つなごう。驚きを。幸せを。

2026 年 3 月 25 日

NTT ドコモビジネス株式会社

AI 時代の IoT 拡大に対応した
「docomo business SIGN™」のセキュリティ・コネクティビティ機能を強化

～SIM を起点としたデバイスセキュリティと、映像・AI 時代の大容量通信に対応～

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）は、「分散」「柔軟」「安全」「リーズナブル」といったニーズに対応する、AI 時代に最適な次世代 ICT プラットフォーム「AI-Centric ICT プラットフォーム®※1」構想のもと、各サービスの具現化・高度化を進めています。

今回、その取り組みの一環として、セキュリティ機能を標準搭載した IoT 向けの NaaS(Network as a Service)である「docomo business SIGN™」※2 の「Value」※3 メニューにおいて、デバイス認証や Telemetry 情報※4 の可視化を実現するアプレット SIM※5 を 2026 年 3 月 25 日より提供開始します。

併せて、高トラフィック用途に対応した、大容量通信を安価に提供するモバイル回線「Advanced」※6 メニューも同日より提供開始し、AI 時代に適した IoT システム全体の安全性と運用効率の向上を実現します。

1. 背景

近年、AI 活用の進展による IoT デバイス数の急増に加え、映像伝送や AI 解析、モデル更新などに伴う通信トラフィックの増大が見込まれています。こうした環境下では、大量の IoT デバイスを前提としたセキュリティの確保と、高トラフィック用途に耐えうる通信基盤の整備が、IoT 活用を進める企業にとって重要な課題となっています。

一方、社会インフラや製造現場などで IoT の導入が進む中、サイバー攻撃の脅威も急速に高まっています。2024 年にはサイバー攻撃関連通信数が 2015 年比で約 10.9 倍に増加し、そのうち約 3 割が IoT デバイスを標的とするなど、リスクが顕在化しています。これを受け、経済産業省が IoT 機器のセキュリティ対策ガイド※7 を発表するなど、AI 活用を含む高度な IoT 利用を進める企業には、より高度なセキュリティ対応が求められています。

こうした背景を踏まえ、NTT ドコモビジネスは、「AI-Centric ICT プラットフォーム®」構想のもと、IoT 領域におけるサービス強化を進めています。

2. 追加メニューの特長

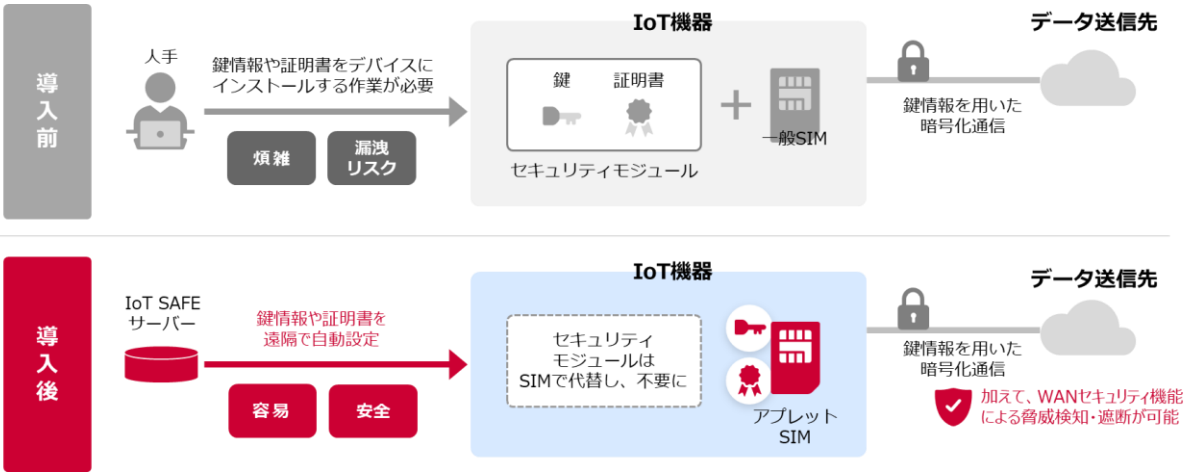
(1)docomo business SIGN™「Value」メニューでアプレット SIM を提供

アプレットSIMは、これまでの実証実験やお客さまとの共創で培ったアプレット技術※8を活用し、デバイス認証の自動化を実現する「IoT SAFE※9」や、通信状況・簡易位置情報などのデバイス情報を把握、管理できる機能である「Telemetry」を提供します。

今回、新たにdocomo business SIGN™「Value」メニューのオプション機能として提供を開始することで、従来は個別ソリューションとして提供していたアプレットSIMの機能を、ポータルから簡単にお申し込みできるようになります。また、設定などを容易に実施できるダッシュボードやサポートメニューの提供(予定)によって、専門的な開発や導入検証などを行うことなく、容易に導入・利用することが可能となります。

①IoT SAFE アプレット

IoTセキュリティの確保に向けては、不正通信や攻撃を検知する事後的な備えに加え、不正デバイスの接続やなりすましといった不正行為の発生自体を防ぐための対策も重要です。不正デバイス排除にはデバイス認証が有効となりますが、大量のデバイスへの鍵情報※10やクライアント証明書※11(以下 証明書)のインストールが必要であり、運用上の課題となります。IoT SAFE アプレットは、このような課題への解決策として、機器の電源投入時にSIM内で鍵情報と証明書を自動生成し安全に保管することにより、IoTデバイスの製造・運用時におけるセキュリティ管理負荷を大幅に低減します。IoT SAFEによるデータ・デバイスの信頼性の確保、WANセキュリティ機能による脅威検知・遮断機能(特許取得済み)との組み合わせにより、IoTシステムに対する多層的な防御が可能になります。



<IoT SAFE のイメージ>

②Telemetry アプレット

Telemetry アプレットでは、SIMアプレットが取得した情報を管理画面から遠隔で確認することができます。一般的なデバイスで、追加開発なく利用いただけるため、幅広いIoTデバイスでのトラブルの原因調査や機器管理に活用でき、お客さまの運用・保守の高度化や想定外利用の防止を実現できます。

a. 運用・保守の高度化

・デバイスが取得した電波強度：信号強度や通信品質を自動収集し、設置場所の検討やトラブル時の原因診断に活用

b. 想定外利用の防止

・基地局情報：おおよその位置を取得し、機器の利用場所や移動有無を把握可能

・SIM 入れ替え検知：機器と SIM の情報を紐づけて管理することで SIM の入れ替えを検知し、想定外の機器での利用を検知可能

<Telemetry アプレット画面イメージ　※画面は開発中のものです>

（2）5G や MEC が利用できる「Advanced」メニューを提供

「Advanced」は、5G に対応しセキュリティ機能を搭載した、キャリア網内でのデータ利活用を可能とするモバイル回線サービスです。インターネットを通らない閉域通信と、MEC（Multi-access Edge Computing）[※12] を組み合わせることで、安全なリアルタイム分析や、映像・AI 活用、ロボティクス制御など機密データや個人情報を扱う用途にも安心して利用できます。また、これらのユースケースで必要となる大容量通信に向けて、大容量でも低廉なプランを提供するとともに、外部へのデータ転送料金が不要な MEC サーバー基盤の特性により、トータルでの運用コストを抑えることが可能となります。

3．提供開始日

2026 年 3 月 25 日

4．利用料金

NTT ドコモビジネス営業担当までお問い合わせください。

5．お申し込み方法

NTT ドコモビジネス営業担当までお問い合わせください。

6. 今後の展開

今後も、「AI-Centric ICT プラットフォーム®」構想のもと、AI 時代に求められる IoT の多様な利用シーンやお客さまのニーズに対応するため、セキュリティ機能のさらなる充実や、IoT データの利活用を支える機能の拡張を進めていきます。

また、さまざまな業界・用途に対応した機能拡張や、パートナー連携を通じて、IoT システムの導入から運用、データ活用までを包括的に支援し、企業の DX 推進および新たなビジネス価値の創出に貢献していきます。

「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 のプラットフォーマー」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。

つなごう。驚きを。幸せを。
docomo Business https://www.ntt.com/about-us/nttdocomobusiness.html

※1：AI-Centric ICT プラットフォームとは、企業が AI を活用して、生産性の抜本的改善、競争力強化やビジネスモデル変革を進める AI 時代に最適な次世代 ICT プラットフォームのことです。

※2：報道発表セキュリティ機能を標準搭載した新たな IoT サービス「docomo business SIGN」の提供を開始(2025 年 9 月 26 日)

※3： Value とは、docomo business SIGN が提供する回線アクセスメニューの 1 つです。セキュリティ機能付きでシンプルな IoT 向けモバイル回線です。

※4：Telemetry 情報とは、遠隔地にあるデバイスから自動的に収集される状態データのことです。

※5：アプレット SIM とは、弊社が提供するアプレットを利用可能な SIM カードをご提供するメニューのことです。

※6：Advanced とは、docomo business SIGN が提供する回線アクセスメニューの 1 つです。大容量向けであり、5G 回線が利用できます。

※7：IoT 機器のセキュリティ対策ガイドは、経済産業省発行の「IoT 機器を開発する中小企業向け製品セキュリティ対策ガイド」です。https://www.meti.go.jp/policy/netsecurity/chusyosecurityguide.pdf

※8：アプレット技術とは、SIM カード内の IC チップに組み込まれて実行される Java ベースの小さなプログラムに関する技術のことです。

※9：IoT SAFE とは、モバイル通信 SIM 内に格納されたセキュリティ機能を持つアプレットを活用し、IoT デバイスとクラウド間の通信を暗号化・認証するセキュリティ方式です。

※10：鍵情報は、データの安全な通信、デジタル署名、認証などのセキュリティ対策で用いられます。

※11：クライアント証明書とは、特定のサービスやシステムへのアクセスを許可されたユーザーやデバイスであることを証明する電子証明書のことです。

※12：MEC(Multi-access Edge Computing)とは、5G 通信において活用される、端末の近傍（キャリア網内など）にサーバーを配置して効率的なデータ処理を行う「エッジコンピューティング」技術のことです。