迫るPCI DSS 4.0 対応

多要素認証（MFA）はRSAにご相談ください!!

2024年4月1日より、実に13年ぶりとなるPCI DSSのメジャー新バージョン「v4.0」の運用が始まります。
前バージョン「v3.2.1」から新項目が64項目追加され、そのうち51項目は2025年3月31日までに準拠する必要があります。本資料では、「ユーザー認証」に絞ってポイントを解説します。

☑ 準拠対象事業者が拡大

PCI DSSの準拠対象事業者は「カード会員データ環境(CDE)のセキュリティに影響を与える可能性のあるすべての事業体」となりました。これによりクレジットカードを取り扱うすべての事業者は準拠を求められる可能性があります。

準拠を求められる可能性のある事業者

金融	流通・小売	通信	エネルギー	その他
▪ クレジットカード会社（プリペイド含む） ▪ 銀行等クレジットカード発行金融機関	▪ 大手百貨店 ▪ スーパー ▪ コンビニ ▪ 量販店 ▪ 鉄道 ▪ 航空会社	▪ 携帯電話会社 ▪ 通信会社 ▪ ISP	▪ 電気 ▪ ガス ▪ ガソリンスタンド等の石油業界	▪ クラウドサービス事業者 ▪ ECサイト ▪ 決済代行業 ▪ QR決済

RSAなら、業種・企業規模を問わずご利用いただける多要素認証ソリューションを提供できます。

☑ 多要素認証が必須の領域が拡大

「全てのカードデータ環境（CDE)へのアクセス」において、多要素認証が必須になりました。　（要件8.4.2）

多要素認証の必須領域

【v3.2.1の場合】
- 非コンソールでのすべての管理者アクセス（8.3.1項）
- 適用範囲すべてへのリモートアクセス　（8.3.2項）

【v4.0の場合】
- 非コンソールでのすべての管理者アクセス　（8.4.1項）
- カード会員データ環境（CDE）へのすべての アクセス　（8.4.2項）
- 適用範囲すべてへのリモートアクセス　（8.4.3項）

RSAなら、オンプレミスでもクラウドでも。さまざまなシステムに実装可能なユニファイド・アプローチでお客様の重要資産へのアクセスを保護します。

☑ 多要素認証の要件が厳格化

実装すべき多要素認証の要件がより厳格化されました（要件8.5.1）
現在実装済みの場合でも、要件と比較をすると不足が生じる可能性があります。

<8.5.1項>
少なくとも異なる2種類の認証要素が使用されている
→ ✕ 二段階認証

RSAなら、お客様のニーズに合わせた多彩な認証方式を選択できます。

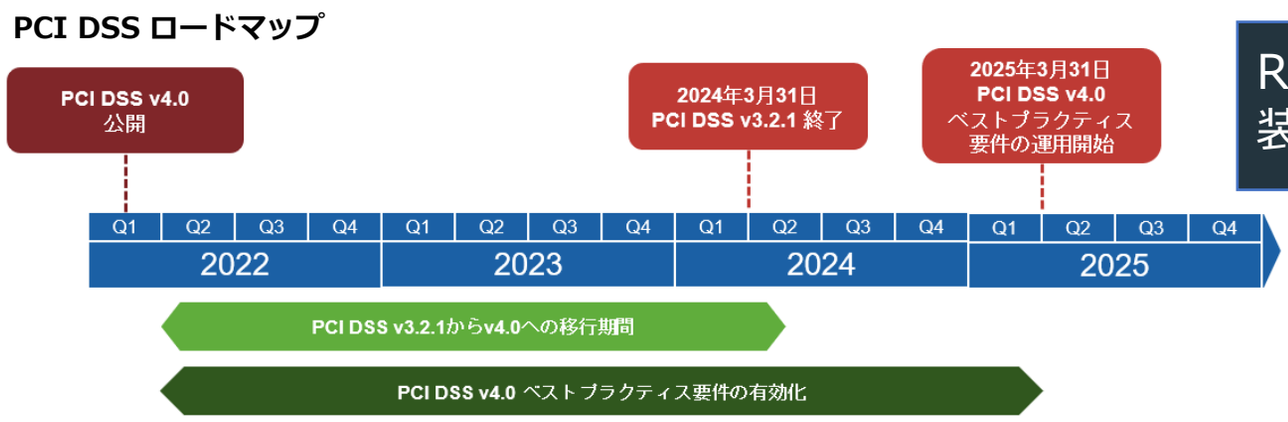
<8.5.1項>
多要素認証システムはリプレイ攻撃の影響を受けない
→ ✕ 中間者搾取が可能なOTP (SMS OTP等)

リプレイ攻撃の影響を受けにくい1分毎に更新されるOTPはじめ、生体、FIDO認証を活用できます。

☑ 2025年3月31日までに実装

多要素認証含む51項目は「ベストプラクティス」として1年間の実装猶予期間が設けられています。

PCI DSS ロードマップ



RSAなら、多様な連携方式に対応し、短期間で実装・ご利用いただくことができます。

PCI DSS v4.0 at a Glance（https://docs-prv.pcisecuritystandards.org/PCI%20DSS/General%20Guidance/PCI-DSS-v4-0-At-A-Glance.pdf）を基にRSA作成

RSA Security Japan合同会社　| Identity事業部 |　https://www.rsa.com/ja/
〒151-0051　東京都渋谷区千駄ヶ谷5-27-3 やまとビル8F | 03-4520-3203 |　info-j@rsa.com

RSA ID Plus

ID Plusは最先端の多要素認証およびアイデンティティ保証ソリューションです。
ゼロトラストセキュリティに基づく便利で安全なアクセスを実現できます。
さまざまな認証方法と動的でリスク主導のアクセス ポリシーによって、SaaSアプリケーションと従来のエンタープライズ リソースを保護します。

2,500万
アイデンティティ

40 年
以上の実績

12,000
社以上のお客様

RSA ID Plus の特徴

特徴①：バラエティーに富んだ認証方式に対応。スマホをお持ちでないユーザーでも問題なし

- スマートフォンアプリによる多彩な認証方式。パスワードレス認証の実現を支援
- 40年の実績を誇るワンタイムパスワードソリューション
- 最新のFIDO2規格対応デバイス

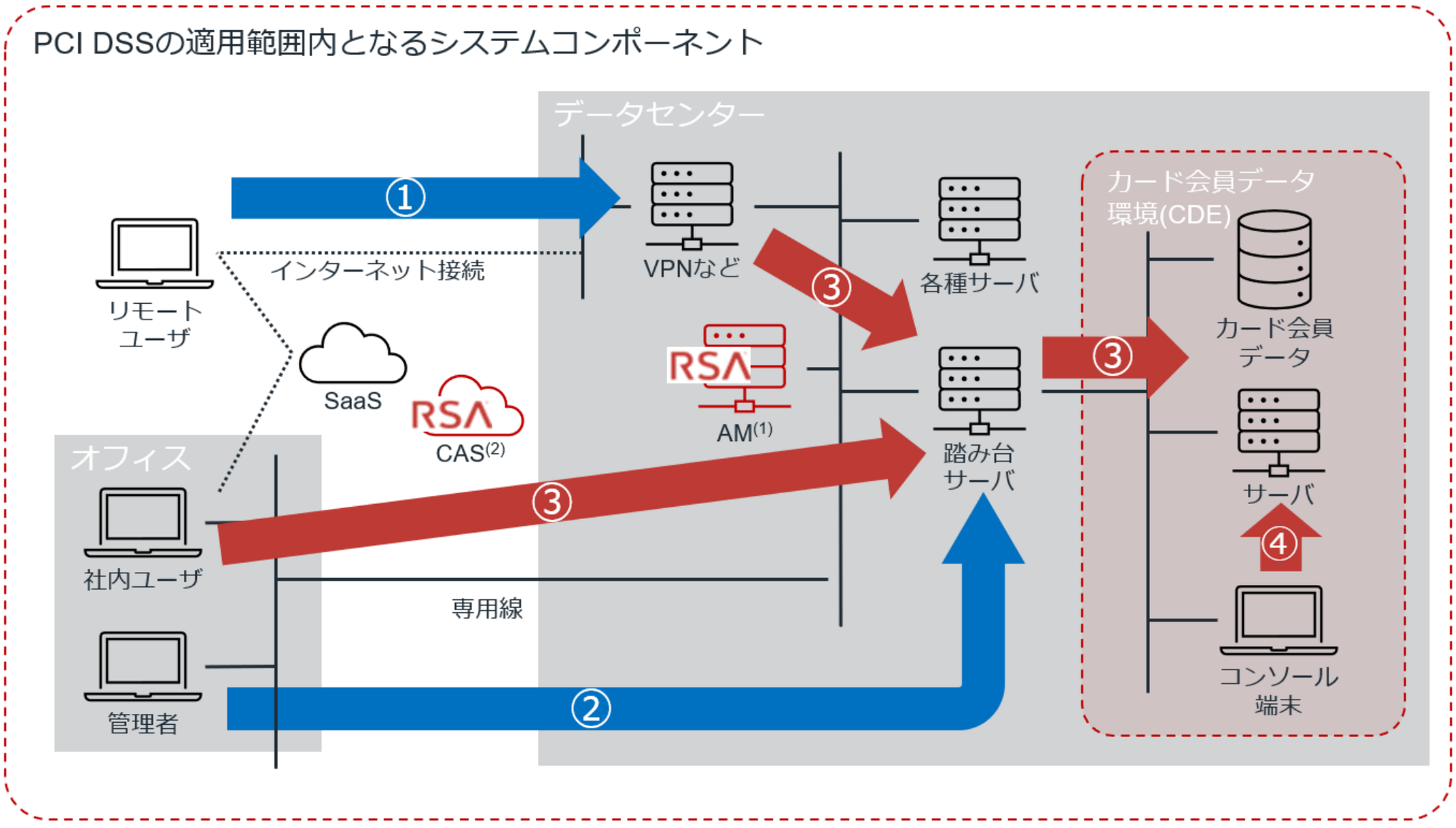
特徴②：クラウドからオンプレミスまで。ハイブリッド環境をシームレスに一括ログイン

- SAML連携により数千種類のクラウドサービスとSSO連携
- オンプレミスリソースにも対応。Webアプリケーション以外のシステムも豊富にサポート
- オンプレミス専用認証サーバーでBCP対策も万全

特徴③：RSA独自のリスクベース認証(Risk AI)でより強固な不正アクセス対策を実現

RSA多要素認証では、ユーザーのアクセス要求に対し、静的／動的両面からリスク評価を行います。その要求が高いリスクを伴う場合は追加認証を行ったり、あるいは認証自体を遮断するなどして、ユーザーの信頼性を高めます。

RSA ID Plus x PCI DSS 4.0 ユースケース



注記

(1) Authentication Manager。RSA SecurID/ID Plusにおいてオンプレ環境内での認証を提供するアプライアンスです。

(2) Cloud Authentication Service。RSA SecurID/ID PlusにおいてSaaS / オンプレ環境の認証を提供するクラウドサービスです。

【PCI DSS3.2.1での対象】

① CDEへのアクセスまたは影響を与える可能性のある環境(PCI DSSの適用範囲内となるシステムコンポーネント)へのリモートアクセスにMFAが要求されます(8.4.3)

② CDE環境へ管理者権限でアクセスする非コンソールアクセスにMFAが要求されます(8.4.1)

【PCI DSS4.0での拡張】

③CDE環境へのすべてのアクセスにMFAが要求されます(8.4.2)
※①で外部からの接続でMFA認証が許可されても、③の認証を透過的に省略することは出来ません

④解釈の余地はありますが、コンソールアクセスについても要件8.4.2での「すべて」に該当すると解釈すれば、MFAが要求される可能性があります。