特集論文

安心・安全なサービスを提供するMDISの取組み

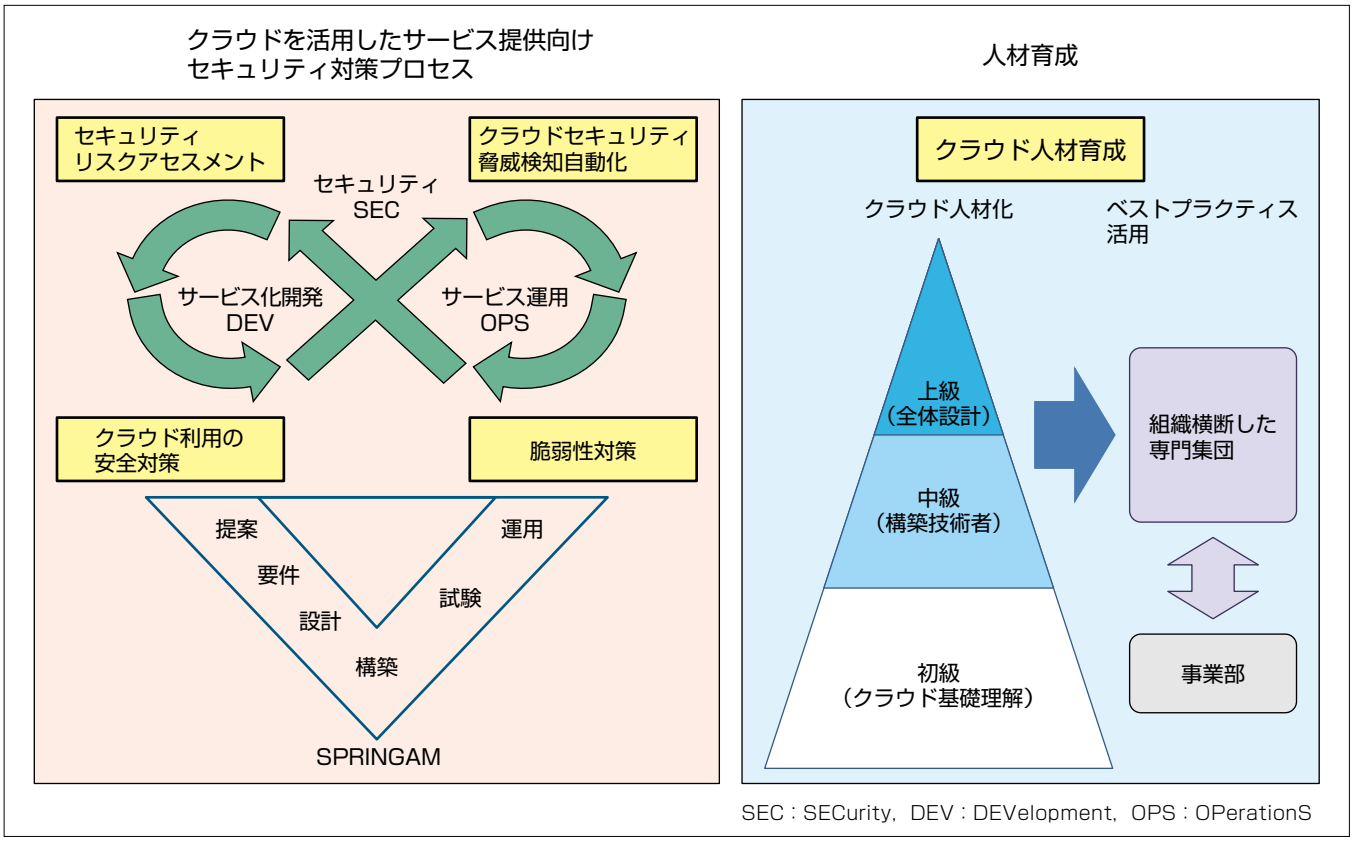
佐藤啓紀*
Hiroki Satou
近藤洋亮†
Yousuke Kondou
河野義哉*
Yoshiya Kouno
大澤伸行*
Nobuyuki Oosawa
砂田英之*
Hideyuki Sunada

MDIS's Approach to Provide Secure and Safety Service

要　旨

IT技術によって新たな価値を創造し，顧客にその価値を提供するサービス提供事業が拡大している。新たな価値の創造には，顧客の持つ多様なデータを収集して迅速に分析するための環境が必要である。多種多様な端末からのデータ収集を可能にするIoT(Internet of Things)の拡大，高速・低遅延・多数同時接続を実現する5G通信の開始，クラウドファーストやクラウドバイデフォルトの浸透によるクラウドの利活用拡大とクラウド上への情報の蓄積増加，AI(Artificial Intelligence)を活用した情報分析力の向上等，技術の進展に伴って環境整備も加速度的に進んでいる。これらの新たな価値の創造に向けた技術革新が進む中，IoT機器の脆弱(ぜいじゃく)性リスク，通信経路上でのハッキングリスク，複雑かつ巧妙化するサイバー攻撃リスク等の様々なリスクが顕在化している。このような環境で，顧客情報の搾取や改ざん，サービス提供の停止等を防止し，安心・安全に事業を継続できる安全管理対策が求められている。

三菱電機インフォメーションシステムズ㈱(MDIS)では，安心・安全なサービスを提供するための取組みとして，システム生産標準“SPRINGAM(System PRoduction and INteGrAtion Methodology)”[(1)]にセキュリティ対策プロセスを追加し，提案・計画段階からのリスクアセスメントと対策の組込みや，運用・保守段階での脆弱性情報の収集と配信による早期の脅威検知等の対策を実施している。また，クラウド利用でも，利活用技術だけでなくセキュリティ対策技術の強化や人材育成も行っている。



SEC：SECurity，DEV：DEVelopment，OPS：OPerationS

システム生産標準“SPRINGAM”へのセキュリティ対策プロセス追加の概念図

MDISでは，商談から保守までのシステムインテグレーションのライフサイクル全般を対象にしたシステム生産標準SPRINGAMを整備して品質・生産性の向上を図っている。顧客に価値を提供するサービス提供事業では，クラウドを活用したサービス提供向けセキュリティ対策プロセスを追加し，サービス運用での対策や次開発への循環を図ると同時に人材育成も行うことで，安心・安全なサービス提供を行えるようにしている。

*三菱電機インフォメーションシステムズ㈱　†三菱電機ITソリューションズ㈱

1. ま え が き

近年，IT技術の進展やクラウドの浸透に伴い，顧客の情報を様々な手段で収集・分析し，新たな価値を創造し，顧客にその価値を提供するサービス提供事業環境が整備されてきた。環境整備が進む一方，サイバー攻撃のリスクも増加しており，顧客からの情報収集・管理を安全に行い，安心・安全に事業を進めるための対策も急務である。

本稿では，MDISでの，安心・安全なサービスを提供するための取組みとして，システム生産標準SPRINGAMへの安全管理対策の追加について述べる。**2章**ではセキュリティリスクアセスメント，**3章**のクラウド利用の安全対策では提案から要件定義の段階でのリスクの洗い出しと対策，**4章**のクラウドセキュリティ脅威検知の自動化では設計段階で想定したセキュリティ上の脅威の自動検知，**5章**では脆弱性対策によって運用段階で日々更新される脆弱性への対策について述べる。最後に**6章**では，クラウド人材育成によるクラウド利活用技術の向上とクラウド特有のセキュリティ対策技術習得について述べる。

2. セキュリティリスクアセスメント

セキュリティリスクアセスメントとは，システム仕様を基に対象システムに存在する脅威を洗い出し，そのインパクトを評価して対策を決めることで脅威を無効化する活動のことを言う(**図1**)。従来，この脅威を洗い出す作業はセキュリティ専門家が手動でシステム仕様と脅威データベースを照合し，脅威の該当／非該当の判定を行っていたため，①作業に時間が掛かる(1～2か月)，②属人性がある，③品質が不安定などの課題があった。

これらの課題に対し，Microsoft社はTMT(Threat Modeling Tool)という分析ツールを提供し，DFD(Data Flow Diagram)形式でシステム構成図を入力することで，自動的に脅威を抽出できるようにしたが，TMTが持つ脅威データベースの内容が不十分なために抽出される脅威一覧の網羅度が低く，実用的ではなかった。そこで，MDISでは，三菱電機情報技術総合研究所とともに，TMTの脅威データベースのカスタマイズ開発(脅威一覧及び判定ルールの追加)に取り組み，実システムを対象にした専門家による手動分析の結果と，開発成果による自動分析の結果の比較評価を行った。

評価の結果，この開発成果を用いることでセキュリティ専門家が1～2か月間要していた“脅威の洗い出し”と同等品質の分析が，一般の技術者でも2～3日間で実施できることが確認できた。

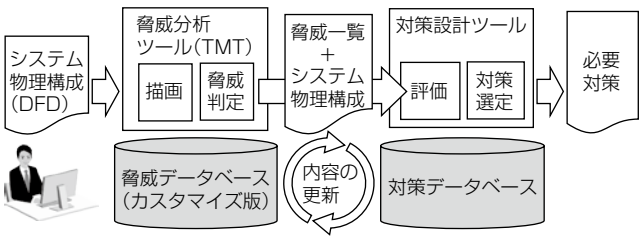


図1．セキュリティリスクアセスメント

3. クラウド利用の安全対策

顧客にクラウドサービスを提供する事業では，サービス自体をMDISで開発・運用することに加えて，他社のクラウドサービスを利用・組み合わせる機会が増えている。MDISでは三菱電機グループ外の他社が提供するクラウドサービスについて，MDISがサービスの契約者の場合には，安全点検結果を社内で確認し，顧客への見積提示・契約締結を行うフローを取り入れている(**図2**)。

2013年に経済産業省のクラウドセキュリティガイドラインが公示されたことを契機に，国内の各企業はクラウドを利用する際に安全点検を行うようになってきている。三菱電機及びMDISでは経済産業省のガイドラインを基にクラウドサービスの利用ガイドラインを策定した。さらにクラウドサービス利用を進めていく中で個人情報や機密情報の扱いに対してMDIS独自の点検項目を付加して安全対策の運用を強化している。

他社のクラウドサービスの選定時に行う安全点検では大きく二つの観点で点検を行う。一つはサービス提供事業者を対象にした点検であり，もう一つはサービスの利用者を対象にした点検である。

サービス提供事業者に対する点検では，情報セキュリ

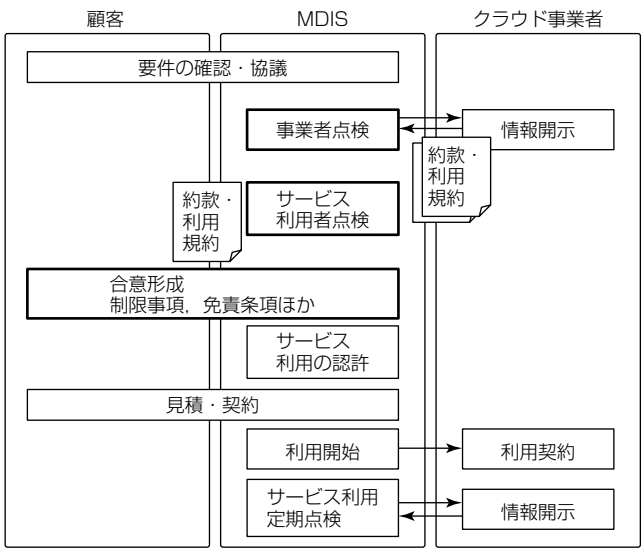


図2．クラウド利用の安全対策の流れ

ティマネジメントシステムであるISMS(Information Security Management System)(ISO/IEC 27001，27017，27018)認証の取得状況，内部統制保証報告SOC2(Service Organization Controls 2)への対応状況を確認した上で，事業者に当該サービスの運営や組織的なリスク対策の状況を可能な範囲で開示を求める。また，提供されるサービスの約款や利用規約を理解し，想定する利用要件とのギャップを明確にして，必要な対策案を検討した上で，リスクが低いと判断できる事業者を選定している。

サービス利用者に着目した点検では，サービス利用に伴うセキュリティのリスクや運用に関わる情報の取扱い等について，対応すべき事項を明確にして後続のサービス構築・運用プロセスへのインプットにしていく。例えば，不特定多数がアクセスできるサービスであれば多要素認証の運用や接続元のネットワーク情報での制限を設ける等の対策を講じる。また，万一問題が発生した場合に被害を局所化させるために，ネットワーク分離や隔離環境からの利用等，対策の方針をこの段階で定めていく。さらに，個人情報の取扱い有無，顧客機密情報の取扱いへの考慮，輸出管理に関する事項など，関連法令の遵守と関連する規定の手続も徹底している。

安全点検を実施後，点検結果に基づきMDISからクラウドサービス提供をする顧客に対して制限事項などを詳細に説明し，見積条件や契約での免責事項を明確にする。実際にサービス利用を開始する際には各事業部門でサービス利用状況を管理し，サービスの継続利用，更には利用終了した後の対応までを対象範囲にするプロセスを確立しているので，安心・安全にクラウドサービスを利用できる。

4．クラウドセキュリティ脅威検知の自動化

AWS(Amazon Web Services)(注1)，Microsoft Azure(注2)等のクラウドサービスは，ISMSやSOC2等の認証に適応し，物理マシンやハイパーバイザー等のインフラ部分については高い水準のセキュリティ対策を実施している。また，セキュリティ関連サービスについても日々機能追加・改良が続けられている。一方で各サービスはAWSの“責任共有モデル”と呼ばれる責任分界を設けており，OS内部や保管データなど利用者が操作する部分のセキュリティ責任は利用者側に委ねられる。そのため利用者の責任範囲で，設定の不備が起因すると推察される“乗っ取り”事故が発生している。また，情報の流出やサイバー攻撃に長期間又は自発的に気づくことができない事例も存在する。もはやクラウドサービスでは，“そのサービスは安全か”よりも“利用者はそのサービスを安全に使用できるか，問題発生時に適切に対応できるか”が問われていることを表している。利用者の責任として必要な対策は多岐にわたるが，クラウド上での問題発生を人手でリアルタイムに発見することは困難であり，問題を自動で検知し，迅速かつ適切に対策を可能にするためクラウドセキュリティ脅威検知の自動化が重要になる。

MDISでは，AWSで誤った公開設定や攻撃発生等を検知するセキュリティ点検ツール群を開発し，クラウドセキュリティ対策を自動化している(**表１**)。その内で“不審操作点検”のツールは，**図３**に示すようにAWSで提供される複数のサービスを組み合わせることで不審な操作を検知する。

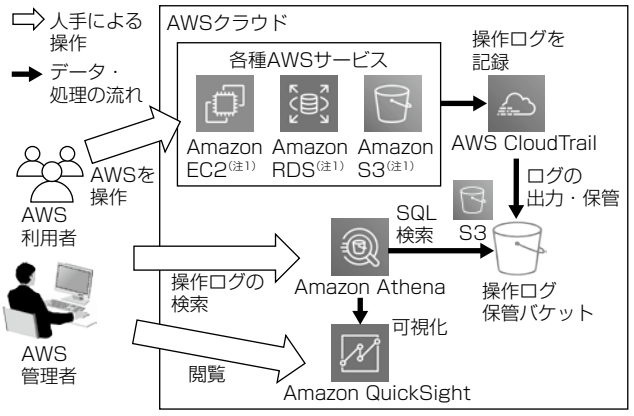
セキュリティ点検ツールは，AWS上での問題を自動検知し，原因分析に必要なログ等の収集を可能にする。AWS提供のセキュリティ機能を組み合わせ，クラウドサービスの機能拡張や新たな脅威の出現に応じて追加・拡張することも容易になっている。

CIS(Center for Internet Security)ベンチマーク等を使った基本的なセキュリティ点検機能は各社も提供しているが，MDISでは影響度の高い脅威に対する点検機能を優先的に提供している。今後も最新の脅威分析を基に必要なセキュリティ対策項目を拡充して，クラウドセキュリティ対策自動化によって，持続的にクラウドサービスの安全性を確保できる。

(注１)　AWS，Amazon EC2，Amazon RDS，Amazon S3は，Amazon Technologies, Inc.の商標である。
(注２)　Azureは，Microsoft Corp.の登録商標である。

表１．セキュリティ点検ツール

ツール	概要
課金点検	課金額が急激に増大していないか点検するための可視化ツール
不審操作点検	不審な時刻・回数の操作が無いか点検するための可視化ツール
公開点検	インターネットに公開された仮想マシン、ストレージは無いかを自動点検するツール
攻撃点検	アカウントに攻撃や不審なふるまいが無いかを自動点検するツール
消し忘れ点検	意図せず起動したままになった仮想マシンはないか自動点検するツール



EC2：Elastic Compute Cloud，RDS：Relational Database Service，S3：Simple Storage Service，SQL：Stuctured Query Language

図３．不審操作点検ツールの動作イメージ

5. 脆弱性対策

安心・安全なサービス提供を実現するには，日々発生するセキュリティリスクを早期に検知し，その深刻度や影響範囲を速やかに分析した上で，対策を講じる必要がある。MDISでは，“脆弱性対策支援デスク(2)”によって，JVN(Japan Vulnerability Notes：JPCERTコーディネーションセンターと独立行政法人情報処理推進機構(IPA)が共同で運営)データベースから脆弱性情報を日次で収集し，顧客システムやMDISサービス提供システムで対象になる脆弱性情報をあらかじめ登録したシステム構成管理の情報と連携させ，当該システムに必要な脆弱性情報をほぼ自動で抽出し，影響確認，原因確認，対策検討と脆弱性に関する情報を一元管理している(**図４**)。さらに，製品名に加えバージョン名やアップデート番号等までを絞り込み対象にすることで，ピンポイントに情報を自動抽出する工夫を加えている。このため，顧客担当システムエンジニアや自社サービス提供の運用部隊が，発生した脆弱性情報を個別に調査する手間を削減でき，脆弱発生から具体的な対策実施までを速やかに行うことができ，安心・安全なサービス提供を実現している。

6. クラウド人材育成

クラウドを安心・安全に利用するためには脆弱性・ハッキングといったサイバー攻撃のリスクを考慮することが必要である。また，クラウドは日々進化し続けるものであり，安心・安全に利用するために，人材育成も継続的に行うことが重要である。そのため，次のようにレベルを定義し，人材育成を実施している(**図５**)。

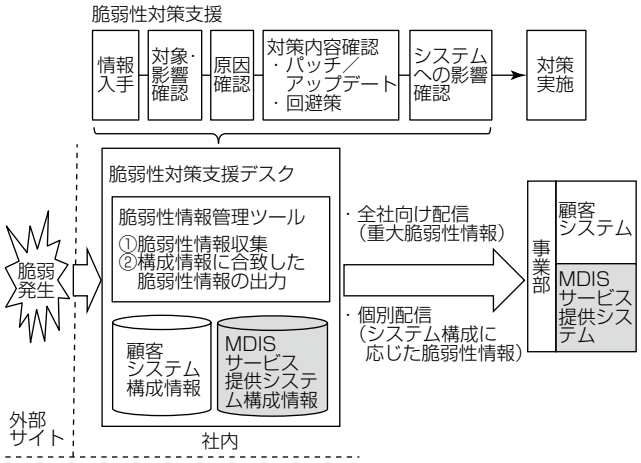


図４．脆弱性対策支援デスク

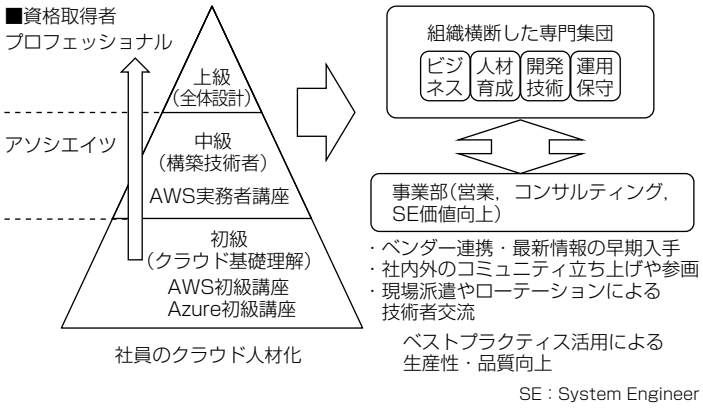


図５．クラウド人材育成

(1) クラウド人材育成の階層別施策

顧客への提案や社内検討等，必要最低限のクラウドの知識を身に付けるための初級講座，クラウドを実際に利用しサービスを組み合わせてシステムを構築・運用し，セキュリティ対策も自身で行えるための中級講座，及びクラウドの最新技術を熟知し，システム設計から構築までの全体設計を自身で行えるための上級講座を設け，認定資格取得までをフォローし，継続的な人材育成を進めている。

(2) コミュニティ活動を通じた情報共有と相互研鑽(けんさん)

社内ではクラウドに関してのコミュニティ活動を通じて組織を横断した活動を行っている。クラウドに関する情報ポータルを開設，実案件などで取得したベストプラクティスなどの情報を社内共有している。

これらの活動を継続的に行い，クラウドを安全に利用するための技術者育成を行っている。

7. む　す　び

MDISでの安心・安全なサービスを提供するための取組みとして，システム生産標準SPRINGAMへのセキュリティ対策について述べた。今後もIT技術の進展に伴い，新しい価値の創造とその価値を提供するサービス提供事業の多様化が予測される。顧客の情報を安全に収集・管理し，安心なサービスを提供できるための事業環境整備のため，最新技術を活用したサービス提供基盤の整備とセキュリティリスクを低減する対策を継続していく。

参 考 文 献

(1) 藤原良一，ほか：プロセス改善による高品質ITソリューションの提供に向けたCMMIレベル５達成への軌跡，三菱電機技報，**80**，No.9，593～598 (2006)
(2) 山足光義，ほか：快適・安心・発展を提供するITソリューション開発運用基盤，三菱電機技報，**90**，No.8，476～480 (2016)