PcVueアーキテクチャと展開

最終更新日:	2022年9月
改訂：	11
コンテンツ ：	PcVueのアーキテクチャと導入ソリューションについて説明します。

コンテンツ

1. 概要

本ドキュメントでは、監視システムの展開オプションについて説明します。
展開とは、与えられた物理ネットワーク構成において、システム要件を満たすために、ワークステーションおよびサーバーに役割を割り当てるプロセスを指します。
本トピックの目的上、監視システムは以下の主要な機能を備えているものとします。

- データ収集 - Modbus、OPCなどの通信プロトコルを用いて、現場値または計算値を表すリアルタイムデータを収集します。
- 履歴データ記録 - リアルタイムデータを記録して、後から監視システム自身またはサードパーティ製アプリケーションからアクセスできるようにします。
- アラーム - アラームの生成と管理。
- HMI - ヒューマンマシンインターフェース。プレゼンテーション層であり、オペレータが監視対象システムと対話するためのグラフィカルインターフェースです。
- ステーション間ネットワーク - 監視システムがネットワークアーキテクチャ内のステーション間でリアルタイムデータと履歴データを共有するためのメカニズムです。
- Webサーバー拡張 - 監視システムのコアアーキテクチャとWebクライアント間のインターフェースに使用されるコンポーネントのセットです。
- サードパーティシステムへのインターフェース - CMMS、GIS、ERP、MESなど

機能と役割の割り当てはライセンスを使用します。
ライセンスの詳細については、お近くの営業担当者にお問い合わせください。

1.1 アーキテクチャ

一般的なアーキテクチャは次のとおりです。

•スタンドアロン - すべての SCADA 機能が 1 つのステーションに組み込まれています。

•マルチステーション -アーキテクチャ- SCADA 機能は、クライアント/サーバー アーキテクチャ内の2つ以上のステーションにまたがります。

•高可用性アーキテクチャ- SCADAの機能と役割は分散化されており、より優れた耐障害性と拡張性を実現します。 マルチステーション展開には、以下のシナリオが含まれます。

- データ取得の冗長性-2つ以上のステーションが冗長(ホットスタンバイ)として構成
- 履歴データの冗長性-2つ以上のステーションが冗長(ホットスタンバイ)として構成
- 共有サーバー

• 3層アーキテクチャ- 1つ以上のステーションをゲートウェイとして使用

• エンジニアリングステーション - バージョン管理機能付 き

• Web &モバイル - Web バックエンドサーバーと Webベースおよびモバイル クライアント

1.2 役割

上記のアーキテクチャでは、次の役割の割り当てが必要です。

•データ収集
- フィールドデバイスとの通信
- リアルタイムデータとアラームの生成
- 他のステーションへのリアルタイムデータとアラームの提供

•履歴データ
- 他のステーションによって生成されたリアルタイムデータとアラームを取得
- データの保存、履歴データの記録と再生を処理
- RDBMS への接続を管理
- 他のステーションに履歴データを提供

• Webバックエンドサーバー
- 他のステーションによって生成されたリアルタイムデータとアラームを取得
- 他のステーションによって生成された履歴データを取得

- IISとのインターフェースを管理

- WebVueクライアント、TouchVueクライアントなどのWebクライアントにサービスを提供

WebScheduler と Web サービス ツールキット クライアント

•ゲートウェイ

- 2つのネットワーク間でデータを安全に転送

- 1つのネットワーク上の他のステーションによって生成されたリアルタイムデータ、アラーム、履歴データを受信

- リアルタイムデータ、アラーム、履歴データを別のステーションに提供

ネットワーク

•UI

- ユーザーに、ミミック、グラフィック、アラーム ビューアー、ログ ビューアー、トレンド ビューアーなどを表示

役割の組み合わせに応じて、Supervisor のステーションはデスクトップ用オペレーティングシステムまたはサーバー用オペレーティングシステムのいずれかで構築するのが適しています。

1.3 アーキテクチャの構成要素

1.3.1 凡例

HTML5

ファイアウォール

Webバックエンドサーバー

独自のアーカイブ

HDSアーカイブ

スタンドアロン

PcVueネットワークアクセス

サーバーステーション

クライアントステーション

中央バージョンフォルダ

フロントビュー

PcVue

構成要素	役割	導入構成
スタンドアロンステーション 	• データの取得 • 過去データ • HMI • 他のステーションとデータを交換する機能はありません	• デスクトップ版アプリケーション • デスクトップOS環境で実行
SCADAステーション 	• データの取得 • 過去データ • HMI	• デスクトップ版アプリケーション • デスクトップOS環境で実行
データ取得サーバーステーション 	• データの取得	• Windowsで動作 • デスクトップOS環境で実行
SCADAステーション 	• データの取得 • 過去データ • HMI	• デスクトップ版アプリケーション • デスクトップOS環境で実行 • サーバーOSにRemote Desktop Servicesを構成し、 シンクライアント等の軽量端末を操作用ワークステーションとして使用する形態。
SCADAステーション 	• データの取得 • 過去データ • HMI	• デスクトップ版アプリケーション • デスクトップ用OS
SCADAステーション 	• データの取得 • 過去データ • HMI	• デスクトップ版アプリケーション • デスクトップ用OS
SCADAステーション 	• データの取得 • 過去データ • HMI	• デスクトップ版アプリケーション • デスクトップ用OS

エンジニアリングステーション

- エンジニアリングステーションは、アーキテクチャやプロジェクト設計に応じて、データ収集サーバー(フィールドデバイスとの通信テスト用)からアーカイブサーバー、あるいはHMIワークステーション(設計用)まであらゆる役割を持つ事ができます。
- プロジェクトの開発と保守
- プロジェクトとライブラリの管理機能
- サードパティの生産ツールとの相互運用性
- デスクトップ版アプリケーション
- デスクトップ用OS

2. アーキテクチャ

このトピックでは、最も一般的なベースアーキテクチャについて説明します。システム要件に合わせて、以下の点から様々なバリエーションが存在します。

- ユーザー数
- オペレーターステーション（HMI）の種類と数
- 可用性
- 柔軟性
- 拡張性
- 耐障害性
- 保守およびアプリケーションライフサイクル管理

詳細についてはテクニカル サポートにお問い合わせください。

2.1 スタンドアロンステーション

✓最もシンプルなアーキテクチャ
✓単一の「オールインワン」ステーションからプロセスを監視および制御する
✓スタンドアロン構成におけるPcVueステーションの全機能を利用可能

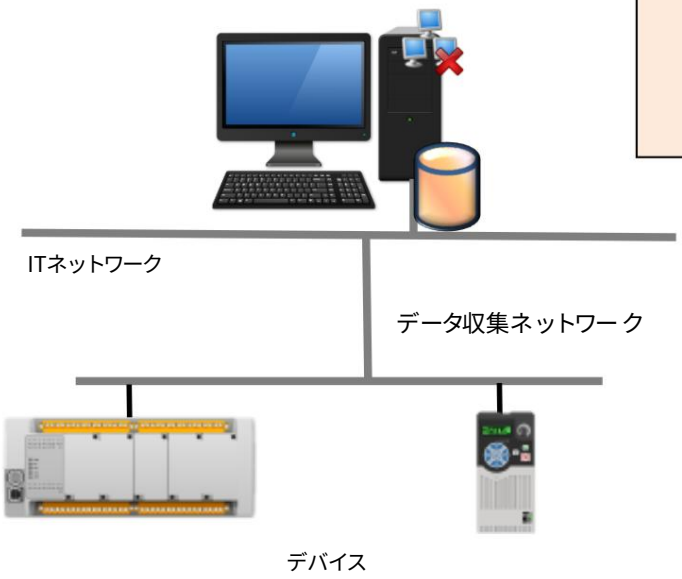


図1 - スタンドアロンステーション

スタンドアロン ステーションは通常、オペレータ パネルであり、すべての機能と役割が 1 つのステーションに統合された最もシンプルなアーキテクチャです。

従来のシングルユーザー構成では、 PcVueは産業用ネットワーク上のすべてのデバイスを監視および制御し、ユーザーからのリクエストも処理します。PcVueは、単一のステーションで数万もの変数をサポートできます。
PcVueシングルステーションは、 PcVueの標準機能を使用してプロセスを監視および制御するオールインワンのスタンドアロン HMI ステーションです。

- ✓ データ収集
- ✓ リアルタイムデータベース
- ✓ HMI
- ✓ アーカイブ
- ✓ アラームとログ
- ✓ トレンド
- ✓ データ処理、レポート
- ✓ ユーザー管理

2.2 マルチステーション

✓ 最もシンプルなマルチステーションアーキテクチャ
✓ プロセスは複数のリモートユーザーステーションから監視されます
✓ データ処理ネットワーク負荷の最適化

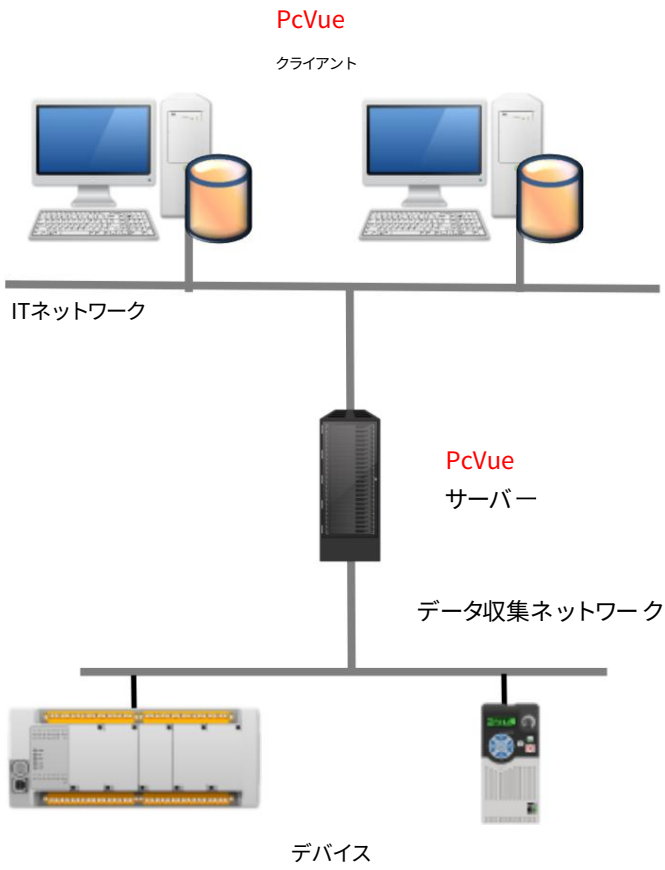


図2 - マルチステーション

最もシンプルなクライアント／サーバー構成であり、単一の産業ネットワーク接続で複数のユーザーステーションを必要とするアプリケーションに適しています。
サーバーはデータソース（プロデューサー）として機能し、各デバイスと通信を行い、クライアント（コンシューマー）ステーションへデータを送信します。
PcVueステーション間の通信は非同期で動作し、PcVue独自のTCP/IPメッセージングを用いてデータをパケット単位で送信します。
サーバーステーションは、フル機能のユーザーステーションとして構成することも、データ収集専用サーバーとすることも可能です。
アプリケーションにおけるすべてのデータ処理はサーバー側で実行されます。履歴データはサーバー側のみに保存することも、各クライアントステーションにローカル保存することも可能です。

クライアントは、プライベート電話回線や衛星リンクなど、十分な容量を持つ TCP/IP をサポートする任意のメデ ィアを使用した接続を介して、別の領域にあるサーバーに接続できます。

通常のバリエーションとしては、データ収集（Data Acquisition）と履歴データ生成（Historical Data production）を2台の異なるサーバーに分離する方法や、クライアント側で履歴データをローカルに生成する構成があります。

2.3 リモートデスクトップサーバーを備えたマルチステーション

クライアントステーションの展開

✓管理の手間とコストを削減
✓低コストのシンクライアント端末
✓シンクライアントにインストール不要

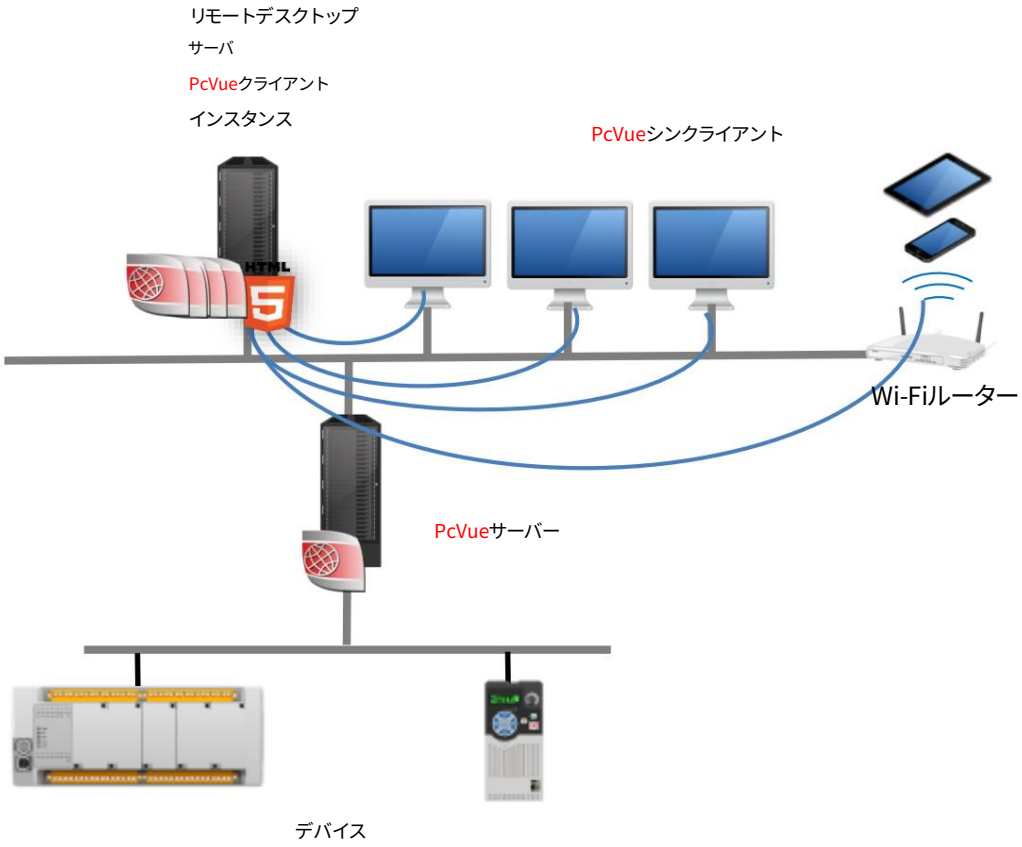


図3 - リモートデスクトップアーキテクチャ

Windows Serverにリモートデスクトップサービスを設定すると、複数のユーザーが1台のサーバーのリソースを 同時に使用し、サーバーにインストールされたアプリケーションを実行できるようになります。
ユーザーは、ネットワーク経由でサーバーに接続されたシンクライアント（ターミナルとも呼ばれます)を使用して アプリケーションを操作します。

この方法でWindows Serverに接続する方法はリモートデスクトップセッションと呼ばれ、リモートデスクトッププロトコル（RDP)と呼ばれる標準プロトコルを使用します。シンクライアント（LinuxまたはUnix上のWyse Thin Computing端末を含む)は、RDPを管理するためにRDPクライアントソフトウェアを使用します。

Windows Server は、リモートデスクトップを使用したセッションに加えて、ローカルモニター、キーボード、マウスを使用したセッションも実行します。これはローカルセッション（またはコンソールセッション、対話型セッションと呼ばれることもあります)と呼ばれます。

RDセッションホストサーバー上で監視制御アプリケーションを実行する場合、各リモートデスクトップセッションまたはローカルセッションから監視制御アプリケーションのインスタンスを実行できます。インストールされる監視制御アプリケーションは1つのみとなります。

このアーキテクチャは、監視制御アプリケーションのネットワークの観点から見ると、クライアント ステーションの展開を合理化する方法として RDS と軽量端末が使用される点を除いて、前のアーキテクチャと同じです。

この例では、 Windows Server がリモート デスクトップ サーバー (RDS) として動作しているステーションにPcVueクライアントがインストールされています。

このステーションはRDセッションホストサーバーであり、 PcVueクライアントインスタンスをホストします。ユーザーは任意のシンクライアントからリモートデスクトップセッションを開き、 PcVueクライアントインスタンスを実行できます。
サーバー上のHTML5インターフェースにより、 HTML5を搭載したシンクライアントは、
準拠した Web ブラウザを使用して、 RDS インスタンスを通じてPcVueアプリケーションにアクセスします。

PcVueサーバーが1台しかない場合は、RDセッションホスト上にも配置できます。

必要な数の同時セッションをサポートするには、RDセッションホストサーバーを複数のクライアントインスタンスをホストするように構成する必要があります。シンクライアントは特別なインストールを必要としないため、アプリケーションのオンサイト展開が容易になります。

2.4 高可用性

✓非常に高いレベルのセキュリティとシステム/データの可用性
✓デュアルネットワークによる安全なクライアントサーバー設定
✓複数のユーザーステーション
✓データ処理とフィールドネットワークのデータ負荷の最適化

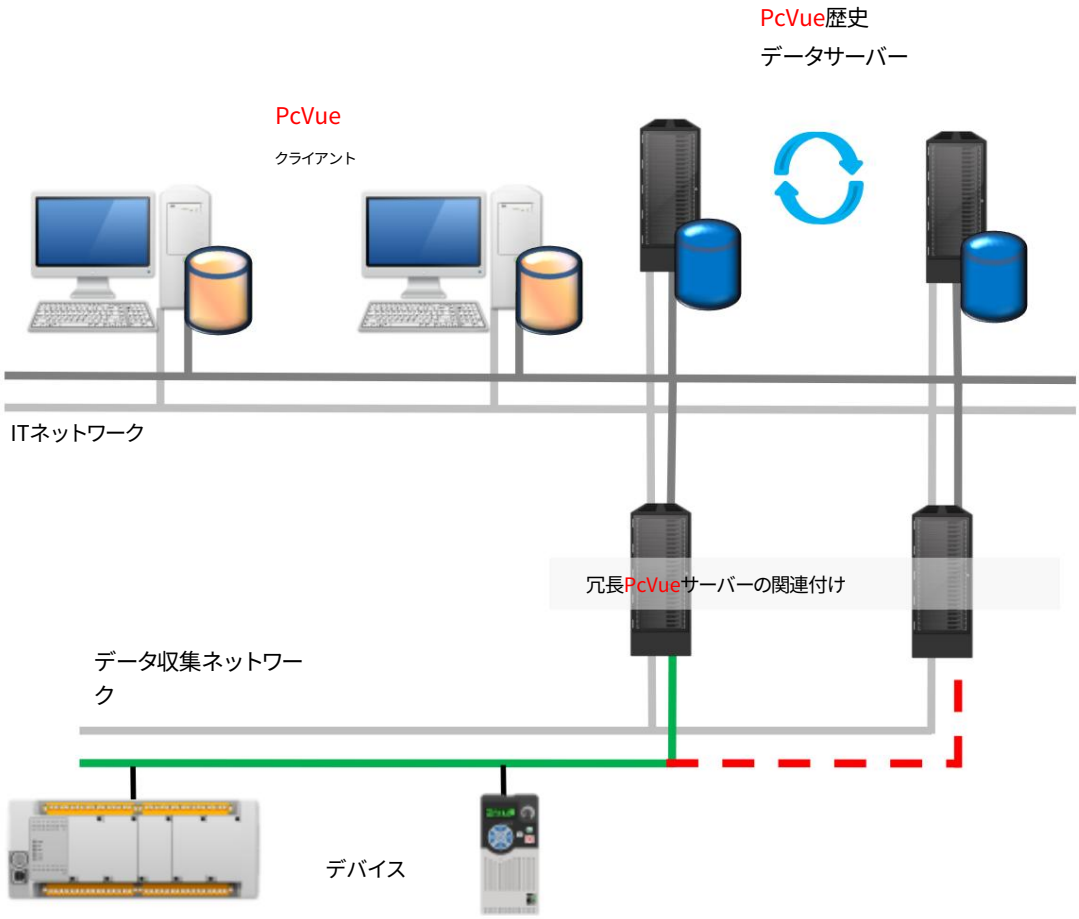


図4 - 高可用性アーキテクチャ

より高い可用性と復元力が求められる場合、より分散化されたこのアーキテクチャにより冗長性と役割の分離が実現します。

これはマルチステーション アーキテクチャに似ていますが、データ取得サーバーおよび履歴データ サーバーが分離され、冗長化されています。

ステーション間ネットワーク（LANおよび/またはWAN)は、フィールドネットワークと同様に二重化できます。これにより、クライアントステーションとデータソースの間には2つの独立したパスが確保されます。各PcVueクライアントステーションは、各サーバーと2つの接続を維持します。

ステーションに接続し、接続が動作不能になった場合にのみサーバー間の切り替えを試みます。

産業用イーサネットネットワーク上では、PcVue は通信メディアの冗長化とデバイスレベルの冗長化の両方を管理できます。
各ステーションは、履歴データの可用性を向上させるためにデータをアーカイブできます。
一般的な構成のバリエーションとして、WebサーバーおよびWebクライアントを追加し、常設のオペレーターと一時的なユーザー接続を組み合わせることもあります。

2.4.1 リアルタイム冗長性

サーバーはPLCへのデータ取得専用であり、クライアントステーションの情報（データベース）をリアルタイムで更新します。クライアントステーションには、プロセスの監視と制御のためのグラフィカルインターフェースが備わっています。
2 台のサーバーは相互に冗長化されており、サイトのクライアント ステーションにデータを供給します。

2.4.2 単一アクティブ取得サーバーモード

サーバーはシングルアクティブ取得サーバーモードで動作します。産業用ネットワークと通信するサーバーは「アクティブ」サーバーと呼ばれます。もう一方のサーバーは「パッシブ」サーバーと呼ばれます。アクティブサーバーのみがPLCシステム上の通信を管理し、クライアントステーションにデータを送信し、パッシブサーバーと同期します。
アクティブサーバーに障害が発生した場合、パッシブサーバーが取得システムとの通信を再開し、クライアントステーションにデータを送信します。切り替えはホットスイッチで行われ、オペレーターにとって完全にシームレスです。
サーバーを起動する場合、次の 2 つのシナリオが考えられます。

フェイルオーバー動作
パッシブサーバーがアクティブに昇格すると：
・産業ネットワークとの通信は即時再開
・新アクティブサーバーは即座に運用可能状態となる

クライアントへのデータ送信
・クライアントステーションは、アクティブサーバーからイベントベースかつ自動的にデータ配信されます（時刻T基準）
・オペレーターはどのステーションからでも同一の操作が可能（制御／コマンド／確認応答／アーカイブ参照など）
ネットワーク状態に関係なく、データの発生元は完全に透過化されています。

アクセス制御と監視
・ユーザープロファイルに応じて、各クライアントワークステーションからサイト情報の全部または一部へアクセス可能
・どのステーションからでも、ネットワーク上の全ステーションおよび収集システム通信の状態を確認可能

システム可視化
システムは、接続されているPLCおよび監視制御アプリケーションをリアルタイム表示し、完全なアーキテクチャ図を提供します。

システムはメンテナンスの問題を考慮し、ネットワークの状態に応じて動作します (例: パッシブ サーバーを強制的にアクティブにする)。

2.4.3 アーカイブの冗長性

2.4.3.1 2つの同期アーカイブデータベースを使用するモード

2台のサーバーは履歴サーバーとしても機能し、それぞれ独立した Microsoft SQL Server のリレーショナルデータベースに並行してログを記録します。
両サーバーは同一の情報を同時に記録します。
設定可能な過去日付範囲を超えたデータは、自動的に削除されます。
これによりデータベース容量が制御され、必要とする履歴の「保持期間（depth）」に対して最適なアクセス時間が保証されます。
削除されたレコードは、必要に応じてバックアップ目的でASCIIファイルから復元できます。
停止（故障または保守）に備えて、欠損データの自動統合処理が定期的に実行されます。
この統合は相互に行われます。
第1サーバーは第2サーバーから不足分の履歴を取得し、第2サーバーも同様に第1サーバーから取得します。
統合完了後、両リレーショナルデータベースは完全に同一の状態になります。
統合処理は、通常のデータベースアクセス（読み取り／書き込み）および通信処理と並行して実行されます。
各 Supervisory Client は、アクティブサーバーの履歴に透過的にアクセスするため、どのクライアントステーションからでも連続した履歴データを利用できます。

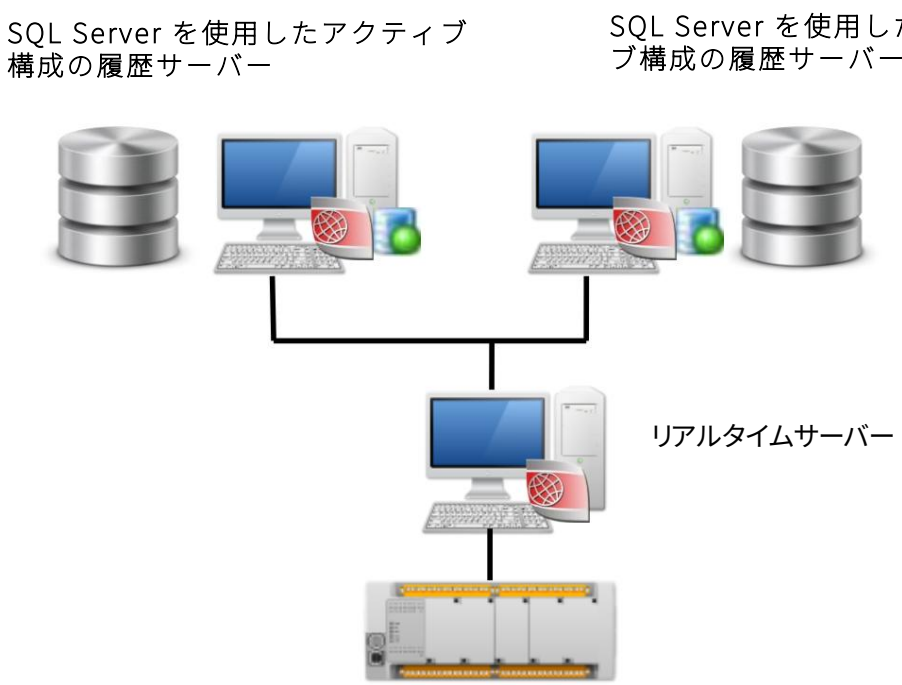


図5 – 2つの同期されたアクティブSQLサーバー

2.4.3.2 アーカイブデータベースが1つのみのモード

原則としては、データベースとSQL Server エンジンをホストし、2 つのリアルタイムサーバー PcVueとは異なるマシン (Windows Server タイプが望ましい) を用意することです。

前述の単一アクティブサーバーの原則に従い、アクティブなPcVueサーバーのみがデータベースに情報を保存します。したがって、いずれの場合も、情報をアーカイブするサーバーが少なくとも1つ存在します。

データベースをホストするサーバーに障害が発生した場合、アクティブなPcVueサーバーが情報をローカルに保存します。SQL Serverデータベースへの接続が回復すると、アクティブサーバーはローカルで生成されたアーカイブを中央データベースに転送します。
統合されたすべての機能により、少なくとも 1 台の PcVue サーバーが利用可能になった瞬間からアーカイブの継続性が確保されます。

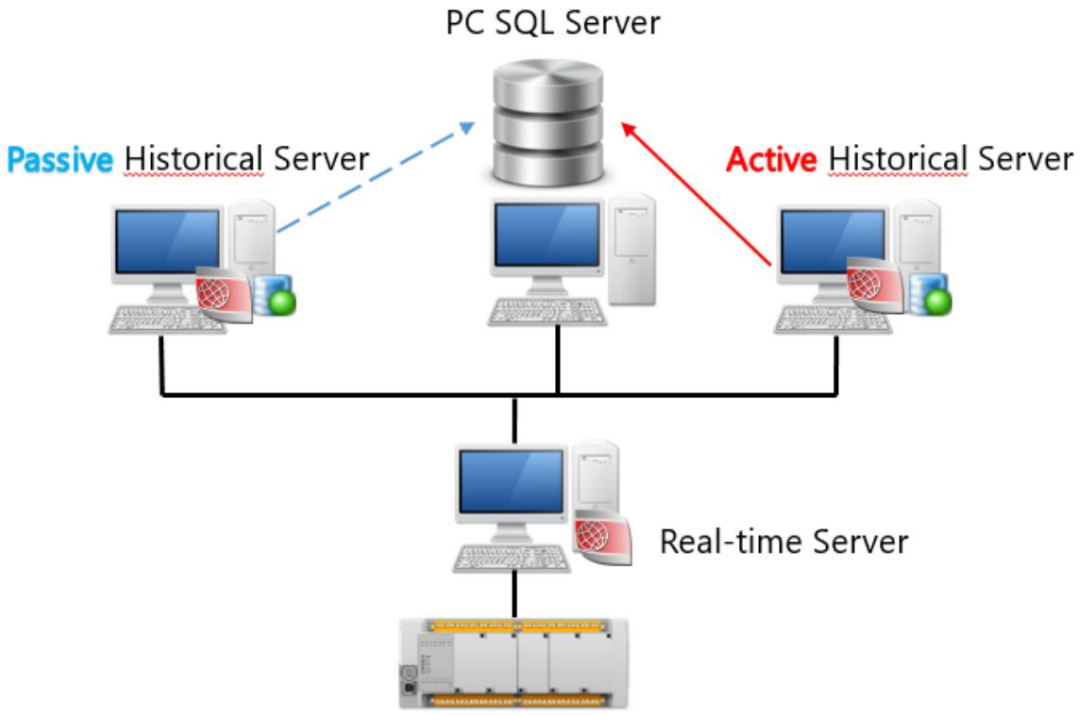


図6 – 単一のアクティブなSQLサーバー

2.4.4 RDS冗長アーキテクチャ

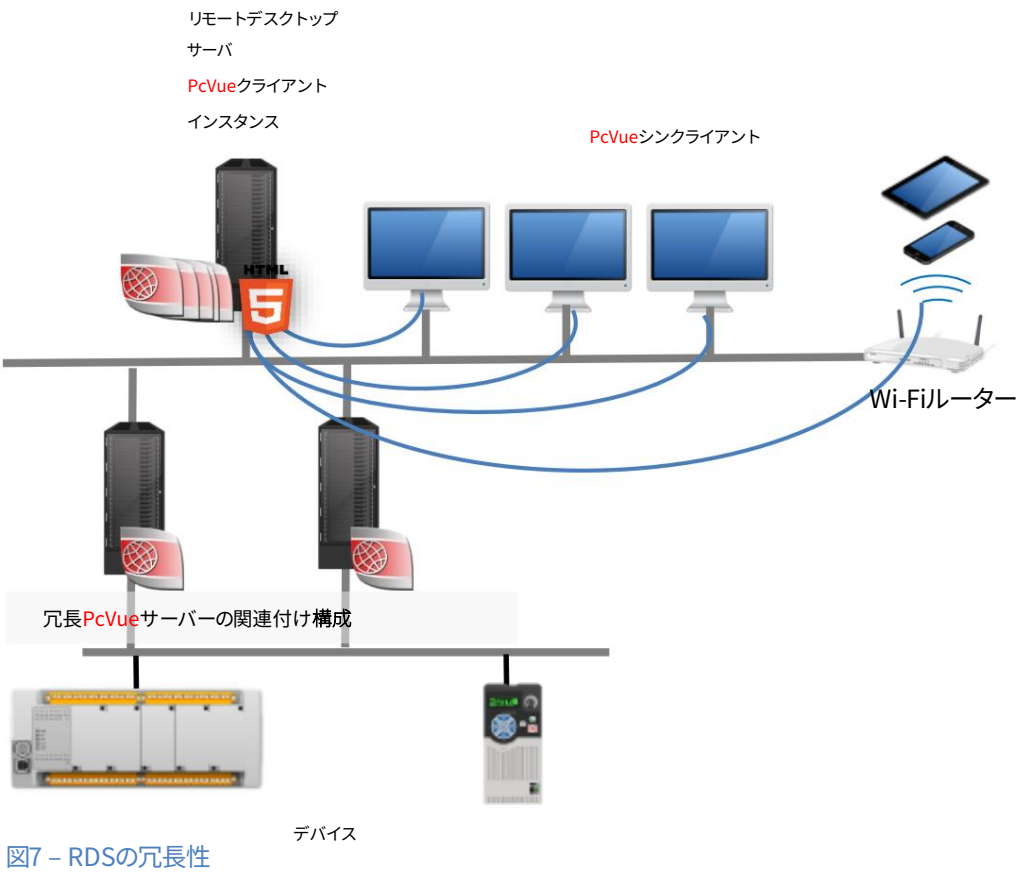


図7 – RDSの冗長性

このアーキテクチャでは、2 つの取得サーバー ステーションによって冗長性が提供されます。

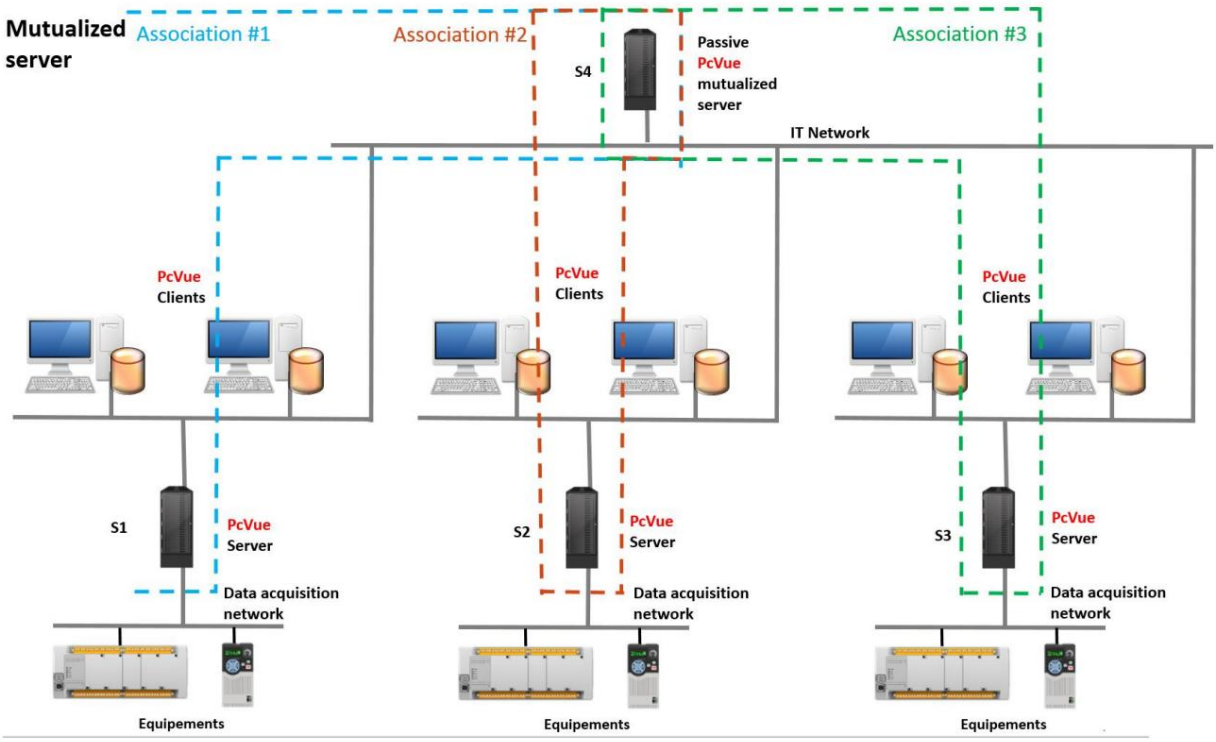
リモート アクセスは、RDS ロールを持つ Windows サーバー ワークステーションによって提供されます。

フェイルオーバーは、取得サーバーのレベルで PcVue によって自動的に管理されます。

2.5 相互サーバー

✓複数のプロセスを監視・制御するための最適化された冗長アーキテクチャ

✓導入とメンテナンスの手間を削減



Mutualized Architecture（共有型冗長構成）
ミューチャライズド・アーキテクチャは、高可用性構成をより効率的に実現するアプローチです。
複数のプロセス、生産ライン、プラント、建物、拠点などを監視・制御する環境において、信頼性の高いネットワークが構築されていれば、1台の高性能サーバーを複数ゾーン共通のスタンバイサーバーとして活用できます。
この「スタンバイサーバーの共有化」により
・冗長性（Redundancy）を確保
・高可用性（Availability）を維持
・サーバー導入台数を削減
・運用・保守コストを最適化を同時に実現できます。
従来のように各ゾーンごとに完全な二重化構成を構築する必要がないため、設備投資を抑えながらエンタープライズレベルの信頼性を提供できる構成です。

上記のアーキテクチャは、プロトコルによって動作しない可能性があります。
詳細については、テクニカルサポートにお問い合わせください。

2.6 多層構成

Multi-level（多層アーキテクチャ）
ネットワーク分離やセキュリティ要件が重要な環境では、ゲートウェイを追加した多層構成を採用できます。

この構成は、
・システムが WAN（広域ネットワーク） にまたがる場合
・クライアント端末やデータ保存先が、より信頼度の低いネットワーク側に存在する場合
といった環境で特に有効です。

ゲートウェイは DMZ（非武装地帯） に配置でき、必要に応じて冗長化も可能です。
これにより、セキュリティを確保しながら高可用性を維持できます。

分散型アーキテクチャの特長
分散構成では、各ステーションがあるデータの「提供元（プロデューサー）」となり別のデータの「利用者（コンシューマー）」にもなるといった柔軟な役割分担が可能です。

さらに、一部のステーションは遠隔地にある中央監視室向けのデータ集約サーバーとして機能させることもできます。

PcVueによるマルチサーバー／マルチクライアント構成
PcVue では、マルチサーバー／マルチクライアント構成の構築、サーバー間の柔軟な連携設定が可能です。

各サーバーは用途に応じて：
・主にフィールド機器からデータを取得するサーバー
・他のサーバーから情報を取得するサーバー（クライアント的役割）として設計できます。

中央サーバーは必要なデータのみを集約する設計とすることで、
・ネットワーク負荷を最適化
・効率的な中央監視を実現
・大規模システムでも高いパフォーマンスを維持
できます。

2.6 多層構成

✓ 非常に大規模なアプリケーションや地理的に広範囲にわたる分散システム
✓ 複数レベルの制御
✓ 柔軟

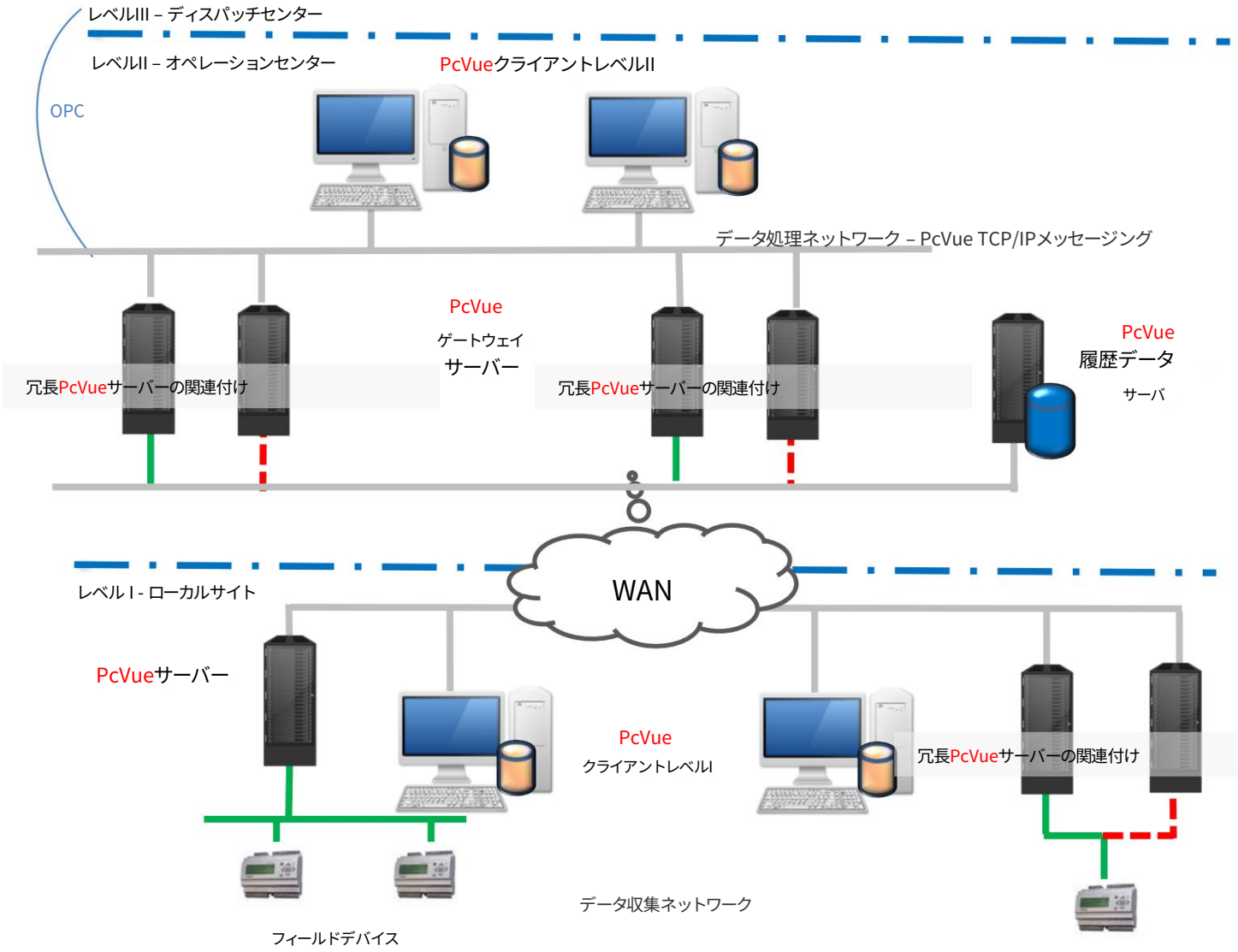


図9 - マルチレベルアーキテクチャ #1

レベルI - ローカル サイトは、広範囲に分散されたPcVueステーションで構成され、フィールド デバイスからデータを取得し、たとえば衛星接続を使用した Wide Aera ネットワークを通じてレベル II にデータを提供します。

レベルII – オペレーションセンターは、レベル I のさまざまなステーションからのデータを一元管理するために PcVueサーバーの冗長接続を備えたアーキテクチャの中核です。各サーバーの接続は、何千ものリアルタイム変数を処理し、より重要な変数をローカルにアーカイブします。

2 台のサーバーを、重要度の低いデータを DBMS にアーカイブする専用サーバーとして使用することもできます。
サーバーステーションに接続されたクライアントステーションは、操作およびエンジニアリングコンソールとして使用され、オペレーターが任意のサイトから変数を監視および制御するのに役立ちます (リアルタイム、アラームなど)。
レベルIII – ディスパッチセンターはアーキテクチャの最上位レベルです。OPC接続を介してレベルIIから統合された主要データを受信します。

2.6.2 マルチレベル: 実装 #2

✓地理的に広範囲に分散したシステム向け
✓複数のレベルの制御
✓大量のデータ/高成長率のプロジェクト向け
✓柔軟

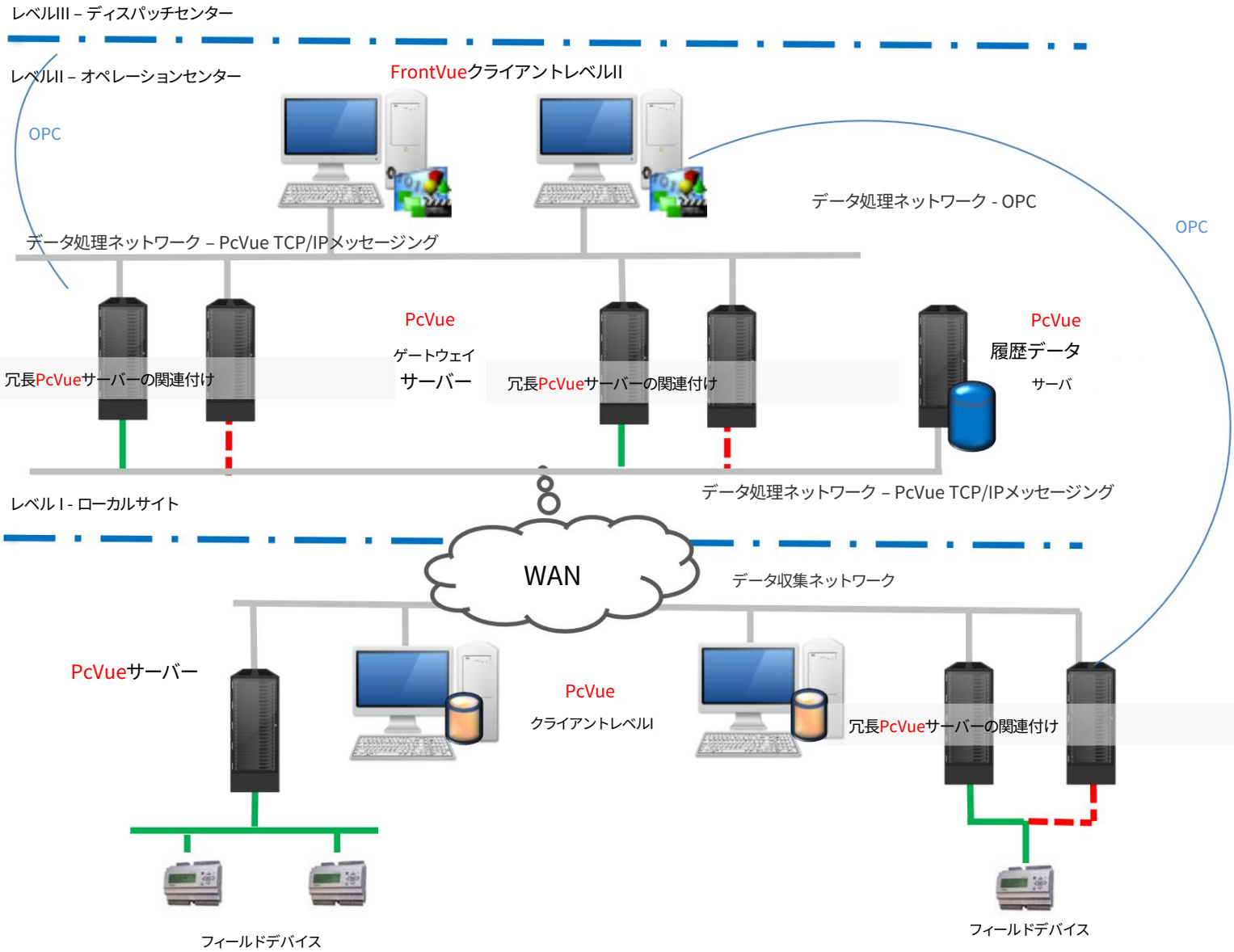


図10 - マルチレベルアーキテクチャ #2

アプリケーションの規模が拡大し（30万変数以上）、システムのスケーラビリティを確保する必要がある場合、リッチな PcVue クライアントを、より軽量な FrontVue HMIクライアントに置き換えることで、アーキテクチャを最適化することが有効です。

FrontVueは、処理機能やアーカイブ機能を内蔵しない、非常に軽量なOPCベースのHMIクライアントです。OPCクライアントとしてPcVueに接続し、PcVue側で管理されているリアルタイムデータの監視・制御、およびアラームや履歴データの表示を行います。

FrontVueは表示されているデータのみを更新するため、以下が可能になります：

クライアントのアプリケーション起動時間を最小化

ネットワーク上のデータ負荷を大幅に削減

また、FrontVueは複数のOPCサーバーへ接続可能であり、以下を実現します：

任意の特定デバイスに関する詳細情報を取得するために、リモートのローカルサーバーへ接続

複数のPcVueサーバーからのイベントを統合し、アラーム／ログビューアにおいて単一の一覧としてオペレーターへ表示

2.7 クラウドアーキテクチャ

2.7.1 アーキテクチャ #1: クラウドの相互運用性

✓ クラウドデータベースにシームレスに接続

✓ PcVue からサードパーティシステムへのデータ共有（例：ERP、SCADA、…

✓ IoTなどの既存デバイスからPcVueにデータを取得する

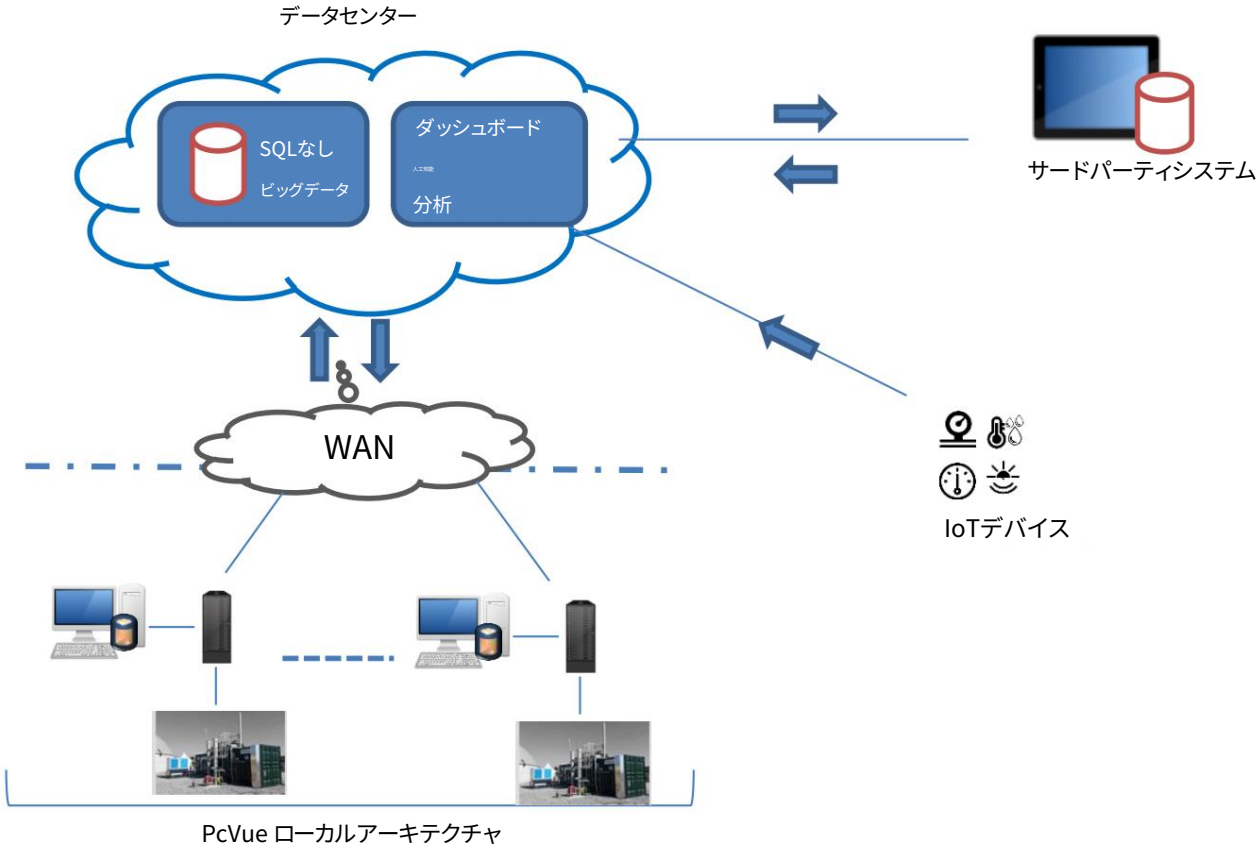


図11 - クラウドデータベースアーキテクチャ

このアーキテクチャでは、1台または複数のPcVueをローカルサイトに展開し、ローカル機器からのデータを監視および制御します。ローカルアーキテクチャは、単一ステーションから複数ステーションまで様々であり、ローカルデータベースが含まれる場合もあります。

各 PcVue サイトは、複数の接続方式を用いてクラウド データベースに接続できます。 -

ADO.netコネクタの範囲を提供するユニバーサルデータコネクタ

=> サードパーティシステムからのデータ共有と取得
=> リアルタイムの大量データには適していません

- MQTTドライバー

=> 大量のデータのリアルタイムデータ交換

このアーキテクチャにより、PcVue はクラウド データベースを活用して次のことが可能になります。

- ERPなどのサードパーティシステムに必要なデータを共有する
  SCADAなど
- ローカルシステム構成外のIoTデバイスからデータを取得する

2.7.2 アーキテクチャ #2: クラウドハイパービジョン

✓ インフラストラクチャとデータ管理の委任

✓ リソースの拡張性

✓ Webおよびモバイルクライアントを導入してあらゆるデータにアクセス

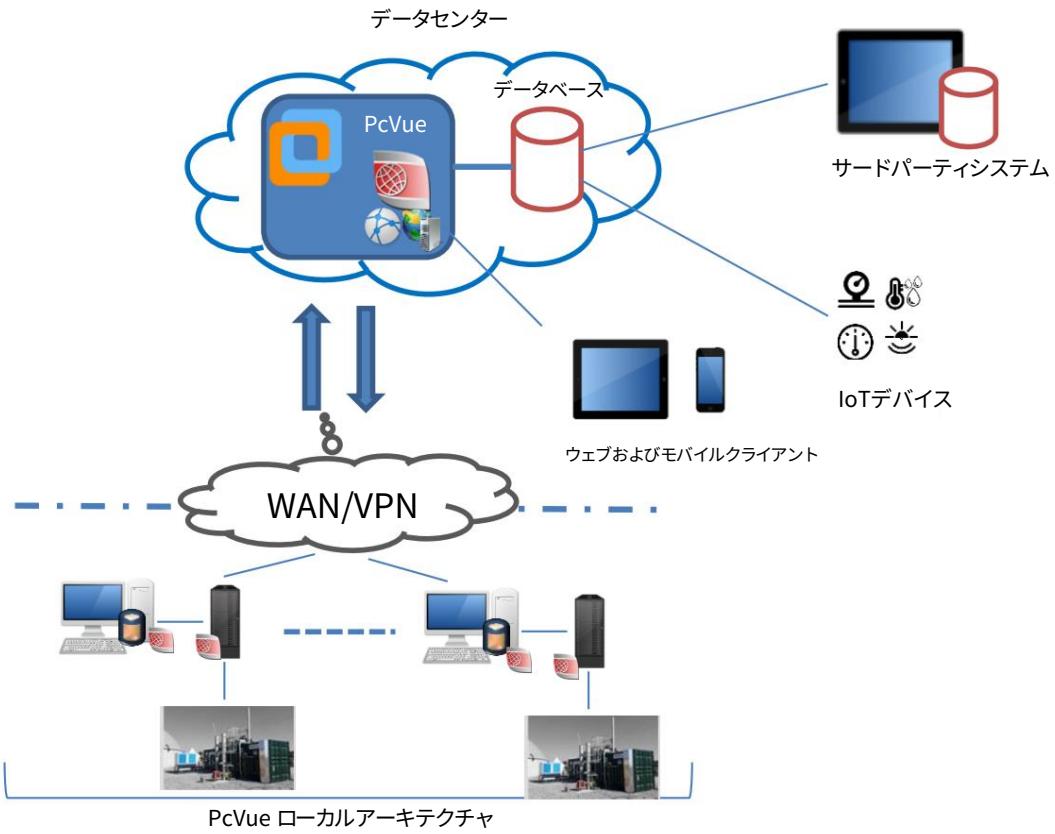


図12: クラウドハイパービジョン

現場レベルでは、1台または複数のPcVueが配備され、ローカル機器からのデータを監視および制御します。ローカルアーキテクチャは、単一ステーションから複数ステーションまで様々であり、ローカルデータベースが含まれる場合もあります。

クラウドレベルでは、PcVueは仮想マシンでホストされます。マルチステーションアーキテクチャ

必要に応じて複数の VM で使用できます。

TCP/IP マルチステーション メッセージングまたはその他のドライバーを使用して、セキュリティ保護された WAN ネットワークを介してローカル PcVue サイトからデータを収集します。

Web クライアントとモバイル クライアントは VM から展開できます。

ユニバーサル データ コネクタまたは MQTT を使用して、サードパーティ システムや IoT デバイスからのデータをデータベースから収集できます。

このアーキテクチャにより、次のことが可能になります。

✓ インフラストラクチャとデータの管理と保守をサードパーティに委託

✓ 最小限の労力で高いリソース拡張性を実現

✓ Webおよびモバイルクライアントを導入してあらゆるデータにアクセス

2.7.3 アーキテクチャ #3: ハイブリッドクラウド

✓ クラウドデータホスティング
- o メンテナンス
- o セキュリティ

✓ 物理的な中央監視室からの統合上位監視

✓ 既存のインフラストラクチャへの統合

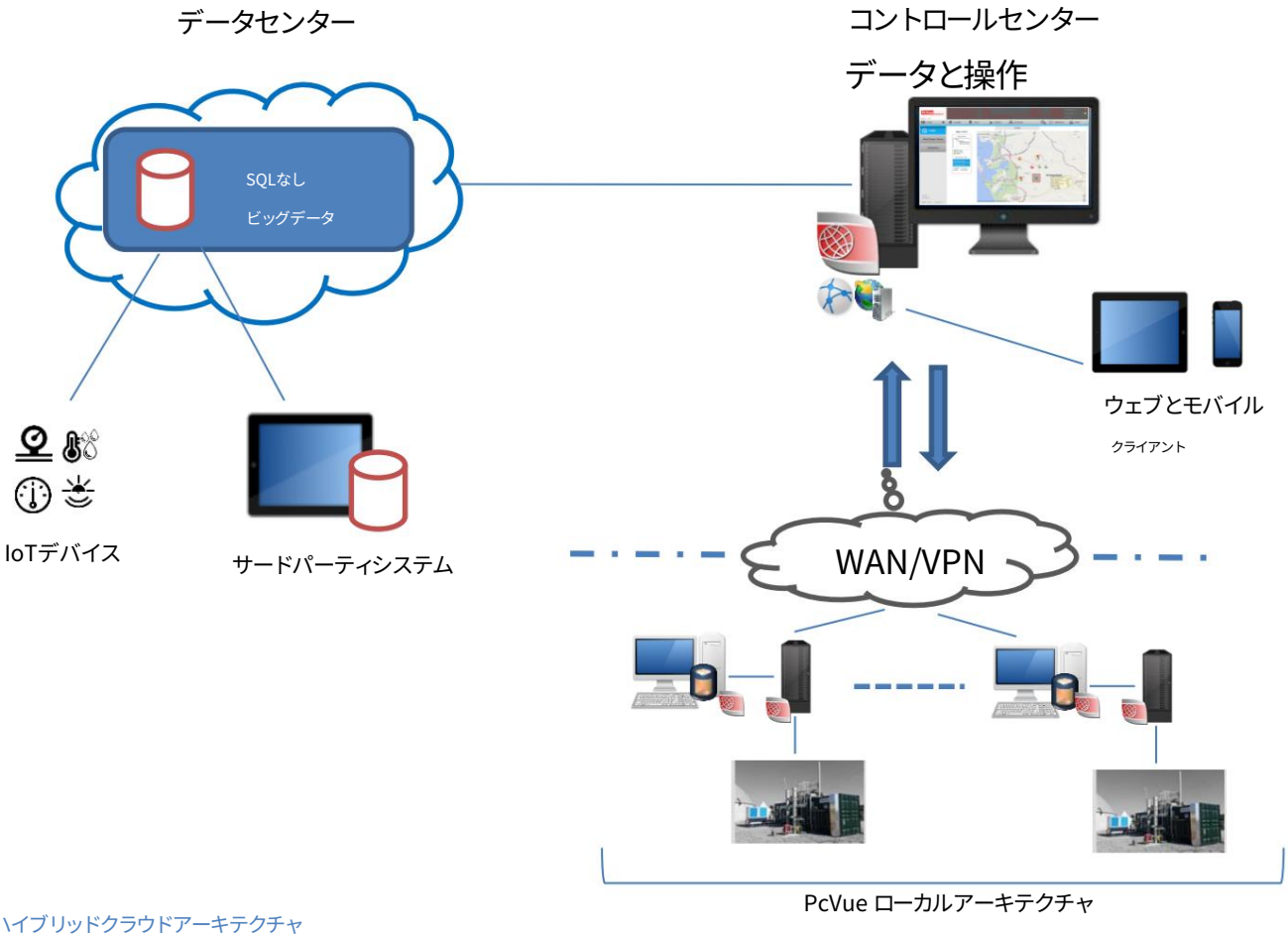


図13: ハイブリッドクラウドアーキテクチャ

このアーキテクチャでは、PcVue は、複数のデータ取得サーバーとクライアントを含む可能性のあるアーキテクチャ内のコントロールセンターでオンプレミスでホストされます。
データはクラウドデータベースに保存されます。PcVueは、UDCまたはMQTTを使用してデータベースに接続されたサードパーティシステムまたはIoTデバイスからデータを取得します。また、データベースにデータを記録することもできます。

PcVueは、安全なWAN/VPNネットワークを介してローカルPcVueサイトからデータを収集します。
TCP/IP メッセージングまたはその他のドライバーを使用して、Web およびモバイル クライアントのサーバーとして機能します。

✓ クラウドでデータをホストし、データのメンテナンスとセキュリティを委任する

✓ クラウド インフラストラクチャを既存のアーキテクチャに統合する

2.8 バージョン管理機能を備えたエンジニアリングステーション

✓ プロジェクトやライブラリのメンテナンスと展開が容易
✓ バージョン数は無制限
✓ 変更履歴の追跡
✓ エラーや損失のリスクを軽減

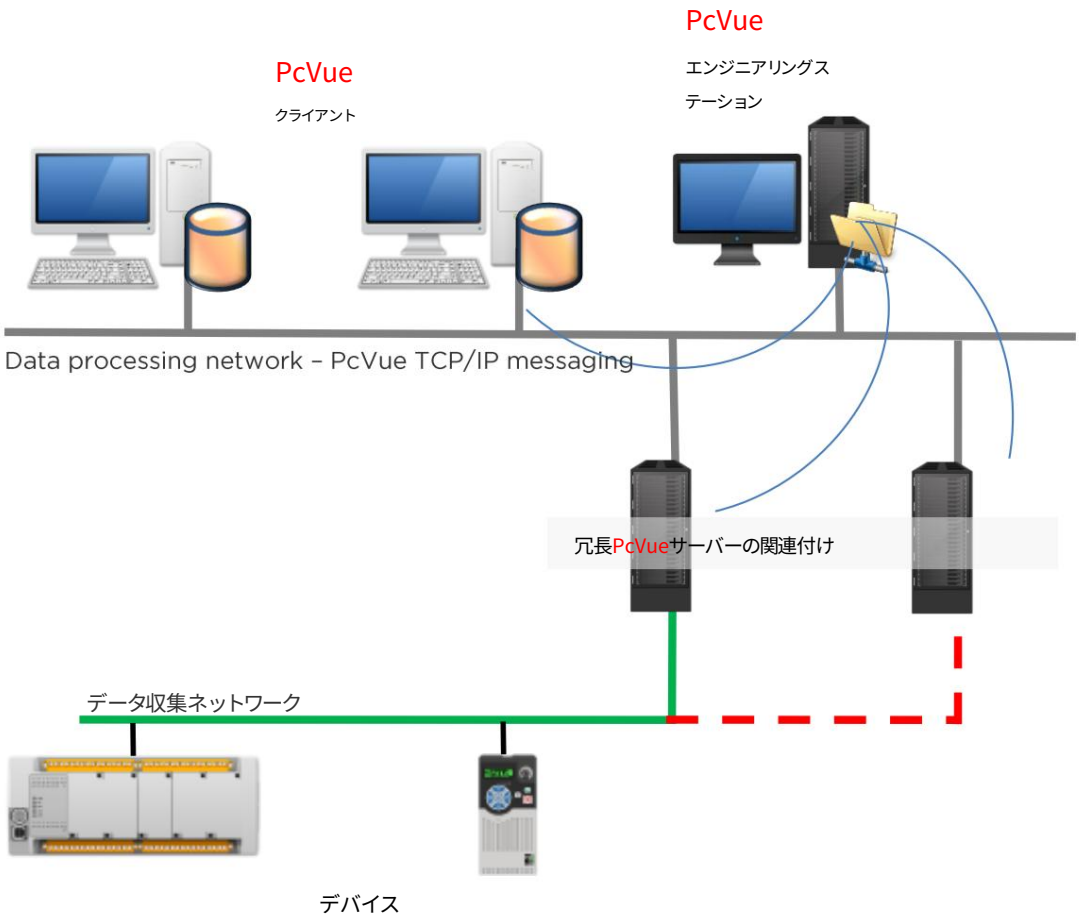


図14 - エンジニアリングステーション

プロジェクトの保守および展開をより簡単かつ迅速に行うために、PcVueには中央プロジェクト管理ツールが標準で組み込まれています。
プロジェクトやライブラリの異なるバージョンは、ネットワーク上の共有ディレクトリに一元管理されます。
これらはネットワーク上のどのステーションからでも読み込みおよび変更することが可能です。
通常は、専用のPcVueエンジニアリングステーションを使用して、中央バージョンディレクトリをホストし、プロジェクトの変更作業を行います。

ユニバーサル データ コネクタまたは MQTT を使用して、サードパーティ システムや IoT デバイスからのデータをデータベースから収集できます。

このアーキテクチャにより、次のことが可能になります。

✓ インフラストラクチャとデータの管理と保守をサードパーティに委託

✓ 最小限の労力で高いリソース拡張性を実現

✓ Webおよびモバイルクライアントを導入してあらゆるデータにアクセス

2.7.3 アーキテクチャ #3: ハイブリッドクラウド

- ✓ クラウドデータホスティング
  - o メンテナンス
  - o セキュリティ
- ✓ 物理的な中央監視室からの統合上位監視
- ✓ 既存のインフラストラクチャの統合

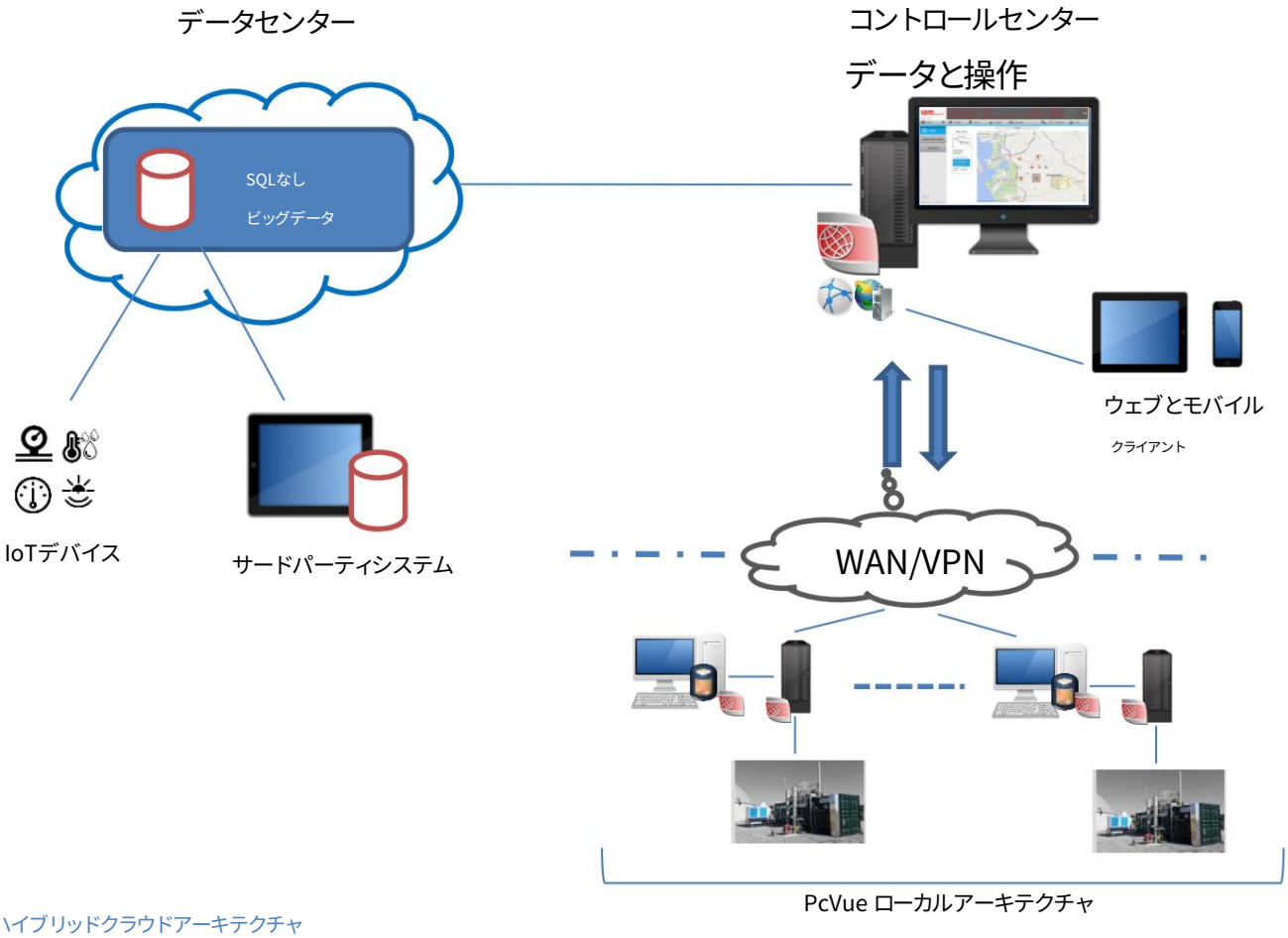


図13: ハイブリッドクラウドアーキテクチャ

このアーキテクチャでは、PcVueはオンプレミス環境の中央監視室に設置され、複数のデータ収集サーバーおよびクライアントを含む構成で運用されます。データはクラウドデータベース上に保存されます。

PcVueは、UDCまたはMQTTを使用してデータベースに接続されたサードパーティ製システムやIoTデバイスからデータを取得します。また、データベースへデータを記録することも可能です。

PcVueは、セキュアなWAN／VPNネットワークを介し、TCP/IPメッセージングやその他のドライバーを使用してローカルのPcVueサイトからデータを収集するとともに、Webクライアントおよびモバイルクライアント向けのサーバーとしても機能します。

このアーキテクチャにより、次のことが可能になります。

✓クラウドでデータをホストし、データのメンテナンスとセキュリティを委任

✓クラウド インフラストラクチャを既存のアーキテクチャに統合

2.8 バージョン管理機能を備えたエンジニアリングステーション

✓ プロジェクトやライブラリのメンテナンスと展開が容易
✓ バージョン数は無制限
✓ 変更の追跡
✓ エラーや損失のリスクを軽減

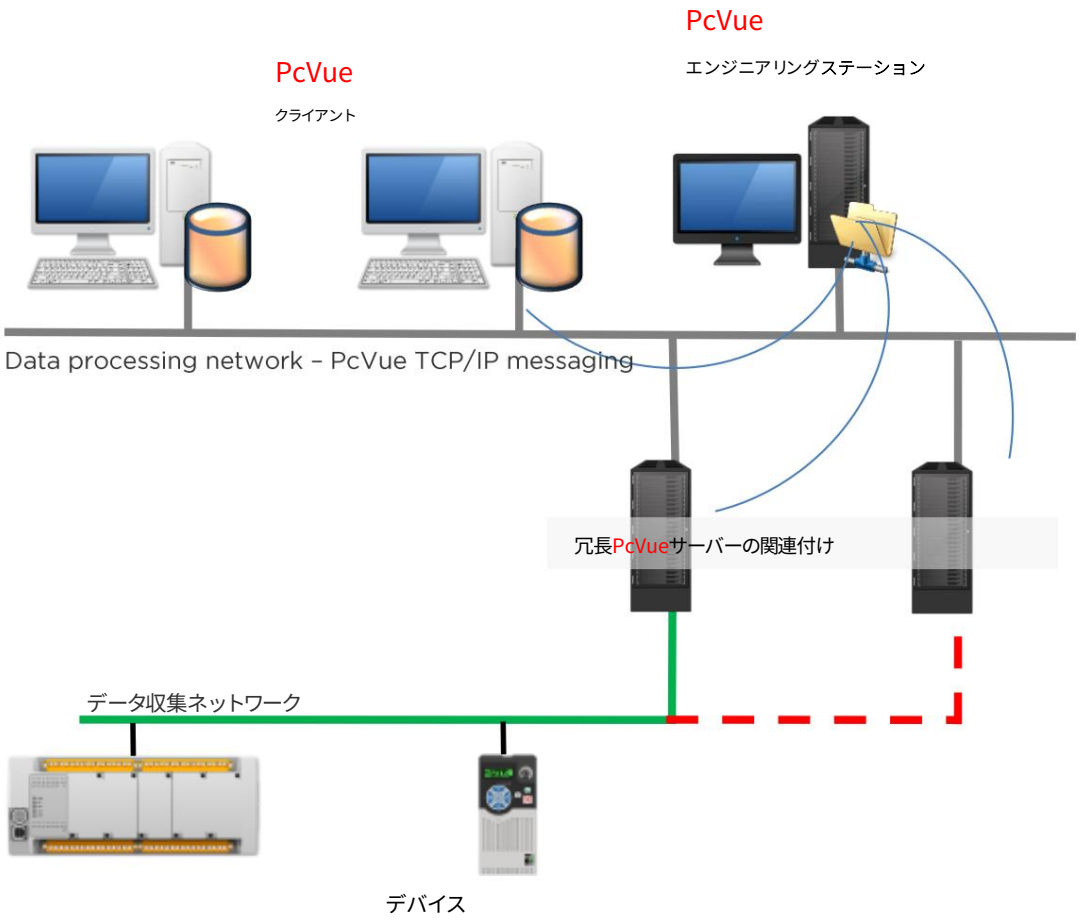


図14 - エンジニアリングステーション

プロジェクトのメンテナンスと展開をより簡単に、より迅速に行うために、 PcVueには中央プロジェクト管理ツールが組み込まれています。
プロジェクトやライブラリの異なるバージョンは、ネットワーク上の共有ディレクトリに一元管理されます。ネットワーク上のどのステーションからでも読み込み、変更できます。
通常、専用のPcVueエンジニアリング ステーションを使用して、中央バージョン ディレクトリをホストし、プロジェクトの変更を行います。

任意のステーションは、任意の種類のバージョンを手動で読み込み実行することができます。また、中央プロジェクトディレクトリから、プロジェクトおよび／またはライブラリの参照バージョンを自動的に読み込み、実行することも可能です。

サポートされている機能は次のとおりです。

- 3種類のバージョン :開発版、運用版、リファレンス版
- バージョンごとの内容を設定可能
- 各バージョンの変更履歴を追跡
- 自動バージョン番号付与システム
- バージョン数は無制限（ストレージの空き容量に依存）

2.9 Webとモバイルのアーキテクチャ

本セクションでは、PcVue 12以降に対応したWebおよびモバイル対応アーキテクチャを展開するためのベストプラクティスおよび一般的な構成パターンについて説明します。

PcVue 12では、Webおよびモバイルコンポーネントの展開や、大規模なIT環境への統合に関して、いくつかの改善が行われています。

特に、Webサーバーレイヤーを産業用ネットワークから分離することが可能となりました。

この新しい役割分離機能を活用し、WebサーバーマシンをDMZ上に配置して産業用ネットワークまたはSCADAネットワークから分離することを強く推奨します。

ただし、この構成はすべての導入シナリオにおいて実用的とは限りません。特に小規模システムにおいては適用が難しい場合があります。そのため、本ドキュメントでは以下のようなさまざまな導入シナリオに焦点を当てています。

- スタンドアロンのオールインワンセットアップのための簡素化されたアプローチ
- 大規模エンタープライズSCADA/HMIシステム
- 小規模システムへのリモートアクセス

2.9.1 イージーモバイルテクノロジー

PcVueの Web およびモバイル ソリューションは、独自の専用テクノロジである EasyMobileTechnology を採用しており、ゲートウェイ/プラグインなしでモバイル アーキテクチャをセットアップし、必要なすべてのセキュリティ機能 (https、Oauth、証明書) と HTML5 テクノロジ、およびメンテナンス ツールを組み込むことができます。

このテクノロジーは次の基準に適合します。

・ゲートウェイ不要、追加プラグイン不要
・クライアント側でのインストール不要
・簡単な設定(スクリプト不要、ウィザードのみ)

- サードパーティのアプリケーションに対応
- エンドユーザー、SI、ITなどあらゆるユーザーに適応
- 安全でスケーラブルなアーキテクチャと通信
- 簡単な診断

2.9.2 Webデプロイメントコンソール

Web Deployment Consoleは、Webまたはモバイルアーキテクチャの設定、展開、および保守を行うためのコンポーネントです。
本コンソールは、以下の機能をサポートしています：

✓ IIS 上の Web サービスと Web アプリの展開
✓ PcVue Webバックエンドエンドポイント管理
✓ データ保護管理
✓ 証明書管理
✓ ユーザーアクセスログとOAuthサーバー管理
✓ IIS監査/診断

Web 配置コンソールは、Web サーバー IIS をホストするサーバー上で実行されます。

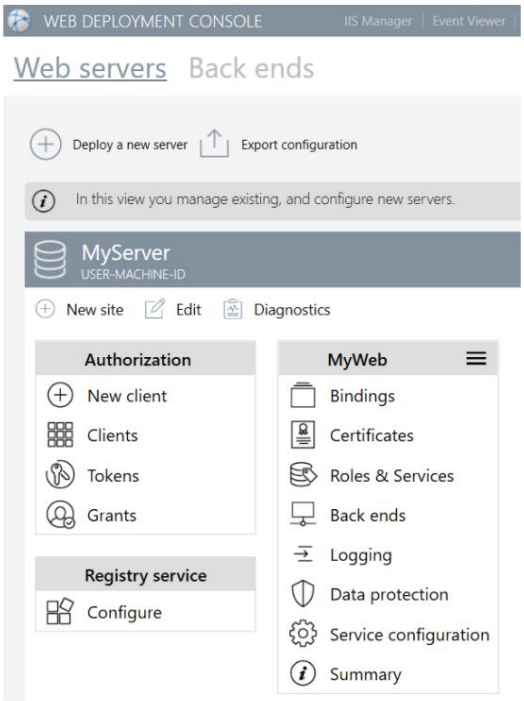


図15 – Webデプロイメントコンソールインターフェース

2.9.3 Webおよびモバイルクライアント

2.9.3.1 HTML5 Webクライアント

WebVueは、Webブラウザとインターネットまたはイントラネット接続を使用して、 PcVueプロジェクトのリモート表示と制御を提供するWebクライアントです。適切なユーザー権限（ユーザー名とパスワード）を持つユーザーは、ネットワーク上のどこからでもPcVue SCADAアプリケーションにアクセスできます。WebVueはWebブラウザで実行されるため、オペレーティングシステムに依存せず、 PcVueのミミックを直接表示します。変更は一切不要です。

PcVue Web サーバーとWebVueクライアント間の通信では、 Microsoft IIS テクノロジとエンタープライズファイアウォールを共同で使用してセキュリティを管理します。

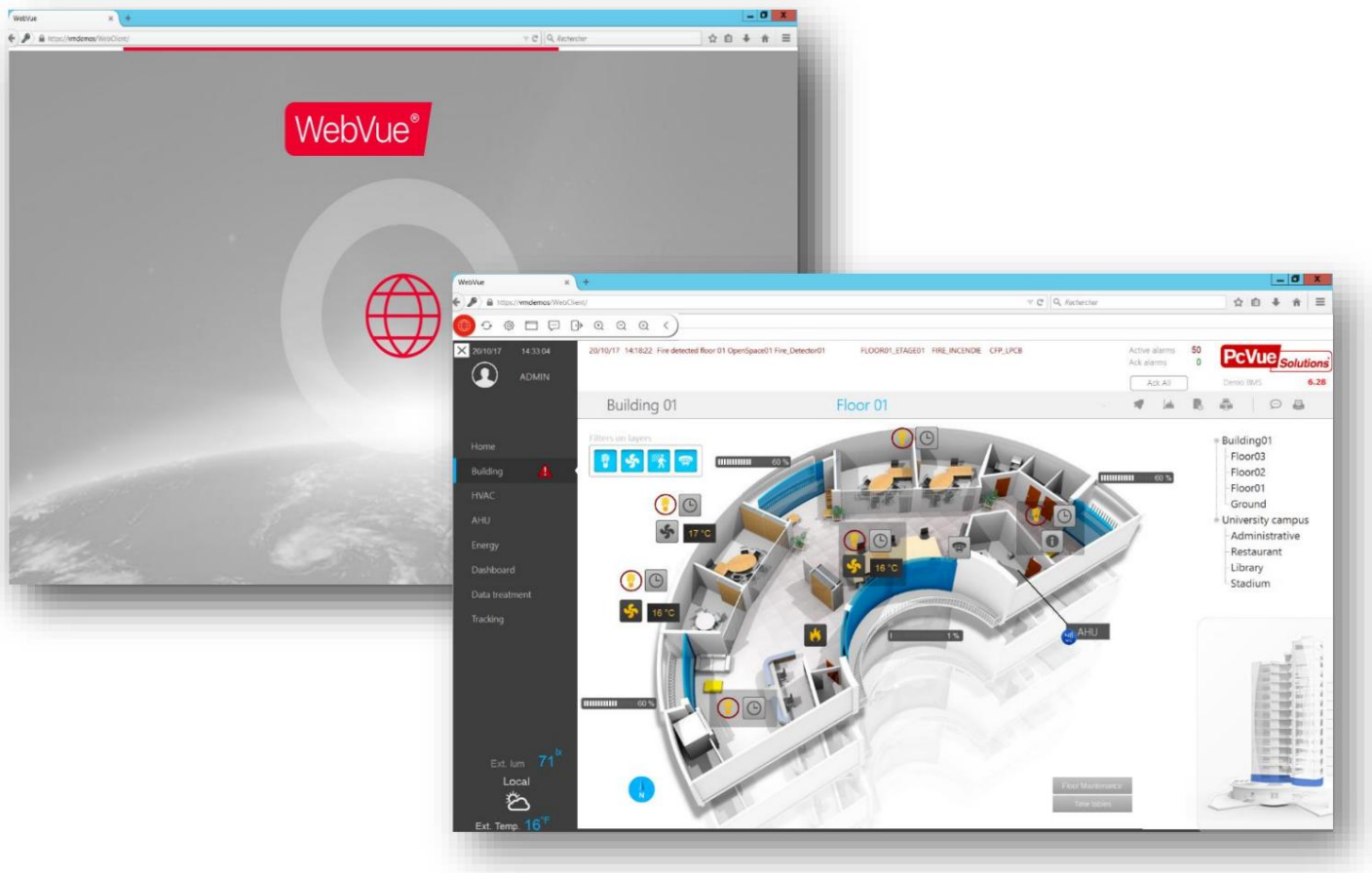


図16 - HTML5 Webクライアントのスクリーンショット

2.9.3.2 TouchVue - アラームとイベント通知を備えたモバイルアプリケーション

TouchVueモバイルアプリケーションを使用すると、モバイルデバイス（タブレット、スマートフォンなど）からPcVue Webサーバーの公開Webサービスにアクセスし、変数のリアルタイム値、各種アラームリスト、履歴リスト、曲線のトレンドなどを確認できます。これにより、オペレータはアラームの確認や値の設定などを行うことができます。

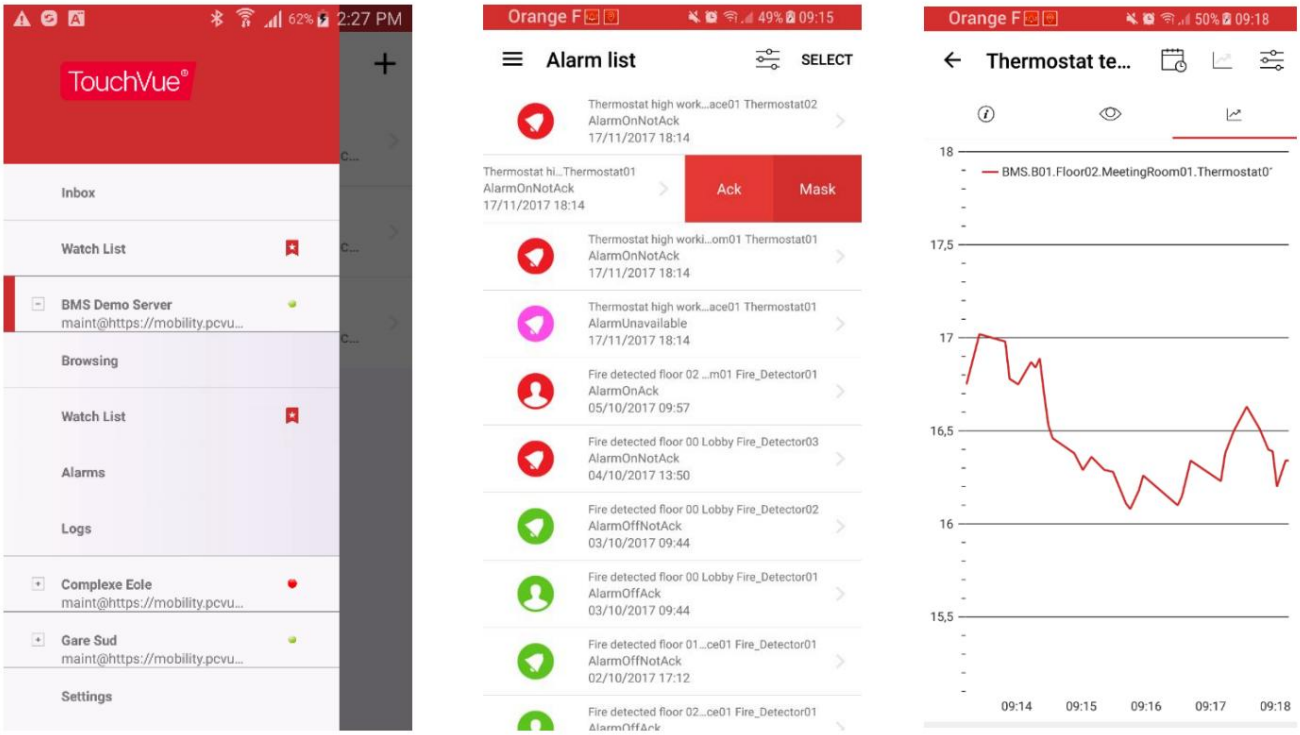


図17 - TouchVueクライアントのスクリーンショット

2.9.3.3 SnapVue – 位置情報に基づいたモバイルアプリケーション

SnapVueは、PcVueプロジェクトのコンテキストサーバーと連携するモバイルアプリケーションであり、モバイルユーザーがナビゲーション操作を行うことなく、自身の位置情報および役割に応じた関連情報へアクセスできるようにします。
ユーザーは、設計段階でカスタマイズ可能なインターフェースを通じて、周囲の設備の監視および制御を行うことが可能です。

また、音声・動画・テキスト・画像によるメッセージを他のユーザーおよびPcVueサーバーとやり取りできるメッセージングシステムなど、運用を支援する各種サービスを提供します。
さらに、ボットシステムにより、あらかじめ定義されたシナリオに基づいてユーザーを支援することも可能です。

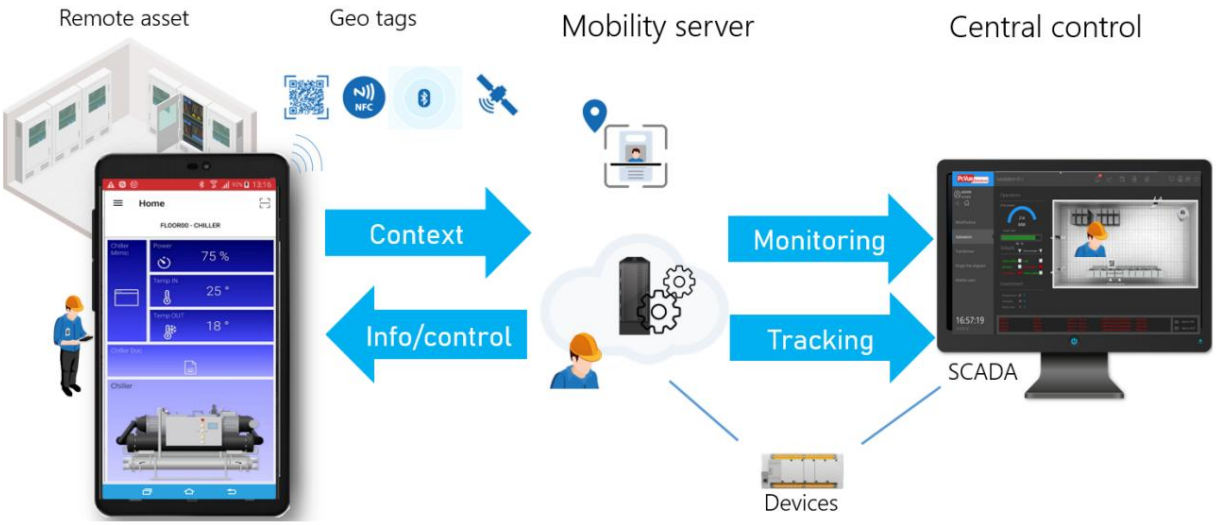


図18 – SnapVue: コンセプト

SnapVue は、以下に示すように地理位置情報のテクノロジーとサービスを使用します。

図19 – SnapVue: テクノロジー

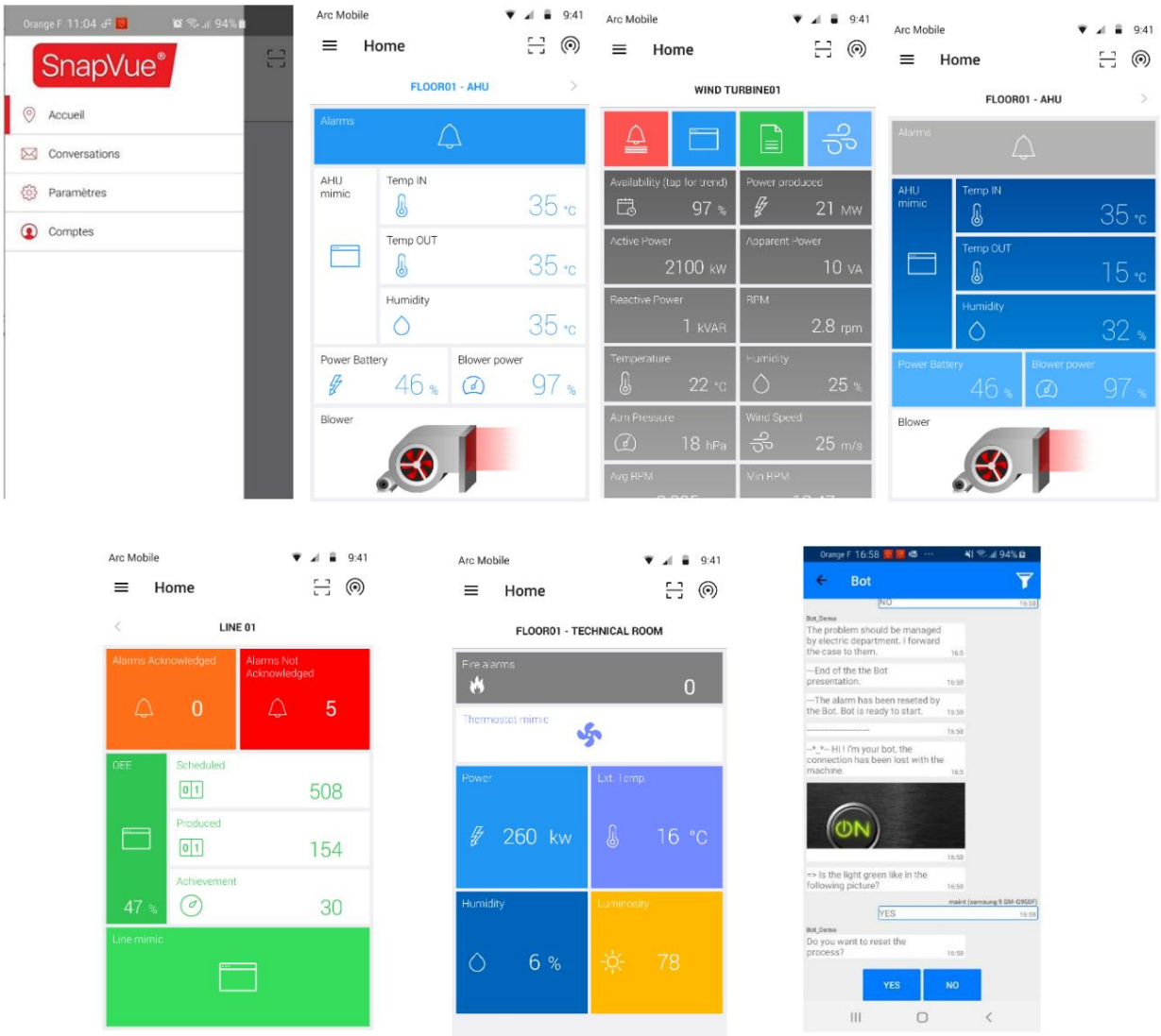


図20 – SnapVue: スクリーンショット

2.9.4 リモートデスクトップアクセス

PcVue は、PC またはその他の端末から Windows リモート デスクトップ機能を使用してリモートで実行できます。

HTML5 テクノロジーにより、どのインターネット ブラウザーからでもこの機能を利用することが可能となります。

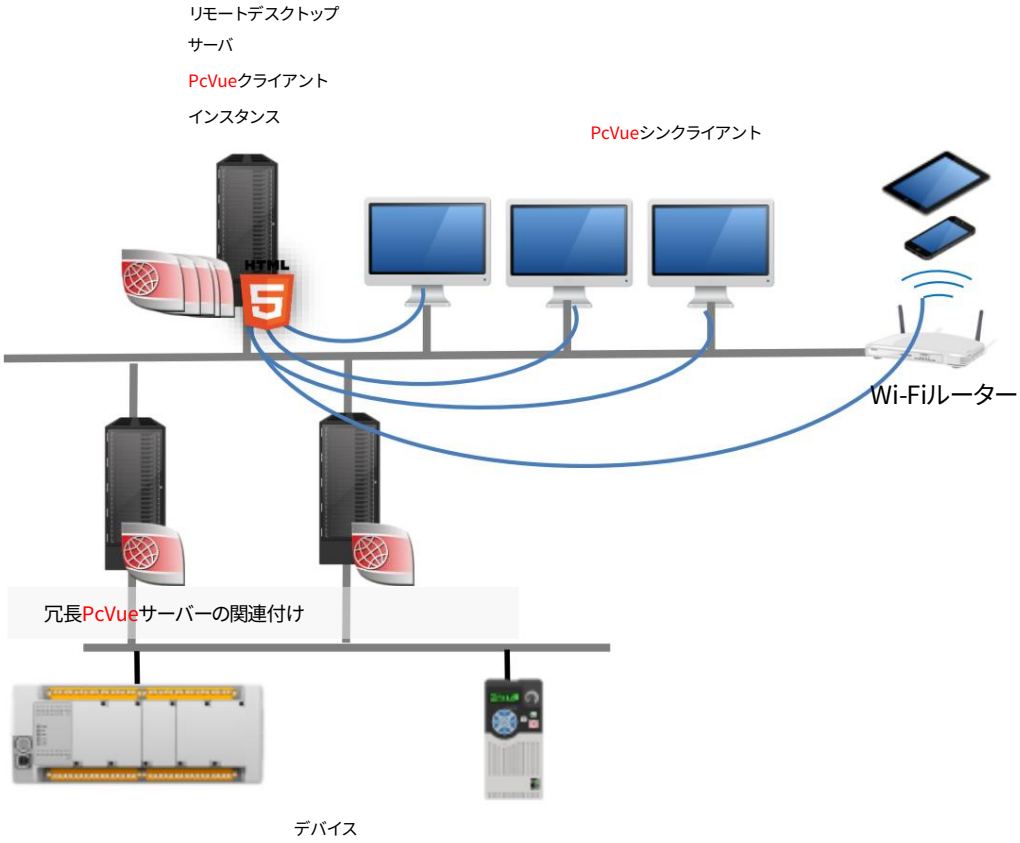


図21 – リモートデスクトップアクセス

2.9.5 アーキテクチャ #1: オールインワン展開

✓ スタンドアロンのオールインワン構成に適したシンプルなアプローチ
✓セキュリティレベルは低め

✓外部から安全に隔離されたプライベートネットワーク環境での使用を想定

2.9.5.1 説明

この導入シナリオでは、 PcVue Webバックエンドステーションとwebサーバーコンポーネントは分離されておらず、同じコンピュータ上でホストされ、実行されます。

WebVueやTouchVueを含む Web およびモバイル クライアントは、Web サーバーと同じネットワークに接続されます。

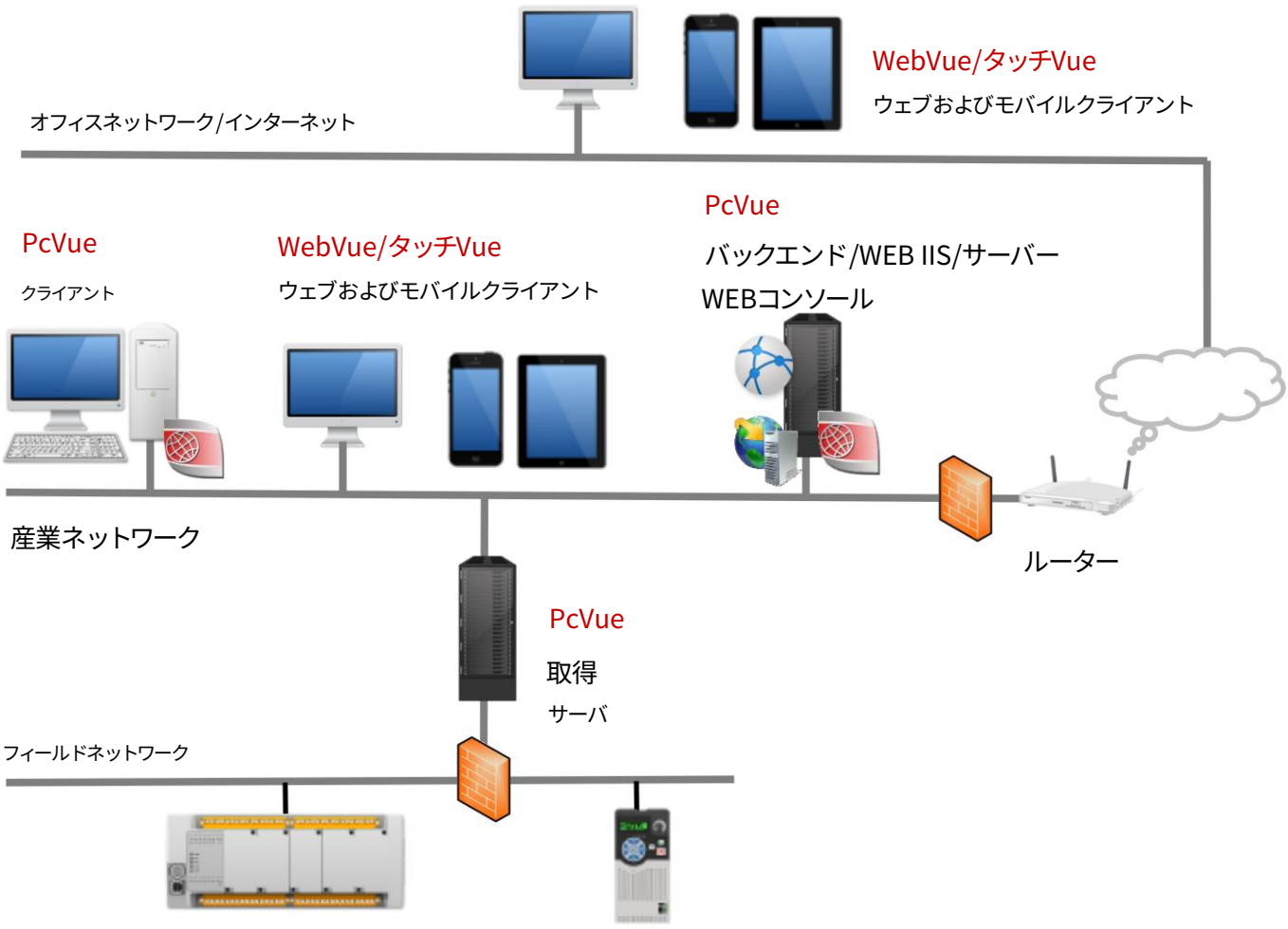


図22 – アーキテクチャ #1 – オールインワン展開

注記：

- IPアドレス範囲およびアドレスは、RFC 6890に記載されている一般的な使用パターンに基づいた説明です。その他のサブネット範囲やアドレスセットを使用することも可能です。

- PcVue SCADA システムのアーキテクチャは単なる説明のためのものであり、実際の設定とは異なる場合があります。
- 産業ネットワークをオートメーション ネットワークから分離することは推奨されていますが、これは単なる説明です。

2.9.5.2 いつ使用するのか?

このアーキテクチャは、Web およびモバイル クライアントがPcVue Web バックエンド ステーションと同じサブネット上にある場合の展開シナリオを対象としています。

この導入シナリオは、ネットワーク（サブネット）がプライベートであり、外部からのアクセスから完全に分離されている場合に有効です。特に、オペレータが使用するコンピュータやデバイスは、産業用ネットワークへの入り口として利用されるリスクを回避するため、外部へのアクセスを禁止する必要があります。

2.9.5.3 使用してはいけない場合

ネットワークが外部ネットワークからの受信要求に対して開かれている場合、または不明なデバイスからの保護されていないアクセスに対して開かれている場合は、この展開を使用しないでください。

特に、インターネット上の Web およびモバイル クライアント システムからのアクセスが必要であり、ネットワーク セキュリティのさらなる手段 (VPN トンネリングなど) が利用できない場合は、この展開戦略を使用しないでください。

2.9.5.4 要件

1. このアーキテクチャの導入には、最低限のネットワークレベルが必要です。
   専門知識など

2. Web およびモバイル クライアント、Web サーバー、PcVue Web バックエンド ステーションを含むすべてのコンピュータ ーとモバイル デバイスが同じサブネット (通常は産業用ネットワーク) 上にある必要があります。

3. このネットワーク上のクライアントは、同一の（定義上プライベートな）ネットワーク上にあるため、Webサーバーマシンを完全に信頼していることが前提となります。

4. このアーキテクチャは、最小限の要件で動作します。
Web サーバー証明書の信頼性。

Web サーバーとの信頼を確立するために、証明機関からの証明書は必須ではありません。

2.9.5.5 利点

1. PcVue Web バックエンドと Web サーバーの両方をホストするには、1 台のコンピュータが必要です。

2. このコンピュータには、複数のネットワーク インターフェイス カードは必要ありません。

3. Web サーバー コンピュータの IP アドレスを使用して Web およびモバイル クライアントに接続すると、すぐに使用できます。

Web サーバー コンピューターの IP アドレスを使用して Web & Mobile クライアントへ接続する場合は、追加設定なしでそのまま動作します。
Windows プラットフォームでは、名前解決のために DNS は必須ではありません。
Windows ベースの Web クライアントからは、Web サーバー コンピューターをホスト名で指定してアクセスすることが可能です。
PcVue Web Server コンピューターで提供するユーザー数が限られている場合は、Windows 10 などの Windows デスクトップ OS 上でも動作させることができます。
ただし、いかなる場合においても、サーバー OS の使用を強く推奨します。
Windows 以外のクライアント デバイス（Android、iOS、Linux）を使用する場合、名前解決のために DNS サーバーの存在が必須となります。
これは、PcVue Web バックエンド ステーションに Windows Server OS を使用し、DNS サーバーの役割（DNS Server ロール）を有効化することで実現できます。

4. 自己署名証明書（self-signed certificate）を使用する場合、特別な設定を行わなくてもそのまま利用できます。
ただし、Webクライアントのユーザーエージェントでセキュリティ例外を追加するか、モバイルクライアントアプリケーションで 「Ignore Certificate Errors（証明書エラーを無視）」オプションを有効にする必要があります。

ネットワーク上からアクセス可能な Active Directory サーバー が存在する場合は、Active Directory サーバーからドメイン証明書を発行することができます。
この証明書は、ドメインポリシーまたは企業の MDM システムを通じて、ドメインに属するすべてのクライアントから信頼されるように設定することが可能です。

1. Windowsデスクトップオペレーティングシステムでwebサーバーをホストする場合は、制限事項があることをご承知おきください。特に、IISが処理できるクライアント接続の最大数には制限があります。

2. Microsoft® Edgeでは、ホスト名がFQDNでない場合、Cookieの保存が許可されません。これにより、Webコンポーネントで問題が発生します。URLを次のように変更することで、この問題を回避できます。

https://<ホスト名>.local

3. 特にWebVueクライアントでは、パフォーマンスが制限される可能性があります。

無効な (部分的に信頼されている、または信頼されていない) 証明書を使用している場合、このような状況ではファイルがWeb ブラウザによってキャッシュされないため、読み込みが遅くなります。

2.9.5.7 Webデプロイメントコンソール

このアーキテクチャは、すべての設定をデフォルト値のままにして、WDC の「クイック セットアップ」ウィザードを使用して簡単に展開できます。
したがって、WDC は PcVue Web バックエンドおよび Web サーバーと同じコンピュータにインストールする必要があります。

2.9.6 アーキテクチャ #2: ネットワーク分離とDMZ

✓大規模SCADA/HMIシステム
✓高いセキュリティレベル
✓ウェブ/モバイルクライアントが産業ネットワークの外部にある場合を対象としています。

2.9.6.1 説明

この導入シナリオでは、PcVue Webバックエンドステーションと Webおよびモバイルクライアントは、異なる物理または論理ネットワーク上、異なるセキュリティ境界内に存在するため、DMZによる分離が必要です。内部ネットワーク（DMZルータのLAN側）はプライベートなセキュアネットワークです。外部ネットワーク（DMZルータのWAN側）は信頼性の低いネットワークで、通常は企業のオフィスネットワークまたはインターネットです。
Webサーバーコンポーネントは DMZ内のコンピュータでホストされ、PcVueバックエンドはセキュアネットワークでホストされます。
このアーキテクチャは、ITネットワークへの最適な統合を提供し、ITガイドラインとプラクティスへの最大限のコンプライアンスを実現します。

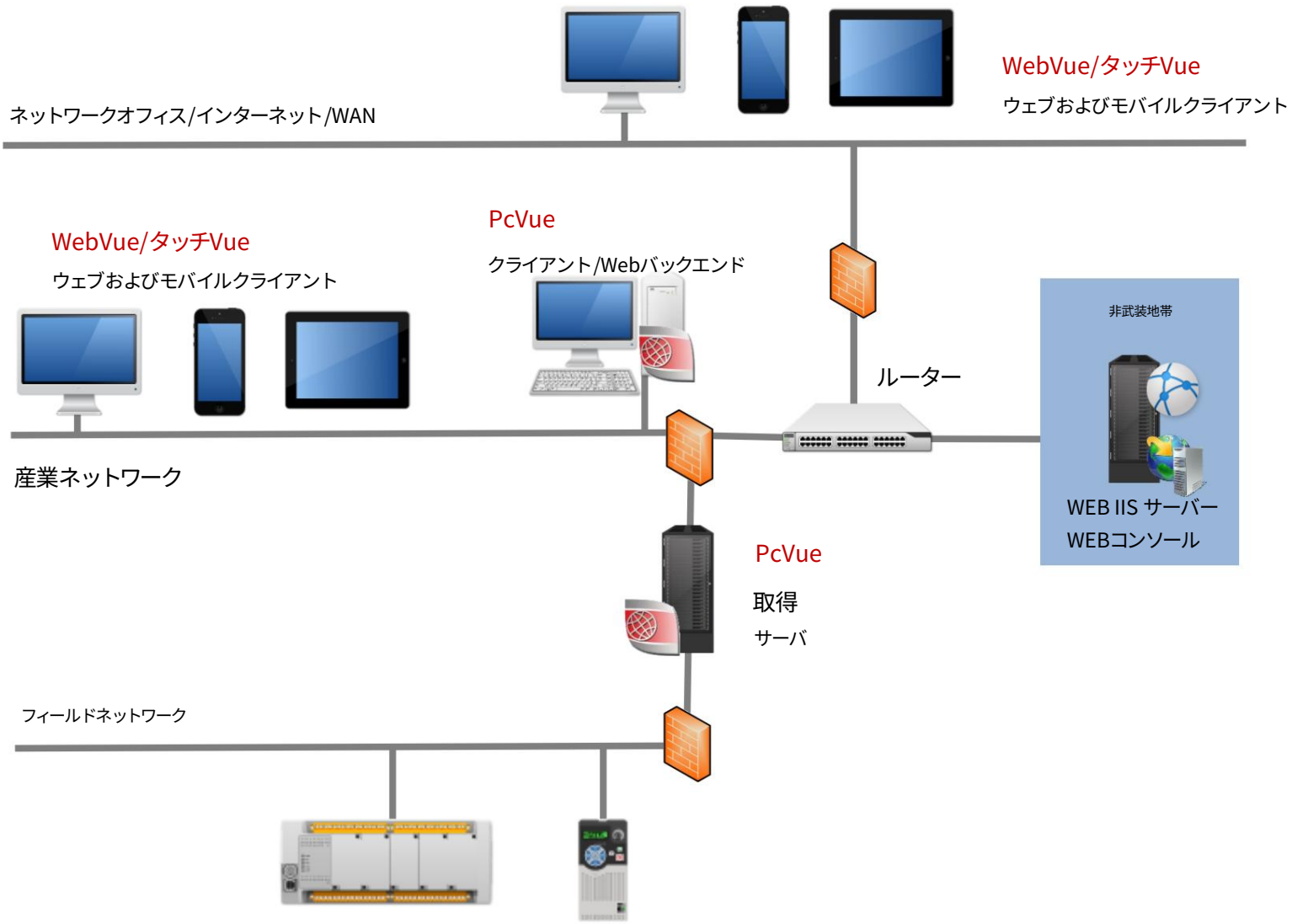


図23 – アーキテクチャ #2 – ネットワーク分離とDMZ

注記：

- IP 範囲とアドレスは、RFC 6890 で説明されている一般的な使用パターンに従った単なる説明です。他のサブネット範囲またはアドレス セットも使用できます。

- PcVue SCADA システムのアーキテクチャは単なる説明のためのものであり、実際の設定とは異なる場合があります。
- 産業ネットワークをオートメーション ネットワークから分離することは推奨されていますが、これは単なる例示です。

2.9.6.2 いつ使用するのか?

Web およびモバイル クライアントが安全な産業ネットワーク上にない場合は、このアーキテクチャの使用をお勧めします。

2.9.6.3 要件

1. このアーキテクチャを導入するために必要なネットワークおよび IT の専門知識は中級から上級です。

2. プライベートネットワークを、保護レベルが低いネットワークから分離するための適切なネットワークインフラストラクチャが必要です。これには、ルーター（および適切なルート設定）と、少なくとも1つのファイアウォールが含まれます。

   単一のファイアウォール設定やデュアル ファイアウォール設定など、一般的な DMZ アーキテクチャがサポートされています。

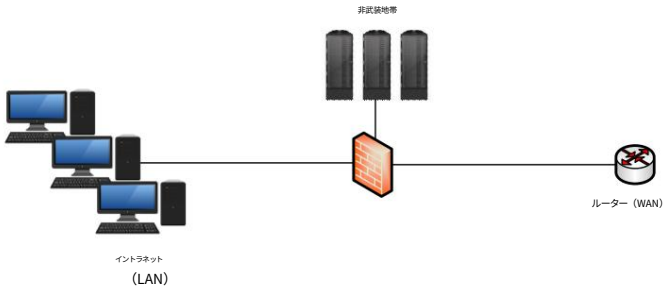


図24 - DMZ – 単一のファイアウォール設定

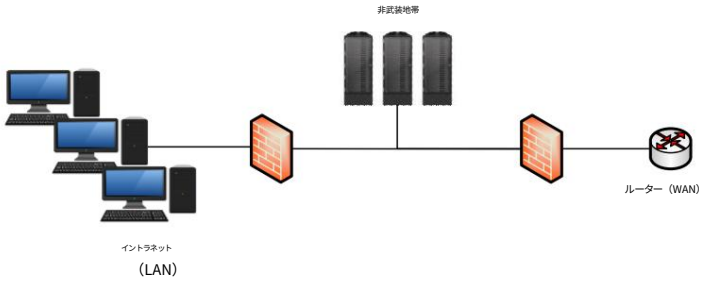


図25 - DMZ – デュアルファイアウォール設定

3. エンドユーザーのIT部門のサポートが必要となる可能性が高く、ネットワーク分離、名前解決および証明書の適切な設定を行う必要があります。

   これには以下の適切な設定が含ます
   ：- DNS

- ルーティング
- ネットワークアドレス変換（またはポート転送）
- 証明書

証明書を発行し、グローバル ポリシーの一部として信頼関係を確保するための企業 PKI として、Active Directory インフラストラクチャが必要になる可能性があります。

4. 信頼度の低いネットワーク上に配置されたWebサーバーコンピューターの正当性を検証し、Man-in-the-Middle（中間者）攻撃を防止するためには、完全に信頼された証明書の使用が必須です。

この証明書は、IT部門（社内ネットワークのActive Directoryサーバー）によって発行することができます。すべてのWebクライアントおよびモバイルクライアントが企業ネットワーク基盤と信頼関係にある場合は、この方法で十分です。

また、この証明書は信頼された認証局（CA）を介してIT部門が発行することも可能です。Webサーバーに企業ネットワーク基盤と信頼関係のない外部のWebクライアントおよびモバイルクライアント（一般的には、インターネット経由でアクセスする端末）からアクセスする必要がある場合には、この方法が必要となります。

さらに、インターネット接続が存在し、かつユーザー組織のポリシーで Let's Encrypt サービスの利用が許可されている場合、WDCのLet's Encrypt®ウィザードを使用して証明書を発行することも可能です。

5. 信頼度の低いネットワーク上において、Webサーバーの名前解決を行うことができるDNSサーバーが必要です。

6. Webサーバーコンピューターには Windows Server オペレーティングシステムが必要であり、PcVue Web バックエンドステーションにおいても、同様に Windows Server オペレーティングシステムを使用することが望まれます。

7. PcVue Web バックエンドステーションは、少なくともIPアドレスによって Web サーバーコンピューターからアクセス可能である必要があります。DMZ 内において名前解決の手段が用意されている場合は、ホスト名によるアクセスも可能です。

・Web サーバーコンピューターの hosts ファイルに専用のエントリを追加する方法

・DMZ からアクセス可能な産業用ネットワーク内の DNS サーバーを使用する方法
これらの手段がすでに利用できない場合、PcVue Web バックエンドステーションの Windows Server オペレーティングシステム上で DNS サーバーの役割（DNS Server ロール）を有効化することも、解決策の一つとなります。

注記：DMZ 内のコンピューターからプライベートネットワークへのアクセスを許可することは、DMZ の一般的な設計パターンおよび運用上のベストプラクティスに反します。ただし、技術的な理由により、この方向への TCP ポート 8090 の開放が必要となります。

2.9.6.4 利点

1. 本アーキテクチャでは、WebサーバーのWebおよびモバイル向けサービス／アプリケーションを完全修飾ドメイン名（FQDN）で公開することにより、インターネットやイントラネットなどの信頼性が低いネットワークからでも、容易にアクセスすることが可能です。

2. ITネットワーク分離のベストプラクティスに準拠し、ネットワーク境界におけるトラフィックの制御および監視を含め、外部ネットワークから産業用ネットワークへの望ましくない着信接続要求が発生しないようにすることで、ネットワークトラフィックを最大限に制御することが可能です。

2.9.6.5 Webデプロイメントコンソール

このアーキテクチャは、WDC のセットアップウィザードのいずれかを使用して導入できます。

「クイックセット アップ」ウィザードのデフォルト設定は、すべての状況に適しているわけではありません。

WDC を Web サーバー コンピューターにインストールする必要があります。

2.9.7 アーキテクチャ #3: リモートアクセスのための簡略化されたNATシナリオ

✓小規模システムへのリモートアクセス

✓管理されたITインフラストラクチャが利用できない環境での使用を想定しています。

2.9.7.1 説明

本デプロイメントシナリオは、単一のプライベートLAN（産業用ネットワーク）に対応する構成であり、Webサーバー、PcVue Webバックエンドステーション、および大半のWeb & Mobileクライアントが同一ネットワーク上に配置されます。
リモート接続のために、専用のインターネット回線が使用されます。

この構成では、Web & MobileクライアントはNAT境界の両側（ローカルおよびリモートのWebクライアント）に分散して配置されます。

技術的には本アーキテクチャをそのまま導入することは可能ですが、追加のセキュリティ対策を講じないままの導入は推奨されません。

想定される対策としては、VPNの利用やクライアントIPアドレスの固定（アドレスロック）などがあります。この場合、本構成は論理的にアーキテクチャ#1と同等となります。
また、ネットワーク境界の専用DMZポートを使用して専用セグメントを構築することで、アーキテクチャ#2の簡易版として構成することも可能です。

いずれの場合においても、アーキテクチャ#2で説明されているように、PcVue Webバックエンドステーションと Webサーバーを分離することを推奨します。これはそれ自体が追加のセキュリティ対策となるからです。

なお、インターネット接続が第三者（ISP）によって提供され、セットトップボックスなどISP管理の機器を使用する必要がある場合は、ネットワーク境界を制御するための専用アプライアンスを設置することを強く推奨します。
特に、「Exposed Host（DMZホスト公開）」のような代替的な構成は避けることを推奨します。

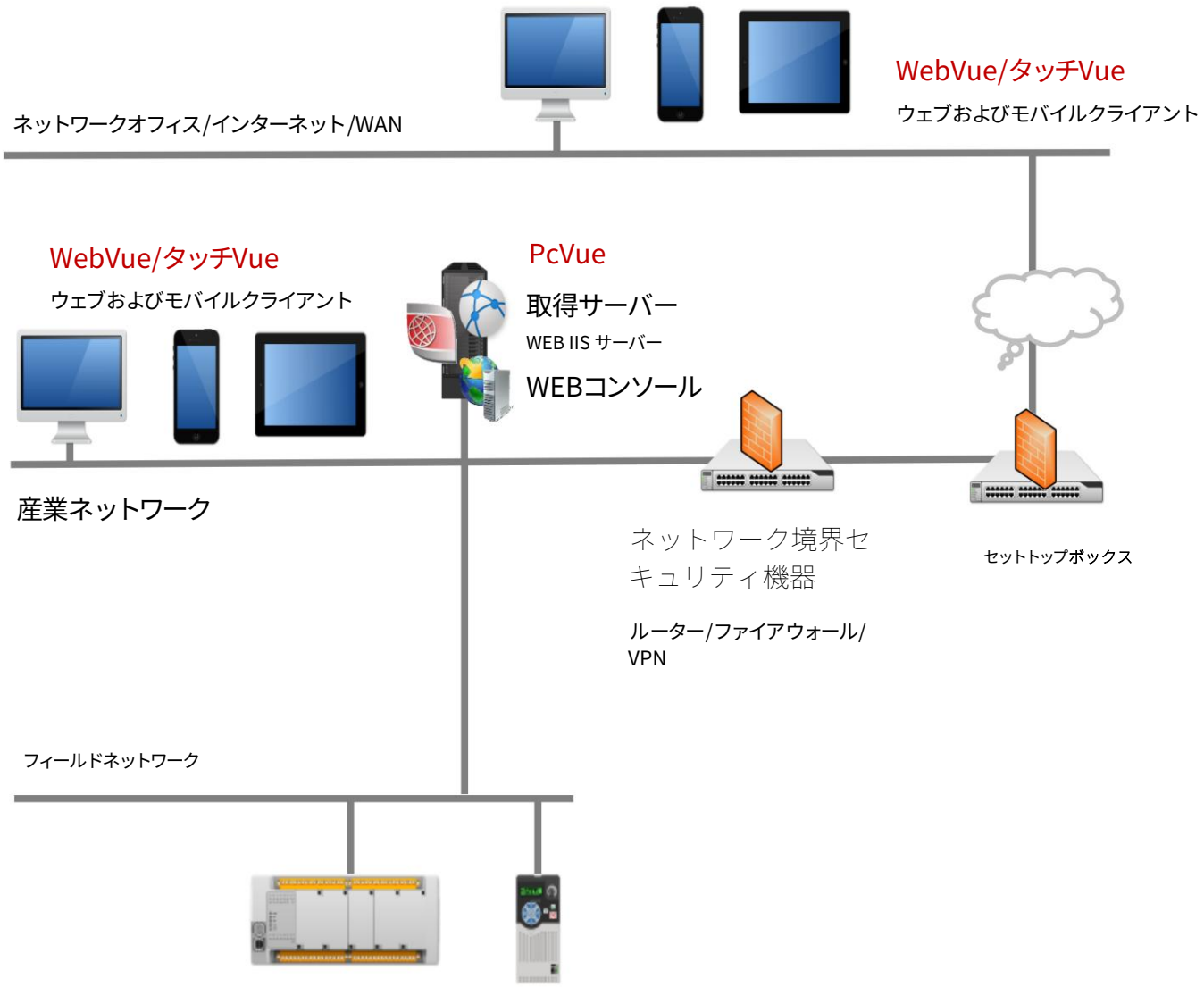


図26 - アーキテクチャ#3 – リモートアクセスのための簡略化されたNATシナリオ

注記：

- IP 範囲とアドレスは、RFC 6890 で説明されている一般的な使用パターンに従った単なる説明です。他のサブネット範囲またはアドレス セットも使用できます。

- PcVue SCADA システムのアーキテクチャは単なる説明のためのものであり、実際の設定とは異なる場合があります。
- ルータ デバイスが WAN に公開される IP アドレスは、ISP によって異なる場合があります。

2.9.7.2 いつ使用するのか?

本デプロイメントシナリオは、ITインフラストラクチャが存在しない環境において、簡易的なリモートアクセスを実現するために必要となる場合があります。

本アーキテクチャを使用して旧バージョンのWebVueを運用している既存システムについては、アーキテクチャ#2への移行、または追加のセキュリティ対策の適用を推奨します。

2.9.7.3 使用してはいけない場合

不十分なネットワーク分離と弱いネットワーク トラフィック制御に関連するリスクを理解しないまま、このアーキテクチャをそのまま実稼働環境や実際のシステムで使用しないでください。

2.9.7.4 要件

1. 本アーキテクチャの導入に必要なネットワークおよびITの専門知識レベルは、初級から中級程度です。

2. プライベートネットワークと保護レベルの低いネットワーク間の接続を確立するためのネットワークインフラが必要です。また、ルーターの両側に配置されたWeb／モバイルクライアントを接続するためのネットワークインフラも必要となります。

3. ネットワーク境界において、ネットワークアドレス変換（NAT）（特にポートフォワーディング）を構成する必要があります。

4. 保護レベルの低いネットワーク上でWebサーバーコンピューターの正当性を検証し、中間者攻撃（Man-in-the-Middle攻撃）を防止するために、信頼された証明書の使用が必須です。

   - 当該証明書は、信頼された認証局（CA）を通じてIT部門により発行される場合があります（企業ネットワークインフラと信頼関係のない外部のWeb／モバイルクライアント（例：インターネット経由）からWebサーバーへアクセスする場合に必要）。

   - インターネット接続が存在し、かつユーザー組織のポリシーでLet's Encrypt®サービスの利用が許可されている場合、WDCのLet's Encrypt®ウィザードを使用して証明書を発行することも可能です。

5. Webサーバーコンピューターは、両ネットワークセグメントからWeb／モバイルクライアントによるアクセスが可能である必要があります。

これは、Webサーバーが両ネットワークセグメント上において同一の完全修飾ドメイン名（FQDN）で認識されている場合に実現可能です。
これが満たされない場合、Web＆Mobileクライアントがプライベートネットワーク外へ通信を出すことなく、FQDNを使用してWebサーバーコンピューターへ直接接続できる必要があります。
このような場合には、NATループバック（ヘアピンNAT）の使用が推奨されます。

これらのいずれの方法も利用できない場合は、WDCを使用して2つの異なるサイトを作成し、それぞれを同一のPcVue Webバックエンドステーションへ接続することを推奨します。

2.9.7.5 利点

1. このアーキテクチャにより、Webおよびモバイルクライアントの便利なアクセスが可能になります。産業ネットワーク上およびインターネットから取得します。

2. このアーキテクチャは、古いWebVueシステムを新しい攻勢へ移行するプロセスにおける第一歩です。

2.9.7.6 制限事項

この展開シナリオでは、ネットワーク境界を制御するために特定のアプライアンスが追加されていない場合、次の理由によりネットワーク セキュリティが制限されます。

- ネットワーク境界およびリモート接続の制御を、**ISPが提供するセットトップボックス（ルーター）**に依存しているため。
- その結果、産業制御システム（ICS）の一部であるコンピュータが、インターネットに直接公開された状態になる可能性があるため。

最悪のシナリオでは、複数のレベルの潜在的なセキュリティの脆弱性を攻撃者が悪用して、産業用制御システムにアクセスする可能性があります。

2.9.7.7 Web デプロイメント コンソール

このアーキテクチャは、いずれかの WDC セットアップ ウィザードを使用して展開できます。
WDC を Web サーバー コンピューターにインストールする必要があります。

2.10 完全なアーキテクチャ

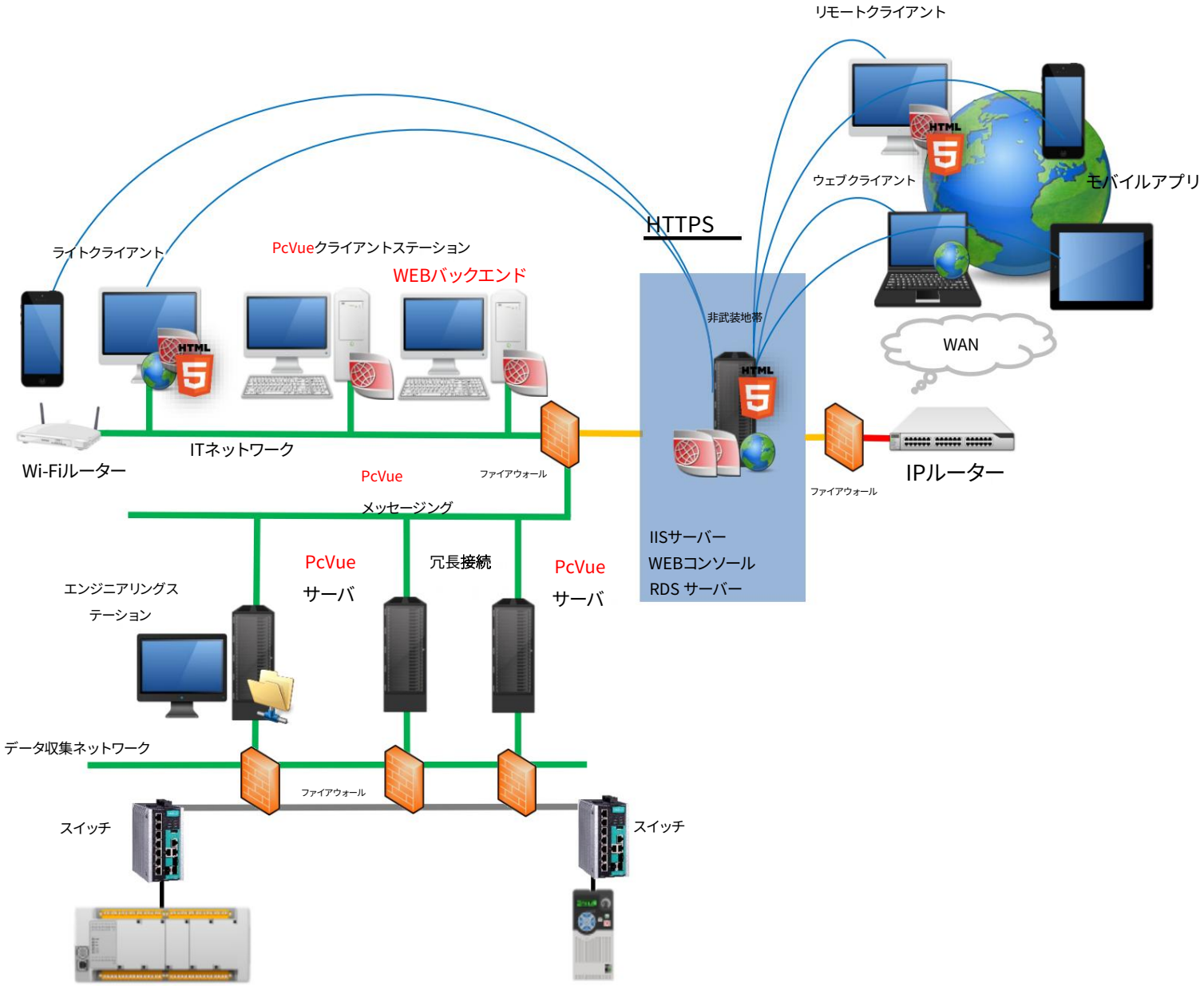


図27 - 完全なアーキテクチャ

このアーキテクチャの例は、以下の要素に基づいて構成されています

- データ収集は、産業ネットワーク上の冗長構成の収集サーバーによって実行されます。
- 開発ステーションは、プロジェクトの集中管理のために使用されます。
- 運用は、ファイアウォールによって隔離されたコンピュータネットワーク上のクライアント端末によって行われます。

- 1つのクライアントステーションがWebバックエンドとして機能します
- ファイアウォールで分離された非武装地帯 (DMZ1) 内の Windows サーバーにインストールされたステーションでは、Web サーバー、モバイル サーバー、および Windows RDS2サーバーがホストされています。
- クライアントアプリはWindowsリモートを使用してRDSインスタンス経由でリモート実行できます。

- HTML5対応ブラウザがあれば、PC、タブレット、スマホのどれでもクライアント画面表示可能です。

- Web クライアントでは標準の Web ブラウザからの操作が可能です。
- モバイル サーバーに接続されたモバイルプリケーションは、スマートフォンやタブレットからのアラームの通知と確認、および制御に使用されます。
- Web サーバーと端末間のやり取りには、セキュアソケット HTTPS3 が使用されます。
- システム全体へのユーザーアクセスは、シングルサインオン（SSO4)のためにWindows Active Directoryによって管理されます。

PcVueマルチレベル アーキテクチャのコンポーネントを保護するには、いくつかの予防措置を講じる必要があります。

したがって、次のことを行う必要があります。

- 異なるネットワーク（例：コンピュータネットワークと産業用ネットワーク）を、同一レベルのセキュリティを必要とする独立した論理領域（VLAN5）を作成することでセグメント化する

- ファイアウォールを使用してデータをフィルタリングします。

DMZとルーターの使用により、ネットワークを外部から分離し、不必要な侵入を防ぎます。

DMZとルーターの使用により、ネットワークを外部から隔離し、望ましくない侵入を防ぐことも可能になります。2つのネットワークコンポーネント間のトラフィックを保護するには、VPN6トンネリングソリューションの構築も必要となる場合があります。通常、VPNはPcVue収集ステーションとTCP/IP経由で通信するPLCの間に構築できます。

---

1 非武装地帯
2 リモートデスクトップサービス
3 HTTPS: セ キ ュ ア ハイパーテキスト転送プロトコル
4 シングルサインオン
5 VLAN :仮想LAN
6 VPN :仮想プライベートネットワーク

ステーション間 TCP/IP メッセージングを使用して通信する複数のリモート監視サイト間

PcVue Solutions は、MOXA と提携して、上記の問題に対処するための完全なハードウェア保護ソリューションを提供します。

- 産業用途に対応したセキュアなファイアウォール／VPNのフルラインアップ
- 異なるネットワークゾーン間におけるトラフィックの制限および制御
- 通信トラフィック制限ルールの作成

2.11 仮想化

✓ 物理的なステーションの数を減らす
✓ 管理の手間とコストを削減
✓ 低価格のシンクライアント
✓ シンクライアントにインストール不要
✓ IT要件に準拠

コンピューティングにおける仮想化（Virtualization）とは、仮想コンピュータのハードウェアプラットフォーム、オペレーティングシステム
（OS）、ストレージデバイス、コンピュータネットワークリソースなどを含む、実体ではなく仮想的なバージョンを作成する技術を指します。

ハードウェア仮想化（プラットフォーム仮想化）とは、OSを備えた実際のコンピュータのように動作する仮想マシンを作成することを意味します。これらの仮想マシン上で実行されるソフトウェアは、基盤となる物理ハードウェアリソースから分離されています。

ハードウェア仮想化において、ホストマシンとは仮想化が実行される物理マシンを指し、ゲストマシンとは仮想マシンを指します。「ホスト」と「ゲスト」という用語は、物理マシン上で動作するソフトウェアと仮想マシン上で動作するソフトウェアを区別するために使用されます。

産業用アプリケーションの仮想化は、IT部門、エンジニアリング部門、運用部門など、多くの関係部門にメリットをもたらします。

7 出典 :Wikipedia

2.11.1 アプリケーション仮想化

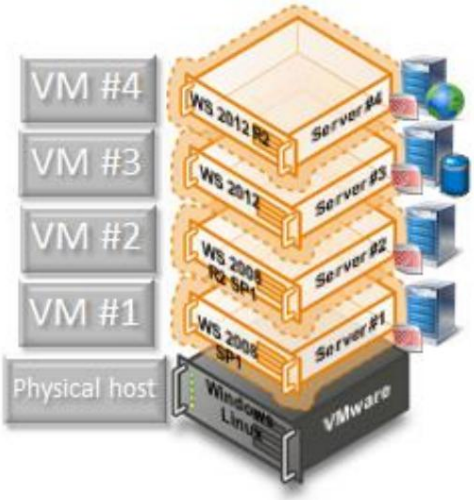
✓ホストコンピュータは、隔離された環境でPcVueまたはFrontVueの異なるバージョンを実行できます。

✓単発的な作業用の作業環境を簡単に構築できます。

✓古いオペレーティングシステムをセットアップすることが可能です

✓Windows 7、Windows 8、Windows 8.1、Windows Server 2008 SP2／2008 R2 SP1、2012／2012 R2、および VMware 上で動作します。

2.11.2 リソースの仮想化

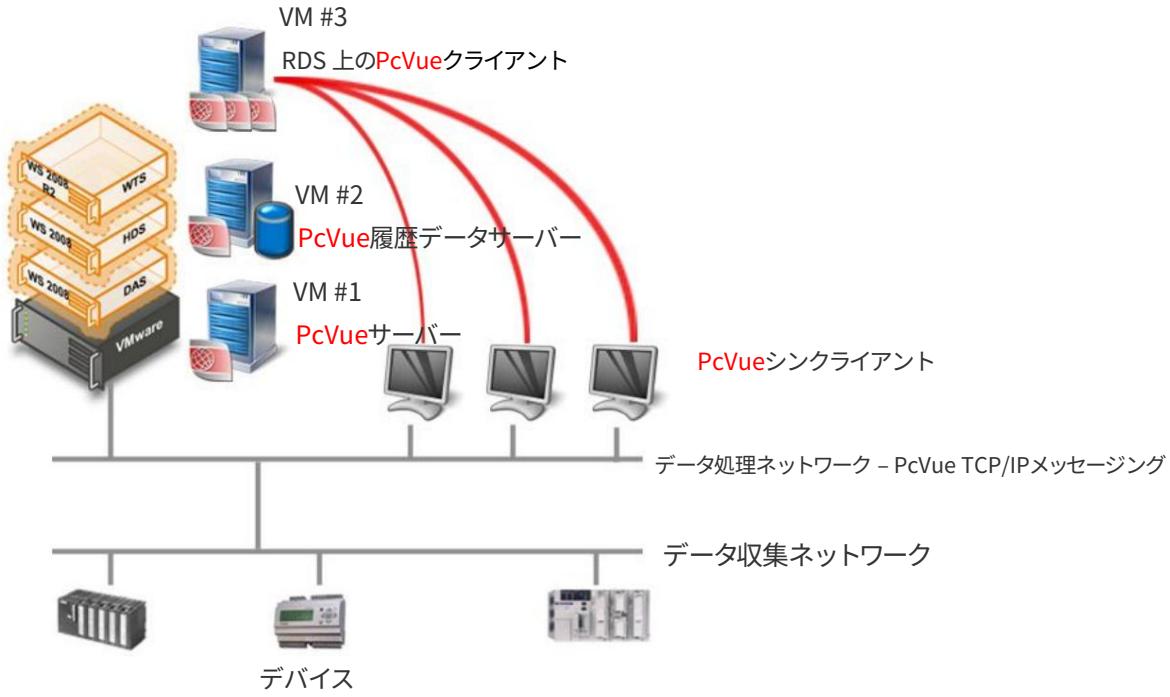


✓仮想化環境により、単一の物理マシン上で異なるオペレーティングシステムを用いた複数の PcVue サーバーを実行可能

✓PcVueライセンスにはさまざまな種類があります

✓リソース最適化ルールに従って仮想マシンを物理ホストに動的に割り当て可能

2.11.3 実装例



ここでは、SCADAアプリケーションはIT管理ステーション上で実行されます。VMwareまたは同等のソフトウェアを搭載した単一の物理マシンが、分離された仮想マシン内ですべてのステーションをホストします。これらの仮想マシンの1つはRDSを実行し、複数のRDSクライアントステーションがサーバーに接続できるようにします。このドキュメントで説明するアーキテクチャのほとんどは、仮想環境に導入できます。

3. 用語集

名前	略語	説明
Microsoft® インターネット情報サービス	IIS	インターネット インフォメーション サービス (IIS) は、Microsoft® が開発し、Windows オペレーティング システムに同梱されている Web サーバーです。IIS は、Microsoft® Windows オペレーティング システムに組み込まれている Web サーバーです。
PcVue Webバックエンドステーション		産業用ネットワーク上の PcVue ステーションは、PcVue マルチステーション システムと実際の Web サーバー (IIS) 間のゲートウェイとして使用されます。 Web バックエンドは、PcVue のメイン プロセスである Sv32.exe を実行します。
Webサーバーマシン Webサーバーコンピュータ		PcVue Web Server Components をホストする IIS Web サーバーを実行しているコンピュータを指します。なお、この Web サーバー上では Sv32.exe（PcVue のメインプロセス）は実行されません。
PcVue WEBサーバーコンポーネント		PcVue Web およびモバイル クライアントに接続するために Web サーバー マシンにインストールされるサービスとアプリのセット。
Webおよびモバイルクライアントシステム		WebブラウザーでWebVueクライアントを実行しているコンピューターとデバイス、またはモバイルデバイス上のTouchVueなどのネイティブモバイルアプリを実行しているコンピューターとデバイス。
ウェブデプロイメントコンソール	WDC	Web サーバー マシンにインストールされるデスクトップ アプリケーション。システム管理者は、これを使用して IIS および PcVue Web サーバー コンポーネントを構成、展開、監視できます。
産業ネットワーク		PcVue SCADA ネットワークを含むネットワークセグメント。 ANSI/ISA-95 情報モデルではレベル 2 産業ネットワークと呼ばれます (SCADA レベルとも呼ばれます)。
非武装地帯	DMZ	DMZ（非武装地帯：Demilitarized Zone）—「ペリメーターネットワーク」とも呼ばれる—とは、組織の外部向けサービスを収容し、通常はインターネットのような信頼されていないネットワークに公開するための、物理的または論理的に分離されたネットワークを指します。 DMZ の目的は、組織のローカルエリアネットワーク（LAN）に対して追加のセキュリティ層を設けることにあります
完全修飾ドメイン名	FQDN	ドメインネームシステム（DNS）のツリー階層内における正確な位置を指定するドメイン名を指します。少なくともセカンドレベルドメインおよびトップレベルドメインを含む、すべてのドメイン階層レベルを指定します。
ドメインネームシステム DNS	DNS	DNS（Domain Name System）は、インターネットまたはプライベートネットワークに接続されたコンピュータ、サービス、その他のリソースの名称を管理する、階層型かつ分散型のネーミングシステムです。
Windows インターネットネームサービス	WINS	WINSは、NetBIOSコンピュータ名のための名前サーバーおよび名前解決サービスである NetBIOS Name Service（NBNS）を、Microsoft が実装したものです。

名前	略語	説明
サブネットワーク	サブネット	サブネット（subnetwork／subnet）とは、IPネットワークを論理的に分割したものです。同一のサブネットに属するコンピュータは、IPアドレスの中で最上位ビット群（ネットワーク部）が共通しています。送信元アドレスと宛先アドレスのルーティングプレフィックス（ネットワーク部）が異なる場合、サブネット間の通信はルータを介して行われます。ルータは、サブネット間の論理的または物理的な境界として機能します。
仮想プライベート ネットワーク	VPN	仮想プライベートネットワーク（VPN）は、公衆ネットワーク上にプライベートネットワークを拡張し、ユーザーが共有ネットワークまたは公衆ネットワークを介して、あたかも自身のコンピューティングデバイスがプライベートネットワークに直接接続されているかのようにデータの送受信を行うことを可能にします。
ファイアウォール		事前に定義されたセキュリティ ルールに基づいて、受信および送信のネットワーク トラフィックを監視および制御するネットワーク セキュリティシステムです。
ネットワークアドレス 翻訳	NAT	NATは、トラフィックルーティングデバイスを通過するパケットのIPヘッダー内のネットワークアドレス情報を変更することで、あるIPアドレス空間を別のIPアドレス空間に再マッピングする手法です。NATゲートウェイのインターネットルーティング可能なIPアドレス1つを、プライベートネットワーク全体で使用できます。
ポート転送	PAT	ポートフォワーディング（port forwarding）またはポートマッピング（port mapping）とは、ネットワークアドレス変換（NAT）の応用の一つであり、ルータやファイアウォールなどのネットワークゲートウェイを通過する際に、通信要求のアドレスとポート番号の組み合わせを別のものへ転送（書き換え）する技術です。この技術は主に、保護されたネットワーク（内部ネットワーク）上のホストで稼働しているサービスを、ゲートウェイの反対側（外部ネットワーク）にあるホストから利用可能にするために使用されます。そのために、通信の宛先IPアドレスおよびポート番号を内部ホストへ再マッピングします。
インターネットサービス プロバイダー	ISP	インターネットサービスプロバイダ（ISP）とは、インターネットへのアクセス、利用またはインターネットへの接続参加に関する各種サービスを提供する組織のことです。
プライベートキー インフラストラクチャー	PKI	Public Key Infrastructure（PKI） とは、デジタル証明書の作成・管理・配布・使用・保管・失効を行い、公開鍵暗号方式を安全に運用するために必要な「役割・ポリシー・手順」の仕組み一式のことです。
証明機関 CA	CA	証明機関（CA）は、デジタル証明書を発行する機関です。 CAは、信頼できる第三者機関である場合もあれば、企業のPKIの一部である場合もあります。
モバイルデバイス 管理	MDM	モバイルデバイス管理（MDM）とは、スマートフォン、タブレット、ノートパソコン、デスクトップパソコンなどのモバイルデバイスの管理を指す業界用語です。MDMは主に、企業データの分離、メールのセキュリティ保護、デバイス上の企業文書のセキュリティ保護、企業ポリシーの適用、モバイルデバイスの統合と管理を扱います。

名前	略語	説明
ハイパーテキスト転送プロトコル セキュアハイパーテキスト転送プロトコル	HTTP / HTTPS	ハイパーテキスト転送プロトコル（HTTP）は、分散型・協調型のハイパーメディア情報システムのためのアプリケーションプロトコルです。HTTP は、World Wide Web におけるデータ通信の基盤となるプロトコルです。 HTTPS (HTTP Secure) は、安全な通信のためのハイパーテキスト転送プロトコル (HTTP) の拡張機能です。 このプロトコルは、HTTP over TLS または HTTP over SSL と呼ばれることもあります。
ヘアピン		ヘアピニング (「NAT ループバック」とも呼ばれます) は、マップされたエンドポイントを使用して、同じ NAT デバイスの背後にある 2 つのホスト間の通信を表します。 ヘアピニングとは、LAN 上のマシンが LAN/ルーターの外部 IP アドレスを介して LAN 上の別のマシンにアクセスできることです (ルーターでポート転送を設定し、要求を LAN 上の適切なマシンに送信します)。
WebSocket		WebSocket (RFC 6455) は、単一の TCP 接続を介して全二重通信チャネルを提供するコンピュータ通信プロトコルです。 WebSocket は、HTTP ポート 80 および 443 で動作し、HTTP プロキシおよび中継サーバーをサポートするように設計されています。 HTTP と同様に、WebSocket は wss バインディング (Web Socket Secure) を通じて暗号化をサポートします。
HTTP/2 - SPDYプロトコル		HTTP/2は、HTTPネットワークプロトコルの大幅な改訂版です。これは、以前の実験的なSPDYプロトコルから派生したものです。 このプロトコルの進化によってもたらされた主な改善点は、レイテンシの短縮、ヘッダー圧縮、TCP多重化、リクエストのパイプライン化の導入により、ウェブサイトの応答性が向上したことです。

一般的な定義の一部は、Wikipedia: The Free Encyclopedia. Wikimedia Foundation, Inc. から引用したものです。正確性や目的への適合性は保証されません。

もくじ

ARCインフォマティーク

本社とパリのオフィス 2 avenue de la Cristallerie
92310 セーヴル - フランス

電話 + 33 1 41 14 36 00 フ
ァックス + 33 1 46 23 86 02
ホットライン +33 1 41 14 36 25
pcvuejporder@pcvue.com
www.pcvuesolutions.com

ドイツ - ミュンヘン
PcVue Gmbh

イタリア - ミラノ
PcVue Srl

英国 – ロンドンコントロール
テクノロジーインターナショナル

アメリカ - ボストン
PcVue株式会社

チリ - サンティアゴ
PcVue チリ

シンガポール - シンガポール
PcVue Sea

マレーシア - クアラルンプール
PcVue Sdn Bhd

中国 - 上海
PcVue 中国

日本 - 名古屋
PcVueジャパン

アラブ首長国連邦 - ドバイ
PcVue DMCC

ARCインフォマティーク
資本金125万ユーロの有限会社

RCSナンテールB 320 695 356
エイプ 5829C
サイレン 320 695 356
VAT番号 FR 19320695356

PcVue アーキテクチャと展開