コンプライアンス・ホワイトペーパー

PCI DSS バージョン 3 に対応するための Secure Shell ガイド

ssh®
Securing the path to your information assets

目次

SSH Communications Security 社について:

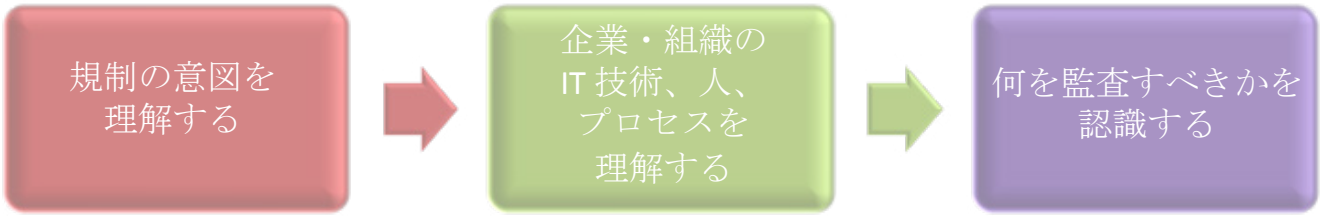
1995年に設立されたSSHコミュニケーション・セキュリティ社は、データ転送のセキュリティ・ソリューションとしての標準プロトコルであるSSHプロトコルを発明・開発した企業です。フォーチュン10に数えられる企業の内の7社を含む世界中の3,000社以上の顧客が、SSH 社の情報保証プラットフォームを採用しています。SSH 社のプラットフォームは、あらゆる業種や規模のビジネスの外部及び内部環境でのデータをデータ損失から保護し、境界セキュリティを強化します。また、同社の二要素認証システムや内部セキュリティ制御管理ソリューションを併せて利用することで、ユーザー鍵の管理やネットワークにおける管理者の通信の監視も含め、より簡単に通信データの保護を強化することができます。

ssh®
Securing the path to your information assets

はじめに

IT 監査担当者は様々な困難に直面しています。彼らは急速に進化する規制要件や技術、出現する脅威に追従するという困難と向きあっています。彼らはまた、IT 技術、ガバナンス、人、プロセスが規制に対応するためのセキュリティの目的に合致しているかしていないかも、理解する必要があります。

これら問題点は、以下のように要約されます。



要は、他の優れた調査担当者同様、セキュリティの監査担当者は、どのような問題を問いただすべきかを知っている必要があるということになります。

クレジットカード情報環境における Secure Shell

Secure Shell(SSH)は、IT基盤のいわゆる縁の下の力持ちです。これはサーバ、アプリケーション、ネットワークを管理、維持、更新するために、アプリケーション開発者やシステム管理者が選択する必須ツールです。ミッション・クリティカルなバックアップやビジネス継続性のためのプロセスも SSH によって保護されています。更に、SSH は IT システムが日々実行する数千の自動化されたプロセスに使用されおり、PCI DSSの対象となるクレジットカード会員データを企業内、企業間で転送する IT システムの運用にも使用されています。

Secure Shell のコアは、その認証基盤にあります。どのように人間のユーザーとアプリケーション･プロセスの両方がそれぞれのアイデンティティと許可を証明するのかという問題です。多くの場合、この認証は Secure Shell のユーザー鍵に基づいたインフラストラクチャを利用して行われます。Secure Shell 接続を受け付けるサーバ及びアカウントに対し身元を証明する公開鍵・秘密鍵ペアの仕組みです。

企業環境内に存在する SSH ユーザー鍵の数は驚くべきものです。SSH コミュニケーション・セキュリティ社があるグローバルな銀行で実施した監査では、150万個以上のSSHユーザー鍵が検出されました。このうち15万個以上の鍵がルート・アクセス権を許可されているだけでなく、所有者が不明な鍵でした。これはアカウントに関連する個人の身元もわからずに最も高いレベルの特権アクセスを、15万個のアカウントに許可していることと同等の状況を表しています。

本ホワイトペーパーは、クレジットカード会員データ環境(CDE)においてSecure Shellの使用がPCI DSSバージョン3の特定の意図、ガイダンス、及び要件にどのように関連するかに焦点をあてます。特にQSAおよび内部セキュリティ調査担当者がPCIDSSの監査の際に確認すべき詳細なガイダンスを提供します。

PCI DSS のコントロール

PCI DSS は、クレジットカード会員データを保護するための技術及び運用上の要件基準を提供します。PCI DSS の仕様、ガイドライン及びその意図は、以下の図1で示される構造化された形で整理されています。

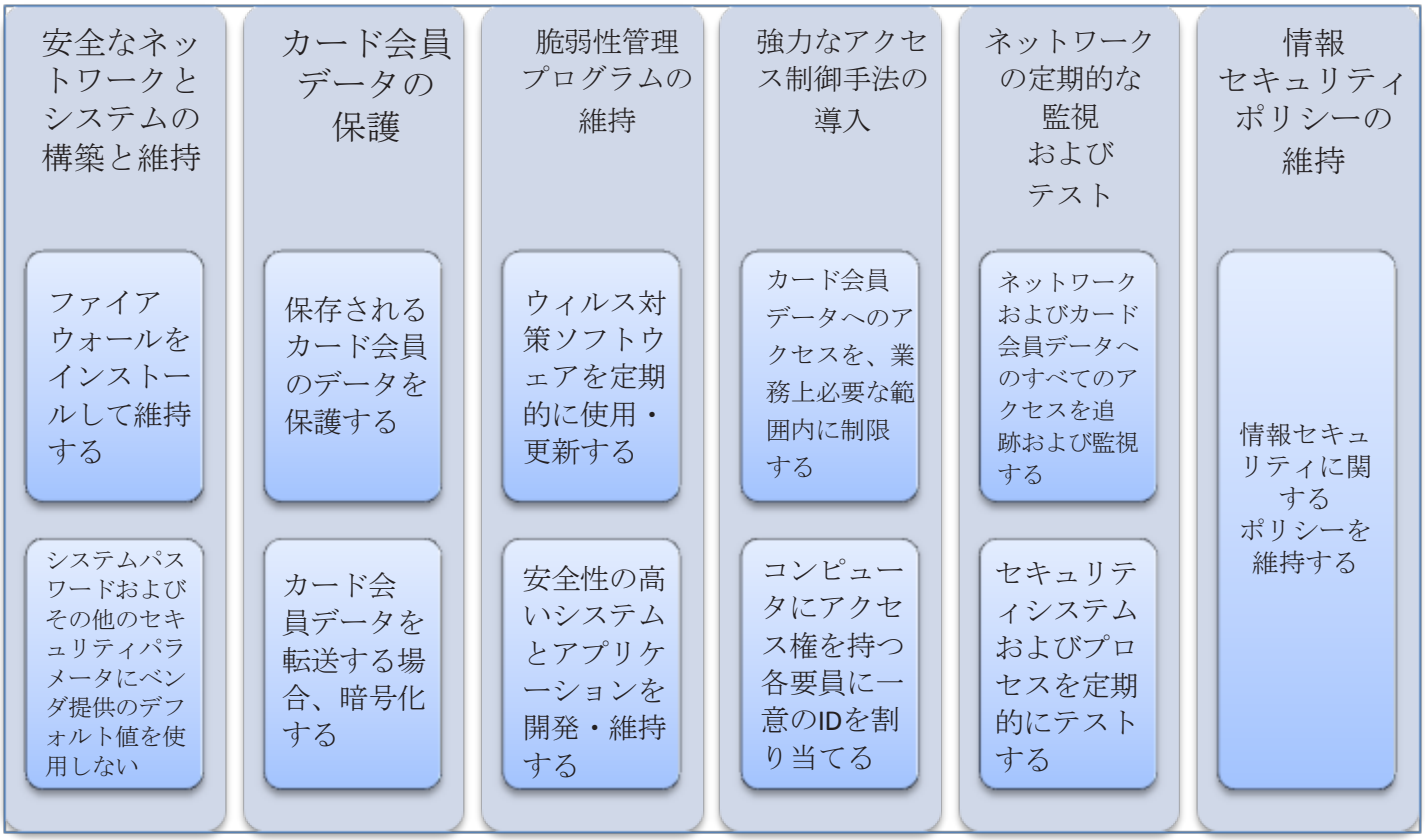


図1: PCI DSS の上位構造

PCI DSS は、上位の各要件にさらに詳しい特定の要件、テスト手順、ガイダンスを提供しています。しかしながら、IT 環境で使用されている技術が多様化しているため、すべての技術に対してPCI DSS が詳細なガイダンスとテスト手順を提供することは現実的ではありません。それゆえ、指定した環境及び監査でどの技術を使用するかは監査担当者が決定すべき事項として残されています。したがって、監査担当者は、監査する環境内でどのような技術が使用されているかの特定し、それに応じて監査する必要があります。

例えば、要件 6(安全なネットワークとシステムの構築と維持)の要件 6.4.2 は、開発/テスト環境と本番環境での責務の分離を指示しています。しかし、それらの環境へのアクセスを許可するために使用することができる技術への指示はありません。それゆえ、監査担当者は特定の環境においてどのようなアクセス技術やプロセスが展開されているかを理解し、責務の分離が維持される方法で適用されていることを確認する必要があります。以下の図 2 では、一般の PCI DSS のコントロール（赤枠）に Secure Shell の技術的詳細に関するガイダンスを付け加え（青枠）説明しています。

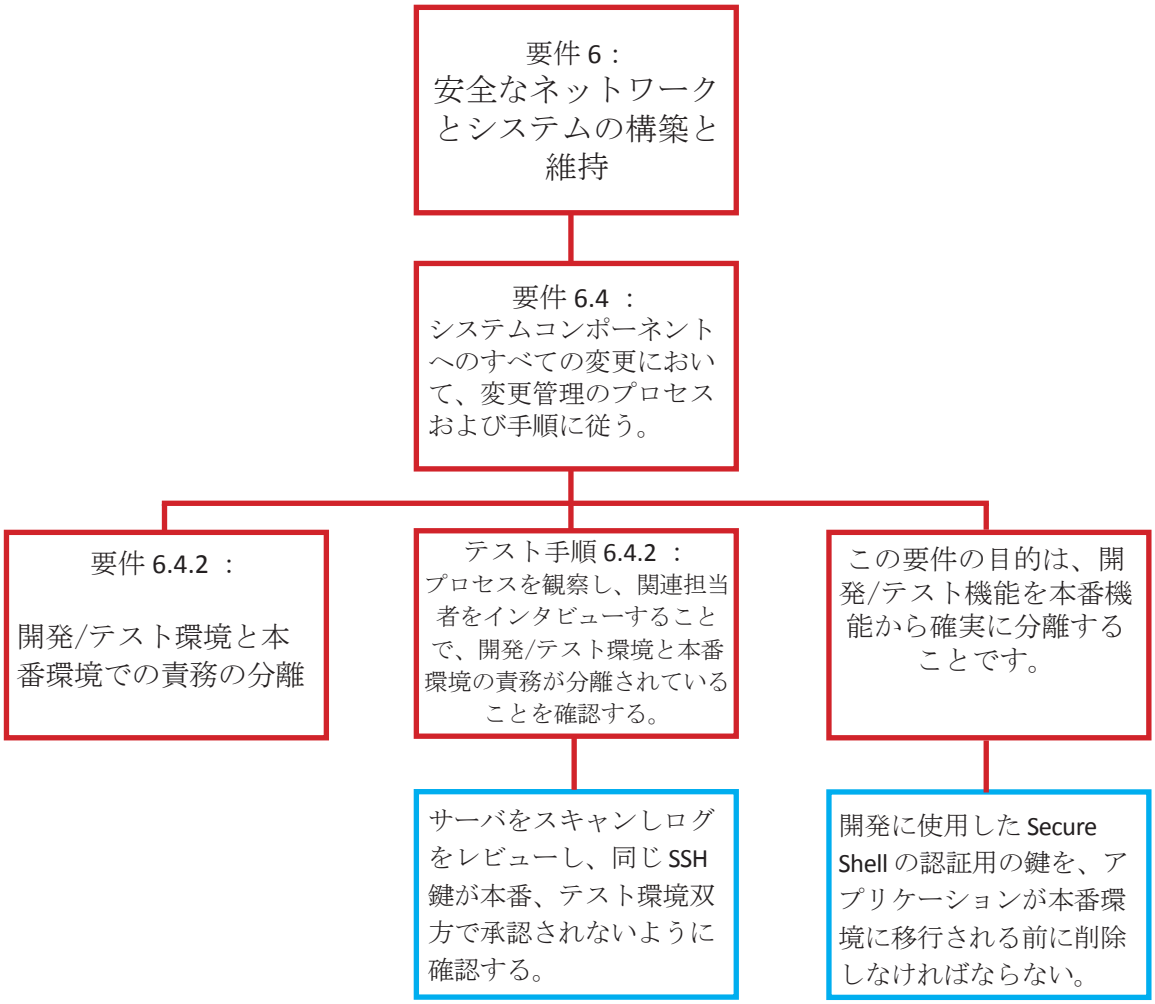


図 **2: PCI DSS** 要件、テスト手順や及び意図は、技術固有のものではない

PCI DSS の監査のための基本的な調査ガイダンス

以下の表 1 は、PCI DSS の監査対象範囲で Secure Shell が展開されている場合の、監査担当者用の調査ガイダンスです。

調査のための基本的な質問事項	ガイダンス
CDE 内にSecure Shell が展開されていますか。	回答がいいえの場合でも、監査担当者はこれを証明するためにスキャンを行う必要があります。
どのシステムが Secure Shell を実装し、どのシステムが実装していませんか。	監査担当者はこれを証明するためにスキャンを行う必要があります。
Secure Shell はどのような目的で使用されていますか。	Secure Shell は下記の用途の複数もしくは全てにおいて利用されている可能性があります：システム管理者アクセス、アプリケーション管理者アクセス、開発者アクセス、機器の管理アクセス、自動化プロセス、ファイル転送、リモートデスクトップ、バックアップ・リストア、システムのフェイルオーバー、VPN アクセス、契約業者あるいはビジネスパートナーとの通信。
Secure Shell セッションの認証に SSH のユーザー鍵認証を使用していますか。	使用されている基本的な認証システムを理解することは、今後の監査手順を決定するものになります。ユーザー鍵は広範囲に展開されているものです。
ユーザー鍵を作成し割当てるための手続きを明記して下さい。	ユーザー鍵はログイン・クレデンシャルです。PCI DSS の認証クレデンシャルに関する全ての手続き及び保護に対する用件は、ユーザー鍵にも適用されます。
ユーザー鍵を追跡するためのプロセスを説明してください。	SSH ユーザー秘密鍵を所有する全ての人又はプロセスは、この秘密鍵に対応する公開鍵があるアカウントへのアクセス権を持ちます。これらの鍵の配布を追跡しコントロールすることは基本的なセキュリティ要件です。
ユーザーの役割が変わるあるいは組織を去る際の鍵の削除の手続きを明記して下さい。	これらの状況下では、ユーザーのアクセス権は削除されなくてはなりません。ユーザーに割り当てられたすべての公開鍵を削除しなくてはなりません。
どのくらいの頻度で鍵が更新されていますか。鍵更新の手続きを明記して下さい。	定期的な鍵更新のポリシーを施行し、実施しなければなりません。
ユーザー鍵を作成しインストールする権限を何人に承認していますか。	新しい SSH の権限付与は中央で行い、他の形式のアクセス及びクレデンシャルを管理する際に使用するのと同様の権限の抑制と均衡が行われなければなりません。
秘密鍵のパスフレーズは保護されていますか。パスフレーズの使用、その強度、更新頻度に対するポリシーがありますか。またこれらが何に対しどのように強制実施されていますか。	SSH ユーザーの秘密鍵は保護されていなくてはなりません。

調査のための基本的な質問事項	ガイダンス
SSH の承認されたユーザーが、権限を与えられていない目的に、SSH でのアクセスを行おうとすることを防止するための制限が実施されていますか。	これは、SSH を使用した自動化プロセス、またインタラクティブなユーザーによるアクセスの双方に当てはまります。
SSH の公開鍵に何らかの制限は設定されていますか。	SSH が承認された目的のみに利用されるということを確実に実施するために、鍵の使用制限を使用することができます。
どのユーザーが SSH 公開鍵ファイルへの書き込みアクセス権を持っていますか。	これらのファイルへのアクセスは、ユーザーが自分の SSH 鍵を作成することを可能とし、バックドアを作ることになります。
SSH セッションにおいて SSH のログインや実行した操作を記録するための監視機能がしかるべき場所に設置されていますか。	システム及びアプリケーション管理者によって行われる特権操作は監視する必要があります。
SSH 鍵は集中ディレクトリ、あるいは NFS 等のファイル共用フォルダに保管されていますか。保管・転送される際に鍵はどのように保護されていますか。	秘密鍵は保管時・転送時ともに保護されていなくてはいけません。
本番環境及び非本番環境間で SSH の通信が行われないようにどのようなメカニズムもしくはコントロール等の保護対策がとられていますか。	アプリケーション開発者及びテスト実施者が使用した鍵はアプリケーション及び OS のイメージを本番環境に移行する前に確実に削除するように手順を再確認して下さい。
SSH サーバー・ソフトウェアの設定およびアップデートを管理・更新するために、どのような規定がありますか。	SSH ソフトウェアは承認された構成で設定しておき、不正設定を未然に防ぐためロックダウンする必要があります。

表 **1. Secure Shell** のガイダンス

これら基本情報を収集することで、監査担当者は詳細な PCI DSS 要件にわたるコンプライアンスを評価することができるようになります。

PCI DSS バージョン 3 に対応するための詳細な Secure Shell ガイド

監査担当者が、Secure Shell が CDE でどのように使用されているかに関する人、プロセス及び技術に関する基本情報を取得したら、次のステップは以下のとおりです。

1. CDE 内で Secure Shell の使用に関する PCI 要件を評価して下さい。
2. CDE が要件に適応しているかを確認して下さい。
3. 要件に適応しているか、いないかを確認後、文書化して下さい。

次の表では、CDE においてどのように SSH が使用され、展開されているかに関して監査担当者が調査すべき PCI DSS の具体的な項目に関する詳細なガイダンスを提供します。

要件 **1:** カード会員データを保護するために、ファイアウォールをインストールして構成を維持する	
PCI DSS 要件	**Secure Shell** ガイダンスとテスト手順
1.1.2 ワイヤレスネットワークを含む、カード会員データ環境とその他のネットワーク間のすべての接続、ネットワーク機器、システムコンポーネントを示す最新ネットワーク図。	許可された SSH のアクセス権限は図で明示する必要があります。更なる認証(例えば、パスワード)を必要とするアクセス又は必要としないアクセス(例えば、公開鍵認証、ケルベロス/AD の SSO は更なる認証を必要としなくてもいい場合があります)を区別する必要があります。鍵の見落としは頻繁に発生し、又クライアント利用者はこの存在を知らない場合が多いため、設定した承認済み鍵のスキャンを実際に行うことを推奨します。
1.1.3 システムとネットワーク内でのカード会員データのフローを示す最新図。	SSH の鍵は自動化されたデータ転送を実行する際によく使用されます。どのようにデータが転送されるかの流れを明示する必要があります。
1.1.4 各インターネット接続、および DMZ (demilitarized zone) と内部ネットワークゾーンとの間にファイアウォールを設置。	DMZ から内部のネットワークへの SSH アクセスは許可すべきではありません(どうしても許可する必要がある場合は、コマンド制限でコントロールする必要があります)。
1.1.6 使用が許可されているすべてのサービス、プロトコル、ポートの文書化、および使用が許可されている業務上の理由（安全でないとみなされているプロトコルに実装されているセキュリティ機能の文書化など）。安全でないサービス、プロトコル、ポートの例として、FTP、Telnet、POP3、IMAP、SNMP v1 および v2 などがある。	SSH は、FTP や Telnet 等のサービスをセキュアにするもしくは置き換えるプロトコルとして推薦されてます。しかし、SSH の設定及び承認済み鍵の管理が不十分な場合は、カード会員データを権限のないアクセスに露呈することになります。SSH の設定ファイル及び承認済みの鍵ファイルが適切に設定されていることを確認する必要があります。SSH はファイル転送、リモート・ログイン、アプリケーションのトンネリング等の暗号化チャネルを提供します。権限がない SSH の使用を防止するために例えば以下のような状況において、鍵の利用制限等のコントロールが正しく設定されている必要があります。 · 外部へのファイル転送 · SSH で VPN を行った内部/外部への通信
1.2 信頼できないネットワークとカード会員データ環境内のすべてのシステムコンポーネントの接続を制限するため、ファイアウォールとルーター設定を構築する。	SSH を利用した自動化アクセスは、正しく適切に設計したコントロールをバイパスすることができます。もし承認済み鍵で CDE の外部からコマンドラインを利用してのアクセスが行える場合、適切に設定されたファイアウォール及びルーターによるセキュリティーレベルが著しく落ちます。もし SSH で CDE とのアクセス(VPN 以外のリモート・ログイン)が可能な場合、意図した目的にのみ使用するように制限が正しく行われていることを確認して下さい。

要件 **2:** システムパスワードおよびその他のセキュリティパラメータにベンダ提供のデフォルト値を使用しない	
PCI DSS 要件	**Secure Shell** ガイダンスとテスト手順
2.2 すべてのシステムコンポーネントに、設定基準を作成する。この基準は、すべての既知のセキュリティ脆弱性をカバーし、また業界で認知されたシステム強化基準と一致している必要がある。業界で認知されたシステム強化基準のソースには以下がある(これらに限定されない)。 • www.nist.gov, www.sans.org, www.cisecurity.org, www.iso.org	Secure Shell の設定のベスト・プラクティスについては以下を参照して下さい。 http://datatracker.ietf.org/doc/draft-ylonen-sshkeybcp
2.2.3 安全でないとみなされているサービス、プロトコル、又はデーモンを使用する場合は、それらにセキュリティ機能を実装する。たとえば、SSH、SFTP、SSL、又は IPSec VPN などの安全な技術を使用して、 NetBIOS、ファイル共有、Telnet、FTP などの安全性の低いサービスを保護する。	安全ではないサービスを保護するか又は置き換えるために SSH の使用が推薦されていますが、SSH 自体もセキュアな方法で展開する必要があります。以下は SSH が適切に展開されているかどうかを確認する方法です。 • どのように Secure Shell のユーザー鍵を展開しているか。 • 管理者の職務変更あるいは退職時に鍵が削除されているか。 • 全ての管理操作がユーザーに紐付けられているか。 • 管理者が自身の鍵をインストールすることができるか。管理者あるいはユーザーが自身の SSH サーバーをインストールできるか。 • 鍵への制限が実装されているか。 • 秘密鍵がパスフレーズで保護されているか。 • 鍵が規則正しく更新されているか • 鍵強度は充分か。
2.5 ベンダデフォルト値およびその他のセキュリティパラメータの管理に関するセキュリティ・ポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。	承認済みの鍵は SSH サーバーにとって重要なセキュリティ・パラメーターです。これらを管理するために適切な手順が実施され、文書化(プロビジョニング、停止、更新等)されている必要があります。
2.6 共有ホスティング・プロバイダは、各事業体のホスト環境およびカード会員データを保護する必要がある。これらのプロバイダは、付録 A:「共有ホスティング・プロバイダの追加 PCI DSS 要件」に示されているように、特定の要件を満たす必要がある。	ホスティング・プロバイダが管理上のアクセス及び自動化プロセスでどのように SSH を使用しているかを再確認して下さい。多数の顧客システムにアクセスする場合 SSH のクレデンシャルは一意で、ホスティング・プロバイダが共用クレデンシャルを使用していないことを確認して下さい。

要件 **3:** カード会員データの保護	
PCI DSS 要件	**Secure Shell** ガイダンスとテスト手順
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。	SSH 鍵はカード会員データの暗号化に使用する暗号鍵に対するアクセス権も提供します。保存したカード会員データを誤用から防ぐため、すべてのシステムでの鍵の保管に関して制限を行う必要があります。最小限、誰が(どのプロセスもしくはシステムを含む)暗号鍵(SSH ユーザー認証に使用する鍵を含む)にアクセスするかを理解していなくてはなりません。
3.7 保存されているカード会員データを保護するためのセキュリティ・ポリシーと操作手順が文書化および使用されており、影響を受ける関係者全員に知られていることを確認する。	資料にはカード会員データへの自動化したアクセス手順(鍵ベース/ケルベロス SSO)を含む必要があります。なぜなら、誰がこのデータへアクセスすることができるかを正確に知っておく必要があるためです。

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	
PCI DSS 要件	**Secure Shell** ガイダンスとテスト手順
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 のホスト鍵は通信機器間の認証を行うため中間者攻撃に対してセキュリティを保てるように(例、信頼された CA のホスト証明書を使用する等)適切に管理しなくてはなりません。ユーザーの認証鍵に関しては、有効な信頼済み第三者に属するものとして認知されたアクセスに必要な承認済み鍵のみが認証で受入れられ、この鍵を利用して行うアクセスにはコマンド制限を行うべきです。
4.3 カード会員データの転送を暗号化するためのセキュリティ・ポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。	SSH でカード会員データを送信する場合、ホスト鍵や承認済み鍵の管理は文書化されている必要があります。

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	
PCI DSS 要件	**Secure Shell** ガイダンスとテスト手順
6.2 すべてのシステムコンポーネントとソフトウェアに、ベンダ提供のセキュリティパッチがインストールされ、既知の脆弱性から保護されている。重要なセキュリティパッチは、リリース後 1 カ月以内にインストールする。	SSH ソフトウェアがベンダあるいはオープン・ソースの推薦に従ってインストールされ更新されていることを確認して下さい。セキュアではない SSH は一切使用してはいけません。
6.3 内部および外部ソフトウェアアプリケーション（アプリケーションへの Web ベースの管理アクセスを含む）を次のようにセキュアに開発する。 • PCI DSS 要件に従って（安全な認証やロギングなど）。 • 業界基準やベストプラクティスに基づいて。 • ソフトウェア開発ライフサイクル全体に情報セキュリティを組み込む。	アプリケーション開発やテストプロセスで SSH が使用されている場合、SSH 展開のためのベスト・プラクティスが正しく適用されていることを確認して下さい。
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、ユーザー ID、パスワードを削除する。	開発やテストに使用した Secure Shell の認証用の鍵は、アプリケーションが本番環境に移行される前に削除しなければなりません。これらの鍵を削除、管理する手順を再確認して下さい。これらの鍵が両方の環境で利用できないように、システムとログをスキャンし確認して下さい。
6.4.1 開発/テスト環境を本番環境から分離し、分離を実施するためのアクセス制御を行う。	自動化されたアクセス（例えば、鍵ベースあるいはケルベロス SSO）は、開発/テスト環境と本番環境の間で許可されるべきではありません。多くの企業・組織が元来プロビジョニングを適切に制御していなかったため、承認済み鍵ファイルや ID 用鍵ファイルを利用したアクセスやログデータを入念に調査することが推奨されます。同じ鍵を開発/テスト環境と本番環境で使用しないで下さい。
6.4.2 開発/テスト環境と本番環境での責務の分離。	開発やテストに使用した Secure Shell の認証用の鍵は、アプリケーションが本番環境に移行される前に削除しなければなりません。開発/テスト環境から本番環境への自動化アクセスが許可されている場合、その分離に有効性はありません。従って、これは許可すべきではありません（適当なコマンド制限を行うことでコントロールが可能となる場合はあります）。
6.4.5 セキュリティパッチの適用とソフトウェアの変更に関する変更管理手順を変更する必要がある。	承認済み鍵の設定及び削除は、重要なセキュリティ及び操作に影響する可能性があるソフトウェアの変更となります。このような変更の適切な承認、取り消し、手順の文書化が必要です。

要件 **7:** カード会員データへのアクセスを、業務上必要な範囲内に制限する	
PCI DSS 要件	**Secure Shell** ガイダンスとテスト手順
7.1 システムコンポーネントとカード会員データへのアクセスを、業務上必要な人に限定する。	これは、どのようにそのアクセスが承認されるかに関わらず、誰がクレジット会員データにアクセス権を持っているかを知っていることを求めるものです。これには鍵及びケルベロス SSO アクセスを利用した SSHアクセスも含まれます。適切なアクセスのプロビジョニングとそれを解除する手順が、確実にアクセスをコントロールするために必要となります。
7.1.1 以下を含む、各役割のアクセスニーズを定義する • 各役割が職務上アクセスする必要のあるシステムコンポーネントとデータリソース。 • リソースへのアクセスに必要な特権レベル（ユーザー、管理者など）。	自動化アクセスで使用されるシェルレベルのアクセス(コマンドライン)は、広範なシステムリソースへのアクセスを提供しますが、これはマルウエアの拡散や手動での攻撃に悪用される可能性も持っています。コマンド制限の使用は各承認済み鍵(結果として一致する秘密鍵があるシステムや個人)に与える特権(アクセスのレベル)を制限するため、可能な場合は常に推薦されます。
7.1.2 特権ユーザー ID に与えるアクセス権を職務の実行に必要な最小限の特権に制限する。	SSH 鍵は特権ユーザー ID への自動化アクセスに頻繁に利用されます。このような場合、特に注意してコントロールする必要があります。このようなアクセスを許可した場合、コマンド制限でコントロールすることが重要です。
7.1.4 適切な権限を持つ関係者による文書化された変更承認を必要とする。	SSH の鍵ベースのアクセス(及びケルベロスを利用した自動化/SSO アクセス)の承認は文書化する必要があります。この文書は、設定・承認済みの鍵とその特権制限の自動監査で使用できるようなフォーム/メディア/システムであることが推薦されます。
7.3 カード会員データへのアクセスを制限するためのセキュリティ・ポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。	文書には SSH の鍵を利用したアクセス又はケルベロス SSO を制限するための手順を指定する必要があります。

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	
PCI DSS 要件	**Secure Shell** ガイダンスとテスト手順
8.1 次のように、すべてのシステムコンポーネントで、非消費者ユーザーと管理者のための適切なユーザー識別および認証の管理が行われるよう、ポリシーと手順を定義して実装する。 8.1.1 システムコンポーネント又はカード会員データへのアクセスを許可する前に、すべてのユーザーに一意の ID を割り当てる。 8.1.2 追加、削除、ユーザー ID の変更、資格情報、およびその他の識別オブジェクトを管理する。 8.1.3 契約終了したユーザーのアクセスを直ちに取り消す。	Secure Shell の要件: 管理者は、Secure Shell 経由でアカウントへアクセスする場合、共通のクレデンシャルを使用してはいません。 • 全ての SSH の承認済みの鍵の使用目的が文書化されていること。 • 従業員又は契約社員が退職する際に承認済みの鍵は削除されること。 • 利用者の役割が変わり、新しい職制ではそのアクセスを必要としない場合、承認済みの鍵が削除されること。 • 従業員又は契約社員は自分の鍵を追加できないこと。
8.1.4 少なくとも 90 日ごとに非アクティブなユーザーアカウントを削除/無効にする。	定期的に使用しないアカウントは、変更されても(例えばパスワードの変更等)気づかれない場合が多いため、攻撃の目標となりやすいです。従ってこれらアカウントは簡単に悪用されやすく、カード会員データへのアクセスに使用される場合があります。これはインタラクティブなユーザーアカウント及び自動化されたアクセスの双方に適用されます。詳細モードを有効にすることで、SSH の鍵の利用をログとして記録できます。ログにより SSH の鍵が最後に使用されたのがいつかを確認することができます。
8.2 一意の ID を割り当てることに加え、すべてのユーザーを認証するため、次の方法の少なくとも 1 つを使用することで、すべてのシステムコンポーネント上での非消費者ユーザーと管理者の適切なユーザー認証管理を確認する。 • ユーザーが知っていること（パスワードやパスフレーズなど） • トークンデバイスやスマートカードなど、ユーザーが所有しているもの • ユーザー自身を示すもの（生体認証など）	SSH のユーザー鍵は認証方法のうちのひとつです。ケルベロス認証はもう一つの認証方法です。所有者情報は、例えば 識別鍵又はケルベロスクレデンシャルを含む keytab ファイル等になります。
8.2.1 強力な暗号化を使用して、すべてのシステムコンポーネントで、送信と保存中に認証情報（パスワード/パスフレーズなど）をすべて読み取り不能とする。	保管されている SSH の秘密鍵は暗号化して保護する必要があります。ネットワーク・ファイル共用(NFS)を使用している場合、暗号化されていない秘密鍵ファイルがシステム起動時にネットワーク経由で送信されているかどうかを確認して下さい。
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 はリモートからのネットワーク・アクセス、特にリモートからのシステム管理に一般に使用されるアクセス方式です。SSH が本目的に対して使用されているかどうかを確認し、その場合認証セキュリティが要件を満たしているかどうかを確認して下さい。

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	
PCI DSS 要件	**Secure Shell** ガイダンスとテスト手順
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。 • 汎用ユーザー 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ー 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ー ID が使用されていない。	SSH 鍵は、各ユーザーアカウントに固有のものであるべきです。共用されている鍵は削除し各ユーザーに対し一意の鍵を提供して下さい。複数のアカウントの間で ID 用の鍵(秘密鍵)が共用されていないことを確認する必要があります。
8.5.1 サービスプロバイダへの追加要件：顧客環境へのアクセス権を持つサービスプロバイダは、各顧客に一意の認証情報（パスワード/パスフレーズなど）を使用する必要がある。	同じ秘密鍵が複数の顧客環境にアクセスできるように設定してはいけません。
8.6 その他の認証メカニズムの使用（たとえば、物理的セキュリティトークン、スマートカード、証明書など）は、これらのメカニズムの使用は、以下のように各アカウントに割り当てる必要がある。 • 認証メカニズムは、個々のアカウントに割り当てなければならず、複数アカウントで共有することはできない。 • 物理/論理制御により、意図されたアカウントのみがアクセスできるようにする必要がある。	SSH ユーザー鍵が認証メカニズムとして使われているかを確認し、セキュリティ・ポリシーが適切な使用を促すために正しいものであることを確認する。
8.7 カード会員データを含むデータベースへのすべてのアクセス（アプリケーション、管理者、およびその他のすべてのユーザーによるアクセスを含む）が以下のように制限されている。 • データベースへのユーザーアクセス、データベースのユーザクエリ、データベースに対するユーザアクションはすべて、プログラムによる方法によってのみ行われる。 • データベースへの直接アクセス又はクエリはデータベース管理者のみに制限される。 • データベース・アプリケーション用のアプリケーション ID を使用できるのはそのアプリケーションのみである（個々のユーザーやその他の非アプリケーション・プロセスは使用できない）。	SSH 経由でのデータベース・アプリケーションへのアクセスが有効になっているかどうかを確認して下さい。承認されていない発信元からの SSH 認証を受け付けないことがアクセス・コントロールで正しく行われていることを確認して下さい。コントロールのベストプラクティスには以下が含まれます。 • 発信元の制限 • コマンドの制限 • 鍵の更新 • 操作ログの取得
8.8 識別と認証に関するセキュリティ・ポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。	文書には、自動化されたアクセスをコントロールするための手順を含む必要があります。

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	
PCI DSS 要件	**Secure Shell** ガイダンスとテスト手順
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ーにリンクする監査証跡を確立する。 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。	「管理者」又は「ルート」等の大きな特権をもつアカウントはセキュリティもしくは運用に大きな影響を与える潜在的な力があります。Secure Shell アクセスにおけるシステムでの目的達成には以下が必要となります。 • 詳細モードを有効にする。 • ログの収集。 • 改ざん防止(例えば、ログ取得の停止等)のための構成の監視。 • 適切な手順なしでの新たな鍵の追加が行えないこと。
10.2.5 識別と認証メカニズムの使用および変更(新しいアカウントの作成、特権の上昇を含むがこれらに限定されない)、およびルート又は管理者権限を持つアカウントの変更、追加、削除のすべて。	承認済みの鍵ファイルへの全ての変更が(ファイルに変更を行うプロビジョニングシステムもしくはその他のシステムによって)記録されていなくてはいけません。承認済みの鍵又は SSH 設定に行われた権限がない変更が検出されなくてはなりません。
10.8 ネットワークリソースとカード会員データへのすべてのアクセスを監視するためのセキュリティ・ポリシーと操作手順が文書化され、使用されており、影響を受ける関係者全員に知られていることを確認する。	共有されている SSH 鍵及び承認済みのファイル、SSH 設定ファイルへの変更に関する手順が正しいことを確認する必要があります。

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	
PCI DSS 要件	**Secure Shell** ガイダンスとテスト手順
11.2.3 重要な変更があった後、内部と外部の脆弱性スキャンを必要に応じて繰り返す（要件 6.1 を参照）。スキャンは有資格者が実施する必要がある。	承認済み鍵の変更管理に関する文書を再確認する必要があります。承認済みの鍵及び ID 鍵が適切に管理されていないと考えられる理由があれば、これらのスキャンを行うべきです。スキャンの結果をもとに、確かに CDE の範囲が適切に定義され、その他の規則が適切に実行されていることを再確認する必要があります。
11.3 ペネトレーションテスト方法を開発し、実装する。 11.3.4 セグメンテーションを用いて CDE を他のネットワークから分離した場合、少なくとも年に一度とセグメンテーションの制御/方法が変更された後にペネトレーションテストを行って、セグメンテーション方法が運用可能で効果的であり、適用範囲内のシステムから適用範囲外のシステムをすべて分離することを確認する。	貫通試験の一環として、外部環境で見つけた ID 鍵を利用して、システムの侵入テストを CDE 内で実施することを推奨します。このようなテストにおいて、CDE 及び外部環境からの鍵スキャンの結果は鍵及びシステムのテストを行う対象を明らかにするよい方法となります。
11.4 侵入検知システムや侵入防止手法を使用して、ネットワークへの侵入を検知および/又は防止する。カード会員データ環境との境界およびカード会員データ環境内の重要なポイントを通過するすべてのトラフィックを監視し、侵害の疑いがある場合は担当者に警告する。すべての侵入検知および防止エンジン、ベースライン、シグネチャを最新状態に保つ。	SSH のアクセス・ログを監視し、SSHの鍵を使用した送信元システムから宛先システムへの承認されていないアクセスに対しセキュリティ・イベントを発行するように設定する必要があります。 IDS/IPS の機器の多くが暗号化トラフィックを解析できません。SSH、SCP、SFTP あるいは RDPが CDE の境界又は環境へのアクセスに利用される場合、これらトラフィックを調査する機能が正しく展開されているかどうかを確認して下さい。
11.5 変更検出メカニズム（ファイル整合性監視ツールなど）を導入して、重要なシステムファイル、設定ファイル、又はコンテンツファイルの不正な変更を担当者に警告し、重要なファイルの比較を少なくとも週に一度実行するようにソフトウェアを設定する。	SSH の承認済み鍵のファイル及び SSH の設定ファイルはセキュリティ上重要なシステム設定ファイルです。これらのファイルに行われた変更を追跡するために監視機能を展開する必要があります。変更管理は以下のような操作を担当者に正しく警告する必要があります。 • 新しい承認鍵の追加 • 鍵の利用に関する設定の変更 • ログ取得ポリシーの変更 • SSH サーバーの設定変更 • 新しい SSH サーバーの追加
11.6 セキュリティ監視とテストに関するセキュリティ・ポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。	変更管理及び SSH アクセスの監視手順が正しく行われていることを確認して下さい。

要件 **12:** すべての社員のための情報セキュリティポリシーを維持する	
PCI DSS 要件	**Secure Shell** ガイダンスとテスト手順
12.2 リスク評価プロセスを実施する。	リスク評価手順は、SSH 鍵の管理状態及び管理されていない鍵から生じる防御の損失(例えば、攻撃が災害対策システムもしくは代替システムへ広がった場合等)について詳細に検討を行う必要があります。
12.3 重要な技術に関する使用ポリシーを作成して、これらの技術の適切な使用を定義する。	SSH 鍵と設定の適切なポリシー管理を確実に実施する必要があります。
12.10.1 システム違反が発生した場合に実施されるインシデント対応計画を作成する。	Secure Shell がセキュリティインシデントにおける主要因となる場合があるかもしれないという理由から、インシデントの対応の目標に対し一貫した方法で SSH が展開され管理されるということを確認することが重要です。SSH の鍵を又はケルベロス SSO を利用した攻撃の広がりを限定していない場合、インシデント対応プランには災対サイトもしくは代替システムへの攻撃の可能性も考慮する必要があります。

要件 **A.1:** 共有ホスティング・プロバイダ向けの **PCI DSS** 追加要件	
PCI DSS 要件	**Secure Shell** ガイダンスとテスト手順
A.1.1 各事業体が、その事業体のカード会員データ環境のみにアクセスできるプロセスを実行するようにする。	異なる事業体の CDE 間でのSSH 鍵ベース及びケルベロス SSO ベースのアクセスを許可してはいけません。
A.1.2 各事業体のアクセスおよび特権が、その事業体のカード会員データ環境のみに制限されている。	ある事業体から他の事業体の CDE への自動化あるいはインタラクティブなアクセスは禁止する必要があります。

結論

Secure Shell は強力なツールです。Secure Shell はシステム、アプリケーション、データへの特権アクセスを提供します。Secure Shell が提供する広範な権限は、不適切な方法でのSecure Shell の展開が PCI DSS の多くの要件に違反するという結果をもたらすことになります。最終的に、監査担当者は CDE 内でどのように Secure Shell が使用されているのか、またどのように使用されているのか調査を行う必要があり、調査から発生する情報を元に必要なアクションを行う必要があります。

SSH コミュニケーションズ・セキュリティ社は、Secure Shell を使用する企業にセキュリティとコンプライアンスをもたらすホワイトペーパー、ツール、サービス、製品を提供しています。弊社が提供するリソースに関しては、**www.ssh.com** を参照して下さい。

参考文献

- **The Challenge of Identity and Access Management in Secure Shell Environments**（ホワイトペーパー）
- **Preventing Data Loss Through Privileged Access Channels**（ホワイトペーパー）
- **SSH Risk Assessor**（無償ツール）
- **Managing SSH Keys for Automated Access**（ホワイトペーパー）

販売代理店

株式会社 ディアイティ
http://www.dit.co.jp

〒135-0016 東京都江東区東陽 3-23-21 プレミア東陽町ビル

Tel. 03-5634-7651　Fax. 03-3699-7048