1B-3

オンデマンドＶＰＮにおける機器とチップの連携に関する一検討

國分　誠　　星川 知之　　鎌仲 裕久

株式会社ＮＴＴデータ

1. はじめに

現在，インターネット上で安全な通信を実現する方法として様々な検討が進められている．オンデマンドＶＰＮ技術では，安全に情報の流通を行うために，ネットワークを利用する人を認証するだけではなくユーザが利用する機器を特定し，人の認証と機器の認証の双方を行う．

本稿では，機器とＩＣチップとの連携を行い，ＩＣチップの耐タンパ性と認証技術を用いて機器の正当性を確保し，安全な情報の流通を実現するモデルを提案し，その有効性を検証する．

2. オンデマンドＶＰＮ技術

インターネットの普及と，安価で容易にブロードバンド環境が利用できるようになるに伴い，従来専用線やISDN などを利用していた分野においても，より大容量でコストの低いインターネットを活用するために，安全な通信路を確保する技術が求められている．一方でＩＰ電話に見られるようなインターネットを利用した任意の機器間を直接接続し，通話するように，任意の機器間で簡易にＰ２Ｐのデータ通信することが求められている．ＩＰ電話ではやりとりできるのは音声データに限られており，声質や通話内容による相手の識別認証が失敗した場合であっても通信からの直接の被害は情報漏洩にとどまる．一方，データ通信においては，認証が失敗した場合，データの漏洩だけでなく改ざんやウィルス混入などによる深刻な被害が発生する．安全な通信路を確保する技術として，ＳＳＬやＩＰ－ＶＰＮ，インターネットＶＰＮなどの技術があげられるが，従来の技術は，サーバとしての登録手続きが必要とされたり，特定のＩＳＰ内での通信に限定されたりするなど，ＶＰＮの使用において制限が発生するとともに，あらかじめ通信する相手の情報や鍵をＶＰＮ機器に設定しておく必要があり，オープンで安全な通信を実現するのは，必ずしも容易なものではなかった．

これに対して，要求に応じて任意の機器間にＶＰＮを構築するオンデマンドＶＰＮ技術の研究開発が進められている（図１）．オンデマンドＶＰＮでは，あらかじめ機器を管理サーバに登録しておくことで，ＶＰＮ接続要求時に，接続可否の判断，機器に必要な構成情報の自動生成，機器への配信設定を行い，ＶＰＮの構築を実現する．構成情報の配信にあたっては，機器が確かに配信先の機器であるかを識別認証する必要があり，接続可否の判断や構成情報の自動生成を行うためには，機器が確かにどのような機器であるかを識別認証する必要がある．

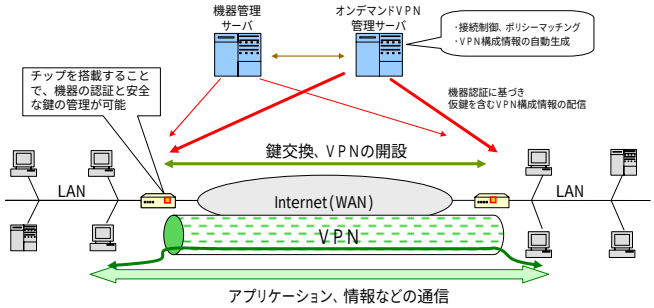

図１．オンデマンドＶＰＮ技術

そこで，本研究では任意の機器間で安全な通信路を確保するために求められる機器の認証技術についての検討結果について述べ，機器の認証に基づく安全なＶＰＮ構築の実現性を示す．

3. 機器認証の手法

任意の機器間で安全な通信路を確保する為には，任意の機器を認証する仕組みが必要である．任意の機器を認証する仕組みとして，ＰＫＩによる機器の証明書を利用する方法が挙げられる．証明書が証明する対象として，確かにその対象であることを証明する「存在証明」と，その対象がどのような特徴を持っているかを証明する「属性証明」の２つに分類される．特に属性証明については，対象の属性に応じて，適用する機能やサービスを変更，制限する場合に利用する際に有効である．

任意の機器間で安全な通信路を確保する場合には，機器の確実な認証と，機器の属性を用いることで，接続の可否を制御することができる．本研究では，特に確実な機器の認証の仕組みについて検討を行った．

確実な機器認証をおこなうためには，機器とサーバ間の認証プロトコルはもちろんのこと，認証される機器自体の改ざんや複製がコストに対して非常に困難であることが保障されていることが重要である．決済端末などは機器全体を耐タンパにする方法がとられているが，オンデマンドＶＰＮ技術を適用する機器は多種多様なため，全ての端末全体を高度な耐タンパ技術を導入し，高レベルのセキュリティを実現すること現実的ではない．そのため，自身を認証する機能を，高い耐タンパ性を持つＩＣカードのチップに集約して実現させ，ＩＣチップを機器とバインドさせる方式に特徴を持たせることにより機器認証の信頼性の向上を実現する事とした．

安全な通信路を確保する上で，特に任意の機器と接続可能とする場合，接続相手が安全な状態や環境である事が重要となる．そのため最初の段階として任意の機器を確実に特定，識別した上で，その機器が保持する様々な属性情報を適切に管理，運用できるようになるのである．安全な状態については，ＯＳのパッチの適用状況やアンチウイルスソフトのパターンファイルの適用バージョン機器の設置場所などを用いることで，機器認証の有効性向上を実現させることとした．

A study of concerning cooperation of equipment and chip in on-demand VPN
Makoto KUNIBU (kunibum@nttdata.co.jp)
Tomoyuki HOSHIKAWA (hoshikawat@nttdata.co.jp)
Hirohisa KAMANAKA (kamanakah@nttdata.co.jp)
NTT DATA CORPORATION

4. 機器認証の方式の提案（研究の成果，結論）

ネットワークシステムにおける人の認証の方法として，人とＩＣカード，ＩＣカードとセンタシステムの認証を組み合わせる事で，センタによる人の識別認証を実現している．この場合，人とＩＣカードは，人の記憶にあるＰＩＮあるいは，生体情報を用いて行う認証により人とＩＣカードがバインドされている．ＩＣチップの認証技術と耐タンパ性を機器でも同様に用いるには，ネットワークの中で識別認証させるための，機器とＩＣチップをバインドしたＩＣチップとセンタシステムの認証を組み合わせる方法が考えられる（図２）．

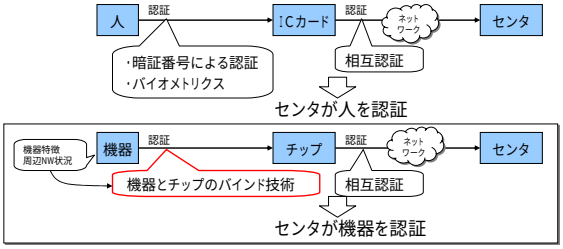

図２．チップを組み合わせた機器の認証

ＩＣチップと機器をバインドさせる方法として，チップと機器の双方に状態管理機能を搭載し，機器の電源起動時および，通常運用中に一定の間隔で双方が互いを監視する仕組みを検討した．具体的には，機器固有の情報を，チップに予め設定するか，チップ内で生成する．機器は，製造時などの第三者による改ざん，複製など行われないことが担保される安全な環境下でチップと同時に設定するか，ＤＨ法などの鍵交換プロトコルを用いて，ＩＤや鍵，証明書など機器固有の情報をチップと共有する．機器は定期的にチップから機器固有情報を読出し，情報の整合性を照合，または認証を行うことでＩＣチップの存在有無，機器固有情報の正当性の確認を行う．不整合が発生した場合には，速やかにセンタにアラームを送付するとともに，機器自身の動作を制限，あるいは電源遮断させるなどの機能を搭載することで，不正が発覚した機器を，機器自身がネットワークから完全に切り離す．機器側で検知した不正なバインド状態をセンタに通知することにより，異常が発生した機器，あるいはＩＣチップの差し替え，抜き取りなどの不正が試みられた機器は，再び正常なＩＣチップを搭載した場合であっても，管理センタで自動的にネットワークから遮断させる免疫機能を搭載する（図３）．これらの機能を搭載することにより，常に正当な機器とチップのバインド状態にある機器のみが安全な通信路の確保を可能とするオンデマンドＶＰＮに参加できる環境を構築した．

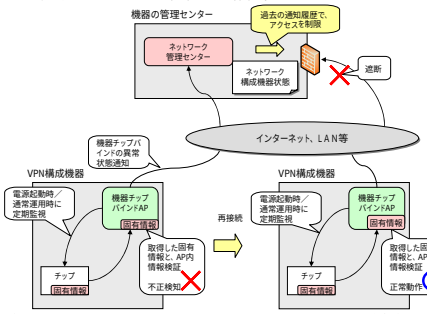

図３．機器とチップのバインドと，不正検知時の動作

機器とチップの状態管理機能は，オンデマンドＶＰＮを構成するセンタ，機器，ＩＣチップ上にそれぞれ搭載されることにより，一定の間隔でお互いを監視できる仕組み（図４）を検討し，より確実な機器とＩＣチップのバインドさせる方式を検討した．

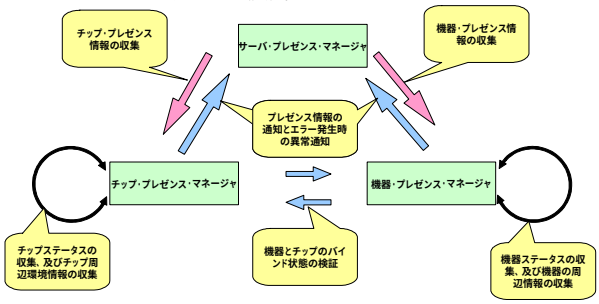

図４．センタ，チップ，機器のプレゼンス管理の概略

5. まとめ

本研究では，機器とチップのバインド技術を用いることで，オンデマンドＶＰＮに参加する機器の識別を可能とし，任意の機器間の安全な通信路の確保における機器認証の確実性，有用性を向上することが可能となった．ただし，本稿に示した技術は一部の実装にとどまり，安全性の検証や，実環境における有効性や，ＩＣチップを利用した認証プロトコルや，チップに配送された鍵の管理方法など，今後さらなる検討を行う必要がある．

機器とチップのバインドにおける，具体的な認証データの交換や認証方法については，照合という簡易な方法を提案したが，さらに機器側の状態管理機能の耐タンパ性の低さを補うために，認証情報の頻繁な更新，安全な共有方法などにおいてもさらに検討を進める必要がある．

謝辞

本研究は，総務省の平成16年度「高度ネットワーク認証基盤技術の研究開発」の委託を受け実施している「オンデマンドVPN技術についての研究開発」に関するものである．関係者各位に感謝する．

参考文献

[1] 早川晃弘，星川知之，高橋成文，鎌仲裕久：”オンデマンドＶＰＮアーキテクチャの提案” 情報処理学会第67回全国大会，2005

[2] 星川知之，國分誠，鎌仲裕久：”機器認証に基づく安全なＶＰＮ構築技術の提案”第 28 回 CSEC 研究発表会，2004

[3] 小尾，他："オープンネットワーク環境で安全な鍵配送を実現するネットワーク基盤"，電子情報通信学会2004年総合大会予稿集，Mar 2004