OPC UA 移行ホワイトペーパー

OPC Classic から OPC UA への移行、確認、導入後運用の実務ガイド

独立行政法人情報処理推進機構　産業サイバーセキュリティセンター
中核人材育成プログラム 9 期生
「OPC UA 移行の課題整理と推進アプローチ」プロジェクト

はじめに

OPC UA 移行は、単なる通信規格更新ではない

Open Platform Communications：「OPC」は、製造現場の設備やシステムの間でデータを受け渡すために使われてきた仕組みです。なかでも OPC Classic、特に OPC DA（1996 年～）は、当時乱立していたベンダー独自プロトコルを統一する規格として広く普及し、長年にわたり、監視、記録、データ収集、上位システムとの連携などを支えてきました。

一方で、OPC Classic は、通信基盤として Windows の古い通信の仕組み（COM/DCOM）に強く依存しています。これは、OS 更新、サーバ更新、ベンダー保守期限などの影響を受けやすいという保守性の問題にとどまりません。セキュリティの面で、次のような構造的な弱点を抱えています。

- プロトコル自体に、暗号化・署名・認証の仕組みがない。通信の保護はすべて DCOM 任せであり、ネットワーク越しでは十分な安全性を確保することが難しい
- DCOM は動的にポートを割り当てるため、ファイアウォールを通しにくい。認証設定（DCOM 設定）も複雑で、トラブルの温床になりやすい
- その結果、現場では、通信を成立させるために「設定を緩めて動かす」運用が採られる場合がある。つまり、つながらない問題を、セキュリティを下げることで解決していることになる

これらは、設定や運用の工夫で後から解消できる種類の問題ではありません。OPC Classic の土台そのものに由来する限界です。

OPC UA は、セキュリティを前提に設計し直された規格である

OPC UA は、まさにこの限界を解消するために作られました。先に挙げた OPC Classic の 3 つの弱点は、OPC UA では次のように解消されています。

- プロトコル自体に、暗号化・署名・認証の仕組みが最初から組み込まれている。通信の保護を DCOM など外部の仕組みに頼る必要がなく、ネットワーク越しでも安全に通信できる
- COM/DCOM に依存せず、あらかじめ決めた 1 つのポートで通信するため、ファイアウォールを通しやすい。Windows 以外の機器・OS でも実装できる
- その結果、セキュリティを確保したまま接続できるため、「設定を緩めて動かす」運用に頼る必要がない

つまり OPC UA は、OPC Classic に後からセキュリティを足したものではなく、「OPC Classic の土台ではセキュリティを確保しにくい」という反省に立って、セキュリティを前提に設計し直された仕組みです。

DX は、通信の性質を変える

この違いが決定的に重要になるのが、DX 推進の場面です。DX では、製造現場のデータを現場の中だけで閉じさせず、共有サーバ、上位システム、全社ネットワーク、クラウドへつないで活用することが前提になります。つまり、これまで「閉じた現場ネットワークの中にあるから守られていた」通信が、境界をまたいで外とつながる通信へ変わっていきます。

閉じたネットワークの中で完結している接続であれば、OPC Classic を使い続けること自体が直ちに危険とは言えません。ただし、その場合でも、運用管理や境界防御などの対策は引き続き必要です。一方、暗号化も認証もない通信を、データ共有のために境界をまたいで通すことは、リスクの性質がまったく異なります。接続相手を確認できず、通信内容を保護できず、誰が何を読み書きしたかを説明できないまま、現場データへの入り口を外に向けて開くことになるからです。

したがって、本書の立場は次の通りです。すべての接続を直ちに OPC UA へ置き換える必要はありません。しかし、共有部との通信、上位システムとの連携など、ネットワーク境界をまたぐ接続は、「余裕ができたら移行を考える」対象ではなく、セキュリティ上の必要性から優先的に OPC UA へ更新すべき対象です。

ただし、OPC UA にすれば自動的に安全になるわけではありません。設定した理由、接続を許可する相手、権限、ログ、変更時の確認、例外的に認めた設定などを、導入後も管理する必要があります。OPC UA は、安全を自動的に保証するものではなく、安全に運用しやすい構成へ近づけるための仕組みとして理解することが重要です。

なお、移行の契機は DX に限りません。Windows やサーバの更新、設備更新、ベンダー保守期限などをきっかけに、OPC UA への移行を検討するケースも増えています。

本書では、OPC UA 移行を、単なる通信規格の更新ではなく、セキュリティリスクを下げられるか、保守を続けられるか、OS 更新に対応できるか、障害時に復旧できるか、データ活用の基盤として使い続けられるかを見直す取り組みとして扱います。

いま問題になりやすいこと

OPC UA が登場してから約 20 年が経過しました。それでも、多くの製造現場では OPC DA を含む OPC Classic が使われ続けています。

長年安定して動いているシステムは、簡単には止められません。設備更新の時期、操業への影響、ベンダー対応、保守契約、周辺システムとの関係を考えながら判断する必要があります。

問題になるのは、OPC Classic が残っていることそのものではなく、次のような状態です。

- どこで OPC が使われているか分からない
- どこに OPC Classic が残っているか分からない
- OPC Classic の通信が、閉じたネットワークの中に収まっているのか、共有部や上位ネットワークへ出ているのか分からない
- 止まった場合に、どの業務や設備に影響するか分からない
- 設定を分かる人や、復旧できる人が限られている
- OS 更新や設備更新のときに、同じ接続状態へ戻せるか分からない
- 誰が、どの範囲で、どのデータを読み書きできるか説明できない
- ログや設定根拠を確認できない

特に 3 点目は重要です。境界をまたぐ接続に OPC Classic が残っていれば、それは保護されていない通信が外とつながっている状態であり、DX を進めるほどリスクが大きくなります。

加えて、海外拠点、輸出設備、グローバル顧客向け案件、サプライチェーン上のセキュリティ確認では、単に「通信できているか」だけでなく、どの接続が、どの相手と、どの範囲で、どのような管理状態にあるのかを説明できることが求められます。海外のサイバーセキュリティ関連制度や顧客要求は、OPC UA の導入そのものを一律に義務づけるものではありませんが、接続相手、通信保護、認証、権限、ログ、脆弱性対応、保守性、説明責任を求める流れは強まっています。

そのため、まず必要なのは「すぐにすべてを OPC UA へ置き換えること」ではありません。自社のどこで OPC が使われているかを把握し、境界をまたぐためにセキュリティ上優先して移行すべき接続、当面残してよい接続、次の更新時に見直す接続を、リスクに基づいて区別し、説明できる状態にすることです。

本書は、OPC UA への一括移行を急がせる資料ではありません。また、OPC Classic を使い続けている現場を否定する資料でもありません。ただし同時に、リスクの高い接続の見直しを先送りしてよいと伝える資料でもありません。製造現場が自社の接続状態を把握し、守るべき接続から優先的に OPC UA へ移行し、関係者や経営層へ説明し、導入後も管理を続けられるようにするための実務ガイドです。

目次

はじめに 2
OPC UA 移行は、単なる通信規格更新ではない 2
OPC UA は、セキュリティを前提に設計し直された規格である 2
DX は、通信の性質を変える 3
いま問題になりやすいこと 4
目次 6
第 1 章　本書の目的と使い方 11
1.1 本書を作成した背景 11
本書でいうシステムの「上位」と「下位」 12
1.2 本書の目的 13
1.3 本書の対象読者 13
1.4 本書で扱うこと 14
1.5 本書のスタンスと解いておきたい誤解 14
1.6 本書の読み進め方 15
1.7 本文と付録の関係 15
1.8 参考資料、検証結果、法規制・顧客要求の扱い 16
1.9 次章へのつながり 17
第 2 章　背景と問題意識 18
本章で分かること 18
2.1 OT/IT 連携の拡大と製造現場を支える OPC 18
2.2 OPC Classic 継続利用における課題 19
2.3 OPC Classic 継続利用がシステム全体のセキュリティに与える影響 20
2.4 OPC Classic 継続利用を経営判断につなげる観点 21

2.5 本章のまとめ 21
第 3 章　Classic と UA の違い 22
本章で分かること 22
3.1 Classic と UA の網羅的比較 22
3.2 リスクアセスメント結果 24
3.2.1 分析アプローチと評価軸 24
3.2.2 分析対象システム構成 24
3.2.3 分析結果 – Classic 継続利用と UA 移行のリスク比較 25
3.2.4 分析結果の総括 26
3.3 本章のまとめ 27
付録との関係 28
第 4 章　なぜ移行が進まないのか 28
本章で分かること 28
4.1 本章の使い方 28
4.2 移行停滞をもたらす 4 つの根本要因 28
4.3 実務者が直面する「9 つのつまずきポイント」 29
4.4 本章のまとめ 30
付録との関係 31
第 5 章　OPC UA 移行の事業上の効果と投資判断 31
本章で分かること 31
5.1 本章の目的と使い方 32
5.2 経営層へ説明する 4 つの論点 33
5.3 稟申時に提示すべき判断材料 35
5.4 経営層向け説明例 37
5.5 成立条件と残るリスク 38
5.6 本章のまとめ 39

付録との関係 40
第 6 章　移行に必要な作業 40
本章で分かること 40
6.1 移行作業の全体像 41
6.2 接続台帳で確認する項目 41
6.3 移行成立性の確認 42
6.4 Gateway/Wrapper を入れた後も確認すべきこと 43
6.5 移行前に最低限決めておくこと 44
6.6 本章のまとめ 44
付録との関係 44
第 7 章　移行方針の決め方 45
本章で分かること 45
7.1 なぜ今、移行を考えるべきなのか 45
7.2 全体の進め方 46
7.3 A/B/C 分類で優先順位を付ける 56
7.4 移行のきっかけとなるイベント 56
7.5 移行方式の選び方 57
7.6 関係者と役割の整理 58
7.7 本章のまとめ 58
第 8 章　移行前後の確認事項 59
本章で分かること 59
8.1 本章の目的と使い方 59
8.2 確認対象を決める 61
8.3 接続の把握 62
8.4 Classic 残置の把握 63
8.5 移行成立性の確認 64

8.6 Gateway/Wrapper 利用時の確認 65
8.7 導入直後の受入確認 66
8.8 変更時の確認 68
8.9 本章のまとめ 69
付録との関係 69
第 9 章　導入後の継続運用 70
本章で分かること 70
9.1 本章の目的 70
9.2 導入後に維持すべき管理情報 71
9.3 設定根拠の管理 72
9.4 証明書・Trust List の管理 73
9.5 認証・権限・書き込み管理 74
9.6 ログ・監視・確認先の管理 75
9.7 変更管理 76
9.8 例外管理 77
9.9 定期レビュー 78
9.10 第 8 章から第 9 章への引き継ぎ 80
9.11 本章のまとめ 80
付録との関係 80
第 10 章 模擬プラント検証から得られた運用・設定の注意点 81
本章で分かること 81
10.1 検証の位置づけ 81
10.2 検証設計の枠組み——何を変えて、何を見たのか 82
10.3 検証結果サマリー—設定別の防御成否マトリクス 83
10.4 証明書自動受け入れ——もっとも見落とされやすい落とし穴 85
10.5 DoS 攻撃——OPC UA 単体では守り切れない領域と、その対処方針 86

10.6 Anonymous 認証の扱い——なぜ「閉域だから大丈夫」が通用しないのか 88
10.7 設定項目別の運用観点と検証から見えた論点 89
10.8 検証から導かれた 5 つの教訓 90
10.9 本章のまとめ 91
付録との関係 92
第 11 章　まとめ 92
11.1 本書の要点 92
11.2 本文・付録・Excel 版の使い分け 93
11.3 実務での進め方 93
11.4 最後に 93
謝辞 94
プロジェクトメンバー 94
付録　実務テンプレート 95
付録 A　接続・移行確認表 96
付録 B　運用管理表 97
付録 C　変更・例外・定期レビュー表 97
別紙 Excel 版について 98
用語集 98
巻末参考資料一覧 102
商標について 104

第 1 章　本書の目的と使い方

本章では、本書を作成した背景、目的、対象読者、扱う範囲、前提としないこと、読み進め方を整理します。

「はじめに」では、本書の結論と全体像を先に示しました。本章では、それを受けて、本書がどのような立場で、誰に向けて、どこまでを扱う資料なのかを整理します。

1.1 本書を作成した背景

OPC UA Version 1.0 が利用可能になってから、約 20 年が経過しました。それでもなお、多くの製造現場では、OPC Classic、特に OPC DA を利用したシステムが残り続けています。

これらのシステムは、長年安定して稼働してきたからこそ、簡単には止められません。設備更新のタイミングが限られること、周辺システムとの接続関係が見えにくいこと、古い OS やソフトウェア、ベンダー保守、担当者の属人化が絡み合っていることなどから、OPC UA への移行は必要性が語られても、具体的な計画に進みにくいのが実情です。

一方で、製造現場を取り巻く環境は変化しています。製造データの活用、制御運用技術（Operational Technology ：「OT」）と情報技術（Information Technology：「IT」）の連携、上位システムへのデータ連携、セキュリティ対策、OS 更新、サーバ更新、顧客要求への対応などにより、製造システムの接続状態や設定根拠を説明する場面は増えています。

また、欧州サイバーレジリエンス法（EU Cyber Resilience Act：「CRA」）などに見られるように、サイバーセキュリティ対策や脆弱性対応に関する要求は高まりつつあります。CRA は、ネットワークにつながる製品などに対し、サイバーセキュリティ対策や脆弱性対応を求める欧州の規制です。これは、OPC UA の導入そのものを一律に義務づけるものではありません。しかし、接続相手、通信保護、認証、権限、ログ、設定根拠を説明できる構成へ見直す必要性を高めています。

本書は、このような問題意識から作成しました。

本書でいうシステムの「上位」と「下位」

OPC は、製造現場の機器やシステム間でデータを受け渡すために使われる通信規格です。図 1-1 は、制御系ネットワークの中で OPC サーバがどこに位置し、どの方向にデータを連携しているかを示した例です。一般に、OPC サーバは、PLC やコントローラなどの現場機器から取得したデータを、監視・制御システムやデータ収集システム、生産管理システムなどへ渡す接続点に位置します。本書では、説明を分かりやすくするため、図 1-1 の OPC サーバから見て、データを利用する側を「上位システム」と呼びます。一方、PLC、コントローラ、センサー、バルブ、ポンプなど、設備や現場機器に近い側を「下位側」または「フィールド側」と呼びます。なお、実際の配置はシステム構成により異なるため、図 1-1 は代表的な連携イメージとして示しています。

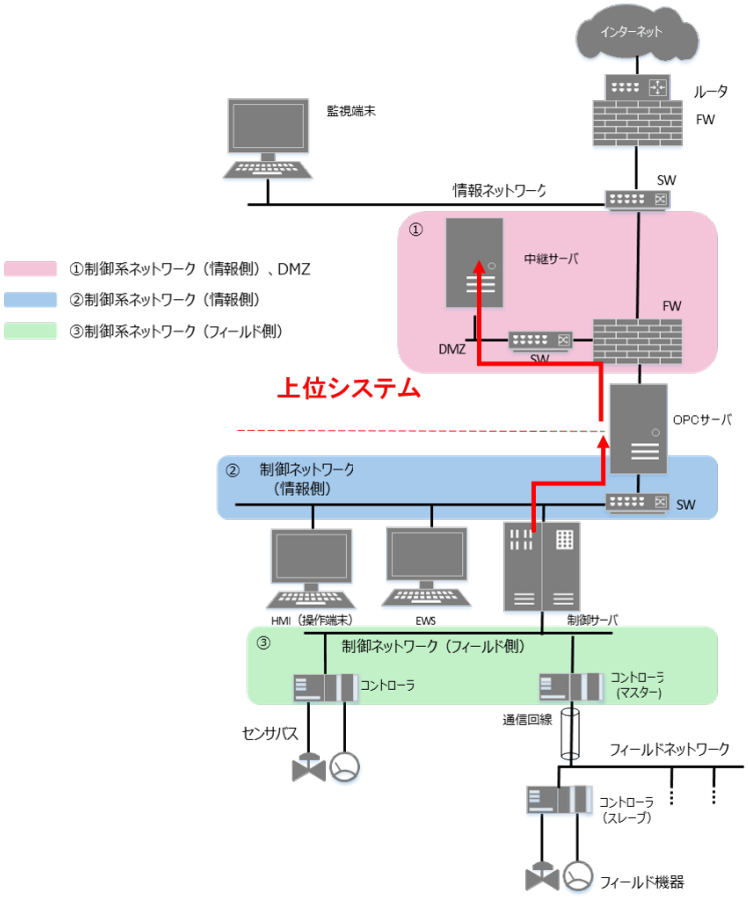


図 1-1　制御系ネットワークにおける OPC サーバのシステム連携概要図 [1]

[1] 制御システムのセキュリティリスク分析ガイド 第 2 版（IPA）を基に作成
https://www.ipa.go.jp/security/controlsystem/ug65p90000019bkg-att/begoj9000000hpm8.pdf

1.2 本書の目的

本書の目的は、OPC Classic、特に OPC DA を利用している現場が、現状を確認し、OPC UA への移行要否や優先順位を検討し、関係者や経営層へ説明できるようにすることです。

本書では、OPC UA 移行を、単なる通信規格の更新ではなく、保守継続性、OS 更新対応、障害復旧性、システム全体のセキュリティ、データ活用基盤を見直す取り組みとして扱います。

ここでいう移行とは、すべての接続を一度に OPC UA へ置き換えることだけを意味しません。新規システムの導入や既存システムの全面刷新では、将来の保守継続、接続管理、認証・権限管理、ログ確認、データ連携を見据え、OPC UA を前提に検討することを推奨します。一方で、既存設備や既存システムでは、設備更新のタイミング、ベンダー対応状況、操業影響、保守期限などの制約により、当面は OPC Classic を残す判断もあり得ます。重要なのは、残すこと自体を否定するのではなく、なぜ残すのか、いつまで残すのか、どのリスクを受け入れているのか、どのタイミングで見直すのかを説明できる状態にすることです。

本書では、移行前の確認、段階的な移行方式、Gateway や Wrapper（詳細は第 7 章参照）を利用する場合の注意点、移行前後の確認事項、導入後の維持管理を、現場で使える形で整理します。

1.3 本書の対象読者

本書は、OPC Classic、特に OPC DA を利用している、または利用状況を確認する立場にある製造現場の関係者を主な対象とします。

会社によって部門名や担当範囲は異なります。そのため、本書では特定の部署名ではなく、次のような役割を持つ読者を想定します。

読者・関係者	本書での主な関心
製造現場の状況を把握している人	OPC 接続が止まった場合の操業影響、監視、記録、帳票、操作への影響を把握したい。
設備、計装、保全に関わる人	設備更新、端末更新、OS 更新、保守期限、障害対応と OPC 接続の関係を整理したい。
工場内のシステムやネットワークに関わる人	サーバ、端末、ネットワーク、上位システム、OPC 製品、Gateway/Wrapper を含む接続関係を把握したい。
製造、設備、システムに関わる管理者	OPC UA 移行の必要性、優先順位、投資判断、関係者への説明材料を整理したい。
情報システムやセキュリティに関わる人	OS 更新、ネットワーク分離、認証、ログ、変更管理との関係を確認したい。

読者・関係者	本書での主な関心
ベンダー、システム構築・保守を支援する委託先	ユーザ側が確認したい情報、責任分界、移行時に必要な確認事項を把握したい。

本書は、OPC UA の詳細仕様を理解している技術者だけを対象にしたものではありません。OPC や Windows の通信設定に詳しくない読者でも読み進められるよう、必要な箇所で短い説明を加えます。

1.4 本書で扱うこと

本書は、製造現場が OPC UA 移行を検討するための実務ガイドです。製品別の導入手順書や、個別案件の設計書ではありません。

本書では、主に次の内容を扱います。

- OPC UA 移行の必要性を、保守継続性、OS 更新、障害復旧、セキュリティ、データ活用の観点から整理すること
- OPC Classic（特に OPC DA）の継続利用で生じやすい課題を整理すること
- 接続元、接続先、用途、通信方式、停止影響、保守期限、書き込み有無など、接続単位で確認すべき観点を整理すること
- Gateway や Wrapper を利用する場合の確認観点を整理すること
- 段階移行、優先順位付け、移行方式選定の考え方を示すこと
- 移行前、OPC Classic を残す場合、Gateway や Wrapper を利用する場合、導入直後、変更時の確認事項を整理すること
- 導入後に維持すべき管理項目を整理すること
- 関係者や経営層への説明に使える論点を整理すること
- 付録として、確認・記入に使えるチェックリストや台帳テンプレートを示すこと

1.5 本書のスタンスと解いておきたい誤解

本書では、次のような前提を取りません。

- OPC UA に移行すれば、自動的に安全になる
- OPC UA に移行すれば、OS 更新やサーバ更新の影響を受けなくなる
- Gateway や Wrapper を導入すれば、OPC Classic に由来するリスクが解消する
- すべての OPC Classic 利用は、危険であり、直ちに廃止すべきである
- すべての接続を一度に OPC UA へ全面更新すべきである

- 特定製品の既定値や推奨設定を、すべての環境に共通するものとして扱える
- 本書だけで法規制の適用可否や法的義務を判断できる

これらの前提を置かない理由は、製造現場の構成、設備更新時期、ベンダー対応状況、保守契約、操業影響、社内規程、顧客要求が現場ごとに異なるためです。

本書では、OPC UA 移行を一律の正解として示すのではなく、各現場が自社の状況を確認し、自分事として移行、残置、段階移行、導入後運用を説明できる状態にすることを重視します。

1.6 本書の読み進め方

本書は、最初から順に読んでも、目的に応じて必要な章から読んでも使える構成にしています。

目的	主に参照する章
移行の必要性や背景を理解する	第 2 章～第 4 章
関係者や経営層へ説明する	第 5 章
現状を確認する	第 6 章
移行方式や優先順位を決める	第 7 章
移行前後の確認・導入後の維持管理を行う	第 8 章～第 9 章
検証結果から注意点を確認する	第 10 章
実際に記入・確認する	付録

最初にすべての接続を完璧に調べる必要はありません。まずは、止まると困る接続、更新時期が近い接続、上位システムやデータ活用に関係する接続など、代表的な接続を数件選び、関係者に確認するところから始めてください。

詳細な進め方は第 6 章で扱います。

1.7 本文と付録の関係

本文では、OPC UA 移行を検討するための考え方、確認観点、判断軸を説明します。付録では、本文で説明した内容を、読者が実際に記入・確認できる最小限の形式に落とし込みます。

本書の付録は、すべての項目を最初から完全に記入することを求めるものではありません。まずは付録 A「接続・移行確認表」を使い、代表的な OPC 接続を 3 件程度選んで、接続元、接続先、用途、通信方式、書き込み有無、Classic/DCOM 残置、停止影響、確認先を記録してください。

付録 A は、第 6 章の棚卸し、第 7 章の A/B/C 分類、第 8 章の実務確認につながります。付録 B「運用管理表」は、第 10 章で扱う証明書、Trust List（信頼する証明書や発行元の一覧）、Anonymous（匿名接続）、証明書自動受け入れ、Security Policy などの確認観点を、第 9 章の導入後運用へ引き継ぐために使用します。付録 C「変更・例外・定期レビュー表」は、OS 更新、証明書更新、設備更新、Gateway/Wrapper 変更、例外設定、定期レビューを管理するために使用します。

また、各社の実務で利用しやすいように、別紙 Excel 版として「01_OPC_UA 接続・運用管理台帳」を主たる参考テンプレートとして提供します。Excel 版は、本文付録 A〜C と同じ考え方をもとに、記入欄や入力候補を詳細化したものです。必要に応じて、「02_資産管理台帳」「03_証明書管理台帳」「04_UA 環境構築チェックリスト」を任意の詳細版として併用できます。各社の既存の資産管理表、変更管理表、保守記録、セキュリティ管理ルールに合わせて、列の追加、削除、名称変更、シート分割、既存台帳への転記を行って構いません。

重要なのは、台帳を増やすことではなく、必要なときに「どの接続が、何のためにつながっているか」「どこに Classic/DCOM が残っているか」「なぜその設定にしたか」「誰が承認し、いつ見直すか」を説明できる状態にすることです。

1.8 参考資料、検証結果、法規制・顧客要求の扱い

本書では、公開済みの公式資料、公的機関の資料、ベンダー公開資料を参考にします。本文では、それらを要約・解説する形にとどめ、図表、製品画面、写真、長文をそのまま転載することはしません。

また、本書では、公開資料による一般論、プロジェクト固有の検証結果、そこから得られる示唆を区別して扱います。特に、第 10 章で扱う模擬プラント検証は、すべての製造現場構成を完全に再現したものではありません。検証結果をそのまま全現場に一般化するのではなく、OPC Classic と OPC UA が混在する構成で見落としやすい確認観点を抽出する材料として扱います。

法規制や顧客要求については、OPC UA 移行を自動的に義務づける根拠としてではなく、判断を補助する材料として扱います。たとえば CRA のような規制についても、OPC UA 導入そのものを求めるものとしてではなく、接続状態や管理状況を説明する必要性を高める外部要因の一つとして位置づけます。出発点になるのは、自社の実態です。どこに OPC Classic が残っているのか、それが止まった場合にどの業務へ影響するのか、保守期限や復旧体制に不安

はないか、ログや権限を説明できるかを整理したうえで、法規制や顧客要求を判断材料の一つとして位置づけます。

個別案件における法的義務や適用可否は、本書だけで判断せず、社内の関係部門や専門家と確認してください。

1.9 次章へのつながり

本章では、本書を作成した背景、目的、対象読者、扱う範囲、前提としないこと、読み進め方を整理しました。

次章では、なぜ OPC UA 移行を単なる通信規格更新ではなく、保守継続性、OS 更新対応、障害復旧性、システム全体のセキュリティ、データ活用基盤の見直しとして考える必要があるのかを整理します。製造現場で OPC がどのように使われてきたのか、OPC Classic を使い続ける場合にどのような課題が生じやすいのかを確認し、第 3 章以降の比較、移行停滞要因、経営説明、棚卸し、段階移行へつなげます。

第 2 章　背景と問題意識

本章で分かること

なぜ OPC UA 移行を考える必要があるのかを、製造現場を取り巻く環境変化と、OPC Classic 継続利用時に生じやすい課題から整理します。

2.1 OT/IT 連携の拡大と製造現場を支える OPC

製造現場では、PLC・DCS・SCADA・HMI・ヒストリアンなどを通じて、多様なデータが日々生成・蓄積されています。これらのデータは従来、監視制御、現場改善、保全対応など、主として OT 領域の中で利用されてきました。

製造現場のデータ連携には、機器メーカー独自の通信、フィールドネットワーク、産業用 Ethernet、データベース連携、ファイル連携など、目的や階層に応じてさまざまな方法があります。その中で OPC は、産業オートメーション分野において、異なるベンダーの機器やソフトウェア間でデータ交換を行いやすくするための標準仕様群として、長く利用されてきました。製造現場では、PLC・DCS・SCADA・HMI などの制御系システムや、ヒストリアンなどの監視・情報系システムの間で、プロセスデータを受け渡すためのインターフェースの一つとして広く採用されています。ベンダーや機器の違いを越えたデータ連携を支える手段の一つとして、OPC は多くの現場でデータ連携基盤の一部を担ってきました。

本書では、このうち Microsoft の COM/DCOM を基盤とする従来型の規格群、すなわち OPC DA、OPC A&E、OPC HDA を総称して「OPC Classic」と表記します。OPC Classic は、Windows の COM/DCOM 技術を利用して、OPC Client と OPC Server が標準的にデータ交換できるようにした仕組みです。COM/DCOM は Windows 上のアプリケーション同士を連携させる技術で、ネットワーク越しの接続では権限やファイアウォールの設定も関わってきます。

OPC Classic は、豊富な対応製品と運用実績を背景に、多くの現場で利用されてきました。一方で、OPC を取り巻く環境は変化しています。製造業では、生産性向上、データに基づく業務改善、サプライチェーンの強化などを目的として、デジタル技術や IoT を活用する取り組みが進んでいます。これに伴い、設備や制御システムで生まれる OT データを、製造実行システム（Manufacturing Execution System：「MES」）、企業資源計画（Enterprise Resource Planning：「ERP」）、分析基盤などの IT 領域でも活用したいという要請が高まっています。こうした変化により、OPC に期待される役割も広がっています。

表 2-1 OPC に求められる役割の変化

これまで OPC が担ってきた主な役割	現在求められる追加的な観点
現場システム間でデータを受け渡す	接続元・接続先、通信経路を把握する
監視・制御に必要なデータを安定して届ける	必要な相手に、必要な範囲でデータを届ける
ベンダーや機器が異なってもデータ連携できるようにする	接続できる相手や操作できる範囲を管理する
現場内の安定稼働を支える	上位システムや IT 領域との連携を前提に維持・更新する

OPC UA は、OPC Classic で扱われてきたデータアクセス、アラーム・イベント、履歴データなどの考え方を引き継ぎながら、UA ネイティブな通信では COM/DCOM を前提としない、プラットフォーム非依存の産業用通信仕様として策定されました。また、通信保護、認証、権限管理などを仕様として扱える点が、OPC Classic との大きな違いで、第 3 章で詳しく扱います。

2.2 OPC Classic 継続利用における課題

OPC Classic を使い続けること自体が、直ちに問題になるわけではありません。ただし、従来構成のまま運用を続けると、OS 更新やネットワーク変更時の影響確認、COM/DCOM に起因する設定管理、保守期限への対応、セキュリティ要件との整合などが、運用負荷やリスクとして顕在化する場合があります。

表 2-2 OPC Classic 継続利用における主な問題点

問題点	概要	詳細を扱う章・節
COM/DCOM への依存	OPC Classic は Windows の COM/DCOM 技術に基づくため、OS 更新やネットワーク変更時に、DCOM 設定・権限設定・ファイアウォール設定などの影響を受ける場合があります。	第 3 章
DCOM セキュリティ強化への対応	Microsoft の DCOM セキュリティ強化により、更新後もクライアント／サーバ間の通信が期待どおり動作するかを確認する必要があります。	第 3 章
OS・製品ライフサイクルへの依存	OS、OPC 関連製品、ドライバ、監視・記録系システムの保守期限が近づくと、既存の OPC 接続を維持できる範囲や更新時の選択肢が限られていきます。	第 6 章
セキュリティ要件への対応	OT/IT 連携の拡大に伴い、認証、権限管理、通信保護などの要件への対応が課題になります。	2.3 節、第 3 章

これらは直ちに障害となるものではありませんが、運用を続けるほど確認すべき範囲は広がっていきます。

2.3 OPC Classic 継続利用がシステム全体のセキュリティに与える影響

セキュリティ面の影響は、OPC Classic を利用する個々のサーバやアプリケーションだけでは完結しません。OPC Classic は現場機器と監視・情報系システムの間で使われるため、個々の接続設定や保護レベルが、接続先の範囲や上位システムとの連携にも影響します。

その理由は、OPC Classic の接続条件・権限・通信許可が、OPC 製品だけでなく Windows や DCOM、ネットワークの設定にもまたがるためです。表 2-3 に、OPC Classic を使い続ける場合に、システム全体のセキュリティへ影響しやすい観点を示します。

表 2-3 OPC Classic 継続利用がシステム全体のセキュリティに与え得る影響

OPC Classic 継続利用時に生じやすい状況	システム全体への影響
Windows 権限、DCOM 設定、OPC 製品設定、ファイアウォール設定をまたいで接続条件が決まる	接続可否や権限の確認先が分散し、セキュリティレビューや障害時の切り分けに時間がかかります
DCOM/RPC の通信に合わせて、ファイアウォール例外や広い通信許可が必要になる場合がある	ネットワーク境界やセグメント分離を見直す際に、例外設定の妥当性を判断しにくくなります
読み取り・書き込みの扱いが、OPC 製品設定、Windows 権限、クライアント側の実装にまたがる場合がある	読み取り専用のつもりの接続でも、書き込み経路や操作可能範囲を確認する負荷が高くなります
古い OS、旧 OPC 製品、旧ドライバ、既存 HMI・SCADA との組合せで運用されている場合がある	セキュリティ更新、端末交換、上位システム更新の際に、影響範囲の確認対象が広がります

このように、OPC Classic 継続利用時のセキュリティ上の論点は、単に「古い通信方式を使っていること」ではありません。接続条件・権限・通信許可が複数の管理箇所に分散し、システム全体の保護レベル、変更のしやすさ、障害時の復旧性に影響する点にあります。

OT/IT 連携が広がるほど、通信相手の確認、接続元の制御、権限の最小化、不要な通信の排除、通信経路の把握といった管理が重みを増します。OPC Classic の継続利用は、個別機器や個別アプリケーションの問題にとどまらず、システム全体のセキュリティ体制に関わる論点として捉えておきたいところです。

この点が、OPC UA 移行を考える理由の一つになります。OPC UA への移行は、単に通信方式を置き換えるだけでなく、接続範囲・通信経路・権限・通信保護を見直し、将来のセキュリティ要件に対応しやすい構成へ進む機会にもなります。ただし、OPC UA を導入すれば自動的に安全になるわけではありません。まずは現行の OPC Classic 接続がシステム全体にどう関係しているかを整理しておくことが出発点になります。

2.4 OPC Classic 継続利用を経営判断につなげる観点

ここまで述べた技術・運用・セキュリティ上の確認観点は、操業の継続性、保守体制、投資判断といった経営判断の材料にもつながります。OPC Classic を使い続けるか、OPC UA への移行を検討するかは、現場の通信方式だけで決まるものではなく、設備更新や上位システム更新、データ活用の計画と合わせて判断すべき事柄です。 重要なのは、すぐにすべてを置き換えることではなく、現状を踏まえて判断できる状態にしておくことです。状況を整理しないまま更新時期を迎えたり、問題が顕在化してから対応方針を検討したりすると、選べる手段が限られてしまいます。これらの影響は、操業影響、保守・復旧影響、セキュリティ・説明責任、将来対応・外部要因といった経営判断の材料にもつながります。ただし、本章では詳細な経営説明までは扱いません。これらを経営層へ説明するための論点整理は、第 5 章で扱います。

2.5 本章のまとめ

本章では、OPC UA 移行を考える背景と、OPC Classic 継続利用時に確認すべき問題意識を整理しました。

- OT/IT 連携の拡大により、OPC に求められる役割は広がっている。
  OPC は、製造現場のデータ連携を長く支えてきました。現在は、現場内のデータ受け渡しに加えて、接続元・接続先、通信経路、権限、書き込み可否を説明できることが重要になっています。
- OPC Classic の継続利用では、更新時・変更時の確認範囲が広がりやすい。
  OPC Classic を使い続けること自体が直ちに問題になるわけではありません。ただし、COM/DCOM、OS、製品ライフサイクル、権限設定、ファイアウォール設定などが関係するため、更新時や障害時に確認・復旧が難しくなる場合があります。
- セキュリティ上の論点は、個別サーバだけでなくシステム全体に関係する。
  OPC Classic では、接続条件や通信許可が Windows、DCOM、OPC 製品、ネットワーク設定にまたがる場合があります。そのため、通信相手、操作範囲、不要な通信、書き込み経路を把握しておく必要があります。
- OPC UA 移行は、経営判断や設備更新計画と合わせて考える必要がある。
  重要なのは、すぐに全てを置き換えることではなく、現状を踏まえて判断できる状態にすることです。どの接続を移行するか、どの接続を当面残すか、どの更新時期に見直すかを説明できるようにすることが出発点になります。

次章では、OPC Classic と OPC UA の違いを、通信方式、セキュリティ機能、運用管理の観点から比較します。

第 3 章　Classic と UA の違い

本章で分かること

- OPC Classic から OPC UA への進化が、単なる機能のバージョンアップではなく、Windows および COM/DCOM に依存した通信方式から、プラットフォーム非依存性や標準化されたセキュリティ機能を備えた通信方式への移行である点と、その技術的背景を理解できます。
- 現場の課題（OS 更新の負担、セキュリティ不安、データ活用の限界）が、OPC UA によってどのように改善される可能性があるのか、また経営上どのような価値に結びつくのかを整理できます。
- UA 化によって何が変わり、何が変わらないのかを整理し、OS 更新時の確認事項や証明書管理、通信設定など、移行後も必要となる実務上の留意点を把握できます。

3.1 Classic と UA の網羅的比較

OPC Classic と OPC UA の根本的な違いは、「Windows および COM/DCOM 技術に依存したデータ通信」から、「通信保護、認証、証明書管理、情報モデルを標準仕様として扱えるデータ連携」への転換にあります。以下に、現場（製造・計装部門）の運用目線と、経営層への説明に使える「システム投資としての意味」を整理した対比表を示します。

表 3-1 OPC Classic と OPC UA の主な違い

評価観点	OPC Classic	OPC UA	現場にとってのメリット	ビジネス上のメリット
通信基盤	Windows COM/DCOM に強く依存	プラットフォーム非依存（Linux、組み込み OS 等も可）	OS やネットワーク構成変更時の影響範囲が明確になり、障害切り分けが容易になる	特定 OS や製品のサポートライフサイクルへの依存を低減できる
安全な接続	Windows 側の暗号化設定や各ベンダーの製品実装に依存	標準で暗号化・証明書管理（Trust List）、通信を保護する仕組み（SecureChannel）をサポート	「どのサーバと、どのクライアントを信頼するか」を現場で明示的に管理できる	工場ネットワークの証明書認証や暗号化を活用した多層防御の基盤となる
利用者認証	製品ごとの実装差が大きく、OS のアカウント管理と混ざりやすい	Anonymous（匿名接続）、ユーザ ID/パスワード、証明書認証を標準化	「誰がデータを書き換えることができるか」のポリシー設定を整理・統一しやすい	外部のベンダーや協力会社によるリモートメンテナンス時のセキュリティガバナンスが強化される
権限制御	製品依存（個別カスタマイズが必要なケース多数）	AccessLevel、UserAccessLevel、RolePermissions による細粒度制御	「読み取り専用（監視）」と「書き込み可能（制御）」の権限分離を設計・設定しやすくなる	誤操作や悪意あるデータ改ざんによる、製品クオリティ低下や操業停止リスクを低減する
監査	各ベンダーの製品ログ実装に依存（追跡困難な場合あり）	標準仕様として「監査イベント」をサポート	「いつ、誰が、どの操作を行ったか」を記録・確認しやすくなる	サイバーインシデント発生時の原因究明を行いやすくなり、対外的な説明責任を果たせる
データ表現	リアルタイムの数値（Tag 情報）が中心	データ、品質、タイムスタンプ、履歴、イベント、情報モデル拡張	単なる数字の羅列ではなく、意味（コンテキスト）を持ったデータを上位システムへ渡せる	生産データの利活用（DX や AI 解析）の準備コストを下げられる可能性がある

OPC UA を導入すれば、現場を悩ませてきた「DCOM 設定の複雑さ」からは解放されます。しかし、「OS 更新の影響がゼロになる」という誤解は禁物です。UA アプリケーションも OS の上で稼働するため、OS アップデートによる「証明書ストアの仕様変更」「サービス起動順のズレ」「ファイアウォール設定の初期化」といった影響は依然として残ります。また、通信ポートについても「UA だから標準の IANA 登録ポート 4840 番で固定」と思い込まず、各ベンダーのエンドポイント URL 定義（アドレス＋ポート）を確実に個別確認する必要があります。

本章で整理した Classic と UA の違いは、技術仕様の比較にとどまらず、保守継続性、OS 更新時の復旧性、接続・権限の説明可能性にも関係します。これらを経営層へ説明する際は、本章の技術項目をそのまま並べるのではなく、第 5 章で整理する操業影響、保守・復旧影響、セキュリティ・説明責任、将来対応・外部要因の論点に置き換えて説明します。

本章のリスクアセスメントは、仮想企業・仮想システムを前提として実施したものであり、実在の特定企業・システムに対する評価結果ではありません。実環境への適用にあたっては、対象システムの構成・運用条件に応じた個別のリスク分析が必要です。以下の分析結果は、OPC Classic から OPC UA への移行に伴うリスク変化の傾向を理解するための参考情報としてご活用ください。

3.2 リスクアセスメント結果

前節（3.1）で整理した OPC Classic と OPC UA の技術的差異を踏まえ、本節では IPA の「制御システムのセキュリティリスク分析ガイド 第 2 版」に準拠したリスクアセスメントを実施しました。以下では、分析のアプローチ、対象システム構成、および分析結果を順に示します。

3.2.1 分析アプローチと評価軸

IPA のガイドラインに準拠し、「資産ベース」と「事業被害ベース（シナリオベース）」の二軸でリスクを体系的に特定しました。

準拠ガイド：IPA「制御システムのセキュリティリスク分析ガイド 第 2 版」

アプローチ	概要
① 資産ベース分析	保護すべき資産（通信経路）を列挙し、各資産の重要度を評価する。通信経路ごとに Classic /UA それぞれのリスク値を算出し比較する。
②表 3-2 資産ベース分析 表 3-3 事業被害ベース分析	攻撃経路・脅威シナリオを想定し、具体的な事業被害（製品供給停止、設備破壊等）の観点からリスクを評価する。
リスク評価軸	発生可能性 × 影響度（事業被害）の 2 軸の掛け合わせにより、リスクレベル（A～E）を判定する。 ※ A（最高リスク）> B > C > D > E（最低リスク）

3.2.2 分析対象システム構成

IPA のガイドラインを参照し、下図に示す仮想の制御システム構成にてリスク分析を実施しました。本構成は、情報ネットワーク、DMZ、制御ネットワーク（情報側・フィールド側）の 4 層構造を持つ典型的な産業制御システムを模しています。

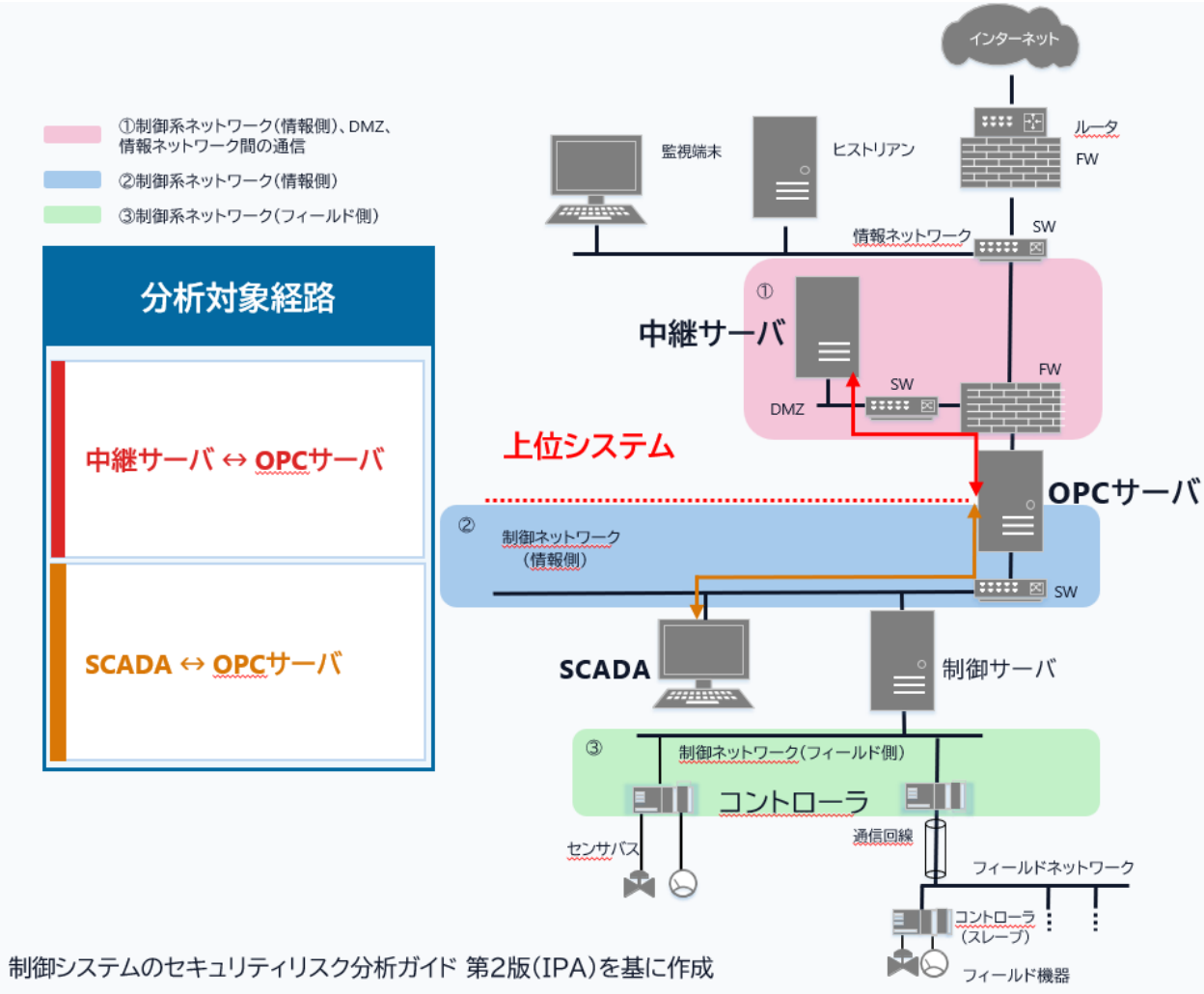


図 3-1 仮想システムの制御システム構成図 [2]

分析対象通信経路：

- 中継サーバ ↔ OPC サーバ
- SCADA ↔ OPC サーバ

上記の通信経路は、大きく分けて①制御ネットワーク（情報側）・DMZ・情報ネットワーク間の通信、②制御ネットワーク（情報側）の内部通信の 2 つのゾーンに分類されます。

3.2.3 分析結果 – Classic 継続利用と UA 移行のリスク比較

4 つの通信経路と 2 つの事業被害シナリオについて分析を行った結果、すべての経路・シナリオにおいて UA 移行後にリスク値が改善することが確認されました。

[2] 制御システムのセキュリティリスク分析ガイド 第 2 版（IPA）を基に作成
https://www.ipa.go.jp/security/controlsystem/ug65p90000019bkg-att/begoj9000000hpm8.pdf

表 3-2 資産ベース分析 – 通信経路別リスク比較

通信経路	Classic	UA
中継サーバ ↔ OPC サーバ	B	D
SCADA ↔ OPC サーバ	A	C

※ リスク値：A（最高）> B > C > D > E（最低）

表 3-3 事業被害ベース分析 – シナリオ別リスク比較

事業被害シナリオ	Classic	UA
製品供給停止（制御 NW）	B	D
品質不良（情報 NW）	B	D

3.2.4 分析結果の総括

【結論】 Classic 継続利用は、全通信経路・全事業被害シナリオにおいてリスクが高い状態にあります。UA 移行により、すべてのリスク値が改善されることが確認されました。

資産ベース分析では、SCADA ↔ OPC サーバ間の通信経路において、Classic 時のリスクが最高レベル（A）であるのに対し、UA 移行後はリスクレベル C（中程度）まで低減されます。これは、OPC UA の標準的な暗号化・認証機構（SecureChannel、Trust List、ユーザ認証の標準化）により、通信の安全性が構造的に向上するためです。

事業被害ベース分析では、「製品供給停止」シナリオにおいて Classic 継続時のリスクが最高（B）であり、UA 移行後も D になる結果となりました。これは、制御ネットワークへの攻撃が物理的な被害に直結し得るため、通信プロトコルの改善だけではリスクを完全に解消できないことを示しています。ただし、OPC UA の細粒度権限制御（AccessLevel、RolePermissions）や監査イベント機能により、リスクの部分的な低減は見込めます。

以上の分析結果は、3.1 節で整理した技術仕様の差異がリスク面でどのように現れるかを定量的に示したものです。これらの結果を、第 5 章で整理する操業影響、保守・復旧影響、セキュリティ・説明責任、将来対応・外部要因の論点に反映し、経営層への説明資料として活用します。

3.3 本章のまとめ

本章では、OPC Classic と OPC UA の違いを、通信方式、セキュリティ機能、運用管理、データ活用の観点から整理しました。

- OPC Classic と OPC UA の違いは、単なる機能差ではなく、通信基盤と管理方法の違いである。
  OPC Classic は Windows の COM/DCOM に強く依存します。一方、OPC UA はプラットフォーム非依存の考え方を取り、通信保護、認証、証明書、権限、監査、情報モデルなどを標準仕様として扱える点に特徴があります。
- OPC UA では、接続や権限を管理項目として整理しやすくなる。
  接続相手、認証方式、Trust List、書き込み権限、ログ確認先などを明示しやすくなるため、障害時の切り分け、変更時の確認、監査対応、上位システム連携を進めやすくなります。
- ただし、OPC UA に移行しても運用確認は不要にならない。
  OS 更新、ファイアウォール、証明書ストア、サービス起動、Endpoint、ログ設定などの影響確認は引き続き必要です。OPC UA は自動的に安全な状態を維持する仕組みではなく、設定根拠と運用ルールを残して管理する必要があります。
- 本章で整理した設定項目は、導入後も確認・記録する対象になる。
  SecurityPolicy、MessageSecurityMode、認証方式、証明書、Trust List などは、導入時だけでなく導入後の運用でも確認が必要です。実際の記録は付録 B「運用管理表」へつなげます。
- リスクアセスメントにより、UA 移行によるリスク低減効果を確認した。
  仮想システムを用いた評価において、Classic 継続利用はすべての通信経路および事業被害シナリオで高リスク（最高レベル A 含む）であるのに対し、UA への移行によってすべてのリスク値が改善されることを確認しました。ただし、「設備破壊」など物理的影響を伴うリスクについては、通信プロトコルの安全化だけでゼロにすることはできないため、物理的・組織的な多層防御の適用が必要です。

次章では、これだけの違いがあるにもかかわらず、なぜ多くの現場で OPC UA 移行が進みにくいのかを、組織・計画面と現場実務面から整理します。

付録との関係

本章で整理した SecurityPolicy、MessageSecurityMode、認証方式、証明書、Trust List の違いは、導入時だけでなく導入後の運用でも確認が必要です。実際に自社環境で確認する場合は、付録 B「運用管理表」を用いて、採用している通信保護設定、認証方式、証明書、Trust List、例外有無を記録してください。

第 4 章　なぜ移行が進まないのか

本章で分かること

本章では、OPC Classic から OPC UA への移行において、多くの製造現場が直面する「移行が進みにくくなる理由」を明らかにします。具体的には、以下の 2 つの側面から移行が進みにくくなる主な要因を解説します。

- 組織・計画的な要因：なぜ社内での優先度が上がらず、投資計画化できないのかという 4 つの根本要因。
- 現場・実務的な要因：設定・構築の現場で実務者がつまずき、検証がストップしてしまう「9 つの困りごと」。

4.1 本章の使い方

本章は、移行のフェーズや読者の立場に応じて、以下のようにご活用ください。

- プロジェクト責任者・推進リーダーの方：社内の検討会や経営層への進捗報告において、「なぜ現場の移行が進まないのか」「どこにリソースや予算を投入すべきか」を整理するための材料として活用してください。
- 現場の製造（OT）部門・実務担当者の方：4.4 節の「9 つのつまずき分類表」を【事前確認チェックリスト】としてお使いください。ベンダーへ構築を依頼する前、あるいは模擬プラント等での検証を開始する前に、自社で決めておくべき事項（データ範囲、承認フロー、責任境界など）の漏れを防ぐために役立ちます。

4.2 移行停滞をもたらす 4 つの根本要因

OPC Classic から OPC UA への移行は、単なる通信ソフトウェアのバージョンアップではなく、制御ネットワーク全体のアーキテクチャおよび運用体制の変更を伴います。我々が実施した課題整理と、ユーザ・ベンダー・中核人材育成プログラム参加企業を対象としたアンケート

で得られた回答を踏まえると、OPC Classic から OPC UA への移行が進みにくい背景は、主に次の 4 つの観点で整理できます。

表 4-1　OPC UA への移行が進みにくい主な要因

要因	なぜ①（直接的要因）	なぜ②（背景）	根本要因
優先度が上がらない	今は大きな問題が発生していない	潜在的なリスク（セキュリティや保守停止）が見えていない	必要性の可視化不足
影響範囲が分からない	どこに Classic の資産や通信が残っているか不明	最新のネットワーク構成図や資産台帳が整備されていない	現行構成・資産の把握不足
運用への不安	証明書や Trust List の管理が難しそうに見える	制御系と情報系の間で管理責任が曖昧になっている	移行・運用ノウハウ不足
計画化の難しさ	既存設備が UA に未対応である	設備の更改・修繕タイミングと連動できていない	段階移行設計の不足
	移行範囲が決められない	一括更新以外にどのような選択肢があるか分からない	移行方式に関する理解不足

アンケート回答からは、「現状のままで安定稼働している」「Windows Update や DCOM 仕様変更への対応に不安がある」「既存設備が UA に未対応であり二重運用の負担が大きい」「セキュリティ強化だけでは投資対効果（ROI）として経営層への訴求が弱く、リソースが割けない」といった声が確認されました。これらは、OPC UA 移行が単なる通信方式の変更ではなく、保守・運用・責任分界の見直しを伴うことを示しています。

4.3 実務者が直面する「9 つのつまずきポイント」

課題整理、アンケート結果、後述（第 10 章）する模擬プラントを使用した検証時に確認された設定・運用上の論点を踏まえると、実務では次の 3 分類 9 項目で立ち止まりやすいことが分かります。

表 4-2　実務者が直面する 9 つのつまずきポイント

分類	つまずきポイント	現場で起きやすいこと	製造部門が先に決めること
接続・データ設計	接続設定	どの端末から、どの OPC UA サーバの Endpoint（接続先 URL）へつなぐか分からない	接続元、接続先、用途を明確にする
接続・データ設計	タグ公開範囲	必要なタグだけでなく、不要な内部データまで公開してしまう	相手方に取り込み・開示を許可するタグ範囲を決める
接続・データ設計	書き込み制御	参照目的の接続なのに、Write（書き込み）経路が残る	書き込み可とするタグを厳選し、承認者を決める
セキュリティ・認証	証明書管理	UA 製品が作成した証明書の場所や有効期限が分からない	証明書の保管場所、発行元ルール、管理・承認者を決める
セキュリティ・認証	Trust List 運用	Rejected（拒否）された証明書を、誰が Trusted（信頼済み）へ移すか決まっていない	Trust List への登録・削除の担当と承認フローを決める
セキュリティ・認証	認証方式	検証時の Anonymous（匿名）接続が本番に残る	本番で許可する認証方式を事前に決める
セキュリティ・認証	Classic /DCOM 設定	Classic 共存時に Windows 側の DCOM 設定やエラー確認先が分からない	DCOM 設定資料と、エラー時のログ確認手順を残す
運用・責任分界	ログ確認	通信エラーや認証エラーの際、UA 製品ログか OS ログか分からない	ログ保存先と一次確認者を決める
運用・責任分界	責任分界	ベンダー任せとなり、障害時に制御側・インフラ側のどちらが見るか曖昧になる	製造、情シス、外部ベンダーの役割と責任境界を決める

4.4 本章のまとめ

本章では、OPC UA 移行が進みにくくなる理由を、組織・計画面と現場実務面から整理しました。

- 移行が進まない理由は、技術の難しさだけではない。優先度が上がらない、影響範囲が分からない、運用に不安がある、設備更新と計画を合わせにくい、といった要因が重なることで、移行検討が止まりやすくなります。

- 現場でのつまずきは、「何を、誰が、いつ確認するか」が決まっていないことから生じやすい。
  接続元・接続先、公開するタグ、書き込み可否、証明書、Trust List、認証方式、ログ確認先、責任分界などは、技術設定であると同時に、事前に確認者と判断者を決めておくべき運用項目です。
- 移行を進めるには、必要性の説明と現状把握を分けて進める必要がある。経営層には、保守停止、復旧遅延、セキュリティ対応、データ活用への影響を説明し、現場では、どの接続がどこに残り、どの設定や責任分界が未確認かを整理します。

次章では、移行や残置管理を経営層へ説明するための事業上の効果と投資判断について説明します。

付録との関係

本章で整理した「つまずきポイント」は、技術的な知識不足だけでなく、確認先、判断者、承認者が決まっていないことから生じる場合があります。接続元・接続先・用途・Classic/DCOM 残置は付録 A、証明書・Trust List・認証方式は付録 B、変更時や例外設定は付録 C に記録することで、確認漏れを減らすことができます。

第 5 章　OPC UA 移行の事業上の効果と投資判断

本章で分かること

本章では、OPC Classic、特に OPC DA を利用している、または利用状況を確認する立場にある製造現場の関係者が、経営層へ何を説明すべきかを整理します。

本章の目的は、OPC Classic の技術課題を細かく説明することではありません。現場で起きている、または今後起き得る困りごとを、経営層が投資判断、優先順位判断、リスク受容判断を行える論点に変換することです。

ここで重要なのは、「OPC Classic は古いから危険」「OPC UA は新しいから導入すべき」と単純に説明しないことです。OPC Classic 継続利用で問題になりやすいのは、端末故障や OS 更新後に同じ通信状態へ戻しにくいこと、設定や復旧手順を分かる人が限られること、接続範囲や書き込み権限を説明しにくいこと、将来の上位システム連携やデータ活用で制約になり得ることです。

一方で、OPC UA へ移行すれば、すべてが自動的に解決するわけではありません。OPC UA は、接続先、認証、証明書、権限、ログ、監査記録などを管理項目として整理しやすくする仕組みを持ちますが、製品仕様、設定、保存運用、役割分担が伴わなければ、十分な説明可能性は成立しません。

本章では、Classic 継続利用のリスクを、次の 4 つの経営論点に整理します。

- 操業影響
- 保守・復旧影響
- セキュリティ・説明責任
- 将来対応・外部要因

5.1 本章の目的と使い方

本章は、製造部門、設備管理部門、保全部門、工場システム担当、製造 IT、OT セキュリティ担当などが、経営層や管理層へ OPC UA 移行、段階移行、Classic 残置管理の必要性を説明する場面で使うことを想定しています。

すべての論点を経営層へ同じ重みで説明する必要はありません。自社の状況に合わせて、特に判断が必要な論点を選びます。たとえば、古い OS や保守期限切れ端末が残っている場合は、保守・復旧影響を中心に説明します。品質記録や上位システム連携に使われている接続がある場合は、操業影響や将来対応を中心に説明します。監査、顧客確認、海外案件、グローバルサプライチェーンに関係する場合は、セキュリティ・説明責任と外部要因を中心に説明します。

ただし、説明に使わない論点を無視してよいわけではありません。主要論点として扱わない項目は、補足資料、残るリスク、今後確認する項目として整理します。

本章で指す「残置管理」とは、Classic を当面残す接続について、残す理由、期限、責任者、見直し時期を明確にして管理することです。Classic を残すことは、何もしないことではありません。

本章では、経営層へ説明するための論点を整理します。具体的な接続棚卸しは第 6 章、移行優先度や移行方式の検討は第 7 章、移行前後や Classic 残置時の確認は第 8 章、導入後の維持管理は第 9 章で扱います。

5.2 経営層へ説明する 4 つの論点

経営層へ説明する際は、DCOM 設定、証明書、Trust List、SecurityPolicy、Anonymous、Gateway／Wrapper の方式差などの技術詳細をそのまま並べるよりも、事業影響に翻訳して説明する方が伝わりやすくなります。

本章では、次の 4 論点に整理します。

表 5-1　経営層に説明すべき 4 論点

論点	現場側が確認すること	経営層へ伝えること	関連する章
①　操業影響	止まると何に影響するか	移行の優先対応が高い接続	第 6 章・第 7 章
②　保守・復旧影響	更新後に戻せるか	復旧遅延・属人化のリスク	第 6 章・第 8 章
③　セキュリティ・説明責任	接続・権限を説明できるか	監査・顧客確認への備え	第 8 章・第 9 章
④　将来対応・外部要因	今後の要求に耐えられるか	新規・海外・更新方針	第 7 章・第 11 章

①　操業影響

操業影響で現場側が確認すべきことは、OPC 接続が止まった場合に、どの業務へ影響するかです。OPC Classic は DCOM 設定不備などにより通信接続の不具合が発生するリスクが潜在しております。一方で OPC 接続は、画面監視だけでなく、品質記録、帳票作成、アラーム連携、データ収集、上位システム連携、保全データ取得などに使われている場合があります。通信停止が直ちに設備停止につながらなくても、品質記録の欠損、監視不能、手入力作業の増加、操業判断の遅れにつながる可能性があります。

経営層へは、「今通信できているか」ではなく、「止まった場合に何が困るか」を説明します。停止影響が大きい接続、書き込み経路を持つ接続、品質記録や上位システムに関係する接続は、優先して確認・見直し、OPC-UA 移行箇所の対象にします。

②　保守・復旧影響

保守・復旧影響で現場側が確認すべきことは、端末故障、OS 更新、サーバ更新、担当者交代の後に、同じ通信状態へ戻せるかです。

OPC Classic は、Windows の COM/DCOM、Windows 権限、ファイアウォール、サービスアカウント、OPC 製品設定、ベンダー固有設定など、複数の設定に影響を受ける場合があります。設定内容や復旧手順が属人化していると、平常時は動いていても、障害時や更新時に切り分けに時間がかかります。

経営層へは、移行費用だけでなく、Classic を継続利用する場合の復旧遅延、旧 OS 延命、外部ベンダー依存、確認工数、属人化も比較対象にする必要があると説明します。

OPC UA へ移行しても、OS 更新の影響がなくなるわけではありません。しかし、接続先、認証、証明書、権限、ログ確認先などを管理項目として整理しやすくなるため、更新時や障害時に確認すべき対象を明確にしやすくなります。

③ セキュリティ・説明責任

セキュリティ・説明責任で現場側が確認すべきことは、誰が接続でき、どの範囲のデータを読み取り、どの範囲を書き込めるかを説明できるかです。

監査や顧客確認で問われるのは、OPC を使っているかどうかだけではありません。接続元、接続先、通信経路、認証、権限、書き込み有無、ログ確認先、例外設定、残置理由を説明できるかが重要になります。

OPC UA には、接続相手の確認、認証、通信保護、権限管理、ログ確認を整理しやすくする仕組みがあります。ただし、OPC UA を導入すれば自動的に安全になるわけではありません。証明書、Trust List、認証、通信保護設定、権限、ログなどは、導入後も見直せる管理情報として残す必要があります。

したがって、経営層へは「セキュリティ機能を入れる投資」ではなく、「接続状態、権限、ログ、例外、残置理由を説明できる状態を維持する投資」として説明します。

④ 将来対応・外部要因

将来対応・外部要因で現場側が確認すべきことは、現在の接続方式が、今後の設備更新、上位システム連携、データ活用、海外展開、顧客要求に対して制約にならないかです。

日本国内の既存設備では、OPC UA 移行を直ちに求める制度的な圧力は、現時点では限定的な場合があります。そのため、既存設備については、操業影響、更新時期、保守期限、復旧性を踏まえて、段階的に移行判断することが現実的です。

一方で、海外では、制御システムや産業システムに対するサイバーセキュリティ要求が強まっています。たとえば EU の CRA は、デジタル要素を持つ製品について、設計・更新・維持を通じたサイバーセキュリティを求める規制として位置づけられています。また、NIS2 Directive は、EU の 18 の重要分野におけるサイバーセキュリティの共通枠組みを強化するものです。

これらの制度は、OPC UA の導入そのものを一律に義務づけるものではありません。しかし、接続相手、通信保護、認証、権限、ログ、脆弱性対応、保守性、説明責任を求める流れは強まっています。OPC Foundation も、OPC を産業オートメーション分野における安全で信頼性の高いデータ交換の相互運用標準として説明しており、Industrie 4.0 の Asset Administration Shell と OPC UA を関連づける仕様整備も進められています。

このため、新規設備、海外拠点、輸出設備、グローバル顧客向け案件では、OPC UA を前提にしないことが、将来の説明負荷、追加改修、顧客要求への対応遅れ、調達条件との不整合につながる可能性があります。特に、将来の上位システム連携、データ活用、リモート保守、サプライチェーン上のセキュリティ確認を考える場合、OPC UA を前提にした方が説明しやすい場面が増えると考えられます。

日本でも、現時点で海外と同じ強さの圧力があるとは限りません。しかし、製造データ活用、OT/IT 連携、顧客確認、サプライチェーンセキュリティ、海外制度への対応が進むにつれて、同様の説明要求が将来的に強まる可能性があります。そのため、既存設備は段階的に見直し、新規設備や全面更新では OPC UA を標準方針として検討することが望ましいです。

ただし、外部制度や規格が自社に直接適用されるかどうかは、対象製品、販売地域、自社の立場、契約条件、顧客要求によって異なります。経営層へは「海外制度があるから全設備を直ちに移行する」と説明するのではなく、「海外では説明要求が強まっており、日本でも将来同様の流れが来る可能性があるため、新規・更新案件では OPC UA を前提にし、既存設備は残置理由と見直し時期を明確にする」と説明します。

5.3 稟申時に提示すべき判断材料

OPC UA 移行の技術的な移行計画（移行の対象案、段階移行の計画案等）は製造部門、設備管理部門、保全部門、工場システム担当、情報システム部門、セキュリティ担当、ベンダーなどが現状を確認したうえで、計画案として整理しておく必要があります。

経営層には、その計画案に対して、事業上の優先順位、投資の妥当性、実施時期、残るリスクの受容、全社方針との整合を判断してもらいます。

したがって、現場側が経営層へ稟申する際には、単に「OPC UA へ移行したい」と説明するのではなく、次のような判断材料を提示します。

表 5-2　稟申時に提示すべき判断材料

提示する項目	提示すべき判断材料	説明の観点	関連する章
移行・残置の対象案	対象接続、用途、停止影響、書き込み有無	どの接続を優先的に扱うか	第 6 章・第 7 章
段階移行の計画案	更新予定、停止可能時期、保守期限	いつ、どの更新機会に合わせるか	第 7 章
Classic 残置案	残置理由、期限、復旧手順、責任者	どのリスクをいつまで受け入れるか	第 8 章・第 9 章
費用・体制案	調査、検証、構築、切替、運用負荷	移行費用と継続利用負担を比べる	第 7 章・第 9 章
新規・海外案件の方針案	外部要求、顧客確認、将来連携方針	OPC UA を標準方針にする範囲	第 7 章・第 11 章

稟申側は、移行対象や残置対象を整理する際に、技術的に置き換えやすいかだけで判断しないようにします。停止影響が大きい接続、書き込み経路を持つ接続、保守期限が近い接続、復旧手順が不明な接続、人に依存している接続を優先的に確認します。

段階移行では、全面更新だけを前提にしません。設備更新、OS 更新、サーバ更新、上位システム更新、保守契約更新、監査対応など、既存の更新イベントに合わせて移行しやすい単位から計画します。具体的な A/B/C 分類や移行方式の選定は、第 7 章で扱います。

Classic を当面残す案を出す場合は、「移行できないから残す」だけでは不十分です。残す理由、残す期限、残る Classic 区間、復旧手順、責任者、次回見直し時期を示し、経営層に残るリスクを説明します。Classic を残す場合も、残る理由、期限、影響、復旧性を説明できるかを確認し、継続管理は第 9 章で扱う構成になっています。

費用・体制案では、初期構築費用だけでなく、調査、検証、切替、切戻し、導入後運用、教育、外部依頼、既存構成を残す場合の確認工数も含めます。

新規設備、全面更新、海外案件、輸出設備、グローバル顧客向け案件では、OPC UA を標準方針として扱う範囲を提示します。これは、直ちに全既存設備を移行するという意味ではありません。将来の追加改修や説明負荷を避けるため、新規・更新案件では最初から OPC UA を前提に検討するという方針を明確にするものです。

5.4 経営層向け説明例

経営層へ説明する際は、技術機能を並べるのではなく、自社の判断に関係する言葉に置き換えます。本章では、4 つケースを例に、説明文を示します。自社の状況に近いものを選び、参考にしてください。

例 1：設備更新・OS 更新に合わせて説明する場合

設備更新、OS 更新、サーバ更新の機会に合わせて、OPC 接続を更新後も継続して安定稼働および障害時の早期復旧ができる状態へ見直しを行います。

現在の OPC Classic 接続は、平常時には安定して稼働しています。一方で、古い Windows 設定、製品固有設定、担当者やベンダーの知見に依存している接続では、更新後の通信確認や障害時の切り分けに時間がかかる場合があります。

また、OPC 接続は、監視だけでなく、品質記録、帳票作成、データ収集、上位システム連携にも使われています。通信が止まった場合、設備停止に直結しなくても、記録欠損、監視不能、手入力作業の増加、操業判断の遅れにつながる可能性があります。

本件では、更新時期が近い接続、停止影響が大きい接続、品質記録や上位システムに関係する接続を優先して確認します。そのうえで、OPC UA への移行、Gateway／Wrapper による段階移行、または Classic の期限付き残置に分けて対応します。

例 2：セキュリティ・監査対応として説明する場合

監査、顧客確認、社内のリスク管理に備え、重要な OPC 接続から、接続先、権限、書き込み範囲、ログ確認先、例外設定を説明できる状態に整備します。

OPC UA には、接続相手の確認、通信保護、権限管理、ログ確認を整理しやすくする仕組みがあります。ただし、OPC UA を導入しただけで、監査や顧客確認に説明できる状態が自動的に維持されるわけではありません。

そのため、証明書の期限、Trust List（接続相手として信頼する証明書や CA 証明書の一覧）、認証方式、権限、ログや監査記録の確認先、例外設定を、重要接続から確認できる状態にします。例外を残す場合は、理由、期限、見直し日を明確にします。

本件では、監査や顧客確認に対して説明しやすい管理状態へ移行します。

例 3：Gateway／Wrapper を使う段階移行として説明する場合

既存設備をすぐに全面更新できない接続については、Gateway／Wrapper を活用し、上位システム側から段階的に OPC UA へ移行します。

Gateway／Wrapper は、既存の OPC Classic 接続を活かしながら、上位システム連携やデータ活用の準備を進めるための現実的な手段です。一方で、Gateway／Wrapper を使っても、OPC Classic に由来する課題がなくなるわけではありません。

下位側や中継区間に Classic 接続、古い OS、旧ベンダー製品が残る場合は、その範囲を管理対象として明確にします。

本件では、Gateway／Wrapper を全面更新までの橋渡しとして使用します。OPC UA に切り替えた範囲、Classic が残る範囲、管理担当、障害時の確認先、書き込み経路、次回見直し時期を整理したうえで、段階移行を進めます。

例 4：新規設備・海外案件・将来標準への対応として説明する場合

新規設備、全面更新、海外案件、グローバル顧客向け案件では、将来の保守性、顧客確認、上位システム連携、データ活用を見据え、OPC UA を標準方針として検討します。

日本国内の既存設備では、OPC UA 移行を直ちに求める制度的な圧力は限定的な場合があります。そのため、既存設備については、操業影響、更新時期、保守期限、復旧性を踏まえて、段階的に判断することが現実的です。

一方で、海外では、制御システムや産業システムに対するサイバーセキュリティ要求が強まっています。CRA、NIS2、IEC 62443、Industrie 4.0、サプライチェーンセキュリティ要求などを背景に、接続方式、認証、権限、ログ、保守性、脆弱性対応を説明する場面は増えています。

本件では、既存設備を直ちに全て置き換えるのではなく、新規設備、全面更新、海外案件、グローバル顧客向け案件について、OPC UA を標準条件として仕様に入れる方針を提案します。

既存設備については、残置理由、見直し時期、責任者を明確にしながら段階的に見直します。

5.5 成立条件と残るリスク

OPC UA 移行の効果は、導入しただけで成立するものではありません。接続先、認証方式、証明書、権限、ログ、書き込み経路、変更時確認、例外設定を、運用管理の対象として維持して初めて効果が出ます。

OPC UA へ移行しても、OS 更新、サーバ更新、ファイアウォール、名前解決、時刻同期、証明書期限、ログ設定などの影響を受ける場合があります。そのため、「OPC UA にすれば OS 更新の影響がなくなる」とは説明しません。

Gateway／Wrapper は、段階移行の手段として有効な場合があります。上位システム側を OPC UA 化したい場合や、既存の OPC Classic サーバをすぐに置き換えられない場合には、現実的な選択肢になり得ます。

ただし、上位側が OPC UA に見えても、下位側に OPC Classic、COM/DCOM、古い OS、旧ベンダー製品が残る場合は、その区間のリスクは残ります。Gateway／Wrapper は Classic リスクを解消する装置ではなく、Classic 区間を明確にしたうえで管理するための手段として扱います。

Classic を残す場合は、残置そのものを否定するのではなく、残す理由、期限、影響、復旧性、責任者、見直し時期を明確にします。期限や見直し条件がない残置は、設備更新、OS 更新、担当者交代、監査対応のたびに負担を増やす可能性があります。

特に、新規設備、海外案件、輸出設備、グローバル顧客向け案件では、Classic 残置の説明負荷が国内既存設備より大きくなる可能性があります。そのため、残置判断では、現在の操業影響だけでなく、将来の顧客確認、海外制度、サプライチェーン要求、データ活用計画も確認対象に含めます。

5.6 本章のまとめ

本章では、OPC Classic 継続利用を、製造現場の関係者が経営層へ説明しやすい事業上の論点として整理しました。

要点は次の 3 点です。

- OPC Classic 継続利用の問題は、「古いから危険」ではなく、止まった場合の操業影響、更新時の復旧性、接続・権限の説明責任、将来のデータ活用や外部要求への対応に影響する点にある。
- 経営層へは、現場側が移行・段階移行・Classic 残置の計画案と判断材料を用意し、投資判断、優先順位判断、残るリスクの受容、新規・海外案件での標準方針について承認を求める。

- 海外では制御システムへのセキュリティ要求が強まっており、日本でも将来的に同様の説明要求が強まる可能性がある。そのため、新規設備や全面更新では OPC UA を前提に検討し、既存設備では残置理由と見直し時期を明確にすることが重要である。

この判断を行うためには、まず自社の OPC 接続の所在、用途、停止影響、書き込み有無、Classic/DCOM 残置、保守期限を確認する必要があります。

第 6 章では、判断材料をそろえるための接続棚卸しと確認作業を扱います。第 7 章では、棚卸し結果をもとに移行優先度と段階移行方針を整理します。第 8 章では、移行前後や Classic 残置時の確認事項を扱い、第 9 章では、導入後に維持すべき管理情報と継続運用を扱います。

付録との関係

経営層へ説明する際は、一般論として OPC Classic のリスクを述べるだけでは不十分です。自社のどの接続が、どの業務に関係し、どの更新時期や保守期限に影響されるのかを示す必要があります。

まずは、付録 A「接続・移行確認表」を使い、代表的な OPC 接続について、接続元、接続先、用途、通信方式、書き込み有無、Classic/DCOM 残置、停止影響、A/B/C 分類、確認先・次の対応を整理します。最初からすべてを完璧に調べる必要はなく、代表的な OPC 接続を数件選び、付録 A に記録して第 7 章、第 8 章、第 9 章へつなげる流れが示されています。

付録 A で整理した結果は、第 7 章の移行優先度と移行方式の判断に使います。移行前後や Classic 残置時の確認事項は第 8 章で確認し、証明書、Trust List、認証、権限、ログ、例外、Classic 残置、Gateway/Wrapper などの継続管理は第 9 章へ引き継ぎます。

第 6 章　移行に必要な作業

本章で分かること

OPC Classic（特に OPC DA）を利用している企業・現場担当者が、移行前に何を確認し、どの接続から着手し、Gateway/Wrapper を使う場合に何を管理すべきかを整理できます。優先順位の付け方や移行方式の選定（A/B/C 分類、4 方式比較）については第 7 章を参照してください。本章は、その判断に必要な「材料」を揃えるための実務手順です。

OPC UA への移行は、製品を単純に置き換える作業ではありません。ユーザ側でまず確認すべき単位は「製品」ではなく「接続」です。どの機器とどのシステムが、何の目的で、どの通信方式を使ってつながっているかを把握することが出発点になります。

すべての接続を一度に調べようとすると、作業が大きくなりすぎます。まずはユーザ側で影響を説明しやすい、以下の代表的な接続を 3 件選んで確認することから始めてください。

- 止まると困る接続
- 古い OS や保守期限が気になる接続
- 上位システムやデータ活用に関係する接続

6.1 移行作業の全体像

ユーザ側で接続の棚卸し、移行成立性の確認、役割分担の決定を行うために、以下の 6 ステップで進めます。各ステップの成果物が、第 7 章の優先順位付け（A/B/C 分類）と移行方式選定の判断材料になります。

ステップ	やること	確認すること	成果物・判断材料
1	接続を洗い出す	接続元、接続先、用途、通信方式	OPC 接続の一覧
2	Classic 残置を確認する	DA、A&E、HDA、DCOM、Gateway 経由、DCOM 設定資料・権限・ログ手順の有無	移行後も残るリスク
3	停止影響を確認する	停止時に影響する工程、監視、記録、帳票、制御	優先度判断の材料
4	保守期限を確認する	OS、ミドルウェア、OPC 製品、ベンダー支援期限	更新タイミングの候補
5	移行成立性を確認する	UA 対応可否、タグ数、更新周期、書き込み有無、ログ	移行方式の候補
6	役割分担を決める	製造、保全、情シス、セキュリティ、ベンダーの責任範囲	障害時・変更時の対応体制

6.2 接続台帳で確認する項目

接続台帳は、ユーザ側の移行判断の起点になります。以下の項目を、確認できる範囲で記入していきます。各項目の「見落とした場合の影響」を意識すると、優先順位を付けやすくなります。

確認項目	確認すること	見落とした場合の影響
接続元・接続先	どの機器、PC、サーバ、ソフトが通信しているか	障害時に切り分け先が分からなくなる
通信方式	DA、A&E、HDA、UA、Gateway 経由のどれか	Classic 区間の残置を見誤る
DCOM 把握状況	DCOM 設定資料、権限、ログ確認手順があるか	Classic 区間の復旧や切り分けが長期化する
用途	監視、記録、帳票、制御、上位連携など	停止影響を正しく評価できない
読み取り・書き込み	読み取り専用か、書き込み経路があるか	不要な書き込みリスクを残す
公開タグ範囲	移行後に公開するタグ、取り込むタグの範囲	不要なタグ公開やデータ不足が起きる
品質情報・タイムスタンプ	値だけでなく品質と時刻を扱えるか	上位活用時にデータの信頼性を説明しにくい
OS・保守期限	Windows、ミドルウェア、OPC 製品、ベンダー支援期限	更新時期を逃す
ログ保存先	接続、認証、証明書、書き込み、Gateway ログの確認先	障害時の初動が遅れる
責任分界	製造、保全、情シス、セキュリティ、ベンダーの担当範囲	設定変更や障害対応が止まる

6.3 移行成立性の確認

OPC UA に接続できることだけで「移行できた」と判断しないことが重要です。ユーザ側で継続して使える状態にするには、性能・セキュリティ・運用・保守まで確認する必要があります。

観点	確認すること	判断の目安
技術	下位機器や上位システムが UA に対応しているか	直置換できるか、Gateway が必要かを判断する
性能	タグ数、更新周期、再接続時間、負荷に問題がないか	操業に必要な周期で値を取得できるかを見る
セキュリティ	接続相手を誰が信頼設定し、証明書切れや設定変更時に誰が対応するか（Trust List、認証方式、SecurityPolicy）	本番運用で接続できない、例外設定が放置される、といった問題を防げるかを見る
書き込み制御	書き込み可能タグ、承認者、書き込みログ、不要な書き込み経路の有無を確認できるか	誤操作や不要な制御書き込みを防ぐ
運用	ログ確認先、一次切り分け担当、変更時の確認手順をユーザ側で説明できるか	障害時に現場が迷わない状態にする
保守	OS、製品、ベンダー支援、社内対応人材が継続できるか	移行後も維持できる構成かを判断する

6.4 Gateway/Wrapper を入れた後も確認すべきこと

Gateway や Wrapper は、ユーザ側が段階移行を進めるための有効な手段です。ただし、これらを使っただけで Classic のリスクが消えるわけではありません。上位側（IT システム側）からは UA 化できているように見えても、下位側（OT システム側）に OPC Classic や DCOM が残る場合があります。

※Wrapper/Proxy の考え方は、OPC Foundation “OPC Unified Architecture - Part 8: Data Access”, Annex A “OPC COM DA to UA mapping” を参照して整理しています。ユーザ側では名称よりも、どちら側に Classic 区間が残るかを確認することが重要です。

方式	分かりやすい説明	主な注意点
Wrapper	OPC Classic サーバを、OPC UA クライアントから使えるように見せる仕組み	下位側の Classic 区間は残る
Proxy	OPC UA サーバを、既存の OPC Classic クライアントから使えるようにする仕組み	上位側が Classic 前提のまま残る
Gateway	Classic と UA の間を中継・変換する広い仕組み	変換範囲、責任分界、ログ、書き込み経路、Classic 残置箇所を明確にする

現場で多い「下位 Classic・上位 UA」構成では、上位を UA 化しても、下位 Classic 区間の DCOM 依存・OS 更新・保守・人材・障害切り分けの課題は残ります。Gateway や Wrapper は段階移行を支援する有効な手段ですが、Classic リスクを自動的に解消するものではありません。

6.5 移行前に最低限決めておくこと

技術的な設定に入る前に、以下の 5 点はユーザ側の現場・情シス・セキュリティとベンダーで合意しておくことを推奨します。これらの合意がないまま技術検討を進めると、後工程で手戻りが発生しやすくなります。

決めること	決めておく理由
どの接続から着手するか	全件一括ではなく、停止影響や更新期限の大きい接続から進めるため
Classic 区間をいつまで残すか	Gateway や Wrapper が恒久的な残置にならないようにするため
誰が接続相手の信頼設定と証明書を管理するか	接続できない、証明書切れに気づかない、信頼設定が増え続ける、といった問題を防ぐため
誰がログを最初に確認するか	障害時に製造・情シス・ベンダー間で対応が止まらないようにするため
例外設定をどう承認し、いつ見直すか	Anonymous 許可や弱い SecurityPolicy などを、理由不明のまま放置しないため

6.6 本章のまとめ

本章では、接続台帳、Classic 残置状況、停止影響、保守期限、移行成立性、責任分界といった移行判断に必要な情報を整理しました。

次章ではこれらの棚卸し結果をもとに、どの接続を優先するか（A/B/C 分類）、いつ移行するか、どの方式を選択するかを判断します。

棚卸しは目的ではなく、移行計画を作るための出発点です。

付録との関係

本章で確認した接続元・接続先、用途、通信方式、Classic/DCOM 残置、停止影響、書き込み有無、保守期限、責任分界は、付録 A「接続・移行確認表」に記録します。最初から全接続を網羅する必要はありません。まずは代表的な接続を 3 件程度選び、未確認の項目は「未確認」として、確認先と次の対応を残してください。

第 7 章　移行方針の決め方

本章で分かること

OPC UA への移行を「いつ」「どこから」「どの方式で」進めるかを判断する考え方が分かります。具体的な棚卸し手順や接続台帳の作り方は第 6 章を参照してください。本章は、棚卸しの結果を踏まえて優先順位を付け、移行方式を選び、経営層に説明するための判断軸を提供します。

こんな方に読んでほしい

- OPC Classic を使っているが、今後どうすべきか悩んでいる方
- 経営層や上位部門に「なぜ移行するのか」を説明する必要がある方
- 設備更新や OS 更新を控えており、タイミングを見計らっている方
- 移行にかかるコスト・リスクを現実的に把握したい方

7.1 なぜ今、移行を考えるべきなのか

OPC Classic（COM/DCOM＝Windows が古くから持つ通信の仕組み）は長年にわたり産業用通信の基盤として機能してきました。しかし、以下のリスクが年々高まっており、「いつかやる」では間に合わなくなる可能性があります。

表 7-1 OPC Classic 継続利用時に起こる主なリスク

リスク	具体的に何が起こるか	影響度
Windows DCOM 制限強化	2022 年以降の Windows 更新（KB5004442 等）で DCOM の認証要件が厳格化。未対応の DCOM 利用アプリケーションでは、Windows 更新後に接続や起動に影響が出る可能性があります	★★★
OS・サーバの保守切れ	対象 OS ごとの保守期限は Microsoft Lifecycle で確認。保守終了後はセキュリティ更新や技術サポートを受けられない場合があります	★★★
セキュリティ脆弱性	DCOM は動的ポートを使用し、ファイアウォール設定が困難。攻撃対象になりやすい	★★★
ベンダーサポート終了	製品・ドライバによっては Classic 対応のサポートが縮小・終了し、交換部品や支援体制の確保が難しくなる場合があります	★★☆
Industry 4.0 への対応遅れ	クラウド連携・データ分析・予知保全などの新技術が Classic では実現困難	★★☆

※ ★が多いほど影響が大きいリスクです（★★★＝最大）

※DCOM 認証強化に関する記述は Microsoft KB5004442 を、OS・サーバの保守期限は Microsoft Lifecycle の各製品情報を参照しています。Windows Server 2012/2012 R2 は 2023 年 10 月 10 日に延長サポートが終了しています。

【ポイント】移行は「攻め」だけでなく「守り」でもあります。現行システムの延命にもコストがかかる以上、計画的に進める方が合理的です。

7.2 全体の進め方

移行は単独の大規模プロジェクトとして進めるのではなく、第 6 章で整理した棚卸し結果をもとに、優先順位を付け、既存の更新イベントに合わせて段階的に進めるのが現実的です。本章ではその判断軸を示します。

表 7-2 A/B/C 分類の目安

フェーズ	本章で扱う判断軸	参照
優先順位付け	A/B/C 分類により、3 か月以内に着手するもの、更新時期に合わせるもの、様子見にするものを区別する	7.3
タイミング判断	OS 更新・設備更新・上位システム更新・証明書更新・監査対応など、既存イベントを移行のきっかけとする	7.4
方式選択	Wrapper/Proxy/Gateway/Native の 4 方式から、自社の状況に応じて選ぶ	7.5
役割分担	製造・保全・情シス・セキュリティ・ベンダー・経営層の責任範囲を整理する	7.6
経営説明	段階移行と投資平準化の論点を、経営層に説明できる形にまとめる	7.7

【前提】 本章を読む前に、第 6 章の手順に沿って代表的な接続を 3 件程度棚卸ししてください。棚卸し結果がないと、A/B/C 分類もタイミング判断もできません。

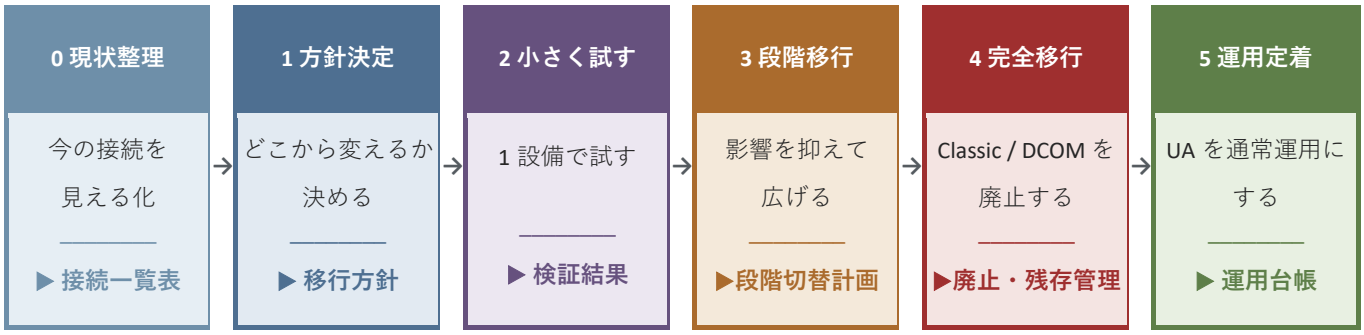
表 7-3 第 6 章の棚卸し結果と第 7 章の判断軸の対応

第 6 章で棚卸しした結果	現場での意味	第 7 章で使う判断軸	判断への使い方	付録 A／別紙 Excel 版との対応
接続元・接続先・用途	どの設備・PC・サーバが、何のためにつながっているか	A/B/C 分類、役割分担	止まると困る接続か、誰が影響を説明できるかを判断する	付録 A／01 Excel「01_接続・移行確認」：接続元、接続先、用途、確認先
通信方式	OPC Classic、OPC UA、Gateway 経由など、どの方式で通信しているか	方式選定、Classic 残置判断	Classic 区間が残るか、Wrapper/Gateway/Native 化のどれを検討するかを判断する	付録 A／01 Excel「01_接続・移行確認」：通信方式、Classic/DCOM 残置、Gateway/Wrapper 有無
DCOM 把握状況	DCOM 設定、権限、ログ手順を説明できるか	A/B/C 分類、移行タイミング	復旧や OS 更新時の不安が大きい接続は、優先度を上げて検討する	付録 A／01 Excel「01_接続・移行確認」：Classic/DCOM 残置、確認先・次の対応
停止影響	停止時に監視、記録、帳票、制御へ影響するか	A/B/C 分類	操業影響が大きいものは A 候補、影響が限定的なものは B または C 候補とする	付録 A：「A/B/C 分類」「停止影響」「次の対応」欄
OS・製品・ベンダー保守期限	古い OS、OPC 製品、ベンダー支援期限が近いか	移行タイミング、A/B/C 分類	OS 更新、設備更新、保守更新のタイミングで移行を計画できるかを見る	付録 A／01 Excel「01_接続・移行確認」：保守期限、更新予定（詳細：任意詳細 Excel「02_資産管理台帳」）
UA 対応可否・タグ数・更新周期	現行のデータ量や速度で UA 化できる見込みがあるか	移行方式選定	直接置換できるか、Gateway/Wrapper が必要か、追加検証が必要かを判断する	付録 A：「A/B/C 分類」「次の対応」欄／任意詳細 Excel「04_UA 環境構築チェックリスト」
読み取り・書き込み有無	上位側から値や設定を書き込む経路があるか	A/B/C 分類、方式選定、役割分担	書き込みあり・不明の接続は、権限、ログ、承認者を確認したうえで優先度を判断する	付録 A／01 Excel「01_接続・移行確認」：書き込み有無（権限は付録 B／01 Excel「02_運用管理」）
タグ範囲、品質情報、タイムスタンプ	値だけでなく、データの正常性や時刻を説明できるか	方式選定、上位活用判断	MES、Historian、品質分析、帳票で使う接続は、移行後も同じ意味で使えるかを確認する	付録 A／01 Excel「01_接続・移行確認」：タグ・品質・時刻（詳細：任意詳細 Excel「04_UA 環境構築チェックリスト」）
ログ保存先	障害時にどのログを見ればよいか	方式選定、役割分担、導入後運用への引き継ぎ	Gateway や UA 化後に、接続失敗、証明書エラー、書き込み履歴を追えるかを確認する	付録 B／01 Excel「02_運用管理」：ログ保存先、一次確認者
責任分界	製造、保全、情シス、セキュリティ、ベンダーの担当範囲	役割分担、経営説明	設定変更、障害対応、証明書・権限管理を誰が判断するかを決める	付録 A／01 Excel「01_接続・移行確認」：確認先・次の対応（管理担当は付録 B／01 Excel「02_運用管理」）

以下に、OPC Classic から OPC UA へ段階的に移行する際の全体像と、代表的な移行方式の位置づけを示します。

図 7-1: OPC Classic → OPC UA 移行ロードマップ

フェーズ 0 から 5 までの 6 段階で、現状整理から運用定着まで段階的に進めます



Created With DALL-E

ポイント

一度にすべてを切り替える必要はありません。

フェーズ 0 で現状を整理し、優先度の高い接続から小さく試して、影響を確認しながら段階的に広げます。

対象に応じて Classic / DCOM を廃止できる状態（フェーズ 4）を目指します。

すぐに廃止できない接続は、残す理由と見直し時期を決めて管理し、そのうえで通常運用へ定着させます（フェーズ 5）。

図 7-2: 移行方式の位置づけ

移行を始める場所（上位側／下位側）と、目指す構成（暫定／最終）で方式を整理します

記号の意味：o 既存資産を残して UA と接続する暫定方式（Wrapper / Proxy）

△ 上位側または下位側から始める部分移行

◇ 複数設備・複数方式を UA に集約する方式（Gateway）

★ Classic / DCOM を廃止し、UA を直接実装する最終形（Native 化）

	暫定方式	最終方式
上位側中心	o Wrapper 既存 Classic Server を残し、上位側から OPC UA で利用 △ 上位側移行 HMI / MES 側を先に UA Client 化	◇ Gateway 複数設備・複数方式のデータを OPC UA に集約 ★ Native 機器・アプリ側に OPC UA を直接実装
下位側中心	o Proxy 既存 Classic Client を残し、OPC UA 側との接続を橋渡し △ 下位側移行 設備側・制御側から UA 化	★ 下位側 UA Native 制御側を OPC UA Native に置き換え、Classic / DCOM 通信を廃止

Created With DALL-E

位置づけ

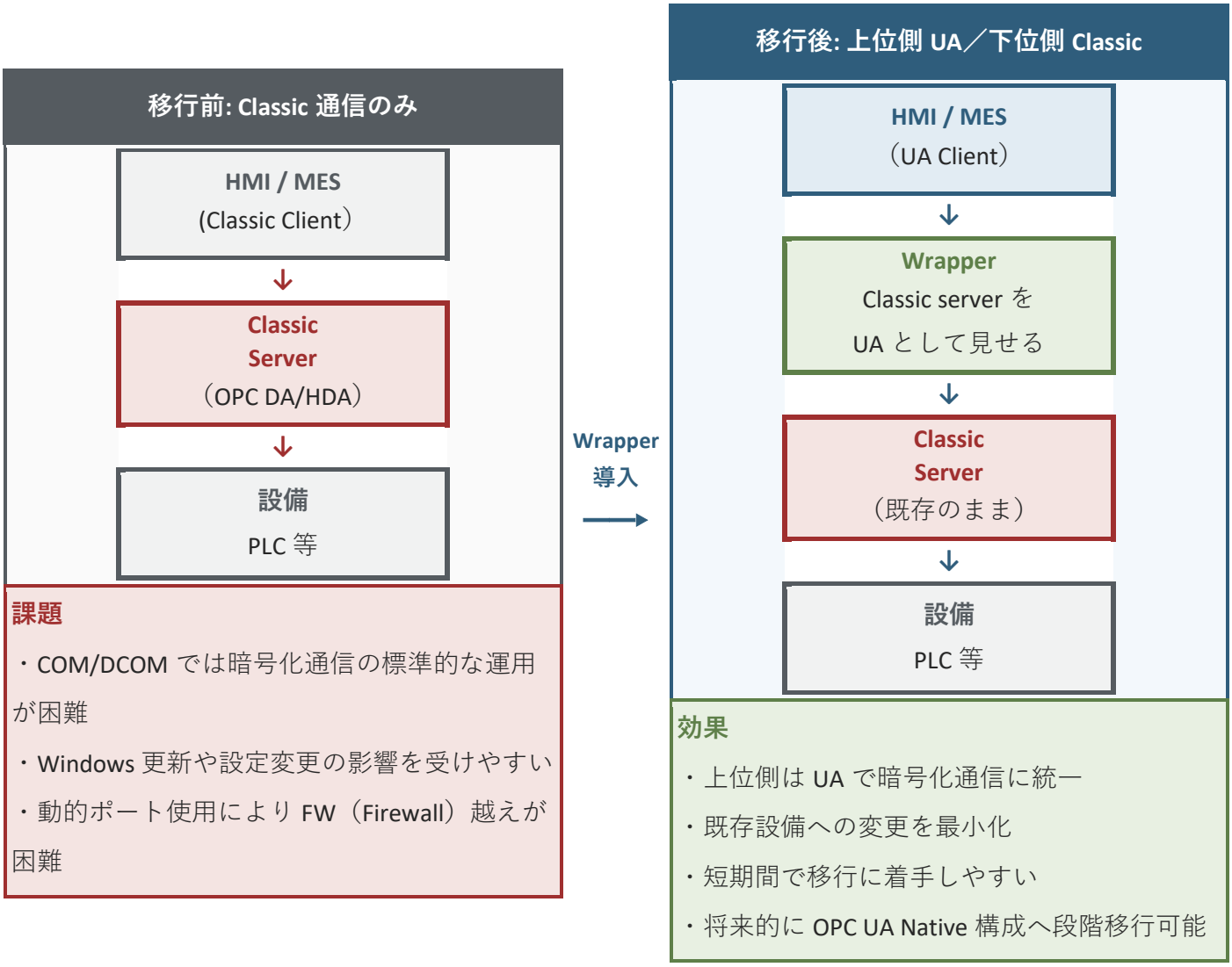
Wrapper / Proxy は、既存資産を残しながら OPC UA へ接続するための暫定的な橋渡しです。

Gateway は、複数設備や複数方式のデータを OPC UA に集約する方式です。

Native 化は、Classic / DCOM を廃止し、OPC UA を直接利用する最終構成として位置づけます。

図 7-3: Wrapper 方式

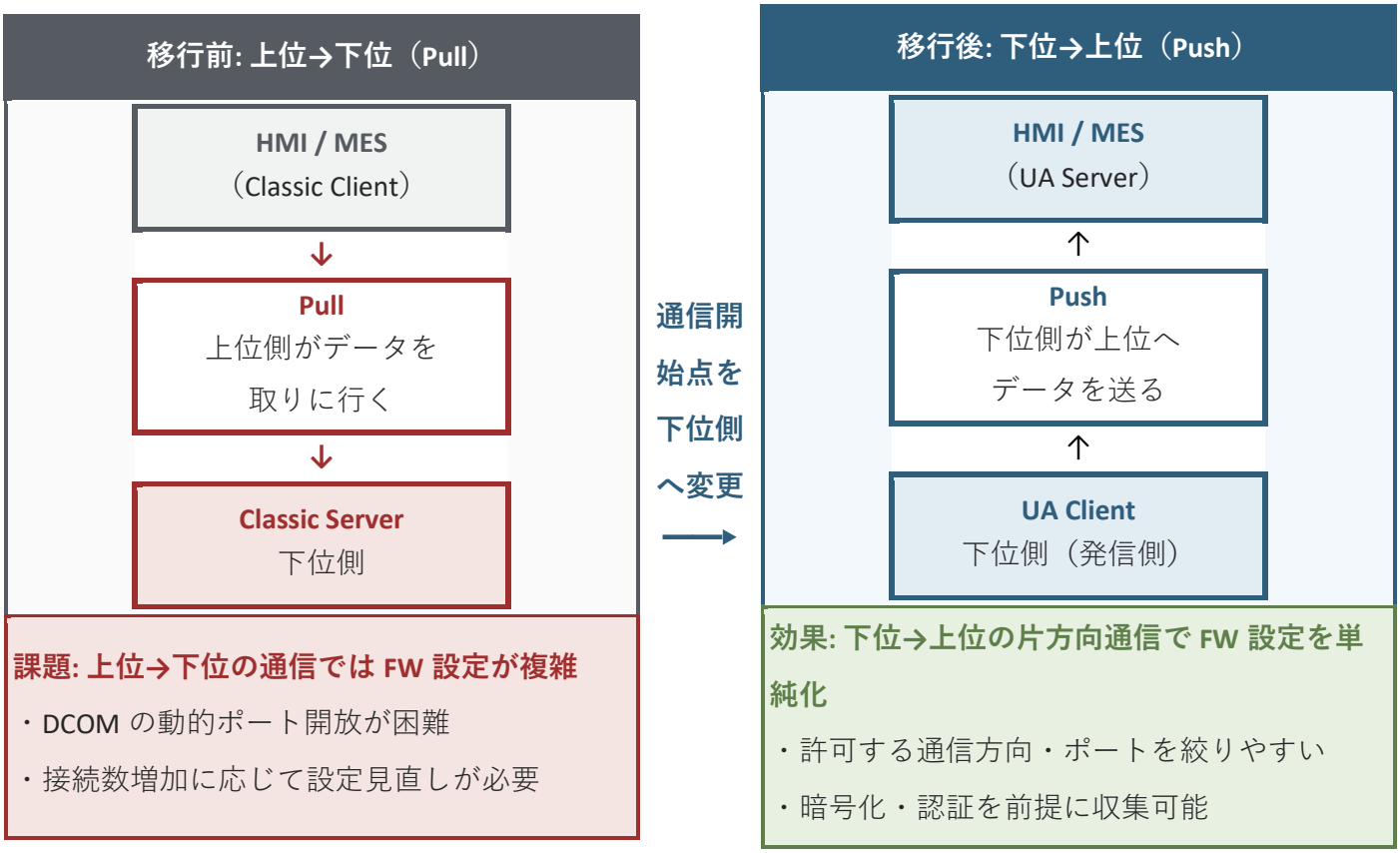
既存 Classic Server を残したまま、Wrapper を介して上位側から OPC UA で接続できるようにする方式



Created With DALL-E

図 7-4: 下位側起点接続

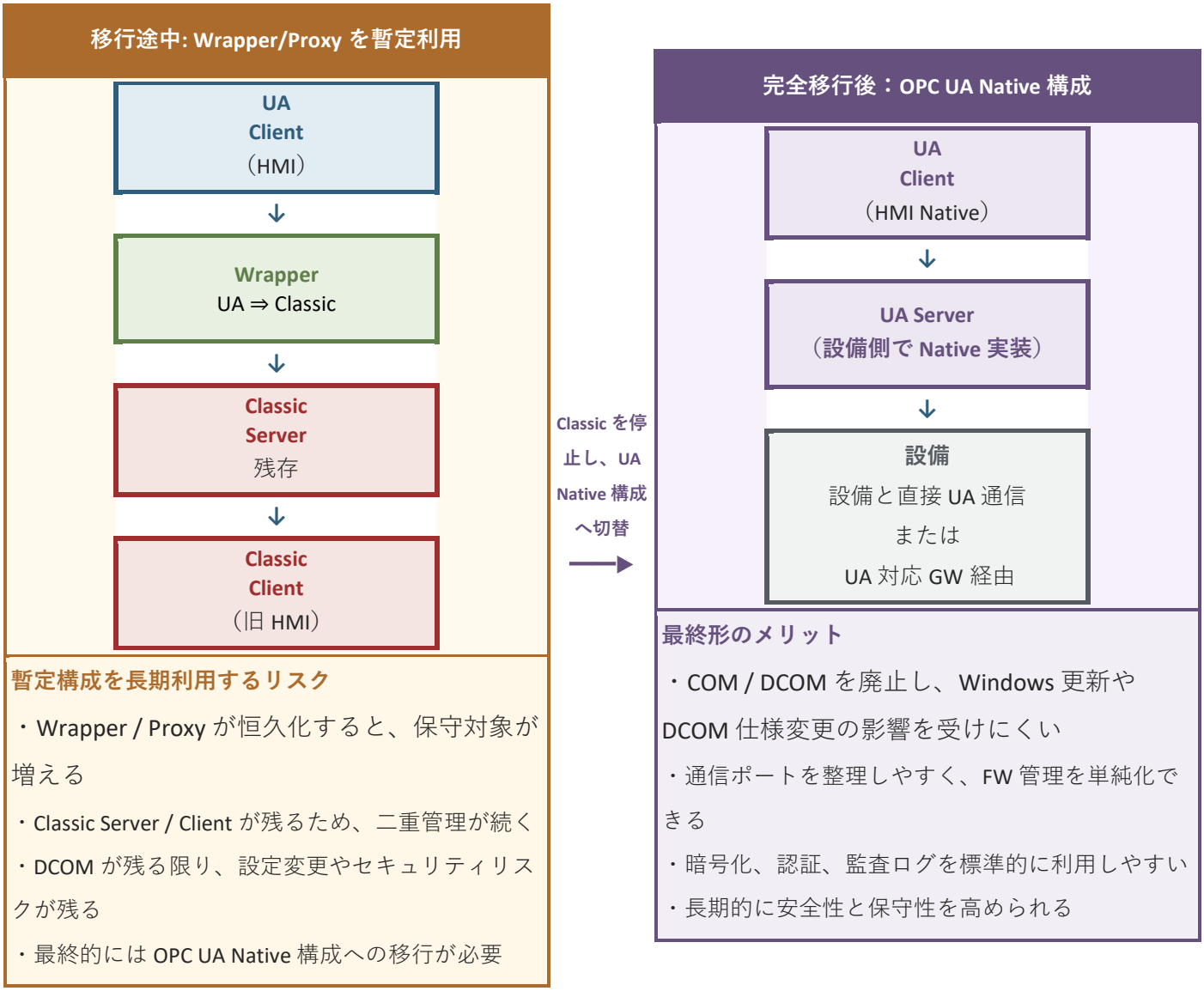
上位側から取りに行く通信を減らし、下位側から発信（Push）するパターン



Created With DALL-E

図 7-5: 完全移行

Wrapper/Proxy は移行途中の暫定手段とし、最終的には Classic Server / Client を廃止して OPC UA Native 構成へ移行する方式

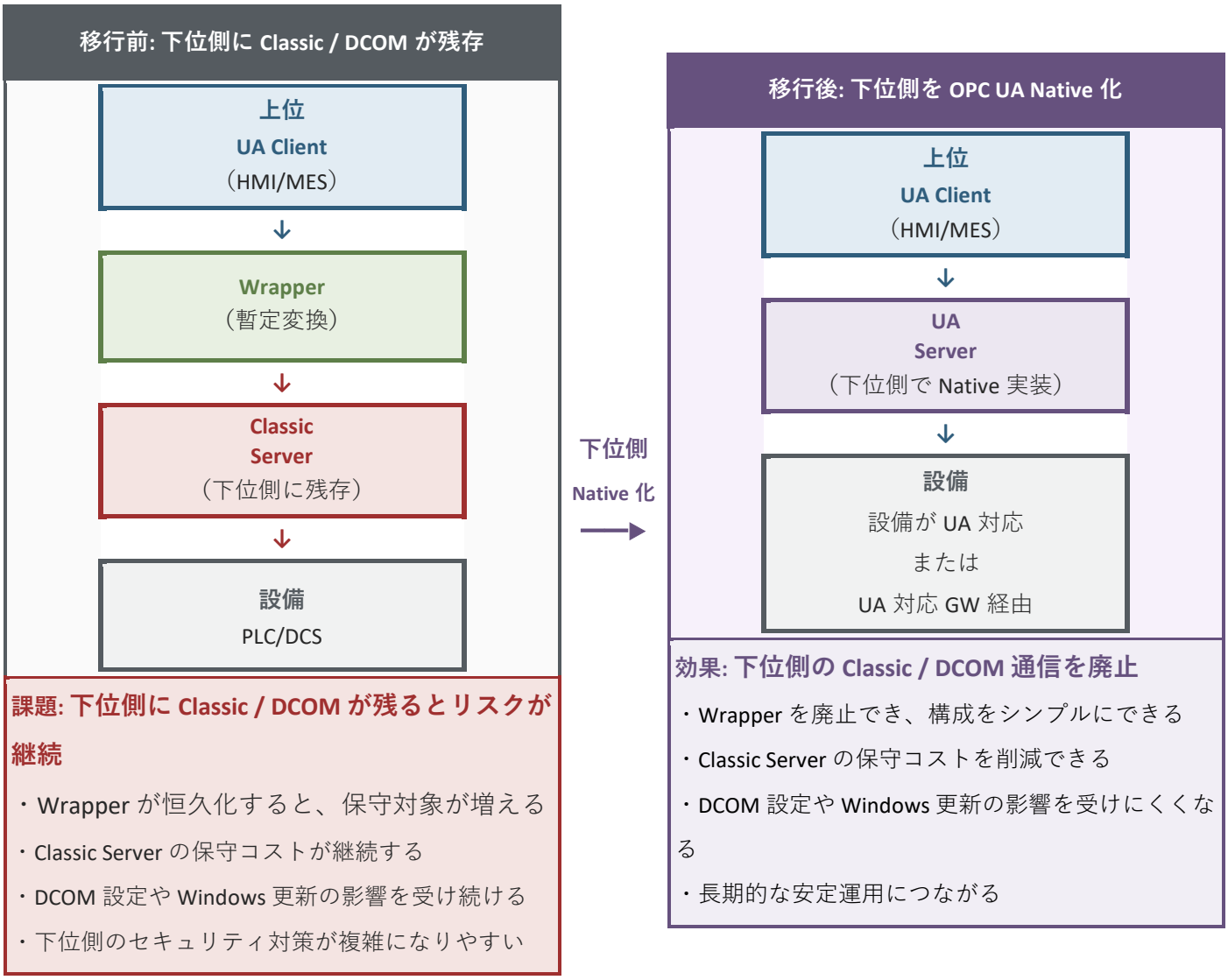


Created With DALL-E

図 7-6：下位側の OPC UA Native 化

下位側に残っている Classic Server や転送アプリを OPC UA Native に置き換え、

Classic / DCOM 通信を廃止する方式



Created With DALL-E

共通凡例: 図の色と記載の意味

図中の色は、OPC UA 移行における通信方式・変換層・残存リスクを識別するために用います。

色／表記	意味	具体例
赤（Classic / DCOM）	OPC Classic、COM / DCOM を利用する領域。OPC UA 標準の暗号化・認証・証明書管理の対象外。	Classic Server、Classic Client、DCOM 通信線
青（OPC UA）	OPC UA 通信を利用する領域。暗号化・認証・証明書運用の対象。	UA Client、UA Server、OPC UA 通信線
緑（変換・集約）	既存構成を残しながら、OPC UA との接続や複数設備の集約を行う領域。	Wrapper、Proxy、Gateway
紫（OPC UA Native）	機器・アプリが OPC UA を直接実装し、Classic / DCOM に依存しない領域。	OPC UA Native 対応機器、OPC UA Native 対応アプリ

活用方法

図 7-1・7-2 で移行方針の全体像を確認し、図 7-3 から図 7-6 で Classic / DCOM が残る箇所、責任分界、廃止時期を確認します。

赤色の領域が残る場合は、残す理由・管理方法・見直し時期を明確にします。

7.3 A/B/C 分類で優先順位を付ける

棚卸しの結果をもとに、すぐに移行すべきものと、更新時期に合わせて対応するものを分けます。重要なのは、すべてを A にしないことです。全部を最優先にすると、結局どれも進まなくなります。現場影響・コスト・停止可否を見ながら、現実的な順番を決めます。

A/B/C 分類を行う際は、付録 A「接続・移行確認表」に記録した停止影響、Classic/DCOM 残置、保守期限、書き込み有無、更新予定を確認します。詳細な点数化を行わない場合でも、A/B/C 分類、判断理由、次の対応を残すことで、後から判断の経緯を確認できます。

分類	判断の目安	推奨対応
A（最優先）	止まると影響が大きい／古い OS に依存／Classic 残置リスクが高い	先行して計画化する（3 か月以内に計画着手）
B（計画的）	重要だが、すぐに更新しなくてもよい	設備更新やシステム更新に合わせて移行する
C（様子見）	現時点では影響が小さい	残置管理し、期限を決めて定期的に見直す

7.4 移行のきっかけとなるイベント

既存システムの OPC UA 移行は、単独プロジェクトとして進めるよりも、既存の更新タイミングに合わせる方が、コストを抑えやすく、現場の負担も軽くなります。以下のイベントを、既存接続の移行、段階移行、または残置見直しの「きっかけ」として活用してください。新規導入や全面刷新時の方式選定は、次節の Native 方式を含めて検討します。

移行のきっかけ	確認すべきこと
OS 更新	Windows 更新による DCOM 影響、証明書、ファイアウォール設定
設備更新	下位機器が OPC UA に対応しているか
上位システム更新	Gateway や Wrapper を継続するか、最初から UA 対応のシステムに置き換えるか（Native 化）
証明書更新	信頼する相手リスト（Trust List）の更新、期限切れ証明書の処理、再接続テスト
監査対応・顧客要望	設定根拠、権限管理、ログ保全、例外管理、Classic 残置理由、見直し時期

【効果】 この考え方により、二重投資を抑えながら、Classic 依存のリスクを少しずつ減らせます。

7.5 移行方式の選び方

OPC UA 移行には複数の技術的アプローチがあります。自社の状況に応じて、最適な方式を選択してください。各方式の技術的な前提（Wrapper/Proxy の定義、Gateway 運用時の確認項目など）は第 6 章を参照してください。

ユーザ側負担欄の見方：ここでいう負担は、ライセンス費用だけでなく、システム停止範囲、上位改修量、設定変更、検証工数、保守継続を含めた総合的な負担感を示します。

方式選定では、導入しやすさだけで判断しないでください。特に Wrapper や Gateway を使う場合、上位側から UA 接続に見えても、下位側に Classic 区間が残ることがあります。表 7-3 の通信方式、UA 対応可否、タグ数、更新周期、書き込み有無、品質情報、タイムスタンプ、ログ確認先を踏まえて、方式を選定します。

方式	概要	導入しやすさ	ユーザ側負担	Classic 依存	選定目安
Wrapper（ラッパー）方式	既存設備を変更せず、UA サーバとして見せる	◎ 容易	小：既存設備流用、停止範囲小	残る	まず移行を始めたい
Proxy（プロキシ）方式	Proxy が間に入り、既存の Classic クライアントはそのままで、UA サーバへつなげる	◎ 容易	小〜中：上位変更抑制、変換管理が必要	クライアント側に残る	クライアント側を変更できない
Gateway（ゲートウェイ）方式	複数種類の Classic 通信（リアルタイム値＝DA、アラーム＝A&E、履歴＝HDA）をまとめて UA 化	○ 中程度	中〜大：複数通信の統合・検証が必要	一部残る	DA/A&E/HDA を統合したい
Native（ネイティブ）方式	最初から UA 対応機器・システムを採用	× 高難度	大：設備・上位双方の更新が必要	残らない	新規開発や全面刷新時

※Wrapper/Proxy の考え方は、OPC Foundation “OPC Unified Architecture - Part 8: Data Access”, Annex A “OPC COM DA to UA mapping” を参照して整理しています。

【判断の目安】 既存の OPC Classic サーバを維持しつつ、上位側から段階的に UA 化したい場合は、Wrapper 方式が候補になりやすいです。既存設備を流用しやすく、停止範囲と初期負担を抑えて移行を開始できます。段階的に Gateway（ゲートウェイ）や Native（ネイティブ）へステップアップできます。ただし下位側の Classic 区間は残るため、第 6 章の Gateway/Wrapper 運用上の確認項目を併せて参照してください。

7.6 関係者と役割の整理

OPC UA 移行は IT 部門だけでは進められません。現場・設備・情報システム・セキュリティ・ベンダー・経営層が、それぞれ何を担当するかを最初に決めておきます。

関係者	主な役割
製造部門	接続用途、停止影響、書き込み要否を伝える
設備管理・保全部門	停止可能時期、設備更新時期、保守依存先を整理する
情報システム部門	OS、端末、ネットワーク、ログ保存を管理する
セキュリティ部門	証明書、認証方式、Trust List、例外承認を決める
ベンダー	UA 対応可否、設定支援、トラブル時にどこまでがベンダーの責任か（責任分界）を確認する
経営層	優先順位、予算、段階移行方針を承認する

7.7 本章のまとめ

本章では、第 6 章で棚卸しした接続をもとに、A/B/C 分類、移行きっかけイベント、4 方式の選択、役割分担、経営説明という 5 つの判断軸を整理しました。次章以降では、これらを実務に落とすためのチェックポイント（第 8 章）と、導入後の継続運用（第 9 章）を扱います。

第 8 章　移行前後の確認事項

本章で分かること

移行前、Classic 残置、Gateway/Wrapper 利用時、導入直後、変更時に何を確認すべきかが分かります。

8.1 本章の目的と使い方

ここでいう OPC Classic とは、OPC DA、OPC HDA、OPC A&E など、COM/DCOM を基盤として利用してきた従来型 OPC 仕様群の総称です。OPC DA はその代表的な方式で、本書では主に OPC DA を対象に扱います。特にリモート接続では、Windows の COM/DCOM、RPC、権限設定、ファイアウォール設定の影響を受けます。

DCOM は、Windows 上のアプリケーション同士が通信する仕組みで、OPC DA で使われることが多いです。Gateway、Wrapper、Proxy 等は、中継ソフト・装置の実装例として扱い、OPC UA 仕様上の一般概念とは区別します。

本章の表は、合否判定だけを目的とするものではありません。現場が確認すべき対象を順に洗い出し、未確認事項、追加検証事項、ベンダー確認事項、第 9 章へ引き渡す事項を明確にするために使用します。

表 8-1 本章で確認するステップ

確認ステップ	何を確認するか	使う表	次に取る対応	主な関係者
確認対象の選定	どの接続から確認するか	表 8-2	代表接続を選び、表 8-3 へ進む	製造、保全、情シス
接続の把握	接続元、接続先、用途、書き込み有無	表 8-3	Classic 残置、移行成立性、中継構成の確認へ進む	製造、保全、ベンダー
Classic 残置の確認	OPC Classic/DCOM が残る区間、理由、復旧性	表 8-4	第 5 章の経営リスク説明、第 7 章の分類へ反映する	保全、情シス、ベンダー
移行成立性の確認	技術、性能、セキュリティ、保守、体制	表 8-5	移行可否、追加検証、ベンダー確認事項を整理する	製造、保全、情シス、ベンダー
Gateway/Wrapper 利用時確認	変換区間、タグ、品質情報、時刻、ログ確認先	表 8-6	中継構成のリスクと追加確認事項を整理する	情シス、保全、ベンダー
導入直後の受入確認	接続、タグ、品質、書き込み、ログ確認先	表 8-7	受入可否を判断し、第 9 章へ引き渡す情報を整理する	製造、保全、情シス、ベンダー
変更時確認	OS 更新、証明書更新、設備更新、ネットワーク変更	表 8-8	変更影響を確認し、必要に応じて再試験・引き継ぎを行う	情シス、保全、設備管理、ベンダー

8.2 確認対象を決める

すべての OPC 接続を一度に詳細確認するのは現実的ではありません。まず、操業影響、書き込み有無、Classic 残置、保守期限、属人性、データ活用への影響から、優先して確認する代表接続を選びます。推奨は、止まると困る接続、保守期限が近い接続、上位システムやデータ活用に関係する接続の 3 件程度です。

表 8-2 確認対象を選ぶ観点

観点	確認内容	優先的に確認する対象	確認結果の目安	次に取る対応
操業影響	接続停止時に、監視、記録、品質確認、帳票、操作へ影響するか	止まると工程や品質判断に影響する接続	影響大／影響小／未確認	影響大の接続から表 8-3 へ進む
書き込み有無	読み取りだけか、設定値や制御値の書き込みを伴うか	書き込みあり、または書き込み可否が不明な接続	なし／あり／不明	あり・不明の場合は表 8-3、表 8-5 で詳細確認
Classic 残置	OPC Classic や DCOM が残っている可能性があるか	旧設備、旧 OS、Gateway 経由の接続	なし／あり／不明	あり・不明の場合は表 8-4 へ進む
保守期限	OS、OPC サーバ、Gateway、上位端末の保守期限が近いか	保守期限が近い、または不明な接続	余裕あり／期限近い／不明	期限近い・不明の場合は第 7 章の分類へ反映
属人性	設定内容や復旧手順を説明できる人がいるか	特定担当者や旧ベンダーに依存している接続	説明可能／一部可能／不明	不明の場合は確認先を整理し、表 8-3 へ進む
データ活用	MES、Historian、品質分析、帳票に使われているか	上位システムや分析基盤に関係する接続	関係あり／なし／不明	関係ありの場合はタグ、品質情報、時刻を重点確認
更新予定	設備更新、OS 更新、上位システム更新と関係するか	近く更新予定がある接続	更新予定あり／なし／不明	更新予定ありの場合は表 8-8 も確認する

8.3 接続の把握

OPC 接続の確認では、機器名や IP アドレスだけでなく、接続の用途、書き込み有無、品質情報、タイムスタンプ、ログ確認先を確認します。これらが分からないと、移行成立性、Gateway/Wrapper 利用時の影響、導入直後の受入確認を判断しにくくなります。

表 8-3 OPC 接続確認表

確認項目	用語の補足	確認内容	確認先・確認方法	確認結果の目安	次に取る対応
接続元・接続先	どの機器・ソフトが、どこへつながるか	PLC、DCS、OPC サーバ、Gateway、上位端末の関係を確認する	構成図、現場確認、ベンダー確認	一致／差異あり／不明	差異あり・不明の場合は構成図を補正し、関係者へ確認
通信方式	OPC Classic、OPC UA、Gateway 経由などの通信方法	OPC Classic、OPC UA、Gateway 経由、Wrapper 経由のどれかを確認する	製品設定、接続設定、ベンダー確認	UA のみ／Classic あり／不明	Classic あり・不明の場合は表 8-4 へ進む
用途	その接続を何に使っているか	監視、記録、帳票、品質確認、制御、保守のどれかを確認する	製造、品質管理、保全への聞き取り	明確／一部不明／不明	不明な用途は停止影響を確認し、表 8-2 へ戻す
書き込み有無	上位側から値や設定を変更できるか	読み取りのみか、設定値・制御値の書き込みがあるかを確認する	画面、設定、操作手順、ベンダー確認	なし／あり／不明	あり・不明の場合は表 8-5、表 8-7 で重点確認
公開タグ・取り込みタグ	上位へ見せる、または中継ソフトが取り込むデータ項目	どのタグ群を公開・取り込みしているかを確認する	OPC クライアント、Gateway 設定、上位システム	範囲明確／過不足あり／不明	過不足あり・不明の場合は表 8-6 で確認
品質情報	データが正常か異常かを示す情報	Good、Bad、Uncertain などが確認できるか	クライアント画面、上位システム表示、ログ	確認済／確認不可／未確認	確認不可・未確認の場合は表 8-6 または表 8-7 で再確認
タイムスタンプ	データに付く時刻情報	元データ時刻、中継時刻、上位取得時刻のどれを使うか確認する	製品設定、上位システム、ベンダー確認	意味明確／複数あり／不明	不明の場合は品質記録・帳票への影響を確認
ログ確認先	異常時に見る記録の場所	接続失敗、認証失敗、証明書エラー、書き込み履歴をどこで見るか確認する	OPC サーバ、Gateway、Windows イベントログ、上位端末	確認先明確／一部不明／不明	不明の場合は表 8-7 で受入前に確認し、第 9 章へ引き継ぎ

確認結果は、「確認済／未確認／差異あり／不明」などの状態で残します。

8.4 Classic 残置の把握

OPC UA クライアントから接続できるようになっても、下位側や中継区間に OPC Classic/DCOM が残る場合があります。この場合、UA 化された範囲と Classic が残る範囲を分けて確認する必要があります。特に、残置理由、残置期間、OS 更新時の影響、復旧性は、保守継続性や経営リスクの説明に関係します。

表 8-4 Classic 残置確認表

確認項目	用語の補足	確認内容	確認先・確認方法	確認結果の目安	次に取る対応
残置区間	Classic が残る通信区間	PLC－OPC Classic サーバ間、OPC Classic サーバ Gateway 間など、Classic/DCOM が残る場所を確認する	構成図、接続設定、ベンダー確認	なし／あり／不明	あり・不明の場合は残置理由を確認
残置理由	なぜ UA 化できないか	PLC が UA 非対応、設備更新待ち、ベンダー制約などを確認する	設備仕様、保守契約、ベンダー確認	明確／一部不明／不明	不明の場合はベンダー確認事項にする
残置期間	いつまで残るか	一時的か、次回設備更新までか、当面継続かを確認する	設備更新計画、保守計画	期限あり／期限なし／不明	期限なし・不明の場合は第 7 章の分類と第 9 章の残置管理へ引き継ぎ
DCOM 影響	Windows 上のアプリ間通信の仕組み	DCOM 設定、Windows 権限、ファイアウォールが通信に関係するか確認する	情シス、ベンダー、設定資料	影響あり／影響なし／不明	影響あり・不明の場合は OS 更新時に表 8-8 で再確認
OS 更新影響	Windows 更新で通信に影響する可能性	OS 更新後に OPC Classic 通信が維持できるか、事前確認が必要かを見る	情シス、保全、ベンダー	確認済／要確認／不明	要確認・不明の場合は変更時確認に追加
復旧性	故障時に同じ接続状態へ戻せるか	端末交換、アプリ再導入、設定復元の手順があるか確認する	手順書、担当者、ベンダー	復旧可能／手順不足／不明	手順不足・不明の場合は第 9 章へ引き継ぎ
解消候補	Classic をなくす機会	設備更新、上位更新、Gateway 更新時に UA 化できるか確認する	設備管理、ベンダー	解消候補あり／当面困難／不明	解消候補ありの場合は第 7 章の段階移行へ反映

Classic を残すこと自体を否定するのではなく、残る理由、期限、影響、復旧性を説明できるかを確認します。継続管理は第 9 章で扱います。

8.5 移行成立性の確認

OPC UA 移行は、接続できるかだけでは判断できません。タグ数や更新周期が業務に合うか、書き込み範囲が意図どおり制限されるか、障害時にどのログを誰が確認するか、OS や OPC サーバ更新時に再確認できるかを合わせて確認する必要があります。

表 8-5 移行成立性チェック

観点	用語の補足	確認内容	確認先・確認方法	確認結果の目安	次に取る対応
技術	UA 対応、タグ変換、名前空間など	対象機器・ソフトが UA 接続に対応し、タグ階層や名前空間を扱えるか確認する	仕様書、ベンダー確認、接続試験	成立／条件付き／未確認	条件付き・未確認の場合は追加検証を計画
性能	タグ数、更新周期、遅延など	必要なタグ数、更新周期、遅延、欠損許容に収まるか確認する	性能試験、上位システム確認	成立／要検証／不成立	要検証の場合は試験条件を定義
セキュリティ	証明書、認証、暗号化など	証明書、認証方式、暗号化、書き込み制限が確認できるかを見る	情シス、セキュリティ、ベンダー	確認済／一部未確認／未確認	未確認項目は導入直後確認と第 9 章へ引き継ぎ
書き込み制限	上位側から値を変更できる範囲	書き込み可能タグが必要最小限か、読み取り専用接続に書き込み経路が残っていないか確認する	画面、権限設定、操作試験	制限確認済／過大疑い／不明	過大疑い・不明の場合は受入前に是正または例外扱い
保守	更新や障害対応を継続できるか	OS 更新、OPC サーバ更新、Gateway 更新時に再確認できるか	保守契約、更新計画、ベンダー確認	対応可能／要調整／不明	要調整・不明の場合は第 7 章の段階移行へ反映
体制	誰が確認・復旧・判断するか	製造、保全、情シス、ベンダーの役割が明確か確認する	関係者レビュー	明確／一部不明／不明	不明の場合は責任分界を整理
切戻し	問題時に元に戻す方法	移行後に問題が出た場合の切戻し条件と手順があるか確認する	作業計画、ベンダー確認	あり／不足／なし	不足・なしの場合は移行前に補強

8.6 Gateway/Wrapper 利用時の確認

Gateway、Wrapper、Proxy 等の中継ソフト・装置を使う場合に、変換区間、公開タグ、取り込みタグ、品質情報、タイムスタンプ、書き込み経路、ログ確認先を確認します。

Gateway/Wrapper を使うと、上位システムからは UA 化されたように見える場合があります。しかし、中継区間に Classic が残ることや、公開タグ、取り込みタグ、品質情報、タイムスタンプ、書き込み可否、ログ確認先が中継ソフト・装置の設定に依存することがある。製品名だけで判断せず、構成上どの区間を変換しているかを確認します。

表 8-6 Gateway/Wrapper 利用時の確認表

確認項目	用語の補足	確認内容	確認先・確認方法	確認結果の目安	次に取る対応
変換区間	どこで通信方式を変えているか	Classic から UA、UA から UA など、どの区間を中継しているか確認する	構成図、製品設定、ベンダー確認	明確／一部不明／不明	不明の場合は構成図を補正し、表 8-4 も確認
中継方式	Gateway、Wrapper、Proxy 等の中継方式	中継ソフト・装置がどの役割を担っているか確認する	製品名、設定画面、ベンダー確認	明確／一部不明／不明	製品名だけでなく構成上の役割を確認
公開タグ範囲	上位へ見せるタグの範囲	上位システムへ公開するタグが必要範囲に収まっているか確認する	Gateway 設定、上位システム	適正／過不足あり／不明	過不足あり・不明の場合はタグ範囲を見直す
取り込みタグ範囲	中継ソフトが読み込むタグの範囲	中継ソフト・装置に取り込むタグが意図どおりか確認する	中継ソフト設定、検証結果	適正／過不足あり／不明	過不足あり・不明の場合は設定確認を追加
品質情報	値が正常か異常かを示す情報	Good/Bad/Uncertain の有無だけでなく、Classic 側品質情報が UA 側 StatusCode へどう変換されるか、ベンダー固有品質情報が失われないか確認する	クライアント画面、上位表示、ログ、ベンダー確認	意味まで確認済／値のみ確認／未確認	値のみ確認・未確認の場合は受入前に再確認
タイムスタンプ	データに付く時刻	元データ時刻、Wrapper/Gateway 処理時刻、上位システム取得時刻のどれを表示・記録しているか確認する	製品設定、上位システム、ベンダー確認	意味明確／複数あり／不明	帳票、品質記録、トレーサビリティへの影響を確認
書き込み経路	中継経由で値を変更できる経路	Gateway 経由で書き込み可能なタグがあるか確認する	設定、操作試験、ベンダー確認	なし／あり／不明	あり・不明の場合は表 8-5、表 8-7 で重点確認

確認項目	用語の補足	確認内容	確認先・確認方法	確認結果の目安	次に取る対応
ログ確認先	異常時に見る記録の場所	OPC サーバ、Gateway、中継ソフト、上位端末、Windows ログのどこを見るか確認する	管理画面、ログ設定、ベンダー確認	明確／一部不明／不明	不明の場合は導入直後確認までに確認
障害時挙動	切断や再接続時の動き	切断、再接続、証明書エラー、タグ欠損時の挙動を確認する	試験、ベンダー確認、ログ	確認済／要検証／未確認	要検証・未確認の場合は追加試験を計画

品質記録、帳票、トレーサビリティに使う接続では、値が合っていても品質情報やタイムスタンプの意味が変わると運用上の問題になります。中継ソフト・装置を使う場合は、値だけでなく、品質情報と時刻の意味を確認します。暫定利用の期限管理や定期見直しは第 9 章で扱います。

8.7 導入直後の受入確認

導入直後の受入確認では、接続できたかだけでなく、値・品質情報・時刻・書き込み範囲・ログ確認先を見ます。第 8 章では受入確認までを扱い、その後の証明書、Trust List、権限、ログの維持管理は第 9 章で扱います。

表 8-7 導入直後の受入確認表

確認項目	用語の補足	確認内容	確認先・確認方法	確認結果の目安	次に取る対応
接続確認	UA クライアントから接続できるか	想定した接続先、Endpoint、通信経路で接続できるか確認する	OPC UA クライアント、サーバ設定	OK／差異あり／NG	差異あり・NG の場合は設定を確認し、受入保留
Endpoint/MessageSecurityMode/SecurityPolicy 確認	Endpoint（接続先 URL）、MessageSecurityMode（通信保護モード）、SecurityPolicy（通信保護方式）	想定 Endpoint（接続先 URL）、MessageSecurityMode（通信保護モード）、SecurityPolicy（通信保護方式）が使用されているか、MessageSecurityMode None または SecurityPolicy None が残っていないか確認する	UA クライアント、サーバ設定、Endpoint 一覧	OK／例外あり／NG	例外あり・NG の場合は受入保留または第 9 章の例外管理へ引き継ぎ

確認項目	用語の補足	確認内容	確認先・確認方法	確認結果の目安	次に取る対応
証明書確認	接続相手を確認する電子的な証明	証明書エラーなく接続できるか確認する	クライアント画面、サーバログ	OK／警告あり／NG	警告あり・NG の場合は証明書設定を確認し、第 9 章へ引き継ぎ
Trust List 反映確認	信頼する相手証明書の一覧	クライアント・サーバ双方で必要な証明書または CA が Trust List に登録され、不要な証明書が使われていないか確認する	証明書ストア、Trust List、接続ログ	OK／過不足あり／不明	過不足あり・不明の場合は設定根拠を残して第 9 章へ引き継ぎ
認証確認	誰が接続できるかを確認する仕組み	想定した認証方式で接続できるか確認する	認証試験、ユーザ設定	OK／例外あり／NG	例外ありの場合は第 9 章の例外管理へ引き継ぎ
Anonymous 確認	Anonymous（利用者を識別しない接続）。UserTokenPolicy（接続時に使える認証方式の設定）で確認する	Anonymous 接続が許可されていないか、許可する場合は理由と範囲が説明できるか確認する	UserTokenPolicy（認証方式設定）、接続試験、サーバ設定	無効／例外あり／不明	例外あり・不明の場合は第 9 章の例外管理へ引き継ぎ
タグ確認	データ項目の名称や階層	値、単位、タグ名、階層が現場の想定どおりか確認する	現場値との照合、上位画面	OK／差異あり／未確認	差異あり・未確認の場合はタグ範囲を再確認
品質確認	値が正常か異常かを示す情報	品質情報が確認でき、Classic/UA 変換時に意味が変わっていないか確認する	クライアント画面、上位システム、ベンダー確認	OK／意味未確認／未確認	意味未確認・未確認の場合は受入前に再確認
時刻確認	データに付く時刻	元データ時刻、中継処理時刻、上位取得時刻のどれを表示・記録しているか説明できるか確認する	上位表示、設定、ベンダー確認	OK／不明点あり／未確認	不明点ありの場合は帳票・品質記録への影響を確認
書き込み確認	上位から値を変更できる範囲	書き込み可能範囲が意図どおり制限されているか確認する	権限設定、操作試験	OK／過大疑い／未確認	過大疑い・未確認の場合は受入保留または例外扱い
ログ確認	異常時に見る記録	接続失敗、認証失敗、証明書エラー、書き込み履歴を確認できるか見る	サーバログ、Gateway ログ、OS ログ	確認先明確／一部不明／不明	不明の場合は第 9 章へ引き継ぎ前に確認先を決める
引き継ぎ確認	継続管理に渡す情報	設定根拠、確認結果、担当者、復旧手順の所在が確認できるか	関係者レビュー	引き継ぎ可／不足あり／未確認	不足あり・未確認の場合は第 9 章へ渡す項目を整理

8.8 変更時の確認

OPC 接続は、設備そのものを変更しない場合でも、OS 更新、証明書更新、ネットワーク変更、上位端末追加、Gateway 更新によって影響を受ける場合があります。変更時には、接続、タグ、品質情報、タイムスタンプ、書き込み可否、ログ確認先、Classic 残置の有無を再確認します。

表 8-8 変更時確認表

変更イベント	用語の補足	確認すること	確認先・確認方法	確認結果の目安	次に取る対応
OS 更新	Windows やサーバ OS の更新	OPC 通信、サービス起動、証明書ストア、ログ、DCOM/RPC 設定、DCOM 強化変更の影響、ファイアウォール許可範囲を確認する	情シス、保全、ベンダー、更新試験	影響なし／要再設定／未確認	要再設定・未確認の場合は更新前に試験または切戻し準備
証明書更新	接続相手を確認する証明の更新	有効期限、新旧証明書、Trust List 反映、接続確認を行う	証明書管理画面、接続試験	OK／警告あり／NG	警告あり・NG の場合は第 9 章の証明書管理へ引き継ぎ
設備更新	PLC、DCS、サーバ等の更新	タグ変更、接続先変更、書き込み有無、Classic 残置有無を確認する	設備仕様、現場確認、ベンダー確認	影響なし／変更あり／未確認	変更ありの場合は表 8-3～表 8-6 を再確認
OPC サーバ更新	OPC 通信ソフトの更新	設定移行、互換性、品質情報、ログ、切戻し手順を確認する	ベンダー、更新試験、ログ確認	OK／差異あり／NG	差異あり・NG の場合は設定差分を確認
Gateway／中継ソフト更新	Gateway、Wrapper、Proxy 等の中継ソフト・装置の更新	変換設定、公開タグ、取り込みタグ、品質情報、タイムスタンプ、書き込み経路、ログ確認先を確認する	中継ソフト設定、上位表示、ベンダー確認	OK／差異あり／未確認	差異あり・未確認の場合は表 8-6 を再確認
ネットワーク変更	IP、FW、セグメント変更など	OPC UA は Endpoint ごとのポート・名前解決、Classic/DCOM は RPC 動的ポート・通信方向を確認します。FW、セグメント、NAT 有無も確認する	情シス、ネットワーク担当、通信試験	影響なし／要設定変更／未確認	要設定変更の場合は接続試験を実施

変更イベント	用語の補足	確認すること	確認先・確認方法	確認結果の目安	次に取る対応
上位端末追加	MES、Historian、監視端末などの追加	証明書、Trust List、認証方式、UserTokenPolicy（認証方式設定）、公開タグ範囲、ログ確認先を確認する	接続試験、設定確認、ベンダー確認	OK／例外あり／NG	例外ありの場合は第 9 章へ引き継ぎ
タグ追加・変更	データ項目の追加・変更	用途、公開範囲、品質情報、タイムスタンプ、書き込み可否を確認する	製造、品質管理、上位担当	影響なし／影響あり／未確認	影響ありの場合は受入確認を再実施

「UA なら OS 更新の影響がない」とは扱いません。OPC UA でも、証明書ストア、サービス起動、ファイアウォール、Endpoint、名前解決、時刻同期、ログ設定の影響を受ける場合があります。Classic 残置がある接続では、DCOM/RPC 設定、RPC 動的ポート、Windows イベントログも確認対象に含めます。変更申請、承認フロー、台帳更新、定期レビュー、例外期限管理は第 9 章で扱います。

8.9 本章のまとめ

本章で確認した結果のうち、設定根拠、証明書、Trust List、認証、権限、ログ、変更管理、例外管理として継続的に維持すべきものは、第 9 章「導入後の継続運用」で扱います。

証明書は第 8 章では導入直後・変更時に接続できるかを確認し、第 9 章で有効期限、更新、削除、配置先を継続管理します。Trust List は第 8 章では接続時に信頼設定が反映されているかを確認し、第 9 章で登録理由、承認者、棚卸し、不要証明書削除を管理します。認証、権限、ログ、Gateway/Wrapper、Classic 残置についても同様に、第 8 章では確認と受入、第 9 章では維持管理を扱います。

本章の確認項目は、IPA 制御システムセキュリティ関連資料、IEC 62443、NIST SP 800-82、OPC UA Specification Part 2: Security Model、The OPC UA Security Model for Administrators、OPC UA Specification Part 4: Services、Microsoft DCOM Hardening、Gateway/Wrapper 関連資料に対応しています。詳細な出典一覧は巻末の参考資料一覧にまとめます。

付録との関係

本章で確認した結果は、付録 A「接続・移行確認表」および付録 C「変更・例外・定期レビュー表」に記録します。導入直後や変更時に確認した証明書、Trust List、認証方式、書き込み権限、

ログ確認先、例外設定のうち、継続的に管理すべき項目は、第 9 章および付録 B「運用管理表」へ引き継ぎます。

第 9 章　導入後の継続運用

本章で分かること

OPC UA 導入後に、何を記録し、何を定期レビューし、何を変更管理すべきかが分かります。本章は「維持する章」です。第 8 章で確認した結果を、導入後も見直せる管理情報として残すことを扱います。OPC UA は証明書、Trust List、認証、通信保護設定、権限、ログなどを扱える仕組みを備えていますが、導入すれば自動的に安全な状態が維持されるわけではありません。

9.1 本章の目的

重要なのは、設定値だけではなく、なぜその設定にしたか、誰が承認したか、いつ見直すかを確認できる状態にすることです。これにより、端末更新、OS 更新、設備更新、監査、障害対応、担当者交代に備えることができます。まずは証明書期限、Trust List、書き込み権限、ログ確認先、例外期限など、接続停止や説明困難につながりやすい項目から優先して管理します。

OPC UA への移行は、接続できた時点で完了するものではありません。証明書、Trust List、認証、権限、ログ、Gateway/Wrapper、Classic 残置を継続的に管理しなければ、「接続はできているが、なぜその設定なのか説明できない」状態になります。

表 9-1 導入後に放置すると起きやすい問題

放置されやすいもの	起きやすい問題	現場への影響	継続運用で維持する管理情報
設定根拠	なぜその設定にしたか分からなくなる	変更時・監査時・障害時に説明できない	設定理由、承認者、変更日
証明書・秘密鍵	期限切れ、不要証明書の残存、秘密鍵の不適切な保管	接続障害、なりすましリスク、復旧時の混乱	有効期限、配置先、更新担当、秘密鍵の保管場所・アクセス権限
Trust List	何を信頼しているか説明できない	旧端末や不要アプリを信頼し続ける	登録理由、承認者、見直し日、削除・失効状況
認証	Anonymous や共有アカウントが残る	誰が接続したか分かりにくい	認証方式、利用者、用途、例外理由

放置されやすいもの	起きやすい問題	現場への影響	継続運用で維持する管理情報
通信保護設定（MessageSecurityMode/SecurityPolicy）	None や弱い設定が残る	通信保護の説明ができない	Endpoint、通信保護設定、採用理由
権限	過大権限、書き込み範囲の不明確化	意図しない書き込みや復旧時の混乱	読み取り、書き込み、管理権限の範囲
ログ	異常時にどこを見ればよいか分からない	障害切り分けが遅れる	ログ種別、保存先、確認者、取得できる内容
Gateway/Wrapper／中継ソフト	暫定利用が固定化する	Classic 残置や変換範囲が見えなくなる	変換区間、残置理由、見直し予定
Classic 残置	Classic/DCOM リスクが残る	OS 更新・端末交換時に復旧しにくい	残置区間、保守期限、解消予定
復旧手順	手順の所在や最新版が分からなくなる	端末交換・障害時に同じ接続状態へ戻しにくい	復旧手順書、確認済み設定、切戻し条件、担当者
責任分界	製造、保全、情シス、ベンダーの役割が曖昧になる	障害時の判断遅れ、依頼漏れ、対応重複が起きる	担当範囲、一次確認者、承認者、ベンダー連絡先

注：安全性や説明可能性は、設定・記録・更新・見直しを継続して初めて維持できます。

9.2 導入後に維持すべき管理情報

導入後の継続運用では、設定値だけでなく、設定根拠、証明書、秘密鍵、Trust List、権限、ログ、Gateway/Wrapper、Classic 残置、例外設定を確認できる状態にしておく必要があります。これらの管理情報は、監査のためだけではなく、端末交換、OS 更新、証明書更新、設備更新、担当者交代時に、同じ接続状態を維持するために使用します。

表 9-2 導入後に維持すべき管理情報

管理情報	残す内容	主な担当	更新タイミング	備考
設定根拠	なぜその設定にしたか、誰が承認したか	情シス、保全、セキュリティ	設定変更時	既存の変更管理記録に含めてもよい
証明書・秘密鍵情報	発行日、有効期限、配置先、更新担当、削除状況、秘密鍵の保管場所・アクセス権限	情シス、ベンダー	発行・更新・削除時	小規模環境では資産管理表と兼用可
Trust List 情報	信頼済み証明書、登録理由、承認者、見直し日、削除・失効状況	情シス、セキュリティ	端末追加、証明書更新時	試験時に自動受け入れした証明書は本番移行前に削除する

管理情報	残す内容	主な担当	更新タイミング	備考
認証・権限情報	利用者、役割、読み取り、書き込み、管理権限	情シス、製造、保全	人員変更、権限変更時	アカウント管理表と兼用可
通信保護設定情報	Endpoint、通信保護設定、採用理由、例外理由	情シス、セキュリティ	構成変更、製品更新時	None や Sign のみの採用理由を残す
公開タグ情報	公開範囲、書き込み可否、用途、上位システム	製造、保全、ベンダー	タグ追加・変更時	Gateway 設定資料と兼用可
ログ確認先	ログ種別、保存先、一次確認者、取得できる内容	情シス、保全	構成変更、障害後	一覧表で十分
Gateway/Wrapper／中継ソフト情報	変換区間、公開タグ、取り込みタグ、品質情報、タイムスタンプ、書き込み経路、ログ確認先	保全、情シス、ベンダー	更新時、構成変更時	-
Classic 残置情報	残置区間、理由、保守期限、解消予定	保全、設備管理	OS 更新、設備更新時	OS 更新、端末交換、DCOM 設定変更、イベントログ確認と連動して見直す
例外情報	例外内容、理由、補完策、承認者、期限	セキュリティ、情シス、製造	例外承認時、期限前	放置防止が目的

注：重要なのは、必要なときに「なぜその設定か」「誰が承認したか」「今も有効か」を確認できることです。

9.3 設定根拠の管理

設定根拠の管理では、設定値そのものよりも、「なぜその設定にしたか」を残すことが重要です。たとえば、Anonymous を許可しない理由、特定の証明書を Trust List へ登録した理由、通信保護設定を選んだ理由、書き込み可能タグを許可した理由、Gateway を残した理由を記録しておくことで、変更時、障害時、監査時、担当者交代時に判断の経緯を確認できます。

表 9-3 設定根拠として残すべき項目

設定項目	用語の補足	残すべき理由	残す管理情報	見直しタイミング
Anonymous	利用者認証情報を送らずに接続する方式。アプリケーション証明書とは別の概念	誰が利用したか分かりにくい接続を放置しないため	許可／不許可、理由、例外有無、対象範囲	導入時、端末追加時、レビュー時
通信保護設定（MessageSecurityMode/SecurityPolicy）	署名・暗号化の有無と、使用する暗号方式の設定	通信保護の方針を説明するため	Endpoint、通信保護設定、採用理由、例外理由	構成変更、製品更新時、監査前
証明書登録	接続相手のアプリケーション証明書を信頼すること	なぜその相手を信頼しているかを説明するため	証明書名、用途、登録理由、承認者、有効期限	端末追加、証明書更新、棚卸し時
Trust List	信頼済み証明書の一覧	不要端末や試験用証明書を残さないため	登録日、登録理由、削除・失効状況、見直し日	四半期、端末撤去時、障害後
書き込み可能タグ	上位から値や設定を変更できるタグ	操業影響に直結するため	対象タグ、用途、承認者、ログ確認先、切戻し条件	タグ追加、権限変更、監査前
ユーザ・ロール	利用者や役割ごとの権限	過大権限や共有アカウントを避けるため	利用者、役割、読み取り／書き込み／管理権限	人員変更、権限変更、定期レビュー
Gateway/Wrapper 残置	中継ソフト・装置を使って変換している状態	暫定利用の固定化を防ぐため	変換区間、残置理由、見直し予定、責任分界	構成変更、設備更新、半期レビュー
Classic 残置	OPC Classic/DCOM が残る区間	OS 更新や復旧性のリスクを見失わないため	残置区間、理由、保守期限、解消予定	OS 更新、設備更新、年次レビュー
ログ取得範囲	どのイベントや操作が記録されるか	障害時に説明できる範囲を把握するため	ログ種別、保存先、保存期間、取得できる内容	構成変更、障害後、監査前

注：設定根拠は、技術担当者だけのメモにしません。製造、保全、情シス、セキュリティ、ベンダーのうち、誰が判断し、誰が承認したかを残します。

9.4 証明書・Trust List の管理

証明書と Trust List は、OPC UA で接続相手を確認するための重要な管理項目です。ただし、証明書を作成して Trust List へ登録しただけでは十分ではありません。発行、配置、秘密鍵保護、承認、更新、失効、削除、棚卸しを運用に載せ、どの端末・アプリをなぜ信頼しているかを説明できる状態にしておく必要があります。バックアップや端末交換のために秘密鍵を扱う場合も、誰が扱えるか、どこに保管するか、不要になったものを削除したかを残します。

表 9-4 証明書・Trust List 管理の流れ

段階	管理すること	残す管理情報	確認者・承認者	注意すること
発行	誰が、どの端末・アプリ用に発行したか	証明書 ID、用途、発行日、発行元	情シス、ベンダー	試験用と本番用を混同しない
配置	どこに配置したか	配置先、格納場所、対象アプリ	情シス、保全	端末交換時に再配置できるようにする
秘密鍵保護	秘密鍵へアクセスできる人・サービスを制限する	保管場所、アクセス権限、バックアップ有無	情シス、セキュリティ	共有フォルダ等へ無管理に置かない
Trust List 登録	信頼する証明書を登録する	登録日、登録理由、対象接続、承認者	情シス、セキュリティ、保全	Rejected から無条件に登録しない
承認	接続相手として信頼してよいか確認する	承認者、確認内容、承認日	製造、保全、情シス	用途と接続元を確認する
更新	有効期限前に証明書を更新する	旧証明書、新証明書、更新日、影響範囲	情シス、ベンダー	更新後に接続試験を行う
接続再確認	証明書更新後に実際の接続を確認する	確認日、対象接続、接続結果、確認者	情シス、保全、ベンダー	更新作業だけで終わらせず、接続試験を残す
失効	信頼しない証明書を無効扱いにする	失効理由、失効日、影響範囲	情シス、セキュリティ	失効しただけで設定から消えたとは限らない
削除	不要な証明書を Trust List やストアから削除する	削除日、削除対象、確認者	情シス、保全	旧端末や試験用を残さない
棚卸し	信頼済み証明書が今も必要か確認する	棚卸し日、不要証明書、対応結果	情シス、セキュリティ	四半期や端末撤去時に実施する

注：試験時に自動受け入れした証明書を、本番移行後も Trust List に残さないようにします。不要な証明書、旧端末の証明書、失効済み証明書は、削除・失効状況を確認します。失効は「信頼しない状態にすること」、削除は「Trust List や証明書ストアから不要な証明書を取り除くこと」です。製品や運用によって扱いが異なるため、ベンダーに確認します。

9.5 認証・権限・書き込み管理

認証と権限は、接続できるかだけでなく、誰が、どの範囲を読めるか、何を書き込めるかを説明するために管理します。特に書き込み可能タグは、誤操作や意図しない変更が操業に影響する可能性があるため、用途、承認者、ログ確認先を明確にしておきます。ユーザ ID/パスワードを使う場合は、通信保護設定との組み合わせを確認します。SecurityPolicy None や MessageSecurityMode None との組み合わせは、本番系では原則避け、残す場合は例外管理の対象にします。

表 9-5 認証・権限・書き込み管理表

観点	管理すること	残す管理情報	見直しタイミング	注意すること
認証方式	Anonymous、ユーザ名、証明書などの採用状況	採用方式、採用理由、例外有無	導入時、端末追加時	Anonymous 許可は例外として扱う
ユーザ ID/パスワード	ユーザ名・パスワードを使う接続	利用者、用途、通信保護設定（MessageSecurityMode/SecurityPolicy）、例外理由	利用者追加、監査前	通信保護設定が None の状態と組み合わせないことを原則とする
ユーザ	誰が接続できるか	利用者、所属、用途、承認者	人員変更、退職、異動	共有アカウントの常用を避ける
ロール	役割ごとの権限	ロール名、対象範囲、権限内容	権限変更、レビュー時	過大権限を避ける
読み取り権限	誰がどのタグを読めるか	対象タグ、利用者、用途	タグ追加、利用者追加	不要な公開範囲を広げない
書き込み権限	誰がどのタグへ書けるか	対象タグ、用途、承認者、切戻し条件	書き込み追加、操作変更	操業影響を確認する
管理権限	設定変更できる人・端末	管理者、操作範囲、承認者	担当変更、監査前	管理者を必要最小限にする
ログ確認先	認証失敗や書き込み履歴を確認する場所	ログ種別、保存先、一次確認者	構成変更、障害後	製品により取得できる粒度が異なる
例外	標準から外れる設定	例外理由、補完策、期限、承認者	期限前、レビュー時	例外を通常運用にしない

注：認証できることと、適切な権限で接続できることは別です。読み取り専用のつもりでも、設定や製品仕様により書き込み経路が残る場合があるため、書き込みタグは独立して確認します。

9.6 ログ・監視・確認先の管理

ログ管理では、ログを保存しているだけでなく、どの異常を、どのログで、誰が確認するかを決めておく必要があります。接続断、認証失敗、証明書エラー、書き込み履歴、Gateway/Wrapper ログ、上位システムログを確認できる状態にしておくことで、障害時の切り分けや監査対応に備えやすくなります。確認頻度は目安で、現場規模、接続数、操業影響、既存の監視体制に応じて調整してよいものです。

表 9-6 ログ・監視で確認する項目

ログ種別	見る目的	主な確認先	確認頻度の目安	記録・対応
接続断	通信不安定や端末停止の把握	OPC UA サーバ、クライアント、Gateway	月次、障害時、変更後	発生日時、対象接続、復旧内容
認証失敗	不要端末や誤接続の把握	UA サーバログ、認証ログ	月次またはレビュー時	利用者、端末、失敗理由
証明書エラー	期限切れ、未信頼、失効の把握	Trusted/Rejected、証明書ログ	月次、証明書更新時	対象証明書、対応結果
書き込み履歴	誰が何を書いたかの把握	UA サーバ、上位システム、Gateway	月次、操作後、障害時	対象タグ、値、時刻、操作者
タグ変換エラー	Gateway/Wrapper での変換不整合の把握	Gateway ログ、変換ログ	障害時、変更後	対象タグ、品質情報、時刻の扱い
品質情報異常	データ欠損や異常値の把握	OPC クライアント、上位システム、履歴 DB	月次、品質異常時	品質値、影響範囲、補完策
時刻ずれ	タイムスタンプ不整合の把握	時刻同期ログ、Gateway、上位ログ	変更後、障害時	時刻差、原因、修正内容
設定変更	設定変更の追跡	変更管理記録、製品ログ	変更時、監査前	変更者、変更理由、承認者
OS・サービス	サービス停止や OS 影響の把握	Windows イベントログ、サービスログ	障害時、OS 更新後	イベント ID、復旧内容、影響範囲

注：「ログを見れば必ず分かる」とは書きません。製品や設定により、取得できるログの粒度、保存期間、書き込み内容の記録範囲は異なります。必要なログが残らない場合は、上位システム、OS ログ、作業記録、変更管理記録などで補完します。

9.7 変更管理

変更管理では、変更作業そのものだけでなく、変更によって影響を受ける管理情報を更新することが重要です。OS 更新、OPC サーバ更新、Gateway/Wrapper 更新、証明書更新、ネットワーク変更、設備更新のたびに、接続状態、設定根拠、証明書、Trust List、権限、ログ確認先、Classic 残置を見直します。第 8 章の表 8-8 は「変更時に何を確認するか」、第 9 章の表 9-7 は「変更後に何を更新・維持するか」です。

表 9-7 変更時に更新すべき管理情報

変更イベント	更新・確認すべき管理情報	反映先の例	承認・確認者	注意すること
OS 更新	OPC サービス、証明書ストア、通信、ログ、復旧手順	変更記録、復旧手順、ログ確認先一覧	情シス、保全	UA でも OS 更新影響は確認する

変更イベント	更新・確認すべき管理情報	反映先の例	承認・確認者	注意すること
OPC サーバ更新	設定、タグ、接続先、互換性、切戻し手順	設定根拠、公開タグ情報、変更記録	情シス、ベンダー	更新後に設定差異を確認する
Gateway/Wrapper 更新	変換区間、取り込みタグ、公開タグ、品質情報、時刻、ログ	中継ソフト情報、ログ確認先	保全、情シス、ベンダー	変換範囲が変わっていないか確認する
証明書更新	新旧証明書、Trust List、失効・削除状況	01_OPC_UA 接続・運用管理台帳の証明書・Trust List 情報欄	情シス、セキュリティ	旧証明書を残さない
上位端末追加	証明書、認証、権限、公開タグ、ログ確認先	資産管理、権限情報、Trust List	情シス、製造、保全	必要な端末だけを信頼する
タグ追加・変更	公開タグ、書き込み可否、品質情報、タイムスタンプ	公開タグ情報、設定根拠	製造、保全、ベンダー	上位の帳票・分析への影響を確認する
ネットワーク変更	Endpoint、FW、名前解決、時刻同期、ログ	ネットワーク変更記録、接続情報	情シス、保全	接続できるだけでなくログも確認する
設備更新	Classic 解消、残置理由、保守期限、移行分類	Classic 残置情報、A/B/C 分類	設備管理、保全、情シス	更新機会を Classic 解消の判断材料にする
ベンダー保守	作業端末、接続経路、権限、作業ログ、例外	作業記録、例外管理表	保全、情シス、ベンダー	一時的な例外を残しっぱなしにしない

9.8 例外管理

例外管理は、標準から外れる設定を認めるための抜け道ではありません。むしろ、例外が放置され、通常運用として固定化することを防ぐための仕組みです。Anonymous 許可、ユーザ ID/パスワード利用時の SecurityPolicy None、MessageSecurityMode None、証明書自動受け入れ、広すぎる書き込み権限、Gateway/Wrapper 暫定利用、Classic 残置などは、理由、影響、補完策、承認者、期限を残します。SecurityPolicy None や MessageSecurityMode None を絶対禁止と断定するのではなく、本番系では原則避け、残す場合は例外管理の対象にします。

表 9-8 例外管理表

項目	残す内容	記入例	確認者	注意すること
例外内容	何が標準・推奨から外れているか	一時的に Anonymous を許可	情シス、セキュリティ	例外を通常運用にしない
対象範囲	どの接続、端末、タグ、期間が対象か	ライン A の保守端末のみ	製造、保全	範囲を広げすぎない
例外理由	なぜ標準設定にできないか	旧設備が認証方式に非対応	保全、ベンダー	理由が不明な例外を残さない
想定影響	何が起き得るか	接続元を識別しにくい	セキュリティ、製造	操業影響と説明負荷を確認する
補完策	例外を補う管理策	閉域、期間限定、読み取り専用、作業ログ確認	情シス、保全	補完策なしの例外を避ける
承認者	誰が例外を承認したか	製造責任者、情シス責任者	関係部門	現場だけ、情シスだけの判断にしない
期限	いつまで例外を認めるか	設備更新まで、次回定修まで	承認者	期限なしにしない
解消条件	何がそろえば標準へ戻すか	UA 対応設備へ更新したら無効化	保全、設備管理	条件を具体化する
次回見直し日	いつ再確認するか	2026 年 10 月レビュー	情シス、保全	見直し日を過ぎた例外を放置しない

注：特に、Anonymous 許可、証明書自動受け入れ、広すぎる書き込み権限は、理由と補完策なしに残しません。

9.9 定期レビュー

定期レビューでは、毎回すべてを詳細に確認するのではなく、月次、四半期、半期、年次、変更時で確認対象を分けます。月次ではログや証明書エラー、四半期では Trust List や不要権限、半期では Gateway/Wrapper や Classic 残置、年次では移行優先度や役割分担を見直します。接続数が少ない環境では、変更時・障害時・年次レビューを中心に簡素化してもよいですが、証明書期限、不要な Trust List 登録、例外期限は見落とさないようにします。

表 9-9 定期レビューの目安

頻度の目安	確認すること	主な確認情報	主な担当	結果の扱い
月次目安	接続断、認証失敗、証明書エラー、書き込みログ	ログ、証明書エラー、操作記録	情シス、保全	異常傾向を記録し、必要時に調査
証明書期限前	有効期限、更新計画、Trust List 反映、更新後の接続確認	証明書情報、更新予定、接続試験結果	情シス、保全、ベンダー	期限切れによる接続障害を防ぐ
四半期目安	Trust List、不要証明書、不要ユーザ、公開タグ範囲	Trust List 情報、証明書情報、権限情報	情シス、セキュリティ	不要な信頼・権限を削除
半期目安	Gateway/Wrapper 暫定利用、Classic 残置、保守期限	中継ソフト情報、Classic 残置情報、保守契約	保全、設備管理、情シス	解消計画、更新計画へ反映
年次目安	移行優先度、リスク評価、役割分担、障害対応手順	A/B/C 分類、リスク評価、手順書	製造、保全、情シス、管理職	次年度計画や投資判断へ反映
変更時	変更によって影響する設定、証明書、権限、ログ確認先	変更記録、設定根拠、ログ確認先	変更担当、承認者	変更後の管理情報を更新
障害後	原因、復旧手順、ログ、設定差異、再発防止	障害記録、ログ、変更記録	保全、情シス、ベンダー	手順と管理情報を更新
担当変更時	管理表、証明書期限、例外、ログ確認先、ベンダー連絡先	引き継ぎ資料、管理台帳	前任者、後任者、上長	属人化を防止

注：定期レビューは、形式的な棚卸しで終わらせず、証明書更新、Trust List 削除、不要権限削除、Gateway/Wrapper 暫定利用の見直し、Classic 解消計画、例外期限の更新につなげます。

9.10 第 8 章から第 9 章への引き継ぎ

表 9-10 第 8 章から第 9 章への引き継ぎ情報

第 8 章で確認したこと	第 9 章で維持する管理情報
Endpoint、通信保護設定	設定根拠、例外情報
証明書エラー有無	証明書情報、更新予定、秘密鍵保護
Trust List 登録状況	登録理由、承認者、削除・失効状況、棚卸し予定
Anonymous や認証方式	認証方式、利用者、例外理由、見直し予定
書き込み可能タグ	書き込み権限、用途、承認者、ログ確認先、切戻し条件
取り込みタグ範囲・公開タグ範囲	公開タグ情報、Gateway/Wrapper 情報、変更管理
品質情報・タイムスタンプ	データ利用上の前提、補完策、変更時確認事項
Gateway/Wrapper 変換区間	中継ソフト情報、Classic 残置情報、見直し予定
Classic 残置区間	残置理由、保守期限、解消予定、A/B/C 分類との関係
ログ確認先	ログ種別、保存先、一次確認者、取得できる内容
未確認・例外ありの項目	例外管理表、期限、補完策、次回見直し日

9.11 本章のまとめ

OPC UA への移行は、接続方式を変えるだけでは完了しません。証明書、秘密鍵、Trust List、認証、通信保護設定、権限、ログ、変更管理、例外管理を継続的に見直すことで、接続状態を維持し、将来の端末更新、設備更新、監査、障害対応に備えやすくなります。

付録との関係

本章で扱う導入後運用は、付録 B「運用管理表」と付録 C「変更・例外・定期レビュー表」に対応します。証明書、Trust List、認証方式、通信保護設定、書き込み権限、ログ確認先、設定根拠は付録 B に記録し、OS 更新、証明書更新、設備更新、Gateway/Wrapper 変更、例外設定、定期レビューは付録 C で管理します。別紙 Excel 版を利用する場合も、すべての項目を最初から入力する必要はなく、導入後に維持すべき項目から順に記録してください。

第 10 章 模擬プラント検証から得られた運用・設定の注意点

本章で分かること

OPC UA が「設定次第でどれだけ守れるか」「何を設定しても守れない領域はどこか」を、模擬プラント検証の結果に基づいて整理します。読み終えると、自社の本番環境に持ち帰るべき設定方針と、運用設計で埋めるべき穴が見えるようになります。

10.1 検証の位置づけ

本章で扱う検証は、製造現場そのものを再現することを目的としたものではなく、Classic／UA 混在構成において確認が必要となる通信保護、認証、証明書管理、Trust List 運用、ログ確認などの観点を抽出するために構築した模擬プラント環境（以下「ラボ検証環境」、図 10-1 参照）で実施したものです。

ラボ検証環境は、現場で実際に多く見られる典型構成を再現する形で環境構築を行っています。

ただし、実際の製造現場には固有のネットワーク設計、運用ルール、製品実装差が存在するため、本章の結果はそのまま自社環境に当てはまるとは限りません。「設定の方向性を判断する材料」として読み、本番適用前には必ず自社環境に応じた検証を行ってください。

本章の前提

本章の結果は、以下の 3 点を前提として読んでください。

前提	本章での扱い
ラボ環境と本番環境の差	ネットワーク構成、機器構成、運用負荷、攻撃環境はすべて本番と完全一致ではない。挙動の方向性は確認できるが、性能値・閾値は本番で再測定が必要。
製品依存性	OPC UA 仕様は共通だが、製品ごとに既定値・実装の解釈差がある。本章は仕様の挙動を確認する目的で行っており、特定製品の優劣評価ではない。
攻撃手法の詳細非公開	攻撃手順・使用ツール・ペイロード内容は、本ガイド読者層（製造・設備管理部門）の業務に不要で、悪用リスクも考慮して記載していない。設定の効果の議論に絞ることとする。

図 10-1 ラボ検証環境の典型構成（イメージ）

構成のポイント：

- 上位層と現場層を Gateway 製品で中継し、上位は OPC UA、下位は OPC Classic という「混在構成」を再現
- OT/IT 境界にネットワークセグメンテーション（ファイアウォール／L3 スイッチ）を配置し、現場層を保護
- 上位 UA 側の通信路保護・認証・証明書管理と、下位 Classic 側の DCOM/Windows 認証は別レイヤとして独立管理
- 実際の現場では PLC、HMI、計装サーバ、データヒストリアン等が複数並ぶが、本図は最小単位の論理構成のみを示す

10.2 検証設計の枠組み——何を変えて、何を見たのか

OPC UA のセキュリティは「単一の機能」ではなく、複数の独立したレイヤの組み合わせによって成立します。本検証では、そのうち実運用で設定差が生じやすい 3 つのレイヤに着目し、それぞれを「セキュリティ機能あり」「セキュリティ機能なし」で組み合わせて挙動を比較しました。

セキュリティレイヤー	セキュリティ機能あり	セキュリティ機能なし	現場でセキュリティ機能なしが選ばれやすい理由
①通信路の保護（署名・暗号化）	Sign & Encrypt（署名＋暗号化）	None（無保護）	初期動作確認の容易さ、性能影響への懸念、製品既定値の踏襲
②利用者の特定（認証）	X.509 証明書認証 または ユーザ ID/パスワード	Anonymous（匿名）	クライアント側設定の手間、ID 管理運用の不在、検証時の暫定設定が残置
③相手の信頼（証明書受け入れ）	Trust List への手動登録	自動受け入れ（auto-accept）	初回接続時の利便性、運用手順の未整備、検証用設定の本番混入

これらに加え、検証では 3 種類の攻撃シナリオを設定しました。

攻撃シナリオ	攻撃の狙い	成功時に起きること
不正接続	認証や信頼関係を回避して、正規でない端末から OPC UA サーバへ接続する	アドレス空間の列挙、タグ値の参照、書き込み可能タグへの不正書き込み
中間者攻撃（MITM）	正規クライアントと正規サーバの間に割り込み、通信を盗聴または改ざんする	タグ値の読み取り（情報漏洩）、書き込み値の改ざん（制御撹乱）
DoS 攻撃（サービス妨害）	大量のセッション要求やリソース消費により、サーバの応答を停止または遅延させる	正規クライアントからの監視・記録・制御の中断

10.3 検証結果サマリー—設定別の防御成否マトリクス

通信路の保護と認証の組み合わせ（4 パターン）を、3 つの攻撃シナリオに対して試した結果が次の表です。「o」は攻撃が防げたこと、「×」は攻撃が成立したことを意味します。

通信保護状態	認証	不正接続	中間者攻撃	DoS 攻撃
None（無保護）	Anonymous	×	×	×
None（無保護）	ユーザ ID/パスワードまたは証明書	o※1	×（資格情報漏洩）	×
Sign & Encrypt	Anonymous	×※2（誰でも接続可）	o	×
Sign & Encrypt	ユーザ ID/パスワードまたは証明書	o	o	×

※1 通信路が暗号化されていなくても、ユーザ ID/パスワードや証明書による「本人確認」の仕組みは働くため、正体不明のクライアントからの接続は拒否できます。ただし、通信が暗号化

されていない状態では、やりとりの内容（パスワードなど）が経路上で読み取れる状態になります。そのため、物理的に外部から隔離されたネットワーク上でしか、このパターンを安全とは言えません。

※2 自動受け入れ設定が防御成否を分ける決定的要因

上記マトリクスのうち「Sign & Encrypt ＋ Anonymous」の行では、証明書の自動受け入れ設定（auto-accept）の有無で不正接続に対する結果が大きく異なります。

- 自動受け入れ ON：攻撃端末が生成した自己署名証明書がサーバの Trust List に自動登録され、暗号化されたセキュアチャネルが成立しました。以降、攻撃端末はタグの閲覧・書き込みを含む全操作を実行できました。暗号化は有効でしたが、接続相手の正当性は一切検証されていません。
- 自動受け入れ OFF：同じ攻撃端末の証明書は Rejected ディレクトリに隔離され、セキュアチャネルの確立自体が拒否されました。管理者がその証明書を Trusted ディレクトリに手動で移動しない限り、接続は成立しません。

この結果は、Sign & Encrypt（暗号化）を有効にしただけでは不十分で、証明書の信頼管理（自動受け入れ OFF＋Trust List の手動管理）が不正接続防御の成否を決定づけることを示しています。

この表から読み取れる 4 つのこと

① 通信路の保護と認証は、独立した別レイヤです。両方を強くしないと総合的な防御は成立しない。「証明書認証だから安全」「暗号化しているから安全」という単独の主張は不十分。

② Anonymous 認証は、暗号化しても本質的に脆弱です。誰でも接続できる以上、正規クライアントを偽装した端末からの接続を拒めません。設定の組み合わせの中で最も致命的な弱点になりやすいです。

③ 中間者攻撃は、通信路の暗号化だけで防げる種類の攻撃ではありません。サーバ証明書の正当性をクライアント側が検証していなければ、攻撃者が用意した「正規サーバを装ったサーバ証明書」を受け入れてしまいます。後述する証明書の自動受け入れ問題はここに直結します。

④ DoS 攻撃は、OPC UA レイヤの設定だけでは防ぎ切れない。これは仕様や製品の欠陥ではなく、DoS 対策が本質的に多層防御の問題に当たることを示しています（10.5 節で詳述）。

10.4 証明書自動受け入れ——もっとも見落とされやすい落とし穴

OPC UA の多くの製品には、初回接続を容易にするため「自動受け入れ（auto-accept）」モードが用意されています。これは、未知のクライアントまたはサーバが提示する証明書を、人の手による承認なしに Trust List へ登録する設定です。検証環境を立ち上げる段階では極めて便利な機能ですが、本番運用に持ち越すと致命的な穴になります。

検証結果：自動受け入れ ON 時の挙動

本検証では、サーバ側の証明書自動受け入れが ON の状態で、攻撃者が用意した正規でない自己署名証明書を提示する不正クライアントから接続を試みました。結果、その不正クライアントの証明書はサーバ側で自動的に「信頼済み」として登録され、以降の接続が成立しました。本来であれば、未知の証明書は Rejected 側に隔離され、管理者が確認・承認するまで Trusted へ移動されないのが正しい運用フローですが、この承認ステップが自動受け入れ設定によって省略されている状態です。

自動受け入れ ON 時の接続成功後、攻撃端末はサーバ上で以下の操作を実行できることが確認されました。

- セキュアチャネルの確立（暗号化通信の成立）
- セッションの有効化（Anonymous 認証による即時アクセス）
- アドレス空間の再帰的列挙（サーバ上の全ノード構造の取得）
- 読み取り可能な変数の値取得
- 書き込み可能なタグへの値書き込み（物理出力に直結するデジタル出力・アナログ出力を含む）

つまり、暗号化は有効に機能していましたが、暗号化された通信チャネルの先にいる相手が「正規の端末か、攻撃者の端末か」をサーバは区別できていませんでした。これは「暗号化されているが認証されていない」状態で、鍵のかかった部屋で不審者と二人きりになっているような状況に例えられます。

検証結果：自動受け入れ OFF 時の挙動

同じ攻撃を、自動受け入れを OFF に設定したサーバに対して試みた場合、不正クライアントの証明書は Rejected 側に隔離され、サーバ管理者がそれを目視確認・拒否することで接続を防げました。これは、OPC UA 仕様が想定している正しい証明書管理フローが機能した状態です。

実務上の含意

自動受け入れの設定有無は、製品の管理 UI から「設定一つで切り替わる」項目です。検証時の利便性のために ON にし、本番で OFF に戻し忘れる——というのは、運用現場で十分に起こり得るシナリオです。本番投入前のチェックリストに、以下を必ず入れてください。

- OPC UA サーバ／クライアントの双方で、証明書自動受け入れが OFF になっていることを管理画面で確認
- Trust List（信頼済み）に登録されている証明書を一覧化し、各々がどの正規端末・正規アプリのものか説明できるか確認
- Rejected 側に滞留している証明書がないか確認（あれば、それは過去の不正接続試行か、登録漏れの正規端末の痕跡）
- 証明書の追加・削除を行う運用手順書と承認者が決まっているか確認

OPC UA 仕様（Security Model for Administrators）は、証明書管理の運用レベルを 4 段階の Tier（Tier 1〜Tier 4）に分類しており、自動受け入れに近い運用は Tier 1 相当、相互認証＋手動承認＋失効管理を備えた運用が Tier 4 相当と位置づけられています。製造ラインの重要度に応じて目指す Tier を定め、自社の現状がどこにあるかを把握することが、証明書運用設計の出発点になります。

10.5 DoS 攻撃——OPC UA 単体では守り切れない領域と、その対処方針

検証結果の表で示した通り、DoS 攻撃はどの設定パターンでも完全には防げませんでした。これは OPC UA の欠陥ではなく、DoS 攻撃が本質的に「資源の有限性」を突く攻撃で、アプリケーション層の認証・暗号化では原理的に止められないという特性に起因します。OPC UA 仕様（Part 2 Security）も、DoS への対策はメッセージフラッディング・リソース枯渇・アプリケーションクラッシュの三つに分けて考えるべきとしており、それぞれに異なる層の対策を組み合わせる必要があると述べています。

OPC UA レイヤでできること

- 同時セッション数の上限設定、認証失敗時のレート制限など、サーバ側の防御パラメータを適切に設定する
- 不要なエンドポイントを公開しない（特に Anonymous エンドポイントを残さない）
- 接続失敗・セッション切断のログを記録し、異常な急増を検知できるようにする

検証で確認された影響の一例

本検証では、OPC UA の接続確立プロセス（セキュアチャネル確立フェーズ）に存在する既知の脆弱性を突く攻撃を複数パターン試行しました。その中で最も深刻な影響をもたらしたケースでは、検証用の産業用コントローラ（PLC に相当）が以下の経過をたどりました。

- 攻撃開始から数秒以内にサーバの CPU 使用率が 100%に達した
- 正規クライアントからの新規接続・既存接続ともに応答不能となった
- コントローラが自動的に STOP 状態に移行した（安全保護機能の発動）
- コントローラの復旧には手動介入が必要であった

この結果は、DoS 攻撃が IT 環境における「サービス停止」にとどまらず、OT 環境では「物理プロセスの中断」に直結し得ることを示しています。化学プロセスの温度・圧力制御、製造ラインの搬送・加工制御、ユーティリティのポンプ運転など、コントローラの停止が安全性に直結するプロセスでは、このリスクは特に重大です。

なぜ OPC UA の設定だけでは防げないのか

OPC UA の接続確立プロセスは、「通信路の保護（暗号化）」を確立するフェーズと、「利用者の認証」を行うフェーズが分離されています。DoS 攻撃の多くは、暗号化が確立される途中の処理段階——証明書の解析、鍵の導出、チャネル状態の割り当てなど——を狙います。これらの処理はユーザ認証よりも前に実行されるため、認証設定はもちろん、暗号化の設定も防御に寄与しません。これが、全設定パターンで DoS 攻撃が成功した技術的な理由で、OPC UA 仕様（Part 2 Security）が指摘する「認証前の処理段階に対する攻撃面」に相当します。

OPC UA レイヤの外側でやるべきこと

- ネットワークセグメンテーション：OT/IT 境界にファイアウォールを置き、OPC UA サーバへ到達可能な送信元を許可リスト方式で限定する（ホワイトリスト型）
- 帯域制限・接続レート制限：境界機器側で、単位時間あたりの新規接続数や帯域を制限する
- 監視と検知：SIEM や SCADA 監視で接続数・トラフィック量の異常を可視化し、運用側で早期検知できる体制を整える
- 冗長化と縮退運転設計：DoS 攻撃によりサーバが応答停止しても、最小限の操業継続ができるバックアップ経路や手動運転手順を準備しておく

経営層向けの説明：「OPC UA を適切に設定・運用することで、なりすましや盗聴・改ざんのリスクを大きく低減できます。一方で『大量の通信を投げつけて止める』タイプの攻撃は、OPC UA だけでは止められません。これは欠陥ではなく、ネットワーク防御や境界防御と組み合わせて初めて成立する性質のものです。CISA など制御システム向けのガイドが多層防御（Defense in Depth）を推奨しているのは、この性質に対応するためです。」

10.6 Anonymous 認証の扱い——なぜ「閉域だから大丈夫」が通用しないのか

現場で最も多く残る設定の一つが、Anonymous（匿名）認証の有効化です。製品の初期設定で有効になっていること、検証時に便利なため有効にしたまま運用に入ること、アカウント管理が行われていないこと、「閉域だから問題ない」と判断されること、これらが残置の典型的な経緯です。

Anonymous 認証が残ると失われる 4 つのこと

失われるもの	説明	経営・運用への影響
利用者の特定	誰が接続したのか、ログ上「Anonymous」としか残らない	障害時の影響範囲特定、監査対応、内部不正調査が困難
権限の細分化	全 Anonymous 接続が同じ権限になる	「読み取り専用ユーザ」「保守ユーザ」「監視ユーザ」のような最小権限設計ができない
接続拒否の手段	正規でないクライアントが接続してきても、認証情報がないため拒否のしようがない	閉域が破られた瞬間に、全タグへの自由なアクセスを許す
変更責任の追跡	書き込み可能タグを設定していた場合、誰がいつ書き換えたかが追えない	事故発生時の原因究明と再発防止策が立てられない

「閉域だから大丈夫」という主張が成り立たない理由は、閉域の前提自体が時間とともに崩れるからです。設備更新、外部ベンダーの保守作業、リモートメンテナンス回線の開設、上位システムからのデータ連携、これらの変更のたびに、当初想定していた「外と切り離されている」状態は侵害されていきます。Anonymous 認証を許容している場合、閉域前提が崩れた際に、OPC UA 側の利用者識別や権限制御による防御が十分に機能しなくなる。

現実解：完全廃止が難しい場合の補完策

- 期間限定での例外許可：理由・補完策・解除期限・承認者を「例外管理表」に記録し、定期見直しの対象に入れる

- 読み取り専用エンドポイントの分離：書き込み権限のあるエンドポイントは認証必須にし、Anonymous は読み取り専用エンドポイントに限定する
- 接続元 IP 制限：境界側で Anonymous エンドポイントへの到達元 IP を限定する（多層防御）

10.7 設定項目別の運用観点と検証から見えた論点

検証を通じて最も重要な教訓の一つは、「暗号化」「認証」「認可」は完全に独立した別の仕組みであるという事実です。

- 暗号化（Sign & Encrypt）は通信路を保護しますが、誰が通信しているかは保証しません。
- 認証（ユーザ ID/パスワード、証明書）は通信相手を確認しますが、通信路が暗号化されていなければ認証情報自体が盗聴されます。
- 認可（権限制御）は認証済みの相手に何を許可するかを決めますが、Anonymous 認証ではユーザ ID が存在しないため権限制御が機能しません。

この三層がすべて適切に設定されて初めて、OPC UA のセキュリティは機能します。検証では、暗号化が有効でも認証が不十分な状態（例：Sign & Encrypt ＋ Anonymous ＋ 自動受け入れ ON）で、攻撃者が暗号化されたセキュアチャネルを正常に確立し、タグの閲覧・書き込みに成功しました。「暗号化している＝安全」という誤解は、OT 現場で最も危険な設定判断ミスにつながります。

ここまでの考察を、本番運用で確認すべき設定項目ごとに整理し直したものが次の表です。各項目について「OPC UA 仕様書上の意味」「検証で見えた問題」「製造部門が現場で確認すべきこと」を並べています。

設定・運用観点	仕様書上の意味	検証で見えた問題	製造部門が確認すべきこと
Anonymous 認証	認証なしでサーバへ接続できる状態。Part 4 が定義する UserIdentityToken のうち、最も弱い種類	暗号化していても、誰でも接続可能なため不正接続を防げない。認証情報がないためログ追跡も不可	本番エンドポイントで無効化されているか／例外がある場合に管理表へ理由が記載されているか
証明書自動受け入れ	未知の証明書を自動的に Trust List 登録する設定。仕様の正規フロー（手動承認）を省略するモード	攻撃者の自己署名証明書も自動登録された。本番運用では、自動受け入れを無効化し、Trust List を手動管理する運用を基本とすることが推奨される。	本番投入前に OFF に戻したか／Trust List の登録内容を全件説明できるか／Rejected の滞留を定期確認しているか
Trust List 管理	信頼する証明書のホワイトリスト。Part 12 Certificate Management が管理プロセスを定義	登録の積み上げで「誰の証明書か分からない」状態に陥りやすい。期限切れ放置で停止事故も起こり得る	登録一覧の棚卸し責任者／追加・削除の承認フロー／期限管理の手段
SecurityPolicy（通信路保護）	署名・暗号化のアルゴリズム選択。None から Aes256_Sha256_RsaPss まで段階がある	None のままだと中間者攻撃で盗聴・改ざんが成立。製品既定値が None 寄りの場合がある	本番エンドポイントが Sign & Encrypt 以上か／弱い設定が残っていないか／許可ポリシー一覧を文書化しているか
UserAccessLevel / RolePermissions	タグ単位・ロール単位のアクセス権限定義。Part 3/5/6 が規定	未設定だと「読み取り想定だが実際は書き込み可能」の状態が残る	書き込み可タグの一覧／書き込みを許可した理由／承認者と最終確認日
監査ログ	接続、認証失敗、証明書イベント、書き込み等を時系列で記録する仕組み	ログがどこに保存されるかを把握していないと、障害時の切り分けと監査対応に支障をきたす	ログの保存先／保存期間／一次確認者／集約先（SIEM 等）の有無
DoS 耐性パラメータ	同時セッション数上限、認証試行レート制限など製品側の防御パラメータ	OPC UA 設定だけで DoS を完全に止めるのは不可能。境界防御との組合せが前提	境界 FW での送信元 IP 制限／同時接続数の監視／異常検知の仕組み

10.8 検証から導かれた 5 つの教訓

本章の検証と考察を、本番運用へ持ち帰るべき教訓として整理すると、次の 5 点になります。

① OPC UA 化は「安全になる」ではなく「安全に運用しやすくなる」

OPC UA は仕様として安全機能を備えるが、設定と運用が伴わなければ防御は成立しない。経営層への説明でこの一文を必ず添えること。

② 通信路の保護と認証は別レイヤ。両方を強くする

暗号化だけ、または認証だけでは防げない攻撃が存在する。Sign & Encrypt + 証明書認証またはユーザ ID/パスワードを基本構成とする。

③ Anonymous は原則無効。例外は管理表で時限管理

「閉域だから大丈夫」は時間とともに崩れる前提。Anonymous 残置は運用負債として可視化する。

④ 証明書自動受け入れは検証用設定。本番投入前に必ず OFF

切替忘れは現場で頻発するヒューマンエラー。チェックリストの最上位項目とする。

⑤ DoS は OPC UA 単体では止まらない。多層防御で取り組む

境界 FW、セグメンテーション、監視、縮退設計を組み合わせる。OPC UA 設定だけで完結させようとしない。

10.9 本章のまとめ

本章は、OPC UA が備えるセキュリティ機能を「設定の組み合わせ」として分解し、模擬プラント環境での検証結果に基づいて、何が守れて何が守れないかを示しました。OPC UA は適切に設定・運用すれば、Classic 時代と比較して通信路の保護、利用者の特定、権限の細分化、操作の追跡可能性を大きく向上できる基盤です。同時に、Anonymous 残置・自動受け入れ放置・DoS 対策の境界依存といった、運用設計で埋めるべき穴も明確になりました。

本章で提示した 5 つの教訓は、第 8 章の実務チェックポイント、第 9 章の継続運用、付録の各管理表テンプレートに反映されています。

経営層向け説明例

「OPC UA への移行は、製造システムの通信を『誰がつないでいるか説明できる』『どの経路が守られているか説明できる』『何かあったときに追跡できる』状態へ変えていく取り組みです。模擬プラント検証で確認したのは、OPC UA が正しく設定されていれば、なりすましや盗聴・改ざんのリスクを低減できるという事実と、設定を誤れば防御が崩れるという事実の両方です。技術導入と運用設計はセットで投資する必要があります。」

付録との関係

本章の模擬プラント検証で確認した SecurityPolicy、MessageSecurityMode、Anonymous、自動受け入れ、Trust List、証明書、ログ確認先の論点は、付録 B「運用管理表」および付録 C「変更・例外・定期レビュー表」に反映します。検証結果をそのまま自社環境に当てはめるのではなく、自社の接続・設定・運用に照らして、例外設定や未確認項目を残さないように確認してください。

第 11 章　まとめ

11.1 本書の要点

OPC UA 移行は、通信規格を置き換えるだけの作業ではありません。どの接続が、何のために使われ、停止すると何に影響するかを把握し、Classic/DCOM 残置、Gateway/Wrapper、証明書、Trust List、認証、ログ、変更管理を継続的に説明できる状態にすることが重要です。

本書の立場は、既存の OPC Classic 利用を直ちにすべて否定することではありません。一方で、新規にシステムを導入する場合や、既存システムを全面刷新する場合は、将来の保守継続、接続管理、認証・権限管理、ログ確認、データ連携を見据え、OPC UA を前提に検討することを推奨します。既存システムについては、棚卸し結果と更新タイミングを踏まえ、優先度の高い接続から段階的に移行・見直しします。Classic を残す場合は、残置理由、期限、責任者、見直し時期を管理します。

最初からすべてを完璧に調べる必要はありません。まずは代表的な OPC 接続を 3 件程度選び、付録 A に接続元、接続先、用途、通信方式、書き込み有無、Classic/DCOM 残置、停止影響、次の対応を記録します。その結果をもとに、第 7 章の A/B/C 分類、第 8 章の移行前後確認、第 9 章の導入後運用へ進めます。

11.2 本文・付録・Excel 版の使い分け

対象	使い方
本文	背景、判断軸、確認観点、導入後運用の考え方を理解する
付録 A〜C	ホワイトペーパー単体で確認・記入できる最小版
01_OPC_UA 接続・運用管理台帳	付録 A〜C を Excel で継続管理する主たる参考テンプレート
02〜04 任意詳細 Excel	資産、証明書、構築・受入確認を必要に応じて深掘りする詳細版

11.3 実務での進め方

- 付録 A で代表 3 接続を選び、接続元、接続先、用途、通信方式、書き込み有無、Classic/DCOM 残置、停止影響を確認します。
- A/B/C 分類を行い、すぐに着手すべき接続、更新時期に合わせる接続、残置管理する接続を分けます。
- 導入・変更時には、証明書、Trust List、認証方式、書き込み権限、ログ確認先、例外設定を確認します。
- 導入後は、付録 B と付録 C を使い、設定根拠、承認者、期限、見直し日を残します。

この流れを一度で完成させる必要はありません。代表接続の確認から始め、移行判断、受入確認、導入後運用へ段階的に広げてください。

11.4 最後に

台帳やチェックリストは、作成すること自体が目的ではありません。必要なときに接続、設定、残置理由、承認者、見直し時期を説明できる状態を保つことが目的です。本書と付録、別紙 Excel 版を組み合わせ、自社の設備構成と運用体制に合わせて、無理なく継続できる形へ調整してください。

謝辞

本書の作成にあたり、OPC Classic、UA の利用状況や移行に関するアンケートにご協力いただいた企業・関係者の皆様、誠にありがとうございました。

本プロジェクトの実施にあたり、株式会社 Puerto　代表取締役　本田 寿明様には大変貴重なご意見や情報をご提供いただき、模擬プラントを使用した検証におきましても多大なるご協力をいただきました。ここに深く感謝申し上げます。

また、産業サイバーセキュリティセンター中核人材育成プログラムの講師である、 越島 一郎先生、橋本 芳宏先生、玉木 欽也先生、ならびに産業サイバーセキュリティセンター調査分析部サイバーインシデント調査室長の中山 顕様にはプロジェクトのメンター・講師とし て、ご指導・ご助言をいただきました。改めて御礼申し上げます。

最後に、1 年間という長期間の本プログラムに快く送り出してくださった所属企業の皆様方に、深く御礼 申し上げます。この 1 年間、非常に広範囲かつ専門的な学びを得ることができ、本プログラムでしか得られない知見・仲間を得ることができました。誠にありがとうございました。

プロジェクトメンバー

本書は、独立行政法人情報処理推進機構 産業サイバーセキュリティセンター 中核人材育成プログラムにおける第 9 期受講生 卒業プロジェクト「OPC UA 移行の課題整理と推進アプローチ」の成果物として作成されました。

リーダー　長谷川 和也、濵元 誠治

メンバー　伊藤 隼、楠 麟太郎、小谷 憲作、中島 しおり、星 隼人

付録　実務テンプレート

付録 A～C と別紙 Excel 版の使い分け

本付録は、OPC UA 移行検討に必要な情報を、現場で記入・確認できる最小限の形にしたものです。すべての項目を最初から完全に記入する必要はありません。まずは、止まると困る接続、更新時期が近い接続、上位システムやデータ活用に関係する接続など、代表的な OPC 接続を 3 件程度選び、付録 A または「01_OPC_UA 接続・運用管理台帳」に記入してください。未確認の項目は空欄にせず、「未確認」「要確認」「ベンダー確認」「情シス確認」などと記入し、確認先と次の対応を残します。

接続 ID	接続元	接続先	用途
付録 A 接続・移行確認表	最小限の入口表	最初に使う	代表 3 接続について、接続元、接続先、用途、通信方式、書き込み有無、Classic/DCOM 残置、停止影響、A/B/C 分類、次の対応を確認する。
付録 B 運用管理表	導入後に維持する項目の確認表	導入・見直し時	SecurityPolicy、認証方式、証明書、Trust List、書き込み権限、ログ確認先、設定根拠を残す。
付録 C 変更・例外・定期レビュー表	変更・例外・見直しの記録表	変更・例外・レビュー時	OS 更新、証明書更新、Gateway/Wrapper 更新、Anonymous 許可、SecurityPolicy None 等の例外、Classic/DCOM 残置の見直しを管理する。
01_OPC_UA 接続・運用管理台帳	付録 A～C を Excel で扱う主たる参考テンプレート	最初に使う	付録 A～C を Excel で継続管理したい場合に使う。まずは「01_接続・移行確認」の必須項目だけでよい。
02_資産管理台帳	資産・ネットワーク詳細の任意詳細版	必要に応じて使う	資産 ID、ホスト名、OS、IP、Endpoint、OPC UA 役割、管理部署などを詳細に管理したい場合に使う。既存の資産台帳がある場合は、無理に二重管理しない。
03_証明書管理台帳	証明書期限・更新管理の任意詳細版	必要に応じて使う	証明書 ID、有効期限、更新担当、格納先、更新手順、失効・期限接近を個別管理したい場合に使う。
04_UA 環境構築チェックリスト	構築・受入確認用の任意詳細版	構築・受入時に使う	新規構築、設定変更、受入試験のときに使う。日常運用の台帳ではなく、接続確認、証明書、認証、ログ、読み書き、セキュリティ設定を確認するためのチェックリストとして扱う。

01_OPC_UA 接続・運用管理台帳と 02〜04 の任意詳細版の違いは、01 が全体を追う主たる参考テンプレートであるのに対し、02〜04 は必要な分野だけを深掘りする補助資料である点です。最初から 02〜04 まで開いてすべてを埋める必要はありません。

まず 01_OPC_UA 接続・運用管理台帳で接続の全体像、移行優先度、次の対応を押さえ、資産情報、証明書、構築確認を詳しく管理したい場合だけ 02〜04 を使います。

付録 A　接続・移行確認表

接続 ID	接続元	接続先	用途	通信方式	書き込み有無	Classic/DCOM 残置	停止影響	A/B/C 分類	確認先・次の対応
OPC-001				Classic／UA／Gateway／不明	なし／あり／不明	なし／あり／不明	大／中／小／未確認	A／B／C／未判定	
OPC-002				Classic／UA／Gateway／不明	なし／あり／不明	なし／あり／不明	大／中／小／未確認	A／B／C／未判定	
OPC-003				Classic／UA／Gateway／不明	なし／あり／不明	なし／あり／不明	大／中／小／未確認	A／B／C／未判定	

注：未確認の項目は空欄にせず、「未確認」と記入し、確認先と次の対応を残してください。

付録 B　運用管理表

管理項目	確認すること	状態	管理担当	見直し時期	備考
通信保護設定	SecurityPolicy、MessageSecurityMode、例外有無	OK／要確認／例外あり			
認証方式	Anonymous、UserName、証明書認証の扱い	OK／要確認／例外あり			
証明書	発行元、有効期限、更新担当、配置先	OK／要確認／期限接近			
Trust List	登録理由、承認者、不要証明書の有無	OK／要確認／削除要			
書き込み権限	書き込み可能タグ、承認者、ログ確認先	OK／要確認／過大疑い			
ログ確認先	接続失敗、認証失敗、証明書エラー、書き込み履歴	OK／一部不明／不明			
設定根拠	なぜその設定にしたか、誰が承認したか	OK／要確認／未記録			

付録 C　変更・例外・定期レビュー表

区分	対象	確認すること	状態	期限・見直し日	承認者・確認者	次の対応
変更	OS 更新	接続、証明書、ログ、Gateway 影響を確認したか	OK／要確認／対象外			
変更	証明書更新	更新後に Trust List と接続試験を確認したか	OK／要確認／対象外			
変更	Gateway/Wrapper 更新	変換区間、品質情報、タイムスタンプ、ログに差異がないか	OK／要確認／対象外			
例外	Anonymous 許可	理由、範囲、補完策、解除期限があるか	例外あり／期限超過／解除済			
例外	SecurityPolicy None 等	本番系で残す理由と補完策があるか	例外あり／期限超過／解除済			
レビュー	Classic/DCOM 残置	残置理由、期限、解消予定を見直したか	OK／要確認／期限超過			
レビュー	証明書・Trust List	不要証明書、期限切れ、未承認証明書を確認したか	OK／要確認／削除要			

別紙 Excel 版について

別紙 Excel 版「01_OPC_UA 接続・運用管理台帳（参考テンプレート）」は、本付録 A〜C を詳細化したものです。本文と付録では最小限の確認項目を示し、実務で継続管理する場合は、この Excel 版へ展開して使用できます。

資産情報、証明書情報、UA 環境構築・受入確認をさらに詳細に管理したい場合は、任意の詳細版として「02_資産管理台帳」「03_証明書管理台帳」「04_UA 環境構築チェックリスト」を必要に応じて使用できます。

記入例は仮想例で、特定製品の推奨構成や本番環境での実証結果を示すものではありません。各社の設備構成、既存の管理台帳、変更管理ルール、セキュリティ管理ルールに合わせて、自由に改変して使用してください。

用語集

本書で使用する専門用語を以下に整理します。各章に散在していた用語解説を統合し、五十音順・アルファベット順に配置しました。各用語の詳細な使用文脈については各章の本文を参照してください。

用　語	説　明
A/B/C 分類	OPC UA への移行優先度の分類。最優先の A（3 か月以内）、設備更新等に合わせる B、当面現状維持とする C の 3 段階で管理する。（→第 7 章）
AccessLevel UserAccessLevel RolePermissions	OPC UA のアクセス権限定義。タグ自体の公開範囲（AccessLevel）、ユーザ毎の実効権限（UserAccessLevel）、役割毎の権限（RolePermissions）を細微に制御する。（→第 3 章、第 9 章、第 10 章）
Anonymous（アノニマス）認証	接続者を特定せずに誰でも接続を許可する匿名認証方式。監査ログが残らず権限の細分化もできないため、本番環境では原則無効化が推奨される。（→第 8 章、第 9 章、第 10 章）
COM/DCOM	Windows のアプリ間通信技術。OPC Classic の基盤だが、ファイアウォール通過などの設定が複雑で、Windows OS の更新による接続影響を受けやすい。（→第 2 章、第 3 章、第 8 章）
CRA（欧州サイバーレジリエンス法）	デジタル接続製品にセキュリティ対策と脆弱性対応を義務付ける欧州法案。OT 環境における接続・認証・ログなどの説明責任を高める背景となっている。（→第 1 章、第 5 章）
DCS	分散型制御システム。製造プロセスの制御ユニットを分散配置して統合管理するシステムであり、OPC データの主要な接続元・接続先となる。（→第 2 章）
DCOM/RPC	DCOM とリモート手続き呼び出し（RPC）の組み合わせ。OPC Classic のリモート接続で用いられ、設定が複雑で OS 更新やネットワーク設定の影響を受けやすい。（→第 3 章、第 8 章）
DoS 攻撃	大量の通信要求でシステムを過負荷にし、正常なサービスを妨害する攻撃。防ぐにはネットワーク境界防御（ファイアウォールや帯域制限）による多層防御が必要。（→第 10 章）
エンドポイント（Endpoint）	OPC UA サーバの接続窓口。サーバ URL、セキュリティポリシー、メッセージセキュリティモードの組み合わせで定義され、不要な窓口の公開は避けるべきとされる。（→第 3 章、第 9 章、第 10 章）
ERP	企業の会計、生産、販売などの業務データを統合管理する基幹業務システム。OPC UA が連携する上位システムの一つ。（→第 2 章）
Gateway（ゲートウェイ）	OPC Classic（DA 等）と OPC UA の通信を仲介・相互変換するソフトウェアや機器。下位に Classic 区間が残るため、DCOM 等のリスク管理が引き続き必要。（→第 6 章、第 7 章、第 8 章）
HMI	操作員が設備の監視や操作を行うための端末・画面インターフェース。OPC 通信においては、主にクライアント側として機能する。（→第 2 章）
ヒストリアン（Historian）	工場やプラントの操業データを時系列で高速・大量に記録・蓄積するデータベースシステム。OPC UA のデータ連携先となる。（→第 2 章）
IT	情報技術。MES や ERP など業務・情報系システムの領域を指し、OT-IT 連携において制御データの分析や経営管理への活用先となる。（→第 2 章）
監査ログ（監査イベント）	接続、認証、証明書イベント、データ書き込みなど、セキュリティやシステム操作の履歴を時系列で自動記録する OPC UA の標準機能。（→第 3 章、第 9 章、第 10 章）
権限	読み書きや設定変更を実行可能なユーザ・グループの範囲定義。ロール（役割）やタグ単位できめ細かなアクセス制御を行う。→「AccessLevel…」も参照。（→第 3 章、第 9 章）

MES	製造実行システム。工場の生産計画や作業指示、実績、品質管理などを行うシステムで、OPC UA と連携して現場データを収集する。（→第 2 章）
MessageSecurityMode	OPC UA 通信でメッセージ自体に署名や暗号化を施すかどうかの設定。None（無保護）、Sign（署名のみ）、SignAndEncrypt（署名＋暗号化）がある。（→第 3 章、第 9 章、第 10 章）
MITM（中間者攻撃）	通信を行う二者の中間に悪意ある第三者が割り込み、盗聴や改ざんを行う攻撃。OPC UA では通信路の署名・暗号化（Sign & Encrypt）によって防ぐ。（→第 10 章）
Native（ネイティブ）方式	新規導入や全面刷新時に、機器やソフトウェア自体が最初から OPC UA に対応している状態でシステムを構築する移行方式。（→第 7 章）
OPC	産業オートメーション分野で、異なるメーカーの機器やソフト間でデータを安全・確実に交換するための標準規格。（→第 1 章、第 2 章）
OPC A&E	OPC Classic の一つ。プロセスや機器で発生した異常（アラーム）や状態変化（イベント）を上位に通知する規格。（→第 2 章）
OPC Classic	OPC DA、A&E、HDA などの初期 OPC 規格の総称。Windows の COM/DCOM 技術に依存しており、セキュリティ設定や OS 更新の影響を受けやすい。（→第 1 章、第 2 章、第 3 章）
OPC DA	OPC Classic の代表的な規格。制御機器のプロセスデータ（タグ値）をリアルタイムに読み書きする用途に特化している。（→第 2 章、第 3 章）
OPC HDA	OPC Classic の一つ。データベース等に記録された過去の履歴データ（時系列データ）にアクセスするための規格。（→第 2 章）
OPC UA	OPC Classic の後継規格。OS 非依存で動作し、堅牢なセキュリティ機能（暗号化、証明書認証等）と高度なデータ表現力を備える。（→全章）
OT	制御運用技術。工場やプラントの物理設備を監視・制御する領域。PLC、SCADA、DCS など現場寄りのシステムが該当する。（→第 2 章）
PLC	プログラマブルロジックコントローラ。工場の設備や機械の制御を自律的に行うための産業用制御装置であり、OPC の通信先となる。（→第 2 章）
Proxy（プロキシ）方式	既存の OPC Classic（DA）クライアントから OPC UA サーバへ接続できるように仲介する方式。クライアント側の更新を必要としない。（→第 6 章、第 7 章）
Rejected（拒否済み）	OPC UA で未承認の接続要求（証明書）を一時的に隔離・保管する領域。管理者が確認して信頼済み（Trusted）へ移動するまで接続は拒否される。（→第 9 章、第 10 章）
残置管理	移行対象とならず残存する OPC Classic 機器や DCOM 設定等について、残置の理由・期限・リスク対応策・定期見直し計画を台帳に記録して管理すること。（→第 5 章、第 7 章、第 9 章）
SCADA	産業設備や各種プロセスを一元的に監視・制御し、データを収集・表示する上位システム。（→第 2 章）
SecureChannel（セキュアチャネル）	OPC UA クライアントとサーバ間で確立される暗号化された通信路。セキュリティポリシーにより通信保護強度が定義される。（→第 3 章、第 10 章）
SecurityPolicy（セキュリティポリシー）	OPC UA で使用する暗号化アルゴリズムや通信保護方式の組み合わせ（None、Basic256Sha256 など）の定義。（→第 3 章、第 8 章、第 9 章、第 10 章）
SIEM	セキュリティ情報およびイベント管理。各種システムから収集したログをリアルタイムに一元分析し、サイバー攻撃や異常の早期検知を図るシステム。（→第 10 章）

Sign & Encrypt（署名＋暗号化）	OPC UA のセキュリティ設定において、データの盗聴を防ぐ「暗号化」とデータの改ざんを防ぐ「電子署名」を同時に適用する動作モード。（→第 10 章）
接続台帳	工場・拠点内のすべての OPC 通信について、接続元・先、用途、バージョン、責任部署、DCOM 等の残置有無などを一覧にした管理用台帳。（→第 6 章、第 7 章、付録 A）
証明書（Certificate）	クライアントやサーバが正当な接続相手であることを証明するためのデジタル身分証明書。OPC UA では X.509 規格に準拠する。（→第 3 章、第 8 章、第 9 章、第 10 章）
自動受入れ（auto-accept）	未知の証明書を自動的に信頼リストへ追加する検証用の利便機能。本番環境での有効化はセキュリティ上の致命的な脆弱性となる。（→第 8 章、第 9 章、第 10 章）
秘密鍵	デジタル証明書と対となる非公開の暗号鍵情報。なりすましを防ぐために厳重に保護し、保管やアクセス権限、バックアップを管理する。（→第 9 章）
多層防御（Defense in Depth）	複数の防御層を組み合わせてシステム全体を保護するアプローチ。OPC UA 設定のほか、ファイアウォール、SIEM 監視等を組み合わせる。（→第 10 章）
Trust List（信頼リスト）	接続を信頼する相手（クライアントまたはサーバー）のデジタル証明書を登録しておくホワイトリスト。リスト外の相手からの接続は拒否される。（→第 3 章、第 8 章、第 9 章、第 10 章）
Trusted（信頼済み）	デジタル証明書が「信頼リスト（Trust List）」に登録され、正常に接続が許可されている状態。（→第 9 章、第 10 章）
Wrapper（ラッパー）方式	既存の OPC Classic（DA）サーバにかぶせ、OPC UA サーバのように振る舞わせる変換方式。既存サーバ側の更新が不要。（→第 6 章、第 7 章）

巻末参考資料一覧

- CISPA （Alessandro Erba 氏らの研究） 「OPC UA Rogue Server Attack PoC」
  https://publications.cispa.saarland/3421/
- MITRE Corporation 「MITRE ATT&CK for ICS」
  https://attack.mitre.org/matrices/ics/
- OPC Foundation 「OPC UA Security Architecture」
  https://opcfoundation.org/security/
- Microsoft 「DCOM Hardening （CVE-2021-26414）」
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26414
- Toshiaki Honda 「Industrial Control Systems and OPC UA Research on encrypted communication monitoring and inappropriate command detection」
  https://nitech.repo.nii.ac.jp/records/6967
- B. Farnham, R. Barillère, CERN, Geneva, Switzerland 「MIGRATION FROM OPC-DA TO OPC-UA」
  https://proceedings.jacow.org/icalepcs2011/papers/mopms025.pdf
- Tom Hannelius Mikko, Salmenperä, Seppo Kuikka 「Roadmap to adopting OPC UA」
  https://ieeexplore.ieee.org/document/4618203/
- WOONGGY KIM MINYOUNG SUNG 「Standalone OPC UA Wrapper for Industrial Monitoring and Control Systems」
  https://doi.org/10.1109/ACCESS.2018.2852792
- IEC （国際電気標準会議） / ISA 「IEC 62443 シリーズ」
  https://www.iec.ch/blog/understanding-iec-62443
- NIST「NIST SP 800-82r3 （Guide to OT Security）」
  https://csrc.nist.gov/pubs/sp/800/82/r3/final
  OPC Council Japan, Technical Committee 「OPC UA のセキュリティ対策と証明書の運用」
  https://jp.opcfoundation.org/
- 日本 OPC 協議会 技術部会 「OPC UA 情報モデルの設計ガイドライン バージョン 1.0」
  https://opcfoundation.org/wp-content/uploads/2025/10/library_whitepaper_UAInformationModel_r3.pdf

- European Commission 「EU Cyber Resilience Act」
  https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
- OPC Foundation 「What is OPC?」
  https://opcfoundation.org/ja/about/what-is-opc/
- European Commission 「NIS2 Directive: securing network and information systems」
  https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
- OPC Foundation 「OPC Unified Architecture - Part 2: Security Model」
  https://reference.opcfoundation.org/specs/OPC-10000-2
- OPC Foundation「The OPC UA Security Model for Administrators」
  https://opcfoundation.org/wp-content/uploads/2014/05/OPC-UA_Security_Model_for_Administrators_V1.00.pdf
- OPC Foundation 「OPC Unified Architecture - Part 4: Services」
  https://reference.opcfoundation.org/specs/OPC-10000-4
- OPC Foundation 「OPC Unified Architecture - Part 8: Data Access」
  https://reference.opcfoundation.org/specs/OPC-10000-8
- OPC Foundation 「OPC Unified Architecture - Part 12: Discovery and Global Services」
  https://reference.opcfoundation.org/specs/OPC-10000-12
  Microsoft 「KB5004442 - Manage changes for Windows DCOM Server Security Feature Bypass （CVE-2021-26414）」
  https://support.microsoft.com/help/5004442
- Microsoft 「Microsoft Lifecycle - Windows Server 2012 / Windows Server 2012 R2」
  https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2012
  https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2012-r2
- IANA 「Service Name and Transport Protocol Port Number Registry - port 4840」
  https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?search=4840
- Industrial Digital Twin Association （IDTA） 「Asset Administration Shell Specifications」
  https://industrialdigitaltwin.org/en/content-hub/aasspecifications

商標について

本文中に記載されている会社名、製品名、サービス名は、各社の商標または登録商標である場合があります。本書では説明のためにこれらを使用しており、特定製品の推奨、保証、認定を示すものではありません。