平成22年3月4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21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

○　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21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21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21年中の不正アクセス行為の認知件数は2,795件で、前年と比べ、506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17年 | 平成18年 | 平成19年 | 平成20年 | 平成21年 |
|---|---|---|---|---|---|
| 認知件数（件） | 592 | 946 | 1,818 | 2,289 | 2,795 |
| 海外からのアクセス | 53 | 37 | 79 | 214 | 40 |
| 国内からのアクセス | 487 | 855 | 1,684 | 1,993 | 2,673 |
| アクセス元不明 | 52 | 54 | 55 | 82 | 82 |

#### (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（2,321件）、次いで一般企業（466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17年 | 平成18年 | 平成19年 | 平成20年 | 平成21年 |
|---|---|---|---|---|---|
| プロバイダ（件） | 356 | 602 | 1,372 | 1,589 | 2,321 |
| 一般企業 | 203 | 325 | 437 | 685 | 466 |
| 大学、研究機関等 | 12 | 6 | 1 | 5 | 4 |
| その他 | 21 | 13 | 8 | 10 | 4 |
| うち行政機関 | 17 | 5 | 5 | 6 | 3 |
| 不明 | 0 | 0 | 0 | 0 | 0 |
| 計 | 592 | 946 | 1,818 | 2,289 | 2,795 |

※　「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（2,277件）、次いで利用権者（注２）からの届出によるもの（487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（21件）、発見者からの通報によるもの（７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17年 | 平成18年 | 平成19年 | 平成20年 | 平成21年 |
|---|---|---|---|---|---|
| 警察活動（件） | 33 | 535 | 1,326 | 1,567 | 2,277 |
| 利用権者からの届出 | 505 | 358 | 415 | 656 | 487 |
| アクセス管理者からの届出 | 30 | 45 | 61 | 60 | 21 |
| 発見者からの通報 | 14 | 3 | 2 | 4 | 7 |
| その他 | 10 | 5 | 14 | 2 | 3 |
| 計 | 592 | 946 | 1,818 | 2,289 | 2,795 |

### (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（2,152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）（345件）、情報の不正入手（電子メールの盗み見等）（185件）、インターネットバンキングの不正送金（34件）、ホームページの改ざん・消去（33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）（２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20年 | 平成21年 |
|---|---|---|
| インターネット・オークションの不正操作（件） | 1,559 | 2,152 |
| オンラインゲームの不正操作 | 457 | 345 |
| 情報の不正入手 | 46 | 185 |
| インターネットバンキングの不正送金 | 37 | 34 |
| ホームページの改ざん・消去 | 152 | 33 |
| 不正ファイルの蔵置 | 5 | 2 |
| その他 | 33 | 44 |

## 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21年中における不正アクセス禁止法違反の検挙件数は2,534件、検挙人員は114人と、前年と比べ、検挙件数は794件増加し、検挙人員は23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2,532件、114人、不正アクセス助長行為（注４）に係るものがそれぞれ２件、１人であった。

表２－１　検挙件数等の推移

| 区分＼年次 | | 平成17年 | 平成18年 | 平成19年 | 平成20年 | 平成21年 |
|---|---|---|---|---|---|---|
| 不正アクセス行為 | 検挙件数 | 271 | 698 | 1,438 | 1,737 | 2,532 |
| | 検挙事件数（注５） | 94 | 84 | 86 | 101 | 95 |
| | 検挙人員 | 113 | 130 | 126 | 135 | 114 |
| 不正アクセス助長行為 | 検挙件数 | 6 | 5 | 4 | 3 | 2 |
| | 検挙事件数 | 6 | 3 | 2 | 3 | 1 |
| | 検挙人員 | 6 | 5 | 4 | 3 | 1 |
| 計 | 検挙件数（件） | 277 | 703 | 1,442 | 1,740 | 2,534 |
| | 検挙事件数（事件） | 94 (重複6) | 84 (重複3) | 86 (重複2) | 101 (重複3) | 95 (重複1) |
| | 検挙人員（人） | 116 (重複3) | 130 (重複5) | 126 (重複4) | 137 (重複1) | 114 (重複1) |

※　(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2,529件であり、セキュリティ・ホール攻撃型（注７）は３件であった。

表２－２　不正アクセス行為の態様の推移

| 区分＼年次 | | 平成17年 | 平成18年 | 平成19年 | 平成20年 | 平成21年 |
|---|---|---|---|---|---|---|
| 識別符号窃用型 | 検挙件数 | 264 | 698 | 1,438 | 1,736 | 2,529 |
| | 検挙事件数 | 90 | 84 | 86 | 100 | 94 |
| セキュリティ・ホール攻撃型 | 検挙件数 | 7 | 0 | 0 | 1 | 3 |
| | 検挙事件数 | 5 | 0 | 0 | 1 | 1 |
| 計 | 検挙件数（件） | 271 | 698 | 1,438 | 1,737 | 2,532 |
| | 検挙事件数（事件） | 94 (重複1) | 84 | 86 | 101 | 95 |

※　(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（2,084件）が最も多く、次いで、共犯者等から入手したもの（167件）、他人から購入したもの（92件）となっている。

また、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（61件）、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（58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）、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（８件）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20年 | 平成21年 |
|---|---|---|---|
| 識別符号窃用型（件） | | 1,736 | 2,529 |
| | フィッシングサイトにより入手したもの | 88 | 2,084 |
| | 共犯者等から入手したもの | 7 | 167 |
| | 他人から購入したもの | 24 | 92 |
| | 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 | 163 | 61 |
| | 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 | 1,368 | 58 |
| | 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 | 26 | 12 |
| | 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 | 48 | 8 |
| | 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 | 6 | 0 |
| | その他 | 6 | 47 |
| セキュリティ・ホール攻撃型 | | 1 | 3 |

### (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（57人）、次いで交友関係のない他人によるもの（49人）、ネットワーク上のみの知り合いによるもの（８人）となっている。

また、被疑者の年齢についてみると、30歳代（35人）が最も多く、20歳代（33人）、10歳代（31人）、40歳代（13人）、50歳代（２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59歳であった。

表３－２　年代別被疑者数の推移

| 区分＼年次 | 平成17年 | 平成18年 | 平成19年 | 平成20年 | 平成21年 |
|---|---|---|---|---|---|
| 10歳代（人） | 35 | 40 | 39 | 48 | 31 |
| 20歳代 | 40 | 44 | 39 | 42 | 33 |
| 30歳代 | 27 | 28 | 34 | 35 | 35 |
| 40歳代 | 9 | 15 | 12 | 11 | 13 |
| 50歳代 | 5 | 2 | 2 | 1 | 2 |
| 60歳代 | 0 | 1 | 0 | 0 | 0 |
| 計 | 116 | 130 | 126 | 137 | 114 |

※　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（2,245件）が最も多く、次いで好奇心を満たすため（165件）、オンラインゲームで不正操作を行うため（63件）、嫌がらせや仕返しのため（34件）、顧客データの収集等情報を不正に入手するため（19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20年 | 平成21年 |
|---|---|---|
| 不正に金を得るため（件） | 1,498 | 2,245 |
| 好奇心を満たすため | 17 | 165 |
| オンラインゲームで不正操作を行うため | 120 | 63 |
| 嫌がらせや仕返しのため | 52 | 34 |
| 顧客データの収集等情報を不正に入手するため | 12 | 19 |
| 料金の請求を免れるため | 3 | 4 |
| その他 | 35 | 2 |
| 計 | 1,737 | 2,532 |

(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（2,529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（2,147件）、次いで電子メール（167件）、オンラインゲーム（88件）、インターネットバンキング（83件）、ホームページ公開サービス（16件）、会員専用・社員用内部サイト（10件）、インターネットショッピング（３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20年 | 平成21年 |
|---|---|---|---|
| 識別符号窃用型（件） | | 1,736 | 2,529 |
| | インターネット・オークション | 1,381 | 2,147 |
| | 電子メール | 39 | 167 |
| | オンラインゲーム | 138 | 88 |
| | インターネットバンキング | 14 | 83 |
| | ホームページ公開サービス | 133 | 16 |
| | 会員専用・社員用内部サイト | 21 | 10 |
| | インターネットショッピング | 5 | 3 |
| | その他 | 5 | 15 |

## ４　都道府県公安委員会による援助措置

平成21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17年 | 平成18年 | 平成19年 | 平成20年 | 平成21年 |
|---|---|---|---|---|---|
| 援助措置（件） | 4 | 3 | 0 | 1 | 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　パスワードの適切な管理・設定

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、知人等による不正アクセス行為、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、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を適切に管理する。また、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、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。

ウ　スパイウェア等の不正プログラムに対する注意

電子メールに添付し、若しくはサイト上に蔵置したファイルからスパイウェア等の不正プログラムに感染させ、又はインターネットカフェ等のコンピュータにキーロガー（注９）等の不正プログラムを仕掛け、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。

(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・オークション、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っては、ワンタイムパスワード（注10）等により個人認証を強化するなどの対策を講ずる。

イ　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。

ウ　パスワードの適切な設定

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や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。

エ　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11）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等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 | 関連会社社員のＩＤ・パスワードを用いて不正アクセスを行い、顧客情報を取得した上、その情報を書き込んだＣＤ－Ｒを持ち出した不正アクセス禁止法違反及び窃盗事件 |

社内のシステム開発業務を担当していた男（44）は、会社が保有する顧客情報を不正に取得して売却しようと企て、平成21年１月、同社の認証サーバーコンピュータに関連会社社員のＩＤ・パスワードを用いて不正アクセスを行い、顧客情報を取得した上、その顧客情報を書き込んだＣＤ－Ｒを持ち出した。平成21年６月、不正アクセス禁止法違反及び窃盗罪で検挙した（警視庁）。

| | |
|---|---|
| 2 | 他人のＩＤ・パスワード等を使用してインターネットバンキングに不正アクセスを行い、電子マネーを購入後、現金に換金してい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 |

無職の男（21）は、平成20年12月、出身高専のＦＴＰサーバに侵入し、ファイルに書かれていた被害者のインターネットバンキングのＩＤ・パスワード等を入手してインターネットカフェ等から不正アクセスを行い、身元を隠すためいったん電子マネーを購入後、現金に換金した。平成21年４月、不正アクセス禁止法違反及び電子計算機使用詐欺罪等で検挙した（京都）。

| | |
|---|---|
| 3 | メールを盗み見して入手したＩＤ・パスワード等を使用してインターネットバンキングに不正アクセスを行い、現金を不正送金してい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 |

清掃業の男（35）は、平成21年１月、インターネットサイトに掲示されていたメールアドレス・パスワードを使用してメールを盗み見た後、メールに書かれていたインターネットバンキングのＩＤ・パスワード等を使用してインターネットカフェから不正アクセスを行い、拾得した他人の運転免許証を使用して不正取得した銀行口座に不正送金した。平成21年７月、不正アクセス禁止法違反及び電子計算機使用詐欺罪等で検挙した（石川）。

| | |
|---|---|
| 4 | インターネット・オークションに出品可能な他人のＩＤ・パスワードを販売するとともに、自らもオークション詐欺を行っていた不正アクセス禁止法違反及び詐欺事件 |

留学生の男（23）は、平成20年１月から３月までの間、共犯者から入手したＩＤ・パスワードがインターネット・オークションに出品可能かを確認するためそのＩＤ・パスワードを使用して不正アクセスを行い、出品可能なＩＤ・パスワードを販売して

いた。また、自らプラズマテレビをインターネット・オークションに架空出品し、詐欺を行った。平成21年３月、不正アクセス禁止法違反及び詐欺罪で検挙した（群馬）。

| 5 | 他人のＩＤ・パスワードを不正入手し、インターネット・オークションに不正アクセスを行った不正アクセス禁止法違反及び詐欺事件 |
|---|---|

とび職の男（24）らは、平成20年５月から６月までの間、インターネット上で購入した他人名義のＩＤ・パスワードを使用して、インターネットカフェからインターネット・オークションに不正アクセスを行い、商品を売ると偽り落札者から代金をだまし取った。平成21年10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（静岡）。

（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　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　キーロガー
　キーボードでどの文字が入力されたかを記録するプログラムをいう。

注10　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11　リカバリーソフト
　正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。

## 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 21 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 149 件（平成 20 年：155 件）であった。（注２）

平成 21（2009）年は同 20（2008） 年と比べて、6 件（約 4%）減少した。

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 254 件（平成 20 年：334 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 211 件（平成 20 年：276 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。

20 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。

110 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 37 件である。

【主な内容】

パスワード推測：42 件

ソフトウェアの脆弱性やバグを利用した攻撃：18 件

システムの設定内容を利用した攻撃：2 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 81 件の届出があった。

【主な内容】

ファイル等の改ざん、破壊等：32 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：19 件

資源利用（ファイル、CPU 使用）：16 件

踏み台とされて他のサイトへのアクセスに利用された：5 件

証拠の隠滅（ログの消去など）：2 件

裏口（バックドア）の作成：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。6 件（平成 20 年：14 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、37 件（平成 20 年：44 件）の届出があった。

【主な内容】

正規ユーザへのなりすまし：31 件

メール不正中継：2 件

メールアドレス（ドメイン）の詐称：2 件

ソーシャルエンジニアリング：1 件

オープンプロキシ：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。

149 件の届出中、実際に被害に遭った計 96 件（平成 20 年：120 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】

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：16 件

ID、パスワード管理の不備によると思われるもの：11 件

設定の不備（セキュリティ上問題のあるデフォルト設定を含む）によるもの：6 件

DoS 攻撃・その他によるもの：9 件

原因不明：54 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：62 件

クライアント：23 件

メールサーバ：20 件

ルータ：4 件

ファイアウォール：2 件

その他のサーバ：12 件

不明：2 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

149 件の届出を被害内容で分類した 160 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 107 件（平成 20 年：156 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】

オンラインサービスの不正利用：32 件

ファイルの書き換え：30 件

ホームページ改ざん：14 件

踏み台として悪用：7 件

データの窃取や盗み見：7 件

サービス低下：5 件

メール不正中継：2 件

オープンプロキシ：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 21 年は、ID／パスワード不備や脆弱性が原因でサイトに侵入されて他サイト攻撃のための踏み台にされたりウェブページを改ざんされたりしたケースや、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が特に目立っていたと言える。特に「なりすまし」被害については、原因が不明なケースがほとんどであった。「なりすまし」被害以外では、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
「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
「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
「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
「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

【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.mspx

MyJVN（セキュリティ設定チェッカ、バージョンチェッカ）
http://jvndb.jvn.jp/apis/myjvn/

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 21 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。

### (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 7,435 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 1,146 件の報告があった。

[1/1-3/31: 171 件、4/1-6/30: 278 件、7/1-9/30:469 件、10/1-12/31: 228 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 500 件の報告があった。

[1/1-3/31: 26 件、4/1-6/30: 74 件、7/1-9/30:28 件、10/1-12/31: 372 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 2 件の報告があった。

[1/1-3/31: 2 件、4/1-6/30: 0 件、7/1-9/30:0 件、10/1-12/31: 0 件]

#### 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 20 件の報告があった。

[1/1-3/31:3 件、4/1-6/30:6 件、7/1-9/30:4 件、10/1-12/31:7 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 1,021 件の報告があった。

[1/1-3/31: 182 件、4/1-6/30: 200 件、7/1-9/30: 303 件、10/1-12/31:336 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 4,746 件の報告があった。**
[1/1-3/31:300 **件**、4/1-6/30:823 **件**、7/1-9/30:2,337 **件**、10/1-12/31:1,286 **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**]

2009 **年** 1 **月**　Microsoft **セキュリティ情報 (緊急** 1 **件含) に関する注意喚起**
2009 **年** 2 **月**　Microsoft **セキュリティ情報 (緊急** 2 **件含) に関する注意喚起**
Adobe Flash Player **の脆弱性に関する注意喚起**
2009 **年** 3 **月**　Microsoft **セキュリティ情報 (緊急** 1 **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**
2009 **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**
2009 **年** 5 **月**　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**
JavaScript **が埋め込まれる** Web **サイトの改ざんに関する注意喚起**
2009 **年** 6 **月**　Microsoft **セキュリティ情報 (緊急** 6 **件含) に関する注意喚起**
2009 **年** 7 **月**　**韓国、米国で発生している** DDoS **攻撃に関する注意喚起**
Microsoft **セキュリティ情報 (緊急** 3 **件含) に関する注意喚起**
Microsoft ATL **を使用した複数製品の脆弱性に関する注意喚起**
Adobe Flash Player **及び** Adobe Acrobat/Reader **の脆弱性に関する注意喚起**
ISC BIND 9 **の脆弱性を使用したサービス運用妨害攻撃に関する注意喚起**
2009 **年** 8 **月**　Microsoft **セキュリティ情報 (緊急** 5 **件含) に関する注意喚起**
2009 **年** 9 **月**　Microsoft **セキュリティ情報 (緊急** 5 **件) に関する注意喚起**
**複数製品の** TCP **プロトコルの脆弱性に関する注意喚起**
2009 **年** 10 **月**　Microsoft **セキュリティ情報 (緊急** 8 **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**
**マイクロソフト社を騙るマルウエア添付メールに関する注意喚起**
Web **サイト経由でのマルウエア感染拡大に関する注意喚起**
2009 **年** 11 **月**　Microsoft **セキュリティ情報 (緊急** 3 **件) に関する注意喚起**
2009 **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**

Adobe Flash Player の脆弱性に関する注意喚起
Adobe Reader 及び Acrobat の未修正の脆弱性に関する注意喚起

イ　活動概要（報告状況等の公表）

発行日：2010-01-12 [ 2009 年 10 月 1 日～ 2009 年 12 月 31 日]
発行日：2009-10-08 [ 2009 年 7 月 1 日 ～ 2009 年 9 月 30 日]
発行日：2009-07-09 [ 2009 年 4 月 1 日 ～ 2009 年 6 月 30 日]
発行日：2009-04-07 [ 2009 年 1 月 1 日 ～ 2009 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] 264 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.jpcert.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。

## 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 143 件であった(詳細は http://jvn.jp/ 参照。)

[1/1-3/31:31 件、4/1-6/30: 45 件、7/1-9/30: 36 件、10/1-12/31: 31 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 79 件であった。

[1/1-3/31:16 件、4/1-6/30: 30 件、7/1-9/30: 17 件、10/1-12/31: 16 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
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
接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
マルウエア対策ユーザサポートシステムの研究開発
証明可能な安全性をもつキャンセラブル･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21年12月8日から12月28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。

タレスジャパン株式会社
大日本印刷株式会社
デュアキシズ株式会社

#### (2)　調査

警察庁が平成21年10月から平成21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

信州大学
東京都市大学
静岡大学

イ　企業

株式会社コア
三和コムテック株式会社
メデイアファイブ株式会社
GMOインターネット株式会社
株式会社福山コンサルタント

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）

**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、（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)

**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
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**　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。
(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。

**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
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。（実証実験においては、特に、医療分野でのネットワーク利用におけるセキュリティ確保、利便性向上に効果があることが分かっている。）

**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中。
(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中。

(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中。
(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**　その他認証技術

**テーマ名**　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

**開発年度**　平成20年度～平成22年度

**実施主体**　株式会社ラック、財団法人九州先端科学技術研究所、株式会社セキュアウェア、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）

**背景、目的**

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の見間違え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。

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。

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。

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。

**研究開発状況（概要）**

・平成20年度より以下の研究開発を実施中。
(1) 攻撃及び関連マルウェアの高速・高精細攻撃検知・収集
(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
(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
(4) 実環境で有効に機能させるための実証実験
・平成22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21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、マルウエアの収集機構・収集したマルウエ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・攻撃検出機構の開発、マルウェアの分析精度の高度化を行った。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。

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更に高速化が可能な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開始した。また海外研究機関と連携し、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を進めた。

**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**　マルウエア対策ユーザサポートシステムの研究開発

**開発年度**　平成21年度～平成23年度

**実施主体**　株式会社日立製作所、KDDI株式会社

**背景、目的**

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および自動駆除の仕組みを実現することを目的とする。

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）に基づくアンチウィルスソフトである。

アンチウィルスソフトでは、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。

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、ボ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ボットや既知のボットのみを取り扱っており、アンチウィルスソフトと同様な問題が見受けられる。

また、情報処理推進機構（IPA）では、ウィルス情報iPedia（ウィルス情報データベース）において、届出されたウィルスやボットなどを中心に、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。

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、アンチウィ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。

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。

**研究開発状況（概要）**

・ 平成２１年度より以下の研究開発を実施中。

（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エ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、マルウエ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。

（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１０分程度で完了することを実現する。

**詳細の入手方法（関連部署名及びその連絡先）**

独立行政法人情報通信研究機構　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**　証明可能な安全性をもつキャンセラブル・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

**開発年度**　平成20年度～平成21年度

**実施主体**　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）

**背景、目的**

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している。

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。

**研究開発状況（概要）**

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。

(1) 安全性評価基準の理論的枠組みの構築

(2) 証明可能安全性をもつキャンセラブル認証技術の研究開発

(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ている。

(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

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ている。

(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の構築

(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する。

**詳細の入手方法（関連部署名及びその連絡先）**

独立行政法人 産業技術総合研究所　情報セキュリティ研究センター

電話: 03-5298-4722　Web: http://www.rcis.aist.go.jp/

**将来の方向性**

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。

**対象技術**　その他認証技術等

**テーマ名**　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

**開発年度**　平成20年度～

**実施主体**　株式会社日立製作所（経済産業省からの委託）

**背景、目的**

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している。

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ている。

**研究開発状況（概要）**

(a) 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

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ている。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ている。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影響評価を行っている。

(b) 情報漏えい対策技術の強度評価に関する研究開発

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ている。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の確立を目指している。

(c) 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

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」をまとめている。

**詳細の入手方法（関連部署名及びその連絡先）**

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
中西 潤、山田 知明（Tel:044-549-1214　Fax:044-549-1382）

**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、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。

(別添2)

| 企業名（及び略称）タレスジャパン株式会社 | |
|---|---|
| 代表者氏名　ミッシェル　テオヴァル | |
| 所在地（郵便番号及び住所）〒107-0052　東京都港区赤坂４丁目９番９号　赤坂MKビル４階 | |
| 関連部署名及び電話番号　インフォメーションシステムセキュリティー 03-5785-1975 | |
| URL　http://www.thalesgroup.com/ | |
| 対象技術 | 技術開発状況 |
| その他認証技術等 | 耐タンパー性のハードウェアセキュリティーモジュール(HSM)上で暗号秘密鍵だけでなく企業および政府機関独自の認証アルゴリズム保護実行することで、コンピュータウイルス感染や内部犯等による組織内ネットワークからの機密識別情報の漏洩や認証アルゴリズムの改ざんを防止することができます。<br>この技術を既存のパスワード認証基盤や生体認証基盤に実装することで電子化された機密識別情報のエンド・ツー・エンドによる暗号化認証が可能となり強固な認証基盤が構築できます。認証処理中でもサーバー上のメモリやファイルシステムおよび認証データーベース上において機密情報が平文で漏洩することを防ぎます。 |

| 企業名（及び略称）大日本印刷株式会社 | |
|---|---|
| 代表者氏名　代表取締役社長　北島　義俊 | |
| 所在地（郵便番号及び住所）〒162-8001　東京都新宿区市谷加賀町一丁目１番１号 | |
| 関連部署名及び電話番号　ＩＰＳ事業部　セキュリティソリューション営業部 | |
| URL　http://www.dnp.co.jp/bf/ss/ | |
| 対象技術 | 技術開発状況 |
| その他認証技術等<br>（2009年） | 【ＵＳＢシンクライアント】<br>専用ＵＳＢデバイスをＰＣのＵＳＢポートに挿入し、ＰＣを起動することにより、そのＰＣをシンクライアント端末として利用できる。システムはＵＳＢデバイス、認証用サーバ、業務用サーバで構成され、データ保存はサーバのみ可能で、ＰＣのＨＤＤや外部記憶装置への保存は不可能となる。ＵＳＢデバイスには、ＵＳＢフラッシュメモリのほかに小型のICカードが組み込まれており、フラッシュメモリ内のサーバ接続プログラムの正当性をＩＣカードの電子署名機能により確認している。この手続きを経て、正当性が確認された端末のみ業務用サーバに接続できるため、不正な接続を排除し、企業のネットワークにおいて、高い安全性を確保することが出来る。 |

| 企業名（及び略称）大日本印刷株式会社 | |
|---|---|
| 代表者氏名　代表取締役社長　北島　義俊 | |
| 所在地（郵便番号及び住所）〒162-8001　東京都新宿区市谷加賀町一丁目１番１号 | |
| 関連部署名及び電話番号　ＩＰＳ事業部　セキュリティソリューション営業部 | |
| URL　http://www.dnp.co.jp/bf/ss/ | |
| 対象技術 | 技術開発状況 |
| その他認証技術等<br>（2005年） | 【ＳＳＦＣ】<br>「Shared Security Formats Cooperation」の略。１９０社以上の国内の主要な企業が参加している。１枚の非接触ＩＣカードをＩＤカードとして用いて、セキュリティを向上させることを目的としたアライアンス。<br><br>ＳＳＦＣ仕様では、ＩＤ情報と入室情報などは、共有情報として定義されている。他の同種の仕組みと比較して、ＳＳＦＣで特徴的なところは、各セキュリティシステムが利用する情報は業界別に割り当てており、業界が同じ場合はその領域を共同利用する点である。現在定義されている業界は、ゲートシステムを中心とした業界、監視カメラ業界、ファニチャー業界、プリンター業界と、少し色合いが異なるがソフト業界もＳＳＦＣ情報を利用している。<br><br>最も大きな特徴は、異なる業界のシステムやアプリケーション間でデータ連携が可能となるようＳＳＦＣで仕様を策定している点である。<br><br>この仕組みが仕様として策定されている為、副巣の機器を一度に導入することになく、必要な時期に必要なセキュリティ機器を導入すればよいと言うメリットと、連携によるセキュリティの向上と利便性を利用者に提供可能としている。<br><br>これらの各仕様はアライアンス参加企業にのみ限定して公開されており、物理的セキュリティ（入退室管理、監視カメラなど）とＳＳＦＣ対応セキュリティ機器利用のための論理的セキュリティを、１枚のＩＤカードを用いて融合しているだけでなく、福利厚生面等でも利用者の利便性向上を実現している。<br><br>現在、ＳＳＦＣアライアンス事務局は大日本印刷株式会社内に設置されている。 |

| 企業名（及び略称）大日本印刷株式会社 | |
|---|---|
| 代表者氏名　代表取締役社長　北島　義俊 | |
| 所在地（郵便番号及び住所）〒162-8001　東京都新宿区市谷加賀町一丁目１番１号 | |
| 関連部署名及び電話番号　ＩＰＳ事業部　セキュリティソリューション営業部 | |
| URL　http://www.dnp.co.jp/bf/ss/ | |
| 対象技術 | 技術開発状況 |
| その他認証技術等<br>（2006年） | 【ICカードによるネットワーク管理型PC個人認証】<br>情報システム利用者の権限情報と認証情報をサーバで集中管理し、ＰＣの不正利用、情報漏洩をシャットアウトする、ＩＣカードを利用したＰＣセキュリティシステム。ＳＳＦＣ製品との連携も可能。<br><br>●クライアント機能<br>ＩＣカードログオン認証/スクリーンロック、外部記憶デバイス利用制御、電子証明書（ＰＫＩ）の利用、ＳＳＦＣ連携機能（ＩＣカードの入室情報チェック）、操作ログ送信、など。<br><br>●管理サーバ機能<br>ユーザ認証情報、ポリシーをサーバにて一括管理<br><br>●管理者機能<br>ＰＩＮロック時やカード紛失時など、ユーザに対する緊急サポートをＷｅｂ上から容易に行うことが可能。 |

| 企業名（及び略称）大日本印刷株式会社 | |
|---|---|
| 代表者氏名　代表取締役社長　北島　義俊 | |
| 所在地（郵便番号及び住所）〒162-8001　東京都新宿区市谷加賀町一丁目１番１号 | |
| 関連部署名及び電話番号　ＩＰＳ事業部　セキュリティソリューション営業部 | |
| URL　http://www.dnp.co.jp/bf/ss/ | |
| 対象技術 | 技術開発状況 |
| その他認証技術等<br>（1999年,2009年） | 【ＩＣカード用ＰＫＩドライバ】<br>ＩＣカード内に格納された電子証明書や秘密鍵とブラウザ等の上位アプリケーションソフトとのＩ/Ｆ機能を提供するドライバソフトウェアで、各社の認証アプリケーションの部品として利用されている。<br>ＣＳＰ(※１)とＰＫＣＳ＃１１規格に対応している。<br><br>また新たに、異なるカードベンダーが提供するＩＣカードとＰＫＩ（※２）でも、相互利用が可能なＰＫＩアプリケーション規格「ＪＩＳ　Ｘ６３２０－１５」に準拠したＩＣカードとＰＫＩドライバ（Windows,Linux）の提供を２００９年１２月より開始した。<br><br>（※１）<br>ＣＳＰドライバは、Microsot社が定めた暗号ライブラリの規格である『CryptoAPI』に準拠しており、ＷｅｂブラウザのInternet ExplorerやメーラーのOutlook ExpressやWindowsメールがこれをサポートしています。<br><br>（※２）<br>ＰＫＩ（公開鍵暗号認証基盤;Public Key Infrastructure）とは、公開鍵暗号方式を用いて暗号化、デジタル署名、認証などを行うセキュリティインフラ。信頼できる認証局が電子証明書を発行して公開鍵の名義人を証明する。 |

| | |
|---|---|
| 企業名（及び略称）デュアキシズ株式会社 | |
| 代表者氏名　名古屋　貢 | |
| 所在地（郵便番号及び住所）〒103-0015　東京都中央区箱崎１－２<br>日本綜合地所サンワールドビル２F | |
| 関連部署名及び電話番号　開発部 050-5808-4021 | |
| URL　http://www.duaxes.co.jp/ | |
| 対象技術 | 技術開発状況 |
| その他認証技術等 | 通信データ中のヘッダからデータ部分までをハードウェアでチェックできる高速回路の開発を行っている。ハードウェア処理するため、1Gbpsや10bps、さらに高速な40Gbpsや100Gbpsの処理速度に対応することがｋな王である。この回路で、通信データの監視やユーザ毎の認証機能を実現することが可能である。<br>本技術は通信機器のプラットフォーム技術であり、多数の特許を包括的に取得済みである。出願件数を含めると、関連特許は300件近くに及んでいる。開発年は2004年である。<br>本技術を用いた製品開発も行っている。主な用途としてURLフィルタリング装置やメールフィルタリング装置、帯域制御装置などであり、既に、これらの装置を販売している。 |

(別添3)

【大学】

| 大学名　信州大学工学部 | |
|---|---|
| 所在地（郵便番号及び住所）　〒380-8553　長野市若里四丁目17番1号 | |
| 関連部署及び電話番号　総務グループ　庶務係 ／ 026-269-5004 | |
| URL　http://wwweng.cs.shinshu-u.ac.jp/ | |
| 対象技術 | 技術の概要・特徴など |
| その他 | 「いつ、どこで、だれが」印刷するのかを、印刷物受取人と印刷が許可されたプリンタによるPKI処理により制御するプリンティングシステムを研究し、これを塩尻市役所の業務で評価。 |

| 大学名　東京都市大学　情報処理センター研究室 | |
|---|---|
| 所在地（郵便番号及び住所）　〒158-8557　世田谷区玉堤1-28-1 | |
| 関連部署及び電話番号 | |
| URL | |
| 対象技術 | 技術の概要・特徴など |
| ネットワーク | IPパケットごとに認証情報をうめ込むことでパケット単位での認証を可能とするシステム。 |

| 大学名　静岡大学　情報基盤センター | |
|---|---|
| 所在地（郵便番号及び住所）　〒422-8529　静岡市駿河区大谷836 | |
| 関連部署及び電話番号　情報基盤センター ／ 054-238-4683 | |
| URL　http://www.ipc.shizuoka.ac.jp/icenter/ | |
| 対象技術 | 技術の概要・特徴など |
| ネットワーク<br>サーバ<br>クライアント<br>通信情報<br>データ | 大学の教員、学生の教育研究業務全般における情報リスクを最小にするような情報セキュリティ管理システム(ISMS)を構築し運用中である。<br>ISO27001を2007年に取得している。 |

【企業】

| 事業体(研究所)名　株式会社コア | |
|---|---|
| 所在地（郵便番号及び住所）　〒154-8552　東京都世田谷区三軒茶屋1-22-3 | |
| 関連部署及び電話番号　社長室 ／ 03-3795-5111 | |
| URL　http://www.core.co.jp/ | |
| 対象技術 | 技術の概要・特徴など |
| ネットワーク<br>クライアント<br>通信情報<br>その他 | ITILver3に準拠し、データセンターからPCプラットフォームまですべてのIT資産の「見える化」とコスト削減を実現します。 |

| 事業体(研究所)名　三和コムテック株式会社 | |
|---|---|
| 所在地（郵便番号及び住所）　〒106-0032　東京都港区六本木3-4-3　三和ビル | |
| 関連部署及び電話番号　カスタマーサービス企画 ／ 03-3583-2518 | |
| URL　http://www.sct.co.jp/ | |
| 対象技術 | 技術の概要・特徴など |
| サーバ<br>通信情報 | ・Webサイトを365日診断し、発見された弱点(脆弱性)とその対策を365日お知らせするセキュリティサービス<br>・診断に合格したサイトに証明マークを表示することで安全性を証明<br>・PCI-DSS(ペイメントカード業界データセキュリティ基準)、VISAが定めているAIS/CISP、MasterCardのSDPや、米国連邦政府系機関、また国際的かつ最高水準のセキュリティ基準に準拠・適合<br>・ハッカーが狙う対象となるWebサーバー以外のサーバーや、各種Webアプリケーションも対象とする<br>・診断項目は10,000を超え、ほぼすべてのサイト構成要素を診断対象とする。 |

| 事業体(研究所)名　三和コムテック株式会社 | |
|---|---|
| 所在地（郵便番号及び住所）　〒106-0032　東京都港区六本木3-4-3　三和ビル | |
| 関連部署及び電話番号　カスタマーサービス企画 ／ 03-3583-2518 | |
| URL　http://www.sct.co.jp/ | |
| 対象技術 | 技術の概要・特徴など |
| ネットワーク<br>サーバ<br>通信情報 | IBMI(AS/400,System I)のセキュリティに特化した製品。<br>・FTP、データ転送、ODBC接続などによる不正ダウンロードを防止<br>・重要なファイルのアクセス監視及び変更履歴監視<br>・ユーザーの操作履歴を画面で記録(画面遷移の記録)<br>・ログオンしたまま放置された端末の不正使用を防止<br>・不当なパスワードの作成防止<br>・不正アクセスログに対するリアルタイム検知(メッセージ送信やアクションを実行)<br>・ユーザープロファイルの一元管理(一覧表示、変更)<br>・監査帳票・アクセスログ集計帳票を簡単に作成可 |

| 事業体(研究所)名　メディアファイブ株式会社 | |
|---|---|
| 所在地（郵便番号及び住所）　〒810-0001　福岡県福岡市中央区天神3丁目14-31<br>天神リンデンビル2階 | |
| 関連部署及び電話番号　092-761-0078 | |
| URL　http://www.media5.co.jp/ | |
| 対象技術 | 技術の概要・特徴など |
| 通信情報 | キャノンITソリューションズ製のメールフィルタリングソフトを利用し、企業内から送信される電子メールに対して監視を行い、検出された異常内容を提携企業にレポートとして提出するサポート業務。提携企業からの技術面、運用面に関する問い合わせ対応。 |

| 事業体(研究所)名　GMOインターネット株式会社 | |
|---|---|
| 所在地(郵便番号及び住所)　〒150-8512　東京都渋谷区桜丘町26番-1号　セルリアンタワー | |
| 関連部署及び電話番号　システム本部 ／ 03-5456-2687 | |
| URL　http:// www.gmo.jp/ | |
| 対象技術 | 技術の概要・特徴など |
| クライアント<br>通信情報 | ASP型のVPNサービス<br>・ファイル共有(セキュア)<br>・リモートデスクトップで自宅PCの操作<br>・Webカメラのチェック |

| 事業体(研究所)名　株式会社福山コンサルタント | |
|---|---|
| 所在地（郵便番号及び住所）　〒812-0013　福岡市博多区博多駅東三丁目6番18号 | |
| 関連部署及び電話番号　システム課 ／ 092-471-0211 | |
| URL　http://www.fukuyamaconsul.co.jp/ | |
| 対象技術 | 技術の概要・特徴など |
| データ | １．製品概要<br>感熱式指紋センサー<br>現在の多くの機器に採用されている静電式センサーに比べて、強度・耐久性が高く、光学式センサーにくらべて軽量・コンパクトな感熱式センサを採用。さらに、残留指紋が残らないスイープ式（センサーに指を滑らせます）。残留指紋からの指紋採取は不可能であり、利用者の心理的不安もありません。<br>指紋はUSBメモリ内の秘匿領域へ保存<br>登録された指紋情報はPC内へは一切保存せず、製品本体に保存されます。<br>この保存領域はPCからは一切アクセス不能な秘匿領域です。また、指紋情報は特徴点をデータ化して保存しているため、指紋情報の不正利用はできません。<br>指紋照合は1秒以内、360度スイープ対応<br>入力された指紋は、1秒以内に照合されます。高精度認証テクノロジーにより、センサーに対して斜めや180度反対からスキャンを行っても、認証判断が可能です。<br>ドライバーのインストールレス<br>ユーザー権限のPCで使用する際に、専用USBドライバーのインストールが不要です。 |

**ハードウェア暗号化**

リムーバブルディスクに書き込まれるデータは、コントローラチップにより自動暗号化されます。

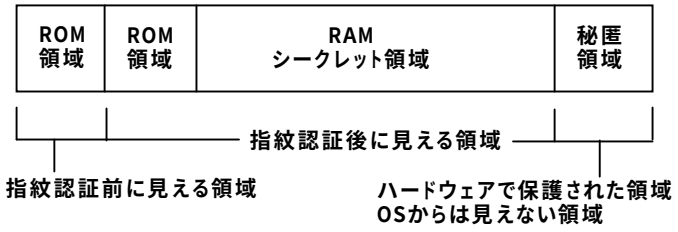
**Windowsオートラン機能搭載（サスライト社特許）**

BioDataSec2.0はCD-ROM領域とファイルの読み書きができるリムーバブルディスクで構成されています。CD-ROM領域にアプリケーションを格納することにより、指紋認証後にアプリケーションを自動起動することができます。

**シンクライアントの起動デバイス対応**

CD-ROM領域にLinuxOSを搭載することができます。高価なシンクライアントPCがなくても、既存のPCにBioDataSec2.0を接続することにより、シンクライアント環境を実現することができます。

**概念図**




**２．ハードウェア仕様**

| | |
|---|---|
| 対応OS | Windows XP/2000/VISTA |
| インターフェース | USB2.0 |
| 外形寸法(mm)<br>（L x H x W） | 102.5 x 11.5 x 24.0（使用時）<br>83.5 x 11.5 x 24.0（持ち運び時） |
| 重量 | 約19g |
| 消費電力 | 140mA（最大） |
| 指紋センサ | 感熱式スイープセンサ |
| 動作温度 | 0～60℃ |
| 動作湿度 | 20%～90% |
| 登録指数 | 10指 |
| FAR（他人誤認率） | 0.001%未満 |
| FRR（本人拒否率） | 0.1%未満 |
| メモリサイズ | 512MB,2GB |