PCI SSCの活動内容とJCBの取り組み

2014年2月7日

株式会社ジェーシービー
ブランド事業統括部
井上 憲司

JCB 株式会社ジェーシービー

目次

1. カード犯罪の歴史と最新の動向

カード犯罪の動向

- 国際的な組織犯罪。
- 特定国・地域での偽造悪用、EC、ATM不正取引。
  - ー国内不正、クロスボーダー不正が併存。
  - ー全世界的には米国での発生が顕著。
  - ー欧州はIC化などにより減少傾向。
  - ーアジア太平洋地域は、オーストラリア、日本、タイなどが多発国。東南アジアはIC化により低水準。
- 加盟店、プロセッサなどからのデータ漏洩。
- クレジットマスターによるカード番号算出。

カード犯罪の構成要素

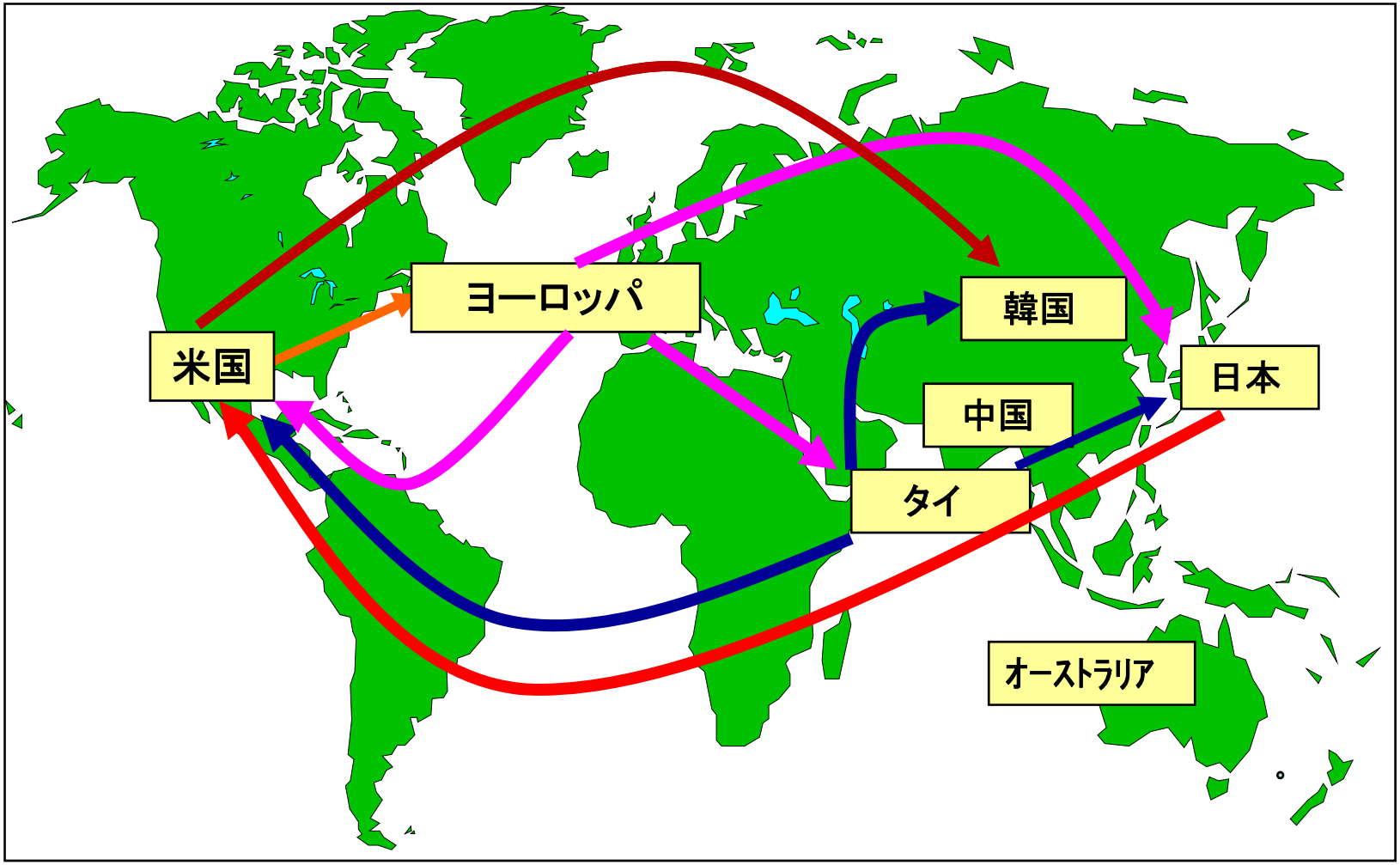
1. 利用可能なカードデータ（データ窃取）
2. プラスチック原板（原板偽造、密輸）
3. 製造・加工（エンボス・エンコードなどの二次加工）
4. 偽造カードや窃取したカードデータの行使
   - 国内・海外加盟店での不正利用
   - 少額取引でのカード番号の有効性チェック
   - 非対面環境でのカード番号のみの行使

アジア・太平洋地域のカード犯罪発生地域の推移

■ 1990年代以降のカード犯罪多発国、地域は以下の通り推移。

- 香港　　：1990
- マレーシア　　：1992 ～ 2005（香港からシフト）
- 日本　　：1995 ～
- オーストラリア　：1999 ～（マレーシアからシフト）
- 台湾　　：1999 ～ 2003（日本からシフト）
- 韓国　　：2000 ～ 2005
- タイ　　：2002 ～（マレーシアからシフト）
- 中国　　：2003 ～
- その他（ベトナム、インドなど）

データ流出地域と不正取引発生地域の傾向



データ窃取の手口の推移

- ハンディスキマー（ホテル、飲食店など）
- 端末内蔵型スキマー
- 非加盟店でのスキミング
- ワイヤータッピング（東南アジアの一部の地域）
- 大量のデータ漏洩（EC加盟店など）

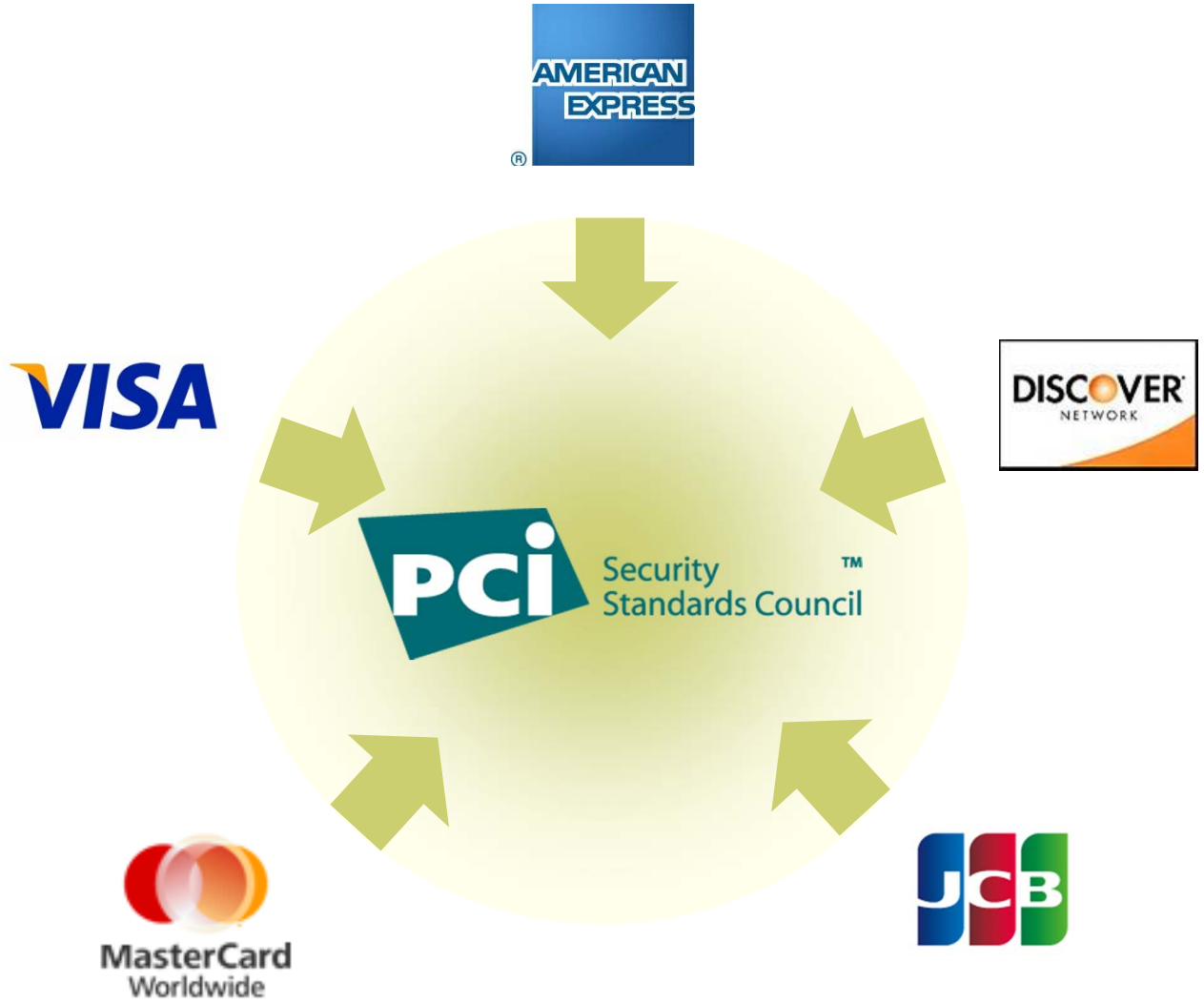
PCIDSSの策定と国際ブランドルール

- ・PCI SSCが策定したPCI DSS基準を策定。
- ・各国際ブランドがPCI DSS推進プログラムを策定。

推進施策	**JCB** JCB Data Security Program (JDSP)	**VISA** Account Information Security (AIS)	**MasterCard** Site Data Protection (SDP)	**American Express** Data Security Operating Policy (DSOP)
基準	**PCI DSS** (**PCI SSC**が策定)			

2. PCI SSCの概要

PCISSCの設立経緯



PCISSCについて

【概要】
・2006年に米国にて設立。
・PCI基準の開発、管理、トレーニング、認知向上努力を担う。

【主なステークホルダー】
・PO（Participating Organization＝参加団体）
・BOA（Board of Advisors）
・QSA（Qualified Security Assessors＝訪問審査機関）
・ASV（Approved Scanning Vendors＝脆弱性診断機関）
・PFI（PCI Forensic Investigators＝フォレンジック調査機関）

PCI DSS（データセキュリティ基準）

安全なネットワークの構築と維持

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こと

要件 2: システムパスワードおよび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こと

カード会員データの保護

要件 3: 保存されたカード会員データを保護すること

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伝送する場合、暗号化すること

脆弱性管理プログラムの整備

要件 5: アンチウィルスソフトウェアまたはプログラムを使用し、定期的に更新すること

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、保守すること

強固なアクセス制御手法の導入

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こと

要件 8: コンピュータにアクセスできる各ユーザに一意の ID を割り当てる。

要件 9: カード会員データへの物理アクセスを制限する。

ネットワークの定期的な監視およびテスト

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。

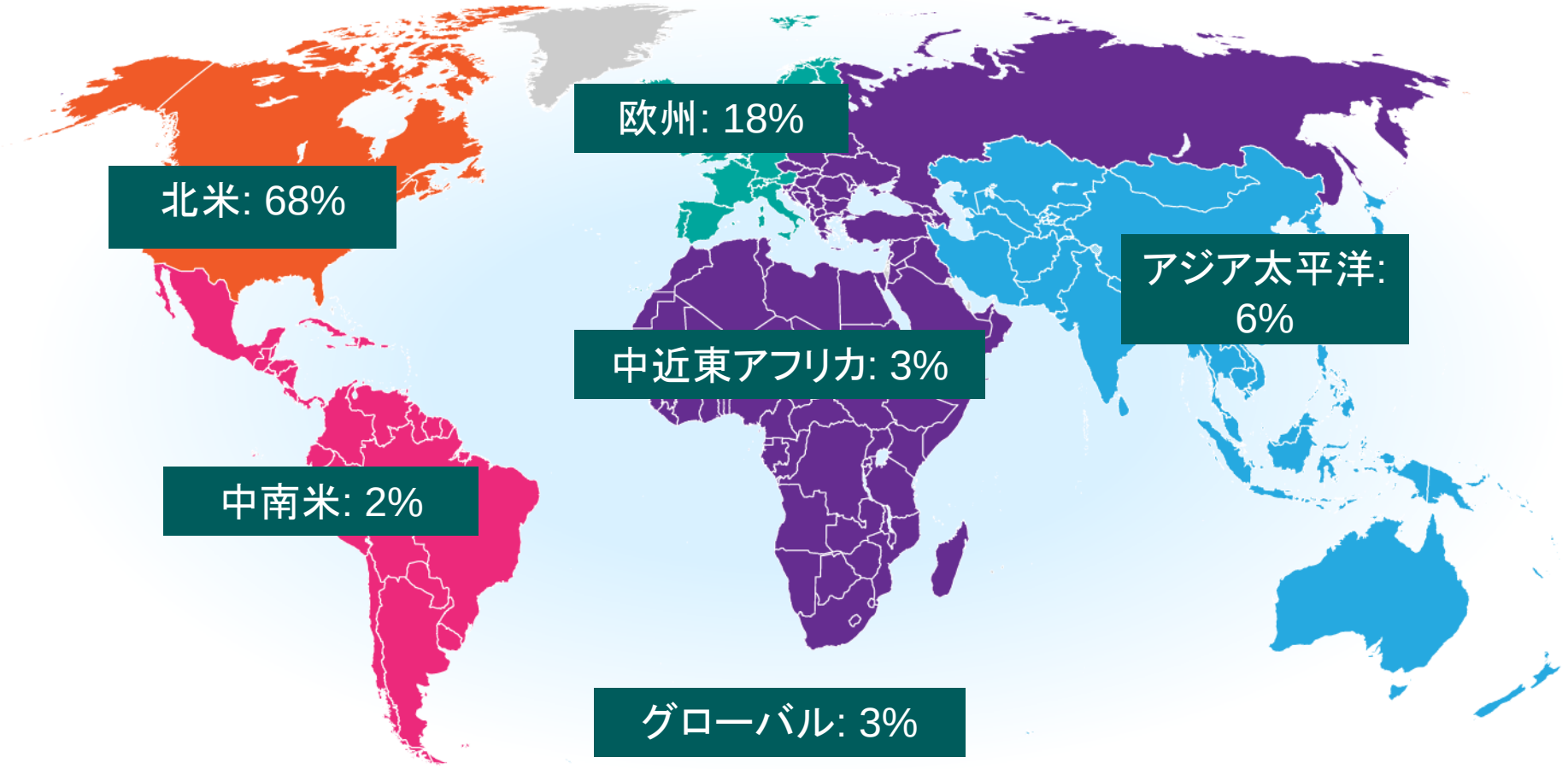
要件 11: セキュリティシステムおよびプロセスを定期的にテストする。

情報セキュリティポリシーの整備

要件 12: 従業員および派遣社員向けの情報セキュリティポリシーを整備する。

PCI SSCのグローバル展開

PCISSC参加企業（PO）の分布



PCISSCの活動原則

PCI SSCの活動範囲

- 各種セキュリティ基準、技術要件の管理、改良。
- PCISSCが認定している審査機関およびその品質の管理。（QSA、ASV、PFIなど）
- PCI基準の認知度向上に関する活動。（広報活動など）

PCI SSCの活動範囲外

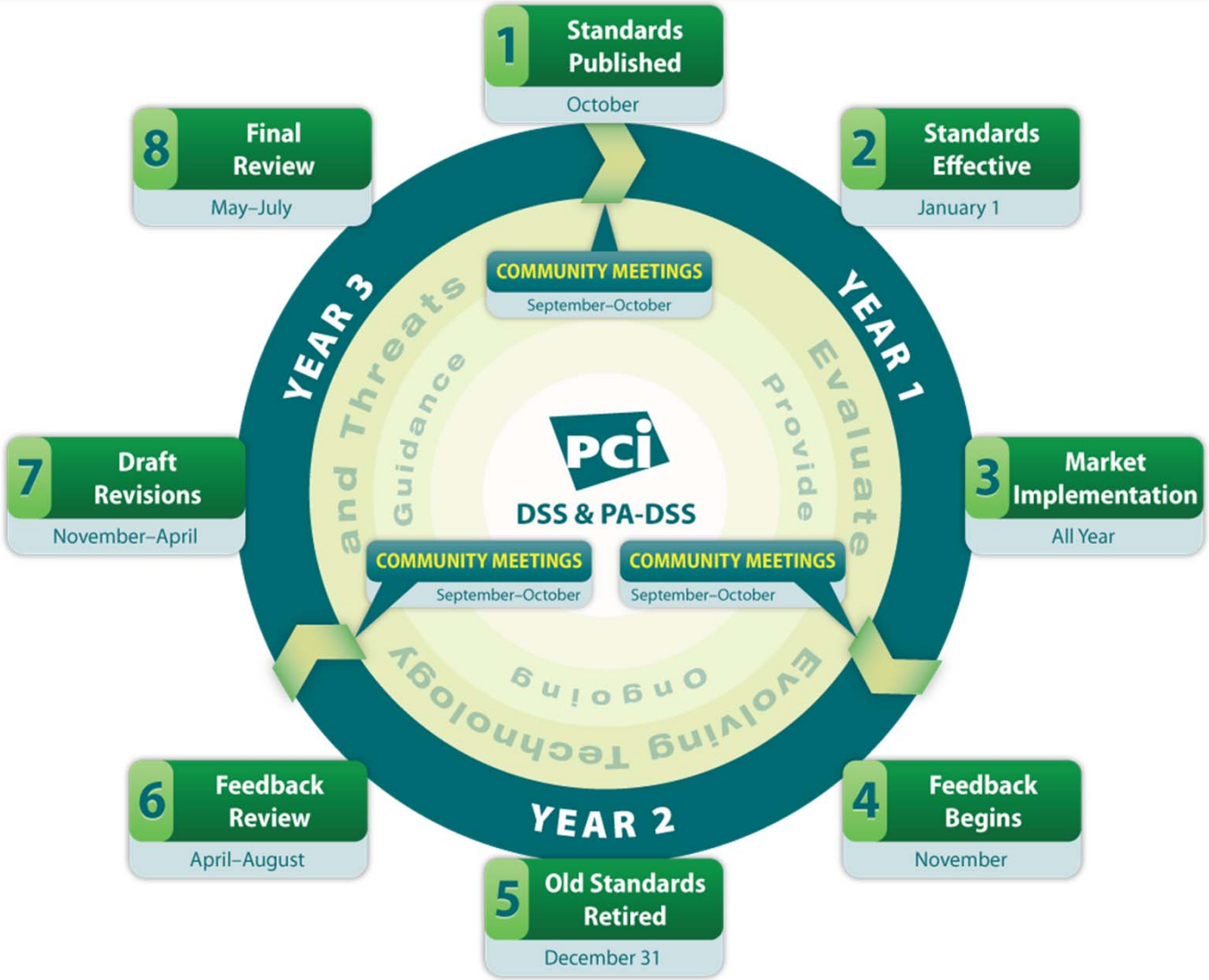
- 国際ブランドが、遵守期限、対象者、レベル分類、ペナルティなどを定める。
- PCI基準準拠に関する各国での推進活動。

PCISSCの体制

PCISSCの主なCommitteeは以下の通り。

- Executive Committee
- Operations Committee
- Standards Committee
- Marketing Committee
- Working Groups
- Task Forces
- Special Interest Groups (SIG)

PCI DSS and PA-DSSのライフサイクル（3年）



PCIDSS Version 3.0について

- 2011年以来の改訂
- 250以上のフィードバック、大半が米国外から
- 大幅な変更はなく、改訂ポイントは以下３点

  ①『準拠範囲＝スコーピングの明確化』

  ②『委託先の準拠範囲の合意、明文化』

  ③『ユーザー内のEducation強化』
- 2013年11月に正式リリース（日本語版は12月リリース）
- 2014年1月1日より発効
- Version 2.0の失効日は2014年12月31日

その他のセキュリティ基準

①PTS Version 4.0

②Card Production Security Requirements

③ATM Security Guideline

④P2PE

⑤Tokenization

⑥Mobile Payment Acceptance

Asia/Pacific Community Meeting概要

- 米国、欧州に次ぐ第3のターゲット地域として2013年より開始。（2013/11にマレーシアのクアラルンプールで開催）
- Stakeholder以外の参加者にもオープン。
- 7回目のアメリカ、欧州よりベーシックな内容をカバー。
- PCI Standards動向、3.0解説、フォレンジックレポートなどバランスよく設定。
- 今後、2days sessionへの移行を検討。
- 他地域と比べて安価な参加フィー設定。
- アジア地域の参加者とのネットワーキング。
- 2014年11月に第2回ミーティング開催。
（オーストラリア・シドニー）

アジア太平洋地域の展開

- グローバル展開の中でのアメリカ、欧州に次ぐ第3の市場（中近東、中南米地域においても普及活動強化中）
- オーストラリア、シンガポールでの普及活動の実績
- 普及活動は、東南アジア、東アジア、オセアニアの3つに区分される
- 多言語対応について
- PO、Board of AdvisorなどStakeholderを募集
- PCISSCから見た日本市場でのPCIDSS進捗状況

サマリー

PCI SSCの活動：

- 「形式的なコンプライアンス」ではなく「セキュリティ強化」を目指す。
- PCIDSSをはじめとするセキュリティ基準、およびその他の付随ドキュメントを整備。
- 各ステークホルダーの意見を集約したセキュリティ基準を策定。
- 適用範囲の軽減など、PCI基準への効率的な準拠手法の検討。
- 日本を含む主要国に対して、グローバルな展開。

3. JCBの取り組みについて

PCIDSSに関するJCBの取り組みについて

- 国際ブランド、イシュア、アクワイアラとして、カード犯罪の動向に応じて、日本、海外にて対応。不正対策の中の重要な柱の一つとして取り組み。
- PCIDSSは、JDSP(JCBデータセキュリティ制度)を推進、展開。
- タスクフォース、各WGなど業界活動への参加。
- PCISSCのメンバーとしての活動への参加。
- PCISSC本部と日本のステークホルダーとの相互理解、協業などの促進、調整。

4. まとめ

まとめ

- PCIDSSの米国における普及により、データ流出事案が欧州、アジア太平洋地域にシフト。一方、米国も大規模店、中小店 を含めて再度ターゲット国に。

- 日本は、アジア太平洋地域においては、PCIDSS推進が決して遅れているわけではないが、発生リスク、インパクトなどを考えると、さらなる取り組みが必要である。

- PCIDSSは、グローバルレベルでデータ流出を抑止、制御するためには合理的、有効な基準である。また派生的に各種基準、ガイドラインなどのラインアップが増加。

まとめ

- 各国のビジネス環境、コストなどとの兼ね合いなどから、対象領域の極小化など様々な方策のさらなる検討が必要である。

- PCISSCでは、グローバルな視点で各施策を協議、検討しているが、グローバル展開においては、SSCと各国のステークホルダーとの相互理解を促進し、各ステークホルダーの意見や努力を調和させていく。

株式会社ジェーシービー

ブランド事業統括部

井上 憲司