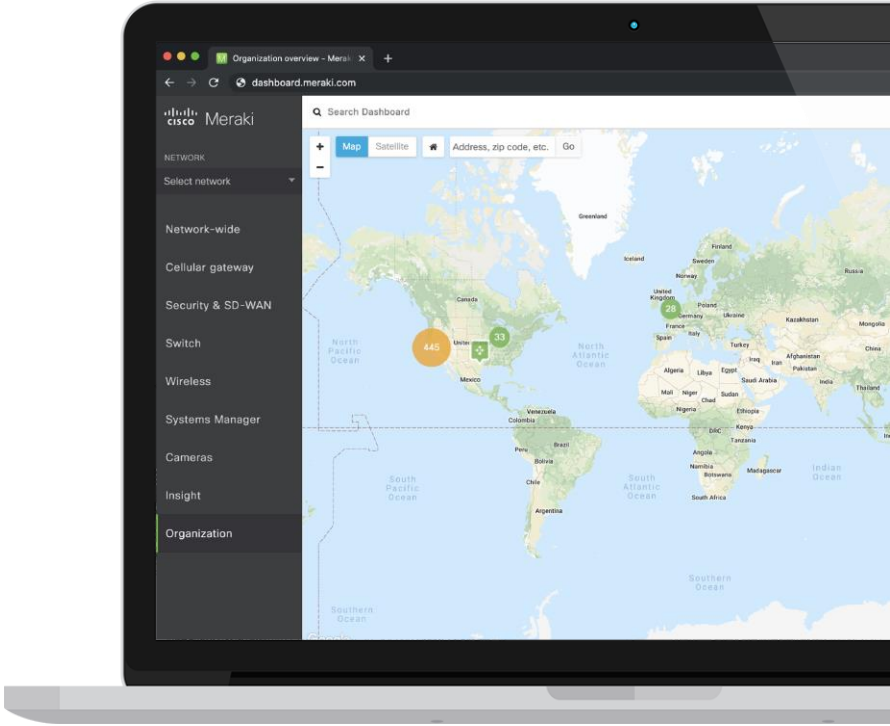
Merakiで実現するシンプルネットワーク

自治体向けクラウド管理するWi-Fi

シスコシステムズ合同会社
Meraki事業　テクニカルソリューションアーキテクト
片山　智

The Meraki Platform

完全なクラウド管理型ITインフラソリューション



cisco Meraki

Meraki Cloud

クラウド管理型ITインフラソリューションとしての実績

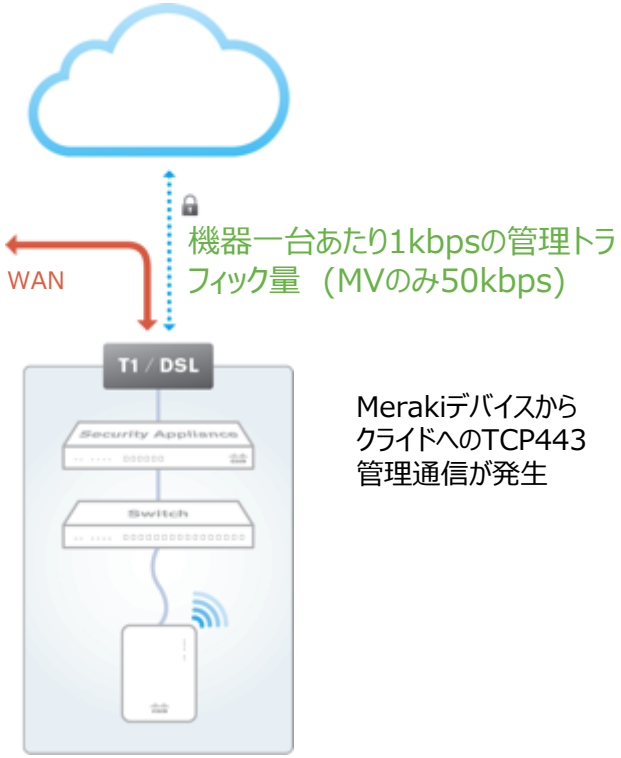
50万以上の
顧客

650万以上の
デバイスが稼働

350万以上の
アクティブな
ネットワーク

cisco Meraki

クラウド管理型ITインフラの特徴



- セキュリティ
  - ユーザトラフィックはクラウドを経由しない
  - HIPAA / PCI 完全準拠 (レベル1認定)
  - 第三者によるセキュリティ監査, 日次での脆弱性テスト
  - 自動ファームウェア/セキュリティアップデート（ユーザスケジュールによる）
- 信頼性
  - 複数データセンタを使用した高可用性
  - 万一クラウドの障害にも影響受けないネットワークファンクション
  - 99.99% アップタイムSLA
- スケーラビリティ
  - 無制限のスループット、ボトルネック無し
  - 機器、拠点の簡単な増設
  - 明瞭な投資判断

Reliability and security information at meraki.cisco.com/trust

ゼロタッチ導入が可能

導入拠点

ダッシュボード

1. 開封して、ケーブル接続

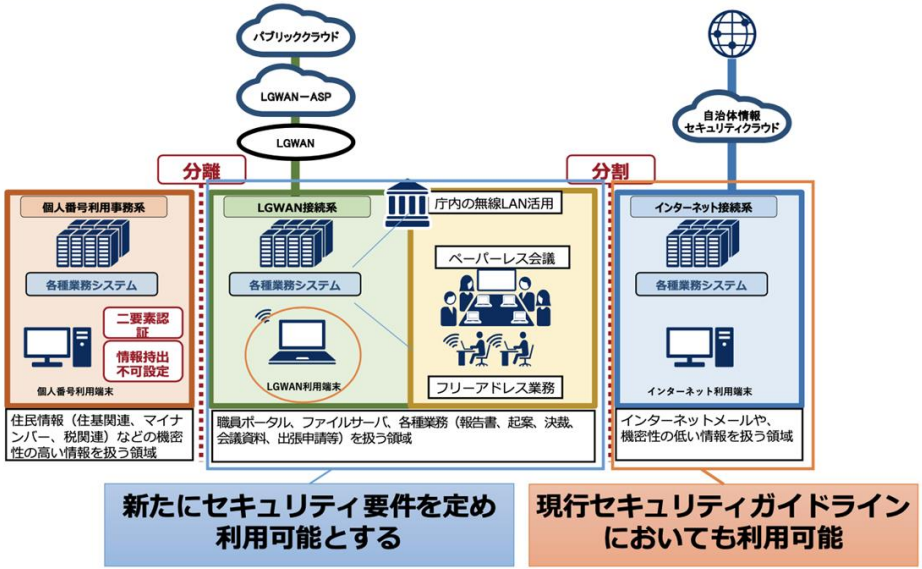
1. ネットワーク設定(テンプレート設定可能)
2. オーダー番号を入力
   -オーダー番号とHWシリアル番号を関連づけ

GIGAスクール 約250自治体 約7,000校　採用実績 *当社調べ

LGWAN接続での庁内無線LANの利用

改定方針

- 現在、自治体では、職員が主に利用するLGWAN接続系において、無線LANの利用は避けることが望ましいとされている一方で、地方公共団体においては、業務効率化の観点から、庁内無線ＬＡＮによる柔軟な職場環境の実現に対するニーズが高まっており、既に導入されている例もある。
- 庁内無線ＬＡＮの利用において、セキュリティ対策が不十分な場合、不正アクセス等のリスクが懸念される。そのため、ＬＧＷＡＮ接続系において庁内無線ＬＡＮを利用する場合のセキュリティ要件を記載する。



次世代自治体ネットワークに求められる要件

環境の変化

働き方改革

ペーパーレス
行政のデジタル化
フリーアドレス
リモートワーク

NW強靭化

三層分離
α/β/β'モデルの対応

新型感染症対策

ソーシャルディスタンス
リモートワーク

次世代自治体庁舎内ネットワーク

NWに求められる要件

高速・安定化

ビデオ会議
IP電話化
電子申請

無線LAN化

モバイル端末活用

セキュリティ強化

マルウェア対策
無線LANセキュリティ
機器の改ざん対策

cisco Meraki

シスコの提案概要

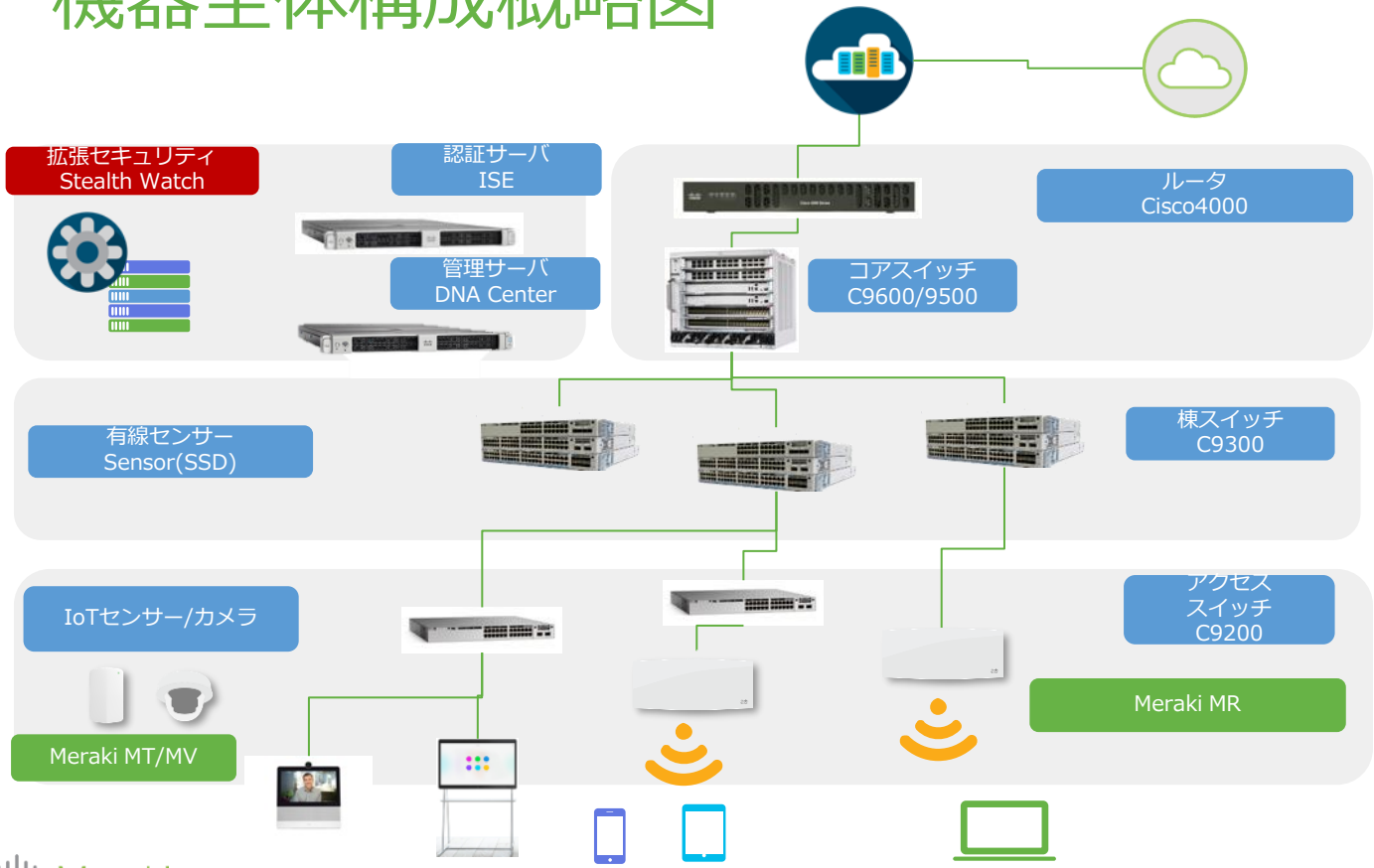
シスコの標準ネットワーク構成で、課題の解決が可能です
管理機能の拡張、セキュリティの拡張、さらに、その両方の利用も可能です

対象機能一覧

	高速・安定化	無線LAN化	セキュリティ強化	機器構成
拡張セキュリティ			＋StealthWatch (+Umbllera) (+Duo)	
拡張機能 IBN（直感的管理） ＋DNA-Center	1. 統合管理（有線無線） 2. 自動化（BasicAutomation） 3. 見える化（Asuurance） (ユーザー、機器、アプリケーション) 4. 無線LAN位置情報 5. SDN（SDA）		1. Wireless IPS 2. ゼロトラスト（SDA）	＋DNA Center ＋Wireless Sensor (AP1800s) ＋Wired Sensor(+SSD) ＋(Thousand Eyes)
標準機能	1. VRFS 2. mGig 3. PoE+ 4. StackWise 5. SMU	1. Wi-Fi6 2. クラウド管理 3. 電波自動調整 4. 通信の可視化と帯域制御 5. テレワーク（Teleworker VPN）	1. Trustworthy/TAM 2. 無線LANセキュリティ（FW, Traffic Shaping, Umbrella DNS Security, Air Marshal）	Cat9k & Meraki キャンパスエッジ -Meraki MR -Catalyst9200/9300/9400/ 9500/9600 -ISE -Router (ISR4000)

cisco Meraki

機器全体構成概略図



クラウド

サーバ室

各フロア

MDF

業務エリア

cisco Meraki

標準機能

高速・安定化

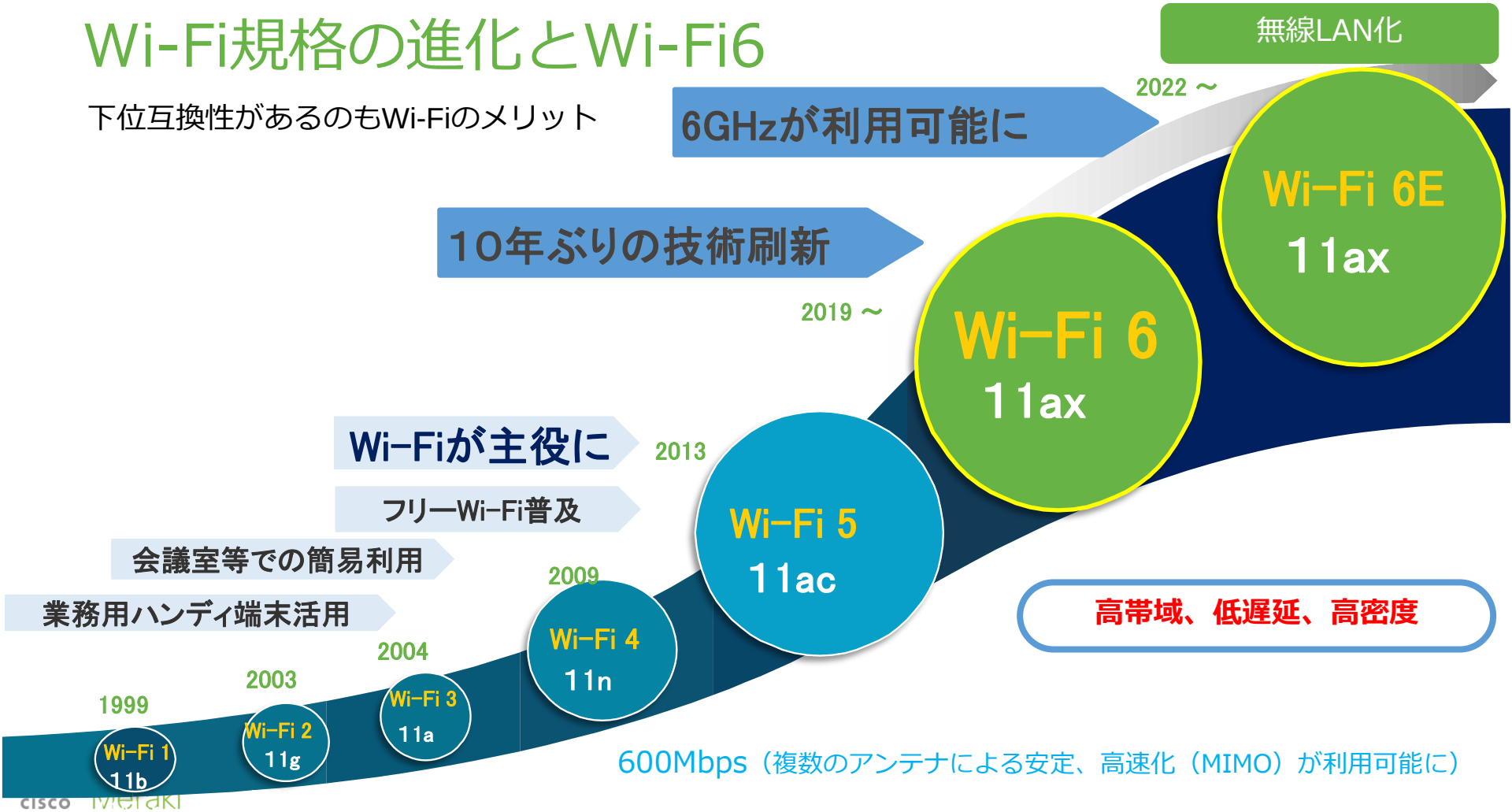
無線LAN化

セキュリティ強化

1. Wi-Fi 6

Wi-Fi規格の進化とWi-Fi6

下位互換性があるのもWi-Fiのメリット



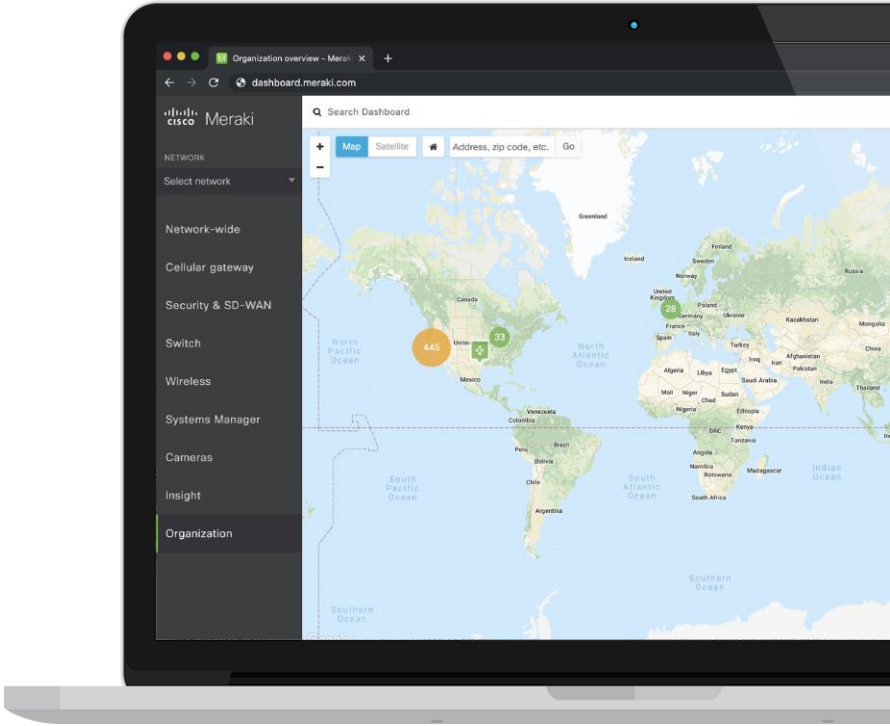
- 100台一斉通信動画
- マルチキャスト配信動画

2. クラウド管理

無線LAN化

The Meraki Platform

完全なクラウド管理型ITインフラソリューション



cisco Meraki

無線LAN化

対象機器
Cisco Meraki MRシリーズ　アクセスポイント

同時利用数

屋内

中小規模の導入に最適 | ミッションクリティカル | ベストインクラス

MR36H
2x2 2 Stream
802.11ax
3-port gigabit switch
1-port Passthrough
Wi Fi 6 CERTIFIED

MR36
2x2: 2Stream
802.11ax
Wi Fi 6 CERTIFIED

MR44
5GHz 4x4: 4Stream
2GHz 2x2: 2Stream
802.11ax
2.5G Mgig
Wi Fi 6 CERTIFIED

MR46/46E
4x4: 4Stream
802.11ax
2.5G Mgig
Wi Fi 6 CERTIFIED

MR56
8x8: 8Stream
802.11ax
5G Mgig
Wi Fi 6 CERTIFIED

cisco Meraki

Meraki クラウド管理型のメリット

①無線コントローラが不要
- 将来アクセスポイントが増えても無線コントローラの増設は不要
- 障害ポイントが軽減される

②導入時、故障交換時の時間及びコストが軽減される
- ゼロタッチで立ち上がるため、人員及び経費の大幅な削減が可能

③アクセスポイント一台からフル機能利用可能
- 他管理製品やソフトウエアは不要/追加時に必要なものはアクセスポイントのみ

④遠隔地からの監視、対応が容易
- 出先機関や支所の利用状況監視、設定変更が可能

⑤管理画面がシンプルかつわかりやすいため専門家でなくてもすぐに操作可能
- わかりやすいWEB管理画面を利用するため専門的な知識は不要

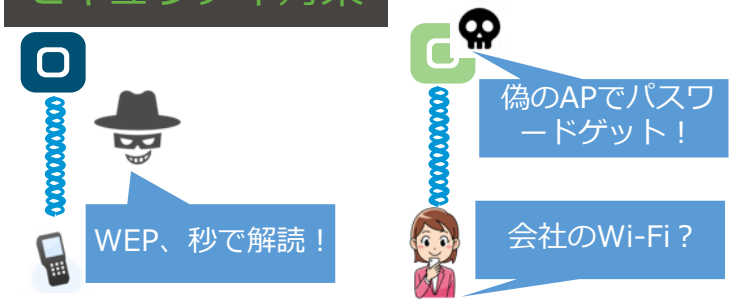
⑥ファームウェアの自動更新
- 新しい安定版バージョンが公開されると自動的にアップグレードがスケジュールされ自動更新

⑦トラブルシュートが迅速
- 機器設定内容が保守業者とも共有され迅速な日本語サポートが可能

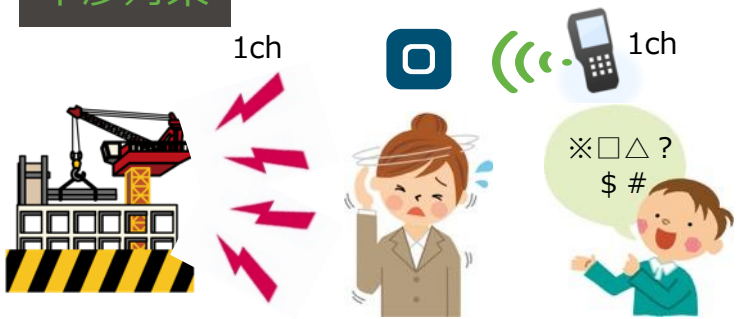
3. 電波調整

参考：Wi-Fiを安全かつ安定的に利用するには

セキュリティ対策



干渉対策



電波の到達範囲

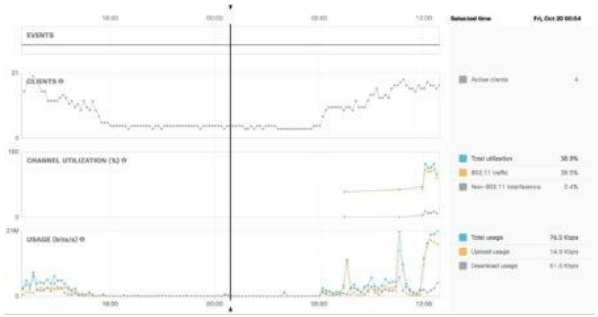
項目	対策
セキュリティ	• WPA2/WPA3の採用 • 認証サーバーの利用
干渉対策	• 5GHz帯の積極活用 • チャネル自動制御の活用
電波の到達範囲	• 双方向通信の確保 • 送信電力自動制御の活用

電波の自動調整
Meraki Auto RF

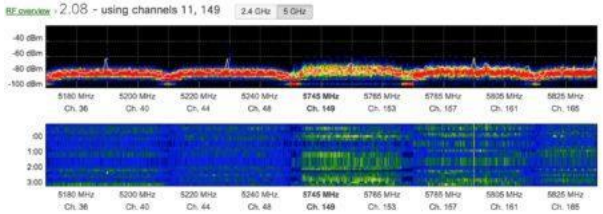
課題
電波干渉がおこり仕事が止まる
適切なサーベイしても電波状況がかわる

無線LAN化

Meraki MRシリーズは専用の監視アンテナを搭載しWi-Fiおよび非Wi-Fi干渉を監視します！

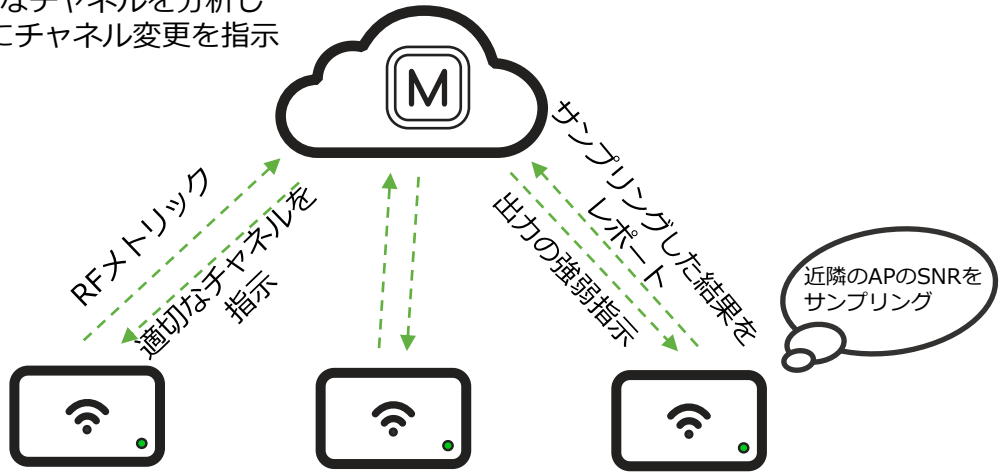


チャネル使用率や負荷を監視



専用アンテナでRFスペクトラム分析

適切なチャネルを分析し
MRにチャネル変更を指示



自動チャネル管理はアクセスポイントが追加されたタイミングや夜間・ネットワーク利用量が少ない時間帯、および手動でチャネル更新ボタンを押した時に発動し、頻繁にチャネル変更を行うことで与える利用者への影響を考慮しています。

cisco Meraki

4. 通信の可視化と帯域制御

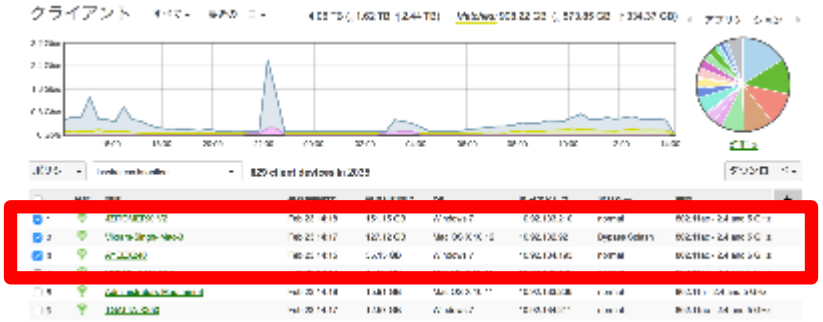
利用端末毎の利用アプリが可視化され、端末・SSID単位で帯域制御が可能

無線LAN化

端末の状態を可視化

- 1400以上のアプリケーションの可視化
- 端末毎の帯域利用量
- 端末の種類

etc…



オンデマンドでポリシーを適用

私用アプリなどで帯域を占有しているユーザを指定して通信をブロックしたり帯域制御のポリシーを適用可能

端末ごとの利用状況を可視化し、不適切な利用がないか確認することも可能ですし、利用アプリを把握することで将来のネットワーク設計へ活用も可能。

必要に応じて利用ポリシーを設定可能

例＞平日8時-17時の動画視聴を制限

Youtube等動画アプリを指定し、特定端末やSSID単位で帯域制御が可能

例＞OSアップデート/アンチウイルスアップデートは業務時間外に限定

大きなトラフィックが発生するアプリについては
業務時間外での利用のみに限定させることが可能

O365やMS Teams・Zoom・Webexなどウェブ会議の通信を優先させるなど業務アプリの適切な利用を実現するために帯域制御は必須機能になります。

無線LAN化

4. テレワーク（Teleworker VPN）

職員の自宅にMRを置いて
リモートワーク環境を構築可能
Teleworker VPN

課題
専用機器を用意するのは
コストがかかる

無線LAN化

自宅

庁舎

テレワーク・在宅勤務

インターネット

モデム

庁内
インフラ

MX

同一APで業務も
プライベートアクセスも
対応

MR
（Teleworker VPN）

MR

庁内と同じSSID

庁内SSID

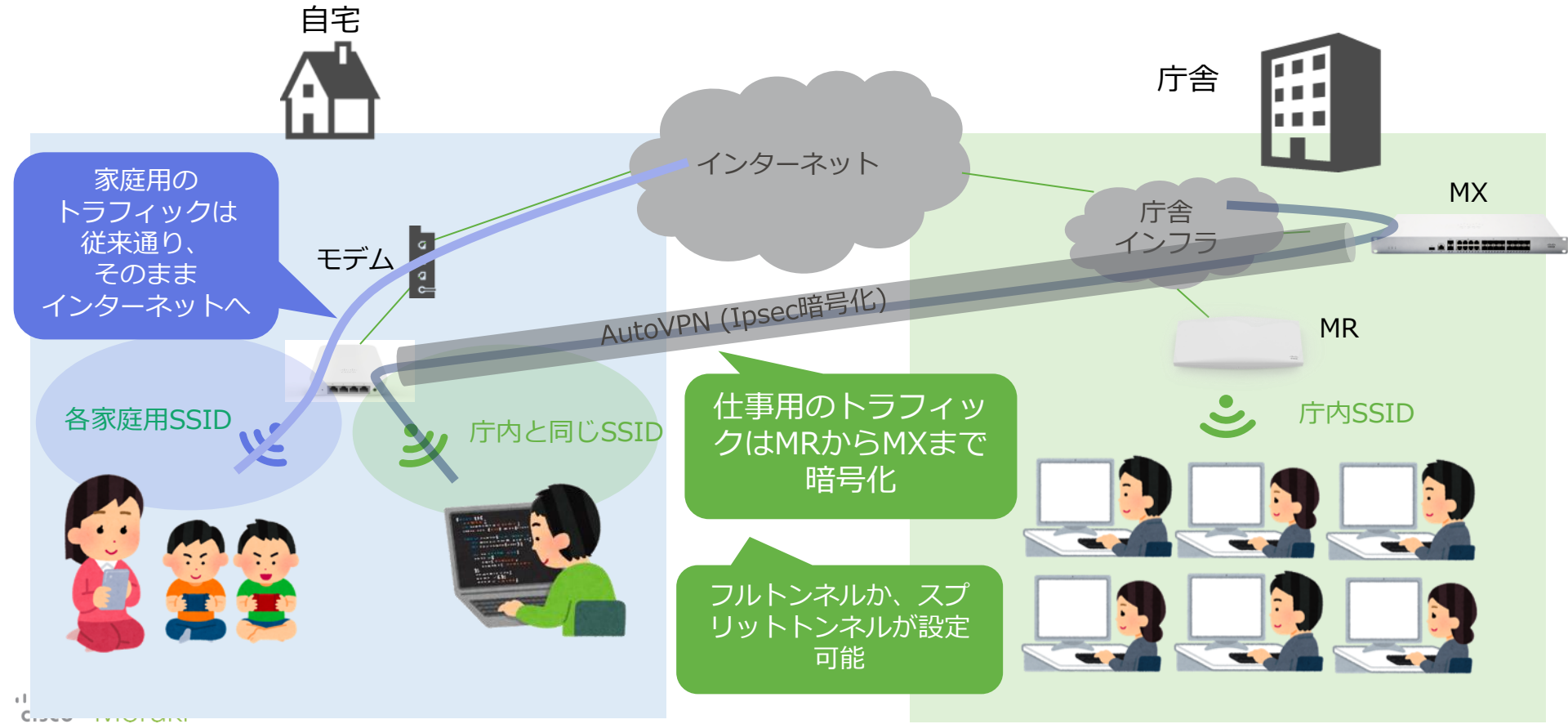
プライベート利用の
SSID追加可能

庁舎と同じ無線環境
端末に設定不要

会社と同じ使い心地を自宅に
提供するアクセスポイント。

Teleworker VPNなら、家庭用の無線LANも共存

無線LAN化



無線AP（MR）でVPN接続
Teleworker VPNのメリット

- ✓ 職員自宅にはAP１台でOK、庁舎にVPN終端用のMXが必要　：　VPNで簡単に暗号化通信ができる
- ✓ AutoVPNテクノロジー　：　庁舎MXも職員自宅APも固定グローバルIP不要
- ✓ 端末に特別な設定不要　：　クライアントVPNのように、VPNソフトウェアのインストールや、設定、管理なしに、庁内と同じように接続ができる。
- ✓ 家庭用の無線LANも共存　：　家庭内のプライベート利用のPCやスマートデバイスは専用のSSIDを設定でき、社内ネットワークと分離してインターネット接続可能、セキュリティも確保
- ✓ 有線機器の利用も可能　：　有線ポートのあるAPは、有線で認証し接続もできる。
- ✓ エンタープライズクラスの電波安定性　：　クラウドが電波の出力やチャネルを自動で調整
- ✓ 管理ポイントはクラウドで一元管理　：　庁内無線設備にもそのまま流用可能

標準機能詳細　：セキュリティ強化

【ポイント】
機器やソフトウェアの改ざんによる情報の抜き取り対策
無線LANの安定したセキュリティ

1. 改ざん防止（Trustworthy/TAM）
2. 無線LANセキュリティ
   （WPA3,不正AP,AirMarshal, Umbrella DNS）

1、改ざん防止（Trustworthy/TAM）

シスコ、ネットワーク製品の強固な改ざん防止システム

課題

ハードウェアにチップの埋め込み
ソフトウエアの改ざん

【不正なチップの埋め込み例】

Figure 8. The Counterfeit A processor board had an "extra" component added.

解決策

Catalyst：ハードウェアとOSに組み込まれた自己診断機能（TrustWorthy）

スイッチ起動時にソフトウェアとハードウェアの信頼性を「アンカー」と呼ばれる独自の情報を事前に設定しています。
このアンカー情報を元に、起動時にハード・OSが正規かつ改ざんがないことをチェックし信頼性・完全性を担保します

Meraki：トラストアンカーモジュールと設定取得時の正当性チェック

ハードウェアとオペレーティングシステムの両方が正当であり、改ざんされていないことを検証するように設計されたシスコ独自のハードウェア（TAM）で構築された、非常に堅牢なハードウェア支援ソリューションです。
クラウド通信リクエストを行うハードウェアの信頼性を検証する手段としてセキュアブートデバイスで使用され、OSが不正に変更されていないことを確認します。TAMは公開鍵と秘密鍵ペアを含み、クラウド通信時にキーのチェックを行います。

2、無線LANセキュリティ

課題

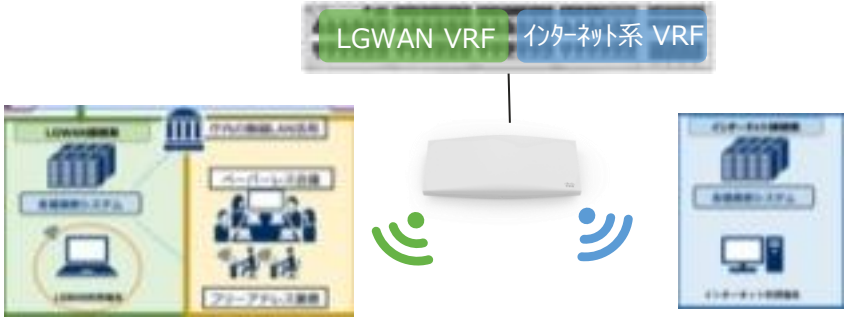
- インターネット系とLGWAN系のネットワークを分離したい
- 不正なAPを設置されて、情報が抜かれないか心配
- 職員以外が無線に接続してこないか心配
- 総務省のガイドラインに適合したい

2、無線LANセキュリティ

課題

- インターネット系とLGWAN系のネットワークを分離したい
- 不正なAPやを設置されて、情報が抜かれないか心配
- 職員以外が無線に接続してこないか心配
- 総務省のガイドラインに適合したい

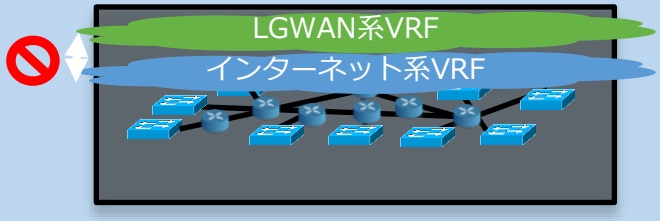
Catalyst9000シリーズスイッチ VRF



解決

インターネット系とLGWAN系の**論理分離**

ネットワーク分離をVLANとACL（アクセスリスト）機能を用いて行う方法がありますが、設計が複雑となり、設定の意図の把握・管理が難しいという課題がありました。仮想ルーティング（VRF）機能を用いることにより、**明確にインターネット系とLGWAN系シンプルな設計で論理的に分離**し、安全に利用することができます。



cisco Meraki

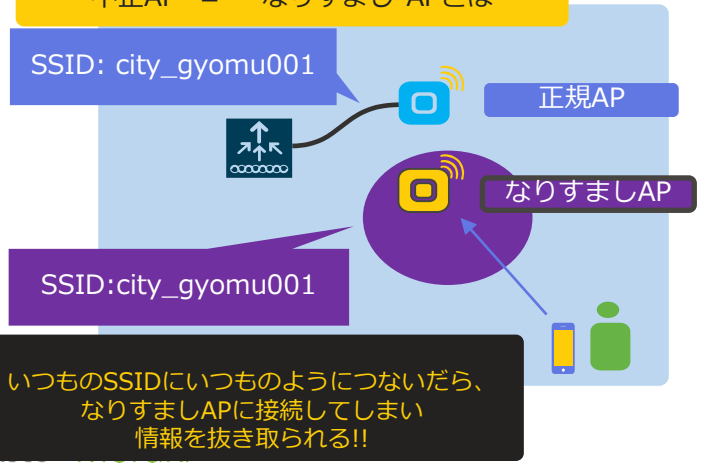
セキュリティ強化

2、無線LANセキュリティ

課題

- インターネット系とLGWAN系のネットワークを分離したい
- 不正なAPを設置されて、情報が抜かれないか心配
- 職員以外が無線に接続してこないか心配
- 総務省のガイドラインに適合したい

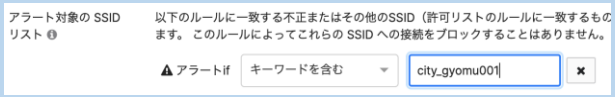
不正AP　＝　“なりすまし”APとは



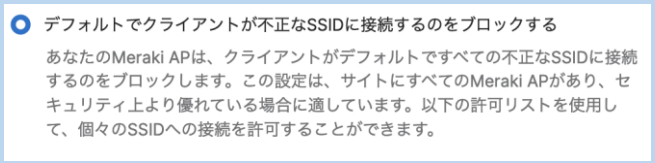
いつものSSIDにいつものようにつないだら、
なりすましAPに接続してしまい
情報を抜き取られる!!

解決

不正APの検知（アラートの生成）



クライアントが不正なSSIDに接続するのをブロック



※参考：SSIDをステルスにしても、ツールで簡単に見えるため、なりすまし対策にはなりません。

2、無線LANセキュリティ

課題

- インターネット系とLGWAN系のネットワークを分離したい
- 不正なAPを設置されて、情報が抜かれないか心配
- 職員以外が無線に接続してこないか心配
- 総務省のガイドラインに適合したい

解決

盗聴防止　通信の暗号化　＊通信の「覗き見」をさせません

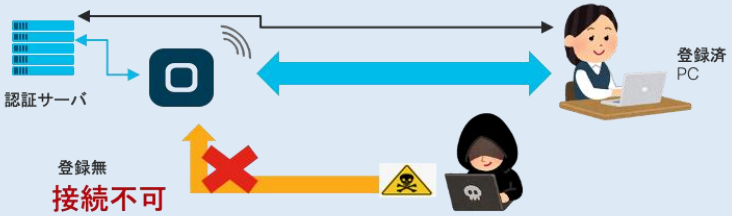
対策方法　（WPA2またはWPA3）

暗号化の仕組みとして
AESが定義されています。

【必要機器】
アクセスポイント
(Meraki MRシリーズ)

解決

不正アクセス防止　＊「登録されていない端末を接続」させません



対策方法
WPA2/3-Enterprize
認証サーバを用いることで、端末毎に
ID/Passwordを登録し、登録外の端末を
接続させません。
【必要機器】
APと、認証サーバ(ISE)

共通のID/Passwordを利用することは、Passwordの漏洩リスクが高いため、業務用では推奨しません。

cisco Meraki

2、無線LANセキュリティ

課題

- インターネット系とLGWAN系のネットワークを分離したい
- 不正なAPを設置されて、情報が抜かれないか心配
- 職員以外が無線に接続してこないか心配
- 総務省のガイドラインに適合したい

解決

対応済み
（詳細は次頁）

- 2013年１月　『企業が安心して無線LANを導入.運用するために』総務省　http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000035.html

安全のためのセキュリティ対策

セキュリティ強化

課題

- 総務省のガイドラインに適合したい

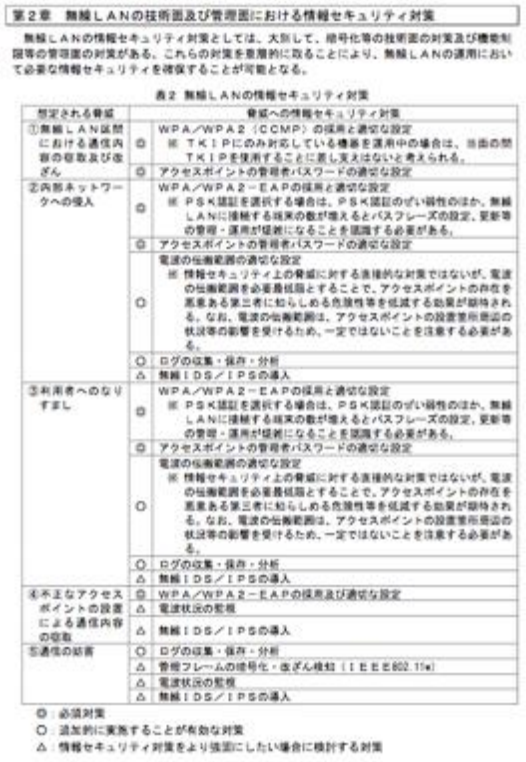
▪ 参照URL:　2013年１月　『企業が安心して無線LANを導入.運用するために』
総務省　http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000035.html


企業等が安心して
無線LANを導入・運用するために

総　務　省
平成25年1月30日

抜粋

- 認証、暗号化は必須項目です。
- 不正機器対策や侵入防御、通信の妨害への対応が推奨されています。


第２章　無線ＬＡＮの技術面及び管理面における情報セキュリティ対策

無線ＬＡＮの情報セキュリティ対策としては、大別して、暗号化等の技術面の対策及び機能制限等の管理面の対策がある。これらの対策を意識的に取ることにより、無線ＬＡＮの運用において必要な情報セキュリティを確保することが可能となる。

表２ 無線ＬＡＮの情報セキュリティ対策

想定される脅威		脅威への情報セキュリティ対策
①無線ＬＡＮ区間における通信内容の窃取及び改ざん	◎	ＷＰＡ／ＷＰＡ２（ＣＣＭＰ）の採用と適切な設定 ※ ＴＫＩＰにのみ対応している機器を運用中の場合は、当面の間ＴＫＩＰを採用することに差し支えないと考えられる。
	○	アクセスポイントの管理者パスワードの適切な設定
②内部ネットワークへの侵入	◎	ＷＰＡ／ＷＰＡ２－ＥＡＰの採用と適切な設定 ※ ＰＳＫ認証を選択する場合は、ＰＳＫ認証のぜい弱性のほか、無線ＬＡＮに接続する端末の数が増えるとパスフレーズの設定、更新等の管理・運用が煩雑になることを認識する必要がある。
	○	アクセスポイントの管理者パスワードの適切な設定
	○	電波の伝搬範囲の適切な設定 ※ 情報セキュリティ上の脅威に対する直接的な対策ではないが、電波の伝搬範囲を必要最低限とすることで、アクセスポイントの存在を悪意ある第三者に知らしめる危険性等を低減する効果が期待される。なお、電波の伝搬範囲は、アクセスポイントの設置箇所周辺の状況等の影響を受けるため、一定ではないことを注意する必要がある。
	○	ログの収集・保存・分析
	△	無線ＩＤＳ／ＩＰＳの導入
③利用者へのなりすまし	◎	ＷＰＡ／ＷＰＡ２－ＥＡＰの採用と適切な設定 ※ ＰＳＫ認証を選択する場合は、ＰＳＫ認証のぜい弱性のほか、無線ＬＡＮに接続する端末の数が増えるとパスフレーズの設定、更新等の管理・運用が煩雑になることを認識する必要がある。
	○	アクセスポイントの管理者パスワードの適切な設定
	○	電波の伝搬範囲の適切な設定 ※ 情報セキュリティ上の脅威に対する直接的な対策ではないが、電波の伝搬範囲を必要最低限とすることで、アクセスポイントの存在を悪意ある第三者に知らしめる危険性等を低減する効果が期待される。なお、電波の伝搬範囲は、アクセスポイントの設置箇所周辺の状況等の影響を受けるため、一定ではないことを注意する必要がある。
	○	ログの収集・保存・分析
	△	無線ＩＤＳ／ＩＰＳの導入
④不正なアクセスポイントの設置による通信内容の窃取	◎	ＷＰＡ／ＷＰＡ２－ＥＡＰの採用及び適切な設定
	△	電波状況の監視
	△	無線ＩＤＳ／ＩＰＳの導入
⑤通信の妨害	○	ログの収集・保存・分析
	△	管理フレームの暗号化・改ざん検知（ＩＥＥＥ802.11w）
	△	電波状況の監視
	△	無線ＩＤＳ／ＩＰＳの導入

◎：必須対策
○：追加的に実施することが有効な対策
△：情報セキュリティ対策をより強固にしたい場合に検討する対策

総務省 企業向け無線LANセキュリティガイドライン

セキュリティ強化

クラウド管理型を導入する事で、重要な項目に対応することが可能です。

情報セキュリティ対策に関する手引書「企業等が安心して無線LANを導入・運用するために」

http://www.soumu.go.jp/main_content/000199320.pdf

ガイドライン記載「想定される脅威」	ガイドライン項目		対応方法	
	優先度	セキュリティ対策	対応	技術内容
①無線 LAN 区間における通信内容の窃取及び改ざん	必須	WPA / WPA2 (CCMP) /WPA3の採用と適切な設定	◎	**WPA / WPA2/WPA3 機能を実装**
②内部ネットワークへの侵入	必須	パスワードや電子証明書を利用したアクセス制御・認証 管理者用パスワードの設定	◎	**IEEE 802.1x 認証に対応** **各機器に管理者用パスパード設定可能**
③利用者へのなりすまし	高	電波の伝搬範囲の適切な設定	◎	**自動調整機能および手動での設定可能**
	高	ログの収集・保存・分析	◎	**クラウドダッシュボードで提供**
④不正なアクセスポイントによる通信内容の窃取	高	無線 IDS / IPS の導入	◎	**監視用アンテナと** **クラウドダッシュボードで提供**
⑤通信の妨害	中	電波状況の監視	◎	**監視用アンテナと** **クラウドダッシュボードで提供**
	低	管理フレームの暗号化・改ざん検知（IEEE 802.11 w）	◎	**IEEE 802.11 w 機能を実装済み**

cisco Meraki

セキュリティ強化

2、無線LANセキュリティ

セキュリティ強化

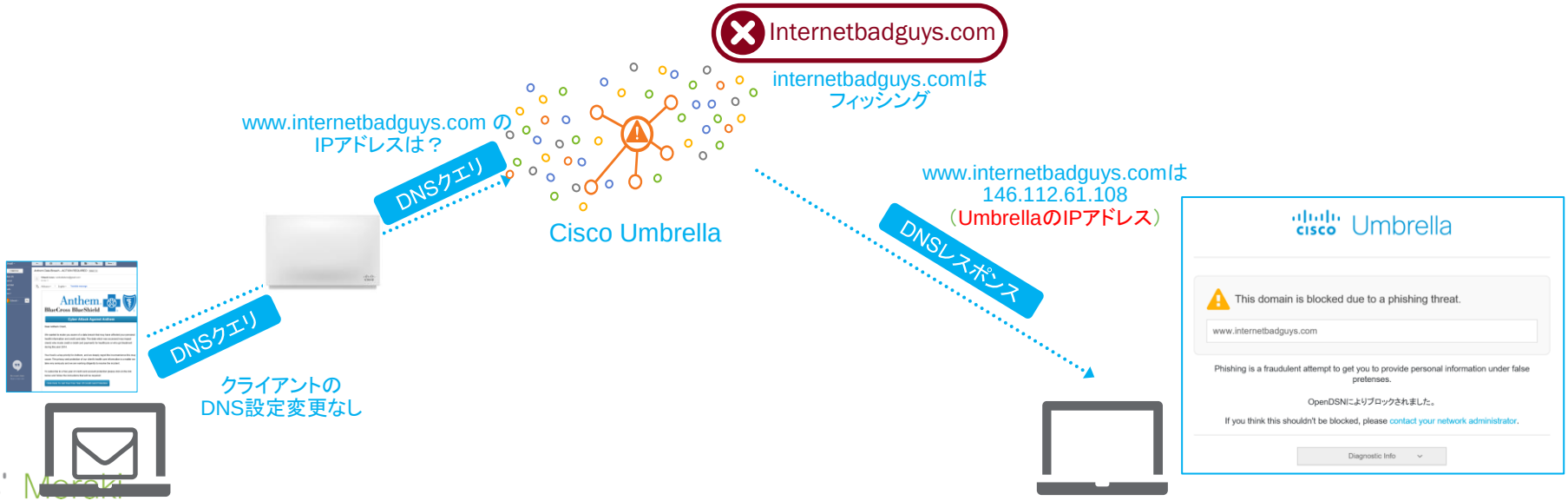
2、無線LANセキュリティ

cisco Meraki

セキュリティ強化

2、無線LANセキュリティ

1. ブラウザがフィッシングメールにあるURLの解決を要求する
2. MRがDNSクエリをインターセプトし、識別子を付けてUmbrellaに送信
3. 問い合わされたドメイン/URLの安全性をUmbrellaがチェック (識別子からポリシー判別)
4. ドメインがフィッシングに分類されていることが判明
5. ブロックページ（フィッシングサイト用）のIPアドレスを回答
6. ブラウザがUmbrellaのブロックページを表示



cisco Meraki

まとめ

- 庁内無線LANよる柔軟な職場環境の実現のため、設定と展開がかんたんなクラウドでの運用

- かんたんだけではなく、セキュリティ対策も十分に考慮された安心・安全なCisco Meraki

Thank you