DX時代のビジネスに求められる「デジタルトラスト」
第1回「オープン化」の観点

金融事業部／アシュアランスイノベーション本部　安達知可良

▸ Chikara Adachi
金融事業部に設置した「FinTechセンター」、およびアシュアランスイノベーション本部に設置した「Digital Trust」「Blockchain Center」をリード。FinTech企業、金融機関双方へのサービス支援、会計監査やシステム監査などに従事。JICPAのブロックチェーン検討専門委員会、Fintech協会のセキュリティ分科会の事務局など複数の社外活動にも従事している。CISA、CISM、ITコーディネータ。当法人 シニアマネージャー。

Ⅰ　はじめに

今、多くの企業がデジタルトランスフォーメーション（DX）を推進しています。最新のデジタル技術を活用することで社会課題が削減され、利便性の高い世界の実現が期待されています。一方で、新しい技術を利用することにより、これまで想定していなかった新たなリスクが発生する可能性を無視することはできません。こうしたリスクへの確実な対策があって初めて、安心・安全にデジタル技術を活用することができるようになります。デジタル技術の活用に向けた信頼構築の活動を、私たちは「デジタルトラスト」と称しています。

Ⅱ　DXによりもたらされる変化

DXとは、単にデジタル化による業務効率化を指しているのではなく、ビジネス環境や社会構造の変革をもたらす取り組みであり、より影響範囲の広い概念とされています。データ利活用により高度に効率化された、いわゆる「データドリブン」な社会実装に向けた活動であると言い換えてもよいかもしれません。そこに向かう道程で起こり得る特徴的な行動変容として、以下三つの観点があると考えられます（＜表1＞参照）。

① オープン化
　ITシステムやデータを組織の外部に開放する
② 共有化
　ITシステムやデータを外部組織と相互利用する
③ 自動化
　ITシステムやデータを活用して業務処理を自動化する

各観点について、どのような行動変容が起こるか、それによる新たなリスクとは何か、どのようなリスク対策が考えられるか等について今号より3回シリーズで考察していきます。第1回目となる本稿では「オー

▶表1　DXによる行動変容の三つの観点

	オープン化	共有化	自動化
ビジネスモデルはどう変わる？	▸ ITシステム管理のオープン化 　▸ アウトソース／クラウドサービス利用 　▸ EDIやAPIによる外部連携 ▸ 労働環境のオープン化 　▸ テレワーク・リモートワークの促進 　▸ 外部リソース利用の拡大	▸ ITシステムの共有化 　▸ ITシステムの共同利用 　▸ コンソーシアム・ブロックチェーン ▸ データの共有化・コモディティ化 　▸ データレイクにより企業内データ共有 　▸ 公共財として企業外にデータ提供	▸ オペレーションの省力化・自動化 　▸ RPAを活用した定型業務の自動化 　▸ 機械学習によるデータ分析 ▸ 業務の自動執行 　▸ スマートコントラクトによる自動執行 　▸ AIによる意思決定の自動化
どんな課題が考えられる？	▸ 外部組織の管理態勢の把握 企業のITシステム運営に係る外部組織の関与が増え、重要度が高まる中、企業がその管理状況を把握するための難易度が上がる ▸ 多様化するサイバー攻撃の防御 さまざまな場所から社内データへのアクセスが可能となり、サイバー攻撃が多様化し防御策の難易度が高まる	▸ ITシステムのガバナンス体制構築 多数の利害関係者が存在するITシステムでは、ガバナンス体制構築には多様な意見調整を要するため難易度が上がる ▸ データのガバナンス体制の重要性 未成熟なデータのガバナンス体制により、安全性、正確性、コンプライアンス等が担保されない	▸ ブラックボックス化するプロセス 多くのAIはプロセスがブラックボックスとなり、プロセスやアウトプットの正確性の検証・証明が困難となる ▸ プログラムコードの重要性 人手を介さず処理が自動執行されるスマートコントラクトでは、プログラムコードそのものの正確性がより重要となる

プン化」をテーマとして取り上げます。

Ⅲ　ITシステムにおける「オープン化」の歴史

ビジネスシステムは「クローズド」から「オープン化」への歴史を経て今に至っています。まずはその歴史を振り返ってみましょう。

1. メインフレーム時代からオープンシステムへ

1960年代頃から大企業を中心に業務のシステム化が進められました。メインフレームと呼ばれた当時のコンピュータは、大型汎用機（ホスト）と端末（ターミナル）を専用線でつなぐ形式で、コンピュータメーカーがハードウェア、周辺機器、ソフトウェアまでを一括して提供していました。

1980年代に入り、OS※1の規格標準化が進み、同じ規格のOSを搭載した機器であればメーカーを問わず同様の操作ができるようになりました。これがビジネスシステムの「オープン化」であり、アプリケーションソフトの汎用性が高まったことにより、利用者は複数の事業者から製品を自由に選択できるようになりました。メーカーが一元的に製品を提供する時代から、利用者側がマルチベンダーの製品を主導的に選択できる時代となったのです。

2. インターネットの登場

1990年代に入りインターネットが普及し、ビジネスの場でも電子メールの活用や、電子商取引（EC）サービス開始等の動きがありました。やがてウェブが普及され始め、通信の暗号化技術も実装され始めるとインターネットの商業利用が本格化しました。多くの企業がウェブサーバーを所有し、世界中とインターネット経由でつながる利便性を享受することになります。

2000年代後期に入り、ウェブ技術がさらに高度化し、異なるウェブサイト同士がAPI※2を利用して相互に連携（マッシュアップ）するサービスが登場しました。UI/UX※3向上に寄与しており、SNS（ソーシャル・ネットワーキング・サービス）等でよく利用されています。

3. 運用業務のアウトソーシング化とクラウドコンピューティングの活用

ホストやサーバーを設置するデータセンターの施設・設備管理、ハードウェアメンテナンス、システムオペレーション等、幅広い領域に及ぶITシステムの運用業務は、かつては企業自身（子会社含む）が行っていましたが、近年は外部委託（アウトソーシング）化を進める傾向にあります。事業者の中には、複数企業から運用業務を請け負うことでスケールメリットを活かす「シェアードサービス」型の事業者も登場しています。

上記は企業が所有するサーバー（オンプレミス環境）の管理を外部委託するケースですが、2000年代に入ると事業者が所有するデータセンター内で、事業者が所有するサーバー上に仮想環境を用意し、それを従量制で企業に貸し出す、いわゆる「クラウドサービス」が登場します。企業は自社の資産を保持することなく、必要な時に必要な容量を借りることができるため、コストメリットが享受できます。

4. モバイル化とIoTの活用

2000年代後期にスマートフォン（スマホ）が登場して以降、BtoCビジネスを中心にモバイル化が進み、顧客のアクセスポイントをPCからスマホにシフトする「モバイルファースト」の発想が広く浸透しました。

ビジネスの場でもモバイル活用が進み、スマホやタブレットを入出力端末として利用したり、スマホの生態認証機能やSMS※4をビジネスシステムへのログイン時の「多要素認証」として利用したり、新たな利用価値が生まれています。近年ではIoT機器※5の普及も進み、RFID（ICタグ）やセンサー等でモノの状態をリアルタイムで把握する、データドリブン経営に向けた取り組みも始まっています。

また、COVID-19の影響もあり、リモートワークが推奨される中、オフィス内からのアクセスに限定していたビジネスシステムを、自宅等からアクセスできるよう急遽対応した企業も少なくありません。専用端末に限定していた時代と比べると、ビジネスシステムへのアクセスポイントは、機種も場所もさまざまなケースが考えられるようになったことで、より機動的な選択が可能となりました。

※1　Operating Systemの略で、機器の基本的な管理・制御機能等を実装したソフトウェア
※2　Application Programming Interfaceの略。プログラムが、異なるプログラムやデータを呼び出して利用するためのインターフェース
※3　User Interface/User Experienceの略。UIは製品・サービスの表示方法と操作性等を意味し、UXは製品・サービスの利用を通じて利用者が得る体験を意味する。
※4　ショートメッセージサービス
※5　世の中に存在するさまざまなモノに、センサー等の通信機能を持たせて、インターネット経由や相互通信によりデータを授受するための機器。ICチップ、センサー、監視カメラ等。

5. 人的交流の拡大とオープンイノベーション

企業の価値創造の場でも「オープン化」が進んでおり、他社や外部人材とコラボレーションすることでより幅広いノウハウやアイデアを得る「オープンイノベーション」といった取り組みも増えつつあります。これを促進するために副業を認める企業や、外部人材と接しやすいコワーキングスペースを活用する企業も増えてきています。

こうした場でITベンチャー企業と大企業が接点を持ち、大企業の持つ顧客基盤に対し、ITベンチャーの先端技術開発力を利用した斬新なサービスを両者共同して開発するような動きも近年注目されています。

Ⅳ　オープン化に伴うリスクとその対策

ITシステムのオープン化により私たちの社会はさまざまな便益を得ていますが、これにより生じるリスクとしてどのようなものがあるか、またその対策として何を考慮すべきか、についてここから考察します。

以下では、「外部事業者管理」と「サイバー攻撃」の二つの観点について触れていきます。

1. 外部事業者管理の観点

(1) 開発事業者に関する留意点

システムのオープン化により製品選択の自由を得た一方、企業は複数存在する事業者の管理が求められるようになりました。システム導入時にSIer※6等の調整役が入ったとしても、開発時に提供したデータの管理状況や、稼働後のメンテナンス体制・障害時の対応体制等を確実なものにするための管理責任は委託元企業に問われることになります。

事業者が多重に再委託している場合で、仮に末端の委託先に起因するインシデントであっても、サービスや顧客に大きな影響を与えかねないため、委託元企業は再委託先の状況も意識する必要があります。全ての委託先を同水準で管理すること困難だとしても、少なくとも全ての関与する再委託先を把握した上、各委託業務に関連するリスクの重要度・影響度を評価し、その度合いに応じて濃淡を付けて対応するリスクベース・アプローチは有効な手段と言えます。

(2) 運用のアウトソーシングに関する留意点

セキュリティ管理体制、障害時の対応体制等の重要な統制活動がブラックボックスの状況では、サービスの信頼を得ることはできません。運用業務をアウトソーシングした場合であっても、日常的に行う重要なオペレーションの実態把握が不可能となってしまう状況は避けなければなりません。

シェアードサービス事業者の中には、複数の委託元企業の要求に対応するため、監査法人と契約し保証報告書（SOCレポート）を作成し、内部統制の評価結果を委託元企業に提供している事例もあります。こうした対応は有効な情報提供手段であることは間違いありません。ただし、評価項目は各社の要求と必ずしも合致していない場合があるため、企業は自社の要求との適合状況を見極めることが重要となります。

クラウドサービスは、事業者が所有する環境を貸与する形であるため、サービスを利用する企業は多数の利用者の1社にすぎません。両者の間に委託－受託の関係は成立しづらい状況であり、利用契約やSLA※7は事業者側のひな形通り締結する事例が多く、利用企業の意向が反映されることは稀（まれ）です。保証報告書等を提供する事業者もありますが、事業者側で特定した項目のみで評価されているケースが殆どであるため、企業としては要求水準が満たされている度合いの確認がよりいっそう重要になります。

(3) コラボレーションの関係に関する留意事項

外部事業者との間は、委託－受託といった「縦」の関係から、コラボレーションといった「横」の関係も増えてきています。例えばAPI接続して双方の顧客を送客し合うようなスキームの場合、双方が委託者であり受託者であるという関係も成り立ち得ます。

こうしたケースにおいては、主従関係でルール整備するのではなく、双方のリスク認識を共有し、協調してルール整備することも有用となります。双方の業務範囲を定義して責任分界点を明確にすることや、双方で相手方に求める管理レベルを提示して、その達成状況を定期的に評価し合うこと等も有効な手段であると考えられます。

また、事故や障害が発生した際の備えとして、一義的な対応主体はあらかじめ特定しつつも、顧客を「たらい回し」にしないよう、協同して対応する体制を構築することも、社会の信頼を得るための重要な要素となります。

2. サイバー攻撃に関する観点

(1) インターネット黎明期（れいめい）のサイバー攻撃

インターネットは社会にさまざまな便益をもたらし

※6　System Integratorの略。システム・インテグレーターは企業のITシステム構築業務を一括して請け負う事業者のこと。
※7　Service Level Agreementの略。サービスを提供する事業者と契約者の間で、提供するサービス品質を保証するレベルを約束した合意書。

ましたが、一方で外部攻撃のリスクが高まりました。ECが普及した2000年代、大量にデータを送りつけてサービスを妨害する「DoS攻撃」や、クレジットカード情報を搾取する「フィッシング」等、企業に財務的影響を与えるサイバー攻撃が広がり始めました。

2000年代後期には攻撃を受けた企業のみならず、そこにアクセスした利用者（顧客や取引先）の端末にも感染させるマルウェア※8が流行しました。攻撃目的が運営会社の社会的信用を失墜させることにシフトしており、多くの企業では経営課題ととらえファイアウォールの設置等の対策を行いました。

(2) 標的型攻撃の猛威

2000年代後半から、メールを利用してマルウェアを内部に送り込む、いわゆる「標的型攻撃」が徐々に認識されるようになります。主な攻撃例では、ある企業を狙ってメールを送り、受信者が添付ファイルを開くと企業のネットワーク内部にマルウェアが侵入し、企業内のデータを搾取し、それを外部に送信するまでを自動で行う、という動きをします。メール自体は通常のものと見分けが付かないため、ファイアウォールで機械的にフィルタリングすることは困難であり、人による判別が重要になります。

その後も標的型攻撃は進化を続け、侵入後に企業内の重要なデータを勝手に暗号化し、それを解くための鍵と引き換えに身代金を要求してくる「ランサムウェア」型の攻撃も増加しています。最近では、要求通りに応じなかった場合には搾取したデータを暴露すると言って脅してくる事例や、身代金を足が付きにくい暗号資産で支払わせる事例等、手口がより巧妙になっています。

IT環境面の対策として、外部攻撃に対抗するWAF※9やIDS/IPS※10等を設置する「入口対策」のほか、ログ管理やモニタリング等により内部侵入後の挙動を検知する「内部対策」、搾取した情報の外部持出を監視する「出口対策」を組み合わせた多層防御対策が有効であるとされています。

標的型攻撃は人のアクションがきっかけとなるため、社員教育や訓練等の人的対策は非常に重要となります。さらにネットを利用するBtoCビジネスの場合には、顧客に対しても注意喚起することも重要となります。

(3) 近年のIT環境の変化による影響

近年ではビジネスシステムへのアクセス方法はさまざまな端末や場所を認めており、これまでのようにネットワーク境界内のみを防御するだけでは対応が難しくなりつつあります。そのため、全てのアクセスを信頼せず、境界内外問わず同様のセキュリティ対策を行う「ゼロトラスト」という発想による防御策も近年注目されています。

また、IoT機器の脆弱性（ぜいじゃく）が多数報告されており、これを狙ったサイバー攻撃が近年増えています。こうした多様化するアクセスポイントを前提とした対策が求められることになります。

(4) 信頼を確実にするサイバー攻撃への対策例

攻撃手法は日々巧妙になっており、最新情報を入手することは容易ではありません。CSIRT※11等の専門組織を設置し、平時には業界内外の専門家と交流して情報収集活動をするとともに、インシデント発生時にはCSIRTが主導して初動対応できるよう体制構築することも重要となります。

自社のシステムにおける攻撃耐性は、人間の健康状態のように外見からは見えにくいものです。そこで定期健康診断を受診するように、専門家による脆弱性診断等を受診することは、信頼性を客観的に証明するための有効な手段となります。

V　おわりに

私たちは、もはやインターネットのない世界には戻れません。また、外部委託を活用することによりコアビジネスに集中できる効率性も実感しています。オープン化によりもたらされたメリットを享受するには、反面のリスクを正しく知り、対応することが必要です。技術の進化は早く、常に新しい可能性が生まれています。ワクワクする未来のために、技術を正しく「恐れ」ながら付き合っていくことが重要です。

お問い合わせ先
EY新日本有限責任監査法人
アシュアランスイノベーション本部
E-mail：Chikara.Adachi@jp.ey.com

※8　代表例として「ガンブラー（Gumblar）」が著名
※9　Web Application Firewallのことでウェブアプリケーションの脆弱性を悪用する攻撃を検出・防御し、ウェブサイトを保護するためのセキュリティ製品を指す。
※10　IDS：Intrusion Detection System 侵入検知システム（不正侵入の兆候を検知するシステム）／IPS：Intrusion Prevention System 侵入防止システム（不正侵入の兆候を検知し遮断するシステム）
※11　Computer Security Incident Response Teamの略。組織内で発生したセキュリティインシデントに対応する組織。