ZEISS Predictive Service

リモートサービスプログラムに関する技術情報

ZEISS Predictive Service
リモートサービスプログラムに関する技術情報

Author :	Dr.Christian Schwindling, Marcus Jacob Carl Zeiss Microscopy GmbH, Germany
Date :	April 2018

このドキュメントではZEISS Predictive Serviceのアーキテクチャーとセキュリティ機能の説明をしています。

ZEISS Predictive Serviceがお客様の環境でどのように運用され、お客様の技術的セキュリティ要件をどのように満たすかを、IT責任者にご理解いただくことを目的としています。また、ファイアウォールを介した通信およびネットワーク セキュリティなどの重要な問題についても含まれます。

Connectivity

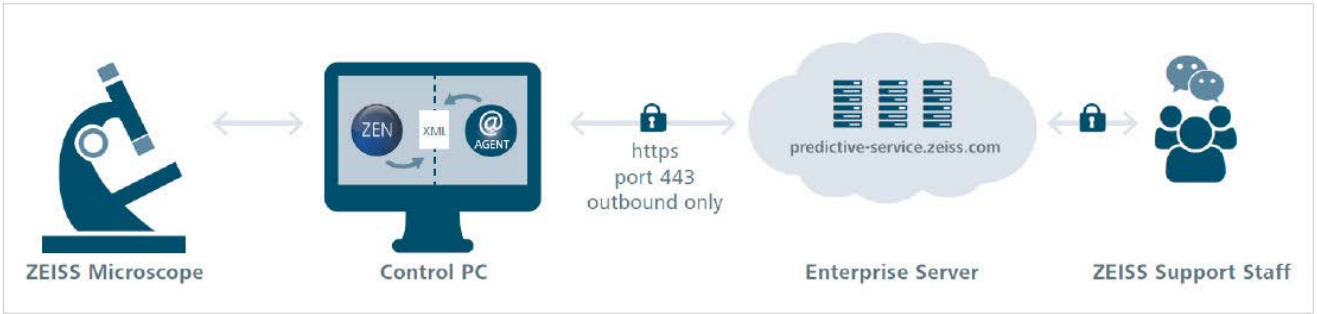

図1 接続イメージ

ネットワーク接続の中心部分は、顕微鏡のコントロールPCにインストールされる小さいソフトウェア パッケージである、いわゆるエージェントです。エージェントは「ZEISS Predictive Service Agent」としてのローカルシステム特権を持つWindowsサービスとして実行されるように設定されています。

エージェントが実行されると、ZEISS Predictive Service AgentはTCPポート443でhttpsプロトコルを使用し、256ビットTLS（トランスポート層セキュリティ）エンドツーエンド暗号化を使用して、predictive-service.zeiss.comにあるZEISSエンタープライズ サーバーとの接続の確立を試みます。この接続は常にアウトバウンド専用です。これは、エージェントが確立された接続を介してのみメッセージを受信できるように、通信チャネルが常にエージェントによって開始されることを意味しています。ZEISS Predictive Service Agentがサーバーとして機能し、（内部）接続用のポートを開くことは決してないため、実質的に典型的な外部からの攻撃が回避されることを知っておくことが重要です。ローカル ネットワークがプロキシ サーバーを必要とする場合は、サーバー アドレスを設定できます。

ユーザー名とパスワードが必要な場合は、強力なAES 256ビット暗号化を使用してZEISS Predictive Service Agentのインストレーション ディレクトリにパスワードが保存されます。predictive-service.zeiss.com外部へのHTTPS接続が既に許可されている場合、通常はファイアウォールの設定を変更する必要はありません。

エンタープライズ サーバーpredictive-service.zeiss.comはMicrosoft Azure Cloudインフラストラクチャーを使用してホスティングされ、国際標準（たとえばISO 27001、HIPAA、FedRAMP、SOC1、SOC2など）に従って証明され、認証されます。
エンタープライズ サーバーで実行されるアプリケーションは、HTTP認証と認可、セキュリティ ロギング サブシステム、すべての機密データ（ログイン データ）の暗号化ストレージ、回線を介したすべてのデータ転送の暗号化（Advanced Encryption Standard (AES) 256ビットを使用したTLS 1.2）を保証するためのトランスポート層セキュリティのサポートなど、業界標準のセキュリティ機能を含むPTC ThingWorxをベースにしています。
ZEISSエンタープライズ サーバーとエージェントの間の通信はSecure WebSocketスタンダードに従っています。

エージェントがHTTPSを介したエンタープライズ サーバーとの安全な接続を確立する初期化フェーズがあります。エージェントとZEISSエンタープライズ サーバーの間の双方向通信を可能にするために、その接続を介してWebSocketアップグレードが行われます。初期化した後、エージェントは、機器の動作状態データの監視またはカスタマー レポートの生成で重要な役割を果たす指定されたデータ値をプッシュします。

データ値は、たとえば、運用時間、コンポーネント レベルの電圧または接続状態などです。同じ確立された接続を介してログ ファイルも転送されます。すべてのデータ転送が、常にエージェントによって開始される確立された通信チャネルを必要とします。したがって、エンタープライズ サーバーは確立されたセキュアな接続を介してのみデータを要求できます。いったん接続が確立されれば、接続の失効によって新しい接続の確立が必要とされるまで、その接続は維持されます。

Connectivity Summary

- Windows service ZeissPredictiveServiceAgent.exe
- Only outbound https, 256-bit TLS/SSL secured connection on port 443
- No open ports for inbound connection
- Proxy server support
- Typically no changes to firewall settings
- Microsoft Azure cloud infrastructure certified and audited according to international standards (ISO 27001, HIPAA, FedRAMP, SOC1 and SOC2)

状態モニタリング

このセクションでは、上記で説明した接続モデルに基づく状態モニタリングの機能を説明します。状態モニタリングとは、関連のある機器の動作状態情報の体系的な取得およびその情報のサーバーをベースとする処理を意味しています。目標は、機器の性能の偏差がユーザーの結果を損なう前に、場合によっては不測のダウンタイムを引き起こす前に、その偏差を検出することです。代表的な例は最大動作サイクルに達した機械的部品の予防的な交換です。機器の動作状態データは、たとえば、運用時間、モーター駆動部品の動作サイクル、部品レベルの電圧、ファームウェアのバージョン、エラーメッセージなどです。具体的なデータの範囲はデバイスによって異なります。

すべての関連データがZEISSの顕微鏡のシステム オペレーティング ソフトウェアによって収集され、別々のログファイルに保存されます（表1参照）。これらのファイルはテキストビューアで開くことができます。ログファイルはエージェントソフトウェアによって継続的に監視されます。新しいデータが保存されると、エージェントはログファイルを解析し、確立された接続を介してデータアイテムをエンタープライズ サーバーに送信します。オペレーティングシステムおよびシステムオペレーションソフトウェア（たとえば、ZEN、SmartSEM）に関する情報はレジストリおよびWindows Management Instrumentation（WMI）を介して取得されます。このデータにはオペレーティングシステムのバージョン、PCのシリアル番号、ハードドライブの使用量が含まれている可能性があります。

データはタイムスタンプ付きでサーバーに保存され、事前に定義されたルールと照合されます。例えばZEISSのサービスエンジニアへの通知などのアクションを連動させることができます。トレーニングを受け、許可されたZEISSのスタッフは、エンタープライズサーバーにログオンし、診断の目的ですべてのデータ セットとその履歴を調査することができます。生の画像や処理済みの画像など、顕微鏡のユーザーから出力された結果がこのデータストリームで転送されることは絶対にありません。

Condition Monitoring Summary

- Only log file data from specific log file storage locations are transmitted (see table 1). These files are fully transparent and plain-text readable
- No user specific information or files are included in continuous monitoring

Device type	Log file name	Description	Path
Electron microscopes	EM Server.log	Information about EM Server	C:¥ProgramData¥Carl Zeiss¥SmartSEM¥Log¥EM Server.log
Electron microscopes	Log Folder	Includes SmartSEM Logs (GIS, FIB,…)	C:¥ProgramData¥Carl Zeiss¥SmartSEM¥Log
Light microscopes	remote service.log.xml	Already parsed information from ZEN.log.xml and ZENCore.log.xml	C:¥ProgramData¥Carl Zeiss¥Remote Service¥remote service.log.xml
Light microscopes	ZEN.log.xml	Information about ZEN software	C:¥ProgramData¥Carl Zeiss¥Logging
Light microscopes	ZENCore.log.xml	Information about ZEN files Core software	C:¥ProgramData¥Carl Zeiss¥Logging
X-ray microscopes	XradiaAppn.log where n=1,2,….N used in system software v11.1 XradiaApp_n.log where n=1,2,….N used in system software v12	Information about Versa system parameters	C:¥Program Files¥Carl Zeiss X-ray Microscopy¥Xradia Versa¥XX.X.XXXX.XXXXX¥Log Files
X-ray microscopes	Centre.log Comms.log FilStore.log Getter.log Healthcheck.log Serial.log TCC.log Tube.log Vac.log Warm.log	X-ray source logs	C:¥Program Files¥Carl Zeiss X-ray Microscopy¥Xradia Versa¥XX.X.XXXX.XXXXX¥logs

表1 ログファイルの概要

Installation

お客様またはお客様のIT部門によるPredictive Serviceの承認後にZEISSの顕微鏡を接続する方法は2つあります。前提条件として、お客様のシステムがすべてのセキュリティ対策（ウイルス対策ソフトウェアなど）を実施し、インターネットに接続されている必要があります。データ セキュリティに関する当社の推奨事項も参照してください。

1. TeamViewerリモート デスクトップ共有を利用したインストール（当社推奨）

- 必要とされるすべての情報およびドキュメントがZEISSに送信され、リモートインストールセッションのスケジュールが設定されます。必要とされる特定のプロキシ設定があるかどうかもお知らせください。プロキシ設定がある場合は、インストールにその設定を利用できるようにしてください。
- TeamViewer Quick Supportソフトウェアをダウンロードするためのリンクが記載された電子メールがZEISSのサービス部から届きます。このソフトウェアはお客様のPCにはテンポラリーでインストールされる点に注意してください。
- TeamViewer Quick Supportソフトウェアを起動し、TeamViewerセッションリクエストとリモートコントロールの要求を受け入れます。
- ZEISSの技術サポートがZEISS Predictive Service Agentをインストールします。
- エージェントソフトウェアとエンタープライズ サーバーの間の接続が確立されたかどうかをテストします。

TeamViewerのセキュリティの詳細情報については、以下を参照してください：
https://dl.tvcdn.de/docs/en/TeamViewer-Security-Statement-en.pdf

2. フィールド サービス エンジニアによるインストール

- 必要とされるすべての情報およびドキュメントがZEISSに送信され、リモートインストールセッションのスケジュールが設定されます。必要とされる特定のプロキシ設定があるかどうかもお知らせください。プロキシ設定がある場合は、インストールにその設定を利用できるようにしてください。
- ZEISSのフィールド サービス エンジニアがZEISS Predictive Service Agentをインストールします。
- エージェントソフトウェアとエンタープライズサーバーの間の接続が確立されたかどうかをテストします。

Technical facts

Ports	443
Protocols	HTTPS, Secure Websocket
URL of ZEISS server	predictive-service.zeiss.com www.predictive-service.zeiss.com
IP addresses	52.174.243.245
Certification of Microsoft Azure cloud infrastructure	ISO 27001, HIPAA, FedRAMP, SOC1 and SOC2
Connection security	TLS 1.2 with AES 256bit
Supported proxy settings for installation	- No authentication - Basic authentication - Digest authentication - NTLM authentication
Available and patched local area network connected to ZEISS system PC	RJ 45 connector for LAN
Security patched and measures according to your local IT security standards	e.g. installing antivirus software; please see recommendations for data security policy on ZEISS Microscopy Systems (see references)
Established and working outbound internet connection	

参考資料

ZEISS Microscopy Systemsに関するデータ セキュリティ ポリシーの推奨事項
AGB 一般取引条件 Predictive Service

※設計、納期および技術的仕様は予告なく変更されることがあります。

カールツァイス株式会社
マイクロスコピーディビジョン

〒160-0003
東京都新宿区四谷本塩町2番8号
Tel 03-3355-0332
Fax 03-3359-2118

大阪営業所　Tel 06-6337-5465
名古屋営業所　Tel 052-777-1415
福岡営業所　Tel 092-713-7662
仙台営業所　Tel 022-224-5655

microscopy.ja@zeiss.com
www.zeiss.co.jp/microscopy