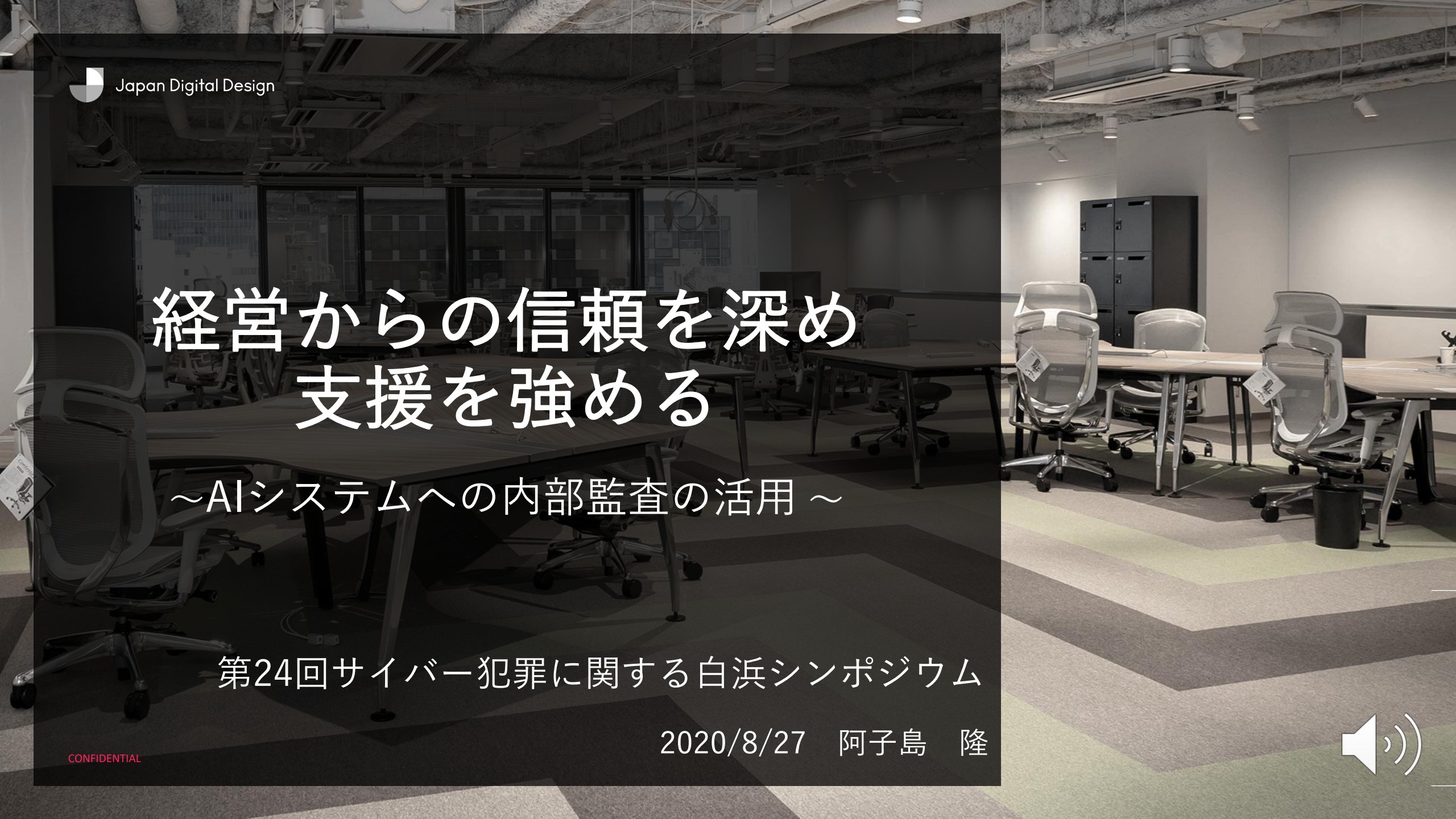


Japan Digital Design

# 経営からの信頼を深め支援を強める

## ～AIシステムへの内部監査の活用～

第24回サイバー犯罪に関する白浜シンポジウム

2020/8/27　阿子島　隆

Agenda

1. サイバーセキュリティ経営ガイドラインV2.0
2. ＡＩシステム監査の視点
3. ＡＩシステム開発・運用の特徴
4. ＡＩシステム監査～ポイントとプロセス
5. ＡＩシステム監査～監査実施モデル

Appendix

説明者の説明・本資料は説明者の見解であり、Japan Digital Designの見解を表したものではありません。

Agenda

# ０．はじめに

1. サイバーセキュリティ経営ガイドラインV2.0
2. ＡＩシステム監査の視点
3. ＡＩシステム開発・運用の特徴
4. ＡＩシステム監査～ポイントとプロセス
5. ＡＩシステム監査～監査実施モデル

# 阿子島　隆（あこしま　たかし）

**Japan Digital Design**

Technology & Design Div. /
Corporate Planning Div.
Internal　Auditor
CISA　CIA　CCSA　CFE

## ＩＴ

ＰＧ・ＳＥ・基盤・
構想・企画・開発・
ＰＭ・合併（システム統合）

1984～2004

日清紡
プルデンシャル生命
日本火災・日本興亜損保
（現 損保ジャパン）

1983~1984
日清紡
経理

## 業務

2004～2016

SOMPOひまわり生命
合併（事務統合）
保険契約管理・保険金等支払

**Japan Digital Design**
2020/4～

## 監査

2016
～2020/3

IT監査
業務監査

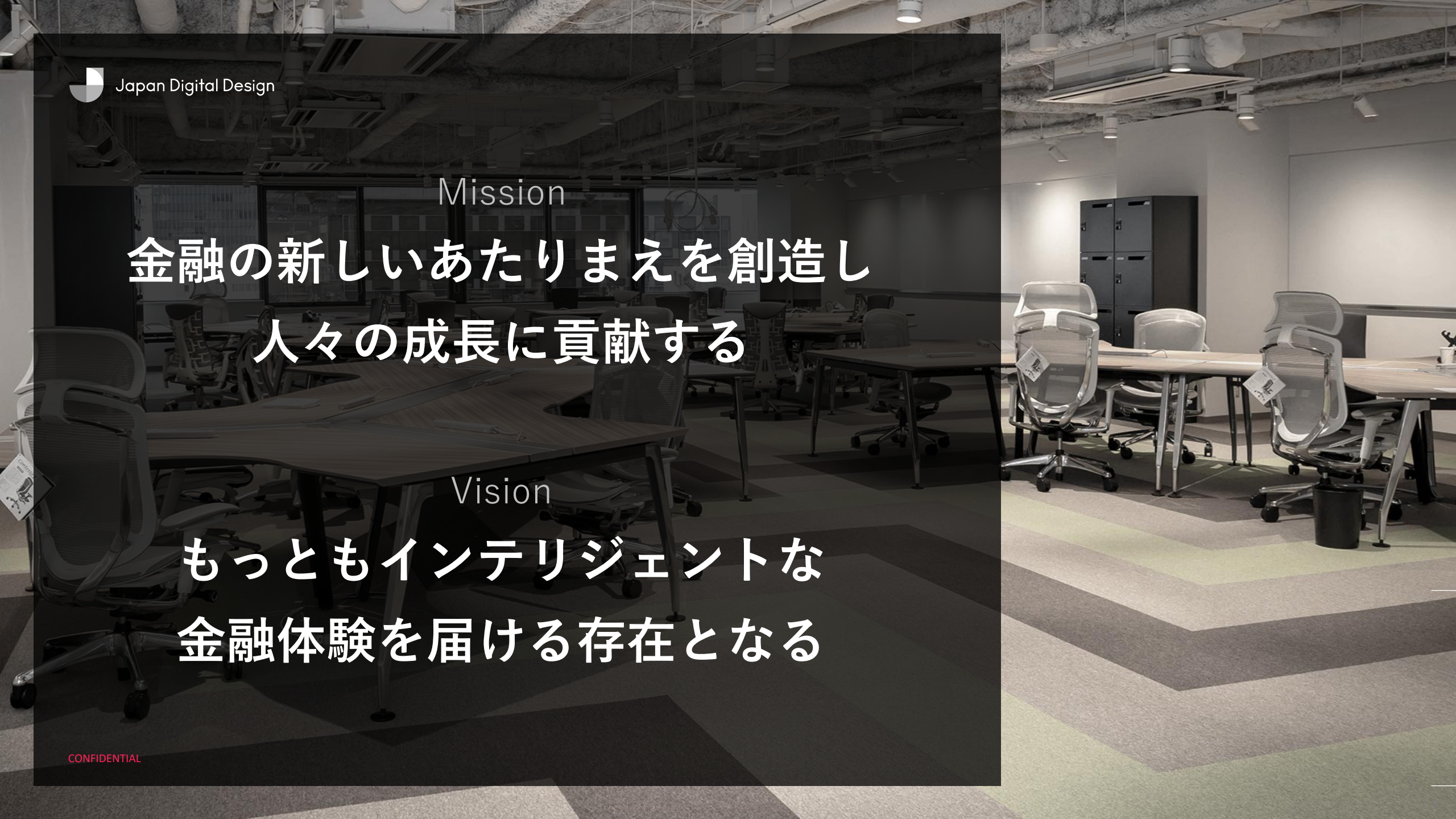
## 社外活動

- ✓ 日本内部監査協会
- ✓ ISACA東京支部
- ✓ 情報処理技術者試験委員・情報処理安全確保支援士試験委員

# Japan Digital Design

- ✓ 2017年10月02日 設立
- ✓ 三菱UFJフィナンシャル・グループの直接子会社
- ✓ 「銀行業高度化等子会社」

  銀行および銀行持ち株会社は、他業禁止として子会社にできる業種が規制されていましたが、改正銀行法(2017/04)によっていわゆるFinTech子会社が認めれられることとなりました



Japan Digital Design

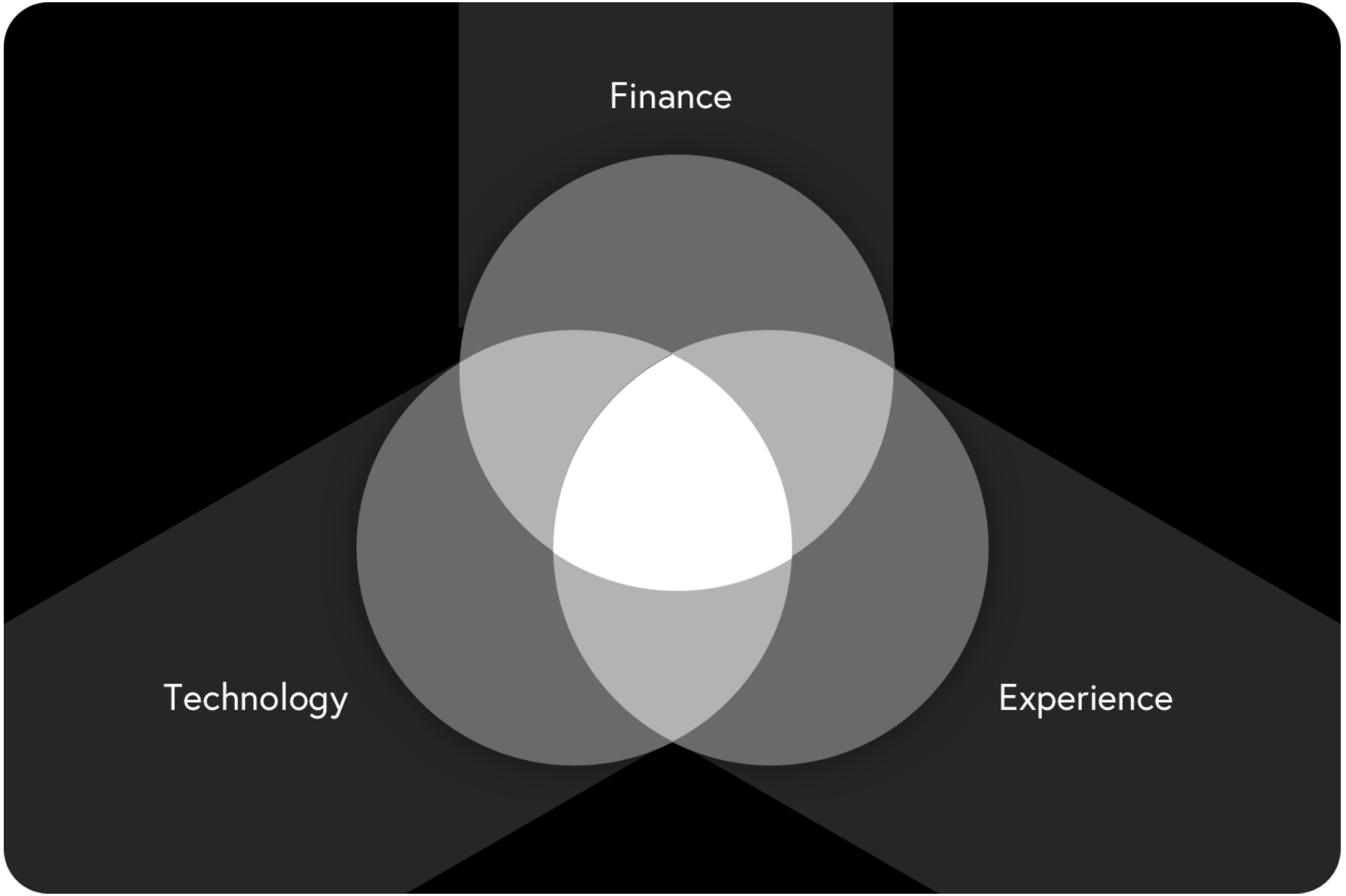
Mission

# 金融の新しいあたりまえを創造し
# 人々の成長に貢献する

Vision

# もっともインテリジェントな
# 金融体験を届ける存在となる

JDDのご紹介




金融ビジネス、テクノロジー、体験デザインの機能が融合されたチームを社内に組成し、新規事業アイデアの創出からAI研究開発、技術実証実験、社会実装までを高速に実現できる組織を目指します。

# Careers

Principles

## 常に学び誰よりも早く実践する

環境の変化をとらえ、自ら学び、すぐに実践する
新しいことに挑戦し、実践を通じて自らを成長させる

## オープンマインドである

常識や固定概念にとらわれず、物事の本質を見極める
グローバルな視点に立ち、多様な価値観を受け入れる

## プロフェッショナルである

強い意思を持ち、目標に向かって最後までやりきる
自由と責任の分別を持ち、自らを律する

雇用体系も新しく：副業**が**できる、副業**で**できる、
勤務体系：**週１日～週５日まで、多様な働き方**があります
詳しくは　▶　https://open.talentio.com/1/c/japan-d2/requisitions/920

Agenda

1. サイバーセキュリティ経営ガイドラインV2.0
2. ＡＩシステム監査の視点
3. ＡＩシステム開発・運用の特徴
4. ＡＩシステムの監査～ポイントとプロセス
5. ＡＩシステムの監査～監査実施モデル

## ■ サイバーセキュリティは経営問題

✓ セキュリティ対策の実施を「コスト」と捉えるのではなく、**将来の事業活動・成長に必須なもの**と位置づけて**「投資」**と捉えることが重要

## ■ 経営者が認識すべき3原則

✓ 経営者は、サイバーセキュリティ**リスクを認識**し、**リーダーシップによって対策を進める**ことが必要

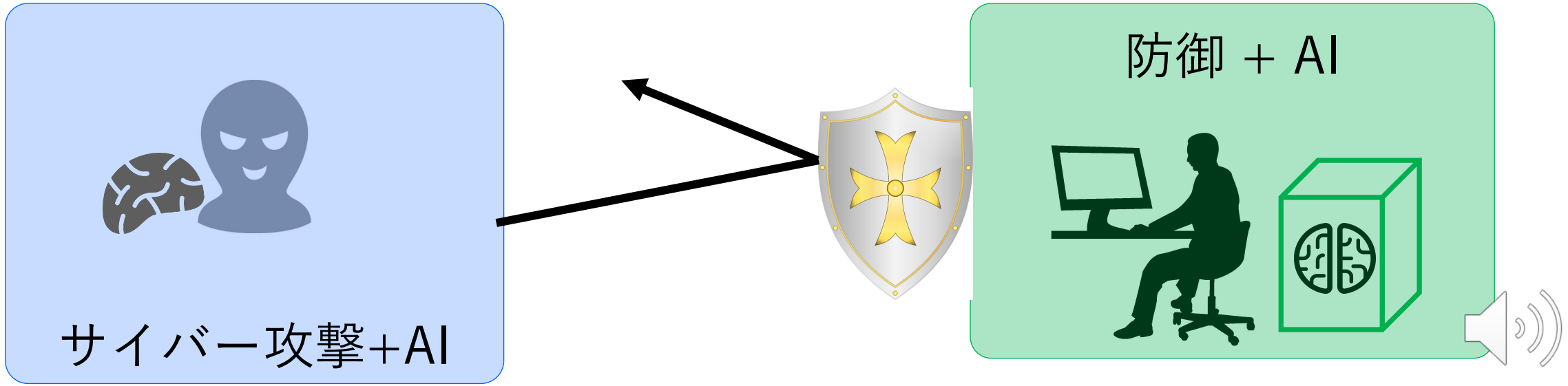
✓ 自社は勿論のこと、ビジネスパートナーや委託先も含めた**サプライチェーンに対するセキュリティ対策**が必要

✓ 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、**関係者との適切なコミュニケーション**が必要

## ■ 経営者

セキュリティ対策の実施 ＝ コスト

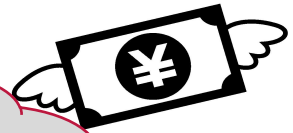
将来の 事業活動・成長に必須なもの ＝ 投資



ＡＩ

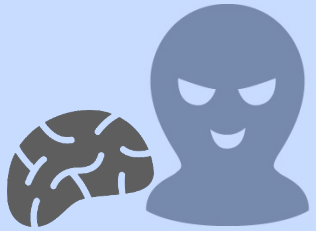
サイバーセキュリティ

ＩＤＳ　ＩＰＳ　ＳＩＥＭ　ＷＡＦ・・・
End Point Security ・・・・・

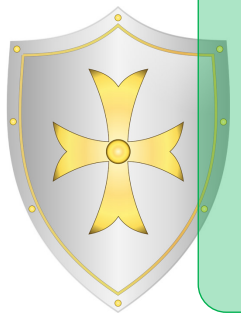


？？？？
○？　Ｘ？

最新の・・



サイバー攻撃+AI



防御 + AI

## ■ 内部監査に求められていること

◆内部監査は、規程・マニュアルの違反をみつけたり、営業店の 成績をつけることではない。

◆金融機関には「内部監査を通じて、自律的な経営改善を図る」 ことが求められている。

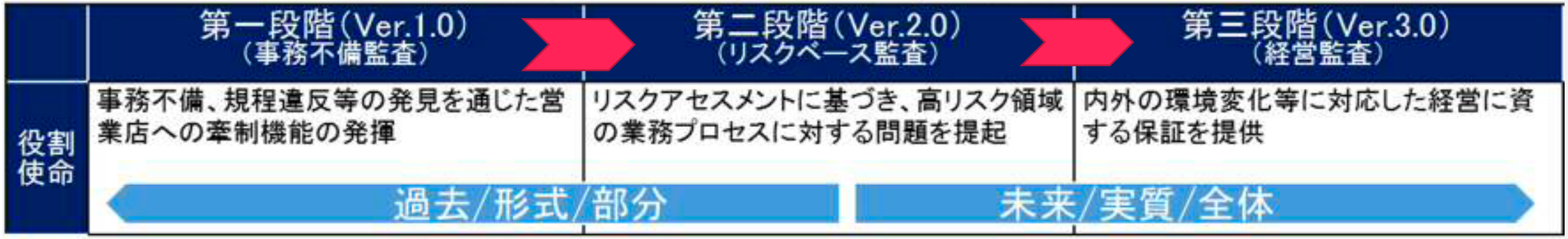
- ✓ 経営にとって重要なリスクを識別する。
- ✓ 重要な問題があれば指摘する。
- ✓ 自ら対応策を提言したり、関係部署にその策定を促す。
- ✓ 問題の改善が図られたことを確認する。

（内部監査態勢の整備　2019年9月　日本銀行金融機構局 金融高度化センター　より）

# ■ 内部監査の高度化　（金融機関の内部監査の高度化に向けた現状と課題　令和元年6月　金融庁）

- ➢ 事後チェック型監査からフォワードルッキング型監査への転換　（過去から未来へ）
- ➢ 準拠性監査から経営監査への転換　（形式から実質へ、部分監査から全体監査へ）

図表１　内部監査の水準（概念図）



■ 内部監査の実施 ・・積極的協力、情報提供→課題の発見→改善（予算措置）

## ● サイバーセキュリティ対応の適切性・有効性

例

✓ フレームワーク（NIST、NISC、IPA・・）

✓ **入口対策**
（F/W・WAF・IDS・IPS・ウイルス対策ソフト・従業員教育）

✓ **出口対策**
（通信の検知・遮断）

✓ **内部対策**
（不審ソフトの強制終了・ファイル暗号化・管理者モニタリング・ウイルスチェック）

✓ **新技術（ＡＩの有効性評価・導入効果・他社事例）**

例

## ■ 内部監査の評価 → 経営層へ報告

- 好取り組み・・適切性・有効性・効率性に優れた対応

- 課題の明確化・・
  - ✓ 業界他社や類似業種との比較
  - ✓ リスクベース
  - ✓ 脆弱性
  - ✓ 経営課題として、取り組みが必要（資源投入：ヒト・モノ・カネ）

- 客観的評価者：経営者に意見。リスクの明示。背中を押す。

Agenda

1. サイバーセキュリティ経営ガイドラインV2.0
2. ＡＩシステム監査の視点
   （１）加速するAI利用
   （２）ＡＩシステム監査の視点
3. ＡＩシステム開発・運用の特徴
4. ＡＩシステム監査～ポイントとプロセス
5. ＡＩシステム監査～監査実施モデル

# 2．AIシステムの監査の視点

## （１）加速するＡＩ利用

製造業：IHI・故障予知診断、予防保全

運輸：NVIDIA・SoCサプライヤー　　SoC: System on Chip

インフラ：パナソニック・インフラ点検サービス

農業：ボッシュ・病害予診断測

医療：日立製作所・画像による支援

防犯：NEC・画像による不審者の自動分類

金融：SMBCFG/JCB・不正検知　ＡＩ

金融：投資/運用・三菱UFJ国際投信

金融：審査・みずほ銀行（Ｊスコア）

金融：顧客サービス・三井住友銀行

「AI白書2019」（IPA）をもとに阿子島が作成

# （２） AIシステムの監査の視点

リスクは？　　そもそも監査必要？

監査項目は？　　監査プロセスは？

監査手法は？　　AIに詳しい？？

どのようにして
監査を実施するか

・基準や指針

＋

・AIの一定の専門知識

1210 — 熟達した専門的能力 内部監査人は、自らの職責を果たすために必要な「知識、技能およびその他の能力」を備えていなければならない。
（IIA：専門職的実施の国際フレームワーク　IPPF）

# （２） AIシステムの監査の視点

## 明確な基準や指針が見つからない場合

手がかりを探す

①公表されている「システム監査」の基準・指針・ガイドライン

②有識者の講演内容・書籍・試案・ISACAでの研究活動

③ＡIシステム特有の開発工程や事象（事項）に注目

④各国から出される指針的情報

作る

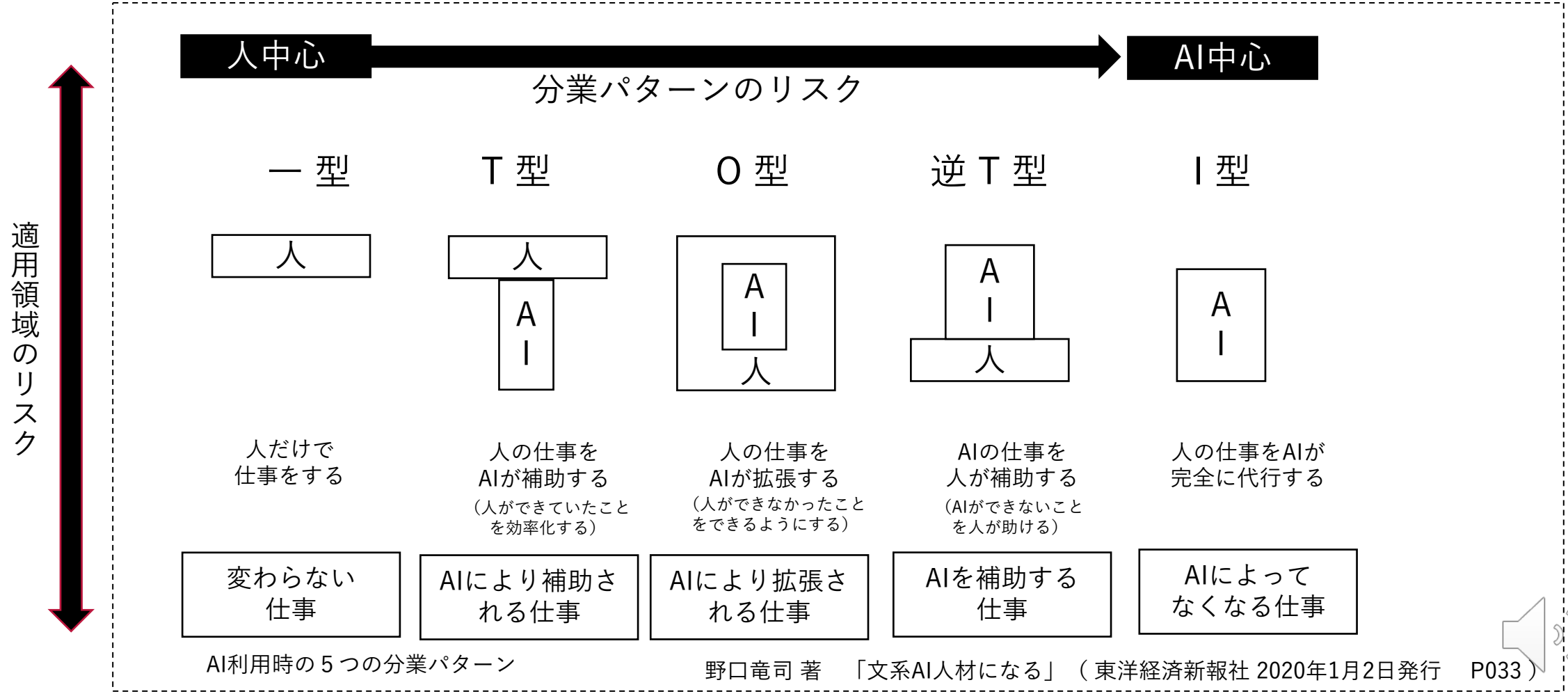
- ✓ 全体像を作る
- ✓ 自社のＡＩシステムに適合する事項に焦点をあてる
- ✓ チェック項目を抽出し、AIシステムのリスクを把握・評価する

# 【参考】ＡＩシステムのリスク　～どのように把握・評価するか～

リスクとは、目標の達成に影響を与える事象発生の可能性（IIA：専門職的実施の国際フレームワーク　IPPF）

リスク ＝ [ 適用領域 × 分業パターン ] × 発生可能性

影響のおおきさ




AI利用時の５つの分業パターン

野口竜司 著　「文系AI人材になる」（ 東洋経済新報社 2020年1月2日発行　P033 ）

Agenda

1. サイバーセキュリティ経営ガイドラインV2.0
2. ＡＩシステムの監査の視点
3. ＡＩシステム開発・運用の特徴
4. ＡＩシステム監査のポイントとプロセス
5. ＡＩ利用システムの監査実施モデル

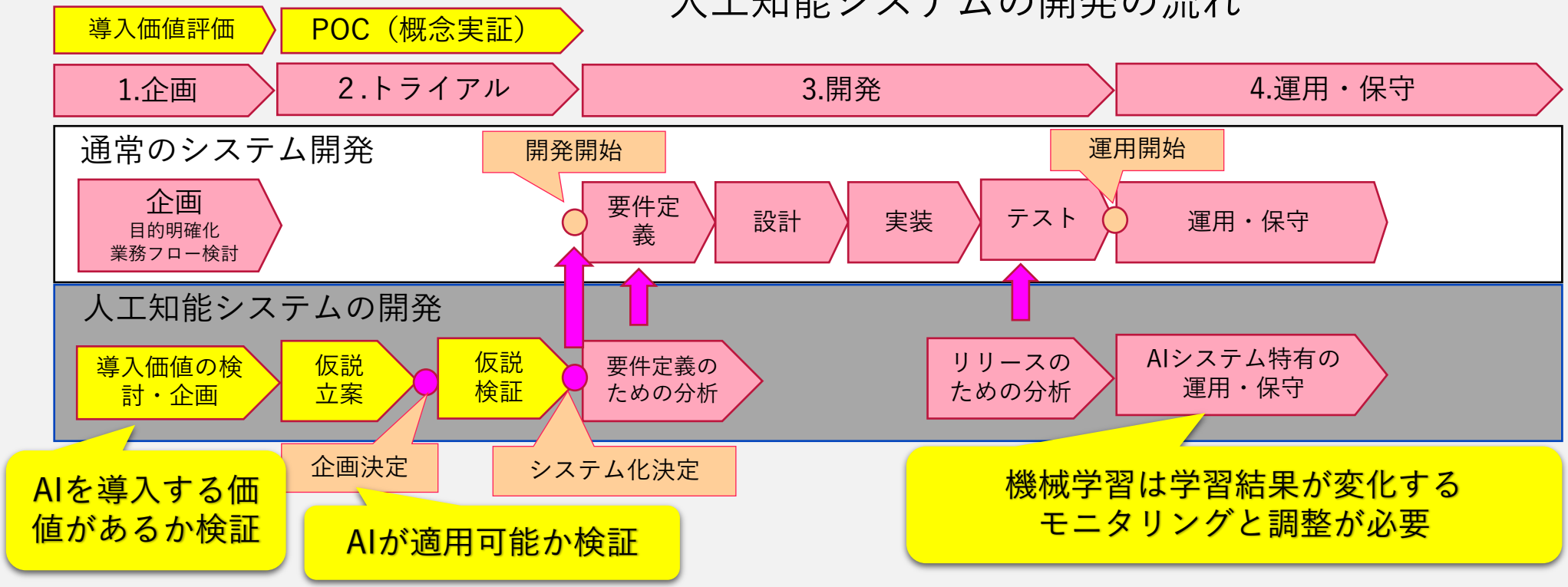
# 3．AIシステム開発・運用の特徴

AIシステム特有の開発・運用工程

特有の工程やAI自体の特性に着目

✓ AIシステムの特徴的な工程を把握
✓ リスクを認識

## 人工知能システムの開発の流れ




本橋洋介著「人工知能システムのプロジェクトがわかる本－企画・開発から運用・保守まで－」翔泳社2018年2月15日初版を参考に作成、一部阿子島が追記。

Agenda

1. サイバーセキュリティ経営ガイドラインV2.0
2. ＡＩシステム監査の視点
3. ＡＩシステム開発・運用の特徴
4. ＡＩシステム監査のポイントとプロセス
5. ＡＩシステム監査～実施モデル

4.ＡＩシステム監査のポイント・プロセス

監査のポイント（基準）

実施プロセス（手法）

実施する内部監査の
✓ 妥当性
✓ 有効性
✓ 効率性

| | （A）ポイント（基準） | （B）プロセス（手法） |
|---|---|---|
| ①「システム監査」の基準・指針やガイドライン | ◎ | ◎ |
| ②AIシステム特有の開発工程や事象（事項）に着目 | ◎ | ◎ |
| ③有識者の講演・書籍・試案、ISACAでの研究活動で情報 | ◎ | ○ |
| ④各国から出される指針的情報 | ◎ | ○ |

# （A）監査ポイント（基準）は

（１）７つのポイント

①AIガバナンス

②AIシステム開発
・変更管理

③データ管理

④運用管理

⑤利用者支援

⑥安全対策

⑦AIシステム間連携

# 詳しくみると

## ①AIガバナンス

### 基本方針

- 導入と開発の方針・原則
- 経営の承認
- 関係者への周知
- 人間の尊重と個人の尊厳

### 管理態勢

- 責任者の明確化
- 開発・運用・保守体制
- 関係者の権限と責任
- ホワイトボックス・ブラックボックスの境界明確化と説明責任
- リスク＆コントロール

## ②AIシステム開発・変更

### 企画・計画

- 開発･導入計画策定
- 計画の経営承認
- リスク＆コントロール
- 費用対効果の明示
- 開発計画の妥当性
- 達成目標・撤退基準

### 開発

- 機能条件・利用条件
- テスト実施・UAT
- プロジェクト管理

## ④運用管理

### 保守運用

- ビックデータの考慮
- 保守工程の考慮
- 目的通りの運用

### 可用性・BCP

- 可用性・BCP
- 廃棄計画
- データ廃棄

## ③データ管理

### 入力

- 信頼性
- 網羅性・十分性
- プライバシー保護

### 処理

- 学習モデルの適切性
- 学習モデルの定義・検証可能性
- 学習モデルの権利帰属

### 出力

- 出力結果の検証・不適切結果への補正
- 出力結果のプライバシー侵害防止対策

## ⑤利用者支援

### アカウンタビリティ

- ステークホルダへの説明責任
- AIシステムの技術特性の情報提供・受領

### 利用者支援

- AI特性の理解促進・支援機能の提供
- 利用を選択する機会の提供

## ⑥安全対策

### 生命・身体・財産

- AIシステムの結果が危害を及ぼさない考慮
- AI判断と人間判断の責任分岐点の明確化

### 倫理

- 個人の尊厳や自律の尊重

### 制御可能性

- 開発時に制御可能性の考慮
- リスク評価時の制御可能性の考慮

### セキュリティ管理

- 可用性・インテグリティ・機密性の確保
- オープンソースの利用有無、技術の確認

### プライバシー

- プライバシー保護対策
- プライバシー侵害の検知

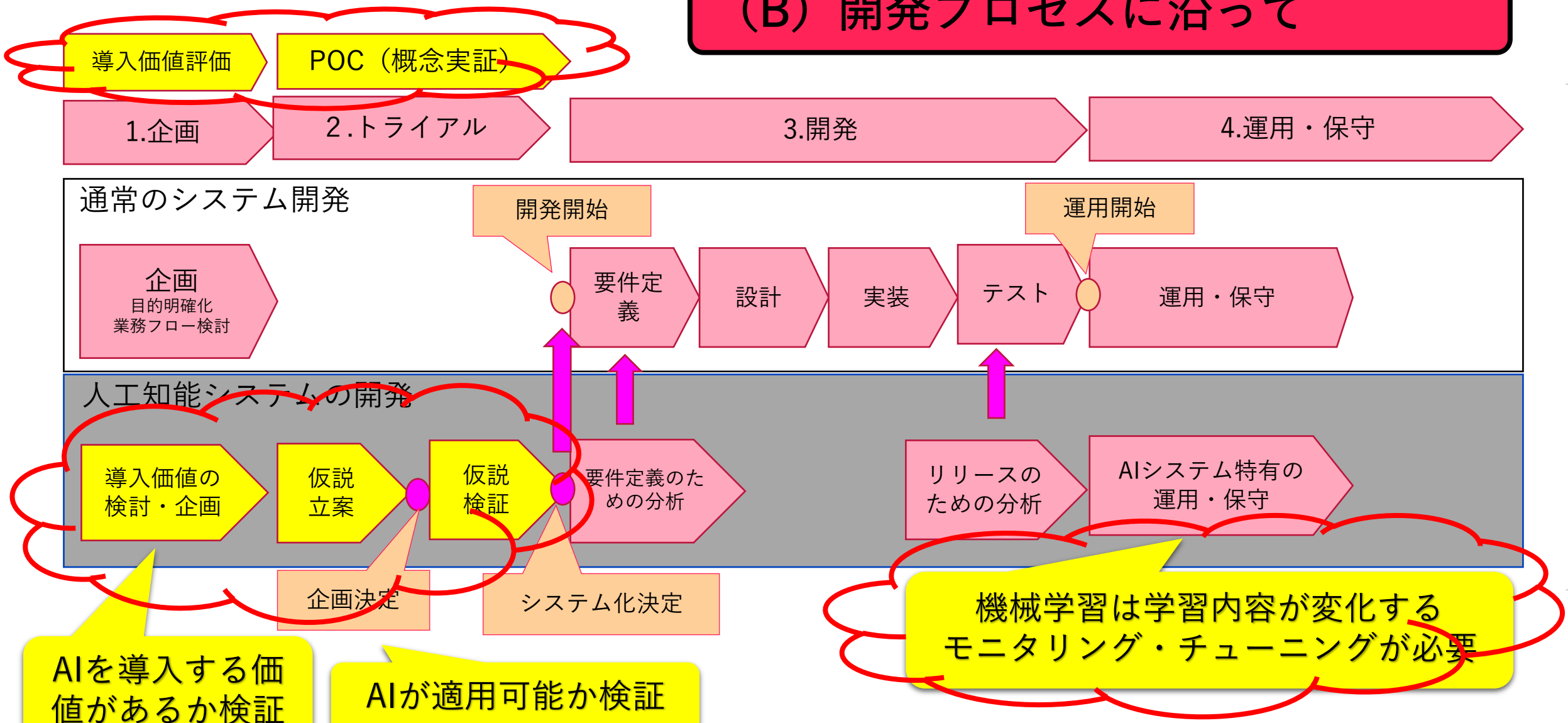
### 知的財産

- 知的財産権の考慮

## ⑦AIシステム間連携

- 連携を考慮した運用
- 相互接続のリスク

# （B）開発プロセスに沿って




本橋洋介著「人工知能システムのプロジェクトがわかる本－企画・開発から運用・保守まで－」（翔泳社2018年2月15日初版）　を参考に作成、一部阿子島が追記。

Agenda

1. サイバーセキュリティ経営ガイドラインV2.0
2. ＡＩシステム監査の視点
3. ＡＩシステム開発・運用の特徴
4. ＡＩシステムの監査～ポイントとプロセス
5. ＡＩシステム監査～実施モデル

- 「監査ポイント（基準）」について、・・「基準」
- ＡＩシステムの開発プロセスに沿ってインタビューする・・「手法」


## ◆ ＡＩシステムに特有な工程 ◆

❶価値評価（経営への価値）、❷POC（概念実証）
❻学習と評価、チューニング、❽ユーザー教育
❿学習の再評価（過学習していないか）

## ◆ 通常のシステム開発工程 ◆

③要件定義（業務要件・システム要件）
④設計　⑤開発（実装）⑦テスト（ST・UAT）
⑧導入　⑨運用

# AIシステムの監査実施モデル（案）

When

（◎強く確認、○確認）

| 監査プロセス（開発工程） / ポイント（What） | ❶価値評価 | ❷POC | ③要件定義 | ④設計 | ⑤開発（実装） | ❻学習と評価、チューニング | ⑦テスト | ❽導入ユーザー教育 | ⑧運用 | ❿学習の再評価 |
|---|---|---|---|---|---|---|---|---|---|---|
| ①AIガバナンス | ◎ | ◎ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| ②AIシステム開発・変更管理 | ○ | ○ | ◎ | ◎ | ◎ | ○ | ○ | ○ | ○ | ○ |
| ③データ管理 | ◎ | ◎ | ◎ | ◎ | ○ | ◎ | ◎ | ○ | ◎ | ◎ |
| ④運用管理 | ○ | ○ | ◎ | ◎ | ○ | ◎ | ◎ | | ◎ | ◎ |
| ⑤利用者支援 | ○ | | ◎ | ◎ | | | ○ | ◎ | ◎ | ○ |
| ⑥安全対策 | ◎ | | ◎ | ○ | How | | ○ | ◎ | ◎ | ○ |
| ⑦AIシステム間連携 | ◎ | | ◎ | ◎ | | ○ | ○ | ○ | ◎ | ○ |

# 監査プロセスで何をどうチェックする？　求める証跡・インタビューの内容は？



| ①　AIガバナンス | | |
|---|---|---|
| 基本方針 | 導入と開発の方針・原則 | AIシステムに関わる開発と活用の方針やAI開発原則は策定されているか？ |
| | 経営層の承認 | AIシステムに関わる基本方針は経営層により承認されているか？ |
| | 関係者への周知 | 定められた基本方針がAIシステムの開発者、運用、保守および利用者に周知されているか？ |
| | 人間の尊重と個人の尊厳 | 基本方針に人間の尊厳と個人の自律を尊重する倫理原則は含まれているか？ |
| 管理態勢 | 責任者の明確化 | AIシステムについての責任体制（開発・運用・保守・利用）が明確になっているか？ |
| | 開発・運用・保守体制 | AIシステムの開発、運用、保守の体制は整備されているか？ |
| | 関係者の権限と責任 | AIシステムに関わる者の責任、権限は明確になっているか？ |
| | ホワイトボックス・ブラックボックスの境界明確化と説明責任 | AIシステムで行う処理について「ホワイトボックス」「ブラックボックス」の境界を明確にし、説明可能になっているか？ |
| | リスク＆コントロール | AIシステムに係るリスク評価は実施されているか？<br>AIシステムに係るリスクを識別しコントロールを定義しているか？ |

| ② AIシステムの開発と変更管理 | | |
|---|---|---|
| 計画 | 開発・導入計画策定 | AIシステムの開発計画は策定されているか？ |
| | 計画の経営承認 | AIシステムに関わる開発計画は経営層により承認されているか？ |
| | リスク＆コントロール | 開発計画にはリスク分析とその対応は考慮されているか？ |
| | 費用対効果の明示 | AIシステムの開発計画の費用対効果は明確になっているか？ |
| | 開発計画の妥当性 | AIシステムの開発スケジュールは適切に設定されているか？ |
| | 達成目標・撤退基準 | AIシステムの開発に関する達成目標が設定され、推進、もしくは撤退に関する判断ポイントは設定されているか？ |
| 実施 | 機能条件・利用条件 | AIシステムの機能、および非機能を含めた要件が定義され、設計書は策定されているか？<br>AIシステムの開発や利用条件は適切に設定されているか？ |
| | テスト実施・UAT | AIシステムに関するテスト、もしくは動作検証（ｼｽﾃﾑ・ﾕｰｻﾞｰ）は行われているか？ |
| | プロジェクト管理 | 開発プロジェクトの管理は適切に行われているか？ |

| ③　データ管理 | | |
|---|---|---|
| 入力 | 信頼性 | ＡＩシステムに入力するデータの信頼性を検証しているか？ |
| | 網羅性・十分性 | ＡＩシステムに入力するデータの網羅性・十分性を確認しているか？ |
| | プライバシー保護 | AIシステムに入力するデータに個人情報が含まれている場合には、プライバシーの保護対策を講じているか？ |
| 処理 | 学習モデルの適切性 | ＡＩシステムで行うデータ処理で使用する、学習モデルの適切性を確認しているか？ |
| | 学習モデルの定義・検証可能性 | ＡＩシステムで行うデータ処理で使用する、学習モデルは明確に定義され、検証可能となっているか？ |
| | 学習モデルの権利帰属 | ＡＩシステムで行うデータ処理に利用する、学習モデルの権利帰属について取り決めをしているか？ |
| 出力 | 出力結果の検証・不適切結果への補正 | AIシステムで出力した結果は適切か、また不適切な結果が出た場合の補正の扱いは決められているか？ |
| | 出力結果のプライバシー侵害防止対策 | AIシステムで出力した結果について、利用者及び第三者のプライバシー侵害の防止対策を実施しているか？ |

| ④　運用管理 | | |
|---|---|---|
| 保守・運用 | ビックデータの考慮 | ビッグデータとの連携は行われているか。正確に実施されているか？適切性を評価しているか？ |
| | 保守工程の考慮 | AIシステムの保守は定義されているか。適切に実施されているか？ |
| | 目的通りの運用 | AIシステムは当初の目的通り利用されているか。<br>想定内、想定外は明確になっているか？ |
| 可用性・BCP | 可用性・BCP | AIシステムの可用性を確保しているか。<br>障害発生時の対応は考えられているか？ |
| | 廃棄計画 | AIシステムの廃棄後の事務・システムの対応は考えられているか？（システム移行、ｏｒ代替システム） |
| | データ廃棄 | ＡＩシステムのデータ廃棄は考慮されているか。適切に行われているか？ |

| ⑤　利用者支援 | | |
|---|---|---|
| アカウンタビリティ | ステークホルダへの説明責任 | AIを利用するシステムでステークホルダーに対して説明責任が果たせるような対応がなされているか？ |
| | AIシステムの技術特性の情報提供の受領 | AIを利用するシステムの技術的特性について、AI開発会社から情報提供と説明を受けているか（AI開発会社のアカウンタビリティ） |
| 利用者支援 | AI特性の理解促進と支援機能の提供 | AIを利用するシステムで利用者が、AIの特性やリスクを理解し、利用に当たっての支援を受けられる機能を持っているか？ |
| | 利用を選択する機会の提供 | AIを利用するシステムで利用者にAI利用の選択の機会が提供できるようになっているか？ |

# ⑥　安全対策

| | | |
|---|---|---|
| 生命・身体・財産 | AIシステムの結果が危害を及ぼさない考慮 | AIシステムの判断、分析結果等が利用者や第三者の生命・身体・財産に危害を及ぼすことがないような考慮をしているか？ |
| | AI判断と人間判断の責任分岐点の明確化 | AIシステムの判断と、人間の判断の責任分界点（境界）を明確にしているか？ |
| 倫理 | 個人の尊厳や自律の尊重 | AIを利用するシステムの開発で個人の尊厳や自律を尊重するようなことを考慮しているか？ |
| 制御可能性 | 開発時に制御可能性の考慮 | 制御可能性という観点でAIを利用するシステムを開発しているか？ |
| | リスク評価時の制御可能性の考慮 | 制御可能性という観点でリスクを評価しているか？ |
| セキュリティ管理 | 可用性・インテグリティ・機密性の確保 | AIを利用するシステムで可用性、インテグリティ、機密性を確保しているか? |
| | オープンソースの利用有無、技術の確認 | AIを利用するシステムでオープンソースの技術を使用しているか？<br>また、オープンソース技術利用上で特別に考慮していることはあるか？ |
| プライバシー | プライバシー保護 | AIを利用するシステムの開発と利用でプライバシー保護の対策は？ |
| | プライバシー侵害 | AIを利用するシステムの開発と利用でプライバシー侵害をモニタリングし侵害が判明した場合の対応策は考慮しているか？ |
| 知的財産 | 知的財産権の考慮 | 知的財産権保護を考慮した対応をとっているか？ |

| ⑦　AI間連携 | | |
|---|---|---|
| AI間連携 | 連携を考慮した運用 | 他システムとの連携という視点で、AIを利用するシステムの運用で考慮していることはあるか？ |
| | 相互接続のリスク | AIを利用するシステムを相互接続している場合にリスクを検討しているか？ |

Agenda

1. サイバーセキュリティ経営ガイドラインV2.0
2. ＡＩシステム監査の視点
3. ＡＩシステム開発・運用の特徴
4. ＡＩシステムの監査のポイント・手法
5. ＡＩシステムの監査～監査プロセス
6. 最後に

■　AI・DX・サイバー

✓AIの利用は急激に加速

✓デジタルトランスフォーメーションの時代

✓これまでと異なる技術・IT・IoTの利用が加速

✓AI開発原則、開発利用倫理の論議に厚み

■　新型コロナウィルス感染症（COVID-19）

✓ビジネス、政府および地域社会に大きな課題

✓危機への対応、ビジネスの継続（BCP）

✓DXの急加速＝組織存続の重要条件　認識、適用が急加速

✓ＩＴ・セキュリティ・内部監査・リスク評価：課題認識

# Thank you.

Agenda

1. サイバーセキュリティ経営ガイドラインV2.0
2. ＡＩシステム監査の視点
3. ＡＩシステム開発・運用の特徴
4. ＡＩシステムの監査のポイント・手法
5. ＡＩシステムの監査～監査プロセス

Appendix

～監査実施モデルでの証跡例～

# 監査では何をチェックするか？　証跡は？　インタビューの内容は？

| 監査観点 | 確認内容（例） |
|---|---|
| ❶価値評価 | |
| 開発と活用の方針は策定されているか | AI開発原則・導入計画書 |
| 基本方針が経営層により承認されているか | 経営層での審議・承認 |
| 定めた基本方針はAIシステムの開発者、運用、保守および利用者に周知されているか | AI開発原則・関係者間の論議・各種議事録、検討記録 |
| 開発、運用、保守体制の整備、責任・権限は明確か | 開発構想書・基本計画書 |
| 開発計画の費用対効果は明確か | 開発構想書・基本計画書<br>POC評価結果 |

～監査実施モデルでの証跡例～

| 監査観点 | 確認内容（例） |
| --- | --- |
| ❷POC（概念実証） | |
| 「ホワイトボックス」「ブラックボックス」の境界を明確にし、説明可能になっているか | 開発構想書・基本計画書 |
| AIに係るリスクを識別・評価し統制を組み込んでいるか | 開発構想書・基本計画書 |
| インプットとなるデータを事前に評価しているか | POC評価結果 |
| AIの能力と制限・課題を認識・評価しているか | POC評価結果 |

| 監査観点 | 確認内容（例） |
| --- | --- |
| ③要件定義（業務要件・システム要件） | |
| リスクとその対応は考慮されているか | 基本計画書・要件定義書 |
| 開発スケジュールは適切か | 基本計画書・要件定義書 |
| 達成目標が設定され、推進・撤退に関する判断ポイントは設定されているか | 基本計画書・要件定義書 |
| 機能要件・非機能要件、AIの利用範囲や条件は設定されているか | 基本計画書・要件定義書 |
| AIシステムに関するテスト・動作検証の計画はあるか | 基本計画書・要件定義書 |
| ユーザーの教育・習熟工程を考慮しているか | 基本計画書・要件定義書・テスト計画 |
| AIの可用性は定義されているか | 基本計画書・要件定義書・CGP |
| AI（データ）の廃棄を考慮しているか | 基本計画書・要件定義書 |
| データの検証工程とレベルを考慮しているか | 基本計画書・要件定義書 |
| AI非稼働時のBCPを考慮しているか | 基本計画書・要件定義書・CGP |
| 個人情報・機微情報の保護対策を施しているか？ | 基本計画書・要件定義書 |

～監査実施モデルでの証跡例～

| 監査観点 | 確認内容（例） |
| --- | --- |
| ④設計 | |
| 設計書は作成されているか？ | 基本計画書・設計書 |
| 開発スケジュールは適切か | 基本計画書・設計書・WBS |
| 機能要件・非機能要件は定義されているか。 | 要件定義書・設計書 |
| AIの利用範囲や条件は設定されているか | 要件定義書・設計書 |
| 既存システムとの連携を定義しているか | 要件定義書・基盤設計書 |
| ネットワーク・連携を定義しているか | 要件定義書・基盤設計書 |

| 監査観点 | 確認内容（例） |
| --- | --- |
| ⑤開発（実装） | |
| 開発の進捗状況 | 進捗状況表・工数予実表・WBS・各種議事録 |
| 課題の抽出と解決は順調か | 課題管理表・障害管理表・各種議事録 |

～監査実施モデルでの証跡例～

| 監査観点 | 確認内容（例） |
| --- | --- |
| ❻学習と評価、チューニング | |
| 学習の到達目標、確認方法は明確か | 基本計画書・チューニング計画書 |
| チューニングの実施状況と評価状況 | チューニング評価書 |
| 評価への対応（過学習の抑制） | チューニング計画・評価書 |
| 学習の評価者の育成計画 | 要件定義書・部門教育計画 |
| 学習結果やAIの結果を経営層は承認しているか | 経営会議体への報告・審議 |

～監査実施モデルでの証跡例～

| 監査観点 | 確認内容（例） |
| --- | --- |
| ⑦テスト（UT・IT・ST・UAT） | |
| テストの進捗状況（進み遅れ） | テスト工程進捗確認書 |
| テスト工程の完了承認プロセスの妥当性 | 判定会議議事録・次工程承認書 |
| ユーザーの関与状況・テスト日程 | UAT計画書・WBS |
| ユーザー教育計画・実施状況 | ユーザー研修計画・実施報告 |

～監査実施モデルでの証跡例～

| 監査観点 | 確認内容（例） |
| --- | --- |
| ⑧導入、❽ユーザー教育 | |
| 利用者はAIの特性やリスクを理解しているか<br>使用者を支援できる機能を備えているか？ | 要件定義書・ユーザー研修計画・研修実施報告書・<br>ユーザーマニュアル |
| 利用者にAI利用を選択する機会を提供できるようになっているか？ | 要件定義書・ユーザー研修計画・<br>ユーザーマニュアル |
| AI稼働不能時の業務運営要領は準備しているか | 業務運用マニュアル・<br>ユーザーマニュアル |

～監査実施モデルでの証跡例～

| 監査観点 | 確認内容（例） |
| --- | --- |
| ⑨運用 | |
| 運用工程の計画は作られているか | 運用計画書・手順書 |
| AI稼働不能時のBCPはあるか | BCP（通常部分・AI部分） |
| 目的通り利用・運用されているか。<br>想定内・想定外が明確になっているか？ | 障害管理表・開発効果評価・<br>稼働後のチューニング評価書 |
| AIシステムの保守は定義され、実施されているか？ | 運用計画書・障害管理表 |
| AIシステムの運用開始を経営層は承認しているか | 経営会議体への報告・審議 |

～監査実施モデルでの証跡例～

| 監査観点 | 確認内容（例） |
| --- | --- |
| ⑩学習の再評価（過学習していないか検証） | |
| 稼働前・稼働後のチューニング計画はあるか | チューニング計画書・運用計画書 |
| チューニング時の、ユーザーとシステム部門との業務分担は定められているか | チューニング計画書・運用計画書 |
| チューニング時の、評価方法・評価基準は定められているか | チューニング計画書・運用計画書 |
| 運用後のチューニングの実施状況と評価状況 | チューニング評価書 |