リスクの可視化から見直す情報漏えい対策

セコムトラストシステムズ株式会社
後藤　忍

はじめに

本年4月に同一企業グループで発生した情報漏えい事案は大きな話題になりました。３月に発生した大震災による原発の放射能漏れに続いての事であり、上半期を一文字で表すと「漏」であると言う人もいます。情報漏えい事案発生以降、多くの企業が、類似事案防止の観点からインターネット網と社内ネットワークの接点に生じる脅威への緊急対策を実施し、外部公開サーバのセキュリティ診断の需要が高まっています。しかし、今回の事案に対して、インターネット経由での攻撃を防げばよいといった一面的な捉え方をするのではなく、水が高い所から低きに流れるがごとく最も弱いポイントが破綻したと捉えるべきです。そして誰しもが「わが社は本当に大丈夫か？」と懸念を抱いた今こそ、インターネット経由の脅威に加え、情報漏えいが発生する可能性をすべて洗い出し、自社にとって最も弱いポイントを見極めた上で次の一手を打つべきであると考えます。その為には、リスクの所在について網羅性をもって明らかにする所からはじめる必要があり、リスクを判りやすく可視化する手法についてご紹介します。

１．企業の情報漏えい対策

企業の重要情報（顧客データ等）が格納されているデータベースはよく金庫に例えられます。
サーバは金庫室であり、サーバにアクセスできる端末環境は金庫が設置されているビルの入り口といった具合です。リアルの世界ではオフィスビルの一階にゲートが設けられているのをよく見かけるようになりました。又、顧客情報、重要システム、バイタルレコード等の保管室等はセンサーで監視し、異常を検知すると直ちに警備員がかけつけます。さらに権限のない者が仮に侵入したとしても、外に出ることができないアンチパスバックというシステムもあります。

サイバーの世界で同じ仕組みがあったとすると、データベースへのアクセスは何重ものセキュリティシステムで守られており、データベースのどのデータに誰がいつアクセスしたかはすべてリアルタイムに監視され、異常があればセッションを切った上にネットワーク経由で犯人を追跡するといった具合になります。

しかし、このようなシステムを実現している企業は現実的には皆無でしょうし、現在の企業のセキュリティ対策は江戸時代の関所に似ていると感じます。関所は江戸時代に「入り鉄砲に出女」というポリシーで、国内治安維持を目的として運営されていました。江戸から出る婦女は関所を通過する際、乗物の戸を開き、笠頭巾を取り、手形を提示し、改女に入念に調べられました。また、江戸に入る鉄砲は火薬や弾丸含めて厳重な取り締まりを受け、長持なども中に武器がないか調べられました。逆に江戸から出る武器についてはまったく取り調べがなかったといいます。

関所と改女はサイバーの世界のFirewallとWAF（Web Application Firewall）を連想させるのですが、このように単層のラインを設け、そこで出入りを監視しコントロールをするという方式が企業の情報漏えい対策の主流であったように思います。そして昨今は単層の関所方式の限界が指摘され、例え侵入されたとしても重要情報が外に漏れないよう多段防御によるインターネットの出口対策についてさまざまなアイデアが出てきています。

その一方で、外部の委託先や取引先との接点及び社員や社内常駐している派遣社員からの漏えいなどインターネット経由を除いた脅威についての対策は、企業の現場に赴くとまだまだ取組みが不十分であるという印象を否めません。対策を実施しているとか、していないではなく、課題としてすら挙げられていないというケースがよく見られます。

たまたまガンブラーなどの流行で外部委託先からのアクセスが課題になったり、USB利用禁止などの部分的な対策を行っている事でよしとしているとい

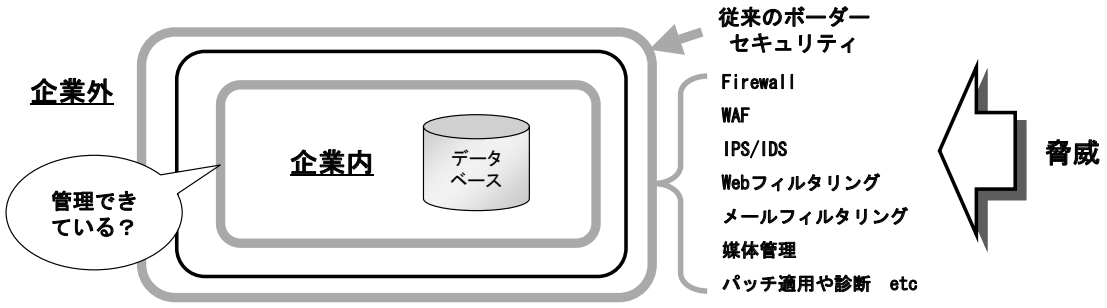

図1　脅威への対策の概念図

うのが実状であり、企業のセキュリティにおいて内部ネットワークやインターネット以外のポイントは「社員だから大丈夫」とか「長年、お付き合いのある委託先だから」「インターネットの口さえ守れば大丈夫」などの思い込みにより、対策がおろそかになっているのではないでしょうか。この部分に光を当て、内外すべての脅威を明らかにしないと本当の意味で情報は守れません。次項からはこのようなリスクをいかに洗い出すかという点について述べます。

2．リスク洗い出しの方法論

前項で情報漏えいの可能性を網羅的に把握すると述べましたが、リスクの把握に参考となる手法として幾つかのモデルがあります。NIST Risk Management Guide for Information Technology Systems（SP 800-30）、ISO/IEC 21827（ISSEAが開発したセキュリティエンジニアリングプロセス評価モデル）、ISO/IEC TR 13335（GMITS）などがそうです。SP 800-30は情報のオーナーやITシステムオペレーションの運用に関する最終決定者（Designated Approving Authority）、情報システムのセキュリティ責任者や経営者など幅広い層をターゲットにしたガイドラインです。リスクアセスメントのステップは次のようになっています。

- **Step 1**　System Characterization（システムの特徴の把握）
- **Step 2**　Threat Identification（脅威の特定）
- **Step 3**　Vulnerability Identification（脆弱性の特定）
- **Step 4**　Control Analysis（管理策の分析）
- **Step 5**　Likelihood Determination（発生可能性の決定）
- **Step 6**　Impact Analysis（インパクト分析）
- **Step 7**　Risk Determination（リスクの決定）
- **Step 8**　Control Recommendations（管理策の決定）
- **Step 9**　Results Documentation（文書化）

Step 1 System Characterization（システムの特徴の把握）では、システムの機能、システム及びデータの重要性や機密性を定義します。リスクアセスメントをはじめるにあたっての基礎データの収集です。次に**Step 2** Threat Identification（脅威の特定）でさまざまな脅威を洗い出します。例えば人的な脅威については、ハッカーやクラッカー、金銭取得等を目的とする犯罪者、テロリスト、産業スパイ、従業員（退職者を含む）に分け、それぞれにThreat Action（脅威の行動）を定義していきます。この際、挑戦や脅迫などといったMotivation（動機）にも着目せよとありますが、あまり詳細なステップは記載されていません。

Step 3 Vulnerability Identification（脆弱性の特定）は、NISTが公開している脆弱性データベース

（http://nvd.nist.gov/home.cfm）やベンダーが公開している脆弱性、脆弱性スキャンツールからの情報、ドキュメントレビューやオンサイトでのヒアリングを用いて、Threat-Source（何が？）とVulnerability（どのような脆弱性をついて）とThreat Action（どのような攻撃をする）の組み合わせ表（表1）を作成します。この組み合わせ表を用いてのリスク分析は通常よく行われていると思います。

Vulnerability	退職した従業員のIDがシステムから削除されていない。
Threat-Source	退職した従業員
Threat Action	企業のネットワークにダイアルし、機密データにアクセスする。

表1　脆弱性と脅威の組み合わせ

Step 4 Control Analysis（管理策の分析）で対策の検討を行います。その後、Step 5 Likelihood Determination（発生可能性の決定）でThreat-Sourceに強い動機があるか？及びStep 6 Impact Analysis（インパクト分析）で脅威が顕在化した場合の影響の大きさは？といった対策の優先順位付けの為の評価を行い、Step 7 Risk Determination（リスクの決定）以降でリスクの定量化→コントロールと代替コントロールの検討→リスクアセスメント報告書の作成をもってリスクアセスメント*が完了します。

これらの一連の手順での分析は有効であり、実際に利用されている組織もあると思います。しかし、Step 2 Threat Identification（脅威の特定）とStep 3 Vulnerability Identification（脆弱性の特定）についてもう少し詳細な手順を付け加えると、よりリスク洗い出しの網羅性を担保できるのではと考え、次項にそのステップについて記載します。

3.アクセス経路別のリスクの洗い出し

前述のように情報漏えい対策の網羅性を高める為には、脅威と脆弱性の洗い出しフェーズの精度に拠ります。よってもう少し詳細なステップを当該フェーズに付け加えることにします。

例えば物理的なセキュリティリスクの洗い出しの場合は人が動く導線を想定し、ゾーニングと併せてチェックを行いますが、それと同様にデータベースへの社内外からのアクセス経路、いわば情報の導線を特定し、経路別に脆弱点がないかをチェックするのです。

あるECサイトのデータベース内の情報を例に、アクセス経路別に分析を行なうステップについてご紹介します。

ステップ1
リスク洗い出しのスコープの決定

リスク分析を行なう範囲を決定します。（※ここではECサイトのシステムの内部セグメントにあるデータベースとします。）

ステップ2
データベースにアクセスする業務の洗い出し

まず、関係する業務をすべて洗い出します。業務から洗い出す事により、確実に簡単にデータベースのアクセス経路等の情報収集ができます。
例）コンテンツメンテナンス業務、コールセンター業務、システムメンテナンス業務等

ステップ3
データベースにアクセスする業務詳細の確認

ステップ2で業務を洗い出した後、業務を行なう拠点、業務を行なう社員や派遣社員の特定（Threat Sourceに相当）を行ないます。

ステップ4
データベースへアクセスするすべての経路及びその他のデータ伝送経路の特定

業務単位で、遠隔地の拠点からのアクセス経路、遠隔地の外部委託先からのアクセス経路、緊急メンテナンスの為の自宅からのアクセス経路、データセンターのメンテナンスルームからのアクセス経路、インターネット経由（会員のPC）というようにすべての経路を図2のように洗い出していきます。

＊リスクアセスメント：リスク分析からリスク評価までのすべてのプロセス(JIS TR Q 0008:2003)」

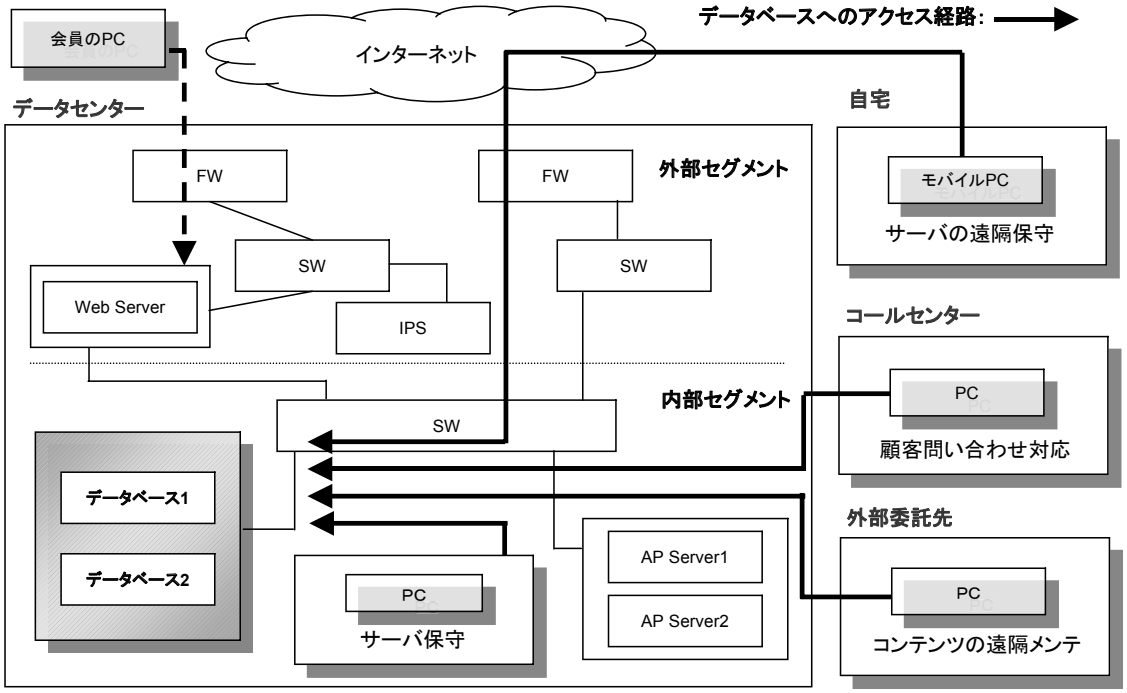

図2　データベースへのアクセス経路図の例

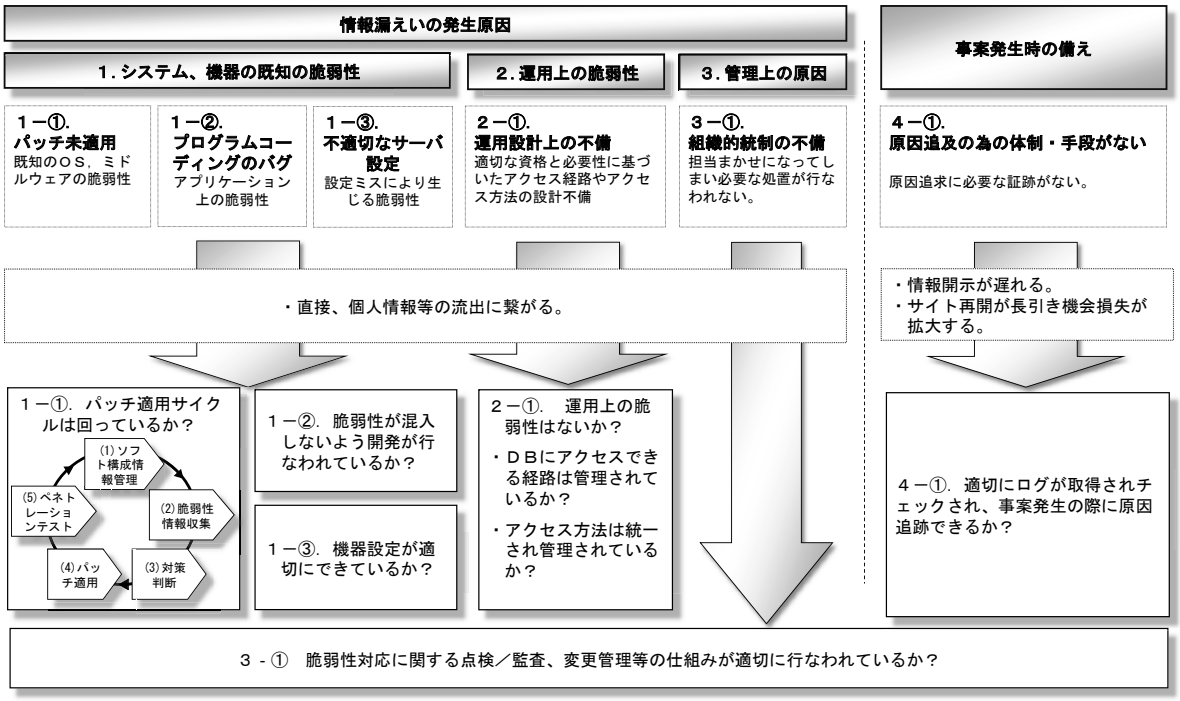

図3　情報漏えいの発生原因分類と分析のポイント

ステップ5
データベースへのアクセスの詳細確認

ステップ4とほぼ並行してアクセス経路別に誰が、いつ、どのような方法(ツール等)を用いて、どのようなデータにアクセスするかの組み合わせを特定します。データベースにアクセスする端末が設置されている部屋の入退室管理の内容や監視カメラのログの取得期間などのチェックも必要です。

ステップ6
アクセス経路別に脅威と脆弱性の洗い出し

脅威と脆弱性の洗い出しは、図3に示す情報漏えいの発生原因を念頭に置いて行ないます。図3の上段の1－①～3－①までが、直接個人情報等の重要情報の漏えいに繋がる原因です。これらに起因したどのような事案が自社に発生するかを洗い出します。

4－①は事案発生時、被害拡大に繋がる原因です。例え事案が発生しても早期に原因究明でき、情報開示およびシステム再開ができる備えが必要です。サイバーの世界ではリアルな世界と違って現行犯逮捕はできません。ログの取得を前提として、ログの解析等の対応については予め手順化されている必要があります。いざとなって慌てるようでは遅きに失するので、見落としてはいけないポイントです。

指摘しておきたい点として、脆弱性洗い出しの粒度があります。図3 1－①パッチ未適用を例にとると、図4のような脆弱性解消の為のパッチ適用のステップ(あるべき姿)に着目します。それぞれのステップが確実に実施されているか？実施されていないとしたら何が問題なのか？というような粒度で分析を行っていきます。パッチを適用しているか否かといった単純なベースラインによるチェックでは本質的な問題にたどり着かないからです。経験上、パッチ未適用の多くは技術的な問題の前に人的運用の問題が存在することが多いと考えられます。

このようにアクセス経路別に詳しく分析していくとよく見つかる脆弱性についてご紹介します。

(1) データベースのデータ参照制限を設けておらず、業務担当者がSELECT ALLで業務に必要のないすべての顧客情報(ID、パスワード、カード情報)を参照できてしまう。

(2) INSERT,UPDATE,DELETEに限定したデータベースログしか取得していない為、誰がいつどのようなデータを参照したか証跡がなく、事案発生時の原因追求が難しい。

(3) データベースにアクセスする端末で利用している独自ツールのログに、参照データ(個人情報など)が平文で保管されている。このように管理者が認識していない場所に重要データが保管されているケースがある。これでは、データベースだけを守っても意味がない。

これらの脆弱性はアクセス経路別に逐一精査し

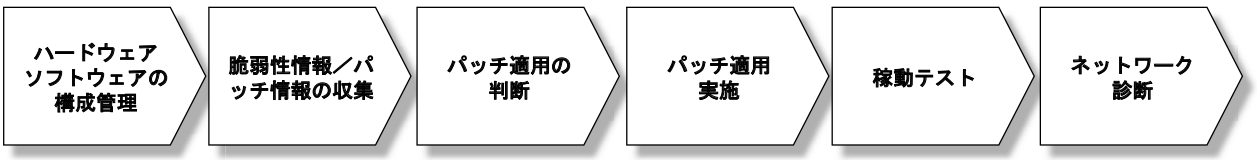

図4　パッチ適用のステップ

No.	アクセス					リスク	リスク詳細	改善策	区分
	拠点	部署	端末	手段	人				
1	本社オフィス	システム部	業務用PC	SQL-plus	パートナー30名	不正持出し	クレジットカード番号関連情報をデータベースから抽出し、業務用PCから印刷することによって不正に外部へ持出せてしまう。	クレジットカード番号情報のデータテーブルを暗号化する。	漏えい防止
2					社員5名	同上	社員はSQL-plusで抽出した情報をメールに添付して外部に送ることができる。	・メール監視システムを導入する。 ・データテーブルを暗号化する。	漏えい防止
3				FTP	社員5名	不要なサービスが有効	DBログにカード情報が平文で格納されており、FTPによりログファイルを取得する事ができる。	・DBログは直ちに他の要塞化したログ収集サーバに退避する。	漏えい防止
4				-	社員5名 パートナー2名	情報漏えい原因の特定が行えない	SELECT操作ログまでは取得されていないため、情報漏えい時に原因の特定が行えない可能性がある。	特定の行や列に対する SELECT を監査出来るファイングレイン(FGA)監査ログを取得する。	事後対策

表2　本社オフィスからデータベースにアクセスする経路のリスク分析の例

ないとなかなか気付かないポイントです。上記の表2のようにまとめ、データベースへのアクセス経路図(図2)と紐づければ、誰が担当している業務のどこにどのような脆弱性があるかを判りやすく可視化できます。

これでStep 2　Threat Identification(脅威の特定)とStep 3 Vulnerability Identification(脆弱性の特定)の部分をより効果的に実施していく事ができ、漏れなく改善すべきポイントを拾い上げることができます。このような作業を基点として、SP800-30のStep 4 Control Analysis(管理策の分析)以降の対策の決定および対策の優先順位付けへと繋げていきます。

アクセス経路別のリスク洗い出しの利点について、可視化と網羅性の確保以外にもう一つ付け加えておきます。例えばチェックリストを用いて監査を実施する場合、チェック項目毎に○：実施、△：一部実施、×実施していないなどのように合否チェックを行いますが、対象は漠然とサーバ全体、ネットワーク全体、端末全体とグループ化してチェックしているのが一般的です。

目的によりこのような粗い粒度のチェックも有効ではありますが、誰が何を改善すればいいのか判りやすく可視化するという点においては、拠点別、部門別にやるべき事を明確に整理できるアクセス経路別の分析は都合が良いと考えます。

アクセス経路別のリスク洗い出しを実際にやってみて判ることは、往々にして情報漏えい対策の対応がもぐら叩きになってしまっているという事です。当初システムを開発した担当者がいなくなり、アクセス経路やアクセスできる権限などの設計の考え方も明文化されておらず、そのシステムのセキュリティには疑問を抱かず日々運用がなされています。
改めてセキュリティ品質をシステム及びシステム運用のライフサイクルに練りこむような品質保証体制が必要と感じます。

4．最後に

過去の経験を振り返りますと企業のシステム及

び運用は、十分にセキュリティを考慮して設計されてはおらず、可用性偏重になっているものが多く見受けられました。パフォーマンスが気になるからとデータベースのログは取らず、運用に便利だからと過剰な権限を社員や委託先に付与しがちです。

「去るものは日々に疎まれ生ける者は日々に親しむ」という中国の詩があります。人は目の前からいなくなると忘れ去られてしまうという意味であり、人は見えないものには注意を払いません。システムや運用上のセキュリティ品質はシステム停止に繋がる品質と違って通常目に見えることはありません。日々に疎まれ、システム責任者や経営層は知る由もないのが実状ではないでしょうか。

しかし、それらはやがて情報漏えい事案という大きなインパクトをもって顕在化する可能性をはらんでおり、今が過日発生した大きな情報漏えい事案を他山の石とし、セキュリティリスクの総点検を行なう良い機会であると思います。是非、情報漏えいへの取組みを日々に親しむものにしていただきたいし、我々もそうなるように益々励んでまいります。

（参考文献）

「セキュリティはなぜやぶられたのか」ブルース・シュナイアー著、井口耕二翻訳　日経ＢＰ社

「関所　その歴史と実態」大島延次郎著　新人物往来社

「ネットワークセキュリティHACKS　プロが使うテクニック＆ツール　100+」Andrew Lockhart著、渡辺勝弘、鶴岡信彦、黒川原佳訳　オライリー・ジャパン

「今、必要な情報セキュリティマネジメント」村田一彦著　ジャストシステム

「ＩＴリスクの考え方」佐々木良一著　岩波新書

National Institute of Standards and Technology「Risk Management Guide for Information Technology Systems」（Special Publication 800-30）Gary Stonebumer,Alice Goguen,and Alexis Feringa
http://csrc.nist.gov/

迫りくるネットワークセキュリティのパラダイムシフト 注目を集めるネットワーク仮想化技術と OpenFlow/SDN

東京エレクトロン デバイス株式会社　ビジネス・デベロップメント部
水本　真樹

はじめに

先の東日本大震災を契機として、いま企業ではクラウド環境にITインフラを移行しようという流れが加速している。災害に備えたBCP（事業継続計画）の観点から、ビジネスの価値の源泉であるシステムを自社内のオンプレミスな環境で稼働させるのではなく、堅牢なデータセンターに移すことで、その安全性の確保を図ろうというのがそのねらいだ。

その一方で、こうしたクラウド環境へのニーズの高まりは、かねてより指摘されてきたセキュリティに関する懸念を改めて顕在化させている。具体的には、企業がこれまで自社内のオンプレミスの物理的な環境で確保していたのと同等のセキュリティを、仮想化技術を基盤とするクラウド環境においていかに確保するかが重要な課題として指摘されている。

そうした課題を解消するためには、特にネットワークにおいて、パラダイムシフトともいうべき技術革新が不可欠だといえる。ここでは、今後、企業の主要なITの利用形態になると目されるハイブリッドなクラウド環境において、セキュリティの担保に貢献するものとして注目されるネットワーク仮想化技術を取り上げ、その最新の技術動向と関連する業界の動きにもスポットを当てたい。

クラウド環境における ネットワーク仮想化の必然性

周知の通り、クラウド環境においては、サーバやストレージなどの物理リソースを隠蔽して分割利用する仮想化技術を基盤に様々なサービスが展開されている。近年、そうしたサーバやストレージに関する仮想化技術が急速に進化を遂げ、例えば物理的には1台のサーバを複数台のように扱ったり、複数のストレージを1つにまとめてその領域を分割するといったことが可能となっている。

これに対しネットワークの仮想化はというと、20年以上も前から利用されているVPNやVLANがいまだ現役であり、サーバやストレージの仮想化が提供する柔軟性や拡張性と比較し、それは極めて限られたものでしかないというのが実情だ。

今後、企業システムは、単一のクラウドからプライベート／パブリック間の相互連携、あるいはプライベートネットワークとクラウドの相互接続へと進化していくことが想定される。そうした環境にあって、ネットワークセキュリティを担保しながら、仮想化やアプリケーション分散化といったクラウドの提供する付加価値を享受するためには、サーバリソースやストレージリソースを含むインフラをトータルに仮想化するネットワーク仮想化技術が不可欠だといえる。

ネットワーク仮想化技術とは、端的に言うなら、スイッチやルータといった物理ネットワーク機器のリソースをアプリケーションなど上位プロトコルに対して隠蔽する技術だ。その利用により、クラウドネットワークの上に仮想化のレイヤを設けることで、ユーザーの要求に応じて、ネットワークやサーバ、ストレージなどのリソースを仮想的なスライスとして提供するということが可能となる。

現在のところ、大規模なネットワークを物理的に共有しながら、トラフィックについての分離を行って論理的なセキュリティを担保するための仕組みとしては、クラウド基盤環境においてもVLANが広く利用されている。複数のVLANを通過させるためにトランクポートを設定し、ユーザーごとに論理的に分割するための識別情報としてタグIDを付加して動作させるという形である。

しかし、こうした方法では、クラウド環境で提供されるプロビジョニングのメリットが十分に活かし切れないという問題がある。具体的には、プロビジョニングによって動的に追加されたサーバをいざネットワークに接続するとなると、ネットワーク管理者が各種設定や物理接続などを手作業

で変更する必要があり、相応の手間と時間を要するわけだ。このように仮想化によってモビリティを増したサーバ環境に対し、ネットワーク側がいかに追随していくかが重要な課題として浮上してきており、そうした課題を解消するものとして期待が寄せられているのがネットワーク仮想化技術だというわけである。

新たな設計思想に基づく ネットワーク技術の登場

そうしたネットワーク仮想化を支える技術として、最近、とりわけ注目を集めているのが「OpenFlow」だ。これは「ソフトウェア定義ネットワーク（Software Defined Network : SDN）」に基づくもので、SDNでは一元的に管理を行うコントローラがスイッチやルータなどの機器に対してソフトウェア的に指示を出すことで、フロー制御等の設定が可能になる。OpenFlowでも、フローテーブルを機器側に保持し、リモートでその内容をコントロールできるようになっている。

OpenFlow登場の背景には、既存技術に捉われない新たな設計思想・技術に基づいてインターネットのアーキテクチャを根底から考え直そうとする動きがある。例えば、現在、規格策定が進められている、「NWGN（NeW Generation Network）」や「FI（Future Internet）といった次世代ネットワークへの取り組みもこれにあたり、これらは現在のIPとは異なる技術に基づいて設計されるクリーン・スレート・アーキテクチャである。これらの技術の研究開発は、すでに実証フェーズを迎えている段階で、2020年頃には標準化が見込まれている。

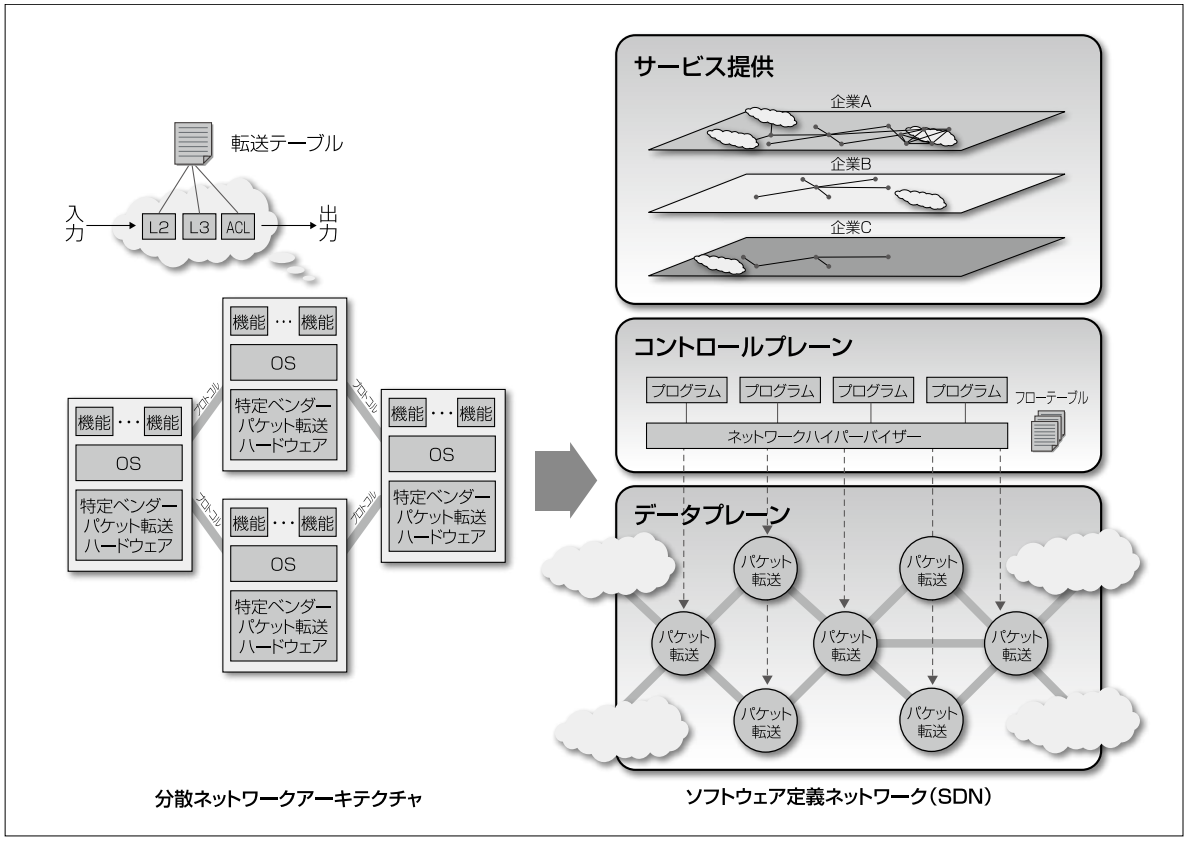

図1　ネットワーク仮想化で具現化する次世代インフラストラクチャ

日本においても様々な実証が進められている。

OpenFlowは、まさにそうした次世代ネットワークに向けた取り組みの中から生み出されたものである。その特徴は、入力ポートとMACアドレスやIPアドレス、ポート番号などの組み合わせによるフローエントリベースでネットワーク制御を行うことができる点と、セキュアチャンネル経由でコントローラからリモート制御ができる点で、通信品質の確保やネットワークの利用効率の向上などが期待されている。

OpenFlow仕様の最初のドラフトを作成したMartin Casadoによると、開発のきっかけはこれまでのネットワークは設計者が直面する様々な問題に対し対応できないことは明確だったためだということだ。コンピュータと異なり、ネットワークは強固なセキュリティを確保するためにプログラム化をすることができなかった。そのため運用者がセキュリティポリシーを適用しなければならなかったが、これは対応の遅れや事故やエラーの原因となる。彼がきっかけとなり、Stanford大学を始めとした同じ思いを持つコミュニティの力によってネットワークセキュリティに大きな転機が訪れようとしている。OpenFlowはWANや巨大なデータセンター、ネットワーク仮想化、モビリティ、non-IPネットワークなどに有効な解決策を提供していくだろう。

現在OpenFlowの推進には、ユーザー主導による新たなネットワーク技術の策定を目指すONF（Open Networking Foundation）が当たっており、この団体にはGoogleやYahoo、Facebookといった米国の主要なユーザー企業のほか、ネットワーク機器を提供する主要ベンダーなど44社も参加している。余談ではあるが、こうした構造からは、ONFがインターネットに関する標準化を行うIETF（Internet Engineering Task Force）と同様の役割を、NWGNやFIといった次世代ネットワークの分野で担おうと画策しているものとも考えられる。

OpenFlowをめぐっては、現状ではまずIP上に適用するという取り組みが進められており、データセンター内のサーバ間接続の用途に向けた製品などがすでに市場投入されている。SDNアーキテクチャに基づく製品自体は、かねてより各ネットワーク機器ベンダーから提供されてきてはいるが、その利用にはすべてそのベンダーの製品で統一しなければならないといった問題がある。これに対しOpenFlowは、その設計技術がオープンになっており、OpenFlowの仕様をサポートする複数のメーカーのコントローラやスイッチなどを自在に組み合わせて利用することが可能である。例えば、OpenFlowコントローラを開発している米国Nicira Networksなどは、オープンソースでOpenFlowに対応している分散仮想スイッチ「Open vSwitch」や、スイッチ提供メーカーとの提携を模索しているようである。

こうしたOpenFlowコントローラで制御できるフローを利用すれば、複数の物理スイッチや仮想スイッチで構成される仮想化環境において論理ポートや論理スイッチを構成することができる。これにより、例えば、プライベートネットワークにおいてアプリケーションの要求に応じる形で、ネットワークを仮想的に分割してシステム利用者に提供するといったことも可能になる。様々なセキュリティサービスを統合化したり、セキュリティポリシーをプログラマブルに適用する分散ファイアウォールや統合セキュリティシステムを開発できる可能性も広がる。注目されつつあるCloudStack、OpenStackなどのクラウド管理システムを起点に、ハイブリッドクラウドやクラウド間ネットワークを統合する動きも出てきている。

ライブマイグレーション実行時のネットワーク側の課題を解消

一方、冒頭でも触れた、震災を契機に加速している企業におけるBCPの取り組みにおいても、ネットワーク仮想化が持つ意義は大きい。一般にBCP

対応では、システムを広域分散させて冗長化することで、有事に際して速やかなサービスの回復を図ることになるが、そうした対策を効果的に支援する技術にライブマイグレーションがある。これは、仮想マシン上のサーバOSやアプリケーションを、稼働させたまま別の物理サーバ上に移動するというものだ。

ただし、ここで問題となるのが、地理的に異なるネットワークに配置された物理サーバ間を仮想サーバが移動することにネットワーク側が追従できないということだ。というのも、仮想マシンのIPアドレスといったレイヤ3の情報が移動先でも引き継がれるため、移動先で同一のネットワーク接続を持つことが求められるのである。このため、遠隔でライブマイグレーションを行うには、専用回線や機器を敷設する、あるいはリカバリ対象を一部のサービスに制限するという対応が必要となる。

これに対し、回線等の敷設を行うことなく、より柔軟なライブマイグレーションを実施するには、大規模でフラットなレイヤ2網を構成し、ネットワーク機器において物理的な接続や設定変更なしに対応できるようにしておくという方法がある。これに関しては、先頃、日本電信電話株式会社（以下NTT）が実施した遠隔ライブマイグレーションの実証実験が大いに参考になろう。NTTでは、米国Nicira社の仮想ネットワーク制御技術とOpenvSwitch、KVMというオープンな技術を用いて、専用のハードウェア機器を用いることなく、ソフトウェアによってトンネリング手法の一種であるL2 over L3による論理ネットワークを構築。遠隔地にある武蔵野と厚木の両センター間での遠隔ライブマイグレーションを実現している。

※NTTがNicira社と共同で遠隔ライブマイグレーションに成功
http://www.ntt.co.jp/news2011/1108/110802a.html

現実的なアプローチとなるオーバーレイネットワーク

最後に、企業におけるオンプレミスとクラウド、クラウド間のネットワーク接続におけるネットワーク仮想化のメリットをまとめておきたい。現在では、これらの接続を実現するために、データセンター内に他のユーザーからネットワーク的に隔離されたユーザー企業の専用領域を作り、その専用領域とユーザーのデータセンターとを、VPN回線やタグVLANを利用して、LANのセグメントを論理的に分割してつなぐという方法がとられている。ネットワーク仮想化では、こうした作業に伴う煩雑さをトータルに解消する。

ネットワーク仮想化には、大きく分けて2つのアプローチがある。1つは、ネットワークのエッジ側に存在する仮想マシンや物理サーバの接続を仮想化して、論理的にネットワークで接続するというオーバーレイネットワーク方式。そしてもう1つが、ネットワークのコア側をスライスする方式である。

このうち、現在のシステム環境に適用し易いのは、やはり前者のオーバーレイネットワーク方式である。何よりも、既設ネットワーク資源を活かすことができることに加え、物理的な回線の抜き差しやスイッチの設定変更などの手間も不要なので、機器のコストや運用コストの削減を実現できる。さらに、VLAN数の制限に縛られないプライベートネットワークを実現し、マルチテナントのクラウドの構築や課金処理など付加価値サービスの提供なども容易となる。

レイヤ2のクラウドや仮想化のインフラでは冗長構成なども考慮し、トラブルを回避する対策が必要でリング構成やマルチパス技術をベースにした大規模なイーサネット・ファブリックが用いられていくだろう。こうした冗長化は物理的な制約や相対的なコストがかかるため、OpenFlow技術とレイヤ3のマルチパス、ソフトウェア、仮想マシンを

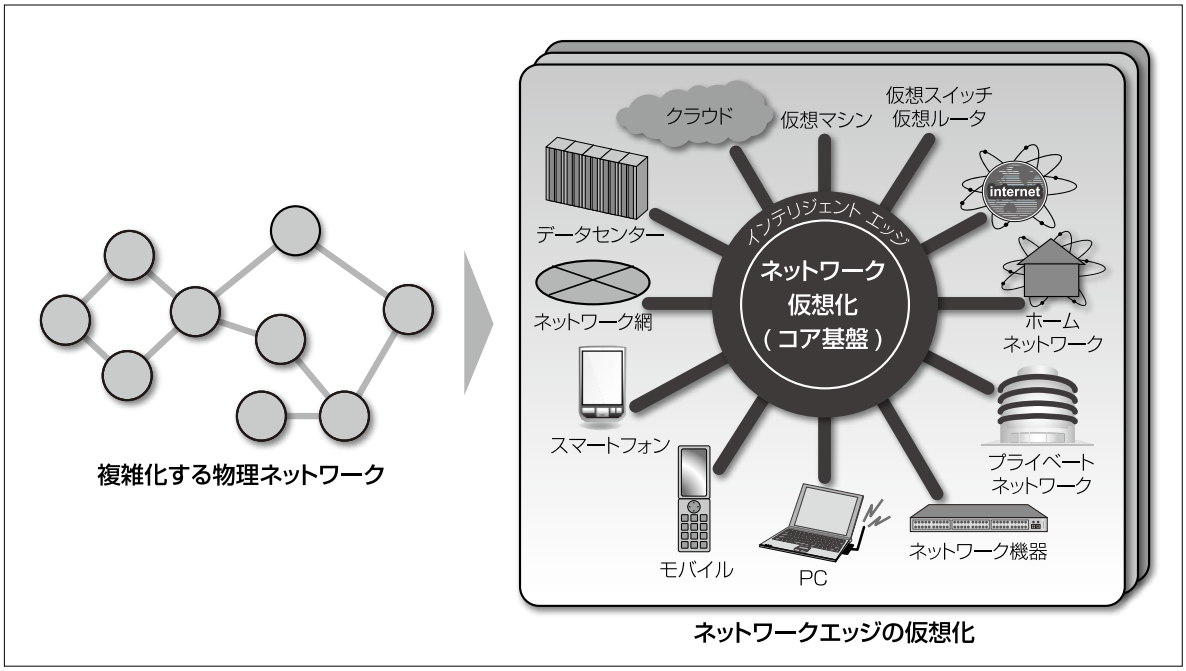

図2　インテリジェントエッジのオーバーレイネットワーク方式は、ネットワーク仮想化の現実解

利用したスイッチ技術とを組み合わせるオーバーレイネットワーク技術も出てきている。

さらに、本記事執筆中にも新たなVXLAN（Virtual eXtensible Local Area Network）仕様がIETFにドラフトが提出されている。これはレイヤ2オーバーレイヤ3（L2 over L3）のオーバーレイネットワーク技術であり、今後も目が離せない。またライブマイグレーションによる仮想マシンのインスタンス化や、インフラ内での仮想マシンの移行に対して自動的に追従するための仮想スイッチ処理や、プロファイル適用を外部スイッチにオフロードするエッジ仮想スイッチなどに関する標準として、IEEE802.1Qbgなどがいま審議されつつある状況だ。

今日では、例えば、電力は利用するものから保有するものへ、ICTについては所有するものから利用するものへといった社会インフラの大きな変化が起きており、こうした流れは今後一層加速していくことになる。ここで紹介したネットワーク仮想化や次世代ネットワークの世界でもパラダイムシフトと呼べる転換がいままさに眼前において展開されている。日本の競争力強化のためにも、そうした動向をしっかりと見据え、その動きに決して乗り遅れないことが何よりも肝要だ。