

2026年3月25日

NTTドコモビジネス株式会社

**簡単導入で安価に OT セキュリティ対策を始められる NTT ドコモビジネスの
「OsecT」が、「Global InfoSec Awards 2026」にて 6 部門受賞
～「Market Disruptor OT Security」賞を含む 6 部門を受賞～**

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、以下 NTTドコモビジネス)が提供中の OT^{*1}セキュリティサービス「OsecT^{*2}」(以下 本サービス)は、米国の大手セキュリティ情報誌 Cyber Defense Magazine(以下 同誌)が 2026年3月24日(現地時間)に発表した「Global InfoSec Awards 2026」において「Market Disruptor OT Security」賞を含む 6 部門で賞を受賞しました。

今回受賞した本サービスは、幅広い企業に対する OTセキュリティサービスの普及を目的とした、安価で簡単に導入可能な国産 OT-IDS^{*3}です。



1. 賞の内容

「Global InfoSec Awards」は、サイバーセキュリティ分野において、製品に独自の価値があると評価された企業を対象とする賞で、今年で 14 回目を迎えます。CISSP^{*4}などの認定セキュリティ専門家で構成された審査員が、革新性、ソリューションの独自性、市場への影響力、現実のサイバーセキュリティ課題への対応力を基準に評価の上、受賞企業を決定します。

「OsecT」は、最先端のサイバーフィジカルシステムセキュリティプロダクト^{※5}に対して授与される「Market Disruptor OT Security」賞を筆頭に、「Cutting Edge Cyber Physical Systems (CPS) Cybersecurity」賞「Visionary ICS^{※6}/SCADA^{※7} Security」賞、「Best Solution Internet of Things (IoT) Security」賞、「Pioneering Managed OT Security (MOTS)」賞、「Editor's Choice OT Asset Visibility」賞の合計6部門で賞を受賞しました。

<受賞式の模様(左からプラットフォームサービス本部 マネージド&セキュリティサービス部 セキュリティサービス部門 担当課長 英敏秀、同部門 担当部長 戸畑洋介)>



2. 評価のポイント

審査員による評価のポイントは以下の通りです。

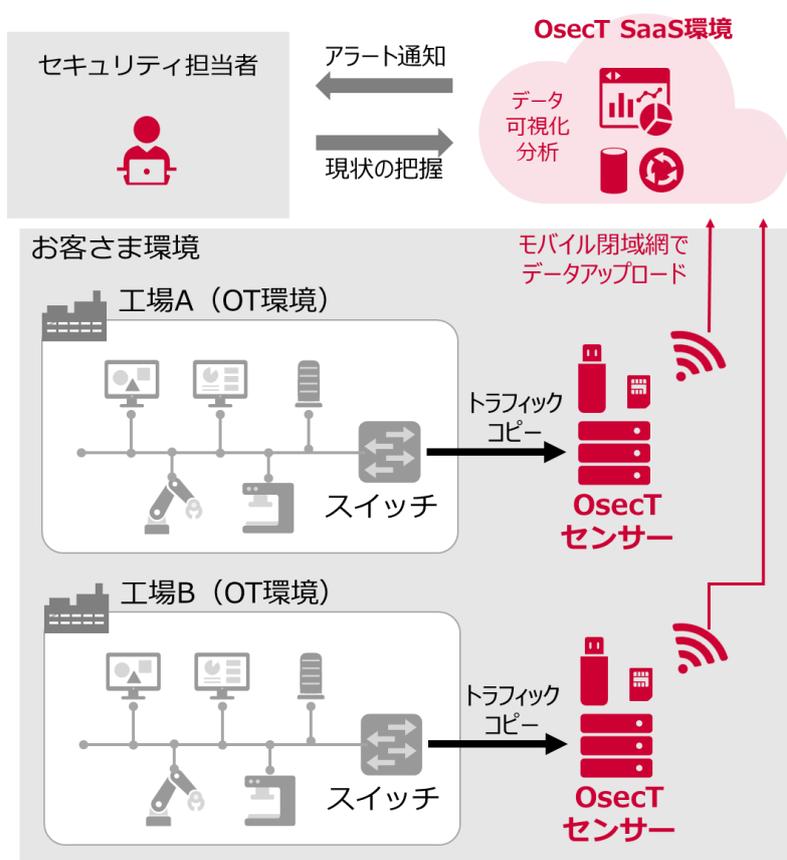
- ・サイバーフィジカルシステムおよび ICS/OT 環境の保護における高い革新性
- ・ICS/SCADA セキュリティおよび OT 資産の可視化に対する先進的なアプローチ
- ・IoT およびマネージド OT セキュリティ機能における顕著な進歩
- ・重要インフラおよび OT ネットワークの保護を支援する明確な市場インパクト

3. 本サービスの概要と特長

NTT ドコモビジネスは、大企業から中小企業まですべての企業を対象に、工場やプラントなどに使われる生産設備などを最適に動かす OT システムのセキュリティ対策を推進しています。

本サービスは、工場などの OT 環境のトラフィックデータをセンサー機器を介して収集・蓄積・分析することで、異常な通信の早期発見を実現します。具体的には、OT 環境内のデータ通信を、「OsecT」センサー経由で分析を行う「OsecT」 SaaS 環境に流すことで、OT 環境に設置された機器の OS バージョンや機器同士の接続構成を見える化します。加えて、未知の機器接続、不自然な流量の通信などの異常を早期発見します。

<「OsecT」 SaaS 版^{※8}のサービスイメージ>



主な特長として以下の点があげられます

- ① OT-IDSの基本機能である「OTネットワークの可視化」と「サイバー脅威の早期検知」機能を具備しながら、既存製品と比較して大幅に安価である点
- ② モバイル閉域網の付属により、メンテナンスやクラウド連携のための回線敷設不要で、センサー機器を既存OT環境のスイッチにLANケーブルを接続するだけで、簡単に導入可能である点
- ③ SaaS上に配備されたWebポータルにより、遠隔地のセキュリティ担当者が各地の工場のデータを一元的に監視、把握できる点

- ④ センサーから SaaS への通信はモバイル閉域網を利用、SaaS 上の Web ポータルは弊社にて管理しているため、お客さまによる ASM^{※9}が不要である点
- ⑤ ソフトウェアは弊社による内製開発のため、お客さま/販売パートナー様の要望を取り込みやすい点。また、ハードウェアも含めて完全国産にてご提供可能な点。
- ⑥ 発出されたセキュリティアラートについてのお問い合わせが可能なセキュリティ運用サポートが付帯可能な点

4. 今後の展開

2026 年内に、IT 領域と OT 領域を横断した SOC サービスの提供開始、ASEAN 地域での「OsecT」の提供開始や、製造・物流システムにおける AI ロボットのセキュリティ保護領域への展開をめざします。

「NTT コミュニケーションズ株式会社」は 2025 年 7 月 1 日に社名を「NTT ドコモビジネス株式会社」に変更しました。私たちは、企業と地域が持続的に成長できる自律・分散・協調型社会を支える「産業・地域 DX のプラットフォーム」として、新たな価値を生み出し、豊かな社会の実現をめざします。

つながり。驚きを。幸せを。



<https://www.ntt.com/about-us/nttdocomobusiness.html>

- ※1: OT(Operational Technology)とは、工場や発電所などに使われる、システムや設備を最適に動かすための制御・運用技術の総称です。
- ※2: 「OsecT(オーセクト)」とは、工場の生産ラインなどを支える制御システムのセキュリティリスクを可視化・検知する NTT Com が提供するサービスです。
- ※3: OT-IDS とは、OT 環境のネットワークを監視するための資産可視化・侵入検知システムのことで。
- ※4: CISSP とは、安全で安心なサイバー世界の実現に向けて活動する国際的な非営利会員団体である ISC2 が認定を行っている国際的に認められた情報セキュリティ・プロフェッショナル認定資格です
- ※5: サイバーフィジカルシステムセキュリティプロダクトとは、サイバー空間と物理空間の高度な連携により実現されるサイバーフィジカルシステムに対するセキュリティプロダクトのことで。サイバーフィジカルシステムでは、物理空間の多種多様なデータを収集し、収集したデータを基にサイバー空間において各種分析を行います。分析結果を基に、物理空間に対して制御指示などの働きかけを行います。
- ※6: ICS とは、製造業や生産拠点などで用いられる産業用設備をコントロールする情報システムのことで。
- ※7: SCADA とは、ICS の一部であり、電子化されたデータ処理・制御システムを示す概念のことで。
- ※8: クラウド環境を利用しないオンプレミス版もご提供しています。
- ※9: ASM とは、外部から攻撃を受ける可能性のある資産の脆弱性対応などを管理する営みのことで。