特集論文

クラウドシステム構築のためのセキュリティ基盤(3) ー仮想ネットワークー

清水直樹* 高畑泰志**
都築宗徳*
平井 肇*

Security Platform for Cloud Computing Based Systems—Virtual Network—

Naoki Shimizu, Munenori Tsuzuki, Hajimu Hirai, Yasushi Takahata

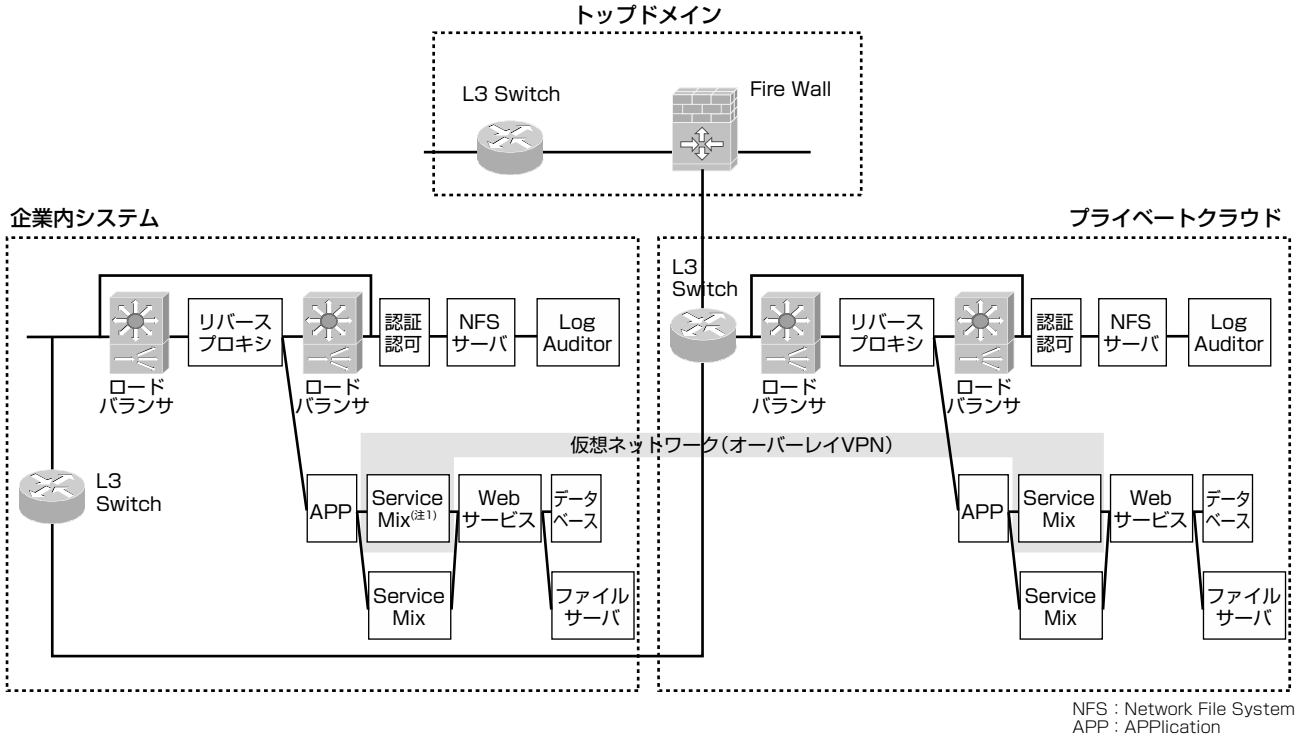
要 旨

クラウド環境は，企業の情報システムとして期待されているが，セキュリティの面で課題が残されている。通常，クラウド環境はネットワーク経由で利用されることから，ネットワーク上のデータ転送の面でもセキュリティを向上させることが必要である。

ネットワーク仮想化技術は，物理ネットワークとは独立した仮想ネットワークを構築し，仮想ネットワークで接続された機器間でセキュアに通信することを可能にする。三菱電機では，要求が発生した場合に動的にオーバーレイネットワーク(オーバーレイVPN(Virtual Private Network))を構築し，VPN内でのみ通信することが可能なオンデマンドグループ通信を実現するネットワーク仮想化技術“分散型仮想ネットワーク”を提案し，研究開発を行ってきた。

今回，“クラウド環境活用に向けた企業内既存システムとの連携実証実験”で，分散型仮想ネットワークをネットワーク仮想化技術に適用し，クラウド環境におけるネットワーク仮想化の実証実験を行った。

実証実験においては，企業内システムとプライベートクラウドにまたがるオーバーレイVPNを分散型仮想ネットワークによって構築した。オーバーレイVPNに接続する装置間では，企業内システムとプライベートクラウドの境界を越えて仮想ネットワーク上の通信が行える一方で，オーバーレイVPNに接続しない装置間では仮想ネットワーク通信を行うことができず，仮想ネットワークによって論理的にネットワークが分割されていることを確認した。



ネットワーク仮想化実証実験の論理接続図

クラウド環境活用に向けた企業内既存システムとの連携実証実験で，分散型仮想ネットワークによって企業内システムのService Mixとプライベートクラウドの Service Mix各1台について，企業内システムとプライベートクラウドにまたがるオーバーレイVPNを構築した。オーバーレイVPNを構成するService Mix間でのみ仮想ネットワーク上の通信が可能である。

*情報技術総合研究所 **同研究所(情報学博士)

1. まえがき

ネットワーク仮想化技術は，ネットワーク的に同じものを分割し，またネットワーク的に異なるものを結合して仮想のネットワークを構成し，仮想ネットワークで接続された資源をセキュアに利用することを可能にする。

近年台頭してきたクラウドコンピューティング環境(以下“クラウド環境”という。)は企業情報システムとして期待される一方で，セキュリティ上の課題があることからその利用が拡大していないのが現況である。クラウド環境はネットワークによって接続されたコンピュータ資源を利用者がその空間的配置などを意識せずに利用するシステムであり，クラウド環境の利用はネットワーク経由であることから，ネットワーク仮想化の適用によってクラウド環境利用におけるセキュリティを向上させることが可能である。

本稿では，クラウド環境活用に向けた企業内既存システムとの連携実証実験で行ったネットワーク仮想化手法の調査と，クラウド環境におけるネットワーク仮想化実証実験について述べる。

2. ネットワーク仮想化手法

ネットワーク仮想化手法は，暗号化等によって情報を秘匿することによって他者との独立を実現する方式と，ネットワークを多層化して他者との独立を実現する方式に分けることができる。情報の秘匿によるネットワーク仮想化技術の多くは，インターネット経由でVPNを構成することを目的としており，代表的な技術としてIPsec(Security Architecture for Internet Protocol)-VPN，SSL(Secure Socket Layer)-VPNなどが挙げられる。一方，ネットワークを多層化する仮想化方式は，専用の伝送／交換機器が必要となることから通信キャリアのネットワークを含めて主には閉域網でVPNを構築する技術であり，代表的な技術としてVLAN(Virtual Local Area Network)，IP-VPN，オーバーレイVPNなどが挙げられる。

当社では，P2P(Peer to Peer)技術に基づいたオーバーレイVPNの技術である分散型仮想ネットワーク[(1)(2)]を提案し研究開発を行ってきた。分散型仮想ネットワークはアプリケーション層で物理的なネットワークと独立した仮想の上位層ネットワーク(オーバーレイネットワーク)を構築するので，閉域網に限らず自由にネットワーク仮想化を実現することが可能である。今回の実証実験では，ネットワーク仮想化手法として分散型仮想ネットワークを適用した。

3. ネットワーク仮想化実証実験

3.1 分散型仮想ネットワーク

分散型仮想ネットワークの目的はオンデマンドグループ通信の実現である。オンデマンドグループ通信は，企業における業務など利用者の行動に応じた特定メンバー間の通信が可能なグループをオンデマンドで構成し，

(1) 関係者外への漏えいのない安全なグループ通信
(2) 時限プロジェクトなど期限付きネットワークのための動的なグループ構成
(3) ユーザーの属性に基づくアクセス制御

を実現する。例えば**図1**に示すように各プロジェクトや拠点に対応するグループを生成して，同一グループに属する端末間でのみ通信することが可能になる。

3.2 分散型仮想ネットワークのパケット転送

多くの端末を収容するスケーラビリティとネットワークの障害に耐え得る信頼性を持たせるため，分散型仮想ネットワークではオーバーレイネットワークの構築と管理に特化した専用装置DVC(Distributed Virtual network Controller)をネットワーク上に分散配置してオーバーレイネットワークを構築する。

図2で各DVCは隣接するDVCとP2P技術によって接続されており，リング状のDVCのネットワークが構成されている。そして各DVCにユーザー端末が接続される。

分散型仮想ネットワークではID情報を用いてユーザー端末間のパケット転送を行う。ID情報は通信グループのIDとユーザーのIDからそのユーザー端末が接続するDVCを検索するためのデータベースである。このデータベースは通信グループIDとユーザーIDのハッシュ計算値を検索キーとして構成されており，DVC間で分散管理される。ハッシュ計算値によるデータベースが分散管理されることから分散ハッシュテーブル(Distributed Hash Table：

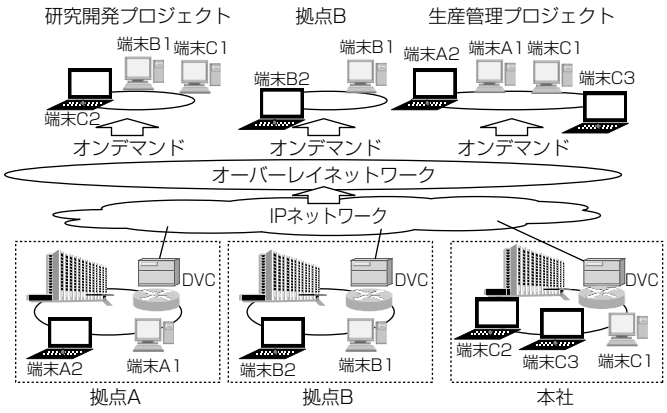


図1．オンデマンドグループ通信

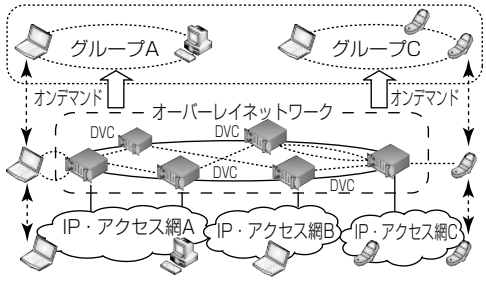


図2．分散型仮想ネットワーク

DHT)[3]と呼ばれる。

図3に示すように，ユーザー間で通信する場合に送信パケットは，

①送信元端末aは，あて先端末bへのパケットを自分の送信元接続DVCであるDVC1に送信

②DVC1からあて先端末bのID情報を管理するDVC2までは，DHT探索によって転送

③DVC2であて先端末bの接続先DVCがDVC3と判定され，DVC3まで転送

④DVC3からあて先端末bに転送

という手順であて先端末まで届けられる。

グループIDとユーザーIDをキーとしたあて先情報管理が行われているので，同一グループに所属しない端末間のパケット転送についてはあて先DVCの検出に失敗する結果となり，同一グループ内に閉じたセキュアな通信が可能となる。

3.3　分散型仮想ネットワークを構成する技術

分散型仮想ネットワークは仮想ネットワーク制御ソフトウェア，仮想ネットワークドライバ，仮想ネットワーク管理ソフトウェアの3種類のソフトウェアによって構成される。**図4**に各ソフトウェアの接続構成を示す。

3.3.1　仮想ネットワーク制御ソフトウェア

仮想ネットワーク制御ソフトウェア(以下“制御ソフトウェア”という。)は，IPネットワーク上にオーバーレイネットワークを構成し，仮想ネットワークを用いた通信機能を実現するためのソフトウェアであり，パケットの中継処理を行うサーバとして設置する。制御ソフトウェアはID情報のデータベースを管理し，ID情報に基づいて端末ごとに通信の可否を判定してパケットのルーティングを行う。制御ソフトウェアが動作する装置がDVCである。

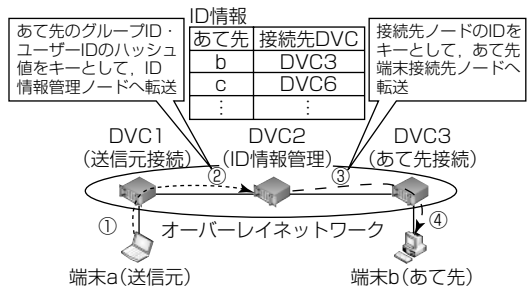


図3．分散型仮想ネットワークのパケット転送

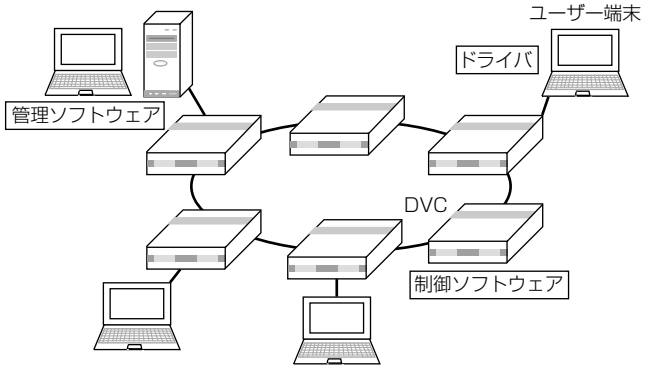


図4．仮想ネットワークソフトウェアの接続構成

3.3.2　仮想ネットワークドライバ

仮想ネットワークドライバ(以下“ドライバ”という。)は，ユーザーアプリケーションから受信したパケットをカプセル化して仮想ネットワークに送出するためのソフトウェアである。仮想ネットワーク通信を行う各端末にインストールして用いる。ドライバはホストの内部に仮想的なネットワークインタフェース(NIC)を生成するので，ユーザーアプリケーションに手を加える必要はなく，インタフェースを変更するだけで仮想ネットワークを使用することができる。

3.3.3　仮想ネットワーク管理ソフトウェア

仮想ネットワーク管理ソフトウェア(以下“管理ソフトウェア”という。)は，制御ソフトウェアとドライバによって構成される仮想ネットワークの接続状態の収集と可視化をするソフトウェアである。管理ソフトウェアが収集した情報はウェブブラウザを用いて画面表示することができる。

3.4　実証実験構成

図5に実証実験の仮想ネットワーク構成を示す。物理ネットワーク上では，企業内システム内，プライベートクラウド内の各装置はレイヤ2スイッチ(L2SW)によって相互に接続されている。また，企業内システムとプライベートクラウドはレイヤ3スイッチ(L3SW)で接続されている。物理ネットワーク上ではすべての装置が接続された状態であり，通信可能なネットワークとなっている。

DVCは企業内システムにDVC1，プライベートネットワークにDVC2が配置されている。VN(Virtual Network)管理は管理ソフトウェアが動作する仮想ネットワーク管理である。

ネットワークの仮想化は図中のService Mixに適用した。Service Mixはオープンソースの ESBである。ここではService Mixが動作する装置をService Mixと呼んでいる。

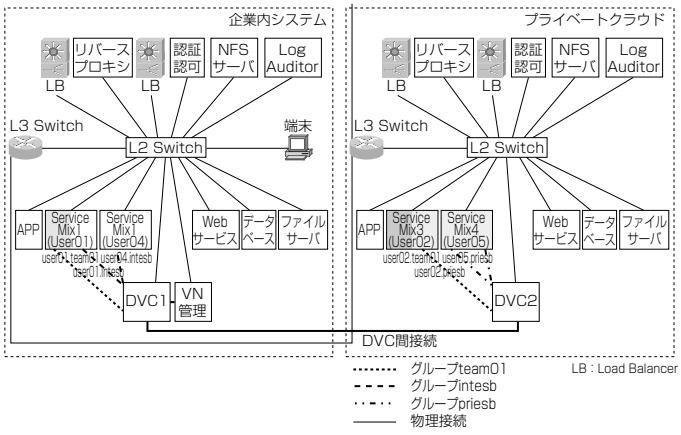


図5．実証実験の仮想ネットワーク構成

企業内システムのService Mix1(S.M.1)とService Mix2(S.M.2)が参加するグループintesb，プライベートクラウドのService Mix3(S.M.3)とService Mix4(S.M.4)が参加するグループpriesb，企業内システムとプライベートクラウドにまたがったS.M.1とS.M.3が参加するグループteam01の3個のオーバーレイネットワークを構成している。各Service Mixには所属するグループに対応する仮想ネットワーク用の名前が与えられる。2個のグループに所属するS.M.1とS.M.3は各グループに対応した2個の名前を持っており，通信するグループに応じて使い分けられる。

3.5 実証実験結果

実証実験ではアプリケーションとしてpingを使用し，企業内システムのService Mixからプライベートクラウドの Service Mixをpingによってサーチすることによって，ネットワーク仮想化の効果について確認を行った。企業内システムのS.M.1からプライベートクラウドのS.M.3に対して実行したグループteam01を使用したpingでは，両S.M.ともグループteam01に所属しており，仮想ネットワーク上をパケットが転送され，pingのReplyがS.M.1に到着することが確認できた。一方，S.M.1からプライベートクラウドのS.M.4に対して実行したpingでは，グループteam01，グループpriesbのいずれのグループを使用した場合にもpingの応答は返らず，仮想ネットワークによって両S.M.が遮断されていることが確認できた。また，企業内システムのS.M.2からプライベートクラウドのS.M.3／S.M.4に対して実行したpingについても応答は返らず遮断されていることが確認できた。

クラウド環境ではネットワークで接続されたコンピュータ資源が多数の利用者によって使用されるため，関係しない装置間を遮断することは不正行為の防止などセキュリティの向上において効果的である。また，クラウド環境は仮想マシンによって構成されることも多く，ネットワーク仮想化による論理的な遮断はクラウド環境におけるセキュリティ向上に効果的であると考えられる。

4. むすび

今回の実証実験では，プライベートクラウド環境を併用する企業ネットワークで，ネットワーク仮想化の実験を行った。具体的には仮想ネットワーク制御ソフトウェア(制御ソフトウェア)と仮想ネットワーク管理ソフトウェア(管理ソフトウェア)を使用して，企業システムとプライベートクラウド間の通信路を論理的に分割できることを確認した。

実験結果から，制御ソフトウェアによってあらかじめ許可された組合せの装置(Service Mix)間だけが通信可能で，他の組合せでは通信不可能となるように制御できていることを確認できた。また，管理ソフトウェアによって通信可否の組合せ(アクセスリスト)の集中管理と，組合せに基づく通信制御を可視化できることを確認した。

この実験の構成はネットワーク仮想化機能を確認するための最小限の構成となっており，実際のネットワーク構成を考慮してクラウド環境への本格的な展開を図るためには更なる機能拡張が必要である。本稿の締めくくりとして，今後の検討課題となる主要な拡張機能について述べる。

(1) 様々な機器，接続環境への対応

ロードバランサやVLANなどの導入によって，機器構成とネットワーク構成の対応が複雑化している現実のネットワーク環境下でも，ネットワーク仮想化機能を利用できるようにする。

(2) 管理機能の高度化

物理層，仮想層の両方を統合的に管理するネットワークリソースマネジメントを実現するため，管理ソフトウェアの機能を拡張し，物理層のネットワーク構成管理や経路制御も統合的に行えるようにする。

(3) セキュリティ

今回の実証実験では各ホストに専用ソフトウェアを載せて通信することが前提であり，ホストの設定に頼ることがセキュリティ上の弱点となり得る。例えば仮想ネットワークインタフェースをプロキシサーバやルータのような外部の通信機器に集約し，ホストからの通信を強制的に仮想ネットワークへ通すような構成が考えられる。

なお，この研究開発は，経済産業省平成21年度“新世代情報セキュリティ研究開発事業(4)”によって実施したものである。

参考文献

(1) 平井　肇，ほか：分散型仮想ネットワークにおける転送効率化方式の検討と試作機開発，電子情報通信学会技術研究報告，**107**，No.525，265～270（2008）
(2) 斉藤泰孝，ほか：分散型仮想ネットワークの基本コンセプト，電子情報通信学会2007年総合大会講演論文集，No.B-7-55（2007）
(3) Stoica，I.，et al.：Chord： A Scalable Peer-to-peer Lookup Service for Internet Applications，SIGCOMM Computer Communication Review，**31**，149～160（2001）
(4) 経済産業省：平成21年度“新世代情報セキュリティ研究開発事業(クラウドコンピューティングセキュリティ技術研究開発)”公募仕様書（2009）