

共創事例から学ぶ、データを守りビジネスを加速する"セキュリティの鍵"とは

FUJITSU JOURNAL / 2018年6月22日



サイバー空間上であらゆるサービスをつなぎ、新たなイノベーションを生み出していく現代。ビジネスのデジタル化が加速する中、新規ビジネス創出を支える攻めのセキュリティが不可欠です。また自社の強みを生かすだけでなく、自社にはない専門性を持ったパートナーとの連携も欠かせません。データを守り、ビジネスを止めずに加速させていくシステムを実現する鍵とは何でしょうか。そのヒントを探ります。

【Fujitsu Forum 2018 カンファレンスレポート】

本カンファレンスでは、冒頭、富士通サイバーセキュリティ事業戦略本部 本部長 飯島淳一が、加速するデジタルトランスフォーメーションを背景に、新規サービス開発時におけるセキュリティ確保の重要性についてお伝えしました。続いて、TKCシステム開発研究所取締役副所長の魚谷 仁

司氏、セコムトラストシステムズ取締役常務執行役員の藤川 春久氏、みずほフィナンシャルグループ IT・システム企画部長の高橋 達浩氏の順にビジネス変革に取り組む先進企業3社が、それぞれのCo-creationの取り組みを紹介しました。

現場やデータ利活用に携わる人々も巻き込んだセキュリティ対策を



富士通株式会社
サイバーセキュリティ事業戦略本部 本部長
飯島 淳一

最近、多くのお客様の声を伺って感じるのは、セキュリティに対する取り組みが変化していることです。リスクの最小化や対策の有効性評価、自力ではまかなえない部分のアウトソース、コンプライアンス対応といった観点に加え、最近では、お客様の新商品やサービスを支えるセキュリティを求める声が増えています。ビジネスの観点で言えば「守りのセキュリティ」だけでなく「攻めのセキュリティ」が求められているということです。

今や、デジタル化の加速によって、ハードウェアという製品だけでなく、サービスモデル、それにセキュリティという3つの要素が渾然一体となって新しい商品やサービスが生まれています。それを踏まえると、サイバー空間の中でサービスがつながり、データが価値を持つようになった今、脅威からICTを守り、データの正しい流れを担保することが不可欠なのです。

そのためには、CIOやCISOだけでなく、現場やデータ利活用を考える部門の人々もセキュリティについて考えなければなりません。商品開発の早い段階から、UX（ユーザーエクスペリエンス）も考慮しつつ、セキュリティの考え方やデータ保護の仕掛けをあらかじめ組み込んでいくことが肝要です。

会計事務所やパートナーを支援、「自利利他」でセキュリティに取り組むTKC



株式会社TKC
取締役執行役員
システム開発研究所 副所長
兼 技術研究・開発支援センター長
魚谷 仁司氏

TKCは、全国の税理士や公認会計士、ひいてはその顧客である法人・組織を支援してきました。日本の会計事務所の約3分の1がTKCに所属しており、法人税申告件数の4.6社に1社で同社の仕組みが使われています。そして、法人会計業務のすべてを網羅すべく、財務から販売管理、給与に至るまでさまざまなシステムやサービスを開発しています。サイバー空間上にビジネスを構築しているTKCにとって、セキュリティは生命線であり、必須条件です。

そのため、TKCでは様々な取り組みを実施してきました。例えば、TKC全国会に所属する全国の会員事務所をセキュアな通信網で結び、自社でデータセンター（TKC Internet Service Center）を構築、運営することで、会員事務所様や、その関与先企業様に、24時間365日、安心・安全・便利なクラウドサービスを提供しています。

1. セキュリティインフラの共有

(1)TISC (TKC Internet Service Center)



TKCでは、当社のお客さまである会計事務所とその関与先企業、地方公共団体、中堅・大企業に、安全かつ安心してTKCシステムをご利用いただけるよう「TKCインターネット・サービスセンター（TISC）」を運営しています。その最大の特長は、世界最高水準の情報セキュリティ対策や災害に強い堅牢な建物といったインフラ面に加え、当社社員が24時間365日、サービスの稼働状況を監視するなど運用面でも万全のサービス体制をとっていることです。このTISCを拠点として、各種アプリケーションやアウトソーシングなどのサービスを組み合わせ、“安全・安心・便利”なクラウドサービスを提供し、お客さまの事業活動を支援します。



クラウド事業者のための
個人情報管理のベストプラクティス

ISO/IEC 27018の
認証を取得！ (H27.10.12取得)

TISCのクラウドサービスでお預かりする個人情報の増加に伴い、この度、パブリッククラウドにおける個人情報の保護に特化した国際規格「ISO/IEC 27018」の認証を新たに取得しました。

「ISO/IEC 27018」は、クラウドサービス提供事業者がお客さまからお預かりする個人情報について、厳格に運用・管理されていることを第三者機関が客観的に証明するものです。

「ISO/IEC 27018」の認証を、正式な審査機関による審査を経て取得した企業は、国内では初、世界でも3社目となります。

アウトソーシング受託企業としてのTKCの取り組み

当社は、お客さまが業務を委託される際に客観的な評価ができるよう、ISOなどの標準規格の認証を取得しています。

- ISO/IEC 27001(ISMS)
- ISO/IEC 27018 **NEW**
- 86号監査:受託業務に係る内部統制の評価
- LGWAN-ASPサービス接続登録事業者
- eLTAXベンダ認定/ eLTAX認定委託先事業者

©TKC 2018

TKCの会員である会計事務所には小規模な事業者が多く、機密性の高い情報を扱う一方で、高度なセキュリティ対策を実現しようとするコスト負担が大きすぎます。そこで、次世代ファイアウォール製品など高度なセキュリティ製品やインフラの共有、ウイルス対策製品の無償配布、エンドポイントセキュリティサービスを提供するなど、会計事務所のセキュリティ強化を支援する取り組みも長年にわたって続けてきました。その一環として、富士通の資産管理ソリューション「[IT Policy N@vi](#)」を利用しています。『管理されている』のではなく、『守られている』という安心感を与えられるソフトウェアだと評価しています。さらに、国税関係書類のスキャナ保存制度に対応した証憑ストレージサービスのために自社でタイムスタンプ局を開設、無償で

「SkyPDF」を提供し、個々の会計事務所が安価に利用できるようにしています。

最近では「銀行信販データ受信機能」や「TKCモニタリング情報サービス」といった、FinTechを生かした新たなサービスも、万全のセキュリティ体制のもとで開始しています。こうした新たな付加価値を産むサービスを進める中で、いかに上流工程でセキュリティの仕組みを取り入れることが大切であるかを感じています。

このようなサービスはさまざまなパートナーとつながらなければ実現できませんし、セキュリティは1社だけで確保できるものではないことも痛感しています。TKCの社是である「自利利他」を実践し、他の利益を考えてこそセキュリティは確保できると考えています。今後もCo-creationの概念を重視してサービスの提供に取り組んでいきます。

「本人認証プラットフォーム」の提供を通じて「共想」に取り組むセコム



セコムトラストシステムズ株式会社
取締役 常務執行役員
藤川 春久氏

セコムトラストシステムズは2000年ごろから、物理的な対策も施した電子認証局を構築し、PKI技術を用いた証明書発行サービス「[セコム認証サービス](#)」を展開してきました。堅牢な鍵管理システムを構築し、土業様向け証明書やEV-SSL証明書の発行、電子署名やタイムスタンプサービスなどを提供しており、さらに地方公共団体組織認証基盤（LGPKI）の認証局構築に向けた準備を進めています。その一環で、業界団体の「CA Browser Forum」に参加し、SSL/TLSといったセキュリティ標準をブラウザでどう扱うべきかの議論にも加わってきました。

- 新たな技術(生体認証、ブロックチェーン等)の導入で、利用者の**安全性**と**利便性**を向上
- 安全な認証基盤と身元確認で、提供者の構築および運用**コスト**を削減



Copyright © 2018 SECOM CO.,LTD. All right reserved.

2015年以降、私たちが最も力を入れているのが、新しい本人認証プラットフォームの開発です。銀行やショッピングなどいろいろなオンラインサービスが登場した結果、私自身、数えてみると実に50個くらいのIDとパスワードを使っています。この管理は大きな負担です。数種類のパスワードを使い回している人も多いと思いますが、これはセキュリティ上危険性があります。一方、サービスを提供する側にとっては、新たなサービスを作るたびに、認証システムや個人情報を管理する仕組みを作ることになり、コストがかさんでいます。

そこで、安全性を確保しながらユーザーの利便性を高め、「できればIDとパスワードをなくしてしまう」ことを目的に開発を進めているのが本人認証プラットフォームです。事業者にとっても、こうした共通のプラットフォームを利用することで、コストを大幅に下げることができます。本人認証は事業者が競争する領域ではなく、コストになっているため、セコムトラストシステムズがそこを肩代わりしていきたいと考えています。

今後、本人認証プラットフォームでは、スマートフォンが対応している生体認証を活用する他、複数の異なるサービスにまたがるシングルサインオンやオンラインでのスピーディな身元確認などを実現していく計画です。先日発足した「証券コンソーシアム」でも、本人認証プラットフォームを用いた新たなサービスをリリースする予定です。この共想に興味を持たれる方がいれば、ぜひ一緒にいいサービスを作っていけたらと思います。

生き残るためにCo-creationを通じて新たな価値作りに取り組む、みずほフィナンシャルグループ



株式会社みずほフィナンシャルグループ
IT・システム企画部長
高橋 達浩氏

金融業界は、金融ビッグバン、リーマンショックを経て、テクノロジーの進化を踏まえた新しい金融のあり方を模索する時代にさしかかっています。そこで、鍵を握るのがFinTechです。みずほフィナンシャルグループでは、この最新技術を活用することで、ビジネス拡大に向け、踏み込んだ取り組みを進めています。

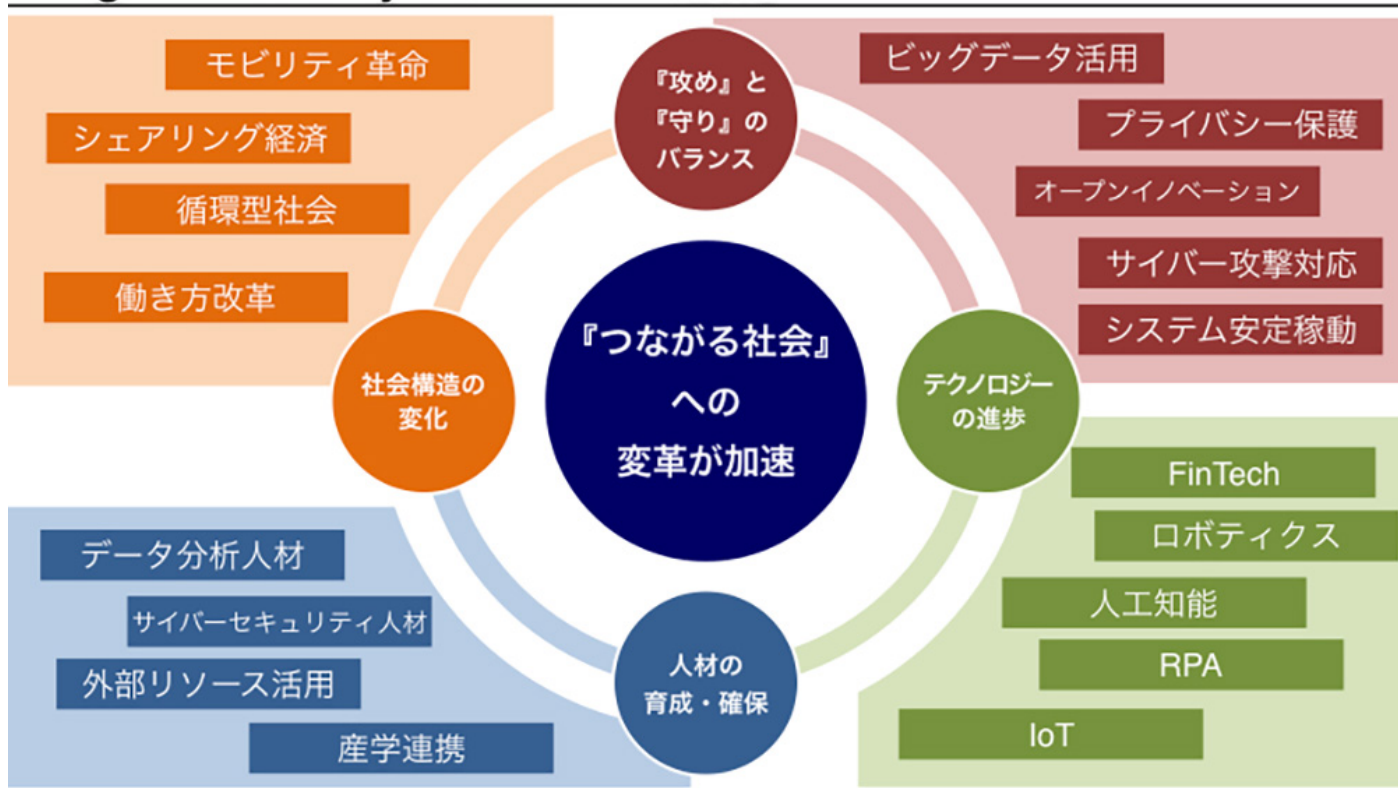
具体的な活用事例としては、融資を申し込まれたお客様への貸し出し条件をスピーディに決定する日本初のFinTech サービス「AIスコア・レンディング (J.Score)」を2017年9月より開始。また、FinTechやIoTを活用した新たな事業領域を創出するための「Blue Lab」というインキュベーターカンパニーを2017年7月に設立。金融業の枠組みに限定せず、あらゆる産業・業種に視野を広げ、次世代のビジネスモデルを創造しています。さらに、2016年3月、富士通と共同で、ブロックチェーン技術を活用した国際証券決済の実証実験を行い、関係者の間で取引情報を共有、処理することで決済に要する時間を3日から即日短縮できることを実証しました。

FinTechを活用することで、今後弊社のビジネスがどれだけ伸びるかは、経営資源であるデジタル空間のデータの「マネジメント」と「人材の育成」にかかってくるものと考えています。その意味で、セキュリティはデジタル空間への「入場券」であり、デジタルトランスフォーメーションを進める上での必須要件です。

データマネジメントで重要なことは、新規商品やサービス開発の際、「セキュリティ・バイ・デザイン」の視点で、要件定義や設計段階からセキュリティを組み込むことです。また、デジタル

空間の活動、つまりログを収集、可視化し、データとして利活用できるようVisibility（ビジビリティ）を実現することも大事です。データをしっかり管理し守りながら、新しいビジネスのスピードも落とさないことが肝要です。

Digital × Security これからの『進化』



このような「守り」と「攻め」の両面でデータをマネジメントするために必要なのが、「人材の育成と確保」です。サイバーセキュリティの専門人材は、国内外で不足しており、自社での採用や育成だけでは限界があります。そこで、みずほフィナンシャルグループ全体で実戦経験を積む「サイバー道場」を実施。サイバー攻撃への対応スキルの向上と隠れた人材の発掘につなげていきます。

以上のように、ビジネスのデジタル化が進む中、攻めと守りのバランスをとりながら新たなサービスを開発していくには、共創の精神と人員の育成が鍵となります。そして、デジタルテクノロジーとセキュリティの進化による安心・安全なインフラが、今後ますます必要不可欠になっていくと考えています。

あらゆる領域にまたがりワンストップでサイバーセキュリティを提供

最後に再び飯島が登壇し、カンファレンスを次のように締めくくりました。

3社様にそれぞれの取り組みをご紹介いただきましたが、共通していたことが2つあると思います。1つは共創、Co-creationの重要性。もう1つは、社会構造の変化に対し、「人材」と「テクノロジー」と「セキュリティ」の三本柱で立ち向かう構図です。

デジタル空間上でビジネスを推進していく上でセキュリティは必須であり、情報システム部門だけでなく現場の各部門も一緒に取り組んでいく必要があります。さらに、自社内外の関係者を巻き込んでエコシステムを形成し、Co-creationを進めていくことが重要です。

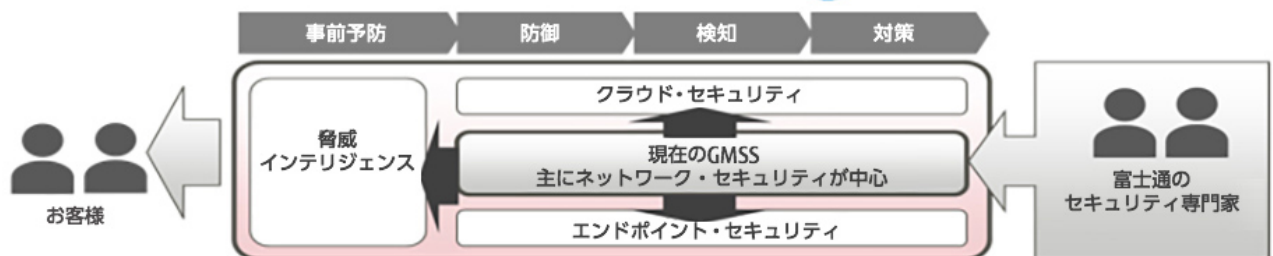
富士通ではこのサイバーセキュリティ分野に対し、アセスメント・コンサルティング、テクノロジー、インテグレーション、オペレーションという4つの領域でサービスを提供してきました。個々の領域を単品で提供するのではなく、富士通グループの力やパートナーシップを活用し、その間をつなげるプロセスや検証を通した品質確保、情報共有といったものも含め、ワンストップで提供していきます。

さらに富士通は5月9日、[マネージドセキュリティサービスの機能強化を発表](#)しました。

マネージド・セキュリティサービスの強化 (5/9プレス発表)



- ・ サービスの対象領域をエンドポイントやクラウドに拡大
- ・ プロアクティブな対策を組み込むための脅威インテリジェンス活用



- ・ 「GMSSエクスプレス・サービス」の販売開始
 - ・ 主にSMBマーケット向けに典型的な要件を事前に組み込み済
 - ・ これにより、平均的な導入を最大1/3に短縮

Copyright 2018 FUJITSU LIMITED

これまで主にサービスを提供してきたネットワーク領域に加え、パートナーシップを活用し、クラウドやエンドポイント領域にも対象拡大しています。同時に、プロアクティブな予防対策のために、脅威インテリジェンス情報を活用してサービス全体を強化します。これを、世界計11拠点のセキュリティオペレーションセンターを通し、グローバルなパートナーとのアライアンスも活用しながら展開し、今後もセキュリティに裏打ちされた価値創造を支援していきます。



登壇者



株式会社TKC
システム開発研究所 副所長
取締役執行役員
魚谷 仁司 氏



セコムトラストシステムズ株式会社
取締役 常務執行役員
藤川 春久 氏



株式会社みずほフィナンシャルグループ
IT・システム企画部長
高橋 達浩 氏



富士通株式会社
サイバーセキュリティ事業戦略本部 本部長
飯島 淳一