

【「IT監査保証の判断基準」研究プロジェクト】

サイバー時代のITと監査

Auditing Information Technology
in the Cyber age

成田 和弘

システム監査技術者,CIA,CISA

「IT監査保証の判断基準」研究プロジェクト

主査；松尾 明（公認会計士、公認情報システム監査人、
TOGAF9認定アーキテクト）

メンバー名	所属など
石島 隆	公認会計士、システム監査技術者
遠藤 正之	博士（システムデザイン・マネジメント学）、 システム監査技術者
毛塚 恵太	PwCあらた有限責任監査法人
杉山 哲男	大和ネクスト銀行
鈴木 夏彦	日本電気（株）
長野 加代子	（株）ピーアンドアイ
成田 和弘	システム監査技術者、CIA、CISA
米川 弘幸	システム監査技術者、CISA

※ 五十音順

2

「IT監査保証の判断基準」研究プロジェクト

■ 概要

- ドラッカーの『テクノロジストの条件』を基本書として用い、その後の環境変化を再認識し、理論的背景としてまとめて公表する

■ 2016年度活動成果

- システムプロジェクト評価の研究
- COSO in the Cyber Ageの仮翻訳と研究
- 米国のヘルスケアの動向の研究
- FinTech等の金融の動向の研究
- サイバーセキュリティ対応等の日米比較

3

自己紹介

■ 銀行員（営業店も経験）

■ システムは…ちょうど30年の経験

- 勘定系システム、分散システムインフラ構築、セキュリティポリシー策定、システムアライアンス（関連IT会社設立など）、職員組合中央執行委員（委員長）、インターネット議決権行使、CRMシステム、IT投資管理、IT戦略の策定、各開発案件の立ち上げ・推進・プロジェクトマネジメント、合併・システム統合、大規模アウトソーシング契約の締結、BCP/DR体制構築等
- システム監査は6年、現在はシステム開発の品質管理
- CIA、CISA、情報処理技術者（ITストラテジスト、上級シスアド、システムアナリスト、プロジェクトマネージャー、システム監査、情報セキュリティアドミニストレータ、データベース）
- システム監査学会 理事、「法とシステム監査」研究プロジェクト、「IT監査保証の判断基準」研究プロジェクト、「ITを利用したガバナンス」研究プロジェクト
- ISACA 基準委員会委員、法務委員会委員、メンバーシップ委員会委員、COBIT研究会、情報セキュリティ研究会、内部監査におけるシステム監査研究会
- IIA CIAフォーラム ベストプラクティス（金融）研究会、IT監査ケーススタディ研究会
- PMI プロジェクトマネジメント研究会

…他

4

Agenda

- ヘルスケアの動向とテクノロジー
- FinTechのテクノロジーと動向
- サイバー時代の
テクノロジーマネジメントと内部統制
- 日本のITの現状と課題解決へのアイデア
- サイバー時代の監査

5

ヘルスケアの 動向とテクノロジー



6

ヘルスケアの動向とテクノロジー

米国の医療保険制度

- 医療保険の相互運用性と責任に関する法律 (HIPAA; 1996年)
 - 労働者の転職・失業時の健康保険の保護
 - 電子医療取引の標準化と導入の推進
 - 経済的および臨床的健全性のための医療情報技術に関する法律 (HITECH; 2009年)
 - 電子健康記録 (EHR)
 - プライバシー規定とセキュリティ規定
 - 患者保護並びに医療費負担適正化法 (PPACA; 2010年;**オバマケア**)
 - 保険未加入者への加入促進策
 - トランザクションの運用ルール、保険の識別子、電子的な資金送金および電子ヘルスケア請求の添付書類の基準
- **医療保険制度の向上・普及促進とともに、医療・保険事務の電子化による効率化を国が推進**

出典：CMS, Transactions Overview, <https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Transactions/TransactionsOverview.html>

7

ヘルスケアの動向とテクノロジー

米国のヘルスケア政策

- 保健社会福祉省(HHS)
 - **メディケア・メディケイド・サービスセンター(CMS)**
 - 国民医療保障プログラムと関連基準を管轄
 - **管理の簡略化**
 - 書類削減、医療制度全体のビジネスプロセス合理化
 - 電子取引、コードセット、一意の識別子の管理
 - **国家保健情報センター(ONC)**
 - 最先端の健康情報技術と健康情報の電子交換実施の調整
 - **連邦保健アーキテクチャ(FHA)**
 - 相互運用性のある電子カルテ
 - **連邦保健相互運用性モデリング標準(FHIMS)**
 - 各種現行標準間の調整、統合

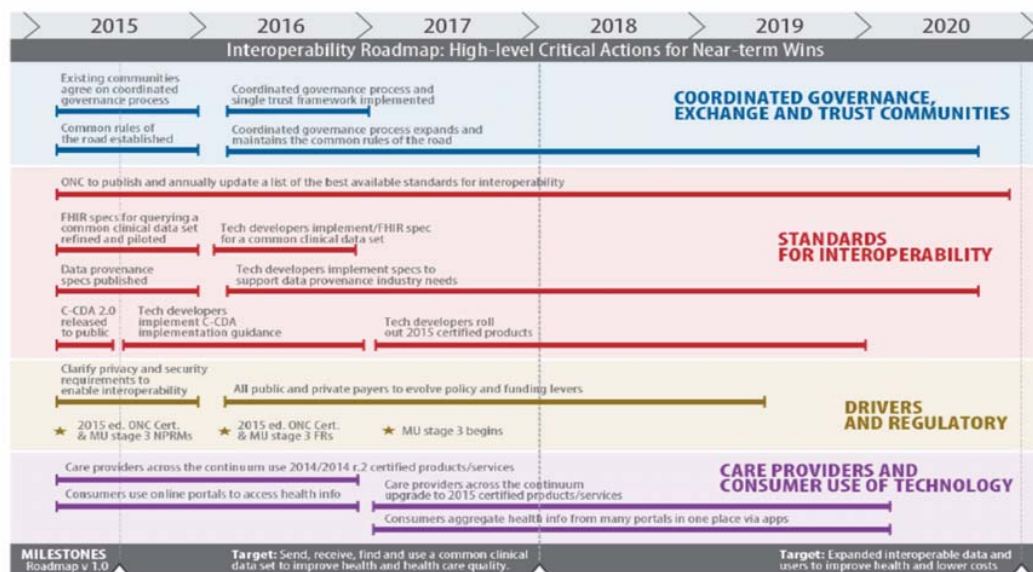
出典：CMS, About CMS, <https://www.cms.gov/About-CMS/About-CMS.html>, HealthIT.com, About ONC, <https://www.healthit.gov/newsroom/about-onc>, HealthIT.com, Federal Health Architecture (FHA), <https://www.healthit.gov/policy-researchers-implementers/federal-health-architecture-fha>, FHIMS.ORG, The FHIMS Program, <http://www.fhims.org/index.html>

8

ヘルスケアの動向とテクノロジー

連邦保健アーキテクチャ（FHA）のロードマップ

Figure 2: Timeline of Select High-Level Critical Actions for Near-Term Wins



Disclaimer: Timeframes noted are approximate estimates.

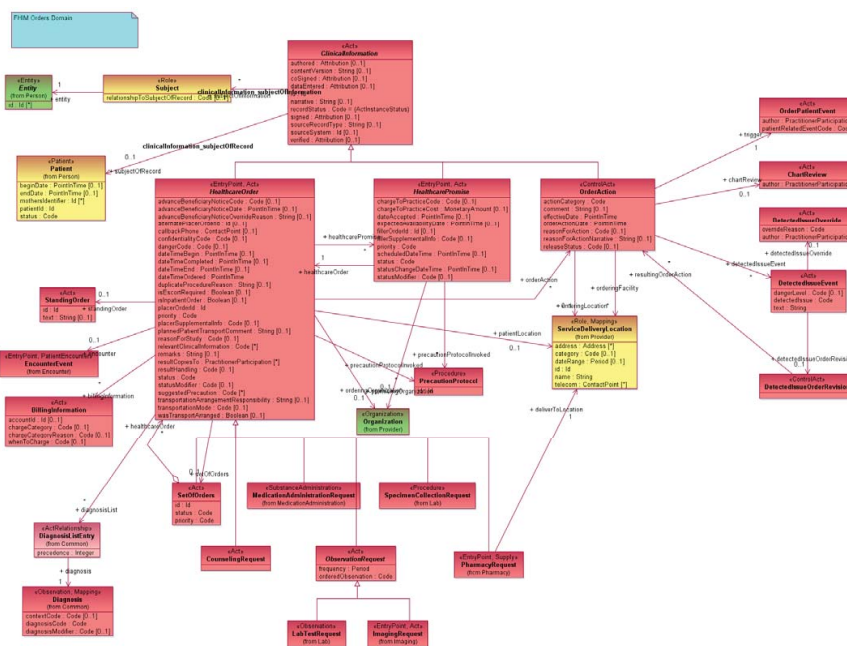
出典：国家保健情報センター，Connecting Health and Care for the Nation A Shared Nationwide Interoperability Roadmap DRAFT Version 1.0, <https://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf>

9

ヘルスケアの動向とテクノロジー

連邦保健相互運用性モデリング標準(FHIMS)

■ Orders



出典 : FHIMS.ORG, FHIM::Orders::Orders, http://www.fhims.org/content/420A62FD03B6_root.html

10

ヘルスケアの動向とテクノロジー

日本におけるヘルスケアの取組みと課題

- 健康・医療戦略推進本部
 - **健康・医療戦略**（2014年7月22日閣議決定）
 - 医療等データ利活用基盤構築・ICT 利活用推進
 - **2020年までの達成目標は、医療・介護・健康分野のデジタル基盤を構築し、医療等情報を利用すること**
- 次世代医療ICT基盤協議会
 - **「医療情報取扱制度調整ワーキンググループとりまとめ」**（2016年12月）
 - **医療情報匿名加工・提供機関の制度化と認定**
 - 認定された医療情報匿名加工・提供機関が、収集・蓄積した情報を匿名加工した上で、ビッグデータとして医療行政や、研究機関・製薬企業等の利用に供する
 - **共通の基盤を整備する支援機関の創設**
 - データの統一的な利活用実現のため、国が主導して相互の連携のための共通の基盤を整備

出典：次世代医療ICT基盤協議会, 医療情報取扱制度調整ワーキンググループとりまとめ, 2016.12,
http://www.kantei.go.jp/jp/singi/kenkouiryou/jisedai_kiban/pdf/161227_wg-b_torimatome.pdf

11

FinTechの テクノロジーと動向



12

■ Data Sharing and Open Data for Banks

(2014年)

■ 「銀行間の競争と消費者の利益」に銀行APIを活用

- 英国規制当局が推進
- データ保護とプライバシーの設計原則
- 匿名化情報の公開
- 技術標準
 - ユースケース毎の標準化
 - 口座移管, 事業融資, マネー管理, 決済, 口座振替, 本人確認, オープンデータの公開
 - 個人情報へのアクセス技術
 - REST, JSON, HTTPS/ HSTS/ TLS, OAuth2.0

■ Open Banking Standard (2015年)

- 仕様等の体系、要件、基本原則などが定められ、**詳細な仕様やルールを、工程表に沿って2019年3月までに順次策定**する計画

出典：Open Data Institute, Data sharing and open data for banks, 2014.12,
<http://https://www.gov.uk/government/publications/data-sharing-and-open-data-for-banks>
 Open Data Institute, The Open Banking Standard, 2015.9, <https://theodi.org/open-banking-standard>

13

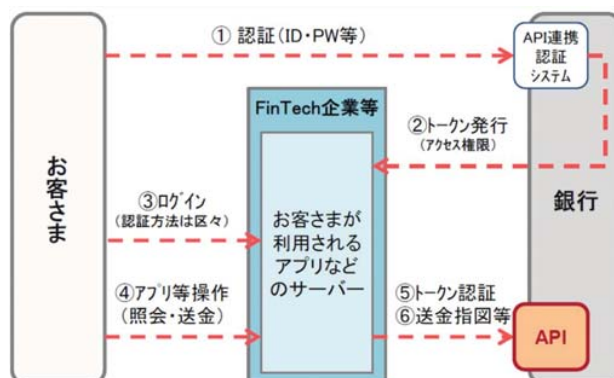
■ 銀行法等の一部を改正する法律 2017.5.26成立

- 電子決済等代行業の登録制
- 電子決済等代行業者との連携協働方針、接続基準の策定と公表、導入の努力義務

■ 「オープンAPIのあり方に関する検討会報告書 (全国銀行協会 2017年3月)

- API仕様の標準化
- セキュリティ対策
- 利用者保護

…の基本的な考え方



オープンAPIの基本的な仕組み (OAuth2.0)

出典：金融庁, 国会提出法案 (第193回国会) 銀行法等の一部を改正する法律案,
<http://www.fsa.go.jp/common/diet/193/01/riyuu.pdf>
 全国銀行協会, オープンAPIのあり方に関する検討会報告書, 2017,
https://www.zenginkyo.or.jp/fileadmin/res/news/news290316_2.pdf

14

FinTechのテクノロジーと動向

ブロックチェーン技術

- ブロックチェーン；多数のレコードをブロック化し、暗号署名で、次のブロックと結合。

➤ **改ざんが困難な記録技術**

- 様々なブロックチェーンプラットフォーム

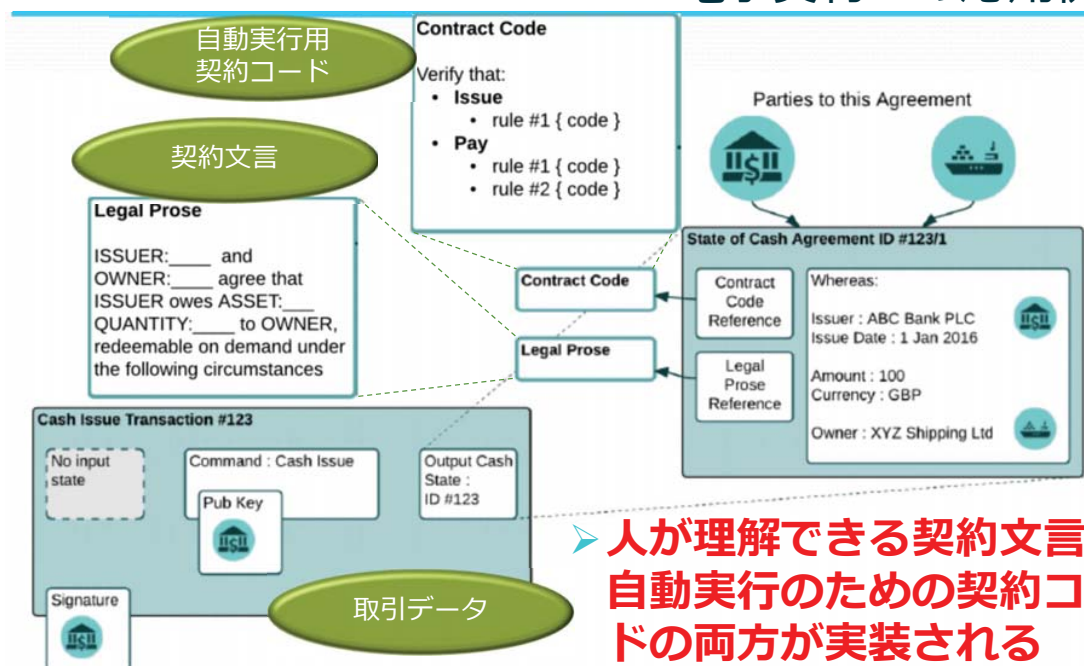
	パブリック型	コンソーシアム型	プライベート型
管理主体	なし	複数組織	単一組織
参加者	自由	許可制	
コンセンサス	マイニング	コアノードによる合議制	
処理時間	長い	短い	
実装例	仮想通貨(Bitcoin, Ethereum, etc)	銀行間送金、証券取引等(Ripple, Hyperledger Fabric, etc)	

経済産業省,ブロックチェーン技術を活用したシステムの評価軸整備等に係る調査 調査報告書, 表2-3をもとに作成
 出典：UK Government Chief Scientific Adviser, Distributed Ledger Technology: beyond block chain, 2016,
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf,
 経済産業省,ブロックチェーン技術を活用したシステムの評価軸整備等に係る調査 調査報告書, 2017,
http://www.meti.go.jp/english/press/2017/pdf/0329_004b.pdf

15

FinTechのテクノロジーと動向

電子契約への応用例



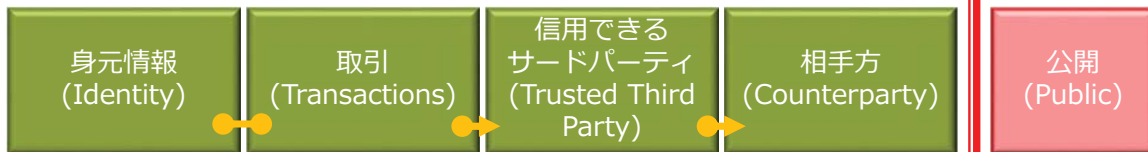
出典：Richard Gendal Brown, James Carlyle, Ian Grigg, Mike Hearn, Corda: An Introduction, Figure 2 & Figure 4, 2016.8, https://docs.corda.net/_static/corda-introductory-whitepaper.pdf

16

FinTechのテクノロジーと動向

仮想通貨ビットコイン

■ 伝統的なプライバシーモデル



■ ビットコインのプライバシーモデル

- ビットコインは、お金を渡したことを取り消せないようにする仕掛け（秘密鍵を失うとすべて失う）
- **全取引が公開**される代わりに、**身元情報を秘匿**

➤ **ブロックチェーンの用途は多種多様**

出典：Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System,
<https://bitcoin.org/bitcoin.pdf#search=%27Satoshi+Nakamoto%27>

17

FinTechのテクノロジーと動向

日本におけるブロックチェーン技術への取り組み

■ 「ブロックチェーン連携プラットフォーム」(仮称)

- 連携・協働型の実証実験環境

➤ **信用できる電子証明書の普及が鍵**

■ 情報通信技術の進展等の環境変化に対応するための銀行法等の一部を改正する法律 2016.5.25成立

- 仮想通貨の交換業者の登録制
- **マネロン・テロ資金供与対策規制（本人確認）**
- 預託金銭の分別管理等の利用者保護

出典：金融庁、情報通信技術の進展等の環境変化に対応するための銀行法等の一部を改正する法律の概要,
<http://www.fsa.go.jp/common/diet/190/01/gaiyou.pdf>
 全国銀行協会、ブロックチェーン連携プラットフォーム（仮称）の基本構想, 2017,
<https://www.zenginkyo.or.jp/fileadmin/res/news/news290413.pdf>

18

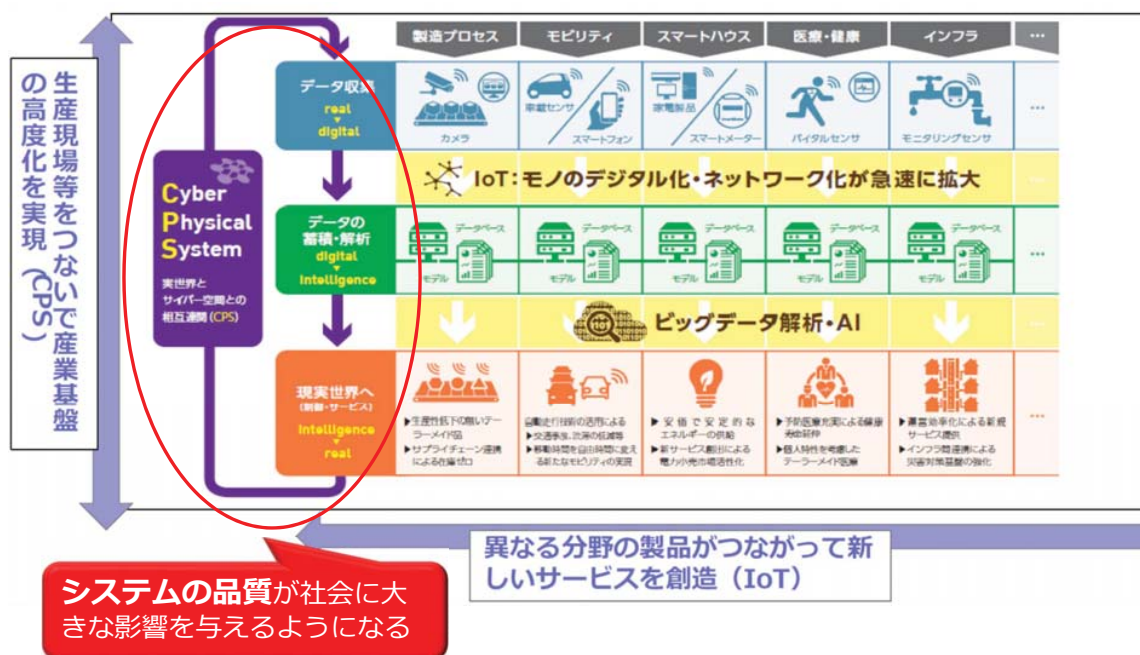
サイバー時代の テクノロジーマネジメント と内部統制



19

サイバー時代のテクノロジーマネジメントと内部統制

サイバーフィジカルシステムの時代



出典：IPA, つながる世界の開発指針, 2016

20

サイバー時代のテクノロジーマネジメントと内部統制

ドラッカーの炯眼・・・技術革命と情報革命

- 文字の発明
 - 灌漑文明において技術が人間の生活にもたらした大革命が四大文明を生んだ
 - 統治の機構(非属人的な政府と官僚),社会的な階層,知識の体系化と制度化(文字,学校と教師,自然の法則),個人(美術,文学,宗教)
- 印刷の発明
 - **活版印刷による書物の大量生産が社会を一新し、技術革命を意図して体系的に行えるようになった**
 - 蒸気機関,蒸気船,鉄道,郵便,光学機械,電信 …
 - **蒸気機関の50年後に鉄道が世界を一変させた**
 - 新産業と新技術が既存の産業と事業を陳腐化
 - 既存企業は**新技術をマネジメントして、自己革新を行うことを迫られている。**

出典：P.F.ドラッカー, テクノロジストの条件, 2005,ダイヤモンド社

21

サイバー時代のテクノロジーマネジメントと内部統制

ドラッカーの炯眼・・・IT革命は産業革命になれるか

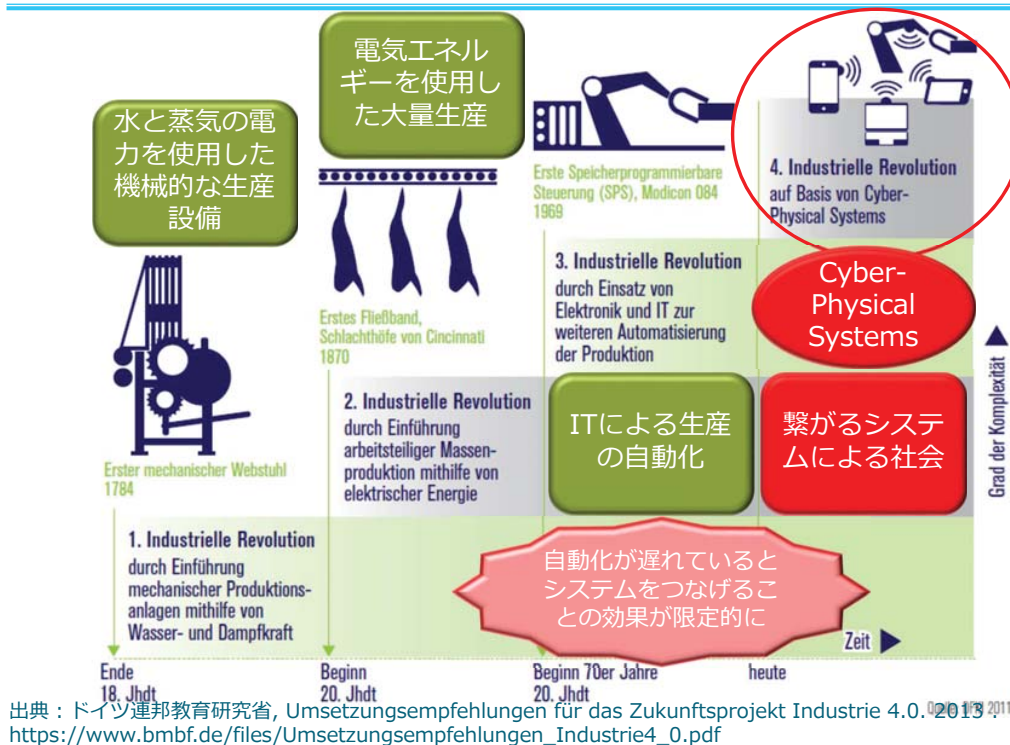
- コンピュータの出現
 - 単なる高速の計算機ではない「情報機器」であり、「情報理論」と「情報技術」が必要になる
- **現在はプロセスのルーチン化にとどまる**
 - IT革命は、今日までのところ、IT革命前から存在していたもののプロセスを高速化したにすぎない。実体上はいささかの变化ももたらしていない。
- **eコマースは産業革命の鉄道**
 - 170年前の鉄道を同じように経済と社会と政治を一変させる。距離が消え、**中小企業でさえグローバルな競争力を必要とする。**
- **これからさらに相当数の新産業が生まれる**
 - 多くはIT、コンピュータ、インターネット関連ではない。(バイオ、魚の養殖…)

出典：P.F.ドラッカー, テクノロジストの条件, 2005,ダイヤモンド社

22

サイバー時代のテクノロジーマネジメントと内部統制

ITと第4次産業革命



23

サイバー時代のテクノロジーマネジメントと内部統制

ドラッカーからの宿題

- われわれは技術革命がもたらしつつある**新しいニーズと新しい能力にふさわしい新しい制度を構築し**、われわれの信ずる価値観を具体化させ、われわれが正しいと考える目的を追求し、**人間の自由、尊厳、目的に奉仕**させなければならない。

出典：P.F.ドラッカー, テクノロジストの条件, 2005,ダイヤモンド社

24

サイバー時代のテクノロジーマネジメントと内部統制

COSO IN THE CYBER AGE

- COSO (トレッドウェイ委員会支援組織委員会)
 - 「内部統制の統合的枠組み」 (1992年)
 - **企業不正の発生を防止する内部統制の枠組み**
 - 米SOX法は内部統制システムの構築・運用と有効性の検証を義務化
 - 「**内部統制の統合的フレームワーク**」 (2013年)
 - **進展するテクノロジーの利用等17の原則**

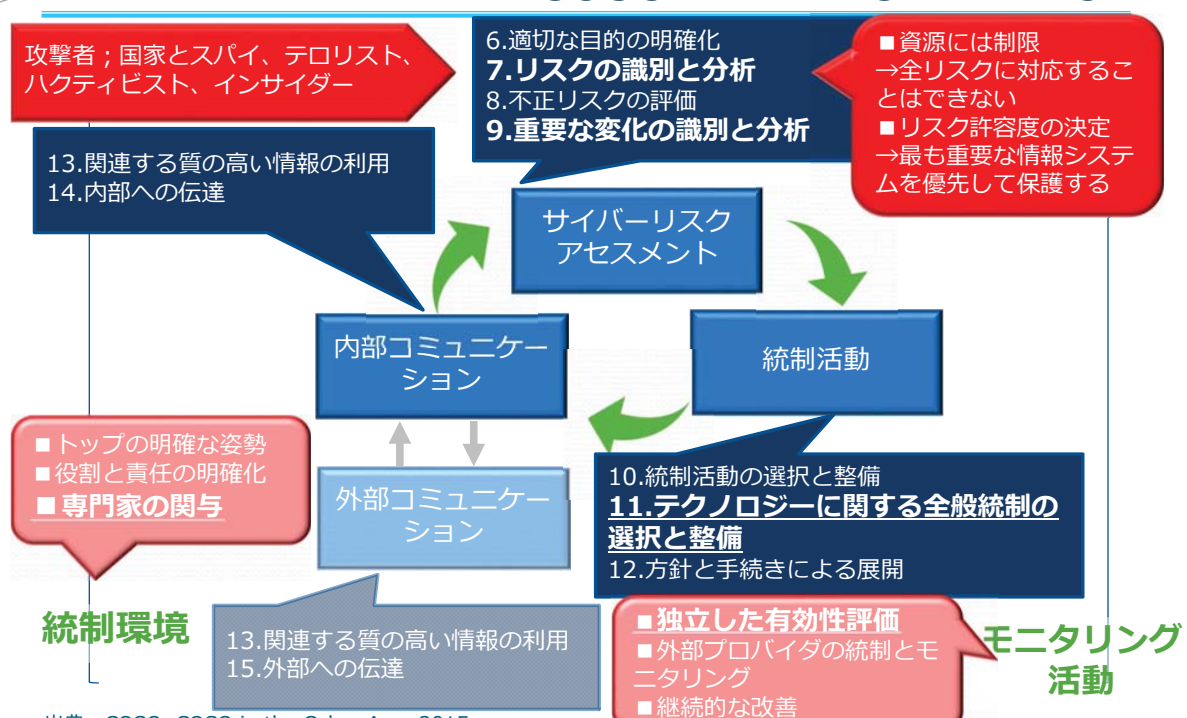
統制環境	リスク評価	統制活動	情報と伝達	モニタリング活動
1.誠実性と倫理観へのコミットメントの表明 2.監督責任を果たす 3.組織、権限と責任の確立 4.能力に対するコミットメントの表明 5.説明責任を強化する	6.適切な目的の明確化 7.リスクの識別と分析 8.不正リスクの評価 9.重要な変化の識別と分析	10.統制活動の選択と整備 11.テクノロジーに関する全般統制の選択と整備 12.方針と手続きによる展開	13.関連する質の高い情報の利用 14.内部への伝達 15.外部への伝達	16.日常的なおよび/または独立した評価の実施 17.不備の評価と伝達

出典：COSO, COSO in the Cyber Age, 2015,
https://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf

25

サイバー時代のテクノロジーマネジメントと内部統制

COSO IN THE CYBER AGE



出典：COSO, COSO in the Cyber Age, 2015,
https://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf

26

サイバー時代のテクノロジーマネジメントと内部統制

三線防御モデル

■ 透明性の高い内部統制と第三者による評価

防御ライン	例	取り組み方
第一線	フロントオフィス、お客様窓口	取引ベース、リアルタイム
第二線	リスクマネジメント、コンプライアンス、法務、人事、財務、事務、システム	リスクベース、リアルタイムまたは定期的
第三線	内部監査	リスクベース、定期的

- 機能別専門家である第二線が適切に枠組みを管理し、第一線が責任をもってリスクに対応
- 上記から独立し、組織横断的に強力な閲覧権をもつ内部監査がリスクベースで確認することで、**透明性の高い内部統制を実現**

自らのプロセスの評価・改善を行う能力が組織の信用に直結する

出典：Basel Committee on Banking Supervision. The internal audit function in banks, 2012.
<http://www.bis.org/publ/bcbs223.htm>

27

日本のITの現状と
対策のアイディア

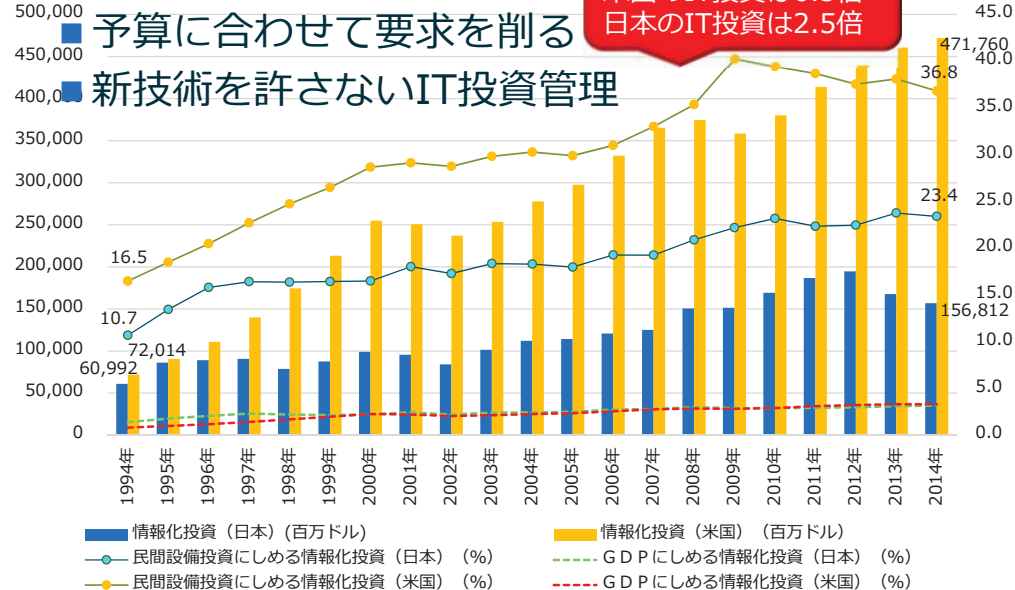


28

日本のITの現状と対策のアイディア

日米の情報化投資の差

IT投資をケチった日本

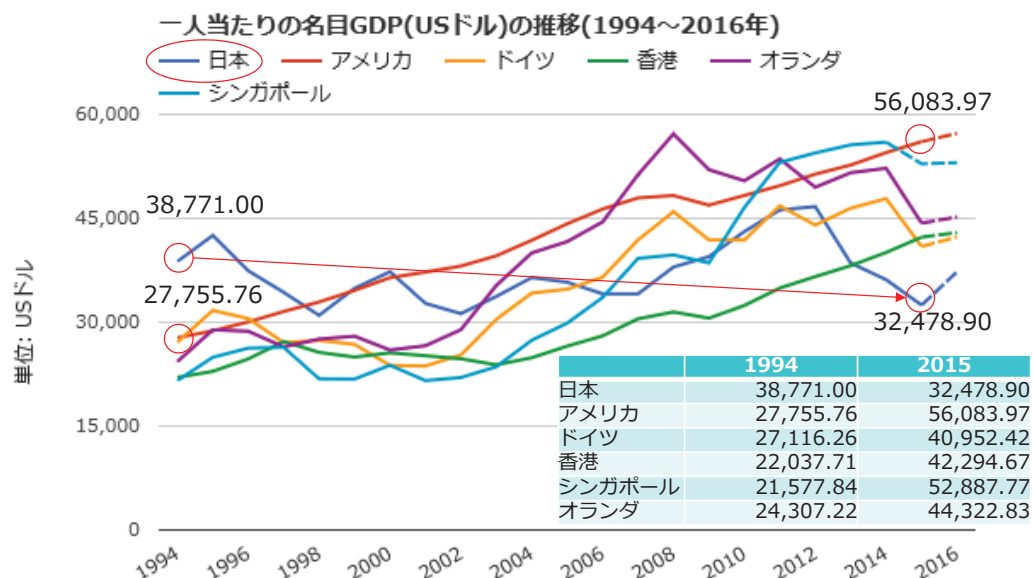


29

日本のITの現状と対策のアイディア

20年前より低い日本の生産性

テクノロジーマネジメントの失敗との指摘



出典：世界経済のネタ帳
http://ecodb.net/exec/trans_country.php?type=WEO&d=NGDPDPC&c1=JP&c2=US&c3=DE&c4=HK&c5=NL&c6=SG&s=1994&e=2016

30

日本のITの現状と対策のアイディア

新しい技術に弱く、新ビジネスに冷たい日本

- 米国
 - 1998年頃の通信関連銘柄への投資が、**グーグル、アマゾンなど新たな経済**を生んだ
- 日本
 - ソフトバンク、楽天など新興勢力と既得権益との対立
 - 世界でも屈指の通信インフラを整備したが、**インターネットに適合した規制改革は途上**
 - **マイナンバーカードの交付率8.4%（2017年3月）**
- エストニア（1991年に独立を回復した人口130万の国）
 - 独立直後から**インターネットを徹底活用したICT立国**
 - 2002年から**全国民にeIDを配布**、投票、医療等をすでに電子化し、**電子政府のお手本**とされる

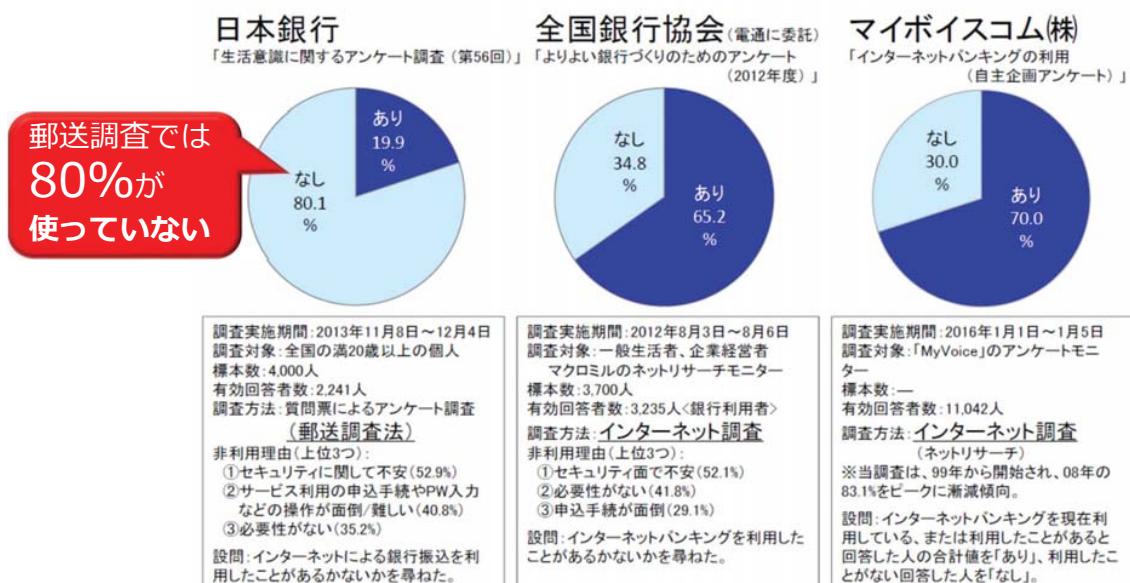
出典：総務省、マイナンバーカードの市区町村別交付枚数等の公表について(平成29年3月8日現在)、
http://www.soumu.go.jp/main_content/000472674.pdf
 ラウル・アリキヴィ、前田陽二、未来型国家エストニアの挑戦、2016、インプレイスR&D

31

日本のITの現状と対策のアイディア

いまだに進まないインターネットの活用

個人顧客向けインターネット・バンキングの利用率調査



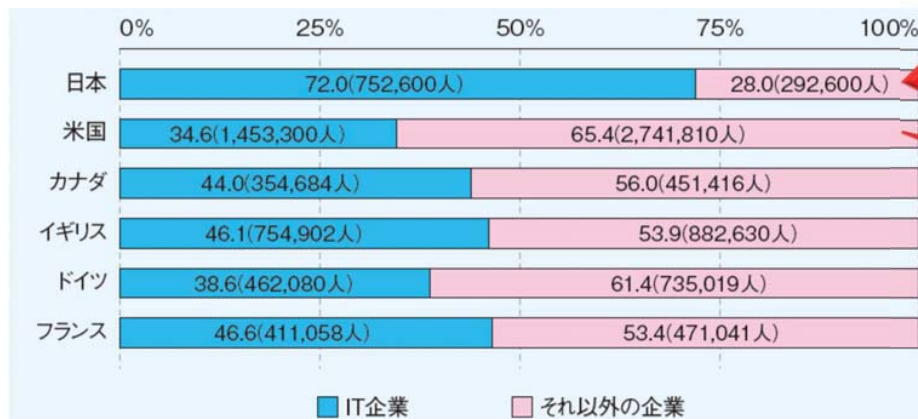
出典：インターネットと銀行サービスの再考、日本銀行 岩下直行、2016年
https://www.boj.or.jp/announcements/release_2016/data/rel160314a2.pdf

32

日本のITの現状と対策のアイディア

日本のIT技術者の遍在と不遇

■ IT人材の所属先毎の割合



日本企業は、
多重下請けの
外部委託でIT
開発

米国企業は、
必要なIT人材
を雇用して自
らIT開発

- ユーザー企業のITはIT企業に頼らざるを得ない
- 日本のIT人材の年収…**本当に人が足りないと思ってる？**
 - **米国**のプログラマの年収は平均年収の**174.6%**
 - 日本**のプログラマの年収は平均年収の**83.5%**

出典：IPA，IT人材白書2017，http://www.ipa.go.jp/jinzai/jigyoku/hakusyo_dl_2017.html

33

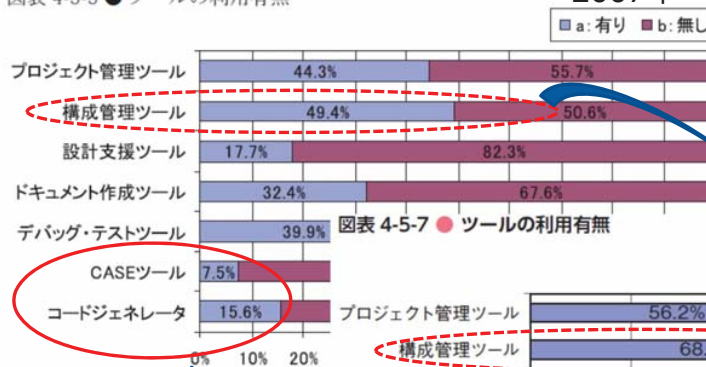
日本のITの現状と対策のアイディア

IT技術者は複雑化するシステムに素手で取り組んでいる

■ IT業務の自動化は進んでいない

図表 4-5-5 ● ツールの利用有無

2007年



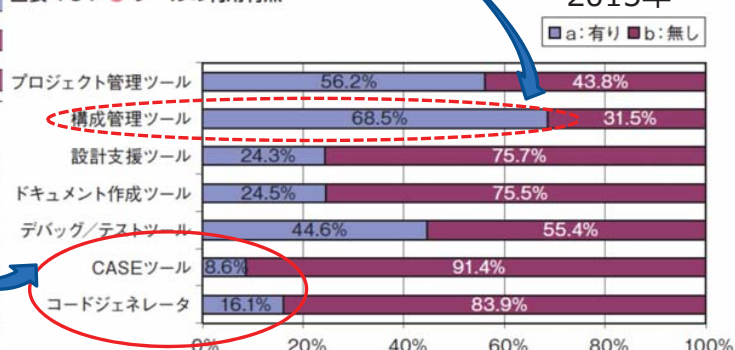
■ **96.8%は役割分
担を明確化しやす
いウォーター
フォール型で開発**

管理ツールは普及

2015年

- **開発スタイルは
10年前と
変わらない**

図表 4-5-7 ● ツールの利用有無



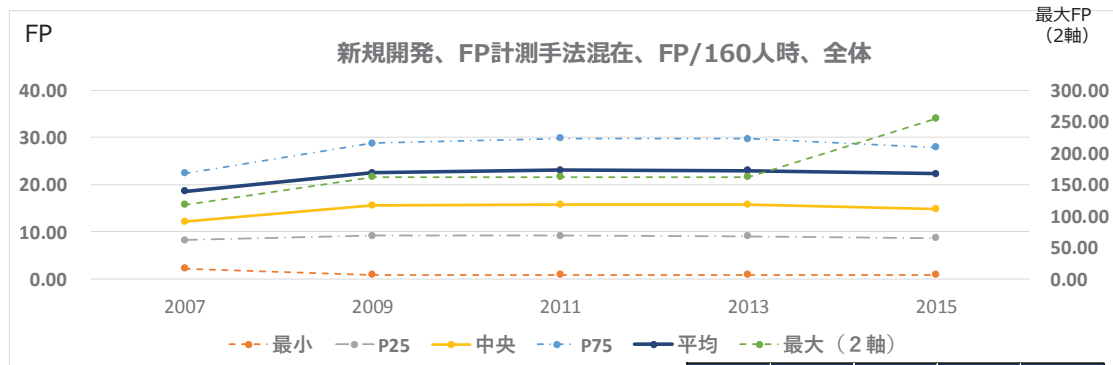
出典：IPA，ソフトウェア開発データ白書2008年，ソフトウェア開発データ白書2016-2017年

34

日本のITの現状と対策のアイデア

ITの生産性は維持するのがやっと

■FP生産性の推移（1人月≒160人時あたり）



➤ 打ち手がないので
ITの生産性は
変わっていない

	2007	2009	2011	2013	2015
N	242	444	516	566	626
最小	2.13	0.84	0.84	0.84	0.84
P25	8.15	9.18	9.10	9.06	8.70
中央	12.21	15.57	15.82	15.76	14.89
P75	22.43	28.77	29.82	29.78	27.94
最大 (2軸)	118.21	162.51	162.51	162.51	255.43
平均	18.57	22.54	23.07	22.93	22.32

出典：IPA、「ソフトウェア開発データ白書2008年」「ソフトウェア開発データ白書2010-2011年」
「ソフトウェア開発データ白書2012-2013年」「ソフトウェア開発データ白書2014-2015年」
「ソフトウェア開発データ白書2016-2017年」より作成

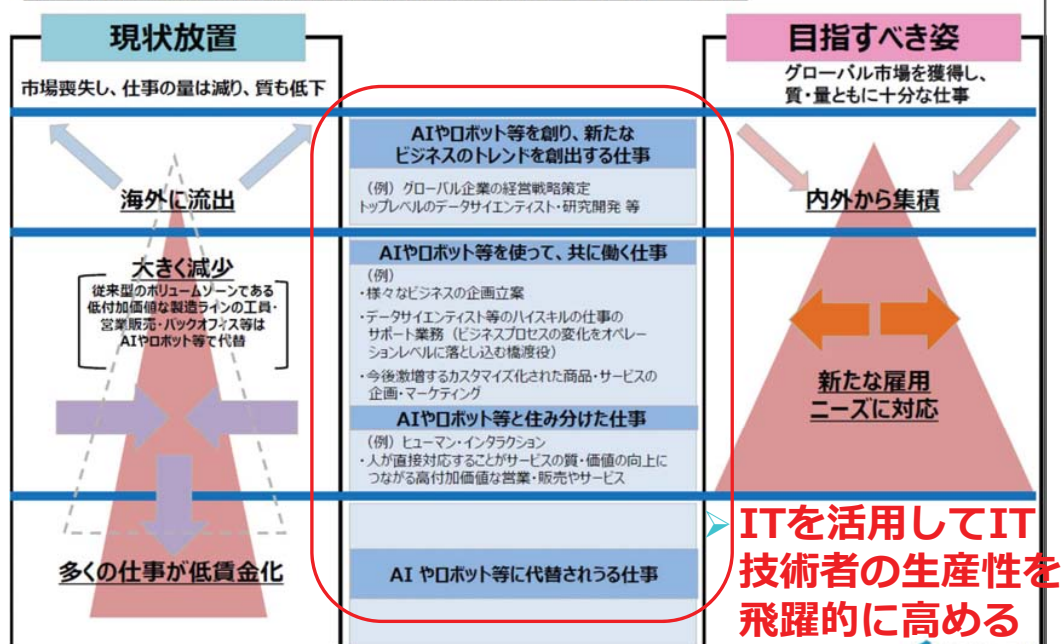
35

日本のITの現状と対策のアイデア

「新産業構造ビジョン」

～第4次産業革命をリードする日本の戦略

第4次産業革命による就業構造変革の姿（イメージ）



出典：経済産業省、「新産業構造ビジョン」～第4次産業革命をリードする日本の戦略」
http://www.meti.go.jp/committee/summary/eic0009/pdf/018_02_00.pdf

36

日本のITの現状と対策のアイディア

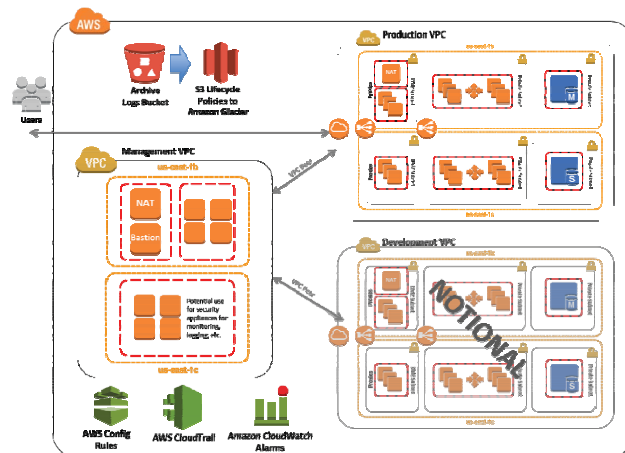
FedRAMPを参考に…IT技術を社会的に共有

■ 米国はクラウドファースト政策

- 政府機関が開発するソフトウェアを他省庁でも再利用できるようにすることを義務付け

■ FedRAMPの設立

- クラウドの調達基準の認証制度
- 連邦政府組織間でセキュリティ評価を共用



■ クラウドは組織を超えた技術の標準化を可能にする

- The Quick Start template **automatically configures** the AWS resources and deploys a multi-tier, Linux-based web application in a few simple steps, in **about 30 minutes**.

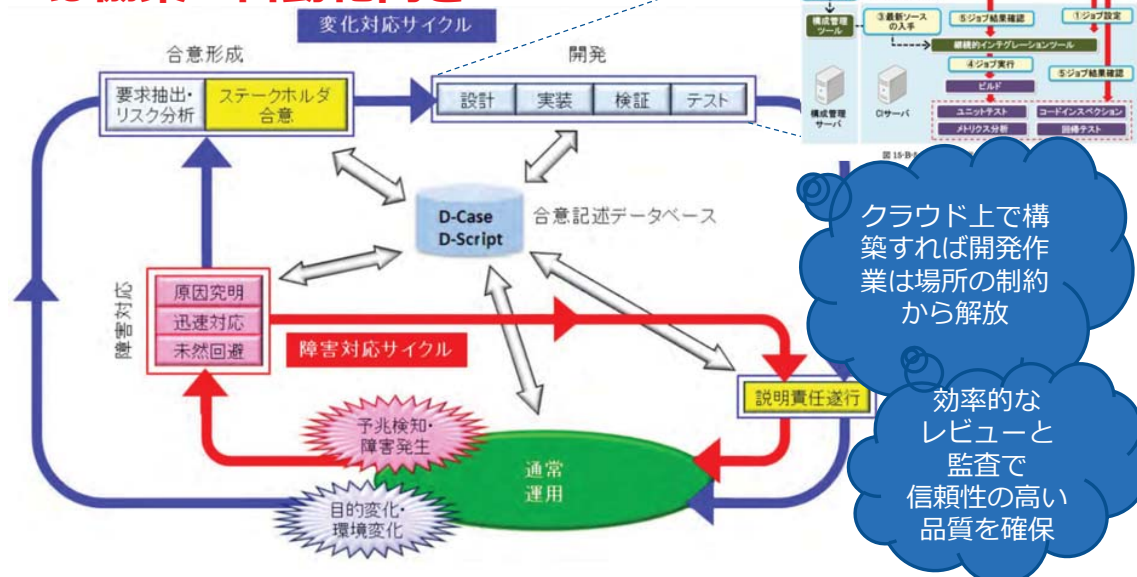
出典：アマゾンウェブサービス, <https://aws.amazon.com/jp/quickstart/architecture/accelerator-nist/>

37

日本のITの現状と対策のアイディア

開発のライフサイクルの自動化

➤ 工程が明確なライフサイクルは協業・自動化向き



出典：科学技術振興機構、「DEOSプロジェクト研究成果集」

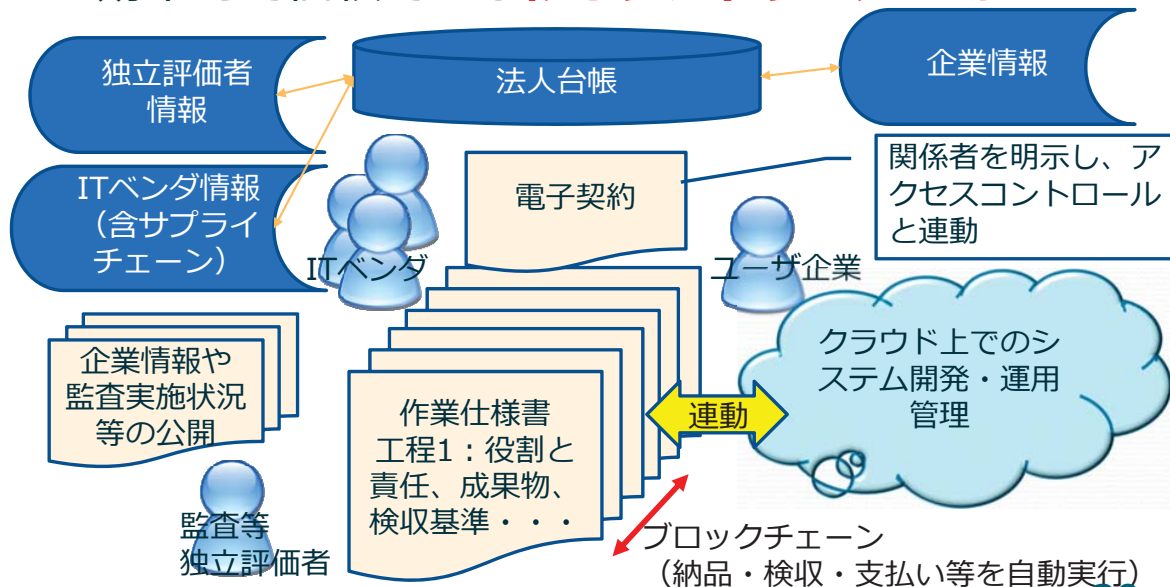
IPA、「先進的な設計・検証技術の適用事例報告書 アジャイルプロセスにおける実践的な品質向上施策の適用事例」

38

日本のITの現状と対策のアイデア

IT技術者をクラウド上で仮想的に流動化

- 開発関係者が電子化した開発契約で繋がる
効率的で信頼できる**仮想ソフトウェア工場**



39

サイバー時代の監査



40

サイバー時代の監査

サイバー時代の監査の目指すもの

- **信頼できるシステム** 情報とシステムの品質
 - 徹底した自動化と機能共用により、システム開発・運用とセキュリティの生産性を飛躍的向上
 - 監査の開発工程・ツールへの組み込み
- **信頼できる組織** プロセスの評価・改善を行う能力
 - 透明性の高い内部統制と第三者による評価
 - 内部監査による三線防御と外部監査
- **信頼できる社会** 信頼できる情報システムと組織
 - 信頼のサプライチェーンとエコシステム
 - 高度なサービスを責任をもって提供してくれるパートナーの選別とエコシステムの構築
 - クラウドはサイバーフィジカル社会の基盤

41

サイバー時代の監査

知識労働の生産性を向上させる6つの条件

IT技術者と監査人は
「知識労働者」



1. 仕事の目的を考える
2. 働く者自身が生産性向上の責任を担い、みずからをマネジメントする
3. 継続してイノベーションを行なう
4. **みずから継続して学び、人に教える**
5. 知識労働の生産性は量よりも質の問題であることを認識する
6. 知識労働者は、組織にとってコストではなく資本財であることを理解する

出典：P.F.ドラッカー、2005、「テクノロジストの条件」,ダイヤモンド社

42

サイバー時代のT監査

「IT監査保証の判断基準」研究プロジェクト

■2017年度活動計画

- グローバルな標準、基準の動向調査
(OpenGroupのFACE、NISTのフレームワーク、FedRAMP等)
- ビジネスとシステムの最新動向の研究
- 監査、評価手法、ツール等の標準、基準の動向調査
- 上記を踏まえ、**COBITの改定の提言**を英語でISACAに行う

■研究会；原則第2金曜18:30～市ヶ谷
(法政大学新一口坂)

参加登録は、システム監査学会ホームページから

43



Thank you

この資料の内容には発表者個人の見解が含まれます。
また、発表者の所属会社とは関係ありません。

44