民間企業有志による
AI利活用のための
支援ツールに関する報告

2020/3/4

はじめに（ご説明する研究活動について）

- 今回ご説明する「民間企業有志によるAI利活用のための支援ツールに関する報告」は、民間ソフトウェアベンダーのユーザ会において、ＩＣＴに関わるテーマ毎に会員企業の有志が１年間研究した結果をまとめたもののの一つです。
- 本テーマの研究メンバーは、以下企業の情報システム部門等から参加しています。
  - 保険業（損保、生保）、製造業（自動車、化学）、建設業

  ※この活動での提言は、必ずしも各企業を代表した意見ではありませんので、実企業名を記載しておりません。ご了承ください。

目次

1.研究概要

- ✓研究テーマの選定
- ✓背景
- ✓研究の目標
- ✓研究スコープ

2.研究内容

- ✓解決すべき課題
- ✓課題へのアプローチ
- ✓AiALの紹介
- ✓検証について

3.終わりに

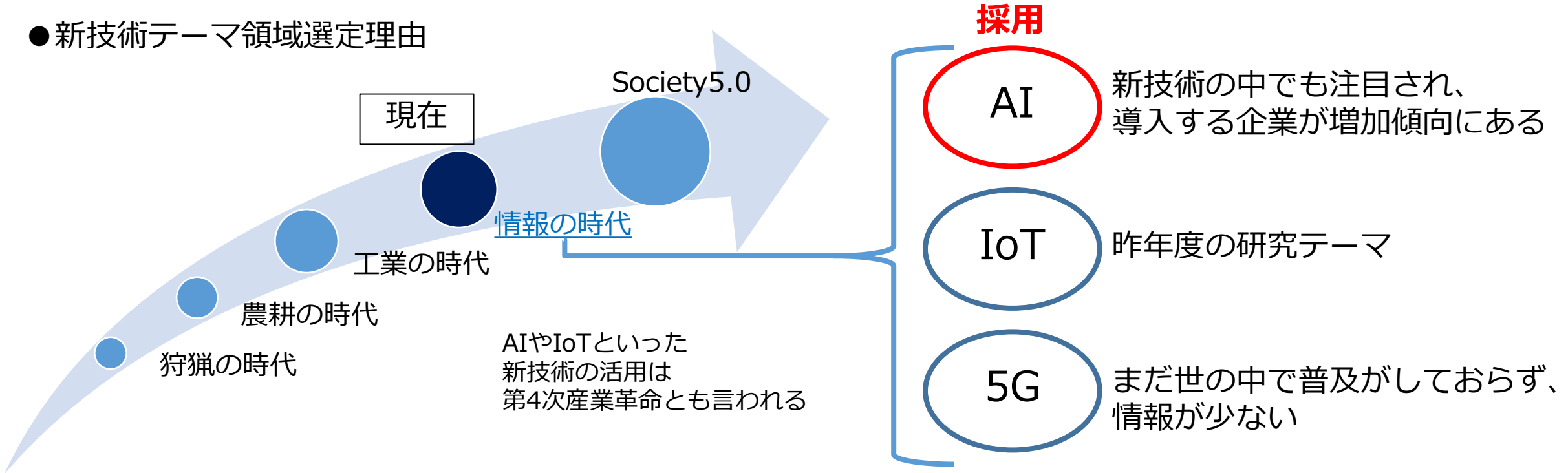
- ✓考察
- ✓今後の展望

研究テーマの選定

●企業の情報セキュリティを考える分科会 募集要項

概要：企業内の情報セキュリティは、従来からの範疇だけでなく、
IoT機器との連携や国際ルールへの対応など、その守備範囲は広がってきています。
また、日本で行われる大規模なイベント（オリンピックやワールドカップ）などに乗じた悪質な攻撃も懸念されています。本分科会では、現在の情報セキュリティの課題を広い視野で洗い出し、今後、企業として必要となる情報セキュリティを検討・検証します。

●新技術テーマ領域選定理由

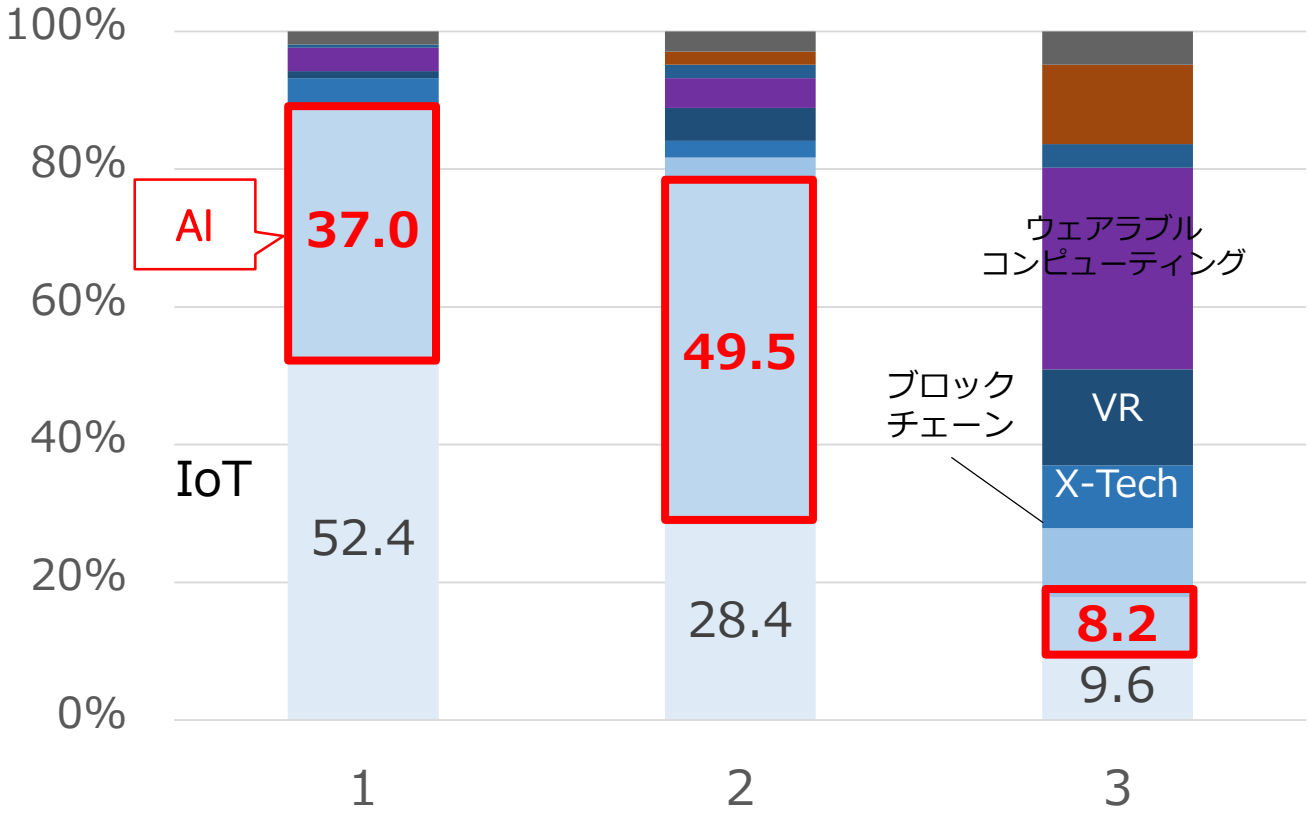


背景

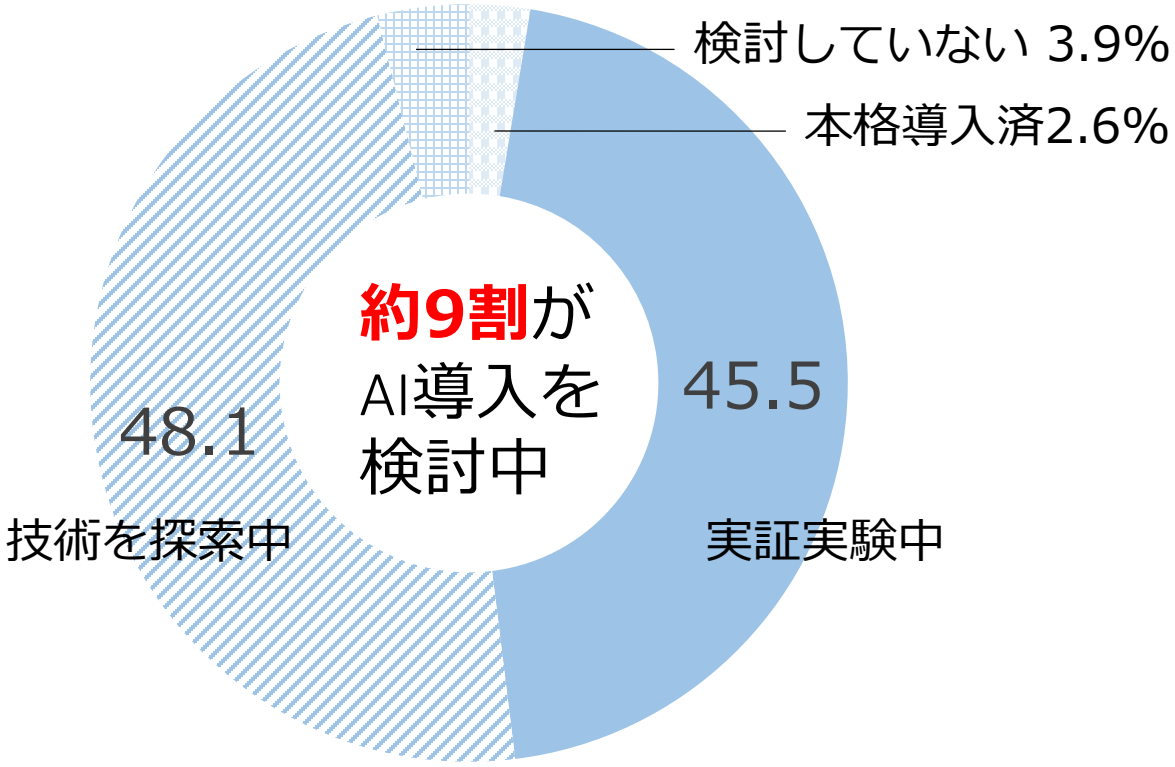
多くの企業でAIの導入について関心が高く、導入を検討している

企業が着目するデジタルビジネス領域（n=207）

nはアンケート対象企業数



AIを1位に選んだ企業の導入検討状況（n=77）



(2017) 【JUAS】20170518 デジタル化の進展に対する意識調査.pdfより

研究目標

【最終成果物】

AIの導入を検討している企業がセキュアに導入するためのチェックリスト

【選定の経緯】

新技術の中でも注目されているAIだが、**未だ厳密に定義されていない**。
その中で、AI利活用は情報セキュリティの検討が不十分なのではないかと考えた。
また、業界・企業規模に関わらず、AI利活用において
情報セキュリティを検証できるツールは有用であると考えた。
今回、総務省が作成した「AI利活用ガイドライン」を参考にしつつ、AIの利用形態を整理し、アクターや責任分界点を確認した。

研究スコープ

日本でまだ着手できていない領域を研究の対象とした

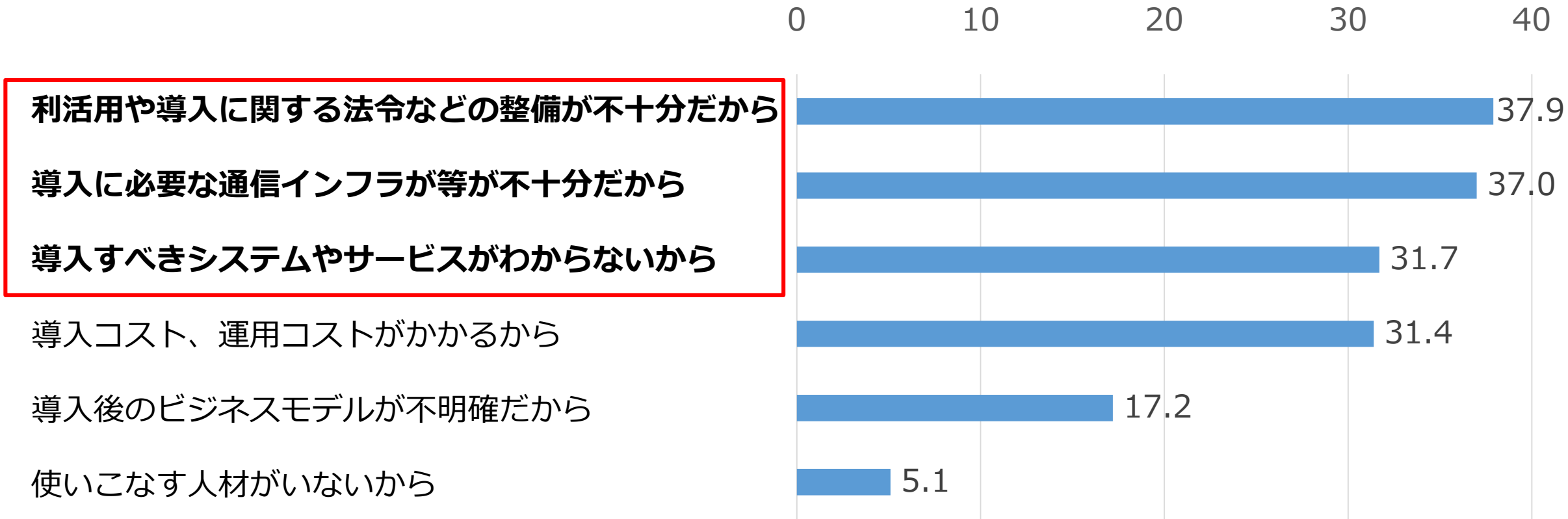
●日本とEUのAI利活用の取組状況

	日本	EU
AI利活用ガイドライン 我々の取り組みスコープ	○ 総務省発行 「AI利活用ガイドライン」	○ Ethics Guidelines for Trustworthy AI
AIを導入する際のチェックリスト	×	○ Trustworthy AI Assessment List
チェックリストを改善するための仕組み	×	○ Technical and non-technical methods to realize Trustworthy AI

解決すべき課題

現段階でAIシステムの導入が進まないのはAIがよくわからないから

●企業がAIを導入しない理由

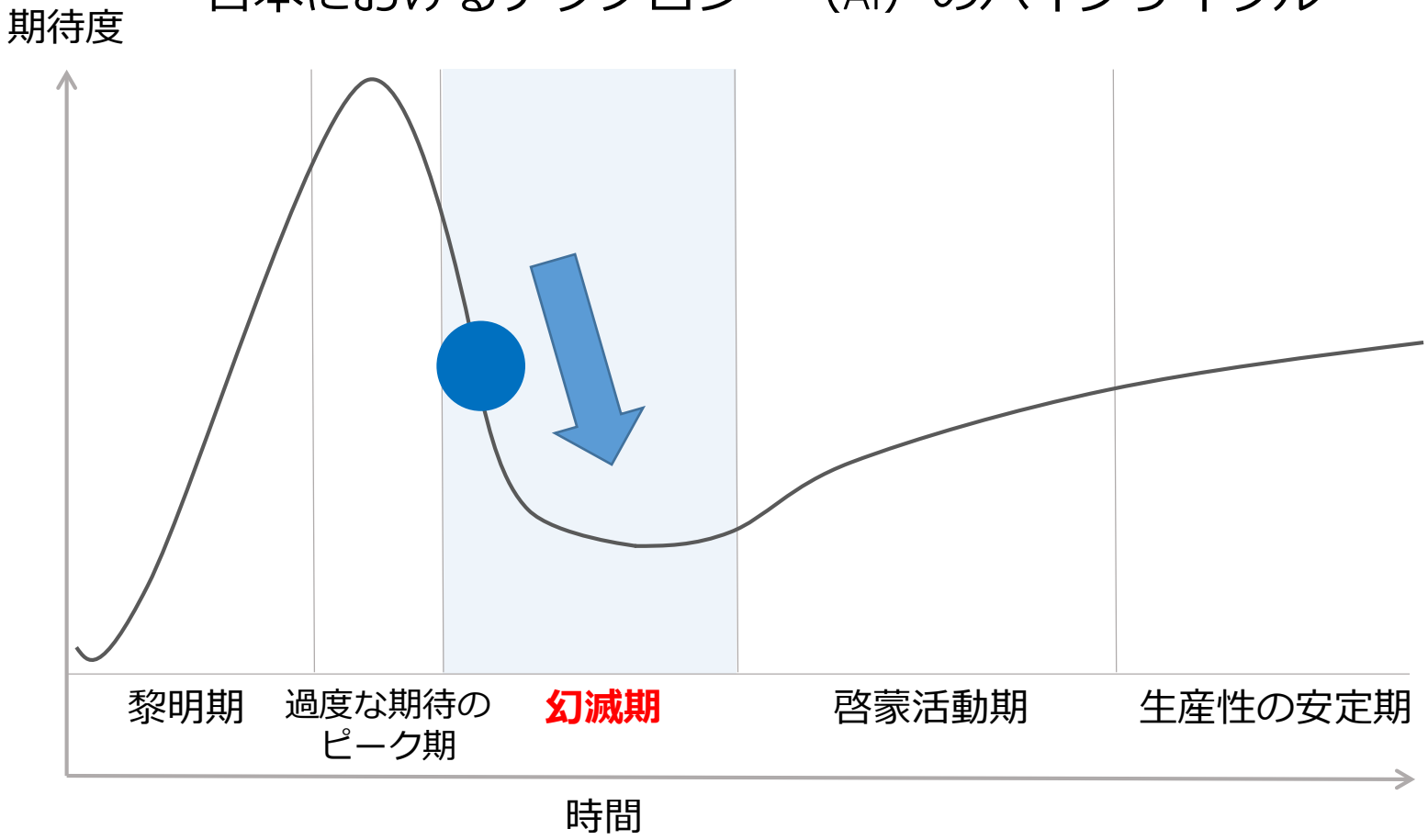


平成30年版 情報通信白書（総務省）より
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd132220.html

解決すべき課題

今後、AIも通常のシステム同様セキュリティが課題になると推測される

日本におけるテクノロジー（AI）のハイプサイクル



- ✓ 主流な採用までにかかる年数が、5～10年と言われている
- ✓ 企業などが概念実証（PoC）などの取り組みを通し、単に期待を抱いていたところからリアリティーに直面するようになった困難が表れている
- ✓ 同時にこれは、採用／導入領域を見極めるタイミングである

ZDNet Japan (参照 2020-02-12)より
https://japan.zdnet.com/article/35144733/

課題へのアプローチ

企業でのAI導入が本格化する前に、課題を解決する方法を検討

●最終成果物の作成までの経緯

★最終成果物完成

調査 （6月~7月）	選定 （8月）	確認 （9月～10月）	決定、作成 （11月～12月）	検証、改善 （1月～2月）
日本だけでなく、OECDなど諸外国においてもガイドラインの整備が進んでいることを確認	「AI・データの利用に関する契約ガイドライン」(経済産業省)と「AI利活用ガイドライン」(総務省)より本分科会の活動内容から後者を選定	「AI利活用ガイドライン」の内容をチームで分担して確認	「AI利活用ガイドライン」の内容をチェックリスト化することで、容易にその記載事項を確認できるようにする方針に決定	メンバーの企業内でAIシステムの利活用を行う部所に検証してもらい、フィードバックを受け改善

AI導入支援ツール

アイアル

AiAL(AI Assessment List)

- ✓ 誰でも簡単にAIを導入可能
- ✓ 導入者の立場や導入のフェーズによって使い分け可能
- ✓AIのビジネス要件とシステム要件が一目瞭然

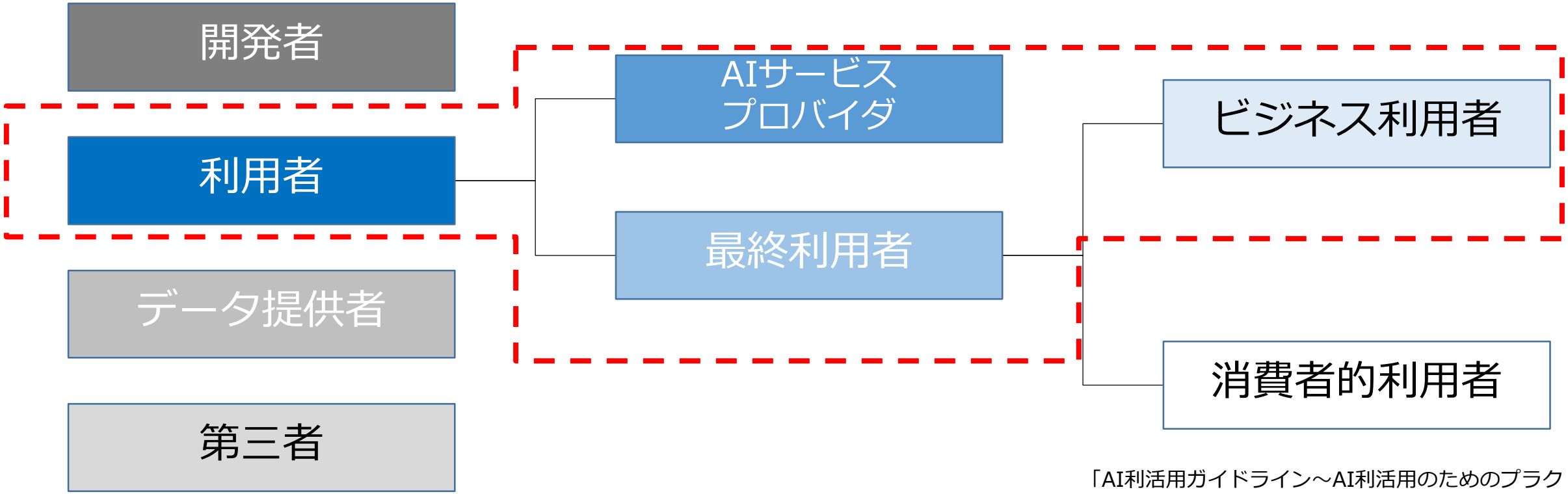
チェックリスト

SEQ	大分類	中分類	小分類（チェック項目）	用語集	解説書
①-ア-1	適正利用の原則	適正な範囲・方法での利用	消費者的利用者等からAIの性質等について問合せがあった場合、適宜提供できる状態ですか？	●	●
①-ア-2	適正利用の原則	適正な範囲・方法での利用	AIソフトのアップデート時期を把握し、定期的に最終利用者と共有をしていますか？	●	
①-ア-3	適正利用の原則	適正な範囲・方法での利用	アップデート時期についてAIサービスプロバイダと定期的に共有していますか？	●	
①-ア-4	適正利用の原則	適正な範囲・方法での利用	AIシステム又はAIサービスを適正な範囲・方法で利用する際の知識・技能を習得するための教育を自組織内の従業員に対し定期的に実施していますか？	●	
①-イ-1	適正利用の原則	人間の判断の介在	人間の判断の介在の要否について基準等を設けていますか？？		●
①-イ-2	適正利用の原則	人間の判断の介在	人間の判断が必要であった場合、各フェーズにおける責任の所在を明確にしていますか？		
①-イ-3	適正利用の原則	人間の判断の介在	人間の判断が必要であった場合、判断すべき項目を明確にしていますか？		
①-イ-4	適正利用の原則	人間の判断の介在	人間の判断が必要であった場合、基準や判断項目について定期的に確認、もしくは見直しを実施していますか？		
①-イ-5	適正利用の原則	人間の判断の介在	人間の判断が必要であった場合、人間による稼働に移行した場合に問題が生じないための事前対策を講じていますか？		●
①-ウ-1	適正利用の原則	関係者間の協力	AIの利活用により生じ得る又は生じた事故、セキュリティ侵害・プライバシー侵害等によりもたらされる又はもたらされた被害の性質・態様等に応じて、予防措置及び事後対応に取り組めるよう関係者間の協力を得られる状況ですか？	●	●
①-エ-1	適正利用の原則	社会的および環境的幸福(持続可能で環境に優しいAI)	AIシステムの開発、展開、使用の環境への配慮、ならびに影響を測定する（データセンターで使用されるエネルギーの種類と消費量、Co2排出量など）仕組みを確立しましたか？	●	
①-エ-2	適正利用の原則	社会的および環境的幸福(持続可能で環境に優しいAI)	AIシステムのライフサイクルが環境に与える影響を減らすための対策を講じましたか？	●	
②-ア-1	適正学習の原則	AIの学習等に用いるデータの質への留意	利用するAIの特性及び用途を踏まえ、AIの学習等に用いるデータの質（正確性や完全性など）を確保していますか？		●

AiALのご紹介

AiAL想定ユーザーは「利用者」

●関係する主体の整理



「AI利活用ガイドライン～AI利活用のためのプラクティカルリファレンス～より作成
https://japan.zdnet.com/article/35144733/

AiALのご紹介

誰でも簡単にAIを導入できるツールを開発

●成果物一覧

①AI Assessment List
（AIを導入するためのチェックリスト）

②AiAL利用説明書

③チェック項目解説書

AiALのご紹介　①AI Assessment List

導入者の立場、導入のフェーズによりリストの絞り込みが可能

●AiALのイメージ

主体		フェーズ				【参考項目】		SEQ	大分類	中分類	小分類（チェック項目）
AIサービスプロバイ	ビジネス利用者	AI構築	システム実	デプロイ	運用/利	AI固有	セキュリティ関連項				
●		●	●	●	●	●	●	①-ア-1	適正利用の原則	適正な範囲・方法での利用	消費者的利用者等からAIの性質等について問合せがあった場合、適宜提供できる状態ですか？
●		●	●	●	●		●	①-ア-2	適正利用の原則	適正な範囲・方法での利用	AIソフトのアップデート時期を把握し、定期的に最終利用者と共有をしていますか？
	●	●	●	●	●		●	①-ア-3	適正利用の原則	適正な範囲・方法での利用	アップデート時期についてAIサービスプロバイダと定期的に共有していますか？
●		●	●	●	●			①-ア-4	適正利用の原則	適正な範囲・方法での利用	AIシステム又はAIサービスを適正な範囲・方法で利用する際の知識・技能を習得するための教育を自組織内の従業員に対し定期的に実施していますか？
●	●	●	●	●	●	●		①-イ-1	適正利用の原則	人間の判断の介在	人間の判断の介在の要否について基準等を設けていますか？？
●	●	●	●	●	●	●		①-イ-2	適正利用の原則	人間の判断の介在	人間の判断が必要であった場合、各フェーズにおける責任の所在を明確にしていますか？
●	●	●	●	●	●	●		①-イ-3	適正利用の原則	人間の判断の介在	人間の判断が必要であった場合、判断すべき項目を明確にしていますか？
●	●	●	●	●	●	●		①-イ-4	適正利用の原則	人間の判断の介在	人間の判断が必要であった場合、基準や判断項目について定期的に確認、もしくは見直しを実施していますか？
●		●	●	●	●	●		①-イ-5	適正利用の原則	人間の判断の介在	人間の判断が必要であった場合、人間による稼働に移行した場合に問題が生じないための事前対策を講じていますか？
●	●			●	●		●	①-ウ-1	適正利用の原則	関係者間の協力	AIの利活用により生じ得る又は生じた事故、セキュリティ侵害・プライバシー侵害等によりもたらされる又はもたらされた被害の性質・態様等に応じて、予防措置及び事後対応に取り組めるよう関係者間の協力を得られる状況ですか？
●		●						①-エ-1	適正利用の原則	社会的および環境的幸福(持続可能で環境に優しいAI)	AIシステムの開発、展開、使用の環境への配慮、ならびに影響を測定する（データセンターで使用されるエネルギーの種類と消費量、Co2排出量など）仕組みを確立しましたか？
●		●						①-エ-2	適正利用の原則	社会的および環境的幸福(持続可能で環境に優しいAI)	AIシステムのライフサイクルが環境に与える影響を減らすための対策を講じましたか？
●	●	●				●	●	②-ア-1	適正学習の原則	AIの学習等に用いるデータの質への	利用するAIの特性及び用途を踏まえ、AIの学習等に用いるデータの質（正確性や完全性など）を確保していますか？
●	●	●				●	●	②-ア-2	適正学習の原則	AIの学習等に用いるデータの質への	AIによってなされる判断について、あらかじめ精度に関する基準を定め、精度が当該基準を下回った場合には、データの質に留意して改めて学習させていますか？
●	●	●		●		●	●	②-イ-1	適正学習の原則	不正確又は不適切なデータの学習等による	AIが不正確又は不適切なデータを学習することにより、AIのセキュリティに脆弱性が生じるリスクが存在することを周知する仕組みを構築していますか？
●	●	●		●			●	②-イ-2	適正学習の原則	不正確又は不適切なデータの学習等による	AIのセキュリティにリスクを認知した際に対応する手順を準備していますか？
●			●	●	●			③-ア-1	連携の原則	相互接続性と相互運用性への留意	AIサービスをネットワーク経由で利用する場合、通信先との相互接続性・相互運用性に留意していますか？
	●		●	●	●			③-ア-2	連携の原則	相互接続性と相互運用性への留意	AIサービスをネットワーク経由で利用する場合、AIサービスプロバイダが通信先との相互接続性・相互運用性に留意していることを確認していますか？

AiALのご紹介　①AI Assessment List

利用者の立場、導入のフェーズによりリストの絞り込みが可能

（例）AIサービスプロバイダーがAiALを利用する場合

Before

主体		フェーズ				【参考項目】		SEQ	大分類	中分類
AIサービスプロバイ	ビジネス利用者	AI構築	システム実	デプロイ	運用/利	AI固有	セキュリティ関連項			
●	●	●	●	●	●		●	⑥-イ-2	プライバシーの原則	パーソナルデータの収集・前処理・提供等におけるプライバシーの尊重
●	●		●				●	⑥-ウ-1	プライバシーの原則	自己等のプライバシー侵害への留意及びパーソナルデータ流出の防
●	●	●	●	●	●	●		⑦-ア-1	尊厳・自律の原則	人間の尊厳と個人の自律の尊重
	●	●	●	●	●	●		⑦-ア-2	尊厳・自律の原則	人間の尊厳と個人の自律の尊重
	●	●	●	●	●	●		⑦-イ-1	尊厳・自律の原則	AIによる意思決定・感情の操作等
	●		●	●	●			⑦-ウ-1	尊厳・自律の原則	AIと人間の脳・身体を連携する際の生命倫理等の議論の参照
	●		●	●	●	●		⑦-ウ-2	尊厳・自律の原則	AIと人間の脳・身体を連携する際の生命倫理等の議論の参照
	●	●	●	●	●			⑦-エ-1	尊厳・自律の原則	AIを利用したプロファイリングを行う場合における不利益への配慮
	●	●	●	●	●	●		⑦-エ-2	尊厳・自律の原則	AIを利用したプロファイリングを行う場合における不利益への配慮
●	●	●	●	●	●	●	●	⑧-ア		
●	●	●	●	●	●	●		⑧-ア	公平性の原則	
●	●	●	●	●	●	●		⑧-ア-3	公平性の原則	AIの学習等に用いられるデータの代表性への留意
●	●	●	●	●	●	●		⑧-ア-4	公平性の原則	AIの学習等に用いられるデータの
●	●	●	●	●	●	●		⑧-ア-5	公平性の原則	AIの学習等に用いられるデータの

チェック不要な項目

After

主体		フェーズ				【参考項目】		SEQ	大分類	中分類
AIサービスプロバイ	ビジネス利用者	AI構築	システム実	デプロイ	運用/利	AI固有	セキュリティ関連項			
●	●	●	●	●	●		●	⑥-イ-2	プライバシーの原則	パーソナルデータの収集・前処理・提供等におけるプライバシーの尊重
●	●		●				●	⑥-ウ-1	プライバシーの原則	自己等のプライバシー侵害への留意及びパーソナルデータ流出の防
●	●	●	●	●	●	●		⑦-ア-1	尊厳・自律の原則	人間の尊厳と個人の自律の尊重
●	●	●	●	●	●	●	●	⑧-ア-1	公平性の原則	AIの学習等に用いられるデータの
●	●	●	●	●	●	●		⑧-ア-2	公平性の原則	AIの学習等に用いられるデータの代表性への留意
●	●	●	●	●	●	●		⑧-ア-3	公平性の原則	AIの学習等に用いられるデータの代表性への留意
●	●	●	●	●	●	●		⑧-ア-4	公平性の原則	AIの学習等に用いられるデータの
●	●	●						⑧-ア-5	公平性の原則	AIの学習等に用いられるデータの
●	●								公平性の原則	学習アルゴリズムによるバイアスへの
●	●								透明性の原則	AIの入出力等のログの記録・保存
●	●								透明性の原則	AIの入出力等のログの記録・保存
●	●	●							透明性の原則	説明可能性の確保
●	●	●							透明性の原則	説明可能性の確保
●	●	●				●		⑨-イ-3	透明性の原則	説明可能性の確保

チェック不要な項目が表示されない

AiALのご紹介　②AiAL利用説明書

チェックリストの使い方で利用者が迷わない工夫を凝らした

利用上の
注意点を明記

AiALの各項目
について
詳しく解説

利用説明書

1.利用にあたっての注意点
- ・AI Assessment List（以下、AIAL）は、総務省より令和元年8月9日に発表された「AI利活用ガイドライン～AI利活用のためのプラティカルリファレンス～」に基づいて作成
- ・当該ガイドラインは様々なシステムを想定して作成されていることから、対象システムによって省略可能な項目もあるため、各項目回答の必要性については利用企業で判断のこと
- ・AIALの想定利用者は、「AIサービスプロバイダ」、「ビジネス利用者」を対象とする（図1参照）
- ・AIALのチェック項目は「利用主体」および「フェーズ」ごとに分かれているため、主体およびフェーズごとにフィルタリングを行ない、選定のこと（詳細は2項および図2を参照）

2.各項目の説明　（必要なチェック項目に抽出するための項目です。具体的な実施イメージは図2参照）

項目		説明
事前作業時の使用項目		
	主体	AIALを利用する企業の立場によって、「AIサービスプロバイダ」、「ビジネス利用者」のいずれかでフィルタリングをかけ、項目を確定（●が担当） ・AIサービスプロバイダ；利用者のうち業としてAIサービスまたはAI付随サービスを他者に提供する者 ・ビジネス利用者；利用者のうち業としてAIサービスまたはAI付随サービスを他者に利用する者
	フェーズ	AI利活用原則を考慮すべきフェーズ（タイミング）ごとにフィルタリングをかけ、対象項目を確定（●が該当） ・AI構築；AIソフトを構築し、トライアルを通じて検証を行うフェーズ ・システム実装；AI構築フェーズで作成されたAIソフトをシステムに導入し、検証を行うフェーズ ・デプロイ；システム実装フェーズで作成された AIを消費者的利用者等（自身を含む）が利用可能な状態にするフェーズ ・運用/利用；消費者的利用者等に対し、デプロイされた AIを運用するフェーズ
	AI固有	●の場合、そのチェック項目がAI固有のチェック項目であることを示す（参考項目のため当該観点でチェックした場合のみ利用）
	セキュリティ関連項目	●の場合、そのチェック項目がセキュリティに関係することを示す（参考項目のため当該観点でチェックした場合のみ利用）
チェック時の使用項目		
	SEQ	シーケンス番号。X-Y-Z X；大分類（＝原則）を示す。例）③ ⇒ 連携の原則 Y；中分類（＝原則内のア～エ）を示す。例）③-ア ⇒ 相互接続性と相互運用性への留意 Z；小分類（チェック項目）を示す。大分類、中分類が同じチェック項目の通し番号
	大分類	AI利活用10原則
	中分類	AI利活用10原則の中項目（ア、イ、ウ、エ）
	小分類（チェック項目）	AIAL利用者が回答する設問
	用語集	●の場合、用語集あり。中分類、小分類（チェック項目）の青字用語について説明がある項目。用語説明は付属の用語集を参照
	解説書	●の場合、解説書あり。解説書への記載内容；小分類（チェック項目）の具体的な事例 等
回答者記入欄		
	回答	「実施済み」、「一部実施済み」、「未実施」から選択
	補足	補足事項があれば記入（任意）

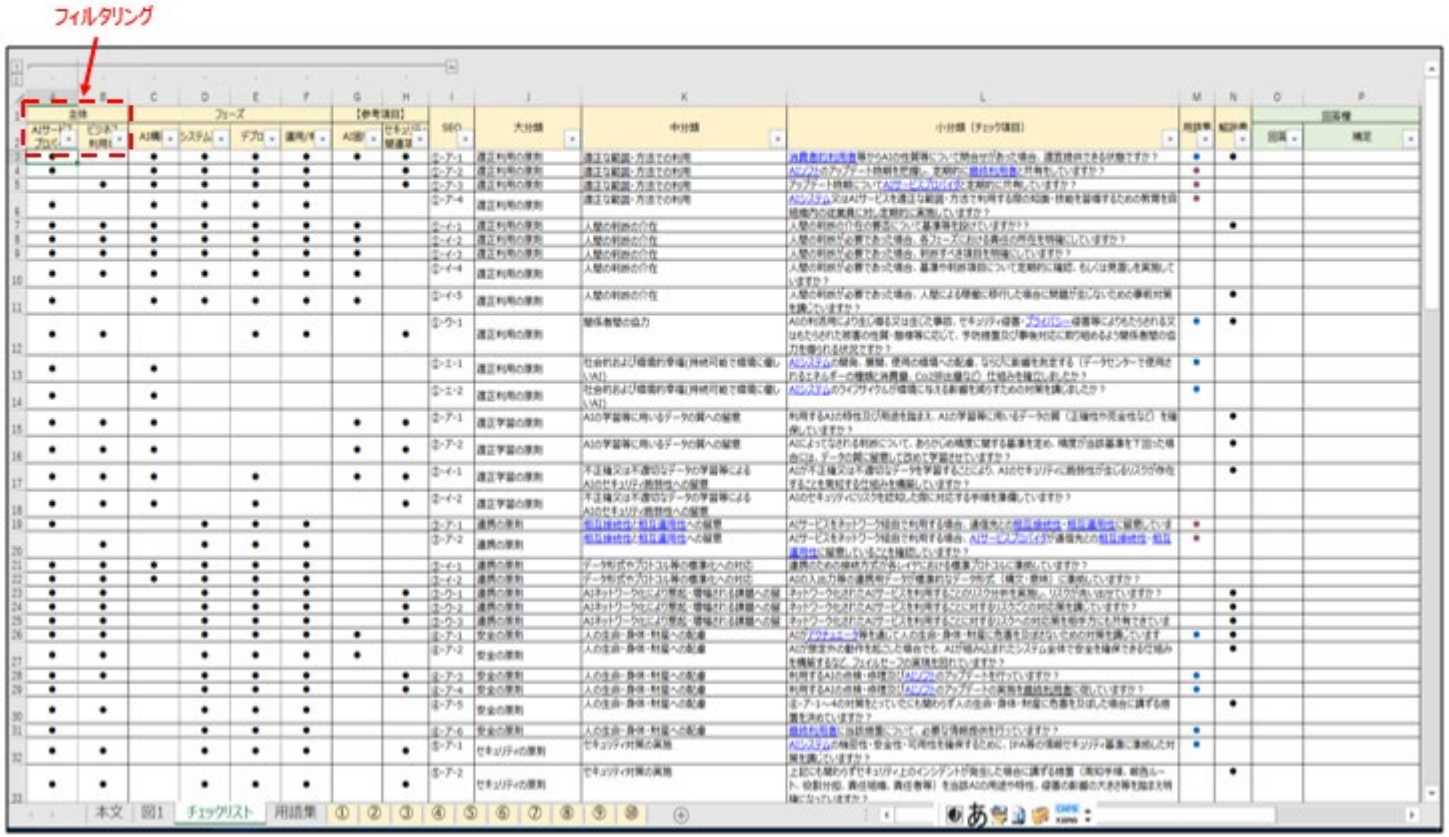
AiALのご紹介　②AiAL利用説明書

チェックリストの使い方で利用者が迷わない工夫を凝らした

利用手順を明記

【図2】AIAL利用イメージ

手順1
立場（「AIサービスプロバイダ」or「ビジネス利用者」）に応じた列を"●"でフィルタリング



AiALのご紹介　③チェック項目解説書

チェック項目の詳細が確認できる

主体		フェーズ				【参考項目】		SEQ	大分類	中分類
AIサービスプロバイダー	ビジネス利用者	AI構築	システム実装	デプロイ	運用/利用	AI固有	セキュリティ関連項目			
•	•		•	•	•		•	⑤-ア-2	セキュリティの原則	セキュリティ対策の実施
•				•	•		•	⑤-イ-1	セキュリティの原則	セキュリティ対策のためのサービス提供等
•				•	•		•	⑤-イ-2	セキュリティの原則	セキュリティ対策のためのサービス提
	•			•	•		•	⑤-イ-3	セキュリティの原則	セキュリティ対策のためのサービス提供等
•	•	•		•		•	•	⑤-ウ-1	セキュリティの原則	AIの学習モデルに対するセキュリティ
	•	•		•			•	⑤-ウ-2	セキュリティの原則	AIの学習モデルに対するセキュリティ
•	•	•		•			•	⑤-ウ-3	セキュリティの原則	AIの学習モデルに対するセキュリティ

チェック項目解説書

SEQ ⑤-ア-2	⑤セキュリティの原則　ア.セキュリティ対策の実施

出典：【総務省】【AIネットワーク社会推進会議】2019報告別紙1 付属資料　AI利活用原則の各論点に対する詳説　19頁
URL： https://www.soumu.go.jp/main_content/000637098.pdf

セキュリティ侵害時の措置の例としては次のようなものが挙げられる
- 初動措置（当該AIを含むシステムの急用度等の文脈に応じ、必要な手順にて実施）
  - 当該システムのロールバック、代替システムの利用等による復旧
  - システムの停止（可能な場合）
  - ネットワークからの遮断　（可能な場合）
  - セキュリティ侵害の内容確認
  - 関係者への報告
- 補償・賠償等（補償・賠償等を円滑に行うための保険の利用）
- 重大な損害が生じた場合等は、第三者機関の設置とその機関による原因調査・分析・提言等

SEQ ⑤-ウ-1	⑤セキュリティの原則　ウ. AIの学習モデルに対するセキュリティ脆弱性への留意

出典：【総務省】【AIネットワーク社会推進会議】2019報告別紙1 付属資料　AI利活用原則の各論点に対する
URL： https://www.soumu.go.jp/main_content/000637098.pdf

リスクの措置の例としては次のようなものが挙げられる
- 学習が不十分であること等の結果、学習モデルが正確に判断することができるデータに、人間には判別できない程度の変動を加え、そのデータをインプットすること等により、作為的に当該学習モデルの判断を誤らせることができるリスク
  （例：Adversarial example攻撃）
- （教師あり学習において）学習において不正確なラベリング等がなされたデータを混在させることで、誤った学習が行われるリスク
- 学習モデルが容易に複製できるリスク
- 学習モデルから学習に用いられたデータをリバースエンジニアリングできるリスク

検証の概要

AiALを実際の現場で使って頂き、フィードバックを得た

検証の目的	-AiALの使用性、有効性を確認する -AiALの課題や改善点を明らかにする
検証方法	実際にAIシステム導入を実施している企業担当者にAiALを渡し、各設問への回答とコメント、フィードバックを受領した
検証対象企業	計2社（製造業1社、保険業1社）
検証期間	2020/01/27～2020/02/07

検証結果

118のチェック項目の内、８４%が有効な項目となった

業種（AI活用業務）	回答対象項目数	回答可能	回答不可	その他	備考
製造業（製造工程）	１１８	**９９**	１９	0	全１１８項目回答があった
保険業（保険請求受付）	７１	**６０**	6	5	AIの業務利用上、７１項目を対象に回答があった

検証後の指摘を踏まえた対応

AiALの改善プロセスも本分科会の中で実施

指摘事項	対応内容	
重複している質問項目があった	改善済	７１項目に整理 （統合：４１件、廃止６項目）
専門用語や事例がないと わかりずらい項目があった	改善済	用語集や解説書（事例集）を 付属資料として添付
適性学習の原則・安全の原則の項目の うち該当しないものがあった	保留	この指摘は、AIの適用範囲の特性によるものであり、AiAL検討時の前提となっていないものであった。 各業種でのAI利活用における課題とした。

今回作成したAiALの課題（1）

- ✓ AiALのチェック項目は、十分有効であるが、AIの適用状況を考慮する工夫が不足している。
- ✓ 各原則の間に、相反する意味（二律背反、アンチノミー）となるものがあり、AIの適用範囲に応じて、最適な範囲を見つける必要がある。二律背反となっている原則の例を次に示す。
  - ➢ ⑧公平性の原則-イ：「公平性の確保」 ↔ 「精度の向上」
  - ➢ ⑨透明性の原則-ア：「セキュリティの確保」 ↔ 「ログの取得」 ↔ 「プライバシーの確保」
- ✓ 検証を行った結果、AIを適用する業界や業種などの特性を考慮しきれていないことが分かった。
- ✓ 今後AIの導入がますます進むであろう分野（医療、自動運転 等）での有用性検証を行なえなかったため、当該分野固有の有用性については実運用を踏まえた評価が必要である。

今回作成したAiALの課題（2）

- ✓ EUにおけるAI利活用に関する自己点検･自己評価の取り組みと比較し、差分があることを確認した。
  - ➢ EUガイドラインだけにある項目について、 AiAL ①適正利用の原則追加した。

●EU「Trustworthy AI Assessment List」とAiAL の対比表

AiAL だけにある項目

EUガイドラインだけにある項目

欧SEQ	EU Trustwrothy Assessment List			総SEQ	AIAL	
①-ア	人間の代理と監督	基本的権利		⑦-ア	尊厳・自律の原則	人間の尊厳と個人の自律の尊重
-	人間の代理と監督	-		⑦-エ	尊厳・自律の原則	AIを利用したプロファイリングを行う場合における不利益への配慮
①-イ	人間の代理と監督	人的機関		⑦-イ	尊厳・自律の原則	AIによる意思決定・感情の操作等への留意
①-ウ	人間の代理と監督	人的監視		⑦-ウ	尊厳・自律の原則	AIと人間の脳・身体を連携する際の生命倫理等の議論の参照
②-ア	技術的な堅牢性と安全性	攻撃とセキュリティに対する回復力		④-ア	安全の原則	人の生命・身体・財産への配慮
②-イ	技術的な堅牢性と安全性	フォールバック計画と一般的な安全性		⑤-ア	セキュリティの原則	セキュリティ対策の実施
②-ウ	技術的な堅牢性と安全性	正確さ		⑤-イ	セキュリティの原則	セキュリティ対策のためのサービス提供等
②-エ	技術的な堅牢性と安全性	信頼性と再現性		⑤-ウ	セキュリティの原則	AIの学習モデルに対するセキュリティ脆弱性への留意
-	技術的な堅牢性と安全性	-		①-ア	適正利用の原則	適正な範囲・方法での利用
-	技術的な堅牢性と安全性	-		①-イ	適正利用の原則	人間の判断の介在
-	技術的な堅牢性と安全性	-		①-ウ	適正利用の原則	関係者間の協力
-	技術的な堅牢性と安全性	-		②-ア	適正学習の原則	AIの学習等に用いるデータの質への留意
-	技術的な堅牢性と安全性	-		②-イ	適正学習の原則	不正確又は不適切なデータの学習等によるAIのセキュリティ脆弱性への留意
-	技術的な堅牢性と安全性	-		③-ア	連携の原則	相互接続性と相互運用性への留意
-	技術的な堅牢性と安全性	-		③-イ	連携の原則	データ形式やプロトコル等の標準化への対応
-	技術的な堅牢性と安全性	-		③-ウ	連携の原則	AIネットワーク化により惹起・増幅される課題への留意
③-ア	プライバシーとデータガバナンス	プライバシーとデータ保護の尊重：		⑥-ア	プライバシーの原則	最終利用者及び第三者のプライバシーの尊重
③-イ	プライバシーとデータガバナンス	データの品質と整合性		⑥-イ	プライバシーの原則	パーソナルデータの収集・前処理・提供等におけるプライバシーの尊重
③-ウ	プライバシーとデータガバナンス	データへのアクセス		⑥-ウ	プライバシーの原則	自己等のプライバシー侵害への留意及びパーソナルデータ流出の防止
④-ア	透明性	トレーサビリティ		⑨-ア	透明性の原則	AIの入出力等のログの記録・保存
④-イ	透明性	説明可能性		⑨-イ	透明性の原則	説明可能性の確保
④-ウ	透明性	連絡		⑨-ウ	透明性の原則	行政機関が利用する際の透明性の確保
⑤-ア	多様性、非差別および公正	不公平なバイアス回避		⑧-ア	公平性の原則	AIの学習等に用いられるデータの代表性への留意
⑤-イ	多様性、非差別および公正	アクセシビリティとユニバーサルデザイン		⑧-イ	公平性の原則	学習アルゴリズムによるバイアスへの留意
⑤-ウ	多様性、非差別および公正	利害関係者の参加		⑧-ウ	公平性の原則	人間の判断の介在（公平性の確保）
⑥-ア	社会的および環境的幸福	持続可能で環境に優しいAI		なし		
⑥-イ	社会的および環境的幸福	社会的影響		なし		
⑥-ウ	社会的および環境的幸福	社会と民主主義		なし		
⑦-ア	説明責任	監査可能性		⑩-ア	アカウンタビリティの原則	アカウンタビリティを果たす努力
⑦-イ	説明責任	悪影響の最小化と報告		⑩-イ	アカウンタビリティの原則	AIに関する利用方針の通知・公表
⑦-ウ	説明責任	トレードオフの文書化		-	-	-
⑦-エ	説明責任	救済能力		-	-	-

今後の展望

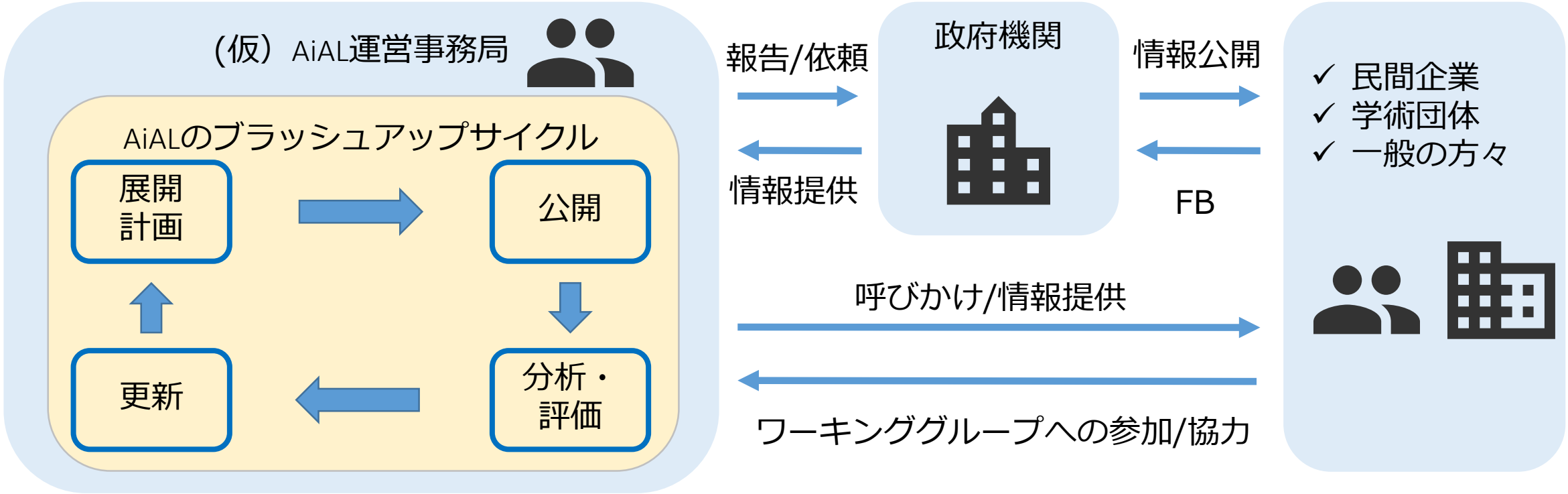
AiALは、AIの社会実装・技術・法制度などの変化に合わせて、
更新し続けることが必要であり、活動を継続して行くことが重要

- ✓AIをビジネス利用して行くためには、「AI利用の指針」に基づいた「自己点検・自己評価」をしていく仕組みは必要であり、さらに、「中立的立場による評価」の仕組みも必要である
- ✓「AI利用の指針」は、総務省が公開している『AI利活用ガイドライン』があり、「自己点検・自己評価」は、AiALがその役割を果たすと考えている
- ✓「中立的立場による評価」は、監査が考えられるが、監査法人などから具体的な表明はされていない状況である。クラウドサービスの評価と同じように、今後、AIの利用が広がり、市場の要求に応じて制度が確立されることを願う
- ✓当研究会の活動を継続し、検証結果を踏まえて、AIネットワーク社会推進会議と連携してAI利用の自己点検・自己評価して行く仕組みの確立を推進していきたい

今後の展望

AiALは、AIの社会実装・技術・法制度などの変化に合わせて、
更新し続けることが必要であり、活動を継続して行くことが重要

●AiAL改善のイメージ図



ご清聴ありがとうございました

Appendix

AIに関するガイドライン一覧

ガイドライン名	団体	発行日	URL
Tenets	Partnership on AI	2016/9/28	https://www.partnershiponai.org/tenets/
Asilomar AI Principles	Future of Life Institute (FLI)	2017/2	https://futureoflife.org/ai-principles/
人工知能学会倫理指針 Ethical Guideline	人工知能学会(JSAI)(Japan)	2017/2/28	http://ai-elsi.org/wp-content/uploads/2017/05/JSAI-Ethical-Guidelines
国際的な議論のためのAI開発ガイドライン	総務省（Japan）	2017/7/28	https://www.soumu.go.jp/main_content/000490299.pdf
Ethically Aligned Design	IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems	2019/3/25	https://ethicsinaction.ieee.org/
「人間中心のＡＩ社会原則」 Social Principles of Human-centric AI	統合イノベーション戦略推進会議（人間中心のAI 社会原則会議）(Japan)	2019/3/29	https://www.cas.go.jp/jp/seisaku/jinkouchinou/
Ethics Guideline for Trustworthy AI	European Commission (High Level Expert Group on AI(HLEG))	2019/4/8	https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai
Recommendation of the Council on Artificial Intelligence	OECD	2019/5/22	https://legalinstruments.oecd.org/en/instruments/OE
AI利活用ガイドライン／AI利活用原則	総務省（Japan）	2019/8	https://www.soumu.go.jp/main_content/000637097.pdf

参考文献（ガイドラインを除く）

参考文献	団体	発行日	URL
デジタル化の進展に対する意識調査	JUAS	2017/5/18	http://www.juas.or.jp/cms/media/2017/03/digitalization2017.pdf
AI・データの利用に関する契約ガイドライン	経済産業省	2018/6	https://www.meti.go.jp/press/2018/06/20180615001/20180615001-1.pdf
平成30年版　情報通信白書	総務省	2018/7	https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/pdf/index.html
機械学習システムのセキュリティに関する研究動向と課題	宇根正志氏	2018/8/15	https://www.imes.boj.or.jp/research/papers/japanese/18-J-16.pdf
AI活用戦略	経団連	2019/2/19	https://www.keidanren.or.jp/policy/2019/013_honbun.pdf
日本企業のAI・IoTの導入状況	日本経済研究センター 田原健吾氏	2019/3/20	https://www.soumu.go.jp/main_content/000610197.pdf
報告書2019	総務省	2019/8/9	https://www.soumu.go.jp/main_content/000637096.pdf
ＡＩ利活用原則の各論点に対する詳説	総務省	2019/8/9	https://www.soumu.go.jp/main_content/000637098.pdf
報告書2019概要	総務省	2019/8/9	https://www.soumu.go.jp/main_content/000637103.pdf
AIガイドライン比較表	総務省	2019/8/9	https://www.soumu.go.jp/main_content/000637099.pdf
ZDNet Japan(2019年版ハイプサイクル)	ZDNet Japan	2020/2/12	https://japan.zdnet.com/article/35144733/