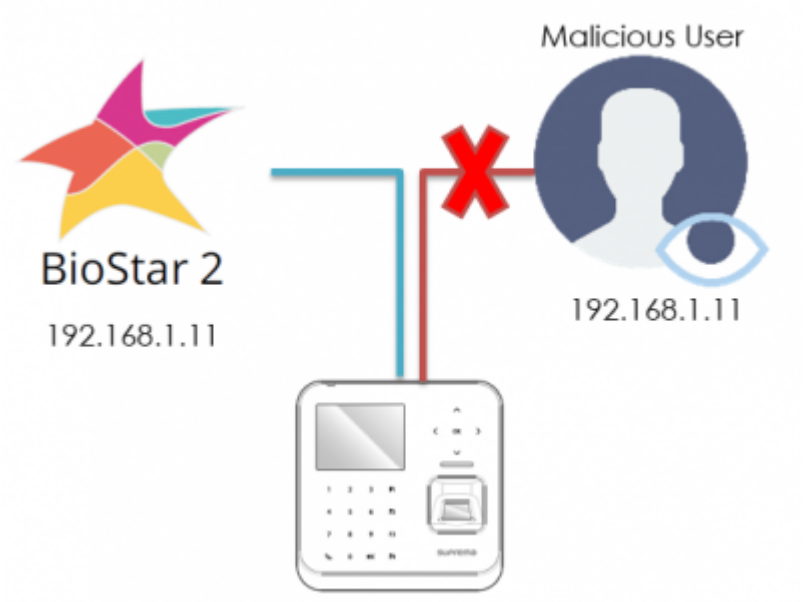
目次

システム構成, BioStar 2, TLS, セキュリティ通信

デバイスとサーバー間のセキュリティ通信の構成(TLS/SSL)

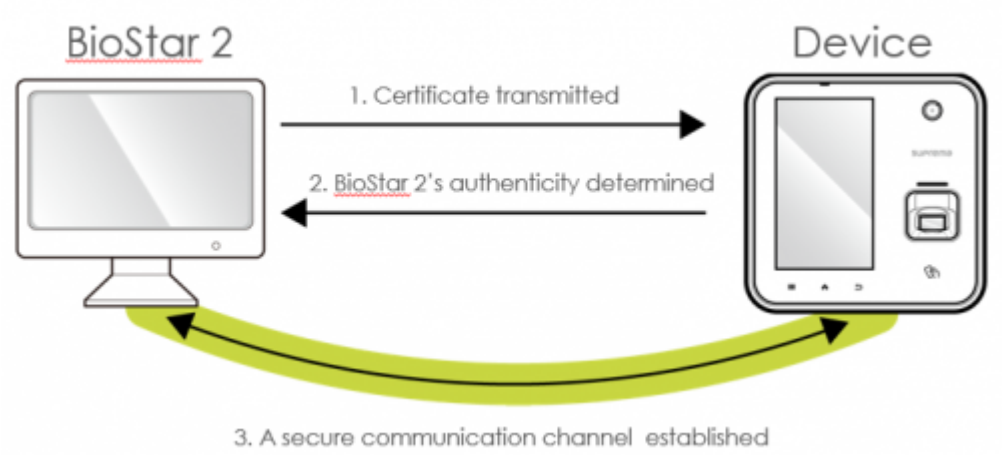
概念

サーバーとデバイス間の通信を行うためのトランスポート階層セキュリティ(TLS:Transport Layer Security/SSL:Secure Sockets Layer)機能がBioStar 2.4に具現されました。
この機能はハッカーのような悪性のユーザーがサーバーIP
が同一かのように装ってデバイスにアクセスすることを遮断します。



1)

このセキュリティは、デバイスにデジタル認証書を保存して具現します。
デバイスがサーバーに接続されると、デジタル認証書で暗号化キー(セッションキー)を交換してサーバーIDを確認します。



BioStar 2はTLS 1.2バージョンをサポートします。
セキュリティに関する詳細情報は以下を参照してください。 FAQ article

構成

この機能が有効となっている間は、デバイスへのアクセスが制限されることがあります。
デバイスのサーバーへの再アクセスには、数分程度を要します。

サポートデバイス/ファームウェアバージョン
- BioEntry W2 FW 1.1.0 以上
- BioStation L2 FW 1.2.0 以上
- BioStation A2 FW 1.3.0 以上
- BioStation 2 FW 1.4.0 以上
- FaceStation 2 FW 1.1.0 以上
- CoreStation FW 1.0.0 以上
- BioEntry P2 FW 1.0.0 以上

次のステップに従ってセキュリティ通信を構成してください。この機能は基本的に設定されていません。
1. BioStar 2にログインしてください。
2. **設定(Setting)**をクリックしてください。
3. **セキュリティ**をクリックしてください。
4. **詳細なセキュリティ設定**タブで、**端末の暗号化通信**を使用(Use)に設定してください。

VeriSign、Comodo、GoDaddyといったCA(認証機関)の外部証明書を使用するには、
外部証明書を使用するを設定した後に**アップロード(Upload)**
を押し、証明書をアップロードしてください。

注意
暗号化通信機能を使用する間にデバイスのネットワークアクセスが物理的に解除された場合は、
セキュリティ通信オプションを解除しないでください。
該当機能が消えた場合にはBioStar
2証明書が削除され、サーバーに再びアクセスできなくなります。
デバイスをサーバーに再度アクセスするには、デバイスに保存された証明書を削除するか、デバ

> イスを工場出荷時の初期化が必要です。
> BioEntry W2またはBioEntry
> P2のようにLCD
> がないデバイスの場合、デバイス説明書で初期化方法に対する説明を参照してください。
> 次のFAQ文書を参照してください。: Factory Default W2 / P2

1)

icon designed by Madebyoliver from Flaticon