

資料編

(参考資料)

資料編（参考資料）

1. 平成14年中のハイテク犯罪の検挙及び相談受理状況について・・・ 3
2. 平成14年中の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について・・・ 7
3. 平成14年中のいわゆる出会い系サイトに関係した事件の検挙状況について・・・ 43
4. 平成14年度我が国におけるインターネット治安情勢の分析について
 - ◇ 平成14年度第2／四半期・・・ 49
 - ◇ 平成14年度第3／四半期・・・ 55
 - ◇ 平成14年度第4／四半期・・・ 61
5. 委員発表資料
 - ◇ 社会における情報セキュリティ対策について・・・ 67
 - ◇ 情報セキュリティに関する脅威について・・・ 79

別冊1 ハイテク犯罪等に係る被害状況の調査《報告書》

別冊2 ハイテク犯罪等に係る被害状況の調査《調査集計表》

平成14年中のハイテク犯罪の検挙及び相談受理状況等について

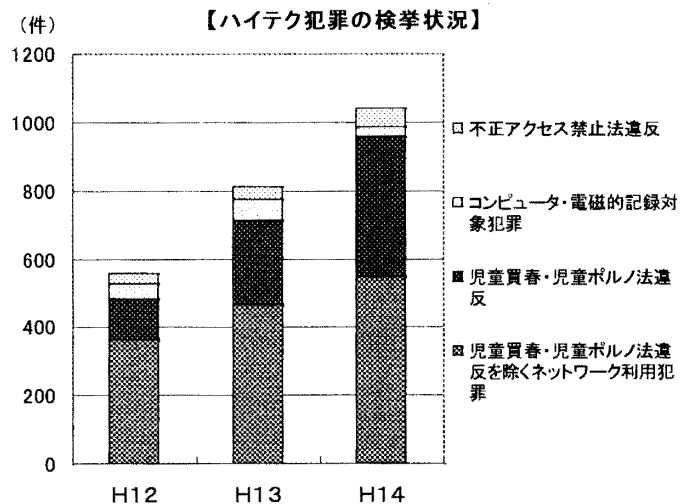
1 ハイテク犯罪の検挙件数は1,039件、うちネットワーク利用犯罪は958件で前年の712件と比べて約35%増加。

○ ネットワークを利用した児童買春・児童ポルノ法違反が増加。

・ 児童買春・児童ポルノ法違反のうち児童買春事件は268件で前年比約2.3倍、青少年育成条例違反は70件で前年比7倍にそれぞれ増加。

(すべて出会い系サイト利用)

○ 不正アクセス禁止法違反が51件、前年の35件から約1.5倍に増加。

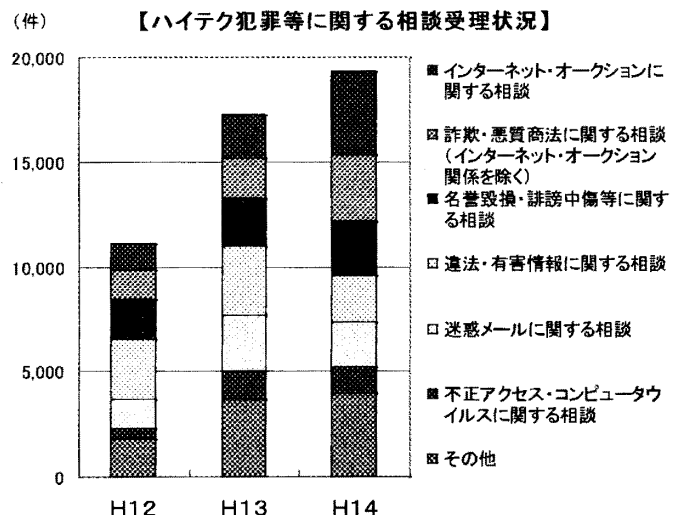


2 ハイテク犯罪等に関する相談受理件数は、19,329件で前年の17,277件と比べて約12%増加。

○ インターネット・オークションに関する相談が、前年比約1.9倍に増加。

○ ネットワークを使った詐欺・悪質商法に関する相談が前年比約1.6倍に増加。

※ 相談受理件数は、都道府県警察に寄せられた相談として警察庁に報告があったもの。



3 推進した対策等

- 産業界との連携のための総合セキュリティ対策会議の開催
- 企業等のWebサイトからの個人情報流出事案に関する注意喚起と情報提供
- ホームページ書き換え被害(Webサーバ用プログラム「Apache」のセキュリティホール対策)に関する注意喚起と情報提供
- インターネット治安情勢の分析と広報啓発による情報セキュリティ意識の高揚

◇ハイテク犯罪の検挙状況

(件)

罪 種	年		平成14年	平成13年	平成12年
			増 減		
不正アクセス禁止法違反	51	+16	35	31	
コンピュータ、電磁的記録対象犯罪	30	-33	63	44	
電子計算機使用詐欺	18	-30	48	33	
電磁的記録不正作出・毀棄	8	-3	11	9	
電子計算機損壊等業務妨害	4	0	4	2	
ネットワーク利用犯罪	958	+246	712	484	
児童買春・児童ポルノ法違反	268	+151	117	8	
児童買春・児童ポルノ法違反	140	+12	128	113	
詐欺	112	+9	103	53	
わいせつ物頒布等	109	+6	103	154	
青少年保護育成条例違反	70	+60	10	2	
脅迫	33	-7	40	17	
著作権法違反	31	+3	28	29	
名誉毀損	27	-15	42	30	
その他	168	+27	141	78	
合 計	1,039	+229	810	559	

※ その他には、覚せい剤取締法違反等の薬物事犯、銃砲刀剣類所持等取締法違反、売春防止法違反、商標法違反等がある。

◇平成14年中の主なハイテク犯罪検挙事例

不正アクセス禁止法違反事件

会社員が、自社及び他社のデータが管理されている特殊法人の研究開発用サーバに当該他社の社員のID及びパスワードを使用して不正にアクセスし、当該他社が開発していた部品に係る機密情報を入手した。
(平成14年5月検挙・警視庁)

コンピュータ・電磁的記録対象犯罪

【電子計算機使用詐欺事件】

知人のクレジットカード番号等を無断で使って、オンラインショッピングで電子マネーを不正に購入し、インターネット通販サイトから米をだまし取った。
(平成14年8月検挙・和歌山)

【支払用カード電磁的記録不正作出事件】

クレジットカード偽造グループが、風俗エステ店の客等のクレジットカードからスキミングの手口により不正に入手したカードの会員情報を、プラスチック板の磁気部分に記録して、支払用カードを不正に作った。
(平成14年1月検挙・警視庁、静岡)

ネットワーク利用犯罪

※ネットワーク利用犯罪とは、犯罪の構成要件に該当する行為についてネットワークを利用した犯罪、又は、構成要件該当行為ではないものの、犯罪の敢行に必要な不可欠な手段としてネットワークを利用した犯罪をいう。

【児童買春・児童ポルノ法違反事件】

携帯電話の出会い系サイトで書き込みをした女子中学生に「エッチなバイトで稼がないか。」等とメールで送信して誘い出し、児童買春をした。
(平成14年9月検挙・埼玉)

女子中学生が「裸の写真OK」等とインターネット上に書き込んだことから、この中学生と携帯電話のメールで交渉を行い、これに応じた中学生に現金を与えてわいせつな写真を撮影して児童ポルノを製造した上、CD-Rに記録してインターネットを利用して販売した。
(平成14年2月検挙・大阪)

【詐欺事件】

インターネット・カフェに設置されたパソコンを利用して他人のID及びパスワードを無断で使用し、インターネット・オークションの認証サーバに不正アクセスし、同オークションに「DVDソフト出品、傷はありません。」等と同会員になりすまして虚偽の情報を掲示し、落札者に対して代金の振込方法をメールで指示して他人名義の銀行口座に代金を振り込ませ、44人から総額約240万円をだまし取った。

なお、不正アクセス禁止法違反でも検挙。(平成14年1月検挙・茨城、栃木)

インターネット・オークションに「商品券50万円分を最低価格42万円で売却する。」などとの嘘の情報を掲示し、購入希望者から自分の銀行口座に代金を振り込ませる方法により、約80人から総額約1,800万円をだまし取った。(平成14年9月検挙・石川)

【わいせつ物頒布等事件】

ファイル共有交換ソフト「WinMX」のファイル共有機能をインストールしたパソコンを使用して、インターネット上で不特定多数の者に対してわいせつ画像を閲覧できる状態にして、わいせつ物を公然と陳列した。(平成14年3月検挙・岐阜)

【業務妨害・脅迫事件】

従業員が社内ネットワークのサーバーに保存されていた業務データを削除した上、自宅のパソコンから会社社長や同僚に「今後もデータを消す。」などとメールを送信し脅迫した。(平成14年11月検挙・宮崎)

【著作権法違反事件】

勤務先で使用していた地図測量ソフトを無断で複製した上、インターネット上のファイル公開用サイトに蔵置し、不特定多数の者がダウンロードできる状態にした。

(平成14年9月検挙・宮城)

【名誉毀損事件】

インターネットを利用して男性会員勧誘のための架空の会員制クラブを設け、被害女性のホームページから無断で入手した顔写真、架空の氏名、年齢や「5,000円で同女の電話番号等を提供する。」等との文書を掲載した同クラブの勧誘広告を、不特定多数の者に電子メールで送信し、被害者の名誉を毀損した。

なお、クラブの会員登録料名下に現金をだまし取り、詐欺罪でも検挙。

(平成14年6月検挙・埼玉)

◎その他

【覚せい剤取締法違反事件】

インターネットの掲示板に覚せい剤密売の広告を掲載し、購入希望者とメール交換により取引の方法を約束し、約30人に対して約60グラムを売り渡し、250万円を売り上げた。

(平成14年6月検挙・京都、警視庁、福島、長崎)

【ストーカー規制法違反事件】

かつて交際していた女性に対して、約80回にわたり、携帯電話のメールを使い「部屋の窓閉めないでよ。昨日寝たのは11時半ころかな。明日も来る。」などの内容のメッセージを送信し、女性を監視していると思われるような内容を伝えストーカー行為を行った。

(平成14年10月検挙・長崎)

【薬事法違反事件】

薬局開設、医薬品販売業の許可を受けずに、ホームページに医薬品である不能治療薬「威哥王」(イガワン)の広告を掲載し、インターネットを利用して約180人に販売した。

(平成14年5月検挙・警視庁)

【銃刀法違反事件】

インターネット・オークションに改造けん銃を出品し、落札者に対して同改造けん銃を売り渡した。

(平成14年5月検挙・長野)

◇相談受案件数

	平成14年	平成13年	平成12年
インターネット・オークションに関する相談	3,978	2,099	1,301
詐欺・悪質商法に関する相談 (インターネット・オークション関係を除く)	3,193	1,963	1,396
名誉毀損・誹謗中傷等に関する相談	2,566	2,267	1,884
違法・有害情報に関する相談	2,261	3,282	2,896
迷惑メールに関する相談	2,130	2,647	1,352
不正アクセス、コンピュータウイルスに関する相談	1,246	1,335	505
その他	3,955	3,684	1,801
合 計	19,329	17,277	11,135

※ その他の相談には、プロバイダや有料サービス会社とのトラブルやネットワークセキュリティ全般に関する相談が含まれる。

◇平成14年中の主な相談事例

1 インターネット・オークションに関する相談

- オークションでパソコンを落札し、代金を指定の口座に振り込んだ後に出品者の評価を確認したところ、50件以上の悪い評価がついていた。詐欺にあったのではないかと不安である。
- インターネット・オークションに車体番号、ナンバー、車検証がないという盗難車らしい高級車が出品されている。
- 私がオークションに出品している商品の紹介写真をそのまま使って出品している者がいる。

2 詐欺・悪質商法に関する相談

- 自宅でインターネットをしていたところ、知らない間に国際電話に接続されたようで、国際電話会社から高額な電話料金の請求を受けた。
- インターネット上に「ワールドカップのチケットを1試合につき250枚確保している」という内容の広告があり、チケット購入代金を振り込んだが、チケットが届かない。

3 名誉毀損・誹謗中傷に関する相談

- インターネット上の掲示板で、1年くらい前から名前を出されて誹謗中傷を受け、最近では、毎日の行動内容などの情報も書かれた上、携帯電話に「死ね」等とメールで送られてくる。
- インターネット上の掲示板に「こんな社長ではだめだ」、「最悪の会社」等と会社を誹謗中傷する書き込みをされている。

4 迷惑メールに関する相談

- 中学生の間に、「メールを転送しないと殺される」といった内容のチェーンメールが広まっている。
- アダルト関係の広告メールが、頻繁に送られてくる。受信拒否のメールを送っているが、毎回発信元のメールアドレスを変えて送信してくる。

5 違法・有害情報に関する相談

- インターネット上の掲示板に動物虐待に関する書き込みがあり、虐待の様子画像を流している。
- 小学生の子どもにインターネットを使わせるに当たって、アダルトサイトなど有害なサイトが見られないようにしたいが、どのようにすればよいか。

6 不正アクセス、コンピュータウイルスに関する相談

- 手帳に記載してあったパスワードを見た交際相手が、メールを盗み見ている。
- 知らない人から「あなたから、ウイルス付きのメールが来た」と抗議を受けたが、何者かがメールアドレスを詐称してウイルスをばらまいているようだ。

7 その他

- 近く退職を予定している社員が、会社のパソコンに保存されたデータを個人のパソコンにコピーして自宅に持ち帰っているようである。会社の情報セキュリティポリシーの策定について教えて欲しい。
- インターネットでチャットに参加していたところ、ネットストーカーに付きまとわれ、わいせつなメッセージを送りつけられて困っている。

平成15年2月20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14年1月1日から平成14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14年中の不正アクセス禁止法違反事件の検挙状況等について

平成14年中に全国の都道府県警察から警察庁に報告のあった不正アクセス行為を対象とした。

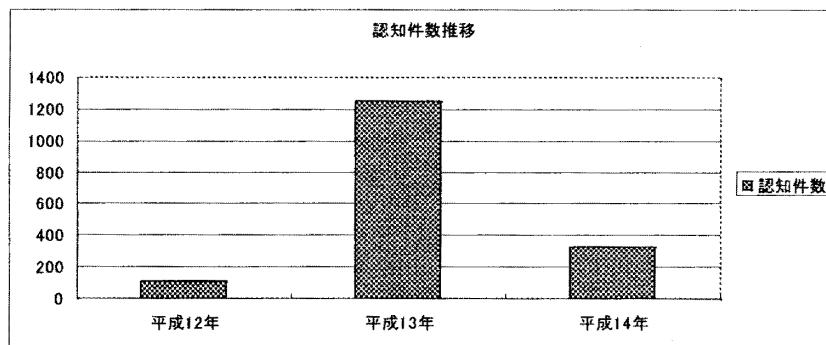
なお、本文中平成12年の数字は、不正アクセス禁止法の施行日である平成12年2月13日から平成12年12月31日までの間のものである。

1 不正アクセス行為の発生状況及びその特徴

(1) 認知件数（注1）（注2）

平成14年中の不正アクセス行為の認知件数は329件で、前年と比べ、924件減の大幅減少となった。

減少の原因は、前年に多発したホームページ書き換えプログラムによるホームページ書き換え事案等（935件）のセキュリティ・ホール攻撃型（注3）事案が平成14年は激減したためであり、官民挙げた広報活動や、修正プログラムの普及によりセキュリティ・ホールの解消が進んだことがうかがえる。



	平成12年	平成13年	平成14年
認知件数	106	1,253	329
海外からのアクセス	25	448	13
国内からのアクセス	73	258	286
アクセス元不明	8	547	30

(2) 被害に係る特定電子計算機のアクセス管理者（注4）

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243件と最も多く、次いで一般企業の62件となっている。

被害に係る特定電子計算機のアクセス管理者	平成12年	平成13年	平成14年
プロバイダ	59	182	243
一般企業	25	429	62
大学、研究機関等	8	101	3
その他	14	139	21
うち行政機関	—	—	12
不明	0	402	0
計	106	1,253	329

※「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事業者をいう。
「大学、研究機関等」には、大学、高等学校等の学校機関及びその附置機関を含む。
「その他」の「うち行政機関」には、国の行政機関、独立行政法人、特殊法人、地方公共団体及びこれらの附属機関を含む。
なお、平成12年及び平成13年は「その他」の内訳の集計をしていない。

(3) 認知の端緒

認知の端緒としては、警察職員によるいわゆるサイバーパトロールや被疑者の取調べ等の警察活動が185件と最も多く、次いで利用権者（注5）からの届出が92件、アクセス管理者からの届出が47件の順となっている。

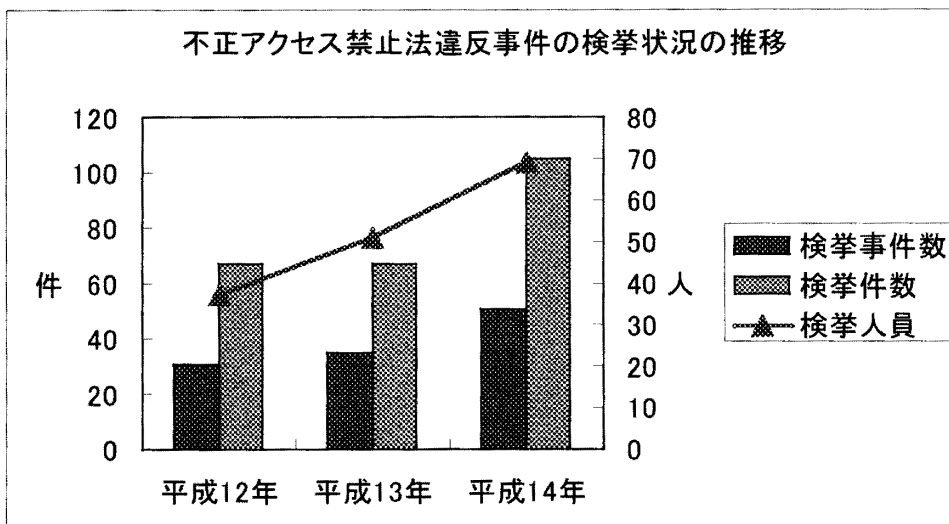
(4) 不正アクセス行為後の行為

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入札、販売代金の取得等）が177件と最も多く、次いでホームページの改ざんが38件、インターネットの利用が18件、電子メールの盗み見が17件、パスワード変更が13件、バックドア（注6）・ツールを仕掛けたものが10件の順となっている。

2 不正アクセス禁止法違反事件の検挙状況

検挙状況は、検挙事件数（注7）、検挙件数及び検挙人員ともに増加している。

検挙事件の多くは識別符号窃用型（注8）であり、インターネット・オークションや電子メール等のサービスを対象とする事犯が目立ったほか、インターネット・バンキング等の金融サービスを対象とした事犯もみられた。これらの多くは、他人により推知されやすいパスワードが設定されていた。このほか、高度な技術を用いてサーバのセキュリティの脆弱性を突くセキュリティ・ホール攻撃型もみられた。



		平成12年	平成13年	平成14年
不正アクセス行為	検挙事件数	30	35	51
	検挙件数	62	66	102
	検挙人員	34	51	68
不正アクセス助長行為	検挙事件数	4	1	2
	検挙件数	5	1	3
	検挙人員	5	1	3
計	検挙事件数	31 (重複3)	35 (重複1)	51 (重複2)
	検挙件数	67	67	105
	検挙人員	37 (重複2)	51 (重複1)	69 (重複2)

3 不正アクセス行為の検挙事例

1	プロバイダの認証サーバに対するバッファ・オーバーフロー攻撃（注9）に係る不正アクセス禁止法違反事件
---	---

外国人留学生の男（24）が、自己の技量を試す目的で、プロバイダの認証サーバに対して、当該サーバのセキュリティ・ホールにバッファ・オーバーフロー攻撃を仕掛けて不正アクセスし、ハッキング・ツールの蔵置を行った。また、当該サーバを踏み台として、別のプロバイダの複数のサーバに対しても不正アクセスし、ホームページを改ざんした。14年1月、不正アクセス禁止法違反で検挙した（警視庁、滋賀）。

2	インターネット・オークションの識別符号を窃用した不正アクセス禁止法違反及び詐欺事件
---	---

大学生の男(20)が、インターネット・オークションを利用して金を騙し取る目的で、他人のインターネット・オークション用ID及びパスワードを使用してオークションサービスのサーバに不正アクセスし、架空の出品を行い、落札者44人から総額約240万円を、インターネットを利用して購入した他人名義の銀行口座に振り込ませて騙し取った。14年1月、不正アクセス禁止法違反及び詐欺で検挙した(茨城、栃木)。

3	他人の電話回線を利用した不正アクセス禁止法及び有線電気通信法違反事件
---	------------------------------------

無職の男(36)が、通信料金及びインターネット接続料金の課金を免れる目的で、他人の電話回線に自己の電話回線を接続した上、別の他人のインターネット接続用ID及びパスワードを使用してプロバイダの認証サーバに不正アクセスし、インターネットを利用した。14年4月、不正アクセス禁止法違反で検挙し、5月、同人を有線電気通信法違反で追送致した(岐阜、福島)。

4	リマインダ機能を利用して入手したパスワードを使用して他人の電子メールを盗み見した不正アクセス禁止法違反事件
---	---

男子中学生(14)が、好奇心から、同級生である女子中学生の無料電子メール・サービス用のパスワードをリマインダ機能(注10)を利用して不正に入手した上、ID及び当該パスワードを使用してメール・サーバに不正アクセスし、電子メールを盗み見た。14年4月、不正アクセス禁止法違反で検挙した(徳島)。

5	無料電子メールサービスの識別符号を窃用した不正アクセス禁止法及び電気通信事業法違反事件
---	---

社員の男(32)が、嫌がらせの目的で、出会い系サイトで知り合った女性の電子メールアドレスのIDからパスワードを推測して電子メールサービス事業者のメールサーバに不正アクセスし、電子メールの内容を盗み見たほか、当該アドレスを使用して卑わいな内容の電子メールを送るなどした。14年5月、不正アクセス禁止法違反及び電気通信事業法違反で検挙した(香川)。

6	特殊法人の研究開発用サーバに係る不正アクセス禁止法違反事件
---	-------------------------------

会社員の男（28）が、他社の技術情報を盗み見る目的で、自社及び他社のデータが管理されている特殊法人の研究開発用サーバに他社の社員のID及びパスワードを使用して不正アクセスし、当該他社が開発していた部品に係る機密情報を入手した上、当該他社の社員のID及びパスワードを特定する方法を自社の社員に電子メールで通知した。また、当該電子メールを見た別の社員（40）ら2人が、別の他社社員のID及びパスワードを使用して当該研究開発用サーバに不正アクセスした。14年5月、不正アクセス禁止法違反で会社員3人を検挙した（警視庁）。

7	インターネット・バンキング利用の不正送金事件に係る不正アクセス禁止法違反、私電磁的記録不正作出・同供用及び電子計算機使用詐欺事件
---	--

会社員の男（31）が、他人の口座から金を不正に得る目的で、銀行のインターネット・バンキング用の認証サーバに、当該銀行の顧客サポート・サービスに従事していた当時に知り得た口座開設者の口座番号、暗証番号等の識別符号を使用して不正アクセスし、当該口座をインターネット・バンキングが利用できる状態に変更した上、送金に必要な識別符号を使用して当該サーバに不正アクセスし、自己が開設した他人名義の銀行口座に不正に送金した。14年5月、不正アクセス禁止法違反、私電磁的記録不正作出・同供用及び電子計算機使用詐欺で検挙した（警視庁）。

8	オンライン・トレード利用の株式取引に係る不正アクセス禁止法違反及び私電磁的記録不正作出・同供用事件
---	---

会社員の男（32）が、社内で自己に対する評価が低いことに不満を抱き、会社を困らせる目的で、自己が開発に携わった派遣先証券会社のオンライン・トレード用の認証サーバに、当該システムの開発時に盗み見た当該証券会社の口座開設者のID及びパスワードを使用して不正アクセスし、当該口座開設者になりすまして株式売買を行った。14年6月、不正アクセス禁止法違反及び私電磁的記録不正作出・同供用で検挙した（警視庁）。

9	インターネット接続料金を免れる目的の不正アクセス禁止法違反事件
---	---------------------------------

会社員の男（34）が、インターネット接続料金の課金を免れる目的で、勤務当時知り得た会社の顧客のインターネット接続用ID及びパスワードを使用してプロバイダの認証サーバに不正アクセスし、インターネットを利用した。14年10月、不正アクセス禁止

法違反で検挙した（愛知）。

4 検挙事件の特徴

(1) 犯行の手口

識別符号窃用型の不正アクセス行為で検挙した46事件（83件）における当該識別符号（ID及びパスワード）の入手方法は、利用権者のパスワードの設定・管理の甘さにつけ込み入手するものが最も多く23事件（34件）であった。その内訳は、パスワードがIDから容易に推知できるもの（例えば、IDが「keisatsu1234」に対して、パスワードを「keisatsu」や「1234」としているもの。）や単純な文字列であったもの（例えば、パスワードを「aaaa」としているもの。）が17事件（28件）、リマインダ機能における質問への安易な回答が設定されていたものが6事件（6件）である。

また、元システム管理者など、立場上、識別符号を知りうる者によるものが17事件（33件）、識別符号が記された電子メールや封書の誤配によるものが2事件（2件）みられた。

一方で、サーバのセキュリティ・ホールにバッファ・オーバーフロー攻撃を仕掛けた事案のように、高度なコンピュータ技術及び電気通信技術を用いてセキュリティの脆弱性を突くセキュリティ・ホール攻撃型も引き続きみられた。

(2) 被疑者

元社員や元交際相手等利用権者の顔見知りの者による犯行は33事件（56件）であり、全くの他人による犯行は19事件（49件）であった。（1事件は、利用権者と顔見知りの者及び他人の複数の被疑者がいる。）

また、検挙した被疑者の年齢は、20代が30人と最も多く、次いで30代が26人、40代が7人、10代が6人の順となっている。最年少の者は14歳であり、最年長の者は47歳であった。

(3) 犯行の動機

不正アクセス行為の動機としては、元勤務先や元交際相手等に対する嫌がらせや仕返しに19事件（29件）と最も多く、次いで好奇心や自己の技量を計るために試みるものが13事件（32件）、利用料金の請求を免れるためが5事件（14件）、メールを盗み見るためが3事件（6件）、不正に金を得るためが2事件（6件）の順となっている。（重複計上あり。）

(4) 利用されたサービス

識別符号窃用型の不正アクセス行為で検挙した46事件（83件）において、当該識別符号を入力することにより利用できるサービス別に見ると、無料電子メールなどの電子メール・サービスが11事件（19件）と最も多く、次いでインターネット・オークション・サービスが10事件（13件）、インターネットへの接続サービス（ダイヤルアップ・サービス）が6事件（15件）、無料ホームページ作成サービスが6事件（9件）、金融サービス（インターネット・バンキング等）が3事件（8件）の順となっている。

(5) その他

不正アクセス禁止違法違反のほか、他の罪についても検挙した事件は、17事件であった。

	事 件 数
電子計算機損壊等業務妨害	2
電気通信事業法違反	3
詐欺	2
電子計算機使用詐欺	1
私電磁的記録不正作出・同供用	7
恐喝未遂	1
有線電気通信法違反	1
組織的な犯罪の処罰及び犯罪収益の規制等に関する法律違反	1
偽計業務妨害	2
医師法違反	1
有印私文書偽造・同行使	1

※重複計上あり。

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条の援助規定に基づくアクセス管理者に対する助言・指導を5件（北海道1、愛知2、大阪1、島根1）実施した。

6 防御上の留意事項

(1) サーバの適切な管理

セキュリティ・ホール攻撃型の不正アクセス行為の発生件数は大幅に減少したが、この種手口による事犯は、一旦発生すれば被害が大きくなる危険があることから、引き続きセキュリティ水準の維持・向上が必要であり、特にサーバの管理者等はインターネット上などで常にセキュリティ情報を確認し、使用しているオペレーティング・システム又はアプリケーション・プログラムにセキュリティ・ホールが発見されたことを知ったときは、速やかに修正プログラムをインストールするなどセキュリティ・ホールを解消するための措置を講じる必要がある。

(2) 識別符号の適切な設定・管理

識別符号窃用型の不正アクセス行為で検挙した46事件（83件）中、23事件（34件）が利用権者のパスワードの設定・管理の甘さにつけ込んで入手するものであったことから、利用権者においては、他人による推知が難しいパスワードを設定すること、リマインド機能に関しては、アクセス管理者及び利用権者において、パスワード再発行時に必要となる情報（質問に対する回答）を、他人による推知が困難となるような仕組み及び内容とすることが必要である。

そのほか、利用権者等においては、パスワードを定期的に変更するなど識別符号を適切に設定・管理する必要がある。

一方で、アクセス管理者は、サーバを適切に管理するだけでなく、利用権者に対して識別符号の適切な設定・管理について注意喚起を行うなどの不正アクセス行為を防止するために必要な措置を講ずるよう努める必要がある。

(注1) 認知

ここで認知とは、被害届出を受理した場合のほか、余罪として確認した場合、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その他関係資料により不正アクセス行為の事実確認ができた場合としている。

(注2) 件数

件数とは、被疑者が行った犯罪構成要件に該当する行為の数をいう。

なお、不正アクセス行為の件数の計上については、ひとつのアクセス制御機能に対するひとつの手口による侵害行為が1回あったことをもって1件としている。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、短期間にひとつのアクセス制御機能に対して同一手口による侵害が連続的に行われ、実質上1回の行為とみなしうる場合は包括して1件としている。

(注3) 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、バッファ・オーバーフロー攻撃による不正アクセス行為が該当する。

(注4) アクセス管理者

アクセス管理者とは、ネットワークに接続しているコンピュータ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店主がそれぞれアクセス管理者である。

(注5) 利用権者

利用権者とは、ネットワークに接続されたコンピュータをネットワークを通じて利用することについて、当該コンピュータのアクセス管理者の許諾を得た者をいう。

例えば、プロバイダからインターネット接続サービスを受けることを認められた会員や、企業からLANを利用することを認められた社員が該当する。

(注6) バックドア

バックドアとは、部外からネットワークを通じて不正にサーバに侵入するための裏口のことである。クラッカー等は、一度侵入に成功したサーバにバックドアを設置することにより、当該バックドアを通じて次回以降の侵入を容易に行うことが可能となる。バックドアの設置方法は巧妙化してきており、当該サーバのアクセス管理者が存在に気付かない場合があるほか、削除しても再起動後に自動的にバックドアが設置されるツールが当該サーバに組み込まれている場合もある。バックドアが設置されたサーバから確実に当該バックドアを駆除するためには、オペレーティングシステムの再インストール及び修正プログラムのインストールを行うことが望ましい。

(注7) 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には1事件と数える。

(注8) 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ID及びパスワードを使用して、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9) バッファ・オーバーフロー攻撃

コンピュータに対して、通常処理できる容量を超えるデータを送信することにより、当該コンピュータへのプログラムの追加、改ざんを行うことをいう。

(注10) リマインダ機能

利用権者がパスワードを忘れてしまった時に、アクセス管理者が何らかの方法で本人確認を行った上でパスワードを再発行する機能である。本人確認の方法としては、サービス利用のための登録時に、本人が決めた情報を登録しておき、パスワードの再発行時にその情報を利用権者に入力させるもの（例えば、「出身小学校は？」等の質問に対して、あらかじめ登録しておいた情報を答えとして入力すると、パスワードが再発行される）などがある。

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届出状況について

平成14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被害届出件数は619件（昨年：550件）であった(注2)。平成14年は、ワーム感染及びワーム形跡（未感染）に関する届出が大幅に減少した一方、侵

入やアクセス形跡、DoS（サービス妨害）の届出が増加し、ワーム感染以外の実被害届出件数が219件（昨年：197件）と増加した。

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

(1) 手口別分類

意図的に行う攻撃行為による分類である。重複があるため、届出件数とは異なり総計は790件（昨年：333件）となる。なお、この件数には、ワームに関する届出は含まれていない。

ア 侵入行為に関して

侵入行為に係わる攻撃等の届出は671件（昨年：193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。94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。そのなかで実際に侵入の被害を受けたのは4件であった。

(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。135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106件である。

パスワード推測：4件

ソフトウェアのバグを利用した攻撃：47件

システムの設定内容を利用した攻撃：33件

(ロ) 不正行為の実行及び目的達成後の行為

実際に侵入を受けた106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：65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：42件

資源利用（ファイル、CPU使用）：20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：24件

裏口の作成：5件

証拠の隠滅：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る攻撃である。22件（昨年：11件）の届出があった。

過負荷を与える攻撃：15件

例外処理を利用した攻撃：3件

SPAMメール：4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、97件（昨年：94件）の届出があった。

メール中継に関するもの：18件

そのうちメール中継に実際に利用されたもの：16件

メールアドレス(ドメイン)の詐称：48件

その他：31件

(2) ワーム別の分類

ワームの種類による分類である。ワームに関する届出は、実際にワームに感染した届出6件、ワームには感染しなかった届出34件、合計40件であった。主なワームの届出件数は以下の通りである。

Nimda：16件（うち感染：0件）

CodeRed：12件（うち感染：2件）

Spida：9件（うち感染：0件）

その他（Slapperなど）：21件（うち感染：4件）

(3) 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106件（昨年：97件）、ワームに感染した6件（昨年184件）、メール中継に係わる問題（弱点）のあった16件（昨年：25件）などの計151件（昨年：307件）を分類すると以下ようになる。

ID、パスワード管理の不備によると思われるもの：3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：48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：33件

不明：67件

(4) 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。

WWWサーバ：86件

メールサーバ：29件

DNSサーバ：5件

FTPサーバ：10件

ファイアウォール：7件

ルータ：3件

Proxyサーバ：2件

その他のサーバ・不明：68件

クライアント：410件

(5) 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225件（昨年

: 375件) である。

WWW書き換えの被害は26件(昨年: 177件)と減少したが、ファイルの書き換え(プログラム埋め込み、ファイル削除含む)77件(昨年39件)、不正アカウント作成12件(昨年: 4件)、パスワードファイルの盗用7件(昨年: 4件)と被害内容が深刻になってきている。

なお、対処に係わる工数やサービスの一時停止、代替機の準備などに関する被害は除外している。

メール中継に利用された: 16件

サーバダウン: 4件

不正アカウント作成: 12件

WWW書き換え: 26件

パスワードファイル盗用: 7件

サービス低下: 15件

オープンプロキシ: 1件

ファイルの書き換え: 77件

その他: 110件

(6) 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14年1月1日から12月31日の間にJPCERT/CCに届出のあったコンピュータ不正アクセスが対象である。

(1) 不正アクセス関連行為の特徴および件数

届出のあった不正アクセス関連行為（注1）に係わる報告件数は1,435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1,160件の報告があった。
[1/1-3/31: 289件、4/1-6/30: 199件、7/1-9/30: 304件、10/1-12/31: 368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57件の報告があった。

[1/1-3/31: 24件、4/1-6/30: 14件、7/1-9/30: 9件、10/1-12/31: 10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39件の報告があった。

[1/1-3/31: 15件、4/1-6/30: 4件、7/1-9/30: 12件、10/1-12/31: 8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: 6件、4/1-6/30: 4件、7/1-9/30: 4件、10/1-12/31: 6件]

オ その他

コンピュータウィルス、SPAMメールの受信、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等について176件の報告があった。

[1/1-3/31: 31件、4/1-6/30: 51件、7/1-9/30: 44件、10/1-12/31: 50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]

DNS resolver の脆弱性に関する注意喚起
OpenSSH サーバプログラムの脆弱性に関する注意喚起
Apache Web サーバプログラムの脆弱性に関する注意喚起
TCP 1433番ポートへのスキャンの増加に関する注意喚起
SNMPv1 の実装に含まれる脆弱性に関する注意喚起

イ 緊急報告

[新規]

OpenSSL の脆弱性を使って伝播する Apache/mod_ssl ワーム

[更新]

OpenSSL の脆弱性を使って伝播する Apache/mod_ssl ワーム（更新）

ウ 技術メモ

[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 4）
関係サイトとの情報交換（Version 4）

エ 活動概要（届出状況等の公表）

発行日：2003-01-17 [2002年10月1日 ～ 2002年12月31日]

発行日：2002-10-18 [2002年7月1日 ～ 2002年9月30日]

発行日：2002-07-19 [2002年4月1日 ～ 2002年6月30日]

発行日：2002-04-23 [2002年1月1日 ～ 2002年3月31日]

オ JPCERT/CC レポート

[発行件数] 50件

[取り扱ったセキュリティ関連情報数] 217件

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

（注2）ここにあげた件数は、JPCERT/CC が受け付けた報告の件数である。実際

の攻撃の発生件数や、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。

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。

情報通信危機管理基盤技術の研究開発

暗号アプリケーションプログラムインターフェース基盤技術に関する研究開発

出所不明の packets 流出を許さないセキュアな情報通信ネットワークに関する研究開発

次世代証拠基盤技術に関する研究開発

情報セキュリティ高度化のためのデータ保護技術に関する研究開発

相互接続時のセキュリティポリシーの管理技術に関する研究開発

属性認証を用いたサービスの相互接続技術に関する研究開発

大規模ネットワークセキュリティの確保に向けた研究開発

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

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

2. 民間企業で研究を実施したもの

平成14年11月11日から12月13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、別紙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。

Argusシステムズ・グループ 株式会社

RSAセキュリティ 株式会社

株式会社 アクセスチケットシステムズ

インターネット セキュリティ システムズ 株式会社

エヌ・ティ・ティ アイティ 株式会社

エヌ・ティ・ティ・ソフトウェア 株式会社

九電情報サービス 株式会社

シーア・インサイト・セキュリティ 株式会社

シスコシステムズ 株式会社

ジャパン・インフォメーション・テクノロジー 株式会社

株式会社 セキュアプロバイダ

大日本印刷 株式会社

株式会社 東芝

株式会社 ドリームウェア

日本オラクル 株式会社

日本電気システム建設 株式会社

株式会社 ネットコム

富士ゼロックス 株式会社

株式会社 ランデック

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～平成 15 年度
実施主体	独立行政法人通信総合研究所
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処するため、ネットワーク上に生じた異常を的確に検出・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、平成 12 年度に、総務省通信総合研究所に、不正アクセス模擬実験装置等を備えたネットワークセキュリティ施設、危機管理用安全対策施設、検証実験用テストフィールド、の 3 つからなる情報通信危機管理研究施設を整備し、不正アクセス行為やサイバーテロを検証・再現し、対策を講じるための研究開発を開始した。平成 13 年度にはこれらの施設を拡充し、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、およびサービス不能攻撃への対処方法の検討、等を進めた。また、不正アクセス模擬実験装置を実ネットワークに接続し検証する方法の研究開発、および電磁波漏洩対策に関する研究開発、等に着手した。平成 14 年度以降は、不正アクセスに関する各種事例を更に収集し、サービス不能攻撃等への対処方法の検討を更に進める。また、他組織の脆弱性データベースとの接続実験に着手し、電磁波漏洩対策に関する研究開発を更に推進する。
詳細の入手方法（関連部署名及びその連絡先）	独立行政法人通信総合研究所 情報通信部門 非常時通信グループ 大野浩之 電話 042-327-5542
将来の方向性	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。

対象技術	その他の認証技術
テーマ名	暗号アプリケーションプログラムインターフェース基盤技術に関する研究開発
開発年度	平成 13 年度～平成 15 年度
実施主体	日本電気株式会社（通信・放送機構(TAO)からの委託）
背景、目的	<p>政府・自治体、各企業における申請業務、調達・購買業務の電子化が数年内に本格化する動きにあり、電子文書の真正性や機密性を確保する電子署名技術、暗号化技術の重要性は日々増している。電子政府や電子商取引などのアプリケーションには、プラットフォームフリーの JAVA が採用され始めており、電子文書交換のための標準フォーマットについても XML が定着しつつある。しかしながら、署名・暗号化ライブラリとのインターフェース（暗号 API）は未だ標準化に至らず、各々のアプリケーションが個別に対応しているため、互換性を損なっているのが現状である。また、XML 文書に対して暗号化を施した文書の格納フォーマット（以下、XML 暗号文書フォーマットという）も、アプリケーション毎に個別に定義しているため、XML 暗号文書の相互運用性も確保できない。</p> <p>そこで、電子政府システムや電子商取引システムなどへの適用を想定して XML 暗号文書フォーマットを策定し、JAVA 実行環境における XML 署名・暗号化のための API を実現するとともに電子署名、暗号化処理を実現するアーキテクチャの構築を目的とする研究開発を実施する。</p>
研究開発状況（概要）	<ul style="list-style-type: none"> ・平成 13 年度から以下の研究開発を実施中。 <ul style="list-style-type: none"> (1)XML 文書に対する署名・暗号インターフェース (2)Web クライアントのブリッジ機能 ・平成 15 年度末に上記研究開発完了予定。
詳細の入手方法（関連部署名及びその連絡先）	<p>通信・放送機構 (http://www.shiba.tao.go.jp)</p>
将来の方向性	<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>

対象技術	その他の認証技術
テーマ名	出所不明の packets 流出を許さないセキュアな情報通信ネットワークに関する研究開発
開発年度	平成 13 年度～平成 15 年度
実施主体	株式会社東芝（通信・放送機構(TAO)からの委託）
背景、目的	<p>電子投票など、サーバに多数のコネクションが集中するケースでは、DoS(Denial of Service)攻撃等のサイバー攻撃によって、サービスが致命的なダメージを受ける危険性がある。そのため、サーバ自体にコネクションを張る前の段階で、不正な通信を排除することが求められる。</p> <p>また、不正な通信と正しい通信を判別するためには、利用者認証と機器認証を組み合わせるなどの方法によって、より厳密な認証を実現することが望まれる。</p> <p>これらの技術の実現によって、不正な通信をより早期に発見・遮断し、ネットワークの不正利用防止と重要システムの保護を可能とする研究開発を実施する。</p>
研究開発状況（概要）	<ul style="list-style-type: none"> ・平成 13 年度から以下の研究開発を実施中。 <ul style="list-style-type: none"> (1)ネットワーク層における段階的な利用者・機器認証を行うプロトコル (2)上記プロトコルを用いたポリシーベースの各種管理技術 ・平成 15 年度末に上記研究開発完了予定。
詳細の入手方法（関連部署名及びその連絡先）	<p>通信・放送機構 (http://www.shiba.tao.go.jp)</p>
将来の方向性	<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>

対象技術	その他の認証技術
テーマ名	次世代証拠基盤技術に関する研究開発
開発年度	平成 13 年度～平成 15 年度
実施主体	株式会社日立製作所（通信・放送機構(TAO)からの委託）
背景、目的	<p>電子政府の実現には、電子文書の証拠性が必須であるが、電子文書の証拠性確保は電子署名などの暗号技術に依存しており、20～30 年以上の期間にわたって証拠性を確保しない限り、これらの電子文書は補助的にしか扱うことはできない。また、電子文書の保存のみならずネットワーク上の様々な行為などの証拠性の確保も、電子文書の証拠性を長期間維持する基盤技術の実現の研究として実施する必要がある。本研究では、以上に対応する技術開発を実施する。</p>
研究開発状況（概要）	<ul style="list-style-type: none"> ・平成 13 年度から以下の研究開発を実施中。 <ul style="list-style-type: none"> (1)電子文書の証拠性を長期にわたって維持する技術 (2)証拠性保証基盤システム (3)証拠性保証システムにおけるネットワークモデル (4)ヒューマンインターフェイス ・平成 15 年度末までに上記研究開発完了
詳細の入手方法（関連部署名及びその連絡先）	<p>通信・放送機構（http://www.shiba.tao.go.jp）</p>
将来の方向性	<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>

対象技術	侵入検知技術
テーマ名	情報セキュリティ高度化のためのデータ保護技術に関する研究開発
開発年度	平成 13 年度～平成 15 年度
実施主体	日本電気株式会社、東京工業高等専門学校、株式会社富士総合研究所、リコーシステム開発株式会社、東京工業大学、エヌ・ティ・ティ・コミュニケーションズ株式会社（平成 13 年度まで三菱電気株式会社も参加）（通信・放送機構(TAO)からの委託）
背景、目的	<p>ネットワーク上の資源は、ネットワーク機器やサーバ・クライアント装置などのハードウェア、ハードウェア上で様々なサービスをネットワーク利用者に提供するアプリケーションなどのソフトウェア、そして利用者のユーザデータに大別できる。ハードウェアとソフトウェアは、サイバー攻撃により破壊を受けても入れ替えることで修復することが可能であるが、人間の知的生産の結果であり各ユーザにとって最も重要な資産であるユーザデータは、バックアップがない限り再生することは不可能である。</p> <p>さらに、次世代インターネットプロトコルである IPv6 では、ユーザは特別の知識なしに情報機器等をネットワークに接続し、その利便性を享受できる反面、グローバルネットワークアドレスの使用により、LAN 内に置かれたユーザデータに対するサイバー攻撃の危険性が増加すると考えられる。</p> <p>以上により、ネットワーク上に存在するユーザデータをどのように守るかが重要な課題となりつつあることから、サイバー攻撃に対して耐性を持つネットワークとして、保存装置等の周辺機器が OS の管理から独立して動作することで、データに対する不正アクセスの防止、データの保存、復旧を図るためのアーキテクチャを研究・開発し、さらにこのアーキテクチャを保存装置以外の周辺機器に応用し、セキュリティ面で高機能な外部装置を開発することを目的とする。</p>
研究開発状況（概要）	<ul style="list-style-type: none"> ・平成 13 年度から以下の研究開発を実施中。 <ul style="list-style-type: none"> (1)データ保護機能を有する電子保存技術 (2)データ保護機能を有する分散環境自動構築技術 ・平成 15 年度末までに上記研究開発完了予定。
詳細の入手方法（関連部署名及びその連絡先）	<p>通信・放送機構（http://www.shiba.tao.go.jp）</p>
将来の方向性	<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>

対象技術	その他の認証技術
テーマ名	相互接続時のセキュリティポリシーの管理技術に関する研究開発
開発年度	平成 13 年度～平成 15 年度
実施主体	富士通株式会社、九州大学、株式会社富士通プライムソフトテクノロジー (通信・放送機構(TAO)からの委託)
背景、目的	<p>電子政府や電子商取引など、異なるネットワークのインターネット相互接続ニーズが高まる中、相互接続時におけるセキュリティレベルの一貫性の確保が大きな問題として認識されている。この問題への対応として、特定のサイトで集中的にセキュリティ管理を行う方法があるが、このような方法は非常に大きな負荷の集中を招きやすく、スケーラビリティの問題が指摘されている。</p> <p>また、将来的には、パソコンだけでなく全ての携帯電話や PDA(Personal Digital Assistants)などが P2P(Peer to Peer)型のネットワークを構成する可能性もある。</p> <p>このような莫大な数のネットワークの相互接続と将来的な分散ネットワーク環境を念頭に、集中管理型ではなく自律分散型でネットワーク相互間のアクセス制御を実現し、セキュリティレベルの一貫性を確保するセキュリティ管理システムの開発を実施する。</p>
研究開発状況 (概要)	<ul style="list-style-type: none"> ・平成 13 年度から以下の研究開発を実施中。 <ul style="list-style-type: none"> (1)相互接続時のセキュリティポリシー管理技術 (2)標準化活動と普及促進 ・平成 15 年度末までに上記研究開発完了予定。
詳細の入手方法 (関連部署名及びその連絡先)	通信・放送機構 (http://www.shiba.tao.go.jp)
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	その他の認証技術
テーマ名	属性認証を用いたサービスの相互接続技術に関する研究開発
開発年度	平成 13 年度～平成 15 年度
実施主体	株式会社日立製作所（通信・放送機構(TAO)からの委託）
背景、目的	電子政府、商行為、組織内業務など、将来的には非常に多くの分野で各種の電子申請、取引行為が実施されるものと思われる。このとき、特定の資格を持った人の申請機能や特定の会員・組織に属する人に限ったアクセス制御機能が必要になるが、本研究では、単独のサービス内に閉じた申請ではなく、複数の独立したサービスが連携することによって新たなサービスを提供するという、サービスの相互接続を前提とした電子申請に対応した技術開発を実施する。
研究開発状況（概要）	<ul style="list-style-type: none"> ・平成 13 年度から以下の研究開発を実施中。 <ul style="list-style-type: none"> (1)資格証明機能の拡張技術 (2)アプリケーション利用時の制御技術 ・平成 15 年度末に上記研究開発完了予定。
詳細の入手方法（関連部署名及びその連絡先）	通信・放送機構（ http://www.shiba.tao.go.jp ）
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	大規模ネットワークセキュリティの確保に向けた研究開発
開発年度	平成 14 年度～平成 16 年度
委託先	松下電工株式会社、工学院大学、安川情報システム株式会社 NTT アドバンステクノロジ株式会社（通信・放送機構（TAO）からの委託）
背景、目的	<p>最近の不正アクセス件数の増加等、システム運用・管理に対する脅威が増加する中で、より安全性・信頼性の高い大規模ネットワークシステムを構築するために、セキュリティの確保が不可欠であり、セキュリティ侵害への対処方法や再発防止などの対策を行うことを可能にするセキュリティ運用の仕組みの研究開発が求められている。</p> <p>そこで、分散化・階層化された様々なネットワーク機器等の情報（稼働状況、通信のやりとりを記録したデータ、アクセスログ等）の集中的な管理と不正データの発信源探査を基盤とする統合的なセキュリティ運用の仕組みについて研究開発を行う。</p>
研究開発状況（概要）	<ul style="list-style-type: none"> ・平成 14 年度より以下の研究開発を実施中。 <ul style="list-style-type: none"> (1) 様々な機器のログを集中的に管理するための仕組みの研究開発 (2) 送信元 IP アドレスを偽装したデータから真の発信元を探査するための発信源探査技術の研究開発 ・平成 16 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）	通信・放送機構（ http://www.shiba.tao.go.jp ）
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	その他の認証技術
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
開発年度	平成12年度から
実施主体	独立行政法人 産業技術総合研究所 グリッド研究センター
背景、目的	<p>電子政府、電子自治体、ネットバンキング、電子商取引などの様々なサービスが、インターネットから誰でもいつでも利用できるようにと、Web アプリケーションとして構築される動きが急激に拡大しつつある。しかし、Web アプリケーションのアクセス制御機能は、統一された安全規格があるわけではなく、各サイトで個別にその都度設計・実装が行われており、その安全性は、システムの発注者が仕様書に安全基準を正しく盛り込めるか、あるいは、受注者が自主的に正しい設計・実装を行うかにかかっている。我々のこれまでの調査で、なりすましアクセスを許してしまう欠陥のあるサイトが、実際に数多く運用に供されていた事実が判明している。</p> <p>こうしたアクセス制御機能の欠陥（セキュリティ脆弱性）の問題は、新技術の開発というアプローチで回避できるものではなく、発注仕様書の作成、システムの開発、納品物の検収に携わる各現場の技術者が、安全なアクセス制御に関する正しい知識を持つ他に解決の道はない。</p> <p>この研究は、実運用サイトに存在した欠陥の原因を分析し、正しい設計・実装のための技術情報を事例に基づいて公表することで、同じ欠陥が繰り返し生産される事態を防止することを目的とする。</p>
研究開発状況（概要）	<p>平成14年度の成果：</p> <p>秘密情報を含まない cookie に頼ったアクセス制御方式の欠陥について調査し、国内の5つのサイトにおいて、のべ4百万～5百万人分ほどと推定される個人情報（ユーザ番号（ないしユーザ名）を送信するだけでパスワードなしに誰でもいつでも閲覧可能な状態にあったことを指摘した。これらの事例を基に、この欠陥の原理と解決策を解説する文書を公表した。</p> <p>13年度から14年度にかけて運用を開始した政府認証基盤（GPKI）および地方公共団体組織認証基盤（LGPKI）において、通信路の信頼の起点となるはずのルート証明書およびそのフィンガープリント（真正性確認情報）が、信頼できない通信路によって配布されており、誤った安全確認手段を国民に習慣づけてしまう危険性があることを指摘した。</p> <p>平成13年度の成果：</p> <p>クロスサイトスクリプティング脆弱性について調査し、国内の大手サイト8か所において個人情報が漏洩する可能性があり、うち3サイトではクレジットカード番号も盗まれ得る状態であることを指摘した。また、プライバシーマークおよびオンラインマークの取得事業者から無作為に抽出した50サイトと、銀行22サイトのうち、約8割に同脆弱性が残存していることを確認した。10月には、経済産業省からこの問題について周知徹底を図るよう関係団体に要請する通知がなされた。</p> <p>平成12年度の成果：</p> <p>国内18か所のWebメールサービスのうち7ヶ所に、URLに含まれるセッションIDが漏洩することが原因でメールの内容を盗み見られる欠陥があることを指摘し、事例に基づく原因の解説を公表したところ、「REFERER 問題」として広く知られることとなり、他のサービスにおいても同様の欠陥が自発的に修正されることとなった。</p> <p>現在の研究状況：</p> <p>アクセス制御機能の欠陥には他にも様々な形態のものがあり、現在も調査を継続中である。 アクセス制御機能の欠陥を機械的に検出する診断ソフトウェアの研究開発を進めている。</p>
詳細の入手方法	<p>これまでに公開した論文、資料等は下記のURLより入手できる。 http://SecurIT.etl.go.jp/</p>
将来の方向性	<p>Web アプリケーションを含むシステムの発注仕様書で安全基準を指定するのに利用できる、実効的な欠陥防止対策リストの作成。</p>

対象技術	侵入検知技術
テーマ名	ネットワーク侵入検出システム IDA (IntrusionDetection Agent system)の研究開発
開発年度	
実施主体	情報処理振興事業協会技術センター (研究協力機関：早稲田大学、日本総合研究所、SRA、上越教育大学)
背景、目的	<p>インターネットの普及に伴い、増加している侵入（不正アクセス）は、特定のサイトだけをターゲットにしたものでなく、どのようなサイトでも起りうる。このような状況下で、どのサイトにも容易に導入可能な、独自の侵入検出システム IDA を研究開発する。</p> <p>IDA は、ホストベースのネットワーク侵入検出を目的としたシステムであり、従来の侵入検出システム (IDS) のように、ネットワーク上に分散したホストのログをサーバに集中させることなく、モバイルエージェントによって必要な情報のみ収集し、それを解析して侵入を検出するものである。</p> <p>また IDA は、システムに重要な被害を与える攻撃を重点的に検出し、なおかつ頻繁なアップデート等を必要としない軽量な IDS の開発を目的とし、複数のサイトを踏み台としている攻撃の起点を追跡する機能も併せて開発する。</p>
研究開発状況（概要）	<p>(1) リモートアタック検出機能</p> <p>軽量でかつ未知のリモートアタック（システム上になんら権限を持っていない状況からの侵入）を検出可能な手法を研究開発し、侵入検出システム IDA 上に実装する。軽量化のために、「痕跡」という侵入に付随して発生する事象からの検出から侵入解析を始める。痕跡検出後の侵入判定手法として、多変量解析の一分野である判別分析を用いている。これにより未知のリモートアタックも検出可能になる。</p> <p>(2) インターネット上の侵入追跡機能</p> <p>踏み台の起点を追跡するための、情報公開サーバシステムの開発を行う。LAN 内の接続情報を分散処理し、踏み台を追跡するために必要な情報のみ Web サーバ上で公開する方式を開発する。公開情報をもとに、踏み台を追跡することが可能になる。</p> <p>(3) IDS 保護のための機能</p> <p>侵入検出システムそのものが攻撃対象になった場合の防御メカニズムを研究開発する。すなわち侵入判定に係わるプロセスや、ログファイル等の保護を行う。これはカーネルレベルでのアクセス制御を行うことによって実現する。この保護機能は IDA だけでなく、Linux ベースのホストベース IDS で実装可能である。</p> <p>(4) 各種ソースコードの公開</p> <p>IDA 及び Linux 用の拡張セキュリティモジュール群 LSM (Linux Security Module) のソースコードを公開した。また、IDA から派生したマルチホストベースの侵入検出システム (IDA サーバ・クライアント版) 及び単一ホスト上のみで動作する侵入検出システム (IDA スタンドアロン版) のソースコードも公開した。</p>
詳細の入手方法	<p>これまでに公開された論文等は下記の URL より入手可能。また上記開発ソフトおよびマニュアルについても、同様の URL にて入手可能。</p> <p>http://www.ipa.go.jp/STC/IDA/japanese/</p>
将来の方向性	<p>本研究で得られた「痕跡」に基づく検出手法および多変量解析による判定手法は、他の IDS ネットワークベース IDS も含む。</p>

企業名（及び略称）	Argus Systems Group inc. (Argus)
代表者氏名	Paul McNabb
所在地（郵便番号及び住所）	1809 Wood field Drive Savoy, IL 618745
関連部署名及び電話番号	全社 +01-(217) 355-6308
URL	http://www.argus-systems.com/company/offices/
対象技術	技術開発状況
ファイアウォール 1995年開発	・イントラ内サーバへの侵入・攻撃の防止 コンパートメント間の通信をOSレベルで制御することにより不正な通信をブロックし、企業内の大切なサーバやデータを守ります。
その他認証技術 1995年開発	・スーパーユーザ・アカウントの不正使用を防止 全ての特権を持つスーパーユーザが事実上、存在しなくなるため不正な手段で取得したIDや内部ユーザによる不正アクセスも防止します。
その他アクセス制御技術 1995年開発	・トロイの木馬、バッファオーバーフロー攻撃の無力化 あらかじめ設定されたセキュリティポリシーをOSレベルで強制することにより不正プログラムによる攻撃を無効にします。 ・Webページの改ざん防止 Webページを外部アクセスからは書き込み不可なコンパートメントに設定し、ハッカーによる改ざん、破壊を防止します。 ・PKI、IDS等、他のセキュリティの無力化防止 PKIやIDS、暗号化、ファイアウォール等、従来のセキュリティ製品自体の無力化を狙った攻撃からガードし、TOTAL的に高度なセキュリティを実現可能

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）	〒100-0005 東京都千代田区丸の内1-3-1 東京銀行協会ビルチング13F
関連部署名及び電話番号	マーケティング統括本部 (03) 5222-5240
URL	http://www.rsasecurity.co.jp
対象技術	技術開発状況
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 1985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	武田 守也
所在地（郵便番号及び住所）	〒160-0023 東京都新宿区西新宿 8-11-1 日東星野ビル 2F
関連部署名及び電話番号	マーケティング部 03-5338-8865（代表）
URL	http://www.accessticket.com
対象技術	技術開発状況
その他認証技術 平成 12 年度 ～平成 14 年度	<p>PKI（公開鍵インフラ）等の認証技術によって、電子行政、インターネット上の商行為、イントラネットにおける組織内業務などの局面で、個人の身許を確認する手段が整備されてきた。しかし、アクセス制御という観点で考えると、個人認証だけでは不十分である。実際、個人認証では、印刷、転記などのアクセス権を管理したり、不正行為を防止する手立ては提供されない。</p> <p>アクセス制御に求められる認証は、単なる個人の身許の認証ではなく、個人に帰属するアクセス権とアクセスルールを併せて認証する機能である。これを、個人の認証と対照させる意味で、「アクセス権の認証」と呼ぶが、実用のアクセス制御では、アクセス権認証によって確認されたアクセス権・アクセスルールを遵守(enforce)させるためのコンテンツの永続保護の技術も必要となる。</p> <p>当社は、公開鍵暗号を用いて、PKI と同等のオープン性を保ちながら、アクセスルールを含む「アクセス権の認証」を実現する技術を開発している。また、コンテンツの永続保護に関しても、基本的な技術の開発を終え、様々なフォーマットの文書やイメージ、html、動画などに対応し、今後はコンテンツの機密性に応じ暗号アルゴリズムや鍵長の選択機能も実装する予定。</p>

企業名（及び略称）	インターネット セキュリティ システムズ株式会社（ISS）
代表者氏名	林 界宏
所在地（郵便番号及び住所）	〒141-0021 東京都品川区上大崎三丁目 1 番 1 号 JR 東急目黒ビル
関連部署名及び電話番号	マーケティング部 03-5740-4072
URL	http://www.isskk.co.jp
対象技術	技術開発状況
侵入検知技術（1997 年）	<p>不正侵入検知システム（IDS）は、セキュリティ上の不審な動きを監視し、問題が発生した場合に警告する。弊社 IDS は、シグネチャによるパターンマッチング分析／プロトコル分析／ビヘイビア分析を採用。Gigabit 環境にも対応可能なネットワーク型とホスト型（サーバ用、クライアント用）があります。</p> <p>不正侵入検知システムにより</p> <ol style="list-style-type: none"> 1) 不正・不審な活動の状況把握 サイト／ホストに対する内外からの不正アクセスや疑わしい活動を把握する。ユーザのネットワーク利用状況などの把握も可能。不審な動きを早期に発見することにより、情報漏洩などを未然に防ぐことができます。 2) 不正侵入・攻撃に対する迅速な対応・防御支援 サイト／ホストに対する不正アクセスや攻撃の兆候をリアルタイムに検出すると、管理者に警告通知をすることができます。 3) 不正侵入に関する情報（ログ）の記録および保存 侵入者の特定やログ情報の保管、ログ改竄、消去された場合 IDS のログにて検証可能。

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	橋田 幸雄
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	http://www.ntt-it.co.jp/
対象技術	技術開発状況
その他の認証技術	<p>ワンタイムパスワード認証技術技術-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： http://www.ntt-it.co.jp/goods/lji/int/popup/index.html</p>

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）	〒231-8554 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
URL	http://www.ntts.co.jp/
対象技術	技術開発状況
その他の認証技術	<p>シングルサインオン認証と統合アカウント管理に関する技術</p> <ol style="list-style-type: none"> 1. シングルサインオン認証/アクセスコントロール： <ul style="list-style-type: none"> 1回の認証を受けるだけで、そのユーザが利用可能な各システム（OS、DB、アプリケーション等ユーザID/パスワードが設定されているもの）に自動ログオンでき、各システム本来の実アカウント/パスワードを隠蔽化。 また、利用者の権限によるWebコンテンツのアクセスコントロールを実現。 2. ポリシーベースの統合ユーザ管理： <ul style="list-style-type: none"> システム毎に存在するアカウント情報やユーザ情報をLDAPベースで統合管理する。 3. ユーザ認証技術と統合ユーザ管理技術の連携： <ul style="list-style-type: none"> 上記両技術は互いに連携し、大規模なクライアントサーバ型イントラネット環境から300万ユーザ規模のWeb系エクストラネット環境までの共通的な認証基盤を効率的に実現。 4. 各種ユーザ認証技術との連携： <ul style="list-style-type: none"> 指紋等のバイOMETRICS認証やICカード、電子証明書技術、VLAN認証、ユビキタス等、さまざまなユーザ認証技術と連携。 5. 相互認証方式の検討： <ul style="list-style-type: none"> 独立した認証システム（認証により守られたWebサービス）間をSOAP、SAML等のWebサービスの標準連携機能を用いて、安全に、かつ、個々の認証システムのセキュリティを守りながら、利用者に統合されたひとつの認証システムとして関連するWebサービスを提供。

企業名（及び略称）	九電情報サービス株式会社
代表者氏名	五嶋 皓洋
所在地（郵便番号及び住所）	〒810-0004 福岡県福岡市中央区渡辺通 2-1-82 電気ビル第2別館3階
関連部署名及び電話番号	技術企画室 Tel 092-781-9671 Fax 092-711-7223
URL	http://www.kyuden-is.co.jp/
対象技術	技術開発状況
その他認証技術	<p>双方向ワントタイムパスワード認証システムとファイアウォール制御を連携したアクセス制御技術</p> <p>ホットスポットなどのモバイル環境から社内ネットワークにアクセスする際、「双方向ワントタイムパスワード認証システム」、「ピア・ツウ・ピアSSLストランスポート」、「ファイアウォール（FW）」の3つのセキュリティ要素を結合させ遠隔地から安全なWebアクセスを可能とした技術。</p> <p>●インターネット上のセキュリティに関して</p> <p>モバイル端末と「双方向ワントタイムパスワード認証システム」間は通信の都度リアルタイムにワントタイムパスワードを双方向に交換すると共に暗号化通信により、なりすまし等からの脅威に対応。FWを経由し社内へアクセスを行う際には、「双方向ワントタイムパスワード認証システム」上で認証されてから、社内への接続が許可されるため、第三者の不正アクセスを拒絶。認証システムではユーザ情報は管理されておらず、ユーザ情報流出などからリスクから保護されている。</p> <p>●社内ネットワーク（FWの内側）へのアクセスに関して</p> <p>認証済みの通信パケットをFWを透過して社内へ接続する際は、FWの外側と内側と設置したサーバ間において、暗号化されたピア・ツウ・ピアSSLストランスポート技術を使用した通信を行う事で、現用FWのセキュリティポリシー（通過ポートの修正）は変更せずに不正なアクセスから防護できる。</p> <p>●既存技術との優位点</p> <ul style="list-style-type: none"> ・一般的に普及している携帯電話を使用した、遠隔地からの利用（リモートアクセス：RAS）と比較すると、公開されたインターネット網を使用することで、従来の方式に比べて安価に情報基盤が構築できるため、ネットワーク費用も大幅に削減可能。 ・サービスを提供するコンピュータ（サーバ）は、外部からの攻撃に対して考慮する必要がなくなり、システム開発の生産性が向上する。 ・複数の高度なセキュリティ技術を複合した（分散化された2要素認証）。 <p>【特許出願番号 2002-299528（リモートアクセス方法及びリモートアクセスシステム）】</p>

企業名（及び略称）	シーア・インサイト・セキュリティ株式会社
代表者氏名	向井 徹
所在地（郵便番号及び住所）	〒104-0061 東京都中央区銀座 2-2-19 藤間ビル 6F
関連部署名及び電話番号	技術開発部門 03-3561-1552
URL	http://www.seerinsight.co.jp/
対象技術	技術開発状況
侵入検知技術	<p>開発年度 平成 13 年～平成 14 年度</p> <p>・「ログ情報のリアルタイム監視による侵入検知とログ情報の改竄保護システム」</p> <p>サーバのログ情報をリアルタイムで監視し、不正行為に対する異常検知を行うと共に、ログ情報を改竄や削除から保護する為の技術を実用化した。本システムは UNIX と Windows の OS プラットフォームに対応しており、汎用性が高い。また、電子文書証明センターとの連携でログ情報の原本性証明を行う事が可能であり、電子政府や電子自治体、金融機関などの高度なセキュリティ対策に有効である。</p>
その他認証技術	<p>開発年度 平成 13 年～平成 14 年度</p> <p>・「LAN ユーザの個人認証・操作履歴管理と情報視覚化による不正認証検知システム」</p> <p>IC カードやバイオメトリクス認証システムや、認証 V-LAN スイッチ等と連携した認証アプリケーションソフトウェアと、LAN 上の PC クライアントユーザの操作履歴を取得・管理するためのソフトウェアを実用化した。又、情報視覚化技術を用いてネットワーク情報を視覚化し、グループモニタリングによる不正認証検知システムを実用化した。</p>

企業名 (及び略称)	シスコシステムズ株式会社
代表者氏名	代表取締役社長 黒澤 保樹
所在地 (郵便番号及び住所)	〒107-0052 東京都港区赤坂二丁目 14 番 27 号 国際新赤坂ビル東館
関連部署名及び電話番号	官公庁営業部 03-5545-2168
URL	http://www.cisco.com/jp/
対象技術	技術開発状況
その他認証技術 <開発(実装)年> LEAP:2000 年 PEAP: 2002 年(draft)	<p>■無線 LAN から特定電子計算機(ネットワークに接続された電子計算機)へのアクセスを制御する相互認証技術(LEAP/PEAP)</p> <p>LEAP(Lightweight Extensible Authentication Protocol : EAP Cisco Wireless)及び PEAP(Protected EAP)は、いずれも IEEE802.1X 標準に基づき、無線 LAN 端末と認証サーバを相互認証するプロトコルである<注>。</p> <p>LEAP は、Cisco 社が開発したプロトコルで、認証サーバと無線 LAN 端末の相互認証を行い、PEAP では、相互認証の手続き自体をあらかじめ暗号化された通信路を用いて行う。</p> <p>LEAP/PEAP の適用により、ネットワークにログオンできない(未認証の)無線 LAN 端末は、アクセスポイント(基地局)からネットワーク内部への通信ができない。ユーザ認証には、RADIUS サーバが利用され、中央集中型の認証が可能で、ユーザ毎かつセッション毎に WEP キーが動的に生成され、WEP キーの解読が困難であるとともに、万が一解読された場合でも被害は最小限である。</p> <p>LEAP/PEAP の実装により、無線 LAN からの不正アクセスの多くを防ぐことが可能である。</p> <p><注>PEAP は Cisco Systems、Microsoft、RSA Security が Draft を提出し、IETF Working Group Security Area にて標準化作業中</p> <p>関連 URL : http://www.ietf.org/proceedings/02mar/slides/eap-3/index.html</p>

企業名 (及び略称)	ジャパン・インフォメーション・テクノロジー株式会社 (JIT)
代表者氏名	石崎 利和
所在地 (郵便番号及び住所)	〒101-0051 東京都千代田区神田神保町 3 丁目 10 番地 3 松晃ビル 5F
関連部署名及び電話番号	03-3511-8971
URL	http://www.jit-g.co.jp
対象技術	技術開発状況
その他認証技術 開発期間 2000 年 1 月より 2002 年 7 月 合計 2 年 6 ヶ月 侵入検知技術 開発期間 2000 年 1 月より 2002 年 7 月 合計 2 年 6 ヶ月	<p>1. サービスの概要</p> <p>現状のセキュリティ技術は情報システムに対するセキュリティ技術です。しかし、重要な物は情報システムと言う器ではなく情報と言う中身です。この重要な情報に対するセキュリティ技術を確立させ、不正アクセス、侵入、情報漏洩、情報改竄に対し強力なセキュリティ技術を確立し総合セキュリティシステムを開発しました。</p> <p>2. 商品</p> <p>データベースのカラム単位に暗号化を自動的に行う事により従来の技術では不可能だったデータベースの暗号化技術を確立しました。更に、利用者認証、利用権限、データの改竄検知機能を付加し不正アクセス、データ漏洩、データ改竄を防止いたします。</p> <p>3. 効果</p> <p>ハッキング、情報漏洩、情報改竄を防止しプライバシーを保護する日本発世界初の技術を開発することにより、全世界の Web システムに導入されることに成ります。アウトソーシング出来なかった機密性の高いシステムもアウトソーシング出来るように成ります。結果 e-コマースの健全な発展を育成する基礎技術となり経済界に大きなインパクトを与えます。</p>

企業名（及び略称）	株式会社セキュアプロバイダ
代表者氏名	小川 秀治
所在地（郵便番号及び住所）	〒150-0002 東京都渋谷区渋谷 1-5-2 須藤ビル 203
関連部署名及び電話番号	営業企画部 03-3400-7839（代表）
URL	http://www.s-provider.co.jp
対象技術	技術開発状況
その他認証技術 開発年：1997年	<p>脳内記憶情報により本人確認を行う認証技術</p> <p>ワンタイムパスワード認証方式でありながら、個人の「記憶」というバイOMETRICS認証の要素をも兼ね備えた認証技術。利用者側に特殊デバイスの常備携帯・変換プログラムのインストール作業等を一切必要とせず、サーバにインストールするだけで実現できる。ワンタイムパスワード認証方式のチャレンジ&レスポンス方式の一種と言え、その手法は以下の通り。</p> <p>認証サーバは、利用者からのユーザ ID 入力があれば、利用者のブラウザに乱数が表示されたマトリクス表（チャレンジコード）を送付する。利用者はブラウザのマトリクス表から、利用者自身が設定した「抜き出し位置」にある数字を抽出・「変換法則」で変換してパスワード（レスポンスコード）を作成し認証を行う。認証サーバは、利用者と同じ法則でパスワードを生成しておき、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。</p>

企業名（及び略称）	大日本印刷株式会社
代表者氏名	矢野 義博
所在地（郵便番号及び住所）	〒162-8472 東京都新宿区榎町7番地
関連部署名及び電話番号	アプリケーション開発部 03-3513-2740
URL	www.dnp.co.jp/bf
対象技術	技術開発状況
その他認証技術 開発年：H13年	<ul style="list-style-type: none"> ◆ICカードを用いた本人認証技術 ◆ICカード内部でのデジタルサイン技術 ◆X.509の電子証明書を用いたアクセス認証／制御 ◆PKI技術（#11,CSP）で、SSLおよびS/MIMEが利用可能 ◆PC/SC環境下でのICカード抜き差し検知技術によるスクリーン制御

企業名	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）	〒105-8001 東京都港区芝浦一丁目1番1号
関連部署名及び電話番号	e-ソリューション社 渉外担当 03-3457-2652
URL	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～2002年開発）
2. 侵入検知技術	<ul style="list-style-type: none"> ・Webサーバ、メールサーバ、DNS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サーバの安全性を高める侵入検知・防御技術（2000～2002年開発） ・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） ・Webサーバの通信状態や負荷状態を監視することにより、Webサーバに過剰な負荷をかけ、Webサーバ機能をダウンさせるDoS攻撃やDDoS攻撃を検出・防御する技術（2001～2002年開発）
3. その他認証技術	<ul style="list-style-type: none"> ・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） ・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）

企業名（及び略称）	株式会社ドリームウェア
代表者氏名	田中光一
所在地（郵便番号及び住所）	〒160-0023 東京都新宿区西新宿8-14-24 西新宿KFビル7F
関連部署名及び電話番号	
URL	http://www.log saver.jp/
対象技術	技術開発状況
その他認証技術	<p>【背景・目的】</p> <p>不正アクセス行為の手口は巧妙になる一方で、さらに内部使用者による不正行為も問題視されている。そこで、完全に不正アクセスを防御する事は不可能だという事を前提に、今までになかったAfterセキュリティに焦点を。具体的にはログファイル管理に着目した。</p> <p>【適用技術】</p> <p>既存には無いPacketWriting方式を適用する事により、発生するログファイル（ログデータ）を、リアルタイムでCD-Rへ記録する事を可能とした。これにより保全性のあるログファイルを管理する事が可能となる。保全性のあるログデータを分析する事により、初めて完全な分析結果を得る事ができると考える。</p>

企業名（及び略称）	日本オラクル株式会社
代表者氏名	新宅 正明
所在地（郵便番号及び住所）	〒102-0094 東京都千代田区紀尾井町 4-1 ニュートンコート
関連部署名及び電話番号	テクノロジーコンサルティング本部アドバンステクノロジー&サポートセンター 03-5213-6666（代表）
URL	http://www.oracle.co.jp/
対象技術	技術開発状況
侵入検知技術 開発年：H13年 : H14年 その他認証技術 開発年：H12年 : H14年	<p>■以下の2つの技術を組み合わせることで、不正侵入を検知する。</p> <p>1) 機密データに対するアクセスのみの監査を行うことで、システムへの侵入と機密データの窃取を検知する技術。</p> <p>2) 機密データに対するアクセスがあった場合に、任意のトリガー（ロジック）を起動する技術。</p> <p>3) データベース管理者の不審なアクセスに対しても監査を行って機密データへの窃取を検知する技術。</p> <p>■大規模ウェブアプリケーションの構築に不可欠なシングルサインオンを実現する技術。</p> <p>■大規模クライアントサーバーアプリケーションの構築に不可欠なシングルサインオンを実現する技術。</p> <p>■生体的特長を利用してデータベースに認証を行う技術。</p> <p>■ICカード等を利用してデータベースに認証を行う技術に加え、ウェブアプリケーションに対するシングルサインオンおよびアカウントの属性に依存した詳細なアクセス制御までを統合的に実施する技術。</p> <p>（関連URL http://www.oracle.co.jp/9i/index.html）</p>

企業名（及び略称）	日本電気システム建設株式会社
代表者氏名	代表取締役社長 横山 清次郎
所在地（郵便番号及び住所）	〒140-8620 東京都品川区東品川一丁目39番9号
関連部署名及び電話番号	ネットワーク事業本部サービスソリューション開発本部サービス開発部 03-5463-7302
URL	http://www.nesic.co.jp/cyber/solution/product/iplocks/
対象技術	技術開発状況
その他認証技術	<p>弊社は米国 I P L O C K S社が開発した IPLocks-DAS のポリシーAPI、UDRカスタマイズ及び販売、技術サポート、保守サービスを行います。</p> <p>IPLocks-DASは、データベースの正常性(データ内容、構造、アクセス権)を監視・監査するシステムです。DBを擬似リアルタイムで監視することで、ファイアウォールの機能しないネットワーク内部でのDB改竄、誤操作、紛失、重複を即座に警告し、システム復旧時間の大幅短縮、損失セーブに貢献します。</p> <p>また、特許申請中の学習機能を搭載し、データ変更の正常、異常をより正確に判断できるようになります。</p>

企業名（及び略称）	株式会社ネットコム
代表者氏名	閻 躍軍
所在地（郵便番号及び住所）	〒111-0036 東京都台東区松が谷 4 丁目 24 番 3 号 藤ビル 3F
関連部署名及び電話番号	張 書明 大崎雄介 陳 海波 03-5827-0588
URL	http://www.netcome.co.jp/
対象技術	技術開発状況
侵入検知技術	<p>ホームページ改ざん防止技術「Cobra Homepage Gaurd」</p> <p>不正アクセス行為で最も多くの被害を受けているウェブサイトにおいて、掲載情報が有意味情報へ改ざんされることを防止し、被害を最小限に抑える。</p> <ol style="list-style-type: none"> 1. Firewall 外の Web サーバ上には、暗号化されたコンテンツを置き、ユーザのアクセス要求に対して都度データを複合化、送信する。 2. クラッカーが直接ファイルを変更すると、複数の方法で検知し、VPN 経由でバックアップのサーバから正常なファイルを転送する。およそ 1 秒程度で元の状態に戻すと同時に、管理者へ SMS などと通知する。 <p>基礎技術になっている Cobra 暗号は、カオス理論を使用した暗号の中でも最先端のもの。従来の方式に比べて遥かに暗号化/復号化の処理速度が速いほか、処理の前後でファイルサイズを変更させないことが可能になるなど、今後一層の大容量化が進むデジタル・コンテンツ配信にも、十分に対応できる暗号方式。携帯電話などでの組み込み利用も可能。</p>

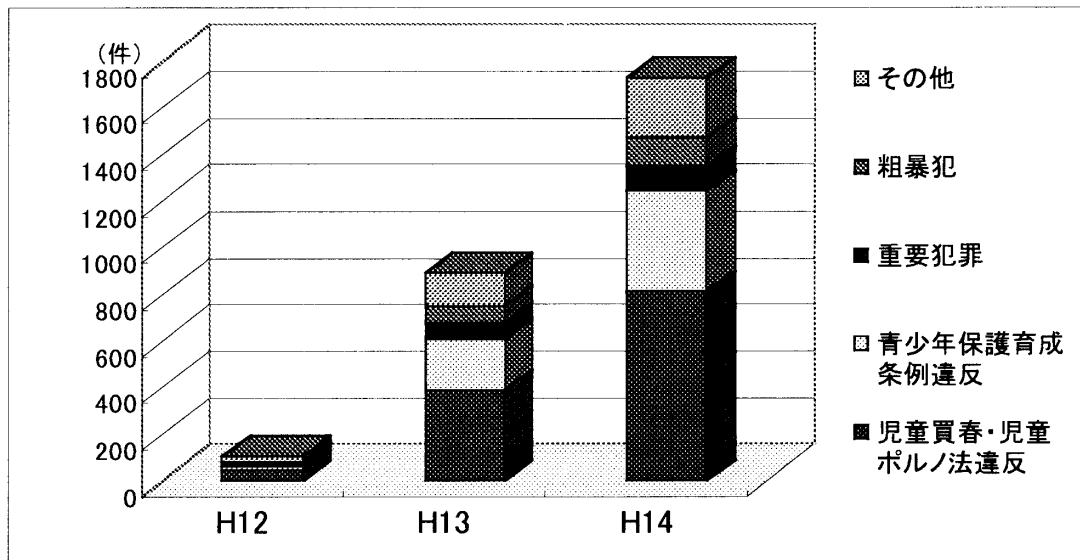
企業名（及び略称）	富士ゼロックス株式会社
代表者氏名	有馬 利男
所在地（郵便番号及び住所）	〒164-0012 東京都港区赤坂二丁目 17 番 22 号 赤坂ツインタワー東館
関連部署名及び電話番号	NBC beat 事業部（03-5352-7536）
URL	http://www.net-beat.com/
対象技術	技術開発状況
ファイアウォール技術 （平成 13 年開発） その他認証技術 （平成 14 年開発） その他認証技術 （平成 13、14 年開発）	<p>インターネットデータセンタにおける WWW およびメールサービスを前提とし、メール送受信、ホームページ公開、WWW 参照などの一般的なインターネット利用を可能としつつ、外部からのすべてのアクセス（内部からのアクセスのレスポンスを除く）を受け付けないことによる、原理的に耐性の高い不正アクセス防止技術</p> <p>インターネット上の制御サーバが VPN を確立すべきホストを認証し、制御サーバの指示に従って特定の他ホストからの VPN 確立要求のみを許可することにより、不正アクセスへの耐性を高めた VPN 技術</p> <p>あるネットワーク領域内（たとえば社内）にもメールサービスを稼働させて配信経路を制御することにより、当該領域内宛のインターネットメールをインターネットを経由せずに、もしくは VPN を経由して配信することにより、当該領域外への情報漏洩を防止する技術</p>

企業名（及び略称）	株式会社ランデック
代表者氏名	鬼頭 行夫
所在地（郵便番号及び住所）	〒456-0032 名古屋市熱田区三本松町 15-13
関連部署名及び電話番号	システム開発部 052-889-1472
URL	http://www.landec.co.jp/Web-acuman/Web-acuman.htm
対象技術	技術開発状況
侵入検知技術 (2002年1月開発)	<p>Web-Server・Home Page-Server などにハッカーなどが不正進入し、内部データを改ざんする不正行為を監視・復旧・稼動報告する技術。</p> <p>〔技術公開〕</p> <ol style="list-style-type: none"> ① Web-Server などのファイルを改ざんしたログを記録。 ② Web-Server の改ざんされた部分を修復。 ③ Web-Server の改ざん・復旧ログを指定メール送信。 ④ Web-Server にアタックしたグローバル IP アドレスの分析内容報告をメール添付ファイル送信。 (アタック回数・アタックインターバルなど) ⑤ IIS・Apache プログラムの再起動。(定期リフレッシュ) ⑥ Windows・Linux OS などのコンパクト化も研究実現。 <p>以上の特記機能を有した“侵入検知技術”は、当社の研究活動により Web-Server 稼動状況が目に見えるテクノロジーの実現に近づける。</p>

平成14年中のいわゆる出会い系サイトに関係した事件の検挙状況について

1 出会い系サイトに関係した事件の検挙数

※対象は、インターネット上で異性間の出会いの場を提供する電子掲示板、チャット等のいわゆる出会い系サイトが関係した事件として警察庁に報告のあったもの。



	H12	H13	H14	前年比
児童買春・児童ポルノ法違反	41	387	813	2.1倍
青少年保護育成条例違反	20	221	435	2.0倍
重要犯罪（殺人・強盗・強姦等）	15	73	100	1.4倍
粗暴犯（暴行・傷害・脅迫・恐喝）	7	66	128	1.9倍
その他（児童福祉法違反等）	21	141	255	1.8倍
計	104	888	1,731	1.9倍

(件)

2 特徴

- いわゆる出会い系サイトに関係した事件の検挙数は、前年と比べて約1.9倍に増加。
- 児童買春・児童ポルノ法違反は813件（全体の約47%）で前年と比べて約2.1倍、青少年保護育成条例違反は435件（全体の約25%）で前年と比べて約2.0倍にそれぞれ増加。両者で全体の約72%を占める。
- 全事件のうち、携帯電話を使用したものが平成12年は59件（約57%）、13年は714件（約80%）、14年は1,672件（約97%）と年々増加。
- 被害者1,517人のうち、18歳未満の児童が1,273人（約84%）で大半を占める。
- 検挙された被疑者に占める少年の割合が、平成12年は10人（約11%）、13年は110人（約13%）、14年は297人（約20%）と年々増加。

出会い系サイトに関係した事件検挙事例

【殺人】

携帯電話の出会い系サイトで知り合った女性から金をだまし取ったものの、詐欺事実が発覚するのを免れるため、女性を殺害した。（平成14年3月検挙・鳥取）

【強盗】

携帯電話の出会い系サイトに書き込みをしていた被害男性に対して、女性を装って「一緒に遊びませんか。」などとメールで誘い出し、包丁を突きつけて脅し、現金と携帯電話を奪った。（平成14年11月検挙・岡山）

【逮捕監禁・強盗】

携帯電話の出会い系サイトを使って呼び出した男性を車に乗せて連れ回した上、金属バットで殴るなどして、消費者金融から現金を借りさせ、その金を奪った。（平成14年8月検挙・大阪）

【強姦】

携帯電話の出会い系サイトで知り合った女性をホテルに連れ込み、カッターナイフを突きつけて強姦した。（平成14年2月検挙・埼玉）

【わいせつ目的誘拐】

携帯電話の出会い系サイトで知り合った小学6年の女子を誘い出し、ホテルでわいせつな行為をした。（平成14年12月検挙・京都）

【強制わいせつ】

携帯電話の出会い系サイトで「車で送ってくれる人を探している」等と書き込んだ女性とメール交換の上、待ち合わせ場所を指定して誘い出し、わいせつな行為をした。（平成14年4月検挙・鹿児島）

【傷害】

携帯電話の出会い系サイトで知り合った女性から別れ話をされたことに腹を立て、女性に殴る蹴るなどの暴行を加え傷害を負わせた。（平成14年5月検挙・福岡）

【恐喝】

少年を含む被疑者5人は共謀の上、携帯電話の出会い系サイトを利用して美人局を企て、男性をホテルに誘い出し、現金を脅し取った。（平成14年12月検挙・新潟）

【脅迫】

インターネットの出会い系サイトで中学生を装い、知り合いとなった女子中学生に裸体の写真を送信させた上、「交際しなければ写真をばらす」等と脅迫メールを送った。
(平成14年3月検挙・警視庁)

【詐欺】

携帯電話の出会い系サイトの掲示板に「お願い助けて」等と金の援助を求める書き込みを行い、これを閲覧してメール送信してきた男性から現金20万円を自分名義の口座に振り込ませてだまし取った。
(平成14年3月検挙・茨城)

【児童買春・児童ポルノ法違反】

携帯電話の出会い系サイトで書き込みをした女子中学生に「エッチなバイトで稼がないか。」等とメール送信して誘い出し、児童買春をした。
(平成14年9月検挙・埼玉)

携帯電話の出会い系サイトにモデル募集の広告を掲載し、応募してきた無職の女性(16歳)と性交類似行為をし、その行為をデジタルカメラで撮影するなどして児童ポルノを製造した。
(平成14年5月検挙・和歌山)

【青少年保護育成条例違反】

携帯電話の出会い系サイトに「中3メル友募集」等の書き込みをした女子中学生と知り合い、みだらな性行為をした。
(平成14年3月検挙・宮城)

【名誉毀損】

インターネット上の出会い系サイトの掲示板に被害者の女性の自宅住所、電話番号を書き込んだ上、あたかも不倫を願望しているかのような内容を掲載し名誉を毀損した。
(平成14年5月検挙・警視庁)

【売春防止法違反】

女子高校生を含む3人が、女子中学生に対して暴行を加えた後、「援助交際して金を持ってこい。」などと脅し、携帯電話の出会い系サイトを使って勧誘した男を引き合わせて売春させ、その金を受け取った。
(平成14年10月検挙・徳島)

出会い系サイトに関係した事件の検挙数等

罪 種		年		平成13年	平成12年
		平成14年	前年比		
重 要 犯 罪	殺 人	6	0	6	1
	強 盗	24	14	10	2
	強 姦	53	9	44	8
	略取誘拐	3	0	3	1
	強制わいせつ	14	4	10	3
暴 行		3	0	3	1
傷 害		18	5	13	0
脅 迫		24	8	16	2
恐 喝		83	49	34	4
窃 盗		39	16	23	0
詐 欺		25	1	26	1
児童買春・児童	児童買春	787	408	379	40
ポルノ法違反	児童ポルノ	26	18	8	1
青少年保護育成条例違反		435	214	221	20
そ の 他		191	99	92	20
合 計		1,731	843	888	104

※ 対象は、インターネット上で異性間の出会いの場を提供する電子掲示板、チャット等のいわゆる出会い系サイトが関係した事件として警察庁に報告のあったもの。

【携帯電話・パソコン別】

区 分	件 数(構成比)	携帯電話を使用した事件が増加傾向 (構成比) H 1 2 5 9 件 (約57%) H 1 3 7 1 4 件 (約80%) H 1 4 1, 6 7 2 件 (約97%)
携帯電話	1, 6 7 2 (97%)	
パソコン	5 9 (3%)	
計	1, 7 3 1	

【被害者のうち児童、女性の数の推移】

	被害者数	児 童		女 性
			女 性	
平成12年	1 0 2	71 (70%)	68(67%)	96 (94%)
平成13年	7 5 7	584 (77%)	574(76%)	699 (92%)
平成14年	1, 5 1 7	1,273 (84%)	1,255(83%)	1,398 (92%)

※児童とは、18歳未満の者をいう。

※ () は被害者数に対する構成比

【被害者のうち未成年、高校生、中学生の数】

	女 性	男 性	計
未 成 年	1, 2 8 6 (85%)	3 1 (2%)	1, 3 1 7 (87%)
高 校 生	6 8 6 (45%)	1 2 (0.8%)	6 9 8 (46%)
中 学 生	3 6 4 (24%)	3 (0.2%)	3 6 7 (24%)

※未成年とは、20歳未満の者をいう。

※ () は被害者1, 5 1 7人に対する構成比

我が国におけるインターネット治安情勢の分析について

1 概要

- サイバーフォースセンターの 24 時間監視体制
 - － 全国の警察施設に対するサイバー攻撃の監視
- インターネット治安情勢を分析
 - － 平成 14 年度第 2 / 四半期分のデータによる
- 我が国初の情勢分析
 - － この種の統計に基づく分析は今までなかった

2 分析結果に見る特徴

- 発信元はイタリア、米国、中国、韓国の順が多い。(別添 1)
- 攻撃手法にも国別特徴。(別添 2)
- 攻撃件数は日々激変。(別添 3)
- 約 1 割が侵入やサービス妨害を意図。(別添 4)
- クラッカーも未明には眠る？(別添 5)

3 分析結果の活用

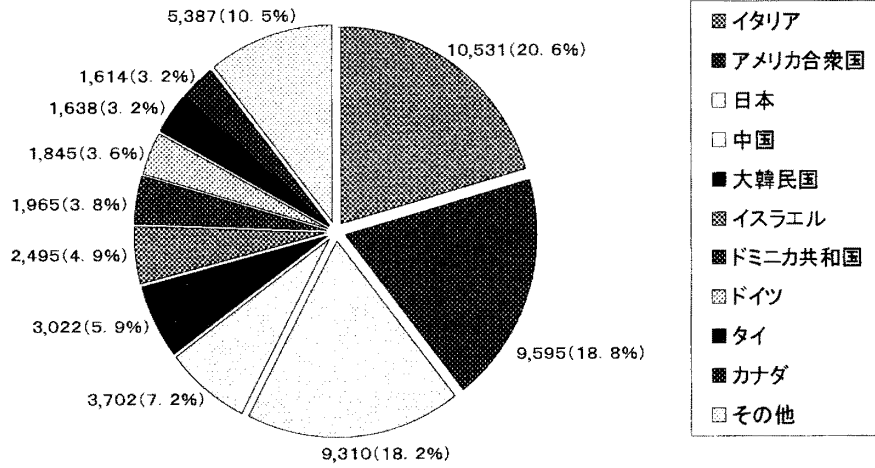
- 国民への啓発
 - ・ 警察庁 HP を利用したセキュリティ意識の高揚
- 重要インフラとの連携強化
 - ・ サイバーテロ防御の推進
- 諸外国との連携強化
 - ・ 各国法執行機関との情報交換・共有

4 今後の施策

- さらにタイムリーで詳細な情報提供
 - ・ 警察庁セキュリティポータルサイト(平成 15 年 3 月運用開始予定)への掲載
- 分析手法についての継続的な調査研究
- 情報の価値の高度化
 - ・ 産官学の情報共有の促進(重要インフラ、内閣官房、大学等)

(以上)

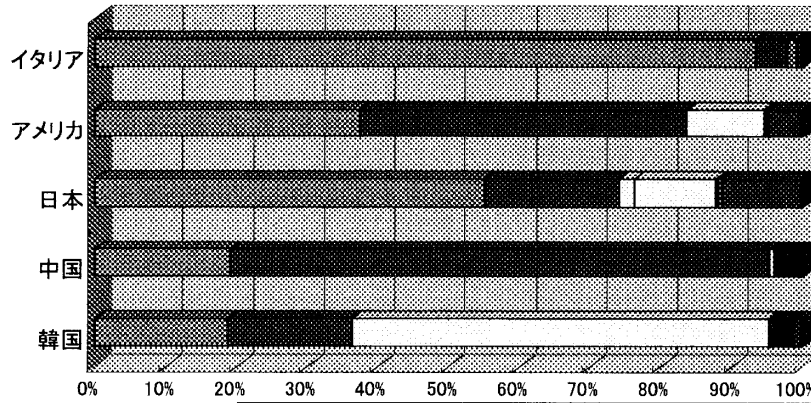
攻撃の発信元の国別分析



※発信元が必ずしも攻撃元とは限らない

国別攻撃手法

別添2

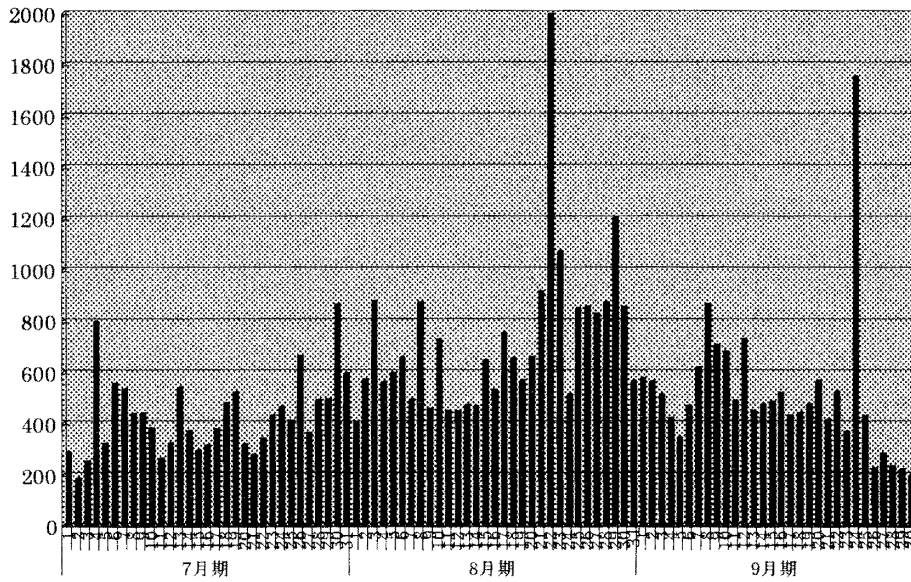


	Ping攻撃	ポートスキャン	バックドア接続要求	DNSへの攻撃	Webサーバへの攻撃	DoS攻撃	その他	合計
イタリア	9,837 93.4%	476 4.5%	0 0.0%	0 0.0%	3 0.0%	143 1.4%	72 0.7%	10,531 100.0%
アメリカ	3,598 37.5%	4,429 46.2%	1,050 10.9%	0 0.0%	50 0.5%	12 0.1%	456 4.8%	9,595 100.0%
日本	5,145 55.3%	1,761 18.9%	206 2.2%	1,074 11.5%	19 0.2%	51 0.5%	1,054 11.3%	9,310 100.0%
中国	713 19.3%	2,819 76.1%	24 0.6%	0 0.0%	122 3.3%	9 0.2%	15 0.4%	3,702 100.0%
韓国	566 18.7%	532 17.6%	1,783 59.0%	6 0.2%	97 3.2%	6 0.2%	32 1.1%	3,022 100.0%

※発信元が必ずしも攻撃元とは限らない

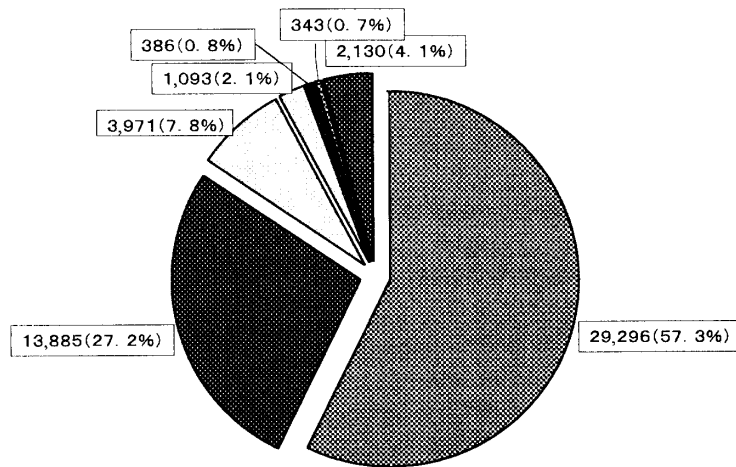
攻撃状況の推移

別添3



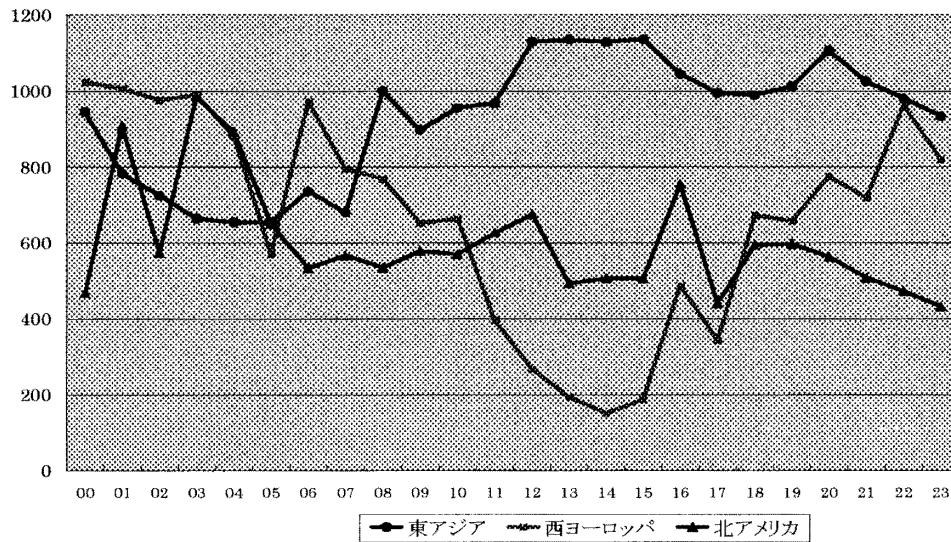
攻撃手法による分析

別添4



- | | |
|--------------|-------------------------|
| ■ Ping攻撃 | ■ ポートスキャン(サーバ使用サービスの確認) |
| □ バックドア接続要求 | □ DNSへの攻撃 |
| ■ Webサーバへの攻撃 | ■ DoS攻撃 |
| ■ その他 | |

地域別の攻撃の時間的推移 別添5



我が国におけるインターネット治安情勢の分析について (平成14年度第3/四半期)

1 概要

- サイバーフォースセンターの24時間監視体制
 - － 全国の警察施設に対するサイバー攻撃の監視
- インターネット治安情勢を分析
 - － 平成14年度第3/四半期分のデータによる

2 分析結果に見る特徴

- 発信元はイスラエル、米国、日本、韓国の順が多い。(別添1)
 - － 第2/四半期トップのイタリアは、約4%にとどまる
- 攻撃手法にも国別特徴。(別添2)
 - － 第2/四半期と同様、発信元からの攻撃手法に国別特徴がみられる
- 攻撃件数は日々激変。(別添3)
 - － 攻撃件数は、第2/四半期より14%増加して、約58,000件
- 約1割が侵入やサービス妨害を意図。(別添4)
 - － 侵入やサービス妨害を意図した攻撃は、第2/四半期と同じく約1割

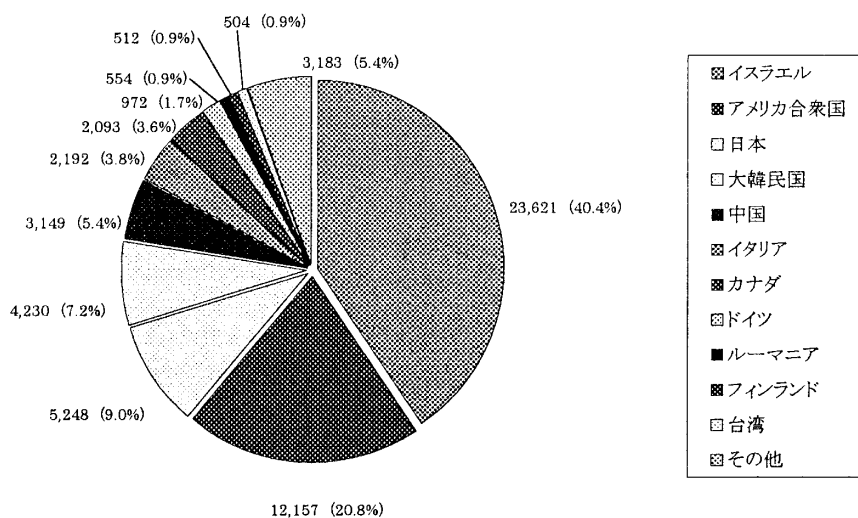
3 分析結果の活用

- 国民への啓発
 - － 警察庁ホームページを利用したセキュリティ意識の高揚
- 重要インフラ事業者との連携強化
 - － サイバーテロ防御の推進
- 諸外国との連携強化
 - － 各国法執行機関との情報交換・共有

(以上)

攻撃の発信元の国別分析

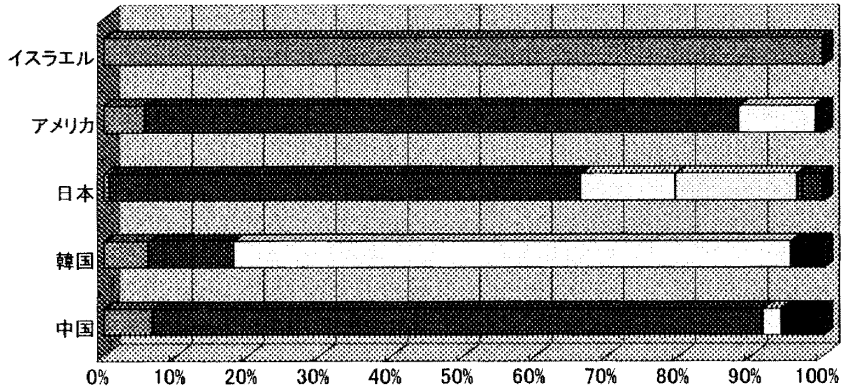
別添1



※発信元が必ずしも攻撃元とは限らない

国別攻撃手法

別添2



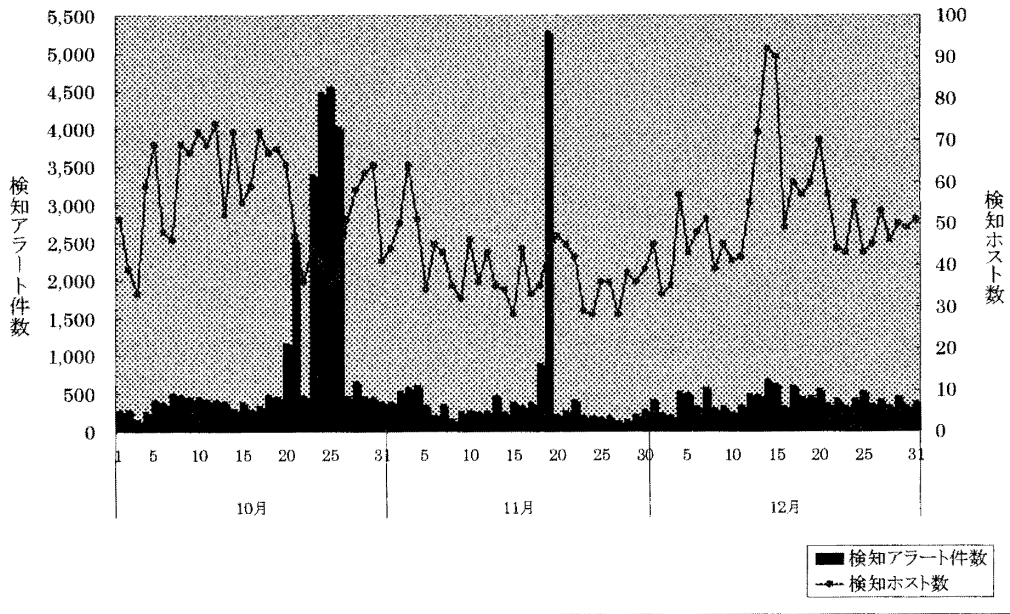
- Ping攻撃
- ポートスキャン
- バックドアへの接続要求
- DNSへの攻撃
- Webサーバへの攻撃
- DoS攻撃
- その他

	Ping攻撃	ポート スキャン	バックドア接 続要求	DNS への攻撃	Webサーバ への攻撃	DoS攻撃	その他	合 計
イスラエル	23,600 99.9%	6 0.0%	10 0.0%	0 0.0%	0 0.0%	0 0.0%	5 0.0%	23,621 100.0%
アメリカ	688 5.7%	10,046 82.7%	1,297 10.7%	0 0.0%	81 0.7%	4 0.0%	39 0.3%	12,157 100.0%
日本	44 0.8%	3,435 65.5%	695 13.2%	866 16.9%	10 0.2%	23 0.4%	155 3.0%	5,248 100.0%
韓国	263 6.2%	503 11.9%	3,274 77.4%	0 0.0%	164 4.4%	6 0.1%	0 0.0%	4,230 100.0%
中国	211 6.7%	2,675 85.0%	80 2.5%	0 0.0%	174 5.5%	9 0.3%	0 0.0%	3,149 100.0%

※発信元が必ずしも攻撃元とは限らない

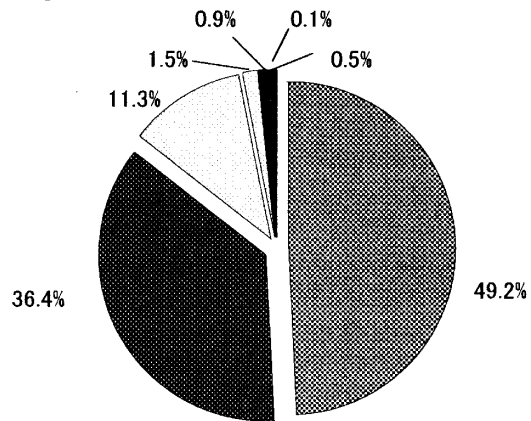
攻撃状況の推移

別添3



攻撃手法による分析

別添4



- | | |
|--------------|-------------------------|
| ■ Ping攻撃 | ■ ポートスキャン(サーバ使用サービスの確認) |
| □ バックドア接続要求 | □ DNSへの攻撃 |
| ■ Webサーバへの攻撃 | ■ DoS攻撃 |
| ■ その他 | |

我が国におけるインターネット治安情勢の分析について
(平成14年度第4/四半期)

1 概要

- サイバーフォースセンターの24時間監視体制
 - － 全国の警察施設に対するサイバー攻撃の監視
- インターネット治安情勢を分析
 - － 平成14年度第4/四半期分のデータによる

2 分析結果に見る特徴

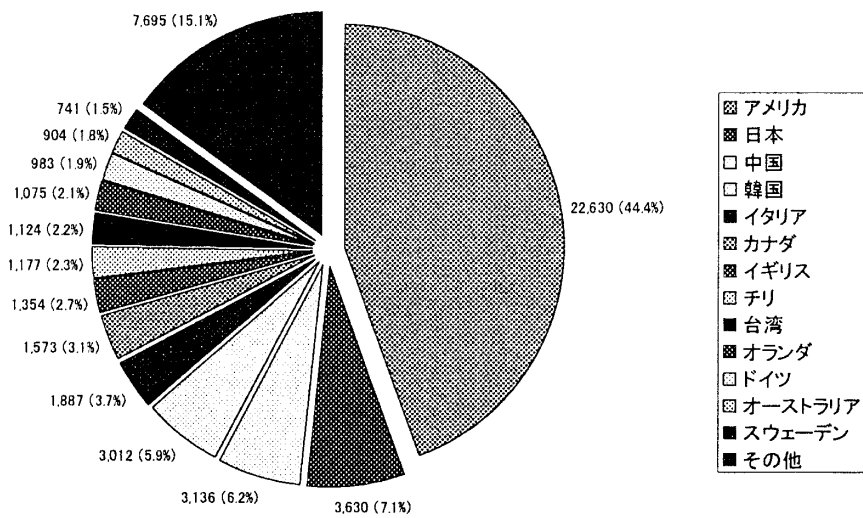
- 発信元は米国、日本、中国、韓国の順が多い(別添1)
- 攻撃手法にも国別特徴(別添2)
 - － 発信元からの攻撃手法に国別特徴がみられる
- 攻撃件数は日々激変(別添3)
 - － 攻撃件数は、前四半期より13%減少、約51,000件
- 依然、活動するSlammerワーム(別添4)
 - － 攻撃の約43%がSlammerワーム

3 分析結果の活用

- 国民への啓発
 - － 警察庁セキュリティポータルサイト(平成15年3月1日開設・愛称「@police」)を利用したセキュリティ意識の高揚
- 重要インフラ事業者との連携強化
 - － サイバー攻撃に対する防御の推進
- 諸外国との連携強化
 - － サイバー犯罪技術情報ネットワークシステム(CTINS)等を通じた各国法執行機関との情報交換・共有
- 官学の連携強化
 - － 共同研究の推進

攻撃の発信元の国別分析

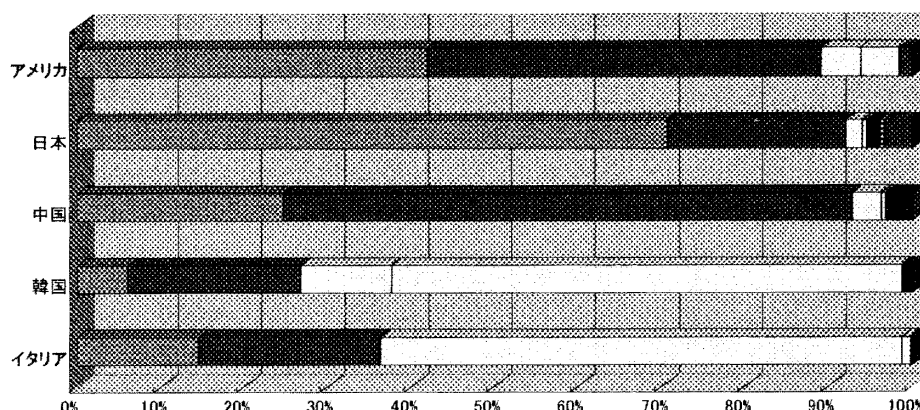
別添1



※発信元が必ずしも攻撃元とは限らない

国別攻撃手法

別添2



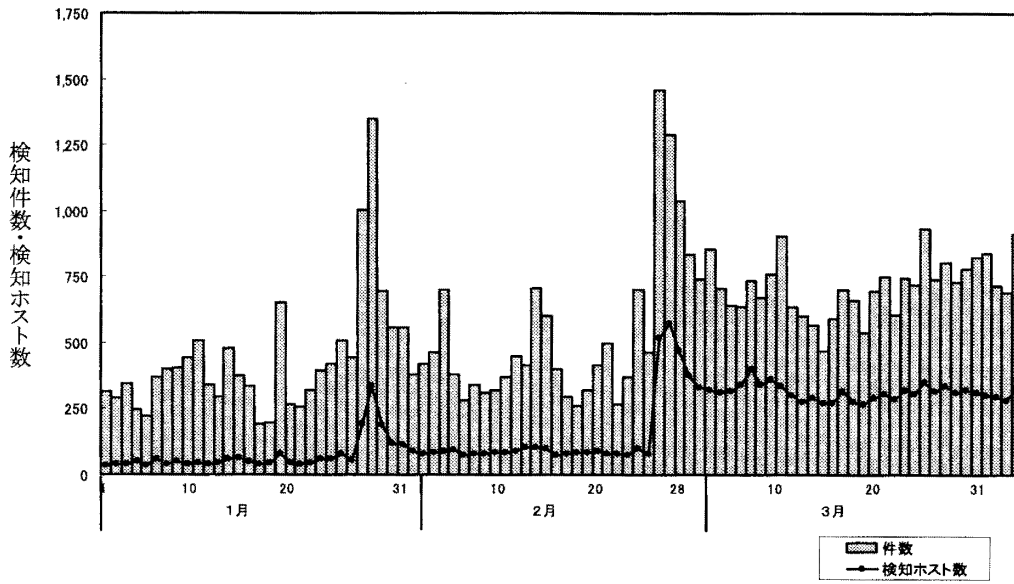
- ワーム
- ポートスキャン
- Ping攻撃
- バックドア接続要求
- Webサーバへの攻撃
- DoS攻撃
- その他

国	ワーム	ポートスキャン	Ping攻撃	バックドア接続要求	Webサーバへの攻撃	DoS攻撃	その他	合計
アメリカ	9499 42.0%	10651 47.1%	1089 4.8%	1050 4.6%	10 0.0%	7 0.0%	324 1.4%	22630
日本	2571 70.8%	770 21.2%	72 2.0%	21 0.6%	55 1.5%	20 0.6%	121 3.3%	3630
中国	776 24.7%	2135 68.1%	111 3.5%	16 0.5%	91 2.9%	7 0.2%	0.0%	3136
韓国	182 6.0%	625 20.8%	326 10.8%	1840 61.1%	33 1.1%	3 0.1%	3 0.1%	3012
イタリア	275 14.6%	411 21.8%	1178 62.4%	19 1.0%	0.0%	2 0.1%	2 0.1%	1887

※発信元が必ずしも攻撃元とは限らない

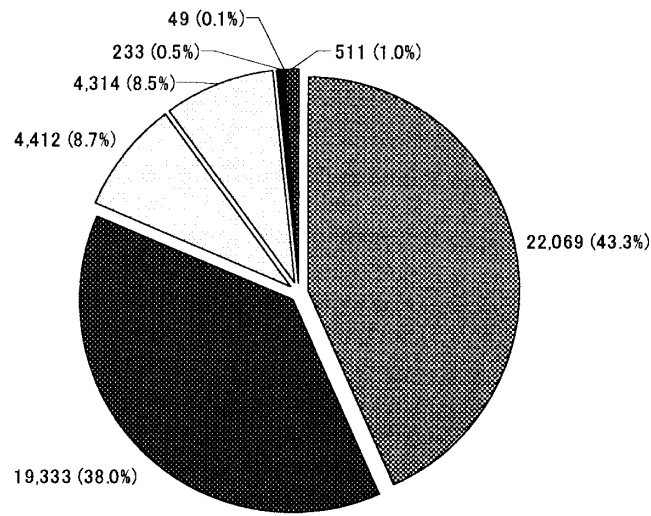
攻撃状況の推移

別添3



攻撃手法による分析

別添4



☒ ワーム ■ ポートスキャン □ Ping攻撃 □ バックドア接続要求 ■ Webサーバへの攻撃 ☒ DoS攻撃 ■ その他



**社会における
情報セキュリティ対策について**

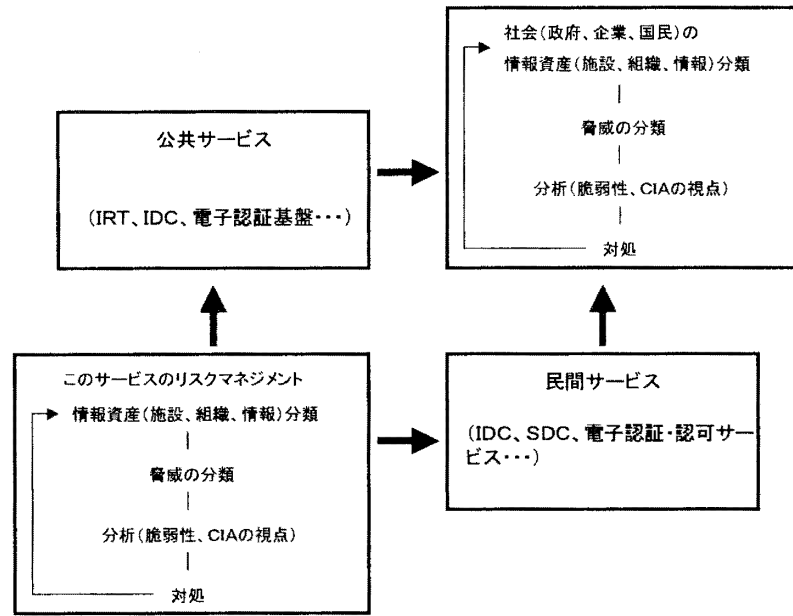
セコムトラストネット株式会社

代表取締役社長 田尾 陽一



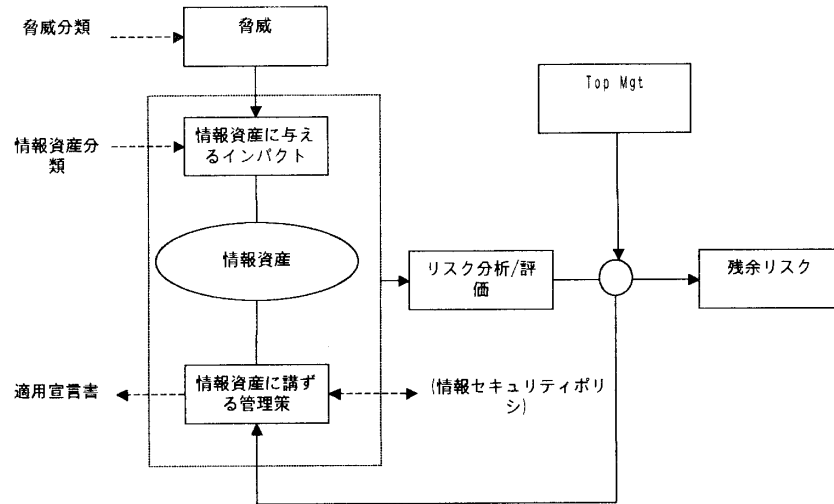


社会のリスクマネジメント





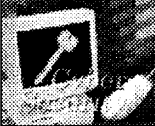
リスク分析の概念的フレームワーク





BS7799ガイドラインのリスク分析方法

		リスクアセスメントの実施内容
1	資産の識別及び査定	(1) ISMS適用範囲の資産のリストアップ (2) CIA+ごとに定義された尺度に基づき資産を評価
2	脅威のアセスメント	(1) 資産に関連した脅威のリストアップ (2) 発生の可能性及び厳しさに従って脅威に値を割り付け
3	脆弱性のアセスメント	(1) 資産に関連した脆弱性をリストアップ (2) 脆弱性を識別し、発生の可能性及び厳しさに従って脅威に値を割り付け
4	既存及び計画されたセキュリティ管理策の識別	(1) 以前のセキュリティレビューに従って、資産リストに関連した既存の管理策/計画された管理策をすべて識別し文書化
5	リスクアセスメント	(1) 上記のアセスメントの結果として、資産、脅威、脆弱性の情報を統合し、リスクを査定
6	セキュリティ管理策の識別及び選択並びにリスクの低減	(1) 資産のそれぞれについて、詳細管理策のなかの管理目的を識別 (2) 脅威と脆弱性から詳細管理策を選択 (3) それによってリスクがどれだけ低減したかを評価
7	リスクの許容	(1) 許容可能か不能かを識別 (2) 許容不能のリスク低減策の再検討



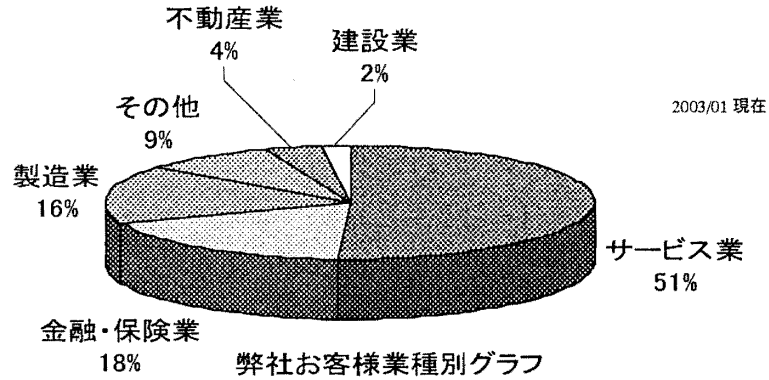
脅威の分類

	分類	脅威
1	災害	地震、水災、風害、雷害、塩害、火災、 塵埃、電磁波・静電気、小動物、 公共インフラ停止（電力、ガス、水道、通信、交通）
2	災害(テロなど)	テロ・脅迫、物理的破壊
3	故障・障害	空調故障、電源故障、 ネットワーク故障、ハードウェア故障、ソフトウェア故障、 過負荷、輻輳、伝送エラー
4	無権限(不正)	施設への侵入、ネットワークへの不正アクセス、 システムへの不正アクセス、情報への不正アクセス、 不正プログラム、なりすまし、通信傍受、 機材・ソフトの持出し盗難、機密情報の持出し、 施設設備の無許可使用、ハードの無許可使用、 ソフトの無許可使用
5	過失	資源の誤用、メンテナンスエラー、入力ミス、操作ミス
6	準拠違反(法、ポリシー)	関連法規違反、不法コピー、セキュリティポリシー違反
7	要員	労働争議、欠員(健康障害)



不正アクセスの現状

不正侵入検知サービスの導入状況



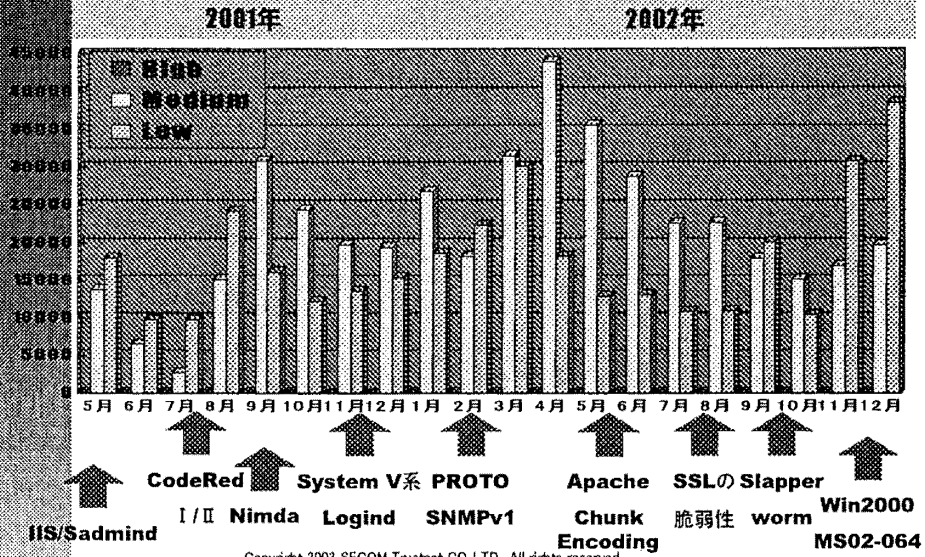
不正侵入検知サービスの導入はネットワークセキュリティに対する意識が高い一部の企業への導入に止まっているが、潜在需要的なニーズは高いと考えられる。

今後は、不正アクセス手段の巧妙化や24時間監視が必要になることで、インターネット環境が整っているあらゆる企業での需要が見込まれる。



不正アクセスの現状

1センサー(サイト)あたりの月間不正アクセス平均値





不正アクセスの現状

Slapper ワームに関して ①

2002年 6月 24日

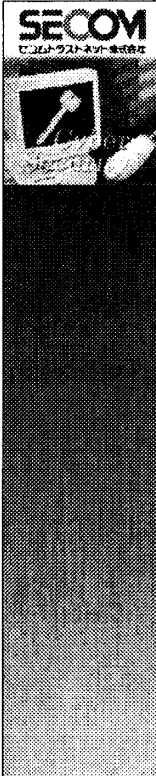
SSLの脆弱性がCERTから報告 (CERT Advisory CA-2002-18)

- SSLの鍵交換プロセスで、オーバーフローが発生
- オーバーフローが発生することにより、遠隔から管理者権限の取得が可能である

2002年 9月 17日

Slapper ワームの出現をCERTが報告 (CERT Advisory CA-2002-23)

- 6月24日に報告されたSSLの脆弱性を利用
- Linux サーバを対象に感染活動をするワーム
- 拡散型サービス不能攻撃を可能とするバックドアを用意



不正アクセスの現状

Slapper ワームに関して ②

セコムトラストネットでは

ワームのソースと検証ツールを入手し、ワームの実態の調査と影響を解析

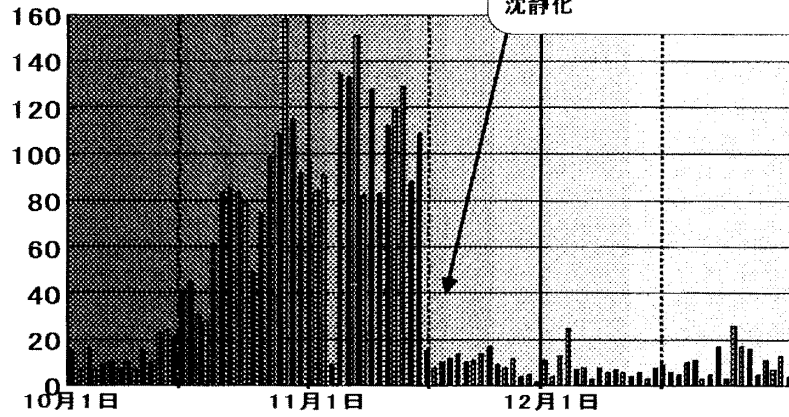
- 検証環境で**OpenSSL**が稼動する**www**サーバ(**Linux**)を、リモートから取得成功。
- 同時に対策(**OpenSSL**のバージョンアップ)の有効性を確認
- **2002年10月**にセンサーによる検出が可能となった
- お客様に**Slapper**ワームに関するアナウンス



不正アクセスの現状

Slapper ワームに関して③

ワームの活動 (2002年10月～12月)

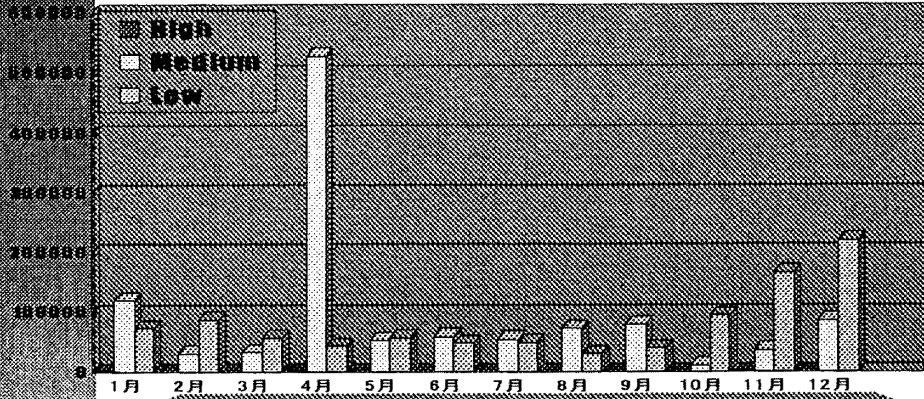


Slapper ワームは特定サイトで大量発生したため、このサイトで対策されたために、急激に沈静化



不正アクセスの現状

A社(サイト)2002年度の不正アクセス数の推移



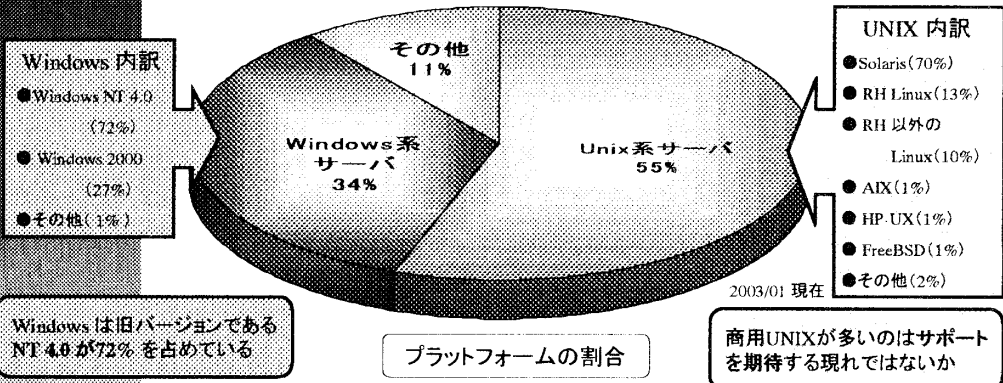
不正アクセスはセキュリティインシデント(セキュリティホールの報告やワームの出現など)によりダイナミックに変動する。つまり全く不正アクセスの影響のないサイトはあり得ない。



不正アクセスの現状

セキュリティ診断の実績

サーバ診断は、割合としてUNIXとWindowsが多くを占める。
 その他はファイヤーウォールやルータである。



Windows は旧バージョンである NT 4.0 が72% を占めている

プラットフォームの割合

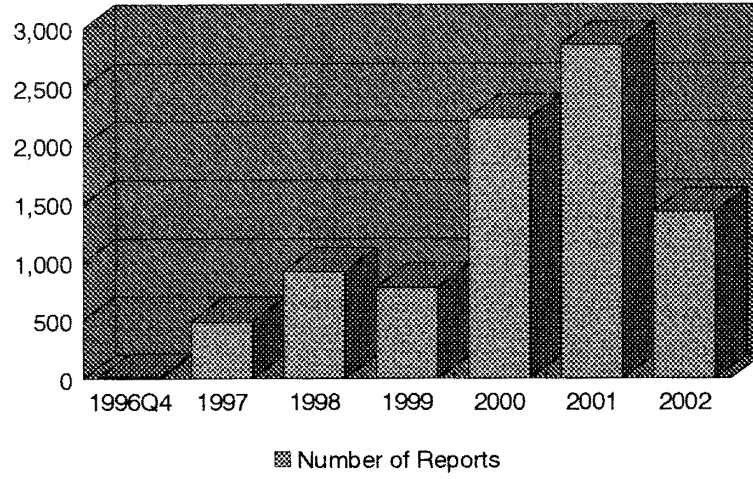
商用UNIXが多いのはサポートを期待する現れではないか

情報セキュリティに関する脅威について

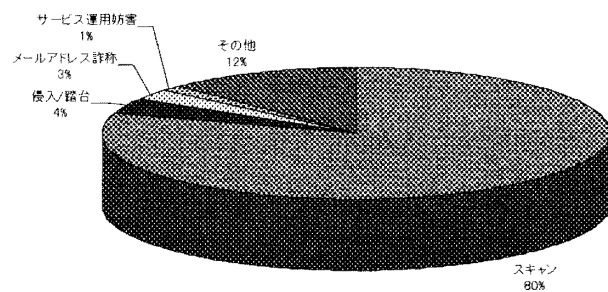
山口 英

奈良先端科学技術大学院大学

Statistics@JPCERT/CC



2002年JPCERT/CCが受け取った報告の分布



■ スキャン ■ 侵入/踏台 ■ メールアドレス詐称 ■ サービス運用妨害 ■ その他

最近の動向

- Port Scanning & Probe
 - ほぼ毎日発生.
 - 重大なセキュリティインシデント発生の前には必ず Port scanning が行われているので、その前兆行為として認識しておくべき
- 侵入
 - パスワードクラックによる直接侵入は以前として報告されている
 - ・ しかしながら、最近では使い捨てパスワードの利用や暗号化通信路の利用により、このような侵入は減りつつある
 - 通常はバッファオーバーフローの弱点を利用して、システムに "shell-code" を埋め込み、その実行を狙う
 - ・ サーバにバッファオーバーフローのバグがあると重大な脅威となる
 - ・ 現在流布されている多くの攻撃ツールが、この手法を利用
- Denial of Services (DoS)
 - 攻撃対象に対して大量のトラフィックを送りつけることによりサービス停止
 - 分散型DoSも広がりつつある
- SPAM
- ネットワーク伝搬型ウイルス

●不正侵入後

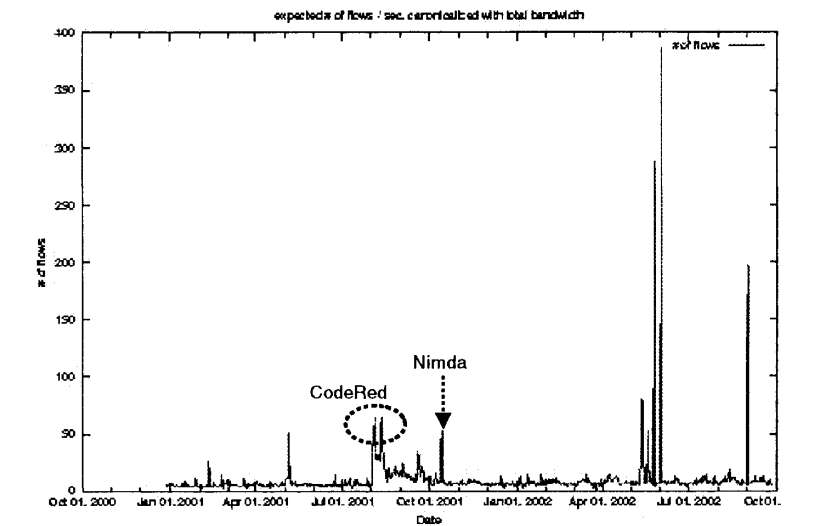
ルート権限を持つシェル、パスワードファイル改ざん
裏口、トロイの木馬、パケット盗聴プログラム
ログ改ざん、証拠隠滅

●ポートスキャン: Finger, TELNET, IMAP, POP, HTTP, NFS, DNS, X

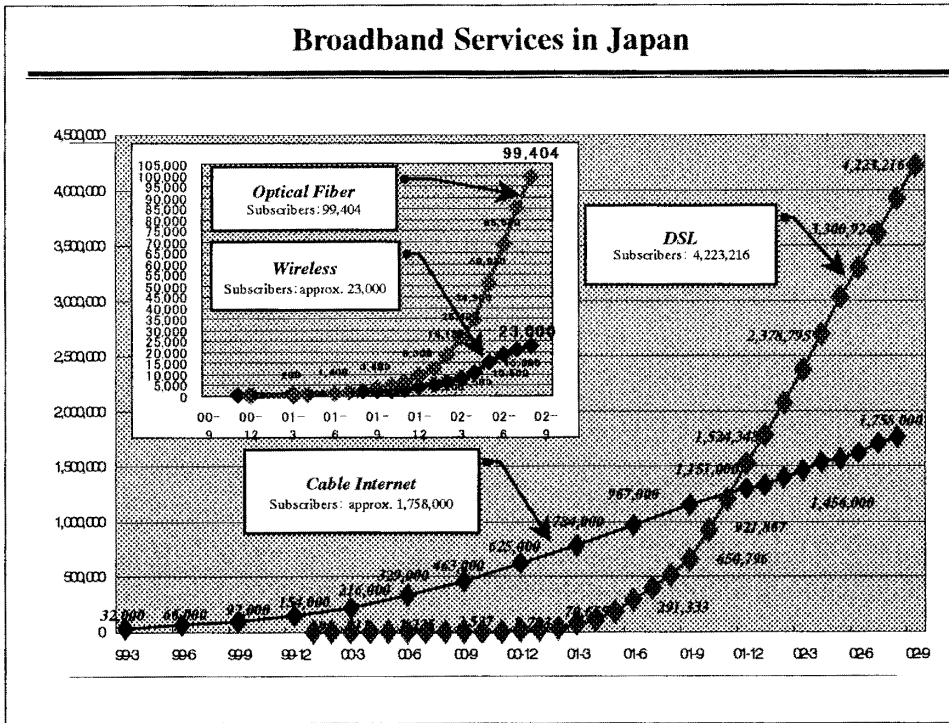
最近の攻撃の特徴

- 攻撃手法の高度化が著しい
 - 脆弱性情報が発表されてから48時間後に、当該脆弱性を利用した攻撃が観測されている
 - 攻撃ツールの開発と交換
 - 攻撃ツールを開発するユーザが増えている
 - ツールはインターネット上で交換される
 - 攻撃のための情報交換が積極的に行われている
 - bugtraq
 - 特定のWWWサイトやIRCチャンネル(アングラ系)
 - アマチュアとはいえレベルのツールが多い
 - 実質的に被害を与えることができるシステムが増えてきている
 - インターネットでの不正アクセスは「愉快犯」的なものが多いというのは、もはや嘘

実際のDoSトラヒック



Broadband Services in Japan



脅威分析の方向性(1)

- 技術的な視点からの体系化・分類
 - Network components (switches and protocols, etc.)
 - Computers
 - Software (applications and operating systems)

 - システムに対する被害インパクトに注目した分類
 - システム運用者・経営者に対して直接訴えかけるプライオリティ付け
 - 実務者にとって役立つ脅威分析

 - 司法機関にとっての分類
 - 犯罪行為と非犯罪行為
-

脅威分析の方向性(2)

- 内部者によるトラブル発生をどのように考えるのか

- 実は情報システムに対する最大の脅威は正規ユーザ
 - しかも犯罪行為に該当しないが、システムに対するインパクトは一番大きなものを引き起こす
 - 経済的損失も大きい、内部に隠蔽される

- ソフトウェアトラブルをどのように考えるのか

- バグによるシステム停止も実は大きな問題
 - 近年のシステム運用では、ソフトウェアトラブルは常に考えなければならない要素となっている
 - 犯罪行為でもないが、経済的損失は発生
 - ソフトウェアベンダの対応も限定的
-

まとめ

- JPCERT/CCの報告から

- トラブル発生件数は増加
- 技術的には高度化が著しい
- Port Scan / Intrusion / DoS / SPAM / Virus

- 脅威分析の方向性

- さまざまな視点が存在
 - 視点を混ぜて議論すると訳がわからないことに
 - 取り扱いにくい領域が存在
 - 内部者によるトラブル
 - ソフトウェア・バグ
 - そのほかも存在
-