第三章　サイバー脅威と日本の安全保障

加藤　　朗

１．はじめに

コンピュータが姿を現したのは、1940年代半ばのことであり、それほど古い話ではない。しかしながら、現代社会の生活を営む上で、不可欠なものとなっている。インターネットはいうに及ばず、道行く自動車のエンジンはマイクロコンピュータで制御されているし、金融システム、電話回線などもまた巨大なコンピュータによって管理されている。現代社会において、コンピュータに全く依存することなく機能している要素を見つけることはきわめて困難になってきているのである。

しかしその一方で、コンピュータシステムに対する電子的攻撃、いわゆるサイバー攻撃の脅威が高まってきている。果たしてそれはどのようなものなのか、またどのような対策が可能なのか。本稿ではその問題について分析することとしたい。

２．サイバー脅威とは何か

本稿の目的は、サイバー脅威が日本の安全保障に与える影響について分析することである。その前にまず、サイバー脅威とはどのようなものなのかを明らかにしておきたい。情報化時代の戦争形態について精緻に分析したものとして米国防大学のマーチン・リビッキの研究があるが(注1)、それによればサイバー戦は情報戦争（information　warfare）の１つの形態として位置づけられている。国防省の定義によれば、情報戦争とは、「情報優勢を獲得するため、敵の情報及び情報システムに対して行われる各種の行動。その際、味方の情報および情報システムの防護も並行的に行われる。（Actions taken to achieve information superiority by affecting adversary information, information-based processes, an information systems while defending one's own information, information-based process, and information systems.）」ものとされている(注2)。このサブカテゴリーとしてサイバー戦を考えるのならば、「コンピュータとネットワークからなる電子的空間において、情報の攻防を行う情報戦争の一形態」ということになろう。

(1) 一般的な特徴

コンピュータのネットワーク化が爆発的に進むようになったきっかけは、いうまでもなく、米国国防省がインターネットを民間に開放するようになったことである。現在、コンピュータのネットワークは、各企業や官庁内部で構成される LAN（Local Area Network）あるい

は家庭の個別の端末が、インターネットによって相互に結ばれている形を取っている。多くの場合、サイバー攻撃の対象となるのはこの中で企業や官庁の LAN を構成しているコンピュータである。従って、サイバー攻撃とは、具体的には LAN 内の特定のコンピュータのデータを窃取・改竄するか、そのコンピュータによって制御されているハードウエアを外部から制御するという形を取ることになろう。攻撃者は、 LAN の内側にいることもあれば、外側にいることもある。そして後者の場合には、攻撃はインターネット経由でなされることになるのである。インターネットは現在世界中からアクセスすることが可能であるから、インターネット経由で攻撃を行う場合には、物理的距離や国境によって制約を受けることはない。

サイバー攻撃の最大の特徴は、ネットワークに接続されたコンピュータと、コンピュータやネットワークに関する知識を持っていれば行うことができるということである。従来型の物理的攻撃であれば、ある程度の量の火器をそろえるとともに、それらを扱う人員を訓練しなければならないが、それには多大の経費と時間を必要とするため、かなりの規模の組織的な活動を行わなければならない。しかし、サイバー攻撃に関しては、個人レベルであっても国家と匹敵する攻撃を行うことが、理論的には可能なのである。

(2) 攻撃方法

今述べたように、サイバー攻撃のエントリーコストはきわめて低い。また、攻撃手段となるソフトウエアツールはインターネット上のハッカーサイトから容易に入手可能である。

ウイルス

自分自身を複製し、ネットワーク経由でほかのコンピュータに感染する能力を持ち、感染したコンピュータのデータを消去したりパスワードを窃取したりするプログラムをウイルスという。「I love you ウイルス」のように、電子メールの添付ファイルにウイルスを潜ませて送付するのがもっとも典型的な形態である。特に、メール閲覧ソフトが、ある種のファイルに関しては自動読み込みするような設定になっている場合、感染する可能性は高くなる。

サービス拒否（Denial of Service）攻撃

通信ソフトウエアは、ある程度の通信量を想定して作成されている。従って、実際の通信量がその想定よりも多くなった場合には、そのソフトウエアは動作が不安定になったり機能が麻痺したりする。そうした状態を意図的に作り出すために、短時間に膨大な量の電子メールを送付することをサービス拒否（Denial of Service: DOS）攻撃という。ニムダウイルスが、ある特定の時間にホワイトハウスに大量の電子メールを送りつける設定になっていることが判明し、ホワイトハウスのコンピュータの IP アドレスを変更したことがあったが、その際意図されていたのがこの DOS 攻撃である。

セキュリティ・ホール攻撃

現代のコンピュータのソフトウエアは、きわめて複雑なアルゴリズムを持ち、膨大な行数のプログラム言語からなっている。そのため、どこかに「抜け穴」が生まれてしまうケースが多い。たとえば、あるソフトウエアに、「一時に5000文字以上の文字情報を受信した場合、その後の動作が不安定になる」といったようなセキュリティ・ホールがあった場合に、5000字以上の文字情報を送付して動作を不安定化し、攻撃者の意図する動作を実現させるようなことを行うことが、セキュリティ・ホール攻撃である。たとえば、オペレーティングソフトであるウインドウズや、インターネットブラウザであるインターネットエクスプローラなどには、時々セキュリティ・ホールが発見されるため、マイクロソフト側でそれを埋めるためのパッチが公開されている。

ロジック爆弾

ある条件下で起動し、攻撃側が意図する結果を引き起こすようなプログラムをソフトウエアの作成段階で埋め込むことが、ロジック爆弾である。世界中でウインドウズが使われている現在、その中にロジック爆弾が仕掛けられていたとしたらその影響はきわめて深刻なものとなる。たとえば、2000年12月31日23時59分59秒から、2001年１月１日０時０分０秒の間に、コンピュータにトラブルが発生するのではないかと考えられたいわゆる「Ｙ２Ｋ」事件は、意図されたものではないにしても、ある種のロジック爆弾がソフトウエアに存在していた事例である。

エミュレート

攻撃対象のコンピュータを、「正規のユーザー」として直接操作することがエミュレートである。コンピュータを直接操作することが最も簡単かつ確実な方法だが、正規ユーザーのパスワードを窃取することができれば、ネットワークを通じてアクセスし、正規のパスワードを入力することで目的のコンピュータにアクセスすることができるようになる。そうなれば、侵入者は正規ユーザーと同じサービスを受けることができることになる。侵入者が、内部の事情に通じた本当のインサイダーであることも考えられる。

(3) サイバー戦の脅威

現在のところ、サイバー戦の手段として想定されるのは、上記に列挙したようなものである。また、ネットワークサーバーは、正規と見なされるユーザーに対しては要求されたサービスを提供することになるため、ネットワークに接続されている限り、外部からの攻撃を完全に遮断することは不可能である。特に、技術的な専門知識を有する内部者が攻撃を行った場合、防御することはほとんど不可能である。

ただこれらは、結局のところコンピュータ内の電子的データに対する攻撃にすぎない。問

題なのは、こうした電子的攻撃が物理的な破壊に結びつくか否かである。この点について結論を先にいえば、イエスである。攻撃対象の LAN のホストコンピュータをエミュレートできれば、システムの起動や停止、本来と異なる動作など、あらゆる操作を実行できる。また、今やほとんどの工業製品に内蔵されている制御用のマイクロプロセッサに、たとえば○年○月○日に動作を停止するようなコードが書かれたロジック爆弾を埋め込むことができれば、社会全体にわたる混乱を引き起こすことができる。特に、サイバー攻撃によって通信や金融、生活インフラなどが重大な障害を受けた場合、深刻な社会不安が生起することになろう。

３．サイバー攻撃の限界

前項でみたように、サイバー攻撃には、現代社会の基盤であるコンピュータシステムを麻痺させる可能性が、あくまで理論的なものであるが存在する。しかし、現実の世界において運用すべき兵器システムとしてサイバー攻撃をとらえた場合には、そこに内包される限界が明らかになる。ここではそれを概観することとしたい。

(1) 防御手段

ファイアウォール

前述したように、ネットワークに接続されている限り、そこを経由した侵入を完璧に防御することは困難である。しかしながら、適切な防護措置を講じれば、かなりの程度侵入に対抗できる。そのひとつが、ファイアウォールである。ファイアウォールとは、LAN サーバーとインターネットの間に設置された、通信のフィルタリングを行うための専用コンピュータである(注3)。ファイアウォールは、通信内容や送信元の情報を常に監視しており、ある基準を満たすような通信が内部に侵入するのを阻止するための処理を行っている。たとえば、不正侵入の兆候であるログイン試行と失敗の反復、コンピュータの内部情報を探るようなアクセス、既知の侵入パターンによる攻撃、ブラックリストに含まれるインターネットサイトからのアクセスなどが、ファイアウォールによって監視されている。

こうした処理は、純粋にデジタル的に行われている。すなわち、イエスかノーの二者択一であり、中間は存在しない。この点が、プロトコルの戦いであるサイバー戦と従来の物理的な武力行使との決定的な違いの１つである。数学的論理に支配されるサイバー戦と異なり、物理現象に支配されるこれまでの戦闘においては、100％目標に命中するミサイルや、全く役に立たない装甲など存在しない。兵器の効果はあくまで確率によって決定されてきたのである。しかし、サイバー戦とは純粋に論理的なものであり、防護基準に抵触するアクセスは100%排除されるのである。そう考えれば、有効な攻撃方法は事実上有限であることから、既知の侵入パターンの排除が可能なファイアウォールは非常に有効な手段

であり、コンピュータが侵入される可能性を大幅に低下させることができる。他方、これまでの防護基準に引っかからないような新しい種類の攻撃に対応することは不可能であることには注意しなければならない。

なお、もっとも確実な侵入防護手段は、もちろん外部のネットワークから物理的に切り離すことである。物理的に接続されていないコンピュータにアクセスすることは不可能であるから、重要なシステムを運用する間は外部ネットワークから切断することが、最も有効な防護手段となる。

ワクチン

ワクチンとは、コンピュータ内に潜んでいるウイルスを検出し、必要があればそれを駆除するソフトウエアのことである。現在のところ、世界に存在するネットワークサーバーの大半がユニックスやウインドウズであること、潜伏・感染の手法は対象システムの種類によって限定されることから、ウイルスの種類も無限にはならない。また、ウイルスを作成するためには対象システムに関する高度な知識が必要であることから、潜伏性が高く感染力の強い悪性のウイルスは、それほど数多く存在するわけではない(注4)。

物理的破壊の問題

制御コンピュータをエミュレートしたりロジック爆弾を仕掛けることによって、列車を衝突させたり、飛行機を墜落させたりといった物理的な破壊活動を行うことは、原理的には可能である。しかしながら、サイバー攻撃の技術だけでこうした理論的可能性を実行に移すことは不可能である。たとえば、列車を衝突させるためには、攻撃者が列車制御システムに侵入するだけではなく、列車制御システムの構成や操作手順、あるいは鉄道運行ダイヤグラムの構造を熟知していなければならない。ウインドウズのような汎用システムならともかく、列車制御システムのようなカスタムシステムの場合は、そのシステム固有の概念を熟知していなければ、大事故を引き起こすことはできないのである。同じように、飛行機を墜落させるにも、管制システムの構造や人間の判断に基づくバックアップシステムなど、持っておかなければならない知識は数多くある。そのシステムの運用に長けたインサイダーでない限り、コンピュータに関する知識と、こうしたカスタムシステムの運用に関する知識を共に身につけることはきわめて難しい。逆に言えば、インサイダー自身が攻撃者であるか、インサイダーの協力を得ることができれば、物理的破壊に結びつくようなサイバー攻撃を行うことは可能だということでもある。

被害復旧

サイバー攻撃は、物理的破壊だけではなく、データの改竄や窃取といった電子的破壊を目的とすることも考えられる。たとえば銀行のオンラインシステムが攻撃され、データが大幅に書き換えられた場合、社会が受ける打撃は計り知れない。

ただ、確かにこうした攻撃によって大きな混乱は引き起こされるだろうが、復旧することは不可能ではない。コンピュータネットワークが物理的に破壊されたのではない限り、バックアップを用いることによってデータの復旧は短時間で行うことが可能になる。もちろん、破壊された情報を復旧させるためには、データを頻繁にバックアップしておくことが必要である。ただ、その作業は、面倒なことをのぞけば、きわめて有効なサイバー攻撃対策なのである。

(2) 軍事的脅威としてのサイバー戦

以上で検討したように、サイバー戦を完全に防護することは困難だが、同時に限界も存在している。

まず、サイバー戦とはプロトコルの戦いであり、侵入自体を100%防ぐことは難しい一方で、ある攻撃を100%防護することが可能だということを指摘しなければならない。この点もまた、物理的な戦闘との相違である。ねらって放たれた銃砲弾から自らを完全に防護することは難しいが、既知のウイルスであれば、それを駆除することは100%可能なのである。特に、ファイアウォール、ワクチン、バックアップの重要性は、どんなに強調しても強調しすぎることはない。

次に、物理的な破壊を伴う攻撃を行うことは普通考えられているよりも困難であることも指摘しなければならない。物理的破壊をもたらすためには、コンピュータに関する知識だけではなく、攻撃対象となっているシステムに関する専門的な知識が必要なのである。ただし、インサイダーが攻撃者であったり、攻撃に協力したりする場合に、この困難さは解消する。そう考えると、個人的なセキュリティ・クリアランスの確保などがサイバー戦対策として重要だということである。

以上の分析をふまえれば、軍事的脅威としてのサイバー攻撃についても、自らある姿を描き出すことができる。軍事的手段としてのサイバー攻撃には、２つの種類がある。

まず第１は、軍事的目標に対する攻撃である。たとえば、開戦劈頭の数分間だけでも相手側の警戒監視システムや指揮統制システムを無力化することができれば、奇襲的攻撃によって相手の軍事力のほとんどを破壊することができる。もう１つは、社会インフラに対する攻撃である。

しかし、いずれにしても、さまざまな限界がある。まず、軍事的手段に要求されることは、効果が確実なことである。たとえばレーダー基地を目標に発射された対レーダーミサイルは、ほぼ確実に目標を破壊することができるのである。命中率の問題はあるにしても、それは攻撃弾数を増やすことによって確率的に解決することができる。しかしながら、サイバー攻撃の場合には、その効果がきわめて不確実である。適切な防護措置がとられていれば、データ

の改竄や相手のシステムの誤動作を引き起こすことは難しくなる。このように効果が不確実である以上、軍事的手段としての信頼性は低くならざるを得ない。相手の指揮統制システムが無力化されたかどうかわからない時点で、攻撃部隊を送り込むことはきわめて危険である。したがって、何らの予備情報もなしに、奇襲的攻撃の補助手段としてサイバー攻撃を用いる可能性は低いと考えられる。

ただし、相手の防護体制に関して確実な情報を把握することができていれば状況は異なる。繰り返し述べているように、サイバー攻撃は、ある種の攻撃に関しては100%防護可能だが、ある種の攻撃に関しては100%防護不可能である。したがって、相手側システムのセキュリティホールなり侵入パスワードなりを平時から探知することができていれば、有事の際にそこを衝くことによって大きな効果を得ることができる。そう考えると、サイバー戦において重要なのは、平時における伝統的な意味での情報戦、諜報戦ということになろう。

次の社会インフラに対する攻撃だが、これも前述したとおり、物理的破壊をもたらすようなサイバー攻撃を行うことは困難である。特に、十分な時間、資金、人材を投入して適切な防護措置をとっている社会であれば、システムに侵入すること自体が困難であるし、まして特殊なシステムを外部から誤動作させるためにはさまざまな特殊知識が必要とされる。ただし、前述したように、インサイダー協力者の問題はどうしても残る。すなわち、攻撃したいシステムを運営しているインサイダー協力者をリクルートすることができれば、その人物を通じて攻撃を行うことができるからである。たとえば、電力システムを運用しているエンジニアそれぞれの金銭的・異性スキャンダルなどの個人的弱点や思想的志向に関する精緻な調査を行い、必要とされる人物に工作を行って自らのエージェントにするようなことがきわめて有効な手段なのである。そう考えると、ここにおいてもやはり重要なのは、平時における伝統的な意味での情報戦・諜報戦ということになる。

４．日本のサイバー攻撃対策

ここまでサイバー攻撃の脅威について分析してきたが、結論としていえることは、適切な措置を講じていればサイバー攻撃からの防護は可能である以上、十分な時間、資金、人材を投入して防護体制を構築する必要があること、また伝統的な意味での情報戦・諜報戦が大きな意味を持つことである。そこで最後に、我が国においてどのようなサイバー戦対策がとられているかをみることとしたい。

まず、平成11年９月には、古川官房副長官を議長として、内閣官房および関係12省庁による情報セキュリティ関係省庁局長等会議が発足し、12年の１月21日には、そこから「ハッカー対策等の基盤整備にかかる行動計画」が決定されている。しかしその矢先の24日に、政府関係機関のホームページが改竄されるという事件が発生したこともあり、２月には「不正アクセス行為の禁止

等に関する法律」が施行される。そして、２月29日には内閣安全保障・危機管理室に情報セキュリティ対策推進室が設置され、その後はその部局を中心としてサイバー攻撃対策が進められることになる。そこでは、情報セキュリティポリシーに関するガイドライン（12年７月決定）や、重要インフラのサイバーテロ対策に係る特別行動計画（12年12月決定）、サイバーテロ対策に係わる官民の連携・連絡体制、電子政府の情報セキュリティ確保などが検討されている。

しかし、その年の５月には、I love you ウイルス問題が発生し、13年２月には中国語のホームページに、日本のサイトへの攻撃を予告する内容が掲載され、DOS 攻撃をはじめとする被害が国内で発生するという事件があった。これまでのところ、日本に対するサイバー攻撃は、ホームページの改竄であったり、企業のウェブサーバーへの DOS 攻撃といった、それほど害の大きくないものであったが、それでもサイバー攻撃の脅威が高まっていることが一般に認識されるようになった。そのため、IT 戦略本部で作成された「e-Japan 重点計画」において、「高度情報通信ネットワークの安全性および信頼性の確保」に向けた施策がとりまとめられているなど、行政レベルではさまざまな対策が進められている。

ただし、これらはあくまで防護のための指針を提示したものであって、実際に十分な防護措置をとるかどうかはまた別の問題である。それについては今後投入する資金や人材によって左右される。

これまで述べてきたように、サイバー攻撃から防護する手だては、電子的なものには限られない。特に重要なのは、インサイダー協力者への予防策であり、今後検討しなければならない課題である。情報戦・諜報戦は日本がもっとも苦手とする分野ではあるが、官庁、自衛隊、企業内にインサイダー協力者を作られることがないように、個人レベルのセキュリティの確保も重視していかなければならない。

また、サイバー攻撃対策としてもう１つ重視されているのが「結果管理(consequence management)」と呼ばれる手法である。前述したとおり、システムへの侵入それ自体を阻止することはきわめて難しい。もちろん防護措置をとることによってほとんどの問題は解決するにしても、それでもある程度被害を受ける可能性は残る。そのため、予防することだけを考えるのではなく、何らかの被害がでることを前提として、それが連鎖反応的な打撃をもたらさないように、ダメージコントロールのための措置をとっておくことが結果管理という概念である。こうした考え方にたった対策も必要となろう。

５．まとめ

コンピュータなしでは、現代の社会は一瞬たりとも機能することはできない。確かにそのことによって人間の生活は飛躍的に便利になったが、同時に新たな脆弱性が生まれることとなった。サイバー攻撃とは、その脆弱な部分を標的とする新たな脅威である。しかし、サイバー攻撃の脅

威は、時として誇張されすぎるきらいがある。確かに、コンピュータが麻痺したり、データが信頼できなくなってしまったらその影響は計り知れないものがある。しかし、適切な防護措置さえ施されていれば、対応可能な程度にダメージを押さえることは十分に可能なのである。サイバー攻撃対策を考える上で求められることは、決して油断することなく、かつ過度に恐れないことなのである。

－ 注 －

1．Martin C. Libicki, *What is Information Warfare?* (Washington,D.C.: U.S. Government Printing Office,1995)

2．Department of Defense, *Glossary of Defense Acquisition Management Acronyms and Terms* (2001), (Jan 2001), http://www.dsmc.dsm.mil/pubs/glossary

3．もちろん、サーバー内にソフトウエアとしてファイアウォール機能を付加することも可能である。

4．たとえば、I love you ウイルスが感染するのはウインドウズコンピュータだけであり、マッキントッシュには感染しなかった。なお、I love you ウイルスは Visual BASIC と呼ばれるコードで書かれたきわめて初歩的なものであり、それほど悪性なものではなかった。