Instron® Connect – ネットワークアーキテクチャとセキュリティ

はじめに

ここでは、Instron Connectのネットワークアーキテクチャとセキュリティの特徴を説明します。お客様のビジネス分野や技術分野に関する意思決定に関わる方々に向けて、お客様の環境においてInstron Connectがどのように機能するか、また、どのようにセキュリティ技術に関する要求に適合するかを理解していただくことを目的にしています。重要な問題としての企業内のファイアウォールやネットワークセキュリティ下の通信についての疑問への回答になると考えます。Instron Connectの目的は、世界中の何処にインストロンの試験機システムのオペレータがいても、インストロンのアプリケーションの専門家、テクニカルサポートやサービスエンジニアにコンタクトが取れるようにすることです。Instron Connectと接続することにより、お客様はシステムの稼動時間を増やすことができ、滞りのない有効なサポートを経験できるとともに、インストロンからの重要なお知らせやソフトウェアアップデート情報を受け取ることができます。

なぜ、Instron Connectを使用するのでしょうか？

業務の遂行に必要不可欠な機器やプロセスが複雑になるとともに、稼動時間を維持し関連業務プロセスをスムーズに行うことがますます重要になっています。企業にとって、いろいろな案件を処理するにあたり、必要な専門知識・技術を全て社内で確保するのは難しいことです。社外のパートナーや専門家と連携することは、1つの解決策になります。

発生した問題を監視でき、診断でき、アクションが取れる専門家と、リアルタイムの情報を共有することで、お客様のビジネスに高い生産性と収益性をもたらすことができます。Instron Connectは、お客様の施設にある試験機とグローバルに展開するインストロン製品専門家との間の安全な架け橋となります。

お客様にとっての利点

遠隔からの迅速なテクニカルサポート

Instron Connectシステムを通じて、モニタ画面を安全に共有できるとともに、必要なサービスの要求をすることができます。診断のため、試験メソッドや試験のサンプルデータのファイルを簡単に送付できます。

リマインダー設定によりリスク低減

リマインダー設定により、試験機の校正の認証期限切れを防ぐとともに、あらかじめ日程設定ができるので、不必要な装置停止を避けることができます。

ソフトウェアとハードウェアのアップデート

ソフトウェアのアップデートに関するお知らせが自動的にきますので、インストロンのシステムを最高の状態で稼動させることができます。

どの試験機システムが、Instron Connectに対応できるのでしょうか？

Instron Connectは、Bluehill Universalソフトウェア で作動する、インストロンの全ての試験システムについて適応可能です。しかしながら、Instron Connectを通じてインストロンと共有されるシステム診断情報内容は、システムにより異なります。システム診断情報により、インストロンのテクニカルサポートは、お客様の試験機システムを遠隔から診断するのに必要な情報を得ることができます。例えば、試験機のメカニカルリミットが動作して試験機が止まったとき、インストロンは安全なポータルサイトにログインすることにより、これを把握することができます。

Instron Connectは、どのように機能するのでしょうか？

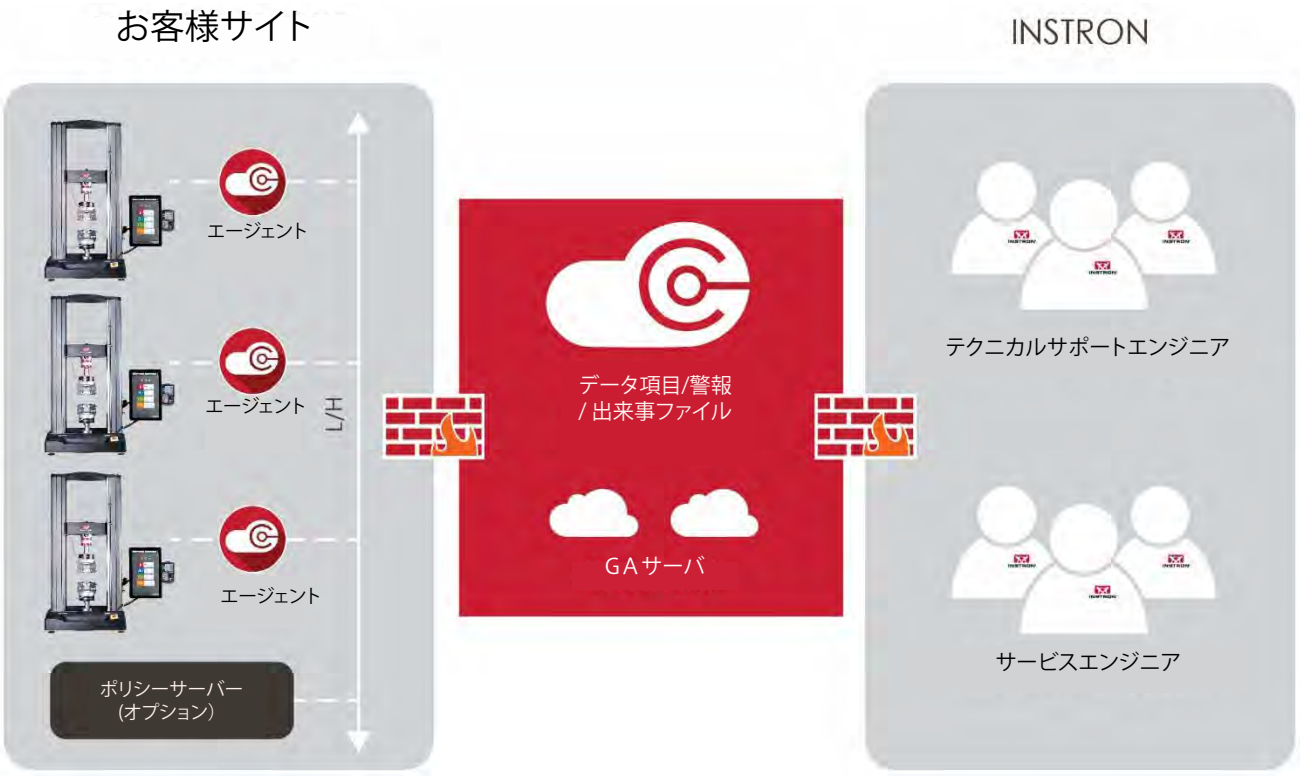
Instron Connectは、お客様の施設におけるインストロン装置の状態、動作パラメータ、機器の構成を監視します。これは、インストロンの試験システムに組み込まれた、監視エージェントのソフトウェアを通じて行われます。このエージェントは、Instron Connectのクラウドサーバと安全に通信を行います。

データを受け取ると、クラウドの中で動作するInstron Connectアプリケーションは、お客様の装置の動作状態を評価し、データを傾向分析します。問題が検知できたら、クラウドサーバは、インストロンのサービスエンジニアに知らせます。サービスエンジニアは、クラウドサーバ上のデータを解析することにより、稼動中の装置を停止させることなく遠隔から問題を診断します。

もし、より詳細な診断が必要な場合は、インストロンのサービスエンジニアに連絡して、直接試験機システムを診断**する**選択できます。お客様は、試験機の操作端末のスクリーンから、サービスエンジニアの遠隔操作を見ることができます。

診断が成されると、必要なソフトウェアのアップデートやその他のソフトウェアの設定の調整などを行い、問題を修正することができます。お客様の承認のもと、サービスエンジニアは多くの問題を遠隔から解決することができます。

システムの全体像



技術的概要

Instron Connectは、接続されている装置を管理するクラウドをベースとした、先進的なソフトウェア・システムであるPTC社のThingWorx IoT Cloud Servicesによって動作します。このCloud Servicesは、ISO 27001:2013認証済みのデータセンターから提供され、セキュリティや拡張性、インフラストラクチャ、オペレーションは業界規格に従っています。

Instron Connectは、3つの主要な部分から構成されています。

1. Bluehill Universalのような、インストロンのソフトウェアにより試験機システムを制御しているオペレータダッシュボードにおいて動作するInstron Connectのエージェント・ソフトウェア。
2. 装置情報へのアクセスを与えるInstron Connectクラウドサーバとアプリケーション。
3. Bluehill Universalのようなインストロンのソフトウェアに組み込まれているInstron Connectのインターフェース。試験システムのユーザーがヘルプを見る、お知らせを見る、ソフトウェアのアップデートをダウンロードする、ファイルをアップロードするといった時に開くポータルです。更に、ソフトウェア・エージェントと通信を行い、システムの診断情報（お客様の試験データファイルではありません）を、Instron Connectクラウドサーバへ、データ送信する役割を持っています。

Instron Connectのソフトウェア・エージェントは、インストロンのシステムを監視して、システムの健全性と構成状況を示す主要データ項目の状態をチェックしています。エージェントは、クラウドサーバ環境と周期的に通信し、このような主要データ項目の最新版をアップデートします。

Instron Connectは、お客様の既存のネットワークやセキュリティ・インフラストラクチャを活用します。エージェントが443ポートを使ってアウトバウンド通信でクラウドサーバとの接続ができる限り、遠隔接続のためポートが変更されることはありません。必要なのは、インターネットとの接続ができる環境です。

セキュアなPTC社ThingWorx Firewall-Friendlyによる通信方法では、エージェント側のコンピュータが固定・動的パブリックTCP/IPアドレスを持っている必要はありません。それは、インストロン側からお客様の施設におけるエージェントへアクセスを開始することは、決してないからです。お客様の施設におけるエージェント側が、クラウドサーバとの全ての通信を開始するのであり、双方向の通信は、接続が開始され承認されてからのみ発生します。

エージェントは特定のパラメータを監視し、クラウドサーバにデータ差分のみを送信するので、インストロンが使用するお客様のネットワークの通信量を極小化します。

また、おおよそ1分間に1度、エージェントはクラウドサーバに「心臓の鼓動」のように小さなメッセージを送り、エージェントが起動されていることを確認します。このようなメッセージがあれば、インストロンのテクニカルサポートはお客様からのリクエストに備えることができます。例えば、エラーログの要求や、遠隔からの作業の開始などです。これの動作はエージェントの操作により、リクエストが開始されます。

セキュリティ

お客様が、遠隔接続により稼動時間の延長や業務改善についての利点を享受できる一方、システムにアクセスしようとするハッカーや第三者の脅威が増大しています。どの接続方式も秘密情報やアクセスを保護するセキュリティ対策を提供できなければならないし、同時にお客様が既に持っているITポリシーやインフラストラクチャについてのセキュリティ戦略に違反または変更をすることがあってはなりません。

Instron Connectは、主要な情報セキュリティに関する懸念に焦点を当てて設計されており、次のような特長を持っています。

- ***お客様の施設にある既存のネットワークセキュリティを維持する*** Instron Connectは、特許取得済みの Firewall-Friendly™ 通信を利用することにより、お客様の既存のセキュリティインフラストラクチャを活用します。

- ***許可されていない第三者からデータを守る*** インストロンとお客様の装置の間の全ての通信は、Transport Layer Security（TLS）暗号化を用いることにより、安全に保護されます。銀行が使う安全なオンライン取引と同じ方法です。

- ***接続の検証方法およびなりすまし対策を提供*** システムは、通信すべきクラウドサーバにのみ繋がることを確認します。なりすましデバイスのデータおよび妨害コマンドを防止する方法が提供されます。

- ***インストロンのテクニカルサポートのユーザーを確実に認証する*** システムへの全てのアクセスは集中管理され、強力なパスワード認証が要求されます。インストロンのテクニカルサポートの全てのユーザーの操作は、すべて監査されてトレーサビリティがあります。

- ***インストロンのテクニカルサポートはデータのアクセス範囲、閲覧、オペレーションなど権限を制限*** 認証されたインストロンのテクニカルサポートがアクセスできる範囲は、責任を持つ製品および役割に対応するアクセスレベルに制限されます。

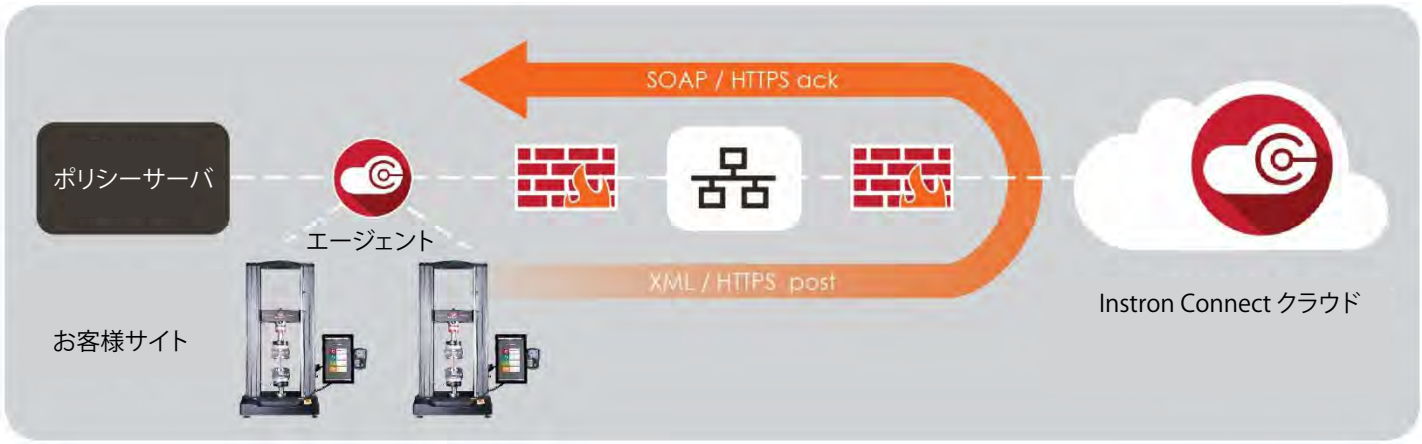
- ***安全なクラウドのインフラストラクチャにおけるオペレーション*** Instron Connectオペレーションは、ISO 27001:2013認証済みで、毎年SSAE-16 SOC 2の監査を受けているデータセンターで実行されます。オペレーションの専門家は、定期的なセキュリティのテストと見直しを実施し、データとデータアクセスを確実に保護します。

既存のITまたはセキュリティのインフラストラクチャの変更は不要

Instron Connect は、TLS暗号化を用いたHypertext Transfer Protocol（HTTP）に従って双方向通信を提供できるFirewall-Friendly技術を使っています。全ての通信は、標準TLSの443ポートからアウトバウンドに発信されます。遠隔からの監視や診断をサポートするために、他のポートを開いたり、既存のITセキュリティのインフラストラクチャを変更したりする必要はありません。

パブリックまたは固定IPアドレスは不要ですし、推奨されません。通信は、プロキシサーバや、ネットワークアドレス変換（NAT）、仮想ローカルエリアネットワーク（VLANs）に適合します。

Firewall-Friendly通信



エージェントが、全ての通信を開始

- VPNやパブリックIPアドレスは不要
- LANやWi-Fi、セルラ無線をサポート
- データや、ファイル、通信ポートの双方向交換が可能

安全な通信

- **アウトバウンドの接続のみ（443ポート上のhttps）**
- **TLS暗号化**
- **プロキシサーバとVLANをサポート**

強力な暗号化を用い、データを保護

お客様の施設の試験機システムとInstron Connectクラウドの間の全ての通信は、秘密保護のために強力な暗号化と業界標準の2048bitキー暗号化を用いたTLS プロトコルを使います。

接続の認証による、不正に対する防止策

TLS プロトコルは、通信の信頼性を確保し、確実に通信を受け入れます。プロトコルは、データを送信する前に、暗号化された接続により必ずエージェントにサーバの認証をさせます。

インストロンエンジニアの認証

Instron Connectのアプリケーションへのアクセスは、インストロンのテクニカルサポート、ソフトウェア開発、製品管理の各分野の熟練したスタッフのみに限定されています。インストロンのクラウドサーバは、各々のインストロンのユーザーがアクセスする場合、独自のユーザーIDとパスワードを要求します。パスワードは厳格に管理され、各々のユーザーは90日ごとにパスワードを変更しなければなりません。コンピュータがオン状態で、アプリケーションが操作されないまま開かれていると、データは危険な状態にあります。このような状態を避け、承認外の使用を防止するため、システムは10分間操作していないユーザーを自動的にログオフします。

インストロンのサービスエンジニアのアクセス管理

インストロンのサービスエンジニアのユーザーのアクセス管理は、作業ベースと機器ベースのアクセス管理を通して実行されます。これらの2つの方法は、広範囲の観点で組み合わされており、インストロンのサービスエンジニアが効率的に仕事をしつつ、機密保持を必要とする情報を守ることができます。作業ベースのアクセス管理において、Instron Connectシステムの管理者はThingWorxポータルにテクニカルサポートを割り当て、作業権限を分類し、実行できる作業を定義します。各々のサービスエンジニアは、ThingWorxポータルのアプリケーション、ページと操作に対して、権限により分けられたアクセス権を与えられます。機器ベースのアクセス管理の方法では、各々のサービスエンジニアがアクセス可能な特定の機器が定義されます。この管理方法では、デバイス情報の閲覧を、サービスエンジニアが責任を持つ機器だけに制限します。

監査ログ

監査ログには、ユーザーのシステム内や装置とのやりとりに関する情報が含まれています。そこにあるデータは、インストロンのクラウドサーバにも残され、試験機システムにも残されます。インストロンのテクニカルサポートは、許可されているインストロン製品だけの監査ログを見ることができるのです。ユーザー設定または機器がシステムから取り除かれた場合でも、ユーザー設定および機器に関わる全てのデータは、監査ログに残され続けます。

データの機密性と組織的なセキュリティ対策

インストロンは、システムにおいて適切なデータの機密性とセキュリティが確保されるよう、Instron Connectを運用しています。インストロンは、適用される秘密保持に関する法令を遵守し、データの機密性とセキュリティを確保する手段を以下のように採っています：

- お客様のネットワークと機器類への遠隔からのアクセスは、お客様との合意のもとにのみ実施されます。
- インストロンの全てのテクニカルサポート・サービスエンジニアには訓練が施され、お客様のデータが機密である可能性があること、またテクニカルサポート・サービスエンジニアはお客様の機密を確実に尊重すべきことを理解させています。
- 個人データは機密とされます。インストロンから連絡を取る上で、お客様から連絡先をいただくことがあるかも知れません。この情報は、Instron Connectと関連したテクニカルサービスを提供する目的、およびセキュリティ管理のみに使われます。
- 監査できる記録は、契約期間内に遠隔サービスを行った記録について、各々のお客様について保存されます。記録は、遠隔サービスが第三者によって行われ、そのようにお客様により合意されている場合にも保存されます。

情報収集について

Instron Connectが監視するエージェントは、各々の装置について予め決められたデータを収集します。これらの収集されたデータは、インストロンのテクニカルサポートが、試験機システムの問題を診断し、解決するときに役に立ちます。これらのデータは、モータの電圧、リミットセンサやシステム障害などです。試験機の状態と試験機の構成に関する情報だけが、インストロンに伝達されます。インストロンは、お客様の慎重な意向と指示なく、お客様の機密かつ所有権下にある試験データ、試験結果、および試験メソッドに関する情報を閲覧、収集する権限を決して持ちません。テクニカルサポート活動の中で、より推奨される試験方法を得るため、または試験機システムの問題を早期解決するため、Instron Connectを通じてインストロンに試験メソッドファイルや試験データファイルをアップロードすることが望ましいと判断される場合があります。

その場合、インストロンは、受け取った試験データについて、適切なデータセキュリティと非公開に関する規定に従い扱います。アプリケーション・テクニカルサポートを提供するため、モニタ画面の共有が必要なときは、インストロンの試験システムのユーザーが「同意します」をクリックして、インストロンのテクニカルサポートに試験機システム画面の閲覧を許可しなければなりません。この遠隔からの画面共有作業は、短時間、通常は30分で終了します。また、お客様側のユーザーは、いつでも画面共有作業を終了することができます。この画面共有作業時に、インストロンのテクニカルサポートは、画面上で試験データを見るだけでなく、メソッドデータと試験データファイルを開けることができます。これらのファイルはインストロンにアップロードされたのと同様に、同じセキュリティ対策が適用されます。インストロンは、画面共有作業中にこれらを記録し、画面コピーを取ることはありません。お客様の製品についてお客様の試験システムで採取された試験データが、試験システムの問題を診断する上で有益でない限り、インストロンはこれらの情報を見たり、収集したりすることはありません。

解除に関する方針

Instron Connectの唯一の目的は、お客様がインストロンの試験システムを使用する際の技術を向上させることです。しかしながら、インターネット接続ができない、独自のセキュリティに関する方針による理由のため、必ずしも全ての研究機関がInstron Connectに接続できるわけではないことは良く理解できます。Instron Connectは、次のどちらかの方法により解除できます。

1. 試験システムからインターネット接続を外す。
2. Bluehill Universalのようなインストロンのソフトウェアにおいて、管理メニューからパスワードを入力し、Instron Connectの接続をオフする。

もし、Instron Connectに接続していなくても依然として、サービス契約の内容に基づいて、これまでと同様、電話やメール、現地訪問を通じて、お客様はインストロンの世界標準のお客様サポートを受けることができることをご承知ください。

ソフトウェアのダウンロード

Instron Connectに接続している場合、試験システムは定期的にInstron Connectクラウドサーバをチェックし、インストロンのソフトウェアの新しいバージョンがリリースされているかどうか調べます。もし、新バージョンが取得可能な場合は、Instron Connectの画面の「ダウンロード」ボタンを押すことにより、最新版をダウンロードすることができるようになります。ダウンロードが開始されると、ダウンロードされるフォルダのリンクがメッセージセンターのメッセージに現われます。お客様は、フォルダの中のインストロンのBluehill Windowsのインストーラーパッケージを開くことにより、ソフトウェアをインストールすることができます。

お客様によっては、現在バージョンのソフトウェアのままで使用する必要があり、アップデートできない場合もあると思います。Instron Connectは、ソフトウェアのダウンロード機能をオフにしても、お客様は依然としてInstron Connectの他の全ての機能を活用することができます。ソフトウェアアップデートのお知らせとダウンロードの機能を解除するには、インストロンのソフトウェアの管理メニューからパスワードを入力して、この機能をオフにしてください。Instron Connectの他の機能には、影響を与えません。注意していただきたいのは、将来、Instron Connectのインフラストラクチャに変更が生じた場合、ソフトウェアアップデートが可能になってないと、Instron Connectの機能が低下したり、使用できない可能性があります。

エージェント通信のネットワーク設定

Instron Connect エージェントがクラウドサーバと通信できるためには、エージェントからインターネットへの標準HTTPS通信のポートがポート443に許可されてなければなりません。データとファイルの通信は、クラウドサーバと行います。お客様のネットワークがアクセス制御リスト（ACL）またはHostsファイルを使ってのアウトバウンドの通信を制限している場合、次のIPアドレスの制限を解除してください。

IP アドレス	URL	説明
34.195.150.174	https://instron-prod.cloud.thingworx.com	Instron Connect Server

注）IPアドレスはThingWorxの例の場合であり、URLはThingWorxの例の場合です。