平成２０年２月２９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19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19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19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。

１　不正アクセス行為の認知状況

(1)　認知件数

平成19年中の不正アクセス行為の認知件数は1,818件で、前年と比べ、872件増加した。

表１－１　不正アクセス行為の認知件数の推移

区分＼年次		平成15年	平成16年	平成17年	平成18年	平成19年
認知件数（件）		212	356	592	946	1,818
	海外からのアクセス	35	37	53	37	79
	国内からのアクセス	158	303	487	855	1,684
	アクセス元不明	19	16	52	54	55

(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（1,372件）、次いで一般企業（437件）となっている。

表１－２　被害を受けた特定電子計算機のアクセス管理者の推移

区分＼年次		平成15年	平成16年	平成17年	平成18年	平成19年
プロバイダ（件）		98	126	356	602	1,372
一般企業		76	202	203	325	437
大学、研究機関等		16	6	12	6	1
その他		22	22	21	13	8
	うち行政機関	3	12	17	5	5
不明		0	0	0	0	0
計		212	356	592	946	1,818

※　「プロバイダ」とは、インターネットに接続する機能を提供する電気通信事業者をいう。

「大学、研究機関等」には、高等学校等の学校機関を含む。

「その他」の「うち行政機関」には、独立行政法人、特殊法人、地方公共団体及びこれらの附属機関を含む。

(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（1,326件）、次いで利用権者（注２）からの届出によるもの（415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（61件）、発見者からの通報によるもの（2件）の順となっている。

表１－３　認知の端緒の推移

区分＼年次	平成15年	平成16年	平成17年	平成18年	平成19年
警察活動（件）	100	146	33	535	1,326
利用権者からの届出	78	172	505	358	415
アクセス管理者からの届出	12	29	30	45	61
発見者からの通報	19	7	14	3	2
その他	3	2	10	5	14
計	212	356	592	946	1,818

(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等）が最も多く（1,347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）（246件）、インターネットバンキングの不正送金（113件）、情報の不正入手（電子メールの盗み見等）（55件）、ホームページの改ざん・消去（25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）（1件）の順となっている。

表１－４　不正アクセス行為後の行為の内訳

区分＼年次	平成18年	平成19年
インターネット・オークションの不正操作（件）	593	1,347
オンラインゲームの不正操作	257	246
インターネットバンキングの不正送金	39	113
情報の不正入手	14	55
ホームページの改ざん・消去	32	25
不正ファイルの蔵置	5	1
不明	2	0
その他	4	31

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19年中における不正アクセス禁止法違反の検挙件数は1,442件、検挙人員は126人と、前年と比べ、検挙件数は739件増加し、検挙人員は４人減少した。その内訳をみると、不正アクセス行為に係るものがそれぞれ1,438件、86人、不正アクセス助長行為（注４）に係るものがそれぞれ４件、４人であった。

表２－１　検挙事件数等の推移

区分＼年次		平成15年	平成16年	平成17年	平成18年	平成19年
不正アクセス行為	検挙件数	143	142	271	698	1,438
	検挙事件数（注５）	58	65	94	84	86
	検挙人員	76	88	113	130	126
不正アクセス助長行為	検挙件数	2	0	6	5	4
	検挙事件数	2	0	6	3	2
	検挙人員	2	0	6	5	4
計	検挙件数（件）	145	142	277	703	1,442
	検挙事件数（事件）	58（重複2）	65	94（重複6）	84（重複3）	86（重複2）
	検挙人員（人）	76（重複2）	88	116（重複3）	130（重複5）	126（重複4）

※　(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1,438件であり、セキュリティ・ホール攻撃型（注７）は無かった。

表２－２　不正アクセス行為の態様の推移

区分＼年次		平成15年	平成16年	平成17年	平成18年	平成19年
識別符号窃用型	検挙件数	141	131	264	698	1,438
	検挙事件数	56	62	90	84	86
セキュリティ・ホール攻撃型	検挙件数	2	11	7	0	0
	検挙事件数	2	4	5	0	0
計	検挙件数（件）	143	142	271	698	1,438
	検挙事件数（事件）	58	65（重複1）	94（重複1）	84	86

※　(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（1,157件）が大きく増加したほか、スパイウェア（注８）等のプログラムを使用して識別符号を入手したもの（55件）等、巧妙な手口により識別符号を入手したものも依然として発生している。

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（139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（39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（31件）等、特に高度な技術を有していない者でも行うことができ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

区分＼年次		平成18年	平成19年
識別符号窃用型（件）		698	1,438
	フィッシングサイトにより入手したもの	220	1,157
	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	139
	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	197	55
	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	49	39
	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	31
	他人から購入したもの	12	7
	共犯者等から入手したもの	0	3
	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	19	2
	その他	3	5
セキュリティ・ホール攻撃型		0	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窃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（1,373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（57件）、ネットワーク上のみの知り合いによるもの（8件）となっている。

また、被疑者の年齢についてみると、10歳代及び20歳代が最も多く（それぞれ39人）、次いで30歳代（34人）、40歳代（12人）、50歳代（2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51歳であった。

表３－２　年代別被疑者数の推移

区分＼年次	平成15年	平成16年	平成17年	平成18年	平成19年
10歳代（人）	16	26	35	40	39
20歳代	26	21	40	44	39
30歳代	24	23	27	28	34
40歳代	9	17	9	15	12
50歳代	1	1	5	2	2
60歳代	0	0	0	1	0
計	76	88	116	130	126

※　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（1,186件）が最も多く、次いでオンラインゲームで不正操作を行うため（133件)、嫌がらせや仕返しのため（62件)、好奇心を満たすため（55件)、料金の請求を免れるため（２件）の順となっている。

表３－３　不正アクセス行為の動機の内訳

区分＼年次	平成18年	平成19年
不正に金を得るため（件）	419	1,186
オンラインゲームで不正操作を行うため	211	133
嫌がらせや仕返しのため	31	62
好奇心を満たすため	26	55
料金の請求を免れるため	1	2
顧客データの収集等情報を不正に入手するため	10	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（1,438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（1,178件)、前年と比べ大きく増加した。次いで、オンラインゲーム（171件)、会員専用・社員用内部サイト（33件)、電子メール（22件)、電子掲示板（13件)、ホームページ公開サービス（9件）の順となっている。

表３－４　利用されたサービスの内訳

区分＼年次		平成18年	平成19年
識別符号窃用型（件）		698	1,438
	インターネット・オークション	394	1,178
	オンラインゲーム	223	171
	会員専用・社員用内部サイト	6	33
	電子メール	21	22
	電子掲示板	5	13
	ホームページ公開サービス	7	9
	インターネットバンキング	38	4
	インターネットショッピング	0	3
	会員・顧客データベース	2	0
	その他	2	5

４　都道府県公安委員会による援助措置

平成19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・指導は無かった。

表４－１　都道府県公安委員会の援助措置実施件数の推移

区分＼年次	平成15年	平成16年	平成17年	平成18年	平成19年
援助措置（件）	5	3	4	3	0

５　防御上の留意事項

(1)　利用権者の講ずべき措置

ア　フィッシング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等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を送信し、それらによりＩＤ・パスワードを不正に取得する事案が発生していることから、発信元に心当たりのない電子メール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発生しているため、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。

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、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３月から平成18年10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だまし取った。平成19年１月、不正アクセス禁止法違反、詐欺罪等で検挙した（警視庁、岡山、広島、熊本）。

２	**オンラインゲーム上にキーロガー（注11）を仕掛けて入手した他人の識別符号を用いて同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**

中学生の男(15)らは、平成17年12月から平成18年５月までの間、オンラインゲーム上のアイテムを収集する目的で、ゲーム内のチャットを利用して、キャラクターの速度が速くなるプログラムがあるとの甘言によって他の利用者にキーロガーをダウンロードさせ、他人の識別符号を入手し、これを使用して同オンラインゲームを運営する会社のコンピュータに不正アクセス行為を行った。平成19年２月、不正アクセス禁止法違反で検挙した（静岡）。

３	**一つのパスワードに様々なＩＤを組み合わせてＩＤを特定する方法でインターネット証券会社の識別符号を入手し、他人になりすまし、同証券会社の個人情報を閲覧した不正アクセス禁止法違反事件**

会社員の男(31)は、平成18年11月、インターネット証券会社の他人の証券情報を見るため、一つのパスワードに様々なＩＤを組み合わせてＩＤを特定する方法で検索するプログラムを自作し、これを使用して、利用権者のＩＤ・パスワードを入手し、同会社のコンピュータに不正アクセス行為を行った。平成19年３月、不正アクセス禁止法違反で検挙した（警視庁）。

４	**インターネット・オークション会社の元従業員が、在職中に顧客の識別符号を不正に入手した上、インターネットカフェを利用して、同社オークションに架空出品して代金をだま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(23)は、平成18年６月、元勤務先のインターネット・オークション会社の

コンピュータに、在職中に不正に入手した同会社の顧客の識別符号を入力して、インターネットカフェから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だまし取った。平成19年１月、不正アクセス禁止法違反及び詐欺罪で検挙した（岐阜）。

５	**インターネット上に流出した識別符号を入手し、他人になりすまして、インターネットショッピングで商品を詐取するとともに、インターネットバンキングで不正送金を行った不正アクセス禁止法違反、詐欺及び電子計算機使用詐欺事件**

会社員の男(33)は、平成19年６月から平成19年10月までの間、ファイル共有ソフト（注12）「ウィニー」を使用して、コンピュータ・ウイルスに感染し、同ソフトの使用によりインターネット上に流出していた他人の識別符号を入手し、他人になりすまして不正アクセス行為を行った。そして、インターネットショッピングにおいて商品を詐取し、インターネットバンキングにおいて自己名義の銀行口座への不正送金を行った。平成19年10月、不正アクセス禁止法違反、詐欺罪及び電子計算機使用詐欺罪で検挙した（愛知、警視庁、高知）。

６	**同僚の識別符号を不正に入手し、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を行い、自己名義の銀行口座に不正送金した不正アクセス禁止法違反及び電子計算機使用詐欺事件**

派遣社員の男(26)は、平成19年９月、勤務先の同僚の財布からインターネットバンキング利用に係る識別符号を入手して、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、同僚の口座から自己名義の銀行口座へ不正送金を行った。平成19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）。

（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、特定電子計算機をだれに利用させるかを決定する者をいう。

例えば、インターネットへの接続や電子メールの受信についてはプロバイダが、インターネットショッピング用のホームページの閲覧についてはその経営者が、それぞれアクセス管理者となる。

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などして、受信者が偽のウェブサイトにアクセスするよう仕向け、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、又はこれを知っている者の求めに応じて、アクセス管理者や利用権者に無断で第三者に提供する行為をいう。

注５　事件数

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用のパスワードであって、認証のたびにそれを構成する文字列が変わるもの。これを導入することにより、識別符号を盗まれても次回の利用時に使用できないこととなる。

注10　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ったかを記録するプログラムをいう。

注12　ファイル共有ソフト

　同種のソフトウェアを利用する不特定多数のコンピュータの中から特定の情報を持つコンピュータを探し出し、特定のサーバコンピュータを経由せずに、不特定多数の者が相互に直接情報を共有するソフトをいう。

第２　不正アクセス関連行為の関係団体への届出状況について

１　独立行政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１９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218件（昨年：331件）であった。（注２）

平成19(2007)年は同18(2006)年と比べて、全体的な件数は大幅に減少しているが、被害があった届出件数は昨年と同じであった。

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項目に該当するものがあるため、それぞれの分類での総計件数はこの数字に必ずしも一致しない。

(1) 手口別分類

意図的に行う攻撃行為による分類である。1 件の届出について複数の攻撃行為を受けている場合もあるため、届出件数とは一致せず総計は430件（昨年：553件）となる。

ア　侵入行為に関して

侵入行為に係わる攻撃等の届出は392件（昨年：517件）あった。

(ｱ) 侵入の事前調査行為

システム情報の調査、稼動サービスの調査、アカウント名の調査等である。

29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。

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55件である。

【主な内容】

パスワード推測：42件

ソフトウェアのバグを利用した攻撃：34件

システムの設定内容を利用した攻撃：5件

(ｳ) 不正行為の実行及び目的達成後の行為

侵入その他、何らかの原因により不正行為を実行されたことについては255件の届出があった。

【主な内容】

ファイル等の改ざん、破壊等：109 件
資源利用（ファイル、CPU 使用）：89 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：41 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：1 件

イ　サービス妨害攻撃

過負荷を与えたり、例外処理を利用してサービスを不可もしくは低下させたりする攻撃である。7 件（昨年：17 件）の届出があった。

ウ　その他

その他にはメール不正中継やソーシャルエンジニアリング、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、31 件（昨年：19 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：16 件
メールの不正中継に関するもの：2 件
正規ユーザへのなりすまし：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。

218 件の届出中、実際に被害に遭った計 162 件（昨年：162 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おり、手口が巧妙化するとともに原因究明が困難な事例が多いことが推測される。

【主な要因】
ID、パスワード管理の不備によると思われるもの：27 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：23 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
DoS 攻撃・その他によるもの：26 件
原因不明：80 件

(3) 電算機分類

不正アクセス行為の対象となった機器による分類である。（被害の有無は問わない）

【主な対象】

クライアント：78 件
WWW サーバー：43 件
メールサーバー：17 件
ルータ：9 件
その他のサーバー：40 件
不明：38 件
※1 件の届出で複数の項目に該当するものがある

(4) 被害内容分類

実際に被害に遭ったケースにおける被害内容による分類である。機器に対する実被害があった件数は 237 件（昨年：229 件）である。なお、対処にかか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】

ファイルの書き換え：93 件
ホームページ改ざん：18 件
サービス低下：6 件
メールの不正中継に利用された：2 件
サーバのダウン：2 件
不正アカウント作成：1 件
※1 件の届出で複数の項目に該当するものがある

(5) 対策情報

平成 19(2007)年は、SSH で使用するポートへの攻撃で侵入された被害（ID、パスワードの設定不備が主な原因）や、OS もしくは Web アプリケーションなどの脆弱性を突かれたことによる被害が特に目立っていたと言える。しかしながら、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。改めて原点を見つめ直し、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
- 脆弱性の解消（修正プログラム適用不可の場合は、運用による回避策も含む）
- ルータやファイアウォールなどの設定やアクセス制御設定
- こまめなログのチェック

また、ホーム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。

【システム管理者向け】

「情報セキュリティに関する啓発資料」
http://www.ipa.go.jp/security/fy18/reports/contents/

「脆弱性対策のチェックポイント」
http://www.ipa.go.jp/security/vuln/20050623_websecurity.html

「安全なウェブサイトの作り方　改訂第 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/

【ホームユーザ向け】

「IPA セキュリティセンター・個人ユーザ向けページ」
http://www.ipa.go.jp/security/personal/

「コンピュータを守るために最低限必要なセキュリティ対策」（マイクロソフト）
http://www.microsoft.com/japan/athome/security/protect/default.aspx

ウイルス対策を含むセキュリティ関係の情報・対策などについては、下記ページを参照のこと。

「IPA セキュリティセンタートップページ」
http://www.ipa.go.jp/security/

注１　コンピュータ不正アクセス
システムを利用する者が、その者に与えられた権限によって許された行為以外の行為を、ネットワークを介して意図的に行うこと。

注２　ここにあげた件数は、コンピュータ不正アクセスの届出を IPA が受理した件であり、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１９年１月１日から１２月３１日の間に JPCERT/CC に届出のあったコンピュータ不正アクセスが対象である。

(1) 不正アクセス関連行為の特徴および件数

届出のあった不正アクセス関連行為(注１)に係わる報告件数(注２)は 3,140 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 1,611 件の報告があった。

[1/1-3/31: 215 件、4/1-6/30: 238 件、7/1-9/30:575 件、10/1-12/31: 583 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 9 件の報告があった。

[1/1-3/31: 4 件、4/1-6/30: 0 件、7/1-9/30: 3 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 18 件の報告があった。

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

[1/1-3/31: 6 件、4/1-6/30: 2 件、7/1-9/30: 2 件、10/1-12/31: 1 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 716 件の報告があった。

[1/1-3/31: 208 件、4/1-6/30: 137 件、7/1-9/30: 208 件、10/1-12/31:163 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 775 件の報告があった。
[1/1-3/31: 86 件、4/1-6/30: 290 件、7/1-9/30: 239 件、10/1-12/31: 165 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]

07 年 1 月 Microsoft セキュリティ情報（緊急 3 件含）に関する注意喚起
Cisco IOS に複数の脆弱性
Cisco IOS の SIP パケットの処理に関する脆弱性
「CCC クリーナー」の脆弱性に関する注意喚起
07 年 2 月 Microsoft セキュリティ情報（緊急 6 件含）に関する注意喚起
ベリサイン マネージド PKI サービスに使用される ActiveX コントロールの脆弱性に関する注意喚起
Sun Solaris in.telnetd の脆弱性を使用するワームに関する注意喚起
Windows アニメーションカーソル処理の未修正の脆弱性に関する注意喚起
ID やパスワードを聞き出そうとする電話に関する注意喚起
07 年 4 月 Microsoft セキュリティ情報（緊急 5 件含）に関する注意喚起
07 年 5 月 Microsoft セキュリティ情報（緊急 7 件）に関する注意喚起
Java Web Start の脆弱性に関する注意喚起
国内金融機関を装ったフィッシングサイトに関する注意喚起
複数の脆弱性を使用する攻撃ツール MPack に関する注意喚起
ID やパスワードを聞き出そうとする電話に関する注意喚起
07 年 6 月 Microsoft セキュリティ情報（緊急 4 件含）に関する注意喚起
複数の Cisco 製品における DoS の脆弱性に関する注意喚起
ファイル圧縮・解凍ソフト Lhaplus の脆弱性に関する注意喚起
TCP 5168 番ポートへのスキャン増加に関する注意喚起
07 年 7 月 Microsoft セキュリティ情報 (緊急 3 件含)に関する注意喚起
07 年 8 月 Microsoft セキュリティ情報 (緊急 6 件含)に関する注意喚起
07 年 10 月 Microsoft セキュリティ情報 (緊急 4 件含)に関する注意喚起
07 年 11 月 Microsoft セキュリティ情報 (緊急 1 件含)に関する注意喚起
07 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

アップル QuickTime の未修正の脆弱性に関する注意喚起

イ　活動概要（届出状況等の公表）

発行日：2008-01-15 [2007 年 10 月 1 日～ 2007 年 12 月 31 日]
発行日：2007-10-26 [2007 年 7 月 1 日 ～ 2007 年 9 月 30 日]
発行日：2007-07-19 [2007 年 4 月 1 日 ～ 2007 年 6 月 30 日]
発行日：2007-04-19 [2007 年 1 月 1 日 ～ 2007 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] 363 件

(3)　定点観測システム

インターネット定点観測システム(ISDAS）を運用することによって、ワームの感染活動や弱点探索のためのスキャンなど、セキュリティ上の脅威となるトラフィクの観測を行い、セキュリティ予防情報を提供している。
（詳細は http://www.jpcert.or.jp/isdas/参照。）

(4) 脆弱性情報流通

日本国内の製品開発者(ベンダ）などの関連組織とのコーディネーションを行ない、JVN (Japan Vulnerability Notes）にて公開した脆弱性情報は 200 件であった(詳細は http://jvn.jp/参照。）
[1/1-3/31: 63 件、4/1-6/30: 46 件、7/1-9/30: 43 件、10/1-12/31: 48 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 100 件であった。
[1/1-3/31: 28 件、4/1-6/30: 23 件、7/1-9/30: 18 件、10/1-12/31: 31 件]

注１　不正アクセス関連行為とは、コンピュータやネットワークのセキュリティを侵害する人為的な行為で、意図的(または、偶発的）に発生する全ての事象が対象になる。

注２　ここにあげた件数は、JPCERT/CC が受け付けた報告の件数である。実際のアタックの発生件数や、被害件数を類推できるような数値ではない。また類型ごとの実際の発生比率を示すものでもない。一定以上の期間に渡るアクセスの要約レポートも含まれるため、アクセスの回数と報告件数も一般に対応しない。報告元には、国内外のサイトが含まれる。

アクセス制御機能に関する技術の研究開発の状況

1　国で実施しているもの

総務省又は経済産業省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。

ユビキタスネットワーク認証・エージェント技術の研究開発
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
持続的な安全性を持つ暗号・電子署名アルゴリズム技術の関する研究開発～安全な暗号技術を利用し続けるための暗号利用フレームワーク～
次世代ハッシュ関数の研究開発
適切な暗号技術を選択可能とするための新しい暗号等技術の評価指標～暗号の技術的評価に関する研究開発～
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と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19年11月22日から12月21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。

ソフトバンクテレコム株式会社
株式会社トリニティーセキュリティーシステムズ

(2) 調査

警察庁が平成19年11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600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」又は「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

北海道情報大学
岩手県立大学
石巻専修大学
信州大学
岡山大学
広島大学
熊本大学

イ 企業

アイ・ビー・エス・ジャパン株式会社
エクストリームネットワークス株式会社
NTTコミュニケーションズ株式会社
東北インテリジェント通信株式会社

（別添1）

対象技術 その他認証技術

テーマ名 ユビキタスネットワーク認証・エージェント技術の研究開発

開発年度 平成15年度～平成19年度

実施主体 (株)日立製作所 （総務省からの委託）

背景、目的

ユビキタスネットワークの進展とともに、地球上のあらゆる場所までネットワークが張り巡らされ、ユーザは自由に会話したり、情報コンテンツへ自由にアクセスできるようになる。一方これに伴い、通信内容の漏洩や不正な情報へのアクセスによって、ユーザのプライバシーが侵害されたり、データの遺失が発生したりする危険性が増加している。従来の中央集中型の認証システムでは、認証サーバに対して大量の端末・機器からのアクセス要求が発生するとサーバ処理がボトルネックとなる問題があった。また、認証サーバの障害がサービス全体に影響を及ぼすという問題や、ユーザ毎やサービス提供場所毎にきめ細かなセキュリティポリシを設定して認証・認可を行うには管理コストがかかり過ぎるという問題があった。これらの問題を解決し、いつでも、どこでも安心してコミュニケーションや電子商取引を行える、高性能かつ高信頼な分散型認証プラットフォーム技術を確立する。

研究開発状況（概要）

（1） 端末の位置情報やユーザの履歴情報等のコンテキスト情報を収集し、状況を判断して認証・認可を行うコンテキスト・アウェア利用者認証技術を開発。

（2） モバイルユーザに対して、異なるセキュリティレイヤ／ドメイン間で認証関連情報を安全かつ高効率に交換可能な認証エージェント連携技術を開発。

（3） 分散化した機器や提供される個々のサービスに対するアクセス制御ルールを動的かつ高効率に生成し配布するアクセス制御ポリシ自動構成技術を開発。

（4） ネットワークの利用状況に応じてピア・ツウ・ピアな通信経路を動的かつ階層的に構成し、これらの通信経路を利用して高効率なデータ交換を可能とする仮想アクセス空間構成・利用技術を開発。

上記技術の試作及び実フィールドでの実証評価を実施。

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）

(株)日立製作所システム開発研究所 045-860-3088

将来の方向性

上記認証プラットホーム技術を確立し、高度情報通信ネットワーク社会の安全性・信頼性の確保に資する。

対象技術 侵入検知技術

テーマ名 広域モニタリングシステムに関する基盤技術の研究開発

開発年度 平成16年度～平成18年度

実施主体 横河電機(株)、(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した。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した。

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。
(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。

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した。

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。
(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。

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した。

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。
(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

- H19.1.25 モバイル属性認証実証実験を実施。
- 平成18年度末に開発終了。
- 現在、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した。

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。

(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。

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した。本研究の結果として得られた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。

(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。

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12月18日 実験システムデモを実施。

・ 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した。

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。

(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。

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　その他認証技術

テーマ名　持続的な安全性を持つ暗号・電子署名アルゴリズム技術に関する研究開発
～安全な暗号技術を利用し続けるための暗号利用フレームワーク～

開発年度　平成19年度～平成21年度

実施主体　株式会社エヌ・ティ・ティ・データ
（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

計算機の演算能力の向上や暗号に対する解読技術の進展などを背景として、電子政府推奨暗号を始めとする暗号は、常に危殆化の危険にさらされている。暗号危殆化に関して、特に深刻な影響が予想されるのは、危殆化した公開鍵暗号アルゴリズムから計算された秘密鍵が漏洩するという問題である。また、ハッシュ関数が危殆化した場合においても、電子署名付き文書の改ざんや偽造文書へのすり替えという問題が起こり得る可能性があると考えられる。

こうした問題への対応策としては、より安全な公開鍵暗号アルゴリズムやハッシュ関数への移行が必要となるが、既に生成された電子署名付き文書や暗号化データがシステムやアプリケーションをまたがって分散された環境に広く流通している場合があり、移行上の制約要因となっている。

他方、既存の暗号技術においては、秘密鍵の漏洩などへの対処は考慮されているが、危殆化が発生した際に、電子署名及び暗号化データの有効性を継続的に保証することまでは考慮されていない。したがって、電子署名の更新を行う場合には、最初に電子署名生成者にデータを全て戻し、そのデータに対して安全なアルゴリズムで電子署名を再計算する必要がある。このため、これら一連の電子署名の更新に係る過重なコスト負担がネックとなり、危殆化対策が立ち行かなくなることが懸念されている。また、ネットワーク上のサーバやストレージ等にレプリケーションされたデータやRFIDタグに格納されている情報、デジタルコンテンツなどとして広く流通している暗号化データの再暗号化を行う場合においても、同様な問題が存在する。

このような状況を踏まえ、本研究開発では、危殆化対策の一環として、安全性や利便性、危殆化対策に係るコスト低減を十分考慮しつつ、電子署名の更新及び暗号化データの再暗号化を可能とし、それらの有効性を継続的に保証するための技術を確立する。

研究開発状況（概要）

・平成19年度より以下の研究開発を実施予定。
(1) 電子署名及び暗号化データの有効性を継続的に保証するための仕組みとその最適化手法
(2) 電子署名更新技術
(3) 再暗号化技術
・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

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

対象技術 その他認証技術

テーマ名 次世代ハッシュ関数の研究開発

開発年度 平成19年度～平成21年度

実施主体 株式会社日立製作所、国立大学法人神戸大学、国立大学法人福井大学
（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

電子データの真正性確保やユビキタス機器を利用したシステムおけるユーザの認証などを実現するための技術など、安心・安全のための情報通信技術の必要性が高まっている。また、ユビキタス環境では、情報を発信・受信する計算機・端末が、サーバ、従来のPCといった処理能力に優れたものから、携帯電話やICカード等の小型で比較的制限が多い電子機器と多様化しており、これらの機能は、多様なプラットフォームで利用可能である必要がある。

このような課題の解決手段として、メッセージ認証子を用いて、改ざん検知や機器認証を行う方法や電子署名を用いて電子文書の真正性を確保する方法が利用されている。これらの方法はいずれもハッシュ関数を利用しており、ハッシュ関数の安全性がこれらの技術の根幹となっている。しかし、近年の学会において、現在最も広範に用いられている専用ハッシュ関数であるSHA-1やMD5が、衝突耐性という安全性に関して脆弱であることが報告されている。

このような背景から、安心・安全のための情報通信技術の研究開発の一環として、本研究では、下記に示すようなハッシュ関数（専用ハッシュ関数）を次世代ハッシュ関数と定め、その実現のための研究開発を実施する。

・次世代ハッシュ関数

衝突困難性、一方向性、第二原像困難性など、一般的にハッシュ関数に求められる安全性に関して理論的な根拠を有すること。

実運用上の各種安全性要件に応じた安全性強度を有すること。

多様な実装条件下における実装性能に優れた汎用性を有すること。

研究開発状況（概要）

・平成19年度より以下の研究開発を実施予定。

(1) 次世代ハッシュ関数の設計技術

(2) 次世代ハッシュ関数の実装技術

・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

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 適切な暗号技術を選択可能とするための新しい暗号等技術の評価手法
～暗号の技術的評価に関する研究開発～

開発年度 平成19年度～平成21年度

実施主体 富士通株式会社
（情報通信研究機構（NICT）が実施する委託研究の委託先）

背景、目的

暗号に対する解読技術は日進月歩発展を遂げており、電子政府推奨暗号を始めとする暗号は、常に危殆化の危険にさらされている。広範な用途に利用されている公開鍵暗号技術であるRSA暗号においては、素因数分解問題の困難性を安全性の根拠としていたが、計算機の演算能力の向上から素因数分解が可能となる桁数が増えてきている。このような状況から、RSA暗号の次段階として、RSA暗号と比較して、より短い鍵長で同等の強度を実現できる、楕円曲線暗号が期待されている。

しかしながら、楕円曲線暗号においては、一方向性関数の性質により、演算を行うことが非常に困難となる楕円曲線上の離散対数問題を安全性の根拠としているが、素因数分解問題の困難性を安全性の根拠とするRSA暗号と比べて、解読技術の研究開発や暗号強度等安全性の評価が必ずしも十分なされているとは言えないのが現状である。このような状況から、暗号に関する研究者の間に、楕円曲線暗号の安全性に対して疑問視する声があるのも事実である。

他方、複数の異なる暗号要素技術を組み合わせて使用するシステム等では、これらの暗号要素技術間の強度、性能のトレードオフを検討する必要があり、その際、鍵長と強度との関係を比較した、米国NISTのFIPS800-57（次頁の表１及び表2を参照）などが参考にされている。

しかしながら、これらについては、実験データが明らかになっておらず、データの入手についても制約を伴うことから、その実験結果が本当に正しいかどうかを付加的に検証することが困難となっている。

さらに、楕円曲線暗号の攻撃手法は、一般的な楕円曲線に適用できる手法、特殊な楕円曲線に適用できる手法など幾つか考えられており、使用される楕円曲線の種類も何種類か存在するが、攻撃実験を基にした、同一の評価基準による楕円曲線相互の暗号強度比較・評価・検証はこれまで行われていないのが実態である。

このような状況を踏まえ、本研究開発では、一般的な楕円曲線暗号を中心として、実際に攻撃実験を行い、その実験データを基に、各種楕円曲線間の鍵長と強度の比較や、RSA暗号等他の暗号要素技術との強度比較をより精密に行う。また併せて、鍵長の寿命を予測することにより、鍵更新時期などの運用方針に役立てるとともに、複数の異なる暗号要素技術を組み合わせて使用するシステム等での強度バランスを明確にする

研究開発状況（概要）

・平成19年度より以下の研究開発を実施予定。

（1） 攻撃プログラムの設計・開発

（2） 暗号強度比較・評価・検証技術

・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

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19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、マルウエアの収集機構を整備するとともに収集したマルウエアの分析機構の開発に着手した．マルウエアの分析結果を用いて観測点からのセキュリティログの分析精度を向上する手法の研究に着手した。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、異なる機関に属する複数の観測点で収集したログから、共通の攻撃をその組織が有する情報を、互いに開示することなく、解析する技術の開発に着手した。攻撃ベクタの捕捉能力と解析能力の向上のため、仮想マシンモニタを用いて不正アクセス発生時点のメモリ、ディスク内容を捕捉する研究に着手した。またメモリ内容を自動分類し、高精度でメモリ内の攻撃ベクタを捕捉できる機械学習アルゴリズムの開発に着手した。

詳細の入手方法(関連部署名及びその連絡先)

独立行政法人情報通信研究機構　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 次世代型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)

〒105-0011
東京都港区芝公園3－5－8　機械振興会館3階
財団法人日本情報処理開発協会　電子商取引推進センター
主任部員　　藤本　昌宏
電話番号:03-3436-7511
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　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～平成19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を活用するための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を利用して医療情報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）

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した成果をふまえ、TPMを搭載したPCにおける情報資産の重要性に応じた運用管理マニュアルを作成する。

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並びに運用管理マニュアル等の成果は、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　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～平成19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）

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」の技術開発を行い、実験運用を開始した。

また電子認証の適切な普及に役立つノウハウをドキュメント化するため「電子認証プラクティスフォーラム」を立ち上げ、各組織の共通ノウハウを蓄積する仕組みの開発と実験を行っている。

詳細の入手方法（関連部署名及びその連絡先）

〒101-0047
東京都千代田区内神田2－3－4　国際興業神田ビル6階
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、我が国に対するインターネットにおけるIPアドレスの不正利用を排除し、安全・安心な電子認証基盤の構築が望まれる。また、電子認証に関する汎用的なノウハウが継続的に更新されていく体制作りが必要である。

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。

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基礎技術開発を行い、複数の重要な基盤技術を開発した。さらに、リーディング企業とのパートナーシップの下、数十プロセッサを越える分散型組込系システムのセキュリティアーキテクチャを開発した。

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

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18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洩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（フェー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いた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19年度までに、以下のような特徴を持つ認証・データ管理方式のプロトタイプ実装を行いアイデアが実現可能であることを示した。1）不正アクセスにより記録情報が漏えいしたり、認証トークンや携帯端末などが盗まれたりしたとしても、それらから、保存されている平文やパスワードを求めることが困難。2）一つのノードがクラッシュしたとしても保存データの復元が可能。3）フィッシング詐欺などにより入力パスワードが取られたとしても利用者へのなりすましが困難。

また、実行時に攻撃によりウィルス等の不正コードを実行させられることを防ぐ安全性検証機能付きC言語コンパイラについて、実用プログラムを処理できる処理系を完成させ、ホームページ上で一般に公開した。

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 Web: http://www.rcis.aist.go.jp/

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。本事業で開発した技術については、継続的に開発維持を行い、実用に供していく。

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）

本研究において開発したシステムの構成は下図の通りである。

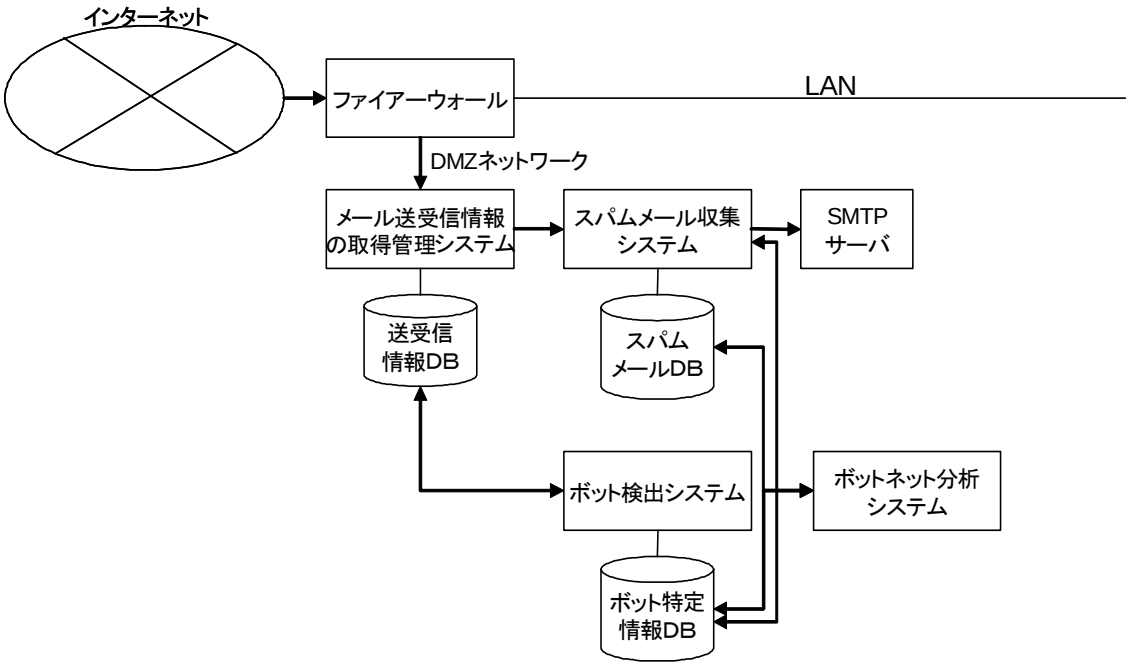

図 1:開発成果物の構成

ファイヤー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グループ　グループリーダー　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

ボットネット検知の精度を高めるために、本研究によりボットのIPアドレスと推定されるデータと、既存のボットのIPアドレスデータとの比較を行う。その上で、本システムのユーザサイトにおける運用を目的として、商用化を視野に入れた開発を行う。

（別添2）

企業名（及び略称） ソフトバンクテレコム株式会社	
代表者氏名　　専務取締役CTO　弓削　哲也	
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　045(451)4502	
URL　http://www.softbanktelecom.co.jp/	
対象技術	技術開発状況
ファイアウォール技術 （2007年）	外出先から（公衆無線LANや携帯電話によるインターネットアクセスなどにより）社内ネットワークにアクセスするリモートアクセスが広く利用されているが、利用者がその利用中に異なるネットワーク（公衆無線LAN⇔携帯電話等）の間を移動する場合には、安全性と利便性に関して、以下の①～③にあげる課題がある。 ①　接続に関する処理が移動の度に必要 移動の度に現在の場所に最適なネットワークの検索およびその接続処理、社内ネットワークへのIPSec等の接続処理が必要となる。 ②　移動前後で接続セッションが切断 移動の度にIPSec等のセッションおよび利用中の業務サーバとのセッションが切断されて、アプリケーションが中断する。 ③　セキュリティ上の問題 社内の顧客情報等の重要な情報が、社外のどのような場所からでも閲覧できる。 以上の課題を単一のシステムで解決可能な「セキュリティを確保したまま、かつFMC環境下で快適に利用できるリモートアクセス」を実現する。主な特徴は以下の通りである。 【特徴1】ネットワークへの自動接続 現在の場所に応じた最適なネットワークおよび、あらかじめ定められたポリシーに従って、社内ネットワークに自動的に（複雑な操作不要で）接続する。 【特徴2】暗号化セッションを含むシームレスハンドオーバ 移動しても、利用中の社内ネットワークへのIPSec等の接続およびアプリケーションとのセッションが継続されて、再接続する必要がない。 【特徴3】場所に応じたアクセス制御 あらかじめ管理者が登録した場所（IPアドレス）ごとに、社内ネットワークへのアクセスポリシーを定めることができる。

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	経営企画本部　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。

（別添3）

【大学】

大学名　北海道情報大学	
所在地（郵便番号及び住所）　〒069-8585　北海道江別市西野幌59-2	
関連部署名及び電話番号　011-385-4411	
URL　http://www.do-johodai.ac.jp/	
対象技術	技術開発状況
ネットワーク サーバ データ	学内の実習設備および学内外からのメールサーバに対するアクセスを統合した認証を行い管理する。本学で利用する事を目的としているので製品化はしていない。

大学名　岩手県立大学	
所在地（郵便番号及び住所）　〒020-0173　岩手県岩手郡滝沢村滝沢字巣子152-89	
関連部署名及び電話番号　研究・地域連携室 019-694-3330	
URL　http://www.iwate-pu.ac.jp/	
対象技術	技術開発状況
サーバ クライアント	1.　RSA公開鍵方式による強固な個人認証を高速に安価に実行する半導体プロセッサチップを提供。 2. プロセッサ自体は、独自開発した64ビット汎用プロセッサにRSA秘密鍵を安全に保管する機構およびRSA公開鍵方式によるデジタル署名計算を高速に実行する機構を付加したもの。 3. ゲート規模約52000ゲート、消費電力約7mw、1024ビットデジタル署名計算時間約260ms 4. 住基カードの次世代版チップを狙ったもの。 5. VDEC機構の協力を得て4.9mm角チップを実現すみ。

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　0225-22-7711	
URL　http://www.emerging.jp/pegriot/j-crypt/	
対象技術	技術開発状況
クライアント	管理者がグループ員の情報管理状況を的確に把握し、監視・指導できるシステム。本システムは、情報の漏えいを防ぐのみならず、情報管理に対する意識を高める教育にも大いに役立ちます。

大学名　信州大学工学部	
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　026-269-5003	
http://wwweng.cs.shinshu-u.ac.jp/	
対象技術	技術開発状況
ネットワーク サーバ 通信技術 データ	RSA暗号処理の高速化。

大学名　岡山大学総合情報基盤センター	
所在地（郵便番号及び住所）　〒700-8530　岡山県岡山市津島中1-3-1	
関連部署名及び電話番号　086-251-7232	
URL　http://www.okayama-u.ac.jp/user/cc/	
対象技術	技術開発状況
データ	大学などの組織においてLANアクセス環境を提供する場合、特に学会などのイベント開催時には組織内利用者とそれ以外の利用者（部外者）が混在して利用することが多い。このような場合、部外者でも組織内限定サービスを利用できるなどの問題が生じる。 この問題に対して、本システムでは、部外者からの組織内限定サービスへのアクセス保護を、管理コストを増加させずに可能にする。すなわち、部外者が組織内限定サービスへアクセスした場合でも、サーバ側での設定に基づいたアクセス制御を行うことが可能である。 また、本システムは既存の組織内ネットワークを利用するため、LANアクセス環境の提供が場所によらず容易に行えるという特徴を持つ。

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.ferec.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し、ネットワークへの不正アクセスを防止する。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。

大学名　熊本大学総合情報基盤センター	
所在地(郵便番号及び住所)　〒860-0081　熊本県熊本市黒髪2-39-1	
関連部署名及び電話番号　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	1.現在プロトタイプです。 2.毎日DNSクエリアクセスのログ解析を自動的に行います。 3.組織内からランダムに組織外サイトを攻撃するボット等を検出します。

【企業】

事業体(研究所)名　アイ・ビー・エス・ジャパン株式会社	
所在地（郵便番号及び住所）　〒243-0432　神奈川県海老名市中央2-9-50 海老名プライムタワー12F	
関連部署及び電話番号　ソリューション技術部 046-234-9200	
URL　http://www.ibsjapan.co.jp/Catalog/Software/Security/N-Stealth.html	
対象技術	技術開発状況
サーバ	■N-Stalker Infastructure EditionInfrastructureエディションは、従来のN-Stealthセキュリティと特許申請中のコンポーネントごとのWEBアプリケーションセキュリティスキャン技術を使って、3万5千点以上のWEBアプリケーションでの脆弱性を指摘します。 ■N-Stalker Enterprise EditionEnterpriseエディションでは、開発・QA段階から、デプロイメント、プロダクション過程における、総合的なWEBアプリケーションの脆弱性を、N-Stealthの3万5千点以上のデータベースおよび特許申請中のコンポーネントごとのWEBアプリケーションセキュリティスキャン技術を使って指摘します。 N-StealthはWEBサーバのセキュリティ上の脆弱性を事前に見つけることにより、ハッカーの侵入を防ぎます。N-Stealthは3万件以上の脆弱性を網羅しています。剛健なWEBサーバの構築、メンテナンスに必須です。N-Stealthはローカルおよびリモート双方のWEBサーバをスキャンします。IPアドレスを入力し、ランするだけの簡単操作で、数分でサーバの脆弱性をレポートします。 ITコンサルタント、システム管理者、ITプロフェッショナルにご利用いただけます。 ・3万5千件以上の脆弱性チェック ・SANS／FBI（www.sans.org）トップ10／20をスキャン ・HTTPおよびHTTPS（SSL）をサポート ・N-Stealthログアナライザ --WEBサーバーログをスキャンし、ハッカーの攻撃をモニター ・OS検出 ・FastTrackにより速い検出 ・侵入検出およびそのテスト ・プロキシサーバーサポート ・グラフィックなレポートテンプレート ・バーチャルホストのサポート ・リモートスキャン -テストしたいシステムにソフトをインストールすることはありません ・False positiveフィルター ・バッファオーバーフローエンジン ・Bugtraq／CVE互換

事業体(研究所)名　アイ・ビー・エス・ジャパン株式会社	
所在地(郵便番号及び住所)　〒243-0432　神奈川県海老名市中央2-9-50 海老名プライムタワー12F	
関連部署及び電話番号　ソリューション技術部 046-234-9200	
URL　http://www.ibsjapan.co.jp/Catalog/Software/Security/AnthaVPN.html	
対象技術	技術開発状況
通信情報	高いセキュリティをポケットの中に。AnthaVPNはWindows Mobile5.0端末の、IPSECクライアントです。主要VPNゲートウェイをサポートしているため、既存環境での利用が可能です。 ・セキュアーで標準規格に対応したネットワークアクセス anthaVPNは、多くのVPNゲートウェイに対応した、モバイル用にデザインされたIPSecクライアントです。IPSec VPNのデファクトスタンダードといえるanthaVPNは、既存のゲートウェイでの動作を可能にするので、新たなインフラ構築の時間と費用を削減する事が出来ます。 ・高性能で強力なセキュリティ anthaVPNは、強力なセキュリティを提供しながらRSA Soft Tokenのような認証オプションに沿った現在および、過去のアルゴリズムをサポートします。Certicomの特化されたデバイスの専門知識と、モバイルデバイスをセキュアーにする理想的なECCの組込により、高い性能が維持されています。 ・最も強力な政府のセキュリティ基準に合致 anthaVPNは、厳しい政府のセキュリティ基準に合致し、今日の政府のシステムで動作可能であり、更に強力な認証のためのDDCAC(Department of Defense Common Access Card)に対応しています。 ・非常にシンプルでわかりやすいユーザーインターフェース ・日本国内、外の多くのVPNゲートウェイで利用可能 ・パラメータの受け渡しにより、ユーザーアプリとの連動が可能

事業体(研究所)名　エクストリームネットワークス株式会社	
所在地(郵便番号及び住所)　〒112-0002　東京都文京区小石川1-4-1 住友不動産後楽園ビル17F	
関連部署及び電話番号　03-5842-4011	
URL　http://www.extremenetworks.co.jp/products/blackdiamond/index.htm http://www.extremenetworks.co.jp/products/summit/index.htm http://www.extremenetworks.co.jp/technology/universal_port/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	Chassis型のL2／L3スイッチであるBlackDiamondシリーズ、およびBox型のL2／L3スイッチであるSummitシリーズを提供。これら製品上で動作するOS“ExtremeXOS”は、CPU DoS Protection, ACL, Protocol Anormary Detection, 各種L2／L3セキュリティやネットワークログイン認証機能などのセキュリティ機能を提供。また、一部のハイエンド製品ではCLEAR-Flowによるリアルタイムなディープパケットインスペクションが可能。 さらに、ネットワークログイン認証によるログイン／ログオフなどのイベントをトリガとしたダイナミックプロビジョニングを可能にするユニバーサルポート機能を提供し、セキュアなプラグアンドプレイを実現。

事業体(研究所)名　エクストリームネットワークス株式会社	
所在地(郵便番号及び住所)　〒112-0002　東京都文京区小石川1-4-1 住友不動産後楽園ビル17F	
関連部署及び電話番号　03-5842-4011	
URL　http://www.extremenetworks.co.jp/products/SecurityAppliances/sentriant.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	SentriantはOut-of-Band接続による脅威の検知／隔離が可能なセキュリティアプライアンス。ビヘイビアベースの脅威検知方法を採用しており、シグネチャや経験則に基づかずに攻撃発生時にシグネチャが存在しない新たな脅威も検知することが可能。 また、未使用IPアドレス スペースを利用して脅威を確認する機能を提供。 また、弊社スイッチ製品の提供するCLEAR-Flowとの組み合わせにより、ギガビット／10ギガビットで構築されたネットワーク全体を広範囲に監視可能。

事業体(研究所)名　NTTコミュニケーションズ株式会社　先端IPアーキテクチャセンタ	
所在地(郵便番号及び住所)　〒160-0023　東京都新宿区西新宿3-20-2 東京オペラシティタワー21F	
関連部署及び電話番号　03-6800-3250	
URL　http://www.ocn.ne.jp/business/vpn/mpvpn	
対象技術	技術開発状況
通信情報	SIP技術、IPv6技術を融合させて、IPv6端末、機器ごとに個別の暗号化通信・アクセス制御・複数のVPN構築などを自在にできるようにするサービス。

事業体(研究所)名　東北インテリジェント通信株式会社	
所在地(郵便番号及び住所)　〒980-0811　宮城県仙台市青葉区一番町3-7-1電力ビル	
関連部署及び電話番号　技術本部技術部 022-799-4221	
URL　http://www.tohknet.co.jp/corp/internet/gateway/index.html	
対象技術	技術開発状況
ネットワーク	高速イーサネット(V-LAN)の閉域網からインタネット接続を行う時のファイアウォールサービスを提供する。