QRコード決済サービスのセキュリティ

QRコード決済が盛り上がりを見せており、様々なサービスやアプリケーションがリリースされ利用促進の気運が高まっている。一方で、不正決済などのセキュリティ事故を背景に不安を抱く利用者も多く、正しくセキュリティが実装された安全な決済サービスが求められている。

多様なQRコード決済サービスの登場

「キャッシュレス」の利用促進が求められる中、クレジットカードや非接触ICカード・スマートフォン決済[1)]に加え、新しい決済の手段として「QRコード決済」と言われる決済手段が盛り上がりを見せている。多種多様なサービスやアプリケーションが提供されているが、提供している事業者は、決済を本業とする金融事業者（銀行・カード会社等）だけでなく、通信会社やプラットフォーマーのようなIT企業、または流通系のサービス会社など、様々な企業・業種からの参入があり、新興企業も目立つ。

また、一言にQRコード決済と言っても、顧客提示型（CPM）[2)]・店舗提示型（MPM）[3)]といったQRコードの提示の仕方が異なるサービスも混在している。

これらのサービスやアプリケーションは、提供されるサービスや実装されている機能も千差万別であり、また登録が必要な個人情報の種類や本人確認の手段も様々で、セキュリティの強度も一様ではない。

QRコード決済サービスに潜むセキュリティリスク

QRコード決済サービスを利用する上でのセキュリティリスクとは何か。端的に言えば不正に決済が行われてしまうリスクだが、攻撃者に不正に利益を与えてしまう様々な事象を含む。例えば、決済履歴や決済金額の改ざん、決済をせずに商品を入手する、キャンペーンポイントを不正に大量取得する、他人の資金（サービス内にチャージされた金額等）を不正に利用するなど、多様な攻撃が発生している。

では、こういった事象に陥ってしまうリスクはどこに潜んでいるのか。CPMとMPM（静的／動的）それぞれで内在するリスクは異なるが以下に幾つか紹介する。

①「QRコード」自体に潜むリスク

QRコードは、誤り補正機能[4)]や高速読み取り、大容量など機能性を重視して開発された。また、スマートフォンのカメラさえあれば、誰でも簡単に読み取ることができたり、QRコードを作成できることなど汎用性や利便性の高さが特徴の技術である。

しかし、これを「決済」というセキュリティの担保が必要な用途で使用する場合には、利便性や汎用性の高さが、攻撃者が簡単に他人のQRコードを複製できる、改ざんできる、窃取できるといった、他人になりすまして決済を行うことが可能となるリスクにつながる。

実際に、QRコードを表示してレジ待ちをしている間に後ろからQRコードを盗まれて不正に決済される（CPM）、店舗に設置したQRコードを攻撃者が作成したQRコードに貼り替えて店舗の売上が横取りされる（静的MPM）、といった事例が発生している。

②サービス仕様やアプリ機能に潜むリスク

最近のQR決済サービスやアプリケーションは、決済機能単独のアプリケーションではなく、ポイントアプリや取引履歴管理アプリ、ショッピングアプリ等の、既に提供済みのサービスアプリケーションに後から決済機能を追加実装した形で提供されるものが多い。

こういった場合、決済サービスとそれ以外のサービスとのアカウント連携やデータ連携など、実装される機能が増え、全体の考慮がなされずにセキュリティリスクが埋め込まれてしまうケースがある。

NOTE

1) 交通系ICカードや電子マネーカード、おサイフケータイなど、NFC (Near Field Communication) 技術を使用した決済方法を指す。
2) 顧客のスマートフォンに表示されたQRコードを、店舗の端末で読み取り決済を行う方式。QRコード決済と言いつつ、現状ではQRコードを読み取るための端末が未導入の店舗も多く、従来型のバーコードを利用したバーコード決済も未だ多く採用されている。
3) 店舗が提示するQRコードを顧客のスマートフォンのカメラで読み取り決済を行う方式。MPM方式には、印刷済みの固定QRコードを読み取る方式 (静的MPM) と、タブレット等の端末を使用して決済ごとに動的に変更されるQRコードを読み取る方式 (動的MPM) の二種類ある。
静的MPM方式は、店舗に新たな端末の設置が不要で手軽に導入できるメリットがある一方、提示するQRコードの管理に注意が必要であったり、店舗売上 (POSレジ) との連動が決済と同時にできないなど、運用に注意すべき点がある。
4) コードの一部が汚れたり欠損した場合でも、コード中に格納されたデータを補正・復元する機能を有している。
5) 統一コード (JPQR) 利用者向けのガイドラインとなってはいるものの、統一コードを利用しない事業者についても参照することが推奨されている。

また、攻撃が成立すれば多額の利益が生まれやすい決済という機能が組み合わされることで、今までは問題になっていなかった既存サービスに内在するリスクが顕在化する場合もある。

実装すべきセキュリティ対策の例

様々なQRコード決済サービスやアプリケーションが存在するが、サービスやアプリケーションごとに提供される機能や実装方式は千差万別であり、何処にどの様に対策を実装すればいいのか、どのような種類の対策が必須なのか、絶対の正解はない。

また、キャッシュレス推進協議会が公開するガイドライン[5]でもセキュリティについて言及されているが、具体的な対策や実装方式は各事業者に委ねられている。

以下に、先に挙げたリスクへの対策例を幾つか紹介するが、これを闇雲に実装すればよいというのではなく、事業者は自社のサービス仕様をふまえた上で、必要な箇所に適切に対策を適用する必要がある。

①QRコードへのリスク対策

QRコードを「決済」で安全に利用するために考慮すべき対策として次のような例が挙げられる。具体的な実装方式については様々な方法があり、またこれらの他にも検討するべき対策は存在する。

- QRコードに格納されるデータ（決済情報）を、他人が簡単に読み取りや推測などをできないようにすることで攻撃者による複製・複写を防止する。
- ワンタイム化や、有効期限の設定など、攻撃者が再利用して簡単に使えないようにする。

②サービス仕様に沿ったセキュリティ機能の実装

サービス仕様の中にセキュリティリスクを内在させないためには、次のような対応が必要である。

第1に、連携機能を含めたサービス全体のフローに沿って攻撃リスクシナリオをベースに評価しておく必要がある。

例えば、店頭で利用するQRコード決済と、ECサイトでのネット決済では、リスクも必要なセキュリティ対策も異なる。両者のサービスを連携する場合、それぞれの違いの狭間にリスクがないか、連携したことで新たなセキュリティホールができていないかを確認する必要がある。

第2に、サービス仕様を検討する際には、サービス仕様のリスク分析と同時に必要なセキュリティ対策についてもあわせて検討することが求められる。

例えば、魅力あるキャンペーンやポイント還元を企画した場合に、攻撃者がどのように狙ってくるのか。こうした新機能の追加で既存のサービスに内在するリスクの顕在化についての分析とその防止策である。

セキュリティ対策の確認というと、技術的な実装にばかり目がいきがちだが、提供するサービス仕様が前提となっていることを踏まえたリスク分析は欠かせない。

利用者に安心してQR決済サービスを使ってもらうために、確実で堅牢なセキュリティ対策を実装するには、リスク分析とシミュレーション評価が必須である。

Writer's Profile

関口 八千代 Yachiyo Sekiguchi
NRIセキュアテクノロジーズ
上級セキュリティコンサルタント
専門は決済セキュリティ
focus@nri.co.jp