レガシー・マイグレーションにおけるセキュリティ上の問題点

Security Issues of Legacy Migration

杉浦　昌*　　谷川哲司*
Masashi Sugiura　　Tetsuji Tanigawa

要　旨

オープン技術の発展により，従来型の業務システムをUNIXマシンやPC，TCP/IPネットワークに置き換える，レガシー・マイグレーションの動きが進んでいます。

本稿では，レガシー・マイグレーションを，ITセキュリティの観点から論じます。

In step with the improvement of open technologies, the legacy migration has been advancing, which converts the old office systems into UNIX machines and PCs, or TCP/IP network.

This paper describes the issues of the legacy migration in terms of IT security.

1．まえがき

いわゆるオープン技術の発展により，メインフレーム（大型計算機）やオフコンなどから構成される従来型の業務システムをUNIXマシンやPC，TCP/IPネットワークに置き換える，レガシー・マイグレーションの動きが進んでいます。

本稿ではこのレガシー・マイグレーションをセキュリティの観点から考察し，その問題点と課題，あるべき方向性について論じます。

なお，ここではオープンという言葉をTCP/IP技術やいわゆるUNIX，Linux，IBM-PCの進化発展形であるPC（パーソナル・コンピュータ）のアーキテクチャなどの，設計情報や内部構造が公開されていたり規格化や標準化が進んでいる技術，および完全に内部情報の公開までは至っていないもののWindowsマシンのようにある程度のデファクト化やコモディティ化が進んでいる技術ないし製品一般の意味で用いています。

2．レガシー・マイグレーションとは

従来多くの業務システムでは，いわゆるメインフレームやオフコン上で専用のアプリケーションを動かし，独自手順により通信を行うような，閉じられたネットワーク上で専用のシステムを構築することが普通でした。しかし，TCP/IP技術やインターネットの発展，UNIXサーバやPCの低価格化と普及を背景として，従来の伝統的（レガシー）なシステムをこれらのオープンなシステムに移行（マイグレーション）する動きが出てきました。これがレガシー・マイグレーションです。

レガシー・マイグレーションでは，UNIXマシンやPC，TCP/IP機器を用いて装置価格や運用コストの低減を図ります。

図1はレガシー・マイグレーションの概念図です。

図1（a）は従来の業務システムです。本社のコンピュー

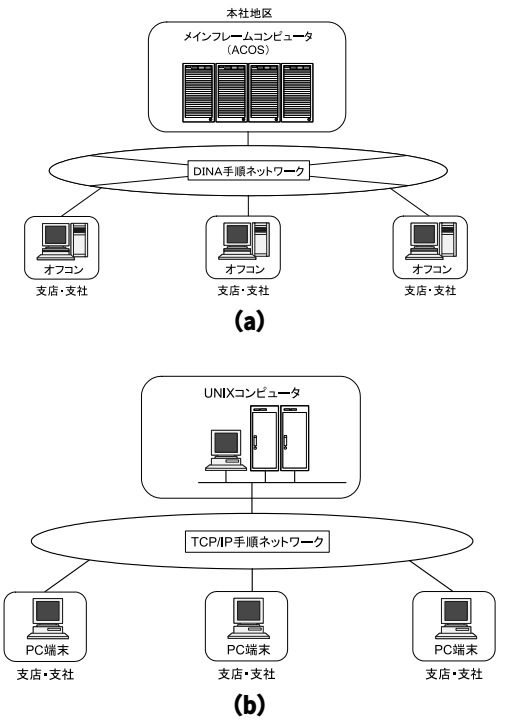

図1　レガシー・マイグレーション
Fig.1　Legacy migration.

＊ IT基盤システム開発事業部
IT Platform Systems Development Division.

タルームにメインフレームコンピュータ（図中ではACOS）があり，支社，支店にあるオフコンとの間で，独自手順（ここではDINA）で通信します。

図1（b）は，この業務システムをレガシー・マイグレーションで改変した例です。メインフレーム上で動くアプリケーションをUNIXサーバ上に移植し，支社，支店の端末をオフコンから一般のPCに換えています。UNIXサーバと支社，支店とを結ぶネットワークは同じく専用線ではあるものの，通信手順にTCP/IPを採用しています。

3．レガシー・マイグレーションにおけるセキュリティ上の問題点

レガシー・マイグレーションにおけるセキュリティ上の問題は様々な原因によって発生しますが，ここでは多くのシステムにおいて発生する可能性のある，技術のオープン化に起因する問題（リスク）について述べます。

3.1　技術資料の公開によるセキュリティリスクの増大

オープン技術では，装置内部や通信プロトコルの詳細な情報が広く公開されています。これはオープン技術の大きなメリットではありますが，その情報に基づいて，悪意を持った人が新たな攻撃手法を開発できてしまうという欠点もあります。

通信プロトコルの場合，たとえばNEC製のACOSで多く使われているDINA手順に関する技術情報は一般には公開されていません。したがって，もしも悪意を持った人がこのような独自技術のプロトコル上で何らかの攻撃を行おうとした場合，まずDINA手順に関する技術情報をNEC社内の技術部門から不正に入手するか，あるいは現実のシステム上で測定機器を用いてDINA手順を観測し，それを解析するかした上で攻撃の手法を考えねばなりません。そして，攻撃のためのツールを開発し，その試験を行う場合も，攻撃対象となるシステムと同一のDINAプロトコルで通信するシステムを自分で用意するか，あるいは実際に攻撃対象となるシステムの上でこっそりと行わなければなりません。これは，攻撃を行う者にとっては大きな障害となります。

もちろん，独自仕様に習熟しているベンダーの技術者であれば，その知識を悪用して攻撃や破壊，盗聴を行うことは可能ですが，そのようなことができる人間が内部の関係者に限定されてしまうため，悪意ある行為を行った者を追跡して明らかにすることも容易になります。

一方，たとえばこれがオープン技術であるTCP/IPのプロトコルの場合，伝送路上の電気信号の取り決めからパケット構造，通信手順，ポート番号など，多くの技術情報を簡単に入手することが可能です。攻撃ツールの開発や予行を行うためのツール類や機器もDINA環境に比べ，比較的低価格で容易に準備することができます。

プログラムの場合も同様です。オープン技術では伝送路上の通信プロトコルやモジュール間の通信手順，インタフェースなどが規定されているため，悪意を持った人にとってもそれらは有益な情報となります。商用ソフトウェアの場合はソースコードが公開されていないものもありますが，オープン技術の場合はプログラムの動作やインタフェースに関する技術解説書が多く市販されていますし，プログラムの動作を解析するためのツール類や評価環境も容易に手に入ります。

したがって，第三者からの攻撃に遭う可能性は，ベンダーの独自仕様のシステムよりもオープン技術を用いたシステムのほうが高いといえます。

3.2　脆弱性情報の公開

技術情報だけでなく，脆弱性情報の公開によっても問題が発生します。

従来，オープン技術の世界では，技術の共有と公開が盛んでした。このため，セキュリティ上の脆弱性の情報も一般に公開されるのが普通です。たとえば，米国のセキュリティ関係の非営利団体であるCERT/CC（Computer Emergency Response Team Coordination Center：コンピュータ緊急対応チーム）のような組織では，セキュリティ情報を公開して広く危険と対応策を告知しています。日本においてもJPCERT/CC（Japan Computer Emergency Response Team Coordination Center：有限責任中間法人JPCERTコーディネーションセンター），IPA（Information-technology Promotion Agency, Japan：独立行政法人 情報処理推進機構）などの団体や，多くのベンダーやセキュリティ専門会社がセキュリティ情報や対応策を公開しています。

しかし，悪意のある人間がこのセキュリティ情報を入手した場合，その情報をもとにして新たな攻撃を行える危険性があります。

3.3　共通の構造を持つことによる脆弱性の継承

オープンな通信技術であるTCP/IPは，同じくオープンなOSであるUNIXやC言語とともに発達してきたため，多くのコンピュータや通信機器，PCにおいても，もととなったUNIXコンピュータのプログラムモジュールを流用していたり，その構造を踏襲したりしている場合が多々あります。

このため，ある脆弱性がそのまま，あるいは似た形で多くのコンピュータやソフトウェアに継承されています。

たとえば2001年8月に世界中で大流行したCodeRedは，Windows NTもしくはWindows 2000上で動作するIIS（Internet Information Server）に存在するセキュリティ・ホールを攻撃するワームでした。CodeRedはIISのプログラムにバッファオーバフローを起こさせることによって感染するとともに，ある特定のサイトに対して使用不能攻撃を仕掛けます。このとき，Windows NTやWindows 2000だけでなく，一部のルータがこのワームによって機能を停止したため多くのネットワークで障害が発生し，さらに大きな問題となりました。これは，TCP/IPの通信機器であるルータも，CodeRedにより被害を受けたコンピュータと同様のプログラム構造を持っていたため，感染までには至らなかったもののバッファオーバフローによる動作の不具

合が発生したからです。これが，たとえば独自のアーキテクチャを持つ一部の機種のACOSのような，スタックポインタの格納エリアがプログラム格納エリアと完全に分離された構造を持つCPUであったなら，基本的には被害は発生しなかったと思われます。

このように，オープンなシステムはセキュリティ上の脆弱性が広く継承されてしまうという危険性があります。

3.4 攻撃ツールの氾濫

オープンな世界の特徴として，攻撃ツールの氾濫という問題があります。

インターネットの初期の段階では，攻撃目的を意図したツール（ソフトウェア）は多くはなく，ほとんどが研究開発用のツールや管理者用のツールでした。しかし，インターネットが社会インフラとして様々な分野で利用されるようになり，一般の人にも用いられるようになってくると，攻撃行為やウイルス，ワームの作成行為によってアンダーグラウンドの世界で名を上げようとする者や，インターネット上の商取引において不当な利益を上げたり利用者情報を不正に入手したりしようとする者が現れてきました。実際，アンダーグラウンドの世界では，攻撃ツールを作成する専門家や，不正に得た情報を交換する場が存在します。しかもインターネットは，現在のところ高い匿名性がある一方で追跡性が低い場合が多いため，その気になれば攻撃に用いることのできるツール類を誰でも容易に入手して使用することができます。

これは，攻撃用のツールがほとんど存在あるいは流通していない従来のシステムとは大きな違いです。

3.5 セキュリティパッチ，修正プログラムの管理と実施の問題

オープンの世界のメリットとして，世界中の多くの専門家が日々セキュリティについて研究し，その対応策を開発しているということが挙げられます。このため，多くのベンダーがセキュリティ対策のための情報公開やセキュリティパッチ，修正プログラムの公開を行っています。

しかし業務システムの場合，利用しているアプリケーションとの競合や動作の不具合が発生しないことを確認したりするため，それらのセキュリティパッチや修正プログラムをシステム部門が事前に評価した上で，適切な指示と管理のもとで組織的に適用する必要があります。このため，評価したセキュリティパッチや修正プログラムを組織内に配布する連絡体制や管理体制，それらを配布するための装置，組織内での適用状況を監視する装置などが必要となります。

ベンダーによっては，インターネットを介してそのサイトにアクセスすることにより，自動的にセキュリティパッチや修正プログラムをダウンロードして適用するような機能を提供している場合があります。このようなシステムは利用する側から見れば非常に便利な機能ではありますが，これを利用するためには，業務システムをインターネットに接続しなければならず，そのため，新たにセキュリティ対策が必要となります。また，多くの利用者がいっせいにそのサイトに接続した場合，内部ネットワークの帯域を占有してしまい，業務に支障が出る場合があります。

さらに，情報システム部門の動作確認が取れていないうちに利用者がセキュリティパッチや修正プログラムを適用してしまったり，適用時期がばらばらになって組織内に様々なバージョンのソフトウェアが搭載された機器が混在したりします。これは，業務システムの安定動作にとって大きな問題となります。

以上述べたように，レガシー・マイグレーションにおいては，本質的にセキュリティ上のリスクが高まります。

4．レガシー・マイグレーションにおけるセキュリティ対策の考え方

レガシー・マイグレーションにおけるセキュリティ対策には，大きく分けて2つの考え方があります。以下に，その例を用いて説明します。

4.1 オープン系ネットワークと同等の対策を行う方法

ネットワーク機器やサーバ，PC端末など，システムの構成要素のすべてについてセキュリティ対策を施す方法です。

考え方としては自然ですが，セキュリティ維持のために多くの費用と工数が必要となります。ある領域ごとにファイアウォールを設置して，その領域内のネットワーク機器やサーバを守ります。セキュリティ情報を常に収集し，セキュリティパッチや修正プログラムが発表されたら，ただちにシステム内のすべての機器に適用します。ネットワーク上の適切な場所に侵入検知システム（Intrusion Detection System：IDS）を設置して，人為的な攻撃や，ウイルス，ワームによる攻撃および感染を検出するようにします。ファイアウォールや侵入検知システムの記録や各サーバの通信記録を監視するための人員を配し，システムを常に安全な状態に維持します。

このような対策を行うためには，ネットワークシステム全般の管理責任の体制作りや日々の運用管理が必要です。

特にPC端末は，その導入の手軽さからセキュリティ対策が疎かになりがちですが，セキュリティパッチ適用の責任者と作業手順を定めるとともに，いわゆる相性と呼ばれるアプリケーションソフト間の相互干渉による動作不安定を避けるため，搭載するソフトを厳しく制限したりする必要があります。

広い範囲に広がった組織の場合，その部署にPC端末のセキュリティ対策を行うことのできる技術者がいない場合もあります。そのような場合は，接続するPC端末を社内ルールで厳しく制限するとともに，接続するPCの設定変更や維持管理を中央の管理部門で一括して行うようなことも必要になります。

4.2 オープン系ネットワークと同等の対策を行う方法の例

図2にこの方法を採用したシステムの例を示します。

従来のシステムでは，本社の計算機センターにメインフレームコンピュータを置き，全国の支社に配置されたオフコンとの間を専用線またはISDN回線で結んで業務を行っていました。これに全面的にオープン技術を取り入れて改変したのが図2です。メインフレーム上のアプリケーションを UNIXサーバに移植し，オフコンもPC端末に変更しました。通信プロトコルをTCP/IP化し，ネットワーク機器を入れ替えました。オープン化したネットワークに接続されるPC端末上には専用のアプリケーションを搭載することはせず，市販のOSと一般的なブラウザソフトを用いることにして，開発費用とメンテナンス工数の削減を図りました。

セキュリティ保護の点から，業務システムが動作するサーバと，PC端末と通信するWebサーバとを分離し，その間はアプリケーションの作り込みによる独自手順で通信を行うようにしました。ファイアウォールを設置するとともに，不正なアクセスやウイルス，ワームの増殖，それらに起因する急激なトラヒック増加を検出するため，ネットワーク監視装置や侵入検知システムを要所要所に配置しました。

セキュリティの観点から，業務系システムに接続された機器は業務専用の利用とし，電子メールや日常業務などのいわゆるOA業務には用いてはならない規則としました。しかし，PC端末の場合，容易にその流用や転用が可能です。このため，フロッピーディスクや外部メモリ媒体を介したり，OA用PCの誤接続やルール違反の行為がなされたりすることによって業務系システムにウイルスやワームが広がる危険性を考慮し，その対策を施さなければなりません。

そこで，本業務系ネットワークにおいては接続するPC端末を厳しく制限するとともに，接続を許可したサーバやPC端末に対しては常に最新のセキュリティ対策を施す一方で，それが業務アプリケーションと競合して不具合を起こさないよう，搭載するソフトウェアや各種の設定までを厳密に管理しました。

具体的には，各支社・支店に配置されたすべてのPC端末のセキュリティ責任者を決め，PC端末上に搭載されたOSやアプリケーションのバージョン管理やパッチ適用を行うようにしました。一部の部門についてはその部門にセキュリティ技術に詳しい担当者を設定することができなかったため，その部門のPC端末はOSやアプリケーションのインストールから設定まで本社の情報システム部門で行い，変更が必要になった場合には代替用のPC端末を本社の情報システム部門から送付するようにしました。緊急にセキュリティパッチを適用したり設定変更を行う必要が生じた場合には，情報システム部門のセキュリティ管理者あるいは近隣の地区のセキュリティ管理者が直接訪問して作業を行うようにしました。

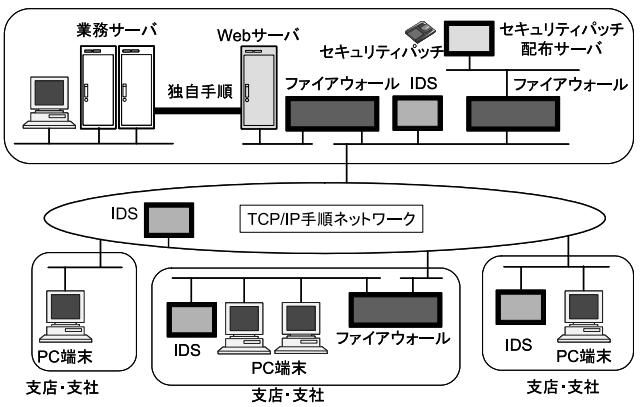

図2　オープン系ネットワークと同等の対策を行う方法
Fig.2　Security measures equivalent to open network system.

PC端末のセキュリティパッチの適用は，その端末がインターネットに接続可能であれば，OSのベンダーが提供するアップデートの仕組みを利用するなどの手段が可能です。しかしそのためには，本業務システム内のPC端末がインターネット上のWebサイトにアクセス可能となるようにしなければなりません。これは，インターネットと接続するための機器が必要となるだけでなく，その運用管理にも多くの工数が必要となります。また，インターネットとの間で自由な通信を許してしまうとそれがセキュリティ上の脆弱性となってしまうため，接続先を制限する必要があります。

さらに，セキュリティパッチが公開された際，システム内の多くの端末から同時にベンダーのサイトにアクセスが集中すると，ネットワークの帯域を圧迫してしまうため，その対処も必要となります。その上，利用者からすればアップデート用のサイトを閲覧できるのにその他のサイトを閲覧することができないのは不便で不自然であると感じることがあります。

本事例のシステムでは，これらのことを勘案し，インターネットとの接続は行わず，PC端末のアップデートを配布するための専用のサーバをネットワーク内に配置して，そこからパッチソフトをダウンロードさせるような運用としました。

現在のところこの業務系システムは，電子メールや日常業務などのいわゆるOA系のシステムとは分離されています。しかし，同様のシステムが連携なく同時に2つ存在することは費用面，運用面で大きな無駄があるので，次の機会には業務系システムとOA系システムを統合する計画があります。このときには，組織内の全システムのセキュリティレベルを業務系システムに要求されるレベルまで引き上げる必要があるので，さらに高度なセキュリティ対策を導入することが必要です。

4.3　閉じられたネットワークとする方法

業務系ネットワークを独立のネットワークとし，外部から完全に遮断することによってセキュリティを保つ方法です。

ネットワークそのものや接続する機器を物理的に隔離した上，厳しく管理し，ネットワーク上を通すアプリケーションも必要最低限のものにします。ネットワークに関する

情報は原則的に非公開とし，その存在自体も関係者以外には漏らさないようにします。利用者を制限し，誰がいつシステムを利用したかを記録に残します。

サーバやPC端末の設定変更やアプリケーションの追加，変更も行いません。セキュリティパッチの適用も，原則的には行いません。

4.4 閉じられたネットワークとする方法の例

図3はこの方式の実施例です。従来の業務システムでは，ホストコンピュータから全国の専用端末に対し，専用線を介して業務データを配信します。専用端末どうしの通信はなく，データ量もそれほど多くないため，専用回線は数十Kbpsから数百Kbps程度の速度です。これにオープン技術を取り入れ，図3のようなシステムとしました。ここで用いている専用端末は，複雑な動作を制御する機能を低価格で実現するため，装置の内部にPCを内蔵しています。専用端末として作られているため，内部のPCにはディスプレイやキーボードは接続されておらず，保守や緊急時にのみ接続する設計になっています。IPアドレスはあらかじめ設定した固定値とし，DNSも用いません。ネットワーク内の各ルータは，中央のコンピュータと各端末との間でのみ通信が可能となるような設定としてあります。さらに，通信を許可された経路であっても，所定のアプリケーションデータのみを通すようにしています。

ネットワーク機器やPC端末は通常のフロアから物理的に隔離した部屋に設置し，その部屋に入れる人を制限します。端末を操作することのできる利用者も制限し，さらに，サーバ側で利用状況の記録を取っています。

ネットワーク構成やアプリケーションの種類，利用しているポート番号等のセキュリティに関係する情報は利用者に公開しないようにしています。

本システムでは，万一，一部の端末がウイルスやワームに感染した場合でも，端末間の通信ができない設計になっているため，他の部門の端末への感染を防ぐようになっています。また，専用回線の帯域がそれほど大きくないため，感染した端末から大量のトラヒックが送信されても，センター側のサーバに大きな影響が出ないようになっています。

感染した端末は，その端末がつながっているネットワークのルータを制御して通信を遮断し，本システムから切り離します。感染した端末は，感染の原因や経路を調査した上で，ソフトをクリアインストールして修復します。

セキュリティ耐力のない設計なので一般に用いるには問題のある方式ですが，それを理解し正しい運用が可能となるような方策を講じた上で限定的に用いるならば，効果があります。

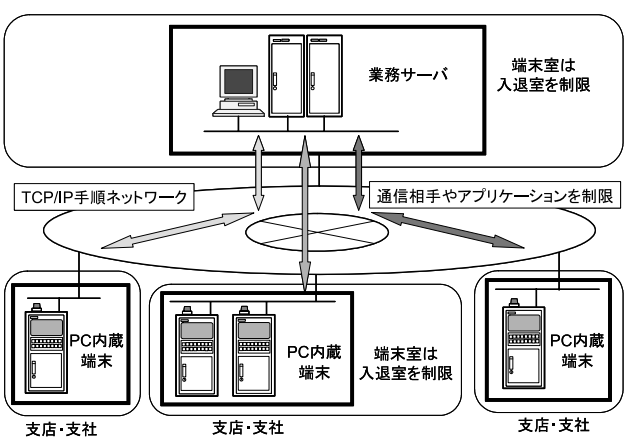

図3 閉じられたネットワークとする方法
Fig.3 Security measures equivalent to closed network system.

5. むすび

レガシー・マイグレーションにおいてオープン技術を用いる以上は，オープン技術が持つセキュリティ上の脆弱性も引き継ぐことになります。このため，たとえそれが閉じられた業務系のシステムであってもOA系と同様の考え方でセキュリティ対策を施さなければなりません。コスト低減のためにはオープン技術の採用は効果的ですが，それに伴ってセキュリティ対策にも留意し，相応の費用と工数を投入する必要があります。場合によってはレガシー・マイグレーションを行うことによってセキュリティ対策に必要な費用が増大し，その不利益がオープン技術を取り入れるメリットを上回ってしまうこともあります。

レガシー・マイグレーションは，このようなセキュリティ上の問題まで検討した上で進めないと，費用の削減につながらないばかりかセキュリティ上のリスクまでも増大する危険性がありますので，事前に十分な検討を行うことが必要です。

筆者紹介

Masashi Sugiura
杉浦（すぎうら） 昌（まさし） 1983年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部セキュリティ技術センターセンター長。

Tetsuji Tanigawa
谷川（たにがわ） 哲司（てつじ） 1985年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部セキュリティ技術センターコンサルティングマネージャー。