Qualys SSL Labs
SSL Server Test

2016/01/13
INTER-Mediator勉強会2016-#1

松尾 篤（株式会社エミック）

株式会社エミック

Agenda

- Qualys SSL Labs SSL Server Testとは
- HTTPSサーバー設定の主要確認点

本題の前にお知らせ

- 昨年からINTER-Mediatorのサイトに HTTPSでアクセスできるようになりました
- https://inter-mediator.com/ のみ

Qualys SSL Labs

SSL Server Testとは

Qualys SSL Labs
SSL Server Test

- インターネットにあるWebサーバーの
  SSL設定をさまざまな観点からチェック
  - 古くて弱い暗号を使っていないか
  - 適切にサーバーが設定されているか
  - 脆弱性がないか etc.

Qualys SSL Labs
SSL Server Test

QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

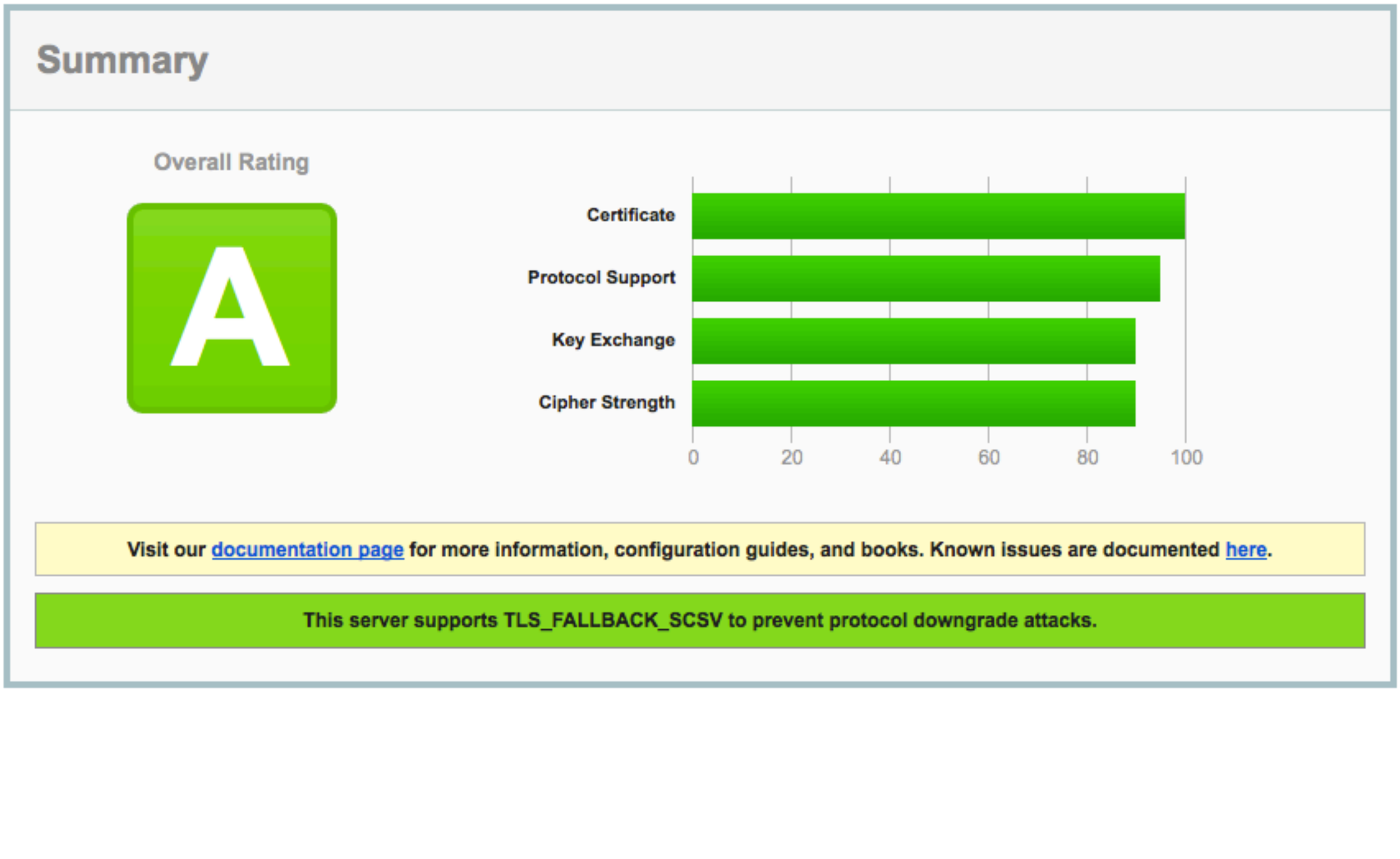
Domain name: inter-mediator.com Submit

☑ Do not show the results on the boards

確認方法

- https://www.ssllabs.com/ssltest/ を開く
- “Do not show the results on the boards”をチェック
- “Submit”ボタンを押す

Qualys SSL Labs
SSL Server Test



HTTPSサーバー設定の主要確認点

HTTPSサーバー設定の主要確認点

- プロトコルのバージョン
- 暗号スイートの設定
- 圧縮設定の解除

プロトコルのバージョン

- 最新規格であるTLS 1.2の使用を推奨
- SSLv3を無効にする
  - POODLE対策

暗号スイートの設定

- Apache HTTP Serverの場合は
  SSLCipherSuiteディレクティブで設定
  - 後述のガイドラインを参照
- サーバー側の設定を優先させる

圧縮設定の解除

- SSL圧縮を無効にする
- CRIME攻撃対策、TIME攻撃対策
- SSLCompression off（Apache）

より詳しくは

- IPAが公開しているガイドラインを参照
  - SSL/TLS暗号設定ガイドライン
  - https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

まとめ

- Qualys SSL Labsで公開WebサイトのSSL/TLS設定を確認しましょう
- “SSL/TLS暗号設定ガイドライン”を読んで設定を見直しましょう