「暗号化通信におけるリスク」

～ SSH に潜む落とし穴 ～

“暗号化すれば安全ですか？”

＜付録. 2＞　SSH に関わるセキュリティ基準

2015 年 09 月

〈付録. 2〉 SSH に関わるセキュリティ基準

SSH に関連する各種情報セキュリティ基準への対応状況を以下に記載する。

＜PCI DSS＞

以下に PCIDSS の詳細要件に対して SSH に関連する項目を抜粋する。

【凡例：○：単独で実現可能　△：運用次第で対応可能　×：実現不可】

PCIDSS 要件		OpenSSH 対応可否	Tectia SSH 対応可否	SSH における対応内容
要件 3　カード会員データの保護				
3.5.1	暗号化鍵へのアクセスを、必要最小限の管理者に制限する。	△	△	サーバに格納されている SSH 鍵のアクセス権を適切に設定/管理する。 (OS 側での制限)
要件 4　オープンな公共ネットワーク経由でカード会員データを転送する場合、暗号化する				
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転送する場合、以下のような、強力な暗号化とセキュリティプロトコル（SSL/TLS、IPSEC、SSH など）を使用して保護する。 ・信頼できる鍵と証明書のみを受け入れる。 ・使用されているプロトコルが、安全なバージョン又は設定のみをサポートしている。 ・暗号化の強度が使用中の暗号化方式に適している。	○	○	SSH プロトコルを利用することで対応可能である。

<付録.2> SSHに関わるセキュリティ基準

PCIDSS 要件		OpenSSH 対応可否	Tectia SSH 対応可否	SSH における対応内容
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・維持する				
6.3.1	アプリケーションがアクティブになる前、又は顧客にリリースされる前に、開発/テスト/カスタムアプリケーションアカウント、ユーザ ID、パスワードを削除する。	△	○	各サーバにログインし、不要な SSH 鍵やユーザ ID があれば削除する ※Tectia 製品を利用することで、不要な SSH 鍵を簡単に検出/可視化が可能。
要件 8　システムコンポーネントへのアクセスを確認・許可する				
8.3	従業員（ユーザと管理者を含む）および第三者（サポートやメンテナンス用のベンダアクセスを含む）によるネットワークへのリモートアクセス（ネットワーク外部からのネットワークレベルアクセス）に二要素認証を組み込む。	○	○	SSH では公開鍵認証の他にパスワード認証も組み合わせる等、簡単に 2 段階認証を行うことが可能である。
8.5	次のような、グループ、共有、又は汎用の ID やパスワード、又は他の認証方法を使用しない。 ・汎用ユーザ ID およびアカウントが無効化又は削除されている。 ・システム管理作業およびその他の重要機能に対する共有ユーザ ID が存在しない。 ・システムコンポーネントの管理に共有および汎用ユーザ ID が使用されていない。	○	○	SSH 鍵ファイル、ユーザ ID はユニークなものを設定し利用する ※Tectia SSH 製品を利用することで SSH 鍵利用時の作業効率化が可能。

PCIDSS 要件		OpenSSH 対応可否	Tectia SSH 対応可否	SSH における対応内容
要件 10 ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する				
10.1	システムコンポーネントへのすべてのアクセスを各ユーザにリンクする監査証跡を確立する。	△	○	デフォルトでは取得できる情報が少ないため、ログ設定をチューニングすることでより詳細な証跡が取得可能であるが、監査証跡の検索に掛かる時間や手間が大幅に掛かる。 ※Tectia 製品を利用することで手間をかけずに、SSH 通信の監査証跡を取得することが可能。
10.2	次のイベントを再現するために、すべてのシステムコンポーネントの自動監査証跡を実装する。 ・カード会員データへのすべてのアクセス。 ・ルート権限又は管理権限を持つ個人によって行われたすべてのアクション。	△	○	

＜ISO/IEC27001＞

以下に ISO/IEC27001 の詳細要件に対して SSH に関連する項目を抜粋する。

ISO/IEC27001 要件		OpenSSH 対応可否	Tectia SSH 対応可否	SSH における対応内容
A.9 アクセス制御				
A.9.1 アクセス制御に対する業務上の要求事項				
A.9.1.1 アクセス制御方針	アクセス制御方針は，業務及び情報セキュリティの要求事項に基づいて確立し，文書化し，レビューしなければならない。	△	○	SSH鍵情報を一覧化し管理する ※Tectia 製品を利用することで、SSH 鍵の状態を簡単に把握することが可能。
A.9.2 利用者アクセスの管理				
A.9.2.5 利用者アクセス権のレビュー	資産の管理責任者は，利用者のアクセス権を定められた間隔でレビューしなければならない。	△	○	各サーバにログインし、不要な SSH 鍵やユーザ ID の有無を確認する。 ※Tectia 製品を利用することで、不要な SSH 鍵を簡単に検出可能。
A.9.2.6 アクセス権の削除又は修正	全ての従業員及び外部の利用者の情報及び情報処理施設に対するアクセス権は，雇用，契約又は合意の終了時に削除しなければならず，また，変更に合わせて修正しなければならない。	△	○	各サーバにログインし、不要な SSH 鍵やユーザ ID の有無を確認する。 ※Tectia製品を利用することで、不要なSSH鍵を簡単に検出/削除可能。

ISO/IEC27001 要件		OpenSSH 対応可否	Tectia SSH 対応可否	SSH における対応内容
A.10 暗号				
A.10.1 暗号による管理策				
A.10.1.1 暗号による管理策の利用方針	情報を保護するための暗号による管理策の利用に関する方針は，策定し，実施しなければならない。	○	○	SSHプロトコルを利用することで対応可能である。
A.10.1.2 鍵管理	暗号鍵の利用，保護及び有効期間（lifetime）に関する方針を策定し，そのライフサイクル全体にわたって実施しなければならない。	△	○	SSH 鍵の状態確認、SSH 鍵の更新や削除等を定期的に実施する。 ※Tectia 製品を利用することで、鍵管理の効率化が可能。
A.12 運用のセキュリティ				
A.12.4 ログ取得及び監視				
A.12.4.3 実務管理者及び運用担当者の作業ログ	システムの実務管理者及び運用担当者の作業は，記録し，そのログを保護し，定期的にレビューしなければならない。	△	○	デフォルトでは取得できる情報が少ないため、ログ設定をチューニングすることでより詳細な証跡が取得可能である。 ※Tectia 製品を利用することで手間をかけずに、SSH 通信に関する監査証跡を取得することが可能。

〈補足〉

オープンソースの SSH 製品では上記の各種セキュリティ基準を満たすことができない項目があるが、Tectia SSH 製品を利用することで手間をかけず、上記の各種セキュリティ基準を満たすことが可能である。

Tectia SSH 製品シリーズの各製品における各種セキュリティ基準への対応について以下に記載する。

Tectia SSH 製品名	セキュリティ基準		備考
	PCI DSS	ISO/IEC27001	
Universal SSH Key Manager	6.3.1 8.5	A.9.1.1 A.9.2.5 A.9.2.6 A.10.1.2	本製品を導入することで、不要な鍵の検出や定期的な鍵のアクセス制御状態確認等が容易に行えるので、SSH 鍵運用の効率化という形で対応可能。
Crypto Auditor	10.1 10.2	A.12.4.3	本製品を導入することで、容易に監査証跡の取得/保存が行え、サーバ側での変更は必要最小限に抑える形で対応が可能。
・Tectia SSH Client/Server ・Tectia ConnectSecure	3.5.1 4.1 8.3	A.10.1.1 A.12.4.3	PCI DSS 3.5.1 については OS 側の鍵ファイルのアクセス権限の話であるが、鍵の保存場所自体を必要最小限の権限がついた別の場所に変更といった対応が可能。