Cisco PCI DSS 3.2 ワイヤレス セキュリティ コンプライアンス補足ドキュメント

改訂：2018 年 7 月 30 日

はじめに

年々、ネットワーク攻撃がまん延して高度化が進み、検出が困難になっています。小売業者の公共性を考えると、ネットワークへの侵入地点には、企業内のラップトップ、デスクトップ、スマートフォンだけでなく、公衆 Wi-Fi やインターネットを使用する e コマース サーバまで含まれます。このため、小売ネットワークには 2 つの大きな課題があります。第 1 の課題は、多くのリモート ロケーションを管理する複雑さに対処することです。第 2 の課題は、大規模なエンタープライズ ネットワークが直面している脅威と同等の対応をしたセキュリティ保護機能を備えることです。

今日の攻撃の多くは、異なるレイヤからさまざまな手法を駆使してネットワークに侵入しようとする複合型の攻撃です。古いファイアウォールでは、大容量ファイルや HTTPS で暗号化されたトラフィックなどを検査することができないため、こうした攻撃には対応できません。

クレジット カードによる支払いを受け入れるビジネスでは、PCI 基準の遵守を維持することが不可欠です。PCI DSS（Payment Card Industry Data Security Standard）には、安全なネットワークの構築と維持、ネットワークの定期的な監視とテスト、強力なアクセス制御手段の実装など、6つの高度な目標があります。これらの目標は、カード所有者の個人情報を含むクレジットカードデータを保護し、安全性を確保する上での特定の要件に対処できるようにするものです。PCI コンプライアンスを維持することで、ビジネスにおいて多額のペナルティを受ける危険性は回避できますが、完全なネットワーク セキュリティ ソリューションとして評価されているわけではありません。あくまでネットワークをできるだけ安全なものにしていく上での重要な通過点と考える必要があります。

シスコと PCI DSS 準拠

2007 年以来、シスコと Verizon 社は提携して、Payment Card Industry（PCI）コンプライアンス ガイダンスの提供を続けています。その成果である Cisco® Compliance Solution for PCI は、Verizon Qualified Security Assessor（QSA）評価対象であるシスコ研究施設の具体的な構成においてガイダンスを実装するために開発されたものです。PCI DSS（Payment Card Industry Data Security Standard）3.0、3.1、3.2 の各リリースに関して、シスコのお客様から当然のように尋ねられる質問があります。

- バージョン 2.0 から 3.2 への重要な変更点は何ですか。
- 現在の Cisco Compliance Solution for PCI にどのような影響がありますか。

この補足ドキュメントでは、以下のトピックについて説明します。

- PCI の対象範囲、ベンダー機器評価、既存の Cisco Compliance Solution for PCI 実装のエンタープライズ アーキテクチャに対する PCI DSS 3.2 の影響
- ワイヤレス導入に関連する PCI DSS 2.0 から 3.2 への重要な変更点

Cisco Compliance Solution for PCI

Cisco Compliance Solution for PCI は、次のような企業向けガイダンスとコンポーネントレベルの設定を提供します。

- エンタープライズ アーキテクチャ：リファレンス アーキテクチャを使用してコンプライアンス ガイダンスを検証します。リファレンス アーキテクチャは、さまざまな規模のブランチ オフィス、WAN、データセンター、および

インターネット エッジ テクノロジーで構成されています。クレジット カードのトランザクションがブランチ ロケーションで発生し、企業を通じて加盟店銀行に送信される際のセキュリティとそれぞれのコンプライアンス統制について詳細に規定しています。

評価：Cisco Compliance Solution for PCI のアーキテクチャ セクションは引き続き有効です。基準の更新によるガイダンスへの影響はありません。

- コンポーネント：Cisco Compliance Solution for PCI では、PCI をサポートするコンポーネントのネイティブ機能を評価するために標準化されたメトリックが使用されています。このメトリックは、機能スコアカードと呼ばれ、対象のデバイスに対して PCI DSS の関連セクションをまとめたものです。

評価：Cisco Compliance Solution for PCI のスコアカードは引き続き有効です。基準の更新によるガイダンスへの影響はありません。

PCI DSS の一般的な変更において常に混乱を引き起こす最も重要な要素の 1 つに、PCI 対象範囲の定義があります。

PCI 3.0 ～ 3.2 基準には、以下のように、PCI の対象範囲とセグメントを明確にして対象のシステムを規定する文言が含まれています。

- セキュリティ サービスを提供する（認証サーバなど）
- セグメンテーションを促進する（内部ファイアウォールなど）
- カード所有者データ環境のセキュリティに影響を与える（名前解決または Web リダイレクト サーバなど）

また、この基準では、セグメンテーション定義で初めて「分離」という用語を使用しています。PCI 3.0 ～ 3.2 基準では「対象外システム」が明確化され、侵害されてもカード所有者データ環境のセキュリティに影響を及ぼす可能性のないシステムと定義されています。要件 11.3 は、カード所有者データ環境の境界におけるテストを拡大することを目的とした表現となっています。機密情報へのアクセスがないことを検証するために、内部境界および外部境界に対して侵入テストが必要であることが明記されています。

3.2 における重要な変更点（要件別）

要件 1：データを保護するためにファイアウォールを導入して設定を維持する。

要件 1.1.3：ネットワーク構成図に関する要件から派生した新規要件。システムとネットワーク間のすべてのカード所有者データ フローを示すデータ フロー図を維持管理する（即時発効）。

要件 1.1.6：Simple Network Management Protocol（SNMP）バージョン 1 および 2 を「安全でないプロトコル」のリストに追加（即時発効）。

要件 2：システム パスワードやその他のセキュリティ パラメータにベンダーが設定したデフォルト値を使用しない。

要件 2.1：システムおよびアプリケーションのクレデンシャルを含むすべてのパスワードに適用されているベンダーのデフォルト値を変更し、不要なデフォルト アカウントを削除または無効化することを明確化（即時発効）。

要件 2.2.2/2.2.3：「必要な」サービスと「安全な」サービスを分けることで、システム設定基準がより規範的かつ明示的になるように変更（即時発効）。

要件 2.4：新規要件。すべての PCI システム コンポーネントの現在のインベントリを維持し、設定基準を策定する（即時発効）。

要件 3：保存データの保護。大きな変更なし

要件 4：公衆ネットワーク経由でカード所有者データや機密情報を送信する場合は暗号化する。

要件 4.1：Bluetooth、CDMA、衛星通信を「オープンな公衆ネットワーク」の例に追加（即時発効）。

要件4.1：オープンな公衆ネットワーク（インターネット、ワイヤレステクノロジー、携帯電話テクノロジー、General Packet Radio Service（GPRS）、衛星通信など）経由で機密性の高いカード所有者データを送信する場合、強力な暗号化方式とセキュリティ プロトコルを使用して保護する。カード所有者データを送信するワイヤレス ネットワーク、またはカード所有者データ環境に接続されているワイヤレス ネットワークは、業界のベスト プラクティスを採用し、認証や送信用に強力な暗号化方式を導入する（SSL/初期 TLS を使用している場合、PCI DSS 付録 A2 の要件を満たす）。

以上の要件に対応するセキュリティ コントロールとして SSL および初期の TLS は利用できない。SSL または初期の TLS からの移行に対応するため、以下の規定が設けられている。

- 新しい実装では、SSL または初期の TLS をセキュリティ コントロールとして使用しない。
- 2018 年 6 月 30 日以降は、すべての事業体が SSL/初期の TLS をセキュリティ コントロールとして使用することを中止し、安全なバージョンのプロトコルのみを使用する（一定の POS POI 端末の除外についてはこの箇条書きの最後の項目を参照）。
- 2018 年 6 月 30 日までは、既存の実装で SSL/初期の TLS を使用している場合、正式なリスク軽減策および移行計画を整備する。
- SSL および初期の TLS に対する既知の攻撃を受ける可能性が低いことを検証可能な場合、該当の POS POI 端末（および接続先である SSL/TLS ターミネーション ポイント）は、2018 年 6 月 30 日以降も引き続きセキュリティ コントロールとして使用可能。

要件 5：ウィルス対策ソフトウェアを実行し、定期的に更新する。

要件 5.1.2：「一般的にマルウェアの影響を受けない」システムでは、進化を続けるマルウェアの脅威を評価する。

要件 6：安全性の高いシステムとアプリケーションを開発し、保守する。

要件 6.5.x：新規要件。PAN（Primary Account Number）とSAD（Sensitive Authentication Data）がメモリ内で処理される方法を記録するためのコーディング手法に関する要件（2015 年 7 月 1 日発効）。

要件6.5.10：新規要件。認証とセッション管理の障害から保護するためのコーディング手法に関する要件（2015年7月1 日発効）。

要件 7：

データへのアクセスを、業務上知る必要がある対象に制限する。大きな変更なし

要件 8：

コンピュータにアクセス可能な担当者に固有 ID を割り当てる。

要件 8.3：ユーザ、管理者、およびすべての第三者（ベンダーによるサポートやメンテナンスのためのアクセスなど）に二要素認証を適用することを明確化（即時発効）。

要件 8.5.1：さまざまな顧客環境にアクセスするサービス プロバイダーは、顧客ごとに異なるクレデンシャルを使用する（2015 年7 月 1 日発効）。

要件8.6：多要素認証を使用して、すべての非コンソール管理アクセスと、カード所有者データ環境へのすべてのリモート アクセスを保護する。8.2 に記載した 3 つの認証方法のうち少なくとも 2 つが認証に使用されている必要がある。1 つの要素を 2 回使用することは（2 つの異なるパスワードを使用するなど）、多要素認証とは見なされない。この要件は、事業体のネットワーク内から CDE への非コンソール アクセス権を持つ管理者、および事業体のネットワーク外からのすべてのリモート ネットワーク アクセス（ユーザ、管理者、および第三者を含む）に適用される（注：事業体のネットワーク内からの非コンソール管理アクセスに対する多要素認証は、2018 年 1 月 31 日までは努力目標であるが、それ以降は必須要件となる）。

要件 9：カード所有者データへの物理アクセスを制限する。

要件 9.3：新しい手順。退職した従業員による物理アクセスが失効していることを確認する（即時発効）。

要件 9.9.x：新規要件。クレジット カード データを取得する POS 端末を改ざんや不正な変更/交換から保護する。要件には、端末、担当者トレーニング、デバイス検査などのリストが含まれる（2015 年 7 月 1 日発効）。

要件 10：ネットワーク リソースおよびカード所有者データへのすべてのアクセスを追跡および監視する。

要件 10.2.x：管理者権限の使用や変更、追加、削除、および監査ログ システムの停止/一時停止などのログ要件を強化（即時発効）。

要件10.6.2：要件の更新または明文化。すべての「非クリティカル」および「セキュリティ対象外」アセットのログを「定期的に」レビューして、悪意のあるアクティビティが発生していないかを調べる（即時発効）。

要件 11：セキュリティ システムおよびプロセスを定期的にテストする。

要件 11.1.1：新規要件。承認されているすべてのワイヤレス アクセス ポイントのインベントリとその業務上の正当性に関する要件（即時発効）。

要件11.2：ガイダンスの追加。すべてのシステムがスキャンされ、すべての脆弱性が対応されたことを示すために、四半期ごとのスキャン プロセスで複数のスキャン レポートをまとめることを認める（即時発効）。

要件11.3：侵入テスト手法の明確化、セグメンテーション制御テストの追加、修復検証のための再テストに関する要件（2015 年 7 月 1 日発効）。

要件 12：情報セキュリティに対応するポリシーを維持する。

要件 12.2.b：新規要件。環境に大幅な変更があった場合はリスク評価を実施する（即時発効）。

要件12.8.x：新規要件。サービス プロバイダーの責任範囲に関する PCI 要件を詳細にまとめた「責任マトリックス」を維持する（即時発効）。

要件 12.9：新規要件。適用されるすべての PCI DSS 要件をサービス プロバイダーが維持することを書面で顧客に通知する（2015 年 7 月 1 日発効）。

PCI DSS 3.2 ワイヤレス セキュリティ要件

シスコ ワイヤレス テクノロジーは、ブランチ内のモバイル クライアントの接続を提供します。リスクを高めることなく、ゲスト アクセスやインベントリ管理などの従来のビジネス機能のための接続を保護できます。モバイル POS などの革新的なカスタマー エクスペリエンス サービスでも同様の安全性を実現します。シスコ ワイヤレス テクノロジーは、ビジネス機能を拡張するだけでなく、不正検出機能をシームレスに提供します。業界トップクラスのパフォーマンスを誇る Cisco Aironet アクセス ポイントを使用することで、セキュアで信頼性の高いワイヤレス接続を屋内外両方の環境で実現できます。シスコでは特定のビジネス ニーズやトポロジを対象とした幅広いポートフォリオのアクセス ポ

イントを提供しています。シスコ ワイヤレス コントローラは、ネットワークの構築や運用、管理をシンプル化することでCisco Unified Wireless Networkの運用コスト全体を削減します。また、Cisco SDAネットワークのポリシーとセキュリティを、有線ネットワークからワイヤレス エッジまで拡張します。

主な PCI 対応機能

Cisco Unified Wirelessにおける主なPCI対応機能は、ワイヤレス クライアントの安全な接続の確保（4.1、4.2）と不正AP検出（1.1）です。

設計上の考慮事項

ブランチにおけるワイヤレス テクノロジーに関する不正検知は、組織でのワイヤレス導入の有無に関わらず、最低でも四半期に1回は必要です。ハッカーがブランチに侵入し、不正なワイヤレス デバイス（アクセス ポイント、ワイヤレス対応プリンタ、または無線対応USBスティックなど）を導入するおそれがあります。不正なデバイスを導入することでハッカーがリモート（たとえば駐車場）からブランチにアクセスできるようになり、それを検出するのは困難です。PCI DSSには、不正デバイスを検出するための方法がいくつか用意されています。Cisco Unified Wirelessには、継続的に不正を検出しながら、正常なワイヤレス トラフィックは通過させるというメリットがあります。PCI-DSSでは、ワイヤレス テクノロジーが信頼できないネットワーク接続であると示されています。ブランチのワイヤレス テクノロジーには、カード所有者データ環境をセグメント化して保護するために、ファイアウォールと侵入検知サービスが必要です。ステートフル ファイアウォールでは、ワイヤレス環境との間のトラフィックを制限するように設定しなければなりません（有効化しているすべてのサービス、プロトコル、ポートに関してビジネス上の正当な理由を文書で記録する必要があります）。それ以外のすべてのアクセスは拒否しなければなりません。ワイヤレス ネットワークにPOS クライアントを含める場合、強力なワイヤレス暗号化技術を実装する必要があります。また、ワイヤレス クライアントは、他のワイヤレス クライアントからも保護する必要があります。たとえば、ハンドスキャナとモバイルPOSを使用する場合、スキャナはPOSとは別のSSIDとネットワーク上に存在し、ファイアウォールと侵入検知サービスで正当なビジネス上のアクセスに限定して保護する必要があります。

シスコでは、進行中のワイヤレス戦略により、エンタープライズ ワイヤレスの導入にUnified Wireless（コントローラベース）アーキテクチャを使用することを推奨しています。自律型のCisco IOSアクセス ポイントについては、機能強化されていません。今後のセキュリティおよびユーザの拡張機能は、Unified WirelessとSDAのコントローラベースアーキテクチャで開発されます。

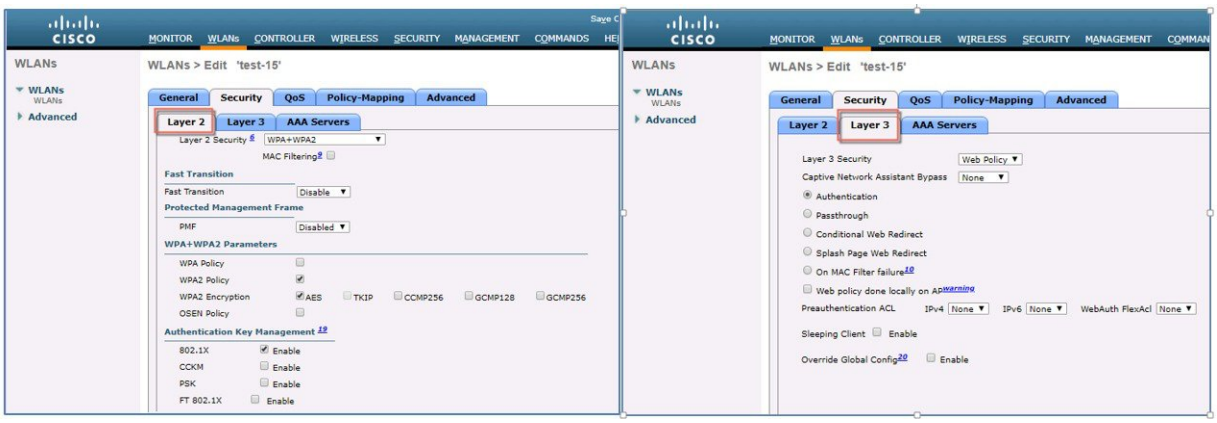
PCI 評価の詳細：対応すべきその他の PCI 要件

可能な限り、該当するCisco Wireless Control System機能を示すスクリーンショットを示しています。

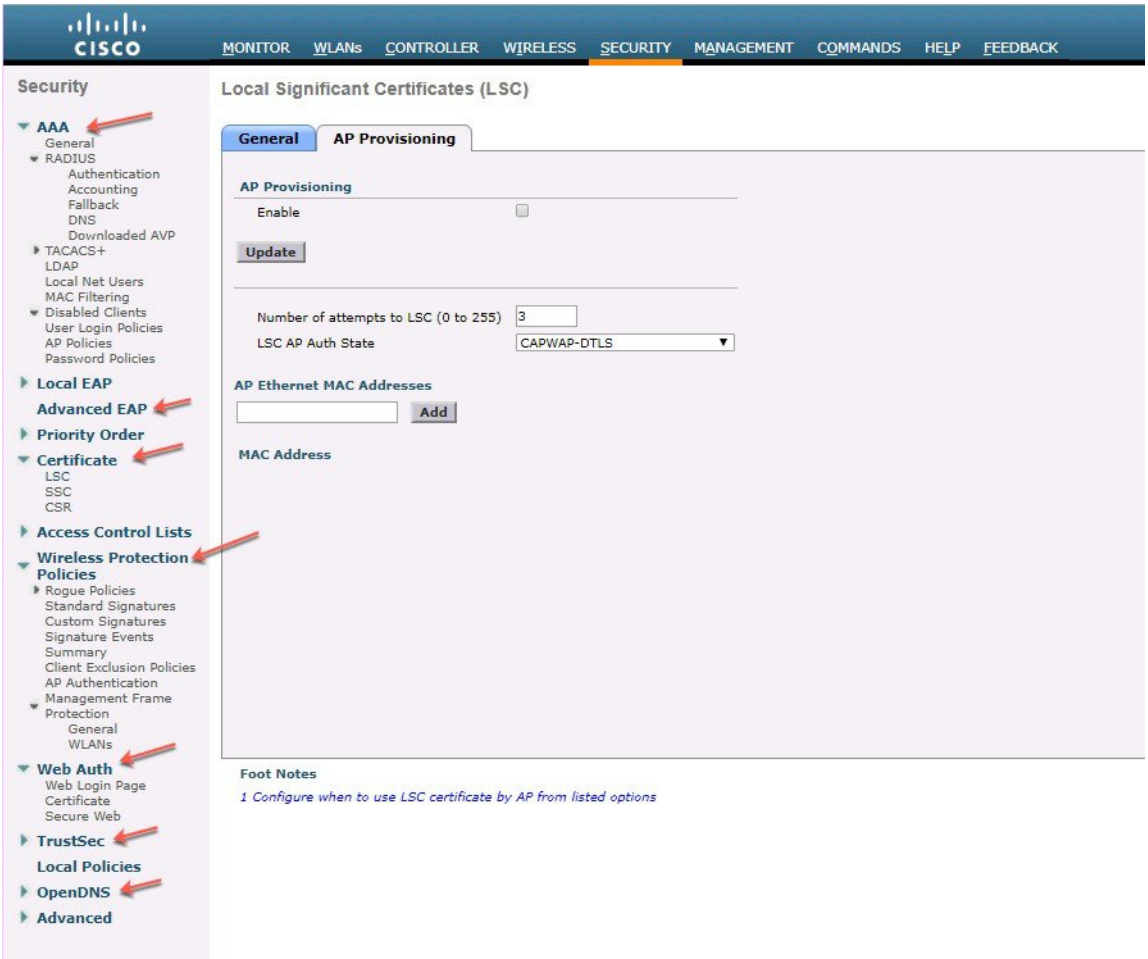
要件 2：システム パスワードやその他のセキュリティ パラメータにベンダーが設定したデフォルト値を使用しない。

- PCI 2.1.1 - カード所有者データ環境に接続しているワイヤレス環境またはカード所有者データを送信するワイヤレス環境の場合、ワイヤレスベンダーのデフォルト設定（デフォルトのワイヤレス暗号化キー、パスワード、SNMPコミュニティ ストリングなど）を変更します。Cisco Unified Wireless Networkは、Wi-Fi Protected Access（WPA）とWPA2の両方をサポートし、WLCに自動脆弱性スキャン機能を提供して、最適とは言えない暗号化方式を使用しているWLANを識別します。デフォルトのPSKはなく、設定時にすべてのPSKまたはIdentity PSKを生成する必要があります。Cisco Unified Wireless Networkアーキテクチャでは、アクセス ポイントでSNMPを使用することはありません。

以下は、WLANセキュリティのレイヤ2およびレイヤ3設定のスクリーンショットです。



以下の Cisco Wireless Controller セキュリティ設定画面のスクリーンショットは、PCI DSS セキュリティ コンプライアンス要件を上回るセキュリティ機能を網羅しています。

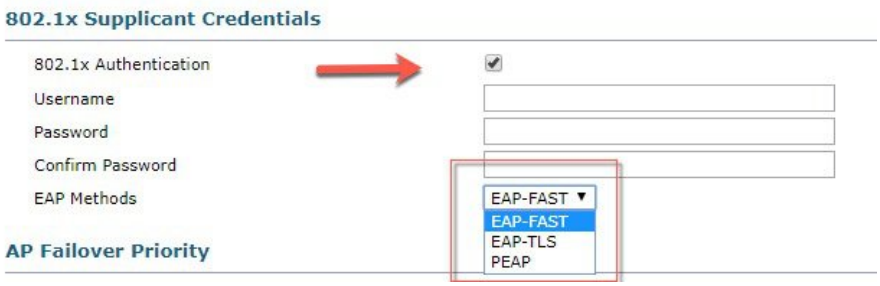


Cisco Aironet AP のセキュリティを強化するため、リリース 8.7 以降では新しい AP サプリカント認証方式が追加されています。AP サプリカントは、802.1 x 認証をサポートしているスイッチ ポートと連携して動作します。現在は、EAP 認証方式（EAP-TLS、EAP-PEAP、EAP-FAST）のいずれかを使用して、AP 全体または AP ごとに AP 802.1x サプリカ

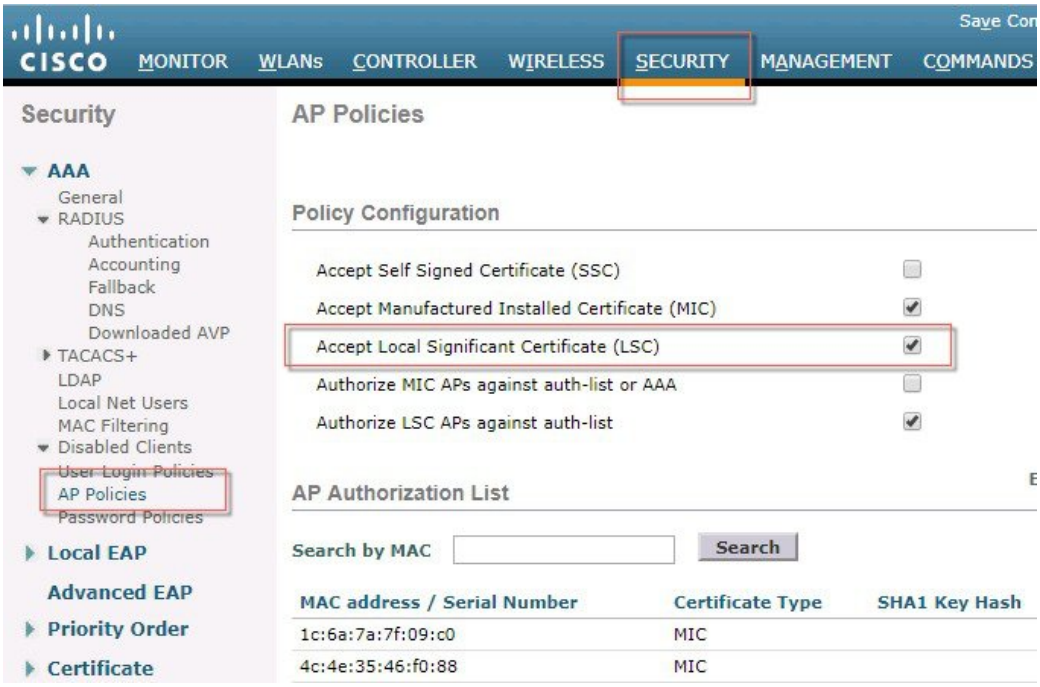
ントを有効化するオプションがコントローラに追加されています。EAP-TLS またはEAP-PEAP 方式を選択すると、MIC 証明書または LSC 証明書のいずれかを使用してコントローラと AP 間の TLS 外部トンネルが確立されます。新しい EAP-FAST 認証サプリカントは、Wave-1 AP でサポートされています。

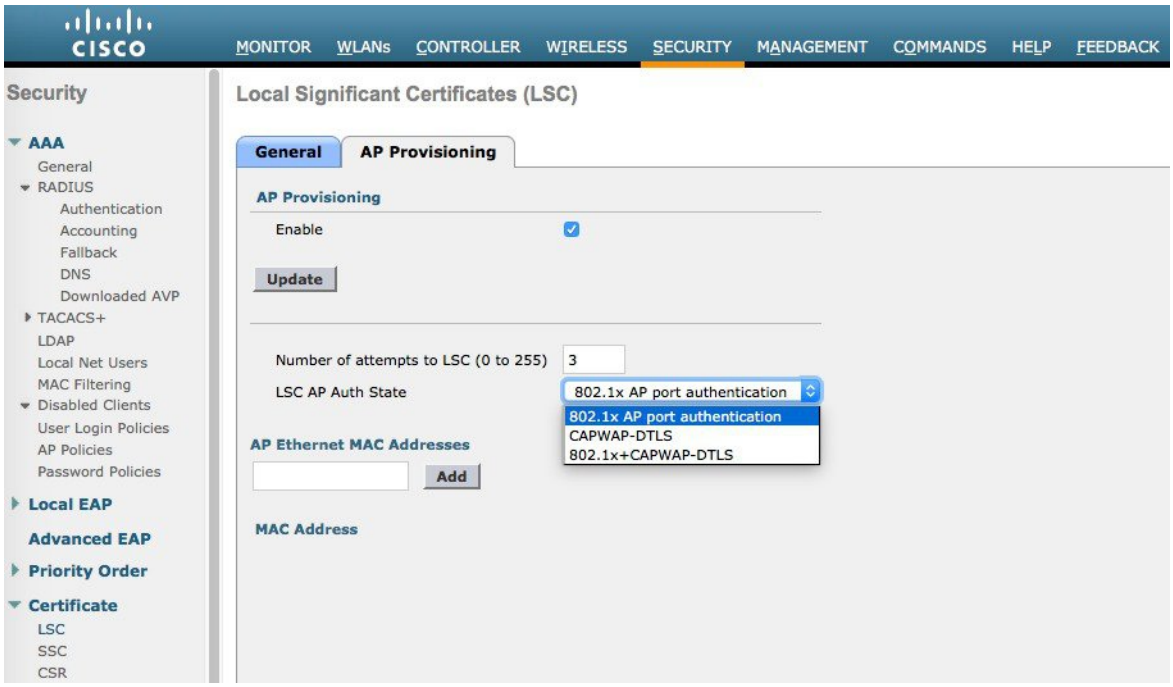
EAP-FAST/TLS/PEAP 認証方式は、Wave-2 AP（1800、2800、3800、4800 シリーズ）でサポートされています。

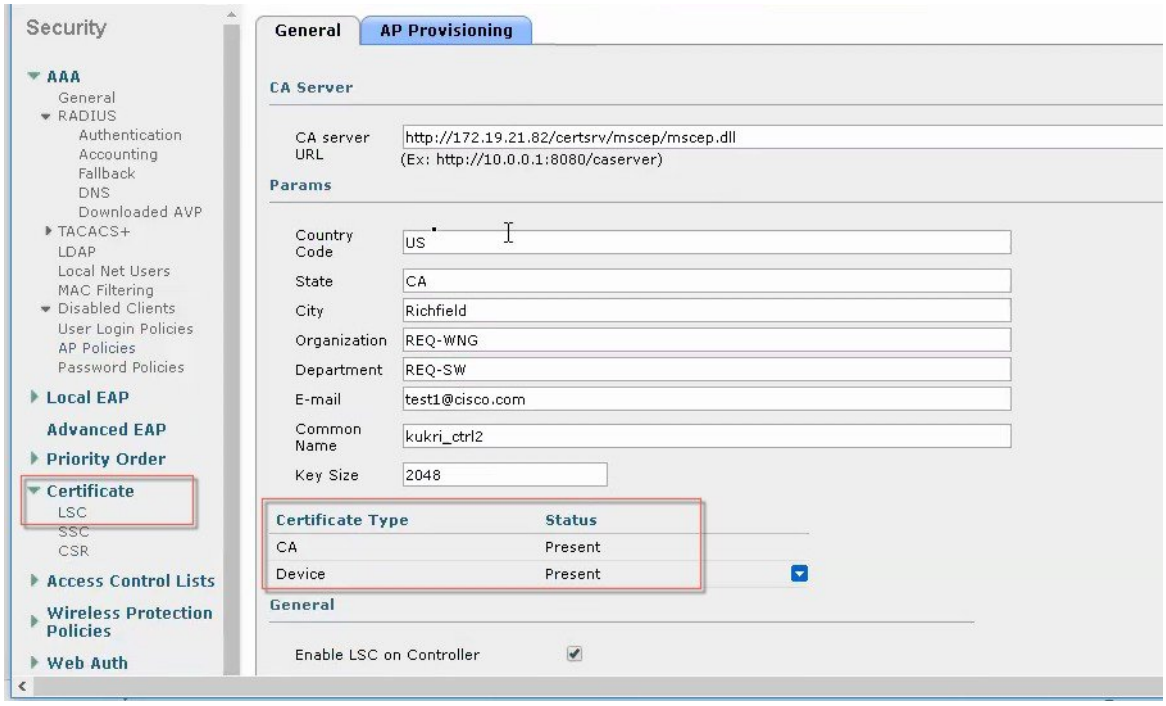
AP の CAPWAP DTLS LSC サポートは、AP への証明書のプロビジョニングおよびダウンロードに使用されます。リリース 8.7 では、Flex、Local、Mesh モードの RAP がサポートされています。



次のスクリーン ショットは、LSC 設定での AP プロビジョニングを示しています。







要件 4：SSL と初期の TLS を使用している事業体は、できるだけ早期に強力な暗号化プロトコルにアップグレードする。また、SSL や初期の TLS が存在しない環境に新たに導入してはならない。本バージョンの発行時点では、POS POI 支払い環境で既知の脆弱性を不正利用するのは困難であるが、常に新しい脆弱性が発生する可能性があるため、組織は責任を持って脆弱性の傾向に関する最新情報を取得し、既知の脆弱性の影響を受けるかどうかを判断する。

要件 4.1：

オープンな公衆ネットワーク経由で機密性の高いカード所有者データを送信する場合、強力な暗号化方式とセキュリティ プロトコルを使用して保護する。以上の要件に対応するセキュリティ コントロールとして SSL および初期の TLS は利用できない。SSL または初期の TLS からの移行に対応するため、以下の規定が設けられている。

- 新しく実装する場合は、SSL または初期の TLS をセキュリティ コントロールとして使用しない。
- すべてのサービス プロバイダーは、2016 年 6 月 30 日までに、安全なサービスを提供する。
- 2018 年 6 月 30 日以降は、すべての事業体が SSL/初期の TLS をセキュリティ コントロールとして使用することを中止し、安全なバージョンのプロトコルのみを使用する（一定の POS POI 端末の除外についてはこの箇条書きの最後の項目を参照）。
- 2018 年 6 月 30 日までは、既存の実装で SSL/初期の TLS を使用している場合、正式なリスク軽減策および移行計画を整備する。
- SSL および初期の TLS に対する既知の攻撃を受ける可能性が低いことを検証可能な場合、該当の POS POI 端末（および接続先である SSL/TLS ターミネーション ポイント）は、2018 年 6 月 30 日以降も引き続きセキュリティ コントロールとして使用可能。

（注） 支払いデータの保護を規定した PCI DSS（PCI Data Security Standard）に準拠するには、2018 年6 月 30 日までに SSL/初期の TLS を無効にし、より安全な暗号化プロトコルである TLS 1.1 以降（TLS v1.2 を強く推奨）を実装する必要があります。

Cisco Unified Wireless Network では、以下に示すように、WebAuth および Web Management 用のセキュリティ暗号化方式として、暗号化オプションに High を指定して TLS v1.2 を使用することができます。

```
(5520-MA1) >config network secureweb cipher-option ?

high            Configure whether or not to use TLSv1.2 for web admin and web auth.
rc4-preference Configure RC4 cipher suite preference for SSL/TLS 1.0 based web administration and web authentication.
sslv2           Enable or disable SSLv2 for both web administration and web authentication.
```

サポートされている AP DTLS 暗号化方式は以下のとおりです。

```
(5520-MA1) >config ap dtls-cipher-suite ?

ECDHE-ECDSA-AES128-GCM-SHA256        Select ECDHE-ECDSA-AES128-GCM-SHA256 cipher
ECDHE-ECDSA-AES256-GCM-SHA384        Select ECDHE-ECDSA-AES256-GCM-SHA384 cipher
RSA-AES128-GCM-SHA256        Select RSA-AES128-GCM-SHA256 cipher
RSA-AES128-SHA        Select RSA-AES128-SHA cipher
RSA-AES256-GCM-SHA384        Select RSA-AES256-GCM-SHA384 cipher
RSA-AES256-SHA        Select RSA-AES256-SHA cipher
RSA-AES256-SHA256     Select RSA-AES256-SHA256 cipher
```

TLS 1.2 SHA2 ファミリ（非 AEAD）

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256（0x6b）
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（0xc028）
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（0xc027）
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256（0x67）

（注） TLS 1.2 暗号化方式を適用する際に、その方式をサポートしていない古い AP または Wave-2 非対応の AP がネットワークに存在する場合は、細心の注意を払ってください。TLS 1.2 をサポートしていない AP はダウンし、ネットワーク カバレッジの問題が発生します。

使用する AP DTLS バージョンは、DTLS バージョン 1.0 または 1.2、もしくはその両方をコントローラで設定できます。

```
(Cisco Controller) >config ap dtls-version ?

dtls1.0             Select DTLS1.0 version
dtls1.2             Select DTLS1.2 version
dtls_all            Select all DTLS versions for backward compatibility

(Cisco Controller) >config ap dtls-version
```

（注） DTLS 1.2 プロトコルを適用する際に、そのプロトコルをサポートしていない古い AP または Wave-2 非対応の AP がネットワークに存在する場合は、細心の注意を払ってください。IOS ベースの AP と Wave-1 対応の AP がダウンし、ネットワークの中断が発生します。

次の表では、IOS および COS Wave-2 ベースの AP でサポートされている認証方式および TLS バージョンについてまとめています。また、IOS ベースおよび COS ベースの AP でサポートされている CAPWAP TLS バージョンも示しています。

SW Version	IOS AP - Port Auth		IOS -AP - CAPWAP	COS AP - Port Auth		COS-AP CAPWAP
8.3	EAP FAST	TLS 1.0	TLS 1.0	No support		TLS 1.0/1.2
8.5	EAP FAST	TLS 1.0	TLS 1.0	No support		TLS 1.0/1.2
8.6	EAP FAST	TLS 1.0	TLS 1.0	EAP FAST	TLS 1.0	TLS 1.0/1.2
8.7	EAP FAST	TLS 1.0	TLS 1.0	EAP-FAST, EAP-TLS, PEAP	TLS 1.0	TLS 1.0/1.2
8.8	EAP FAST	TLS 1.0	TLS 1.0	EAP-FAST, EAP-TLS, PEAP	TLS 1.2	TLS 1.0/1.2

図 *1 :*

		5508,2504,8510	5520,3504,8540,vwlc
COS AP	UI(when we use HTTS)	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8
	Local-EAP	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8
	WPA2-EAP(ccmp)	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8
	LDAP	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8
	webauth	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8
	NMSP	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8
	local Auth on flex	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8	TLS1.0- 8.0, 8.2 TLS1.2 – 8.3,8.5.,8.6,8.7,8.8
	.1x Supplicant	TLS1.0- 8.0, 8.2, 8.3,8.5.,8.6,8.7 TLS1.2 –8.8	TLS1.0- 8.0, 8.2, 8.3,8.5.,8.6,8.7 TLS1.2 –8.8
	CAPWAP	TLS1.0- 8.0, 8.2 TLS1.0/1.2 –8.3,8.5.,8.6,8.7,8.8	TLS1.0- 8.0, 8.2 TLS1.0/1.2 –8.3,8.5.,8.6,8.7,8.8
	Mesh	TLS1.0- 8.0, 8.2 TLS1.0/1.2 –8.3,8.5.,8.6,8.7,8.8	TLS1.0- 8.0, 8.2 TLS1.0/1.2 –8.3,8.5.,8.6,8.7,8.8

		5508,2504,8510	5520,3504,8540,vwlc
IOS AP	UI(when we use HTTS)	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8
	Local-EAP	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8
	WPA2-EAP(ccmp)	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8
	LDAP	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8
	webauth	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8
	NMSP	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8
	local Auth on flex	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8
	.1x Supplicant	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8
	CAPWAP	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8	TLS1.0- 8.0, 8.2,8.3,8.5,8.6,8.7,8.8

その他の関連資料：

PCI データ保護基準バージョン 3.2

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1525790995255

Cisco PCI DSS 設計および実装ガイド

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Compliance/Compliance_DIG/Compliance_DIG.pdf

Cisco SAFE SSL/TLS 脆弱性対応

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone/ssl-tls-vulnerability-response.pdf

PCI セキュリティ スタンダード カウンシル

https://www.pcisecuritystandards.org/document_library

シスコ ワイヤレス導入ガイド

https://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-technical-reference-list.html

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/