H13－セキュリティWG－1

情報セキュリティにおける
新しい脅威と対応技術の動向

平成14年3月

電子商取引推進協議会

セキュリティWG

はじめに

近年、情報セキュリティが侵害されることによって様々な被害が引き起こされている。例えば、ウイルスやワームと呼ばれる有害プログラムはインターネットを介して蔓延しており、悪意のある者による EC サイトや官公庁などへの不正なアクセスによる被害についても、新聞等を通じて報道されている。

EC サイトは、このような脅威から自らを守り、利用者に対して安全で信頼できるサービスを提供することが必要であり、そのためには、脅威に対する知識を身につけ、脅威に対する技術動向を把握することが大切である。

EC サイトに対する脅威には、取引業者や消費者の悪意ある行動によるものや、災害により引き起こされるものなどもあるが、本報告書においては、特に EC サイト外部の第三者からの攻撃や EC サイト運用上の不手際によって引き起こされる脅威を中心とした脅威の分析および脅威に備えるための技術動向について調査を行い、その結果を報告する。

本報告書が、EC サイトの安全と信頼を守ることへの理解に繋がり、読者の皆様が携わる事業活動への一助となれば幸いである。

目次

1　脅威についての整理

1.1　不正アクセスによるネット被害

インターネットの利用者は、日本国内でも既に 2,000 万人を超え、企業内での利用や企業間での利用はもとより、インターネットを活用したビジネスや家庭からの利用も急増している。インターネット上で提供されるサービスについても、ショッピングやオークションをはじめ、インターネットバンキングや地方自治体からの各種情報提供など多くのサービスが出現し、インターネットは既に社会の構造の1つとして定着し始めているといえるだろう。

一方で、近年はインターネットに関連する事件が新聞や雑誌をかなり賑わすようになってきた。表 1-1に示されているのは 2000 年 4 月から 2001 年 12 月にかけて発生した主な事件である。ここに示されている事件は、ネット被害の中でもとりわけ事件性のあるものに限られており、被害規模の小さなものやウイルス／ワームによる被害の個々のケースまで合わせると、その被害規模はかなりのものであることが想像できる。

では、被害を引き起こす不正アクセスの推移はどうなっているのだろうか。図 1-1に示すのは、JPCERT/CC へ届出のあったインシデント報告件数の推移である。インシデントには、プローブやスキャン、その他不審なアクセス、サーバプログラムの不正中継、電子メールの送信ヘッダ詐称といった内容のものまでも含まれており、インシデント数から不正アクセスの件数を類推できるものではないが、少なくとも、2000 年に入ってから急激に不正アクセスが増加している傾向があることがわかる。

また、不正アクセスを引き起こす一因でもある情報システムの脆弱性についても、米国 SecurityFocus 社からの報告（図 1-2）にもあるように、脆弱性に関する報告件数は増え続けており、世の中の脆弱性についての関心が益々高まってきていることを示している。

表 1-1 2000 年 4 月以降の主なインターネット事件

（日経 BP 社「セキュリティ完全対策」をもとに加筆修正）

年月	内容	掲載先
2000年4月	検索サイト「goo」無料メールの設定情報流出	4/7 日本経済新聞
	宇宙事業団、迷惑メール2万7000通--サーバー不正使用される	4/8 日本経済新聞
	ヤフーやCNN攻撃、カナダの警察当局、少年ハッカーを逮捕--接続妨害した疑い	4/20 日本経済新聞
2000年5月	他人のパスワード利用、ネットゲーム仲間摘発--会社員と中2、不正アクセス容疑で	5/1 日本経済新聞
	「ラブ・ウイルス」、逮捕の比男性釈放--捜査令状取得に3日間、人も機器も消える	5/10 日本経済新聞
	警視庁、容疑で書類送検、他人にID盗み、高3ネット接続	5/22 日本経済新聞
2000年6月	ホームページ改ざん、地図大手のゼンリン、ハッカー進入し被害	6/6 日本経済新聞
	警察庁が捜査開始、「リキッド社」にハッカーが侵入	6/8 日本経済新聞
	他人のID盗みネットに接続、容疑の男逮捕	6/9 日本経済新聞
	「リキッド」不正アクセス、容疑の元役員逮捕--「自分の情報見たかった」	6/11 日本経済新聞
	ナイキにハッカー、貿易の自由化批判	6/22 日本経済新聞
2000年7月	ハッカー・ウイルス、今年は被害172兆円に--世界の大企業対象、米社が予測	7/8 日本経済新聞
	NASA電算機に侵入、容疑者を逮捕	7/13 日本経済新聞
2000年8月	他人のパスワードを使いネットに接続、大阪、容疑の男逮捕	8/3 日本経済新聞
	ネット犯罪摘発急増、上半期21件、詐欺目立つ	8/10 日本経済新聞
	禁止法施行後、不正アクセス被害、半年間で35件確認	8/31 日本経済新聞
2000年9月	生保会社メール、不正にアクセス、容疑の元社員を書類送検	9/11 日本経済新聞
	札幌地裁判決、ホームページ侵入、富山の会社員有罪	9/21 日本経済新聞
	京大研究所、ホームページ書き換えられる	9/26 日本経済新聞
2000年10月	マイクロソフトにハッカー、基本設計情報、盗難の可能性	10/28 日本経済新聞
	米マイクロソフト、ハッカー、開発中ソフト接触--改変や持ち出しは否定	10/28 日本経済新聞
2000年11月	「詐称メール」、大分大が困惑、ドメイン名を悪用	11/1 日本経済新聞
	ハッカー集団初摘発、ネットで侵入法伝授、容疑の3人逮捕	11/24 日本経済新聞
	ハッカー集団初摘発、容疑の3人逮捕--マニア「遊び感覚」で犯行	11/24 日本経済新聞
2000年12月	千葉県のホームページ、一部改ざんされる	12/1 日本経済新聞
	国家公安委ホームページ、女性写真入り「偽物」、本物へのアクセス妨害	12/10 日本経済新聞
	日韓友好のホームページ消去、容疑の男逮捕	12/12 日本経済新聞
	名古屋地検岡崎支部、ハッカー集団のリーダー格起訴	12/14 日本経済新聞
	ネット不正アクセス容疑、宮崎2少年書類送検	12/14 日本経済新聞
	広告メールを12万通不正転送、研究所のサーバー侵入	12/15 日本経済新聞
	解雇された会社のネット契約不正変更、容疑の男を逮捕	12/18 日本経済新聞
	東証のメール、ウイルス混入、会員8000人に配信	12/21 日本経済新聞
2001年1月	リーダー格、犯罪認める、集団ハッカー事件初公判--名古屋地裁支部	1/22 日本経済新聞
	マイクロソフトのサイト、また接続不能、今度はハッカー被害	1/26 日本経済新聞
	マイクロソフトが再びハッカー被害	1/27 日本経済新聞
	米マイクロソフト、サイト接続、再び不能に--今度はハッカーが攻撃	1/29 日経産業新聞
2001年2月	ダボス会議にハッカー、森首相やゲイツ、ソロス、アラファト氏、カード情報盗まれる	2/5 日本経済新聞
	不正アクセス被害、昨年、過去最多の143件、中継点に悪用多く--IPAまとめ	2/8 日経産業新聞
	昨年2－12月、不正アクセス27人逮捕--昨年、ネット犯罪摘発も倍増	2/10 日本経済新聞
	HPに中国語、改ざん被害70件、警察庁調べ	2/23 日本経済新聞
2001年3月	厚生労働省が被害、ホームページ一部改ざん	3/14 日本経済新聞
2001年5月	印パ、サイバー戦争ぼっ発、ハッカーグループが印外務省HPに侵入？	5/9 日本経済新聞
	東京都財団など、HP改ざん被害	5/9 日本経済新聞
	尼崎市のホームページ、一部改ざんされる	5/9 日本経済新聞
	米中サイバー戦争、終息の見通し、中国ハッカー「休戦」を宣言	5/12 日本経済新聞
	「米国ひぼう」にホームページ改ざん--甘い管理が被害拡大、知らぬ間に“共犯者“	5/18 日本経済新聞
2001年6月	不正アクセス2割が被害、昨年、企業や大学で--警察届け出は5.3%止まり	6/14 日本経済新聞
2001年7月	今年上半期、ウイルス届け出3倍、新種まん延9569件に	7/6 日経産業新聞
	わいせつ画像に、塾のHP改ざん、容疑の元職員逮捕	7/11 日本経済新聞
2001年8月	コード・レッド、さらに悪質「2」混じる--簡単に不正侵入	8/7 日経産業新聞
	新ウイルス「コード・レッド」、日本で数千台感染か、IPA指摘	8/7 日本経済新聞
	ネット犯罪58%増、詐欺、競売絡み目立つ--上半期まとめ	8/9 日本経済新聞
	電気通信事業法違反、電子メールに初適用、盗み見容疑の女送検	8/9 日本経済新聞
	気象庁のサイト改ざん、中国のハッカー犯行認める声明	8/15 日本経済新聞
	道議会HPまた攻撃、一斉接続障害なし	8/16 日本経済新聞
	文科省にウイルス、文書公開システム休止	8/17 日本経済新聞
	サイトに新手のハッカー侵入、接続したらパソコン故障--被害2500人超す	8/30 日本経済新聞
2001年9月	他人のID盗みHP侵入の疑い、38歳女性を逮捕	9/5 日本経済新聞
	コンピュータウイルス被害、不正アクセス件数も最悪	9/7 日経産業新聞
2001年10月	中小の7割、ネットで「脅威」、ウイルス被害3割--福井県産業支援センター調べ	10/10 日本経済新聞
	不正ネット接続、更に1人逮捕、計8容疑者に	10/18 日本経済新聞
	関空ホームページ改ざん、すでに復旧	10/22 日本経済新聞
2001年11月	東大阪市内の専門学校生、交際女性のパスワード再発行させ悪用	11/1 mainichi INTERACTIVE
	米のネット詐欺被害　総額・平均額とも昨年以上	11/8 mainichi INTERACTIVE
	他人のIDとパスワードを不正に利用、容疑者逮捕	11/8 mainichi INTERACTIVE
	法務省のメールサーバー　不正使用の可能性明らかに	11/15 mainichi INTERACTIVE
	ハッカー侵入、顧客のクレジット番号盗む　米プレイボーイ・コム	11/21 mainichi INTERACTIVE
	他人のHPに「裏ページ」　勝手に作成、送検	11/22 mainichi INTERACTIVE
2001年12月	キーボートの操作歴を記録するソフト利用し他人のID、パスワード盗み、商品代金騙し取る	12/19 mainichi INTERACTIVE
	就職内定辞退の偽メール　パスワード盗む　立命館大生	12/26 mainichi INTERACTIVE

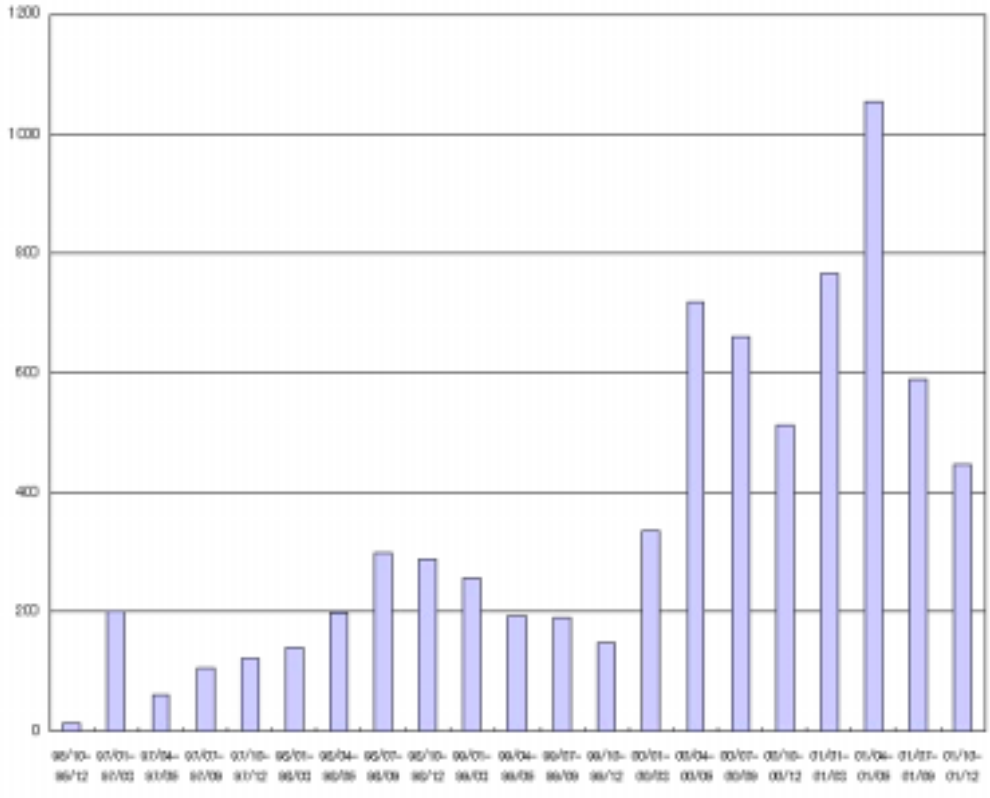

図 1-1 インシデント報告件数の推移（JPCERT/CC ホームページより）

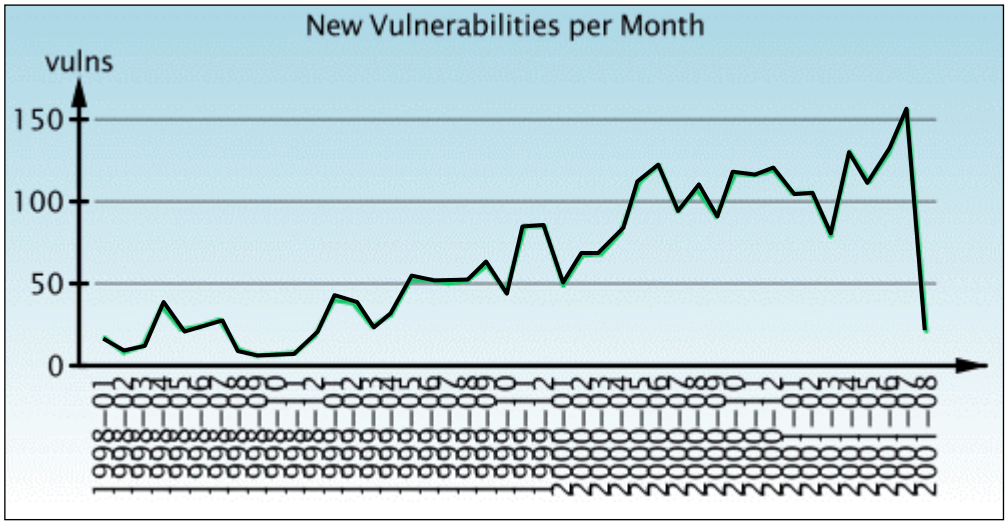

図 1-2 脆弱性報告件数の推移（SecurityFocus 社ホームページより）

また、ウイルス／ワームの届出に関する推移についても、情報処理振興事業協会（IPA）より発表されているが、こちらについては図 1-3に示すように 2000 年 11 月より急増し、月に 2,000 件の報告を超えるケースも頻繁になってきている。

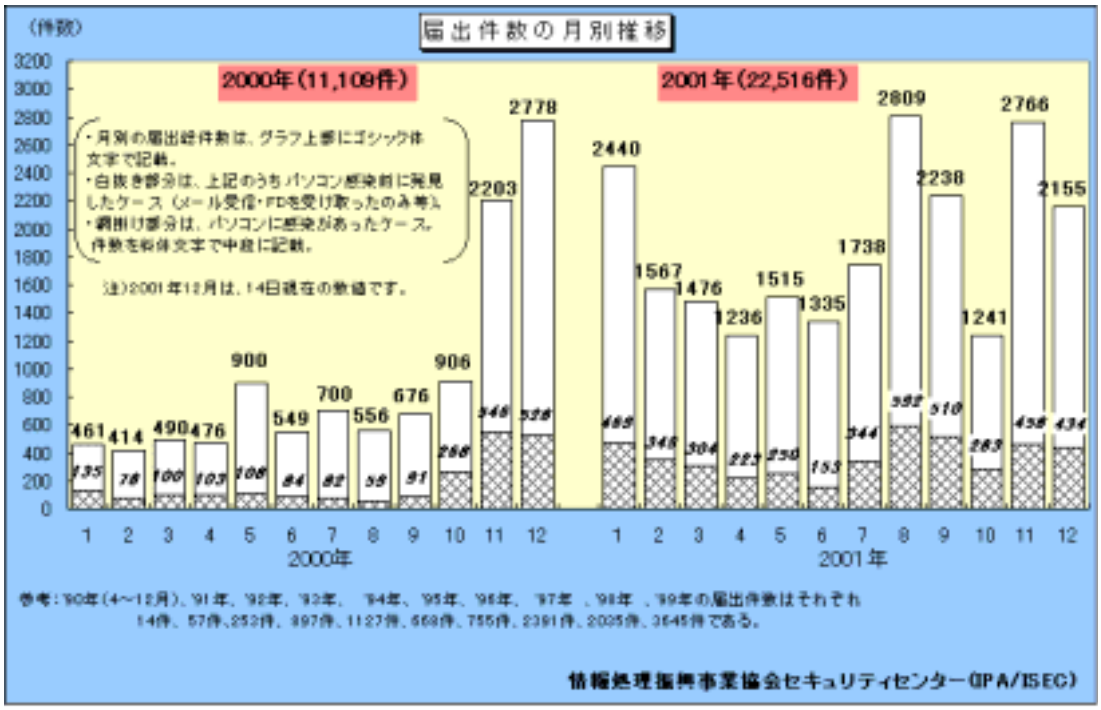

図 1-3 ウイルス届出件数の推移（IPA ホームページより）

以上のように、ハッカーやクラッカーが直接システムに対して行う不正アクセスや、ウイルス／ワームによるものを含めて、日本国内のネット被害は拡大傾向にある。

1.2 不正アクセスの形態とネット被害

企業等にある情報システムや、企業･家庭内のパソコンへの不正アクセス開始の糸口は、主に次の5つのパターンに分類できると考えられる。

① パスワードの不正使用

何らかの不正な手段によって他人の ID･パスワードを入手したり、パスワードクラック（2.1.1.2(2)を参照）を行うことにより ID･パスワードを見つけ出して、システムへ侵入する

② セキュリティホールを利用した侵入

プログラムのバグを利用して、第三者が外部から任意のプログラムを実行したり管理者権限を奪ってシステムを不正利用する

③ リモートアクセスの入口からの侵入

保守用や外部からのアクセス用に設けられた入口や、ワーム等により仕掛けられたバックドアからシステムへ侵入する

④ 機器の設定ミスを利用した侵入

ネットワーク機器やサーバのデフォルトアカウント等を利用したり、機器のセキュリティ設定ミスにつけこむことにより、システムへ侵入する

⑤ 一般ユーザの利用するパソコンへのウイルス／ワームの送り込み

ウイルス／ワームを企業･家庭内のパソコン等へ送り込むことにより、システム上のファイルを破壊したり、意図しない動作を実行したりする

図 1-4は、不正アクセスの開始からネット被害に至る主な経路である。この図から分かるように不正アクセスの形態は複雑化してきており、それらに対して行うべき対策も多岐に亘ったものが必要となってきている。

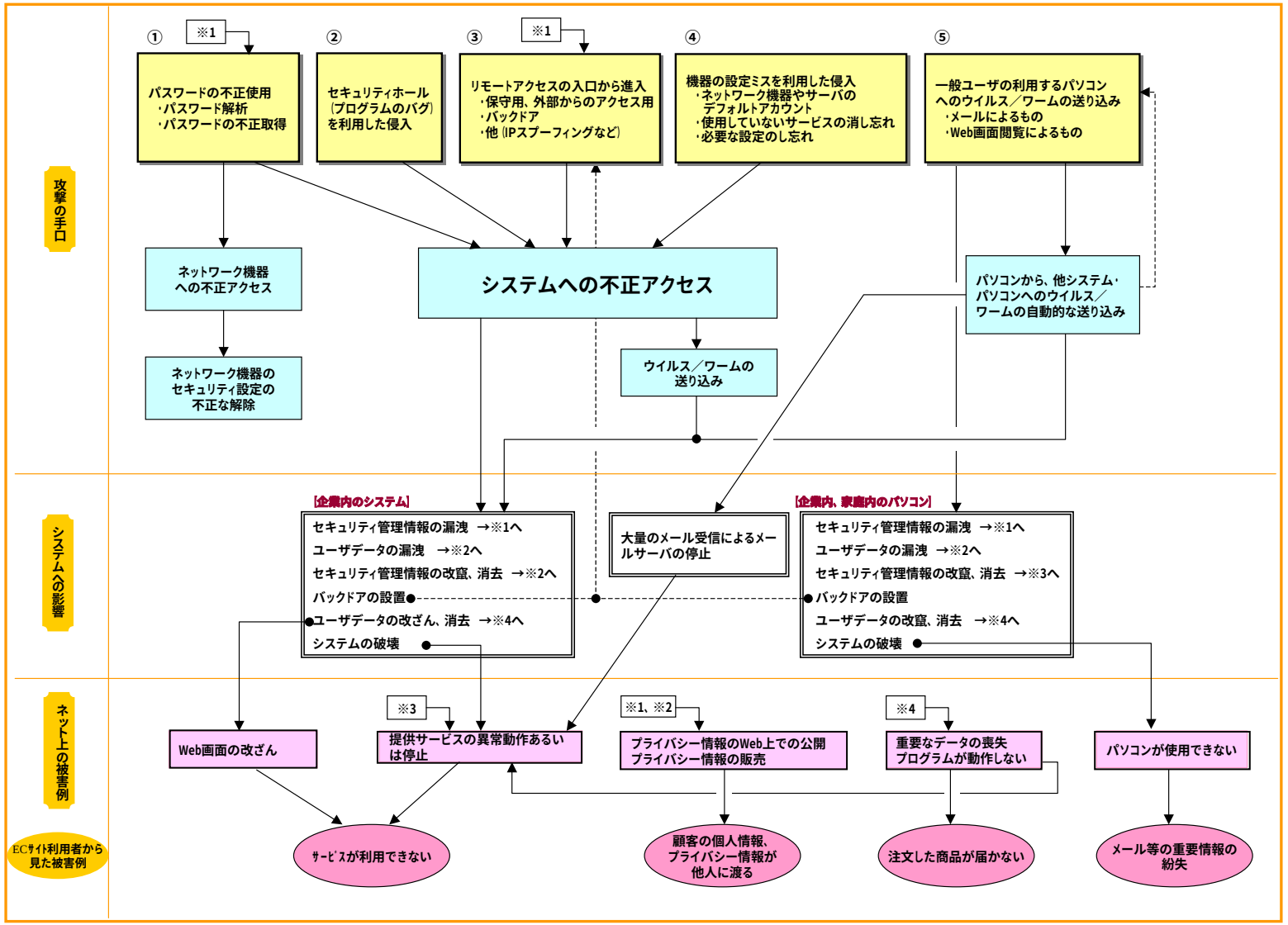

図 1-4 不正アクセスの攻撃手口からネット上の被害に至る大まかな経路図

2 脅威の分析

EC におけるセキュリティ対策を検討するにためには、何が脅威なのかを明確にすることが重要である。これまで認証については電子商取引推進協議会の中でも専門のワーキングを設け検討を重ねてきたが、ホームページの書き換えに見られるような不正アクセスの事例を見ると、今一度脅威についての分析を行い、脅威を再整理してみることは、個々の対策が十分なものであるかを検証する上でも必要と思われる。

1) 脅威とは

本報告書における「脅威」については、次のように定義する。

- 「脅威」とは

  EC 事業をインターネットなどの不特定多数が利用するネットワークを使って行う上で、EC サイトの外部の者が行う不正行為により、EC 事業が脅かされること。

ここで、不正行為とは「不正アクセス」、「サービス妨害」、「ウイルス／ワーム」による攻撃のことを指す。

EC サイト内部の関係者による不正アクセスや破壊行為についても見逃してはならない脅威であるし、「脅威」から二次的に生じる問題についても重要な検討事項ではあるが、これらについては言及するに留め、外部からの脅威に関する分析を中心に行う。

2) 脅威の内容

本章では以降、脅威の具体的な分析を行っていくが、ここではその全体を整理する。

まず、脅威となる行為を行う者たちについてであるが、大別すると下記のようになる。

表 2-1 脅威の行為者の分類

名 称	概 要
ハッカー	OS などシステムプログラムへの技術的興味から、システムの問題点を指摘する意図で行動する者たちで、高度技術を次々と作り出す
クラッカー	技術的な興味よりは、破壊行為を行うことにより、世間の注目を浴びたいという動機で行動する者たち
スクリプト・キディ	ハッカーが開発したハッキングツールを遊び感覚で試す者たちで、現在の脅威の行為者の多くはこれに属する また、無差別に攻撃を行うため問題が多い
テロリスト、 犯罪組織	教科書問題などの政治的な意図を持って特定の国のサイトを攻撃したり、経済的な理由や特定の企業に被害を与えるといった目的で攻撃を行う者たちで、集団で組織的に行動する

特に「スクリプト・キディ」が、違法な行為をしているという意識を持たずに、無差別に攻撃をしてくる点は近年問題となってきている。背景としてはツールを使う程度でも簡単に不正アクセスできてしまうような安易な設定のままのサイトが存在していることも一因である。

具体的な脅威となる行為・攻撃として、次のものがある。

表 2-2 脅威の行為・攻撃の分類

行為・攻撃	内 容
不正アクセス	サイトのサーバ OS やサービスにログインし、サービスを不正に利用したり、顧客情報の取得、データ改ざん、システム破壊を行う
DoS 攻撃	サイトに直接ログインはせず、大量のデータを送りつける等により、相手に迷惑を与えることを目的としている
ウイルス／ワーム	電子メールや FD などのメディアを媒介として伝染する有害プログラムで、システムに潜伏し自己のコピーを他システムに伝染するとともにシステム破壊を行う

以降、これらについて詳しい分析を行う。

2.1 不正アクセスに関する分析

不正アクセスとは、いずれかの手口を用いて、攻撃対象のサイトの OS またはサービスにアクセスし、不正にサービスを利用する行為である。不正アクセスの手口については、以下で詳細を説明する。

実際には、それぞれの手口を実行する前に下調べを行う段階があり、図 2-1に示すように、実世界の犯罪同様に攻撃対象の調査･絞り込みを行い、侵入できそうだと判断した上で攻撃を開始する。

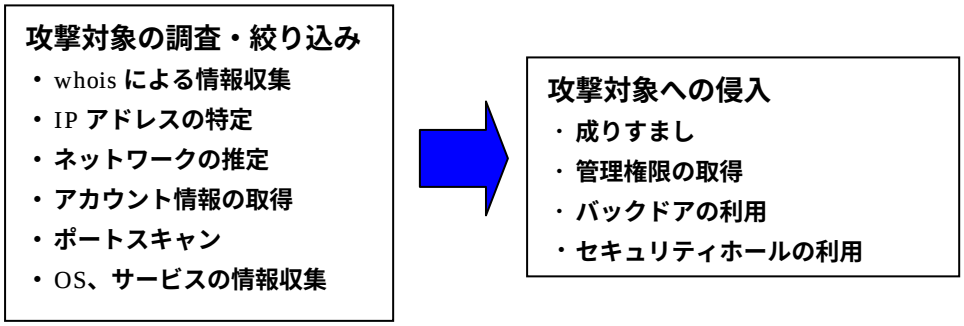

図 2-1 調査･絞り込みから攻撃対象への侵入へ

2.1.1 成りすまし

2.1.1.1 攻撃の概要

システムが提供するサービスを利用するために行う認証プロセスをいずれかの手法を用いて、迂回したり、不正に入手した正規ユーザの ID･パスワードを用いて、不正にシステムを利用する行為である。ただし、ここでは管理者アカウントへの成りすましは含めない。

2.1.1.2 攻撃の手口

(1) NULL アクセス

NULL アクセスとは匿名ログインや、認証を必要としないサービスを利用してシステムにアクセスする手法である。ルータ等の設定用の Telnet や TFTP、Windows NT/2000 での NULL セッションを利用すると、認証を経ずにシステムの一部の情報を読み出すことが可能となる。

(2) パスワードクラック

Telnet や FTP、POP など多くのサービスが ID･パスワードを用いてユーザ認証をしている。何らかの方法でユーザ ID が判明していれば、後はパスワードを推測するだけとなる。このパスワードを調べる手法をパスワードクラックと呼び、これには推測したパスワードを実際に入力してチェックする方式と、パスワードファイルを入手し、オフラインで解析する方式がある。実際には後者が使われることが多い。

パスワードクラックの推測方法としては、次の2つの方法がある。

① 辞書攻撃

実際に使用されるパスワードでは、ユーザが覚えやすいように電話番号や有名人の名前などが使われることが多い。このことを利用して、パスワードとして使われる言葉を辞書として集めておき、これに攻撃対象のシステムのパスワードの処理と同じ処理を施し、パスワードファイルと突き合わせることによってパスワードを解析する。このための辞書はネットワークで簡単に入手可能である。また解析するためのツールも GUI 化されたものがあり、高度な知識がなくても使えるような状況にある。

② ブルートフォース攻撃

これは別名「総当り攻撃」とよばれるもので、パスワードとして使われる文字の全組合せを自動生成して、確認する方法である。時間がかかるが必ず見つかるという方法である。

(3) 盗聴

これは、電話の盗聴と同様に、ネットワークを流れるデータを読み取り、パスワード等の情報を抽出する。通常、自分の IP アドレス宛ての情報しか読み出せないが、ネットワークの障害対応のためにすべての情報を読み出し解析するソフトや機器があり、これを使うことで、他人の情報を容易に読み出すことが可能である。このような機器やソフトウェアを HUB に接続したり、サーバにプログラムを潜ませるなどの方法で盗聴を行う。

実際にはすべての情報を記録するのではなく、「パスワード」など認証に関係するキーワードを抽出する。

(4) システム初期設定の利用

OS や各サービスのインストール時に設定されている初期ユーザを利用し、システムにログインする。これらの初期設定ユーザの情報は雑誌や解説書にも情報が掲載されており、簡単に知ることができる。中には管理権限をもつアカウントもあり、これを放置したままにすることは非常に危険である。特に、テスト用や開発用に立ち上げたサーバに多く見られる。

(5) ソーシャルエンジニアリング

この手口は、人間の弱さや管理の甘さをついた手法で電話でユーザに成りすまして、管理者に「幹部が至急システムを使えるようにしたいので教えてほしい」などと言い、パスワードを聞き出すなどの手法である。

また、起動したままの PC を利用したり、破棄された書類や記録媒体、PC からデータを読み出してアカウントの情報を取得するなどの手口もある。

2.1.1.3 想定される影響

(1) **システムを不正に利用される**

正規のユーザに成りすまし、システムが提供している各種サービスを不正に利用されてしまう。

(2) **個人情報の漏洩、ストーキング行為**

他人に成りすますことで、他人のメールを見るなどして個人情報を不正に得る。これにより、成りすまされた個人のプライバシーの侵害や、ストーキング行為などが行われる。

(3) **詐欺**

他人のアカウントを使用することにより、ショッピングを不正に行うなどの詐欺行為が行われる。

(4) **個人情報の売買**

成りすました個人の情報を集めて名簿業者に売買するなど、個人情報の漏洩の問題が生じる。

2.1.1.4 攻撃への対策

(1) **匿名サービスの制限**

TFTP、anonymousFTP などの匿名で利用できるサービスは停止する。

(2) **パスワードファイルのアクセス権の設定、内容の暗号化**

パスワードファイルに対して OS のアクセス制御の機能を使用し、アクセス権を設定する。また、/etc/shadow など、セキュリティを強化した機構を採用する。

(3) **データの暗号化、ワンタイムパスワード、デジタル証明書の利用**

盗聴による被害を防止するため、SSL などを使って通信内容を暗号化する。また認証方式として単純な ID･パスワード以外の機能を利用する。

(4) **不正侵入検知システム（IDS）による監視**

IDS を導入し、不正アクセスの兆候を監視する。

(5) **システムの設定のチェック（初期設定のままとしない）**

OS やアプリケーションに初期設定として設定されているアカウントを削除するなど、インストールしたままで放置せず、設定を検討・実施した上で運用するようにする。

(6) **運用管理者の作業内容の見直し、教育の実施**

運用面からの見直しを行うとともに、運用管理関係者へ、攻撃と攻撃への対処に関わる教育を行うようにする。

(7) **PC、記録媒体、紙文書の廃棄方法の強化**

離席時に PC をロックする。また、PC を廃棄する場合にはデータを完全に消去する。また、記録媒体や処理の廃棄に対しては、基準を設けて実施する。

(8) **複数の認証手段を組合せる**

ID・パスワード単独ではなく、重要なサービスに対しては IC カードやバイオメトリクスなど複数の認証手段を組合せる。

2.1.1.5 被害の事例

- 2001 年 9 月 5 日　他人の ID を盗み HP に侵入の疑い、38 歳女性を逮捕（日本経済新聞）
- 2000 年 8 月 3 日　他人のパスワードを使いネットに接続、大阪、容疑の男性逮捕（日本経済新聞）

2.1.2　管理者権限の不正取得

2.1.2.1 攻撃の概要

本来、管理者のみが使用可能な管理者アカウント（特権ユーザ、root、administrator）を不正に取得してシステムへログインしたり、不正プログラムを管理者権限で起動することで、システム情報の参照または改ざんを行うための手段とする行為である。

2.1.2.2 攻撃の手口

(1) **セキュリティホールの利用**

セキュリティホールによっては、それを悪用することで管理者権限を不正に取得できるケースがある。直接管理権限が直接取得できない場合でも、任意のプログラムを実行できるような

場合、管理権限を取得するためのプログラムを送り込み実行する場合がある。

(2) **パスワードクラック**

成りすまし攻撃の場合と同じ。

(3) **盗聴**

成りすまし攻撃の場合と同じ。

(4) **システム初期設定の利用**

成りすまし攻撃の場合と同じ。

(5) **ソーシャルエンジニアリング**

成りすまし攻撃の場合と同じ。

2.1.2.3 想定される影響

(1) **システムを不正に利用される**

「成りすまし」の場合と同様、システムの提供するサービスやリソースを不正に利用される。また、管理者権限のため一般ユーザの場合よりも自由に使われてしまう可能性がある。

(2) **システム改ざん・破壊**

管理者権限を使用し、システムの設定ファイルを自由に改ざんすることが可能であり、ファイルを消去し、システムの回復が不可能なまでに破壊することもできる。いわゆるホームページの書き換えも、この被害の一部である。

(3) **他システム攻撃のため踏み台として悪用される**

ファイルの改ざんなどの目に見える被害を与えずに、他のサイトへの攻撃を目的とした仕掛けを準備するため、また防御側からの追跡を困難にするための隠れみのとして悪用される。

二次的な被害として、最終的に攻撃対象となったサイトからの損害賠償等を請求される事態も生じる場合がある。

(4) **個人情報の漏洩**

「成りすまし」の場合は、被害は成りすまされた個人の範囲であるが、管理者権限を取得されると、全顧客の情報など、より広範に個人情報が漏洩する被害が生じる可能性がある。

2.1.2.4 攻撃への対策

(1) **セキュリティホール対策（修正プログラムの適用）**

セキュリティホールの情報を収集し、自システムに関係のある情報が公開された場合、できるかぎり早急に修正プログラムを適用することが大切である。

(2) **パスワードファイルのアクセス権の設定、内容の暗号化**

成りすまし攻撃の場合と同じ。

(3) **データの暗号化、ワンタイムパスワード、デジタル証明書の利用**

成りすまし攻撃の場合と同じ。

(4) **不正侵入検知システムによる監視**

成りすまし攻撃の場合と同じ。

(5) **システムの設定のチェック（初期設定のままとしない）**

成りすまし攻撃の場合と同じ。

(6) **運用管理者の作業内容の見直し、教育の実施**

成りすまし攻撃の場合と同じ。

(7) **PC、記録媒体、紙文書の廃棄方法の強化**

成りすまし攻撃の場合と同じ。

(8) **複数の認証手段を組合せる**

成りすまし攻撃の場合と同じ。

(9) **改ざんチェックツールの利用**

直接的には管理権限の取得の防止とはならないが、最終的なファイル改ざんを防止するために、ファイルの改ざんをチェックし、オリジナルファイルに戻すツールを導入することも対策として有効である（3.4.3.3を参照）。

2.1.2.5 被害事例

ホームページの書き換え事件等多数ある。各事件での詳細は不明につき、事件の特定はできなかった。

2.1.3 セキュリティホールを使った攻撃

2.1.3.1 攻撃の概要

システムを構成するプログラムのバグ（セキュリティホール）を利用し、本来システム想定していな

い処理を実行させることにより、不正アクセスの入口とする行為である。

2.1.3.2 攻撃の手口

(1) バッファオーバーフロー

セキュリティホールで多く見られる問題点がこの「バッファオーバーフロー」である。

プログラムは広い意味で何らかの入力を受け入れ、処理した結果を返信している。この処理で、プログラムが入力データのサイズのチェックを正しく行っていないと、図 2-2のように、メモリ上にある受信バッファの領域を越え、プログラムの戻り値を保存しているスタックの領域にまで受信データが入り込むことがある。このような状態になると、処理が終了して OS に制御が戻る時、本来の戻りアドレスではなく、攻撃者が入力したアドレス値とすることができる。こうなると攻撃者は任意のプログラムを実行することが可能になり、サービスが管理者権限で実行されている場合は、攻撃者はほぼすべての処理を実行する権限を不正に取得できてしまう。

これが典型的な「バッファオーバーフロー」攻撃である。

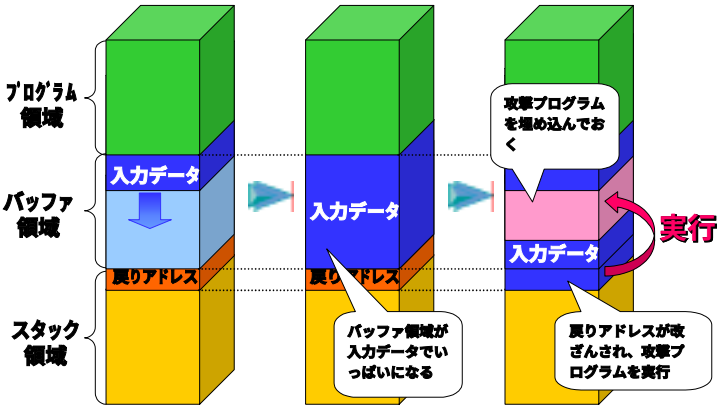

図 2-2 バッファオーバーフロー

(2) クロスサイト・スクリプティング

Web を記述する HTML、XML 等のマークアップ言語のソースを動的に生成する仕組みを設けている場合に問題となることがあり、あるサイトに書かれているスクリプトが他のサイトへクロスして実行されることから、「クロスサイト・スクリプティング」と呼ばれている。

悪意のあるものが Web サーバシステム上にクロスサイト・スクリプティングを書き込むことによって、様々なセキュリティ侵害が可能となる。例えば、攻撃者が他のサイトにある悪意のあるプログラムをダウンロードさせるスクリプトを記述するように事前に処理を行った場合、そのページにアクセスした者は、使用するパソコンが悪意のあるプログラムに侵害されるといったことが発生する可能性もある。また、ページにアクセスした時にアクセスした者の cookie を他のサ

イトへ転送することも可能である。cookie は、第三者に漏洩しないことを前提に利用されているのであるが、クロスサイト･スクリプティングによる漏洩が発生すれば、その cookie を用いたサービスの不正利用が行われる可能性もある。

2.1.3.3 想定される影響

(1) **管理者権限の不正取得による攻撃からの被害**

バッファオーバーフロー等の攻撃により、管理者権限が不正に取得された場合、システムの改ざん･破壊、他システムの攻撃の踏み台など、さまざまな被害が予想される。

(2) **ウイルス／ワームの侵入による被害**

2001 年に発生した「CodeRed」、「Nimda」などのウイルス／ワームはセキュリティホールを感染手段として利用している。対策が不十分な場合、同様の感染被害をこうむる可能性がある。

2.1.3.4 攻撃への対策

(1) **セキュリティホール情報の収集**

まずは、使用している OS やソフトウェアについて、セキュリティホールに関する情報を収集する必要がある。メーカや各種団体が情報を収集し、無償あるいは有償のサービスを提供しているので、これらの情報を頻繁に参照し、新たな問題がないか把握することが重要である。

(2) **セキュリティホール診断の活用**

使用しているシステムに重要なセキュリティホールがある場合、修正プログラムを適用することが重要である。運用中のアプリケーションへの影響を考慮し、検証の上、できる限り早く適用することが大切である。ただし、修正プログラムを適用することによってこれまで正常に動いていたプログラムに影響する可能性もあるため、慎重に行うことが必要である。

(3) **セキュリティホールの正しい把握**

対策のためにはシステムに存在するセキュリティホールを正しく把握することが重要である。十分に把握できていない場合、各社がサービスを行っているセキュリティホール診断を活用する方法も有効である（3.3.2を参照）。

2.1.3.5 被害事例

ホームページの書き換え事件等多数ある。各事件での詳細は不明につき、事件の特定はできなかった。

2.2 DoS 攻撃に関する分析

DoS （Denial of Service）攻撃は、直接攻撃対象とするサイトのサーバにアクセスする不正アクセスと異なり、大量のデータやメールを送ることで、業務妨害や迷惑を与える脅威である。一見して正常データと同じであるため、対策には不正アクセスの場合とは違った検討が必要である。

2.2.1 攻撃の概要

業務の妨害などの嫌がらせ目的のため、大量のパケットや伝送データなど不正データをシステムに送信し、サーバ処理能力を低下させたり、システムを停止させる行為が DoS 攻撃である。

2.2.2 攻撃の手口

2.2.2.1 DoS 攻撃

この攻撃は大量のパケットを攻撃対象のサーバに送信することによりサーバの処理能力を低下またはダウンさせたり、ネットワークを過負荷にして帯域を食いつぶすことで正常なパケットを流れにくくしたりする攻撃である。

DoS 攻撃にはその手法により下記の4種類のタイプが存在する。

(1) Smurf 攻撃

この攻撃は Ping コマンドの機能を悪用した攻撃である。Ping コマンドは宛先のホストの IP を指定し、そのホストとの通信が可能かを確認するために使用されるコマンドである。具体的には ICMP Echo Request を送り、ICMP Echo Reply の返信を確認する。攻撃者は送り元の IP アドレスを攻撃対象に偽造し、宛先のアドレスをブロードキャストアドレスとすることで、一斉に攻撃対象のアドレス宛に ICMP Echo Reply を送りつける。

(2) Flood 系攻撃

Flood 系攻撃には、大別すると SYN Flood 攻撃、UDP Data Flood 攻撃、Syslog Flood 攻撃がある。

このうち、SYN Flood 攻撃は TCP の 3 Way Handshake を利用したものである。TCP はコネクション型の通信であるため、クライアントから接続要求（SYN パケット）があると、SYN/ACK パケットを返信してクライアントからの応答を待つ。ここで攻撃側は応答のパケットを返信しないままにすると、サーバ側は返事を待ち続ける状態となってしまう。これを大量に行うと、サーバ側で待ちの処理が大量に発生し、システムリソースが不足となり、最悪の場合

はシステムダウンとなる。

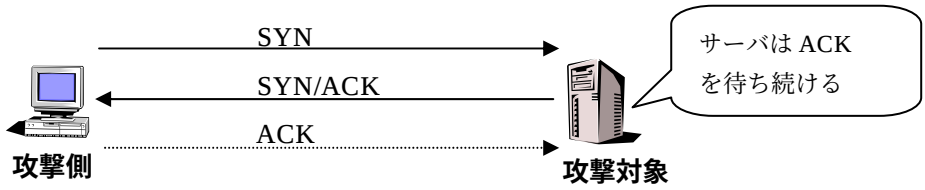

図 2-3 SYN Flood 攻撃

(3) **奇形パケットを利用した攻撃**

大量のパケットを送ることなくサーバをダウンさせてしまうのがこの攻撃である。通常はありえない奇形パケットを送信することで、それに対応してないサーバの場合には、意図しない処理が実行され、最悪はシステムダウンとなる場合がある。代表的な攻撃として“Ping of Death”と呼ばれるものがある。

(4) Echo/Chargen **ループ**

この攻撃は、UNIX の Echo と Chargen サービスを悪用したもので、2台の攻撃対象のサーバ間でエコーバックの無限ループを作り出し、ネットワークの帯域を食いつぶして事実上処理不能の状態にしてしまう攻撃である。

2.2.2.2 DDoS 攻撃

DoS 攻撃の場合は、攻撃は1ヶ所から行われるが、これでは攻撃元を突き止められたり、攻撃に使われるデータも少なく攻撃の効果が小さい。これを図 2-4のように、予め攻撃を仕掛けるプログラムを複数のサイトに組み込む準備をし、コマンドを送るなどの指示を与えて、複数のサイトから一斉に攻撃対象のサイトへの DoS 攻撃を仕掛ける方法である。この手法から DDoS（分散 DoS 攻撃、Distributed DoS）攻撃と呼ばれている。

最近の例では CodeRed の例のように、攻撃プログラムを仕掛ける手段として、ウイルス／ワームを利用するケースが出現した。

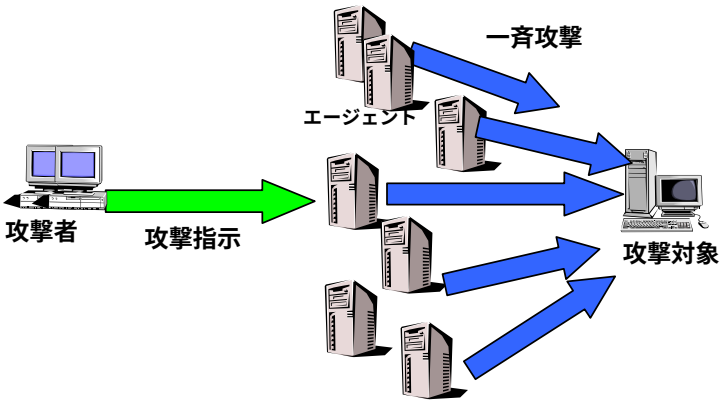

図 2-4 DDoS 攻撃

2.2.2.3 メール爆弾

この攻撃は、大量のメールを攻撃対象のメールサーバに送りつけることで、メールサーバのディスクをパンクさせ、サービスを停止させる攻撃である。メール自体は正常なデータであるため、他のメールと識別することが難しい点が問題である。

2.2.3 想定される被害

2.2.3.1 本来業務の遅延・停止

大量のパケット送信によりサーバの処理能力の大半が奪われ、顧客へのサービスの遅延･停止が発生する。その結果として、ビジネスでの経済的な損失やシステムの復旧のためにコストがかかるといった影響も発生する。

2.2.4 攻撃への対策

DoS 攻撃が、正常なパケットを利用した攻撃である場合は、防御することは非常に困難である。ただし、個別の手法については、メーカやベンダより、対応する修正プログラムを出しているところもある。

また、2.2.4.1～2.2.4.5で示す対策方法を検討してみるとよい。

2.2.4.1 OS のバージョンアップ、不要サービスの停止

Flood 系の DoS 攻撃については OS のバージョンアップで対応できる。また Echo/Chargen ループに関しては Echo サービスを停止させることで対策が可能である。

2.2.4.2 パケットフィルタリングの利用

攻撃の手法によっては、ルータなどでフィルタリングの設定を行うことで対策が可能な場合がある。

2.2.4.3 不正プログラムの排除

DDoS 攻撃の場合、攻撃を行うためのマシンを多数用意する必要があるが、ウイルス／ワーム対策と同様にサイト内のホストに対して定期的に不正なプログラムが存在しないかどうかの検査を実施することで、自サイトが攻撃に加担しないように防止することが大切である。

また、家庭においても常時接続されるパソコンが増えてきており、これらについても同様に注意が必要である。

2.2.4.4 メール爆弾の対策

メール爆弾による被害に対する完全な対策はないが、次の点をチェックすることである程度の対策は行うことができる。

(1) **不正中継を無効にする**

メール爆弾で攻撃する側はメールの発信元を隠し、かつ大量のメールを効率よく送信するため、踏み台にするメールサーバを利用するケースが多い。従って、自サイトがメール爆弾の加害者とならないためにも、自組織（ドメイン）とは無関係の第三者メールの中継をしないよう設定することが対策となる。

＜参考＞

- IPA 「spam メール中継対策」
  http://www.ipa.go.jp/security/ciadr/antirelay.html

- JPCERT/CC 「電子メール配信プログラムの不正利用」
  http://www.jpcert.or.jp/ed/2000/ed000004.txt

(2) **不正中継するサーバからのメールを拒否する**

不正中継可能なサーバを調査･公開している ORBS〔http://www.orbs.org/〕等を参考に、メール爆弾が送られてくる可能性のあるサーバからのメールを拒否するよう設定する。

この場合、必要なメールまで受信できなくなる可能性もあるので十分検討した上で実施することが望ましい。

(3) **コンテンツフィルタリングの導入**

メールのコンテンツフィルタリングソフトを導入し、メール受信のポリシーを設定することでメール爆弾と思われるメールをフィルタリングすることが可能となる。

この場合についてもポリシーの設定に検討が必要である。

2.2.4.5 負荷分散装置の導入

負荷分散装置の一部には、大量のトラフィックを一旦バッファリングし、平準化してサーバに渡す機能を有したものがある。このような装置を導入することで、システムダウンに至る確率を下げることが可能である。

2.2.5 被害事例

- 2001 年 7 月　CodeRed による米ホワイトハウスへの攻撃
- 2001 年 2 月　米 Yahoo、CNN、アマゾンドットコム、eBay が攻撃される

2.3 ウイルス／ワームに関する分析

2001 年になって ADSL（非対称デジタル加入者線）やケーブル TV 等をアクセス網とした常時接続サービスであるブロードバンド（高速大容量）通信の普及や低料金化でインターネット人口が広がりをみせる中、コンピュータウイルス／ワームの被害が一層、深刻化している。IPA によると、2001 年 1 月 1 日から 12 月 27 日までの 1 年間のウイルス／ワーム届出数は計 24,261 件で、前年の 11,109 件を大きく上回り、過去最高となった。

ウイルスの定義については、必ずしも定まったものはないが、広義の定義と狭義の定義があり、広義には、「ウイルス（狭義）」、「ワーム」、「トロイの木馬」と呼ばれているすべてのものを含む悪意のある行動を起こすプログラムのことを指している。経済産業省（旧、通商産業省）が 1995 年に定めた「コンピュータウイルス対策基準」では、ウイルスの定義を広義の定義として記しており、その内容は以下のとおりとなっている。

コンピュータウイルス：

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり次の機能の 1 つ以上有するもの。

- 自己伝染機能
  自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能
- 潜伏機能
  発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまでの症状を出さない機能
- 発病機能
  プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能

ウイルスの狭義の内容については、ワーム、トロイの木馬と比較してみると、おおよそ以下のように考えられる。

- ウイルス（狭義）
  単独では存在・行動ができず、他の実行ファイルなどに感染し行動する。また、自己増殖機能を持ち、実行されると電子メールの添付ファイルやフロッピーディスク、CD-ROM などの媒体を通じて感染する。感染後、潜伏期間を経て発病するが、発病のタイミングについてはウイルスにより異なる。
- ワーム
  上記ウイルス（狭義）とは異なって、感染対象ファイルを必要とせず、単独で存在・行動する。自己増殖能力を持ち、自分自身を複製することによって増殖する。主に電

子メールの添付ファイルを通じて増殖するが、Web の閲覧による感染やワーム自らが感染可能なサーバを見つけ出して増殖するケースもある。

- トロイの木馬

  プログラムの中に、本来の処理に影響しないよう、悪意のあるコードを書き込み、プログラム実行の際、本来の処理に加えて悪意のあるコードを実行するもの。トロイの木馬自身は、自己増殖能力を持たない。

上記3種類の増殖･感染方法を比較すると次表のようになる。

表 2-3 「ウイルス」、「ワーム」、「トロイの木馬」の比較

種別	自己増殖	感染方法
ウイルス	○	他の実行プログラムに感染する
ワーム	○	単独で感染する
トロイの木馬	×	― ― ―

本報告書では、広義の定義のウイルスについては、狭義のウイルスとの用語の混乱を避けるために、以降「ウイルス／ワーム」と記すことにする。

以前はウイルス／ワームと言えば、例えば「Melissa」などの電子メール添付型のマクロウイルスが猛威を振るっていたが、次第に自分自身がメール送信機能を備えたワーム型のものが登場し、次第に被害規模も広がってきた。それと同時に被害の深刻さも増大しており、最近ではシステムを破壊するウイルス／ワームが次々と出現している（図 2-5参照）。

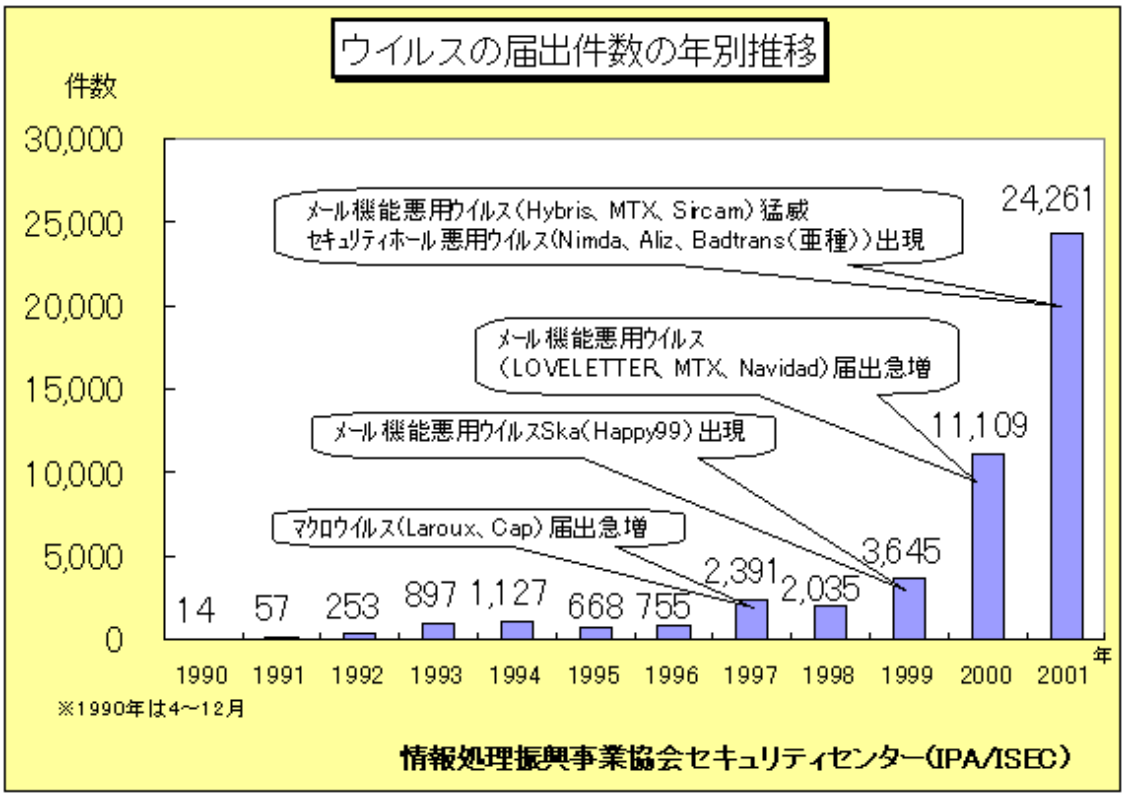

図 2-5 ウイルスの届出件数の推移（IPA ホームページより）

本章では 2001 年度に猛威を振るったウイルス／ワームの中でも代表的な4つのウイルス／ワームをトピックスとして報告することとする。

- Sircam（サーカム）
- Badtrans.B（バッドトランス B）
- CodeRedⅡ（コードレッドⅡ；コードレッドの亜種の１つ）
- Nimda（ニムダ）

これらに共通する特徴は、マイクロソフト社の Windows 環境で実行可能なファイルを利用したウイルス／ワームが主流となっていることである。

そして、これまでのウイルス／ワームは添付ファイルをクリックしなければウイルス／ワームへの感染はなかったのだが、Nimda や Badtrans.B のように製品の脆弱性を利用することでメールを見ただけ（プレビュー表示）で感染するようなウイルス／ワームが現れてきた。

こうしたウイルス／ワームに対処するには従来から利用されている各社のウイルス対策ソフトウェアによる検査に加えて、これらのウイルス／ワームの対象になるマイクロソフト社の Internet Explorer 等に修正プログラムを適用し、製品の脆弱性に対応することが重要となる。ウイルス／ワームに関する情報については、次のサイトが参考となる。

＜参考サイト＞

マイクロソフト㈱のセキュリティページ

http://www.microsoft.com/japan/security/

コンピュータ緊急対応センター（JPCERT/CC）のページ

http://www.jpcert.or.jp/

情報処理振興事業協会 セキュリティセンター（IPA/ISEC）のページ

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

日本コンピュータセキュリティ協会（JCSA）のページ

http://www.jcsa.or.jp/

表 2-4に、2001 年に発生した主なウイルス／ワームを挙げる。これらのウイルス／ワームの IPA への届出件数月別推移については、図 2-6に示す通りとなる。

表 2-4 2001 年のウイルス／ワーム一覧（IPA ホームページより）

ウイルス／ワーム名	
W32/Zoher	（2001.12.27 掲載）
W32/Maldal	（2001.12.25 掲載）
W32/Badtrans の亜種	（2001.12. 1 更新）
W32/Aliz	（2001.11.30 更新）
W32/Klez	（2001.11. 9 掲載）
W32/Nimda	（2001.11. 9 更新）
W32/Magistr	（2001. 9.10 更新）
W32/Apost	（2001. 9. 7 掲載）
W32/CodeRed	（2001. 8.16 更新）
W32/Sircam	（2001. 7.24 掲載）
W32/Badtrans	（2001. 6.13 掲載）
VBS/Haptime	（2001. 6.13 掲載）
VBS/Homepage	（2001. 5. 9 掲載）
VBS/SST（AnnaKournikova）	（2001. 2.15 掲載）
W32/Navidad	（2001. 1.12 更新）
W32/Hybris	（2001. 1. 5 更新）

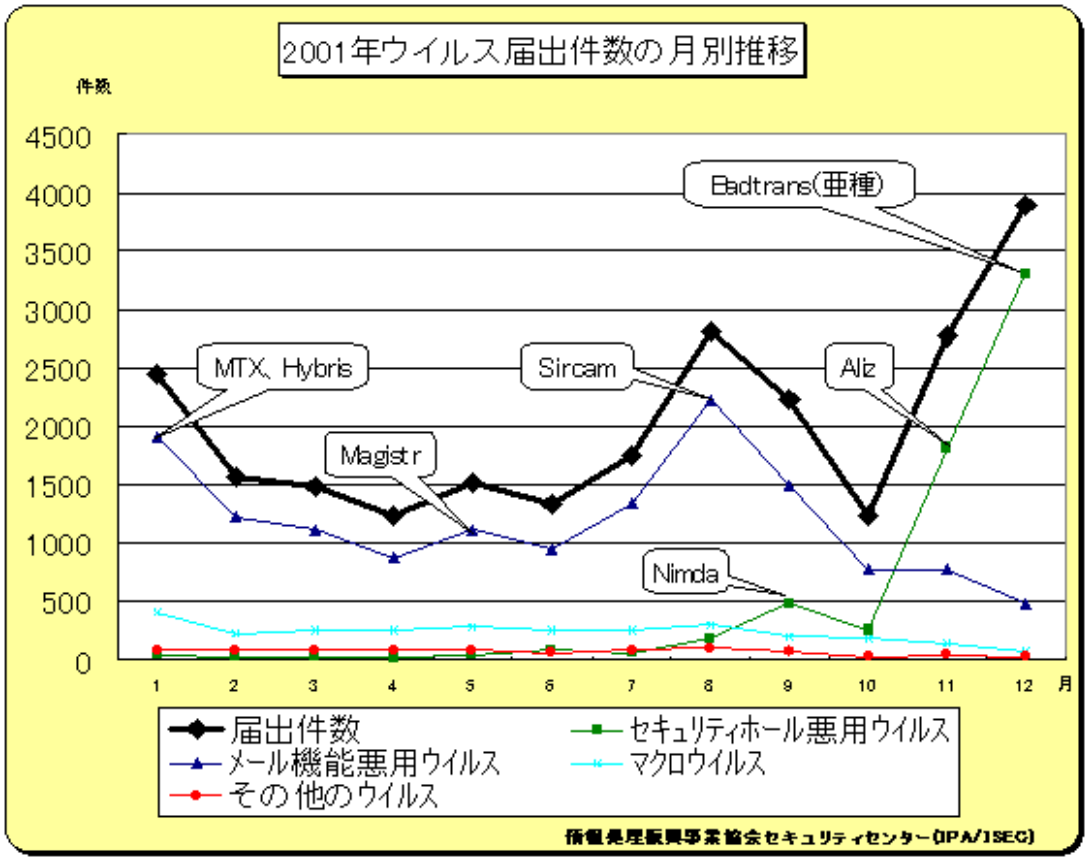

図 2-6 2001年ウイルス届出件数の月別推移(IPA ホームページより)

2.3.1 Sircam（サーカム）

2.3.1.1 概要

(1) **発生・流行時期**

2001 年 7 月中旬に発見され、7 月から 8 月にかけて大流行した。

(2) **感染の仕方**

このワームに感染すると自分自身をメールの添付ファイルに埋め込んで、利用者のメールアドレス帳に記載された全てのメールアドレスだけでなく、ブラウザのキャッシュも検索して、Web ページに掲載されている全ての第三者メールアドレスにも迷惑メールとして送信する。

【送信されてくるメール内容】

宛先：

Outlook、Outlook Express のアドレス帳の登録アドレスすべて、ならびに「テンポラリ・インターネット・ファイル」フォルダ（Web ブラウザのキャッシュフォルダ）にあるファイルの中から任意に取得したアドレス

件名:

ランダムなファイル名
「マイドキュメント」フォルダにあるドキュメントファイルおよび画像ファイルに入っているデータから取得

本文:

＜英語バージョン＞
1 行目: Hi! How are you?
---------- 以下のいずれか一つ ----------
・I send you this file in order to have your advice
・I hope you can help me with this file that I send
・I hope you like the file that I send you
・This is the file with the information that you ask for
最終行: See you later. Thanks

本文:

＜スペイン語バージョン＞

1 行目: Hola como estas ?
---------- 以下のいずれか一つ ----------
・Te mando este archivo para que me des tu punto de vista
・Espero me puedas ayudar con el archivo que te mando
・Espero te guste este archivo que te mando
・Este es el archivo con la informacion que me pediste
最終行: Nos vemos pronto, gracias.

添付ファイル: 件名に拡張子が付けられたもの

この添付ファイルの拡張子は DOC、XLS、ZIP に見えるが、よく確認すると実はアプリケーション（または MS－DOS アプリケーション）という、134KB 以上の添付ファイル（拡張子は BAT、COM、EXE、LNK、PIF の中のいずれか）となっている

(3) 感染による影響

感染による影響は、以下の通り。

- 毎年 10 月 16 日に C ドライブのすべてのファイルとディレクトリを削除する。
- 起動時にハードディスクの未使用スペースを埋めてしまうことがある。
- MS-Word、MS-Excel などのデータファイルに感染し、添付ファイルとして送信する。

(4) 拡散状況

Sircam は、電子メールの件名と添付ファイル名をランダムに選ぶことで、ワームではないように見せかけているため、メールを受け取った人がワームと気づかずに感染した添付ファイルを実行してしまい、一気に拡散した。

(5) その他

Sircam に関する各社の情報や対応状況は、下記の URL を参照するとよい。

- (株)シマンテック
  http://www.symantec.com/region/jp/sarcj/data/w/w32.sircam.worm@mm.html
- トレンドマイクロ（株）
  http://www.trendmicro.co.jp/virusinfo/default3.asp?VName=TROJ_SIRCAM.A
- 日本ネットワークアソシエイツ（株）
  http://www.nai.com/japan/virusinfo/virS.asp?v=W32/SirCam@MM&a=S
- F-Secure Corporation
  http://www.f-secure.com/v-descs/sircam.shtml

2.3.1.2 メカニズム

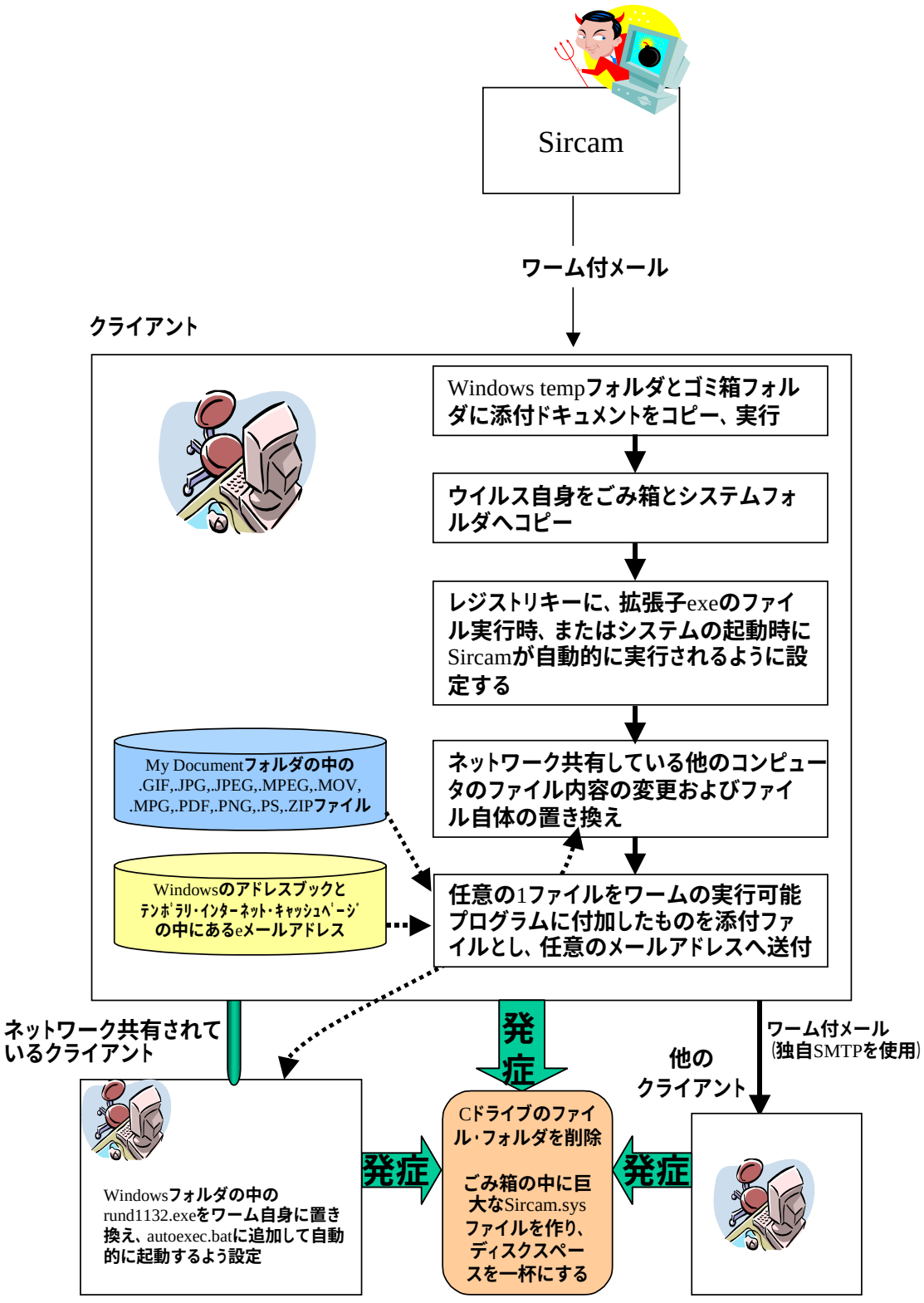

図 2-7 Sircam のメカニズム&動き

2.3.1.3 報告された被害

Sircam による被害については2001年7月21日～2002年1月8日の累計届出件数が1,441件となっている。また、下記のURLを参照するとよい。

http://www.ipa.go.jp/security/topics/sircam.html（IPAホームページより）

2.3.1.4 対策状況

各社ウイルス対策ソフトウェアベンダから対策に関する情報が提供されており、手動での駆除方法も説明されている。また、各社より駆除ツールが無償提供されている。

2.3.1.5 得られた教訓

ワーム駆除に関し、以下の点に心がけるとよい。

- 「ごみ箱」内のワーム駆除の確認
  このウイルス／ワームは「ごみ箱」にも潜伏するので、駆除したつもりでも残っている場合がある。そのために同じ者から何回もワームが送信されるといったことがある。
- 「autoexec.bat」ファイルの確認
  感染したPCの「autoexec.bat」ファイルに自分自身（sirc32.exe）を起動する行を追加することにより、毎回PC起動時にワームが送信される。
- システム管理者によるワーム駆除・システム破棄の対応
  一過性の対応としては、駆除ツール等を用いてワームの駆除を行うことが大切であるが、基本的には、感染したシステムは破棄しない限り新たな問題が起こる可能性が残される。システム管理者は、その点に留意し、対処すべきである。

2.3.2 Badtrans.B（バッドトランス B）

2.3.2.1 概要

(1) **発生・流行時期**

Badtrans.B が国内で発見されたのは 2001 年 11 月下旬である。

(2) **感染の仕方**

このワームは Windows95/98/ME/NT/2000 で動作する 32 ビットのワームであり、マイクロソフト社から報告されている脆弱性を利用して Outlook で開いたとき、Outlook Express ではプレビューしただけで感染するワームである。もちろん、実行した際も感染する。また、このワームは一般にメールの添付ファイルとして届く。

【送信されてくるメール内容】

- メールの送信パターン 1:

```
メールの送信者:
--------------
先頭に '_'（アンダースコア）が付いたアドレス

    例) "Name" <_address@abc.co.jp>
```

- メールの送信パターン 2: 以下のアドレスのいずれかの場合もある。

```
メールの送信者:
--------------
" Anna" <aizzo@home.com>
"JUDY" <JUJUB271@AOL.COM>
"Rita Tulliani" <powerpuff@videotron.ca>
"Tina" <tina0828@yahoo.com>
"Kelly Andersen" <Gravity49@aol.com>
" Andy" <andy@hweb-media.com>
"Linda" <lgonzal@hotmail.com>
"Mon S" <spiderroll@hotmail.com>
"Joanna" <joanna@mail.utexas.edu>
"JESSICA BENAVIDES" <jessica@aol.com>
" Administrator" <administrator@border.net>
" Admin" <admin@gte.net>
"Support" <support@cyberramp.net>
"Monika Prado" <monika@telia.com>
"Mary L. Adams" <mary@c-com.net>
" Anna" <lindaizzo@home.com>
"JUDY" <JUJUB@AOL.COM>
"Tina" <tina08@yahoo.com>
```

- メールの件名のパターン 1:

```
メールの件名:
--------------
"Re:"
```

- メールの件名のパターン 2:

  先頭に 'Re:' が付く、以前に送ったメールの返信の件名

- メールの件名のパターン 3:

  空の件名

- メールの本文：

  メールの本文:

  空の本文

- 添付ファイル名：

  以下の単語の組合せで、拡張子が二重につく。

  X . Y . Z

  X は、fun, Humor, docs, info, Sorry_about_yesterday, Me_nude, Card, SETUP, stuff,YOU_are_FAT!, HAMSTER, news_doc, New_Napster_site, README, images, Pics, SEARCHURL, S3MSONG のうちから任意の１つ。

  2 番目の Y は、DOC, MP3 から任意の１つ。

  最後の Z は, pif, scr から任意の１つ。

  例１） Sorry_about_yesterday.DOC.pif

  例２）Humor.MP3.scr

(3) 感染による影響

このワームは、MAPI（ Messaging API ）コマンドの機能を利用するとともに、Internet Explorer の既知のセキュリティ脆弱性を利用して自己増殖するワームである。更に、ユーザのキーボード操作を記録するトロイの木馬がインストールされるため、 感染した場合にはワームの作者によって情報セキュリティが侵害される可能性がある。

(4) 拡散状況

このワームは、該当する電子メールを受け取った場合、Outlook Express でプレビューしただけで感染してしまう可能性があり、その為に多くの人が感染するとともに、感染していることを知らないで使っている人から何度もワームが大量に送信される状況が発生している。

2.3.2.2 メカニズム

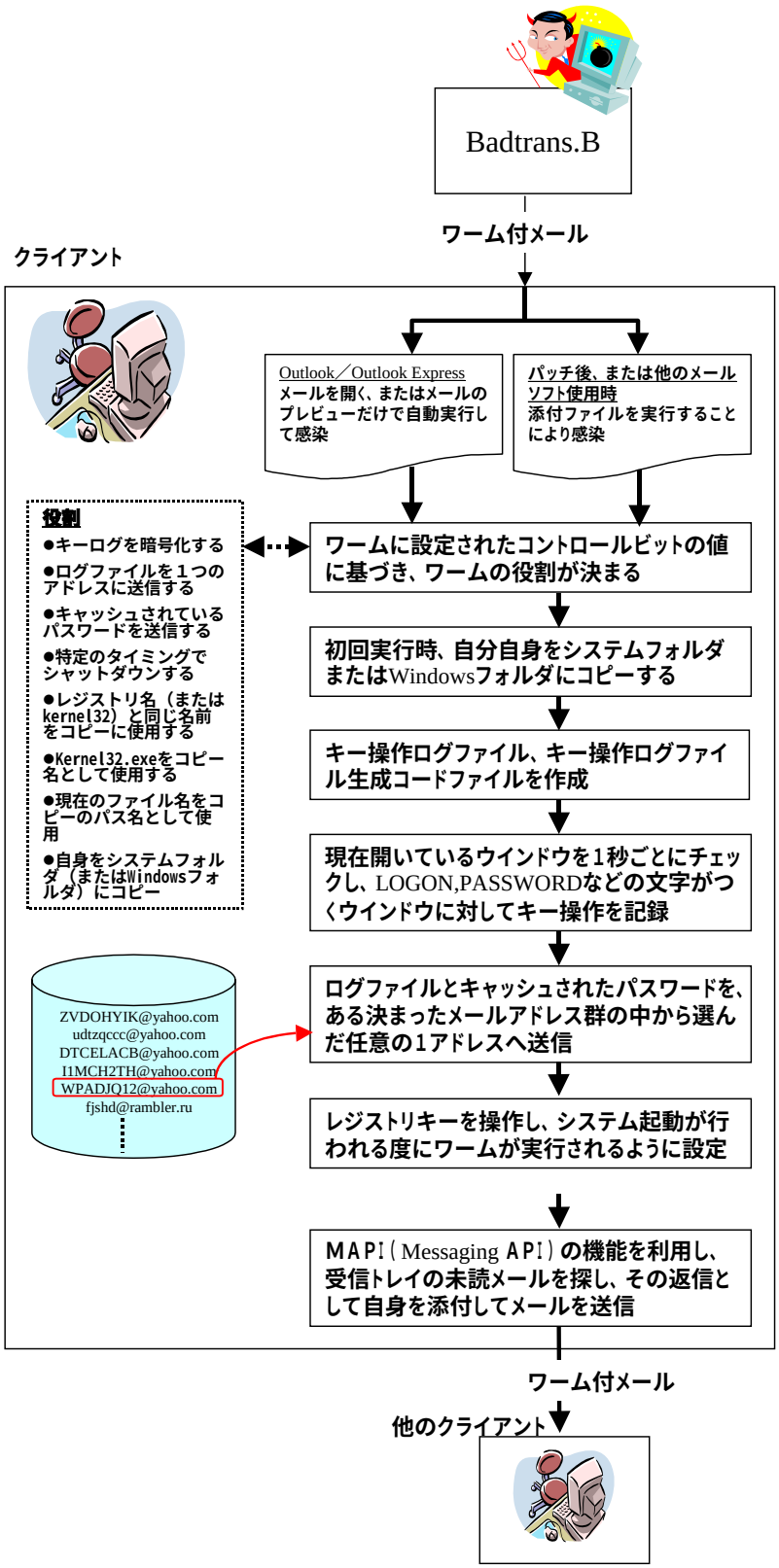

図 2-8 Badtrans.B のメカニズム&動き

2.3.2.3 報告された被害

IPA/ISEC に 2001 年 11 月 30 日までに寄せられた Badtrans.B の届出･相談は、合わせて 800 件以上になっている。

2.3.2.4 対策状況

本ワームは、既知の脆弱性を利用している。従って、利用者は次の対策を施すことによって、ワームに対して自動的に感染することはなくなる。ただし、添付ファイルを意図的に開くことなどによる感染は防止できないため、不用意にそのような行為を行わないようにする注意が必要である。

- Internet Explorer 5.01 の場合、SP2 を適用する
- Internet Explorer 5.5 の場合、SP2 を適用する
- Internet Explorer 6 の Outlook Express を含む標準構成以上でのインストールを行う

2.3.2.5 得られた教訓

ワーム駆除に関し、以下の点に心がけるとよい。

- このワームではユーザのキーボード操作を記録するトロイの木馬がインストールされるため、 感染した場合にはワームの作者によって情報セキュリティが侵害される可能性がある。そのため、感染するとパスワード等が盗まれる可能性があるので、感染した場合は、ワームによる影響から復旧した後、パスワード等を変更しておくことが必要となる。

2.3.3 CodeRedⅡ（コードレッドⅡ）

2.3.3.1 概要

(1) **発生・流行時期**

2001 年 8 月 1 日より CodeRed の活動が再開されているが、それに加えて新種の CodeRedⅡは 2001 年 8 月上旬に発見された。

(2) **感染の仕方**

CodeRedⅡでは感染力が増強されており、レジストリを書き換えたりバックドアをインストールするなど、より悪質なものになっている。このウイルス／ワームは感染後 24～48 時間感染行動を続け、その後、バックドアを残したままサーバを再起動させる。また、日本語環境においては、一部の OS では、トロイの木馬の起動用アドレスが変わるため、ブルースクリーンまたは再起動が発生する。

具体的には、Web サービスに対して特殊な URL を指定した要求を発行することで、リクエストを受けた Web サーバがバッファオーバーフローを引き起こし、その URL に埋め込まれたプログラム（CodeRedⅡ）を実行して感染する。

(3) **感染による影響**

オリジナルの CodeRed では、ホワイトハウスの Web サーバに DoS 攻撃を行うという影響があったが、その亜種である CodeRedⅡでは、攻撃者がリモートで Web サーバのアクセスをコントロールすることを可能にするという、オリジナルの CodeRed とは異なった影響を持っている。

(4) **拡散状況**

2001 年 8 月 10 日現在、IPA/ISEC に報告された届出･相談件数は CodeRed／CodeRedⅡ を合わせて、100 件を超えている。また、CodeRed／CodeRedⅡからの攻撃を受けたとの情報は多く、国内で数千のサーバが感染していた可能性があると言われている。

このウイルス／ワームが多数のマシンに感染し、それぞれが更に感染行動をとることによって、広範囲に亘って影響を与える可能性があり、対処を行わないことで自らのマシンが他のマシンへ攻撃するための踏み台となってしまう可能性がある。 特に、個人管理や SOHO で使用している等の管理の行き届いていないサーバへの感染が被害を増幅させることになる。

(5) **その他**

上記の内容と若干重複するが、IPA の調査結果によれば、CodeRed と CodeRedⅡの相違は次表のようになる。詳細については、IPA ホームページを参照されたい。

表 2-5　CodeRed と CodeRedⅡの相違点（IPA ホームページより）

相違点	CodeRed	CodeRedⅡ
行動パターン	日付により行動パターンを変更	感染後 24～48 時間感染行動を続け、その後サーバをリブートし感染を停止 2001 年 10 月 1 日以降は活動を停止
攻撃先スキャニング・パターン	ランダムな IP アドレスを攻撃	感染した自ホストに近い IP アドレスを優先して攻撃
攻撃の記録	ログ上の連続する文字が「N」	ログ上の連続する文字が「X」
Web 改ざん	一部 Web が書き換えられることがある	Web の書き換えは行わない
バックドアのインストール	インストールしない	インストールする

2.3.3.2 メカニズム

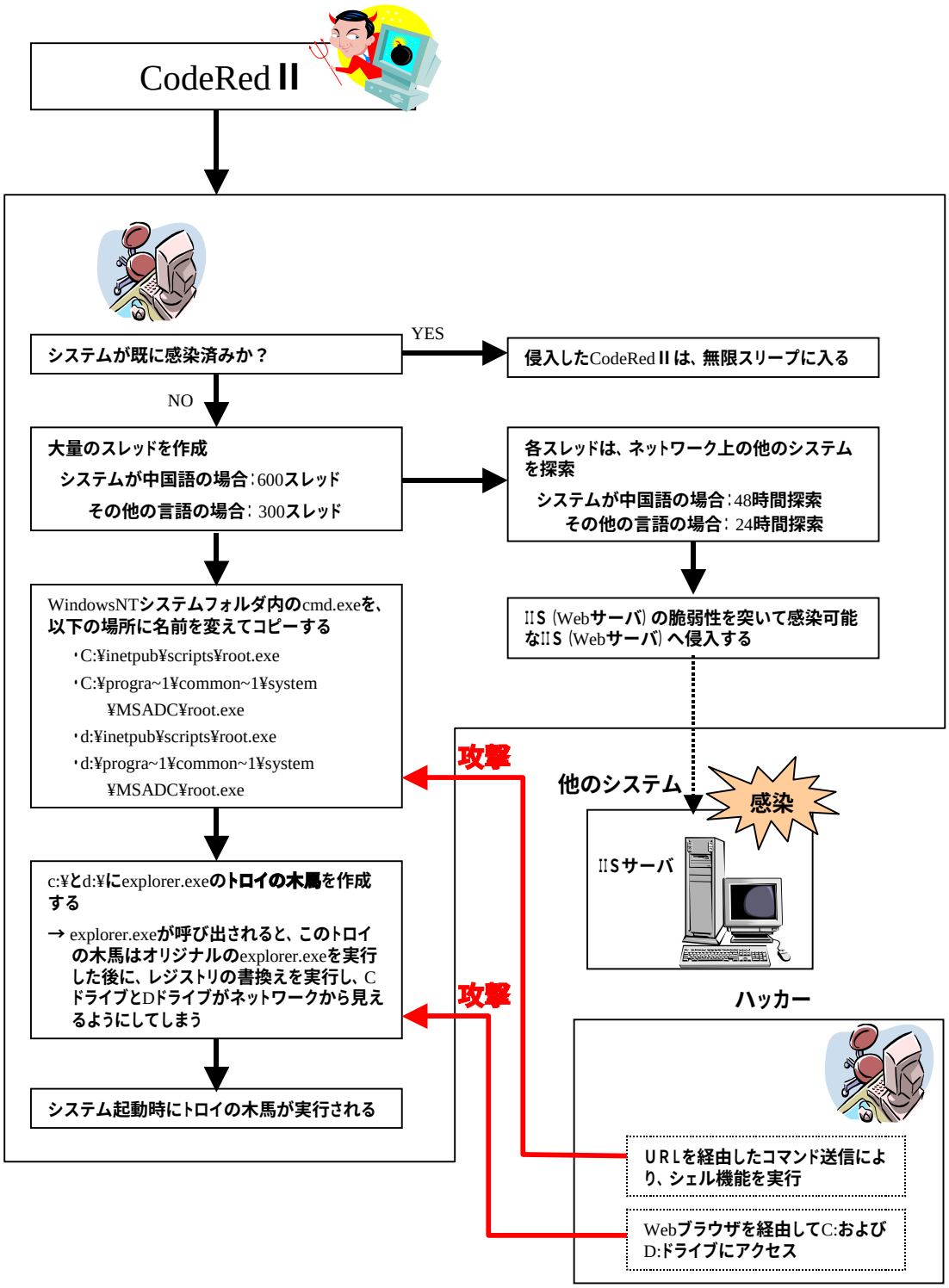

図 2-9 CodeRedⅡのメカニズム&動き

2.3.3.3 報告された被害

CodeRed によって改ざんされた Web ページには、赤い文字で " Hacked by Chinese "等の文字列が表示される。しかし、CodeRedⅡは Web 改ざんを行わず静かに感染するため、人気のある Web サイト等で感染し、被害が大きくなってしまったようである。

2.3.3.4 対策状況

CodeRedⅡの攻撃は既知の弱点を利用したものである。サーバ管理者は、既知の弱点に対する対策を適切に施すことで、安全に運用することが可能である。

また、ウイルス／ワームに関する情報は IPA のセキュリティセンターホームページ上や各ウイルス対策ソフトウェアベンダから脆弱性検査ツール／駆除ツールが提供されており、マイクロソフト社のホームページ上等でセキュリティに関する情報が既に提供されている。また、各ルータベンダからは、ルータに対しての対処に関する情報も提供されている。

また、今後もソフトウェアの脆弱性を狙った亜種が発生する可能性があるため、提供される修正プログラムを迅速に適用していく体制が必要である。

2.3.3.5 得られた教訓

対策として以下の点に留意するとよい。

- ADSL 等の利用により個人ユーザや SOHO で使用されているサーバ（管理されていないサーバ）が感染した場合は被害を増大させる結果になるため、このようなサーバに対しても対応を行うことが必要である。方法としては、パーソナルファイアウォールの導入やセキュリティ対応のブロードバンドルータ導入などが挙げられる。

2.3.4 Nimda（ニムダ）

2.3.4.1 概要

(1) **発生・流行時期**

このワームは、2001 年 9 月中旬に出現が確認された。

(2) **感染の仕方**

このワームは、改ざんされたホームページを見ただけで感染する可能性があるため注意が必要である。また、更にメール機能を悪用して readme.exe という名称の添付ファイルを送信し、そのワーム付メールを受け取ると、Outlook ではメールを開いただけで、Outlook Express ではプレビューしただけでも感染する。

また、ワーム感染や不正アクセスの複数手段を組合せており、クライアントと Web サーバの両方に影響を与える。感染の広がり方は、感染ルートがいくつもあるために複雑になっている。感染方法については、2.3.4.2を参照されたい。

(3) **感染による影響**

このワームに感染した場合、「多大なトラフィックによるインターネットおよび LAN の速度低下」、「CPU 使用率 100%」、「コンテンツの改ざん（スクリプトが追加される）」、「トロイの木馬の設置」などシステムに非常に深刻な影響がある。また、このワームは破壊活動として、ファイルを削除したりハードディスクをフォーマットするなど、使用者や所有者に重大な損害を与えることがある。

2.3.4.2 メカニズム

感染経路は、タイプ別に分類すると以下の4タイプになる。

このワームについては、メカニズムが非常に複雑なため、詳細についてはシマンテック社のサイト（http://www.symantec.com/region/jp/sarcj/data/w/w32.nimda.a@mm.html）等を参照されたい。

(1) **直接感染**

ランダムにクライアント PC へ攻撃を仕掛け、そのクライアント PC へワームのコピーを転送する。

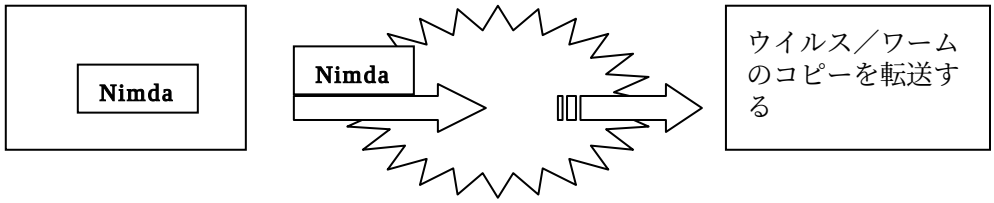

図 2-10 直接感染

(2) Web ページ経由

クライアント PC から、Nimda に感染した IIS（Web サーバ）上の改ざんされた Web ページを見るだけで感染ファイル「Readme.exe」が実行される。

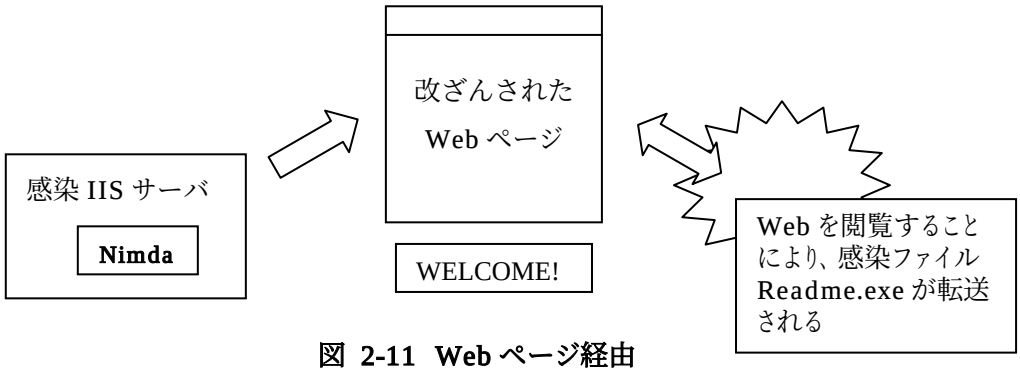

図 2-11 Web ページ経由

(3) ネットワーク共有経由

クライアント PC にワームが侵入すると、全ドライブの全フォルダにウイルス／ワームのコピーを作成し、コピーされたファイルを実行する等により感染する。

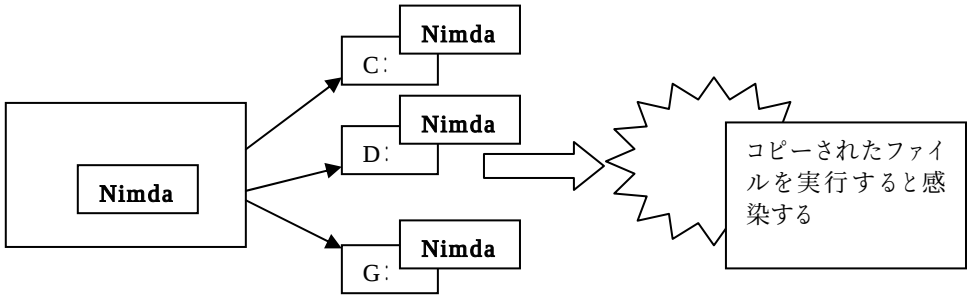

図 2-12 ファイルコピー経由

(4) メール経由

クライアント PC にワームが感染するとそのマシンがワーム付メールを自動送信する。感染パターンは受信側のメールソフトウェアによって次の 2 通りがある。

① 受信したマシンが修正プログラムを適用していないマイクロソフト社の Internet Explorer のコントロールを使用しているメールソフトウェアの場合

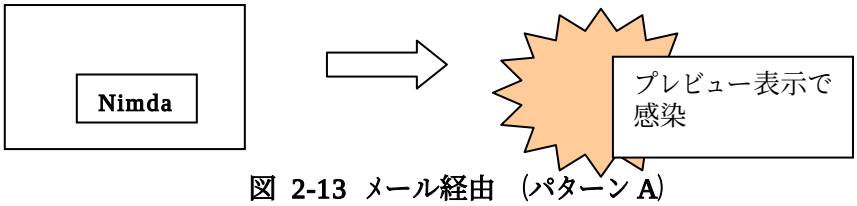

図 2-13 メール経由 (パターン A)

② 受信したマシンが修正プログラムを適用していないマイクロソフト社の Internet Explorer のコントロールを使用していないメールソフトウェアの場合

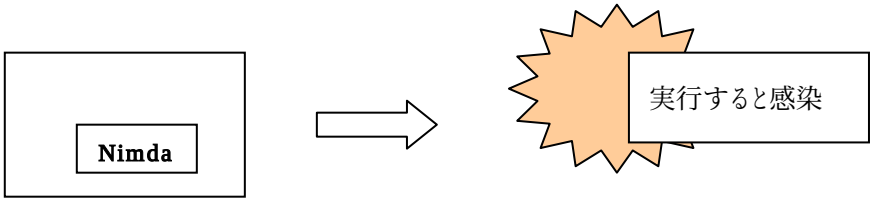

図 2-14 メール経由 (パターン B)

2.3.4.3 報告された被害

新種ワーム Nimda の IPA/ISEC への届出件数は、9 月 26 日現在までで 294 件あり、そのうち実害件数は 189 件 (64.3%) となっている。

2.3.4.4 対策状況

Nimda の攻撃は既知の弱点を利用したものである。サーバ管理者は、既知の弱点に対する対策を適切に施すことで、安全に運用することが可能である。また、サーバ管理者は、常に最新の修正プログラムを適用する必要があると考えられる。

ワームに関する情報は IPA/ISEC のホームページ上や各ワーム対策ソフトウェアベンダから提供されており、マイクロソフト社のホームページでもセキュリティに関する情報が既に発信されている。

しかし、今後もソフトウェアの脆弱性を狙った亜種が発生する可能性があるため、マイクロソフト社からセキュリティ情報を入手し、提供される修正プログラムを迅速に適用していく体制が必要である。

2.3.4.5 得られた教訓

以下の点について心がけるとよい。

- 我々が利用しているシステムは、ウイルス／ワームから潜在的な脅威を受けているため、サーバ管理者は、日常的にサーバの状態を監視する必要がある。
- システム管理者やネットワーク管理者は、最新の修正プログラムに関する情報を定期的にかつ迅速に適用する必要がある。

2.3.5 今後の対策のために

ウイルス／ワームに対する対策は、システム管理者のみならず、インターネットを利用するユーザが、対策を実施することが重要である。しかしながら、まだ対策を十分に実施することに慣れていないユーザが多いようである。下記サイトは、今後の対策のために参考となるサイトである。インターネットを利用するすべてのサーバ管理者やユーザがこれらのサイトを活用し、セキュリティの確保と維持を認識することが望まれる。

- IPA/ISEC
  http://www.ipa.go.jp/security/index.html
- ウイルス対策ソフトウェアベンダ
  トレンドマイクロ㈱ http://www.trendmicro.co.jp/
  ネットワークアソシエイツ㈱ http://www.nai.com/japan/
  ㈱シマンテック http://www.symantec.com/region/jp/
- マイクロソフト㈱のサイト
  http://www.microsoft.com/japan/technet/security/ (TechNet セキュリティセンター)
  http://www.microsoft.com/japan/enable/products/security/
  (ホームユーザ向けセキュリティ対策 早分かりガイド)

3 セキュリティ対策技術と対応製品の最新動向

3.1 セキュリティ対策技術マップ

これまでに述べてきた、不正アクセスやウイルス／ワームからの情報セキュリティ上の脅威を含め、情報システム設備の盗難や情報システム／サービスの運営上、情報の漏洩が、故意あるいは過誤より発生することもある。

こういった情報システムのセキュリティに関わる被害を防ぐためには、セキュリティポリシーの策定からリスクの洗出し・評価、および対応策の策定・実行、セキュリティポリシーや対応策の見直し等、情報セキュリティマネジメント全体として捉えることが必要であり、その他にも、制度や法律による対応等が考えられるが、本章では、その中でも特に、技術による対応について考察する。

情報セキュリティ対策を行うための技術は、大きく以下の4区分に分かれる。

1) 脅威に対する警戒のためのもの
2) 脅威を予防するためのもの
3) 脅威を監視するためのもの
4) 脅威による被害から復旧するためのもの

そこで、脅威について分類を行い、脅威とその脅威に対する対応技術との関係を整理してみた。その結果を表 3-1に示す。

この表に示されている対応技術の中から、テーマを下記の5つに絞り、各テーマ毎に技術体系と技術概説、最新トピックスと動向および今後の課題について、3.2以降で触れていく。

＜テーマ＞

- 認証技術
- 不正アクセス対策
- データの保護技術
- ウイルス対策技術
- 通信の保護技術

表 3-1 脅威と対応技術

脅威の区分	脅威	攻撃手段	対応技術			
			警戒	予防	監視	被害からの復旧
取引相手による契約にかかわる脅威	ログイン時の認証に関わる成りすまし･否認拒否	･成りすまし ･否認拒否		･ワンタイムパスワード、生体認証を利用した電子認証 ･ICカードを利用した電子認証		
	特に、リモートからの認証に関わる成りすまし、否認拒否	･成りすまし ･否認拒否		･PKIの利用		
通信にかかわる脅威	情報の漏洩	･盗聴情報の解読		･通信データの暗号化技術の導入 － SSL － IPSec － Kerberos		
	改ざん･破壊	･盗聴情報の改ざん、破壊		･通信データの暗号化技術の導入 － SSL － IPSec － Kerberos など		
サイトの内外部からのサイトシステムへの攻撃	システム内情報（ﾃﾞｰﾀ、ﾌﾟﾛｸﾞﾗﾑ）の ･不正取得 ･漏洩 ･改ざん ･破壊 他サイト攻撃への踏み台化	･権限のない者によるシステムへの不正なアクセス	･ログ解析ツールの利用 （ﾛｸﾞ監視、統計ﾃﾞｰﾀ作成）	･ファイアウォールの利用 ･セキュアOSの利用	･IDSの利用 （ﾈｯﾄﾜｰｸ監視、ﾎｽﾄ監視）	･ファイル改ざん検知ツールの利用 （ﾊﾞｯｸｱｯﾌﾟﾃﾞｰﾀからのﾌｧｲﾙﾘｽﾄｱ時の検証）
		･権限のない者による、システム内データへの不正なアクセス	･ログ解析ツールの利用 （ﾛｸﾞ監視、統計ﾃﾞｰﾀ作成）	･データの暗号化技術の導入 ･電子透かし技術の導入 ･DBMS ･脆弱性診断ツールの利用		
		･セキュリティホールの利用	･ログ解析ツールの利用 （ﾛｸﾞ監視、統計ﾃﾞｰﾀ作成） ･ネットワークトラフィックの解析	･脆弱性診断ツールの利用 ･ファイアウォールの利用	･IDSの利用 （ﾈｯﾄﾜｰｸ監視、ﾎｽﾄ監視） ･ファイル改ざん検知ツールの利用	
		･ウイルス／ワーム		･ウイルス対策ソフトの利用	･ウイルス対策ソフトの利用	･ウイルス対策ソフトベンダから出される復旧用プログラム
	サービス運用妨害	･DoS攻撃	･ログ解析ツールの利用 （ﾛｸﾞ監視、統計ﾃﾞｰﾀ作成）	･ファイアウォールの利用 ･ウイルス対策ソフトの利用	･IDSの利用 （ﾈｯﾄﾜｰｸ監視、ﾎｽﾄ監視）	
設備の盗難	記憶媒体上にある情報の漏洩	･パソコン、HD、CD-ROM、FD等の盗難		･データの暗号化技術の導入 ･データ完全消去を行うソフトウェアの利用 ･盗難防止用ワイヤーロックの利用		
業務運営にかかわる脅威	情報の漏洩	･業務関係者の過誤、恣意		･二重入力方式や、確認画面使用による入力過誤の防止		

3.2 認証技術

3.2.1 認証に関する技術体系

現在利用されている認証方式は ID･パスワード方式が主であるが、この方式には以下のような問題点がある。

- パスワードを知られたら、成りすましは自由である。
- パスワードを知る方法は無数にある。
- 本人は成りすまされていることに気づかない。
- システム的に異常を検知する仕組みがなければ、管理者さえも気づかない。

今後認証の重要性がますます高まるにつれ、認証に関するセキュリティ対策が必要となる。通常の ID･パスワード方式よりもセキュアな認証技術を目指した方式としては、以下のようなものがある。

- ワンタイムパスワード
- 公開鍵暗号方式
- バイオメトリクス認証

以下では、これらの方式について概説する。

3.2.2 個々の技術の概説

3.2.2.1 ワンタイムパスワード

ワンタイムパスワードは、使い捨てのパスワードを生成する「トークン」と、認証を行う認証サーバから構成される。認証方式は、乱数を使用する「チャレンジ＆レスポンス方式」とトークンと認証サーバが生成前のカウンタなどのデータを同期させる「同期方式」がある。チャレンジ＆レスポンス方式は、サーバで生成する乱数（チャレンジメッセージ）を用いて、クライアント側で入力されたパスワードとチャレンジメッセージを演算することにより一度限りのパスワードを生成する方式であり、同期方式は、クライアント側のトークンで、時刻またはカウンタと同期をとりながら“使い捨て”のパスワードを生成し、認証サーバで認証を行った後に一度使用したパスワードを破棄する方式である。いずれにせよパスワードを盗まれても、同じパスワードでは二度とアクセスできないため、セキュリティ強度は高まる。

製品としては、Security Dynamics 社の「SecurID」や Secure Computing 社の「SafeWord」などが代表的である。

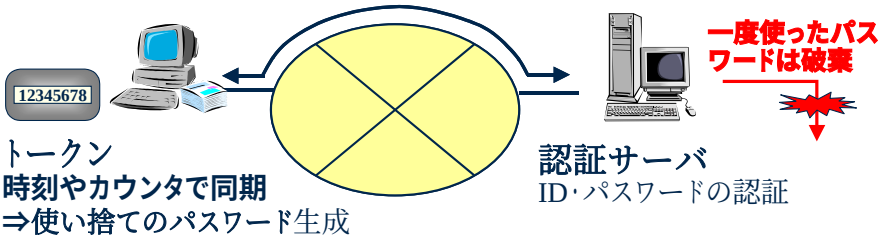

図 3-1 同期方式（ワンタイムパスワード）

3.2.2.2 公開鍵暗号方式

公開鍵暗号方式は、データ暗号化方式の1つであり、認証に用いられる技術の1つである。この方式では「公開鍵」と「秘密鍵」の2種類の鍵が利用され、以下の特性を持つ。

- 「秘密鍵」で暗号化したものは、「公開鍵」でしか解読できず、「公開鍵」で暗号化したものは「秘密鍵」でしか解読できない。
- 「秘密鍵」は、それを生成した所有者が安全な場所に保管し、他人には一切公開しない。一方、「公開鍵」は公開しておく。
- 「秘密鍵」は本人しか所持しておらず、かつ「秘密鍵」で暗号化したものは「公開鍵」でしか解読できないことから、認証基盤として利用できる。

SSL のクライアント認証では、この公開鍵暗号方式を利用している。

ユーザは個の秘密鍵を安全に保管する必要があり、保管方法として、対タンパ性（※注）を持つ IC カードに秘密鍵を格納するのが現在のトレンドである。ただし、所有者と IC カードの間の認証は、存在しないか、PIN による認証がほとんどである。

今後、重要性が高まるにつれ、所有者と IC カード間の認証に、バイオメトリクスを利用した製品が出てくると思われる。

（注）対タンパ性：悪意を持った者が不正な手段によって情報を読み取ろうとしても、それを阻止する性質を指す。

3.2.2.3 バイオメトリクス認証

顔や声など人間の生体的特徴を抽出して数値化することをバイオメトリクス（ Biometrics：計量生物学、生物測定学）といい、そのような人間の生体的特徴を利用して本人確認をすることを バイオメトリクス認証という。現在利用されている代表的な方法には次のようなものがある。

- 指紋

  それぞれの指紋に固有の特徴点（隆起、分岐点など）を抽出し、この抽出した情報を元に本人認識を行う方法
- 顔貌

  カメラ撮影等で入力した顔の特徴データを元に、本人認識を行う方法
- 音声

  それぞれの声紋をデジタル化し、個々の声紋と照合して本人認識を行う方法
- サイン

  署名の特徴点（スピード、筆圧、ストロークなど）を解析し、照合する方法
- 虹彩

  眼球内の虹彩の違いを判別することで本人認識を行う方法
- 掌形

  掌の全体的な形や指の長さ・太さなどにより、本人認識を行う方法

バイオメトリクス認証では他人が成りすますことが実質不可能であり、更には、認証を行うために物を携帯する必要がなく、パスワード等を記憶する手間もないため、今後はあらゆる認証に利用されるであろう。

バイオメトリクス認証は現在も利用されているが、導入するためには高価な装置が必要であり、また認証情報（個人情報）の保管の難しさから、最重要である入退室管理、PC へのログインなどのオフラインの用途が主となっている。

今後は公開鍵暗号方式を補完する認証方式として、利用されてくるものと考えられる。

また、バイオメトリクス全般に言えることだが、身体障害、外傷、病気等によって認証精度が左右されたり、認証そのものが不可能な場合があり、まだ発展段階にある技術と言ってよい。広く浸透するためには、複数のバイオメトリクス認証方法あるいは他の認証方式との組合せが必要である。

3.2.3 技術・製品に関する最新トピックス、動向

3.2.3.1 BioPassword

ログイン時の ID・パスワードのキー入力のリズムから、複合的に本人を認証できる。ID・パスワード方式のセキュリティ強度を比較的安価に若干強化できる製品もある。

＜参考サイト＞

http://biopassword.com/

3.2.3.2 マウスの握り方で常時本人確認

マウスをクリックするたびに、マウスの握り方をチェックして本人認証を行う。ログイン時だけでなく、操作している間、認証をし続ける。

日経インターネットテクノロジー　2002.1　pp.18-20

3.2.3.3 カードリーダ不要のカードによる認証

カード情報を暗号化し、音にして発信する機能を持っている。発信された音データは、マイクの搭載してあるパソコンや携帯電話等のインターネット接続端末によって受信、暗号化され、インターネット上の認証局にて認証を受ける仕組みとなっている。

＜参考サイト＞

http://www.marubeni.co.jp/news/nl/nl010402.htm

3.2.3.4 デジタル証明書対応指紋認証装置

指紋読み取り装置内にデジタル証明書を格納し、公開鍵暗号方式で認証を行う。

＜参考サイト＞

http://www.sony.co.jp/Products/puppy/index.html

3.2.4　今後の課題

ログイン時の認証をいくらセキュアなものにしても、その後もログインした人間が、使い続けているかどうかを確認する方法がない。本人がログオフせずに席を離れても、第三者がその端末に近づけないような環境や運用ができていれば問題はないのだが、それを実現することは結構大変である。

例えば、端末に向かっている間、一定時間間隔ごとにリアルタイムで本人を認証し続ける仕組みも、今後検討が必要であると考えられる。

現在、マウスの握り方を利用して、クリックするたびに認証を行うようなものも研究レベルでは存在している。また、前記キー入力のリズムから認証を行うものもリアルタイム認証に応用可能だと考えられる。

3.3 不正アクセス対策

3.3.1 不正アクセス対応技術

3.3.1.1 不正アクセスの定義

1999 年 8 月 6 日に成立、2000 年 2 月 13 日に施行された「不正アクセス行為の禁止等に関する法律」、通称不正アクセス防止法によれば、不正アクセスとは以下のような行為をさす。

- 他人の ID・パスワードを無断で使用
- セキュリティホールを利用して侵入
- 他人の ID・パスワードを無断で第三者に提供（販売・掲示板などでの公開・口頭伝達）

現在一般的に不正アクセスと呼ぶときにはこの定義を用いることが多いが、この定義には「不許可（無権限）アクセス」と「許可（権限）の濫用（他人が使用することを含む）」が混在している。不正アクセス対応技術の面から見ると、正規の ID・パスワードを使用して正常手順でアクセスしたセッションは、それが「許可（権限）の濫用」であることを判断して何らかの対処を行うことは原理的に不可能である。従って、今回の調査における「不正アクセス」とは、「不許可（無権限）アクセス」に限定し、許可されていない者・物（人間とは限らない）が情報システムにアクセスを行うこととする。なお、不正アクセス防止法では不正に情報にアクセスする行為が成功した場合にのみこの法律が適用されるのであり、不正に情報にアクセスしようとしても未遂の場合には罰則の対象とならない。この点もこの法律の不備な点として指摘されている。

なお、より広義の意味では「インターネット上を流れるデータを傍受する」という行為も不正アクセスと呼ばれる場合があるが、ここではそれを含めない。

3.3.1.2 不正アクセス対応技術の概説

(1) ファイアウォール

不正アクセス対応技術としてファイアウォールと呼ばれる機能・装置をインターネットと LAN との接続点に置き、公開しないサービスのポートに対するアクセスを遮断したり、特定の IP アドレスからのアクセスを拒否したりすることができる。

ファイアウォールの機能には上述のように IP レベルのフィルタリング機能、ポートレベルのフィルタリング機能の他に AP レベルのフィルタリング機能（ゲートウェイ機能）がある。実際の製品はこれらの機能が複合していることが多い。

新しいファイアウォール技術としては後述する侵入検知システムと連動してダイナミックにセ

ッションを切断する技術等がある。

ファイアウォール技術だけでは、セキュリティホールを突いた攻撃や DoS 攻撃、ウイルス／ワームによる攻撃等に対する対処等に限界があるため、他の手法と組合せて不正アクセスへの対処を行うことが望ましい。

(2) 侵入検知システム（IDS）

侵入検知システム（IDS）とは、知識として保持する不正アクセスの攻撃パターンと合致する攻撃を検知したときに警告を発したり、場合によっては通信を阻止したりするシステムである。ネットワーク上に流れるパケットを監視する「ネットワーク監視」とサーバ上のシステム監査ログなどを監視して不正な行動を検知する「サーバ監視」、およびその両方を行う「ハイブリッド型」がある。不正アクセス攻撃やセキュリティホールは日々新たに報告されている（※注）ので、常に検索パターン（シグネチャ）を最新に保つ必要がある。ちなみに、ある製品では現在 1,200 個以上のシグネチャを保持し、1日1個の割合でシグネチャを追加しているとのことである。

また、通常と異なる通信パターンを統計的に検出して警告を発する機能を有する製品もある。シグネチャとの比較によって検出する機能を「不正検出」と呼ぶのに対して正常と異なるアクセスの振舞いを検出する機能を「異常検出」と呼ぶ。異常検出方式は不正検出方式と比べて処理が複雑でハードウェアに高い処理能力が求められる傾向があるが、シグネチャの更新が不要という利点がある。ただし、異常のパターンと正常のパターンの境界を明確に定義することは困難であり、これは今後の課題でもある。

IDS によって不正アクセスの検知を行ったとしても、不正アクセスに対する迅速な対応を IDS 導入の目的とする以上は、検知後の対応を行う手順や体制を明確にしておくことが必要である。

注：Common Vulnerabilities and Exposures（CVE）はセキュリティホールの情報などを一元的に共有する目的で運用されており、一般に公開されている。http://cve.mitre.org/を参照されたい。

(3) セキュア OS

セキュア OS とは、一般の OS をセキュリティ的に強化し、外部から不正アクセスの攻撃などを受けても簡単には破れないようにした OS である。

例えば、OS が管理するメモリ空間を保護すべきエリアとそれ以外のエリア等に分け、OS のコア部分やアプリケーションの実行部分などを保護エリアに置いて外部から万一の侵入を受けても OS そのものやアプリケーションに被害が及ばないようにしている例や特権ユーザの権限を制限している例などがある。

導入実績としては、オンラインバンキング、国内官庁系、認証局などが挙げられる。

セキュア OS は一般の OS に比較してかなり高価ものもあるが、不正アクセスから保護すべきシステムには積極的な採用が望まれる。

(4) その他

その他、不正アクセス対応技術としては次のようなものがある。

- ルータでアクセス可能な IP アドレスを制限する。
- Web サーバのコンテンツが改ざんされた場合、そのことを検知したり、バックアップからデータ復旧を行う技術（3.4.3.3を参照）。
- 他の Web サイトから ActiveX や Script 言語によって不正なマクロやワームなどを送り込まれないようにゲートウェイで保護する技術（3.5.3.2を参照）。

3.3.1.3 技術／製品に関する最新トピックス、動向

(1) **ファイアウォール**

ファイアウォール技術としてはセッションの通信履歴を管理して動的にフィルタリングを行う機能も実装されつつある。また、ファイアウォール装置そのもののセキュリティレベルの向上が図られている製品もある。

代表的な製品は CheckPoint 社の FireWall-1 である。FireWall-1 の最新バージョン NextGeneration が 2001 年 8 月に発売開始されている。

最近はファイアウォール技術そのものの進化よりも、周辺機能（負荷分散、二重化、多数のファイアウォールの統一管理、VPN 等）が充実してきている。また、ブロードバンドの普及により、サーバだけでなく個人の PC への不正アクセスを防止したり、個人情報の流出を防止するためのパーソナルファイアウォールの需要が高まっている。

(2) **侵入検知システム**

最も普及している製品は、インターネットセキュリティシステムズ（ISS）社の RealSecure である。

ISS 社は RealSecure を核としたセキュリティ監視サービスも提供しており、最近こうしたサービスの需要が高まっている。

侵入検知システムは通信パケットすべてをチェックするため、一定の通信容量を越えるとパケットすべてをチェックすることができなくなる。今後ネットワークが広帯域化するにつれこれが大きな課題となると考えられる。

(3) **セキュア OS**

商用のソフトウェアとして、代表的な製品は、下記のとおりである。

- マルチプラットフォーム （UNIX、Windows、Linux 等） 対応
  eTrust Access Control （コンピュータ・アソシエイツ）

- UNIX 対応

  Trusted Solaris （サン・マイクロシステムズ）

  Virtual Vault （ヒューレットパッカード）

  Pit Bull （アーガス・システムズ・グループ）

(4) **その他**

近年、ウイルス／ワームがメールを通じて蔓延する事象が多発しているため、インターネット経由で送受信するメッセージの内容をチェックし、ウイルスを発見した場合にエンドユーザに配信される前にブロックするメールゲートウェイ製品が登場している〔3.5.3.1を参照〕。また、メールによる機密情報流出に対応するため、メールフィルタリングソフトウェアも発売されている。

3.3.1.4 今後の課題

不正アクセス防止法では、許可された人間がその権限を悪用したり、その人の ID･パスワードを無断で使用して情報を漏洩したりする事象も含むが、今回の不正アクセス対策技術の調査ではこれを除外した。ファイアウォールもIDSもセキュアOSも正規ユーザが正規手続きで情報にアクセスすることを拒むことはできない。しかし、現実に最も多大な被害を及ぼす脅威はまさにこのような不正アクセスなのである。従って、これら技術的対策が不可能な脅威に対しては組織としてのセキュリティポリシーの策定、セキュリティ教育の徹底、罰則規定の強化等組織的、運用的な対策が必須である。

また、IDS のシグネチャの更新や OS のセキュリティ修正プログラムの適用等についてもリリース後可及的速やかに実行する体制を構築する必要がある。しかし現実にはセキュリティ修正プログラムを適用すると今まで動作していたアプリケーションが動作しなくなる等の問題があって、うまく行っていない例が多い。これらの点も課題といえる。

＜参考サイト＞

http://www.forescout.com/whatwedo.html

3.3.2 脆弱性診断

3.3.2.1 脆弱性診断の定義

脆弱性診断技術は「情報システムのみを対象として脆弱性を診断する」と言う意味と、「その組織のセキュリティポリシーおよび組織のセキュリティに対する意識、情報システムのセキュリティ対策および制度上の対策までを含めてその組織における情報資産に対するセキュリティレベルを診断す

る」と言う広義の意味がある。今回の調査では前者の意味に限定する。

3.3.2.2 脆弱性診断の種類

脆弱性診断は、ネットワークを経由して不正アクセス攻撃に対する防御力を診断するネットワーク診断と、サーバ上でセキュリティホールの有無を調査するホスト診断の二種類がある。どちらも既に報告されている攻撃方法をシミュレーションして既に対策がとられているかどうかを診断するものであり、未知の攻撃に対する脆弱性を診断することはできない。攻撃方法やセキュリティホールは日々新たに発生しているため、常に最新の技術が求められているという点については侵入検知システムと同様である。

3.3.2.3 技術動向

脆弱性診断ツールには下記のものがある。

- Internet Scanner、System Scanner （ISS㈱）
- eTrust Content Inspection （コンピュータ・アソシエイツ㈱）
- NetRecon、Enterprise Security Manager （㈱シマンテック）
- HFNetChkPro （シャブリック・テクノロジーズ）

ただし、脆弱性診断の場合は診断サービスを提供しているベンダが多い。診断サービスの内容は上記のツールを用いてレポートを作成するレベルから実際に攻撃者と同様の攻撃を仕掛けて診断を行うものまで様々である。

また、無線 LAN 環境での脆弱性診断ツールも登場している。無線 LAN は、最近その利用が広がりつつあるが、その一方で許可されていない者からのアクセスされる機会も増えるものと考えられる。無線 LAN 環境対応の脆弱性診断ツールにより、例えばアクセスポイントの脆弱性や設定のチェック等を行うことによってこういった脅威にも対応することができる。

脆弱性診断ツールというと、脆弱性の診断を行うだけのものが大半であるが、中には脆弱性に対する修正プログラムの適用までを行ってくれるツールもある。例えば、未適用の修正プログラムがあればネットワーク内のマシンに対してプッシュ型で配信する機能を備えた製品も登場している。

また、Web に特化した脆弱性診断ツールも製品化されている。

3.3.2.4 今後の課題

脆弱性診断は、診断ツールによる診断に加え、攻撃者に匹敵する不正アクセス技術を駆使してセキュリティホールが無いかどうかを診断するサービスを求められている。しかし現実にはそのような診断を行うことのできる技術者は限られており、仮に技術者を確保できたとしても診断を行うコストはかなり高額になる。また、診断した結果発見された脆弱性をすべて改善したとしても未知のセキュリティホールが無いことを保証することはできない。そういった意味で、現状ではどのレベルまでコストをかけるかを判断するためにリスク分析を行う必要がある。また、脆弱性診断ツールは常に最新のものを用い、定期的に実施する必要がある。これらサービスの効率的な実施が今後の課題と言える。

3.4 データの保護技術

3.4.1 データの保護に関する技術体系

3.4.1.1 データの種類による分類

まず、ここで議論を進めるにあたり、扱うデータを定義する必要がある。不当な利用が困難である仕組みが施されているべきであるデータは、以下の2つに分類できる。

1) 公開･流通情報
- 情報の存在および内容概要は誰もが簡便に知り得る
  （映画の予告編、CD のビデオクリップなど）
- 情報自体の取得は自由に行われる
- 情報の利用は、正当な利用条件の確認・認証を経た上で、可能な限り自由に、かつ簡便に行われるべきである

2) 機密情報
- 情報の存在自体を特定の利用者以外に対して秘密にしておくことが望ましい
- 正当な利用者は、セキュリティ確保のためのある一定の手順を経て、情報にアクセスする

この2つは、その性格の違いから適用されるべき保護技術に異なる部分があると考えられるため、保護技術についても分けて考えるべきである。なお、この両者は関連して運用される場合もあり得る。例えば、公開･流通情報である映画本体と、機密情報である映画利用権（暗号化された映画を復号する鍵など）というように一体として機能する例も一般的である。

3.4.1.2 運用シーンによる分類

どのような場面で情報が保護されるべきかによって技術は、以下の2つの体系に分けて考えられる。

1) ファイルシステム／データベース（DB）関連技術
- 主に記憶媒体／装置内におかれた状態でのデータについての保護を目的とするもの
- 業務用情報管理および保存のため、従来から検討されて来た歴史を持ち、現時点である程度実績があると考えられるもの

2) デジタル情報流通関連技術

- 主に有線／無線のネットワーク、あるいは放送による伝送路上でのデータの保護を目的とするもの
- 文書およびコンテンツのデジタル化、およびネットワークの高速・大容量化に従って近年急速に関心を呼んでいる、ネットを介したデジタル情報流通ビジネス関連技術

以上の分類によって、4種のセグメントに体系づけて検討を行う。

3.4.2 個々の技術の概説

上記3.4.1で4種のセグメントに分類できることを示した。以下では、それぞれに属する技術を検討する。

3.4.2.1 ファイルシステム／DB 上での公開・流通情報

このセグメントにおいては、他に比較して大量の情報が対象となる。他にも共通するものを含めて、このセグメントにおける技術を列挙し、説明する。

(1) 暗号化

情報をある特定の鍵で暗号化し、移動あるいは保存させた後、利用時に鍵を持っている者のみが復号して利用に供することができる。

暗号方式は各種提案、運用されているが、大別すると共通鍵方式（暗号時と復号時に用いる鍵が共通）と公開鍵方式（暗号時と復号時に用いる鍵が対をなす、異なる鍵）に分類できる。

ここで、このセグメントに適する暗号方式は、主に共通鍵方式である。これは、扱うデータ量が比較的大規模であり、利用時の復号が高速に行われるべきであることから、暗号／復号処理速度の面から共通鍵方式が有利と考えられるからである。

具体的な共通鍵方式としては、従来、DES（Data Encryption Standard）が広く用いられてきたが、鍵長が実質 58 ビットであることからコンピュータの高速化によって全数探索法が現実的な脅威となってきた。そのため、近年、次世代の標準方式として鍵長を 128 ビットする AES（Advanced Encryption Standard）が提案されており、今後この標準方式が普及していくことが予想される。

(2) 電子透かし

原情報に、ある特定の手段によって著作権者等の別情報を埋め込み、利用時あるいは検証時にある特定の手段によって埋め込まれた情報を取り出し、著作権者の確認等を行う。例えば原情報のヘッダに著作者情報等の管理情報を付記する方式に比較して、電子透かしでは両者が一体化されているため、著作者情報のみの改変等が困難である。

広く知られており、かつ利用されている例が多い技術としては、埋め込まれた情報が人間に知覚できにくく、埋め込まれた情報が壊れにくい（情報全体を細切れにするなどの加工をした後でも、埋め込まれた情報が取り出せる）という特徴を持つ方式がある。

この方式のみを電子透かしとする意見もあるが、技術的分類としては、この方式を含んで4種類の技術がある。それぞれの代表的使われ方の概要を列挙する。

なお、原情報としては静止画像、動画像、音楽、テキスト等種々が考えられるが、現時点で最も普及しているのは静止／動画像を対象としたものである。

- 不可知で壊れにくい
  原情報の著作権者を埋め込み、不正なコピーを抑制する
- 不可知で壊れ易い
  画像に作成時刻、作成者等を埋め込み、後で完全に取り出せることで改ざんされていない証拠とする
- 可知で取り外しが可能
  画集の絵に「サンプル」と印字して無償で広く配り、内容概要を知ってもらえる
  実際の利用には「サンプル」の字が邪魔であるため、利用したい場合には正規に利用権を購入してもらい、その利用権を用いて印字を消し去る
  また、この可知透かしを消し去る際に不可知透かしを生成、埋め込む作業を同時に行うことも、その後の不正利用抑制に有効な方式として提案されている
- 可知で取り外せない
  ニュース映像に半透明のロゴを一体化して入れる（米国の TV ニュース映像として実運用）ことで、容易に著作権者を判定でき、不正な再利用や販売を防止する

このセグメントにおいては、上記4種類すべてが適用可能であるが、主に、最初の“不可知で壊れにくい方式”が使われている。この方式における技術要件は以下の通りである。

- 原情報は別情報の埋め込みによって、ある程度のノイズを受けるが、そのノイズから別情報の内容を知ることは技術的に困難であること、かつ、そのノイズが許容範囲内であること（原情報との差分が極めて小さいこと）
- ディジタルコピー直後はもちろんであるが、ある程度の編集や加工、例えば一部の切り取り、デジタル→アナログ→デジタル変換（画像をプリントアウトし、スキャナで読み取るなど）などを施した後でも、ある特定の手段によって埋め込まれた情報が取り出せる

これらの要件を満足させるため、種々の方式が提案されている。原情報が画像である場合、画像情報に周波数変換（DCT、FFT、wavelet など）を施し、変換後の情報に対して透かし情報を埋め込む方式が各種実用化されている。この処理は、原情報に直接埋め込む方式に比較して重くなるが、画像の加工／圧縮等の攻撃に対する耐性に優れている。

＜参考＞

http://www.ist.fujitsu.com/sukashi/index.html

(3) **機密情報との一体化**

公開･流通情報利用時に、その公開･流通情報に付随する機密情報の内容を確認、あるいは利用することが、上述した映画再生等でしばしば行われる。そのため、公開･流通情報と機密情報の両者のリンクを保護することが重要になる。

このリンク管理を、ファイルシステムレベルで実現し、高いセキュリティ性を保証する方式が標準化された。画像等のコンテンツを扱うファイルシステムとして一般化が進んでいるUDFv2.0 に拡張を加えた UDFv3.0（セキュア UDF；Universal Disk Format）が、この標準化方式である。

セキュア UDF では、コンテンツに対して、その属性情報等をファイルシステムレベルで関連付けて関する方式であり、その関連情報はアプリケーション層からは改変等が困難であることから、高いセキュリティレベルを保つことが可能である。このセキュア UDF は、2001 年度に JIS 化された。

また、上述した電子透かしの方式を用いて、原画像に機密情報を埋め込むことで一体化することも検討されている。この場合は、機密情報量に制限がつくこと（大量情報の埋め込みは原画像へのノイズが大きい）、透かし情報読み出し後の運用上の機密性維持が問題として存在し、実用化のための課題となっている。

＜参考＞

http://www.oitda.or.jp/jislist-j.html

3.4.2.2 流通過程における公開・流通情報

最近のネットワーク（有線、衛星放送を含む無線）の高速大容量化に伴い、このセグメントの重要性が増している。つまり、映画等のコンテンツをテープ、ディスクに入れて販売、配布するのではなく、ネット経由で自由にやりとりすることが広く行われるようになってきた。

このセグメントにおいては、自由に情報をやりとりすることが要件であるため、特に保護すべき対象とはならないと考えることができる。しかしながら、情報自体を改ざんされたり、不正利用されたりすることは防止すべきである。従って、「3.4.2.1ファイルシステム／DB 上での公開･流通情報」で述べた暗号･透かしの技術が必要となる。

なお、通信全般の保護技術については、3.6にまとめて解説してあるので、そちらを参照して頂

きたい。

3.4.2.3 ファイルシステム／DB 上での機密情報

このセグメントにおいては、攻撃対象となるデータの存在場所がある程度特定できてしまうため、強固な保護が重要である。

(1) 暗号化

ここでの暗号化は、先に述べた共通鍵方式に加えて、公開鍵方式を用いることが多い。その理由としては、扱うデータ量が比較的少ないので、暗号／復号処理の遅い公開鍵方式でも致命的なネックとはなり難いこと、後で述べる認証にも関連してくるが、鍵の搬送および検証性に優れていることが挙げられる。

具体的な公開鍵方式としては、RSA が一般的であるが、近年、RSA より短い鍵長で同等の機能および強度を持つと言われる楕円曲線方式も注目されるようになってきた。

(2) 機密領域管理

記憶媒体あるいは記憶装置内において、アプリケーションあるいはユーティリティソフトからアクセス不可能な領域を確保し、通常のユーザが操作不可能なレベル、具体的にはファイルシステムレベル等からのみアクセスさせる方式の採用が始まっている。この領域に、機密情報本体、あるいは、通常領域においた（暗号化されている）機密情報を復号する鍵を保持することで高いセキュリティを維持する。

具体的例としては、上述のセキュア UDF を光磁気ディスクに実装する方式として採用されている。

(3) 完全性／原本性保証

記憶されている情報が、格納時と同じ内容であることを保証する、あるいはどこからか不正にコピーされてきたものでないことを保証する技術である。

ここで用いられる方式としては、以下のものが挙げられる。

① 電子署名

情報全体からメッセージダイジェストと呼ばれる一定長のデータを生成し、そのデータを公開鍵方式の秘密鍵で暗号したものを電子署名と呼び、これを元情報に付属させる。

情報内容検証時に、再度、情報全体からメッセージダイジェストを生成し、保存されていた電子署名を公開鍵方式の公開鍵で復号したものと比較し、両者が一致すれば元情報は改ざんされていないと証拠付ける。

ここで、メッセージダイジェストから元情報を再生できないことが重要であり、これは一方向性関数と呼ばれる技術を用いることで解決する。

一方向性関数としては SHA-1 と呼ばれる方式が一般的である。

② ログ管理

情報記憶の際、あるいは更新等の処理の際、「誰が」、「何時」、「どのような処理を」、「何に対して」、「どのように行ったか」、などのログ管理情報を装置内部で生成し、元情報とともに管理する。

この管理情報を上記の機密領域に保持し、必要に応じて参照または検証することにより、時系列を追って情報の履歴を検証することができる。

装置内部で管理情報を生成する際、装置固有の秘密鍵等の秘密情報を使用することで検証の信頼性は高くなるが、この秘密情報の装置内での管理が課題となる。これについては、専用のハードウェア内に保持し、開封などの攻撃の際に自動的に情報を消滅させる方式などが提案されている。

③ データ修復

何らかのトラブル時に、不正に利用されないことを確認、保証した上で修復する技術である。従来から、冗長情報を付記することで破壊された情報を修復する技術は多数開発され、実際に使用されてきた。しかしながら、3.4.4の今後の課題の項でも述べるが、不正に利用されないことの確認、保証は非常に難しい問題である。

特に、このセグメントで扱う機密情報は、例えば映画の利用権等のユーザが購入した権利情報に代表されるように、修復できることが絶対条件であり、かつ、不正を起こさせる動機があるという状況にある。

具体的な方式としては、ユーザ、あるいは利用環境を特定できる情報を元に、データを再交付する方式が用いられることが多い。しかしながら、この方式においても、プリペイド情報の修復の必要が生じた場合への対処方法としては、不正行為排除が完全に可能とは言い難い。

④ 所有者認証

①電子署名でも述べたように、公開鍵、秘密鍵を用いた公開鍵方式による認証が一般的になりつつある。これは PKI（Public Key Infrastructure）と呼ばれる方式に則ったものである。公開鍵を認証局に登録し、証明書を発行してもらうことで、その公開鍵と対をなす秘密鍵の所有者の確認が可能になる。これをもとに、機密情報の正当な所有者であるか否かの認証を行う。

PKI の詳細については、3.6.2.4を参照されたい。

3.4.2.4 流通過程における機密情報

このセグメントにおいては、オープンなネット上を重要な情報が流れることによって、不正を行おうとする悪意を持った者の目にさらされるという点から、厳密な保護技術が必要とされる。

このセグメントにおける保護技術としては、上記3.4.2.3で述べた技術のうち、機密領域管理を除くすべての技術が必要となり、これに加えて更に下記の技術が必要となる。

(1) 相互認証

上述の所有者認証では、PKI に基づく電子証明書による認証を紹介したが、流通過程に機密情報を流す場合、これを更に発展させ、証明書を相互に交換し合うことにより、相互で相手認証することが必要になる。この仕組みについても PKI の枠組みの中で標準化が進んでいる。

相互認証を行った結果、後述の3.6.1で紹介するようにオープンなネット上に安全なパイプを通すことが可能になり、その後の情報授受に必要な仕掛け（暗号化鍵の共有など）ができあがる。

(2) 個人情報管理

後述する今後の課題の中でも触れるが、ユーザ利便性のため、認証用個人情報をセンター管理する方式が考えられている。個人認証の方式としてのバイオメトリクス認証については、3.2.2.3を参照されたい。その場合、ネットワーク上を個人が特定できる情報が流れることになり、プライバシー保護の点から非常に重大な問題となることが想定される。

これを解決するために種々の方式が考えられている。前述した暗号化は、その1つである。暗号化されることにより、盗聴されても誰の個人情報か判定不可能であることを根拠とする。

更に、ネットを流れる情報は個人を特定する認証には使えるが、この情報から個人を再合成することはできない、という技術が開発されている。例えば、指紋情報の場合、指紋を採取した後、その情報から特徴点のみを抽出して送る方法である。この方法では、認証時に、再び同様の処理を行って特徴点を送り、センター側で保存されている特徴点と照合するが、この特徴点の情報から逆に個人を探し出すことは不可能となる。これは、特徴点の情報が、指紋採取処理、特徴点抽出処理毎に、まったく異なるものであること、情報として縮合されているため、元の情報（指紋全体）を合成することは不可能であること、を根拠としている。

3.4.3　技術・製品に関する最新トピックス、動向

3.4.3.1 公開・流通情報

実際のビジネスとして扱う情報は、主に、映画等の映像、音楽、ゲーム等のアプリケーションが挙げられる。これらについて個々に状況を説明する。

(1) DVD-ROM による映画配布

アナログのビデオカセットに代わり、デジタル化された映画を DVD-ROM のディスクに収納して販売されるようになってきた。この方式においては、種々の保護技術が用いられているが、個々の詳細は安全上の配慮で秘匿されているため、紹介が困難である。

概要は、次の通りである。

- 映画本体は暗号化されている
- 復号鍵が、ディスクと専用プレーヤ（ハード、ソフトがある）間でのやりとりの結果としてプレーヤにセットされる
- 鍵は階層化されていて、１つの映画の鍵が破られたとしても、他に影響する可能性が低い
- この例では、公開・流通情報である（暗号化）映画本体と、機密情報である復号鍵はディスクに一体化されている。

(2) 衛星放送による映画、スポーツ実況配信

専用再生装置（セットトップボックス）を用いたビジネスが展開されている。これについても、安全上の配慮から詳細は秘匿されている。概要としては、専用装置とセンターとが通信することによって、センター側で後述する利用権等の機密情報を個々のユーザ毎に作成し、専用装置に送り込むプロセスを行っている。

この例では、公開･流通情報である（暗号化）映画／実況本体は無料で不特定多数に放送され、機密情報である復号鍵は、別途、特定者のみが利用可能な形で放送され、専用装置内にセットされて用いられる。

(3) 携帯電話＋フラッシュメモリを用いた音楽配信

「ケータイ de ミュージック」という名称でのサービスが行われている。専用のハードウェアを搭載した携帯電話に、フラッシュメモリカードを挿入し、電話経由で音楽を取得するという仕組みである。今後、電話回線のデータスピードの改善とともに発展が期待される。

この例では、公開･流通情報である（暗号化）音楽本体は不特定多数向けにセンターに用意されており、ユーザが電話経由でダウンロードしたり、友人がダウンロードしてものをもらったりする。一方、機密情報である復号鍵は、別途、特定者のみが利用可能な形でセンターに用意され、電話で送出される。この方式によって、比較的大規模データである音楽本体は利用者毎に暗号化する必要が無くなり、センター負荷が軽くなることによって実運用上の利点がある。

＜参考＞

http://www.keitaide-music.org/index_j.html

(4) **ゲーム等アプリケーションプログラム配信**

携帯電話、ゲーム機あるいはパソコン上で動くプログラムを配信するサービスが始まっている。

ここでは、本章で述べてきたデータの保護技術だけではなく、悪意を持ったプログラムによる、機器内情報あるいは機器自体への悪影響を防止する技術が重要になる。これについては、2 章で、不正アクセス対策、DoS 攻撃対策、ウイルス／ワーム対策等として説明されているので、そちらを参照頂きたい。

3.4.3.2 機密情報

具体的な情報の種類ごとに状況を説明する。

(1) **暗号化された映画や音楽を、利用時に復号再生するための鍵**

通常、共通鍵方式の鍵である。映画、音楽が同一であれば、その鍵も同一である。従って、その映画については誰もがその鍵を利用できることになり、不正流用を防ぐ工夫が重要であるため、種々の方式が開発されている。前述した PKI ベースの認証によって、カスタマイズ情報とともに運用させる仕組みが一般的になりつつある。

具体的にはユーザ固有情報（IC カード、バイオ情報、装置 ID、媒体 ID 等）を安全性が確保された通信路を経由して交換し、相互に他者を特定した上で鍵を交換するなどである。

(2) **公開・流通情報利用の権利を回数券的に前払いしたプリペイド情報**

この情報は、前述した「不正使用のないことを保証したデータ修復」の問題を抱えている。この課題についての詳細は、今後の課題の中で後述する。実際のサービスについては現時点では始まっていない、と言うべきである。

(3) **個人情報（指紋等のバイオメトリクス情報、口座番号、住所録、電話番号、メールアドレス、スケジュール）管理**

上述したセンターでの一括管理方式以外に、フラッシュカード、IC カード等の可搬媒体に安全に保管し、必要に応じて読み出したり、持ち運んで別の装置（電話等）で利用したりする形態があり得る。この場合、媒体が一種の機密領域として機能すると考えられる。

3.4.3.3 データ改ざん検知の動向

これまでデータの保護技術について述べてきた。保護の前提として、データが改ざんされているか否かの確認が重要になるので、ここではデータ改ざん検知についてまとめる。

システムへの不正侵入によってデータが改ざんされたか否かを調べるツールとして、整合性チェックツールがある。著名なものとしては、Tripwire 社のものがあるが、その他にもいくつかのツールが販売または配布されている。

整合性チェックツールの働きは、システム内のファイルが変更･削除･追加されていないか否かを調べることである。

また、この分野では、Web 改ざん検索ツールが最近注目されている。Web 改ざん検索ツールもいくつかの会社から提供されており、その主な働きは、ファイル改ざんの検知、検知後のファイル自動修復、改ざんイベントの記録および管理者への改ざん発生の通知である。

＜参考＞

http://rr.sans.org/audit/aide.php

3.4.4 今後の課題

これまで、現状の技術について述べてきたが、その中でも種々の不備が指摘されている。その主なものについて、課題を説明する。

3.4.4.1 公開・流通情報

基本的に誰でも入手可能な情報であるため、以下の課題がある。

(1) **脅威耐性**

公開･流通情報については、性格上その存在を明らかにしているので、攻撃対象となるのは不可避である。従って攻撃のために投資される時間とコストに対して、得られる不正収入や栄誉をできるだけ低くする工夫が必要である。例えば、暗号化された映画を1本解読すると、他の全ての映画が解読できる仕組みは、脅威耐性が低いということになる。

具体的な対策の提案としては、鍵の階層化や鍵長の長大化が挙げられる。しかし、鍵管理コストの上昇、復号時におけるオーバヘッドの増加の問題があり、広く大衆に使ってもらうという大目的に反してしまう方向であるため、その折り合い点を見出すことが難しい。

(2) **課金処理と分配**

この情報自体は無料配布可能であるが、実際の配布に当たっては配給業者においてコス

トを要する。また、これ以外に、システム開発者、コンテンツクリエータ、再生機器製作、販売者、課金収集者、障害対応者、などで費用が発生する。従って、公開･流通情報の配給は、その後の利用者に対する課金処理とその分配の機構と密接に絡んでいることが必須であり、それを基にした機構が必要である。

3.4.4.2 機密情報

利用者が料金を支払って入手した権利や個人特定情報を扱うため、高い信頼性が要求されるとともに、トラブル対策が重要である。

(1) バックアップ対策

正当に入手した情報を、個人の範囲内でバックアップすることは Fair Use の考え方として、法律で保護されている。しかし、例え個人の範囲内であっても明らかに違法と考えられるバックアップ利用法がある。初期のプリペイド情報をパックアップしておき、使い切った後でバックアップ情報を戻すことで再び利用可能となってしまう問題（リストア攻撃と呼ばれる）である。上述したように、この問題の技術的解決は非常に難しい。

具体的提案としては、時刻変更が不可能な時計あるいは戻しが不可能なカウンタを用いて、時系列／順序管理を厳密に行うことによって、悪意あるリストア攻撃を排除する方式がある。この方式においても、時計あるいはカウンタと判断部分との間での介入をどう防止するかなど、議論が収束していない。

(2) 認証に用いる個人情報の管理

認証に用いる個人情報の管理に関しては、上記3.4.2.4、3.4.3.2で述べたように、センターで一括管理する場合と個人が携帯する可搬媒体に収納する場合のいずれの場合にも難しい問題が存在する。特に、情報が個人に関するものであるため、プライバシー保護の点からも扱い方には十分な配慮とユーザに対する説明が重要である。

① センター管理方式

この情報をセンターにおいて一括管理する方式においては、自分固有の端末等の機器を持ち歩くことなく、どこからでもその場の機器／環境を通じてセンターにアクセスして認証し、種々の情報／サービスを利用することが可能となるため、利便性は高くなる。

しかしながら、このセンターにおける管理では、プライバシー問題を解決できないとする考え方がある。つまり、指紋等のバイオメトリクス情報は不変であるため、トラブル発生後に変更できない、などの問題が指摘され、これに対する大衆の不信感を払拭できていない、と言われている。この解決策の1つとして3.4.2.4で述べたように、特徴点を扱うことで元情報を復元できない仕組みを作る方式がある。しかしながら、特徴点によって個人を特定できること、トラブル後の変更が困難であること、の本質的解であると広く認められるまでには至っていない。

② 個人所有物内管理方式

一方、個人が携帯する可搬媒体に収納する方式においては、従来のクレジットカードを携帯する等の運用に近く、かつ使用時ごとの ID・パスワード入力の必要が無くなるなどユーザ利便性が向上する可能性があり、大衆にとって受け入れ易いことが考えられる。しかし、収納されている情報の質が従来のカードとは比較にならない程に重要であるため、トラブル時の迅速な情報無効化等の厳密な運用が求められる。具体的には、トラブル等で所有者の手元を離れた際に内部情報を自動的、あるいはリモート指示によって消去する方式等の開発が望まれるが、現時点では実用的な技術レベルに達していない。

3.5 ウイルス／ワーム対策技術

3.5.1 ウイルス／ワーム対策に関する技術体系

IPA からの報告にもあるように、ウイルスの感染経路の約 90%は、電子メールであるといわれている。電子メール経由で入ってくるウイルスへの対策としては、従来よりウイルス対策ソフトウェア製品・サービスが複数のベンダから提供されており、これら製品・サービスを利用することにより既知のウイルス／ワームの侵入を防ぐというのが、基本的なウイルス／ワーム対策技術である。

3.5.2 個々の技術の概説

3.5.2.1 ウイルス／ワームの検知・駆除技術

(1) **パターンマッチング方式**

パターンマッチング方式は、ウイルスコード内の特徴的な部分を「パターン」として取り出してデータベース化しておき、それを検索対象のファイル内容と照合する方法である。同じコードを持っていた場合、そのファイルはウイルスであると特定する。

新種ウイルス／ワームが発見されるたびに、解析技術者はウイルス／ワームを解析し、識別用のパターンを抽出してデータベース（＝パターンファイル）に追加登録を行う。

検索プログラムはパターンファイルを参照しながら、検査対象ファイル内に登録されたウイルス／ワーム識別用パターンがないかどうかを調べる。該当するパターンがあれば感染ファイルであることを警告し、なければプログラムを終了する。ファイル以外にシステム領域（ブートセクタ、パーティションテーブル）の検索も可能である。

この方式の問題点は、検索ソフトのパターンファイルに登録されていないものはウイルス／ワームとして検出できないことである。そのため、常に新しいパターンファイルに更新していく必要がある。また、解析されていない新種ウイルス／ワームに対しても効果がない。

(2) **チェックサム方式**

チェックサム方式は、実行可能ファイル（拡張子が.COM、.EXE、.SYS など）のバイト数に変化がないかを常時監視する方法である。実行可能ファイルにウイルス／ワームが取りついて感染する場合、一般にファイルサイズが増加する。この性質を利用し、実行可能ファイルのバイト数の変化によってウイルス／ワーム感染の有無を調べることができる。

まずウイルス／ワーム感染していない状態で、実行可能ファイルのバイト数をデータベースに登録しておく。システムに変更があったり、アプリケーションを追加した場合にも再登録する必要がある。そして、その状態に変化がないかをリアルタイムで参照比較する。もし相違点があれば、ウイルス／ワームに感染したことがわかる。

この方式の問題点は、ウイルス／ワームの侵入までは防げないことである。ファイルの状態に変化があったときに警告を発したのでは、結果的に事後報告となり、ユーザが行動を起こすときには既に手遅れとなっている可能性がある。更に、ファイルの状態が変更された原因も特定することができない。ウイルス／ワームではなく、ソフトのインストールなどでファイルを改変する正常なプログラムまでもがチェックサムの網にかかってしまう。

(3) **ルールベース方式（＝動作監視方式）**

ルールベース方式は、コンピュータ環境内のウイルス／ワームによる異常動作を監視して、ウイルス／ワーム感染を防止する方法である。ウイルス／ワームに感染すると、システム領域の書き換え、実行型のプログラムファイルへの書き込み、特殊なメモリ常駐といった、通常ではあり得ない異常な命令を出すことが多くある。この異常な動作をルールとして定義し、そのルールに合致した活動をするものをウイルス／ワームとして検出する。「ルール」に則ってウイルス検出を行うので「ルールベース」と呼ばれている。

ルールベース方式は、既知のウイルス／ワームばかりではなく、未知のウイルス／ワームに対しても有効である。また、ウイルス／ワームが感染発病活動を行う前に、その活動を未然に防ぐことができる。

この方式の問題点は、本当にウイルス／ワームかどうかの確認が難しいことである。ウイルス／ワームに似た活動をするけれども、実際には正規のアプリケーションということもあり得る。そのため、実際にはルールベース方式のみでウイルス／ワームだと断定することはなく、他の方式と組合せてウイルス／ワーム検出を行う。

3.5.2.2 ウイルス／ワーム対策ツール

(1) **ウイルス／ワーム対策ツール（クライアント型）**

クライアント型のウイルス対策ツールは、クライアント1台ずつ個々にインストールするものである。最新のウイルス／ワームに対応するためには、ウイルス／ワームのパターンファイルを定期的に更新する必要があるが、クライアント型の場合、1台ずつ個別に更新を行わなければならない。しかし、最近のウイルス対策ツールは、インターネット接続中に自動的に最新のパターンファイルをチェックしてインストールし、最新のウイルスから常に保護された状態にすることができる。

＜主な製品名＞

Norton AntiVirus 2002 （㈱シマンテック）

ウイルスバスター 2002 （トレンドマイクロ㈱）

Virus Scan 4.5 （日本ネットワークアソシエイツ㈱）

(2) **ウイルス／ワーム対策ツール（サーバ型）**

サーバ型のウイルス対策ツールは、企業等で大量のクライアントを集中管理する必要があ

る場合を想定して開発されたものである。パターンファイルやエンジンのアップデートファイルの配布をサーバから全クライアントについて集中的に行うことができる。これにより、全社的なアップデート時のコストや配布漏れ、インストールの失敗も減少する。また、最新のサーバ型ウイルス対策ツールは、新種ウイルスに対して、ベンダ側のシステムと Web 経由で自動的に連携、即座にパターンファイルを生成し、企業システムに配布を行う。

＜主な製品名＞

Norton AntiVirus Enterprise Solution 4.6 （㈱シマンテック）

ウイルスバスター コーポレートエディション （トレンドマイクロ㈱）

ePolicy Orchestrator（日本ネットワークアソシエイツ㈱）

3.5.3 技術・製品に関する最新トピックス、動向

3.5.3.1 ISP のメールチェックサービス

近年の動向の1つとして、ISP によるメールチェックサービスが挙げられる。このサービスは、ISP がウイルス対策ソフトウェアベンダから出されている製品を導入することにより、ISP 経由で電子メールを受信する場合には予めウイルス／ワームのチェックおよび駆除を行い、送信する場合には相手へ届く前に ISP 側でウイルス／ワームチェックおよびウイルス／ワーム駆除を行うものであり、このサービスは、大手 ISP では導入がかなり進んでいる。ウイルス対策をインフラに組み込むことによって、より効率的にウイルス／ワーム付きメールを食い止めることが可能となる。

また、メールのウイルス／ワーム対策サービス以外にも、メールの監査やメールの安全な保管を行うサービスも登場してきている。

3.5.3.2 Web 経由の感染に対する対策

Nimda のように Web 閲覧するだけで感染してしまうウイルス／ワームが出現し、これまでのようにメール経由の感染だけでなく Web 経由の感染に対しても備える必要性が高まってきている。このような感染への対策として Web プロキシ型のウイルス対策製品が出現している。Web プロキシ型のウイルス対策製品では、インターネットと LAN の接続点に設置することにより、Web 感染型ウイルスの検知･駆除をプロキシレベルで行い、これにより社内ネットワーク等の LAN の入口で感染を食い止めることが可能となる。その仕組みとしては、メールの場合と同じくパターンファイルとの比較によるものである。これら製品は、Web 感染型ウイルス／ワームのチェックだけではなく、メール感染型のウイルス／ワームチェックおよび FTP のチェックを併せて行うタイプのものもある。

3.5.3.3 セキュリティ機能を備えたブロードバンドルータ

2001 年秋以降、数社からセキュリティ機能を備えたブロードバンドルータが発売されている。製品によって異なるが、これらのルータでは、ウイルス／ワーム対策機能やファイアウォール機能、IDS 機能、URL フィルタリング機能などを備えている。

ウイルス／ワーム対策機能の特徴としては、ウイルス／ワームの定義ファイルの更新を自動で実行するため、これまでのように人手で実行するよりも容易に対応することが可能となり、定義ファイル更新のミスも防ぐことができる。

＜参考サイト＞

トレンドマイクロ㈱

http://www.trendmicro.co.jp/gatelock/index.asp

㈱チェックポイント

http://www.checkpoint.co.jp/press/2001/sofaware121101.html

3.5.4 今後の課題

既知のウイルス／ワームに対しては、基本的には既知ウイルス／ワームのプログラムパターンをデータベース化し、対象のファイルと比較することによってウイルス／ワーム検査を行っていたが、問題は未知のウイルス／ワームの対策である。

未知のウイルス／ワームに対しては、まだ十分な機能を擁した対策ソフトウェアやサービスは出現していないようであるが、各ウイルス対策ソフトウェア・サービスベンダは、対策を進めつつある。

例えば、シマンテック社では、定義ファイルの更新に依存しない技術を開発しており、新種ウイルスへの対応を進めている。同社では、2001 年 6 月より、VBScript や JavaScript プログラムの動きを監視することで不正プログラムを発見する「スクリプト・ブロッキング機能」を搭載し始めた。これはVBScriptやJavaScriptベースのウイルスが増加していることに対応する技術であり、未知のウイルスでもメールソフトに含まれるアドレスを一気に採取するような怪しい行動を検出するものである。

3.6　通信の保護技術

3.6.1　通信の保護に関する技術体系

「通信の保護」とは、主にネットワーク上を流れるデータの保護であり、通信相手を確認し、盗聴を防止し、改ざんを検知することである。一方、通信に利用する回線設備の利用形態を分類すると、おおよそ以下のようになる。なお、(4) は (1) ～ (3) の分類とはレベルが異なるが、便宜上並べて示す。

(1) **専用の通信回線を利用した形態**

お店を借り切って専有して使っている形態に例えることができる。所謂、基幹システム系はこのような形態をとる場合が多かった。

(2) **閉域網を利用した形態（IP－VPN、広域 LAN など）**

会員制クラブの利用に例えることができる。クラブオーナーの責任で利用グループ間を分離し防音設備しているような形態である。

(3) **オープンなインターネット回線を利用する形態**

誰でも出入り自由なお店を利用している形態に例えることができる。秘密に会話したいなら、利用グループ自身が防音設備等を用意する必要がある。

(4) **ユーザ認証のやりとりを外部回線経由で行う形態（リモートアクセス）**

上記のようなお店やクラブに外部と話すための窓が付いている形態に例えることができる。

以上のどの利用形態についても、「通信相手確認」、「盗聴防止」、「改ざん検知」が必要である。しかし、これらには定量的な軽重があり、また、状況に応じて対策のレベルも変わる。例えば、「(1) 専用の通信回線を利用した形態」の場合は設備が物理的にある程度隔離されているため、システム設置者とシステム保守者を信用して通信相手確認や盗聴防止を軽微にした運用も可能であろう。また、改ざん検知についても軽減できるだろう。「(2) 閉域網を利用した形態」の場合もシステム提供者とシステムの造りを信用することにより、ユーザ側の対策を省略したり軽減したりすることができる。

これに対し「(3) オープンなインターネット回線を利用する形態」や「(4) ユーザ認証のやりとりを外部回線経由で行う形態」では、脅威があることを前提としたスタンスで対策を行うことが必要である。

この節では、通信アプリケーションによる技術的対応に関して説明するが、通信を保護するためにはこれだけでは十分でなく、

a. 通信システムの適切な選択、設置
b. 暗号技術等を応用した通信アプリケーションの適用
c. 通信システム運用者の適切な運用
d. 通信システム使用者の適正な使用

e. 関連法の整備

等の総合的適用によって実現されるべきものである。

上に記した“回線設備の利用形態”に対応させて、通信保護対策方式を例示すると表 3-2のようになる。

表 3-2 通信保護に関する対策方式(定性的な例示)

	通信相手確認	盗聴防止	改ざん検知
1．専用線	設備上の保証＋対策	設備上の保証＋対策	MAC 応用 etc
2．閉域網	運用上の保証＋対策	運用上の保証＋対策	MAC 応用 etc
3．インターネット	電子署名応用 etc	共通鍵暗号応用 etc	電子署名応用 etc
4．リモートアクセス	ﾊﾟｽﾜｰﾄﾞ、電子署名応用 etc	共通鍵暗号応用 etc	電子署名応用 etc

上記のような対策方式の具体例を幾つか例示する。ここで示す例には、様々なレベルのものが混在しており、同列に並べるべきでないものも含まれていることをお断りしておく。3.6.2「個々の技術の解説」では、上記 a.「通信システムの適正な選択、設置」に関して最近注目されている IP-VPN および、b.「暗号技術等を応用した通信アプリケーションの適用」に関する主な技術(下記の項目)についての概説を加えることとする。

- SSL/TLS（安全なソケット通信）
- IPSec（安全な IP）
- Kerberos（ネットワーク認証）
- SSH（安全な遠隔実行シェル）
- PGP、S/MIME （暗号メール）
- PKI（公開鍵基盤）

3.6.2 個々の技術の概説

3.6.2.1 IP-VPN

VPN(Virtual Private Network)とは、オープンなネットワークの上で、仮想的に専用線のようなネットワークを構築する技術のことである。この VPN 技術の中でも最近注目されているのは、IP ネットワークをベースとした IP-VPN である。

IP-VPN は、表 3-3のように分類することができる。従来より、IP ネットワーク上で信頼性を高めた通信方式としては ATM／フレームリレー方式があるが、この方式は専用の機器を導入しなければならなかったり通信費が高い等のコスト面でのデメリットや、アドレス管理等の設定作業がサービ

ス運用時に煩雑になりがちであるという運用面でのデメリットもあった。そこで、通信コストを下げた方式として、インターネット VPN 方式が登場した。この方式ではコストダウンとのトレードオフで、信頼性は ATM／フレームリレー方式の場合よりも低下する。また、ATM／フレームリレーと同程度の信頼性を持ち、通信コストも下げた方式として、MPLS（Multi-Protocol Label Switching）のように、単独のキャリアによって独自に構成される IP ネットワークを利用した方式が登場している。IP-VPN を採用する際には、利用する場面に対して必要となる信頼性とコストの両面からどの方式を選択するかを検討する必要がある。

表 3-3 IP-VPN の分類

	方式	通信コスト	信頼性
IP-VPN	インターネットVPN （IPSec等のトンネリング技術利用）	安い	低い 高信頼性のためには、専用機器が必要
	ATM／フレームリレー	高い	高い ただし、アドレス管理等の運用が煩雑
	キャリア独自のIPネットワーク利用 （MPLS等）	安い	高い（ATM／フレームリレーと同等） 運用も比較的容易

(1) インターネット VPN

インターネットVPN方式は、インターネット上で、仮想トンネリング技術を利用してユーザ認証やデータ暗号化を行う方式である。仮想トンネリング技術としては、様々な技術を利用することができるが、IPSec を利用するケースが増えているようである。IPSec については、3.6.2.2(2)で触れることにする。

(2) キャリア独自の IP ネットワーク利用

上記 MPLS に代表される、単独のキャリアにより構成された IP ネットワークを利用した方式のネットワークサービスが各社から提供されるようになってきている。具体的な提供サービス例については、表 3-4を参照頂きたい。

表 3-4 国内の IP-VPN サービス

（日経コミュニケーション 2001.11 月号掲載の表を再加工）

	キャリア独自のIPネットワーク			インターネットVPN		
	MPLS方式	OBN方式	仮想ルータ方式	IPSec方式	L2TP方式	GMN-CL方式
NTTコミュニケーションズ	Arcstar IP-VPN					
KDDI	KDDI IP-VPN					
日本テレコム	SOLTERIA					
NTT PC	SuperEBN	SuperOBN				
インテック・コミュニケーションズ	EINS					
富士通	FENICSビジネスIP ネットワークサービス					
フュージョン コミュニケーションズ			Fusion IP-VPN			
パワードコム	Powerd-IP MPLS					
AT&Tグローバル・サービス	ユニバーサルVPN					
NTT-ME						Xephion高速IPエクストラネットサービス
NTT東日本／西日本					フレッツ・オフィス	
ケーブル＆ワイヤレスIDC				IP VPN-インターネット ルータベース		

この表からも分かるように、MPLS 方式のサービスが増えてきているが、この MPLS 方式の特徴は、送信元より送出する各パケットに配送先のラベル付けを行い、ラベル情報をネットワーク内のルータが識別することによりパケットの振り分けを行うことである。また、MPLS では帯域制御や優先制御が可能となる。

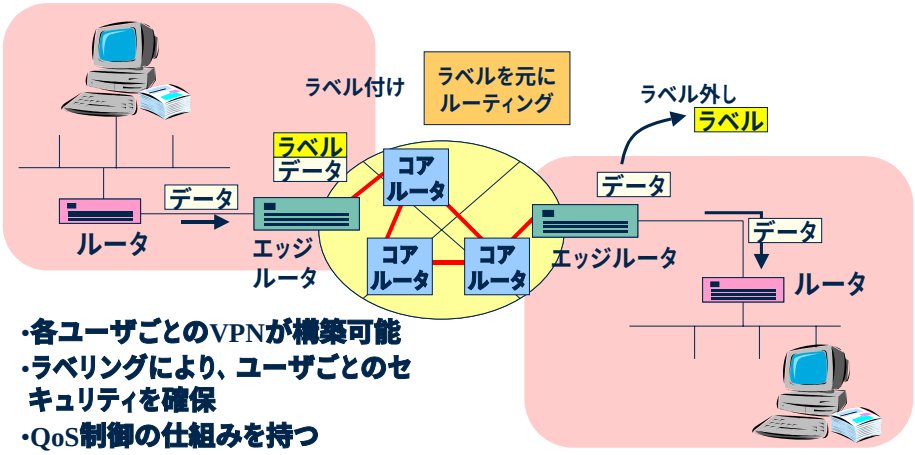

図 3-2 MPLS（概念）

3.6.2.2 暗号技術等を応用した通信アプリケーション

(1) SSL/TLS

SSL はプロセス間通信のためのソケットに安全化機能を付加するというスタンスで Netscape Communications 社が提唱したものである。その後、IETF（Internet Engineering Task Force）でインターネット標準化が図られ、これを TLS（Transport Layer Security）と呼び直している。代表的な Web ブラウザがこの技術を実装したため、広く普及しており、クライアント側のユーザは特に意識せずに使える環境になっている。このため Web 上のショッピングサイトでも広く用いられているが、SSL を装備したサーバ側の処理はその分重くなるので、処理の集中が予想されるようなショッピングサイトの場合、アクセラレータを用意するなどのシステム上の配慮が必要になる。

SSL/TLS は、公開鍵方式と共通鍵方式を組合せた方式であり、WWW サーバとクライアント間の認証等に利用される。この場合の認証手順を簡単に記すと、次のようになる。

①クライアントから WWW サーバへリクエストを送付する

②WWW サーバは、証明書をクライアントへ送信する

③クライアント側で証明書を認証し、その結果 WWW サーバの公開鍵を取り出す

④クライアントは共通鍵を作成し、WWW サーバの公開鍵で暗号化して送信する

⑤WWW サーバは共通鍵を取り出す
⑥データを共通鍵で暗号化し、両者間で通信を行う

なお、SSL は OSI 参照モデルのセッション層で実現される機能として位置付けられるので、WWW に限らず、メールや遠隔ログインなどのアプリケーションにも適用可能である（アプリケーションに透過的に暗号／復号等を適用可能）。「盗聴」を防ぐ「暗号化機能」、「改ざん」を防ぐ「メッセージダイジェスト機能」、「成りすまし」を防ぐ「認証機能」、通信双方で各機能の準備をする「ネゴシエーション機能」等を備える。

また、OpenSSL プロジェクトによって開発された OpenSSL ツールキットというものもあり、これはいくつかの簡単なライセンスの制約下でなら、入手と商用・非商用の利用は自由となっている。

(2) IPSec

IP（インターネットプロトコル）そのものに認証機能や暗号化機能等の枠組みを付加しようとするものであり、IETF が VPN のプロトコルとして標準化した。SSL/TLS 機能を実現するセッション層より更に下層である OSI 参照モデルのネットワーク層で実現される機能として位置付けられる。よって、アプリケーションに透過的に適用できるという性格が更に強く、ゲートウェイに該当機能を持たせることにより運用できる。このため、オープンなインターネット回線を利用して VPN 化を図る手法の代表例になる。現時点では必ずしも広く普及していないが、相互通信の検証や製品への実装が進みつつある。このような製品やソフトを組み込むことにより、IPSec を導入できる。IPSec を用いた方式は、将来の EC では重要な方式になるであろう。なお、アドレス空間を抜本的に拡張した次世代インターネットプロトコル IPv6 にはこの IPSec が組み込まれている。

IPSec は IP のセキュリティ強化を行うための技術の総称であり、具体的には以下のような枠組みの複合体になっている。それは IKE（Internet Key Exchange；鍵交換）、ESP（Encapsulation Security Payload；IP データグラムの積荷の暗号化）、AH（Authentication Header；完全性チェックヘッダ）である。IKE で用いる鍵交換方式、ESP で用いる暗号化方式、メッセージダイジェスト方式などは複数の中から選んでネゴシエーションできる。

(3) Kerberos

信頼の置けないオープンなネットワークに接続されたクライアント／サーバシステムにおいて、クライアント／サーバ双方の身元確認と秘密通信を実現するために、全クライアント／サーバが暗号化の鍵データを事前に KDC（Key Distribution Center；鍵配布センタ）に登録して運用する、ネットワーク認証システムである。「信頼の置ける第三者機関による認証」という概念に基づく。用いる暗号は対称鍵暗号系である。クライアントユーザが必要なときに鍵データが書かれた「チケット」を KDC に取りに行くのだが、その際、毎回、クライアント固有の秘密情報を提示するのではなく、事前に「チケット認可チケット」を入手しておくところに特徴があ

る。

この辺りの操作は印鑑登録証明制度に例えられる。すなわち、KDC は印鑑証明を発行する役所に例えられ、「チケット認可チケット」は印鑑登録証に、「チケット」は印鑑証明書に例えられる。印鑑登録証明制度では、事前に印鑑登録をして印鑑登録証を入手しておいた上で、ある手続きを行いたいときに、役所に出向き、印鑑登録証を提示して印鑑証明書をもらう。手続き時には、必要書類に印鑑証明書を添付して用いる。同様に Kerberos では、事前に「チケット認可チケット」を入手しておいた上で、あるサービスを受けたいときに KDC に「チケット認可チケット」を提示して「チケット」をもらい、あるサービスを受けるためには、その「チケット」を添付する。

Kerberos は、X Window System で有名な MIT（マサチューセッツ工科大学）の Project Athena（アテナ・プロジェクト）で開発された技術であり、MIT での運用、OSF/1 などのデータ回線終端装置での採用など、かなりの歴史と実績がある。一方、昨今でも、Windows2000 や Mac OS X などが機能を取り入れたこと、運用や実装に関する議論などで、話題を提供している。

本方式は、その開発されてからの期間の割にはあまり普及していないとも言えるが、本システムで用いる Realm という領域単位がインターネットの Domain 概念と親和性が高いことや、大手 OS での実装が進みつつあることなどから、普及の可能性がある。

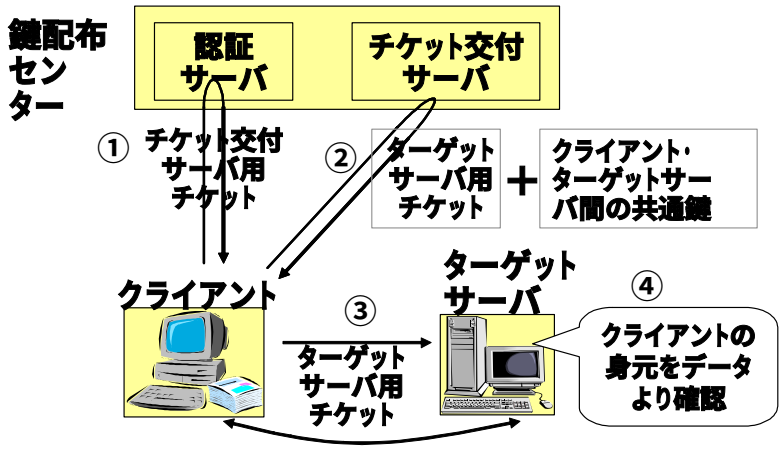

図 3-3 Kerberos の仕組み

(4) SSH

Web 上でショッピングサイト等を運営する場合、悪質なクラッカーから直接攻撃を受けたり、踏み台にされることを想定する必要がある。このような観点から、利便性を損なうことなく、遠隔から安全にサーバにアクセスできるようにしておくことは重要である。遠隔から安全にサーバにアクセスする方式の代表例として SSH（Secure Shell）がある。UNIX の r 系コマンドや telnet などには、盗聴、固有のセキュリティホール、IP Spoofing といった危険があるので、現在、オープンなネットワークではまずこれらを用いないで、SSH のコマンドを用いるのが一般的である。SSH Communications Security 社が管理する SSH2 やオープンな OpenSSH などを導入することになる。

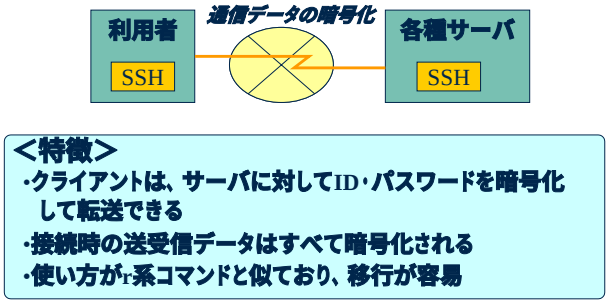

図 3-4 SSH

3.6.2.3 暗号メール

電子メールは「はがき」に例えられるように、もともと秘匿性に乏しい。電子メールを暗号化する方式として次のようなものが知られている。

- PGP（Pretty Good Privacy）

  本文を IDEA で暗号化することにより機密性を保証し、デジタル署名に RSA を採用することによって、完全性と真正性の保証を可能にする方式

- S/MIME（Secure Multipurpose Internet Mail Extensions）

  認証局を設けてデジタル証明書を利用する方式

  本文を DES、RC2 等の方式で暗号化を行うことにより機密性を保証し、証明書に RSA 方式を採用することによって、完全性と真正性を保証する

- PEM（Privacy Enhanced Mail）

  本文を DES で暗号化することにより機密性を保証し、デジタル署名に RSA を採用することによって、完全性と真正性の保証を可能にする方式

- MOSS（MIME Object Security Service）
  本文を DES で暗号化することにより機密性を保証し、デジタル署名に RSA を採用することによって、完全性と真正性を保証する方式
- KPS（Key Predistribution System）
  国産の暗号鍵管理技術であり、公開鍵と秘密鍵を用いて暗号化を行う方式
  従来の公開鍵暗号方式では、認証局を設けて証明書の発行等を行うが、KPS では認証局を必要とせず、個別に発行される“ Private-ID ”とメールアドレス等の公開されている情報を使用している

今のところ、PGP と S/MIME が事実上の標準に近いと言える。PGP と S/MIME の基本的機能の枠組みは共通だが、「通信相手の信頼性を確認するポリシー」に違いがある。PGP がエンドユーザの“信用の輪”を通じて信頼性を確立するのに対し、S/MIME は信用ある第三者機関 CA（認証局）の階層的信用を拠り所にする。

しかし、暗号メールそのものが一般ユーザにそれほど浸透していない側面もある。また、テロや犯罪抑止の観点から暗号メールの普及を疑問視する社会情勢も逆風である。一方、インターネットの常時接続やブロードバンドの普及に伴い、プライバシー情報の漏洩に関する一般ユーザの意識が高まりつつある。暗号メールの普及が、今後どのように推移するか興味深い。

3.6.2.4 PKI

実商取引において印鑑やシグニチャやその公的証明等が使われるように、インターネット上の商取引でも同様な機能が必要である。企業や個人の公開鍵を第三者機関に登録し、認証機関（CA）が発行する電子証明書によって、企業や個人を電子認証する環境を公開鍵基盤（PKI）という。環境と称するように、暗号メールなどのアプリケーション等とはやや次元の異なるものである。暗号メール S/MIME 使用時に PKI 環境を利用する、SSL 使用時に PKI 環境を利用する、というように用いる。また一部のデスクトップアプリケーション（Adobe Acrobat、Microsoft Office XP など）の署名機能でも用いられる。電子署名法など法整備も整いつつあり、民間レベルの認証サービスが立ち上がりつつある。

PKI の導入に当たっては、利用目的、対象、コストなどの設定条件をクリアにするとともに、CA（認証局）の選定をはじめとする運用方針を固める必要がある。技術面も重要だがシステム運用の方針が特に重要であり、課題も残されている。今後の整備に期待したい。

なお、PKI に関するより詳細な情報については、ECOM の認証･公証 WG から出されている報告書等を参考にされたい。

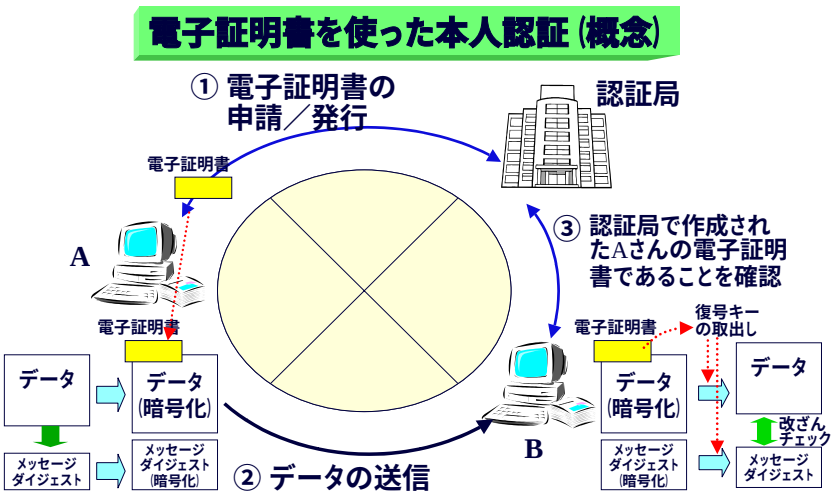

図 3-5 電子証明書

3.6.3 技術・製品に関する最新トピックス、動向

NetSecurityの2001年国外ニュースのページから、関連のありそうなものを抽出すると、例えば以下のようになる。

- 通信の安全性を実現する発光ダイオードを開発（東芝ヨーロッパ社）（2001.12.27）
- WEP （Wireless Equivalent Privacy）Security アップグレード版の内容が公開される（2001.12.26）
- 新しい暗号標準を採用（米商務省）（2001.12.13）
- FBI が法の執行のため、通信業社にネットワーク改善を要求（2001.12.5）
- 新しい活用を求めてセキュアシェル（SSH）のスキャン増加中（2001.11.2）
- 無線セキュリティへの取り組みを強化（IBM 社）（2001.10.18）
- 無線製品対応の新セキュリティ技術を公開（NextComm 社）（2001.10.4）
- 無線データ通信の安全性を脅かすハッキングツール公開される（2001.8.30）
- 研究チームが SSH を悪用したハッキングツールを開発（カリフォルニア大学バークレー校）（2001.8.30）
- 電子メールの安全性を確保するため、業界団体を創設（OpenPGP Alliance）（2001.6.7）
- 無線 LAN 規格に深刻な脆弱性が確認される（カリフォルニア大学バークレー校）（2001.2.15）
- 電子署名アルゴリズムに脆弱性を発見（Bell Labs 社）（2001.2.15）
- 次世代の WAP セキュリティ技術を開発（eMobile 社）（2001.1.25）

（https://www.netsecurity.ne.jp/ より抜粋）

上記から傾向を抽出すると、

- 無線関係のセキュリティ方式
- 暗号化メール
- SSH 等のセキュリティホール
- 新暗号関連

が話題になっていると言える。

3.6.4 今後の課題

今後の主な課題として、以下を予想する。

- 非 PC 機器にまで広く IP 接続が拡大することが予想される IP 次世代（IPv6 世代）運用時の技術課題

  基本的な枠組みは既に固まっていると思われる。また、セキュリティ運用の観点から述べると、現行 IPv4＋IPSec にほぼ等しい、とも見なすことができる。しかし、ショッピングサイト等を運用する立場から考えると、アクセスしてくる対象が非 PC 機器にまで広がり、アクセス形態も変容することが予想される。

  具体的にどのように変容していくかは予測が難しいが、これらを想定した諸課題の抽出が必要となるだろう。また、次世代推移時の混在環境の対応準備等も必要となるだろう。

- 携帯電話、無線 LAN 等のワイヤレス通信関連の課題

  次世代携帯電話サービスや、セッション再開機能を備える WTLS（Wireless Transfer Layer Security）ベースのワイヤレス VPN、Kerberos 認証スキームなど多様な展開が予想される（多様すぎて具体的技術課題を絞りきれない側面もある）。

- ブロードバンド常時接続形態の普及に伴う諸課題

  昨今、ADSL をはじめとしたブロードバンド常時接続形態が急速に普及している。EC にとってもビジネスチャンスの拡大に繋がるが、セキュリティ上の課題も増大している。一般ユーザに利便性と安心の双方を提供する方式、環境の整備が必要になる。

- 電子証明書の管理・運用に関わる諸課題

  法的な証になる証明書等には、発行時だけでなく途中審査や廃棄確認などの適正な管理が求められる。PKI の運用においても同様であり、証明書の失効や廃棄の管理は大きな課題である。CRL（証明書廃棄リスト）ファイルを用いる方法では、定期的な配布間の時間遅れや大容量ファイルのダウンロードによるサーバの負荷増大の問題があり、

OCSP（オンライン証明サービスプロトコル）により廃棄を問い合わせる方法では、トラフィックの問題、DoS 攻撃の問題等が懸念されている。証明書廃棄に関わるトラブルは商取引上の深刻なトラブルに繋がる恐れがあるため、技術・運用の両面から、課題の克服が必要になる。

上記のような課題の整備を通じ、いわゆる“ユビキタスな（遍在する）EC 環境”が実現できれば望ましい。

■ 本報告書の執筆に携わったメンバー（企業名 50 音順）

アンリツ株式会社	技術統轄本部研究所	崎田　一貴
株式会社イーアイティー	システム開発部	森田　純生
沖電気工業株式会社　ＳＳＣ	ﾌﾞﾛｰﾄﾞﾒﾃﾞｨｱｿﾘｭｰｼｮﾝ部	本多　祐司
川鉄情報システム株式会社	ＮＷＳ事業部	鈴木　伸幸
ｺﾝﾋﾟｭｰﾀ･ｱｿｼｴｲﾂ株式会社	フィールドサービスグループ	森　　宣彦
株式会社三和銀行	EC 業務部	清水 比佐雄
東京電力株式会社	システム企画部	志水　　祐
株式会社東芝	ｅ－ソリューション社	山田　朝彦
東北電力株式会社	情報通信部	三嶋　　一
日本電気株式会社	ＮＥＣソリューションズ	清水　雅子
株式会社日立情報システムズ	ｼｽﾃﾑｲﾝﾃｸﾞﾚｰｼｮﾝ本部	柴田　利幸
株式会社富士通研究所	コンピュータシステム研究所	小谷　誠剛
富士電機株式会社	事業開発室	糸岡　　崇
マイクロソフト株式会社	ﾃﾞｨﾍﾞﾛｯﾊﾟｰﾏｰｹﾃｨﾝｸﾞ本部	加藤　健二
電子商取引推進協議会		重松　孝明
電子商取引推進協議会		川村　尚哉

■レビュー等のその他活動に携わったメンバー（企業名 50 音順）

株式会社イーアイティー	事業推進部	友澤　　敦
石川島播磨重工業株式会社	情報システム部	高橋　佳祐
株式会社ＮＴＴデータ	ビジネス企画開発本部	宮武　達也
佐川急便株式会社	ＩＴ戦略本部	吉岡　賢宏
住友海上リスク総合研究所	調査第四部	藤本　正代
中部電力株式会社	情報システム部	杉原　武司
電子商取引安全技術研究組合	常務理事　植村　泰佳	
日本コムシス株式会社	営業統括本部	田村　純一
財団法人日本情報処理開発協会	情報セキュリティ対策室	高取　敏夫
日本信販株式会社	セキュリティ情報部	大竹　秀一
日本電気株式会社	ＮＥＣネットワークス	宮地　利雄
株式会社日立製作所	システム開発研究所	藤山　達也
富士重工業株式会社	情報システム部	飯塚　光二
富士通株式会社	ソフトウェア事業本部	天野　大緑
株式会社富士通中部ｼｽﾃﾑｽﾞ	経営推進統括部	西垣　義則
富士電機情報ｻｰﾋﾞｽ株式会社	情報ＳＩ事業部	佐藤 美香子
ﾌﾟﾗｲｽｳｫｰﾀｰﾊｳｽｸｰﾊﾟｰｽｺﾝｻﾙﾀﾝﾄ株式会社	テクノロジー本部	野田　政輝
松下電器産業株式会社	東京支社　網野　幾夫	
三菱電機ｲﾝﾌｫﾒｰｼｮﾝｼｽﾃﾑｽﾞ株式会社	ｲﾝﾀｰﾈｯﾄﾋﾞｼﾞﾈｽｼｽﾃﾑ部	佐藤　勝幸
三菱電機ｲﾝﾌｫﾒｰｼｮﾝｼｽﾃﾑｽﾞ株式会社	関西支社	神野　和司
三菱電機ｲﾝﾌｫﾒｰｼｮﾝﾃｸﾉﾛｼﾞｰ株式会社	システム技術部	小嶋　好彦
安田火災海上保険株式会社	企業商品業務部	大原　克之

平成 14 年 3 月発行
発行：電子商取引推進協議会
東京都港区芝公園 3-5-8
機械振興会館 3F
Tel 03-3436-7500
e-mail info@ecom.jp

この資料は再生紙を使用しています。