NEWS RELEASE

NTT
日本電信電話株式会社

２００１年６月1日

IPv6上の高度な商用サービスを実現する ネットワークセキュリティ技術を開発

－インターネット上で、より安全な専用線サービスや有料マルチキャストサービスが可能に－

日本電信電話株式会社(以下ＮＴＴ、東京都千代田区　代表取締役社長：宮津純一郎)では、IPv6ネットワークをめぐる開発動向が、IPv6ネットワーク同士の相互接続技術の開発からIPv6の特徴を活かした新しいネットワーク・サービスの開発へと移行しつつある状況を先取りし、商用サービスを目指すIPv6セキュアネットワーク構築技術「DVPN(Dynamic Virtual Private Network)」とマルチキャストストリーム利用制御技術「InfoPrism」（いずれもコードネーム）を開発しました。

ともに、光ネットワークや広帯域移動通信などの普及によって、人々がインターネットを社会生活のあらゆる場面で活用するようになった場合でも、「いつでも」「どこでも」「誰（どんな電子機器）とでも」「自由自在に」つながる次世代インターネット社会を現実のものとするネットワーク利用技術です。これらにより、本格的なIPv6ネットワーク・サービスを実現できます。

インターネットの爆発的な普及にともなうIPアドレスの枯渇やルータの負荷増大に対処するため、それらの問題を解決する次世代インターネット・プロトコルIPv6の導入・普及に向けた活動が、世界各国の相互接続実験をもとに急ピッチで進められています。

ＮＴＴ情報流通プラットフォーム研究所では、1996年から次世代インターネットの標準プロトコルである、IPv6ネットワークの構築技術および運用管理技術の確立に取り組み、アジア・アメリカ・ヨーロッパの３大陸を結ぶ世界でも最大規模のネットワークを構築し実証実験を行ってきました。この実証実験の成果を踏まえ、IPv6インターネットの利用拡大を実現する、柔軟なセキュアネットワーク構築技術と、マルチキャストストリーム利用技術を開発しました。

DVPNは、IPv6対応端末に備わるセキュアなEnd-to-End通信能力を活かしながら柔軟なネットワーク構築を可能にした技術です。本技術は、認証局が利

用者に一括して認証を与え、End-to-End通信に際して第三者機関が動的にその正当性を確認し、端末がそれに基づいて通信を制御することにより実現します。この技術を用いることにより、必要なときに望む通信相手（あるいは端末）と安全につながることができます。また、現行のインターネットでは困難であった、LANの内外を問わず特定の端末間であたかも専用線のようにセキュアな通信を効率的に行えるため、インターネットの利用方法が飛躍的に拡張します。

InfoPrismは、IPv6のマルチキャスト配信機能を活かしたコンテンツ（動画像など）のストリーム配信サービスにおいて、利用権限を有したユーザのみにコンテンツを利用させる利用制御技術です。配信するコンテンツに対してユーザごとに異なる暗号化を行い、さらに一定時間ごとに暗号鍵を変更するなどの対策を施しているため、マルチキャスト配信では難しかったユーザごとの細かな利用制御を可能にします。インターネット上での加入者限定有料放送サービスなどへの適用が考えられます。

＜DVPNの主な特徴＞　【図１、図２参照】

DVPNは、IPv6対応端末ごとにデジタル証明書を検証する従来のセキュアネットワーク構築技術と異なり、第三者機関が通信時に動的にデジタル証明書を検証する方法を採用しています。これにより、インターネットをあたかも専用線のように利用するVPN(Virtual Private Network)サービスに、次のような特徴を付け加えます。

1)　End-to-EndのCUG (Closed Users Group)構成

機密性を有する内容などについて通信する場合、CUGと呼ばれる特定の端末間でのみ通信を許容する仮想的なネットワークを構成してインターネットを利用する方法があります。現行インターネットで端末がプライベートアドレスを利用している場合、一般的には、LAN単位でしかCUGが構成できませんでしたが、DVPNではLANの内外を問わず必要な端末間でCUGを構成できます。このため、peer-to-peerアプリケーションの利用に適したネットワークを提供できます。しかも、従来のVPNでは固定的にCUGを構成していたのに対し、DVPNではCUG管理システムにより動的にデジタル証明書検証が行われるため、必要に応じて柔軟にCUGを構成できます。

2)　アクセス制御/暗号化処理のボトルネックの解消

DVPNでは、個々の端末で分散してアクセス制御/暗号処理を行うことにより、暗号/認証ゲートウェイを介さない直接通信を可能にしました。このため、高価な高性能暗号処理ゲートウェイも不要になり、ネットワーク全体の大幅なコスト削減を可能にします。また、暗号処理ゲートウェイの過負荷によるトラフィックの渋滞問題も解消します。

3)　CUG管理システムの外部委託によるコスト削減

　これまでは、LANの中にセキュリティ装置を設置する必要があり、組織管理情報を隠蔽したままネットワーク運用業務を外部委託することは困難でした。しかし、DVPNでは、組織情報と切り離してネットワーク運用システムのみを外部委託できます。このため、手間のかかるセキュアネットワーク運用作業を集約し、コスト削減を図れます。

4)　多様なVPNサービスメニューの提供

　個々の端末が行うアクセス制御/暗号処理と連携して、CUG管理システムが通信利用状況を一元的に管理するため、セキュアネットワーク内の通信状況を解析できます。このため、通信時間や通信量に応じたきめ細かなVPNサービスのメニュー提供が可能です。

＜InfoPrismの主な特徴＞　【図３参照】

　InfoPrismは、マルチキャスト配信では利用制御ができないという問題に対して、暗号技術を利用することでユーザごとの利用制御を実現する技術です。

1)　暗号化による利用制御の実現

　インターネット上の放送ともいえるマルチキャストでは、放送と同じく配信そのものを特定のユーザ向けに制御することができません。ユーザごとに利用可否を制御するためには、たとえ配信されたとしてもコンテンツを利用することのできない仕組みをつくる必要があります。InfoPrismでは、コンテンツを共通鍵で暗号化し(暗号化コンテンツ)、その共通鍵を利用権限のあるユーザごとに個別の暗号鍵を用いて暗号化し(暗号化共通鍵)、暗号化コンテンツと共にストリーム配信します。これにより、利用権限のあるユーザは、固有の暗号鍵で暗号化共通鍵を復号し、取り出した共通鍵によって暗号化コンテンツを復号し利用することができます。逆に利用権限のないユーザはコンテンツを復号することができません。

2)　一定時間ごとの暗号鍵変更

　一定時間ごとにコンテンツを暗号化する鍵を変化させる仕組みになっています。このため、経路上での暗号鍵取得などによる不正利用に対するセキュリティ強化が図られているだけでなく、コンテンツの一部のみを利用するといった細かなニーズにも対応します。

3)　先行鍵配送により鍵到達の信頼性を確保

　ユーザごとに異なる鍵情報を配信するため、一斉に配信すると時差が生じて、ユーザ数が多くなった場合、コンテンツ配信に間に合わなくなる恐れが

あります。この問題を解消するために、暗号化コンテンツよりも先行して鍵を配送する仕組みになっています。

＜今後の予定＞

（DVPNの今後）
　CUG管理システムのカバーするVPN規模のスケールアップを図るなど改良を加える一方、具体的な商用サービスへの適用を図っていく予定です。
　現在のところ、ＮＴＴコミュニケーションズが2001年４月からIPv6を用いた商用インターネット接続サービスの提供を行っており、その一環として行われている竹中工務店とのVPN共同実験の中に、DVPN技術も使って実験を行う予定になっています。

（InfoPrismの今後）
　基本原理の確立を踏まえ、商用サービスに適用できるよう、機能拡充や課金システムとの連携などを図る予定です。

　いずれも、６月６日から開催されるNetWorld+Interop 2001 Tokyoにおいて、ＮＴＴコミュニケーションズのブースに参考出展されます。

・図１．DVPNサービスイメージと特徴
・図２．セキュアな遠隔テレビ会議システムへの適用例
・図３．InfoPrismシステム構成

【本件に対する問い合わせ先】
ＮＴＴ情報流通基盤総合研究所
企画部　広報担当　倉嶋、佐野、池田
TEL:0422-59-3663
E-mail:koho@mail.rdc.ntt.co.jp