

平成23年3月3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22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22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22年中に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22年中の不正アクセス行為の認知件数は1,885件で、前年と比べ、910件減少した。

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18年	平成19年	平成20年	平成21年	平成22年
認知件数 (件)		946	1,818	2,289	2,795	1,885
	海外からのアクセス	37	79	214	40	57
	国内からのアクセス	855	1,684	1,993	2,673	1,755
	アクセス元不明	54	55	82	82	73

##### (2) 被害に係る特定電子計算機のアクセス管理者<sup>注1</sup>

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(1,405件)、次いで一般企業(457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18年	平成19年	平成20年	平成21年	平成22年
プロバイダ (件)		602	1,372	1,589	2,321	1,405
一般企業		325	437	685	466	457
大学、研究機関等		6	1	5	4	2
その他		13	8	10	4	21
	うち行政機関	5	5	6	3	13
不明		0	0	0	0	0
計		946	1,818	2,289	2,795	1,885

「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。

注1 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となる。

(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（1,488件）、次いで利用権者<sup>注2</sup>からの届出によるもの（314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（66件）、発見者からの通報によるもの（9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 18年	平成 19年	平成 20年	平成 21年	平成 22年
警察活動（件）		535	1,326	1,567	2,277	1,488
利用権者からの届出		358	415	656	487	314
アクセス管理者からの届出		45	61	60	21	66
発見者からの通報		3	2	4	7	9
その他		5	14	2	3	8
計		946	1,818	2,289	2,795	1,885

(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、情報の不正入手（個人情報の不正入手）が最も多く（1,453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）（255件）、ホームページの改ざん・消去（45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<sup>注3</sup>用ホームページデータの蔵置）（40件）、インターネットバンキングの不正送金（22件）、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）（10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21年	平成22年
情報の不正入手（件）		185	1,453
オンラインゲームの不正操作		345	255
ホームページの改ざん・消去		33	45
不正ファイルの蔵置		2	40
インターネットバンキングの不正送金		34	22
インターネット・オークションの不正操作		2,152	10
その他		44	60

注2 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、当該特定電子計算機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 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。

## 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22年中における不正アクセス禁止法違反の検挙件数は1,601件、検挙人員は125人と、前年と比べ、検挙件数は933件減少し、検挙人員は11人増加した。その内訳をみると、不正アクセス行為に係るものがそれぞれ1,598件、123人、不正アクセス助長行為<sup>注4</sup>に係るものがそれぞれ3件、4人であった。

表2 - 1 検挙件数等の推移

区分		年次				
		平成18年	平成19年	平成20年	平成21年	平成22年
不正アクセス行為	検挙件数	698	1,438	1,737	2,532	1,598
	検挙事件数 <sup>注5</sup>	84	86	101	95	103
	検挙人員	130	126	135	114	123
不正アクセス助長行為	検挙件数	5	4	3	2	3
	検挙事件数	3	2	3	1	3
	検挙人員	5	4	3	1	4
計	検挙件数 (件)	703	1,442	1,740	2,534	1,601
	検挙事件数 (事件)	84 (重複3)	86 (重複2)	101 (重複3)	95 (重複1)	104 (重複2)
	検挙人員 (人)	130 (重複5)	126 (重複4)	137 (重複1)	114 (重複1)	125 (重複2)

(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<sup>注6</sup>が1,597件であり、セキュリティ・ホール攻撃型<sup>注7</sup>は1件であった。

注4 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 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。

注7 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。

表2 - 2 不正アクセス行為の態様の推移

区分		年次	平成18年	平成19年	平成20年	平成21年	平成22年
識別符号窃用型	検挙件数		698	1,438	1,736	2,529	1,597
	検挙事件数		84	86	100	94	102
セキュリティ・ホール攻撃型	検挙件数		0	0	1	3	1
	検挙事件数		0	0	1	1	1
計	検挙件数 (件)		698	1,438	1,737	2,532	1,598
	検挙事件数 (事件)		84	86	101	95	103

### 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の(1,411件)が最も多く、次いで、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(70件)、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(57件)となっている。また、スパイウェア<sup>注8</sup>等のプログラムを使用して識別符号を入手したものの(14件)、共犯者等から入手したものの(12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(12件)等も依然として発生している。

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21年	平成22年
識別符号窃用型 (件)		2,529	1,597
フィッシングサイトにより入手したものの		2,084	1,411
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の		58	70
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		61	57
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の		8	14
共犯者等から入手したものの		167	12
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		12	12
他人から購入したものの		92	4
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の		0	0
その他		47	17
セキュリティ・ホール攻撃型		3	1

注8 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。

(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、元交際相手や元従業員等の顔見知りの者によるものが最も多く（65人）、次いで交友関係のない他人によるもの（36人）、ネットワーク上の知り合いによるもの（24人）となっている。

また、被疑者の年齢についてみると、20歳代（39人）が最も多く、30歳代（35人）、10歳代（29人）、40歳代（17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58歳であった。

表3 - 2 年代別被疑者数の推移

区分 \ 年次	平成18年	平成19年	平成20年	平成21年	平成22年
10歳代（人）	40	39	48	31	29
20歳代	44	39	42	33	39
30歳代	28	34	35	35	35
40歳代	15	12	11	13	17
50歳代	2	2	1	2	5
60歳代	1	0	0	0	0
計	130	126	137	114	125

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（1,455件）が最も多く、次いで嫌がらせや仕返しのため（66件）、好奇心を満たすため（33件）、オンラインゲームで不正操作を行うため（19件）、顧客データの収集等情報を不正に入手するため（18件）、料金の請求を免れるため（4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21年	平成22年
不正に金を得るため（件）	2,245	1,455
嫌がらせや仕返しのため	34	66
好奇心を満たすため	165	33
オンラインゲームで不正操作を行うため	63	19
顧客データの収集等情報を不正に入手するため	19	18
料金の請求を免れるため	4	4
その他	2	3
計	2,532	1,598

(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（1,597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、会員専用・社員用内部サイトが最も多く（1,432件）、次いでオンラインゲーム（71件）、電子メール（36件）、ホームページ公開サービス（25件）、インターネットショッピング（16件）、インターネットバンキング（7件）、インターネット・オークション（2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21年	平成22年
識別符号窃用型（件）		2,529	1,597
会員専用・社員用内部サイト		10	1,432
オンラインゲーム		88	71
電子メール		167	36
ホームページ公開サービス		16	25
インターネットショッピング		3	16
インターネットバンキング		83	7
インターネット・オークション		2,147	2
その他		15	8

4 都道府県公安委員会による援助措置

平成22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・指導はなかった。

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18年	平成19年	平成20年	平成21年	平成22年
援助措置（件）		3	0	1	0	0

5 防御上の留意事項

(1) 利用権者の講ずべき措置

ア フィッシングに対する注意

電子メールにより本物のウェブサイトに酷似したフィッシングサイトに誘導し、ID・パスワードやクレジットカード情報を不正に取得する事案が多発していることから、発信元に心当たりのない電子メールに注意する。また、金融機関等が電子メールで口座番号や暗証番号、個人情報を問い合わせることはなく、これらの情報の入力を求める電子メールはフィッシングメールであると考えられることから、情報を入力しない。

## イ スパイウェア等の不正プログラムに対する注意

ファイル共有ソフトやウェブサイト上に蔵置したファイルを用い、スパイウェア等の不正プログラムに感染させ、他人の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、信頼できないファイルを不用意に開いたり、ダウンロードしたりしない。また、不特定多数が利用するコンピュータでは重要な情報を入力しない。さらに、スパイウェア対策やコンピュータ・ウイルス対策（対策ソフト、オペレーティングシステム及びソフトウェアのアップデート等）を適切に講ずる。

## ウ パスワードの適切な設定・管理

利用権者のパスワードの設定の甘さにつけ込んだ不正アクセス行為、知人等による不正アクセス行為、他人から購入したID・パスワードによる不正アクセス行為が発生していることから、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やIDの一部を使ったパスワード等、パスワードの推測が容易なものは避ける、複数のサイトで同じパスワードを使用しないなどの対策を講じる。また、パスワードを定期的に変更する、知人等に自己の識別符号の一時利用を認められた際は、その利用が終了した時点で確実にパスワードを変更するなどパスワードは適切に管理する。

## (2) アクセス管理者等の講ずべき措置

### ア フィッシング、スパイウェア等への対策

フィッシング、スパイウェア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、インターネットショッピング、オンラインゲーム、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つては、ワンタイムパスワード<sup>注9</sup>等により個人認証を強化するなどの対策を講ずる。

### イ SQLインジェクション攻撃<sup>注10</sup>への対応

セキュリティホール攻撃の一つであるSQLインジェクション攻撃を受け、クレジットカード番号等の個人情報が大量に流出する事案が発生していることから、アクセス管理者は、プログラムを点検してセキュリティ上の脆弱性を解消するとともに、攻撃の兆候を即座に検知するための侵入検知システム等を導入し、SQLインジェクション攻撃に対する監視体制を強化する。

### ウ ウェブサイトの安全な管理

ウェブサイト管理用のID・パスワードが不正に取得されて、アクセス管理者の意図しない命令が入力され、ウェブサイトが閲覧された際にその命令が実行され、閲覧者をウイルス等が蔵置されたウェブサイトに誘導する事案が多発したことから、アクセス管理者は、ウェブサイトの更新の際には、ID・パスワードを暗号化することや更新に利用する端末を限定することなどにより安全な管理を徹底する。

注9 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つて、認証の度にそれを構成する文字列が変わるものをいう。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 SQLというプログラム言語を用いて、企業等が個人情報を管理するデータベースを外部から不正に操作する行為をいう。

## エ 識別符号の適切な管理

識別符号を知り得る立場にあった元従業員による不正アクセス行為も引き続き発生していることから、従業員が退職した時や特定電子計算機を利用する立場でなくなった時には、当該従業員に割り当てていたIDを削除したり、パスワードを変更したりするなど識別符号の適切な管理を徹底する。

## オ パスワードの適切な設定・運用体制の構築

利用権者のパスワードの設定の甘さにつけ込んだ不正アクセス行為が発生していることから、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したり、定期的にパスワードの変更を促す仕組みを構築したりするなどの措置を講ずる。

## 6 検挙事例

1	<b>フィッシングにより他人のID・パスワードやクレジットカード番号等を不正に入手し、インターネットショッピングにおいて商品をだまし取った不正アクセス禁止法違反及び詐欺事件</b>
---	--

無職の男(32)らは、平成20年9月から平成21年11月までの間、フィッシングにより他人のID・パスワードやクレジットカード番号等を入手し、会員専用サイトに不正アクセスを行い、個人情報を入力した上、それを用いて他人になりすましてインターネットショッピングにおいて商品をだまし取った。平成22年8月までに、不正アクセス禁止法違反及び詐欺罪で検挙した(広島、岡山、静岡、福岡、愛媛)。

2	<b>スパイウェアにより他人のID・パスワードを不正に取得し、オンラインゲームに不正アクセスするなどした不正アクセス禁止法違反事件</b>
---	---

会社員の男(29)らは、平成22年4月から6月までの間、スパイウェアを組み込んだウェブサイトを開設して他人のID・パスワードを不正に取得し、それを用いてオンラインゲームに不正アクセスを行い、入手したオンラインゲーム上のアイテムを現金に換金した。平成22年11月、不正アクセス禁止法違反で検挙した(神奈川)。

3	<b>他人のID・パスワードを使用して航空会社のウェブサイト不正アクセスを行い、マイレージをだまし取るなどした不正アクセス禁止法違反及び電子計算機使用詐欺等事件</b>
---	--

会社員の男(52)は、平成20年6月、取引先会社従業員のID・パスワードを使用して航空会社のウェブサイト不正アクセスを行い、同人の口座内のマイレージを自らが同人名義で開設したインターネットショッピングサイト内の口座に移し替え、それを使用して商品を購入した。平成22年4月、不正アクセス禁止法違反、電子計算機使用詐欺罪等で検挙した(警視庁)。

4	パスワード再発行機能を悪用して他人のID・パスワードを不正入手し、オンラインゲームに不正アクセスするなどした不正アクセス禁止法違反等事件
---	--

無職の少年（18）らは、平成22年2月から3月までの間、オンラインゲームのパスワード再発行機能を悪用して他人のID・パスワードを不正に入手した上、それを用いてオンラインゲームに不正アクセスを行い、入手したオンラインゲームのアイテムや仮想通貨を現金に換金した。平成22年9月までに、不正アクセス禁止法違反等で検挙した（愛知、宮城、福島）。

5	フィッシングにより他人のID・パスワードを不正に入手してSNS <sup>注11</sup> に不正アクセスを行い、女性会員になりすまして出会い系サイトに勧誘した不正アクセス禁止法違反等事件
---	---

無職の男（24）らは、平成20年8月、フィッシングにより入手した他人のID・パスワードを用いてSNSに不正アクセスを行い、女性会員になりすましてSNSで出会った者に電子メールを送信し、自らが経営する出会い系サイトに誘導した。平成22年3月までに、不正アクセス禁止法違反等で検挙した（警視庁、宮城）。

注11 ソーシャルネットワーキングサービス（Social Networking Service）の略。登録したユーザのみが参加できるインターネット上のウェブサイトをいう。

## 第2 不正アクセス関連行為の関係団体への届出状況について

### 1 独立法人情報処理推進機構（IPA）に届出のあったコンピュータ不正アクセスの届出状況について

平成22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197件（平成21年：149件）であった。（注2）

平成22（2010）年は同21（2009）年と比べて、48件（約32%）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、「侵入」および「なりすまし」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365件（平成21年：254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309件（平成21年：211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。

18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。

152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60件である。

#### 【主な内容】

パスワード推測：21件

ソフトウェアの脆弱性やバグを利用した攻撃：11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139件の届出があった。

【主な内容】

ファイル等の改ざん、破壊等：48件

資源利用（ファイル、CPU使用）：43件

プログラムの作成・設置（インストール）、トロイの木馬などの埋め込み等：31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：14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。8件（平成21年：6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メールアドレス詐称、正規ユーザになりすましてのサービス不正利用、ソーシャルエンジニアリングなどが含まれ、48件（平成21年：37件）の届出があった。

【主な内容】

正規ユーザへのなりすまし：36件

ソーシャルエンジニアリング：5件

メールアドレス（ドメイン）の詐称：3件

メール不正中継：1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。

197件の届出中、実際に被害に遭った計123件（平成21年：96件）を分類すると以下ようになる。

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がますます多くなっており、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：16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：13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：7件  
DoS 攻撃・その他によるもの：12件  
原因不明：75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】

WWW サーバ：98件  
メールサーバ：24件  
クライアント：15件  
ファイアウォール：2件  
ルータ：1件  
その他のサーバ：21件  
不明：3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

197件の届出を被害内容で分類した214件中、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140件(昨年：107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】

ホームページ改ざん：35件  
オンラインサービスの不正利用：35件  
踏み台として悪用：25件  
ファイルの書き換え：20件  
サービス低下：6件  
データの窃取や盗み見：5件  
不正アカウントの作成：2件  
サーバダウン：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22(2010)年は、いわゆる「ガンブラー」によるウェブサイト改ざんの被害が特に多かったと言える。また、その被害原因の多くが不明なケースだったことから、こうした改ざんを行うための攻撃手口の巧妙化が伺える。その他では、なりすましによってオンラインゲームなどのサービスを勝手に使われて

金銭被害が出たケースや、SSH<sup>1</sup>で使用するポートへの攻撃で侵入（ID、パスワードの設定不備が主な原因）され、他のコンピュータを攻撃するための踏み台に悪用されていた被害も目立っていたと言える。主に原因不明なケースが多く見受けられたが、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多く見受けられる。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、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）
- ・ ルータやパーソナルファイアウォールの活用
- ・ 無線 LAN の暗号化設定確認（WEP は使用せず、できる限り WPA2 を使用する）

下記ページなどを参照し、今一度状況確認・対処されたい。

#### 【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](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4版」

<http://www.ipa.go.jp/security/vuln/websecurity.html>

「JVN (Japan Vulnerability Notes)」 脆弱性対策情報ポータルサイト

<http://jvn.jp/>

「SQL インジェクション攻撃に関する注意喚起」

[http://www.ipa.go.jp/security/vuln/documents/2008/200805\\_SQLinjection.html](http://www.ipa.go.jp/security/vuln/documents/2008/200805_SQLinjection.html)

「ウェブサイトで利用されている DNS サーバの既知の脆弱性への注意喚起」

[http://www.ipa.go.jp/security/vuln/documents/2009/200912\\_dns.html](http://www.ipa.go.jp/security/vuln/documents/2009/200912_dns.html)

---

<sup>1</sup> SSH(Secure Shell)：ネットワークを介して遠隔のコンピュータと通信するためのプロトコルの一つ。

「古いソフトウェア製品を利用しているウェブサイトへの注意喚起」

[http://www.ipa.go.jp/security/vuln/documents/2009/200903\\_update.html](http://www.ipa.go.jp/security/vuln/documents/2009/200903_update.html)

「ウェブサイト管理者へ：ウェブサイト改ざんに関する注意喚起」

<http://www.ipa.go.jp/security/topics/20091224.html>

【個人ユーザ向け】

「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/>

「マイクロソフトセキュリティ At Home」(マイクロソフト社)

<http://www.microsoft.com/japan/protect/default.aspx>

「MyJVN」(セキュリティ設定チェック、バージョンチェック)

<http://jvndb.jvn.jp/apis/myjvn/>

「一般利用者へ：改ざんされたウェブサイトからのウイルス感染に関する注意喚起」

<http://www.ipa.go.jp/security/topics/20091224.html>

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

「IPA セキュリティセンタートップページ」

<http://www.ipa.go.jp/security/>

注1 コンピュータ不正アクセス

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

注2 ここにあげた件数は、コンピュータ不正アクセスの届出を IPA が受理した件であり、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）に報告（調整対応依頼）があった不正アクセス関連行為の状況について

平成 22 年 1 月 1 日から 12 月 31 日の間に JPCERT/CC に報告（調整対応依頼）のあったコンピュータ不正アクセスが対象である。

本年度、データ集計カテゴリーの見直しを行った結果、集計結果に以下の変更があります。

- ・「ウ 電子メールの送信ヘッダを詐称したメールの配送」は廃止し、報告件数は「カ その他」に集計。
- ・「カ その他」にて集計していたマルウェア配布サイトやマルウェア公開サイトに関する報告は、新たに「ウ マルウェア」を新設し、集計。

### (1) 不正アクセス関連行為の特徴および件数

報告（調整対応依頼）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 11,769 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 2,291 件の報告があった。

[1/1-3/31: 322 件、4/1-6/30:349 件、7/1-9/30:492 件、10/1-12/31: 1128 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 1,922 件の報告があった。

[1/1-3/31: 809 件、4/1-6/30: 561 件、7/1-9/30:353 件、10/1-12/31: 199 件]

#### ウ マルウェアサイト

閲覧することで PC がマルウェアに感染してしまう攻撃用サイトや攻撃に使用するマルウェアを公開しているサイトについて 4,425 件の報告があった。

[1/1-3/31: 1,410 件、4/1-6/30: 1,478 件、7/1-9/30:965 件、10/1-12/31: 572 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。

[1/1-3/31:0 件、4/1-6/30:2 件、7/1-9/30:5 件、10/1-12/31:4 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 1,786 件の報告があった。

[1/1-3/31: 373 件、4/1-6/30: 388 件、7/1-9/30: 487 件、10/1-12/31:538 件]

#### カ その他

コンピュータウイルス、SPAM メールを受信等について 1,334 件の報告があった。

[1/1-3/31:271 件、4/1 -6/30:407 件、7/1-9/30:459 件、10/1-12/31:197 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]

2010年1月	Web サイト改ざん及びいわゆる Gumblar ウイルス感染拡大に関する注意喚起 Microsoft セキュリティ情報 (緊急 1 件) に関する注意喚起 Adobe Reader 及び Acrobat の脆弱性に関する注意喚起 Microsoft Internet Explorer の未修正の脆弱性に関する注意喚起
2010年2月	FTP アカウント情報を盗むマルウェアに関する注意喚起 Microsoft セキュリティ情報 (緊急 5 件含) に関する注意喚起
2010年3月	Microsoft Internet Explorer の脆弱性 (MS10-018) に関する注意喚起
2010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 Adobe Reader 及び Acrobat の脆弱性に関する注意喚起 Oracle Sun JDK および JRE の脆弱性に関する注意喚起 いわゆる Gumblar ウイルスによってダウンロードされる DDoS 攻撃を行うマルウェアに関する注意喚起
2010年5月	Microsoft セキュリティ情報 (緊急 2 件含) に関する注意喚起
2010年6月	社内 PC のマルウェア感染調査を騙るマルウェア添付メールに関する注意喚起 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起 Adobe Flash Player および Adobe Acrobat/Reader の脆弱性に関

	<p>する注意喚起</p> <p>Windows のヘルプとサポートセンターの未修正の脆弱性に関する注意喚起</p> <p>Adobe Reader 及び Acrobat の脆弱性に関する注意喚起</p>
2010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
2010年8月	<p>Windows シェルの脆弱性 (MS10-046) に関する注意喚起</p> <p>Microsoft セキュリティ情報 (緊急 8件含) に関する注意喚起</p> <p>Adobe Flash Player の脆弱性に関する注意喚起</p> <p>Adobe Reader 及び Acrobat の脆弱性に関する注意喚起</p>
2010年9月	<p>Microsoft セキュリティ情報 (緊急 4件含) に関する注意喚起</p> <p>Adobe Flash Player の脆弱性に関する注意喚起</p>
2010年10月	<p>攻撃用ツールキットを使用した Web サイト経由での攻撃に関する注意喚起</p> <p>Adobe Reader 及び Acrobat の脆弱性に関する注意喚起</p> <p>Microsoft セキュリティ情報 (緊急 4件含) に関する注意喚起</p> <p>アクセス解析サービスを使用した Web サイト経由での攻撃に関する注意喚起</p>
2010年11月	<p>Adobe Flash Player の脆弱性に関する注意喚起</p> <p>Microsoft セキュリティ情報 (緊急 1件含) に関する注意喚起</p> <p>Adobe Reader 及び Acrobat の脆弱性に関する注意喚起</p>
2010年12月	<p>不適切な設定で Asterisk を利用した場合に発生し得る不正利用に関する注意喚起</p> <p>Microsoft セキュリティ情報 (緊急 2件含) に関する注意喚起</p>

#### イ 活動概要 (報告状況等の公表)

発行日：2011-01-12 [ 2010年10月1日～2010年12月31日]

発行日：2010-10-07 [ 2010年7月1日～2010年9月30日]

発行日：2010-07-07 [ 2010年4月1日～2010年6月30日]

発行日：2010-04-08 [ 2010年1月1日～2010年3月31日]

#### ウ JPCERT/CC レポート

[発行件数] 49件

[取り扱ったセキュリティ関連情報数] 287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やウイルス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、JPCERT/CC における分析や情報発信に活用しているほか、ウェブサイトにて観測情報を提供している。  
(詳細は <http://www.jpccert.or.jp/isdas/>参照。)

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

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

### 3 脆弱性対策情報について

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 181 件であった(詳細は <http://jvn.jp/>参照。)

[1/1-3/31:26件、4/1-6/30:41件、7/1-9/30:41件、10/1-12/31:73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、JVN にて公開した脆弱性情報は 66 件であった。

[1/1-3/31:06件、4/1-6/30:20件、7/1-9/30:09件、10/1-12/31:31件]

## 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。

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

継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 ~

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手法 ~ 暗号の技術的評価に関する研究開発 ~

インシデント分析の広域化・高速化技術に関する研究開発

ネットワークセキュリティ技術の研究開発

マルウェア対策ユーザサポートシステムの研究開発

認証可能な安全性をもつキャンセルラブル・バイオメトリクス認証技術の構築とそれを利用した個人認証インフラストラクチャ実現に向けた研究開発

生体認証サービスにおける情報漏えい対策（キャンセルラブルバイオメトリクス）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22年11月25日から12月27日までの間にアクセス制御技術に関する研究開発状況の募集を行ったところ、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。

株式会社グローバルワイズ  
株式会社ハーモニックセキュリティ

#### (2) 調査

警察庁が平成22年10月から平成22年11月にかけて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る。

ア 大学

佐賀大学  
信州大学  
神奈川大学  
北海道大学  
国土館大学  
奈良先端科学技術大学院大学  
岩手大学  
東北大学  
九州大学

イ 企業

シスメックス R A 株式会社  
株式会社アクアシステムズ  
K D D I 株式会社  
株式会社メトロ  
三菱電機株式会社  
株式会社日立ソリューションズ  
株式会社シー・エス・イー  
ヌリテレコム株式会社  
株式会社インテリジェントウェイブ  
ログイット株式会社

また、それぞれの研究開発の概要は別添3のとおりである。

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。

アンケート調査は、次の条件により抽出した1,300団体を対象に実施した。

・大学

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

・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  
上場企業、店頭公開企業及び未上場企業から無作為に抽出

(別添1)

<b>対象技術</b> 侵入検知技術
<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、(株)KDDI研究所、パナソニック電工(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)
<b>背景、目的</b> 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する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、ウィ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。
<b>研究開発状況(概要)</b> ・平成17年度から平成21年度にかけて以下の研究開発を実施し、委託研究開発を終了。 (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22年度 標準化を目指した応用研究としてNICTトレーサブルネットワークグループにてCYBEXやDNSSECなどとの連携技術の研究開発を実施。
<b>詳細の入手方法(関連部署名及びその連絡先)</b> 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 ( <a href="http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm">http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm</a> ) 電話 042 - 327 - 6011
<b>将来の方向性</b> 不正アクセス、DoS攻撃、ウィ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。

<b>対象技術</b>	その他認証技術
<b>テーマ名</b>	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～
<b>開発年度</b>	平成19年度～平成21年度
<b>実施主体</b>	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)
<b>背景、目的</b>	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>
<b>研究開発状況(概要)</b>	<ul style="list-style-type: none"> <li>・平成19年度より以下の研究開発を実施。 <ol style="list-style-type: none"> <li>(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</li> <li>(2) 電子署名更新技術</li> <li>(3) 再暗号化技術</li> </ol> </li> <li>・平成21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 連携研究部門 委託研究グループ (<a href="http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm">http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm</a>) 電話 042 - 327 - 6011</p>
<b>将来の方向性</b>	上記セキュリティ技術を検証し、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> 次世代ハッシュ関数の研究開発
<b>開発年度</b> 平成19年度～平成21年度
<b>実施主体</b> 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）
<p><b>背景、目的</b></p> <p>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に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。</p> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>・次世代ハッシュ関数</li> </ul> <p>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。</p> <p>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。</p> <p>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。</p>
<p><b>研究開発状況（概要）</b></p> <ul style="list-style-type: none"> <li>・平成19年度より以下の研究開発を実施。 <ol style="list-style-type: none"> <li>(1) 次世代ハッシュ関数の設計技術</li> <li>(2) 次世代ハッシュ関数の実装技術</li> </ol> </li> <li>・平成21年度末に開発終了。</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 連携研究部門 委託研究グループ  （<a href="http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm">http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm</a>）  電話 042 - 327 - 6011</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>	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～
<b>開発年度</b>	平成19年度～平成21年度
<b>実施主体</b>	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)
<b>背景、目的</b>	<p>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。</p> <p>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。</p> <p>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FIPS800-5などが参考にされている。</p> <p>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。</p> <p>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が存在するが、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。</p> <p>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。</p>
<b>研究開発状況(概要)</b>	<ul style="list-style-type: none"> <li>・平成19年度より以下の研究開発を実施。 <ol style="list-style-type: none"> <li>(1) 攻撃プログラムの設計・開発</li> <li>(2) 暗号強度比較・評価・検証技術</li> </ol> </li> <li>・平成21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 連携研究部門 委託研究グループ (<a href="http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm">http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm</a>) 電話 042 - 327 - 6011</p>
<b>将来の方向性</b>	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>	インシデント分析の広域化・高速化技術に関する研究開発
<b>開発年度</b>	平成20年度～平成22年度
<b>実施主体</b>	株式会社ラック、財団法人九州先端科学技術研究所、株式会社セキアウェア、株式会社セキュアブレイン、株式会社クリプト ジャパンデータコム株式会社、KDDI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）
<b>背景、目的</b>	<p>近年のコンピュータセキュリティインシデント（以下、「インシデント」と略す。）は、正規のWebサイトを装いつつ、ユーザがそのWebサイトを参照するだけで、マルウェアをダウンロードさせられたり、ソーシャルエンジニアリング手法を駆使して、特定の個人に関連する偽の情報を流したり、URLの見間違いを誘発するなどの工夫が施されており、ますます巧妙化の傾向を強めてきている。</p> <p>こうした状況の中で、情報通信研究機構（NICT）においては、広域のネットワークを想定し、スキャンを中心とした攻撃検知とその原因となり得るマルウェア等の解析により、インシデントを迅速かつ正確に検知し、対策を導出するための研究開発を行うために、nicter（Network Incident analysis Center for Tactical Emergency Response）と呼ばれるインシデント分析センターの構築を進めている。</p> <p>現状のnicterでは、ネットワークにおける攻撃情報の収集地点に偏りがあり、攻撃情報の種別についても網羅性が乏しい。また収集した情報を一元管理しているため、その分析性能などに多くの課題を抱える。しかしながら、これまでのnicterにおいて培われてきた高度な分析能力を十分に活用し、それらの効率的な機能配分を行うことにより、日本全土を広域にカバーする、高性能なインシデント分析システムの構築が可能であると考えられる。</p> <p>本研究開発では、このような広域分散型のインシデント分析システムの構築により、広く日本でどのような攻撃が起こっているのか、その攻撃にどのような地域性があるのか、その攻撃は具体的にどのようなマルウェアに起因しているのか、その攻撃への対策をどのように講じるべきかを効率的に解決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20年度から次の研究開発を行い、現在、協力先団体にセンサを設置し、実証実験を実施している。</li> <li>(1) 攻撃及び関連マルウェアの高速・高精細攻撃検知・収集</li> <li>(2) 階層拠点間の分散協調のための分析結果情報の匿名化・秘匿化技術</li> <li>(3) 階層拠点における分散協調型セキュリティオペレーションの基盤技術</li> <li>(4) 実環境で有効に機能させるための実証実験</li> <li>・実環境でシステムの有効性等を評価し、平成22年度末に研究開発を完了する予定である。</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 連携研究部門 委託研究グループ  （<a href="http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm">http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm</a>）  電話 042 - 327 - 6011</p>
<b>将来の方向性</b>	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> 侵入検知技術
<b>テーマ名</b> ネットワークセキュリティ技術の研究開発
<b>開発年度</b> 平成18年度～平成22年度
<b>実施主体</b> 独立行政法人情報通信研究機構
<p><b>背景、目的</b></p> <p>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。</p> <p>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。</p>
<p><b>研究開発状況（概要）</b></p> <p>平成22年度には、これまでに研究開発・整備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、マルウェアの収集機構・収集したマルウェアの分析機構に関して、日本全国規模の観測網構築に向けた観測対象ネットワークの更なる拡充、より高度な観測アーキテクチャー・攻撃検出機構の開発を進め、マルウェアの分析精度の高度化及び攻撃元のマルウェアをリアルタイムに識別する技術開発を行った。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し、実運用に向け開発を進めた。</p> <p>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、その組織が有する情報を互いに開示することなく、共通の攻撃を解析する技術について、従来までの公開鍵暗号を利用した方式に比較して高速化が可能な秘密鍵暗号によるアルゴリズムを開発し、その有効性を検証した。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技術を開発し、逐次解析器による再現フローの自動化とデータ蓄積を進めた。また海外研究機関と連携し、APIシーケンスを自動分類し、高精度で攻撃ベクタを捕捉できる機械学習アルゴリズムの開発を進めた。</p>
<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 情報通信セキュリティ研究センター推進室 042-327-5774</p>
<p><b>将来の方向性</b></p> <p>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。</p>

<b>対象技術</b> その他認証技術
<b>テーマ名</b> マルウェア対策ユーザサポートシステムの研究開発
<b>開発年度</b> 平成21年度～平成23年度
<b>実施主体</b> 株式会社日立製作所、KDDI株式会社
<p><b>背景、目的</b></p> <p>本研究開発では、ユーザパソコンに負荷がかかる実行コードの解析をnicter等の解析機能を有する外部のシステムが担うことにより、効率的なマルウェアの検出及び自動駆除の仕組みを実現することを目的とする。</p> <p>ユーザにおけるマルウェア対策として一般的なものは、セキュリティベンダ等が提供している、シグネチャ（マルウェア検査パターン）に基づくアンチウイルスソフトである。</p> <p>アンチウイルスソフトでは、シグネチャを採用しているため、既知のマルウェアに対しては十分対応できるが、未知のマルウェアや、一定期間感染行動等の挙動を見せないマルウェアの疑いのある怪しい実行コードに対しては、現状十分に対応できていない。また、新しいマルウェアが現出した場合、セキュリティベンダ等が対応するパターンファイルを更新するまでに一定の時間を要するため、ユーザが必要なときに、必要なものをタイムリーに入手できるところまでには至っていない。</p> <p>その他にも、総務省、経済産業省の連携プロジェクトとして設置されたサイバークリーンセンター（CCC）において、ポット対策の一環として、ユーザ向けに、駆除ツール（CCCクリーナー）が提供されている。このような駆除ツール（CCC クリーナー）についても、既に感染行動が見られるポットや既知のポットのみを取り扱っており、アンチウイルスソフトと同様な問題が見受けられる。</p> <p>また、情報処理推進機構（IPA）では、ウイルス情報iPedia（ウイルス情報データベース）において、届出されたウイルスやポットなどを中心に、それらの主な動作内容や対処法などの解析結果を公開している。</p> <p>コード難読化やコード自己変貌化に代表されるように、昨今、マルウェアの高度化・巧妙化が進展する中で、上述のように未知のマルウェアや一定期間感染行動等の挙動を見せないマルウェアの疑いのある怪しい実行コードのように、アンチウイルスソフトによる対応では十分カバーし切れない領域が存在している。</p> <p>セキュリティベンダ等による取り組みを補完しつつ、そのような未知のマルウェアも対応できるように、検体の解析に基づくマルウェア判定をベースとした駆除ツールを、実時間に近い形でユーザに提供していくことが必要になってきている。</p>
<p><b>研究開発状況（概要）</b></p> <ul style="list-style-type: none"> <li>・ 平成21年度より以下の研究開発を実施中。</li> <li>(1) ユーザパソコンへの負荷をかけず、実行コードがマルウェアかどうかをユーザサポートセンターで解析するとともに、マルウェアを駆除するツールを自動的に提供するフレームワークを確立する。</li> <li>(2) ユーザのパソコン上で検査プログラムを実行してから、ユーザに対して駆除ツールが提供されるまでの一連の手続きが速やかに完了する技術を確立する。</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 連携研究部門 委託研究グループ  (<a href="http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm">http://www2.nict.go.jp/q/q265/s802/itakukenkyu.htm</a>)  電話 042 - 327 - 6011</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> その他認証技術等
<b>テーマ名</b> 証明可能な安全性をもつキャンセルラブル・バイオメトリクス認証技術の構築とそれを利用した個人認証インフラストラクチャ実現に向けた研究開発
<b>開発年度</b> 平成20年度～平成21年度
<b>実施主体</b> 独立行政法人産業技術総合研究所（経済産業省からの委託）
<p><b>背景、目的</b></p> <p>現在、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が急速に変化・拡大しており、経済活動全体の停滞や国民全体の生命・財産そのものに関わるリスクをもたらしかねない状況が生まれつつある。そこで「新世代情報セキュリティ研究開発事業」では、これまでの対症療法的な対策だけでなく、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実施することを目指す。</p> <p>本事業では、生体情報が自由に取り換えのできない情報であることに起因する生体認証特有の脆弱性を解決するために、テンプレート保護技術と更新可能なバイオメトリクス認証の安全性評価について研究する。すでに、キャンセルラブル・バイオメトリクスやバイオメトリック暗号と呼ばれる技術の枠組みの中で、これらの問題を解決するための様々な手法が提案されているが、明確な安全性の基準が存在せず、真に実用的な技術が生まれていない。よって、本事業では、安全性評価基準の理論的な枠組みの構築、証明可能な安全性をもつ生体認証技術の研究開発を主たる目的とする。また、各モダリティに対する認証プロトコルの開発や安全性に対する実験、開発したプロトコルの実装も併せて行う。</p>
<p><b>研究開発状況（概要）</b></p> <p>平成 20 年度より以下の研究開発を行っており、平成 21 年度末に開発終了予定である。</p> <p>(1) 安全性評価基準の理論的枠組みの構築</p> <p>(2) 証明可能安全性をもつキャンセルラブル認証技術の研究開発</p> <p>(1)、(2)において、暗号理論的なアプローチを用いて安全性の定式化を行うとともに、汎用性の高い安全な認証プロトコルの開発を行った。</p> <p>(3) 各モダリティのアルゴリズム調査、解析と応用手法の研究開発</p> <p>各モダリティに対して、モダリティの特徴を生かした認証プロトコルの開発や、なりすまし攻撃に対する安全性評価実験などを行った。</p> <p>(4) バイオメトリクス認証を組込んだID連携認証技術のプロトタイプ構築</p> <p>(1)、(2)で開発した認証プロトコルのテスト実装として、開発プロトコルを組み込んだID連携システムのプロトタイプを構築した。</p>
<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 産業技術総合研究所 情報セキュリティ研究センター</p> <p>電話：03-5298-4722 Web：http://www.rcis.aist.go.jp/</p>
<p><b>将来の方向性</b></p> <p>本人確認のための重要な基盤技術となりつつある生体認証システムの安全性評価基準や評価体制を確立することで、より安全で安心な社会の実現に貢献していく。</p>

<b>対象技術</b>	その他認証技術等
<b>テーマ名</b>	生体認証サービスにおける情報漏えい対策（キャンセラブル・バイオメトリクス）の研究開発
<b>開発年度</b>	平成20年度～平成21年度
<b>実施主体</b>	株式会社日立製作所（経済産業省からの委託）
<b>背景、目的</b>	<p>現在、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が急速に変化・拡大しており、経済活動全体の停滞や国民全体の生命・財産そのものに関わるリスクをもたらしかねない状況が生まれつつある。そこで「新世代情報セキュリティ研究開発事業」では、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実施することを目指す。</p> <p>本事業では、漏えいが許されない情報の一つである指紋や静脈、虹彩などのバイオメトリクス情報の安全な利活用の実現を目的として、生体特徴情報を無効化するキャンセラブル・バイオメトリクス技術を生体認証サービスプロバイダに適用した場合の管理・運用の在り方について調査・研究を実施し、強度評価手法と、運用ガイドラインの作成を進める。</p>
<b>研究開発状況（概要）</b>	<p>(1) 情報漏えい対策型の生体認証サービスフレームワークの研究開発</p> <p>生体認証サービスシステムの運用モデルを検討し、リスク分析評価を行い、システム要件を明確にした。また、情報漏えい対策型の技術（キャンセラブル・バイオメトリクス）を適用した場合と、従来型とを比較し、情報漏えい対策型の生体認証サービスフレームワークを確立した。さらに、本フレームワークに基づいた、情報漏えい対策型の生体認証サービスシステムに対するプライバシー影響評価を行った。</p> <p>(2) 情報漏えい対策技術の強度評価に関する研究開発</p> <p>情報漏えい対策技術の強度について調査し、有識者WGにてレビューを実施し、強度基準および強度評価方法を検討した。これにより、上記のサービスフレームワークに対する強度基準となる評価項目を明確化し、強度基準および評価方法を確立した。</p> <p>(3) 情報漏えい対策型の生体認証サービスの運用ガイドラインの研究開発</p> <p>海外・国内の生体認証サービスの動向を調査するとともに、上記システム要件、生体認証サービスに要求される運用時のセキュリティ要件について、実証システムによるガイドラインの有効性実証・フィードバックを行いながら、有識者WGにて整理し、「情報漏えい対策型の生体認証サービスの運用ガイドライン」をまとめた。</p>
<b>詳細の入手方法（関連部署名及びその連絡先）</b>	<p>株式会社日立製作所 セキュリティ・トレーサビリティ事業部  セキュリティソリューション本部  （Tel:044-549-1214 Fax:044-549-1382）</p>
<b>将来の方向性</b>	<p>対症療法的ではなく根本的な生体認証システム上の問題である「生涯不変な特徴の漏えい」に対して、上記のように、解決に資する技術（キャンセラブル）および、その運用指針を確立することで、安全・安心な生体認証サービスを社会に提供することが可能となる。</p>

(別添2)

企業名(及び略称) 株式会社グローバルワイズ	
代表者氏名 代表取締役 伊原栄一	
所在地(郵便番号及び住所) 愛知県刈谷市若松町2-55-1	
関連部署名及び電話番号 プロダクト事業部 NETMETRIX担当 03-5419-7980	
URL <a href="http://www.g-wise.co.jp/">http://www.g-wise.co.jp/</a>	
対象技術	技術開発状況
侵入検知技術 2004年	同一ネットワーク上に存在する全てのノードに対してパケットを送信し、その応答によりノードの端末情報を収集する技術。 セグメントやV-LAN、WANなどネットワーク構成による制限はない。 事前に端末に管理用ソフトウェアをインストールする必要がないため、未知(未登録)の端末からも情報を取得することができる。 あらかじめ接続許可端末のリストを登録すれば、未許可の端末のネットワーク接続や、ログインユーザの変更など状態の変化を検知する。 <b>【取得情報】</b> <ul style="list-style-type: none"><li>・IPアドレス</li><li>・MACアドレス</li><li>・コンピュータ名</li><li>・OS情報(Windows、MACOS、Linuxなど) 他</li></ul>

企業名（及び略称）株式会社ハーモニックセキュリティ	
代表者氏名 代表取締役 國米 仁	
所在地（郵便番号及び住所）〒558-0041 大阪市住吉区南住吉4丁目1番32号	
関連部署名及び電話番号 本社 06-6608-6765	
URL <a href="http://www.mneme.co.jp">http://www.mneme.co.jp</a>	
対象技術	技術開発状況
その他認証技術  開発年 2005年～ 2008年	<p>故意による機密情報の持ち出しと思われる事件が続発しています。意図的な持ち出しを防ぐのはなかなか困難ですが、正しくログインできても単独ではデータへのアクセスは許されず、複数の権限ある担当者が全てログインできた場合にのみデータへのアクセスが許される認証権限分散方式を採用すれば事件抑止の一助になります。当社では認証権限分散機能を持つ『権限分散クリプトニーモ』を発表しています。これは、10人の登録オペレータの中の任意の3人が共同で作業した場合にのみアクセスが完了する権限分散型本人認証ソフトに、常態では暗号鍵を存在させないデータ暗号化復号機能を付加したものです。データ暗号化機能を切り離して認証権限の分散化機能のみを使用することも可能です。復号後の平文データの持ち出しの可能性は残りますので故意による持ち出しを必ず根絶できるというものではありませんが、監視ソフトや行動抑制ソフトとの連携を適切に行えば故意による持ち出しの抑止に大きく貢献できるものと考えています。製品概要とQ&amp;Aを以下のサイトに掲載しています。</p> <p><a href="http://www.mneme.co.jp/neme/img/bunsan.pdf">http://www.mneme.co.jp/neme/img/bunsan.pdf</a>（製品概要）</p> <p><a href="http://www.mneme.co.jp/neme/pdf/qa.pdf">http://www.mneme.co.jp/neme/pdf/qa.pdf</a>（Q&amp;A）</p>

## 別添 3

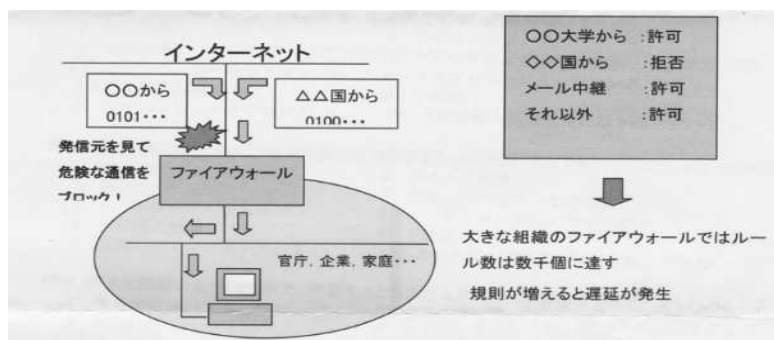
## 【大学】

大学名	佐賀大学総合情報基盤センター
所在地	〒840-8502 佐賀市本庄町 1
窓口部署名 / 電話番号	/ 0952-28-8592
ホームページのURL	<a href="http://www.cc.saga-u.ac.jp/">http://www.cc.saga-u.ac.jp/</a>
対象技術	技術の概要・特徴など
ネットワーク	<ul style="list-style-type: none"> <li>・無線LANや情報コンセントを利用する際に、利用者を認証するためのシステムです。</li> <li>・webによる平易なインターフェースを持ち特別なソフトウェアを導入することなく利用可能です。</li> <li>・利用者の認証後、ネットワークが利用でき、利用終了後、即座に閉鎖します。</li> <li>・IPv4だけでなく、IPv6にも対応しています。</li> <li>・既に10年以上の運用実績があります。</li> </ul>

大学名	信州大学
所在地	〒380-8553 長野市若里4 - 17 - 1
窓口部署名 / 電話番号	総務 G (庶務) / 026-269-5004
ホームページのURL	<a href="http://wwweng.cs.shinsh-u.ac.jp">http://wwweng.cs.shinsh-u.ac.jp</a>
対象技術	技術の概要・特徴など
サーバ 通信情報 データ	PKI処理を高速に実行するアクセラレータ

大学名	信州大学
所在地	〒380-8553 長野市若里4 - 17 - 1
窓口部署名 / 電話番号	総務 G (庶務) / 026-269-5004
ホームページのURL	<a href="http://wwweng.cs.shinsh-u.ac.jp">http://wwweng.cs.shinsh-u.ac.jp</a>
対象技術	研究開発状況
ネットワーク 通信情報 データ	数多くの質問を用意し、それらを適宜提示して各個人のその人らしさを認証する

大学名	神奈川大学
所在地	〒259-1293 平塚市土屋2946
窓口部署名 / 電話番号	理学部情報科学科 / 046-359-4111
ホームページのURL	
対象技術	研究開発状況
ネットワーク	<p>パケットフィルタリングは、ネットワークセキュリティを確保する基本的手法である。フィルタ運用の際は、外部に脅威の存在が認められる度にルールが追加されるが、その脅威が除去されたことを確認する手段がないため、ルールは増加の一途を辿る。ルールの増加はパケット転送の遅延を招き、やがて通信品質の低下を引き起こす。</p> <p>本研究では、ルールの構成と配置を最適化することで転送の遅延を最小にする方法を構築する。</p> <p>ここで考案する方法は、パケット通信を行うあらゆるネットワーク機器に適用できることから、ネットワーク全体の通信の品質を向上することに広く貢献する。これまで、パケットフィルタを最適化するさまざまな研究が行われてきた。</p> <p>神奈川大学田中研究室では、これまでにパケットフィルタリングをモデル化し、フィルタを構成するルール集合によって決まるネットワーク機器の負荷を定義した。そして、ルールの入れ替えと併合を行う場合に、負荷が減少するための必要十分条件を与えた。クワイン・マクラスキ法を基にしたルールの併合と入れ替え法に基づく最適化アルゴリズムを提案し、フィルタの負荷を50%程度に軽減できることを示した。</p> <p>その後、課題とされた評価パケット数の計算量についても、多項式時間の概算値の計算法を提示し抜本的な解決をはかった。従来は、パケットの頻度分布が一様であることを仮定していたが、ネットワーク機器の到着パケットを観察することで評価パケット数に換える方法を提案し、現実のネットワーク機器の運表を継続しながら適応的にフィルタを再構成する方法に目途をつけた。今後は、これらの理論的結果を踏まえ、実際のネットワーク環境での実装実験を行い、実用化を目指す。</p>



大学名	北海道大学数学連携研究センター
所在地	〒060-0812 札幌市北区北12西7北海道大学
窓口部署名 / 電話番号	
ホームページのURL	<a href="http://www.math.sci.hokudai.ac.jp/center/">http://www.math.sci.hokudai.ac.jp/center/</a>
対象技術	研究開発状況
データ その他	PDFへの長期署名を埋め込み時刻認証との連携のもとにファイルの作成時刻を保証する。これにより、論文を電子ファイルのみで出版した場合でもプライオリティ(成果の先着権)が確実に担保される。現在、開発を終えており、今後の発展を模索している。

大学名	国士舘大学理工学部
所在地	〒154-8515 世田谷区世田谷4-28-1
窓口部署名 / 電話番号	国士舘大学理工学部 / 03-5481-3251
ホームページのURL	<a href="http://www.kokushikan.ac.jp">http://www.kokushikan.ac.jp</a>
対象技術	研究開発状況
通信情報 データ	将来のクラウド化のもつ脆弱性について、検証を行うことを目的とし、その欠点を回避するためのクライアントが対応すべき技術を開発中であり未だ成果を公開するに至っていない。

大学名	国立大学法人奈良先端科学技術大学院大学
所在地	〒630-0192 奈良県生駒市高山町8916-5
窓口部署名 / 電話番号	
ホームページのURL	<a href="http://www.naist.jp">http://www.naist.jp</a>
対象技術	研究開発状況
ネットワーク 通信情報	近年、インターネットにおいて、大量のパケットを送信することでサービスの妨害を行うサービス不能攻撃(DoS攻撃)が問題となっている。このDoS攻撃への対策として提案されている、攻撃元までの経路を追跡し攻撃者を特定するIP Tracebackという手法に関し、研究を行っている。

大学名	岩手大学工学部
所在地	〒020-8551 岩手県盛岡市上田4-3-5
窓口部署名 / 電話番号	工学研究科デザイン・メディア工学専攻 / 019-629-2838
ホームページのURL	<a href="http://www.mn.cis.iwate-u.ac.jp/research/index.html">http://www.mn.cis.iwate-u.ac.jp/research/index.html</a>
対象技術	研究開発状況
サーバ	<p>近年のコンピュータウィルスは実行可能圧縮という圧縮や難読化が施され、アセンブラコードの検査によるウィルス判定が難しくなっている。</p> <p>商用のアンチウィルス対策ソフトウェアは独自開発した解凍機能を有しているが、処理が複雑すぎて解凍できない場合が多発している。そこで私たちはウィルスを実行させて、それ自身の解凍ルーチンでウィルスの中身をメモリに展開させた後に実行を止めて、その中身をベイジアンフィルタで検査する方法で80%の解凍・解析に成功した。しかしながら、この方法では毎回ウィルスを実行するために処理に時間が掛かる。</p> <p>現在、解凍前後の情報を記憶させることで、2回目以降の検査を実行可能圧縮のまま可能にする新方式について研究を進めている。</p>

大学名	東北工業大学工学部情報通信工学科松田研究室
所在地	〒982-8577 宮城県仙台市太白区八木山香澄町35-1
窓口部署名 / 電話番号	情報通信工学科松田研究室 / 022-305-3424
ホームページのURL	<a href="http://www.ice.tohtech.ac.jp/jp_ng/labs/matsuda.html">http://www.ice.tohtech.ac.jp/jp_ng/labs/matsuda.html</a>
対象技術	研究開発状況
ネットワーク サーバ クライアント	データリンク層における通信制御を、低コストに実現する研究を開発し、性能試験を実施している。

大学名	九州大学
所在地	〒819-0395 福岡市西区元岡744
窓口部署名 / 電話番号	大学院システム情報化科学研究情報学部門 / 092-802-3801
ホームページのURL	<a href="http://itslab.cace.kyushu-u.ac.jp/">http://itslab.cace.kyushu-u.ac.jp/</a>
対象技術	研究開発状況
ネットワーク サーバ クライアント 通信情報 データ	<p>暗号および暗号プロトコル技術、コンピュータシステムセキュリティ技術等の情報セキュリティ関連研究開発を実施している。</p> <p>暗号および暗号プロトコル分野： 暗号技術に基づくデータプライバシー保護手法（2007-）、公開鍵認証基盤（2003-）、電子投票（2002-）、ハッシュ関数（2002-）、デジタルフィンガープリンティング（2002-）、配達保証付き電子メール（2002-）、ソフトウェア難読化（2002-）、認証付き鍵交換（2001-）</p> <p>コンピュータシステムセキュリティ分野： BFIDタグのプライバシー、侵入検知システム、VM-Based Logging Scheme（2008-）、キャンセルブルバイオメトリクス（2006-）、オペレーティングシステム(OS)の安全性（2003-）、迷惑メール対策（2003-）、インサイダー脅威対策（2010-）</p> <p>ネットワークセキュリティ分野： パケット生存時間を用いた確率的パケットマーキングによるIPトレースバック手法、ネットワーク管理とセキュリティのための視覚化、P2P Trust Model（2008-）、Formal verification of access Control（2008-）、内容の類似性を用いたトラックスパム判別（2008-）、ポリモーフィックワームの検知手法（2007-）、ボット検知手法（2007-）、SIPにおけるend-to-mobileセキュリティ（2007-）、P2Pルーティングアルゴリズム（2007-）、ファイヤーウォールポリシーのフォーマルメソッド（2007-）、ポートスキャン検出（2005-）、ピアツーピアネットワークの匿名性保護（2005-）、モバイルエージェントの安全性（2003-）</p>

【企業】

企業名	シスメックス R A 株式会社
所在地	〒399-0702 長野県塩尻市広丘野村1850-3
窓口部署名 / 電話番号	ITX部営業課 / 03-5719-5587
ホームページのURL	http://www.sysmex-ra.co.jp/
対象技術	技術の概要・特徴など
通信情報	<p>Ipssec暗号化アダプタBOX</p> <p>IPsecによる強固なセキュリティ機能： 強力な暗号化と認証機能を持ったIPsecにてプロトコルやアプリケーションに関係なく転送される通信データ(TCP/UDPパケット)のセキュリティ機能を高めることができます。</p> <p>簡単接続： イーサネットインターフェースを2ポート装備し、通信機器とLANケーブルの間に中継器として挟み込むだけで通過する通信データは自動的に暗号化され送信先へと転送されます。 また、通信機器へは競って変更や特殊なアプリケーションをインストールする必要はなく、通信機器に迅速に組み込むことができます。</p> <p>柔軟設定 設定はPC上から専用ツール(NSSetup)にて行います。 認証キーの設定のみで完了する基本的な対向通信から、詳細なセキュリティポリシーの設定による経路別の動作指定といった応用的な用途まで幅広く柔軟に対応できます。</p> <p>高速・安定動作 ASICによるハードウェア処理により、最90Mbps(AES、512byte/pkt双方向通信時のSmartbit値)の高速で安定した動作を実現しています。</p> <p>NAT対応 NAT-Traversal/UDP-EncapsulationによるNAT越えを実現</p> <p>RoHS指令対応</p>

企業名	株式会社アクアシステムズ
所在地	〒160-0022 新宿区新宿1-10-4
窓口部署名 / 電話番号	/ 03-5363-5556
ホームページのURL	http://www.aqua-systems.co.jp
対象技術	技術の概要・特徴など
通信情報	Oracleデータベースへのアクセスを監査しログを保管する

企業名	KDDI株式会社
所在地	〒102-8460 東京都千代田区飯田橋3-10-10ガーデンエアタワー
窓口部署名 / 電話番号	ネットワーク技術本部技術戦略部 / 03-3347-0077
ホームページのURL	http://www.kddi.com
対象技術	技術の概要・特徴など
サーバ	<p>2000年に多数のWebサイトを一齐に改ざんされた事件や、2010年には多くの人が集まるサイトにウイルスが埋め込まれる事件など、今もなおホームページの改ざん事件が頻発しています。</p> <p>企業のホームページの中には、200回/月の頻度で更新されるという統計結果も出ており、Webアプリケーションなどの脆弱性を完全に排除しきれないことで発生する改ざん攻撃に対する脅威が高まっています。</p> <p>そこでKDDIでは、センター局から各地のWebサイトを巡回して、改ざんの有無を監視するシステムを開発しました。</p> <p>これは定期的によりモートのWebサイトからホームページファイルをダウンロードして、前回取得したファイルと新たなファイルを比較します。</p> <p>もし改ざん化が検知されると、ホームページの構文を解析し、改ざんに見られる特徴の有無とその組み合わせを検査して「更新」と「改ざん」を見分けてアラームを発信します。</p> <p>また、Webサーバーの問題やネットワーク遅延も「障害」としてアラームを発信します。</p>

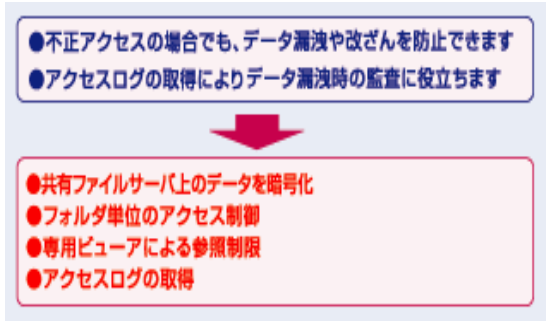

企業名	メトロ株式会社
所在地	〒141-0011 東京都品川区北品川5-9-15渡辺ビル
窓口部署名 / 電話番号	営業本部第三営業部 / 03-5789-1022
ホームページのURL	<a href="http://www.metro.co.jp/">http://www.metro.co.jp/</a>
対象技術	技術の概要・特徴など
クライアント	<p>ハードディスク暗号化</p> <p>OS領域やシステムファイル領域を含め、ハードディスク全体をを自動で暗号化するため、ユーザが特別な操作をする必要がなく、暗号化を意識せずに、これまでと同様にPCを使用することが可能です。また、ロックを解除する鍵そのものも暗号化するため、ハードディスクを抜き取り、何らかのツールで解析を試みたとしても、除法を解読することは不可能です。</p> <p>OS起動前のログイン認証</p> <p>OS起動前の認証機能で、第三者による不正ログインを防止します。CheckPointFullDiscEncryptionの認証をパスしなければ、OSを機動することさえできません。</p> <p>またログイン試行回数の制限ができるため、設定回数を超えるパスワード入力失敗時にアカウントをロックすることが出来ます。</p>

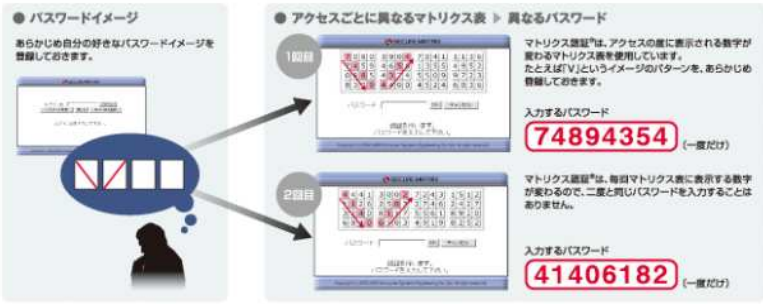
企業名	メトロ株式会社
所在地	〒141-0011 東京都品川区北品川5-9-15渡辺ビル
窓口部署名 / 電話番号	営業本部第三営業部 / 03-5789-1022
ホームページのURL	<a href="http://www.metro.co.jp/">http://www.metro.co.jp/</a>
対象技術	技術の概要・特徴など
クライアント	<p>メディアの暗号化</p> <p>USBメモリやCD/DVDメディア、外部メモリーカード、外付けハードディスクなど、リムーバルメディアは、MEが導入されていないPCでもデータの暗号・複合ができるので、利便性を損ないません。またCD-R/RW、DVD-R/RWへの複合書込も可能です。</p> <p>デバイス制御機能</p> <p>PCに損悪USBや工学ドライブ、無線LAN、Bluetooth、プリンタなど、各ポート/デバイスの利用を制限し、企業内のデータとエンドポイントPCを保護します。</p> <p>外部メディアの利用が必要なユーザにのみの利用許可、また、通常利用禁止しているユーザに一時的に利用を許可するといった、臨機応変な対応も可能です。</p>

企業名	三菱電機株式会社
所在地	〒100-8310 東京都千代田区丸の内2-7-3
窓口部署名 / 電話番号	総務部企画課 / 03-3218-9075
ホームページのURL	<a href="http://www.mitsubishielectric.co.jp">http://www.mitsubishielectric.co.jp</a>
対象技術	技術の概要・特徴など
データ	ファイルの暗号化による情報漏洩防止 ハードディスクの逐次暗号化

企業名	三菱電機株式会社
所在地	〒100-8310 東京都千代田区丸の内2-7-3
窓口部署名 / 電話番号	総務部企画課 / 03-3218-9075
ホームページのURL	<a href="http://www.mitsubishielectric.co.jp">http://www.mitsubishielectric.co.jp</a>
対象技術	技術の概要・特徴など
サーバ	WebシステムのSaaS型診断サービス

企業名	ログジット株式会社
所在地	〒170-0005 東京都豊島区南大塚2-25-15
窓口部署名 / 電話番号	監理部 / 03-5918-1531
ホームページのURL	<a href="http://www.logit.co.jp">http://www.logit.co.jp</a>
対象技術	技術の概要・特徴など
通信情報	Eメールのアーカイブでの監査認証

企業名	株式会社日立ソリューションズ
所在地	〒140-0002 東京都品川区東品川4-12-7日立ソリューションズタワーA
窓口部署名 / 電話番号	広報・宣伝部広報グループ / 03-5780-2111
ホームページのURL	http://www.hitachi-solutions.co.jp/
対象技術	技術の概要・特徴など
サーバ 通信情報 データ	<p>ファイルサーバの暗号化、アクセス制御、ログ取得 ファイルサーバ上のデータを暗号化、フォルダ単位でのアクセス制御でデータの漏洩や改ざんを防ぎます。また、ファイルサーバ上の暗号化したデータへのアクセスログを取得します。</p>   <p>データ参照のための認証も、ID、パスワードを入力する手動ログイン、自動ログイン、USBトークンを資料した証明書ログイン等があります。</p> <p>秘文シリーズ 「秘文」はオフィスのIT環境において、情報の持ち出しのコントロール、また持ち出した情報を保護することで安全な情報の活用を実現する「秘文AEシリーズ」、セキュリティ運用状況の把握と可視化により、マネージメントを実現する「秘文MEシリーズ」、システム管理者が不在でも、「ファイル持ち出し」や「暗号化」など機能をPC一台から低コストで導入・運用できる「秘文LEシリーズ」があります。</p>

企業名	株式会社シー・エス・イー
所在地	〒150-0044 東京都渋谷区円山町23-2アレットウーサ渋谷ビル
窓口部署名 / 電話番号	事業企画部マーケティング課 / 03-3463-5633
ホームページのURL	http://www.cseltd.co.jp/
対象技術	技術の概要・特徴など
ネットワーク サーバ クライアント	<p>SECUREMATRIXは、株式会社シー・エス・イーが開発した、認証デバイスを一切使わない本人認証システムです。人が頭の中に思い描くイメージからワンタイムパスワードを生成する「マトリクス認証」方式を採用し、セキュリティおよび利便性の向上、コスト削減のすべてを同時に実現します。</p> <p>&lt;マトリクス認証の仕組み&gt;</p> <p>「マトリクス認証」は、ユーザがあらかじめ設定した「位置」と「順番」(＝イメージパスワード)を使って、マトリクス表(アクセスするたびにランダムに表字が変わる乱数表)から、その位置と順番に当てはまる数字を抜き出してワンタイムパスワードとして認識させる認証方式です。パスワードは「ワンタイム(使い捨て)」になるため、強固な認証を実現できます。</p>  <p>複雑なパスワードをもう覚える必要はありません。また高価な認証デバイスを利用する必要はありません。コストを削減したい「企業」や、セキュリティを高めたい「IT管理者」、また面倒なことはしたくない「社員」など、様々な立場の方が抱えるパスワードに関する悩みを一気に解決するのが「SECUREMATRIX」です。</p>

企業名	株式会社インテリジェントウェイブ
所在地	〒104-0033 東京都中央区新川1-21-2芽場町タワー
窓口部署名 / 電話番号	セキュリティシステム事業部 / 03-6222-7151
ホームページのURL	http://www.iwi.co.jp
対象技術	技術の概要・特徴など
クライアント データ	<p>&lt;概要&gt;</p> <p>CWATは、インテリジェントウェイブが金融企業向けシステムのインフラ構築で培った技術を基に開発した、パソコンからの情報漏洩を防止するソフトウェアです。</p> <p>ユーザのパソコン操作を監視し、セキュリティポリシーに違反した操作を検知し、管理者に通知するとともに、警告情報(警告ログ)とパソコンの操作情報(監視ログ)を蓄積します。外部デバイスの接続や外部記憶メディアへのデータ書出し、印刷、メール送信、Web操作、閲覧中のウインドウタイトル等、ユーザのPC操作をきめ細かく監視できます。また、セキュリティポリシーに違反した不正な操作については監視サーバにリアルタイムに警告を発信するとともに、操作の中止等の対処を行うことも可能です。さらに、CWATで蓄積した「警告ログ」によって不正操作を即座に把握し、不正操作を「監査ログ」によって追跡する(つきとめる)ことができます。これにより効率かつ効果的にログ運用が可能になります。社内のPCを集中管理し、企業の生産性を低下させることなく柔軟な企業情報セキュリティ環境を実現できます。</p> <p>&lt;特徴&gt;</p> <ul style="list-style-type: none"> <li>・トータルな企業情報セキュリティ 「情報漏洩の防止」、「フォレンジック(証跡管理)」双方の観点から企業情報セキュリティを管理します。</li> <li>・類のない充実した「ログ」機能 情報セキュリティ管理の基本となる「ログ」。CWATでは、記録される操作内容・項目が極めて充実しているのが特長です。</li> <li>・優れたリアルタイム性 CWATが検知した様々な操作に対して、警告の発言や操作の中止など、リアルタイムに対処することが可能です。</li> <li>・グローバルに展開可能 マルチ言語対応により海外を含めたワールドワイドなセキュリティ対策が可能。</li> <li>・柔軟なセキュリティポリシー設計 CWATのポリシーは、端末、ユーザ、組織、エリア、ユーザーグループ、端末グループを対象に適用でき、さらに曜日・時間帯毎に設定できるので、企業の業務に沿った柔軟な運用が可能です。</li> </ul>

企業名	株式会社インテリジェントウェイブ
所在地	〒104-0033 東京都中央区新川1-21-2芽場町タワー
窓口部署名 / 電話番号	セキュリティシステム事業部 / 03-6222-7151
ホームページのURL	http://www.iwi.co.jp
対象技術	技術の概要・特徴など
データ その他	<p>1.概要</p> <p>Microsoft OfficeやAdobe PDFなどで作成した文書ファイルを暗号化し          捜査権限を付与することで、情報漏洩/改竄を防止し、文書ファイルの          操作ログを取得することにより内部統制強化を支援します。</p> <p>2.特徴</p> <p>まったく意識せず文書ファイルの暗号化が可能</p> <p>EUCSecureは、利用するPCにEUCSecureクライアントプログラムをイン          ストールすることにより、細かな設定なしにWord形式、Excel形式、PDF          形式の文書ファイルの暗号化、複合化を行うことができます。また、          AES(Advanced Encryption Standard)暗号方式の暗号エンジンを採用し          ているため、標準かつ安全性の高い情報セキュリティが容易に実現し          ます。ファイル単位はもちろん、フォルダ単位でのファイル一括暗号          化、利用制限設定もすることができます。</p> <p>文書ファイルの利用用途に合わせた利用条件設定が可能</p> <p>EUCSecureは、文書ファイルを暗号化する際に文書ファイルは配布利用          先の利用用途に合わせてファイルの「参照・編集(更新)・印刷・削除」          といった利用条件を付与することが可能です。サーバと接続できない          状態やコピーされたファイルの利用条件も設定することができます。          ファイル利用の有効期限を設定することもできます。</p> <p>文書ファイル操作ログの取得と蓄積</p> <p>文書ファイルの暗号化・利用条件の設定により、その文書ファイルで          行われた参照、編集(更新)、印刷といったファイル操作の利用履歴(ロ          グ)を取得します。また、取得したログは簡易ビューワ機能により文書          ファイル内での参照が可能です。また、専用のログサーバプログラム          を特定のサーバ機器に導入することにより、上記のファイル操作に加          え、文書ファイルの削除操作についてもログを取得することが可能と          なります。この機能により、多数の文書ファイルの操作履歴をログサ          ーバで一元的に管理、参照することが可能となります。</p>