補足情報

SSL および初期の TLS からの移行

バージョン 1.1
日付: 2016 年 4 月
作成者: PCI SSC

概要

早急に移行することをお勧めします。

20 年以上にわたって一般的な暗号化プロトコルとして普及してきた Secure Sockets Layer（SSL）は、セキュリティ脆弱性にさらされているとはいえ、現在でも広く利用されています。

SSL v3.0 は 1999 年に TLS v1.0 に更新され、その後 TLS v1.1 および v1.2 に更新されました。SSL および初期の TLS は、プロトコルに未修正のセキュリティ脆弱性が存在するため、現在では最低限のセキュリティ基準も満たさなくなっています。事業体が早急に安全な代替プロトコルにアップグレードし、縮退した SSL および初期の TLS を無効にすることがきわめて重要です。

PCI DSS v3.1 では、SSL および初期の TLS は強力な暗号化の例から削除されました（2015 年 4 月）。

リスク内容

SSL/TLS では、チャネル（Web ブラウザと Web サーバ間など）を暗号化して、通信チャネル上を伝送されるデータのプライバシーと信頼性を確保します。SSL v3.0 のリリース以降、複数の脆弱性が発見され、最近では 2014 年に、安全な接続からデータを抽出して攻撃することが可能なセキュリティ脆弱性の詳細（CVE-2014-3566）が研究者によって公表されました。この脆弱性は POODLE（Padding Oracle On Downgraded Legacy Encryption）という通称でよく知られ、SSL v3.0 でセキュリティ保護された暗号化メッセージの解読を可能にする中間者攻撃です。

POODLE などの脆弱性を修正する方法が分かっていないため、SSL プロトコル（すべてのバージョン）は修正できません。SSL および初期の TLS は、公開の、または信頼されていない通信チャネル上で支払いデータを保護するための強力な暗号化を事業体が実装する場合のセキュリティニーズを満たさなくなりました。また、最近の Web ブラウザでは、ユーザが新しいプロトコルに移行していない Web サーバにアクセスすることを防ぐため、SSL 接続が禁止されるようになり始めました。

対応方法

最善の対応は、SSL を完全に無効化してなるべく新しい暗号化プロトコルに移行することです。本書の発行時点では TLS v1.1 以上とされていましたが、TLS v1.2 への移行を検討することが強く推奨されます。TLS v1.1 のすべての実装が安全と見なされているわけではないので注意が必要です。安全な TLS 構成の指針については、NIST SP 800-52 rev 1 を参照してください。

PCI DSS への影響

PCI DSS v3.1 では、SSL および初期の TLS は強力な暗号化および安全なプロトコルの例ではなくなりました。PCI DSS 要件への直接的な影響を以下に示します。

要件 2.2.3	安全でないとみなされている必要なサービス、プロトコル、またはデーモンに追加のセキュリティ機能を実装する。
要件 2.3	強力な暗号化を使用して、すべてのコンソール以外の管理アクセスを暗号化する。
要件 4.1	オープンな公共ネットワーク経由で機密性の高いカード会員データを伝送する場合、強力な暗号化とセキュリティプロトコルを使用する。

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 を利用することは推奨できません。SSL および初期の 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ます。

- 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（新しい実装と既存の実装のガイダンスについては次のセクションを参照）
- すべてのサービスプロバイダは、**2016 年** 6 月 30 日までに、安全な TLS サービスを提供する必要がある
- **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、プロトコルの安全なバージョンのみを使用する必要がある（一定の POS POI 端末の許容についてはこの箇条書きの最後の項目を参照）

- 2018 年 6 月 29 日以前に既存の実装で SSL/初期の TLS を使用している場合は、正式なリスク緩和および緩和計画が整備されている必要がある
- SSL および初期の TLS が既知の攻撃を受けやすいものでないことを検証可能な POS POI 端末(および SSL/TLS 端末)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することができる

SSL または初期の TLS を使用している場合、PCI DSS の付録 A2「SSL/early TLS を使用している事業体向けの PCI DSS 追加要件」の要件が適用されます。

「新規」と「既存」の実装について

脆弱なプロトコルの使用に依存していない実装は「新規の実装」とみなされます。「新規」の実装とみなされる例を以下に示します。

- 現在、安全なプロトコルのみを使用している環境へのシステムの導入
- 現在、安全なプロトコルのみを使用しているシステムへのアプリケーションの導入
- 安全なプロトコルをサポートする他のシステム/ネットワークと通信を行う新しいシステムまたはネットワークの構築

新しい実装で既存の脆弱なプロトコルの使用をサポートする必要がない場合は、安全なプロトコルと強力な暗号化のみを実装し、脆弱なプロトコルへの縮退を許容しない構成にする必要があります。

注: *新しい電子商取引の実装では、消費者の Web ブラウザをサポートする必要がある既存インフラストラクチャとはみなしません。*

「既存」の実装とは、脆弱なプロトコルの使用に依存している実装です。「既存」の実装とみなされる例を以下に示します。

- 現在、脆弱なプロトコルを使用またはサポートする必要がある環境へのシステムの導入
- 現在、脆弱なプロトコルを使用またはサポートする必要があるシステムへのアプリケーションの導入
- 現在、脆弱なプロトコルを使用している他のシステム/ネットワークと通信を行う新しいシステムまたはネットワークの構築

SSL/初期の TLS の使用を続けると環境がリスクにさらされるため、既存の実装を速やかにアップグレードすることが推奨されます。

リスク緩和および緩和計画の準備

リスク緩和および緩和計画は、事業体が準備し、安全なプロトコルへの移行計画の詳細および移行の完了までに SSL/初期の TLS に関連するリスクを軽減するために事業体が導入している対策を記述した文書です。リスク緩和および緩和計画は、PCI DSS 評価プロセスの一部として評価者に提供する必要があります。

リスク緩和および緩和計画に記載する情報のガイダンスと例を以下に示します。

- 脆弱なプロトコルをどのように使用しているかについての説明(以下のような情報を含む)
  - 該当プロトコルを使用している環境の種類(例: プロトコルを使用している支払チャネルや機能の種類)
  - 伝送するデータの種類(例: ペイメントカードのアカウントデータ、管理接続などの要素)
  - 該当プロトコルを使用またはサポートするシステムの数と種類(例: POS POI 端末、決済切替 など)
- リスク評価の結果と導入したリスク低減策:
  - 事業体は環境のリスクを評価し、文書化して、脆弱なプロトコルの廃止が完了するまでのリスク緩和に有効なリスク低減策を実施する必要があります。
- 脆弱なプロトコルに関連する新しい脆弱性を監視するために実施しているプロセスの説明:
  - 事業体は新しい脆弱性について予防に努め、常に情報に通じている必要があります。新しい脆弱性が発表される都度、事業体は自社環境がさらされるリスクを評価し、移行が完了するまでの期間に追加のリスク低減策を実施する必要があるかどうかを判断する必要があります。
- SSL/初期の TLS が新しい環境に実装されていないことを確実にするために実施している変更管理プロセスの説明:
  - 事業体が脆弱なプロトコルを現在使用していない、またはサポートしていないのであれば、脆弱なプロトコルを環境に導入する理由はありません。変更管理プロセスには、変更によって環境に新しいセキュリティの弱点が生じていないことを確認するための変更の影響評価が含まれます。
- 目標移行完了日(2018 年 6 月 30 日以前)を含む移行プロジェクト計画の概要:
  - 移行計画の文書には、移行するシステム/環境および全体的な移行の完了期限を記載します。全体的な移行の完了期限は 2018 年 6 月 30 日以前にする必要があります。

よくある質問

リスク緩和策とはどのようなものですか?

脆弱なプロトコルを現在使用している環境では、リスク緩和策を導入し、継続的に使用することが、安全な代替手段が完成するまでの脆弱な環境の保護に役立ちます。

リスク低減に役立つ対策の一部を以下に示します。

- 脆弱なプロトコルを使用する機能を統合して対象システムの数を減らし、脆弱なプロトコルをサポートするシステムの数を削減することによって、攻撃対象領域を極力縮小する。
- 不要な場合には、Web ブラウザ、JavaScript、セキュリティに影響するセッションクッキーの使用を削除または無効化する。
- 下位バージョンのプロトコルへのダウングレード要求を検出およびブロックすることによって、脆弱なプロトコルを使用した通信の数を制限する。
- SSL/初期の TLS を既知の IP アドレス(これらのプロトコルの使用を必要とするビジネスパートナーなど)のみに許可するファイアウォールを構成し、その他のすべての IP アドレスの SSL/初期の TLS によるトラフィックをブロックするなどして、脆弱なプロトコルの使用を特定の事業体に制限する。
- 侵入防止システムの対象範囲の拡大、署名の更新、悪意のある行為を示すネットワークアクティビティのブロックによって検出/防止機能を強化する。
- 疑わしいアクティビティを積極的に監視し(脆弱なプロトコルへの縮退要求の異常な増加を特定するなど)、適切に対応する。

また、事業体は該当するすべての PCI DSS 要件を確実に実施する必要があります。該当する要件の一部を以下に示します。

- 新しい脆弱性に関する最新情報を維持して予防に努める(例: 脆弱性通知サービスやベンダのサポートサイトに登録して新しい脆弱性の出現に関する最新情報を入手する)。
- ベンダの推奨事項を適用して使用テクノロジを安全に構成する。

どのような移行オプションがありますか?

SSL/初期の TLS に代わるセキュリティコントロールとして実装および使用可能な追加暗号化措置の例を以下に示します。

- 安全に実装され、SSL/初期の TLS の縮退を許可しない構成にした、最新の安全なバージョンの TLS にアップグレードする。
- SSL/初期の TLS 上で送信する前に強力な暗号化でデータを暗号化する(例: フィールドレベルまたはアプリケーションレベルの暗号化を利用して、データを送信前に暗号化する)。
- 強力に暗号化されたセッション(IPsec トンネルなど)を先に設定してから、安全なトンネル内で SSL のデータを送信する。

また、2 因子認証を前述のコントロールと組み合わせて使用する方法で認証を保証することもできます。

選択する代替暗号化コントロールは、個別環境の技術および業務上の必要性に応じて異なります。

小規模な加盟店環境の場合はどうですか?

小規模な加盟店を含め、あらゆる種類の事業体が SSL/初期の TLS の問題によって影響を受けます。小規模加盟店は、顧客データのセキュリティを確保するため、カード会員データ環境から SSL/初期の TLS を削除するために必要な措置を取ることが重要です。

POI 環境の場合、小規模加盟店は端末提供者またはアクワイアラー(加盟店銀行)に問い合わせて、POS POI 端末が SSL の脆弱性の影響を受けるかどうかを判断してください。

その他の環境(仮想端末、バックオフィスサーバ、ユーザコンピュータなど)の場合、小規模加盟店は SSL/初期の TLS が使用されているかどうか、およびどこに実装されているかを確認し、直ちにアップグレードすることが可能か、それともアップグレードを延期する業務上の理由があるかを判断する必要があります(延期期限は 2018 年 6 月 30 日まで)。

使用環境について検討を推奨する事項

- システムで使用している Web ブラウザのバージョンを確認する（古いバージョンでは SSL/初期の TLS を使用し、必要に応じて新しいブラウザにアップグレードする）
- ファイアウォール構成で SSL をブロックできるかどうかを確認する
- すべてのアプリケーションおよびシステムのパッチが最新であるかどうかを確認する
- システムを確認および監視して、セキュリティの問題を示唆している可能性がある怪しい活動を特定する

また、安全な代替環境への移行を計画する際には、リスク緩和および緩和計画を作成する必要があります。

加盟店は SSL/初期の TLS をサポートする POI 端末をどう扱えばよいでしょうか?

現在既知の攻撃を受けやすいものでないことを検証可能であれば、SSL および初期の TLS を引き続き使用することができますが、SSL は廃止されるテクノロジであり、今後セキュリティ脆弱性が高まる可能性があります。できる限り、POI 環境に TLS v1.1 以上を使用することを強く推奨します。POI の新しい実装では、TLS 1.2 以上に対応し、これを使用することをぜひ検討してください。SSL/初期の TLS が不要な環境では、SSL/初期の TLS バージョンへの縮退の利用を無効にすることが推奨されます。

SSL/初期の TLS を使用している POI 端末の実装をレビューする場合、評価機関は、関係文書（POI ベンダが提出した文書、システム / ネットワーク構成の詳細など）をレビューして、既知の攻撃を受けやすい実装かどうかを判断する必要があります。

POS POI 環境が既知の攻撃を受けやすい場合、安全な代替環境への移行計画を直ちに開始する必要があります。

注: 現状で攻撃を受けやすくない POS POI を許容するかどうかは、現在の既知のリスクに基づいて判断します。POI 環境が攻撃を受けやすくなるような新しい攻撃が導入された場合は、POI 環境を更新する必要があります。

POS POI 環境の脆弱性が比較的低いのはなぜですか?

PCI DSS は、SSL および初期の TLS が POS（Point of Sale）加盟店端末装置（POI）およびターミネーションポイントで引き続き使用されることを許容しています。これは、発行時点の既知の脆弱性をこれらの環境で攻撃することが一般に困難になっているためです。

たとえば、現在の SSL の脆弱性の一部は、攻撃者がクライアント/サーバ通信を傍受し、クライアントへのメッセージを操作することによって攻撃されます。攻撃者の目的は、クライアントを騙してセッションの侵害に利用できるような追加データを送信させることです。以下の特徴を持つ POS POI 端末は、一般にこの種の脆弱性に対する防止効果が高くなります。

- 複数のクライアントサイド接続（POODLE 攻撃が容易になる）をサポートしていない端末
- ISO 20022（Universal Financial Industry Message Scheme）/ISO 8583-1:2003（Financial Transaction Card Originated Messages – Interchange Message Specifications）または同等の基準に準拠したペイメントプロトコル（反射攻撃による漏えいの可能性があるデータ量を制限する）
- Web ブラウザソフトウェア、JavaScript、セキュリティに関連するセッションクッキーを使用しない端末

注: これらの特徴は参考例に過ぎません。実際には、実装ごとに単独で評価して脆弱性の程度を判断する必要があります。

攻撃は進化を続けるものであり、組織は新しい脅威に対応する準備をしておく必要があることを銘記してください。SSL/初期の TLS を使用しているすべての組織は、早急に強力な暗号化プロトコルへのアップグレードを計画する必要があります。

POS POI 環境で SSL/初期の TLS を暫定的に使用する場合は、最新のパッチを適用し、必要な拡張のみを有効にする必要があります。

POI 環境をサポートするペイメントプロセサーにとって、これはどういう意味を持ちますか?

ペイメントプロセサー、ペイメントゲートウェイ、取引処理サービスを提供するその他の事業体など、あらゆる種類の事業体が SSL/初期の TLS の問題の影響を受けます。これらの事業体は SSL/初期の TLS の使用を見直し、他の事業体と同様の方法で移行を計画する必要があります。

POI 端末を利用する支払決済事業体が引き続き SSL/初期の TLS を使用する場合、（前述の「POS POI 環境の脆弱性が比較的低いのはなぜですか?」のセクションの説明に従って）POI 通信が脆弱ではないことを検証する必要があります。

支払決済事業体が同じ終端点で複数の支払チャネル（例: POI と電子商取引）に対応している場合、2018 年 6 月 30 日までにすべての脆弱なチャネルを安全な代替環境に確実に移行する必要があります。POI 環境が脆弱ではないとみなされる場合、事業体は以下の選択肢を検討する必要があります。

- POI チャネルを安全な代替環境に移行して、POI と電子商取引の両方で引き続き同じ終端点を使用できるようにする。
- POI チャネルを移行しない場合は、別の終端点/インターフェイスを使用して、安全な代替環境に移行した電子商取引トラフィックから SSL/初期の TLS を使用する POI トラフィックを分離することができる。

電子商取引環境の場合はどうですか?

Web ベースの環境の性質上、電子商取引の実装は脆弱性リスクが最も高く、SSL/初期の TLS の既知の脆弱性によるリスクが差し迫っています。

そのため、新しい電子商取引 Web サイトで SSL/初期の TLS を使用またはサポートすることはできません。

当面、SSL/初期の TLS を使用している顧客をサポートする必要がある電子商取引環境については、なるべく早急に移行を開始し、2018 年 6 月 30 日までにすべての移行を完了する必要があります。移行を即座に実施できない場合は、リスク緩和および緩和計画にその理由を記載する必要があります。

移行が完了するまでの間、SSL/初期の TLS をサポートするサーバの数を極力少なくすることが推奨されます。脆弱なシステムの数を削減することで、攻撃にさらされる可能性が低減し、疑わしいトラフィックの監視を強化するなどのリスク緩和策の効率化にも役立つ場合があります。

また、電子商取引加盟店は、顧客に安全なプロトコルに対応した Web ブラウザへのアップグレードを勧めることが推奨されます。

移行プロセスはどこから開始すればよいでしょうか?

事業体が安全な代替環境への移行を計画する際に役立つ推奨手順を以下に示します。

1. 脆弱なプロトコルに依存および対応しているすべてのシステムコンポーネントとデータフローを特定する
2. 各システムコンポーネントとデータフローについて、脆弱なプロトコルを使用する業務上または技術上の必要性を特定する
3. 業務上または技術上サポートする必要性がない脆弱なプロトコルのすべてのインスタンスを直ちに削除または無効化する
4. 脆弱なプロトコルの置換に使用するテクノロジを特定し、実装する安全な構成を文書化する
5. 更新の手順とスケジュールの概要を記載した移行プロジェクト計画の文書を作成する
6. 脆弱なプロトコルを環境から削除するまでの間、既知の攻撃を受けるリスクの軽減に有効なリスク低減策を実施する
7. 移行を実施し、変更管理手順に従って確実にシステムの更新をテストし、承認を受ける
8. 新しいプロトコルへの移行が完了した時点でシステム構成基準を更新する

セキュリティコントロールとして使用しない SSL および初期の TLS を環境に残しておくことはできますか?

はい。セキュリティコントロールとして使用しない限り、SSL および初期の TLS をシステムに残しておくことはできます。

また、ASV スキャンで CVSS 4 以上のスコアが付けられた、または事業体の脆弱性スキャンで「高」にランク付けされたすべての SSL/TLS 脆弱性は、PCI DSS 要件 11.2 に準拠して、所定の期間内(例: ASV スキャンの場合は四半期に一度)に対処する必要があります。規定された脆弱性管理プロセスに従い、SSL/TLS の脆弱性への対処方法を文書化します。たとえば、攻撃を受けやすくない POI 通信のみに SSL/TLS を使用する、SSL/TLS は存在するが、セキュリティコントロールとして使用しない(通信の機密性の保護に使用しないなど)といったことを記載します。

SSL/初期の TLS の使用によってカード会員データの侵害が生じない場合、移行期日は適用されますか?

はい。SSL/初期の TLS からの移行期日は、将来予想されるペイメントカードデータの侵害件数とは無関係です。PCI DSS 要件の目的は、多層防御手法によってカード会員データの侵害を防ぐことにあります。データ侵害の可能性が公表されるまで待ってから所有データのセキュリティ対策を取ることは有効なセキュリティ手法とはいえず、PCI DSS ではサポートされていません。

SSL の存在は ASV スキャンの結果にどう影響しますか?

SSL v3.0 および初期の TLS には複数の脆弱性が存在し、その中には現在 CVSS(Common Vulnerability Scoring System: 共通脆弱性評価システム)のスコアが 4.3 になる脆弱性もあります。CVSS は NVD(米国脆弱性データベース)によって定義され、ASV が使用を義務付けられて

いる評価システムです。中または高リスクの脆弱性（CVSS の脆弱性スコアが 4.0 以上）は修正し、修正後に影響するシステムを再度スキャンして問題に対処したことを示す必要があります。

ただし、既知の修正方法が存在しない脆弱性の場合には、緩和策として、できる限り早急に安全な代替環境に移行することが推奨されます。安全な代替環境に即座に移行できない場合は、ASV と協力して以下のように特別な事情を文書化する必要があります。

- *2018 年 6 月 29 日以前:* 移行を完了した事業体は、リスク緩和および緩和計画を実施したこと、および所定の期日までに移行を完了するよう作業を進めていることを確認する文書を ASV に提出する必要があります。ASV は、「ASV Scan Report Executive Summary（ASV スキャン報告書の要約）」の「Exceptions, False Positives, or Compensating Controls（例外、誤検出、または代替コントロール）」に、この確認を受領したことを例外として記載する必要があります。対象ホストが該当するすべてのスキャン要件を満たしている場合、ASV はそのスキャンコンポーネントまたはホストの結果として「合格」を発行することができます。
- *2018 年 6 月 30 日以降:* SSL/初期の TLS からの移行が完了していない事業体は、「Addressing Vulnerabilities with Compensating Controls（代替コントロールによる脆弱性への対処）」の手順に従って、対象システムが特定の脆弱性の影響を受けやすいものではないことを検証する必要があります。たとえば、システム上に存在する SSL/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場合（通信の機密性の保護に使用しないなど）がこれに当たります。

特定の脆弱性の影響を受けやすいものではないことが検証された POS POI 端末および終端点を持つ事業体は、該当システムの NVD スコアが低く算定される可能性があります。この場合、ASV は ASV プログラムガイドに従い、（報告に必要なその他のすべての要素に加えて）以下の情報を提供する必要があります。

- NVD による脆弱性の評価
- ASV による脆弱性の評価
- ASV と NVD の評価が一致しない理由

たとえば、ASV は、特定の脆弱性が一般的な NVD 評価システムで定義されているよりも特定の POS POI 環境で攻撃を受けにくいと判断する可能性があります。その場合、ASV は対象システムの特定の脆弱性について評価システムの該当要素のランクを変更することができます。

この種の調整を行う場合、ASV は一般的な傾向や仮定に基づいて調整を行うのではなく、クライアント固有の環境、システム、コントロールを考慮する必要があります。スキャンを受ける顧客は、ASV と協力して環境の概要を提示する必要があります。そうしなければ、CVSS のスコアを変更することが適切かどうかを ASV が判断できません。

このような権利を行使する場合、ASV は正当な注意義務を果たし、CVSS スコアの変更を裏付ける十分な根拠があることを確認する必要があります。これらの変更はすべて ASV プログラムガイドに定義されたプロセスに従う必要があります。

すべての ASV スキャン レポートは ASV プログラムガイドのプロセスに従って作成する必要があります。

これは、リスク緩和および緩和計画を整備した事業体は SSL/初期の TLS の脆弱性のパッチ処理を行う必要がないことを意味しますか?

いいえ。移行期日を理由にして脆弱性のパッチ処理を遅らせることはできません。新しい脅威やリスクも該当する PCI DSS 要件（6.1、6.2、11.2 など）に従って管理する必要があり、事業体は、セキュリティの更新プログラム、修正、パッチが存在する場合は脆弱性に対処する必要があります。

安全なプロトコル（TLS v1.2 など）および安全ではないプロトコル（SSL/初期の TLS など）をサポートするサービスにはどのような影響がありますか?

多くのサービスプロバイダ（共有ホスティングプロバイダなど）は、PCI DSS 要件に準拠する必要がある事業体および準拠する必要がない事業体を含む幅広い顧客層にプラットフォームやサービスを提供します。顧客の CDE をサポートするサービスプロバイダは、顧客に代わって該当する要件を満たしていること、または PCI DSS 要件に準拠したサービスオプションを顧客が利用するために提供していることを実証できます。サービスプロバイダは、提供しているセキュリティプロトコル、別のオプションの構成方法、安全ではないとみなされている構成を利用した場合の影響を顧客に明確に伝える必要があります。

たとえば、Web ホスティングプロバイダが TLS v1.2 とこれより脆弱なプロトコルをサポートするホステッド Web プラットフォームを加盟店に提供している場合、ホスティングプロバイダは顧客の PCI DSS 準拠に対応するため、TLS v1.2 のみを使用し、SSL/初期の TLS に縮退しないようにサービスの使用を構成する明確な手順を顧客に示す必要があります。顧客側から見ると、PCI DSS の実装の一部としてこのプラットフォームを使用している加盟店は、TLS v1.2 を使用し、SSL/初期の TLS に縮退しない構成オプションを確実に設定する必要があります。

混在ホスティング環境により脆弱なプロトコルが存在すると、ASV スキャンが失敗する原因になります。ASV スキャンが失敗した場合、サービスプロバイダと ASV は「Exceptions, False Positives, or Compensating Controls（例外、誤検出、または代替コントロール）」のプロセスに従い、たとえば、サービスプロバイダが SSL/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こと、および脆弱なプロトコルへの縮退を許可しない安全な構成オプションが顧客の使用に供されていることを確認するなどの方法で、リスクへの対処方法を文書化する必要があります。対象ホストが該当するすべてのスキャン要件を満たしている場合、ASV はそのスキャンコンポーネントまたはホストの結果として「合格」を発行することができます。