2.4.3 韓国の取り組み

韓国は現在ブロードバンド・インターネットの普及率で世界のトップを走っているが、これには大統領主導による一貫した政策の下で、適切な情報化施策が推進されてきたことがその要因として挙げられている。本項では、まず韓国をブロードバンド大国に押し上げた一連の施策について概要を説明し、次に 2003 年 1 月に発生したスラマーワームによる大規模なインターネット障害事件における影響やその原因の分析、また事件後におけるセキュリティ対策について概説する。

(1) 情報化社会進展に向けた取り組み

1996 年 情報化促進基本計画
1999 年 Cyber Korea 21 計画
2001 年 情報通信基盤保護法の施行
2002 年 e-Korea Vision 2006

(2) Cyber Korea 21

1999 年 3 月、韓国情報通信部は Cyber Korea 21(韓国の知識ベース情報社会に向けてのビジョン)と題するレポートを発表した。これは、21 世紀が知識ベース社会へ移行するという認識のもと、次の 4 年間に注力する 3 つのテーマとして、知識ベース社会のための情報基盤の強化、情報基盤を活用した国の生産性の向上、情報基盤上の新規事業の育成を掲げている。そして、2002 年までに世界トップ 10 以内の IT 立国になることを目標とし、以下に示す具体的な施策を挙げている。

a) 情報通信インフラの整備
   - KII の効率的な整備
   - インフラのオープン・スタンダード化促進
   - 国家規模の情報教育の提供、コンピュータ・リテラシー認証システムの導入
   - 知識基盤社会へ向けた法規制の改善
   - 情報システムの安全と信頼性の確保等

b) 情報インフラの活用による生産性の向上
   - 効率的な電子政府の構築
   - 既存産業の生産性の改善等

c) 新規産業と雇用の創出
   - インターネット・ベースの新規産業の育成
   - IT 研究開発と関連人材の育成等

(3)　情報通信基盤保護法

韓国では、2001 年に「情報通信基盤保護法」が公布・施行されており、同法では、国の情報セキュリティ体制、重要インフラの指定、重要インフラに関する情報セキュリティ対策等を規定している。

この法律には、情報共有・分析センター（ISAC）の役割・責務等が規定されており、電気通信、金融分野において ISAC が設立されている。

(4)　e-Korea Vision 2006

「Cyber Korea 21」の目標実現は 2002 年度とされていたが、予定以上の速さで計画が進み 2001 年度には目標が達成された。そのため、韓国政府は情報化促進のための 3 番目の基本計画として e-Korea Vision 2006 を策定した。e-Korea Vision 2006 における主要目的は以下の通りである。

a) 全市民の情報活用能力の引き上げ
b) 情報化による全産業の生産性の向上
c) 透明性･生産性の高い優れた政府の実現
d) 世界最高の情報インフラ構築と IT 産業国としての飛躍
e) 国際協力強化によるグローバル情報社会の主導

具体的目標としては、2006 年までにインターネット利用人口を国民の 90%に拡大する、企業間の電子取引を活性化し主要産業の電子取引率を 4%から 30%に引き上げる等が掲げられている。

(5)　SQL Slammer ワームによる大規模インターネット障害

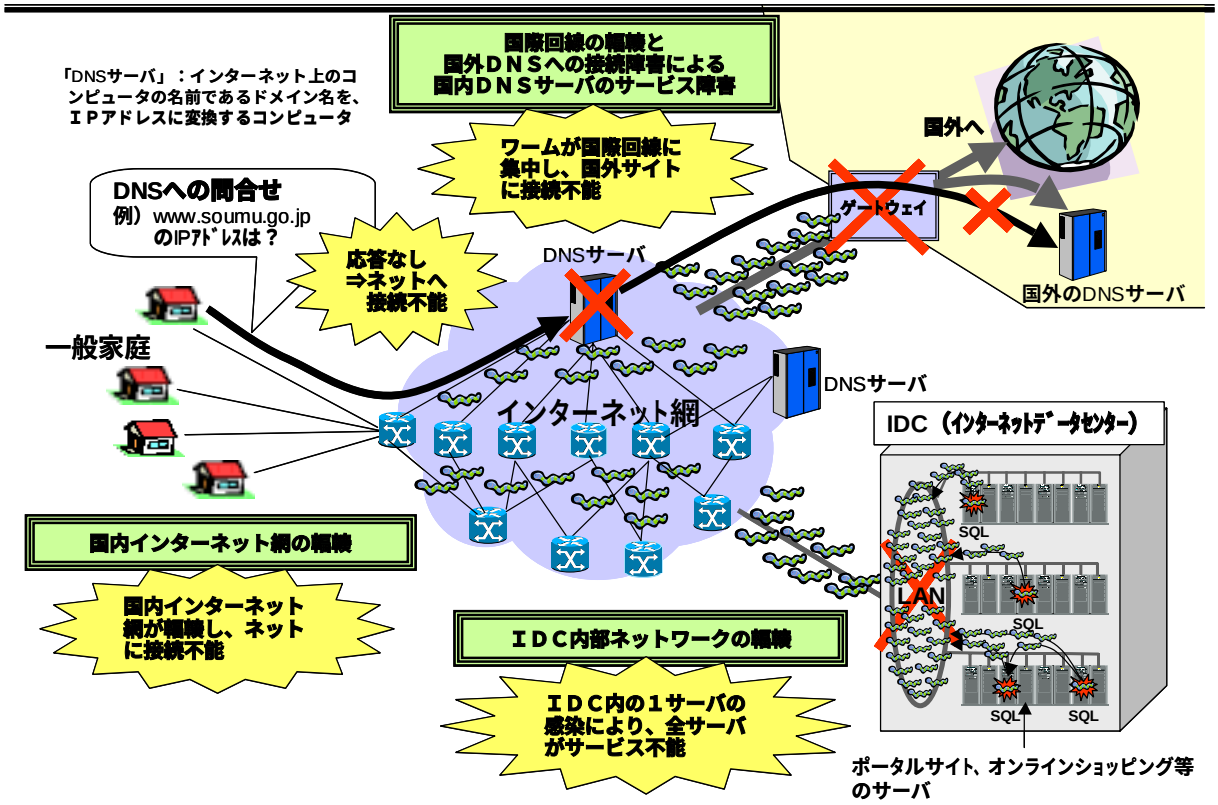
上記に示した一連の政策の効果もあって、韓国はブロードバンド・インターネットの普及率において世界トップクラスとなったが、2003 年 1 月に起こった大規模インターネット障害事件によって、その足元が案外脆いものであることが露呈された。

この事件は、SQL Slammer と呼ばれる Microsoft SQL Server 2000 の脆弱性を攻撃するワームにより、韓国国内の多数のシステムが感染しサーバが過負荷状態になるとともに、ワームが送出する大量のパケットによって国外向けのリンクが輻輳し、結果として数時間に渡ってインターネットアクセス障害が発生したというものである。

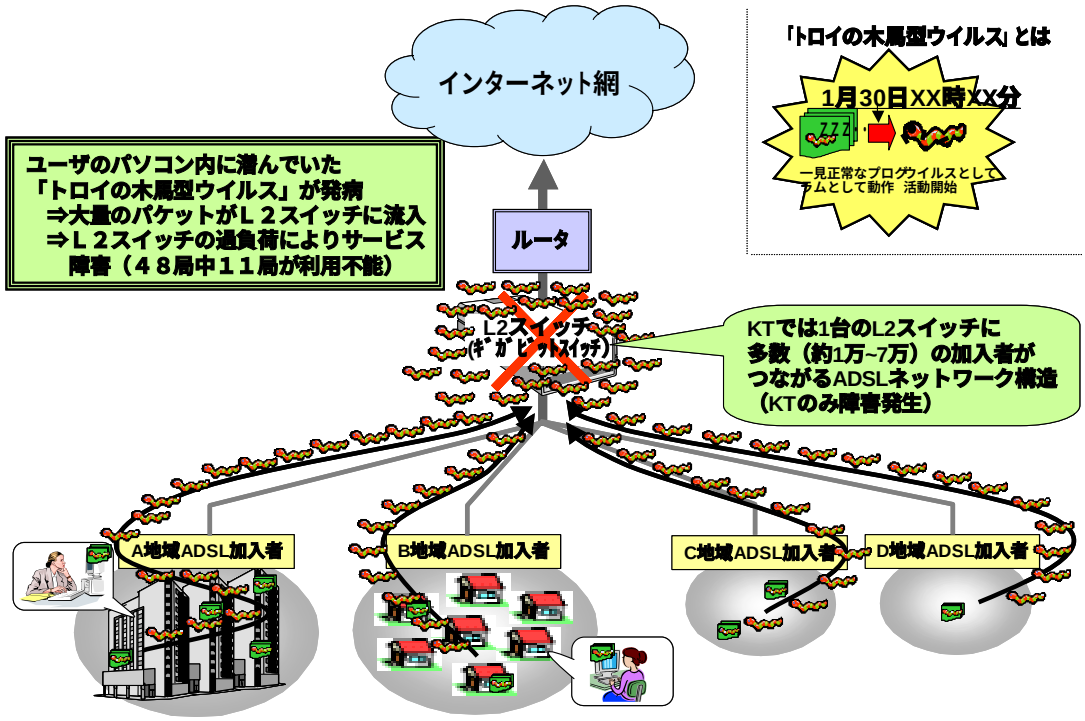
○経過

2003年1月25日　SQLワームにより、大規模なインターネット障害が発生
2003年1月30日　トロイの木馬により、KTのADSL網で大規模障害が発生
2003年2月18日　情報通信部の事故調査団が「事故調査結果」を発表

韓国インターネット障害（1月25日）のイメージ



韓国ＡＤＳＬ障害（1月30日）のイメージ



事態を重く見た韓国政府は、事件後すぐに調査団を構成し被害の状況及び原因の調査･分析を行い、他国と比較して韓国国内で被害が大きくなった要因として以下の項目を挙げている。

韓国に被害が集中した理由 (韓国官民合同調査団報告より)

1　他国に比べ多数のＳＱＬサーバがワームに感染

【参考】SQLワーム感染台数

韓国 8,848台(11.82%)　日本 1,288台(1.72%)　中国 4,708台(6.29%)　米国 32,091台(42.87%)

（インターネットデータ分析協力協会(CAIDA）より）

2　国際回線の輻輳及びルートＤＮＳサーバの不在

国際向け回線容量が大量の異常トラフィックに耐えられず、国際回線が輻輳。また、国内にルートDNSサーバがなく国外への問合せが集中したため国内DNSサーバに過負荷

3　高いブロードバンド普及率

広く普及した高速回線を通じて急速にワームが拡散

4　ＩＤＣ内の脆弱性

IDC内の設置サーバがLANで接続されているため、一部の脆弱なサーバがワームに感染するとLANで接続された他のサーバにも急速に被害が拡散

5　一般ユーザの低いセキュリティ意識

セキュリティパッチ等の未実施、不正コピー製品の使用

6　障害発生が、インターネット利用の多い昼間であったこと

欧米は深夜、中国は春節連休期間であったため、相対的に被害小

【参考】

韓国及び日本 25日(土)14:30　　中国 25日(土)13:30

欧州(英国) 25日(土)5:30　　米国 25日(土)0:30

また、調査団はこの事件を教訓として、国家的次元で情報保護レベルが画期的に向上するような情報保護強化対策の必要性を示唆している。具体的な政策的示唆点は以下の通りである。

韓国情報通信部の官民合同調査団の提言

1　情報セキュリティに関する認識の向上
　システム管理者及び一般ユーザのセキュリティ意識向上を図るとともに、セキュリティパッチファイルの適用、ワクチン情報のアップデート等の情報セキュリティ活動を一般化。

2　ルートＤＮＳサーバの韓国誘致の必要性
　国際回線障害による韓国内DNSサーバの障害を予防するため、ルートDNSサーバの韓国への誘致が必要。

3　インターネットのトラフィック管理を通じた早期予報・警報体制の確立
　異常トラフィックの発生を早期にモニタリングし、予報・警報を出すことができるシステムを開発。これを活用して数分以内にインターネット全体のトラフィックを遮断することができる早期対応体系を構築。

4　制度改善
　障害発生時に、IDC管理者がIDC内のサーバの異常なトラフィックを遮断するなどの緊急措置を可能とするなど、IDCの安全基準の強化等。

5　障害対応専門家組織の構成
　障害発生時の緊急対応、及び効果的なアフターケアを可能とするために、産学官の専門家からなるグループを構成。

今回のインターネット障害を踏まえ、総務省では、今後のインターネット・セキュリティ対策の充実・強化を目的として、韓国現地調査を実施し、インターネット障害の状況や要因を調査するとともに、今後の日韓の協力･連携の重要性について意見交換を行い、

- 日韓の Telecom-ISAC 相互間の連携
- インターネットの安全性･信頼性の確保に向けた両国間の連携強化

についての対話を今後も進めていくこととしている。

(6)　韓国のインターネット障害を踏まえた日本の教訓

韓国における大規模インターネット障害は、「セキュリティ対策が不備だと、一つのワームで、国中のインターネットが麻痺する」という実例といえる。

また、「電子政府や重要インフラのセキュリティだけを強化しても、一般ユーザのセキュリティ対策が不備だと、一国のインターネット基盤が麻痺する」という実例でもあり、我が国においても、類似の脅威に備え万全を期すことが必要である。

【日本の状況】

SQL Slammer **ワームに関して、日本国内では、**SQL **ワームの感染は若干あったものの、大きな被害は発生せず、日本のセキュリティ対策は、概ね良好だったと考えられる。しかし、セキュリティ対策が貧弱で、中央省庁のホームページが相次いで改竄された** 2000 **年の時点であったら、日本も同じ被害を蒙ったかもしれないとの指摘もあり、今後も、セキュリティ対策の確実な実施を怠らないことが重要である。**

【韓国情報通信部の事故調査報告に関して】

韓国情報通信部の事故調査団による提言の中で、特に、日本においても教訓とすべき点は次のとおりである。

①高いブロードバンド普及率

日本でもブロードバンド・常時接続が、一般家庭を含め拡大しており、リスクは確実に増大している。

②インターネット・トラフィック管理を通じた早期予報・警報体制の確立

日本でも、テレコム ISAC **が、広域モニタリングの実現に向けた取り組みを進めている。大規模ネット障害を早期に検知し、被害の拡大を極小化するために、その早期実現が望まれるとともに、日韓はじめ国際的な連携が重要である。**

③一般ユーザのセキュリティ意識の低さ

韓国では、セキュリティ法制度やセキュリティ専門機関が充実していたにも係わらず、一般ユーザの意識や対策の実施が伴っておらず、大規模障害が発生した。

事故調査報告によると、①「1 **月** 25 **日のインターネット障害及び** 1 **月** 26 **日の情報通信部の国民行動要領を発表した後も、多くのユーザがセキュリティパッチを当てなかった。」、②「このため、**1 **月** 26 **日～**29 **日の４日間、ＫＴは、約** 4,000 **名のユーザを対象に電話でパッチの適用を周知した」とされている、**

日本でも、ユーザのセキュリティ意識の向上を図り、対策の確実な実施を一層促進することが重要ではある。

一方、一般ユーザの意識向上には限界があり、未対策ユーザも相当数存在することを前提にしたセキュリティ対策（ネット側のセキュリティ強化等）を展開することが重要である。

2.4.4 英国の取り組み

英国では、英国貿易産業省(DTI)が、情報技術の発展と、それによる社会の急速な変化に対応しなければならない産業界を支援するための総合的な産業支援ログラム、情報社会イニシアチブ(ISI)を推進してきた。英国政府は、英国を世界で最も情報化の進んだ国家とすることを目指しており、それには「知識先導型経済」を構築することが必須であるとしている。なお、英国政府は、現代的な知識先導型経済のキーとなるのはデジタル技術であることを強調し、電子商取引が個々のビジネス、市場そして経済全体を革新的に変遷させるとしている。英国では、このような取り組みの一環として、インターネットセキュリティに関する取り組みが行われている。本項では、まず英国のセキュリティ政策の動向について概説し、次に英国における認証制度、さらには法制度について概説する。

(1) セキュリティ政策の動向

英国においては、1978 年に政府機関 GCHQ(Government Communications Headquarters：政府通信本部)の管轄下に、CESG(Communications Electronics Security Group)が設置された。CESG は、設置法により、セキュリティ保護という役割が明確に定義された組織であり、政府の情報セキュリティ全体に責任を負っている。主な業務は以下の通りである。

- 政府の情報セキュリティポリシの策定
- 政府及び公的機関のオフィシャルユーザに対するアドバイス／コンサルティングの提供
- 暗号製品開発
- 政府向け暗号製品／システムの評価・提供
- 産業界との連携
- トレーニングコースの運用
- ITSEC（Information Technology Security Evaluation Criteria）の運営

また、重要インフラ保護のために、以下の 2 つの組織を設立している。これらの組織は、米国における NIPC や CIAO と同様の役割を担っている。

a) NISCC（National Infrastructure Security Coordinating Centre）
b) IAAC（Information Assurance Advisory Council）

a) NISCC

NISCC は、1999 年、英国海外情報部（MI5）及び中央情報局（GCHQ）により設立された組織で、米国の NIPC と同様の役割を担っている。サイバー犯罪の技術捜査、重要イ

ンフラの脆弱性に関する分析、警察への情報提供などを主な業務としている。民間部門に対しては、セキュリティ警告や情報セキュリティ対策関連情報などを提供している。

b) IAAC

IAAC は、2000 年に、産官学からの資金提供を受けて設立された、ロンドン大学キングスカレッジ内に本部を置く非政府機関であり、官民が協力してセキュリティポリシの作成にあたっている。米国の CIAO と同様の役割を担っており、脅威のアセスメントと早期警告、リスク及び影響分析、セキュリティ基準／ガイドラインの設定、教育等の業務を行っている。

(2) 認証制度

英国では、情報システムのセキュリティや安全な電子商取引のために、以下の認証制度を定めている。

① BS7799
② ITSEC
③ TrustUK

a) BS7799

BS7799 は、1995 年に初めて発行された情報セキュリティ管理に対する標準規格である。1999 年夏に BSI によって新たに出版された BS7799 は二部に分かれており、電子商取引やモバイル･コンピューティング、アウトソーシングなどに関する規定が新たに追加されている。

- BS 7799-1: 1999 Code of practice for information security management
  第一部は、組織の中で情報セキュリティの開発、導入、維持に関わる担当者のための参考文献として発行された。
- BS 7799-2: 1999 Specification for information security management systems
  第二部では、情報セキュリティ管理システム(ISMS)の構築、導入、文書化の要件を規定。組織が現行の ISMS に対してリスク評価を行い、その結果としてどのようなセキュリティ･コントロールが導入されるべきかを規定し。ISMS 評価のベース、BS7799 取得審査時のクライテリアとなるものである。

なお、BS7799 は、2000 年 2 月に ISO、IEC として採択されている。

b) ITSEC

ITSEC には、コンピューター・セキュリティ侵害のモニター、テスティング手法及び技

術の維持、個々の評価テストのモニター、評価の結果決定する保証レベルの認証が含まれている。実際の評価テストは、認証機関によって指名された第三者機関 CLEFs29 に委託される。CLEFs として承認されるためには、現在、英国内で第三者機関として認定されているのは、Admiral Management Services Ltd.、EDS Ltd.、Logica UK Ltd.、Syntegra、IBM Global Services の 5 社である。

ITSEC の評価後の保証レベルは E1 から E6 まであり、数字が大きい方がレベルが高いことになる。

なお、ITSEC は、政府機関の通信電子セキュリティグループ（CESG）及び DTI によって共同で行われており、日常の運営は、CESG の職員を配置した認証機関(CB28)が行っている。

c) TrustUK

オンライン・ショッピングを促進する目的で、質の低い顧客サービスや電子商取引における不正行為対策として、ウェブサイトの安全認証マーク制度が 2000 年 1 月に発表された。この認証制度は、新たな法規制に頼らず、業界自主規制によって安全な電子商取引を促進しようとする動きの一つである。

同スキームでは、業界団体が顧客のプライバシー保護、安全な決済方法、返品、価格設定、苦情処理、児童向けのマーケティング、既存の法規制遵守などの基準を規定し、TrustUK がその規定を審査のうえ認定する。各団体に属するメンバー企業は、ウェブ上で小売販売を行う際に TrustUK マークを使用できるが、その規定を遵守する義務を負い、団体側がこれを監視する。同スキームの認証取得のために業界団体にかかるコスト、はメンバー数によって年間 1,000 ポンドから 5,000 ポンドとなる。

(3) 法制度

a) コンピュータ不正使用法

1990 年に制定されたコンピュータ不正使用法は、不正アクセスやコンピュータウィルスを含んだ、サイバー犯罪に対応する包括的な法律であり、被害国も犯人の国籍も、英国である必要なく処罰できるものとなっている。例えば、コンピュータデータもしくはプログラムの権限によらない改変を犯罪とし、それに対して 5 年以下の拘禁刑もしくは無制限の罰金が課されることになる。

b) 電子商取引に関する法律

英国では、1997 年に「信頼できる第三者機関の許可に関する協議」に着手し、ここでの法令策定作業を経て、2000 年 5 月に「電子通信法」が国内法として制定された。同法では産業界側の自主的な「自己規制許可」制度を設けることにより、最低限の品質・サービス基準の確保を目指しており、5 年間でこの制度が実効力を持てば、政府としての法制度

は構築しないとしている。

3 情報セキュリティ対策上の課題

3.1 重要インフラ防護の現状と課題

本項においては、我が国の重要インフラをサイバーテロ等から防護するための体制を明らかにするとともに、英国及び米国における重要インフラ防護体制との比較の下に、いかなる課題が存在するのかについて考察することとする。

3.1.1 我が国、英国及び米国における重要インフラ防護体制の現状

(1) 我が国における重要インフラ防護体制

我が国においては、「重要インフラのサイバーテロ対策に係る特別行動計画」（平成12年12月15日 情報セキュリティ対策推進会議決定）及び「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」（2001年10月10日 情報セキュリティ対策推進会議決定）に基づき、電子政府等に対するサイバー攻撃などの事案が発生し、又は発生する恐れのある場合において、政府として緊急に執るべき措置に関する検討及び各省庁への助言等を行うために、政府の組織として2002年４月１日に内閣官房情報セキュリティ対策推進室にNIRT（National Incident Response Team）が設置された。

NIRTは、サイバー攻撃等による電子政府に係る障害の発生又はその恐れがある事案及びその他政府として危機管理対応が必要となる情報セキュリティに係る事案が発生した場合に、各省庁等の行う措置に関する助言、指導、調整等を実施することとされており、その活動の対象となる機関には、国の行政機関のほか、民間重要インフラ事業者等も含まれている。

また、重要インフラの一つである電気通信分野においては、昨年７月にTelecom-ISAC Japanが設立され、本年３月末からサービス提供が開始されている。

(2) 英国における重要インフラ防護体制

英国においては、政府部内にUNIRAS（Unified Incident Response and Alert Scheme）が設置され、政府機関を対象としたインシデント対応活動と民間重要インフラを対象としたインシデント対応活動の双方を実施している。

UNIRASは、政府機関及び政府重要情報を取り扱う取引先民間企業を対象としたインシデント対応組織として、1992年に内務省に設置された。英国内の重要インフラ保護のため、各重要インフラ関連企業と政府機関、政府機関内の連携強化を目的とする省庁横断型機関として、1999年にNISCC（National Infrastructure Security Coordination Center）

が設置されると、これを機に、UNIRAS は NISCC の一部に吸収され、活動の対象を政府機関等から重要インフラ関連組織全般に広げ、現在に至っている。

NISCC は、重要インフラ関連企業との関係構築・連携強化を目的にセキュリティ関連製品の紹介やセキュリティ専門家の派遣、セキュリティ関連情報の提供などを行い、UNIRAS は、インシデント対応を行っている。

英国においては、国民に不可欠な主要サービスを保護するため、基盤となるネットワークシステムを提供・管理する重要インフラ関連企業と政府との協働連携を推進する施策として、1999 年に内務省により「重要インフラ防護プログラム（Critical National Infrastructure Protection Program）」が策定された。同プログラムにおいては、８つの産業分野（通信、金融、上下水道、エネルギー、運輸、医療、中央省庁、緊急サービス）を重要インフラとして指定し、NISCC が関連企業との連携、UNIRAS がインシデント対応を実施することとしている。

同プログラムは、UNIRAS のインシデント対応時における他の政府機関等との連携についても規定している。具体的には、CESG（Communications-Electronics Security Group：英国政府における情報セキュリティ技術機関）からの技術支援、MI5 や国防省との情報共有、DSTL からの技術支援及び技術者等の派遣、被害の大きなインシデント対応時における NISCC 内の EARG（Electronic Attack Response Group）との協働、NISCC 関連組織との情報共有などであり、重要インフラ保護についての、UNIRAS を中心とした政府部内の連携体制が明確にされている。

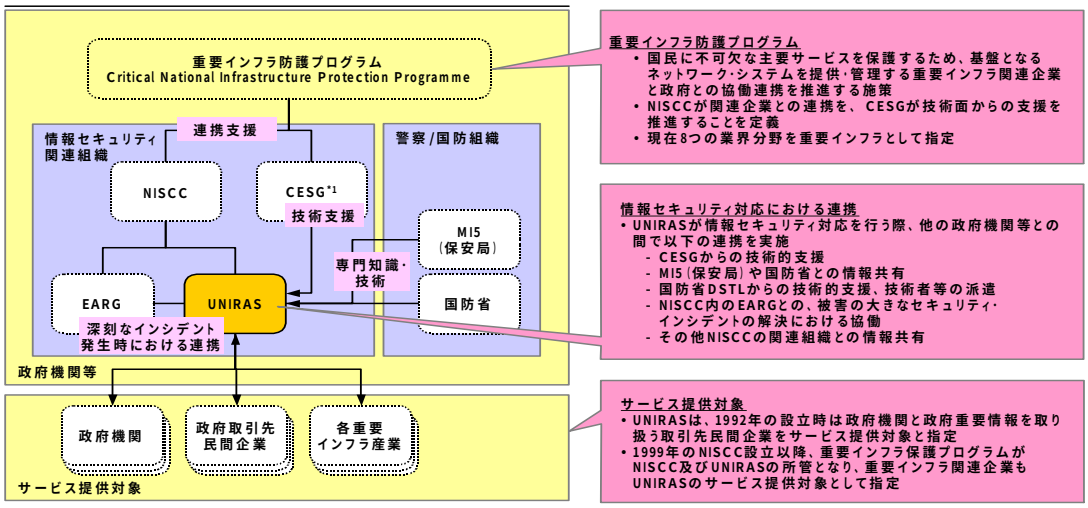


図3-1-1　UNIRASを中心とした重要インフラ防護に関する連携関係

(3) 米国における重要インフラ防護体制

米国における重要インフラ防護のため体制としては、インシデント情報を同一業界内で分析・共有するための組織として、民間の重要インフラ業界ごとに ISAC（Information Sharing and Analysis Center）が設置されている。

1996 年、米国のクリントン前大統領は、大統領令 13010 号（Executive Order 13010）により、PCCIP（President's Commission on Critical Infrastructure Protection：大統領重要インフラ防護委員会）を設置し、今後の重要インフラ防護戦略の立案を指示した。翌 1997 年、PCCIP は、その検討結果を"Critical Foundations：Protecting America's Infrastructures" としてとりまとめ、クリントン前大統領は、これを受けて、PDD63（President Decision Directive 63：大統領決定指示 63 号）を発令し、重要インフラ保護のための課題とそれに取り組むための実施体制を明らかにした。

ISAC は、PDD63 において、重要インフラ関連産業に対して、設立が要請されたものである。さらに、2000 年に公表された「情報システム防護のための国家計画<第１版>（National Plan for Information Systems Protection version1.0)」において、ISAC 未設立の業界に対する設立の促進及び官民連携プロセスの構築が要請された。

米国においては、現在までに、Telecom ISAC（通信業界)、IT-ISAC（IT 業界)、FS/ISAC（金融業界)、Electric Power ISAC（電力業界）をはじめとして１０以上の重要インフラ業界において ISAC が設置されている。

インシデントには、業界毎にそれぞれ一定の傾向がある場合が多いことから、インシデント対応に関して、業界毎に各企業が協力することは非常に有益であり、ISAC は、この点に着目して、特定の業界に属する企業において発生したインシデントに関する情報を収集・分析し、その結果を業界内で共有することを主たる業務としている。

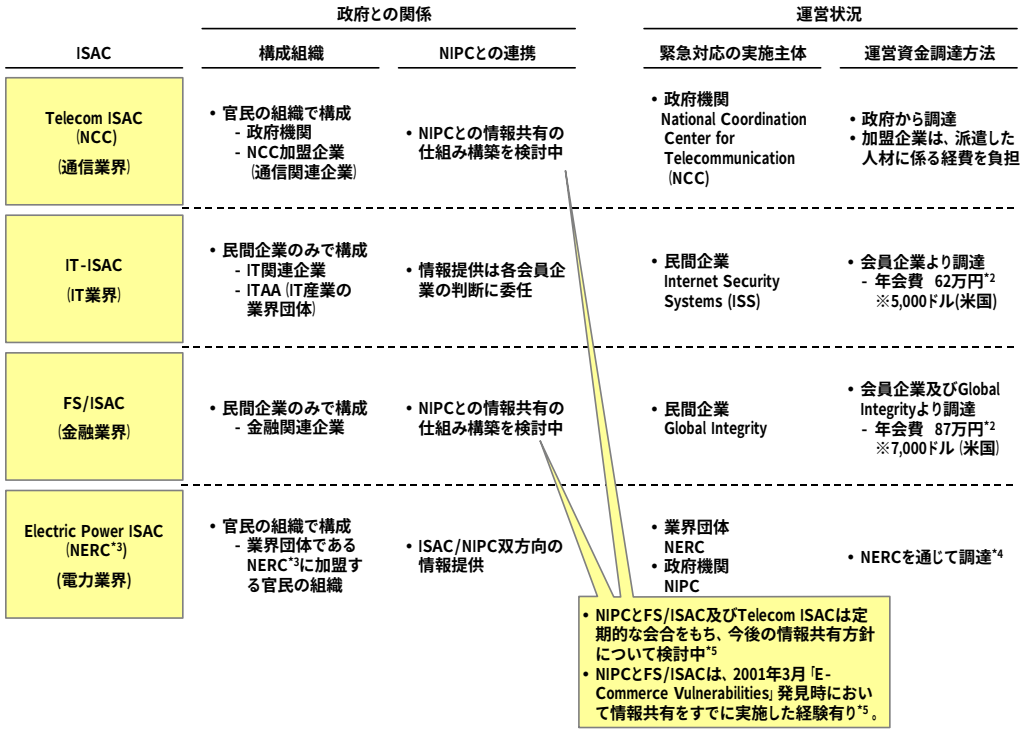


図 3.1-2 米国における各 ISAC の活動

3.1.2 我が国における重要インフラ防護体制の課題

前項において、我が国、英国及び米国における重要インフラ防護体制について概観したが、英国と米国の体制を比較した場合、双方は明確な対照をなしている。英国では、政府機関及び重要インフラ産業全般を対象としたインシデント対応については、政府部内に設けられた UNIRAS が一元的に対応している。一方で、米国では、重要インフラ産業毎に ISAC を設立し、それぞれが連携を図りつつ独自に活動するという、いわば分散型の対応により、業界毎のインシデント情報の共有と連携の強化を図るとともに、FBI（米国連邦捜査局）内に設置された NIPC（National Infrastructure Protection Center：国家インフラ防護センター）と各 ISAC との間の情報共有を求めることにより、政府と重要インフラ産業との間の連携を図っている。

我が国においては、NIRT が政府機関及び民間重要インフラ事業者等（情報通信、金融、航空、鉄道、電力、ガス、地方公共団体）の双方を対象とするインシデント対応組織として政府に設置されており、UNIRAS が政府機関・重要インフラについて一元的にインシデント対応を行う英国の体制と似ている。しかしながら、NIRT は、重要インフ

ラ事業者に対し情報提供・助言等の活動を行う場合は、原則としてこれを所管する省庁を通じて対応することとされ、直接支援等を行う場合には、事業者からの支援要請があり、かつ、これを所管する省庁の同意がある場合に限られるなど、NIRT が第一義的に重要インフラ事業者のインシデント対応を実施する仕組みにはなっておらず、我が国の体制と英国の体制を同一視することはできない。
他方で、「サイバーテロ対策に係る官民の連絡・連携体制について」においては、「各重要インフラ分野内における情報共有及び検討体制については、事業者間で共通する課題がある場合など、情報共有等が有効な場合に業界団体を中心として行うこととする」とされ、重要インフラ業界に対し、必要に応じて、業界としてのインシデント対応のための取り組みが求められている。

したがって、我が国における重要インフラ産業における情報セキュリティの確保は、NIRT による活動と重要インフラ業界において必要に応じて実施する取り組みの双方が相俟って図られることが基本となっていると考えられる。
その意味では、我が国における体制は、その制度設計の基本的な考え方においては、むしろ米国における分散型の体制に近いものと考えられる。

しかしながら、我が国の重要インフラ分野におけるインシデント対応体制の整備レベルは、業界としての取り組みが未だ情報連絡等にとどまっており、ISAC の設立が電気通信業界のみに止まっている現状においては、我が国の体制は、英米に比べて脆弱であると言える。したがって、電気通信業界以外の重要インフラ業界においても、ISAC をはじめとする業界としてのインシデント対応体制が一日も早く整備されることが望まれるところである。

また、既に設立されている Telecom-ISAC Japan についても、現状の提供サービスは、脆弱性データベースとアラートサービスのみであり、インシデント情報を収集・分析して業界内でこれを共有するという ISAC 本来の取り組みは未だ準備段階である。サイバーテロ対策における情報通信インフラ防護の重要性に鑑みれば、Telecom-ISAC Japan の取り組みの加速・強化は喫緊の課題である。

3.2 高度化・多様化する攻撃手法への対応

3.2.1 現状

インターネットを一部の学術機関や企業の研究開発機関といった、限られた場所で限られた人々が利用していた 1990 年代前半においては、クライアントやサーバは直接インターネットに接続されていることが多く、現在ほどセキュリティを考慮する必要性がなかった。しかし、インターネットが本格的に普及し始めた 1990 年代後半、利用者層が広がるにつれて従来の限られた人々のみが利用しているネットワークではなくなり、それまでには無かった悪意をもったアクセスを考慮せざるを得なくなったため、セキュリティ対策を講じる必要性が徐々に高まってきた。

1990 年代前半においては、クライアント、サーバ共にグローバルアドレスを持ち、telnet や ftp、finger といったプロトコルが開放されていることが普通であった。ゆえに現在のように高度な不正アクセスが行われるといったことはまれで、アカウントを調査してパスワードを推測しログインするといったような比較的原始的かつ直接的な侵入が行われるといったことが多かった。

そこで、セキュリティ対策としてクローズアップされたのがファイアウォール技術に代表されるセキュリティ技術であった。ネットワークを通信層の高いところ（セッション層以上）で分断し、アクセス制御やログ機能、アドレス変換機能等を備え、限られた通信のみを中継するという機能が実装され、インターネットとの接続性を維持したまま安全性を向上することが可能となった。

また、クライアントに目を向けると、クライアントを狙ったウィルスも数多く登場し、無防備なクライアントが次々とウィルス感染した。当時はダウンロードしたファイルを実行することによって感染するといった形態が多く、ウィルスを駆除するためにウィルス除去ソフトが開発され、クライアントでのセキュリティ対策として現在では一般的に行われるようになってきている。

ファイアウォールに代表されるようなアクセス制御が一般的に行われるようになり、ウィルス除去ソフトの導入が進むにつれ、直接かつ単純な不正アクセスやサイバー攻撃を行うことができる環境が減少していったため、不正アクセス・サイバー攻撃の手法は次第に高度化し、多様化してきているのが現状である。

(1) 不正アクセス手法の現状

a) rootkit

サーバに不正侵入を行った場合、通常は何らかの痕跡がサーバ上に残るため、不正侵入者はできる限りその痕跡を隠蔽しようとする。その隠蔽を行う手段として比較的よく利用

されるのが rootkit と呼ばれるプログラム群である。これらは侵入調査を行うためのコマンドを置き換えてバックドアプログラムの存在を隠蔽したり、不正侵入に関する部分のシステムログを自動消去したりするといったことが簡単にできるようになっている。これらのツールも年々進化しており、ローダブルカーネルモジュールを使った rootkit が登場している。この rootkit はコマンドを置き換えることなくファイルやプロセスの隠蔽を可能にすることができるため、侵入されていることすら分からないという非常に危険性の高いものとなっている。また、攻撃元と攻撃対象との間を ssh を使い通信経路を暗号化することによって、通信内容を知られなくするといった手法をとることもあり、その発見は次第に困難となってきている。

b) Web アプリケーションを狙ったセキュリティ・ホール攻撃

インターネットが爆発的に普及した原因として WWW は大きな役割を果たして来た。WWW はプログラムを実行するための CGI というインターフェースを持っており、フォームを使ってユーザから情報を入力させたり、情報を得たり、掲示板といったインタラクティブなシステムには欠かせない機能となっている。その他にも、通信のたびにセッションが切れるという HTTP の特性を回避するために、利用者の端末にセッション情報等を保存する HTTP Cookie といった技術も数多く使用されている。これらはそれぞれの機能が HTTP というプロトコル上のデータとして処理されているため、基本的にはファイアウォール上で内容のチェックはされず、直接的にクライアントサーバ間でデータのやり取りが行われている。このデータを不正に操作することで、Web サーバに誤動作を行わせることができればファイアウォールのアクセス制御をすり抜けることができるために、最近では Web アプリケーションを攻撃するという手法が盛んに行われている。以下に代表的な Web アプリケーションへの攻撃例をあげる。

① Session Hijack

Web アプリケーションでは画面遷移を行うために何らかのセッション情報をデータとして引き回している。一般的にはランダムな URL パラメータ、もしくは HTTP Cookie にセッション情報を保持させるのであるが、そのセッション情報が盗まれてしまった場合に実際の利用者以外の人間がそのセッションを横取りすることができる。これは利用者本人に成りすましが可能なため、個人情報の搾取やショッピング等も本人が行ったかのようにできる。

② SQL Injection

Web アプリケーションとデータベースが連携している場合、ユーザの入力値に従って、何らかのデータベースへの問い合わせが発生しているはずである。例えばログイン情報がデータベースに格納されているとすると、ユーザ名とパ

スワードの入った SQL クエリが発行されているはずである。ここで、入力パラメータに不正な文字列を入れることでアプリケーションの誤動作を引き起こし、任意の SQL 文を実行させることが可能な場合がある。こういった SQL 文の不正挿入を SQL Injection と言う。上記の例でいえば、任意の SQL 文が発行できれば、ユーザ名とパスワードを全て入手することができるなど、大きなセキュリティ・ホールとなり得る。これらは HTTP のプロトコル上では正常利用のためにファイアウォールでは防御が出来ない。

③ OS Command Injection

上記の SQL Injection と類似するが、こちらはユーザからの可変引数に OS のコマンドを入れ込むことで OS のコマンドを実行させてしまう攻撃である。こちらも HTTP プロトコルとしては正常なために、ファイアウォールでは検出が出来ない。また、コマンドが実行されたことが通常の Web サーバのログに残らないために、何かをやられたことに気づくことすら難しいといったことも充分考えられる。

④ Cross Site Scripting

Web アプリケーションの入力チェックが正しく行われていないことを利用し、サイトをまたがってスクリプト等を実行させることで Web ページを偽造したり cookie を盗み取ることのできる攻撃方法である。HTTP Cookie にセッション情報やアカウント情報が含まれている場合、前述のセッションハイジャック等が可能となるためにさらに危険な攻撃に繋がる可能性がある。なお、本攻撃については攻撃そのものもさることながら風評被害についても無視できないものとなっている。

上記の攻撃手法は、いずれも Web アプリケーションがパラメータのチェックを行っていないために起きる問題であるが、ファイアウォールを通り抜けて直接内部のマシンを操作できてしまうところにこの攻撃の危険性の高さがあると言える。

(2) サイバー攻撃手法の現状

a) DoS/DDoS 攻撃

インターネット上に存在するサイトに対して、大量にデータを送りつけたり、不正なパケットやデータを送りつけて継続してサービスを提供出来なくするような攻撃をサービス不能攻撃という。このような攻撃は以前より存在していたが、TFN や Stacheldraht 等に代表される DDoS(Distributed Denial of Service:分散型サービス不能攻撃)と呼ばれる攻撃も盛んに行われている。これは、すでに知られているセキュリティ・ホールを利用しサーバやクラ

イアントに不正侵入を行い、バックドアプログラムを仕掛けてそれらの端末を踏台とし、リモートコントロールを行う仕組みになっている。その上で攻撃対象に向かって各端末から大量のトラフィックを発生させることでネットワーク帯域を消費し、サービスの継続を出来なくする攻撃である。実際に Yahoo!、eBay といった有名なサイトがこの攻撃を受け、サービス継続ができなくなるという妨害行為をうけた。これらの攻撃は明らかに悪意を持ったものが攻撃のきっかけをもっているが、実際に攻撃を行っているそれぞれのデバイスは不正侵入を受けた機器であり、その点では被害者である。しかし、最終的な攻撃目標からすれば、それらは加害者でもある。この攻撃は被害者になりうると同時に加害者になりうるという危険性を持っている攻撃である。また、こういった攻撃の場合、送信元アドレスが偽装されることが多く、そもそもの攻撃元が判明しないことが往々にしてありうるために追跡が困難なことが多い。

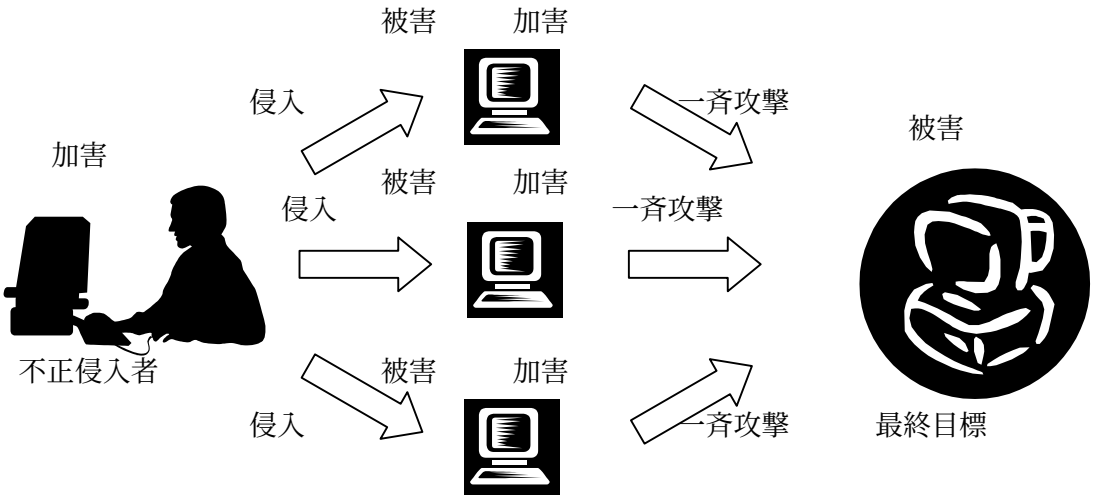


図 3.2-1 DDoS **攻撃**

b) **高度化するウィルス**

現在、ウィルスは非常に多様化しており、感染手法も高度化の一途をたどっている。感染した場合のインパクトは従来とは比較にならないくらい大きなものとなっているのも現在のウィルスの特徴である。古いウィルスが感染した端末そのものに攻撃を行うのに対し、CodeRed **や** Nimda **に代表される現在のウィルスは以下のような特徴を持っており、危険性が非常に高くなっている。**

⑤ WW **ブラウザやメールクライアントといったソフトウェアのセキュリティ・ホール、バッファ・オーバフローといったセキュリティ・ホールを利用する。**

⑥ **ネットワークを積極的に利用し爆発的な攻撃力、感染力を持つ。**

⑦ **メール等を使い、通常のメールを偽装して受信した人を欺き操作させるとい**

った巧妙な手口が利用される。

⑧ 一般ユーザが被害者ではなく、知らぬ間に加害者となる可能性がある。

⑨ 輻輳が原因でネットワークが利用できなくなる。

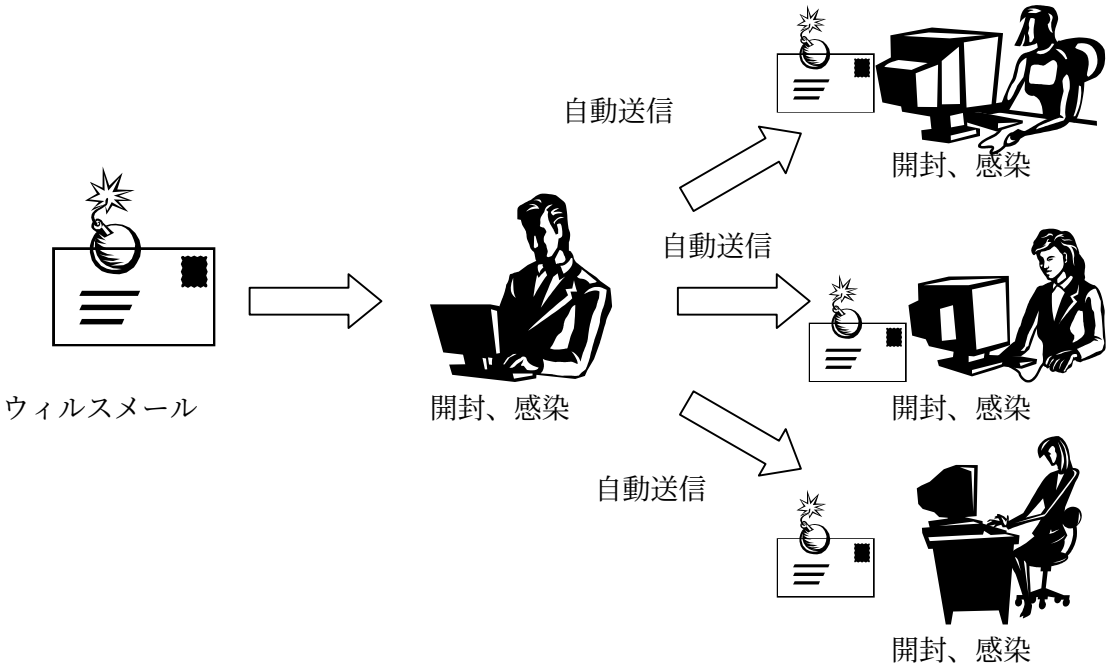


図 3.2-2 **ネットワークを使ったウィルス感染**

c) **スパム**

必要が無いのにも関わらず勝手に送られてくる広告メールを一般的にスパム・メールと呼んでいるが、これらについても手段の多様化が進んでいる。大量にメールを配信するために、オープンリレー状態のメールサーバを常時探索している。スパム・メール送信者はインターネットに繋がっているマシンを広域的に探索しており、オープンリレーのサーバを非常に早く見つけ出す。リレーサーバが見つかった場合はそこを踏み台としてメールの送信を行うが、リレー方法についても年々様々な手法が開発されている。最近ではオープンリレーのメールサーバのみならず、HTTP のオープンプロキシを使用してスパム送信を行うといったことも数多く行われるようになってきている。このことによって、インターネット回線の不必要な帯域消費を引き起こすばかりでなく、送信メールアドレスを偽り、到達不可能なメールアドレスに向けて大量メール送信を行うことでエラーメールがリレーサーバに滞留し、サーバダウンを引き起こすなど、重要なインフラ障害を引き起こすことが充分起こり得る現状となっている。

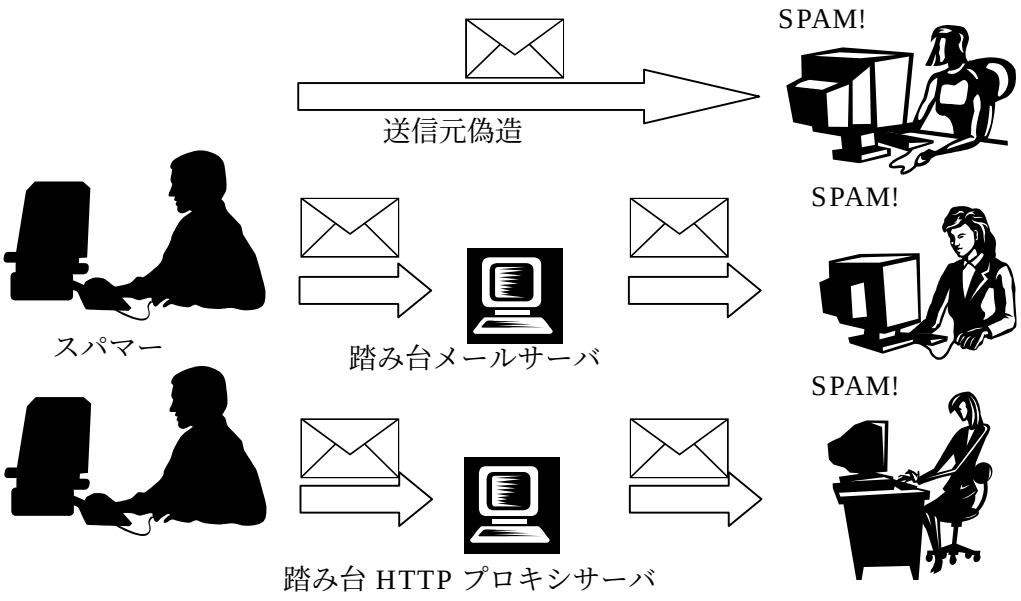


図 3.2-3 SPAM **の特徴**

3.2.2 **対応**

前述のとおり、新しい攻撃手法は続々と開発されつづけており、サイバーテロに利用された場合は甚大な被害を及ぼす。そのために充分な対策を行う必要があるが、決め手となる有効な対策が存在しないのが現状である。そこで、以下に現状可能であり、行われている対策と問題点を列挙する。

(1) **不正アクセスへの対策**

a) rootkit **対策**

rootkit **を検出するソフトウェアが配布されており、それらを利用すればいくらかの検出は可能であるが、全ての** rootkit **に対応していないために完全な対策とはいえない。また、カーネルローダブルモジュールを使った** rootkit **を埋め込まれた場合は、コマンドを入れ替えると言う方法ではなく、メモリを直接操作し、例えばディレクトリ情報の書き換えやプロセス情報の書き換えが行われるため、コマンドのバイナリファイルが正しいからといって実行結果が正しいとは限らない。その場合は** rootkit **の検出自体が非常に困難であり、不正侵入を受けているかどうかすらわからない場合がある。**

b) Web **アプリケーション対策**

CGI プログラム等の Web アプリケーションに入力される変数値に対しての入力チェックや無害化（サニタイジング）が行われれば本脆弱性の多くは防御できる。しかし、現実的に全ての Web アプリケーションに対して漏れなく上記対策を行うことは困難であるため、Web アプリケーションを中継し、HTTP ヘッダだけでなく HTML 上のデータ部分も含めてチェックする Web アプリケーション専用ファイアウォールも商品化されている。しかし、全ての攻撃が防げるわけではなく、また検出パターンの設定が困難であったり、個人ユーザが購入できる価格に無いなど、現時点で全ての一般ユーザまでふくめての有効な解決策であるとは言い難い。

(2) サイバー攻撃への対策

a) DoS/DDoS 対策

今のところ、DoS/DDoS に対する決定的な対策はない。現在考えうる対策としては QoS 装置の導入や DoS/DDoS と判断した場合にパケットを高速に破棄する装置の導入を行うということが考えられる。QoS 装置は TCP コネクションのパケット送信時間やウィンドウサイズを調整することにより、エンド to エンドでの通信速度を操作するものである。しかし、機器の価格が総じて高価であり、企業ユーザであれば導入可能であるが、個人ユーザが導入することは不可能である。さらに DoS/DDoS を検出する機能を持つ負荷分散装置等も存在するが、QoS と同様に個人ユーザが使用できるものではない。接続 ISP で ingress filter といった、送信元からの通信を遮断してもらうといった対処方法も可能であるが、ISP は多くのユーザを集約して装置に収容しているため、簡単にできるものではない。インターネットの特性上、ネットワークの輻輳を起こすことはそれほど難しくないため、利用者側で回避のしようが無いのが現実である。

b) ウィルス対策

ウィルス対策としてはクライアントに導入するウィルス除去ソフトがあげられるが、メール中継サーバに導入するサーバ型のソフトも利用されている。ウィルス除去ソフトは基本的にウィルス検出用のパターンを持っており、メールの添付ファイルや Web からダウンロードした圧縮ファイルなどを自動で展開し、ウィルスパターンと照合する。ウィルスが発見された場合は自動的にウィルスを除去することが可能であるが、パターンの更新が行われなければ、新しいウィルスには対応できず、常に最新のウィルスパターンを使用しなければならない。よって、運用が正しく行われていなければウィルスからの防御は困難である。また、実際のウィルスの流行とパターン作成、配布に時間差が生じるため、ごく短時間で感染するようなウィルスの場合はパターン更新が間に合わないといったこともあり、その場合は防御が不可能である。ウィルス対策についてはウィルス除去ソフトを利用者がインストールするかどうかは利用者の判断に任されており、利用者の端末まで含めて安全を確保することを考えると現状では完全な対策は困難であるといえる。

c) SPAM 対策

インターネットで使用されているメールプロトコルの特性として、発信者を偽造することが可能であること、ネットワーク側で送信の制限が困難であることから、こちらも今のところ決定的な対策がない。現在ある対策としては、パターン認識技術を利用し、SPAM と思われるキーワードを持ったメールを自動的に振り分けるソフトウェアを利用するというもの、また、不正な第三者中継ができてしまうサーバをブラックリストとして提供するサービスを使用し、そのようなサーバからのメールは受信しないといったことも可能であるが、それらは必要なメールについても拒否されてしまう可能性があるため、運用が困難である。

上記のように不正アクセス手法、サイバー攻撃手法のいくつかには、個別の対策は存在するが、それが充分であるかと言えばまだまだと言わざるを得ないのが現状である。

3.3 インターネット自体に内在する脆弱性への対応

3.3.1 プロトコルの脆弱性

(1) ルーティングプロトコルの脆弱性

a) データパケットと制御パケットの回線非分離

インターネットで使用される経路情報をやり取りするプロトコルをルーティングプロトコルという。このルーティングプロトコルで使用される制御パケットは、データパケットと同一の回線を通る。これはインターネット技術の大きな特徴である。そのため、データパケットの量が非常に多く回線が輻輳している場合には、制御パケットの伝送が阻害され、ルータに対して経路情報が送れなくなり、制御不能という事態が発生する可能性がある。

また、データパケットと制御パケットに区別が無いことは、一般ユーザでも制御パケットをルータに対して送信できるということを意味している。これはセキュリティ的に危険な状態である。

こういった問題の対策として制御用に別の回線を使用することも考えられるが、費用の面でも設定の面でも不可能に近い。制御情報を別回線でやり取りするプロトコルも開発されてはいるものの、当面は現状のプロトコルが使用されると考えられる。

b) 貧弱な authentication(認証) 機能

インターネットを形成する組織間においては、相互に保持している経路情報を交換するために、BGP (Border Gateway Protocol) というルーティングプロトコルが使用される。

ある組織が別の組織と経路情報のやり取りを行うためには、それぞれの組織のルータが BGP ピアという関係になる必要がある。現在では簡易な認証機能が実装されてはいるものの、歴史的背景・運用の煩雑さ・効果への疑問、等の理由から、実際には使用されることは少ない。

認証機能を使用しないことによって、BGP ピアの成りすまし等の事件が考えられる。幸いにしてこの種の事件は今のところ発生して無いが、潜在的に危険性を含んでいるといえる。

こういった問題の対策として、IPsec や PKI を用い、認証と完全性を保障する Secure BGP という方法も検討されている。

また、組織内における経路情報の伝播には OSPF (Open Shortest Path First) というプロトコルが使用される。OSPF についても簡易な認証機構が用意されているものの、BGP と同様の理由で通常は使用されていない。経路情報が組織内で閉じているとはいえ、危険な状態である。

c) authorization(認可) 機能の欠落

BGP では、ピア相手に対して authorization(認可) の機能がない。そのため、相手から広報された経路情報については、基本的にはすべて受け入れる。つまり経路情報の正当性は保障されず、間違った経路情報でも受け入れてしまう。

例えば組織 A が誤って組織 B の経路情報をインターネットに広報すると、誤った経路情報が世界中に伝播することになる。その結果として、組織 B 宛のパケットが、間違った経路の広報をした組織 A に吸い込まれるという危険が考えられる。実際にこの種の事例はたびたび発生している。

こういった問題の対策として、受け取った経路情報について IP アドレスの割り当て情報を用いて正当性を確認する方法も検討されている。

d) 不安定な経路情報

通常、経路情報はネットワークに変化があったときのみ広報されるが、設定ミスや機械の不具合等により、不安定な経路情報が断続的にインターネットに広報されることがある。これを経路のフラップという。不安定な経路情報は全世界に波及し、これを受け

取ったルータは CPU 能力やメモリを消費するため動作に悪影響がある。運用技術者はこの影響が自組織に波及しないように、フィルタを設定してブロックしている。

3.3.2 DNS(Domain Name System)の脆弱性

(1) ルートサーバ(root servers)

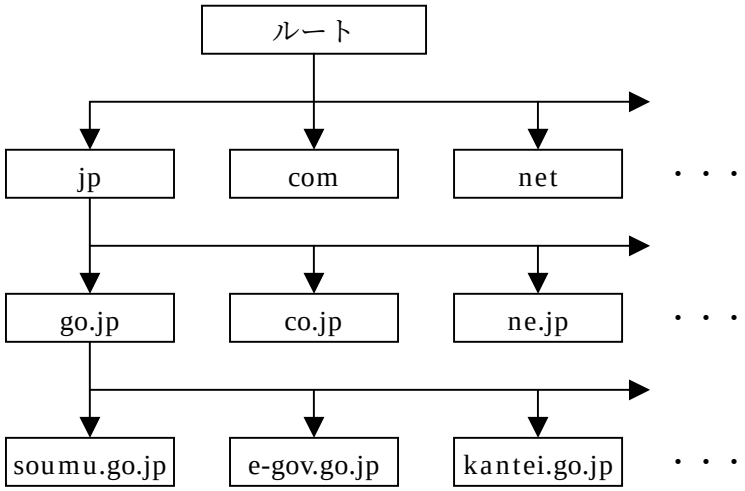
① DNS の役割

一般にインターネットの利用者は、好きなサーバにアクセスするために、アクセスしたいサーバのドメイン名を含むホスト名をクライアントで指定する。

例えば、総務省の Web サーバにアクセスするためには、”www.soumu.go.jp”または”総務省.jp”を Web ブラウザで指定する。総務省が提供する情報を Web ブラウザが画面に表示するためには、総務省の Web サーバと通信しなければならないが、通信するためには”www.soumu.go.jp”または総務省.jp”というホスト名から総務省の Web サーバの IP アドレスを調べなければならない。別のホストと通信するためには、そのホストの IP アドレスを知る必要があるためである。

② DNS の仕組み

クライアントが DNS を利用するためには、DNS サーバの IP アドレスを少なくとも 1 つは知っている必要がある。その DNS サーバが世界中のあらゆるホスト名の IP アドレスを知っているわけではないが、DNS は図 3.3-1 のように世界中の DNS サーバが木構造になって構成されており、クライアントが問い合わせた DNS サーバが知らない情報であっても、その DNS サーバが少なくともルートサーバの IP アドレスを知っていれば、世界中のあらゆるドメイン名に関する情報を知ることができるようになっている。



※ 矢印はドメイン名の一部を管理する権限を委任していることを示す

図 3.3-1 木構造の DNS サーバ群

例えば、www.soumu.go.jp の IP アドレスは、以下の手順で調べることができる。

- ルートサーバに、jp を管理する DNS サーバの IP アドレスを問い合わせる。
- jp を管理する DNS サーバに、go.jp を管理する DNS サーバの IP アドレスを問い合わせる。
- go.jp を管理する DNS サーバに、soumu.go.jp を管理する DNS サーバの IP アドレスを問い合わせる。
- soumu.go.jp を管理する DNS サーバに、www.soumu.go.jp の IP アドレスを問い合わせる。

③ ルートサーバの重要性

ルートサーバの IP アドレスを知っていれば、世界中のあらゆるドメイン名に関する情報を知ることができることは前述した。

しかし、機器の故障や不正アクセスなどに起因する障害により、ルートサーバに問い合わせることができなくなったら、アクセスしたいサーバの IP アドレスを利用者自身が知らなければ、どのサーバにもアクセスできなくなってしまう。

④ ルートサーバを対象にした攻撃

現状では 13 台のルートサーバがあるため、すべてのルートサーバに問い合わせることができなくなる可能性は高くない。

しかし、2002 年 10 月には、ルートサーバを対象にした大規模な攻撃があったが、一部の不具合で全体に影響が出ないような DNS の分散型の情報構造により、実害はほとんどなかった。なお、13 台のうち 9 台は一時的にインターネットトラフィックの応答速度低下等の影響を受け､攻撃の影響がなかったルートサーバは 4 台のみであったと、新聞などのマスコミで報道され大きな話題になった。

このときの攻撃では以下の理由により一般の利用者には大きな影響はなかったが、インターネットを利用するために必要不可欠な DNS を対象にした攻撃によって、事実上インターネット全体を麻痺させる可能性があることを世界中に知らしめた。

- 一般の DNS サーバは過去に調べた情報を一定期間は保存しておくため、毎回ルートサーバに問い合わせる必要はない。
- ルートサーバが機能しなかった時間は 1 時間程度であり、一般の DNS サーバが過去に調べた情報を保存しておく期間と比べて長くなかった。
- 機能し続けたルートサーバがあった。

もし、より多くのルートサーバが半日や 1 日といった長時間にわたって機能しなくなったならば、その影響は計り知れない。

このときの攻撃の手法は DDoS（分散型サービス不能攻撃）と呼ばれ、サーバが機能しなくなるように（サービス不能化)、複数のホストから（分散して）一斉に攻撃する手法が使われた。一般に、1 回ごとのアクセスについては悪意を持つ者による不正アクセスかどうかを完全に見極めることはできないため、完全に防御する方法はないと考えられている。

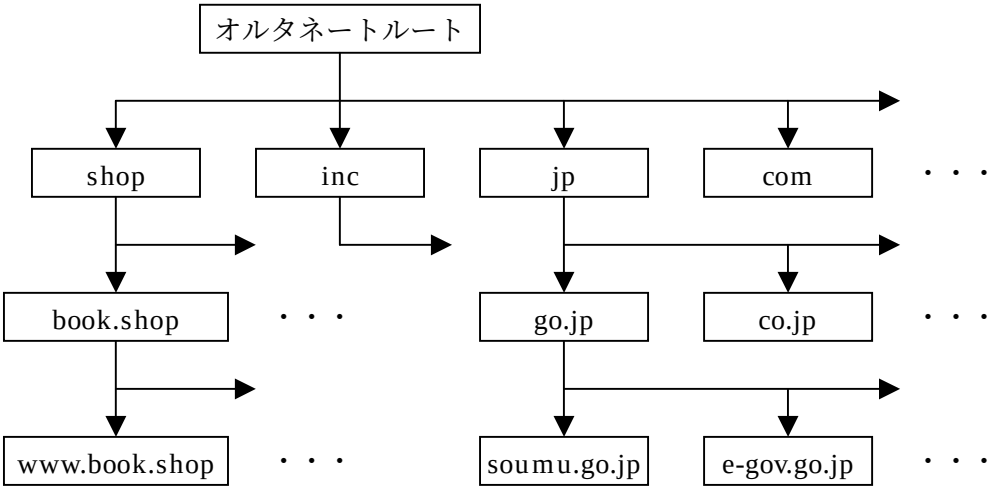
(2) 情報の信頼性

① オルタネートルート(alternate roots)

一般に利用されている DNS のルートサーバは ICANN(http://www.icann.org/)の管理下にある。

しかし、ICANN に管理されずにもっと自由にドメイン名を使うために、ICANN が管理するルートサーバから独立したルートサーバを設置する組織が現れ、オルタネートルートと呼ばれている。

その中には、図 3.3-2 のように ICANN の管理下にある情報も調べられるようになっているルートサーバも存在する。



※ shop や inc などの ICANN の管理下にはないドメイン名が存在する

図 3.3-2 ICANN **の管理下にある木構造とは異なる** DNS **サーバ群**

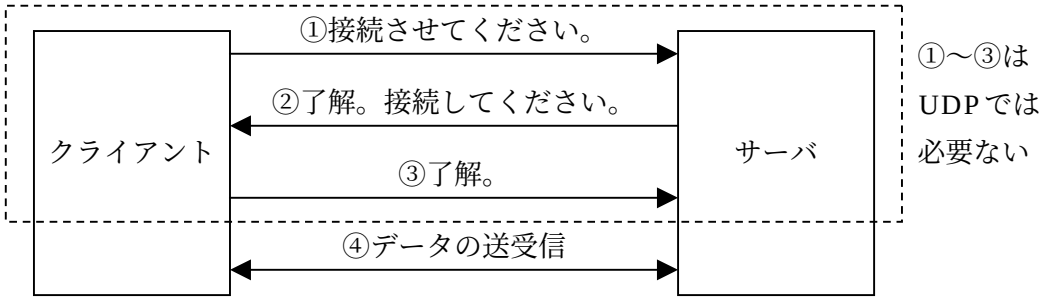
一般の利用者は、インターネット接続業者など、インターネットに接続するサービスを提供する管理者が用意した DNS **サーバを利用する。現在は、それらの** DNS **サーバがオルタネートルートの管理下にある情報を調べられるようになっていることは稀だが、一般に利用されるようになると、利用者が気付かないうちに偽った情報を提供され、利用者が意図しないサーバにアクセスするように誘導される可能性が高まる。**

もし、本物のサーバに似せた偽物のサーバに誘導されると、本物のサーバにアクセスするつもりで送信したパスワードやクレジットカード番号などの重要な情報を、悪意を持つ第三者に知られる危険性などがある。

② DNS **のプロトコル**

クライアントが DNS **サーバに問い合わせるためのプロトコルには一般に高速なレスポンスに適したプロトコルである** UDP(User Datagram Protocol)**が使用されている。**

Web **ブラウザが** Web **サーバにアクセスするために使用される** HTTP(HyperText Transfer Protocol)**では、**TCP(Transmission Control Protocol)**と呼ばれるプロトコルが使用されているが、**TCP **では以下のようにデータの送受信④の前に①～③のような接続の手続きが必要である。**



※ ①～③は TCP にはあるが DNS で使用される UDP にはない手続き

図 3.3-3 TCP でデータを送受信するまでの手続き

TCP では、サーバは、①で知ったクライアントの IP アドレス宛てに②を送信し、再びクライアントから③を受信しない限りデータの送受信を開始しない。

しかし、UDP では①～③のように、コネクションを確立して通信状態を管理したり、誤り訂正のためにパケットを再送するといった通信の信頼性を保証する機能がないため、いきなりデータを送受信する。

そのため、例えば、悪意を持つ者が自分が使用する IP アドレスを偽り、本物のサーバの代わりに不正な結果をクライアントに送信することが容易であり、利用者が意図しないサーバにアクセスするように誘導される可能性が TCP を使用する場合と比べて高い。

DNS の信頼性を向上させる様々な仕組みが考案されているが、それらは普及しておらず、一般の利用者にとって信頼性は向上していない。

(3) 信頼性向上に向けた課題

現状のインターネットでは、通信するために、通信したい相手の IP アドレスか、DNS によって IP アドレスに対応づけられたドメイン名を含むホスト名を知っている必要がある。そのホスト名は IP アドレスと比べれば覚えやすいが、ホスト名を知らない場合は推測するか検索サイトなどのポータルサイトを利用するのが一般的であろう。

総務省の Web サーバ（www.soumu.go.jp）を例にとると、www や go.jp はインターネットでの慣習や規則などを知っていれば容易に推測できるし、soumu は「総務」をローマ字で表記した文字列なので覚えやすい。もし soumu であることを知らなかったとしても、検索サイトで「総務省」と入力すれば、容易に www.soumu.go.jp を見付けることができるだろう。

しかし、推測やポータルサイトの利用によって、必ず通信したい相手と通信できるとは限らない。容易にホスト名を推測できる Web サーバや、ポータルサイトを利用してアクセス

できる Web サーバばかりが、一般の利用者が通信したい相手とは限らない。

推測したホスト名を DNS で見付けられずにアクセスできなかった経験や、ポータルサイトを利用してもアクセスしたいサイトを見付けられなかった経験がある利用者も多いことだろう。

推測したホスト名でアクセスして、まったく期待していなかった別のサイトにアクセスしてしまうこともある。DNS においてホスト名を管理する単位であるドメイン名は、先に申請した者が使用してきた歴史があるため、有名な企業や製品などの名称を、その名称を使用してきた者よりも先に、別の者がドメイン名として申請し使用していることで、利用者が期待していないサイトにアクセスさせられることがある。このようなドメイン名については国境を越えて訴訟になることもあり、新聞などのマスコミで取り上げられることが少なくない。

また、前述したように現状では DNS の信頼性が高くないため、利用者は気付かずに偽の相手と通信する可能性もある。

このような現状は、誰もが安心して利用できるとは言えず、インターネットの積極的な利用を妨げる要因の一つになっている。

現状ではインターネットの用途は Web サイトへのアクセスと電子メールが主流であり、通信の相手が直接個人になることは稀だが、インターネット電話が普及し、移動する個人ともインターネットを介して通話することを考慮するならば、移動に伴って IP アドレスが変化することも考慮しなければならない。ただし、個人が使用する IP アドレスについては、誰もが簡単且つ確実に知ることが可能であり、しかも個人の識別情報として利用することが想定されているため、個人情報の漏洩やプライバシー保護についても十分に考慮し取扱う必要がある。

3.3.3 ネットワーク機器の脆弱性

ネットワーク機器とは、この章では主にルータとスイッチを指す。

ルータの不具合としては次のような例がある。あるルータは、BGP の経路情報に付加されるコミュニティと呼ばれる情報を多数付けた経路を受け取ると動作不能に陥ったり、細かく分割された経路を多数受け取るとメモリを圧迫し不具合を起こしたりすることがある。

また、スイッチについても、たとえばファームウェアの不具合により、ある特定の条件でパケット転送に失敗することがある。

このような機能的な不具合だけでなく、セキュリティ的な脆弱性も存在する。ネットワーク機器はパケット転送以外にもさまざまな付加機能を持つため、そこにセキュリティ・ホールが発生することがある。2002 年 2 月に公にされた SNMP 機能のセキュリティ・ホー