シャチ不正チェックサーバ

Ver 0.9b

任天堂株式会社発行

目次

改訂履歴

版	改訂日	改　訂　内　容
0.8	2010/01/19	初版
0.9	2010/01/22	管理 UI について追記 公開鍵を変更 据え置き機の対応を考慮して、エンディアンをネットワークバイトオーダーで統一

1　本文書について

1.1　内容

本文書は、シャチでクライアントが送信してきたデータが正常なデータかを認証し、正常なデータであると確認できた場合は、その認証情報を証明する署名を発行する機能を持つ不正チェックサーバに関する資料です。

2　利用方法

2.1　任天堂認証サーバでの認証処理

最初に任天堂の認証サーバにて認証処理を行い、認証トークンを取得します。

これは正規の任天堂の製品からのアクセスを証明するための手続きで、独自サーバにアクセスする際には認証サーバから取得した認証トークンを取得し、その認証トークンを独自サーバに送信することで、認証処理を行います。

2.2　ポケモンデータを準備

不正チェックサーバへ送信するポケモンのデータを連結します。

不正チェックサーバが同時に処理できるポケモンの最大数は特に設けていません。

※ 1 ポケモンあたりのデータサイズは 236byte を想定しています。

2.3　不正チェックサーバへデータ送信

バイト位置	サイズ(byte)	説明
0	可変	認証トークン(末尾'¥0')
認証トークンサイズ ＋0	2	ゲームモード 0～32767 (ネットワークバイトオーダー)
認証トークンサイズ ＋2	ポケモンデータサイズ ＊ ポケモン数	連結したポケモンデータ

上記データを http://125.206.241.227/pokemon/validate へPOSTしてください。

※リリース時にはドメインを割り当て、SSL を利用するようになります。

2.4　不正チェック結果の解析

不正チェックサーバへデータを POST すると、レスポンスで不正チェックの結果が返ってきます。

まずは、HTTP レスポンスコードを取得して、通信に成功したのかを判定します。レスポンスコードと結果の関係は以下の表の通りとなります。

レスポンスコード	説明
200	不正チェック成功
400	ゲームモードが不正
401	認証トークンが不正
その他	サーバエラー

不正チェックが成功した場合は、body に不正チェックの結果として以下のデータが返ってきます。

正常なデータとして認証（送信したポケモンの数=n）

バイト位置	サイズ(byte)	説明
0	1	ステータスコード(成功=0)
1	4	ポケモン 1 の認証結果コード(ネットワークバイトオーダー)
5	4	ポケモン 2 の認証結果コード(ネットワークバイトオーダー)
:		
1+4*(n-1)	4	ポケモン n の認証結果コード(ネットワークバイトオーダー)
1+4*n	128	不正チェック通過署名

不正なデータとして認証

バイト位置	サイズ(byte)	説明
0	1	ステータスコード(失敗=not0)
1	4	ポケモン 1 の認証結果コード(ネットワークバイトオーダー)
5	4	ポケモン 2 の認証結果コード(ネットワークバイトオーダー)
:		
1+4*(n-1)	4	ポケモン n の認証結果コード(ネットワークバイトオーダー)

正常なデータとして認証された時には署名が返ってきますので、以降ポケモンのデータが正しいかの判断は、この署名を利用して判定することができるようになります。GPF や GDS などの、他の独自サーバでポケモンデータが改ざんされていないかを確認したい時に利用します。

3 署名

3.1 データが改ざんされていないかの確認方法

レスポンスには、不正チェックを行ったポケモンデータを連結したデータの RSA-SHA1 を署名データとして付加しています。

つまり、ポケモンデータを連結したデータの SHA1 で求めたハッシュ値と、署名データを RSA 公開鍵(1024bit)で復号化したデータが一致すれば、不正チェック通過後にポケモンデータが改ざんされていない事を確認することが出来ます。署名データを復号化するための公開鍵は以下です。BASE64 でエンコードされていますので、デコードして利用してください。

```
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDZh9Rl5O6uWC0BcxXwDqNA
DFELLlHhXXfQOtyyXIMBcfVp+9JqeNxpaU3dLO+kqarRoNmqmXBb8IA49Xdk
7qWrfWo4OGeK7CYulSoc27ji/2jcky5/jjrs0f5SgurKQWHCID/wmPedZzXm
RBThhfuz7AQ9g42bSxkHIzHD95hX5QIDAQAB
```

2010 年 1 月 22 日現在