ニーズに合わせて2つの製品を組み合わせた「NetNucleus IPSec」による組込み機器ソリューション

世の中のネットワーク化が進むなかで、パソコンのみならずプリンタや白物家電までさまざまな機器がインターネットに繋がる時代を迎え、暗号技術を用いてIPパケットの機密性を実現するIPsecに大きな関心が寄せられています。当社は、市場で定評のあるSafeNet社のIPsec(QuickSec) およびRSAセキュリティ社の暗号ライブラリ(BSAFE)の2つを組み合わせた「NetNucleus IPSec」を提供しています。今後は、携帯電話などのモバイル機器分野にも注力するとともに、よりお客様のニーズに合わせた製品とサービスを提供していきます。

安全なネットワークに不可欠なIPsec

携帯電話やPDA、プリンタから家電製品など、今やあらゆる機器がネットワークに繋がるようになってきました。また、組込み機器にも大量のデータが保存できるようになり、インターネットを通じて重要な情報をやり取りするケースも増えてきています。

こうした中、IPパケットを暗号化してネットワーク上のデータを保護するプロトコルであるIPsecへの注目が高まっています。IPsecはOSに組み込むミドルウェアとして提供されるため、既存のアプリケーションに手を加える必要はなく、現状の資産を有効に活用することが可能です。そのため、アプリケーションは暗号通信を意識することなく、これまでと同じ手順で通信を行いながら、安全にデータのやり取りができます(図-1)。

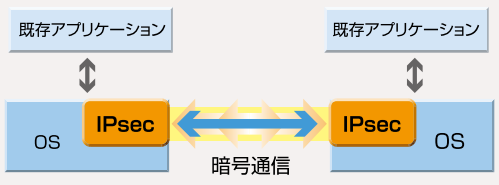

図-1　IPsecの概要

IPsecを使用すると、通信相手の機器の認証／安全な鍵交換／IPパケットの暗号化によって通信内容の保護が実現できます。これにより、なりすましや盗聴、改ざんといった不正行為を防止でき、大切なデータを安全に通信することが可能となります。

例えば、パソコンの世界では Windows Vista に採用されている「プラグ・アンド・プレイ(PnP)」機能を有効に活用するため、IPv6 が標準でサポートされており、あらかじめIPアドレスを設定していない状態でも、電源を入れると自動的にアドレスが設定できる仕組みが盛り込まれています。PnPは、家電製品などのパソコン以外の機器との通信を実現可能とするキーとなる技術であり、IPv6 普及の重要な役割を果たすと考えられます。従来は、中央で監視するというサービスが主流でしたが、現在のインターネットはPeer to Peer(PtoP)型アプリケーションにより、双方向性が重視されている状況です。

IPv4 は PtoP モデルではなく、クライアント／サーバモデルに近い概念で設計されていたため、自分を守るため外から来るものは拒むという対策がとられてきました。しかし、IPv6 時代に突入し、PtoP が定常的に使われる世の中になると、自分のコミュニケーション対象を選び、互いに安全に通信できることが必須となります。特に企業のプライベート網の場合、私たちが日常業務で使用するデジタル複合機(MFP)など、双方向性が重視され、サーバの経由なしでクライアント相互通信が必要となります。アメリカ政府が調達するプリンタを見ても、2008年度調達分からIPsec の実装が義務付けられました。こうした状況から考えると、IPsecの利用でフラットな IP の中で VPN を構築できるというメリットが重要になってきます。

最新の規格と実績を持つ2製品を統合

こうした動きに対応して、当社では「NetNucleus IPSec」(当社の登録商標)によるソリューションを提供しています。

NetNucleus IPSecは、SafeNet社のIPsec(QuickSec)と、RSAセキュリティ社の暗号ライブラリを組み合わせた製品です(図-2)。SafeNet社の製品は、IPA(独立行政法人 情報処理推進機構)や、JNSA(日本ネットワークセキュリティ協会)などが行っているIPsec相互接続性検査では、高い接続性を示している製品です。また、IKEv2(Internet Key Exchange version2)に対応することによりナット・トラバーサル(注1)もサポートするなど、新しい規格へもいち早く対応しています。

また当社は、RSAセキュリティ社と2004年春からアライアンスを締結し、当社の無線LANセキュリティ製品である

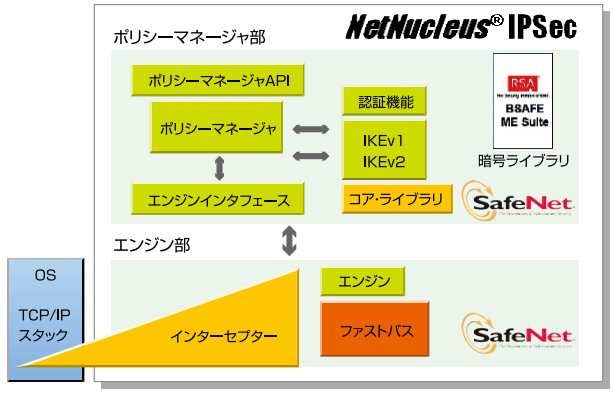

図-2　NetNucleus IPSecの構成

NetNucleus WPAにもBSAFEを使用しています。RSAセキュリティ社は、認証と暗号化の技術で世界最先端企業であり、同社の暗号ライブラリを使用することで知的財産権を侵害することなく高い信頼性を実現しています。

NetNucleus IPSecは、このようにSafeNet社のIPsecの暗号機能をRSAセキュリティ社のBSAFEに置き換えることで、IPsecの最新規格へいち早く対応し、より信頼性の高い暗号機能を持つIPsec環境を構築することが可能となりました。さらにIPsecエンジン部分の一部をハードウェアアクセラレータに置き換えることが可能で、ソフトウェアのみでの処理に比べて高速化が実現でき、CPU負荷の低減も図れるため、高いパフォーマンスが要求される組込み機器にも対応することが可能です。

当社では、NetNucleus IPSecをより多くのお客様に安心してお使いいただくため、次のようなサービスを提供しています。

(1) コンサルテーション

今まで培ったノウハウに基づく、セキュリティ導入のコンサルテーションを実施しています。

(2) ターゲットプラットフォームへの移植

NetNucleus IPSecはLinuxをベースに開発していますが、組込み機器で使用実績の高いVxWorksやモバイル機器向けのWindowsCE、WindowsMobileにも対応しています。またお客様環境での動作確認も行っています。

(3) カスタマイズ

使用しない機能を削除したり、お客様が準備したハードウェアアクセラレータ対応を行います。

(4) テクニカルサポート

設定方法や使用方法・疑問など、RSAセキュリティ社／SafeNet社と協力して、お客様からの質問に迅速に回答します。

モバイル機器のIPsecマーケットに注力

当社では、携帯電話のIPsec通信にも注目しています。飛躍的な普及を遂げた携帯電話は高機能化が進み、メールで文書や画像のやりとりやスケジュール管理ができるようになっています。第三世代と言われている携帯電話には暗号化の技術が盛り込まれており、電波を傍受しただけでは内容を把握することができません。しかし、有線／無線を問わないシームレスな環境では認証やセキュリティレベルの統一が考慮されている必要があり、すべての経路でIPsecを使用して通信することによって、より安全な通信が可能となります(図-3)。また、これらは携帯電話に限らず、PDAやハンディターミナルなど、インターネットに接続する機器すべてにあてはまります。

当社は、自社開発製品を提供するのはもちろん、お客様のニーズに合わせてこうした優れた製品を組み合わせたソリューションを提案することにもノウハウを持っています。最新規格に対応し実績のあるNetNucleus IPSecは、まさにそうした製品の1つであり、お客様に安心して利用いただけるソリューションとなっています。

NetNucleus IPSecはすでにOA機器分野、特にMFPへの採用が決定しています。また、携帯電話をはじめとするモバイル機器向けの製品も開発が完了しており、今後はモバイル機器分野への展開に注力していきます。

(エンベデッドプラットフォーム・
ソリューション事業部　早川正文)

(注1)ナット・トラバーサル(NAT traversal)：NAT越えの問題をクリアする方法の1つ。IPsecデータグラムをUDPでカプセル化してNATを通過して送受信できるようにする機能。

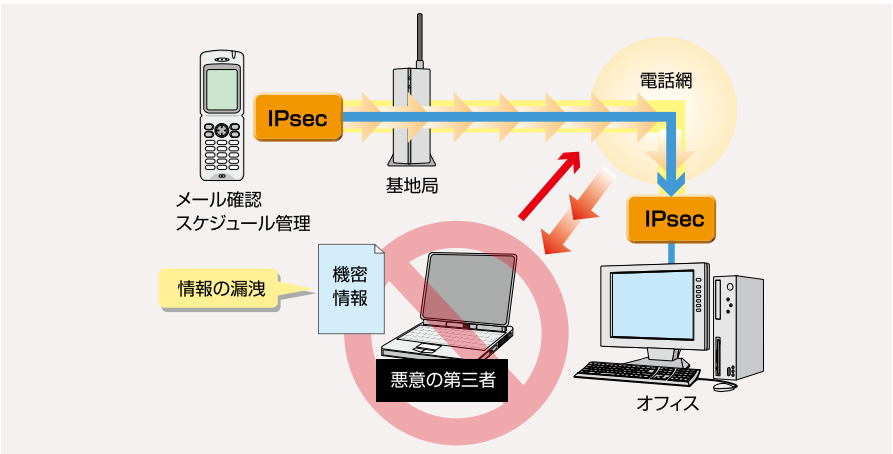

図-3　NetNucleus IPSecのモバイル分野への適応