1．論文

インターネット社会の安全性を確保するための国際的取り組みに関する考察

Consideration of International Effort for Security on the Internet

宮田 裕之，土橋 喜
Hiroyuki Miyata,　Konomu Dobashi

愛知大学現代中国学部
Faculty of Modern Chinese Studies Aichi University

目　次

はじめに

情報化社会の発展に伴い，現代社会の基盤を支える多くの分野において，業務の効率性や生産性を向上させるためにコンピュータ・システムが導入されている．一般企業や政府関係などのさまざまな日常的な業務だけでなく，電気・ガス・公共交通機関などの重要なインフラストラクチャにおける運用や維持管理にもコンピュータ・システムは不可欠になっている．先進国をはじめとした多くの国々においてコンピュータ・ネットワークは産業や社会を支える重要な社会基盤であり，故障や操作ミスなどによりこれらのコンピュータ・システムが停止するような異常な事態が発生すると，社会に対してさまざまな影響を与えかねない．

このようなことからコンピュータ・システムの障害は，一旦犯罪に悪用されると人々の社会生活に対して大きな悪影響を及ぼす危険性があることが指摘される．近年ではこれらのコンピュータに依存した情報化社会の弱点を狙い，社会を混乱させようとくわだてるサイバーテロの発生が懸念されはじめている．さらにコンピュータを利用したサイバー戦争を重要な国家戦略として位置づけている国もある．ダン・バートンの著書によれば，アメリカ，ロシア，インド，イスラエルなどでは，サイバー戦争を前提としたデジタル兵器の開発を行っているといわれている[1].

新聞などのメディアによればソフトウェアの欠陥であるセキュリティホールを狙い，官公庁や企業のコンピュータに悪意を持って不正侵入し，データの改竄やシステムを停止させるなどのクラッキングが最近も頻繁に発生しており，実際に企業の業務が停止に追い込まれる事態も起きている[2]．コンピュータに危害を与えるコンピュータウイルスの流布も，年々件数が増加し被害も増加傾向にあり，国際的に深刻な社会問題となっている．このようなコンピュータ犯罪による被害は，経済的に大きな損失を与えるだけでなく，人々が利用する日常の通信を麻痺させるなど，社会を混乱に陥れることがしばしばである．

国家や企業などのコンピュータに不正アクセスを行い，それらの組織に対して何らかの悪影響を与えようとするサイバー攻撃は，ネットワークを使用すれば場所を問わずどこからでも行うことができる特徴を持っている．さらにインターネットでは通信経路が常に一定ではないため，攻撃者を特定することを困難にしている．サイバー攻撃を事前に防ぎ，攻撃者の所在を特定するためには．国内のみならず海外においても幅広い情報収集活動が必要となり，場合によっては多国間で捜査協力を行い，捜査情報を共有する必要もある．

しかし現時点ではサイバーセキュリティ関連の法制度や捜査体制は十分に整備されているとは言いがたく，攻撃者を特定したり摘発したりすることが困難な状況にある．これらのサイバー犯罪の発生を防ぎ，犯罪者を取り締まることを目的とした国際的な法律の制定や捜査機関の設立が急務とされている．

現在多くの国々においてサイバーテロあるいはサイバー攻撃への対策が重要視され，法律・条約の制定や専門の捜査機関の設置がすすめられている．サイバーテロやサイバー攻撃を取り締まる法制度が整備されるなかで，他方ではコンピュータ・ネットワーク上で送受信される情報を監視するシステムが設けられるなど，ネットワーク上で行われる不正な活動を監視しようとする動きもある．だがそれらの監視システムが整備されることによって，本来守られるべき通信の自由と秘密および個人のプライバシーを侵害する危険性も高まることが問題点として指摘されている．

本論は小規模な不正アクセスによるサイバー攻撃だけでなく，被害が広範囲に広がるサイバーテロやサイバー戦争などを防ぐため，情報セキュリティを確立するための国際的な取り組みについてまとめた．さらにサイバーテロの発生を防ぐため，それらを取り締まるために制定された法律や制度についても取り上げ，ネットワーク監視システムなどの弊害や，それらから保護されるべき市民の権利について論じる．

第1章　現代社会とサイバーテロの脅威

1．テロリズムの変化

2001 年 9 月 11 日米国ニューヨークのマンハッタンにある世界貿易センタービルで発生した旅客機突入によるビル崩壊事件以降，テロという言葉が盛んに使われている．この事件以降マスコミの報道や政府の見解などでは，テロという言葉を無差別な殺人を伴う破壊活動を指すものとして使用されることが多くなった．テロまたはテロリズムの本来の意味は，意図的・計画的に不法な手段によって政治的な目的を達成するため，暗殺や暴行などの手段を認める主張であり，またそれに基づいて実際に暴力的な行動を起こすことである．テロの結果として一般市民を巻き添えにしたり，人々に恐怖感を与えることにもなる．米連邦捜査局(FBI)国家インフラストラクチャ保護センター(NIPC: National Infrastructure Protection Center)の報告では，「テロリストの組織は，通常社会の尊厳となる象徴的なターゲットを攻撃する．そうしたシンボルへの攻撃が成功すれば，市民はそれまで安全だと信じていた社会から個人的に切り離され，政府に対して不安感を抱くようになる．このようなテロリストの破壊的な行動によって，市民を守るべきはずの政府の能力に対して，人々が疑問を抱くようになる．このようなときに市民は他者からの影響に最も左右されやすくなる」と指摘している．言い換えれば人々に恐怖心を植え付けることにより，暗殺や暴行などの不法な手段によって，政治的な目的を達成しようとすることがテロリズムの本質的な目的であるといえる[3].

2．サイバーテロとサイバー攻撃

サイバーテロ(cyberterrorism)とは，一般的には国家や社会基盤を混乱させる目的で，コンピュータ・システムへ不正に侵入し，破壊活動を行うことを指す比較的新しい造語である．現代用語の基礎知識には「コンピュータ・ネットワークを通して国防，治安をはじめ通信・交通など，国民生活を支える重要インフラのコンピュータ・システムに侵入し，国家や社会の重要な基盤を機能不全に陥れることを目的としたテロ行為」であると解説されている．

また NIPC の報告には，「コンピュータと通信を悪用することによる犯罪行為であり，各種のサービスを破壊または停止させることにより，特定地域の住民に混乱と不安をもたらし，恐怖を生み出す犯罪行為である」とサイバーテロをより広く定義している[4]．さらにこの定義に付随して，テロリズムは伝統的な物理的破壊行為を意味するものであったが，最近の情報化時代ではサイバーテロの定義について，より実態を反映したものに再定義するべきであると主張している．これまでは政府機関や社会のインフラを担うコンピュータ・システムを破壊したり，緊急通報システム，電話サービス，銀行システム，インターネットなどの重要なサービスを管理するコンピュータ・システムを破壊したりして，市民の社会生活を混乱させるテロリズムなどがサイバーテロの代表と見なされていた．

これに対してサイバー攻撃(cyberattack)は，「インターネット経由で他のコンピュータに不正アクセスを行い，相手の国家や企業にダメージを与えようとする行動のことである．実際に行なう内容は不正アクセスとまったく同じだが，政治的な意図を持って行われる不正アクセスがサイバー攻撃と呼ばれる傾向にある（IT 用語辞典 e-words）」．

サイバー攻撃の手法は多数あるが，その攻撃となる対象により大きく分けて２つのタイプがあるといわれている．ひとつは攻撃したい組織内の特定のサーバーを目標と定め，そのサーバーにダメージを与えて運用を停止させることを目的に，様々な不正アクセスによる攻撃を加える．これはターゲットになる企業や国家などの組織が特定されており，目標とされる組織に対する恨みなどから嫌がらせをするために行われる．あとひとつは目標となるサーバーを特定して行うものではなく，主に OS などのソフトウエアが持つセキュリティホールを狙い，混乱の原因となるデータやウイルスを無差別に送りつけるものである．主に社会全体を混乱させるのが目的で行われることが多い．

ここでは被害が特定の企業や組織に限定され，政治的な意図の少ないものをサイバー攻撃とみなし，被害が多数に及び多分に政治的な目的を持ち，地域の住民に混乱と不安をもたらして恐怖感を与えるようなものをサイバーテロと考えることにする．

3．サイバーテロの脅威

サイバーテロに対しては，被害が甚大になった場合を想定して十分な警戒が必要であるという意見がある．これに対して社会の重要インフラなどのシステムは，たとえ不正侵入に成功してシステムをコントロールできたとしても，さまざまな防御体制が用意されており，社会が破局的な状態に陥ることを防いでいる．不正侵入やクラッキングよりも，爆弾を仕掛けるほうが簡単であるといわれ，サイバーテロを過大評価すべきではないという意見もある．このような意見がある中で，物理的テロとサイバーテロの同時実行や，原子力発電などに代表される重要インフラと通信などの情報インフラへの同時多発テロの実行などは，十分な対策を考えておく必要がある．しかしサイバーテロに対する恐怖感を必要以上にあおると社会的混乱を引き起こす危険性もあるため，この点で充分注意することが重要である[31].

今後はサイバーテロだけで犯罪を行うのではなく，従来の武力や爆弾などによるテロ攻撃と組み合わせ，テロの効果を倍加させることを目的として行われることも危惧されるようになった．コンピュータを使いネットワークから侵入して破壊行為などを行うだけがサイバーテロではなく，爆発物などにより直接コンピュータセンターを物理的に破壊する行為も，サイバーテロと同様かそれ以上の被害をもたらす．爆発物などを使用する破壊活動は以前からテロリストが用いてきた伝統的な手法である．このような攻撃方法ではコンピュータに関する専門的な知識は不要であり，ネットワークから相手のコンピュータ・システムへ侵入するサイバー攻撃より，物理的な被害をも同時に伴う分より多くの被害を与えることが想定される．

サイバーテロは攻撃対象がコンピュータ・システムであること以外は伝統的なテロ行為と同じであるが，今後のサイバーテロは従来のテロリズムが持つ側面をも併せ持つといえる．わずかな資金で甚大な被害を与える可能性があるサイバー攻撃に関心を抱く人々はテロリストだけではない．個人をはじめ国家や民間組織，または既成の社会から正統的とはみなされない宗教的集団であるカルト集団まで様々であり，サイバーテロの目的は軽いいたずらから恨みばらしまで含まれ多種多様である．

これまでのところサイバーテロによる直接的な死傷者は出ていないといわれている．だが死傷者が出ていないからさほど脅威ではないと結論を急ぐことはできない．安保克也らによればネットワークからの直接的な攻撃で人を死傷させることは難しいが，間接的な攻撃では死傷者が発生する可能性もある．サイバーテロとして狙われる対象は軍事施設だけではなく，電気やガスなどの重要なライフラインも攻撃対象にされるため，一般市民を巻き添えにした無差別テロに発展する可能性もあるといわれる[6]．サイバーテロは社会に政情不安をもたらすことを目的としているため，社会生活と密着したライフラインへの攻撃は無差別的な要素を持つとともに，施設自体の攻撃は二次的な目的でしかない．現に中東のイスラエルやパレスチナ自治区をはじめとした世界の紛争地域では，市民の日常生活と結びついた公共交通機関のバスが爆破されるテロがたびたび発生しており，市民に多大な恐怖感を与えているのである．

以下にダン・バードンの著書を参考に，現段階で想定される重要インフラと関連させたサイバーテロの被害例を挙げてみたい[1]．サイバー攻撃によって航空管制システムのコンピュータを破壊し航空管制を麻痺させた場合，航空機同士の衝突事故が起こる危険性が高くなる．今後も航空機は増加するため，特に混雑する飛行場近辺の上空や離着陸時における事故の危険性が高まるといえる．発電所の発電量や電気の供給を管理するコンピュータを破壊して電力の供給に障害を与えれば，大部分が電気によって支えられている現代の社会生活は麻痺状態になり，人々の生活に混乱をもたらすことが予想される．貯水量の多い大規模なダムの水門を予告もなく突然開いて放水させ，河川の水量を増やして下流にある都市を浸水させることも考えられる．

なかでもサイバー攻撃に関するケースで最も恐ろしいものは，原子力関連施設への攻撃である．原子力発電所などの原子力技術関連施設はコンピュータによって管理されている．そのため原子力発電を行う際に使用される核融合炉の炉心温度を管理するコンピュータを悪意に操作して炉心温度を上昇させた場合，1986 年にウクライナのチェルノブイリ発電所で発生した原子炉融解事故に類似した事故を人為的に引き起こすことができる．放射能汚染が国境を越えて蔓延すれば，地球規模での問題にもなりかねず，その被害は計り知れないものがある．

さらにサイバー攻撃だけでテロを実行するよりも，生物・化学兵器の利用や爆弾テロなどと同時攻撃を加え，電話の 110 番や 119 番などに代表される緊急通報システムの破壊と組み合わせることにより，負傷者の救助を遅らせ死傷者の数を増やすなど，従来の攻撃手段の効果を高めるものとして利用される

危険性も否定できない．これまで見てきたように社会のあらゆる場面でコンピュータが使用されている現代社会では，サイバーテロの脅威に対して防衛策を実施しなければならない．先進国ほどコンピュータ・システムへの依存度が高く，サイバーテロによる被害は現代社会の崩壊をもたらしかねない危険性を持っている[7]．安保克也らによれば米国ではすでにサイバー攻撃による被害件数は 250 万件以上であり，その被害総額は国家予算規模に上るのではないかといわれている[8]．そのため米国ではサイバーテロによる脅威は．ミサイルや核兵器，生物・化学兵器などによる大量殺戮兵器の拡散と同程度に重大であるとみなす軍事専門家も存在する．

核兵器の開発には科学技術の知識に基づいた高度な技術力が必要であるが，その破壊力は極めて甚大であり，北朝鮮の核開発には世界中が注目した．これに対して生物・化学兵器は少ない人数でも使い方次第で大きな被害を与えうる危険性があることから，「貧者の核兵器」と呼ばれる．生物・化学兵器は製造コストが核兵器に比べて安く，僅かな量でも核兵器に相当する人的被害を与えることができるからである．これらの生物・化学兵器と同様にサイバー攻撃は，わずかな資金と労力で大きな被害を与えうる危険性を持つと見なされており．テロリストらがコンピュータを有用な兵器として注目し研究しても不思議ではない．このようなことから宮脇はサイバーテロを「第三の貧者の核兵器」として警戒すべきであると指摘している[5]．

(1) サイバーNGO の出現

環境保護や原子力発電の廃止あるいは野生動物保護など政治的な主張を掲げる NGO が，関連する国際会議の開催や国際条約の締結に合わせ，問題の当事国となっている政府機関や企業のウェブサイトに対し，政治的な抗議活動の一環として不正アクセスなどによるサイバー攻撃を行うことがある．このように政府機関や大企業のコンピュータに対し，意見を同じくする者が集団となってサイバー攻撃を仕掛ける非政府組織を，宮脇磊介は「サイバーNGO」と呼んでいる．これらの集団も攻撃対象となる組織や個人に被害を与える危険性があることから，インターネット上のテロリストと同様に問題があると指摘している[9]．サイバーNGO の中には多数の参加者を集め，議員や政治団体などに電子メールで抗議文を送ったり，インターネット上に公開されている掲示板やメーリングリストなど利用して自分達の意見を多量に書き込んだりすることもある．

(2) ハクティビズムの台頭

ハクティビズムとは，攻撃者を意味する「ハッカー」と政治的行動主義を意味する「アクティビズム」を合成した造語である[10]．政治思想や価値観あるいは宗教観において自己の確立した主張を持ち，自己の思想や宗教観と敵対する組織や団体に対し，インターネット上で様々な攻撃を行っている．イスラエル，パレスチナ，インド，パキスタンなどの国々で多く見られ，最近では中国などにも類似の攻撃を行う集団が存在していることが確認されている．日本の靖国神社や官公庁のサーバーなどはその攻撃対象となった．これらハクティビストの活動は年々活発化すると予想されており，ハクティビズムはインターネット上で行われるゲリラ的な政治活動の現われとみなされる．敵対するウエブサーバーに不正侵入して内容を書き換えることにより,政治的なメッセージの宣伝を行ったり，サーバーが処理しきれないほどのデータを送りつける分散型サービス拒否攻撃（DDoS 攻撃，Distributed Denial of Service）を行うことも多い．近年では新興宗教団体などの組織もサイバーテロに興味を示している[11]といわれて

おり，現実にカルト集団として中国政府に一切の活動を禁じられた法輪功が，2002 年 6 月テレビ用通信衛星の送受信機に侵入し，何百万人もの視聴者へ政治的な宣伝メッセージを送る事件が発生した[12].
この事件の発生は民間団体であってもサイバーテロの実行が可能なことを実証する結果になった.

(3)歴史教科書問題とサイバーデモ

サイバーデモとは，インターネット上で主張を同じくする賛同者が多数参加して，政治的な目的を実現するための統一行動を行い，特定のウエブサイトなどに対して不正アクセスなどを行うものと解されている．日本においては 2001 年に歴史教科書問題が起きた際に最初のサイバーデモが発生した．新しい歴史教科書を作る会によって作成された教科書が公表されると，2000 年から 2001 年にかけて日本を含むアジア諸国で社会問題となった. これが首相の靖国神社参拝とあいまって中国・韓国などの近隣諸国と深刻な外交問題に発展していた．これら日本の歴史教科書問題に関する抗議活動として 2001 年 3 月，文部科学省，自由民主党，産経新聞社など合計 6 ヶ所のウェブサイトが中国や韓国などから攻撃された．この事件では極めて多数の賛同者が，予め定められた時刻に攻撃対象のサーバーに対し同時にアクセスを行う攻撃が行われ，サーバーの処理能力を超える過大な負荷により，ウェブサイトが提供する正常なサービスを停止させるなどの被害を与えた(図 1).

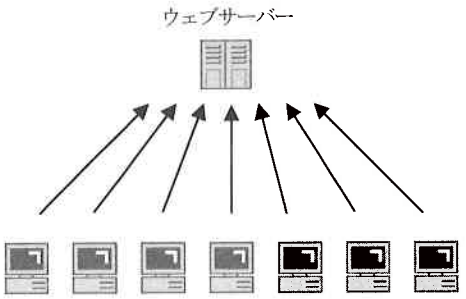

図 1）ウェブサーバー攻撃の概略図

この事件の直前には同時アクセスの準備として，インターネット上で賛同者を募り，特定のサイトを攻撃するために作られた専用ソフトが不特定多数の人々に配付されていた．この専用ソフトを使用すれば画面をクリックだけで，コンピュータに関する高度な知識がない者でも，簡単に攻撃に参加することができる仕組みになっていた．これによって多くの賛同者が容易に攻撃に参加することができたため被害を大きくした．また一時的ではあるが同じ意見を持つ賛同者が，インターネット上で一つの仮想的な組織を結成して攻撃に参加する統一行動が見られた．これらの点からこの事件はインターネット上で行われる「サイバーデモ」の一種であったと見なされている．この事件では近隣諸国からの DDoS 攻撃やクラッキングが行われたことが明らかであった．しかし日本以外からの国から攻撃を行っているため，当時の日本の法律で裁くことは困難であり，誰一人として逮捕されることはなかった.

同様のサイバーデモは，2005 年 4 月に中国の上海などいくつかの主要都市で反日デモが発生した際にも起きており，中国の日本大使館のウエブサーバーに大量の不正アクセスが行われ，接続障害を起こし

て運用停止に追い込まれた．そのほかこの事件と相前後して，日本国内の特定の自治体や企業にも不正アクセスが行われ，ホームページが改竄されるなどの被害が発生したことは記憶に新しい．

(4)官庁ホームページ改竄事件

2000年1月24日，科学技術庁のウエブサーバーが不正侵入され，ホームページの内容が何者かによって中国語と英語の文章に改竄される事件が発生した．改竄された文章は日本の歴史認識や南京大虐殺の悲惨さを訴える内容のものであり，日本人を軽蔑する言葉も併記されていた．さらに1月25日には，総務庁のホームページが南京大虐殺を非難する文章に改竄され，総務庁統計局のサーバー上で公開していた統計データが全て消去されていた．これらの改竄事件以降，運輸省や毎日新聞社などのホームページを改竄する事件が合計16件発生し，不正アクセスの数は9省庁で3万2000回にも及んだとされている．さらに人事院，大蔵省，防衛庁，文部省などのサーバーに対して不正アクセスの痕跡が見られたが，不正侵入を防御するためのファイアウォールを導入するなどの安全対策が採られていたため，ホームページを書き換えられることはなかった[13].

最初のホームページ改竄事件発生から2日後の2000年1月26日に，警視庁は麹町警察署に捜査本部を設置して，電子計算機損壊等業務妨害罪の疑いで捜査を開始した．警視庁の捜査により16件の攻撃のうち12件が中国から，1件が米国から，2件が東京大学のサーバーを踏み台にして不正アクセスされたことが判明した．しかし事件発生当時，東京大学のサーバーではログ（利用状況やデータ通信の記録）を保存しない設定にしており，また不正侵入された省庁のサーバーでは侵入者によってログが削除されていたため，不正な侵入者や攻撃者を特定する証拠が残っておらず，犯人を検挙することはできなかった．中国や米国からの不正アクセスについても，海外からのアクセスであるため侵入者の特定が難しく，事件は犯人不明のまま未解決となっている．

政府機関のホームページが不正な侵入者によって改竄されたことから，日本政府のコンピュータに対する安全管理が不十分なものであることが明らかになった．ホームページの不正な書き換え事件は，国民に対してコンピュータ社会における脅威や危機感を強く感じさせることになった．この事件前後から，政府や地方自治体，企業においてコンピュータのセキュリティ対策が重要視されるようになっており，同年1月21日に，日本政府は「ハッカー対策等の基盤整備に係る行動計画」を発表したばかりであり，セキュリティ問題に積極的に取り組んでいくことを表明した矢先の出来事であった．

事件が2000年1月24日に発生した原因として考えられているのが，前日の23日に大阪で開催された南京大虐殺に関係した集会である．この集会は南京大虐殺の認識に疑問を投げかける内容であったため，この集会に気づいた中国政府外交部は日本政府外務省に対し集会の開催中止を要求した．しかし日本政府は憲法に記載されている「集会・表現の自由」を理由に中国政府の要求を断った．このような日本政府の対応に反発した中国のハッカーたちが，日本政府に対して抗議をするためホームページを改竄したとする見方が有力である．これらの点から見て，官庁ホームページ改竄事件はハクティビズム思想に基づいたサイバーテロの走りであると宮脇磊介は著書の中で述べている[14].

5. 中国の状況

(1) 紅客

中国では一般的にハッカーのことを「黒客」と呼んでいるが，近年では新しい種類のハッカーとして出現した「紅客」の活動が目立つようになっている．ニューズウィーク日本版に記載されたメリンダ・リウの記事に，インターネット上で活動する中国のナショナリストを取り上げたものがある．それによれば紅客の大半は，インターネット上で活躍する 20 代の中国ナショナリストといわれ，1998 年ごろからアメリカをはじめとした NATO(北大西洋条約機構)諸国や台湾，日本，インドネシアなどのウェブサイトを攻撃しているといわれている[15].

紅客の最大の攻撃目標は台湾にあるといわれ，1999 年夏に李登輝総統が「一つの中国」の原則に逆らい，「国と国」としての協議を主張した際に，紅客の集団は台湾政府に関連した 20 あまりのウェブサイトに対して，一ヶ月で 7 万 2000 回にのぼる攻撃を行ったとされている．2000 年 3 月に行われた台湾の総統選挙の際には，中国本土の紅客が台湾のコンピュータ・ネットワークを混乱させることによって選挙を妨害しようと企て，台湾のコンピュータ・ネットワークへ攻撃を行い，紅客と台湾国防部のコンピュータ専門家との間で，台湾海峡を挟んでお互いにサイバー攻撃が行われたといわれている．台湾の軍事アナリストによれば，これらのハッカー行為には中国の紅客だけでなく，軍の専門家も攻撃に加わっていたのではないかと推測されている．

さらに 1999 年コソボ紛争において，セルビアのベオグラードで米軍機による中国大使館への誤爆事件が発生したが，その直後には中国の紅客が米国政府のネットワークに対し報復的な攻撃を行った．米国政府はこの不正アクセスの中に，中国からの IP アドレスが含まれていることを明らかにした．その後 2001 年に南シナ海上空で米海軍の電子偵察機 EP-3 と中国の戦闘機 F8 が接触事故を起こした際にも，米国政府関連の公式サイトをはじめとして，何百ものウェブサイトが紅客の攻撃に曝され，米国のハッカーと紅客との間でいわば民間レベルのサイバー攻撃が行われた．紅客の登場は中国の若者の間でナショナリズムが高まっていることを示しているが，彼らのサイバー攻撃能力は危険性を秘めており，ネットワーク社会における新たな脅威とみなされている．

(2) 超限戦構想

中国の軍事科学院や国防大学をはじめとした人民解放軍の諸機関は，『超限戦』というサイバー戦争の効用に関する本を出版した[16]．1999 年に空軍大佐の喬良氏と王湘穂氏の共著である『超限戦』の中では「技術力に勝るアメリカに対抗するには，中国は“型にとらわれない戦争”に活路を見出すべきだ」と論じられている．この本は中国国内だけでなく海外からも注目を浴び，中国がサイバー戦争への準備を本格的に進めているのではないかという疑念を抱かせた．この超限戦は非対称戦とも呼ばれ，2001 年 9 月 11 日の米国ニューヨークで発生した同時多発テロと理論的な関連もあるといわれている．

超限戦とは制約なき戦争すなわちあらゆる戦術を駆使する戦争という意味であり，「サイバー攻撃，暗殺，爆弾テロ，生物･化学兵器，金融錯乱，環境破壊，メディア戦」など，これまでタブーとされてきた戦術を効果的にミックスさせ，勝利を得るためにあらゆる手段を動員して戦争を遂行することを主張している[17]．超限戦の内容を読み解いていくと，台湾や日本，米国などの外国を標的とした最近の中国人紅客によるサイバー攻撃は，彼らの唱える「新軍事革命」がすでに現実のものとして実行されてい

ることを示している．サイバー攻撃を伴う戦争では，戦争相手国の情報化が進んでいればいるほど自国にとって有利な状況になる．米国は情報産業の最先端国であり最も社会システムの情報化が進んでいる．逆に現状の中国ではそれほどコンピュータ・システムが普及しておらず，社会システムの情報化が進んでいる部分が少ないため，自国のコンピュータ・ネットワークへサイバー攻撃されたとしても被害は少ない．故にサイバー攻撃を用いることは中国にとって有利な攻撃であると言える．中国がサイバー戦略を積極的に導入する理由として，現在の軍事力が未だ十分なものではないとする見方が人民解放軍内部にあるものと考えられる．事実，通常兵器や核兵器を使用する戦争では米国の圧倒的な軍事力に対して核弾頭数や軍事技術の面で明らかに劣っている．だがサイバー攻撃を用いれば状況は一変し，情報化の進んでいる米国や先進諸国に甚大なダメージを与え，中国にとって有利な状況に持ち持ち込める可能性もある．中国にとってサイバー攻撃は大国の軍事的脅威から逃れるための必要な手段といえるのである．中国が米国を意識する理由としては，近い将来台湾の独立によって中台戦争が勃発した場合，米国が軍事介入するのを恐れているとの見方が有力である．今のところ台湾が独立する可能性は低いと見られているが，尖閣諸島問題や南沙諸島問題，中印国境紛争にみられるように，中国が諸外国との間で抱えている問題は今も多々存在している．将来起こり得る戦争に備えるのは国家の安全保障を考慮する上で当然のことであり，中国のサイバー戦略に関する能力の向上はアジアの安全保障を考える上で憂慮すべき問題である．

6. サイバーテロ対策の難しさ

コンピュータ・システムに障害が発生した場合，その原因がテロリストのサイバー攻撃によるものか，またはシステムが内部に持つバグなどの不具合によるものか，原因を特定することが困難な場合が起きる．そのためサイバー攻撃の被害にあったと明らかになった場合でも，それはセキュリティ管理者がシステムの設計や運営・保守に落ち度があったとして責任を問われることになりかねない．そのため多くの場合は被害が公表されずに隠蔽されることもある．また公表されている件数より実際にはもっと多くの被害が発生しているといわれている．しかし被害原因の特定が難しいことから組織による被害情報の未公表もあり，正確なサイバー攻撃の被害情報収集は難しい状況にある．このように正確な情報がないことがセキュリティ対策の遅れの原因になっている．サイバー攻撃の被害にあった場合は届出を義務化したり，被害にあったコンピュータを第三者が検証をしたりするなど，被害情報を積極的に収集する機関が必要であるといえる．

第２章　ネットワーク・セキュリティに係る法制度と組織の整備

1. 不正アクセス禁止法の制定

サイバー攻撃によるコンピュータ犯罪を取り締まるためには，まず制定された法律が必要である．政府は増加するコンピュータ犯罪に対処するため，関連する法律の整備を行ってきた．「不正アクセス禁止法」は1999年８月に国会で成立し，2000年２月より施行されたもので，現時点ではネットワーク上で行われる不正アクセス行為を取り締まる唯一の法律である．正式名称は「不正アクセス行為の禁止等に関する法律」といい，「不正アクセス禁止法」は略称である．マスコミなどではしばしば略称の方が用いられている．

不正アクセス禁止法は，IDやパスワードの不正使用およびその他の攻撃手法を使い，使用許可のないコンピュータへの不正なアクセスを犯罪行為として定義している．同法第1条に「この法律は，不正アクセス行為を禁止するとともに，これについての罰則及びその再発防止のための都道府県公安委員会による援助措置等を定めることにより，電気通信回線を通じて行われる電子計算機に係る犯罪の防止及びアクセス制御機能により実現される電気通信に関する秩序の維持を図り，もって高度情報通信社会の健全な発展に寄与することを目的とする．」とある．

この法律が施行される以前は，不正侵入などによりコンピュータ上のデータの改竄や削除を行った場合には，「電子計算機損壊等業務妨害罪」という法律で罰せられていた．しかしこの法律では不正侵入してデータを盗み見るだけでは処罰の対象とはならず，刑法上の詐欺罪や民法で規定されている不正行為を行わない限り罪を問われることはなかったため，さまざまな問題を引き起こしていた[18].

現在でも多くのネットワークでは，基本的にIDとパスワードでユーザーを識別しており，他人のIDを不正使用したアクセス行為は，ネットワークの信頼性を損なう危険性を多分に持っている．そのため不正アクセス禁止法では，次の3つの行為を犯罪とした．

(1) 他人のIDやパスワードの盗用などにより，他人になりすましてアクセス認証を行い，コンピュータを不正に利用可能にする行為は犯罪となる．
(2) セキュリティホールなどシステムの欠陥を悪用するなど，なりすまし以外の攻撃手法を用いて，他者のコンピュータに侵入して利用可能にする行為なども処罰の対象となる．
(3) さらネットワークの出入り口となるゲートウェイ端末に不正侵入し，内部のコンピュータを利用可能にする行為も犯罪となる．

不正アクセス行為に対する処罰は1年以下の懲役若しくは50万円以下の罰金を科すと規定されている．また認証情報として使われるIDやパスワードを，利用者以外の者に提供してはならないと定め，システム管理者に対して，認証情報の適切な管理を行うことやコンピュータを不正アクセス行為から防御することを求めている[19].

2. サイバーフォースの設置

サイバー攻撃などのハイテク犯罪が近年増加していることに対応するため，2001年に警察庁はコンピュータセキュリティに関する専門の技術者部隊として「サイバーフォース」を設置した[20]．サイバーテロ発生の未然防止や被害の拡大防止，および犯罪の検挙を行うことが主な役割である．サイバーフォースは全国（札幌，仙台，さいたま，東京，名古屋，大阪，広島，高松，福岡）に配置され，都道府県警と連携した対策を実施している．この機関が設置されたことにより，政府機関などのコンピュータシステムを狙った不正侵入やサイバー攻撃に対し，迅速かつ的確に対処するための体制が整えられた．

全国のサイバーフォースの司令塔的役割を担っているのが，東京に設置されている「サイバーフォースセンター」である．ここでは全国の警察機関と基幹通信網のインターネット接続点に設置された侵入検知システムを24時間体制で監視しており，関係機関に情報提供を行っている．またハイテク犯罪やサイバーテロに関する警察各部門への技術的支援や調査・分析など的確な対応を行うため，警察庁技術センターとも連動させて，サイバーポリス体制をより強化している．警視庁では2000年2月より専門の捜

査員が24時間体制でインターネット上をパトロールするハイテク犯罪対策センターを開設している．サイバーフォースの具体的な活動内容は以下の通りである[21].

(1) 攻撃手法等の情報収集

セキュリティ関連の情報収集に加え諸外国の警察機関との情報交換，攻撃プログラムの検証，解析プログラムなどの作成を行う．

(2) 事前防御

サイバーテロの発生を未然に防ぐため，サイバーテロに対するコンピュータ・システムの脆弱性をテストするための機材及びツールを開発する．日本独自の強力なファイアウォールの開発などセキュリティ技術の開発を目指している．

(3) 緊急対処

攻撃パターンに沿うかたちで即時に防御する手法を確立する．特に未知の攻撃手法を用いられた場合でも効果的な対処が可能なシステムの開発を行い，サイバーテロの被害拡大を防止する．

(4) 共通基盤構築

サイバーテロ事件の検挙を目的とし，複雑なログ情報の集約・分析を自動的に行うツールの開発および改竄，削除されないログの保存技術を開発する．

(5) 重要インフラとの連携

警察組織が実際に運用されているネットワークを管理しているわけではない．ネットワークは民間企業が所有・管理しているため，サイバー攻撃の防御には民間企業の協力が不可欠である．そのため情報通信，金融，鉄道・航空，電力・ガス，政府・行政サービスなど社会を支える重要なインフラを管理している企業と連携し，セキュリティ関連の情報交換を行っている．

(6) 脆弱性の評価

コンピュータに対してサイバー攻撃を模倣した実験を行いネットワークの脆弱性を評価，外部からの攻撃に対して弱い部分の修復およびシステムの管理状況を調査する．セキュリティに問題がある場合，どうすればセキュリティが向上するのかについてのアドバイスも行っている．

(7) 事案の認知・緊急対処

事件発生時には即時に関係各省へ通報を行う．またリアルタイム検知ネットワークによる監視を行い，テロ発生時における情報収集および緊急対処を速やかに行うことで被害を最小限に押さえる任務を担う．

(8) 海外関係機関との連携強化

海外関係機関と研修生の交換，サイバー犯罪技術情報ネットワークシステムの構築を行い，海外の捜査機関との情報交換やシステムの構築などで連携を深める．

警察庁では「@police」(http://www.cyberpolice.go.jp/)というセキュリティ情報に関するウェブサイトを設けている(図2)．このサイトにおいてサーバー管理者や個人ユーザー向けに，ネットワーク・セキュリティに関する情報を公開している．全国の警察施設（57拠点）に設置された不正侵入検知システムおよ

びファイアーウォールの検知状況を分析し，インターネット定点観測として公表している．この中には実際に行われた攻撃の国別発信元や，攻撃手法などの分析結果を月毎にまとめた情報も含まれている．そのほか警察庁が収集した海外のセキュリティ情報や，インターネットを経由した全国の警察施設に対する攻撃なども公開しており，セキュリティ対策を検討する上で参考になるものである．

警察庁はこれらのウエブサイトなどを通して，攻撃手法の研究やセキュリティ情報を企業へ提供するなど，官民が協力してサイバー攻撃に対抗していくための体制づくりを行っている．しかし，ネットワーク上を流れる情報は日々増加する一方であり，増加し続ける情報量に対し調査分析能力が追い付いていない状況である．現状では警察などの捜査機関が国内のネットワークを守ることは不可能に近い．そのため捜査機関に頼る前に，自分のコンピュータは自分で守る意識を持ち，積極的にセキュリティに関する情報を集め，絶えずセキュリティ対策を実行していく必要がある．

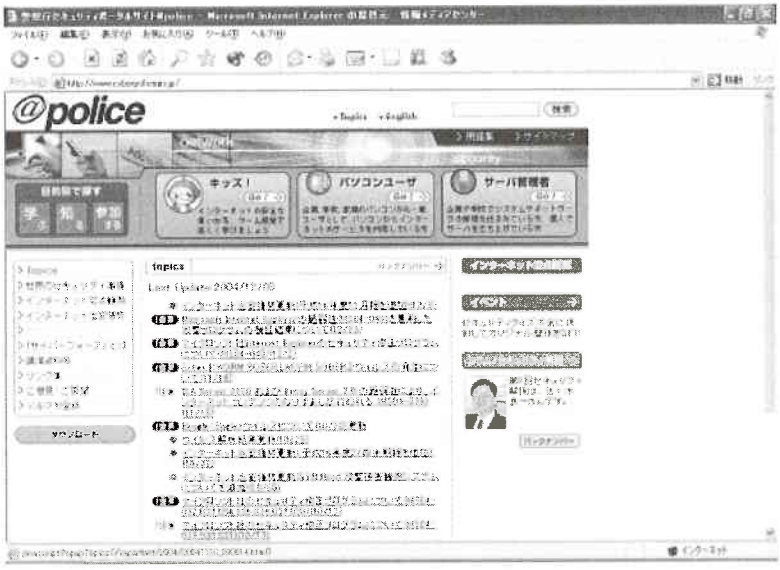

図2）警察庁がネットワーク・セキュリティに関する情報を公開しているウェブサイト
(http://www.cyberpolice.go.jp/)

3. サイバー犯罪防止条約

サイバー攻撃やサイバー犯罪といったものは国境の概念に乏しく，国境を容易に越えられるネットワーク上で行われることが多く，一国だけの捜査機関による捜査活動のみで海外からの攻撃者を特定するのは困難なことが多い．そのためサイバー犯罪の捜査には多国間の捜査協力が不可欠となってきており，サイバー犯罪に関する捜査活動において，捜査機関の国際的な協力体制を実現するための条約が締結されている．

サイバー犯罪防止条約はサイバー犯罪に関する初の国際条約である．2001 年に日米欧の 30 ヶ国が調印して条約が発効した．1997 年から欧州評議会(Council of Europe)が中心となって条約制定のための検討を始め，欧州評議会に加えアメリカ，カナダなどの諸国が条約策定のための作業を行った．サイバー犯罪防止条約の批准国には，コンピュータウイルスの作成や配布あるいは不正アクセスやデータの改竄など，コンピュータに関わる犯罪を自国の国内法の犯罪として扱えるようにするため，これらの行為を禁

止する国内法の制定を義務づけられている．さらに捜査機関の国際的な協力体制の実現や，インターネット接続事業者(プロバイダー)への通信記録保持の義務化や，個人情報の保護なども盛り込まれている[22].

(1) 条約におけるサイバー犯罪の規定

条約では想定されるサイバー犯罪の類型を定めている．国によって犯罪として規定されるものが異なるため，サイバー犯罪とみなされるものの基準を作り，批准国が条約を元に自国の法整備を行うことを要求している．サイバー犯罪防止条約の第2条から第13条において，サイバー犯罪として規定されているものは次のようなものがある．

① 違法なアクセス（非権限者によるアクセスすなわち不正アクセス）
② 違法な傍受（ネットワーク上で行われる不正な盗聴）
③ データの妨害（非権限者によるデータの破損，削除，改竄，隠蔽）
④ システムの妨害（非権限者によるデータの入力・破損・改竄などによるシステムの機能に対する重大な妨害）
⑤ 装置の濫用（犯罪目的のソフトや装置の製造と保有，ウイルスの作成）
⑥ コンピュータに関連する偽造（電子証明書の偽造，データの改竄，削除など）
⑦ コンピュータに関連する詐欺（データの改竄やシステムの機能を妨害するなどして他人に財産上の損害を与える）
⑧ 児童ポルノに関する犯罪（コンピュータ・システムを通じた児童ポルノの製造・提供およびその取得と保有）
⑨ 著作権および関連する権利の侵害に関する犯罪（著作物に関する著作権保護）
⑩ 未遂および幇助または教唆（上記で述べた犯罪の実行幇助と教唆）

(2) 捜査手続きの統一化

条約の第14条から第23条においては，捜査の手続きに関する取り決めを定めている．捜査が迅速に行えるように，国によって異なる刑事手続法や捜査手続きをある程度統一することを条約締約国に求めている．捜査時に証拠を集めやすいように，通信記録の迅速な保全と部分的な開示や確保を義務づけ，捜査当局がシステムに内蔵されているデータの応急保全が可能になるように，立法化などの措置を締約国に求めている．またインターネット接続業者へはアクセスログの提出命令のほかに，システムに内蔵されているデータの捜索・差し押さえや電子データの傍受などが可能なシステムの導入を求めている．

(3) 捜査の国際協力とデータ保全

条約の第24条から第35条においては，捜査の国際協力を築き，できるかぎり広範囲に相互に捜査協力することを原則としている．条約加盟国の要請に応じて，犯罪人の引渡し，自発的な情報提供，データの迅速な保全，通信記録の迅速な開示，通信データのリアルタイム収集と傍受などにおいて，相互に援助を提供することを条約批准国に求めている．

(4) 条約と国内法の課題

サイバー犯罪防止条約に基づき条約批准国は，国内法の改正と捜査手順の改正を進めている．しかし国によって犯罪とされる基準に差があり，このような場合に他国の基準に一致させるよう法律の整備を行なっていく必要がある．しかし，その際に国によってはこれまでより厳しい規制になる恐れもある．しいては国民に対して保証されている「表現の自由」「通信の秘密」といった権利を侵害する結果になり，法的規制の基準が国際水準により強制的に，より厳格なものへと変更されることが起こり得る[23]．サイバー犯罪防止条約は欧米の安全保障に対する考え方をグローバル化する動きと見ることもできる．元々欧米には法で禁じられていなければ何をしても自由であるから，逆に法で禁ずべきもの，違法であるものを明示的に規定すべきだとする考え方があるといわれる．サイバー犯罪防止条約は元々欧米諸国を中心に原案が作成されたものである．そのためこの条約は欧米流の安全保障に対する考え方を，世界全体に対してグローバル・スタンダードとして押しつける結果になりかねない側面をもっている．このような観点から，海外からの外圧によって法律が立法化される恐れがあり，各国からこの条約に対する問題点が指摘されている．従来の法律制定の考え方では，法は国民の意志によりその国の文化や生活習慣を考慮して定められるべきものであり，他国が法律の制定に口を挟むことは歓迎すべきことではないとされていた．しかし近年では，サイバー犯罪やそれを防止する国際的な捜査体制を実現するため，国内の法律の制定においても，国際的な協力体制を前提とすることが要求される状況になっている．

(5) 個人情報保護への対応

日本においては2000年8月に通信傍受法（犯罪捜査のための通信傍受に関する法律）が施行された．この法律では薬物および銃器関連犯罪，集団密航の罪，組織的殺人犯罪といった4つの犯罪に限り，犯罪捜査の一環として，検察や警察が裁判所の令状に基づき，電話や電子メールなどの通信傍受を許可している[24]．しかしサイバー犯罪防止条約への加盟により，これまでの4つの犯罪に加えて通信の傍受を許可する犯罪の種類を増やすことが検討されており，そのため通信の秘密やプライバシーの保護といった国民の権利の侵害が危惧されるようになった．さらに2001年9月に発生したニューヨーク世界貿易センタービルでのテロ事件以降の世界的な流れとして，個人のプライバシー保護を重視することよりも，社会の安全を重要視する風潮が高まっている．

法務省は2003年サイバー犯罪防止条約批准に向けて，関連した国内法を整備するための要綱をまとめた．その中でインターネット接続事業者に対し，捜査令状がなくても電子メールの通信履歴の提出を要請できるなどの内容が含まれており，憲法で定められている通信の秘密や信書の自由を侵害しかねないと指摘されている．サイバー犯罪防止条約に署名している国の中では，日本は条約の批准に対し最も積極的な活動を行っている国のひとつであり，条約批准後も個人情報保護をどのように考えていくべきか積極的な議論が必要である．

他方欧米においては，サイバー犯罪防止条約に規定されている項目について，プライバシーを侵害する恐れのある項目が多々あると指摘され，条約の批准に対する賛否についての議論が活発に行われている．サイバー犯罪防止条約が批准されれば，他国の捜査機関が他国の通信事業者に対し，電子メールなどの通信記録の提出を要求することができることなどが問題になっている．例えば米国で発生したある犯罪において，コンピュータを使って日本の協力者と電子メールの送受信を行っており，電子メールで情報交換が行われていたとする．その犯罪の捜査にはサイバー犯罪防止条約が適用されることになり，海外の捜査機関がインターネット接続業者に電子メールの通信記録の提出を要請すれば，メールの通信内容を容易に入手できるようになる．これはサイバー犯罪条約が適用される範囲が曖昧であることから，海外の捜査機関によって自国民個人の通信の秘密やプライバシーが侵害される危険性が大きくなること

を意味している．さらに山下幸夫はサイバー犯罪条約では捜査機関に，従来よりも強力な捜査権限を与える一方で，その濫用をチェックし監督するシステムが何も設けられていないことも問題であると指摘している[25].

サイバー犯罪防止条約がサイバーテロを含めたサイバー犯罪を取り締まる上で有用な条約であることは確かであり，条約の内容を実現するための国際協力も必要である．だが攻撃手法が常に進化し続けるサイバー犯罪に対抗するには，条約の批准や国内法の整備といった時間を要する制度そのものの基本的な方法論にも問題があるといえる．

4. インシデント・レスポンス

(1) CSIRT

インシデント・レスポンス(Incident Response)とはコンピュータ・セキュリティに関する用語で，人為的な不正アクセスが原因で障害が発生した場合に，それらの復旧を行うために対応することである．インシデントは偶発的な出来事や重大な事変を意味し，セキュリティに関する出来事や事件の場合は，セキュリティ・インシデントということもある．このようなインシデントを未然に防ぎ，障害が発生した場合に迅速な対応を行うため組織の設立が行われている．そのような組織を一般的に CSIRT(Computer Security Incident Response Team)と呼んでおり，コンピュータやネットワーク・セキュリティが危険にさらされるような悪意を持ったインシデントに対応する組織である[26].

CSIRT の設立のきっかけは 1988 年に一人の人間がネットワークに放ったワームによって，当時のインターネット全体が麻痺した事件である．ワームはウイルスの一種とも考えられているが，ネットワーク上で爆発的な速度で自己増殖を繰り返しながら破壊活動を行う不正なプログラムである．放置するとコンピュータを動作不能にしたり，ネットワーク全体に障害を発生させて通信不能にするものもある．

この事件を解決するために，多くの接続組織間で緊密に連絡を取り合うことが必要となった．このインターネット・ワーム事件をきっかけとして，米国のピッツバーグにあるカーネギーメロン大学のソフトウエア工学研究所の中に，世界初の CSIRT として CERT/CC (Computer Emergency Response Team / Coordination Center)が民間組織として設立された．

1990 年代には世界的に同様の組織が相次いで設立され，日本においても 1996 年に JPCERT/CC(Japan Computer Emergency Response Team / Coordination Center)が設立された[27]．JPCERT/CC ではインターネット上で発生する不正侵入やサービスの妨害などのセキュリティ・インシデントに対して，さまざまな支援活動を行っている．支援活動には日本国内におけるセキュリティ・インシデントの発生状況の把握，報告の受付，サイバー攻撃の手口の分析，再発防止のための対策の検討と助言，関連技術の調査・研究および普及・啓発と教育事業などがある．

現状のセキュリティ対策においては，多くの場合に如何にして不正アクセスからの攻撃を防御するかという技術開発や，侵入防止設備の導入が重視される．しかし攻撃者の技術とセキュリティ技術はいたちごっこを続けており，現段階では完璧と言えるセキュリティ対策はありえない．そのため CSIRT の活動はクラッキングされた場合に被害の拡大を迅速に防ぎ，速やかに復旧することが中心となっている．火災の延焼を食い止めるには初期段階の迅速な消火が重要であるように，サイバー攻撃による被害の拡大を抑えるにも，適確な判断に基づいた迅速な対処が必要なのである．

(2) 情報交換

インターネットには国境がなく，1つのインシデントが1つの国や地域だけで局所的に起こるとは限らない．そのため1つのCSIRTだけでは解決できない問題が生じる場合が数多く発生し，異なるサービス対象範囲を持ついくつかのCSIRTが情報交換をしながら協力して対処する必要がある[28]．万一事件が発生した場合，CSIRT同士が協力して迅速な緊急対処を円滑に進めるには，日頃からの情報交換や組織同士の交流，信頼関係が欠かせない．こうしたCSIRT同士の情報交換や相互支援・協調を目的としたフォーラムであるFIRST(Forum of Incident Response and Security Teams)が1992年に設立され，CSIRT同士の情報交換に利用されている[29].

(3) 設立母体と支援活動

CSIRTの設立母体は教育機関，研究機関，政府機関，民間企業，軍事組織など多種多様であり，活動の目的や内容もそれぞれのCSIRTによって大きく異なる．CSIRTの支援活動は組織によって多様化しており，インシデントが発生した場合にそのサイトに出向いて，原因の調査や分析に加えて復旧作業を行う場合もあり，また復旧のための一般的なコンサルティングだけを行う場合もある．

(4) 情報セキュリティセンター

日本政府は2000年2月に情報セキュリティ対策推進会議を設置し，電子政府のセキュリティを確保するため，セキュリティポリシーの策定，システムの監視体制，サイバー攻撃が発生した場合の緊急事態への対応，人的基盤の整備などを行ってきた．その後情報セキュリティ問題に取り組む我が国政府の役割と機能を見直し，2005年4月25日には情報セキュリティに関する我が国のナショナルセンターとして，情報セキュリティセンター(NISC; National Information Security Center)を設置した．NISCでは情報セキュリティ政策に関する基本戦略の立案，政府機関における緊急事態発生に対応するためのセキュリティ情報や攻撃情報の収集，重要インフラのセキュリティ対策などに取り組む．これによってサイバー攻撃が発生した場合の緊急対処に備え，迅速に原因を解明し，対応措置を講じることや，広く情報提供を行ってサイバー攻撃の発生防止に努める対策を実施する．

(5) 今後の展望

セキュリティ・インシデントに関する企業向けの組織としてISAC(Information Sharing and Analysis Center)があり，情報共有分析センターと訳される[30]．インシデントの発生に対して，企業自身で対応可能とすることを目的に設置された．そのためどのような侵入が行われたかの調査や，侵入に対する復旧対策の検討などを行い，業界全体としてセキュリティ情報を共有している．米国では重要な基幹産業ごとにISACが設置され，TELECOM ISAC，ENERGY ISACなど数多くの組織がある．ISACは業界全体としてセキュリティ対策などの知識や技術水準の共有と向上に努めている．

日本でも2002年にTelecom-ISAC Japanが設立され活発な活動を行っている．この組織は通信事業者の情報通信基盤の安全性確保を目的として，通信サービスの提供を妨害するさまざまなインシデントの収集と分析を行っている．分析結果を会員間で共有することにより，今後のインシデントに対応できる頑強な情報通信基盤によるサービスの提供を目指している．

しかしセキュリティ・インシデントに対する個人向けの対応は今後の課題である．JPCERT/CC などをはじめとした各 CSIRT の情報は個人に対しても効果的であるといえるが，OS などのソフトウエアメーカーからの情報や，警察庁など公的機関からの情報も有効である．一般人を対象としたセキュリティ教育も行われ始めているが，多くの人々がセキュリティ情報を理解でき，インシデントに適切に対応できかどうかは疑問といわざるを得ないのが現実の状況であり，今後の対策が必要となっている．

自らのセキュリティは自らの責任において守るべき必要があること，単一の CSIRT が一国のあらゆる組織のセキュリティを守ることは難しいこと，同一の属性を持つ組織群を対象とする専門の CSIRT の設置は，セキュリティに関する知識・情報の集約や素早い対応を実現しやすいことから，CSIRT の設置が増えていくのは歓迎すべきである[31]．今後，日本国内においても大学が学生や教職員を守るための CSIRT や，通信回線サービス業者などのネットワーク組織が顧客を守るための CSIRT，ソフトウェア開発会社が自社製品の利用者を守るための CSIRT など多くの CSIRT が設置され，各種 CSIRT が連携してインターネットのセキュリティ確保に貢献するよう活動していくことが望まれる．

5. 中国におけるサイバーセキュリティ対策

(1) 独自 OS の開発

現在市場に出回っているコンピュータのハードウェアとソフトウェアに関する技術の大半は米国に依存しているのが現状である．特にコンピュータの中心部である CPU や，基本ソフトの Windows はすべて米国製である．OS の内部構造などは公開されていない部分も多いため，セキュリティや国家の安全保障を考えると様々なリスクが存在する．中国やタジキスタンをはじめとしたアジア諸国において，米国産の情報機器やソフトウェアを利用しているのでは国内の安全保障は得られないと考え，自国の技術を開発するプロジェクトが進んでいる．

中国 IT 白書の調査結果によれば，中国国内で使われている大半のコンピュータも，米マイクロソフト社の製品である Windows が搭載されている．中国政府は国内のコンピュータに使われるソフトウェアが米国企業に握られていることを懸念している，高額なライセンス料金の支払いや，使用するソフトウェアが米国企業一社へ依存していることに問題があるとし，米国企業にソフトウェアを支配されないようにするため，国策によって OS の開発を行っている[32]．中国科学院ソフトウエア研究所と北京大学傘下のソフト会社である北京方正が中心となり，『紅旗 Linux』と呼ばれる独自の OS を開発している．中国政府の情報産業部は，紅旗 Linux の開発元である北京中科紅旗軟件技術有限公司に 3000 万元(約 4 億円)を投入し開発を援助している[33]．その結果 2004 年には Red Flag Linux Desktop 4 が発売され市場に出回り始めた．

紅旗 Linux は Windows XP を模倣して作られたインターフェースを持ち，Windows に関する用語と紅旗 Linux に関する用語の相互解説が書かれたマニュアルが用意されているなど，Windows を使い慣れた者が紅旗 Linux に馴染み易いように配慮して作られている[34]．中国政府は官公庁や国立大学および企業などに対して Windows の使用を止め，紅旗 Linux を使用するよう奨励している．中国の郵便局の基幹システムには紅旗 Linux が採用され，2001 年 12 月には北京市当局が市政府機関へ紅旗 Linux を導入することを決定した．政府機関が紅旗 Linux の採用を決定する動きが強まるにつれ，紅旗 Linux の売上は年々増加傾向にある．さらに 2003 年からは Red Flag Linux Desktop を Acer 社のパーソナル・コンピュータに搭載して東南アジア地域に広く出荷しており，中国のソフトウェア産業の発展に大きく寄与している．

(2) 暗号の規制

1999 年 10 月，中国政府は情報の安全を保護して国家の安全と利益を守るため，電子商取引に関連した法規として，コンピュータ用暗号製品などの販売や利用を管理する「商用暗号管理条例」を公布施行した[35]．企業は暗号製品，暗号技術を含む設備を輸入したり輸出したりする際に，必ず事前に国家暗号管理機構の批准を受けなければならない．また国内販売時にも同機構へ許可申請を行い，同機構が指定する製品品質検査測定機構による検査測定に合格しなければならない．

また北京国家保密(機密保護)局が 2000 年 1 月 25 日に公表した規定では，外資系企業を含む会社は，ネットワーク上で重要なデータを保護する目的で使用している暗号化ソフトを当局に登録し，国産の暗号化ソフトを使用しなければならないとしている[36]．国産の暗号化ソフトウェアを使用することで，政府や国内の民間企業が保有している機密情報を，海外の産業スパイや情報機関から保護することが目的である．

(3) 外部ネットワークとの隔離

2000 年 1 月 1 日に実施された「コンピュータ情報システム国際インターネット機密保護管理規定」では，国家機密を扱うコンピュータ・システムを，インターネットやその他の公共情報網との接続を禁じ，物理的に隔離するよう求めている[37]．外部のネットワークとの隔離は外部からの攻撃を防ぐ最も効果的な方法であり，中国政府は積極的に政府の重要な情報ネットワークを外部から隔離する政策を導入している．

(4) 中国語ドメインの普及

近年中国では中国語ドメインの普及が進められている[38]．中国語ドメインが普及すれば，従来使用されている英語ドメインでは中国国内のネットワークへアクセスすることが難しくなり，海外からの攻撃者には中国語に関する知識が要求されるようになる．つまり，中国語と英語の言葉の壁を利用して国内のネットワークを保護し，中国と米国のハッカーの間でたびたび発生しているサイバー戦争による被害を抑えることができるのである．

中国語ドメインの登録は 2000 年 1 月より開始され，中国インターネット情報センターCNNIC(China Internet Network Information Center)の発表によれば，登録開始初日に 3 万 6000 人が登録を申請したとされている．しかし，中国語ドメインを支えるシステムとソフトウェアの開発が遅れており，ドメインの普及の足枷になっている．

これらの中国政府によるセキュリティ対策は，米国企業の製品が市場を独占している状況から抜け出し，独自の技術で開発した独自規格の製品を使用することで，国内のネットワーク・セキュリティを確保し，国内のソフトウェア産業を発展させるための政策とみることができる．ソフトウェア産業における米国企業の一極支配が進む中，こうした米国製品の市場支配から逃れようとする動きは増えていくのではないだろうか．

第３章　ネットワーク監視システムに関する諸問題

1. ネットワーク監視システム

サイバー攻撃を取り締まる際の一つの問題として，コンピュータ・システムの不具合や障害が，テロや攻撃を目的とした意図的なものなのか，あるいは悪意のない人為的なミスによる障害なのか，あるいはコンピュータの自然故障なのかを見極めることが難しい点があげられる．コンピュータは完成された製品とは言い難く，ソフトウェアの欠陥やハードウェアの不具合による障害が起こりやすいため，これらの障害が故意かどうかの見極めが，障害発生の初期段階において重要となる．

仮にコンピュータ・システムの障害がサイバー攻撃によるものであるのならば，早急に対策を講じる必要性がある．だが，自然故障とサイバー攻撃による被害では区別がしにくい場合があり，判断が難しい．そのためサイバー攻撃に対し迅速な対応をするにはテロリストやコミュニティーの動向を監視するなど，事前の情報収集活動が重要であると考えられている．現在テロリストや国際犯罪集団の動向を監視するものとして，米国連邦捜査局(FBI)のカーニボー(Carnivore)やエシュロンなどのように，ネットワーク上で送受信される情報を監視するシステムが構築されている．

2. カーニボーと電子メールの傍受

カーニボーは米国連邦捜査局(FBI)によって設けられた電子メール傍受システムである[39]．米国内のインターネット接続業者(ISP)と協力し，接続業者が所有するサーバーを利用して交わされる電子メールを傍受することができる．これらの電子メール傍受システムにより，テロリストや国際犯罪集団の間で交わされる電子メールを傍受し犯罪捜査に役立てている．米国司法省はこの傍受システムを容認しており，合法的に犯罪捜査の手段として通信の傍受が許可されている．ちなみに米国では，国内で完結する通信を傍受することは原則的に禁止されているが，外国発着の通信を米国内で傍受することには何ら制限がない．

FBI では犯罪捜査の過程で，捜査対象の容疑者が送受信する通信内容を傍受するため，カーニボーをインストールしたコンピュータをインターネット接続業者に設置していた[40]．FBI がカーニボーを使用できるのは，犯罪の容疑者について裁判所の命令が得られた場合に限られている．通常は 20 台ほどのコンピュータが裁判所の命令に応じて監視を行える体制になっていた．裁判所の命令の期限が過ぎれば，FBI はカーニボーをインターネット接続業者から撤去しなければならない．

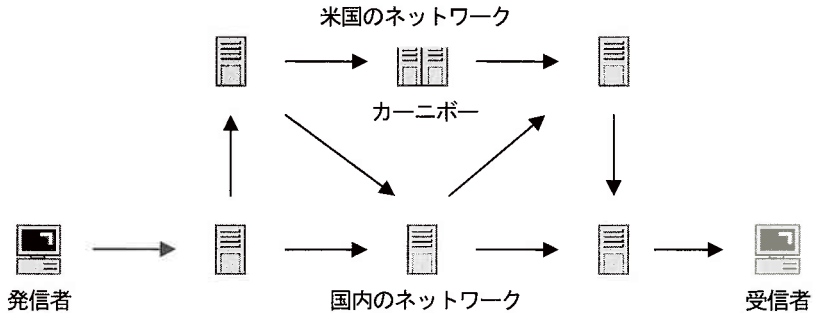

図 3）カーニボーとメールの通信経路概略図

傍受されるメールは米国内でやりとりされるものだけではなく，米国外でやりとりされるメールであっても傍受可能である．なぜならインターネットは米国国防総省が 1970 年代頃から開発した分散ネット

ワーク技術であり，米国国防総省を中心としたネットワークとして構築されている．回線の混雑具合や設備の影響によって通信経路は変化し一定の経路のみを使用するとは限らない．インターネット上のデータの約 7 割は何らかの時点で米国を通るとする試算もあり，米国国外に住んでいる者同士で交わされる電子メールであっても，メールの配送途中に米国内に設置されているメールサーバーを経由する可能性は高い[41]．それゆえ日本国内で送受信しているからといってカーニボーに傍受されていないとは言い切れないのが現状であり，知らない間に他人にメールの内容を見られている恐れがある(図 3)．

海外向けのネットワークは米国内でも限られた場所にしか設置されていないため，数箇所に盗聴施設を設置すれば，海外との間でやりとりされるメールの大多数を傍受することができる．元 NSA 職員のウエイン・マッドセンは論文の中で，「NSA は 1995 年までに，米国内のバックボーンの主要中継地点 9 ヶ所に『スニッファー(盗聴器)』を設置した」と明らかにしており，インターネットの一般利用が本格化しはじめた早い時期から盗聴体制を固めていたことを裏付けている[42]．傍受された電子メールの内容が FBI の捜査官以外の人間に漏れることも考えられ，企業の情報を盗み出す産業スパイの手に渡ってしまった場合，企業に莫大な損失を与えかねない．このような電子メール傍受システムは国民のプライバシーを侵害するおそれの強いものであり，市民団体などから反対の声があがっている．また，テロリストや国際犯罪者集団が暗号化されていない平文のメールを使用して情報をやりとりしているとは考えにくく，この通信傍受システムがテロ捜査にどれほどの効果を上げているのか疑問であるといえる．ネットワーク上で交わされる電子メールは日々増加の一途を辿っており，傍受システムの暗号解析の処理能力向上が課題ともいわれている．

2005 年 1 月，FBI は米国議会に提出した活動監督報告書により，カーニボーを廃止したことを明らかにした．現在はカーニボーと同様の監視機能を持つ商用ソフトウエアを利用している．裁判所の命令に従い，データ収集が可能なインターネット接続業者に，従来の傍受業務を委託しているようである[43]．

3. エシュロンによる通信傍受

エシュロンとは米国，英国，カナダ，オーストラリア，ニュージーランドの諜報機関が UKUSA 協約に基づき運用している通信傍受システムである．フランス語の「梯団」が元々の意味であったが，アメリカの軍事用語では「三角編隊」を意味する．エシュロンは諜報機関内部で開発中の製品に仮に付けられるコードネームとして使われていた．この傍受システムは米国家安全保障局(NSA)が中心となって運用しており，地球全体をカバーするグローバルな通信傍受システムといわれている．エシュロンの歴史は 1947 年に米英の対共産圏通信傍受協定として結ばれた UKUSA 協定に由来し，その後 1970 年代から 1980 年代にかけて残る三国が加わり現在に至っている[44]．

(1) 傍受システムの概要

エシュロン用傍受アンテナにより傍受された情報は，直ちに米国家安全保障局(NSA)や英政府情報本部(GCHQ)にあるコンピュータへ送られる．傍受活動で中心的な役割を果たす「辞書(ディクショナリー)」と呼ばれるコンピュータには各国の重要人物や組織の名前のほか，「テロ」や「爆弾」など特定の用語や言い回しが登録されており，自然言語処理を利用して該当する単語や文脈を分析し，疑わしい交信を記録する．一説によれば，毎分 300 万件もの通信を処理できる解析能力を持つとされている[45]．

エシュロンは文字情報の解析を得意としており，FAX や電子メールの普及は皮肉にもエシュロンの情報収集活動にとって好都合な傍受環境を作り上げることになった．電子メールの場合は，ほぼ 100%の確率で傍受されていると指摘する専門家もいる[46]．しかし世界各国の言語を自動的に解析処理できるコンピュータは未だ開発されておらず，電話など音声通信の傍受では英語をはじめとした主要な言語しか処理できない[47]．そのため声紋による人物特定ができる程度ではないかと専門家は指摘している[48]．ワープロ打ちの FAX であれば容易に処理できるが，手書きで書かれた FAX の判別処理は困難なこと，空中を飛び交う電波の傍受は得意であるが，近年増加している光ファイバーを使用した通信を傍受できないなど，その傍受能力は限定されていると考えられている[49]．

(2) 傍受施設の概要

エシュロンの無線通信傍受施設は世界に数十箇所あり，主にエシュロン構成国である 5 ヶ国に設置されている．その他の地域ではドイツのバートアイブリングやキプロス，青森県三沢市にある三沢基地などの米軍基地内に設置されており，エシュロン加盟 5 ヶ国以外の遠隔地における地域を対象とした通信傍受を行っている．三沢基地は世界第 2 位の規模を有する諜報活動用の基地であり，東アジアを対象とした情報収集活動を担っている．東アジア地域の経済活動が発展していくにつれ，冷戦終結以降その重要性は増している[50]．

(3) 傍受活動の対象

冷戦終結後のエシュロンの傍受活動は，これまでの軍事情報傍受中心の活動から経済分野の情報収集が重要視され，政府機関や大規模商社などの民間通信を傍受するようになったといわれている．エシュロン加盟国が欧州，日本を含むアジア諸国との経済競争を進める上で，自国の民間企業にとって有利な取引ができるよう手助けをしているとの疑惑がある[51]．また世論に大きな影響力を与える政治家や有名人などを対象とした盗聴活動も行なっており，個人ではローマ法王や故マザー・テレサ，民間団体ではグリーンピース(環境保護団体)，アムネスティ・インターナショナル(人権保護団体)などが盗聴対象にされていたとする証言もある[52]．こうした盗聴活動は国境を越え，法的な許可を得ないまま非合法に行なわれている．

(4) エシュロンの動向

エシュロンのこれらの活動に対し，欧州評議会とフランスは国民のプライバシー保護や，民間企業を対象とした機密情報の盗聴により，企業間の公正な取引を侵害されているとして，エシュロン特別委員会を設置し独自に調査活動を行った．だが個人や企業のプライバシーを侵害している明白な証拠は見つからず，2001 年 9 月に欧州議会で採択された報告書の中で独自の暗号技術を用いて暗号化された電子メールの常用により，情報を保護するしかないとの結論を出している[53]．また米国ではプライバシー保護の観点からエシュロンの行動を規制しようとする動きが議会を中心に強まっており，英国やニュージーランドでも情報機関による自国の市民や企業に対する盗聴活動を規制しようとする動きが強まっている[54]．

4. 情報機関による盗聴行為の弊害

外国情報機関による盗聴を防ぐには．国際協定で盗聴行為を規制し，暗号化ソフトウェアの普及を促進させるなどの対策が考えられる．だが情報機関の活動は国家の安全保障に関わる問題であることが多く，国際的な規制の対象になりにくい．そのため，情報機関組織内部の自己規制に頼るしかないのが現状である．米国は2001年以降，情報収集能力が国家の命運を決めるとしてNSAを含む情報機関の強化を打ち出しており，情報機関が行っている盗聴行為を規制するのは難しい状況である[55].

エシュロンをはじめとした情報機関の盗聴に対抗するには，企業や研究機関，個人などが自らのプライバシーを自身で自衛していくしかない．具体的には暗号化ソフトウェアを使用してプライバシーや機密事項を含むメールを暗号化し，情報を読み取りにくくするなど情報を暗号化する工夫が有効である．だが，暗号化ソフトの普及により暗号化された情報の流通量が増加すればエシュロンの情報収集活動に支障を与えかねないとし，米国政府は暗号化ソフトウェアを開発している企業に対して，暗号の強度を落として解読しやすいものに限定し，ソフトウェアの仕様書や暗号を解読するマスターパスワードを，政府情報機関に提出しなければ販売できないようにする販売輸出規制を行なっている[56]．より確実なプライバシー保護を考えるのであれば，多数普及している米国製の商用ソフトウェアではなく，オープンソースコミュニティで開発された暗号化ソフトウェアの導入や，米国依存の情報産業の体制を改め，独自規格の暗号化ソフトウェアを新たに開発する必要がある．

情報革命は一般市民に恩恵をもたらす一方，国家機関が国民の通信を監視するための近代的な技術を得ることも可能にした．エシュロンのような通信傍受システムの出現は，高度監視社会の到来を告げているものと見ることができる．企業秘密や個人のプライバシーをどうやって守るべきなのか，積極的に議論する必要がある．

おわりに

便利な道具には使い方次第で凶器になり得るものも多い．それはコンピュータも同じである．インターネットは便利なものであるが，知らない誰かのコンピュータと相互に繋がっており，誰もが第三者によるサイバー攻撃の被害者になりかねない危険な側面も持っている．そのため利用者側がこうしたインターネットの危険性を認識し，自分の身は自分で守るという意識を高めていく必要がある．インターネットでは国境の壁が無いため，こうした自己責任の原則が求められるようになってきている．しかしセキュリティ対策といっても幅が広く万全な対策はないため，一人で手に負えるようなものではない．そのため一方的にコンピュータの所有者に責任を押し付けるのではなく，誰もが安心して使えるようなシステムをソフトウェアメーカーが提供することが，セキュリティ対策における一番の良策であろう．コンピュータの設定を特別に弄らなくても安全が確保されるよう，コンピュータメーカーやソフトウェアベンダーは努力するべきである．加えて国や企業は一般市民に対してセキュリティ教育を充実させるべきである．

インターネットの一般家庭への普及は，インターネット上を流れる通信情報を国家機関が盗聴することで，国民の思想や行動を監視することができる社会を作りあげる危険性もあることが明らかになった．第3章で述べたようにインターネットを流れる情報を盗聴することは，手紙や電話といった従来の情報伝達手段を盗聴するのに比べると簡単であることが明らかである．米国をはじめとした海外の諜報機関が，テロ対策や犯罪捜査を目的として，電子メールの盗聴装置を設置している．これらの高度な盗聴装

置の設置は，有史以来の高度な監視社会が整備されはじめていることを示していると考える．極論ではあるが，IT 革命と呼ばれるほどの情報通信技術の革新は，国民を監視する技術をも発展させており，我々の知らない間に監視社会が進んでいるのである．我々はこのような課題の解決にも取り組んでいかなければならない．

引用文献

[1]ダン・バードン，『ブラックアイス―サイバーテロの見えない恐怖』2003 年 株式会社インプレス p. xvi.

[2]IT 用語辞典 e-Words，「サイバー攻撃関連のニュース」，http://e-words.jp/

[3]ダン・バードン，『ブラックアイス―サイバーテロの見えない恐怖』2003 年 株式会社インプレス p. xi.

[4]National Infrastructure Protection Center Highlights June 15, 2001 p. 2.
(http://permanent.access.gpo.gov/websites/www.nipc.gov/publications/highlights/highlights2001.htm)

[5]宮脇磊介，『サイバークライシス―「見えない敵」に侵される日本』(PHP 研究所，2003) p. 104.

[6]安保克也，下畑法近，『ネットワーク時代のテロリズム しのび寄る脅威との闘い・サイバーセキュリティ』(三修社，2003) p. 12.

[7]江畑謙介，「軍事 サイバーテロ」『世界』2000 年 7 月号 岩波書店 p. 107.

[8]安保克也，下畑法近，『ネットワーク時代のテロリズム しのび寄る脅威との闘い・サイバーセキュリティ』(三修社，2003) p. 55.

[9]宮脇磊介，『サイバークライシス―「見えない敵」に侵される日本』(PHP 研究所，2001) p. 39.

[10]宮脇磊介，『サイバークライシス―「見えない敵」に侵される日本』(PHP 研究所，2001) p. 40.

[11]宮脇磊介，『サイバークライシス―「見えない敵」に侵される日本』(PHP 研究所，2001) p. 43.

[12]吉原恒淑，『サイバー攻撃態勢を整える中国軍事戦略の脅威』フォーサイト 2002 年 9 月号 新潮社 p. 36.

[13]宮脇磊介，『サイバークライシス―「見えない敵」に侵される日本』(PHP 研究所，2001) p. 22.

[14]宮脇磊介，『サイバークライシス―「見えない敵」に侵される日本』(PHP 研究所，2001) p. 30.

[15]メリンダ・リウ，「サイバー戦争の危うい影」『ニューズウィーク日本版』2000 年 3 月 22 日号 p18

[16]吉原恒淑，『サイバー攻撃態勢を整える中国軍事戦略の脅威』フォーサイト 2002 年 9 月号 新潮社 p. 35.

[17]ジェイムズ・アダムズ，『「サイバー戦争」はすでに始まっている』フォーサイト 2000 年 4 月号 新潮社 p. 107

[18]藤原宏高，『サイバースペースと法規制』(日本経済新聞社，1997) p. 18.

[19]「不正アクセス行為の禁止等に関する法律」，情報処理推進機構，(http://www.ipa.go.jp/)
(http://www.ipa.go.jp/security/ciadr/law199908.html)

[20]中田光一，「サイバーテロ対策の現状と取組み」『法律のひろば』2002 年 3 月号 帝国地方行政学会 p. 21.

[21]中田光一，「サイバーテロ対策の現状と取組み」『法律のひろば』2002 年 3 月号 p. 25.-27.

[22]外務省，「サイバー犯罪に関する条約」（略称：サイバー犯罪条約）
(http://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html)

[23]矢野直明，『インターネット術語集 II』(岩波新書，2002) p. 109.

[24]矢野直明，『インターネット術語集』(岩波新書，2000) p. 128.

[25]山下幸夫，「サイバー犯罪条約が日本の捜査活動を拡大する」『中央公論』2002 年 10 月号 反省社 p. 155.

[26]松尾正浩，山口英，「内外 CSIRT の現状」『情報処理』第 42 巻 第 12 号 情報処理学会 p. 1164.

[27]JPCERT/CC, http://www.jpcert.or.jp/
[28]松尾正浩，山口英，「内外 CSIRT の現状」『情報処理』第 42 巻 第 12 号 情報処理学会 p. 1165.
[29]First, https://www.first.org/about/
[30]佐々木良一，「インシデント・レスポンスのための組織」，
(http://www.cyberpolice.go.jp/column/index.html)
[31]松尾正浩，山口英，「内外 CSIRT の現状」『情報処理』第 42 巻 第 12 号 情報処理学会 p. 1168.
[32]湯木進悟，「中国に紅旗 Linux あり」『MYCOM PC WEB』毎日コミュニケーションズ，
(http://pcweb.mycom.co.jp/articles/2004/03/31/redflaglinux/)
[33]川崎貴一，『インターネット犯罪』(文藝春秋，2001) p. 200.
[34]湯木進悟，「中国に紅旗 Linux あり」『MYCOM PC WEB』毎日コミュニケーションズ，
(http://pcweb.mycom.co.jp/articles/2004/03/31/redflaglinux/)
[35]NTT データ国際事業推進本部，「中国の電子商取引（EC）：発展する市場と IT 政策」，デジタルガバメント，
アジアマンスリーニュース 2004 年 12 月号，(http://e-public.nttdata.co.jp/index.htm)
[36]莫邦富，「中国が模索するサイバー戦略の内幕」『フォーサイト』新潮社 2000 年 3 月号 p. 39.
[37]莫邦富，「中国が模索するサイバー戦略の内幕」『フォーサイト』新潮社 2000 年 3 月号 p. 39.
[39]莫邦富，「中国が模索するサイバー戦略の内幕」『フォーサイト』新潮社 2000 年 3 月号 p. 39.
[39]宮脇磊介，『サイバークライシス—「見えない敵」に侵される日本』(PHP 研究所，2001) p. 60.
[40]長谷川英一，「米国におけるサイバー・セキュリティ政策関連動向」，ニューヨーク情報サービス産業懇話会，
(http://www.jif.org/column/0010/1.html)
[41]産経新聞特別取材班，「エシュロン—アメリカの世界支配と情報戦略」(角川書店，2001) p. 115
[42]産経新聞特別取材班，「エシュロン—アメリカの世界支配と情報戦略」(角川書店，2001) p. 116
[43]Wired News，FBI が『カーニボー』を廃止、商用ソフトに切り替え
(http://hotwired.goo.ne.jp/news/culture/story/20050120202.html)
[44]岸本卓也，「史上最強の盗聴機関エシュロン」『世界』2000 年 7 月号 岩波書店 p. 103.
[45]岸本卓也，「米英の盗聴システム「エシュロン」の脅威」，
『エコノミスト』2001 年 6 月 26 日号 毎日新聞社 p. 42.
[46]鍛冶俊樹，「秘密組織の通信傍受網「エシュロン」の姿が見えてきた」
『エコノミスト』2000 年 5 月 23 日号 毎日新聞社 p. 50.
[47]岸本卓也，「米英の盗聴システム「エシュロン」の脅威」
『エコノミスト』2001 年 6 月 26 日号 毎日新聞社 p. 45.
[48]鍛冶俊樹，「秘密組織の通信傍受網「エシュロン」の姿が見えてきた」
『エコノミスト』2000 年 5 月 23 日号 毎日新聞社 p. 50.
[49]岸本卓也，「米英の盗聴システム「エシュロン」の脅威」
『エコノミスト』2001 年 6 月 26 日号 毎日新聞社 p. 44.
[50]ダンカン・キャンベル，「通信諜報包囲網・エシュロンの実態」『世界』2000 年 10 月号 岩波書店 p. 213.
[51]ダンカン・キャンベル，「通信諜報包囲網・エシュロンの実態」『世界』2000 年 10 月号 岩波書店 p. 216.
[52]岸本卓也，「米英の盗聴システム「エシュロン」の脅威」
『エコノミスト』2001 年 6 月 26 日号 毎日新聞社 p. 43.
[54]産経新聞特別取材班，「エシュロン—アメリカの世界支配と情報戦略」(角川書店，2001) p. 200

[54]岸本卓也, 「史上最強の盗聴機関エシュロン」『世界』2000年7月号 岩波書店 p. 105.

[55]岸本卓也, 「米英の盗聴システム「エシュロン」の脅威」
『エコノミスト』2001年6月26日号 毎日新聞社 p. 45.

[56]岸本卓也, 「史上最強の盗聴機関エシュロン」『世界』2000年7月号 岩波書店 p. 106.

参考文献

01) 安保克也(他 著), 『ネットワーク時代のテロリズム しのび寄る脅威との戦い・サイバーセキュリティ』(三修社, 2003)

02) 石川巌, 「エシュロン関連部隊の分遣隊が駐屯 三沢のエシュロン疑惑と射撃場」『軍事研究』2000年12月号 (ジャパンミリタリー・レビュー)

02) 上田正尚, 『情報セキュリティーの現状と動向』(日本国際問題研究所, 2002)

03) 歌代和正「商用ネットワークにおけるネットワークセキュリティ確保の取り組み」『情報処理』Vol.42 No.12 (情報処理学会, 2001)

03) 江畑謙介, 「サイバー・テロ(特集 ネット社会—何が起きているのか—サイバースペース最前線)」『世界』2000年7月号(岩波書店)

04) 江口謙介, 「軍事情報 進まないサイバーテロ対策と中国のサイバー戦能力」『世界週報』2001年1月2日号(時事通信社)

05) 大河原克行, 「サイバーテロ 目に見えるテロより恐ろしいIT社会の魔の手(特別リポート)」『エコノミスト』2001年10月23日号(毎日新聞社)

06) 岡田仁志, 『情報通信ネットワークに対する脅威の実態』(日本国際問題研究所, 2002)

07) 鍛冶俊樹, 「エシュロンへの反発も薄れ「反テロ」で結束する大国情報機関」『エコノミスト』2002年1月8日号(毎日新聞社)

08) 鍛冶俊樹, 『エシュロンと情報戦争』(文藝春秋, 2002)

09) 鍛冶俊樹, 「秘密組織の通信傍受網『エシュロン』の姿が見えてきた」『エコノミスト』2000年5月23日号(毎日新聞社)

10) 加藤朗, 『サイバー脅威と日本の安全保障』(日本国際問題研究所, 2002)

11) 川上高司, 『テロリストの情報戦争(IW)と日米協力』(日本国際問題研究所, 2002)

12) 河﨑貴一, 『インターネット犯罪』(文藝春秋, 2001)

13) サイバー刑事法研究会, 『欧州評議会サイバー犯罪条約と我が国の対応について』(経済産業省, 2002)

14) 産経新聞特別取材班, 『エシュロン—アメリカの世界支配と情報戦略』(角川書店, 2001)

15) ジェイムズ・アダムズ, 「『サイバー戦争』はすでに始まっている」『フォーサイト』2000年4月号 (新潮社)

16) 情報処理推進機構, 『情報セキュリティの現状』(独立行政法人 情報処理推進機構, 2002)

17) 岸本卓也, 「史上最強の盗聴機関エシュロン」『世界』2000年7月号 (岩波書店)

18) 岸本卓也, 「欧州評議会報告書草案を入手 米英の盗聴システム『エシュロン』の実態」『エコノミスト』2001年6月26日号 (毎日新聞社)

19) 佐々木良一,『インターネットセキュリティ入門』(岩波書店, 1999)

20) 大規模プラント・ネットワーク・セキュリティ対策委員会, 『大規模プラント・ネットワーク・セキュリティについて ～重要システムのサイバーテロリズム・クラッキング対策のあり方～』(通商産業省, 2000)
21) ダンガン・キャンベル, 「通信諜報包囲網・エシュロンの実態」『世界』2000年10月号 (岩波書店)
22) ダンガン・キャンベル, 「閉鎖されるエシュロンの主要基地」『世界』2001年8月号 (岩波書店)
23) ダン・バートン(星睦 訳),『ブラックアイス～サイバーテロの見えない恐怖～』(インプレス, 2003)
24) 喬良(他 著), 『超限戦 21世紀の「新しい戦争」』(角川書店, 2001)
25) 寺島実郎, 「IT革命の影としてのエシュロン」『世界』2002年7月号 (岩波書店)
26) 戸村哲, 「我が国政府におけるネットワークセキュリティ確立への取り組み」『情報処理』Vol.42 Vol.12 (情報処理学会, 2001)
26) 中田光一, 「サイバーテロ対策の現状と取組み」『法律のひろば』2002年3月号 (帝国地方行政学会)
27) 橋本靖明, 『法的側面から見たサイバーテロ』(日本国際問題研究所, 2002)
28) 浜田和幸, 『サイバーテロ—ITと金融ビジネスのアキレス腱』(PHP研究所, 2000)
28) 林紘一郎(他 著),『IT2001—何が問題か』(岩波書店, 2000)
29) 古谷幸広(他 著),『インターネットが変える世界』(岩波書店, 1996)
30) 藤原宏高, 『サイバースペースと法規制』(日本経済新聞社, 1997)
30) 星野俊也, 『サイバー空間における脅威と安全保障・危機管理のあり方』(日本国際問題研究所, 2002)
31) 松尾正浩(他 著), 『内外CSIRTの現状』「情報処理」Vol.42 No.12 (情報処理学会, 2001)
31) 宮脇磊介,『サイバークライシス—「見えない敵」に侵される日本』(PHP研究所, 2001)
32) 宮脇磊介, 『経済広報 2001年5月号「国家の危機管理・企業の危機管理を考えるリテラシー」』(経済広報センター, 2001)
33) 村井純,『インターネット』(岩波書店, 1995)
35) 村瀬一郎、鈴木裕信, 「国外の政府レベルのネットワークセキュリティ確立への取り組み」『情報処理』Vol.42 No.12 (情報処理学会, 2001)
34) メリンダ・リウ, 「サイバー戦争の危うい影 中台関係 中国のハッカーによる総統選の妨害に神経をとがらせる台湾当局」『ニューズウィーク日本版』2000年3月22日号(ティービーエス・ブリタニカ)
35) 莫邦富, 「中国が模索するサイバー戦略の内幕」『フォーサイト』2000年3月号(新潮社)
36) 矢沢修次郎, 『ネットワーク社会化と紛争形態の変化—ハードな安全保障からソフトな安全保障へ』(日本国際問題研究所, 2002)
37) 矢野直明,『インターネット術語集』(岩波書店, 2000)
38) 矢野直明, 『インターネット術語集 II』(岩波書店, 2002)
38) 山口英, 「ネットワークセキュリティに係る動向」『情報処理』Vol.42 No.12 (情報処理学会, 2001)
38) 山下幸夫, 「サイバー犯罪条約が日本の捜査活動を拡大する(特集 情報管理社会はここまで来ている)」『中央公論』2002年10月号(反省社)
39) 山下幸夫, 「『サイバー犯罪条約』が日本の捜査活動を拡大する」『中央公論』2002年10月号(反省社)
40) 湯川鶴章, 「歴史教科書問題で日本狙うサイバーテロ(IT革命最前線[33])」『世界週報』 2001年5月8/15日号 (時事通信社)
41) 吉原恒淑, 「サイバー攻撃態勢を整える中国軍事戦略の脅威」『フォーサイト』2002年9月号(新潮社)
42) 吉村英二, 「『自由の檻』を超えて エシュロンと私たちの自由(リレー連載・監視社会[2])」『技術と人間』2002年4月号(技術と人間)