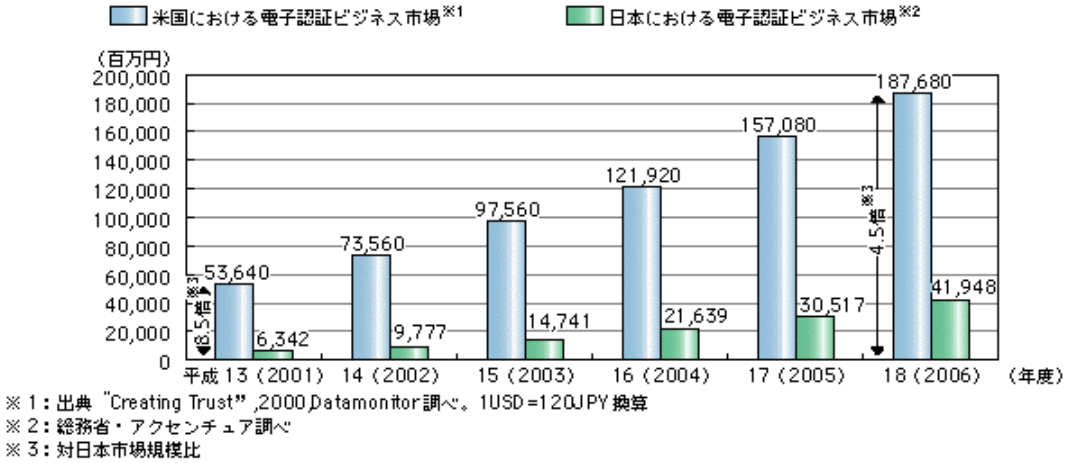
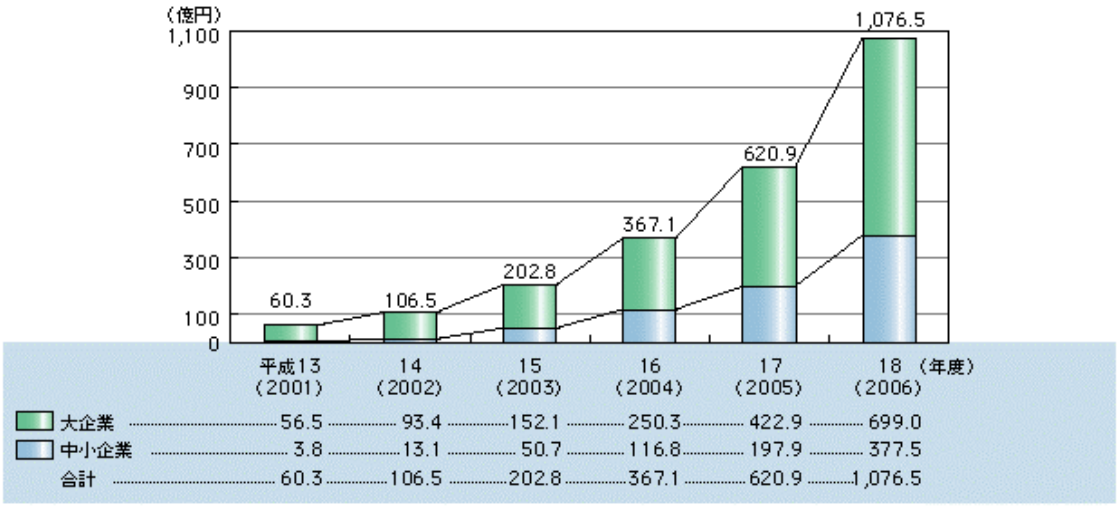


図 2.2-19 **米国の電子認証ビジネス市場規模予測との比較**

（注 1**）一方の鍵から他方の鍵を導き出すことの数学的な困難性に基づいて生成される、異なった鍵のペアにより暗号化と復号を行う方式。鍵のペアは、「公開鍵」（誰でも入手可能な一方の鍵）と、「秘密鍵」（所有者が厳重に管理するもう一方の鍵）で構成される。**

c) ASP **市場**

ASP（Application Service Provider）**は、ユーザ企業がパッケージソフトウェア等のアプリケーションを自ら所有することなく、**ASP **事業者からインターネットを介して提供されるアプリケーションを利用するサービスであり、主に企業におけるシステム運用・管理等のアウトソーシングの一環として利用されている。システムの導入・運用・更新への迅速な対応、設備投資・運用失敗等に係るリスク回避、ハッキング等に対するセキュリティ対策向上等の面で効果が高く、コストの削減にも寄与するものとして今後更に普及することが予想される。**2001 **年度における** ASP **市場(注)は** 60.3 **億円と推計され、**2006 **年度には** 1,076.5 **億円と、約** 18 **倍に増加すると予想されている（図** 2.2-20**）。利用者の内訳をみてみると、**2001 **年度は、大企業が** 56.5 **億円でシェアが** 9 **割以上、中小企業は** 3.8 **億円と** 1 **割にも満たない。**2004 **年度頃から中小企業においても市場が立ち上がり始め、**2006 **年度には、大企業が** 699.0 **億円でシェアが** 6 **割強、中小企業が** 377.5 **億円と** 3 **割強になると見込まれ、市場規模自体はいずれも順調に拡大するが、とりわけ中小企業のシェアが増加すると予想される。** ASP **を活用したアプリケーションの種類としては、現状ではグループウェアや** e **マーケットプレイス等が多いが、将来的には基幹業務や人事・総務等の多様な業務へ適用が広がることが期待される。**



（出典）「IT と企業行動に関する調査」

図 2.2-20 ASP **市場規模推計**

（注）ここでは、顧客ごとのカスタマイズを行わず、汎用アプリケーションのみを取り扱うものの市場を推計している。特定の顧客専用にカスタマイズされたアプリケーションを開発・提供するものなどは含んでいない。

d) **電子商取引市場**

インターネットの普及やブロードバンド化の進展に伴い、我が国では電子商取引の利用が拡大しており、既に 4 **分の** 1 **近くの企業が販売業務や調達業務のいずれか又は両方において電子商取引を利用している**(注 1) **（図** 2.2-21**）。電子商取引市場は、パソコン・家電製品等の最終消費財や有料ネットワークコンテンツ等のサービスの取引を行う「電子商取引(最終消費財)市場」と、企業間における原材料取引を行う「電子商取引（中間財）市場」に分類されるが、ここではそれぞれの市場について、市場規模の推移及び企業の具体的取り組みについてみることとする。**

まず、電子商取引（最終消費財）市場について市場規模(注 2)**をみると、**2001 **年は** 1 **兆** 2,218 **億円（対前年比** 96.0**%増）となっており、着実に拡大を続けている（図** 2.2-22**）。**

他方、電子商取引（中間財）市場について市場規模をみると、2001 年は 53.9 兆円（対前年比 41.5%増）となっており、電子商取引（最終消費財）市場同様、着実に拡大が進んでいる。

これまで、電子商取引（中間財）市場は、電機産業や自動車産業等、部品点数の多い組立・加工産業を中心に、主に大企業である部品調達企業の主導による普及が進められてきた。しかし、インターネットが広く普及するとともに、その利用方法は多様化しており、現在では、中小企業を含めた販売企業の主導による電子商取引（中間財）市場への参入例も現れている。

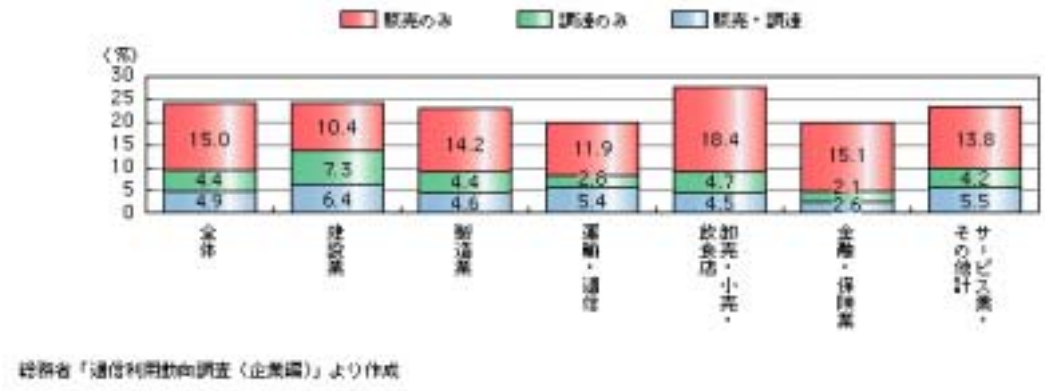


図 2.2-21 我が国企業における電子商取引の利用状況

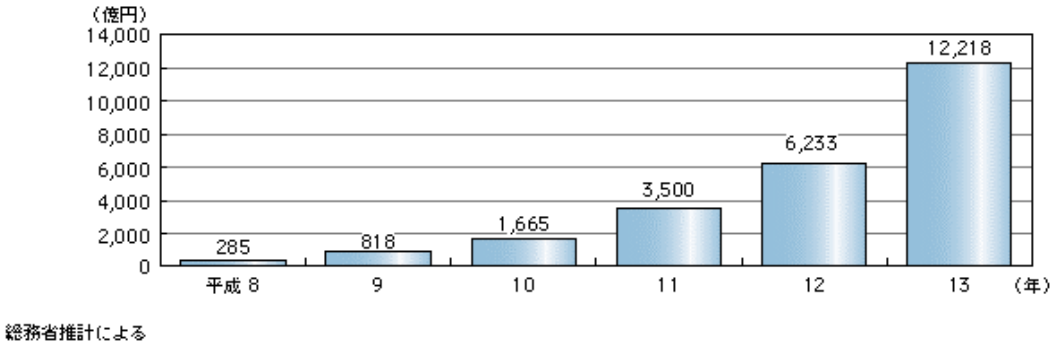


図 2.2-22 電子商取引(最終消費財)市場の推移

（注 1）総務省「通信利用動向調査（企業編）」におけるホームページを利用している企業の割合に、「デジタル様式でない商品の販売（受注を含む）」、「e マーケットプレイス（調達活動）の利用」、「デジタル様式の商品の販売（受注を含む）」の合計を乗じて算出している。

（注 2）市場規模の推計に当たっては、最終消費財市場、中間財市場ともに、電子商取引を「TCP／IP を用いたネットワーク上で財･サービスの受発注を行う商取引」と定義している。

e) 情報通信ベンチャー企業の起業環境

我が国においては、個人の消費や企業の設備投資の抑制、リストラの進行等による産業活力の低下が懸念されているところである。このような中、経済社会のダイナミズムの源泉であり、また経済成長はもとより雇用創出の原動力である起業に対する期待が高まっているが、中でも独自の技術やビジネスモデルを基礎とするいわゆるベンチャー企業については、経済の活性化に資するものとして高い期待が寄せられている。

ベンチャー企業の育成による経済的な効果を大きなものにするためには、より高い市場の成長が期待できる産業において、重点的な育成を図ることが効果的であると考えられる。

1995 年から 2000 年にかけての市場規模の推移を産業別にみると、情報通信産業は年平均成長率 7.5%と、全産業中で最も高い成長率となっており、近年における情報通信産業の市場の成長率が高いことが分かる。産業の活性化、経済の持続的な成長を実現するため、ベンチャー企業、とりわけ情報通信ベンチャー企業の育成が重要であることがうかがえる。

情報報通信産業はムーアの法則やギルダーの法則等にみられるように、一般に技術の進展の速い産業であるといえる。そのため、情報通信ベンチャー企業には技術の進展に対応した経営スピードや事業環境の変化に対応していくことが必要となると考えられる。

情報通信ベンチャー企業は非情報通信ベンチャー企業に比べて、早期に黒字化を見込んだ事業計画を立てている割合が高く、情報通信ベンチャー企業の 79.5%が設立後 3 年以内での黒字化を予定している。また、実際 58.1%の企業が設立後 3 年以内までに単年度黒字（初年度から黒字、設立後 3 年以内で単年度黒字の合計）となっており、事業計画に基づく早期の黒字化が図られている（図 2.2-23、図 2.2-24）。

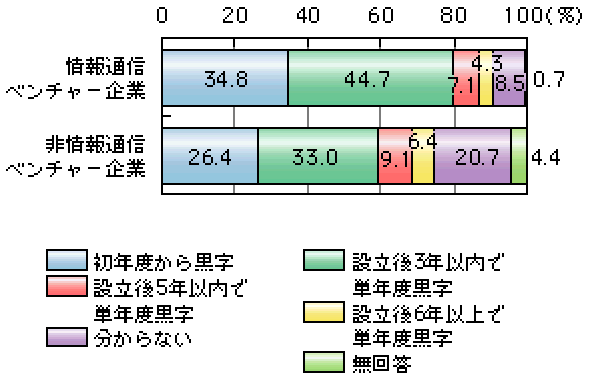
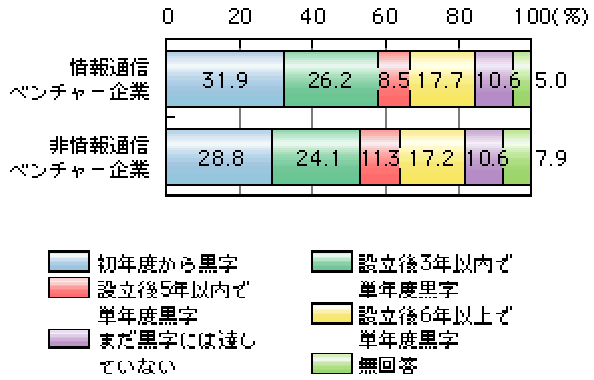


図 2.2-23 **創業時の事業計画**



図表①~④ （出典）「IT と企業行動に関する調査」

図 2.2-24 **創業後の事業経営状況**

(4) **電子政府・自治体の進展**

政府及び地方公共団体では、効率・簡素・透明・便利な行政の実現を図るため、自宅や職場にいながら行政に関する情報の入手、住所・戸籍や税の申告・納付といった手続等をインターネットで行うことができる電子政府・電子自治体の構築へ向けた取り組みを推進している。

国の行政機関における申請・届出等手続のオンライン化数が、2001 **年度末に** 590 **件（実施率** 5.3%**）に達するなど、国民・企業と国との間のオンライン化は着実に進展している。また、国の行政機関内部の情報化についても、パソコン一台当たりの職員数が** 1.2 **人、約** 8 **割のパソコンがネットワークに接続されるなど、整備が進む。他方、地方公共団体においても、**80%**以上の団体がホームページを開設しているほか、パソコンや庁内** LAN **の整備等が進展している。さらに、政府では、地方公共団体における申請・届出等手続のオンライン化のための環境整備として、各省庁においてアクションプランを策定している。**

電子自治体の実現による効果として、住民・企業は、「手続事務対応の迅速化」、「行政サービスの利便性向上」、「行政サービスコストの削減」を期待している。地方公共団体においては、電子化に当たって「情報公開の推進」、「情報共有の推進」等の取り組みを実施している。電子自治体の推進は、地方公共団体の職員の業務遂行に当たって、仕事の質の向上やスピードアップに一定の効果があがることを期待している。

2.3 インターネット上の脅威

この節においてはまずインターネット上にどのような脅威が存在するかを分類する。脅威にはインターネットを利用する個人に作用するものと政府・企業などに作用するものとがある。個人の経済活動を始めとする様々な活動に深刻な影響を与える点で個人に対する脅威も重大だが、政府・企業などの大規模なネットワークに作用するものはとくに大規模かつ広範な被害を及ぼしうる。そこで、この節においてはこのような広範な被害を実際にもたらした “サイバーインシデント” の例をとりあげて分析するとともに、現在のところは幸いまだ発生していないものの、今後の備えのために、それが “テロ” と呼ぶべきレベルに達した場合も想定して論じる。

2.3.1 脅威の種類

人為的に作り出される脅威の種類には、(1) **外部からの侵入行為（不正アクセス）と、**(2) **サイバー攻撃（サービス妨害）とがある。**

(1) 外部からの侵入行為 （不正アクセス）

a) 盗聴

盗聴は、ネットワーク上を流れるデータを第三者が不正に入手することである。例えば、メール以外やパスワードなどが盗聴の対象となる。今後は、 IP 電話やIP電話会議システムが普及することにより、音声が盗聴される危険も増加すると考えられる。

b) 個人情報流出

個人情報流出とは、コンピュータ内に保管された個人情報データが不正に読み出されたり送り出されたりすることである。

なお、個人情報流出は、外部からの不正アクセスによるものだけではなく、個人情報を管理する企業におけるメールの誤操作やWWWの設定ミスなどによって流出する場合も少なくない。企業において顧客の個人情報が外部に流出した場合、人権侵害を引き起こすとともに、企業の信用も大きく傷つけられることになる。

c) データの改竄・消去

改竄とは、コンピュータ内に保存されたデータが不正に書き換えることであり、消去はコンピュータ内の情報を失わせることをいう。コンピュータの設定データが書き換えられた場合や、銀行オンラインのコンピュータなどが含むデータが改竄されると大きな金額の被害をもたらす危険性がある。また広範囲に目に見える影響をあたえているのは WWW ページの書き換えである。2000 年には科学技術庁、総務庁・同庁統計局、運輸省、通産省のホームページが改竄され、2001 年に 70 以上の日本企業のホームページが次々に改竄される事件も発生している。

d) 踏台

踏台とは、目的のコンピュータに直接侵入することが困難な場合に、不正アクセスを媒介させるために不正に使用するコンピュータのことをいう。不正アクセスのためには、まず踏台となるコンピュータに侵入し、そこに送りこんだプログラムによって目的のコンピュータに侵入する。踏台にはセキュリティが弱いコンピュータが選択される。踏台の例としては企業内部のネットワークに侵入するためにその企業の従業員の家のコンピュータが使用されるケースがあげられる。

e) **裏口（バックドア）プログラム**

裏口プログラムとは、プログラムの中に作成者または配布者だけが知っている秘密のアクセス方法が用意されているものをいう。例えば、そのプログラムの配布者がユーザに気づかれることなくそのコンピュータにアクセスし、管理権限を奪い取ることを可能にする SubSeven **という裏口プログラムが** 2001 **年に公開されている。**

f) **トロイの木馬**

トロイの木馬とは、プログラムの内部にデータ破壊などを行う機能をもっているものをいう。トロイの木馬も一見無害なプログラムを装っている点で裏口プログラムと同様だが、そのプログラムがデータ破壊などの機能をもっている点が異なっている。有用な機能と破壊的な機能とが一体化されたプログラムに存在する場合もあるが、ウィルスやワームなどを内蔵した「運び屋」あるいは 「投下プログラム (droppers) **」とよばれるものもある。**

g) **時限爆弾・論理爆弾**

コンピュータにインストールされた時点では発症しないが、一定の時間がたったり、ある事象が発生したりしたときに発症するプログラムをそれぞれ時限爆弾、または論理爆弾という。

h) **なりすまし**

なりすましとは、ネットワーク上において特定の他人になりすますことである。他人のメールアドレスや名前を詐称したり、他人の IP **アドレスを使用しているように見せかけたり、他人のクレジットカード番号を使用したりすることがこれにあたる。**

(2) **サイバー攻撃 （サービス妨害）**

サイバー攻撃とは、ネットワークを介してコンピュータやネットワークそのものを操作したり大量のデータを送りつけたりすることによって、それらの機能を一時的または永久的に失わせる事象のことである。サイバー攻撃は必ずしも政府や企業のコンピュータシステムやネットワークのみが対象ではなく、個人のパソコンも対象となる。

a) DoS **攻撃** (Denial of Service **攻撃、サービス不能化攻撃**)

インターネットなどに接続されたサーバに大量のデータを送って過大な負荷をかけ、サーバの処理能力を著しく低下させたり、機能停止に追いこむことを DoS **攻撃という。**

DoS 攻撃の手法としては、「ping」 という、コンピュータの応答を調査するためのコマンドを多量に実行させる方法や、膨大な量のメールを送りつける 「メール爆弾」 などの方法がある。

b) DDoS 攻撃 (分散 DoS 攻撃、Distributed Denial of Service 攻撃)

DDoS 攻撃は DoS 攻撃の一種である。DoS 攻撃においてサーバが機能停止するほど大量のデータを 1 台のコンピュータからサーバに送りこむのは困難であり異常が検出されて防御されやすい。そこで、多数のコンピュータから同時にサーバにデータを送りこむ DoS攻撃がDDoS 攻撃である。

DDoS 攻撃に使用されるコンピュータは踏台であり、インターネット上であらかじめ多数の踏台を用意するのはそれほど難しいことではない。したがって、大規模な DDoS 攻撃が比較的容易に実現できるのが現状である。安価で少人数で実行が可能であり、技術的にも特別難しくはないため、サイバーテロの手段としても使われる可能性が高く、大きな脅威となっている。

c) セキュリティ・ホール攻撃

コンピュータシステムへの侵入やコンピュータ内のデータの不正な操作につながる可能性がある弱点（セキュリティ・ホール）を利用したサイバー攻撃のことがセキュリティ・ホール攻撃である。

セキュリティ・ホール攻撃の攻撃対象は不特定多数の個人のパソコンの場合もあり、不特定または特定のサーバの場合もある。個人のパソコンが対象になるときにはウェブブラウザやメールソフトのセキュリティ・ホールが狙われることが多い。また、サーバが対象になるときは、オペレーティング・システムのセキュリティ・ホールが狙われることが多い。よく狙われるセキュリティ・ホールの例としては「バッファ・オーバフロー」がある。これは、一時的にデータを格納するための 「バッファ」 にその容量以上のデータが送られた結果、プログラムが停止したり誤動作したりするというセキュリティ・ホールである。

セキュリティ・ホール攻撃では、このようなセキュリティ・ホールを利用して管理者権限を取得し、不正侵入を行う場合もある。上述のDDoS 攻撃の一手段としてもセキュリティ・ホール攻撃が使用される。セキュリティ・ホール攻撃の手法やそれへの対策・課題については 3.2 節において記述する。

d) コンピュータ・ウィルス

コンピュータ・ウィルスとは、コンピュータに入りこんでコンピュータ中のファイル

やプログラムに寄生してそれらを改竄したり消去したりするプログラムのことをいう。本来は生物としてのウィルスと同様にコンピュータ内のプログラムに寄生して爆発的に増殖するものをいうが、寄生性のないもの (ワーム、バクテリア) や増殖性がないまたは弱いものも含めた総称としても使用されている。ウィルスへの感染は、エンドユーザのパソコンにはおもにメールの添付文書に寄生したウィルスによって起こり、WWW サーバなどへはサーバ間で交換するデータのなかにウィルスがまぎれることによって起こる。

e) スパム

スパム (SPAM) とは、不特定多数のネットワーク利用者に対して無差別的に電子メールを送ったり、多数のニュースグループに無差別的にメッセージを投稿したりすることをいう。このようにして送られたメッセージはスパム・メール、スパム・メッセージなどと呼ばれる。

2.3.2 サイバーインシデントの増加傾向

(1) サイバーインシデントとは

JPCERT/CC は、「インシデント報告のガイドライン」において、サイバーインシデントを、「情報システムの運用におけるセキュリティ上の問題として捉えられる事象」と定義している。具体的には、

- システムのアクセス権限に対する影響（サーバープログラムの権限や管理者権限の盗用、一般ユーザ権限の盗用、サービスの盗用又は悪用、アクセス拒否の記録）
- システムの可用性やサイト業務に対する影響（許容できる又は許容できない遅延又は停止）
- 外部への影響（外部からのインシデントレポートの受領、外部への予期しないアクセスの検出）

などが挙げられる。実際には影響が発生していない事象であっても、何らかの影響を受けた疑いがある、もしくは放置しておくとセキュリティ上の影響が生じるおそれがある場合であれば、コンピュータセキュリティインシデントと捉えられる。

(2) サイバーインシデントの推移

a) ウィルス

1997 年～2002 年のウィルス届出件数の推移を図 1 に示す。届出件数の中には、アンチウィルスソフト等によって事前にウィルスを検出し、感染を未然に防いだ事例も含まれる。2000 年にメール感染型、2001 年にセキュリティ・ホール悪用型のウィルスが出現し

たことから、これらの期間に届出件数が急激に増加している。ただし、アンチウィルスソフトの導入が進んだことにより、実際に被害にあった割合は低下している。

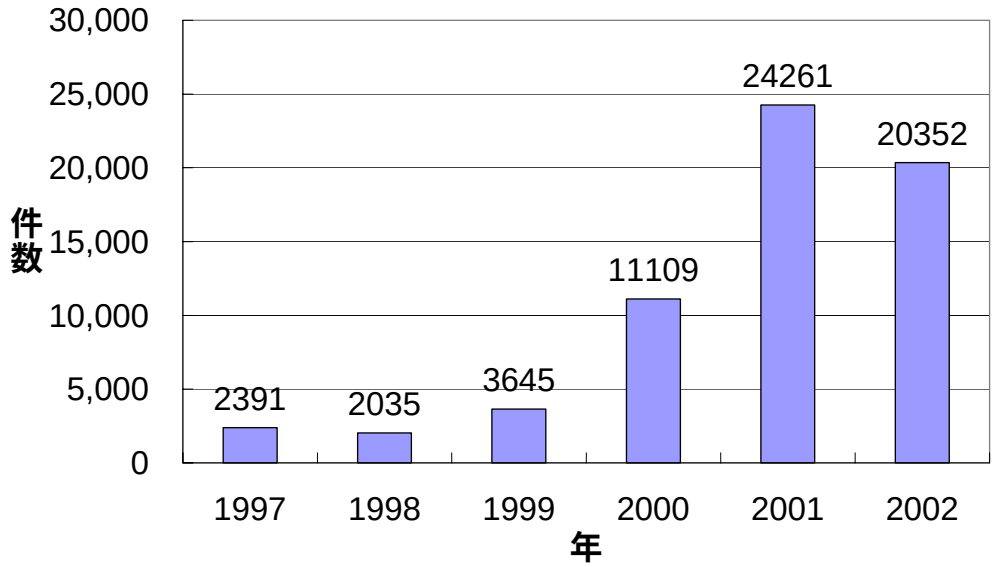


図 1: ウィルスの届出件数の推移 (出典: IPA/ISEC「2002 年ウィルス発見届出状況」)

b) 不正アクセス

1997 年～2002 年の不正アクセス届出件数の推移を図 2 に示す。2001 年以降、個人ユーザの常時接続環境の普及やワームの出現により、届出件数が急激に増加している。2001 年はワーム感染・形跡が多数を占めていたが、2002 年にはアクセス形跡(未遂)や DoS 攻撃が増加している。また、不正アクセスの届出者は、2001 年が一般法人 43%、教育・研究機関 27%、個人 30%に対し、2002 年は一般法人 24%、教育・研究機関 9%、個人 67%と大きく変化しており、ブロードバンド・常時接続環境の普及により、個人ユーザが不正アクセスを受ける危険性が高くなっていることがわかる。

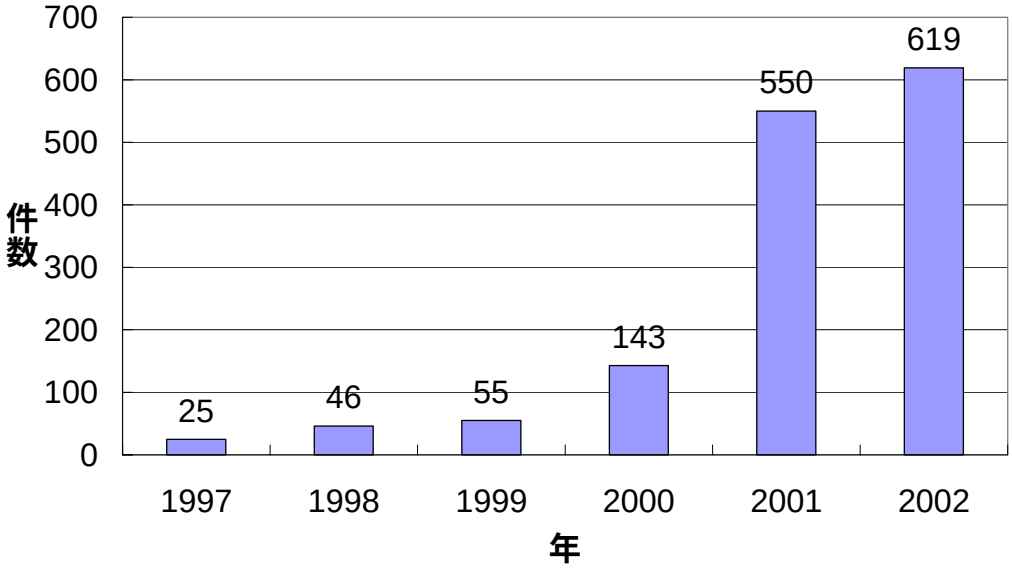


図 2: 不正アクセスの届出件数の推移

(**出典**: IPA/ISEC**「コンピュータ不正アクセスの届出状況について」**)

(3) **過去に起こった主なサイバーインシデント**

a) Code Red

Code Red **は、マイクロソフト社製の** Web **サーバである** IIS (Internet Information Service) **の脆弱性を悪用し、**TCP/80 **ポートを用いてリモートのサーバに自身のコードを送り込み、そこで実行させることで繁殖するワームである。**2001 **年** 7 **月に発見され、全世界の** IIS **を利用した** Web **サーバをターゲットとして急速に繁殖した。また、**2001 **年** 8 **月には、その亜種であり、より強力な感染力を持つ** Code Red II **も発見されている。**

Code Red **は、具体的には、**Web **サービス** (TCP/80) **に対して特殊な** URL **を指定した** HTTP **の** GET **要求を発行する。**IIS **がこの要求を受け付けると、**Microsoft Index Service **の全文検索エンジンに利用される** ISAPI **エクステンションのセキュリティホールによってバッファ・オーバフローを引き起こし、 その** URL **に埋め込まれたプログラム** (Code Red **ワーム**) **を実行する。**

Code Red **に感染したサーバでは、メモリ上の** Web **サーバープログラムが、全ての** HTTP **要求に対して決まったメッセージを返すように書き換えられる場合がある。これにより、全ての** Web **ページが改竄されたように見える。さらに、感染したサーバは、日付によって以下のような動作を行う。**

- **毎月** 1～19 **日: 次のターゲットをランダムに生成した** IP **アドレスで決定し、同じく特殊な** URL **による** Web **サービス要求を発行して繁殖を試みる。**

- **毎月** 20〜27 **日**: **ホワイトハウスの** IP **アドレス宛に** DDoS **攻撃を行う。(ただしホワイトハウスは実際に攻撃が開始される以前にアドレスを変更しており被害はなかった**)
- **毎月** 27 **日〜月末**: **活動を休止する。**

Code Red II **は、**Code Red **と同様にして** IIS **が動作する** Web **サーバに感染し、他のサーバへの攻撃を行う。さらに、不正侵入のためのバックドアを仕掛ける。**Code Red II **に感染したサーバは、**24〜48 **時間にわたりワームの繁殖活動を続けた後、バックドアを残してリブートする。**

Code Red **は、**IIS **だけでなく、一部のルータなど、**HTTP **を受け付けるネットワーク機器にも与える。具体的には、上述の不正な** HTTP **要求によってバッファオーバランが発生し、ルータ等がハングアップしたり、再起動を繰り返したりする。これにより、通信が不安定もしくは不可能な状態に陥る。**

さらに、2 **次的な被害として、感染先を求めて無差別に** HTTP **要求を出すため、トラフィックが増大し、ネットワークがダウンするという事態も引き起こす。**

CodeRed **が悪用しているセキュリティホールは、被害が拡大する** 1 **ヶ月前に修正プログラムが公開されていたが、適用しているコンピュータが少ない、もしくは、回避策をとっていなかったことが被害を拡大する原因となった。**

b) Nimda

Nimda **は** 2001 **年** 9 **月に出現したワームで、マイクロソフト社製の** Web **ブラウザ、メールクライアント、**Web **サーバのセキュリティホールを突いたものである。感染経路が一つではなく複数の経路を有し、**Web **サーバとクライアントの両方に感染するのが、従来にない大きな特徴である。**

Nimda **の第** 1 **の感染経路は** Web **である。**Nimda **は、セキュリティパッチが適用されていない** IIS **サーバを探し、そこに不正な** Java **スクリプトを埋め込み、さらに自分自身も埋め込もうとする。この感染した** Web **サーバにアクセスすると、ワームのファイルをダウンロードするようにメッセージが表示され、ファイルをダウンロードするとローカル** PC **にも感染する。マイクロソフトの** Web **ブラウザである** Internet Explorer **で、セキュリティパッチが適用されていない場合には、このファイルダウンロードが自動的に実行される。**

第 2 **の感染経路は、**PC **の共有ドライブである。ローカル** PC **に感染すると、**PC **の全ドライブ（**A〜Z **のドライブ）に自分自身をコピーする。また、ローカル** PC **に** HTML **ファイルがあると、そこに悪意のある** Java **スクリプトを埋め込む。こうした活動は、ネットワークの共有ドライブに対しても行われるため、他のクライアント** PC **も感染することになる。**

第 3 **の感染経路は、電子メールの添付ファイルである。ワームが添付されたメールを、**

セキュリティパッチが適用されていない環境で、マイクロソフトのメールクライアントである Outlook Express か Outlook によって受信すると、添付ファイルを読むかプレビューするだけで、添付されたワームが実行されて感染してしまう。感染した PC は、不特定多数の宛先に対し、ワームを添付したメールを自動的に送信してしまう。

また、Code Red と同様に、感染の過程で、ネットワークのトラフィックが増大し、ネットワークがダウンする被害も生じる。

Nimda は Web ページと電子メールの両方によって感染することから、被害が急速に拡大し、Web やメールのサービス停止に追い込まれる例もあった。また、出現した時期が 2001 年の米国同時多発テロの直後であったため、大きな混乱を生じる結果になった。

CodeRed と同じく、マイクロソフト社からは事前にセキュリティホールの修正プログラムが公開されていた。二つのセキュリティホールが悪用されていたが、それぞれ 6 ヶ月前、1 年前に対策されたものである。ここでも未対応ホストが被害を受けた。

c) Klez

Klez は、Internet Explorer のセキュリティホールを悪用したウィルスで、電子メールの添付ファイルによって感染する。オリジナルは 2001 年 10 月 26 日に発見されているが、その後亜種も様々なものが出現している。

Klez は、ウィルスを添付したメールを Outlook Express でプレビューするか、Outlook で開いたときに感染する。Nimda と同じセキュリティホールを悪用されたことにより、自動的な感染が行われることとなった。感染した PC は、これらのメールクライアントのアドレス帳に登録されている全てのアドレス宛に、ウィルスを添付したメールを送信する。送信者のアドレス欄には、ウィルスが作成した架空のアドレスが記載される。

2002 年 1 月に出現した亜種では、Windows の System フォルダに自分自身をコピーし、Windows が起動するたびにウィルスが実行されるようにレジストリの変更を行う。また、共有しているネットワーク上にも自身をコピーし、感染を拡大する。さらに、送信者のアドレスをアドレス帳から取得したものに設定するため、実際にはウィルスに感染していないのにウィルスの送信元とされてしまう例もある。

Klez ウィルスは、亜種も含めて毎月 6 日に発病する。発病すると、PC の C ドライブのデータが破壊される。

情報処理振興事業協会(IPA)「2002 年ウィルス発見届出状況」によれば、2002 年に国内で届出のあったウィルス被害(20,352 件)のうち、約半数にあたる 9,648 件が Klez (亜種含む)に関するものであった。2003 年 5 月時点でも、引き続きウィルス被害届出の上位を占めている。

このセキュリティホールに関しても、7 ヶ月前にマイクロソフト社より修正プログラムが公開されていた。

d) SQL Slammer

2003 年 1 月､全世界のネットワークで UDP/1434 ポート宛のパケットが急激に増加し、ネットワーク利用に支障をきたす事態が発生した。その原因となったのが SQL Slammer である。

SQL Slammer は、マイクロソフト社の SQL Server 2000 に感染するワームである。Slammer に感染したホストは、Windows の API 関数を利用してランダムな IP アドレスを生成し、そのアドレスの UDP/1434 ポート宛に Slammer 自身を繰り返し送信し続ける。その結果､大量の UDP/IP トラフィックを発生させて回線の輻輳やルータの負荷上昇を招き、ネットワークのパフォーマンスに深刻なダメージを与える。一般的なワームと異なり、感染対象に破壊的なダメージを与えたり、不正侵入のための裏口を仕掛けたりすることはないが、大量のトラフィックを発生させることで、実質的な DoS 攻撃を行う。

SQL Slammer は､事件発生の半年以上も前に脆弱性が発見され､マイクロソフトからもセキュリティパッチが提供されていたにも関わらず、被害が拡大した。すなわち、多くのホストでセキュリティ・ホールが塞がれていないという実態が問題となった。その背景には、多くのユーザが、セキュリティパッチの適用によってシステムの他の部分が正常に動作しなくなるという、いわばパッチの副作用への懸念から、適用に慎重になっているという事情があるものと見られている。

また､SQL Slammer による被害が特に大きかったのが韓国であった｡総務省の訪韓調査によれば、韓国ではブロードバンド普及率が高く、ワームが急速に拡散したこと、全てのポートを開く設定にする傾向があり、攻撃対象となるサーバが日本と比較して多かったこと、上記の事情や不正コピーのためにセキュリティパッチを適用していないサーバが多数存在したことが、韓国での被害の拡大の原因と考えられている。

e) ネットバンキングでの預金不正引出し

2003 年 2 月、ネットバンキングの ID とパスワードを不正に入手し、当該口座から約 1600 万円を架空名義の自分の口座に振り込んだ疑いで、元シンクタンク社員ら 2 名が逮捕された。

事件の手口は、都内を中心に 100 ヶ所以上のインターネットカフェの端末に､「キーロガー」と呼ばれる、キーボードから入力された文字を全てテキストデータとして記録するプログラムを仕掛けておき、後日収集したログからネットバンキング利用者の ID とパスワードを入手して、そのネットワンキング利用者に成りすまして不正にアクセスし、自分が作った別銀行の架空口座にお金を振り込み、ATM から引き出したというものであった。キーロガーはネット上で容易に入手できるため、同様の手口は誰にでも実行可能と言える。

この事件では、ネットバンキング利用者、インターネットカフェ、銀行のそれぞれについて、危機意識の欠如、認識の甘さが指摘された。具体的には以下の通りである。

- **ネットバンキング利用者…不特定多数の人が利用し、何らかの仕掛けがなされている可能性も否定できないようなインターネットカフェの端末で、銀行口座の ID とパスワードを入力していた。**
- **インターネットカフェ…利用者が変わるたびに端末を初期状態に戻す作業を行わず、前の利用者の痕跡をそのまま残していた。**
- **銀行…ID とパスワードのみで認証を行っていた。銀行によっては ID、パスワードに加えて、乱数表の指定された箇所の数字を入力して認証を行うものもあり、これを用いれば本章で挙げた手口の犯行は防止できた。**

2.3.3 サイバーテロ

(1) サイバーテロの脅威

我が国の銀行・金融サービス、通信、運輸、電力、石油・ガス、水道、緊急サービス、行政サービスなどのサービスは、現在、高度に情報化・ネットワーク化されており、今後もこれらの国民生活や社会経済活動を支えるインフラの情報化・ネットワーク化の流れはますます加速するものと考えられる。

一方で、これらのインフラへの依存が大きくなるにつれて、そのサービスの停止は、国民生活や社会経済活動に大きな影響を与えることとなる。例えば、最近でも、銀行などの金融機関での情報システムのダウンによる経済活動の混乱や、航空管制システムのダウンによる大量の航空便の運休といった事態が発生している。現在までのところ、サイバーテロにより、重要インフラが大きな被害を受けるという事態は発生していないが、サイバーテロが組織的かつ大規模に行われ、通信回線設備攻撃による通信ダウン、航空管制や鉄道の運行システム攻撃による公共交通機関の停止、金融機関や証券取引所のシステムの攻撃による経済取引活動の停止、電力供給システムへの攻撃による停電、あるいは病院や消防などの緊急設備に対する攻撃による緊急活動の停止といった事態が発生した場合には、国民生活や社会経済活動さらには国民の生命に対して深刻な被害が出ることが予測される。

サイバーテロは、日本の直接的な安全保障にとっても大きな脅威となり得る。湾岸戦争で、米国及びその同盟国に対する潜在的な敵国や主要テロ集団は，通常の兵器や軍事力では米国に勝つことは非常に難しいことを知った。それに続くアフガニスタンやイラクでの戦争により、これらの国々や集団は、その事実を改めて再認識したと考えられる。米国及びその同盟国に対する潜在的な敵国や集団が，通常の軍事力ではなく、サイバーテロによって米国の強力な軍事力に対抗しようとする可能性を否定することはできない。

(2) サイバーテロの特徴

インターネットなどを利用したサイバーテロの第一の特徴は、物理的な距離に依存せずにインターネット経由で情報システムを攻撃することにより、直接、敵国の経済的な基盤を破壊できるということである。従来の戦争においても、軍事設備や施設ではなく、エネルギー供給、通信、輸送、生産といった、敵国の経済的基盤を直接破壊することで戦いを優位に進めるという戦略がしばしば実行されているが、サイバー攻撃は、極論をすれば、長距離ミサイルによって、敵国の経済の中枢を攻撃するのと同等のインパクトを与える可能性もあると言える。

サイバーテロの第二の特徴は、テロを行うためのコストが非常に低いことである。従来のテロによって、国家の重要インフラを形成する情報システムや情報通信ネットワークを

物理的に破壊するためには、テロ実行者に対する訓練や武器を用意するために多くの資金が必要であった。しかしサイバーテロに必要となる多くのクラッカーツールはインターネットから手に入れることが可能であり、インターネットに接続された通常のパソコンとある程度の専門的な知識があれは、サイバーテロを実行することは、比較的容易であるとも言われている。この特徴は、小規模で資金力が弱く、これまでは比較的限られた地域で活動を行っていたテロリスト組織などや反社会的な思想をもつ個人が、国家を危機に陥れる大規模なサイバーテロを実行する危険性があることを示している。1997 年に米国防総省が行った「エリジブル・レシーバー」と呼ばれるサイバーテロの演習（擬似攻撃）では、30 人あまりのチームが、インター－ネットで容易に手に入れることができるクラッカーツールを使用して、電力送電システムや国防総省の指揮統制システム等への侵入に成功したと言われている。

サイバーテロは、さらに、罰則や報復による抑止が難しいという特徴もある。サイバーテロは、インターネット等を使用して遠隔からテロを実行することが可能であるため、犯人は安全な場所から攻撃を行うことができる。また、現在、サイバー攻撃を行った犯人を即座に特定することは技術的に難しい。さらに重要インフラに対するサイバー攻撃が、絶えず行われていると言われる通常のクラッカーによる攻撃なのか、国家やテロ集団が起こしたサイバーテロであるのかを判定し、サイバーテロを起こした集団に対する何らかの罰則や報復等といった措置を取るためには、さらに長い時間が必要となる。このようにサイバーテロを抑止するためには、従来の罰則や報復といった力による抑止を越えた対応が必要になる可能性もある。

(3) サイバーテロの攻撃方法

現在、サイバーテロは、「サービス拒否攻撃(DoS, DDoS)」、「セキュリティ・ホール」、「コンピュータ・ウィルス」、「裏口プログラム」、「トロイの木馬」、「時限爆弾・論理爆弾」といった、インターネットのクラッカーサイトで手に入れることが可能なツール、あるいはそのようなツールを改造したものが使用されると考えられる。米国の「エリジブル・レシーバー」の例が示すように、セキュリティ対策が十分ではない情報システムに対しては、このようなツールを使用したサイバー攻撃であっても、十分に大きな混乱を引き起こし、例えば「混乱を引き起こすことによる組織活動の宣伝」程度の目標を達成することは容易であると思われる。また、以上のようなインターネットから手に入れることが可能なツールではなく、国家あるいはそれに匹敵するレベルで、情報システムに対する高度な専門知識を持つ者を集め、サイバーテロ用のツールの開発が行われている可能性もある。

この他、情報システムの設計、構築、運用に関わる内部関係者が、内部からシステムの攻撃を行ったり、テロリストに情報システムの情報を横流ししたりした場合、サイバーテロにより非常に深刻な被害が発生することは、容易に想像できる。このような事態を防ぐためにも、従来から行われている内部関係者に対する教育、意識啓発、情報管理、監査と

いった活動は非常に重要である。

重要インフラを支える情報通信システムや情報通信ネットワークは、高度に発展・複雑化しているが、今後もこれらのシステムを支える技術は急速な発展を続けると考えられるが、この技術の発展は、また新たな脆弱性が発生する危険性があるということも示している。サイバーテロリストは、この技術の発展の裏に潜むシステムの脆弱性を発見し、攻撃を行うため、サイバーテロを防止するためには、技術の進歩に合わせて、継続的にシステムの脆弱性を発見、対策を行うことが重要となる。また防御・対策技術はどうしても攻撃技術に遅れるという事実を認め、サイバーテロに対する防御・対策という観点のみではなく、新たな攻撃手段を積極的に発見する観点から対策を行うべきという考え方もある。

サイバーテロに対する危機管理においては、技術的な予防措置を講ずることはもちろん重要であるが、情報通信ネットワークや情報システムが外部と接続されている限り、サイバーテロを完全に防止することはできない。日本国際問題研究所（JIIA）では、平成 13 年度の外務省委託研究として、「ＩＴ革命と安全保障」という論文を発表しており、その中で、攻撃があり得ることを前提とした結果管理の側面の強化を強調している。つまり、完全な安全の確保を必要とするような情報システムはネットワークから隔絶する。そして、それ以外の情報システムは攻撃を前提としてリダンダンシーを確保することにより、波及性を阻止し、バックアップを確実にすることが重要であると述べている。またこの論文中では、サイバー空間からの攻撃に対し、技術的な対応をするのみならず、その攻撃を誘発している政治的な背景を理解し、それに対しても効果的な対策を講じる必要性についても論じられている。

サイバーテロの対象となる重要インフラの多くは、民間企業が保持・運営しているため、官と民が協力してサイバーテロに対応する必要がある。特に、サイバーテロの影響は即時に広範囲に及ぶことが多いため、サイバーテロ発生時に迅速な対応ができることが重要である。

サイバーテロは、インターネット等を使用して遠隔からテロを実行できるという特質を有しており、その防止・抑制のために国際的に協調して有効な手段をとる必要があることから、法的拘束力のある国際文書の作成が必要との認識が高まっている。その具体的な取り組みとして、1997年2月より、欧州評議会刑事問題欧州委員会に専門家会合を設置し、サイバー犯罪に関する条約案の検討が開始された。条約案の検討には、英、独、仏、伊などの欧州各国のほか、オブザーバー国として米、加、墨及び我が国も参加し、2001年11月6月には条約案の取りまとめが行わた。その後、本案は、2001年11月8日に欧州委員会閣僚委員会会合において正式採択され、我が国も2001年11月23日に行われた署名式典において署名を行っている。

現在、我が国においては、条約の批准に向け、国内法の整備に向けた検討を行っているところである。しかしながら、国際協力のもとで効果的なサイバーテロ対策を行うためには、多くの技術的な取り組みも必要である。

2.4 インターネット・セキュリティに対する取り組み

2.4.1 我が国の取り組み

2.1章に示した通り、我が国においては、「5年以内に世界最先端のIT国家となる」という目標が、2001年1月のe-Japan戦略において掲げられて以来、「e-Japan重点計画」(2001年3月)、「e-Japan2002プログラム」(2001年6月)として、政府の行うべき施策を定めた各種計画が策定・実行されてきている。IT分野における発展の速度は速く、諸外国と比較した位置付けや実施された施策の評価に基づいて適宜計画の見直しを行う必要があり、e-Japan戦略においてもそれまでの実績を基に計画が見直され、2002年6月に「e-Japan重点計画-2002」として、高度情報通信ネットワーク社会の形成のために政府が重点的に実施すべき施策が策定された。

「e-Japan重点計画-2002」においては、重点政策5分野として、重点的に施策を行うべき5つの分野を掲げているが、その中でインターネット・セキュリティに関する取り組みは、「高度情報通信ネットワークの安全性及び信頼性の確保」の分野として取り上げられており、本項ではこれまでの成果とともに施策の内容について概説する。今後はこれら施策を確実に実行に移し、国民が安心して利用できる安全性・信頼性の高い高度情報通信ネットワークをできるだけ早期に実現することが重要である。

(1) 課題と方向性

2001年9月の米国における同時多発テロ等を踏まえたサイバーテロ対策、サイバー犯罪条約署名等の国際的な取り組みのほか、電子政府の前倒し実現・電子自治体の推進への対応、国民が安心してネットワークを利用できるような環境整備について重点的に進められている。

(2) 主要施策

a) サイバーテロ等からの電子政府及び重要インフラの防護対策の充実強化

サイバーテロ等の脅威から電子政府や重要インフラを防護するため、各省庁におけるポリシー運用の徹底や防御・監視体制の強化、官民における重要インフラ防護のための作業、緊急対処能力の向上を推進する。

b) 国際協調のとれた情報セキュリティ対策推進体制の整備

国際的な動向を踏まえた刑事基本法制や捜査体制の整備、情報セキュリティ技術評価・認証事業の国際相互承認、情報セキュリティに関する国際的な連携・協力を推進する。

c) **情報セキュリティに係わる国内全体の人的・技術的基盤等の整備**

情報セキュリティに係わる技能標準、暗号技術の評価や事業者のセキュリティに関する評価基準の整備、情報提供・相談受付体制の充実や普及啓発、研究開発の推進により、情報セキュリティに係わる重層的な基盤を整備する。

d) **個人情報の保護**

個人情報保護法、行政機関個人情報保護法等に基づいて、官民を通じる個人情報の適正な取り扱いの確保を図る。

(3) **これまでの主な成果**

a) **政府部内における情報セキュリティ対策**

- **電子政府の実現に対応した政府のとるべき措置について、「電子政府の情報セキュリティ確保のためのアクションプラン」としてとりまとめ。**
- **緊急対応支援チーム**(NIRT)**を創設し、同チームの運営マニュアル等を整備。**
- **情報機器等の情報セキュリティ国際規格**(ISO/IEC 15408)**に基づいた評価・認証事業を開始。**

b) **重要インフラのサイバーテロ対策**

- **重要インフラ(情報通信、金融、航空、鉄道、電力、ガス)における連絡・連携体制を構築。**
- **機動的技術部隊(サイバーフォース)を整備。**

c) **民間部門における情報セキュリティ対策及び普及啓発**

- **「コンピュータ・ウィルス監視装置」の導入を行う民間事業者に対する税制上の優遇措置を実施。**
- **小学校及び中学校において情報モラルなどの学習を実施。**

d) **情報セキュリティに係わる制度・基盤の整備**

- **支払い用カードの偽造等の犯罪に関する罰則を整備。**
- **携帯電話等を用いたインターネット利用の急増に対処するための安全性・信頼向上策、迷惑メールへの技術的対策等について基準を策定。**
- **情報セキュリティマネジメントに関する国際規格**(ISO/IEC 17799)**を国内規格化。**

e) **個人情報の保護**

- **個人情報の保護に関する法律案提出。**
- **行政機関の保有する個人情報の保護に関する法律案、独立行政法人等の保有する個人情報の保護に関する法律案、情報公開・個人情報保護審査会設置法案、行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律も整備等に関する法律案提出。**

f) **情報セキュリティに係わる人材育成**

- 電気通信主任技術者試験に情報セキュリティに関する試験科目を追加。
- 情報処理技術者試験に情報セキュリティアドミニストレータ試験を導入。
- 米 CERT/CC へ専門技術要員の派遣。

g) 情報セキュリティに係わる国際連携

- 第 2 回 G8 ハイテク犯罪対策官民合同ハイレベル会合を開催。
- アジア・太平洋ハイテク犯罪対策担当実務者会議を開催。
- アジア太平洋地域の CSIRT(Computer Security Incident Response Team)による国際会議を開催。
- 米国国務省との間において IT フォーラムを開催。

(4) 今後の具体的施策

a) 政府の情報セキュリティ確保

- 情報セキュリティポリシーの実効性の確保(内閣官房、全府省)
- 電子政府の情報セキュリティ確保のための体制の整備(内閣官房)
- 地方公共団体の情報セキュリティ確保の支援(総務省)

b) 重要インフラのサイバーテロ対策

- 特別行動計画における取り組みの強化(内閣官房、関係府省)
- 内閣官房における緊急対処体制の整備(内閣官房)
- 警察における緊急対処体制の整備(警察庁)
- 防衛庁における緊急対処体制等の整備(防衛庁)

c) 民間部門における情報セキュリティ対策及び普及啓発

- 情報セキュリティ意識の向上(警察庁)
- 産業界との連携の強化(警察庁、総務省、経済産業省)
- 信頼性向上施設等の導入支援(総務省)
- 情報通信ネットワークにおける情報セキュリティ評価手法の確立(総務省)
- 電気通信事業における情報セキュリティ対策の認定(総務省)
- 不正アクセス対策・ウィルス対策等に関する情報提供体制の強化(経済産業省)
- 情報セキュリティマネジメント規格の普及啓発(経済産業省)

d) 情報セキュリティに係わる制度・基盤の整備

- 刑事基本法制等の整備(警察庁、総務省、法務省、外務省、経済産業省)
- 電気通信事業における安全・信頼性対策(総務省)
- 暗号技術の標準化の推進(総務省、経済産業省)
- 情報セキュリティ評価・認定事業の国際相互承認(経済産業省)

e) 個人情報の保護

- 個人情報の適正な取り扱いに関する基本法制の整備(内閣官房、内閣府を含む全府省)

- 行政機関及び独立行政法人等の保有する個人情報の適正な取り扱いに関する法制の整備(総務省を含む全府省)

f) 情報セキュリティに係わる研究開発
   - 国防・治安に係わる情報セキュリティ技術の研究開発の推進
   - 情報セキュリティに関する基盤技術の研究開発の推進(警察庁、総務省及び経済産業省)

g) 情報セキュリティに係わる人材育成
   - ハイテク犯罪対策に係わる人的基盤の整備(警察庁)
   - 防衛庁における情報セキュリティ等に係わる人材教育(防衛庁)
   - IT セキュリティ技能標準の策定・普及(経済産業省)
   - 情報セキュリティ評価技術者の育成(経済産業省)

h) 情報セキュリティに係わる国際連携
   - ハイテク犯罪対策に係わる国際連携の強化(警察庁、総務省、外務省、法務省及び経済産業省)
   - 各国警察関係期間との連携強化(警察庁)
   - 米国国防総省等との連携強化(防衛庁)
   - 情報セキュリティに関するグローバル情報交換ネットワークの構築(経済産業省)

2.4.2 米国の取り組み

インターネット発祥の地である米国では、ネットワークの発展に伴い比較的早期より国防、電気、ガス、電話、交通等の重要インフラがインターネット接続されることとなった。一方で、それら重要インフラへの不正侵入等の試みが頻繁に検出されるようになると、重要インフラへのサイバー攻撃が国家安全保障上の脅威となるとの認識が高まり、世界に先駆けてサイバーセキュリティに関する取り組みを実施するようになった。また、2001 年 9 月に米国において発生した同時多発テロによって、テロリスト等によるサイバーテロの脅威が改めて認識され、国家レベルでのセキュリティ対策の強化が検討されている。

本項では、主に重要インフラ保護という観点から、米国におけるサイバーセキュリティに関する取り組みについて概説する。

(1) Eligible Receiver

1997 年 6 月、国防総省は省内ネットワークや通信・電力等重要インフラのサイバー攻撃に対する脆弱性を調査するため、「Eligible Receiver」と呼ばれる実験を行った。この実験は、国家安全保障関連の機関に勤める職員 30 名がハッカーに扮して、一般人と同等の条件で以

下のような課題に取り組み、システムの脆弱性を調査するというものであった。

- 通信・電力等重要インフラの管理システムのスイッチ切断
- 国防総省のコンピュータネットワークへの不正侵入

実験の結果、3 ヶ月という期間の間に、特別な知識を持たないわずか 30 名ものメンバーが、通信・電力等の重要インフラを麻痺させ、国防総省のネットワークを不正に制御可能であることが判明した。これは、少人数で、米国を国家安全保障上の危機に陥れることができることを意味し、この結果に大きな衝撃を受けた米国政府は、サイバーセキュリティ対策を重点課題として取り上げるようになった。

「Eligible Receiver」実験の結果、国防総省を始めとする政府機関においては、積極的にサイバーセキュリティ対策に取り組むようになった一方で、民間では重要インフラ防護に対する取り組みが遅れていたため、米国政府は以下に示す一連の重要インフラ防護政策を実施した。

1996 年 7 月	クリントン前大統領が重要インフラ保護委員会(PCCIP)を設置
1997 年 10 月	PCCIP が勧告を提出
1998 年 5 月	大統領令 63 号(PDD63)を発令
2000 年 1 月	国家情報システム保護計画(第 1 版)を発表

(2) PCCIP による勧告

PCCIP は、米国の安全保障や国民生活にとって必要不可欠である重要インフラを防護するための方策を検討し、下記の内容を勧告した。

- 民間のサイバーセキュリティに関する意識を高めるため、広範囲に渡るプログラムを開発する。
- 産官の協力と情報共有を促す。
- 現行法を見直し、重要インフラ防護の障害となる要因があれば排除する。
- 重要インフラ防護に適用できる技術を発展させる研究開発プログラムを推進する。
- 重要インフラ防護に関して、重要決議や勧告を効果的に行うための国家的な取り組みを推進する。

(3) 大統領令第 63 号(PDD63)

PCCIP の勧告を受けて、クリントン前大統領は大統領令第 63 号(PDD63)を発令した。PDD63 には、以下の内容が示されている。

- 2000 年までに政府の情報システムのセキュリティを著しく高め、2003 年までに信頼性が高く、安全かつ相互接続した情報システムを構築する。
- 早急にサイバー攻撃への警告及び対応を行う国立センターを設置する。
- 連邦政府機関がサイバー攻撃や物理的攻撃に対する各自の情報システムの脆弱性を

認識し、対策を講じることで、新たな脅威にさらされる機会を減少させる。

- 連邦政府が、州政府や民間の手本となるような重要インフラ防御策を講じる。
- 官民が協力して重要インフラを防護できるよう民間の自主的な参加を促す。
- 個人のプライバシー保護や市場の自由競争を妨げないサイバーセキュリティ対策を実施する。
- サイバーセキュリティ対策全般において、議会への参加と協力を求める。
-

さらに、PDD63 では以下に示す体制を構築し、これらの課題に取り組むように命じている。

- 国家調整官の任命
  初代調整官としてリチャード・クラーク氏を指名。
- 国家インフラ防護センター(NIPC)を設置
- 情報共有分析センター(ISAC)を設置
- 国家インフラ保証会議(NIAC)を設置
- 重要インフラ保証局(CIAO)を設置

(4) 国家情報システム保護計画(第 1 版)

クリントン前大統領は、PDD63 に基づき具体的な計画として「国家情報システム保護計画(第 1 版)を定めた。本計画の概要を以下に示す。

a) 目標 1： 準備と防衛

重要インフラへの大規模な攻撃が遂行される可能性を最小限に抑えるために必要な措置をとり、攻撃が仕掛けられても持ちこたえるインフラを構築する。

施策 1： 重要インフラの構成要素及びそれらの相互依存性を分析し、脆弱点を明確化する。

b) 目標 2： 検知と対応

攻撃をタイムリーに検知・分析し、その制圧、迅速な回復、被害を受けたシステムを再構成するための手段を講じる。

施策 2： サイバー攻撃及び不正侵入を検知する。

施策 3：法的整合性を保ちつつ重要インフラを防護する諜報･捜査機構を確立する。

施策 4： サイバー攻撃の警告や情報を迅速に通知する。

施策 5： サイバー攻撃に対する対処、システム復旧、再構成手順を確立する。

c) 目標 3： 強固な基盤の構築

重要インフラへのサイバー攻撃に対応するための人材育成及び組織・法制度の整備を行う。

施策 6： 施策 1-5 を促進する研究開発を支援する。

施策 7： サイバーセキュリティの専門家を積極的に育成・訓練する。

施策 8： サイバーセキュリティに対する市民の認識を高める。
施策 9： 施策 1-8 を促進するための法整備と財政支出を行う。
施策 10： これらの活動遂行にあたり、市民のプライバシー・個人情報保護の権利を保障する。

(5) 同時多発テロ以後

このように、米国における重要インフラ保護を目的としたサイバーセキュリティ対策の基本的枠組みは、大統領令第 63 号(1998 年)及び国家情報システム保護計画(第 1 版、2000 年)によって規定されているが、その後 2001 年 9 月に発生した同時多発テロを契機に、サイバーテロに対する脅威の認識が強まったことを受けて、ブッシュ政権では以下に示すようなサイバーセキュリティ対策の強化を実施している。

a) 国土安全保障省(DHS)及び本土安全保障会議(HSC)

2001 年 10 月にブッシュ大統領より行政命令が発令される。

DHS は、テロリストの脅威あるいは攻撃から米国を守るための包括的国家戦略の構築とその実施にあたっての総合調整を行うことを使命としている。また HSC は、本土安全保障に関して、あらゆる角度から大統領に助言・支援を行うもので、大統領、副大統領を始めとして関係省庁・機関の長などで構成される。

b) サイバー安全保障局

上記 DHS の創設と併せて、サイバースペースの安全保障を担当する部署としてサイバー安全保障局が設置された。

c) 大統領重要インフラ保護会議

2001 年 10 月にブッシュ大統領より行政命令が発令される。

重要インフラとしての情報システム保護のため、大統領重要インフラ保護会議を設置するなどの体制強化を行った。本会議は、関係省庁・機関等の代表者で構成され、各省庁・機関の取り組みの相互理解や調整、民間や州・地方政府との協力等を目的としている。

d) ギルモア委員会勧告

国防総省等からの委託によりテロリズム対策の評価・勧告を行う「大量殺戮兵器によるテロリズムへの米国内対応能力を評価する諮問パネル」(通称 ギルモア委員会)が構成され、同委員会が公表した報告書では、サイバーテロリズムに対するセキュリティ確保についても言及されている。

e) GOVNET 構想

2001 年 10 月、連邦調達庁は大統領サイバーセキュリティ特別顧問のリチャード・クラーク氏からの要請に基づいて、商用インターネットとは切り離された政府専用の IP ベースのネットワークの構築に向けた RFI を提出した(GOVNET 構想)。

f) 米国愛国者法

2001 年 10 月、テロリズム対策の強化を図るための法律である「米国愛国者法」が成立した。同法は、テロリスト捜索等のため、政府機関による情報の収集や共有、移民の拘束、テロ協力者の取調べ、テロ組織と関連ある銀行口座や資産の凍結等に関する法執行機関や諜報機関の権限拡大を目的とするものである。

g) サイバーセキュリティ研究開発法

2002 年 11 月、米国のコンピュータとネットワークのセキュリティに関する研究開発を推進する「サイバーセキュリティ研究開発法」が成立した。これを受けて米国政府は 2003 年度から 2007 年度までの間に 8 億 7800 万ドルを投じ、ネットワークセキュリティ研究センターの設置や研究の支援、人材育成を進める予定である。50 以上の大学で大学院レベルを中心に情報セキュリティの教育コースを実施するなど、日本に比べてはるかに人材育成体制が整備されている米国であるが、本法律では、より一層の充実を目指している。

(6) サイバーセキュリティ計画(National Strategy to Secure Cyberspace)

同時多発テロから 1 年経過した 2002 年 9 月、米国政府はサイバーセキュリティ計画案を発表し、2003 年 2 月に「セキュアなサイパースペースのための国家戦略（National Strategy to Secure Cyberspace)」として発表を行っている。本計画中では、サイバースペースのセキュリティとは、ホームユーザから連邦政府まで国のサイバーインフラの所有者全てに大きく依存しているため、それぞれの個人や組織には、サイバースペースの中で各自が所有する部分を保護する責任がある、と述べられており、本計画では、各個人や組織が自らの役割を果たすことができるよう、サイバーセキュリティを実現するためのロードマップ及び手段が提供されている。

「セキュアなサイバースペースのための国家戦略」（National Strategy to Secure Cyberspace）の概要

○３つの戦略目標

①重要インフラに対するサイバー攻撃の予防
②サイバー攻撃に対する脆弱性の低減
③サイバー攻撃の被害と回復時間の最小化

○５つの優先課題

下記５分野について、４７項目の行動・勧告をとりまとめ。

①国家的なサイバーセキュリティ対応システム
②脅威と脆弱性の低減計画
③セキュリティ意識の啓発と訓練計画
④政府サイバースペースのセキュア化
⑤国家安全保障と国際協力

国家的なサイバーセキュリティ対応システムにおいては、官民の連携が重要であり、政府の関係機関とともに、民間のＩＳＡＣ（情報共有・分析センタ）が重要な役割を果たす。政府は、民間の各分野におけるＩＳＡＣの設立、既存のＩＳＡＣの分析能力の向上を促進すべきとしている。

また、セキュリティ脅威や脆弱性の低減計画の一つとして、インターネットに内在する脆弱性の改善（DNS、BGP 等のインターネットプロトコロの改善等）を図り、インターネット構造をセキュア化することが必要としている。

各優先課題についての主要活動は、下記のとおりである。

優先課題Ｉ：国家サイバー空間セキュリティ対応システム

①国家レベルのサイバーインシデントに対応するための官民の連携体制を確立する。
②サイバー攻撃の戦略的及び戦術的分析並びに脆弱性評価の開発に必要資金等を提供する。
③サイバー空間の健康状態の概況を共有するための民間部門の能力開発を奨励する。
④サイバー空間セキュリティの危機管理を調整するＤＨＳの役割を支援するためサイバー警報・情報ネットワークを拡張する。
⑤国のインシデント管理を改善する。
⑥全国的な官民の維持・非常時計画策定への任意参加の手続きを調整する。

⑦連邦システムのためのサイバーセキュリティ維持計画の訓練を行う。
⑧サイバー攻撃、脅威及び脆弱性を含む官民の情報共有を改善、拡充する。

優先課題Ⅱ：セキュリティ脅威と脆弱性の低減計画
①サイバー空間攻撃での攻撃を防止し、訴追する法執行機関の能力を高める。
②脅威及び脆弱性の潜在的な影響をよりよく理解するために、国家的な脆弱性評価の手続きを創設する。
③プロトコル及びルーティングの改善によりインターネットの機構をセキュア化する。
④信頼できるデジタル制御システム及び監視制御・データ取得システムの利用を促進する。
⑤ソフトウェアの脆弱性を低減し、修正する。
⑥インフラの相互依存性を理解し、サイバーシステム及び通信の物理的セキュリティを改善する。
⑦連邦のサイバーセキュリティ研究開発計画の優先度付けを行う。
⑧新しく出現するシステムを評価し、セキュア化する。

優先課題III：セキュリティ意識の啓発と訓練計画
①全ての米国人（企業、一般の労働者、一般国民）が、サイバー空間のそれぞれの部分をセキュア化できるような力をつけるための、包括的で国家的な認識プログラムを促進する。
②国家のサイバーセキュリティの要求を支援するための適切な訓練及び教育計画を促進する。
③既存の連邦サイバーセキュリティ訓練プログラムの効率を高める。
④よく調整され、広く認められた専門家のためのサイバーセキュリティ検定への民間部門の支援を促進する。

優先課題IV：政府サイバースペースのセキュア化
①連邦のサイバーシステムに対する脅威及び脆弱性を継続的に評価する。
②連邦のサイバーシステムの利用者を認証し、これを維持する。
③連邦の無線ＬＡＮをセキュア化する。
④政府の外部委託や調達におけるセキュリティを改善する。
⑤州政府や地方政府に、ＩＴセキュリティ計画立案を検討し、類似の政府との情報共有分析センターに参加するよう、奨励する。

優先課題Ⅴ：国家安全保障と国際協力

①サイバー関連の対敵情報活動を強化する。
②攻撃者特定及び対応のための能力を改善する。
③サイバー攻撃に対応するため、米国の国家安全保障共同体内部の調整を改善する。
④産業界と協力し、国際機関を通じて、情報インフラの防護と地球規模の「セキュリティ文化」の促進に焦点を当てた、国際的な官民の対話及び連携を促進する。
⑤サイバー攻撃が出現した際に検知するための、国内及び国際的な監視・警報ネットワークの設立を促進する。
⑥欧州評議会サイバー犯罪条約に参加するよう、あるいは、その法律や手続きが少なくとも同程度に包括的なものであることを確保するよう、他国に働きかける。