルサイズが小さくなり情報量を削減できます。 ・　受け渡す相手がSystemwalker Desktop Encryptionを導入していない場合は、パスワードつきの自己複合形式ファイルに暗号化して受け渡せます。

企業名（及び略称）	富士通株式会社
所在地（郵便番号及び住所）	〒211-8588　神奈川県川崎市中原区上小田中4-1-1
関連部署名及び電話番号	サービスビジネス本部セキュリティサービス推進部　03-6424-6249
URL	http://segroup.fujitsu.com/secure/

対象技術	技術開発状況
データ	Secure Package 情報保護サービス 情報保護加工（暗号化による配送時のドキュメントの保護） ・配布するドキュメントに対する操作（印刷、保存）を制限できます。 ・ドキュメント参照時にSecure Packageセンターで認証を行うため、正規の受信者以外はドキュメントを参照できません。 ・送信後のドキュメントを回収（参照不可能）にできます。 ・送信先を誤った場合。 ・交渉打ち切り、社員の退社など参照資格がなくなった場合。 ・ドキュメントの参照行為を確認できます。確認手段には以下の2種類があります。 ・履歴情報（送信後画面） ・通知メール

企業名（及び略称）	富士通株式会社
所在地（郵便番号及び住所）	〒211-8588　神奈川県川崎市中原区上小田中4-1-1
関連部署名及び電話番号	サービスビジネス本部セキュリティサービス推進部　03-6424-6249
URL	http://segroup.fujitsu.com/secure/

対象技術	技術開発状況
ネットワーク サーバ クライアント サービス	富士通のSOC：「富士通ITマネージメントセンタ」より、お客様インターネットサイトを24時間365日監視し、クラッカーによる不正アクセスに迅速に対応します。また、監視状況を集計・分析して月報（Web等）を提供します。

企業名（及び略称）	富士通株式会社
所在地（郵便番号及び住所）	〒211-8588　神奈川県川崎市中原区上小田中4-1-1
関連部署名及び電話番号	サービスビジネス本部セキュリティサービス推進部　03-6424-6249
URL	http://segroup.fujitsu.com/secure/

対象技術	技術開発状況
サーバ サービス	米国Qualys Guard, IIS社のInternet Scanner等を使用したセキュリティのアセスメントサービス。

企業名（及び略称）	富士通株式会社
所在地（郵便番号及び住所）	〒211-8588　神奈川県川崎市中原区上小田中4-1-1
関連部署名及び電話番号	サービスビジネス本部セキュリティサービス推進部　03-6424-6249
URL	http://segroup.fujitsu.com/secure/

対象技術	技術開発状況
ネットワーク サーバ クライアント サービス	お客様の運用に合わせたファイアーウォールの最適な設計、構築と24時間365日監視・障害対応体制の提供により、ファイアーウォール運用におけるお客様の負担を大幅に削減する。

企業名（及び略称）	富士通株式会社
所在地（郵便番号及び住所）	〒211-8588　神奈川県川崎市中原区上小田中4-1-1
関連部署名及び電話番号	サービスビジネス本部セキュリティサービス推進部　03-6424-6249
URL	http://segroup.fujitsu.com/secure/

対象技術	技術開発状況
サーバ クライアント サービス	お客様の環境に合わせたウィルス対策システムを構築し、24時間365日ウィルス対策ソフトの稼働監視を実施します。また、エキスパートによるウィルス駆除にも迅速に対応します。

企業名（及び略称）	富士通株式会社
所在地（郵便番号及び住所）	〒211-8588　神奈川県川崎市中原区上小田中4-1-1
関連部署名及び電話番号	サービスビジネス本部セキュリティサービス推進部　03-6424-6249
URL	http://segroup.fujitsu.com/secure/

対象技術	技術開発状況
ネットワーク サーバ 通信情報 データ サービス	診断ツールと富士通独自ノウハウで、インフラ・OS・ミドルウェアを診断するサーバスキャンでは対応していない、お客様固有開発のWebアプリケーションの脆弱性を診断・評価・分析し、その危険性と具体的な対策指針をご提供します。

企業名（及び略称）	富士通株式会社
所在地（郵便番号及び住所）	〒211-8588　神奈川県川崎市中原区上小田中4-1-1
関連部署名及び電話番号	サービスビジネス本部セキュリティサービス推進部　03-6424-6249
ＵＲＬ	http://segroup.fujitsu.com/secure/

対象技術	技術開発状況
ネットワーク サーバ クライアント 通信情報 データ サービス	システム利用者の運用にWindowsセキュリティ修正プログラムの適用やウィルスパターンファイルの更新などのセキュリティ対策をシステムで統合管理ある環境をご提供します。

企業名（及び略称）	富士通株式会社
所在地（郵便番号及び住所）	〒211-8588　神奈川県川崎市中原区上小田中4-1-1
関連部署名及び電話番号	サービスビジネス本部セキュリティサービス推進部　03-6424-6249
ＵＲＬ	http://segroup.fujitsu.com/secure/

対象技術	技術開発状況
データ サービス	個人データの安全管理措置をトータルの支援 ・情報削減の兆候をSOCよりリモート監視。 ・最先端のプロダクト（非接触スマートロード、手のひら静脈認証、操作抑止ツール、暗号化ツール、入退室管理等）を含めたPDCA一貫したソルーション。

企業名（及び略称）	株式会社ブリッジ･メタウェア
所在地（郵便番号及び住所）	〒244-0801　神奈川県横浜市戸塚区品濃町548-2　東戸塚ＮＳビル４Ｆ
関連部署名及び電話番号	045-822-0780
ＵＲＬ	http://www.bridgemw.co.jp/

対象技術	技術開発状況
サービス	ｗｅｂソリージョンにおける動的ｗｅｂページ等のユーザーアプリケーションをプログラミングの側面（ソースコード）から監査し、脆弱性を排除した作りにする事を目的とするサービスである。

企業名（及び略称）	株式会社プロティビティジャパン
所在地（郵便番号及び住所）	〒100-0004　千代田区大手町1-1-3　大手センタービル22F
関連部署名及び電話番号	管理部　03-5219-6600
ＵＲＬ	http://www.protiviti.jp/

対象技術	技術開発状況
サービス	個人情報保護法に対応したプライバシー&情報セキュリティリスク管理パッケージ。Risicare（リジカーレ）

企業名（及び略称）	マカフィー株式会社
所在地（郵便番号及び住所）	〒150-0043　東京都渋谷区道玄坂1-12-1 渋谷マークシティウェスト　20F
関連部署名及び電話番号	03-5428-1100
ＵＲＬ	http://www.mcafee.com/jp/

対象技術	技術開発状況
ネットワーク	〈ＩｎｔｒｕＳｈｉｅｌｄ〉システムの脆弱性を狙った攻撃や侵入、ＭＳプラスト、Ｓａｓｓｅｒの様なワームおよびＤｏＳ攻撃に対して、高精度の検知とリアルタイムの防御が可能です。これらの攻撃に対して、予防、被害拡大の防止、問題発生時の適切な対応のための情報提供により、高度なセキュリティを実現します。

企業名（及び略称）	マカフィー株式会社
所在地（郵便番号及び住所）	〒150-0043　東京都渋谷区道玄坂1-12-1 渋谷マークシティウェスト　20F
関連部署名及び電話番号	03-5428-1100
ＵＲＬ	http://www.mcafee.com/jp/

対象技術	技術開発状況
サーバ クライアント	＜ＶＳＥ＞・ウィルスの他、ワーム、アドウエア/スパイウェア、バッファオーバフローにも対応。 ・　ＤＦ ・　強力なリモート管理。（ひとつのコンソールから、エンタープライズ全体に対し、すべての監視、設定機能が使えます） ・　管理者へのアラート機能。（管理者があらゆる組合せのシステムアラートの設定、定義が可能で、それぞれを個別に有効にしたり、優先順位をつけることができます） ・　リアルタイムオンデマンドスキャンとスケジュールスキャン対応。 ・　ｅＰＯとの連携により中央管理とグラフィカルレポートによる統合管理が可能。

企業名（及び略称）　　マカフィー株式会社	
所在地（郵便番号及び住所）〒150-0043　東京都渋谷区道玄坂1-12-1 渋谷マークシティウェスト　20F	
関連部署名及び電話番号　　03-5428-1100	
ＵＲＬ　　http://www.mcafee.com/jp/	
対象技術	技術開発状況
ネットワーク	＜WS＞McAfee WebShield Appliance v3.0は、容易に設定できるインターネットゲートウェイのためのソリューションで、ＳＭＴＰ、ＨＴＴＰ、ＦＴＰ、およびＰＯＰプロトコルの受信・送信トラフィックをスキャンします。比類のないパフォーマンスとウィルスの検知・駆除機能を提供し、あらゆる規模の企業にとって無用なスパム形式のメールや迷惑なコンテンツを防止します。スパウェアやアドウェア、増加が著しいフィッシングメールなどにも幅広く対応する製品です。

企業名（及び略称）　　マカフィー株式会社	
所在地（郵便番号及び住所）〒150-0043　東京都渋谷区道玄坂1-12-1 渋谷マークシティウェスト20F	
関連部署名及び電話番号　　03-5428-1100	
ＵＲＬ　　http://www.mcafee.com/jp/	
対象技術	技術開発状況
クライアント	＜ＡＳａＰ＞ ・　プログラム、エンジン、ウィルス定義（ＤＡＴ）ファイルを完全自動で更新するので手間がなく安心。 ・　（エージェントなので）動作が軽い。エージェント容量はわずか５ＭＢ ・　同ＬＡＮ内の1台がインターネットに接続していれば、全ＰＣの更新が可能。 ・　いつでもどこでもＷｅｂでウィルス対策レポート閲覧可能。 ・　100ＫＢ程度の差分アプデートにも対応。

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）	
関連部署名及び電話番号	
ＵＲＬ	
対象技術	技術開発状況
ネットワーク 通信情報 データ	概要：networkの通信を記録し、必要なときに解析、復元してnetwork利用を監視します。また記録されたパケットメンテは暗号化され、原本性を確保し、法的証拠として企業の雇用を守ります。 特徴： ① 優れた安全性（装置のセキュリティ機能）。記録されたデータはハッシュ値が付与され、暗号化されます。管理端末からの操作ログが記録されます。アクセス権限もシステム管理者、データ閲覧者、監査者に細分化されています。 ② 自社は拡張性。記録装置は選択自由で大容量も対応しています。 ③ 既存のシステムに一切影響を与えません。スイッチのミラーポートからパケットを取得するためのｎｅｔｗｏｒｋへの負荷がかかりません。構成変更も必要ありません。

企業名（及び略称）	横河電機株式会社
所在地（郵便番号及び住所）	〒180-8750　東京都武蔵野市中町2-9-32
関連部署名及び電話番号	コーポレート・コミュニケーション・センター　渉外室 0422-52-5533
ＵＲＬ	tp://www.yokogawa.co.jp/

対象技術	技術開発状況
サーバ	ＳｅｃｕｒｅＴｉｃｋｅｔはＳＳＬ－ＶＰＮ機能を搭載したＷｅｂサーバの総合セキュリティソフトです。 [特徴] ・ 多様なデバイスをサポートする強力・安全な“ユーザ認証”各種デバイス（ＵＳＢトークン、ＵＳＢディスク等）に対応したワンタイムパスワードやバイオメトリスクや、携帯電話に対応しています。 ・ 多様な認証機能と連携した“ＳＳＬ－ＶＰＮ”特別なハード不要！特別なクライアント不要の簡単導入！サービス単位のアクセス制御が可能です。 ・ Ｗｅｂサーバへの不正アクセスを強力にブロックする“リバースプロキシ”各種サービスに対するグループ単位のアクセスコントロール、ダイナミックなセッション管理、他認証を統合するシングルサインオンが可能です。

企業名（及び略称）	横河電機株式会社
所在地（郵便番号及び住所）	〒180-8750　東京都武蔵野市中町2-9-32
関連部署名及び電話番号	コーポレート・コミュニケーション・センター　渉外室 0422-52-5533
ＵＲＬ	http://www.yokogawa.co.jp/

対象技術	技術開発状況
ネットワーク データ	ＩＥＥＥ802.1XとＲＡＤＩＵＳ認証ソフトウェアを搭載したアプライアンス製品。ＩＥＥＥ802.1Xは、有線認証スイッチと無線ＬＡＮに、ＲＡＤＩＵＳは電話回線（ＲＡＳ）にクライアントＰＣを接続する時の認証プロトコルの規定です。これらを搭載するＡＳシリーズは、Ａｓ－Ｃ／ｈ、Ａｓ－Ｃ/ｍ、Ａｓ－Ｆの３機種より構成されます。これらは、ＥＡＰ－ＴＬＳ、ＥＡＰ－ＴＴＬＳ、ＰＥＡＰの認証プロトコルに対応しています。Ａｓ－Ｃ/ｈ、Ａｓ－Ｃ/ｍでは認証ソフトウェアを加えてＣＡ機能を搭載しディジタル証明書を発行することが可能です。外部のＬＤＡＰサーバとの連携も可能です。Ａｓ－Ｆは、小型で駆動部がバッテリバックアップ機能を搭載し小規模オフィスや支社支店や各フロアエッジへの配置が可能です。Ａｓ－Ｃをセンターに配置し、ＰＲＯＸＹよりエッジに配置したＡｓ－Ｆと分散構成をとることが可能です。

企業名（及び略称）	リコーテクノシステムズ株式会社
所在地（郵便番号及び住所）	〒111-0053　東京都大東区浅草橋5-20-8　SCタワー
関連部署名及び電話番号	マーケティング本部マーケティング推進室マーケティング推進部 03-5835-7011
ＵＲＬ	http://www.r-ts.co.jp/

対象技術	技術開発状況
ネットワーク サーバ クライアント サービス	ＩＴＳｈｅｒｉｆｆ　Box（ファイアウォール）による外部攻撃侵入からのネットワーク保護。またウィルス対策を行ないます。監視センターから24時間365日ITＳｈｅｒｉｆｆ　Boxやお客様サーバ、ネットワーク機器を遠隔監視し、異常検出時の対応を行ないます。さらに月間の監視結果レポート・コンタクトセンターによるお客様対応窓口を提供します。