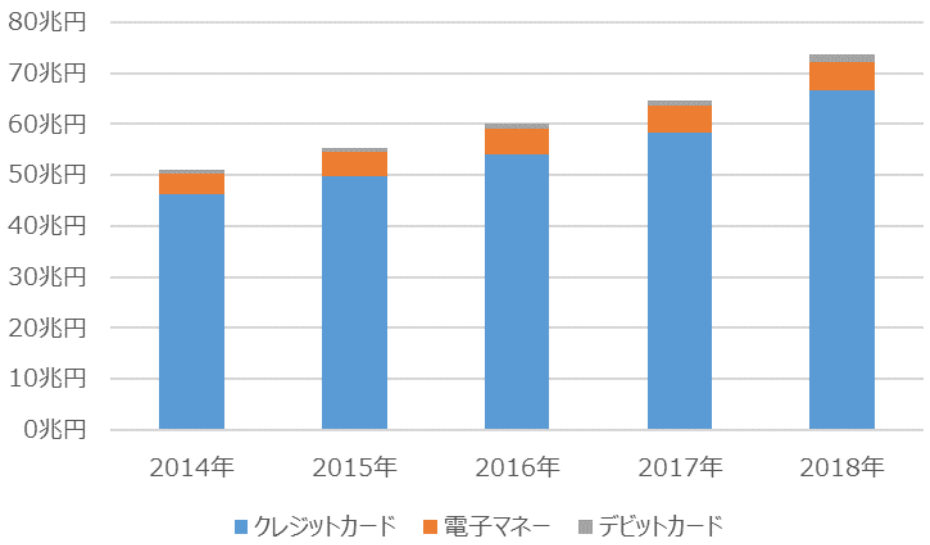
2020 年 2 月 28 日

サービス＆セキュリティ株式会社 e-Gate センター

# スマホ決済サービスのセキュリティ対策

## 1. はじめに

2019 年 10 月の消費税増税に伴い、キャッシュレス決済でポイント還元を受けられる事業が始まりました。中でも、スマホひとつで簡単に行えるスマホ決済サービスはさらに注目を集めています。




**【図 1】キャッシュレス決済の利用額推移**

(出典：日本クレジット協会「日本のクレジット統計」、日本銀行「決済動向」)

一方、2020 年 1 月に情報処理推進機構（IPA）が発表した「情報セキュリティ 10 大脅威 2020」によると、個人における脅威としてスマホ決済サービスの不正利用が 1 位に挙げられています。今回はこのスマホ決済サービスの特徴とセキュリティ対策についてご紹介いたします。

## 2. スマホ決済サービスとは？

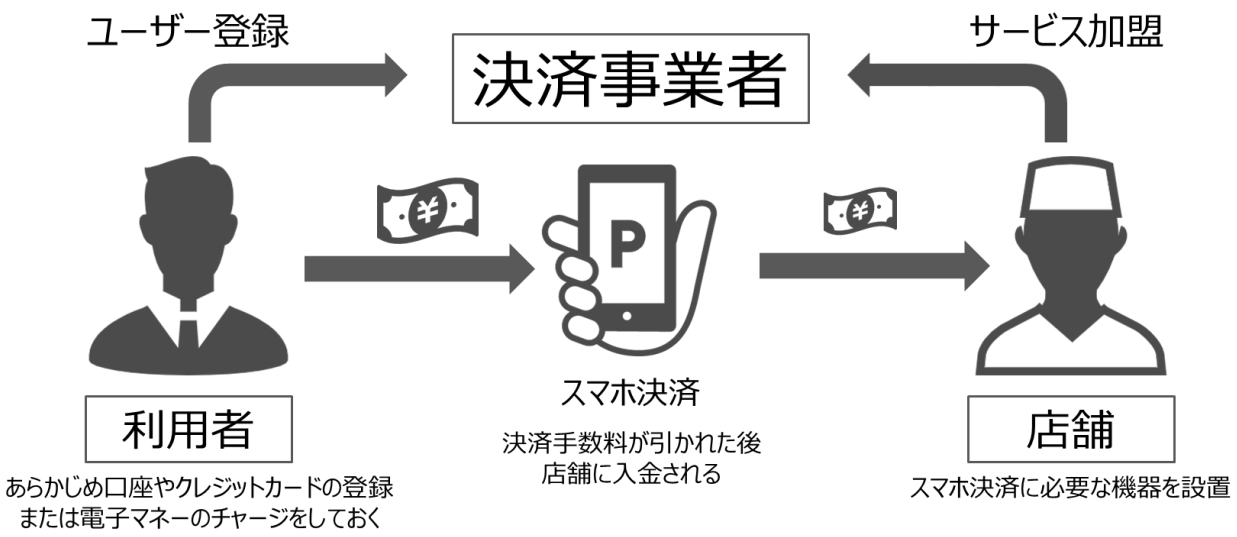
スマホ決済アプリのひとつ、PayPay による 2018 年 12 月の「100 億円あげちゃうキャンペーン」をご存じの方も多いのではないでしょうか。あの大規模なキャンペーンをきっかけにスマホ決済を始めた方も少なくないと思われます。

PayPay 以外にも多くの決済アプリが展開されており、すでに広く浸透しつつあるスマホ決済サービスですが、そもそもスマホ決済サービスとはどういったものなのかを、まず説明していきたいと思います。

スマホ決済サービスとは、財布やクレジットカードを持ち歩かなくてもスマホひとつで簡単に買い物やサービスの利用ができるという便利な支払い方法です。レジにスマホをかざしたり、アプリで QR コードを読み取ったりするだけで、ほんの数秒で決済が完了します。交通系 IC を登録しておけば電車やバスもスマホひとつで乗り降りできるため、IC カードを忘れたり紛失したりという心配もありません。

今や国内のほとんどの世代でスマホが普及しているため、スマホ決済サービスは手軽で便利なメリットが多い支払い方法として人気を集めています。

スマホ決済サービスを成り立たせるためには、利用者側と店舗側の両方が、決済事業者が提供するスマホ決済サービスに対応している必要があります。利用者側と店舗側、それと決済事業者のやり取りを図にすると次のようになります。




**【図 2】スマホ決済の仕組み**

スマホ決済サービスには、大きく分けると 2 種類の決済方式があります。

■非接触型 IC 決済

スマホを専用端末にかざすだけで決済が完了するという方式です。スマホに搭載された無線通信系の技術を使って、スマホに登録されたクレジットカードや電子マネーから支払いを行います。

無線系通信の技術には NFC や Felica、Bluetooth などが使われます。その中でも Felica は日本で広く普及しており、交通系 IC カードや電子マネーカードに採用されています。スマホにモバイル Felica が搭載されていれば、スマホをカードリーダ―にかざすだけで決済が完了します。

■QR コード決済

画面に表示される QR コードを読み取ることで決済が完了する方式です。

QR コード決済には 2 つのパターンがあります。ひとつは、店舗側が掲示した QR コードを利用者側がスマホの専用アプリで読み取る「ユーザースキャン方式」。もうひとつは、利用者側がスマホの専用アプリで QR コードやバーコードを表示させて店舗側の POS 端末で読み取る「ストアスキャン方式」です。どちらの方式でも、最終的にはクレジットカードやチャージした電子マネーを利用して決済を行います。

QR コード決済は、QR コードを読み取れるスマホやタブレットさえあれば対応できるため、店舗側にとっては初期費用を抑えられるというメリットがあります。また、ユーザースキャン方式であれば、店舗側の手間が少なく、現金を扱わなくても済むため、店主が一人で切り盛りするような小規模な飲食店や屋台などとも相性の良い決済方法です。

## 3. スマホ決済サービスのセキュリティ面におけるメリットとデメリット

### 3.1 スマホ決済サービスのセキュリティ面におけるメリット

スマホ決済サービスについて、その他のキャッシュレス決済と比較した場合のセキュリティ面におけるメリットを紹介します。

■盗難のリスクがない

クレジットカードを盗難された場合、不正利用されてしまう可能性があります。しかし、スマホを盗難された場合は、スマホのロック機能やアプリの認証機能によってロックされている場合が多いため、不正利用されるリスクはクレジットカードを盗難された場合よりも低いと言えるでしょう。

■スキミングのリスクがない

スキミングとは、クレジットカードやキャッシュカードなどの磁気情報を読み取ることで情報を盗む手法です。スマホ決済サービス、特に QR コード決済では、QR コードを読み取るだけなのでスキミングのリスクはありません。

■一定時間でデータが無効となる

スマホに表示された QR コードは、一定時間が過ぎると無効になります。仮に何らかの原因で決済用の QR コードを盗難された場合でも数分後には使えなくなるため、安全性が高いといえるでしょう。

### 3.2 スマホ決済サービスのセキュリティ面におけるデメリット

便利でセキュリティ面のメリットも大きいスマホ決済ですが、デメリットもあります。スマホ決済サービスならではの注意すべき点を紹介していきます。

■偽造 QR コードのリスク

QR コードには決済に必要なさまざまな情報が含まれていますが、人間の目では含まれている情報を理解できません。そのため、不正な情報が含まれていたとしても対応しづらく、偽造 QR コードを読み取ってしまうリスクがあります。

偽造 QR コードを読み取ることで引き起こされる被害には、次のようなものが考えられます。

・偽造 QR コードによるスマホの乗っ取り

偽造 QR コードにはさまざまな情報を組み込むことができます。偽造 QR コードを読み取ることで不正なプログラムをダウンロードさせられてしまい、スマホの脆弱性を悪用され乗っ取られてしまうケースがあります。スマホを乗っ取られてしまうと、連絡先などの個人情報の漏洩につながるだけでなく、端末を悪用されて振り込め詐欺などのさまざまな犯罪に利用される可能性もあります。

・偽造 QR コードによる不正送金

第三者が本物の QR コードの上に偽造 QR コードのシールを貼り付けたり、本物の QR コードを少し書き換えたりすることで、支払いの際に正規の販売者ではなく、改ざんした第三者に代金が支払われてしまうケースがあります。こうなると、正規の販売者に代金が支払われなくなるだけでなく、犯罪グループに資金提供したことにもなり、非常に大きな問題です。

**【図 3】偽造 QR コードによる不正送金の手口**

■フィッシング詐欺による不正ログイン

フィッシング詐欺とは、インターネット上の正規のサービスになりすまして、悪意ある第三者が利用者からログイン情報などを盗む詐欺行為です。

フィッシング詐欺によってスマホ決済サービスの認証情報を盗まれてしまった場合、または、インターネット上の他のサービスで使っている ID とパスワードが漏洩してしまい、それがスマホ決済サービスで使用しているものと同じであった場合、不正ログインの被害に遭う可能性が高くなります。

さらに、クレジットカード情報が盗まれてしまった場合、そのクレジットカード情報は悪意ある第三者の手元のスマホの決済アプリに登録されてしまい、クレジットカードの本来の所有者のあずかり知らぬところで商品を購入されてしまいます。

■QR コードを無断利用されるリスク

店舗での QR コード決済時に肩越しに QR コードを撮影されてしまった場合、数分でその QR コードは無効になってしまいますが、その数分の間に不正利用されてしまう可能性もあるため、QR コード決済時には注意が必要です。

■アプリの脆弱性を悪用されるリスク

アプリに脆弱性が発見された場合、その脆弱性を解消したバージョンが公開され、利用者がアプリをアップデートすることで、悪意ある第三者に悪用される可能性は低くなります。しかし、そのアプリをインストールしたものの結局は使わずに放置してしまっていた場合、アップデートがなされず脆弱性が悪用される可能性が高くなってしまいます。

## 4. スマホ決済サービスのセキュリティ対策

スマホ決済サービスには不正利用されるリスクがあるということを紹介してきました。そこで、スマホ決済サービスの利用者はどのような対策ができるのかを紹介していきます。

■ログイン時は正規のサイトを利用する

フィッシング詐欺対策として、メールや SMS、広告などから誘導された Web サイトではなく、正規サイトからログインすることが推奨されます。

Web サイト上でアカウント情報やクレジットカード情報を求められた場合はすぐに入力してしまうのではなく、URL を確認するなどして正規のサイトであるかどうかを確認することが大切です。

■スマホ決済サービスの利用履歴などをこまめに確認する。

万が一、不正利用の被害に遭ってしまった場合にいち早く気付けるよう、スマホ決済サービスの利用履歴や連携している銀行口座、クレジットカードの明細を、できるだけ頻繁に確認することが大切です。

また、被害に遭った場合に速やかに対処できるよう、利用停止の手続き方法や利用しているサービスや金融機関の連絡先、被害についての相談先を事前に確認しておくことも大切です。

■セキュリティ対策がなされたサービスを利用する

サービスを利用する前にアプリのセキュリティ対策の有無を確認し、ログイン手順にワンタイムパスワードなどの多要素認証を採用しているアプリを利用することが推奨されます。

ワンタイムパスワードの他にも、アプリのセキュリティ対策として次のようなものが挙げられます。

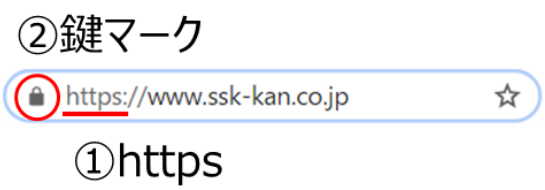
・SSL による暗号化通信

SSL とは、送受信しているデータを暗号化する通信手順です。インターネット上の通信を暗号化することで、悪意ある第三者からの盗聴やデータの改ざんを防ぐことができます。

実際に SSL が適用されているかどうかは、以下の二つの方法で簡単に確認することができます。

①Web サイトの URL アドレスが、https から始まっている。

②ブラウザの URL アドレス入力欄の脇に、鍵のマークが表示されている。




**【図 4】SSL が適用された URL アドレスの例**

・クレジットカードの本人認証サービス「3D セキュア」

3D セキュアとは、クレジットカード会社が推奨する本人認証サービスです。従来のインターネット上でのクレジットカード決済は、クレジットカードに記載されている「クレジットカード番号」や「有効期限」、「セキュリティコード」などの情報のみで行うことができました。しかし、3D セキュアを利用した場合、クレジットカードに記載されている情報に加え、事前に登録しておいた「自分しか知らないパスワード」を認証の際に要求されます。そのため、万が一クレジットカード情報が盗まれてしまった場合でも「なりすまし」などの不正利用を未然に防ぐことができます。

3D セキュアを利用するには、3D セキュアに対応したクレジットカードを利用し、事前にカード発行会社にパスワードを登録しておく必要があります。また、スマホ決済アプリも 3D セキュアに対応している必要があるので、そちらもスマホ決済サービスを利用する前に確認しておく必要があります。

## 5. 参考情報

・日本クレジット協会

日本のクレジット統計

https://www.j-credit.or.jp/information/statistics/download/toukei_03_h_2019_180619.pdf

・日本銀行

決済動向

https://www.boj.or.jp/statistics/set/kess/release/index.htm/

・IPA 情報処理推進機構

情報セキュリティ 10 大脅威 2020

https://www.ipa.go.jp/security/vuln/10threats2020.html

・三井住友カード株式会社

QR コード決済とバーコード決済のしくみとメリットについて

https://www.smbc-card.com/cashless/kojin/contrast_qrcode_barcode.jsp

・PayPay 株式会社

【完全網羅】スマホ決済の仕組みと種類別メリット・デメリットを徹底解説

https://paypay.ne.jp/store-media/sppay/0024_spp_works/

・トレンドマイクロ株式会社

スマホ決済を安全に利用するために確認したい 7 つのポイント

https://www.is702.jp/special/3533/

## 6. e-Gate の監視サービスについて

今回は主に利用者の方向けのセキュリティ対策についてご紹介させていただきましたが、サービス提供者側のセキュリティ対策も肝要です。安定したサービスの運用には、不正な通信を検知するためのセキュリティ対策の導入と、そのログの監視が重要です。e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。“e-Gate“のセキュリティ監視サービスをご活用頂きますと、迅速なセキュリティインシデント対応が可能となります。

また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、診断の結果、検出されたリスクへの対策をご提案させていただいております。

監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。

■総合セキュリティサービス「e-Gate」 e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた IT 運用のノウハウと最新のメソッドで構築した次世代 SOC“e-Gate センター“。この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”サービスです。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。リンク先のコンテンツは予告なく、変更、削除される場合があります。

※掲載した会社名、システム名、製品名は一般に各社の登録商標 または商標です。

**«お問合せ先»**

サービス＆セキュリティ株式会社

〒150-0011

東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F

TEL 03-3499-2077

FAX 03-5464-9977

sales@ssk-kan.co.jp