無線LANセキュリティ要件の検討

無線LANセキュリティ要件SWG

2011年3月

本資料は、両面2in1で印刷されることを想定して、ページ数を調整しています。

目次

本検討の目的等

- 目的
  - 民間においては、無線LANを活用している事例が多くなってきている。また、無線LANの機能を内蔵したIT機器も増加している。一方、無線LANにおけるセキュリティ要件に関しては、十分に整理されていないと考える。そのため、無線LANを活用するユースケースに応じたセキュリティ要件を検討することにより、各省での効率的かつセキュアな情報システム環境の構築へ寄与したい。
- 前提:
  - 一般業務で使用するメール、文書、ウェブ閲覧等を行なう業務を前提としている。
  - 本検討では、現在、一般業務で利用されている有線LANのセキュリティ要件と同等のレベルを確保することを前提としている。
  - 本検討中では、無線LAN経由で共有する共有ファイルサーバの設置も視野に入れ、検討を行なった。ただし、共有ファイルサーバの設置は、必須ではなく。共有ファイルサーバの設置に関しては、必要性の検討やアクセスコントロール等を別途検討する必要があることに留意していただきたい。
- 検討のレベル:
  - 本検討結果で示す要件が、無線LANを構築する場合の必要十分な要件ではなく、複数のケースにおけるベストプラクティスを示している。

無線LAN導入のメリット

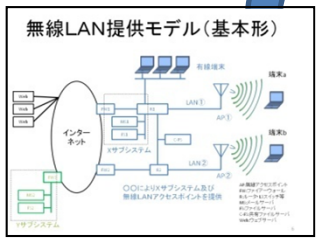
- モビリティの提供
  - レイアウト変更・組織変更に伴うネットワーク配線工事コストの削減
  - パソコンの移動を可能にすることにより、仕事を行なう場所の自由度の拡大による生産性向上
  - 会議室等でネットワーク接続によるデータ共有することによるペーパレスの実現
- 回線インフラの提供
  - 来訪者向けのインターネット接続回線としての提供
  - 有線LANの一部障害時におけるバックアップ回線としての活用
  - 効率的にLANを拡張する手段としての活用

資料のまとめ方

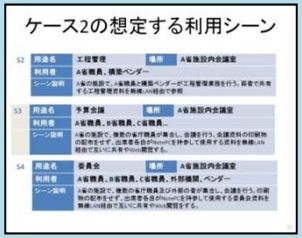
ケース分類に従って、各ケースごとに記述

ケース分類

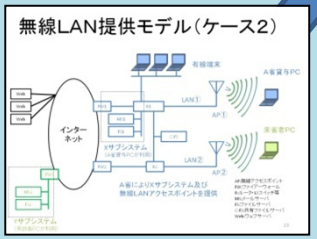
ケースの想定するシーンに応じて、無線LANの提供モデルを記述



無線LAN提供モデル（基本形）

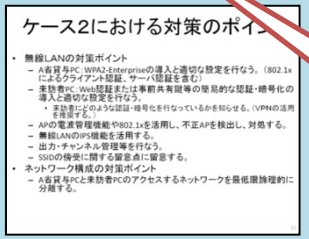


ケース〇の想定するシーン



無線LAN提供モデル（ケース〇）

ケース〇における対策のベストプラクティス



ケース〇における対策のポイント

脅威一覧

無線LAN提供モデルを前提として、脅威一覧の脅威に対する対策を脅威毎に記載

脅威毎に記述した対策をまとめて記述

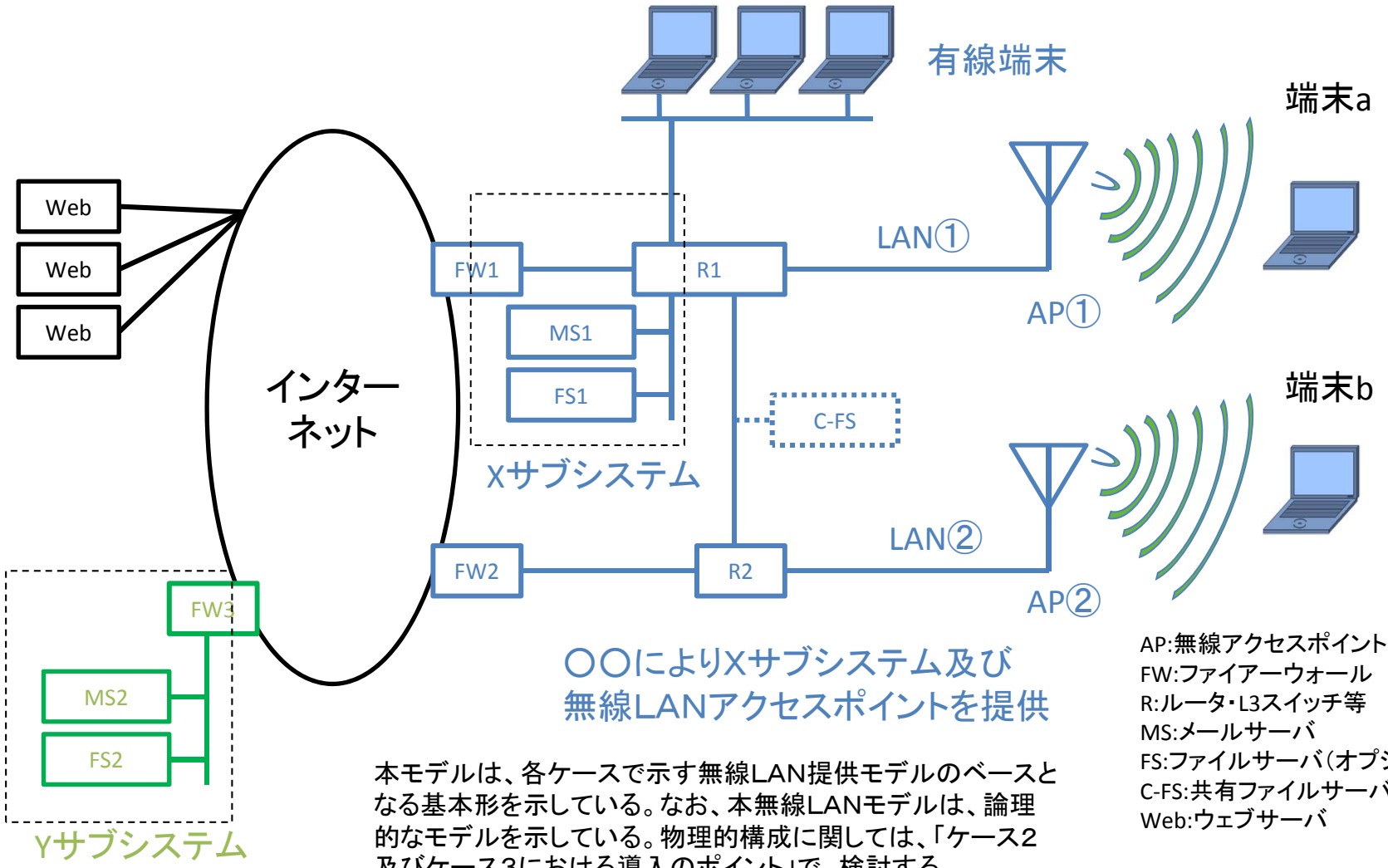
脅威一覧

無線LANを導入運用する場合に想定される脅威を一覧として整理した。脅威のカテゴリとして、機密性、可用性、完全性の視点からも分類した。

C.I.A	脅威	定義
機密性	ただのり	認証が無い状態で、許可されていないユーザが、無線LANネットワークを使用すること
	無線LANへの侵入	許可されていないユーザが不正に認証を行い、無線LANネットワークを使用すること。手法としてはBruteForceAttackやDictinaryAttackなどがある。
	通信内容の盗聴	他人の無線LAN通信を傍受し、内容を見ること
		他人が暗号化を施している通信を解読し、盗聴すること
機密性・可用性	不正AP*1への接続	不正APに接続したユーザのトラフィックデータを盗み見るために、不正にAPへ接続させること
	不正AP*1の設置	不正にAPを設置することで電波妨害を行うこと
可用性	電波干渉	無線LANサービス以外の同一周波数帯の電波を利用することで、電波干渉によるスループット低下・通信断を引き起こすこと
	Wi-Fi DoS	大量の802.11トラフィックを送信することで、サービス不能・低下状態にすること
完全性	無線トラフィックの改ざん	通信相手になりすまして改ざんした無線トラフィックを攻撃相手に対して見せること
N/A＊2	サブシステムへの侵入	無線LANの認証を完了後、ネットワークに本来アクセスのできない者が、サブシステム等へ侵入すること
N/A＊2	SSIDの傍受	電波の傍受によりSSID(ESSID)を把握すること

*1　不正AP：正規に設置されたアクセスポイント（AP）以外のAPを指す
*2　本来、無線LANの脅威ではないが、一般に議論されるポイントであるため記載。

無線LAN提供モデル（基本形）



本モデルは、各ケースで示す無線LAN提供モデルのベースとなる基本形を示している。なお、本無線LANモデルは、論理的なモデルを示している。物理的構成に関しては、「ケース2及びケース3における導入のポイント」で、検討する。

AP:無線アクセスポイント
FW:ファイアーウォール
R:ルータ・L3スイッチ等
MS:メールサーバ
FS:ファイルサーバ（オプション）
C-FS:共有ファイルサーバ
Web:ウェブサーバ

ケースの分類

無線LANに求められるセキュリティ要件をまとめるために、想定するA省の提供するサービス内容を基に、5つの想定されるケースに分類した。

ケース名	ケース概要	想定するA省の提供するサービス内容
ケース1	職員専用 利用型	•A省職員は、有線LAN環境と同じサービスをA省貸与PCを無線LAN環境に接続して利用する。 •来訪者には、無線LAN環境を利用させない。
ケース2	職員・来訪者 混在型	•A省職員は、有線LAN環境と同じサービスをA省貸与PCを無線LAN環境に接続して利用する。 •来訪者は、A省の無線LAN環境を経由して、インターネットのみへアクセスし、インターネット経由で、自らのシステム環境を利用する。 •A省職員及び来訪者で共有するデータを保存するファイルサーバを共有ファイルサーバとする。
ケース3	来訪者 提供型	•A省職員は、無線LAN環境を利用しない。 •来訪者は、A省の無線LAN環境を経由して、インターネットのみへアクセスし、インターネット経由で、自らのシステム環境を利用する。
ケース4	仮設型	•国際会議場や研修施設で一時的もしくは、仮設的に、A省職員は、A省貸与PCを無線LAN環境に接続し、インターネットへアクセスし、インターネット経由で、A省のシステム環境を利用する。
ケース5	ホットスポット 利用型	•A省職員は、A省貸与PCを、予め敷設されている第3者の提供する無線LAN環境に接続し、インターネットへアクセスし、インターネット経由で、A省のシステム環境を利用する。

白紙ページ

各ユースケースにおける対策の検討

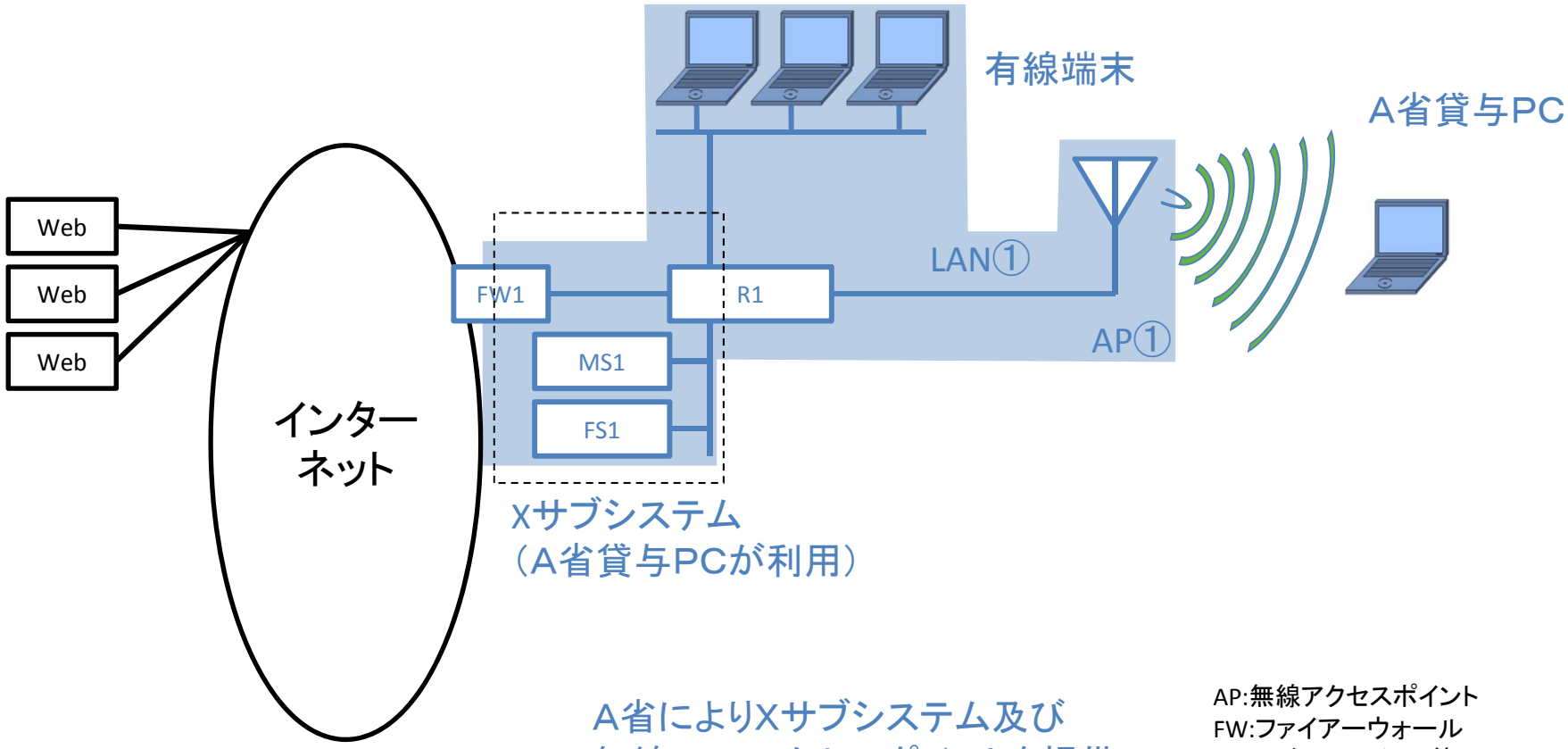
ケース1の想定する利用シーン

ケース名	ケース1	ケース概要	職員専用利用型
想定するA省の提供するサービス内容	•A省職員は、有線LAN環境と同じサービスをA省貸与PCを無線LAN環境に接続して利用する。 •来訪者には、無線LAN環境を利用させない。		

利用シーン

S1-1	用途名	通常業務利用	場所	A省施設内
	利用者	A省職員		
	シーン説明	A省の施設で、A省職員だけが無線LANを使用し、通常業務、省内会議を行う。ペーパーレス化の推進、引越時の工事の不要など、コスト削減に寄与する。		

無線LAN提供モデル（ケース1）



A省によりXサブシステム及び
無線LANアクセスポイントを提供

AP:無線アクセスポイント
FW:ファイアーウォール
R:ルータ・L3スイッチ等
MS:メールサーバ
FS:ファイルサーバ（オプション）
C-FS:共有ファイルサーバ
Web:ウェブサーバ

ケース1における対策のベストプラクティス

想定する脅威	脅威に対する対策
ただのり	802.1x（クライアント認証）の導入と適切な設定を行なう。
無線LANへの侵入	802.1x（クライアント認証）の導入と適切な設定を行なう。
通信の盗聴	WPA2-enterpriseの導入と適切な設定を行なう。
不正APへの接続	802.1x（サーバ認証）の導入と適切な設定を行なう。
不正APの設置	APの電波管理機能や802.1xを活用し、不正APを検出し、対処する。
電波干渉	出力・チャンネル管理等の電波管理を行なう。
Wi-FI DoS	無線LANのIPS機能を活用する
無線トラフィックの改ざん	WPA2-enterpriseの導入と適切な設定を行なう。
サブシステムへの侵入	想定しない。
SSIDの傍受	SSIDの傍受に関する留意点に留意する。

ケース1における対策のポイント

- 無線LANの対策ポイント
  - WPA2-enterpriseの導入と適切な設定を行なう。（802.1xによるクライアント認証、サーバ認証を含む）
  - APの電波管理機能や802.1xを活用し、不正APを検出し、対処する。
  - 無線LANのIPS機能を活用する。
  - 出力・チャンネル管理等を行なう。
  - SSIDの傍受に関する留意点に留意する。

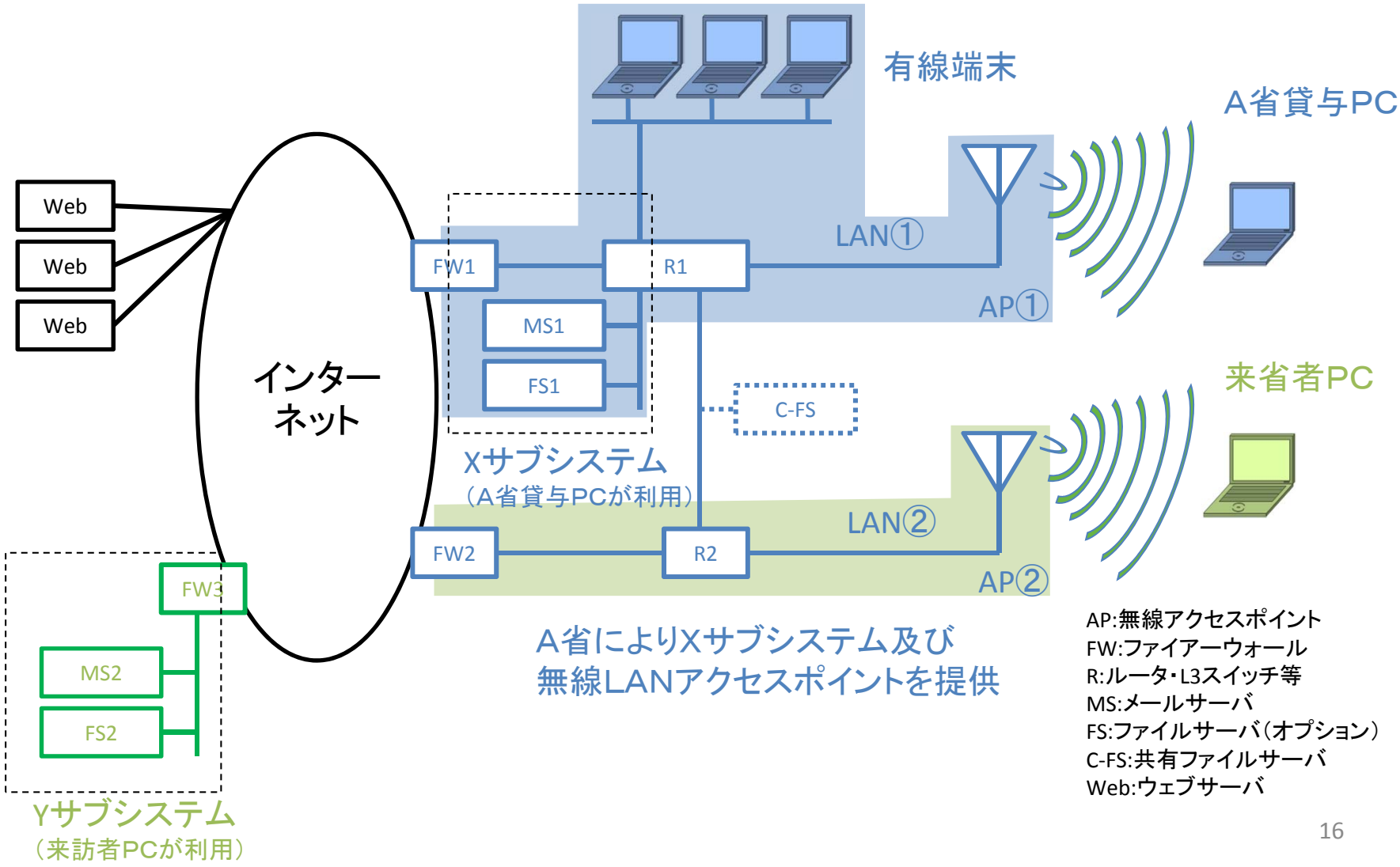
ケース2の想定する利用シーン

ケース名	ケース2	ケース概要	職員・来訪者混在型
想定するA省の提供するサービス内容	•A省職員は、有線LAN環境と同じサービスをA省貸与PCを無線LAN環境に接続して利用する。 •来訪者は、A省の無線LAN環境を経由して、インターネットのみへアクセスし、インターネット経由で、自らのシステム環境を利用する。 •A省職員及び来訪者で共有するデータを保存するファイルサーバを共有ファイルサーバとする。		

利用シーン

S2-1	用途名	工程管理 会議利用	場所	A省施設内会議室
	利用者	A省職員、システム構築ベンダー		
	シーン説明	A省内の施設で、A省職員とシステム構築ベンダーが工程管理の会議を行なう際に利用する。両者で共有する工程管理資料等を無線LAN経由で参照する。		
S2-2	用途名	他省庁との協議	場所	A省施設内会議室
	利用者	A省職員、B省職員、C省職員…		
	シーン説明	A省の施設で、複数の府省職員が集合し、会議を行う。会議資料の印刷物を配布せず、出席者各自が各省貸与PCを持参して無線LAN経由で、会議資料等を互いに共有したり、インターネット上のWebを閲覧する。		
S2-3	用途名	審議会・委員会利用	場所	A省施設内会議室
	利用者	A省職員、B省職員、C省職員、外部専門家、有識者		
	シーン説明	A省の施設で、複数の府省職員及び外部の専門家、有識者が集合し、審議会・委員会を行う。審議会・委員会の印刷物は、配布をせず、出席者各自がPCを持参して無線LAN経由で、会議資料等を互いに共有したり、インターネット上のWebを閲覧する。		

無線LAN提供モデル（ケース2）



AP:無線アクセスポイント
FW:ファイアーウォール
R:ルータ・L3スイッチ等
MS:メールサーバ
FS:ファイルサーバ（オプション）
C-FS:共有ファイルサーバ
Web:ウェブサーバ

ケース2における対策のベストプラクティス

想定する脅威	脅威に対する対策
ただのり	A省貸与PC：802.1x（クライアント認証）の導入と適切な設定を行なう。 来訪者PC：Web認証、または、事前共有鍵等の簡易的な認証の導入と適切な設定を行なう。
無線LANへの侵入	A省貸与PC：802.1x（クライアント認証）の導入と適切な設定を行なう。 来訪者PC：Web認証、または、事前共有鍵等の簡易的な認証の導入と適切な設定を行なう。
通信の盗聴	A省貸与PC：WPA2-enterpriseの導入と適切な設定を行なう。 来訪者PC：対応しない、または、事前共有鍵等の簡易的な暗号化の導入と適切な設定を行なう。 来訪者にどのような認証・暗号化を行なっているか知らせる。（VPNの活用を推奨する）
不正APへの接続	A省貸与PC：802.1x（サーバ認証）の導入と適切な設定を行なう。 来訪者PC：対応しない、または、事前共有鍵等の簡易的な認証の導入と適切な設定を行なう。 来訪者にどのような認証・暗号化を行なっているか知らせる。（VPNの活用を推奨する）
不正APの設置	APの電波管理機能や802.1xを活用し、不正APを検出し、対処する。
電波干渉	出力・チャンネル管理等の電波管理を行なう。
Wi-FI DoS	無線LANのIPS機能を活用する。
無線トラフィックの改ざん	A省貸与PC：WPA2-enterpriseの導入と適切な設定を行なう。 来訪者PC：対応しないまたは事前共有鍵等の簡易的な暗号化の導入と適切な設定を行なう。 来訪者にどのような認証・暗号化を行なっているか知らせる。（VPNの活用を推奨する）
サブシステムへの侵入	R1及びR2でLAN①とLAN②を分離する。
SSIDの傍受	SSIDの傍受に関する留意点に留意する。

ケース2における対策のポイント

- 無線LANの対策ポイント
  - A省貸与PC：WPA2-Enterpriseの導入と適切な設定を行なう。（802.1xによるクライアント認証、サーバ認証を含む）
  - 来訪者PC：Web認証または事前共有鍵等の簡易的な認証・暗号化の導入と適切な設定を行なう。
    - 来訪者にどのような認証・暗号化を行なっているかを知らせる。（VPNの活用を推奨する。）
  - APの電波管理機能や802.1xを活用し、不正APを検出し、対処する。
  - 無線LANのIPS機能を活用する。
  - 出力・チャンネル管理等を行なう。
  - SSIDの傍受に関する留意点に留意する。
- ネットワーク構成の対策ポイント
  - A省貸与PCと来訪者PCのアクセスするネットワークを最低限論理的に分離する。

ケース3の想定する利用シーン

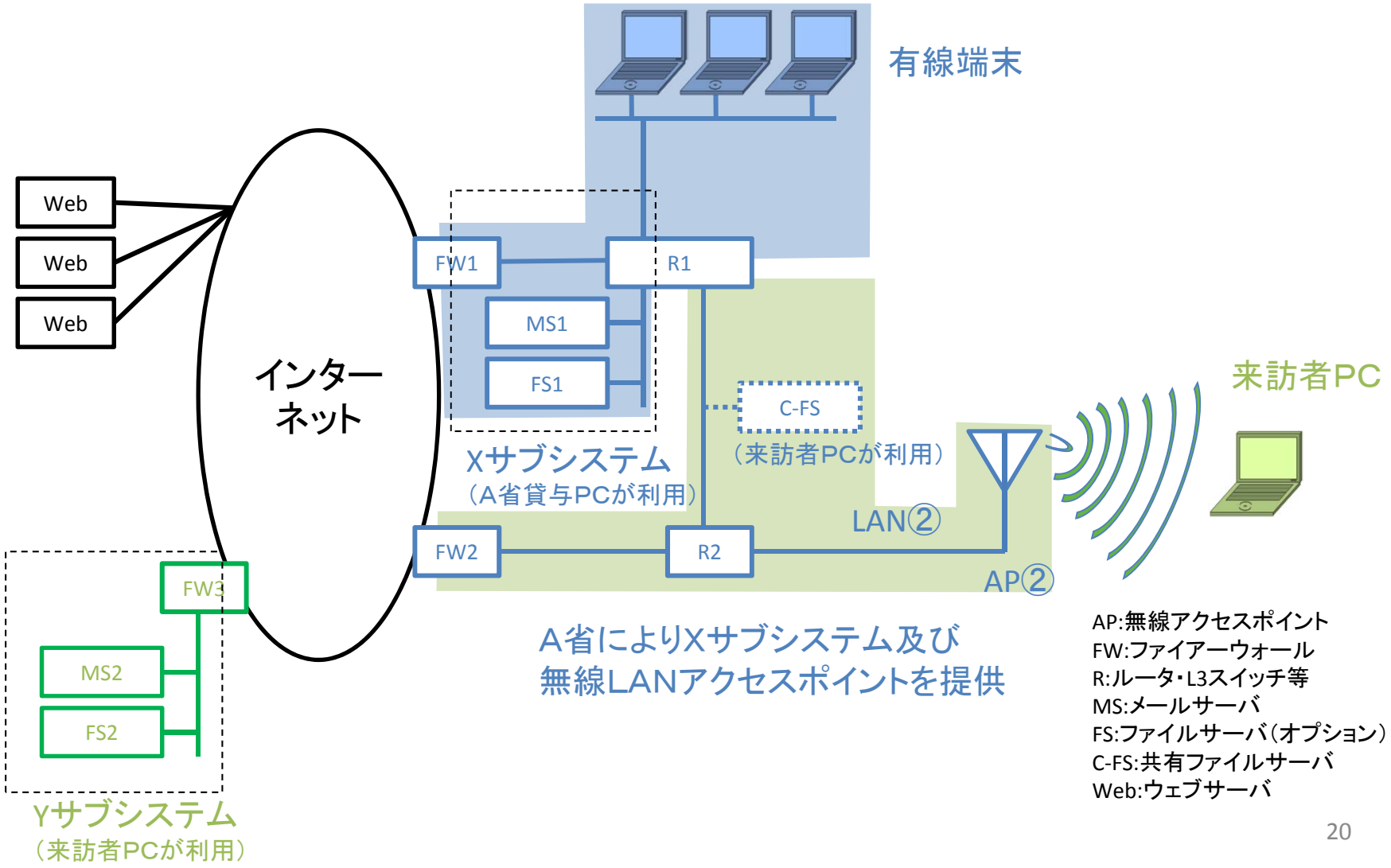
ケース名	ケース3	ケース概要	来訪者提供型
想定するA省の提供するサービス内容	•A省職員は、無線LAN環境を利用しない。 •来訪者は、A省の無線LAN環境を経由して、インターネットのみへアクセスし、インターネット経由で、自らのシステム環境を利用する。		

利用シーン

S3-1

用途名	ゲストアクセス	場所	A省施設内
利用者	来訪者（B省職員、外部機関、ベンダー）		
シーン説明	A省の施設で、A省職員以外の外部の来訪者へ無線LANを経由し、インターネットアクセスサービスを提供する。これにより外部の者は、インターネットを経由し、所属のシステムへ接続して業務をすることができる。		

無線LAN提供モデル（ケース3）



AP:無線アクセスポイント
FW:ファイアーウォール
R:ルータ・L3スイッチ等
MS:メールサーバ
FS:ファイルサーバ（オプション）
C-FS:共有ファイルサーバ
Web:ウェブサーバ

ケース3における対策のベストプラクティス

想定する脅威	脅威に対する対策
ただのり	Web認証、または、事前共有鍵等の簡易的な認証の導入と適切な設定を行なう。
無線LANへの侵入	Web認証、または、事前共有鍵等の簡易的な認証の導入と適切な設定を行なう。
通信の盗聴	対応しない、または、事前共有鍵等の簡易的な暗号化の導入と適切な設定を行なう。 来訪者にどのような認証・暗号化を行なっているか知らせる。(VPNの活用を推奨する)
不正APへの接続	対応しない、または、事前共有鍵等の簡易的な認証の導入と適切な設定を行なう。 来訪者にどのような認証・暗号化を行なっているか知らせる。(VPNの活用を推奨する)
不正APの設置	APの電波管理機能や802.1xを活用し、不正APを検出し、対処する。
電波干渉	出力・チャンネル管理等の電波管理を行なう。
Wi-FI DoS	無線LANのIPS機能を活用する。
無線トラフィックの改ざん	対応しない、または、事前共有鍵等の簡易的な暗号化の導入と適切な設定を行なう。 来訪者にどのような認証・暗号化を行なっているか知らせる。(VPNの活用を推奨する)
サブシステムへの侵入	R1でXサブシステムをLAN①やLAN②から分離する。
SSIDの傍受	SSIDの傍受に関する留意点に留意する。

ケース3における対策のポイント

- 無線LANの対策ポイント
  - Web認証または事前共有鍵等の簡易的な認証・暗号化の導入と適切な設定を行なう。
    - 来訪者にどのような認証・暗号化を行なっているかを知らせる。（VPNの活用を推奨する。）
  - APの電波管理機能や802.1xを活用し、不正APを検出し、対処する。
  - 無線LANのIPS機能を活用する。
  - 出力・チャンネル管理等を行なう。
  - SSIDの某中に関する留意点に留意する。
- ネットワーク構成のポイント
  - Xサブシステムと来訪者PCのアクセスするネットワークを最低限論理的に分離する。

ケース4の想定する利用シーン

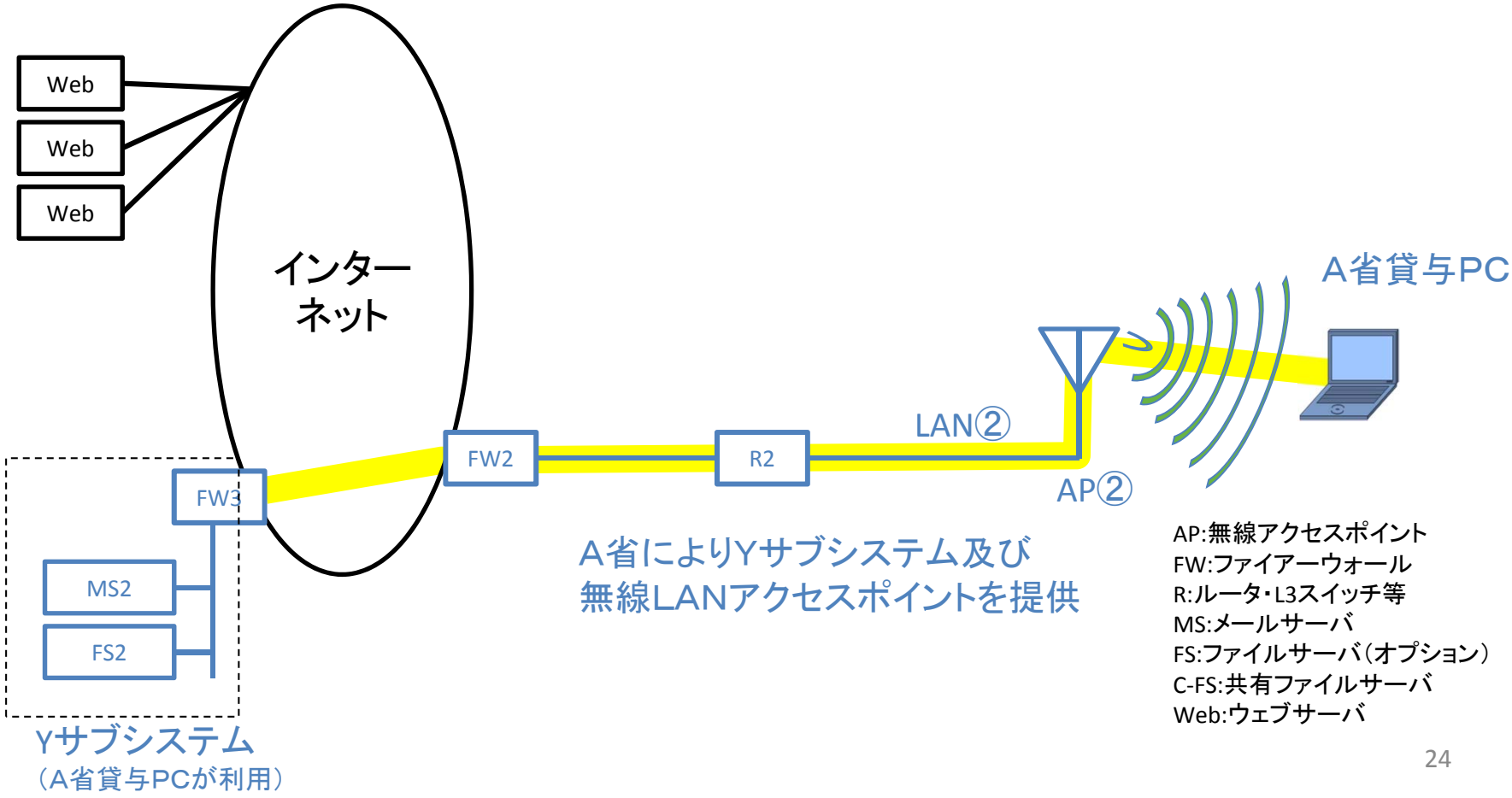
ケース名	ケース4	ケース概要	仮設型
想定するA省の提供するサービス内容	•国際会議場や研修施設で一時的もしくは、仮設的に、A省職員は、A省貸与PCを無線LAN環境に接続し、インターネットへアクセスし、インターネット経由で、A省のシステム環境を利用する。		

利用シーン

S4-1

用途名	省外施設での会議や研修施設での利用（無線LANのみ自前構築）	場所	他省庁施設、民間施設
利用者	A省職員		
シーン説明	A省外の施設を利用して、会議や研修を行う。このとき、構内LANは施設の既存設備を利用し、無線LAN環境は独自に敷設する。 A省職員は、無線LANを経由し、VPN接続でA省のシステムにアクセスして業務を行う。		

無線LAN提供モデル（ケース4）



ケース4における対策のベストプラクティス

想定する脅威	脅威に対する対策
ただのり	Web認証または事前共有鍵等の簡易的な認証の導入と適切な設定を行なう。 ただし、FW3とA省貸与PC間でVPN接続が必要である。 WPA2-Enterprise(AES-CCMP)の導入と適切な設定で対策を行なうことも可能である。
無線LANへの侵入	Web認証または事前共有鍵等の簡易的な認証の導入と適切な設定を行なう。 ただし、FW3とA省貸与PC間でVPN接続が必要である。 WPA2-Enterprise(AES-CCMP)の導入と適切な設定で対策を行なうことも可能である。
通信の盗聴	対応しない、または、事前共有鍵等の簡易的な暗号の導入と適切な設定を行なう。 ただし、FW3とA省貸与PC間でVPN接続が必要である。 WPA2-Enterprise(AES-CCMP)の導入と適切な設定で対策を行なうことも可能である。
不正APへの接続	対応しない、または、事前共有鍵等の簡易的な認証の導入と適切な設定を行なう。 ただし、FW3とA省貸与PC間でVPN接続が必要である。 WPA2-Enterprise(AES-CCMP)の導入と適切な設定で対策を行なうことも可能である。
不正APの設置	APの電波管理機能や802.1xを活用し、不正APを検出し、対処する。
電波干渉	出力・チャンネル管理等の電波管理を行なう。
Wi-FI DoS	無線LANのIPS機能を活用する。
無線トラフィックの改ざん	対応しない、または、事前共有鍵等の簡易的な認証の導入と適切な設定を行なう。 ただし、FW3とA省貸与PC間でVPN接続が必要である。 WPA2-Enterprise(AES-CCMP)の導入と適切な設定で対策を行なうことも可能である。
サブシステムへの侵入	FW3とA省貸与PC間でVPN接続を行なう。
SSIDの傍受	SSIDの傍受に関する留意点に留意する。

ケース4では、LAN②の部分を一時的もしくは、仮設として利用する場合を想定し、対策を検討した。LAN②の部分を恒久的もしくは、本格的に設置する場合は、ケース1のモデルを基に検討していただきたい。

ケース4における対策のポイント

- 無線LANの対策ポイント
  - Web認証または事前共有鍵等の簡易的な認証・暗号化の導入と適切な設定を行なう。
    - ただし、FW3とA省貸与PC間でVPN接続が必要である。
    - WPA2-Enterprise(AES-CCMP)の導入と適切な設定で対策を行なうことも可能である。
  - APの電波管理機能や802.1xを活用し、不正APを検出し、対処する。
  - 無線LANのIPS機能を活用する。
  - 出力・チャンネル管理等を行なう。
  - SSIDの某中に関する留意点に留意する。
- ネットワーク構成の対策ポイント
  - Yサブシステムと A省貸与PC間でVPN接続を行なう。

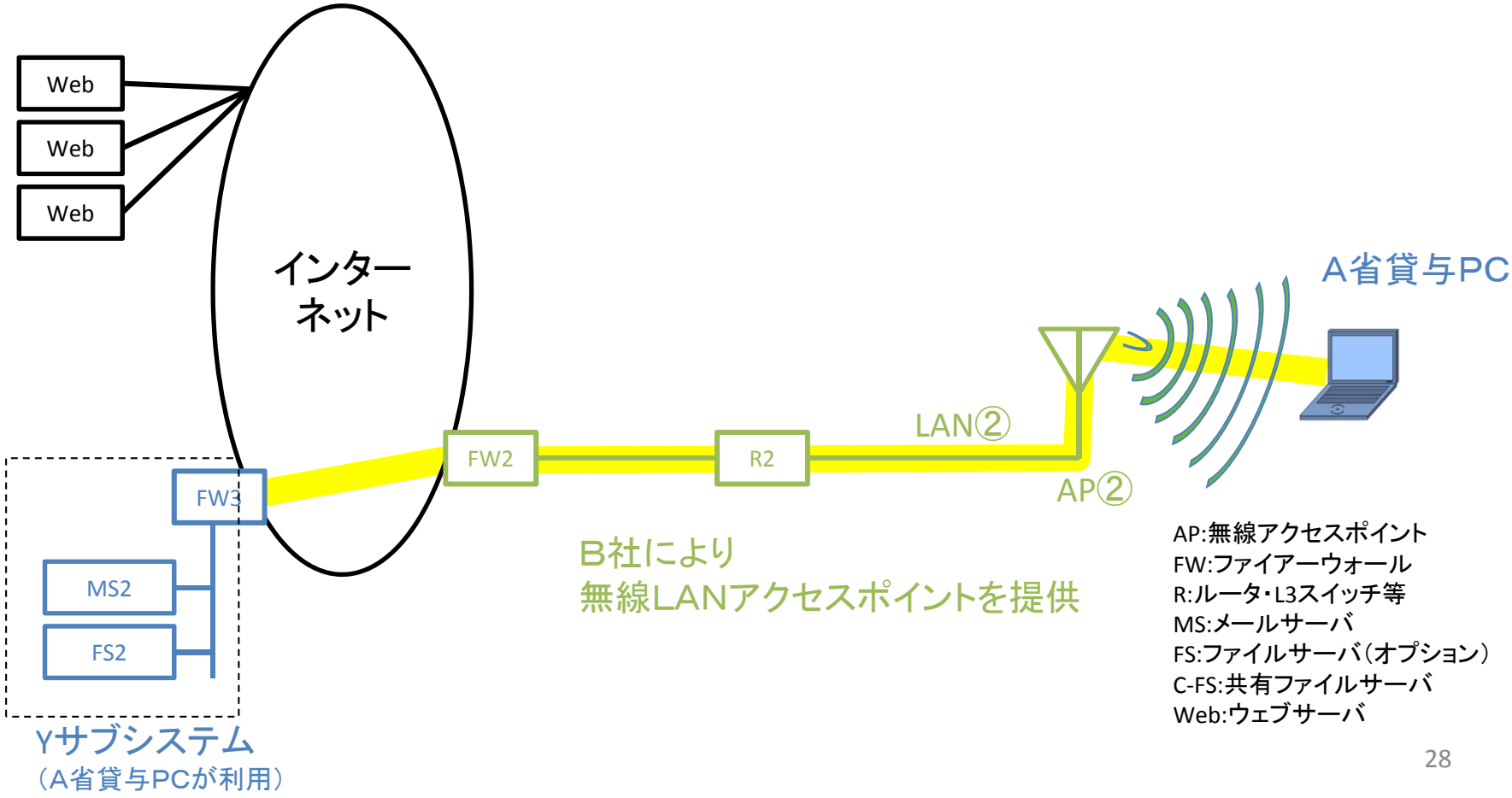
ケース5の想定する利用シーン

ケース名	ケース5	ケース概要	ホットスポット利用型
想定するA省の提供するサービス内容	•A省職員は、A省貸与PCを、予め敷設されている第3者の提供する無線LAN環境に接続し、インターネットへアクセスし、インターネット経由で、A省のシステム環境を利用する。		

利用シーン

S5-1	用途名	省外施設での会議、研修利用（自前設備無し＝ホットスポット）	場所	他省庁施設、民間施設
	利用者	A省職員		
	利用シーン説明	A省外の施設を利用して、会議や研修を行なう。このとき、無線LANは施設の既存設備を利用する。A省職員は、無線LANを経由し、VPN接続でA省のシステムにアクセスして業務を行う。		

無線LAN提供モデル（ケース5）



AP:無線アクセスポイント
FW:ファイアーウォール
R:ルータ・L3スイッチ等
MS:メールサーバ
FS:ファイルサーバ（オプション）
C-FS:共有ファイルサーバ
Web:ウェブサーバ

ケース5における対策のベストプラクティス

想定する脅威	脅威に対する対策
ただのり	FW3とA省貸与PC間でVPN接続を行う。 （B社の提供する認証・暗号化を適切に設定する。）*1
無線LANへの侵入	FW3とA省貸与PC間でVPN接続を行う。 （B社の提供する認証・暗号化を適切に設定する。）*1
通信の盗聴	FW3とA省貸与PC間でVPN接続を行う。 （B社の提供する認証・暗号化を適切に設定する。）*1
不正APへの接続	FW3とA省貸与PC間でVPN接続を行う。 （B社の提供する認証・暗号化を適切に設定する。）*1 不正APからの攻撃を想定して、A省貸与PCへのパーソナルFWやアンチウイルスソフトウェアの導入が必要である。
不正APの設置	可用性が必要な場合、B社の対応を確認する
電波干渉	可用性が必要な場合、B社の対応を確認する
Wi-FI DoS	可用性が必要な場合、B社の対応を確認する
無線トラフィックの改ざん	FW3とA省貸与PC間でVPN接続を行う。 （B社の提供する認証・暗号化を適切に設定する。）*1
サブシステムへの侵入	FW3とA省貸与PC間でVPN接続を行う。
SSIDの傍受	可用性が必要な場合、B社の対応を確認する

*1 B社のサービスに依存します。

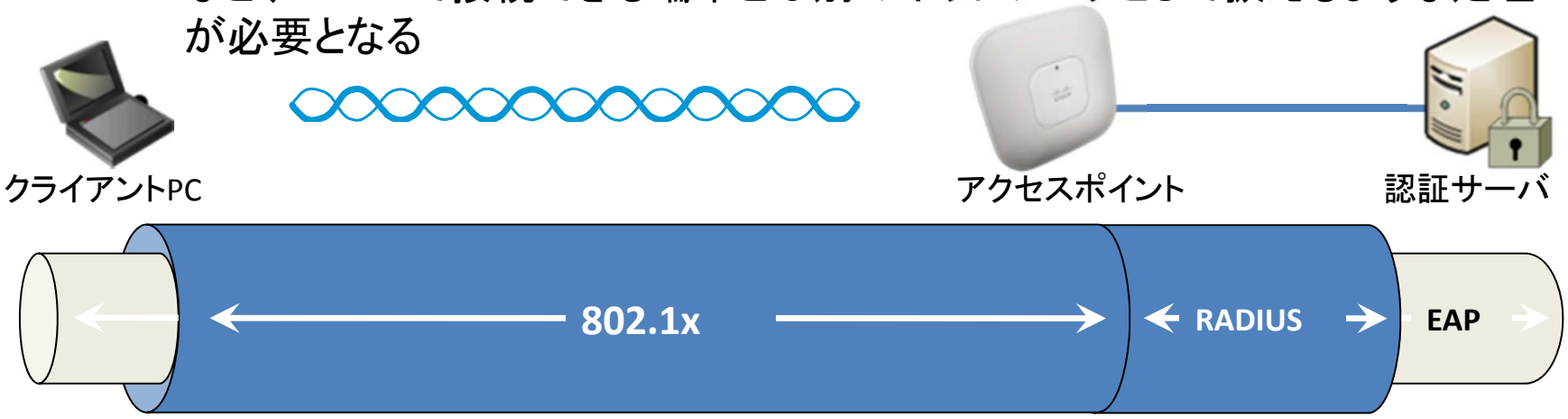
ケース5における対策のポイント

- 無線LANの対策ポイント
  - FW3とA省貸与PC間でVPN接続を行う。
    - ただし、B社の提供する認証・暗号化を適切に設定する。
  - 不正APからの攻撃を想定して、A省貸与PCへのパーソナルFWやアンチウイルスソフトウェアの導入が必要である。
  - 可用性が必要な場合、以下のB社による対策を確認する。
    - 不正APの設置への対応
    - 電波干渉への対応
    - Wi-Fi DoSへの対応
    - SSIDの傍受への対応
- ネットワーク構成の対策ポイント
  - Yサブシステムと A省貸与PC間でVPN接続を行う。

対策解説

対策解説：802.1Xの導入と適切な設定

- IEEE 802.1Xの導入と適切な設定を行なう。
  - ネットワーク認証の規格。有線でも用いられる
  - 実際に認証を行うための認証情報はEAPを利用する。
  - 具体的なEAPの種類として、PEAP/EAP-FAST/EAP-TLSの中から選定することが望ましい
  - 各手法のクレデンシャル(認証資格情報)の運用方法については、有線と同等のポリシーを使う
  - 802.1Xを利用できない端末についてはアクセスできるセグメントを制限するなど、802.1Xで接続できる端末とは別のネットワークとして扱えるような処理が必要となる



対策解説：WPA2-Enterpriseの導入と設定

- WPA2-Enterpriseの導入と適切な設定を行なう。
  - WPA2-Enterpriseを使用し、暗号アルゴリズムにはAES-CCMPを利用する
  - Radiusサーバが用意できない、もしくは用意しないような暫定的な用途としてはWPA2-Personal のAES-CCMPも利用可能だが、事前共有鍵方式となるので鍵の使用方法には注意を払うこと(長期の同一鍵による運用はしないなど)

暗号化方式	概要	推奨利用方法
WEP	古いデバイスにも実装されていることが多いが、高速な解読手法が広く知られている	基本的には推奨しない。WEPしか利用できない端末があったときに、解読されることを前提として利用する
WPA2-Personal (AES-CCMP)	AESとキーローテーションにより強固なセキュリティとなっている。PersonalではPSK(事前共有鍵)を使うため他のユーザとも同じ事前共有鍵を使うことになる。Personalでは認証としての機能もまかなうためこの点は注意がいる	利用者で共通の鍵を使うことが許容されるかどうかで判断する。一般には家庭用とや一時的な利用などに有効とされる
WPA2-Enterprise (AES-CCMP)	Personalと同様だが、暗号化鍵の提供を802.1X認証で得る。そのため無線インフラとしては各ユーザを識別したうえでのアクセス提供が行われる。	802.1X認証にともない暗号鍵が提供されるため、安全性・拡張性で企業などの組織で広く利用される。

対策解説：簡易的な認証・暗号化の導入と設定

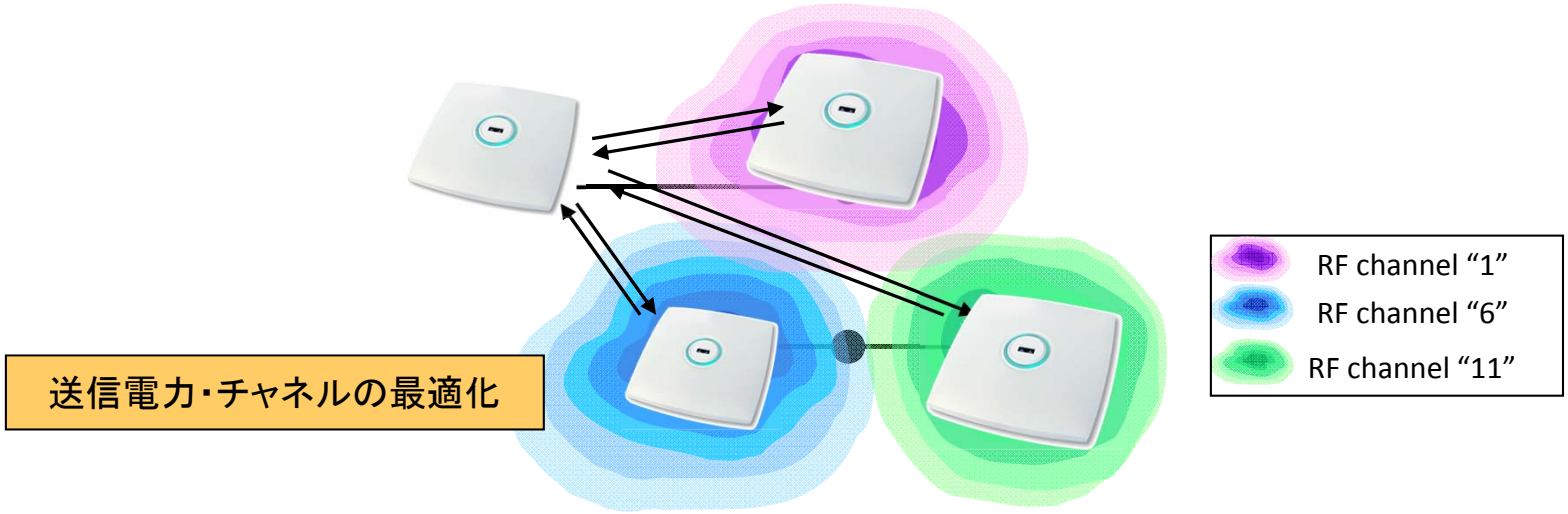
- Web認証または事前共有鍵(例えばWEP/WPA2 Personal)等の簡易的な認証の導入と適切な設定を行なう。
  - WPA2-Personalを使用する場合は、暗号アルゴリズムには、AES-CCMPを利用する
  - 来訪者が使う端末は何がつながってくるか予測できないためWebブラウザを利用した認証を用いる。
  - 事前共有鍵の場合はその構造上ユーザを識別することができないため、サービス提供者はその点に留意し、サービスの提供を行う

(事前共有鍵の場合、パスフレーズが漏えいした場合の影響範囲が広い)

暗号化方式	概要	推奨利用方法
Web認証	Webブラウザにクレデンシャルを入力することで通信可能となる方式。Web認証によるネットワーク接続自体は標準化されていないため他の方式が選択できる場合はそちらが推奨される。また、Web認証する場合は認証が通らない限り無線クライアントが他のクライアントと通信できない仕組みであることが求められる	ゲストユーザなどアクセスに利用する端末が明確でない場合に利用される。
WEP/WPA2-Personal	事前共有鍵による認証となるため、個人の識別ができない。また、各ユーザで共有しているため鍵の変更などをした場合の影響範囲が広く限定的な用途に向いている	一般には家庭用とや一時的な利用などに有効とされる

対策解説：出力・チャンネル管理等電波管理

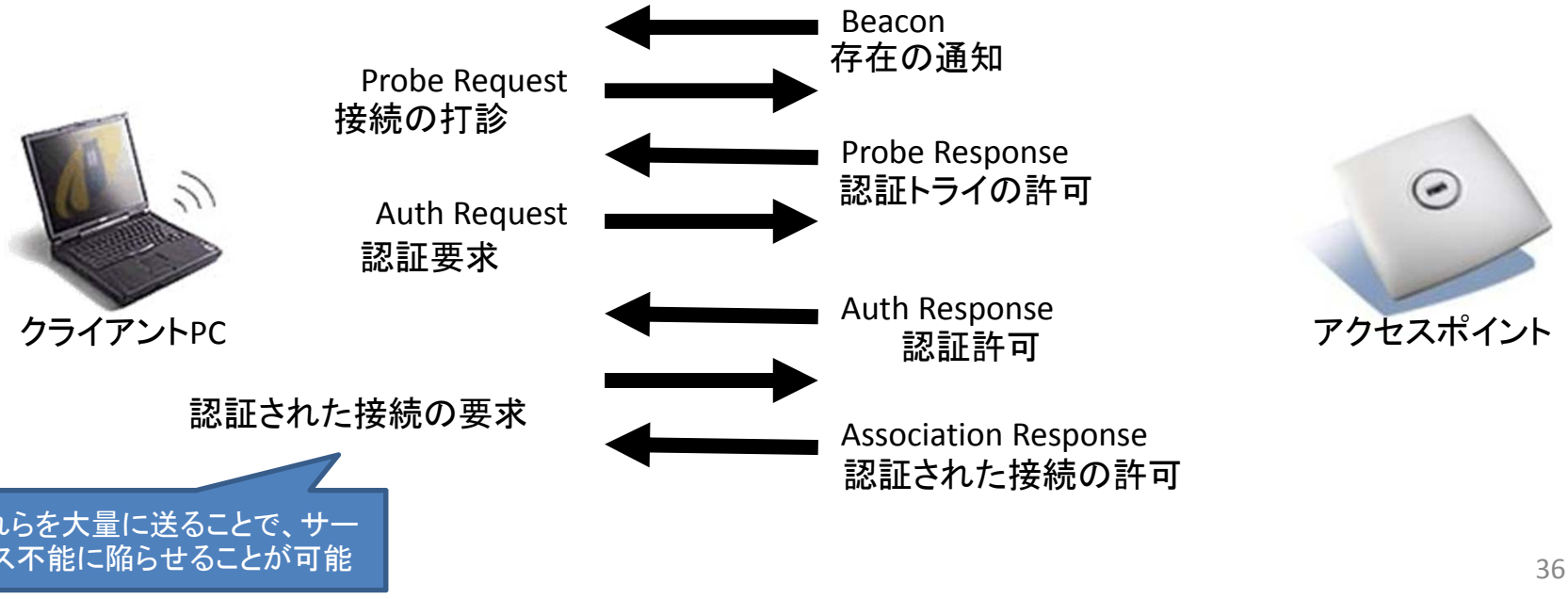
- 出力・チャンネル管理等の電波管理を行なう。
  - 無線LANでは同一周波数帯での通信はフレームの衝突が起きるため原理上いかなる仕組みを講じても同一周波数帯で通信が起きないようチャネル(周波数帯の帯域)を変更するか出力の調整を行い衝突を抑止する機構が必須となる
  - 電波環境は常に変動することを前提とする。そのため、サービス利用不能とならないように可用性向上を目的とし、チャネルの変更・出力の変更が行われる機能を用いる
  - 調整方法については手動で定期的(数十分程度間隔)に変更することは現実的ではないため自動で一定間隔で調整できる機能を用いる



対策解説：無線LANのIPS機能

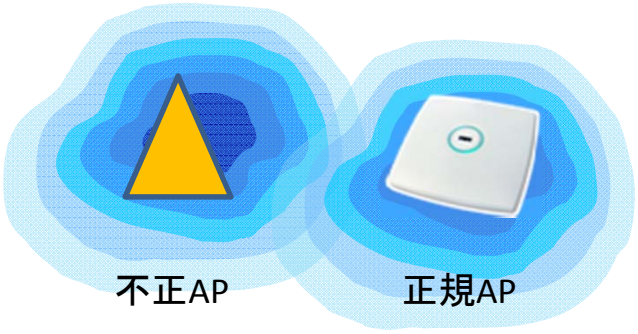
- 無線LANのIPS機能を活用する。
  - 802.11 マネージメントフレームなど(接続要求など) を繰り返し投げつけることでAPをサービス不能状態にする攻撃が存在するため、一定のボリュームのマネージメントフレームを受け取った際に一定時間その端末からの接続要求は処理せずにすべてブロックするような仕組みを持つこと

※IPS機能という名称でなくとも上記のような機構を持つことをここでは便宜上IPS機能と呼んでいる

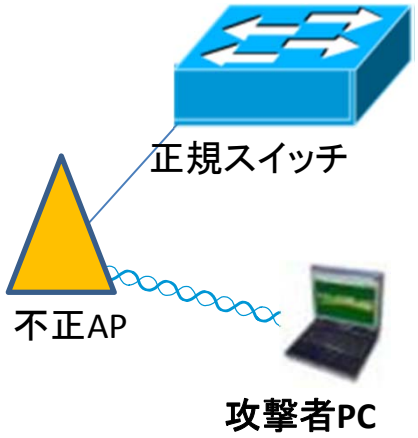


対策解説：APや802.1xによる不正AP検出①

- 定義は一般にさまざまだがここでは「自組織において正規に認可されていないAP」とする
- 不正APにもさまざまなタイプが存在する
  - 内部ネットワークに接続している不正AP(主に組織内の人が勝手に設定する例)
  - 組織内のユーザに接続させ情報を抜き取ることを目的におかれた不正AP(悪意のあるAP設置など)
- 不正APは以下のような問題を引き起こす可能性がある
  - 干渉源となる(可用性の低下)
  - 内部ネットワークに対するバックドアとなる(機密性の低下)



干渉源となる



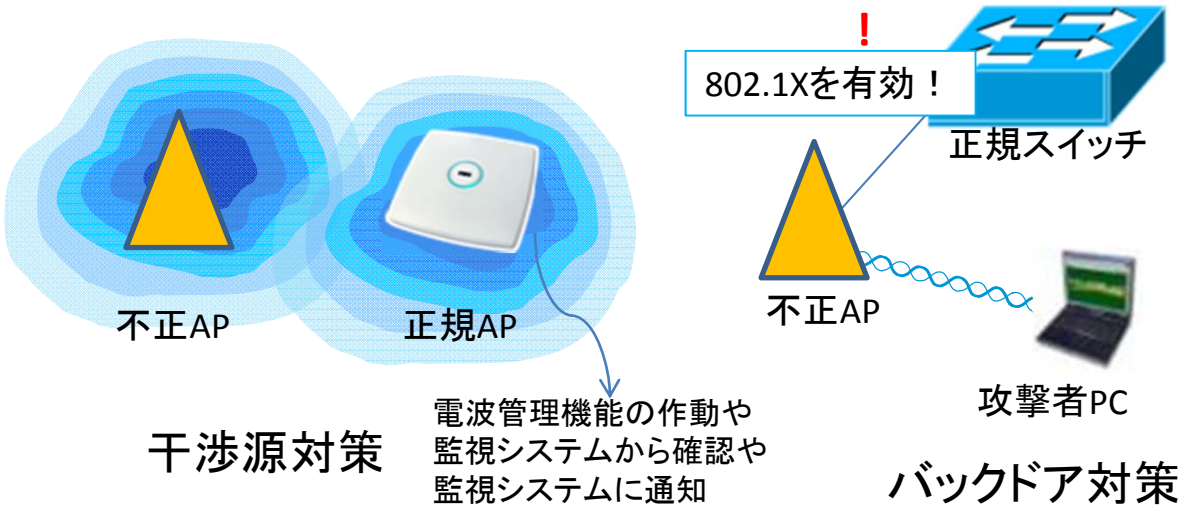
バックドアになる

対策解説：APや802.1xによる不正AP検出②

- APの電波管理機能や802.1xを活用し、不正APを検出し、対処する。
  - 対・干渉源

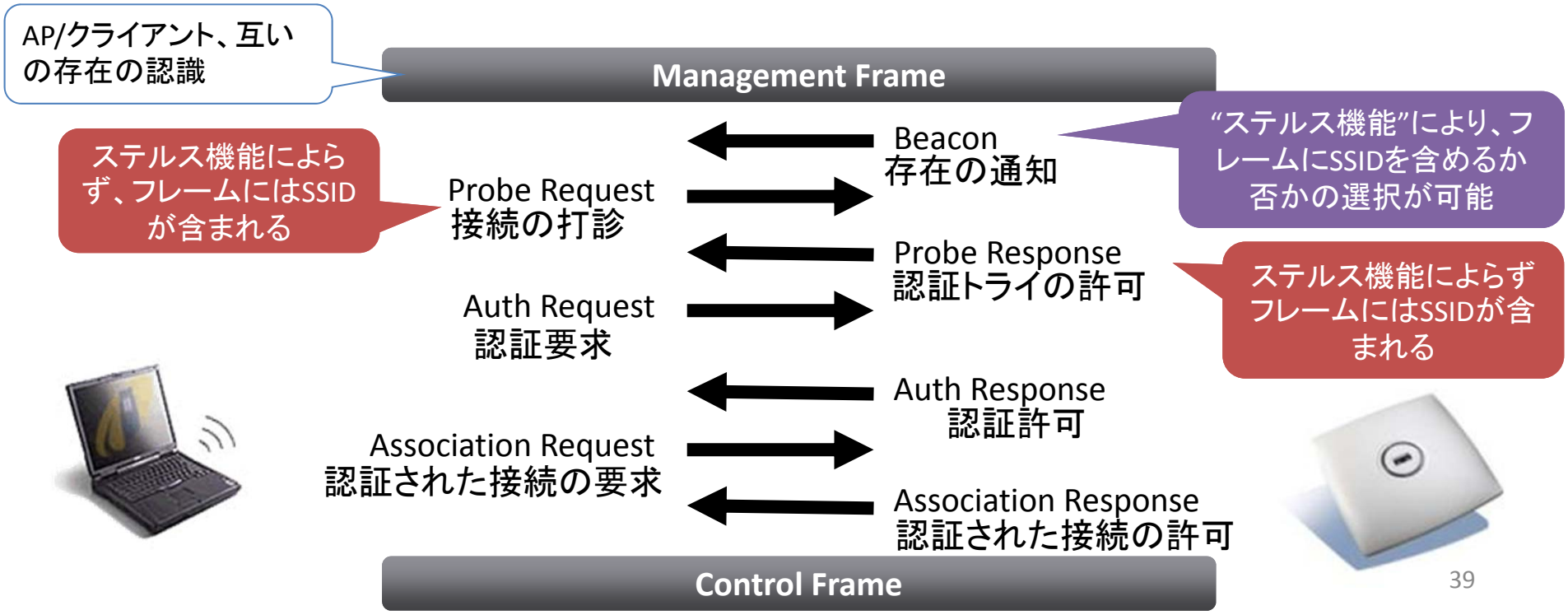
    APの機能で、電波的に検知し、不正APの存在を検知する。撤去するなど対処を行う
  - 対・内部ネットワークに対するバックドア

    有線側で802.1X認証を行い、正規のAP以外は接続できないようにする(APが802.1X
    サプリカント機能を持つことが必要)



対策解説：SSID傍受に関する留意点

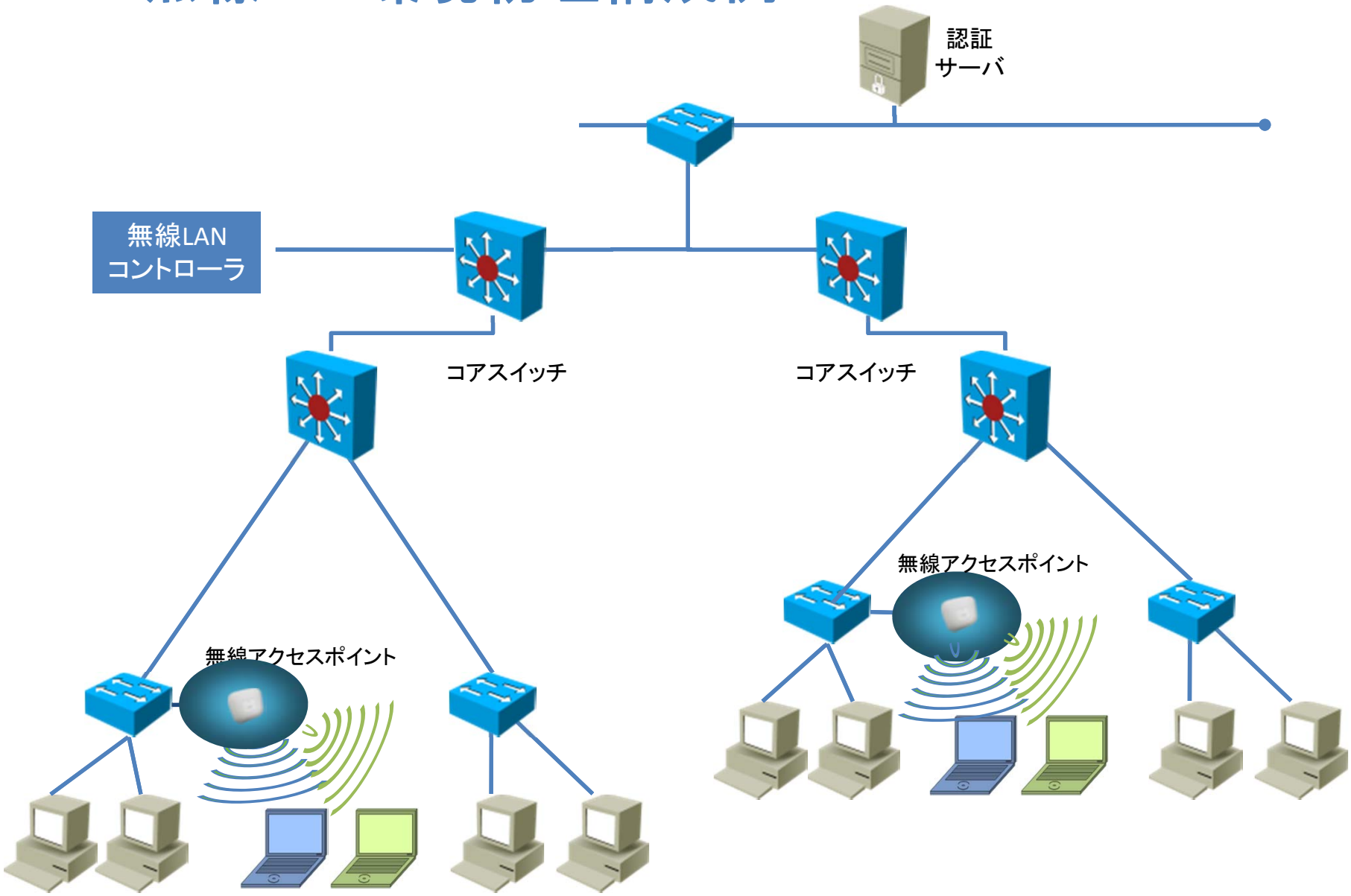
- SSIDの傍受に関する留意点
  - SSIDの情報については接続要求パケットであるAssociation Requestなどに含まれているため、事実上セキュリティの機能は果たしていない
  - このため、一般に言われるステルス機能(ProbeパケットにSSIDを含めない機能)は大きな効果を持たない。逆にシステムによっては接続性を低下させることもあるためステルス機能を具備することは問題ないが使用を必須とはしない



無線LAN環境の構築に必要な機器等

- **無線アクセスポイント（AP）**
  - 無線LANコントローラの指示に従い、PCと無線による通信を行ないネットワークに接続する
- **無線LANコントローラ**
  - APを集中管理し、設定・電波調整などを行う
  - APと連携し、以下の機能を具体的には提供する
    - WPA2-Enterprise(AES-CCMP), WPA2-Personal(AES-CCMP)の認証・暗号化機能
    - 802.1X(EAP-TLS/PEAP/EAP-FAST)などによるPC等の認証機能
    - 自動電波出力調整及びチャネル調節などの電波管理機能
    - 電波管理機能を活用した不正APの検出機能
    - Wifi-DoS対策機能
- **認証サーバ**
  - Web認証、WPA2-Enterprise等におけるPC等の認証を行なう

無線LAN環境物理構成例



白紙ページ

白紙ページ

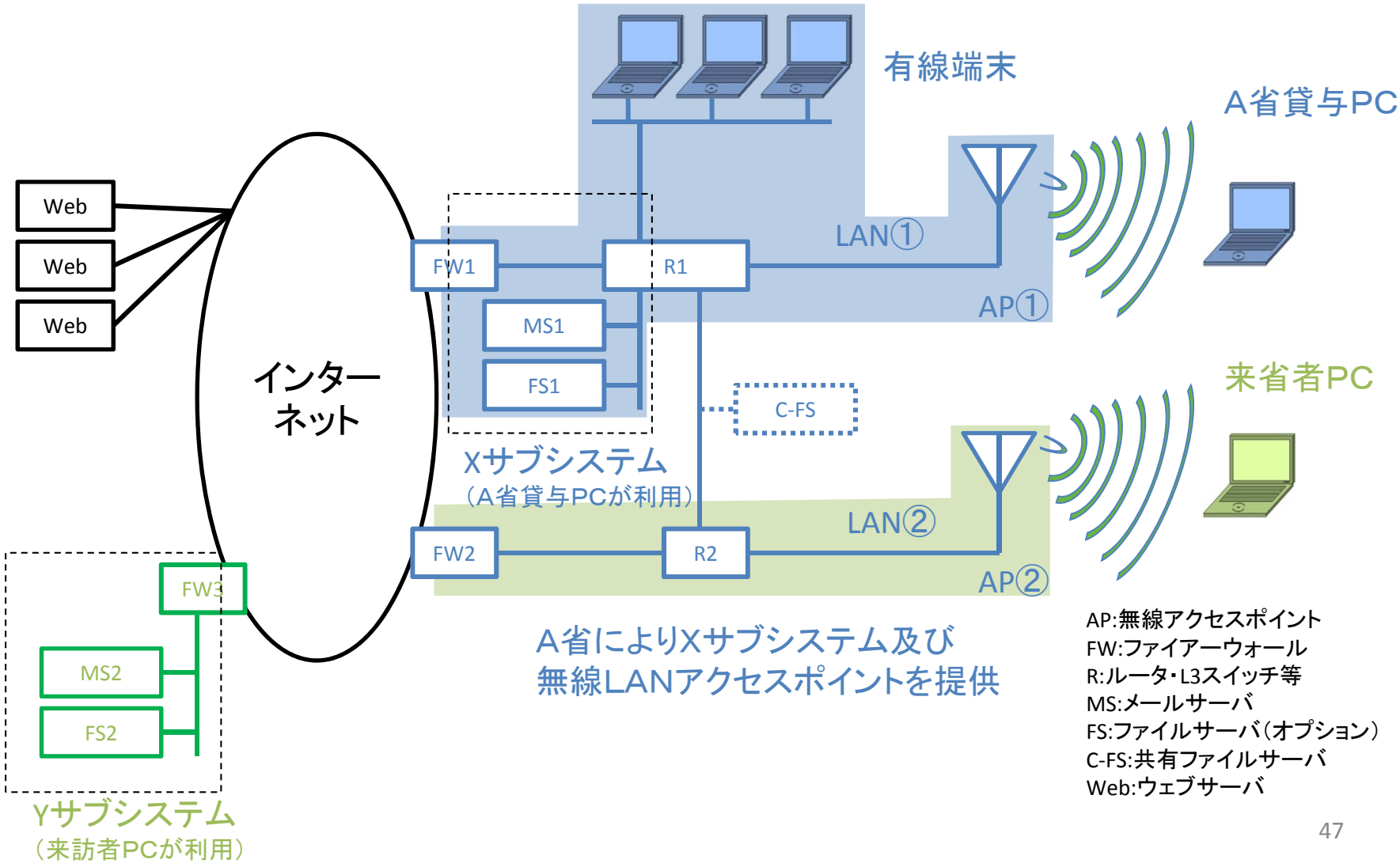
ケース2及びケース3における導入のポイント

モデルと物理構成

- 「無線LAN提供モデル」は、論理的なモデルを示したものである。
- 実際に無線LAN環境を構築するにあたっては、一つの論理的なモデルに対して、複数の物理構成が考えられる。ここでは、完全に物理構成を網羅することは、困難なため、ケース2、ケース3に関して、想定される主なFW、R、AP等の物理構成をいくつか示し、構成の特徴とポイントを考察する。
- そのため、各ケースにおいては、いづれの物理構成であっても、論理的なセキュリティレベルは、同等であると考えられることに留意していただきたい。

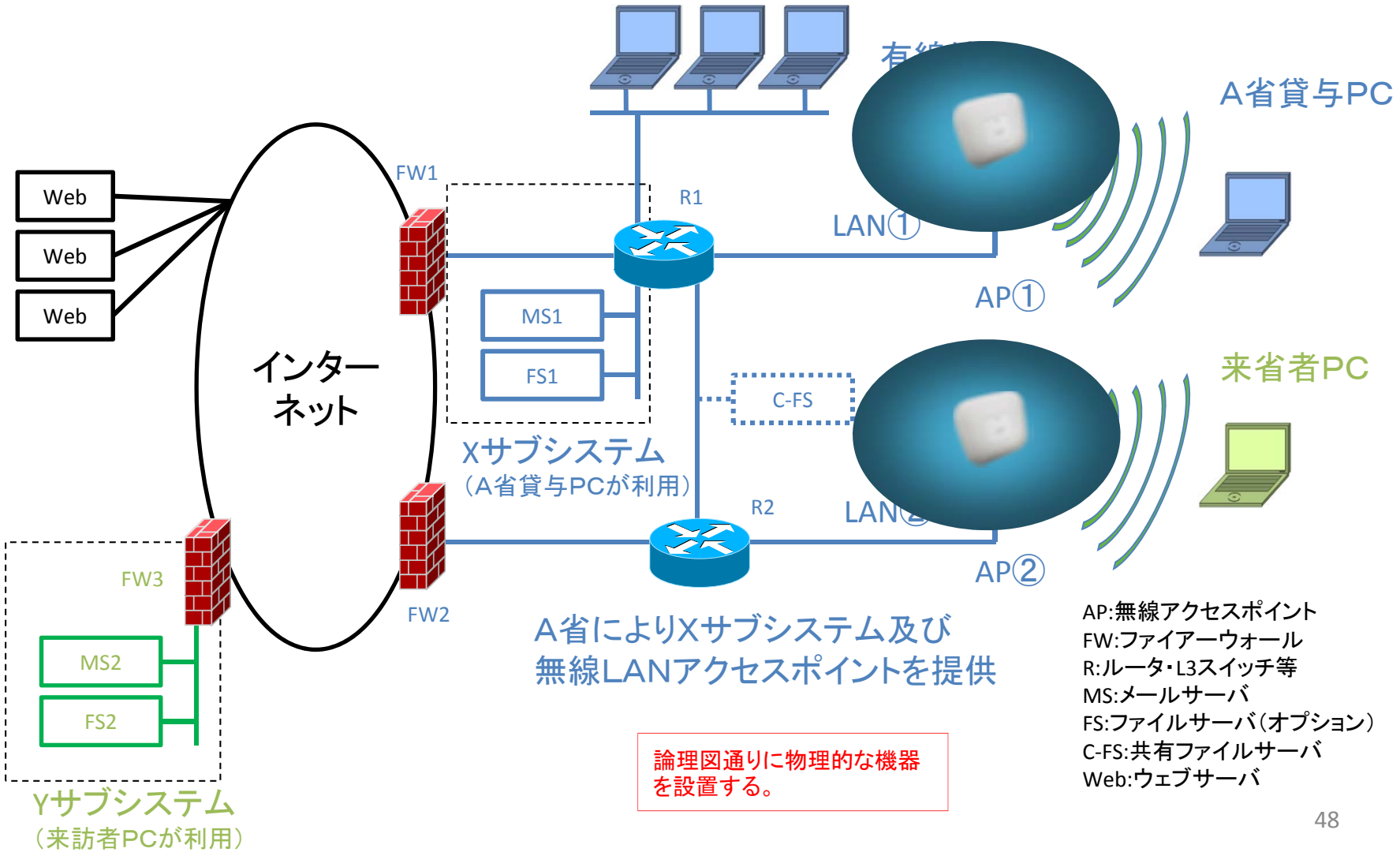
ケース2における物理構成の特徴とポイント

無線LAN提供モデル（ケース2）

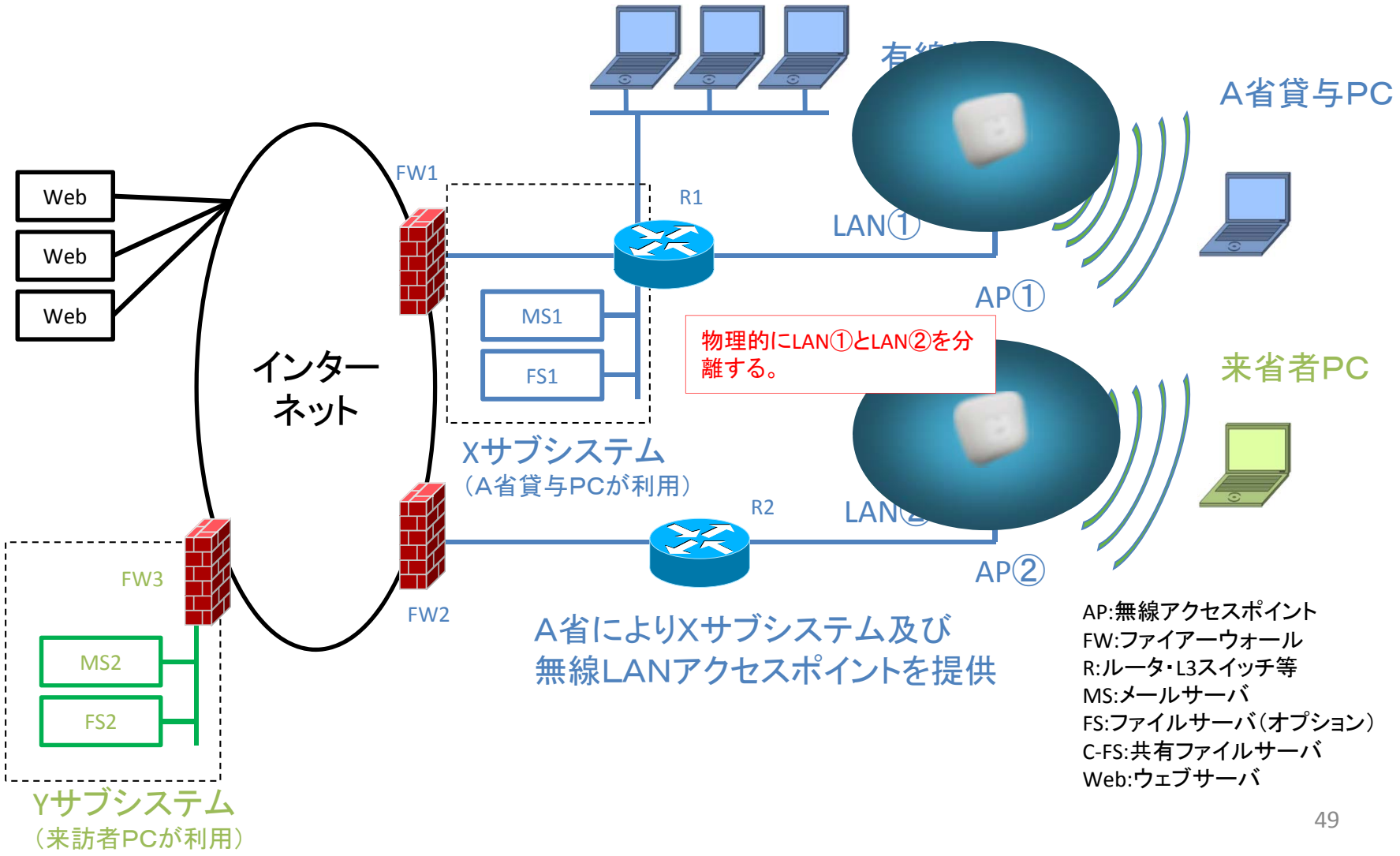


AP:無線アクセスポイント
FW:ファイアーウォール
R:ルータ・L3スイッチ等
MS:メールサーバ
FS:ファイルサーバ（オプション）
C-FS:共有ファイルサーバ
Web:ウェブサーバ

ケース2における無線LAN提供物理構成（ケース2-a）

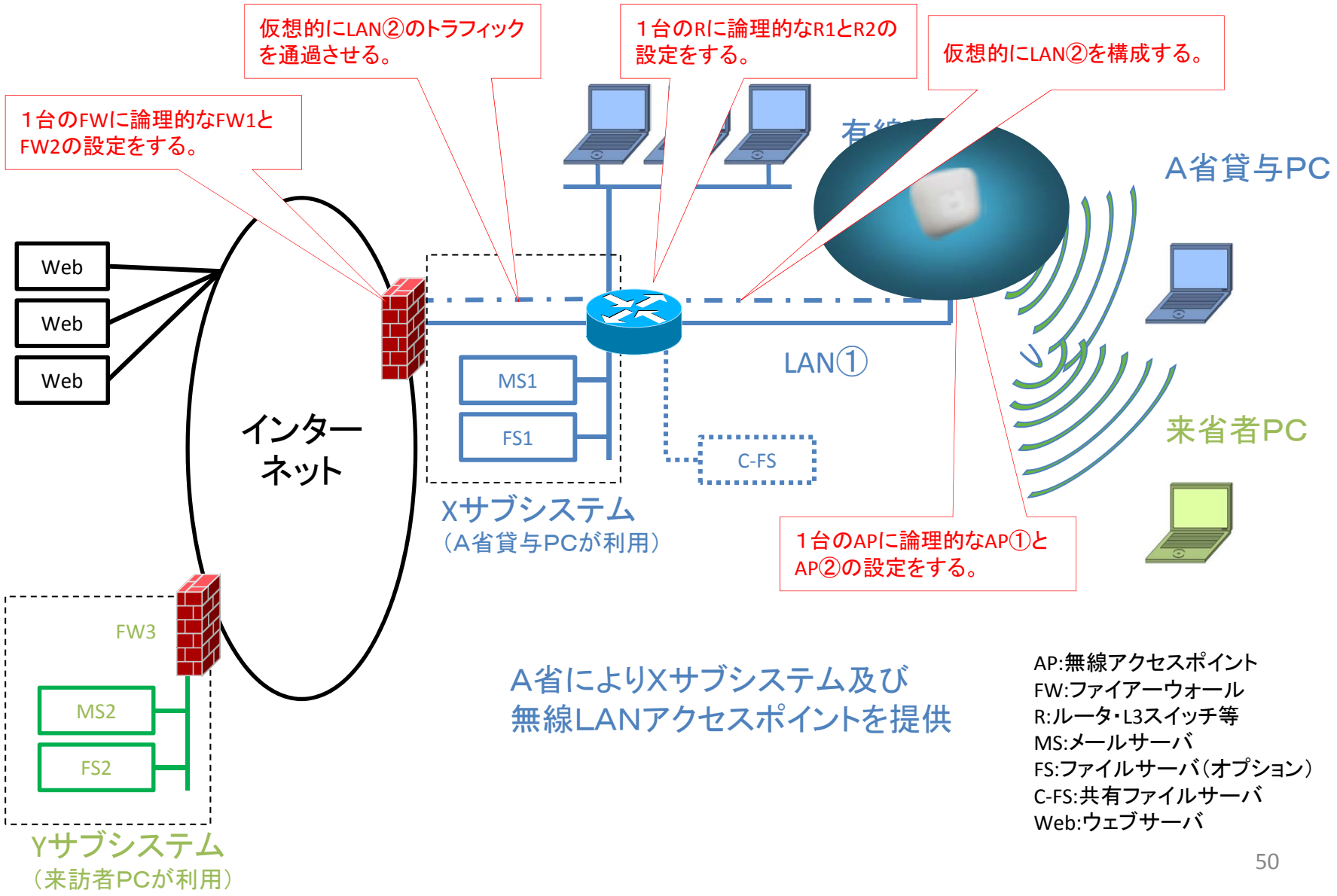


ケース2における無線LAN提供物理構成（ケース2-b）



AP:無線アクセスポイント
FW:ファイアーウォール
R:ルータ・L3スイッチ等
MS:メールサーバ
FS:ファイルサーバ（オプション）
C-FS:共有ファイルサーバ
Web:ウェブサーバ

ケース2における無線LAN提供物理構成（ケース2-c）



A省によりXサブシステム及び
無線LANアクセスポイントを提供

AP:無線アクセスポイント
FW:ファイアーウォール
R:ルータ・L3スイッチ等
MS:メールサーバ
FS:ファイルサーバ（オプション）
C-FS:共有ファイルサーバ
Web:ウェブサーバ

構成の特徴とポイント

	構成の特徴	ファイルサーバの提供	A省機器構成	ネットワーク機器コスト
ケース2-a	AP、FW、LANを物理的に分離し、R1とR2で論理的に分離する。	ファイルサーバで共有可能	AP×2台 FW×2台 R×2台 LAN×2系統	高
ケース2-b	LAN①とLAN②を物理的に分離する。	ファイルサーバを共有不可	AP×2台 FW×2台 R×2台 LAN×2系統	やや高
ケース2-c	AP、FW、LANは、物理的に一つのものを活用し、論理的にLAN①とLAN②を分離する。	ファイルサーバを共有可能	AP×1台 FW×1台 R×1台 LAN×1系統	低

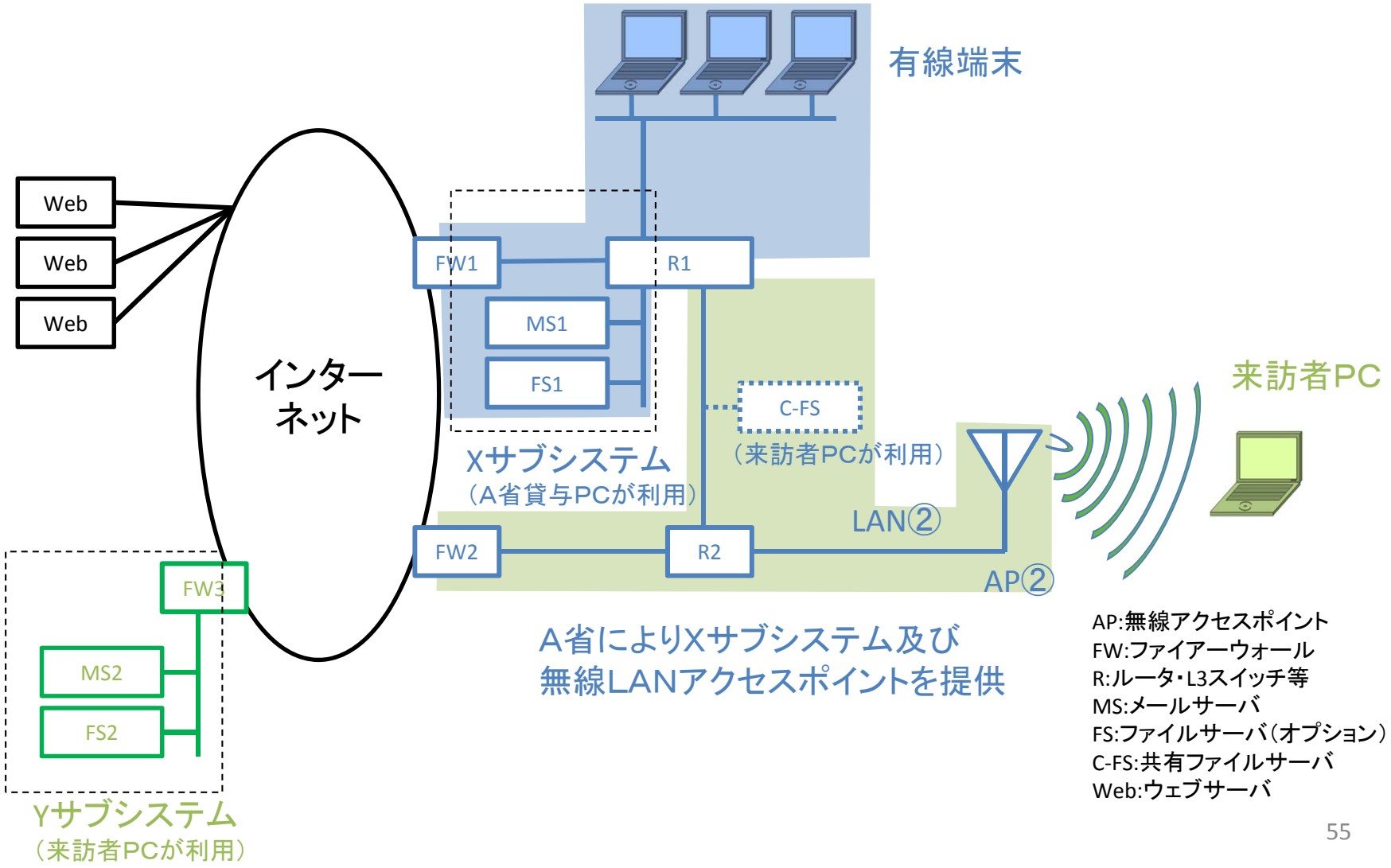
ケース2-a、ケース2-b、ケース2-cを選択するためには、適用するネットワークのリスク、ファイルサーバの共有の必要性、必要なLAN系統数を含む機器構成、ネットワーク機器コストを考慮していただきたい。

白紙ページ

白紙ページ

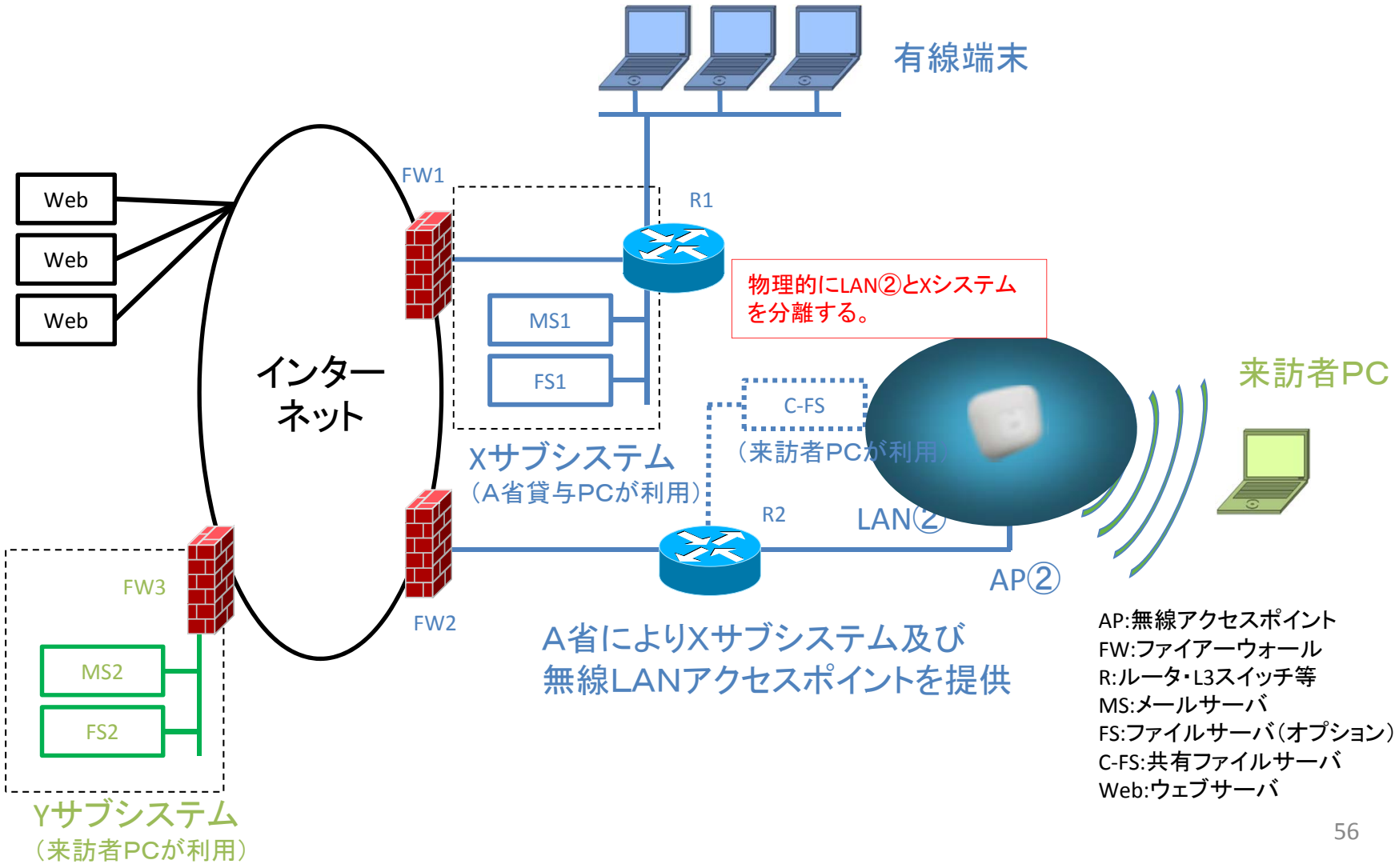
ケース3における物理構成の特徴とポイント

無線LAN提供モデル（ケース3）



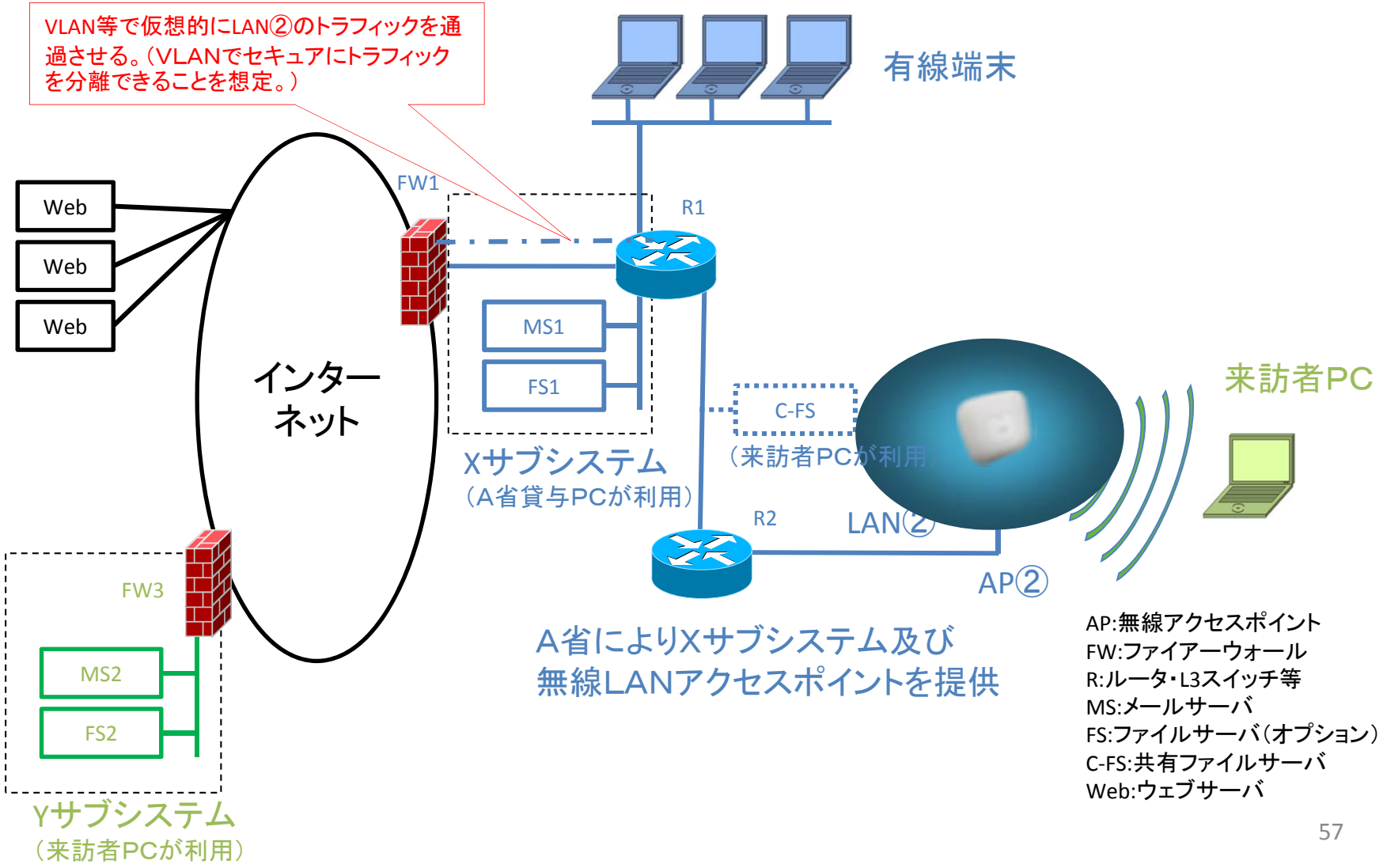
AP:無線アクセスポイント
FW:ファイアーウォール
R:ルータ・L3スイッチ等
MS:メールサーバ
FS:ファイルサーバ（オプション）
C-FS:共有ファイルサーバ
Web:ウェブサーバ

ケース3における無線LAN提供物理構成（ケース3-a）



AP:無線アクセスポイント
FW:ファイアーウォール
R:ルータ・L3スイッチ等
MS:メールサーバ
FS:ファイルサーバ（オプション）
C-FS:共有ファイルサーバ
Web:ウェブサーバ

ケース3における無線LAN提供物理構成（ケース3-b）



AP:無線アクセスポイント
FW:ファイアーウォール
R:ルータ・L3スイッチ等
MS:メールサーバ
FS:ファイルサーバ（オプション）
C-FS:共有ファイルサーバ
Web:ウェブサーバ

構成の特徴とポイント

	構成の特徴	ファイルサーバの提供	A省機器構成	ネットワーク機器コスト
ケース3-a	XシステムとLAN②を物理的に分離する。	ファイルサーバを提供可能	AP×1台 FW×2台 R×2台 LAN×2系統	高
ケース3-b	XシステムとLAN②をR1で論理的に分離する。	ファイルサーバを提供可能	AP×1台 FW×1台 R×2台 LAN×1系統	低

ケース3-a、ケース3-bを選択するためには、適用するネットワークのリスク、必要なLAN系統数を含む機器構成、ネットワーク機器コストを考慮していただきたい。

まとめ

- 以下の各ケースに応じた無線LANのセキュリティ対策を実施する必要がある。
  - 職員専用利用型
  - 職員・来訪者混在型
  - 来訪者提供型
  - 仮設型
  - ホットスポット利用型
- それぞれのケースにおいても、物理構成を決定する場合は、以下の点を考慮する必要がある。
  - 適用するネットワークのリスク
  - 必要なLAN系統数を含む機器構成
  - ネットワーク機器コスト

留意事項

- Wi-Fi Alliance(http://wi-fi.org/)の認証済み機器であることの確認
  - 無線機器は相互接続できる機器であることが重要である。そのため、無線LANに使用する機器は、Wi-Fi Allianceの認証済み機器であることを確認する必要がある。
- 規格化・標準化されている認証・暗号化方式の採用
  - 認証・暗号化に用いる方式は、「 電子政府推奨暗号リスト」やWi-Fi Alliance等で客観的評価が行なわれ、規格化・標準化されている方式を採用すべきである。
- セキュリティに関する技術動向への留意
  - 無線LANのセキュリティは、有線LANのセキュリティ等と同様に、日々、大きく変化している。そのため、無線LANのセキュリティに関する技術動向へは留意し、対応することが重要である。
- 有線LANのセキュリティの確保
  - 無線LANのみのセキュリティを確保するだけでなく、有線LANに機器を接続する際に不正な機器を接続されないためのセキュリティ対策も検討することも重要である。
- 変化する電波環境への対応の必要性
  - 電波環境は、さまざまな周波数が存在し、使用されているチャンネルや無線機器の出力が常に変化している。そのため、これらの変化する電波環境へ対応をすることが必要である。
- Web認証は、無線アクセスポイントや無線LANコントローラで行なうことが必要
  - Web認証を無線アクセスポイントや無線LANコントローラで行なわない場合、Web認証を行なう前に無線PC間で通信できる可能性がある。そのため、Web認証は、無線アクセスポイントや無線LANコントローラで行なう必要がある。
- 事業継続の検討の必要性
  - 無線LANに限らず、セキュリティにおいては、何らかの理由により情報システムが利用できなくなる場合を想定し、事業継続をどのように行なっていくかを検討する必要がある。無線LANの場合、大規模な妨害電波等による無線環境が利用できなくなる可能性を考えると、最低限の有線LANの準備等も検討する必要がある。
- 無線LANの効果的な導入を行なうためのポイント
  - 無線LANの効果的な導入を行なうためには、有線LANの通信の暗号化、無線機器の冗長化、電波干渉の詳細な測定機器の導入、ゼロタッチコンフィグレーションによる効率的なAP設置、PoE(Power over Ethernet)の活用によるAPへの電源・通信の同時供給等も合わせて検討する必要がある。

用語①

- IEEE 802.1X
  - IEEEが策定した認証規格。サプリカント(認証対象クライアント)からオーセンティケーター(認証機器)までをEAPというプロトコルで、オーセンティケーターから認証サーバまでをRadiusで通信する。この認証結果によりサプリカントに対して通信認証認可を与える仕組みをIEEE 802.1Xでは規定している。
- EAP(Extensible Authentication Protocol)
  - 認証プロトコルの一つ。さまざまなクレデンシャル(認証資格情報)や認証方法が可能となるよう複数の手法がある。EAP-TLS/EAP-FAST/EAP-PEAPなどがある。
- Wi-Fi Alliance
  - 無線LAN製品の普及促進を目的とした業界団体。IEEEの規定だけでは各社の無線機器による相互接続性が保証されないため独自に接続性の認証を行っている。事実上の標準として各種ガイドラインで要件として参照されている。認証はWi-Fi認証、Wi-Fi Certificationなどと呼ばれている。いくつかの機能・項目ごとに個別の認証が設けられている。本検討ではWi-Fi 802.11a/b/g, WPA2-Enterprise/Personalが大きくかかわる。
- WPA(Wi-Fi Protected Access)
  - Wi-Fi認証のうち、認証プログラムに関する認証。IEEE 802.11i を基にしており現在ではWPA2を実装するのが通常となっている。WPAのうちEnterpriseはIEEE 802. 1Xの認証の結果得られる鍵を利用する。WPAのうちPersonalは事前共有鍵を用いる。また暗号化アルゴリズムとしてTKIPもしくはAES-CCMPが存在するがセキュリティ強度としてAES-CCMPの利用が推奨である。
- AES-CCMP
  - AESは、Advanced Encryption Standardの略で、アメリカ国立標準技術研究所（NIST）によってアメリカ合衆国の新暗号規格 (Advanced Encryption Standard) として規格化された共通鍵暗号方式である。鍵長は128ビット、192ビット、256ビットの3つから利用できる。CCMPは、Counter Mode with Cipher Block Chaining Message Authentication Code Protocol の略で、改ざん検出プロトコルである。CCMPでは，データの暗号化と並行してメッセージの完全性を確認するMIC（Message Integrity Check）を算出する。WPA2では、暗号化アルゴリズムとしてAES-CCMPの実装が必須である。
- WPA2-Enterprise
  - IEEE802.11iに準拠し、Wi-Fi Allianceが企業向けに推奨している無線LANのセキュリティ方式。暗号化アルゴリズムとしてAES-CCMPを使用する。ユーザ認証にIEEE802.1xを利用するため、RADIUSサーバが必要になる。
- WPA2-Personal
  - IEEE802.11iに準拠し、Wi-Fi Allianceが個人や小規模企業向けに推奨している無線LANのセキュリティ方式。暗号化アルゴリズムとしてAES-CCMPを使用。アクセスポイントと端末に事前共有鍵（Pre-Shared Key）をあらかじめ設定しておくことで認証・接続を行う。

用語②

- WEP
  - Wired Equivalent Privacyの略で、RC4アルゴリズムをベースにした秘密鍵暗号方式。IEEE802.11によって標準化されており、IEEE 802.11bのセキュリティシステムとして採用されている。秘密鍵に40ビット、128ビットを使用するが、WEPそのものに様々な脆弱性が発見・報告されている。
- SSID
  - Service Set Identifierの略で、IEEE 802.11 無線LANにおけるアクセスポイントの識別子である。1つのアクセスポイントに複数のSSIDを設定することは可能で、SSIDごとに認証やセキュリティのレベルを分けることも可能である。
- EAP-TLS
  - EAP認証プロトコルの一つ。サーバ、クライアントの双方で電子証明書を使用し、相互認証を行う。相互に証明書を発行・管理するため手間とコストがかかるものの、高度なセキュリティ性を保つことができる。
- EAP-FAST
  - EAP認証プロトコルの一つ。サーバ、クライアントの双方でProtected Access Credential（PAC）を使用し、相互認証を行う。シスコシステムズが開発し、IETFによってRFC4851として定義されている。EAP-FASTの認証は次の2つのフェーズに分かれて行う。フェーズ1では相互に認証されたトンネルを確立する。クライアントおよびサーバはPACを使用して相互に認証し、セキュアなトンネルを確立する。フェーズ2では、確立されたトンネルでクライアントの認証を実行する。クライアントは認証用のユーザ名およびパスワードを送信してクライアント許可ポリシーを確立する。 フェーズ0（任意）はあまり使用されないが、PACを使用してクライアントを動的にプロビジョニングできるようにする。このフェーズでは、ユーザとネットワークの間にユーザ単位のアクセス証明書がセキュアに生成される。このユーザ単位の証明書（PAC）は、EAP-FAST認証のフェーズ1で使用される。
- PEAP
  - Protected EAPの略。EAP認証プロトコルの一つ。サーバ側は電子証明書を使用し、クライアント側はID・パスワードを使用して相互認証を行う。PEAP の認証は、次の 2 つのフェーズに分かれて行う。フェーズ 1 では、サーバ側で TLS 認証を実行することで、暗号化トンネルを作成し、一般的で信頼されたセキュリティ方法の 1 つである Secure Sockets Layer（SSL）を使用した Web サーバ認証に似た方法でサーバ側の認証を実現する。PEAP のフェーズ 1 が確立されると、ユーザに固有のすべての情報を含むすべてのデータが暗号化される。PEAP 認証のフェーズ 2 のフレームワークは拡張可能であり、TLS トンネル内で EAP-GTC や Microsoft Challenge Authentication Protocol（MS-CHAP）Version 2 などの方法を使用してクライアントを認証できる。

用語③

- RADIUS
  - Remote Authentication Dial-In User Serviceの略で、元々はダイヤルアップユーザの認証を実現するためのIP（UDP）プロトコル。現在では、ユーザの認証やアカウンティング（利用の事実の記録）のために一般的に利用されている。IEEE802.1xでは、オーセンティケーター(認証機器)から認証サーバまでの間のイーサネット上のプロトコルとして使用する。
- RC4
  - RC4はRon Rivestにより1987年に開発されたストリーム暗号であり、このアルゴリズムで発生させた疑似乱数列と平文との排他的論理和が暗号文となる。
- ストリーム暗号
  - ストリーム暗号とは、平文をビット単位あるいはバイト単位などで逐次、暗号化する暗号である。これに対して、平文を64ビットや128ビットなどの固定長のブロックに分割して暗号化する暗号はブロック暗号という。ストリーム暗号とブロック暗号とが、現代の主要な共通鍵暗号である。

用語④

- IEEE802.11
  - IEEE(米国電気電子学会)でLAN技術の標準を策定している802委員会が1998年7月に定めた無線LANの標準規格群。2.4GHz周波数帯を使った直接拡散方式、周波数ホッピング方式、赤外線方式のそれぞれについて規定されている。現在では802.11a/b/g/nなどを総じてさす場合の呼称として使われる
- IEEE802.11a
  - IEEE(米国電気電子学会)でLAN技術の標準を策定している802委員会が定めた無線LANの規格の一つで、5GHz帯（5150-5350、5470-5725MHz）の無線で約54Mbpsの通信を行う仕様。IEEE802.11n Draft 2.0(W52/W53)及びIEEE802.11a(W52、W53)無線LANの使用は、電波法令により屋内に限定される。
- IEEE802.11b
  - IEEE(米国電気電子学会)でLAN技術の標準を策定している802委員会が定めた無線LANの規格の一つで、2.4GHz帯の無線で約11Mbpsの通信を行う仕様。
- IEEE802.11g
  - IEEE(米国電気電子学会)でLAN技術の標準を策定している802委員会が2003年6月に策定した、無線LANの標準規格の一つで、2.4GHz帯で約54Mbpsの通信を行う仕様。
- IEEE802.11j
  - IEEE(米国電気電子学会)でLAN技術の標準を策定している802委員会が2004年12月に策定した、日本向けの無線LAN規格。日本国内で4.9GHz帯を利用するための規格で、日本国内の無線規制基準も満たし、屋内だけでなく屋外でも使用できる。主に有免許で屋外利用に使われるため普及帯の製品に実装されていることは少ない
- IEEE802.11n
  - IEEE(米国電気電子学会)でLAN技術の標準を策定している802委員会が2009年9月に策定した、無線LANの規格の一つで、2.4GHz帯または5GHz帯の無線でデータレートとしては最高600Mbpsの通信を行う仕様。なお、W52/W53（5150-5350MHz）での無線LAN利用は、電波法令により屋内に限定される。

参考文献①

- IEEE 802.1
  - http://standards.ieee.org/about/get/802/802.1.html
- IEEE 802.1X, “Port-Based Network Access Control”
  - http://standards.ieee.org/getieee802/download/802.1X-2010.pdf
- IEEE 802.11-2007
  - http://standards.ieee.org/getieee802/download/802.11-2007.pdf
- IEEE 802.11a-1999 High-speed Physical Layer in the 5 GHz band
  - http://standards.ieee.org/getieee802/download/802.11a-1999.pdf
- IEEE 802.11b-1999 Higher Speed Physical Layer Extension in the 2.4 GHz band
  - http://standards.ieee.org/getieee802/download/802.11b-1999.pdf
- IEEE 802.11g-2003: Further Higher Data Rate Extension in the 2.4 GHz Band
  - http://standards.ieee.org/getieee802/download/802.11g-2003.pdf
- IEEE 802.11i-2004
  - http://standards.ieee.org/getieee802/download/802.11i-2004.pdf
- IEEE 802.11j-2004 standard
  - http://standards.ieee.org/getieee802/download/802.11j-2004.pdf
- IEEE 802.11n-2009
  - http://standards.ieee.org/getieee802/download/802.11n-2009.pdf

参考文献②

- “PPP EAP TLS Authentication Protocol”，RFC2716
  - http://www.ietf.org/rfc/rfc2716.txt
- “Remote Authentication Dial In User Service (RADIUS)”，RFC2865
  - http://tools.ietf.org/rfc/rfc2865.txt
- “RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)”，RFC3579
  - http://tools.ietf.org/rfc/rfc3579.txt
- “IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines”，RFC3580
  - http://tools.ietf.org/rfc/rfc3580.txt
- “Extensible Authentication Protocol (EAP)”，RFC3748
  - http://www.ietf.org/rfc/rfc3748.txt
- “The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST)”，RFC4851
  - http://www.ietf.org/rfc/rfc4851.txt
- “The EAP-TLS Authentication Protocol”，RFC5216
  - http://www.ietf.org/rfc/rfc5216.txt
- “Microsoft's PEAP version 0 (Implementation in Windows XP SP1)”，PEAPv0
  - http://tools.ietf.org/id/draft-kamath-pppext-peapv0-00.txt
- “Protecting EAP with TLS (EAP-TLS-EAP)”，PEAPv1
  - http://tools.ietf.org/id/draft-josefsson-pppext-eap-tls-eap-00.txt
- Wi-Fi、Wi-Fi.org
  - http://wi-fi.org/
- WPA2(Wi-Fi Protected Access 2)，Wi-Fi.org
  - http://www.wi-fi.org/knowledge_center/wpa2
- “Deploying Wi-Fi Protected Access (WPA) and WPA2 in the Enterprise”, Wi-Fi.org
  - http://www.wi-fi.org/files/wp_9_WPA-WPA2%20Implementation_2-27-05.pdf

参考文献③

- 政府機関の情報セキュリティ対策のための統一基準（第4版）解説書
  - http://www.nisc.go.jp/active/general/pdf/K303-081C.pdf
- “安心して無線LANを利用するために”，総務省
  - http://www.soumu.go.jp/main_sosiki/joho_tsusin/lan/pdf/lan_1.pdf
- “電子政府推奨暗号リスト”，暗号技術検討会
  - http://www.cryptrec.go.jp/list.html
- ”Guide to Computer Security Log Management “,SP800-92
  - http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf
- “Recommendation for EAP Methods Used in Wireless Network Access Authentication”，NIST SP800-120
  - http://csrc.nist.gov/publications/nistpubs/800-120/sp800-120.pdf
- “Announcing the ADVANCED ENCRYPTION STANDARD (AES)”，NIST FIPS197
  - http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
- “Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies”，DoDi 8420.01
  - http://www.dtic.mil/whs/directives/corres/pdf/842001p.pdf
- “大企業・中堅企業の情報システムのセキュリティ対策　～脅威と対策～”無線LAN利用環境のための運用上のセキュリティ対策，独立行政法人情報処理推進機構
  - http://www.ipa.go.jp/security/fy18/reports/contents/enterprise/html/421.html
- “無線LANのセキュリティに係わる脆弱性の報告に関する解説”，産業技術総合研究所 情報セキュリティ研究センター
  - http://www.rcis.aist.go.jp/TR/2009-01/wpa-compromise-summary.html
- “Breaking 104 bit WEP in less than 60 seconds”
  - http://eprint.iacr.org/2007/120.pdf
- “Stream Ciphers”，RSA Laboratories Technical Report TR-701
  - http://security.ece.orst.edu/koc/ece575/rsalabs/tr-701.pdf

サブサーキング開催状況

検討メンバー・検討会開催状況

- CIO補佐官
  - 内閣府　野村　邦彦
  - 内閣府・内閣官房　平林　元明
  - 内閣法制局　川合　浩司
  - 外務省　窪田　文啓
  - 環境省　満塩　尚史
  - 衆議院　宮崎　晋吾
- ベンダー
  - シスコシステムズ合同会社
  - 株式会社ラック
- オブザーバ
  - 内閣官房情報セキュリティセンター
  - 総務省
  - 独立行政法人　情報処理推進機構
  - 独立行政法人　産業技術総合研究所（花岡　悟一郎）

- 第1回検討会　2010年10月22日
  - 検討方法について
  - 利用シーンについて
- 第2回検討会　2010年11月8日
  - 利用シーン及びケース分けについて
  - 無線LANの規格について
- 第3回検討会　2010年11月26日
  - 無線LANの脅威に
  - SSID、無線LANの暗号化について
- 第4回検討会　2010年12月10日
  - 脅威一覧について
  - 脅威に対する対策・手法について①
- 第5回検討会　2010年12月22日
  - 脅威に対する対策・手法について②
- 第6回検討会　2010年1月14日
  - まとめについて