特集論文

全社共通無線LANの構築と展開

軽部正人*　藤井崇裕**
鎌田真吾*
内田有紀*

Implementation and Deployment of Company－wide Standardized Wireless LAN

Masato Karube, Shingo Kamata, Yuki Uchida, Takahiro Fujii

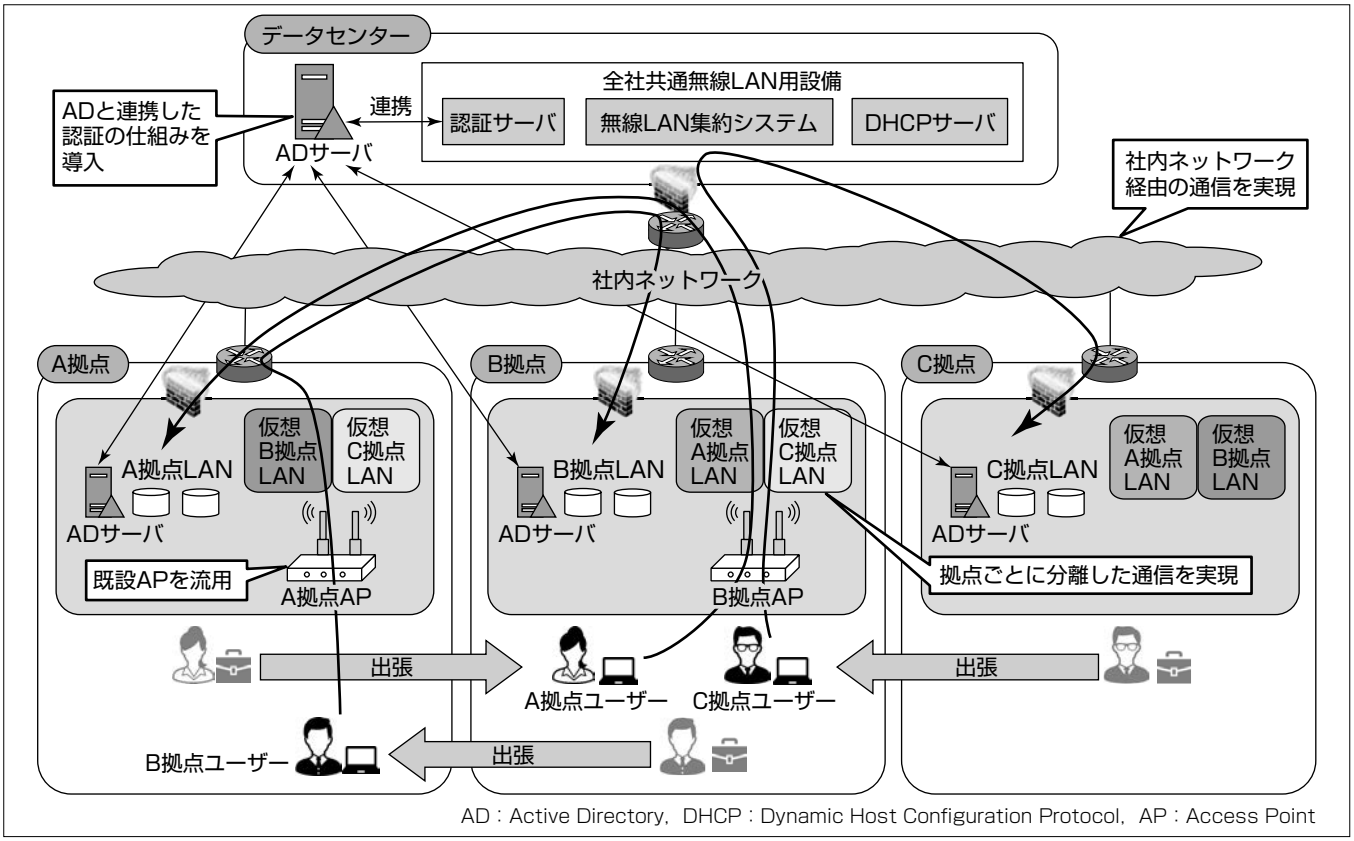
要　旨

近年，多様な働き方を可能とする“働き方改革”実現のため，労働環境の改善に取り組む企業が増えている。働き方改革の重要な施策の一つとして，いつでもどこでもセキュアに簡単に社内ネットワークに接続できる無線LANの構築が挙げられる。三菱電機は，全国に約40拠点が存在するが，拠点ごとにセキュリティ要件や利用するシステムが異なるため，それぞれが独自にネットワークを構築している。よって，他拠点に出張する際は，社内であるにもかかわらず出張先拠点の社内ネットワークに接続できず，インターネットVPN(Virtual Private Network)接続サービスを利用して，自拠点に接続している。

そこで，各拠点のセキュリティ要件を満たしつつ，他拠点から自拠点のネットワークに接続できる出張者用の全社共通無線LANを構築・展開した。

出張者のパソコンに自動で自拠点用のIP(Internet Protocol)アドレスを付与する仕組みとし，自席と同じネットワーク環境で，システムを利用できるようにした。また，全社共通無線LAN接続時の認証には，Active Directory(注1)参加時にパソコンに自動付与される“コンピュータアカウントパスワード”を活用することで，ユーザーの接続操作を簡略化するとともに，無許可の持込みパソコンの接続をシステム的に規制し，セキュリティレベルを向上させた。社内展開に際しては，出張の受入れが多い本社ビルへ早期に導入したことで，多くの拠点に利便性が認識され，全社への展開が加速された。

（注1）　Active Directoryは，Microsoft Corp.の登録商標である。



AD：Active Directory，DHCP：Dynamic Host Configuration Protocol，AP：Access Point

全社共通無線LANの構成

社員が他拠点に出張した時に，自身が所有しているパソコン等を出張先拠点の無線LANに接続するだけで，自拠点のシステムを利用できる。なお，無線LANの認証段階で出張元拠点を自動判別し，無線LAN集約システムで社内ネットワーク内の通信経路を接続拠点ごとに論理分割することによって，セキュリティ要件が異なる拠点ごとの通信が混在しないようにした。

*三菱電機㈱ IT戦略室　**三菱電機インフォメーションネットワーク㈱

1. まえがき

近年，多様な働き方を可能にする“働き方改革”実現のため，労働環境の改善に取り組む企業が増えている。働き方改革の一つとして，ノートパソコン，タブレット端末を用いたペーパーレス会議や，社員一人ひとりに固定した席を割り当てずに社員が状況に応じて働くスペースを自由に選択できるフリーアドレス型オフィスなどの導入が進められている。このような取組みを行う上で重要になるのが，いつでもどこでもセキュアに簡単に社内ネットワークに接続できるネットワーク環境である。そこで，これらを実現するための，社内ネットワークの無線LAN化が急務となっている。

2. 全社共通無線LANの構築

2.1 背　景

三菱電機は，全国に製作所，研究所，支社など約40拠点を構え，それぞれの拠点にIT部門が存在して社内ネットワークを構築している。製作所，研究所など拠点ごとに事業内容が異なり，セキュリティ要件も異なるため，三菱電機の社員が他拠点に出張した際，出張先拠点の社内ネットワークに接続できなかった。そこで，出張者は，社外にいる時と同様にインターネットVPN接続サービスを用いて，自拠点のネットワークにアクセスしていた。社内の出張にもかかわらず，一度インターネットに接続しなければならず，接続手順や通信速度等の問題が発生していた。

2.2 課　題

三菱電機の既存の無線LANでの課題は次のとおりである。

⑴　セキュリティ要件

出張先拠点の無線LANから社内ネットワークに接続する際，拠点ごとのセキュリティ要件を保つ必要がある。

⑵　接続手順

従来，社内ネットワークに接続するには，パソコンをインターネットに接続し，社内ネットワークに接続するためのインターネットVPN接続サービスを起動し，ユーザー認証を行う必要があった。この手順を簡略化し，セキュアで簡単に社内ネットワークに接続できるようにする。

⑶　通信速度

自拠点で社内ネットワークに接続した場合と同等の通信速度とする。

⑷　コスト低減

出張時に必須であったデータ通信端末のコストを低減する。

2.3 全社共通無線LAN

2.3.1 ADと連動したセキュア接続

無線LAN接続時の認証フェーズで，Active Directory（AD）と連携し，AD内に登録された属性情報（所属拠点情報）に応じて，論理分割したネットワークの割当てを行う。論理分割によって，出張先拠点の無線LANからは切り離された状態で，自拠点のネットワークに接続できるようにした。

2.3.2 通信コストの抑制及び通信レスポンスの改善

出張先拠点のネットワークからは論理的に切り離しつつ，直接自拠点のネットワークへ接続できるようにすることで，出張時にインターネット経由でのVPN接続を行う必要がなくなり，モバイルサービス用のデータ通信端末が不要な構成にした。

また，出張先拠点に出張者向けの専用設備を構築せずに，既設無線LAN設備に機能統合する仕組みとし，全社的な環境整備にかかるコストを抑制した。

併せて，インターネットを経由しない構成とすることで，通信レスポンスを改善した。

2.3.3 既存データベースを活用した無線LANの認証方式

既存AD内の属性情報（パソコンの所属や管理情報）を活用することで，別途認証のためのデータベースの構築・運用を不要にした。

無線LANに接続する時にADと連携してコンピュータ認証を行うことで，電子証明書による端末制限と同等レベルの制御を実現した。

2.3.4 シームレスな無線LAN接続

出張者が接続する無線LANのSSID（Service Set IDentifier）(注2)を全拠点で統一することで，出張時に拠点の無線LANの対応エリアに入ると，自動的に無線LANに接続する仕組みにした。

無線LANに接続する時に，その都度ユーザーが認証情報を入力する必要がなく，ユーザーの利便性向上を図った。

（注2）　無線アクセスポイントを識別するための名称

2.4 全社共通無線LANの設計・構築

全社共通無線LANでは，社員がどの拠点へ出張してもパソコンの設定を変更せずに自動的に自拠点のネットワークに接続でき，自席と同じネットワーク環境でシステムを利用できるようにすることを大前提として，検討を開始した。そのため，パソコンのIPアドレス取得と，社内ネットワークに接続するための認証行為を，どの拠点に出張しても自動的に行う仕組みが必要であった。

2.4.1 出張時のIPアドレス付与とアクセス制御の仕組み

IPアドレスを自動取得するには，DHCPを利用するのが一般的な手法である。

出張時に拠点を移動した時に，出張先拠点にいながら自拠点だけへ通信できるようにするためには，出張元拠点と出張先拠点の組合せでの通信のアクセス制御が必要になる。しかし，社内ネットワークの構成上，拠点ごとにパソコンに割り当てるIPアドレスが異なるため，各拠点内に出張元拠点数分のIPアドレス帯の割当てが必要になり，管理負荷が高くなる（**図1**）。

アクセス制御及びIPアドレス帯の管理負荷を軽減する

ため，出張時にパソコンに割り当てるIPアドレス帯を出張先拠点にかかわらず統一し，管理するIPアドレス帯の必要数を削減する仕組みが必要であった。

この仕組みに，オーバーレイネットワーク技術を採用した。オーバーレイネットワークは，物理ネットワークのトポロジーを意識せずに，物理ネットワーク上に仮想的な論理ネットワークを構成する技術である。この技術を用いることで，出張者用IPアドレスをセンター設備にオーバーレイすることと，センター及び各拠点で同一の出張者用IPアドレスを構成することができるようになり，パソコンに割り当てるIPアドレス帯を削減しつつ，どの出張先拠点でも同じIPアドレスの利用が可能になった(**図2**)。

また，製作所，研究所，支社ごとに求められるセキュリティ要件が異なるため，出張先拠点から自拠点のネットワークだけに接続できるようにアクセス制御を行う必要がある。しかし，オーバーレイネットワークによって，どの拠点へ出張しても付与するIPアドレスが，拠点出張用アドレスとなるため，ファイアウォールでのアクセス制御も容易になった(**図3**)。

2.4.2 IPアドレス自動取得の仕組み

どの拠点に出張しても，自拠点出張用のIPアドレスにするためには，パソコンの所属拠点を判別し，それに応じたIPアドレスを自動的に付与する仕組みが必要であった。

この課題を解決するために，認証用のデータベースにパソコンの所属拠点情報を付与し，認証時にパソコンの所属拠点を判別できる構成にした。参照先データベースには，既に全社端末情報を保持しているADを採用し，コスト抑制も実現した。パソコンに付与した拠点情報を基に，出張時に所属拠点ごとの専用のIPアドレスを割り当て，DHCPサーバから払い出すIPアドレス帯は，どの拠点に出張した際も変わらない仕組みを実現した(**図4**)。

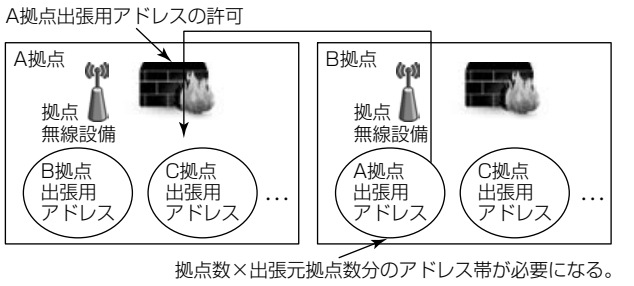


図1．各拠点に出張元拠点のアドレス帯を準備した場合

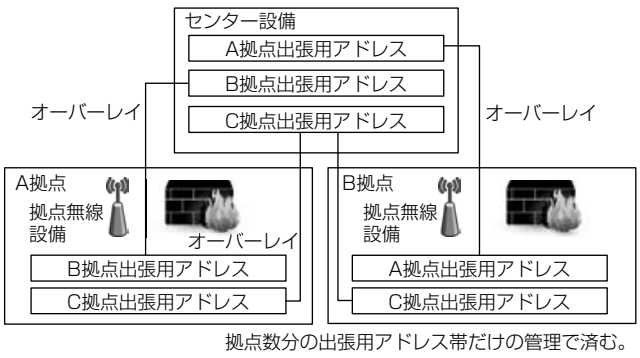


図2．オーバーレイネットワークの論理構成

2.4.3 自動認証の仕組み

これまで出張時に利用していたモバイルサービスは，社内ネットワークに接続する都度，ユーザーが認証情報を入力する必要があり，ユーザーの操作が煩雑であった。

この課題を解決するために，全社共通無線LANでは，セキュリティレベルを保ちつつ，無線接続時の認証までの接続操作を簡略化できる仕組みを実現する必要があった(**図5**)。

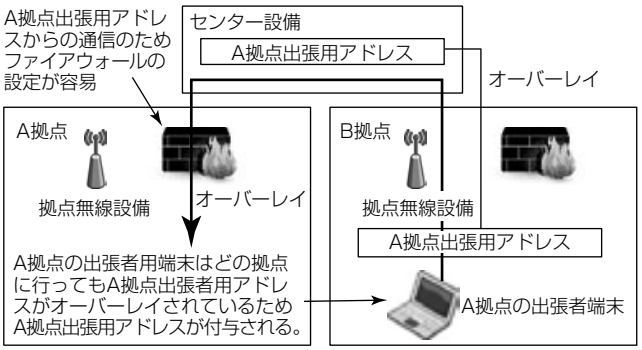


図3．出張時の通信経路

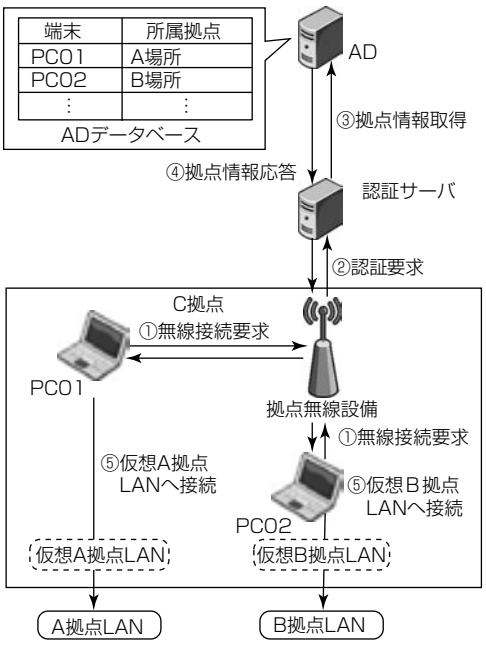


図4．パソコンの所属拠点判別の仕組み

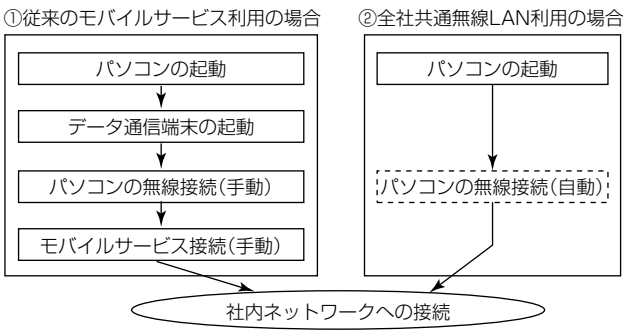


図5．モバイルサービスと全社共通無線LANの接続操作比較

これらを満たす認証情報として，**2. 3. 3項**でも利用しているADの機能であるコンピュータアカウントパスワードを採用した。

コンピュータアカウントパスワードは，パソコンがADドメインへ参加する時に，ユーザーには見えない形でパソコンとADの間で自動的に設定される。そのため，ユーザーが無許可の持込みパソコンなどに認証情報を流用することや，画面のぞき見による認証情報の流出などを未然に防止でき，社内ネットワークに求められるセキュリティレベルを充足した。

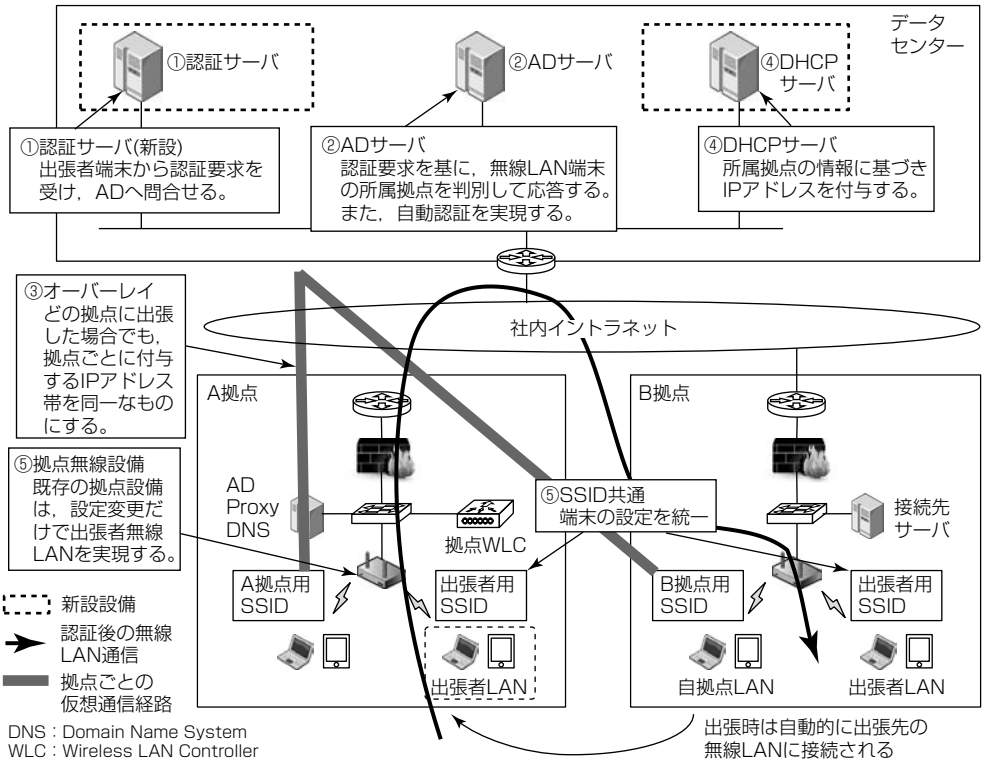


図6．全社共通無線LANの全体構成

また，全社共通無線LANに用いるSSIDの仕様を全拠点で統一し，パソコンへSSID及び認証情報を事前設定することで，パソコン起動に合わせて，自動的に無線LANに接続できるようにした。これらの組合せによってセキュアかつシームレスな無線LAN接続を実現した。

接続操作手順の簡略化によって，パソコン起動から社内ネットワークへの接続時間は，従来のモバイルサービスでは約60秒であったが，全社共通無線LANでは約10秒となり，1回当たり約50秒の短縮を実現した。

2. 4. 4　全社共通無線LANの実装

2. 4. 3項のとおり，全社共通無線LANは，オーバーレイネットワーク技術とパソコンの所属先の判別によって，自動的に自拠点用のIPアドレスを付与する機能を実現した。また，自動認証によって，ユーザー操作を省きつつ，セキュリティレベルも担保する構成にした。

全社共通無線LANは，既に整備済みの拠点の無線LAN設備を有効活用しつつ，データセンターに認証サーバとDHCPサーバだけを導入してこの機能を実現しており，最小のコストで最大限の効果を生み出している(**図6**)。

3. 全社展開に向けて

このサービスでは，専用の無線LAN設備を個別に構築することなく，拠点側の無線LAN設備に全社共通無線LAN用のSSID及び認証に係る設定追加をするだけで全社共通無線LANの機能を利用できるようにした。

本社ビルでは，既にビル全館で利用できる拠点の無線LANが整備されており，全社共通無線LANを追加導入することによって，ビル全館で出張者が社内ネットワークに接続できる環境を整備した。

出張者向けサービスのため，自拠点に全社共通無線LANを導入しても自拠点単独では恩恵を受けない。そのため，各拠点は全社共通無線LANの導入に消極的であったが，全社へ導入することによって全体的な効果が得られることを周知し，導入を促進した。各拠点からの出張の受入れが多い本社ビルへ全社共通無線LANを早期に導入したことで，多くの拠点に全社共通無線LANの利便性が認識され，各拠点での展開の加速に貢献した。

4. 効　果

全社共通無線LANの利用状況は，のべ約6,330台/月となり，以前と比較してパソコン起動から社内ネットワークへの接続工数を88時間/月短縮している。また，通信レスポンスに関しても，従来のインターネットVPN接続サービスと比較して応答速度が5～6倍になるなど，大幅に改善した。

5. むすび

全社共通無線LANの導入によって，社内拠点への出張者がインターネットVPN接続サービスを用いることなく，簡単に社内ネットワークに接続できる事例について述べた。

今後，全社共通無線LANの接続元となる拠点の無線LANを低コストで整備し，全拠点の無線LAN化を推進していく。