IoTセキュリティソリューション
～スタンドアロン端末のネットワーク化～

CYTHEMIS™のご紹介 補足資料

TOSHIBA

東芝インフラシステムズ株式会社
セキュリティ・自動化システム事業部
2021.10.6

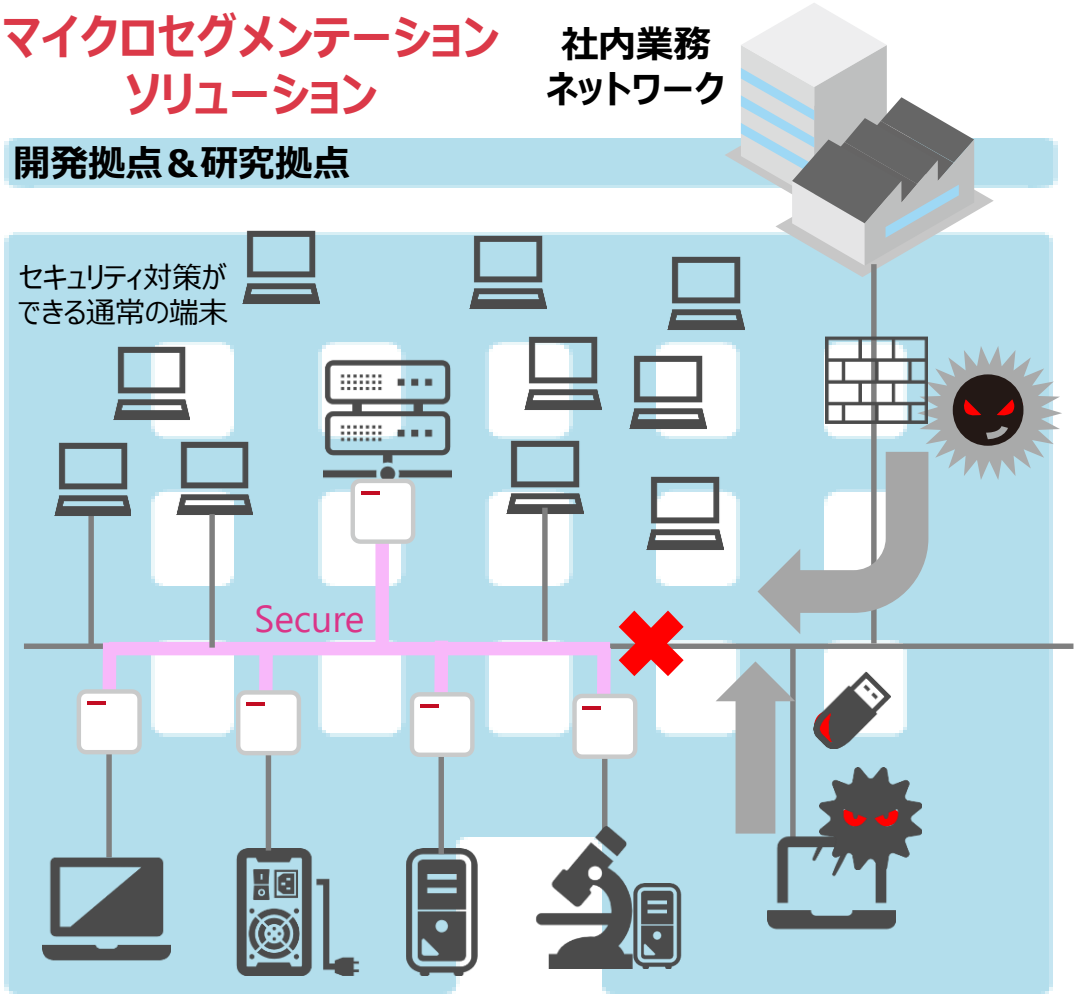
01

CYTHEMIS™ のご紹介

CYTHEMIS ・・・外付けのセキュリティデバイス群とそれらを管理するシステム

認証技術で、様々なセキュリティ脅威を遮断しながら
“つなぎたい端末だけをセキュアに接続することができる” セキュリティソリューション

マイクロセグメンテーション ソリューション



エンドポイント (PCを含む研究・開発施設内のセキュリティ対策ができない端末)

手軽に導入

セキュアに
つなげる

＜想定脅威＞
USBメモリ経由、標的型攻撃による社内感染
端末経由でのマルウェア・ランサムウェア感染、
イントラネット内部からの不正アクセス、
不本意なアップデートなど

＜エンドポイントの例＞
開発用PC、実験・計測用端末、シミュレーション端末、
大型計測装置管理端末、研究装置管理端末、
医療機器など

名称の由来

CYTHEMIS™

CYTHEMIS(サイテミス)は、CYBER(サイバー)とTHEMIS(テミス)の造語。

THEMISは、ギリシャ神話の『法、秩序、掟、正義の女神』。

彼女が手に持つ天秤は正邪を測る「正義」を、剣は「力」を象徴し、「剣なき秤は無力、秤なき剣は暴力」に過ぎず、正義と力が法、秩序の両輪であることを表している。

これに対応して、機器認証を実施するデバイスを天秤、プライベートCAなど強力な権限機能をもつ管理サーバを剣、に見立てる。

手軽に導入できる理由①デバイス：設置の容易さ

エンドポイント自体には手を付けず、セキュリティ対策を施します。
エンドポイントのイーサネットの口に外付けのデバイスをはさんでもらうだけです。
様々なセキュリティ機能を集約、外出しにし、セキュリティ状態を常に最新に保つことで、お客様のエンドポイントを各種マルウェアやランサムウェアから守ったり、各種セキュリティ機能を代行します。

コスト削減

PKIベースの高いセキュリティでカバーされる、様々なセキュリティ対策のコストを抑えることができます。

※PKI･･･Public Key Infrastructure

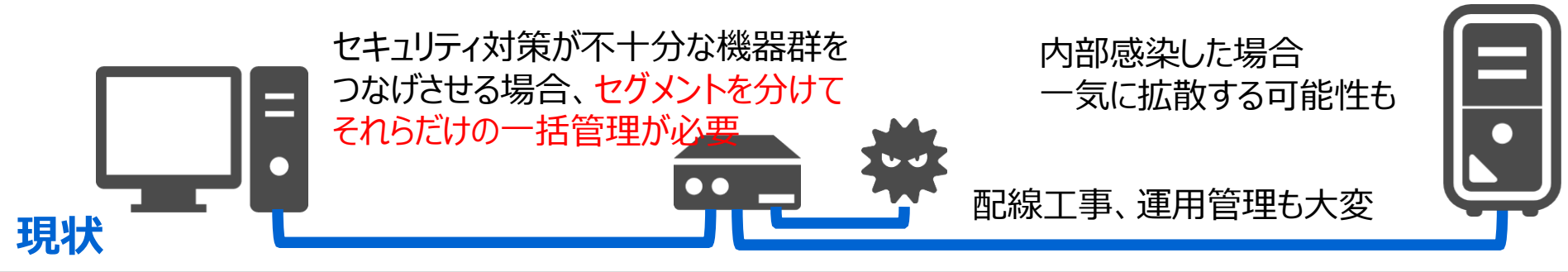
手間要らず

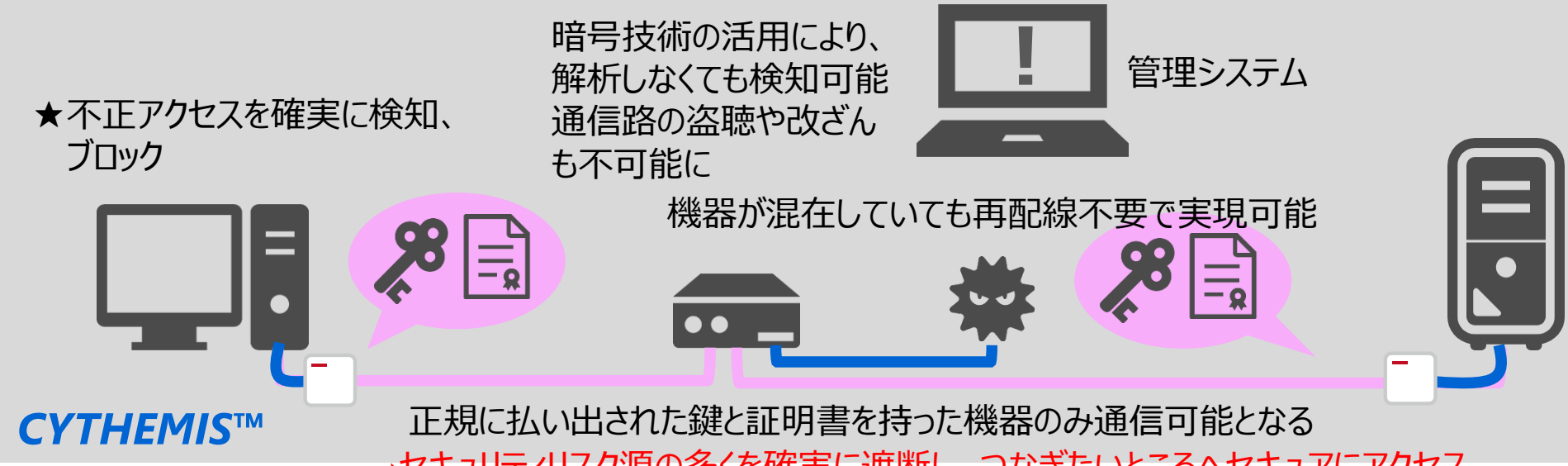
PKIベースのセキュリティに必要な鍵や証明書の発行、書込み、管理の手間が不要で、パスワードベースではない、**セキュアな機器認証が実現**できます。

セキュアにつなげる理由①機器認証

PKIベースの暗号技術を利用し、相互認証※が成功した場合しか通信しないので、
想定外のアクセスは全て除外することができます。
通信先が限定されているユースケースならではのアプローチです。

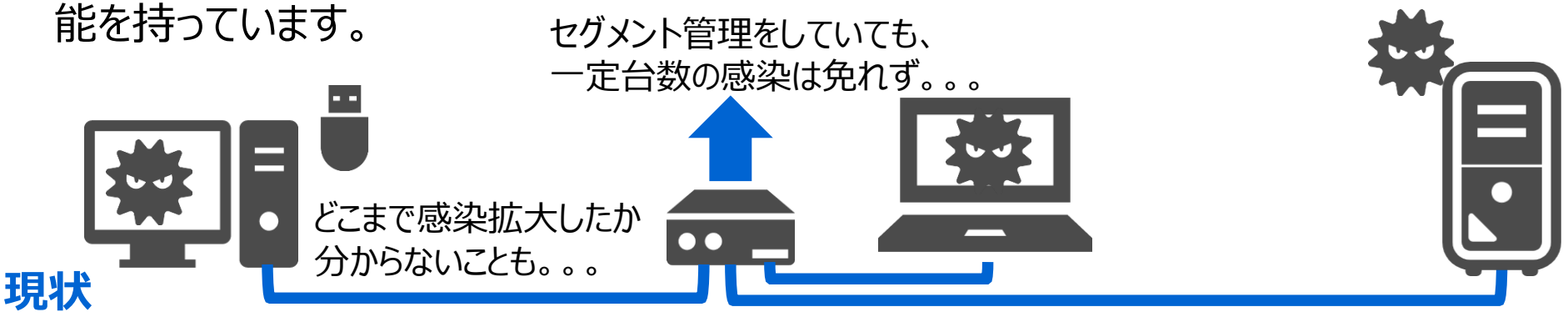
※通信の送信元、送信先の正当性を暗号技術を使い、厳格に確認。なりすましは不可能

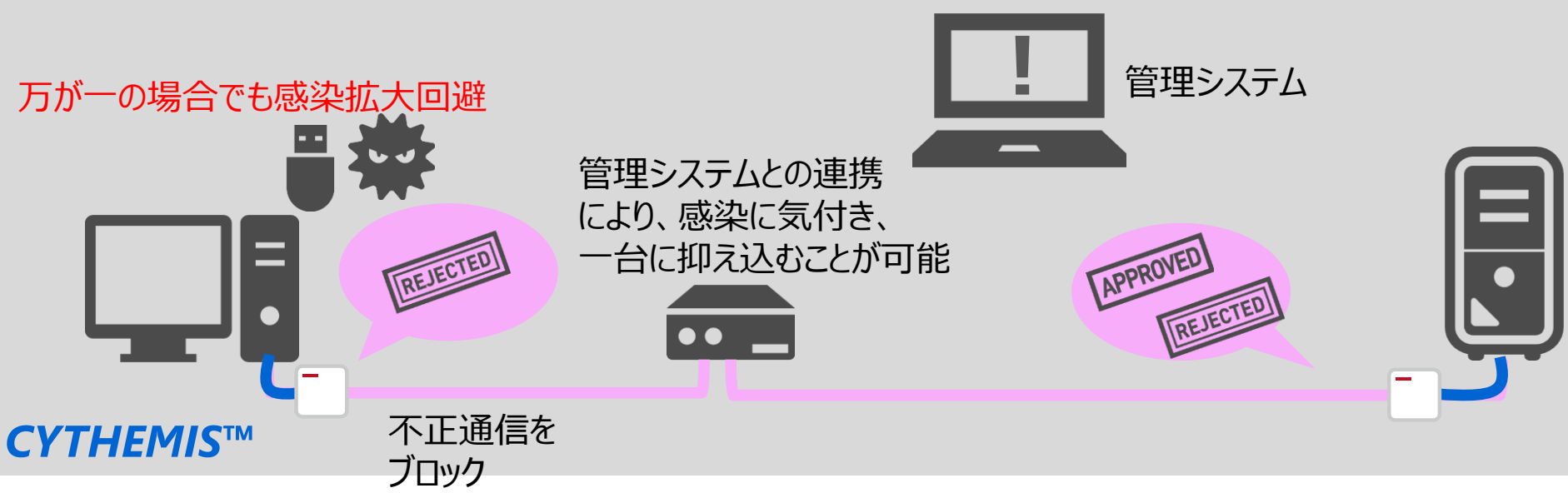




セキュアにつなげる理由②ホワイトリスト

エンドポイントのネットワークの入口で守っていても、USBメモリなどを使って、後ろからマルウェアに感染してしまう可能性も残されています。そのために、ホワイトリストの機能を持っています。





セキュアにつなげる理由③鍵管理専用ハードウェア

国際的なセキュリティ規格の認証であるCommon Criteriaや米国連邦標準FIPS140-2に適合したハードウェアを使い、セキュアに鍵管理を行います。
管理システムに利用するHSMや、外付けデバイスに実装されているSAMは、非常に高い耐タンパ性を持ち、内部の情報を解析、改ざんすることが非常に難しいセキュリティ製品です。

※Common Criteria・・・ISO/IEC15408セキュリティ製品の認証スキーム

暗号技術を使っても、鍵が漏洩してしまっては全く意味がありません

HSM Hardware Security Module

システム側の鍵管理をがっちり行うために必要な装置。鍵を払い出す管理システム側でのセキュアな鍵管理が必要なサービスで活用しています。

SAM Secure Application Module

デバイス側の鍵管理をがっちり行うために必要なデバイス。鍵の漏洩を防止し、なりすましができないようにしています。デバイス側は、物理的にアクセスできるという意味で、システム側以上に鍵への脅威が増すため、このデバイスの活用が有効です。

手軽に導入できる理由②管理システム：設定・管理の容易さ

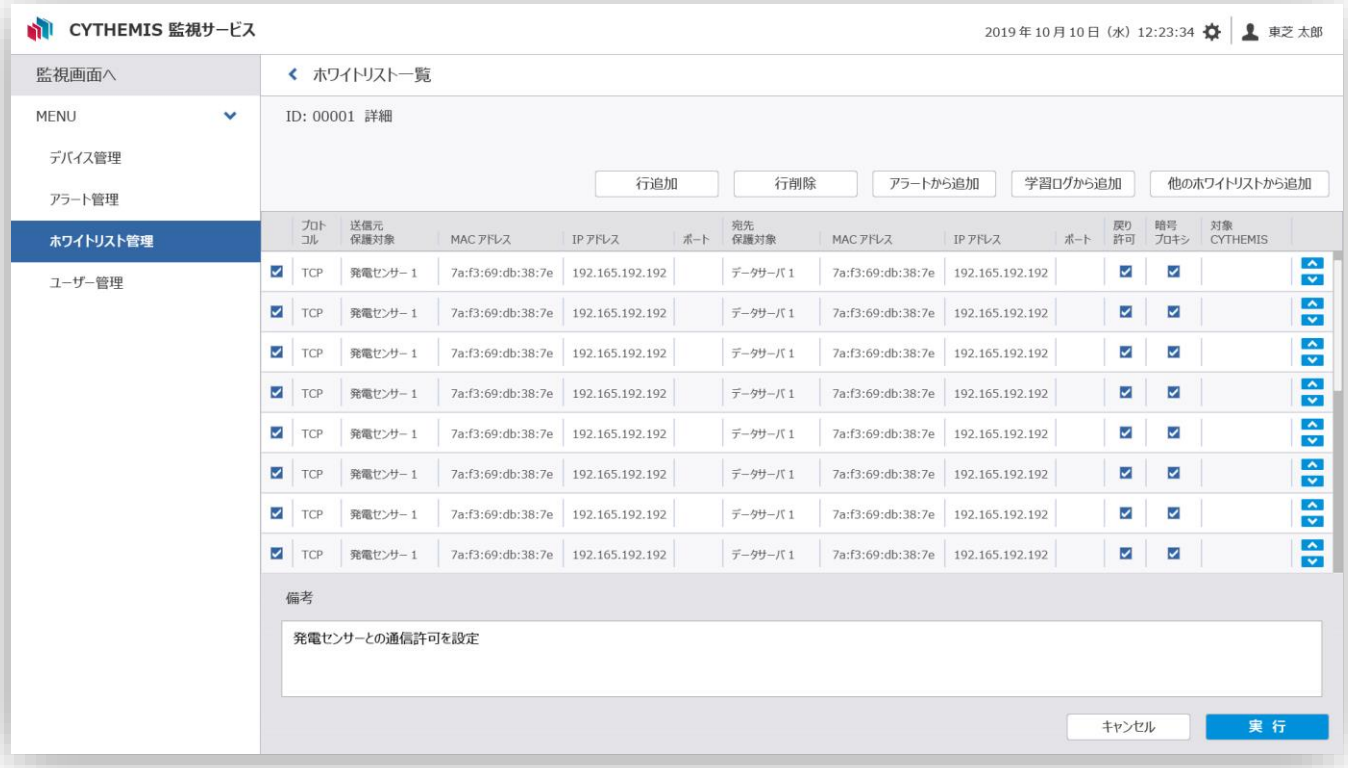
管理システム

- ネットワークの見える化
- インシデントの見える化
- エンドポイントの資産管理
- ホワイトリストの一元管理

不正アクセス発生時は、ポップアップで即座に
通知。指定メールアドレスに送付も可能

手軽に導入できる理由③管理システム：４つのモード

パススルーモード	CYTHEMISをつけてないのと同じ状態。初期設定時、メンテナンス時などに利用
学習モード	状態としてはパススルーと同じだが、デバイスを流れる通信をキャプチャし、CYTHEMIS適用ネットワーク全体のホワイトリストを自動作成。学習時間を設定可能。
IDSモード	ホワイトリストに載っていない通信を不正アクセスとみなし、検知し、アラームを上げる。
IPSモード	ホワイトリストに載っていない通信を不正アクセスとみなし、検知し、アラームを上げ、その通信を遮断する。



ホワイトリスト設定

通信毎にTLS ON/OFF可能

IPアドレス、ポート毎に記載可能

送信元はワイルドカード可能

グループ毎にファイルを分けて記載可能

他のソリューションとの比較

ウィルス対策ソフトやEDRに近い位置づけ

装置を守る

ゾーンを守る

	CYTHEMIS	ファイアウォール UTM	windows標準 ファイアウォール
脅威			
マルウェア	○ 外部・内部からも 感染をブロック	△ セグメント内部からの 感染は回避不可	× OS上で動作しているため、 感染してしまうと無効化も
なりすまし	○ 相互認証で なりすましも防御	× IPアドレス改ざんされると ブロック不可	× IPアドレス改ざんされると ブロック不可
盗聴・改ざん	○ 通信データの暗号化により データ改ざんもブロック	×	×
運用			
通信先制御	○ 管理システムで 一元管理可能	△ セグメント内部までは 不可能	△ アプリケーション毎はできても 細かい制御は難しい
不正アクセス検知	○	△ 管理ツールが別途必要	× 特になし
エンドユーザによる 設定変更	○ 管理者のみ	○ 管理者のみ	× 付与権限によっては 変更可能

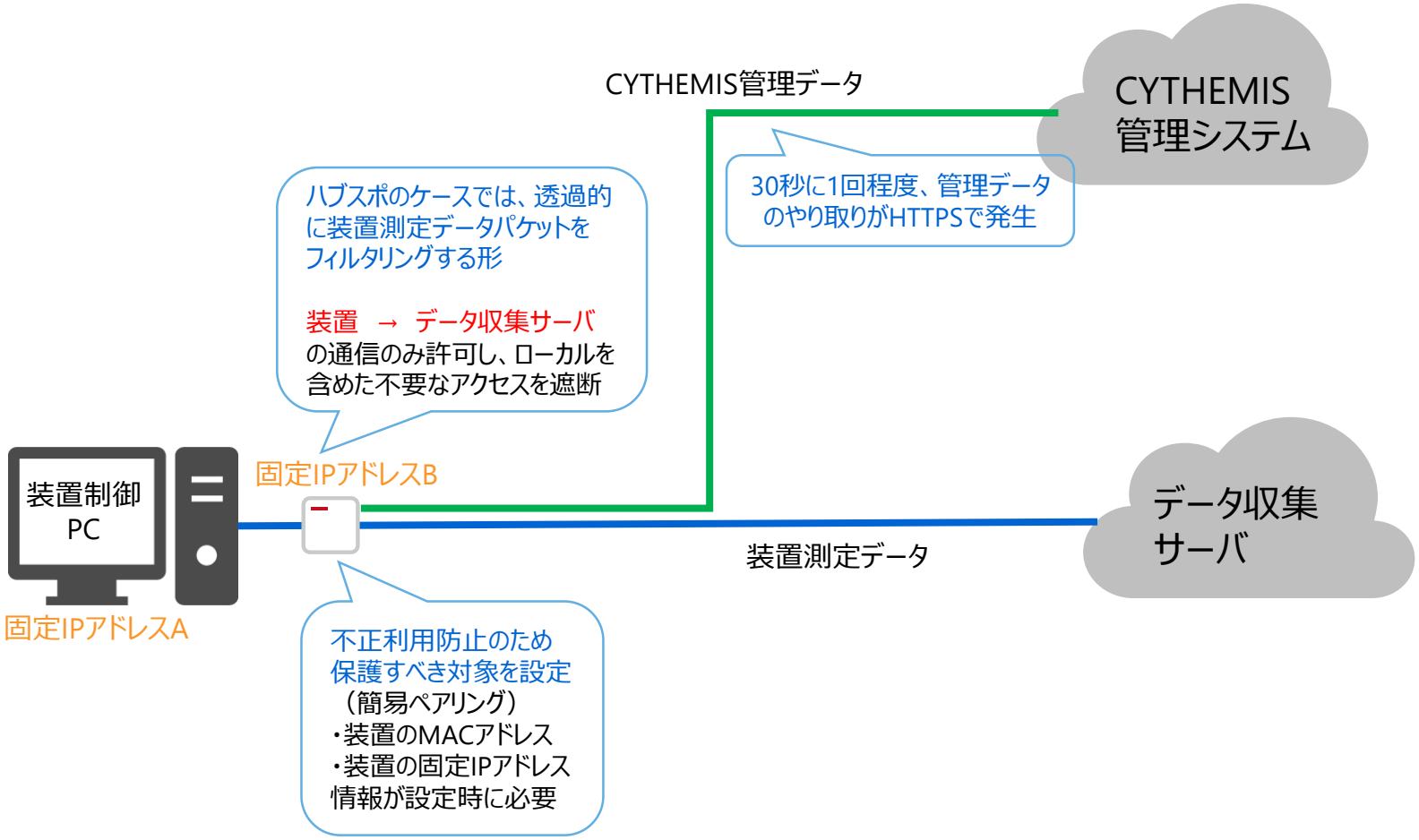
仕様一覧

項目	仕様
対応プロトコル	TCP, UDP上で動作するアプリケーションプロトコル
準拠仕様	TLS 1.2 IEEE 802.21 （マルチキャスト用グループ鍵管理技術）
インターフェース	イーサネット
スループット	約70Mbps
管理デバイス最大数	200台
セキュリティ認定	Common Criteria （ISO/IEC 15408）取得予定
電源	AC100V 50/60Hz
動作温度	0°C ～ 50°C
デバイスサイズ	幅 84mm × 奥行 84mm × 高さ 38mm
今後の拡張機能	高速化

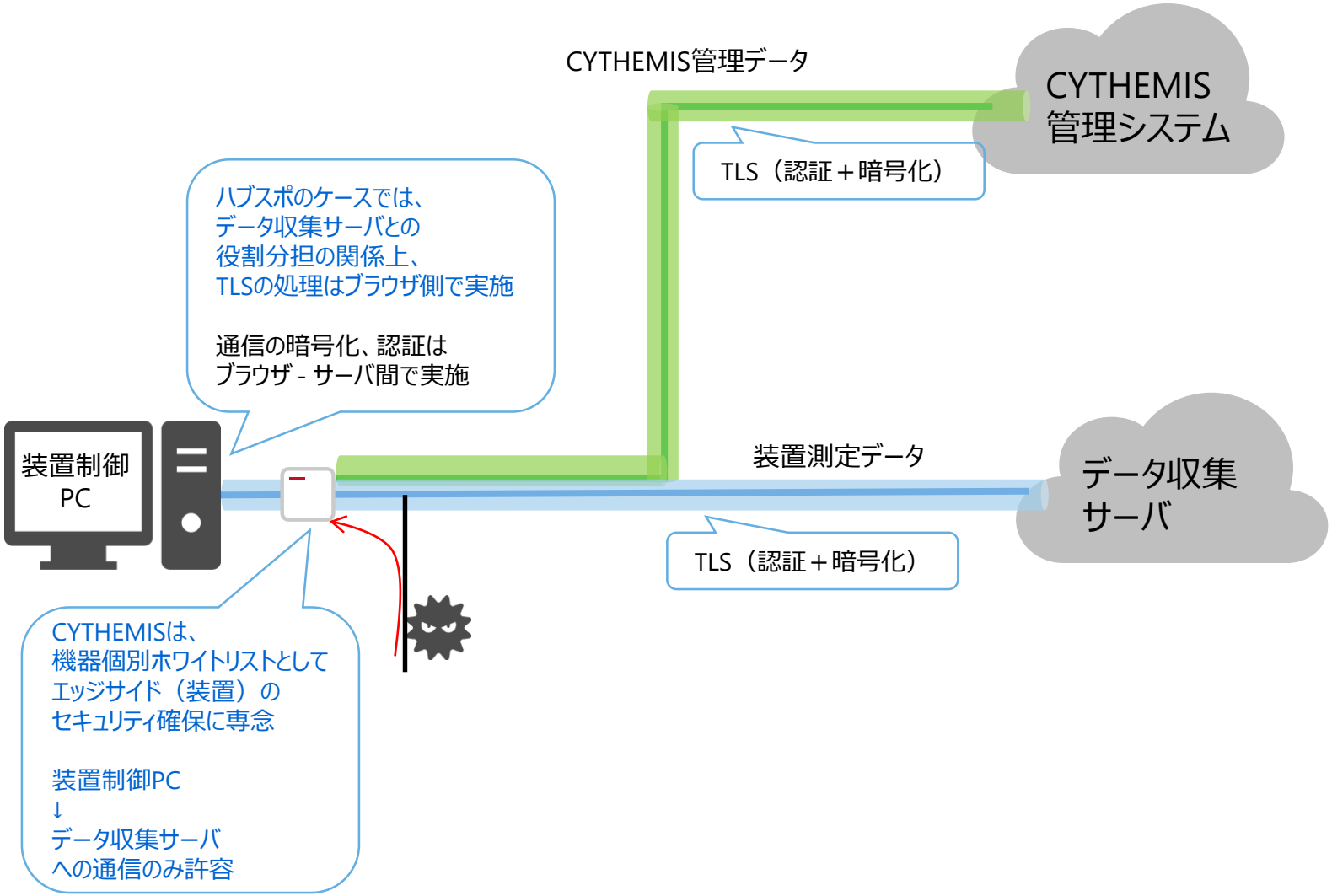
02

ハブアンドスポークでの制約について

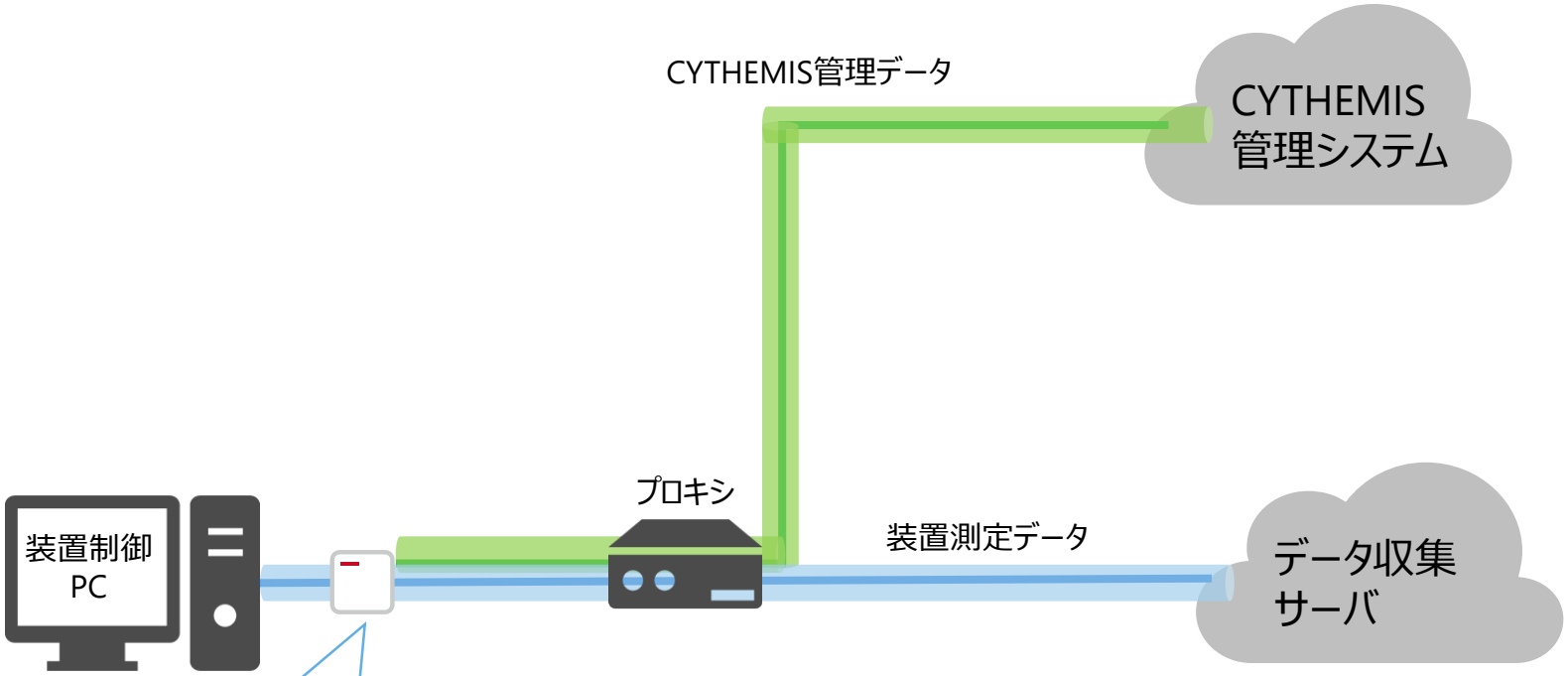
装置とCYTHEMISデバイスの関係



セキュリティ機能の棲み分け



NAT/NAPT制約について



現状は、IPアドレスでしか指定できないため、
プロキシ経由だと、外部への通信をほぼ許容
することになるため、NAT/NAPT制約をお願いしています。

今後、FQDNでも指定できるようにし、プロキシ利用でも
問題ないように改造を予定しています。

03

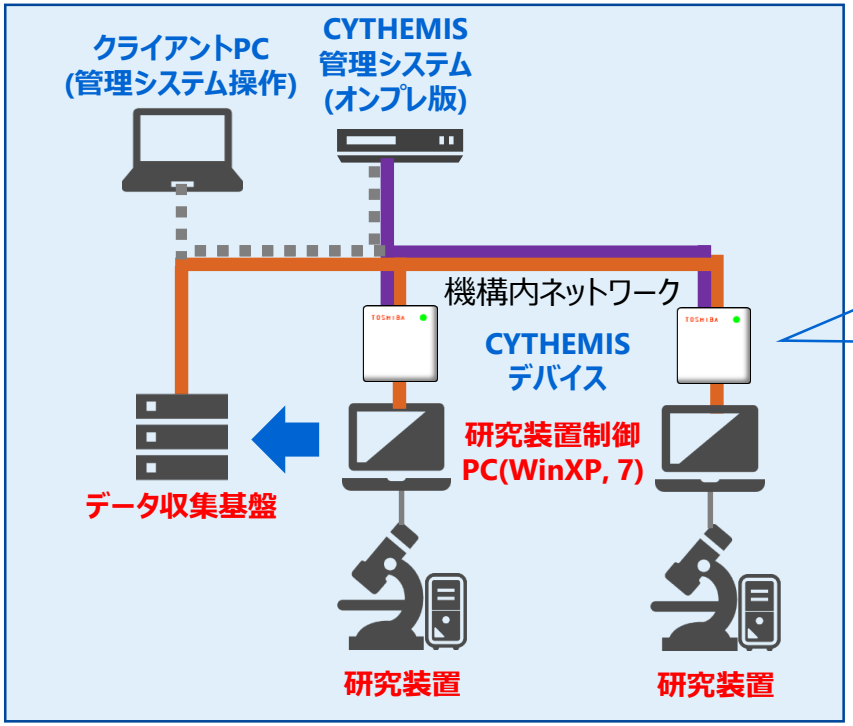
ユースケース

NIMS様オンプレ　①研究装置のIoT化

研究装置制御PC　→　オンプレミスデータ収集基盤　データ転送

CYTHEMISデバイス管理
CYTHEMIS管理システム操作
データ転送（研究装置制御PC　→　データ収集基盤）

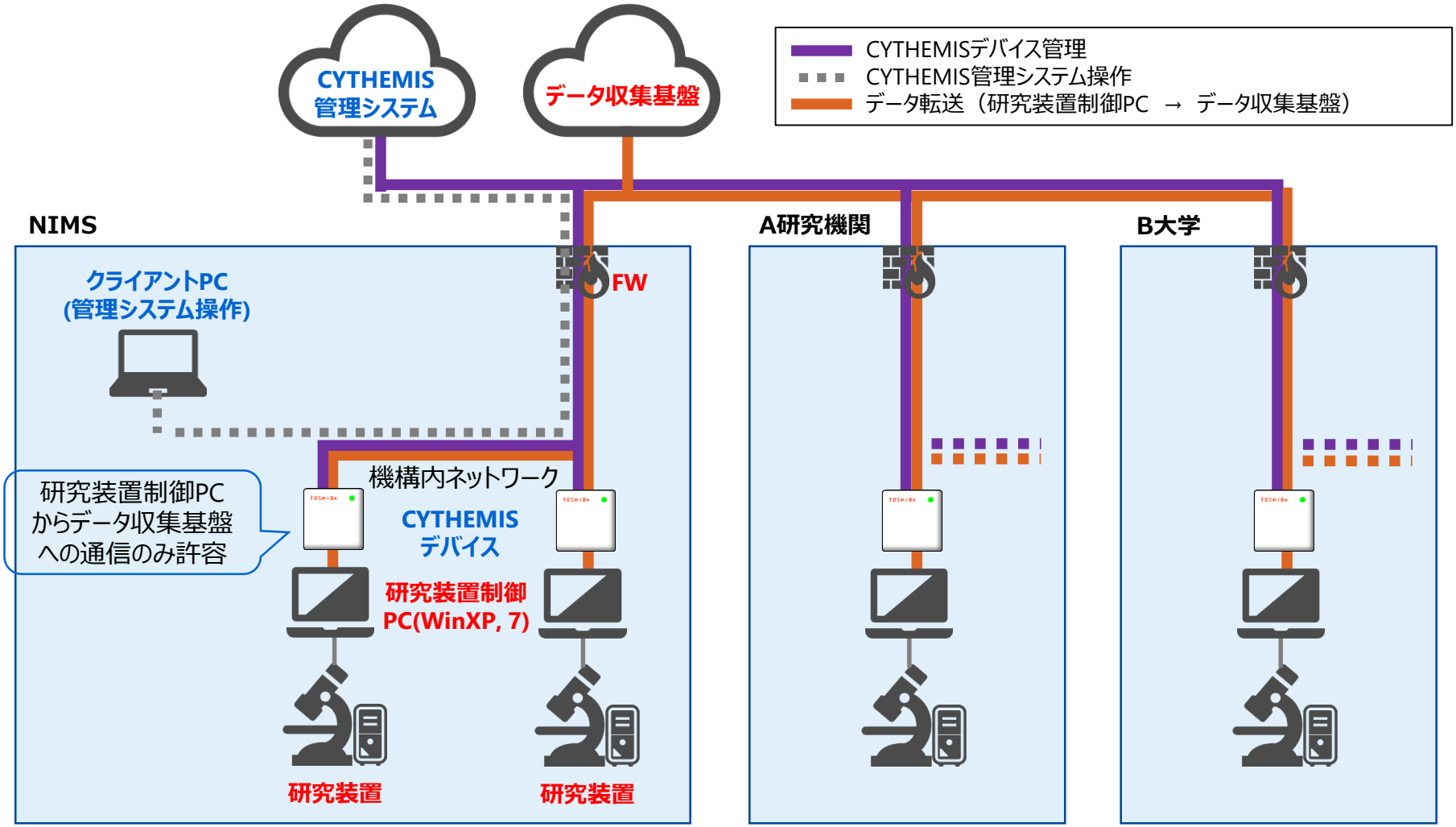
NIMS



研究装置制御PCからデータ収集基盤への通信のみ許容

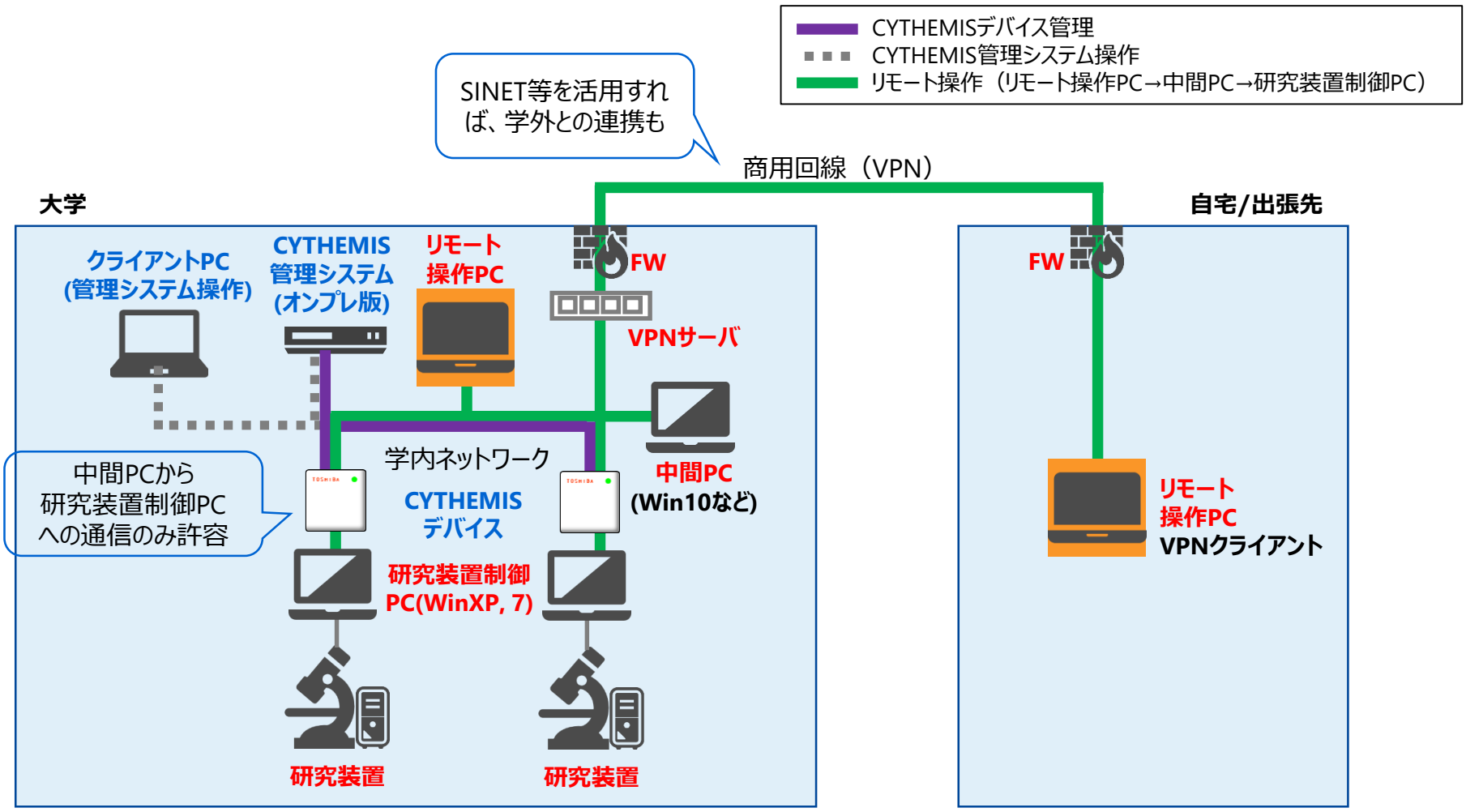
ハブ&スポーク　②複数拠点にまたがる研究装置のIoT化

研究装置制御PC　→　クラウドデータ収集基盤　データ転送



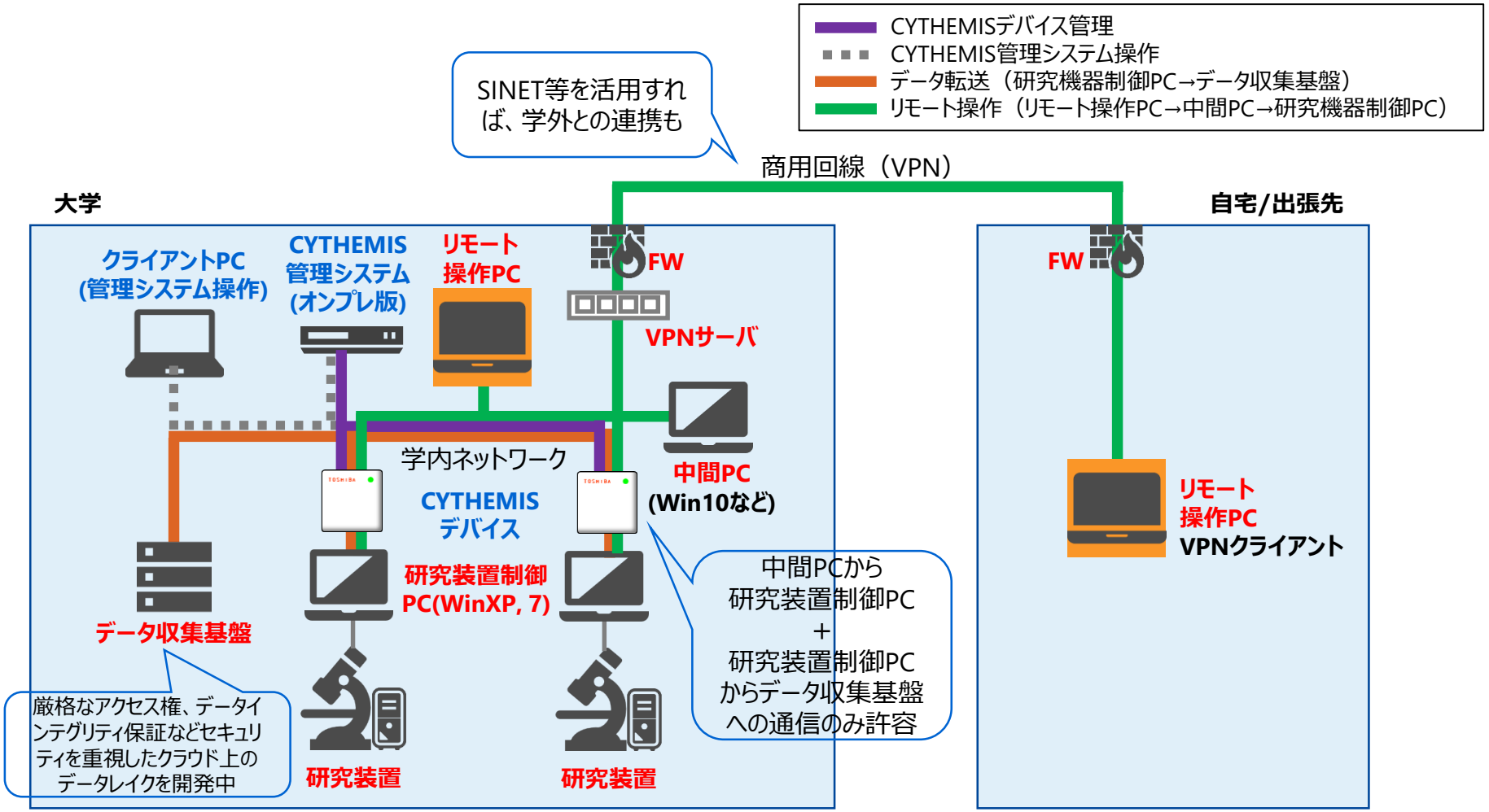
大学研究室・企業（物性系、サイエンス系）　③装置のリモート操作

リモート操作PC → (中間PC) → 研究装置制御PC リモート操作



大学研究室・企業（物性系、サイエンス系）　④装置のリモート操作+データ転送

リモート操作PC → (中間PC) → 研究装置制御PC リモート操作
研究装置制御PC → オンプレミスデータ収集基盤 データ転送



TOSHIBA

ご清聴ありがとうございました