平成19年２月22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18年１月１日から12月31日までの不正アクセス行為の発生状況を公表する。

○　アクセス制御機能に関する技術の研究開発の状況

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

３　掲載先

○　国家公安委員会ﾎｰﾑﾍﾟｰｼﾞ　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18年中の不正アクセス禁止法違反事件の認知・検挙状況等について

平成18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

平成18年中の不正アクセス行為の認知件数は946件で、前年と比べ、354件増加した。

表１－１　不正アクセス行為の認知件数の推移

	平成12年	平成13年	平成14年	平成15年	平成16年	平成17年	平成18年
認知件数（件）	106	1,253	329	212	356	592	946
海外からのアクセス	25	448	13	35	37	53	37
国内からのアクセス	73	258	286	158	303	487	855
アクセス元不明	8	547	30	19	16	52	54

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

(2)　被害に係る特定電子計算機のアクセス管理者（注１）

被害に係る特定電子計算機のアクセス管理者をみると、プロバイダが最も多く（602件）、次いで一般企業（325件）となっている。

表１－２　被害を受けた特定電子計算機のアクセス管理者の推移　（単位：件）

被害に係る特定電子計算機に係るアクセス管理者	平成12年	平成13年	平成14年	平成15年	平成16年	平成17年	平成18年
プロバイダ	59	182	243	98	126	356	602
一般企業	25	429	62	76	202	203	325
大学、研究機関等	8	101	3	16	6	12	6
その他	14	139	21	22	22	21	13
うち行政機関	-	-	12	3	12	17	5
不明	0	402	0	0	0	0	0
計	106	1,253	329	212	356	592	946

※　「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、警察職員による被疑者の取調べ等の警察活動によるものが最も多く（535件）、次いで利用権者（注２）からの届出によるもの（358件）、被害を受けた特定電子計算機のアクセス管理者からの届出によるもの（45件）、発見者からの通報によるもの（３件）の順となっている。

表１－３　認知の端緒の推移

認知の端緒（件）	平成12年	平成13年	平成14年	平成15年	平成16年	平成17年	平成18年
アクセス管理者からの届出	30	168	47	12	29	30	45
利用権者からの届出	23	118	92	78	172	505	358
警察活動	35	930	185	100	146	33	535
発見者からの通報	7	21	0	19	7	14	3
その他	11	16	5	3	2	10	5
計	106	1,253	329	212	356	592	946

(4) 不正アクセス行為後の行為

不正アクセス行為後の行為としては、インターネット・オークションの不正操作（他人になりすましての出品・入札等）が最も多く（593件）、次いで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）（257件）、インターネットバンキングの不正送金（39件）、ホームページの改ざん・消去（32件）、情報の不正入手（電子メールの盗み見等）（14件）、不正ファイルの蔵置（不正なプログラムやフィッシング（注３）用ホームページデータの蔵置等）（５件）の順となっている。

表１－４　不正アクセス行為後の行為の内訳

不正アクセス行為後の行為	平成17年 件数（件）(※)	平成18年 件数（件）
インターネット・オークションの不正操作	356	593
オンラインゲームの不正操作	140	257
インターネットバンキングの不正送金	5	39
ホームページの改ざん・消去	31	32
情報の不正入手	18	14
不正ファイルの蔵置	21	5
不明	32	2
その他	9	4

※　平成17年の件数については、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

(1)　検挙件数等

平成18年中における不正アクセス禁止法違反の検挙件数は703件、検挙人員は130人と、前年と比べ、それぞれ426件、14人増加した。その内訳をみると、不正アクセス行為に係るものがそれぞれ698件、130人、不正アクセス助長行為（注４）に係るものがそれぞれ５件、５人であった。

表２－１　検挙事件数等の推移

		平成12年	平成13年	平成14年	平成15年	平成16年	平成17年	平成18年
不正アクセス行為	検挙件数	62	66	102	143	142	271	698
	検挙事件数（注５）	30	35	51	58	65	94	84
	検挙人員	34	51	68	76	88	113	130
不正アクセス助長行為	検挙件数	5	1	3	2	0	6	5
	検挙事件数	4	1	2	2	0	6	3
	検挙人員	5	1	3	2	0	6	5
計	検挙件数（件）	67	67	105	145	142	277	703
	検挙事件数（事件）	31 (重複3)	35 (重複1)	51 (重複2)	58 (重複2)	65	94 (重複6)	84 (重複3)
	検挙人員（人）	37 (重複2)	51 (重複1)	69 (重複2)	76 (重複2)	88	116 (重複3)	130 (重複5)

※　(重複)とは、不正アクセス行為と不正アクセス助長行為の重複を示す。

(2)　不正アクセス行為の態様

検挙件数を不正アクセス行為の態様別にみると、識別符号窃用型（注６）が698件であり、セキュリティ・ホール攻撃型（注７）はなかった。

表２－２　不正アクセス行為の態様の推移

		平成12年	平成13年	平成14年	平成15年	平成16年	平成17年	平成18年
識別符号窃用型	検挙件数	61	52	83	141	131	264	698
	検挙事件数	29	33	46	56	62	90	84
セキュリティ・ホール攻撃型	検挙件数	1	14	19	2	11	7	0
	検挙事件数	1	3	5	2	4	5	0
計	検挙件数（件）	62	66	102	143	142	271	698
	検挙事件数（事件）	30	35 (重複1)	51	58	65 (重複1)	94 (重複1)	84

※　(重複)とは、識別符号窃用型とセキュリティホール攻撃型の重複を示す。

3　検挙事件の特徴

(1)　不正アクセス行為の手口

検挙した不正アクセス禁止法違反に係る不正アクセス行為の手口についてみると、フィッシングサイトを開設して識別符号を入手したもの（平成17年１件、平成18年220件）、スパイウェア（注８）等の不正なプログラムを使用して識別符号を入手したもの（平成17年33件、平成18年197件）などの高度なコンピュータ技術を悪用したものが急増した。

その一方で、ＩＤ等から容易に推測されるパスワードが使用されていたなど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（178件）、識別符号を知り得る立場にあった元従業員、知人等によるもの（49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（20件）等、特に高度な技術を有していない者でも行えるものも発生している。

表３－１　不正アクセス行為に係る犯行の手口の内訳

犯行の手口		平成17年 件数（件）	平成18年 件数（件）
識別符号窃用型		264	698
	フィッシングサイトにより入手したもの	1	220
	スパイウェア等のプログラムを使用して識別符号を入手したもの	33	197
	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	95	178
	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	33	49
	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	16	20
	ファイル交換ソフトや暴露ウイルスで流出した識別符号を含む情報を利用したもの	0	19
	他人から購入したもの	69	12
	共犯者等から入手したもの	12	0
	その他	5	3
セキュリティ・ホール攻撃型		7	0

(2)　被疑者

不正アクセス禁止法違反に係る被疑者と識別符号を利用された利用権者の関係についてみると、交友関係のない他人によるものが最も多く（638件）、次いで元交際相手や元従業員等の顔見知りの者によるもの（50件）、ネットワーク上のみの知り合いによるもの（15件）となっている。

また、被疑者の年齢についてみると、20歳代が最も多く（44人）、次いで10歳代（40人）、30歳代（28人）、40歳代（15人）、50歳代（２人）、60歳代（１人）の順となっている。 平成16年以降、10歳代の被疑者が30%前後を占めている。

なお、最年少の者は14歳、最年長の者は61歳であった。

表３－２　年代別被疑者数の推移　（単位：人）

年齢	平成12年	平成13年	平成14年	平成15年	平成16年	平成17年	平成18年
10歳代	6	2	6	16	26	35	40
20歳代	13	28	30	26	21	40	44
30歳代	16	5	26	24	23	27	28
40歳代	2	16	7	9	17	9	15
50歳代	0	0	0	1	1	5	2
60歳代	0	0	0	0	0	0	1
計	37	51	69	76	88	116	130

※　不正アクセス助長行為に係る被疑者を含む。

(3)　不正アクセス行為の動機

不正アクセス行為の動機としては、不正に金を得るため（419件）が最も多くなった。また、前年と比べ、オンラインゲームで不正操作を行うためが急増した（平成17年25件、平成18年211件）。

表３－３　不正アクセス行為の動機の内訳

動機	平成17年	平成18年
	件数（件）	件数（件）
不正に金を得るため	167	419
オンラインゲームで不正操作を行うため	25	211
嫌がらせや仕返しのため	31	31
好奇心を満たすため	20	26
顧客データの収集等情報を不正に入手するため	23	10
料金の請求を免れる	0	1
自分の技量を図るため	2	0
その他	3	0

(4)　利用されたサービス

検挙した不正アクセス禁止法違反に係る識別符号窃用型の不正アクセス行為（698件）について、当該識別符号を入力することにより利用されたサービスをみると、インターネット・オークションが最も多く（394件）、次いで、オンラインゲーム（223件）、インターネットバンキング（38件）、電子メール（21件）、ホームページ公開サービス（７件）の順となっている。

前年と比べ、オンラインゲームが利用された場合（平成17年42件、平成18年223件）、インターネット・オークションが利用された場合（平成17年154件、平成18年394件）が急増した。

表３－４　利用されたサービスの内訳

利用されたサービス		平成17年 件数（件）	平成18年 件数（件）
識別符号窃用型		264	698
	インターネット・オークション	154	394
	オンラインゲーム	42	223
	インターネットバンキング	33	38
	電子メール	14	21
	ホームページ公開サービス	8	7
	会員専用・社員用内部サイト	8	6
	電子掲示板	0	5
	会員・顧客データベース	2	2
	その他	3	2

(5)　その他

不正アクセス禁止法違反と併せて検挙した犯罪には、詐欺、電磁的記録不正作出・同供用、電子計算機損壊等業務妨害、電子計算機使用詐欺等があり、金銭目的の犯罪が多い。

４　都道府県公安委員会による援助措置

平成18年中、不正アクセス禁止法第６条の規定に基づき、都道府県公安委員会がアクセス管理者に対して行った助言・指導は３件（北海道１件、静岡１件、島根１件）であった。

表４－１　都道府県公安委員会の援助措置実施件数の推移

	平成12年	平成13年	平成14年	平成15年	平成16年	平成17年	平成18年
援助措置（件）	6	21	5	5	3	4	3

5　防御上の留意事項

(1)　利用権者の講ずべき措置

ア　フィッシングサイトに対する注意

電子メールにより本物のサイトに酷似したフィッシングサイトに誘導し、ＩＤ・パスワードを不正に取得する事案が急増していることから、発信元に心当たりのない電子メールに注意するとともに、ＩＤ・パスワードの入力を要求するサイトについては、そのＵＲＬが金融機関等を装った別の事業者のものではないか確認する。

イ　スパイウェア等の不正プログラムに対する注意

スパイウェア等の不正プログラムを含んだ電子メールやＣＤを送りつけ、それらによりＩＤ・パスワードを不正に取得する事案も増加していることから、発信元に心当たりのない電子メールやＣＤ等が送付されてきた際は、不用意に本文や添付ファイル等を開封しないように注意するとともに、スパイウェア対策やコンピュータ・ウイルス対策（最新のウイルス対策ソフト、オペレーティングシステムの利用）を適切に講ずる。

特に、他者のサーバを介してインターネット上で商品を販売する者等のインターネット上で営業を営む者にあっては、顧客等とのメールのやり取り等を通じてスパイウェアに感染し、自己のパソコン内に保存しているインターネットバンキングの自己の預貯金口座等の情報が流出する事案が増加しているため、インターネットバンキング等に使用するパソコンと顧客との通信に使用するパソコンを分けて使用するなどの配慮が必要である。

また、インターネットカフェ等の不特定多数の者が利用する場所に設置されたコンピュータでは、不正プログラムが動作している可能性があることから、重要な情報を入力しないなどの注意が必要である。

ウ　パスワードの適切な設定・管理

利用権者のパスワードの設定・管理の甘さにつけ込んだ不正アクセス行為も多発していることから、パスワードを設定する場合には、ＩＤと全く同じパスワード、ＩＤの一部を使ったパスワード等、ＩＤ等からの推測が容易なものは避けるとともに、パスワードを他人に教えない、パスワードを定期的に変更するなどの対策を講じて、自己の識別符号を適切に設定・管理する。

(2)　アクセス管理者の講ずべき措置

ア　フィッシング・スパイウェア等への対策

フィッシング等により不正に取得したＩＤ・パスワードを使用した不正アクセス行為が多発していることから、インターネット・オークション、インターネットバンキング等のサービスを提供する事業者にあっては、識別符号(ＩＤ・パスワード)に加え、ワンタイムパスワード（注９）等により個人認証を強化するなどの対策を講ずる。

イ　パスワードの適切な設定

利用権者のパスワードの設定・管理の甘さにつけ込んだ不正アクセス行為が多発していることから、アクセス管理者は、容易に推測されるパスワードを設定できないようにする仕組みを活用するなどの措置を講ずる。

ウ　不特定多数の者が利用できるコンピュータの適切な管理

インターネットカフェ等の不特定多数の者が利用する場所に設置されたコンピュータの管理者は、利用者の本人確認の励行、コンピュータへのリカバリーソフト（注10）の導入、利用終了時におけるブラウザ等の履歴の削除、プログラムのインストール制限を行うなどの措置を講ずるとともに、利用者に対してＩＤ・パスワード等を入力する際の危険性について注意喚起する。

6　検挙事例

1	**インターネット・オークション会社のホームページを複製したフィッシングサイトで入手した識別符号で他人になりすまし、同社オークションに架空出品して代金を騙し取った不正アクセス禁止法違反及び詐欺事件**

無職の男(34)らは、平成17年９月から平成18年４月までの間、インターネット・オークション会社の偽のログイン画面を設置し、同ログイン画面へ誘導する電子メールをオークションの会員に送信し、これを本物のログイン画面と誤信した会員が入力した識別符号を不正に入手した。そして、当該識別符号を使用して同社のコンピュータに不正アクセス行為を行い、同社オークションにおいて商品を売ると偽り多数の落札者から代金を騙し取った。平成18年５月、不正アクセス禁止法違反及び詐欺罪で検挙した（京都、静岡、熊本）。

2	**インターネットバンキングのセキュリティ対策ソフトウェアを装ったスパイウェアをＣＤで送りつけ識別符号を盗み取り、使用した不正アクセス禁止法違反、電子計算機使用詐欺及び電子計算機損壊等業務妨害事件**

無職の男(31)は、平成17年10月、インターネットバンキングを利用している法人に対して、インターネットバンキングのセキュリティ対策ソフトウェアを装ったスパイウェアを記録したＣＤ－Ｒを送りつけ、同法人のインターネットバンキング利用に係る識別符号等を取得し、インターネットバンキングのコンピュータに不正アクセス行為を行って、同法人の口座から自己の管理する他人名義の口座に対して約300万円の送金操作を行った。また、スパイウェアにより識別符号等を外部に送信させることによって、同法人の業務を妨害した。平成18年４月、不正アクセス禁止法違反、電子計算機使用詐欺罪及び電子計算機損壊等業務妨害罪で検挙した（千葉）。

3	**勤務先のインターネットカフェにキーロガー（注11）を仕掛けて入手した他人の識別符号を用いてオンラインゲーム上のアイテムを収集した不正アクセス禁止法違反事件**

インターネットカフェの従業員の男(26)は、平成17年１月、オンラインゲーム上のアイテムを収集する目的で、勤務先のインターネットカフェのコンピュータにキーロガーを仕掛け、同店を利用した客の識別符号を入手し、同店のコンピュータから客になりすまして当該オンラインゲーム会社のコンピュータに不正アクセス行為を行った。平成18年５月、不正アクセス禁止法違反で検挙した（岡山）。

4	インターネット・オークション画面のＩＤからパスワードを推測し他人になりすまし同インターネット・オークションで架空出品して代金を騙し取った不正アクセス禁止法違反及び詐欺事件

無職の男(31)らは、平成17年11月、インターネット・オークションの画面に表示されているＩＤからパスワードを推測し、これを使用して運営会社のコンピュータに不正アクセス行為を行い、商品を売ると偽り多数の落札者から代金を騙し取った。平成18年６月、不正アクセス禁止法違反及び詐欺罪で検挙した（岩手）。

5	国家試験の受験申請データを見るために元勤務先の財団法人の識別符号を不正に使用した不正アクセス禁止法違反事件

無職の男(61)は、平成18年２月、興味本位から元勤務先の財団法人が管理する国家試験業務用のコンピュータに、在職中に知り得た識別符号を入力して不正アクセス行為を行い、約6,100件の申請者データを読み出した。平成18年４月、不正アクセス禁止法違反で検挙した（警視庁）。

6	オンラインゲーム会社のホームページを複製してフィッシングサイトを開設した不正アクセス禁止法違反及び著作権法違反事件

中学生の男(14)は、平成18年２月から３月までの間、オンラインゲーム会社のホームページを複製したフィッシングサイトを開設し、同ゲームの運営者を装い「違反行為をしたが反省文を入力すれば罰則を免除する」旨のメールを会員に送りつけ、当該フィッシングサイトに誘導し識別符号、反省文等を入力させ、不正に入手した識別符号を使用して同ゲームのコンピュータに不正アクセス行為を行った。平成18年５月、不正アクセス禁止法違反及び著作権法違反で検挙した（警視庁）。

（注）

注１　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２　利用権者

利用権者とは、特定電子計算機をネットワークを通じて利用することについて、当該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３　フィッシング

金融機関を装って電子メールを送信する等して、受信者が偽のウェブサイトにアクセスするよう仕向け、そこに個人の識別符号（ＩＤ、パスワード等）、クレジットカード番号等を入力させ、それらを不正に入手する行為をいう。

注４　不正アクセス助長行為

他人の識別符号をどのコンピュータに対する識別符号であるかを明らかにして、またはこれを知っている者の求めに応じて、アクセス管理者や利用権者に無断で第三者に提供する行為をいう。

注５　事件数

事件数とは、事件単位ごとに計上した数であり、一連の捜査で複数の件数の犯罪を検挙した場合は１事件と数える。

注６　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・オークション用の識別符号を使用して、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７　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、セキュリティの脆弱性を突いて操作指令を与えるなどの手法による不正アクセス行為が該当する。

注８　スパイウェア

パソコン内のファイル又はキーボードの入力情報、表示画面の情報等を取り出して、漏えいする機能を持つプログラムのことをいう。

注９　ワンタイムパスワード

インターネット銀行等における認証方法として、識別符号のほかに、毎回異なる文字列を入力してサーバーに送信するもの。識別符号を盗まれても次回の利用時に使用できない。

注10　リカバリーソフト

通常に動作しているコンピュータの状態を記録しておき、必要に応じてその状態に戻すソフトのことをいう。

注11　キーロガー

インストールしたコンピュータにおいて、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のことをいう。

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18年1月1日から12月31日の間にIPAに届出のあったコンピュータ不正アクセス（注１）が対象である。

コンピュータ不正アクセスに関する届出件数は331件（昨年：515件）であった。（注２）

平成18年は同17 年と比べて、届出件数が大幅に減少しているが、被害があった届出件数は若干の減少に留まっている。

届出のうち実際に被害があったケースにおける被害内容の分類では、ファイルの書き換え（プログラムの埋め込み含む）及びホームページの改ざんによる被害届出が多く寄せられた。

以下に、種々の切り口で分類した結果を示す。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項目に該当するものがあるため、それぞれの分類での総件数は届出件数に必ずしも一致しない。

(1) 手口別分類

意図的に行う攻撃行為による分類である。1件の届出について複数の攻撃行為を受けている場合があるため、総計は届出件数とは異なり、553件（昨年：726件）であった。

ア　侵入行為

侵入行為に係る攻撃等については517件（昨年：650件）の届出があった。

(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については、157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については、108件の届出があり、これらのうち実際に侵入につながったものは80件であった。

【主な内容】

パスワード推測：57件

ソフトウェアのセキュリティホールを利用した攻撃：31件

システムの設定内容を利用した攻撃：4件

(ｳ) 不正行為の実行

侵入その他、何らかの手法により不正行為が実行されたことについては、252件の届出があった。

【主な内容】

ファイル等の改ざん、破壊等：110件

資源利用（ファイル、CPU使用）：68件

踏み台として他のサイトへのアクセスに利用された：34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：22件
裏口（バックドア）の作成：3件
証拠の隠滅（ログの消去など）：3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については、17件（昨年：29件）の届出があった。

【主な内容】
過負荷を与える攻撃：15件
大量の迷惑メール送り付け：2件

ウ　その他

その他にはメール不正中継や正規ユーザになりすましてのサービス不正利用などが含まれ、19件（昨年：47件）の届出があった。

【主な内容】
メールアドレス(ドメイン)の詐称：9件
メールの不正中継に関するもの：3件
正規ユーザへのなりすまし：2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。

331件の届出中、実際に侵入を受けた94件（昨年：98件）、DoS攻撃等によるサービス妨害12件（昨年：21件）など実際に被害に遭った計162件（昨年：176件）を分類すると以下のようになる。

被害原因としてID、パスワード管理不備や古いバージョン使用、パッチ等未導入などが多くなっているなど、基本的なセキュリティ対策が成されていないサイトが狙われていると推測される。また、原因が不明なケースも多くなっている。

【主な要因】
ID、パスワード管理の不備によると思われるもの：46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：31件
設定の不備(セキュリティ上問題のあるデフォルト設定を含む)によるもの：6件
その他によるもの：22件
原因不明：57件

(3) 機器別分類

攻撃や被害の対象となった機器による分類である。

【主な対象】
クライアントＰＣ：74件
ファイアウォール：70件

WWWサーバー：60件
ルータ：47件
メールサーバー：17件
その他のサーバー・不明：64件

(4) 被害内容別分類

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229件（昨年：206件）である。なお、対処に要する工数、サービスの一時停止、代替機の準備などは被害から除外している。

【主な被害内容】
ファイルの書き換え（プログラムの埋め込み含む）：92件
ホームページの改ざん：34件
サービス低下：16件
メールの不正中継に利用された：2件
不正アカウント作成：1件

(5) 対策情報

基本的なセキュリティ対策を実施していれば被害を免れていたと思われるケースが非常に多く見受けられる。システム管理者は以下の基本事項を再点検して総合的な対策を行うことが望まれる。

- ID やパスワードの厳重な管理及び設定
- セキュリティホールの解消（パッチ適用不可の場合は、運用による回避策も含む）
- ルータやファイアウォールなどの設定やアクセス制御設定
- 定期的なログのチェック

また、個人ユーザにおいても同様に以下の点に注意することが望まれる。

- Windows Update やOffice Update など､OS やアプリケーションソフトのアップデート
- パスワードの設定と管理（複雑化、定期的に変更、安易に他人に教えないなど）
- 無線LAN やPC 共有についてのセキュリティ設定確認
- ルータやパーソナルファイアウォールの活用

下記ページなどを参照し、今一度状況確認・対処されたい。
「安全なウェブサイトの作り方　改訂第2版」
http://www.ipa.go.jp/security/vuln/websecurity.html
「情報セキュリティ対策ベンチマーク」
http://www.ipa.go.jp/security/benchmark/
「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
「サイバークリーンセンター」
https://www.ccc.go.jp/

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、下記ページを参照されたい。

「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、IPAが受理したコンピュータ不正アクセスの届出に係る件数であり、不正アクセス等に関する実際の発生件数や、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。

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１8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)に係る報告件数(注２)は2,582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1,252件の報告があった。

[1/1-3/31: 501件、4/1-6/30: 340件、7/1-9/30:219件、10/1-12/31: 192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17件の報告があった。

[1/1-3/31: 6件、4/1-6/30: 8件、7/1-9/30: 1件、10/1-12/31: 2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130件の報告があった。

[1/1-3/31: 125件、4/1-6/30: 1件、7/1-9/30:3件、10/1-12/31: 1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34件の報告があった。

[1/1-3/31: 5件、4/1-6/30: 17件、7/1-9/30: 1件、10/1-12/31: 11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526件の報告があった。

[1/1-3/31: 84件、4/1-6/30: 163件、7/1-9/30: 159件、10/1-12/31:120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623件の報告があった。

[1/1-3/31: 73件、4/1-6/30: 132件、7/1-9/30: 330件、10/1-12/31: 88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]

Microsoft セキュリティ情報（緊急6件含）に関する注意喚起

Microsoft XML コアサービスに未修正の脆弱性

2006年11月 Microsoft セキュリティ情報（緊急5件含）に関する注意喚起

2006年12月 Microsoft セキュリティ情報（緊急3件含）に関する注意喚起

TCP 2967番ポートへのスキャン増加に関する注意喚起

Microsoft 製品に含まれる脆弱性に関する注意喚起

Microsoft 製品に含まれる脆弱性に関する注意喚起

TCP 139番ポートへのスキャン増加に関する注意喚起

夏期休暇明けの対応について

Microsoft 製品に含まれる脆弱性に関する注意喚起

Microsoft Windows VML の処理に未修正の脆弱性

Microsoft PowerPoint 未修正の脆弱性に関する注意喚起

RealVNC サーバの認証が回避される脆弱性に関する注意喚起

Microsoft Word の脆弱性に関する注意喚起

Microsoft 製品に含まれる脆弱性に関する注意喚起

sendmail の脆弱性に関する注意喚起

Microsoft Excel 未修正の脆弱性に関する注意喚起

Microsoft Windows メタファイル処理の脆弱性に対するセキュリティ更新プログラムについて

Adobe Flash Player 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

DNS の再帰的な問合せを使った DDoS 攻撃に関する注意喚起

イ　活動概要（届出状況等の公表）

発行日：2007-01-17 [2006年10月1日～ 2006年12月31日]

発行日：2006-10-17 [2006年 7月1日～ 2006年9月30日]

発行日：2006-07-19 [2006年4月1日～ 2006年6月30日]

発行日：2006-04-21 [2006年1月1日～ 2006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] 330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ックの観測を行い、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172件であった(詳細は http://jvn.jp/参照)
[1/1-3/31: 27件、4/1-6/30: 36件、7/1-9/30: 64件、10/1-12/31: 45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60件であった。
[1/1-3/31: 16件、4/1-6/30: 12件、7/1-9/30: 15件、10/1-12/31: 17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。実際の攻撃の発生件数や、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が取り組む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り、具体的には、独立行政法人自ら又は委託による研究、国からの委託又は補助による研究である。

実施テーマは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
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
異種ネットワーク相互接続環境下における最適情報通信サービス実現のための制御技術の研究開発
インターネットにおけるトレースバック技術に関する研究開発
大容量データの安全な流通・保存技術に関する研究開発
異なるCA間の認証ローミング技術に関する研究開発
ネットワーク認証型コンテンツアクセス制御技術の研究開発
ネットワークセキュリティ技術の研究開発
次世代型電子認証基盤の整備
高信頼性端末の電子認証基盤の調査研究
電子認証フレームワークのIPアドレス認証の展開に関する調査研究
ユビキタスネットワーク向けセキュアアセットコントロール技術の研究開発
情報漏えいに堅牢な認証・データ管理方式とそのソフトウェアによる安全な実装・検証手法に関する研究開発
アクセスグラフに基づくボットネット検出技術の研究開発

２　民間企業等で研究を実施したもの

(1)　公募

警察庁、総務省及び経済産業省が平成18年11月16日から12月15日までの間にアクセス制御技術に関する研究開発状況の募集を行ったところ、応募者は次のとおりであった。それぞれの研究開発の概要は、別添２のとおりである。

なお、別添２の内容は当該企業から応募のあった内容をそのまま掲載している。

サイバーエリアリサーチ株式会社
大日本印刷株式会社

株式会社トリニティーセキュリティーシステムズ
日本通信株式会社
株式会社ニーモニックセキュリティ
日本ユニシス株式会社

(2)　調査

警察庁が平成18年９月から10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。

・大学

国公立・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

・企業

業種分類が「情報・通信」「サービス」「電気機器」「金融」である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

石巻専修大学
茨城大学
岩手県立大学
熊本大学
信州大学
広島大

イ　企業

NECソフトウェア北陸
NECネクサソリューションズ株式会社
NECフィールディング株式会社
株式会社NTTPCコミュニケーションズ
RSAセキュリティ株式会社
TCBテクノロジーズ株式会社
アルプスシステムインテグレーション株式会社
インターネットセキュリティシステムズ株式会社
インテック・ウェブ・アンド・ゲノム・インフォマティクス株式会社
ウィッツェル株式会社
エントラストジャパン株式会社
カシオ計算機株式会社
クオリティ株式会社
クボタシステム開発株式会社
サイエンスパーク株式会社
株式会社シー・エス・イー
株式会社シーフォーテクノロジー
株式会社システックス
シャープ株式会社
株式会社セキュアブレイン

株式会社ソフテック
株式会社ソフトクリエイト
大日本印刷株式会社
デジタルアーツ株式会社
東芝ソリューション株式会社
株式会社トリニティーセキュリティーシステムズ
株式会社バーテックスリンク
ハミングヘッズ株式会社
株式会社ハンモック
株式会社日立製作所
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
富士ゼロックス株式会社
富士通株式会社
富士通エフ・アイ・ピー株式会社
富士通サポートアンドサービス株式会社
株式会社富士通北陸システムズ
マイクロソフト株式会社
三菱電機エンジニアリング株式会社
三菱電機株式会社
ユニアデックス株式会社
株式会社ラック

（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、大量のセキュリティログから効率的・高精度にインシデントを分析する技術等に着手し、平成17年度には、実時間処理を可能とするインシデント分析システムのプロトタイプを構築した。

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　情報通信セキュリティ研究センター推進室

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)、(株)日立製作所、沖電気工業(株)、(株)KDDI研究所
(情報通信研究機構（NICT）が実施する委託研究の委託先)

背景、目的

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及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
(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
(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
(4) 広域モニタリングシステムのオペレーション方式

･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　連携研究部門　委託研究グループ
（http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm）電話　042－327－6011

将来の方向性

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

対象技術 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)、(株)日立製作所、日本電気(株)
(情報通信研究機構（NICT）が実施する委託研究の委託先)

背景、目的

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。

本研究では、接続相手として安全であるか否かを、測定可能かつ客観的な指標を相互に確認したり、外部機関との情報連携や全体傾向からの分析によってアラートを生成したりする仕組みをもとに、リコメンドとして提示することで、アクセス制御等の意思決定者が行う対策を支援する意思決定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) 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　連携研究部門　委託研究グループ
（http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm）電話　042－327－6011

将来の方向性

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

対象技術 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)日立製作所、(株)エヌ・ティ・ティ・ドコモ、(株)KDDI研究所、日本電気(株)
(情報通信研究機構（NICT）が実施する委託研究の委託先)

背景、目的

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が、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）認証及び正確なサーバ認証が必須である。

これら認証において問題となるのは、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であるため、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があるため、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) 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。
- なお、研究終了後は、モバイルITフォーラムを通じた成果の普及展開を計画中。

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　連携研究部門　委託研究グループ
（http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm）電話　042－327－6011

将来の方向性

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

対象技術 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)日立製作所（情報通信研究機構（NICT）が実施する委託研究の委託先）

背景、目的

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、具体的にはモバイル端末自身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開発する。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

(2) 複合認証システム技術

(3) セキュアモバイル端末利用システム

・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　連携研究部門　委託研究グループ

（http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm）電話　042－327－6011

将来の方向性

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

対象技術 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)日立製作所

(情報通信研究機構(NICT)が実施する委託研究の委託先)

背景、目的

近年、RFIDタグを利用した流通管理のコスト削減や、ユーザの利便性を高めた簡便な電子マネーサービスが普及しつつある。しかし、現在利用されている安価なRFIDタグの多くは十分なセキュリティ機能を備えているとは言えず、たとえば、ICカードに保存されている利用履歴などが、ユーザに感知されること無く簡単に読み取られてしまう、などの脅威が指摘されている。セキュリティ機能の導入が中々進まない背景には、RFIDタグのように安価であることが要求されるチップに高度な暗号機能を盛り込むことが現実的でない、というコスト面の課題が挙げられる。

本研究開発では、非接触ICカードなどのRFIDタグにおいて利用可能な認証機能を実現することを目標とし、認証技術の基本となる暗号学的ハッシュ関数を開発する。本研究の結果として得られるRFIDタグに信頼性の高い認証機能を利用すれば、セキュリティやプライバシが必要とされるようなシーンにおけるRFIDタグ利用の可能性が広がると考えられる。

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) 認証方式の設計技術

(2) 認証方式の安全性評価技術

(3) 認証方式の実装技術

・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 連携研究部門 委託研究グループ

(http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm) 電話 042－327－6011

将来の方向性

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

対象技術 その他認証技術等

テーマ名 異種ネットワーク相互接続環境下における最適情報通信サービス実現のための制御技術の研究開発

開発年度 平成17年度～平成19年度

実施主体 エヌ・ティ・ティ・コミュニケーションズ(株)
(情報通信研究機構(NICT)が実施する委託研究の委託先)

背景、目的

我が国では2001年のIT戦略本部による「e-Japan戦略」を契機として、2003年の「e-Japan戦略II」、2004年の「e-Japan戦略II加速化パッケージ」等のIT国家戦略の中で地域の情報化を目指した様々な施策が実施され、政府及び地方自治体を取り巻く公共ネットワークの整備が急速に進められてきた。

これらの取り組みによって、我が国の公共ネットワークの整備は急速に進展し、世界でもトップクラスのIT国家の仲間入りを果たしたが、一方で、それらの公共ネットワークの整備はそれぞれの施策の中で異なる時期に、異なる目的、異なるポリシー等に基づき設計・構築されてきたため、多種多様なネットワーク仕様が混在するHeterogeneous(異種)ネットワーク環境下にあると言える。

しかしながら、これら異種ネットワークを相互に接続するための機構は未だ未整備の状況にあるため、各地域の様々なネットワーク上に散在する情報やサービスを必要に応じて有機的に連携させ、利用することが可能となれば、利用者にとって真に便利な高付加価値サービスを提供することが可能になると考えられる。このため、本研究開発では、国や自治体などが異種ネットワークによって相互に接続された環境において、サービスを効果的に相互提供・利用することを可能とする技術の開発を行う。

研究開発状況(概要)

・平成17年度より以下の研究開発を実施中。

(1) マルチレイヤに跨る環境情報に基づく最適通信制御技術

(2) 高信頼ネットワークサービス環境構築技術

(3) 異種ネットワーク上での高度マッチメイキング技術

(4) 異種ネットワーク相互接続利用基盤を評価する実証実験

…全国地域情報化推進協会の協力を得て、防災情報の伝達・共有及び災害医療に関するフィールド実験を実施した。(平成18年10月～12月)

・平成19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 連携研究部門 委託研究グループ
(http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm) 電話 042－327－6011

将来の方向性

国や自治体などが異種ネットワークによって相互に接続された環境において、サービスを効果的に相互提供・利用を可能とする基盤技術の確立に資する。

対象技術 侵入検知技術

テーマ名 インターネットにおけるトレースバック技術に関する研究開発

開発年度 平成17年度～平成21年度

実施主体 日本電気(株)、奈良先端科学技術大学院大学、KDDI(株)、松下電工(株)、
(株)クルウィット、(財)日本データ通信協会
(情報通信研究機構(NICT)が実施する委託研究の委託先)

背景、目的

インターネットに対する攻撃・脅威によるインシデントは年々増大している。従来からインターネットを監視するという受動的な警戒に関しての技術開発が実施されているが、これに対し、攻撃の予兆を検出した時にその攻撃の発生場所を探索するという能動的な警戒が考えられる。

この能動的な警戒を実現するために必要となる「トレースバック技術」の研究開発については、IP層におけるトレースバックの研究は十数年にわたって進められており、理論は成熟しつつあるが、フィールド広域に対する実装が行われている例は少ない。またそれより上位のアプリケーション層に関しては、理論研究さえ未成熟である。このため、本研究開発では、インターネットにおけるトレースバック技術に関しての実運用環境への実装を目指した研究開発を行う。なお、不正アクセス、DoS攻撃、ウイルス発信等の攻撃はそのIPパケットのソースアドレスが詐称されている例も多く、攻撃源の把握が困難であるが、本研究開発ではソースアドレス詐称があってもその発信源を把握できるトレースバック技術を開発する。

研究開発状況(概要)

・平成17年度から以下の研究開発を実施中
(1)全体アーキテクチャーの設計
(2)トレースバック・アルゴリズム
(3)トレースバック用データ収集装置(プローブ装置)
(4)トレースバック・プラットフォームの実証実験
・平成21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　連携研究部門　委託研究グループ
(http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm) 電話　042－327－6011

将来の方向性

不正アクセス、DoS攻撃、ウイルス発信等に対してその発信源を探索して対策を講じることができるようになると同時に、抑止力として期待される。

対象技術 その他認証技術

テーマ名 大容量データの安全な流通･保存技術に関する研究開発

開発年度 平成17年度から平成19年度までの3年間

実施主体 (株)日立製作所、東京理科大、エヌ･ティ･ティ･コミュニケーションズ(株)
(情報通信研究機構(NICT) が実施する委託研究の委託先)

背景、目的

近年社会生活において、ネットワークインフラはますます身近なものとなってきている。特に、わが国においては、すでに世界最高水準のブロードバンドネットワークインフラの整備が進み、現在は、さらにユビキタスネットワーク社会の実現に向けて、さまざまな取り組みがなされている。

ユビキタスネットワーク社会の技術環境の特徴として、

- 多様で複雑なブロードバンドネットワークの進展･普及
- コンテンツの大容量化･多様化
- 情報処理端末の小型化･モバイル化

の各点が挙げられるが、これらは、人々の生活をより便利に豊かにする上で望ましい特徴である反面、セキュリティの観点からは、逆に、情報漏洩の危険性や一旦漏洩した場合の被害の拡大につながる懸念がある。これらの懸念を払拭しなければ、ユビキタスネットワーク社会の進展は図れない。

本研究開発では、ユビキタスネットワーク社会における情報漏洩を防止する技術を確立するために、通信路、コンテンツ、ストレージの3つの観点から研究開発を実施する。

研究開発状況(概要)

・ 平成 17 年度より以下の研究開発を実施中。

(1)機密情報を安全、高速、低消費電力で伝送する技術

(2)機密情報を利用者の役割等に応じ、選択的に開示する技術

(3)機密情報を安全かつ効率的に保存する技術

･平成19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 連携研究部門 委託研究グループ

(http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm) 電話 042－327－6011

将来の方向性

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

対象技術 その他認証技術

テーマ名 異なるCA間の認証ローミング技術に関する研究開発

開発年度 平成17年度から平成18年度までの2年間

実施主体 (株)テプコシステムズ、三菱電機(株)
(情報通信研究機構(NICT)が実施する委託研究の委託先)

背景、目的

今後、ネットワークが提供するサービスの数が一段と増大し、より多くのサービス提供者への個人情報の登録機会が増えていくことが見込まれる中で、利用者はどこから個人情報が漏えいするか分からないという脅威や、フィッシング詐欺のように意図せず個人情報を不正に搾取されてしまうという脅威に一段とさらされるとともに、こうした脅威を嫌う利用者によるサービス離れが加速し、健全なサービス市場の発展が阻害されることが懸念されている。

こうした状況の中で、一部のサービス提供者においては、不正アクセスを抑制するために「電子署名及び認証に関する法律」の認定を受けた民間認証局等で発行されている公開鍵証明書を用いて、サービス利用時の本人確認や送受信データの真正性確保等をより厳格に実施していく意向が強くなってきている。また、サービス利用者の間では、認証に必要な個人情報の登録機会が少なく、情報漏えいの危険性を低く抑えやすい認証への期待が高まっている。

本研究開発においては、異なるCA間の連携場面を想定し、公開鍵証明書のような、システム処理や情報端末処理等に係る負荷が大きい認証情報や、情報漏えいの危険性があるアイデンティティ情報について、CA間での受け渡しが発生しない、匿名性、安全性、処理効率性の高い認証方式を開発するとともに、その中に含まれるCA間の認証ローミングのためのプロトコルを開発する。

研究開発状況(概要)

・平成17年度より以下の研究開発を実施中。

(1)異なるCA間でアイデンティティ情報の受け渡しが発生しない高速かつ安全な認証方式の開発

(2)(1)を実環境で有効に機能させるための実証実験

…平成18年8月30日にセブンイレブンと中央大学の協力により、本研究の成果を活用した在籍証明書発行のデモを実施し、さらにその成果について報道発表を行った。また、同様のデモを平成18年11月22日に市川市役所にて実施した。

・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　連携研究部門　委託研究グループ
(http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm) 電話　042－327－6011

将来の方向性

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

対象技術 その他認証技術

テーマ名 ネットワーク認証型コンテンツアクセス制御技術の研究開発

開発年度 平成18年度～平成20年度

実施主体 富士通(株)、東京工業大学
(情報通信研究機構（NICT）が実施する委託研究の委託先)

背景、目的

インターネットの普及、低価格化により、ネット上での情報流通、商取引などの機会の増加が見込まれている。また、医療、金融など、いわゆるミッションクリティカルな分野にもその利用が拡大し、遠隔診断、リアルタイム受発注などでの応用も計画されている。一方、インターネット上での詐欺、情報不正入手など、いわゆるネット犯罪も増加傾向にあり、健全なネットワーク社会の発展への影響が不安視されている。

ネットワークの危険性が高まる中、より高いセキュリティが通信システムにも求められている。現在の通信システムはID／パスワード、電子証明書など、単一の証明システムにより運営されているケースが多いが、脅威に対応するためにはこれらを複合的に利用し、セキュリティ強度を高めていく必要が出てきている。利用者の目的に従い複雑化する認証を統合的に扱い、その認証に応じてネットワークを制御し、コンテンツの流通を管理できる技術の開発を行う。

複数の認証技術・機関にまたがる認証技術を統合的に扱うためには、アプリケーションにおける利用者認証、利用している機器、ネットワークなどの利用環境の、それぞれのレイヤで認証と管理を行う仕組みが必要となる。しかし、現状では各レイヤでの管理は独立して行われているため、これを総合的に判断する仕組みは規定されていない。また、利用者、環境などは複数の対象、複数管理機関が存在するが、これらを含めた全体の状況を認証するシステムが必要となる。

複数の認証技術・機関にまたがる認証を統合的に扱える技術「複数認証連携技術」と、その認証応じてネットワークを最適に制御する「ポリシーやコンテンツに応じたネットワーク制御技術」の二つの基盤技術の開発を行う。

研究開発状況（概要）

・平成18年度より以下の研究開発を実施中。

(1) 複数認証連携技術

(2) ポリシーやコンテンツに応じたネットワーク制御技術

(3) 複数認証ドメイン管理基盤技術

・平成20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　連携研究部門　委託研究グループ
（http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm）電話　042－327－6011

将来の方向性

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

対象技術 侵入検知技術

テーマ名 ネットワークセキュリティ技術の研究開発

開発年度 平成18年度～平成22年度

実施主体 独立行政法人情報通信研究機構

背景、目的

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

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

研究開発状況（概要）

平成18年度には、これまでに研究開発した広域に設置された観測点からのセキュリティログの分析手法に加えて、より詳細な分析が可能なログを収集する機構を新たに整備し、それにより得られたログの分析手法の開発に着手した。この結果をこれまでに構築したインシデント分析システムプロトタイプに反映する作業に着手した。また、マルウエアによるネットワーク影響トラヒックから攻撃ベクターを抽出し、攻撃検知技術に利用する研究を、再現ネットワーク上に攻撃影響トラフィック再現・収集機構を構築して行うことに着手した。

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　情報通信セキュリティ研究センター推進室　042-327-5774

将来の方向性

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

対象技術 その他認証技術

テーマ名 次世代電子認証基盤の整備

開発年度 平成17年度～平成18年度

実施主体 財団法人日本情報処理開発協会及び日本電気㈱他7社（経済産業省からの補助金）

背景、目的

現在、部門内あるいは企業内といった閉じた範囲でそれぞれ認証技術が適用されている。企業の枠を超えた共同体全体の最適化に向けたプラットフォームとして、各サービスの連携による最適化を実現し、さらにはサービスの複合による価値の向上を実現するため、複数のサービスから共有可能な次世代認証基盤の技術基盤の開発を目的とする。

研究開発状況（概要）

平成17年度

平成17年度は電子認証技術とそれを取り巻く環境について調査研究開発を行い、以下の3つの開発成果をあげた。

(1)主にBtoC分野でのシステムと機能、情報の流れと管理方法、関与者の運用と責任範囲、関与者の利益分配方法、関与者間の契約及び制度からなるビジネスモデルを策定

(2)日本国内の実情に合う保証レベル、審査要件とビジネスルール要件から成る規範、認証手段の運用要件、技術要件から成る基準を、電子認証ポリシーガイドライン規範基準編として策定

(3)認証属性情報処理機能、アクセス制御情報処理機能を備えるSP(サービスプロバイダ)の基盤ソフトウェア、及びCSP(クレデンシャルサービスプロバイダ)-SP連携機能、利用者情報管理機能を備えるポータルサイトサーバの基盤ソフトウェアを開発し評価実験を実施

平成18年度

平成18年度は、平成17年度の成果を踏まえてビジネスモデルの汎用化研究、電子認証ポリシーガイドラインの基準規範に沿った運用の評価方法の調査研究、より柔軟性のある基盤ソフトウェアの開発に重点を置き、以下の成果をあげた。

(1)BtoB分野の事業者のヒアリング調査等を踏まえ、同分野での有望なビジネスモデル、関与者の役割と責任、ルール雛型の検討を行い、BtoB電子認証ビジネスモデルを策定

(2)BtoB分野に対応するため、自然人以外(法人等)も含めて認証に関わる要件を整理し、電子認証ポリシーガイドライン基準規範編に追加拡充を実施

(3)CSPの評価に関わる事項を調査･整理し電子認証ポリシーガイドラインCSP評価仕様編として策定

(4)平成17年度評価実験の課題を整理し、電子認証基盤ソフトウェアを認証連携機能モジュール、サービス連携機能モジュール、クライアントモジュール構成とすることで、多様なシステム構成が組めるよう機能強化を実施。また、電子認証基盤ソフトウェアを導入しシステム構築を行う際の手引きとなるシステム導入ガイドラインを作成すると共に、システムテストなどに役立つサンプルソフトウェアを含むソフトウェアパッケージを作成

(5)大阪商工会議所、リスクモンスター株式会社の協力を得て、サービス連携実証実験システムの構築、電子認証ポリシー、各種契約書等を作成し、モニター企業による実証実験を行い、上記(1)～(4)の妥当

性、フィージビリティを検証

詳細の入手方法（関連部署名及びその連絡先）

〒143-0016

東京都大田区大森北1丁目23番5号第一小田ビル5F

日本PKIフォーラム推進本部

本部長　加藤　晴彦

電話番号：03-5297-2311

URL：http://www.japanpkiforum.jp/

将来の方向性

主に中小のインターネット関連企業に向け、異業種サービス連携等による付加価値を高めたサービス提供を目指した電子認証基盤の普及・推進を図っていく。

対象技術 その他認証技術

テーマ名 高信頼性端末の電子認証基盤の調査研究

開発年度 平成17年度～

実施主体 社団法人日本画像情報マネジメント協会（経済産業省からの委託）

背景、目的

現在、情報通信ネットワークを介したさまざまなサービスが利用可能となりユーザーの利便性は大きく向上している一方、パーソナルコンピュータ(PC)等の端末に対するセキュリティ上の脅威も増大している。例えば、セキュリティ・ホールなどを通じ、PCにスパイウェアが埋め込まれ、ネット・バンク等のID・パスワードが盗まれるといった新たな脅威も生じている。

本事業では、こうした現状を踏まえ、国際的な業界団体TCG(Trusted Computing Group)が提唱する強い耐タンパ性を持つTPM(Trusted Platform Module(*))を搭載したPCに注目し、安全性確保の観点からTPM搭載PCを活用していくに当たって必要な技術要件に係るガイドラインを作成する。

また、国際的な整合性と相互運用性に留意しつつ、TPM搭載PCのソフトウェアの設定等を遠隔で管理することを可能とする構成検証プロトコルを作成するとともに、TPM搭載PCを利用して医療画像等の情報資産を取扱う実証的調査も行う。

*TPM（Trusted Platform Module）耐タンパ性の高機能セキュリティチップ

研究開発状況（概要）

（ガイドラインの策定）

信頼できるコンピューティング環境を構築する業界団体TCG（Trusted Computing Group）が策定するTPMに関する業界標準について調査研究を行い、各種デバイスのセキュリティ・アーキテクチャに係るガイドラインを作成する。

（通信仕様の試験実装及び実証）

TPMを搭載したPC間でモジュール構成証明(Attestation)を行うネットワークプロトコルであるTNC(Trusted Network Connect)仕様に基づいた試験実装と実証を実施する。

詳細の入手方法（関連部署名及びその連絡先）

〒101-0032

東京都千代田区岩本町2－1－3和光ビル7階

社団法人日本画像情報マネジメント協会

電話番号：03-5821-7351

URL：http://www.jiima.or.jp

将来の方向性

TPMを搭載したPC間でモジュール構成証明を行うTNC(Trusted Network Connect)仕様に基づいた試験実装等の成果は、今後、TCG及びIETFにおける同仕様の国際標準策定作業に向けた提案をなするとともに、先導的な事例として同仕様の普及の促進に貢献すると期待される。

対象技術 その他認証技術

テーマ名 電子認証フレームワークとIPアドレス認証の展開に関する調査研究

開発年度 平成17年度～

実施主体 社団法人日本ネットワークインフォメーションセンター（経済産業省からの委託）

背景、目的

高度情報通信ネットワークの基幹であるインターネットは、電子政府を始め、企業、教育機関、医療機関等において幅広く利用されており、その安全性を確保するための方法の1つとして、電子認証が行われている。

電子認証では、ネットワーク等を通じたアクセス元の本人性を電子的に確認する仕組みとして、第三者による証明となる認証局（Certification Authority）が構築・運営されているが、利用場面毎に体系だったフレームワークが構築されておらず、このことが適切な電子認証の利用や普及の妨げになっている。

本事業は、日本国内のIPアドレス等のネットワーク登録情報を活用した電子認証に係る実証試験を行い、電子認証の普及に必要な仕組みとなる「電子認証フレームワーク」を策定することにより、日本国内の情報インフラの根幹となる電子認証基盤の構築に資することを目的とする。

研究開発状況（概要）

当センターが管理運営するIPアドレス、AS番号などの登録情報を活用し、インターネットの安定性向上を図る電子認証について調査研究を行うと共に、電子認証の適切な普及を図るためのベストカレントプラクティスを策定する「電子認証フレームワーク」の構築に関する調査研究および研究開発を行っている。

登録情報を活用した電子認証については、インターネットサービスプロバイダー（ISP）におけるルーティング（経路制御）の信頼性向上に役立つ「経路情報の登録機構」の技術開発を行う。

また電子認証の標準技術的なノウハウの蓄積および集約を図る活動「電子認証フレームワーク」の調査研究を行っており、電子認証技術の実用性向上と普及を図る。

詳細の入手方法（関連部署名及びその連絡先）

〒101-0047
東京都千代田区内神田2-3-4　国際興業神田ビル6F
社団法人日本ネットワークインフォメーションセンター
技術部・インターネット推進部
電話番号：03-5297-2311
URL：http://www.nic.ad.jp/

将来の方向性

当該事業で開発する電子認証を利用したIPアドレスとルーティングレジストリの連携機構の適用により、信頼のおけるIPアドレスの登録情報管理が実現するとともに、インターネットにおけるIPアドレスの不正利用を排除することにより、安全・安心な電子認証基盤の構築を目指すものとする。

対象技術 その他認証技術等

テーマ名 ユビキタスネットワーク向けセキュアアセットコントロール技術の研究開発

開発年度 平成17年度～平成19年度

実施主体 独立行政法人産業技術総合研究所 情報セキュリティ研究センター (経済産業省からの委託)

背景、目的

情報技術の進歩や社会情勢の変化に伴い、情報セキュリティに係る脅威は急速に変化・拡大していることから、これまでの対症療法的な対策だけではなく、長期的な視点に立って、情報セキュリティ上の問題の根本的な解決を目指した研究開発を行っていくことが極めて重要となっている。

そこで本研究開発では、このような根本的な問題解決を目指した研究開発を実施することを目的とし、対症療法的ではなく根本的な情報セキュリティ上の問題解決に資する技術であって、情報セキュリティ総合戦略に掲げられている「高回復力・被害局限化の確保」及び「高信頼性」のための基盤強化に資する研究開発を実施する。ユビキタスネットワークの進展に伴い国民生活の至るところに情報デバイスが浸透し，これらを使った新しい便利なサービスが次々に開発されつつあり，これらのサービスの発展が今後の日本の国際競争力を高めると期待されている．しかし，現状では利便性とスピードを優先するあまり，莫大な量に及ぶ個人のプライバシー情報と機密情報をデバイス等を通じて獲得するにもかかわらず，提供するユビキタスサービス自体の不正利用者に対する安全性や利用者のプライバシーや機密に関わる情報管理は必ずしも重視されていない．

そこで本事業では，産業技術総合研究所がこれまでに蓄積している暗号／認証技術，脆弱性検証技術，不正利用者追跡技術などに関する最新の理論的な知見を生かし，ユビキタスネットワーク関連分野のリーディング企業とパートナーシップを組むことにより，次世代の信頼性の高いユビキタスネットワークを構築する基盤技術の確立を目指す．

研究開発状況 (概要)

匿名認証と匿名情報連携、不正利用者追跡、脆弱性検証等の想定される課題について、平成17年度は単独での研究開発および環境整備を行うとともに、将来の技術展開に向けたコーディネーションおよび、その実施に必要な調査を行った。平成18年度は、企業との共同研究体制の構築と、プライバシー保護技術、不正利用者追跡技術、脆弱性検証技術の基礎技術開発を行っている。

詳細の入手方法 (関連部署名及びその連絡先)

独立行政法人産業技術総合研究所 情報セキュリティ研究センター

電話:03-5298-4722

将来の方向性

上記のような、対症療法的ではなく根本的な情報セキュリティ上の問題解決に資する技術を確立することで、より高次元で安全・安心を実現可能とする社会基盤となっていく。

対象技術 その他認証技術等

テーマ名 情報漏えいに堅牢な認証･データ管理方式とそのソフトウェアによる安全な実装･検証手法に関する研究開発

開発年度 平成17年度～平成19年度

実施主体 独立行政法人産業技術総合研究所 情報セキュリティ研究センター (経済産業省からの委託)

背景、目的

情報技術の進歩や社会情勢の変化に伴い、情報セキュリティに係る脅威は急速に変化･拡大していることから、これまでの対症療法的な対策だけではなく、長期的な視点に立って、情報セキュリティ上の問題の根本的な解決を目指した研究開発を行っていくことが極めて重要となっている。

そこで本研究開発では、このような根本的な問題解決を目指した研究開発を実施することを目的とし、対症療法的ではなく根本的な情報セキュリティ上の問題解決に資する技術であって、情報セキュリティ総合戦略に掲げられている「高回復力･被害局限化の確保」及び「高信頼性」のための基盤強化に資する研究開発を実施する。具体的には「事故は起こりうるもの」との前提に立ち，仮に情報の一部が漏えいしたりシステムの一部に脆弱性が存在したとしてもある程度の安全性を確保するための技術 (フェイルセーフなセキュリティ技術) に関する研究開発を，方式の設計から実装に至るまでの各工程を見直すことにより行う．それによりビジネス継続性や人災を含む災害復旧能力の向上に貢献する．

研究開発状況 (概要)

平成17年度では、コアモジュールとなる認証鍵共有方式の既存方式を調査し、それらを、必要となる情報、情報漏洩の影響、ユーザビリティ等の観点から、計算機･ネットワーク環境も利用しつつ比較を行い最適な方式の提案を行った。さらに提案する方式の実装を含めた安全性検証に用いる手法の検討を行い、その手法自体の実装に着手した。結果として、クライアントやサーバが不正アクセスを受け流出した情報が解析されたとしても、利用者が設定しているパスワードや保存しているデータを保護できる方式のプロトタイプを開発すると共に、それらを安全に実装するための安全性検証機能付きC言語処理系の開発を行った。18年度は、提案した認証･データ管理方式をクラスタ構成にすることでノードの破壊に対する耐性を高めると共に、処理系や実行時検証コードの性能を向上させる。

詳細の入手方法 (関連部署名及びその連絡先)

独立行政法人産業技術総合研究所 情報セキュリティ研究センター

電話:03-5298-4722

将来の方向性

上記のような、対症療法的ではなく根本的な情報セキュリティ上の問題解決に資する技術を確立することで、安全･安心な社会の構築を実現する。

対象技術 認証技術

テーマ名 アクセスグラフに基づくボットネット検出技術の研究開発

開発年度 平成17年度～平成18年度

実施主体 株式会社 三菱総合研究所 (経済産業省からの委託)

背景・目的

インターネット上でボットネットを悪用した詐欺や攻撃などによる経済的被害が急増している。ボットネットは、ワームによって乗っ取られたＰＣで、遠隔からコントロールすることで、フィッシング詐欺メールやスパムメールの送信、DDoS攻撃などを行うために悪用されている。インターネット上のボットネットを検出し、それらを無効化したり、それらを発信元とするメールをブロックすることができれば、インターネット上で発生する被害を大幅に減らすことが可能になる。従来、受信するメール全体のアクセス関係から送信元の脅威を推定する研究は行われていなかった。そのため、本研究では、メールサーバで受信されるメールの送信元IPアドレスおよび送信先メールアドレスのアクセス関係から、送信元の脅威を推定することでボットネットを検出する技術を開発することを目的とする。

研究開発状況 (概要)

ここ数年、広域に構築されたボットネットによるDDoS攻撃が増加している。ボットネットのように、様々なプロバイダをまたいだネットワークからの攻撃はきわめて防御が難しい。インターネットの安定を維持するためには、攻撃を未然に防ぐためボットネットを検出する技術開発が必要である。ボットネットの主要な用途はスパムメールの送信とされている。電子メールのヘッダ情報には、電子メールの送信元IPアドレスが記録されているため、この情報を抽出し、さらに送信先メールアドレスとの空間構造からボットネットワークの存在を検出する技術を研究している。現在、検出技術の実装を終え、収集したスパムメールからボットネットと考えられるアドレスブロックを検出することが可能である。今後の課題として、時系列に沿ってアドレスブロックを比較し、ボットネットワークの時間的振る舞いを検証すること、多くのスパムメールを収集することで、ボットネットの一部が、インターネットのどの部分に影響を及ぼしているのかを考察することがあげられる。本技術は、部分データから全体を推測できることが特徴であり、エンドユーザ環境においても利用可能なため、SOHOユーザ、家庭環境をボットネットの影響から守るために役立たせることが期待できる。

詳細の入手方法 (関連部署名及びその連絡先)

〒100-8141
東京都千代田区大手町2－3－6
株式会社三菱総合研究所 情報セキュリティ研究部 部長 村瀬一郎
Tel:03-3277-5605, Fax: 03-3277-3473, E-Mail: murase@mri.co.jp
URL: http://www.mri-security.jp/

将来の方向性

本事業では、平成18年度末までに、以下の技術に関する研究開発を実施する予定である。

(1) ボット検出技術の研究開発

メール送受信情報管理データベースから、送信元IPアドレス、送信先メールアドレスを取得し、以下に示すグラフ構造分析手法を用いて送信元の脅威を計算する。これによって得られた脅威度の高い送信元は、ボットであると判定することができる。

(2)メール送受信情報の取得管理技術の研究開発

受信するメールの送信元IPアドレス、送信先のメールアドレス情報を抽出し、送受信情報データベースに保存する。SMTPサーバの処理に依存しないよう、SMTPの前段で取得し、処理したメールは、通常のSMTPサーバに転送する。

⑶ スパムメール収集技術の研究開発

(1)によって求められた脅威度に基づいて、脅威度の高い送信元IPアドレスをボットネットに属するPCとみなし、これらから送られてきたメールをスパムメールと判断してスパムメールデータベースに保存する。

⑷ ボットネット分析技術の研究開発

(1)から(3)により得られた情報を基に、ボットネットに属するPC間の相互の関係性を分析し、あるボットネットに属すると想定される複数のPCのアドレスを示す。

(別添2)

企業名(及び略称) サイバーエリアリサーチ株式会社	
代表者氏名 山本 敬介	
所在地(郵便番号及び住所) 静岡県三島市一番町18-22 ｱｰｻｰﾌｧｰｽﾄﾋﾞﾙ4F	
関連部署名及び電話番号 055-991-5544	
URL http://www.surfpoint.jp/	
対象技術	技術開発状況
その他認証技術等 開発年 2000年	オンラインゲーム業界で問題となっているRMT(Real Money Trading)対策として、海外からの不正アクセスをブロックすることが必要。 これを実現する手段としてIPアドレスデータベースを開発。IPアドレスによりアクセスユーザーが日本国内であるか海外であるかを自動認識することが可能で、オンラインゲーム業界においては、判定結果を元に中国からのアクセスを遮断することに成功している。 ●具体的な閲覧制限モデル 1.海外からの不正なアカウント(ID)登録やゲームサーバへのアクセスをブロック。 2.海外からProxyサーバを使用したなりすましをブロック。 3.登録・認証時の住所などの都道府県判定に使用し、虚偽登録・認証をブロック。 ●IPアドレスの取得方法とサービス提供方法 日本国内に割り振られたIPアドレスレンジを独自調査し、一般コンシュマーのインターネット接続に利用されるISPの利用するIPアドレス、および企業専用線に利用されるIPアドレスを調査収集。 海外割り当てのIPアドレスレンジにおいて、日本国内での利用が確認されたものについて、および匿名性を保つために利用されているプロキシサーバのIPアドレスも同様に調査収集。 上記により、海外およびプロキシサーバ経由のアクセスユーザーのコンテンツ閲覧を遮断することを可能にするデータベースを構築。 このデータベースをWEBサーバ(Apache IISに対応)上で動作するサーバモジュールとして提供することで、導入先の作業工数を削減するソリューションとして展開。

企業名（及び略称）大日本印刷株式会社 IPS事業部	
代表者氏名　蟇田 栄	
所在地（郵便番号及び住所）〒162-8472東京都新宿区榎町7	
関連部署名及び電話番号 ICカードビジネス開発本部アプリケーション開発部	
ＵＲＬ　http://www.dnp.co.jp/jis/news/2006/060807.html	
対象技術	技術開発状況
その他認証技術等 (平成18年)	ICカードによるネットワーク管理型PC個人認証： 情報システム利用者の権限情報と認証情報をサーバで集中管理し、PCの不正利用、情報漏洩をシャットアウトする、ICカードを利用したPCセキュリティシステム。SSFC製品との連携も可能。 ●クライアント機能 ICカードログオン認証/スクリーンロック、外部記憶デバイス利用制御、電子証明書（PKI）の利用、SSFC連携機能（ICカードの入室情報チェック）、操作ログ送信、など。 ●管理サーバ機能 ユーザ認証情報、ポリシーをサーバにて一括管理 ●管理者機能 PINロック時やカード紛失時など、ユーザに対する緊急サポートをWeb上から容易に行うことが可能。

企業名（及び略称）	株式会社トリニティーセキュリティーシステムズ （T-SS）
代表者氏名	代表取締役社長 林 元徳
所在地（郵便番号及び住所）	〒101-0031 東京都千代田区東神田一丁目7番8号 アルテビル東神田8階
関連部署名及び電話番号	戦略企画本部 03－5835－0287
URL	http://www.trinity-ss.com

対象技術	技術開発状況
その他認証技術等 （2004年）	IPN (Identified Private Network) ワンタイムパスワード相互認証方式「SAS-2」（Simple And Secure password authentication protocol, ver. 2）と、業界標準の暗号化方式AESを組み合わせ、端末間の相互認証とネットワークを利用して送受信されるデータの安全性を実現する。 「SAS-2」は、認証に必要な認証鍵をパケットごとに更新し、その認証鍵をネットワークに流すのではなく、認証鍵を生成するためのハッシュ値のみを通信することで、認証鍵の盗聴による「なりすまし」を不可能としている。また、データの暗号化にはAESを利用し、暗号化されたパケット以外は破棄することで不正アクセスを遮断する。さらに暗号化と復号に必要な暗号鍵は、相互認証を行うためのハッシュ値から動的に生成することにより、ネットワーク上を流れず、また、生成された暗号鍵の再利用はできない。 このように高度なセキュリティを確保しながらも認証や暗号化・復号に要する処理負荷が極めて軽く、スループットの劣化がほとんど発生しない。

企業名（及び略称）	日本通信株式会社
代表者氏名	代表取締役社長　三田　聖二
所在地（郵便番号及び住所）	〒140-0013　東京都品川区南大井6-25-3 ﾋﾞﾘｰｳﾞ大森
関連部署名及び電話番号	事業開発室　03-5767-9406
URL	http://www.j-com.co.jp

対象技術	技術開発状況
侵入検知技術 （既に商品化し販売中）	不正アクセスに対する侵入検知技術（侵入防御技術を含む。以下同様とする。）は、従来、大企業の本社やデータセンターのような大規模なネットワークを防御するために開発されており、大型かつ高価な製品が主流となっていました。これに対し、当社グループは小規模な事業所、家庭または個人で利用するノートPC等の小規模なネットワークを防御する侵入検知技術（以下、「本件技術」という）を開発しました（商品名：「Ally ip100」）。 従来の侵入検知技術は、既知の不正アクセスの特徴をデータベース化し、個々のアクセスを当該データベースと照合することで不正な侵入を検知し、また防御する方法（いわゆる前科者リストとの照合）によっていました。 この方法では、データベースを備える必要があるため、以下の理由により、大型かつ高価な設備となることは免れません。 1)　個々のアクセスをデータベースと照合するため、相当高いコンピューティングパワーを必要とする 2)　データベースを常に更新し続けなければならない また、当然ながら、データベースに登録されていない、未知の種類の不正アクセスには対応することができません。 本件技術では、データベースと照合する方法ではなく、IPネットワークのプロトコルの特徴（例えば、TCPの3 way handshake）を活用することにより、個々のアクセス要求に対して、パケットに独自のタグ(TAG-UR-IT)を付け、その判別を行うことで、以下の機能を提供します。 （1）アンチ・スキャニング 不正アクセスの前に行われる、ネットワークのポートスキャニング（偵察）を検知し、防御します。 （2）不正侵入防御 プロトコル上に意図しないアクセスを検知し、防御します。 （3）異常パケット遮断 プロトコルに違反したパケットや短期的に大量発生したセッションを検知し、通信を遮断します。 本件技術は、データベースを備える必要がないため、プログラムサイズが小さく、小型かつ比較的低価格での提供が可能です。 また、ネットワークの構成変更、アドレス変更に依存しない「プラグアンドプロテクト」と称する技術により初期設定や設置を容易に行うことができます。

	さらに、本件技術はブロードバンドルーター等、グローバルIPが割り当てられる装置そのものに組み込むことが可能であり、この種の装置全てに対して不正侵入を防御できる可能性を有しています。

企業名（及び略称）	株式会社ニーモニックセキュリティ
代表者氏名	國米　仁
所在地（郵便番号及び住所）	〒530-0057大阪市北区曽根崎2丁目16番19号
関連部署名及び電話番号	本社　06-6361-5311
ＵＲＬ	http://www.mneme.co.jp

対象技術	技術開発状況
本人認証技術 平成１２年から開発開始	どんなに頭の良い攻撃者が如何に手の込んだ攻撃方法を考え出しても、個々人それぞれが長い人生の中で蓄積してきた無尽蔵とも言える当該人物固有の記憶を当該人物の主観的な文脈通りに取り出すことはできないという原理を基に、懐かしい昔の写真などの長期視覚記憶を活用する本人認証技術（人物・事物・風景の写真やイラストを画面に多く並べ、その中に長期記憶となっている写真やイラストを暗証画像として混ぜておき、これら暗証画像を過不足なく選択すると本人であると認証）を応用した本人認証製品が既に以下の用途で実際に活用。 ・オンラインでのアクセス時のユーザ認証（フィッシング排除機能あり） ・ＰＣや携帯端末のログオン認証・所有者認証 ・常態では暗号鍵を存在させないデータ暗号化ソフトの鍵復元

企業名（及び略称）	日本ユニシス株式会社
代表者氏名	富田　孝志
所在地（郵便番号及び住所）	〒135 - 8560　東京都江東区豊洲1 - 1 - 1
関連部署名及び電話番号	商品企画部　03 - 5546 - 4111
ＵＲＬ	http://www.unisys.co.jp/ubiquitous/idagent.html

対象技術	技術開発状況
本人認証技術 平成１２年から開発開始	技術開発状況： ICカードによるネットワーク管理型PC個人認証 1.　クライアントＰＣ セキュリティ Windows ログオン認証、スクリーンロック、利用者制限、外部メディアの利用制限 2.　認証サーバによるネットワーク型管理 利用者、PC毎に異なる情報セキュリティポリシーの設定、PC利用ログの集中管理、Active Directoryとの自動連携 3.　SSFC 対応 SSFCフォーマットのICカードを読み取り、入退室システムとの連携を実現（ICカードに入室情報が確認できない場合はPCを利用できないなど） 4.　PKI 対応 電子証明書や秘密鍵をICカードに格納し、PKIを利用可能（接触型ICカードのみ）

(別添3)

[大学]

大学名　石巻専修大学	
所在地（郵便番号及び住所）　986-8580 宮城県石巻市南境新水戸1	
関連部署名及び電話番号　0225-22-7716	
URL　http://www.isenshu-u.ac.jp/general/	
対象技術	技術開発状況
データ	株式会社エマージングテクノロジーズと株式会社アドテックシステムサイエンスとの共同開発。 Windowsアプリケーションソフトとハードウェア（USB）キーの組み合わせで動作する情報セキュリティシステム。

大学名　茨城大学　工学部	
所在地（郵便番号及び住所）　316-8511 茨城県日立市中成沢町4-12-1	
関連部署名及び電話番号　0294-38-5135	
URL　http://kuro.cis.ibaraki.ac.jp/~kurosawa/KuroIwa.htm	
対象技術	技術開発状況
通信情報	CMAC：米国政府（NIST）に標準認証コードとして採用されている。

大学名　岩手県立大学	
所在地（郵便番号及び住所）　020-0193 岩手県岩手郡滝沢村滝沢字巣子152-52	
関連部署名及び電話番号　地域連携研究センター　019-694-3330	
URL　http://www.iwate-pu.ac.jp/	
対象技術	技術開発状況
データ	①アクセス制御を行うものではなく、別の視点からその補完を行う。 ②ホームページデータ（含む属性データ）の改ざん防止を行う。 ③ホームページデータそのものにその真正性を証明する機能を付与。 ④真正性の付与は、ホームページ製作者がデジタル署名データを付与することで達成する。（RSA暗号ディタル署名） ⑤ホームページコンテンツとディジタル署名との照合チェックを定期的にパトロールして実施するパトロールサーバを置く。 ⑥パトロールサーバ自身の安全のため、パトロールサーバはインターネットを介さず、イントラネットによりFTPサーバ、Webサーバを監視する。 ⑦パトロールサーバは、不正侵入の危険の高いFTPサーバを主として監視し、ホームページの正規更新と改ざんとを見分ける。正規更新と判定したもののみをWebサーバへ移す。改ざんと判定したものはバックアップデータへ復旧するとともに改ざんデータを記録し、管理者とホームページ製作者へ通知する。 ⑧ディジタル署名のための鍵格納媒体はUSBトークンで、署名操作は画面上のワンクリックで達成される。 ⑨同類他製品はすべてサーバ管理者が判断して真正証明データを付与しているのに対し、本方式は作成者が付与するのでより間違いがない。

大学名　熊本大学総合情報基盤センター　ネットコミュニケーション研究部	
所在地（郵便番号及び住所）　860-8555 熊本県熊本市黒髪2-39-1	
関連部署名及び電話番号　熊本大学　総合情報基盤センター　事務室 096-342-3824	
URL　http://www.cc.kumamoto-u.ac.jp/	
対象技術	技術開発状況
ネットワーク	DNSクエリアクセスを監視して、セキュリティインシデントを検知し、ファイアウォールやDNSサーバと連携して該当IPアドレスレベルでアクセス制御を行う。アクセス制御自動的に行われ、アクセス制御テーブルが溢れないように工夫している。 DNSのログ機能を使い、簡単なスクリプトで実現できるのが特徴である。 直接該当プロトコルのパケットやストリームを見ずにDNSクエリパケットのアクセスの特徴を検知し、DNSクライアントの状況を判断する独自発想に基づくセキュリティインシデント検知システムである。

大学名　信州大学　大学院　工学系　研究科　情報工学専攻　情報セキュリティ講座	
所在地（郵便番号及び住所）　380-8553　長野県長野市若里4-17-1	
関連部署名及び電話番号	
URL　http://security.cs.shinshu-u.ac.jp/	
対象技術	技術開発状況
通信情報 データ	プリンタ出力における ①出力先の指定 ②印刷物を受け取る人の指定 ③目前印刷 を可能にする。

大学名　広島大学　情報メディア教育センター	
所在地（郵便番号及び住所）　739-8511　広島県東広島市鏡山1-4-2	
関連部署名及び電話番号　情報化推進部広報グループ　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、株式会社ネットスプリングにて開発した製品である。

【企業】

事業体(研究所)名　NECソフトウェア北陸	
所在地（郵便番号及び住所）　920-2141 石川県白山市安養寺1番地	
関連部署及び電話番号　第三ソリューション事業部 0761-93-4621	
URL　http://www.hnes.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 データ 施設	人の動線（入退室など）に合わせ、セキュリティ対策の重要な要素である「人、物、情報」を統合的に管理するソリューションシステム。

事業体(研究所)名　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	
関連部署及び電話番号　03-5730-5000	
URL　http://www.nec-nexs.com/	
対象技術	技術開発状況
サーバ データ	ホスト型Web Application FireWall。サーバーにインストールして検知、検証、改竄復旧などの機能をもつ。SQLインジェクション、XSS対策に使用可。

事業体(研究所)名　NECフィールディング株式会社	
所在地（郵便番号及び住所）　108-0073 東京都港区三田1-4-28 三田国際ビル20F	
関連部署及び電話番号　コーポレート・コミュニケーション部 03-3452-7093	
URL　http://www.fielding.co.jp/	
対象技術	技術開発状況
ネットワーク サーバ データ	顧客サイトにIDS、IPSを設置し、リモートからモニタリングを行う。不正なアクセスを検知、または防御した時に当社監視センターへ通報するとともに、顧客の管理者へ通知を行う。毎月レポートを提出して報告する。（Webポータルによるリアルタイムにレポートすることも可能）

事業体(研究所)名　NECフィールディング株式会社	
所在地（郵便番号及び住所）　108-0073 東京都港区三田1-4-28 三田国際ビル20F	
関連部署及び電話番号　コーポレート・コミュニケーション部 03-3452-7093	
URL　http://www.fielding.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 データ 施設	ソリトンシステムズ社の認証システム（SmartON）をベースに、物理認証（入退室管理）からネットワークへの接続コントロール、サーバへのログオン認証を統合するシステムのインテグレーション。

事業体(研究所)名　株式会社NTTPCコミュニケーションズ	
所在地（郵便番号及び住所）　105-0004 東京都港区新橋6-1-11 ダヴィンチ御成門	
関連部署及び電話番号　経営企画部 03-3432-9684	
URL　http://www.nttpc.co.jp/	
対象技術	技術開発状況
ネットワーク	ユーザのシステム環境や利用用途に応じて、様々なVPNサービスを提供する。また、複数の通信事業者のネットワークサービスとの組み合わせでも提供しているので、冗長性に優れたネットワークの構築が可能となる。

事業体(研究所)名　RSAセキュリティ株式会社	
所在地（郵便番号及び住所）　100-0005 東京都千代田区丸の内1-3-1 東京銀行協会ビルヂング１３F	
関連部署及び電話番号　技術統括本部 03-5222-5200	
URL　http://www.rsasecurity.co.jp/	
対象技術	技術開発状況
サーバ 通信情報	①認承管理：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承。認承方法として、パスワード、電子証明、ワンタイムパスワード等を使用可能。 ②シングルサインオン：一度認証成功したユーザには認承トークンを発行。認承トークン有効期間内であれば、ユーザは再認承することなく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。 ③ルーツ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に基づいての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。

事業体(研究所)名　RSAセキュリティ株式会社	
所在地（郵便番号及び住所）　100-0005 東京都千代田区丸の内1-3-1 東京銀行協会ビルヂング13F	
関連部署及び電話番号　技術統括本部 03-5222-5200	
URL　http://www.rsasecurity.co.jp/	
対象技術	技術開発状況
クライアント 通信情報	一分間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形成し表示するカード型のデバイスを、認証を希望するユーザ側に配備し、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承側に送付する。認承側（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承装置に転送して認証の代行を依頼し、その回答により認承の可否を決定する。認承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発生し、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。

事業体(研究所)名　RSAセキュリティ株式会社	
所在地（郵便番号及び住所）　100-0005 東京都千代田区丸の内1-3-1 東京銀行協会ビルヂング13F	
関連部署及び電話番号　技術統括本部 03-5222-5200	
URL　http://www.rsasecurity.co.jp/	
対象技術	技術開発状況
クライアント	ユーザ情報やパスワードを記憶するサーバと、ユーザのPCから一旦ICカード等で認承されれば、事前に登録されたIDやパスワードのサーバからダウンロードされる。ユーザがパスワードを記憶する必要がなく、複雑なパスワードの設定が可能。ICカード紛失時にユーザが事前に登録された個人情報を回答すれば緊急のパスワード発行も可。答えるべき個人情報の数や許容する回答率をポリシーで管理でき、ICカードを紛失した場合と忘れた場合に別々で設定可能。その個人情報はどこにも保存されず、一定の正解率の場合にのみ暗号学的に処理され緊急パスワードが発行される。

事業体(研究所)名　TCBテクノロジーズ株式会社	
所在地（郵便番号及び住所）　108-0075 東京都港区港南2丁目11番19号 大滝ビル	
関連部署及び電話番号　管理部 03-5715-0623	
URL　http://www.tcbtech.co.jp/	
対象技術	技術開発状況
ネットワーク クライアント	不特定多数の利用者がアクセスする環境（ホテル、大学、コンベンションホールなど）でのアクセスコントロール（認証、帯域制御など）を行う。

事業体(研究所)名　TCBテクノロジーズ株式会社	
所在地（郵便番号及び住所）　108-0075 東京都港区港南2丁目11番19号 大滝ビル	
関連部署及び電話番号　管理部 03-5715-0623	
URL　http://www.tcbtech.co.jp/	
対象技術	技術開発状況
通信情報	ソフトウェアベースのSSL VPN。他のSSL VPN製品とは異なる次の様な特徴を持っている。 ①ハイパフォーマンス・ハイスループット ②全てのアプリケーションが使用可能 ③格段のコストパフォーマンス

事業体(研究所)名　TCBテクノロジーズ株式会社	
所在地（郵便番号及び住所）　108-0075 東京都港区港南2丁目11番19号 大滝ビル	
関連部署及び電話番号　管理部 03-5715-0623	
URL　http://www.tcbtech.co.jp/	
対象技術	技術開発状況
通信情報	IP電話やビデオ会議製品を使用した通話において、FirewallやNATの内側から外側に向けての通信をトンネリング技術を用いて①Firewallのセキュリティを低下させることが無く、②内部のアドレス情報を隠蔽して通話を行うことができる。 また、IP電話やビデオ会議製品による、音声、映像、データ通信の内容をAES方式（128bit/192bit/256bit）で暗号化し、通信内容の秘密を守ることができる。対応通信プロトコル：SIP、H.323、T.120

事業体(研究所)名　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 東京都大田区雪谷大塚町1-7	
関連部署及び電話番号　セキュリティーソリューション部 03-5499-8181	
URL　http://www.alsi.co.jp/	
対象技術	技術開発状況
ネットワーク クライアント	Inter SafeはURLデータベースに基づいて組織内のクライアントPCのインターネットアクセスをコントロールするウェブフィルタリングソフトである。ブラウザからの簡単な操作で、企業や教育機関にとって不要なサイトや有害なサイトへのアクセスをコントロールする。

事業体(研究所)名　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 東京都大田区雪谷大塚町1-7	
関連部署及び電話番号　セキュリティーソリューション部 03-5499-8181	
URL　http://www.alsi.co.jp/	
対象技術	技術開発状況
データ	Document Securityはドキュメント（ファイル）単位での作成、編集、保存、利用、破棄というライフサイクル全般をユーザ単位で管理する強力な情報漏洩対策ソリューションである。閲覧、編集、コピー＆ペースト、プリントスクリーン、印刷、印刷透かし、削除等を制御する。

事業体(研究所)名　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 東京都品川区上大崎3-1-1	
関連部署及び電話番号　03-5740-4050	
URL　http://www.isskk.co.jp/	
対象技術	技術開発状況
ネットワーク サーバ	Proventia不正侵入防御アプライアンスを導入することにより、インシデントが発生する前にはネットワークを防御することが可能となる。このアプライアンスは、顧客の組織が影響を受ける前にインターネット上の不正な攻撃を阻止する。事前に攻撃を阻止することはネットワークの動作を維持するための唯一有効な方法である。この結果、ITの資産管理に必要な負担を減らすことができ、またセキュリティの侵害を予防することができる。 ネットワークにインラインに設置することにより、Proventia侵入防御アプライアンスは顧客のビジネスに影響をあたえずに脅威を阻止する。 利点：リアルタイムの攻撃対応する商用レベルのパフォーマンスを達成し、不正なコードそして複合的な脅威をブロックする。Proventia侵入防御アプライアンスに使用されている技術により、NSS GroupのIPS Group Test（Edition 1）において、NSS Approvedアワードを取得した。 事前防御ー700以上のシグネチャでデフォルトのブロックレスポンス設定されている。これにより複合型の脅威の伝播を食い止めることができる。 世界をリードするセキュリティ調査能力とISS X-Forceのセキュリティ情報X-Forceは、一日24時間世界規模でイベントを監視し、調査そして開発を行っている。この結果がただちに製品のアップデートに反映され、最新の既知および未知の脅威に対応する。

事業体(研究所)名　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 東京都品川区上大崎3-1-1	
関連部署及び電話番号　03-5740-4050	
URL　http://www.isskk.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	ISSが提供するマネージドセキュリティサービスとは、監視センター（Security Operation Center＝SOC）より、顧客のサイトにあるセキュリティデバイスをセキュリティ専門技術者が24時間365日有人監視／運用／管理を行うサービスである。 ・監視サービス　MSS ・防御サービス　MPS 　セキュリティ専門技術者がリモートより監視／運用を行い、セキュリティの検証およびウィルス／ワームや不正アクセス検知時に迅速な対応を行う。 　ISSの監視センター（以下、SOC）は日本以外にも、米国（2拠点）、イタリア、ベルギーの世界5拠点に展開している。各拠点は密接に連携してバーチャルにひとつのSOCとして機能し、世界規模で監視活動を日々行っている。これらのSOCは、世界中で起きている脅威情報および運用バックアップデータシステムをリアルタイムに共有しているので、有事の際の迅速な対応を可能にしている。 　また、ISSが誇る世界最大の脆弱性研究チームX-Forceの検知／防御技術情報と脅威分析チームによる情報を元にセキュリティ脅威に対する事前防御を可能にしている。

事業体(研究所)名　インテック・ウェブ・アンド・ゲノム・インフォマティクス株式会社	
所在地（郵便番号及び住所）　136-0075 東京都江東区新砂1-3-3	
関連部署及び電話番号　先端IT事業部 03-5665-5011	
URL　http://www.webgen.co.jp/	
対象技術	技術開発状況
クライアント	デジタル証明書の発行、失効などを簡単に管理、運用できるパッケージである。これによりPKIに基づいた認証局の構築や運用が容易に行える。 ・PKIを簡単に構築（高度なPKI知識不要） ・各種PKIアプリケーション用証明書をサポート ・特定のアプリケーションと連携が可能 ・大規模PKIへの移行が可能。

事業体(研究所)名　ウィッツェル株式会社	
所在地（郵便番号及び住所）　102-0072 東京都千代田区飯田橋4-8-13 タカラビル	
関連部署及び電話番号　営業本部 03-5212-7123	
URL　http://www.witswell.co.jp/	
対象技術	技術開発状況
クライアント データ	Windowsへのログインをパスワードからバイオメトリクスオンラインサイン照合に置き換える。ユーザはログイン時に予め登録されたサインを入力することでWindowsにログオンできる。サイン認証はローカルPCとサイン認証サーバのどちらかを選択できる。

事業体(研究所)名　ウィッツェル株式会社	
所在地（郵便番号及び住所）　102-0072 東京都千代田区飯田橋4-8-13 タカラビル	
関連部署及び電話番号　営業本部 03-5212-7123	
URL　http://www.witswell.co.jp/	
対象技術	技術開発状況
クライアント データ	ZAURUSのパワーオン時にサイン照合を行うことにより、使用者を確認する。

事業体(研究所)名　ウィッツェル株式会社	
所在地（郵便番号及び住所）　102-0072 東京都千代田区飯田橋4-8-13 タカラビル	
関連部署及び電話番号　営業本部 03-5212-7123	
URL　http://www.witswell.co.jp/	
対象技術	技術開発状況
クライアント データ	Windows Mobile搭載機のパワーオン時にサイン照合を行うことにより、使用者を確認する。

事業体(研究所)名　エントラストジャパン株式会社	
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2-23 アセンド神保町ビル3F	
関連部署及び電話番号　03-5211-8900（代表）	
URL　http://japan.entrust.com/	
対象技術	技術開発状況
サーバ 通信情報	より安価に、より容易な運用で、より高い認証を実現する。乱数表を活用した二要素認証で、ユーザー認証を強化する。機器認証やナレッジベース認証など、多様な認証方式にも対応している。

事業体(研究所)名　エントラストジャパン株式会社	
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2-23 アセンド神保町ビル3F	
関連部署及び電話番号　03-5211-8900（代表）	
URL　http://japan.entrust.com/	
対象技術	技術開発状況
サーバ	webシングルサインオン（SSO）、一元的なアクセスコントロール機能を提供する。 ◎複数ドメインにまたがるシングルサインオン ◎ルールベースの柔軟なアクセス権管理 ◎リアルタイムのセッション管理 ◎アクセス権限の集中管理 ◎Webサービスセキュリティに対応 ◎多様な認証方式に対応

事業体(研究所)名　エントラストジャパン株式会社	
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2-23 アセンド神保町ビル3F	
関連部署及び電話番号　03-5211-8900（代表）	
URL　http://japan.entrust.com/	
対象技術	技術開発状況
サーバ クライアント 通信情報 データ	デジタル証明書を発行するための認証機関（CA）を構築することができる。PKI市場で大きなシェアを誇る製品である。 ・Entrust Authority Security Manager

事業体(研究所)名　エントラストジャパン株式会社	
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2-23 アセンド神保町ビル3F	
関連部署及び電話番号　03-5211-8900（代表）	
URL　http://japan.entrust.com/	
対象技術	技術開発状況
通信情報 データ	JavaアプレットでHTMLフォームに暗号化し、デジタル署名を提供する。 特別なPCクライアントソフトウェアを利用せずに、Webシステムに高度なセキュリティをもたらす。

事業体(研究所)名　エントラストジャパン株式会社	
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2-23 アセンド神保町ビル3F	
関連部署及び電話番号　03-5211-8900（代表）	
URL　http://japan.entrust.com/	
対象技術	技術開発状況
クライアント 通信情報 データ	認証や、Eメールやファイルのデジタル署名・暗号化など高度なWindowsデスクトップセキュリティを提供する。 ・Entrust Entelligence Security Provider ・Entrust Entelligence Messaging Server

事業体(研究所)名　カシオ計算機株式会社	
所在地（郵便番号及び住所）　151-8543 東京都渋谷区本町1-6-2	
関連部署及び電話番号　CSR推進室 03-5334-4901	
URL　http://www.casio.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 施設 その他	TFT技術を用いた高性能指紋認証デバイスを開発･販売している。乾燥して荒れた指や、汗でぬれた指など、これまでのデバイスでは認証困難な指でも認証可能。かつ約4㎜の薄さを実現している。すでに2万台近くの販売実績を有する。2006年には撮像エリアを拡大し、周辺回路も一体化した改良モデルも開発し、サンプル出荷を開始した。

事業体(研究所)名　カシオ計算機株式会社	
所在地（郵便番号及び住所）　151-8543 東京都渋谷区本町1-6-2	
関連部署及び電話番号　CSR推進室 03-5334-4901	
URL　http://www.casio.co.jp/	
対象技術	技術開発状況
サーバ クライアント データ	①指紋認証 VeriPat（弊社独自） ②ICカード（Mifare/Felica/I-CODE）認証 ③MDSR（弊社独自）暗号化

事業体(研究所)名　カシオ計算機株式会社	
所在地（郵便番号及び住所）　151-8543 東京都渋谷区本町1-6-2	
関連部署及び電話番号　CSR推進室 03-5334-4901	
URL　http://www.casio.co.jp/	
対象技術	技術開発状況
データ	MDSR（弊社独自）暗号化を利用。 メモリカードをあらかじめ指定した端末のみでアクセス許可。

事業体(研究所)名　カシオ計算機株式会社	
所在地（郵便番号及び住所）　151-8543 東京都渋谷区本町1-6-2	
関連部署及び電話番号　CSR推進室 03-5334-4901	
URL　http://www.casio.co.jp/	
対象技術	技術開発状況
その他	コピー牽制地紋印刷。

事業体(研究所)名　クオリティ株式会社	
所在地（郵便番号及び住所）	
関連部署及び電話番号	
URL	
対象技術	技術開発状況
サーバ クライアント	クライアントPCにインストールされたCLTモジュールがPC上で行われた操作を記録し、サーバに送信、データベースに保存する。 クライアントPC上で行われた ・プロセス起動 ・ファイルアクセス ・印刷 ・メール送信 など記録することが可能。

事業体(研究所)名　クオリティ株式会社	
所在地（郵便番号及び住所）	
関連部署及び電話番号	
URL	
対象技術	技術開発状況
ネットワーク クライアント	TopLayer Net works社が販売しているSecure Controllerを機能を利用して不正PCのネットワーク接続を抑止するソリューション。 管理者があらかじめ設定したポリシ（適用パッチのバージョン、禁止ソフトの存在など）に抵触するPCは検疫セグメントに接続される。

事業体(研究所)名　クオリティ株式会社	
所在地（郵便番号及び住所）	
関連部署及び電話番号	
URL	
対象技術	技術開発状況
クライアント その他	クライアントPC上で動作するプロセスを常時監視。 起動抑止対象のプロセスの実行をクライアント上で禁止する設定は管理者側から行うことが可能。 一度設定されたクライアントは、オフライン状態であっても起動制御が行われる。 クライアントにインストールされているソフトウェア情報を収集することが可能であるため、使用禁止ソフトの存在やパッチ摘用状況などを把握することも可能である。

事業体(研究所)名　クオリティ株式会社	
所在地（郵便番号及び住所）	
関連部署及び電話番号	
URL	
対象技術	技術開発状況
データ	クライアントPCに接続されたリムーバブルメディアへのデータ書き込みを抑止する。 制御はデバイスドライバレベルで行われているため、OSを介した全てのデータ書き込みを抑止できる。

事業体(研究所)名　クオリティ株式会社	
所在地（郵便番号及び住所）	
関連部署及び電話番号	
URL	
対象技術	技術開発状況
データ	PDFファイルを暗号化し、復号鍵をサーバ上で管理するシステム。 DKS Plusによって暗号化された文書を閲覧するためにはクライアント側のAdobe Readerに専用のPluginのインストールが必要となり、閲覧できる機器が限定される。 また、復号鍵をダウンロードするためにはDKSサーバへのログインが必要であり、DKSサーバ上に登録されたアカウント情報を知らない限り鍵を入手することはできない。 万一、アカウントが不正に流出するようなことがあってもDKSサーバ上でアカウントを抹消するだけで文書の閲覧が不能となる。退職等によって閲覧権限を失った場合でも、文書側には手を加える必要はなく、サーバ側の設定を行うだけで良い。

事業体(研究所)名　クオリティ株式会社	
所在地（郵便番号及び住所）	
関連部署及び電話番号	
URL	
対象技術	技術開発状況
データ	クライアントPC上に存在するファイルを検索し、個人情報が含まれていると思われるものをリストする。クライアントPCユーザはリストされた各ファイルについて内容、個人情報有無、用途などについて管理者に報告する。

事業体(研究所)名　クオリティ株式会社	
所在地（郵便番号及び住所）	
関連部署及び電話番号	
URL	
対象技術	技術開発状況
その他	管理者はクライアントPCにインストールするソフトウェアをあらかじめ暗号化しておく。 クライアント側でアプリケーションが起動された時、クライアントにインストールされているKey Serverクライアントモジュールがサーバと認証を結び、復号化鍵をダウンロードし、アプリケーションを複合化し、実行可能とする。 また、サーバモジュールは鍵のダウンロードを記憶しているため、購入ライセンス以上のアプリケーションの起動を抑止することが可能となる。

事業体(研究所)名　クボタシステム開発株式会社	
所在地（郵便番号及び住所）　556-8601 大阪府大阪市浪速区敷津東1-2-47	
関連部署及び電話番号　総務部 06-6648-3111	
URL　http://www.ksi.co.jp/	
対象技術	技術開発状況
サーバ 通信情報	WebSignOnは、リバースプロキシ型シングルサインオンのApacheモジュールである。 主な機能は以下の3つ。 ･シングルサインオン ･URLベースでのアクセス制御 ･セッション管理 特徴としては、 ･Webアプリケーションのシングルサインオンを実現 ･Webアプリケーション上の認証、アクセス制御を一元管理 ･WebアプリケーションサーバをDMZ内に配置することでセキュリティを強化 ･個々に独立していたWebアプリケーションのユーザ情報を統一 が可能になる。

事業体(研究所)名　サイエンスパーク株式会社	
所在地（郵便番号及び住所）　228-0024 神奈川県座間市入谷1-1538-11	
関連部署及び電話番号　新規事業推進本部 046-255-2544	
URL　http://www.sciencepark.co.jp/	
対象技術	技術開発状況
クライアント データ	内部犯行を想定した情報漏えいを強固に防止するドライバベースの情報漏えい防止、監視システム。 近年、USBメモリの利用が簡単にできるようになり、不正にファイルデータを持ち出す問題が大きくなっている。本システムの導入により、USBメモリ、外付のハードディスク、CD-Rなどを含むリバーブルメディアへのファイル持ち出しを防止する。 運用上、ファイル持ち出しが必要な場合は、申請･許可のワークフローを内蔵し、許可されたデータのみが持ち出し可能となる。この制御はDriverwaveというカーネルレベルのプログラムにより行われているために強固なセキュリティを保つ。 また、内部監査に必要なファイルアクセスログ、印刷ログなどを記録し、管理者が閲覧可能となっている。

事業体(研究所)名　株式会社シー･エス･イー	
所在地（郵便番号及び住所）　150-0044 東京都渋谷区円山町23-2 アレトゥーサ渋谷ビル	
関連部署及び電話番号　プロダクツ販売部 03-3463-5633	
URL　http://www.cseltd.co.jp/	
対象技術	技術開発状況
その他	「マトリクス認証」（イメージとワンタイムパスワードのコラボレーションによる新しい認証技術）により、簡単かつ安全な本人認証を実現する。WEBブラウザを使用するため、 ①端末の種類や社内外を問わずに利用できる ②ユーザへの機器やソフトの配布が不要 という特徴がある。 また、Windowsのドメインログオンにも「マトリクス認証」が使用可能となっている。

事業体(研究所)名　株式会社シーフォーテクノロジー	
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5F	
関連部署及び電話番号　経営企画室 03-5447-2551	
URL　http://c4t.jp/	
対象技術	技術開発状況
データ	Windows対応の情報漏洩対策ソフトウェアである。導入や利用が簡易なため、今すぐに情報セキュリティ対策を実施しようと希望するユーザに最適である。 「CRYPTY」シリーズに搭載している自社開発の暗号「C4Custom」は「スピード」と「安全性」のセキュリティバランスに優れている。USBメモリタイプの「CRYPTY U」や秘密分散技術を搭載した「CRYPTY S」などラインナップの充実を図っている。

事業体(研究所)名　株式会社シーフォーテクノロジー	
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5F	
関連部署及び電話番号　経営企画室 03-5447-2551	
URL　http://c4t.jp/	
対象技術	技術開発状況
データ	「C4CS」は米国商務省管轄の国立標準技術研究所（NIST)が暗号モジュールのセキュリティ要件を規定した「FIPS140-2」の適合認定を受けた暗号ライブラリである。 第三者評価を受けているため、アルゴリズム実装の安全性が証明されている。 自社開発の暗号「C4Custom」のほか、電子政府推奨暗号を多数搭載している。

事業体(研究所)名　株式会社シーフォーテクノロジー	
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5F	
関連部署及び電話番号　経営企画室 03-5447-2551	
URL　http://c4t.jp/	
対象技術	技術開発状況
その他	情報セキュリティ・マネジメント・システム（ISMS）構築や、米国商務省管轄の国立標準研究所（NIST）が規定した暗号モジュールのセキュリティ要件「FIPS140-2」の適合認証取得などの支援サービスを行っている。 当社のコンサルティングサービスの特徴は、ISMS構築や「FIPS140-2」適合認定取得を実際に当社が行った経験に基づいているため、ユーザにとってより実際的な支援を行えることにある。

事業体(研究所)名　株式会社システックス	
所在地（郵便番号及び住所）　380-0936 長野県長野市岡田町78-11	
関連部署及び電話番号　026-226-7277	
URL　http://www.systex.co.jp/	
対象技術	技術開発状況
その他	webで指紋の登録、認証を可能とした。これによりwebシステムのログインや利用権限のコントロールを可能とする。

事業体(研究所)名　シャープ株式会社	
所在地（郵便番号及び住所）	
関連部署及び電話番号	
URL	
対象技術	技術開発状況
データ	1)ホームサーバに蓄積したコンテンツをパソコンを用いて外出先からも視聴可能。 2)ホームサーバのコンテンツの個人的な視聴の範囲にとどめるために、家庭内のサーバで登録されたPCのみ外出先から視聴可能とするアクセス制限技術を開発。 3)外出先から同時にアクセス可能なPCは1台のみで強固な暗号化を施しているので盗聴や情報漏えいの心配はない。

事業体(研究所)名　株式会社セキュアブレイン	
所在地（郵便番号及び住所）　102-0083 東京都千代田区麹町2丁目6番地7号 麹町RKビル4階	
関連部署及び電話番号　03-3234-3001	
URL　http://www.securebrain.co.jp/	
対象技術	技術開発状況
クライアント 通信情報	PhishWall：フィッシング詐欺の防御製品。真正サイト確認、認証機能。Webアクセス時にPhishWallが正しいWebサイトを自動的に確認し、ブラウザのツールバーに青信号灯火。

事業体(研究所)名　株式会社セキュアブレイン	
所在地（郵便番号及び住所）　102-0083 東京都千代田区麹町2丁目6番地7号 麹町RKビル4階	
関連部署及び電話番号　03-3234-3001	
URL　http://www.securebrain.co.jp/	
対象技術	技術開発状況
クライアント 通信情報	Internet SagiWall：不正な詐欺サイトからインターネットユーザを保護する製品。フィッシング詐欺、ワンクリック詐欺の自動判定機能サイトブロック、国名表示。

事業体(研究所)名　株式会社セキュアブレイン	
所在地（郵便番号及び住所）　102-0083 東京都千代田区麹町2丁目6番地7号 麹町RKビル4階	
関連部署及び電話番号　03-3234-3001	
URL　http://www.securebrain.co.jp/	
対象技術	技術開発状況
クライアント データ	ZHR（Zero Hour Response）：ウィルス、ワーム、Bot、スパイウェアなどを分析システムにより自動解析し、ワクチンを生成する。

事業体(研究所)名　株式会社セキュアブレイン	
所在地（郵便番号及び住所）　102-0083 東京都千代田区麹町2丁目6番地7号 麹町RKビル4階	
関連部署及び電話番号　03-3234-3001	
URL　http://www.securebrain.co.jp/	
対象技術	技術開発状況
その他	偽装サイト自動検知サービス：金融機関のWebサイトのフィッシングサイトをインターネットから自動的に発見するサービス。

事業体(研究所)名　株式会社ソフテック	
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5F	
関連部署及び電話番号　セキュリティ・ソリューション事業部 03-3412-6008	
URL　http://www.softek.co.jp/	
対象技術	技術開発状況
サーバ データ	WebProbeは、Webアプリケーションにおけるログイン（ユーザ認証）機能を伴う「セッション管理の脆弱性（欠陥）」を簡単な操作で検査するツールである。 「特長」・・・ ①世界初の「セッション管理」脆弱性検査ツール ②技術的な検査スキルのノウハウを製品化 ③GUI、操作ガイドに従った検査（ノウハウの手続化） ④リーズナブルな価格設定。 「概要」・・・ ①スキャン系ツールでは検出できない「セッション管理系の欠陥」を世界で唯一ツールで検出可能 ②従来手作業で行わざるを得なかった「セッション追跡パラメータ」（セッションID）の推定を自動化 ③推定した「セッション追跡パラメータ」を基に、20項目を越える脆弱性を検出し、詳細な解説とともに問題点をリストアップ ④改善の余地がある不適切な設計に関する問題点も指摘

事業体(研究所)名　株式会社ソフトクリエイト	
所在地（郵便番号及び住所）　150-0002 東京都渋谷区渋谷2-22-3 渋谷東口ビル	
関連部署及び電話番号　ネットワークソリューション部 03-3486-1526	
URL　http://www.softcreate.co.jp/	
対象技術	技術開発状況
ネットワーク	社内ネットワークへの持ち込みPCの不正接続を防止するシステム。 接続を許可していないPC＝「不正PC」がネットワークに接続しようとした時に、そのPCを検知し排除する。システムの構成として1セグメントにつき1台のセンサー（小型アプライアンス）とセンサーを管理するマネージャー（サーバ機）。 [L2Blockerのブロックの仕組み] ネットワークへの接続を許可していないPCからARPRequestを受けた場合、偽装されたARPReplyを送信し、接続をブロックする。 [特徴] ①既存ネットワークにL2BlockerセンサーをHUBに差し込むだけで設置が可能。（ネットワークやPCの設定変更なし） ②L2Bマネージャーによる集中管理 不正PC検知時等、イベントのメール通知機能及びSyslogサーバへの送信機能。 ③エンタープライズユーザ対応 センサーをグループ管理し、グループ毎の接続管理を行う機能。複数人の管理者ユーザを設定。権限をセンサー別に設定する機能。

事業体(研究所)名　大日本印刷株式会社　IPS事業部　ICカードビジネス開発本部	
所在地（郵便番号及び住所）　162-8472 東京都新宿区榎町7番地	
関連部署及び電話番号　IPS事業部　ICカードビジネス開発本部 03-3513-2720	
URL　http://www.dnp.co.jp/bf/ic_card/index.html	
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	ICカード内に格納された電子証明書や秘密鍵とブラウザ等の上位アプリケーションソフトとのI/F機能を提供するドライバソフトウェア。 CSPとPKCS#11規格に対応している。

事業体(研究所)名　大日本印刷株式会社　IPS事業部　ICカードビジネス開発本部	
所在地（郵便番号及び住所）　162-8472 東京都新宿区榎町7番地	
関連部署及び電話番号　IPS事業部　ICカードビジネス開発本部 03-3513-2720	
URL　http://www.dnp.co.jp/bf/ic_card/index.html	
対象技術	技術開発状況
クライアント	耐タンパ性の高いICカードにワンタイムパスワード生成アプリケーションを搭載し、ICカード内部でワンタイムパスワード生成を完結している為、セキュリティに優れている。 利用者は、専用のビューアにICカードを挿入して、ビューアに表示されたワンタイムパスワードを読み取り、ネットワークの本人認証時に使用する。

事業体(研究所)名　大日本印刷株式会社　IPS事業部　ICカードビジネス開発本部	
所在地（郵便番号及び住所）　162-8472 東京都新宿区榎町7番地	
関連部署及び電話番号　IPS事業部　ICカードビジネス開発本部 03-3513-2720	
URL　http://www.dnp.co.jp/bf/ic_card/index.html	
対象技術	技術開発状況
クライアント 通信情報 データ	TranC'ertはICカードを利用したデスクトップセキュリティソリューションである。 ①PCの不正利用、情報漏洩をシャットアウトする。 ②ICカード所有と暗証番号（PIN）入力の2要素認証により、セキュリティの高い認証が可能である。 ③情報システム利用者の権限管理と認証情報を管理サーバーで集中管理する。 ④ユーザーに特別なスキルは必要ない。 ⑤ICカード内の電子証明書の利用が可能となる。

事業体(研究所)名　デジタルアーツ株式会社	
所在地（郵便番号及び住所）　100-0014 東京都千代田区永田町2-13-10 プルデンシャルタワー15階	
関連部署及び電話番号　経営企画本部 03-3580-3030	
URL　http://www.daj.co.jp/index.htm	
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	概要）主として、下記の機能を提供。 ①WEB（インターネット）へのアクセスを制限するフィルタリング機能（カテゴリ分類を含む） ②WEBメールの送信制限機能 ③掲示板への書き込み制限機能 ④アクセスログの蓄積、検索機能（レポート機能）　など。 特徴）　WEBのアクセス制御については、 ①有害サイトや犯罪等に関るURLデータベース（平成18年10月時点で約1億8000万ページ）によるアクセス制御 ②独自技術（特許取得）のコンテンツフィルタリング機能に基づくリアルタイムアクセス制御、の併用を特徴とする。

事業体(研究所)名　東芝ソリューション株式会社	
所在地（郵便番号及び住所）	
関連部署及び電話番号	
URL	
対象技術	技術開発状況
サーバ	不正侵入防御ソフトウェア「AntiHacker-Pro（アンチハッカープロ）」 AntiHacker-Proは、インターネットビジネスと安全・確実に立ち上げるために、様々な攻撃からWebサーバを守る不正侵入防御ソフトウェアである。ファイアウォールでは防げない攻撃に対応。外部からの不正アクセスを即座に検出・遮断し、Webサーバの安全を高める。 ・ インライン設置型アーキテクチャにより検出した不正アクセスを確実に遮断する。 ・ 脆弱性（セキュリティホール）の情報に基づき不正侵入検知を行いますので、急速に感染を広めるワームなどの侵入も阻止する。 ・ HTTPなどのプロトコルデコードやプロトコル異常検知などを併用した検知メカニズムを採用し、精度の高い不正侵入防止システムを実現。 ・ 特許出願中のDDoS防御機能も搭載。SYN FloodなどのDoS/DDoS攻撃からもWebサーバを防御する。 ・ 業界初のL7パラメトリック分析方式による未知攻撃検知・防御機能を搭載している。 ・ パケットフィルタ機能も備えている。 ・ 本製品はOSを含んでいるため、OSを用意する必要はない。

事業体(研究所)名　東芝ソリューション株式会社	
所在地（郵便番号及び住所）	
関連部署及び電話番号	
URL	
対象技術	技術開発状況
サーバ データ	PKI/ICカードシステム「TARGUSYS」 　電子証明書を使ったPKI認証に対応したICカードシステム。クライアントPCにインストールしICカードを利用可能にする「TARGUSYSクライアント」と、TARGUSYS対応ICカードを発行する「TARGUSYS統合管理サーバ」から成る。 ①「TARGUSYSクライアント」 1.TARGUSYS対応ICカードのための暗号ミドルウェア 2.MicrosoftCryptAPI、PKCS#11の各インターフェイスに対応 3.電子証明書と秘密鍵を各5組使用可能（株式会社東芝製TARGUSYS標準ICカードを使用時） 4.指紋照合オプション 5.対応OS：Windows98SE、XP、2000/2003 ②「TARGUSYS統合管理サーバ」 1.電子証明書及びICカードのライフサイクル管理システム 2.RSA鍵生成、各種認証局システムと連携した電子証明書一括生成 3.認証局システムとして、VeriSign　MPKI、RSA　CMS、MS Windows2000/2003電子認証サービスに対応 4.電子署名法に基づく特定認証業務に対応可能 5.対応OS：Windows2000/2003Server

事業体(研究所)名　東芝ソリューション株式会社	
所在地（郵便番号及び住所）	
関連部署及び電話番号	
URL	
対象技術	技術開発状況
施設	1.動画像（複数枚の連続画像）による登録、認証方式を採用。静止画認証方式と比べて顔情報データが格段に多いため、顔の向き、表情に影響されにくく、より正確な認証が可能である。 2.入力された顔画像から個人を際立たせる“その人らしさ”を抽出する。この抽出された特徴を中心に比較を行うため、他人との識別能力に優れ、より正確な認証が可能である。 3.照合実施時毎に顔情報を更新する学習機能を搭載しており、顔の輪郭や頬髭、髪型など、経時変化と呼ばれる時間の経過に伴う微妙な変化にも対応している。 4.顔認証では、運用する場所の照度（明るさ）が課題ですが、FacePassでは、画像入力方法を改善し、照明環境の影響を受けにくくしている。 5.照合時のカラー顔画像を、通行履歴として記録する。通行者の名前や通行時刻などと併せて確認できるので、不正が行われた場合の追跡も容易である。また、カメラの存在自体が、不正に対する心理的抑止効果を発揮する。 6.登録した顔情報、記録される顔画像履歴など、個人を特定できる顔画像には、特殊な暗号化処理を施すことで、情報を保護している。 7.照合に要する時間は約1秒。煩わしさを感じない、快適な通行が可能である。 8.認証は、1対1照合、1対N照合を選択可能です。1対N照合では、装置の前に立つだけで照合処理が行われる。衛生的で抵抗感の少ない、自然な認証が可能である。 9.様々なタイプの電気錠や自動ドアに対応している。また設置は、既設建物、新築建物を問わない。 10.本体の簡単な操作で利用者の登録や削除が行える。また、1台の登録照合機で登録した顔情報を、最大8台までの照合機へ配信し、登録照合機を含めて最大9箇所での認証が行えるネットワーク構築が可能である。複数フロアにまたがる運用も容易である。

事業体(研究所)名　株式会社トリニティーセキュリティーシステムズ	
所在地（郵便番号及び住所）　101-0031 東京都千代田区東神田1-7-8 アルテビル東神田8階	
関連部署及び電話番号　戦略企画本部 03-5835-2323	
URL　http://www.trinity-ss.com/	
対象技術	技術開発状況
サーバ 通信情報 データ	サーバサイドスクリプトなどで動的に生成されるHTMLを含め、ブラウザに表示されている情報や画像の不正利用を防ぐソリューション。ブラウザで表示されている画像などのコピー・保存・印刷などを禁止し、悪意あるユーザからの不正利用を防止する。 現在稼働中のシステムに手を加えることなく導入でき、簡単な運用管理で情報を強力に保護する。

事業体(研究所)名　株式会社トリニティーセキュリティーシステムズ	
所在地（郵便番号及び住所）　101-0031 東京都千代田区東神田1-7-8 アルテビル東神田8階	
関連部署及び電話番号　戦略企画本部 03-5835-2323	
URL　http://www.trinity-ss.com/	
対象技術	技術開発状況
クライアント データ	セキュリティ製品を「便利」「快適」に、月額利用料金だけでユーザサポートまで利用できるセキュリティサービスを提供。 ファイルの編集や印刷など、ユーザ毎の利用権限をサーバで一元管理。権限のコントロールを柔軟に行えるため、社内外の情報流通はスムーズなまま、重要な情報を強力に保護する。

事業体(研究所)名　株式会社トリニティーセキュリティーシステムズ	
所在地（郵便番号及び住所）　101-0031 東京都千代田区東神田1-7-8 アルテビル東神田8階	
関連部署及び電話番号　戦略企画本部 03-5835-2323	
URL　http://www.trinity-ss.com/	
対象技術	技術開発状況
通信情報	IPN技術を搭載したVPNルータ。 拠点間の確実な相互認証と暗号化通信を同時に実現。WANを介する環境でもセキュアなネットワークを構築することが出来る。 IPN技術とは、IPN（の概念）を実現する、ワンタイムパスワード認証方式「SAS-2」と暗号化方式「AES」を組み合わせたトリニティーセキュリティーシステムズ（以下、T-SS）独自の技術。 IPN（Identified Private Network）とは、T-SSが提唱する新たなネットワークセキュリティの概念。情報を交換する2者間で（第3者を介さず）確実に相互認証することにより、信頼のおけるセキュリティゾーンを形成し、その中で安心して情報のやり取りができる世界を構築する仕組み。 SAS-2（Simple And Secure password authentication protocol,ver.2）とは、高知工科大学　清水明宏教授考案のワンタイムパスワード認証方式、動的暗号鍵生成アルゴリズム。

事業体(研究所)名　株式会社トリニティーセキュリティーシステムズ	
所在地（郵便番号及び住所）　101-0031 東京都千代田区東神田1-7-8 アルテビル東神田8階	
関連部署及び電話番号　戦略企画本部 03-5835-2323	
URL　http://www.trinity-ss.com/	
対象技術	技術開発状況
通信情報	IPN技術を搭載した無線LANアクセスポイント/無線LANカード。 無線LAN構築時に課題となっていた、脆弱性と運用の煩雑さを解決。無線LANアクセスポイントと無線LANカードとの組み合わせで相互認証を実現し、認証サーバ等の設置/運用が不要。 IPN技術とは、IPN（の概念）を実現する、ワンタイムパスワード認証方式「SAS-2」と暗号化方式「AES」を組み合わせたトリニティーセキュリティーシステムズ（以下、T-SS）独自の技術。 IPN（Identified Private Network）とは、T-SSが提唱する新たなネットワークセキュリティの概念。情報を交換する2者間で（第3者を介さず）確実に相互認証することにより、信頼のおけるセキュリティゾーンを形成し、その中で安心して情報のやり取りができる世界を構築する仕組み。 SAS-2（Simple And Secure password authentication protocol,ver.2）とは、高知工科大学　清水明宏教授考案のワンタイムパスワード認証方式、動的暗号鍵生成アルゴリズム。

事業体(研究所)名　株式会社トリニティーセキュリティーシステムズ	
所在地（郵便番号及び住所）　101-0031 東京都千代田区東神田1-7-8 アルテビル東神田8階	
関連部署及び電話番号　戦略企画本部 03-5835-2323	
URL　http://www.trinity-ss.com/	
対象技術	技術開発状況
通信情報 データ	自然に使えて「情報」を強力に守る、をコンセプトに開発された情報保護&セキュリティソリューション。ファイルの編集や印刷などユーザ毎の利用権限をサーバで一元管理。権限のコントロールを柔軟に行えるため、社内外の情報流通はスムーズなまま、重要な情報を強力に保護する。

事業体(研究所)名　株式会社トリニティーセキュリティーシステムズ	
所在地（郵便番号及び住所）　101-0031 東京都千代田区東神田1-7-8 アルテビル東神田8階	
関連部署及び電話番号　戦略企画本部 03-5835-2323	
URL　http://www.trinity-ss.com/	
対象技術	技術開発状況
データ	WMVなどの動画ファイルを暗号化し、正規ユーザのPC以外での利用を禁止し、著作権を管理するソリューション。ダウンロードしたPCでのみ利用可能にしたり、閲覧期間などを設定し、ファイル交換などによる不正なコンテンツ利用を防止し、著作権を管理する。

事業体(研究所)名　株式会社トリニティーセキュリティーシステムズ	
所在地（郵便番号及び住所）　101-0031 東京都千代田区東神田1-7-8 アルテビル東神田8階	
関連部署及び電話番号　戦略企画本部 03-5835-2323	
URL　http://www.trinity-ss.com/	
対象技術	技術開発状況
データ	EXEファイルを暗号化し、正規ユーザのPC以外での利用を禁止し、著作権を管理するソリューション。ダウンロードしたPCでのみ利用可能にしたり、閲覧期間などを設定し、ファイル交換などによる不正なコンテンツ利用を防止し、著作権を管理する。DLLなどのプログラムファイルにも対応。

事業体(研究所)名　株式会社トリニティーセキュリティーシステムズ	
所在地（郵便番号及び住所）　101-0031 東京都千代田区東神田1-7-8 アルテビル東神田8階	
関連部署及び電話番号　戦略企画本部 03-5835-2323	
URL　http://www.trinity-ss.com/	
対象技術	技術開発状況
データ	Adobe ReaderやInternet Explorerで表示可能なコンテンツを暗号化し、正規にダウンロードしたPC以外での利用を禁止するソリューション。ダウンロードしたPCでのみ利用可能にしたり、閲覧期間などを設定し、ファイル交換などによる不正なコンテンツ利用を防止し、著作権を管理する。Internet Explorer内で表示されているFLASHや動画ファイルにも対応。

事業体(研究所)名　株式会社トリニティーセキュリティーシステムズ	
所在地（郵便番号及び住所）　101-0031 東京都千代田区東神田1-7-8 アルテビル東神田8階	
関連部署及び電話番号　戦略企画本部 03-5835-2323	
URL　http://www.trinity-ss.com/	
対象技術	技術開発状況
データ	HTMLに埋め込まれた静的コンテンツを暗号化して、不正利用から守るコンテンツ保護ソリューション。ブラウザで表示されている画像などのコピー保存･印刷などを禁止し、悪意あるユーザからの不正利用を防止する。

事業体(研究所)名　株式会社バーテックスリンク	
所在地（郵便番号及び住所）　101-0054 東京都千代田区神田錦町3-15 名鉄不動産竹橋ビル	
関連部署及び電話番号　ソリューション本部 03-5259-5126	
URL　http://www.vertexlink.co.jp/	
対象技術	技術開発状況
データ	世界で最初に商用化されたURLフィルタリングソフト。 大企業、官公庁、学校など多くのユーザで利用されている。

事業体(研究所)名　株式会社バーテックスリンク	
所在地（郵便番号及び住所）　101-0054 東京都千代田区神田錦町3-15 名鉄不動産竹橋ビル	
関連部署及び電話番号　ソリューション本部 03-5259-5126	
URL　http://www.vertexlink.co.jp/	
対象技術	技術開発状況
データ	URLフィルタリング、アンチウィルス、Emailフィルタリングなど、複数のゲートウェイセキュリティを一元管理できる。 SSLスキャナはHTTPSトラフィックのフィルタリングが可能。

事業体(研究所)名　ハミングヘッズ株式会社	
所在地（郵便番号及び住所）　104-0052 東京都中央区月島1-2-13 ワイズビルディング2F	
関連部署及び電話番号　管理部 03-3531-7281	
URL　http://www.hummingheads.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 データ	会社内の各クライアントPCのデータ操作について監視を行い、その結果について履歴を残す。また、アクセス権により、持ち出し行為を禁止する。 平成15年より開発したEvolution/SVの商品により、FDやUSB、メール添付したデータについて自動的に暗号化することにより、外部への情報漏洩を防止する。

事業体(研究所)名　株式会社ハンモック	
所在地（郵便番号及び住所）　169-0075 東京都新宿区高田馬場1-30-4 30山京ビル	
関連部署及び電話番号　NWS事業部　企画課 03-5287-5661	
URL　http://www.hammock.jp/	
対象技術	技術開発状況
クライアント データ	AssetView HYPERは、導入、運用が簡単で低コストのクライアントPC管理ツールである。 ニーズに合わせて多彩な機能から選択できる高い柔軟性が特徴になる。 主な機能：PC 資産管理／リモートコンソール／セキュリティパッチ・ソフトウェア配布／稼動監視、操作履歴管理／デバイス使用制限／WEBアクセス制限／不正PC検知・遮断

事業体(研究所)名　株式会社ハンモック	
所在地（郵便番号及び住所）　169-0075 東京都新宿区高田馬場1-30-4 30山京ビル	
関連部署及び電話番号　NWS事業部　企画課 03-5287-5661	
URL　http://www.hammock.jp/	
対象技術	技術開発状況
クライアント データ	AssetView GOLDは2005年度トップシェアを獲得したAssetView HYPERのノウハウを踏襲し、内部統制時代にマッチした次世代クライアントPC統合管理ツールである。 特徴としてはExcectiveView（経営責任者向け統合レポート）を搭載し、情報システム部門、経営責任者の観点から、社内のクライアントPC統制をPDCAサイクルで運用、実現出来る仕組みや、独自プロトコルの採用によりネットワークの負荷を軽減した点が挙げられる。 また、新しく監査機能を実装した事により、個人情報・機密情報が、社内のどこにいくつあるのかといった分析が行える様になった。 各機能でのPDCAサイクルでの運用実現以外にも、ニーズに合わせてひとつの機能からでも導入可能な柔軟性も兼ね備えている。 日本版SOX法（金融商品取引法）のIT統制に対応すべく、SOX法準備ツールとしての製品の位置づけとなる。

事業体(研究所)名　株式会社日立製作所システム開発研究所	
所在地（郵便番号及び住所）　215-0013 神奈川県川崎市麻生区王禅寺1099	
関連部署及び電話番号　企画室 044-959-0321	
URL　http://www.sdl.hitachi.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 データ 施設	「Secureplaza」は、世の中のニーズに沿ったセキュリティシステムを実現するため、 ①ステップ別ソリューション ②目的別ソリューション の2つのアプローチによるソリューションを提供する。それぞれの段階、目的に応じた製品群や専門の知識、組織をパッケージ化したものを提供する。

事業体(研究所)名　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	
関連部署及び電話番号　03-5780-2111（代）	
URL　http://hitachisoft.jp/	
対象技術	技術開発状況
サーバ 通信情報	共有ファイルサーバ上のデータを暗号化、フォルダ単位でのアクセス制御でデータの漏洩や改ざんを防ぐ。 ①共有フォルダの暗号化：管理者によるサーバー上からの情報漏洩防止・不正接続PCからの情報漏洩防止 ②アクセス制御：暗号フォルダへの不正アクセスの禁止 ③View機能：暗号フォルダ内のファイルのコピー・印刷・保存等の禁止 ④ログ取得：暗号フォルダへのアクセスログの取得

事業体(研究所)名　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	
関連部署及び電話番号　03-5780-2111（代）	
URL　http://hitachisoft.jp/	
対象技術	技術開発状況
サーバ クライアント	指静脈認証システム「静紋」は、指内部の静脈パターンを人体に安全な近赤外線で撮影・画像処理して認証するバイオメトリクス装置。コンパクトさと使いやすさを追求しながら、優れた認証精度を兼ね備えている。 ①高セキュリティ・・外部からは見えない指内部の静脈の特徴を利用するため、偽造・盗難によるなりすましが極めて困難である。 ②高精度・・指内部の静脈の特徴を画像処理して認証するため、指の表皮の傷や汚れの影響を受けにくく、優れた認証精度を実現する。 Windowsログオンやユーザアプリケーションと連携した認証の強化。

事業体(研究所)名　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 東京都千代田区神田須田町2-2-2	
関連部署及び電話番号　システム部 03-5209-1413	
URL　http://www.falconsc.com/	
対象技術	技術開発状況
サーバ 通信情報 データ	覚えやすく忘れにくい独自の認証方式を採用し、Webベースのシステムに対するアクセス制御、シングルサインオンを実現する。また、リバースプロキシとしても利用できるため、サービス用のサーバをDMZに配置しなくても利用できる

事業体(研究所)名　富士ゼロックス株式会社	
所在地（郵便番号及び住所）　107-0052 東京都港区赤坂二丁目17番22号	
関連部署及び電話番号　03-3585-3211	
URL　http://www.fujixerox.co.jp/	
対象技術	技術開発状況
データ	コピーすると浮き出す「隠し文字」を文書と同時にプリントし、文書のセキュリティを確保する。

事業体(研究所)名　富士ゼロックス株式会社	
所在地（郵便番号及び住所）　107-0052 東京都港区赤坂二丁目17番22号	
関連部署及び電話番号　03-3585-3211	
URL　http://www.fujixerox.co.jp/	
対象技術	技術開発状況
データ	文書出力時にICカード認証を行うことでセキュリティを強化し、紙文書による情報漏洩リスクを低減するシステムである。

事業体(研究所)名　富士ゼロックス株式会社	
所在地（郵便番号及び住所）　107-0052 東京都港区赤坂二丁目17番22号	
関連部署及び電話番号　03-3585-3211	
URL　http://www.fujixerox.co.jp/	
データ	ICカードによる個人認証機能により、コピーやプリント時の出力制限が可能となり、ドキュメント情報の漏洩防止と共に複合機やプリンターからオンデマンド出力ができる。

事業体(研究所)名　富士通株式会社	
所在地（郵便番号及び住所）　105-7123 東京都港区東新橋1-5-2 汐留シティセンター	
関連部署及び電話番号　サービスビジネス本部安心安全ビジネス推進室 03-6424-6249	
URL　富士通ポータル：http://jp.fujitsu.com/ 富士通セキュリティポータル：http://segroup.fujitsu.com/secure/	
ネットワーク	Systemwalker Desktop Inspectionは、パソコンが業務サーバに接続する前にセキュリティに関する検査を行い、不合格の場合はネットワーク機器と連携して検疫（業務サーバからの隔離）を行う機能を提供する製品である。セキュリティポリシーを満たしていないパソコンが原因のセキュリティ被害を防ぐことが可能である。 ①パソコンに特別なソフトウェアをインストールしない運用も可能である。 ②パソコンの検査時間は10秒程度で、利用者に負担をかけない。 ③認証スイッチ連携による検疫と認証ゲートウェイ装置連携による検疫の両方の方式に対応しており、ネットワーク環境に応じて使い分けが可能である。 ④さらに高いレベルのセキュリティが必要な環境においては、ネットワークバイオ認証による認証、検疫システムにより、強力な不正アクセス対策および情報漏洩対策を実現可能である。

事業体(研究所)名　富士通株式会社	
所在地（郵便番号及び住所）　105-7123 東京都港区東新橋1-5-2 汐留シティセンター	
関連部署及び電話番号　サービスビジネス本部安心安全ビジネス推進室 03-6424-6249	
URL　富士通ポータル：http://jp.fujitsu.com/ 富士通セキュリティポータル：http://segroup.fujitsu.com/secure/	
対象技術	技術開発状況
サーバ	Systemwalker Centric Manager（システムウォーカー セントリックマネージャー）は、システム運用のライフサイクル（導入／設定～監視～復旧～評価）に従い、ソフトウェア資源の配付、システムやネットワークの集中監視、リモートからのトラブル復旧などの優れた機能で運用管理作業の軽減と、信頼性の高いシステムの構築を実現する統合運用管理製品である。 ①システム運用のライフサイクルに従い、トータルに運用管理を支援。 優れた運用管理機能で管理者の作業負荷を軽減する。 1)システムやネットワーク異常のリアルタイム監視、異常の予兆検知によるトラブルの事前回避、トラブルの迅速な復旧と自動対処を実現する。 2)分散するサーバやクライアントのソフトウェア／ハードウェア資源を一括管理し、ソフトウェアの導入／保守作業工数を削減する。シームレスな運用管理操作で管理者の作業を支援する。 3)システム運用に関する一連の管理操作は集中管理画面からスムーズに行える。 4)マルチプラットフォーム環境も、ビジュアルな管理画面から統一された操作で集中管理できる。 ②インターネットビジネス化を実現するさまざまな業務の安定稼動を支援。実績のある運用管理機能で、最新のビジネス環境を統合管理する。 1)イントラネットからインターネットにまで広がるIT資産を、安全なセキュリティポリシーで統合管理する。 2)クラスタシステムや公開ゾーンの管理、ブロードバンドにも対応し、24時間365日稼動のインターネットビジネス実現を支援する。 3)部門内システムから超大規模システムまで、様々なシステム環境を集中監視することで、運用コスト削減と安定稼動を実現する。 ③システム運用のセキュリティ強化を支援。 1)操作者毎に使用できる運用管理者機能をきめ細かく設定でき、役割に応じた操作制御を行える。 2)システム上に散在するログを収集・一元管理し、システム監査のための証跡管理が行える。 3)UNIXサーバの特権操作に対して、ユーザ毎のアクセス制御、監査ログ採取を行い、サーバの安全な運用を実現する。

事業体(研究所)名　富士通株式会社	
所在地（郵便番号及び住所）　105-7123 東京都港区東新橋1-5-2 汐留シティセンター	
関連部署及び電話番号　サービスビジネス本部安心安全ビジネス推進室 03-6424-6249	
URL　富士通ポータル：http://jp.fujitsu.com/ 富士通セキュリティポータル：http://segroup.fujitsu.com/secure/	
対象技術	技術開発状況
クライアント データ	企業の重要データへのアクセスが可能な社員は、悪意を持てばいつでも情報を持ち出すことができる。情報漏洩の多くが企業内部から発生しているというデータもある。FENCEシリーズは、重要データの暗号化[FENCE-Pro]、外部への持出し抑止[FENCE-G]、USBキーを使用した認証[FENCE-AP]、PC上の操作情報の認跡記録[FENCE-Tracer]等の機能を提供する。これらのシリーズ製品の組み合わせにより、多岐に渡る情報漏洩リスクから顧客情報などの重要データを守る。 ①FENCE-AP［認証］：本人認証により、アクセス権限のない利用者の、システムへの侵入を防ぐ。認証として、USBキーを利用し、不正アクセスの防止に役立てる。 ②FENCE-Pro［暗号］：データを暗号化し、セキュリティを確保する。社内で管理する場合も、社外へ持ち出す場合も、重要データを暗号化することで、情報漏洩を未然に防止する。 ③FENCE-G［漏洩防止］：CD-Rなどの外部デバイスや、印刷、メールの添付ファイルなどによるデータの持ち出しを制御し、企業内部からの情報漏洩を防止する。 ④FENCE-Tracer［認跡］：PC上の重要なデータに対する各種操作情報を認跡として記録し、これを専用ビューアにより、参照・管理することで、不正アクセスの抑止効果が得られる。

事業体(研究所)名　富士通株式会社	
所在地（郵便番号及び住所）　105-7123 東京都港区東新橋1-5-2 汐留シティセンター	
関連部署及び電話番号　サービスビジネス本部安心安全ビジネス推進室 03-6424-6249	
URL　富士通ポータル：http://jp.fujitsu.com/ 富士通セキュリティポータル：http://segroup.fujitsu.com/secure/	
対象技術	技術開発状況
データ	Systemwalker Desktop Right Master（システムウォーカー デスクトップ ライツ マスター）は、組織でのファイル共有において、機密情報、個人情報などが含まれるファイルを暗号化することで保護する。そして、ファイルにアクセス許可を設定することで、ファイルへの操作を制限して、情報の外部漏洩を防ぐことを目的とした製品である。 ①ライセンス管理：サーバに登録したファイルを使用するユーザ／グループによって、閲覧、印刷、復号などの操作に対するアクセス許可を設定できる。 ②ファイル操作制限：サーバに登録されたファイルについて、クライアントPCで使用するアプリケーションから、ファイルに設定されているライセンスに従って、閲覧、印刷、復号などの操作を制御できる。 サーバからローカルマシン上に移動してきたファイルについても同様に、設定されているライセンスにしたがって、閲覧、印刷、復号などの操作を制御できる。 ③ユーザ情報の管理：Wicrosoft Active Directoryのユーザ情報での一元管理が可能である。1台のクライアントPCを複数のユーザが使用する場合に、ユーザごとのライセンスや設定に従った運用を行うことができる。 ④重畳印刷：保護されたMicrosoft Officeファイルの印刷時に、ユーザIDとライセンス取得日時を挿入できる。これにより複写して配付することを牽制できる。 ⑤オフライン環境での利用：オフラインライセンスを付与することによって、Systemwalker Desktop Right Masterライセンス配信サーバと接続できない環境でも一時的に保護されたファイルを閲覧できる。

事業体(研究所)名　富士通エフ･アイ･ピー株式会社	
所在地（郵便番号及び住所）　135-8686 東京都江東区青梅2-45	
関連部署及び電話番号　セキュリティビジネス部 03-5531-0200	
URL　http://www.fip.fujitsu.com/	
対象技術	技術開発状況
データ	メインフレームからPCに至るまでマルチプラットフォーム、さらにはマルチベンダーOSに対応した暗号化ツール。 ［主な機能］ ①改竄検出機能。圧縮･暗号化前と復元･復号化後にハッシュ値を算出して比較し、ファイルが正しく復元･復号化されているかをチェックする。 ②ワンタイム鍵生成機能。利用者が指定した鍵から毎回別の鍵に内部で変換する。同じデータを同じ鍵で暗号化しても別の暗号データになるので、解読されにくくなる。 ③固定長圧縮機能。圧縮･暗号化ファイルをメインフレームと受け渡しする場合、転送ソフトで利用しやすいよう、固定長ファイル形式で出力できる。

事業体(研究所)名　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）　105-0011 東京都港区芝公園1-4-1 メソニック38MTビル	
関連部署及び電話番号　経営企画室 03-6430-2300	
URL　http://www.fsas.fujitsu.com/index.html	
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 データ	CXS型のシステムで、複数のバイオ認証、サーバでの一元管理を取り入れたバイオ認証システム。 さらに、業務アプリケーションの様々な場面にタイミングフリーに組み込めるApiをCXSからWEBアプリまで具備。

事業体(研究所)名　株式会社富士通北陸システムズ	
所在地（郵便番号及び住所）　921-8611 石川県金沢市増泉3-4-30	
関連部署及び電話番号　076-241-4500	
URL　http://jp.fujitsu.com/group/fjh/	
対象技術	技術開発状況
クライアント データ	コンピュータシステム上のファイルやネットワークを流れるデータの機密保護を目的としたファイル暗号製品である。 ①厳重に保管： 大量データ、大きなデータも暗号化と圧縮で厳重に保管、安心である。SecureBoxは重要資料など、パスワード設定ひとつで簡単に暗号化して、バックアップできる。取引先への郵送なども安心である。暗号化と同時に圧縮もできるので、別途圧縮ソフトを用意しなくても使用量を節約できる。非常に強度の高い暗号化アルゴリズム（AES）を実装している。 ②安全なメール： 企業間の取引において、添付ファイルを暗号化せずメールを送信するのは心配である。SecureBoxでは利便性を追求し、メールに添付するファイルやフォルダをクリックし、パスワードを入力するだけで自動的にメールソフトを起動する。添付ファイルは自己復号形式のファイルとして作成できる。この場合、送信相手はSecureBoxをインストールしなくても添付ファイルを復号することができる。 ③リカバリー： パスワード忘れなど緊急事態が発生しても、企業の情報資産を損失することなく安心である。利用者がミスを起こした場合のリカバリー機構を設けておくことは企業として当然必要である。リカバリーできなかった場合は、取引先や自社に多大な被害を与えることになる。SecureBoxでは利用者がパスワードを忘れてしまったり、不在時に緊急でデータを確認したい場合のために、リカバリー機構を用意している。 ④PCデータの保護： 通常のパソコン操作で重要資料を守る。利用者は暗号化／複合化ということを意識する必要がない。社外でモバイル端末を使用時、万が一パソコンの置き忘れや盗難が発生しても、情報が漏えいすることはない。

事業体(研究所)名　マイクロソフト株式会社	
所在地（郵便番号及び住所）　151-8583 東京都渋谷区代々木2-2-1 小田急サザンタワー	
関連部署及び電話番号　技術企画室 03-5334-9230	
URL　http://www.microsoft.com/japan/	
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	Internet Security & Acceleration Server 2006（以下ISA Server 2006）は、統合されたエッジセキュリティゲートウェイである。 IT環境をインターネットの脅威から保護しつつ、ユーザがアプリケーションやデータにセキュリティで保護された状態で、迅速にリモートアクセスできるようになる。 ①セキュリティで保護されたアプリケーション公開： ISA Server 2006を使用したセキュリティで保護されたアプリケーション公開により、企業ネットワークの外部リモートユーザが、企業のExchange Server、Sharepoint Server、その他のWebアプリケーションサーバを安全にアクセスできるようになる。 ②ブランチオフィスゲートウェイ： 企業ではISA Server 2006をブランチオフィスゲートウェイとして使用し、ネットワークの帯域幅を有効に使用しながら、支社に接続したり、支社をセキュリティで保護したりできる。 ③Webアクセス保護： ISA Server 2006では、プロキシファイアウォールのハイブリッドなアーキテクチャ、詳細なポリシー、詳細なコンテンツ検査、包括的な警告および監視機能により、Webアクセス保護を提供する。

事業体(研究所)名　マイクロソフト株式会社	
所在地（郵便番号及び住所）　151-8583 東京都渋谷区代々木2-2-1 小田急サザンタワー	
関連部署及び電話番号　技術企画室 03-5334-9230	
URL　http://www.microsoft.com/japan/	
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	Microsoft Antigenサーバセキュリティ製品により、企業はウィルススパムおよび不正なコンテンツから電子メールや*コラボレーションサーバ（ファイルサーバ）を保護できる。*:sharepoint server Antigenは電子メールおよびコラボレーションサーバを包括的に保護できる。 Antigenの利点は以下の3点である。 ①高度な保護：電子メールのインフラストラクチャ複数層で提供されるマルチエンジンにより、電子メールによる脅威から強力に保護される。 ②可用性と制御：Microsoft ExchangeおよびWindowsベースのSMTPサーバとの密接な統合により、可用性と管理制御を最大限に発揮できるようになる。 ③安全なコンテンツ：組織では内部および外部の通信から不適切な言語（キーワード）や危険な添付ファイルを除去できる。

事業体(研究所)名　マイクロソフト株式会社	
所在地（郵便番号及び住所）　151-8583 東京都渋谷区代々木2-2-1 小田急サザンタワー	
関連部署及び電話番号　技術企画室 03-5334-9230	
URL　http://www.microsoft.com/japan/	
対象技術	技術開発状況
クライアント 通信情報 データ	情報やサービスをより管理しやすく、安全な環境で保護するオペレーティングシステム。 危険なソフトウェアへの脆弱性を緩和し、攻撃から防御し、問題が発生しないうちに危険なソフトウェアを除去する機能を備えている。 また、高度な監査／レポート機能を装備しており、IT管理を合理化し、少ないコストでコンプライアンスを実現することができる機能を持つ。

事業体(研究所)名　マイクロソフト株式会社	
所在地（郵便番号及び住所）　151-8583 東京都渋谷区代々木2-2-1 小田急サザンタワー	
関連部署及び電話番号　技術企画室 03-5334-9230	
URL　http://www.microsoft.com/japan/	
対象技術	技術開発状況
データ	RMSは情報の作成者または所有者が設定したアクセス許可に基づいて、機密情報の利用を制限できる情報保護ソリューションである。ドキュメントの閲覧、編集、コピー印刷、およびメールの転送を制限できる。 情報の利用者は、アクセス許可が設定されたコンテンツに対して、RMSサーバから与えられた権限に合わせた操作しか行えない。 ファイアウォールの内外問わずに、情報の利用を制限できるため、過失や操作ミスによってどのような経路を辿っていても、過失や操作ミスによる機密情報の流出や改ざんを予防できる。

事業体(研究所)名　三菱電機エンジニアリング株式会社　鎌倉事業所	
所在地（郵便番号及び住所）　247-0065 神奈川県鎌倉市上町屋730	
関連部署及び電話番号　情報技術部　電波情報課 0467-41-2559	
URL　http://www.mee.co.jp/pro/sales/media/misty.html	
対象技術	技術開発状況
通信情報 データ その他	耐タンパセキュアボード「MISTYKEYPER2」は、耐タンパ機構による鍵管理機能を備えた暗号処理装置。システム利用者の秘密情報である暗号鍵を専用のハードウェア内に保管管理し不正アクセスから保護。

事業体(研究所)名　三菱電機(株)情報技術総合研究所	
所在地（郵便番号及び住所）　247-8501 神奈川県鎌倉市大船5-1-1	
関連部署及び電話番号	
URL　http://www.mitsubishielectric.co.jp/corporate/randd/information_technology/	
対象技術	技術開発状況
通信情報	PON（Passive Optical Network）は光ファイバーケーブルを分岐し、多数の加入者側装置が光ファイバーケーブルを共有している。 従って、信号を暗号化しない場合には、他のユーザ宛のデータが盗聴可能である。 本装置ではAES128によるデータの暗号化を行い盗聴を防止する。 また、IEEE802.1x認証機能を有し、なりすましを防止する。

事業体(研究所)名　ユニアデックス株式会社	
所在地（郵便番号及び住所）　135-8560 東京都江東区豊洲1-1-1	
関連部署及び電話番号　商品戦略部 03-5546-4900（代表）	
URL　http://www.uniadex.co.jp/	
対象技術	技術開発状況
ネットワーク クライアント	膨大な数のクライアントが全社に分散している今日、たった1台のクライアントのセキュリティホールの放置がウイルスの全社への蔓延や、システム侵入、データ改ざん、情報漏洩という致命的な出来事にまで発展しかねない。ユニアデックス株式会社のクライアント検疫ソリューションでは、以下のことを実現する。 ・全クライアントの常時検疫（検査） ・未対策クライアントの隔離 ・対策実施後のネットワークへの復帰 すなわち、パッチを適用しないクライアントPCを検査し、ネットワークより隔離する。これにより、 ・未対策PCへの新ウィルス感染 ・他PCへのウィルス蔓延 ・ネットワーク使用不能（Dos）の防止 ・ウィルスによる情報漏洩 を防ぐ。隔離されたPCは、治療によって脆弱性対策が実現される。 また、以下のような他のツールと連携して、クライアントのセキュリティ対策を実現することが可能である。 ・クライアントPCのセキュリティ管理を含めて一元的なIT資産管理のため、IT資産管理ツール（例、ユニアデックスADMi-21）と連携する。 ・クライアントPCへの最新セキュリティパッチの適用のため、自動パッチ適用ソリューション（例、WSUS）と連携する。 ・クライアントPCのネットワークからのウィルス感染を防御のため、パーソナル・ファイアウォール製品（例、ウィルスバスターコーポレートエディションアドバンス）と連携する。

事業体(研究所)名　ユニアデックス株式会社	
所在地（郵便番号及び住所）　135-8560　東京都江東区豊洲1-1-1	
関連部署及び電話番号　商品戦略部　03-5546-4900（代表）	
URL　http://www.uniadex.co.jp	
クライアント	IDAgentはICカード（社員証など）を利用した情報システムの個人認証ソリューションである。日本ユニシス株式会社と大日本印刷株式会社と協同で開発を行い、クライアント部を大日本印刷株式会社が担当し、サーバ部を日本ユニシス株式会社並びにユニアデックス株式会社にて担当した。IDAgentの主な特徴としては、 ・ ICカードの所有とパスワード入力による二相認証により、厳密な個人認証が可能である。 ・ PCログオン認証、スクリーンロック、簡易パスワード入力（シングルサインオン）、PC利用者制限、外部記憶媒体の利用制御、操作ログ収集などの機能により情報システムの不正使用、情報漏洩の防止に貢献する。 ・ 社員証のICカード化と合わせてご検討いただくと効果的である。SSFC（Shared Security Formats Cooperation）対応機器と連携し、トータルなオフィスセキュリティを実現することが可能である。 ・ 認証サーバを利用することで、ユーザー情報の集中管理を実現する。 ・ PKI（公開鍵基盤）を利用することが可能である。 特に、情報システム利用者のアクセス権限情報と認証情報をサーバで集中管理することによって、ユーザーや管理者の負荷を軽減し、大規模システムへの対応を可能にした。例えば、紛失時のICカード失効処理、組織変更や人事異動に伴う認証情報の変更など、ICカードを回収せずに、管理者ツールにて一元的に行うことができるため、スムーズな運用を実現する。

事業体(研究所)名　ユニアデックス株式会社	
所在地（郵便番号及び住所）　135-8560　東京都江東区豊洲1-1-1	
関連部署及び電話番号　商品戦略部　03-5546-4900（代表）	
URL　http://www.uniadex.co.jp/	
対象技術	技術開発状況
クライアント	PCセキュリティサービス（マカフィー・スイート）では、 ・ウィルススキャン（ウィルス駆除） ・パーソナルファイアウォールプラス（不正アクセス防止） ・プライバシーサービス（個人情報保護） ・スパムキラー（迷惑メール防止） の4つのセキュリティパッケージがひとつになった個人向けサービスである。

事業体(研究所)名　ユニアデックス株式会社	
所在地（郵便番号及び住所）　135-8560　東京都江東区豊洲1-1-1	
関連部署及び電話番号　商品戦略部　03-5546-4900（代表）	
URL　http://www.uniadex.co.jp/	
対象技術	技術開発状況
クライアント	nProtect Personalでは、 ･フィッシング機能 ･アンチワーム機能 ･入力内容暗号化機能 ･アンチウイルス機能 ･不正アクセス遮断機能 これらのセキュリティパッケージがひとつになった個人向けサービスである。

事業体(研究所)名　ユニアデックス株式会社	
所在地（郵便番号及び住所）　135-8560　東京都江東区豊洲1-1-1	
関連部署及び電話番号　商品戦略部　03-5546-4900（代表）	
URL　http://www.uniadex.co.jp/	
対象技術	技術開発状況
その他	i-フィルターは、お子様がインターネットを利用する際にアダルトサイトなどの有害ページを表示させないサービスである。 ブロックカテゴリ設定･使用時間設定等が可能である。

事業体(研究所)名　株式会社ラック	
所在地（郵便番号及び住所）　105-7111　東京都港区東新橋1-5-2　汐留シティセンター11F	
関連部署及び電話番号　管理本部　広報室　03-5537-2620	
URL　http://www.lac.co.jp	
ネットワーク サーバ 通信情報 データ	・　株式会社ラックのセキュリティエンジニアが提供する最新の定義ファイルで最新の対策が行える。 ・　様々な構成に柔軟に対応することが可能。 ・　日本語対応で操作がわかりやすい。 ・　様々なWAF機能を包括。

事業体(研究所)名　株式会社ラック	
所在地（郵便番号及び住所）　105-7111 東京都港区東新橋1-5-2 汐留シティセンター11F	
関連部署及び電話番号　管理本部　広報室 03-5537-2620	
URL　http://www.lac.co.jp/	
対象技術	技術開発状況
ネットワーク サーバ 通信情報	・Webアプリケーションを狙った攻撃をシャットアウト。 ・セキュリティの向上とコスト削減を同時に実現。 ・次世代ASICが多くの機能を実現。

事業体(研究所)名　株式会社ラック	
所在地（郵便番号及び住所）　105-7111 東京都港区東新橋1-5-2 汐留シティセンター11F	
関連部署及び電話番号　管理本部　広報室 03-5537-2620	
URL　http://www.lac.co.jp/	
対象技術	技術開発状況
ネットワーク クライアント	Webアクセス制御 アンチスパイウェア IMコントロール/P2Pコントロール SSL暗号化対応 容易な管理

事業体(研究所)名　株式会社ラック	
所在地（郵便番号及び住所）　105-7111 東京都港区東新橋1-5-2 汐留シティセンター11F	
関連部署及び電話番号　管理本部　広報室 03-5537-2620	
URL　http://www.lac.co.jp/	
対象技術	技術開発状況
ネットワーク	IPSのための高性能アプライアンス 信頼の検知手法 Virtual IDS/IPS シグネチャの更新とユーザ定義シグネチャ

事業体(研究所)名　株式会社ラック	
所在地（郵便番号及び住所）　105-7111 東京都港区東新橋1-5-2 汐留シティセンター11F	
関連部署及び電話番号　管理本部　広報室 03-5537-2620	
URL　http://www.lac.co.jp/	
対象技術	技術開発状況
ネットワーク	ネットワークIPSとしての基本機能を網羅。既存の冗長化されたネットワーク環境において、高セキュリティレベルを確保するハイ・アベイラビリティ（H/A）機能を搭載。さらには、プロトコル分析モジュールとISSが誇る世界最大級（民間組織）セキュリティ、専門研究機関「X-Force」がproventia Net-work IPSを支える2つのコアとなっている。

事業体(研究所)名　株式会社ラック	
所在地（郵便番号及び住所）　105-7111 東京都港区東新橋1-5-2 汐留シティセンター11F	
関連部署及び電話番号　管理本部　広報室 03-5537-2620	
URL　http://www.lac.co.jp/	
対象技術	技術開発状況
ネットワーク サーバ	株式会社ラックが誇る国内最大級のリモートセキュリティ監視センタJSOCにて、ネットワークセキュリティに関するプロフェッショナルであるセキュリティアナリストが24時間、365日の体制で顧客のFW、IDS、IPSのログを自身の目で分析、危険性の有無を判断している。危険性があると判断した場合には、顧客に迅速に連絡し、その場で最適なコンサルティングを行う。

事業体(研究所)名　株式会社ラック	
所在地（郵便番号及び住所）　105-7111 東京都港区東新橋1-5-2 汐留シティセンター11F	
関連部署及び電話番号　管理本部　広報室 03-5537-2620	
URL　http://www.lac.co.jp/	
対象技術	技術開発状況
サーバ	FW、IDSなどのセキュリティ製品の導入だけでなく、より有効なセキュリティ対策を講じるため、セキュリティを考慮したサーバの設定やアップデートを行い、堅牢なセキュアサーバを構築する。

事業体(研究所)名　株式会社ラック	
所在地（郵便番号及び住所）　105-7111 東京都港区東新橋1-5-2 汐留シティセンター11F	
関連部署及び電話番号　管理本部　広報室 03-5537-2620	
URL　http://www.lac.co.jp/	
対象技術	技術開発状況
サーバ	ネットワークに不正接続するPCを検知、強制排除して、即時に通報。ハードウェアー体型のため、余計なサーバ管理の必要もなく、承認PCを登録するだけで設定が可能。