システムを効果的に保護するためのPcVueベストプラクティスガイド 2024

ホワイトペーパー

産業用および自動化システムの監視の確保

この文書は誰をターゲットにしていますか？

このドキュメントでは、産業設備および自動化設備の監視を安全に行うために検討すべき質問事項を提示し、さらに PcVue を使用する際に適用すべき推奨手法を説明します。

用語集

OT	運用技術
IT	情報技術
ICS	産業用制御システム
POC	実証実験
SOC	セキュリティオペレーションセンター
SIEM	セキュリティ情報およびイベント
CIO	管理最高情報責任者
CISO	最高情報セキュリティ責任者
RDS	リモートデスクトップサービス

1. サイバーセキュリティアプローチを定義する際に自問すべき重要な質問

1. 質問

なぜシステムを安全に保つ必要があるのでしょうか?

- システムに内在するリスクは何ですか?
- 法的義務はありますか?

システムのどの部分をセキュアにする必要がありますか?

- 何ができて、どこまでの技術範囲を対象にしますか？
- どのような要件が適用されますか?

専門知識が必要ですか？

- どのようなサポートがありますか？

必須の機能は何ですか?

- 既存のソフトウェアではどのようなことが可能ですか？
- 既存のプロジェクトにはどのような機能が必要ですか？

システムの安全性を保証するにはどうすればよいですか?

- システムの要素は安全ですか?
- 必要に応じて認証は可能ですか？

2. なぜシステムは安全であるべきなのか

2. なぜシステムは安全であるべきなのか

- 重要なシステムに潜む現実的なリスク
- 重要なシステムにおける実際のリスク
- 産業情報システムの特性

監視（スーパービジョン）ソリューションは、自動化されたプロセスの運用や、設備および人の安全に関わるシステムなど、プロジェクト環境および重要な運用条件下で導入されます。

IPベースの統合は、異種機器の統合や相互運用性（インターオペラビリティ）、および監視システムの展開を容易にします。

しかしその一方で、プロジェクトの方法論や使用する製品に「セキュリティ」要素が組み込まれていない場合、セキュリティリスクを生じさせます。

さらに、IoT機器、モビリティ、よりオープンで相互接続されたシステムを統合するアーキテクチャの進化により、新たな脅威が生まれており、サイバーセキュリティの重要性はますます高まっています。

センシティブシステムと現実のリスク

すべての産業設備や自動化システムは、サービス品質や生産性の制約があるため、あらゆる障害に敏感であり、それが実際の被害につながる可能性がある。

12の重要な産業を4つのカテゴリーに分類

- 異なる種類の設備が混在しているシステム

食べ物 水 管理 健康	民間活動 司法活動 軍事活動	エネルギー ファイナンス 交通機関	通信 電子 映像・音響 情報 産業

- 重要なリスク
  - 多様な攻撃
  - ヒューマンエラー
  - システム脆弱性

- 実際の影響
  - 人と物資の安全
  - 公衆衛生リスク
  - 環境リスク
  - 事故、侵入
  - 悪意ある行為
  - 国家の機能・行動能力への影響
  - サービス拒否
  - 経済リスク
  - 知的財産
  - データ漏えい

産業情報システムの特徴

産業システムの情報システムは、管理系の情報システムとは異なる特徴を持っており、
それらを理解することがセキュリティ確保の重要性を理解するために必要です。

システムの目標

物理的な施設の管理

プロセスを規制

データの取得と処理

機能面

ビジネス上の制約

リアルタイム制約

運用上の安全制約

高可用性

ステークホルダー文化

オートメーションの専門家

電気技術機器技師

プロセスエンジニアリングの専門家

異なる種類の構成要素

設備の寿命が長いため、複数世代の技術が同じ
施設上に重なって存在することになる。

環境物理

生産工場 :ほこり、温度、振動、電磁気、近くの有害
な製品、外部環境など

地理的な場所・位置

倉庫、工場、公共の道路、田舎（ポンプ場、変電所）

インシデント管理

多数のパラメータと環境の複雑さにより
インシデントの再現性が制限される

ライフサイクル

10年以上
（最長40年）

よくある誤解と事実

「私たちの産業ネットワークは分離されており、保護されています。」

産業情報システムはネットワークに接続されることが多く、時にはインターネットに直接接続されることもあります。USBキーやメンテナンスコンソール物理的に隔離されたシステムも含め、ウイルス拡散の主要な媒介物となります。産業ネットワークの絶縁は必須ですが、それだけでは十分ではなく、他の手段で補完する必要があります。

「私はプロトコルと独自のデータベースを使用しているので、保護されています。」

独自システムであっても、相互運用性（例えばOS）やコスト削減の理由から標準コンポーネントを含んでいる場合があります。また、独自システムは、セキュリティ分析の対象になっていない可能性があるため、脆弱性を抱えている可能性があります。

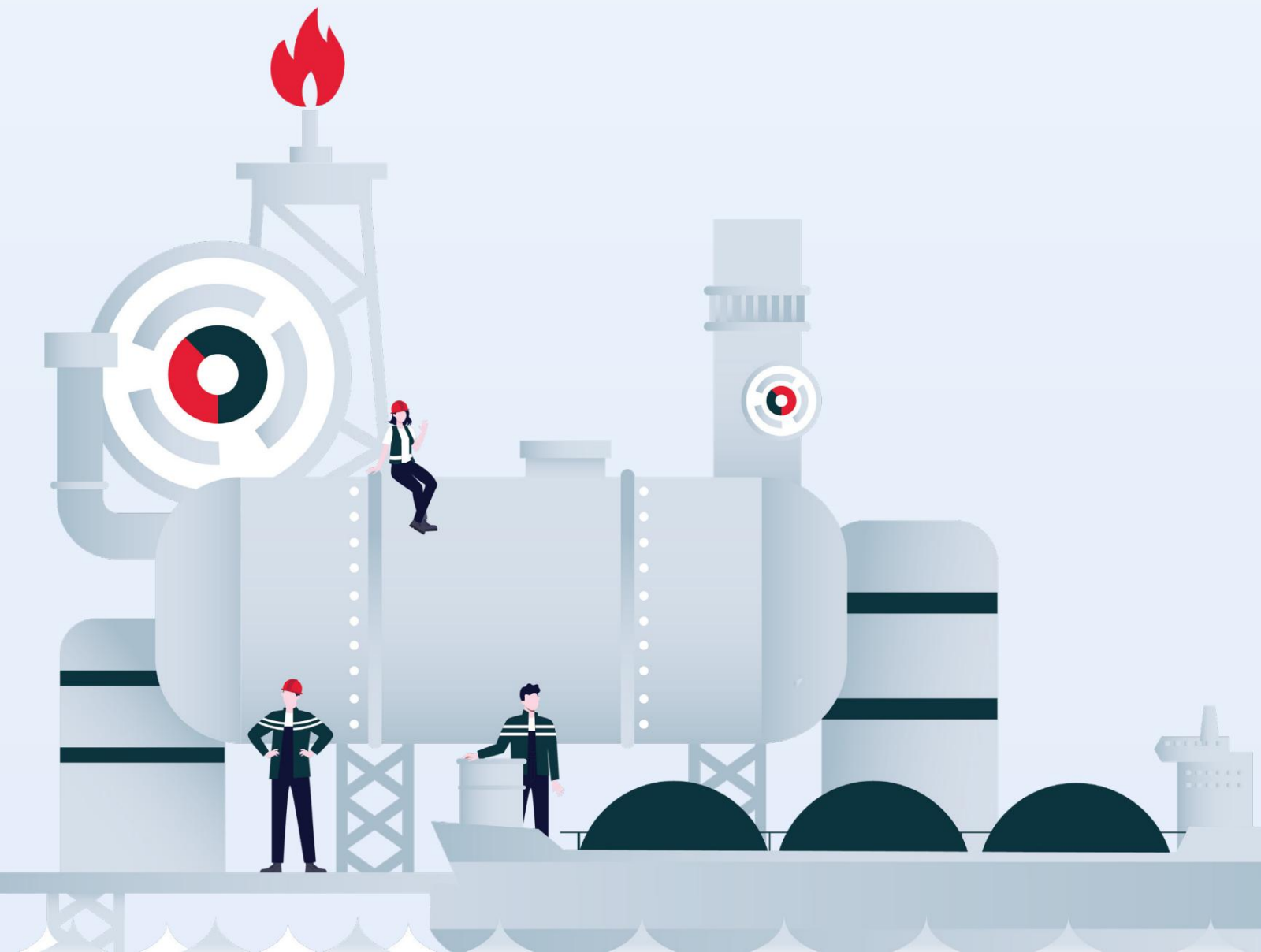
暗号化・認証・通信フィルタなどのセキュリティ機能を入れると、工場システムで必要な高速な応答や安定した運転ができなくなると言われている。

現在の機器性能では、暗号化などのセキュリティ機能を導入してもシステム性能の問題はほとんどありません。さらに、サイバーセキュリティは事前に計画して導入できるため、計画停止などを利用すれば生産やプロセス効率に影響を与えずに実装することが可能です。

サイバー攻撃は、窃盗や火災などの物理的な事件に比べ、常に影響が小さい。

攻撃により、物理的なサイバー攻撃よりも特定が困難で、より悪質な（産業妨害、生産の減速）設備の全体的機能不全が生じる可能性があり、復旧に非常に長い時間（数週間）を要する可能性があります。

3. システムをシンプルかつ効果的に保護するための方法

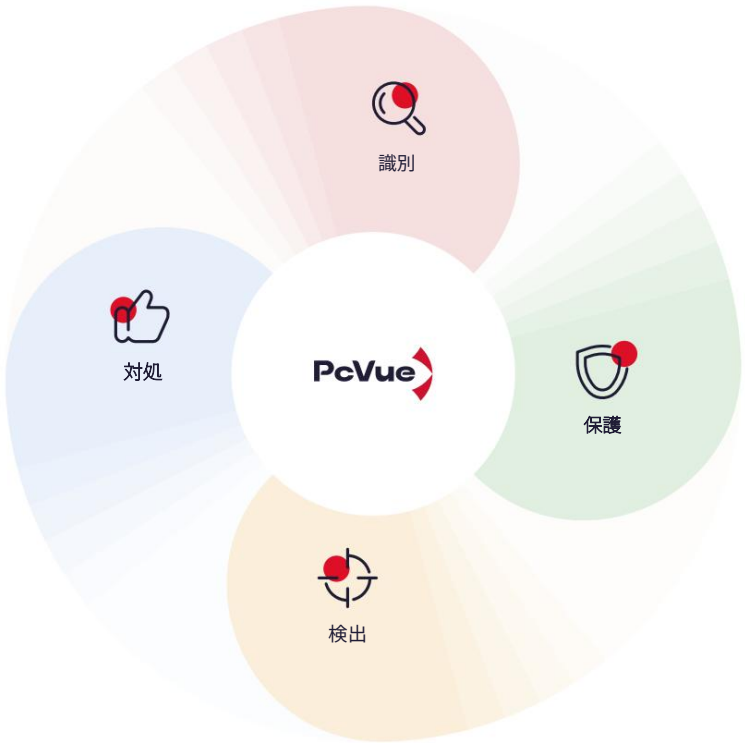


3. システムをシンプルかつ効果的に保護するための方法

- システムを分析して脆弱性を見つける
- 外部からの侵入（サイバー攻撃）を防ぐ
- 異常やトラブルを検知する
- システムを復旧できる状態にしておく

PcVue 監視プラットフォームは、サイバーセキュリティの 4 つの柱を中心に監視システムのセキュリティを強化できるデバイスとテクノロジーをベースとしています。

- システム分析と脆弱性の特定
- 侵入を制限するためのシステム保護
- 異常の監視と検出
- 運用条件の維持 - トラブル時の活動の再開



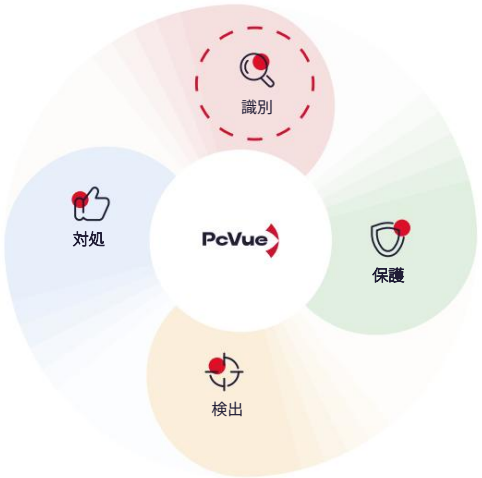
サイバーセキュリティ

システムを分析 - 脆弱性を特定する

システムの分析と脆弱性の特定は、システムのセキュリティを確保するための重要な前提条件です。

内容は次のとおりです:

- システムのセキュリティ境界と監視システムを確立する
- 必要な対策や設備を決める



サイバーセキュリティ

新しいシステム

この調査はシステム設計段階で実施されます

既存のシステム

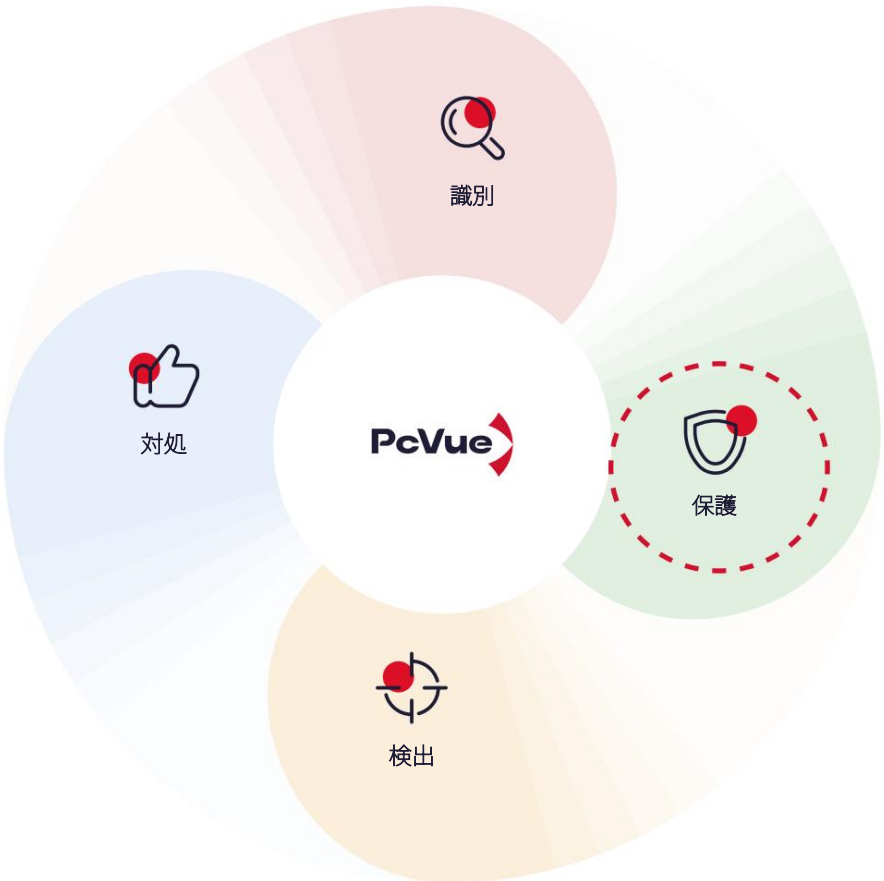
システムのネットワーク構成を把握するために、機器一覧やネットワーク構成図を作成する必要があります。
その際には、監視ツールなどのメーカー提供ツールを利用できます。
また、必要に応じて当社のコンサルティングサービスも支援できます。

覚えておくポイント

- この取り組みを進めるために、当社のサービスがサポートします。

侵入からシステムを保護する

システムとその脆弱性を十分に理解することで、システム管理者は必要なセキュリティ対策を判断することができます。これはサイバーセキュリティにおける重要な基本原則の一つです。当社のソリューションは、さまざまな保護手段を提供しています。

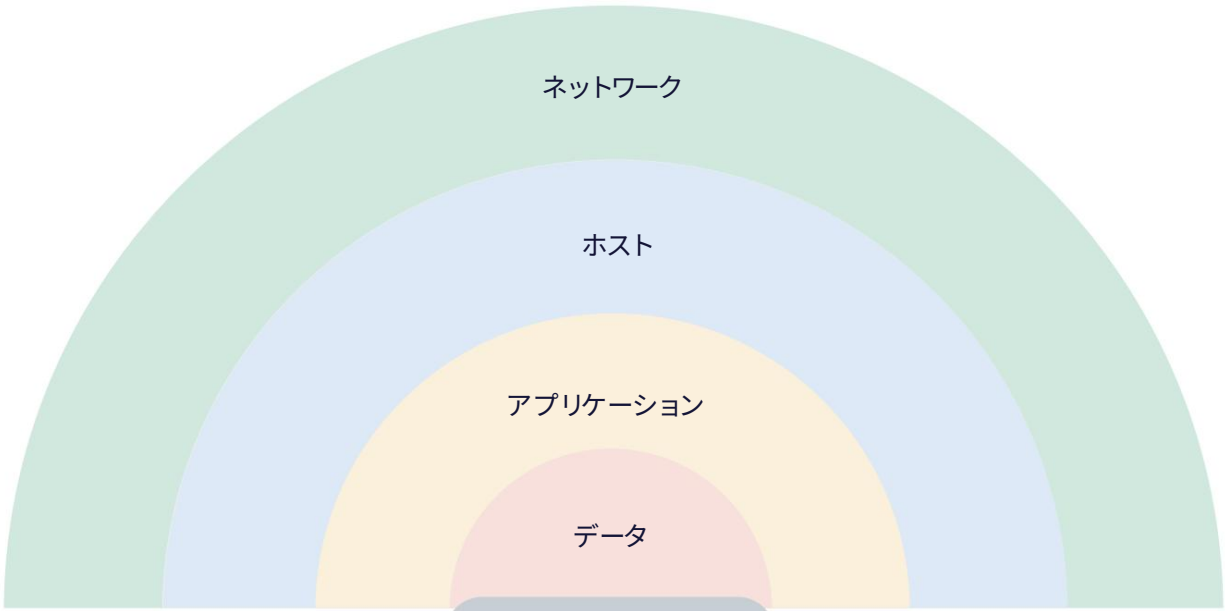


サイバーセキュリティ

基本原則 :多層防御

セキュリティレイヤー別

システム保護は、システム内にセキュリティの層を段階的に適用する、多層防御の基本原則に基づいています。



システムと攻撃者の間に複数のセキュリティ層を適用する

あらゆる独立した方法を使用して様々な種類の攻撃からシステムを保護する

セキュリティ対策

- 暗号情報
- 機器
- データ
- 処理
- 組織

いずれかのレイヤーに障害が発生した場合でも、他のレイヤーは動作を継続し、データを保護します。

全ての層でセキュリティ対策を行う

インストールするソフトウェアを信頼できますか?

ソフトウェアを使用する前に、それが正規のものであり、発行元によって作成されたものであることを確認してください。元の形式に準拠していること、つまり整合性が損なわれておらず、コンポーネントが変更されていないことを確認してください。これが最初のセキュリティ層となります。

バージョン11.2以降、PcVueのパッケージインストールとバイナリはデジタル署名されており、ファイルの整合性と信頼性が保証されます。これはインストール時だけでなく、その後の実行時も同様です。

ソフトウェアの配布を容易にするため、PcVueはサーバー経由で一括ダウンロードが可能です。

FTP

実用的なサービスには、安全対策が必要です。
例えば、セキュアFTP接続のみを受け付けるサーバーの使用などです。
さらに、当社サーバーからダウンロードしたファイルの完全性を確認できるよう、ダウンロード可能なすべてのソフトウェアコンポーネントの一意の署名である「ハッシュ」を提供しています。この手法により、ダウンロードされたファイルが当社が作成したものと完全に一致することを保証します。ファイルが改変または破損している場合、ハッシュは一致しません。PcVue 11.2以降では、この種の検証で最も広く使用されているアルゴリズムの一つであるSHA-256を採用しています。

注意事項

PcVueはインストールの信頼性と完全性を保証します。

安全なダウンロード

- 安全な接続によるサーバーへのアクセス

認証と整合性

- インストールするファイルは発行者によって作成され、デジタル署名されています
- SHA-256アルゴリズムによるダウンロードの整合性の検証

安全なインストール

- インストールコンポーネントの署名
- 署名されたバイナリ

インストール時にプロジェクトを安全にするために、どのような対策を講じるべきか？

ソフトウェアをインストールする際には、使用する機能について事前に検討する必要があります。実際には、特定のコンポーネントをインストールすると、ソフトウェアが攻撃にさらされる可能性があります。そのため、必要なコンポーネントのみをインストールし、攻撃対象領域を最小限に抑えることが重要です。

PcVueではインストール時に、以下のようなコンポーネントを選択してインストールすることができます。

- データ収集コンポーネント
- 設定ファイル
- Webコンポーネント
- SDKとAPI
- …

アプリケーションプロジェクトおよびオブジェクトライブラリは、運用ネットワークとは別の安全な媒体（ホワイトステーション）を使用して展開する必要があります。

PcVueには統合されたバージョン管理機能があり、すべてのシステム構成要素に対して同一のプロジェクトバージョンおよび参照ライブラリが展開されることを保証します。PcVueは各ステーションで使用されているバージョンを常に確認し、不一致がある場合にはオペレーターに警告します。

注意事項

インストール時:

- プロジェクトに必要なコンポーネントのみをインストールする
- オペレーティングネットワーク外部の安全なメディア（ホワイトステーション）を介してプロジェクトとライブラリを展開します
- すべてのワークステーションで弊社既定のバージョンを使用する

システムがITの前提条件を満たしていることを確認する必要があります。

PcVueのような監視ソフトウェアは、システムのセキュリティを確保するために、一定数の要件への適合が求められるITインフラストラクチャで使用されます。適切な導入とツールは、考慮すべき重要な要素です。

ニーズに応じて展開を調整する

PcVue ソリューションは、高いレベルのセキュリティを維持しながら、現在の制約を満たすさまざまな展開の可能性を提供します。

適切な実行モードを選択する

Windowsでは、ソフトウェアをサービスとして実行する方法と、アプリケーションとして実行する方法があります。
サービスとしての実行モードは、ユーザーインターフェースを必要とせず、ユーザーの操作なしで長期間継続して稼働する必要があるソフトウェアに適しています。
PcVueのような監視ソフトウェアでは、これはオペレーション用データ収集サーバーやヒストリカルサーバーなどのサーバーワークステーションに該当します。

一方、アプリケーションとしての実行モードは、ユーザーがグラフィカルインターフェースを通じて操作する用途に適しています。
これはPcVueのクライアントワークステーションに対応します。
これら2つのモードを使い分けることで、ユーザーインターフェースを持たないサーバー機能と、ユーザーが操作するクライアント機能を分離でき、適切なセキュリティレベルを保ちながらシステムを構成することが可能になります。

注意事項

サーバー ワークステーションをサービスとして、クライアント ワークステーションをアプリケーションとして展開します。

ウェブとモバイルの展開

Webクライアントやモバイルアプリケーションなど、さまざまな種類のシンクライアントを展開するためのソリューションには、必要なすべてのセキュリティ機能を統合する必要があります。これにはHTTPS、OAuth、証明書、HTML5などの技術に加え、保守・運用のためのツールも含まれます。
これらのソリューションを導入するには、本書の別章で説明されている安全なネットワークアーキテクチャも必要になります。
PcVueのWebおよびモバイルソリューションはクライアント／サーバーモードで動作し、Windowsの IIS（Internet Information Services） コンポーネントに依存しています。これにより、IISに備わっている各種セキュリティ保護機能を活用することができます。

PcVue は、Web またはモバイル アーキテクチャを定義、展開、管理するための展開コンソール Web をネイティブに統合します。
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アプリケーションの
- 展開
- データ保護管理
- 証明書管理
- ユーザーアクセスの登録とOAuthサーバー管理
- IIS監査/診断

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

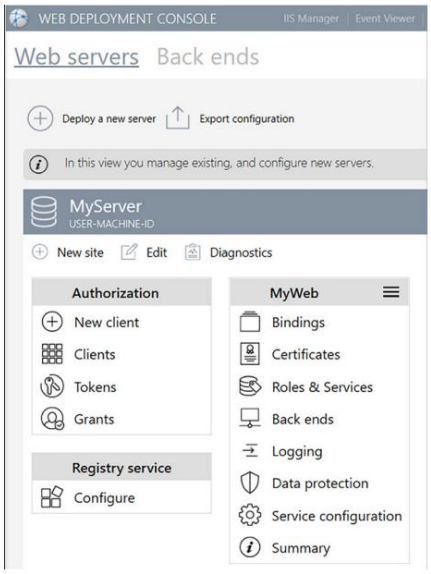


図1 - Webデプロイメントコンソール

注意事項

Web およびモバイルの展開には次のものが必要です。

- HTTPSによるセキュア通信プロトコルの実装
- セキュリティ証明書の使用と管理
- OAuthとの互換性
- 構成、メンテナンス、診断を可能にするコンソール

仮想環境

PcVueの標準的なクライアント/サーバーアーキテクチャに加えて、当社の製品は VMware® や Hyper-V™ などの仮想化環境でも使用されます。

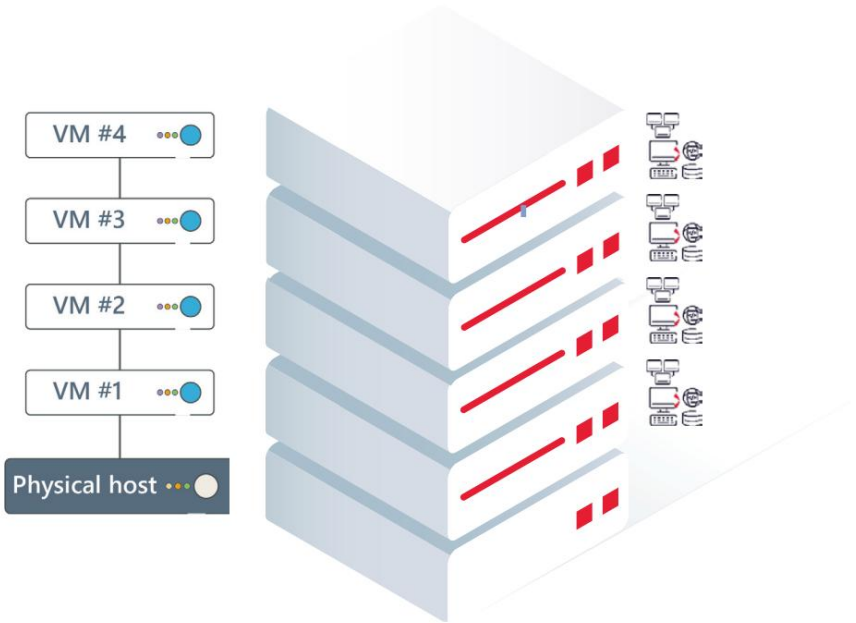


図 2 - 仮想環境

これらの環境により、1台の物理的なPcVueマシン上で、異なるオペレーティングシステムを使用した複数のPcVueアプリケーションサーバーを運用することが可能になります。
このマシンは、セキュリティが確保されたコンピュータールームに設置し、電源バックアップを備えることができます。
これにより、PCクライアントインフラ内での機器の地理的な分散を避けることができ、ハードウェア資源への物理的アクセスに関する脆弱性を低減できます。
その結果、PcVueアプリケーションのサービスレベルと可用性を維持したまま、運用の継続性を確保することが可能になります。

注意事項

仮想環境を展開して次のことを行います。

- サーバー管理を一元化し、単一の安全な場所に集約する
- 物理的なマシンリソースへのアクセスに関連するセキュリティ侵害を制限する

Windows リモート アクセス デスクトップ

リモート アクセス デスクトップ (RDS とも呼ばれます) は、サーバー上でアプリケーションをホストし、そのアプリケーションがインストールされていないスマートフォン、タブレット、または PC でリモートで実行できるようにする Windows 機能です。

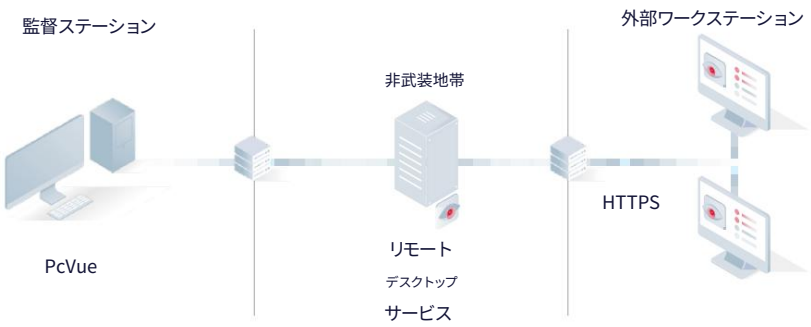


図3 - リモートデスクトップアーキテクチャ

これは、RDS機能がインストールされたサーバーにPcVueをインストールする構成です。
PcVueは、「ライトクライアント」と呼ばれるクライアント端末にはインストールされません。
このような構成では、中央サーバー上の1つのステーションに管理を集約できるという利点があります。
また、このサーバーへのアクセスや保守作業は限定されるため、セキュリティ上の脆弱性を低減することができます。データのやり取りは、キーボードやマウスの操作情報に限定され、通信には HTTPSプロトコル が使用されます。
そのため、データ破損のリスクを低減することが可能です。
さらに、RDS機能はWindowsのセキュリティ機能の恩恵を受けることができます。

注意事項

Remote Desktop Services 環境を導入することで、次の利点があります。

- サーバー管理を単一の場所に集中させ、セキュリティを向上させる
- HTTPS によるリモート通信のセキュリティを確保する
- ワークステーションへのソフトウェアインストールに関連するセキュリティ脆弱性を低減する
- Windows のセキュリティ機能を活用する
- 送受信データの破損リスクを低減する
- ネットワーク上を流れるのは キーボード操作およびマウス操作のみである

公開鍵インフラストラクチャ

データのセキュリティを確保するには、公開鍵インフラストラクチャ (PKI) を使用して、次の機能を提供するデジタル セキュリティ証明書を管理する必要があります。

- データへのアクセス管理（認証）
- データの整合性の検証
- データのプライバシー

データセキュリティを確保するため、公開鍵基盤（PKI）を用いてデジタルセキュリティ証明書を管理し、以下を提供する必要があります：

- データへのアクセス管理（認証）
- データ完全性の検証
- データプライバシー

これらの証明書は、OPC UAやICCP向けのIEC 62351といった特定のセキュア通信プロトコルにおいて特に有用です。通常、監視システムのユーザーはPKI管理のためにITサービスに依存しています。ユーザーが自律的に運用できるよう、PcVueは証明書を作成・展開するための統合PKIを提供します。

注意事項

データのセキュリティを確保するには、公開鍵 (PKI) のインフラストラクチャが必要です。PcVue は、必要なセキュリティ証明書を自律的に管理するための統合 PKI を提供します。

このアーキテクチャは、交換されるデータのセキュリティを保証しますか？

ネットワークアーキテクチャは、データのやり取りを安全にするよう設計する必要があります。
すなわち、アクセスを厳格に定義し、ネットワークの性質に応じてデータフローを制御することを意味します。
したがって、外部ステーション（管理ネットワーク、インターネットなど）から、機器が設置されている産業ネットワークへ直接アクセスできないようにする必要があります。
一般的に、取得サーバーステーション（acquisition server）は、設備と直接接続されているため潜在的な脆弱ポイントとなります。
そのため、他のネットワークから分離（アイソレーション）しておく必要があります。このため、以下の推奨事項に従うことをお勧めします。

- Routerを使用してネットワークをセグメント化する。

  - 物理ネットワークを分離し、論理的にはVLANにより領域を分割する
  - DMZを利用してネットワークを分離し、不正侵入を防止する
  - 2つのゾーン間の通信を保護するため、トンネリング技術を利用する

- ファイアウォールによるデータフローのフィルタリング

  Firewall を導入し、データフローを制御する。特に、ネットワーク外部から内部への通信を重点的に管理する。
  - 送受信トラフィックを、送信元アドレス・宛先アドレス・プロトコル・ポートに基づいてフィルタリングする

- 送受信データの保護（Secure data exchanges）
  - HTTPS による通信の利用
  - セキュリティ機能を備えたオープンプロトコルの使用（例：OPC UA、SNMPv3、IEC規格など）

PcVue は、標準的な TCP/IP レイヤーに基づくステーション間メッセージ通信を使用し、Ethernet ネットワーク上でマルチステーションのクライアント／サーバーアーキテクチャを構築することを可能にします。

一方、既存のクライアント／サーバーアーキテクチャにおいては、同一バージョンでプロジェクトアプリケーションが設定された PcVueワークステーションを追加したとしても、自動的にシステムへ参加することはできません。

この新しいステーションは、プロジェクト管理者が明示的に当該ステーションを登録し、アプリケーション内で維持すべきステーション間の関係を定義するまで、既存のステーションに接続することはできません。

PcVue は非常に柔軟性と拡張性に優れたプラットフォームであり、さまざまなアーキテクチャ構成に対応できます。
以下の図は、構成例の一つを示しています。

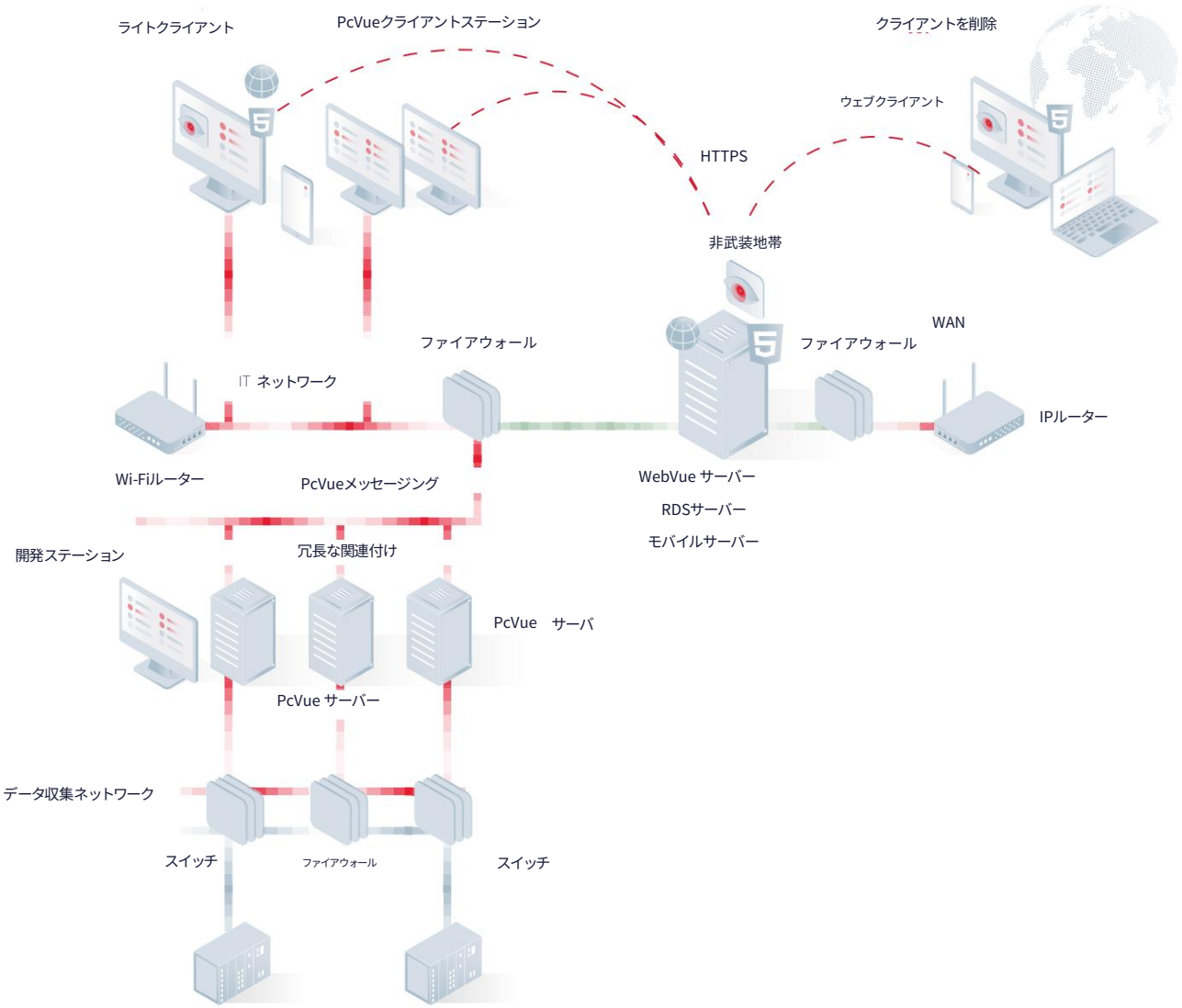


図4 - アーキテクチャの例

このサンプルアーキテクチャは、次の要素を中心に構築されています。

・データ収集は、産業ネットワーク上に配置された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、プロジェクトを一元管理するために使用されます。承認対象となるアーキテクチャでは、このステーションをネットワークから分離し、プロジェクトの基準バージョン（リファレンス）を展開するために、認証された専用の安全な媒体を使用することが求められます。

・運用操作は、ファイアウォールを介し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ワークステーションから実行されます。

・**非武装地帯（DMZ）**に配置され、ファイアウォールによって隔離されたWindows Server上のコンピュータには、Webサーバー、モバイルサーバー、およびWindows Remote Desktop Services（RDS）サーバーがホストされています。

- Windows リモート デスクトップを使用して、RDS インスタンス経由でクライアントをリモート実行できます。
- サーバーにインストールされたインターフェースにより、HTML5 に対応したすべての端末でクライアント インスタンスを表示できます。
- Web クライアントを使用すると、標準的な Web ブラウザから操作が可能です。
- モバイル サーバーに接続されたモバイル アプリケーションを使用することで、スマートフォンやタブレットからアラームの通知・確認や制御を行うことができます。
- Web サーバーと端末間の通信には、HTTPS によるセキュア ソケットが使用されます。
- 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（SSO）を可能にするWindows Active Directoryによって管理されます。
- PcVueはALLIED Telesisと提携し、上記の課題に対処するための包括的なハードウェア保護ソリューションを提供しています：
- 幅広いラインナップのセキュアな産業用ファイアウォール/VPN
- ネットワーク内の異なるエリア間のトラフィックの制限と制御
- トラフィック制限の設定

注意事項

- ルーターを使用してネットワークをセグメント化する
- データをフィルタリングする
- 「トンネリング」ソリューションを活用する：暗号化と認証
- ファイアウォールを使用してデータ通信を保護する
- サーバーを非武装地帯（DMZ）に隔離する

産業用および自動化システムの監視体制の確保

フィールド機器とデータ収集サーバー間のデータ交換には、監視システムにおいて考慮しなければならない特有のリスクが存在します。
使用されるプロトコルの多様性、その動作モードの違い、および性質（独自仕様か標準か）により、現在の脅威に対する耐性はプロトコルごとに異なります。
最も古いプロトコルは、多くの場合、セキュリティ上の制約を満たすことができません。
一方、国際標準に基づく新しいプロトコルには、必要なセキュリティ機能が備わっていることが一般的です。

相互運用性の観点から可能な限り、PcVueは産業用通信プロトコルのセキュリティ機能を統合しています：
• OPC UA（認証および認可のためのOPC-Securityサポート）および統合PKIによる証明書の導入
• SNMP - PcVueのSNMP Manager実装は、認証、完全性保証、および暗号化を可能にするSNMP v3をサポートしています。
• IECプロトコル
• MQTT（TLS経由）ネットワークのセキュリティ確保に関する推奨事項は、フィールドネットワークにも同様に適用されます（セグメンテーション、フィルタリング）。

注意事項

- セキュリティメカニズムを統合したプロトコルの使用を推奨する
- IT/OTネットワーク間でセグメンテーションとフィルタリングを適用する
- 獲得フローにルーターとVPNトンネルを使用する

安全性とアーカイブデータの完全性を確保する方法

監視（SCADA）によって生成される履歴データは、企業組織においてますます重要かつ戦略的なものになっている。そこから得られる教訓としては、次のような点があります：

・トレーサビリティ要件への対応
・プロセスの十分な理解とその分析
・運用またはインフラの最適化
・インシデント発生後の分析（第三者による分析を含む）

一方で、生成されたデータや履歴情報は、製造プロセスの特性や企業のコアビジネス、機密情報を明らかにする可能性があります。

サイバー犯罪の脅威に直面する中で、履歴データの生成およびアクセスに関する原則は、当社製品に組み込まれたセキュリティ対策に基づいています：

- ユーザー権限に応じて、データアクセスはフィルタリングおよび制限されます
- データは複数の形式で生成されます（独自フォーマット〔第三者からアクセス不可〕、Microsoft SQL Server など）

データのセキュリティおよび完全性は、組織内で運用されている Windows Server や Microsoft SQL Server が提供する標準的なセキュリティ機能によって、さらに強化することが可能です。

例えば ：

・ユーザー認証は、Microsoft SQL Server において「接続（connection）」というオブジェクトとして管理されます。したがって、この接続を利用するアプリケーションのみがインスタンスへアクセスする権限を持ち、それ以外のアプリケーションはシステムから拒否されます。

・接続の作成時には、管理者がデータ管理に関する権限を割り当てることができます。
このために、SQL Server では「サーバーロール（Server Roles）」と呼ばれる権限モデルが用意されています。

・接続が作成されただけでは、データベースエンジンのリソース（データベース、テーブル、機能など）にアクセスすることはできません。
アクセスするためには、その接続を対象となるデータベースのユーザーに関連付ける必要があります。

・ユーザー作成後は、そのユーザーに対してロールを割り当て、実行可能な操作範囲を定義することが重要です。（接続管理、バックアップ、読み取りアクセス、削除・変更など）

注意事項

・データへのアクセスは、ユーザー権限に応じてフィルタリングおよび制限されます

・データは複数の形式で生成されます（独自フォーマット〔第三者からアクセス不可〕、Microsoft SQL Server型データベースなど）

・データのセキュリティおよび完全性は、Windows ServerおよびMicrosoft SQL Serverが提供する標準機能により強化されます

システムユーザーの要件は何ですか?

ユーザー権限の管理は、監視システムの保護において不可欠です。
なぜなら、これによりユーザーの操作範囲を制御できるからです。
例えば、PcVueアプリケーションの機能は、接続しているオペレーターのユーザー権限によって異なります。
PcVueを使用する前に、ユーザーはアカウントにログインし、ユーザー名と対応するパスワードで本人確認を行う必要があります。
このユーザーアカウントの設定により、運用時に利用可能なプロジェクトの機能（例：ユーザーが起動できるウィンドウなど）や、設定ツールおよびオペレーティングシステムへのアクセス権が決定されます。
また、ユーザーアカウントを使用して、そのユーザーに関連付けられたウィンドウの選択を行ったり、ユーザーがログインした際に実行するプログラムを選択したりすることも可能です。

役割を定義する

まず、監視における各ユーザーの権限範囲に応じて、役割を定義します（管理者、開発者、オペレーターなど）。
PcVueでは、各ユーザーアカウントには、ログインに使用する名前とパスワード、および権限を定義するプロファイルが関連付けられています。
設定できるユーザー数に制限はありませんが、同一の端末では、一度に1人のユーザーしかログインできません。
ユーザーがログインしている端末に応じて、適用される権限が異なる場合があります。
また、ゾーンの設定も可能です。
プロファイルの設定により、ユーザーのアクセス権限を付与します。
同じプロファイルを複数のユーザーに関連付けることができます。
設定可能なプロファイルの数に制限はありません。
新しいユーザーが作成されると、そのユーザーにプロファイルが関連付けられます。

アクセス権限の管理を最適化

次に、利用可能なオプションを選択して、アクセス権限の管理を最適化する必要があります：

- ユーザーの自動切断

操作がない状態が続いた後のタイムアウト時間を、設定可能

- パスワードの有効期間の設定
- パスワードの強度チェック
- 階層レベルとプロファイル

・特定ミミック、コマンド変数、および履歴データへのアクセス制御、ならびにアラームのアクノリッジおよびマスキング機能

・マルチステーション環境において、接続先ワークステーションに応じたユーザープロファイルの割り当て

・初回ログイン時におけるパスワード変更の強制

・ログイン試行が3回失敗した場合のユーザーアカウントのロック機能

・ユーザーアカウント情報の暗号化

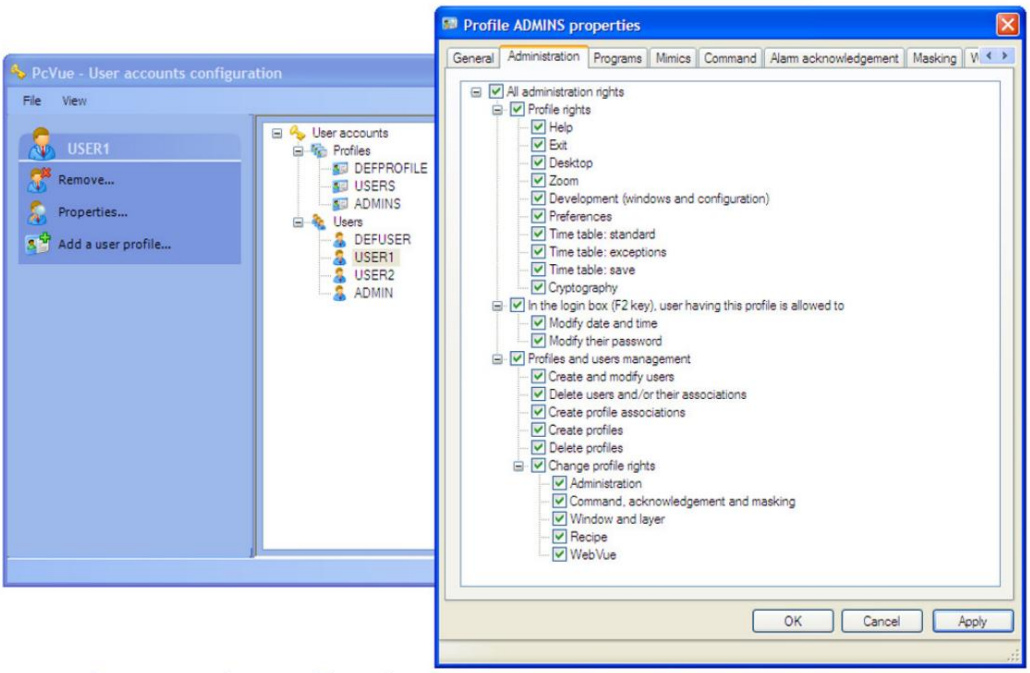


図5 - ユーザープロファイルの設定使用権管理と企業ディレクトリの使用

一部の企業では、ITアーキテクチャにおいて、自社のコンピュータ資源を利用する可能性のあるすべてのユーザーを一覧管理する中央ディレクトリの使用を義務付けています。
PcVueは、ユーザーの識別および認証を確実に行うために、WindowsのActive Directoryを利用することが可能です。

この場合、ユーザーはSupervisor内で直接定義されるのではなく、「PcVueプロファイル」と「Active Directoryグループ」との関連付けにより、監視アプリケーション内での権限およびユーザー権限が決定されます。
これには、操作・指令の実行権限や、アラームの承認権限（レベルや優先度別など）が含まれます。

これらの連携処理は完全に自動化されており、運用レベルではユーザーからは意識されない（透過的に動作する）仕組みとなっています。
また、ディレクトリの暗号化についても確認する必要があります。

適切なライセンスモードを選択してください

ユーザー権限にかかわらず、PcVueライセンスに「開発モード」が含まれている場合にのみ、プロジェクト設定レベルでの変更が可能となります。当然のことながら、「ランタイム」ライセンスでは、製品設定メニューへのアクセスは一切許可されません。この原則により、「開発モード」のライセンスのみを展開することで、アプリケーションの変更機能に対する制限が強化されます。
また、これらの原則は、ユーザー権限の管理によってさらに強化されています。なぜなら、たとえ開発を許可するライセンスを使用してステーションにアクセスしたとしても、必要なプロファイルとパスワードを持っていない場合、そのユーザーはプロジェクトの開発機能にアクセスできないからです。

ユーザーアカウントの追跡

システムの利用者、特に利用者の資産に関する全体像を把握しておくことが不可欠です。
不要なアカウントやプロフィールは削除する必要があります。汎用アカウント（例えば、チーム用のアカウントなど）は禁止すべきです。
インシデントや攻撃が発生した場合に、事象の経過を把握できるよう、ユーザーの活動はログに記録される場合があります。

注意事項

- 役割を定義
- ユーザーアカウントのマッピングと追跡
- 権利管理の最適化
- 可能であれば会社のディレクトリ権限を使用
- ディレクトリの暗号化をチェック

PcVueで利用可能なセキュリティ機能一覧

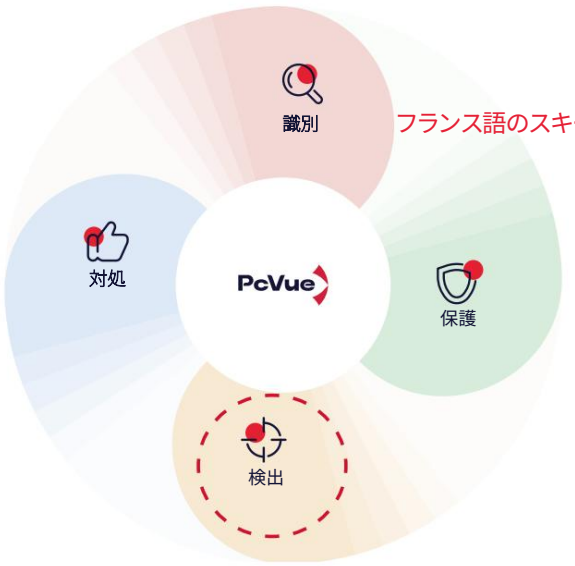
対応機能／対応技術	コメント
セキュアHTTP（HTTPS）	WebVueとWebServicesはプロキシ対応インターフェースです
プロキシ	PcVue 認証のメカニズムを使用することも、Active Directory のみを使用して LDAP 認証を委任することもできます。
未使用の機能やインターフェースを無効化またはアンインストールする機能。 例: Telnet、FTP アクセス、WEB インターフェイス、 プロトコル制御コマンド、インターフェイス シリア ル、USB ポート...	オプション機能のほとんどは既に無効化またはブロックされている可能性があります。新しいバージョンでは、セキュリティ強化のため、デフォルト設定がより制限されています。
公開鍵インフラストラクチャ（PKI）	統合PKIサポート

図6 - 利用可能なセキュリティ機能の表

異常の検出

識別および保護の各ステップが実施された後は、システムが期待どおりに動作していることを確認し、基準状態と比較して異常な挙動を検出する必要があります。

PcVueは、アプリケーションおよびネットワークの両面において設備の健全性を監視するためのさまざまな手段を提供しており、監視システムのモニタリングおよび診断のための多くのツールを備えています。



サイバーセキュリティ

システムの動作を診断するには?

監査診断

診断監査は、PcVueのコンポーネントの一つであり、監視システム内部の動作に関する情報を表示することができます。主な用途は診断支援ですが、システム全体が正常に動作しているかを確認する目的でも使用できます。
2種類のトラッキングページが用意されています。

カウンターと監視

このビューでは、監視システム内部のカウンターの詳細一覧を表示します。

Object：システムリソースおよびアプリケーションオブジェクトに関するカウンタ
Instance：PcVueハンドラ間のメッセージカウンタおよびそれらに割り当てられたメモリ
Time：各ハンドラにおけるメッセージ処理時間
Flow：変数ツリー内の変数のリアルタイム値の遷移に関連するデータフロー

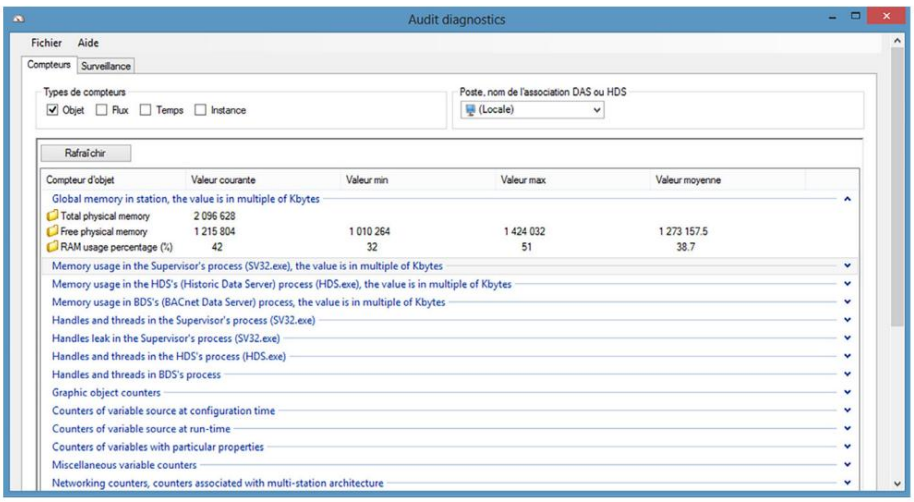


図7 - 診断ツール

監視

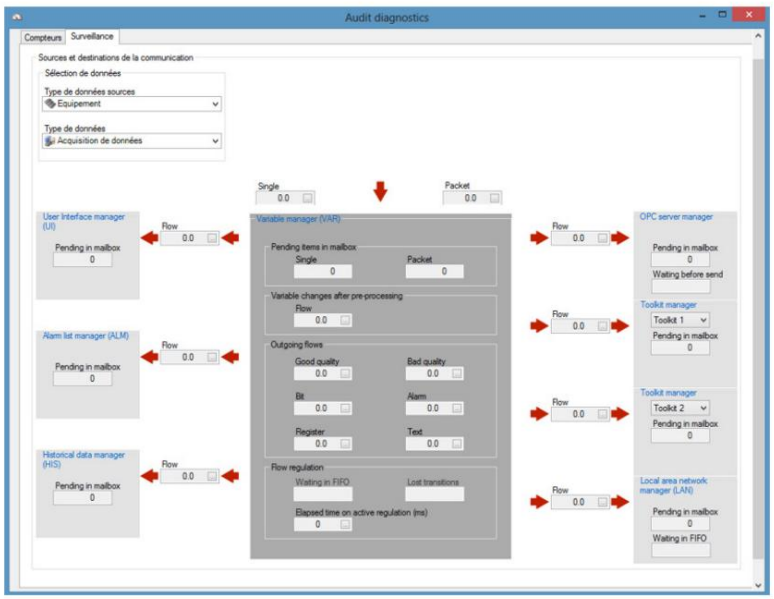


図8 - フローの可視化

このビューでは、PcVue内部の異なるモジュール間のデータ交換の詳細を即座に確認できるほか、遷移時の対応するデータストリームの詳細情報や変数のリアルタイム値も確認できます。

これにより、ユーザーはシステムの健全性を分析できます。

2つのビューが用意されています。1つはデータ取得フロー（PcVueへの受信データ）を表示するビュー、もう1つは書き込みストリーム（PcVueから送信されるデータ）を表示するビューです。

産業用および自動化システムの監視体制の確保

イベントログ

PcVueは、アラーム、オペレーター操作、値の変化などのイベントを記録するデータロギング機能を備えています。これらのイベント履歴ファイルは、専用のビューア画面を通じてオペレーターが確認できます。

システム変数

PcVueは、管理者の稼働状態（処理中リクエスト数、保留中リクエスト数、アーカイブ処理量 など）を示す多数のシステム変数を提供します。
これらのデータは、監視画面上で瞬時値、メーター表示、トレンドグラフなど、さまざまな形式で可視化でき、必要に応じて履歴として保存することも可能です。
さらに、PcVueのSNMPエージェント機能により、サードパーティ製の監視システムへデータを送信することもできます。

イベントログ

PcVueのすべてのモジュールは、イベントログに収集されたトレースを生成します。これらのログはローカルトレースファイルとして保存され、SIEM（セキュリティ情報イベント管理）内で一元管理することもできます。このログ記録は、システムの機能不全、侵入の疑いなど、事後分析が必要なあらゆるケースで役立ちます。

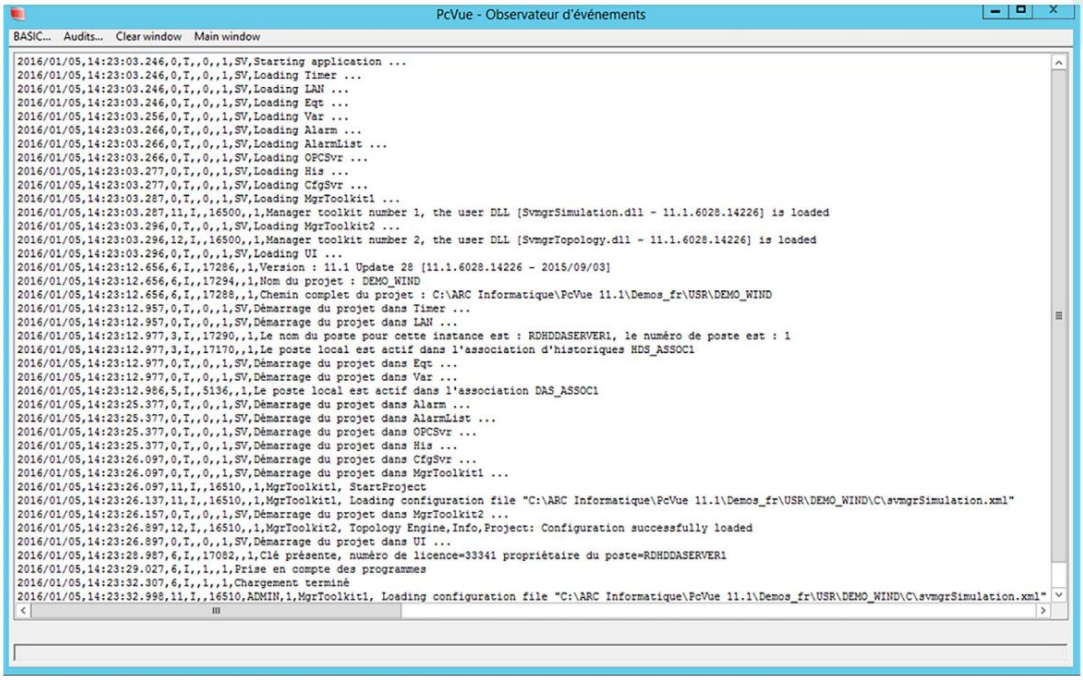


図9 - イベントビューアー

イベントに関するレポートの分析結果を、IT監視ツールへ提供する必要があります。

SYSLOG と Windows イベント ログ

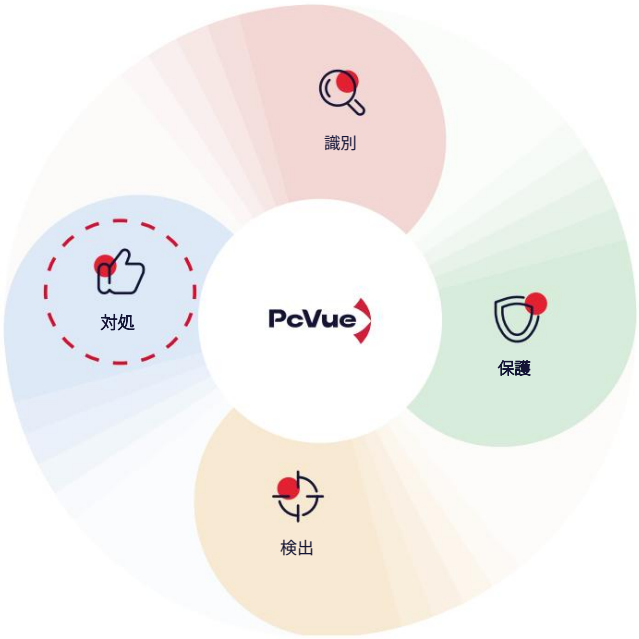
PcVueは、イベントログをサードパーティ製の監視ツールへ集約し、イベントの相関分析および解析に活用することが可能です。
WindowsイベントビューアおよびSYSLOG（UDP／TCP／TLS、RFC 3164およびRFC 5424）に対応しており、ログおよびトレースに関するANSSIおよびIEC 62443の要件にも準拠しています。

覚えておくポイント

- 組み込みの監査および診断機能でシステムの動作を検証
- トレーサビリティツールを参照
- システムデータをIT監視ツールと共有

運用条件におけるメンテナンスの確保

- 活動再開の許可



PcVueは、イベント発生後にアプリケーションの正常な動作を迅速に復旧するための高度なプロジェクトバージョン管理機能を標準で備えています。
本機能は構成リポジトリに基づいており、アプリケーション全体（オブジェクトライブラリ、データベース設定、ユーザー権限など）を一元管理するアクセスポイントを提供します。
また、Microsoft Windows Server によるセキュリティ機能と連携することで、情報へのアクセスは、アプリケーションの変更権限を持つユーザーのみに制限されます。
通常は、PcVue SCADAアプリケーション専用の開発用ワークステーションを用い、中央ディレクトリ上でプロジェクトのバージョン管理および変更作業を行います。

認証が求められるシステム構成においては、本ワークステーションを分離するとともに、改ざんされていないことが保証された専用のセキュア媒体を使用して、基準となるプロジェクトバージョンを展開することが推奨されます。
これにより、データの完全性およびシステム運用の信頼性を確保します。
さらに、バージョン管理に基づくトレーサビリティを提供することで、アプリケーション全体のデータを保全・保護することが可能です。

例えば、以下のようなバージョン管理が可能です：

・N-1バージョン：問題発生時に、迅速に前バージョンへロールバック可能

・Nバージョン：すべての検証・適格性確認を完了し現在運用中のバージョン

・N+1バージョン（複数可）：開発中のバージョン（検証・適格性確認の実施状況は状況に応じて異なる）

また、コメント機能により、各バージョンの状態や必要な情報を記録でき、変更履歴のトレーサビリティを確保します。

さらに、バージョン管理機能は、以下のような展開にも対応します：

・新しいデータセットをシステム全体の各ノードへ自動配信し、データの整合性および一貫性を確保します。

・新たに追加されたワークステーションに対して、検証済みの基準バージョンを自動的にダウンロードし、未検証または古いデータの使用を防止します。

・一時的に停止していたステーションにおいても、起動時に保有するプロジェクトバージョンが最新であるかを自動的に確認し、必要に応じて最新版をダウンロードします。

・問題発生時には、N-1バージョンへ迅速にロールバックし、基準バージョンとして復元することが可能です。

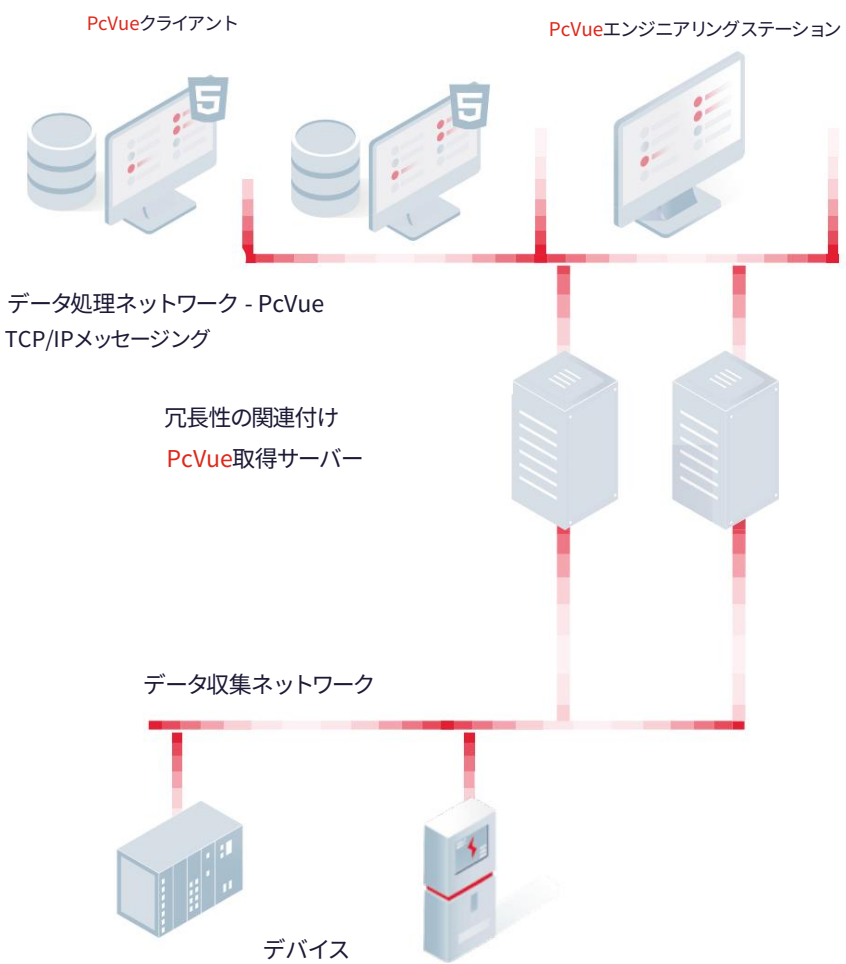


図10 - 集中型バージョン管理のアーキテクチャ

4. ARCのサイバーセキュリティーへの取り組み

ARCのサイバーセキュリティへの取り組み

デザイン製品

安全性の側面は、当社の製品が設計および開発される条件に大きく依存します。

これは特定の原則に基づいています:

設計、開発、認定、生産プロセス
当社のISO 9001品質管理システムには、
- 仕様策定方法論、設計、開発
- 検証計画
- 資格取得計画
- ユニットテストのためのソフトウェアロボットの使用
- ベータサイトでの本格的な検証
- フルスケールプロジェクトにおける社内プラットフォーム認定（負荷とパフォーマンスの測定）
- 回帰テスト
- 異常追跡のための品質システム
- 当社は、これらの研究、開発、または認定を下請けに出していません。

ARC グループ以外の企業も取り扱っています。
- 当社の製品には監視およびログ記録のメカニズムがあり、異常を検出し、顧客診断の段階を容易にする
- アーキテクチャのさまざまなコンポーネントの動作状態。顧客がシステムの動作を知り、制御できるようにする

セキュリティとプロジェクト管理

はじめに述べたように、監視プロジェクトのセキュリティ アプローチは、製品またはテクノロジ (スーパーバイザー、VLAN ネットワーク アーキテクチャ、Web アクセスなど) に導入された予防措置やデバイスだけに基づくことはできません。

そのためには、調査、仕様策定、試験、試運転といった段階を含むプロジェクト方法論に、この側面を組み込む必要があります。これは運用•保守段階においても同様です。

このため、当社の「サービス」には、準備プロジェクトと構築または保守フェーズの両方におけるトレーニング サービス、サポート、アドバイスが含まれており、これにより当社はお客様をサポートし、お客様の監視システムの範囲内でこのテーマに関する当社の経験をお客様に活用していただくことができます。

当社は、次のようなプロジェクトでお客様をサポートしてきました。

- 原子力環境におけるエネルギー生産施設の運用
- 原子力環境における安全および実験の実施（SIL II に分類されるプロジェクト）
- 安全物品および人員のための輸送インフラストラクチャまたは一般に公開されているインフラストラクチャの監視
- エネルギー輸送ネットワーク
- その他…

セキュリティポリシー

あらゆる努力を払っているにもかかわらず、当社の製品には、統合されているシステムを危険にさらす可能性のある脆弱性が存在する可能性があります。これらの脆弱性の影響を最小限に抑えるため、ARC Informatiqueは、お客様、当局、そして一般の方々に対して透明性のある対応を徹底しています。

実際には、製品の設計段階を超えて、当社は次のことに取り組んでいます。

1. 安全なソリューションの導入を支援するために、当社のノウハウをお客様やパートナーに提供します。

2. 当社の製品に関するアラートの積極的な監視とフォローアップを確実に実施します。

3. CERT（コンピュータ緊急対応チーム）のネットワークと、これらのCERTのコミットメントと推奨事項を遵守するITセキュリティ関係者と連携して行動する。

4. 当社製品に関する既知の脆弱性について、社内で発見されたものか第三者によるものかを問わず、セキュリティアラートとして透明性をもって情報提供します。

5. アラートが発生した場合、直ちにリスクを軽減するための情報をお客様にできるだけ早く提供するために、セキュリティ速報を提供します: https://www.pcvuesolutions.com/security

6. フィードバックを活用して、より安全な製品を設計します。

出典

PcVue - Webおよびモバイル展開におけるセキュリティ運用のベストプラクティス

PcVue - アーキテクチャと展開

PcVue

LET'S ENGINEER

ARCインフォマティーク

www.pcvue.com

PcVue – 安全な監視
産業および自動化システム EN
発行番号: AT-2024-14-08 v.4

swiss safety center ISO 9001 ISO 14001 ISO 27001 certified system

PcVue ARC Informatique is IEC62443-4-1 certified