

クレジットカード情報の非保持化に向けた トークン決済のご案内



ヤマトフィナンシャル株式会社

-ver.1.0-

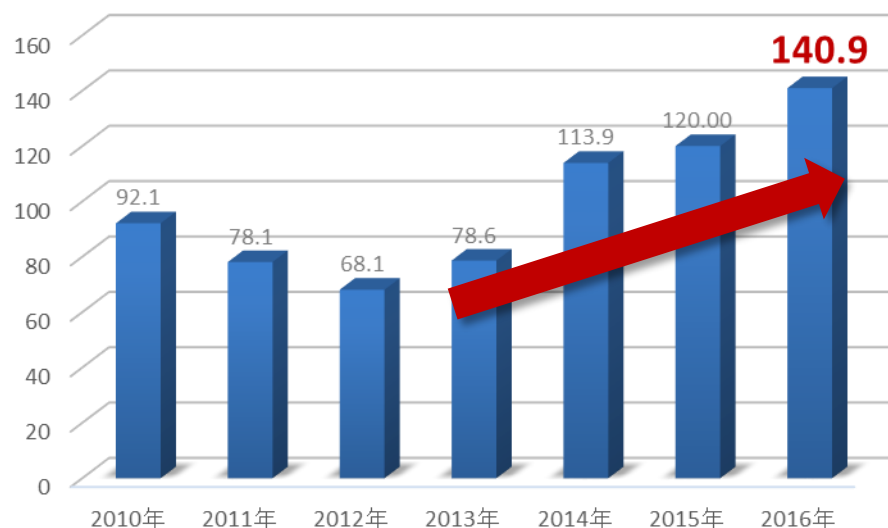


1.クレジット取引の不正利用被害の増加

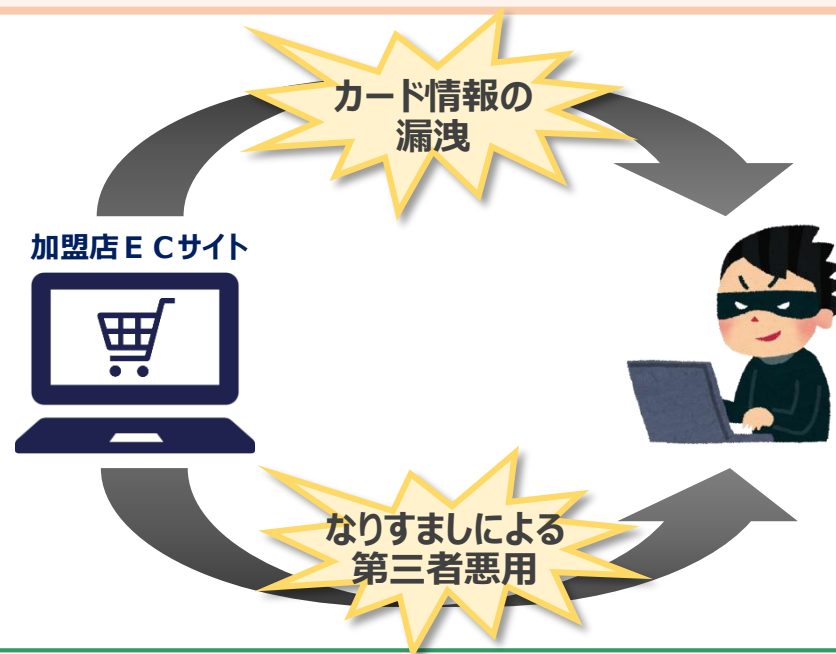
E C市場の拡大により近年クレジット取引は急増、
これに伴い不正利用も増加の一途をたどっている

不正利用の被害額は
4年間で約2倍に
また**62%がE C**による被害

なりすまし被害の原因は
偽造カード等から
カード情報漏えいに
よるものに変化



出典：一般社団法人 日本クレジット協会「クレジットカード不正使用被害の発生状況」より
(2017年3月)



2.2020年に向けたクレジットカードセキュリティの強化

(1) 経済産業省が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を発表

クレジットカードの取引が拡大する一方で、カード情報の漏洩や不正利用も増加しています。政府は2020年のオリンピック・パラリンピック開催に向けて、クレジットカード取引における「国際基準のセキュリティ環境」を整備することを目指し、2018年6月までに施行予定の「改正割賦販売法」において**加盟店に対するセキュリティ対策を義務化**、これを実現するための指針として実行計画を定めました。

(2) 「実行計画」における対策の3本柱と加盟店様の対応内容

① カード情報の漏えい対策（カード情報を盗らせない）

EC

■ 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 **PCI-DSS※準拠**

※PCI-DSS

Payment Card Industry Data Security Standards。クレジットカード情報および取引情報の安全管理を 目的に、国際カードブランド5社（VISA、JCB、American Express、Master card、Discover）により策定された クレジットカード業界における国際セキュリティ基準。

2018年3月までに

PCI-DSSの準拠、またはカード情報の非保持化

② 偽造カードによる不正利用対策（偽造カードを使わせない）

対面

■ クレジットカードの「**100% IC化**」の実現

■ カード決済端末の「**100% IC化**」の実現

2020年3月までに

店頭のカード決済端末のIC化対応

③ ECにおける不正利用対策（ネットでなりすましをさせない）

EC

■ **多面的・重層的**な不正利用対策の導入

2018年3月までに

3Dセキュア、セキュリティコード、属性・行動分析、配送先情報などを活用した多面的・重層的な不正利用防止

3.カード情報の非保持化について

クレジットカード決済を提供している加盟店様においては
2018年3月までのカード情報の非保持化が必要となります

カード情報の非保持化とは、カード情報を電磁的に送受信しないこと、

加盟店様で保有する機器・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

以下の様な場合は「カード情報の保持」になります



カード情報を保持する加盟店様は**PCI-DSSへの準拠が必要**です

【参考資料1】カード情報とみなされないもの

(1) 窃取されても「無価値」であるため悪用されないもの

① トークナイゼーション

自社システムの外で不可逆的な番号に置き換え、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。

元のカード番号 4980 1234 1234 1234

→ **1Q2a 32eF 5L0q 2A3x 58d1**

トークン方式の決済

② 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すことで自社内ではカード番号を特定できないもの。

元のカード番号 4980 1234 1234 1234

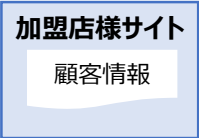


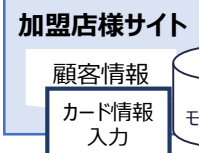
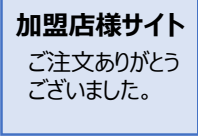
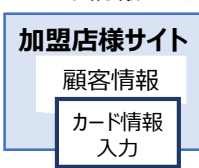
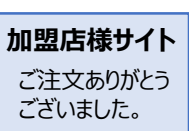
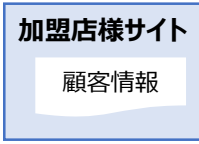
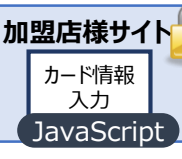
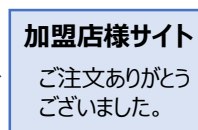
→ **4980 1200 0000 1234**

(2) 自社で保有する機器、ネットワークに保存しないもの

電話受注等、EC以外の通販において、カード情報を電話、FAX、はがき等のように機器やネットワークを介さず保存する場合は「非保持」となります。

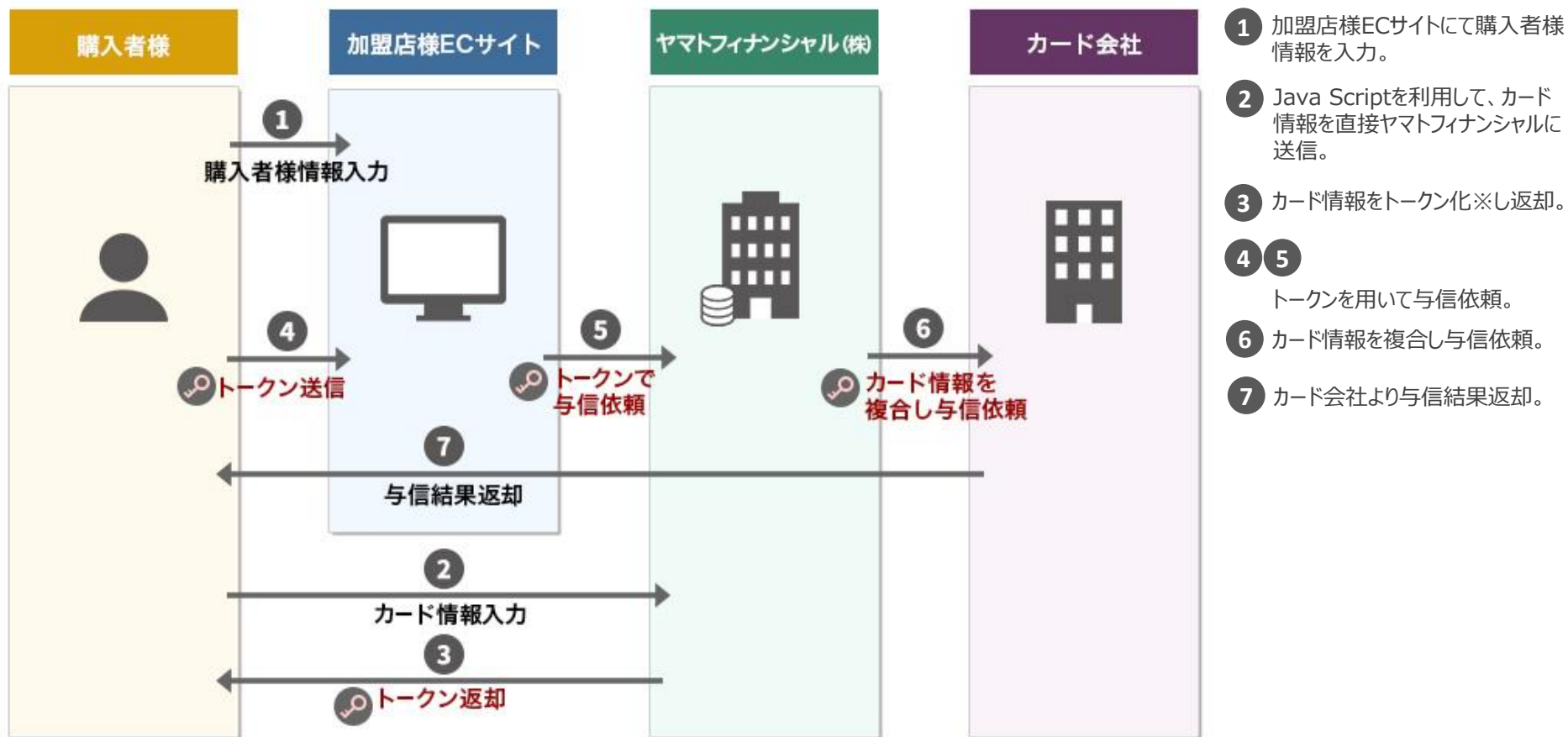
4.決済方式別に見たカード情報の非保持

2016年度の実行計画より「保存」、「処理」に「通過」が加わり
非保持を満たすためには**リンク方式またはトークン方式の導入が必要**となります

決済方式	カード情報	画面遷移	画面遷移イメージ	画面区分
リンク方式	○ 非保持	✕ 当社側のサイトに遷移する	①加盟店サイトにて顧客情報を入力  → ②お支払手続き画面に遷移 カード情報を入力  → ③決済完了 	顧客情報入力画面
				加盟店様
				カード情報入力画面
モジュール方式 (SDK方式)	✕ 加盟店サーバを通過	○ 加盟店サイトで完結するため違和感がない	①加盟店サイトにて顧客情報カード情報を入力  → ②決済完了 	顧客情報入力画面
				加盟店様
				カード情報入力画面
API方式	✕ 加盟店サーバを通過	○ 加盟店サイトで完結するため違和感がない	①加盟店サイトにて顧客情報カード情報を入力  → ②決済完了 	顧客情報入力画面
				加盟店様
				カード情報入力画面
トークン方式	○ 非保持	○ 加盟店サイトで完結するため違和感がない	①加盟店サイトにて顧客情報を入力  → ②入力したカード情報はトークン化して送信  → ③決済完了 	顧客情報入力画面
				加盟店様
				カード情報入力画面
				決済代行会社

5.トークン方式について

カード情報をトークン化する決済方式を導入いただくことで
カード情報を非保持化に対応することができます



※ 発行されたトークンは一度与信に利用すると無効となります。

6. 2つのトークン方式

(1) モーダルウィンドウ式

- ① 加盟店様ECサイトで
購入者様情報を入力。
- ② 当社が提供するカード情報
入力画面にて、カード情報を入力。
- ③ 加盟店様ECサイトにて入力項目
の確認、決済を実行。
- ④ 決済完了。



セキュリティ ◎ 操作性 ✕

(2) 組込式 (2017年11月リリース予定)

- ① 加盟店様ECサイトで
購入者様情報を入力。
- ② 加盟店様ECサイトでカード情報
を入力 (カード情報をトークン化)。
- ③ 加盟店様ECサイトにて入力項目
の確認、決済を実行。
- ④ 決済完了。



セキュリティ ○ 操作性 ◎

7. 多面的、重層的な不正利用対策

従来の本人認証（3Dセキュア）やセキュリティコードだけでなく
属性・行動分析や配送情報による不正利用対策が必要となります

（１）第三者からの利用を防ぐ本人確認（3Dセキュア、セキュリティコード）

ヤマトフィナンシャルでは本人認証（3Dセキュア）やセキュリティコードを標準サービスとして提供しています。

① 本人認証（3Dセキュア）



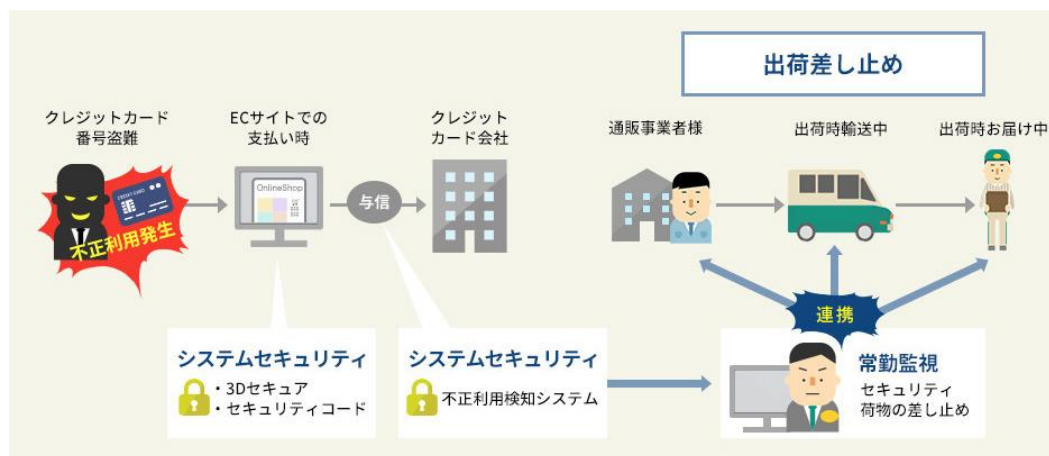
国際カードブランドVISA、Master、JCBが採用している本人認証サービス。
カード番号、有効期限に加え、インターネット専用のID・パスワードを購入者様に入力していただく事により本人承認する事で第三者によるクレジットカードの不正利用を防止します。

② セキュリティコード



クレジットカード番号とは別に、カードの裏面または表面に記載された3桁もしくは4桁の番号。コードは券面上だけで確認でき、第三者による不正利用を防げる方法として有効です。

（２）配送情報の活用



商品配送に宅急便をご利用の場合は、クレジットカードの売上確定を出荷情報をもとに行っております。
また、常勤監視を実施しているため、不正利用の懸念がある取引を発見した場合は、ヤマト運輸に連携し出荷の差し止めを行う事で不正利用の防止を図っています。

【参考資料 2】PCI-DSSの要求基準

対象となる範囲において下記の要件をすべて遵守、
これらを自己、もしくは第三者の確認によって証明することでPCI-DSSに準拠

（１）安全なネットワークの構築と維持	【要件1】カード会員データを保護するために、ファイアウォールをインストールして構成を維持する。 【要件2】システムパスワードおよび他のセキュリティパラメーターにベンダー提供のデフォルト値を使用しない。
（２）カード会員データの保護	【要件3】保存されるカード会員データを保護する。 【要件4】オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する。
（３）脆弱性プログラムの維持	【要件5】すべてのシステムをマルウェアから保護し、ウィルス対策ソフトウェアまたはプログラムを定期的に更新する。 【要件6】安全性の高いシステムとアプリケーションを開発し、保守する。
（４）強力なアクセス制御手法の導入	【要件7】カード会員データへのアクセスを、業務上必要な範囲内に制限する。 【要件8】システムコンポーネントへのアクセスを確認・許可する。 【要件9】カード会員データへの物理アクセスを制限する。
（５）ネットワークの定期的な監視 およびテスト	【要件10】ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する。 【要件11】セキュリティシステムおよびプロセスを定期的にテストする。
（６）情報セキュリティ・ポリシーの維持	【要件12】すべての担当者の情報セキュリティに対応するポリシーを維持する。

また、適用レベルについては取扱規模により異なります。

	EC加盟店 取扱規模（年間）	適用内容
レベルA	①～④の2つ以上に該当 ① VISA 600万件以上 ② Master 600万件以上 ③ JCB 100万件以上 ④ AMEX 250万件以上	QSA※による訪問審査 ※Qualified Security Assessors:認定審査会社
レベルB	4ブランドいずれかが100万件以上	自己問診（SAQ※）
レベルC	4ブランドいずれも100万件未満	※Self Assessment Questionnaire

出典：日本カード情報セキュリティ協議会「PCI DSS準拠の方法とJCDSCによるサポート体制」より（2016年7月25日版）