加盟店におけるPOSのEMV対応と非保持化対応のポイント

～クレジット取引セキュリティ対策協議会　実行計画より～

2017年９月6日

オムロンソーシアルソリューションズ株式会社

SOCIAL AUTOMATION
CREATE OUR FUTURE

プレゼンテーションに先立って

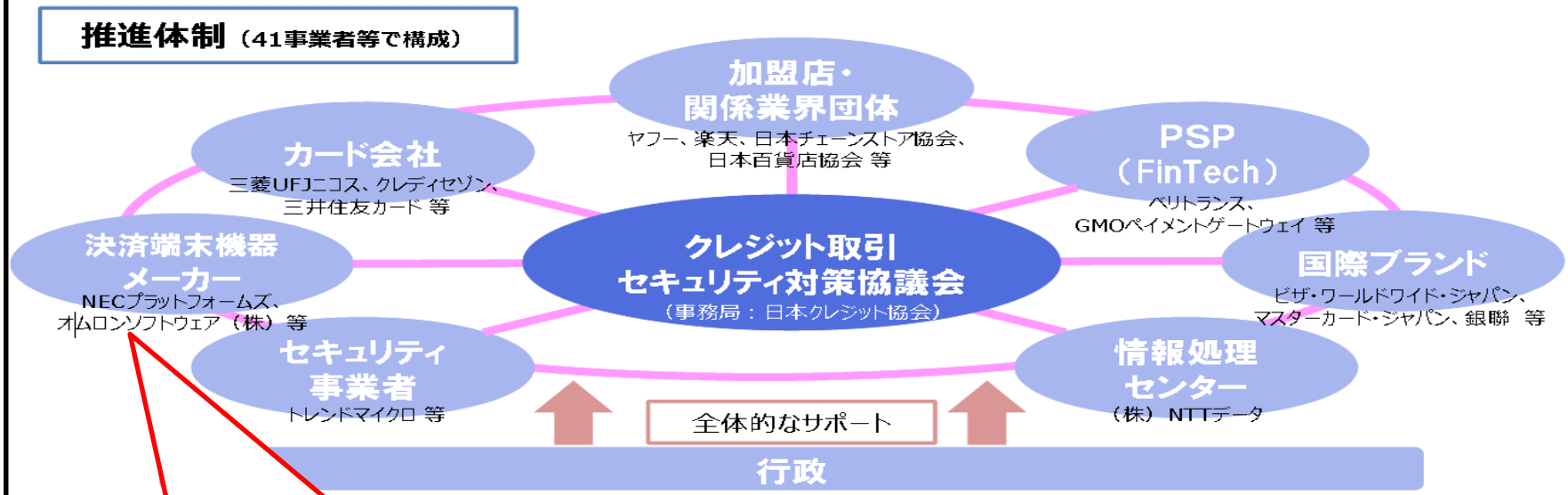
本プレゼンテーションは、クレジットセキュリティ対策協議会における実行計画を元に、同協議会とクレジット協会が作成したものを元としております。記載された内容は協議会のWG2委員として現時点の情報を元に作成したもので、加盟店における実施策の有効性等を保証するものではありません。また、対策案について将来に更に効果的な方策が発案される可能性を否定するものではありません。

2017年9月6日
オムロンソーシアルソリューションズ株式会社
EFTS事業本部　矢是泰士

0. 協議会とプロフィール

クレジット取引セキュリティ対策協議会

- 2020年に向け、**「国際水準のセキュリティ環境」**を整備することを目指し、クレジット取引に関わる**幅広い事業者及び行政が参画**して設立（2015年3月）。
- **目標**、**各主体の役割**、**当面の重点取組**をとりまとめた**「実行計画」**を策定（2016年2月）。
- **日本クレジット協会**を中心に、**「実行計画」の推進体制を構築**。今後、目標達成に向け、**進捗状況を管理・評価**し、**必要な見直し**を行っていく（2016年4月～）。



カード偽造防止対策（WG2）、実現方式検討SWG、非保持化SWGなどに委員として参画

POS向けIC対応ガイドラインの策定

OPOS技術協議会にてEMV対応手順を策定（CAT手順）

0. 企業プロフィール

・国内ではじめてとなるCAT（Credit Authorization Terminal）を開発し、クレジット処理端末の製造販売、および国内標準化等に参画してきました。

CATS-300/900

・POSシステム、大手量販店様むけソフトウェア開発・保守

・POS等向け、オールインワン決済端末「eZPAD」 ‘17.3 リリース

EMV-L1/L2、PCI-PTS、非接触（Felica/NFC）
PCI-PTS(SRED)/DUKPT対応予定

eZPAD

・クレジット/ポイント等の決済中継サービス「OTAC」の運営

1．「実行計画」における対策の３本柱

(1) カード情報の漏えい対策

◇カード情報を盗らせない

- 加盟店におけるカード情報の「非保持化」
- カード情報を保持する事業者のPCIDSS準拠

(2) 偽造カードによる不正使用対策

◇偽造カードを使わせない

- クレジットカードの「100%IC化」の実現
- 決済端末の「100%IC対応」の実現

(3) ECにおける不正使用対策

◇ネットでなりすましをさせない

- 多面的・重層的な不正使用対策の導入

2．加盟店におけるセキュリティ対策

※「対面取引」とは、クレジットカード券面を使用して決済を行う取引
※「非対面取引」とは、クレジットカード券面を使用しないで決済を行う取引

加盟店種別	具体的な対策	目標期日	法的義務
①対面取引及び非対面取引を行っている加盟店	○自社のクレジット決済システムのIC対応	2020年（平成32年）3月末	割賦販売法上の義務あり ※法律施行2018年(平成30年)6月予定
	○カード情報の非保持化を基本とし、保持する場合はPCI DSS準拠	2018年（平成30年）3月末	
	※以下、EC取引に限る ○自社での不正使用被害状況の把握等の体制整備、クレジットカード会社又はPSPとの迅速な情報共有 ○クレジットカード会社及びPSPとの協力による、本人認証、券面認証、属性・行動分析等の方策を基本とした多面的・重層的な対策	2018年（平成30年）3月末	
②対面取引のみ行っている加盟店	○自社のクレジット決済システムのIC対応	2020年（平成32年）3月末	
	○カード情報の非保持化を基本とし、保持する場合はPCI DSS準拠		
③非対面取引のみ行っている加盟店	○カード情報の非保持化を基本とし、保持する場合はPCI DSS準拠	2018年（平成30年）3月末	
	※以下、EC取引に限る ○自社での不正使用被害状況の把握等の体制整備、クレジットカード会社又はPSPとの迅速な情報共有 ○クレジットカード会社及びPSPとの協力による、本人認証、券面認証、属性・行動分析等の方策を基本とした多面的・重層的な対策	2018年（平成30年）3月末	

3．カード情報保護対策

(1)「非保持化」「カード番号」の定義

◆非保持化の定義

カード情報を電磁的に送受信しないこと、すなわち「自社で保有する機器・ネットワークにおいて「カード情報」を『保存』『処理』『通過』しないこと」をいう。

※非保持化の考え方は加盟店を対象としている

※ICに対応した決済専用端末を通過し、直接外部の情報処理センター等に伝送される場合は除く

◆カード番号とはみなさないもの (窃取されても"無価値"なため、悪用されない。)

トークナイゼーション	自社システムの外で不可逆な番号等に置き換え、自社システム内ではクレジットカード番号を特定できないもの
トランケーション	自社システムの外でクレジットカード番号を国際的な第三者機関に認められた桁数を切り落とし、自社内では特定できないもの

◆以下媒体でのカード番号の保存は、非保持とみなす

紙（クレジット取引伝票、カード番号を記したFAX、カード番号を記した申込書、メモ等）
紙媒体をスキャンした画像データ
電話での通話（通話データ含む）

3．カード情報保護対策

(2)非保持化と「同等/相当」のセキュリティ方策についての評価

- ◆ 暗号化等の処理によりカード番号を特定できない状態及び自社内で復号できない仕組みとし、非保持と同等/相当のセキュリティが確保できる場合、「非保持化」と同等/相当の措置として扱う。(例:PCI P2PE（PCI Point to Point Encryption）)
- ◆ 「非保持化」と同等/相当のセキュリティ措置により、百貨店・スーパー等で採用されている「ASP/クラウド接続型による内回り方式」においてもPCI DSS準拠を不要とすることができる。

(3)EC以外の非対面取引におけるカード情報保護

- ◆ メールオーダー、テレフォンオーダー等のEC加盟店以外の非対面加盟店において、カード情報を電話・FAX・はがき等での顧客からの注文によりカード決済をする場合、紙媒体のまま保存する場合は非保持となる。
- ◆ カード情報を電磁的情報として自社で保有する機器・ネットワークにおいて「保存」、「処理」、「通過」する場合は、PCI DSS準拠を求める。

4．POSのIC対応について　ガイドライン等

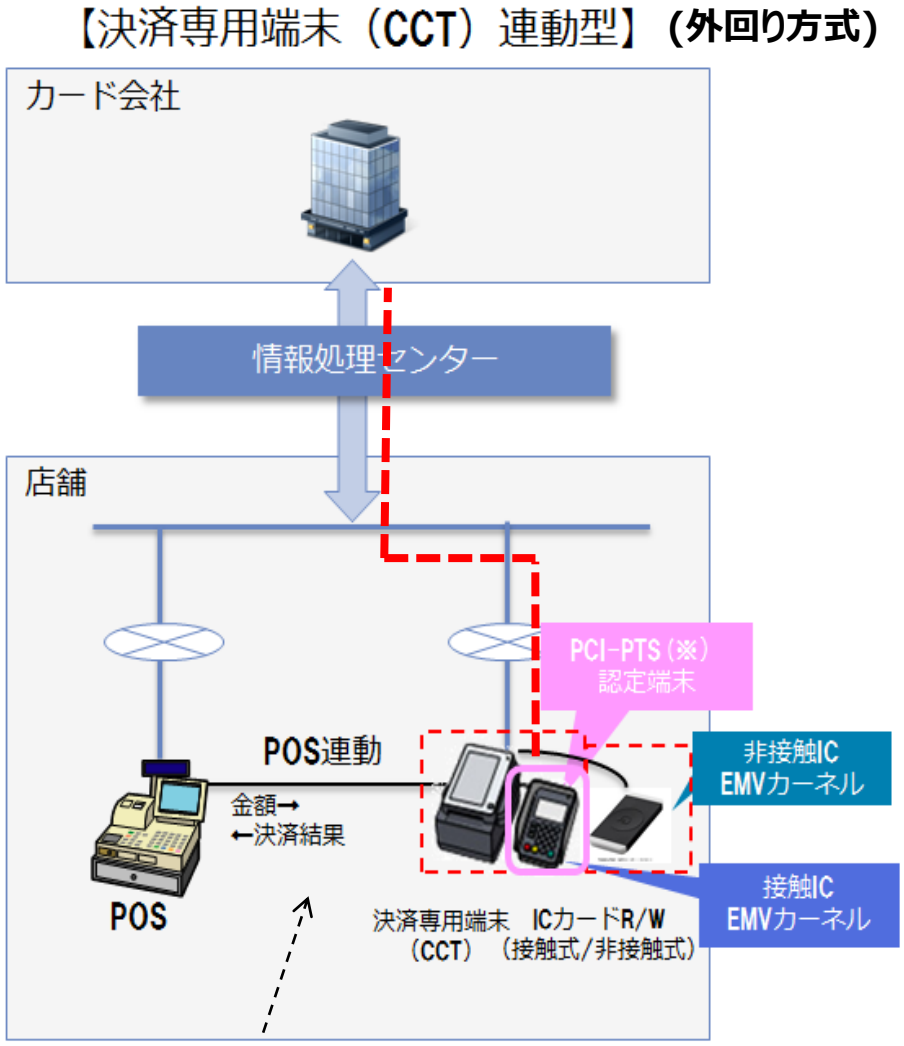
（１）協議会作成　POS対応ガイドライン

ICカード対応 POSガイドライン		Ⅰ．概要把握	Ⅱ．企画・設計		Ⅲ．試験	Ⅳ．導入		Ⅴ．運用・保守		各ドキュメントの主な対象読者
			端末関連	情報処理センタとの接続関連	端末認定・テストプロセス	端末操作・表示等	店員教育・啓発	運用要件	端末管理情報	
ドキュメント名と主な記述範囲	ICカード対応ＰＯＳガイドライン（第Ⅰ部：端末機能編）		●	●		●		●	●	ＰＯＳベンダ 加盟店ＩＴ担当
	ICカード対応ＰＯＳガイドライン（第Ⅱ部：接続運用編）			●				●		ＰＯＳベンダ 加盟店ＩＴ担当
	ICカード対応ＰＯＳ導入の手引き ～全体概要編～	●				●	●	●		加盟店ＩＴ担当 加盟店売場担当
	ICカード対応ＰＯＳ導入の手引き ～認定・試験プロセス概要編～		●		●				●	ＰＯＳベンダ 加盟店ＩＴ担当
	ICカード対応ＰＯＳ導入の手引き ～取引処理フロー解説編～		●		●					加盟店ＩＴ担当

（２）その他

・OPOS　1.14.1版をベースに「CAT手順/EVRW手順」をEMV対応

5．カード情報保護対策・決済端末のIC対応



※POS連動する「決済結果」にはカード情報を含めないこと

◆仕組み

・IC対応した決済専用端末（CCT）とPOSシステムの間で取引金額や決済結果等を連動する仕組み

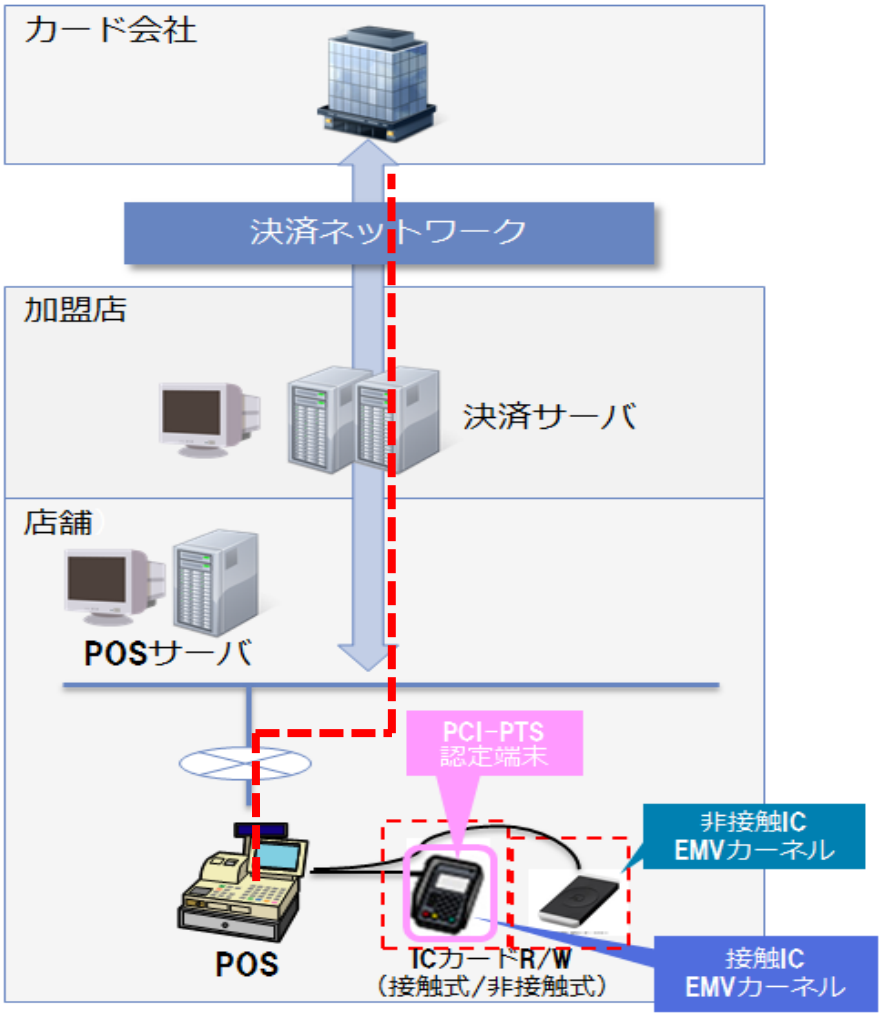
◆参考

・加盟店あるいはカード会社等が所有するIC対応した決済専用端末から直接、外部の情報処理センターに伝送される仕組み。

・決済機能はPOSシステムの外側となるため、オーソリゼーションやクレジットカードの売上処理は、カード情報をPOS端末やPOSシステムの機器・ネットワークに「保存」、「処理」、「通過」せずに行われ、カード情報の非保持化が実現できる。

5．カード情報保護対策･決済端末のIC対応

【決済サーバ設置型】　(内回り方式)



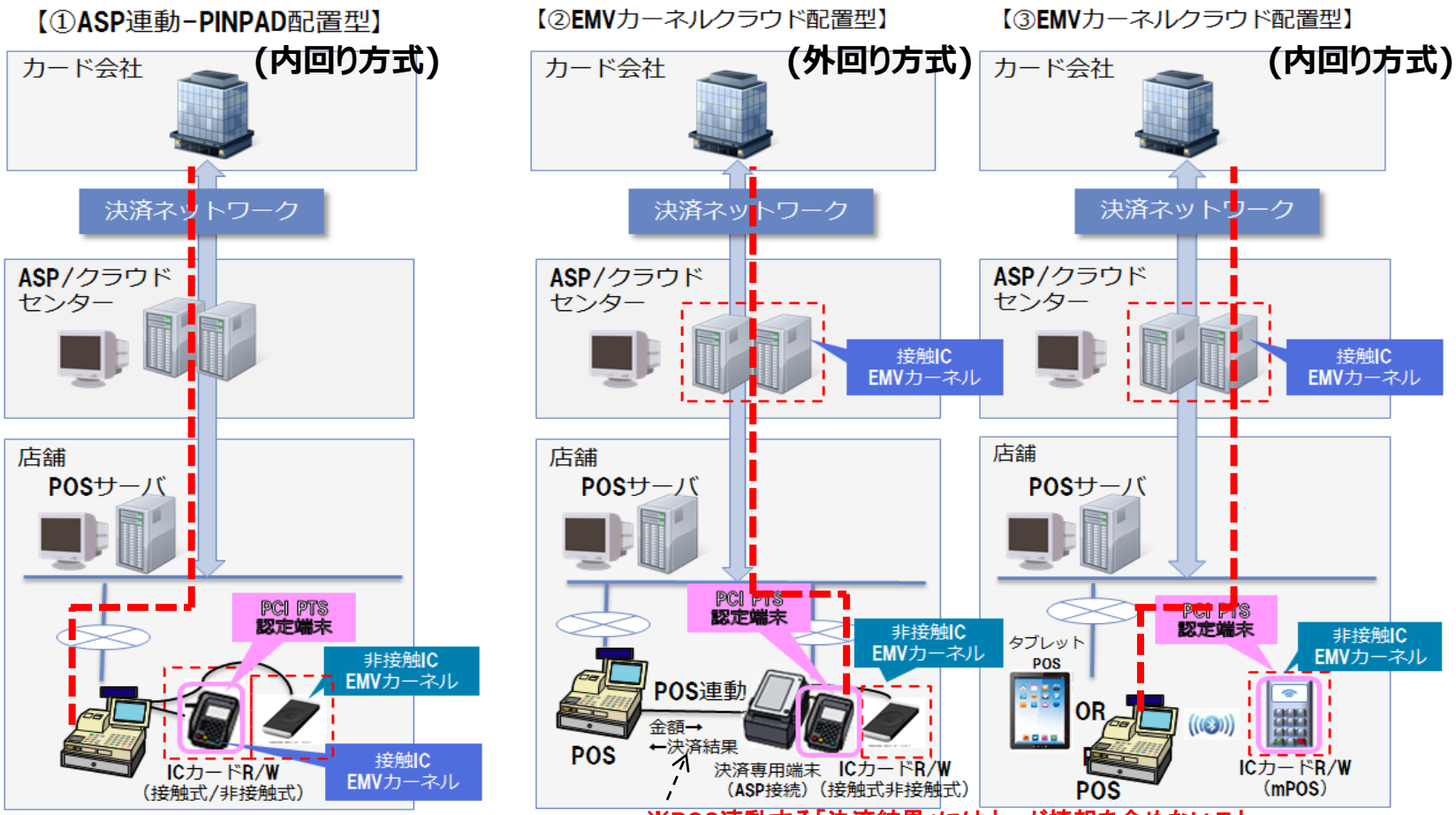
◆仕組み

・POSシステムで決済を行うが、EMVカーネルがIC-PINPADにある仕組み

◆参考

・カード情報はPOSシステムを通過してカード会社に伝送されるため、「PCI DSS準拠」又は「非保持化と同等/相当のセキュリティ措置」を講じることが必要となる。

5．カード情報保護対策･決済端末のIC対応



※POS連動する「決済結果」にはカード情報を含めないこと

◆仕組み

・POSシステムと加盟店の外側の事業者（ASP）との間で取引金額や決済結果を連動させる仕組み

◆参考

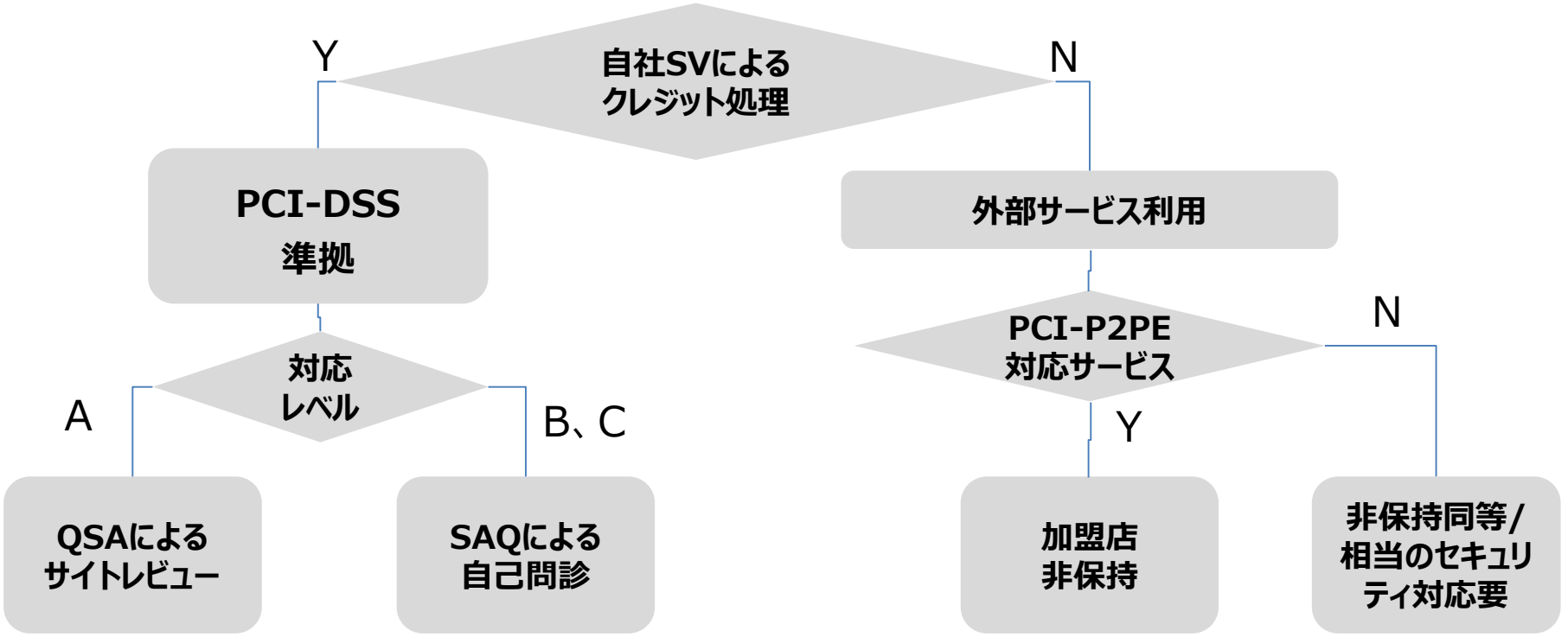
・上記②については、カード情報がIC対応の決済専用端末から直接社外のASP/クラウドセンターに伝送されるため、加盟店におけるカード情報の非保持化が同時実現。

・上記①及び③の場合には、カード情報が自社内ネットワークを保存・処理・通過するため、非保持にならず、「PCI DSS準拠」又は「非保持化と同等/相当のセキュリティ措置」を講じることが必要。

SOCIAL AUTOMATION
CREATE OUR FUTURE

5．カード情報保護対策･決済端末のIC対応

POS（内回り）においてカード情報保護対策をどう考えるか？



※PCI-P2PEソリューション利用により準拠
項目は331→33項目に削減される

SAQの詳しい内容に関しては日本カード情報セキュリティ協議会（JCDSC）http://www.jcdsc.org/を参照

（参考）PCI-DSS準拠方法について

改定版　日本におけるクレジットカード情報管理　スキーム

対　象	形　態	基　準 加盟店は年間カード売上件数	レベル		クレジットカード情報管理の対応	PCIDSS検証方法
PSP	非対面／ネット	全て	ー	①	PCIDSS準拠	
加盟店	非対面／ネット・ネット以外	4ブランドにより決定（※2）	A	②	クレジットカード情報非保持（※1）またはPCIDSS準拠	オンサイトレビュー および ネットワークスキャン
	対面／POS			③		
	非対面／ネット・ネット以外	レベルA以外	B	④		自己問診 および ネットワークスキャン
	対面／POS	100万件以上、レベルA以外（※3）		⑤		
	対面／POS	100万件未満（※4）	C	⑥		
	対面／スタンドアローン	全て	ー	ー	クレジットカード情報非保持対応済み（※1）	

※1　クレジットカード情報非保持とは、自社のサーバーにおいてクレジットカード情報を「保存」「処理」「通過」しないことを指す。

※2　① VISA　：600万件以上
② Master　：600万件以上
③ JCB　：100万件以上
④American Exp　：250万件以上

このリストを基に4ブランドにより対象企業を選別する

※3　いずれかのブランドにおいて、100万件以上を指す。

※4　いずれのブランドにおいても、100万件未満を指す。

6．「非保持化」と同等/相当のセキュリティ措置

- ここでは、「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画-2017-」（2017年3月8日／クレジット取引セキュリティ対策協議会）に基づき、**対面加盟店における非保持と同等/相当のセキュリティ確保を可能とする措置に関する具体的な技術的要件**について扱うものとする。

「実行計画2017」

（２）対面加盟店におけるカード情報の非保持化について

■ASP/クラウド接続型（内回り方式）

オーソリゼーションやクレジットカードの売上処理のため、カード情報が決済端末からPOSシステム又は社内システムを介してASP事業者・情報処理センター等外部事業者へ送られる方式である。

この場合、カード情報が自社内機器・ネットワークを「保存」、「処理」、「通過」するため、「非保持」とならず、原則としてPCI DSS準拠が必要となる。ただし、暗号化等の処理によりカード番号を特定できない状態とし、自社内で復号できない仕組みとすれば、仮に窃取されてもカード情報として不正使用することは極めて困難であり、非保持と同等/相当のセキュリティが確保できるため、本実行計画においては、これを「非保持化」と同等/相当のセキュリティ措置として扱うものとする。こうした措置の一例として、PCI P2PE（PCI Point to Point Encryption）がある。

（略）

（４）「非保持化」と同等/相当のセキュリティ措置について

前述（２）の「ASP/クラウド接続型（内回り方式）」等のように「非保持」とならない場合においても、非保持と同等/相当のセキュリティ確保を可能とする措置に関する具体的な技術要件について検討するため、本協議会の下に本件を扱う「サブ・ワーキンググループ」を設置し、技術要件を定め、対面加盟店における具体的なソリューションの検討を促すこととする。