

平成13年2月9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

不正アクセス禁止法の施行日から平成12年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

警察庁、総務省又は経済産業省のいずれかの予算で実施しているアクセス制御機能の研究開発の状況及び昨年末に募集した民間企業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/>

経済産業省ホームページ <http://www.meti.go.jp/policy/netsecurity/>

## 不正アクセス行為の発生状況

### 第1 平成12年中の不正アクセス禁止法違反事件の検挙状況等について

不正アクセス禁止法の施行日（平成12年2月13日）から平成12年12月31日までの間に警察庁に報告のあった不正アクセス行為（以下「期間中の不正アクセス行為」という。）が対象である。

### 4 不正アクセス行為の発生状況及びその特徴

期間中の不正アクセス行為は、106件であった。そのうち、海外から不正アクセス行為が行われたことが判明しているものは、25件あった。

	認知件数	
被害に係る特定電子計算機のアクセス管理者別	プロバイダ	59
	大学	8
	情報通信企業	6
	その他	33
	計	106

	認知件数	
認知の端緒別	アクセス管理者からの届出	30
	利用者からの届出	23
	発見者からの通報	7
	被疑者の取調べ	35
	その他	11
計	106	

これらを被害に係る特定電子計算機のアクセス管理者別に見ると、プロバイダが59件と最も多く、次いで大学が8件の順となっている。

また、認知の端緒の主なものとしては、警察への届出等が60件（アクセス管理者からの届出が30件、利用者からの届出が23件、その他発見者からの通報が7件）、被疑者の取調べ等の警察活動が35件あった。

なお、不正アクセス行為後の行為としてホームページの改ざん、消去を伴うものが33件、DDoS用攻撃ツール（Trinity V3）（参考1を参照）を仕掛けられていたものが2件あった。

### 5 不正アクセス禁止法違反事件の検挙状況

期間中の不正アクセス禁止法違反の検挙件数は31事件（67件）、検挙人員は37人であった。その内訳は、不正アクセス行為が30事件（62件）、34人であり、不正アクセス助長行為が4事件（5件。3事件は不正アクセス行為でも検挙。）、5人（2人は不正アクセス行為でも検挙。）であった。

不正アクセス行為の態様については、30事件中29事件（61件）が識別符号窃用型（不正アクセス禁止法第3条第2項第1号の他人の識別符号を無断で入力する行為をいう。）であり、残りの1事件（1件）がセキュリティ・ホール攻撃型（不正アクセス禁止法第3条第2項第2号及び第3号のアクセス制御機能による特定利用の制限を免れる情報又は指令を入力する行為をいう。）であった。また、不正アクセス助長行為で検挙した事件は、いずれも識別符号がどの特定電子計算機の特定利用に係るものであるかを明らかにして提供していたものであった。

なお、検挙人員37人中31人が成人であり、6人が少年であった。

事 犯 別	検挙事件数	検挙件数	検挙人員
不正アクセス行為	30	62	34人
不正アクセス助長行為	4	5	5人
計	34 (重複3)	67	39人 (重複2人)

## 6 検挙事例

### 違法薬物販売目的の他人の識別符号を使用した不正アクセス禁止法違反等事件

無職の男(34)が、クラッキング・ツール等を利用して入手した他人のID・パスワードを使用して不正にインターネットに接続し、ホームページを開設した上、薬物販売の広告を掲示し、薬物の購入希望者とメールのやり取り等をするとともに、同ホームページで販売する目的で医薬品や向精神薬を自宅に所持していた。12年3月、不正アクセス禁止法違反、薬事法違反及び麻薬及び向精神薬取締法違反で検挙した(千葉)。

### 音楽配信会社のメールサーバに対する不正アクセス禁止法違反事件

音楽配信会社の元役員(32)が、役員当時知り得た社長等のID・パスワードを使用して同社のメールサーバに侵入し、電子メールの内容を盗み見た。12年6月、不正アクセス禁止法違反で検挙した(警視庁)。

### 2ショットチャット掲示板に対する不正アクセス禁止法違反事件

建設会社の会社員(32)が、被害者が開設した有料掲示板「2ショットチャット」に対し、認証機能が甘いことに乗じ、CGIプログラムを使用してセキュリティ・ホールを突き、識別符号を入力することなく接続した。12年6月、不正アクセス禁止法違反で検挙した(北海道、富山)。

### オンラインゲームに係る不正アクセス禁止法違反事件

派遣会社の社員(23)が、クラッキング・ツールを利用して入手した他人のID・パスワードを使用して不正に米国のオンラインゲーム・サーバに侵入し、ゲームを行った。その際、同ゲームのチャット上で知り合った少年に対し同ID・パスワードを教示した。12年4月、不正アクセス禁止法違反で検挙した(警視庁)。

### レンタル・サーバ業者のウェブ・サーバに対する不正アクセス禁止法違反等事件

無職の男(33)が、総当たりにより探知した元勤務先の広告会社のID・パスワードを使用して同社の契約会社のウェブ・サーバに侵入し、ホームページのデータを削除した。12年8月、不正アクセス禁止法違反及び電子計算機損壊等業務妨害罪で検挙した(大阪)。

### **i モード電話機用のウェブ・サーバに対する不正アクセス禁止法違反事件**

無職の男(23)が、iモード電話機用の掲示板から入手した他人のID・パスワードを同電話機のメール・サービスを利用してハッカー仲間である会社員(25)に提供、さらに、同会社員が、同ID等をハッカー仲間である大学生(25)に提供し、同大学生が、同ID等を使用して不正にiモード電話機用のウェブ・サーバに侵入し、掲示板の内容を書き換えるなどした。12年10月、不正アクセス禁止法違反で無職の男ら3人を検挙した(警視庁)。

### **ホームページ提供サービス業者のウェブ・サーバに対する不正アクセス禁止法違反等事件**

韓国関連の情報交換のためのホームページを開設する会社員(31)が、自己のホームページの掲示板に嫌がらせの書き込みをされたことに立腹し、同書き込みをした者が開設する韓国関連のホームページに係るID・パスワードを推測により探知し、不正にホームページ提供サービス業者のウェブ・サーバに侵入し、本人に無断で退会届をすることにより同ホームページのデータを消去した。12年10月、不正アクセス禁止法違反及び電子計算機損壊等業務妨害罪で検挙した(警視庁)。

### **解雇された会社の識別符号を窃取した不正アクセス禁止法違反等事件**

情報通信関連会社の元社員(25)が、同社を解雇されたことに立腹し、同社に金銭的損害を与える目的で、在職中に知り得た同社のID・パスワードを使用して不正にインターネットに接続するとともに、同社に高額のインターネット接続料が請求されるように契約内容を変更する旨の虚偽の情報をプロバイダのサーバに送信して事実証明に関する電磁的記録を不正に作出したほか、ホームページ上で前記ID等を公開した。12年10月、不正アクセス禁止法違反及び電磁的記録不正作出罪で検挙した(警視庁)。

### **広域にわたるハッカー・グループによる不正アクセス禁止法違反事件**

ハッカー・グループの主犯格の男(30)が、クラッキング・ツール等を利用して入手した他人のID・パスワードを使用して不正に国立大学、観光協会及びプロバイダの各サーバに侵入するとともに、自己の運営する掲示板において、前記国立大学のサーバに係る同ID等の掲示、観光協会及びプロバイダに対する不正アクセス手法の教示等を行った。また、同教示を受けた同グループのメンバーである主婦(42)、大学生(23)が、それぞれクラッキング・ツールの利用等教示を受けた手法により入手した他人のID・パスワードを使用して不正に国立大学又は観光協会のサーバに侵入した。12年11月、不正アクセス禁止法違反で主犯格のほかハッカー・グループのメンバー2人を検挙した(愛知、秋田、宮城、警視庁、広島)。

## 7 検挙事件の特徴

### (1) 犯行の手口

不正アクセス行為で検挙した30事件(62件)の手口としては、ユーザのパスワード管理の甘さにつけ込んだID・パスワードの入手が12事件(14件)と最も多く、次いでトロイの木馬(参考2を参照)系のコンピュータ・ウイルス等のクラッキング・ツールによるID・パスワードの入手やセキュリティ・ホール攻撃が8事件(14件)、他人からのID・パスワードの入手が6事件(25件)の順となっている。

なお、クラッキング・ツールの中では、トロイの木馬系のコンピュータ・ウイルスを利用したものが多く、識別符号の入手等にクラッキング・ツールを使用した事件中3事件(5件)で使用されていた。いずれの被疑者も、クラッキング・ツールをネットワーク上のホームページからダウンロードし、又は雑誌の付録CD等から入手していた。

このほか、犯行の発覚を免れるため、海外のプロキシ・サーバを使用していた事件(2事件(2件))もあった。

### (2) 被疑者の特徴

検挙した37人の被疑者の年齢は、30代が16人と最も多く、次いで20代が13人、10代が6人の順となっている。最年長の者は48歳であり、最年少の者は15歳であった。

なお、検挙人員には含まれないものの、刑事責任の無い少年が不正アクセス行為を行っていたもの(補導処分)もある。

### (3) 犯行の動機

不正アクセス行為の動機としては、利用料金の請求を免れるため13事件(34件)と最も多く、次いで嫌がらせ・仕返しが5事件(7件)、メールの盗み見5事件(5件)、なりすまして別の犯罪等の発覚を免れるため3事件(7件)、いたずら目的が2事件(3件)の順となっている。少年被疑者にあつては、特段の罪悪感を持たずに犯行に至っているのが目立つ。

### (4) その他

不正アクセス行為が別の犯罪の手段として利用されていた事案は、8事件(12件)であった(薬事法及び麻薬及び向精神薬取締法違反事件、業務妨害事件、詐欺事件、名誉毀損事件、電子計算機損壊等業務妨害事件、著作権法違反事件、電磁的記録不正作出事件)。

## 5 都道府県公安委員会による援助措置

都道府県公安委員会は、不正アクセス行為を受けたアクセス管理者からの申出への対応として、不正アクセス禁止法第6条の援助規定(平成12年7月1日施行)に基づくアクセス管理者に対する助言・指導を、平成12年12月31日までに6件(東京、滋賀、大阪、北海道、京都、神奈川)実施している。

## 6 防御上の留意事項

### (1) トロイの木馬対策

トロイの木馬系のコンピュータ・ウイルスの感染を予防するため、不審な電子メールを受信した場合にはメールの添付ファイルを不用意に開かないことなどに留意する。

### (2) 識別符号の適切な管理

推測されやすいパスワードの解消、パスワードの定期的な変更、使用されなく

なったID・パスワードの抹消等識別符号の適切な管理を行う。

(3) サーバの適切な管理

セキュリティ・ホールの解消、適切に設定されたファイアウォールの設置、ログの保存・監査等サーバの適切な管理を行う。

(4) その他

- ・「情報システム安全対策指針」(平成11年国家公安委員会告示第19号)を参考に一般的な対策も併せて講ずることが望ましい。
- ・都道府県警察においては、不正アクセス禁止法に基づく援助を行っているほか、ハイテク犯罪相談を行っているので、被害が発生した場合には、都道府県警察のハイテク犯罪相談窓口連絡する(相談窓口一覧:警察庁ホームページ<http://www.npa.go.jp/>)。

(参考)

1 DDoS(Distributed Denial of Service)攻撃ツール(Trinity V3)について

DDoS攻撃とは、インターネット上の複数のコンピュータにDoS攻撃(標的となるサーバコンピュータに過剰な負荷をかけるなどして当該サーバコンピュータのサービスを妨害する攻撃)用のツールを仕掛け、攻撃者の使用するコンピュータからの命令により一斉にDoS攻撃を行い、標的となるサーバコンピュータのサービスを妨害するものである。DDoS攻撃ツールが仕掛けられていた場合は、システムの再インストールにより攻撃用ツールを削除するとともに、OS及びアプリケーションのバージョンアップ並びに定期的点検等により再発に注意しなければならない。

なお、Trinity V3は、昨年9月に発見されたDDoS攻撃ツールの一種で、検出のためには次の2つの項目の確認が必要とされている。

ポート33270の開閉状態を確認する。

通常は使用されていないポート番号のため閉じられているが、DDoS攻撃ツール(Trinity V3)が仕掛けられると解放状態となる。

ファイルを点検する。

DDoS攻撃ツール(Trinity V3)を仕掛けられたコンピュータには、`/usr/lib/`のディレクトリー下にidle.soというファイル及び`/var/spool/uucp/`のディレクトリー下にuuicoというファイルが存在する。

2 トロイの木馬について

トロイの木馬とは

「トロイの木馬」は、コンピュータに悪影響を及ぼしたり、ユーザを欺くプログラムを内包していながら、普通のアプリケーションプログラム等の体裁を有しているプログラムであり、通常、コンピュータ・ウイルスの一種として扱われている。パソコンにトロイの木馬が仕掛けられると、ユーザは業務処理やゲームなどを行っているつもりでも、背後では別の機能が作動していて、パスワードを盗むなどの被害を与えている。トロイの木馬の語源は、古代ギリシャのトロイ戦争で、都市国家トロイが、中に敵軍兵士が潜んでいるとも知らずに、門前におかれた大きな木馬を内部に引き入れ、敗れたという故事にちなんでいる。

トロイの木馬は、実際に発生している不正アクセス禁止法違反事件でも使用されており、不正アクセス行為の発生の一因にもなっている。

トロイの木馬の特徴

トロイの木馬には多くの種類があるが、これらのほとんどはインターネットから容易に入手することができる。これまで検挙された不正アクセス禁止法違反事件で

は、SubSeven、BackOrifice及びDeepThroatという名称のトロイの木馬が用いられた。これらは、不正アクセス行為の対象となるコンピュータに仕掛けるプログラム（サーバプログラム）とサーバプログラムが仕掛けられているコンピュータを遠隔操作するため他のコンピュータ（行為者のパソコン等）において作動するプログラム（クライアントプログラム）により構成される。

不正アクセス禁止法違反事件において識別符号を窃取されたコンピュータのいくつかには、実際にこれらのサーバプログラムが仕掛けられていた。これらは、インターネットを経由した遠隔操作により、Windowsにおいて用いられるインターネット接続用のID・パスワードの窃取、情報の改ざん等を行う機能を有している。

#### 被害の予防方法

トロイの木馬は、サーバプログラムとクライアントプログラムが連携して機能するものであるから、被害を予防するには、サーバプログラムが仕掛けられることを防ぐのが第一である。そのためには、コンピュータ・ウイルスの感染予防と同様に、メール等により外部から送られてきた添付ファイルやいかがわしいサイトからダウンロードしたプログラムを不用意に実行しないなどの注意が必要である。このようなプログラムを添付されたメールは、件名を偽りソフトウェアベンダからのバージョンアップ等の案内になりすましたもの、添付ファイルの種類を変更し画像ファイルやビデオファイルになりすましたもの等さまざまな偽装を施していることがほとんどであることに注意しなければならない。

ほとんどのサーバプログラムは、コンピュータ・ウイルスのワクチンソフトにより検出・駆除が可能であることから、それらを導入・常駐させることも有効な予防方法である。また、シェアウェアのトロイの木馬専用の検出・駆除ソフトウェアがインターネット上で提供されている。（ソフト名The Cleaner、<http://www.moosoft.com/>）

#### （注1）

##### 不正アクセス行為の認知の考え方

認知とは、被害届を受理した場合のほか、余罪として発覚した場合、報道を踏まえて確認した場合、援助の申出を受理した場合等不正アクセス行為の事実確認ができた場合とすることとしている。

#### （注2）

##### 不正アクセス行為の件数の計上について

- ・ 一のアクセス制御機能に対する一の手口による侵害行為を1件とする。ただし、被疑者が異なる場合（共犯を除く。）はそれぞれ1件として計上し、短期間に一のアクセス制御機能に対して同一手口による侵害が継続的に行われた場合は包括して1件とする。
- ・ 不正アクセス行為と他の罪とが併合罪又は観念的競合の関係にある場合、これを別件として扱い、1件計上する。

## 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 情報処理振興事業協会（IPA）に届出のあったコンピュータ不正アクセスの状況について

平成12年2月13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被害届出件数は128件であった(注2)。

以下に、種々の切り口で分類した結果を示す。各々の件数には未遂(実際の被害はなかったもの)も含まれる。また、1件の届出にて複数の分類に該当するものがあるため、それぞれの項目での総計件数はこの数字に必ずしも一致しない。

#### (1) 手口別分類

意図的に行う攻撃行為による分類である。重複があるため、届出件数とは異なり総計は132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58件あった。

###### a 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。21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。いずれの場合も、実際の侵入は受けていない。

ポートスキャンもしくはポートへのアクセス：21件

###### b 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。37件の届出があり、これらのうち実際に侵入を受けたものは36件である。

セキュリティホールを利用した攻撃：11件

手口・経路の不明な侵入行為：26件

手口の不明な侵入行為のうちパスワード推測の疑いのあるもの：5件

###### c 不正行為の実行及び目的達成後の行為

bのうち実際に侵入を受けた36件について、その後行われた種々の行為である。1件の侵入で種々の行為が行われているため重複がある。

ファイル等の改ざん、破壊等：22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：10件

不正アカウントの作成(追加)：9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：6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たサービスを不可もしくは低下させる攻撃である。6件の届出があった。

攻撃：6件

そのうちsmurf攻撃であると思われるもの：3件

##### (ウ) その他

その他には、ソーシャルエンジニアリングや、サービスの外部からの利用が含まれ、68件の届出があった。2000年の被害で特徴的な攻撃(嫌がらせであると思われる)のは、メールアドレス詐称である。春頃から蔓延している模様で、26件の届出があった。メール中継に利用されたケースの中にも、当該メールがアドレス詐称のものであると思われるものが多くなっている。

その他：68件

メール中継に関するもの：36件

そのうちメール中継に実際に利用されたもの：35件

オープンプロキシの利用：1件

メールアドレス(ドメイン)の詐称：26件

その他：5件

## (2) 原因別分類

不正アクセスを許した問題点/弱点による分類である。

実際に侵入を受けた36件、メール中継に係わる問題(弱点)のあった35件、オープンプロキシ利用の1件などの計75件を分類すると以下のようになる。

ID、パスワード管理の不備によると思われるもの：5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：22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：23件

不明：25件

## (3) 電算機分類

攻撃や被害の対象となった機器による分類である。

ファイアウォール：4件

メールサーバ：60件

Webサーバ：15件

各種サーバ：32件

クライアント(個人ユーザ環境)：4件

その他、不明：14件

各種サーバ：DNS、Web、mailなどのサーバ。1台で複数機能を有するものを含む。

## (4) 被害内容分類

被害内容による分類である。

機器に対する実被害があった届出件数は81件である。対処に係わる工数やサービスの一時停止、代替機の準備などに関する被害は除外している。

メール中継に利用された：38件

これらのうち

侵入行為によりシステムを改ざん等されて利用されたもの：3件

メール中継・アドレス詐称メール送付に伴う二次的被害

サーバダウン：6件

サービス低下：11件

侵入された：36件

侵入に伴う被害(1件の侵入で複数被害のあるものを含む)

ファイル改ざん等トータル：22件

うち、Web改ざん：12件

その他ファイルの改ざん：17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：10件

不正アカウントの作成(追加)：11件

踏み台：9件

メール中継・送信に利用された：4件

サービス妨害攻撃その他によるサーバダウン、サービス低下：9件

その他、機器への実際の被害はなかったもの：49件

#### (5) 対策情報

(2)の被害原因分類にもあるように、基本的な(既知の)対策をとっていなかったために被害にあってしまったものが多くなっている。下記ページなどを参照し、今一度状況確認・対処されたい。

「**セキュリティ対策セルフチェックシート**」

<http://www.ipa.go.jp/security/ciadr/checksheet.html>

「**コンピュータ不正アクセス被害防止対策集**」

<http://www.ipa.go.jp/security/ciadr/cm01.html>

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

「**IPAセキュリティセンタートップページ**」

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

(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が受理した件数であり、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 コンピュータ緊急対応センター(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12年2月13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)に係わる報告件数は2,084件であった。(注2)

#### ブローブ、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1,701件の報告があった。

[2/13-3/31: 133件、4/1-6/30: 610件、7/1-9/30: 557件、10/1-12/31: 401件]

#### 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108件の報告があった。

[2/13-3/31: 9件、4/1-6/30: 30件、7/1-9/30: 30件、10/1-12/31: 39件]

### システムへの侵入

管理者権限の盗用が認められる場合を含め、システムへの侵入について 106 件の報告があった。

[2/13-3/31: 23件、4/1-6/30: 32件、7/1-9/30: 24件、10/1-12/31: 27件]

### 電子メール配送プログラムへのアクセス

電子メール配送プログラムへの、電子メールの中継を目的としたアクセスについて 102件の報告があった。

[2/13-3/31: 24件、4/1-6/30: 27件、7/1-9/30: 27件、10/1-12/31: 24件]

### 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 packets 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 29件の報告があった。

[2/13-3/31: 1件、4/1-6/30: 8件、7/1-9/30: 14件、10/1-12/31: 6件]

### その他

インターネットを介して伝播するワーム、トロイの木馬、コンピュータウイルス、IP アドレスを詐称したパケットの偽造、Web ページの改竄等について 43件の報告があった。

[2/13-3/31: 4件、4/1-6/30: 4件、7/1-9/30: 14件、10/1-12/31: 21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）。

### 緊急報告

[ 新規 ]

IMAP から POP2 への変換サーバプログラムについて (Version 2)

[ 更新 ]

automountd サーバプログラムを悪用したアタック (Version 3)

POP サーバプログラムを悪用したアタック (Version 4)

NFS マウントデーモン mountd を悪用したアタック (Version 2)

ポートスキャンを用いた不正アクセス (Version 2)

named サーバプログラムを悪用したアタック (Version 2)

statd サーバプログラムを悪用したアタック (Version 2)

ネットワークニュースのサービスを悪用したアタック (Version 4)

phf CGI プログラムを悪用したアタック (Version 2)

年末年始休暇中に多発したアタックについて (Version 4)

### 技術メモ

[ 新規 ]

Web ページの改竄に対する防衛 (Version 3)  
サービス運用妨害攻撃に対する防衛 (Version 2)

[ 更新 ]

コンピュータセキュリティインシデントへの対応 (Version 2)  
関係サイトとの情報交換 (Version 2)  
sendmail バージョンアップマニュアル (Version 10)  
電子メール配送プログラムの不正利用 (予期しない中継) (Version 4)

#### 活動概要 (届出状況等の公表)

発行日: 2001-01-30 [ 2000年10月1日 ~ 2000年12月31日 ]

発行日: 2000-10-27 [ 2000年7月1日 ~ 2000年9月30日 ]

発行日: 2000-07-31 [ 2000年4月1日 ~ 2000年6月30日 ]

発行日: 2000-04-28 [ 2000年1月1日 ~ 2000年3月31日 ]

(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) 平成12年通期の報告件数については、JPCERT/CC の web ページを参照されたい。

(注 3) 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

不正アクセス行為の禁止等に関する法律 (平成 11 法律第 128 号) 第 7 条の規定に基づき、アクセス制御機能に関する技術の研究開発の状況を次のとおり公表する。

##### 1. 国の予算で実施しているもの

警察庁、総務省又は経済産業省のいずれかの予算で実施している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る。具体的には、国立研究所で実施している研究、国からの委託研究、国からの補助事業により実施している研究等である。

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。

インターネットアプリケーションのセキュリティ脆弱性に関する研究  
情報通信危機管理基盤技術の研究開発  
制御系システムにおけるセキュリティ機能共通基盤の研究開発  
大規模プラントのネットワーク・セキュリティ技術開発 / 実証実験  
大規模プラントネットワークにおける遠隔操作、遠隔保守のためのセキュア通信プ

## ロトコル

ネットワーク侵入検出システム IDA(Intrusion Detection System)の研究開発  
ネットワークセキュリティ・リスク分析システム機能の拡張に関する研究  
不正アクセスの高感度検出及びグローバル警戒機構に関する研究  
不正アクセス発信源追跡技術に関する研究開発

## 2. 民間企業で研究を実施したもの

平成12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を募集した。その間の応募者は以下のとおりであり、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申告のあった内容をそのまま掲載している。

R S A セキュリティ (株)  
(株) アクセスチケットシステムズ  
エヌ・シー・エル・コミュニケーション (株)  
エヌ・ティ・ティアイティ (株)  
エヌ・ティ・ティコミュニケーションズ (株)  
エヌ・ティ・ティソフトウェア (株)  
沖電気工業 (株)  
(株) データコントロール  
(株) 東芝  
日本電気 (株)  
ノベル (株)  
富士ソフト A B C (株)  
(株) 山田洋行

### 研究開発テーマ名：

インターネットアプリケーションのセキュリティ脆弱性に関する研究

### 実施主体：

経済産業省 電子技術総合研究所

### 背景：

どんなに高度なセキュリティ機構を研究・開発したとしても、その安全性は実装段階でのミスが無ければの話である。実際、広く普及しているインターネットアプリケーションの多くに致命的な安全上の欠陥が続々と見つかっているのが現状である。この研究は、そうした欠陥がなぜ生じたのかを詳しく分析し、その情報を公開することによって、技術者が同じ過ちを繰り返さないよう啓発することを目的とする。

### 研究開発の概要：

現実に使用されているインターネットアプリケーション(ウェブブラウザ、電子メールソフトウェア、Java、Servlet、JavaScript、ウェブアプリケーション等)について、安全上の欠陥を洗い出し、開発・運用責任者に対して報告して修正を促すとともに、その欠陥が生じた技術的原因を詳しく分析して、実例を用いたわかりやすい解説文書を一般公開する。この解説文書を多数蓄積することによって、安全上避けなければならない誤った実装方法の技術データベースを構築することを目標とする。

詳細の入手方法：

<http://SecurIT.etl.go.jp/>

将来の方向性：

技術的に新規性の無い(すなわち既知の)欠陥を引き続き保有しているウェブアプリケーションは多数現存していると考えられる。これらを逐一探し出して修正するよう足す作業を、作業手順をマニュアル化するなどして、外部に委託することが考えられる。

また、機械的に欠陥を探し出す診断ソフトウェアの研究 開発へと発展させられる可能性がある。

対象技術 侵入検知技術

テーマ名 情報通信危機管理基盤技術の研究開発

開発年度 平成12年度～

実施主体 総務省通信総合研究所

背景、目的

我が国の電子政府構想の根幹を揺るがし、我が国経済の将来を背負う電子商取引などを危機的状況に陥れる不正アクセスやサイバーテロに対して、不正アクセスやサイバーテロなどに対処するため、ネットワーク上に生じた異変を的確に検出・分析し、対策を提示する先端的要素技術を研究開発する。

研究開発状況(概要)

今後極めて大きな市場が見込める電子商取引等のIT市場の発展を阻害する恐れのある不正アクセスやサイバーテロを未然に防止するため、郵政省通信総合研究所に、不正アクセス行為分析設備等を備えたネットワークセキュリティ研究施設、危機管理用安全対策施設、不正アクセス行為やサイバーテロを検証・再現し、対策を検証するための実験用施設(テストフィールド)等を整備し、不正アクセスに関する各種事例を記録し検証する方法の開発、サービス不能攻撃への対処方法、ルートサーバ攻撃対策、インターネット機器への新しい攻撃に対抗する技術等の研究開発について、平成13年度以降の実施に向け、現状分析等を実施している。

詳細の入手方法(関連部署名及びその連絡先)

総務省通信総合研究所 非常時通信研究室 大野浩之  
042-327-5542

将来の方向性

今回の施設整備をもとに、ナショナルセキュリティや国民経済・生活に対する大きな脅威となってきた「サイバーテロ」や大規模不正アクセスに対抗する国家レベルのネットワーク危機管理技術の研究、標準化等を行い、現実のサイバーテロや情報戦争に対応できる技術の獲得を目指す。



研究開発テーマ名：「制御系システムにおけるセキュリティ機能共通基盤の研究開発」

実施主体：新日本製鐵株式会社（情報処理振興事業協会（IPA）から委託）

#### 背景

現状、閉鎖的である大規模プラントの制御系システムネットワークが、将来オープン化された際、セキュリティ対策として実用性の高いセキュリティ機能共通基盤を開発・公開することを目的とし、その成果を利用したハードウェア、ソフトウェア製品の開発を促進し、産業の情報化の発展に寄与することを目指すものである。

#### 研究開発の概要

制御系システムのオープン化動向から想定されるモデルシステムを基に、セキュリティに関する全体要件を定義する要件定義作業と、全体要件を体系立てて個別要件として切り分け、それぞれが求めるセキュリティ機能をアプリケーションの機能ブロックとして中項目レベル相当で設計を行う外部設計作業で構成される。

要件定義作業は、モデルシステム、セキュリティポリシー、セキュリティ機能要件を検討し、要件定義書としてまとめる作業である。

外部設計作業は、要件定義の結果を踏まえ、それぞれの機能の必要性、関連を再度見極めた上でアプリケーション設計を行い、外部設計書としてまとめる作業である。

#### 詳細の入手方法

現在作業中であり、報告書としてまとめられていないため、後日、情報処理振興事業協会（IPA）のWebにて公開予定。

#### 将来の方向性

当研究開発は、外部設計書の作成までであるため、今後もこの成果物を元に内部設計、プログラム開発、検証実験を進め、成果の一般公開と開発した機能の製品化に取り組んでいく必要がある。

研究開発テーマ名：「大規模プラントのネットワーク・セキュリティ技術開発／実証実験」

実施主体：日本アイ・ピー・エム株式会社（情報処理振興事業協会（IPA）から委託）

#### 背景

基幹産業のネットワーク・システムに対するセキュリティ対策の必要性から、「大規模プラント・ネットワーク・セキュリティ対策委員会」が平成10年3月に、「大規模プラント・ネットワーク・セキュリティについての中間報告」（以下、中間報告書）をまとめた。この内容を受けて、大規模プラント・ネットワークに対する対策の妥当性を検証するための実験を行い、実験結果に基づいて「侵入経路別のセキュリティ対策」、「防止技術の研究開発」などの技術開発をすることにより、その有効性を示すものである。

#### 研究開発の概要

本研究開発は、実証実験1と実証実験2の2つの実験で構成される。

実証実験1では、大規模プラント・ネットワークの安全性を多面的な角度から具体的に明らかにする方法論を確立し、それを大規模プラントに用いられているネットワークに実際に適用し、その安全性を検証するとともに妥当性を確認した。

実証実験2では、中間報告書で示された対策等をもとに選定した技術開発テーマに対応するセキュリティ対策技術を開発し、実証実験1と同様の方法論で実証実験を実施し、開発した技術の有効性や効果を検証した。

#### 詳細の入手方法

情報処理振興事業協会（IPA）のWebにて報告書を公開。

<http://www.ipa.go.jp/security/fy11/report/contents/intrusion/plant-security/index.html>

#### 将来の方向性

これらの成果は、今後の大規模プラントのネットワークがサイバーテロなどの脅威に対抗してその安全性を確保する基盤を整備する上で大いに役立ち、また、社会基盤を構成する他のネットワークにこの新たに作成した方法論を適用することにより、より広く社会インフラのネットワークの安全性を高めることに貢献できることは極めて社会的意義の大きいことである。

研究開発テーマ名：「大規模プラントネットワークにおける遠隔操作、遠隔保守のためのセキュア通信プロトコル技術の研究開発」

実施主体：株式会社日立製作所（情報処理振興事業協会（IPA）から委託）

#### 背景

本研究は、遠隔操作・遠隔保守における業界標準（または推奨）のセキュアな通信プロトコルの確立を目指し、ベンダの実装方法の違いによるセキュリティ上の脆弱性のばらつきをなくし、一定のレベル以下に均一化することを目的とするものである。

#### 研究開発の概要

本研究の目的は、情報系ネットワーク上に存在する端末装置から制御系のシステムに対して遠隔操作及び遠隔保守をセキュアに行うための通信プロトコル、及びその周辺のプロトコル、データ構造などを策定することであり、その成果物は通信プロトコルの仕様書である。この仕様書を策定するために実施する作業は以下の通りである。

- ( 1 ) 技術調査：W e b 環境における遠隔監視、遠隔操作、遠隔保守などに関する調査を行う。
- ( 2 ) 操作に対する仕様調査：従来の監視制御システムで行われてきた操作に対する仕様を調査する。
- ( 3 ) 通信プロトコル仕様の策定
- ( 4 ) 検証実験用ソフトウェアの開発：策定したプロトコルの動作確認、想定した脅威についての検証を行うためのソフトウェアを開発する。
- ( 5 ) 検証実験：開発したソフトウェアを用いて、通信プロトコル仕様の妥当性を検討・評価する。

#### 詳細の入手方法

現在作業中であり、報告書としてまとめられていないため、後日、情報処理振興事業協会（ I P A ）の W e b にて公開予定。

#### 将来の方向性

本通信プロトコルの重要性を広めるため、学会発表を行い、また、ユーザ企業等にプレゼンテーションを行い有効性を認知してもらうことが考えられる。

研究開発テーマ名：

「ネットワーク侵入検出システムIDA (Intrusion Detection Agent system) の研究開発」

実施主体：情報処理振興事業協会 (IPA) 技術センター (研究員を招聘して実施)

#### 背景

侵入検出システム (IDS) は、認証・アクセス制御とならぶセキュリティ技術であり、昨今はパケット情報から侵入を検知するネットワークベース型を中心に、普及しつつある。ネットワークベース型では、DoS攻撃、ポートスキャン等の検出を中心に行う。一方のホストベースのIDSは、ホスト上のシステムログから侵入を検出するため、システム内の詳細な情報から侵入が検出できる。また、ネットワーク内部からの侵入者の検出に強いといわれている。本プロジェクトでは、ホストベースIDSの開発を行っている。研究分野では最近の主流である、特権プロセスを中心とした、システムコールを解析することにより侵入を検知する。本プロジェクトでは特に、

- ・システムに対して低負荷で、かつ、未知の侵入検出が可能
  - ・管理、運用が容易
  - ・侵入追跡が可能
- を目的に研究開発を行っている。

#### 研究開発の概要

本プロジェクトでは、痕跡と定義した侵入事例の多くに付随する事象を検知し、それを解析することによって、侵入を検出する。痕跡は侵入検出のトリガーであり、それにより限られた事象のみ解析して侵入を判定するため、判定負荷が減少できる特徴がある。痕跡は通常行為からも発生するので、痕跡検出後に、それを発生させた原因が侵入行為かそうでないか判定しなければならない。本プロジェクトでは、その判定に既知の侵入に対する知識および多変量解析を用いている。

一方、本プロジェクトでは、侵入追跡機能も構築している。ネットワーク接続情報をもとに、LAN内ではモバイルエージェントによる侵入追跡を行っている。上記の侵入判定に必要な情報も、エージェントが併せて収集する。インターネット上の追跡については、サイト間の追跡に必要な情報を追跡時に容易に入手可能なシステムを現在構築中である。

#### 詳細の入手方法

ウェブページ：<http://www.ipa.go.jp/STC/IDA/jp/>

#### 論文

1. 浅香 緑、"モバイルエージェントによる侵入検出システムのための情報収集方式"、電子情報通信学会論文誌、Vol.J81-D-1 No.5, pp.532 -539,1998
2. M. Asaka et.al, "Local Atacck Detection and Intrusion Route Tracing," IEIC E Trans. on Commun. Vol.E-82-B No.11, pp.1826-1833, 1999
3. M. Asaka et.al, "A New Intrusion Detection Method Based on Discriminant Analysis,"

## 研究開発テーマ名：「ネットワークセキュリティ・リスク分析システム機能拡張 2」

実施主体：千代田化工建設株式会社（情報処理振興事業協会（IPA）からの委託）

### 背景

プラント・ネットワーク・セキュリティという問題に対し、平成10年度、平成11年度と、過去2年間のリスク分析システムの検討・開発において、リスク分析手法の検討、プロトタイピング、ネットワーク機能の拡張強化といったフェーズを経て、FT & ETを適用したリスク分析システムを構築してきた。

ネットワークセキュリティ・リスク分析システムの一般公開に向け、これまで開発されてきたリスク分析ツールに対し、機能拡張、操作ガイド表示機能の追加を中心とした作業を行い、セキュリティに関する知見とプログラミング技術によって、ネットワークセキュリティ等に関する知識を有する者が利用可能なシステムを提案することを主目的とする。更に、これまでは、十分な検討がなされていなかったネットワークセキュリティ・リスクの確率について、本システム上での確率における方向性を明確にするための検討および実装を行う。また、セキュリティホールを利用した侵入ルート探索のアルゴリズムについて検討を行う。

### 研究開発の概要

- (1) ネットワークセキュリティ・リスクの FT & ET 解析の拡張  
現在までのネットワークシミュレーション機能に対するネットワークセキュリティ・リスクの FT & ET 解析を可能とするよう機能を拡張する。
- (2) 侵入ルート探索範囲拡張の検討  
セキュリティホールも含めた侵入ルート探索を可能とするためのアルゴリズムについて検討を行う。
- (3) ネットワークセキュリティのリスク分析における発生確率の検討  
本システム上で表現可能なリスク発生確率について検討を行う。
- (4) リスク分析システム・ソフトウェアの整備  
リスク分析システムを一般公開可能なシステムとするべく、開発ソフトウェアの整備を行う。

### 詳細の入手方法

現在作業中であり、報告書等としてまとめられていないため、後日、情報処理振興事業協会（IPA）の Web もしくは開発者の Web にて公開予定である。

### 将来の方向性

今年度の研究及び開発により、基本的な機能の範囲に関しては一応整った状態になる。より一般的なネットワークのリスク分析に利用可能なツールとしての整備としては、アイテムの追加登録、その動作環境を広げるため C 言語もしくは Visual Basic などによるコンバートなどが考えられる。

研究開発テーマ名：「不正アクセスの高感度検出及びグローバル警戒機構に関する研究」

実施主体：株式会社NTTデータ（情報処理振興事業協会（IPA）からの委託）

#### 背景

インターネット上の情報セキュリティ確保には、不正アクセスの発見、防止が重要だが、不正の手口は日々高度化し個別対応では限界がある。また、ネットワーク上の膨大なアクセス情報を網羅的に調査することは非現実的である上、実際に検出される情報は不正アクセスの一部分に過ぎないことが多い。従って、わずかな異常から迅速に不正アクセスの実態全体を検知する高感度検出技術が必要である。

さらに、不正アクセスの多くは他のサイトを踏み台として利用するため、不正防止には、その検出のみならず、アクセス経路の特定も重要である。

本研究開発では、膨大なトラフィック中の微小な異常を検出する新手法、及びネットワーク地図情報と連携した広域捜査診断システムを開発し、その有効性を検証することを目的とする。

#### 研究開発の概要

- (1) インターネット技術動向に対応するセキュリティシステムの研究  
ネットワーク型IDS（Intrusion Detection System）に関する調査、ネットワーク管理システムに統合されたIDSに関する研究、IDS間通信についての研究を行う。
- (2) スタンドアローンIDSの開発  
ネットワーク上に分散して配備され、それ自体で独立に動作可能なIDSとして、ネットワークを監視し不正アクセスを検知し、記録を保存する。
- (3) 分散協調型侵入検出システムアプリケーションの開発  
スタンドアローンIDSドライバを提供し、さらに、攻撃者追跡機能及び広域スキャン検出機能のプロトタイプアプリケーションを提供する。
- (4) セキュリティシステム間通信機能の開発  
「分散協調型侵入検出システムアプリケーション」または「スタンドアローンIDS」からの通信の要求を受け、IDS情報、アラート情報等の通信を行う。
- (5) ネットワーク地図情報と連携した捜査診断機能の開発  
不正アクセス情報とネットワーク地図情報を結合する管理システム機能を提供する。

#### 詳細の入手方法

これまでに公開された報告書等は下記URLより入手可能。また、今年度分の報告書、開発ソフトに関しては、納入後、情報処理振興事業協会（IPA）のWebまたは開発者のWebにて公開予定。

<http://www.ipa.go.jp/security/fy11/report/contents/intrusion/highlysensitive-ids/index.html>

<http://www.cysol.co.jp/security/security.html>

#### 将来の方向性

本研究開発により開発された技術をスタンダードとし、ツールの普及、改良を図ることによりグローバルな警戒機構を構成することなどが考えられる。



対象技術：侵入検知技術

テーマ名：不正アクセス発信源追跡技術に関する研究開発

開発年度：平成11年度～13年度

実施主体：株式会社エヌ・ティ・ティ・データ、東日本電信電話株式会社  
(通信・放送機構(TAO)からの委託)

#### 背景、目的

- ・ インターネットを活用した電子商取引等の高度なアプリケーションの発展のためには、その基盤インフラであるインターネットが、不正アクセスの侵害的行為の脅威から守られ、安全性が確保されていることが重要であり、不正アクセスそのものを抑止するような研究開発が求められている。
- ・ そこで、個々のネットワークに監視ツールを導入する等、不正アクセスを監視する技術、及び、監視情報をもとに不正アクセス発信源の追跡を可能とするような技術に関する研究開発を行い、インターネットの安全・信頼性の向上に寄与することを目的とする。

#### 研究開発状況(概要)

- ・ 平成11年度より以下の研究開発を実施中。
  - (1) パケット発信源追跡に関する研究開発
  - (2) 次世代不正アクセス検知技術の研究開発
  - (3) 発信源追跡技術の不正利用防止技術の研究開発
- ・ 平成13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)

- ・ 総務省総合通信基盤局データ通信課 (03-5253-5854)

#### 将来の方向性

- ・ 不正アクセスを抑止し、セキュリティの高いインターネットを実現するため、当該技術の標準化を目指す。

企業名（及び略称）	RSAセキュリティ株式会社
代表者氏名	山野 修
所在地（郵便番号及び住所）	〒105-0001港区虎ノ門1-26-5虎ノ門17森ビル11F
関連部署名及び電話番号	マーケティング統括本部 03-3539-7668
U R L	www.rsasecurity.com/japan/
対象技術	技術開発状況
その他認証技術 （時刻によって 変化するパスワ ードを生成する アルゴリズムと その認証方法 1 985年）	一定間隔(通常一分)で変化する乱数を、その時点での時刻と秘匿されている番号から一定のアルゴリズムで生成し表示するカード型のデバイスを、認証を希望する利用者側に配備し、利用者は認証希望時にその時表示されている乱数をパスワードとして認証側に送付する。認証側、例えば一般のアプリケーションは送付されたパスワードを別途設置された認証装置に転送して認証の代行を依頼し、その回答により認証の可否を決定する。認証装置は、パスワード受信時の時刻と予め登録されている当該利用者の秘密番号から利用者デバイスと同じアルゴリズムで乱数を生成し、送付されたパスワードの妥当性（一致）を検証し結果を回答する。利用者デバイスと認証装置間の時計の差を補償するため、認証装置では、前回認証時までの累積時間差を記憶し乱数生成時に時刻を調整したり、許容できる範囲の複数の時刻について乱数を生成し、いずれかとの一致を確認して認証を許可するなどの処理を行う。

企業名（及び略称）	株式会社アクセスチケットシステムズ
代表者氏名	代表取締役社長 佐藤進一
所在地（郵便番号及び住所）	新宿区西新宿三丁目2の1 1 新宿三井ビル2号館1 1階
関連部署名及び電話番号	技術推進部 03-3342-6551
U R L	www.accessticket.com
対象技術	技術開発状況
その他認証技術 （技術の名称 アクセスチケッ ト技術） 開発年1997年	アクセスチケット技術は、公開鍵暗号を直接的な方法でアクセス制御に適用することを特徴とする技術である。証明書（公開鍵）を個人ユーザではなく、被アクセス対象（コンテンツやサービス）に発行し、この公開鍵による公開鍵暗号計算手続きによってアクセス権の認証・アクセス制御を行う。ユーザにはアクセスチケットと呼ばれるデータが発行され、ユーザが保持する識別用ブラックボックス関数（トークン）と組み合わせることで公開鍵暗号の個人鍵に相当する計算手続きが可能となる。アクセスチケット技術の主な利点は、ACL（Access Control List）への問い合わせが不要である、オフラインでのアクセス制御が可能である、アクセス権の検証手順は標準の公開鍵暗号アルゴリズムに基く（オープンアーキテクチャ）、認証プロトコルが規定されているため様々なプロトコルの上に実装可能である（ICカード、TCP/IP、http、Bluetoothなど）、実行効率に優れる、偽造・成りすましに対して耐性を有する、等である。 関連URL： <a href="http://www.accessticket.com/about.html">http://www.accessticket.com/about.html</a>

企業名（及び略称）	エヌ・シー・エル・コミュニケーション株式会社（NCLC）
代表者氏名	代表取締役社長 織田 博靖
所在地（郵便番号及び住所）	〒103-0001 東京都中央区日本橋小伝馬町4番9号小伝馬町第一生命ビル
関連部署名及び電話番号	ネットワークセキュリティ事業部 03-3667-2675
URL	<a href="http://www.nclc.co.jp">http://www.nclc.co.jp</a>
対象技術	技術開発状況
ファイアウォール技術	米国RapidStream, Incの開発による、専用RISCプロセッサによりStateful Packet Inspection Firewall、VPNトンネリング、トラフィックシェーピング、ロードバランスの同時高速処理を実現する技術。1998年より開発。 URL: <a href="http://www.rapidstream.com">http://www.rapidstream.com</a>
侵入検知技術	米国NFR Security Inc.の開発による、フラグメント化されたパケットを完全なTCPセッションの再構築によりの確に補足する技術、及び独自のスクリプト言語N-Codeによりシグネチャ・監視ツールの容易なプログラミングを可能にする技術。1996年より開発。 URL: <a href="http://www.nfr.com/products/technology.html">http://www.nfr.com/products/technology.html</a>
その他の認証技術	米国ActivCard, Incの開発による、時間・アクセス回数・秘密鍵の三種の変数に基づくワンタイムパスワード生成技術、及びICカードでのデジタル証明書格納、PKI鍵ペア生成、S/MIMEによるセキュアeメール、デジタル署名、SSLを用いたセキュアウェブアクセス技術。1998年より開発。 URL: <a href="http://www.activcard.com">http://www.activcard.com</a>

企業名（及び略称）	エヌ・ティ・ティ アイティ株式会社（NTT-IT）
代表者氏名	戸島 知之
所在地（郵便番号及び住所）	〒231-0032 横浜市中区不老町2-9-1 関内ワイズビル
関連部署名及び電話番号	ITソリューション事業部 045-651-7514
URL	<a href="http://www.ntt-it.co.jp/">http://www.ntt-it.co.jp/</a>
対象技術	技術開発状況
その他の認証技術  （ワンタイムパスワード認証技術 - PERM認証）	<p>ワンタイムパスワード認証技術 - PERM認証 -</p> <p>毎回の認証の度に、パスワードを変更することにより、ネットワーク途中でのパスワードの盗聴に対してセキュリティ耐性の強い認証方法としてワンタイムパスワード認証方式がある。ワンタイムパスワード認証は、サーバとの間で時間同期する方式（例えば一定時間毎にパスワードをサーバとクライアントで特定演算により更新）とチャレンジレスポンス方式（サーバから与えられたチャレンジコードに対してクライアント側で特定演算した結果を返送）があるが、PERM認証は、後者の方式を採用しており、かつ、ソフトウェアで簡易に実現でき安全性が高い方式として技術開発した。</p> <p>本PERM認証を用いた応用例として、暗号転送メールPop-up MAILを技術開発している。Pop-up MAILは、会社に届いたメールを一旦、暗号した後、ファイアウォールの外にあるPop-upメールサーバに転送して、事前に登録した利用者は、社外からその転送サーバにアクセスして本人あてのメールを確認したり返信したりできる。社外からファイアウォールに穴をあけずに、社外からメールを確認でき、かつ、暗号化されているため他人に見られる心配のない転送メールである。転送サーバにアクセスする際、本人確認のためにPERM認証方式を適用している。</p> <p>関連ホームページ： <a href="http://www.ntt-it.co.jp/goods/1ji/int/popup/index.html">http://www.ntt-it.co.jp/goods/1ji/int/popup/index.html</a></p>

企業名（及び略称）	エヌ・ティ・ティ・コミュニケーションズ株式会社
代表者氏名	鈴木 正誠
所在地（郵便番号及び住所）	〒100-8019 東京都千代田区内幸町一丁目1番6号
関連部署名及び電話番号	ソリューション事業部 e-ガバメント・ディベロップ営業部 03-3500-7305 ソリューション事業部 ITビジネス推進部 03-5363-2220
URL	<a href="http://www.ntt.com/">http://www.ntt.com/</a>
対象技術	技術開発状況
侵入検知技術 （H11.7開発）	以下の1)～6)を組合せて不正侵入を体系的に防止する技術。 1)セキュリティポリシー/スタンダード/マニュアル等の規定作成技術：ポリシーの規定の他、具体的な保護策を記述するスタンダード、利用規定を考慮したマニュアル等を体系的に作成する技術。 2)セキュリティ要件を満たしたSI技術：必要なセキュリティ要件を洗い出し、セキュリティ要件を満たした設計、構築を行なう技術 3)セキュリティホール調査技術：CERT、CIACの報告だけでなく、独自のデータベースによる方法で500種類以上の擬似攻撃を準備し、弱点を明確にする技術。 4)運用者向けのトレーニング：運用システム部門担当者を対象としたセキュリティ基礎教育を体系的に行なう技術。 5)ログ解析/モニタリング：200種類以上の項目を網羅したFWログ解析、300種類以上の監視項目に対応した24時間対応不正アクセス監視を行なう技術。
その他の認証技術 （H12.8開発）	e-Security ASP：インターネットを使った情報提供やWeb業務アプリケーションといったWebベースのプライベートネットワーク構築に欠かせない認証/認可（シングル・サイン・オン）や暗号化通信を実現するアプリケーションを複数ユーザで利用するASP。（関連HP <a href="http://www.ntt.com/tras/ec/SecIO/">http://www.ntt.com/tras/ec/SecIO/</a> ）

企業名（及び略称）	エヌ・ティ・ティ ソフトウェア株式会社
代表者氏名	鶴保 征城
所在地（郵便番号及び住所）	横浜市中区山下町233-1
関連部署名及び電話番号	eエンタープライズ事業部 / 03-5782-7261
U R L	<a href="http://www.ntts.co.jp">http://www.ntts.co.jp</a>
対象技術	技術開発状況
その他の認証技術	<p>以下の機能を開発</p> <p>Windowsクライアントから下記のシステムへのシングルサインオンをする  Unixサーバ、WindowsNTサーバ、WindowsNTドメイン、Lotus Notes、  Windowsアプリケーション、Webアプリケーション</p> <p>上記システムへのアクセス状況（ログオン成功、失敗など）のログを収集する</p> <p>Windowsクライアントの利用者を特定し、認められたユーザ以外がログオンできないようにする</p> <p>Unixサーバ、WindowsNTサーバ、WindowsNTドメインのアカウント情報を一元管理（作成、変更、削除）する</p> <p>Unixサーバ、WindowsNTサーバ、WindowsNTドメインの各アカウントのパスワードを自動的に変更し、パスワードを隠蔽化する</p> <p>（関連U R L <a href="http://www.ntts.co.jp/ps/csIguard/">http://www.ntts.co.jp/ps/csIguard/</a>）</p>

企業名（及び略称）	沖電気工業株式会社
代表者氏名	篠塚 勝正（取締役社長）
所在地（郵便番号及び住所）	〒105-8460 東京都港区虎ノ門1-7-12
関連部署名 / 電話番号	SSC BS事業部 システム開発第1部 / 048-431-7336 SSC IT開発センター / 027-325-1111
URL	<a href="http://www.oki.co.jp/">http://www.oki.co.jp/</a>
対象技術	技術開発状況
<p>侵入検知技術 「ネットワークセキュリティに関する不正侵入検知技術」 開発年：H12年</p> <p>その他の認証技術 「アイリス認識による個人確認技術の開発」 開発年：H7年～</p>	<p>インターネットからの不正アクセスを検出する従来の侵入検知システムでは、不正アクセスの特徴をあらかじめ登録しておき、実際に発生したアクセスと比較して不正アクセスを検出するシグネチャ解析技術が主流です。しかしながら、最近のサーバに対する過負荷攻撃のように、個々のアクセスには不正の特徴が無い無駄なトラフィックを大量に発生させる事でサーバのサービスを妨害する攻撃が現れてきました。本技術ではシグネチャ解析技術に加えて異常解析技術(確率推論)を用いることにより、トラフィックの起伏を観測し日常よりトラフィックが集中する攻撃やネットワーク上での異常状態を検知する事が可能です。さらに、確率推論方式はシグネチャに依存しないため、シグネチャが登録されていない未知の攻撃の検知も期待できます。</p> <p>当社では、人の目のアイリス(虹彩)紋様が、人によって異なっていることを利用して本人確認をする技術を開発し、コンピュータ単体、あるいはネットワークに接続されたコンピュータへの、アクセス制御に応用し、パスワードの代わりに利用できる技術を開発しました。この技術を実用化したアイリス認識装置は2種類に分類でき、1つは個人用コンピュータ(パソコン)でも使える程の価格と大きさを実現したタイプ、もう1つは、顔の映像から目の位置を検出してアイリスを撮影する自動照合タイプです。いずれの装置も、他人誤認識率(False Accept Rate)が120万分の1以下という、非常に高い精度で本人確認が可能です。</p> <p>詳しくは、下記URLをご参照下さい。 <a href="http://www.oki.co.jp/OKI/RDG/JIS/iris/index.html">http://www.oki.co.jp/OKI/RDG/JIS/iris/index.html</a></p>

企業名（及び略称）	株式会社データコントロール
代表者氏名	原 健人
所在地（郵便番号及び住所）	〒106-0032 東京都港区六本木2-2-8 ケルビンビル5階
関連部署名及び電話番号	営業本部 営業部 03-3582-2110
U R L	<a href="http://www.datacontrol.co.jp">http://www.datacontrol.co.jp</a>
対象技術	技術開発状況
ファイアウォール技術	<p>弊社は米国WatchGuard社（本社：ワシントン州シアトル市）からインターネット接続用ルータと社内ネットワークの間に設置するだけで、簡単にインストールする事ができるプラグアンドプレイのファイアウォール専用ハードウェアセキュリティ製品、WatchGuard FireboxIIシリーズを輸入し、販売をおこなっています。機能としてはパケットフィルタリングや、アプリケーションプロキシ等のファイアウォール機能に加え、スタティック/ダイナミックNAT（IPマスカレード）のネットワークアドレス変換、NT PDC、RADIUS、内部認証等のユーザ認証、CyberPatrolによるWebアクセス制御が有ります。</p> <p>販売にあたって、弊社では販売後のインストールサービス（システムインテグレーション含む）やダイレクトサポートサービスがあり、万一、故障が生じたときの修理サポートもご用意しています。（参照：米国WatchGuardホームページ <a href="http://www.watchguard.com">http://www.watchguard.com</a>）</p>

企業名（及び略称）	株式会社 東芝
代表者氏名	取締役社長 岡村 正
所在地（郵便番号及び住所）	〒212-8572 川崎市幸区堀川町7番地
関連部署名及び電話番号	官庁システム開発推進部 03-3457-4123
U R L	www.toshiba.co.jp
対象技術	技術開発状況
1. ファイアウォール技術	・ CheckPoint社のパケットフィルタリングベースのソフトウェアファイアウォールを当社ハードウェアと一体化し運用を容易にしたファイアウォール技術（2000年開発）
2. 侵入検知技術	<ul style="list-style-type: none"> <li>・ Webサーバに対するリクエストを既知不正アクセスのパターンと比較し、不正アクセスには即座にそのセッションを遮断することによってWebサーバの安全性を高める侵入検知技術（2000年開発）</li> <li>・ Internet Security Systems社のセキュリティ監視ツールを利用してセキュリティ監視システムを構築するサービス技術（2000年開発）</li> </ul>
3. その他の認証技術	<ul style="list-style-type: none"> <li>・ インターネット標準の公開鍵基盤（PKI）認証を実現する認証局システムをVeriSign社製品などを利用して構築するサービス技術（1999年開発）</li> <li>・ Webサーバにおける公開鍵認証やS/MIME対応のICカードシステム技術（2000年開発）</li> </ul>

企業名（及び略称）	日本電気株式会社（NEC）
代表者氏名	西垣 浩司
所在地（郵便番号及び住所）	東京都港区芝5丁目7-1（NEC本社ビル）
関連部署名及び電話番号	第一SL・パーソナルIDシステム営業部 TEL：03-3798-2940
URL	<a href="http://www.nec.co.jp/">http://www.nec.co.jp/</a>
対象技術	技術開発状況
その他の認証技術 （指紋認証技術） 1997年	<p>身体の一部である「指紋」を厳密な本人認証に利用する指紋技術を開発し、SecureFingerの名称で製品出荷している。NECでは、20年前から日本国内をはじめとして世界の司法分野に指紋自動識別システムを納入した実績を持つ。特に、NEC独自の「特徴点とリレーション」方式により、世界最高レベルの照合精度を実現すると同時に指紋画像の復元を防止してプライバシー保護も実現している。SecureFingerは、この技術を利用している。また、NECでは指紋認証システムを構築するための各種ハードウェアからソフトウェアを製品化すると同時に指紋システム構築に関するノウハウ提供サービスを行っており、指紋認証システム構築に対するトータルソリューションを提供している。</p> <p>これから展開されようとしている「電子社会」における様々な『認証』に、忘れない、無くさない、盗まれない「指紋認証」技術が重責を果たす。</p> <p>指紋認証URL <a href="http://www.sw.nec.co.jp/pid/">http://www.sw.nec.co.jp/pid/</a></p>

企業名（及び略称）	ノベル株式会社
代表者氏名	フィリップ・ケー・ウェルチ
所在地（郵便番号及び住所）	東京都世田谷区三宿1-13-1
関連部署名及び電話番号	マーケティング本部 03-5481-1645
U R L	www.novell.co.jp
対象技術	技術開発状況
その他の認証技術	<p>ネットワークに接続する際、認証デバイス（ICカード、トークン、バイオメトリックス、PKI等）の利用を可能にする技術。複数の認証デバイスやPKI、パスワードなどの組み合わせによるネットワークセキュリティ強化手法である「多要素認証」や、認証に用いるデバイスによってアクセス可能なデータの重要度を細かく設定できる「格付け認証」の機能に大きな特徴がある。また増大するネットワーク利用者数を効率的に管理する技術であるディレクトリサービスに対応。今後普及が予想される教育機関や企業内での身分証としてのICカード利用を、ネットワークへに対するセキュリティ管理まで拡張することを可能とする。2000年8月に製品化。</p> <p>詳細情報は：<a href="http://www.novell.co.jp/products/nmas/">http://www.novell.co.jp/products/nmas/</a></p>

企業名（及び略称）	富士ソフトABC株式会社
代表者氏名	野澤 宏
所在地（郵便番号及び住所）	〒247-0072 神奈川県鎌倉市岡本二丁目13番18号
関連部署名及び電話番号	ネットワーク部 045-323-1411
U R L	www.fsi.co.jp/
対象技術	技術開発状況
その他の認証技術	名称「FSIABC本人電子認証」
本人認証技術	特長：非常に手軽に導入でき、かつ信頼性が高い。
平成12年3月	1．インターネットを利用したオンライン認証である。
開発完了	2．認証キーとして名刺サイズのCD-Rを利用する。そのために携帯性にすぐれどのマシンからも認証できる、また特別な読取装置を必要としない。
	3．認証コードを画像データから生成するため第三者から判別が容易にでき不正利用を抑止できる。
	4．CD-Rは大容量で認証コード以外の広告や規約の配布にも利用できる。
	・基本的なメカニズムは、事前に顔写真のような第三者から容易に判別できる
平成12年3月	画像データを元とした認証コードを認証局に登録しておく。これと別にこの
特許出願	認証コードを記録し暗号化したミニCDカード™を利用者に配布しておく。
	利用者は自分の認証CDをパソコンのCDドライブにセットし、認証を要求すると、あらかじめPCにセットアップされている認証クライアントソフトによりCD内のデータが読み出され認証局に送信され登録されているデータと比較が行なわれる。暗号には当社が東京電機大学と共同開発した秘密鍵方式ストリーム暗号「FSAngo」を使用している。

企業名（及び略称）	株式会社山田洋行
代表者氏名	山田 正志
所在地（郵便番号及び住所）	〒150-0002 渋谷区渋谷2-10-6
関連部署名及び電話番号	情報通信システム部 03-3475-1557
U R L	www.yamada.co.jp
対象技術	技術開発状況
侵入検知技術 (2000年 開発済み)	<p>目的：HTML等のファイルの削除、移動、名前の変更、書き込みの防止</p> <ul style="list-style-type: none"> <li>・ 不法侵入者からのコンテンツ書き換え防止</li> <li>・ トロージャン等の不正なアクセスからの防止</li> <li>・ HTML, CGI, GIF, JPEG、Web環境ファイルその他の大切なファイルの入っているディレクトリのハッカーからの防御</li> </ul> <p>機能(HTTPProtect)</p> <p>OmniSecure社は、Webサイト、ファイル、e-Mailを防護するセキュリティ製品を開発しています。多くの脅威の中での1つがスーパーユーザーになって不法にアクセスされることです。OmniSecure社のコア技術は、Virtual Private Disk(VPDisk)という技術でユーザーレベルのアクセス権とスーパーユーザーとしての管理者のレベルを切り分ける事で、この問題点に対応しています。HTTPProtectを導入した場合には、スーパーユーザー権を持ったハッカーは、いかなるコンテンツも変更できません。</p> <p>又、Webに入ってくる人に対する認証とは、無関係な独自の技術でもありません。その為に、HTTPProtectをイントラネット、エクストラネット、一般的Webアクセスに導入することが出来ます。</p> <p>開発状況：現在Linux上でのバージョンを開発済み</p>