計装クラウドサービスのセキュリティ対策

Security Measures for Instrumentation Cloud Service of Digital Manufacturing Solutions

深井　英五 FUKAI Eigo　　天木　　智 AMAKI Satoru　　金井　　遵 KANAI Jun　　伊東　　雄 ITO Yu

IT（情報技術）とOT（制御・運用技術）のデータ連携が可能な計装クラウドサービスの製造現場への適用が始まっている。その中核をなすクラウド型PLC（Programmable Logic Controller）はクラウドシステム上に配置された制御コアからOTの現場機器を制御するシステム構成であり，制御データがインターネットを介することから，従来システムの構成とはセキュリティ要件が異なる。

東芝グループは，独立行政法人 情報処理推進機構（IPA）(注1)のガイドラインにのっとった資産ベースの脅威分析結果とゼロトラストアーキテクチャーに基づいた計装クラウドサービスのセキュリティ対策を実現した。

The trend of introducing instrumentation cloud services that facilitate collaboration between operational technology (OT) and information technology (IT) data is accelerating with the aim of driving advancements in digital manufacturing. Cloud-based programmable logic controllers (PLC) on the instrumentation cloud service of digital manufacturing solutions are playing a key role in these services, however, introducing further enhanced security measures compared to conventional OT systems using hardware-based PLCs is essential because they control devices used in OT systems from a control core via the Internet.

The Toshiba Group has conducted asset-based security threat analyses compliant with guidelines published by the IPA (Information-technology Promotion Agency, Japan). Founded on the results of analyses, we have achieved practical implementation of security measures appropriate for the instrumentation cloud service of digital manufacturing solutions along with zero-trust architecture approaches.

1. まえがき

製造業においては，労働人口の減少やカーボンニュートラルへの対応が必要となっており，スマートマニュファクチャリング化への要求が増している。東芝グループは，従来システムでは困難であったITとOTの連携を実現した計装クラウドサービスを提供し，製造現場の効率化だけでなく，変化し続ける製造現場の運用にも柔軟性を持たせて生産性を大幅に向上させる活動を推進している(1)。

計装クラウドサービスは，クラウド型PLCであるMeister Controller Cloud PLCパッケージ typeN1（以下，typeN1と略記）を中核としたサービスで，OTの現場にとどまっていたデータをクラウドシステム上で連携・展開することを特長としている。クラウドシステム上で動作する制御コアのtypeN1から製造現場にある現場機器を制御するもので，クラウドシステムと製造現場にあるエッジエージェント装置とがインターネットを介して接続したシステム構成となっている。このようなシステム構成のため，セキュリティシステムを通すことで脅威を防ぐ境界型防御のアーキテクチャーを備えた従来の制御システムとはセキュリティ要件も異なっている。

また，産業用分野で求められるOTセキュリティは，ITセキュリティとは異なり，システムの可用性が重視される。

東芝グループは，typeN1及びMeister nV-Tools Cloudのセキュリティ対策を進めるにあたって，パブリッククラウドサービスが持つセキュリティ対策を有効に活用しながら，ゼロトラストアーキテクチャーに沿ったセキュリティ対策を実施した。

ここでは，東芝グループの計装クラウドサービスのシステム構成を示した後，実運用を考慮して実施した脅威分析の結果とゼロトラストアーキテクチャーに沿ったセキュリティ対策について述べる。

2. 計装クラウドサービス

図1に，計装クラウドサービスの構成を示す。従来は製造現場の制御システムに組み込まれていた制御コアを，クラウド型PLCのtypeN1に移行し，プログラム開発や，デバッグ作業，案件管理・問い合わせなどはテレワークで実施できる。計装クラウドサービスは，typeN1，typeN1の開発環境であるMeister nV-Tools Cloud，及び顧客システムの様々な機器情報やプログラムなどのデータを利活用するため

（注1） 我が国のIT国家戦略を技術面や人材面から支えるために設立された機関。

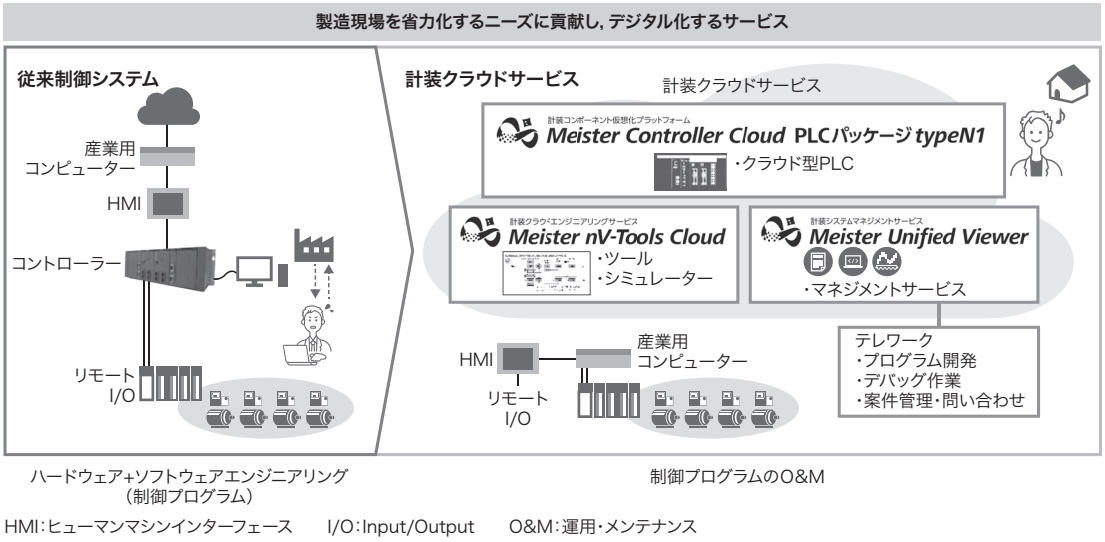


図1．計装クラウドサービス

計装クラウドサービスは，typeN1，Meister nV-Tools Cloud及びMeister Unified Viewerから構成される。

Differences between conventional OT system and instrumentation cloud service of digital manufacturing solutions

のデータ管理プラットフォームであるMeister Unified Viewerで構成される。これらの特長について，以下で述べる。

2.1　typeN1

クラウドシステムと製造現場をインターネットで接続し，クラウドシステム上でOTとITソリューションの連携を容易にするクラウド型PLCである。導入時にシステム運用を柔軟にするだけでなく，将来にわたって継続的な機能改善を実現する。

2.2　Meister nV-Tools Cloud

クラウド型PLCだけでなく，従来のハードウェアPLCにも対応するクラウドベースのエンジニアリング環境において，制御プログラムの開発だけでなくデバッグのためシミュレーション環境も提供している。

2.3　Meister Unified Viewer

コンポーネントベンダー，システムインテグレーター（SIer），EPC（Engineering, Procurement, Construction）コンストラクター，及び最終顧客の全てが，システムの製品ライフサイクルにおける技術・生産・品質情報を共有し利活用するための，データ管理プラットフォームである。

3．脅威分析

typeN1とMeister nV-Tools Cloudのセキュリティ対策を立案するにあたり，システムに内在する脅威とその影響度を把握する必要がある。脅威分析手法の種類とその特徴を**表1**に示す。typeN1の開発では，詳細リスク分析手法の一つでありIPAが推奨する“制御システムの資産ベースセキュリティリスク分析手法”を活用した。この手法では，システムを構成する資産に対する脅威と，そのリスク（影響度）を詳細に把握することが可能である。リスクに応じて対策に優先度付けを行うことにより，開発コストを有効活用したセキュリティ対策を立案した。

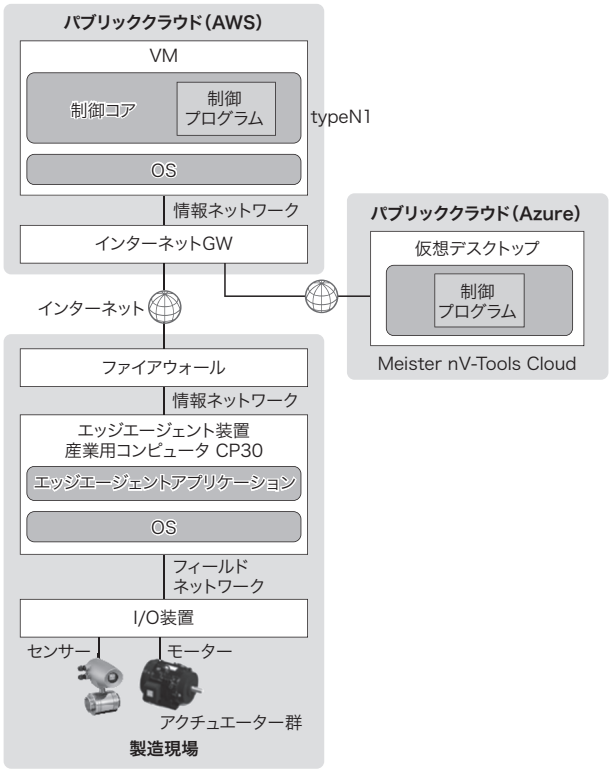
表1．制御システムの資産ベースの脅威分析手法の種類と特徴

Features of four asset-based security threat analyses for OT systems

手法名	分析方法	長所及び短所
ベースラインアプローチ	既存の標準や基準を基にセキュリティ対策要件を定め，自システムの対策の適合性をチェックする。	作業工数は少ないが，基本的には対策基準に対する適合レベルチェックであり，自システムの状況に沿ったリスク分析にはなっていない。
非形式的アプローチ	分析担当者の知識や経験によってリスク分析を実施する。	作業工数，精度ともに属人性が高いため，分析結果の判断が難しい。
詳細リスク分析	自システムの構成資産を重要度，脅威，脆弱（ぜいじゃく）性の評価指標に従って，リスク分析する。	自システムに対する正確なリスク分析が可能であり，セキュリティ投資の優先順位付けにも活用可能である。大きな作業工数が必要となる場合がある。
組み合わせアプローチ	上記のうちの複数の分析手法を併用し，作業の効率化，及び分析精度の向上を図る。	組み合わせ方法については指針が示されていないため，属人性が高い。

3.1　システム構成

typeN1とMeister nV-Tools Cloudのシステム構成を，**図2**に示す。PLCの制御プログラムを実行する制御コアはパブリッククラウド上のVM（Virtual Machine）に構築し，製造現場のアクチュエーターに制御信号を伝えるエッジエージェント装置は製造現場に設置された産業用コンピューターに構築する。制御コアとエッジエージェント装置は特定のペアで動作する構成となっている。Meister nV-Tools Cloud



OS：基本ソフトウェア　GW：ゲートウェイ

図2. 計装クラウドサービスにおける制御コアと製造現場の接続

パブリッククラウド上のtypeN1とMeister nV-Tools Cloudは，製造現場と一般のインターネット回線を介して接続されるため，従来の制御システムとはセキュリティ要件が異なる。

Connections between control core and devices at manufacturing site

表2. 資産に内在する高リスクの脅威の一覧

Lists of high-risk threats underlying in assets

環境		パブリッククラウド（AWS）		製造現場		パブリッククラウド（Azure）
資産		VM	情報ネットワーク	産業用コンピューター	情報ネットワーク	仮想デスクトップ
資産種別	機器	○		○		○
	ネットワーク		○		○	
重要度		2	2	2	2	2
脅威	不正アクセス	B	–	B	–	B
	物理的侵入	B	–	B	–	C
	不正操作	–	–	B	–	–
	過失操作	B	–	B	–	B
	不正媒体・機器接続	–	–	B	–	–
	プロセス不正実行	B	–	B	–	B
	マルウェア感染	B	–	B	–	B
	情報窃取	C	–	B	–	B
	情報改ざん	B	–	B	–	C
	情報破壊	B	–	B	–	C
	不正送信	B	–	B	–	–
	機能停止	B	–	B	–	B
	高負荷攻撃	B	–	–	–	B
	窃盗	–	–	B	–	–
	盗難・廃棄時における情報の搾取	C	–	B	–	C
	経路遮断	–	C	–	C	–
	通信輻輳（ふくそう）	–	B	–	B	–
	無線妨害	–	–	–	B	–
	盗聴	–	B	–	B	–
	通信データ改ざん	–	B	–	C	–
	不正機器接続	–	B	–	B	–

は，パブリッククラウド上の仮想デスクトップに構築される。各パブリッククラウド，製造現場間はインターネット回線を介して接続される。

3.2　脅威分析

IPAの脅威分析手法によるtypeN1を構成する資産に内在する高リスクの脅威の一覧を**表2**に示す。資産ベースのリスク分析におけるリスク値はAからEの5段階のレベルで評価され，Aが最もリスクが高く，Eは最もリスクが低い。リスク値が高いという分析結果は，重要な資産において発生する脅威に対する対策が不十分であることを意味している。資産の重要度は3段階で評価され，3で重要度が最も高いことを示す。重要度2は，例えばシステム停止により製造停止や社会の混乱を招くようなものではなく，製造能力の低下を与えるようなレベルを示している。

パブリッククラウドであるAWS[注2]の環境では，一般のインターネット回線を利用するため，不特定多数からアクセス可能であり，不正アクセス，高負荷攻撃，マルウェア感染のリスクが高いと判断した。制御コアの不正利用，情報改ざん，機能停止などの攻撃は製造現場での製造不良や稼働率低下を招くため，顧客事業への影響を勘案し，リスクが高いと判断した。

製造現場では，インターネット回線に接続するリスクに加え，物理的侵入や窃盗など第三者による物理的な攻撃に対するリスクも高いと判断した。特定の制御コア以外と接続することにより，製造設備の不正利用（破壊を含む）の危険もあるため，不正アクセスのリスクは高いと判断した。また，製造現場に接続される情報ネットワークへのアクセスが容易な場合，情報漏洩（ろうえい）につながる盗聴攻撃はリスクが高い。

パブリッククラウドであるAzure[注3]の環境では，Meister nV-Tools Cloudからクラウド型PLCの不正停止指令を送ることによる稼働率低下や，不正な制御プログラムをダウン

（注2） Amazon社が提供するクラウドコンピューティングサービスの総称。

（注3） Microsoft社が提供するクラウドコンピューティングサービスのプラットフォーム。

ロードさせることによる製造不良を引き起こすため，機能停止，プロセス不正実行のリスクが高いという結果であった。

4. セキュリティ対策

typeN1は，3章で述べた脅威分析の結果とゼロトラストアーキテクチャーに基づいてセキュリティ対策を実施した。ゼロトラストは，NIST（米国国立標準技術研究所）のSpecial Publication 800-207[2]に示されているシステム設計の概念である。ネットワークが侵害されている場合にも，リクエストごとに正確かつ最小限のアクセス権限を与えられるようにシステムを設計することをいう。以下に，typeN1におけるセキュリティ対策の特長とその詳細について述べる。

4.1 typeN1のセキュリティ対策の特長

typeN1のセキュリティ対策における特長を以下で述べる。

4.1.1 ゼロトラストの考え方の採用

近年，攻撃手法の多様化や，社内ネットワークが初期感染源となるインシデントの増加などから，企業内ネットワークを信用しない考え方に移行しつつある。OTシステムではシステム停止時の影響が甚大なことから，システム全体への波及を防ぐためゼロトラストの考え方が浸透していくと考えられる。ゼロトラストでは，ネットワークの場所によらない全ての通信の保護や，リソースへのセッション単位での動的な認証・認可制御，デバイスとアプリケーションの整合性及びセキュリティ動作の監視などが求められており，クラウド型PLCはこれらの要件に合致するよう設計されている。

4.1.2 可用性とゼロトラストの両立

ゼロトラストアーキテクチャーの実現例では，脆弱（ぜいじゃく）性による不正侵入を防止するため，パッチの即時適用が要素技術とされている。一方でOTシステムでは可用性要件から，即時のシステム停止を伴うパッチ適用が難しいことが多い。そこで，可用性を損なわずに脆弱性による不正侵入を防ぐホワイトリスト型の実行制御対策を導入しており，パッチ適用までの安全性を担保している。

4.1.3 ゼロトラストでの継続運用

ゼロトラストでは，セキュリティ脅威の変化などに柔軟に対応できるように，運用開始後も柔軟な運用時対策が求められる。typeN1もログ監視や脆弱性監視などにより，継続的に安全性を担保できるセキュリティ運用を実現している。

4.2 対策の詳細

typeN1では前節で述べた特長を実現するために，**図3**

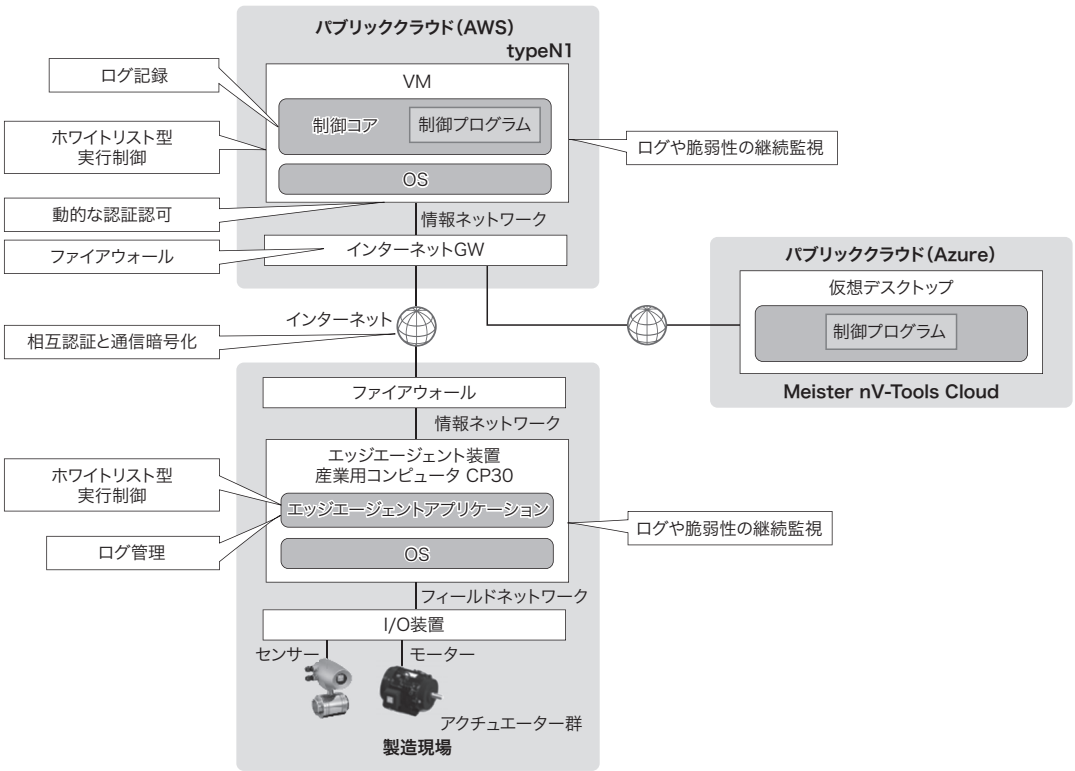


図3. 導入した主要なセキュリティ対策

脅威分析結果とゼロトラストアーキテクチャーに基づきセキュリティ対策を実施した。

Main security measures implemented in instrumentation cloud service

及び以下に示すセキュリティ対策を導入した。

4.2.1　機器間の相互認証と通信暗号化

クラウド型PLCでは，クラウドシステム又は製造現場などの設置場所や，サーバー又はクライアントといった役割で区別することなく，通信相手をmTLS（mutual Transport Layer Security）によって相互認証する。これにより不正アクセス，情報改ざん，ネットワーク盗聴などの脅威に対応する。また，クラウドシステム側ではファイアウォールを導入し，DDoS（Distributed Denial of Service）攻撃を含む想定しない相手からの通信を遮断している。

4.2.2　関与者の役割細分化と認可ポリシーの決定

クラウド型PLCでは，システムを運用する際に，顧客や，クラウド運用者，メンテナンス実施者など，システム運用に携わる関与者を細分化して，それぞれの関与者に対して必要最低限となるように認可ポリシーを定義した。

4.2.3　ポリシー変更の動的な変更への対応

PKI（Public Key Infrastructure）に基づく証明書の無効化による認証ポリシーの変更，及び権限情報の変更による動的な認可ポリシーの変更が可能な仕組みとなっており，万一，鍵漏洩などの情報窃取の脅威が発生した際にも対応できる。

4.2.4　アプリケーション実行時の整合性確認

OTシステムでは可用性要件から脆弱性が見付かった場合にも即座にパッチが適用できない場合がある。パッチ適用までの間に脆弱性を悪用されることを防ぐため，ホワイトリスト型の実行制御技術[3]によりアプリケーションの整合性を確認することでプロセス不正実行やマルウェア感染の脅威から保護している。

4.2.5　製造現場・クラウドシステム双方での認証などのログ記録

製造現場側では認証ログ，アプリケーションの整合性異常を保存し，クラウドシステム側にも認証ログなどを保存する。

4.2.6　記録されたログや脆弱性の継続的監視

記録したログは定期的に監視する運用とした。また，脆弱性は開発時だけでなく，運用開始後もSBOM（Software Bill of Materials）に基づいて確認する仕組みとしている。

5. あとがき

東芝グループはスマートマニュファクチャリングを推進するために，typeN1を中核とした制御システムを提供している。制御コア及びエッジエージェント装置がインターネットを介して接続され，インターネット及び情報ネットワークでのセキュリティ対策が必要なことからtypeN1は，従来の境界型防御のアーキテクチャーから，より積極的なゼロトラストのセキュリティアーキテクチャーとした。継続してセキュリティ脅威の変化などに柔軟に対応できるように，運用開始後も柔軟な運用時対策を含め将来にわたりセキュアにサービス提供可能にした。今後も，ITとOTが持続的かつセキュアに適用可能な計装クラウドサービスを提供していくとともに，工場の生産性や品質だけでなく労働者の安全性の向上にも貢献していく。

文　献

⑴ 深井英五，ほか．製造現場とITをつなぐOTコンポーネント．東芝レビュー．2024，**79**，4，p.15–21．<https://www.global.toshiba/content/dam/toshiba/jp/technology/corporate/review/2024/04/a05.pdf>，（参照 2025-06-05）．

⑵ NIST. Special Publication 800-207. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>, (accessed 2025-04-09).

⑶ 春木洋美，ほか．インフラの安心・安全な長期運用を支える制御システムセキュリティ技術．東芝レビュー．2018，**73**，5，p.11–14．<https://www.global.toshiba/content/dam/toshiba/migration/corp/techReviewAssets/tech/review/2018/05/73_05pdf/a04.pdf>，（参照 2025-06-05）．

深井　英五　FUKAI Eigo
スマートマニュファクチャリング事業部 計装技術部
計測自動制御学会会員
Instrumentation & Control Equipment Engineering Dept.

天木　　智　AMAKI Satoru
総合研究所 インフラシステムR&Dセンター
システム制御・ネットワーク技術開発部
電気学会・情報処理学会会員
System Control and Network R&D Dept.

金井　　遵　KANAI Jun, D.Eng.
総合研究所 AIデジタルR&Dセンター セキュリティ基盤研究部
博士（工学）
情報処理学会・電子情報通信学会会員
Security Research Dept.

伊東　　雄　ITO Yu
スマートマニュファクチャリング事業部
計測制御機器部
Microelectronics System Components Dept.