高度情報通信ネットワーク社会における
治安基盤の指標（ベンチマーク）に関する調査
報告書

平成14年6月

警 察 庁

1. はじめに 4

2. 体感的なITインフラの変化とセキュリティ侵害の関係 5

2.1. ITインフラ側の変化 6
2.2. 不正アクセス側の変化 7

3. ITインフラ重要度の変化 8

3.1. 情報インフラとしてのネットワーク利用の普及 I 8
3.1.1. Webは、媒体として重要な位置をしめている 8
3.1.2. Webは、商取引のインフラとして機能している 8
3.1.3. 電子メールの利用 9
3.2. 情報インフラとしてネットワーク利用の普及II 10
3.2.1. 電子商取引の市場規模 10
3.2.2. 電子商取引対GDPの割合 11
3.3. ITインフラ利用者の増加 12
3.3.1. インターネット利用者の増加 12
3.3.2. 常時接続端末の増加 13
3.4. インターネット利用状況の変化 14
3.4.1. インターネットトラフィックの変化 14
3.4.2. サーバ数の増加 15
3.4.3. WWWコンテンツの拡大 16
3.5. インターネット利用者側の問題 18
3.5.1. インターネット利用上の問題 18
3.6. 被害を防ぐための対策 19
3.6.1. データセキュリティへの対策とウイルス対策 19
3.6.2. ファイアウォールでの限界 20

4. 不正アクセスの被害 21

4.1. 企業のクラッキングされた経験 21
4.2. 不正アクセス被害の内容 I 22
4.2.1. IPA/ISECへの届出の内容 22

4.2.2. JPCERT/CCへの届出の内容 24
4.2.3. ISS社監視サービスでの検出内容 25
4.3. 不正アクセス被害の内容Ⅱ 26
4.3.1. IPAウイルス発見届出状況 26
4.3.2. 個人情報の漏洩 26
4.4. 不正アクセス被害の増加 27
4.4.1. CERT/CCが受け付けた不正アクセス報告 27
4.4.2. JPCERT/CCが受け付けた不正アクセス報告 28
4.4.3. IPA/ISEC、JPCERT/CC不正アクセス届出件数の推移 29
4.4.4. ハイテク犯罪検挙件数 30
4.4.5. 不正アクセス行為の発生状況 31
4.4.6. 「不正アクセス」記事件数 32
4.4.7. 改竄されたホームページ数の推移 33
4.4.8. 新聞記事件数とWeb改竄件数の比較 34
4.4.9. 関連する指標 35
4.5. 脆弱性情報の推移 38
4.5.1. CERT/CC-Advisory 38
4.5.2. X-FORCE 39
4.5.3. Bugtraq 40
4.5.4. Microsoft社 Security Bulletin 41
5. Ⅱ関連の保険について 42
5.1. 損害保険の利用について 42
6. 調査結果の分析 43
6.1. IT許容リスクの減少 43
6.2. セキュリティ侵害行為被害遭遇確率の増加 44
6.2.1. 脅威の増加 44
6.2.2. 脆弱性の増加 47
7. まとめ 50

1. はじめに

昨今のインターネットの普及の状況は、個人、企業、政府自治体などあらゆる方面において、インフラとしての重要度を増してきているといえる。個人においては、インターネットバンキングやショッピング、情報の検索やブロードバンドの普及によるエンターテイメント、教育及び学習での利用、また、企業では電子商取引の発展や販売、製造における情報交換メディアとしての役割、政府や自治体においてもネットワークインフラの積極的な利用展開が進みつつある。

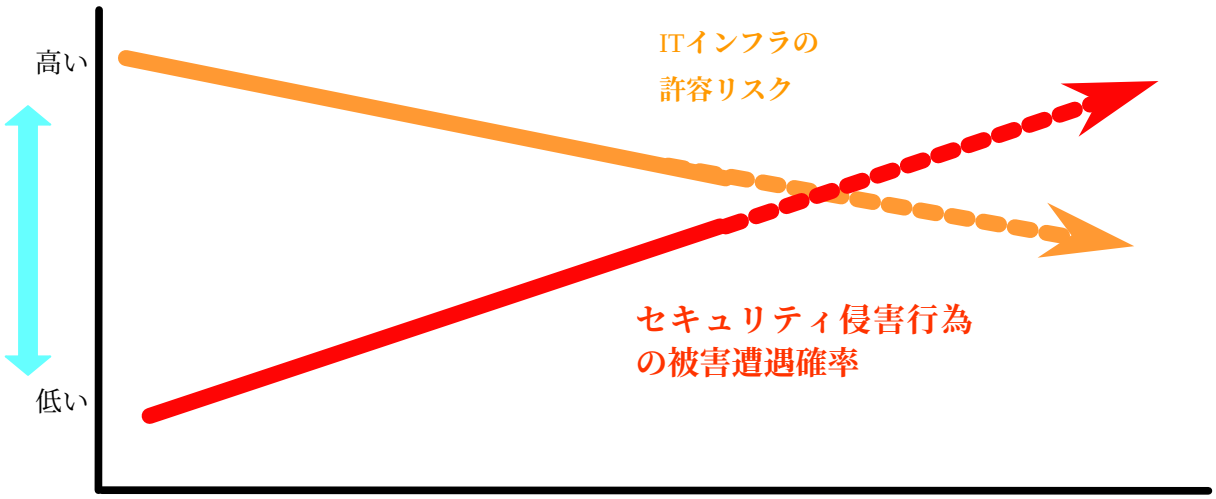
政策、法律面においても平成13年3月、「5年以内に世界最先端のIT国家となることを目指す」こととした「e-Japan戦略」、さらに「e-Japan重点計画」が策定された。また、平成13年1月、「高度通信ネットワーク社会形成基本法」（いわゆるIT基本法）が施行され、今後「超高速アクセスが可能な世界最高水準のネットワーク」等のインフラ整備を推進している。

しかしながら、一方で平成200年1月から2月に発生した官庁のホームページの改竄事件や2001年2月の.jpドメインサイトに対する集中的な不正アクセス被害、また2001年5月、7月、9月に発生したワーム等による大量感染被害など、セキュリティ、サイバーテロ、ハイテク犯罪への問題がクローズアップされている。法制面においても2000年2月施行の「不正アクセス禁止法」等、情報セキュリティ対策が重要であることが認識されている。

本調査はインターネットに係る我が国の社会経済活動における情報セキュリティ上のリスクを把握するため、各種統計資料及び、実際のデータからモデルを提示して試算を行い、情報セキュリティに係る基礎データをうることを目的とし、試算結果をまとめたものである。

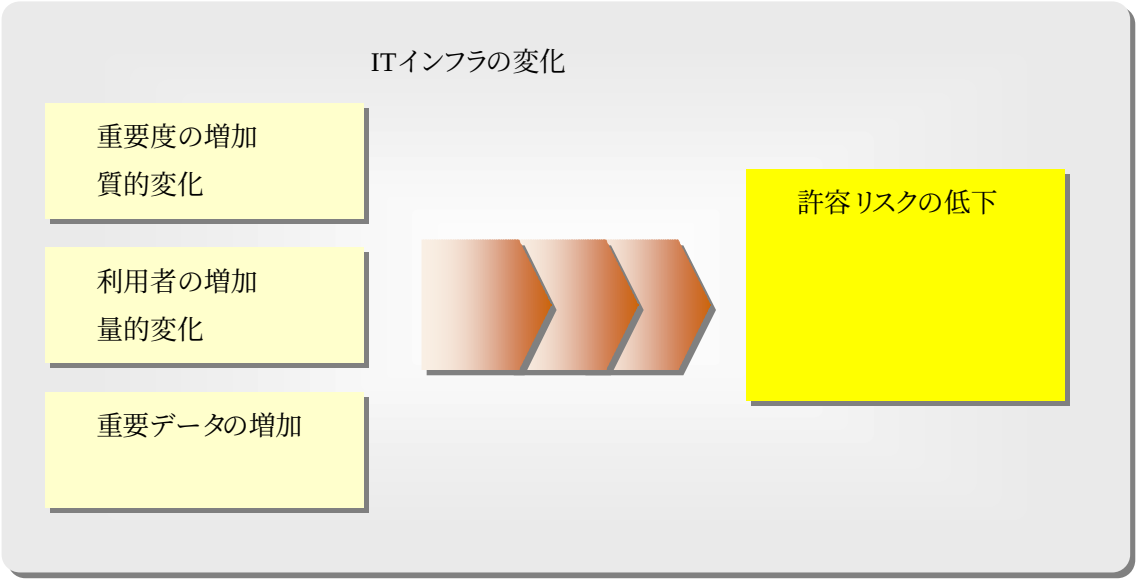
2. 体感的なITインフラの変化とセキュリティ侵害の関係

ネットワークの普及に伴い、ITインフラの重要度が増している。
また、これにあわせるように、不正アクセス等セキュリティ侵害行為のターゲットとなる確率が増えていると思われる。 ここでは、この二つの流れについて、統計情報等を元に裏づけを行う。



2.1. ITインフラ側の変化

インターネットの急速な普及に伴い、ITインフラは社会、経済のインフラストラクチャとして重要な機能を果たしている。また、その状況も変化している。すなわち、インフラの重要度の増加という質的な変化、利用者の増加という量的な変化、そして直接に商品、金銭、個人のプライバシーにかかわるような重要データが増加している点である。
これらの要因によってITインフラの障害、停止、改竄、不正アクセスなどセキュリティ被害に対する許容リスクはますます低下していると考えられる。

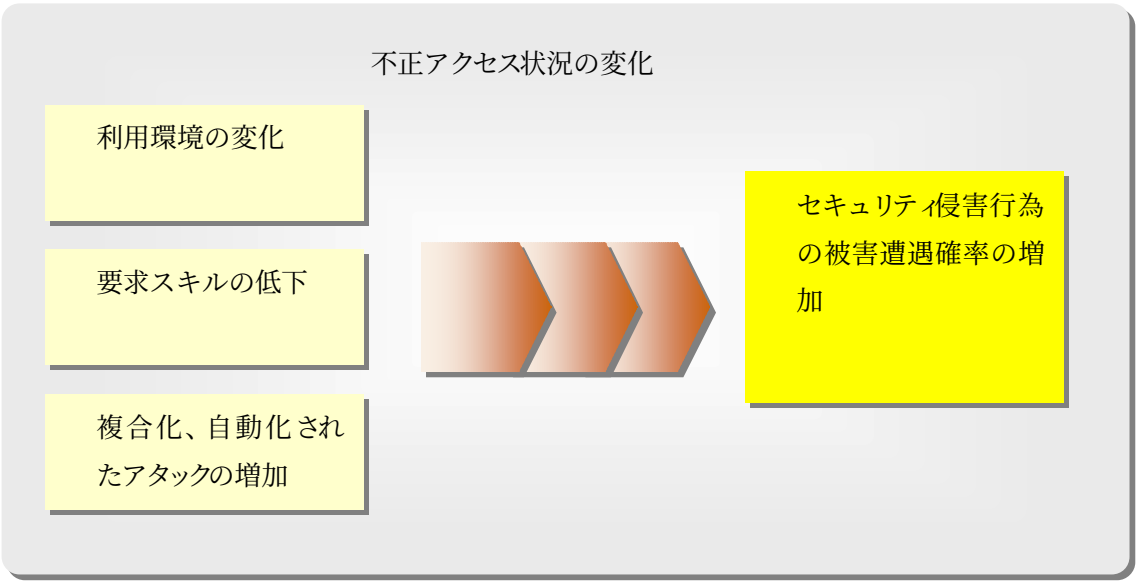


2.2. 不正アクセス側の変化

不正アクセス等セキュリティ侵害行為の状況をみると、常時接続やブロードバンドの普及など利用環境が大きく変化している。さらに、GUIを備えるなど攻撃者が容易に利用できるさまざまなツールが出回っていることや、多くの脆弱性情報が容易に入手可能になり、攻撃者の必要な要求スキルはますます低下している。

一方、特に2001年は複数の手段をくみあわせ、しかも自動化された攻撃ツールが登場し、「複合型の脅威」が問題となった。これらの攻撃は旧来のファイアウォールのみでは防ぐことが困難である。

これらの要因から不正アクセスの被害遭遇確率が増加していると考えられる。

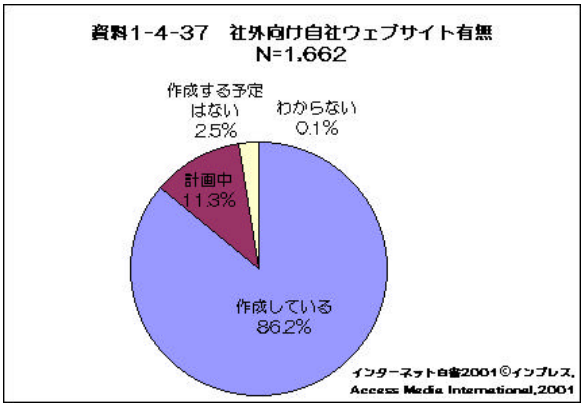


3. ITインフラ重要度の変化

3.1. 情報インフラとしてのネットワーク利用の普及 I

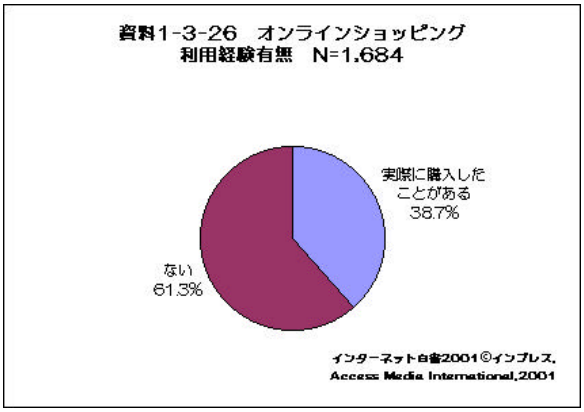
3.1.1. Webは、媒体として重要な位置をしめている

5年前であれば、企業のWebを運営しているのは、社内の有志であり、簡単な企業紹介にとどまるものがほとんどであった。しかし、現状では、単なる情報提供にとどまらず、製品情報の提供やカタログの配布、また、ソフトウェアの配布やバージョンアップ等、事業の根幹にかかわる利用が行われている。



3.1.2. Webは、商取引のインフラとして機能している

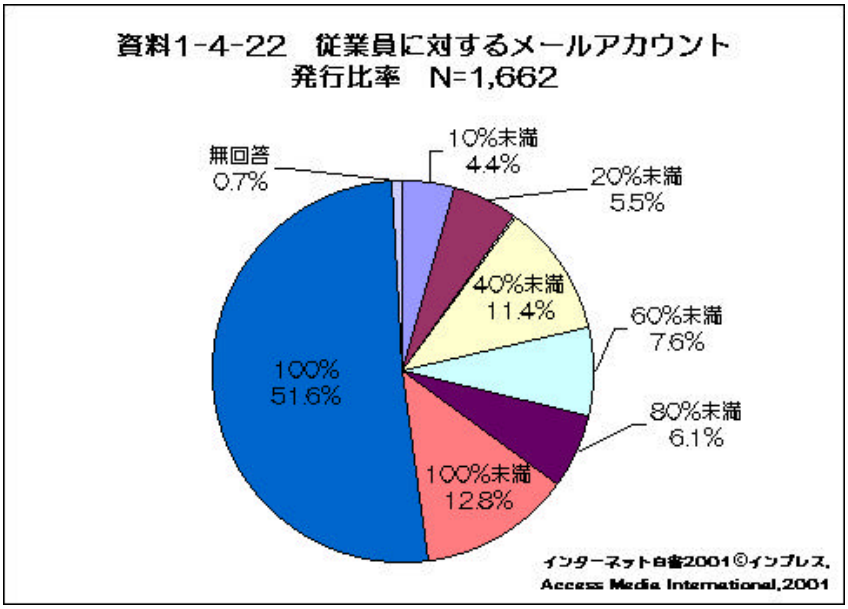
また、近年ではオンラインバンクや商品販売のプラットフォームとして利用されており、このようなケースでは、事業の重要な基盤としてWebが利用されている。



3.1.3. 電子メールの利用

一方でメールの推移を見ると、すべての従業員にメールアカウントを発行している企業が、50%を超え、70%以上の従業員にメールアカウントを発行している企業は、7割に上る。

実際の企業活動においても、メールは電話と並ぶコミニュケーション手段として地位を確立したと考えられる。すでに、取引先との連絡、企業の情報発信、社内の連絡などにおいて、媒体として重要な位置を確立しているといえる。



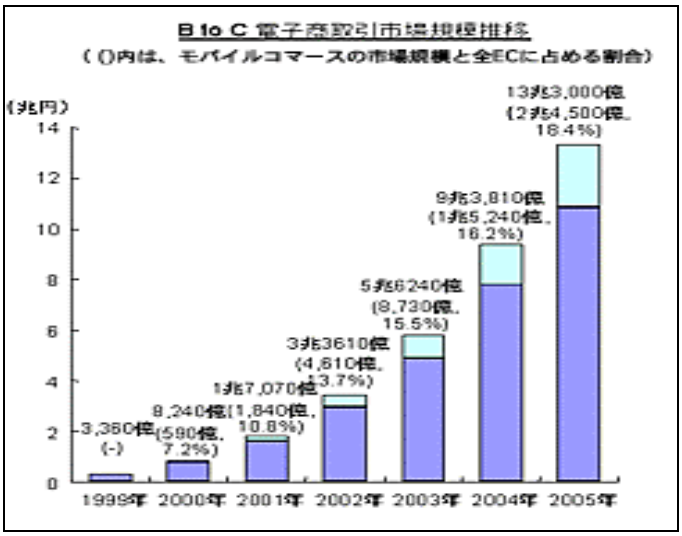
3.2. 情報インフラとしてネットワーク利用の普及II

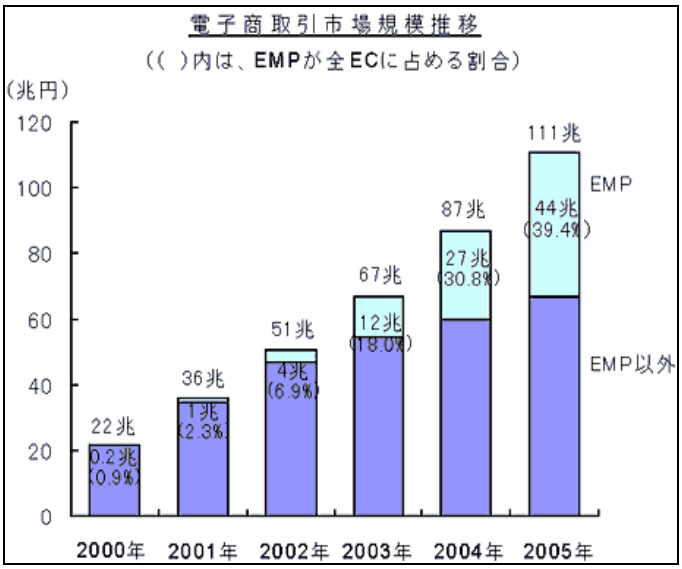
3.2.1. 電子商取引の市場規模

電子商取引は、遠隔地でもインターネットを利用できるところであれば、どこであっても24時間アクセスができる利便性があることから、企業対個人（B to C）、企業対企業（B to B）いずれにおいても急増している。今後もB to B,B to Cともに拡大、成長が予測されている。

B to Cにおいては携帯電話やPDAを利用するモバイルコマースの増加も予測されている。

また、企業間取引においては、複数の売り手と買い手がある種の市場を形成するE-マーケットプレイス（EMP）の割合が増加している。

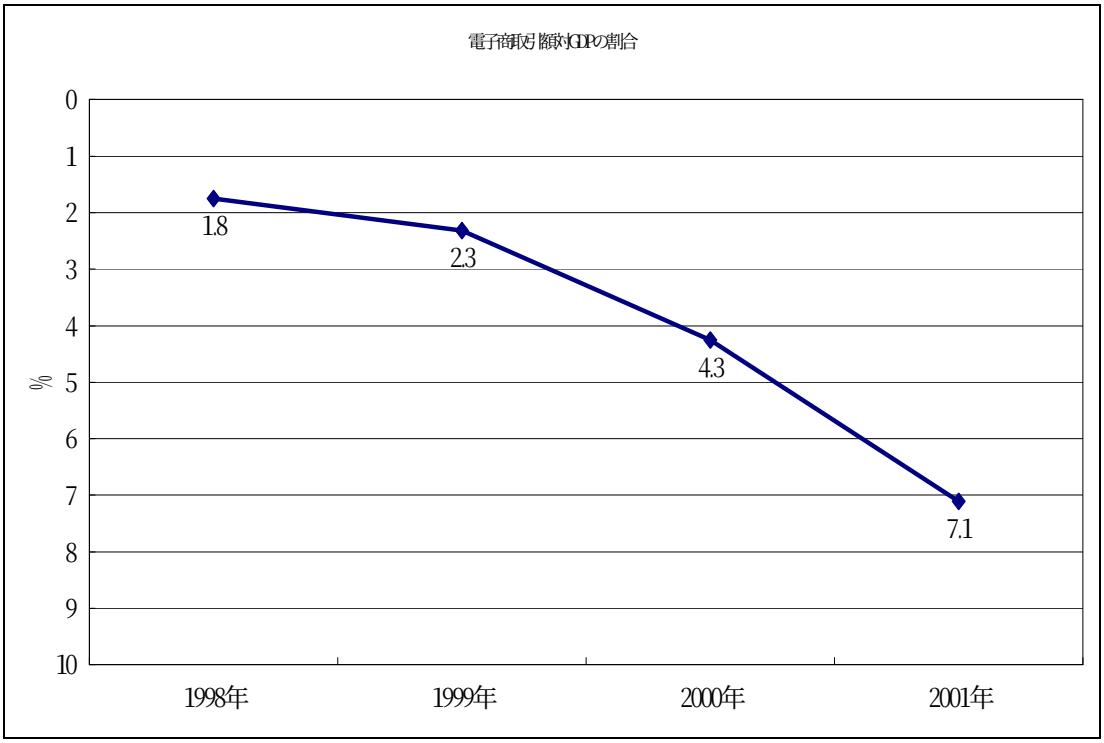




アクセンチュア、ECOM、経済産業省「平成12年度電子商取引に関する市場規模、実態調査」

3.2.2. 電子商取引対GDPの割合

電子商取引金の増加は国民経済全体（GDP）に占める割合でみると、1998年の1.7%から2001年では7.1%と4倍以上に増加している。経済への影響度はそのままリスクへの許容範囲が狭まっていくことを示している。



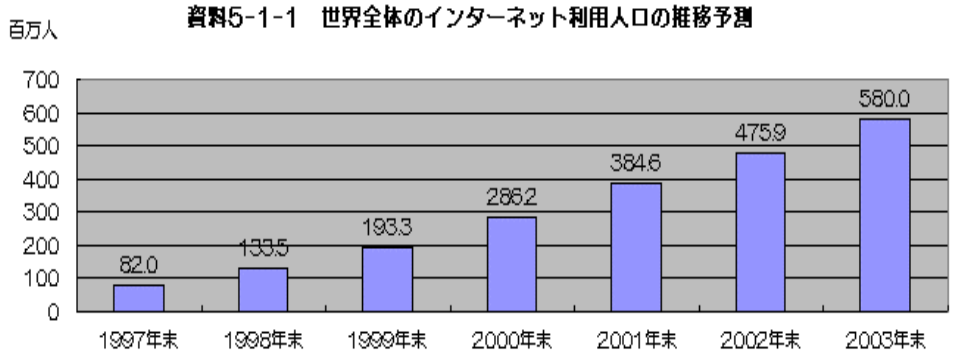
通商産業省 「日米電子商取引に関する市場規模調査」、
内閣府 「国民経済計算」(GDP2001年は速報値より)

3.3. ITインフラ利用者の増加

3.3.1. インターネット利用者の増加

一方で、インターネットの利用者が増加した事も、不正アクセスが拡大した要因として見逃せない。世界レベルでみると、2000年は、1997年の 7倍程度の利用者となっている。特に日本を除くアジア太平洋地域の伸びは驚異的で、2000年末には全世界が前年度1.48倍であるのに比べ、2.26倍にも達している。

資料5-1-1　世界全体のインターネット利用人口の推移予測



内訳　　百万人

地域名	1997年末	1998年末	1999年末	2000年末	2001年末	2002年末	2003年末
アメリカ合衆国	41.2	64.7	85.0	102.0	115.5	128.0	140.0
カナダ	2.4	4.3	9.6	13.0	15.8	18.4	21.0
ヨーロッパ	21.4	32.9	49.5	72.5	122.0	163.0	212.0
日本	8.8	14.3	18.3	30.4	36.3	42.0	48.0
アジア太平洋地域(日本を除く)	7.0	14.5	27.0	61.1	83.5	107.0	134.0
南アメリカ	0.6	1.5	2.3	4.2	6.5	9.5	13.0
その他の地域	0.6	1.3	1.6	3.0	5.0	8.0	12.0
全世界	82.0	133.5	193.3	286.2	384.6	475.9	580.0

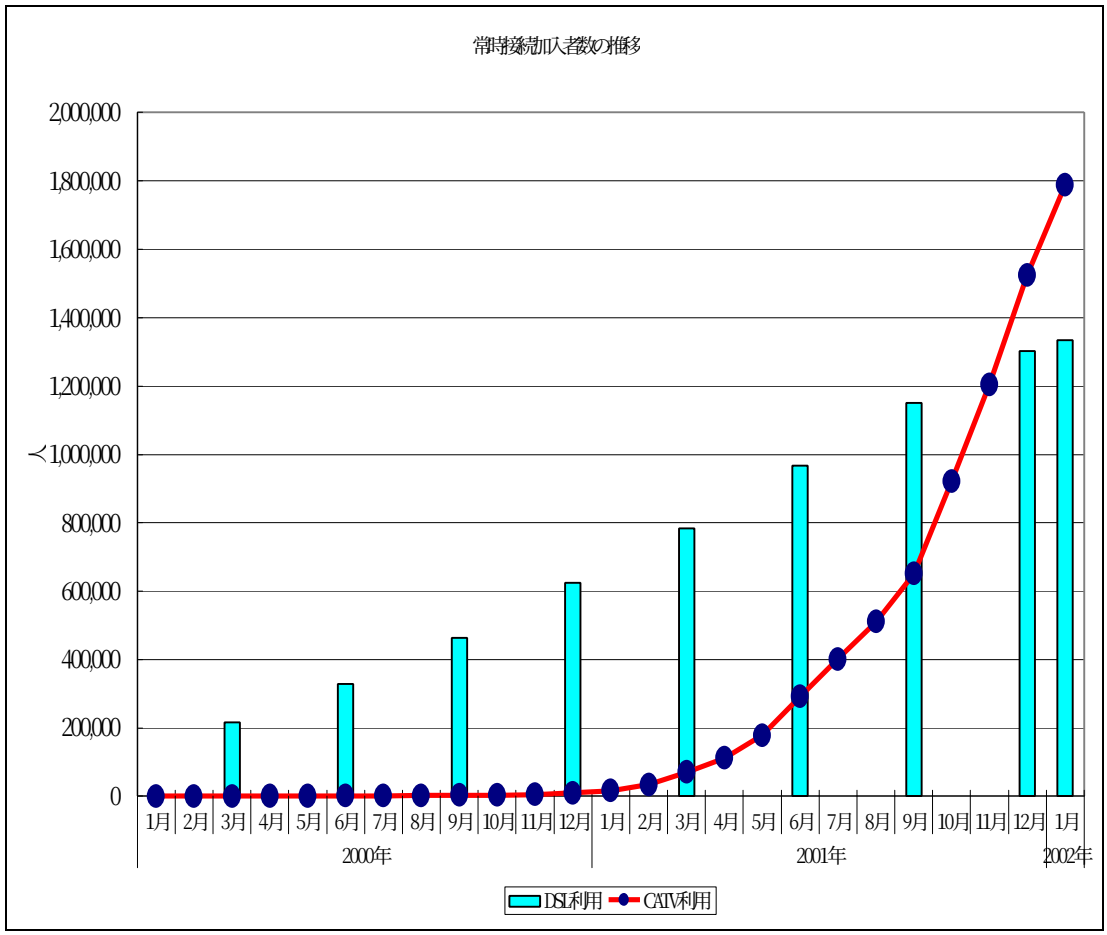
©Access Media International,2001

インターネット白書　2001

3.3.2. 常時接続端末の増加

DSL加入者は2001年1月以降急激に拡大している。全体の利用者が増えたことに加えて、常時接続の利用が増えたことは、インターネット環境に大きく影響している。

PCを単純に常時接続の環境に置いた場合、一般的にセキュリティ対策が甘く、他のサイトへの不正アクセスを行うための、踏み台として利用されたり、ワームが増殖するための基盤のひとつとなっている。CATVによる常時接続の加入者も2001年末では120万人を超えている。

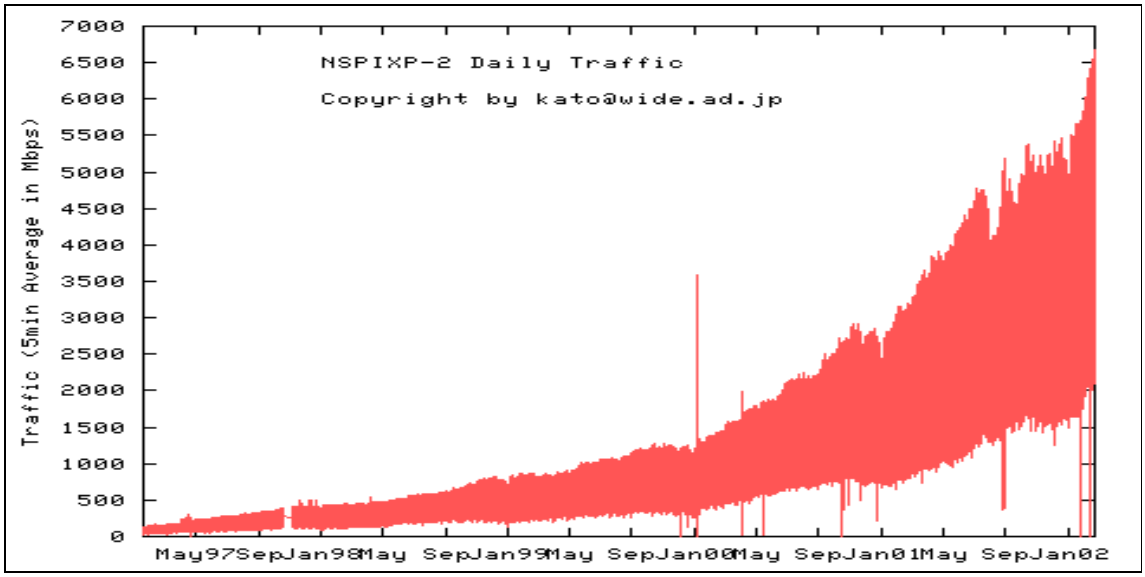


総務省　総合通信基盤局　DSL普及状況公開ページ及び
インターネット接続サービスの利用者数等の推移【平成14年1月末現在】速報）
より作成

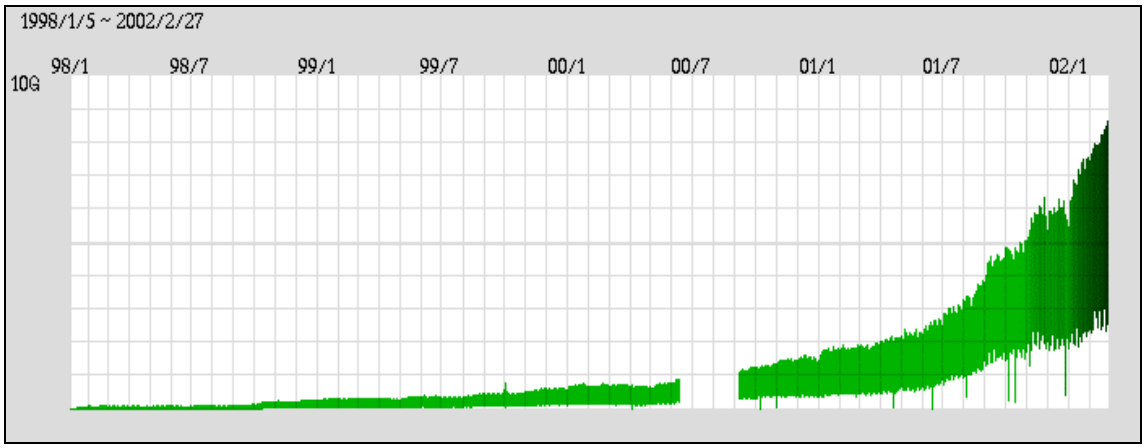
3.4. インターネット利用状況の変化

3.4.1. インターネットトラフィックの変化

インターネットのバックボーン回線はISP(インターネットサービスプロバイダ)の相互接続点であるIX（インターネットエクスチェンジ）から放射状に構築されている。したがって、IXの トラヒック量の変化を見ることにより、インターネット全体の トラヒックを見て取ることができる。代表的なIXのひとつであるNSPIXP2をみても、2000年1月以降急激な増加をみせており、2002年2月ではピーク時6.5Gbpsを超えている



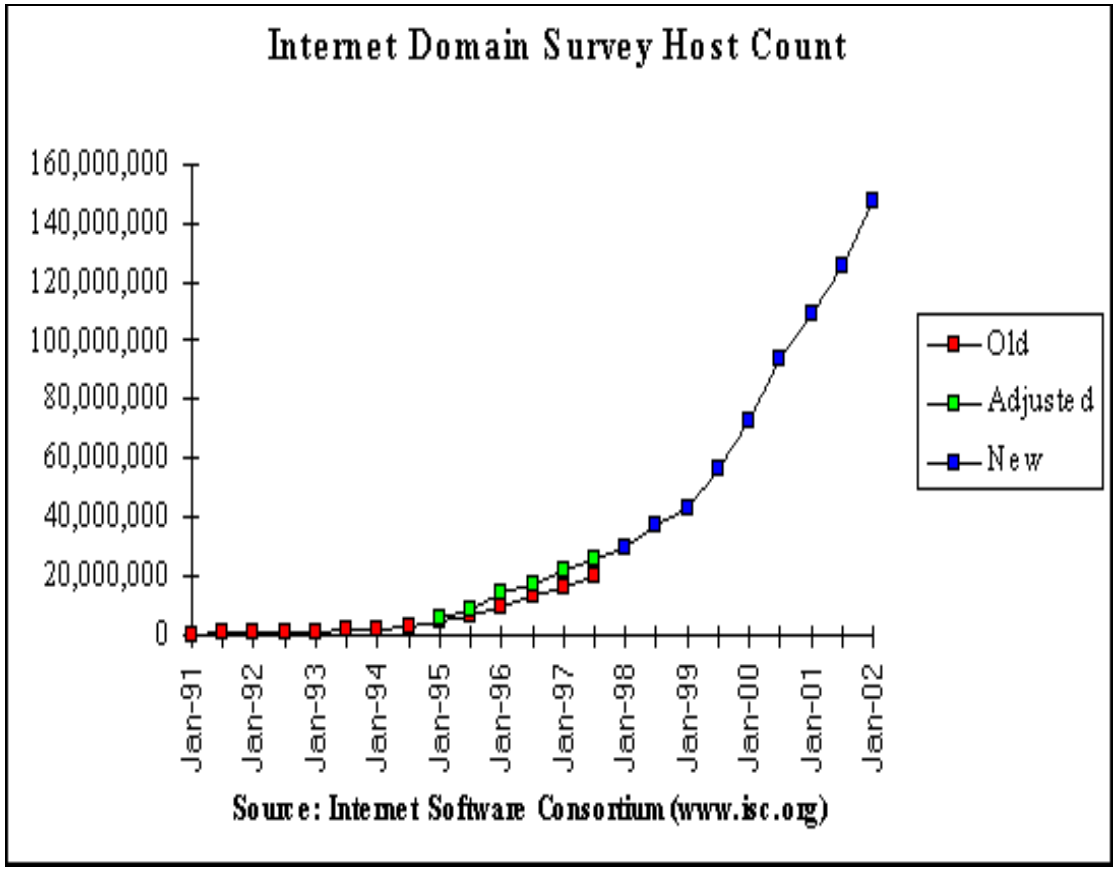
NSPIXP2　Wideプロジェクト資料より



JPIX　日本インターネットエクスチェンジ資料より
両グラフとも、1日における最大値、最小値の振幅

3.4.2. サーバ数の増加

1990年代前半では、100万台以下であったホスト数は1996年には1000万台を超え、1999年以降急激に増加率が高まっている。2001年1月において、接続台数は1億台を超え、2002年1月では1億5千万台となっている。[1]



[1] Old (1997年以前)ではDNSから接続Hostを計算。
New (1998年以降)ではIPアドレスから割り当て済みHostを計算。

3.4.3. WWWコンテンツの拡大

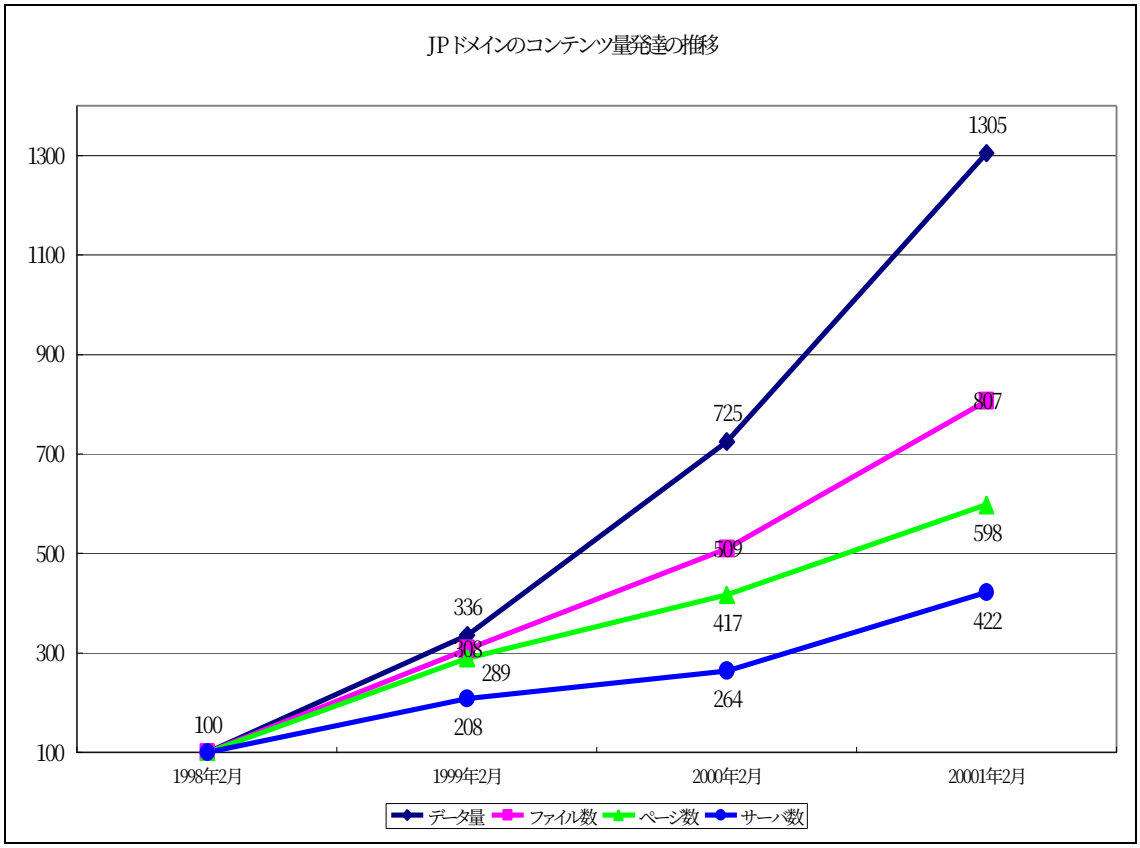
インターネット利用の拡大とともに、WWWコンテンツも大容量化、多様化してきている。

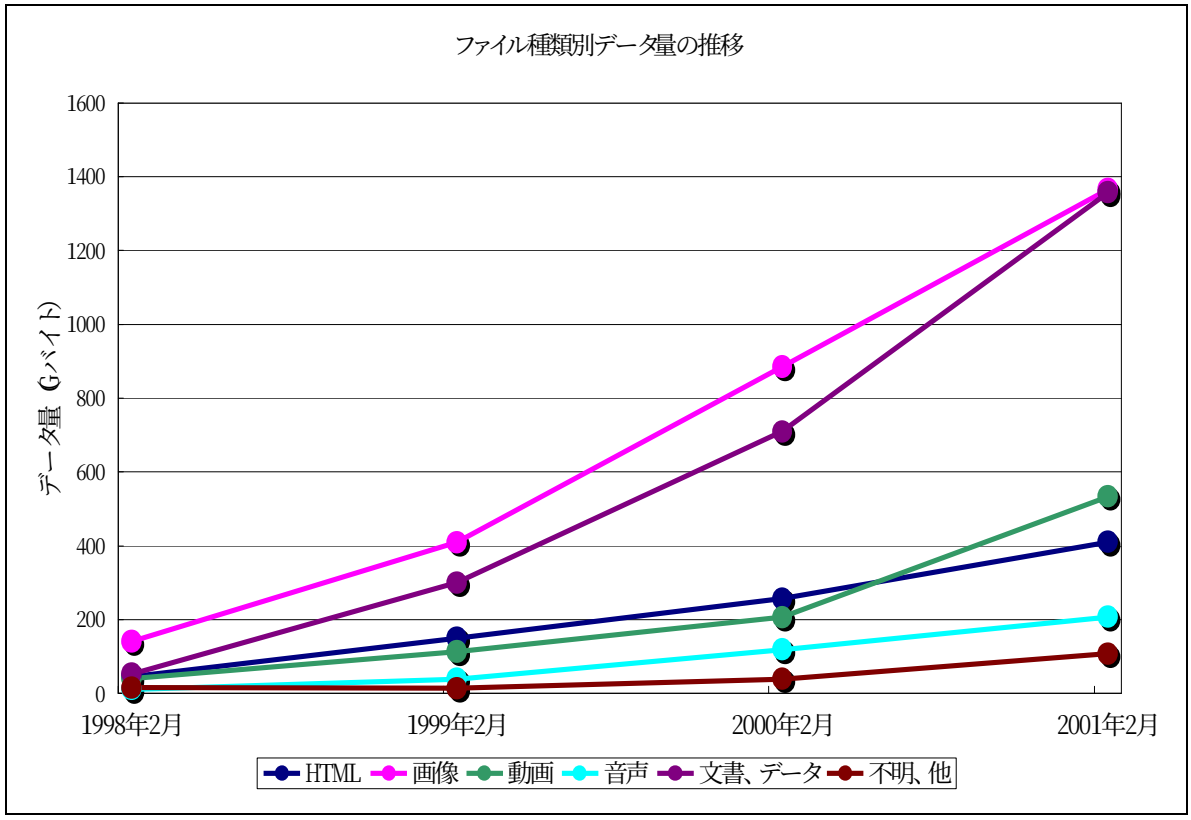
2001年2月の数値ではWWWサーバ数は1998年2月の4倍以上、データ量は13倍以上になっている。

これらのサーバでどのような情報が発信されているのかをファイル種別ごとにみると、文章．データや画像ファイルのほかに動画が増加傾向にある。今後ブロードバンドの普及とともに動画、音声が増加していくものと思われる。

グラフは1998年2月を１００として推移をしめす。

	1998年2月	1999年2月	2000年2月	2001年2月
総データ量（Gバイト）	305	1024	2214	3980
総ファイル数（万ファイル）	1891	5822	9267	15260
総ページ数（万ページ）	1020	2950	4250	5101
WWWサーバ数（台）	36000	75000	95000	152000





郵政省　現総務省）郵政研究所
第1回から第7回WWWコンテンツ統計調査より作成[2]

2.「WWWコンテンツ調査」は統計用サーチ型ロボットエンジン(Loki)によりJPドメインのWWWページを探索訪問し、調査している。
各ファイルの種類は拡張子により判断している。拡張子の分類は以下のとおり

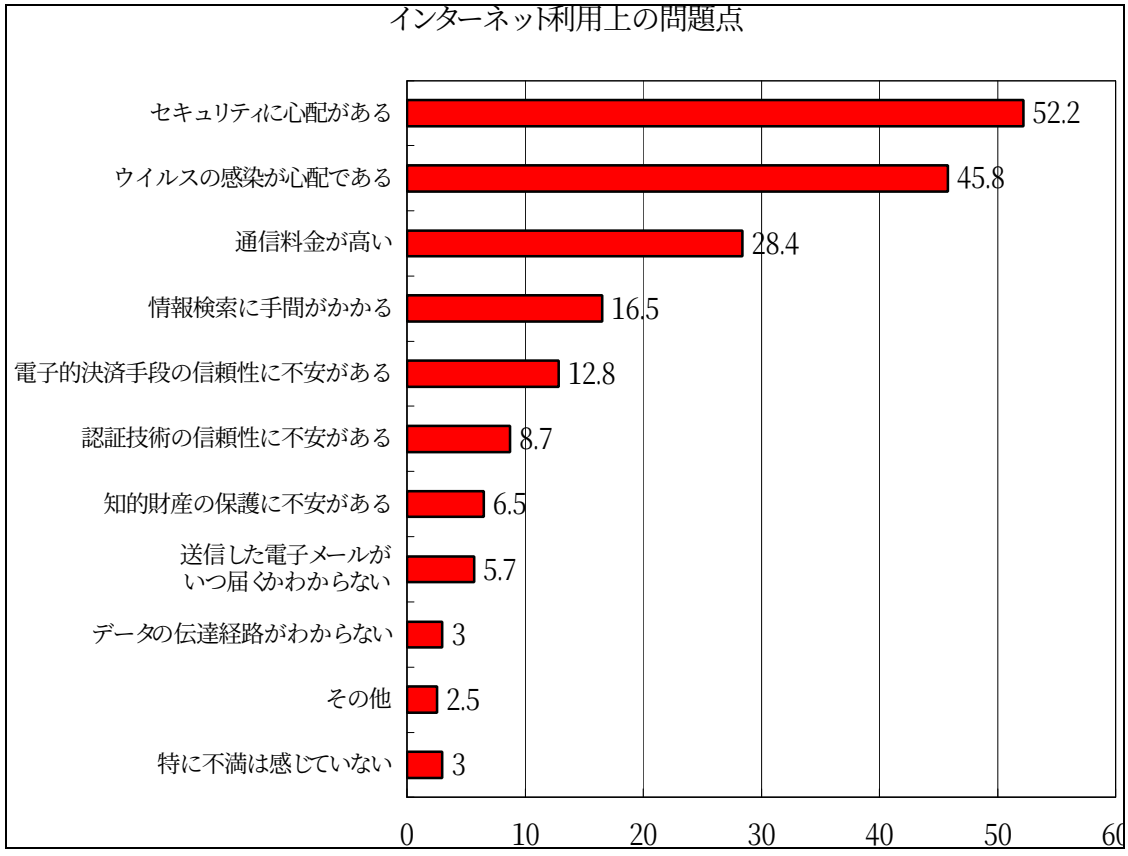
HTML	.html, .htm
画像	.jpg, .gif, .bmp, .pict, .tif, .eps, .png
動画	.mpg, .avi .mov
音声	.au, .ra, .midi, .mp3, .rmi, .wav
文書、データ	.pdf, .txt, .doc, .jbw, .lzh, .tar, .xls, .exe, .java
不明、他	その他のファイル

3.5. インターネット利用者側の問題

ここまで、インターネットの利用が拡大することを見てきたが、一方で利用者へのアンケートからはインターネットの利用には問題点、セキュリティへの不安があることが示されている。

3.5.1. インターネット利用上の問題

インターネット接続している企業(従業員100人以上、1718社)へのアンケートから、利用上の問題点として最も多くあげられているのがセキュリティへの心配である。ウイルスも広くセキュリティとしてとらえるとすれば、利用上の問題点とはセキュリティへの心配であるということができる。

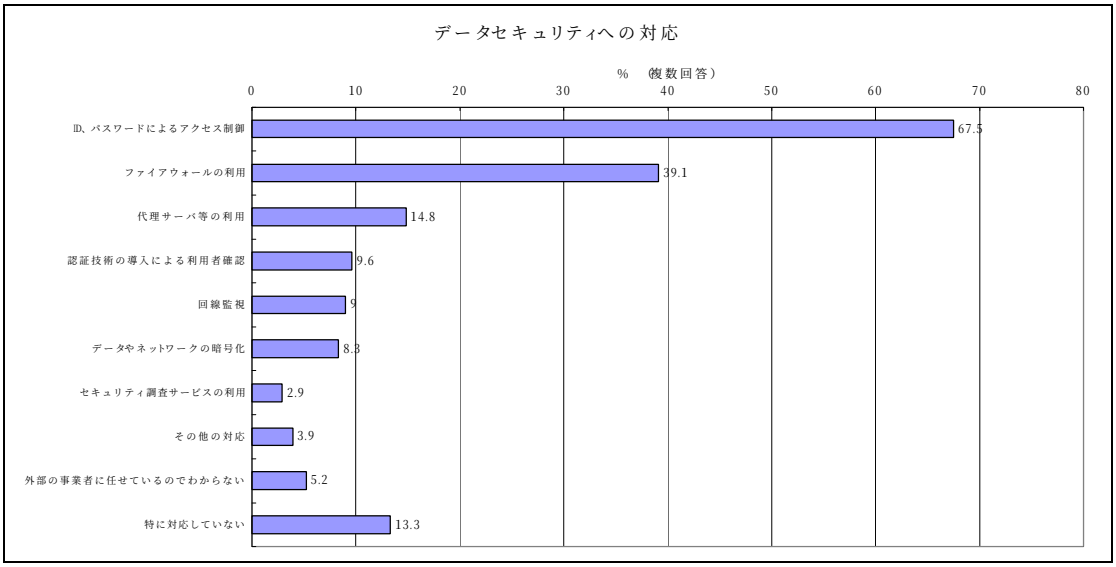


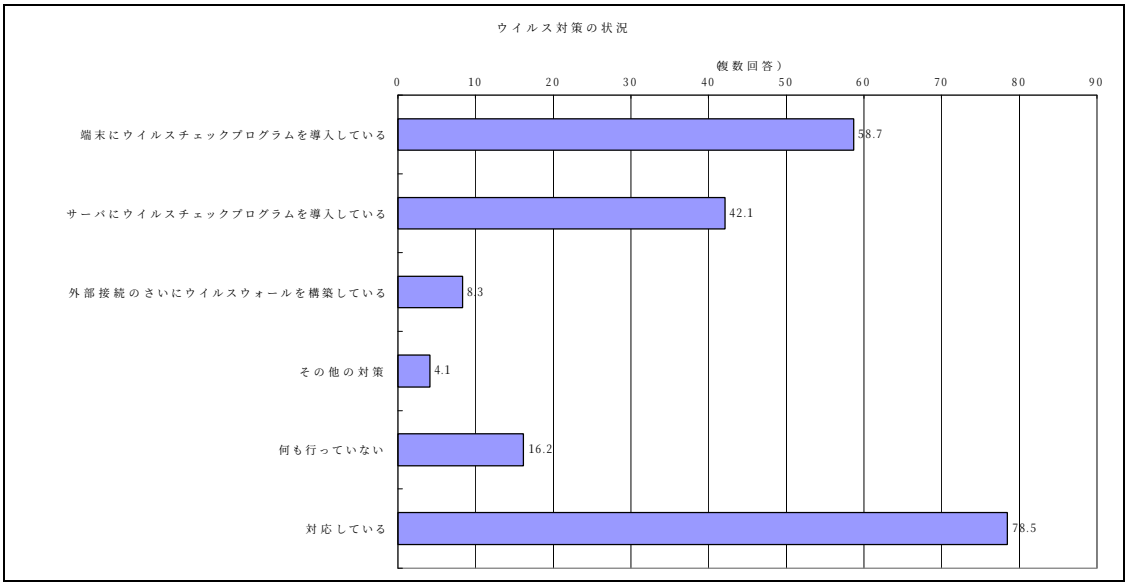
総務省「平成12年度通信利用動向調査（企業編）」

3.6. 被害を防ぐための対策

3.6.1. データセキュリティへの対策とウイルス対策

セキュリティ被害を防ぐための対策に対する総務省のアンケート結果を見ると、ファイアウォールの設置という最も基本的な対処も40%以下であり、その他の対応はほとんどなされていない状況[3]である。ウイルス対策については、何らかの対応がなされている企業が多いことがわかる。





総務省　平成12年通信利用動向調査　（企業編）

[3] 調査期日は2000年11月である。

3.6.2. ファイアウォールでの限界

ファイアウォールの設置は基本的な対応策の一つではあるが、その限界も認識する必要がある。2001年に発生したCodeRedワームは公開用WebサーバにHTTPを利用して感染するため、通常のファイアウォールでは阻止することができず、短期間のうちに数十万台といわれるサーバが感染した。Solarisマシンを踏み台にして、マイクロソフト社のIISを攻撃し、Webページを改竄するSadmin/IISもIISのセキュリティーホールを利用して大量の改竄被害が発生した。複数の感染経路を持つNimdaでは自宅に持ち帰り感染したNote　PCを社内ネットにつないだことにより社内からの感染被害が発生する。この場合にも社内からの攻撃であるので、ファイアウォールは通常機能しない。

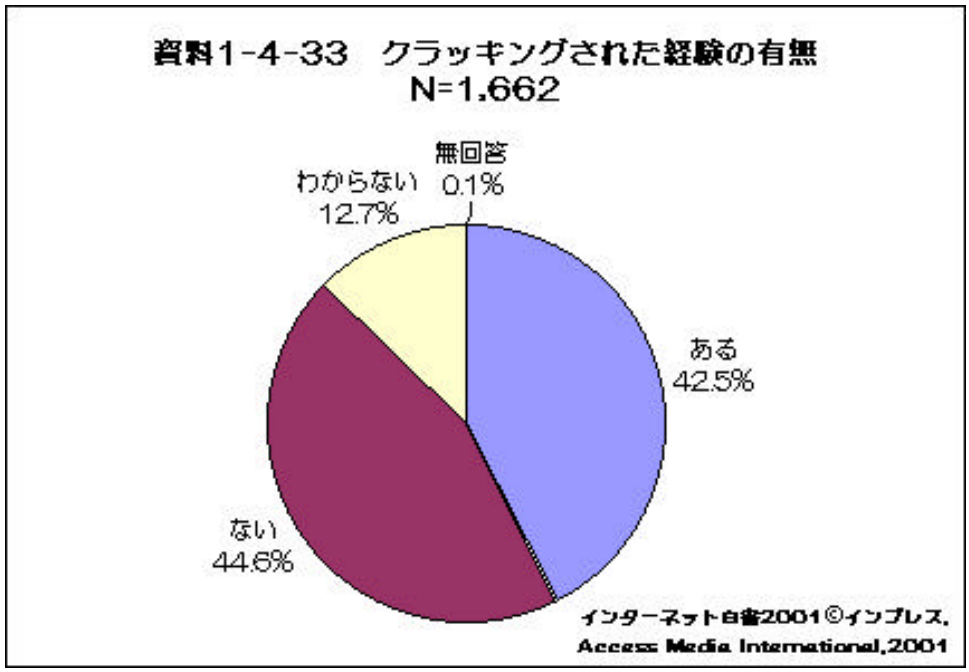
ファイアウォールの限界として以下の項目をあげることができる。

- ファイアウォールそのものの脆弱性を利用するもの
- 設定ミス、セキュリティホール、DOS攻撃
- E-Mailを介したワームやウイルス
- 外部Webページのコンテンツに含まれたスクリプトによる攻撃
- Webサーバの脆弱性をつくような、外部に開いているポートを介しての攻撃
- Web書き換え、WebサーバへのDos攻撃など
- 不正なメール中継

4. 不正アクセスの被害

4.1. 企業のクラッキングされた経験

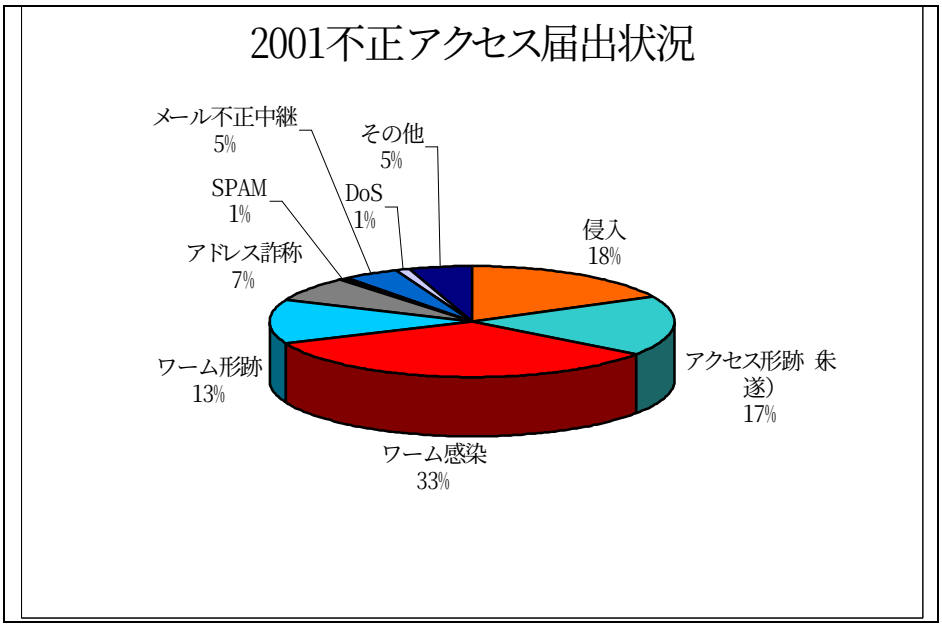
Webの改竄に限らず、不正アクセスを経験したサイトは、42.5%にも達している。このアンケートにおいては、クラッキングの経験の定義を「アタックの痕跡までを含み、実際の被害の有無は問わない」としている。

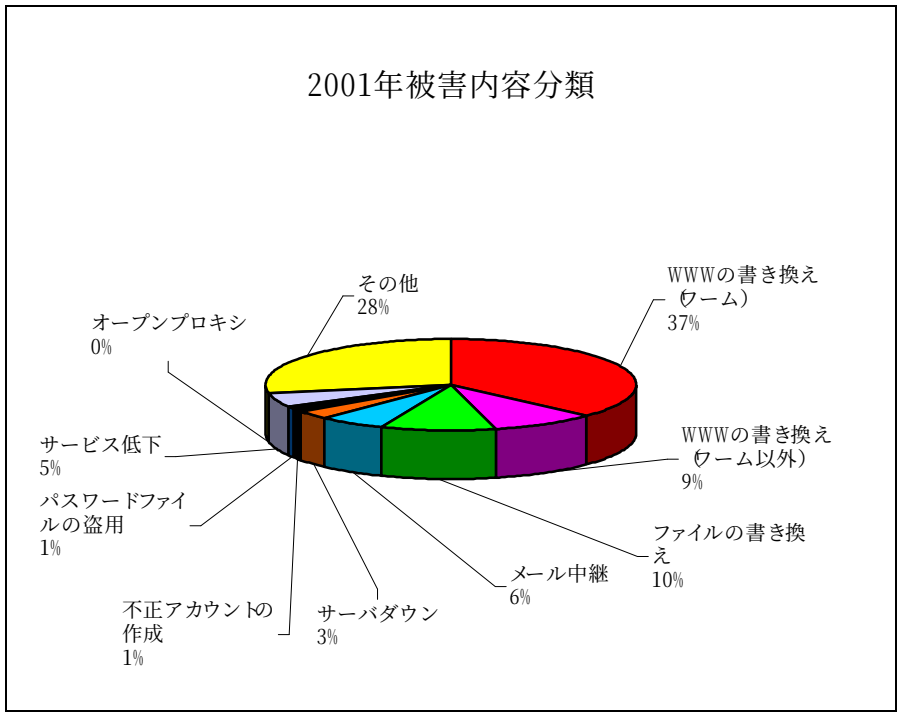


4.2. 不正アクセス被害の内容Ⅰ

4.2.1. IPA/ISECへの届出の内容

2001年に情報処理振興協会（略称IPA）に届出のあった550件のうち、実際に被害に及んだケースは約7割である。アクセス形跡（未遂）とはファイアウォールやサーバのログに不正アクセスの形跡があったものである。特にワーム感染とワーム形跡をあわせると46%であるが、これらはSadmin/IIS、CodeRed、Nimdaなどのセキュリティホールを複合的に悪用する新しいタイプの不正アクセスと考えられる。IPAにおいても「今後新たな脅威としてとらえる必要がある」としている。 特にこれらのタイプの不正アクセスでは、感染後、自らが感染元となり、被害者から加害者へ立場が逆転してしまう場合がある。届出を行った企業はセキュリティに関心の高い企業であると考えられ、ログの監視などで未遂のアクセス形跡を把握しているケースが17%である。セキュリティ対策が不十分である場合には被害がその企業内に拡大するか、2次感染先からの指摘によるまで対応がとられずに、さらに被害を拡大させてしまうケースが少なくないと思われる。届出のうち実際に被害に及んだケースに関する内容を分類すると半数近くがWebサーバの書き換えの被害である。2001年5月のsadmin/IISワームの感染による被害が影響している。一方ワームの感染を除いて考えると、メール中継が6%、サーバダウンおよびサービス低下をDOSと考えて足し合わせ8%、さらにその他が28%あり、攻撃が多様であることを示している。

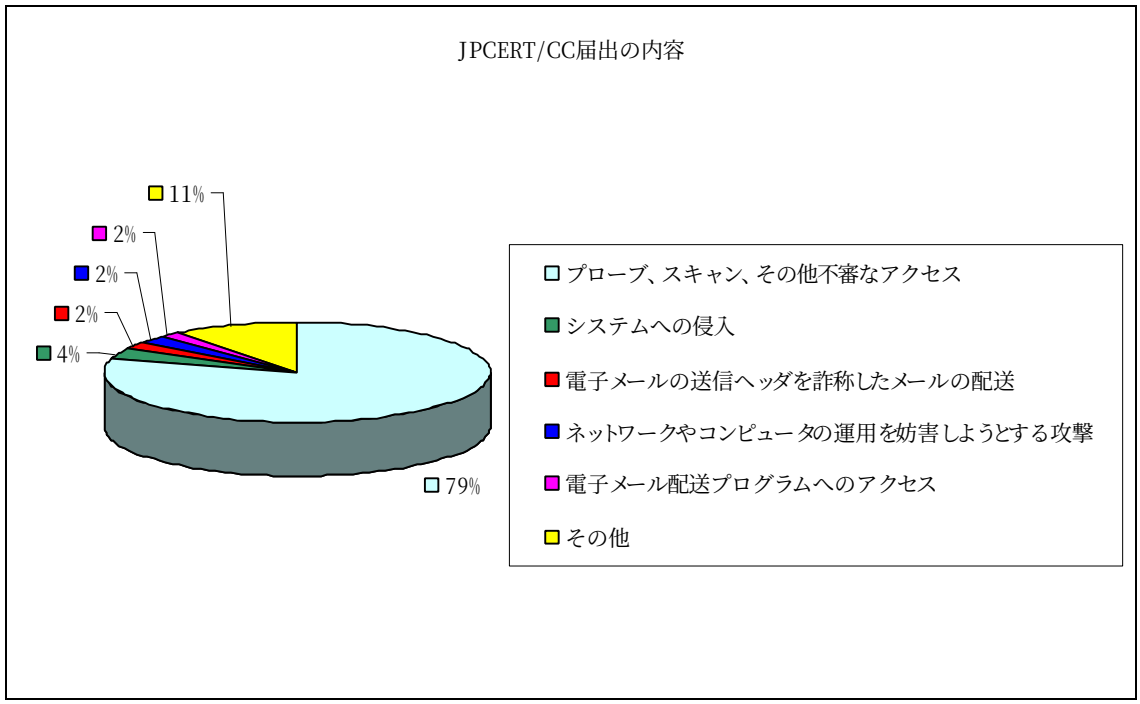




情報処理振興協会セキュリティセンター（IPA/ISEC）
2001年不正アクセス届出状況

4.2.2. JPCERT/CCへの届出の内容

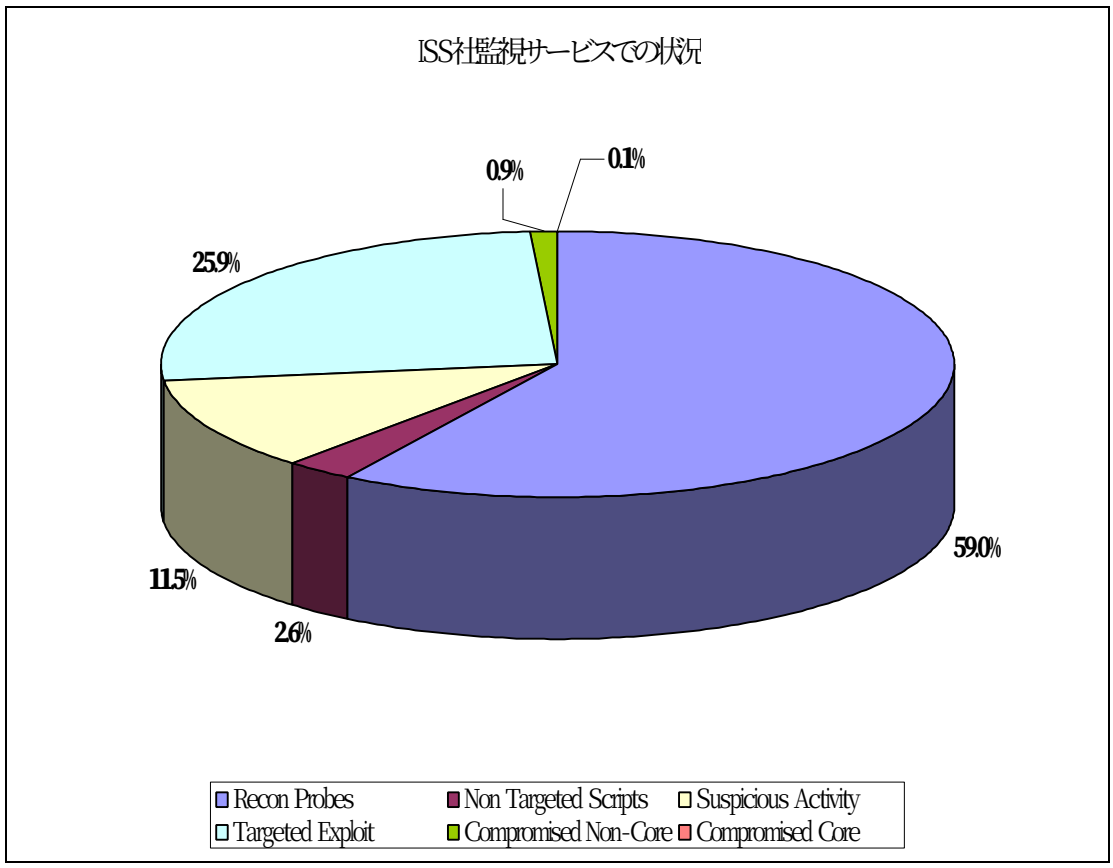
2001年コンピュータ緊急対応センター（JPCERT/CC）に届出のあった２８５３件の状況を見ると、プローブ、スキャン、その他不審なアクセスに関する報告が約8割である。 この中には防御に成功したもの、システムのアクセス権において影響を生じていないものも含まれている。JPCERT/CCへの届出が任意であることから、常時ログ監視を行うなど比較的セキュリティ意識の高い管理者からの届出が多い状況を考慮する必要がある。しかしながら、運用を妨害するDOS攻撃（各種サーバ、ネットワーク装置が対象となる）、メール配送プログラムへのアクセスなど攻撃の対象はWebサーバに限らないことがわかる。



コンピュータ緊急対応センター（JPCERT/CC）資料より

4.2.3. ISS社監視サービスでの検出内容

インターネットセキュリティシステムズ社（ISS社）ではでの全世界7箇所に設置された監視センターにて、顧客に監視サービスを提供している。200年から2001年に対応を行ったインシデントの内訳をみると、プローブなどスキャン系の割合が半数を超えるが、一方で対象の,脆弱性を正確に認識し,明確な悪意をもった攻撃であることをしめすTargeted Exploitも25%以上である点に注目する必要がある。[4]



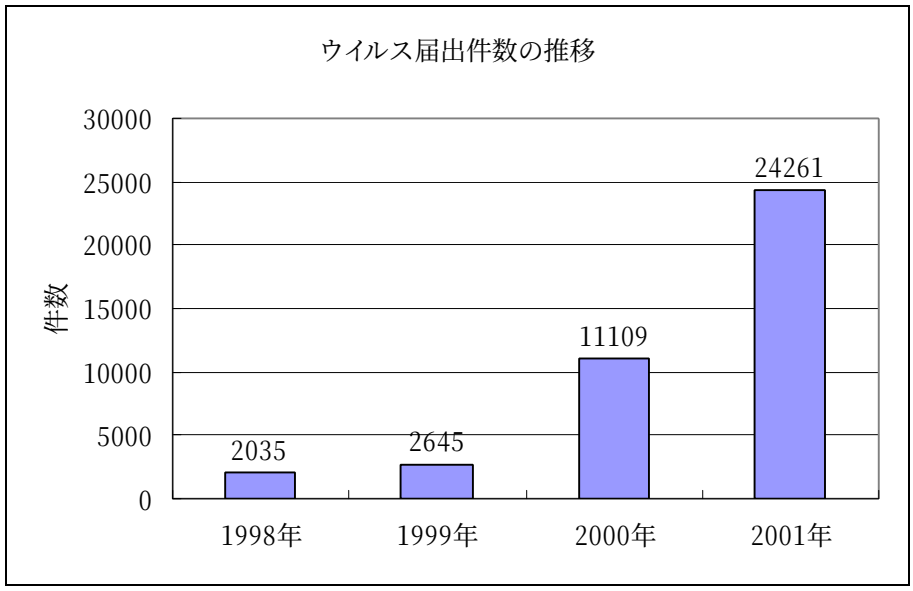
インターネットセキュリティシステムズ社資料

[4] インシデントは次の6種類に分類されている。

Recon Probes	偵察、プローブ、などいわゆるスキャン系アクティビティ
Non Trageted Scripts	攻撃対象を特定しないスクリプトによるアクティビティ
Suspicious Activity	意図的な攻撃か疑わしいアクティビティ
Targeted Exploit	明らかに攻撃対象を特定しているアクティビティ
Compromised Non Core	重要ではないがファイルの改竄を行うアクティビティ
Compromised Core	重要ファイルの改竄アクティビティ

4.3. 不正アクセス被害の内容Ⅱ IPAウィルス発見届出状況

2001年は前年に比べて2倍以上の届出があった。メール機能を悪用するものが多くあるが、セキュリティホールを悪用するものが急増している。また、Nimdaなど複数の感染経路を持つ複雑化したウイルスが現れている。



情報処理振興事業協会（IPA/ISEC）資料

4.3.2. 個人情報の漏洩

個人情報の漏洩も問題としても見逃せない。具体的な件数を明らかでないものの、民間企業、地方自治体などで重大な個人情報漏洩事件が相次いで報道されている。

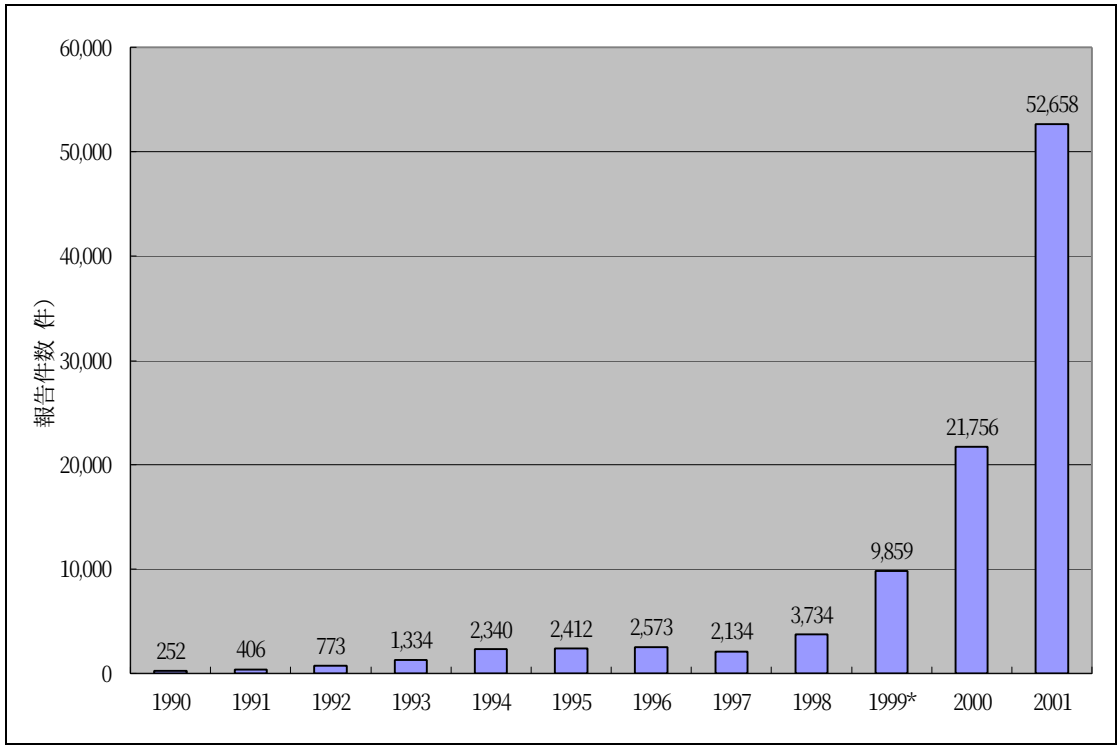
たとえば、銀行からの2万件に及ぶ顧客データの流出。電気通信会社からの顧客情報の流出。大手インターネットプロバイダの利用会員のIDとパスワードの流出。大手人材派遣会社では登録スタッフ9万人分の個人データがインターネット上に流出、売買されてしまった事件。地方自治体では、全市民19万人に相当する住民票データが流出、これを名簿業者がインターネットのウェブサイトで販売していた。販売データは個人の住所、氏名、生年月日、性別、識別コードなど32項目が一覧表の形で掲載されていたとされる、などである。

電子化された個人情報は複製が可能なため、大規模な漏洩を引き起こす可能性がある。また、いったん複製され、一人歩きし始めたデータは無限に再生産される。高度情報化社会の個人情報の漏洩は 2次流通を阻止できないという点でも大きな問題がある。

4.4. 不正アクセス被害の増加

4.4.1. CERT/CCが受け付けた不正アクセス報告

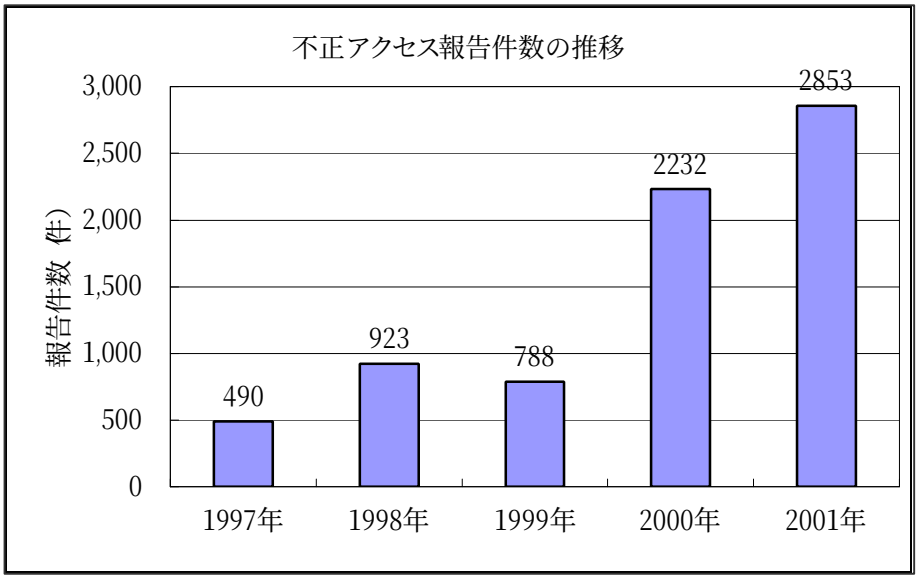
米国コンピュータ緊急対応センタ（CERT/CC）が受け付けた不正アクセスの件数の推移を見ると1998年以降、毎年前年の2倍以上の件数となっている。



米国コンピュータ緊急対応センター資料より

4.4.2. JPCERT/CCが受け付けた不正アクセス報告

コンピュータ緊急対応センター（JPCERT/CC）への不正アクセス届出の件数を見ると、200年は前年の2.8倍にも増加している。

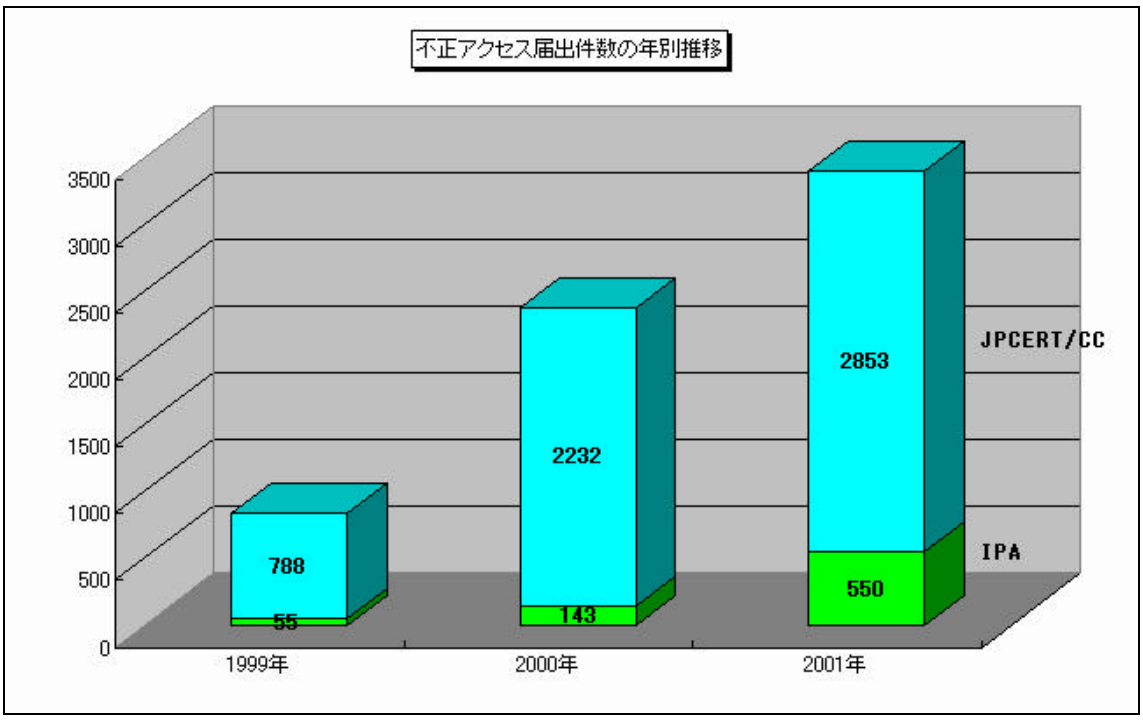


コンピュータ緊急対応センター（JPCERT/CC）資料より

4.4.3. IPA/ISEC、JPCERT/CC不正アクセス届出件数の推移

情報処理進行事業協会セキュリティセンター（IPA/ISEC）の2001年に受け付けた不正アクセスの届出は550件で前年（2000年）の143件から約3.8倍にも達している。IPAでは増加要因として、「個人ユーザの常時接続環境の普及」、「ワームの出現」としている。

なお、下図はIPA/ISECおよびJPCERT/CCの3年間の届出件数の推移をまとめて示している。



情報処理振興事業協会セキュリティセンター(IPA/ISEC)2001年不正アクセス届出状況

4.4.4. ハイテク犯罪検挙件数

2001年（平成13年）の検挙件数をみると、前年（2000年）に対して、約45%増加している。
また、ネットワーク利用犯罪が全体の88%を占めている。2000年2月施行の不正アクセス禁止法による検挙数も今後増加する傾向にあると思われる。

		平成13年	平成12年	平成11年
コンピュータ電磁的記録対象犯罪		63件	44件	110件
	電子計算機使用詐欺	48件	33件	98件
	電磁的記録不正作出・毀棄	11件	9件	7件
	電子計算機損壊等業務妨害	4件	2件	5件
ネットワーク利用犯罪		712件	484件	247件
	児童買春・児童ポルノ法違反	245件	121件	9件
	わいせつ物頒布等	103件	154件	147件
	詐欺	103件	53件	23件
	名誉毀損	42件	30件	12件
	脅迫	40件	17件	件
	著作権法違反	28件	29件	21件
	その他	151件	80件	35件
不正アクセス禁止法違反		35件	31件	件
合　　計		810件	559件	251件

その他には、銃砲刀剣類所持等取締法違反、薬事法違反、商標法違反、恐喝等がある。

警察庁　平成12年,13年ハイテク犯罪の検挙および相談受理状況等について

4.4.5. 不正アクセス行為の発生状況

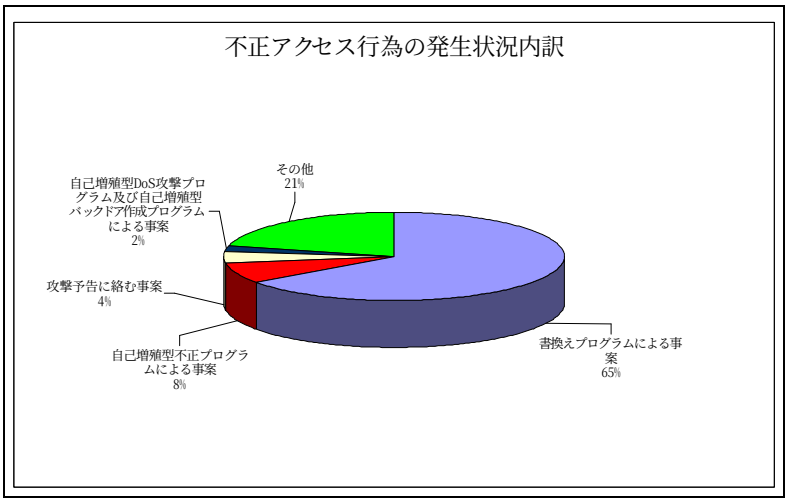
平成13年中に警察庁に報告のあった不正アクセス行為は1,253件で、前年の件数と比較して、約12倍となった。このうち、海外から不正アクセス行為が行われたことが判明しているものは448件で、前年の約18倍となった。発生状況の内訳のうち、特にホームページ書換え事案が65%をしめる。

		平成13年	平成12年	増減
認知件数	海外からのアクセス	448	25	423
	国内からのアクセス	258	73	185
	不明	547	8	539
	計	1,253	106	1,147

不正アクセス行為の大幅な増加の要因としては、

- ホームページ書換えプログラムによるホームページ書換え事案（813件）
- 自己増殖型不正プログラムによる事案（94件）
- 攻撃予告に関連すると思われるセキュリティホール攻撃型（55件）
- 自己増殖型DoS攻撃プログラム及び自己増殖型バックドア作成プログラムによる事案（28件）

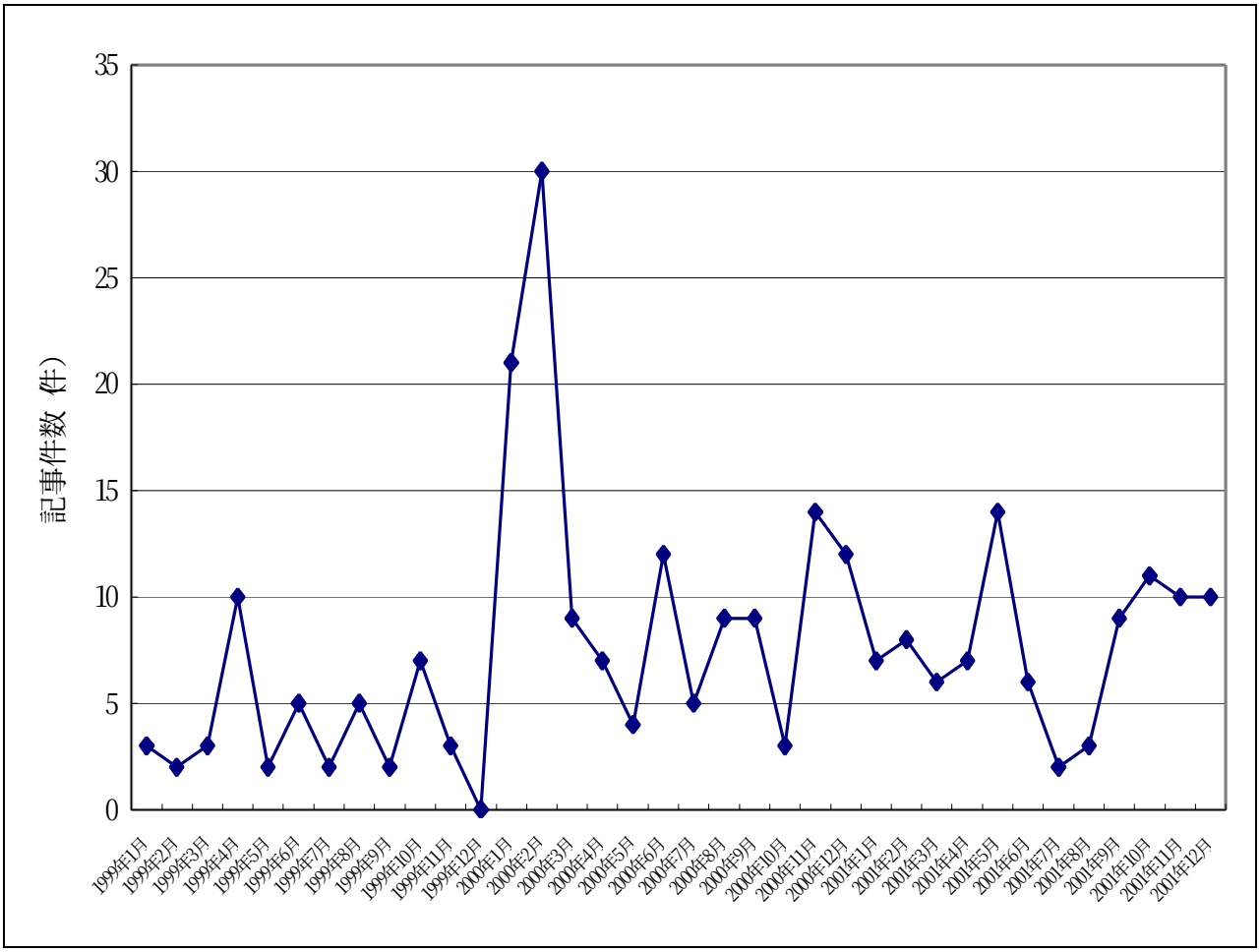
の発生が挙げられる。



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」

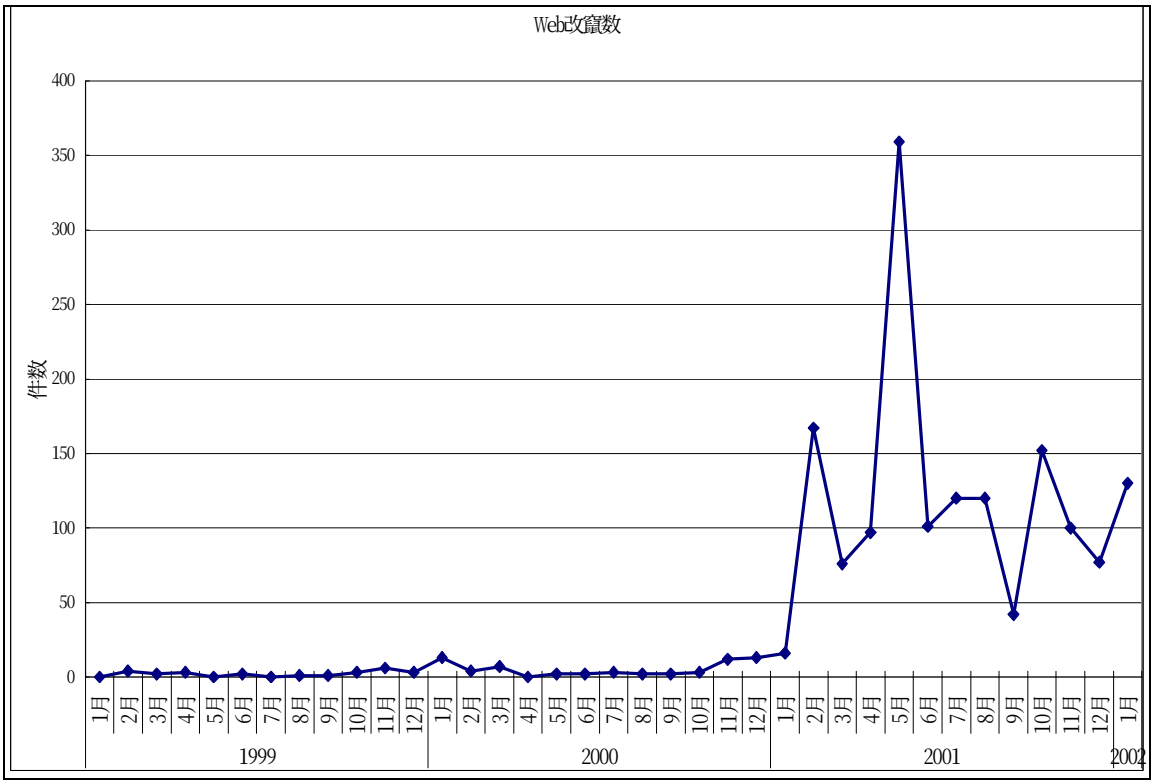
4.4.6. 「不正アクセス」記事件数

1991年1月より2001年12月までにA紙に掲載された記事の件数の移推を示す。記事件数と事件数との直接的な関連性をみてとることはできないが、2000年1月の集中的な官公庁Web改竄事件、2001年5月に発生したSadmind/IIS脆弱性を利用した多数のサイトへのWeb改竄事件など社会的な影響が高い場合には記事件数が多くなっている。なお、2000年11月には各県警などでの「県内で初の逮捕者、集団摘発」等の記事がおおくみられた。



4.4.7. 改竄されたホームページ数の推移

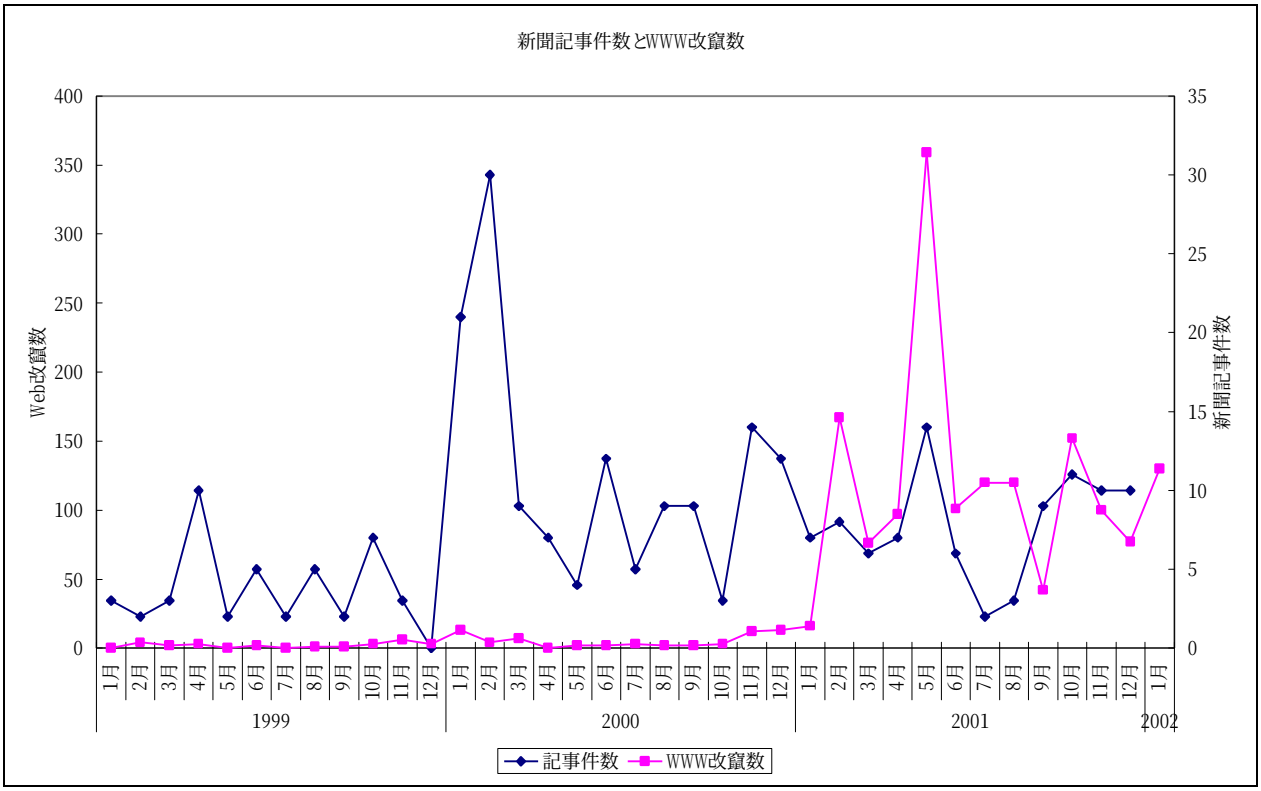
2001年5月の急増はSadmind/IISの脆弱性をついた攻撃により多数のサイトが被害をうけた。それ以降は多少の変動はあるものの、100件前後を中心に増加の傾向にある。



Everyday People クラッキングされてしまった日本のサイト より作成

4.4.8. 新聞記事件数とWeb改竄件数の比較

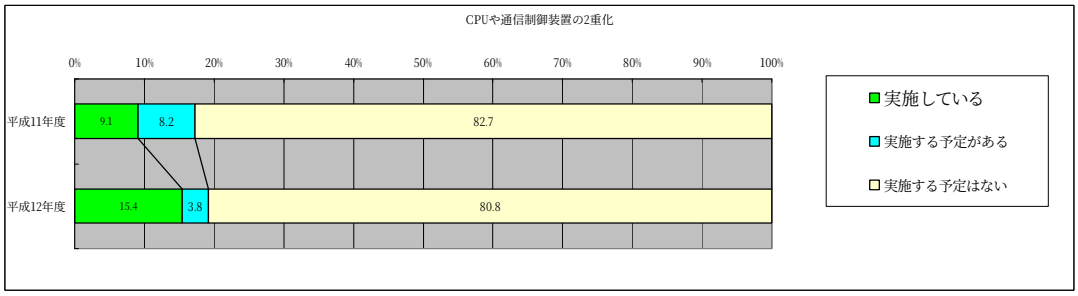
試みに前出の新聞記事件数と改竄されたホームページ数の相関関係を調べてみたが。2001年5月のSadmind/IISによる大規模なWeb書換えの事件以外は特に強い相関関係は見られなかった。

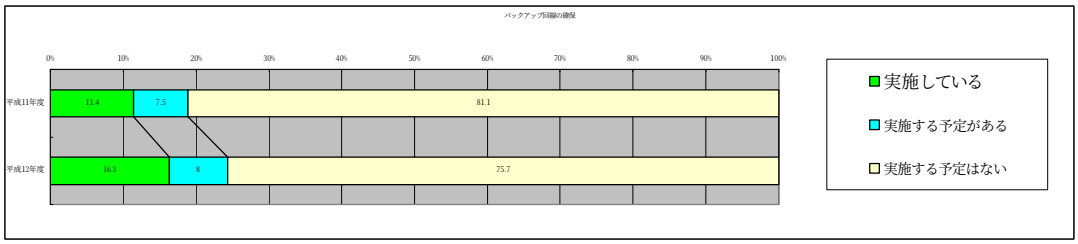


4.4.9. 関連する指標

4.4.9.1. 二重化されたネットワークの割合・数の推移

CPU,通信制御装置、バックアップ回線等の2重化の割合は高まっている。これはシステム全体の稼動において、可用性を高く保つ必要性が高まっているといえる。

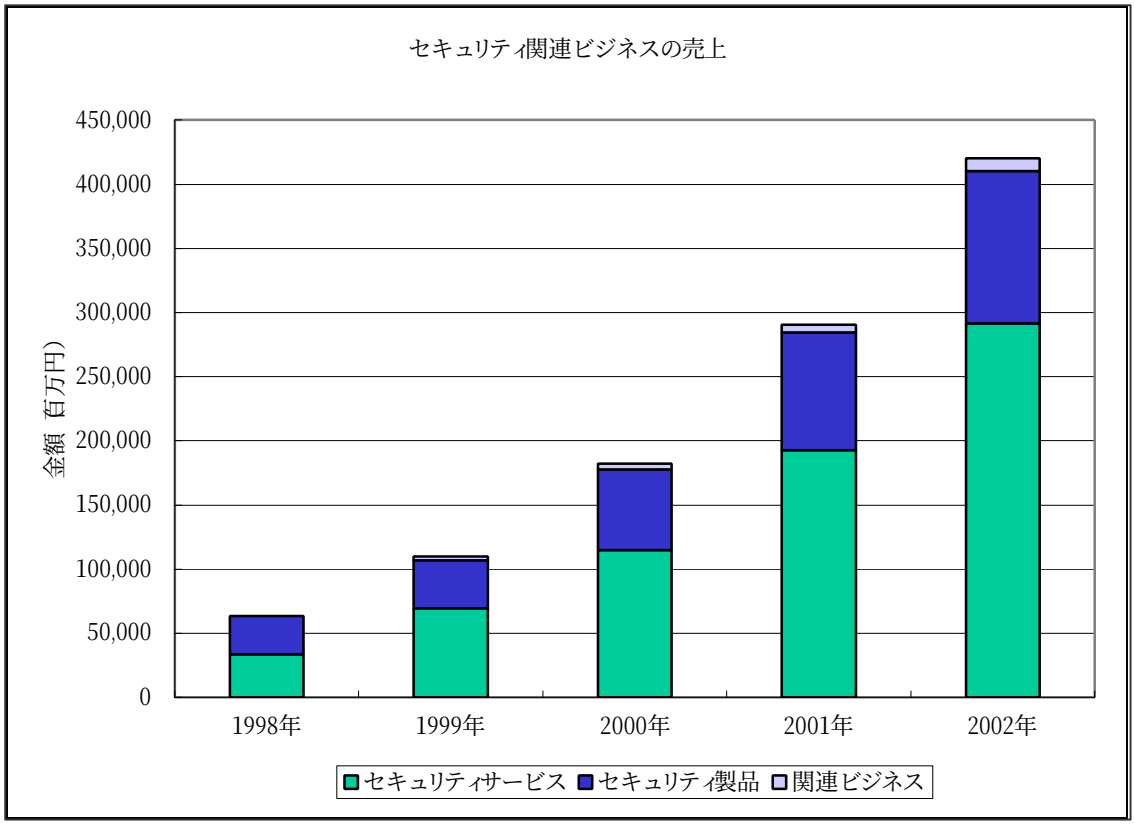




総務省「平成12年度、11年度通信利用の動向調査」（企業対象編）

4.4.9.2. セキュリティプロダクトの売上の推移

ネットワークセキュリティに関連する製品、セキュリティサービス[5]の売上額は1999年から2000年に160%以上の伸びを示し、それ以降も対前年度比140%以上の高い伸び率が予測されている。

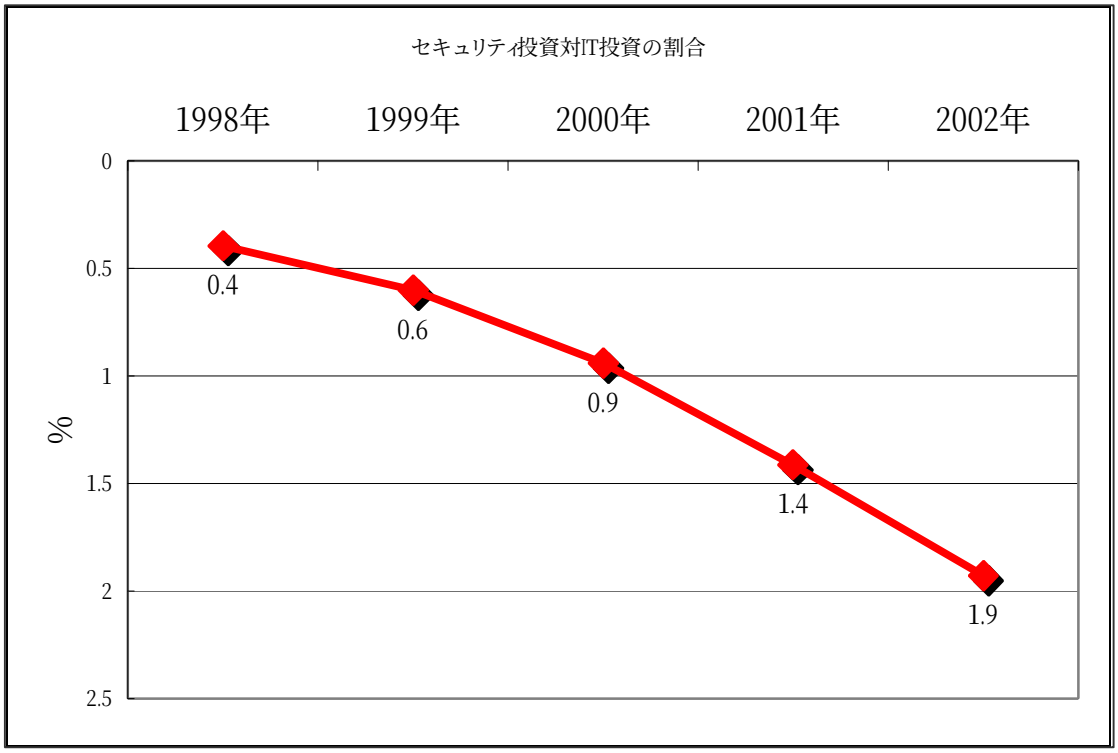


富士キメラ総研　ネットワークセキュリティビジネス調査総覧　2000年、2001年

[5] セキュリティサービスとはセキュリティ検査、不正アクセス監視サービス、セキュリティポリシ策定サービス等。 関連ビジネスには、保険サービス、セキュリティ技術者認定・教育等である。

4.4.9.3. セキュリティへの投資状況（IT投資に対する割合）

IT全体への投資が伸び悩む中でセキュリティ関連への投資は増加している。1998年の0.4%から2002年には1.9%と約5倍の増加である。セキュリティ関連への投資とは、すなわち守るべき資産の価値が高まっていることを表している。



IT投資額： 総務省 情報通信白書

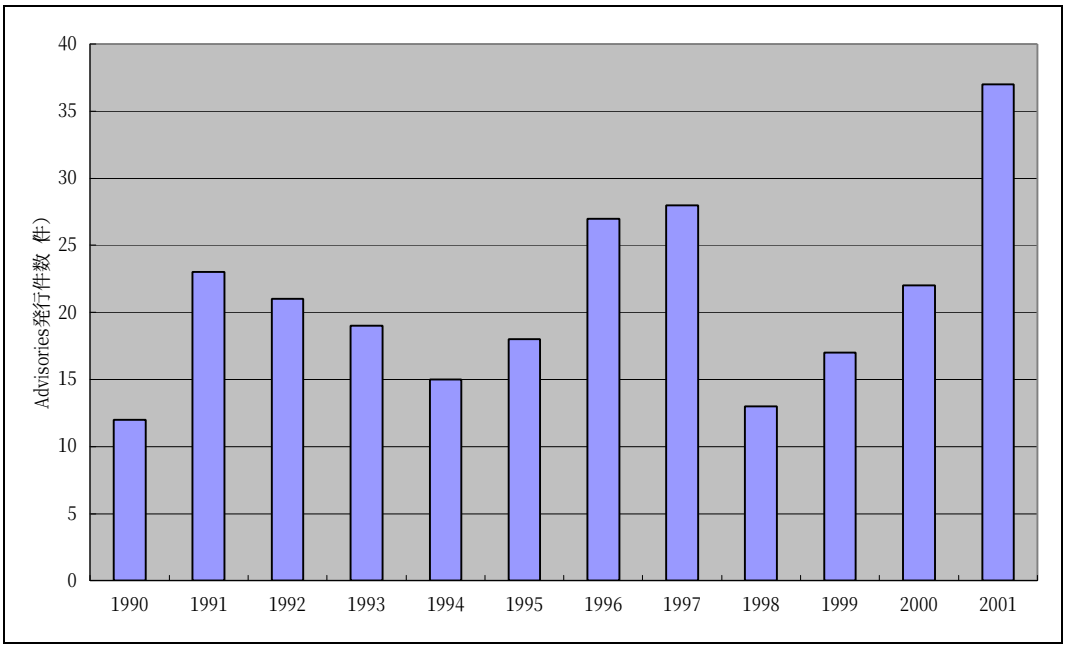
セキュリティ投資額：富士キメラ総研 ネットワークセキュリティビジネス調査総覧

より作成

4.5. 脆弱性情報の推移

4.5.1. CERT/CC-Advisory

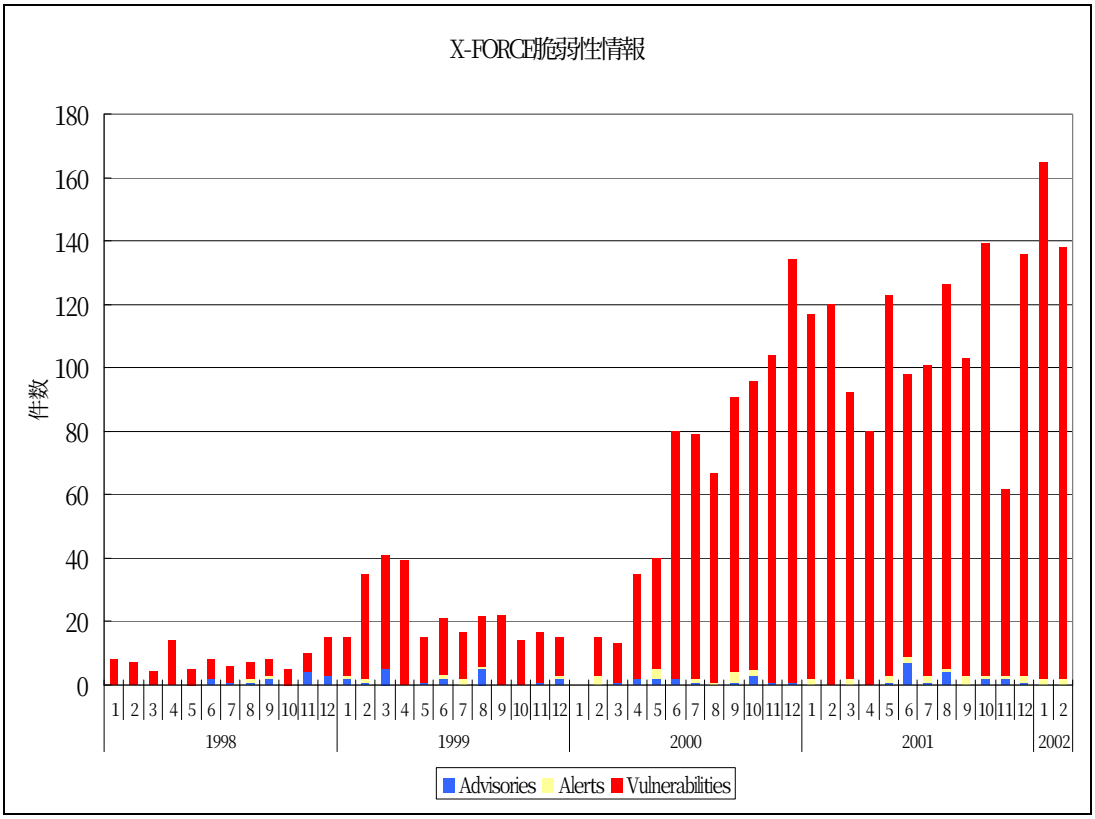
米国コンピュータ緊急対応センター（CERT/CC）より発行される脆弱性情報であるAdvisoryの発行件数である。1998年以降増加傾向であり、特に2001年は多くの脆弱性について注意が喚起された。



米国コンピュータ緊急対応センター（CERT/CC）資料より

4.5.2. X-FORCE

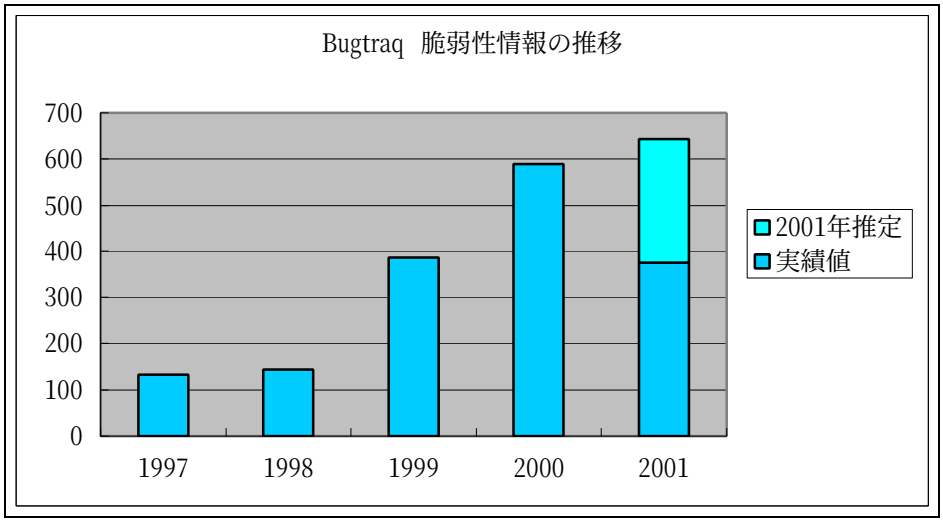
インターネットセキュリティシステムズ社（以下ISS社）の研究部門であるX-FORCEによる、脆弱性情報の通知件数を示す。月ごとの変動はあるものの、通年では発見される脆弱性は確実に増加している。



インターネットセキュリティシステムズ社　X-FORCEページより作成

4.5.3. Bugtraq

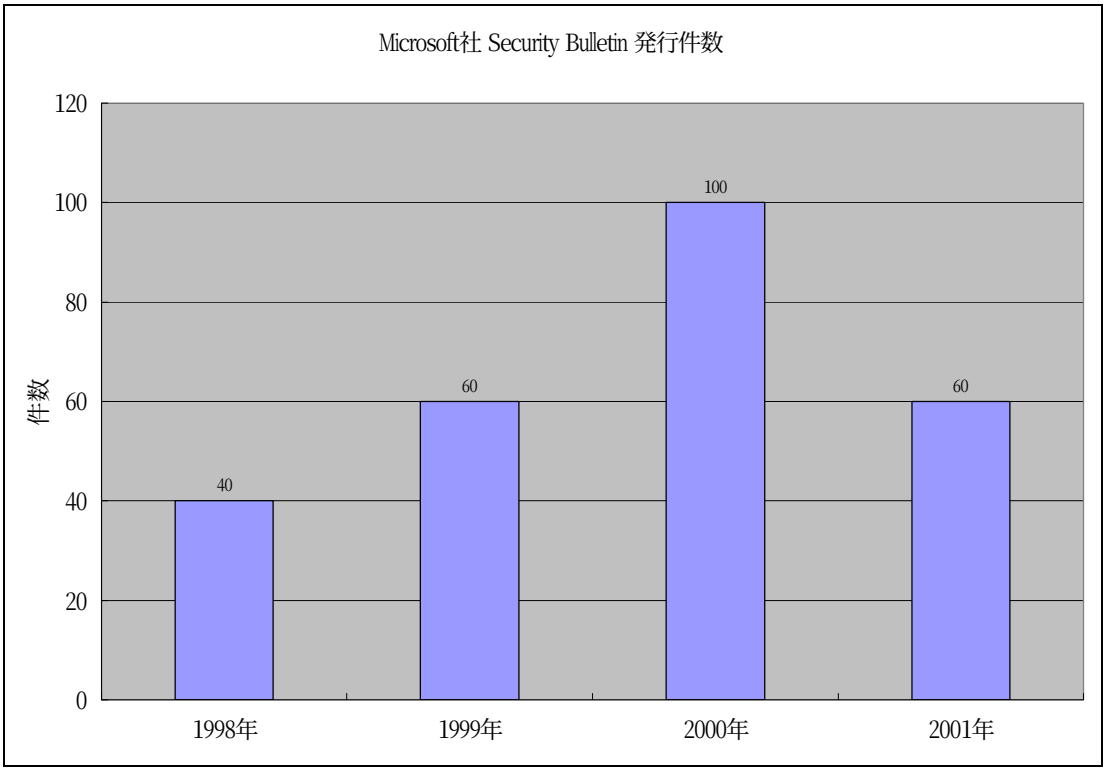
SecurityFocus社のBugtraq脆弱性情報の推移である。 2001年は7月末までの件数から7分の12とした。（2001年 8月以降は集計値が公開されていないため）。



SecurityFocus社統計資料より作成

4.5.4. Microsoft社　Security　Bulletin

Microsoft社の発行するWindows等自社製品についての脆弱性、修正パッチの情報であるSecurity Bulletinの1998年[6]から2001年までの発行件数をしめす。 2001年は前年よりすくないものの、おおむね増加の傾向にある、Microsoft社の製品はクライアント上では圧倒的な利用率であり、サーバにおいても、WindowsサーバやWebサーバ（IIS）等はインターネット上で多く利用されており、同社の製品の脆弱性は多くの利用者に影響があるといえる。



Microsoft社Securityページより

[6] 1998年は6月から12月まで20件の掲載があったため、通年で40件と仮定した。

5. Ⅱ関連の保険について

5.1. 損害保険の利用について

ネットワークの安全とセキュリティのリスクを補償するサービスが注目されている。コンピュータのハードウェアやメディアの破損に対する保険は従来より存在したが、1998年前後よりセキュリティ関連の保険に対する要望の高まりや、1998年1月の金融規制緩和などの動きを背景とし、不正アクセス、ネットワークの中断による利益損害や日常の業務を継続するための費用を補償する保険が次々と発売されている。リスク評価などを併せトータルな補償サービスを提供する会社も増えている。

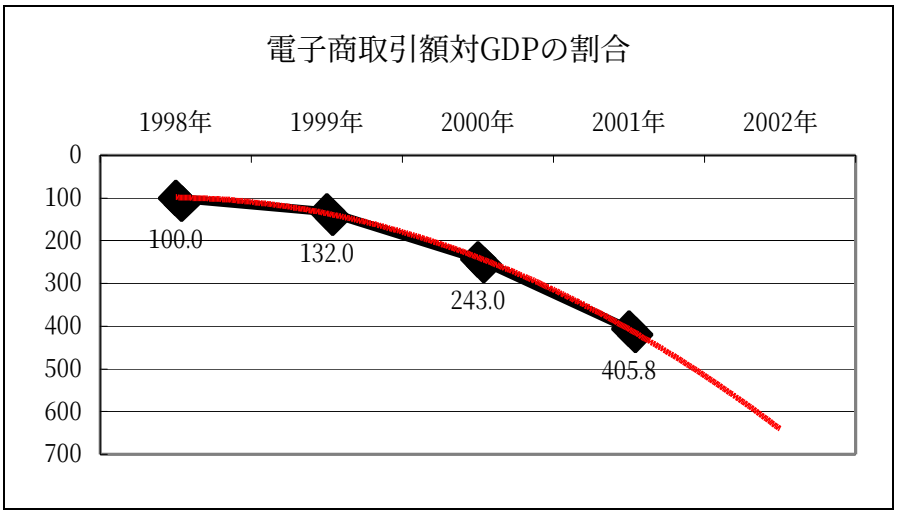
主な損害保険会社のセキュリティ関連保険

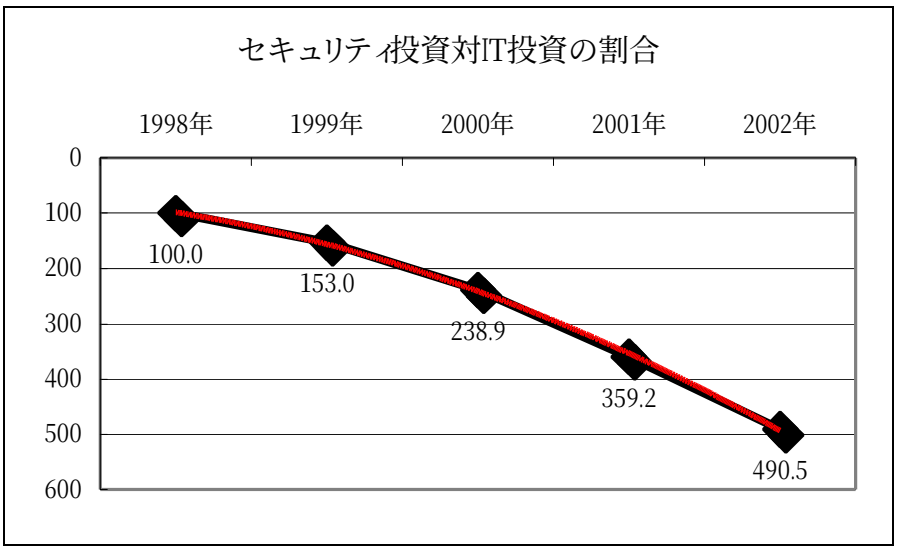
企業名	保険概要
A社	1998年1月より、不正アクセス、ウイルスや従業員の不正行為による被害後のセキュリティ際策費用、資金損害の補償など
B社	ネットワークシステムの物損害や運営不能の補償とウイルス、ハッカーによるデータ改竄など
C社	1998年6月より、情報機器への直接損害などと営業継続費用やネットワークを通じた業務上の損害補償など
D社	コンピュータ総合保険をベースにオールリスクで物損害、費用損害、利益損害を担保する特約を新設など

6. 調査結果の分析

6.1. IT許容リスクの減少

GDPに対する電子商取引の割合の増加、及びIT投資に対するセキュリティ投資の割合の増加を、1998年を100としてグラフ化した。 実際の値を黒線でプロットし、近似曲線を赤線でしめす。
両グラフから、インフラの重要度は増加し、リスクに対しての許容度は（2次関数的に）低下しているといえる。





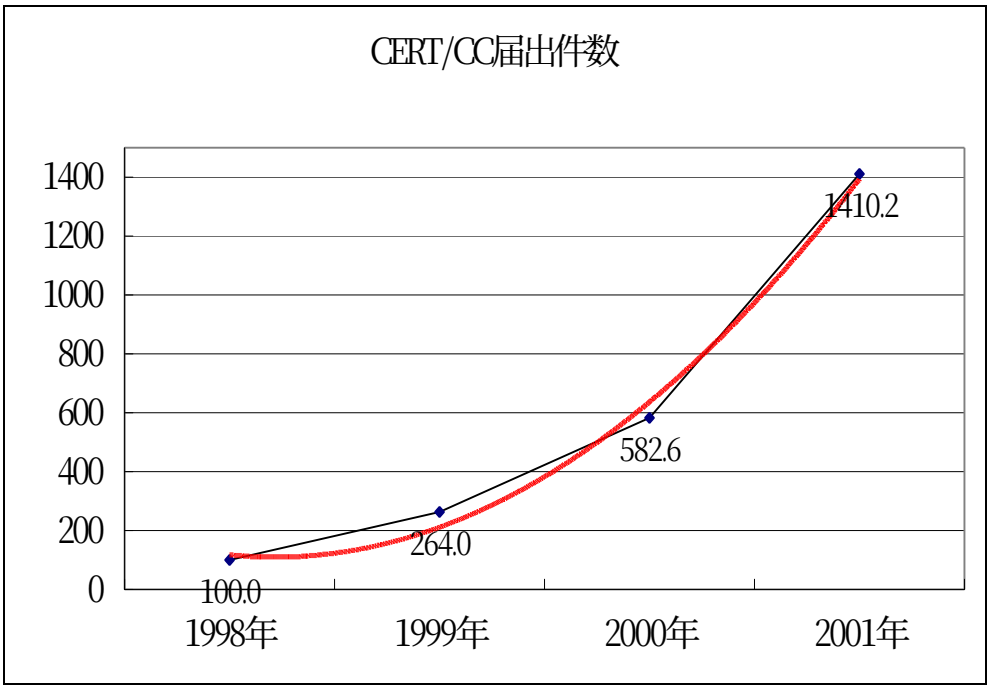
6.2. セキュリティ侵害行為被害遭遇確率の増加

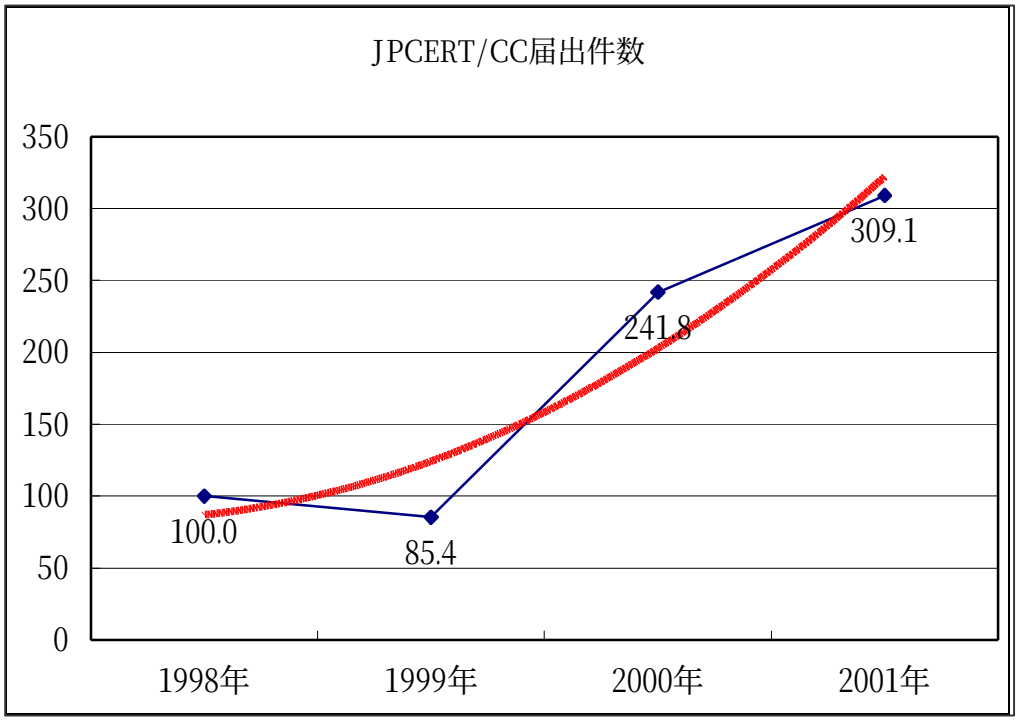
不正アクセスの被害遭遇確率を（脅威、脆弱性）とする。脅威に関するデータと、脆弱性に関するデータをそれぞれ個別に1998年を100として増加の割合をグラフ化した。

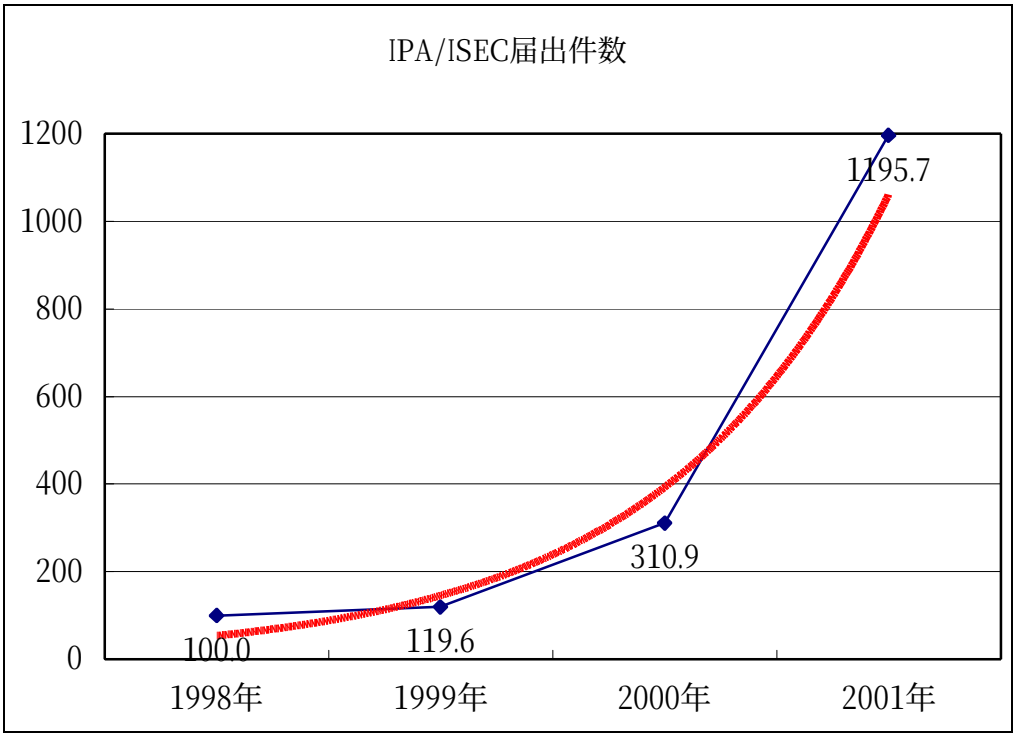
6.2.1. 脅威の増加

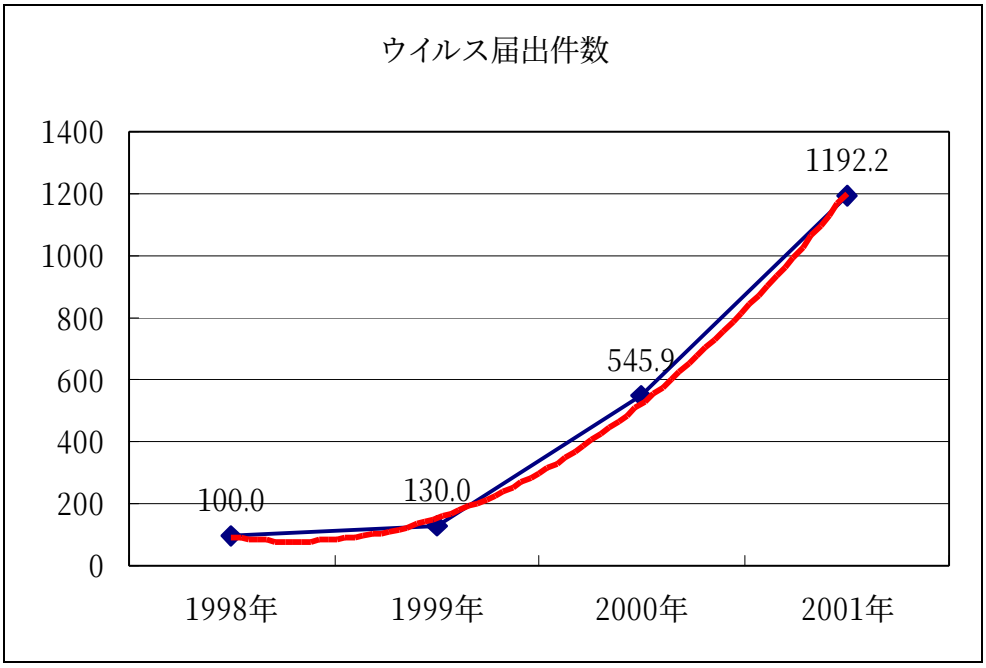
以下のデータについて、検討する。各グラフとも赤線は近似曲線をあらわす。この結果から、各データともに急激な増加傾向にあることがわかる。なお、公安委員会等による「不正アクセス行為の発生状況」については、2000年、2001年の2年度分のデータのみであるため、解析対象としていないが、今後は重要な参考値の一つであると考える。

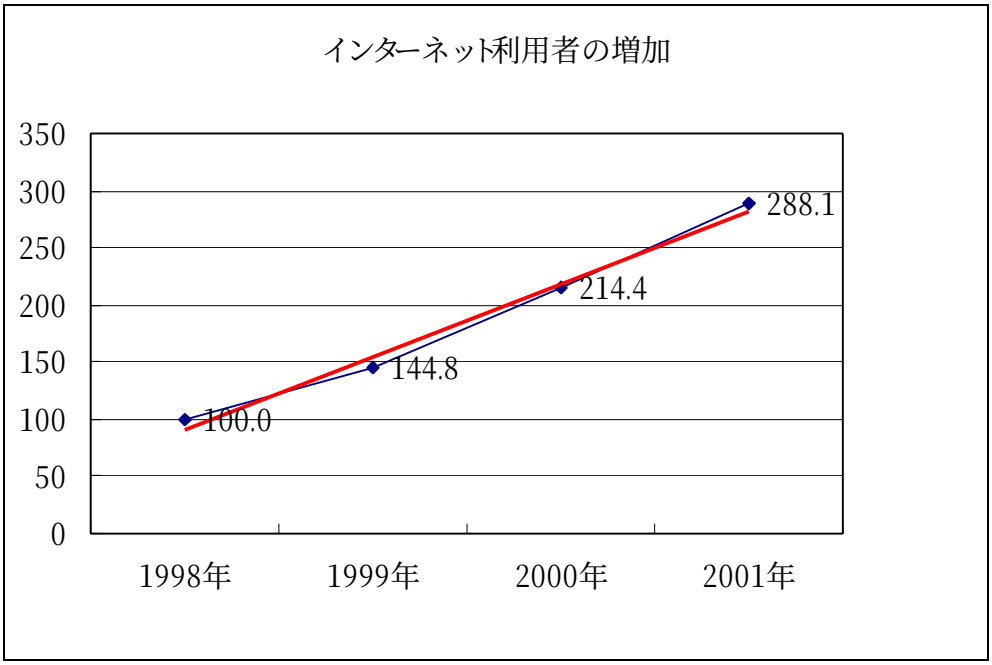
- CERT/CCへの不正アクセス届出件数
- JPCERT/CCへの不正アクセス届出件数
- IPA/ISECへの届出件数
- IPA/ISECのウイルス発見届出件数
- インターネット人口の増加




JPCERT/CC届出件数
350
300
250
200
150
100
50
0
100.0
85.4
241.8
309.1
1998年
1999年
2000年
2001年

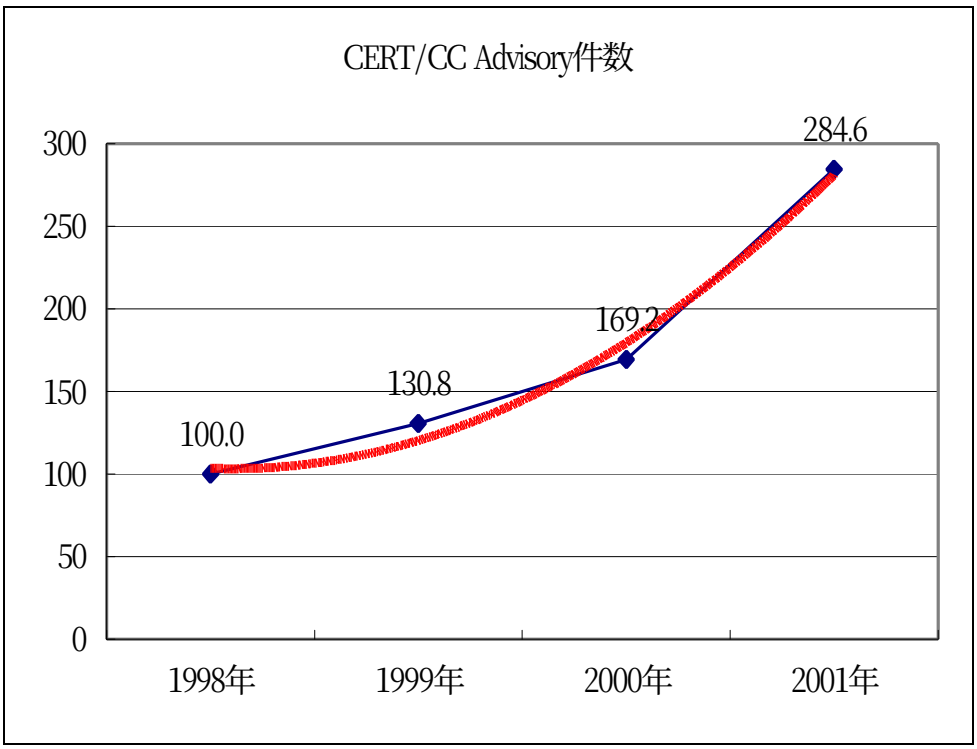

IPA/ISEC届出件数
1200
1000
800
600
400
200
0
100.0
119.6
310.9
1195.7
1998年
1999年
2000年
2001年

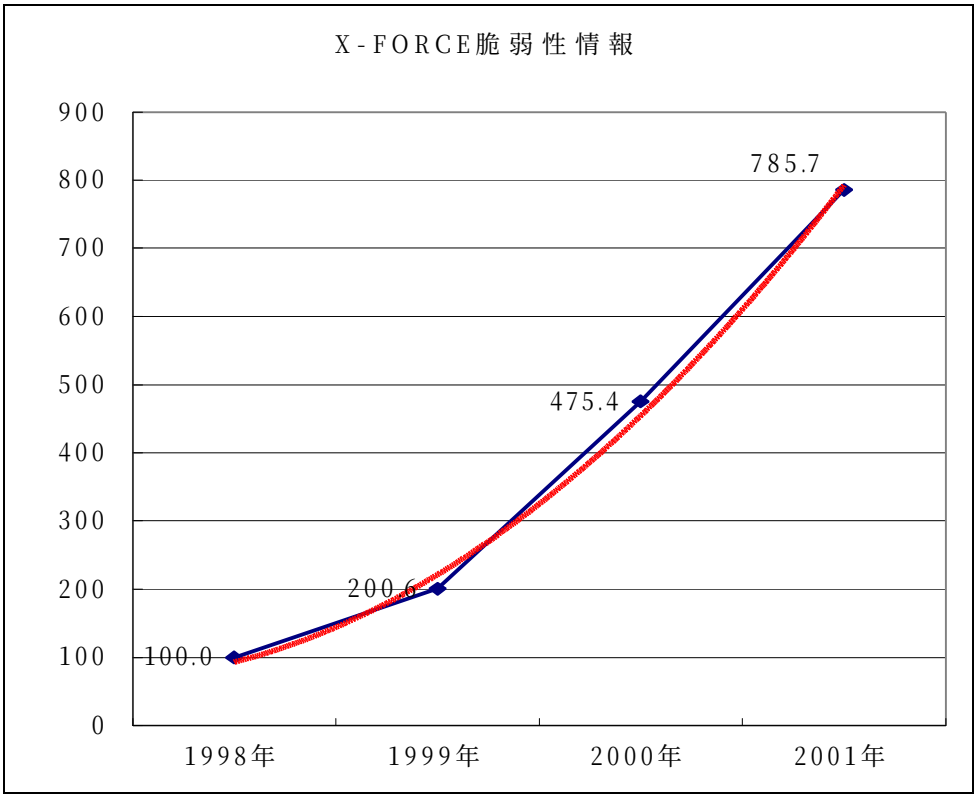

ウイルス届出件数
1400
1200
1000
800
600
400
200
0
100.0
130.0
545.9
1192.2
1998年
1999年
2000年
2001年


インターネット利用者の増加
350
300
250
200
150
100
50
0
100.0
144.8
214.4
288.1
1998年
1999年
2000年
2001年

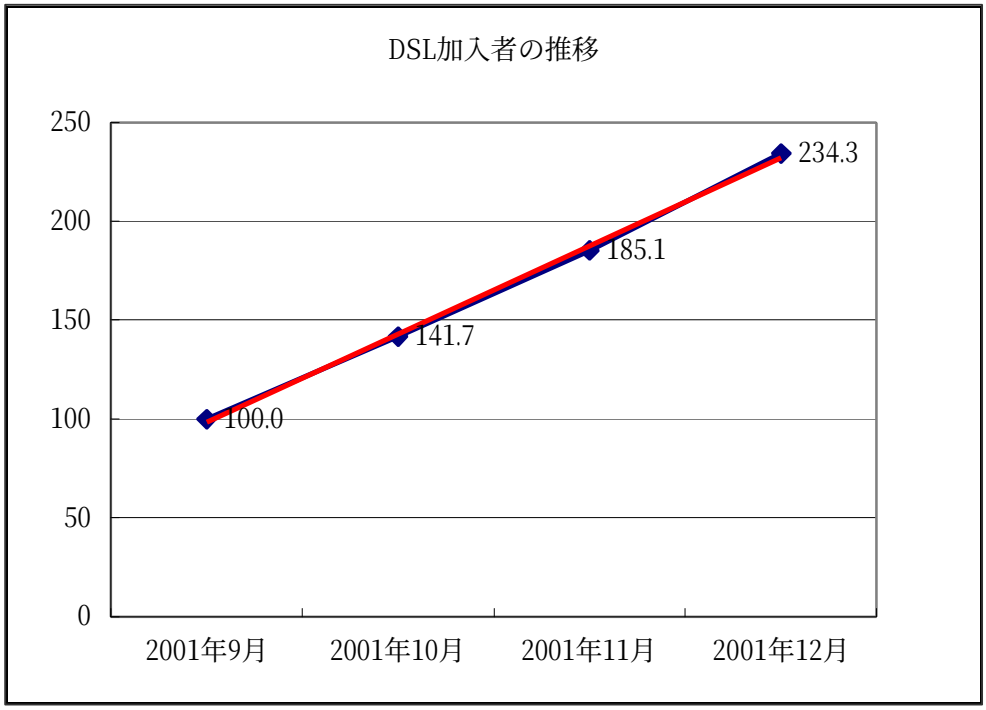
6.2.2. 脆弱性の増加

脆弱性の増加はCert/CCのAcvisory件数、及びISS社のX-Force脆弱性情報（Vulnerabilities、Advisories、Alertsの合計）件数について、さらに、Microsoft社のSecurity Bulletin発行件数を1998年を100としたグラフで示す。DSL加入者の増加については、2001年9月を100とし、12月まで4ヶ月を最近の傾向としてとらえグラフ化する。Security Bulletin以外はいずれも急激な増加傾向にあることがわかる。




X-FORCE脆弱性情報
900
800
700
600
500
400
300
200
100
0
100.0
200.6
475.4
785.7
1998年
1999年
2000年
2001年


Microsoft社Security Bulletinの推移
300
250
200
150
100
50
0
1998年
1999年
2000年
2001年


DSL加入者の推移
250
200
150
100
50
0
234.3
185.1
141.7
100.0
2001年9月
2001年10月
2001年11月
2001年12月

7. まとめ

調査結果の分析より、ITインフラのリスクに対する許容度及びセキュリティ侵害行為に遭遇する可能性について重み付けを行い、グラフを示す。 2つのグラフから、ITインフラのリスクに対する許容度は減少傾向にあり、セキュリティ侵害行為の遭遇確率は増加傾向にあることがわかる。
なお、各重み付けは経験から仮定したものであり、重みの割合についての正当性は今後の調査等により、修正の必要が生じる可能性がある。
リスクの許容度の減少については、電子商取引額対GDP比とセキュリティ投資対IT投資の割合について、4:6で加重平均を行うことによって表す。
セキュリティ侵害行為に遭遇する可能性については、脅威及び脆弱性について以下の表に掲げた項目の値を用いた加重平均から数値化し、さらに、得られた値を

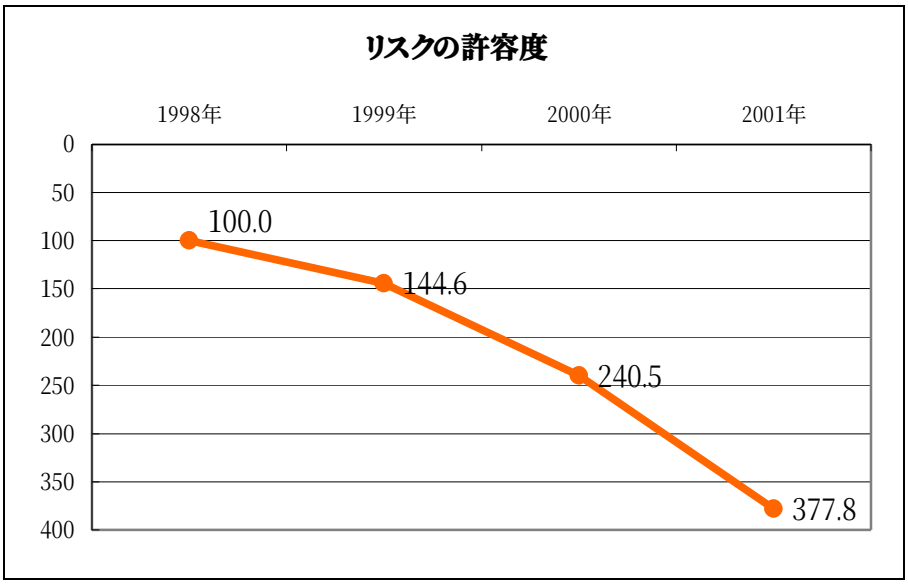
$$(\text{脅威})^{0.6} \times (\text{脆弱性})^{0.4}$$

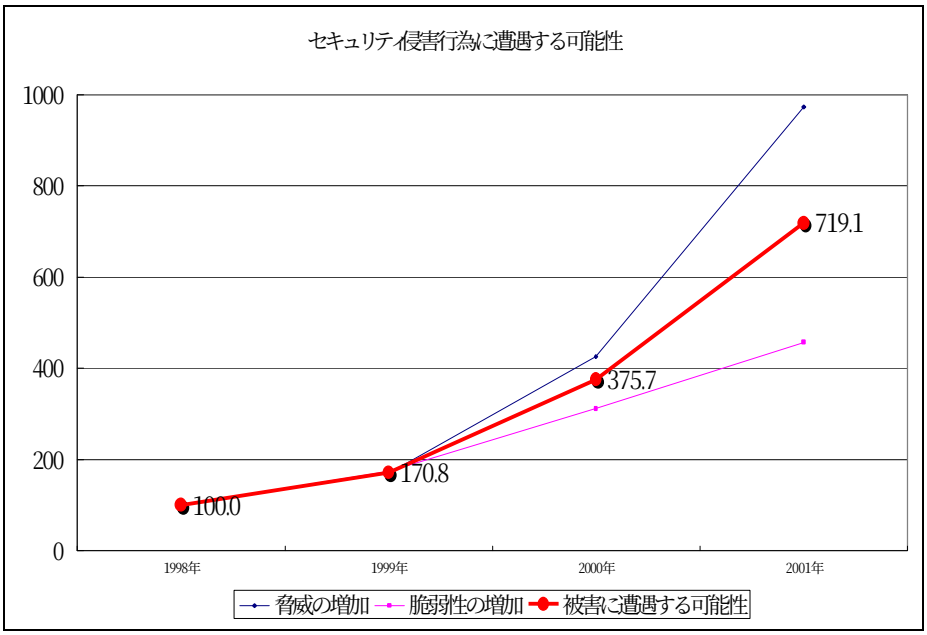
として試算する。脅威、脆弱性の加重の割合はそれぞれ下記とする。

脅威に関する項目	重み	備考
CERT/CCへの不正アクセス届出件数	38%	脅威は国境に無関係。また、全件数が多く特定報告者に左右されにくい。
JPCERT/CCへの不正アクセス届出件数	26%	国内の脅威をあらわす一面として重要。
IPA/ISECへのウイルス発見届	16%	複合化したウイルスの被害も依然として脅威である。
IPA/ISECへの不正アクセス届出件数	12%	件数の絶対値が少なく、個人からの届出が多いため不確定要素もある。
インターネット人口の増加	8%	インターネット人口増加は無視できない。
公安委員会等不正アクセス行為の発生状況		今後は指標として重要となると考えるが今回は計算から除外。

脆弱性に関する項目	重み	
CERT/CC Advisory件数	45%	重要な脆弱性の報告機関として信頼性がある。
ISS社X-FORCE脆弱性情報	35%	民間最大規模といわれるデータベースとして実績がある。
Microsoft社Security Bulletin	20%	多くのユーザが利用している。
DSL加入者の推移	10%	常時接続による脆弱性の増加は見逃せない。

以上、分析結果と仮定した値から、最終的に次の2つのグラフが作成できる。これは、ITインフラのリスクに対する許容度の低下とセキュリティ侵害行為に遭遇する可能性の増加を裏付けるものとなっている。





なお、本調査で仮定したパラメータなど仮説の検証をするためにも今後も継続的な調査が必要であろう。また、ユーザの意識の調査においてはアンケート方式が有効であると思われるが、これも継続的な実施により変化の推移を把握することが可能となる。