



J20
IN JAPAN SINCE 1992

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



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)



Webセキュリティ

IronPort WSA
ASA CX



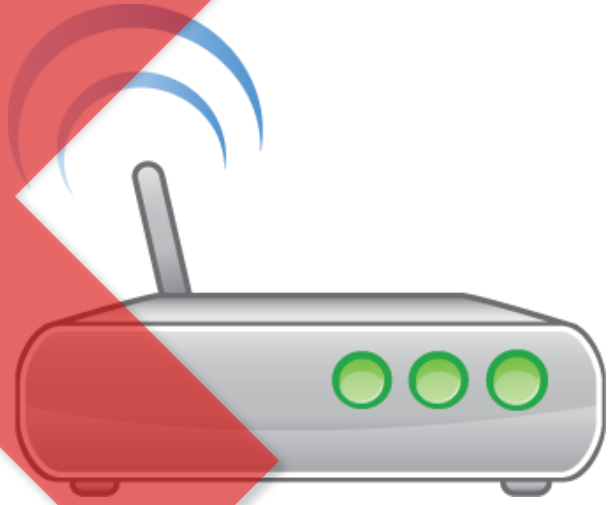
Wireless LAN

Cisco
Aironet シリーズ

オフィスでスマートデバイスを使いたい



スマホ&タブレット



アクセスポイント

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



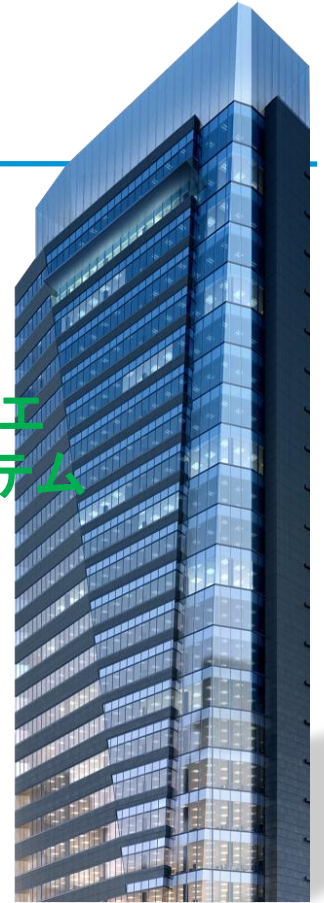
アクセスポイント










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！



iPhone 4 S
デュアルコアA5チップ。まったく新しい8メガピクセルカメラと光学システム。iOS 5とiCloud。新しくSiriも搭載。史上最高のiPhoneです。

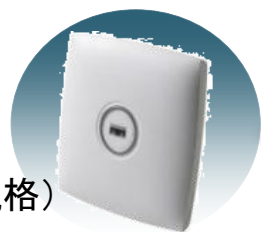


**IEEE802.11n対応！ もちろんタブレットPCやノートPCも！
さらにスマホ導入済、あるいは検討段階の企業はすでに40%越え(*)！**

(*) 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

- $-20^{\circ}\text{C} \sim 55^{\circ}\text{C}$ 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

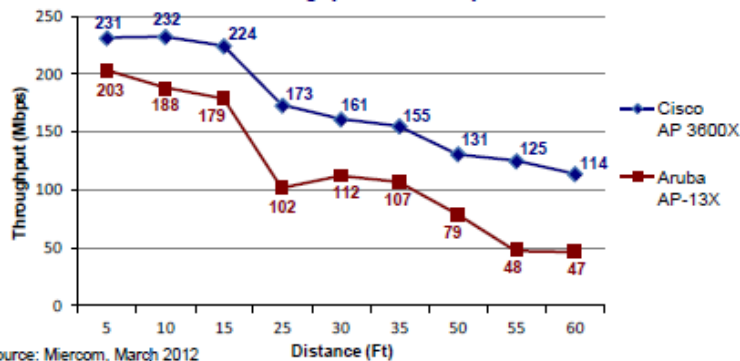
ClientLink 2.0

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

Figure 2: Cisco AP 3600X
TCP Downstream Throughput – Three Spatial Stream Client



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

**BEST OF
INTEROP**
InformationWeek
analytics



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ンネルを変更
- 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

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		AnyConnect 2.5.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 S II, Galaxy Tab 7/8.9/10.1
Linux		iPhone 4S	5.0 or later	HTC	Desire, EVO, Flyer etc
		iPod Touch (2 nd 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トまたは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

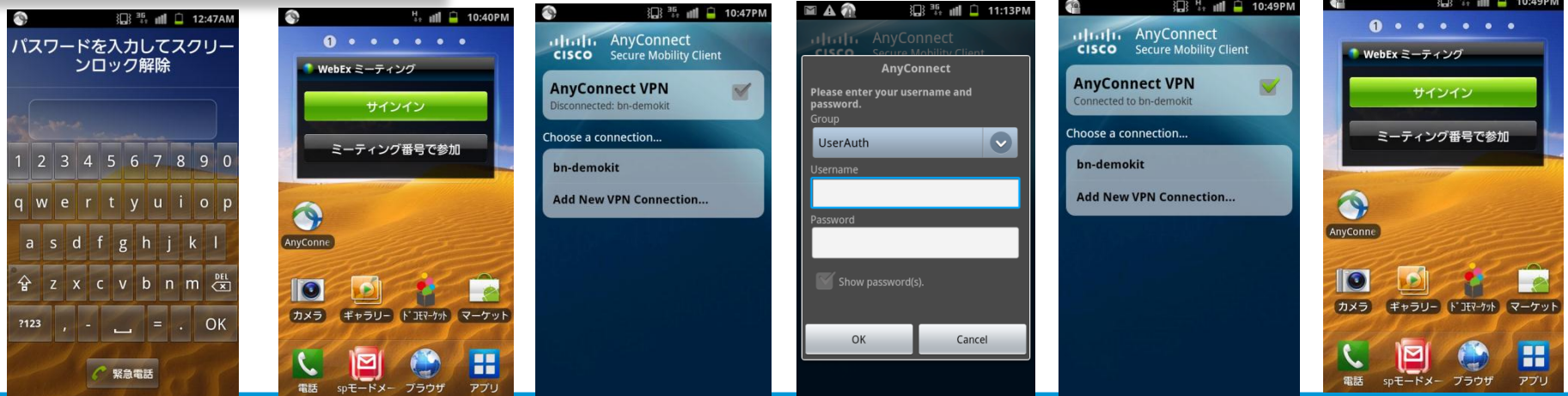
(※最新の情報はGoogle Play (Android Market) で検索)



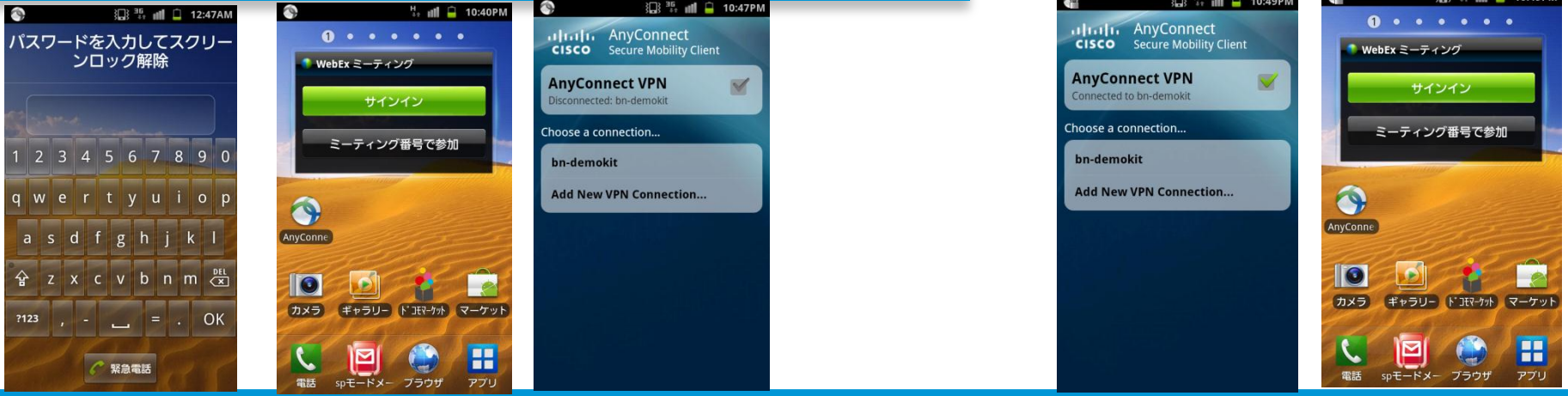
Cisco ASAとの連携	iPhone/iPad	Android端末
AnyConnect (SSL VPN)	○ iOS4.1/4.2.1以降	○ 端末に依存
端末標準のVPN (L2TP over IPsec)	○	○ Android2.1、ASA8.4(1)以上

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)

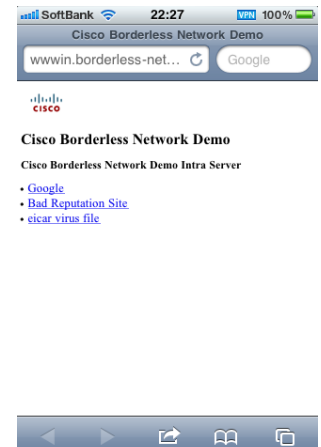
京セラコミュニケーションシステム

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



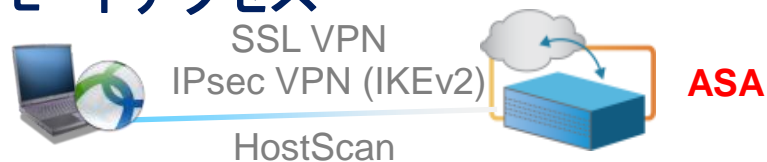
Cisco AnyConnectセキュアモバイルクライアント 3.1

AnyConnect 3.1

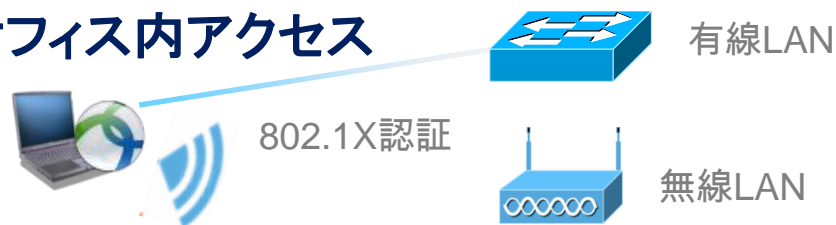
あらゆるシチュエーションに対応

- 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

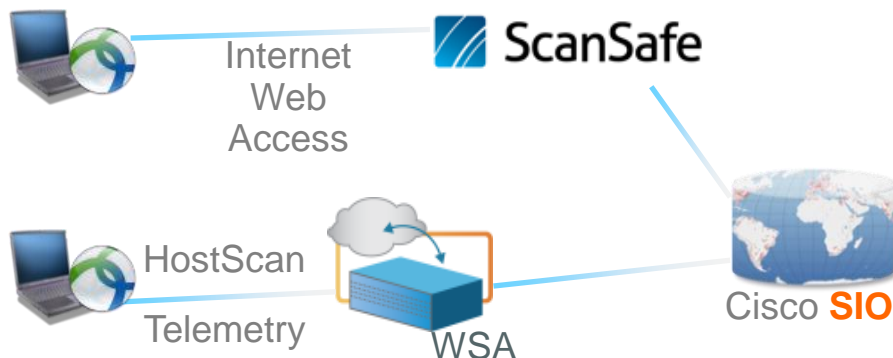
リモートアクセス



オフィス内アクセス



インターネットアクセス



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

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)

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 or ブラウザでのアクセス
- 機能が豊富(提案の幅が広い)

- 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)。

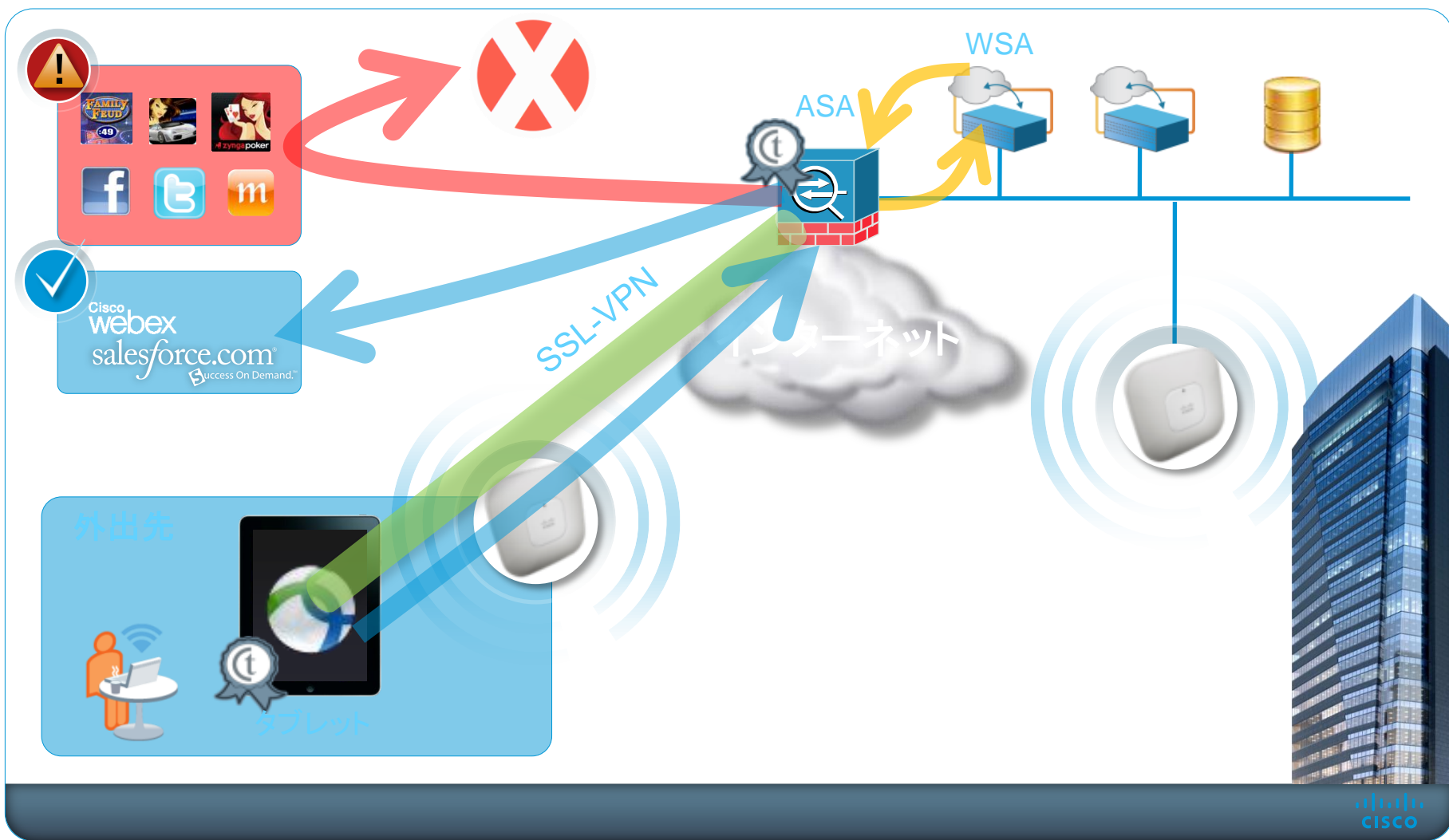
(注1) ASA8.3以降のFailover構成時であれば、双方のライセンスの合計分を利用可能。

(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。

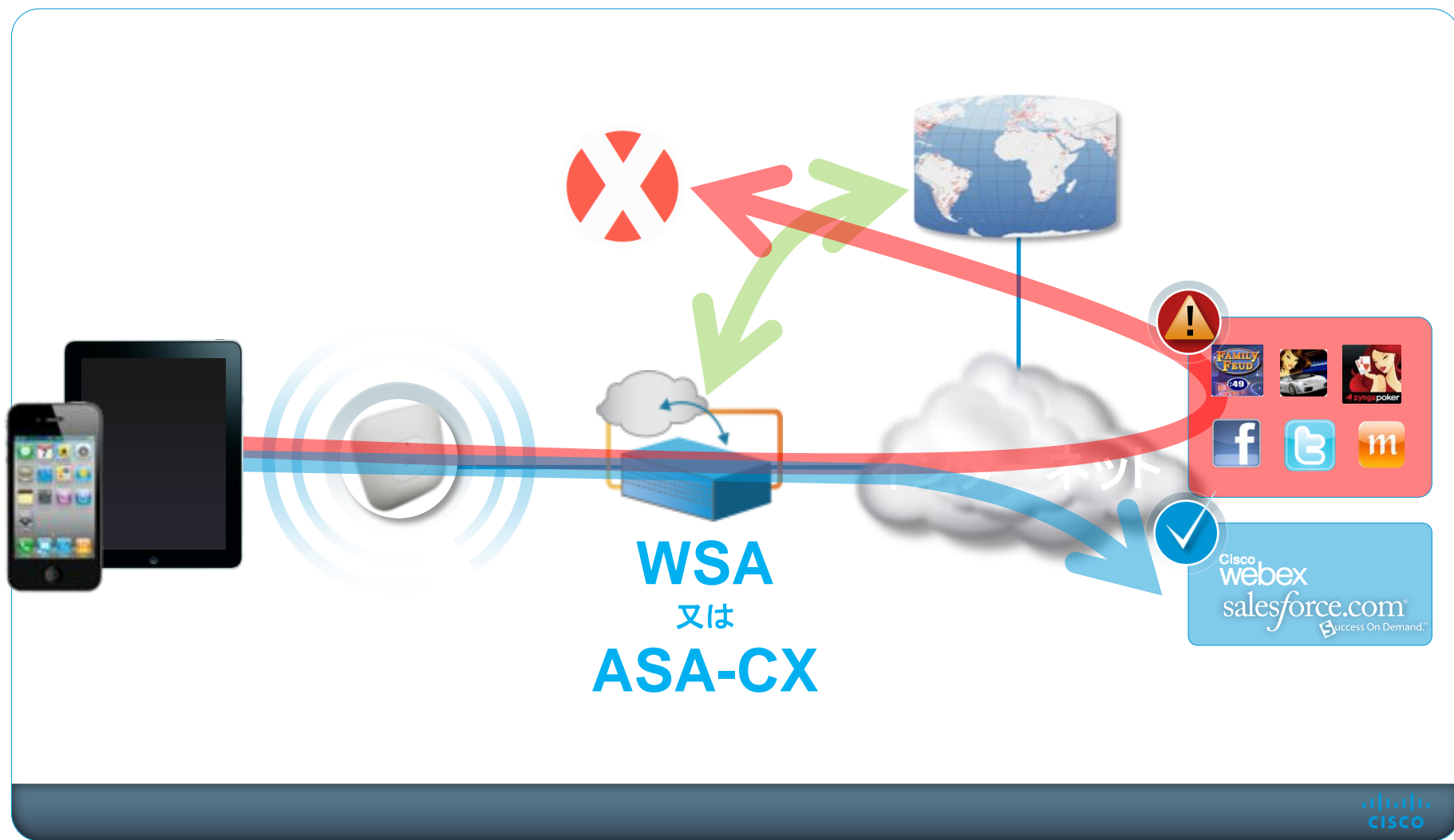
Webセキュリティ 次世代型ファイアウォール

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

コンテキスト・アウェア
人・アプリ・デバイスの識
別



脅威への対応
ウェブセキュリティ



ASA 5500-X

クラシックファイアウォール・IPS・VPN

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？

WSA

- Caching (WSA)
- AV Scanning
- Data Loss Prevention
- Explicit Proxy (WSA)
- SOCKS Proxy* (WSA)
- No backhauling (SS)
- Add'l policy actions:
Time-based controls,
warn

- URL Filtering
- Web Reputation
- Web Applications (like
Facebook, LinkedIn, Twitter)
- User identification
- SSL Decryption
- Policy actions: allow/block
- End user notification
- Top N reports

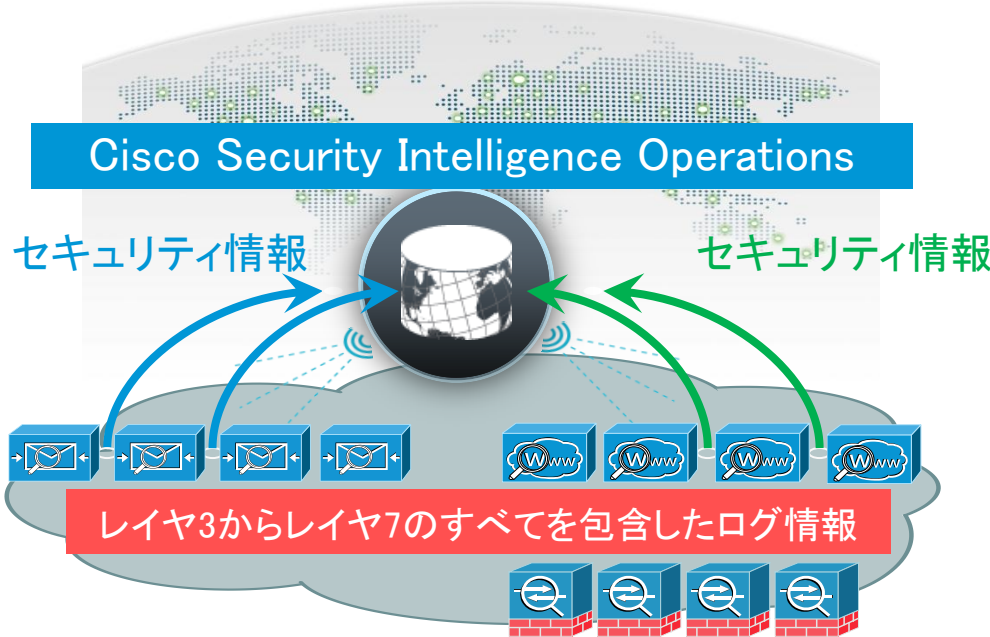
ASA CX

- Inline firewall
- Non-web applications (like
Skype, Oracle BI)
- Network protocols (like SMTP,
DNS, ICMP)
- Layer 3-7 access rules
- Networking capabilities like
NAT, Routing, VPN
- Inbound Threat Prevention*

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”」

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

se

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

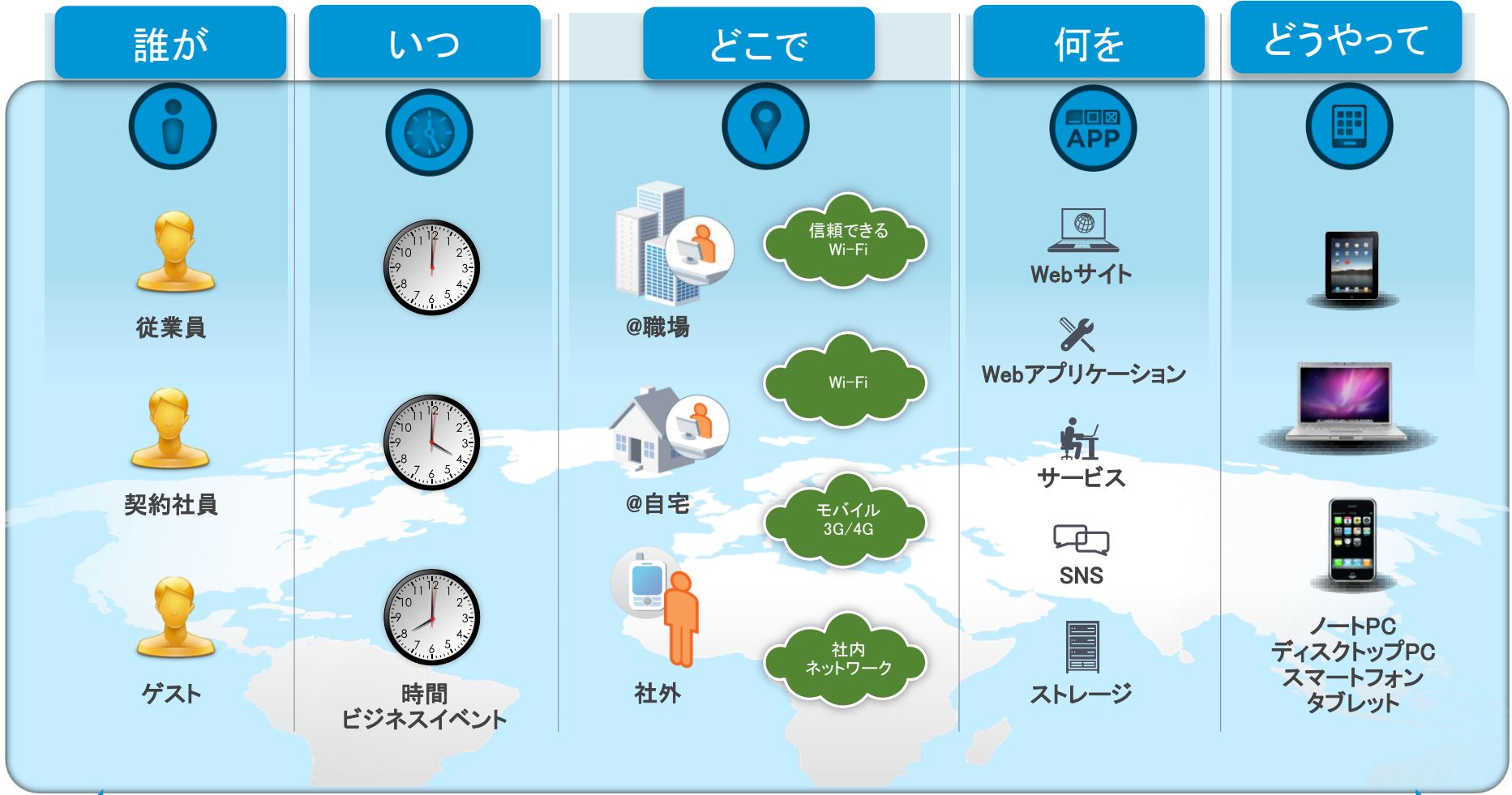
Name	Time
Troj/Agent-LQA	11/09/2009 17:09
Troj/Agent-LPO	11/06/2009 12:48
Troj/Dloadr-CWS	11/06/2009 08:32
Troj/Agent-LNC	11/05/2009 15:21
Troj/Zbot-KD	11/05/2009 13:00
Troj/Agent-LNC	11/05/2009 13:00
Troj/Dloadr-CWK	11/04/2009 11:42
Troj/FakeAV-AGU	11/02/2009 14:08
Troj/Agent-LNR	10/30/2009 12:23

IP Address	Volume (m)	Country
62.28.89.32	4.3	PT
209.235.255.154	3.4	US
60.213.48.250	3.1	CN
213.165.64.20	2.9	DE
96.9.175.234	2.9	US
91.194.188.90	2.7	PL
210.211.111.2	2.6	--
90.183.38.157	2.6	CZ
209.242.26.205	2.6	US
90.183.38.155	2.6	CZ

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

The screenshot displays the Cisco Identity Services Engine (ISE) management console. The interface includes a navigation menu (Home, Monitor, Policy, Administration) and a Task Navigator. The main content area is divided into several sections:

- Metrics:** Active Endpoints (21), Active Guests (0), Posture Compliance (0%), Mean Time To Remediate (0.0 sec), and Profiled Endpoints (16).
- System Summary:** A table showing system utilization and latency for ISE1.
- Identity Stores (PIP):** A table showing authentication counts for AD1.
- Authentications:** A table showing a total of 34 authentications.
- Authentication Failure:** A section showing a total of 9 failures.
- Profiled Endpoints:** A section showing 16 unique endpoints.

Overlaid on the right side of the screenshot is a large blue box with a fingerprint icon and the text "ISE". Below the authentication logs, there are five blue boxes with Japanese text: "誰が" (Who), "何を" (What), "どこで" (Where), "いつ" (When), and "どのように" (How). Below these boxes are five circular icons representing a person, an app, a location pin, a clock, and a building.

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
グ

端末検疫

ゲスト
アクセス

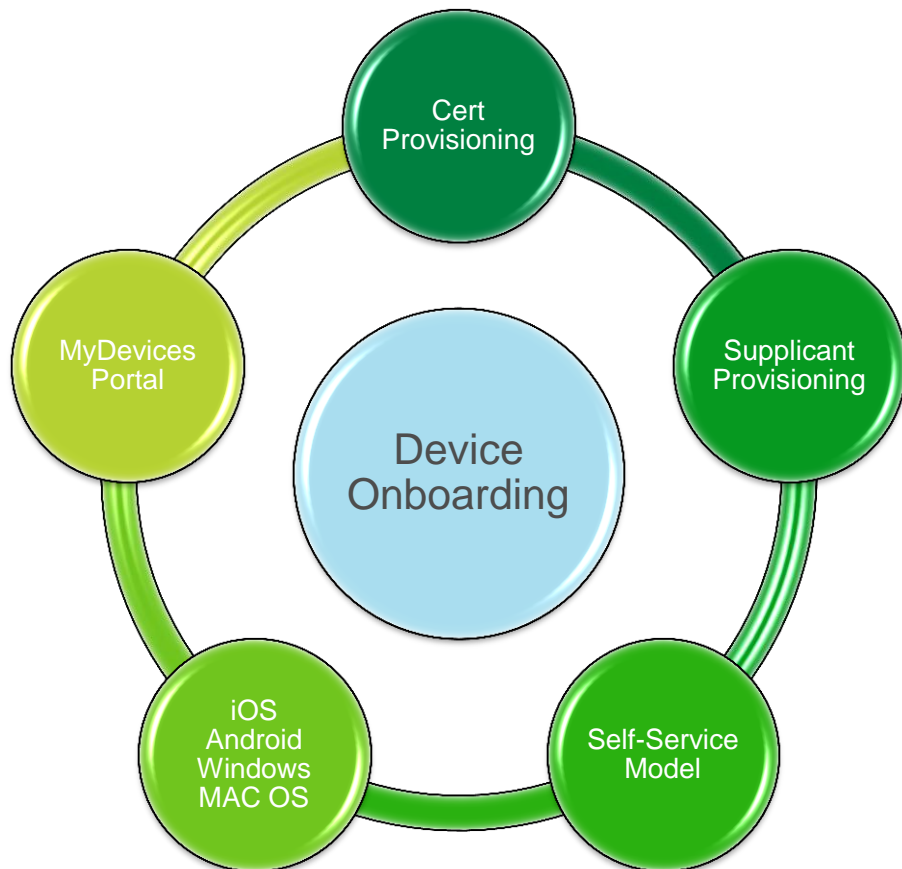
BYOD管理

統合
モニタリング

ISE BYOD Release

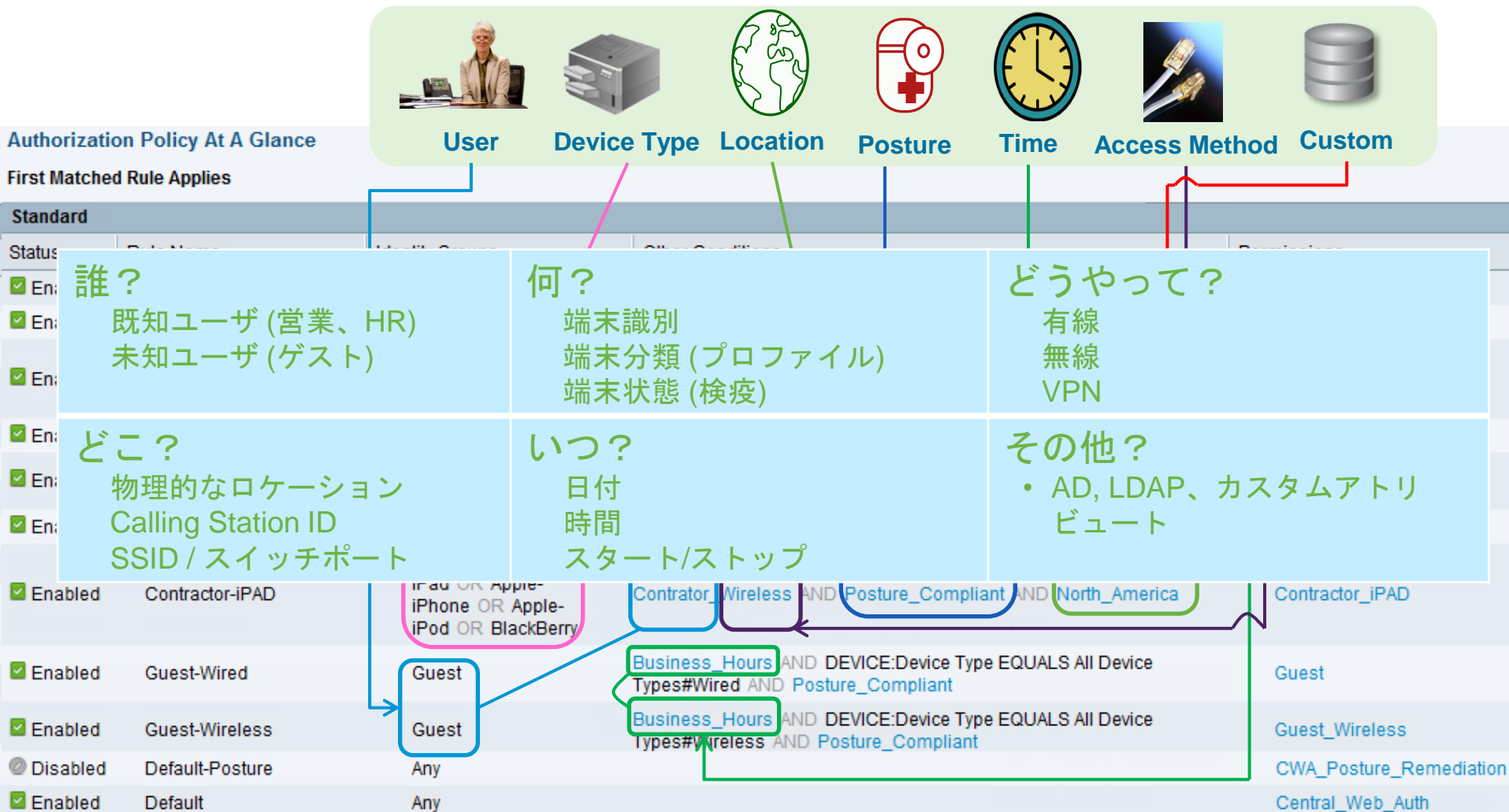
Identity Services Engine 1.1.1 (“minor release”)

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ブ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)
* Dual SSID Only
 - Android – 2.2 and above
 - 802.1X using EAP-TLS or PEAP
- 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



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

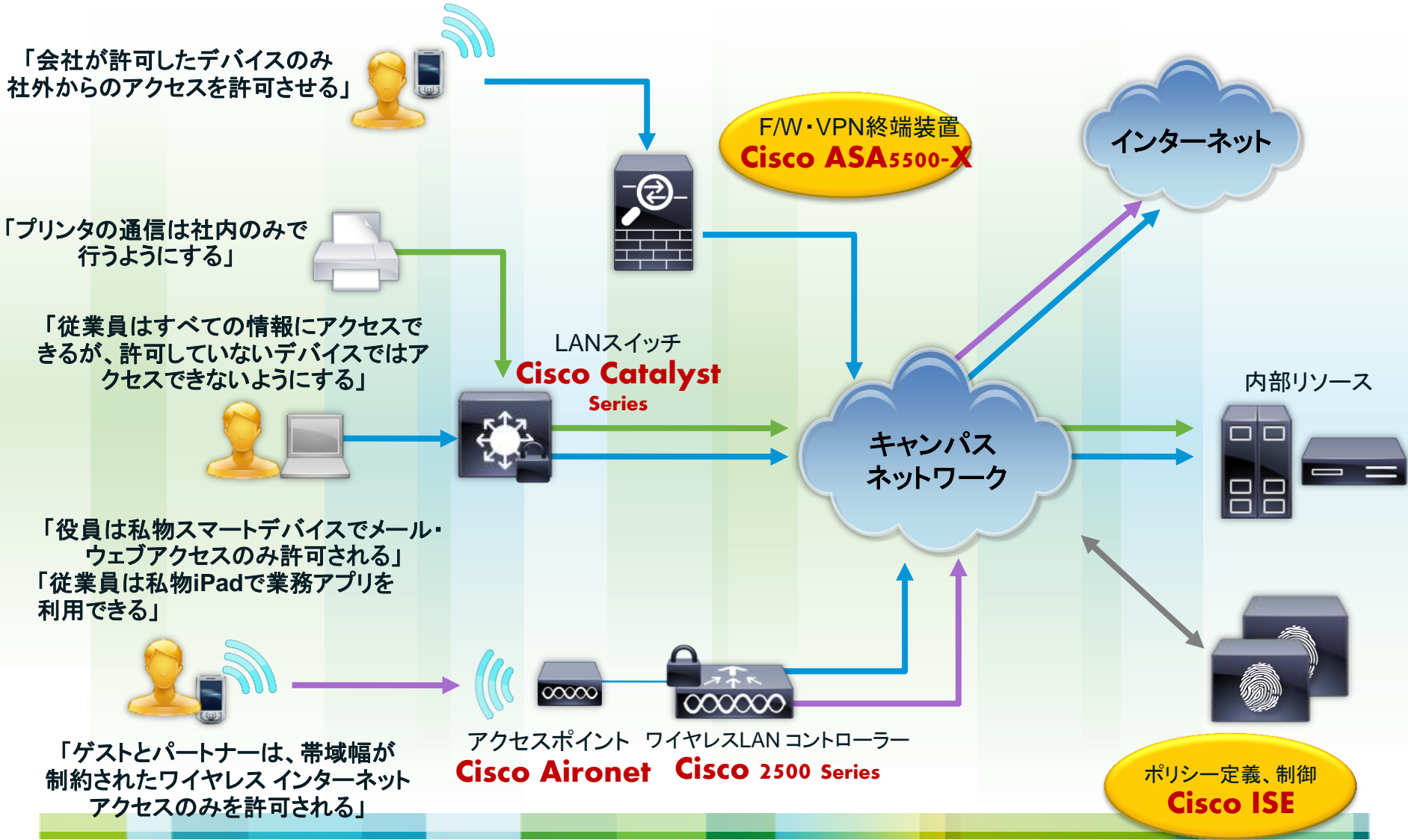


証明書認証ではなくユーザ名/パスワード認証を行ったスマートデバイスはBYOD端末と判断

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/

ASA Remote Access VPN 設定ガイド for Smart Phones

Date : 22 Sep 2011

tetsato@cisco.com

1. 基本設定 (共通)

- a) ASDM 設定 共通
- b) 認証設定
 - I. ローカルユーザ AnyConnect L2TP
 - II. 外部ユーザ認証 (Windows AD) 共通
- c) 証明書 共通
- d) アドレスプールの設定 共通

2. VPN 設定

- a) AnyConnect 設定 AnyConnect
- b) L2TP/IPSec の設定 L2TP

3. クライアント設定

- a) AnyConnect 設定
- b) L2TP/IPSec 設定

4. 補足説明

The screenshot shows the Cisco Partner Central website interface. The top navigation bar includes 'Japan (国)', 'ようこそ, Masako Arashima | アカウント | ログアウト | シスコについて | 日本のオフィス | My Cisco'. The main content area is titled 'セキュリティ 関連資料'. Below this is a table with columns for 'ホーム', 'カテゴリ', '製品', 'Level', and 'タイトル / 内容 / 日付 / イベント名'. The table lists several documents related to ASA and AnyConnect configurations.

ホーム	カテゴリ	製品	Level	タイトル / 内容 / 日付 / イベント名
ホーム パートナーセントラル SELL & MARKET CISCO セールス テクノロジー セキュリティ 関連資料	- All -	- All -	- All -	
	Technical	ASA	Level2	ASA5500 総合テクニカルガイド (2012/03/15) ASA5500 シリーズのほぼ全ての機能を網羅した技術説明資料です。ASA の技術的な説明や解説が必要な場合の教科書としてご利用ください。ソフトウェアバージョン 8.4(2), 8.5(1), 8.6(1) を使用。33MB、400 ページ超の資料です。
	Technical	Router/Switch	Level2	AnyConnect 設定ガイド for IOS IKEv2 (2012/03/15) 本資料は ISR G2 ならびに ASR1000 と AnyConnect 3.0 を IKEv2 IPsec VPN 接続する流れを説明しています。初めて設定する場合などの参考資料としてご利用ください。
	Technical	Ironport	Level2	WSA Administration Lab (2012/02/27) CTU Security 2012 Feb で提供したラボが PEC 上でもご利用いただけます。 www.cisco.com/jp/go/psnet からログイン後、Ironport Lab で検索すると、GOLDLab: Web Security Appliance Administration を選択できます。本資料はこちらの日本語訳資料としてご利用ください。なお本 Gold Lab は 後日別の内容に変更/削除される事があります。

參考資料

【参考資料1】 本日も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/>

Japan [閉] ようこそ, Maiko Arashima | アカウント | ログアウト | シスコについて | 日本のオフィス | My Cisco

製品 & サービス | テクニカルサポート | 購入案内 | トレーニング & イベント | パートナー

セキュリティ

概要 | 製品およびソリューション | ベネフィット | テクノロジー

お問い合わせ

セキュリティ

資産を保護し、従業員の効率を高めます。

すべての製品を表示 >

サイバー攻撃に立ち向かう力 - Cisco SecureX

巧妙化するサイバー攻撃への対抗力と、スマートフォン、クラウド化への対応力を備えた、最新の包括的ネットワークセキュリティアーキテクチャの全貌とは？

[詳細はこちら](#)

主な製品

すべてのセキュリティ製品

ネットワーク セキュリティ

侵入型のソフトウェア攻撃と侵入アクセスを検知してブロックできるネットワークセキュリティインフラストラクチャを構築します。

ネットワーク セキュリティ

侵入型のソフトウェア攻撃と侵入アクセスを検知してブロックできるネットワークセキュリティインフラストラクチャを構築します。

Eメールおよび Web セキュリティ

電子メールベースのスパム、ウイルス、および Web の脅威で生じる損害の大きいダウンタイムを削減

セキュリティ管理

Cisco インフラストラクチャのセットアップ、モニタリング、および管理を簡素化します。

セキュリティで保護されたアクセス制御

ネットワークセキュリティポリシーを適用し、ユーザおよびホスト アクセス制御を保護し、ネットワークアクセスを動的な条件に基づいて制御します。

セキュア モビリティ

SSL VPN、IPv6 over IPv4 トンネル、およびユーザープロファイルでモバイル接続を保護します。

【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 檜原盛史による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 世界で一番、
IN JAPAN SINCE 1992 ネットワークの力を信じている。

