

無料SSL証明書「Let's Encrypt」の設定方法

ステップ ①

J-web管理画面へ管理者権限でログインします。

(j-webドメイン管理画面URL: <https://admin.aiosl.com/>)

① 以下の必要事項を入力してください。

「アカウント」: **root**

「ドメイン」: **ご契約ドメイン名** (例: manual.aiosl.com)

「パスワード」 **管理者パスワード** (「J-webご設定について」の書面に記載)

② 必要事項入力後[認証]ボタンを押すと、管理者権限でログインできます。

※当社ホームページ (<https://corp.aiosl.jp/login/>) からでもログイン可能です。

ステップ ②

「SSL設定」ボタンを押下します。

アカウント名:	ディスク使用量:	ドメイン名:	FTP/Mailサーバ名:
root (ドメイン管理者)	使用量 49.3M / 契約量 20.0G 1%未満	manual.aiosl.com	srv7.ssl.aiosl.com


新規利用者登録 | 自動応答構築 | フィルター設定 | 接続先設定 | ログアウト

FTPアカウント管理 | webアプリ設置 | アクセス制御 | Web認証設定 | メールフォーム

SQL設定 | PHP設定 | CRON設定 | サポートページ | **SSL設定**

ステップ ③

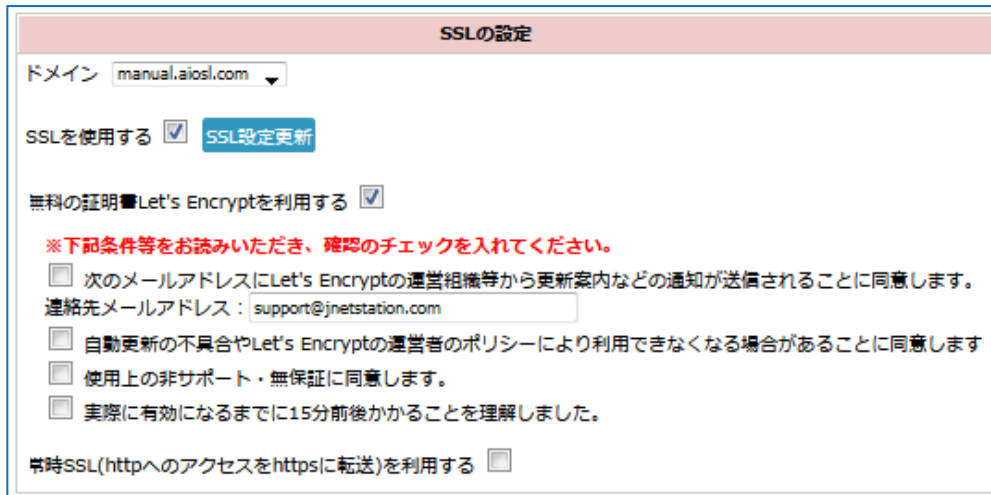
「SSLを使用する」にチェックを入れます。



SSLの設定

ドメイン manual.aiosl.com

SSLを使用する SSL設定更新



SSLの設定

ドメイン manual.aiosl.com

SSLを使用する SSL設定更新

無料の証明書Let's Encryptを利用する

※下記条件等をお読みいただき、確認のチェックを入れてください。

次のメールアドレスにLet's Encryptの運営組織等から更新案内などの通知が送信されることに同意します。
連絡先メールアドレス： support@jnetstation.com

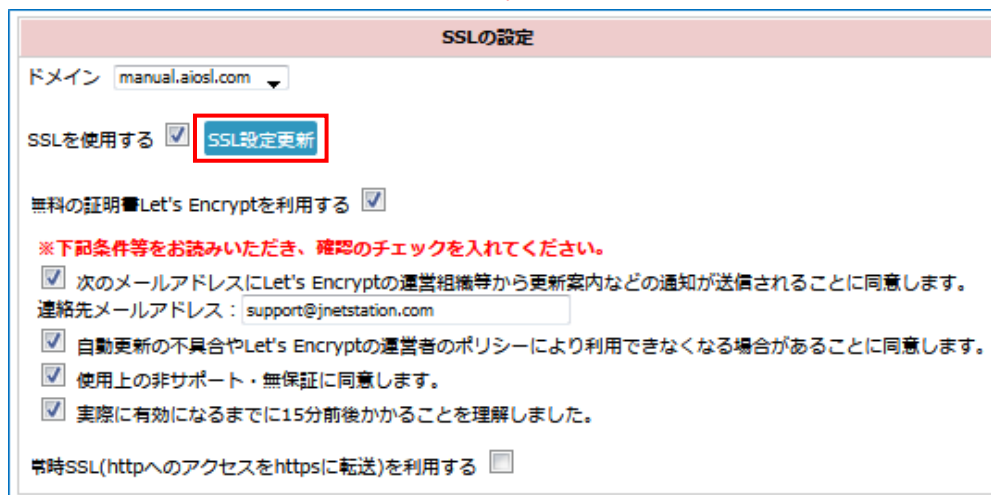
自動更新の不具合やLet's Encryptの運営者のポリシーにより利用できなくなる場合があることに同意します

使用上の非サポート・無保証に同意します。

実際に有効になるまでに15分前後かかることを理解しました。

常時SSL(httpへのアクセスをhttpsに転送)を利用する

・各利用条件を確認し、チェックボックスにチェックを入れてください。
※連絡先メールアドレスは必ず受取可能なメールアドレスを指定してください。



SSLの設定

ドメイン manual.aiosl.com

SSLを使用する SSL設定更新

無料の証明書Let's Encryptを利用する

※下記条件等をお読みいただき、確認のチェックを入れてください。

次のメールアドレスにLet's Encryptの運営組織等から更新案内などの通知が送信されることに同意します。
連絡先メールアドレス： support@jnetstation.com

自動更新の不具合やLet's Encryptの運営者のポリシーにより利用できなくなる場合があることに同意します。

使用上の非サポート・無保証に同意します。

実際に有効になるまでに15分前後かかることを理解しました。

常時SSL(httpへのアクセスをhttpsに転送)を利用する

・各利用条件にチェックを入れたら「SSL設定更新」ボタンを押してください。
※チェック漏れや、連絡先メールアドレスの未記入などがあると設定が出来ません。

※「常時SSL(httpへのアクセスをhttpsに転送)を利用する」のチェックはこの時に入れないことをお勧めいたします。
SSLサイト確認後、修正等がある場合に修正完了後ご設定ください。



設定が完了しました。

manual.aiosl.comのSSLの設定に成功しました。 manual.aiosl.comのLet's Encryptの設定に成功しました。

ご注意

Let's Encryptの証明書が有効になるまでには15分前後のお時間がかかります。

SSLや常時SSLの設定変更が反映されるまでに1分ほどのお時間がかかります。

証明書の設定をしない場合、SSLでアクセスすると警告画面が表示されます。

常時SSL設定を行わない場合、http://～ にアクセスした場合自動的に httpsにはなりません。

SSLの無効化や常時SSLの無効化が反映されるまでに1分ほどのお時間がかかります。

Let's Encryptの無効化は自動更新の停止のみで、既に設定済みの証明書は有効期限が切れるまでは有効なままです。

SSL設定

設定完了の画面が表示されます。

ステップ ④

HTTPSでページが正しく表示されているか、エラーなどが
出ていないか確認します。

HTTPSのページの中にHTTPで読み込むもの(画像やCSS、Javascriptなどが
混入)していると、そのHTTPを盗聴/改ざんされて利用者が危険に晒される恐れがある、
という理由からWebブラウザのURL欄に緑色の鍵マークではなく警告が表示されます。

(正常な場合)



各ページにて正常に鍵マークが表示されるか確認をしてください。
エラー等なければ設定完了です。

鍵マークが正常に表示されない場合



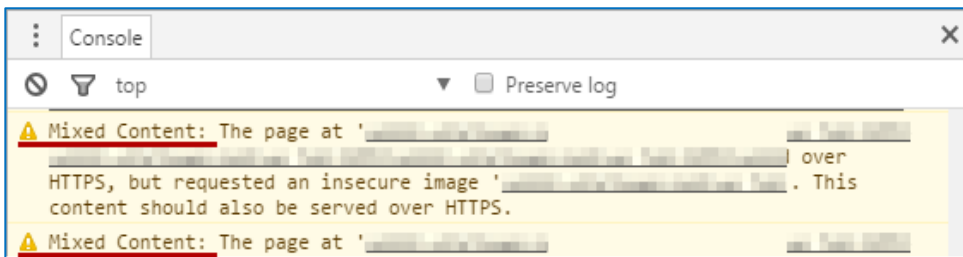
ステップ ⑤

エラーを特定します。

WEBブラウザの開発系ツールを利用すると便利です。

Google Chromeの場合は、デベロッパーツールを起動すると、右上に「!」マークで警告が表示されます。
※キーボードの「F12」キーで起動します。

HTTPとHTTPSの要素が混在する状態「Mixed Content」のエラーを修正しましょう。



「Console」タブで、「! Mixed Content: The page at～」の部分に、原因となる箇所がメッセージなどで表示されます。
その内容をもとにHTMLなどの修正を行い、確認します。
エラーが出なくなるまで修正作業を行い、完了させてください。

各ページにて正常に鍵マークが表示されれば完了です。