



PC間のOPC通信の実装において、DCOMのセキュリティ設定は非常に困難な作業でした。

パート3（全8パート）：

OPC UA 誕生の 10 個の理由

OPC UA 関連記事シリーズのパート2 (SPS-Magazin、第4号) では、OPC UAの誕生のきっかけ、開発と目的について説明しました。パート3では、完全なる新世代の技術、OPC UA (Unified Architecture) の開発のきっかけとなった主な10個の理由について説明します。OPC UAは、OPCの経験と、OPC技術誕生以来14年以上に渡る技術的な変化と傾向に基づくとともに、OPCベンダやユーザからの多くの希望や提言も取り入れています。

1. COM/DCOMの廃止

OPC Classicアプリケーション間のデータ交換は、MicrosoftのCOM技術をベースに自動化しています。Windows OSが世界中に急速に広まり、オートメーションでもWindowsが使用されるようになったことで、OPC技術が幅広く採用される環境が整ったのです。しかし、

2002年の初めに、Microsoftは新しい.NETフレームワークのリリースと、DCOMの廃止を発表しました。将来のWindows OSがDCOMをサポートしないわけではありませんが、OPC Classicの基盤となる技術が今後は開発されず、いずれ廃れた技術となることを意味しています。

2. DCOMの制限

90年代、Microsoftは、産業分野以外のホームコンピュータのエンドユーザにも、Windowsコンピュータを産業用アプリケーションのオートメーションコンポーネントとして使用する専門家のユーザにも高く評価されているいくつかの機能を、COM/DCOMによって導入しました。それらはコピーと貼り付け、ドラッグ&ドロップ、リンクや組込みなどの機能です。さらにDCOMは、認証、認可、暗号化などの必要なセキュリティを備えた完全な通信インフラも提供し、DCOM Securityを使用したリモートコンピュータ上のデータやプログラムのアクセス権限の制御が可能となりました。しかし、同時に、PC間のOPC通信に関わるプロジェクトの管理を行う、セットアップエンジニア、システムインテグレータ、開発者は困難な作業に取り組む必要に迫られました。DCOM Securityを正しく設定するには非常に複雑なタスクを実行しなければならず、高い専門性が求められます。そのため、セットアップエンジニアやシステムインテグレータは、煩雑なプロセスを迅速に終わるために、ネットワークに接続されたすべてのOPCコンピュータに常に幅広いアクセス権限を与えるようになり、認証されていないリモートアクセスからの保護機能が弱まる結果となりました。簡略化されたこの手順はITのセキュリティ要件に反しており、長期的に見ると、過失や妨害工作による損害のリスクを負うこととなります。DCOM Securityの設定は、設定が容易なOPCの通信関係とは正反対の、手のかかる作業でした。

3. ファイアウォールを介したOPC通信

コンピュータの境界を越えたOPC通信が可能であることは、オートメーション産業では最初から認識されていました。しかし、ここでもまた、OPC Classicの通信の制限となったのがDCOMでした。DCOMは、接続の確立、認証、データ転送やその他の多くのサービスの実行に、複数のポートを必要とします。その結果、DCOM通信のために、ファイアウォールに多くのポートを開けておかなければなりません。ファイアウォールにポートを開けるということはセキュリティ上の空白につながり、ハッカーからの攻撃のターゲットとなる可能性があります。OPC Classic製品を使用する際のDCOMの制限を解決する戦略として、OPCトンネリングが最も広く使用されています。

4. non-Windowsプラットフォーム上でのOPCの使用

オペレーティングシステムのコンポーネントとしてDCOMを備えたMicrosoftプラットフォームが産業アプリケーションに「偏在」していたことが、OPC Classicが急速に広まった主要な要因でした。一方で、他のオペレーティングシステムを導入していた場合、OPCの統合構想を実現することはできませんでした。例えば、IT産業ではUNIXやLinuxシステムが多く使われていますし、オートメーションでも、断固としてWindowsオペレーティングシステムの実装を拒否する応用分野もあります。組込みもまた、Windows CEやXP Embedded以外のWindowsが不得意とする分野です。複雑なアプリケーションは、DCOMを実装していないVxWorks、QNX、組込みLinux、RTOSなどの組込みOSで稼動しているフィールドデバイス、PLC、オペレータパネルなどのデバイスに直接組み込まれています。OPCは技術基盤としてDCOMを必要とするため、その基盤が存在しない組込みシステムではOPCを使用した統合構想を実装できないのです。

5. Webサービスを使用した高パフォーマンスのOPC通信

2003年のOPC XML-DA仕様のリリースは、OPC協議会がWindowsプラットフォームとDCOMによる制限から解放される道を初めて示唆した活動でした。今日、多くのOPC XML-DA製品で、Webサービスを基盤とするOPC技術の提供が可能となりました。しかし、XML-DA通信のデータスループットはDCOM DA通信と比べると1/5から1/7の速さで、多くのオートメーションタスクでは許容できないパフォーマンスです。Webサービスを基盤にしたOPC通信の未来は明るいのですが、より高パフォーマンスを実現する必要があります。

6. 統合されたデータモデル

例えば、温度センサーの現在の値、事前定義した制限温度を超えた場合のイベント、過去の温度の平均値などのデータを取得するには、従来のOPC ClassicではData Access、Alarms&Events、Historical Data Accessの3つの異なるOPCサーバーが必要でした。プロセスデータ、イベント、履歴データに異なる方法でアクセスしなければならず、ユーザにとって非常に時間のかかる処理でした。3つのオブジェクトモデルを統合することで、OPC製品のベンダだけではなく、システムインテグレータやユーザもずっと簡単に処理が行えるようになりました。

7. Complex Data構造のサポート

OPCの主要なアプリケーションの1つに、シリアル通信プロトコルやフィールドバス通じてネットワーク接続されたデバイスの操作と監視があります。デバイスを設定するには、データ構造要素の意味などの複雑なデータ構造を、OPCクライアントからデバイスへ、OPCサーバーを介して記述できるようなデータタイプが必要となります。OPC協議会は、Complex Data仕様を導入し、複雑なデータ構造の記述を可能にしました。しかし、わずかな例外を除き、現在市場にあるOPC Classic製品の多くはComplex Data仕様を実装していません。

8. データ損失が発生しないプロセスデータ通信

データアクセスは、当初はプロセスデータの現在の状態をクライアントアプリケーションに周期的に通知するために定義されました。OPCクライアントとリモートのOPCサーバー間の物理的な通信リンクに問題が発生すると、Data Access仕様に基づき通信が切断されます。通信切断中に発生したデータ変更はOPCクライアントには転送されず、データが失われます。このようなデータ損失は、傾向の記録、プロセス監視、プロセス可視化など多くのData Accessプロジェクトでは深刻な問題ではありません。しかし、OPCは要求仕様がより厳しい分野にも応用されつつあります。例えば、OPC技術が化学や製薬業界などで利用される場合、データは途切れることなく記録されなければなりません。その実現のために、各ベンダは固有の機能拡張を行っています。切断された通信を迅速に検知する接続監視システムに基づいた拡張では、通信の切断が発生すると自動的に再接続します。さらに、Data Accessサーバーでのデータバッファリング、多重化、ストア&フォワード概念も実装しています。このような機能拡張は非常に便利ですが、OPC Classicでは定義されていないため機能はベンダごとに異なります。

9. 認証されていないデータアクセスからの保護の強化

Ethernetベースの通信がオートメーション分野で広く使用されるようになり、オートメーションネットワークとオフィスネットワークが接続されるようになりました。それは、垂直統合という新たな道を開く一方、新たなセキュリティリスクを高めることになりました。リモートメンテナンスやリモート制御構想でのOPCの利用も増えています。この分野でも、外部からの認証されていないアクセスからのインストールに対するより厳しいセキュリティ要件を満たす必要があります。ネット犯罪、スパイ行動、破壊行為などが増えており、それに伴いITセキュリティが非常に重要になっています。同様に、OPC利用時のセキュリティ要件も非常に重要です。ベンダによる適切な対策の開発なくしては、OPC Classicはその高いセキュリティ要件を満たすことはできません。

10. メソッドコールのサポート

多くのアプリケーションでは、値の読み込みと書き込みだけではなく、ドライブの起動や停止、デバイスへのファイルのダウンロードなどのコマンドの実行も重要です。OPC Commands仕様では、コマンド実行実現のための定義を行っていますが、ドラフトバージョンでのみ使用可能で、OPC Classicでは実際には検討されませんでした。

OPC UAシリーズのパート4では、OPC UA仕様を詳しく説明します。

<http://industrial.softing.com/>