第二章　情報通信ネットワークに対する脅威の実態

岡田　仁志

１．はじめに

情報通信ネットワークの高度利用は、国民生活を豊かにする可能性を持つ反面において、その脆弱性を突いたサイバーテロリズムの勃発やハイテク犯罪の多発など新しいタイプの脅威を招くおそれがある。こうした事態が起こると、企業や個人の利益に対してのみならず国家の安全保障にとっても重大な挑戦となる。

そこで、情報通信ネットワークに対する脅威の実態について、ハッカーの概念や歴史をたどって現状を把握し、これに対抗する側の状況として、米国における重要インフラ施設保護対策の日本への適用可能性についてふれ、さらにはこうした危機を管理する高度な手段としての国際通信傍受網エシュロンについて、その実効性と諸課題について論じる。

２．情報通信ネットワークの高度利用と脅威の拡大

情報通信ネットワークに対する日常的な脅威として存在するのがハッカーによる攻撃である。ハッカーの概念についてはインターネット黎明期から様々な区分がなされているが、万民に共通して認識された表現は存在しない。基本的には「工学的な技術の習熟度合いが高度であり、常に技術に対し情熱的である人物」を指すと考えられている。その延長線上に「技術と熱意を、悪意もって利用する、もしくは結果的に悪意であると判断される行為を行う人物」を意味するクラッカーと呼ばれる層がある。

(1) ハッカーの歴史

ハッカーの歴史は1980年代、米国における防衛インフラである回線網が学術機関へ解放されたインターネット黎明期に遡る。これら学術機関への開放とともに利用が促進されハッカーと呼ばれる層が生成されたと考える。技術の汎用性と利用者の急速な拡大とともに、ハッカーという呼称が一般化し、明確な区分を持たずインターネット上で高いスキルを持つ層を総称して呼ばれるようになった。

(2) サイバーテロリストの存在について

それらハッカーの中で、これまで見られなかった政治・思想などを活動の源泉とするサイバーテロリストと呼ばれる層が顕在化している。これらハッカーについては以下のように簡

単に定義を試みた。

A：サイバーテロリスト：広義の解釈

インターネット等の通信技術に高いスキルを有し、通信インフラを利用することにより、何らかの破壊活動を行う人物。その活動には根幹的な理由および思想が存在する。

B：サイバーテロリスト：狭義の解釈

・インターネット等の通信インフラを利用し、テロ活動に関わる情報の交信等の活動を行うもの

・インターネット等の通信インフラを利用し、実際の破壊行為のツールとして利用する活動を行うもの

・インターネット等の通信インフラを利用し、テロ活動の正当性を流布する目的に利用する活動を行うもの

３．ハッカーおよびサイバーテロリストの攻撃環境

インターネットを利用して、何らかの破壊活動および準備活動を行う場合、そこには地理的制限、時間的制限などは存在しない。基本的には国家的な制限すら存在しない。コスト的に考えても対効果費用に換算した場合、非常に廉価なものであると考えられる。基本的には高度なスキルを有したハッカーが、悪意を持って環境を利用した場合には以下のような利用が想定される。

A：記憶装置あるいは通信装置としてのコンピュータおよびネットワーク

B：犯罪手段としてのコンピュータおよびネットワーク

C：武器としてのコンピュータおよびネットワーク

対応する事例として以下が想定される。

A：犯罪指示などを暗号化したメール送受信

脅迫文などをヘッダー改竄により匿名でのメール送受信

B：電子盗聴およびデータの不法コピー、情報の改竄

C：ウィルスによるシステムの損傷、ネットワーク延長線上の設備への攻撃

効果として以下の５点が想定される。

A：攻撃に要するコストが低い

B：少数の専門的な技術者だけで遂行が可能

C：実行者の特定が困難

D：地理的・時間的制約がない

E：攻撃が成功した場合の経済・社会へのダメージが大

４．通常的なハッキング行為の具体的なツール群

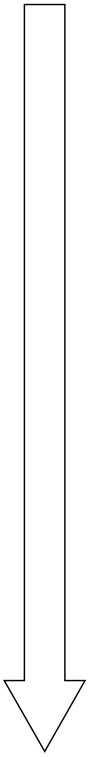
次に、通常行われているハッキング行為について概説すると共に、IDC等による防御の一例を例示するものである。下記は基本的に経験および調査に基づくものであるが、一部想定を踏まえたものである。

本稿においては「ハッキング」は権限を持たないものによるルート権の奪取を指すものとする。サーバおよびネットワークの破壊行為に関しては別途「クラッキング」と表記するものとする。

(1) ハッキング手口　（愉快犯的な行為）

ここでは、愉快犯的な発想によりハッキングを行う一般的な手法について解説する。

ハッキングの手法を簡単に概説すると以下のようなフローとなる。



偽装工作：自分のIPを表に出さないよう偽装工作を行う。
匿名プロクシの連鎖および盗難ID等の収集。

セキュリティホールリストの更新
ネット上に掲示されているような、セキュリティホールのリストを更新し、自分のスキルでハッキングできる、OSおよびデーモンのバージョンを確認する。ハッキング行為においてはネットワークはリスト的な意味合いを持つ。

ターゲット選定
ポートスキャンによるサービスの確認およびOS、バージョンの把握。

ハッキング
通常、既知のセキュリティホールを利用する場合、オプションパケットを利用する。（所要時間３分）

クラッキング
通常、DOS攻撃と呼ばれる大量のパケットを送り込むことによりサーバ自体をダウンさせることができる。（所要時間５秒から10秒）

現状のネットワークでは、特段のセキュリティ対策をとらないデフォルトで運用している管理者が非常に多い。また常にパッチ情報を収集し、改善を行っていないサービス群はハッキングされても当然であると考える。ほとんどのハッキングは既知のセキュリティホールを

狙った愉快犯的な行為であると想定される。一般的な調査では、このような行為は韓国および中国のISPより送られることが多い。どのような目的でこれら行為を行うのかという疑問が生じるが、おそらくは以下の目的であると考えられる。

SMTP不正利用

WEB改竄

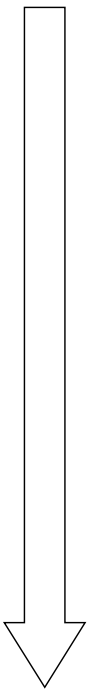
スニッファー行為

個人情報の取得と改竄

破壊行為

(2) ハッキング手口　（確信的な行為）

ここでは、確信的な発想により（目的を有する）ハッキングを行う一般的な手法について解説する。ハッキングの手法を簡単に概説すると以下のようなフローとなる。なお、手法等は(1)で解説したものとほぼ似通うことが多い。



偽装工作：自分のIPを表に出さないよう偽装工作を行う。
匿名プロクシの連鎖および盗難ID等の収集。

セキュリティホールリストの更新
該当ネットワークへの侵入経路の把握。保有する情報と立場により手法は変化する。内部犯行であればメディアによる情報のコピーが可能であるし、容易にパスワードなどを奪取することも可能である。この時点で「成りすまし」行為が完了し、ハッキングは完了したも同然である。

ターゲット確認
ハッキング

現在のところ、十分な管理が行われていても内部の人間による行為に関しては防御の方法は無い。社内の上層部のみのデータに関しても、重役利用のID等は想定が可能であるし、パスワードもしかりである。またスニッファー等が埋め込まれた場合、無防備の状態で、そこにはセキュリティの言葉は存在しなくなる。また、保守点検用のリモート回線を利用される可能性もあり、これら情報が漏洩した場合、被害は甚大なものとなる。

また問題視されるのが、企業におけるインフラの更新の遅さである。管理者を立てることは当然であるが、管理一般にかかる経費の上昇などから、有名企業においても十分な管理がなされていないイントラネットも多くある。

クラッキングに関しては、米国においてストレージ情報を全て初期化してしまうなどの被害が出たケースもあると聞いているが、内部の怨嗟による犯行であり、ここでは取り上げない。ただし、事例としてシステム自体に時限装置を埋め込み、２年後に全てのデータを初期化するなどの行為は十分可能であることに言及しておく。

(3) セキュリティポリシーの欠如

これまでの内容で問題視されるのがセキュリティに対する思考であると考える。基本的にはインターネットはレッセフェール的な発想が強く、自己責任において全てを管理し運用するべきインフラである。

そこには公共性が存在し、秩序ある運用が望まれるのであるが、公共性が高いゆえにあらゆる問題が生じていると考えられる。現状ではハッキング行為自体、法体系がはっきりとせず、また技術の過渡期にもあたることから半ば公然と行われている。

提言として最低限のセキュリティポリシーについて提示する。全てのインフラ利用者が理解し実践したならば、ハッキング行為はかなり困難になり、行為自体の犯罪性も高く認識されると想定される。

一般ユースのセキュリティポリシー

○ 常に自己の環境を把握し、セキュリティホールを塞ぐよう管理する。
○ ファイヤーウォール等は最低限導入する。
○ 不要なサービスは常に停止する。
○ 重要なデータの保管に関しては最低限パスワード管理を行う。
○ ウィルス検知ソフトは常に最新なものを利用する。
○ 悪意のあるサイトが多く存在することから、通常はJAVA・ACTIVE-Xは利用不可にする。
○ クレジット番号などの個人情報は、電子メール等による送信を行わないようにする。

企業レベルのセキュリティポリシー（上記に加え）

○ サーバ構築に関わる人員は最低限で行い、管理者権限を明確にする。
○ サーバエリアは外部から容易に入れない場所にする。
○ 外部からのコネクティビティに関しては厳密に規定する。（RASを含む）
○ パスワード等の更新を定期的に行う。

○ サーバエリアへのメディア持込の禁止。
○ 各クライアントの利用状況を把握する。

上記で上げた内容は、ネットワーク利用上では半ば常識の範囲ではある。これらを維持するに必要な費用等は、その構成により大きく変化するが、想定で端末１台につき2000円/月から、サーバにおいては10万～数千万/月のレベルであると考える。

(4) 想定される次世代型ハッキング

ADSLなどの専用線環境が整備されると共に、これまで概説したハッキングより、より効果的なハッキング手法が蔓延する可能性がある。

○ ウィルスによるデータ漏洩
○ Ｐ２P技術によるデータ漏洩
○ アプリケーションレベルによるデータ漏洩

(5) 補足　一般的に利用されるツール事例

セキュリティポリシーにおいて簡単に解説したが、大半のハッキングは管理の徹底で防御できる範囲の問題である。しかしながら、まだまだ顕在化していない手法および行為があると考えられる。ここでは近隣諸国のハッカーが好んで利用するツールを紹介する。

入手容易性	名　　称	機　　能
やや難	HACKER'S UTILITY	Port Scan
難	Net Lab	Finger、Port Scan、Trace route
容　易	Legion 2.1	共有ファイルをスキャン
容　易	Grinder	Trace Route
容　易	John the Ripper	パスワードクラック定番
難	UpYours!_v3.0	高機能メール爆弾
難	E-Mailer	非常にシンプルな匿名メーラー

これらのうちで、John the Ripperに関しては、入手は簡単であるが、ハック用の辞書などは入手は困難であることを追記する。辞書専門のサイトも存在する。上記に例示したツールは基本的なエントリー用のツールである。これら以外にも、ハッキングに利用できるツール群は多くあり、またツール開発のサイトも存在する。

なお、未確認ではあるが米国のハッカーグループでは特定のサーバ攻撃用の専用ツールが流通しているらしい。これは、ある仕様のメールサーバのルート権限をワンクリックで奪取できるとの話であるが、真偽の程は不明。技術的には可能であると考える。

また、違法コピーおよびフリーウェアなど、責任の担保能力の無い製品の利用が多い。および既存の製品に関しても英語版に比べセキュリティホールの対策が遅い。これは、開発部隊が米国およびインド、イスラエル等に分散されているためである。よって米国で対策されたとしても踏み台として日本が想定されることは十分にありえる。

ブロードバンド等の利便性の向上とともに、急速に拡大しているインフラであるが、日本ではすでに利用者の増加に伴い、以下の問題点が顕在化している。

個人が一時的に管理するサーバによる踏み台の増加（安易なサーバ構築）

接続環境の多様化による、ツール群入手と実行機会の増加

ローカライズアプリケーションによるセキュリティ対策の遅れ

これらを包括的に対処することは現状では不可能である。インターネットの存在自体が、その派生は米国における軍事目的のネットワークであろうとも、現在では世界レベルの情報リソース共有インフラの性格を有している。そこには国家を超越した無法な部分も存在し全てを把握することは不可能である。

5．サイバーテロ予備軍としての若年層ハッカー

(1) 安易なツールの入手と利用機会の拡大

基本的にわが国におけるサイバーテロの可能性に関して一番の問題点は「将来的なサイバーテロ予備軍」と捉える事ができる若年層のハッカーが非常に多く存在すること。現状ではツール群に紹介した程度のプログラムはいたるところで入手することができ、多くの人が保有しているものと考えられる。結果として罪の意識も小さく、安易な利用を行うケースが後をたたない。

これらツールが興味本位での利用にとどまらず、主義・思想に基づき利用された場合、それはテロ行為と捉えることができる。ここでは、一般的なユーザが被害者としてではなく加害者として認定される恐れがある。すなわち、インターネット環境の向上により、比較的安価にサーバ構築が可能となり、多くの方々が趣味としてサーバ構築を行っている。これらサーバが時系列的に適正に管理されるかどうかという点も問題であると考える。

最悪の場合、ROOT権限を奪われ、踏み台となり犯罪に手を貸す可能性が多く潜んでいる。かなりスキルを有する作業であるが、現状では以下のような事例が想定される。

(2) WEB改竄とテロ行為

ここでは架空のサイバーテロリストがテロ行為の一環として行う犯罪を事例として想定した。具体的にはWEB改竄がテロ行為として認められるレベルの犯罪に成長する事例を例示する。

サイバーテロリストはポートスキャン等によりいつでも利用できうるサーバとして日本国内にあるセキュリティの甘いサーバを常に監視し、常時10台近くのROOT権限を有し、かつ匿名プロキシなどのリストを保有するなどの準備を行っている。政治的環境が激変し、わが国と某国政府の間に緊張が走ったとする。両国の和平に否定的な第三国のサイバーテロリストにより以下の行為がされた場合、これはわが国に対するテロ行為と言わざるを得ないであろう。想定事例は以下のとおりである。

仮定：

サイバーテロリストによりルート権限を奪われた202.220.458.**のサーバは踏み台にされ、該当IPより201.225.***.**にある某国教育機関のWEBが書き換えられたうえ、Indexには某国の言語で政治的に問題のあるような表現が羅列されたとする。

対応：

ここで、改竄をうけた国家は一教育機関のサーバデータの書き換えという対応を行うであろうか。おそらくメディアは大きく取り上げるとともに、わが国の姿勢を問い、対応を迫るであろう。また第三国のネットワークから侵入されたとしても、踏み台に利用されたIPが犯行の実行者として足跡を残すために、簡単には操作はできず、犯人の特定は困難なものとなる。

これら行為が、連続して行われた場合、国民感情にどのような影響が出るのか。わが国のインフラは身代わりにされる危険性が高い事を認識しておくことが必要である。

(3) 個人情報漏洩の危険

インターネットを閲覧しリンクをたどること自体なんら危険は無いものと思われるが、中にはIP等を収集しているサイトも多くある。悪質なものであればパスワードリストを収集するなど個人情報にアクセスするものも多くある。Goドメインからこれらのサイトにアクセスした場合、IPおよびルートはピッキング対象となる可能性がある。

費用対比の問題であるが、重要な発信源からの暗号化情報であればピッキングを行い解読する価値もあるが、現在の解読技術では時間がかかりすぎるために、情報の新規性としては乏しいかと考える。

６．米国における重要インフラ保護の現状

情報通信ネットワークに対する攻撃が頻発する状況をうけて、米国においてはこれに対抗するための方策がとられており、公的機関のみならず民間企業においてもCSO(Chief Security Officer)を置くなどして、組織の責務として安全対策がとられることが多い。これに比べると、わが国の企業におけるセキュリティ対策はファイアウォールのアップデートなど技術的な対処が中心であり、企業組織としての対応においては米国におけるそれに比して危機意識の高くないと思われる面も見受けられるところである。

政府機関だけでなく、民間においても電力やガスなどの基盤インフラを提供する公益企業においては高度な危機管理が求められるところであり、これが私的競争の原理では達成されない場合には、事故発生時に生じ得る負の外部効果を避けるべく、法律などの制度を整備して対処することが望ましい。米国においてはこうした危機管理を民間の自主規制によって高度に達成しているが、わが国ではいまだ完成領域に達しているとはいえないのが実情である。

一方、韓国においては重要インフラ保護法案が提出されるなど、はやくから政府の主導による危機管理体制の整備がすすめられている。これは周辺環境の違いなどがもたらす国民的な危機感覚の差異に起因するものであろうが、攻撃理由の如何にかかわらず重要基盤インフラがサイバーアタックによって打撃を受けた場合には社会システムが機能不全に陥ることは避けられないことを考えると、わが国においても同様の法整備を検討すべき時期に至っているといえよう。

すなわち、米国におけるように民間企業が私的競争原理に基づいて高度なセキュリティを自主的に達成しようとするレッセフェール型の政策が適切であるのか、それとも政府の規制によって重要インフラのセキュリティレベルを一定以上に保つようなコマンドアンドコントロール型の政策が妥当であるのか、早急に議論すべき要請が存在するといえよう。

７．通信傍受網によるセキュリティ対策とその課題

情報通信ネットワークへの不正な侵入や攻撃を完全に遮断することが困難であることから、攻撃の過程を即時または事後に監視することによって、秩序の維持と抑止力の向上を図ろうとする政策手法があり得る。具体的な手法としては通信傍受網エシュロンのような監視装置を活用することが有用であるとされている。

しかしながら、通信傍受網は不正な攻撃を把握するだけでなく、通常の通信をも監視対象とするものであるから、刑事司法手続きに則って人権に十分に配慮した場合であってもなお、国民生活の自由に対する抑止効果が働くことが懸念される。また、ヨーロッパなどプライバシー保護意識の高い地域との政策整合性を図りにくいという問題がある。

また、実効性の面においてみると、平常の通信内容に関しては傍受と理解が容易であって確かに監視が可能であるのとは対照的に、不正な攻撃などを行おうとするサイバーテロリスト間の通

信についてみると、解読方法が世に広く知られていない暗号をかけて送信することや、平文レベルにおいても当事者間にしか知りえない符牒を使うなどの対監視技術が高度に活用されるため、その通信内容を傍受によって理解しかつ対策をとることは容易ではない。

このように、情報通信ネットワークのセキュリティ対策においては、国民生活への影響と実効性に十分配慮しながら、政府規制と民間の自主規制のバランスをとる適切なレベルの政策を提案することが求められているといえよう。