PCI DSSなんか怖くない
～良いQSAパートナーの見つけ方～

上野　洋一
QSA、 ISMS主任審査員
国際マネジメントシステム認証機構株式会社　代表取締役社長

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

Copyright International Certificate Authority of Management System All rights Reserved.

国際マネジメントシステム認証機構について

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

略称：ICMS（International Certificate authority of Management System Co., Ltd.）

1999年設立。
2003年ISMS-AC（旧JIPDEC）から認定を受けたISO27001/JISQ27001審査認証機関としてISMS審査事業、2008年PCI SSCの認定セキュリティ評価機関（QSAC）としてPCI DSS監査事業を始めました。PCI DSS監査の実績は国内最多クラスとなります。P2PEについては2016年に認定取得し、2018年国内初であるP2PE準拠の実績を挙げました。

ISMS、PCIともに規格の制定早期より携わる審査スキルを強みとし、ITエンジニアスキルをベースとした審査・監査事業を中心に、情報セキュリティ関連の教育、サービスを提供しています。

ICMSは、セキュリティプロ集団として機密情報を保護し、ビジネスパフォーマンスの向上を支援します。

Copyright International Certificate Authority of Management System All rights Reserved.

ICMS サービスの紹介

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

- 審査/監査
  - ■ ISO/IEC 27001：2013
  - ■ ISO/IEC 27017：2015
  - ■ PCI DSS Qualified Security Assessor Company
  - ■ PCI P2PE Qualified Security Assessor Company
- Solution
  - ■ PCI DSS/P2PE 準拠支援、SAQ策定支援
  - ■ PCI DSS セキュリティサービス
- Education
  - ■ PCI DSS eラーニング
  - ■ ISMS/PCI DSS トレーニング
  - ■ 書籍PCI DSS Version3.2

- **【実績国内最多クラス>国内の主要インターネット決済代行事業者のオンサイト監査実績を持つ**

Copyright International Certificate Authority of Management System All rights Reserved.

1. QSAに要求される13の行動
2. 監査現場
3. オンサイト監査成功の鍵
4. QSAの有効活用
5. まとめ

Agenda

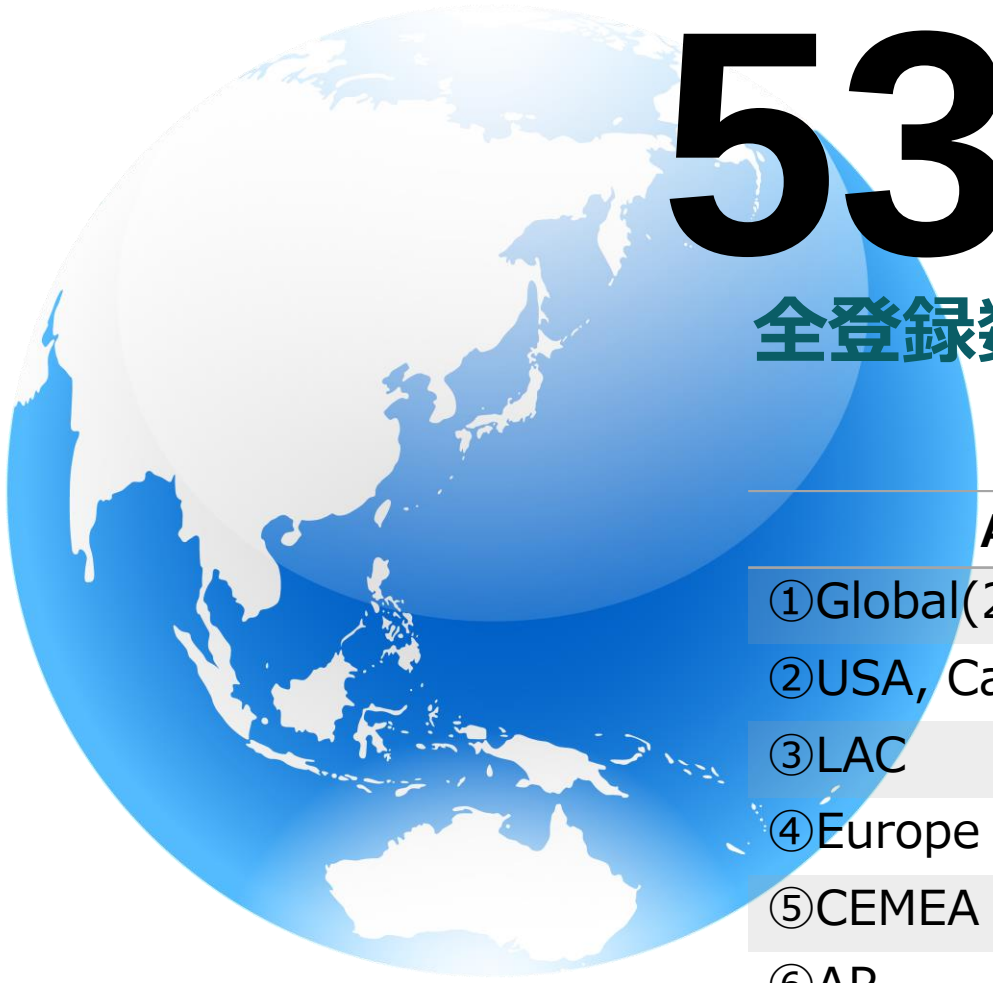
Copyright International Certificate Authority of Management System All rights Reserved.

1.　QSA 13 の行動

Copyright International Certificate Authority of Management System All rights Reserved.

Asia PacificのQSA会社数

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



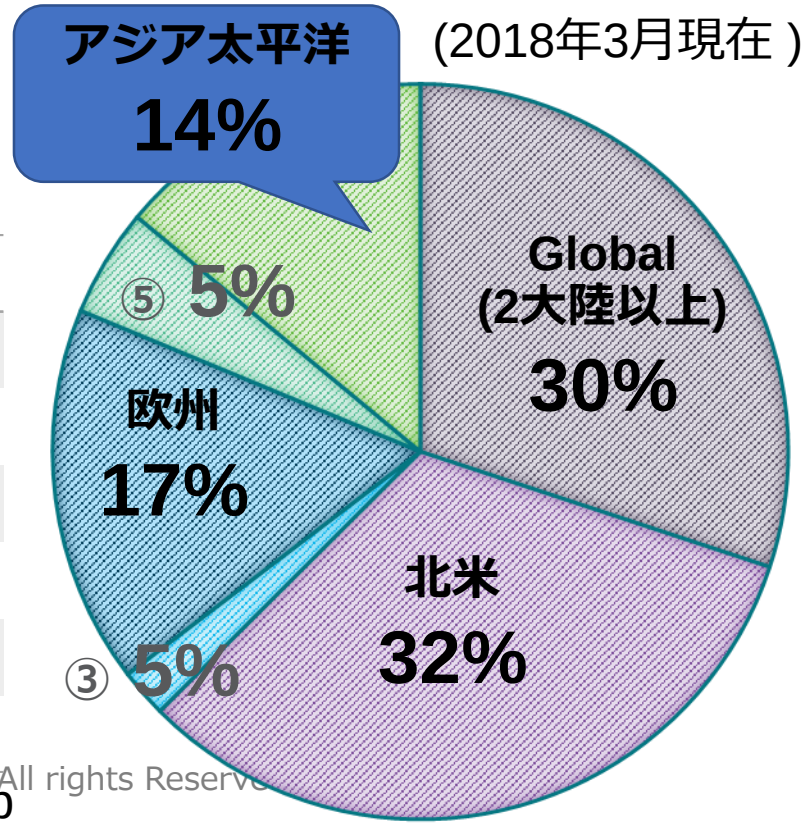
53

*グローバルにAPをカバーしている会社を除く

全登録数 ALL：382

Area	社数
①Global(2大陸以上)	114
②USA, Canada	123
③LAC	8
④Europe	63
⑤CEMEA	18
⑥AP	53

(2018年3月現在)



Copyright International Certificate Authority of Management System All rights Reserve

Source: PCI SSC web

QSAにどのようなイメージを持ちますか？

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

こんな顔のイメージが浮かびませんか?

Copyright International Certificate Authority of Management System All rights Reserved.

QSAにのぞましい行動は？

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

ISO 19011:2012
マネジメントシステム監査のための指針

7.2.2 個人の行動

”専門家としての行動を示すことが望ましい“として13個の行動が示されています。

Copyright International Certificate Authority of Management System All rights Reserved.

QSAにのぞましい行動は？

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

- **倫理的である。すなわち，公正である，信用できる，誠実である，正直である，そして分別がある。**
- **心が広い。すなわち，別の考え方又は視点を進んで考慮する。**
- **外交的である。すなわち，目的を達成するように人と上手に接する。**

Copyright International Certificate Authority of Management System All rights Reserved.

QSAにのぞましい行動は？

- **観察力がある。すなわち，物理的な周囲の状況及び活動を積極的に観察する。**

- **知覚が鋭い。すなわち，状況を認知し，理解できる。**

- **適応性がある。**
  すなわち，異なる状況に容易に合わせることができる。

Copyright International Certificate Authority of Management System All rights Reserved.

QSAにのぞましい行動は？

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

- **粘り強い。すなわち，根気があり，目的の達成に集中する。**

- **決断力がある。すなわち，論理的な理由付け及び分析に基づいて，時宜を得た結論に到達することができる。**

- **自立的である。すなわち，他人と効果的なやりとりをしながらも独立して行動し，役割を果たすことができる。**

Copyright International Certificate Authority of Management System All rights Reserved.

QSAにのぞましい行動は？

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

- **不屈の精神をもって行動する。すなわち，その行動が，ときには受け入れられず，意見の相違又は対立をもたらすことがあっても，進んで責任をもち，倫理的に行動することができる。**

- **改善に対して前向きである。すなわち，進んで状況から学び，よりよい監査結果のために努力する。**

Copyright International Certificate Authority of Management System All rights Reserved.

QSAにのぞましい行動は？

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

- **文化に対して敏感である。すなわち，被監査者の文化を観察し，尊重する。**

- **協働的である。すなわち，監査チームメンバー及び被監査者の要員を含む他人と共に効果的に活動する。**

Copyright International Certificate Authority of Management System All rights Reserved.

目立つイメージ

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

倫理的
Ethical

公正
Fair

粘り強い
Tenacious

観察力
Observant

不屈の精神
Observant

プラス

QSA

サーバー、ネットワーク機器、暗号化、データベース、プログラム
コーディング、最新ＩＴテクノロジー/脅威などの専門家としての知識

Copyright International Certificate Authority of Management System All rights Reserved

QSAのイメージは厳しい

厳格
緻密
教育指導者？？

蛇ににらまれた蛙？

Copyright International Certificate Authority of Management System All rights Reserved.

2.　監査現場

Copyright International Certificate Authority of Management System All rights Reserved.

こんな顔になっていませんか?

心配

不安

Copyright International Certificate Authority of Management System All rights Reserved.

監査前日　こんなことをしていませんか？

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

- **クライントPC内のPAN検索**
- **問題ないサンプリングデータを用意する**
- **カード情報管理状況確認**
- **メンバーへの整理整頓実施依頼**
- **メンバーへの前日教育（余計なことはしゃべらない？）**

Copyright International Certificate Authority of Management System All rights Reserved.

監査中　こんなことしていませんか？

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

- **聞かれたことだけ答える**
- **なるべく現場を見られないようする**
- **サンプリングは用意したものを見てもらうようにする**
- **できる限りデータは隠す**
- **質問はしない**

Copyright International Certificate Authority of Management System All rights Reserved.

監査後

皆さんこんな顔になっていませんか?

これで本当によいですか?

Copyright International Certificate Authority of Management System All rights Reserved.

3.　成功するオンサイト監査への鍵

Copyright International Certificate Authority of Management System All rights Reserved.

QSA13の行動に１つ追加します

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

Copyright International Certificate Authority of Management System All rights Reserved.

監査中の雰囲気が変化します

Copyright International Certificate Authority of Management System All rights Reserved.

こんなことがありました

Copyright International Certificate Authority of Management System All rights Reserved.

4.　QSAの有効活用

Copyright International Certificate Authority of Management System All rights Reserved.

QSAの有効活用

Copyright International Certificate Authority of Management System All rights Reserved.

PCI DSSの最新情報、今後の動向・展望

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

PCI SSCのブログ

PCI Security Standards Council

Contact FAQs Change Your Language...

SEARCH THIS BLOG

PCI Security | Assessors & Solutions | Document Library | Training & Qualification | About Us | Get Involved

< Return to Blog Home

Print

PCI DSS Now and Looking Ahead

POSTED BY LAURA K. GRAY ON 17 MAY, 2018 IN TLS/SSL AND INTERVIEW AND PCI DSS

0

28

0

Today the PCI SSC **published** a minor revision to the PCI Data Security Standard (PCI DSS) to account for dates that have already passed, such as the 1 February 2018 effective date for new requirements and Secure Sockets Layer (SSL)/early Transport Layer Security (TLS) migration dates.

Here we talk with PCI SSC Chief Technology Officer Troy Leach about the impact of this update, and what stakeholders can expect for the future of the PCI DSS.

Copyright International Certificate Authority of Management System All rights Reserved.

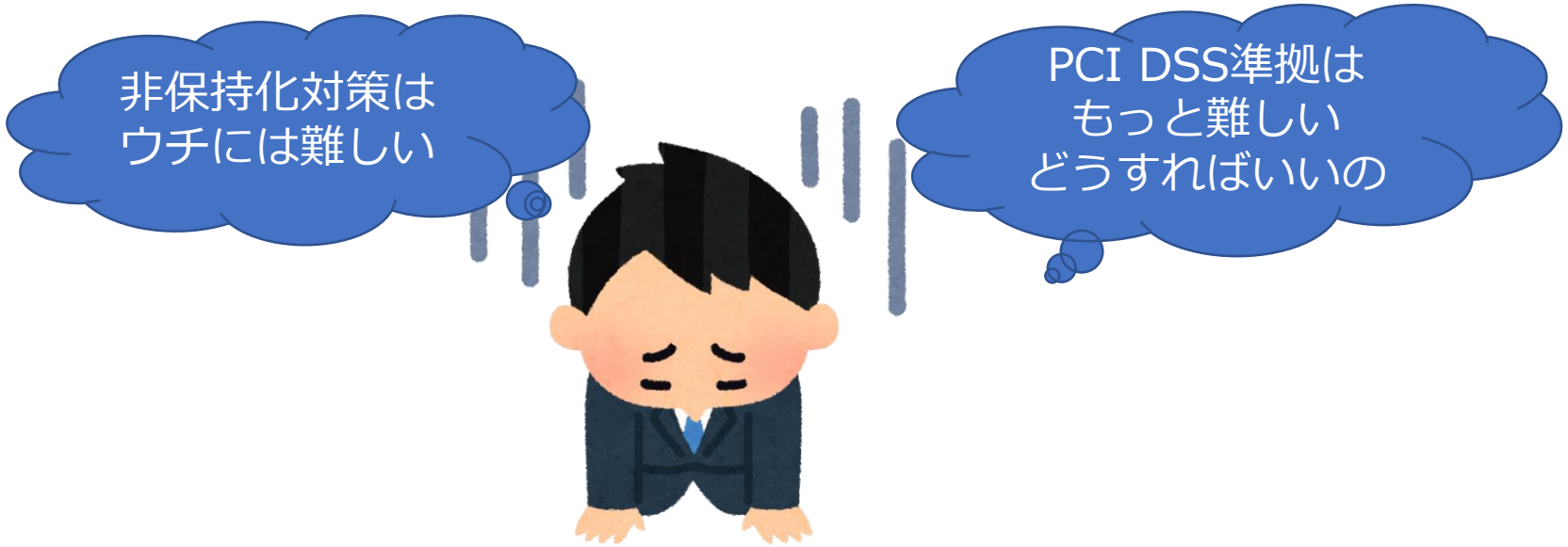
非保持化対策

どのような非保持化対策が
ウチの会社に合ってるのだろう？

非保持化対策したけど
本当にカード情報は残ってないのだろうか。。。

Copyright International Certificate Authority of Management System All rights Reserved.

中小加盟店のPCI DSS



Copyright International Certificate Authority of Management System All rights Reserved.

5.　まとめ

Copyright International Certificate Authority of Management System All rights Reserved.

QSAは皆さんの味方です！

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

Copyright International Certificate Authority of Management System All rights Reserved.

QSAを選ぼう！

Copyright International Certificate Authority of Management System All rights Reserved.

QSAを選ぼう！

Copyright International Certificate Authority of Management System All rights Reserved.

QSAを選ぼう！

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

もう監査は怖くありませんね！

Copyright International Certificate Authority of Management System All rights Reserved.

お問い合わせ

国際マネジメントシステム認証機構株式会社
〒141-0021
東京都品川区上大崎2-24-11　目黒西口M2号館 5階
TEL　：　03-5719-7533
mail　：　suishin@icms.co.jp
URL　：　https://www.icms.co.jp/

Copyright International Certificate Authority of Management System All rights Reserved.