

QRコードの話

2023/11/17 勉強会 @salty_byte



話すこと

- QRコードとは
- 利用例
 - 現実
 - CTF
- ~~作り方~~
- ~~読み取り方~~
- まとめ

QRコードとは

- デンソーウェーブによって、1994年に開発された**2次元コード**
- QR: **Q**uick **R**esponseの略
- 高速読み取りを重視している
- 『QRコード』は、デンソーウェーブの登録商標（日本第4075066号）
- 規格:ISO/IEC 18004、JIS X 0510

https://webdesk.jsa.or.jp/books/W11M0090/?bunsyo_id=ISO/IEC%2018004:2015

2次元コードとは

- 縦と横の二方向に情報を持たせたコード
- 一方向のみの1次元コードに比べ、情報量が飛躍的に増加している

2次元コード: 例

- QRコード
- DataMatrix
- PDF417
- GS1合成シンボル



(90) 123456789012345678901234567890



(01) 0 0614141 99999 6



(余談) 1次元コード

- 一方向にだけ情報を持つコード
- 例: バーコード



↑NW-7

↓ITFコード



123 45678 90123 1

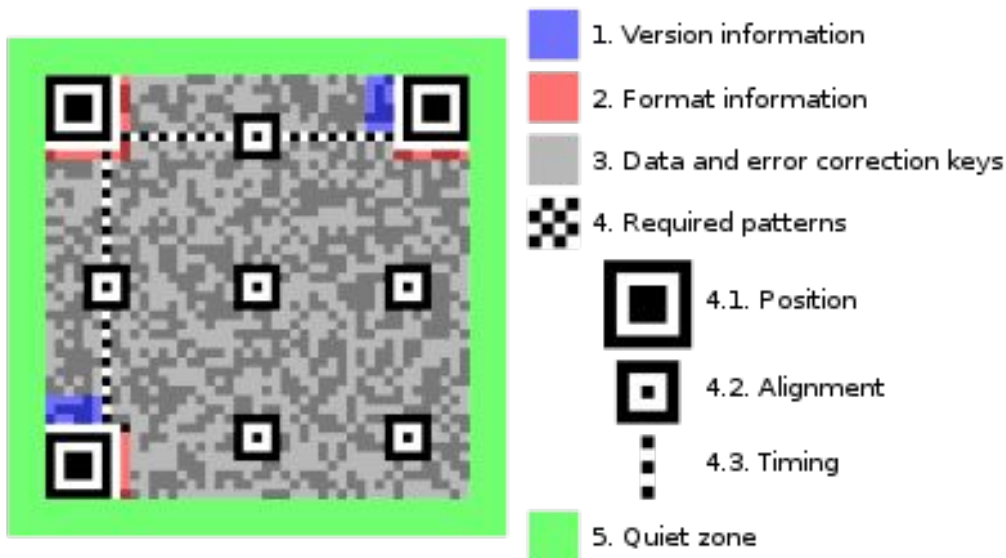


←JANコード

1 234567 890128

QRコード構成

- ファインダパターン(切り出しシンボル)
- アライメントパターン
- クワイエットゾーン
- タイミングパターン
- フォーマット情報
- データ部



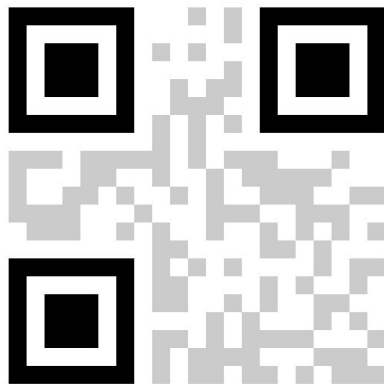
図引用: <https://ja.wikipedia.org/wiki/QRコード>

セル

- QRコードを構成する最小の単位(白黒の正方形)
- モジュールとも表される

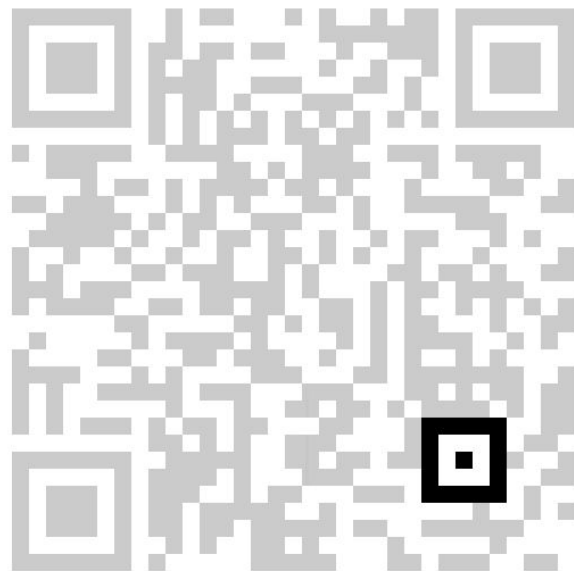
ファインダパターン(切り出しシンボル)

- 3つの四角
- 位置検出用に使われる



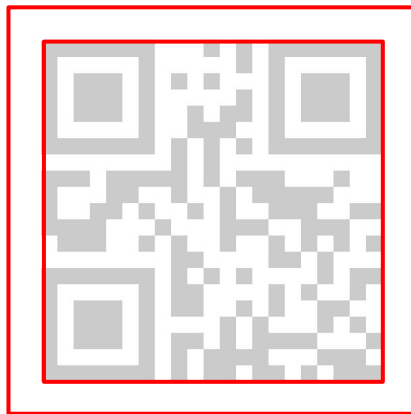
アライメントパターン

- 歪みによる位置ずれを補正する
- サイズが大きくなるモデル2に使われる



クワイエットゾーン

- シンボルの周りにある空白の部分
- 4セル分必要



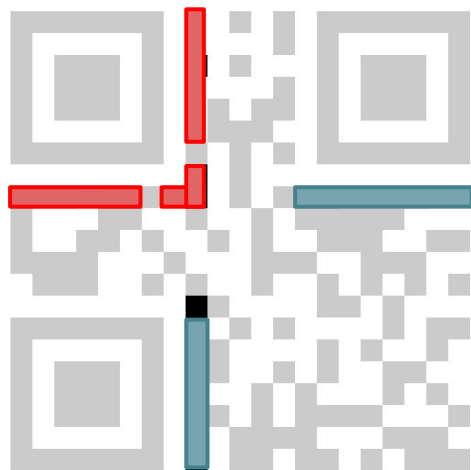
タイミングパターン

- 白セルと黒セルが交互に配置され、シンボル内のセル座標を決定する



フォーマット情報

- 誤り訂正レベルとマスクパターンに関する情報
- 30セル(15bit × 2)で表される



データ部

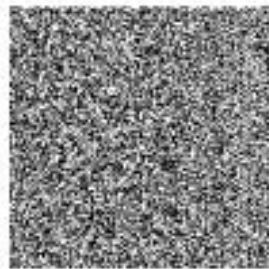
- 残りのセルにデータと誤り訂正符号を配置する

バージョン

- QRコードの中に組み込める情報(セル)の数
- バージョン1～バージョン40までである
- バージョンが1上がる毎に、横と縦のセルが2個増える(計4セル増加する)



バージョン1
(21×21)



バージョン40
(177×177)

仕様

最小シンボルサイズ	21セル× 21セル	
最大シンボルサイズ	177セル× 177セル	
最大データ量	数字	7,089字
	英数字	4,296字
	漢字	1,817字

https://www.keyence.co.jp/ss/products/autoid/codereader/basic2d_qr.jsp#sect_02

QRコード種類

- モデル1
 - バージョン1～14
- モデル2
 - モデル1にアライメントパターンを追加して拡張したもの
 - バージョン1～40



モデル1



モデル2

QRコード種類:派生例

- マイクロQR
 - ファインダパターンが一つ
- iQRコード
 - 横長にすることが可能で、従来のQRコードよりも多くの情報量を格納できる
 - <https://www.qrcode.com/codes/iqr.html>



マイクロQR



iQRコード

誤り訂正符号



- リードソロモン符号が使われる
- 誤り訂正レベルに応じてQRコードが損傷してもある程度は復元できる

誤り訂正レベル	損傷度合
L	7%
M	15%
Q	25%
H	30%
S※	50%

※Sは、iQRコードで利用可能。

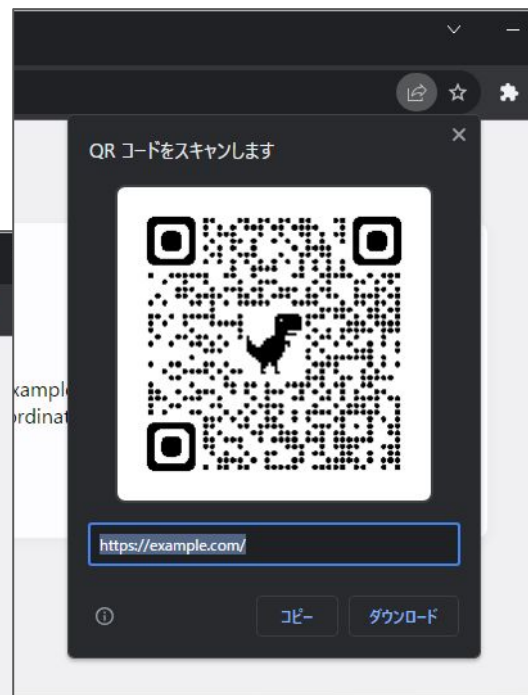
注意点

- 誤り訂正が強力なので、多少マスクした程度では復元ができる
- SNSとかでQRコードを含むスクリーンショットは上げない方がよい

利用例

利用例: 現実

- URLの共有



利用例: 現実

- Wi-Fi接続情報



ネットワーク名 (SSID): test

ネットワークパスワード: aaaa

ASPOSEサイトで生成

<https://products.aspose.app/barcode/ja/wifi-qr>

WIFI:S:<SSID>;T:<WEP|WPA|無記入>;P:<パスワード>;H:<true|false|無記入>;

利用例:現実

- 決済サービス



利用例：現実

- 電車ホームドアの開閉
 - tQRコード



https://www.denso-wave.com/ja/adcd/info/detail_191003_01.html
https://www.denso-wave.com/ja/adcd/info/detail_201118-01.html

利用例:CTF

- 以下のジャンルで出ることがある
 - ステガノグラフィー
 - フォレンジック
 - MISC
- 日本のCTFではそれなりに出題されていたっぽい
- ただし、最近はあまり見かけなくなった感
 - 同じような問題になるからだと推測

利用例:CTF

- ステガノグラフィー
 - 一枚の画像の中に埋め込まれるパターン
 - 簡単なものでは、RGBAとかをいじると出てくる
 - 普通はQRコードではなく、フラグが直でもらえるはず

利用例:CTF

- ステガノグラフィー
 - 複数の画像が集まった巨大な画像が渡され、特定の特徴のある画像のみを黒に塗りつぶすとQRコードが出てくる問題

利用例:CTF

- フォレンジック
 - 一部がかけているQRコードを復元するパターン
 - 例:フォーマット情報が欠けている



利用例:CTF

- フォレンジック
 - 一部がかけているQRコードを復元するパターン
 - 例:フォーマット情報が欠けている+データが並び替えられている



<https://github.com/project-sekai-ctf/sekaictf-2023/tree/main/misc/qr-god>

利用例:CTF

- フォレンジック
 - 一部がかけているQRコードを復元するパターン
 - 右端が残っているのでそこからデータを復元する



<https://eleclog.quitsq.com/2014/01/seccon-ctf-2013-online-forensics-400.html>

まとめ

まとめ

- デンソーウェーブによって開発された2次元コード
- QRコードは登録商標のため、利用の際は注意すること
- QRコードは身の回りのあらゆる場所で使われている
- 派生系もあるため、知識として構成を知っておくといいことあるかも？
 - CTFで出たら得かも

参考文献

株式会社キーエンス

よくわかる2次元コードの基本 VOL.1 [2次元コードの種類]

https://www.keyence.co.jp/ss/products/autoid/codereader/basic2d_qr.jsp

<https://www.denso-wave.com/ja/system/qr/fundamental/qrcode/qrc/index.html>

<https://ja.wikipedia.org/wiki/QRコード>

https://www.jpo.go.jp/news/koho/innovation/01_qrcode.html

付録

QRコード生成/読み取り: CyberChef

Download CyberChef [↓](#) Last build: 4 months ago - Version 10 is here! Read about the new features [here](#) Options [⚙️](#) About / Support [?](#)

Operations

QR

Parse QR Code

Generate QR Code

To Quoted Printable

From Quoted Printable

Chi Square

Frequency distribution

Expand alphabet range

From Base45

LS47 Decrypt

LS47 Encrypt

To Base45

Favourites [★](#)

Recipe [📁](#) [🗑️](#)

Generate QR Code [⏏️](#) [⏸️](#)

Image Format
PNG

Module size (px)
5

Margin (num modules)
4

Error correction
Medium

STEP **BAKE!** ☒ Auto Bake

Input [+](#) [📁](#) [🔄](#) [🗑️](#) [📱](#)

QRコード

Output [🗑️](#) [📁](#) [🔄](#) [📱](#)

悪用例

- QRコードフィッシング
 - 『Quishing』と言うとか言わないとか
 - 見ただけではURLの判別が不可
 - 実際にスキャンしてみないと分からない
 - 画像で送られてくるので、テキストベースのフィルタを回避する

<https://www.antiphishing.jp/report/monthly/202212.html>

悪用例

- 短縮URLによる問題
 - 最近話題になっている話
 - 短縮URLでQRコードを発行していた
 - 利用者がアクセスした際に、本来と違うサイトに送られる状態に

⇒ QRコード使うなら元々のURLで特に問題ないはず
パラメータが長いURLなら、そっちの方を何とかするべきな気がする

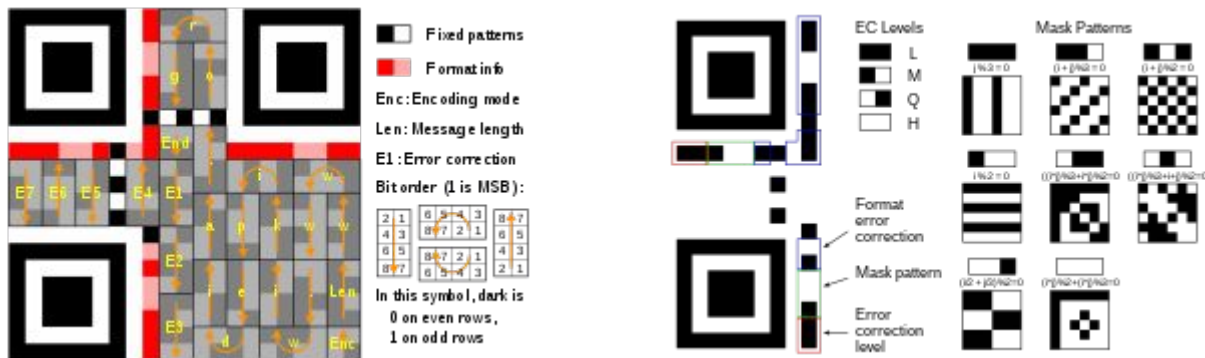
<https://piyolog.hatenadiary.jp/entry/2023/11/12/014635>

活用？例

- USBメモリ持ち出し禁止によるデータ転送の代用
 - PC内のデータを持ち出すためにQRコードにして転送する
 - Xでプログラムを公開している人がいたような気がする

作り方/読み方

- このサイトが分かりやすかったです
 - QRコードをつくってみる : <https://www.swetake.com/qrcode/qr1.html>



図引用: https://en.wikipedia.org/wiki/QR_code