

# Nintendo Wi-Fi Connection

## 独自ゲームサーバ利用説明書

Ver 1.3

任天堂株式会社発行

このドキュメントの内容は、機密情報であるため、厳重な取り扱い、管理を行ってください。

## 目次

---

1	本文書について .....	4
1.1	内容 .....	4
2	利用方法 .....	4
2.1	任天堂認証サーバでの認証処理 .....	4
2.2	NATネゴシエーション処理 .....	4
2.3	GameSpyサーバを利用しつつ独自サーバも利用する場合 .....	5
2.4	GameSpyサーバを利用せず独自サーバのみ利用する場合 .....	6
2.5	独自サーバとの通信におけるセキュリティについて .....	6
2.6	サービス稼動状況の確認 .....	7
2.7	認証トークン仕様 .....	9
2.8	SSLサーバ証明書 .....	9
2.9	利用申請書 .....	10
2.10	ロットチェックに関する注意点 .....	11
2.11	サービス障害時の連絡先 .....	11
2.12	サービスの終了 .....	11

## 改訂履歴

版	改訂日	改訂内容
1.3	2009/02/19	「2.3 GameSpyサーバを利用しつつ独自サーバも利用する場合」で、Wi-Fi Connectionから切断されるまで有効という記述を削除 セーブデータ等に保存してはいけない旨を追記
1.2	2008/10/01	WMS への対応
1.1	2008/03/31	Wii への対応 独自サーバとの通信におけるセキュリティについて追記 認証トークン仕様の詳細化 SSL サーバ証明書に関する説明を追記
1.0	2006/09/11	初版

# 1 本文書について

## 1.1 内容

---

本文書は、Nintendo Wi-Fi Connection 対応ゲームソフトにおいて、任天堂・GameSpy が運営するゲームサーバとは異なる独自のゲームサーバを利用する際の、注意事項や開発する上で必要な情報等を扱っております。

# 2 利用方法

## 2.1 任天堂認証サーバでの認証処理

---

独自サーバを利用する場合でも、Nintendo Wi-Fi Connection 対応ゲームは、必ず最初に任天堂の認証サーバにて認証処理を行ってください。弊社が提供する DWC ライブラリを使えば、アクセスポイントの接続から認証処理までを一連の流れで行うことができます。

独自サーバを利用する場合、大きく分けて 2 通りの方法があります。1 つは任天堂認証サーバでの認証から GameSpy サーバへの接続までを一連の流れで行う方法、もう一つは GameSpy サーバに接続せず、任天堂認証サーバでの認証のみを行う方法です。

GameSpy サーバを利用する場合は DWC ライブラリを、利用しない場合は DWC-DL ライブラリを使用して開発を行ってください。

## 2.2 NAT ネゴシエーション処理

---

P2P 通信を行うゲームは、基本的に DWC ライブラリによるマッチメイク機能を利用してください。独自の NAT ネゴシエーションによるマッチメイク機能、例えば UPnP などを利用してしまうと、他の Nintendo Wi-Fi Connection 対応ゲームとの整合性が取れず、ユーザに混乱を与えてしまいます。

弊社は多数の無線 LAN アクセスポイントと GameSpy の NAT ネゴシエーション機能との相性を検証し、Nintendo Wi-Fi Connection ホームページにおいて、動作確認済み機種一覧を公開しています。ユーザサポートを円滑に行うためにも、この旨ご理解ください。

## 2.3 GameSpy サーバを利用しつつ独自サーバも利用する場合

DWC ライブラリを利用し、アクセスポイントへの接続～任天堂認証サーバでの認証～GameSpy サーバへの接続までを一連で行います。その後も DWC ライブラリを使い、任天堂サーバ・GameSpy サーバの機能を利用します。

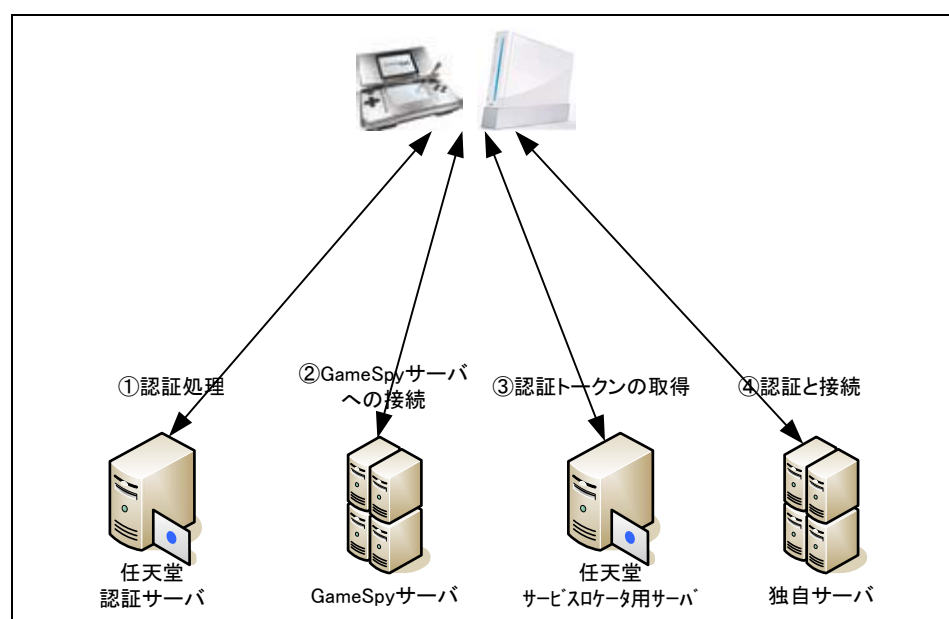
独自サーバに接続する前に、DWC ライブラリのサービスロケータ機能を使い、独自サーバ用認証トークンを取得してください。この認証トークンは、一度取得すれば 24 時間有効とします。ゲーム中では、最初に一度サービスロケータ機能にて認証トークンを取得すれば、有効時間内まで使い回すことができます。認証トークンをセーブデータ等に保存することは禁止です。サービスロケータ機能の詳細は、DWC の関数リファレンスマニュアルをご参照ください。また、認証トークンの詳細は後述の項をご参照ください。

取得した認証トークンを独自サーバに送信し、正常な値かどうかをサーバ側で確認してください。認証トークンの送信方法は規定しませんが、パケットの盗聴などによる認証トークンの不正利用を防ぐため、なるべく通信経路を暗号化してください。

サーバ側の認証トークン確認用プログラムに関しては、DWC (-DL) ライブラリパッケージに同梱する形で弊社からサンプルを提供しています。認証トークンには、Wi-Fi Connection ID・Wii 番号・本体の MAC アドレス・生成時間等が埋め込まれており、サーバ側でそれぞれの値を取得することができます。サーバ側でニンテンドーDS・Wii 本体を特定するための値としてもご利用いただけます。

同一サーバに対して何度も接続する場合は、最初の一度だけ認証トークンを確認し、その後は御社独自の認証方法・セッション管理方法をご利用ください。パフォーマンス上問題がなければ、毎回認証トークンを確認しても構いません。複数のサーバに対して接続する際も同様ですが、最初に接続されるサーバでは、必ず認証トークンを確認してください。

認証トークンを確認することで、確かに任天堂のサーバによる認証処理が行われた機器からの接続であることが確認できます。サーバ間認証のような制限は設けていませんので、この認証トークンを利用しなくても独自サーバへの接続は技術的には可能です。しかし独自サーバ自体のセキュリティを確保するため、必ず認証トークンをご利用ください。

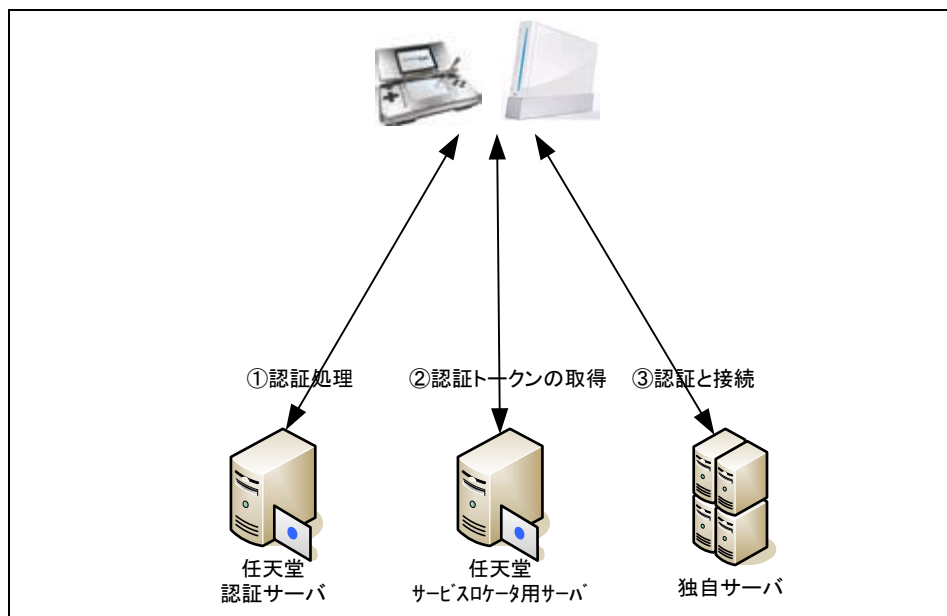


## 2.4 GameSpy サーバを利用せず独自サーバのみ利用する場合

DWC-DL ライブラリを利用し、アクセスポイントへの接続～任天堂認証サーバでの認証を一連で行います。

その後、DWC-DL ライブラリのサービスロケータ機能を使い、独自サーバ用認証トークンを取得してください。

以降の独自サーバとの接続は、「2.3 GameSpy を利用しつつ独自サーバも利用する場合」と同様です。



## 2.5 独自サーバとの通信におけるセキュリティについて

上記の認証トークンの仕組みをご利用いただくことで、認証サーバを経由したニンテンドーDS・Wii 以外からの接続を拒否することができるようになり、独自サーバ側のセキュリティをある程度確保することができます。

さらに、ニンテンドーDS・Wii 側のセキュリティも確保するために、通信パケットの改ざんや、御社の独自サーバに成り済ました偽装サーバとの通信を防ぐようにしてください。これを実現するには、独自サーバが発信するデータに電子署名（RSA 署名・HMAC 値など）を付加し、受信時にデータの完全性を確認する、もしくは独自サーバとの通信に HTTPS プロトコルを採用し、通信開始時にサーバ証明書の正当性を確認するなどの方法が有効です。

## 2.6 サービス稼働状況の確認

御社の独自サーバの稼働状況を、弊社からでも確認できる仕組みを実装してください。その仕組みは、ユーザサポートの切り分けのために利用します。ニンテンドーDS・Wii にサービスを提供しているサーバ自身、もしくはそのサービスの稼働状況を把握できるサーバ上で Web サーバを稼働させ、サービスの稼働状況をテキストデータで応答できる機能を実装し、その URL と応答内容を「Nintendo Wi-Fi Connection Workflow Management System」（以下 WMS）にて申請してください。

稼働状況の応答内容は、そのゲームのサービス全体が、稼働中・一部停止中・停止中のいずれであるかを把握できるようにしてください。各サーバ毎の稼働状況までは不要です。

一般ユーザからの接続を制限する場合は、接続元 IP アドレスによる制限を行ってください。弊社が利用する IP アドレス一覧は、WMS にてご確認ください。

提供いただいた URL へは、弊社のサーバが定期的にアクセスします。特に要望がない限り、5 分に一度、二ヶ所からアクセスしますので、あらかじめご了承ください。またこの仕組みは、HTTPS には対応しているものの、Basic 認証・Digest 認証には対応しておりません。御社の運用ポリシー上これらの認証設定が必須の場合は、その旨 WMS の「概要」に追記してください。

例1) ランキングサービスを冗長化した 2 台のサーバ (A, B) で運営している場合

稼働確認用 URL : <http://hoge.com/status> (URL はゲーム一つにつき一つだけ提供)

応答内容 : サービス稼働中 -> up、サービス一部停止中 -> warn、サービス停止中 -> down

A の状況	B の状況	応答内容
稼働	稼働	up
稼働	停止	up
停止	稼働	up
停止	停止	down

例2) ランキングサービス (A) とダウンロードサービス (B) を運営している場合で、どちらかが停止していてももう一方には影響が無い場合

稼働確認用 URL : <http://hoge.com/status> (URL はゲーム一つにつき一つだけ提供)

応答内容 : サービス稼働中 -> up、サービス一部停止中 -> warn、サービス停止中 -> down

A の状況	B の状況	応答内容
稼働	稼働	up
稼働	停止	warn
停止	稼働	warn
停止	停止	down

例3) 独自認証サービス (A) とランキングサービス (B) を運営している場合で、独自認証サービスが停止するとランキングサービスも利用できない場合

稼働確認用 URL : <http://hoge.com/status> (URL はゲーム一つに付き一つだけ提供)

応答内容 : サービス稼働中 -> up、サービス一部停止中 -> warn、サービス停止中 -> down

A の状況	B の状況	応答内容
稼働	稼働	up
稼働	停止	warn
停止	稼働	down
停止	停止	down



## 2.7 認証トークン仕様

---

認証トークンは、下記の項目等をゲーム毎に異なる鍵にて暗号化した値となります。

- Wi-Fi Connection ID の先頭 13 桁（ニンテンドーDS のみ）
- Wii 番号（Wii のみ）
- MAC アドレス（Wii の場合は無線 LAN インタフェース側）
- トークン生成日時
- ハッシュ値

独自サーバ側でこの認証トークンを復号化し、正当性を確認して認証を行います。複合化後の文字列について、フォーマットが正しいか、ハッシュ値が正しいか、トークン生成日時が 24 時間以内か、などを確認します。復号化・エラーチェック・各値の取り出し方法の詳細は、DWC(-DL)ライブラリパッケージに同梱されている認証トークン確認用プログラムのサンプルをご参照ください。このエラーチェックを正確に行うため、独自サーバのシステム時間は、NTP 等を利用して定期的に調整してください。

復号用の鍵（サービスロケータ開発用/製品用トークン）は、独自サーバ利用申請の承認が下り次第、WMS でお知らせします。

## 2.8 SSL サーバ証明書

---

独自サーバとの通信で SSL を利用される場合、そのサーバに設定する SSL サーバ証明書を、弊社の独自認証局にて発行することができます。発行を希望される場合は WMS にて申請し、CSR ファイルを弊社窓口までお渡しください。

弊社発行の SSL サーバ証明書には、次の特徴があります。

- サーバ証明書の有効期間を最大限に設定していますので、証明書の定期更新は不要です。
- 発行費用はいただきません。
- WiiConnect24 のダウンロードタスクで https を利用する場合は、弊社発行の証明書が必要です。  
※http の場合は不要です。詳しくは、WiiConnect24 プログラミングマニュアルをご参照ください。
- Opera や Internet Explorer、Firefox などのブラウザにはこの認証局は搭載されていないので、パソコンからも接続されるサーバには利用できません。

VeriSign、CyberTrust、RSA などの一般商用認証局や、御社独自の認証局を利用したとしても、WiiConnect24 のダウンロードタスク以外の通信では何ら問題ありません。ただし御社独自の認証局を利用される場合は、その管理に充分ご注意ください。

## 2.9 利用の申請

---

技術面での検証、ロットチェック、ユーザサポート部門への通知を目的として、利用する独自サーバについての情報を申請して頂きます。申請は「Nintendo Wi-Fi Connection Workflow Management System」(WMS)にて行ってください。

WMS での申請には下記の項目等が含まれます。

- 利用目的
- サーバのホスト名 or IP アドレス
- 利用プロトコル (ポート番号)
- 暗号化・署名利用の有無
- 平均通信データサイズ／最大サイズ
- SSL サーバ証明書の認証局
- Wi-Fi Connection 以外での同サーバの利用
- サーバの定期メンテナンス時間
- サーバ稼働確認 URL・確認方法
- サーバ障害時のゲームの挙動
- サーバ障害時の連絡先

## 2.10 ロットチェックに関する注意点

---

弊社でのロットチェックは、本番稼働用のサーバを利用して行います。マスター提出前にはサーバ環境を整え、ロットチェック期間中のメンテナンスは極力お控えください。もし都合により本番稼働用のサーバが利用できない場合は、マスター提出の際にお知らせください。

## 2.11 サービス障害時の連絡先

---

一定期間サービスを停止する予定がある場合、または予期しないサービス停止があった場合は弊社までご連絡ください。連絡先はWMSにてご確認ください。

## 2.12 サービスの終了

---

独自ゲームサーバを利用したサービスの提供を終了する場合は、弊社までお知らせください。認証サーバの登録情報を変更し、最初の認証処理において「サービス終了」メッセージを応答します。

© 2006–2009 Nintendo

任天堂株式会社の許諾を得ることなく、本文書に記載されている内容の一部あるいは全部を無断で複製・複写・転写・頒布・貸与することを禁じます。