PCI DSS 3.0
最新バージョンアップのポイント

2014/2/7

国際マネジメントシステム認証機構株式会社
代表取締役副社長
上野 洋一

国際マネジメントシステム認証機構
International Certificate Authority of Management System

弊社紹介

- 会社名　国際マネジメントシステム認証機構株式会社
- 業務内容　情報セキュリティに関する第三者認証および審査／監査サービスのご提供
- 所在地　東京本社、札幌営業所
- 認定
  - 一般財団法人日本情報経済社会推進協会（JIPDEC）よりJIS Q 27001ISO/IEC27001）の認証機関として認定（ISR010）
  - 米国PCIセキュリティ基準審議会（PCI SSC）より認定セキュリティ評価機関（QSA）として承認

本日のアジェンダ

- PCI DSSVer3.0　前文のポイント
- PCI DSSVer3.0　要件の変更ポイント

本日のアジェンダ

- PCI DSSVer3.0　前文のポイント
- PCI DSSVer3.0　要件の変更ポイント

PCI DSS Ver3.0　目次（前文）

- 概論およびPCIデータセキュリティ基準の概要
- PCI DSS 適用性情報
- PCI DSSとPA-DSSとの関係
- PCI DSS要件の適用範囲
- PCI DSSを通常のプロセスに実装するベストプラクティス
- 代替コントロール
- 準拠に関するレポートの指示と内容

PCI DSS Ver3.0　目次（要件）

- PCI DSS要件およびセキュリティ評価手順の詳細
- 安全なネットワークの構築と維持
  要件1,要件2
- カード会員データの保護
  要件3,要件4
- 脆弱性管理プログラムの維持
  要件5,要件6
- 強力なアクセス制御手法の導入
  要件7,要件8,要件9

PCI DSS Ver3.0　目次（要件）

- ネットワークの定期的な監視およびテスト
  要件10,要件11
- 情報セキュリティポリシーの維持
  要件12
- 付録A：共有ホスティングプロバイダ向けの
  PCI DSS追加要件
- 付録B：代替コントロール
- 付録C：代替コントロールワークシート
- 付録D：ビジネス設備とシステムコンポーネントの
  セグメンテーションとサンプリング

PCI DSS Ver2.0からVer3.0の変更点

変更の種類

- 明確化(Clarification)
  要件の趣旨を明確化する。標準で簡潔な文で要件の目的とする要求が明確に示されていることを確実にすること。

- 追加のガイダンス(Additional guidance)
  特定のトピックにおいて、理解を深めるため、またはさらなる情報もしくはガイダンスを提供するための、説明、定義および/または指示。

- 発展型要件(Evolving Requirement)
  基準を新種の脅威や市場の変化に応じた最新の状態にするための変更。

PCI DSS Ver3.0　前文のポイント

- 概論およびPCIデータセキュリティ基準の概要（明確化）

  PCI DSSは、加盟店、プロセッサー、アクワイアラ、イシュア、サービスプロバイダのほか、カード会員データ（CHD：Card Holder Data）および、機密認証データ（SAD:Sensitive Authentication Data)を保存、処理、または送信するその他事業体などペイメントカードの処理を行うすべての事業体に適用すると明確にした。

- PCI DSS 適用性情報（明確化）

  承認前の機密認証データ（SAD:Sensitive Authentication Data)を保存する場合は保存自体が許可されるのか、どれだけの期間許可されるのか、関連した使用・保存要件について、アクワイアラやペイメントブランドに連絡し確認することが求められている。

PCI DSS Ver3.0　前文のポイント

- PCI DSS要件の適用範囲（追加のガイダンス）

システムコンポーネントの例が記載された
・セキュリティサービス（認証サーバなど）を提供する、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）、または CDE のセキュリティに影響を及ぼす（名前解決や Web リダイレクションなど）システム。
・仮想マシン、仮想スイッチ/ルーター、仮想機器、仮想アプリケーション/デスクトップ、ハイパーバイザなどの仮想コンポーネント。
・ファイアウォール、スイッチ、ルーター、ワイヤレスアクセスポイント、ネットワーク機器、その他のセキュリティ機器を含むが、これらに限定されないネットワークコンポーネント
・ Web,アプリケーション、データベース、認証、メール、プロキシ、ネットワークタイムプロトコル（NTP）、ドメインネームサーバ（DNS）などを含むが、これらに限定されないサーバタイプ
・内部および外部（インターネットなど）アプリケーションを含む、すべての市販およびカスタムアプリケーション
・ CDE 内にあるか CDE に接続されているその他のコンポーネントまたはデバイス

PCI DSS Ver3.0　前文のポイント

- PCI DSS要件の適用範囲2（追加のガイダンス）

サービスプロバイダ対象の明確化
・サービスプロバイダまたは加盟店に代わって、カード会員データの保存、処理、伝送を行うサードパーティ
・ルータ、ファイアウォール、データベース、物理セキュリティ、サーバのコンポーネント管理を行うサードパーティ

サービスプロバイダのPCI DSS評価範囲の明確化（要件12.9に関連）
・第三者サービスプロバイダが自らの PCI DSS 評価を行う場合、自社による PCI DSS 評価の範囲がその顧客に該当するサービスを含んでおり、関連する PCI DSS 要件が審査され、満たされていることが確認されたことを十分に実証する証拠を顧客に提供することが必要

PCI DSS Ver3.0　前文のポイント

- PCI DSSを通常のプロセスに実装する
  ベストプラクティス（追加のガイダンス）

PCI DSSを日常業務（BAU：Business-as-Usual）に組み込む
・セキュリティコントロールの監視
　ファイアウォール,IDS/IPS,ファイル整合性監視,アンチウイルス,アクセス制御の運用を確保する
・セキュリティコントロールの失敗の検出と対応を確実にする
・変更（新システムの追加、システムまたはネットワーク設定の変更）についてPCI DSS要件の変更が必要か確認を行う
　監査ログの設定、四半期毎の脆弱性確認　等々
・組織構造への変更（会社の合併や買収）があった場合は、PCI DSS範囲への影響をレビューする
・PCI DSS要件が引き続き満たされていることを確認するために、監査ログなど要件に関連する事項を継続してレビューする
・ハードウェア、ソフトウェアのテクノロジを年に一度レビューを行い、ベンダーサポートなどPCI DSS要件を満たしていることを確認する

本日のアジェンダ

■PCI DSSVer3.0　前文のポイント

■PCI DSSVer3.0　要件の変更ポイント

PCI DSS Ver3.0　要件のポイント

- 発展型要件として追加された要件
  - 要件1.1.2　最新のネットワーク図
  - 要件1.1.3　カード会員データのフローを示す最新図

⇒　ネットワーク図とデータフロー図を個別に確認する手順になった

PCI DSS Ver3.0　要件のポイント

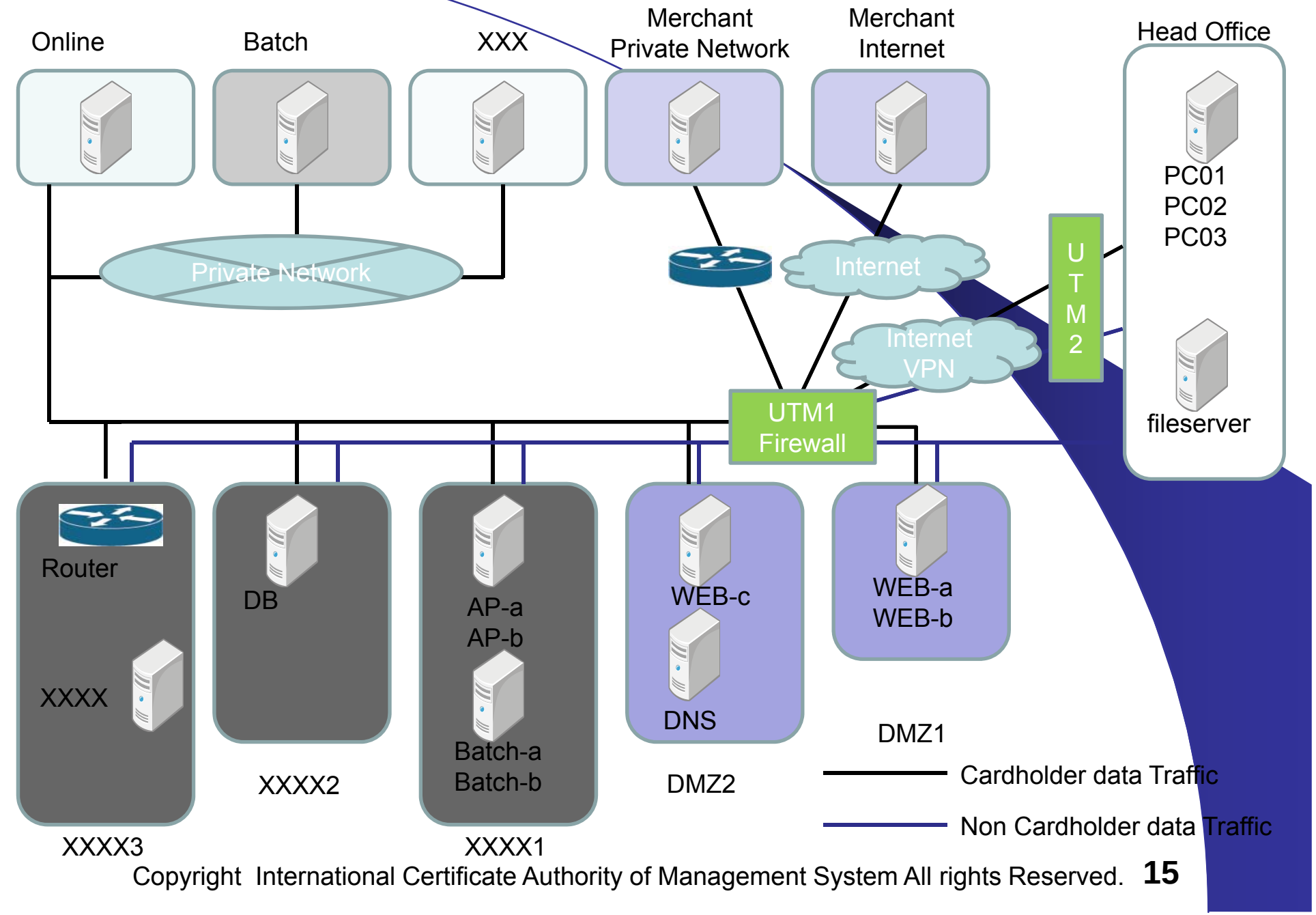
要求されているネットワーク図とは？

High-level Diagrams

The high-level diagram is intended to provide a bird‘s eye view of the assessed environment. This diagram should be designed to identify critical systems and reflect the infrastructure of the assessed networks from a high-level perspective.
The Reporting Instructions state: “Provide one or more simple, high-level diagram(s) showing the overall architecture of the environment being assessed. The diagrams should identify all locations and key systems, and the boundaries between them." (Assessor Newsletter June 2012)

⇒　PCI DSS範囲とその他のネットワーク等の接続を表した図

High Level Network Diagram (Traffic of Card holder Date)



PCI DSS Ver3.0　要件のポイント

要求されているネットワーク図とは？

Detailed Diagrams

According to the Reporting Instructions, the detailed diagram "should provide a more detailed view of the communication points within the environment..."

In this case, the detailed diagram should clearly depict the CDE including the boundaries between the CDE and other segments. Additionally, the security devices and other technical controls which have been implemented to protect the CDE should be identified. (Assessor Newsletter June 2012)

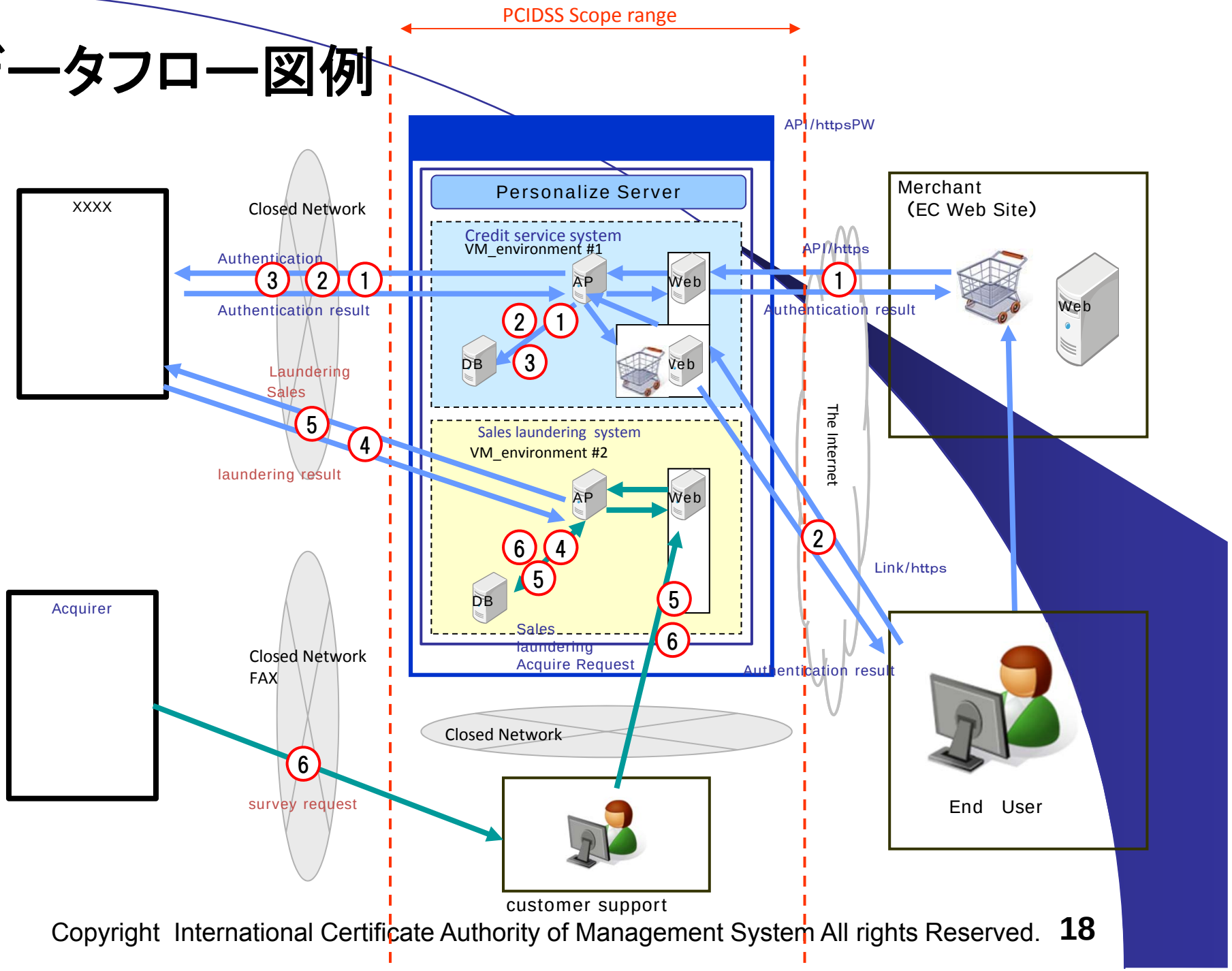
⇒　PCI DSS範囲を含む、組織の詳細ネットワーク図

PCI DSS Ver3.0　要件のポイント

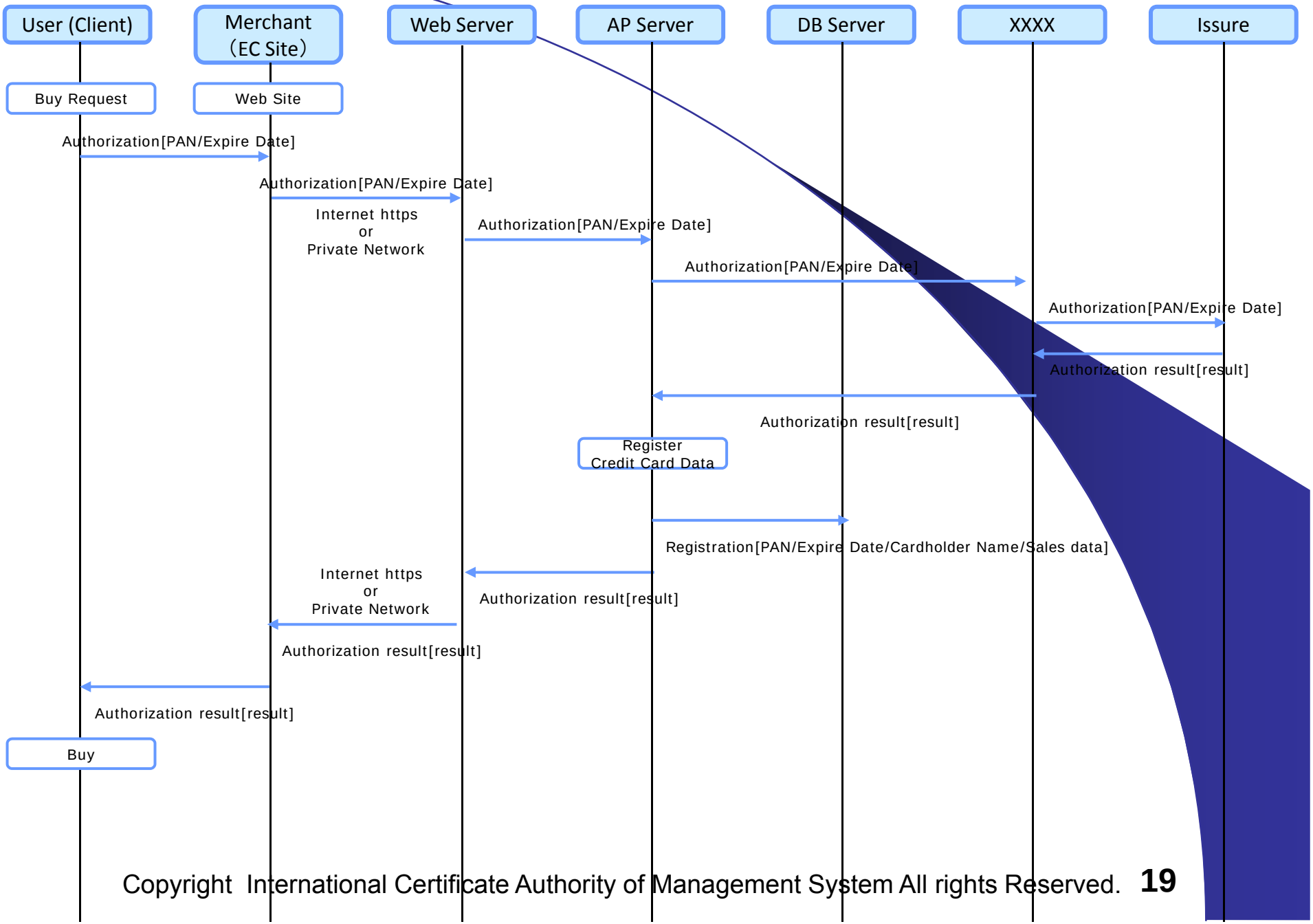
要求されているデータフロー図とは？

承認、キャプチャ、決済、チャージ バック、その他のフローを含め、カード会員の伝送処理についてのフロー図が要求されている

データフロー図例



① Internet or Private Network Authorization API Type



PCI DSS Ver3.0　要件のポイント

- 発展型要件として追加された要件
  – 要件2.4
  PCI DSS範囲にあるシステムコンポーネントの
  インベントリを維持する

⇒PCI DSS範囲のシステムコンポーネントの、ハードウェア(メーカー、タイプ等)、ソフトウェア(ペイメントアプリケーション、DB、OS等)の一覧表を作成する

PCI DSS Ver3.0　要件のポイント

- 発展型要件として追加された要件
  - 要件5.1.2
    一般的に悪意のあるソフトウェアに影響されないとみなされているシステムについても、定期的に評価を行い対象システムに対応しているウイルス等が発見されていないか確認を行う

⇒ AIX、Solaris、HP、ホスト等の安全なソフトウェアと言われているシステムを利用している場合でも、ウィルス等が発見されていないか定期的に確認を行う

PCI DSS Ver3.0　要件のポイント

- 発展型要件として追加された要件
  - 要件8.6
    その他の認証メカニズムが使用されている（たとえば物理的または論理的セキュリティトークン、スマートカード、証明書など）に関する使用手順

⇒　ID/パスワード以外の認証方法を認め、利用方法と手順の作成を行う

PCI DSS Ver3.0　要件のポイント

- 発展型要件として追加された要件
  - 要件9.3
    オンサイト要員の機密エリアへの物理アクセスを制御する

⇒　CDE環境に物理的にアクセス可能な、要員のアクセス権をレビューする

PCI DSS Ver3.0　要件のポイント

- 発展型要件として追加された要件
  - 要件11.1.1
    承認されているワイヤレスアクセスポイントの
    インベントリを維持する

⇒　既に認識されている、承認されたワイヤレスアクセス
ポイントをリスト化し維持する。
また、アクセスポイント設置が承認された理由の
文書化を行う

PCI DSS Ver3.0　要件のポイント

- 発展型要件として追加された要件
  - 要件12.4
    セキュリティポリシーと手順がすべての担当者に関する情報セキュリティ責任を明確に定義していることを確認する

⇒　責任について担当者へのヒアリングを行い確認する

PCI DSS Ver3.0　要件のポイント

- 発展型要件として追加された要件
  - 要件12.8.5
    各サービスプロバイダに対し、どのPCI DSS 要件がサービスプロバイダによって管理され、
    どのPCI DSS が事業体によって管理されるかについての情報を維持する

⇒　サービスプロバイダへ委託している業務が、PCI DSS要件に関連しているか、明確化し維持する

PCI DSS Ver3.0　要件のポイント

- 発展型要件として追加された要件
  - 要件8.2.3
  - 要件10.2.5
  - 要件10.2.6
  - 要件11.5.1
  - 要件12.2

⇒　要求に大きな変化なし

PCI DSS Ver3.0　要件のポイント

- 2015年6月30日までベストプラクティスの要件
  - 要件6.5.10
    不完全な認証管理とセッション管理

⇒　コーディング技法（手順）に不完全な認証管理とセッション管理に関する対処を含める

PCI DSS Ver3.0　要件のポイント

- 2015年6月30日までベストプラクティスの要件
  - 要件8.5.1

    顧客環境へのアクセス権を持つサービスプロバイダは、各顧客に一意な認証情報を使用する必要がある

⇒　サービスプロバイダは、顧客単位に別の認証情報(パスワード/パスフレーズ等)を利用しシステムへアクセスを行う

PCI DSS Ver3.0　要件のポイント

- 2015年6月30日までベストプラクティスの要件
  - 要件9.9(サービスプロバイダ用の追加要件)

    カードの物理的な読み取りによってペイメントカードデータを取り込む装置を改ざんや不正置換から保護する

⇒　POSやCAT端末などを物理的に保護する

PCI DSS Ver3.0　要件のポイント

- 2015年6月30日までベストプラクティスの要件
  - 要件11.3
    ペネトレーションテスト方法を開発し、実装する

⇒　組織で行うべき、ペネトレーションテスト方法を作成し、テストを実施する

PCI DSS Ver3.0　要件のポイント

- 2015年6月30日までベストプラクティスの要件
  - 要件11.3.4

    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

⇒　セグメンテーションが適切に行われているか

　　ペネトレーションテストで確認する

PCI DSS Ver3.0　要件のポイント

- セグメントテーションとは（PCI SSC曰く）

Segmentation = isolation（分離・隔離）= no access

Controlled access ≠ isolation

Controlled access is a DSS requirement and in scope

If it can impact the security of the CDE, it is in scope

Remember non-CHD systems may be in scope too.

⇒PCI DSS範囲に接続されるネットワークは全て
PCI DSS対象範囲

PCI DSS Ver3.0　要件のポイント

- PCI DSS　要件1.2曰く

  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、ファイアウォール構成
  を構築する

・信頼できないネットワークとは

レビュー対象の事業体に属するネットワーク外のネットワーク、
または事業体の制御または管理が及ばないネットワーク
（あるいはその両方）のことである

**⇒セグメントテーションと信頼できないネットワークを
組織として定義しておく必要がある**

PCI DSS Ver3.0　要件のポイント

- 2015年6月30日までベストプラクティスの要件
  - 要件12.9(サービスプロバイダ用の追加要件)

    顧客に代わって所有、保存、処理、送信する
    カード会員データのセキュリティについて、
    または顧客のカード会員データのセキュリティ
    に影響を与える範囲について責任を持つことを
    認める内容の書面による契約書を維持する。

⇒　サービスプロバイダは、委託業務内がPCI DSS要件を明確にし契約を行う必要がある

※同意の正確な言葉づかいに、この要件で提供されているのと同じものを含める必要はありません

PCI DSS Ver3.0　要件のポイント

- その他注意点

  各要件の最後に下記要件が追加された

  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

⇒　**文書化され使用されていること、また 影響を受ける関係者全員に知られていることを確実にする**

ご清聴ありがとうございました

PCI DSS に関連するご質問等がございましたら
下記までお気軽にご連絡ください。

- 業務管理グループ
  Mail ： gyoumu@icms.co.jp
  Tel ： 0120-796-115

