外部接続のセキュリティに関する一考察

乾　泰司
日本銀行システム情報局

組織内で業務や情報伝達など汎用目的に利用される内部ネットワークを外部に接続する際に、「情報（データ）」の授受を安全確実かつ円滑に行うとともに、内部の情報資源が機密漏洩、情報破壊・改竄、業務妨害といったリスクから十分に守られ安全性が確保されるよう、対外接続を進めるに当たっての基本的な考え方を整理。具体的には、①電子広報、データ・情報交換といった接続ニーズおよび主要構成要素を整理し、②対外接続に伴うリスクの類型化を行った後、③リスクと対応する要素技術の整理を行い、④これらを基に基本方針を提示。

Security Consideration of External Connections

Taiji Inui
Information System Services Department, Bank of Japan

In making an external connection (connecting general purpose internal networks used for business operations and transforming information), the basic premise is to secure smooth transmission of information (data) while maintaining the security of internal information assets from the viewpoint of leakage, destruction/tampering, and the obstruction of business. First, needs such as electronic public relations and information/data exchange, as well as elements involved in making external connections must be clarified. Second, risks accompanying external connection must be categorized. Third, how to address these risks must be decided. And lastly basic procedures for dealing with this issue should be considered.

1．はじめに

最近のインターネットの急速な発展について改めて述べる必要はないが、ネットワークとしての拡大に加え、ＴＣＰ／ＩＰ、「ウェブ」等の所謂インターネット技術が、イントラネット、エクストラネットといった企業内、企業間ネットワーク等にも適用されるようになっていると言える[1]。日本銀行でも、ＢＯＪ－ＬＡＮ／ＷＡＮと呼んでいる全職員をユーザとする汎用ネットワークには、インターネット技術を利用している。

社会全体のネットワーク化が進み内部ネットワークも整備されると、「ウェブサイトにアクセスしたい、出張先や出先から社内システムを利用したい、外部の企業とのデータ授受を自動化(オンライン化)したい、広報活動を電子メディアで行いたい」等の要望が出てくることになる。このような多様な要望に対し、たとえネットワークがオープンだからといって全て同一ネットワークで応えることは、セキュリティ上不可能であり、このような観点からも対外接続についての考え方を整理すること[2]が望まれる。

2．ニーズの分類および主要構成要素

対外情報接続に関するユーザーニーズは、接続相手や接続ポイントから①電子広報、②データ・情報交換、③内部から外部へのリモートアクセス、④外部から内部へのリモートアクセス、⑤電子メール等に分類。

[1] 金融界でもインターネット技術を広範に利用するようになったため、米国などでは、監督機関から安全性に関するガイダンス等が出されている（参考文献[1]）。

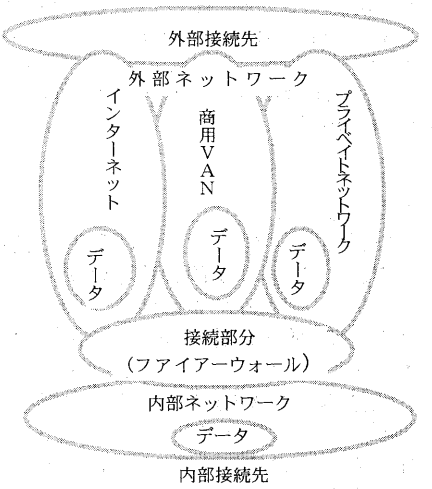
[2] 参考文献[2]参照。

ニーズ	接続相手／地点	概要
電子広報	不特定多数／不特定	一般個人や一般企業等に対し、組織体が保有する情報を広範に公開するためのもの。具体的には、各種の公開ウェブサイトが挙げられる。
データ交換	特定先／特定	予め決められた先から決められたフォーマットでデータや情報を一定の時間内に送受信すること。具体的には、電子決済、統計作成のためのデータ収集、取引先との間のデータ交換等が挙げられる。
内部から外部へのアクセス	不特定多数／不特定	内部ネットワークに接続する端末から外部のシステムにアクセスすること。具体的には、内部ＬＡＮ端末からの公開ウェブサイトへのアクセスや商用データベースの検索等が挙げられる。
外部から内部へのアクセス	特定先／不特定	外部から社内システムにアクセスすること。例えば出張先から内部の顧客データベースへのアクセスなどが挙げられる。
電子メール	不特定多数／不特定	内部ネットワークに接続する端末から外部に対し電子メールの送受信を行うこと。

対外情報接続案件は、概念的には①外部接続先、②内部接続先、③外部ネットワーク、④内部ネットワーク、⑤外部ネットワークと内部ネットワークの接続部分、⑥データ格納・集積部分、の６つが主要構成要素となっている。

これらのうち、外部接続先と内部接続先については専ら業務要件により決まり、内部ネットワークについては基本的には同ネットワークをインフラとして利用するシステム全体を指す。このため対外情報接続案件を検討する際にシステム面からみて重要なポイントは、①利用する外部ネットワーク（インターネット、商用ＶＡＮ、プライベイトネットワーク等）の決定、②外部ネットワークと内部ネットワークの接続形態（オンライン、オフライン等）の決定、および、オンライン接続の場合のファイアウォールの内容選択、③データ格納・集積場所（外部、内部等）の決定といえる。
外部ネットワークについては、現状では、インターネット、商用ＶＡＮ、プライベイトネットワーク等が選択肢となり、採用プロトコル、回線速度、暗号・認証等技術的な差が評価のポイントとなる。一方、ユーザーニーズがこうした既存商品のサービスの枠内におさまらない場合には、自由な設定が可能な（ただし運用負担、コスト負担がある）プライベイトネットワークを構築することとなる。なお、内部ネットワークに外部情報を取り込む手段としては、外部ネットワークを全く利用せず、ＦＤ等の磁気媒体経由による方法もある。

内部ネットワークとの接続形態は、オンライン接続とオフライン接続に分類される。このうち、オンライン接続は、職員が内部から通信を始める「内部起動」と、外部接続先が外部から内部に向けて通信を始める「外部起動」に分類できる。また、オフライン接続については、磁気媒体の「持出し」と「持込み」に分けられる。具体的な接続方法としては、①ファイアウォール、通信サーバ（オンライン）等や、②ＦＤ、ＭＴや切替えスイッチ（オフライン）等があげられる。後述のように、これらの形態如何により対外情報接続に伴うリスクには大きな差異があり、慎重な形態選択が必要。



データの格納・集積場所、データ用サーバの設置場所は、外部と内部に分類される。内部とは、内部(社内)ネットワークの中を指し、外部とは、内部ネットワーク以外の全てを指す。具体的には、商用ＶＡＮ内、インターネットプロバイダー内、情報ベン

ダー内、バリアセグメント[3]内（内部ネットワークと外部ネットワークの緩衝地帯）などが外部と定義される。当該データおよび内部ネットワークの保護の観点から、どこにおくのが最適かを判断する。

3．リスクの整理

対外情報接続を行う場合、業務要件に沿って、主要構成要素を組み合わせて対外情報接続を実現することとなるが、こうした対外情報接続に伴って、種々のリスクに直面することとなる。対外情報接続に伴い新たに顕現化する主なリスクとしては、内部ネットワークへの不正侵入および、外部情報（例えば、広報用に外部に格納しているデータや外部ネットワーク上のデータ）の漏洩、破壊といったものが考えられる。この他、ウィルスへの感染や内部犯行による機密漏洩などの様々なリスクがあるが、ここでは、対外情報接続に伴い新たに発生する主なリスクについて言及。その他のリスクには、業務遂行や信用に対するリスク（これまでにみたリスクの顕現化の結果として組織としての対外信用が失墜するリスク）があるほか、業務妨害として「活動妨害」や「偽装」が存在。なお、「活動妨害」とは、円滑な業務遂行を妨害する行為のことで、例えば、広報用ウェブサーバーに対し、常にアクセスし続ける等の行為を行うことにより、他の人間がアクセス不能となる状況などを指す。「偽装」とは、不正侵入者の身元を秘匿するテクニックとして使用されるほか、外部ネットワーク上で他人と偽って行動する際にも使用される。例えば、外部ネットワーク上で愉快犯が他の組織と偽って、誤った情報を流布するようなケース。このうち、不正侵入については、①システム的には正当なアクセスと認識される「なりすまし」による場合（例・パスワードやユーザーＩＤの盗用）と、②システム的に正当でないアクセスによる「アクセス侵害」の場合（例・セキュリティホールからのクラッキング、盗聴）に分類される。

[3] ＤＭＺ（Demilitarized Zone）とも呼ばれる。

3．1　内部資源に対するリスク

内部資源に対するリスクは、内部ネットワークと外部ネットワークの接続形態によって異なり、オフラインによる接続の場合、内部の何者かの関与がなければウィルス以外の手段によるリスクは遮断可能。なお、ウィルスについては、接続形態がオンライン、オフラインのいずれであるかにかかわらず、リスクを完全に排除することは困難であり、外部ネットワークから入手したファイルを利用する場合には、はじめに必ずウィルスチェックを行うことが必要。

接続形態がオフラインの時は、ＦＤ等の磁気媒体によりデータが持出される場合と、持込まれる場合がある。前者の場合には機密データが持出される（機密文書の持出しと同様な）リスク、後者の場合には「ウィルス」が持込まれるリスクが存在。こうしたオフラインの場合のリスクは、内部ネットワークを構築する以前から存在しているが、ウィルス感染がネットワークを経由して全体に拡大する可能性が高くなっている点に注意を要する。オフライン接続による対外情報接続は、内部犯行のリスクや後述の外部資源に対するリスクに対応すれば、実現が比較的容易。

オンライン接続時のリスクとしては、システム上、①内部ネットワークから外部ネットワークへのアクセスのみを許す仕組みとする場合と、②外部ネットワークから内部ネットワークへのアクセスも許す仕組みとする場合で異なる。内部ネットワークから外部ネットワークへの接続のみを許す仕組みとする場合には、外部から内部へのアクセス経路が無いため、理論上、接続部分（ファイアウォール）に設定ミスや致命的なバグが無い限り外部から内部への不正侵入は困難。ただし、ソフトのバグや内部犯行・内部共謀のケースには、このようなリスクを完全に払拭することができない点は考慮が必要。また、内部から外部への不正アクセス、ウィルス感染のリスクが存在。一方、外部ネットワークから内部ネットワークへのアクセスも許す場合には、内部から外部へのアクセスを許す場合のリスクに

加え、パスワードの漏洩に起因する正当ユーザーへの「なりすまし」リスクが存在するため、これを防御するためには、より厳格なファイアウォールや最新の認証技術（例えば、公開鍵暗号化方式とＩＣカード[4]の組合せによるもの、ＰＫＩ[5]に基づく認証局の利用等）の導入を検討する必要がある。接続相手、接続ポイントが各々不特定多数および不特定（任意）の場合には、両者が特定される場合よりも不正侵入される危険性が相対的に高いため一段と厳しい対応が必要。この間、より技術的な観点からみると、次の点が指摘できる。すなわち、防御すべき内部ネットワークが利用しているプロトコル例えばＴＣＰ／ＩＰとＩＰＸ／ＳＰＸである場合、この２つのプロトコル以外のプロトコルを用いている外部ネットワークを内部ネットワークに接続する場合には、物理的に回線は接続されていても不正侵入リスクは接続するパソコン（またはサーバ）の段階（ＡＰレベル）で遮断可能。ただし、システムについてひととおりの知識をもつ人間であれば、内部にアクセスするためのソフトウェアを容易に導入・起動することができるため、内部犯行への対応を考慮する必要。

３．２　外部資源に対するリスク

外部資源に対するリスクとしては、①回線など外部ネットワーク上のデータに対するリスクと、②格納・集積データに対するリスクがある。外部ネットワーク上を流れるデータ（パスワード等を含む）には、暗号化などの機密保護を行っていない限り、故意・過失に拘らず、盗聴、破壊・改竄される危険性が存在する。ファイアウォール外にある格納・集積データ（例えばインターネットに開放している広報用サーバ内のデータ）は、不特定多数者がアクセス可能なことから、アクセス制御等のセキュリティ対策を講じている場合でも、漏洩、破壊・改竄等あらゆるリスクに晒されている。したがって、これらのリスクについては割り切って（やむを得ないと）考えるか、あるいは、後述のような何らかの方法による対策（バックアップをとった上で破壊・改竄されているか定期的にチェックする等）を講じることが必要となる。特に信用リスクには、留意の必要があり、予め広報部門などと協力して対応策を講じておくことが重要。

４．要素技術の整理

ここまでに整理したリスクに対応するため、今後とくに重点的に検討していく必要がある要素技術は、①内部の情報資源を守る「不正侵入防止技術」と、②外部の情報資源を守る「機密漏洩防止技術」の２点。このうち、「不正侵入防止技術」は、さらに①アクセス侵害防止のための「ファイアウォール技術」と、②「なりすまし」防止のための「認証技術」に大別される。また、「機密漏洩防止技術」については、「暗号化技術」が主たる手段としてあげられる。

４．１　ファイアウォール技術

対外情報接続により生じる新たなリスクに対する最も確実は対策は、オフライン接続を継続する方法。しかし、本方式は内部ネットワークからデータ等を１度出力し、改めて外部ネットワークに入力する（あるいはその逆の操作）という人手を介したオペレーション負担が生じ、データ授受の迅速性に問題がある。このため、内外のネットワークを相互にオンライン接続する一方、両ネットワークの間にアクセス侵害をシステム的に防ぐためのファイアウォールを構築する技術が普及し始めている。ファイアウォール技術は、近年急速に進歩しており、主要ベンダーから新製品が次々発売されている。これらはデータが通過する際におけるチェックの度合（単純にデータの流れを「内→外」の一方向だけに制約するものから、通信プロトコル、アクセス権限等の中味までチェックするものまで多岐に亘る）、構築の難易度、コスト等まちまちであり、流す情報の機密性および商品ごとの特徴を照らし合わせて、採否を検討していく必要がある。ファイアウォールの構築について

---

[4] パスワードの漏洩に対する技術。「知っているもの（パスワード）」ではなく「持っているもの（ＩＣカード）」による認証方法。ＩＣカードのセキュリティについては、参考文献[3]参照。

[5] Public Key Infrastructure(参考文献[4])。

は、種々の参考書に説明されているため、ここでは幾つかの留意点を述べるに留める。まず、ファイアウォールを構成する機器(ハード、ソフト)が正しく設定されていること、特に初期値設定によるセキュリティホールが無いように注意する必要がある。このような設定不備に対しては、市販のツールなどを利用し全設定値について入念に検証する必要があるが、同時に設定値が不用意に変更されないような対策も必要。具体的にはファイアウォールを構成する機器は物理的に安全な「glass house」内に設置し、またこのような機器の設定変更は「glass house」内に設置してある各機器に直接接続したコンソール以外（リモートでは）不可能とするといったことが重要である。また、真に必要なバックアップ経路を除き、外部への接続ポイント（ファイアウォール）は、一箇所に絞り込むといったことも重要である。このほか、タイガーチームのような、内部組織によりファイアウォールの強度、設定状況を定期的にチェックすることも有効である。なお、ファイアウォールの強度は、システム的な設定だけに依存するのではなく、例えば2段のファイアウォールを設けその間に緩衝地帯（ＤＭＺ）を設け、そこでスキルがあり、かつ信頼できる職員が常時監視[6]するといった運用面の対応も極めて重要である。いずれにせよ、完全なファイアウォールが存在するわけではないため、リスクと要件に応じ、システム面、運用面を含め統合的な対応が必要。

４．２　認証技術

認証技術は、ユーザＩＤとパスワードの組み合わせ等により「なりすまし」を防止し、本人確認を行う技術であるが、市中におけるセキュリティ侵害の実例の多くがパスワードの漏洩によるものであることを考えると、対外情報接続においては、場合によっては、ユーザＩＤとパスワードの組み合わせより一段とセキュリティ機能の高い技術の採用を検討することが必要となる。このような認証手段としては、①ＩＣカード、②電子署名、③ワンタイムパスワード、④コールバック、⑤バイオメトリック等の技術が採用されつつあるが、ＰＫＩを利用したＣＡ(Certificate Authority)構築の分野に代表されるように現在急速に進歩しつつある分野といえる[7]。従って、要素技術採用に当たっては、技術動向および必要性を見極めながら、当該技術の採否を慎重に判断する必要。なお、認証技術ではないが、相手を特定する技術としては、ＰＶＣ(Private Virtual Call)も普及している。もちろん、従来から金融における大口決済システム等では、高いセキュリティの認証技術が利用されており、本人認証としては、暗号技術に加えＩＣカードに保持した取引記録をセンター側と突合して初めてアクセスを許可するといったものや端末プログラムの内容をハッシュ値で確認するといた方法が使われている。

４．３　暗号技術

ネットワークやデータベース上の機密データ等を漏洩・改竄から守るため、送信原文（平文）を予め決まったアルゴリズムと「鍵」と呼ばれるパラメータを利用して外部の第３者には読めない形式（暗号文）に生成し直す技術。大口決済システムなどでは、強い暗号を利用しており、約１０年前からトリプルＤＥＳを採用しているものもある。また、暗号鍵の運用等も極めて厳格に行っている。ただ、使用する暗号アルゴリズム,製品は、各々のシステムの用途に合致したものである必要がある[8]。最近では、パソコンレベルで簡単に導入可能な安価な暗号化ソフト製品が市販化されつつあり、鍵交換も様々な方法があるため、システム毎にどのような運用方法をとるについて検討が必要。

５．基本方針

対外情報接続を行うに当たって、外部ネットワークと内部ネットワークの接続部分を全体としてひとつに統合、集約した形で接続することも考えられるが、①接続ニーズが多岐にわたる一方システムの構成要素

---

[6] 最近では、自動監視ツールも市場に見受けられる。

[7] 参考文献[5]参照。

[8] 参考文献[6]参照。

の選択の幅が広いこと、②技術進歩のスピードが早くセキュリティ機能が陳腐化し易いこと、③最も厳しいセキュリティ要件を満たすネットワークを実現する必要があり実現までには相当のコストと長期間を要すること、等から、実際には、個別案件ごとに業務要件、実現の緊要性、コスト・ベネフィット等を踏まえ実現方式（システム要件）を選択し、可能なものから順次実現していく方針が適当と考えられる。例えば、電子広報、データ・情報交換といった、内部ネットワークと切離しても実現可能なもの（場合）は、可能なところから実現し、また、接続相手を特定することによりリスクの削減が可能なものから実現。

接続に当たっては、共用化できるところは極力共用化することにより、経営資源をできる限り有効活用するとともに、システム稼働後の維持管理負担を極力軽減することが望まれるが、標準化される以前に陳腐化する技術もあることから、見通せる範囲で、かつまとめられる範囲で製品レベルで統合するといったことが適当と考えている。

ウィルス対策や内部犯行者による不正アクセス対策については、システム技術面だけで対応することは困難であり、組織全体として対策を検討の要。

インターネット接続を行う場合のファイアウォール構築や認証に関する要素技術（およびハッカー側の不正侵入技術）については、日進月歩の技術進歩を遂げていることから、継続的に調査研究を進めるとともに、①外部ネットワークと内部ネットワークの接点数の極少化（不正侵入リスク顕現化の確率引下げ）、②外部ネットワークと内部ネットワークの接続部分のシステム的な常時監視体制の構築、③よりセキュアな認証方法の確立、等を展望していくことが適当と考えている。

このように、基本的には「確信できるところから、確信できる方法で対応していく」という考えであるが、それでも対応後に状況が変化し、システムに変更を加える必要が生じることがある。

対外接続を進める場合、内部のセキュリティレベルについての見直し,強化の検討も課題の一つである。例えば、①全職員の情報（アクセス権限など）を一元的に管理し、異動、退職等の変化に迅速に対応できるようにすること、②インテリジェントハブ、スイッチなどの導入により、他の端末にパケットが流れないように（Sniff 防止）すること、等が考えられる。また、無許可のモデムが接続されてないよう監視を強化するといったことも重要である。

最後に、このような変化に対応できる技術力のある人材の育成が最も重要なことであるのは言うまでも無い。

なお、本ペーパーに示されている判断、評価は筆者個人のものであり、もし誤りがある場合には、筆者の責任であることを付言する。

参考文献

[1] Federal Reserve Bank of New York, “Sound Practices Guidance on Information Security”, September, 1997

[2] B. Fraser, “Site Security Handbook”, RFC1244, September, 1997 、http://info.internet.isi.edu:80/in-notes/rfc/files/rfc2196.txt

[3] Bank for International Settlement, “Security of Electronic Money”, August, 1996, (日本語訳、日本銀行電算情報局、「電子マネーのセキュリティ」、ときわ総合サービス)

[4] W. Burr, D. Dodson, N. Nazario, W. Polk, “Minimum Interoperability Specification for PKI Components, Version 1”, NIST, September 1997, http://csrc.ncsl.nist.gov/pki/

[5] 「本人認証技術検討 WG 報告書－評価基準(第１版)－」 http://www.ecom.or.jp/about_wg/wg06/h9doc/wg06-list.htm

[6] 宇根正志、太田和夫、「共通鍵暗号を取り巻く現状と課題－DES から AES へ－」、情報セキュリティ・シンポジウム、１９９８年１１月