LED ディスプレイを用いた重ね合わせ QR コード攻撃

鈴木敬太[†1]　福地健太郎[†1]

概要：Quick Response（QR）コードは，スマートフォンで容易に情報を読み取れるため広く普及しているが，利用者が目視で改竄を検出することは困難である．特に，同一の QR コードから異なる情報が読み取れるように改竄された場合，その発見が遅れることによるセキュリティリスクが指摘されている．本研究では，先行研究において提案した重ね合わせ QR コード攻撃手法を LED ディスプレイに適用した．これにより，複数モジュールの改変が可能になり，改竄前の QR コードに対する制限がなくなり，攻撃の自由度を向上させられることが判明した．

1. はじめに

二次元コードの一種である QR コードは，スマートフォンの普及に伴って広く普及し，様々な応用がなされている．QR コードは白と黒のドット（モジュール）のみで構造されており，スマートフォン搭載のカメラで高速に読み取ることができる．また，エラー訂正に優れており，多少の汚損があっても正しいデータを復元して読み取ることができる．これらの理由から，Web サイトへのアクセス，入場券，決済サービスなど様々な用途で使用されている．

しかし，QR コードの普及に伴って，コードの改竄による悪性情報の埋め込みが問題となっている．例えば悪性サイトの URL を埋め込んだ QR コードを，正規の QR コードの上から貼り付けることで利用者を誘導する手口が確認されている[1]．このような攻撃は Quishing[2]あるいは QRishing[3]と呼ばれ，その危険性が様々な調査により指摘されており，現実の悪用事例も増加傾向にある．

QR コードが攻撃の標的にされやすい理由の一つはその構造にある．QR コードは乱雑に白黒のモジュールが並んでいるように見えるため，そこにどのようなデータが埋め込まれているかを目で見て判断することは難しい．ゆえに，データの一部もしくは全体が改竄されていたとしても，それを目視で判別することは困難である．そのため，その対策としては，掲示されている QR コードが改竄されていないかを，設置者が QR コードリーダーを用いて定期的に読み取り，確認することが必要となる．

しかし，そうした対策に対しては，正規データと悪性データの両方が確率的に読み取られるようなコードを用いることでこれを突破する手法が提案されている[4][5][6]．このような対策をすることで，攻撃への対策が遅れ，被害の拡大をもたらす可能性が懸念されている．

一方で，これらの既存手法は注意深く見ると偽装が分かる場合がある．そこで我々はこれまでに，改竄を目視で発見することが困難な手法を開発した[7]．これは 120Hz 以上の高リフレッシュレート液晶ディスプレイを用い，複数の QR コードを高速に切り替えて表示するものである．人間の目にはそれらのコードが融合した像としてしか認識できず，正常な QR コードのように見えるが，QR コードリーダーはそれらのコードを別々に認識する．これにより，正規のコードと悪性コードとを切り替え表示することで，確率的に悪性情報を読み取らせることが可能となる．

図 1　提案手法の概要図

この手法は，既存手法と比較して明確に異常な箇所を目視で見付けることはできない特徴を持つ．しかし予備実験において，点滅モジュールが視認されやすくなる 2 種類の現象が確認された．

一つ目は，視線を高速に動かした場合に，各モジュールの境界線が目立って見える現象である．これは眼球が動いていると点滅する同一のモジュールがずれた状態で網膜に投影され，そのずれが視認されることによって引き起こされていると考えられる．

二つ目は，隣接するモジュールが点滅している際に，それらの境界線が視認される現象である．特に，点滅位相が異なるモジュールが隣接しているとき，つまり白から黒へと点滅しているモジュールと，黒から白へと点滅しているモジュールが隣接しているときは，特に強くその輪郭が確認された．これらの制約から，理論的には複数モジュールを同時に改変した QR コードを表示することが可能であったが，前回行った評価実験においては改変箇所を 1 モジュールに抑えた QR コードを使用した．

評価実験の結果，正規コードからの改竄量の少ない悪性データであれば，見破られる割合は 20%程度に抑えられることが分かった．また，白と黒の出現比率，すなわちデューティ比を変更することによって悪性データを読み取らせる確率を制御できることが確認された．しかし，視認性の

†1 明治大学

課題により攻撃対象となる QR コードが絞られるという課題が残されていた．

本研究では，同手法を LED ディスプレイに適用することで，この解決を図った．近年，LED は高輝度化と低価格化が進み，公共空間におけるデジタルサイネージ等での普及が進んでいる．こうした場所では QR コードによる Web サイトへの誘導がよく行われている．

LED ディスプレイは LCD と比較して応答性能が高いため，本手法による改竄に向く．また高輝度であるため，読み取り側のカメラのシャッタースピードが一般的な室内環境よりも速い値に設定されやすいと予想される．そのため，悪性データの読み取り率の制御をより確実に行える可能性が高いと考えられる．

そこで本研究では LED ディスプレイを用い，攻撃成功率の評価およびデューティ比変更による制御性を検証した．評価実験の結果，同手法は LED ディスプレイにおいても適用可能であることが確認された．さらに，LCD での表示において課題となっていた隣接モジュールに関する制約は LED ディスプレイでは発生せず，同時に改変可能なモジュール数を増やすことにも成功した．これらの結果より，本攻撃手法を LED ディスプレイに適用することで攻撃機会の拡大の懸念があることが示された．

2. 背景

2.1 QR コードを使用した攻撃の現状

近年，QR コードは Web サイトへの誘導のみならず，入場券や決済サービスなど様々な用途で用いられており，攻撃者にとっても新たな攻撃機会が生まれている．1 章で紹介した Quishing 攻撃は年々増加傾向にあることが報告されている[8]．中には，スキャンされた QR コード全体の 2%が悪質な QR コードであるという調査報告も上げられている[9].

主な手口としては，提示されている正規の QR コードの上から偽装 QR コードを貼り付ける手法があり，ポスターや電子決済用の掲示，パーキングメーターなどが攻撃の対象になっている[10][11][12].

Quishing に対する防衛策としては，出所の不明なコードはスキャンしない，URL プレビュー機能の付いた，信頼できる QR コードリーダーを使用するなどがよく挙げられる.

2.2 QR コード偽装の既存手法

正規の QR コードがあるべき場所に悪性 QR コードを提示し，ユーザーにそれを読み取らせる手法は主に以下のタイプがある．

第一の手法は，正規の QR コードの上から，それを覆い隠すように悪性 QR コードを貼り付けるものである．この手法は紙での提示が可能で，エネルギー消費なく悪性コードを表示し続けることができるが，正規 QR コードを読み取ることができなくなる．

第二の手法は，正規コードの一部分に悪性コードを貼り付けるものである[4]．この手法は QR コードの誤り訂正能力を利用し，正規コードが部分的に読めなくともデータを復元可能であることを利用している．こちらも紙での提示が可能で，エネルギー消費なく悪性コードを表示し続けることできる．正規コードを読み取ることが依然として可能であり，確率的に悪性データを読み取らせることができるが，知識のある者が注意深く見ることで見破ることができる．

第三の手法は，正規コードに対し，光を照射して悪性コードが読み取られるようにするものである[13][14]. 正規コード自体は紙でも提示可能だが，悪性コードを読み取らせるためにはエネルギー供給が必要である．この手法も確率的に悪性データを読み取らせることができるが，可視光源を用いている場合は，注意深く見ることで見破ることが可能である．しかし，赤外線を使った場合はこの限りではない．

第四の手法は，モジュールの一部を白と黒のどちらにも読み取れるような色あるいは形状にすることで，正規のデータと悪性データとの両方を確率的に読み取らせるものである[5][6]. 紙での提示が可能で，エネルギー消費なく正規・悪性の両データを表示し続けることができる．ただし，正規の QR コードに対しての改変が必要である．こちらも注意深く見ることで見破ることが可能だが，工夫によって見破り難さを増すことはできる．

先行研究で提案した我々の手法の特徴は，既存手法と比べると以下の特徴を持つ．理論的には正規コードと悪性コードの両方を確率的に読み取らせることが可能である．条件によっては，見破ることは困難であるが，紙での提示は不可能であり，高リフレッシュレートディスプレイでの表示が不可欠である．そのため，改変データをディスプレイに表示させる手段を攻撃者が持っていることが前提となる.

3. 提案手法

提案手法は高リフレッシュレートディスプレイを用い，複数の QR コードを高速に切り替えて表示することで，正規データと悪性データの両方が確率的に読み取られるコードを提示するものである．人間の目にはそれらのコードが融合した像としてしか認識できず，正常な QR コードのように見える．

なお以下では簡単のため，正規データと悪性データが 1 種類ずつあり，それらを交互に表示する場合について述べる．また，二つの QR コードは見た目の大きさおよび，QR コード仕様における「バージョン」，すなわちコードに含まれるモジュール数を既定する値が同じであることを前提とする．

提案手法の基本原理について説明する．2 種類の QR コードを高速に交互表示する場合，色が異なるモジュールは

白と黒とが交互に点滅することとなる．人間の視覚的特性として，高速に点滅する光は明暗が融合し，その中間の輝度の光として認識される．しかし，融合して知覚されるか否かは，その点滅の周波数に影響される．点滅ではなく融合した光として知覚される周波数の下限は「臨界フリッカー周波数」と呼ばれ，一般的に 50Hz 程度であることが報告されている[15].

一方, QR コードリーダー, 特にスマートフォン上に実装されたリーダーは，通常の写真・動画撮影に用いるのと同じカメラを使用している．専用の一次元バーコードリーダーはレーザーや LED 光源の光をバーコードに照射して読み取るが，広く使われている QR コードリーダーは独自の光源を持たず，写真撮影と同じ仕組みで QR コードを撮影し，その画像からデータを取得する．著者らが数台のスマートフォンを確認した限りにおいては，すべての QR コードリーダーが，シャッタースピード 1/60 秒以内の速度で撮影をしていた．なお，この速度はカメラの自動露出補正の働きにより，環境の明るさに応じて増減する．

この差があるため，白と黒の交互に点滅する同じ画素を観察しても, 人間の目には融合して見えるが, QR コードリーダーには撮影タイミングに応じて白色あるいは黒色がカメラに検出され，結果としてどちらかのコードが認識されることとなる．したがって，交互表示の速度は，50Hz 以上が望ましい．

4. 評価実験

本章では, 提案手法による攻撃が LED ディスプレイにおいても適用可能であるか，また，表示のデューティ比を変更することで悪性データを読み取らせる確率を制御可能であるかを検証するための評価実験について述べる．

4.1 実験環境及び予備的調整

実験に使用した環境を表 1 に示す.

表 1 実験環境

使用した QR コード	マイクロ QR コード
使用した LED の数	225 個
QR コードの大きさ	15×15cm^2
部屋の明るさ	0.5lx
カメラとディスプレイの距離	50cm

本実験では，LED 制御に M5Capsule を用い，WS2812B LED（256 個）を搭載した 16×16cm^2 の LED パネルを使用した．今回使用した LED ディスプレイは解像度が低く，一般的な QR コードを表示するための画素数が不足していたため，より少ないモジュール数で構成可能なマイクロ QR コードを表示対象とした．

予備実験を通じ, 今回採用した LED パネルにおいて安定した読み取りを実現するため，以下の 2 点のハードウェア的・ソフトウェア的処置を施した． 第一に, LED 素子間のピッチが広く，点光源が目立つためそのままでは読み取りが安定しなかった．そこで，LED ディスプレイから約 1cm 離した位置に半透明のアクリル板を設置した. これにより，LED の光がアクリル板で散乱・拡散し，モジュール間の暗部（隙間）が埋まることで, 読み取りの安定性が向上した．第二に，LED パネルのサイズ制約により，QR コードの規定にある周囲の余白（クワイエットゾーン）を点灯モジュール（白色）で形成することが困難であった．そのため，表示の白黒を反転させ, 黒色モジュール部分を発光（点灯）させることで，非点灯部分を背景と同化させ，実質的な余白を確保する措置をとった．これらの処置を施した表示例を図 2 に示す.

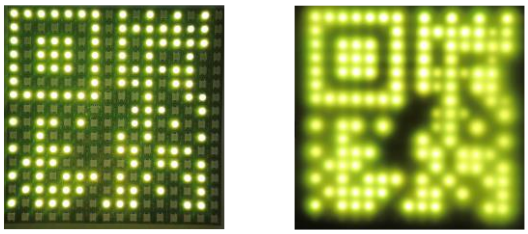

図 2 LED パネルでマイクロ QR コードを表示している様子．右図はアクリル板を載せて撮影したもの.

4.2 液晶ディスプレイ（LCD）における課題の解消

先行研究で LCD を用いた際に生じていた視覚的な不自然さに関する課題について，LED ディスプレイを用いた本環境で検証を行ったところ，以下の二点の改善が確認された.

一点目は，点滅するモジュールが隣接している際に，その境界線が視認されてしまう問題である. LCD ではこの現象を回避するために改変モジュールが隣接しないよう配置を工夫する必要があったが，LED を用いた本実験では境界線が視認されないことを著者らが目視で確認した．そのため，後述する実験は改変モジュールの隣接制約を考慮しないで行った.

二点目は，攻撃の偽装効果を高めるために，点滅モジュール以外の常時点灯モジュールの輝度を調整する必要があるという問題である．著者らが観察した限り，LED においては輝度調整を行わずとも点滅モジュールと常時点灯モジュールとの違いが視認できなかった．明確な原因は不明だが，LED の輝度特性によるものと思われる．今回の実験ではこれを受け，常時点灯モジュールの輝度調整は行わなかった.

これらの改善により，LED ディスプレイにおいては複数モジュールの改変がより柔軟に行えることが確認された．ただし，先行研究で明らかになった，カメラ側のローリングシャッター現象に起因する制約は依然として残るため，改変箇所は局所的である必要がある.

4.3 実験設定と手順

以上の条件を踏まえ，複数モジュールを改変したマイクロ QR コードを用いて評価実験を行った．実験には，図 3 に示すマイクロ QR コードを使用した. それぞれ「fukucha」および「fukuchi」というテキストデータが埋め込まれている．

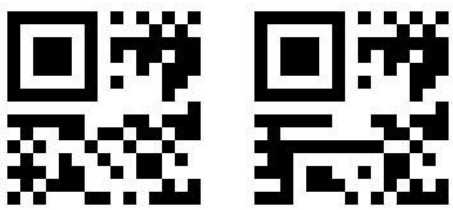

図 3　使用したマイクロ QR コード

実験における表示のデューティ比は，1:1 および 1:2 の 2 条件を設定した．1:2 条件では，「fukucha」を「fukuchi」の 2 倍の時間割合で表示するよう設定した．また，点滅の周波数は，前述した臨界フリッカー周波数を考慮し，60Hz を目標値とした．しかし，実験に使用した LED ディスプレイはリフレッシュレートの上限が約 126Hz であったため，以下の点滅周波数を設定した．デューティ比 1:1 の場合，120Hz での駆動が可能であるため，点滅周波数は 60Hz とした．デューティ比 1:2 の場合，本来であれば 180Hz の駆動が必要だがこれが不可能であるため，1:2 条件に関してはハードウェア限界である 126Hz で駆動させ実験を行った. そのため点滅周波数は 42Hz であった．

実験は，表示されたマイクロ QR コードをスマートフォン（iPhone13 Pro）上の QR コードリーダアプリ（クルクル）を用いて読み取ることで行った．スマートフォンはディスプレイから約 50cm 離した位置に設置し，実験者が任意のタイミングでアプリを立ち上げ，認識されたコードの内容を記録した．

4.4 実験結果と考察

実験結果を表 2 に示す.

表 2　実験結果

デューティ比	Fukucha	fukuchi
1:1	42	8
1:2	50	0

デューティ比 1:1 の条件では，読み取り回数に偏りはあるものの，確率的に双方の QR コードを読み取らせることができた．しかし，デューティ比 1:2 の条件では，出現比率が多いコードのみが読み取られ，少ないコードは一度も読み取られなかった．追加実験として，「fukuchi」の出現比率を「fukucha」の 2 倍にする逆の条件（2:1）でも実験を行ったが，結果は「fukuchi」のみが 50 回読み取られることとなり，同様の傾向を示した．

この原因として, 今回使用した LED パネルの書き換え速度の遅さが考えられる．LED の消灯・点灯の遷移に時間がかかるため，各フレームの表示時間を十分に確保できていない可能性が高い. 特に出現比率の低いコードにおいては，表示が完了した直後に次のフレームへの遷移が始まってしまい，QR コードとして完全な状態で表示されている期間が極端に短くなっていると推測される．実際，実験時 1:1 の条件では 1 回の読み取りに 5〜10 秒程度を要し，カメラがタイミングを捉え難くなっている様子が見られたが，1:2 の条件では 1〜2 秒と即座に読み取りが完了していた．

5. 議論

本実験の結果より，LED ディスプレイを用いた場合においても，提案手法を適用することで，正規データと悪性データを確率的に読み取らせることが可能であることが確認された．特筆すべき点は，LCD を用いた先行研究と比較して，LED ディスプレイでは複数モジュールの同時改変が可能になったことである．LCD の場合，隣接モジュールの境界線が見えてしまう等の制約から，攻撃対象となる QR コードは埋め草コード部に特殊な細工をしたものに限定されていた．しかし，本実験により LED ではその制約が解消されることが示された．これは，特定の構造を持つコードだけでなく，街中で一般的に利用されている標準的な QR コードに対しても本攻撃手法が適用可能であることを意味しており，攻撃機会の拡大の懸念があることが示された．

デューティ比の変更による読み取り確率の制御に関しては，本実験では期待通りの結果が得られなかった．この要因は, 実験に使用した LED ディスプレイの出力限界が約 126Hz であり，かつ応答速度が不足していたことにあると考えられる．しかし，現在街中のデジタルサイネージ等で使用されている商用の LED ディスプレイは, 本実験で使用した機材よりも高速な信号制御が可能であるものが多い．十分なリフレッシュレートと応答速度を持つディスプレイを使用すれば，フレーム間の干渉を防ぎ，設定したデューティ比に応じて正規・悪性コードの表示時間を正確に制御できると考えられる．したがって，高性能な機材を用いる実環境においては，攻撃者が意図した確率で利用者を誘導できる見込みは高い．また，LED の輝度制御は一般にパルス幅変調(PWM)で制御される. そのため LED ディスプレイのドライバレベルへの攻撃が可能な場合は，リフレッシュレートの低いディスプレイであっても攻撃が成立する可能性がある．あるいは，攻撃者が物理的に追加の LED をディスプレイに付加するといった攻撃手法も考えうる．

実環境での攻撃を想定した場合，環境光の影響も無視できない要素である．一般に，屋外などの高輝度環境下で撮影を行うと，カメラの自動露出機能によりシャッタースピードは屋内で撮影するよりも速くなる傾向がある．先行研究において，カメラのシャッタースピードが速いほど攻撃

成功率の制御性が向上することが明らかになっている．LED ディスプレイ自体が高輝度であることに加え，環境光によるシャッタースピードの高速化が相乗することで，実環境では本実験環境よりも攻撃成功率の制御性が高まると推測される．

最後に，読み取り確率の変動要因について述べる．どちらの QR コードが読み取られるかという確率は，デューティ比やシャッタースピードだけでなく，改変モジュールの空間的な配置，読み取りデバイスごとのセンサ性能，そして画像処理アルゴリズムにも左右されると考えられる．本実験では極端な結果となったケースも見られたが，これらの条件を詳細に分析し，最適化することで，デューティ比に近い読み取り結果が得られる可能性はある．今後は，多様なデバイスや環境条件下での挙動検証が課題となる．

6. 結論と今後の課題

本研究では，高リフレッシュレートディスプレイを用いた QR コードの偽装攻撃手法を LED ディスプレイに適用し，その有効性を検証した．評価実験の結果，LCD を用いた先行研究では困難であった複数モジュールの同時改変を行った場合においても，人間の目には正常なコードとして認識させつつ，スマートフォン上の QR コードリーダーに対しては正規データと悪性データの両方を確率的に読み取らせることが可能であることを確認した．これにより，本手法が特定の特殊な QR コードだけでなく，一般的に利用されている標準的な QR コードに対しても適用可能な，汎用性の高い攻撃手法であることが示された．

一方で，デューティ比の変更による読み取り確率の制御に関する検証においては，実験に使用した LED ディスプレイの出力限界および応答速度の制約により，意図した通りの比率で読み取らせることが困難であり，結果に偏りが生じる課題が確認された．しかし，現在街頭や公共空間で稼働している商用の LED ディスプレイは，本実験で使用した機材よりも高速な信号制御が可能である場合が多い．したがって，十分な性能を持つ機材を用いる実環境においては，攻撃者がデューティ比を操作することで攻撃の成功率を自在に制御できる可能性は高い．

今後の課題としては，より高いリフレッシュレートと応答速度を有する高性能な LED ディスプレイを用いた実証実験を行い，デューティ比による制御性を定量的に再評価することが挙げられる．また，有効な対策手段の調査・検討も必要であると考えられる．

参考文献

[1] Krombholz, K., Frühwirt, P., Kieseberg, P. et al.: QR Code Security: A Survey of Attacks and Challenges for Usable Security, Lecture Notes in Computer Science, Vol. 8233, pp. 79-90 (2014).
[2] Sharevski, F., Devine, A., Pieroni, E. et al.: Phishing with Malicious QR Codes, Proc. EuroUSEC '22, pp. 160–171, ACM (2022).
[3] Vidas, T., Owusu, E., Wang, S. et al.: QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks, Proc. FC 2013, Adams, A.A., Brenner, M., Smith, M. Vol. 7862 (2013). ページなし
[4] Dabrowski, A., Krombholz, K., Ullrich, J. et al.: QR Inception: Barcode-in-Barcode Attacks, Proc. SPSM '14, pp. 3-10, ACM (2014).
[5] 大熊浩也，瀧田愼，森井昌克：悪性サイトに誘導する QR コードの存在とそれを利用した偽造攻撃，電子情報通信学会技術研究報告, ICSS, Vol. 118, No. 109, pp. 33-38 (2018).
[6] 瀧田愼，大熊浩也，森井昌克：誤り訂正符号に基づく偽装 QR コードの構成法とその脅威，情報科学技術フォーラム講演論文集, Vol. 17, No. 4, pp. 1-6 (2018).
[7] 鈴木敬太，福地健太郎：高リフレッシュレートディスプレイを用いた重ね合わせ QR コード攻撃，研究報告セキュリティ心理学とトラスト（SPT）, No.69, pp. 1-8(2025).
[8] Morris, J.: QR code 'quishing' scams up 14-fold in five years, available from 〈https://www.bbc.com/news/articles/cq6yznmv3gzo〉 (accessed 2025-06-04).
[9] keepnet: 2025 QR Code Phishing Trends: In-Depth Analysis of Rising Quishing Statistics, available from 〈https://keepnetlabs.com/blog/2024-qr-code-phishing-trends-in-depth-analysis-of-rising-quishing-statistics〉 (accessed 2025-06-04).
[10] Zorz, Z.: Malicious QR codes pop up on traffic-heavy locations, available from 〈https://www.helpnetsecurity.com/2012/12/11/malicious-qr-codes-pop-up-on-traffic-heavy-locations/〉 (accessed 2025-06-04).
[11] エコノミスト編集部：QR 決済でカネをだまし取る「ステッカー型」詐欺とは，週刊エコノミスト・トップストーリー，入手先 〈https://mainichi.jp/premier/business/articles/20190924/biz/00m/020/018000c〉（参照 2025-06-04）.
[12] Barr, L.: FBI warns criminals are using fake QR codes to scam users, abc NEWS, available from 〈https://abcnews.go.com/Politics/fbi-warns-criminals-fake-qr-codes-scam-users/story?id=82371866〉 (accessed 2025-06-04).
[13] Zhou, A., Su, G., Zhu, S. et al.: Invisible QR Code Hijacking Using Smart LED, Proc. ACM Interact. Mob. Wearable Ubiquitous Technol., Vol. 3, ACM (2019).
[14] 鎌田悠希，川口宗也，大東俊博，高山佳久：不可視光レーザ照射を利用した動的偽装 QR コード，研究報告セキュリティ心理学とトラスト（SPT）, 2023-SPT-50, pp. 1-6 (2023).
[15] Jiang, Y., Zhou, K. and He, S.: Human visual cortex responds to invisible chromatic flicker, Nature Neuroscience, Vol. 10, pp. 657-662 (2007).