2004－CSEC－27　(1)
2004／12／20

機器の認証に基づく安全なＶＰＮ構築技術の提案

星川知之[1]　國分誠[1]　鎌仲裕久[1]

現在，インターネット上でネットワークセキュリティを向上する技術について，様々な検討が進められている．安全に情報流通を行うためには，利用する人を認証するだけでなく，機器を認証することが必要となっている．特に高度なセキュリティが求められる場合，IC チップの耐タンパ性や認証技術を用いる方法が有効である．VPN(Virtual Private Network)は，インターネット上で安全に情報を授受する方法として利用されている．本稿では，機器と IC チップとの連携をおこない，さらに環境情報を用いた機器の認証をおこなうことにより，安全なＶＰＮの構築を実現するモデルを提案し，その有効性を検証する．

The proposal of the safe VPN construction technology based on device authentication

Tomoyuki Hoshikawa[1]　Makoto Kunibu[1]　Hirohisa Kamanaka[1]

Today, various examinations are advanced about the technology which improves network security on the Internet. In order to perform safe information circulation, it not only authenticates those who use, but it is necessary to authenticates device. Especially, when advanced security is required, the method using the Tampa-proof nature and authentication technology of IC chip can be considered. VPN (Virtual Private Network) is used as a method of safe information circulation on the Internet. In this paper, by performing cooperation with device and IC chip, and device authentication using environment information further, the model which realizes construction of safe VPN is proposed and the validity is verified.

１．はじめに　（研究の背景，目的）

インターネットの普及により，ブロードバンド環境が安価で容易に利用可能となるに伴い，専用線やＩＳＤＮなどを利用していた分野において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電話が，インターネットを利用して任意の機器間を結び通話するように，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電話では通話のみに限られており，声質や通話内容による相手の識別認証が失敗した場合にも，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であったり，特定のＩＳＰ内での通信に限定されたり，事前に通信する相手の情報や鍵を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，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，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．

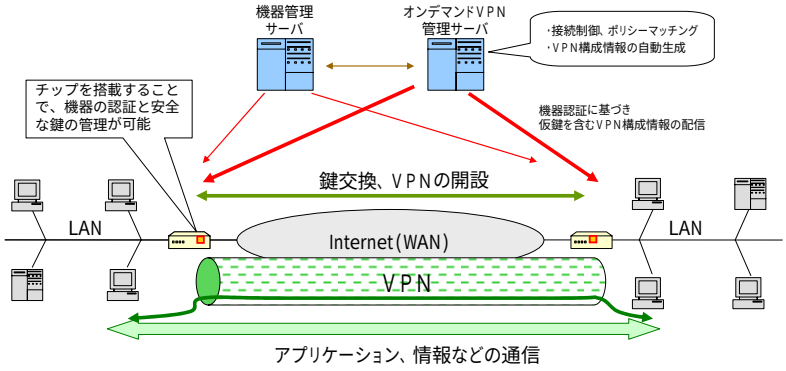

図１．オンデマンドＶＰＮ技術

[1] 株式会社ＮＴＴデータ
NTT DATA CORPORATION

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検討結果についてのべ，機器の認証に基づき安全なＶＰＮを構築できることを示す．

２．機器認証の手法　（研究の手法）

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は，ＰＫＩによる機器の証明書を利用する方法が挙げられる．証明書の対象として，認証の対象が，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したり制限したりする場合に利用する事ができる．

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，機器認証について，確実な機器の認証の仕組みと，機器の属性のあり方とその確認の方法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コピーが非常に困難であることが保障されていることが重要となる．決済端末など機器全体を耐タンパにする方法がとられているが，機器は多種多様なため，高度な耐タンパのレベルを実現することは困難である．そのため，自身を認証する技術を高い耐タンパ性をもつＩＣカードのチップに集約してもたせ，ＩＣチップを機器とバインドさせる方法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．

一方，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，機器の属性は，安全面での機器の状態や環境を示すことができる事が望ましい．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バージョンにより示す頃ができるが，さらに機器の設置環境を確認して属性に反映することにより機器認証の有用性向上を実現する事とした．

３．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や生体情報の認証などによりバインドされている．機器も同様に，ネットワークの中で識別認証させるために，機器とＩＣチップをバインドし，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）．

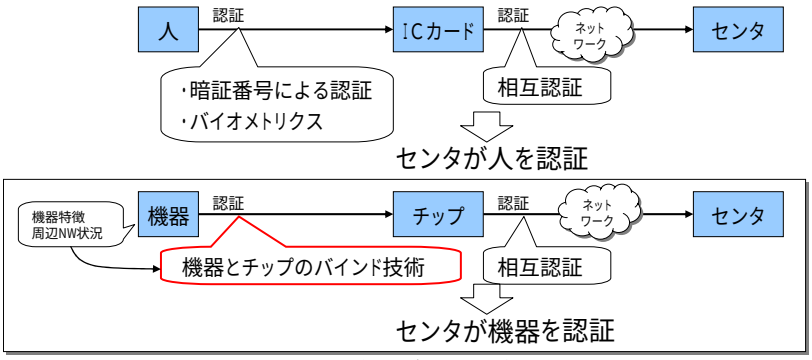

図２．チップを組み合わせた機器の認証

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とした．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の読み出しと照合，または認証をおこない，チップの有無，整合性の確認を行う．不整合が発生した場合には，速やかに機器はセンタにアラームを送付するとともに，速やかに機器自身の通信機能の停止または，電源断にすることで，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．さらに不正を試みた機器は再び正常なチップを搭載した場合も，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）．これにより，常に正当な機器のみが安全な通信路の確保を可能とする環境を実現した．

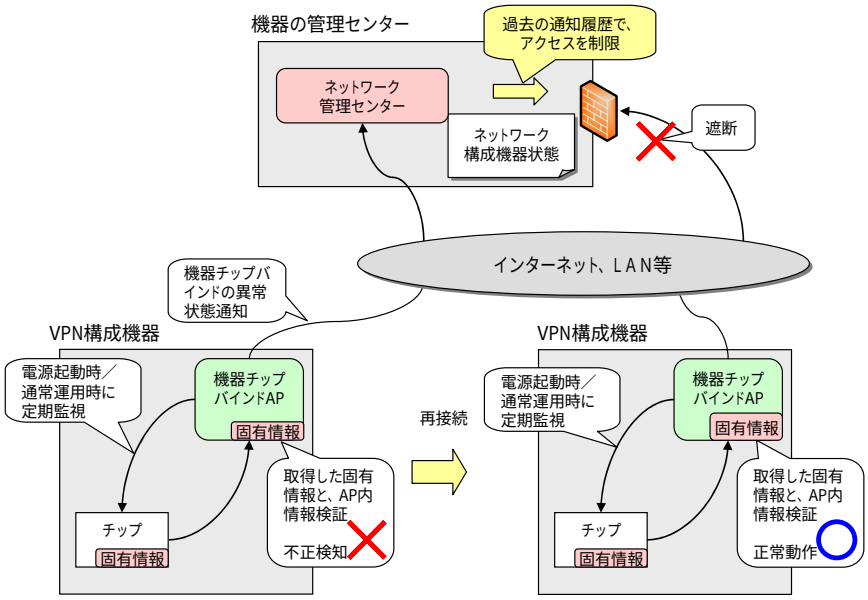

図３．機器とチップのバインドと，不正検知時の動作

機器を利用する上での安全性は，機器自体の安全性に限らず，機器の利用環境条件が影響してくる．いかに安全な機器とネットワークが設定されていても，監視者のいない環境では，悪意をもった利用者によって不正に利用される可能性がある．しかし運用環境自体を技術的に監視することは困難である．一方で，最初の機器設置は，一定の監視や認可のもとで行われる場合が考えられる．そのため，一旦設置された機器が事前の承認なしに不正に移動された場合に，移動を検知する仕組みにより，機器の機能停止などによる不正防止を実現可能とした．機器はネットワークに接続された状態では，様々な環境情報を収集することができる．例えば隣接する機器のＭＡＣアドレスや，サーバに接続するまでのネットワーク経路，ルーティング情報などがあげられる．具体的には，機器は最初の機器設置時にネットワークに関する周辺情報を収集し，保存する．機器は定期的に周辺情報を収集し，事前に収集した情報と比較照合して，自身の位置が変化していないことを検知する仕組みである（図４）．しかし，ネットワークの周辺情報は，隣接した機器の変更や最適な通信のための経路変更など，不定な要素を含む．そのため，位置の移動検知を行うための環境情報としては，複数のネットワーク周辺情報を一定の確率で照合して検証する仕組みとした．

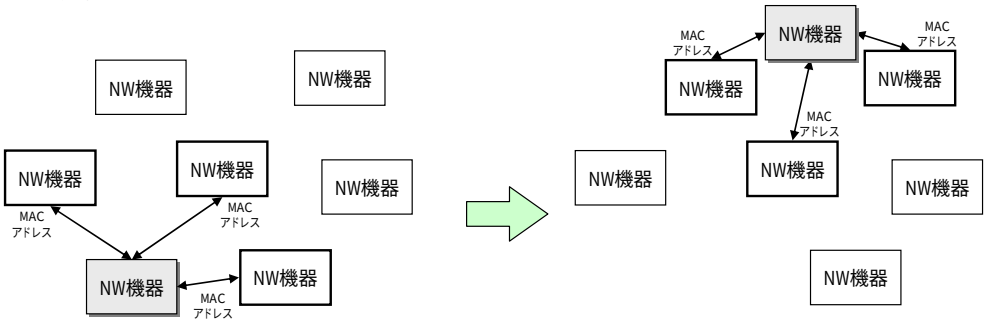

図４．隣接する機器のＭＡＣアドレス情報の収集

４．まとめ（今後の課題）

本研究では，機器とチップのバインド技術と，機器の移動検知技術により，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や，安全な共有方法など，さらに検討を進める検討を進める必要がある．また，バインド技術についても，ＭＡＣアドレスや，ネットワーク経路以外に，より有効な環境情報の選定や照合確立の選定などにより，実際のネットワーク環境や，偽装に対抗する検証，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，「オンデマンド VPN 技術」について研究開発に関するものである．関係者各位に感謝する．