[White Paper]

T-Engine Forum
Ubiquitous ID Center
Specification
DRAFT

930-S304/UID-00025-01.A0.10
2014-06-12

QR Code タグ ucode エンコード仕様
ucode Encoding Specification for QR Code Tag

Number: 930-S304/UID-00025-01.A0.10
Title: QR Code タグ ucode エンコード仕様
ucode Encoding Specification for QR Code Tag
Status: [X] Working Draft, [ ] Final Draft for Voting, [ ] Standard
Date: 2014/06/12

目次（Table of Contents）

更新履歴

バージョン	更新日	更新内容
00.00.01	2006.10.17	初版公開.
01.A0.00	2010.05.19	ucodeQR にキャッシュ情報などの付加情報を追加する方法を追記.
01.A0.10	2014.06.12	ucodeQR のゲートウェイアドレス形式に, Permanent URL 型と短縮型を追加.

QR Code タグ ucode エンコード仕様

ucode Encoding Specification for QR Code Tag

はじめに

規定範囲

本書では，QR Code 仕様の 2 次元バーコードに，ucode をエンコードして格納するためのデータ表現形式を規定する．あくまで QR Code のデータ表現形式を規定するものであり，電子署名のセキュリティ強度やシステムの運用方針については本書で規定しない．

本書の位置付け

本書で規定する内容は，

- QR Code タグに格納するデータを生成するアプリケーション
- QR Code タグにエンコードされた ucode を読み取るアプリケーション

において利用されることを想定している．

参照規定

[1] T-Engine フォーラム，ユビキタス ID センター，「uBNF: ユビキタス ID アーキテクチャ仕様のための BNF 記法」，910-S004/UID-00003, 2006.
[2] T-Engine フォーラム，ユビキタス ID センター，「ucode 解決ゲートウェイ」, 910-S204/UID-00007, 2006.
[3] RFC 2104「HMAC: Keyed-Hashing for Message Authentication」, 1997.
[4] RFC 4648「The Base16, Base32, and Base64 Data Encodings」, 2006.

用語定義

- QR Code

QR Code は，一般的に 2 次元バーコードと呼ばれる印刷型のタグの一種で，1994 年に㈱デンソーウェーブが開発した．現在，QR Code は仕様が公開され，㈱デンソーウェーブは QR Code に関する特許の権利行使を行わないことが宣言されている．1999 年 1 月に，日本工業規格 JIS X 0510 として制定され，2000 年 6 月に ISO の国際規格として制定された（ISO/IEC18004）．

- ucodeRP Gateway

ucode 解決ゲートウェイ仕様[1]を実装したサーバソフトウェア．http ベースのインタフェースにより，ucode 解決機能，署名検証機能をクライアントに提供することを目的としている．

1. ucode エンコード方式

本章では，QR Code 規格の 2 次元バーコードに，ucode を格納するためのエンコード方式を定める．エンコード方式として，以下の 4 種類を規定する．

- 標準形式
- ゲートウェイアドレス形式（Query Part 型）
- ゲートウェイアドレス形式（Permanent Link 型）
- ゲートウェイアドレス形式（短縮型）

1.1. 表記法

本章で用いる型の表記法について規定する．型表記法の一覧を表 1 に示す．ただし，HEXDIG，DIGIT，および VCHAR については，[1]の規定に従う．

表 1: 表記法一覧

```
ALPHADIG       = ALPHA | DIGIT | "-" | "_"
<ucode string> = 32HEXDIG※1  ; ex. 0EFFFEC000000000000000000050123
<ucode64 string>=22ALPHADIG  ; ex. Dv_-wAAAAAAAAAAAAAUBIw (base64url[4] encoding)
<sign string>  = 1*HEXDIG    ; ex. 6455FDB217CFE086953A844DABAC0491B05D91D2
<append string> = <key string> "=" <value string>
<key string>   = 1*ALPHADIG
<value string> = 1*VCHAR
<algo type> = <mac type> | "PBEWith" <mac type>
<mac type> = "HmacMD5"|"HmacSHA1"|"HmacSHA256"|"HmacSHA384"|"HmacSHA512"
※1 : n<element>は，ちょうど n 個の<element>が並ぶことを示す．
```

1.2. パラメタ

エンコードする際に指定可能なパラメタの一覧を表 2 に示す．

表 2: パラメター一覧

パラメタ名	値	意味
X-UIDC-UCODE	<ucode string>	ucode（16 進・キャラクタ表現）
X-UIDC-SIGNATURE	<sign string>	電子署名（16 進・キャラクタ表現）
X-UIDC-ALGORITHM	<algo type>	アルゴリズムの種別

<append string>とは ucodeQR 内に格納するキャッシュ情報や付加情

報である. <append string>はキー名とその値からなる.

1.3. 標準形式

標準形式は, カンマ区切りでパラメタを列挙するエンコード形式である.

```
<qr code string> = "X-UIDC-UCODE=" <ucode string> [","  "X-UIDC-SIGNATURE=" <sign string> [","  "X-UIDC-ALGORITHM=" <algo type> [<append values>]]]
<append values> = "," <append string> [<append values>]
```

図 1: 標準形式

1.4. ゲートウェイアドレス形式

ゲートウェイアドレス形式は, ucodeRP Gateway に対して, http リクエストを送信可能なエンコード形式である. この形式は, ucode を扱う専用アプリケーションがない場合に, Web ブラウザで直接オープンされることを想定したものである.

この形式には, Query Part 型, Permanent Link 型, 短縮型の 3 種類がある.

1.4.1. Query Part 型

Query Part 型は, URL の Query Part 部分に ucode を格納する形式である.

```
<qr code string> = "http://" <rhost> "/" <qpath> "?" <query part>
<rhost> = (署名検証機能付ゲートウェイのホスト名)
<qpath> = (署名検証機能付ゲートウェイソフトウェアのパス)
<query part> = "X-UIDC-UCODE=" <ucode string> ["&"  "X-UIDC-SIGNATURE=" <sign string> ["&"  "X-UIDC-ALGORITHM=" <algo type> [<append values>]]]
<append values> = "&" <append string> [<append values>]
```

図 2: ゲートウェイアドレス形式

1.4.2. Permanent Link 型

Permanent Link 型は, URL のパス部分に ucode を格納する形式である.

```
<qr code string> = "http://" <rhost> ["/" <qpath>] "/ucode/" <ucode string> [ "?"
<query part> ]
<rhost> = (署名検証機能付ゲートウェイのホスト名)
<qpath> = (署名検証機能付ゲートウェイソフトウェアのパス)
<query part> = "X-UIDC-SIGNATURE=" <sign string>   ["&" "X-UIDC-ALGORITHM=" <algo
type> [<append values>]]
<append values> = "&" <append string> [<append values>]
```

図 3: ゲートウェイアドレス形式(Query Part 型)

1.4.3. 短縮型

短縮型は, URL のパス部分に, ucode 値を RFC 4648[4]の「5. Base 64 Encoding with URL and Filename Safe Alphabet」の規定に従ってエンコードした文字列を格納する形式である. ただし, ucode の長さは 128bit 固定であるため, [4]の「3.2 Padding of Encoded Data」が規定するパディングは行わない.

```
<qr code string> = "http://" <rhost> ["/" <qpath>] "/u64/" <ucode64 string> [ "?"
<query part> ]
<rhost> = "(署名検証機能付ゲートウェイのホスト名)"
<qpath> = "(署名検証機能付ゲートウェイソフトウェアのパス)"
<query part> = "X-UIDC-SIGNATURE=" <sign string>   ["&" "X-UIDC-ALGORITHM=" <algo
type> [<append values>]]
<append values> = "&" <append string> [<append values>]
```

図 4: ゲートウェイアドレス形式(短縮型)

2. エンコード例

2.1. 標準形式の例

標準形式でエンコードした例を図 5 に示す.

X-UIDC-UCODE=0EFFFEC000000000000000000000050123,X-UIDC-SIGNATURE=6455FDB217CFE086953A844DABAC0491B05D91D2,X-UIDC-ALGORITHM=HmacSHA1

図 5: 標準形式によるエンコード例

2.2. ゲートウェイアドレス形式の例

ゲートウェイアドレス形式でエンコードした例を図 6, 図 7, 図 8 に示す.

http://rs.uidcenter.org/search?X-UIDC-UCODE=0EFFFEC000000000000000000050123&X-UIDC-SIGNATURE=6455FDB217CFE086953A844DABAC0491B05D91D2&X-UIDC-ALGORITHM=HmacSHA1

図 6: ゲートウェイアドレス形式(Query Part 型)によるエンコード例

http://rs.uidcenter.org/ucode/0EFFFEC000000000000000000005012 3&X-UIDC-SIGNATURE=6455FDB217CFE086953A844DABAC0491B05D91D2 &X-UIDC-ALGORITHM=HmacSHA1


図 7: ゲートウェイアドレス形式(Permanent Link 型)によるエンコード例

http://rs.uidcenter.org/u64/Dv_-w AAAAAAAAAAAAAUBIw	http://rs.uidcenter.org/u64/Dv_-wAAAAAAAAAAAAAAUBIw?X -UIDC-SIGNATURE=6455FDB217CFE086953A844DABAC0491B05D 91D2&X-UIDC-ALGORITHM=HmacSHA1
	

図 8: ゲートウェイアドレス形式(短縮型)によるエンコード例

3. 署名の計算方法

QR Code 規格の2次元バーコードで使用する署名は以下で定義される HMAC で計算する[3].

$$HMAC_K(ucode) = h((K \oplus opad), h((K \oplus ipad), ucode))$$

ここで，h はハッシュ関数であり，MD5，SHA-1，SHA-256，SHA-384，SHA-512 が使える[3]．K は秘密鍵で，ハッシュ関数のブロックサイズより短い場合は 0 でパディングを行なう．$ucode$ は署名の付与される ucode である．$\oplus$ はビットごとの排他的論理和で，$ipad$ ，$opad$ はそれぞれ 16 進数で 0x36，0x5c をブロック長サイズまで繰り返した数値である．カンマ (,) は連結を表す．

QR Code 規格の2次元バーコードに記録する署名は，上で計算した HMAC の値を 16 進数表記の文字列で表現したものである．