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

歌代和正　（株）インターネットイニシアティブ
utashiro@iij.ad.jp

ネットワークのセキュリティ対策

ネットワークサービス事業者が，安全にサービス提供を続けるために必要なセキュリティ対策には，以下のような項目が挙げられる.

- 不正アクセス対策
- 情報セキュリティ対策
- 障害対策
  - 回線障害
  - 機器障害
  - 災害
  - 運用妨害

ネットワーク事業者は，これらの対策を行い，安定したサービスを安全に提供するためにさまざまな形の努力をしている．対策の内容を詳細に説明するには紙面が足りないため，本稿では対策の指針となるガイドラインについて紹介し，その後で筆者が現時点で十分に対策が立てられていなかったり，今後対応が必要だと感じている問題について述べる.

ガイドライン

ネットワークサービス事業者が，安全なサービスを安定して提供するための指針となるガイドラインがいくつか提示されている.

■不正アクセス対策基準

1997年8月8日に，通商産業省告示第363号としてコンピュータ不正アクセス対策基準が制定された．基準は，システムユーザ基準，システム管理者基準，ネットワークサービス事業者基準，ハードウェア・ソフトウェア供給者基準の4つの部分で構成される.

ネットワークサービス事業者としては，インターネットのサービス事業者が大きく意識されている．実際には，ネットワークサービス事業者が考えるべき不正アクセス対策は，多くの部分において一般の企業等で行うべき対策と重複している．そこで，ネットワークサービス事業者特有の項目だけを残し，重複する部分はシステム管理者基準を参照するという形で基準は構成されている.

筆者はこの基準の作成に参加し，主にネットワーク事業者基準を担当した．作成の過程では，ネットワーク運用やサービス提供に携わるスタッフの意見を採り入れ，実践的な内容を盛り込んだつもりである．ただし，基準としてまとめられるにつれて，徐々に具体性に欠ける文面に変容したことは否めない．しかし，それは長期に渡って有効性を保つために，本質的な部分を抽出することで一般化を図った結果であり，現場の知識と経験とを組み合わせることで，その時々に応じた具体性を持つ対策にたどり着くはずである．なお，情報処理開発協会で発行している解説書（ISBN4-89087-009-2）では，それぞれの基準について，具体的に講じるべき対策についても解説している.

【不正アクセス対策基準－ネットワークサービス事業者基準】

1.管理体制の整備
(1) ネットワークサービス事業者の要員の業務範囲を明確にする
(2) 不正アクセスを発見したときの連絡体制および復旧手順を確立し，周知・徹底する
2.ネットワークサービスユーザ管理
(1) ネットワークサービス事業者およびネットワークサービスユーザの責任範囲を明確にする
(2) ネットワークサービス事業者が提供できるセキュリティサービスを明示する
(3) ネットワークサービスユーザとの連絡体制を複数確立し，周知・徹底する
(4) 不正アクセスを行ったネットワークサービスユーザに対するサービスを制限できる仕組みを確立する
(5) ネットワークサービスユーザから要求があった場合，本人の利用情報等を開示する
(6) ネットワークサービスユーザへの不正アクセスを監視できる仕組みを確立する
(7) ネットワークサービスユーザの利用情報等を記録できる仕組みを確立する
3.情報管理
(1) ネットワークサービスユーザの情報は，厳重に管理する
(2) ネットワークサービスユーザの情報を公開する場合は，本人の了解を得る
(3) ネットワーク構成等の重要な情報は，公開しない
4. 設備管理
(1) ネットワークサービスに係る機器は，許可を与えられた者以外立ち入れない場所に設置し，厳重に管理する
(2) ネットワークサービスに係る機器の管理が常に可能な仕組みを確立する
(3) ネットワークサービスに係る機器を遠隔管理する通信回線は，複数確保する
(4) ネットワークサービスユーザにサービスを提供するネットワークは，他の業務のネットワークと分離する
(5) 特定のサービスに関する情報は，そのサービスに関連した機器に限定して流す
5. 事後対応
(1) 異常の連絡を受けた場合または異常を発見した場合は，速やかに原因を追究する
(2) 不正アクセスであることが判明した場合は，関係者と協調して被害の状況を把握する
(3) 関係者と協調して不正アクセス被害の拡大を防止するための処置を行う
(4) 事前に確立した復旧手順を遂行し，関係者と協調して不正アクセス被害の復旧に努める
(5) 不正アクセス被害の原因を分析し，関係者と協調して再発防止策を行う
(6) 不正アクセス被害の拡大および再発を防止するため，必要な情報を通商産業大臣が別に指定する者に届け出る
6.情報収集および教育
(1) セキュリティ対策に関する情報を随時収集する
(2) ネットワークサービスユーザがセキュリティ対策を行う場合に必要な情報を提供する
(3) ネットワークのセキュリティ上の問題およびその対策に関する十分な情報を提供し，必要に応じてその情報を活用するための教育をする
7.監査
(1) ネットワークサービス事業者が行う不正アクセス対策の実効性を高めるため，システム監査の報告を受け，必要な措置を講ずる

■情報通信ネットワークの安全・信頼性基準

電気通信事業者の監督官庁である総務省は，「情報通信ネットワーク安全・信頼性基準」（昭和62年郵政省告示第73号，平成13年3月29日改正）という形でガイドラインを定めている．この基準の項目は非常に多岐に渡るため，全体的な構成のみを**表-1**に示す．

表の各項目について対策が示され，その実施の必要性を第一種電気通信事業用ネットワーク，特別第二種電気通信事業用ネットワーク，その他の第二種電気通信事業用ネットワーク，自営情報通信ネットワーク，ユーザネットワークの5種類のネットワークについて定義している．ネットワークサービス事業者は，例外的なものを除きすべての基準を実施すべきである．

情報セキュリティ管理のうち，ポリシーの策定と危機管理計画の策定については，別表でより詳細な指針が示されている．危機管理計画はサイバーテロを想定したものであり，ネットワークサービスが今後ライフラインとしての使命を担っていく上で，より強固なセキュリティが必要であることを示唆している．現に，その中でサイバーテロの具体的な攻撃法として挙げられているのは，(1) 物理的な攻撃，(2) Webページ改ざん，(3) 分散協調型サービス拒否，(4) コンピュータウィルス，(5) 不正侵入の5つであり，ほぼすべてがインターネットサービスに対するテロ行為を想定している．

■その他のガイドライン

この他にも次のようなガイドラインがネットワーク事業者のセキュリティ確保のための参考になる．

- コンピュータウイルス対策基準
  平成7年7月7日付け通商産業省告示第429号

項目	対策概要
設備基準	
一般基準（11項目 51対策）	ネットワーク全体に対する基本事項など
屋外設備（15項目 20対策）	屋外ケーブル，アンテナなど
屋内設備（7項目 12対策）	通信機器，情報処理機器など
電源設備（7項目 14対策）	電力の供給条件，停電対策など
環境基準	
センターの建築物（4項目 11対策）	立地条件，入出条件など
通信機械室など（6項目 21対策）	機械室の条件，データ類の保管など
空気調和設備（8項目 15対策）	設置の条件，漏水防止など
管理基準	
ネットワーク設計管理（4項目 6対策）	設計指針の明確化など
ネットワーク施工管理（5項目 6対策）	作業行程の明確化，試験管理など
ネットワーク保全・運用管理（9項目 12対策）	保全・運用基準，監視および制御など
設備の更改・移転管理（2項目 2対策）	作業行程の明確化など
情報セキュリティ管理（6項目 7対策）	情報セキュリティポリシーの策定など
データ管理（5項目 7対策）	基準の設定，記録物の管理など
環境管理（2項目 2対策）	建物，空調設備の保全など
防犯管理（6項目 6対策）	管理の手順防犯装置の管理など
非常事態への対応（2項目 7対策）	体制の明確化，復旧対策手順など
教育・訓練（2項目 8対策）	体制，教育・訓練の内容など
現状の調査・分析および改善（4項目 5対策）	基準の設定，改善など
別表3　情報セキュリティポリシー策定のための指針の内容	
別表4　危機管理計画策定のための指針	

表-1　情報通信ネットワークの安全・信頼性基準

- 情報システム安全対策基準
  平成7年8月29日付け通商産業省告示第518号
- 情報システム安全対策指針
  平成9年国家公安委員会告示第9号
- セキュリティ対策セルフチェックシート
  情報処理振興事業協会 セキュリティセンター
- Site Security Handbook (RFC 2196)
- Recommended Internet Service Provider Security Services and Procedures (RFC 3013)

非常時対策

2001年9月に起きたニューヨークテロ事件では，有線無線ともに電話環境が壊滅的な状況に陥った中，インターネットによる情報流通が大きな役割を果たしたと言われている．経済活動をはじめとして，インターネットが担う社会的役割は今後ますます増大し，ライフラインとしての性格を帯びてくると予想される．

ネットワーク事業者は，災害等の非常時においても，いや，非常時においてこそ，そのサービスを安定して提供できるべく努力しなければならない．筆者の所属する事業者もニューヨークに重要なネットワーク設備を持っている．幸い，直接テロ事件の被害を受けることはなかったが，電力の供給停止によってその運営は大きく影響を受けた．当然，自家発電設備は用意されていたが，交通制限によって燃料の補給が間に合わないのではないかという心配に加えて，発電設備の故障が重なり，事件後しばらくの間は予断を許さない状況であった．これは，我々が想定していた以上のことである．特に日本では多くの事業者の重要拠点が東京に集中している状況を考えると，東京に同規模の災害が発生してもサービス提供を継続するためには，ネットワーク設備や運用体制の見直しが必要である．

サイバーテロ対策も重要な課題だ．インターネットは偶発的な事故や障害に対する耐性は高いが，重要な個所を恣意的に狙う攻撃に対しては，意外にもろいとも指摘されている．インターネット全体の重要な機能は，少数の事業者や相互接続点，データセンター等の限られた場所に集中していく傾向にある．これらの重点部分を狙った攻撃からインターネット機能を守るために，各事業者が協力して対策を立てることも重要となる．

情報セキュリティ

ネットワークサービス事業者は，顧客に関する個人情報を厳重に管理する必要があると言われるが，他の業種に比べてその重要性が極端に高いわけではない．むしろ，電子商取引サイトやインターネット銀行・証券サービスの方が重要性ははるかに高い．

事業者自身が管理する情報を守るのは当然のこととして，ネットワーク事業者は，事業者の設備が侵害されることによって，顧客組織の情報セキュリティが危険に晒されることを意識する必要がある．ネットワーク事業者の設備に侵入できれば，特定のネットワーク向けの経路情報を偽って設定し，別の第三者へ送ってしまうことも可能である．適切に設定すれば，それを気づかれずに本来のユーザに転送することもできるだろう．

近年普及しつつある VPN 技術を利用している場合には，状況はさらに深刻である．インターネットの利用者は，それが複数の組織によって利用される公衆ネットワークであることを知っているため，本当に重要な情報を流す際には，盗聴を防ぐために暗号化などの対策を施すことが一般的である．IP VPN の技術を利用すると，インターネットと共通の基盤ネットワークを使って，インターネットの通信と，プライベートネットワークの通信とを混在させることが可能となる．VPN の利用者の多くはそれが安全なネットワークであると思っており，ネットワーク事業者の設備が侵害され悪意を持って運用されると，機密性の高い情報が漏洩する危険が生じる．侵入されなくても，設定のミスによって異なる組織の間で本来流れるべきではないパケットが流れてしまうこともあり得る．想定しない状況が発生したときに，それを検出したり，最悪の事態に陥るのを避けるようなネットワーク設計が必要とされる．

CATV 型のネットワークや，インターネットマンション／ホテルなどでは，間違ったネットワーク設計や設定ミスによって，家庭や部屋の間で利用者が想定しない形で情報が流れてしまうことがある．利用者側に設置する設備で対応するのは，原則として許容できる形態ではない．利用者の情報セキュリティを考慮したネットワーク設計を行うのはネットワーク事業者の責任である．

運用妨害

ネットワーク事業者にとって，障害，事故，災害，故意の攻撃等に備えてネットワークを監視し，回線や設備の冗長化によってトラブルに対応するのは当然である．しかし，正規の通信に見える攻撃や事故によってネットワークが障害を受ける可能性もある．サービス不能（DoS:Denial of Service）攻撃は，サーバやクライアント等のホストの運用を妨害したり，特定の組織のインターネット接続を意図的に溢れさせるために行われることが多いが，ネットワーク事業者の通信回線を輻輳させることでより広範囲に被害を与えることができる．従来は一般のユーザが利用できる帯域幅は数百Kbpsから数Mbps程度であったから，少数の利用者が事業者のバックボーンを使い尽くすのは困難であった．しかし，昨今は個人レベルで数十Mbpsの接続性を持つことも可能となってきたし，（不正侵入によって確保した） 複数の場所から協調して DDoS（Distributed DoS）攻撃を行うことで，たった1人で大規模な事業者のネットワークを機能させなくすることも可能である．

今後この傾向は高まると考えられ，ネットワーク事業者は，故意あるいは不注意や事故によるネットワークの輻輳に対応できる体制を作ることが急務である．

サービス設計

ネットワーク事業者にとって，自身のセキュリティを守ることは大切だが，利用者が安全にネットワークサービスを利用できる環境を提供することもまた重要な業務である．1つのアプローチはセキュリティサービスを提供することだ．たとえば，ファイアウォール，ウイルスチェック，コンテンツフィルタリング，セキュリティ監査，侵入検知，コンサルテーション，セキュリティ情報提供，インシデント対応などがこれに当たる．これらは有償サービスであることが多いが，セキュリティ情報の提供や簡単な監査サービスなどを無償で提供する場合もある．最近の傾向としては，技術の高度化や運用方法の複雑化に伴い，単に製品やサービスの提供だけではなく，運用・管理までを行うマネージドサービスに対する需要が高まっている．

しかし，ネットワーク事業者にとって，セキュリティサービスの提供は本質的ではない．セキュリティ製品やサービスを扱う事業者は他にいくらでもあり，ネットワーク事業者がそれを行うことの利点はあるにしても，どれも支配的なものではない．

ネットワーク事業者が，顧客のセキュリティを確保するために本当に行うべきは，提供するサービスの仕様を決める上で，直接的にしろ間接的にしろ，それが顧客のセキュリティにどう影響するかを十分に考えることであろう．たとえば，不正アクセス基準の中の「ネットワークサービスユーザ管理」「情報管理」「情報

収集および教育」などで指摘されている点をサービス設計の時点で十分に考慮し，誠実に実践するということだ．これらは，たとえば，次のような形でサービス仕様に影響する．

- 複数の選択肢がある場合には，デフォルトを安全な側に設定する．
- より安全な方法が選択できる場合には，それを提供する．
- 利用履歴等のセキュリティ上有用な情報を利用者が「無理なく」参照できるようにする．
- 無思慮な利用者がコストを優先して危険な状況に陥ってしまわないようにする．

これらを実践すると，概してコストが余計にかかりサービス価格に影響したり，利用者の自由度を損なうように見えたりもする．そのため，実践しない事業者のサービスの方が，利用者には一見魅力的に見えてしまうこともある．矛盾する要求をうまく調整して適正なサービスを構築することが事業者に求められるが，利用者側も，必要な部分を削ぎ落として低価格化を図っているようなサービスを見極める目を持つことが重要である．

代表的なネットワークサービスについて，この観点でどのようなことが考えられるかを簡単に挙げてみる．

- サービス全般
  - セキュリティレベルの明示
  - 盗聴されても安全な認証方式の提供
  - 正確な時刻管理
- ダイアルアップ
  - 利用履歴の提示
- メール
  - 送信時のユーザ認証
  - 送受信の暗号化対策
- WWW
  - コンテンツ閲覧時の暗号化対策
  - コンテンツ更新時の暗号化対策
  - 実行スクリプトの運用方針

残念ながら，通常のインターネット接続サービスについて，事業者が積極的に提供できるセキュリティ対策は少なく，それ以上のものはセキュリティサービスという形になる．しかし，一般に利用者は，接続サービスの価格に見合う料金しか負担しようとはしないし，接続サービスはますます低価格が進んでいる．安価なセキュリティ製品やサービスも出てきてはいるが，機能的に不十分なこともあるし，いくら安くても負担増を受け入れない利用者は少なからず存在する．

オプションでセキュリティサービスを用意して責任を利用者に押しつけているだけでは，ネットワーク事業者の責任を十分に果たしているとは言えまい．一般消費者相手に鞘を付けずにナイフを販売するようなものだ，とは少々言いすぎの感もあるが，根ざすところは同じである．

危険性そのものを取り除くのは難題だといって，そこで思考停止すべきではない．たとえば，外部からの接続を受け付ける必要のないネットワークであれば，そうでない場合に比べて容易に安全な環境を構築することができる．そのために DNS，メール，ウェブなどのサーバ機能はすべて事業者からのみ提供し，利用者が用意することを禁ずるのは効果的ではある．しかし，それによって市場競争力を失う可能性もあり，営利企業としては判断が難しいところだ．

SOHO や個人向けの低価格な常時接続や，接続回線の高帯域化が進む社会情勢にあって，ネットワーク事業者が適切な仕様のサービスを用意することは，今後インターネットが社会インフラとして定着していく上で大きな意味を持つ．ネットワーク事業者は，その役割と責任を十分に認識し，社会全体のセキュリティ確保のために努めなければならない．

（平成13年11月12日受付）