# モバイルのセキュリティを守る“ネットワーク クリプトゲート”

**Network CryptoGate : A New Mobile Security Solution**

琴屋 秀平 KOTOYA Shuhei
井上 淳 INOUE Atsushi
大下 敏明 OSHITA Toshiaki

“ネットワーク クリプトゲート”(NCG)は，IETF(Internet Engineering Task Force)標準である移動IP(Internet Protocol)技術，IPセキュリティ技術に準拠し，IPネットワーク上での移動端末機能とセキュリティ機能を統合してサポートした世界で最初の製品である。移動IP技術により，端末が外部のネットワークに移動してもあたかもホームネットワーク上に存在しているように他の計算機と通信を行うことが可能となり，IPセキュリティ技術による暗号化機能，認証機能によりインターネットなどを経由しても安全な通信を提供できる。これらの機能はIP層でサポートされ，任意のアプリケーションが特別な設定や変更なしに利用できる。

Network CryptoGate (NCG) is the first product in the world to successfully combine both mobility and security. NCG adheres to the mobile-IP and IP-security standards of the Internet Engineering Task Force (IETF). Using mobile-IP technology, NCG provides complete accessibility for a mobile terminal as if it was directly connected to its original network when connected to a foreign network. NCG uses IETF standard IP-security technology to encrypt and authenticate data packets, constructing secure connections through the Internet. Because these features are supported at the IP layer, upper-level applications work without requiring either changes or special setups.

## 1 まえがき

近年，パソコン(PC)をはじめとする端末が小型・軽量化，高性能化してきたことにより，外出先などへ端末を携帯することができるようになり，また携帯電話などの通信インフラの整備やインターネットの爆発的かつ広範囲な普及により，外出先や家庭からネットワークに接続するモバイルコンピューティングが現実のものとなっている。また，従来の専用線や公衆電話回線に代わって，インターネットを利用した企業内ネットワークであるイントラネットが採用され始めている。

インターネットを利用した接続は柔軟性と費用の面から大きな利点があるが，ネットワーク上のセキュリティが保証されないという問題点がある。セキュリティの確保には，暗号化技術によるVPN(Virtual Private Network)が用いられるが，イントラネットでの利用を考えると，接続場所が変化する移動端末を含めたセキュリティの確保が必要になる。

NCGは移動IP技術とIPセキュリティ技術を統合してサポートした最初の製品であり，ネットワーク上で端末が移動した場合でも，他の計算機からはあたかも移動していないかのようにアクセスでき，しかも盗聴や改ざんのない安全な通信が実現できる。

ここでは，モバイルセキュリティの要素技術であるIPセキュリティ技術，移動IP技術を紹介し，NCGの構成，特徴およびシステム構成例について述べる。図1にNCGを用いたシステム構成を示す。

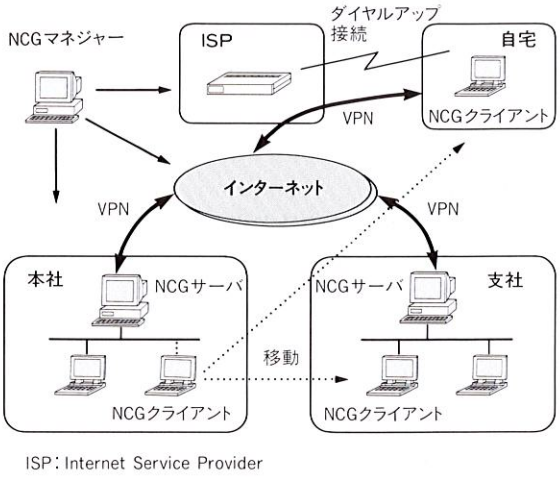


図1．NCGを用いたシステム構成　接続場所にかかわらず同一の環境で端末が使用できる。

System configuration of NCG

## 2 モバイルセキュリティの要素技術

モバイルセキュリティを実現する要素技術について述べる。NCGはIETFのオープンな標準に準拠している。

### 2.1 IP セキュリティ

セキュリティに対する要求を満たすために IP セキュリティプロトコルが RFC (Request For Comment) によって標準化されている[(1)~(5)]。IP セキュリティでは IP パケットの認証および暗号化の方法を定義しており，特定の認証および暗号化アルゴリズムについては規定されていない。IP パケット認証のために認証ヘッダ (AH : Authentication Header) が，IP パケット暗号化のためにカプセル化セキュリティペイロード (ESP : Encapsulating Security Payload) がそれぞれ規定されている。

IP セキュリティでは IP 層で認証や暗号化の処理が行われるため，IP 層以上のプロトコルやアプリケーションにはまったく影響がない。パケット形式を図 2 に示す。

NCG では IP セキュリティに準拠して AH および ESP をサポートしており，認証アルゴリズムとしては Keyed MD5 を，暗号化アルゴリズムとしては DES および Triple-DES を採用している。


図 2．IP セキュリティのパケット形式　暗号化された IP パケットに鍵交換のためのヘッダと AH ヘッダおよび ESP ヘッダが付加される。
IP-security packet format

### 2.2 鍵管理方式

NCG では公開鍵(かぎ)暗号方式を採用している。公開鍵暗号方式では通信エンティティごとに秘密鍵と公開鍵の組みが割り当てられる。通信にあたっては Diffie-Hellman 法により二つの通信エンティティ間の共有マスタ鍵が生成される。送信側ではランダムに生成した値をパケット鍵として各パケットの認証および暗号化を行い，パケット鍵は共有マスタ鍵で暗号化されて，IP パケット内にエンコードされる。パケットの受信側は，パケット鍵を共有マスタ鍵で復号し，必要な認証および復号化を行う。

### 2.3 移動 IP

移動 IP は，移動ノードに割り当てられた固定のホームアドレスを使用して，ネットワーク上の任意の場所に移動した場合でも透過的な通信を実現するプロトコルであり，RFC[(6)~(8)]により標準化されている。

移動 IP での手続きは次のとおりとなる。

(1) 移動情報を受信，管理するホームエージェントが移動ノードの元の接続場所であるホームネットワークに設置される。

(2) 移動ノードがホームネットワークから離れ，移動先に接続した場合，移動ノードは現在位置を示す気付けアドレス (care-of address) を PPP (Point to Point Protocol) もしくは DHCP (Dynamic Host Configuration Protocol)，マニュアル設定などで獲得する。移動ノードは気付けアドレスを含む登録要求をホームエージェントに送信する。

(3) ホームエージェントに登録要求が受理されると，それ以降，移動ノードのアドレス (ホームアドレス) あてに送られるパケットはホームエージェントが代理受信する。代理受信されたパケットは登録された気付けアドレスあての他のパケット内にカプセル化され，移動ノードの現在位置に転送される。

(4) 移動ノードは，転送されたパケットをデカプセル化しホームアドレスあてのオリジナルパケットを取り出す。

(5) 移動ノードがパケットを送信する場合は気付けアドレスではなくホームアドレスをソースアドレスとして使用する。

以上の機構により，移動ノードはホームネットワークを離れて接続された状態でも，ホームアドレスを用いてあたかもホームネットワークに接続されているかのように通信を行うことができる。移動 IP の動作を図 3 に示す。

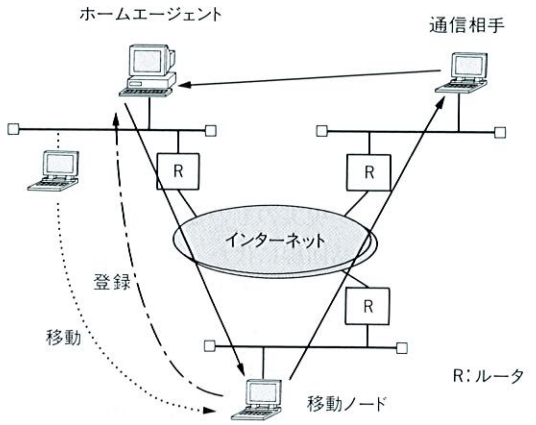


図 3．移動 IP の動作　移動ノードはホームエージェントに移動登録を行う。移動ノードあて通信はホームエージェント経由，移動ノード発は直接通信する三角経路となる。
Mobile-IP scheme

## 3 NCG の構成要素

NCG の構成要素について述べる。

### 3.1 NCG サーバ

NCG サーバは IP セキュリティ機能と移動 IP のホームエージェント機能をサポートし，ネットワークに静的に設置

されるサーバである。各NCGサーバは自身のNCGドメイン（VPNサービスを提供するサブネットの集合）をもち，NCGサーバは暗号化，認証を含むVPNサービスを，NCGドメインからVPNに向けて，またその反対方向に向けて集中的に処理を行う。

また，NCGサーバはそのドメインにホームをもつ移動端末の現在位置の登録を行い，その移動端末のホームアドレスあてに送られてきたIPパケットの現在位置への自動転送を行う。

NCGサーバはSolaris(注1)もしくはWindowsNT®(注2)をサポートした計算機上で動作する。

### 3.2 NCGクライアント

NCGクライアントは，IPセキュリティ機能と移動IPの移動端末機能をサポートしたソフトウェアである。移動IPの移動ノードとして動作するとともにNCGサーバとの間でパケットの暗号化，復号化，認証処理を行う。

NCGクライアントは，WindowsNT®またはWindows®(注3) 95をサポートした計算機上で動作する。

### 3.3 NCGマネジャー

NCGシステムを管理するためのソフトウェアである。NCGシステム全体の構成管理，暗号鍵および公開鍵の生成と配布，NCGサーバおよびクライアントの状態監視を集中して行う。これらの機能はGUI (Graphical User Interface) を用いて容易に操作できる。

NCGマネジャーはSolarisもしくはWindowsNT®をサポートした計算機上で動作する。

## 4 NCGの特徴

NCGの利点および特徴的な機能について述べる。

### 4.1 利点

NCGの利点は次のとおりである。

(1) 既存のVPN製品と異なり，移動端末を含めた動的なVPNが構成できる。また，NCGドメイン内に存在するNCGを用いていない一般の端末間の通信もドメイン外では暗号化される。

(2) VPNを構築する場合，ペイロードだけではなく送信元アドレスやあて先アドレスを含んだIPパケット全体が暗号化できる。

(3) パケット鍵は通信ごとにランダムに生成され，マスタ鍵も時間要素により変化するのでより強力なセキュリティを提供できる。

(4) パケットの認証や暗号化，移動IP処理はIP層で行われ，TCP (Transmission Control Protocol)/IPを用いた既存のアプリケーションはまったく変更することなく使用することができる。

(5) NCGクライアントはネットワーク上のどこに移動しても，同一のアドレスでアクセスすることができ，シームレスな計算機環境が提供できる。また，NCGクライアントがホームネットワークに接続されている場合は，移動IP機能とIPセキュリティ機能は抑止され，不必要なオーバヘッドは発生しない。

### 4.2 システム構築時の特徴技術

実際にNCGを用いてセキュリティシステム構築を行う場合に適用できる技術について述べる。

#### 4.2.1 ファイアウォールとの共存

NCGを既存のファイアウォールと組み合わせて動作させる場合は，既存のファイアウォールの内側にNCGを設置し，ファイアウォールの処理をIPパケットタイプに従って処理するように設定を変更する。これによりNCGで処理すべきIPセキュリティ形式のパケットを選択的に透過させることによって共存することができる。

また，NCGのもつパケット転送抑止機能を用いて，NCGがIPセキュリティ形式のパケットだけを通過するように設定することにより，既存のファイアウォールと並列に設置することが可能となる。図4にそれぞれの構成例を示す。

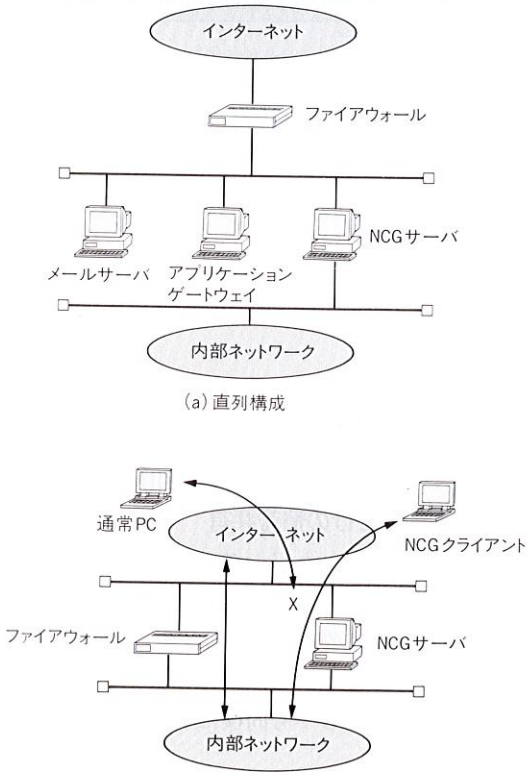


**図4．ファイアウォールとの共存**　既存のファイアウォールと共存するシステム例を示す。
Cooperation with existing firewalls

(注1) Solarisは，米国Sun Microsystems社の商標。
(注2)，(注3) WindowsNT，Windowsは，Microsoft社の商標。

#### 4.2.2 プライベートアドレス対応

大規模なネットワークを運用する組織では，IPアドレスの枯渇に対応するため，プライベートアドレスにより組織内ネットワークを構成することが行われている。プライベートアドレスで運用されるネットワークでNCGを使用する場合は，組織内のホームネットワークに置かれるNCGサーバ（ホームNCG）とは別に組織の内外の境界に置かれる2個のアドレスをもつ境界NCGを設置し，内側と外側で別のIPセキュリティトンネルとして処理を行う。

#### 4.2.3 ローカル個人認証

NCGでは，移動IPの登録メッセージにNCGクライアントを認証するデータを付加し，正しく認証された場合にだけ移動IPの登録を行っている。これにより他の端末が移動端末に“なりすます”ことを防止している。また，移動端末自体が盗難された場合に備えて，パスワードによるローカル個人認証機能がある。NCGクライアント起動時にはパスワード入力が要求され，正規ユーザーであると認証された後，初めて移動IPの登録メッセージが送信される。

図5にローカル個人認証画面を示す。

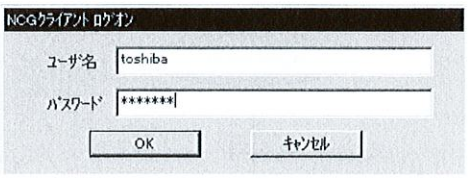


図5．ローカル個人認証　パスワードによるローカル個人認証の画面。
Local user authentication

## 5 応用システム構成

NCGをシステムに導入した場合の応用例について述べる。

### 5.1 特定利用者だけの情報共有

移動端末がホームネットワーク上の特定の利用者に許可されている情報へアクセスを行う場合，端末のアドレスによって利用制限を行うことがしばしばある。NCGを使用した場合，移動時にサーバから認識できるアドレスが変化せず，いつ，どこに移動しても同様にアクセスすることが可能となる。

### 5.2 インターネット電話

NCGを使用すると，移動端末がどこに移動しても同一のアドレスでアクセスできるため，登録を変更することなく電話の転送が可能である。また，プッシュ型の情報伝達が容易に実現できる。

### 5.3 複数の場所にまたがる仮想オフィス

NCGの移動IP機能により，複数のサイトにあるコンピュータを同一のホームネットワークに所属させ，仮想的なネットワークを構築することにより安全に通信することが可能となる。

## 6 あとがき

NCGは，VPNを構築しネットワーク上で安全な通信を提供するとともに，モバイルユーザに対し場所によらず安全でシームレスなネットワークアクセスを提供する先進的なソリューションである。

今後は，次世代のインターネットプロトコルIPv6で標準とされている鍵管理プロトコルであるISAKMP/Oakleyへの対応を行う予定である。

## 文　献

(1) Atkinson, R. rfc1825 Security Architecture for the Internet Protocol. 1995.
(2) Atkinson, R. rfc1826 IP Authentication Header. 1995.
(3) Atkinson, R. rfc1827 IP Encapsulating Security Payload (ESP). 1995.
(4) Metzger, P., et al. rfc1828 IP Authentication using Keyed MD5. 1995.
(5) Karn, P., et al. rfc1829 The ESP DES-CBC Transform. 1995.
(6) Perkins, C. rfc2002 IP Mobility Support. 1996.
(7) Perkins, C. rfc2003 IP Encapsulation within IP. 1996.
(8) Perkins, C. rfc2004 Minimal Encapsulation within IP. 1996.

琴屋　秀平　KOTOYA Shuhei
府中工場 計算機プラットホームインテグレーション部主務。計算機システム構築業務に従事。情報処理学会，IEEE会員。
Fuchu Works

井上　　淳　INOUE Atsushi
研究開発センター 情報・通信システム研究所研究主務。ネットワークソフトウェアの開発に従事。情報処理学会，ACM会員。
Communication & Information Systems Research Lab.

大下　敏明　OSHITA Toshiaki
府中工場 電算機ソフトウェア部主務。
ネットワークセキュリティ製品の開発に従事。情報処理学会会員。
Fuchu Works