ISSN 0369-2302/CODEN:MTDNAF

MITSUBISHI ELECTRIC
Changes for the Better

三菱電機技報

5
2023
Vol.97 No.5

サステナブルな社会と企業のDX推進に資するITソリューション

No.5

特　集　サステナブルな社会と企業のDX推進に資するITソリューション　IT Solutions that Contribute to Sustainable Society and Corporate DX Promotion

巻 頭 言

三菱電機では，サステナビリティ経営を実現する４つのビジネスエリアとして，「インフラ」「インダストリー・モビリティ」「ライフ」「ビジネス・プラットフォーム」を設定しています。

三菱電機技報ではこの４つのビジネスエリアに分類し特集を紹介しています。

今回の特集ではビジネス・プラットフォーム領域の“サステナブルな社会と企業のDX推進に資するITソリューション”をご紹介します。

巻頭言

災害レジリエンス向上のための“都市OS”への期待

Expectations for "City OS" to Improve Disaster Resilience

北上眞二 *Shinji Kitagami*

福井工業大学 情報メディアセンター長 経営情報学科 教授

Professor, Department of Management and Information Sciences, Director of Information and Media Center, Fukui University of Technology

近年，日本国内で豪雨による災害が増えており，年々降雨量が増えているように感じられるが，気象庁の統計によると，この30年間の年降雨量偏差には大きな変化はみられない。ただし，日降雨量200mm以上の年間日数が増えている一方で，日降雨量１mm以上の年間日数が減少傾向にある。これは，地域や時期によって豪雨と渇水の二極化が進んでいることを意味している。現時点では，この二極化する気候変動に伴う災害を完全に予防することは困難であり，災害を乗り越える力を加えた総合的な取り組みとして，災害レジリエンスへの対応が求められている。災害レジリエンスは予防力，順応力および転換力から構成されるが，特に，豪雨と渇水の二極化への対策としては，災害の影響を受け入れつつ臨機応変に対応する順応力の向上が重要となる。

豪雨対策としては，線状降雨帯の多発などに対応するために，国土交通省では流域治水への転換を進めている。流域治水を推進するためには，集水域や河川区域における雨量や河川水位などの監視に加えて，河川流域の内水氾濫や中小河川の逆流などを監視し，流域住民への効果的な災害情報の提供が必要となる。一方の渇水対策としては，水資源循環の適正化を目的とした“雨水の利用の推進に関する法律”が平成26年に施行されている。たとえば，雨水貯留設備（雨水タンク）は，雨水をトイレ用水や散水などの用途に使用することで，緊急時の代替水源としての利用や平常時の節水が可能となる。また，下水道，河川などへの雨水の集中的な流出を抑制する効果もあり，雨水貯留設備の設置について補助金を交付する自治体も多くなってきている。

福井工業大学でも，地域の災害レジリエンスを向上させることを目的に，地方自治体や企業と共同で，LPWA（Low Power Wide Area）を活用した流域環境データ収集・可視化システムや内水氾濫と雨水利用を両立させる雨水タンク管理システムなどに係る研究開発と実証実験に取り組んでいる。これらのシステムでは，気象情報や他の災害情報と組み合わせた流域環境データの可視化や雨水タンクの最適排水制御のために降雨予測サービスとの連携などが必要となる。

このような災害レジリエンス向上のために様々なデータやサービスと連携させるクラウド基盤として，福井工業大学は“都市OS”に注目している。“都市OS”は，防災分野に限らず，スマートシティにおける物流，医療，福祉などに係るデータやサービスを連携させるためのクラウド基盤である。“都市OS”を活用することによって，これまで分野やアプリケーションごとに独立していたデータやサービスを，標準化されたAPI（Application Programming Interface）によって相互運用させることができる。この“都市OS”の枠組みの中で，データ連携基盤として多くの実績を持っているのがFIWARE（Future Internet WARE）である。FIWAREは，欧州連合（EU）の次世代インターネット官民連携プログラム（FI-PPP：The Future Internet Public-Private Partnership）で開発されたオープンソース・ソフトウェアである。また，内閣府の“デジタル田園都市国家構想”における地域データ連携基盤としてFIWAREが推奨されており，高松市や富山市などの地方自治体でも導入が広がっている。ここで，FIWAREはアプリケーションごとに導入しても意味はなく，電力や水道などと同様に，社会インフラとして整備されるべきものである。

先に述べた流域環境データ収集・可視化システムや雨水タンク管理システムは，このFIWARE上での動作または連携を前提として開発を進めている。すなわち，NGSI（Next Generation Service Interfaces）と呼ばれるWeb APIを使って，システムが収集して管理しているデータを利活用できる。たとえば，豪雨時に河川水位の状況によって雨水タンクの排水を抑止したり，渇水時に地域全体の雨水タンクの貯水マップを提供したりするサービスを短時間で開発できるようになる。

三菱電機は，ビルや公共などの分野で，特にエッジ側の設備やシステムに強みを持っているが，今後は，これらを高度に連携させるクラウド側の“都市OS”の整備に向けた取り組みに期待したい。“都市OS”の普及によって，福井工業大学が研究開発に取り組んでいる災害レジリエンス向上を含めたサステナブルな社会の実現が近づくものと考えている。

特集論文

環境データ収集自動化・管理・利活用へ向けたソリューション“cocono”によるカーボンニュートラル達成への貢献

IT Solution "cocono" to Collect and Manage Environmental Data

仁平百合菜* *Yurina Nihei*
谷口初音* *Hatsune Taniguchi*
奥田裕樹* *Hiroki Okuda*
杉本美紀* *Miki Sugimoto*
岩谷俊輔* *Shunsuke Iwaya*

*三菱電機インフォメーションシステムズ㈱

要　旨

近年，日本を始め各国が，2050年のカーボンニュートラル達成に向けて，産業構造や経済社会の変革に取り組んでいる。カーボンニュートラルへの関心が高まるにつれて，環境データの効率的な収集，管理，分析，可視化などのニーズも高まってきているが，システム基盤の整備は追いついておらず，環境管理部門が手作業で対応している例が多い。そこで，三菱電機インフォメーションシステムズ㈱(MDIS)は，GHG(GreenHouse Gas)排出量データ一元管理ソリューション“cocono”を開発した。GHG排出量は，工場やオフィスでの消費エネルギー量，部品や完成品の輸送量・輸送距離などで表される“活動量データ”と，排出係数の積算で算出される。coconoは，企業のシステムに内在する活動量データを自動収集，一元管理し，様々な形での利活用を可能にする。環境管理部門の負荷削減を実現し，企業のカーボンニュートラルへの取組みに貢献する。

1. ま え が き

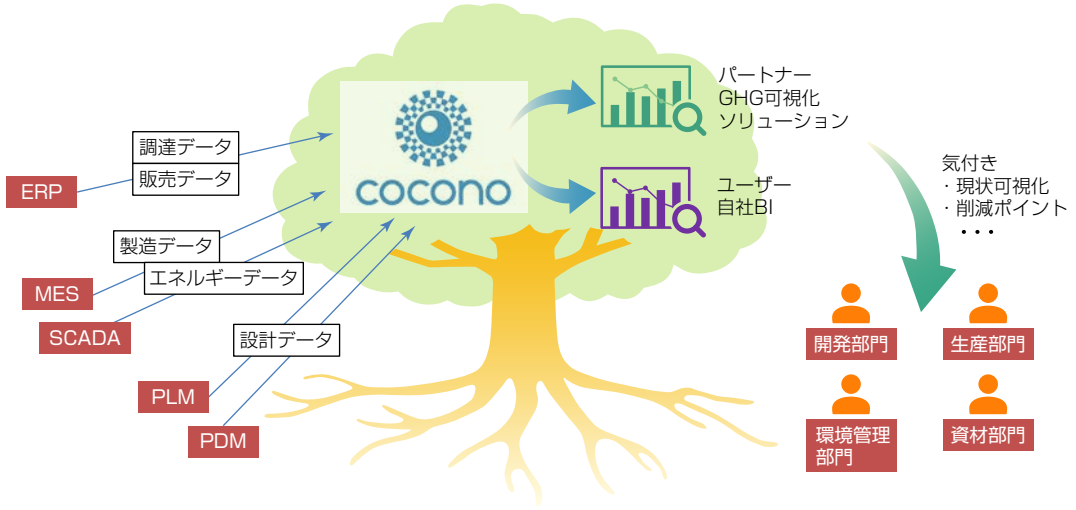
1992年リオデジャネイロで開かれた地球サミットで気候変動枠組条約が採択され，約30年が経過した。GHG排出大国の京都議定書への不参加といった停滞期もあったが，多発する異常気象への世界的危機感の高まり，さらには温暖化の原因が人間活動にあるとの見解が浸透するに至り，カーボンニュートラル＝脱炭素化への動きは世界的，かつ不可逆的なものになっている。産業界でも，気候関連財務情報開示タスクフォース(Task Force on Climate-related Financial Disclosures：TCFD)や国際サステナビリティ基準審議会(International Sustainability Standards Board：ISSB)を中心に，企業に対して，気候変動への取組みに関する情報開示を求める動きが強まっている。日本企業は大企業を中心に素早く対応する姿勢を見せており，その証左としてTCFDに賛同する国別企業数では日本は世界最多である(2023年１月時点)。しかし，具体的な活動となると，これまで積極的に取り組んできた省エネルギー活動の延長にとどまっている例が多い。従来の省エネルギー活動に対して，近年求められる脱炭素経営には次のような特徴がある。

⑴　自社だけではなく，取引先を含めたサプライチェーン全体でのGHG削減が求められている。
⑵　環境管理部門には従来の法対応業務に加えて，カーボンニュートラルへ向けた戦略策定とその推進が求められるようになっている。
⑶　積極的な情報発信を通して，業界全体で好事例の共有が奨励されている。
⑷　伝統的な財務指標とともに，気候変動に関する情報開示が企業に対する新たな評価指標になりつつある。

こうした新しい社会的要請に対応するため，MDISは，GHG排出量データ一元管理ソリューションcoconoを開発した。

coconoは，企業内の各ITシステムからGHG排出量につながる環境データを幅広く集めて，分析や可視化のために必要な集計や加工を行う。coconoで管理するデータは，MDISのパートナー企業のGHG排出量可視化ソリューションなどを通して可視化されることで，具体的な削減活動に利用できる“気付き”を与えて，顧客の各部門にフィードバックする。coconoの概要を**図１**に示す。

本稿では，先に述べた社会的要請への対応が遅れている日本企業の現状と課題について，製造業を中心に取り上げて，coconoによる解決のアプローチを述べる。



ERP：Enterprise Resources Planning，MES：Manufacturing Execution System，SCADA：Supervisory Control And Data Acquisition，
PLM：Product Lifecycle Management，PDM：Product Data Management，BI: Business Intelligence

図１．GHG排出量データ一元管理ソリューションcocono

2．カーボンニュートラル実現へ向けての製造業の現状と課題

GHG排出量を計測する指標は，持続可能な開発のための世界経済人会議(World Business Council for Sustainable Development：WBCSD)などの主導によって開発された“GHGプロトコル”が事実上の標準になっている。GHGプロトコルは，自社が直接排出するGHGの量と，自社以外のサプライチェーン上で間接的に排出されるGHGの量を，Scope1，2，3に分けて算出する。中でも注目が高まっているのが，電力会社からの電力調達を除く間接的GHGの量を示すScope3である。Scope3は更に15のカテゴリーに分かれており，購入した部材などに関わる排出量であるカテゴリー１，部材の上流の輸送での排出量であるカテゴリー４，自社製品が使用される際の排出量であるカテゴリー11，製品の廃棄に関わる排出量であるカテゴリー12などに区分けされる。ISSBが策定を進める気候変動開示基準でも，猶予期間を設けつつも，Scope3の報告が盛り込まれる見通しである。多くの製造業で，Scope3がGHGの総量の過半を占めており，特に組立加工型の場合は，カテゴリー１と11で７～８割に達することが多い。削減の必要性は製造業自身も認識するところであるが，サプライチェーン上の排出量であるため，正確なデータを補足するところから課題に直面する場合が多い。

2.１　課題１：環境データに対して従来以上の精度と鮮度が求められ，人手では対応が困難

環境データの収集，集計業務は，主に環境管理部門が担うが，中小規模の製造業では工場の設備管理部門などが兼務することも多いなど，潤沢な人的リソースが確保されていない場合が多い。従来は，温対法(地球温暖化対策の推進に関する法律)向けの提出書類など定型化された用途向けが主であり，ある特定の時期に現場の各部門からデータ提出を受けて，表計算ソフトウエアで集計するまでを人手で行うことが可能であった。しかし，経営戦略の一環としてカーボンニュートラルを進めることが求められるようになったことで，GHG排出量はもはやKGI(Key Goal Indicator)の一つとして不可欠となり，自(おの)ずとKPI(Key Performance Indicator)となる各要素の実績データについても従来以上の精度と鮮度が必要になった。計画未達の兆候を検知した時点で素早い施策を打てるようにするためである。さらには，Scope3対応のために扱うデータの範囲が格段に広がり，環境データ収集や集計を人手で対応するのはもはや困難になりつつある。

2.２　課題２：サプライチェーン上の企業間での一次データの共有が，一部の企業間にとどまっている

カテゴリー１の排出量を正確に把握するには，部材の仕入先企業などに対して，GHG削減への取組みや，一次データと呼ばれる活動実態に沿うデータの提出を要請する必要がある。しかし現状は，人手，システム基盤共に，製品単位で正しくデータを測定・管理できる環境が整っている企業は少なく，一次データの共有は一部の企業間でしか実現できていない。多くの企業では，二次データと呼ばれる，環境省などの各種団体が提示している標準値を活用している状況である。二次データを活用すると，カテゴリー１を算出することは大幅に容易になるが，あくまで標準値であるため，仕入先企業でGHG削減努力がなされても，その結果を自社に反映させることができない(**図２**)。

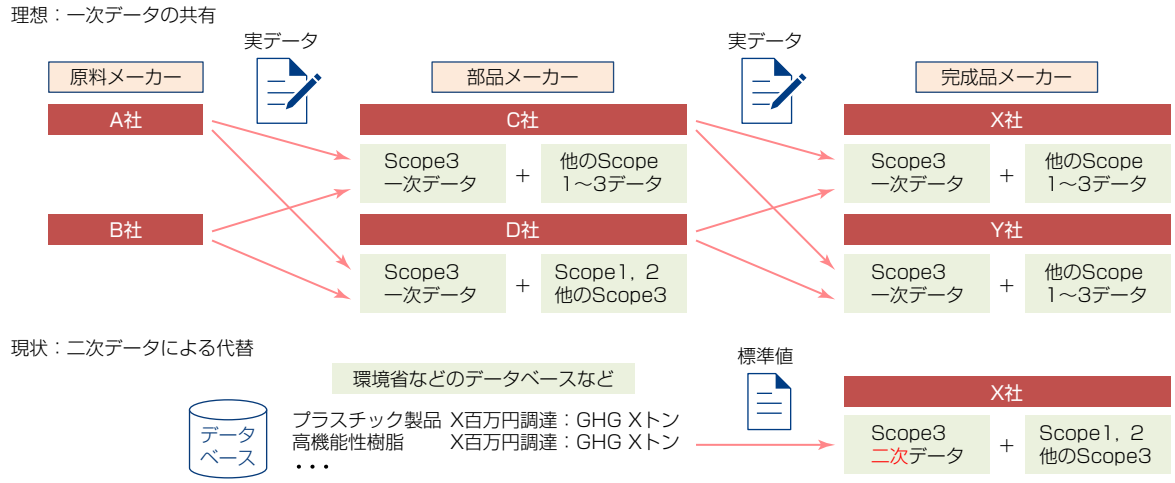


図２．企業間でのデータ共有の理想と現状

2.3　課題３：GHG排出量まで考慮した製品設計がまだ浸透していない

製品利用時に排出されるGHG排出量であるScope3カテゴリー11は，製品寿命の長い高品質の製品を多数出荷・販売していくと，排出量が大きくなってしまうというジレンマがある。それでも，多くの製造業にとって，GHG排出量で最も大きい比率を占めるものであり，削減への取組みが不可避である。現在の製品設計では，機能要件，及び耐荷重性・耐久性・耐熱性などの非機能要件を満たす範囲で最適な部品・素材を選定し，設計作業を進めていく。結果，各種要件を満たす設計は仕上がるものの，Scope3の観点で見ると，環境負荷の大きい部材の採用，遠方の取引先や倉庫からの非効率な輸送が必要といったことが起こる。特に量産品の場合はScope3の著しい増大につながる。設計完了後に，GHG排出量を抑制しようとしても，工夫の余地があるのは生産プロセスすなわちScope1，2での省エネルギーの範囲にとどまってしまう。“品質やコストの８割は，設計時に決まる”と言われるが，製品個々のGHG排出量もまた設計段階でおおむね決まる。そのため，GHG排出量をあらかじめ要件の一つと考えて設計を行う必要があるが，現在の製造業で取り組んでいる企業はまだ少ない。

３．現状の課題に対するcoconoによる解決のアプローチ

coconoは，MESやSCADAといった製造業内の各ITシステムからデータを収集・管理する基盤であるが，パートナー企業のGHG排出量可視化ソリューションや，三菱電機グループ内外の製品・サービスと連携することで更なる機能の充実化を図っている。主に次に挙げる機能を利用企業に提供する。

⑴　多角的なエネルギーダッシュボードによる多様な視点での分析
⑵　カーボンフットプリント（Carbon Footprint of Products：CFP）と呼ばれる製品個別のGHG排出量の算出
⑶　製品設計段階での想定GHG排出量のシミュレーション
⑷　既存ITシステムとの自動的なデータ連携
⑸　企業間での取引対象でのGHG排出量の共有

企業はこれらの機能を活用することによって，各課題の解決を図ることが可能になる。

3.1　課題１に対するアプローチ

人的リソース不足の課題に対しては，データ収集，集計を自動化することで解決できる。coconoは，各システムからGHG排出量管理に必要なデータ，いわゆる“活動量データ”を自動収集することで，環境管理部門の業務負荷軽減につなげる。人手によるデータ収集，集計入力作業でしばしば起こる計算ミスなどのヒューマンエラーも防止できる。データの精度と鮮度が向上することで，企業全体の最新のGHG排出量が常に把握できるようになり，正しい実態に基づいた個別施策をタイムリーに実行することが可能になる。環境管理部門の担当者は，脱炭素戦略の策定と推進といった“人にしかできない業務”に注力できるようになる。

3.2　課題２に対するアプローチ

MDISのパートナー企業のGHG排出量可視化ソリューションの中には，利用企業同士の取引データを基に，主にカテゴリー１に関わるデータを共有する仕組みを提供するものがある。ある利用企業とその仕入先企業が共にこのGHG排出量可視化ソリューションを利用している場合，仕入先企業の正確な実績である一次データを利用企業側が取り込めるようになる。

こうした仕組みによって，利用企業は仕入先企業に対して，GHG削減目標の設定と具体的削減努力を求めやすくなり，仕入先企業側も，継続的な取引の確保をモチベーションとして，積極的に削減努力を推進していく。利用企業側はその努力の結果を，自社にとってのScope3削減という形で取り込むことが可能になる。さらにcoconoとの連携によって，GHG排出量可視化ソリューションへの利用者のデータ入力の負荷を下げることができるため，規模の小さい仕入先企業にも導入を促しやすくなる。

3.3　課題３に対するアプローチ

製造業で，製品の設計者は主にCADを用いて設計業務を行い，その成果である設計情報はPLMやPDMによって世代管理したり，他部門との共有を図ったりする。coconoは，各システムとの連携によって蓄積されたGHG排出量情報を保持しており，PLMやPDMと連携することで，使用する部材情報と，仕入先の想定物流拠点から，原料，部材調達時のGHG排出予定量のシミュレーション結果を算出する。この結果は，設計者や資材部門，時には仕入先企業も含めて共有することで，機能要件や性能要件を満たす範囲で，GHG排出量のより少ない設計を検討することが可能になる（**図３**）。

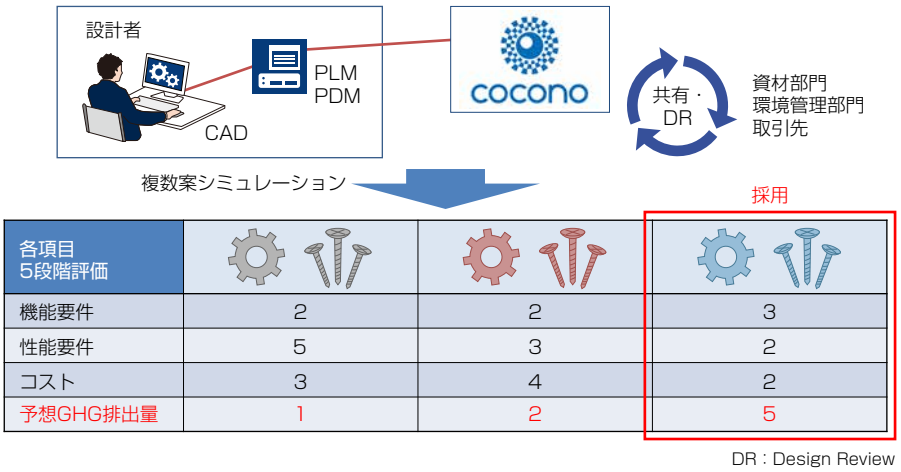


図３．GHG排出量をシミュレーションしながらの設計のイメージ

4．coconoでの技術的な工夫

coconoの主な構成要素は，①パブリッククラウドに構築されたデータ管理基盤，②クラウド上でデータ処理を行うETL（Extract/Transform/Load）ツール，③利用企業のローカル環境からクラウド上にデータをアップロードするためのプログラム，の３点である。開発では，標準のサービスや製品を極力活用して固有のプログラム開発を最小限にすること及び各構成要素をシンプルに疎結合させることを基本方針としている。特異な技術を使わないことで，システムが複雑になることを回避し，利用企業にとっては導入容易性をもたらす。MDISでも運用保守工数を削減することになり，利用企業に対して利用コストの低減，サービスの安定提供といった形で還元する。

4.1　導入容易性の工夫

coconoを利用するに当たっては，利用企業は特別なデータ加工を行う必要はない。クレンジング，格納，集計，他のシステムへ連携するための加工といった必要な処理は，coconoが行うためである。一般に，複数のシステム間でデータ連携を行う際，データ仕様の統一や，送り手側のシステム改修など一定の導入コストがかかるのが通例であるが，そう

いった負担を回避できることがcoconoの特長の一つである。利用企業は，各ITシステムのデータベース上の形式をおおむね踏襲する形で，データを抽出し，所定の場所に出力するだけでよい。MDISが用意するプログラムによって，一定の周期でcoconoにデータをアップロードし，以降のデータ処理や他社GHG排出量可視化ソリューションとの連携はcoconoが担う。

4.2　セキュリティー確保の工夫

coconoは，パブリッククラウド上でデータ管理するため，利用権限のない人間によるアクセスを防ぎ，セキュリティーを確保する必要がある。このため，パブリッククラウドへデータをアップロードできるのは，事前に払い出されたアクセスキーを組み込んだプログラムだけにしている（**図４**）。

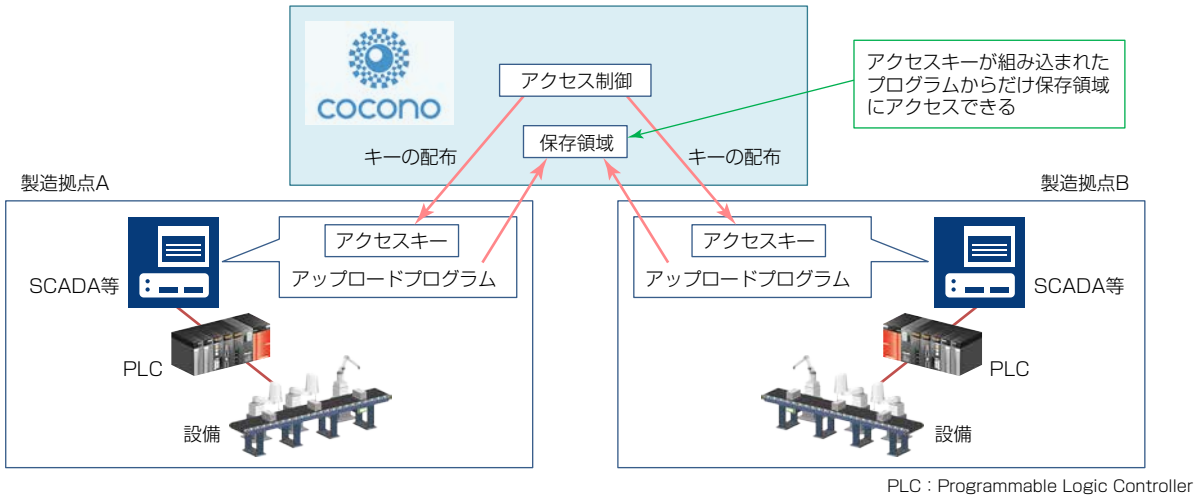


図４．coconoでのセキュリティーの仕組み

また必要に応じて，送信元のIP（Internet Protocol）アドレスを特定し，アクセス制御する仕組みも併用することにしており，セキュリティーの強度を高めている。またMDISで，クラウドの設定を自動チェックするツールも開発・利用することで，運用時の人為的なミスによってセキュリティーホールが生まれることを抑制している。

5．む　す　び

製造業を中心とした日本企業のカーボンニュートラルへ向けた課題，課題解決へ向けたアプローチ，及びMDISのソリューションcoconoを構成する技術要素とその工夫点について述べた。coconoを導入し，既存のITシステムやGHG排出量可視化ソリューション等と連携することで，GHG情報を素早く収集・把握し，具体的な削減活動にこれまで以上に注力できるようになる。Scope3までの情報開示を求める動きは今後も高まると予想され，MDISとしてはcoconoを通して，企業のGHG情報管理の支援を強化していく。

さらに近年，産業界では，カーボンニュートラルへの取組み状況を中心とした自然資本に加えて，人的資本，社会資本などに関する，いわゆる非財務情報の開示が求められるようになっている。環境管理部門が直面しているのと同様に，これからは総務部門や資材部門が，新しい戦略や施策の立案，そのために必要なデータの収集，管理，分析が求められるようになるものと予想される。MDISとしても，coconoが収集・管理する対象データを非財務情報全般に広げることを計画しており，企業を取り巻く社会情勢の変化に機敏に対応していく。

参　考　文　献

(1)　環境省：SBT等の達成に向けたGHG排出削減計画策定ガイドブック（2021）
https://www.env.go.jp/earth/ondanka/datsutansokeiei/SBT_GHGkeikaku_guidbook.pdf
(2)　環境省：TCFDを活用した経営戦略立案のススメ～気候関連リスク・機会を織り込むシナリオ分析実践ガイド ver3.0～（2021）
https://www.env.go.jp/earth/TCFD_guidbook.pdf
(3)　経済産業省：非財務情報の開示指針研究会における取組みの状況（2022）
https://www.cas.go.jp/jp/seisaku/sustainability/dai1/siryou3.pdf

特集論文

DX時代のビジネスを加速する，仮説検証型のサービス創出マネジメント

Management of Emerging Service Based on Cloud Computing with Hypothesis Testing and Hypothesis Verification

小林　敦*　Atsushi Kobayashi
佐藤啓紀†　Hiroki Sato
高橋　渉†　Wataru Takahashi
佐藤　剛†　Takeshi Sato
大澤伸行†　Nobuyuki Osawa

*クラウドセントリック㈱
†三菱電機インフォメーションシステムズ㈱

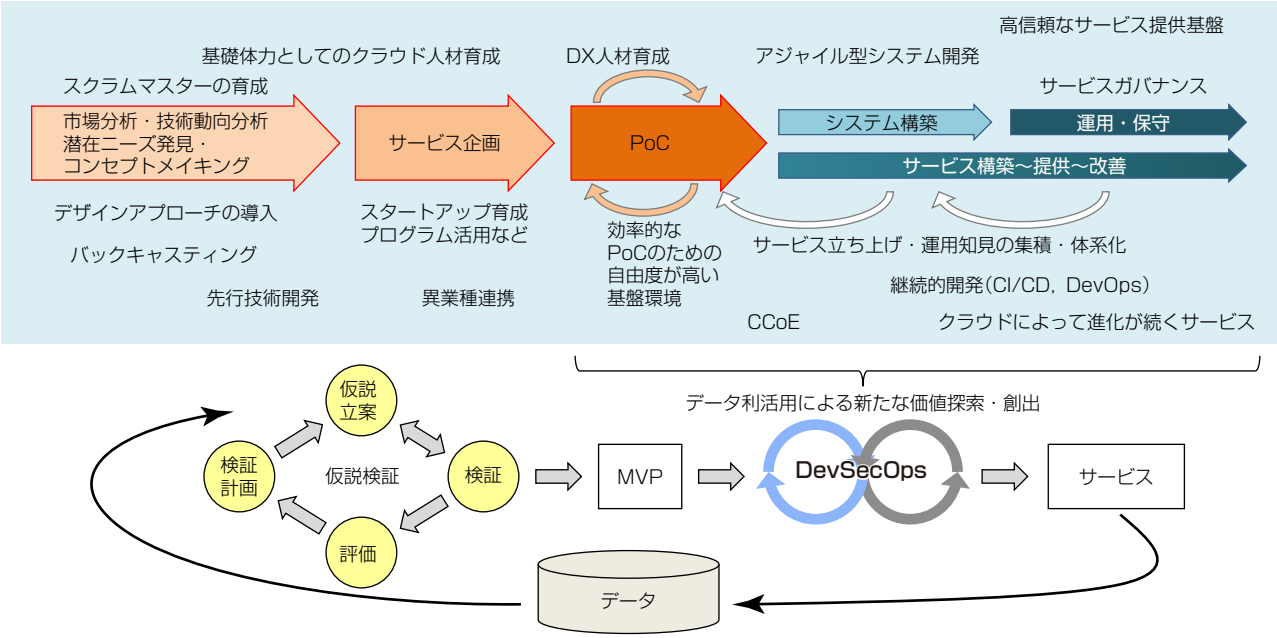
要　旨

三菱電機インフォメーションシステムズ㈱(MDIS)では，仮説検証型の新サービス創出を促進するため，クラウドの利用を基軸としてサービス提供技術を体系化し，自社サービスで実践するとともに，顧客とのサービス共創に適用可能にした。まず，企画構想段階では，デザインアプローチの導入サービスメニューを確立した。また，サービスの実証評価(PoC：Proof of Concept)を効率的に実施する環境の構築と，商用サービスを安心・安全に提供するための非機能要件を克服する技術開発を進めた。さらに，サービスの構想・企画から収益化までのプロセス管理，収益管理やサービスガバナンスの仕組みを確立した。

MDISは，顧客とのサービス共創を推進し，サービスインテグレーターとして顧客のDX(Digital Transformation)に貢献していく。

1. ま え が き

DXの時代には，最先端の技術やアイデアを俊敏にビジネスに取り入れることや，異分野間をつないで新たな複合サービスを創出することが求められる。また，継続的かつタイムリーに価値あるサービスを提供し続けることや，ビジネスの変化に応じてサービス提供システムを柔軟に拡張することも求められる。データから新たな価値を創出し，顧客の課題を解決していくためには，デザイン思考やアジャイル開発，AI／ML(Machine Learning)，データアナリティクス等の手法を取り入れることも必要である。このような状況では仮説検証型の新サービス創出が求められるが，その不確実性は高く，プロセスを的確にマネジメントすることがビジネスのスピード感，ひいてはビジネスの成否につながる。MDISでは，自らサービス事業を推進するとともに，そこで得たビジネス知見や開発資産，応用技術を生かして，顧客とのサービス共創，ひいては顧客のDXへの貢献を目指している。クラウドの特性を生かした仮説検証型の新サービスの創出を**図1**に示す。



CCoE：Cloud Center of Excellence，CI/CD：Continuous Integration/Continuous Delivery，DevOps：Development and Operations，DevSecOps：Development, Security, and Operations，MVP：Minimum Viable Product

図1．クラウドの特性を生かした仮説検証型の新サービス創出

2. クラウドを基本とした技術・知見の体系化

旧来のウォーターフォール型のシステムインテグレーションと異なり，DX時代の新サービス創出は，サービス要件がはっきりせず，システム仕様も定まらないところから始まる。また，システムは常に新しいアイデアや技術を取り入れて進化し続けることが求められる。これらに対応するのはクラウドであり，DX時代のシステムインテグレーターにはクラウドを前提とした技術開発力，ビジネス展開力が必要になる。

また，最先端の技術が最初にクラウド上に実装され提供される時代になった。進化・変化し続けるクラウドを選択しておくことは，将来に向けた様々な可能性を選択することにほかならない。さらに，クラウドを取り入れるということは，コンパクトに試行ができるというクラウドの特質を生かすことも含めて，それに適合するために組織の営みをアジャイルでスピード感があるものに変えることにつながり，組織風土や価値観の変化に発展する。これらの点を考慮して，MDISはクラウドを基軸に据えて，技術と知見の体系化を進めた。

クラウドは“失敗のコスト”を大きく低減し，人々にチャレンジを促して，イノベーションにも貢献するものである[1]。

MDISもクラウドを活用して顧客のイノベーション，及び自社のイノベーションを指向している。

3. サービスの発想・共創

MDISではサービスの構想・企画段階で，自社サービスの創出でデザインアプローチの適用に取り組むとともに，その実践的知見をメニュー化して顧客とのサービス共創にも適用可能にした。ここでは，①潜在ニーズの発見，②コンセプトメイキング，③新サービス創出，④UI(User Interface)デザイン開発・プロモーション，の四つのステップについて，著名なフレームワークも取り入れながら手法を確立した。また，このサービスメニューを金融機関などに提供開始した。

異業種間の共創の知見獲得では，スタートアップ企業とのマッチングプログラムに参画し，①顧客向けの提案，②自社サービスへの適用，③社内利用，の三つの視点で外部のビジネスアイデアや先進技術の取り入れ方，ビジネスの具現化までのプロセスを確立した。また，複数企業に跨(またが)る知的財産権の扱いや技術コンタミネーションの防止などの知見を蓄積してきた。さらに，データ利活用による新サービスの創出に向けて，データサイエンティストによるデータアナリティクスやAI／MLの応用も進めてきた[2]。

4. 基盤技術の確立

MDISでは，ビジネスの成否に直接関わるサービス機能の開発に集中できるようにするため，クラウドを活用する場合の非機能要件への対応や基盤構築の負担を軽減する技術開発を進めた。ここでは，サービス提供事業者としての当事者能力を確保するために，自社で基盤技術を確立し，保有・運用することにした(**図2**)。

4.1　非機能要件への対応技術

クラウドの機能の進化やセキュリティー対策は日進月歩であり，また性能，可用性，拡張性など共通で解決できる課題については一元的に取り組むことがサービス提供ビジネスの迅速化につながる。特にセキュリティーでは，一つの設定ミスがサイバー攻撃では弱点として狙われるため，対策を徹底することや，不正アクセスを早期に検知する仕組みなど技術的な対策に加えて，運用ルール・手順・体制の整備も必要である。MDISではクラウドサービスで活用できる技術や知見を集積し，サービス事業を支える基盤技術として確立した。

4.2　サービス提供基盤の特長

MDISは，様々なクラウドサービスを，三菱電機の“DIAPLANET”[注2]技術を適用して安全に提供可能にした。

(1)　サービス品質の向上

サービスごとに独自に機能を開発することなく利用できる災害対策機能，ログ収集分析機能，アカウント管理機能に加えて，IoT，セキュリティー，データベース等の実装技術を集約し，サービスの可用性やスケーラビリティーを向上させる高信頼なライブラリー群にした。

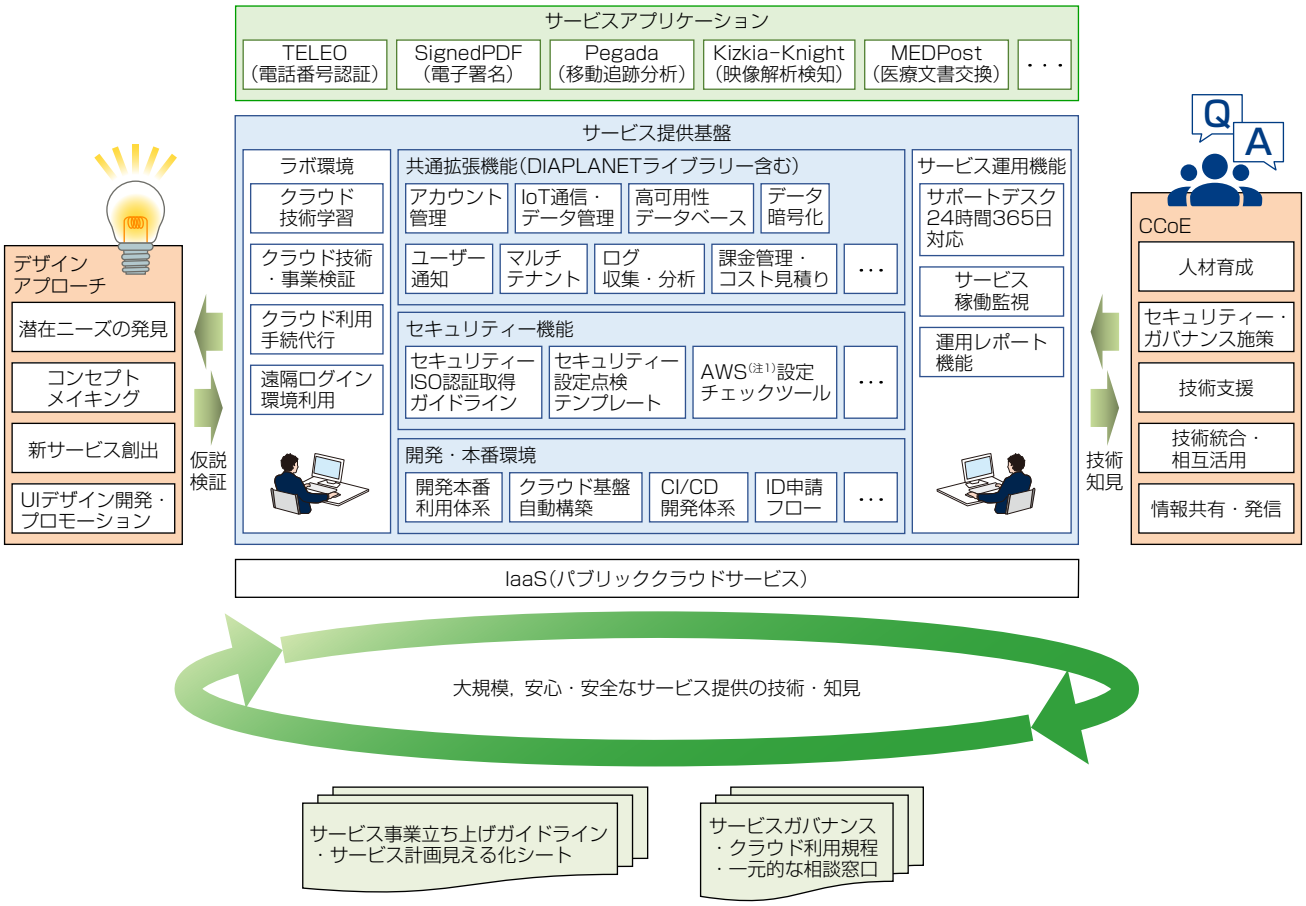
⑵　サービスリリースの迅速化

サービスの事前技術検証を行えるクラウドラボ，高速開発の枠組みをそろえたクラウド開発環境，及び円滑にリリース移行できるクラウド本番環境を提供した。セキュリティーの安全性を担保し，サービスのリリースを迅速化した。

⑶　24時間365日の有人運用

安定したサービス運用に必要な稼働動作ログ監視，運用手順書に基づいた運用対応，及び顧客サポートデスクを設けて，24時間365日対応可能なサービス運用機能を具備した。

（注２）　様々な分野でIoT／ITを活用した付加価値の高いITソリューションを効率良く創出するプラットフォームである。



IoT：Internet of Things，ISO：International Organization for Standardization，IaaS：Infrastructure as a Service

（注１）　AWSは，Amazon Technologies, Inc.の登録商標である。

図２：効率的にPoCを遂行するラボ環境と，非機能要件に対応するサービス提供基盤

4.3　サービス提供支援機能の実装

安全かつ俊敏にサービスを提供するための支援機能として，SRE(Sight Reliability Engineering)やQCD(Quality Cost Delivery)の考え方を取り入れて，俊敏性(市場ニーズや変化の速やかな取り込み)と信頼性(サービス品質の向上と安定性)の両立を図るため，省力化，自動化，信頼性向上に資するツール群を開発した。近年は市販ツールが多数存在しているにもかかわらず独自開発したのは，仮説検証型の新サービス創出は不確実性が高く，そのPoCは小規模であったり短期間で終わったりすることも多く，市販ツールの導入条件(最低利用規模等)が合致しなかったり，機能が過剰で導入コストが高額になったりすることを想定したためである。また，最先端の技術を取り入れた新サービスの提供では，市販ツールでは機能的に追従できず，自社で独自開発せねばならない場合も想定した。これらを考慮してMDISでは，PoCの段階からサービスの進化に追従して支援できるコンパクトな独自ツールを使い，サービス創出を支援するようにした。

クラウド上のセキュリティー設定を点検するツールは，金融情報システム(FISC：The Center for Financial Industry Information Systems)が定めた金融機関の情報システム向け安全対策基準から抽出した135項目を自動点検し，**5. 3節**に

述べるISO/IEC 27017の遵守とFISC対応の高い安全性を確保する。DevSecOpsでのコンテナ開発環境は，クラウドサービスを組み合わせた開発でのビルド・テスト・デプロイ・デリバリーを自動化し，①バージョン・タスク管理，②CI/CD・コンテナ管理，③コンテナ展開を一貫して行う。

4.4　PoCを効率的に推進するラボ環境の構築

クラウドサービスの検証を行うラボ環境として，端末・ネットワーク・クラウドアクセスへの踏み台を多段的に用意した。これによって検証する対象には制限を設けず，利用者とのコミュニケーションから適切な利用権限や設備を提供可能にした。ここでは，安全性を重視する場合には，禁止や制限を優先する“門番”的な運営が考えられたが，自由度が下がるため，“ガードレール”的なポリシーで技術サポート・設備の共同利用・コストの一元管理と多面的にサポートする体制にした。例えばAWSでは，CloudTrail(注3)での操作記録の保存，Elasticsearch(注4)とKibana(注4)での監視，Amazon GuardDuty(注3)による不正利用の検知を共通的な運営とした。また，AWS技術に長(た)けたエンジニアチームを編成して，臨機応変かつ機敏にPoCの試行錯誤での設計や実装に対応するようにした。

端末側ではSplunk(注5)とZabbix(注6)によって使用状況をリアルタイムで監視し，不適切な利用を検知できるようにした。クラウドサービス側でも当該サービスが提供するセキュリティー機能を活用することに加えて，不正が疑われるアクセスの検知やアクセス履歴の記録を一元的に行い，安全に利用できる運用技術を確立した。

（注３）　CloudTrail，Amazon GuardDutyは，Amazon Technologies, Inc.の登録商標である。
（注４）　Elasticsearch，Kibanaは，Elasticsearch B.V.の登録商標である。
（注５）　Splunkは，Splunk Inc.の登録商標である。
（注６）　Zabbixは，Zabbix LLCの登録商標である。

5. サービス立ち上げから収益化までのマネジメント

MDISは，サービスを構想・企画する段階から実際にサービスをローンチして収益化するまでの全プロセスで，自社サービスを例にサービス立ち上げノウハウを体系化し，“サービス事業立ち上げガイドライン”及び“サービス計画見える化シート”としてまとめた。これらを顧客とのサービス共創にも適用し始めている。

5.1　プロセスの見える化

MDISでは従来，システム生産標準“SPRINGAM”(System PRoduction and INteGrAtion Methodology)に従って顧客の情報システムを開発・提供してきたが，近年はこれに加えて，サービス事業開発での生産標準や効率的な開発を推進するための開発指標が必要とされていた。そこでMDISでは，TELEO(2020年７月提供開始)やMistySign(2021年６月提供開始)，nokos(2022年３月提供開始)などサービスを創出してきた中で，サービス開発から立ち上げまでのプロセスの見える化を支援する“サービス事業立ち上げガイドライン”を確立した。

サービス開発では段階が進むごとに規程・基準や開発標準への対応が必要になるが，“サービス事業立ち上げガイドライン”では各段階での対応を時系列に示して，対応すべき社内部門や成果物を明確化した。また，審査を実施すべき局面なども織り込んで実施すべきプロセス全体を見える化した。ガイドラインは，①事業化の基礎検討，②事業化の可否判定，③製品化，④展開，の４段階とした。これをテンプレートとして，顧客の組織や体制に置き換えることで，汎用的なサービス開発から立ち上げまでのプロセスの見える化ができるようにした。

5.2　サービス収益管理手法の確立

MDISでは，サービス事業の収益管理手法を確立した。投資回収管理(開発費を投資額に見立てた売上効果管理)にとどまらず，事業者としての損益管理の意識付けをするとともに経営管理の視点で精緻な損益管理ができるようにした。投資額には開発費用だけでなく販売活動費用や稼働環境維持費用を加えて，経常利益算出に対しては開発規模に基づく期間費用を算入するように，投資効果算出用期間費用率を定める等の改善を図り，Excel(注7)フォーマット上に売上げ，粗利，各種投資費用を入力するとサービス事業開発全体の損益を見える化する“サービス計画見える化シート”とした。累積損益も管理することで，対象サービスの継続や見直し，さらには中止といった判断材料として，事業責任者の意思決定を支援するようにした。

（注７）　Excelは，Microsoft Corp.の登録商標である。

5. 3　ISO/IEC 27017の取得

近年，クラウドサービスセキュリティーの重要性が意識されており，2015年にクラウドサービスセキュリティーに関する国際規格ISO/IEC 27017：2015が制定され，2016年に日本語規格JIS Q 27017：2016が制定された。現在ではクラウドサービスに関する第三者評価制度として広く認知されている。MDISでは，電話発信認証サービスTELEOでISO/IEC 27017認証を2020年に取得し，その取得ノウハウを顧客にも提供可能にしている。

6. サービスガバナンスの確立

MDISでは，クラウドを活用した新サービスを安心・安全に提供するための客観的評価の仕組みとして，クラウド利用規程の制定とクラウド利用したサービス提供に対する審査と支援の仕組みを確立した。

クラウド利用規程は，経済産業省のクラウドセキュリティガイドラインや三菱電機のクラウドサービス利用基準を基に，独自の点検項目を付加した。サービス提供者が行うべきセキュリティー対策やリスク低減策として，多要素認証の採用や接続元のネットワーク情報で制限を設けること等を定めて，機密情報や個人情報を扱う場合の指針等を示した。

また，客観的な審査と支援の仕組みとして，社内の法務・技術・品質保証部門の相談窓口を一本化し，仮説検証型での新サービスの企画検討段階で発生する不確定要素(サービス提供条件，サービス利用者，扱うデータ等)を洗い出して，リスクの見立てと対策案を提供できる体制にした。これによって，提供するサービスの事業効果とリスクのバランスを判断して，サービスガバナンスを効かせて，安心・安全なサービス提供を行えるようにした。

MDISでは，自社内に確立したこれらの仕組みを，顧客のサービスガバナンス確立の支援にも提供可能にしている。

7. 事 例 紹 介

最後に，顧客とともに新たなサービスの創出を目指して仮説検証を進めた事例を述べる。MDISのサービス提供基盤上で，損害保険会社の浸水被害計測サービスのPoCを実施した。水害が発生した際に，保険契約者が自身のスマートフォンでペットボトルと一緒に浸水跡を撮影することで，浸水高を自動推定し，損害保険会社の調査員の訪問を不要にするものである(**図3**)。

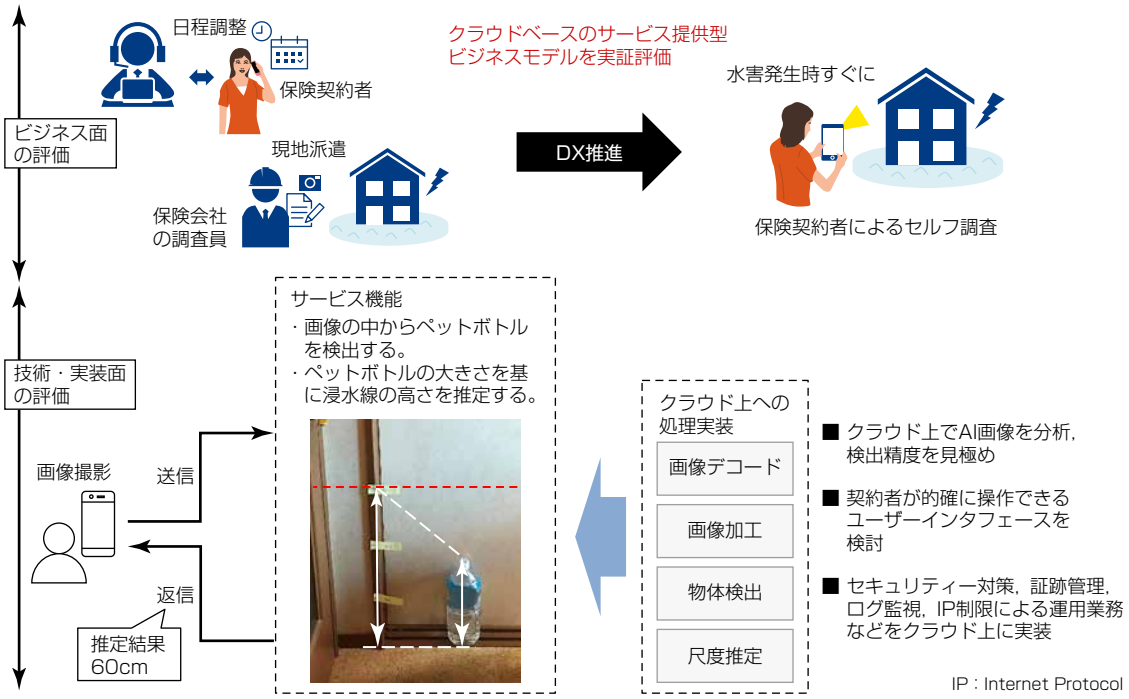


図3：損害保険会社のDX事例

8. む　す　び

三菱電機グループは，循環型デジタル・エンジニアリング企業を指向して，既存のビジネスの枠組みにとどまらない，統合ソリューション創出に向けた取組みを進めている。その中でMDISは，データ利活用技術やデジタル技術を駆使して，顧客のDX推進を担っていく。これを下支えするのはクラウド活用技術・知見の蓄積と発揮のサイクルの形成であり，CCoEを組成してこれを推進している。

さらにMDISではクラウドへの対応力強化のため，2023年４月に㈱スカイアーチネットワークスとの共同出資によってクラウドセントリック㈱を設立した。この会社を中心にトップレベルのクラウドエンジニア集団を形成し，最先端のデジタル技術で顧客のビジネスを成功に導いていく。

参 考 文 献

⑴　斎藤昌義：【図解】コレ１枚でわかる最新ITトレンド［増補改訂４版］，153，技術評論社（2022）
⑵　中村伊知郎，ほか：AIとビッグデータ時代を担うデータサイエンティストの育成とデータ分析の実践，三菱電機技報，**93**，No.8，484～488（2019）

特集論文

金融コンプライアンス録音“nokos”とDX

西　健太朗*
Kentarou Nishi
清水俊介*
Shunsuke Shimizu
馬渡小春*
Koharu Mawatari
鶴田季丸*
Tokimaru Tsuruta
白浜広彬*
Hiroaki Shirahama

*三菱電機インフォメーションシステムズ㈱

Financial Compliance Recording "nokos" and Digital Transformation Promotion of using AI

要　旨

金融機関では，コミュニケーション基盤(電話やディーリングフォン，ウェブ会議ツールやコールセンター基盤)を活用して顧客への迅速かつ正確な対応や多様な顧客のニーズに対応している。金融業界では，投資家の保護や有価証券の発行や売買などの金融取引を公正にすることを目的とした“金融商品取引法”や銀行の業務の公共性に由来する信用維持，預金者保護などと，金融の円滑のための銀行業務の健全で適切な運営を確保することを目的とした“銀行法”，保険業を行う者の業務の健全かつ適切な運営及び保険募集の公正を確保することによって保険契約者などの保護を目的とした“保険業法”などが整備されており，コンプライアンス強化を実現するためにシステマティックな仕組みが求められている。

三菱電機インフォメーションシステムズ㈱(MDIS)は，音声系ソリューションで，1990年代後半から，これら顧客の期待に対応してきた。近年では新しいコミュニケーション基盤で“ウェブ会議の自動録音”，“音声データのテキスト化”，及び“そのデータを利活用”することで，顧客の高まる期待に対応している。ウェブ会議ツールでの会話や画面，動画を自動的に記録するサービス“nokos(ノコス)”は，クラウドベースで容易に導入でき，確実なコンプライアンス管理を実現する。

1. ま え が き

新型コロナウイルス感染症(COVID-19)の拡大によって，リモートでコミュニケーションを取る手段としてウェブ会議ツールの普及が進んでいる。近年，社内の会議にとどまらず，顧客との商談や取引先との打合せにも使われるようになってきた。このため，厳しいコンプライアンス管理が求められる金融機関ではウェブ会議でのやり取りを記録する必要が出てきた。このオンライン営業の普及に伴って顕在化した課題がコンプライアンス管理である。トラブル防止や営業担当の法令遵守意識向上のためには，ウェブ会議でのやり取りを記録する必要がある。

MDISのnokosは，ウェブ会議ツールMicrosoft Teams(注1)(Teams)やZoom Meetings(Zoom(注2))，Webex Meetings(Webex(注3))での会話や画面，動画を自動的に記録するサービスである。クラウドベースで容易に導入でき，確実なコンプライアンス管理を実現する。

ウェブ会議ツールで自動録音されたデータは，電話基盤やコールセンター，ディーリング業務などの通話録音装置で録音されたデータも含めて音声テキスト化を行う。音声データをテキスト化することで，特定キーワード，NGワードなどの検索が容易になり，モニタリング業務の効率化に貢献できる。MDISは独自開発した“高精度テキスト化”で認識率を更に向上させることで，テキストデータとCRM(Customer Relationship Management)の応対履歴の自動連係や，発話内容と社内に蓄積されたナレッジを結び付けた自己解決率向上によるカスタマーサービスの効率化も実現する。あらゆる顧客接点のデータを一つにまとめて，一元化されたビューに表示して分析を可能にする。これによって，インサイトに基づいて迅速にアクションを起こせるようになり，最先端のデータドリブン経営に活用できる。

図1に金融コンプライアンス録音とデジタルトランスフォーメーションの推移を示す。

(注1)　Teamsは，Microsoft Corp.の登録商標である。
(注2)　Zoomは，Zoom Video Communications, Inc.の登録商標である。
(注3)　Webexは，Cisco Technology, Inc.の登録商標である。

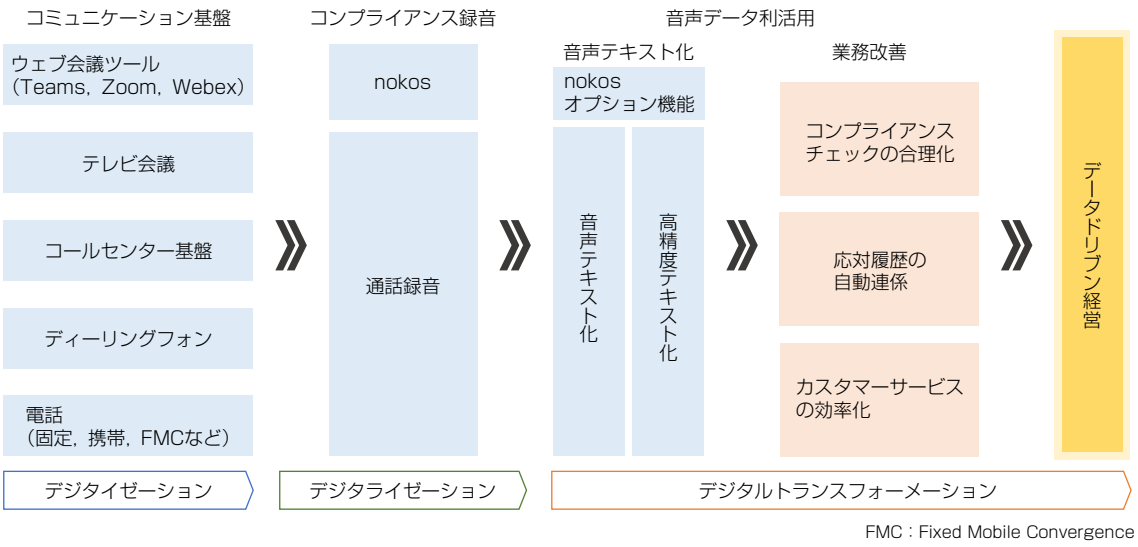


図１．金融コンプライアンス録音とデジタルトランスフォーメーションの推移

2．現状と課題

2.1　変化する電話基盤への対応

金融機関各社は，コンプライアンス強化を目的に過去から渉外担当者の通話録音システムを導入してきた。当初，固定電話から始まった通話録音であったが，アナログ化からIP(Internet Protocol)化への対応や携帯電話の録音も対象に含めた。2020年からは多くの企業で在宅勤務が進んで，勤務場所の制限を取り払う機能としてFMCを活用する企業が増えている。FMCは，“携帯電話を固定電話の代わりに内線のように使う”仕組みであり，携帯電話の保有が一般化する中で，固定電話と携帯電話の通信を一本化し，なおかつ携帯電話で二つの回線が利用できることで注目が集まっている。FMCは，自席の外線を外出先で受け，また，アドレスフリーなオフィス環境で内線子機としても使うことができる。会社の固定電話と従業員の携帯電話間の通信を内線で行うことができるなど，テレワーク環境のように“電話を受ける場所の制限”がなくなるのが大きなメリットである。こういった背景を考慮し，MDISではFMCも録音対象に含めた。働き方の変化に応じて，電話基盤も更なる変革が期待されており，これら新しい電話基盤も録音対象に含めていくことが求められている。

2.2　ウェブ会議ツールの自動録音対応

2020年からコロナ禍でウェブ会議の活用が広がった。ウェブ会議ツールに標準で備わっている録画機能はクライアント側の操作が必要なため，記録するか否かはユーザーに依存してしまう。電話基盤のように自動録音の機能整備ができておらず，渉外担当者はウェブ会議ツールを金融商取引では利用できなかった。企業ユースはTeamsが中心であるが，中小企業や一般顧客の場合は，WebexやZoomによるコミュニケーションが中心であるため，全ての自動録音を網羅する仕組みが求められた。

2.3　AI技術の進化による経営層の期待

自然言語処理で音声通話をテキスト化してNGワードのコンプライアンスチェックの基盤は従来も実装してきた。深層学習(ディープラーニング)やビッグデータの活用が進んで，音声テキスト化の精度が昨今大きく向上している。一方，会話内容をテキストデータに変換できる音声テキスト化は残念ながら100％の精度は出ない。マーケットでは，更に精度の高いものが求められており，顧客の経営トップは厳しい競争を勝ち抜くために，顧客の声を質的データ・定性データ化し，そのデータに基づいて経営的な意思決定を行い，データドリブン経営に活用したいと考えている。

3. MDISの取組みと提案

金融機関では，FMCやウェブ会議ツールなど，新たに顧客の接点になる基盤のコンプライアンス対策に追随していく必要がある。MDISは，20年以上培った音声系ソリューションのノウハウを生かして，こうした新しいコミュニケーション基盤のコンプライアンス強化に追随したシステムやサービスを提供し続けている。

3.1　Teamsの自動録音nokosサービス提供開始

金融機関などでの新たな顧客接点として，ウェブ会議が存在感を増している。新型コロナウイルス感染症の拡大への対策や経営の合理化の中で，金融機関は非対面での取引を増やしてきた。しかし複雑な金融商品の販売や融資などでは，営業員が顧客と一緒に資料を見ながら丁寧に説明をする必要がある。ウェブ会議ツールは，画面共有の機能を駆使することで，遠隔でも対面営業と変わらないサービスを提供できる。特に，厳しいコンプライアンス管理が求められる金融機関では，以前から顧客との会話を全て記録する仕組みを整備してきた。しかし，ウェブ会議ツールには電話や対面のような記録システムが整っていなかった。そこでMDISは，ウェブ会議でのやり取りを全自動で記録することで，コンプライアンスの徹底ができる仕組みを考えた。

nokosは会議の自動録音機能が大きな特長であり，企業でデファクトスタンダードのウェブ会議ツールであるTeamsの音声・動画・共有資料を自動で記録できる仕組みの提供を2022年３月に開始した。nokosはあらかじめ決められたユーザーがTeamsでのやり取りを始めるときにシステムが自動的に記録を開始し，ユーザーには記録中であることがメッセージで伝えられる。記録開始後のユーザーによる停止は不可であるため，録音記録の取得漏れ防止と不正行為に対する牽制(けんせい)を図ることができる。記録したデータは，後から日時やユーザー名で検索し再生やダウンロードが可能で，監査やトラブル発生時の検証に活用できる。

3.2　ZoomやWebexの自動録音や外線接続録音

MDISは，金融機関でのZoom，Webex利用の拡大を背景にコンプライアンス対策に幅広く対応するため，ZoomやWebexのコミュニケーションでも同一インフラに自動録音できる仕組みを提供しており，Teamsの自動録音nokosサービス提供開始以来，金融業界から注目を浴びている。さらに最近ではコールセンター業務でウェブ会議ツールと公衆回線とを外線接続する動きがあり，金融業界だけでなく他の業界でも，その録音機能が注目を浴びている。

3.3　高精度テキスト化とデータドリブン経営分析

MDISは従来，自動録音された音声データをテキスト化し，コンプライアンスチェックを強化する基盤を提供してきた。テキスト化されたデータを応対履歴などに活用して業務効率化を実現した。さらにコールセンターのオペレーターの感情分析，教育への活用など顧客の課題に幅広く寄与している。一般的なテキスト化では，認識精度を向上させるために金融や保険など業界別辞書を整備しているが，会社独自の専門用語に対する認識精度が低い。そのため，テキスト化されたデータを基にしたデータドリブン経営の実現には，音声テキスト化の認識精度を向上させる必要がある。しかし，固有の専門用語を収集し，辞書を人手で作成するためには膨大な労力を要する。そこで，MDISでは，辞書作成作業を効率化するために，三菱電機のAI技術“Maisart”を活用して，営業マニュアルなど企業の資産から，会社独自の専門用語も抽出できる専門用語抽出AIを開発した。これによって自然言語処理されたデータをMDISの優れたデータサイエンティスト(Kaggle(注4)金メダル保有者含む)がマイニングすることでデータドリブン経営を目指す企業に寄与することもできる。

(注４)　Kaggleは，Google LLCの登録商標である。

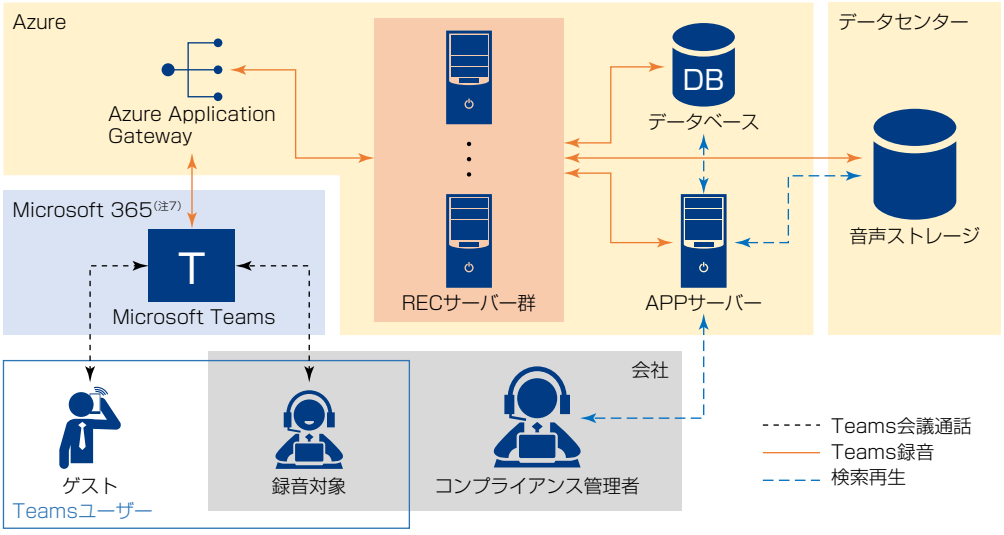
4. コンプライアンス録音と分析基盤

4.1　ウェブ会議の自動録音

図２に，nokosのTeams自動録音の仕組みを示す。MDISではnokosの通話録音ソリューションとしてベリントシステムズ社のVerint(注5) Financial Compliance(VFC)を採用している。各種ウェブ会議ツールと**図２**のAzure(注6)内サーバー

を構成するVFCを連携させることで，ウェブ会議の自動録音システムを構築した。VFCは世界的な金融機関などで多数コンプライアンス対策の実績があり，ユーザーの要件に対応するために優れた機能を備えている。nokosがVFCを採用することで，顧客満足度の向上が期待される。

（注５）　Verintは，Verint Systems Inc.の登録商標である。
（注６）　Azureは，Microsoft Corp.の登録商標である。



（注７）　Microsoft 365は，Microsoft Corp.の登録商標である。
REC：RECording，APP：APPlication

図２．nokosのTeams自動録音の仕組み

4.1.1　ウェブ会議ツールとの連携

自動録音を実現するには，ウェブ会議ツール（Teams，Zoom，Webex）と通話録音システム（nokos）間の双方で録音設定が必要である。ウェブ会議ツール側では，通話録音システムからの音声データ収集に対するアクセス許可が必要であり，通話録音システム側では，ウェブ会議ツール及びユーザー情報の登録が必要になる。ウェブ会議ツールが発する通話開始の信号をトリガーとして，通話録音システムが自動で録音を開始する。ウェブ会議ツールから通話録音システムへ連携されるデータには，音声データだけでなく通話情報のメタデータ（通話開始日時，通話時間，発信者，着信者，通話種別）も含まれる。通話録音システムには音声データと通話情報が紐（ひも）づけて登録され，音声を検索再生する際の検索条件としてそれらが利用可能である。

4.1.2　録音データの権限制御

通話録音システム内のユーザー情報はグループで管理されており，そのグループ構成に基づいた検索再生権限の制御が可能である。そのため，自身の録音を検索再生するといった制御だけでなく，部門長が部下全員の録音を検索再生する，コンプライアンスチェック部門が会社全体の録音を検索再生するといったニーズにも対応できる。

4.1.3　高可用性の実現とセキュリティー強化施策

コンプライアンス対策を目的とした録音システムで録音機能の高可用性は必須要件である。nokosでは録音基盤に，Microsoft AzureリソースのAzure Application Gatewayを組み込むことで録音機能の冗長化を実現している。また，録音した音声には機密性の高い情報が多く含まれるため，音声データの厳重な管理も必須である。nokosでは，音声保存先のストレージとしてFISC（The Center for Financial Industry Information Systems）安全対策基準に準拠したストレージサービスである三菱総研DCS㈱のDibertas（ディバタス）(注8)を採用し，録音基盤（**図２**のAzure環境）と専用線接続することでセキュリティー強化を実施している。

（注８）　Dibertasは，三菱総研DCS㈱の登録商標である。

4.2　高精度テキスト化のための専門用語抽出AI

図３に，専門用語抽出AIによる高精度テキスト化と，そのテキストデータを活用したデータ分析までのフローを示す。まず，専門用語抽出AIに学習させるデータとして，教師なしの重要語抽出手法(1)によって，疑似的な正解とする専門用語を付与したデータを作成する。次に，疑似正解を付与したテキストデータを基に，その文中から正解の専門用語を抽出するように，BERT(2)などの文脈の考慮が可能な事前学習済みの自然言語処理モデルをあらかじめファインチューニングしておく。そして，専門用語辞書の作成時に，顧客の営業マニュアルなどのテキストデータから，学習済みの専門用語抽出AIを用いて専門用語の候補を抽出し，音声認識エンジンに登録する。**図３**の音声系ソリューションの音声認識エンジンが音声データをテキスト化する際に，登録された辞書による補正が行われるため，高精度なテキスト化を実現する。質の良いテキストデータを基にするため，VoC(Voice of Customer)分析や，カスタマーやオペレーターの感情分析，重要文抽出など，経営の意思決定に寄与するデータ分析が可能になる。

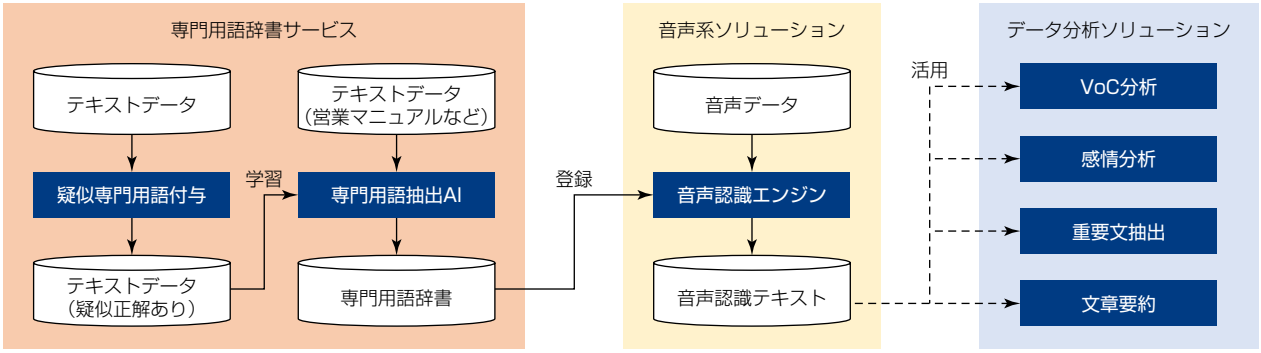


図３．専門用語抽出AIの仕組み

5. む　す　び

MDISは，過去20年以上にわたって，多くの企業に音声系ソリューションを導入し続けてきた。数多くの実績を持ち，全国100店舗を超える大規模な通話録音システムや大規模金融機関の音声テキスト化システムも構築した実績がある。録音機能やテキスト化機能の提供はもちろんのこと，１日10万回を超えるコールにも耐え得るスケーラビリティーや金融機関が求めるSLA(Service Level Agreement)にも対応できるアベイラビリティーも確保できる仕組みを提供してきた。そこで培ったシステム構築・保守・運用のノウハウで新しいコミュニケーションツールであるウェブ会議自動録音のコンプライアンス強化基盤を提供できることが強みである。

電話基盤の通話録音やnokosが持つ自動記録機能と音声認識技術を組み合わせることで，業務効率化，顧客サービスの向上，コンプライアンス強化，コスト削減などに活用できるシステムとして発展させていく。今後は音声認識とAIによる議事録や日報の自動作成，DLP(データ損失防止)といった機能強化を検討している。さらに自然言語処理されたデータをMDISの優れたデータサイエンティストがマイニングすることでデータドリブン経営を目指す企業に寄与することもできる。

AIを用いた音声認識や文章要約技術のレベルは年々向上しており，nokosの記録データも，コンプライアンス管理にとどまらず顧客満足度向上や応対品質向上への活用が可能である。MDISはこの分野での豊富なノウハウ・実績を基に，現時点の技術でできること，できないことを見極めて，三菱電機の情報技術総合研究所とも連携しながら，適切な場面での投入を提案して顧客の課題に対応している。

参　考　文　献

(1) Florescu, C., et al.：Positionrank: An unsupervised approach to keyphrase extraction from scholarly documents, Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics(Volume 1: Long Papers), 1105～1115 (2017)
(2) Jacob, D., et al.：BERT: Pre-training of deep bidirectional transformers for language understanding, Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies(Volume 1: Long and Short Papers), 4171～4186 (2019)

特集論文

AI-OCRとインボイス制度に対応した電子取引サービス“@Sign”

Electronic Transaction Service "@Sign" Compatible with AI-OCR and Invoicing System

村井園美*
Sonomi Murai
小倉大典*
Daisuke Ogura
古賀理沙子*
Risako Koga

*三菱電機インフォメーションネットワーク㈱

要　旨

三菱電機インフォメーションネットワーク㈱(MIND)は，ハンコ手続や紙の印刷のために出社せざるを得ない業務プロセスの見直しを後押しして，ニューノーマル時代の働き方改革に貢献するため，2021年３月から電子取引サービス“@Sign(アットサイン)”を提供している。このサービスは，契約書の締結，見積書／注文書等のファイル授受・保存をオンラインで完結できる。@Signでは，ニーズに合わせた機能追加や，他社連携での機能強化を実施している。@Signの利用で，ペーパーレス化，ワークフロー機能による業務効率化・生産性向上等，サステナブルな社会と企業のDX(Digital Transformation)を推進できる。

1. ま え が き

企業では在宅勤務などのテレワーク，オンライン会議などニューノーマル時代の働き方への対応が求められている。働き方改革には業務の電子化やペーパーレス化推進が重要になり，行政では手続の脱ハンコ化などの改革が進められている。しかし，企業では押印業務が残存しており，ハンコの手続や紙の印刷のために出社せざるを得ない業務プロセスがペーパーレス化推進の阻害要因として課題になっている。ペーパーレス化といっても単に紙文書を電子化するだけでなく，セキュリティー面の考慮や，対象文書によっては電子保存するための法令ガイドラインの要件があり，準拠が必要になる。ニューノーマル時代には，デジタル情報の真実性(本人性，非改ざん性)を担保する電子署名・タイムスタンプなどのIT技術活用が働き方改革推進の鍵になる。

また，2018年に経済産業省が“デジタルトランスフォーメーションを推進するためのガイドライン(DX推進ガイドライン)”を公表し，企業でのデジタル技術の活用を積極的に促進し始めたことによって，様々な企業でDXが推進されている。

MINDでは，企業の働き方改革，電子帳簿保存法(以下“電帳法”という。)・適格請求書等保存方式(以下“インボイス制度”という。)等の法令／制度への対応やDX推進に貢献するため，@Signの提供，機能追加を実施している。サービス利用イメージを**図１**に示す。

本稿では，@Signの主な機能・特長や新たなニーズへの対応のために追加した機能について述べる。

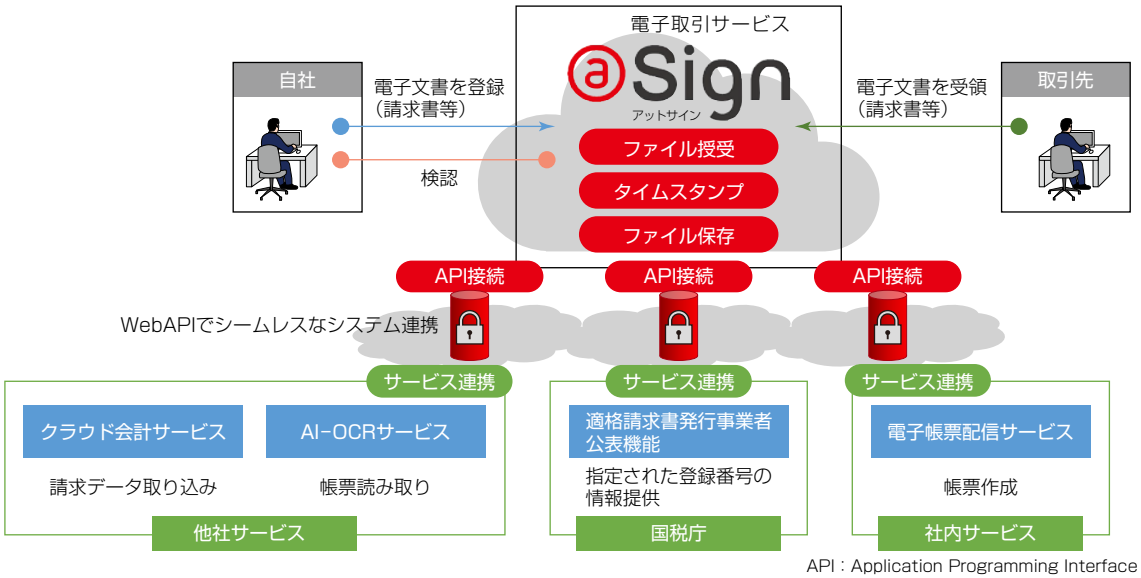


図１．@Signのサービス利用イメージ

2. @Signの機能・特徴

2.1　豊富な機能で様々な要望に対応

@Signは電子契約，電子取引(見積り／注文／納品／請求書等)，電子検認をオンラインで完結できるクラウドサービスであり，業務の電子化に関して幅広く対応している。サービスメニューと対応機能を**表1**に示す。

表1．サービスメニューと対応機能

◎：必須　○：任意　－：未対応

メニュー		説明	ワークフロー	PDFへのファイル添付	文書保存	取引先への送付
画面操作	新規契約	電子契約に利用	◎	－	◎	◎
	新規取引	見積書等の取引に利用	◎	－	◎	◎
	電子検認	社内の電子検認に利用	◎	○	◎ (スキャナー保存含む)	－
	新規保存	文書の保存に利用	－	○	◎ (スキャナー保存含む)	－
	一括検認	定型文書の一括検認に利用 (一括20ファイルまで)	－	－	－	－
文書管理APIオプション		既存システムとの連携	外部システムからの要求(HTTPS REST API)で，PDFや関連ファイルを文書情報として@Signへ登録可能			
ログイン認証オプション		シングルサインオン	Azure(注1)AD認証によるシングルサインオンが可能			
		IPアドレス制限	接続元IPアドレスを指定してアクセス制限が可能			
関連ファイル保存オプション		関連ファイルの保存	文書登録時に関連ファイルの保存が可能			
AI-OCRオプション		案件情報の自動入力	アップロードしたPDFから属性情報を読み取り，また読み込んだ情報をCSVに出力可能 (今後リリース予定)			

(注1)　Azureは，Microsoft Corp.の登録商標である。
PDF：Portable Document Format，AD：Active Directory，IP：Internet Protocol，CSV：Comma Separated Values

2.2　すぐに導入可能で始めやすい

@Signは最短2週間・初期投資不要で始めることができて，ユーザー目線のインタフェースで直感的な操作が可能である。API連携することで，既存の顧客システム経由の電子保存や電子取引も可能である。API連携イメージを**図2**に示す。

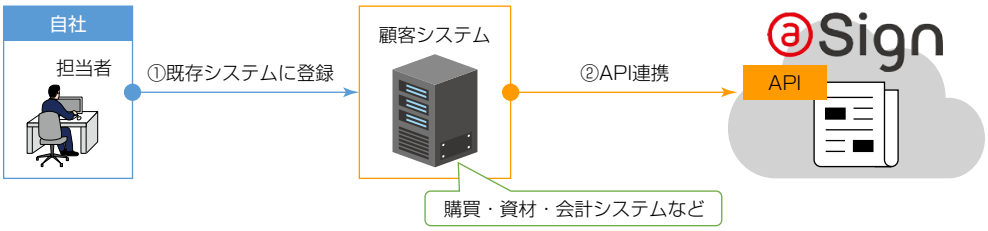


図2．API連携イメージ

@Signでは試使用環境を用意しており，契約前に無償で試使用できる。また，まずは“電子保存だけ”から始めたいなど，少しずつ電子化対応を行いたい場合には，メニュー制御によって一部の機能だけ提供することも可能である。さらに，将来電子化の対応範囲を広げる際は，簡単に機能の拡張ができる。

2.3　各種認定を取得・法令に対応した安心サービス

@Signは，総務大臣の認定する時刻認証業務事業者が発行するタイムスタンプの付与ができる。また，電子証明書による電子署名の付与ができ，主務三省(総務省，経済産業省，法務省)による“電子署名及び認証業務に関する法律に係る認定認証業務の認定”を取得した電子証明書の利用も可能である。電子署名・タイムスタンプを付与することで，“誰が”“いつ”作成した文書であるかということと，文書が改ざんされていないことを客観的に証明できる。さらに，@Signでは電帳法に対応した文書の保存が可能であり，公益社団法人 日本文書情報マネジメント協会(JIIMA(注2))による，電帳法に基づく“電子取引ソフト法的要件認証”及び“電帳法スキャナ保存ソフト法的要件認証”を取得している。

(注2)　JIIMAは，公益社団法人 日本文書情報マネジメント協会の登録商標である。

3. サービス提供での課題

3.1 利便性向上やデータ利活用のニーズへの対応

近年，働き方の変化やデジタル技術の進歩に伴い，多くの企業でDXが推進されている。従来の紙業務も電子化が進んで，効率的な働き方に移行しつつある。@Signではペーパーレス化の実現が可能であり，ワークフロー機能やメール自動送信機能によって業務の効率化に貢献している。しかし，“データの入力については利用者が手作業で実施する必要がある”“他サービスにデータを連携する機能が充実していない”等の点から，利便性やデータの利活用といった面では機能が不足しており，これら機能の拡充が求められた。

3.2 電帳法の改正やインボイス制度への対応

2022年１月１日の電帳法の改正で，電子取引での電子データ保存が義務化された。やむを得ない事情がある場合には，宥恕(ゆうじょ)措置によって２年間は紙での保存も容認されるが，2024年１月１日には電帳法に対応した運用を開始する必要がある。2023年10月１日には，消費税の仕入税額控除の方式としてインボイス制度が開始されるため，企業では両法令を考慮した対応の検討が必要になっている。@Signでは電帳法に対応した保存は可能だが，文書情報を登録する際，インボイス制度で記載要件になっている登録番号や適用税率を登録する機能がなく，データを利活用するためには実装が不可欠であった。

4. @Signへの機能追加

３章に述べた課題を解決するため，追加機能を開発予定(一部開発中)である。

4.1 AI-OCRによる自動入力(利便性向上)

文書情報の自動入力機能を追加するため，OCR技術を活用し，文書に記載された文字をデジタルな文字情報に変換することを検討した。しかしOCRには，手書き文字の認識率が低い，帳票や書類のフォーマットを事前に定義しておく必要がある，といった弱点がある。@Signでは見積書，注文書，請求書等の様々な帳票に対応しており，各企業から発行される帳票のフォーマットも統一されていないため，事前に読み取り位置や項目を定義することは難しい。そこで，OCRにAIの技術を加えたAI-OCRを採用した。AI技術を組み合わせることで，機械学習による文字認識率の向上や，多種多様なフォーマットの帳票で自動的に項目を抽出することが可能である。読み取り機能については，他社のAI-OCRサービスとの連携で機能強化を実施している。AI-OCRを組み込んだシステムの画面イメージを**図３**に示す。

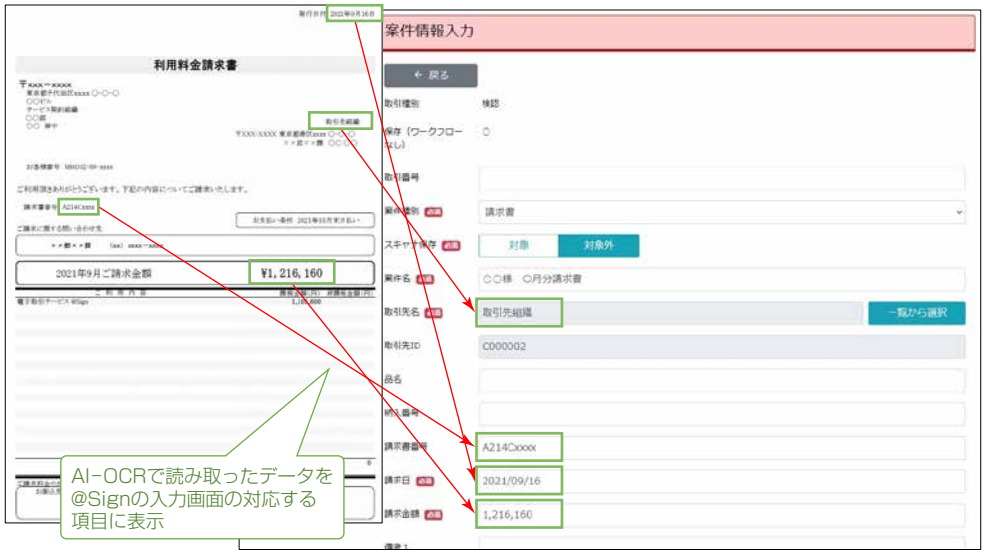


図３．AI-OCRを組み込んだシステムの画面イメージ

4.2　インボイス制度への対応

適格請求書(インボイス)に記載された登録番号や税率ごとの金額を@Signに登録できるよう，入力項目を追加した。

また，適格請求書を発行できるのは適格請求書発行事業者に限られており，受領側は，記載された登録番号が正しいことの確認，適格請求書発行事業者とそうでない事業者とで税額計算の処理を分ける等の対応が必要になる。そのため，国税庁から公開されているAPIと連携することで登録番号が適正なものかを確認する機能を@Signに追加する。この機能で，請求書1枚ずつ登録番号の確認を行う作業を省力化する。

4.3　電子帳票配信サービスとの連携(利便性向上)

MINDの電子帳票配信サービスとの連携によって，請求書の作成から送信までの流れを@Signの操作だけで完結するよう，機能を追加する。具体的には，@Signに登録された帳票作成用データを電子帳票配信サービスに送って，作成された帳票を@Signで保存したり，取引先へ送信したりする。電子帳票配信サービスとの連携イメージを**図4**に示す。

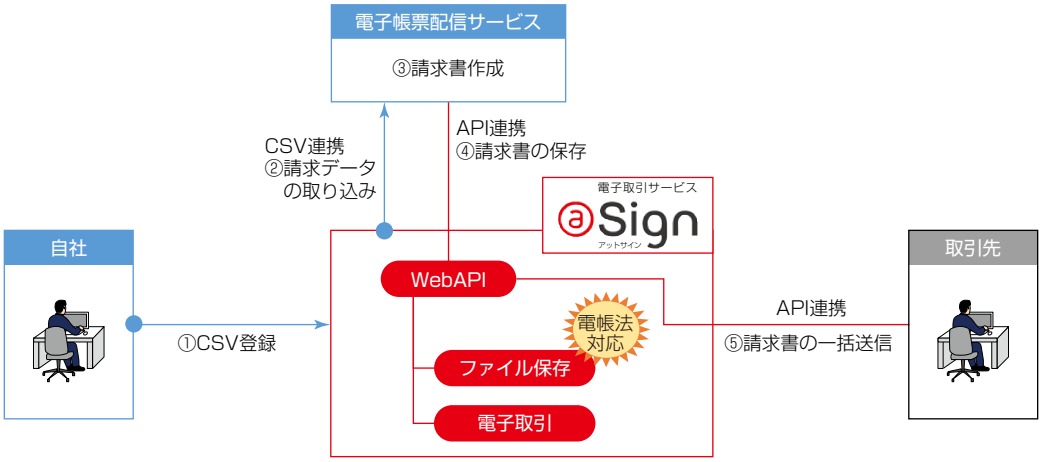


図4．電子帳票配信サービスとの連携イメージ

4.4　クラウド会計サービスとのデータ連携(データ利活用)

請求書から読み取った情報をCSVファイルやAPIで他システムと連携することで，データ利活用を実現する。具体的には，クラウド会計サービスに連携できるよう@Signに機能を追加する。請求書に記載された情報を有効に活用するため，現在は@Signに登録していない明細情報等も自動で読み取ることができるよう，今後，AI-OCRによる読み取り機能の改良も併せて実施していく。クラウド会計サービスとの連携イメージを**図5**に示す。

図5．クラウド会計サービスとの連携イメージ

5. む　す　び

@Signについて，企業のDX推進に資するために組み込んだAI-OCRやそのデータの利活用，インボイス制度への対応を述べた。現在，文書情報のスキャン／入力代行のオプションサービスの提供も検討中であり，今後も継続して機能の強化，サービスの拡大を実施していく。

これからも安心・安全なICT(Information and Communication Technology)と高品質のサービス提供を通じた，活力とゆとりある社会の実現への貢献を目指す。

特集論文

デジタル化の動向と“販売指南”の対応

関根大樹*
Daiki Sekine

*三菱電機ITソリューションズ㈱

Movement of Digitalization and Improvement of "Hanbaishinan"

要　旨

2023年10月から施行される“適格請求書等保存方式(インボイス制度)”の影響によるバックオフィス作業の増加を解決するため，官公庁主導で“中小企業共通EDI(Electronic Data Interchange)(中小企業でも受発注業務のデジタル化を実現できる仕様)”，“JP PINT(電子文書のネットワーク標準仕様等)”，“ZEDI(銀行間資金決済)”が展開され，官民一体となってデジタル化(デジタライゼーション)が進められている。

三菱電機ITソリューションズ㈱(MDSOL)では，官公庁が進めるデジタル化に合わせて，MDSOLが提供する販売管理システム“販売指南”を改修して販売管理業務のデジタル化に対応する。

具体的には，販売指南の取引データを，各省庁のEDI仕様に合わせてデータ変換後，データ連携をして，各業務プロセスの取引にかかる作業負荷を削減することでバックオフィス作業の増加を解決する。また，販売指南の各業務プロセス間の取引データをシームレスに連携する機能を開発し，各取引書類の照合作業を効率化する。

開発する連携機能は，出力定義の設定変更だけで様々な項目を出力できる販売指南の汎用データ出力機能“外部出力”を流用する。これによってルール変更や法改正に柔軟に対応し，保守性や発展性の高いシステムでユーザー業務のデジタル化を支援する。

1. ま え が き

2023年10月から，消費税の仕入税額控除方式がインボイス制度に変更される。中小企業から大企業に至るまでほぼ全ての企業が対応を迫られており，取引先が適格請求事業者であるか否かの確認や，対象となる適格請求書の電子保管等によってバックオフィス作業が増えることが見込まれている。これを解決するため，官公庁主導で業務のデジタル化が推し進められている。“デジタル化”とは，現行の業務プロセス内の紙媒体を電子ファイルに置き換えるだけではなく，デジタルを前提に業務プロセス自体を見直すことを指す。

販売指南は，中小企業をメインターゲットとするMDSOLが開発した販売管理システムである。2022年４月に，電子帳簿保存法対応で取引書類のPDF(Portable Document Format)化機能をリリースしたが，これに続いて業務のデジタル化に対応する。デジタル化した販売管理業務のイメージを**図１**に示す。

本稿では，インボイス制度によるバックオフィス作業の課題，業務のデジタル化による解決策及び販売指南の対応について述べる。

2. 顧客業務の課題

2.1　バックオフィス作業の効率化

インボイス制度に対応するためには，取引先である適格請求書発行事業者から受け取るインボイスを保存し，税務調査の際に速やかに提出できるようにすることが要求される。取引先ごとに何がインボイスであるか確認した上で，納品書と請求書の照合や，請求書と入金額の照合などの作業を進める必要があり，多くの取引先から郵送されてくる紙のインボイスを，都度，確認・保管・管理することになる。従来と比較し作業負荷が増えるため，このバックオフィス作業の効率化が求められる。

2.2　ルール変更や法改正への柔軟な対応

各業務プロセスを効率化するため，EDIを導入している顧客も存在する。しかしEDIの種類ごとに連携項目や通信方法などの仕様が異なり，顧客との取引ルール変更や法改正の際に多大なプログラム改修が発生する。これに投入する時間や費用の削減が必要であり，変更に対して柔軟に対応できる仕組み作りが不可欠である。

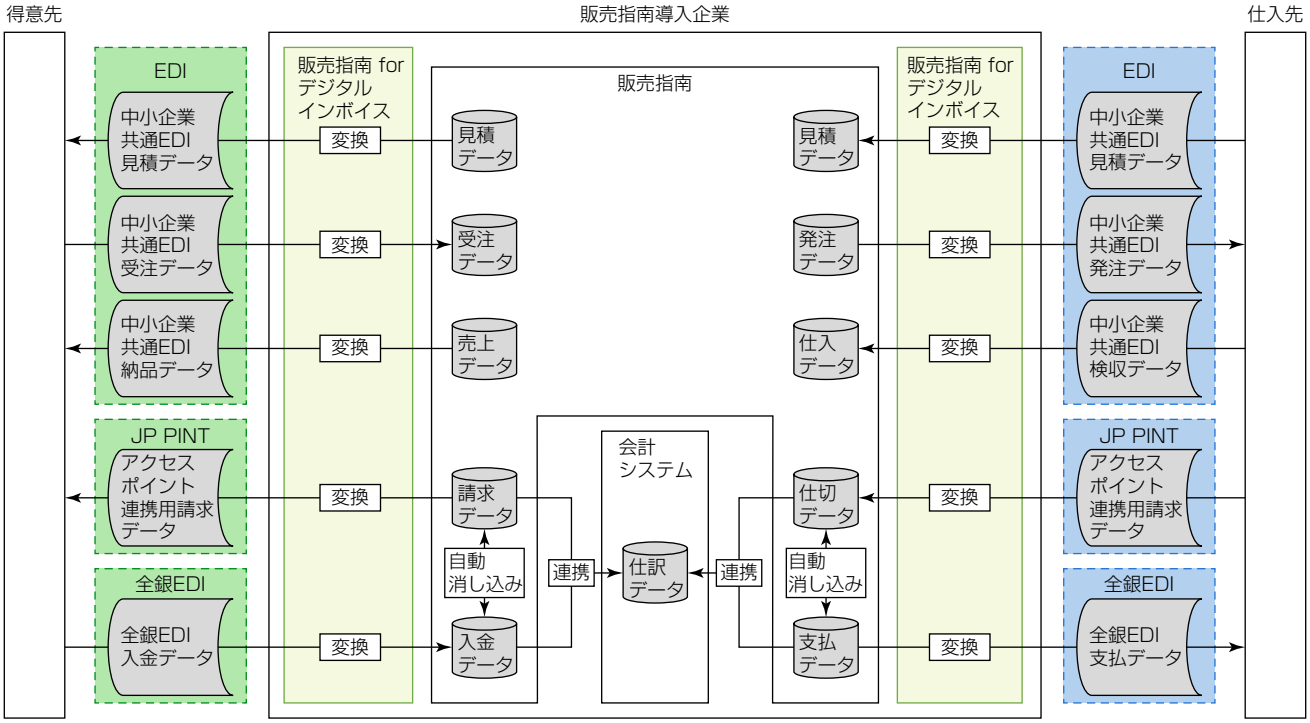


図1．デジタル化した販売管理業務のイメージ

3．官公庁が進める業務のデジタル化

2章に述べた課題解決のため，各省庁はデジタル化を進めている。中小企業庁は受発注業務のデジタル化実現に向けて，国連CEFACT(貿易円滑化と電子ビジネスのための国連センター)の業界横断EDI辞書に準拠した“中小企業共通EDI”を策定した。デジタル庁はデジタルインボイス推進協議会の提言を受けて，日本でのデジタルインボイス国内標準仕様“JP PINT”を公開した。金融庁・金融審議会は“国内送金指図で使用する電文方式をXML(eXtensible Markup Language)電文に移行する”ことを提言し，XML電文に対応した“ZEDI”が一般社団法人 全国銀行協会(全銀協)によって開発された。

3.1　中小企業共通EDI[(1)]

中小企業共通EDIは，中小企業でも低コストに受発注業務のデジタル化を実現できる汎用性の高い仕組みである。受発注業務のEDI仕様が中小企業共通EDIで標準化され，取引先ごとに用意する専用端末や用紙が不要になり，山積みになっていた伝票をデータで一元的に管理でき，中小企業が抱える受発注業務の問題を解決する。

3.2　JP PINT[(2)]

JP PINTは，ヨーロッパ，オーストラリア，シンガポールなどで採用されているグローバルな規格“Peppol”をベースにした請求書の国内標準規格である。4コーナーモデルと呼ばれるアーキテクチャーを採用しており，エンドユーザーは仕組みを理解していなくても利用できる。

3.3　ZEDI[(3)]

ZEDIは，全銀協が構築した金融EDIのことで，商取引に関する情報を振込データに添付してやり取りする仕組みを指す。振込データと取引情報を関連付けることで，これまで手作業であった入金消し込み等の照合作業効率が大幅に向上する。

4. バックオフィス作業のデジタル化に対する販売指南の対応

バックオフィス作業の負荷を削減するため，販売指南では受発注から入金・支払までの業務プロセスのデジタル化を支援する仕組みを構築する（**図2**）。

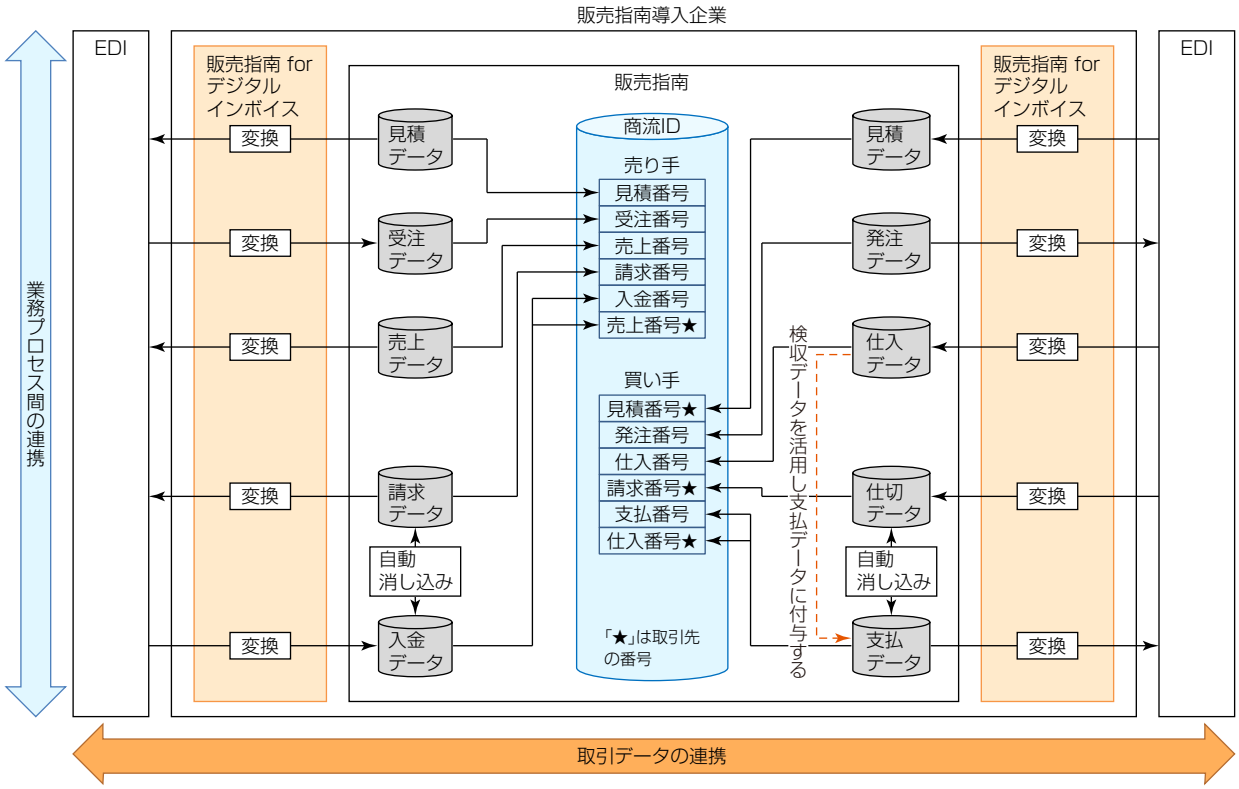


図2．デジタル化した業務に対応した販売指南のデータフロー図

4.1　シームレスなデータ連携

4.1.1　取引データの連携

2. 1節で言及したバックオフィス作業の効率化を実現するために，各省庁のEDIフォーマットと，販売指南が持つ取引データの変換を自動化する機能を実装し連携する。この連携時のデータ変換を自動化することで，各業務プロセスの取引にかかる作業負荷を削減する。

具体的には，中小企業共通EDI及びJP PINTは，販売指南の受発注，入出荷，売上げ・仕入れ，請求データと連携する。ZEDIは販売指南の入金，支払データと連携する。

これによる効果を次に示す。

(1)　受発注～売上げ・仕入れ
　(a)　業務効率アップでコスト削減
　(b)　人的ミスを削減
　(c)　取引データ検索の簡素化
(2)　請求
　(a)　紙の請求書発行廃止による業務負荷削減
　(b)　受領したインボイスの記載事項確認負荷削減
(3)　入金・支払
　(a)　入金と請求の消し込み作業が簡素化され受取企業の業務負荷削減
　(b)　支払の問合せがなくなり支払企業の業務負荷削減

4.1.2　業務プロセス間の連携

2. 1節で言及した各取引書類の照合作業を効率化するため，各業務プロセスの取引データを，プロセス間でシームレスに連携する機能を実装し，作業負荷を削減する。

プロセス間で連携するためのキー“商流ID”を販売指南に実装することで，取引データ，入出金データを関連付けて，納品書と請求書の照合や，請求書と入金額の照合をデジタル化する。

4.2　柔軟なプログラム構造

2. 2節で言及したルール変更や法改正に柔軟に対応するため，出力定義の設定変更だけで様々な項目を出力できる販売指南の汎用データ出力機能“外部出力”を流用し，バージョンやカスタマイズの有無に影響せず対応できる仕組みを構築する。

今回の対応では，データベースに保存している設定情報をドキュメントファイル化することで販売指南と外部出力を疎結合化する。また，近年のEDIデータ形式の主流であるXMLやJSON(JavaScript Object Notation)にも対応する(**図３**)。

このプログラム構造によって，対応ごとのプログラム改修が不要になり，時間や費用の投入を大幅に削減する。

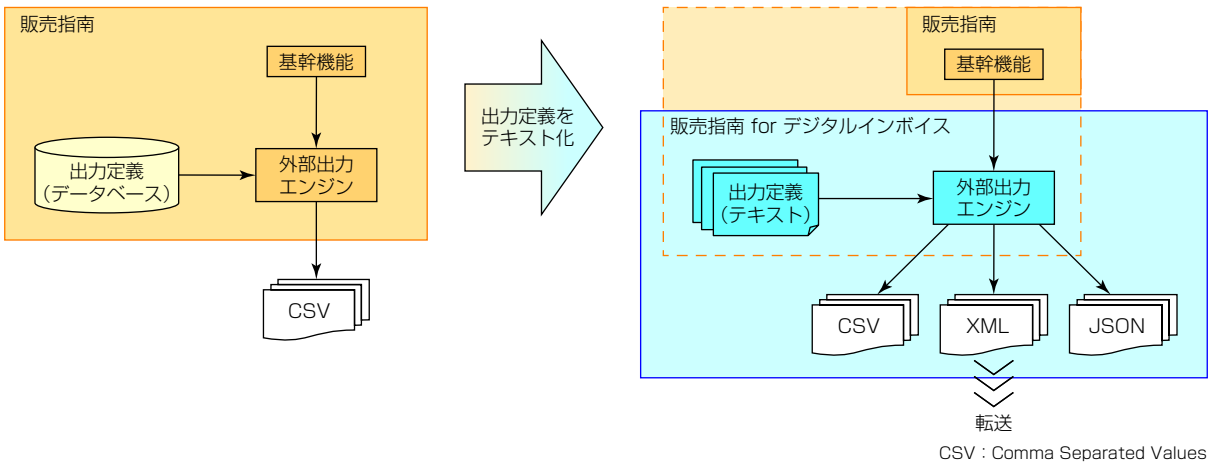


図３．プログラム構造の変更イメージ

5. む　す　び

販売管理システムはカスタマイズが多く発生する分野であり，パッケージ本体のバージョンアップごとにプログラム改修が必要になる。また，ルール変更や法改正にも多大なカスタマイズコストがかかっており，タイムリーな適応の足かせになる。

今回のデジタルインボイス対応では，外部出力を販売指南から切り出すことで疎結合化する。これによって改修にかかる作業を簡素化し，導入期間や費用の大幅削減を図っている。

今後のシステム開発でも，同様の構造でシステムを構築し，保守性や発展性の高いシステム開発を進めることでユーザー業務のデジタル化につなげていく。

参 考 文 献

(1)　次世代企業間データ連携調査事業事務局：中小企業共通EDI標準 概要説明資料 (2018)
https://www.itc.or.jp/datarenkei/dlfiles/edi/6EDIv1.pdf
(2)　デジタルインボイス推進協議会：デジタルインボイスとは｜Peppol(ペポル)について
https://www.eipa.jp/peppol
(3)　一般社団法人 全国銀行資金決済ネットワーク：【S-ZEDI】受取企業様向け利用ガイド (2019)
https://www.zenginkyo.or.jp/fileadmin/res/abstract/efforts/smooth/xml/s-zedi_user_guidance.pdf

特集論文

顧客のセキュリティーライフサイクル全般を支えるサイバーフュージョンセンター

Cyber Fusion Center for Supporting Security Lifecycle of Customers

村松孝俊*
Takatoshi Muramatsu
鈴木貴也*
Takaya Suzuki
高田直樹*
Naoki Takata

*三菱電機インフォーメーションネットワーク㈱

要　旨

三菱電機インフォメーションネットワーク㈱(MIND)は，顧客のセキュリティーライフサイクル全体を横断的に支援するための専門組織として，2022年10月にMINDサイバーフュージョンセンターを設立し，ファシリティーの増強を2022年12月に完了した。MINDサイバーフュージョンセンターではサイバーセキュリティーフレームワークを基盤としており，セキュリティーライフサイクル全体を網羅するサービスを提供することが可能になった。これらのファシリティー・サービスによって，顧客の安心・安全なDX(Digital Transformation)化推進に貢献していく。

1. ま え が き

MINDは，1998年にセキュリティーサービス事業を開始し，2006年にMIND SOC(Security Operation Center：セキュリティーインシデントの発生を監視，データ解析やログ分析を行う)を立ち上げて，脆弱(ぜいじゃく)性情報の提供・セキュリティー機器の運用監視・インシデント通知をメインに顧客のサイバーセキュリティー対策の実現に貢献してきた。

サイバー攻撃の手法は日々高度化しているため，セキュリティー対策を実施していたにもかかわらず巧妙に突破・侵入されて重要な機密情報を盗み出されてしまったなど，深刻な被害を及ぼした事例が増加している。そこで，“侵入を完全に予防することは不可能であり，攻撃を受けた場合にいかに早く復旧するかが重要”という考え方が，近年のサイバーセキュリティー対策では不可欠である。そのため，攻撃を受けた際の検知・防御だけではなく，対応，復旧といったセキュリティーライフサイクル全体を網羅しているNIST(National Institute of Standards and Technology：アメリカ国立標準技術研究所)サイバーセキュリティーフレームワークに基づいた対策が必須になる。また，サプライチェーン攻撃の流行に伴い，取引先となる組織のセキュリティー対策も重要になってきており，セキュリティー対策が取引先選定の基準になるなど，中堅以下の企業のセキュリティー対策も重要視されてきている。

さらに，昨今高度セキュリティー要員の育成・採用は多くの企業の課題になっている。

そこでMINDは顧客の課題を解決するため，MINDサイバーフュージョンセンターを設立した(**図1**)。MINDではこれまで，特定，防御，検知の分野でサービスを提供していたが，攻撃を受けた際の被害範囲の調査や，原因分析に必要になる高度なフォレンジック・侵害調査などの，CSIRT(Computer Security Incident Response Team：セキュリティーインシデントが発生した際の対応と平時の予防を行う)領域へ踏み込んだサービスを提供することで，顧客のセキュリティーライフサイクル全体をサポートする。

図1．MINDサイバーフュージョンセンター

本稿では高度化するサイバー攻撃に備えて設立したMINDサイバーフュージョンセンターについて，設立の際に参照したNISTサイバーセキュリティーフレームワークの概念やMINDサイバーフュージョンセンターの特長，提供を開始したサービス，今後の展望について述べる。

2. NISTサイバーセキュリティーフレームワーク

2.1 NISTサイバーセキュリティーフレームワークの概要

NISTサイバーセキュリティーフレームワーク（以下“NIST CSF”という。）とは，NISTが定める，米国だけでなく世界各国の企業がセキュリティー対策を講じる際に参照しているサイバーセキュリティー対策のフレームワークである(1)。日本国内でも，経済産業省と共同で“サイバーセキュリティ経営ガイドライン”を発行しているIPA（独立行政法人 情報処理推進機構）が，“重要インフラのサイバーセキュリティを改善するためのフレームワーク”として，NIST CSFの翻訳版を公開している(2)。

NIST CSFは，国家での重要インフラが確実に機能することを目的に制定されており，NIST CSFの考え方を基に発行されたNIST SP 800-171は，取引企業からの情報漏洩（ろうえい）を防ぐために業務委託先でのセキュリティー対策を定めたガイドラインで，米国では政府機関が行う調達取引で全世界の取引先企業にNIST SP 800-171への準拠を義務付けており，民間企業でも導入が進んでいる。日本でも“NIST SP 800-171と同じ水準の管理策を盛り込んだ新たな情報セキュリティー基準”である防衛産業サイバーセキュリティ基準を2022年４月に防衛装備庁が発行し，軍事産業だけでなく将来的に国内の他産業でもサプライチェーン全体を守る基準になると考えられる。

2.2 NIST CSFの五つのコア機能

NIST CSFではサイバー攻撃の手法の高度化によって，“侵入を完全に防ぐことは不可能である。攻撃は受ける前提で，攻撃の影響を最小限にとどめて，素早く復旧する。”という近年のサイバーセキュリティー対策の考え方が取り入れられており，組織の種類や規模を問わない共通のサイバーセキュリティー対策として，“特定（Identify）”“防御（Protect）”“検知（Detect）”“対応（Respond）”“復旧（Recover）”という五つのコア機能が規定されている。

ここではその五つのコア機能についてそれぞれ述べる。

(1) 特定（Identify）

システム，人，資産，データ，機能に対するサイバーセキュリティーリスクの管理に必要な理解を深めて，組織のリスクマネジメント戦略とビジネスニーズに適合するようにセキュリティー対策の優先順位付けを行う。

(2) 防御（Protect）

重要サービスの提供を確実にするための適切な保護対策を検討し，発生する可能性のあるサイバーセキュリティーイベントがもたらす影響を抑制する。

(3) 検知（Detect）

サイバーセキュリティーイベントの発生を識別するのに適した対策を検討し，タイムリーな発見を可能にする。

(4) 対応（Respond）

検知されたサイバーセキュリティーインシデントに対処するための適切な対策を検討し，サイバーセキュリティーインシデントがもたらす影響を最小限に封じ込める。

(5) 復旧（Recover）

サイバーセキュリティーインシデントがもたらす影響を軽減するために，通常の運用状態へのタイムリーな復旧を支援する。

これらの機能をまとめて考慮することによって，組織のセキュリティーライフサイクルを，高度かつ戦略的にとらえることが可能になる。

3. MINDサイバーフュージョンセンター

2章で述べたように，MINDでは，近年の高度化するサイバー攻撃に対して，NIST CSFの五つのコア機能を踏まえたセキュリティー対策を考慮していく必要があると考えている。セキュリティー対策が十分に考慮できていない場合，イン

シデント発生時に確認・対処すべき事項の決定や確認した項目に対する判断が難しく，対処が漏れることで，攻撃を止めることができず攻撃者に継続した攻撃を許すなどのリスクが発生する。

MINDがこれまで提供してきた主要なセキュリティーサービスであるマネージドEDR(端末監視)サービスや標的型攻撃対策サービスなどはSOCサービスに分類され，“特定”“防御”“検知”のコア機能に該当する。“対応”“復旧”のコア機能は従来，自組織内に構築するCSIRTの扱う領域であった。しかし，昨今のITシステムの複雑化，サイバー攻撃の巧妙化によって日本のセキュリティー人材不足は深刻化しており，自組織でのセキュリティー人材の確保・育成が難しいという声を聞くことが多くなっている。

そこで，従来のSOC領域(特定・防御・検知)に加えてCSIRT領域(対応・復旧)も支援を可能にするために，組織及び設備をリニューアルしたMINDサイバーフュージョンセンターを設立した。MINDのセキュリティー対策のこれまでとこれからを**図2**に示す。

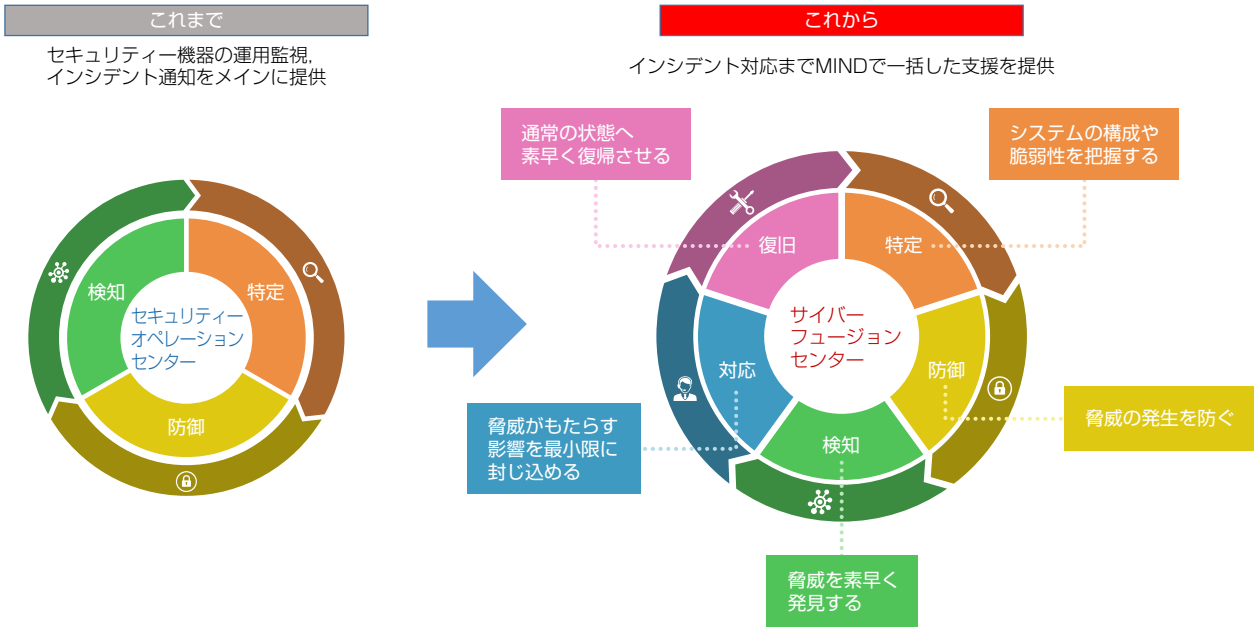


図2．MINDセキュリティー対策のこれまでとこれから

3.1　MINDサイバーフュージョンセンターの特長

3.1.1　安心・安全なセキュリティー運用環境

CSIRT領域で扱うデータは，顧客の機微な情報が多くなる。MINDサイバーフュージョンセンターは，顧客から安心してセキュリティー運用を任せてもらえるよう，人やモノの出入りを防犯的に監視・管理する物理セキュリティー対策，情報通信技術に基づく情報の安全管理，アクセス管理による情報セキュリティー対策を持ったセンターとして設計した。

3.1.2　サイバーインシデント対応の迅速化

サイバーインシデントでのラテラルムーブメント(“横方向への移動”を意味し，攻撃者によるサーバーや他端末などネットワーク全体に感染を広げるアクション)までの所要時間は短くなってきており，迅速な対応が求められている。サイバーインシデント発生時の“検知”から“復旧”までの対応をより迅速にワンストップで提供可能にするため，インフラエンジニアからセキュリティーアナリストまでサービス提供に必要なセキュリティーエキスパートをセンターに集約するとともに，役割・グループを明確化したチーム体制を整備した。また，アナリスト間のコミュニケーションを重視したハニカム構造のデスク配置や，即時に打合せ可能なスタンディングエリアなどを採用するとともに，サービスプラットフォームによる業務の最新化，AIを活用したインシデント分析技術などを採用した。

4. MINDサイバーフュージョンセンターで提供するサービス

この章では，MINDサイバーフュージョンセンターの開設に合わせてMINDが開始した“CSIRT運用支援サービス”について述べる。

4.1　SOCとCSIRT

組織のセキュリティー運用を行う組織の体制を述べる。セキュリティー運用を行う組織として大きく分けてSOCとCSIRTがあり，どちらもセキュリティー対策を行う組織だが，次のとおりの役割分担となっている。

(1)　SOC

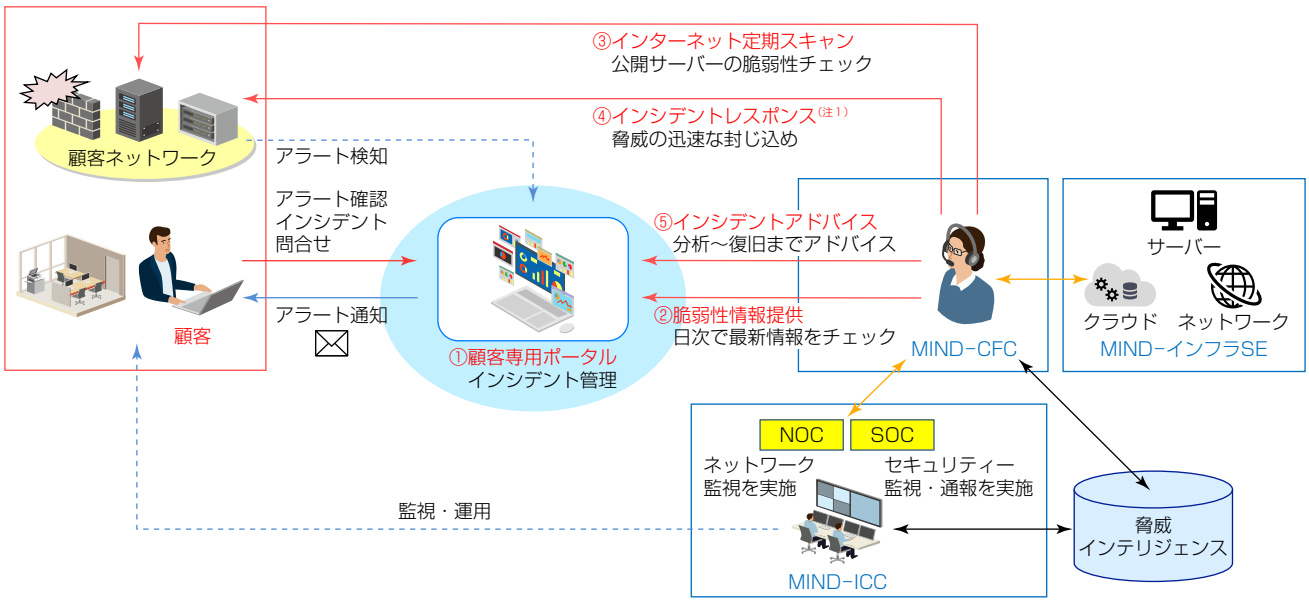
セキュリティー機器から通知されるアラートや，ネットワーク機器，サーバーなどから出力されるログを分析し，対応要否，対応優先度を判断し，通知する組織である。事前の検知や対策を主な業務とする。SOCは，MSS(マネジメントセキュリティーサービス)といった名称で提供されており，外部への委託を利用しているケースも多く見られる。

(2)　CSIRT

セキュリティーインシデントに対応する組織である。自社システムに関する脆弱性情報の収集・対応やインシデント発生時，対応方針を立案し，社内外の組織との情報共有や連携を行う。一般的にインシデントの発生時に社内の調整が入る観点から，CSIRTは社内で運営することが多い。大手の企業ではこのCSIRTを専門の組織として立ち上げているが，中小企業では情報システム部門の担当者がこの役割を実施しているという状況も多い。

4.2　サービス内容

今回提供を開始した“CSIRT運用支援サービス”では，今まで提供していなかった，“対応”“復旧”のサポートを提供し，より顧客に寄り添ったサービスとして位置付けた。サービスの概要を**図３**に示す。



CFC：サイバーフュージョンセンター，ICC：統合運用管制センター，NOC：Network Operation Center
（注１）　現行対応範囲はFirewall(順次拡大)

図３．CSIRT運用支援サービス

新たに提供する“対応”“復旧”では，検知したセキュリティーインシデントをクローズするまでサポートを行う。サポートするインシデントは，MIND SOCで検知したインシデントとユーザーからの申告によるインシデントで，ユーザーからの申告は専用のポータルを提供し，インシデントかもしれないという相談から受け付けて，インシデントアドバイスという形で，端末や機器のログの解析方法や確認の観点をアドバイスするサポートを行う。さらにヒアリングした顧客の環境を考慮した上で，段階を踏んだ対策を立案していき，これによって顧客はCSIRTとして次に実施すべきことが明確になる。

さらに，既存のSOCで提供している“特定”についてもこのサービスで強化しており，顧客のシステムで利用しているソフトウエアの脆弱性情報の収集，提供や，インターネットに公開されているアドレスの脆弱性スキャンの実施も行う。

4.3　サービスの特長

MINDは長年，金融業界や三菱電機向けにSOCのサービスを提供してきたため，SOCに対するノウハウを蓄積している。また，SOCとして顧客CSIRTを長年支えてきたことで，CSIRTとして実施すべきノウハウも持っている。これらを武器に，顧客対応範囲としていたCSIRT領域まで一歩踏み込んで，SOCからCSIRTまでワンストップでのインシデント対応を顧客に提供する。

5. む　す　び

MINDサイバーフュージョンセンター及びCSIRT運用支援サービスは，顧客のシステムDX化が進む中で，DX化したシステムのセキュリティー対策への懸念や，セキュリティーインシデントが発生した際に対応ができるか分からないといった悩みに対応できるサービスである。

SOCサービスで培ったノウハウを活用してサービス提供先の拡販を進めて，５年後には100件規模の顧客を支えるMINDサイバーフュージョンセンターになることを目指す。

参 考 文 献

(1) National Institute of Standards and Technology：Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (2018)
https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf
(2) 独立行政法人 情報処理推進機構：重要インフラのサイバーセキュリティを改善するためのフレームワーク 1.1版 (2018)
https://www.ipa.go.jp/files/000071204.pdf

特集論文

OTネットワークセキュリティー機器“MELWALL”

OT Network Security Device "MELWALL"

高須賀史和*
Fumikazu Takasuka
木村有佑*
Yusuke Kimura

*インフォメーションシステム統括事業部

要　旨

近年，サイバー攻撃の対象として工場や発電所といったプラントやインフラの制御システムが狙われる事例が増えており，設備そのものや，サービスの提供や安全を維持するためのシステムを攻撃されることが懸念されている(1)。

三菱電機では，FA，電力，公共インフラなど幅広い分野での制御システムの知見や技術・経験を生かして，アセスメント・コンサル，セキュリティー対策導入，運用保守までをワンストップで提供するOT(Operational Technology)セキュリティーソリューションサービスを提供している。

OTネットワークセキュリティー対策製品の一つとして当社が提供するOTネットワークセキュリティー機器“MELWALL(メルウオール)”は，既存のネットワーク構成を変更せずにOTネットワークを論理的に分割してセキュリティー脅威の感染拡大防止を実現する。

1. ま え が き

従来，サイバー攻撃の対象は企業の業務システムやウェブサイトなどの情報システムが主体であり，これらのシステムが持つ機密情報を狙う攻撃が主流であった。しかし近年は，工場や発電所といったプラントやインフラの制御に用いられる制御システムが狙われ始めており，設備そのものや，サービスの提供や安全を維持するためのシステムを攻撃されることが懸念されている(1)。実際に大きな被害を受けた事例も存在する(**表1**)。

表1．制御系システムへのサイバー攻撃事例

年	業界／分野	概要
2015	電力	ウクライナ国内の電力施設でのマルウエア感染。首都キーウ北部とその周辺地域で停電が発生した。手動運用に切り替えて，30分以内に電力供給が再開され，約1時間15分後に完全に復電した。
2018	製造（半導体）	台湾の世界的半導体チップメーカーでのランサムウエア感染。重要なコンピュータがWannaCryの亜種に感染し，複数の工場で生産ラインが停止した。影響の大きかった工場では生産再開に約3日かかった。
2022	製造（自動車）	日本の自動車メーカーに自動車の内外装部品を生産する企業でマルウエア被害が発生。これがきっかけで，自動車メーカーの14工場28ラインが停止。約13,000台の生産が見送られることになった。

また，これまで独立したネットワーク内で運用されていることで一定の安全を確保してきた制御システムは，近年のIoT(Internet of Things)及びDX(Digital Transformation)の推進によってITシステムやクラウドへ接続されるようになることで，サイバー攻撃を受けるリスクが高まっている。そのため，制御システムの稼働維持を守りつつDXを推進するには，“つながる”ことによる新たな脅威への対応として，制御系(OT)へのセキュリティー対策導入が必要になる。

企業のセキュリティー対策は，情報系(IT)への対策は普及しつつある。一方で，ITネットワークにつながるOT環境への対策は，その規模や特性によって異なる技術課題があるため，セキュリティー対策が普及していない。

例えば，製造業の多くは工場内に設備を追加導入していく中でネットワーク構成が複雑になり，配線やIP(Internet Protocol)アドレスの変更が必要な境界分離等のセキュリティー対策が難しくなっている。また，保護対象のOT機器は，生産稼働を止められない，又は制御装置に対するサポートOSが更新されないためにOS更新やパッチ適用が行いにくく，サポート切れの古いOSのまま使用されているなど，機器本体への対策が施せない場合もある。

ほかにもOT環境ではIT環境と比べて資産，通信，セキュリティー対策状況などが把握されていない，またOT環境への対策製品導入後もインシデント発生後どのように対処すべきか現場では分からないなど運用面での課題もある。

こうした背景を受けて，当社ではアセスメント・コンサルティングから，ネットワーク・エンドポイントなどへの対策導入，運用保守までをワンストップで提供するOTセキュリティーソリューションサービスを提供している。

当社ではFA，電力，公共設備向けの制御システムの導入，運用・保守を行っている一方，自社の製品，工場，ITシステムへのセキュリティー対策として，製品・サービスのセキュリティー品質に対応する社内体制であるPSIRT(Product Security Incident Response Team)，情報セキュリティーインシデントに対する監視及び発生時に対応する組織であるCSIRT(Computer Security Incident Response Team)を構築するなど取組みを進めている。こうしたIT，OTそれぞれの技術，知見を活用し，このソリューションサービスを提供する。

本稿では，当社が提供するOTネットワークセキュリティー対策製品からMELWALL[2]についてその特長を述べる(**図1**)。MELWALLはOTネットワークの内部での論理的分割(セグメンテーション)をするネットワーク装置であり，OT環境ならではの課題を意識した機能を持っている。

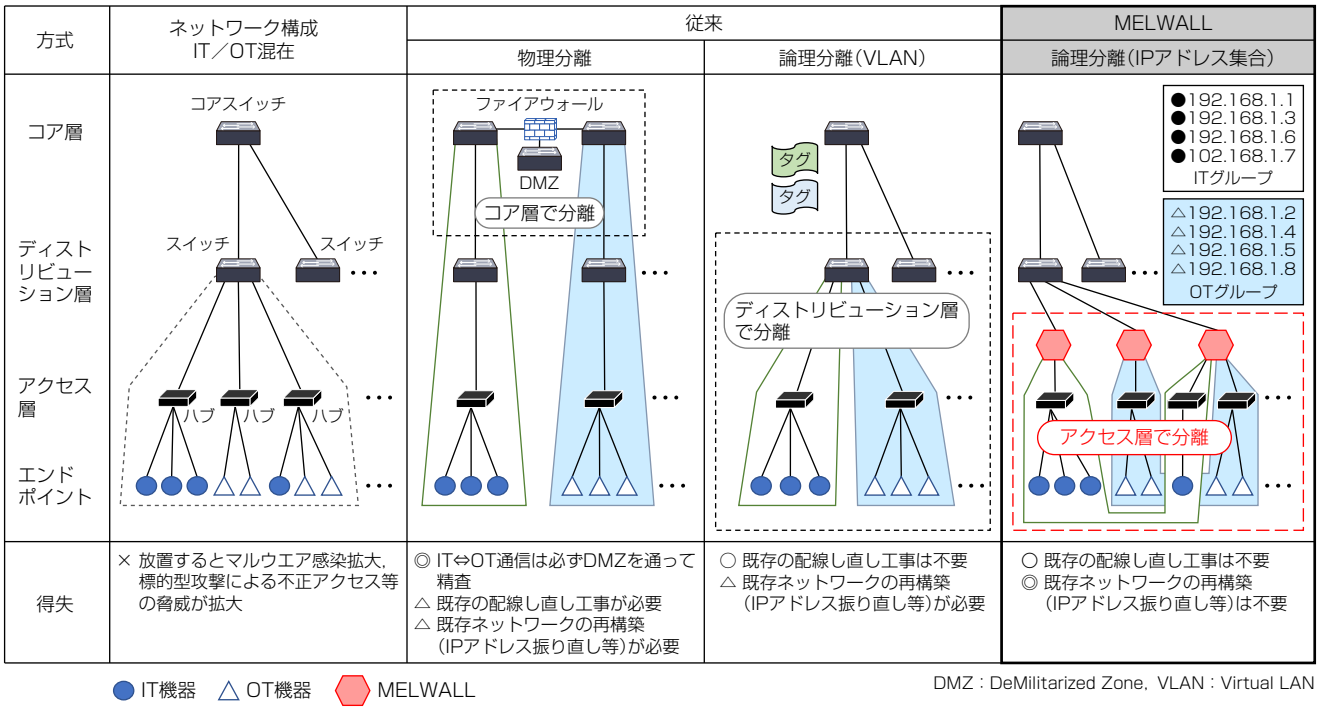


図1．MELWALLの特長

以降**2章**ではOTネットワークでの脅威対策の課題，**3章**では課題を解決するMELWALLの機能，**4章**では導入による効果を実装例とともに述べる。

2．OTネットワークでの脅威対策の課題

OTネットワークへの効果的なセキュリティー対策の一つとして，ネットワークのセグメンテーションが挙げられる。セグメンテーションとは，ネットワークをより小さな個別のネットワークに分割することであり，セグメントごとに固有の通信ポリシーなどを設定することによって，ネットワーク全体のセキュリティーレベルを上げることができる。

セグメンテーションの大きなメリットの一つは，サイバー攻撃を受けた際の被害を局所的に抑えられる可能性があることである。分割されていないフラットなネットワークでは，攻撃者に侵入された場合にネットワーク内のあらゆるIT／OT機器にアクセス可能になり，ネットワーク全体へのウイルス感染，重要な生産データの窃取や生産プログラムの改ざんなど，被害が拡大するおそれがある。また被害の拡大状況を把握することが困難であり，対応に遅れが生じてしまう。

セグメンテーションによって分割されたネットワーク間で不正な通信を遮断するような通信ポリシーが設定されていれば，攻撃者に侵入された場合でも他のセグメントへアクセスできず，一つのセグメントという小さな範囲で被害を抑えられる可能性がある。また被害拡大状況もセグメント単位で判断できる。

セグメンテーションの実施方法としては，ファイアウォールを境界点に設置し，適切な通信だけを通して，不適切な通信は通さないように通信ポリシーを設定する方法が一般的である。しかし，ファイアウォールをOTネットワークに導入する際には次の三つの課題がある。

⑴　ネットワーク構成変更(IPアドレス変更など)が必要

ファイアウォールでのセグメンテーションの場合，VLANを構築する場合が多く，ネットワークに接続するOT機器に対して設定変更作業(IPアドレスの振り直しなど)が必要になり，コストがかかるほか，機器の稼働停止を伴うリスクがある。

⑵　通信制御の設定・運用に膨大な負荷がかかる

従来のファイアウォールでは，IPアドレスベースでポリシー設定をするものが多く，導入時や設定変更時に作業負荷が大きくなる。また，設定者に十分な知識やスキルがないと設定ミスが生じてしまう可能性が高い。

⑶　OT環境内に存在する機器を把握しきれていない

これはIoT機器などの導入を進めている企業に多く見受けられるが，OT環境にある機器を把握しきれておらず，セグメンテーション実施のための十分な情報がないため導入が難しいといった課題がある。

当社では，これらOT環境特有の課題を解決するOTネットワークセキュリティー機器MELWALLを開発している。

3．MELWALLの特長

MELWALLはOTセキュリティーソリューションで提供される製品の一つであり，OTネットワークのセグメンテーションを実現する。MELWALLは**２章**に示す課題を解決する特長的な機能を備えており，特許権も取得(特許第7086257号，特許第7209791号，特許第7209792号)している。また直感的に操作できるGUI(Graphical User Interface)を充実させ，通信ポリシーの設定や運用でのユーザーの作業負荷を軽減する設計になっている。

この章ではMELWALLの特長的な機能について述べる。

3.1　グループ単位での通信制御機能

この機能は**２章**の課題⑴を解決するものである。MELWALLでは，任意のIPアドレスを任意のグループに所属させ，そのグループ間での通信制御を可能にする。そのため機器のIPアドレスを変更することなくMELWALLを導入でき，通信制御を実現できる。またグループ単位で通信の許可／拒否を設定するため，IPアドレス単位でポリシー設定をするよりもポリシー数が膨大になりにくく，設定や管理の作業負荷を軽減する。

3.2　グループ単位でのポリシー設定方式

この機能は**２章**の課題⑵を解決するものである。MELWALLはグループ単位の通信制御を設定するためのGUIに大きな特長を持つ。**図２**に示すポリシー設定画面では，送信元／送信先グループやプロトコル，ポート番号，通信の許可／拒否，ログ取得の有無などが簡単なボタン操作で指定できる。また，グループ単位でのポリシー作成であることからポリシー数が膨大になることなく，導入・運用時にユーザーの作業負荷を軽減できる設計になっている。

図２．MELWALLのポリシー設定画面

3.3　未登録のエンドポイントの検知・グループ分け

この機能は**２章**の課題⑶を解決するものである。MELWALLは自身と同一のネットワーク内に存在する機器を検知す

る機能を持っている。検知した機器がMELWALLに登録されていないIPアドレスを持つ場合，一度UNKNOWN(未分類)グループとして未分類エンドポイント画面に一覧表示される(**図3**)。

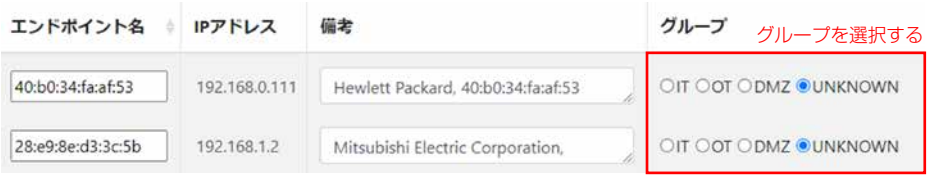


図3．MELWALLの未分類エンドポイント一覧画面

未分類エンドポイント一覧画面ではIPアドレス，MAC(Media Access Control)アドレス，メーカー名などが表示されており，ユーザーがエンドポイントの特定をしやすいようになっている。ユーザーはこれらの情報から，エンドポイントを適切なグループに分類する。またこれらの情報の横にはエンドポイントのグループが表示されており，簡単なボタン操作でエンドポイントのグループ分けを実施できる。

4．MELWALLの導入効果

この章では，**3章**で述べたMELWALLの機能を踏まえて，MELWALLをOT環境に導入した際の効果について述べる。

図4にOT環境へのMELWALL導入例を示す。**図4**左側の対策前ではOTネットワーク内はフラットな構成になっており，OTネットワーク内の機器は全て疎通可能な状態である。また，ネットワーク内には存在を把握できていないOT機器も存在する。このような状況で攻撃者にOTネットワーク内に侵入されると，被害がOTネットワーク全体に広がってしまう。

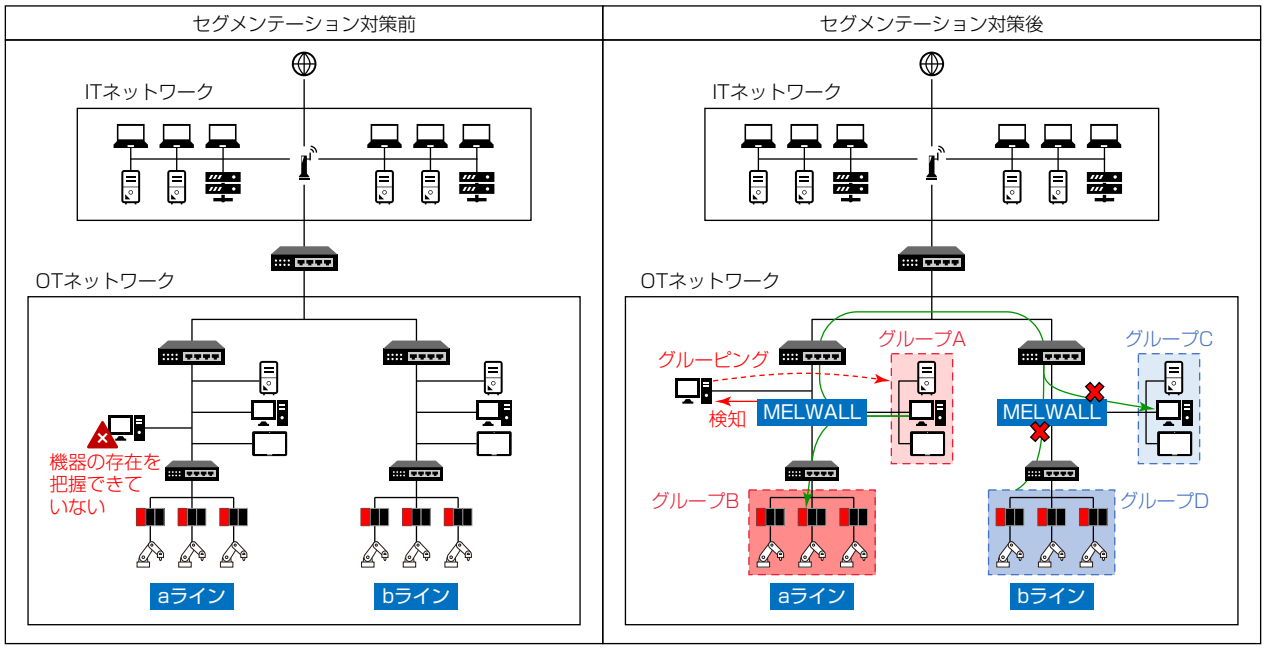


図4．OTネットワークへのMELWALL導入例

図4右側はMELWALL導入後の状態を示す。MELWALLのグループ単位でのポリシー設定機能によって，OTネットワーク内の機器をグループA～Dのようにグループ分けする。グループ単位での通信制御であるため，IPアドレスの変更や大きなネットワーク構成の変更は不要である。またMELWALLの機器検知機能によって，把握できていなかったOT機器の情報を検知し，適切なグループに所属させる作業に活用できる。これらのグルーピングは**3．3節**で述べたGUIで，直感的に設定できる。

図4右側の例では，グループを四つに分割している。これらのグループ間に適切なポリシーを設定することによってOTネットワークのセグメンテーションが実現される。例えばグループAは，グループBとは通信が許可されているが，グループC，Dとは通信が許可されていないとする。このとき，aラインのネットワークに攻撃者が侵入し，グループAに属する機器がマルウエアに感染したとしても，グループAの機器からグループC，Dへの通信が許可されていないことから，bラインへの被害拡大は抑えることができる。また，グループA，B間でも正常な通信だけを許可するような強固なポリシー設定になっていれば，被害の拡大を抑えられる可能性が高くなる。

5. むすび

OTネットワークのセグメンテーションをエンドポイントのグルーピングによって実現するOTネットワークセキュリティー機器MELWALLの特長について述べた。

今後もOT環境の対策導入・運用の課題を踏まえて，MELWALLの機能拡張を進めていくとともに，制御システムの安全性を高める製品・サービスを提供し続けられるよう進化し，社会に貢献していく。

参考文献

(1) 独立行政法人 情報処理推進機構：制御システムのセキュリティ
https://www.ipa.go.jp/security/controlsystem/index.html
(2) 木村敏之：サイバー攻撃から生産ラインを守る新たなネットワーク脅威対策技術，三菱電機技報，**94**，No.8，480～483（2020）

三菱電機株式会社