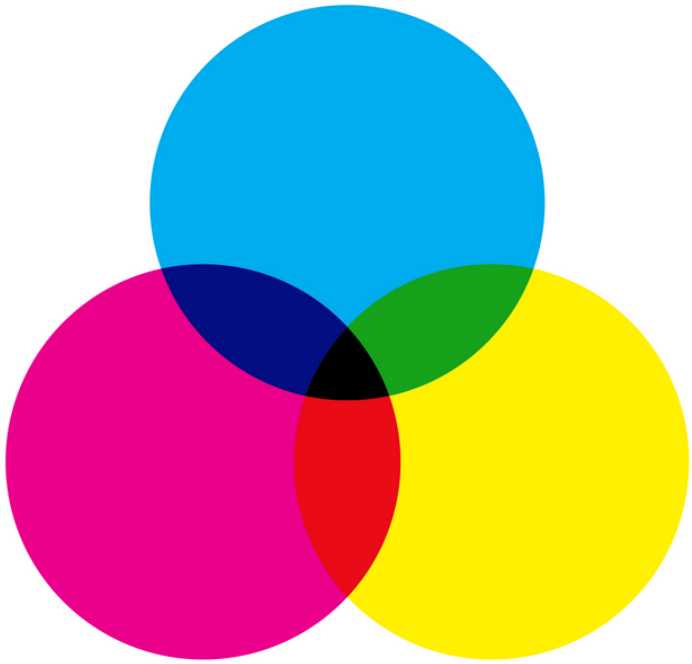
SECURE SKETCH BOOKS

VOLUME 3



クレジットカード業界の新たなセキュリティ基準、「PCI 3DS」とは？

カードの不正利用を防ぐための新たな認証、3Dセキュアに迫る

Edited by

Sakura Tsuruta

NRI SecureTechnologies, Ltd.

はじめに

インターネット上で行われる非対面取引において、クレジットカードによる決済は利便性が高いと言われる反面、不正使用の懸念もあげられます。カード情報不正使用防止の対策方法のひとつである本人認証にはいくつかの手法があり、「3Dセキュア」もそのひとつです。

クレジット取引セキュリティ対策協議会が策定する「実行計画」における対策の3本柱のひとつに「ECにおける不正使用対策」があげられ、ネットでなりすましをさせないための「多面的・重層的な不正使用対策の導入」がうたわれています。

また、 2018年3月1日に2018年版の実行計画(以下、実行計画2018)が公開された「実行計画2018」にも、検討事項として具体的に本人認証の強化策となる「3Dセキュア2.0への移行・導入」も含まれています。

本書では、3Dセキュアの仕組みを組み込んだサービスを提供する際に準拠が求められる『PCI 3DS』について、3Dセキュア環境とPCI 3DSにて求められる要件の対応関係などを踏まえて解説します。

「3D セキュア」のVer1.0と、Ver2.0の違いとは？

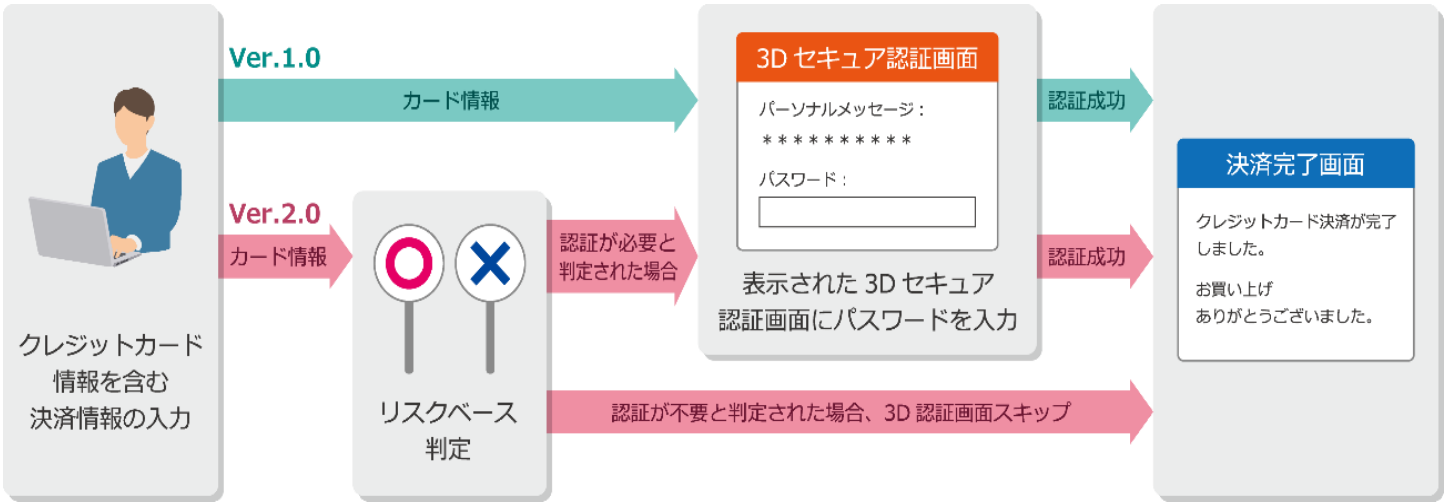
3Dセキュアには、現状、Ver.1.0とVer.2.0の２つの仕様が存在します。Ver.1.0は従来仕様であり、Ver.2.0は2016年10月に公開された次期仕様となります。それぞれのサービスイメージを下図に示します。

■3DセキュアVer.1.0について

Ver.1.0では、クレジットカード情報を入力後、追加で3Dセキュアによる本人確認が要求されます。これにより、セキュリティ強化の観点では一定の効果が期待できましたが、一方で、本人による決済要求であっても、パスワード忘れや、本人確認の煩雑さによって利用者が購入をあきらめてしまう離脱（いわゆる、”かご落ち”）率が高くなる、といった問題がありました。

■3DセキュアVer.2.0について

Ver.2.0では、Ver.1.0に加え、新たに「リスクベース認証」を導入することが必須となるため、上記の懸念が軽減される可能性があります。これは、過去の取引履歴等に基づくリスク分析を行い、リスクが低い利用者に対しては3Dセキュアによる追加の本人確認が不要となる機能です。また、スマートフォン等においても同様に利用可能となります。



3Dセキュアにおける認証情報の保護

3Dセキュアの仕組みのポイントは、本人のみ把握しているパスワード等の認証情報を利用することです。従って、この認証情報を安全に管理することが非常に重要となります。

そのため、ペイメントブランドから、3Dセキュアのサービスを提供する事業者（プロバイダ）へセキュリティの担保が要求されます。具体的に要求されるセキュリティ基準は、各ブランドで個別に定義されており、プロバイダは従来から年次での対応が課せられてきました。

3DセキュアVer.2.0が公開され、利便性および安全性向上のため、取り扱う認証情報が機微になったことや、一部構成に変更が発生していることから、プロバイダは、セキュリティの担保について従来以上に考慮する必要が出てきました。

セキュリティ基準「PCI 3DS」とは

上記の背景を踏まえ、各ブランドで定義されていたセキュリティ基準の統一化が図られました。セキュリティ基準の定義について、ブランドから、PCI DSS等のカード情報を統括的に管理するためのセキュリティ基準を策定しているPCI SSCという団体に移管されました。2017年末に、PCI SSCは「PCI 3DS」というセキュリティ基準を公開し、2018年からはプロバイダはそれに従い対応を進めていくように変更になりました。

PCI 3DS Requirementsは、以下の2領域に大別されています。

①PCI 3DS Core Security Standard
3Dセキュア・プロトコルを用いた本人認証サービスの提供基盤（ACS/DS/3DSS）（※後述）に適用される基準。

②PCI 3DS SDK Security Standard
3Dセキュアのサービスを利用する上で必要になるユーザーインタフェース（モバイルアプリケーション向け）の設計・開発において適用される基準。

本書では、現時点で、日本において関係する上記①「PCI 3DS Core Security Standard」について取り上げます。以降「PCI 3DS」と省略して記載します。

PCI 3DSは、Part1およびPart2で構成されており、Part1は主にPCI DSSの要件の一部、Part2はPCI 3DSの独自要件となっています。Part1においては、PCI DSS準拠を前提に、適用が免除される可能性があります。PCI 3DSの独自要件であるPart2の要件一覧を下表に示します。

パート	概要
P2-1： スコープの妥当性	PCI 3DSの対象となる全てのネットワークおよびシステムコンポーネントを特定し、文書化および検証する。
P2-2： セキュリティガバナンス	3DEおよび関連プロセスの保護のためにリスク管理や責任の割当てを行う。
P2-3： 3DSのシステムとアプリケーションの保護	3DSシステムおよび3DEをサポートするアプリケーションを保護する。
P2-4： 3Dセキュアシステムへの安全な論理アクセス	3DSシステムおよび環境への論理的アクセスを保護する。
P2-5： 3Dセキュアのデータ保護	3DS データを保護する。
P2-6： 暗号化と鍵管理	3DSエンティティの鍵管理およびHSMを保護する。
P2-7： 3Dセキュアシステムの物理的安全性	データセンター環境でACSおよびDSシステムコンポーネントを保護し、3DEに対して技術的および運用面でのセキュリティを導入する。

「3Dセキュア」環境と「PCI 3DS」要件の対応関係

3Dセキュア環境（3DE: 3DS Data Environment）とは、ACS, DS, 3DSS（下図参照）等を含むシステムコンポーネント間において3DS messages（3DSコンポーネント間を流れるデータ群）が連携される領域を指します。PCI 3DSの審査対象スコープは、3DS messagesが流れる3DEおよび3DEにアクセスする環境となります。

3Dセキュアは、イシュア、相互運用、アクワイアラの3つのドメインで構成されており、それぞれのドメインごとに対応するコンポーネントが異なります。

■3DEのドメインとコンポーネントについて

ACS（Access Control Server）

カード番号、デバイスタイプによる3Dセキュア認証の可否、カード保有者の取引内容認証、およびアカウント情報確認する機能を提供するサーバーで、イシュアドメインの主要コンポーネントです。

DS（Directory Server）

3DSサーバーとACSの認証、3DSサーバーとACS間のメッセージの連携、および3DSサーバー、3DS SDK、および3DSリクエスタの検証する機能を提供するサーバーで、相互運用ドメインの主要コンポーネントです。

3DSS（3DS Server）

カード保有者のデバイスと3DSデータの連携を行う機能とDS間の必要な情報を精査・連携する機能を提供するサーバーで、アクワイアラドメインの主要コンポーネントです。

Part2は、審査スコープやガバナンス等の全社的な要件（P2-1、P2-2）、3DSシステムやデータに関わる要件（P2-3、P2-4、P2-5）、鍵管理に関わる要件（P2-6）、およびデータセンター内の施設要件（P2-7）で構成されています。
それぞれの観点を以下に示します。

■PCI 3DS Part2について

Part2-1、2-2

審査対象スコープの見極めや、全社セキュリティが適切に管理されているか等。

Part2-3、2-4、2-5

3DSに関する通信、データの保管について、必要最小限のものに制限されているか、ログが取得されているか等。

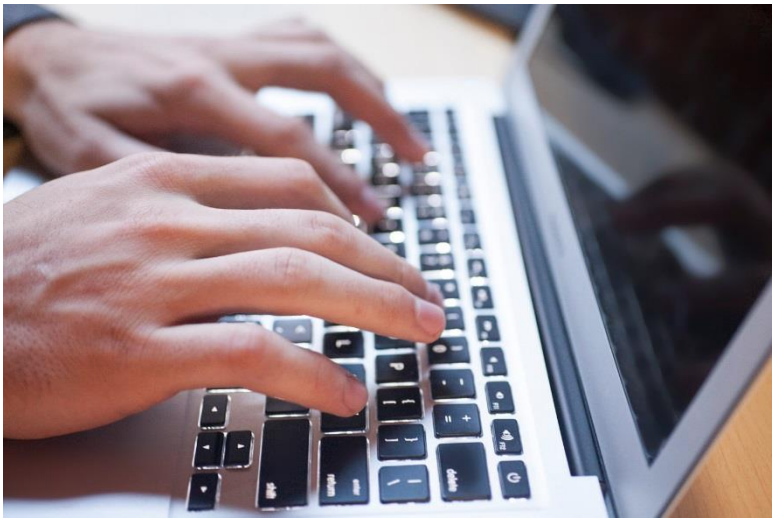
Part2-6

暗号鍵の管理手順が整備されているか、鍵管理に必須なHSMが適切に管理されているか等。

Part2-7

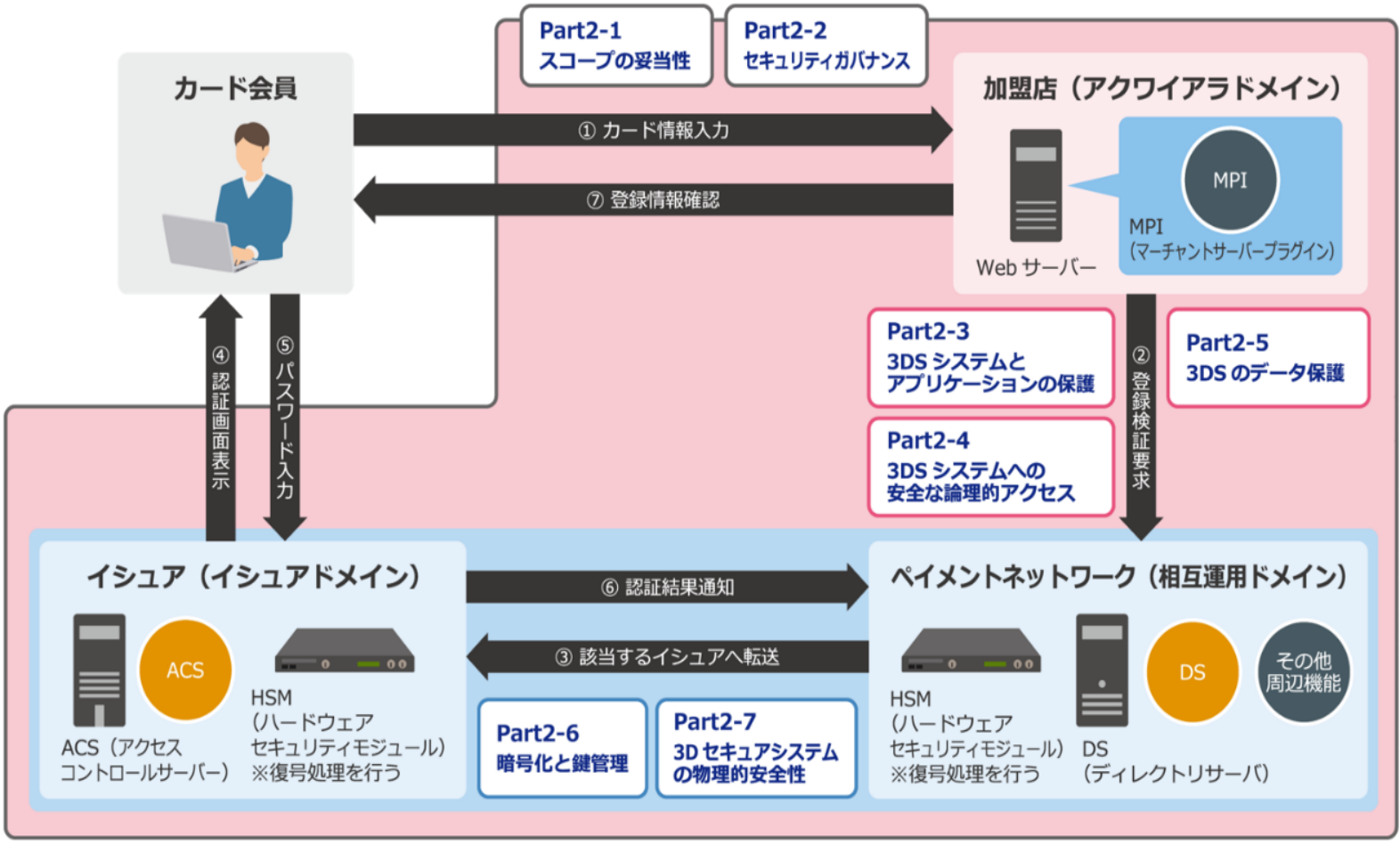
ACSとDSが設置されているデータセンターについて、入退室が適切に管理されているか、物理的な侵入検知の仕組みがあるか、監視カメラの記録が取得されているか等。

Part2-1～2-5については、類似の観点がPCI DSSの要件にも出てきますが、Part2-6、2-7については、PCI DSSにはない観点も規定されています。



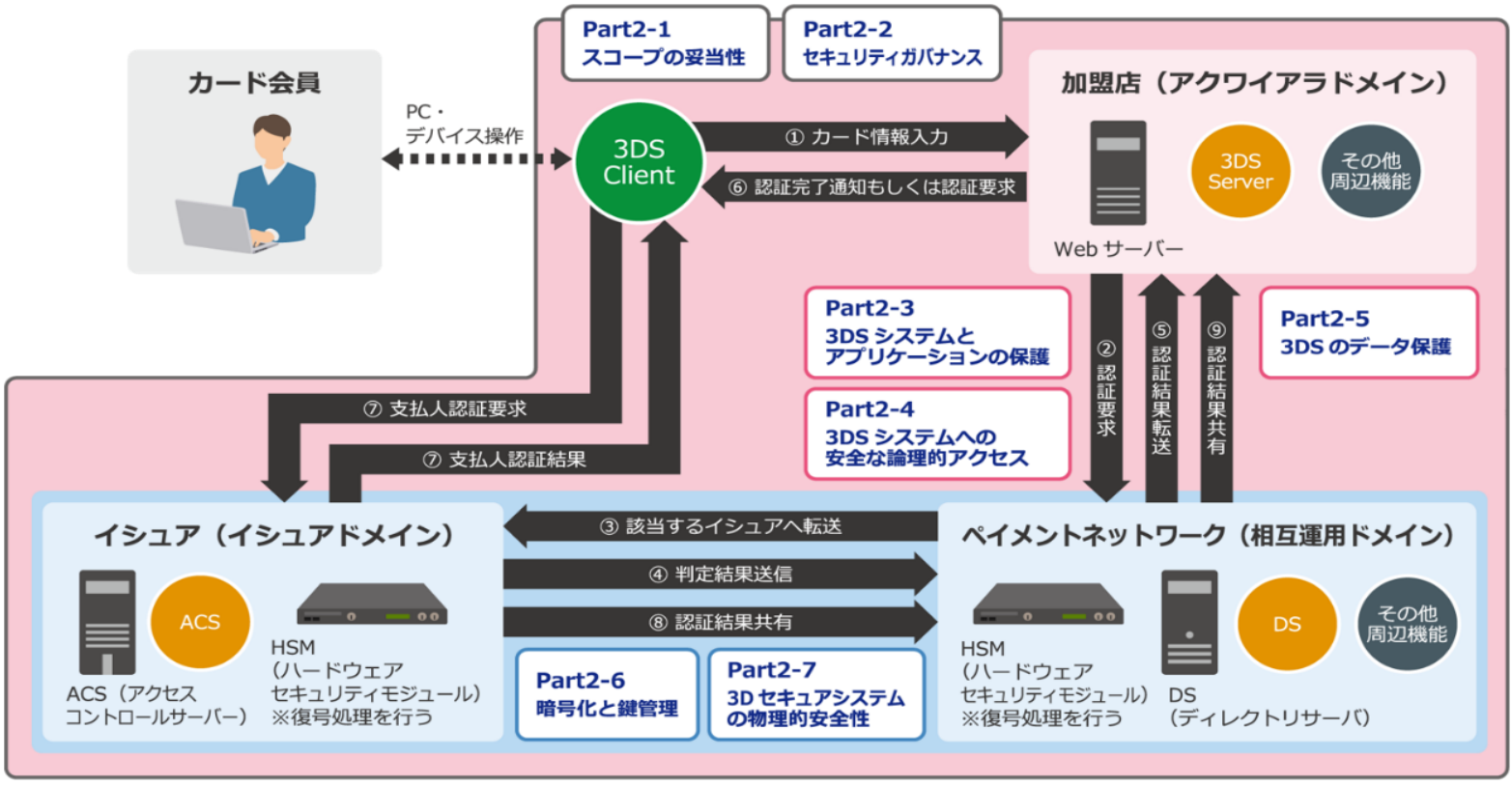
3DEとPCI 3DS Part2の要件の関係について、Ver.1.0およびVer.2.0それぞれのイメージは以下の通りです。

【3Dセキュア Ver1.0の場合】



※PCI 3DS要件の対象箇所を視覚的に表現したものであり、3Dセキュアの仕組みにおける全処理フローを記載したものではありません。

【3Dセキュア Ver2.0の場合】



※PCI 3DS要件の対象箇所を視覚的に表現したものであり、3Dセキュアの仕組みにおける全処理フローを記載したものではありません。

おわりに

今回は、クレジットカードの不正利用を防止するための「3Dセキュア」、そしてそれを実装するためのセキュリティ基準である「PCI 3DS」についてのポイントを解説しました。

NRIセキュアでは、この「3Dセキュア」を評価する「PCI 3DS準拠支援コンサルティング／審査」サービス行っています。本サービスは、加盟店やカード発行会社へ3Dセキュアによる本人認証サービスを提供するプロバイダに対し、NRIセキュアがPCI Security Standards Council（PCI SSC）が認定した日本初の「3DS Assessor（3Dセキュアの仕組みを評価・審査機関）」として提供しているものです。

本サービスを通じて、3Dセキュアの仕組みを組み込んだサービスを提供する際に準拠が求められるPCI 3DSの各セキュリティ要件に対し、審査資格である3DS Assessorを保有する専門審査員が、現状とのギャップ分析や効果的な対策案の提示、訪問審査までをワンストップで支援をしています。興味・関心のある方はぜひお問合せ下さい。

NRIセキュアテクノロジーズ株式会社　マネジメントコンサルティング部　須田、小泉
TEL：03-6706-0622　E-mail： info@nri-secure.co.jp

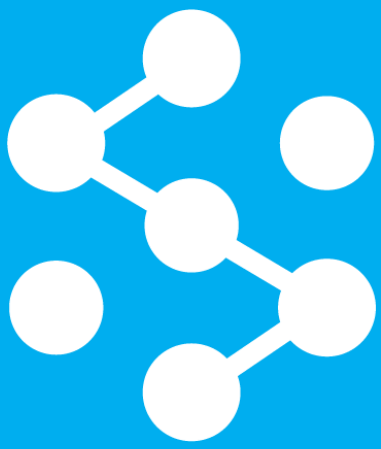
＜参考サービス＞
PCI 3DS準拠支援コンサルティング/審査
https://www.nri-secure.co.jp/service/consulting/pcidss_3ds.html

筆者略歴

鶴田　さくら

大手電機メーカーにて、プラットフォーム系ソフトウェアの開発、プリセールスを経て、2017年に野村総合研究所に入社。NRIセキュア出向後、PCI DSSおよびPCI 3DSの準拠支援を中心とした、セキュリティコンサルティング業務に従事。

NRI SECURE



Secure SketCH

セキュリティ経営をシンプルに

https://www.secure-sketch.com