salesforce app cloud

# Salesforce Shield

## IoT時代を勝ち進むためのセキュリティ戦略

# 膨大なデータを取り扱うIoT時代には セキュリティが経営戦略の鍵になる。

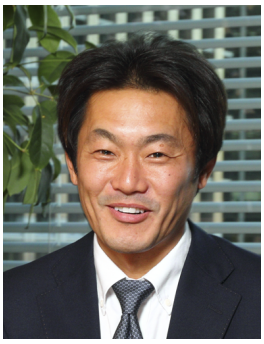
パソコンやモバイル端末だけでなく、モノやセンサーまでがインターネットにつながるIoT時代。
膨大なデータが収集され、価値ある情報を狙ったサイバー攻撃の脅威も飛躍的に高まる中で、企業のリスクマネジメントがますます重要性を増しています。

そこで、セキュリティ・コンサルティングの最前線で活躍されているPwCあらた監査法人の専門家のお二人に、これからのサイバーセキュリティに関する課題と、IoT時代のクラウド活用のポイントを伺いました。

## 綾部（あやべ） 泰二（たいじ） さん　TAIJI AYABE

PwCあらた監査法人　システム・プロセス・アシュアランス部　ディレクター
公認情報システム監査人（CISA）

製造業、情報通信業、金融業などにおけるITガバナンス、システムリスク管理態勢、情報セキュリティ管理態勢やISMSの導入を支援。セキュリティ・インシデントの再発防止策導入に対する支援実績多数。新経済連盟のサイバーテロ対策事務局に携わるなど、企業のシステムリスクへの対応や情報セキュリティに対する数多くの知見を有している。



## 饒村（じょうむら） 吉晴（よしはる） さん　YOSHIHARU JYOUMURA

PwCあらた監査法人　システム・プロセス・アシュアランス部　マネージャー

製造業や金融業を中心に、経営管理、マーケティング、情報管理、内部統制、サイバーセキュリティの分野でコンサルティングやプロジェクト管理の実績多数。マーケティング戦略や事業戦略からビジネス開発の上流分野も得意領域。近年はIoTやクラウドにともなう管理基準および管理体制の構築支援などに従事。

共著：PwCあらた監査法人編「クラウド・リスク・マネジメント」（同文舘出版）

salesforce app cloud

# IoTによるビジネスの進化と新しい業態の登場

IoTビジネスにおいては、データそのものが非常に高い経済価値を持っていきます。例えば、ある国内ベンチャー企業では、人間の排泄物から健康状態を読み取る技術を生み出していますが、こうしたバイオデータには高い経済価値が凝縮されています。

バイオデータといえば、個人のDNAに合わせて薬をカスタマイズして処方するパーソナライズド・メディスンも活用されており、ある製薬企業では、患者の投薬履歴データや保険情報などから、最適な治療プログラムを提供するトータルサービスを始めています。

また、最近では、B2Bの企業が、IoTを基盤にB2BとB2Cを結びつける"B2B2C"企業へと変貌し、部品メーカーが消費者のデータを収集し分析することで、製造メーカーに消費者動向に基づいた提案サービスを提供するようなモデルも出てきています。

さらに、全国で時間貸し駐車場を運営している企業では、駐車場の精算機を本部のサーバーと結び、稼働率や立地条件などのマーケティングデータを分析。最適な駐車料金や課金体系の設定を行うことで、地主と利用客を結びつける"B2C2C"を実現しています。B2C2Cの例では、宿泊施設を貸したい人と借りたい人をマッチングさせる新サービスを提供する民泊も代表例と言えるでしょう。

# 増え続ける膨大なデータ管理へ対応するには

このようにIoT時代における企業経営では、膨大な個人情報やマーケティングデータを収集・分析して、新しい価値を生み出す経営戦略が重要になってきます。その際に、課題となってくるのが、ビッグデータを処理するデータベースの運用にかかるコストと時間です。

この課題への対応の一環としてクラウドを選択する企業が増えているのも事実です。即ち、従来のようにハードウェアを自社で持つ場合には、今後も増え続ける情報を蓄積していくためのハードウェア更新にどれくらいのコストと時間がかかるかわからないし、耐用期間を過ぎたらリプレイスしなくてはなりません。ハードウェアのメンテナンスにずっと縛られ続けることになるのです。

そこで、ハードウェアとの面倒な付き合いから解放されるクラウド利用が重要になるわけです。クラウドならデータ量が増えても、必要な時にすぐにストレージ領域を拡大できるし、メンテナンスや更新からも解放されるので、自社の集中したいビジネス分野へリソースを振り分けられます。

ビジネスにいっそうのスピード感が求められる今、立案したビジネスモデルをいかに早く実現できるかが成否の鍵を握ります。システム構築やメンテナンスにかける時間は短ければ短いほどよいのです。その意味で、ビジネススピードが加速するほどクラウド利用も加速していくものと考えています。

salesforce app cloud

# サイバーセキュリティ対応は企業連携が重要

2015年11月に、日本政府がサイバーセキュリティに関する国際会議を沖縄で開催しました。テーマは「Cyber3」。つまり、モノがネットワークにつながる「サイバーコネクション」が広がり、それを活かすための「サイバーセキュリティ」の対応が必要となり、さらに、インターネットが国を越えた経済基盤になる中で「サイバークライム」をいかに防ぐかということ。こうした課題について、各国の政府関係者、ビジネスリーダー、研究者らが協力して、サイバー攻撃に対処していく姿勢を打ち出しました。

IoT時代のサイバーセキュリティには、今までのセキュリティの考え方と大きく異なる点があります。それは、B2B2C や B2C2C などの拡大により、企業間の情報の受け渡しが増えていく結果、1社が被害に遭うと連鎖的に被害が広がってしまうということ。現状では各社が独自に対策を練っていますが、IoT時代になると企業間で情報連携しながら対策を打っていく必要があるのです。その意味でも、クラウドというセキュアな共通基盤を活用して、一緒に強固なサイバーセキュリティ対策を打つことが効率的な選択肢と言えます。

これは戸建住宅とマンションの違いに例えるとわかりやすいでしょう。戸建住宅(オンプレミス)は自前で建物を建て、メンテナンスし、セキュリティも用意しなくてはなりませんが、マンション(クラウド)なら、インフラやセキュリティは全てプロにお任せして、専有部分だけを利用すればよいわけです。だからこそ、クオリティの高いマンションデベロッパー(クラウドベンダー)選びが大切となるのです。

# サイバーセキュリティ経営ガイドラインの順守

こうした動きを受けて、官公庁も国を挙げた枠組みを作り、企業も巻き込んだ連携に向けて活発に動いています。その一つが、経産省が2015年12月に企業経営者を対象に策定した「サイバーセキュリティ経営ガイドライン」です。

これによると、経営者は全社の情報セキュリティ対策を統括するCISO（最高情報セキュリティ責任者）を任命し、セキュリティリスクに備えて、内部統制と同等の対策を講じて情報開示を行うことを求めています。さらに、2016年度からは ISMS 認証の審査に、同ガイドラインに沿った審査項目を追加し、企業トップの「セキュリティ経営」を評価・認証する機能を加える見通しです。

この指針を順守すれば、サイバーリスク保険の割引をはじめ、万一インシデントが起きた場合の裁判上の免責につながる可能性も高くなりますから、サイバーセキュリティに対する企業経営者の意識を高めるための有効なガイドラインとなるでしょう。

# 「事後対応」ではなく「事前対策」が重要

セキュリティ対策が後手にまわり、ひとたび情報漏洩ともなると、その損害額は莫大なものになります。個人情報が漏洩した場合、多数の顧客情報を取扱う事業や、クレジットカード情報等、質的に重要な情報を取扱う業種によっては数10～数100億円規模の損失が発生しています。

損失の費目としては、

## 1 原因調査･顧客対応

社内で調査チーム、対策本部を設置するなど、多くの人的資源を投入する必要性が生じます。

## 2 法的制裁

個人情報に係る情報セキュリティの欠陥の結果として、様々な法的制裁が会社に対してなされる可能性があります。

## 3 顧客基盤の喪失

業務活動の制限による顧客基盤の喪失や、顧客の信頼低下を引き起こした結果として、売上損失につながる事例が散見されます。

## 4 損害賠償

顧客の信用回復のため企業が自発的な賠償を行うケースも散見されます。

## 5 改善に要するコスト

漏洩が発生した場合、追加的なコントロールの構築費用が発生します。

特に、我々が対応した事例では⑤の改善コストよりも①～④のコストが多額になっているケースが多いと思われます。なお①～④は回避できた損失となります。

情報漏洩の最大の原因は、機密情報を知り得る内部の人間によるものが6割を占めます（PwC調査）。性善説にとらわれずに、社員やパートナーに対する厳格なアクセスコントロールやモニタリング、暗号化など、犯行を起こす可能性の芽を摘み取る高度なセキュリティ対策が非常に有効です。ただし、それでも情報漏洩や不正アクセスは起きるものという意識を持ってください。インシデントが起きた時の対策を入念に準備している企業と、想定外の事態に慌てて蓋をしようとする会社では、解決までにかかる時間も損失額も倍以上違ってくるのです。

その意味でも、高度なセキュリティレベルを担保しているクラウドベンダーの活用は非常に重要です。加えて、グローバル化が進むビジネス展開を考えると、EUや米国など海外の厳しいセキュリティ･レギュレーションもクリアできる、グローバル対応のクラウドならいっそう頼もしいでしょう。

自社のビジネス特性に合わせたクラウドベンダーを活用し、堅牢なセキュリティ対策、ガバナンス態勢の強化を進めていくことを、IoT時代に勝ち残る企業戦略としてぜひお考えください。

# IoT時代のニーズに応えるクラウド選択のポイント。

## 【Salesforceセキュリティ インタビュー】

成田（なりた）　泰彦（やすひこ）さん　YASUHIKO NARITA

セールスフォース・ドットコム
セールスエンジニアリング本部　プリンシパルソリューションエンジニア　(CISSP)

DBセキュリティソフトベンダー、ネットワークセキュリティベンダーなどを経て、2011年1月よりセールスフォース・ドットコムにてセキュリティスペシャリスト。

# IoT化による新サービスが社会を変える

さまざまなモノがインターネットに接続されるIoTの活用が始まっています。例えば、バスの運転手の健康状態をセンサーでモニタリング送信して安全運行に役立てたり、自動車が走りながら渋滞状況を送信したり、家電製品が製造元からアップデートモジュールを受信して自動でアップデートしたり…。こうしたIoT化はこれからもますます進化し、社会の至る所で使われていくことでしょう。

デバイスを利用しているユーザーにとっては、いつ、どんなデータが受信されているかを意識することなく、自動でアップデートされるサービスを享受できます。一方、IoTを利用する企業にとっては、デバイスやセンサーから有益なデータをリアルタイムに収集し、蓄積されたビッグデータを分析。より良いサービスに加工してユーザーへ還元することができます。また、こうしたビッグデータ自体に価値が生じてくれば、企業同士でデータを交換したり、売買したりするようになるでしょう。

salesforce app cloud

# IoT化によるデータの真正性をいかに担保するか

このような人・モノ・企業の三者間でデータが活用されていくIoT化により、これまで存在しなかった全く新しいサービス、デバイス単独では実現できなかった複合的なシステムが登場したり、従来の垣根を越えた異業種企業の連携が実現したりしています。

IoT化による新サービスの出現は、収集したビッグデータをいかに効果的に活用できるかにかかっているため、大前提としてデータの真正性と信頼性が担保されている必要があります。もし、人・モノ・企業の三者間に流れる情報を、悪意ある攻撃者が改ざんしたり、不正なデータを流したりすると、企業が誤った判断をしたり、デバイスが誤動作をしたり、意図しない大きな被害が起きる危険な状況が生まれます。

その意味で、IoTによって大量に発生するデータの格納場所や、そのデータを精製してビジネス展開するシステム環境のセキュリティを確保することは、これからの最重要課題の一つになると言えるでしょう。

# クラウドではサービスレイヤーのセキュリティが重要

IoT時代のインフラとしては、大量のデータの格納場所となる「ストレージレイヤー」と、データの分析や加工を行う「サービスレイヤー」が必要となりますが、今後IoT化の進展によるデータ量の急速な増加を考えると、その発生スピードが速すぎて、従来のようなオンプレミスでシステムを運用していくことは難しくなるでしょう。つまり、効率やコストを考えたら、クラウドの活用は必然となっていくのです。

このストレージレイヤーとサービスレイヤーは連携しながらIoTの新しい仕組みを作りますが、精製前の生のデータを格納するストレージレイヤーに比べて、サービスレイヤーには抽出・加工された価値ある情報、企業経営をリードするような知見や、デバイスを制御できるデータなどが集約されているため、サイバー攻撃はこちらに集中していきます。

だから、企業や官公庁がサービスレイヤーを利用する際には、高いレベルでセキュリティを担保しているクラウド事業者を見極める必要があるのです。

salesforce app cloud

# 最高レベルのセキュリティ認証を受けているSalesforce

Salesforceは、クラウドベンダーのパイオニアとして16年の実績を持ち、その間、情報漏洩やDDoSなどのサイバー攻撃によるサービスダウンは一度もありません。その堅牢性は以下のような厳しい第三者認証を取得していることからも証明されています。

・PCI-DSS:クレジットカード業界団体による認証。最新のバージョン3.1を取得済み。

・FedRAMP:米国連邦政府による認定制度で、行政機関の機密情報を取り扱うにはこの認証が不可欠。

・ISO27018:クラウドセキュリティに関する新しい国際標準規格で、Salesforceはいち早く取得済み。

ISO 27001 Certified

SSAE16 SOC-1,2,3
(2011年まではSAS 70 Type II)

SOC-3 Certified
(2011年まではSysTrust)

Federal Authority to Operate - Moderate Baseline(GSA)

PCI DSS 3.1 Compliant

TUV Certified - Germany

JIPDEC - Japan Privacy Seal

Salesforceは第三者による厳しいセキュリティ認証を取得しています。

# 標準実装のセキュリティ機能に加えて、さらに高度な“Salesforce Shield”も登場

こうした厳しい認証を受けているSalesforceだけに、高度なセキュリティ機能を標準で提供しています。例えば、不正アクセスを防止するためのワンタイムパスワード、指紋認証、ログインフォレンジックなどの厳重なアクセスコントロール機能をご用意。また、サイバー攻撃に備えるためのセキュリティ設定アセスメント、ウェブサイトの脆弱性をチェックするセキュアコーディング、さらに、内部犯行を追跡するアクセスモニタリング、証跡監査などもすべてのユーザーにご利用いただけます。

このように、標準機能だけでも充分セキュアなSalesforceプラットフォームですが、今後いっそう厳格なセキュリティやコンプライアンスが求められる企業には、さらに高度なセキュリティサービス「Salesforce Shield」が必ずお役に立つはずです。加速するIoT時代のセキュリティとコンプライアンスに不可欠となる、いっそうセキュアなシステム環境は、これからもSalesforceが実現していきます。

salesforce app cloud

# Salesforce Shield

## 最高レベルのセキュリティを実現する新サービス

IoT時代を迎え、企業がクラウドに蓄積するデータ量は爆発的に増加しており、厳格な管理ポリシーによるデータへのアクセス管理、漏洩予防がこれまで以上に重要になっています。Salesforceのクラウドは、高度なセキュリティ機能を標準で装備していますが、さらに高度なコンプライアンスとガバナンスを必要とする企業のために、セキュリティをいっそう強化するSalesforce Shieldを提供。3つのサービスで将来に備える最高レベルの安心安全を実現します。

## Salesforce Shield

標準セキュリティ機能に加えて、いっそうの安心安全を提供するサービス

## イベントモニタリング

データの不正な使用を検出し、予防します。

- ユーザー操作の記録
- リアルタイムのアラート（トランザクションセキュリティ機能使用時）
- 予防機能

Salesforceのクラウド上に構築されたすべてのアプリケーションを対象に、詳細な利用状況を監視できます。誰が、いつ、どこから重要なビジネスデータにアクセスしているのかを把握できるだけでなく、利用パターンを分析することも可能。また、セキュリティポリシーを設定することにより、不審操作に対するアラートの送信やユーザー操作のブロックをリアルタイムに実行することができます。

## 項目更新履歴監査

データを長期間保持し、完全監査を可能にします。

- 最長 10 年間のデータ保持とアーカイブポリシー
- クエリベースでの項目履歴の取得

規制の厳しい業界においてコンプライアンスを順守するために、企業はデータの真正性、完全性、信頼性を確保しなければなりません。そこで、項目レベルで最長10年分の変更履歴を保持し、フォレンジックに必要となる監査証跡の作成に利用できるようにします。また、データ保護ポリシーを定義でき、指定したスケジュールに沿って不要なデータを自動的に削除することもできます。

## プラットフォーム暗号化

データベースに格納される機密情報を暗号化することにより保護します。

- 保管されている機密データの暗号化
- 暗号化キーの管理

Salesforce プラットフォームの暗号化機能を利用すれば、保管されている機密データとファイルを指定して、ワンクリックで暗号化できます。暗号化した後でも、検索やワークフロー、入力規則などの重要なアプリケーション機能は影響を受けません。内部犯行などにより万一データが持ちだされても、機密情報の漏洩を防止できます。