【Jun. 8, 2018 システム監査学会　第32回研究大会】
「IT監査保証の判断基準」研究プロジェクト　成果報告

スマート社会に向けたガバナンスとITマネジメントのフレームワークへの提言

Recommendations to Governance and IT Management Framework for Enabling Smart Society

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

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。

- **研究プロジェクトメンバーの業種にかかるビジネスとシステムの最新動向の研究**
- **グローバルな基準・標準に関連する翻訳**
- **COSOおよびCOBITの課題抽出と提言**

「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）

※　五十音順

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（ｼｽﾃﾑﾃﾞｻﾞｲﾝ・ﾏﾈｼﾞﾒﾝﾄ学）、システム監査技術者
杉山 哲男	CIA
鈴木 夏彦	システム監査技術者、CIA、CISA
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

Agenda

- スマート社会とは
- スマート社会のITとビジネス
- スマート社会で生き残るために
- COBIT５の概要と改訂への提言

スマート社会とは

Society 5.0

- **Society 5.0**
  - 政策
    - http://www8.cao.go.jp/cstp/society5_0/index.html
  - 政府広報
    - https://www.gov-online.go.jp/cam/s5/
  - 首相官邸
    - 4度目の産業革命がもたらす5つ目の社会 https://www.kantei.go.jp/jp/headline/seicho_senryaku2013.html

[Source] 内閣府, Society 5.0, http://www8.cao.go.jp/cstp/society5_0/index.html（参照：2018/02/18）

Society 5.0

Society5.0

- 2016年1月に閣議決定された日本の科学技術政策で提唱された「超スマート社会」の呼称。ＩＣＴを最大限に活用し、**サイバー空間とフィジカル空間（現実世界）とを融合させた取組により、人々に豊かさをもたらす**「未来社会の姿として共有し、その実現に向けた一連の取組を更に深化させ、強力に推進し、世界に先駆けて実現していくとしている。

超スマート社会

- 必要なもの・サービスを、必要な人に、必要な時に、必要なだけ提供し、社会の様々なニーズにきめ細かに対応でき、**あらゆる人が質の高いサービスを受けられ、年齢、性別、地域、言語といった様々な違いを乗り越え、活き活きと快適に暮らすことのできる社会**。

[Source] 内閣府,科学技術基本計画（第5期：平成28～32年度）, 2016/01, http://www8.cao.go.jp/cstp/kihonkeikaku/5honbun.pdf. P11（参照：2018/02/07）

スマート社会の新しい価値

- 健康
- ワークライフバランス
- 能力開発
- 社会参加
- 市民活動
- 環境品質
- 個人のセキュリティ
- 主観的な幸福

- 収益と富
- 仕事と収入
- 家庭

□自然資本 □経済資本 □人的資本 □社会資本

[Source] OECD, Measuring Well-being and Progress: Well-being Research, http://www.oecd.org/statistics/measuring-well-being-and-progress.htm(accessed 2018-2-17)

Smart Society

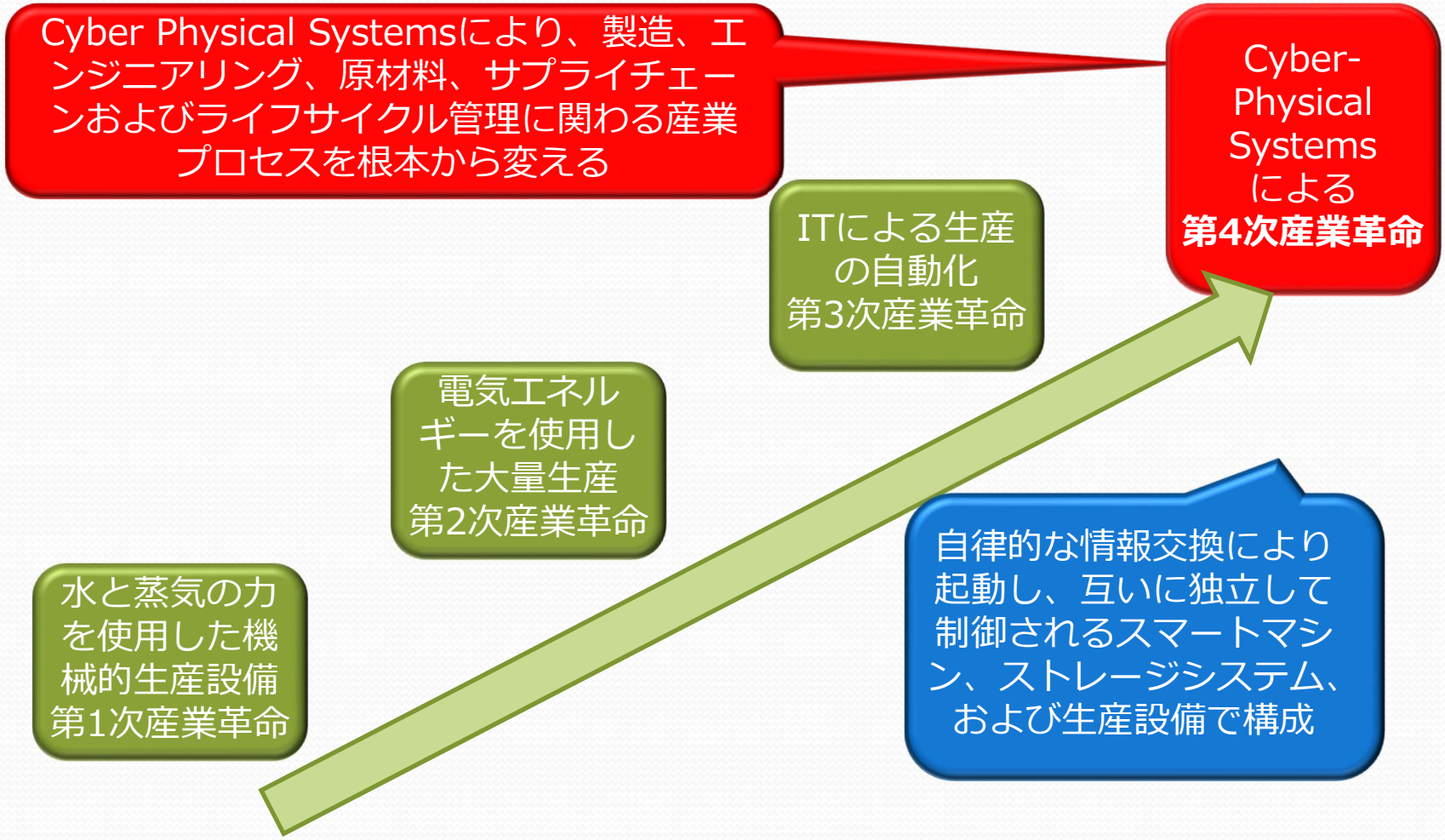
- **Smart ;**
  - **computer-controlled**; (of a device, especially a weapon/bomb) controlled by a computer, so that it appears to act in an intelligent way

[Source] Oxford Advanced Learner's Dictionary 9th edition ,Oxford University Press

- **Smart Society;**
  - SmartSociety is **funded by EU** FP7-FET Future Emerging Technologies n.600854 (Jan.2013-Dec.2016)
    - The Ride Share scenario
    - The Care House scenario
    - The speed bump
    - Smart Tourism

[Source] Smart Society project, http://www.smart-society-project.eu/about/factsheet/index.html, (accessed 2018-2-17)

INDUSTRIE 4.0



[Source] Communication Promoters Group of the Industry-Science Research Alliance, Recommendations for implementing the strategic initiative INDUSTRIE 4.0,April 2013, http://forschungsunion.de/pdf/industrie_4_0_final_report.pdf, P13 (accessed 2018-2-17)

先行するドイツ

- **Implementation Strategy Industrie 4.0**
  - Roadmap for implementation (2015-2035)
    - Horizontal integration via value-added networks
    - Consistency of the engineering over the complete life cycle
    - Vertical integration and networked production systems
    - New social infrastructures for work
    - Continuous development of cross-sectional technologies

（日本語翻訳版） https://www.jetro.go.jp/ext_images/_Reports/01/c982b4b54247ac1b/20150076.pdf

[Source] BITKOM・VDMA・ZVEI:, Implementation Strategy Industrie 4.0, Kehrberg Druck Produktion Service, https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2016/januar/Implementation_Strategy_Industrie_4.0_-_Report_on_the_results_of_Industrie_4.0_Platform/Implementation-Strategy-Industrie-40-ENG.pdf, P15（2018/5/21）

Reference architecture model Industrie 4.0

- **DIN SPEC 91345:2016-04**
  - Life Cycle & Value Stream
    - Type (Development, Maintenance/usage)
    - Instance (Production, Maintenance/usage)
  - Hierarchy Levels
    - Product, Field Device, Control Device, Station, Work Centers, Enterprise, Connected World
  - Layers
    - Business, Functional, Information, Communication, Integration, Asset

[Source] Deutsches Institut für Normung, Reference Architecture Model Industrie 4.0 (RAMI4.0) English translation of DIN SPEC 91345:2016-04,April 2016, P19, Figure 8

NIST Cyber-Physical Systems Framework

- **Cyber-Physical Systems**
  - Cyber-Physical Systems or "smart" systems are co-engineered interacting networks of physical and computational components. These systems will provide the foundation of our critical infrastructure, form the basis of emerging and future smart services, and improve our quality of life in many areas.
- **CPS Conceptual Model**
  - System-of-systems, Cyber-physical Devises, …
- **CPS Framework**
  - Domains (Manufacturing, Transportation,…)
  - Facets (Conceptualization, Realization, Assurance)
  - Aspects (Functional, Business, Human, Trustworthiness, Timing, Data, Boundaries, Composition, Lifecycle)

[Source] NIST Cyber Physical Systems Public Working Group, Framework for Cyber-Physical Systems Release 1.0, May 2016, https://pages.nist.gov/cpspwg/, (accessed 2018-2-17)

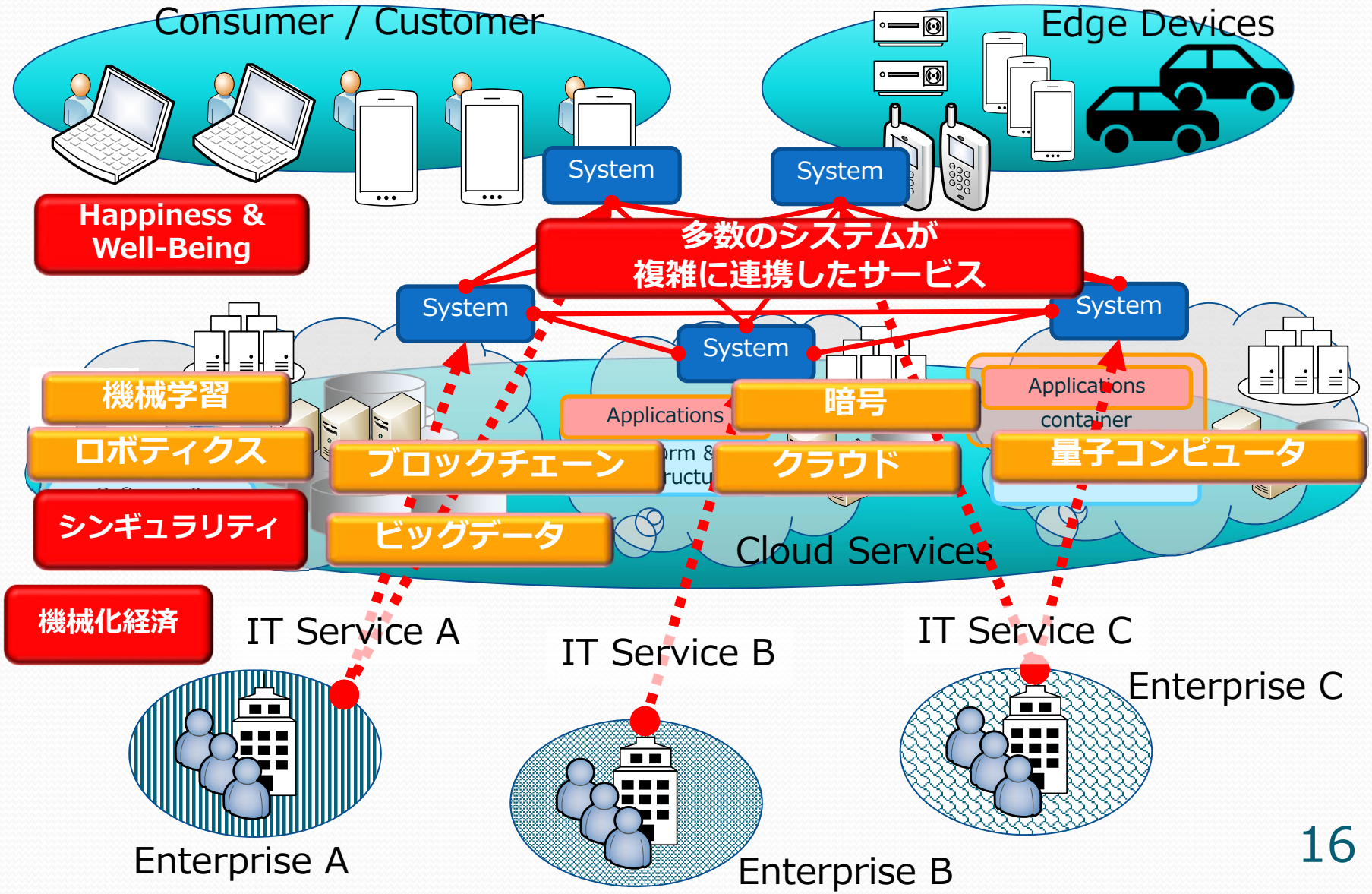
The Open Group IT4IT™

- **IT Value Chain for Service Model Backbone**
- **IT4IT Reference Architecture**
  - Strategy to Portfolio, Requirement to Deploy, Request to Fulfill, Detect to Correct
- **Service Model**
  - Continuous Assessment, Continuous Integration, Continuous Delivery
- **Functional Model**
- **Integration Model**

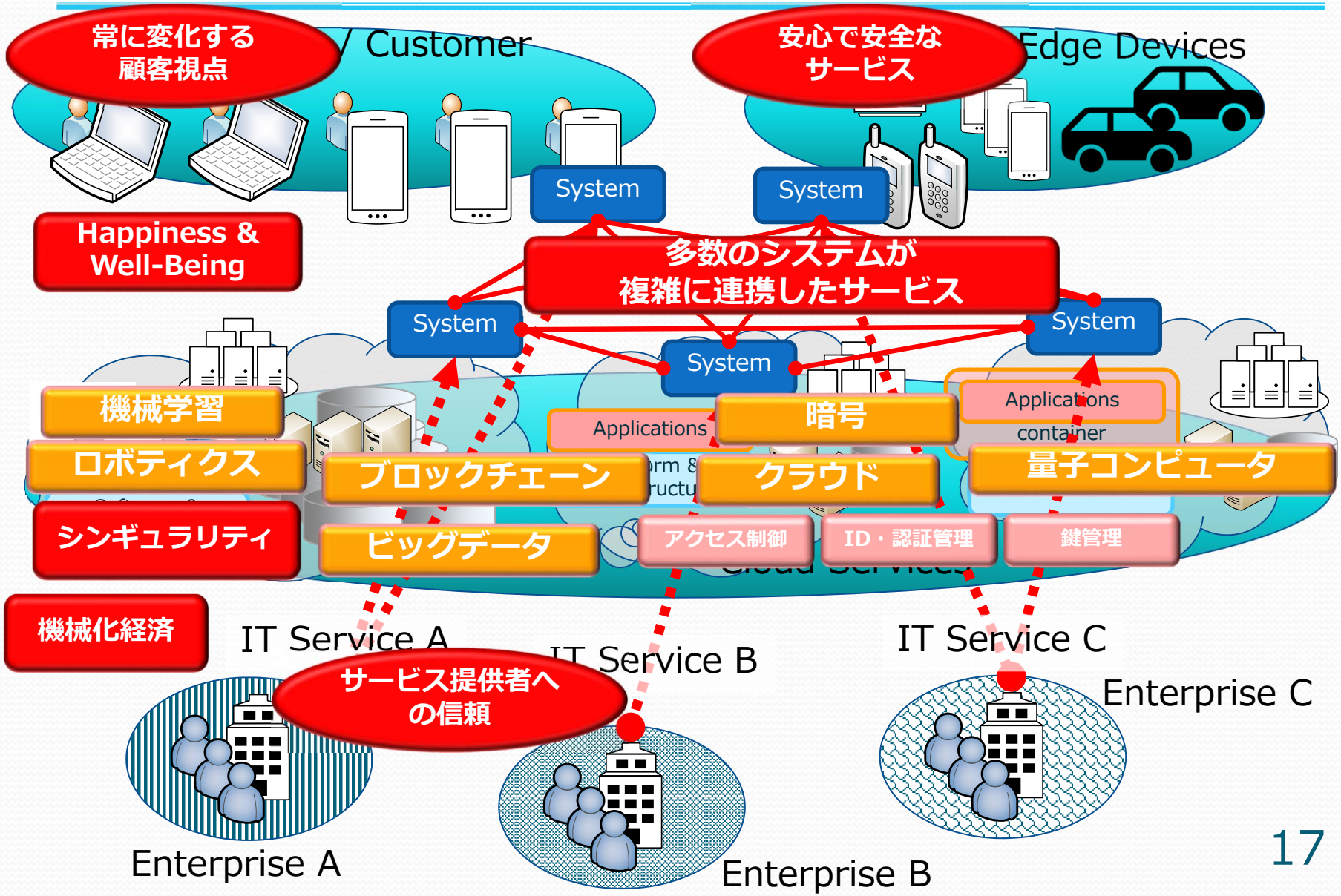
[Source] The Open Group , IT4IT™ Reference Architecture, Version 2.1, Jan 2017, http://pubs.opengroup.org/it4it/refarch21/IT4ITv2.1.html, (accessed 2018-2-17)

スマート社会の ITとビジネス

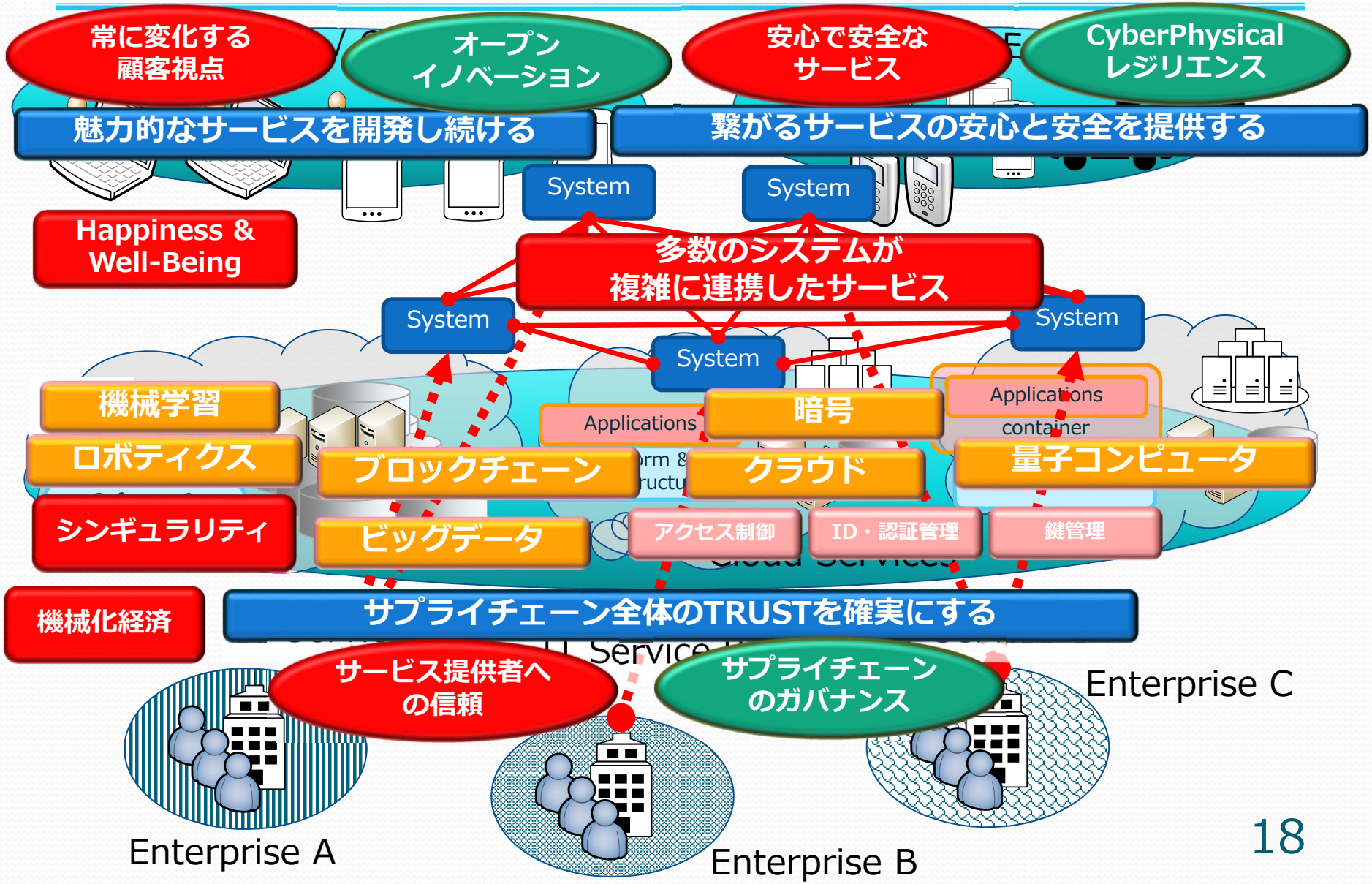
スマート社会のITサービス



スマート社会におけるITサービスへの要求



スマート社会におけるビジネスの目標



スマート社会で
生き残るために

- 魅力的なサービスを開発し続ける
- 繋がるサービスの安心と安全を提供する
- サプライチェーン全体のTRUSTを確実にする

魅力的なサービスを開発し続ける

- **常に変化する「顧客」視点**
  - 技術が進歩し、生産性が高くなるほど「儲からなくなる」…コモディティトラップ
  - 優れた製品を開発してもすぐに陳腐化する
  - 勝者は「顧客」に最高の体験を提供する者
    - QCDは作り手の論理
    - QCD以外の価値；健康、ワークライフバランス、能力開発、社会参加、市民活動、環境品質、個人のセキュリティ、主観的な幸福等

持続可能なサービスにビジネスモデルを変える必要性

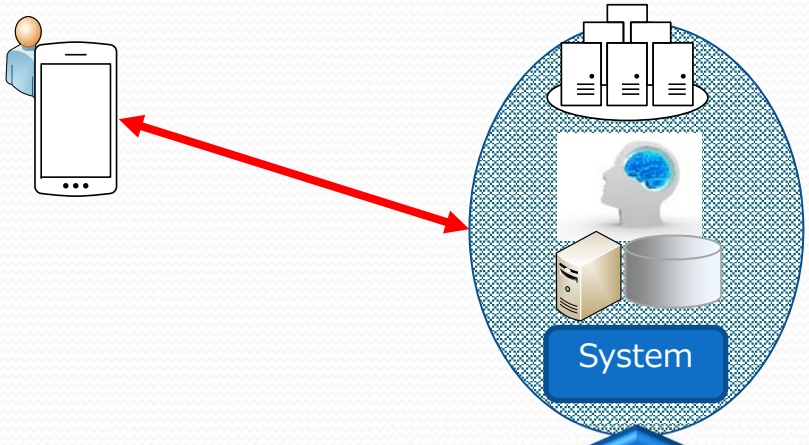
魅力的なサービスを開発し続ける

- **オープンイノベーション**[1]
  - 内部のイノベーションを加速し、同時にイノベーションを外部で利用させるため市場拡大の目的で意図的に知識を流出、流入させる活用法。
    - 単一の組織では不可能な知識の活用や組み合わせを試す機会が増える
    - 多様性により幅広いニーズに応えられるビジネスのエコシステム
- **アジャイル開発**[2]
  - 顧客と協調し、変化に対応しながら、個々人を尊重した対話により、迅速に動くソフトウエアを開発する種々の手法

[Source[1]] Open Innovation Community, Open Innovation: Researching a New Paradigm (2006),Open Innovation, http://openinnovation.net/about-2/open-innovation-definition/, (accessed 2018-5-17)

[Source[2]] Kent Beck他17名の著者たち, 2001, http://agilemanifesto.org/iso/ja/manifesto.html (accessed 2018-5-17)

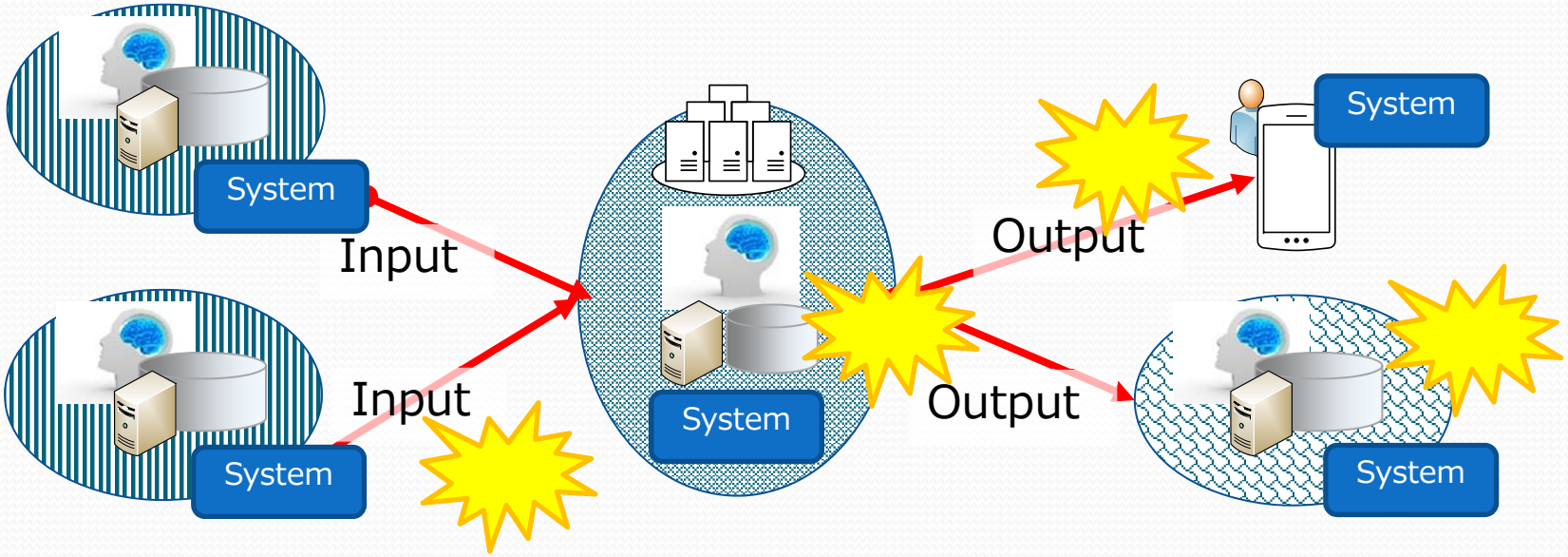
繋がるサービスの安心と安全を提供する



自分のシステムが信頼できる
- システムの機能
- システムの品質
- レジリエンス

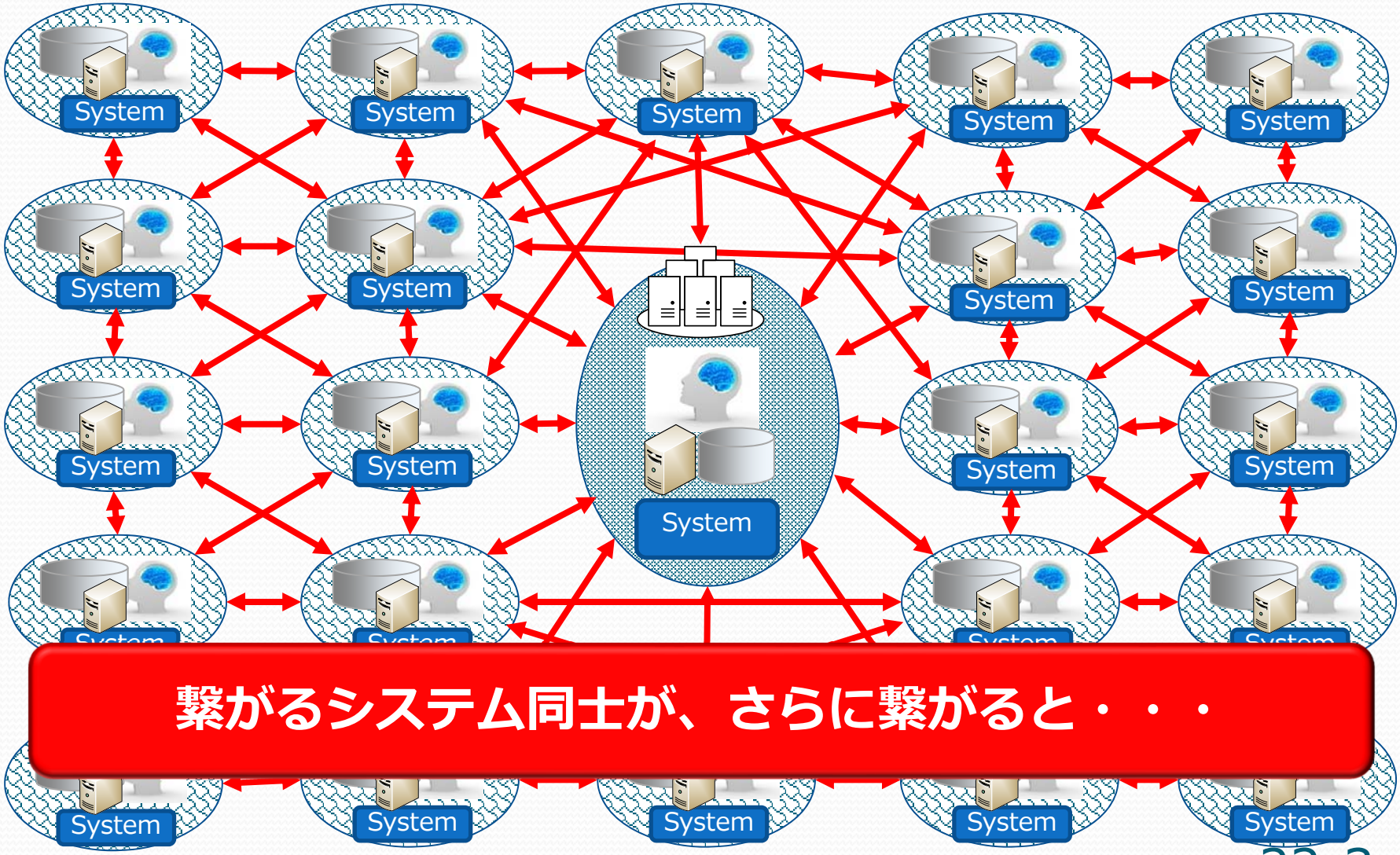
繋がらないシステムは、自分だけを考えればよかった

繋がるサービスの安心と安全を提供する

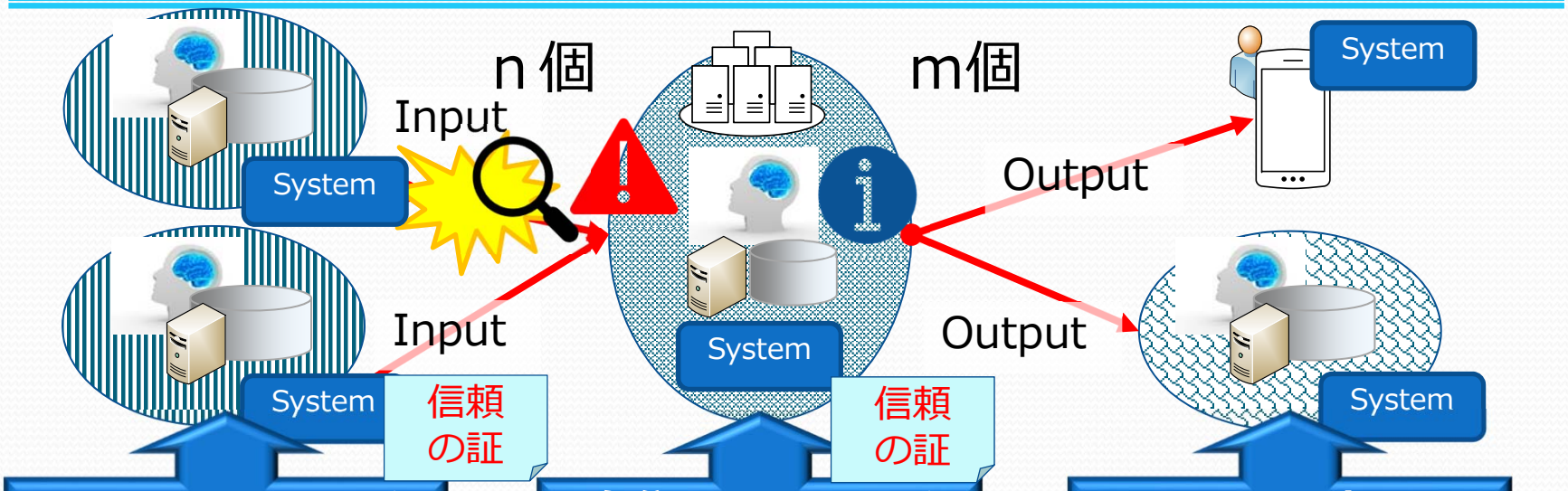


システムが繋がると、その影響は広く伝播する

繋がるサービスの安心と安全を提供する



繋がるサービスの安心と安全を提供する



Inputシステムが信頼できる
- システムの機能
- システムの品質
- レジリエンス

自分のシステムが信頼できる
- システムの機能
- システムの品質
- レジリエンス

Output先に信頼を提供できる
- システムの機能
- システムの品質
- レジリエンス

n 対mの人とシステムを信頼の輪で繋げる

繋がるサービスの安心と安全を提供する

- **安心で安全なサービス**
  - サービスに**レジリエンス**が要求される[1]
    - レジリエンス；リスクの顕在化を回避しながら活動し、リスクの顕在化時も速やかに復旧する能力
  - システムが複雑に連携する「繋がるサービス」では、**セーフティ、セキュリティ、リライアビリティ**が特に重要[2]
    - セーフティ；人の生活や環境へ不適切な影響を与えるリスクの回避・緩和
    - セキュリティ;人や機器やシステムの適切なデータアクセスや情報・データを損なうリスクの回避・緩和
    - リライアビリティ；機器やシステムが適切な機能を失うリスクの回避・緩和

[Source[1]] Erik Hollnagel, Nancy Leveson, David D. Woods,レジリエンスエンジニアリング―概念と指針 ,日科技連出版社, 2012
[Source[2]] 独立行政法人情報処理推進機構 (IPA) ソフトウェア高信頼化センター(SEC), つながる世界の開発指針第2版 ,独立行政法人情報処理推進機構(IPA), 2016, https://www.ipa.go.jp/files/000060387.pdf , (accessed 2018-5-17)

繋がるサービスの安心と安全を提供する

- **Cyber Physicalレジリエンス**
  - 説明可能な安心と安全
    - 適切なリスクとハザードのアセスメントと機能保証
      - 安心と安全の要件を明確化し、実装/テスト/保証
      - 自動テストによる継続的デリバリーと自動監視
    - 品質の証跡を記録し、検証/保管
      - ディペンダビリティ；信頼性パフォーマンス、保守性パフォーマンス、保守サポートパフォーマンス等の可用性の総合的パフォーマンスと影響要因の説明
      - アシュアランスケース；主張が満たされていることを支持する、明示的な前提を含む体系的な論証とその証拠の理路整然とした監査可能な成果物
  - 業務影響度分析（BIA）/業務継続管理（BCM）/災害時復旧計画（DRP)の整備

[Source] ISO,ISO/IEC15026-1:2013 Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary ,ISO,2013, P2

サプライチェーン全体のTRUSTを確実にする

- **コーポレートガバナンスの潮流**
  - 企業ガバナンスは、国や文化や時代等で異なる
  - エージェンシー理論；経営者（エージェント）に対する株主（プリンシパル）の監視力を高め、情報の非対称性を解消する
    - 従来型の企業ガバナンス理論の中心
  - グローバル化、ネットワーク化の進展
    - 自国のガバナンスが他国で通用しない、株主以外の様々なステークホルダーの利害を考慮する必要性
  - 新しい企業ガバナンス理論
    - 企業外部との関わりも含め、多様なステークホルダーのために、「社会倫理」を重視
    - 「国連グローバル・コンパクトの10原則」等、国際的な倫理基準の明文化も進んでいる

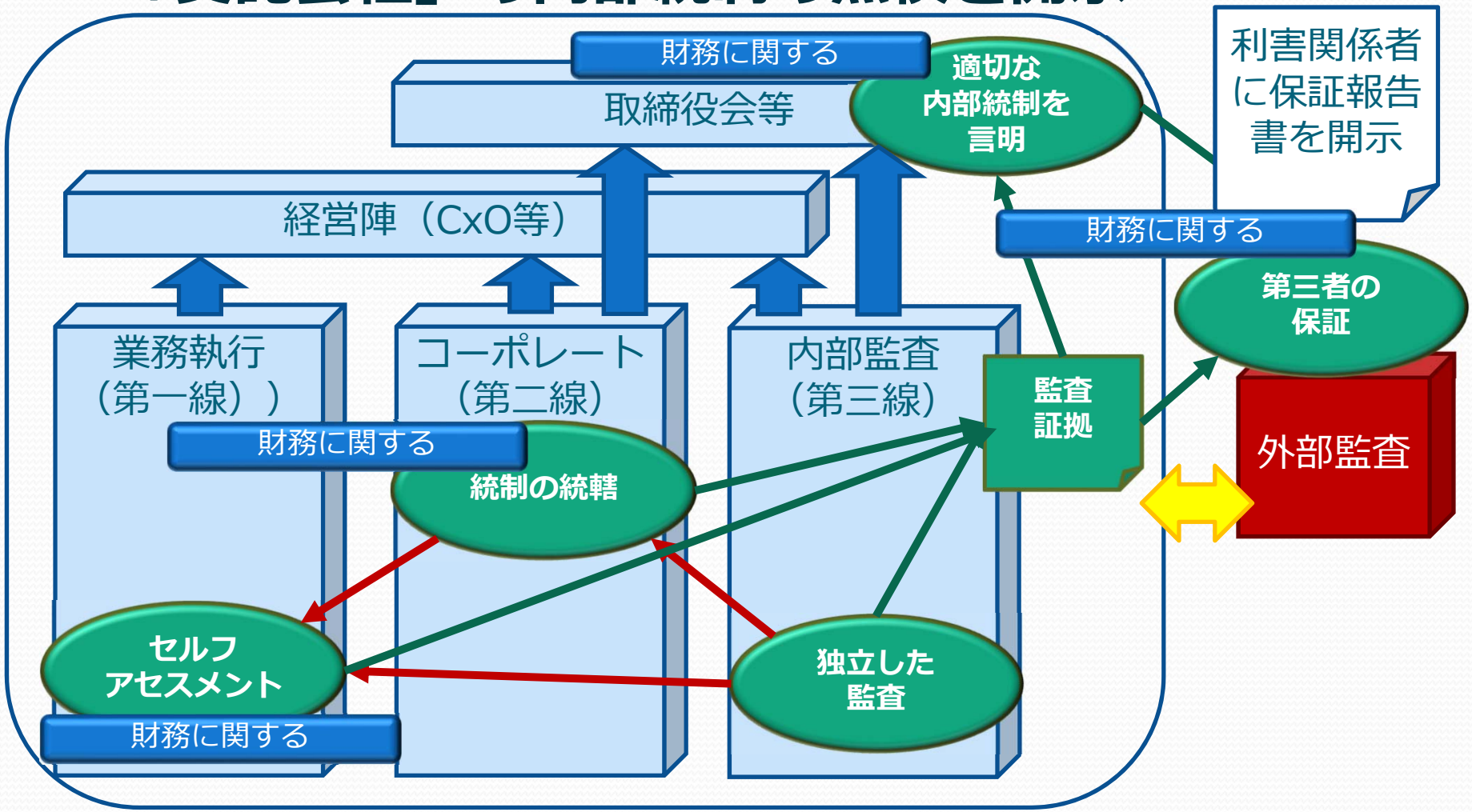
[Source] 入山章栄, 企業ガバナンスと「良い世界を作ること」が、豪鬼する時代がきた(Kindle版）,ダイヤモンド社,2017, 位置No.131

サプライチェーン全体のTRUSTを確実にする

- **サプライチェーンのガバナンス**
  - ガバナンス；組織の目的を達成するための枠組み
  - 新しい価値に貢献する枠組み
    - 新しい価値；健康、ワークライフバランス、能力開発、社会参加、市民活動、環境品質、個人のセキュリティ、主観的な幸福等
  - 価値と目標を共有して共創する枠組み
    - オープンイノベーション
      - 多様なパートナーとの試行錯誤
      - オープンイノベーションとアジャイル開発による顧客との共創
  - サプライチェーンの信頼の見える化の枠組み
    - 戦略マップによる目指す価値と目標の見える化
    - アシュアランスケースによる安心と安全の見える化
    - 第三者保証等による各組織の信頼の見える化

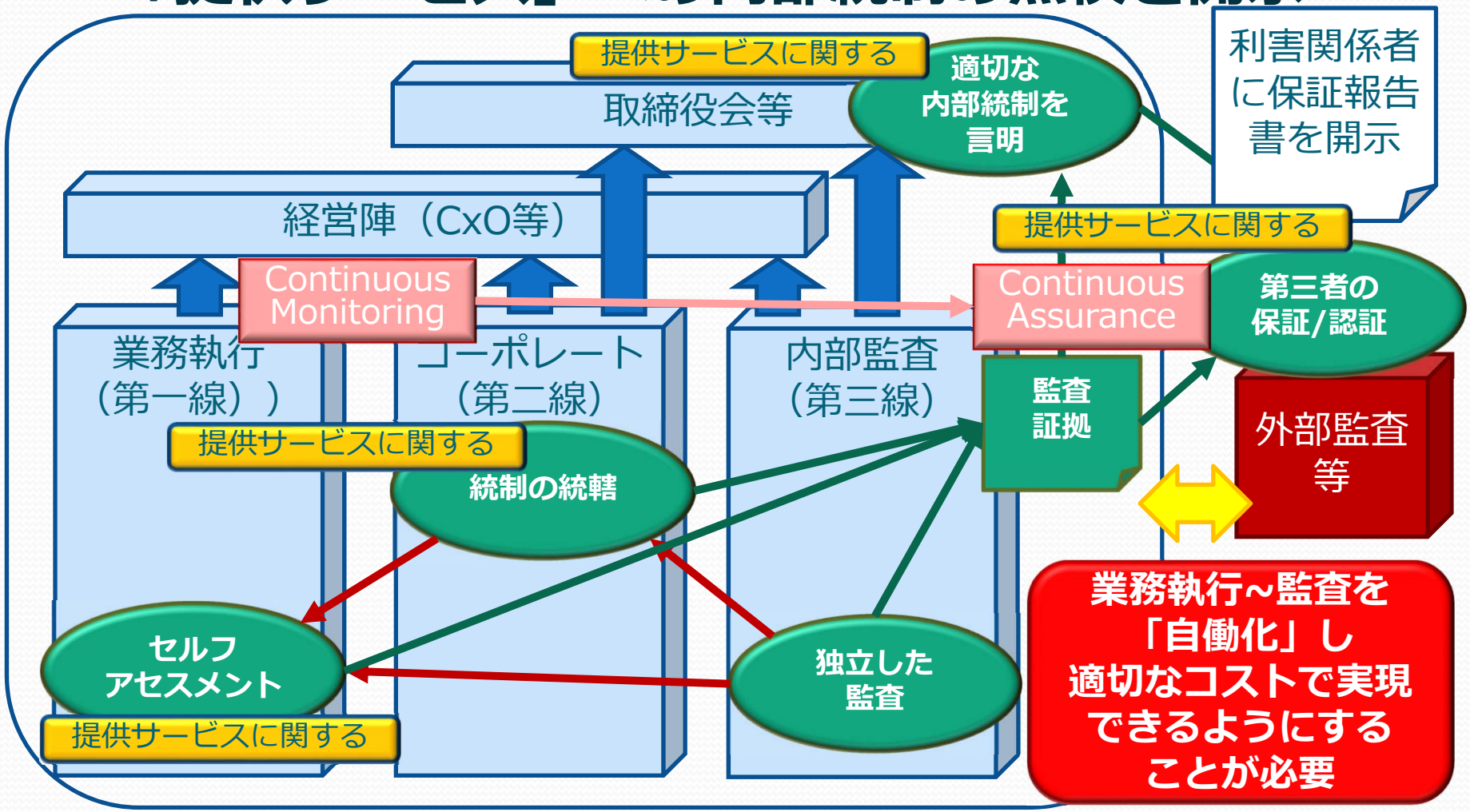
サプライチェーン全体のTRUSTを確実にする

「受託会社」の内部統制の点検と開示



サプライチェーン全体のTRUSTを確実にする

「提供サービス」への内部統制の点検と開示



サプライチェーン全体のTRUSTを確実にする

■サプライチェーン戦略マップ（イメージ）

[Source] Robert S. Kaplan, David P. Norton、戦略マップ【復刻版】（Kindle版）, 東洋経済新報社, 2015 (2014), 位置No.768 図表1-3 を参考に発表者が作成

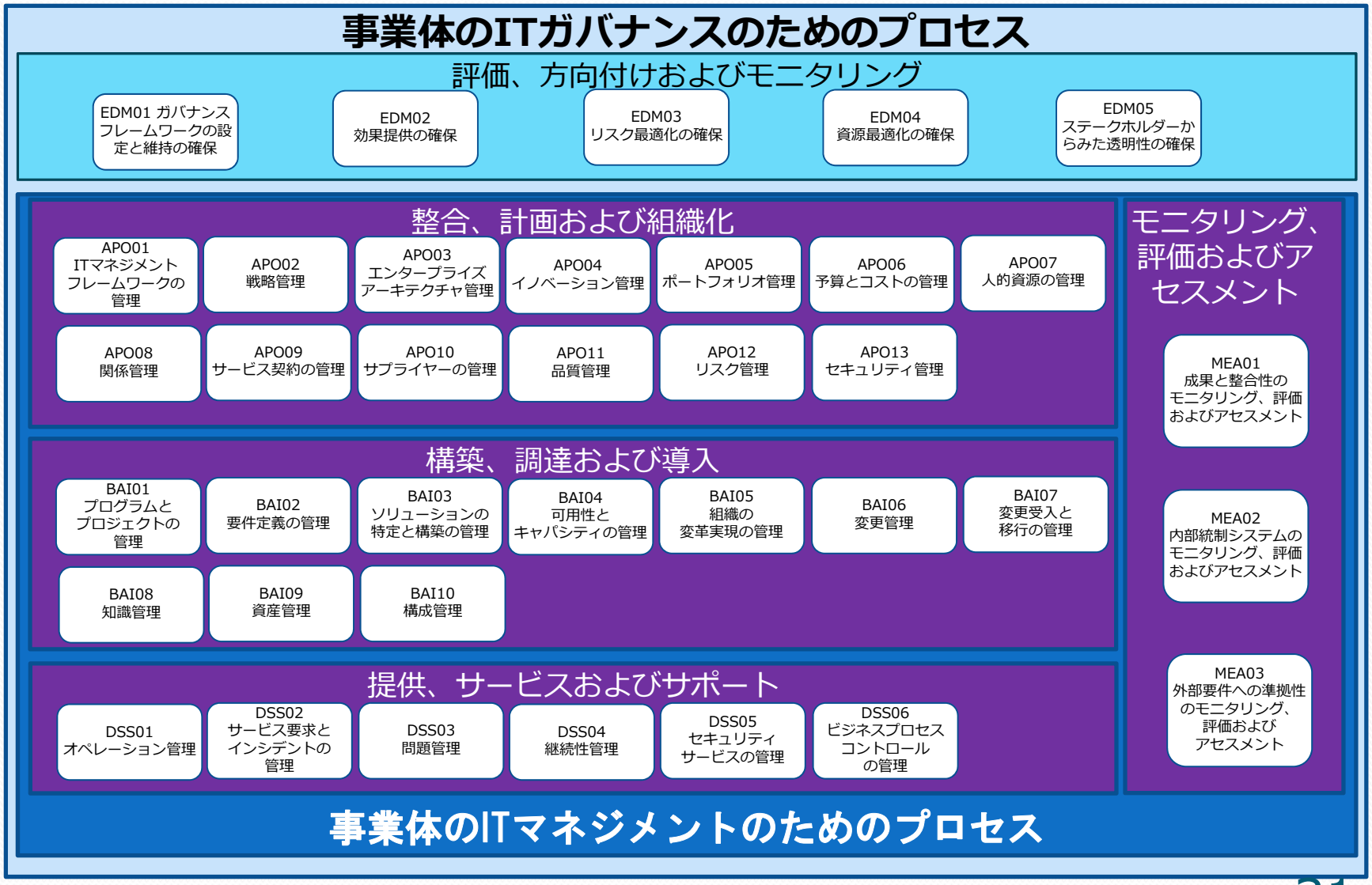
COBIT５の概要と改訂への提言

COBIT5の概要

- **COBIT5とは**
  - IT ガバナンスと IT マネジメントに関わる目標を事業体が達成できるよう支援する、包括的なフレームワーク
  - 効果の実現と、リスクレベルやリソース活用の最適化とのバランスを保つことによって、事業体が IT から最適な価値を生み出すことを支援
  - 組織の内外のステークホルダーの IT に関する利害を踏まえ、また事業全体および IT の機能分野に関わる責任を考慮した上で、事業体全体の IT を包括的にガバナンスし管理することを可能にする。

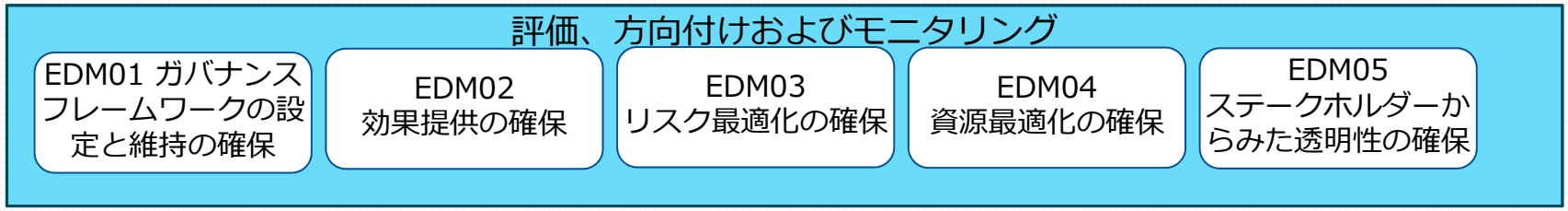
[Source] ISACA, COBIT5: A Business Framework for the Governance and Management of Enterprise IT, ISACA,2012

COBIT5の概要



[Source] ISACA, COBIT5: イネーブリングプロセス, ISACA,2012

事業体の IT ガバナンスのためのプロセス

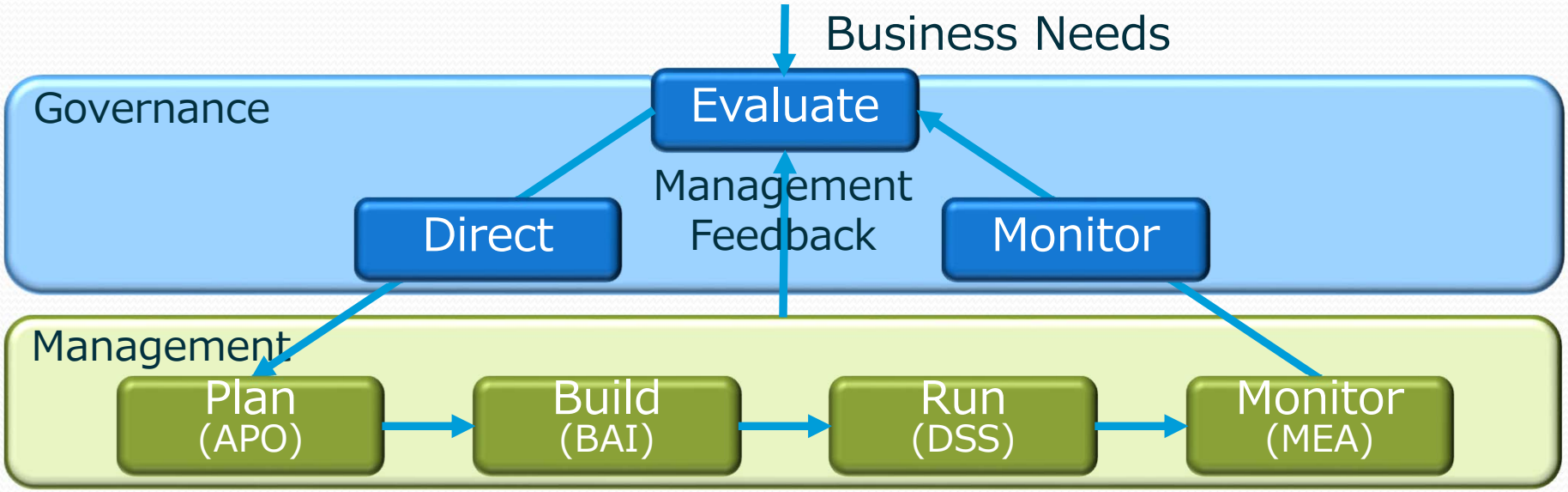


- **評価、方向付けおよびモニタリング（EDM）**
  - **01 ガバナンスフレームワークの設定と維持の確保**
    - 事業体の使命、目標、目的を達成するための責任と権限の明確化
    - 効果的な実現構造、原則、プロセスと実践手法の整備・維持
  - 02 効果提供の確保
    - ビジネスプロセス、IT サービスおよびIT 資産から得られるビジネスへの価値を、最適化する。
  - 03 リスク最適化の確保
    - IT に関する事業体リスクを確実に特定・管理可能にする
  - 04 資源最適化の確保
    - 適切で十分なIT 能力（要員、プロセス、技術）を確保
  - **05 ステークホルダーからみた透明性の確保**
    - IT の成果および整合性に関する測定と報告の透明性の確保

[Source] ISACA, COBIT5: イネーブリングプロセス, ISACA,2012

事業体の IT マネジメントのためのプロセス

- **整合、計画および組織化(APO)**
- **構築、調達および導入(BAI)**
- **提供、サービスおよびサポート(DSS)**
- **モニタリング、評価およびアセスメント(MEA)**



[Source] ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT , ISACA, 2012 , P32 Figure15 --- COBIT5 Governance and Management Key Areas

スマート社会に向けたフレームワークのへ提言

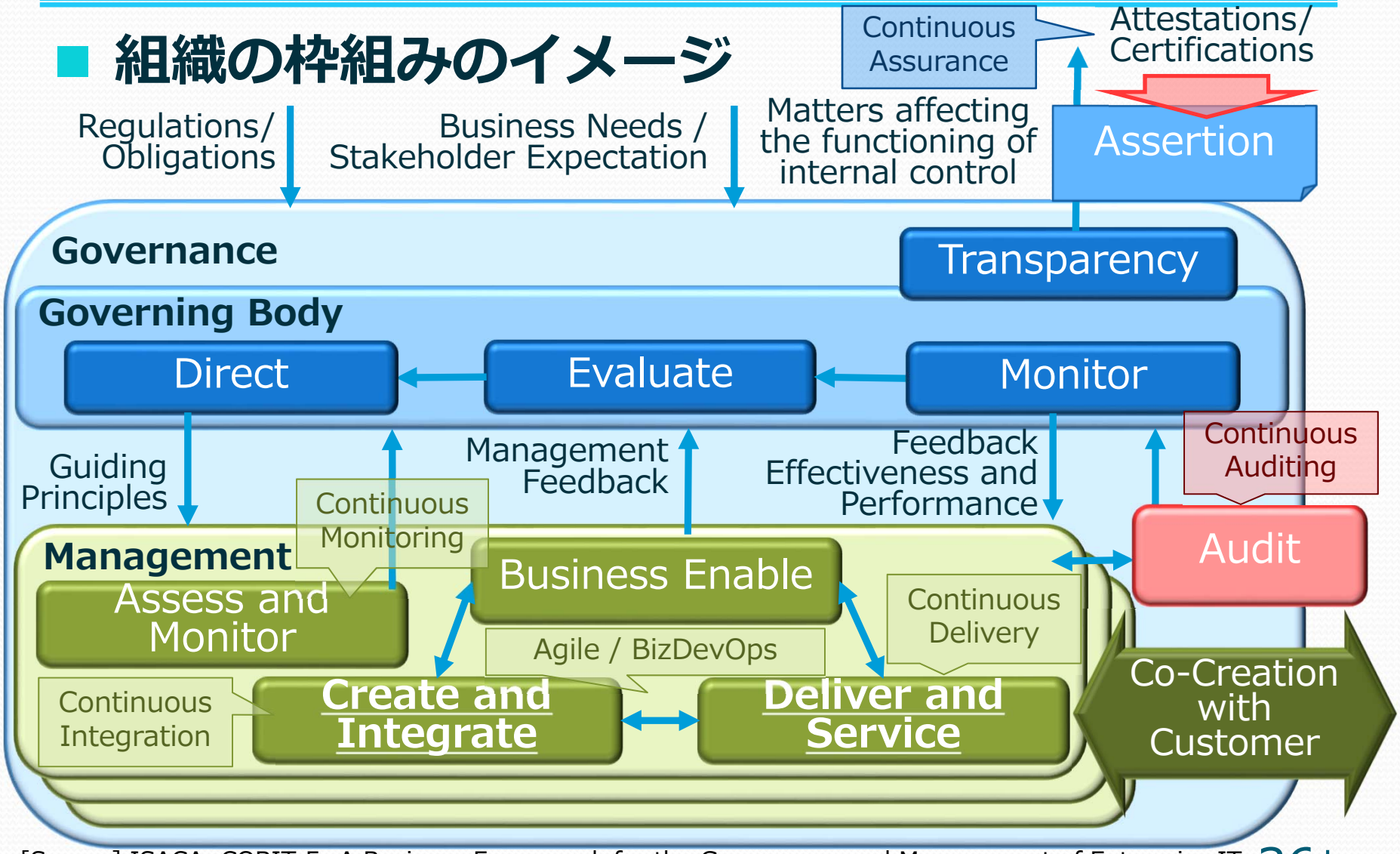
- **ガバナンスの主体は以下を確実にする**
  - 新しい価値への貢献の枠組み
    - 組織、人、システムが新しい価値（健康、ワークライフバランス、能力開発、社会参加、市民活動、環境品質、個人のセキュリティ、主観的な幸福等）にどのように貢献していくかを表明し、実現する
  - オープンイノベーション等による共創の枠組み
    - 組織内外との知識の流出/流入の枠組み
    - アジャイルなサービス開発と提供の枠組み（DevOps/CI/CD）
  - サプライチェーンの透明性確保の枠組み
    - サプライチェーンの目指す価値と目標の可視化
    - サプライチェーンの安心と安全の可視化
    - サプライチェーンの信頼の可視化と監査の独立性

スマート社会に向けたフレームワークのへ提言

- **組織は以下の能力を実装する**
  - オープンイノベーションへの対応
    - 継続的に共創の場を創り出す
    - 顧客とインタラクティブに試行錯誤を繰返す
    - アジャイルで高品質なサービスを創り出す
    - 継続的なデリバリーを実現する
  - Cyber Physicalレジリエンス
    - リスクとハザードのアセスメントに基づくセキュリティ/セーフティ・バイ・デザイン
    - 品質の証跡の記録・検証・保管,ディペンダビリティとアシュアランスケース
    - リスクとハザードのアセスメントに基づくBIA/BCM/DRPの整備

スマート社会に向けたフレームワークのへ提言

組織の枠組みのイメージ



[Source] ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT , ISACA, 2012 , P32 Figure15 --- COBIT5 Governance and Management Key Areas をもとに発表者が作成

50年前の知見に学ぶ

- **「情報時代における経営管理システムの展開」**
  （週間ダイヤモンド1969, 11月17日号 **ハーバート・A・サイモン**）
  - コンピュータは問題解決、あるいは意思決定のような複雑な思考を行える「考える機械」と定義するのが正確。
  - 情報について最も重要なことは、それを処理する人間である。直観的な判断力をもって情報を処理する存在であるわれわれが最も重要である。
  - 実験や努力あるいは失敗を通じて初めて5年後10年後により能率的なMISを作ることができる。
  - ひじょうに輝かしい将来を持つMIS、あるいは情報処理者としての人間について、新しい冒険に入るに際しては、積極的な姿勢をもって、これに臨み、積極的に参加していくことが必要。

5年後10年後の「超スマート社会」の実現のための「実験」「努力」「失敗」を行うことは私達の責任

[Source]ハーバート・A・サイモン,情報時代における経営管理システムの展開, 週間ダイヤモンド1969年11月17日号)

Thank you

この資料の内容は発表者個人の見解です。
発表者の所属会社・組織等とは関係ありません。