世界で一番、
ネットワークの力を信じている。

PSU Week 2012 September

スマートデバイスを活かす
企業インフラ構築ソリューションのご紹介

シスコシステムズ合同会社
ボーダレスネットワーク事業
プロダクトセールススペシャリスト
荒島　麻依子

スマートデバイスの導入および利活用に向けてのアプローチ

スマートデバイスに対応したセキュリティ基盤の構築にあたって

スマートデバイスという名の
「電話機能のついた小型のPC」が社内から
リモート環境に持ち出されるという点のみの違い

今、企業内で通常稼働しているPCに適応されている
「セキュリティレベル」をスマートデバイスにも適応し
セキュリティレベルを同一化する(差分を無くす)

スマートデバイスの社内利用によって生じるリスク

- 管理外のデバイスからのアクセス
- 端末の紛失等による情報漏洩
- 生産性や効率性の低下

具体的には

スマートデバイスを活かす
セキュアなアクセス環境の整備
（社内・社外）

個体識別された端末が社外からネットワーク
接続する際は強制的にVPNに接続

使う人・デバイス・シチュエーションを
意識したアクセス制御

スマートデバイス導入時の検討ポイント

①セキュアなアクセス環境

②認証・認可制御

③端末管理

- Wireless LAN
- リモートVPN
- Webセキュリティ

- 端末認証
- ユーザー認証
- デバイスプロファイリング
- 検疫
- ゲストアクセス認証

- MDM
- アンチウイルス対策

シスコのスマートデバイスソリューション

ポイント

シスコでは、スマートデバイス導入に対応したネットワークから認証までラインナップを展開。全体最適を実現するソリューションの提案に対応。

WirelessLAN

Cisco
Aironet シリーズ

Webセキュリティ

IronPort WSA
ASA CX

リモートVPN

CiscoAnyConnect
セキュア モビリティ

Cisco
ASA 5500-X

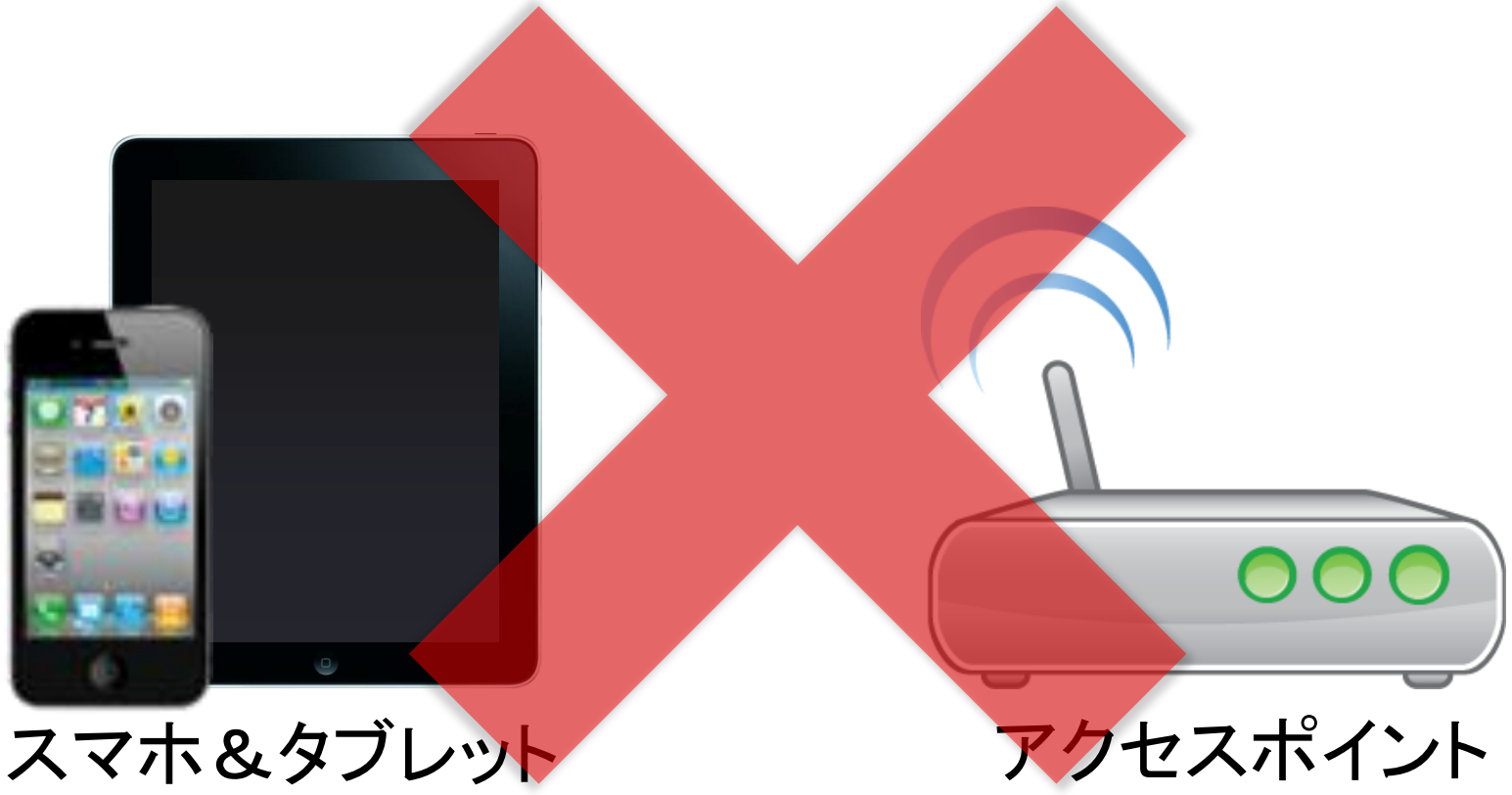
端末認証
ユーザー認証
デバイスプロファイリング
検疫
ゲストアクセス認証

Cisco
Identity Services Engine
(ISE)

Wireless LAN

Cisco
Aironet シリーズ

オフィスでスマートデバイスを使いたい



オフィスでスマートデバイスを使いたい

スマホ＆タブレット

アクセスポイント

PoE スイッチ

- WPA2 エンタープライズ
- AES暗号
- 安定稼働（IEEE802.11n）
- 干渉源を排除するClean Airテクノロジー

- 革新的な企業向けエネルギー管理システムEnergyWise

シスコIEEE802.11n対応アクセスポイント一覧

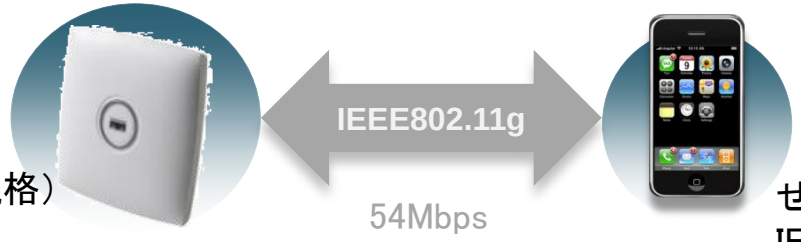
	1260	3500e	3600e	1040	1140	3500i	3600i
							
MIMO	2x3	2x3	4x4	2x2	2x3	2x3	4x4
Stream数	2	2	3	2	2	2	3
動作温度	-20-55℃	-20-55℃	-20-55℃	0-40℃	0-40℃	0-40℃	0-40℃
PoE対応	802.3af	802.3af	802.3af	802.3af	802.3af	802.3af	802.3af
アンテナバリエーション	あり	あり	あり	なし（内蔵）	なし（内蔵）	なし（内蔵）	なし（内蔵）
5GHz帯対応バンド	W52/W53/W56	W52/W53/W56	W52/W53/W56	W52/W53	W52/W53	W52/W53/W56	W52/W53/W56
サイズ(本体のみ、cm)	22.1 x 22.1 x 4.7	22.1 x 22.1 x 4.7	22.1 x 22.1 x 5.4	22.1 x 22.1 x 4.7	22.1 x 22.1 x 4.7	22.1 x 22.1 x 4.7	22.1 x 22.1 x 5.4
重量(本体のみ)	1.04kg	1.04kg	1.13kg	1.04kg	1.04kg	1.04kg	1.13kg
電波自動調整	○	○	○	○	○	○	○
不正AP検出	○	○	○	○	○	○	○
ClientLink	○	○	○(2.0)	×	○	○	○(2.0)
CleanAir	×	○	○	×	×	○	○
バンドセレクト	○	○	○	○	○	○	○
Video over WiFi	○	○	○	○	○	○	○
自律モード	○	×	×	○	○	×	×

最新のスマートデバイスは、すべて11n対応です！

IEEE802.11n対応！　もちろんタブレットPCやノートPCも！
さらにスマホ導入済、あるいは検討段階の企業はすでに40%越え(*)！

(*) 富士キメラ総研　2012法人向けスマートフォン関連 ビジネスの全貌 より

なのに、お客様のインフラ（AP）は11n未対応ではないですか？！



AP1131シリーズ
IEEE802.11a/b/g（旧規格）

せっかく端末は、新規格の
IEEE802.11n対応なのに・・・

エンタープライズ仕様なアクセスポイント

- ほこり・ちりが入り込まない密閉筐体
- 11nで安定かつ高速

AP1140 / AP3600iシリーズ

- アンテナ内蔵ですっきりデザイン
- 店内向けに最適

天井設置イメージ

AP1260 / AP3600eシリーズ

- −20℃～55℃の動作保証
- 駅ホーム、商店街等向けに最適
- 天井裏に本体、天井表面に天井マウントアンテナという組み合わせも可

天井マウントアンテナ
設置イメージ

アクセスポイント Aironet 3600シリーズ

世界最速！IEEE802.11n 450Mbps 対応

業界初4x4 MIMO による 高パフォーマンス化

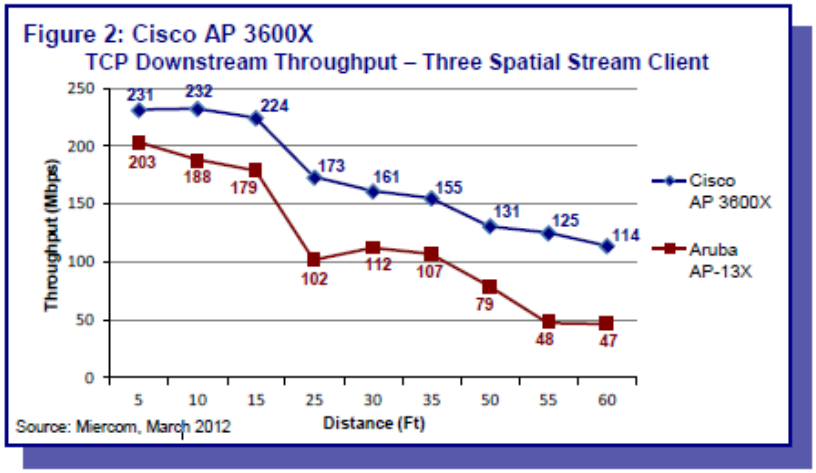
さらなる速度と信頼性のための冗長アンテナデザイン

ClientLink 2.0

全モバイルデバイスのパフォーマンスをさらに向上

CleanAir テクノロジー

もちろん強力なスペクトラム分析による電波監視も搭載



Miercom が Aruba社製品（世界2位）とAironet 3600をラボで徹底比較！

平均67% Aruba社より高いスループットを記録

スマホバッテリー接続時間が38%向上

Cisco CleanAir テクノロジー

高精度干渉検出、分類、チップ レベルでの干渉緩和

検出 | 分類 | 緩和

- CleanAir 専用 ASIC
- Wi-Fi および Wi-Fi 以外の干渉源を検出
- Wi-Fi パフォーマンスへの影響を評価
- 干渉発生によって予防的にチャネルを変更
- 無線品質を監視

通信品質の可視化を実現

リモートVPN　その1

Cisco AnyConnect
セキュア モビリティ クライアント

Cisco AnyConnectセキュアモビリティ クライアント

圧倒的な導入実績

グローバル
⇒8,000万ライセンス

日本
⇒　100万ライセンス

Cisco AnyConnectセキュアモビリティ クライアント

常時接続アクセスを自動で実現 ※
Always On/On-Demand対応による自動再接続

※アプリケーション等によりVPN接続の除外設定を考慮する必要あり

ワンクリックでVPN接続を実現
デバイス証明書連携でVPN認証を実現

統合クライアント
VPN / Wi-Fi / Webセキュリティ / 検疫

マルチデバイス対応
Windows / MAC OS X / iOS /Android OS

構成プロファイルの自動適用
Cybertrust社やVeriSign社の連携

対応OS一覧

2012年8月現在

AnyConnect 3.1		AnyConnect 2.5.X for Apple iOS		AnyConnect2.5.X for Android	
Windows	7 SP1 Vista SP2 XP SP3	iPad/iPad 2 WiFi and 3G	4.2.1 or later	Android VPN Framework in Android 4.0 Devices ※	
Mac OS	10.5 or later	iPhone 3G/3GS/4	4.1 or later	Samsung	Galaxy S, Galaxy SⅡ, Galaxy Tab 7/8.9/10.1
Linux		iPhone 4S	5.0 or later	HTC	Desire, EVO, Flyer etc
		iPod Touch (2nd Generation or later)	4.1 or later	Motorola	ATRIX, XYBOARD, RAZR , RAZR etc.

※ Android 4.0 以降を実行する未サポートのデバイスには、AnyConnect AVF クライアントを推奨します。サポートされているデバイスでは、Android OS バージョンに関係なく、ブランドに固有の AnyConnect クライアントを使用する必要があります。

※ AVF は、基本的な VPN 接続のみ提供します。このような基本的 VPN 機能に依存する AnyConnect AVF クライアントでは、ブランド固有のパッケージが持つフルセットの VPN 機能が提供されません。

対応デバイスに関してはCisco AnyConnect セキュア モビリティ クライアントのリリースノーツまたはCisco AnyConnect セキュア モビリティ クライアント ユーザ ガイドにて必ずご確認ください。これら資料はシスコシステムズ合同会社のウェブサイトに掲載されております。

スマートデバイス向け AnyConnect 2.5.x

スマートデバイス向けAnyConnect 2.5.x

- **AnyConnect for iOS**

  iPhone/iPod Touch (iOS 4.1以降) およびiPad (iOS4.2.1以降)でサポート

  AnyConnect 2.5.4 でGUIの日本語化対応

- **AnyConnect for Android**

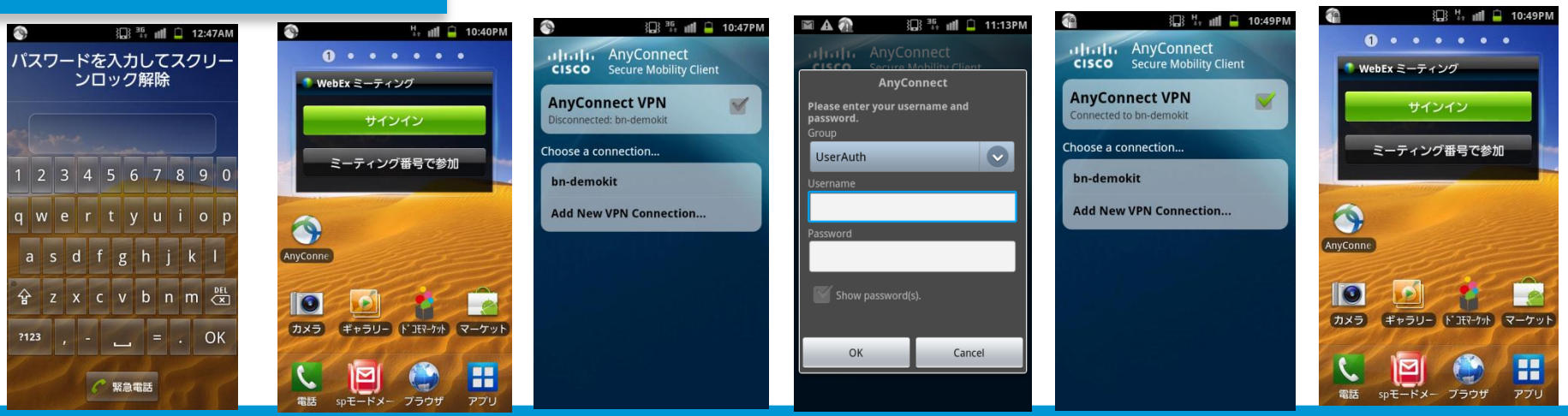
  Samsung GALAXY S/S2/Tab (Android OS 2.3.3以降), Android OS 4.0のほぼ全てのデバイスに対応

  (※最新の情報はGoogle Play (Android Market) で検索)

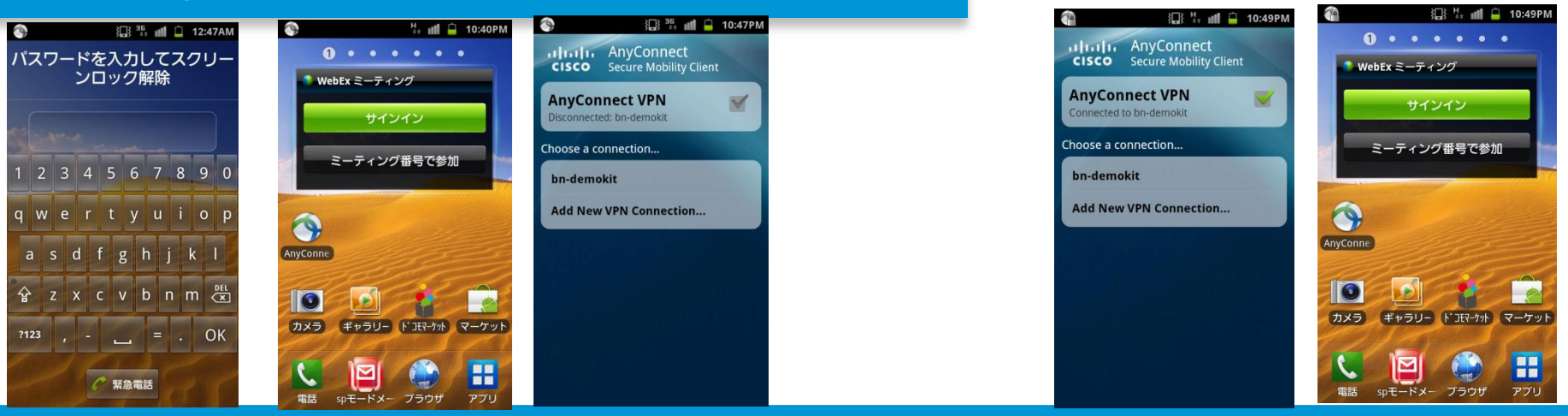
Cisco ASAとの連携	iPhone/iPad	Android端末
AnyConnect (SSL VPN)	○ iOS4.1/4.2.1以降	○ 端末に依存
端末標準のVPN (L2TP over IPsec)	○	○ Android2.1、ASA8.4(1)以上

デバイス証明書利用によるワンクリックVPN

ID/PW認証のVPN



デバイス証明書利用によるワンクリックVPN



「VPN+ 端末識別（証明書）」リモートアクセスソリューション事例

導入事例

ソフトバンクグループ3 社

利用端末：**15,000台以上の iPhone/iPad**

利用用途：リモートアクセスでの端末認証

KDDI

国内初Android大規模事例

利用端末：**2,000台以上の Android**（XOOM）

利用用途：リモートアクセスでの端末認証

サービス化事例

ソフトバンクテレコム

セキュアリモートゲートウェイサービス（**iPhone/iPad対応**）

三菱電機情報ネットワーク

セキュアスマートフォンアクセスサービス（**iPhone/iPad対応**）

NRIセキュアテクノロジーズ

スマートフォン向け端末認証サービス（**iPhone/iPad対応**）

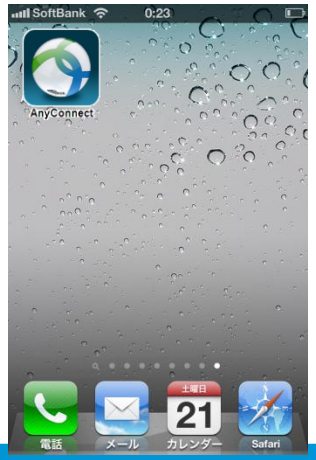
京セラコミュニケーションシステム

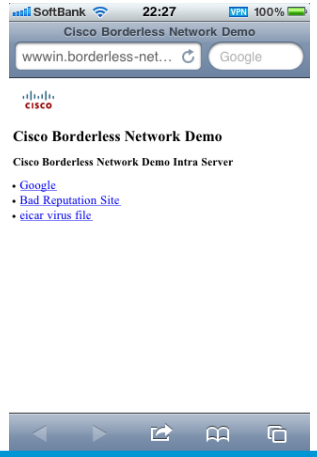
スマートデバイス端末認証サービス（**iPhone/iPad対応**）

オンデマンドVPNによる自動接続VPN（iPhone/iPadのみ）

予め指定されたドメイン(URL)を閲覧する際に自動的にVPN接続が実行。
※オンデマンドVPNを利用するにはデバイス証明書が必須。

オンデマンドVPNによる自動接続VPN



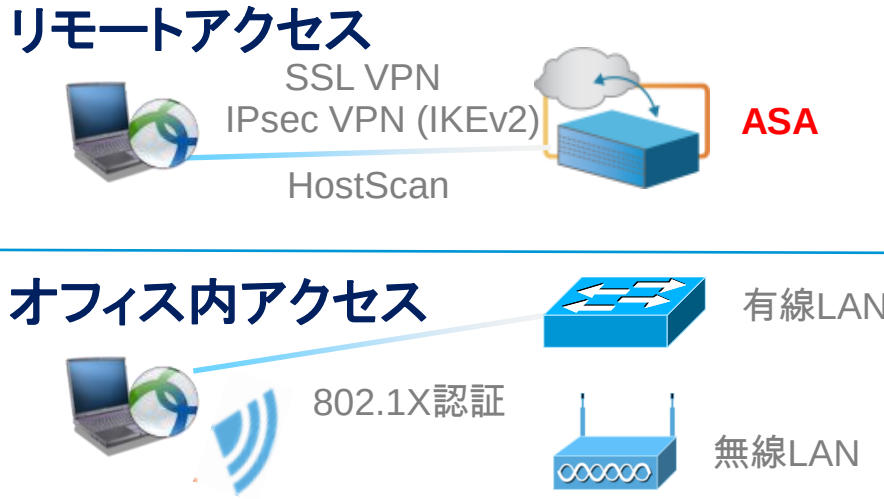


Cisco AnyConnectセキュアモビリティ クライアント 3.1

AnyConnect 3.1

あらゆるシチュエーションに対応

- リモートアクセス：SSL or IPsec/IKEv2 VPNクライアント
- オフィス内アクセス：有線LAN,無線LANの接続管理や802.1Xサプリカント機能
- インターネットアクセス：Webセキュリティ機能



すべてのモバイルワーカーに対応

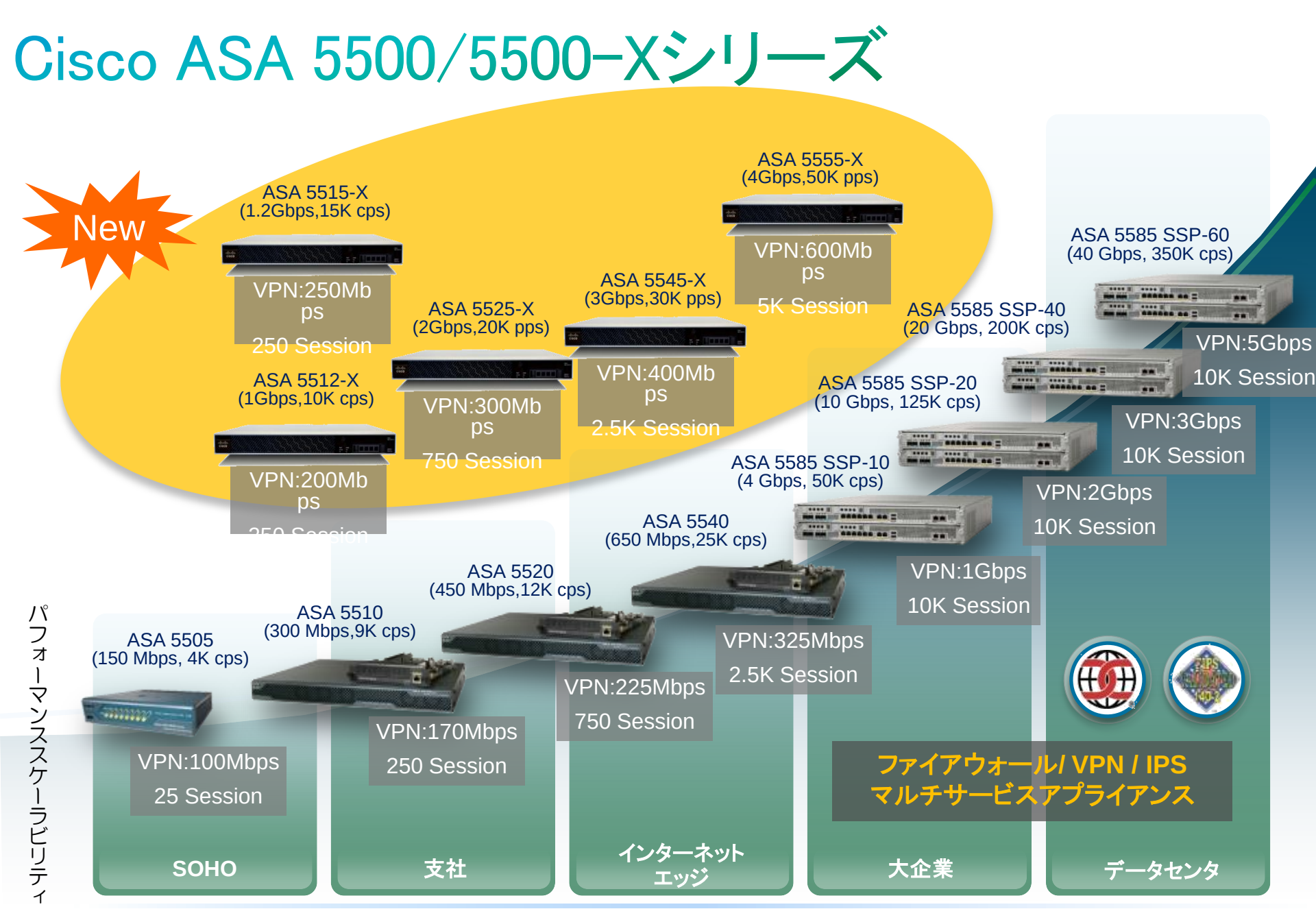
- エンドポイントに必要な機能を統合した　次世代クライアントソフトウェア
  - **VPN クライアント:**
    SSL + IPsec(IKEv2) VPNクライアント
  - **ネットワークアクセスマネージャ:**
    Wired / Wireless コネクション管理
  - **Web セキュリティ**:
    SaaS型 web securityクライアント
  - **検疫**:
    HostScan
  - **テレメトリー**:
    Endpoint telemetry feeds
  - **レポート**:
    Logging, Troubleshooting

- **Tray Icon**
- **Connected**
- **Attention**
- **Error**
- **Connection Transition**

リモートVPN　その2

Cisco ASA 5500
ASA 5500-X

Cisco ASA 5500/5500-Xシリーズ



リモートVPN　その3

Cisco AnyConnect

+

Cisco ASA 5500(-X)

Cisco ASAのリモートアクセスVPN

- ASA 5500（－X）では2種類のVPNプロトコルを採用しています。
- VPN利用時には専用ライセンス（別途解説）をご購入ください※。
- VPN用ライセンスは恒久利用ライセンスです（年更新不要）。

SSL VPN

Clientless VPN(WebVPN)
= SSL/TLS

AnyConnect (SSL)
=TLS/DTLS

ブラウザ(Clientless)

AnyConnectクライアント
(PC, スマートデバイス)

- クライアントソフトウェア or ブラウザでのアクセス
- 機能が豊富(提案の幅が広い)

IPsec

AnyConnect (IPsec)
=IPsec/IKEv2

AnyConnectクライアント
(PCのみ)

- クライアントソフトウェア必須
- 過去：Cisco VPN Client(IPsec/IKEv1)

【参考資料】AnyConnectライセンス一覧

- **AnyConnect Premium License** (ASA5500-SSL-nn) nnはユーザ数

  AnyConnect、Clientless SSL-VPN、CSD（HostScan含む）の機能をすべて利用できるライセンス。同時接続ユーザ数単位で必要（注1）。

- **AnyConnect Essentials License** (ASA-AC-E-55xx) 55xxは筐体モデル

  ASAの筐体のSSL-VPN接続数の上限までAnyConnectが利用できる安価なライセンス。ASAの筐体に1つで良い（注2）。

- **AnyConnect Mobile License** (ASA-AC-M-55xx) 55xxは筐体モデル

  AnyConnect for iPhone等、モバイルデバイスからのAnyConnectを利用する際に必要となる安価なライセンス。ASAの筐体に1つで良い（注2）。

- **Flex VPN License** (ASA-VPN-FL-nn) nnはユーザ数

  一時的にPremium Licenseに相当するフル機能が必要な場合に利用できる60日間の時限ライセンス。同時接続ユーザ数単位で必要。250ユーザより購入可（注1）。

- **Advanced Endpoint Assessment License** (ASA-ADV-END-SEC)

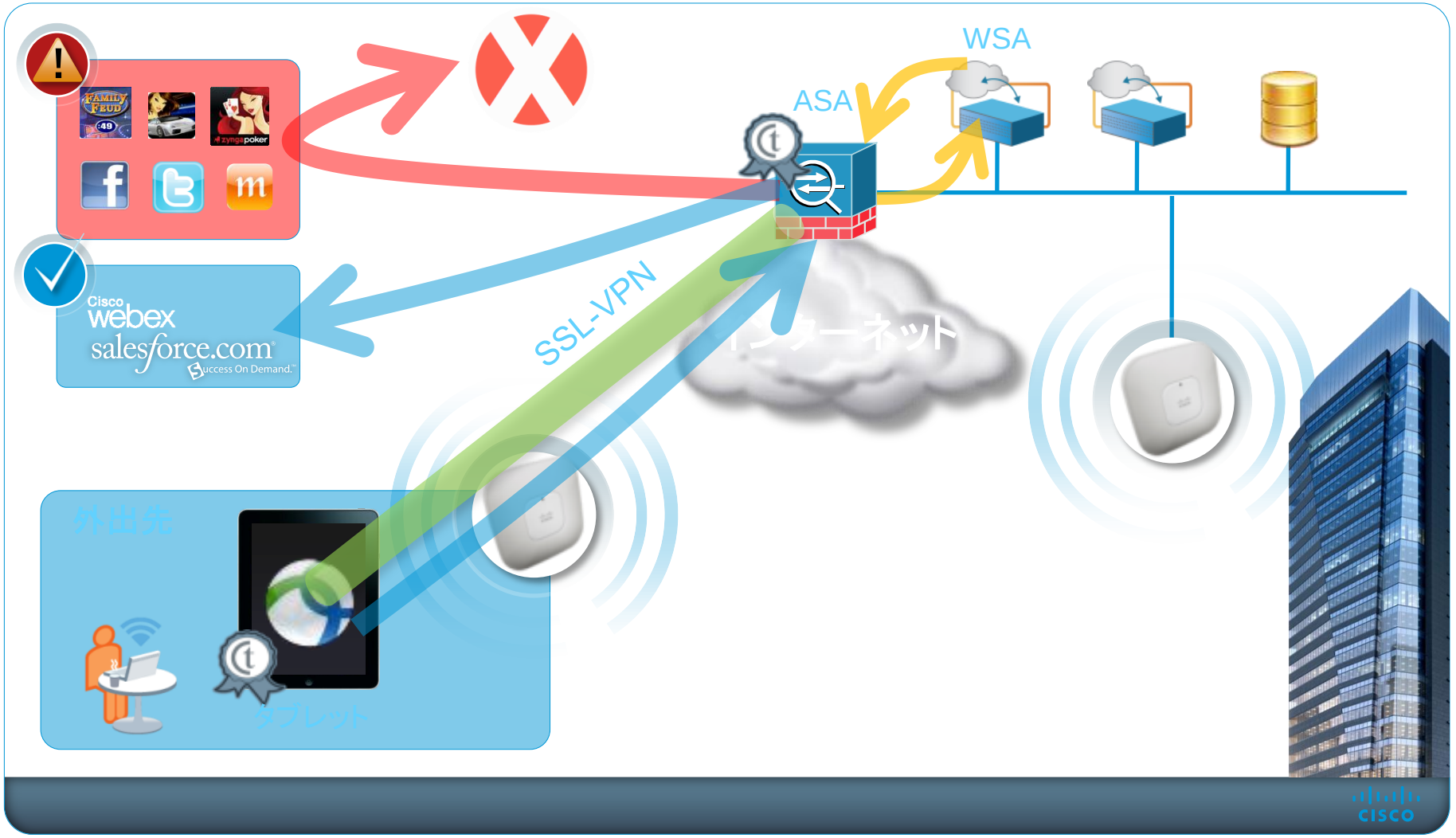
  HostScan実施後に自動修復等を行わせるライセンス。ASAの筐体に1つで良い（注2）。

（注1）ASA8.3以降のFailover構成時であれば、双方のライセンスの合計分を利用可能。
（注2）ASA8.3以降のFailover構成時であれば、どちらかのASAで有効化されていれば良い。

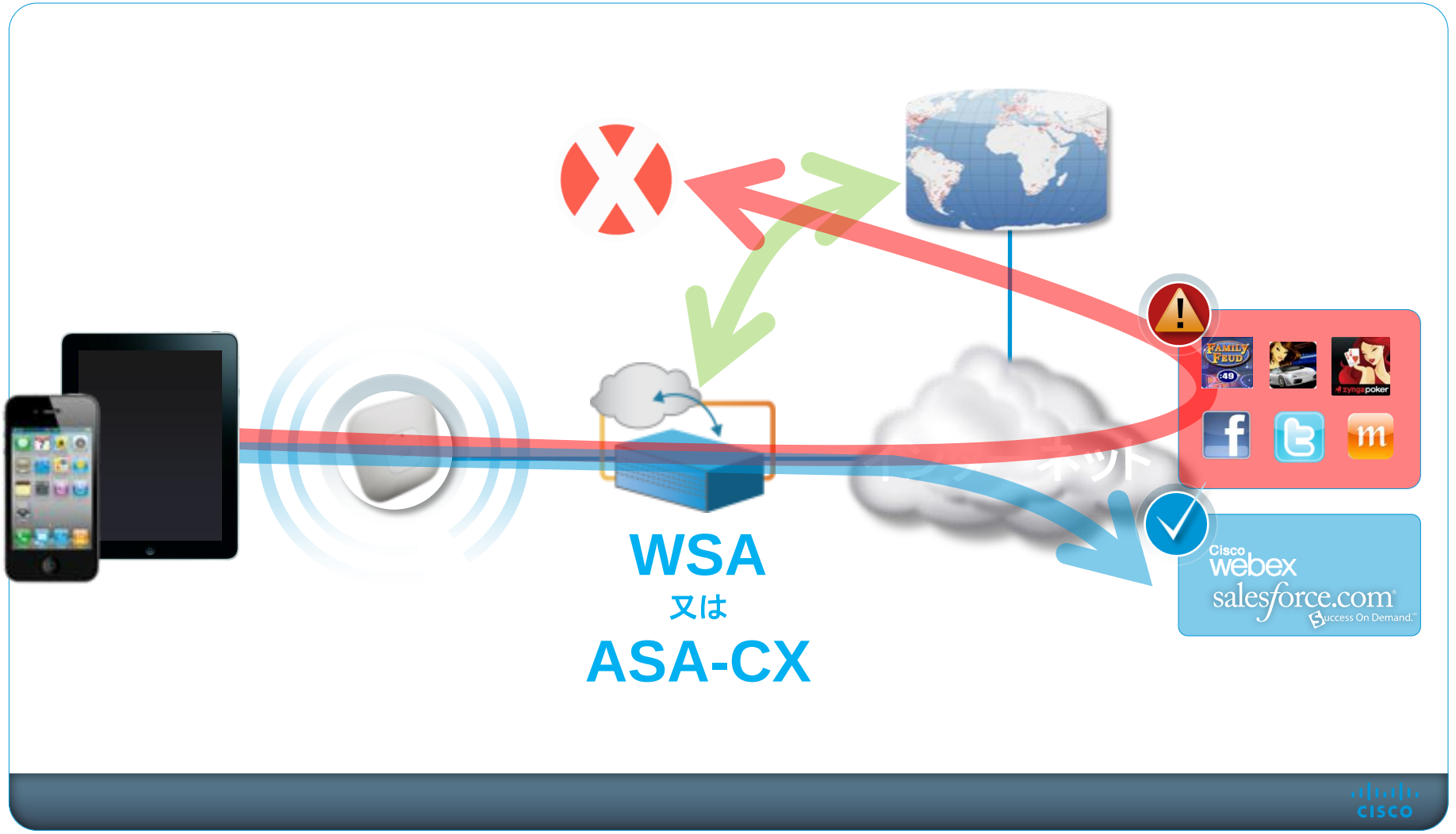
Webセキュリティ
次世代型ファイアウォール

IronPort WSA
or
Cisco ASA CX

【社外】Webセキュリティ for スマートデバイス



【社内】Webセキュリティ for スマートデバイス



選べるWebセキュリティソリューション

IronPort WSA

構成のWebプロキシ/キャッシュエンジン搭載
統合型Webセキュリティアプライアンス

ASA CX

アプリ・ユーザー・デバイスの可視化と制御を実現
次世代型ファイアウォール

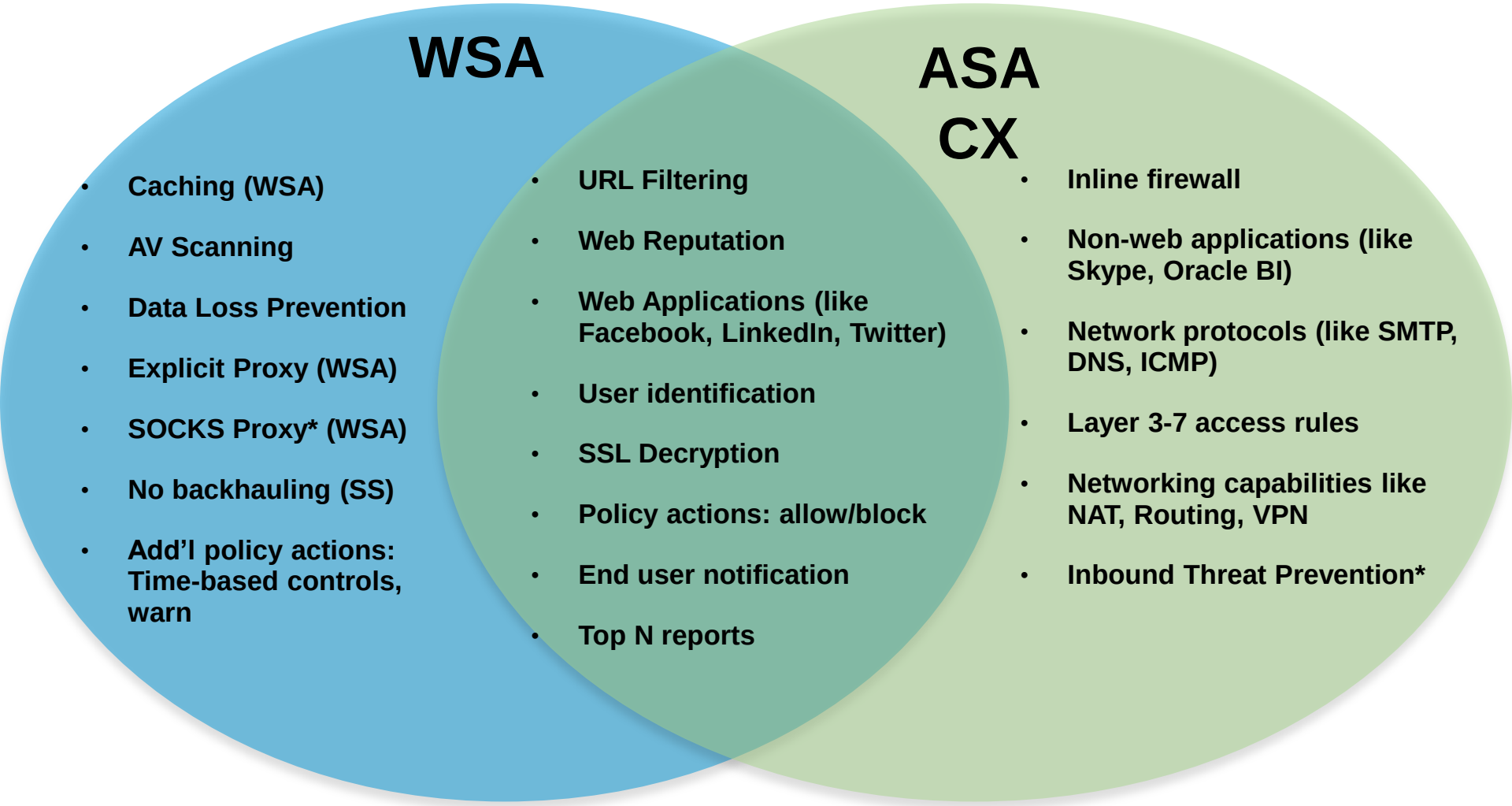
ASA CXとは

- セキュリティの可視化と、カスタマイズ可能なアプリケーション制御機能をもつコンテキスト（利用ユーザーの状態）・アウェアなセキュリティソリューションです。
- ASA 5500-Xにサービスを追加することにより利用可能となります。（ASA5585の場合はアプライアンスとして提供。）

ASA CX （V1）の主な機能

- アプリの可視化と制御
  1000本以上のアプリケーションと7万5000種類以上ものマイクロアプリケーションが制御が可能。
- AD (CD) Agent, NTLM, Kerberos経由でのユーザ識別
- AnyConnectとUser Agent Stringsを利用したデバイス識別
- カスタムカテゴリーを含むURLフィルタ
- 悪意のあるWebサイトへのアクセスをブロックするWebレピュテーション
  世界最大級の規模で運用されているシスコのセキュリティ情報提供サービス Cisco SIO（Security Intelligence Operations）からの脅威情報の配布。
- SSL復号
  SSL暗号化に関らずアプリケーションの識別が可能。

ASA CX & WSA: 違いは？



シスコのグローバルセキュリティ解析センター
SIO（Security Intelligence Operations）

全世界に約30万センサーを展開する
Ciscoのハニーポット

全世界に約70万センサーを展開する
Ciscoのセキュリティアプライアンス

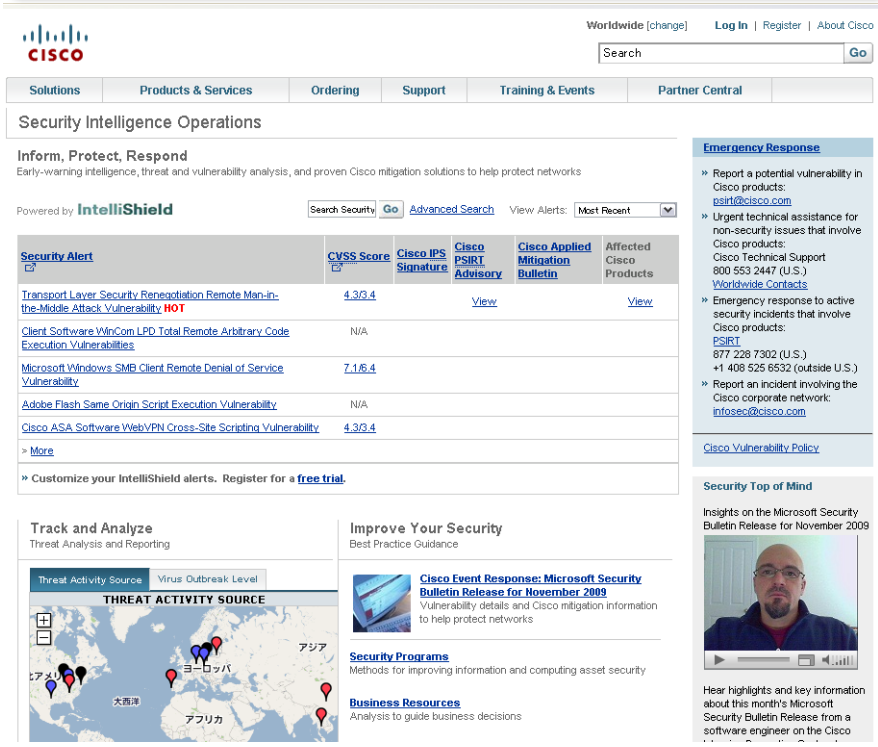
リアルタイムに約100万台のセンサーから集約される
「セキュリティ“ビッグデータ”」

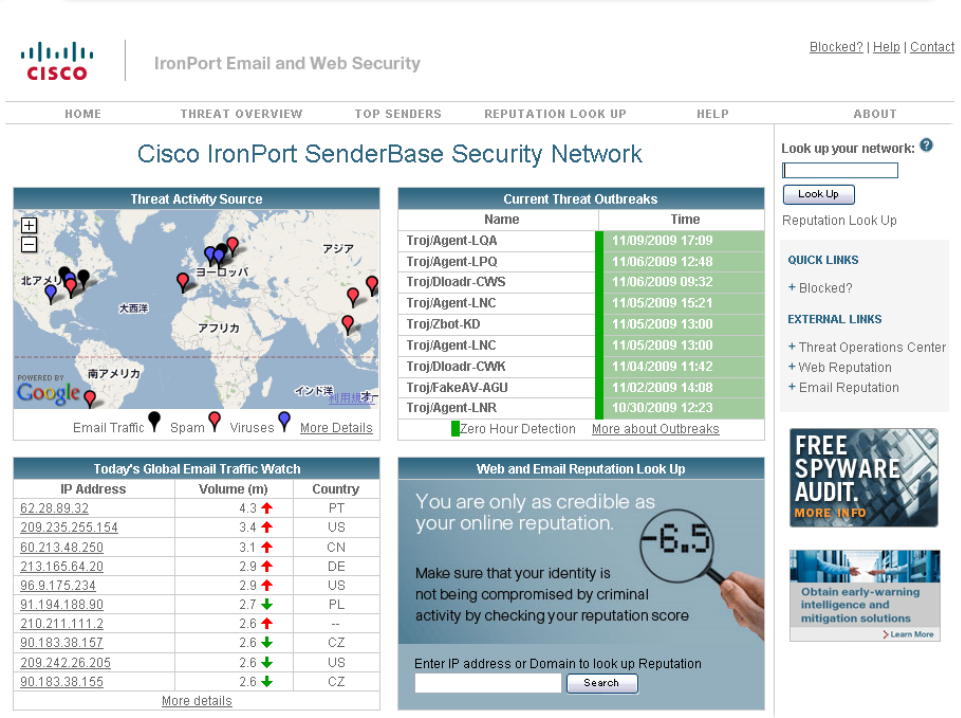

cisco
SIO
200x200
評価されるパラメータとスコア数
1,000,000
世界中に展開する情報収集デバイス
+
50億
HTTP://
1日のWEBリクエスト
10億
1日でサンプリンリングする電子メール数
35%
サンプリングする全世界のインターネットトラフィック
SensorBase
Threat Operations
Dynamic Updates

Cisco SIO WebサイトやSenderBaseサイトから標的型攻撃 (APT) の分析に必要な情報を無償提供

アラートや最新のセキュリティニュース、
今起きている脅威を発信

IronPort Email & Web Security Applianceで
利用するレピュテーション情報を公開

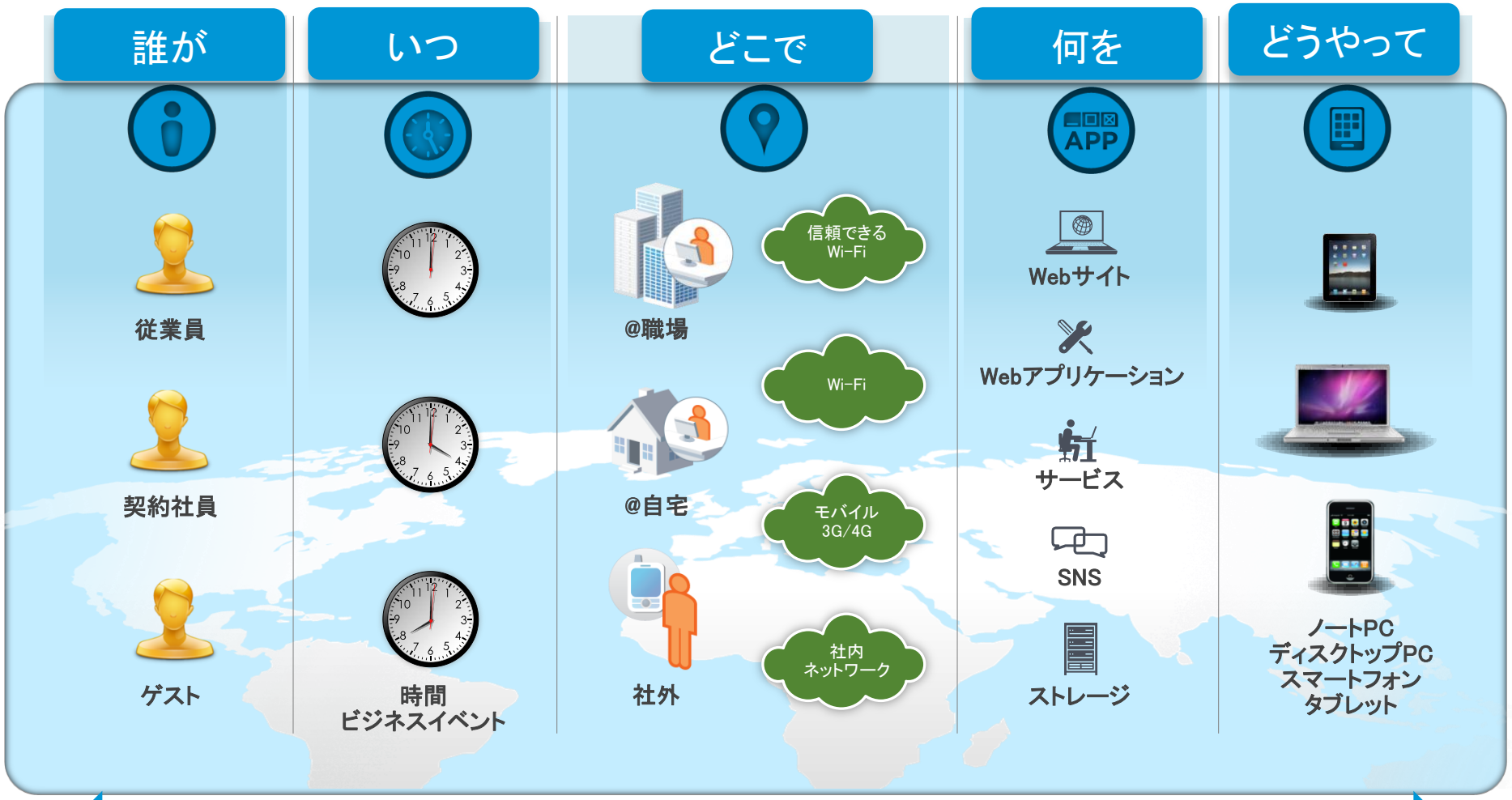




多要素認証
アクセス制御
ポリシー管理

Cisco
Identity Service Engine
(ISE)

ユーザ、デバイスの置かれた状態＝コンテキスト



シチュエーションに基づいたポリシーの適用

ISE（Identity Services Engine）コンセプト

シチュエーションに基づきダイナミックにポリシーを割り当て

CISCO SOLUTION

社内NWへログイン時に全ての
デバイスをプロファイリング

ユーザの所有するデバイス毎に
細かなポリシー適用が可能

有線・無線環境、社内外を問わず、
BYODにおける必須ソリューション

(Bring Your Own Device)

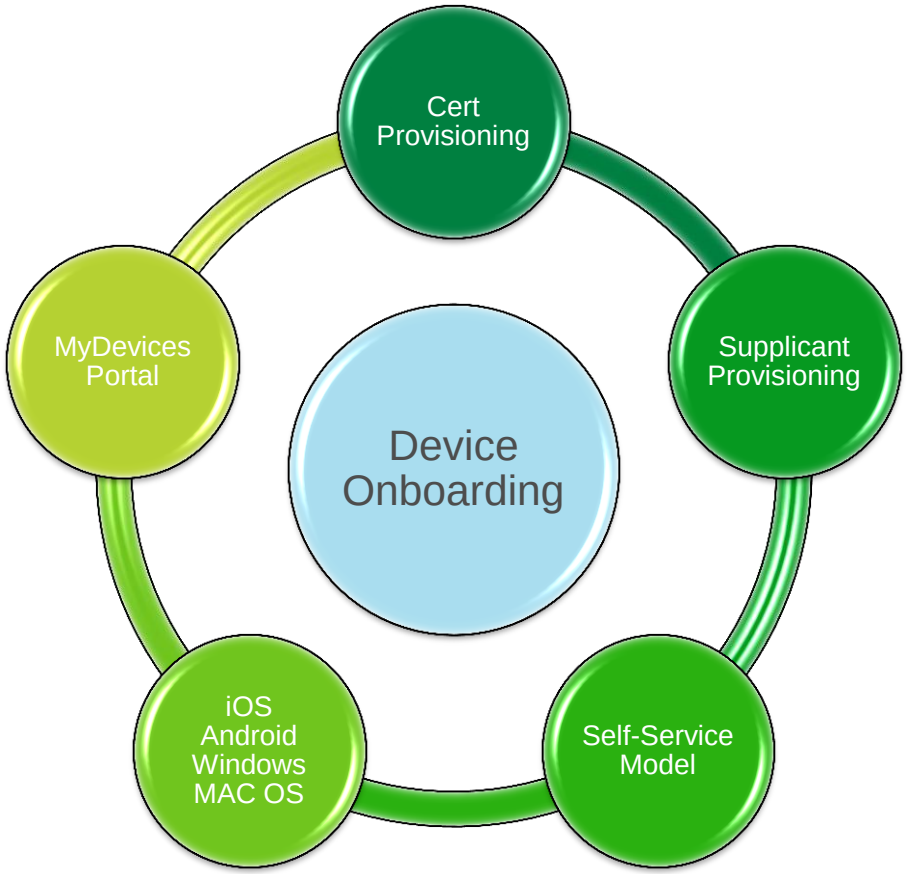
ISE機能紹介

認証・認可	デバイス プロファイリング	端末検疫
ゲスト アクセス	BYOD管理	統合 モニタリング

ISE BYOD Release

Identity Services Engine 1.1.1 (“minor release”)

2012/7/11
リリース

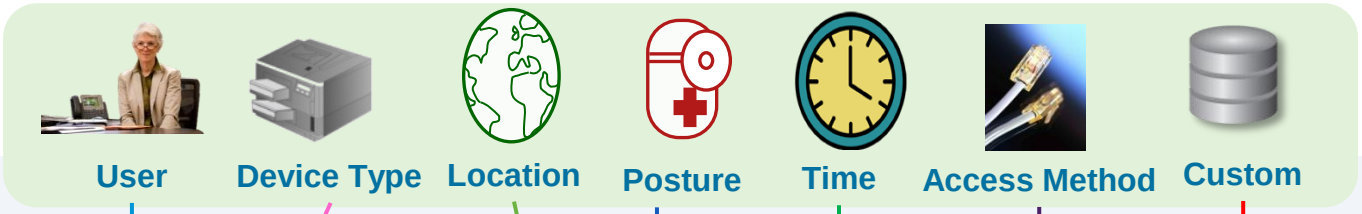


- 証明書プロビジョニング
  - Employee-IDとDevice-IDに基づく証明書
- デバイスネイティブサプリカントのプロビジョニング：
  - Windows: XP, Vista & 7
  - Mac: OS X 10.6 & 10.7
  - iOS: 4* & 5 (iPhone 3G/3GS/4/4S, iPad, iPod)
  - Android – 2.2 and above
  - 802.1X using EAP-TLS or PEAP

* Dual SSID Only

- ユーザ向けセルフサービスポータル
  - 紛失時のブラックリスト化
- セルフサービスモデル
  - IT管理者の仲介プロセスが不要

Cisco ISE によって定義される認証ポリシー



誰？
- 既知ユーザ (営業、HR)
- 未知ユーザ (ゲスト)

何？
- 端末識別
- 端末分類 (プロファイル)
- 端末状態 (検疫)

どうやって？
- 有線
- 無線
- VPN

どこ？
- 物理的なロケーション
- Calling Station ID
- SSID / スイッチポート

いつ？
- 日付
- 時間
- スタート/ストップ

その他？
- AD, LDAP、カスタムアトリビュート

Authorization Policy At A Glance

First Matched Rule Applies

Standard

Status	Rule Name	Identity Groups	Other Conditions	Permissions
Enabled	Contractor-iPAD	iPad OR Apple-iPhone OR Apple-iPod OR BlackBerry	Contrator_Wireless AND Posture_Compliant AND North_America	Contractor_iPAD
Enabled	Guest-Wired	Guest	Business_Hours AND DEVICE:Device Type EQUALS All Device Types#Wired AND Posture_Compliant	Guest
Enabled	Guest-Wireless	Guest	Business_Hours AND DEVICE:Device Type EQUALS All Device Types#Wireless AND Posture_Compliant	Guest_Wireless
Disabled	Default-Posture	Any		CWA_Posture_Remediation
Enabled	Default	Any		Central_Web_Auth

Cisco ISE による多要素認証・認可イメージ

誰が、何（端末識別）を、どうやって（認証方法）アクセスしてきたかを判別

会社支給の端末

個体識別による証明書認証を行ったノートPCやスマートデバイスは会社支給のデバイスと判別

イントラネットのデスクトップPCと同様のフルアクセスを許可

許可された持込端末（BYOD）

証明書認証ではなくユーザ名/パスワード認証を行ったスマートデバイスはBYOD端末と判断

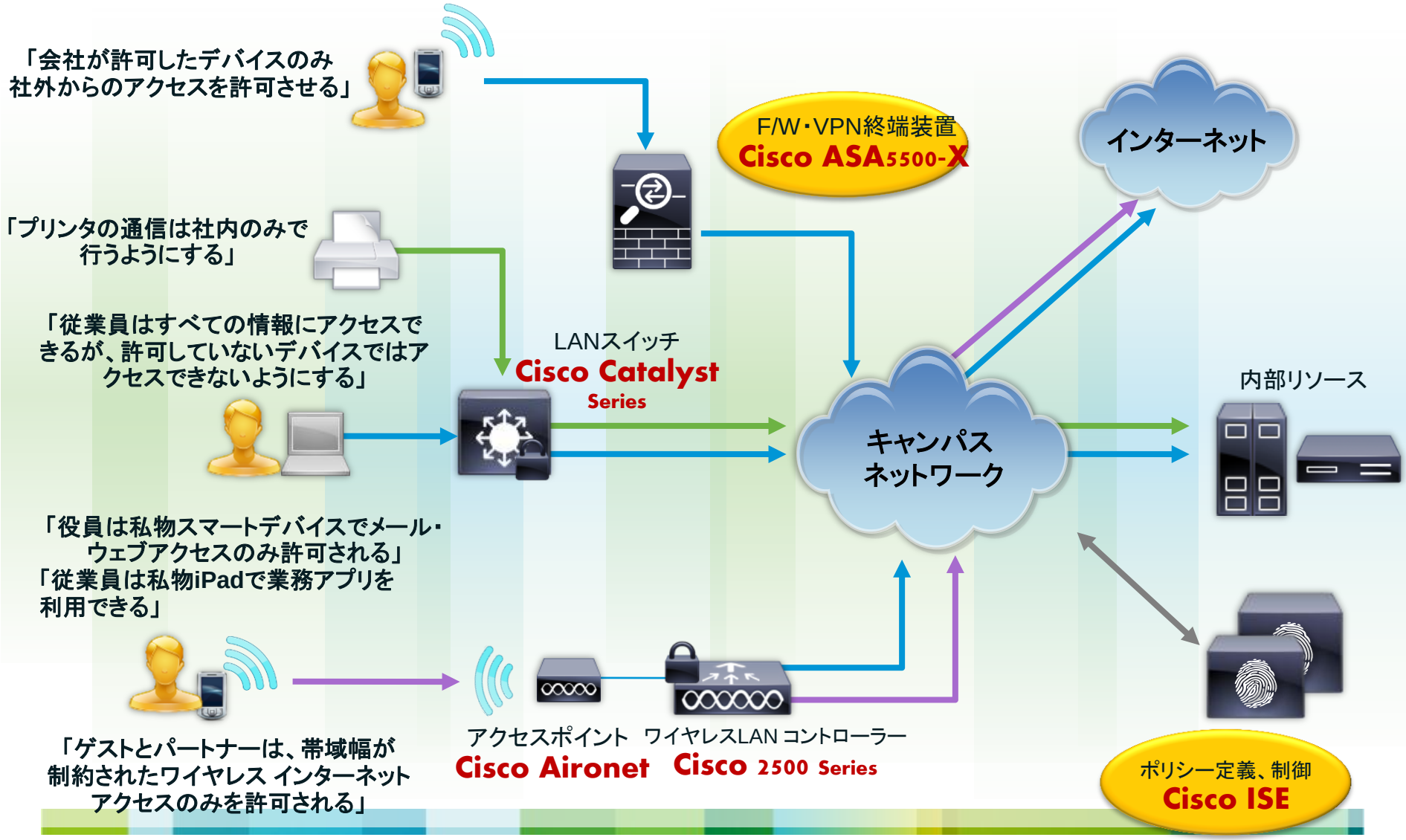
iPhone/iPadは特定のサーバへのアクセスとインターネットアクセスのみ許可

許可されていない持込端末

証明書認証ではなくユーザ名/パスワード認証を行ったスマートデバイスはBYOD端末と判断

Android端末は一時的なインターネットアクセスのみを許可し社内アクセスは不可

まとめ：Cisco ISEによるBYODアクセスポリシー
マルチアクセス環境で柔軟で統一した運用が可能



パートナーセントラルのご紹介

パートナーセントラル

- パートナー様向け情報ポータルサイト。
- **日本スタッフSEによる、日本の技術者に向けた豊富な解説資料。**
- パートナー様向け日本語による各種設定ガイドあり。
  → www.cisco.com/jp/go/partnerdoc/

参考資料

【参考資料1】本日ご紹介申し上げたソリューションの詳細

シスコシステムズ合同会社ホームページ
→「製品＆サービス」
→「セキュリティ」
http://www.cisco.com/web/JP/product/hs/security/

【参考資料2】 BYODおよびセキュリティに関する読み物

シスコシステムズ・ボーダレスネットワーク事業担当部長　楢原盛史によるBYODおよびセキュリティに関する各種投稿記事およびブログ。

IDGインタラクティブ様のCIO Magazineや BLOGSで記事掲載
http://www.ciojp.com/blogs/b/129

日経BP社様のITpro Specialで記事掲載
http://special.nikkeibp.co.jp/ts/article/ab0a/115265/

Thank you.

J20
IN JAPAN SINCE 1992

世界で一番、
ネットワークの力を信じている。