

2026 年 10 月 27 日

オムロン株式会社

NTT ドコモビジネス株式会社

オムロンと NTT ドコモビジネス、製造現場のサイバー脅威に挑む

～FA と IT の知見を融合し、OT/IT 統合セキュリティの設計から運用・教育までをワンストップで支援～

オムロン株式会社(本社:京都府京都市、代表取締役社長 CEO:辻永 順太、以下オムロン)と NTT ドコモビジネス株式会社(旧 NTT コミュニケーションズ株式会社、本社:東京都千代田区、代表取締役社長:小島 克重、以下 NTT ドコモビジネス)は、製造現場の OT(Operational Technology)領域から IT 領域までを統合的に守る「OT/IT 統合セキュリティ」の協業(以下、本協業)を開始します。

両社は、オムロンのファクトリーオートメーション(以下 FA)^{*1} システムと、NTT ドコモビジネスの OT/IT セキュリティソリューションに加え、NTT グループ各社^{*2} のグローバル提供体制、研究開発技術を組み合わせ、製造現場の安定稼働とサイバーセキュリティ対策の両立を支援することをめざします。

1. 背景

製造業では、IoT や AI を活用した生産性向上、予兆保全およびエネルギー利用の効率化に向け、製造現場のデータ活用が進んでいます。一方、IT ネットワークと製造現場の OT ネットワークの接続機会が増え、直近では、AI を悪用したサイバー攻撃をはじめ、外部からの不正アクセスやマルウェア感染など、事業継続に影響を及ぼすセキュリティリスクへの対応がより一層求められています。また、欧州ではサイバーレジリエンス法(CRA)^{*3} など規制への対応が求められており、グローバルに事業を展開する製造業にとって、OT セキュリティ対策の重要性は格段に高まっています。

オムロンと NTT ドコモビジネスは、2022 年 10 月から FA 技術と IT ソリューションを活用した企業間データ連携の共同開発や、データスペース接続の実証実験に取り組んできました。また、2025 年 10 月からは、オムロンのデータフローコントローラ「DX1」^{*4}と、NTT ドコモビジネスの多様なセキュリティ機能とネットワーク機能を統合した NaaS(Network as a Service)^{*5}である「docomo business RINK[®]」などを組み合わせ、製造現場の OT データをクラウドやデータスペース^{*6}へ安全に接続する取り組みを推進しています。

加えて、両社はセキュリティ機能の拡充や対応設備の拡大などを通じて、製造現場におけるデータ活用を支援してきました。こうした連携で培った知見と実績を基盤に、製造現場の安定稼働と安全なデータ活用を支える OT/IT 統合セキュリティの実現に向け、本協業を開始します。

2. 本協業の概要

これまでの両社の取り組みを発展させ、オムロンが提供する、製造現場で稼働する PLC^{*7} に代表されるコントローラおよびセンサやドライブなどの入出力機器で構成される FA システムと、NTT ドコモビジネスが提供する「OsecT」^{*8}をはじめとする OT/IT セキュリティソリューションを組み合わせ、IT ネットワークから製造現場までを一体としてとらえたセキュリティリスクの可視化から対策の導入、監視・運用、教育までを支援するサービスの提供に向けた取り組みを進めます。

オムロンが長年培ってきた製造現場に関する知見と NTT ドコモビジネスの豊富な OT/IT セキュリティソリューションを組み合わせることで、IT 起点の標準的な対策にとどまらず、製造現場の運用実態に適した対策設計と運用支援をワンストップで提供することをめざします。具体的には、以下の 3 点に取り組みます。

(1) 両社による OT/IT セキュリティソリューションの提供

製造現場のセキュリティ対策には、IT 領域における標準的な対策に加え、設備構成や生産ラインの稼働状況、保全業務など、OT 領域特有の運用実態を踏まえた設計・導入が求められます。両社は、IT ネットワークから OT ネットワークまでを対象とした可視化・脅威検知をはじめ、OT/IT 統合セキュリティアセスメントやポリシー策定・体制構築、IT ネットワークと OT ネットワークの分離、セキュアリモートアクセス環境の構築、24 時間 365 日のセキュリティ監視、制御システムセキュリティ教育、インシデント対応訓練などを通じて、OT と IT の境界に生じるセキュリティの死角を低減します。

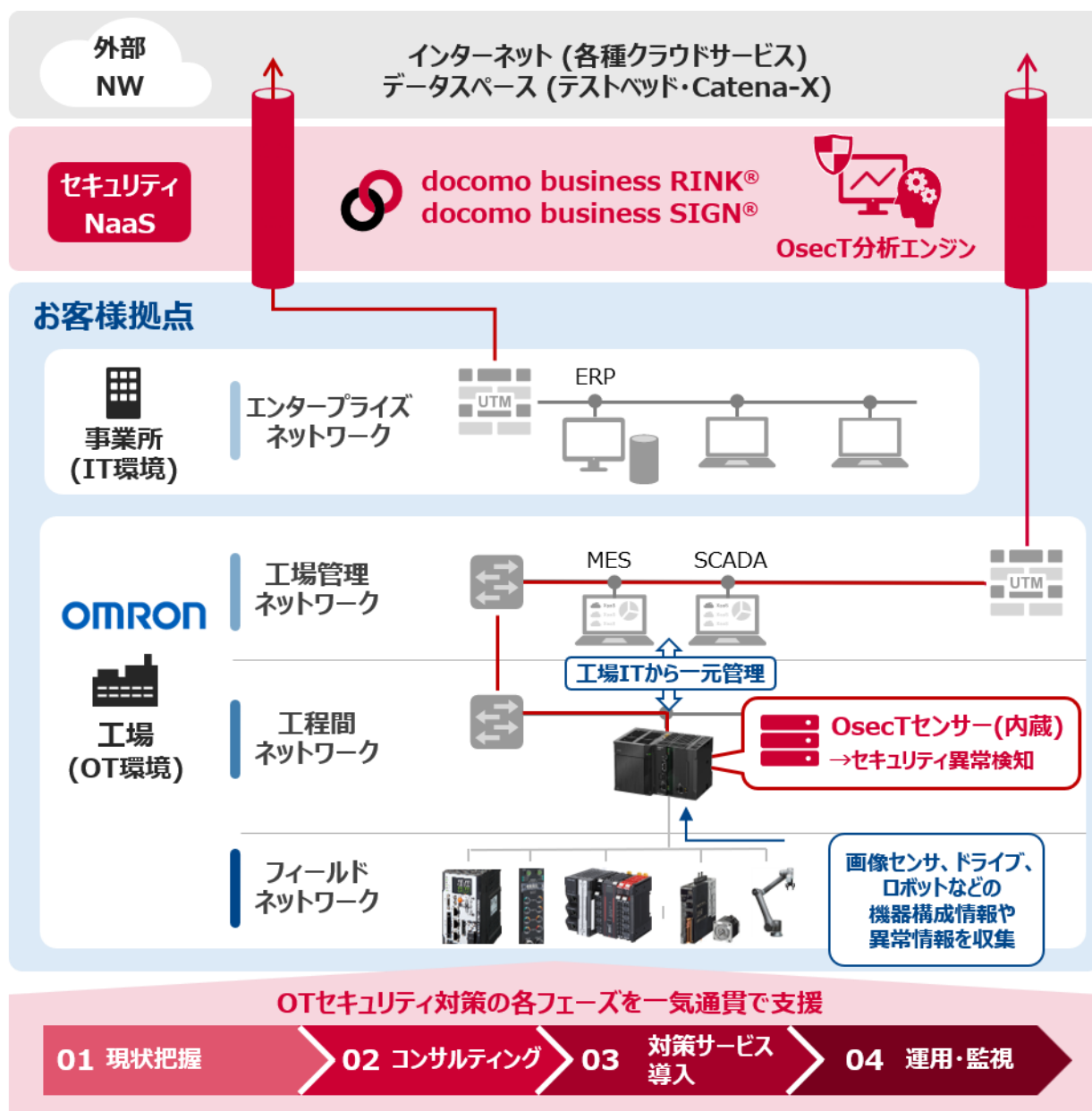
さらに、製造現場を起点に「生産性の向上とセキュリティ対策の両立」をめざし、セキュリティ機能を備えたコントローラなどの制御機器の提供や製造現場の可視化に取り組むとともに、インシデント発生時の早期復旧を支援します。両社はこれらを組み合わせ、国内外のお客さまに OT/IT セキュリティソリューションとして一体的に提案・提供します。

(2) オムロンのコントローラと NTT ドコモビジネスの OsecT 融合による製造現場の監視・可視化

オムロンのコントローラ製品に OsecT の不正通信検知センサ機能^{*9}の組み込みに向けた開発を進めます。本機能をコントローラに組み込むことで、ネットワーク機器を介したセキュリティ監視に加え、これまでネットワーク側からの把握が難しかった、製造現場のセンサやドライブなどの入出力機器に関する構成情報も、コントローラを介して取得・可視化できる仕組みの実現をめざします。さらに、これらの情報を MES^{*10}や SCADA^{*11}など工場管理ネットワーク上のシステムで一元的に管理することで、製造現場のセキュリティ対策の強化と、現場機器の状態のより詳細な把握をめざします。

(3) 提供モデルおよび販売体制の構築

両社の販売チャネルを活用した販売体制を構築し、装置ベンダーに向けた製品セキュリティ対応や、エンドユーザーに向けた工場全体のセキュリティ対策・運用支援など、お客さまの課題に応じた提供モデルを整備していきます。



<本協業のイメージ>

■ 各社の役割

オムロン	製造現場における FA 機器・制御技術、ならびに生産技術・保全領域に関する現場知見の提供 PLC、産業用 PC などへのセキュリティ機能や通信サービスの組み込みに向けた技術開発・検証 製造業のお客さまへの導入提案および製品提供、現場適用支援
NTT ドコモ ビジネス	「OsecT」をはじめとする OT/IT セキュリティソリューション、ネットワーク、監視・運用の提供 セキュリティアセスメント、ポリシー策定・体制構築、制御システムセキュリティ教育、インシデント対応訓練を含む導入・運用支援サービスの提供と、海外拠点を有するお客さまへのグローバル展開支援 製造業のお客さまへの導入提案およびサービス提供、システム構築

3. 今後の展開

今後、両社は製造現場におけるセキュリティ強化とデータ活用の高度化に向け、NTT グループ各社との連携を通じて、以下の3点を軸に本協業の取り組みの拡充をめざします。

- ① NTT グループの OT セキュリティソリューションを組み合わせた提供サービスの拡大(2026 年 10 月より順次開始)
- ② 株式会社 NTT DATA, Inc.および NTT セキュリティ・ジャパン株式会社を中心とした NTT グループのグローバル体制を活用した、海外拠点を有するお客さまへの支援(2026 年内 検討開始)
- ③ NTT グループが有するセキュリティおよびトラスト^{*12}に関する研究開発成果(データサンドボックス技術^{*13}、AI エージェント属性情報レジストリ技術^{*14})を活用した、製造現場の特性に適した技術実装(2027 年 検討開始)

両社は本協業を、製造現場の機器から得られた価値あるデータと知見を安全に活用する「GEMBA DX」^{*15}の実現に向けた重要な一歩と位置づけ、中長期的な技術実装・製品化・国際展開を通じて、国内外の製造業の持続的な競争力向上に貢献していきます。

*1 FA:ファクトリーオートメーションの略。工場における生産設備や制御機器を自動化・高度化する技術領域

*2 NTT グループ各社: NTT、NTT DATA, Inc.、NTT セキュリティ・ジャパン、NTT ドコモビジネスなど、本協業に関連する各社・組織。

各社の役割や提供内容は、今後の検討・協議により具体化していきます。

*3 サイバーレジリエンス法(CRA): EU で導入が進められている、デジタル要素を含む製品に対してサイバーセキュリティ要件を課す規制。製品の設計・開発・上市後の脆弱性対応などが対象となる

*4 DX1: オムロンが提供するデータフローコントローラ。製造現場のデータを収集・加工し、クラウドや外部システムとのデータ連携を支援する機器

*5 NaaS: Network as a Service の略。ネットワーク機能をサービスとして提供する形態。利用企業は機器保有や個別構築の負担を抑えながら、必要なネットワーク機能を利用できる

*6 データスペース: 企業や組織をまたいでデータを安全に共有・活用するための仕組みや基盤

*7 PLC: 工場の自動化において欠かせない、機械が動作を行うための制御装置。プログラマブル・ロジック・コントローラの略。

*8 OsecT: NTT ドコモビジネスが提供する、制御システムや製造現場を対象とした OT セキュリティソリューション

*9 不正通信検知センサ機能: 制御機器や製造現場のネットワーク上の通信を監視し、不正な通信や異常な挙動の検知を支援する機能

*10 MES: Manufacturing Execution System の略。製造実行システム。製造現場における作業指示や生産実績、品質・設備情報などを管理し、生産活動を管理・最適化するシステム

*11 SCADA: Supervisory Control And Data Acquisition の略。工場やプラントの設備・機器から稼働データを収集・監視し、遠隔からの制御を可能にするシステム

*12 トラスト: データや機器の出所・真正性を確認し、安心して取引できる状態をつくること

*13 データサンドボックス技術: データを安全に利用・検証するため、利用範囲や処理環境を制御した領域でデータ活用を行う NTT 株式会社テクノロジーイノベーションセンタ、コンピューティングテクノロジーセンタが有する研究開発技術

*14 AI エージェント属性情報レジストリ技術: AI エージェントの開発・運用主体や実行権限などの属性情報を一元的に登録・管理し、検証可能なデジタル証明書(Verifiable Credentials)により、なりすましや改ざんの検知を可能にする NTT ドコモビジネスが開発を進める技術

*15 GEMBA DX: オムロンが推進する、製造現場の制御機器や設備から得られるデータを活用し、現場課題の解決や生産性向上をめざす取り組み