BeckmanConnectのセキュリティについて

概要

この資料では、BeckmanConnectリモート管理ソリューションのプライバシーおよびセキュリティ機能についてご紹介します。このソリューションは、ベックマン・コールター社のサービス／サポート部門が、お客様のラボラトリーにあるBeckman Coulter装置への安全なリモート接続を介して、リアルタイムでサービスを提供する目的で設計されています。 この資料は、お客様の施設でご使用の装置PCおよびネットワークインフラストラクチャの管理を担当するIT管理者の方が、BeckmanConnectを承認するプロセスの一環としてお読みいただくことを前提としています。

ベックマン・コールター社のリモート管理プラットフォームは、安全なオンラインリモートサポートおよびコラボレーションの世界的なリーダー企業であるTeamViewer GmbHがサポートしています。リモートソフトウエア開発の最先端企業であるTeamViewer GmbHは、クラウドベーステクノロジーのプロバイダーとして高く評価され、Federal Association of IT Experts and Reviewersから5つ星の品質シールを取得しています。[1] TeamViewerは、医療機関、官公庁、銀行、金融機関など、データが重要な役割を果たす多くの業界で選ばれているプロバイダーです。[2]

BeckmanConnectは、HIPAA、GDPRなど各地域のデータプライバシー規制に準拠しながら、リモートアクセスを提供します。具体的には、TeamViewerは識別情報を何も保存せずに2つのエンドポイントを接続する、パススルーとしての役割を果たします。

技術概要

TeamViewerツールは、ベックマン・コールター社のサービス／サポート専門技術者が、お客様の施設にあるBeckman Coulter装置に安全に接続できる、セキュアリモート画面およびファイル共有プラットフォームを提供します。TeamViewerトラフィックはすべて、RSA公開／秘密鍵交換およびAES（256ビット）セッション暗号化によって保護されています。さらに、このプラットフォームは中間者（man-in-the-middle）攻撃や総当たり攻撃を未然に防止するように構成されています。詳しくは**こちら**にあるTeamViewerセキュリティステートメントをご覧ください。[2]

図1. 2ファクタ認証、信頼できるデバイス、およびホワイトリストの使用により、ラボラトリー内のBeckman Coulter装置にアクセスできるのは、ベックマン・コールター社のサポート担当者だけであることが保証されます。

[1] Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.
[2] TeamViewerセキュリティステートメント、**https://dl.tvcdn.de/docs/en/TeamViewer-Security-Statement-en.pdf**

セキュリティ対策

TeamViewerを運用するにはインターネット接続が必要です。Beckman Coulter装置PCをネットワークに初めて接続する際は、事前にBeckmanConnect装置PCのネットワーク要件ドキュメントをお読みになり、装置PCが保護されていることを確認してください。IT要件をよく確認し、サービス条項に同意したうえで、リモートサポート機能を有効化していただく必要があります。

BeckmanConnectは、導入後ただちに最大のセキュリティを提供するように構成されています。

- TeamViewer接続には、ホワイトリストが提供されています。これにより、ベックマン・コールター社のサービス／サポート部門以外からの装置へのアクセスが防止されます。
- クライアント側における発信TeamViewer接続リクエストおよびミーティング機能は、無効に設定されています。
- 接続セッションを開始するには、一意の接続パスワードが常に必要です。このパスワードは、不正接続を防止するためセッションごとに変更されます。
- 安全なTeamViewerセッションの認証に成功した後、ユーザーはTeamViewerクライアントを介した画面表示、リモート制御、またはファイル転送リクエストを手動で承認する必要があります。接続リクエスおよびファイル転送は、TeamViewerセキュアサーバー上でもログに記録されます。
- 注記：機器コントローラPC (Navios EX, DxFlex, Data Innovations Instrument Manager, Aquios CL, CellMekSPS, Navios) は個人情報を含むデータファイル転送はできません。将来のリリースでこの機能が有効になった場合、ユーザーが更新をダウンロードし、インストールの際に新しい機能を承認するまでアクティブになりません。
- ベックマン・コールター社のTeamViewer管理ポータルへのアクセスは、ユーザー名および複雑なパスワードによって制限されています。お客様の地域に適用されるデータおよびプライバシーガイドラインに関する研修を受講済みのベックマン・コールター社の従業員にのみ、アクセスが制限されています。

ファイアウォールの要件

BeckmanConnectは、特殊なファイアウォール構成を必要とせず、安全なリモート接続を実現するように設計されています。ある種の状況では、未知のアウトバウンド接続を遮断する目的で、ファイアウォールがセットアップされている場合があります。このような場合は、接続が正常に行われるようファイアウォールを構成する必要があります。

BeckmanConnectは、ポート443を使用してアウトバウンドTCP接続を確立します。クライアントソフトウェアが次の動作を実行するには、ポート443が必要です。

- 自動更新
- セキュリティ目的で必要なグループポリシーの設定
- ベックマン・コールター社のサービス／サポート担当者からのリモート接続の許可

注：ポート443へのアウトバウンドアクセスがないと、サービスは正常に機能しません。

BeckmanConnectは、世界各地に設置されているセキュアサーバーに接続します。これらのサーバーは、時間の経過とともに変化する可能性のある、多くの異なるIPアドレスを使用します。BeckmanConnectが使用するIPアドレスはすべて、*.teamviewer.comまたは*.beckman.comドメインに解決されます。この情報を利用して、ファイアウォールまたはプロキシサーバー経由で許可する宛先IPアドレスを制限することができます。

BeckmanConnectサービスは、ファイアウォール経由の発信データ接続しか開始しません。そのため、着信接続を遮断し、ポート443を使用する*.teamviewer.comおよび*.beckman.comドメインへの発信TCP接続だけを許可すれば十分です。

まとめ

BeckmanConnectは、ベックマン・コールター社のサービス／サポート担当者がテクニカルサポートの目的でリモートから特定の装置にアクセスするための安全なシステムです。このエンドツーエンドトンネルは暗号化され、お客様を安全な状態に保つための対策が講じられています。アクセスできるのは、適切な訓練を受けたベックマン・コールター社の従業員に限定されています。

詳しくはこちらまでお問い合わせください。

connect@beckman.com

Beckman Coulterの世界各国の事業所の所在地および電話番号については、beckman.comの「Contact Us（お問い合わせ）」よりご確認ください

MULTI-648302.20