asyril
Experts in
Flexible Feeding Systems

ウェブベースのインターフェースで強化されたセキュリティとユーザー保護を確保する方法：

HTTPS 証明書とユーザーアクセスコントロールの導入

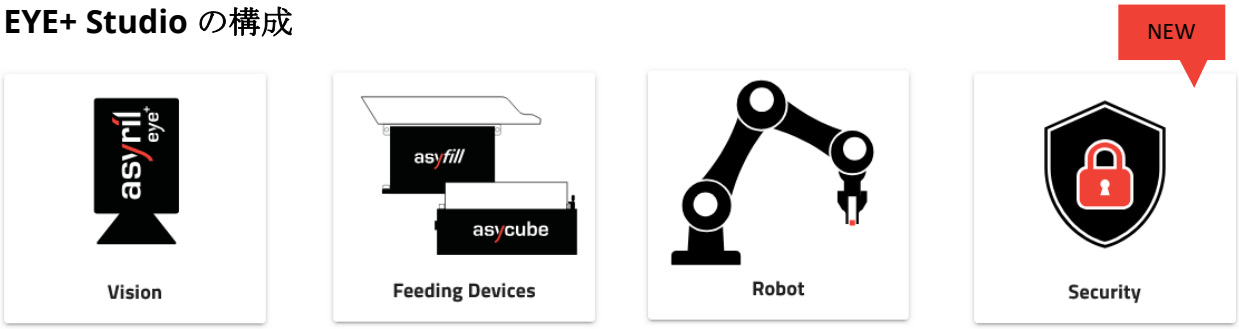
今日のデジタル時代では、セキュリティが最も重要です。企業がウェブインターフェースにますます依存する中、厳格なセキュリティ対策はこれまで以上に必要不可欠になっています。こうした状況で、最新の EYE+ スマートコントロールシステムは、次の 2 つの重要な点に焦点を当てて強化しました。

HTTPS 証明書による安全な接続

厳格なユーザーアクセスコントロール（UAC）

これらの機能は、EYE+ Studio の新しい「セキュリティ」セクションに含まれており、アジリルのウェブインターフェースやデータを保護します。また、２０２７年半ばから適用される EU のセキュリティ基準「サイバーレジリエンス法（CRA）」は、最低限のセキュリティ要件を定めています。特に、製品とアジリル社のセキュリティ能力に対する CE マークに関する視点から、将来のサイバーセキュリティ規制の準備にも対応しています。

EYE+ Studio の構成



安全な接続の重要性

HTTPS とは？

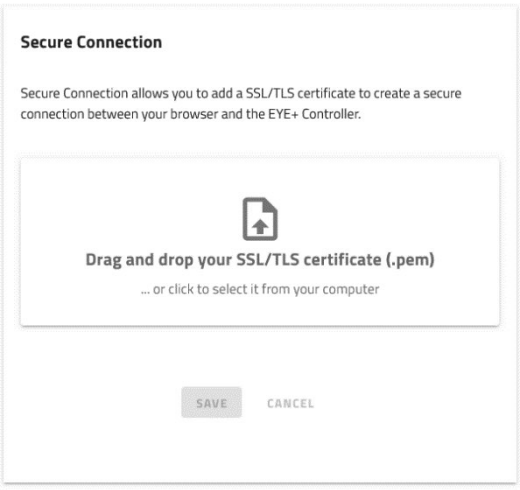
HTTPS（Hypertext Transfer Protocol Secure）とは、HTTP の拡張であり、ユーザーのブラウザとサーバー間のデータ転送を暗号化することで盗聴を防ぎます。

HTTPS 証明書の利点

1. **データの整合性**：HTTPS はデータ転送中の改ざんを防ぎます。
2. **機密性**：暗号化により、特定の受信者だけがデータを読むことができます。
3. **認証**：HTTPS は、ユーザーが正しいウェブサイトと通信していることを確認します。

EYE+スマートコントロールシステムにおける HTTPS

EYE+ プラットフォーム上での HTTPS の有効化プロセスを簡略化し、ユーザーが自社の IT 部門で生成された HTTPS 証明書をアップロードできるようにしました。これにより、EYE+ Studio とユーザー間のデータ転送が暗号化され、安全性が確保されます。この機能を有効にし、SSL/TLS 証明書を追加することで、ユーザーアクセスコントロールを通じて入力したパスワードが暗号化されます。そのため、誰もそのパスワードを読み取れなくなり、社内ネットワークに接続している他のユーザーに意図せずアクセスを許可することを防ぎます。



SSL/TLS 証明書は、すべての企業が周知しているわけではありません。アジリルは、EYE+ スマートコントロールシステムのすべてのユーザーがこのセキュリティ機能を活用できることを望んでいます。当社は、これらの証明書の仕組みや生成方法を説明しています。詳しくは、EYE+ ユーザーマニュアルの「知識データベース」をご参照ください。

ユーザーアクセスコントロール：インターフェースの保護

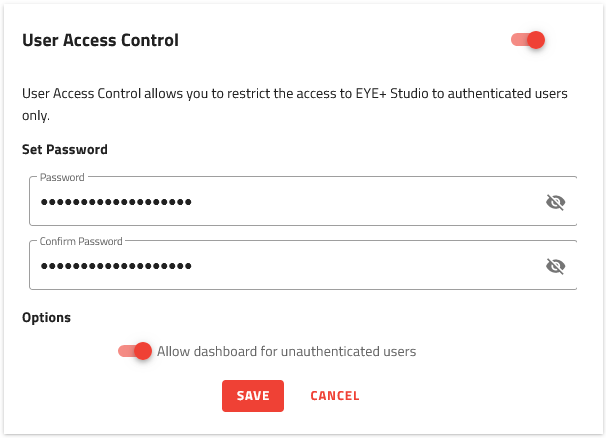
EYE+ スマートコントロールシステムは社内のネットワークに直接接続する必要はありませんが、不正アクセスはどのシステムにとっても大きな脅威となります。アジリルは、許可されたユーザーのみにアクセスを制限することで、悪意のある活動を防ぎ、機密データの安全性を確保します。

EYE+ユーザーアクセスコントロールの利点

1. **パスワード保護**：ユーザーは強力なパスワードを設定して ユーザーインターフェース（UI）を保護できます。
2. **ユーザー認証**：許可されたユーザーのみがシステムにアクセスでき、不正アクセスのリスクを低減します。
3. **アクセスレベル**：許可されたユーザーはダッシュボードへのアクセス権を持ち、そのユーザーだけが自動運転中に必要な情報にアクセスできるようにします。

EYE+ でユーザーアクセスコントロールを有

EYE+ Studio では、ユーザーアクセスコントロールの設定を段階的に案内する手順を提供しています。この機能により、ユーザーが設定した**シングルパスワード**でインターフェース全体を保護するか、または自動運転中にさまざまな指標を監視するオペレーターにのみダッシュボードへのアクセスを許可することができます。



ユーザーアクセスコントロールをニーズに合わせて使用する方法

EYE+ のユーザーアクセスコントロール機能は、許可されていない人からユーザーインターフェースを保護するだけでなく、悪意のあるユーザーがシステムに侵入し、自動運転の重要な要素を破壊するのを防ぐためにも使用できます。例えば、レシピの編集やシステム設定の変更を行う際、パスワードを入力する前に HTTPS 証明書による安全な接続を有効にすることは、パスワードの暗号化を確保するためのグッドプラクティスです。また、強力なパスワードを設定することで、悪意のある人々に意図せずアクセス権を与えるリスクを低減できます。セキュリティを確保するために、パスワード設定のグッドプラクティスは EYE+ ユーザーマニュアルに含まれています。

今日からシステムのセキュリティを強化し、デジタルセキュリティの最前線を行きましょう

HTTPS 証明書と EYE+ のユーザーアクセスコントロール機能の導入は、セキュリティ対策の大きな一歩です。EYE+ コントローラーと EYE+ Studio 間の通信を保護し、許可されたユーザーのみのアクセスに制限し、サイバーセキュリティのグッドプラクティスを文書化することで、アジリルはお客様に安全で信頼性の高いウェブインターフェースを提供します。

製品の開発始めからユーザーのセキュリティを考慮し、ソフトウェアやハードウェアのサプライヤーを慎重に選定し、第三者の関与から保護することで、お客様の設備に悪影響が及ばないようにしています。EYE+ によって取得された画像は、厳格に機械ネットワーク内に保存され、リモートメンテナンス目的以外でクラウドに接続する必要はありません。

サイバー脅威の状況は急速に進化しており、Cyber Resilience Act（CRA）などの規制への対応がますます重要となっています。２０２７年半ばまでには、CE マークを維持するために必須となります。アジリルは、CRA の基準を満たすために積極的なアプローチを取り、サイバーセキュリティの問題からお客様を守ることに重点を置いています。当社の R&D チームは、製品ポートフォリオをこれらの規制に合わせて常に調整し、お客様が十分な事前準備を整えられるように、明確なロードマップに従っています。サイバーセキュリティ対策に関する要件がある場合は、当社の技術センターまでお気軽にお問い合わせください。

EYE+ のセキュリティ機能の使い方についての詳細は、アジリルのオンラインドキュメントをご参照いただき、EYE+ スマートコントロールシステムを更新してください。また、EYE+ シミュレーションをぜひご体験ください。

EYE+ ドキュメント（随時更新）：https://doc.eyeplus.asyril.com/en/4.3/index.html

EYE+ シミュレーション： https://register.eyeplus.asyril.com/

スイス- 本社、R&D、製造

support@asyril.com

+41 26 420 42 42

アメリカ - テクニカルセンター

support.us@asyril.com

+1 612 294-6886

日本 - テクニカルセンター

support.jp@asyril.com

+81 (45) 479-9393

ドイツ - テクニカルセンター

support.de@asyril.com

+49 781 12552870

シンガポール - 営業所

support.sg@asyril.com

+65 98361678