QRコードを開く前に安全かどうか確認する方法（クイッシングガイド）

クイッシングとはQRコードを使ったフィッシング詐欺です。スキャン前の危険サインと、スキャン後に開く前に確認すべきことを解説します。

著者: Lubor Šimůnek • 公開日: August 23, 2026 • セキュリティ

オンライン版: https://appstoryo.com/ja/blog/qr-code-safe-quishing-guide



クイッシングとは何か

クイッシングは、QRコードを悪用したフィッシング詐欺です。攻撃者が作成したQRコードをスキャンすると、認証情報を盗む、マルウェアをインストールする、または偽の支払いページを表示する悪意あるサイトに誘導されます。『QR』と『phishing（フィッシング）』を組み合わせた造語で、人々がQRコードをほとんど疑わずに信頼するために急速に広まっています。

QRコードが特有のリスクを持つ理由

通常のリンクであれば、クリックする前にカーソルを合わせてURLを確認できます。しかしQRコードは、スキャナーが解読するまで宛先を見ることができません。多くのカメラアプリはアドレスを表示せずに即座にブラウザを開くため、悪意あるサイトがデバイスの追跡を開始するのに十分な時間が生まれます。

QRコードはスパムフィルターも完全にすり抜けます。フィルターは不審なテキストや既知の悪意あるURLを探しますが、QRコードの画像は完全に無害に見えます。そのため、フィッシングメールは特に企業を標的とした攻撃でハイパーリンクをQRコードに置き換えるケースが増えています。

現実世界では、パーキングメーターの正規コードの上に貼られたステッカー、偽のレストランメニュー、郵便受けに投函された荷物配達詐欺の通知、『支払いにスキャン』を求める偽の公共充電ステーションなどで見られます。

スキャン前に確認すべき危険サイン

- 元のコードの上に貼られたステッカー。別のQRコードの上に貼られたQRステッカーは典型的な差し替えです。角をめくってみてください。剥がれるならスキャンしないでください。
- 見知らぬチラシの緊急性を煽る言葉。『今すぐスキャンして賞品を受け取る』や『荷物が保留中 — スキャンして再配達を申し込む』はプレッシャーをかける戦術です。
- 未要請のメールや手紙。銀行、配送会社、または政府機関からの予期しない連絡で、QRコードが主な行動を促す要素になっているものは強い警告サインです。

スキャン後、開く前に確認すること

- ドメインは期待通りですか？ 銀行でQRコードをスキャンした場合、URLは公式ドメイン上にあるべきです。
- URLショートナーが使われていませんか？ bit.lyやtinyurl.comなどのサービスは本当の宛先を隠します。URLエキスパンダーサービスを使って実際のアドレスを確認してから訪問してください。
- スペルミスや似せたドメイン。paypa1.com（Lの代わりに数字の1）やg00gle.com（Oの代わりに数字の0）に注意してください。
- 不審なサブドメイン。login.secure.amazon-delivery-jp.comは正当に見えますが、実際のドメインはamazon-delivery-jp.comであり、amazon.comではありません。

QR Code Reader Without Adsの効果

QR Code Reader Without Adsは何かを開く前に完全なURLプレビューを表示するため、リンクを確認して判断する時間を与えてくれます。URLが怪しいと思ったら、単純に『開く』をタップしなければよいだけです。アプリはデバイス上にローカルのスキャン履歴を保持し、データを収集せず、広告も表示しません。App Storeまたは Google Playで『QR Code Reader Without Ads』と検索してください。

QR Code Reader Without AdsはiOS版・Android版とも無料でダウンロードできます。広告なし、トラッキングなし、完全オフラインで動作します。

引用形式: Lubor Šimůnek (2026). *QRコードを開く前に安全かどうか確認する方法（クイッシングガイド）*. AppStoryo, lapnito.cz s.r.o.. https://appstoryo.com/ja/blog/qr-code-safe-quishing-guide
© 2026 lapnito.cz s.r.o.