

いつでも、どこでも簡単・安心に利用できる モバイルネットワークサービスソリューション

MIND Remote Access Services Solution: Easy and Safe Access Anytime, Anywhere

工藤 和仁*
(Kazuhito Kudo)
手束 裕司*
(Yuji Tetsuka)
梶場 純一*
(Junichi Haseba)
平川 佳史*
(Yoshifumi Hirakawa)

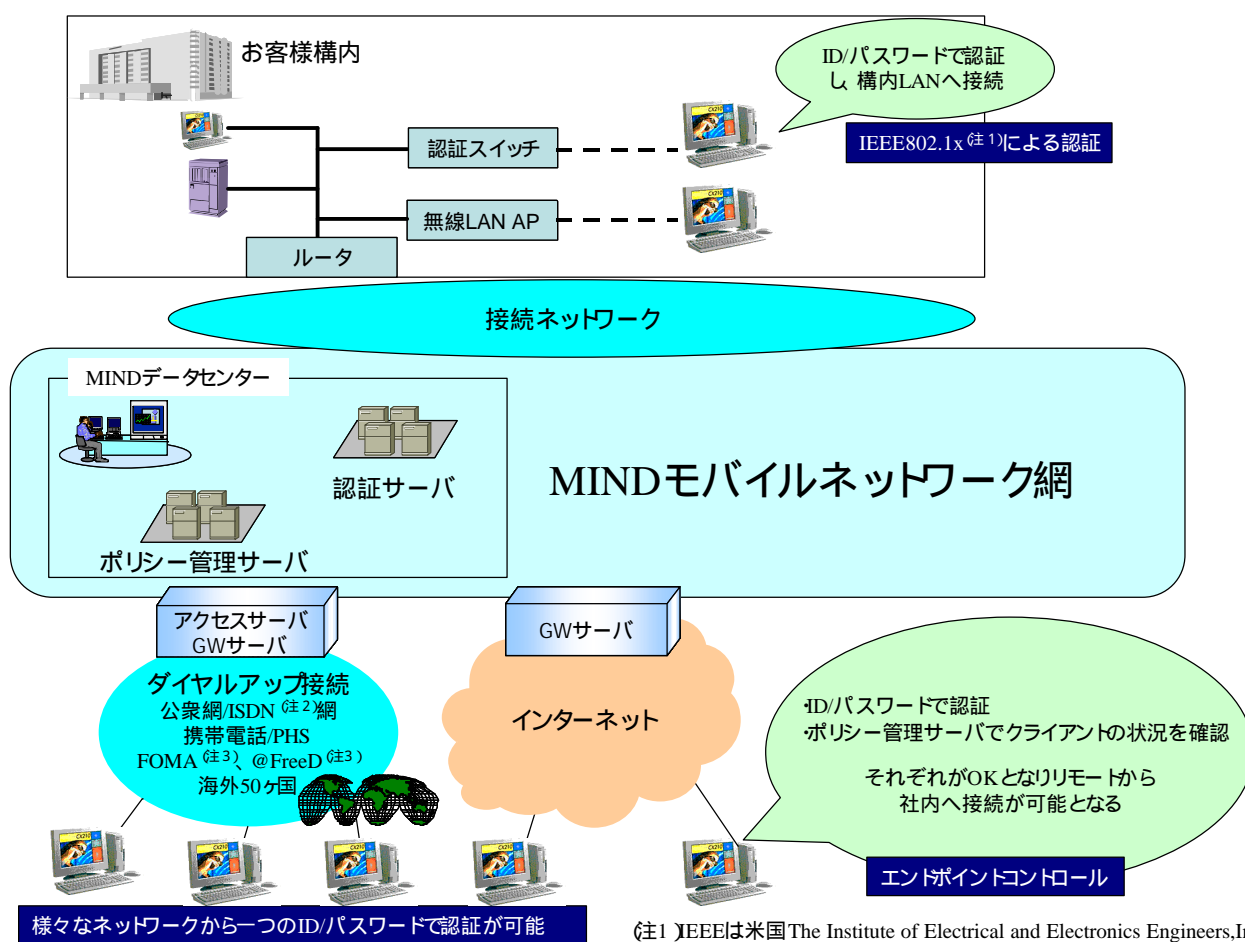
要 旨

ユビキタス社会においては、出先や自宅などの社外から勤務先の社内ネットワークへ、安全でかつ手軽にアクセスできるネットワークの形態が多様化している。

三菱電機情報ネットワーク(株)(MIND)では、1997年から社内ネットワークへのセキュアなアクセス手段として、“MINDモバイルネットワークサービス”(MINDモバイル)を提供している。本サービスは、リモートアクセスに関する様々なサービスを提供しているが、主な特長として、一つのID/パスワードだけで様々なネットワーク

形態からのアクセスが可能であり、かつ接続時の認証も利用者側のセキュリティレベルに合わせて柔軟に選択可能な点などが挙げられる。

本稿では、MINDモバイルの機能概要紹介と、2005年度から新たにサービスを開始した“リモートアクセス端末セキュリティチェックサービス”(エンドポイントコントロール)と、今後サービス開始を予定している“無線LAN認証サービス”や“認証V-LAN (Virtual-LAN)サービス”などについて、技術側面から紹介する。



LAN :Local Area Network ,AP:Access Point ,GW :Gate Way
ISDN :Integrated Services Digital Network ,PHS :Personal Handy phone System

注1 IEEEは米国The Institute of Electrical and Electronics Engineers,Inc.の商標である。
注2 ISDNは東日本電信電話(株)の登録商標である。
注3 FOMA、@FreeDは(株)NTTドコモの商標又は登録商標である。

MINDモバイルネットワークサービスの特長

MINDモバイルネットワークサービスは、従来のリモートアクセスサービスの範囲だけではなく、構内LANへの接続認証、さらには接続端末のセキュリティチェックなど、ユビキタス社会実現に向けた新たなサービスを拡大している。

1. ま え が き

MINDモバイルは、従来のダイヤルアップ網、インターネット網などからのリモートアクセスサービスの基盤に加え、新たなネットワーク接続認証サービスとして、認証スイッチや無線LANアクセスポイントへの接続サービスを計画している。本稿では現状のMINDモバイルネットワークサービスの機能と現在計画中的の新サービスについて、技術側面から紹介する。

2. モバイルネットワークサービスの構成要素

MINDモバイルでは、出張先・外出先などから、社内イントラネットへセキュアにアクセスするためのリモートアクセス環境を提供しており、サービスの特長を以下に示す。

- (1) 通信コストを削減する様々なアクセスメニュー
- (2) 最新技術を採用したセキュリティ対策
- (3) 運用アウトソーシングによる利用者負荷の軽減
- (4) 初期導入コストの軽減

2.1 接続ネットワーク

利用者の環境・形態に合わせた様々なネットワークからリモートアクセスが可能となる様に、以下のような豊富なアクセスメニューを提供している。

(1)ダイヤルアップアクセスサービス

- ・アナログ電話・ISDN・携帯電話・PHSから利用可能。
- ・全国一律の着信課金通信料金で利用が可能。
- ・全国から同一のダイヤル番号で利用が可能。

(2)海外アクセスサービス

- ・主要50ヶ国、約3,000ヶ所のアクセスポイントから利用が可能。
- ・米・英・独・豪・中国からは着信課金での利用も可能。

(3)128Kパケットアクセスサービス

- ・下り128Kbpsベストエフォート方式のパケットサービスが定額制通信料金で利用可能。

(4)閉域専用網を利用したアクセスサービス

- ・(株)NTTドコモの@FreeDによる、定額制通信料金のPHS下り64Kbps通信が利用可能。
- ・(株)NTTドコモのFOMAによる、下り最大384Kbpsのベストエフォート方式パケット通信が利用可能。

(5)インターネットからのアクセスサービス

- ・IPsec (IP Security protocol)型とSSL (Secure Socket Layer) - VPN (Virtual Private Network)型の2方式の暗号通信方式が可能。
- ・インターネット内で通信経路をVPNトンネル化させるセキュアな通信が可能。

2.2 認証システム

利用者のセキュリティニーズに応えるため、最新技術を組み合わせた豊富な認証サービス及び認証デバイスを提供している。

(1) 発信者番号認証サービス

- ・利用者のISDNやPHSの電話番号を事前登録し、登録された電話番号からのみ接続を許可。

(2) ワンタイムパスワード認証サービス

- ・SecurID^(注4)を利用し、ワンタイムパスワード方式で認証。

(3) 指紋認証サービス

- ・指紋認証装置PUPPY^(注5)を利用し、公開鍵暗号方式でパスワードを暗号化して認証。

(4) USBトークン認証サービス

- ・USB (Universal Serial Bus)トークンikey2000^(注6)を利用し、公開鍵暗号方式でパスワードを暗号化して認証。

2.3 運用系システム

MINDモバイルを利用するにあたり、利用者（特に運用担当者向け）に対する運用負荷の軽減を目的に、下記の運用支援サービスを提供している。

(1) 運用支援ツール

- ・Webから、ID登録・パスワード変更・接続ログファイルのダウンロード・利用状況照会などの運用管理ツールを提供。

(2) モバイル専用ダイヤラー

- ・国内・海外のアクセスポイント情報が事前に組み込まれたダイヤルアップツールを提供。

(3) 部門別請求サービス

- ・IDを利用者の部門別に管理・集計し、部門毎に振り分けた請求処理サービスを提供。

(4) ヘルプデスクサービス

- ・お客様側のシステム管理者に代わり、エンドユーザからの直接問合せを24時間365日受け付けるサービスを提供。

(注4)SecurIDは、RSA Security Inc.の登録商標である。

(注5)PUPPYは、ソニー(株)の商標または登録商標である。

(注6)ikey2000は、SafeNet Inc.の登録商標である。

MINDモバイルでは、システム構築に必要な機器の設計・設置、IDの登録・運用までを、MINDがトータルにサービス提供している。そのため、利用者側は通信機器などを一切準備する必要がない。また、MINDの統合運用管制センターICC (Integrated Control Center)が、24時間365日、サービスの稼働監視及びトラブルフォローを実施し、かつ各種管理サーバを遠隔地で二重化するなど、安全・安心への万全な対応を実施している。

3. ネットワーク接続認証サービス

外部ネットワークからの接続認証機能に加え、利用者の社内ネットワークに、特定のクライアント端末だけを接続許可するための各種認証機能が求められている。

そのため、MINDモバイルでは先に述べたような様々なリモートネットワークからの接続認証機能に加え、利用者の社内ネットワーク接続における接続認証付加サービスを提供している。以下に、本付加サービスに関連した主な認証技術を紹介する。

3.1 IEEE 802.1x

IEEE 802.1x (以下802.1x) は、IEEE (米国電気電子技術者協会) の802委員会が制定したLANの標準規格の一つであり、LANスイッチや無線LANのアクセスポイントで利用者端末を認証する技術である。

認証を受け付ける端末には“サブリカント”と呼ぶ認証クライアントソフトが必要であるが、Microsoft^(注7) Windows^(注7) 2000 (SP4以降) やWindows XP, Mac OS^(注8) Xなどでは標準装備されている。LANスイッチや無線LANアクセスポイントなどの802.1x対応機器は、サブリカントから受け取った認証情報を認証サーバであるRADIUS (Remote Authentication Dial In User Service) サーバに転送し、LANの利用を許可するかどうかを判断する。さらに認証局CA (Certificate Authority) が発行するデジタル証明書を利用することによりセキュリティレベルの向上を図ることが可能となる。

3.2 無線LAN認証

無線LAN は1998年のIEEE 802.11b (以下802.11b) の規格化に伴い、1999年頃より製品がリリースされ、現在では機器の低価格化も進み、数多く導入されている。

一方で、無線LANは有線LANと異なり、電波が通ればアクセスが可能となるため、不正アクセスや情報漏洩の危険性などを併せ持っており、そのセキュリティ対策が重要

となる。

従来の無線LANアクセスポイント機器では、SSID (Service Set Identifier) やMAC (Media Access Control) アドレスによる接続認証及び802.11bの標準暗号化方式であるWEP (Wired Equivalent Privacy) を組み合わせて使用されている。しかしながら、最近になってWEPの脆弱性が指摘され、セキュリティレベルの向上を目的とした802.1x、WPA (Wi-Fi Protected Access)、IEEE 802.11iなどの新しい認証技術及び暗号化技術が目されている。無線LANのセキュリティレベルについて、各方式の違いをまとめたものを表1に示す。

表1. 無線LANの認証/暗号化方式の比較

無線LAN認証/暗号方式	セキュリティレベル
WEPのみ	総当たり攻撃による鍵の解読や、ビット反転攻撃によるデータ改竄などの危険性あり
WEP+802.1x	802.1x認証の鍵配布機能で、WEPキーの定期更新が行われるため、総当たり攻撃による鍵の解読危険性は大きく減少している
WPA(TKIP+802.1x)	TKIP(Temporal Key Integrity Protocol)の暗号化方式を使用することにより、鍵長の拡張、暗号鍵の定期更新、MIC(Message Integrity Code)による改ざんの防止、802.1xによる認証技術でWEPの弱点を補う
802.11i	AES(Advanced Encryption Standard)の採用によりWEPが抱えていた暗号化部分の問題を解消

運用上、設置場所が分散しているアクセスポイントの設定を個々に管理するのは非常に煩雑で困難なため、今後は、企業向け無線LANの構築用にアクセスポイントの一括管理及び無線エリア管理を自動化する無線LANスイッチが必須になっていくものと思われる。

3.3 認証VLAN

認証VLANは、802.1xを始め、様々な方式に基づいて端末の認証を行い、その結果によってユーザをそれぞれ適切なVLANに振り分けるセキュリティ技術である。

接続ユーザは、認証制御により予め定義したVLANへ振り分けられるが、ポリシーを満たさない場合は検疫VLANに隔離される。

802.1xの実装状況は、下記のように各メーカー間でかなり違いがあるが、1年以内には大半のスイッチメーカーが802.1xを実装していくものと予想される。

- (1) 802.1xが未実装のもの
- (2) 802.1xは実装されているが、関連機能の実装が遅れているもの
- (3) 802.1xが実装され、運用機能及び付加機能も実装されており、今すぐサービスが利用できるもの

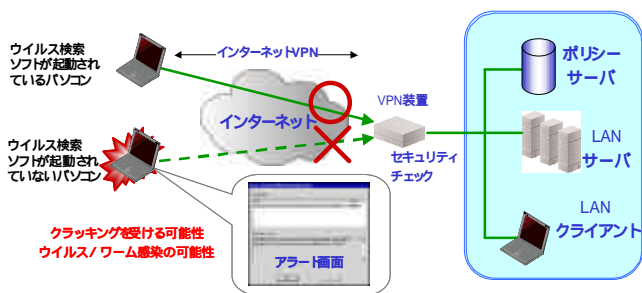
(注7)Microsoft、Windows、Internet Explorer、Outlookは、米国Microsoft Corporationの米国及びその他の国における登録商標である。3
(注8)Mac OSは、米国Apple Computer, Inc.の米国及びその他の国における登録商標である。

4. エンドポイントコントロール (EPC)

EPCとは、社内ネットワークに接続可能なパソコンのWindows関連セキュリティ修正プログラムの適用状況、ウイルスチェックパターンファイルの更新状況などをチェックし、企業のセキュリティポリシーに合致しない端末の接続を拒否する機能である。

一般的には、下記のような内容をチェックする必要がある。

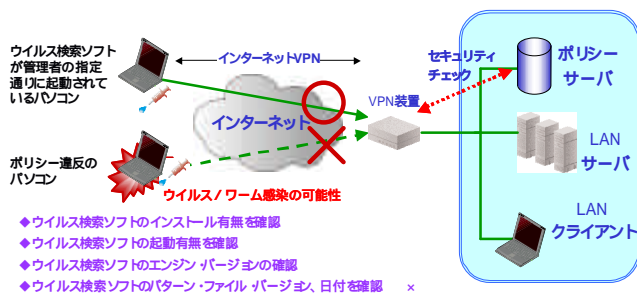
(1) ウイルス検索ソフトが起動されているか (図1)



VPN接続時に、ウイルス検索ソフトが起動されていない場合、接続を遮断する

図1. エンドポイントコントロールの機能

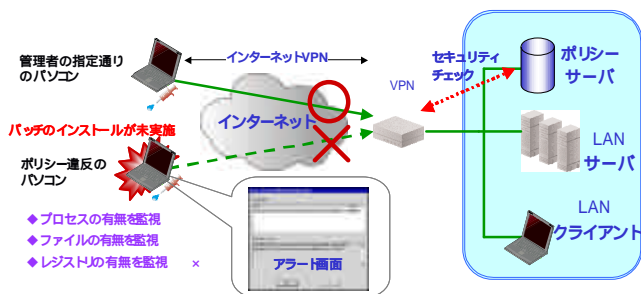
(2) ウイルス検索ソフトは起動されているがパターン・ファイルは最新に更新されているか (図2)



VPN接続時に、ウイルス検索ソフトウェアが管理者の指定通り起動されていない場合、通信を遮断する

図2. エンドポイントコントロールの機能

(3) Windows関連のセキュリティ修正プログラムの適用状況が社内ポリシーに準拠しているか (図3)



VPN接続時に、レジストリ、プロセス、ファイルなどが管理者の指定通りでない場合、通信を遮断する

図3. エンドポイントコントロールの機能

以上の機能により、Windowsの脆弱性など、インターネットに繋がっているだけで感染する脅威などから社内ネットワークを守ることが可能となる。また、アプリケーション制御機能により、指定のアプリケーションのみを接続許可させることも可能である。例えば、社内指定ブラウザとしてInternet Explorer^(注7)、メールソフトとしてOutlook^(注7)が社内標準であれば、このアプリケーションのみで通信するように制御する。この機能により、インターネットメッセージや許可されていないアプリケーションなどの利用を抑制させることが可能となる。

さらに、“検疫”機能として、ポリシー違反している端末を強制的に検疫セグメントに隔離し、セキュリティ対処を施すなどの機能も付加機能として備えている。

5. むすび

ユビキタス社会では、“いつでも、どこからでも”社内システムへのネットワークアクセスが可能となることで、利用者の利便性はますます向上するが、その反面、セキュリティに対する様々な脅威も高まってくる。

本稿ではMINDモバイルの新サービスとして提供を開始したエンドポイントコントロールを始めとする端末のセキュリティチェックサービスや、今後サービス化を予定している802.1x認証/無線LAN認証について紹介した。

MINDモバイルは、今後もセキュリティチェックや、リモートアクセス認証に関する新たなサービスを順次追加していく予定であり、ユビキタス社会における社内ネットワークアクセス環境を、更に簡単で安心なものにしていく所存である。

参考文献

- (1) NPO 日本ネットワークセキュリティ協会 802.1x 相互接続実験報告書,1(2003)
- (2) IEEE802.1xって何ですか?, IT Pro (日経BP)
<http://itpro.nikkeibp.co.jp/free/NNW/NETHOT/20041126/153119/>