Blockchain-protected Security Fabric for IIoT

インダストリアルIoT環境で求められる、広義の「セキュリティ管理」

- アセット（ユーザー、デバイス、アプリ）の追跡・監視

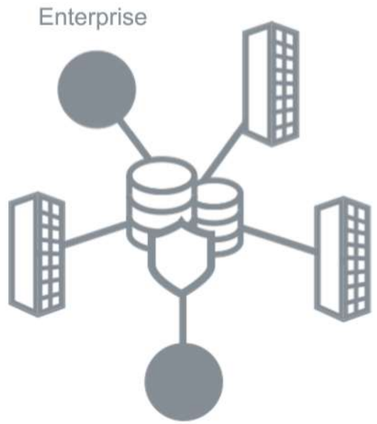
- IoTインフラ環境の健全性監視（遠隔地・無人環境での状態監視）

- 運用分析（使用率、バッテリー。。）

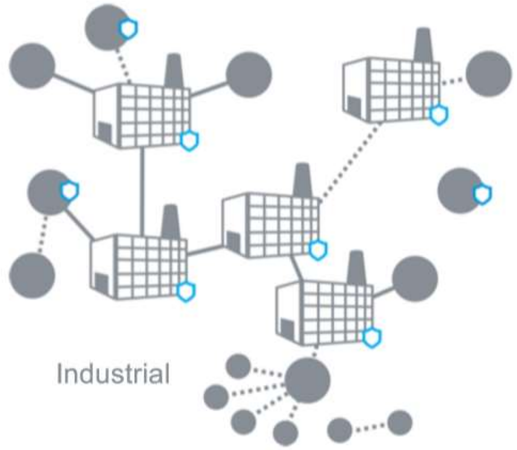
- ソフトウェア・セキュリティの更新

- エッジからサーバーへのデータ・ストリームの保護

Xageセキュリティ



V.S.



エンタプライズIT

全社ITで管理される中央集権管理

ファイアウォールやウイルスチェックでの
セキュリティ対策

システム構成の多様性は苦手

xage SECURITY

インダストリアルOT

サイト・ロケーションごとの分散管理

デバイスごとのクレデンシャル管理

マルチベンダー、マルチ世代

業界特有通信プロトコル

インダストリアルIoTの進展に伴い、必然的にネットワーク接続の必要性が拡大

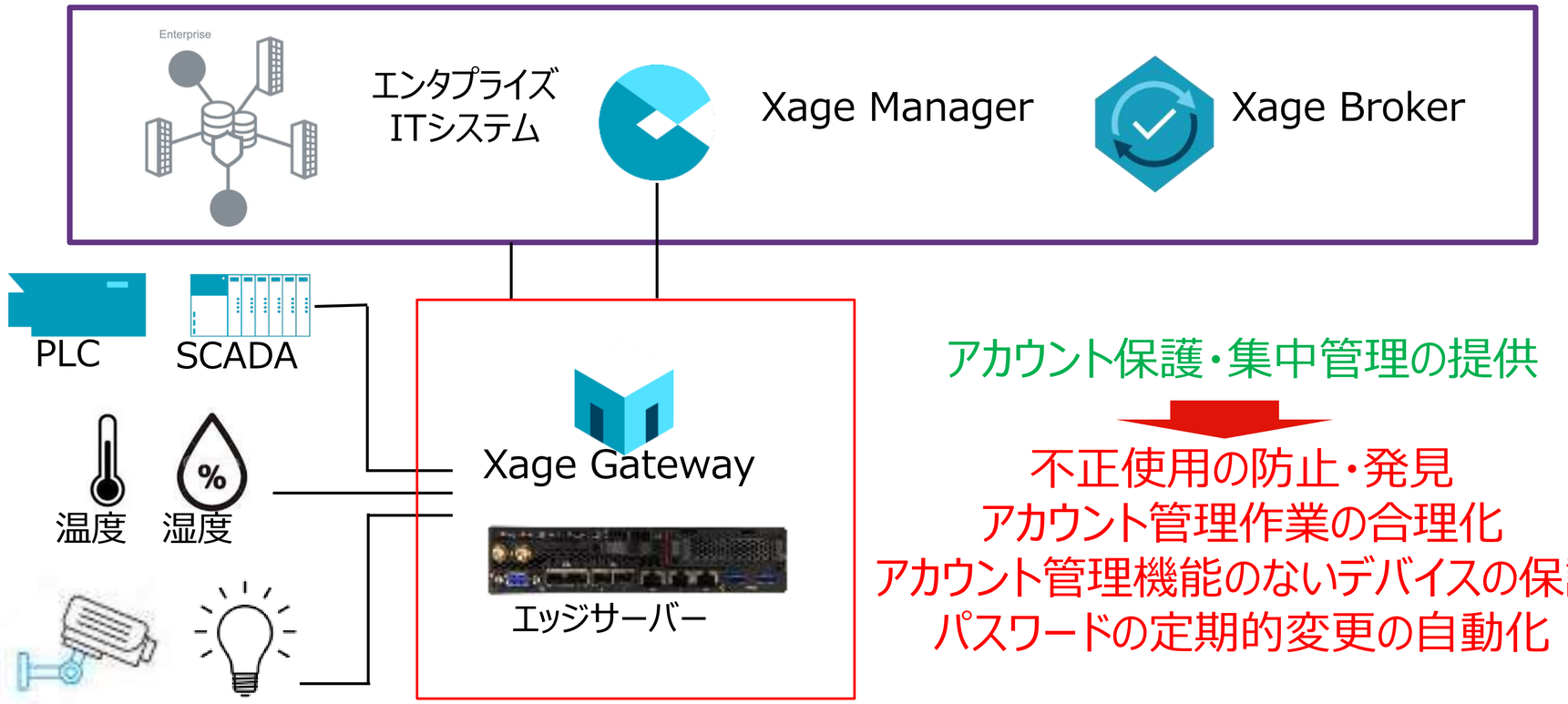
インダストリアル領域でも製品・サービス品質と安全性確保にエンタプライズレベルのセキュリティ管理が必要

Xage Securityソリューション

IoTデバイス・エッジ・サーバーへのアクセスを保護

xage SECURITY

ブロックチェーンで保護された
インダストリアルIoTのためのセキュリティ・ファブリック



アカウント保護・集中管理の提供

不正使用の防止・発見
アカウント管理作業の合理化
アカウント管理機能のないデバイスの保護
パスワードの定期的変更の自動化

などのメリットあり！！

事例：WWに分散した風力タービン設備の保守を迅速かつセキュアに実行

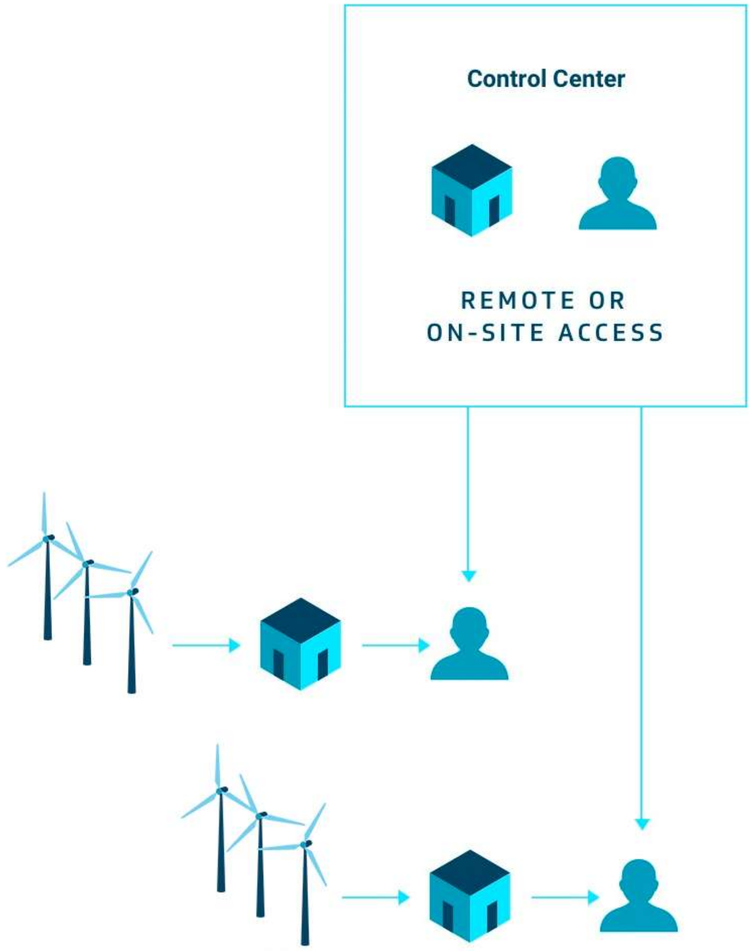
GE Renewable Energy https://www.ge.com/jp/b2b/renewables

課題:

- 風力タービン数35,000+, 国数80+, 従業員、委託作業員数22,000+の管理
- 分散した機材（サイト内および遠隔に存在する）に対して技術員が自身のユーザーIDで円滑にかつセキュアにアクセスし、その証跡を監査目的で活用できる

ソリューション:

- Xage Manager で、AD連携した技術員のユーザーIDとアクセスポリシー管理
- Xage Security Fabricをコントロールセンターと風力タービン設置サイトに設置し、ユーザーIDとアクセスポリシーをセキュアに保持
- Xage Fabricにより、技術員がどこのサイトで作業をしても自身のユーザーIDとMFA*を使用した認証が可能
- Xage Gateways で利用できる簡易的なダッシュボードで指定したデバイスやPC、リレーに対するアクセス制御



MFA * : Muti-Factor Authentication

事例：広範囲に広がる、多機種デバイスに対するアクセス制御

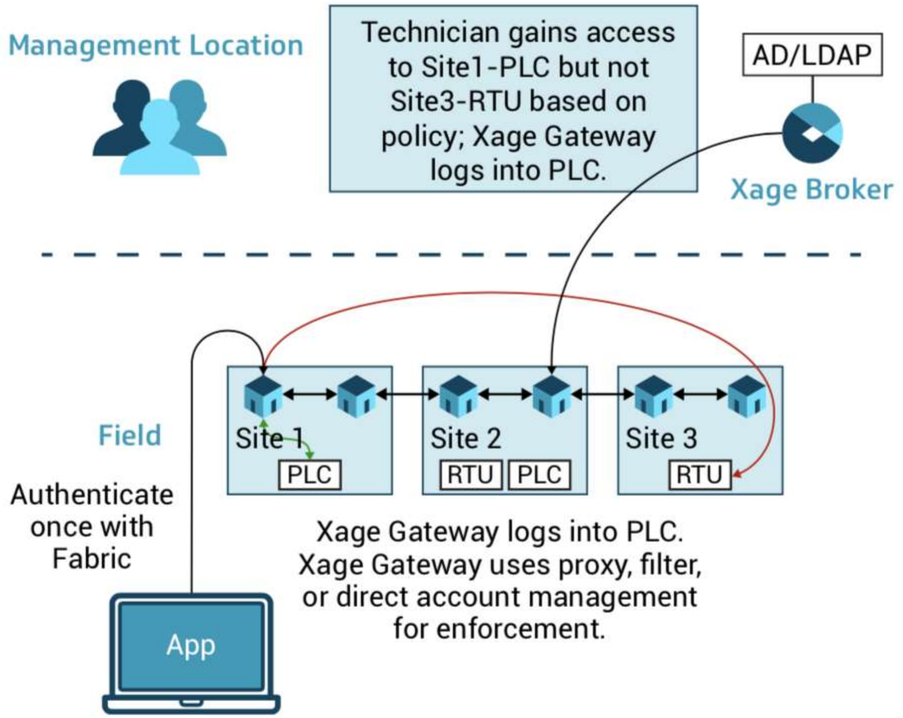
https://www.saudiaramco.com/en/

課題:

- 広範囲に広がりを持つ、百万単位のデバイス群の管理
- 存在するPLCs/RTUs が複数ベンダーの新旧機種にまたがりその間で行われるユーザー/デバイス/アプリのアクセス管理

ソリューション:

- Xage Manager がユーザー/デバイス/アプリ間の通信を管理
- Xage Security FabricでWell Pad(水平坑井)に対するアクセスID認証を行い、ユーザー、デバイス、アプリの通信をトレース
- Xage Enforcement Point (XEP) が油井ごとに設置され、ProxyやFilteringを用いて全体のアクセス制御を実施



適用業界

エネルギー、電気ガスなどの公益事業

自動車、運輸業界

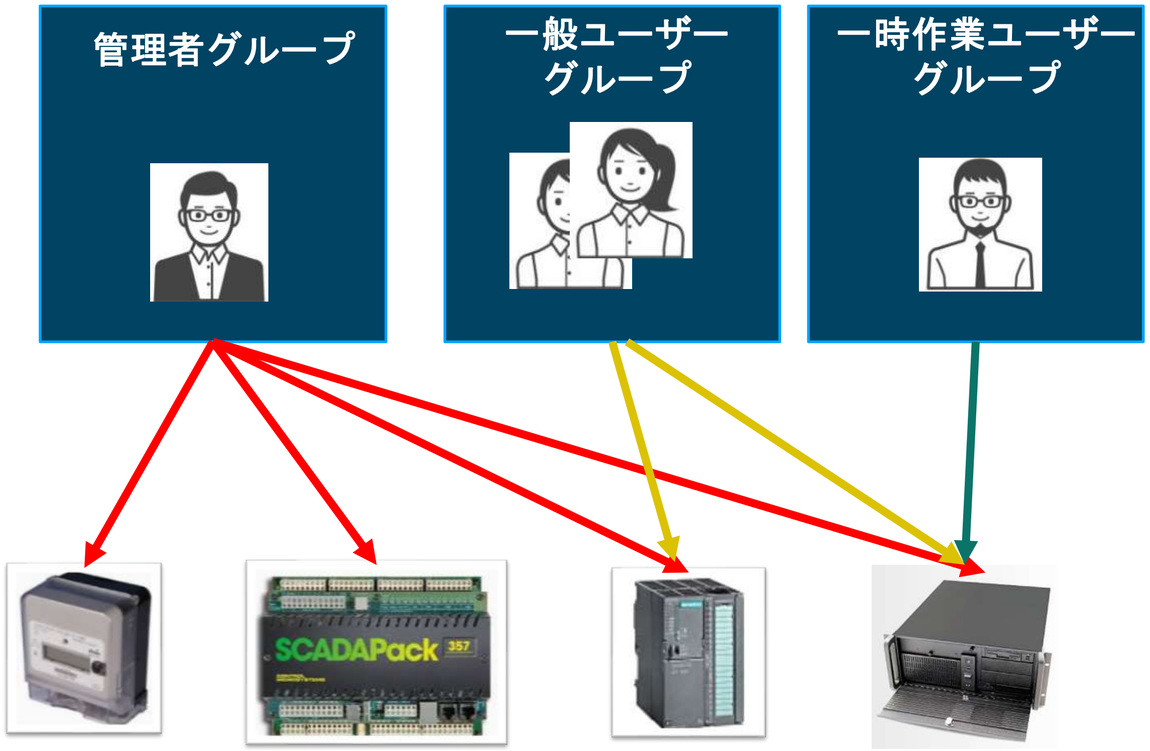
鉱山開発

製造業

ビル管理

ロールベース・アクセス・コントロール - RBAC

デバイス側でなく、ユーザー側の役割に応じてアクセス管理



拡張

基本機能

ユーザーからデバイス（RBAC）

新規対応

デバイスからデバイス（M2M）

新規対応

アプリケーションからデバイス

次期対応

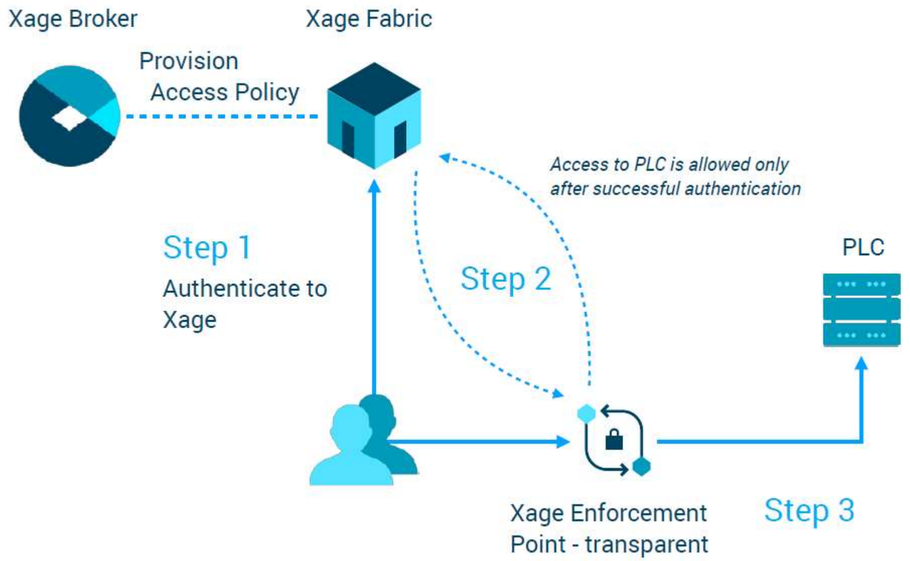
ユーザーからアプケーション

Xage Enforcement Point

- Use Case :

  組み込みの認証メカニズムのない
  デバイスへのアクセス制御

  - 最初にXage Fabric/XEPでアクセス認証後、デバイスへのアクセス許可

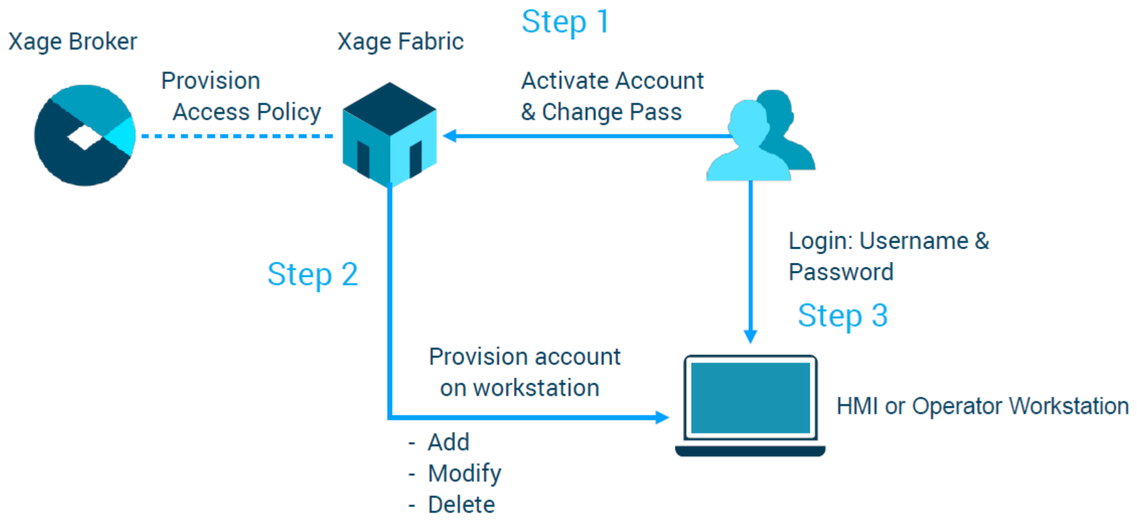


Account Management

- Use Case :

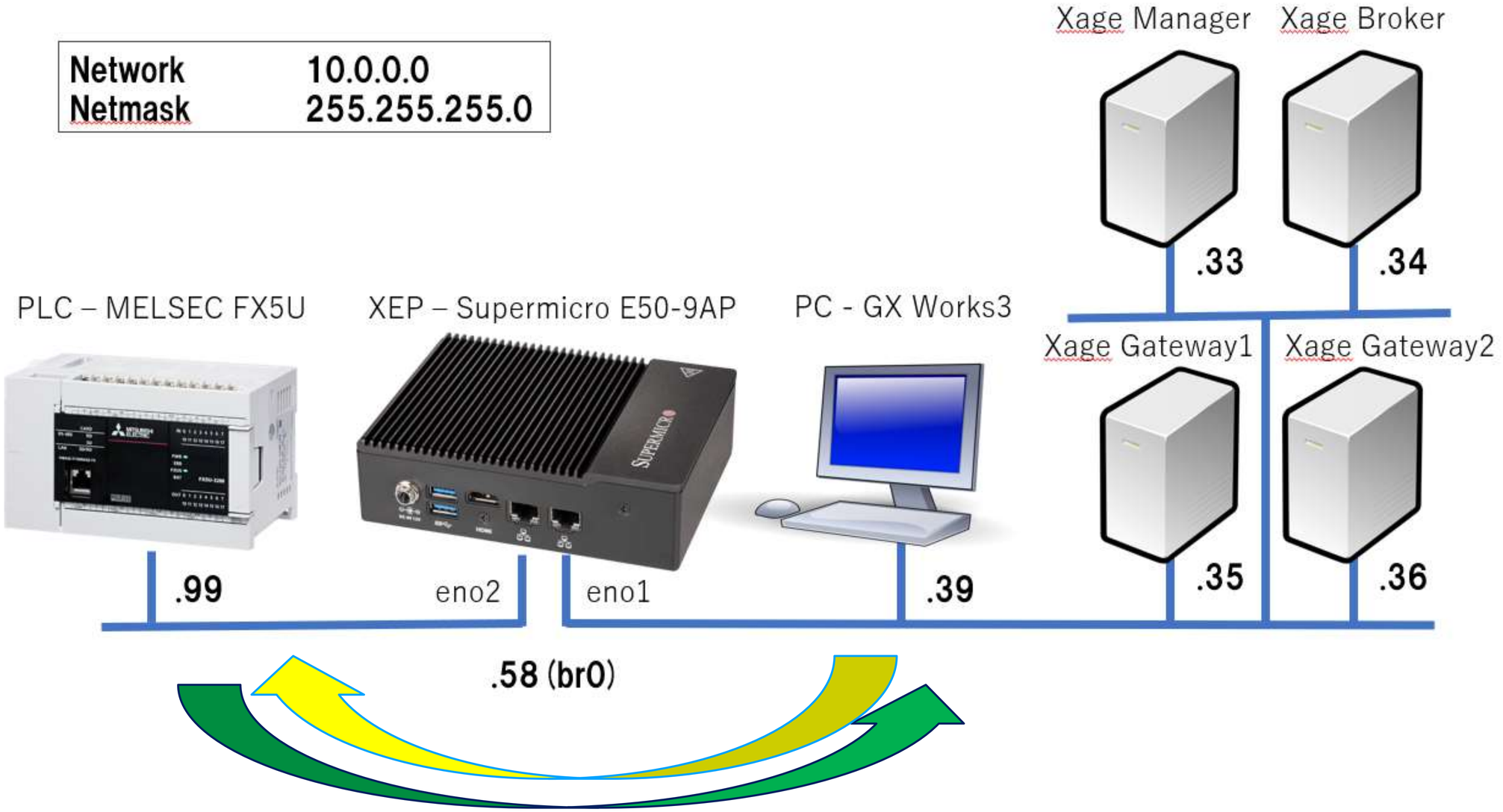
  ローカルに定義済の（多くの）ユーザーを
  管理下に置きたい

  - システム管理者がXage Fabricでアクセスポリシーを定義
  - ユーザーは自身のアカウントのアクティベートを要求
  - アクセスが許可されて、HMIまたはPCにアクセス許可



Xage XEP demo

Network	**10.0.0.0**
Netmask	**255.255.255.0**



Xage Security　PoC　参考サンプル構成

一台のPC上に複数VMでXage Fabricを構成
(Fabric = Broker + Gateway(GW))
ブロックチェーンの要件で最少で３つのVMが必要

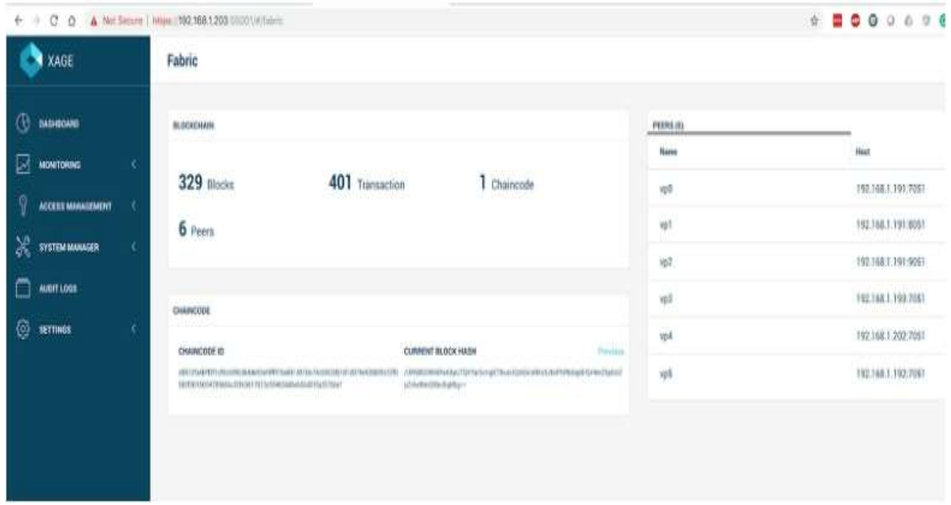
ローカルまたはリモートからの
WEBブラウザー経由でのアクセス

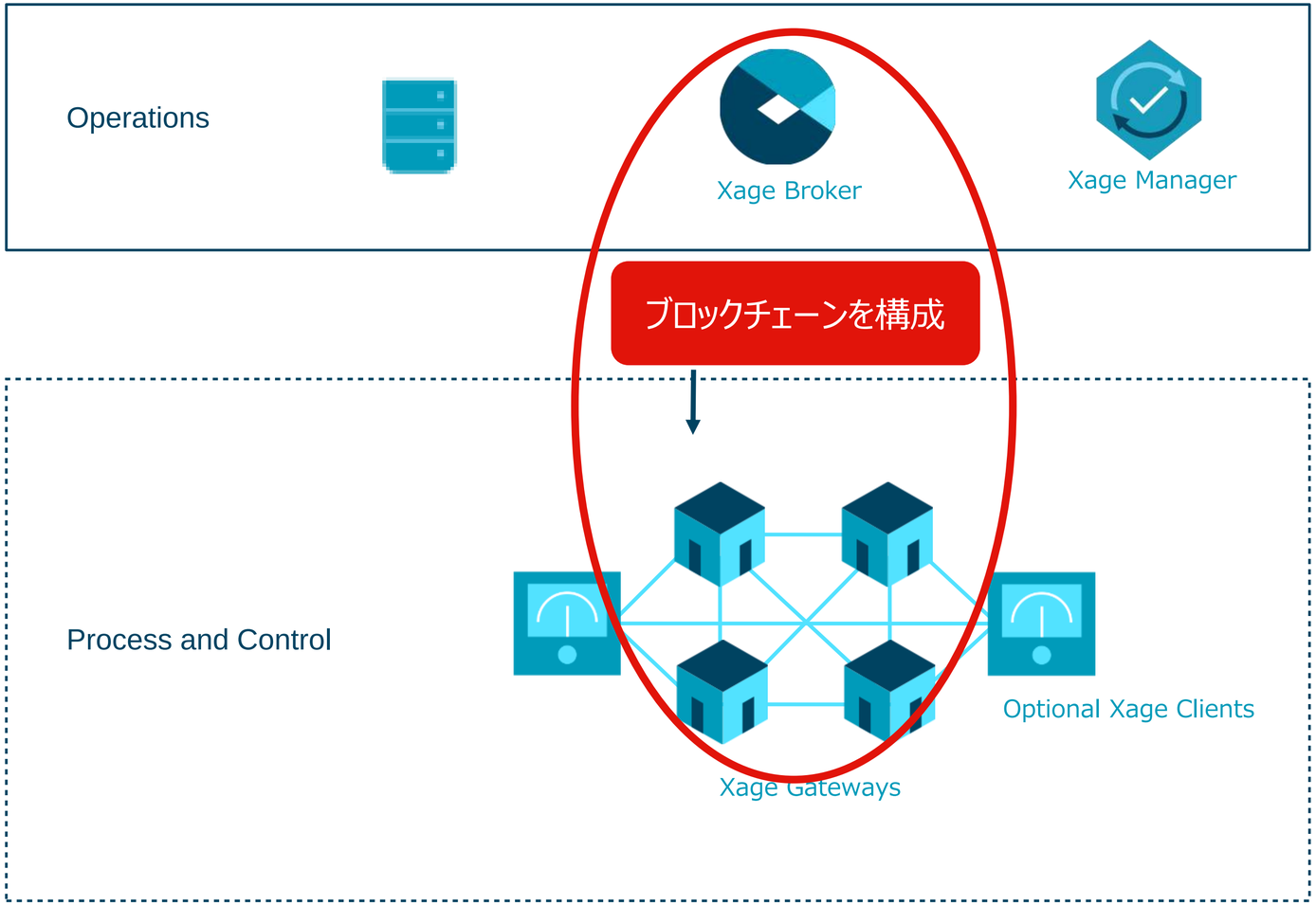
認証機能を持たないIoTデバイス代替で
Xage内でアクセス認証、アクセスログ管を
行えるようにする

Xageのブロックチェーンについて

- ブロックチェーンの一般的な特徴
  - データが分散保存、対障害性
  - 改竄できない、壊れても自動修復
  - 単一障害点が存在しない
  - 合意された情報だけが有効なネットワーク共有型

  な、データベース





認証情報、アイデンティティ、サーティフィケーション、プロファイル、ポリシーなどの保持

コネクテッド・インダストリーズ税制対応

【計画認定の要件】

①データ連携・利活用の内容

・社外データやこれまで取得したことのないデータを社内データと連携

・企業の競争力上重要なデータをグループ企業間や事業所間で連携

②セキュリティ面

必要なセキュリティ対策が講じられていることをセキュリティの専門家(登録セキスペ等)が担保

③生産性向上目標

投資年度から一定期間において、以下のいずれも達成見込みがあること

・労働生産性：年平均伸率２%以上

・投資利益率：年平均15%以上

課税の特例の内容

➢ 認定された事業計画に基づいて行う設備投資について、以下の措置を講じる。

対象設備	特別償却	税額控除
ソフトウェア 器具備品 機械装置	30％	3％ (法人税額の15%を限度) 5％ ※ (法人税額の20%を限度)

【対象設備の例】
データ収集機器（センサー等）、データ分析により自動化するロボット・工作機械、データ連携・分析に必要なシステム（サーバ、ＡＩ、ソフトウェア等）、サイバーセキュリティ対策製品　　等

最低投資合計額：5,000万円

※ 計画の認定に加え、継続雇用者給与等支給額の対前年度増加率≧３％を満たした場合。

経済産業省ホームページ

- セキュリティ面でのXageが有効な項目
  - データ連携を行うシステムの設計（機能面）
    - データにアクセスできる人物・組織を必要最低限に制限する仕組み
    - データ連携を行うシステム間の通信経路が第三者に盗聴されないような仕組み
    - データに対する外部からの不正なアクセスに対して、必要な防御策を講じる
  - 事業実施時の適切なセキュリティ確保策（体制面）
    - 不正なアクセスを検知する体制
      - 検知機能を提供
    - 被害が生じた場合の対処方針を明確化
    - 提供先部門・企業にける適切なセキュリティ対策の確認
    - 定期的に既知の脆弱性がないか確認

xage

Xage 詳細情報

Xage のシステム構成

Xage Manager

- ポリシー管理、アラートなどオーケストレーション管理
- クラウドまたはオンプレミス版を提供

Xage Broker

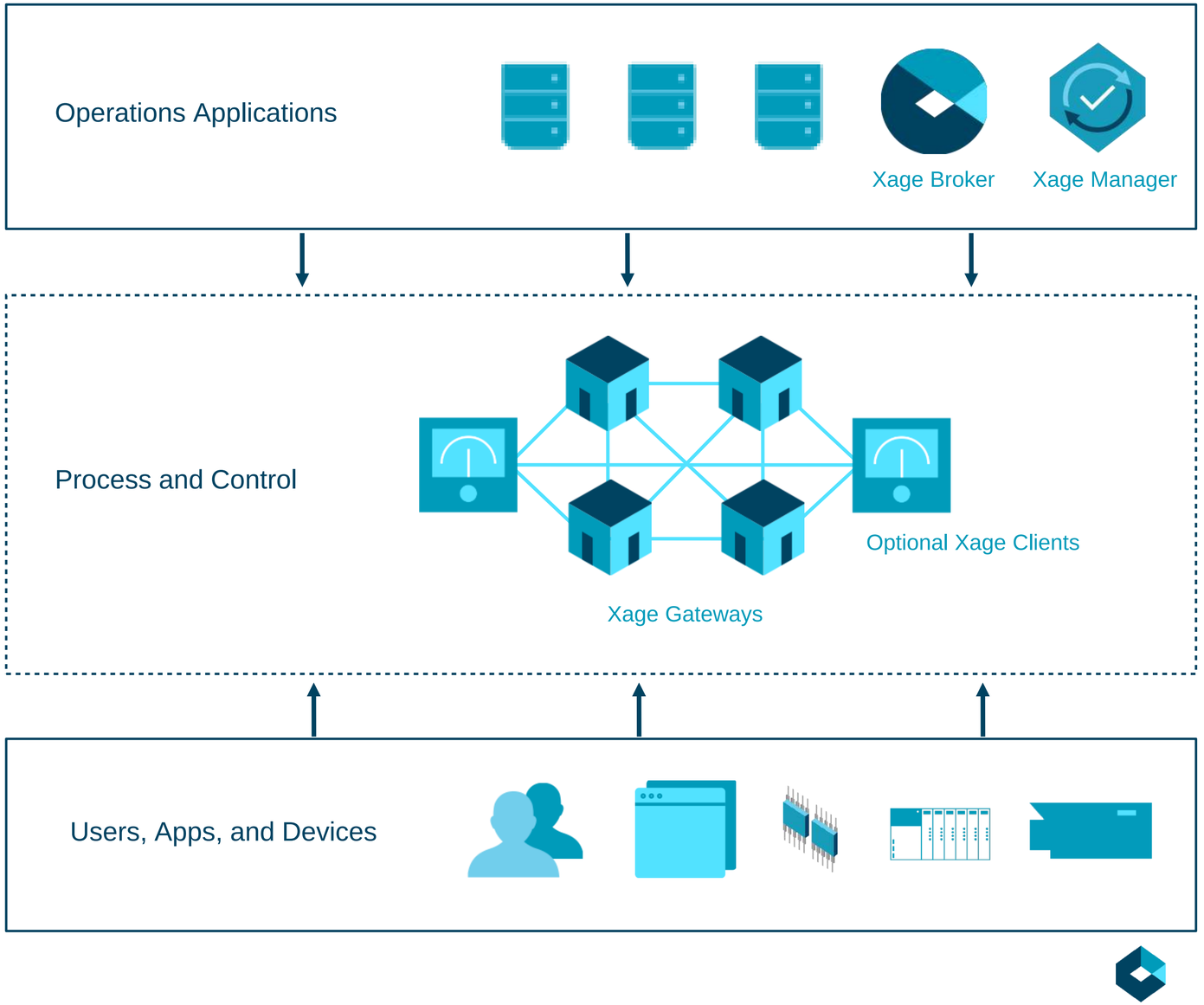
- ADやLDAPと連携してインベントリ管理やアクセスコントロール、ユーザクルデンシャル管理、デバイス管理を行う
- クラウドまたはオンプレミス版を提供

Xage Gateway

- アクセスコントロール、デバイス管理、デバイスアクセスへのリダイレクト、データ管理とファブリックによるセキュリティの担保
- エッジソリューション、業界で使用される汎用プロトコルのサポート

Xage Fabric formed by Brokers and Gateways

- 認証情報の保持、 アイデンティティ、サーティフィケーション、プロファイル、ポリシー
- ブロックチェーン技術、シャミア秘密分散法*との融合



Xage Security サポートプロトコル

Industrial and management protocols

- HTTP(s), SSH, Telnet
- Modbus, MQTT
- EST over HTTPS and CoAP-DTLS
- X.509 certificates with RSA and ECC
- DNP3 (roadmap)
- IEC 61850 (roadmap)
- CAN Bus (roadmap)
- BACNet (roadmap)

Security Services

- Microsoft Active Directory 2012
- Microsoft Certificate Authority
- OpenLDAP and RADIUS

Supported OS and Hardware

- SSG supported on ARM and X86 (5-20MB)
- Dell IoT Gateway 3000 and 5000
- Intel Fog Gateway (roadmap)
- EdgeX, Ubuntu, SUSE, Docker

産業プロトコル	特徴	ターゲット業界、業種
HTTP(s), SSH, Telnet	リモートアクセスの標準プロトコル	すべての業界
Modbus	製造、生産、発電、組み立て、精錬などを含む工業プロセスにおけるPLC、ベンダー固有	製造業一般
MQTT	M2Mの非同期通信、軽量・低遅延・省電力	すべての業界、業種
EST over HTTPS and CoAP-DTLS	HTTP、UDPベースIoT向けプロトコル	
X.509 certificates with RSA and ECC	ITU-Tの公開鍵基盤（PKI）の規格	
DNP3（計画中）	分散ネットワークプロトコル。電力、上下水道、石油など SCADAのオープン通信プロトコルセット	電力、水道、石油など
IEC 61850（計画中）	製造、生産、発電、組み立て、精錬などを含む工業プロセスの通信標準プロトコル	製造、発電など
CAN Bus（計画中）	自動車内電子制御ユニット標準通信方式	自動車、モビリティ製造
BACNet（計画中）	ビルディングネットワーク通信国際規格 空調・衛生・電気・照明・防犯・防災	建築

Xage Security 既存のサポートデバイスの例

デバイス	用途	メーカー
Itron Riva Meters	電気、ガスメーター	Itron
Emerson ROC800	電気、ガス用のRTU	Emerson
Allen Bradley L7x PLCs	PLC	Allen Bradley
Siemens S7 PLCs	PLC	Siemens
Schneider SCADAPack	SCADA	Schneider
ABB Industrial router	電気、ガス用途をメインとしたルーター	ABB
Johnson Controls MAP	Smartメーターなどへのモバイルアクセスサーバー	Johnson Controls
NTT CPE	CPE（VPN装置）	NTT
Wago PLC	PLC	WAGO
監視カメラ	監視カメラ	多種






写真はメーカとデバイスをイメージしていただくためのもので、必ずしもそのデバイスでの実績は表現していません。