スマート制御クラウドサービス“DIAPLANET”

"DIAPLANET"：Cloud Services for IoT/M2M Systems

近年，モノのインターネット(Internet of Things：IoT)の普及によって，多種多様な機器がインターネットに接続可能となり，それらの機器に対する遠隔からの制御・監視・情報収集のニーズが高まっている。同時に，多数の機器から収集したセンサデータを分析・可視化することで，制御の高度化や業務の効率化など新しいサービスの創出が求められている。

今回，M2M(Machine to Machine)通信制御やデータ分析，連携機能を標準で提供し，接続機器選定からアプリケーション構築までをワンストップでシステム構築できるスマート制御クラウドサービス“DIAPLANET(ダイヤプラネット)”の提供を開始した。これによって，これまで個別に構築していたため困難であったシステムの組合せをクラウド上で容易に実現でき，複数機器を高度に制御することで業務を効率化できる。また，DIAPLANETのPaaS(Platform as a Service)機能を活用したエネルギー管理サービスなどのSaaS(Software as a Service)を順次展開していく。DIAPLANETのサービスの主な特長は次のとおりである。

(1) 豊富なPaaS機能によって，IoTシステムをワンストップでシステム構築可能

①M2M通信制御によって，クラウド上で複数の機器を制御することができる。

②当社独自のデータウェアハウス機能によって，長期間にわたって収集した大容量のセンサデータを高速で集計・分析し，搭載するリアルタイム分析機能で故障検出・予兆分析・エネルギー監視を実現できる。

(2) 事前に導入後の効果を検証するトライアル支援サービスを提供

①システム導入検討時に導入後の効果をあらかじめ検証することで，投資リスクを低減できる。また，システム拡張を容易に実現できるため，小規模構成からの適用スタートが可能である。

②コンサルティングを含めた支援サービスの提供によって，ビッグデータの活用方法を提案できる。

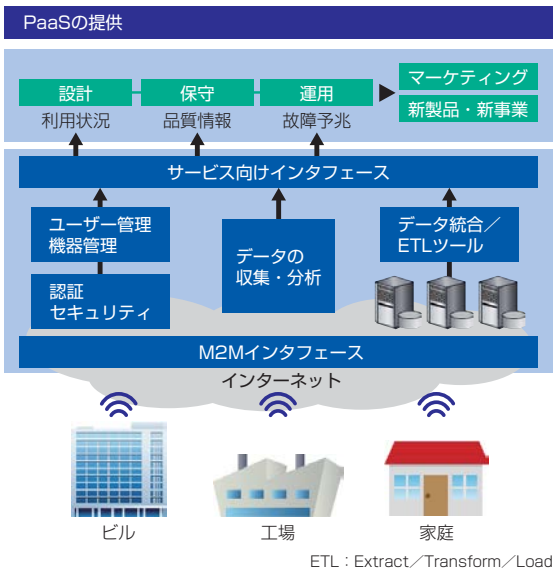
(3) 安全なクラウド基盤を提供

①総務省による情報セキュリティ対策ガイドラインに対して，データセンターを運営している当社のセキュリティ基準を更に加えることで，高いセキュリティ管理レベルを実現できる。

②メンテナンス操作を管理者接続用VPN(Virtual Private Network)経由に限定とすることで，不正侵入リスクを低減できる。

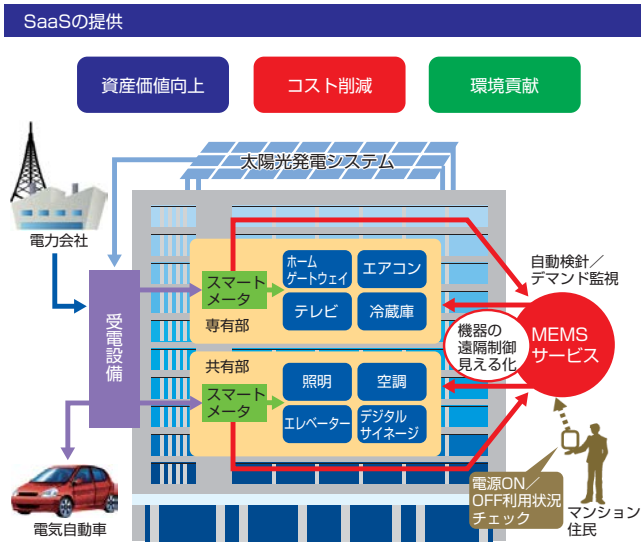
③ウイルス及び脆弱(ぜいじゃく)性対策などの最新の総合セキュリティ技術の採用によって，クラウド基盤の安全性を確保できる。

今後は，DIAPLANETのサービスとして，機器との接続性の強化(当社製機器との接続性保証，代表的な通信プロトコルのサポート拡充など)，IoT／M2Mシステムのサービスインを大幅に短縮するSaaS層の充実など，より高度なサービスを順次提供していく予定である。



ETL：Extract／Transform／Load

M2Mプラットフォームサービス



MEMS：Mansion Energy Management System

MEMSサービス

マイナンバーを安全に集中管理する“パッケージプラス マイナンバーロッカーシステム”

Securely Centralized System for MyNumber "PACKAGEplus MyNumberLocker System"

2016年１月に運用が開始される社会保障・税番号制度（マイナンバー(注)制度）では，重要な個人情報であるマイナンバーをいかにして企業で管理・運用するかが大きな課題である。㈱三菱電機ビジネスシステム（MB）が提供する“パッケージプラス マイナンバーロッカーシステム”（以下“マイナンバーロッカー”という。）は，マイナンバーを高度なセキュリティ環境下で管理・運用するとともに，既に企業で利用されている関連システム（給与計算システム，社会保険労務システム）と柔軟な連携を可能としたシステムである。マイナンバーロッカーのイメージを**図１**に示す。

マイナンバーロッカーでは，給与計算システム等の関連するシステムからの要求に応じて，マイナンバーにアクセスするためのアプリケーションプログラミングインタフェース（API）を提供し，マイナンバーを独立した形で取り扱うことで“取得・保管・利用・提供・廃棄”のライフサイクルを管理できる。また，重要な個人情報となるマイナンバーを他システムから独立して管理し，マイナンバーを含むデータベースや他システムとの通信を暗号化することで“物理的安全管理措置”及び“技術的安全管理措置”に対応している。

マイナンバーロッカーの特長は次のとおりである。

(1)　マイナンバーを完全に独立した形で管理可能

マイナンバーを，各システムに点在させることなく，システムから独立させて集中管理する。

(2)　セキュリティを十分考慮したシステム設計

マイナンバーは，データベース上・通信上いずれも暗号化する。また，本人確認に関する情報（通知カードのスキャンデータ等）は保管しない。

(3)　法人番号を活用した複数会社管理，社会保険労務士業務，個人事業主等への対応

社会保険労務士や個人の事業主も利用可能であり，また，さらに法人番号を利用してグループ会社などの複数の会社を一括管理することができる。

(4)　厳重な利用ログ収集と管理

アクセスログを厳重に管理し，目的外の利用はできないよう制御する。

(5)　定期的なマイナンバー廃棄処理

利用期限の切れたマイナンバーの一括廃棄処理と廃棄証明書の出力ができる。

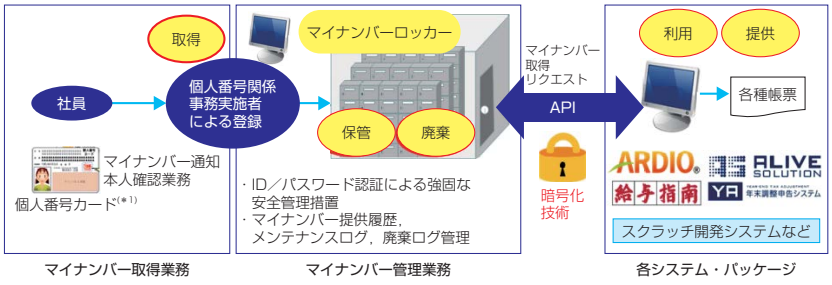
(6)　マイナンバーロッカー単体での導入が可能

マイナンバーロッカーだけを単独で導入し，運用することができる。

(7)　他システムやスクラッチ開発システムとのAPI連携が可能

他システムとの連携も視野に入れてAPIを標準装備し，他社のパッケージ製品やその他スクラッチ開発システムなどとマイナンバーのデータ連係が容易に実現できる。

国は，マイナンバー制度に対する国民の懸念に対し，“制度面における保護措置”と“システム面における保護措置”を定めている。マイナンバーロッカーは**表１**に示すとおり“システム面における保護処置”に着目してシステム要件を設定し，必要な機能を提供している。



マイナンバーの“取得・保管・利用・廃棄”を一元管理するデータベース機能
給与計算システム等から要求に応じてマイナンバーを提供するインタフェース機能
マイナンバー提供履歴，メンテナンス履歴を管理するログ管理機能

＊１　内閣官房社会保障・税番号制度のホームページ（http://www.cas.go.jp/jp/seisaku/bangoseido/）に掲載されている“事業者向けマイナンバー広報資料（平成27年2月版）”６頁記載の画像を引用

図１．マイナンバーロッカーのイメージ

表１．システム面における保護処置に対する提供機能

着目点	システム要件	必要な機能
機密性	特定個人情報は機密情報のため，各システムに点在させることなく独立集中管理する。	独立集中管理
	情報が正当な権限を持つ者以外に利用されないように保護する。	権限管理
	マイナンバーはデータベース上，通信上いずれも暗号化する。	マイナンバー暗号化
	インターネット接続を前提としたシステムにしない。	オンプレミス対応
正当性	利用権限があっても目的外の利用はできないようにする。	利用目的管理
	厳重なアクセスログ，操作ログの収集と管理が必要である。	ログ管理
	利用期限の切れたマイナンバーの一括廃棄処理と廃棄証明書の出力が必要である。	一括廃棄更新
	本人確認の履歴（日付・確認者情報・確認方法）を残すことが望ましい。	本人確認履歴
利便性	自社だけでなく顧問先・個人事業主・グループ会社も管理できるようにする。	複数会社対応
	個人を識別するコード体系がシステムごとに異なる場合にも対応可能にする。	個人ID変換機能
	外部のシステムとマイナンバーの登録・参照ができるようにする。	API装備
	クライアントサーバシステム，Webアプリケーションシステムのどちらにも対応可能にする。	複数API装備
効率性	マイナンバーを管理するシステムであり，行政機関等へ提出する帳票そのものを作成するシステムとはしない。	既存システムの有効利用
	特定個人情報を画面入力だけでなく，一括取り込みを可能とする。	一括取込機能
準拠性	利用目的の拡大等，今後の法律改正に対応可能とする。	利用目的管理

＜取り扱い：㈱三菱電機ビジネスシステム　TEL：03－5309－0621＞