OPC UAを用いた
工場設備のGAIA-X接続検証について

1.GAIA-Xとサイバーセキュリティの必要性
2.GAIA-Xの通信テスト及び必要なセキュリティ対策
3.まとめ

2022年12月9日
オークマ株式会社
情報システム本部　情報システム部
特別主管技師
情報処理安全確保支援士
長屋　友幸

オークマのご紹介

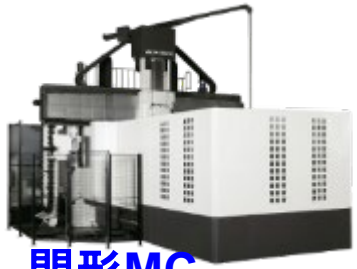
オークマ株式会社　概要

社名	オークマ株式会社
創業	1898年（明治31年）1月　　2022年で124年目
資本金	180億円
従業員	2,310名（連結3,953名）　　2022年3月現在
営業内容	NC工作機械（NC旋盤、複合加工機、マシニングセンタ、NC研削盤）、NC装置、FA製品、サーボモータ、その他、製造・販売
主な海外拠点	アメリカ、ブラジル、オーストラリア、ニュージーランド、ドイツ、オーストリア、ロシア、中国、韓国、タイ、台湾、シンガポール、インドネシア、インド、他

NC旋盤

5軸・複合加工機

立·横MC



門形MC

工作機械の技術の潮流を形成

機電情知融合の先進技術を世界に先駆けて開発
IoTの分野でも世界を牽引

「ないものは創る」

1963 絶対位置検出のNC制御

1972 自動プログラミング機能

1975 ４軸制御旋盤

1981 対話型自動プログラミング機能

1982 加工監視機能

1983 ブラシレスモータ

1984 カラー動画 漢字表示

1987 高速・高精度加工機能

1988 同期制御技術

1989 カム加工機能

1989 AI応用自動プログラミング機能

1991 NC刃物台、NC-ATC

1993 加工管理機能

1997 ネットワーク対応CNC

1998 PREXモータ

2000 ITプラザ

2001 サーモフレンドリーコンセプト

2002 Super NURBS

2004 アンチクラッシュシステム

2008 加エナビ

2009 超高速形状加工機リニアモータ

2012 ファイブチューニング

2013 スマートマシン

2013 スマートファクトリー

2014 サーボナビ

シンクロドライビング

2016 OSP-AI AI機械診断

2017 Connect Plan

2018 ARMROID 超融合ﾛﾎﾞｯﾄ

MU-S600V ﾛﾎﾞｯﾄ機能内包

LASER EX 超複合加工機

2019 3Dキャリブレーション+空間補整

2022 OSP-P500 DXを実現する新CNC

OSP suite

OPC UAを用いた
工場設備のGAIA-X接続検証について

1.GAIA-Xとサイバーセキュリティ対策の必要性
2.GAIA-Xの通信テスト及び必要なセキュリティ対策
3.まとめ

1-1. サイバーセキュリティを前提としたGAIA-X

・昨今、製造現場の設備データをDX(デジタルトランスフォーメーション)に展開し、活用する為にも、**サイバーセキュリティ対策が重要**であると一般的に認識されている。

・その設備自体にサイバーセキュリティ上の脆弱性がある場合は、**脅威リスクが高くなる**ことも一般的に理解されているところである。

・高まっている脅威に呼応するかの様に、サプライチェーンを標的にしたサイバー攻撃が起き、社会インフラに重大なダメージを与える事件が世界中で聞かれる中、そんな脅威に対抗する**欧州ではGAIA－Xを採用した活動**団体が立ち上がっている。

・VEC(Virtual Engineering Community)のIoT／CPS研究分科会で、GAIA－X接続テストWGに参加し、ペネトレーションテストまで実施した接続テストについて報告する。

⇒次頁でGAIA-Xを説明します。 P2/34

1-2.GAIA-Xとは

①審査、認証された者（会社）のみ参加接続可能
②アプリ、データ、通信の取扱いの運用ルール
③運用ルールに加え、用いる技術も指定
④自社は必要な相手（証明書）のみ選択し通信する

欧州地域でGAIA-Xデータセンター構築中

世界中にある欧州企業の会社
ドイツ、フランス、オランダ、ベルギー等
自動車会社、交通機関等のサプライチェーンで構築が進む

⑤取引の為にGAIA-Xへの参加が求められると想定される。

欧州企業と取引のある会社（日本含）

⇒次頁でGAIA-X接続の注意点を説明します。 P3/34

1-3.GAIA-X接続時の注意点

GAIA-Xは、接続が許可された者のみ通信が可能となる一方、GAIA-X内で発生するインシデントは発生元が特定される。

インシデントの発生は故意寓意によらず、接続が停止されビジネスの継続不可リスクが発生する。

インシデントの発生防止、そして一番重要なことは発生時にGAIA-X側にインシデントを拡散を防ぐ必要がある。

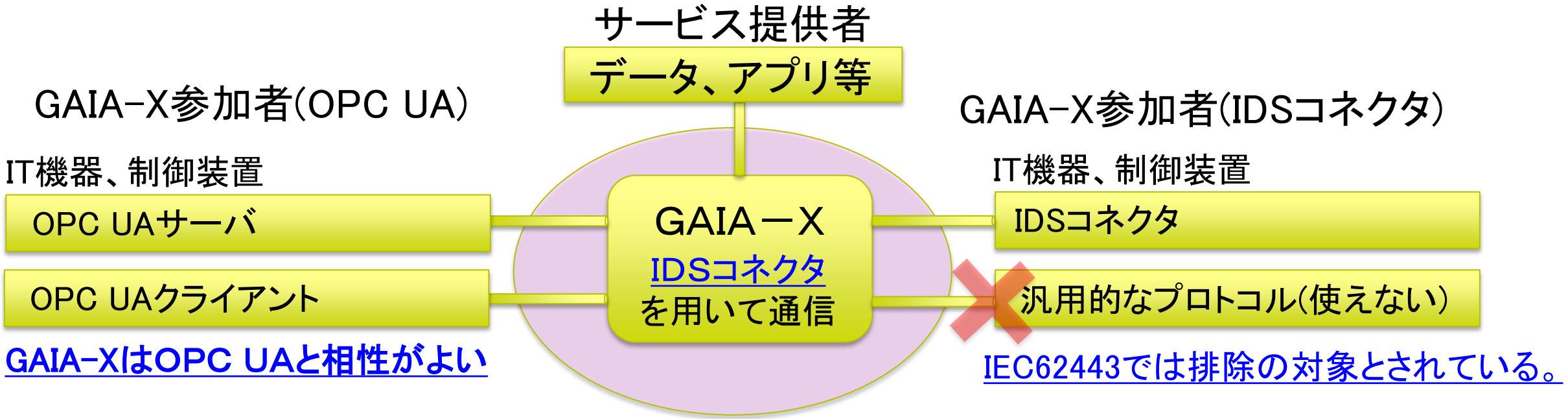
本講演は設備工場及びGAIA-X間の通信テストを通じ、GAIA−Xの技術的理解に加え、セキュリティを重視し、セキュリティ対策の実現性を報告する。

また、情報セキュリティ対策の実現方法においては、スタンダードとして国際規格を意識する。

⇒次頁でGAIA-XとOPC UAについて説明します。 P4/34

1-4.GAIA-X内で役割が増加するOPC UA

- GAIA-XはIDSコネクタというソフトを用いた通信が採用されている。
- ただし、通信仕様はOPC UAであり、OPC UAは工場設備からGAIA-X側への通信機能として用いることができる。
- OPC UA通信の特徴は安全に通信する機能と言える。OPC UAはパスワード通信、証明書通信、暗号通信といった充実した機密データ通信機能を持っている。



網内は通信会社が準備、構内のセキュリティは自社で整備

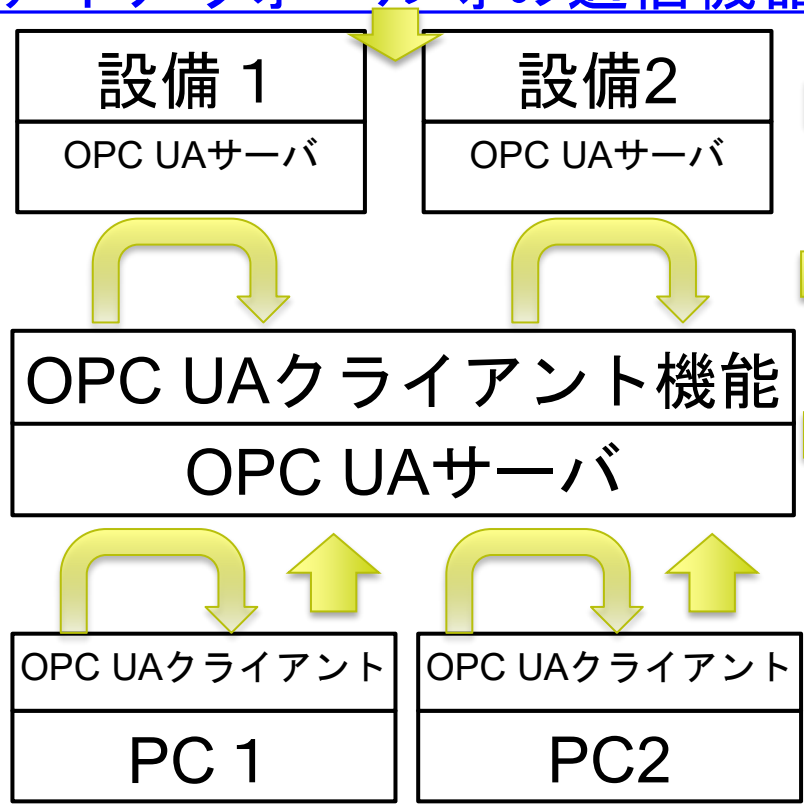
⇒次頁でOPC UAの特徴的な通信を説明します。

1-5.OPC UAの通信の特徴

以下特徴ある通信を理解し、ネットワーク、アプリケーション、データを、配置しシステムを構築することで、様々なセキュリティ対策が可能となる。

OPC UAの通信1ポートでファイル転送やイベント処理等、様々なタイプのデータを送受信可能となるのが特徴である。

ファイアウォール等の通信機器のセキュリティ設定は要注意



理解１：設備は全てOPC UAサーバである

理解2：設備の情報はクライアントから取得する

理解3：２で取得したデータをサーバで公開する

理解４：クライアントからサーバタグに書込可能
クライアント機能は参照のみではない。

GAIA-X接続とその実用性について

1.GAIA-Xとサイバーセキュリティ
2.GAIA-Xの通信テスト及び必要なセキュリティ対策
3.まとめ

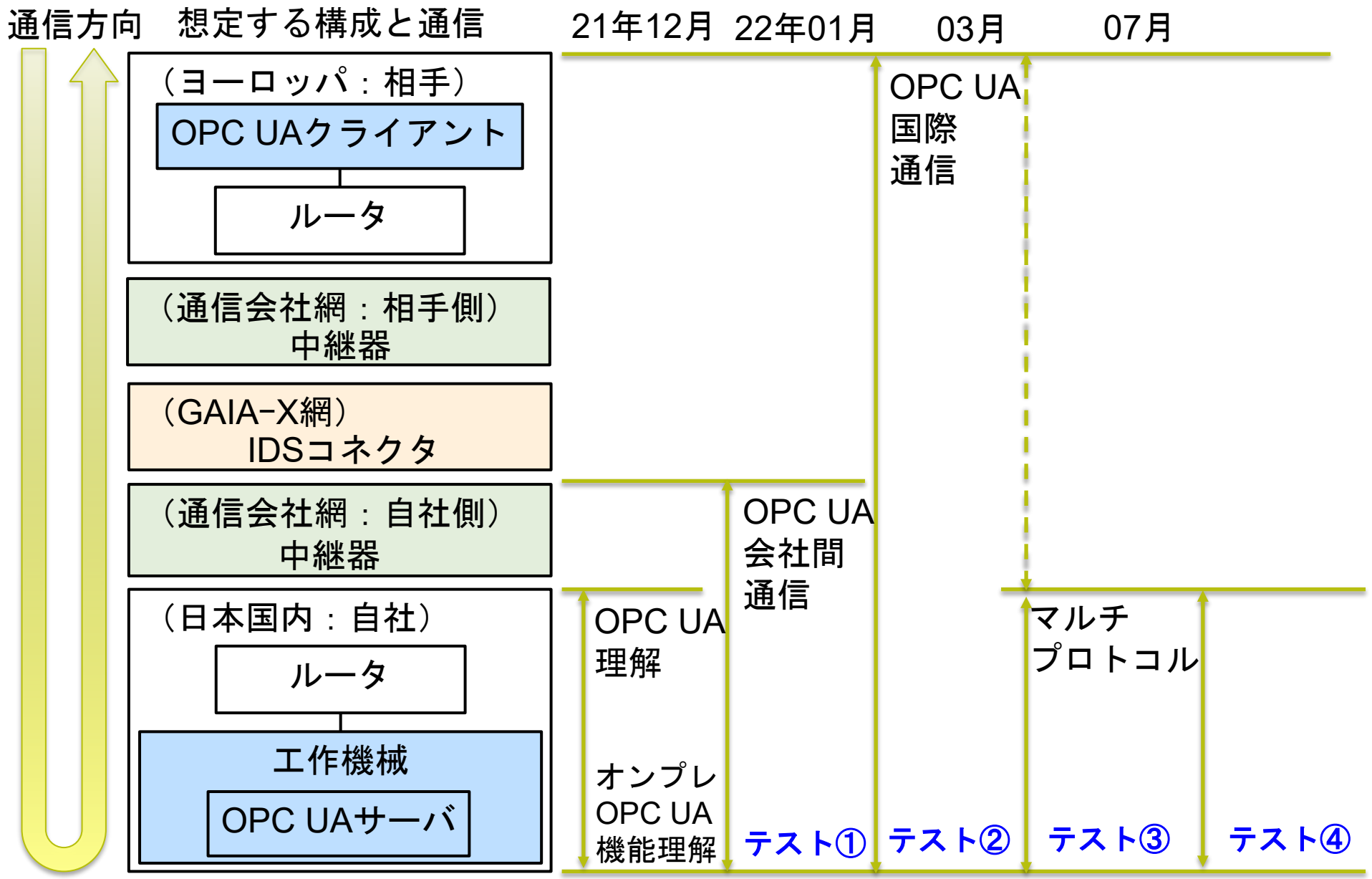
2.GAIA－Xの通信テストの目的

以下テスト①～④を通じ、実際に構築し、可視化する事で、必要な
セキュリティ対策を実証するのが目的である。

2-1.通信中の盗聴や漏洩を防ぐ為に
テスト①暗号化通信での情報交換　を用いる。
2-2.実際の環境を想定し、実用性を計測する為の
テスト②国際通信　を実施する。
2-3.被害対策と加害対策が必要な
テスト③マルチプロトコル通信時に必要なセキュリティ対策　を実現する。
2-4.セキュリティ対策の効果を判定する
テスト④ペネトレーションテスト　を実施する。

⇒次頁から接続テストについて説明します。

GAIA－Xのテスト全体



2-1. テスト①暗号化通信での情報交換

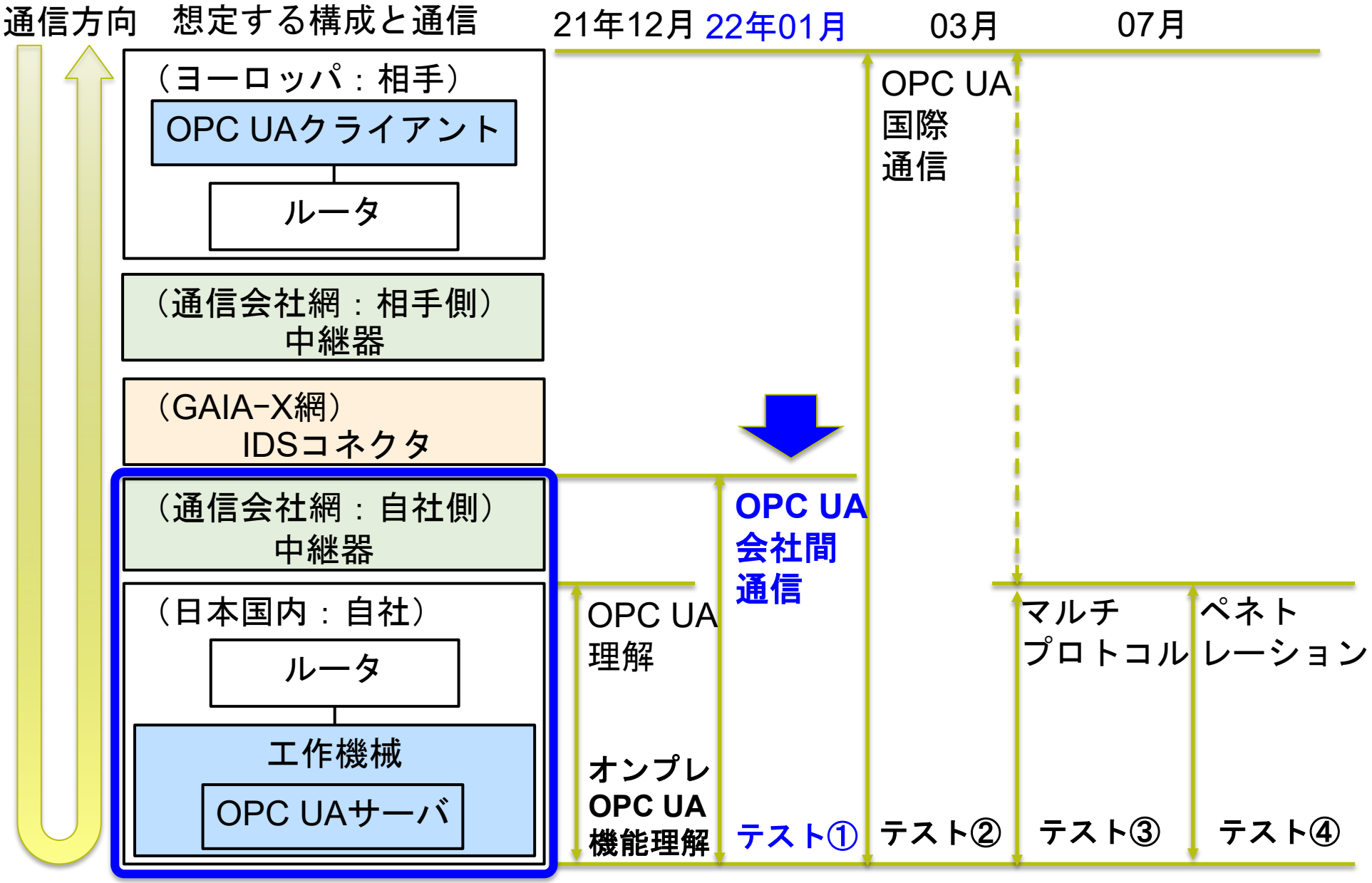
以下3点のテストを通じ、実際に可視化する事で、必要なセキュリティ対策を、設備保守業者、生産技術者、情報技術者間で共有し構築を可能とするのが目的である。
(国際規格IEC62443-3-2の脅威モデル構築時に、脅威を洗い出す必要がある)

2-1.通信中の盗聴や漏洩を防ぐ為に
テスト①暗号化通信での情報交換 を用いる。
2-2.実際の環境を想定し、実用性を計測する為の
テスト②国際通信 を実施する。
2-3.被害対策と加害対策が必要な
テスト③マルチプロトコル通信時に必要なセキュリティ対策 を実現する。
2-4.セキュリティ対策の効果を判定する
テスト④ペネトレーションテスト を実施する。

⇒次頁から接続テスト①について説明します。

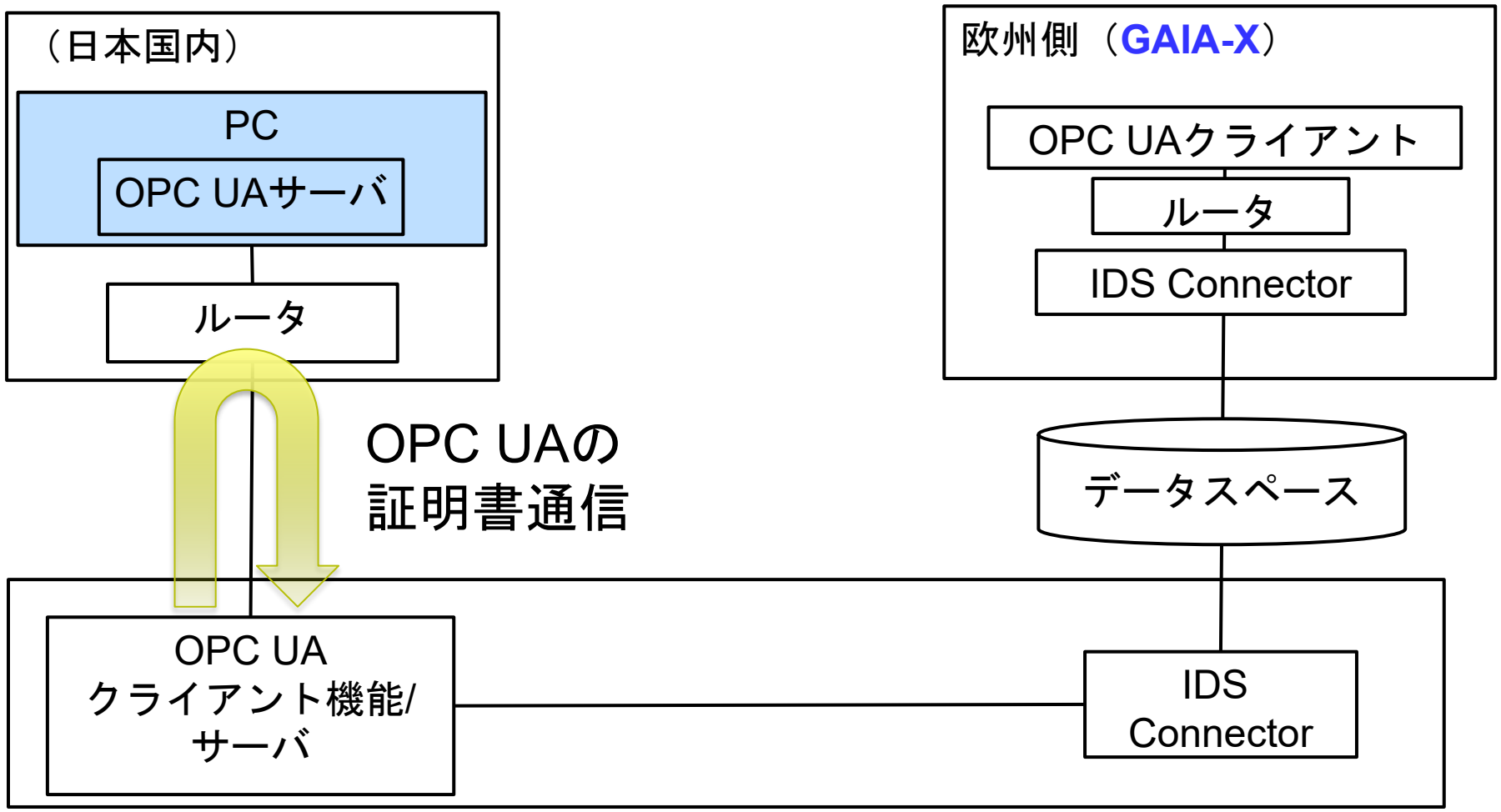
2-1.盗聴や漏洩を防ぐ為のテスト①暗号化通信

OPEN POSSIBILITIES



2-1.盗聴や漏洩を防ぐ為のテスト①暗号化通信

接続テスト環境



接続テスト内容

OPC UAの証明書通信を設定し、OPC UAクライアントから、OPC UAサーバのデータを取得処理できたことを確認

2-1.盗聴や漏洩を防ぐ為のテスト①暗号化通信 （3/3）

盗聴や漏洩を防ぐ為の**①暗号化通信**の結果

・接続テスト
　OPC UAサーバ（PC）で発信するデータを、非暗号及び証明書を用いた
　暗号通信で回線業者側のクライアントアプリ側から取得を実施し、完了した。

・会社間接続
　異なる会社（LAN側、回線業者側）同士の接続は、各文字列や値を厳密に
　合わせ互いに設定する必要があり、コンパニオンスペック（※）の重要性が
　やってみて理解することができた。
（※）OPC UAで使用する設定、値の集合

・OPC UAの知識や通信技術の理解
　OPC UA通信が通常のIT技術者が知識として持つ通信と異なり、OPC UAの
通信機能の特徴が、やってみて理解することができた。

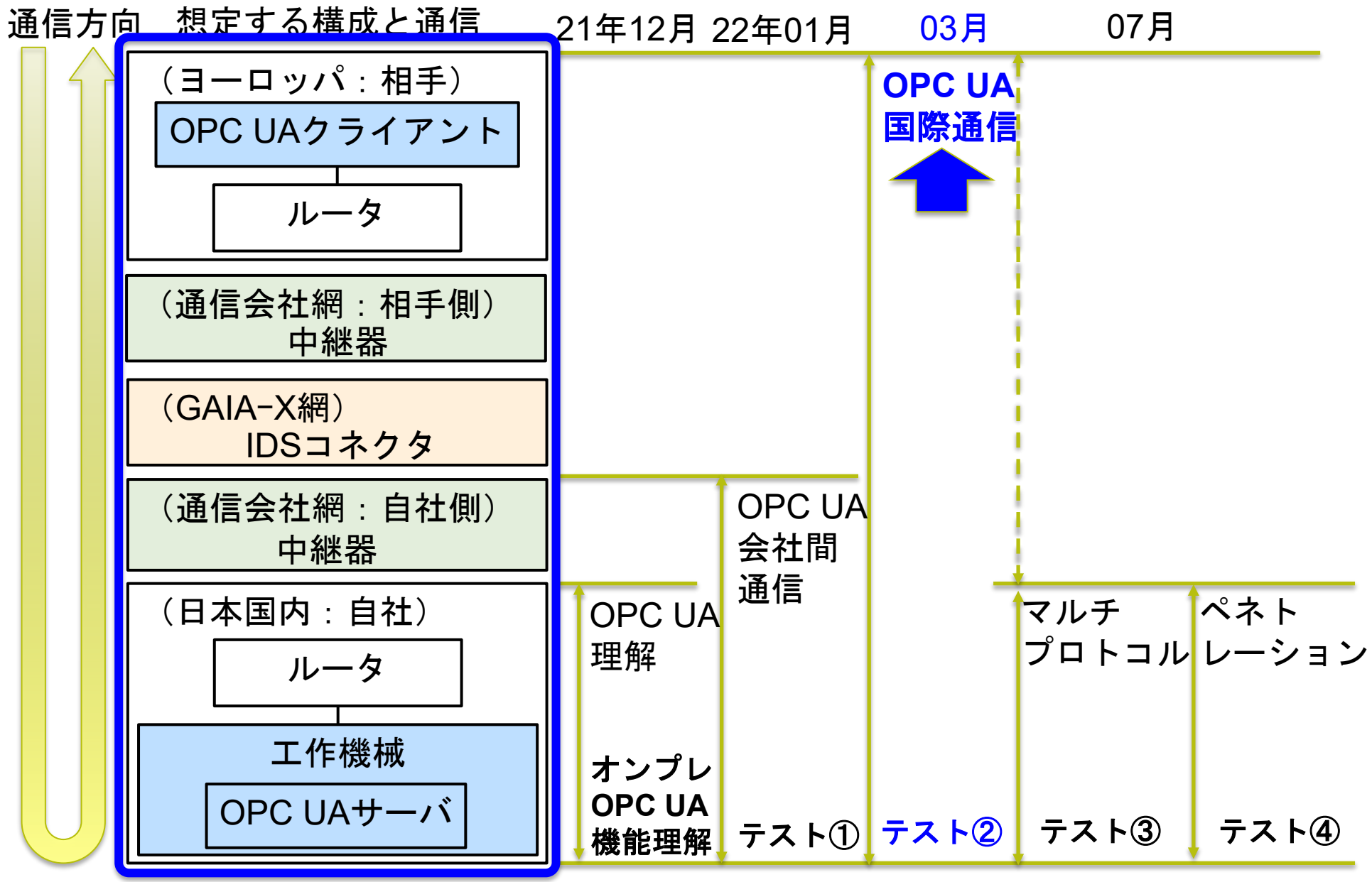
2-2.テスト②国際通信

以下3点のテストを通じ、実際に可視化する事で、必要なセキュリティ対策を、設備保守業者、生産技術者、情報技術者間で共有し構築を可能とするのが目的である。
(国際規格IEC62443-3-2の脅威モデル構築時に、脅威を洗い出す必要がある)

2-1.通信中の盗聴や漏洩を防ぐ為に
テスト①暗号化通信での情報交換 を用いる。
2-2.実際の環境を想定し、実用性を計測する為の
テスト②国際通信 を実施する。
2-3.被害対策と加害対策が必要な
テスト③マルチプロトコル通信時に必要なセキュリティ対策 を実現する。
2-4.セキュリティ対策の効果を判定する
テスト④ペネトレーションテスト を実施する。

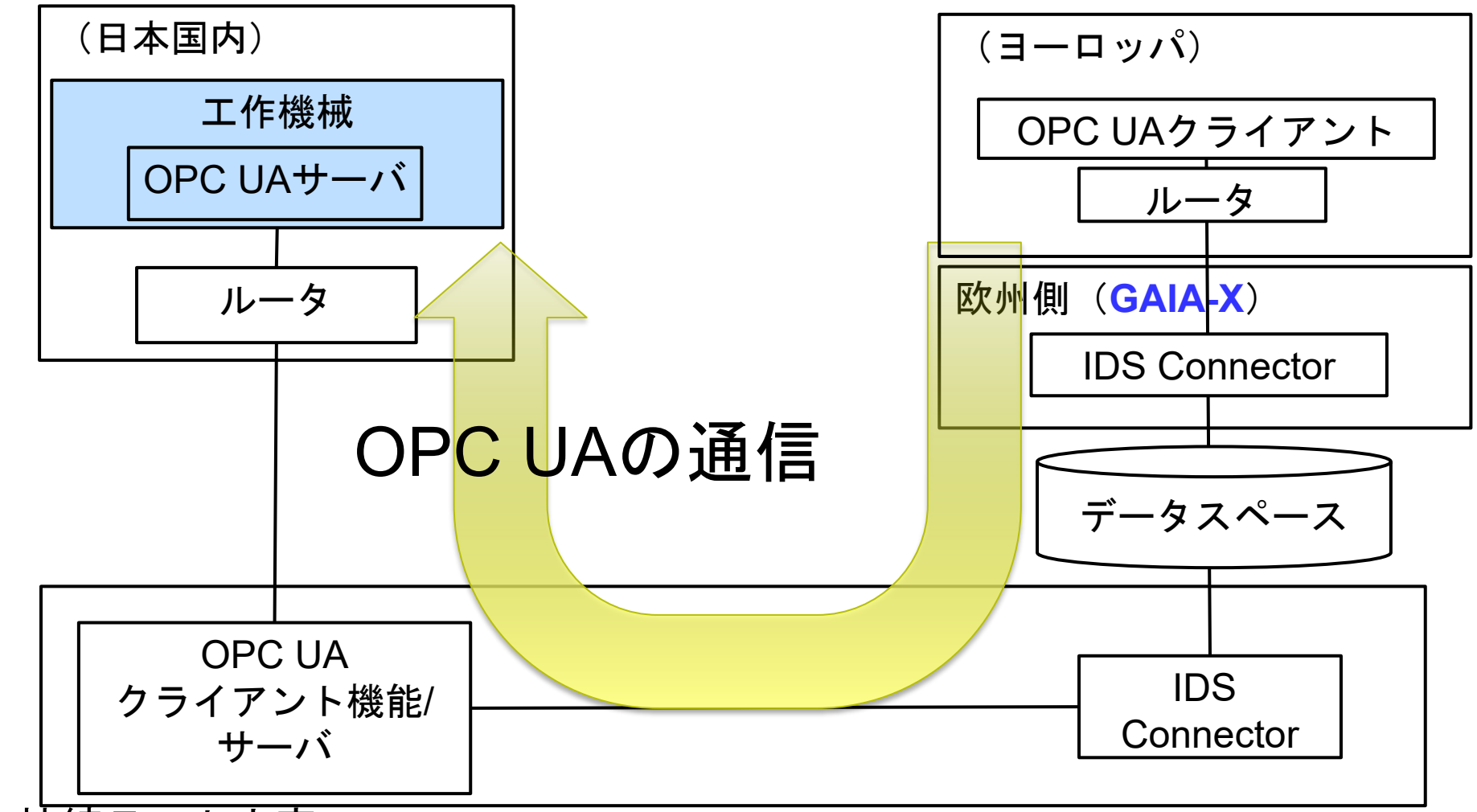
⇒次頁から接続テスト②について説明します。

2-2.実際の環境を想定したテスト②国際通信(1/4)



2-2.実際の環境を想定したテスト②国際通信(2/4)

接続テスト環境



接続テスト内容

OPC UAクライアントから、制御装置のOPC UAサーバからデータを取得処理できたことを確認した。

2-2.実際の環境を想定したテスト②国際通信(3/4)

利用シーンを想定し、実テスト環境を構築し、通信テストを実施した。

実テスト環境

OSP制御装置

PC
OPC UAサーバ/
クライアント

GAIA-X
通信モデム

想定

工作機械
（複数）

中継器

GAIA-X
モデム

2-2.実際の環境を想定したテスト②国際通信(4/4)

②国際通信テストの結果

・テスト①での通信により、特に違和感はなかった。
・心配されていた、データロストや切断は無かった。

・GAIA-X側からの侵入感染、GAIA-X側への感染拡散を防止する構成がビジネスを継続する上で必須となる。
（国際規格であるIEC62443-3-3にも、通信領域をゾーンという単位で区分する条文がある）

上記の理由により、GAIA-X接続をする上で、
テスト③マルチプロトコル通信時に必要なセキュリティ対策、
テスト④③の有効性を評価する　理解が重要である。

工場設備及びマルチプロトコル環境の説明

2-1.通信中の盗聴や漏洩を防ぐ為に
テスト①暗号化通信での情報交換 を用いる。
2-2.実際の環境を想定し、実用性を計測する為の
テスト②国際通信 を実施する。

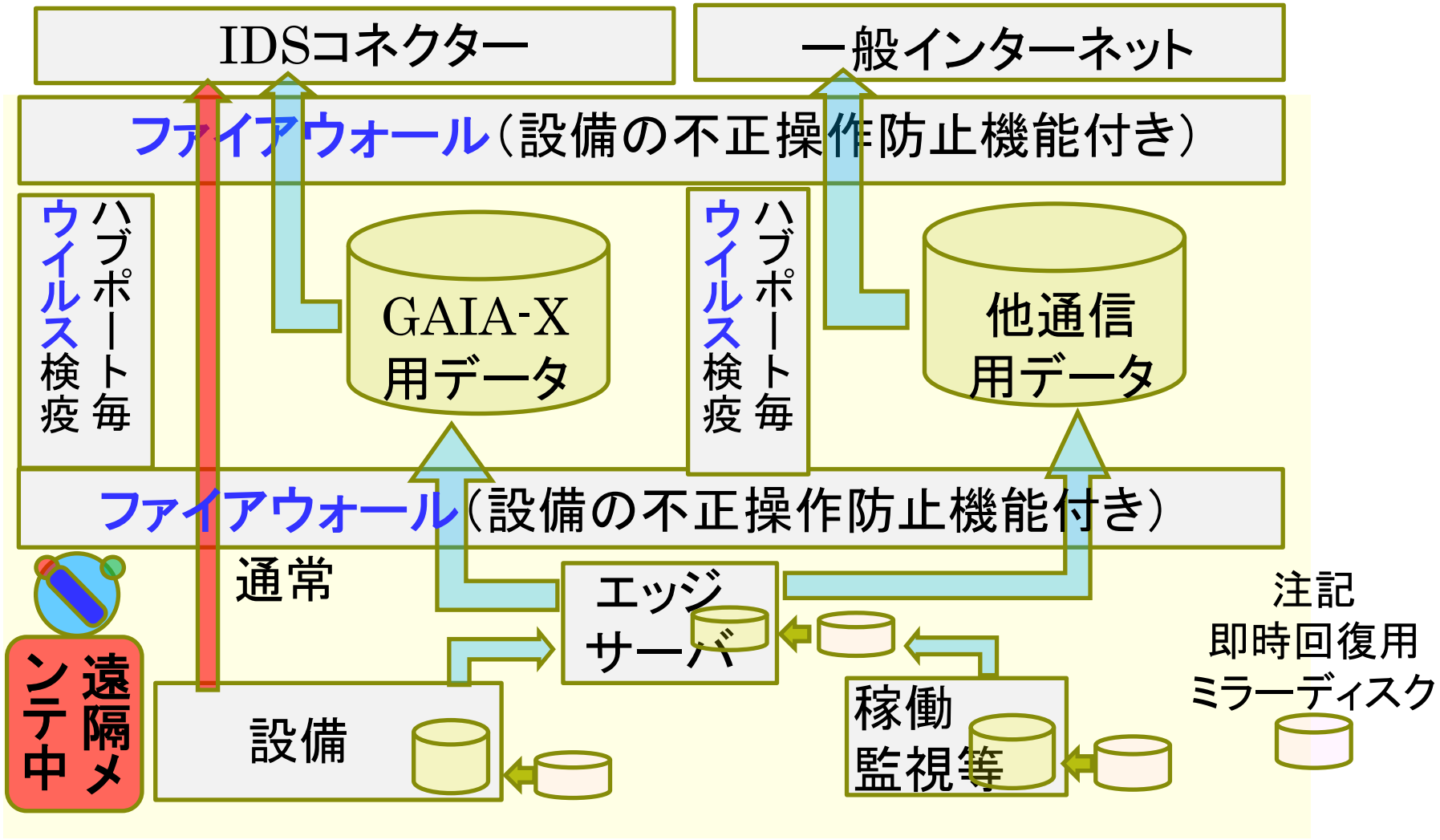
■以下テスト③④結果の説明の前に、前提とした考え方をご説明します。

2-3.被害対策と加害対策が必要な
テスト③マルチプロトコル通信時に必要なセキュリティ対策を実現する。
2-4.セキュリティ対策の効果を判定する
テスト④ペネトレーションテスト を実施する。

⇒次頁から接続テスト③④の前提について説明します。

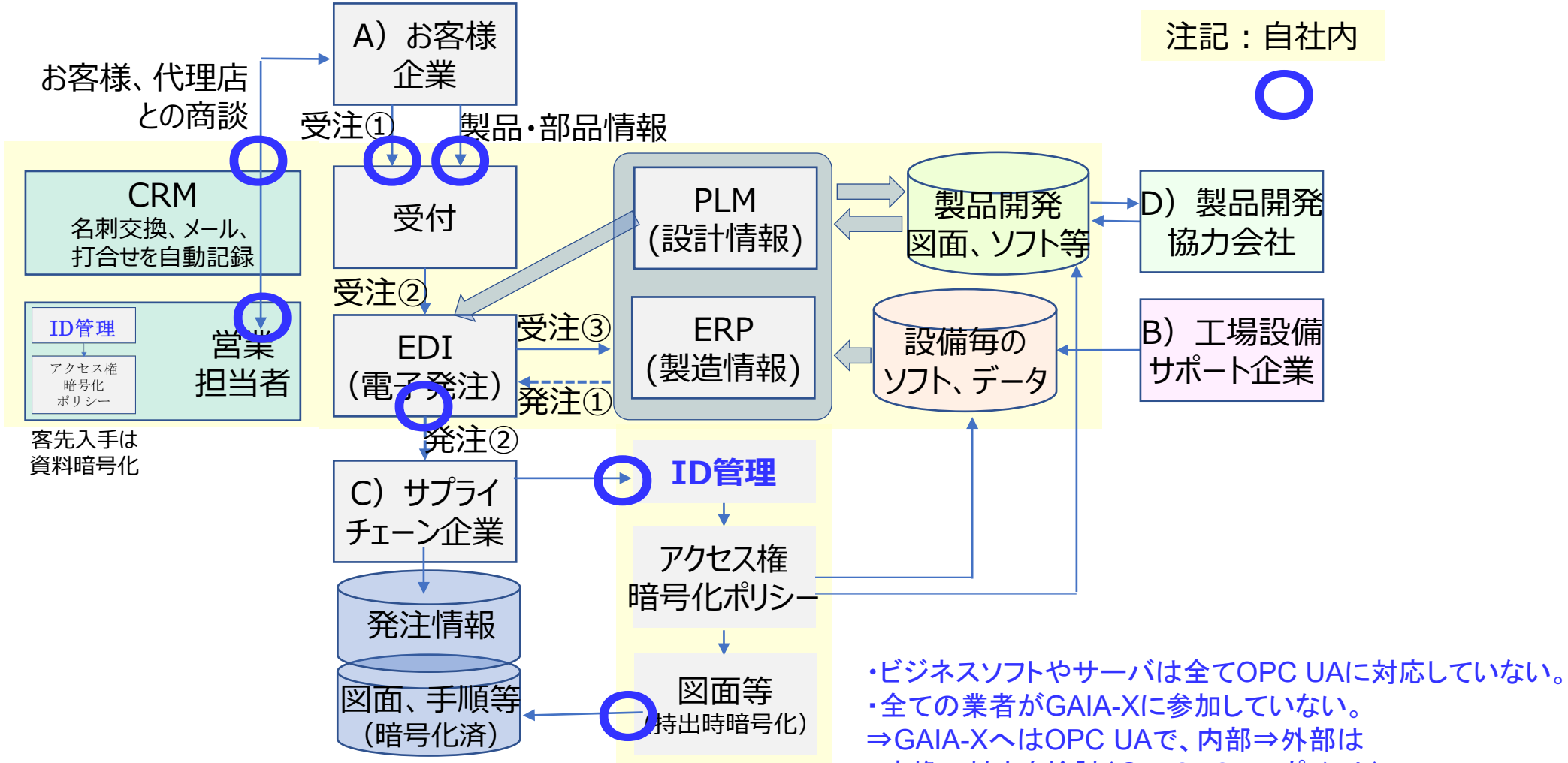
工場設備のセキュリティ対策の考え方　1/2

- 工場内ではGAIA-Xのみでなく他通信も行われる。
- GAIA-X側へのウイルスや不正アクセスによるデータを流出させない。



ビジネス利用時のマルチプロトコル通信の考え方　2/2

- ID、パスワード認証に加え、GAIA-X網内通信時のみログイン可能とする。
- ID乗っ取りに端を発した情報漏洩、破壊のリスクが大きく低減する。
- 暗号化ファイルは、生存期限、印刷制限等様々な制限が可能である。



・ビジネスソフトやサーバは全てOPC UAに対応していない。
・全ての業者がGAIA-Xに参加していない。
⇒GAIA-XへはOPC UAで、内部⇒外部は
変換で対応を検討（〇のOPC UAポイント）

2-3.テスト③マルチプロトコル通信時に必要なセキュリティ対策

以下3点のテストを通じ、実際に可視化する事で、必要なセキュリティ対策を、設備保守業者、生産技術者、情報技術者間で共有し構築を可能とするのが目的である。

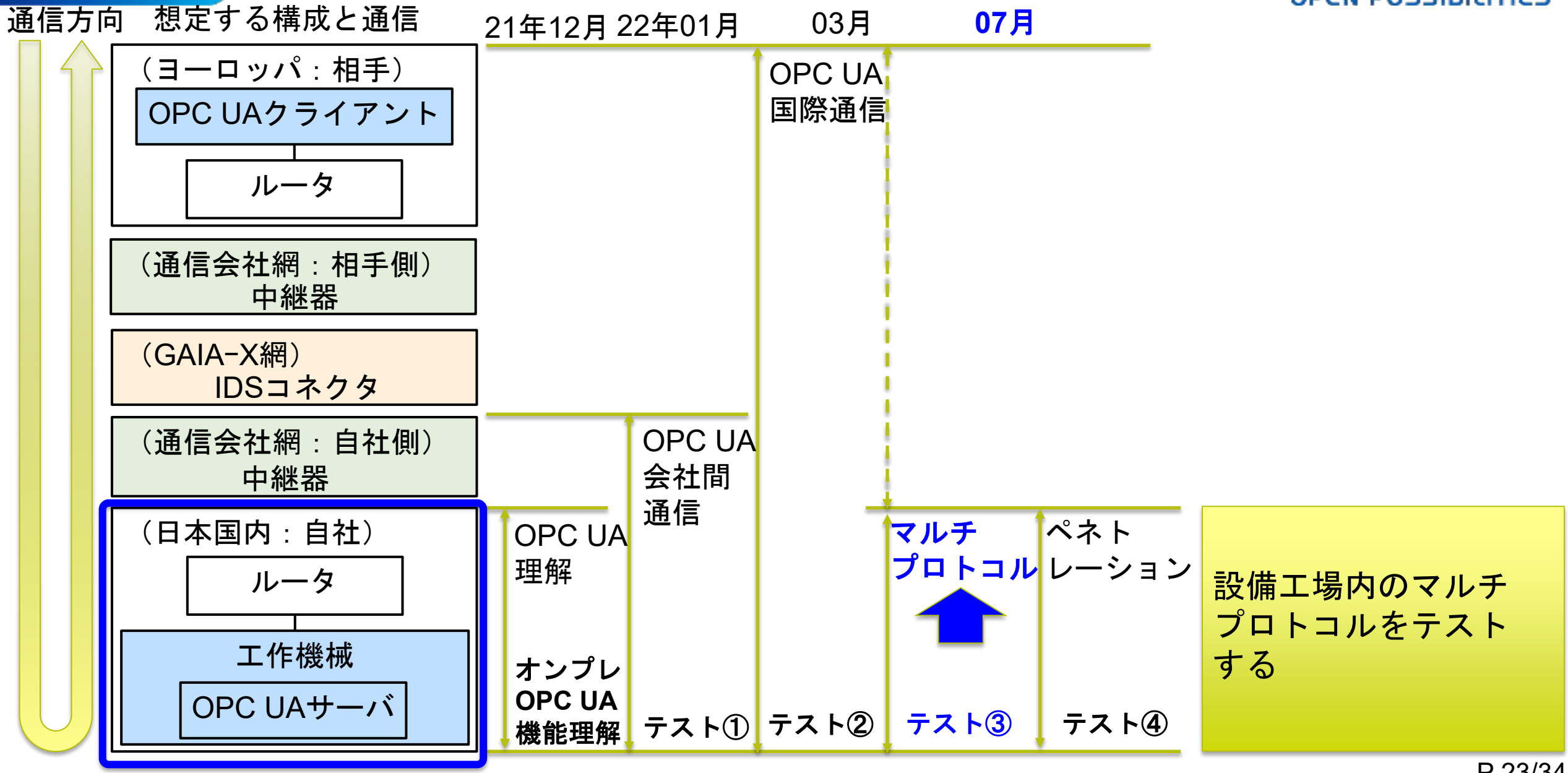
(国際規格IEC62443-3-2の脅威モデル構築時に、脅威を洗い出す必要がある)

2-1.通信中の盗聴や漏洩を防ぐ為に
テスト①暗号化通信での情報交換 を用いる。
2-2.実際の環境を想定し、実用性を計測する為の
テスト②国際通信 を実施する。
2-3.被害対策と加害対策が必要な
テスト③マルチプロトコル通信時に必要なセキュリティ対策 を実現する。
2-4.セキュリティ対策の効果を判定する
テスト④ペネトレーションテスト を実施する。

⇒次頁から接続テスト③について説明します。 P 22/34

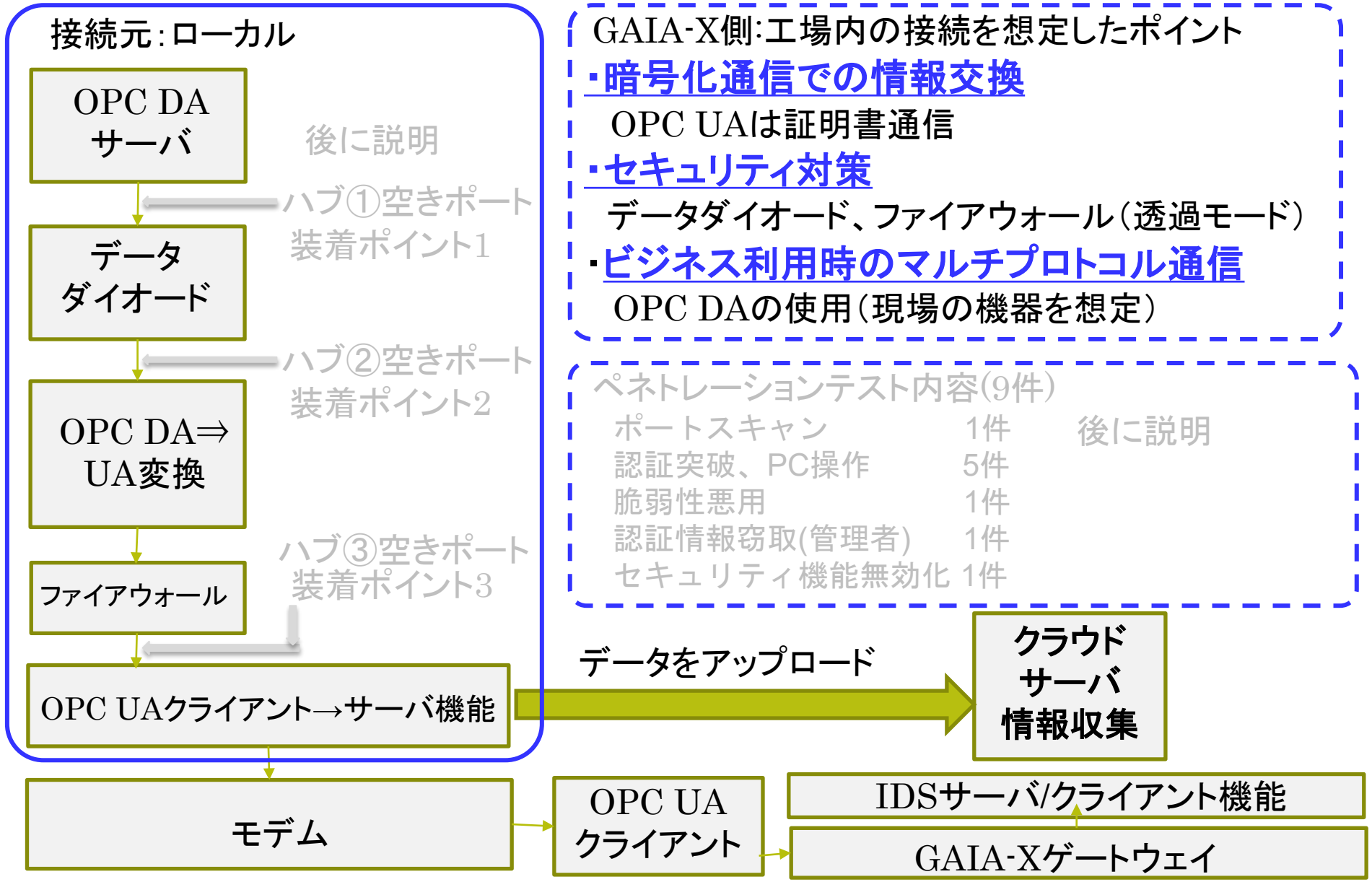
2-3.テスト③マルチプロトコル通信(1/2)

OPEN POSSIBILITIES



2-3.テスト③マルチプロトコル通信(2/2)

設備工場内のマルチプロトコルをテストする



2-4.テスト④ペネトレーションテスト

以下3点のテストを通じ、実際に可視化する事で、必要なセキュリティ対策を、設備保守業者、生産技術者、情報技術者間で共有し構築を可能とするのが目的である。

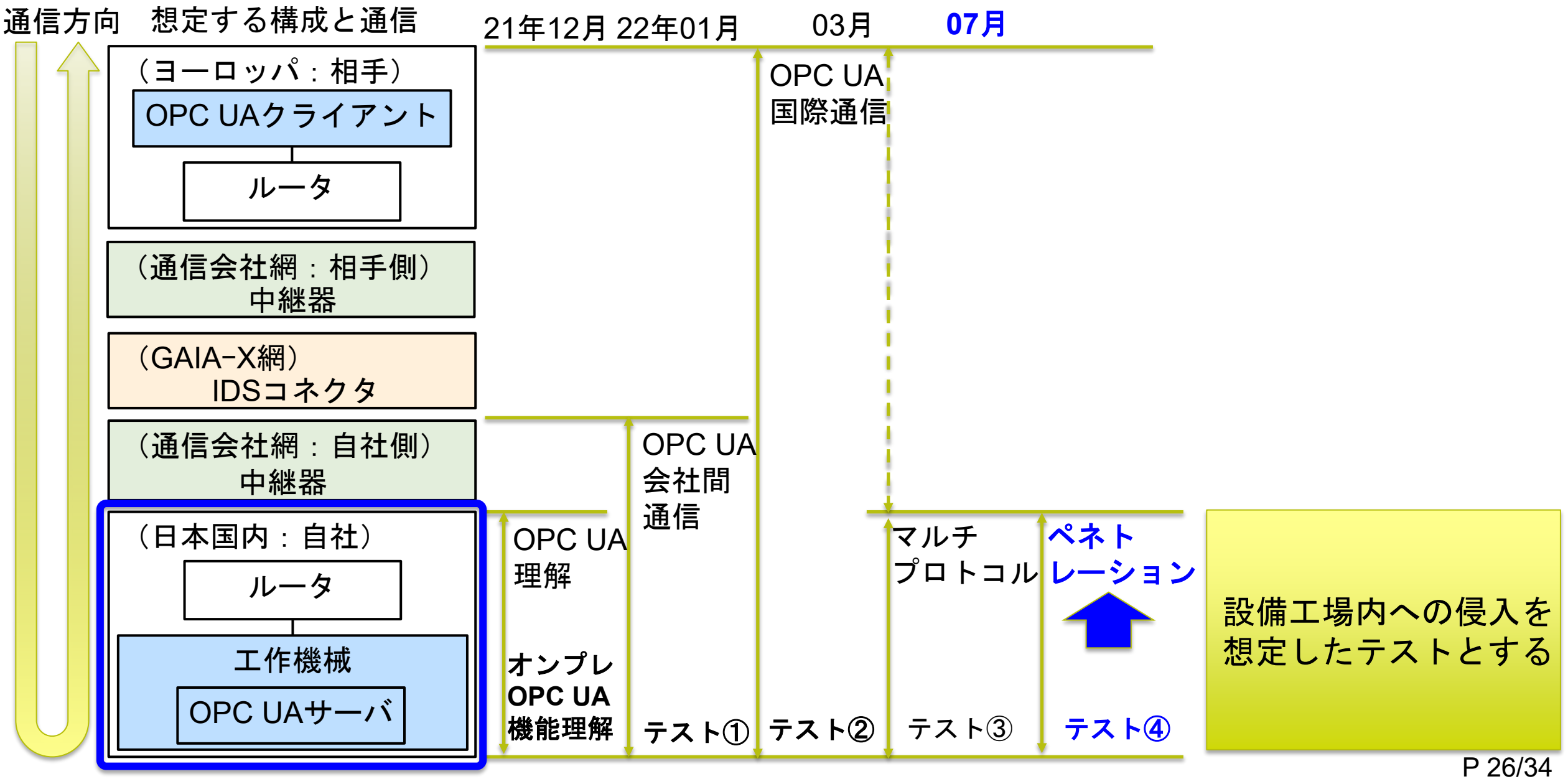
(国際規格IEC62443-3-2の脅威モデル構築時に、脅威を洗い出す必要がある)

2-1.通信中の盗聴や漏洩を防ぐ為に
テスト①暗号化通信での情報交換 を用いる。
2-2.実際の環境を想定し、実用性を計測する為の
テスト②国際通信 を実施する。
2-3.被害対策と加害対策が必要な
テスト③マルチプロトコル通信時に必要なセキュリティ対策 を実現する。
2-4.セキュリティ対策上の効果を判定する
テスト④ペネトレーションテスト を実施する。

⇒次頁から接続テスト④について説明します。 P 25/34

2-4.テスト④ペネトレーションテスト(1/6)

OPEN POSSIBILITIES



2-4.テスト④ペネトレーションテスト(2/6)

「運用」を想定し、攻撃が成立する可能性を絞り込みペネトレーションテストを実施する。

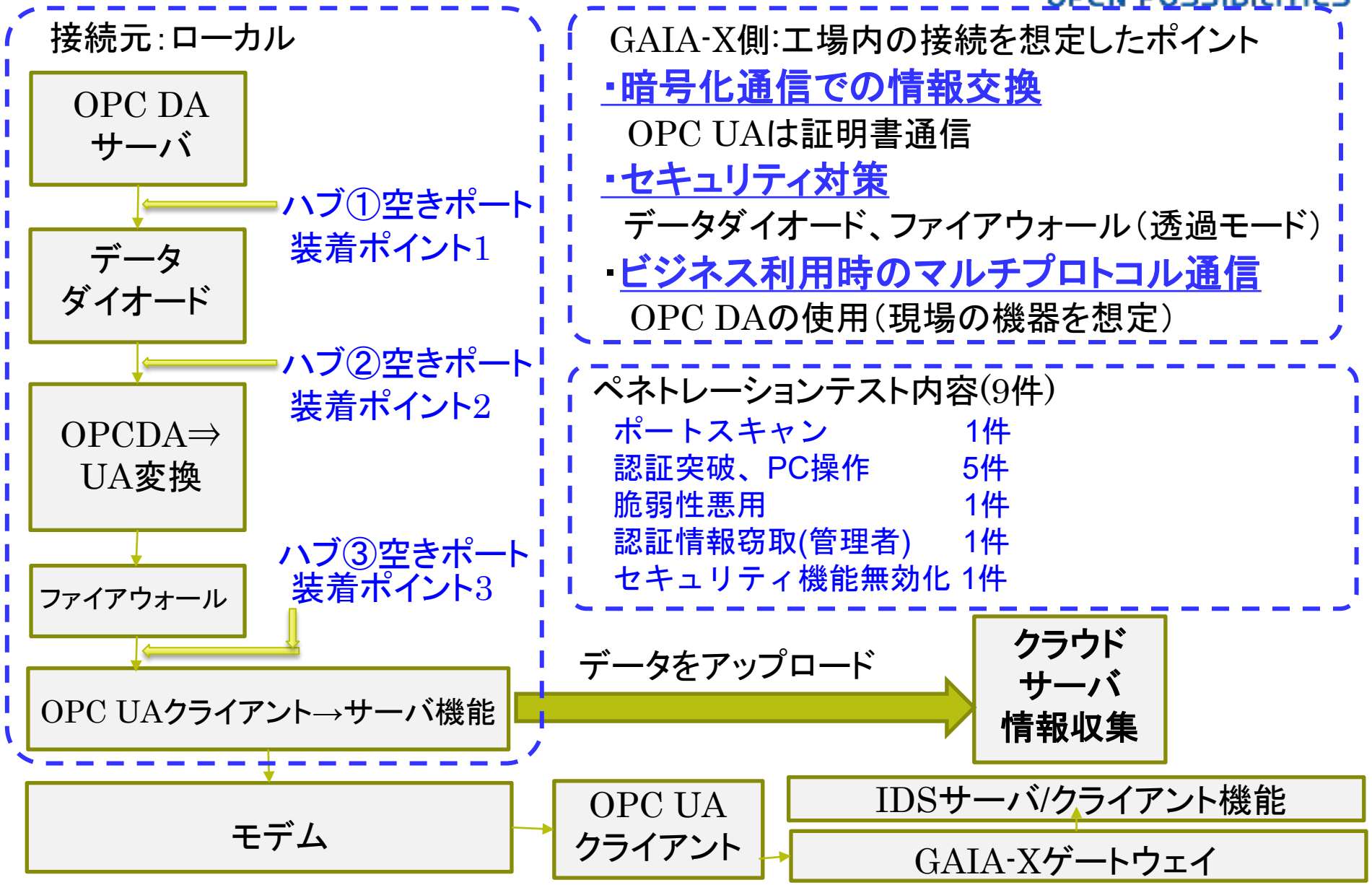
→ サイバー攻撃に対する防御及び、迅速な回復の準備が必要な脅威

↓ 侵入、報収集、破壊（漏洩）対策が必要なリスク

	管理上の脅威 IT管理、利用者 (ISO27001)	設備の脅威 設備及び提供者 (IEC62443)	攻撃者の脅威 脆弱性を用いて攻撃	サプライチェーンへの脅威	誤検知誤作動の脅威	災害の脅威
侵入対策 社外ネットワーク、物理（保守等）のリスク	IDパスワード通信設定は情報部門の担当者が関与していると想定した。	ネットワーク機器は業者任せにしないで自社担当者が設定に関与していると想定した。	OSは最新に更新されていると仮定し、既知の脆弱は無いと想定した。		誤検知によるシステムの継続利用阻害	災害や紛争によるシステムの継続利用阻害
情報収集対策 設備を制御する為に通信するサーバのリスク						
破壊(漏洩)対策 設備本体、関連ネットワークのリスク	攻撃者は一般的な攻撃ツールを使いこなし、現場内のネットワークに何らかの要因で到達し、活動すると想定。					
ビジネス対策 自社製品に対するリスク						

2-4.テスト④ペネトレーションテスト(3/6)

設備工場内への侵入を想定したテストとする

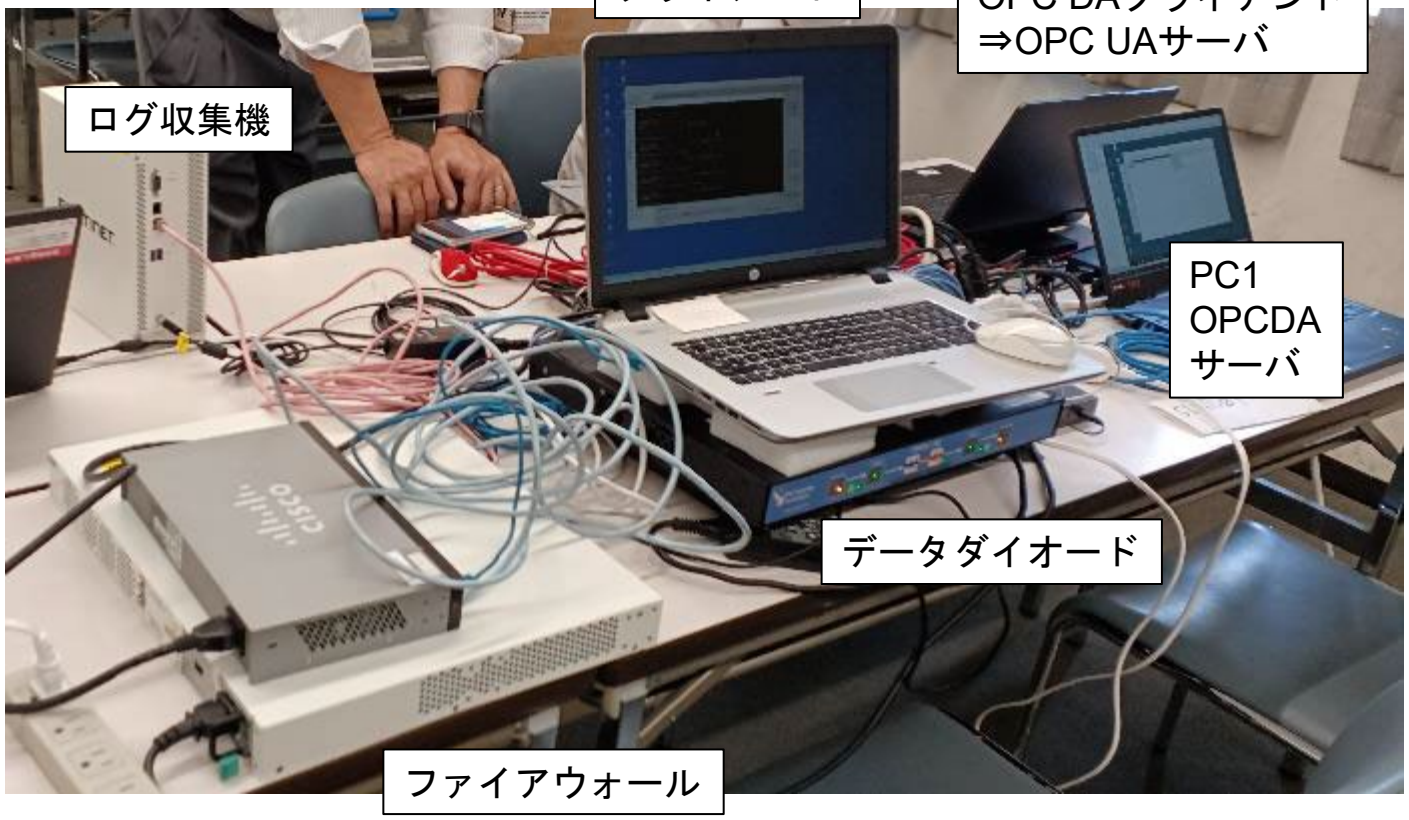


2-4.テスト④ペネトレーションテスト(4/6)

ペネトレーションテストシステム風景(1/2)

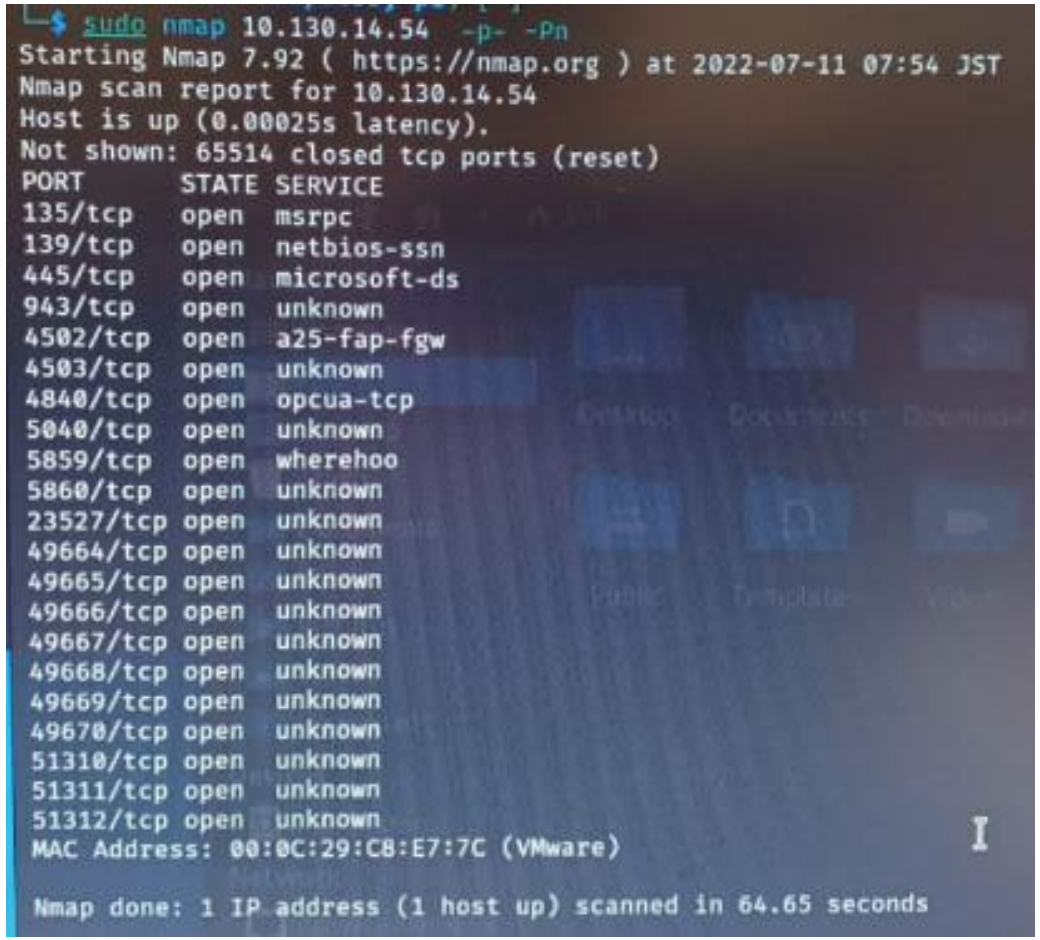
1号機

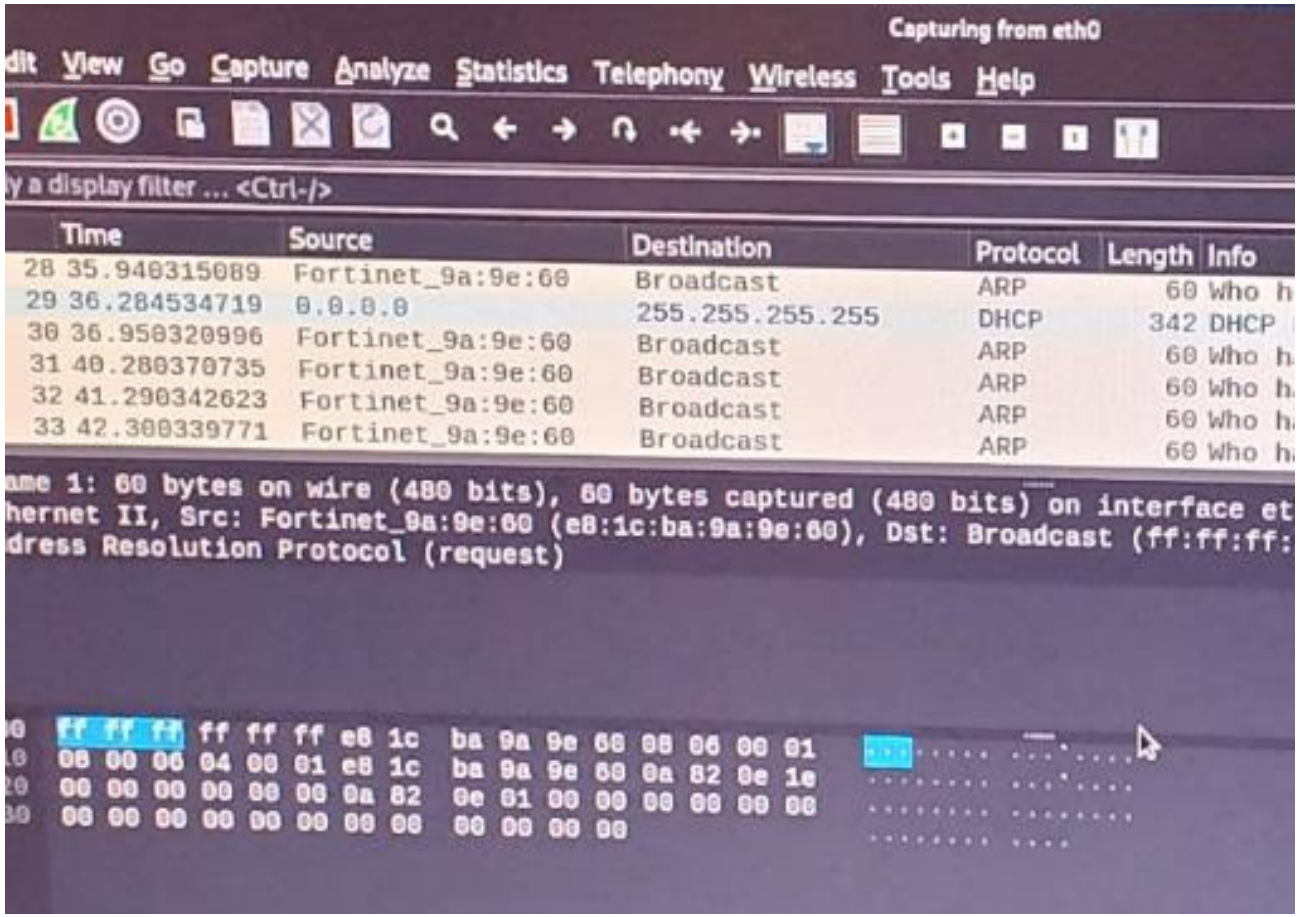
2号機



2-4.テスト④ペネトレーションテスト(5/6)

ペネトレーションテスト画面風景(2/2)





2-4.テスト④ペネトレーションテスト(6/6)

・ペネトレーションテストは簡易的な指導を受け自社で実施した。
結果侵入や盗聴は不可であったが、以下の課題を発見した。

⇒ペネトレーションテストの実際は、ITエンジニアにとって普段実施している正常な応答を想定するテスト業務とは異なり、想定外の戸惑いが多い。
⇒同一機能をもつ複数のツールを使う必要もあり、攻撃を理解しないとツールの操作手順のみでは実施が困難である。

・よってペネトレーションテストは、自社で実施するのもよいが、最終試験では専業の業者に委託すべきである。国際規格であるIEC62443-4-1では「テスターの独立性」が要求されている。

GAIA-X接続とその実用性について

1.GAIA-Xとサイバーセキュリティ
2.GAIA-Xの通信テスト及び必要なセキュリティ対策
3.まとめ

まとめ　1/2

1．GAIA-Xの関連性で顧客、自社、サプライチェーンと広範囲に想定した
　VECの活動において、実現方法としての設備面のみでなく、制度面も含めた総合的なセキュリティ対応、対策を考慮した。

2．実現性を重視し、やってみた上で可視化して共有した
　セキュリティ対応は、常に具体的な脅威に向き合う対応であり、テストを具体的かつ可視化することに努めた。

3．OPC UA、GAIA-X、国際規格といったスタンダードを重視した
　グローバルかつ、工場設備の常時接続を考慮し、OPC UA、GAIA-X、国際規格といったスタンダードの理解に努め、セキュリティ対策の実現性をテストした。

まとめ 2/2

VECの皆様からの全面的なご協力を得て、テストを完遂することができました。
当初、OPC UA、GAIA-Xを理解しておらず、VECの活動において皆様から様々な情報、設備をご提供頂いたことに感謝します。

本サイバーセキュリティの実装を前提として実施した GAIA-Xの通信テストで得られた知見を、VECの皆様、ユーザ各位の高生産性に活用していきます。

また、様々な製品による実験や導入の結果を、弊社製品やサービスを通じて客先に活用頂く。脱炭素、インフラ整備等の社会の様々な課題解決に対し、一層貢献していく所存です。

ご清聴ありがとうございました。