

平成18年2月23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17年1月1日から12月31日までの不正アクセス行為の発生状況を公表する。

アクセス制御機能に関する技術の研究開発の状況

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

### 3 掲載先

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

総務省ホームページ [http://www.soumu.go.jp/joho\\_tsusin/security/security.html](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17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17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17年中の不正アクセス行為の認知件数は592件で、前年と比べ、236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、ホームページ書換えプログラム（コンピュータ・ワーム）によるものである。

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

##### (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（356件）、次いで一般企業（203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
プロバイダ	59	182	243	98	126	356
一般企業	25	429	62	76	202	203
大学、研究機関等	8	101	3	16	6	12
その他	14	139	21	22	22	21
うち行政機関	-	-	12	3	12	17
不明	0	402	0	0	0	0
計	106	1,253	329	212	356	592

「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2）からの届出によるものが最も多く（505件）、次いで警察職員によるサイバーパトロール、被疑者の取調べ等の警察活動によるもの（33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（30件）、発見者からの通報によるもの（14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
アクセス管理者からの届出	30	168	47	12	29	30
利用権者からの届出	23	118	92	78	172	505
警察活動	35	930	185	100	146	33
発見者からの通報	7	21	0	19	7	14
その他	11	16	5	3	2	10
計	106	1,253	329	212	356	592

(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・オークションに関する不正操作（他人になりすましての出品・入札等）が最も多く（356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）（140件）、ホームページの改ざん・消去（31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）（21件）、情報の不正入手（電子メールの盗み見等）（18件）、利用権者のパスワード変更（6件）、インターネットバンキングの不正送金（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	件数 (件)( )
インターネット・オークションに関する不正操作	356
オンラインゲームの不正操作	140
ホームページの改ざん・消去	31
不正ファイルの蔵置	21
情報の不正入手	18
利用権者のパスワード変更	6
インターネットバンキングの不正送金	5
不明	32
その他	9

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) 検挙事件数等

平成17年中における不正アクセス禁止法違反の検挙事件数（注4）は94事件、検挙人員は116人と、前年と比べ、それぞれ29事件、28人増加した。また、検挙事件数、検挙人員の内訳をみると、不正アクセス行為に係るものがそれぞれ94事件、113人、不正アクセス助長行為に係るものがそれぞれ6事件、6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
不正アクセス 行為	検挙事件数	30	35	51	58	65	94
	検挙件数	62	66	102	143	142	271
	検挙人員	34	51	68	76	88	113
不正アクセス 助長行為	検挙事件数	4	1	2	2	0	6
	検挙件数	5	1	3	2	0	6
	検挙人員	5	1	3	2	0	6
計	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)
	検挙件数 (件)	67	67	105	145	142	277
	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)

### (2) 不正アクセス行為の態様

検挙事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5）が90事件、セキュリティ・ホール攻撃型（注6）が5事件であった（うち1事件は、識別符号窃用型及びセキュリティ・ホール攻撃型の両方の不正アクセス行為が行われた。）。

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

### 3 検挙事例

1	<b>公知のIDからパスワードを推測し、他人になりすましてインターネット・オークションに架空出品した不正アクセス禁止法違反、電磁的記録不正作出・同供用及び詐欺事件</b>
---	---

会社員の男(28)らは、インターネット・オークションの会員の公知のIDからパスワードを推測し、当該会員になりすまして不正アクセス行為を行った。また、同会員が登録していた電子メールアドレス等を、同会員が変更する手続きをとった旨の虚偽の情報を送信して事実証明に関する電磁的記録を不正に作出し、インターネット・オークション事業者の事務処理の用に供した。さらに、同インターネット・オークションに携帯電話等を売ると偽り、多数の落札者から代金をだまし取った。平成17年1月、不正アクセス禁止法違反、電磁的記録不正作出・同供用罪及び詐欺罪で検挙した(大分、宮城、警視庁、茨城、兵庫、熊本)。

2	<b>キーロガー(注7)を使用して識別符号を不正取得するなどした不正アクセス禁止法違反事件</b>
---	---

元大学教授の男(50)は、教え子の電子メールをのぞき見る目的で、勤務していた大学のコンピュータにキーロガーを仕掛け、当該コンピュータを利用した同大学の女子学生の識別符号を不正に入手し、平成16年11月から17年1月までの間、これらの識別符号を使用して、自宅、同大学等に設置されたコンピュータから不正アクセス行為を行った。平成17年4月、不正アクセス禁止法違反で検挙した(広島)。

3	<b>クラッキング・ツールを使用して不正取得した識別符号を他の学校等に送りつけた不正アクセス禁止法違反事件</b>
---	---

無職の男(19)は、平成16年11月、自分のハッキングの力量を試す目的で、当時在学していたコンピュータ専門学校のサーバに対し、クラッキング・ツールを使用して不正アクセスを行い、同校生徒約500人分の識別符号<sup>きごう</sup>を不正に取得した。男は、これが原因で退学処分となったことから、同校の信用を毀損する目的で、平成17年2月、以前取得した識別符号を別の専門学校に電子メールで送信し、不正アクセス行為を助長した。平成17年5月、不正アクセス禁止法違反で検挙した(京都)。

4	<b>大手インターネットサービス会社のホームページを複製していわゆるフィッシングサイトを開設した著作権法違反及び不正アクセス禁止法違反事件</b>
---	---

会社員の男(42)は、平成17年2月、インターネットサービス会社が会員に付与した

識別符号を不正に入手する目的で、同社が著作権を有するホームページに酷似した「ログイン画面」をインターネット上に公開し、これを本物の「ログイン画面」であると誤信した者が入力した識別符号を不正に入手するとともに、これらの識別符号を使用して不正アクセス行為を行った。平成17年6月、著作権法違反及び不正アクセス禁止法違反で検挙した（警視庁）。

5

**セキュリティの脆弱性を突いた不正アクセス行為により個人情報を入手した不正アクセス禁止法違反事件**

大学生の男(27)は、平成17年3月、個人情報を入手する目的で、旅行会社が設置・管理するサーバにセキュリティの脆弱性を突いた不正アクセス行為を約19万回行い、同社の会員の氏名、住所、パスワード等の個人情報約16万件を不正に入手した。平成17年6月、不正アクセス禁止法違反で検挙した（警視庁）。

6

**インターネットを通じて購入した他人の識別符号を利用したインターネット・オークションに係る不正アクセス禁止法違反及び詐欺事件**

無職の男(33)と女(23)は、不正に取得したインターネット・オークション会員のID・パスワード約150組をインターネット上の掲示板を通じて購入し、本人確認なく入手することが可能なプリペイド式データ通信カードを使用して、これらのIDに係る利用権者になりすまして、同オークションのコンピュータに不正アクセス行為を行った。また、同インターネット・オークションにおいて、パソコン等を売ると偽り、落札者から代金をだまし取った。平成17年9月、不正アクセス禁止法違反及び詐欺罪で検挙した（茨城）。

7

**企業の顧客名簿を盗むために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**

契約社員の男(40)は、以前、システム開発を行った企業の顧客名簿を売却して利益を得る目的で、当時貸与されていた識別符号を使用して不正アクセス行為を行い、当該企業のコンピュータに蔵置されていた約18万件の顧客情報を入手した。平成17年10月、不正アクセス禁止法違反で検挙した（千葉）。

8

**不正に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するなどした不正アクセス禁止法違反及び電磁的記録不正作出・同供用事件**

大学生の男(21)は、オンラインゲームで他人が使用しているアイテムを不正に収集

し、それを販売して利益を得る目的で、オンラインゲーム会社の契約社員の女(22)をそそのかして実在する複数のオンラインゲーム会員の識別符号を入手し、平成17年6月から8月までの間、会員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。また、これらの会員のパスワードを、会員自らが変更する手続をとった旨の虚偽の情報を送信して事実証明に関する電磁的記録を不正に作出し、当該オンラインゲーム会社の事務処理の用に供した。平成17年11月、不正アクセス禁止法違反及び電磁的記録不正作出・同供用罪で検挙した(北海道)。

9

**スパイウェア(注8)によりインターネットバンキングの利用権者の識別符号を盗み取り、使用した不正アクセス禁止法違反及び電子計算機使用詐欺事件**

無職の男(34)ら2人は、平成17年7月、共謀してスパイウェアを作成し、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、当該スパイウェアを取引上の苦情を装った電子メールに添付して送り付け、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21万円の送金操作を行った。平成17年11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) 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多くが識別符号窃用型であった（90事件（264件））。その多くは、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（37事件（95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（24事件（33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（13事件（16件））等、特に高度な技術を有していない者でも行えるものであったが、スパイウェア等の不正なプログラムを作成し、及び使用して、識別符号を入手したもの（4事件（33件））があるなど、高度なコンピュータ技術を悪用したものも発生している。

また、プログラムの脆弱性を突いてコンピュータを攻撃し、情報を不正取得するなどのセキュリティ・ホール攻撃型の不正アクセス行為（5事件（7件））も発生している。

表4 - 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	事件数 (事件)( )	件数 (件)
識別符号窃用型	90	264
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	37	95
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	24	33
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	13	16
他人から購入したもの	4	69
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	4	33
共犯者等から入手したもの	4	12
フィッシングサイトにより入手したもの	1	1
その他	4	5
セキュリティ・ホール攻撃型	5	7

事件数については、重複計上あり。

##### (2) 被疑者

不正アクセス禁止法違反に係る被疑者についてみると、面識のない他人によるものが最も多く（51事件（211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（35事件（48件））、ネットワーク上のみの知り合いによるもの（11事件（18件））となっている（重複計上あり）。

また、被疑者の年齢についてみると、20歳代が最も多く（40人）、次いで10歳代（35人）、30歳代（27人）、40歳代（9人）、50歳代（5人）の順となっている。

なお、最年少の者は14歳、最年長の者は57歳であった。

表4 - 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
10歳代	6	2	6	16	26	35
20歳代	13	28	30	26	21	40
30歳代	16	5	26	24	23	27
40歳代	2	16	7	9	17	9
50歳代	0	0	0	1	1	5
計	37	51	69	76	88	116

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、元交際相手、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(26事件(31件))、次いで不正に金を得るため(22事件(167件))、オンラインゲームで不正操作を行うため(19事件(25件))、顧客データの収集等情報を不正に入手するため(16事件(23件))、好奇心を満たすため(9事件(20件))の順となっている。

前年と比べ、不正に金を得るため(13事件(135件)増加)、情報を不正に入手するためが増加(11事件(11件)増加)した一方、好奇心を満たすためが減少(6事件(3件)減少)した。

表4 - 3 不正アクセス行為の動機の内訳

動機	事件数 (事件)( )	件数 (件)
嫌がらせや仕返しのため	26	31
不正に金を得るため	22	167
オンラインゲームで不正操作を行うため	19	25
顧客データの収集等情報を不正に入手するため	16	23
好奇心を満たすため	9	20
自分の技量を計るため	4	2
その他	3	3

事件数については、重複計上あり。

(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事件(90事件(264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についてみると、オンラインゲームが最も多く(33事件(42件))、次いでインターネット・オークション(25事件(154件))、電子メール(11事件(14件))、ホームページ公開サービス(9事件(8件))、インターネットバンキング(5事件(33件))の順となっている。

表4 - 4 利用されたサービスの内訳

利用されたサービス	事件数 (事件)( )	件数 (件)
識別符号窃用型	90	264
オンラインゲーム	33	42
インターネット・オークション	25	154
電子メール	11	14
ホームページ公開サービス	9	8
インターネットバンキング	5	33
会員専用・社員用内部サイト	5	8
会員・顧客データベース	2	2
その他	2	3

事件数については、重複計上あり。

(5) その他

不正アクセス禁止法違反の他の罪についても併せて検挙した事件は30事件あり、その内訳は次のとおりである。

表4 - 5 併せて検挙した事件の内訳

罪名	事件数 (事件)( )
電磁的記録不正作出・同供用	17
詐欺	9
電子計算機使用詐欺	3
電子計算機損壊等業務妨害	2
窃盗	2
業務妨害	1
文書偽造	1
著作権法違反	1
わいせつ図画公然陳列	1
脅迫	1
名誉毀損 <sup>き</sup>	1

事件数については、重複計上あり。

5 都道府県公安委員会による援助措置

平成17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4件（静岡1件、愛知2件、福岡1件）であった。

表5 - 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
援助措置(件)	6	21	5	5	3	4

## 6 防御上の留意事項

### (1) 利用権者の講ずべき措置

#### ア 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が多発していることから、利用権者が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は避け、ID等からの推定が難しいものとするとともに、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・管理する必要がある。

#### イ ホームページでのID・パスワード等の入力に関する注意

本物のサイトに酷似したフィッシングサイトを開設し、本物と誤信した者が入力したID・パスワード等を使用した不正アクセス事件が発生している。そのため、心当たりのない電子メールやそれにより誘導されるなどしたホームページの指示をうのみにしてID・パスワード等を入力しないよう注意する必要がある。

#### ウ 不正プログラムへの対策

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・パスワード等を不正に取得した手口がみられたことから、コンピュータ・ウイルス対策やスパイウェア対策（最新のコンピュータ・ウイルス対策ソフトの利用、オペレーティングシステムのバージョンアップ等）を適切に講ずる必要がある。

また、インターネットカフェ等における不特定多数の者が利用できるコンピュータでは、不正プログラムが動作している可能性があることにも注意する必要がある。

### (2) アクセス管理者の講ずべき措置

#### ア 利用権者に対する注意喚起等

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、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の措置を講ずる必要がある。

#### イ プログラムの脆弱性に関する対策

平成17年中においてもセキュリティ・ホール攻撃型の不正アクセス行為による事件が発生していることから、アクセス管理者は、インターネット上で公表される最新のセキュリティ情報を随時確認し、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脆弱性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の措置を講ずる必要がある。

#### 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アクセス管理者は、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とともに、コンピュータへのリカバリーソフトの導入、利用終了時における履歴の削除、プログラムのインストール制限を行うなど

の措置を講ずる必要がある。

## (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

金融機関等を装って電子メールを送信し、受信者が偽のウェブサイトアクセスするよう仕向け、そこで個人の識別符号（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 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5 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6 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7 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。

注8 スパイウェア

パソコン内のファイル、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。

## 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17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9）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515件（昨年：594件）であった。（注10）

2005年は2004年と比べて、侵入やDoSの届出が大幅に増加した。また全体的に見ると、被害があった届出件数が大幅に増加した。

届出のうち実際に被害があったケースにおける被害内容の分類では、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726件（昨年：557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650件（昨年：515件）あった。

##### (ア) 侵入の事前調査行為

システム情報の調査、稼働サービスの調査、アカウント名の調査等である。318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。

87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65件である。

##### 【主な内容】

パスワード推測：45件

ソフトウェアのバグを利用した攻撃：24件

システムの設定内容を利用した攻撃：4件

##### (ウ) 不正行為の実行及び目的達成後の行為

実際に侵入を受けた65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。

##### 【主な内容】

ファイル等の改ざん、破壊等：74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：35件

資源利用(ファイル、CPU使用)：28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：25件

裏口(バックドア)の作成：5件

証拠の隠滅(ログの消去など)：12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。29件(昨年：10件)の届出があった。

##### 【主な内容】

過負荷を与える攻撃：26件

大量のspamメール送り付け：3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、47件(昨年：33件)の届出があった。

##### 【主な内容】

メールの不正中継に関するもの：10件

メールアドレス(ドメイン)の詐称：6件

なりすまし：9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98件(昨年：43件)、メール中継に係わる問題(弱点)のあった8件(昨年：3件)などの計176件(昨年：55件)を分類すると以下ようになる。

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。

##### 【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：42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：28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：14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。

##### 【主な対象】

WWWサーバー：54件

メールサーバー：18件

ファイアウォール：1件

ルータ：159件  
その他のサーバー・不明：82件  
クライアント：197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206件（昨年：72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。

##### 【主な被害内容】

メールの不正中継に利用された：9件  
サーバーダウン：6件  
不正アカウント作成：4件  
WWW書き換え：32件  
パスワードファイル盗用：1件  
サービス低下：16件  
オープンプロキシ：1件  
ファイルの書き換え：69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。一度、原点に戻り、システム管理者は以下の点を確認して総合的に対策を行うことが望まれる。

- ・ ID やパスワードの厳重な管理及び設定
- ・ 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

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

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9 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10 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17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11)に係わる報告件数(注12)は3,485件であった。

#### ア プローブ、スキャン、その他不審なアクセスに関する報告

防御に成功したアタックや、コンピュータ/サービス/弱点の探査を意図したアクセス、その他の不審なアクセス等、システムのアクセス権において影響を生じないか、無視できるアクセスについて3,020件の報告があった。

[1/1-3/31: 1,160件、4/1-6/30: 575件、7/1-9/30:578件、10/1-12/31: 707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22件の報告があった。

[1/1-3/31: 3件、4/1-6/30: 6件、7/1-9/30: 11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13件の報告があった。

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

[1/1-3/31: 2件、4/1-6/30: 0件、7/1-9/30: 3件、10/1-12/31: 3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291件の報告があった。

[1/1-3/31: 36件、4/1-6/30: 78件、7/1-9/30: 75件、10/1-12/31: 102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131件の報告があった。

[1/1-3/31:37件、4/1-6/30: 48件、7/1-9/30: 8件、10/1-12/31: 38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.jpccert.or.jp/>参照。)

#### ア 注意喚起

[新規]

Microsoft Windows メタファイル処理の脆弱性に関する注意喚起

Microsoft Internet Explorer に含まれる脆弱性に関する注意喚起

TCP 1025番ポートへのスキャンの増加に関する注意喚起

Sober ワームの変種に関する注意喚起

Internet Explorer の JavaScript の脆弱性に関する注意喚起

Snort Back Orifice preprocessor の脆弱性に関する注意喚起

Microsoft 製品の脆弱性を使って伝播するワームに関する注意喚起

Microsoft 製品に含まれる脆弱性に関する注意喚起

TCP 1433番ポートへのスキャンの増加に関する注意喚起

DNS サーバーの設定とドメイン名の登録に関する注意喚起

VERITAS Backup Exec に含まれる脆弱性に関する注意喚起

OpenSSH の脆弱性を使ったシステムへの侵入に関する注意喚起

Web 偽装詐欺 (phishing) の踏み台サーバーに関する注意喚起

Microsoft 製品に含まれる脆弱性に関する注意喚起

#### イ 活動概要 (届出状況等の公表)

発行日: 2006-01-16 [ 2005年10月1日 ~ 2005年12月31日 ]

発行日: 2005-10-12 [ 2005年7月1日 ~ 2005年9月30日 ]

発行日: 2005-07-19 [ 2005年4月1日 ~ 2005年6月30日 ]

発行日: 2005-04-19 [ 2005年1月1日 ~ 2005年3月31日 ]

#### ウ JPCERT/CC レポート

[発行件数] 51件

[取り扱ったセキュリティ関連情報数] 285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.jpccert.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95件であった。

(詳細は<http://jvn.jp/>参照。)

[1/1-3/31: 21件、4/1-6/30: 24件、7/1-9/30: 31件、10/1-12/31: 19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48件であった。

[1/1-3/31: 7件、4/1-6/30: 13件、7/1-9/30: 14件、10/1-12/31: 14件]

注11 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12 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

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

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

次世代型電子認証基盤の整備

アクセスグラフに基づくポットネット検出技術の研究開発

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

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

強制的アクセス制御に基づく Web サーバーに関する調査・設計

### 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17年11月18日から12月19日までの間にアクセス制御技術に関する研究開発状況の募集を行ったところ、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。

コンピュータ・アソシエイツ株式会社

日本電気株式会社

データ・フォアビジョン株式会社

(2) 調査

警察庁が平成17年10月から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
- ・ 主なセキュリティに関係する展示会、シンポジウムにおいて出展・講演した企業・団体及び業種分類が「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

青山学院大学  
石巻専修大学  
岡山大学  
広島大学

イ 企業

株式会社アイアイジェイテクノロジー  
株式会社アズジェント  
株式会社アニモ  
株式会社アラジンジャパン  
R S Aセキュリティ株式会社  
株式会社インサイトテクノロジー  
株式会社エイチ・エム・アイ  
N E Cネクサソリューションズ株式会社  
N T Tコムウェア株式会社  
株式会社N T Tデータ  
エムオーテックス株式会社  
エントラストジャパン株式会社  
株式会社大塚商会  
オムロン株式会社  
音響署名株式会社  
グローバルセキュリティエキスパート株式会社  
シーア・インサイト・セキュリティ株式会社  
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  
ジャパンネット株式会社  
株式会社ソフテック  
株式会社ソフトクリエイト  
T I S株式会社  
東芝情報機器株式会社  
トーメンサイバービジネス株式会社  
日本サイバーサイン株式会社  
日本セキュアジェネレーション株式会社  
日本テレコム株式会社  
日本電気株式会社

日本電信電話株式会社  
日本認証サービス株式会社  
日立電子サービス株式会社  
富士通株式会社  
富士通サポート&サービス株式会社  
株式会社富士通ビー・エス・シー  
株式会社マックポートバイオセキュリティー  
三井物産セキュアディレクション株式会社  
三菱電機インフォメーションテクノロジー株式会社  
横河電機株式会社  
株式会社ワイ・デー・ケー

(別添1)

<b>対象技術</b> 侵入検知技術
<b>テーマ名</b> 情報通信危機管理基盤技術の研究開発
<b>開発年度</b> 平成12年度～17年度
<b>実施主体</b> 独立行政法人情報通信研究機構
<b>背景、目的</b> <p>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。</p>
<b>研究開発状況（概要）</b> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>
<b>詳細の入手方法（関連部署名及びその連絡先）</b> <p>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 電話 042-327-5774</p>
<b>将来の方向性</b> <p>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。</p>

<b>対象技術</b>	侵入探知技術
<b>テーマ名</b>	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
<b>開発年度</b>	平成14年度～平成16年度
<b>実施主体</b>	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ー株式会社（情報通信研究機構（NICT）からの委託）
<b>背景、目的</b>	<p>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。</p> <p>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った。</p>
<b>研究開発状況（概要）</b>	<ul style="list-style-type: none"> <li>・ 平成14年度より以下の研究開発を実施。 <ol style="list-style-type: none"> <li>(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</li> <li>(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查するための発信源探查技術の研究開発</li> </ol> </li> <li>・ 平成16年度末に開発終了。</li> </ul>
<b>詳細の入手方法（関連部署名及びその連絡先）</b>	<p>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  （<a href="http://www2.nict.go.jp/ns/s802/itakukenkyu.htm">http://www2.nict.go.jp/ns/s802/itakukenkyu.htm</a>）電話 03-3769-6810</p>
<b>将来の方向性</b>	<p>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。</p>

<b>対象技術</b>	侵入検知技術
<b>テーマ名</b>	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
<b>開発年度</b>	平成16年度～平成18年度
<b>実施主体</b>	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、株式会社KDDI 研究所（情報通信研究機構（NICT）からの委託）
<b>背景、目的</b>	<p>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。</p> <p>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。</p> <p>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。</p>
<b>研究開発状況（概要）</b>	<ul style="list-style-type: none"> <li>・平成16年度より以下の研究開発を実施中。 <ol style="list-style-type: none"> <li>(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</li> <li>(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</li> <li>(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</li> <li>(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</li> </ol> </li> <li>・平成18年度末に開発終了予定。</li> </ul>
<b>詳細の入手方法（関連部署名及びその連絡先）</b>	<p>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</p> <p>( <a href="http://www2.nict.go.jp/ns/s802/itakukenkyu.htm">http://www2.nict.go.jp/ns/s802/itakukenkyu.htm</a> ) 電話 03-3769-6810</p>
<b>将来の方向性</b>	<p>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。</p>

<b>対象技術</b> 侵入探知技術
<b>テーマ名</b> 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
<b>開発年度</b> 平成16年度～平成18年度
<b>実施主体</b> 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）
<p><b>背景、目的</b></p> <p>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。</p> <p>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。</p>
<p><b>研究開発状況（概要）</b></p> <ul style="list-style-type: none"> <li>・平成16年度より以下の研究開発を実施中。 <ol style="list-style-type: none"> <li>(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</li> <li>(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</li> <li>(3) サイト間のアクセス制御技術</li> </ol> </li> <li>・平成18年度末に開発終了予定。</li> </ul>
<p><b>詳細の入手方法（関連部署名及びその連絡先）</b></p> <p>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  （<a href="http://www2.nict.go.jp/ns/s802/itakukenkyu.htm">http://www2.nict.go.jp/ns/s802/itakukenkyu.htm</a>）電話 03-3769-6810</p>
<p><b>将来の方向性</b></p> <p>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。</p>

<b>対象技術</b>	その他認証技術
<b>テーマ名</b>	モバイルセキュリティ基盤技術の研究開発
<b>開発年度</b>	平成16年度～平成18年度
<b>実施主体</b>	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）
<b>背景、目的</b>	<p>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楽しむシーンが増加している。</p> <p>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。</p> <p>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。</p> <p>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。</p>
<b>研究開発状況（概要）</b>	<ul style="list-style-type: none"> <li>・平成16年度より以下の研究開発を実施中。 <ol style="list-style-type: none"> <li>(1) モバイルセキュリティ技術（長期・短期属性認証技術）</li> <li>(2) モバイルセキュリティ検証技術</li> <li>(3) モバイルサービス代行技術</li> <li>(4) モバイルコマースアプリケーション技術</li> </ol> </li> <li>・平成18年度末に開発終了予定。</li> </ul>
<b>詳細の入手方法（関連部署名及びその連絡先）</b>	<p>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</p> <p>(<a href="http://www2.nict.go.jp/ns/s802/itakukenyu.htm">http://www2.nict.go.jp/ns/s802/itakukenyu.htm</a>) 電話 03-3769-6810</p>
<b>将来の方向性</b>	<p>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。</p>

<b>対象技術</b>	その他認証技術
<b>テーマ名</b>	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
<b>開発年度</b>	平成16年度～平成18年度
<b>実施主体</b>	株式会社 日立製作所（情報通信研究機構（NICT）からの委託）
<b>背景、目的</b>	<p>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た。</p> <p>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。</p>
<b>研究開発状況（概要）</b>	<ul style="list-style-type: none"> <li>・平成16年度より以下の研究開発を実施中。 <ol style="list-style-type: none"> <li>(1) 耐タンパ技術に関する研究開発</li> <li>(2) 複合認証システム技術に関する研究開発</li> <li>(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</li> </ol> </li> <li>・平成18年度末に開発終了予定。</li> </ul>
<b>詳細の入手方法（関連部署名及びその連絡先）</b>	<p>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  （<a href="http://www2.nict.go.jp/ns/s802/itakukenkyu.htm">http://www2.nict.go.jp/ns/s802/itakukenkyu.htm</a>）電話 03-3769-6810</p>
<b>将来の方向性</b>	<p>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。</p>

<b>対象技術</b>	その他認証技術
<b>テーマ名</b>	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
<b>開発年度</b>	平成16年度～平成18年度
<b>実施主体</b>	株式会社 日立製作所（情報通信研究機構（NICT）からの委託）
<b>背景、目的</b>	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>
<b>研究開発状況（概要）</b>	<ul style="list-style-type: none"> <li>・ 平成16年度より以下の研究開発を実施中。 <ol style="list-style-type: none"> <li>(1) 認証方式の設計技術</li> <li>(2) 認証方式の安全性評価技術</li> </ol> </li> <li>・ 平成18年度末に開発終了予定。</li> </ul>
<b>詳細の入手方法（関連部署名及びその連絡先）</b>	<p>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</p> <p>(<a href="http://www2.nict.go.jp/ns/s802/itakukenkyu.htm">http://www2.nict.go.jp/ns/s802/itakukenkyu.htm</a>) 電話 03-3769-6810</p>
<b>将来の方向性</b>	<p>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。</p>

<b>対象技術</b> 異種ネットワーク接続技術
<b>テーマ名</b> 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
<b>開発年度</b> 平成17年度～平成19年度
<b>実施主体</b> エヌ・ティ・ティ・コミュニケーションズ株式会社（情報通信研究機構（NICT）からの委託）
<p><b>背景、目的</b></p> <p>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異種ネットワーク環境下にあると言える。</p> <p>一方、公共ネットワークにおいて提供されるサービスには、範囲は限定されるが非常に便利なものや非常に重要な情報を流通しているものが数多くあり、自治体間及び自治体と国の間での共同利用等による有効活用が求められている。</p> <p>本研究は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、有意なサービスを効果的に相互提供・利用するための最適情報通信サービス実現の要素技術の確立を行った上で、実証実験によりその有効性を評価することを目的とする。</p>
<p><b>研究開発状況（概要）</b></p> <p>平成17年度より以下の研究開発を実施中。</p> <ul style="list-style-type: none"> <li>（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に関する研究開発 <ul style="list-style-type: none"> <li>・ サービス相互接続のためのネットワーク環境定義</li> <li>・ マルチレイヤ環境情報自動判定・動的制御技術</li> </ul> </li> <li>（２） 高信頼ネットワークサービス環境構築技術に関する研究開発 <ul style="list-style-type: none"> <li>・ 大量トランザクション処理及び可用性保障を可能にする共有型クラスタリング・分散処理技術</li> <li>・ サーバサイドでの効率的な情報一括管理による機密情報持ち出し防止技術</li> </ul> </li> <li>（３） 異種ネットワーク上での高度マッチメイキング技術に関する研究開発</li> <li>（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</li> </ul>
<p><b>詳細の入手方法（関連部署名及びその連絡先）</b></p> <p>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  <a href="http://www2.nict.go.jp/ns/s802/itakukenkyu.htm">http://www2.nict.go.jp/ns/s802/itakukenkyu.htm</a> 電話：03-3769-6810</p>
<p><b>将来の方向性</b></p> <p>自治体を中心とする地方の公共ネットワークにおいて提供されるサービスを、共有あるいは共同利用するために、一定以上の品質でサービスを提供でき、直轄を越えたネットワーク上のどこにどのような情報やサービスが存在するのかを把握できる環境を整備する。</p>

<b>対象技術</b>	不正アクセス等発信原探索
<b>テーマ名</b>	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
<b>開発年度</b>	平成17年度～平成21年度
<b>実施主体</b>	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)、(有)インターネット応用研究所、(財)日本データ通信協会(情報通信研究機構(NICT)からの委託)
<b>背景、目的</b>	<p>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。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。そのために必要な“トレースバック”技術に関して研究を実施する。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。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。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ことを目的としている。</p>
<b>研究開発状況(概要)</b>	<p>平成17年度から以下の研究開発を実施中</p> <p>(1)全体アーキテクチャーの設計</p> <ul style="list-style-type: none"> <li>・トレースバック機構を構築する上で考慮すべき事項の網羅</li> <li>・基本的なトレースバック方式の開発</li> <li>・トレースバックシステムの相互接続アーキテクチャーの開発</li> </ul> <p>(2)トレースバック・アルゴリズムの開発</p> <ul style="list-style-type: none"> <li>・IPパケットトレースバック・アルゴリズムの開発</li> <li>・アプリケーショントレースバック・アルゴリズムの開発</li> <li>・異なるレイヤ由来の情報からトレースバック能力を向上させるアルゴリズムの開発</li> </ul> <p>(3)トレースバック用データ収集装置(プローブ装置)の開発</p> <p>(3)トレースバック・プラットフォームの開発</p> <p>(4)トレースバック・プラットフォームの実証実験</p>
<b>詳細の入手方法(関連部署名及びその連絡先)</b>	<p>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</p> <p><a href="http://www2.nict.go.jp/ns/s802/itakukenkyu.htm">http://www2.nict.go.jp/ns/s802/itakukenkyu.htm</a> 電話:03-3769-6810</p>
<b>将来の方向性</b>	<p>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、抑止力としての期待をしている。</p>

<b>対象技術</b>	その他認証技術
<b>テーマ名</b>	大容量データの安全な流通・保存技術に関する研究開発
<b>開発年度</b>	平成17年度から平成19年度までの3年間
<b>実施主体</b>	日立・東京理科大・NTT-COM(情報通信研究機構(NICT)からの委託)
<p><b>背景、目的</b></p> <p>ADSLサービスの普及などに伴いインターネットへの常時接続が一般的となった。さらに光ファイバーや無線ネットワーク技術の利用も急激に拡大しており、ネットワーク環境のブロードバンド化・ユビキタス化は今後もさらに進むことが予想される。また、このようなネットワーク環境の進展と同調して、ネットワーク接続型ストレージの利用が増加するとともに、ネットワークに接続される端末のストレージの大容量化が進んでおり、ネットワーク構造的に異なる場所にデータを保管できる効率的なネットワークストレージ環境が実現されつつある。</p> <p>一方、情報端末においては、従来のPC(Personal Computer)利用中心のシーンから、大幅な多様化が進行中である。特に、第三代携帯電話、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、RFID(Radio Frequency Identification)タグなど、比較的小型でリソースが限られた端末を利用する機会が非常に多くなりつつある。この傾向はユビキタスネットワーク社会を迎えるに当たり、さらに顕著になるものと想定される。</p> <p>このようなIT環境の進展の中で、そこでやり取りされるデータは大容量化しており、その一方でそれらのデータに対するセキュリティ(機密性、可用性、完全性など)ニーズもますます高まっている。現時点でも既に「情報漏洩」が深刻な社会問題化しており、2005年4月の個人情報保護法の施行に合せて、その技術的対策の整備が急務となっている。現状でも、暗号技術やアクセス制御技術などの情報漏洩対策のために開発・利用されている基本技術もあるが、上述したユビキタスネットワーク社会においては、さらに以下に示すような問題が挙げられる。</p> <ul style="list-style-type: none"> <li>・ 小型でリソースが限られた端末が主流となる反面、安全性の高い高度な暗号技術の実装にはより困難性が増す</li> <li>・ インターネットを介した通信以外にも、端末間の直接通信等の多様な通信経路が存在するため、従来のアクセス制御技術のような集中管理型の情報漏洩防止技術だけでは不十分である</li> <li>・ ネットワークストレージ環境が進展するのに伴い、地理的、ネットワーク構造的に異なる場所にデータが保管されるケースが一般化され、すべての情報を適切に保護することが困難となる</li> </ul> <p>上記を踏まえて、本研究の目的は、ユビキタスネットワーク社会でやり取りされる大容量データにおいて、その情報漏洩を防止するために上述の問題を解決し得る「安全な流通・保存技術」に関する検討を行うことである。</p>	

### **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
- (4)機密情報を安全、高速、低消費電力で伝送する技術
- ・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 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。

<b>対象技術</b>	その他認証技術
<b>テーマ名</b>	異なるCA間の認証ローミング技術に関する研究開発
<b>開発年度</b>	平成17年度から平成18年度までの2年間
<b>実施主体</b>	テブコシステムズ・三菱電機（情報通信研究機構(NICT)からの委託)
<b>背景、目的</b>	
<p>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主体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。</p> <p>こうした状況の中で、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、ワンストップ型認証への期待が高まっている。また、サービス主体においては、「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。</p> <p>しかしながら、ワンストップ型の認証については、BtoC EC（企業 - 消費者間電子商取引）において、多様なCAやサービス主体が連携する仕組みの構築が進んでいないのが現状である。また、現在のPKIに関しては、電子行政手続き業務やBtoB EC（企業間電子商取引）での利用が中心であり、BtoC EC（企業 - 消費者間電子商取引）に係る広範なサービスへの適用を想定した場合には、システム処理や情報端末処理等への過重な負荷が予想され、必ずしもセキュリティや利便性等の機能が十分発揮されるとは言えない状況である。</p> <p>このような点を踏まえ、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設計するとともに、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ものとする。</p> <p>さらに、匿名性や安全性、処理効率性について、当該方式を用いたときのシステム全体の最適化を図り、複数のCAを含む実環境をフィールドとして、その実効性を検証するものとする。</p> <p>注) ここでいうワンストップ型認証とは、ワンストップサービスの利用にあたって必要となる認証であり、ユーザがある1箇所のCAに認証されれば、そのCAとローミングしている別のCAへの認証が不要になるもの、CA間でユーザの匿名性が維持されるものとして定義される。（なお、本研究開発は、多様なCAで認証インフラを共有することを想定するものではなく、あくまで多様なCA間の認証ローミングを想定するものであることを付記しておく。）</p>	

### **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。

<b>対象技術</b>	認証技術等
<b>テーマ名</b>	次世代型電子認証基盤の整備
<b>開発年度</b>	平成17年度～平成18年度
<b>実施主体</b>	財団法人日本情報処理開発協会及び日本電気(株)他7社(経済産業省からの補助金)
<b>背景、目的</b>	<p>現在、多くの場合、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。</p>
<b>研究開発状況(概要)</b>	<p>平成17年度</p> <ol style="list-style-type: none"> <li>(1) 想定される各関係者の要件整理を行い、システムと機能、情報の流れと管理方法、関係者の運用と責任範囲、関係者の利益分配方法、関係者間の契約及び制度からなるビジネスモデルを策定中。また、並行して国内外の先進事例を調査中。</li> <li>(2) 米国EAP、欧州IDA他の先行プロジェクトを調査・整理し、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作成し、ポリシーガイドライン規範基準として策定中。</li> <li>(3) 技術要件を満たし、認証属性情報処理機能、アクセス制御情報処理機能を具備する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具備するポータルサーバの基盤ソフトウェアの開発とともに、評価実験を実施中。</li> </ol> <p>平成18年度</p> <ol style="list-style-type: none"> <li>(1) ビジネスモデルの改定(モデルの汎用化)</li> <li>(2) 電子認証ポリシーの規範・評価方法に関するガイドラインの策定</li> <li>(3) 基盤ソフトウェアの追加機能開発(コア技術)を行う予定。</li> </ol>
<b>詳細の入手方法(関連部署名及びその連絡先)</b>	<p>日本PKIフォーラム (<a href="http://www.japanpkiforum.jp/">http://www.japanpkiforum.jp/</a>)</p>
<b>将来の方向性</b>	<p>当事業で開発する技術基盤を採用したさまざまな企業間で認証の連携が行われることにより、新たな価値の創造、活力ある企業活動の実現が期待される。</p>

<b>対象技術</b>	認証技術
<b>テーマ名</b>	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
<b>開発年度</b>	平成17年度～平成18年度
<b>実施主体</b>	株式会社 三菱総合研究所（経済産業省からの委託）
<b>背景、目的</b>	
<p>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したり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。これまで、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。</p>	
<b>研究開発状況（概要）</b>	
<p>本研究において開発するシステムの構成は下図の通りである。</p>	
<pre> graph TD     Internet((インターネット)) --&gt; Firewall[ファイアウォール]     Firewall -- DMZネットワーク --&gt; Mail[メール送受信情報の取得管理システム]     Mail &lt;--&gt; MailDB[(送受信情報DB)]     Mail --&gt; Bot[ボット検出システム]     Bot &lt;--&gt; BotDB[(ボット特定情報DB)]     Bot --&gt; Botnet[ボットネット分析システム]     Botnet --&gt; BotDB     Botnet --&gt; SMTP[SMTPサーバ]     SMTP &lt;--&gt; Spam[スパムメール収集システム]     Spam &lt;--&gt; SpamDB[(スパムメールDB)]     Spam --&gt; Botnet   </pre>	
<b>図 1：開発成果物の構成</b>	
<p>ファイアウォールを介してインターネットから受信したメールは、SMTPの処理に依存しないようSMTPの前段で処理を行う。メール送受信情報の取得管理システムは、受信したメールから送信元IPアドレス、送信先のメールアドレス情報を取得し記録する。送受信情報は管理データ</p>	

ベースに保存する。ボット検出システムは、メール送受信情報の取得管理システムによって蓄積された情報から、ボットのIPアドレスを特定しデータベースに保存する。特定されたボット情報をもとに、スパムメール収集システムは、受信したメール全体からスパムメールを抽出し、データベースに保存する。ボットネット分析システムは、特定したボットの情報とスパムメールから、ボットネットに属すボットを特定し、ボット特定情報データベースに保存する。

### 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

Tel:03-3277-5605, Fax: 03-3277-3473

URL: <http://www.mri-security.jp/>

### 将来の方向性

平成17年度と平成18年度に、以下の技術を開発する予定である。

#### （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。

#### （3）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。

#### （4）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。

具体的には、（3）によりスパムメールと判断されたメールおよび正規のメールの文面を相互に比較し、類似度の高いメールをグループに分類する。分類されたメールの送信元を特定することで、同じボットネットの管理下にあるボットを特定することができる。

<b>対象技術</b>	その他認証技術等
<b>テーマ名</b>	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
<b>開発年度</b>	平成17年度～平成19年度
<b>実施主体</b>	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）
<b>背景、目的</b>	<p>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。</p> <p>そこで本研究開発では、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したりするための技術（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。</p>
<b>研究開発状況（概要）</b>	<p>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。</p>
<b>詳細の入手方法（関連部署名及びその連絡先）</b>	<p>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</p>
<b>将来の方向性</b>	<p>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が構築される。</p>

<b>対象技術</b>	その他認証技術等
<b>テーマ名</b>	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
<b>開発年度</b>	平成17年度～平成19年度
<b>実施主体</b>	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）
<b>背景、目的</b>	<p>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。</p> <p>そこで本研究開発では、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がデバイス等を通じて獲得されるにもかかわらず、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。</p> <p>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が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。</p>
<b>研究開発状況（概要）</b>	<p>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った。また、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。</p>
<b>詳細の入手方法（関連部署名及びその連絡先）</b>	<p>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</p>
<b>将来の方向性</b>	<p>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が構築される。</p>

<b>対象技術</b>	認証技術等
<b>テーマ名</b>	強制的アクセス制御に基づく Web サーバーに関する調査・設計
<b>開発年度</b>	平成16年度
<b>実施主体</b>	独立行政法人 情報処理推進機構
<b>背景、目的</b>	<p>近年、セキュアシステム構築のための基盤ソフトウェアとして、セキュアオペレーティング・システムに代表される強制的アクセス制御機能を有するオペレーティング・システムが注目されている。オペレーティング・システムによる強制的アクセス制御は、オペレーティング・システム上のすべてのリソースおよびアプリケーションに対してセキュリティ・ポリシーに沿ったアクセス制御を強制することができるため、インターネット Web サーバー・システムにおける効果的な改ざん防止対策としての活用が望まれている。</p> <p>インターネット環境で運用される Web サーバー・システムにおいて、オペレーティング・システムによる強制的アクセス制御を有効活用するためには、オペレーティング・システムと調和的にアクセス制御を実現する Web サーバーの実現が不可欠である。本プロジェクトは、中央省庁等で利用されるインターネット Web サーバー・システムを想定し、オペレーティング・システムによる強制的アクセス制御機構を有する Web サーバー・システムの実現を目指し、Web サーバーに適したセキュリティ・ポリシー・モデルを明らかにする。</p>
<b>研究開発状況（概要）</b>	<p>平成16年度</p> <ul style="list-style-type: none"> <li>・強制的アクセス制御を採用するセキュリティ・ポリシー・モデルを調査し、そのWebサーバーへの適用性を検証した。また、強制的アクセス制御を実現する既存Web サーバーにおいて、どのようなアクセス制御が行われているかを調査し、その問題点を検証し調査報告書としてまとめた。</li> <li>・アクセス制御に求められる要件を満たすWeb サーバー・システムの外部設計を調査報告書という形でまとめた。</li> </ul>
<b>詳細の入手方法（関連部署名及びその連絡先）</b>	<p>独立行政法人 情報処理推進機構セキュリティセンター  電話 03-5978-7508  <a href="http://www.ipa.go.jp/security/index.html">http://www.ipa.go.jp/security/index.html</a></p>
<b>将来の方向性</b>	<p>将来、電子政府で用いるWeb サーバーの開発に資する</p>

(別添2)

企業名(及び略称)	コンピュータ・アソシエイツ株式会社
代表者氏名	ジョン リューベン (John Ruthven)
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 新宿三井ビル
関連部署名及び電話番号	CAジャパンダイレクト 0120-702-600
URL	<a href="http://www.caj.co.jp/etrust/ac/">http://www.caj.co.jp/etrust/ac/</a>
対象技術	技術開発状況
その他認証技術等 (既に製品化し販売中)	eTrust Access Controlは、サーバOS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する(適切なユーザに適切な権限を与える)ことが可能。情報漏えい、改ざん、侵入、なりすましなどからOS上のリソースを保護。また正常アクセスを含む追跡可能な監査ログを取得する。“誰が”、“いつ”、“どこから”、“何を使って”、“どのリソースへ”という4W1Hに基づいたログを出力。 ログは誰にも改ざんできない仕様となっている。

企業名(及び略称)	コンピュータ・アソシエイツ株式会社
代表者氏名	ジョン リューベン (John Ruthven)
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 新宿三井ビル
関連部署名及び電話番号	CAジャパンダイレクト 0120-702-600
URL	<a href="http://www.caj.co.jp/etrust/eid/">http://www.caj.co.jp/etrust/eid/</a>
対象技術	技術開発状況
侵入検知技術 (既に製品化し販売中)	eTrust Intrusion Detectionは、対部外と対内部者の監視を実現する侵入検知製品。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、ロギングそしてこれらのリアルタイム応答機能が利用可。この単一製品で、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。

<b>企業名（及び略称）</b>	コンピュータ・アソシエイツ株式会社
<b>代表者氏名</b>	ジョン リューベン（John Ruthven）
<b>所在地（郵便番号及び住所）</b>	〒163-0439 東京都新宿区西新宿2-1-1 新宿三井ビル
<b>関連部署名及び電話番号</b>	CAジャパンダイレクト 0120-702-600
<b>URL</b>	<a href="http://www.caj.co.jp/etrust/esm/">http://www.caj.co.jp/etrust/esm/</a>
<b>対象技術</b>	<b>技術開発状況</b>
その他認証技術等 （既に製品化し販売中）	eTrust SiteMinderは、企業のWebアプリケーション向けのセキュリティ基盤および管理基盤として機能し、ユーザ認証とアクセスをきめ細かく制御します。シングルサインオン機能を提供し、シームレスなユーザ認証とアクセス制御の実現により、企業のITに関する全体的な運用コストの削減を実現します。管理対象は、社員、パートナー、サプライヤ、顧客等のあらゆるユーザに対応、重要な情報とアプリケーションを安全に提供し、ビジネスニーズの拡大にも対応可能な拡張性を備えています。  管理面では、ポリシーサーバによる一元化、エンタープライズ規模への対応、更にフェデレーション（アイデンティティ連携）にも対応し、フェデレーションサイトへのシームレスな認証を実現します。

<b>企業名（及び略称）</b>	コンピュータ・アソシエイツ株式会社
<b>代表者氏名</b>	ジョン リューベン（John Ruthven）
<b>所在地（郵便番号及び住所）</b>	〒163-0439 東京都新宿区西新宿2-1-1 新宿三井ビル
<b>関連部署名及び電話番号</b>	CAジャパンダイレクト 0120-702-600
<b>URL</b>	<a href="http://www.caj.co.jp/etrust/etm/">http://www.caj.co.jp/etrust/etm/</a>
<b>対象技術</b>	<b>技術開発状況</b>
その他認証技術等 （既に製品化し販売中）	eTrust TransactionMinder は、Web サービスへのアクセス制御を提供、Web サービスを保護、および管理するためのセキュリティソリューション。Web サービスの利用者が送信したXML メッセージ内のセキュリティ情報を認証することにより、Web サービスへのアクセスにおけるセキュリティを確保する。また、様々な方式のWeb サービスの標準に対応しており、ユーザのアイデンティティに関連づけられている一元化されたセキュリティポリシーに基づいて、認証、許可、連携サービス、セッション管理、監査を行う。  更にフェデレーション（アイデンティティ連携）にも対応し、フェデレーションサイトへのシームレスな認証を実現。

<b>企業名（及び略称）</b>		日本電気株式会社
<b>代表者氏名</b>		金杉 明信
<b>所在地（郵便番号及び住所）</b>		東京都港区芝五丁目7番1号
<b>関連部署名及び電話番号</b>		システム基盤ソフトウェア開発本部 03-3456-1097
<b>URL</b>		
<b>対象技術</b>	<b>技術開発状況</b>	
ファイアウォール技術 (2003年)	<ul style="list-style-type: none"> <li>・ 許可されていないアクセスそのものを防ぐだけでなく、不正アクセスの事前調査活動に対し検知/自動防御。</li> <li>・ NAT/NAPT対応</li> <li>・ DMZ対応</li> <li>・ 通信量制限機能</li> </ul>	

<b>企業名（及び略称）</b>		日本電気株式会社
<b>代表者氏名</b>		金杉 明信
<b>所在地（郵便番号及び住所）</b>		東京都港区芝五丁目7番1号
<b>関連部署名及び電話番号</b>		システム基盤ソフトウェア開発本部
<b>URL</b>		
<b>対象技術</b>	<b>技術開発状況</b>	
侵入検知技術 (2004年)	<ul style="list-style-type: none"> <li>・ プロセスのアクセス監視 プログラムの起動、ファイルアクセス、ネットワークアクセスの監視</li> <li>・ 複合アクセス監視 複数のアクセスの組み合わせによる不正アクセス検知</li> </ul>	

企業名（及び略称）	日本電気株式会社
代表者氏名	金杉 明信
所在地（郵便番号及び住所）	東京都港区芝五丁目7番1号
関連部署名及び電話番号	システム基盤ソフトウェア開発本部
URL	
対象技術	技術開発状況
その他認証技術等 (2004年)	<ul style="list-style-type: none"> <li>・ PKI 認証技術</li> <li>・ シングルサインオン (SAML、Liberty)</li> <li>・ 認証VLAN + PC検疫</li> </ul>

企業名（及び略称）	データ・フォアビジョン株式会社
代表者氏名	大久保 豊
所在地（郵便番号及び住所）	〒104-0045 東京都中央区築地5-6-10 浜離宮パークサイドプレイス15F
関連部署名及び電話番号	ソリューション第三本部 03-5776-8030
URL	
<a href="http://www.dfv.co.jp">http://www.dfv.co.jp</a>	
対象技術	技術開発状況
侵入検知技術	<p>ステルス・エージェントは、内部情報漏洩を防御するソリューションです。MAAT エージェント（アプライアンス製品）、コントロールセンタサーバ、ログウェアハウスサーバから構成されます。ネットワークを流れるパケットを監視することで不正アクセスの検知と遮断を実現します。セグメントに設置されているスイッチングハブにMAATエージェントを接続します。接続は、既存のネットワークに負荷をかけず、MAATエージェントに障害が発生してもネットワークに影響を与えない考慮がされています。不正アクセスとは、「公式」と明示的に登録されていないコンピュータ（*1）からのアクセスや管理者が設定したセキュリティポリシーに違反するアクセスを指します。不正アクセス判定は、パケット毎に行われます。不正アクセスに対するアクションとして以下の4つがあります。</p> <p>リセットパケット遮断・・・TCP パケットに対し、発信元及び発信先の双方にリセットパケットを送信してTCP セッションを強制的に切断します。</p> <p>ARP パケット遮断・・・公式と認められていないコンピュータに対し、偽装ARP パケットを送信し、通信を阻害します。</p> <p>ログ記録・・・パケットをログとしてデータベースに書き出します。専用のログ検索ツールにより、パケットを検索、抽出し、内容を確認することができます。フォレンジックサーバとして活用できます。</p> <p>メール通知・・・不正アクセスがあった旨を管理者にメールします。</p> <p>コントロールセンタ出力・・・管理者向けのコンソールに不正アクセスがあった旨をポップアップ・メッセージで告知します。</p> <p>（*1）非公式コンピュータの検出</p> <p>MACアドレス、IPアドレス、NetBIOS名を組み合わせで判断します。固定IPアドレス、DHCPの両方の仕組みに対応しています。</p>

(別添3)

【大学】

大学名	青山学院大学理工学部 水澤研究室
所在地(郵便番号及び住所)	299-8558 神奈川県相模原市淵辺五丁目10番1号
関連部署名及び電話番号	<a href="http://www.agnes.aoyama.ac.jp/">http://www.agnes.aoyama.ac.jp/</a>
URL	<a href="http://www.agnes.aoyama.ac.jp/">http://www.agnes.aoyama.ac.jp/</a>
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	<ul style="list-style-type: none"><li>・ネットワーク流通データの24時間連続記録</li><li>・プロトコル解析</li><li>・カスタマイズ応談</li></ul>

大学名	石巻専修大学
所在地(郵便番号及び住所)	986-8580 宮城県石巻市南塚新水戸1
関連部署名及び電話番号	理工学部情報電子工学科 0225-22-7716
URL	<a href="http://hyperion.ie.isenshu-u.ac.jp/IE_HP/">http://hyperion.ie.isenshu-u.ac.jp/IE_HP/</a>
対象技術	技術開発状況
データ	<ul style="list-style-type: none"><li>・岩手大との共同研究</li><li>・特許に基づく独自技術(暗号)</li><li>・大学のシーズを岩手県花巻市(R&amp;Dセンター)の企業が製品化</li><li>・岩手県の予算を頂いている(夢県土いわて戦略的研究推進事業)</li></ul>

大学名	岡山大学大学院 自然科学研究科分散システム構成学研究室
所在地(郵便番号及び住所)	700-8530 岡山県岡山市津島中3-1-1
関連部署名及び電話番号	086-251-8147
URL	<a href="http://www.sec.cne.okayama-u.ac.jp/">http://www.sec.cne.okayama-u.ac.jp/</a>
対象技術	技術開発状況
データ	OS(Linux)の変更が不要。データおよびファイル情報の暗号化 通常のファイルシステムでは検知しない

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 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	<a href="http://www.media.hiroshima-u.ac.jp/">http://www.media.hiroshima-u.ac.jp/</a>		
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 アイアイジェイテクノロジー	
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1-105 神保町三井ビルディング	
関連部署名及び電話番号 技術開発部 セキュリティコンサルティンググループ 03-5205-6700	
URL <a href="http://www.iij-tech.co.jp/index.html">http://www.iij-tech.co.jp/index.html</a>	
対象技術	技術開発状況
その他	ネットワーク脆弱性検査サービス。インターネット/オンサイト対応可能。複数のツールを使用。脆弱性による影響の明確化が可能。専門エンジニアによる高品質な作業。NRIセキュア社との協業。事前ヒアリング、検査、説明会を行う

企業名（及び略称） 株式会社 アイアイジェイテクノロジー	
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1-105 神保町三井ビルディング	
関連部署名及び電話番号 技術開発部 セキュリティコンサルティンググループ 03-5205-6700	
URL <a href="http://www.iij-tech.co.jp/index.html">http://www.iij-tech.co.jp/index.html</a>	
対象技術	技術開発状況
その他	webアプリケーション脆弱性検査サービス。インターネット/オンサイト対応可能、NRIセキュア社との協業。脆弱性による影響の明確化が可能。専門エンジニアによる高品質な作業。事前ヒアリング、検査、説明会を行う

企業名（及び略称） 株式会社 アイアイジェイテクノロジー	
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1-105 神保町三井ビルディング	
関連部署名及び電話番号 技術開発部 セキュリティコンサルティンググループ 03-5205-6700	
URL <a href="http://www.iij-tech.co.jp/index.html">http://www.iij-tech.co.jp/index.html</a>	
対象技術	技術開発状況
その他	データベースに特化したセキュリティ検査サービス。オンサイトでの対応。IPLocks社のツールを利用。データベースセキュリティ専門エンジニアによる高品質な作業。事前ヒアリング、検査、説明会を行う

企業名（及び略称） 株式会社 アズジェント	
所在地（郵便番号及び住所）103-0016 東京都中央区日本橋小網町19-7	
関連部署名及び電話番号 技術本部 03-5643-2590	
URL <a href="http://www.asgent.co.jp/">http://www.asgent.co.jp/</a>	
対象技術	技術開発状況
その他	M@gic PolicyシリーズにはCoSMOとQUICKがある。CoSMOは入力された情報資産の特徴から、リスクアセスメントの評価を脅威 - 脆弱性の一覧を提示させることで、支援したり評価後の矛盾点などを分析する。QUICKは選定された規定等通りに運用されているかを運用チェック項目に入力させ、部門単位等で現状分析を行うためのツール。

企業名（及び略称） 株式会社 アニモ	
所在地（郵便番号及び住所）231-0015 神奈川県横浜市中区尾上町2-27 朝日生命横浜関内ビル4 F	
関連部署名及び電話番号 ソフトウェア開発本部 045-663-8640	
URL <a href="http://www.animo.co.jp/">http://www.animo.co.jp/</a>	
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	<p>バイOMETRICS技術の一つとして、音声による本人認証を実現した音声認証エンジンです。本製品は、キーワード方式（登録時にフレーズを決めて、同じフレーズで音声認証を行う）を提供しています。</p> <p>本製品の特徴は以下の通りです。</p> <ul style="list-style-type: none"> <li>・本人確認処理が高速(0.2秒)</li> <li>・電話サービス等での利便性を確保した本人確認を実現可能</li> <li>・非接触タイプなので、心理的負担が少ない</li> <li>・特別な入力デバイスを必要としない（マイクまたは電話機）</li> <li>・言語非依存なので、グローバルに利用可能</li> </ul> <p>また、T-Engine向けのeTRON認証カードへの音声認証機能の組み込みを大日本印刷様と開発しており、PDA等への組み込み実績もあり、非常にコンパクトなエンジンを提供可能です。</p>

企業名（及び略称） 株式会社 アニモ	
所在地（郵便番号及び住所）231-0015 神奈川県横浜市中区尾上町2-27 朝日生命横浜関内ビル4 F	
関連部署名及び電話番号 ソフトウェア開発本部 045-663-8640	
URL <a href="http://www.animo.co.jp/">http://www.animo.co.jp/</a>	
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	<p>バイOMETRICS技術のひとつとして、音声による本人認証を実現した音声認証・識別エンジンです。本製品は、フリーワード方式（登録時及び認証時に自由な発話から音声認証を行う）を提供しています。</p> <p>本製品の特徴は以下の通りです。</p> <ul style="list-style-type: none"> <li>・10秒程度の発話により、認証・識別を行う</li> <li>・電話サービス等での自然な会話の中で本人確認を実現可</li> <li>・キーワード方式との併用で高認証率を達成（実質的に100%）</li> </ul> <p>また、本人確認とは別分野として、通話中の話者を検索する・デジタルコンテンツでの話者検索手段としての利用実績もあります。当社は、学会、雑誌でのバイOMETRICSの場では、常に音声認証ベンダーとして参画しており、複数の県警殿から話者検索のデモを要請されております。</p>

企業名（及び略称） 株式会社 アニモ	
所在地（郵便番号及び住所）231-0015 神奈川県横浜市中区尾上町2-27 朝日生命横浜関内ビル4 F	
関連部署名及び電話番号 ソフトウェア開発本部 045-663-8640	
U R L <a href="http://www.animo.co.jp/">http://www.animo.co.jp/</a>	
対象技術	技術開発状況
通信情報	<p>「VoiceTracking」は従来の全通話録音装置（大型、蓄積目的）ではなく、クライアント型の通話録音・検索・事後活用型のソフトウェアです。</p> <p>本製品の特徴は以下の通りです。</p> <ul style="list-style-type: none"> <li>・交換機に依存せずに、電話接続器により一台からの通話録音が可能</li> <li>・通話録音データに「しおり」（タグ）を付加することにより、効率的な頭出し再生が可能</li> <li>・話速変換技術により、0.5倍速（遅聞き）～3.0倍速（早聞き）が可能</li> <li>・独自の圧縮技術により、データ流出時においても再生不可</li> <li>・通話データの検索（日時、対応者、タグ）機能により、事後の管理が容易</li> </ul> <p>最近のセキュリティでの問題点としてソーシャルエンジニアリングによって人間系からの情報漏洩がウィークポイントとなる場合があります。VoiceTrackingでは、通話を録音することにより、情報漏洩の大きな通り道である通話を監視・管理することができます。</p>

企業名（及び略称） 株式会社 アラジンジャパン	
所在地（郵便番号及び住所）192-0081 東京都八王子市横山町6-9 丸多屋ビル	
関連部署名及び電話番号 インターネットセキュリティ・グループ 0426-60-7191	
U R L <a href="http://www.aladdin.co.jp">http://www.aladdin.co.jp</a>	
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	<ul style="list-style-type: none"> <li>・PKI（デジタル証明書、秘密カギ）、非PKI（ID,パスワード）で使う認証情報を格納し、内部で処理するUSBデバイス</li> <li>・大規模ユーザに於けるトークンマネージメント・システムの提供</li> <li>・FIPS140-1Le2&amp;3, I7SEC LE4設定品</li> </ul>

企業名（及び略称） 株式会社 アラジンジャパン	
所在地（郵便番号及び住所）192-0081 東京都八王子市横山町6-9 丸多屋ビル	
関連部署名及び電話番号 インターネットセキュリティ・グループ 0426-60-7191	
U R L <a href="http://www.aladdin.co.jp">http://www.aladdin.co.jp</a>	
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	<ul style="list-style-type: none"> <li>・未知ウイルスの検出</li> <li>・スパムメール対策</li> <li>・スパイウェア対策</li> </ul> <p>上記3つをゲートウェイで一括して実施できるコンテンツセキュリティウィルス対策製品</p>

企業名（及び略称） 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 東京銀行協会ビルディング13F	
関連部署名及び電話番号 総務 03-5222-5200	
U R L <a href="http://www.rsasecurity.co.jp/">http://www.rsasecurity.co.jp/</a>	
対象技術	技術開発状況
クライアント	一分間隔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交を依頼し、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。

企業名（及び略称） 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 東京銀行協会ビルディング13F	
関連部署名及び電話番号 総務 03-5222-5200	
U R L <a href="http://www.rsasecurity.co.jp/">http://www.rsasecurity.co.jp/</a>	
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	<ul style="list-style-type: none"> <li>・ 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、電子証明、ワンタイムパスワード等を使用可能。</li> <li>・ 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。</li> <li>・ 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。</li> </ul>

企業名（及び略称） 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 東京銀行協会ビルディング13F	
関連部署名及び電話番号 総務 03-5222-5200	
U R L <a href="http://www.rsasecurity.co.jp/">http://www.rsasecurity.co.jp/</a>	
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上から一旦ICカード等で認証されれば、事前に登録されたIDやパスワードが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無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回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） 株式会社 インサイトテクノロジー	
所在地（郵便番号及び住所） 253-0041 神奈川県茅ヶ崎市茅ヶ崎2-1-52 6F	
関連部署名及び電話番号 0467-59-1527	
U R L <a href="http://www.insight-tec.com/">http://www.insight-tec.com/</a>	
対象技術	技術開発状況
データ	<p>概要：</p> <p>監視証跡となるデータベースアクセスの記録・警告・追跡調査を可能にする情報漏洩監視システムです。</p> <p>特徴：</p> <ul style="list-style-type: none"> <li>・パフォーマンスを劣化させずにSQLを記録</li> <li>・「いつ、誰が、何を行った」の操作履歴を記録</li> <li>・情報資産を機密レベル毎に管理し、不正なアクセスを警告</li> <li>・監査証跡となるアクセスログを専用サーバに安全保管</li> <li>・アクセスログは簡単・高速に条件抽出し、迅速に調査、原因特定が可能。</li> </ul>

企業名（及び略称） 株式会社 エイチ・エム・アイ	
所在地（郵便番号及び住所） 550-0014 大阪府大阪市西区北堀江1-5-2 四ッ橋新興産ビル1 1 F	
関連部署名及び電話番号 管理部 06-6110-2551	
U R L <a href="http://www.hmi-jp.com/">http://www.hmi-jp.com/</a>	
対象技術	技術開発状況
サーバ クライアント	<p>USBキーを利用してクライアントPCのアクセス制御を行い、更に真性乱数を利用したランダムパスワードで認証システムの強化。</p>

企業名（及び略称） NECネクソ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 生産技術部 03-5730-5202	
U R L <a href="http://www.nec-nexs.com/">http://www.nec-nexs.com/</a>	
対象技術	技術開発状況
サーバ	<p>Webサーバ搭載型のアクセス制御・改ざん検知、復旧・ログ解析ツール。主な機能は以下のとおり。</p> <ul style="list-style-type: none"> <li>・アクセス解析と不正アクセスのブロック</li> <li>・WEBサーバ内コンテンツの改ざん検知とサービスの停止・復旧</li> <li>・WEBサーバ、FTPサーバのユーザ権限認定の検証</li> <li>・ログの走査と特異点の抽出</li> <li>・パッチの自動更新</li> </ul>

企業名（及び略称） NTTコムウェア株式会社	
所在地（郵便番号及び住所） 108-8019 東京都港区港南1-9-1 NTT品川TWINSアネックス	
関連部署名及び電話番号 広報室	
URL <a href="http://www.nttcom.co.jp/">http://www.nttcom.co.jp/</a>	
対象技術	技術開発状況
サーバ 通信情報 データ	オープンソースソフトウェアを用いシングルサインオンを実現している為、ソフトウェアのイニシャルコストを抑えることができる。社内技術者による内製パッケージであり、迅速なトラブル対応、柔軟なカスタマイズ対応が可能。Linuxで動作する為、ハードウェアコストを抑える事ができる

企業名（及び略称） NTTコムウェア株式会社	
所在地（郵便番号及び住所） 108-8019 東京都港区港南1-9-1 NTT品川TWINSアネックス	
関連部署名及び電話番号 広報室	
URL <a href="http://www.nttcom.co.jp/">http://www.nttcom.co.jp/</a>	
対象技術	技術開発状況
サーバ	<p>LinuxOSをベースに、機能とアプリケーションを限定し、ソフトウェア群を搭載したUSB型メモリデバイス。「USB型」と「HD型」の2つのタイプがあり、使用するシチュエーションに応じて使い分けます。</p> <p>既存PCの活用（USB型）：既存PCに本製品を取付、補助用起動CDによるUSB起動でシンクライアント環境を実現。</p> <p>既存PCの活用（HD型）：既存PCのハードディスクに搭載している既存OSを全て削除し、USBスティックに搭載されたOS起動イメージをHDにインストールして、HDから起動し、シンクライアント環境を実現。</p> <p>デバイス遮断：シンクライアント状態にある既存PCは、PC内のハードディスクやCD-R等の外部記憶装置へのアクセスをOSレベルで禁止しています。</p> <p>セキュアな端末環境：万が一ウイルスがクライアント端末に侵入したとしても、デバイス等へのアクセスが禁止されているので、OSが改ざん・改版される事はありません。再起動すれば全てが元の初期状態に戻ります。</p>

企業名（及び略称） NTTコムウェア株式会社	
所在地（郵便番号及び住所） 108-8019 東京都港区港南1-9-1 NTT品川TWINSアネックス	
関連部署名及び電話番号 広報室	
URL <a href="http://www.nttcom.co.jp/">http://www.nttcom.co.jp/</a>	
対象技術	技術開発状況
サーバ クライアント	AdminITyは、ネットワーク上の機器情報を自動的に収集する事で、社内の資産やライセンス、セキュリティレベルをトータルに管理できるソフトウェアです。NTTコムウェアの検証の元にご提供するセキュリティ辞典を用いて、社内端末にセキュリティレベルを簡単に把握する事が可能です。PC利用者のモラル向上を図る警告メール送付機能や、PCにパッチなどを強制的にインストールするソフト配布機能を装備し、セキュリティ対策の打ち手を強力にサポートします。2005年11月より、セキュリティポリシーを設定するだけで端末が自動スキャンを実行し、ポリシー違反を識別。違反端末には警告表示や強制シャットダウンまで実行できる機能が追加されました

企業名（及び略称） NTTコムウェア株式会社	
所在地（郵便番号及び住所）108-8019 東京都港区港南1-9-1 NTT品川TWINSアネックス	
関連部署名及び電話番号 広報室	
U R L <a href="http://www.nttcom.co.jp/">http://www.nttcom.co.jp/</a>	
対象技術	技術開発状況
サーバ クライアント データ	<p>大切な情報資産を暗号化し保存できます。情報漏洩を防止する簡単で安心なセキュリティ製品です。</p> <p>Terminal Protect（端末保護）：豊富な種類のファイルを暗号化でき、持ち出しファイルやPC盗難等、不慮の流出による情報漏洩を防止します。本システムはサーバや個別のユーザ管理の手間など導入前後の管理作業を行うことなく、PCにインストールするだけの安全簡単なシステムです。</p> <p>Enterprise（共有情報保護）：悪意のあるものや不注意による組織内部からの情報漏洩を防止します。本システムを導入すれば多種類のファイルを暗号化し、また閲覧のみ等の利用制限をユーザやグループ毎に設定が可能となり、NW越しの情報漏洩を強力に防止します</p>

企業名（及び略称） NTTコムウェア株式会社	
所在地（郵便番号及び住所）108-8019 東京都港区港南1-9-1 NTT品川TWINSアネックス	
関連部署名及び電話番号 広報室	
U R L <a href="http://www.nttcom.co.jp/">http://www.nttcom.co.jp/</a>	
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	<p>多機能USBキーSecure Stickを携帯するだけで、簡単に、高いセキュリティ性を保って、どこからでもWEBアプリケーションをご利用頂けます。「通信経路」だけでなく、「利用ファイル」・「ブラウジング」・「アクセスログ」など、リモートアクセス環境における全ての作業にセキュリティを確保しました。NTTコムウェアによる「認証システムの運用・監視」、「管理者へのサポート」、「ハウジングやヘルプデスク運用」の代行も可能。お客様の本業へのリソース集中をお手伝いします。</p>

企業名（及び略称） NTTコムウェア株式会社	
所在地（郵便番号及び住所）108-8019 東京都港区港南1-9-1 NTT品川TWINSアネックス	
関連部署名及び電話番号 広報室	
U R L <a href="http://www.nttcom.co.jp/">http://www.nttcom.co.jp/</a>	
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	<p>セキュリティ診断サービスは、長年大規模ネットワークの構築に携わってきたNTTコムウェア独自のノウハウを用いて、ネットワークの安全性を第三者の立場から客観的に診断するサービスです。セキュリティ診断サービスは、お客様のネットワーク環境に応じて、社外向けに公開しているサーバを診断する「インターネット診断」、社内LANに接続されているサーバを診断する「内部診断」、電話回線を収容するサーバーへの不正侵入可否を診断する「ダイヤルゲート診断」の3つの基本メニューをご用意し、お客様のネットワークセキュリティを総合的にチェックする事が可能です。さらに、2005年度より追加オプションとしてWEBアプリケーション診断を開始いたしました。これにより、4月に施行されました『個人情報保護法』を意識した強力な監査が可能です</p>

企業名（及び略称） NTTコムウェア株式会社	
所在地（郵便番号及び住所） 108-8019 東京都港区港南1-9-1 NTT品川TWINSアネックス	
関連部署名及び電話番号 広報室	
URL <a href="http://www.nttcom.co.jp/">http://www.nttcom.co.jp/</a>	
対象技術	技術開発状況
ネットワーク サーバ データ	NTTコムウェアのご提供する「ネットワークセキュリティ監視サービス」は、お客様のネットワーク及びサーバにIDS(Intrusion Detection System：不正侵入検知システム)センサまたは、IPS(Intrusion Protection System：侵入防御システム)を配置して、弊社側の監視センターから遠隔にて24時間365日体制で不正アクセスの監視を行うサービスです。不正アクセスの可能性がある場合は、遠隔にて可能な対策を講じると共に、お客様システム担当者への連絡、適切な対処方法のアドバイスを行います。お客様はセキュリティ対策に係わる膨大な時間を削減できるだけでなく、不正アクセスの脅威から大切な情報資産を防御でき、安心して本来業務に専念できます

企業名（及び略称） 株式会社 NTTデータ	
所在地（郵便番号及び住所） 135-6033 東京都江東区豊洲3-3-3 豊洲センタービル	
関連部署名及び電話番号 技術開発本部 03-3523-8060	
URL <a href="http://www.nttdata.co.jp/">http://www.nttdata.co.jp/</a>	
対象技術	技術開発状況
ネットワーク クライアント	<p>【ワーム検疫・駆除】クライアントに特別なソフトウェアをインストールする必要なしに、接続PCのワーム感染をチェック。ワームに感染していた場合には駆除を実施。</p> <p>【ワーム感染防御】接続PCのパッチの適用状況をチェックし、脆弱性が存在した場合は、ネットワーク側で保護しながらイントラネットに接続。</p> <p>【ワーム検知・隔離】万が一、ワームがイントラネットに侵入してしまった場合は、ワームセンサがワーム感染活動を検知し、ワーム感染PCを自動隔離</p>

企業名（及び略称） エムオーテックス株式会社	
所在地（郵便番号及び住所） 564-0062 大阪府吹田市垂水町3丁目23-25号 エムオーテックス江坂ビル	
関連部署名及び電話番号 経営企画部 06-4861-8985	
URL <a href="http://www.motex.co.jp/">http://www.motex.co.jp/</a>	
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 その他	<ul style="list-style-type: none"> <li>・ネットワークセキュリティを数値でサポートする</li> <li>・経営者が自社のネットワーク、人の問題に気づき、対策を打てるシステム</li> <li>・人の操作とファイルの動きをログ化し、追跡できる検索システムで情報漏洩経路を特定する。また、全てのログをとることで問題行動を未然に防ぐ。</li> <li>・クライアントインストール型のネットワークマネジメントシステム</li> </ul>

企業名（及び略称） エムオーテックス株式会社	
所在地（郵便番号及び住所）564-0062 大阪府吹田市垂水町3丁目23-25号 エムオーテックス江坂ビル	
関連部署名及び電話番号 経営企画部 06-4861-8985	
URL <a href="http://www.motex.co.jp/">http://www.motex.co.jp/</a>	
対象技術	技術開発状況
通信情報 データ その他	社外から出るメールを監査し、使用状況の全てをログ化し把握する事で、傾向や問題行動をレポートするシステム。 情報漏洩を未然に防ぐ為、キーワードに接触するメールを抑止することも可能。

企業名（及び略称） エムオーテックス株式会社	
所在地（郵便番号及び住所）564-0062 大阪府吹田市垂水町3丁目23-25号 エムオーテックス江坂ビル	
関連部署名及び電話番号 経営企画部 06-4861-8985	
URL <a href="http://www.motex.co.jp/">http://www.motex.co.jp/</a>	
対象技術	技術開発状況
クライアント	<ul style="list-style-type: none"> <li>・1人から始められるネットワーク管理システム</li> <li>・業務の予定と結果を管理し、自分のPCの操作ログを照らし合わせることで、目標達成などに導く。</li> <li>・部下の操作ログなどから、情報漏洩を未然に防ぐマネージメントを可能にする。</li> <li>・社員1人1人がPCやネットワーク資源のコスト意識をもって業務に取り込み、モラル向上につながる。</li> </ul>

企業名（及び略称） エムオーテックス株式会社	
所在地（郵便番号及び住所）564-0062 大阪府吹田市垂水町3丁目23-25号 エムオーテックス江坂ビル	
関連部署名及び電話番号 経営企画部 06-4861-8985	
URL <a href="http://www.motex.co.jp/">http://www.motex.co.jp/</a>	
対象技術	技術開発状況
サーバ	WEBサイトの改ざん自動修復システム クラッカーの攻撃によって改ざんされたWEBページを「書き換えられたら瞬時に本来のデータに書き戻す」という新しい視点から開発されたシステム

企業名（及び略称） 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	
関連部署名及び電話番号 マーケティング部 03-5211-8900	
U R L <a href="http://japan.entrust.com/">http://japan.entrust.com/</a>	
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	Entrust AuthorityはPKIによるセキュリティインフラの核となる認証機関の信頼性を高める管理機能コンポーネント群です。

企業名（及び略称） 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	
関連部署名及び電話番号 マーケティング部 03-5211-8900	
U R L <a href="http://japan.entrust.com/">http://japan.entrust.com/</a>	
対象技術	技術開発状況
クライアント データ	Entrust Entelligence製品群では企業内の様々なアプリケーションに対する総合セキュリティソリューションをシングルポイントで提供でき、強力な認証、デジタル署名、暗号化を実現できます。

企業名（及び略称） 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	
関連部署名及び電話番号 マーケティング部 03-5211-8900	
U R L <a href="http://japan.entrust.com/">http://japan.entrust.com/</a>	
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	Entrust TruePassはデジタル証明書とJAVAアプレッドを利用することにより、HTMLページWebフォームに入力されたデータの永続的な暗号化、デジタル署名を実現するソフトウェアです・

企業名（及び略称） 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	
関連部署名及び電話番号 マーケティング部 03-5211-8900	
U R L <a href="http://japan.entrust.com/">http://japan.entrust.com/</a>	
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	GetAccessは複数のWebサイトに分散する認証システムを統合し、アクセス権限を集中的に管理するソフトウェアです。

企業名（及び略称） 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	
関連部署名及び電話番号 マーケティング部 03-5211-8900	
U R L <a href="http://japan.entrust.com/">http://japan.entrust.com/</a>	
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	Entrust Identity Guardは、二要素認証技術により、VPNリモートアクセス、Windowsドメイン、WEBシステムのログイン認証を強化するソフトウェアです。

企業名（及び略称） 株式会社 大塚商会	
所在地（郵便番号及び住所） 102-8573 東京都千代田区飯田橋2-18-4	
関連部署名及び電話番号 テクニカルプロモーション部 OSMグループ 03-3514-7568	
U R L <a href="http://it.e-otsuka.com/osm">http://it.e-otsuka.com/osm</a>	
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	ファイアウォール機器のレンタル 24h365d監視システム リモートメンテナンス（設定変更、Ver Up） オンサイト保守 ログレポートサービス

企業名（及び略称） オムロン株式会社	
所在地（郵便番号及び住所） 600-8530 京都府京都市下京区塩小路通堀川東入	
関連部署名及び電話番号 経営総務室秘書部 075-344-7000	
U R L <a href="http://www.omron.co.jp">http://www.omron.co.jp</a>	
対象技術	技術開発状況
施設	大人数をすばやくチェックできるセキュリティゲート。入退場の情報を非接触カード、顔認識により入手し、管理・チェックし、不正な入退場の管理、入退場情報の履歴記録を行う。

企業名（及び略称） オムロン株式会社	
所在地（郵便番号及び住所） 600-8530 京都府京都市下京区塩小路通堀川東入	
関連部署名及び電話番号 経営総務室秘書部 075-344-7000	
U R L <a href="http://www.omron.co.jp">http://www.omron.co.jp</a>	
対象技術	技術開発状況
ネットワーク クライアント 通信情報 データ	携帯電話と持ち主間のセキュリティを実現。予め携帯電話のカメラ機能を用いて撮影した持ち主の顔画像を登録し、使用する際に撮影した使用者の顔画像と比較することで、登録者認証を行う。登録者と認証した場合にロックが解除され、使用が可能となる。

企業名（及び略称） 音響署名株式会社	
所在地（郵便番号及び住所） 603-8144 京都府京都市北区小山東花池町24-10	
関連部署名及び電話番号 075-441-5908	
U R L <a href="http://ONKYO-SHOMEI.COM">http://ONKYO-SHOMEI.COM</a>	
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	nCryptone社が開発し特許を所有しているユニークな署名技術を利用した音響署名カードは使用毎に異なる電子音響署名を発信するので、高いセキュリティが保証されます。電話による取引もインターネット同様の本人認証が行えます。

企業名（及び略称） グローバルセキュリティエキスパート株式会社	
所在地（郵便番号及び住所）102-0083 東京都千代田区麹町5-4 KY麹町ビル7F	
関連部署名及び電話番号 ソリューション事業部 03-5211-7731	
U R L <a href="http://www.glbex.com/">http://www.glbex.com/</a>	
対象技術	技術開発状況
その他	ネットワーク内部あるいは外部から、お客様にとって重要な電子的情報リソース（OS、アプリケーション、データベース、ウェブサイト等）に対してハッカーと同じ視点に立ち、疑似侵入を試み、ネットワークやサーバ等の脆弱な点を洗い出して問題点を指摘する診断サービスを行っています。このサービスの中でOSやアプリケーションに備わっているアクセス制御機能が有効に機能しているかチェックを行っています。

企業名（及び略称） グローバルセキュリティエキスパート株式会社	
所在地（郵便番号及び住所）102-0083 東京都千代田区麹町5-4 KY麹町ビル7F	
関連部署名及び電話番号 ソリューション事業部 03-5211-7731	
U R L <a href="http://www.glbex.com/">http://www.glbex.com/</a>	
対象技術	技術開発状況
その他	企業や組織が成長してその構成が複雑になると、認証システムも複雑になりがちです。システム管理の側では管理作業が煩雑になったり、システム間の連携に問題が起こり、作業が手作業になったりします。一方利用者側では複数のIDとパスワードの管理を余儀なくされたりします。当社のアイデンティティ・マネジメントシステム構築サービスでは、単独あるいは複数の製品をシステムに導入し、利用者の個人属性情報の一貫した管理を実現させ、利用者の認証方法の一元化等を実現します。

企業名（及び略称） シーア・インサイト・セキュリティ株式会社	
所在地（郵便番号及び住所）108-0023 東京都港区芝浦3-14-8 芝浦ワンハンドレットビル3F	
関連部署名及び電話番号 経営企画	
U R L <a href="http://www.seerinsight.co.jp/">http://www.seerinsight.co.jp/</a>	
対象技術	技術開発状況
データ	クライアントPCで行われた操作をWindowsやパケット情報から取得し、ログとして保管する。 取得したログの検索やレポートの作成を行うことが出来る。

企業名（及び略称） シーア・インサイト・セキュリティ株式会社	
所在地（郵便番号及び住所）108-0023 東京都港区芝浦3-14-8 芝浦ワンハンドレットビル3F	
関連部署名及び電話番号 経営企画	
URL <a href="http://www.seerinsight.co.jp/">http://www.seerinsight.co.jp/</a>	
対象技術	技術開発状況
データ	サーバのsyslogやイベントを監視し、ログの削除、改ざんから保護、検知、通知、自動修復を行う。

企業名（及び略称） 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 アレトウーサ渋谷ビル	
関連部署名及び電話番号 プロダクツ販売事業部 03-3463-5633	
URL <a href="http://www.cseltd.co.jp/">http://www.cseltd.co.jp/</a>	
対象技術	技術開発状況
ネットワーク サーバ データ	「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します。 WEBブラウザを使用するため 端末の種類や社内外を問わずに利用できる ユーザへの機器やソフトの配布が不要という特徴があります。「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します。 WEBブラウザを使用するため 端末の種類や社内外を問わずに利用できる ユーザへの機器やソフトの配布が不要という特徴があります。

企業名（及び略称） 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	
関連部署名及び電話番号 経営企画室 03-5447-2551	
URL <a href="http://c4t.jp">http://c4t.jp</a>	
対象技術	技術開発状況
通信情報 データ	「TAS」は秘密分散法を用いたセキュリティ・モジュールです。秘密分散法は秘密情報を分散化し、意味のない分散情報（シェア）にして、セキュリティを高める方法です。個々のシェアからは元の情報を一切類推できませんので、情報漏洩防止等を実現できます。また、元の秘密情報に復元するにはあらかじめ設定した個数のシェアを集めればよいので、万が一の紛失や盗難、破壊の際のデータ復旧も可能です。簡易な認証スキームへの応用も可能です。従来の手法よりもシェアのデータ量を軽減できる「 $(k,L,n)$ しきい値秘密分散法」を採用している為、より利用しやすくなっています。

企業名（及び略称） 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	
関連部署名及び電話番号 経営企画室 03-5447-2551	
URL <a href="http://c4t.jp">http://c4t.jp</a>	
対象技術	技術開発状況
クライアント 通信情報 データ	Windows対応の情報漏洩対策ソフトウェアです。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す。 「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ます。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ます。

企業名（及び略称） 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	
関連部署名及び電話番号 経営企画室 03-5447-2551	
URL <a href="http://c4t.jp">http://c4t.jp</a>	
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	「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す。 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ます。 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ます。

企業名（及び略称） ジャパンネット株式会社	
所在地（郵便番号及び住所） 102-0083 東京都千代田区麹町1-4-4	
関連部署名及び電話番号 技術部 03-3265-9254	
URL <a href="http://www.japannet.jp/">http://www.japannet.jp/</a>	
対象技術	技術開発状況
サーバ 通信情報 データ	登記CAシステムを使用した電子証明書発行サービス。 一枚ずつの販売 / CA毎の運用サービスがあり。

企業名（及び略称） 株式会社 ソフテック	
所在地（郵便番号及び住所） 154-0004 東京都世田谷区太子堂1-12-39 三軒茶屋堀商ビル	
関連部署名及び電話番号 技術統括部 03-3412-6008	
U R L <a href="http://www.softek.co.jp/">http://www.softek.co.jp/</a>	
対象技術	技術開発状況
サーバ 通信情報 データ	<p>「Web Probe」はWebアプリケーションにおけるセッション管理の脆弱性に特化した検査ツールである。</p> <p>「Web Probe」では特定の脆弱性情報に対応した診断を行うのではなく、一般的なセッション管理の脆弱性となることの多い検査項目について、Webブラウザと診断対象のWebサーバとのやり取りの記録、解析により診断を行う。</p>

企業名（及び略称） 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	
関連部署名及び電話番号 ソリューション営業部 03-3486-9272	
U R L <a href="http://www.softcreate.co.jp/">http://www.softcreate.co.jp/</a>	
対象技術	技術開発状況
ネットワーク	<p>既存のネットワークに繋ぐだけで不正PC・持ち込みPCがネットワークにつながるのを防止します。</p> <p>ARP Cache Poisoningを利用しています。</p>

企業名（及び略称） TIS株式会社	
所在地（郵便番号及び住所） 105-8624 東京都港区海岸1-14-5 TIS竹芝ビル	
関連部署名及び電話番号 グループサービスセンター 03-5402-2112	
U R L	
対象技術	技術開発状況
その他	<p>高度な専門的技術を有したセキュリティエキスパート・監査士によるセキュリティ脆弱性診断を中心としたトータルセキュリティサービス</p>

企業名（及び略称） 東芝情報機器株式会社	
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
サーバ	インターネットビジネスを安全・確実に立ち上げる為に、あらゆる攻撃からWEBサーバを守る、最適のアプライアンスサーバ。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ます。

企業名（及び略称） トーメンサイバービジネス株式会社	
所在地（郵便番号及び住所） 108-0075 東京都港区南2丁目11番19号 大滝ビル	
関連部署名及び電話番号 管理本部03-5715-0620	
URL <a href="http://www.tomen-g.co.jp">http://www.tomen-g.co.jp</a>	
対象技術	技術開発状況
サーバ クライアント 通信情報	自社のメールサーバの前段に設置し、スパムメールの侵入を未然に防ぐ装置。独自のスパム判定アルゴリズムにより高い検知率を保つ。ウイルスチェック機能もあり。

企業名（及び略称） トーメンサイバービジネス株式会社	
所在地（郵便番号及び住所） 108-0075 東京都港区南2丁目11番19号 大滝ビル	
関連部署名及び電話番号 管理本部03-5715-0620	
URL <a href="http://www.tomen-g.co.jp">http://www.tomen-g.co.jp</a>	
対象技術	技術開発状況
情報通信	ソフトウェアベースのSSL VPNです。他のSSL VPNとは異なる次のような特徴を持っています。 1. ハイスループット・ハイパフォーマンス：SSL VPNゲートウェイを通して、ほぼWi respeedのスループットを実現します。 2. 全てのアプリケーションが使用可能：SSL VPNを利用することによるアプリケーションの使用制限はありません。 3. 格段のコストパフォーマンス

企業名（及び略称） トーメンサイバービジネス株式会社	
所在地（郵便番号及び住所）108-0075 東京都港区南2丁目11番19号 大滝ビル	
関連部署名及び電話番号 管理本部03-5715-0620	
U R L <a href="http://www.tomen-g.co.jp">http://www.tomen-g.co.jp</a>	
対象技術	技術開発状況
通信情報	ビデオ会議をFirewall/NATの配下にあるPCやビデオ会議専用端末から行うことができます。 回線を流れる音声・ビデオ・ドキュメントデータはAESにより暗号化することができます。

企業名（及び略称） 日本サイバーサイン株式会社	
所在地（郵便番号及び住所）102-0072 東京都千代田区飯田橋4-2-1 岩見ビル	
関連部署名及び電話番号 営業本部 03-6825-7099	
U R L <a href="http://www.cybersign.co.jp/">http://www.cybersign.co.jp/</a>	
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ます。 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にログインできます。 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ます。

企業名（及び略称） 日本サイバーサイン株式会社	
所在地（郵便番号及び住所）102-0072 東京都千代田区飯田橋4-2-1 岩見ビル	
関連部署名及び電話番号 営業本部 03-6825-7099	
U R L <a href="http://www.cybersign.co.jp/">http://www.cybersign.co.jp/</a>	
対象技術	技術開発状況
その他	バイオメトリクスオンラインサイン照合エンジンです。開発パートナーは、このサイン照合エンジンを利用して、認証が必要なアプリケーションを開発する事が出来ます。

企業名（及び略称） 日本サイバーサイン株式会社	
所在地（郵便番号及び住所）102-0072 東京都千代田区飯田橋4-2-1 岩見ビル	
関連部署名及び電話番号 営業本部 03-6825-7099	
U R L <a href="http://www.cybersign.co.jp/">http://www.cybersign.co.jp/</a>	
対象技術	技術開発状況
その他	バイOMETRICSオンライン照合機能をサービスするサイン認証サーバです。サイン認証を必要とするアプリケーションは当サーバに入力したサインを通知することで、予め登録されたサインと照合してその結果を知ることができます。

企業名（及び略称） 日本サイバーサイン株式会社	
所在地（郵便番号及び住所）102-0072 東京都千代田区飯田橋4-2-1 岩見ビル	
関連部署名及び電話番号 営業本部 03-6825-7099	
U R L <a href="http://www.cybersign.co.jp/">http://www.cybersign.co.jp/</a>	
対象技術	技術開発状況
クライアント	Pocket PCやZaurusのパスワードオン時にサイン照合を行うことにより、使用者を確認します。

企業名（及び略称） 日本セキュアジェネレーション株式会社	
所在地（郵便番号及び住所）104-0045 東京都中央区築地2-12-10 築地MFビル26号館	
関連部署名及び電話番号 技術部 03-5565-7911	
U R L <a href="http://www.secugen.co.jp/">http://www.secugen.co.jp/</a>	
対象技術	技術開発状況
サーバ クライアント データ	<ul style="list-style-type: none"> <li>・USB接続のPC用指紋読み取り装置（パラレル接続タイプもあり）</li> <li>・USB光学式マウスと指紋読み取り装置を一体化。</li> <li>・指紋読み取り部に硬度7のガラスを使用。抜群の耐久性。</li> <li>・SDK等のソフトウェアとの組合せにより、様々な場面での指紋認証を行うことが可能</li> <li>・SecuGen製の他デバイス（Eye Dハムスター、Eye Dオプティマウス、Eye Dキーボード等）との互換性有り。</li> <li>・デバイスドライバ附属（Windows用）</li> </ul>

企業名（及び略称） 日本セキュアジェネレーション株式会社	
所在地（郵便番号及び住所）104-0045 東京都中央区築地2-12-10 築地MFビル26号館	
関連部署名及び電話番号 技術部 03-5565-7911	
U R L <a href="http://www.secugen.co.jp/">http://www.secugen.co.jp/</a>	
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	<ul style="list-style-type: none"> <li>指紋によるWindows/ネットワークへのログオン</li> <li>指紋によるスクリーンセーバーのワークステーションロックの解除</li> <li>指紋によるフォルダの暗号/復号化</li> <li>ローカルPC用のソフトウェアのため、段階的な導入が可能</li> <li>通常のWindowsログオン画面が置き換わるため、PC紛失あるいは盗難時のPCログオンは基本的に不可能</li> <li>SecuGen製PC用ハードウェアの全てに対応</li> <li>360°認証対応</li> </ul>

企業名（及び略称） 日本セキュアジェネレーション株式会社	
所在地（郵便番号及び住所）104-0045 東京都中央区築地2-12-10 築地MFビル26号館	
関連部署名及び電話番号 技術部 03-5565-7911	
U R L <a href="http://www.secugen.co.jp/">http://www.secugen.co.jp/</a>	
対象技術	技術開発状況
サーバ 通信情報	<ul style="list-style-type: none"> <li>WEBにおける指紋認証機能を提供</li> <li>OTT(One Time Template) 技術により、データ傍受を端とする不正アクセスを阻止</li> <li>アクセスログを収集。イベント管理が容易。</li> <li>ID、パスワード、指紋による様々な認証ポリシーを個別に設定可能。</li> <li>1サーバで複数のWEBサイトを制御可能。</li> </ul>

企業名（及び略称） 日本セキュアジェネレーション株式会社	
所在地（郵便番号及び住所）104-0045 東京都中央区築地2-12-10 築地MFビル26号館	
関連部署名及び電話番号 技術部 03-5565-7911	
U R L <a href="http://www.secugen.co.jp/">http://www.secugen.co.jp/</a>	
対象技術	技術開発状況
施設	<ul style="list-style-type: none"> <li>CPUを実装した組込用指紋認証モジュール</li> <li>高速1:N識別アルゴリズム実装（0.8秒/1000ユーザ）</li> <li>4MBフラッシュメモリ実装。最大1000ユーザレコードを保持。</li> <li>RS232Cインターフェースにより、様々なデバイスに組み込み可能。</li> <li>ユーザレコードのインポート/エクスポートが可能</li> <li>指紋特徴点データ圧縮/復元機能を実装（144～400バイト）</li> <li>左右45°までの認証に対応</li> <li>50000Luxまでの耐光性、±15KVの対静電気性</li> </ul>

企業名（及び略称） 日本セキュアジェネレーション株式会社	
所在地（郵便番号及び住所） 104-0045 東京都中央区築地2-12-10 築地MFビル26号館	
関連部署名及び電話番号 技術部 03-5565-7911	
U R L <a href="http://www.secugen.co.jp/">http://www.secugen.co.jp/</a>	
対象技術	技術開発状況
サーバ クライアント データ	<ul style="list-style-type: none"> <li>・ GUIを実装したSDK</li> <li>・ センサーコントロールから登録認証までの機能を実装</li> <li>・ 主要開発言語をサポート（VB,VC++, VBNeT、C#等）</li> <li>・ API(DLL)COMをインターフェースとして提供</li> <li>・ 任意のユーザデータを指紋情報と一緒に暗号化できる「Payload」機能を実装</li> <li>・ 最大10指までを1データとして生成、暗号化</li> <li>・ 360°認証対応</li> </ul>

企業名（及び略称） 日本セキュアジェネレーション株式会社	
所在地（郵便番号及び住所） 104-0045 東京都中央区築地2-12-10 築地MFビル26号館	
関連部署名及び電話番号 技術部 03-5565-7911	
U R L <a href="http://www.secugen.co.jp/">http://www.secugen.co.jp/</a>	
対象技術	技術開発状況
サーバ クライアント データ	<ul style="list-style-type: none"> <li>・ センサーコントロールから登録認証までの細かな制御を可能にするSDK</li> <li>・ 1指当たり400バイトの特徴点を生成</li> <li>・ 主要開発言語をサポート（VB,VC++, VBNeT、C#等）</li> <li>・ API(DLL)、ActiveXをインターフェースとして提供</li> <li>・ 多種のプラットフォームへ対応可能</li> <li>・ 組み込み用製品「FDA02」とのデータ互換性あり。フィジカルセキュリティとITセキュリティの連携が可能</li> <li>・ 360°認証対応</li> </ul>

企業名（及び略称） 日本セキュアジェネレーション株式会社	
所在地（郵便番号及び住所） 104-0045 東京都中央区築地2-12-10 築地MFビル26号館	
関連部署名及び電話番号 技術部 03-5565-7911	
U R L <a href="http://www.secugen.co.jp/">http://www.secugen.co.jp/</a>	
対象技術	技術開発状況
サーバ クライアント データ	<ul style="list-style-type: none"> <li>・ 高速1:N認証エンジン</li> <li>・ 最近似データ識別と合致候補リスト生成の2大機能を実装</li> <li>・ APIを提供、アプリケーションへの統合が容易</li> <li>・ SecuGen開発キットとの連携</li> </ul>

企業名（及び略称） 日本テレコム株式会社 研究所	
所在地（郵便番号及び住所） 105-7316 東京都港区東新橋1-9-1	
関連部署名及び電話番号 研究所 企画・プロモーション	
U R L <a href="http://www.japan-telecom.co.jp/r_and_d/index.html">http://www.japan-telecom.co.jp/r_and_d/index.html</a>	
対象技術	技術開発状況
その他	インターネットと閉域網とのゲートウェイを利用するお客様に対して、セキュリティ・インターネットサーバをはじめとする、ネットワークの付加価値をご提供するサービス。

企業名（及び略称） 日本電気株式会社 システム基盤ソフトウェア開発本部	
所在地（郵便番号及び住所） 108-8557 東京都港区芝浦2-11-5	
関連部署名及び電話番号	
U R L <a href="http://www.labs.nec.co.jp/Overview/soshiki/software/index.html">http://www.labs.nec.co.jp/Overview/soshiki/software/index.html</a>	
対象技術	技術開発状況
通信情報データ	アクセス権限を持った正規ユーザの故意・過失による機密データの持ち出しを制限し、内部からの情報漏洩を未然に防止する

企業名（及び略称） 日本電気株式会社 システム基盤ソフトウェア開発本部	
所在地（郵便番号及び住所） 108-8557 東京都港区芝浦2-11-5	
関連部署名及び電話番号	
U R L <a href="http://www.labs.nec.co.jp/Overview/soshiki/software/index.html">http://www.labs.nec.co.jp/Overview/soshiki/software/index.html</a>	
対象技術	技術開発状況
サーバクライアントデータ	複数のWEBサーバを遠隔地から一元的に管理して、ホームページのコンテンツや設定ファイルの改ざん検知を行う

企業名（及び略称） 日本電気株式会社 システム基盤ソフトウェア開発本部	
所在地（郵便番号及び住所）108-8557 東京都港区芝浦2-11-5	
関連部署名及び電話番号	
U R L <a href="http://www.labs.nec.co.jp/Overview/soshiki/software/index.html">http://www.labs.nec.co.jp/Overview/soshiki/software/index.html</a>	
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	不正アクセス対策、ホスト型IDSを搭載した中規模向けファイアウォールアプリケーション

企業名（及び略称） 日本電気株式会社 システム基盤ソフトウェア開発本部	
所在地（郵便番号及び住所）108-8557 東京都港区芝浦2-11-5	
関連部署名及び電話番号	
U R L <a href="http://www.labs.nec.co.jp/Overview/soshiki/software/index.html">http://www.labs.nec.co.jp/Overview/soshiki/software/index.html</a>	
対象技術	技術開発状況
通信情報 データ	W3Cで策定された国際標準仕様である、XML署名、暗号仕様に準拠したライブラリ、及びWEBクライアント、ICカード、PKIを利用したシステム構築が容易に可能となるコンポーネントからなる製品。分離署名といった独自技術ももり込まれており、電子申請システム、電子契約システムで多数の採用実績を持つ

企業名（及び略称） 日本電気株式会社 システム基盤ソフトウェア開発本部	
所在地（郵便番号及び住所）108-8557 東京都港区芝浦2-11-5	
関連部署名及び電話番号	
U R L <a href="http://www.labs.nec.co.jp/Overview/soshiki/software/index.html">http://www.labs.nec.co.jp/Overview/soshiki/software/index.html</a>	
対象技術	技術開発状況
その他 (認証情報、アイデンティティ情報)	インターネット標準仕様Liberty Alliance ID-FF1.2に準拠した、アイデンティティ管理、SSOを実現する製品。ユーザ情報、リソース情報、アクセス条件を一元管理し、システム全体のセキュリティ水準を保った管理コストの削減を実現する。ディレクトリ製品、PKI製品との連携機能を持ち、大規模な認証システムの構築が可能

企業名（及び略称） 日本電信電話株式会社 NTT情報流通プラットフォーム研究所	
所在地（郵便番号及び住所）180-8585 東京都武蔵野市緑町3-9-11	
関連部署名及び電話番号 企画担当	
URL <a href="http://www2.pflab.ecl.ntt.co.jp/">http://www2.pflab.ecl.ntt.co.jp/</a>	
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	ネットワーク上における本人性の確認などに用いられる公開鍵証明書を発行、失効などを行うシステム。業務要件に応じて複数の暗号アルゴリズムを選択できるとともに、リアルタイムな証明書有効性の確認ができる

企業名（及び略称） 日本電信電話株式会社 NTT情報流通プラットフォーム研究所	
所在地（郵便番号及び住所）180-8585 東京都武蔵野市緑町3-9-11	
関連部署名及び電話番号 企画担当	
URL <a href="http://www2.pflab.ecl.ntt.co.jp/">http://www2.pflab.ecl.ntt.co.jp/</a>	
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	μFPIは指紋の読み取りから認証までの全ての処理をわずか11×15×1mmのパッケージ内で実行する為、指紋データが外部へ漏洩する事なく、セキュリティの向上を実現できます。得に認証までの全処理を本モジュール内で完結する為プロセッサを持たない様々な機器への適用が可能な事、低消費電力の為電池駆動も可能な事などの特徴があります

企業名（及び略称） 日本電信電話株式会社 NTT情報流通プラットフォーム研究所	
所在地（郵便番号及び住所）180-8585 東京都武蔵野市緑町3-9-11	
関連部署名及び電話番号 企画担当	
URL <a href="http://www2.pflab.ecl.ntt.co.jp/">http://www2.pflab.ecl.ntt.co.jp/</a>	
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	FingerQuickはUSBインタフェースの携帯型本人認証デバイス。指紋の照合によって、予め設定した認証パスワードがPCに出力されます。さらにセキュリティアプリケーションと連携してシングルサインオン、スクリーンロック、ファイル暗号化などが可能です。また、専門ドライバなどのインストールが不要、指紋の照合を本製品の内部で行う為、指紋データなどの個人データが漏洩しない等の特徴があります。

企業名（及び略称） 日本認証サービス株式会社	
所在地（郵便番号及び住所）105-0014 東京都港区芝1丁目10番11号 コスモ金杉橋	
関連部署名及び電話番号 03-5484-1391	
U R L <a href="http://www.jcsinc.co.jp/">http://www.jcsinc.co.jp/</a>	
対象技術	技術開発状況
通信情報 データ	SSL用WEBサーバ証明書、SSL用クライアント証明書、S/MIME（暗号、署名メール）用証明書など多種。なお、広く任意の利用者間で使えるパブリックサービスと特定の企業間の内部および企業間用のプライベートサービスがあります。

企業名（及び略称） 日本認証サービス株式会社	
所在地（郵便番号及び住所）105-0014 東京都港区芝1丁目10番11号 コスモ金杉橋	
関連部署名及び電話番号 03-5484-1391	
U R L <a href="http://www.jcsinc.co.jp/">http://www.jcsinc.co.jp/</a>	
対象技術	技術開発状況
データ	電子証明法認定認証業務、GPKI相互認証済み、対官公庁電子入札、電子申請、届出用電子証明書発行、現在39のシステムによる入札、申請・届出等に利用できる。また、広範囲の利用者に対して発行できることが特徴。

企業名（及び略称） 日立電子サービス株式会社	
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504-2	
関連部署名及び電話番号 社長室広報グループ 045-822-1111(大代表)	
U R L <a href="http://www.hitachi-densa.co.jp/">http://www.hitachi-densa.co.jp/</a>	
対象技術	技術開発状況
その他	アクセス制御製品のインテグレーションからリモート、オンサイトによる運用、保守サービスの提供。セキュアサイクルに基づいたトータルセキュリティサービスを提供。リモートによる24時間365日の監視サービスや、全国のサービス拠点からのオンサイトサービスの提供が可能。

企業名（及び略称） 日立電子サービス株式会社	
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504-2	
関連部署名及び電話番号 社長室広報グループ 045-822-1111(大代表)	
U R L <a href="http://www.hitachi-densa.co.jp/">http://www.hitachi-densa.co.jp/</a>	
対象技術	技術開発状況
その他	LANに接続されるPCクライアントを認証により識別し、正規のユーザ/PCのみ通信可能とするネットワーク構築を行います。また、接続ユーザ/PCのポリシー設定によりアクセス可能範囲を制限する事も可能です

企業名（及び略称） 日立電子サービス株式会社	
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504-2	
関連部署名及び電話番号 社長室広報グループ 045-822-1111(大代表)	
U R L <a href="http://www.hitachi-densa.co.jp/">http://www.hitachi-densa.co.jp/</a>	
対象技術	技術開発状況
その他	IDカードや指紋、指静脈等の生体認証を使用して、入退室を管理出来るシステムを構築致します。映像監視システムを組み込むことにより、監視・管理レベルを上げる事も可能です

企業名（及び略称） 日立電子サービス株式会社	
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504-2	
関連部署名及び電話番号 社長室広報グループ 045-822-1111(大代表)	
U R L <a href="http://www.hitachi-densa.co.jp/">http://www.hitachi-densa.co.jp/</a>	
対象技術	技術開発状況
その他	IEEE802.1x,11i等を利用し、接続時の認証・暗号化を行いセキュアな無線LAN接続環境を実現致します。また、防磁フィルム等を利用し外部からの混信電波を防いだ無線LAN環境を実現可能です

企業名（及び略称） 日立電子サービス株式会社	
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504-2	
関連部署名及び電話番号 社長室広報グループ 045-822-1111(大代表)	
U R L <a href="http://www.hitachi-densa.co.jp/">http://www.hitachi-densa.co.jp/</a>	
対象技術	技術開発状況
その他	インターネットを経由した企業内拠点間接続や外出先からインターネットを使用した企業内ネットワークへの接続時、認証・暗号化を使用してセキュアな接続環境を提供致します

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 アウトソーシング事業本部情報セキュリティセンター 044-754-3353	
U R L <a href="http://jp.fujitsu.com/">http://jp.fujitsu.com/</a>	
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	情報セキュリティ（監視サービス・強化支援コンサルティングサービス・方針立案サービス）市町村向けポリシー立案サービス、取得支援サービス( BS7799・ISMS・ISO15408・プライバシーマーク)、PKI構築サービス、Verisign Ousiteサービス、WEBアプリケーション診断サービス、アタックテストサービス他 ( <a href="http://segroup.fujitsu.com/secure/solution">http://segroup.fujitsu.com/secure/solution</a> 参照)

企業名（及び略称） 富士通サポート&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	
U R L	
対象技術	技術開発状況
ネットワーク 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アプリまで具備しています

企業名（及び略称） 株式会社 富士通ビー・エス・シー	
所在地（郵便番号及び住所） 141-8581 東京都品川区大崎1-11-2 ゲートシティ大崎イーストタワー11F	
関連部署名及び電話番号 ビジネスサポート本部 企画広報部 03-5740-3111	
URL <a href="http://www.bsc.fujitsu.com/">http://www.bsc.fujitsu.com/</a>	
対象技術	技術開発状況
通信情報 データ	業務上の重要データ暗号化によりセキュリティを確保。複数のファイルやフォルダをひとつの圧縮された暗号化ファイルにすることを実現。自動暗号機能により、ユーザが意識することなく暗号化を実現。

企業名（及び略称） 株式会社 富士通ビー・エス・シー	
所在地（郵便番号及び住所） 141-8581 東京都品川区大崎1-11-2 ゲートシティ大崎イーストタワー11F	
関連部署名及び電話番号 ビジネスサポート本部 企画広報部 03-5740-3111	
URL <a href="http://www.bsc.fujitsu.com/">http://www.bsc.fujitsu.com/</a>	
対象技術	技術開発状況
通信情報 データ	企業内部で引き起こされる重要データの漏洩を抑止。ドライバウェアによる強力な情報漏洩抑止機能。Fence-Proとの連携により暗号化ファイルのみの持ち出しを実現

企業名（及び略称） 株式会社 富士通ビー・エス・シー	
所在地（郵便番号及び住所） 141-8581 東京都品川区大崎1-11-2 ゲートシティ大崎イーストタワー11F	
関連部署名及び電話番号 ビジネスサポート本部 企画広報部 03-5740-3111	
URL <a href="http://www.bsc.fujitsu.com/">http://www.bsc.fujitsu.com/</a>	
対象技術	技術開発状況
データ	トークンにより、PCへのアクセスコントロールを実現。PCロック機能により、OSレベルでのロック機能を提供

企業名（及び略称） 株式会社 富士通ビー・エス・シー	
所在地（郵便番号及び住所） 141-8581 東京都品川区大崎1-11-2 ゲートシティ大崎イーストタワー11F	
関連部署名及び電話番号 ビジネスサポート本部 企画広報部 03-5740-3111	
URL <a href="http://www.bsc.fujitsu.com/">http://www.bsc.fujitsu.com/</a>	
対象技術	技術開発状況
通信情報 データ	クライアント上の操作情報を記録

企業名（及び略称） 株式会社 マックポートバイオセキュリティ	
所在地（郵便番号及び住所） 271-0074 千葉県松戸市緑ヶ丘1-221-102	
関連部署名及び電話番号 コンサルティング部 047-363-7337	
URL <a href="http://www.mackport.co.jp/">http://www.mackport.co.jp/</a>	
対象技術	技術開発状況
通信情報	指紋で静脈、顔など人間固有の特徴パターンを利用して、ネットワークアクセス権限を与えるものです。

企業名（及び略称） 三井物産セキュアディレクション株式会社	
所在地（郵便番号及び住所） 101-0054 東京都千代田区神田錦町3-26	
関連部署名及び電話番号 経営企画部 コーポレートマーケティンググループ 村上 03-5217-2383	
URL <a href="http://www.mbsd.jp/">http://www.mbsd.jp/</a>	
対象技術	技術開発状況
データ	クライアント不要、厳密なアクセス制御、高い信頼性とスケーラビリティ、エンドポイントコントロール

企業名（及び略称） 三井物産セキュアディレクション株式会社	
所在地（郵便番号及び住所） 101-0054 東京都千代田区神田錦町3-26	
関連部署名及び電話番号 経営企画部 コーポレートマーケティンググループ 03-5217-2383	
U R L <a href="http://www.mbsd.jp/">http://www.mbsd.jp/</a>	
対象技術	技術開発状況
データ	ボタンひとつで暗号化・復号化。電子証明書の管理や失効リストも不要。様々なセキュリティや業界コンプライアンスに対応。既存のセキュリティ製品とも共存可能

企業名（及び略称） 三井物産セキュアディレクション株式会社	
所在地（郵便番号及び住所） 101-0054 東京都千代田区神田錦町3-26	
関連部署名及び電話番号 経営企画部 コーポレートマーケティンググループ 03-5217-2383	
U R L <a href="http://www.mbsd.jp/">http://www.mbsd.jp/</a>	
対象技術	技術開発状況
データ	ひとつの製品で操作制御・ログ取得・ログ分析など、様々な機能を実現。強力なロギング機能、高機能な検索機能、様々なレポート機能、多彩な制御機能

企業名（及び略称） 三井物産セキュアディレクション株式会社	
所在地（郵便番号及び住所） 101-0054 東京都千代田区神田錦町3-26	
関連部署名及び電話番号 経営企画部 コーポレートマーケティンググループ 03-5217-2383	
U R L <a href="http://www.mbsd.jp/">http://www.mbsd.jp/</a>	
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	未知のワーム等による被害を最小化、不正アクセスからの保護、ネットワーク可用性の維持

企業名（及び略称） 三菱電機インフォメーションテクノロジー株式会社	
所在地（郵便番号及び住所）108-0023 東京都港区芝浦4-15-33 芝浦清水ビル	
関連部署名及び電話番号	
U R L <a href="http://www.mdit.co.jp/">http://www.mdit.co.jp/</a>	
対象技術	技術開発状況
クライアント	PCのアクセス制御（外部機器）と全ての操作ログの収集・分析

企業名（及び略称） 三菱電機インフォメーションテクノロジー株式会社	
所在地（郵便番号及び住所）108-0023 東京都港区芝浦4-15-33 芝浦清水ビル	
関連部署名及び電話番号	
U R L <a href="http://www.mdit.co.jp/">http://www.mdit.co.jp/</a>	
対象技術	技術開発状況
データ	単一プラットフォーム上でのWEBコンテンツ管理、ドキュメント管理、コラボレーション、レコード管理、デジタル資産管理アプリケーションの展開が可能

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 渉外室 0422-52-5533	
U R L <a href="http://www.yokogawa.co.jp/">http://www.yokogawa.co.jp/</a>	
対象技術	技術開発状況
サーバ	<p>概要：</p> <p>インターネット経由によるリモートアクセス環境構築システム WEBアプリケーションへの認証システム。</p> <p>特徴：</p> <p>認証において、書き込みデバイス（USBメモリ、HD、FD）を利用したワンタイムパスワード機能（特許取得） 強力なりバースプロシキ機能 SSL-VPNでのどこでも接続できるネットワーク環境 クライアントPCへのソフトウェアインストールの必要なし</p>

企業名(及び略称)	株式会社 ワイ・デー・ケー	
所在地(郵便番号及び住所)	206-0811 東京都稲城市押立1705番地	
関連部署名及び電話番号	YDKテクノロジーズ 042-378-8111	
URL	<a href="http://www.ydkinc.co.jp/">http://www.ydkinc.co.jp/</a>	
対象技術	技術開発状況	
通信情報	IPv6のAESを含むプロトコルスタック	