事業体とその環境、財務報告フレームワークおよび内部統制システムの理解とシステム監査

Systems Audits for Obtaining an Understanding of the Entity and Its Environment, the Applicable Financial Reporting Framework and the Entity's System of Internal Control

2021年度の振り返りと
2022年度 研究の方向性（中間）

監査保証の判断基準研究プロジェクト

監査保証の判断基準研究プロジェクト 2021年度活動の振り返り

- 主査：松尾明, 副主査：成田和弘（発表者）, メンバー（五十音順）：石島隆, 遠藤正之, 杉山哲男, 鈴木夏彦, 牧野博文, 水野英治
- 原則毎月　Zoomオンラインで開催
- テクノロジーモニタリングの研究と実践を行い、その成果を発表する。
  - 国内外のICT技術およびその標準、基準、規制、政策などの動向
  - ICT活用の背景となるコンピュータサイエンス、経営学、心理学、社会学等の動向
  - ビジネスとシステムおよび社会課題への取り組みの最新動向
  - ICTおよびITサービスの品質管理、テスト、評価、監査に関する動向
- 2021年度の活動実績（2021年６月研究大会以降）
  - 7/19, 9/24, 11/25, 12/23, 2/ 3, 3/ 4, 4/28

国内外のICT技術およびその標準、基準、規制、政策などの動向

- 2021年度にモニタリングしたJISの制改訂
  - Ｑ２２３１３　セキュリティ及びレジリエンス－事業継続マネジメントシステム－　ＪＩＳＱ２２３０１使用の手引（2021年10月発行）
  - Ｘ２０２４６　ソフトウェア及びシステム技術－ソフトウェア及びシステム開発における作業生産物のレビューのプロセス（ 2021年11月発行）
  - Ｘ２５０２０　システム及びソフトウェア製品の品質要求及び評価（ＳＱｕａＲＥ）－品質測定の枠組み（ 2021年11月発行）
  - Ｘ２５０３０　システム及びソフトウェア製品の品質要求及び評価（ＳＱｕａＲＥ）－品質要求の枠組み（ 2021年11月発行）
  - Ｘ３３０２０　情報技術－プロセスアセスメント－プロセス能力のアセスメントのためのプロセス測定フレームワーク（ 2021年11月発行）
  - Ｙ２３５９２　サービスエクセレンス－原則及びモデル（ 2021年11月発行）
  - Ｙ２４０８２　サービスエクセレンス－卓越した顧客体験を実現するためのエクセレントサービスの設計（ 2021年11月発行）
  - Ｙ３０１０５－２情報技術－ＩＴを使用したビジネスプロセスアウトソーシング（ＩＴＥＳ－ＢＰＯ）ライフサイクルプロセス－第２部：プロセスアセスメントモデル（ＰＡＭ）（ 2021年12月発行）
  - Ｑ１７０２９　適合性評価－妥当性確認機関及び検証機関に対する一般原則及び要求事項（ 2022年４月発行）
  - Ｑ１７０００　適合性評価－用語及び一般原則（ 2022年４月発行）

ビジネスとシステムおよび社会課題への取り組みの最新動向

- システム監査基準・管理基準改訂の方向性についての研究
  - 監査領域を示すための「システム監査のタクソノミ」の検討
    - 初版監査基準の実施基準
    - 平成16年版システム管理基準本体相当-国際基準等とのマッピング
    - IPAの「共通フレーム」は新国際基準（ISO/IEC/IEEE 12207：2017, JISX 0160:2021）に対応しないことが確定
  - システム管理基準 追補版（財務報告に係るIT 統制ガイダンス）“相当”の“自主ガイダンス”の検討（※基準改定とは別）
    - 制定後の環境変化の把握、評価と対応
    - 財務報告（会社法）、内部統制（金商法）監査とシステム監査の接点

システム管理基準 追補版相当の自主ガイダンスの検討について

- 2023年3月決算にかかる財務諸表の監査からISA315の2019年改定版が適用される
  - 「事業体とそのビジネスモデルの理解のための考慮事項」
  - 「事業体の内部監査機能を理解するための考慮事項」
  - 「ITを理解するための考慮事項」
  - 「GITCを理解するための考慮事項」
- システム管理基準追補版に関連するその他の基準の更新状況、サイバーセキュリティリスクの拡大やSDGsの動向等、昨今の技術動向や環境変化を踏まえた検証ポイントについて検討する

➢「システム管理基準追補版」との主要な差異について分析し、基準改定検討とは別に学会の研究プロジェクトとして、事業体の適切な情報開示を促進するためのシステム監査について考察

企業会計審議会

- 「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準」自体に大きな変更はない
  - 「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の改訂について（意見書）」の公表について
    https://www.fsa.go.jp/news/r1/sonota/20191213.html

- 監査の品質管理基準についての意見書
  - 「監査に関する品質管理基準の改訂に係る意見書」の公表について
    https://www.fsa.go.jp/news/r3/sonota/20211116.html

International Standards on Auditing（ISA）

- ISA 315 (Revised 2019): Identifying and Assessing the Risks of Material Misstatement https://www.iaasb.org/publications/isa-315-revised-2019-identifying-and-assessing-risks-material-misstatement
  - 追補版のベースとなった日本会計士協会のIT委員会報告3号は2011年12月26日にすでに廃止
    - （参考）ＩＴ委員会実務指針第６号「ＩＴを利用した情報システムに関する重要な虚偽表示リスクの識別と評価及び評価したリスクに対応する監査人の手続について」の公表について https://jicpa.or.jp/specialized_field/post_1591.html
  - 後継であったＩＴ委員会実務指針第６号もISA315（監査基準委員会報告書315）にＩＴに係る適用指針が追加されたことから廃止予定
    - （参考）「ＩＴ委員会研究報告「ＩＴの利用の理解並びにＩＴの利用から生じるリスクの識別及び対応に関する監査人の手続に係るＱ＆Ａ」」（公開草案）の公表について https://jicpa.or.jp/specialized_field/20210423fgb.html

→ 大きな改訂が２つあり、比較検証が困難なことから直接参照・分析することが必要

ISA 315 (Revised 2019)の概要 1/2

ISA315 ; IDENTIFYING AND ASSESSING THE RISKS OF MATERIAL MISSTATEMENT（重要な虚偽表示リスクの識別と評価）

- Requirements《要求事項》
  - Obtaining an Understanding of the Entity and Its Environment, the Applicable Financial Reporting Framework and the Entity's System of Internal Control（企業体とその環境、適用する財務報告フレームワークと企業体の内部統制システムの理解の獲得）
    - A52. The nature and extent of the required understanding is a matter of the auditor's professional judgment and varies from entity to entity based on the nature and circumstances of the entity, including:
      - The size and complexity of the entity, including its IT environment;
      - The auditor's previous experience with the entity;
      - The nature of the entity's systems and processes, including whether they are formalized or not; and
      - The nature and form of the entity's documentation.
    - **必要となる理解の性質と範囲は、**IT環境を含む事業体のサイズと複雑さ、事業体に関する監査人の以前の経験、正式化されているかどうかを含む、事業体のシステムとプロセスの状況、事業体のドキュメントの状況・形式を含む事業体の性質と状況によって**事業体ごとに異なり、監査人の専門的判断が求められる**

[Source] International Auditing and Assurance Standards Board., ISA 315 (Revised 2019) and Conforming and Consequential Amendments to Other International Standards Arising from ISA 315 (Revised 2019), International Federation of Accountants, https://www.ifac.org/system/files/publications/files/ISA-315-Full-Standard-and-Conforming-Amendments-2019-.pdf ,p.30[訳は発表者による] (2022/06/07)

ISA 315 (Revised 2019)の概要 2/2

ISA315 ; IDENTIFYING AND ASSESSING THE RISKS OF MATERIAL MISSTATEMENT（重要な虚偽表示リスクの識別と評価）

- Appendix 5: Considerations for Understanding Information Technology (IT)（IT を理解するための考慮事項）
  - Understanding the Entity's Use of Information Technology in the Components of the Entity's System of Internal Control
  - Scalability

- Appendix 6: Considerations for Understanding General IT Control（GITCを理解するための考慮事項）
  1. The nature of the general IT controls typically implemented for each of the aspects of the IT environment:
  2. Examples of general IT controls that may exist, organized by IT process include:

[Source] International Auditing and Assurance Standards Board., ISA 315 (Revised 2019) and Conforming and Consequential Amendments to Other International Standards Arising from ISA 315 (Revised 2019), International Federation of Accountants, https://www.ifac.org/system/files/publications/files/ISA-315-Full-Standard-and-Conforming-Amendments-2019-.pdf ,pp.97-118[訳は発表者による] (2022/06/07)

環境変化を踏まえた着眼点（案）

- システムの複雑化、規模の拡大への対応
  - システムの複雑化・規模の拡大によるリスクの理解
  - 複雑化したシステムのリスクを指し示すことの出来るタクソノミー

- サイバーリスクへの対応
  - 事業継続にかかわるランサムウェア（≒標的型攻撃被害）被害
    - ✓特権が奪取されるとGITCは瓦解
    - ✓必要なデータが暗号化され決算処理が困難に
    - ✓事業の中断による多額の損害
    - ✓情報漏洩対策への引き当てが必要に・・・
  - 後発的に発見される脆弱性への対応

- アジャイルガバナンスの実装に向けたイメージ
  - 基準はそれぞれの組織のコンテキストに臨機に対応できる原則ベースへ
  - SDGsを含む非財務の業績目標

システムの複雑化・規模の拡大によるリスク

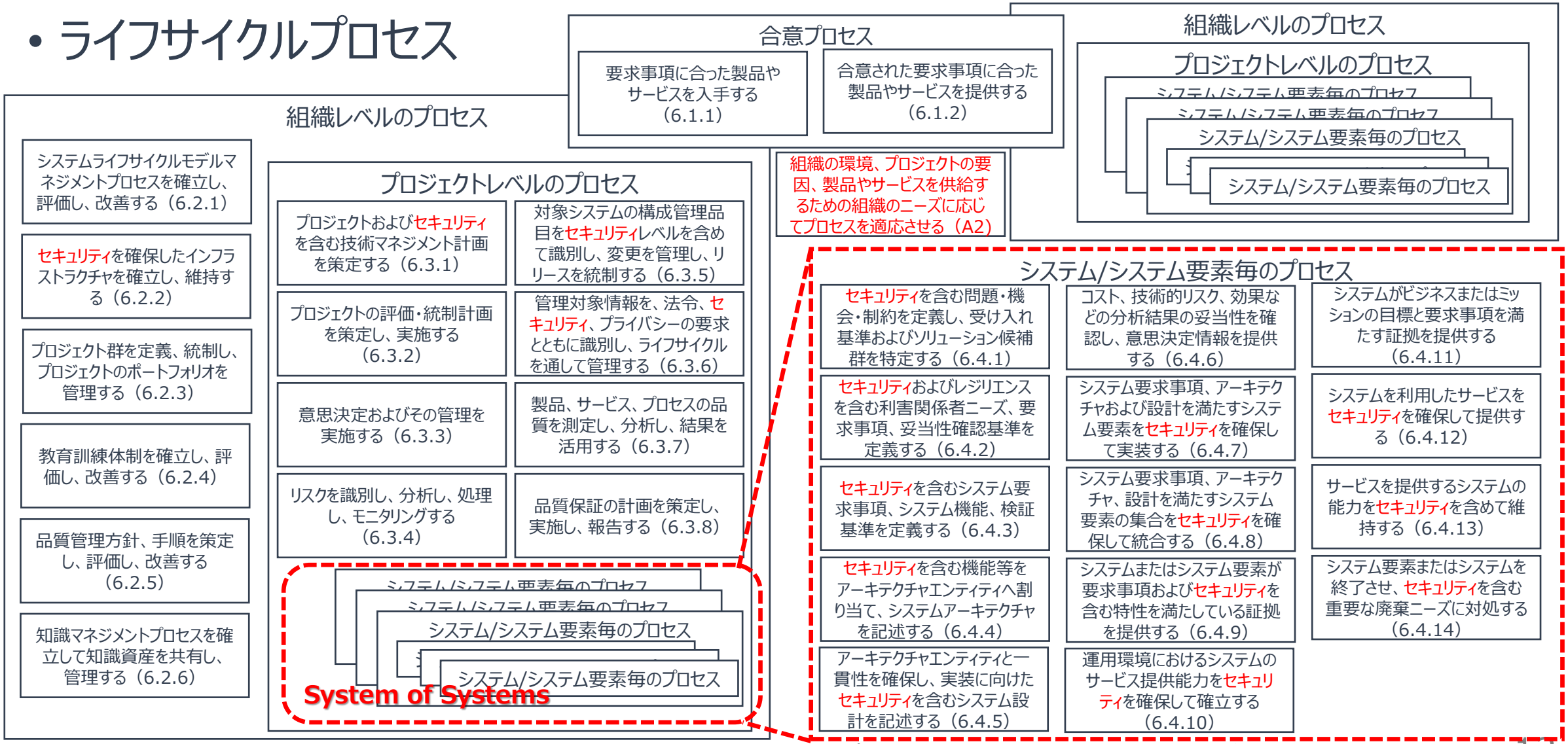
- 各稼働率が99.9%のシステムが連携するサービスの稼働率
  - 5システム　　→99.5%
  - 10システム　→99.0%
  - 100システム →90.0%

  ※　すべてのシステムが独立で、かつサービス提供にすべてのシステムの稼働が必要な場合

- 「重要障害は100年に1度」の高品質システムも多数保有すると..
  - 10システム保有　　→　10年に1回
  - 100システム保有　→　年に1回
  - 1000システム保有　→　年に10回

複雑化したシステムのリスクを指し示すことの出来るタクソノミー

- ライフサイクルプロセス



[Source] 日本産業標準調査会,JIS X 0160:2021 (ISO/IEC/IEEE12207:2017）,ソフトウェアライフサイクルプロセス，日本規格協会, 2021, を参考に発表者が作成。

事業継続にかかわるランサムウェア被害

- サイバーインシデントの主要な攻撃手法として2020 年に最も多かったのは「ランサムウェア」の23%
- ランサムウェアの暗号化解除のための平均支払額は年々上昇し、2020 年の四半期平均支払額は16 万9,446ドルと、2019 年に比べ288.7% 上昇
- ランサムウェアによるサイバー攻撃のうち59% が、ランサムウェアによるデータの暗号化に加えて、機密情報の窃取を行う「二重の脅迫」を用いた戦術
- 2020 年に公表された情報漏えいのうち、ランサムウェア関連のデータ漏えいが36%
- ランサムウェアの被害企業と窃取情報を掲載するための暴露サイト22 種 – 投稿件数急増

➢生産の一時停止はもとより、決算発表の延期を余儀なくされるケースも

[Source]独立行政法人情報処理推進機構（IPA） , 情報セキュリティ白書2021, IPA, 2021, https://www.ipa.go.jp/files/000094186.pdf, p.10 ,(access 2022/4/12)

後発的に発見される脆弱性への対応（NISTIR 8374 ）

- 関連するシステムへの完全なパッチの適用。スケジュールされたチェックを実行して利用可能なパッチを特定し、可能な限り早くインストールする。
- すべてのネットワークシステムでのゼロトラスト原則の採用。すべてのネットワーク機能へのアクセスを管理し、マルウェアが潜在的なターゲットシステム間で増殖するのを防ぐため、実現可能な場合は内部ネットワークをセグメント化。
- 許可されたアプリのインストールと実行のみを許可。許可されたアプリケーションのみを実行するようにオペレーティングシステムやサードパーティソフトウェアを構成。これは、レビュー用のポリシーを採用し、許可リストで許可されたアプリケーションを追加または削除することによってサポートできる。
- ランサムウェア攻撃を阻止する手段を適用することを期待している旨、テクノロジーベンダーに書面で通知する。

[Source] William C. Barker, William Fisher, Karen Scarfone, Murugiah Souppaya, NISTIR 8374 Ransomware Risk Management: A Cybersecurity Framework, National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8374.pdf(2022/04/12) pp.2-3 (発表者仮訳)

基準はそれぞれの組織のコンテキストに臨機に対応できる原則ベースへ

- PMBOK第7版のプロジェクトマネジメントの原理・原則
  - 原則 1　勤勉で、敬意を払い、面倒見のよいスチュワードであること
  - 原則 2　協働的なプロジェクト・チーム環境を構築すること
  - 原則 3　ステークホルダーと効果的に関わること
  - 原則 4　価値に焦点を当てること
  - 原則 5　システムの相互作用を認識し、評価し、対応すること
  - 原則 6　リーダーシップを示すこと
  - 原則 7　状況に基づいてテーラリングすること
  - 原則 8　プロセスと成果物に品質を組み込むこと
  - 原則 9　複雑さに対処すること
  - 原則10　リスク対応を最適化すること
  - 原則11　適応力と回復力を持つこと
  - 原則12　想定した将来の状態を達成するために変革できるようにすること

[Source] Project Management Institute, Inc., プロジェクトマネジメント知識体系ガイド（PMBOKガイド）第7版＋プロジェクトマネジメント標準, PMI日本支部, 2021, p.23

監査保証の判断基準研究プロジェクト 2022年度の活動の方向性

- システム管理基準追補版相当の「自主規制ガイダンス」の検討
  （※経済産業省の基準改定の検討とは関係ありません）
- GOVERNANCE OF THE EXTENDED ENTERPRISE翻訳
- EU　Data Governance Act翻訳
- その他 ビジネスとシステムおよび社会課題への取り組みにかかる最新動向等の研究
  …等

- 原則毎月　Zoomオンラインで開催
- 本日の続きを含め、2022年度の定例研究会での中間報告を予定しています

※　確定した計画は後日学会サイトに掲載いたします

Thank you

この資料の内容は、研究プロジェクト各メンバーの所属会社、所属組織等とは関係ありません。