

# Visaのセキュリティへの 取り組み

**井原 亮二**

ビザ・ワールドワイド  
リスクマネジメント



**VISA**

The Visa logo is centered in the middle-right section of the slide. To its right and above it are several overlapping rectangular blocks in shades of blue and yellow, creating a modern, abstract geometric design.

# 将来予測に関する記述および免責条項

本プレゼンテーションには、1995年私的証券訴訟改革法(the Private Securities Litigation Reform Act of 1995)に定義された意味における将来予測に関する記述が含まれています。将来予測に関する記述は、通常、「目的」、「目標」、「戦略」、「機会」、「継続する」、「可能である」、「であろう」などの用語や、その他の類似した表現を含むことから特定されます。このような将来に関する記述の例としては、会社の戦略と製品の目標、計画、目的についてなどが挙げられますが、それらに限定されるわけではありません。将来予測に関する記述は、その性質上、(i)その記述がなされた時点のことを述べるもので、(ii)歴史的事実を記述したり将来のパフォーマンスを保障するものではなく、(iii)予見または数値化することが困難なリスク、不確実性、及び想定(仮定)、状況の変化の影響下におかれます。したがって、実際の結果が、将来予測に関する記述に比して実質的におよび不利な方向に異なってしまう可能性があり、そのような差をもたらす様々な要因には、新たな法律、規制および市場障壁の影響；インターチェンジ払い戻し手数料、独占禁止、租税等の訴訟や政府による施行の進展；新たな訴訟、調査もしくは訴訟手続き、または係争中の訴訟、調査もしくは訴訟手続きに関連した当社の潜在的リスクの変化；経済的要因；競合他社からの圧力、急速な技術的發展、当社のペイメントネットワークからの金融機関離れ等の業界の進展；システム開発；Visaヨーロッパがその権利を行使してその発行済み株式のすべてを当社が取得するよう要求した場合のコストの発生；組織としての有効性または主要従業員の喪失；買収の不成功、または新たな商品やビジネスを効果的に開発できないこと；自然災害；テロリストによる攻撃、軍事紛争または政治紛争、ならびに公衆衛生における緊急事態；弊社最新の10-K様式年次報告書および弊社最新の10-Q様式四半期報告書の「リスク要因」の項目で検討されているその他の要因、などが含まれます。このような記述には、過剰に依存すべきではありません。

研究、調査結果、リサーチ、推奨、および機会の評価は、情報提供のみを目的とするものであって、マーケティング、法律、規制その他に関するアドバイスとして、これに依拠すべきではありません。推奨や機会については、貴社独自の事業上のニーズおよび適用法や規則に照らして、独立に評価すべきです。Visaは、貴社による、研究、調査結果、リサーチ、推奨、機会の評価、およびそれらのいかなる性質のエラーも含めた使用、又は、その使用を通じて貴社が導き出すかもしれない想定(仮定)もしくは結論についての責任を何ら負いません。統計的有意差が特に記されていないならば、調査結果は方向を示すだけのものとみなされるべきです。

# キャッシュアウト事件 2013年2月20日



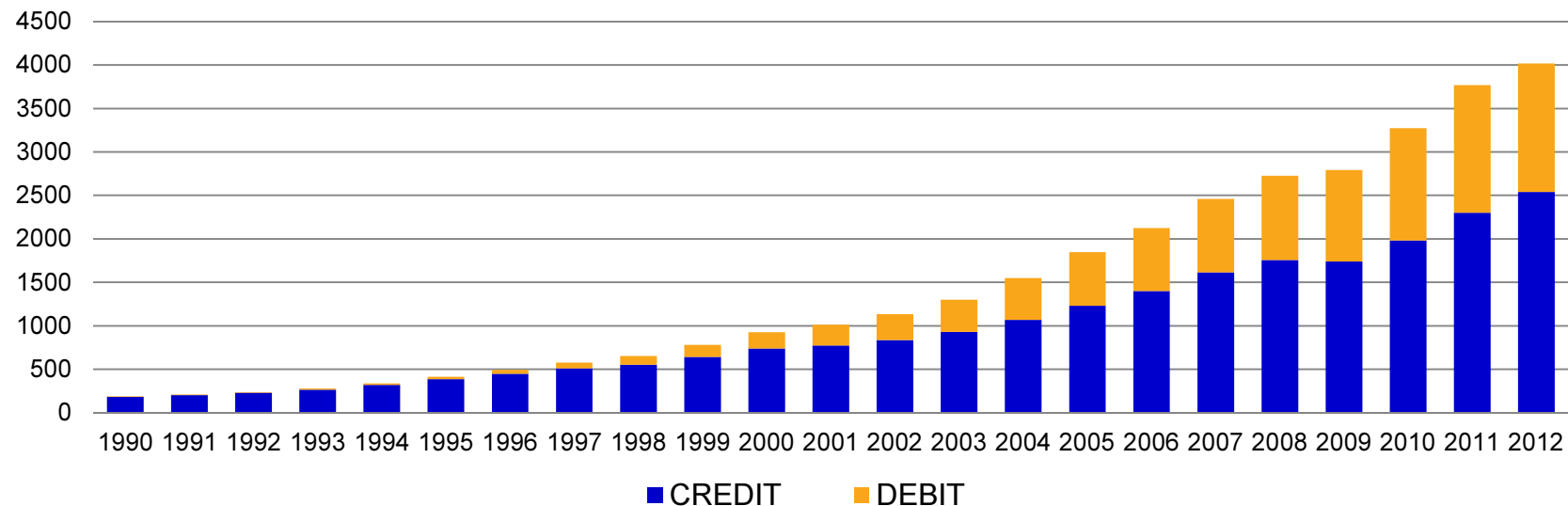
40,500取引、27カ国、\$45百万ドルの損失



# 電子決済のグローバルな成長

2012年12月末時点までの一年間で、ショッピング取扱高は**4.0兆米ドル**。  
その内訳は、**2.5兆米ドル**がクレジットプロダクツ、**1.5兆米ドル**がデビットプロダクツによる。

## Visa Inc. Payments Volume (\$ millions)



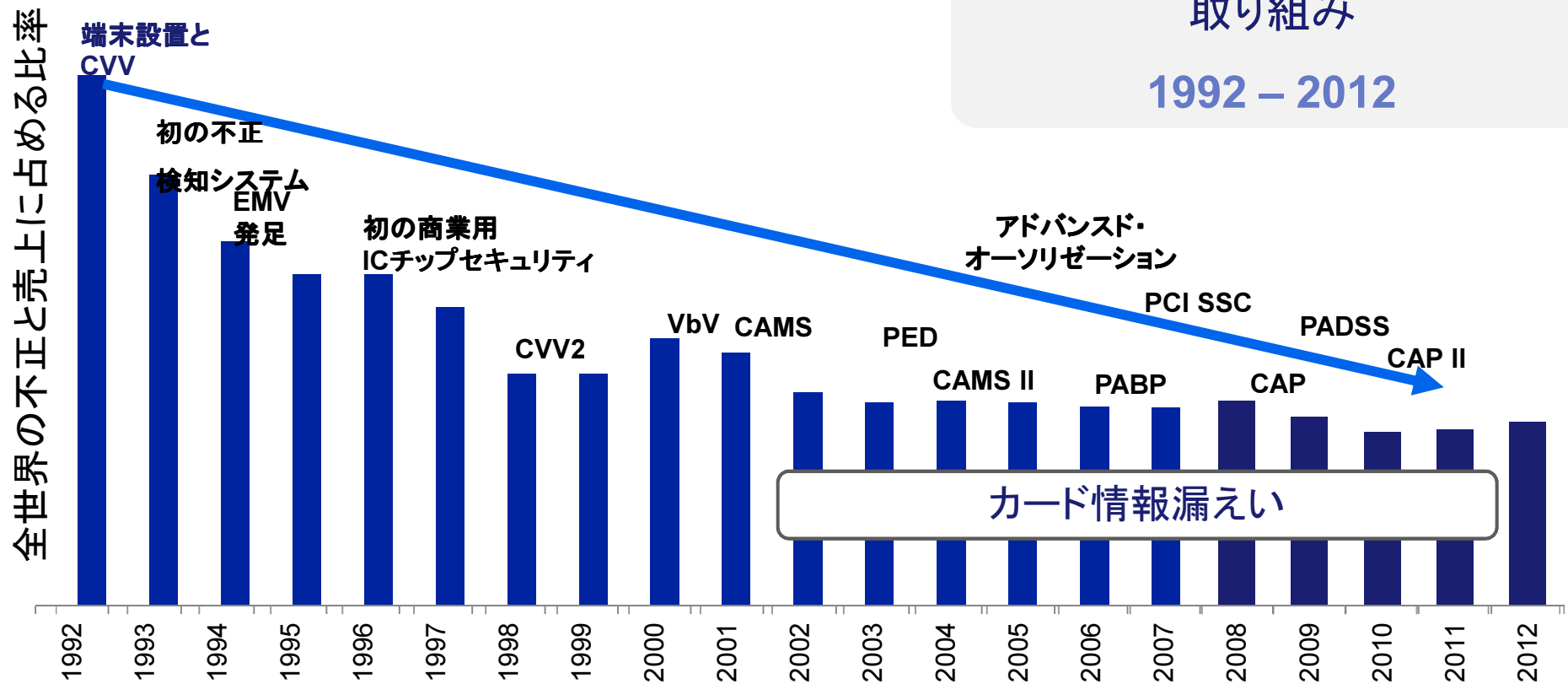
Notes: Credit includes consumer and commercial. Debit includes consumer, commercial, prepaid and online.

Source: Visa Operating Certificates

# Visaのセキュリティ対策

不正とデータセキュリティ  
におけるVisaの革新的な  
取り組み

1992 – 2012

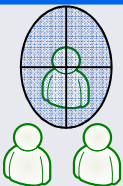

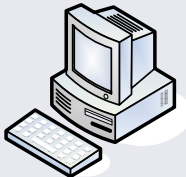


Source: Visa TC40 Fraud Reporting

# カード情報流出事件 手口の傾向

犯罪手口はより高度化している



	従来	新しい傾向	ハイライト
<b>標的</b> 	カード会員, 小規模加盟店, メガストア	EC加盟店/ プロセッサー	少ないが大規模な情報流出事案が甚大な影響
<b>犯罪者</b> 	個人, グループ, 組織犯罪	国際的な連携	洗練され資金の潤沢な国際的なシンジケートが連携
<b>不正種別</b> 	盗難紛失, スキミング, データ盗難	国境を越えたデータ盗難	革新的な手口の一つ 古典的・単純な手口も横行(SQL injections)

# カード情報流出事故 加盟店の影響

- カード情報流出を漏洩させた加盟店は原因調査と対応が完了するまでカードの取扱い停止せざるを得なくなる。
- 多くの加盟店はアクワイアラより事前にカードデータセキュリティに関しての注意予告を受けていなかったと述べている。事故は発生したときに全責任を負わされるのは納得できないとコメントされている。
- カード情報流出事故を経験した加盟店の多くは、以後カード情報を保管せず、PCI DSS準拠しているサービスプロバイダーに保管を委託している。

# カード情報流出に関わる損害補償制度

- 一定規模以上のカード情報(磁気)流出事故が発生した場合、それに起因するイシューの偽造不正被害について一定の範囲内でアクワイアラに補償を求める。
- ただし、事故発生時にPCI DSSに準拠している場合、その補償義務は免責される。

## 2014年10月より強化

- プロセッサー・サービスプロバイダーなどのカード情報流出事故の場合、当該事案のためにイシューがカード再発行を行った場合、その費用(一定額)も補償対象とする。ただし、事故発生時にPCI DSSに準拠している場合、その補償義務は免責される。

一定規模以上のPOSのEMV化が完了している加盟店については前記の補償義務が免責される



# VisaのPCI DSSサイト

<http://www.visa.co.jp/ap/jp/merchants/riskmanagement/accountsecurity>

なぜVisa? 決済の仕組み Visaカードの取扱を始めるにあたって **リスク管理** VISA認証サービス

**アカウント情報セキュリティ** エージェント



## アカウント情報セキュリティ(AIS)プログラム

アカウント情報セキュリティ(AIS)は、機密情報として扱われるべきカード情報や取引情報をVisaの決済システムにおいて保護するために設計されたリスク管理プログラムです。カード発行会社(イシュア)、クレジットカードの加盟店獲得と管理業務を行う加盟店契約会社(アクワイアラ)、加盟店、カード会員など、決済に関わるすべての当事者の利益を、対面取引と非対面取引の両方で守ります。

Visaおよびその他の決済カードブランド会社の協力により、業界共通のセキュリティ要件を設定する目的で、AISプログラムは「ペイメントカード業界データセキュリティ基準(Payment Card Industry Data Security Standards、以下「PCI DSS」)として知られる、業界共通基準を採用しています。ペイメントカード業界セキュリティ基準協議会(Payment Card Industry Security Standards Council、以下「PCI SSC」と言いますが)がPCI DSSとすべての関連書類を所有、整備、配布しています。

加盟店やプロセッサ、決済を代行するサービスプロバイダなど、Visaの決済システムを利用してVisaのカード情報や取引情報を保管、処理、送信しているすべての企業に、AISの遵守が義務付けられています。

### AISプログラムの利点とは？

PCI DSSを導入し遵守することは、顧客情報をセキュリティ侵害や詐欺の危険から効果的に保護するための重要な第一歩と言えます。

適切な情報の安全対策は、貴社のお客様を守るだけでなく、ビジネスリスクを減らし、カード会員情報の流出による損失や処理コストを最小限に抑えます。

AISプログラムの利点としては、下記のようなものが挙げられます。

- ・ 貴社ブランドの品位を向上させ、消費者の信頼度を高めます。
- ・ 消費者の信頼が高まることで、売上や取引が増加します。
- ・ セキュリティ侵害や、それに伴う調査や訴訟などに掛かる不要な費用の発生を防ぎます。
- ・ 情報漏洩や詐欺に伴う、ネガティブな報道の対象となるリスクを削減します。
- ・ 安全対策や予防措置についての理解が深まります。



加盟店様向け情報

[詳しくはこちら](#)



サービスプロバイダ様向け情報

[詳しくはこちら](#)

# PCI DSS

## ジャパン フレームワーク



# 加盟店用PCI DSS遵守基準

バリデーション	LEVEL-1	LEVEL-2	LEVEL-3	LEVEL-4
取引件数	年間6百万件以上	年間1-6百万件	年間2万件-百万件のインターネット加盟店	その他
自己問診	任意	必須	必須	推奨
脆弱性スキャンテスト	必須	必須	必須	推奨
審査機関による訪問 審査	必須	任意	任意	任意

# PCI DSS ジャパン フレームワーク

## 非対面

カテゴリー	タイムフレーム	要件
サービス プロバイダー	<b>2013年3月</b>	PCIDSS 準拠 (QSAオンサイトレビュー)
LEVEL-1 / 2加盟店		PCIDSS 準拠 (QSAオンサイトレビュー) またはカード情報非保持
その他EC加盟店		センシティブ情報非保持、SAQ および脆弱性スキャンテスト

## 対面

カテゴリー	タイムフレーム	要件
LEVEL - 1 / 2 加盟店	<b>2013年3月</b>	センシティブ情報非保持
	<b>2018年3月</b>	LEVEL-1, PCIDSS 準拠 (QSAオンサイトレビュー) またはカード情報非保持 LEVEL-2, SAQ および脆弱性スキャンテストSAQ / Scanning testsまたはカード情報非保持
対面加盟店 (年間 100万件未満)	<b>2013年3月</b>	センシティブ情報非保持、SAQ および脆弱性スキャンテスト
	<b>未定義</b>	カード情報非保持
その他	<b>2018年3月</b>	EMV 端末設置によりセキュリティ強化をはかる

# お客様のカード情報の保護は 関係者全員

(国際ブランド・カード会社・加盟店・サービスプロバイダー・ベンダー)  
の責任です

ありがとうございました

**VISA**