金融DX、IT環境の変化とリスクマネジメント

2022年7月

PROMONTORY
an IBM Company

目次

1．金融機関のデジタルトランスフォーメーションとITガバナンス

（1） 金融DXとは

- DX（デジタル・トランスフォーメーション）

- デジタル化の進展に応じたビジネス・業務の変革の動き
  （金融庁「金融機関のITガバナンスに関する対話のための論点・プラクティスの整理」2019.6）

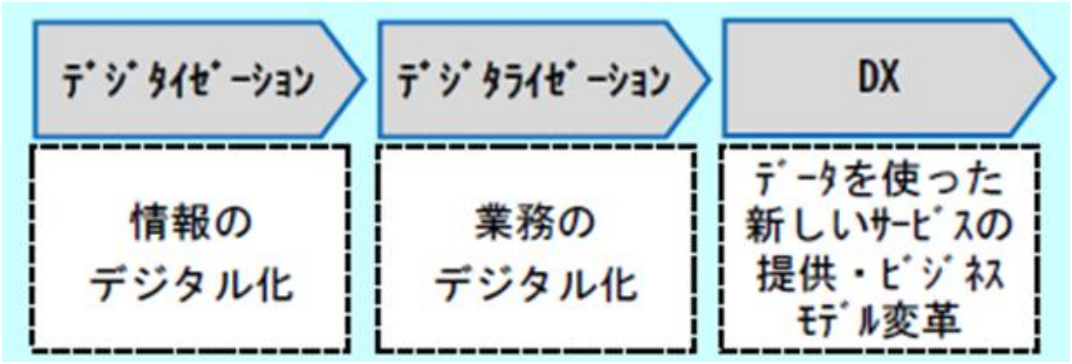
- デジタル技術を活用して経営や業務のあり方を大きく見直し、経営の効率化とより付加価値の高いサービスの提供を目指す動き
  （日銀「わが国の銀行におけるデジタル・トランスフォーメーション（DX）2021.3」）

DXの特色

- DX は、経費削減のみならず、日常的な顧客との接点（顧客接点）の確保とそこでの顧客体験（UX）の向上を通じた、新しい収益の創出を目的とする。

- DXは、日常的な顧客接点から、「静的な」もののみならず、「動的な」ものも含めた様々な顧客データを把握し、高頻度な顧客との接点を確保することにより、顧客の顕在化した需要だけでなく潜在的な需要もデジタル・チャネルを通じて捉えて、これに応えるサービスをきめ細かくタイムリーに提供することを目的とする。

▼ ﾃﾞｼﾞﾀｲｾﾞｰｼｮﾝ、ﾃﾞｼﾞﾀﾗｲｾﾞｰｼｮﾝとの違い



（2） ITガバナンスの重要性

- 金融機関は、持続可能なビジネスモデルを確保する上で、昨今のデジタル化の進展に応じたビジネス・業務の変革の動きである「デジタルトランスフォーメーション」について、取捨選択の上、必要に応じて、経営戦略に取り込むことが求められている。

- デジタルトランスフォーメーションを取捨選択の上、経営戦略に取り込み、企業価値を創出するためには、ITガバナンスが確立していることが不可欠。

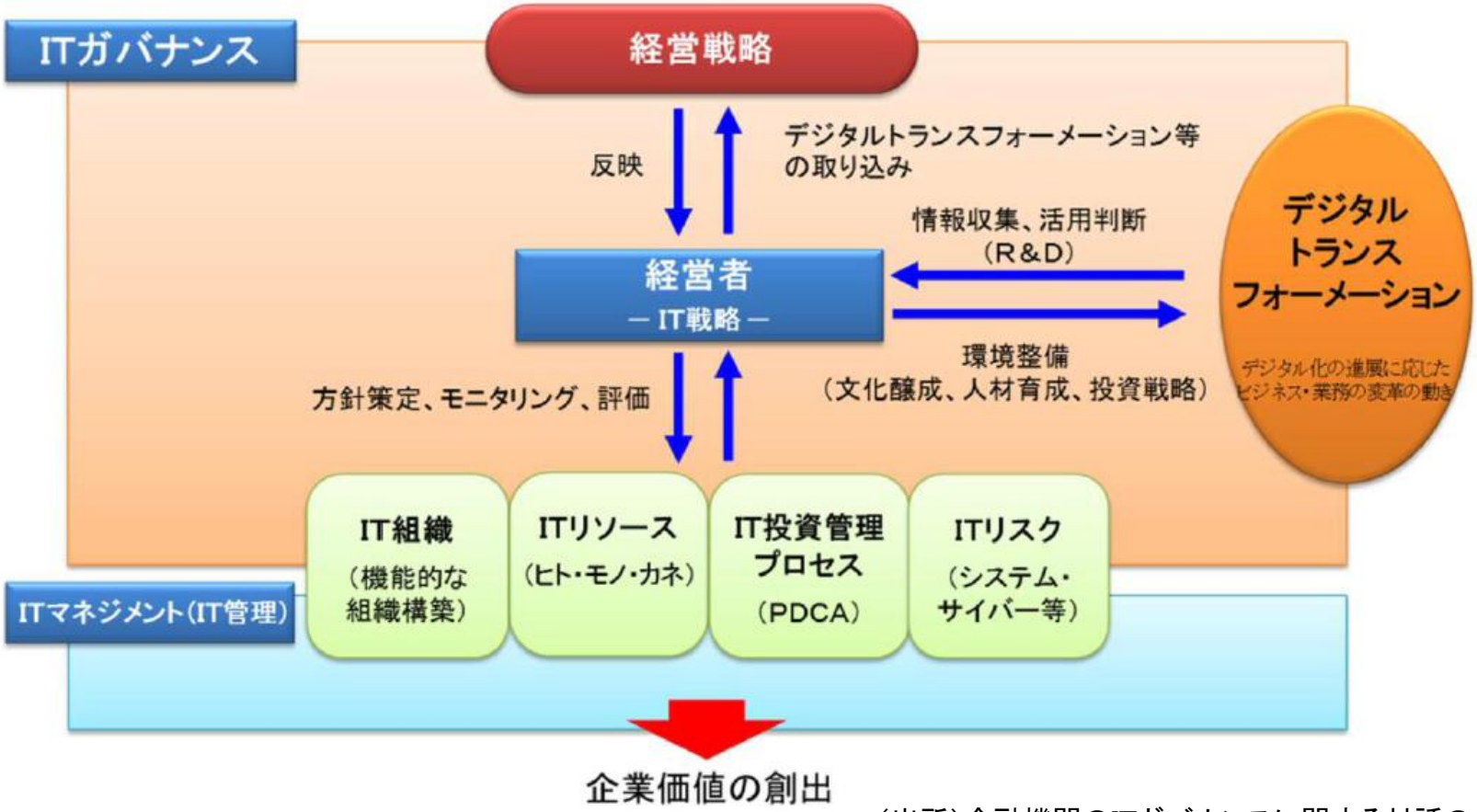
■ ITガバナンスとは

「主にIT化により新たに生じるリスクの極小化と的確な投資判断に基づく経営効率の最大化、すなわち、リスク・マネジメントとパフォーマンス・マネジメントであり、これらを実施するに当たっての、健全性確保のためのコンプライアンス・マネジメントの確立」（日本監査役協会ITガバナンス委員会）

■ ITガバナンスとITマネジメント

経営陣がITガバナナンスを主導し、それに基づき実務部隊がITマネジメントを実施。

IT ガバナンスの概念イメージ



（出所）金融機関のITガバナンスに関する対話のための論点・プラクティスの整理　金融庁2019年6月

(3) 戦略的なシステム投資を行うにあたってのポイント

- システム戦略とは

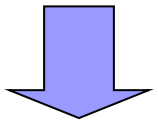
  企業の経営効率を最大化する戦略的なシステム投資を行うための、方向性・目指す目標・考え方

- 戦略的なシステム投資を行うにあたってのポイント

①経営戦略とシステム戦略の整合性を確保すること
②システム投資の優先順位を明確にすること
③システム技術の進化を十分にウォッチすること
④システム投資のROIを確立すること
⑤トップダウン・アプローチであること
⑥委託先との役割分担を戦略的に行うこと

①　経営戦略とシステム戦略の整合性を確保すること

- システムは経営戦略を実現するための重要な武器であるとの認識の下、システム戦略は経営戦略から導かれたものであることが必要。



- ビジネスで何がしたいのか（中長期的なビジネスの目的・目標は何か）
- そのために、どのようなシステムが必要か。どのようなシステム技術を適用することが適当か。

②システム投資の優先順位を明確にすること

- コアコンピタンス領域へのシステム投資とそうでないシステム投資を分けて考えること。
- コアコンピタンス領域とは、他社と差別化すべき（他社に抜きん出るべき）業務領域。
- コアコンピタンス領域は、システム戦略を実現するうえで、積極投資すべき分野。

- 以上を踏まえ、個別投資案件の優先順位を決定。

③ システム技術の進化を十分にウォッチすること

- 最新システム技術の動向は、システム戦略に大きな影響を及ぼす。
  - ー　例えば、クラウド・コンピューティング、ブロックチェーン、AI
- IT部門は、最新システム技術をウォッチし、提案力を向上させることが必要。
- そのためには、提案力のあるIT人材の育成が必要不可欠。

④ システム投資のROI(Return on Investment)を確立すること

- システム投資の費用対効果を評価するためのフレームワークを策定する必要。

- 評価はシステム投資の事前および事後に行う必要。

  事前評価：費用と効果（予想）の比較検討により、投資の是非を決定

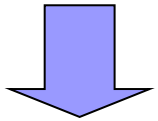
  事後評価：実際にもたらされた効果が、当初予想どおりであったかどうかのフォロー

⇒ 投資決定の際の事前評価は行うが、事後評価（費用対効果の事後フォロー）は、行われていないケースがみられる。

⇒ また、事後評価が、当初目標未達となった場合の責任の所在も曖昧なことが多い（外銀ではシステムオーナーが責任を負う）。

⑤ トップダウン・アプローチであること

- システム戦略はボトムアップでは策定できない。
- 一方、経営層自らがシステム戦略を策定するだけのスキル・ノウハウがない。



- システム戦略を策定するための体制づくりが必要。
- システム戦略委員会（取締役会に属する委員会）の組成が有効。
- システム戦略委員会のメンバーと役割。

（メンバー）

役員と役員以外の専門家

（役割）

－　自社ビジネスと自社システムの双方を理解・把握し、システムを武器とした経営戦略（すなわちシステム戦略）を検討する。

－　システムの新技術を評価し、自社ビジネスへの導入を検討する。

－　以上を踏まえ、経営層に対してシステム戦略に関する提言・助言を行う。

- システム戦略委員会のような組織が組成されない場合には、システム戦略を検討する部署（システム部署であることが殆ど）と経営層との密接な連携が不可欠。

⑥　委託先との役割分担を戦略的に行うこと

- 戦略的な役割分担とは、

・　コアコンピタンス領域（他社と差別化すべき高付加価値領域）には自社リソースを割り当て、そうでない領域（自社で行うに値しない領域）は外部委託する。

・　コアコンピタンス領域とは、
例えば
　ー　戦略的なシステムの開発
　ー　システム開発の上流工程

・　外部委託にあたっては、適切な委託先管理が必要不可欠。

２．クラウドの活用

(1) クラウドとは

「共有化されたコンピュータリソース（サーバ、ストレージ、アプリケーション等）について、利用者の要求に応じて適宜・適切に配分し、ネットワークを通じて提供することを可能とする情報処理形態」

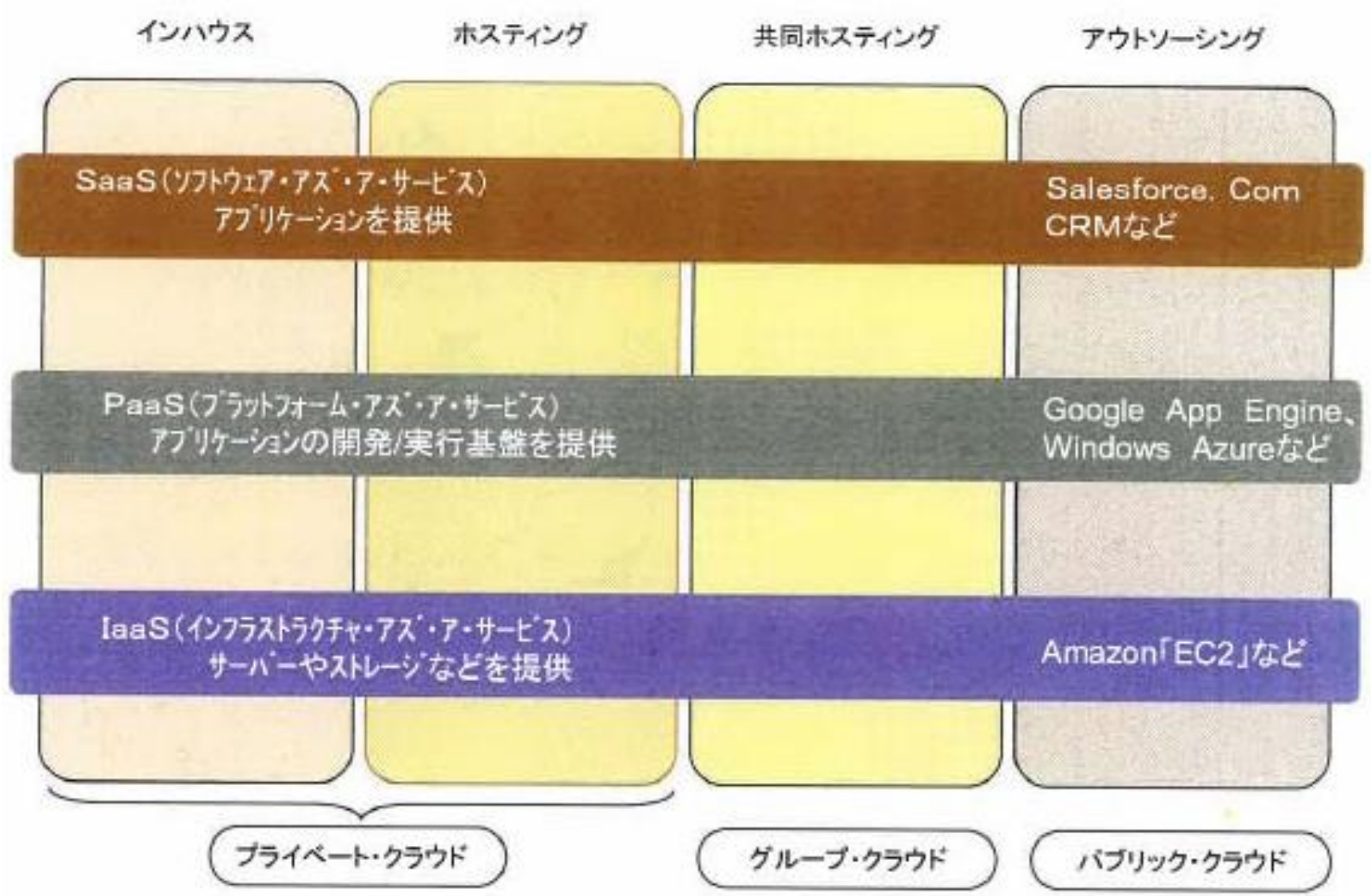
－　経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」

- クラウドは、システムの仮想化技術を利用する。
- 仮想化とは、リソースの物理的特性をそのリソースと相互作用するシステム、アプリケーション、ユーザーから隠蔽する技法により、抽象化すること。これにより、単一の物理リソース（サーバ、ストレージ、ネットワーク等）を複数の論理リソースにみせかけたり、複数の物理リソースを単一の論理リソースに見せかけたりすることが可能となる。
- この結果、例えば、一つの物理的サーバを、複数の論理的サーバに分割し、各々でシステムを稼動させることが可能になる。また、一つのシステムを複数の物理サーバ上に分散して稼動させることが可能となる。

（特性）

- オンデマンド／セルフサービス
  - ベンダーの人手を介することなく、自動化された形態でサービス利用が可能。
- ネットワークを介した利用
  - どこからでもサービス利用が可能。
- リソースの集中貯蔵
  - リソースの保管場所、保管形態を知ることなく、サービス利用が可能。
- 迅速なリソース確保／開放
  - 利用サービス資源の迅速なスケールアウト／インが可能。
- 計測可能なサービス
  - サービス利用の課金の透明性確保が可能。

▼ クラウドのタイプ


インハウス
ホスティング
共同ホスティング
アウトソーシング
SaaS（ソフトウェア・アズ・ア・サービス）
アプリケーションを提供
Salesforce. Com
CRMなど
PaaS（プラットフォーム・アズ・ア・サービス）
アプリケーションの開発/実行基盤を提供
Google App Engine、
Windows Azureなど
IaaS（インフラストラクチャ・アズ・ア・サービス）
サーバーやストレージなどを提供
Amazon「EC2」など
プライベート・クラウド
グループ・クラウド
パブリック・クラウド

(2)クラウドのメリット

■　クラウドの利用により、システム資源の安定性確保や規模拡張に頭を悩ませることなく(コスト負担を含め)、本来のコア業務に専念できる。

■　新規業務開始に必要な機能、サービスを容易に導入できる。

・ コスト削減
  ー　システムの規模拡大に伴うコスト負担削減
  ー　不稼動資源に対するコスト負担削減

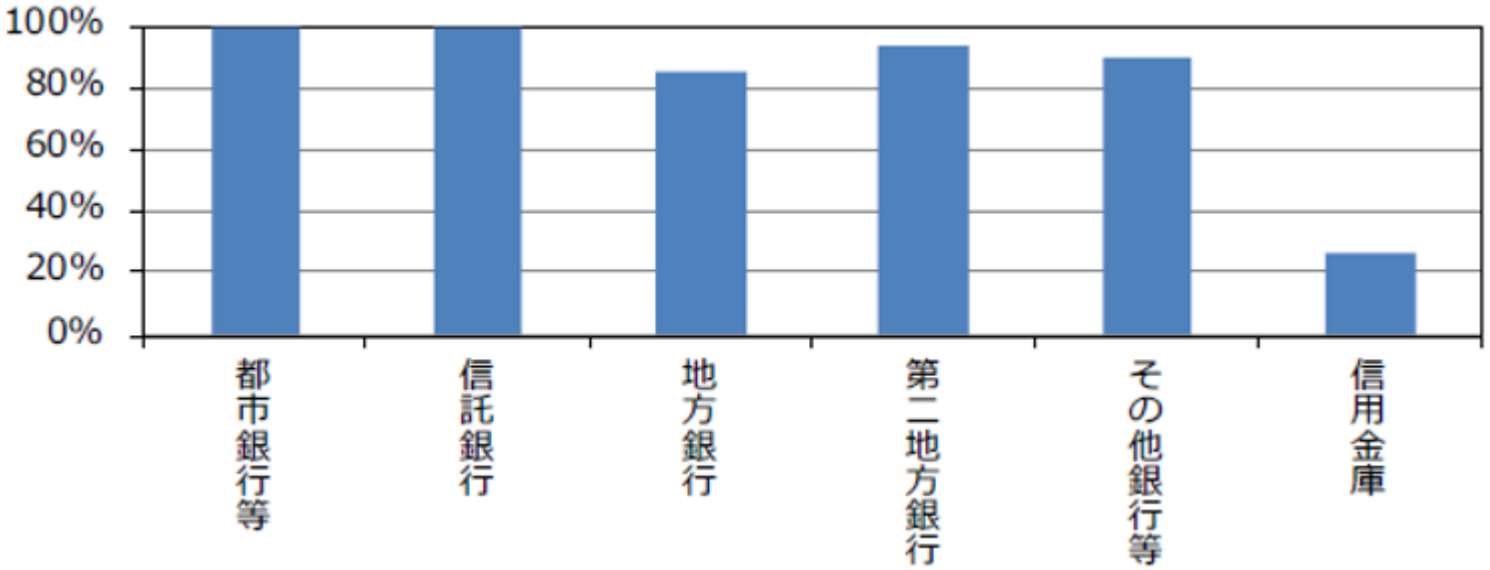
・ 迅速性
  ー　システム資源のスピーディーな提供
  ー　システム開発のスピードアップ

・ データ管理、AIといった新技術、サービスの導入

（3）クラウド活用の現状と今後

■ 多くの金融機関において、システムを構築する上でクラウドは不可欠なサービスとなっている。

▼ クラウドの利用状況



出所：FISCアンケート調査結果（2019年度）

■ もっとも、金融機関におけるクラウドの利用は現状、周辺系システムが中心であり、基幹勘定系システムでのクラウド利用は、デジタル銀行等一部金融機関にとどまっている。

▼クラウドの基幹勘定系システムでの利用状況

29年度	パブリッククラウド	コミュニティクラウド	プライベートクラウド	導入無し
銀行等	4.0%	2.9%	4.0%	89.0%
生保、損保、証券、クレジット	11.3%	3.1%	19.6%	66.0%

（※） 複数回答、構成比。

出所：FISCアンケート調査結果（2019年度）

■ 地域金融機関、デジタル銀行でのクラウド活用事例

年月	行名	システム開発	主な取り組み
2021年5月	北国銀行	日本ユニシス	米マイクロソフトの「アジュール」上で稼働。山口県の西京銀行も24年に移行へ
	ふくおかFG	アクセンチュア	デジタルバンク「みんなの銀行」を米グーグルのクラウド上で稼働
22年1月	東京きらぼしFG	SBJ銀行、SBJ DNX	新韓銀行系の勘定系システムを使い、デジタルバンク「UI銀行」を開業
23年以降	北洋銀行、東邦銀行	日本IBM	地銀10行でつくる「TSUBASAアライアンス」のシステム稼働へ。24年に東邦銀も移行
24年	福島銀行	フューチャーアーキテクト	SBIと組み、米アマゾンの「AWS」上で稼働。30年度に10行程度に導入

出所：日本経済新聞（2022.2.22）

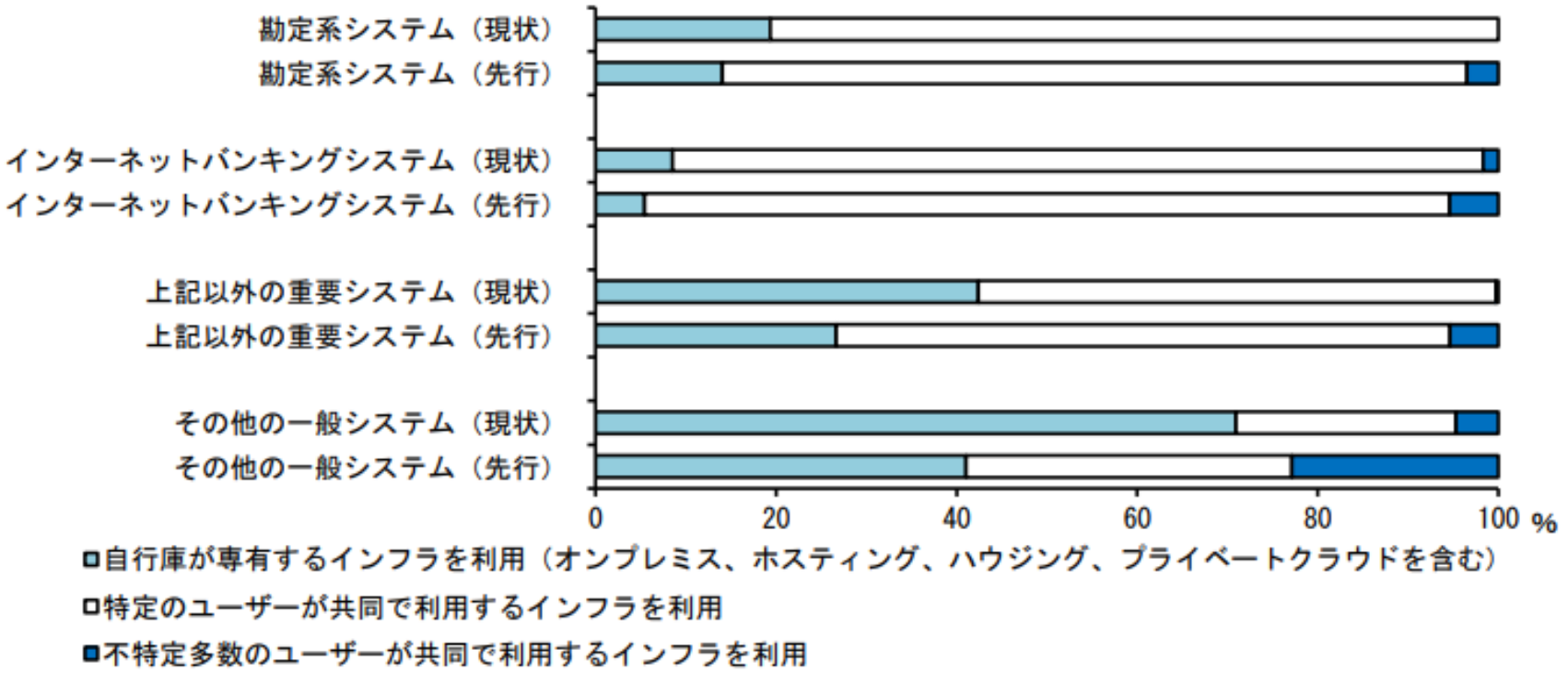
- 政府は、2018 年6月に「政府情報システムにおけるクラウドサービスの利用に係る基本方針」を定め、「クラウド・バイ・デフォルト原則」、すなわち、政府情報システムは、クラウドサービスの利用を第一候補として検討を行うものとする方針を決定。

- 同方針の下、2020年6月にISMAP制度が発足。ISMAPとは、内閣官房（内閣サイバーセキュリティセンター・情報通信技術（IT）総合戦略室）・総務省・経済産業省が所管して発足した政府情報システムのためのセキュリティ評価制度。政府調達の対象となるクラウドサービスは、ISMAP管理基準に基づく第三者の監査を経て、本制度が公表するISMAPクラウドサービスリストに登録されたものに限定される。

- FISCは、金融機関等においてクラウドサービスの利用が拡大する中、クラウドサービスを導入・運用する際にFISC安全対策基準をどのように適用するかについての解説することを目的として、2021年5月に金融機関等におけるクラウド導入・運用に関する解説書（試行版）を発行。当解説書は、適用されるFISC安全対策基準とその適用の仕方、また、最近の動向等を踏まえて追加で考慮すべきクラウド固有の留意事項等が何かを明らかにしたもの。

■ 今後、金融機関におけるクラウド導入はますます拡大していくと考えられる。

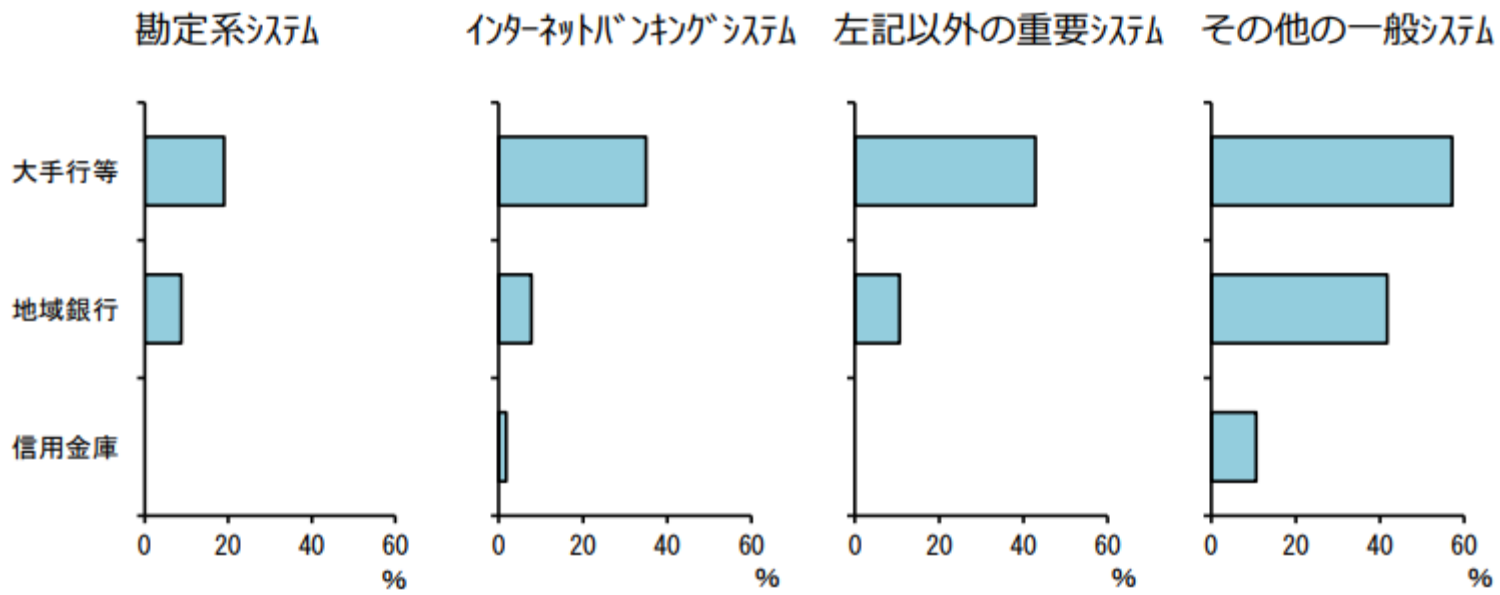
▼ クラウドサービス等の利用の現状と先行き



（注）「上記以外の重要システム」とは、営業店システムや情報系システム等。「その他の一般システム」とは、電子メールシステムやファイルサーバーシステム等。金融機関計。

出所； 銀行・信用金庫におけるデジタライゼーションへの対応状況 （日本銀行、2019.5)

▼ 先行きのパブリッククラウド利用の想定割合



出所； 銀行・信用金庫におけるデジタライゼーションへの対応状況 （日本銀行、2019.5)

(4)クラウドのリスク管理

－　従来のシステム外部委託と同種のリスクとクラウド特有のリスクがある。
－　いずれのリスクについても、クラウド事業者のリスク管理実態が利用先から見えにくくなりがち。

（クラウドに特有、ないしありがちなリスク）

①仕様・サービスが定型的であることに伴うリスク
　－　ID管理、ログ管理、暗号化、アクセス制御、アプリケーション機能、実行環境等
　－　インシデント対応、ヘルプデスク等
②情報開示に制約があることに伴うリスク
　－　インシデント管理 、キャパティ・パフォーマンス管理等
③マルチテナントに伴うリスク
　－　Dos攻撃、他利用者のリスク管理不備による影響等
④技術の新規性に伴うリスク
　－　仮想化、分散化等
⑤データセンターの所在に伴うリスク
　－　リーガルリスク、データ取得・復旧、サービス終了時のデータ消去等

⑥責任共有モデルに伴うリスク

－　クラウドでは「責任共有モデル」と呼ばれる枠組みにより、クラウドの運用・管理を利用者（金融機関）とクラウド事業者で分担するが、このうちクラウド事業者が運用・管理する範囲についても、金融機関側に責務が生じる。

▼ 責任共有モデル

<table>
<tr><th></th><th colspan="3">クラウドの分類 [4]</th></tr>
<tr><th></th><th>IaaS</th><th>PaaS</th><th>SaaS</th></tr>
<tr><td>ユーザー管理</td><td rowspan="3">金融機関</td><td rowspan="2">金融機関</td><td>金融機関</td></tr>
<tr><td>アプリケーションソフトウェア</td><td rowspan="3">クラウド事業者</td></tr>
<tr><td>ミドルウェア、OS</td><td rowspan="2">クラウド事業者</td></tr>
<tr><td>ハードウェア</td><td>クラウド事業者</td></tr>
</table>

・金融機関が直接運用・管理

・クラウド事業者が直接運用・管理
・金融機関はクラウド事業者の運用・管理状況を確認

(資料)日銀「クラウドサービス利用におけるリスク管理上の留意点」(2020.11)

ー　過去のクラウドへの不正アクセスや情報漏えいの多くは、システムやデータへのアクセス権限やネットワーク等に関する利用者の設定ミスにより発生している。

▼ クラウドのセキュリティ管理・対策の不備により発生したインシデント事例

	概要
アクセス管理	・クラウドへシステムを移行した際、機密情報を誤って一般閲覧可能の設定にしたため、URL を入力すれば誰でも閲覧可能となり、機密情報が漏えいした。 ・アクセス時の認証を適切に行っていなかったため、パスワード総当たり攻撃による侵入を許し、クラウド上の情報資産を全て消去されてしまい業務を継続できなくなった。
ネットワークセキュリティ	・クラウドに開発環境を構築した際、テストのために一時的に格納した機密情報の消去を失念し、さらにファイアウォールの設定ミスにより外部からアクセスできる状態になっていたため、パスワード総当たり攻撃を受け、機密情報が漏えいした。 ・WAF[8]の初期設定に関する認識不足に起因する設定不備があったため、WEB サーバーに対して WEB アプリケーションの脆弱性を悪用した不正な指示が行われ、大量のデータが流出した。
セキュリティパッチの適用	・データベース管理システムへのセキュリティパッチの適用漏れから外部の第三者がデータベースにアクセスできる状態になっていたため、ランサムウェア[9]による攻撃を受け、クラウド上のデータが全て利用できなくなった。
情報漏えい対策	・顧客情報の漏えいにおいて、顧客の機微情報やパスワードを暗号化せずに保存していたため、被害が甚大になった。

(資料)日銀「クラウドサービス利用におけるリスク管理上の留意点」(2020.11)

リスク管理の手順・ポイント

- 契約時にクラウド事業者のリスク管理対策を明確化・可視化するための手段を確保する。
  - ・ クラウド利用業務の重要性を踏まえた、実施すべきリスク管理対策の整理（自行リスク管理基準に基づく）。
  - ・ クラウド事業者が提供するリスク管理対策とのGAP分析を行い、クラウド事業者への要求事項を定める。
  - ・ SLAの締結により、クラウド事業者が実施するリスク管理対策を明確にする。
  - ・ クラウド事業者のリスク管理状況をモニタリングするための手段を確保する。
    - ― 定期報告、立入調査権の確保、外部監査結果の入手など

- クラウド利用者が実施するPDCAにクラウド利用に係るリスクを組み込む。
  - ・ 定期的なリスクアセスメントをクラウド利用業務を含めて実施する。
  - ・ クラウド利用に係るリスクのうち、利用先側でモニタリング可能な部分と可能でない部分を区分する。
  - ・ 利用先側でモニタリングできない部分については、クラウド事業者にリスクアセスメントを依頼する。
  - ・ アセスメントの結果、クラウド事業者のリスク管理に要改善事項が発見された場合には、改善要望する。

３．FinTech企業との連携

（１） オープンAPIのメリット

- API（エーピーアイ）とは「Application Programming Interface（アプリケーション・プログラミング・インタフェース）」の略。アプリケーションから、OS等のプラットフォームの機能を呼び出して利用するための、橋渡し（インターフェース）となる仕組みのことをAPIと呼ぶ。

―― 例えばGoogleは「Google Maps API」というAPIを公開しており、これを使うことで、スマホアプリ等の製作者はGoogle Mapの機能を呼び出し、利用することができる。

- 汎用性や利便性が高いプログラムをAPIとして公開することで、同様の機能をゼロから開発するためのコストが削減され、多くのサービスや製品の開発が促進される。

▼ オープンAPIのメリット

効果	効果が得られる背景
① オープンイノベーションの促進	APIを公開することにより、様々な業種の様々な職種の人が自社のサービスにアクセスすることができるようになり、自然と新たな利用方法を考えてもらうことが可能になる。結果として、自社では想定もしていなかったような新たなアイデアが生まれる可能性がある。
② 既存ビジネスの拡大	APIを公開していない場合と比較して、リーチ可能な顧客層が大きく増える。潜在顧客としても想定していなかった層が自社サービスを利用する可能性もある。また、公開したAPIの利用者に課金をすることにより、自社のデータやシステムを新たな収益源とすることができる可能性がある。
③ サービス開発の効率化	自社が公開することの直接的な効果ではないが、APIを公開する企業が増えれば、既に世の中に存在する機能をAPIとして利用することで開発コストを抑制しつつ迅速な新規サービスの開発が可能になる。

（資料） 総務省「ICTによるイノベーションと新たなエコノミー形成に関する調査研究」（平成30年）

オープンイノベーション；

自社だけでなく他社や大学、地方自治体、社会起業家など異業種、異分野が持つ技術やアイデア、サービス、ノウハウ、データ、知識などを組み合わせ、革新的なビジネスモデル、研究成果、製品開発、サービス開発、組織改革、行政改革、地域活性化、ソーシャルイノベーション等につなげるイノベーションの方法論。

- 想定される銀行のオープンAPI

（更新系API)
銀行振込等の決済サービスを外部のアプリから直接行えるようにすること

（参照系API）
家計簿ソフトや会計ソフトなどが銀行の取引明細などを読み出すこと

オープンAPIの影響

- オープンAPIによる銀行とFinTech企業の協業から、利便性の高い金融サービスが生まれる可能性。

- 差別化された利便性の高いサービスの誕生により、顧客の銀行選定基準が変化する可能性。

  （従来）

  立地条件（店舗の近さ）、店舗数、経営の安定性（どの銀行もサービス内容が同等であったことが背景）

  （今後）

  差別化された利便性の高いサービスの提供

（2） オープンAPIの現状と課題

■ 銀行法改正

- 銀行とFinTech企業の協業を促し、利便性の高い金融サービスが生まれる下地とすることを狙い、改正銀行法が成立（2017年6月公布、2018年6月施工）。

- 主な改正内容；

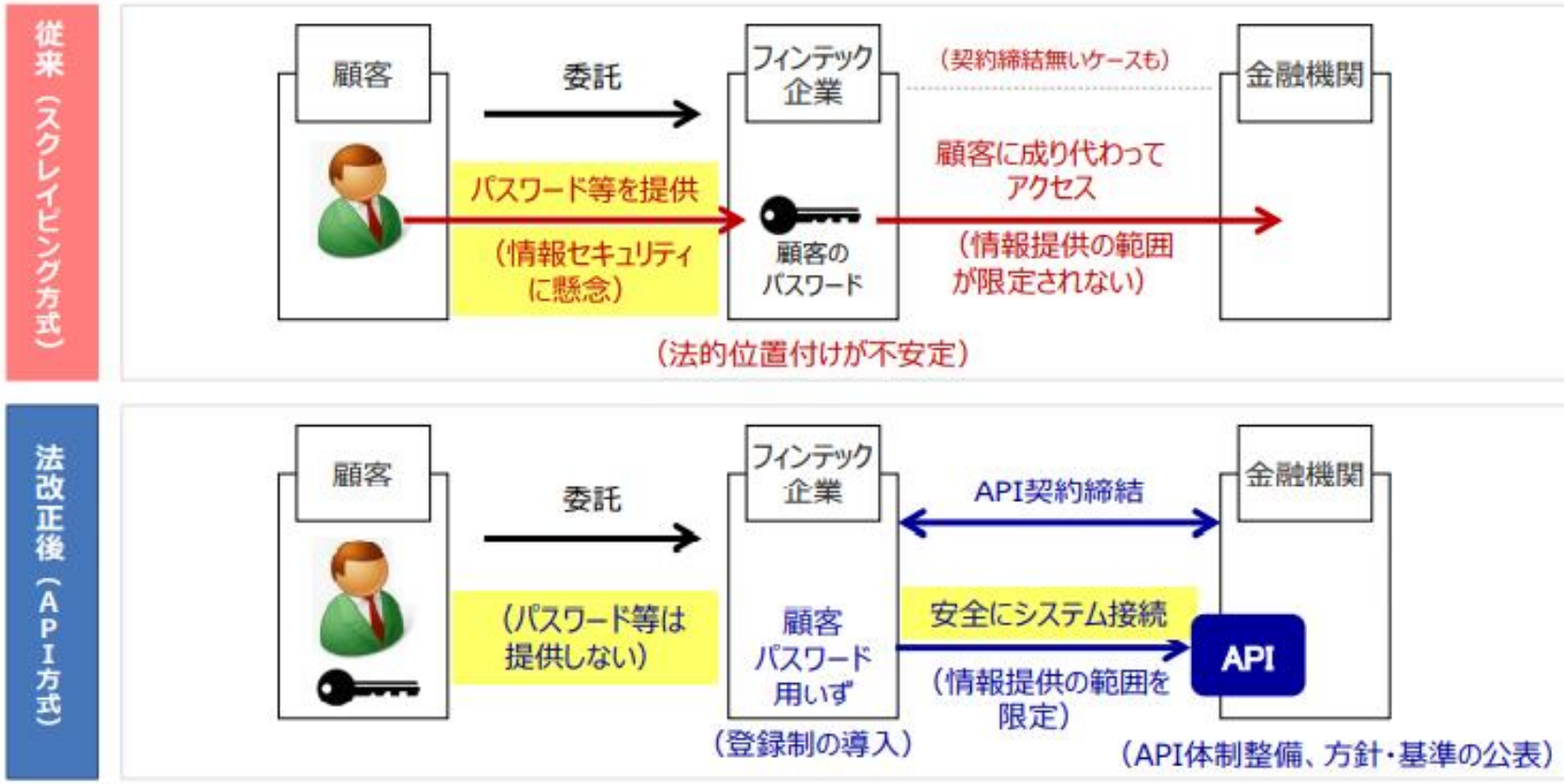
① 銀行や信用金庫に対してオープンAPI（アプリケーション・プログラミング・インタフェース）公開の努力義務を課す

―― 各銀行は正法案の公布後9カ月以内に、API公開を巡る方針を公表。公開することを表明した銀行は、法施行後2年以内をめどにAPIを整備する必要。API公開に当たっては接続に関する契約基準を明らかにし、基準を満たす事業者に対しては原則、API連携を認める必要が生じる。

② 銀行システムに接続する企業に対し、登録制を導入

―― APIに接続する事業者は「電子決済等代行業者」として金融庁に登録することが必要となる。

▼ FinTech企業の連携方式



出所；オープンAPIに対する銀行界の取り組み（2019.10全銀協）

- 2016年10月に「オープンAPIのあり方に関する検討会」が全国銀行協会を事務局として設置され、FinTech事業者や金融機関、関係省庁、有識者等との連携の下で、2017年6月にはAPI仕様の開発原則・開発標準・電文仕様標準を内容とする報告書を作成。

- 2017年6月にFISCが「API接続チェックリスト（試行版）」公表（2018年10月改訂）。

- 2018年3月2日時点で、126行がオープンAPIの導入方針表明。

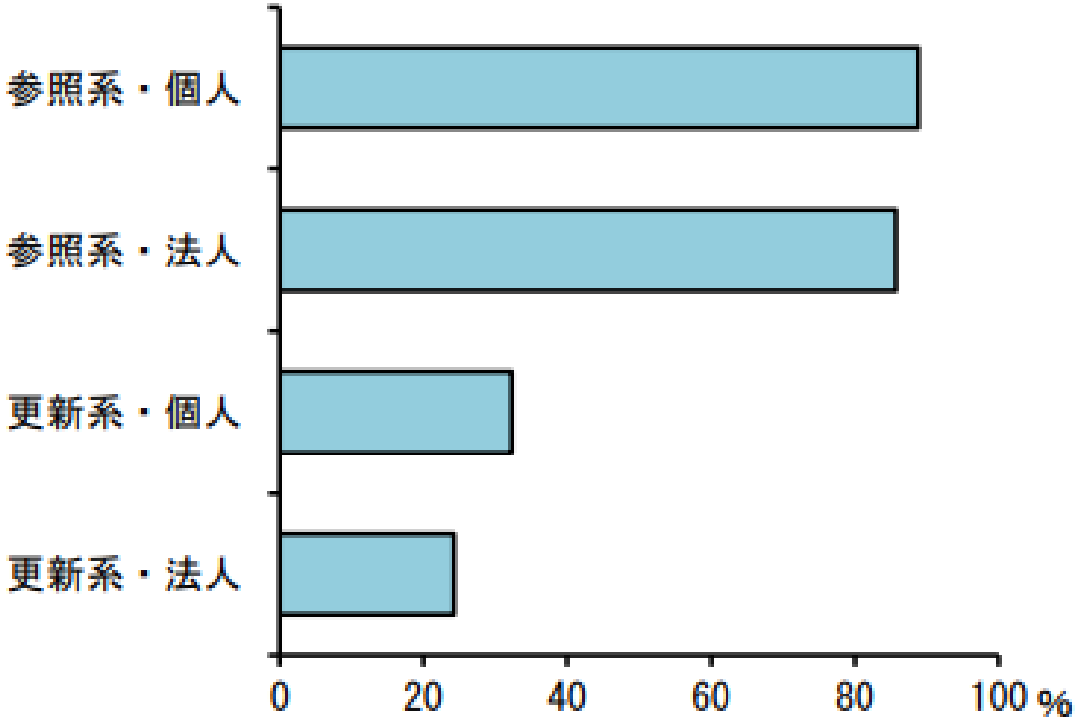
▽金融機関（138先）のAPI公開見通し(※)　（2018年3月2日時点）

		個人向け		
		未定/ 対応予定なし	参照系のみ公開	参照系と更新系を公開
法人向け	未定/ 対応予定なし	9	4	20
	参照系のみ公開	0	13	3
	参照系と更新系を公開	3	4	82

（※）各金融機関の公表資料をもとに集計

- もっとも参照系APIに比べ、更新系APIの提供は進んでいない。

▼ オープンAPIの提供状況（予定を含む）(2018年12月時点）



（注）オープン API 提供（予定）有と回答した比率。金融機関計。

出所； 銀行・信用金庫におけるデジタライゼーションへの対応状況 （日本銀行、2019.5)

■ 銀行によるオープンAPIの事例

- みずほ銀行　ー　LINE

LINEのみずほ銀行公式アカウント画面上で、専用のスタンプ（「入出金教えて！」「残高いくら？」等のスタンプ）を送ると即座に（PINや暗証番号入力の必要なしで）口座残高や直近の10取引の入出金明細が確認可能。

- 住信SBIネット銀行　ー　マネーフォワード

入出金やクレジットカードの履歴をもとに家計簿を作成して、どのようなカテゴリに支出が多いのか、カレンダーと紐づけてどの時期に支出が多いのかなどの分析が可能。また、預金、株式、投資信託などの様々な種類の資産を一括管理してポートフォリオ毎に表示し、資産全体の推移を確認するサービスも提供。

- 三井住友銀行　ー　マネーツリー

三井住友銀行は個人に提供している「三井住友銀行アプリ」に新たに家計管理サービスが追加され、その部分にマネーツリーの提供する「Moneytree LINK」を採用。同アプリ内でSMBCグループ以外の銀行口座や証券口座、クレジットカード、ポイント・マイル、電子マネーなどの金融資産や取引明細も管理ができるようになった。

- ことらプロジェクト

都銀5行（三菱UFJ銀行、三井住友銀行、みずほ銀行、りそな銀行、埼玉りそな銀行）による小口リテール決済インフラ構想（2022年9月稼働予定）。金融機関（2022年2月時点で27行参加予定）とキャッシュレスアプリケーション事業者（PayPay、LINE Pay等）とのJ-debitを活用したAPI連携プラットフォームを構築し、スマートフォンのアプリで電話番号やメールアドレスを指定することにより、個人間の少額資金送金を低い手数料で実行できるようにする。

複数行と複数FinTech業者間が広く参加できるAPI連携プラットフォーム構築という点において注目に値する。

オープンAPIの課題

- 個別の銀行とFinTech企業が連携するだけではなく、多くの銀行、FinTech企業が連携できるAPI共通基盤を構築することが必要。

- オープンAPIはあくまで手段。何を差別化し、どのようなサービスを提供できるようにするかが結局は重要。

- 膨大なデータを蓄積し、顧客との深いリレーションシップをもっているのは銀行であり、銀行が主導権を発揮してオープンAPIを活用する必要。

- FinTeck企業に対して、オープンAPIを通じて銀行のデータを利用させるだけであれば、銀行としてのうまみは少ない。銀行が銀行サービスを新規展開させていくうえで、オープンAPIを活用するとの発想が必要。

- 但し、「取引上の地位が優越する銀行が、契約の見直しを行い、電子決済等代行事業者に正常な商慣行に照らして不当に不利益を与える場合には、独占禁止法上問題となるおそれ」（2020/4月公正取引委員会「「フィンテックを活用した金融サービスの向上に向けた競争政策上の課題について」）。

（3）FinTech企業との連携におけるシステムリスク管理上の留意点

- 金融機関とFinTeck企業が連携して提供する金融サービスにおいて、金融機関とFinTeck企業のどちらに主導権があるかによって、①FinTeck企業が金融機関の外部委託先になるケースと、②ならないケースに分かれる。

- ①のケースにおいては、金融機関は他の外部委託先に関する管理と同等の管理をFinTech企業に対して実施する必要。

- ②のケースにおいては、FinTech企業の業務内容のうち、金融機関に安全対策上の責任が生じる部分について、外部委託先管理に準じて実施する必要がある。具体的には、金融機関の安全対策上の部分責任は，顧客に関するデータの提供又は受入れに由来することから，金融機関の統制の内容は，FinTech企業が顧客の本人確認や顧客データの管理を適切に実施しているか，という部分に集中することとなる。

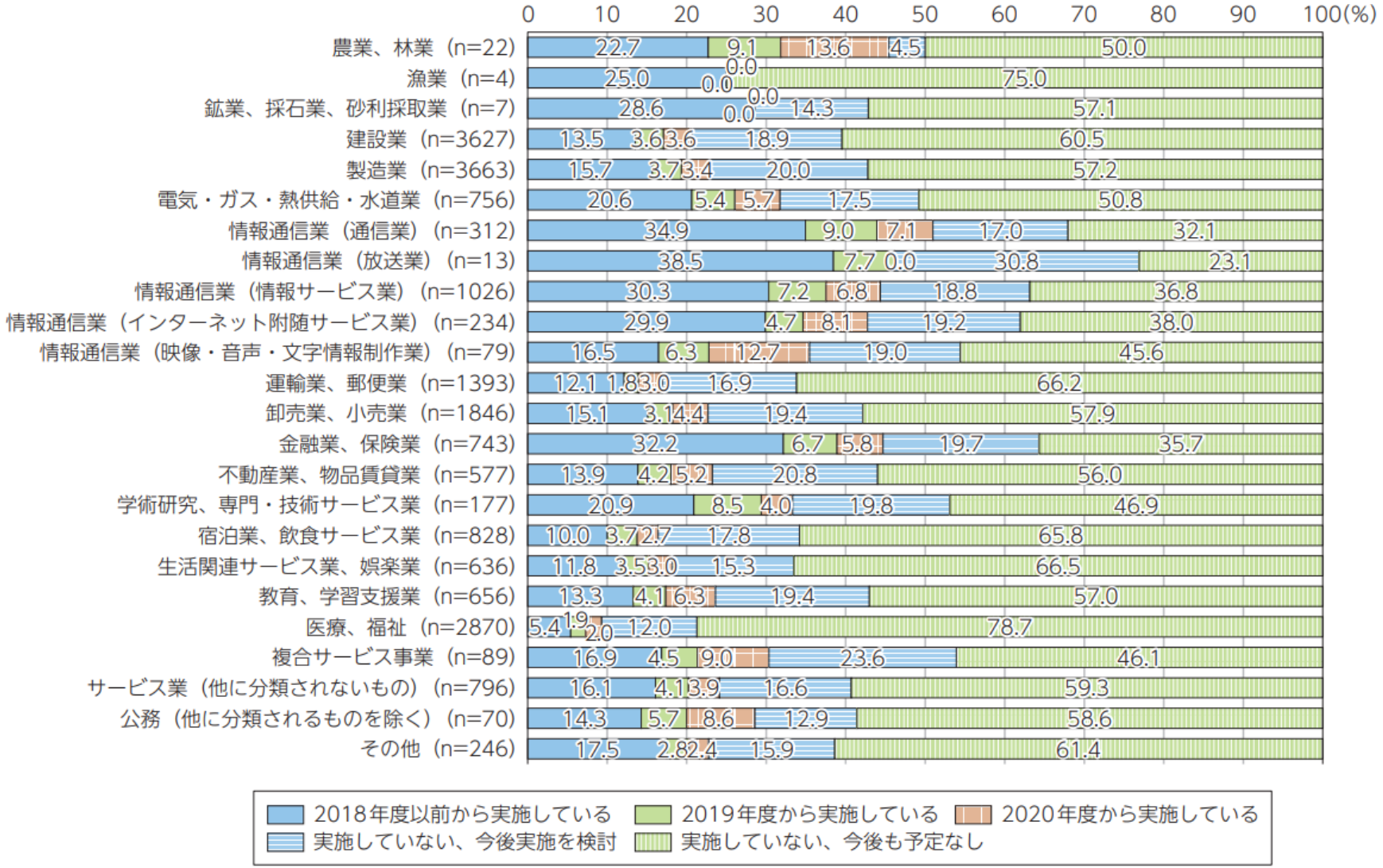
3. 金融DXの推進

（1）金融DXの現状と課題

- 金融機関は、持続可能なビジネスモデルを確保する上で、昨今のデジタル化の進展に応じたビジネス・業務の変革の動きである「デジタルトランスフォーメーション」について、取捨選択の上、必要に応じて、経営戦略に取り込むことが求められている。

- 業種別でみると、金融業・保険業が、情報通信業と並び、DXへの積極的な取り組み姿勢を示している。

▼ 業種別のデジタル･トランスフォーメーション取組状況



（出典）総務省（2021）「デジタル・トランスフォーメーションによる経済へのインパクトに関する調査研究」

■ 金融DXの事例

- MUFG　ー　Grab

MUFGは、フードデリバリーや配車サービスをコア事業とする東南アジアのプラットフォーマーであるGrab と資本提携し、ドライバーの行動情報や加盟店の売上情報等の新しいデータをベースとした、同社のドライバーや加盟店店主を顧客とする貸出サービスを提供。

- 新生銀行　ー　NTTドコモ

新生銀行は、、NTT ドコモが得られる多様なデータをもとに、ユーザーの信用スコアを算出し、同スコアを融資審査に活用する「スマートマネーレンディング」を提供。

- SMFG　ー　コマツ

SMFG はコマツと連携して、建機稼働情報などを扱う既存のデータプラットフォームに、SMFG が新設した金融分析プラットフォームを接続し、建設現場で発生する下請け・孫請け企業の資金需要にタイムリーに対応するサービスを提供。

■ 米国Goldman Sachsの取り組み

- 2015 年、当時の最高経営責任者だった Lloyd Blankfein 氏は、Goldman Sachs はテクノロジー企業になったと宣言した。当時のフルタイムの従業員 33,000 人のうちエンジニアやプログラマの数は 9,000 人。

- 2019 年、Goldman Sachs は、テクノロジーの研究開発に 40 億ドルを投資している。そのうち、53%は銀行運営のために費やし、残り 47%が将来の成長に向けた投資。

- GS Accelerate； 2018 年にスタートした、社内のイノベーションとコラボレーションを推進する全社的なプラットフォーム。開始以来、世界 37 都市から 1,400 件を超えるアイデアが提案されており、実際に 13 件のアイデアに投資が行われ、5 件のサービスがリリースされた。

- 2019 年度の年次報告において、今後の 5 年以上先を見据えた長期の投資計画で、一般消費者向けのオンライン融資や貯蓄用口座等のサービスを提供する Marcus や Apple Card、トランザクションバンキング等の新規事業やテクノロジーへの投資を加速していくとしている。

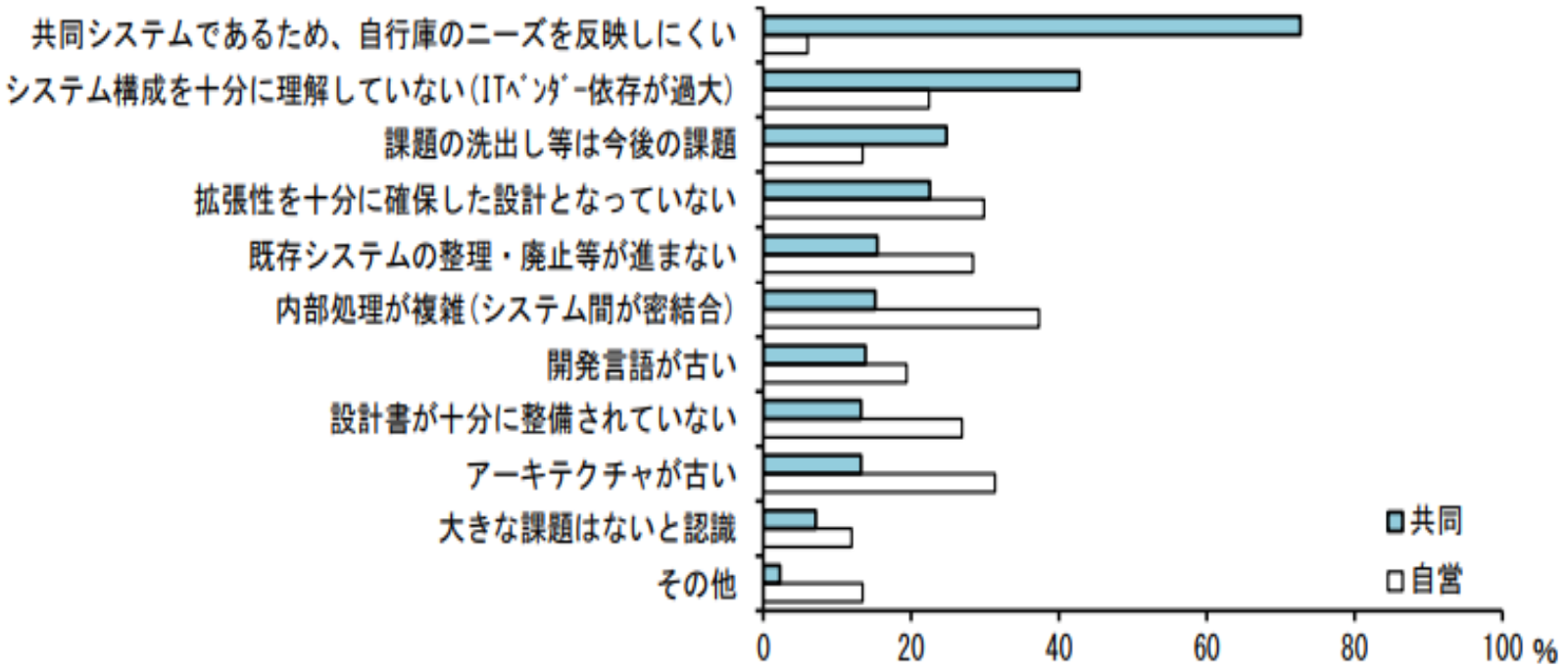
出所； 革新的技術分野の推進に向けた施策および金融分野におけるRegTech/SupTechに関する調査報告書 （三菱総研、2020.6)

■ 我が国においては、金融DXが大きな潮流となっているとまでは言えないのが現状。

（考え得る背景）

- システム内製化率の低さ、外部委託先依存度の高さ
- 特に地域金融機関におけるシステム共同化率の高さ
- システム予算不足、システム予算に占める高い既存システムの維持管理費割合
- 経営陣のリーダーシップ不足
- 将来を見据えたシステム戦略の不在

▼ IT・データ活用を推進するうえでの現行システムの課題



出所； 銀行・信用金庫におけるデジタライゼーションへの対応状況 （日本銀行、2019.5)

(2) 金融DX推進にあたって考慮すべきこと

(a) ビジネス・プラットフォームの創出

■ プラットフォームとは；

ある種の「ステージ」や「事業活動の場」。すなわち幅広い独自の能力を展開でき、しかもそこを拠点として幅広い価値創造活動を制御できる領域。

■ ビジネス・プラットフォームとは；

データ、独自のワークフロー、専門知識を組み合わせて競争優位性を高め、企業を差別化するプラットフォーム。

例）銀行のリスク管理、保険会社の請求処理、小売業者の商品化計画、消費財メーカーのサプライ・チェーンなど。

■ ビジネス・プラットフォームの種類

— 社内プラットフォーム

— 業界プラットフォーム

— 市場横断型プラットフォーム

- ビジネス・プラットフォームの成功事例

TradeLens社のブロックチェーン対応国際貿易配送プラットフォーム

同社は、複数の取引先がイベント・データの発行/登録を通じて連携し、取引状況の詳細データをプライバシー、機密性を損なわずに一元的に共有できるようにすることにより、デジタル・サプライ・チェーンのプラットフォームを構築。荷送人、海上運送人、港湾およびターミナル・オペレーター、内陸輸送、税関などは配送データや積荷書類にモノのインターネット(IoT) やセンサー・データを通じてリアルタイムでアクセスできるようになり、処理を効率化するとともに、国際貿易に携わる複数の関係者間でのデジタル・コラボレーションを可能にした。同社 は、成長するネットワークの統治、プラットフォームの構想策定、オープン・スタンダードの促進を支援するため、エコシステムの参加者からなる業界諮問委員会を設置。税関といった国家機関を含め、175組織以上が当プラットフォームを利用（2019/12月時点）。

(b) データの有効活用

- 世界のデータの約80% は企業のファイアウォールの後ろに隠されている。

（Rometty, Ginni. “We need a new era of data responsibility.” World Economic Forum. January 21, 2018）

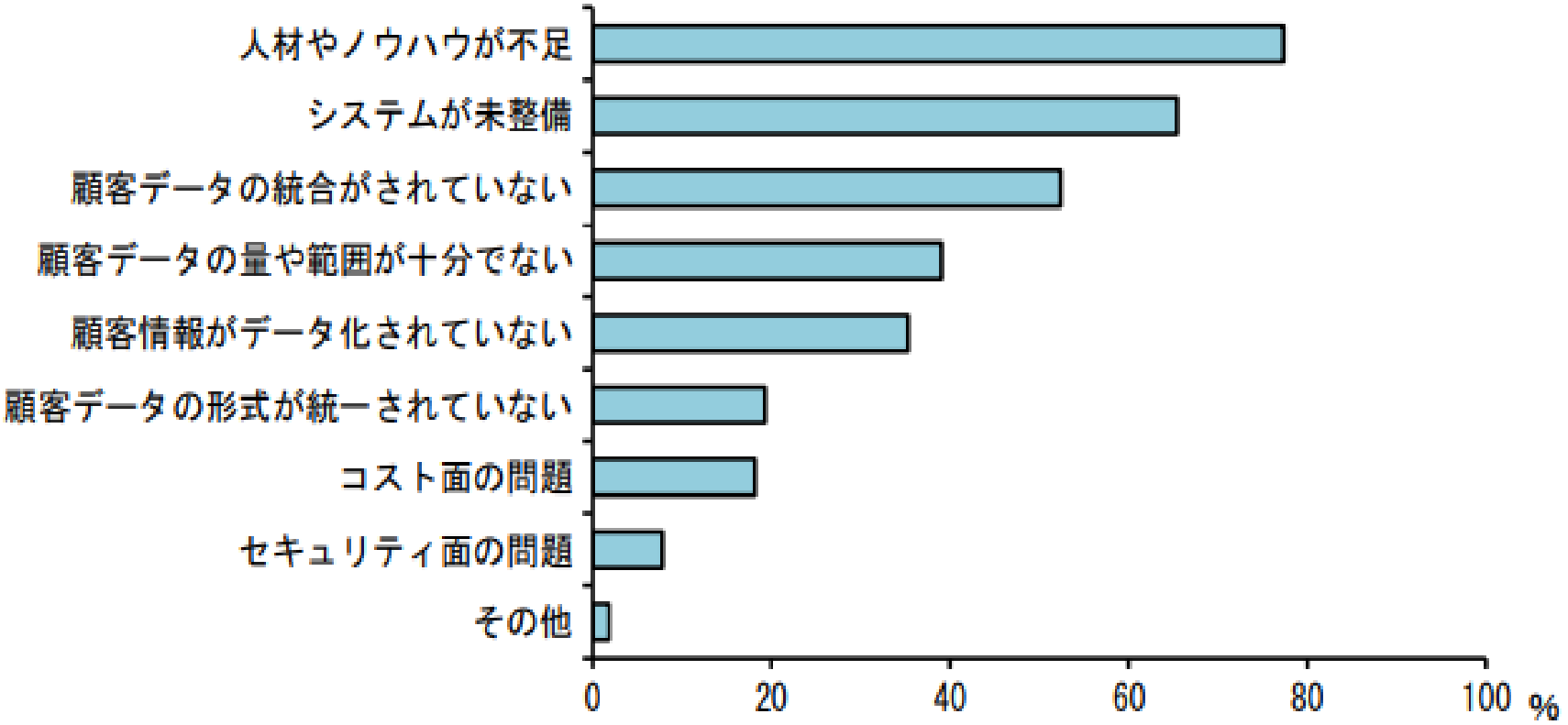
- データを利用するのはその企業の自由ではあるものの、有効活用からは程遠い状況。ビッグデータは保有しているものの、そこから洞察や価値を引き出せていない。

- 一方、プラットフォーム・ビジネス・モデルを導入した企業は、データへのテコ入れを図った結果、一般的なケースで平均の8 倍に上る収益を達成。

（Libert, Barry, Megan Beck and Jerry Wind. “The Network Imperative: How To Survive and Grow in the Age of Digital Business Models.” Harvard Business Review Press. 2016）

- 単にすべてのデータをデータ・レイクに流し込み、後はユーザーに使ってもらうのを待つばかりという方法では、もはや不十分。

▼ 金融機関において顧客データの収集・蓄積・活用を阻害している要因



出所； 銀行・信用金庫におけるデジタライゼーションへの対応状況 （日本銀行、2019.5)

- データを有効活用するためには；

① ビジネス・ニーズと「メタデータ」に裏打ちされた堅固なデータ・ガバナンス

メターデータ

データの内容と文脈の両方を説明するもので、データ間の関係、ソース、履歴を記録。データ・ガバナンスに基づきメタデータは自動生成。

② 非構造化データやリアルタイムのデータの活用

③ データの信頼性の確保、 バイアスの排除

④ AIの活用によるビジネス・プラットフォームのスマート化

AIは、データと人を関連づけ、カスタマー・エクスペリエンスを向上させる。

(c) 迅速なシステム開発

DX推進のためには、迅速なシステム開発が不可欠

- アジャイル； アジャイル（Agile）とは、直訳すると「素早い」「機敏な」「頭の回転が速い」という意味。アジャイル開発は、システムやソフトウェア開発におけるプロジェクト開発手法のひとつで、大きな単位でシステムを区切ることなく、小単位で実装とテストを繰り返して開発を進めていく。従来の開発手法に比べて開発期間が短縮される。

- DevOps； DevOps（デヴオプス）とは、アジャイル方式をソフトウェア開発から総合的なサービスの提供にまで拡大したもので、よりすぐれた製品を目指して迅速にイテレーション(繰り返し行われる短期間の開発工程) を行うために、顧客、製品管理、開発者、および品質保証との緊密な協力を必要とする。

（d）変化に対応できるアーキテクチャの選択

■ 考慮すべきポイント

I. 継続的な変化への対応

II. 新たなテクノロジー(AI、IOT, ブロックチェーン等）の導入容易性

III. アーキテクチャー・コンポーネントの疎結合

- API
- マイクロサービス （ソフトウェア開発の技法の1つであり、1つのアプリケーションを、ビジネス機能に沿った複数の小さいサービスの疎に結合された集合体として構成するサービス指向アーキテクチャ（service-oriented architecture; SOA）の1種））
- コンテナー（ホストOS上に論理的な区画（コンテナー）を作り、アプリケーションを動作させるのに必要なライブラリやアプリケーションなどを1つにまとめ、あたかも個別のサーバーのように使うことができるようにしたもの。ホストOSのリソースを論理的に分離し、複数のコンテナーで共有する。コンテナーはサーバー仮想化に比べオーバーヘッドが少ないため、軽量で高速に動作するのが特徴）

IV. オープン・スタンダードとの整合

V. レガシー・システムの統合、マイグレーション
－ プラットフォームの開発や成長を妨げているのは、自社のアーキテクチャーのどの
面か。どの部分でオープン性や柔軟性が欠けているのか。

(e) クラウドの活用

■ DX推進にあたり、継続的な変化への迅速な対応、新たなテクノロジー(AI、IOT, ブロックチェーン等）の導入容易性、コスト面での優位性を兼ね備えたクラウドを活用することは不可欠。その中でも、ハイブリッド・マルチクラウドはクラウドのメリットを最も活かせるアーキテクチャー。

ハイブリッド・クラウド； パブリック・クラウドとプライベート・クラウドの組み合わせ
ハイブリッド・マルチクラウド； 複数ベンダーのパブリック・クラウドとプライベート・クラウドの組み合わせ

ー オーケストレーション・レイヤーにより、ハイブリッド・マルチクラウドを統合的に管理したり、アプリケーションをクラウド間で簡単に移動させることが可能。

■ ハイブリッド・マルチクラウド導入のメリット

- システムの特性に基づき、様々なクラウドを組み合わせることが可能。
- 様々なクラウドベンダーから最適なサービスを選択することが可能。

（3）金融DX推進にあたってのシステムリスク管理上の留意点

（a）システム環境の変化

① クラウドサービスの利用拡大

② リモートワークの普及

③ ITシステムやデータの外部連携の増加

- 外部の攻撃から守るべき内部と外部の接点（ファイアウォールやVPN装置等）が増えることで、企業のネットワーク管理負荷が高まっていることに加え、サイバー攻撃の高度化・巧妙化により、サイバー攻撃を防ぐことが困難化し、サイバーセキュリティリスクが高まっている。

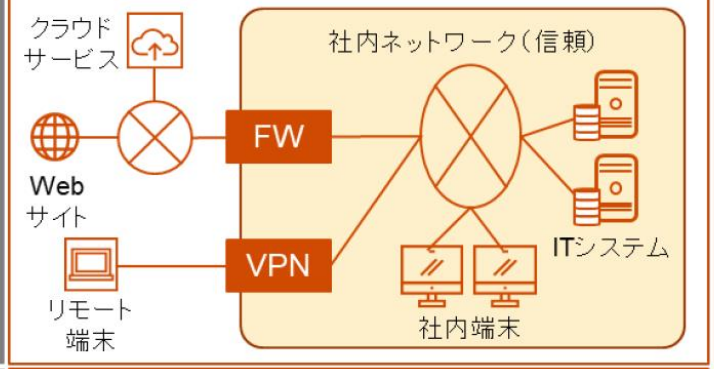
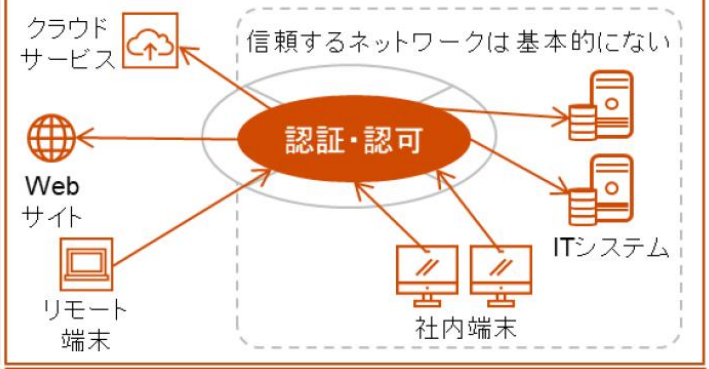
(b) ゼロトラスト

- これまでのセキュリティモデルは、ネットワーク内部を「信頼できるもの」とみなし、外部からの攻撃をファイアウォール等で防ぐ境界型セキュリティが主流。
- ゼロトラストは、内側と外側を区別せずに、すべてのアクセスを「信頼できないもの」として都度検証するセキュリティモデル。
- ゼロトラスト、「企業のネットワークやデバイスからのアクセスを暗黙に信頼せず、常にアクセスの信頼性を検証することで企業の情報資産やIT資産を保護すること」に焦点をあてたセキュリティの考え方。

ゼロトラスト・アーキテクチャのポイント

- ユーザーから企業のITシステムへのアクセスは、デバイス（社内端末、リモート端末等）が接続されたネットワークの場所を問わず、すべてのデバイスからのアクセスに対してセッション単位で認証・認可を行う。
- デバイスやITシステムの状態（IPアドレス、ソフトウェアのバージョン等）、ユーザーの挙動（接続日時、過去の動作等）、通信ログといった内部の情報に加え、脅威インテリジェンス等の外部の情報を収集し、それらの情報をもとにユーザーからのアクセス要求の信頼性を動的に判断し、アクセス可否を決定する。

境界型セキュリティとゼロトラストの違い

	境界型セキュリティ	ゼロトラスト
ネットワーク構成イメージ		
信頼するネットワーク	社内ネットワーク（FW内部のWAN、LAN）	基本的にはない ➢ ITシステムや端末を限りなく小さい単位で信頼できるか評価
情報資産・IT資産の場所	信頼できるネットワーク（社内ネットワーク、特にデータセンター）の内部	場所には依存しない ➢ アクセス元の信頼性を都度評価
端末の種類・場所	基本的には社内に設置した自社の端末を利用 ➢ 外部からはVPN等で接続	場所や端末には依存しない ➢ 信頼性を都度評価 ➢ 個人所有端末や他社の端末も利用可能
セキュリティ対策の考え方	特に重視する境界での入口対策・出口対策に、内部対策を加えた多層防御が基本 ➢ 実際には内部対策が十分でない企業が多い	社内リソースへのアクセスの信頼性を常に評価 ➢ アクセス時に信頼性を動的に評価 ➢ ITシステムや端末単位でセキュリティを確保
侵害時の拡散	ラテラルムーブメント（水平移動）により、内部の他の端末やITシステムへの拡散が懸念される	機器間の通信では常に認証・認可を行うため、拡散のリスクは低い

出所；ゼロトラストの現状調査と 事例分析に関する 調査報告書（PWC、2021.3）

ご清聴、有難うございました。

（連絡先）
日本IBMプロモントリー事業部
江見　明弘（事業部長、マネージング・ディレクター）
Email: aemi@promontory.com