【16】

| | |
|---|---|
| 氏名 | 鍛冶 忠司 |
| 博士の専攻分野の名称 | 博士（情報科学） |
| 学位記番号 | 第 24659 号 |
| 学位授与年月日 | 平成23年3月25日 |
| 学位授与の要件 | 学位規則第4条第1項該当<br>情報科学研究科情報ネットワーク学専攻 |
| 学位論文名 | A Study on Security Techniques for Enterprise Network over Next Generation Network（NGN）<br>（次世代ネットワーク（NGN）上での企業ネットワークのためのセキュリティ技術の研究） |
| 論文審査委員 | （主査）<br>教授 東野 輝夫<br>（副査）<br>教授 村田 正幸　教授 村上 孝三　教授 今瀬 真<br>教授 中野 博隆 |

## 論文内容の要旨

近年、大企業では、本社、支社、SOHOのLANを1つまたは複数の広域ネットワークで接続した企業ネットワークを構築するようになってきている。次世代ネットワーク（NGN）は、IP-VPNよりも安価かつインターネットよりもセキュアな、費用対効果の高いVPNサービスとして注目を集めている。NGNは、通信の品質保証とセキュリティを実現するため、SIPを用いて制御・管理するが、現時点では、NGNのセキュリティ機能はNGN内の通信に限定されている。
本論文では、NGN上で企業ネットワークを構築する際の、企業とNGNを跨る通信のセキュリティ上の課題を解決するための次の3つのセキュリティ技術について研究を行った結果について述べる。
1つ目の技術であるセキュア通信セッション提供サービス（sSCP）は、NGN・インターネット・LANを跨る通信をNGNの呼制御機能と連動して保護する。sSCPは、TLSやIPsecによって通信データを保護するユーザプレーンと、SIPによってユーザプレーンをNGNの呼制御機能と連動して制御する制御プレーンから構成される。sSCPは信頼できる第三者としてすべてのエンティティの認証を代行することで、通信確立時に通信デバイス同士による認証処理を省略する。この結果、セキュア通信セッションを高速に確立できる。
2つ目の技術は、複数のPKIが相互に証明しあう環境でSIPメッセージをTLSによって保護するための技術であり、相互証明環境に向けたTLSハンドシェイクプロトコルのプロファイルおよび認証パス発見・検証サーバを用いた実装方式を提案する。本技術を用いることで多数の認証局を容易に管理できる。
近年、アプリケーションの管理を容易にするため、モバイルコード技術が利用されている。しかし、企業管理者がSOHOを管理することは困難であり、SOHOで動作した悪意のあるサービスが企業ネットワーク全体に害を与えるという問題が懸念される。3つ目の技術は、モバイルコードの電子署名を、モバイルコードを実行する端末だけではなく、端末からアクセス要求を受け取ったサーバでも検証することにより、悪意のあるモバイルコードが動作した場合でも企業ネットワークを保護できる。

提案した3つの技術がNGNの呼制御機能およびセキュリティ機能と連携することにより、セキュアな企業ネットワークを構築できる。

## 論文審査の結果の要旨

近年、大企業では、本社、支社、SOHOのLANを1つまたは複数の広域ネットワークで接続した企業ネットワークを構築するようになってきており、次世代ネットワーク（Next Generation Network, NGN）は、IP-VPNよりも安価であり、かつ、インターネットよりもセキュアな、費用対効果の高いVPNサービスとして注目を集めている。

次世代ネットワーク（NGN）におけるセキュリティ機能は現時点ではNGN内の通信に限定されており、NGN上で企業ネットワークを構築する際の企業とNGNを跨る通信のセキュリティ上の課題を解決するため、本研究では次の三つのセキュリティ技術についての研究を行っている。

一つ目の技術であるセキュア通信セッション提供サービス（sSCP）は、NGN・インターネット・LANを跨る通信をNGNの呼制御機能と連動して保護する技術である。通信セッション提供サービス（sSCP）は、TLSやIPsecによって通信データを保護するユーザプレーンと、SIPによってユーザプレーンをNGNの呼制御機能と連動して制御する制御プレーンから構成される。このうちsSCPは信頼できる第三者としてすべてのエンティティの認証を代行することで、通信確立時に通信デバイス同士による認証処理を省略する。この結果、セキュア通信セッションを高速に確立することができる。

二つ目の技術は、複数のPKIが相互に証明しあう環境で、SIPメッセージをTLSによって保護するための技術であり、相互証明環境に向けたTLSハンドシェイクプロトコルのプロファイル、および、認証パス発見・検証サーバを用いた実装方式を提案している。本技術を用いることで多数の認証局を容易に管理することができる。

近年、アプリケーションの管理を容易にするため、モバイルコード技術が利用されている。しかし、一般に企業管理者がSOHOを管理することは困難であり、SOHOで動作した悪意のあるサービスが企業ネットワーク全体に害を与えるという問題が懸念されている。三つ目の技術は、モバイルコードの電子署名を、モバイルコードを実行する端末だけではなく、端末からアクセス要求を受け取ったサーバでも検証することにより、悪意のあるモバイルコードが動作した場合でも企業ネットワークを保護できる方法を実現している。

提案した三つの技術をNGNの呼制御機能およびセキュリティ機能と連携させることにより、セキュアな企業ネットワークを構築できる。

以上のような理由から、本論文は次世代ネットワーク（Next Generation Network, NGN）環境において、複数の広域ネットワークで接続した企業ネットワークをセキュアなものにし、通信のセキュリティ上の課題を解決するためのセキュリティ技術として有用な手法を提案している。よって、博士（情報科学）の学位論文として価値あるものと認める。