IPTPC認定技術者資格制度
技術者教育プログラム

IPTPC
IP Telephony Promotion Center

テキストサンプル

無線LANデザイナ研修

教育テキスト

- 第4.0版 -

IP電話普及推進センタ

注意事項

- 本テキストの内容については断りなく変更を行うことがあります
- 本テキストの誤りに関連して生じた偶発的、あるいは派生的な損害については、その責任を負いかねます
- 本テキストは無線LANデザイナ研修の評価用に無線LANデザイナ研修テキスト4.0版を基に作成したものです。他の目的での複製、再利用、再使用を禁じます。

第１章

スマートフォンとWi-Fi導入活用の最新動向

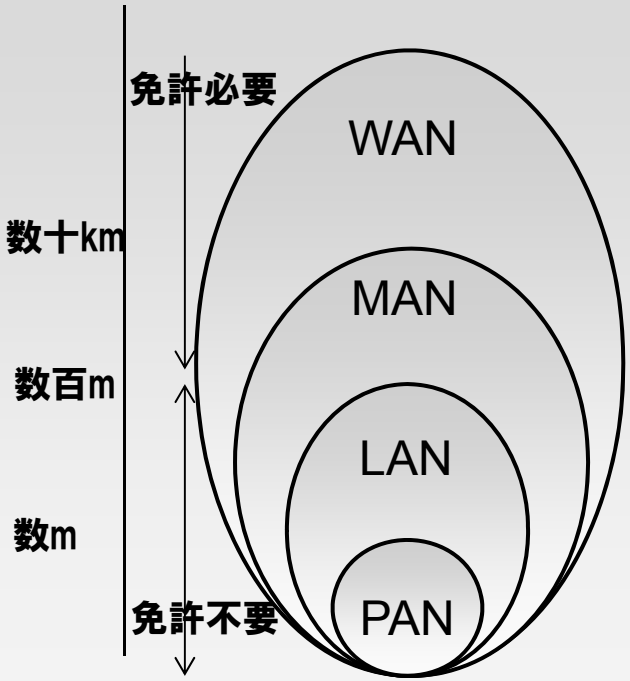
（4.0版）

無線アクセスシステムの分類(エリアサイズ）

エリアサイズによる無線アクセスシステムの分類

無線アクセスシステムはサービスエリアのサイズによっても、下図のようにPAN、LAN、MAN、WANと分類できる。一般的な傾向として、エリアサイズが小さいほど高速な通信が可能である

サービスエリアが小さいPAN、LANは免許不要であるが、MAN、WANは一般に免許が必要である。ネットワークに関連する標準化を行うIEEE802委員会では、それぞれの無線アクセスシステムに対応したタスクグループが活動しており、標準規格を策定している。



	IEEEにおける分類	代表的サービス
WAN	IEEE 802.20	MBWA(日本国内では未サービス)
MAN	IEEE 802.16	モバイルWiMAX
LAN	IEEE 802.11	無線LAN(Wi-Fi)
PAN	IEEE 802.15	Bluetooth、UWB,ZigBee,ANT+

WAN: Wide Area Network MAN: Metropolitan Area Network
LAN: Local Area Network , PAN: Personal Area Network

MBWA: Mobile Broadband Wireless Access, UWB: Ultra Wide Band

1-1-5. 各アクセス方式の特徴（LAN）

無線LAN

ノートPCやスマートフォンなどモバイル端末のネットワーク接続方法としてデファクトスタンダードとなっている。

移動速度	電波範囲	電波出力
低速（歩行程度）	数百m（※）	中

端末がAP(アクセスポイント)のカバーエリアに入っている場合にアクセスができる

① 端末が移動せずに同一のAPを利用

② サービスエリア内のAPをローミングしながら移動

IEEE802.11規格に準拠した無線LAN製品の相互接続性をWi-Fiアライアンスが認定しており、認定された製品にはWi-Fiマークが付与される

Wi-Fiマーク

無線LAN規格	周波数帯	最大伝送速度	主な用途	策定年
IEEE802.11b	2.4GHz	11Mbps	オフィス向け	1999
IEEE802.11a	5GHz	54Mbps	オフィス向け	1999
IEEE802.11g	2.4GHz	54Mbps	オフィス向け	2003
IEEE802.11n	2.4GHz、5GHz	300Mbps～600Mbps	オフィス向け	2009
IEEE802.11ad	60GHz	6.8Gbps	近距離向け	2013
IEEE802.11ac	5GHz	6.9Gbps	オフィス向け	2014
IEEE802.11ah	920MHz	312Mbps	長距離、IoT向け	2016予定

※アンテナなどを工夫することで数十km到達できるシステムもあるが本講座では扱わない。
802.11ad **は**10m **程度、**802.11ah **は**1Km**程度である。**

1-2-3. モバイル端末の内線利用(企業向けFMCサービスの例）

企業向けFMCサービスとしては現在は下記の3方式がある

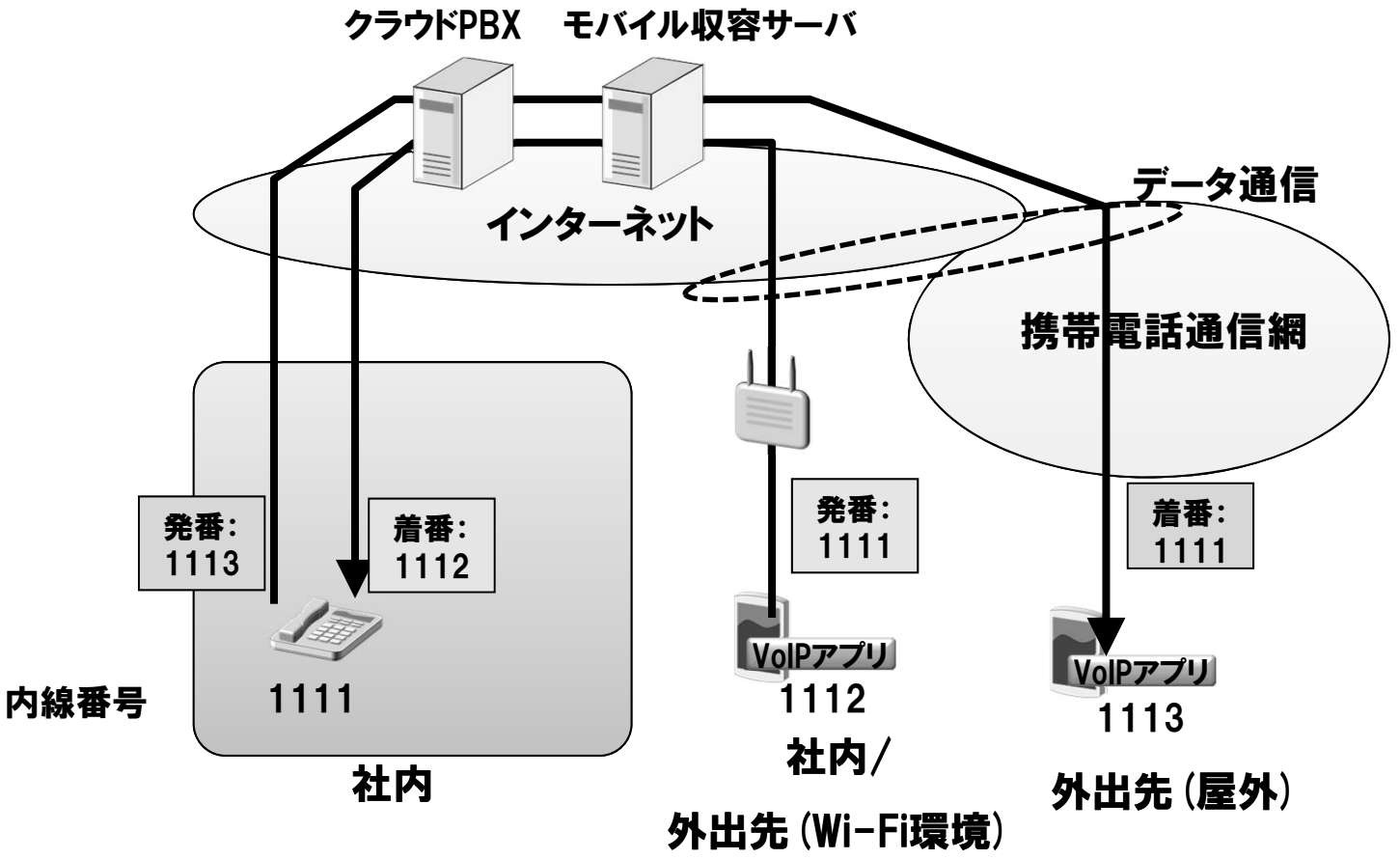
「VoIPアプリ型」、「コールバック転送型」は中小企業、「キャリアFMC型」は中堅～大手企業で導入される傾向にある。

タイプ	方式	特徴
VoIPアプリ型	モバイル端末にインストールした通話アプリケーションにより発着信する。通話はデータ通信を利用する	特長：音声回線を利用しないため海外でも利用可能 課題：データ回線で通信するため音質が保証されない。待ち受け時の電力消費が多い
コールバック転送型	モバイル端末にインストールした発信アプリケーションを用いる。通話は音声通信を利用する	特長：通話時の課金が端末側に発生しない（BYOD向け） 課題：発信操作が2ステップになる。端末の番号通知が行えない
キャリアFMC型	モバイルキャリア網と企業内のPBXが連携しており、モバイル端末では直接ダイヤル発着信を行う。通話は音声通信を利用する	特長：電話発信と同じ手順で内線番号に発信できる 課題：利用するモバイル端末は契約キャリアへの統一が必要

1-2-4. モバイル端末の内線利用の例（VoIPアプリ型）

通話アプリケーション（VoIPアプリ）をユーザのスマートフォンにインストールし、そのアプリケーションを用いてデータ通信により通話を行う。

端末キャリアに依存せず、通話無料であることが特徴。PBXはユーザの拠点に設置される場合もある。



第2章

無線LANの基礎と置局設計

（4.0版）

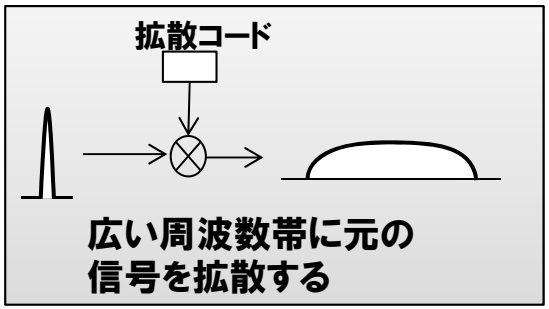
2-1-10. 2次変調(DSSS,OFDM)

2次変調方式

2次変調では、1次変調された信号を広い周波数帯に拡大する。これによりノイズの多い環境でも安定して通信が行える。また複数の信号を多重化するOFDM方式では他の二次変調方式よりも高速化が図れる。

DSSS

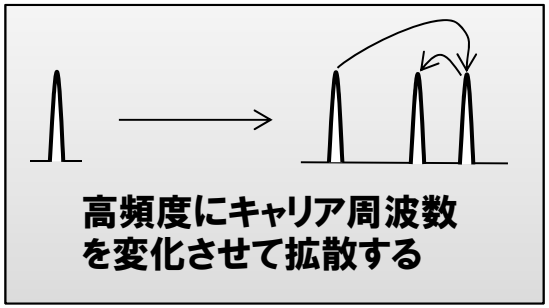
Direct Sequence
Spread Spectrum
直接スペクトラム
拡散変調



ホワイトノイズに近い拡散コードと1次変調波のXORを取ることで広帯域に信号を拡散する。ノイズに強い。拡散コードを工夫することで送信速度を向上できる(CCK方式)
適用例: 802.11b, W-CDMA(3G/3.5G)

FHSS

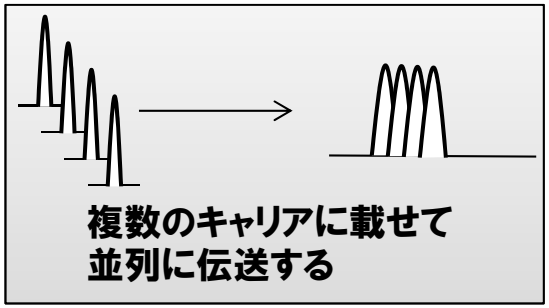
Frequency Hopping
Spread Spectrum
周波数ホッピング
拡散変調



キャリア周波数を高頻度に変化させることで広帯域に信号を拡散する。ノイズに強い。
適用例: Bluetooth

OFDM

Orthogonal Frequency
Division Multiplexing
直交周波数
分割多重

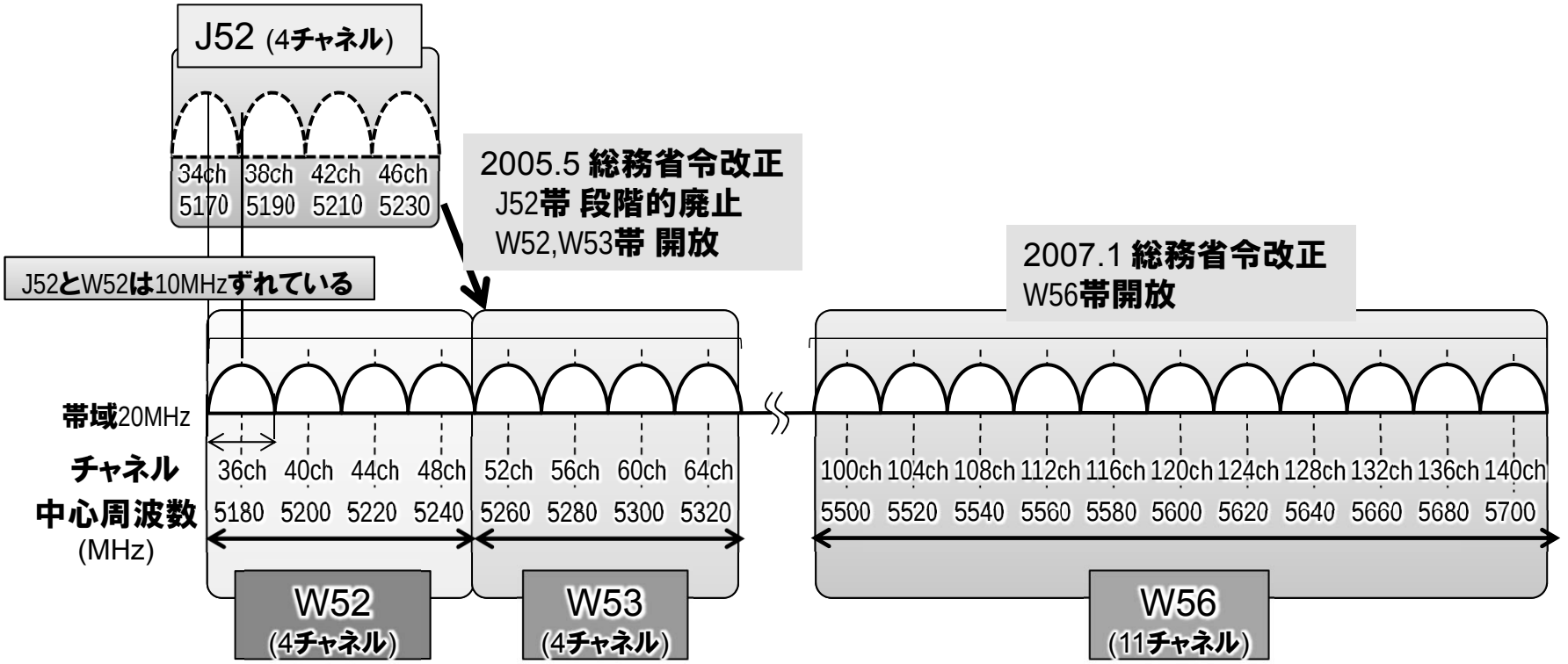


複数のキャリアを重ねて伝送する。それぞれのキャリアは互いに独立して分離できため混ざることなく受信側で信号を分離できる特徴がある(「直交性」)。ノイズ、フェージングに強い。周波数の利用効率が高く、高速な伝送が実現できる
適用例: 802.11a/g/n/ac LTE(3.9G)

2-2-3. 5GHz帯の特徴

5GHz帯無線LANの特徴

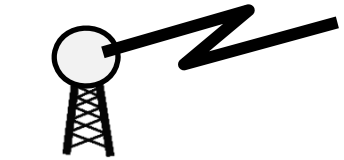
- 5.15~5.35GHz，5.47 ~ 5.725GHzを利用
- 日本国内ではかつて国際規格と互換性のないチャネル（J52 ）であったが、2005年5月の総務省令で国際規格（W52、W53）に合致させた。 2007年1月にはW56を開放し現在は19ch
- チャネル間隔とチャネル帯域幅20MHz。2.4G帯と異なり干渉することなく全チャネルを同時に利用可能



2-2-4. 5GHz帯の特徴（つづき）

- レーダーなどの業務用無線と周波数帯が重なるため無線LAN側での干渉防止措置を実施
  - 屋外利用禁止： W52、W53帯
  - 干渉防止機能搭載：W53、W56帯

  - 干渉防止機能：
    - DFS: APに実装する。気象レーダーの電波を検出すると、衝突しないチャネルに自動的に移動する機能。電源投入時に60秒電波をモニターするため、AP起動後すぐには通信ができない。また万一運用中に同じチャネルで気象レーダーの電波を検知するとチャネルを変更しさらに60秒モニターする。その間通信ができなくなる。運用に注意が必要



気象レーダー

モニター：同じチャネルで気象レーダーの電波の有無をチェック

アクセスポイント

① AP起動時、送信しようとするチャネルを60秒間モニター
② 運用中もモニターしつづける。レーダーの電波を検知したら、送信を停止し、別のチャネルを60秒モニター

    - TPC：APと端末に実装する。他の電波を検出すると送信出力を制御する機能

周波数帯	W52	W53	W56
屋外利用	禁止	禁止	許可
干渉防止機能	なし	DFS、TPC必須	DFS、TPC必須

DFS: Dynamic Frequency Selection
TPC: Transmit Power Control

2-4-7. 置局設計の概要

置局設計とは

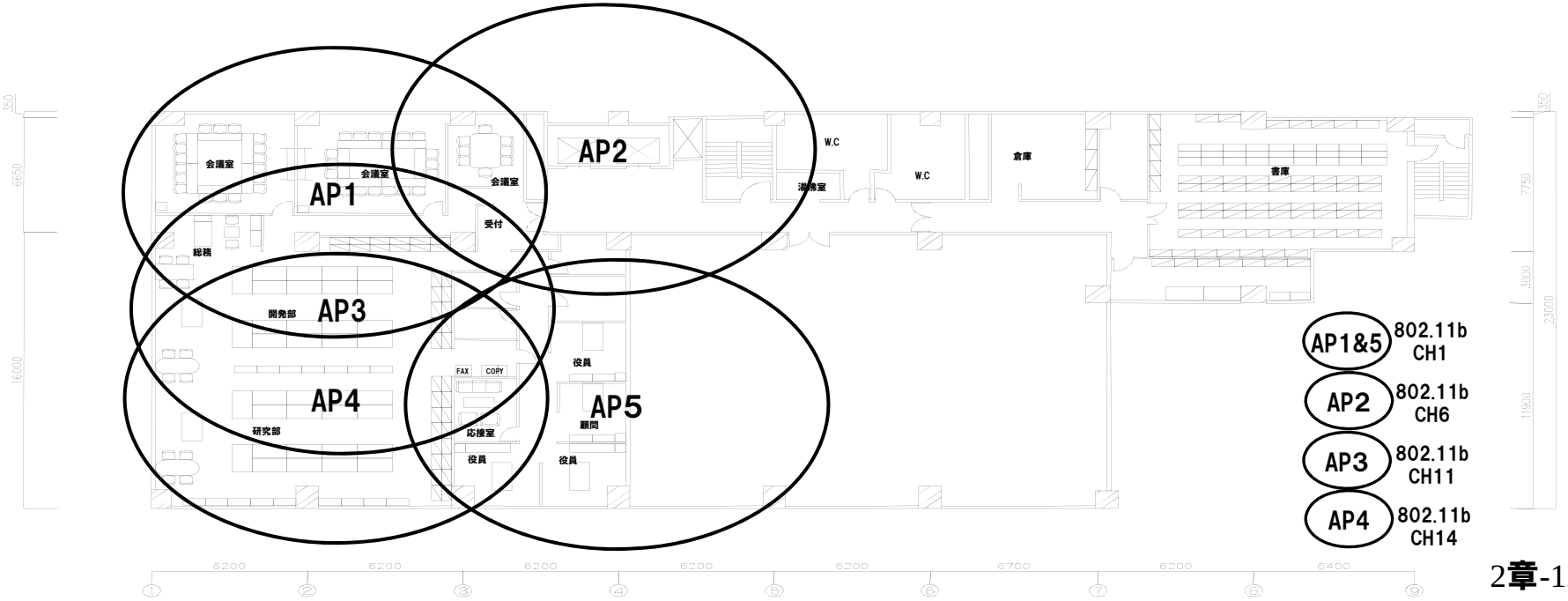
置局設計は電波の到達範囲を把握するもので、「机上設計」と「現地調査」の2つの段階がある。まずは机上で設計を行い、実機を持ち込んで現地でのサイトサーベイを行う。

（１）前提条件：

方式検討、製品選択が完了していること。採用する製品によって伝送特性が異なるため、確定した製品で検討する必要がある。

（２）事前準備：

フロア図面（座席の配置など）、壁の材質（金属、木、石膏、ガラス、コンクリートなど）、配線がどのように施設されているか、等についての情報を入手しておく。



第３章

無線LANの脅威とセキュリティ対策

（4.0版）

3-1-1. 無線LANのセキュリティ脅威と対策

無線LANはLANケーブルなど物理的接続が不要というメリットがある一方、攻撃者の存在に気づきづらい特性があり、特有のリスクがある。対策として、「APを隠す」「データの暗号化」「接続時の認証」がある。 本節ではこれらの技術のポイントと実現方式を説明する

脅威

盗聴	不正接続	不正AP
利用者とAP間の通信をキャプチャして内容を解読する	攻撃者がAPに接続してイントラネットに侵入する	攻撃者が設置した偽APを利用者に接続させる

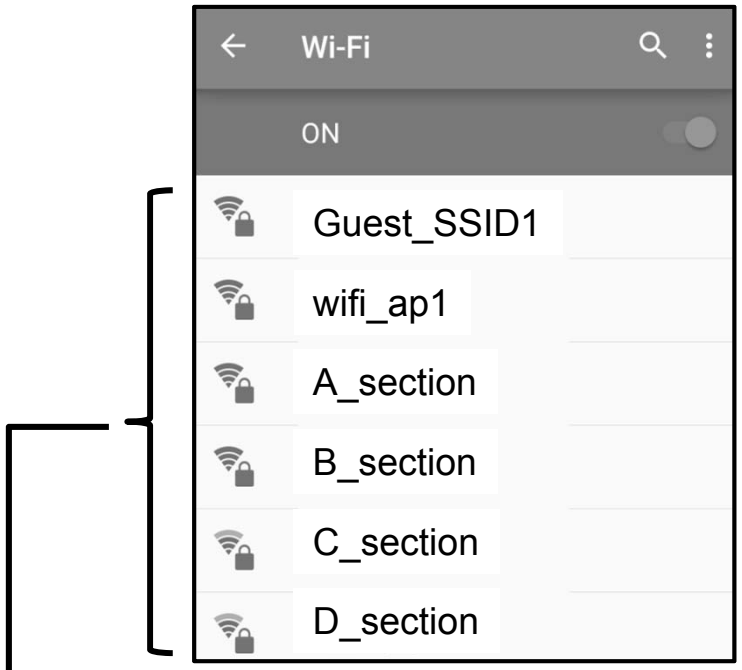
対策

- **APを隠す**
  電波漏洩の防止・SSID隠ぺい
- **（APの）認証**
  802.1X、無線IDS
- **暗号化**
  WEP・WPA（TKIP）・WPA2（AES）
- **認証**
  802.1X、Personal認証
  MACアドレス認証

3-2-4. アクティブスキャンとパッシブスキャンの例 参考

スマートフォンのWi-Fi一覧画面の表示の一例を示す。

スマートフォンやPCのWi-Fi接続画面の一覧に、何も設定しなくても表示されるAPはパッシブスキャンで動作している



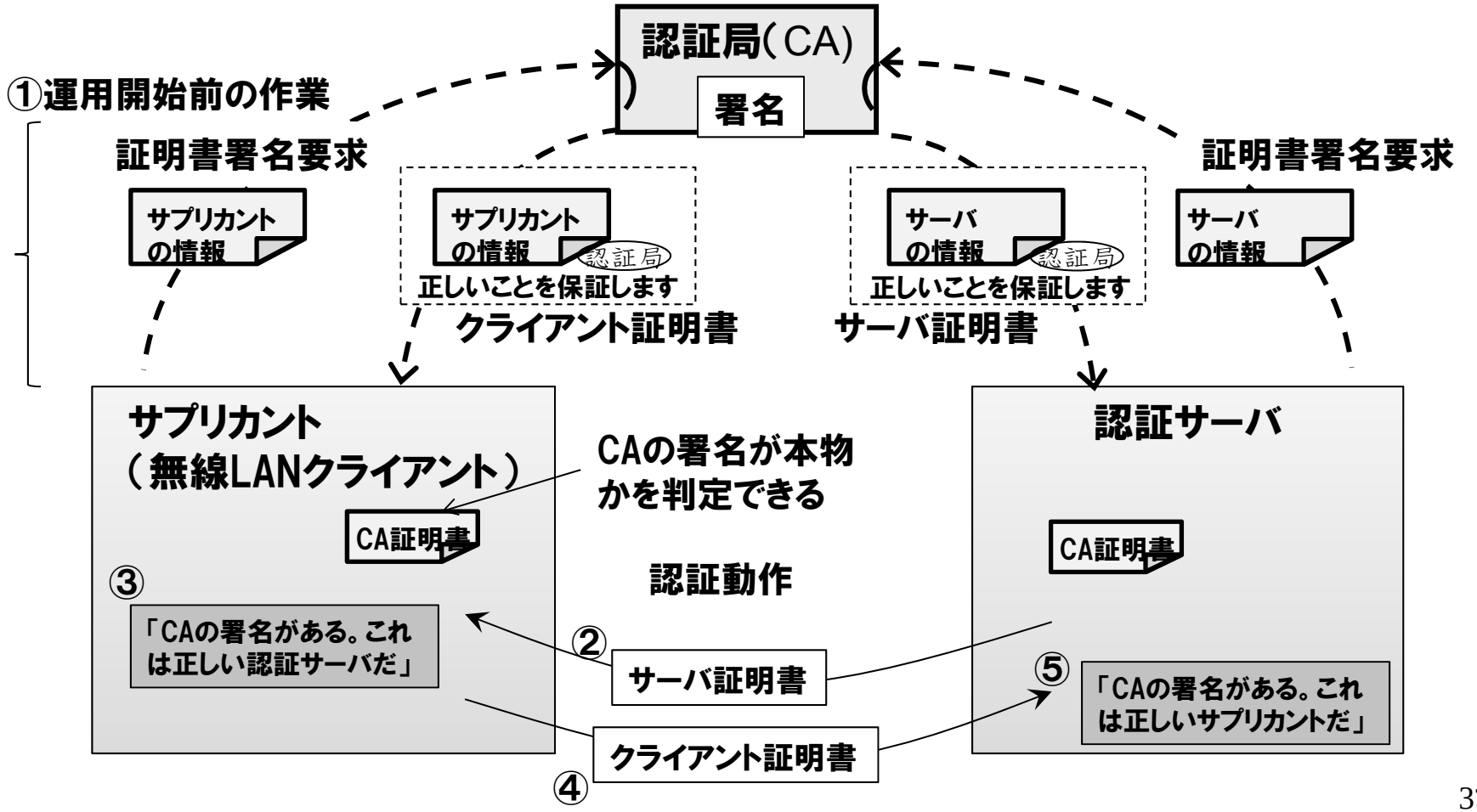
パッシブスキャンで動作中のAP

一覧に表示されず、手動で設定が必要なAPはアクティブスキャンで動作している

アクティブスキャンで動作中のAP

3-3-9. 802.1X認証（証明書を用いた認証概要）

証明書による認証方式では、事前に認証サーバ、サプリカントが作成する自身の情報を、認証局が署名する。署名が本物のCAのものかを判定できる「CA証明書」を認証サーバ・サプリカントに事前にインストールする。 認証時には相手から送付された証明書の署名がCAの者であることを確認して、内容の正当性を判定できる。これらはPKI（公開鍵認証系）と呼ばれるセキュリティ技術で実現されている。



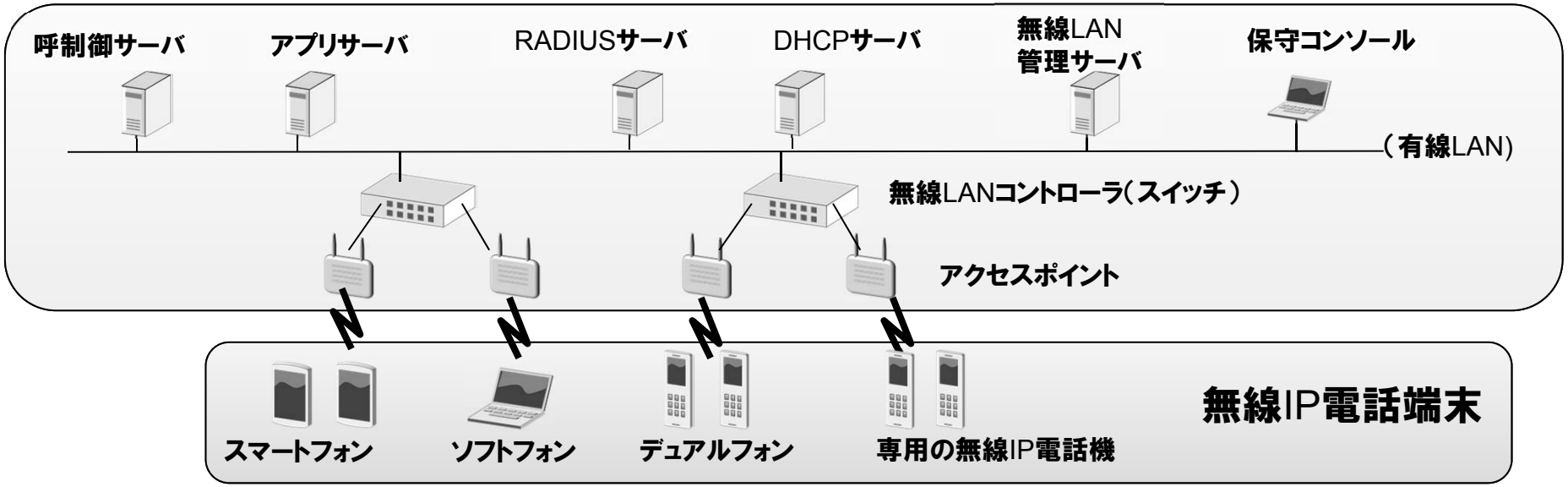
第４章

無線IP電話システム設計

（4.0版）

4-1-1. 無線IP電話システムの構成と動作

無線IP電話システムのネットワーク構成

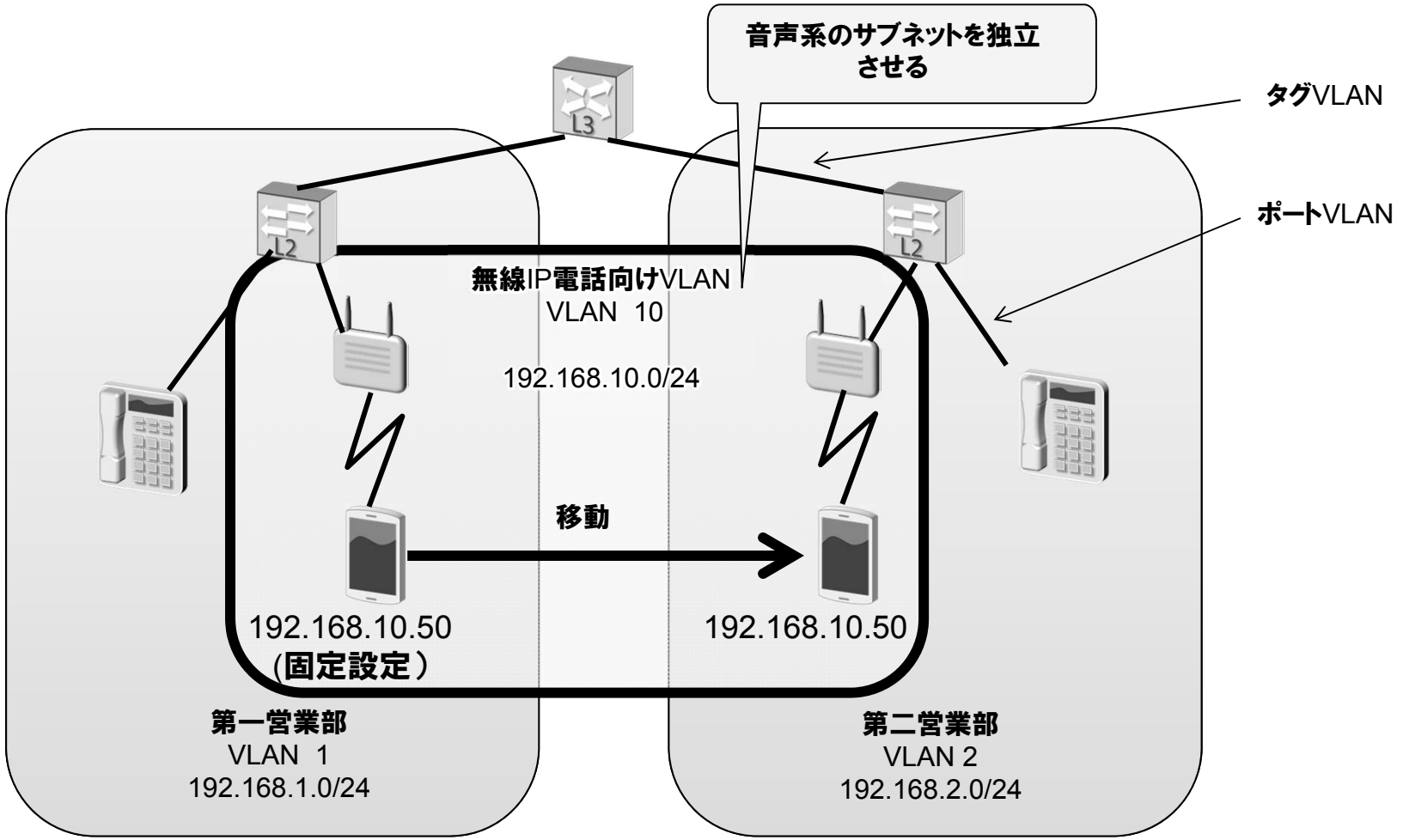


呼制御サーバ	**発信・着信・転送・保留など電話の基本サービスを提供。局線のインタフェースとなるメディアゲートウエイも制御する。アプリサーバとの連携した付加サービスも提供できる**
アプリサーバ	**電話帳など付加サービスを提供する**
RADUISサーバ	802.1X**認証により無線**LAN**コントローラを介して無線**IP**電話端末の認証を行う**
DHCP**サーバ**	IP**アドレスの管理・払い出しを行う**
無線LAN**管理サーバ**	**複数の無線**LAN**コントローラ、**AP**を一元管理する**
無線LAN**コントローラ**	AP**を集中制御・管理する。**802.1X**認証で**RADIUS**サーバの指示により接続制御を行う**
アクセスポイント	**無線クライアントと無線**LAN**による通信を行う。暗号化機能・**QoS**機能・**802.1X**認証機能を搭載するものもある**
無線IP**電話端末**	**電話端末。スマートフォン、携帯電話型、**PC**上での動作などいくつかの実装形態がある**

4-2-2. IPアドレス計画（VLANを用いた方式）

サブネット移動時のIPアドレス変更問題の解決方法の一つが VLANを用いた手法である。

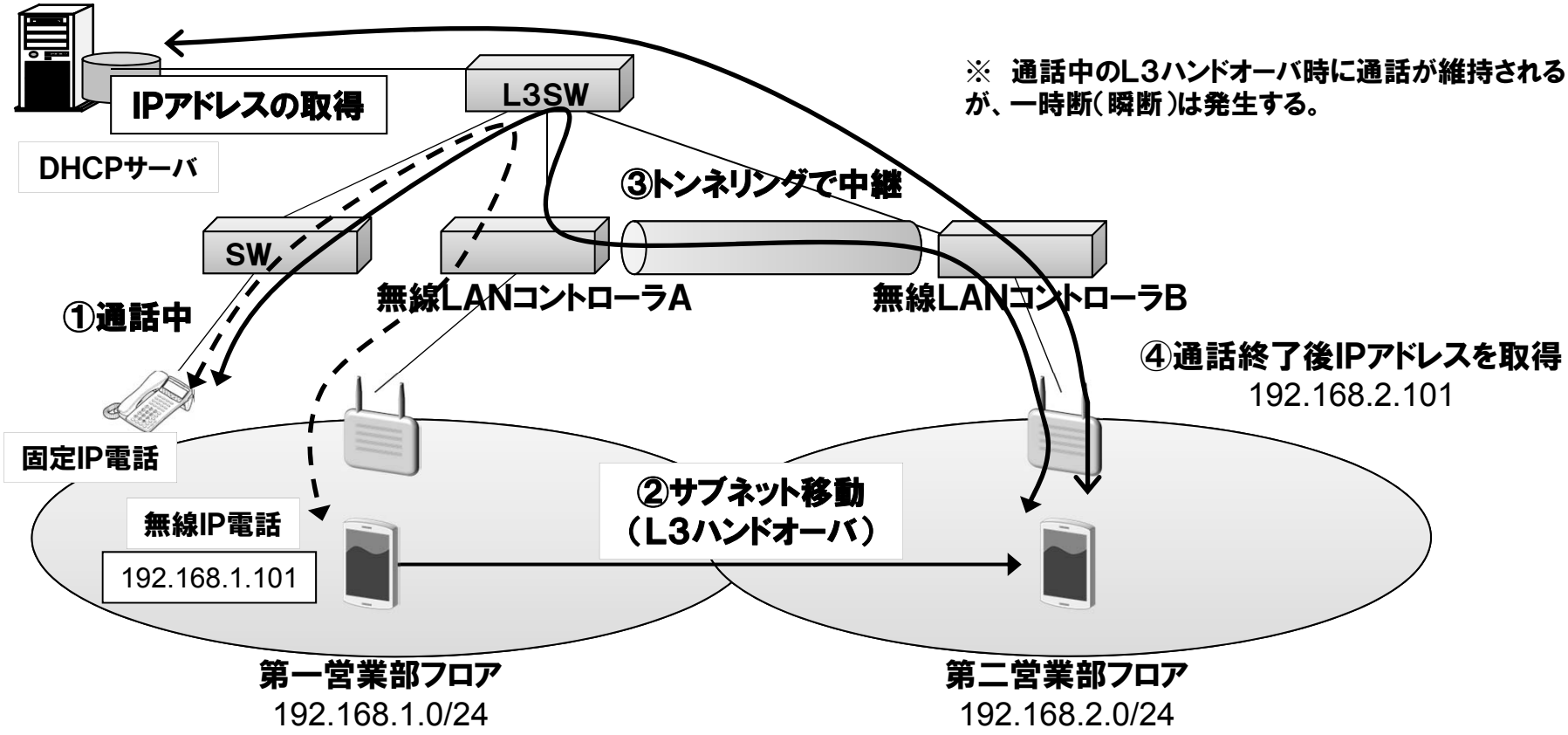
無線IP電話はフロアなど物理的なサブネットとは分離して同一のVLANにグループ化する。
別のフロアに移動しても、無線IP電話は同じIPアドレス帯で接続ができる。



4-2-7. IPアドレス設計と高速ハンドオーバ設計

参考

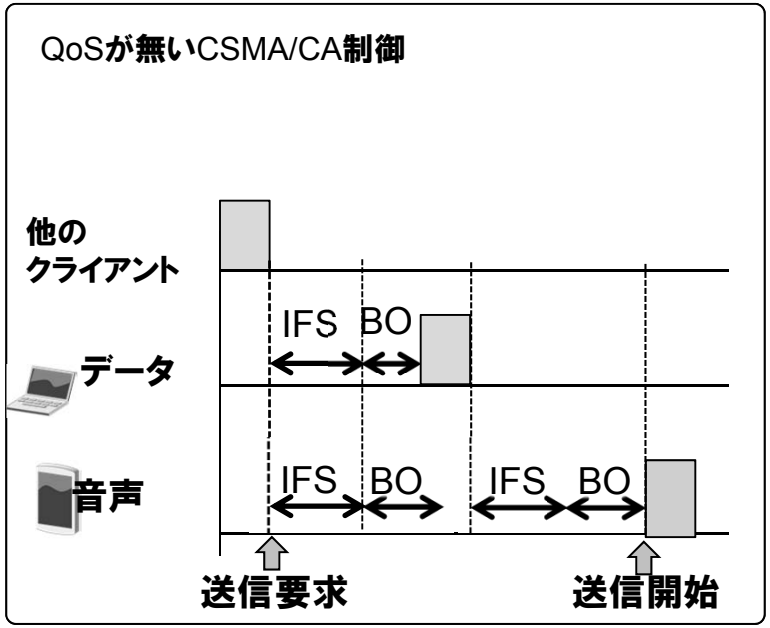
①固定IP電話と無線IP電話は通話中
②無線IP電話は第一営業部から第二営業フロアに移動（無線サービスエリアとサブネットの移動）
③トンネリングによる中継→通話を維持
・コントローラAとBは、無線IP電話機がコントローラBのAP配下に移動してきたことを認識
・コントローラA、B間でトンネリング処理し、コントローラAは音声パケットをコントローラBに中継
④通話終了後、新しいIPアドレスを取得

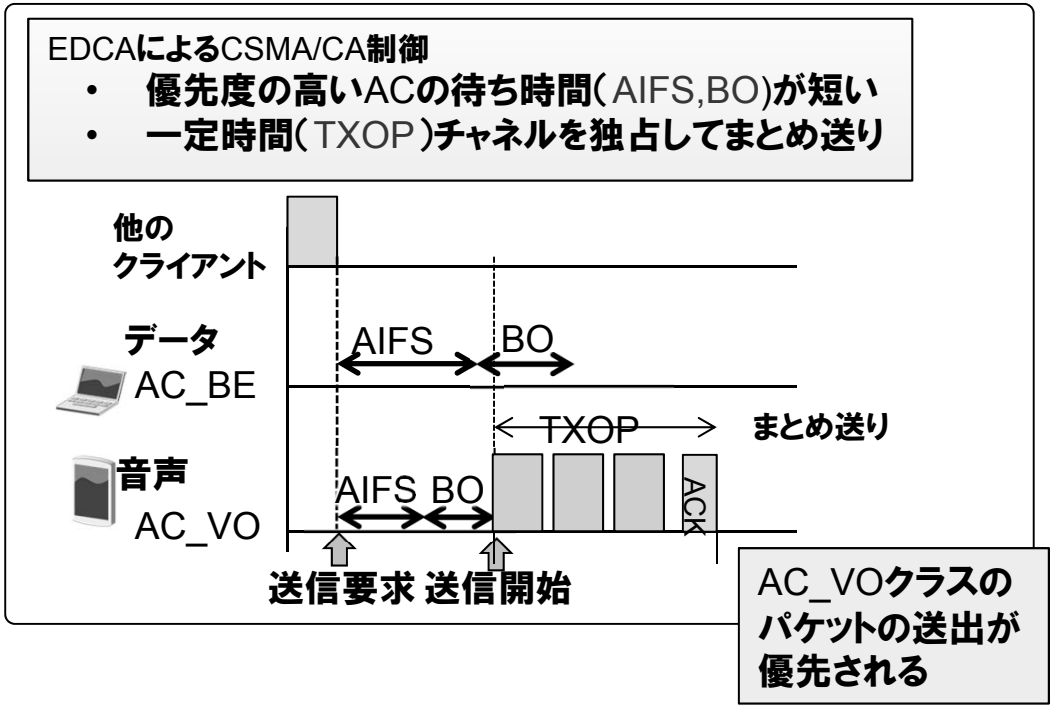


通話中のL3ハンドオーバ時、通話維持の処理例（トンネリング）

4-3-5. EDCA方式による優先制御

EDCA方式では、端末内、無線LAN(CSMA/CA制御)上でパケットの優先制御を行う
QoSが無い場合、音声以外の通信に影響を受けて遅延が増大する可能性があるが、
QoSが有効となることで音声など高優先度通信が無線区間で他の通信の影響を受けにくくなる





参考

EDCAのパラメータ(デフォルト値)

AC	AIFS	CWmin	CWmax	TXOP
AC_VO	2	3	7	1.504
AC_VI	2	7	15	3.088
AC_BE	3	15	1023	0
AC_BK	7	15	1023	0

msec

AIFS: Arbitration Inter Frame Space
TXOP: Transmission Opportunity

BO(Back Off)
0～ CW の範囲のランダム時間
(CW: CWmin≦CW≦CWmaxの整数値 とする)
再送ごとに CW=(CWmin+1)2^n−1 (上限は CWmax)
と増加させる

すなわち、再送ごとにBOを増やしてゆく。

第５章

無線IP電話システム導入・運用

（4.0版）

無線IP電話システムの提案業務の流れ

①受注・導入前の提案業務フロー

受注・導入前に現地サイトサーベイを実施し、無線LAN上で音声を使用できる環境かどうかを見極める必要がある。これを怠ると、導入後に音声品質が悪い、電話そのものが掛けられない、等のトラブルが発生する可能性が高く、顧客満足度を得るにあたって、非常に重要な部分である。

提案業務フロー	主担当	
客先要件確認	営業・SE	無線でのカバーエリア、セキュリティ、使用端末、収容人数(端末別)、既存ネットワーク構成、運用方法等の基本要件の確認
⇩		
机上設計(見積用暫定設計)	営業・SE	AP数、AP設置箇所を暫定的に決定、図面上でのシステム設計、要件を現地で確認
⇩		
暫定設計・見積提示	営業・SE	AP数、AP設置場所が変更になる可能性があることを説明した上で設計・見積を提示
⇩		
現地サイトサーベイ	置局設計部隊	AP数、設置箇所、使用chを決定
⇩		
設計見直し・再見積	営業・SE	無線LANの使用可否および要件に合うシステムを構築できるのか置局設計部隊・営業・SEで確認、APの増減により再設計・見積が必要な場合あり

受注・導入前の提案業務フロー例

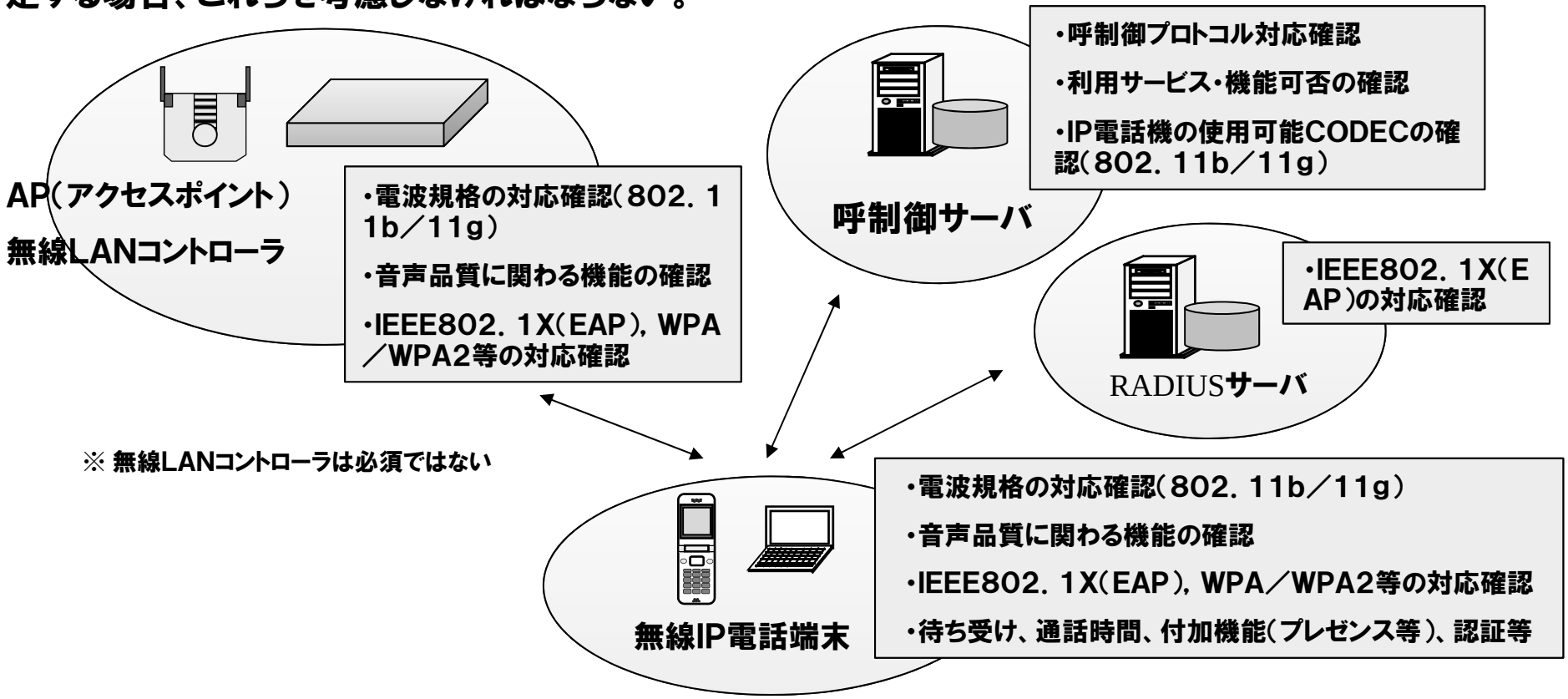
導入・運用ポイント

無線IP電話システム機器選定時の技術検討項目

無線IP電話端末で利用している無線LAN規格は 802.11b/gが主流である。コーデックはG.711とG.729aを標準搭載しているものが主体である。

呼制御プロトコルはSIPが主流であるが、H.323や独自プロトコルを採用しているものもある。

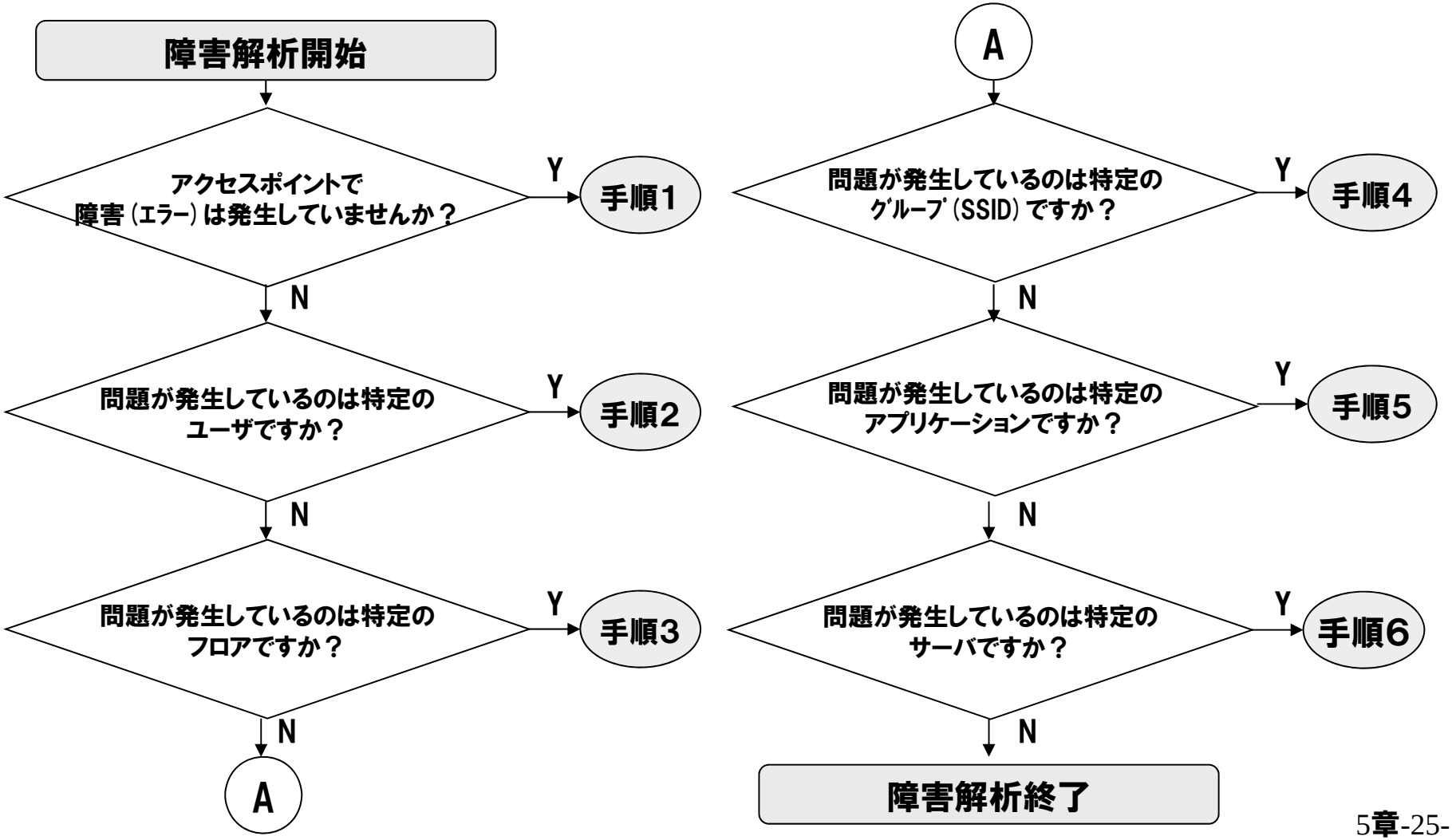
セキュリティはPEAP+WPAを始め各種IEEE802.1X(EAP)認証方式と暗号化方式があり、各機器を選定する場合、これらを考慮しなければならない。



無線IP電話システム運用時のトラブル分析方法

障害申告があった場合、その内容により切り分けを行うフローチャートを示す。

※ 実際の障害は、複数の要因で発生している事が考えられるので、一つ一つ問題を解決する様に対応する。



巻末資料

（無線LANデザイナ研修コース）

（4.0版）

無線通信技術の用語解説

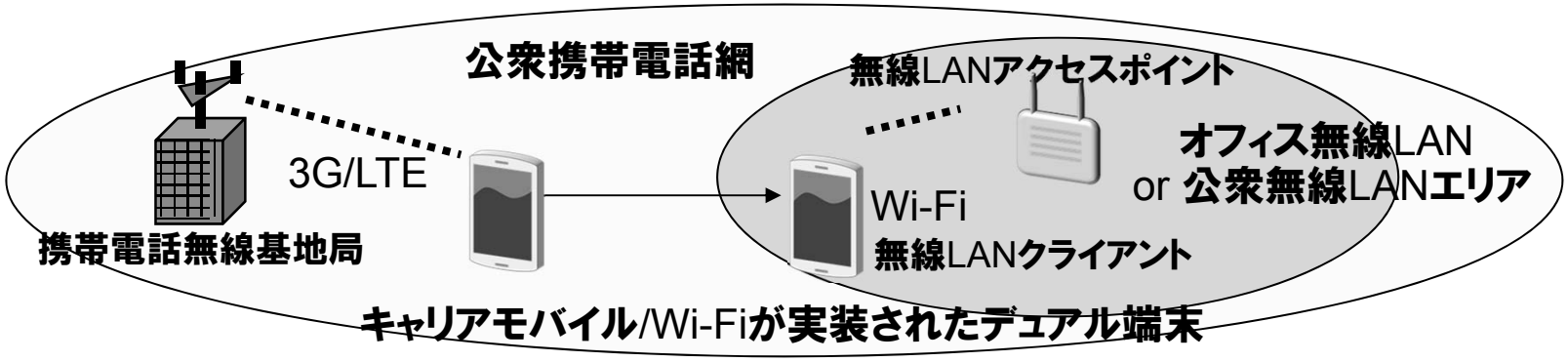
(5) モバイル端末

- **モバイル端末：携帯電話、PHS、スマートフォン、モバイルPC、PDAなどがある。携帯電話/PHSは、最も強度が高い基地局を選択しかつローミング可能な遠隔通信機能を有する。**
- **無線マルチモード端末：1つの無線モバイル端末で、異なるネットワークからのサービスが受けられるように複数の無線インターフェイス（無線周波数帯、多元（チャネル）アクセス方式、プロトコル）を実装する端末のこと。デュアル端末が代表的である。**

2つの無線インターフェイスを実装し、電波状況に応じて自動／手動で切り替えられる端末を、デュアル端末という。

無線LAN通信方式を兼ね備えた携帯電話やスマートフォンもデュアル端末と呼ぶ。オフィスや公衆無線LANエリアでは無線LANクライアントとして無線LANアクセスポイントと通信してイントラネットサービスや公衆無線LANサービスを利用し、その他では携帯電話やスマートフォンとして携帯電話無線基地局と通信して公衆携帯電話サービスを利用する。

IP電話機能を搭載し、無線LAN接続時に企業のIP-PBX(SIPサーバ)もしくはモバイルセントレックスに接続する内線IP電話機として動作するデュアル端末（デュアルフォン）もある

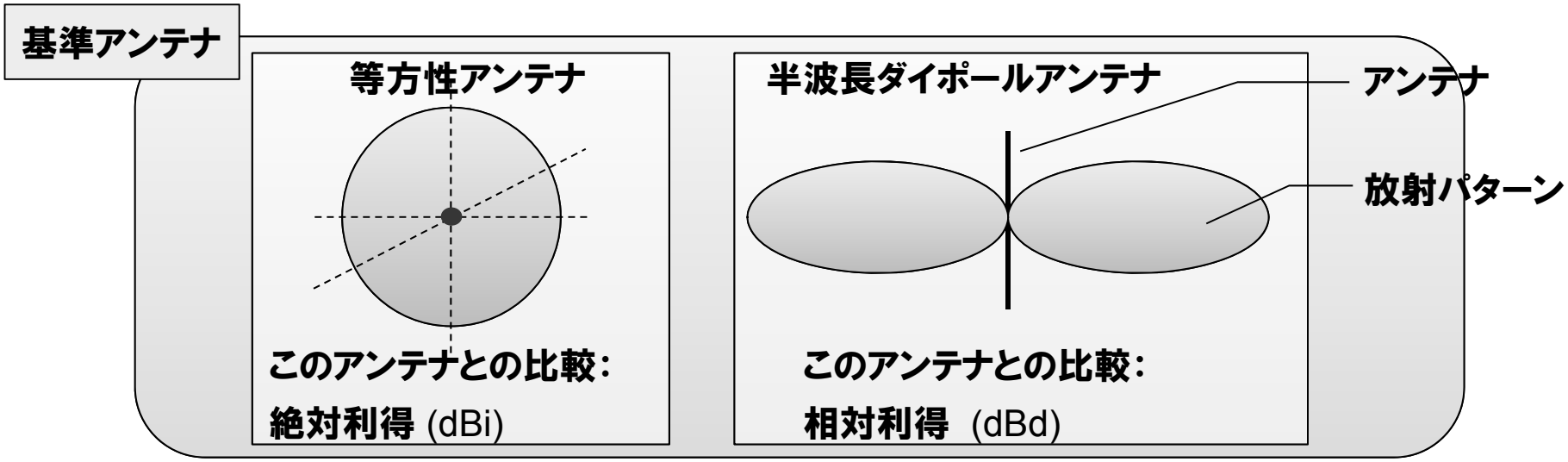


電波の伝搬特性

（３）アンテナの利得（ゲイン）

アンテナの「利得」は、基準アンテナと比較してどの程度の電力が放射されているかを表したものである。基準アンテナとしては、全方向に等しく電波が放射される「等方性アンテナ」、直線状のアンテナから放射される「半波長ダイポールアンテナ」の2種があり、それぞれのアンテナを基準とした送信電力を「絶対利得」「相対利得」と呼び、絶対利得：dBi, 相対利得：dBd で表す。

両者には、絶対利得＝ 相対利得 ＋ 2.15dB の関係がある。



EAP認証

認証方式	クライアント認証	サーバ認証	特徴
EAP-MD5 Message Digest Algorithm 5	ID/Password	なし	【方式概要】 ・標準方式(RFC2284)、一方向認証(クライアント認証のみ)方式 ・暗号化トンネルを作らずに、クライアントの秘密クレデンシャル(ユーザID/Password)のチャレンジレスポンス認証(MD5ハッシュ)にて、サーバがクライアントを認証、クライアントはサーバを認証しない。 【セキュリティ】 ・Key Derivationを実装しないためWEP Keyの定期的な生成・配布をしない、またMD5の脆弱性のため辞書攻撃等のリスクが大きく、かつサーバ認証もないので、セキュリティレベルは非常に低い。

認証方式	クライアント認証	サーバ認証	特徴
EAP-TLS	クライアント証明書	サーバ証明書	【方式概要】 ・標準方式(RFC2716)、双方向認証方式 ・クライアント認証/サーバ認証ともに証明書を利用する双方向認証を行う。 【セキュリティ】 ・Key Derivationを実装しWEP Keyを定期的に生成・配布する。また、クライアント側、サーバ側とも証明書による認証を利用するので、セキュリティレベルは非常に高い。 【導入の難易】 ・クライアント数が多い場合、証明書の運用・管理に手間・費用が必要。