2023年度活動報告
セキュリティWG

三宅　優（KDDI総合研究所）

セキュリティWG

2024年3月25日

セキュリティWGの活動方針

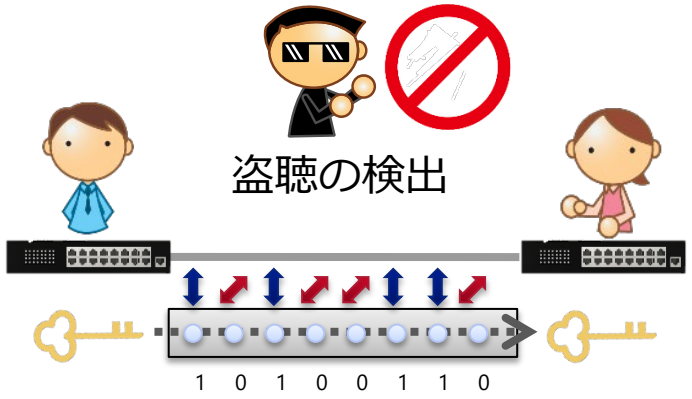
- 活動方針
  - B5G/6G時代に向けて注目されているセキュリティ分野の動向調査と国際的な展開への活動協力を行う
- 対象分野
  - 暗号技術
    - 量子コンピュータの進展により既存暗号が危殆化することが指摘されており、量子コンピュータによる解読に耐えられる暗号技術が求められている
  - AIセキュリティ
    - AI技術の利用拡大や生成AIの機能向上に伴い、AI利用におけるセキュリティ・プライバシー上の問題が指摘されており、セキュリティに関する議論が活発になっている
  - サプライチェーンセキュリティ
    - システムやソフトウェア作成において複数社の製品がコンポーネントとして組み込まれるため、各コンポーネントの安全を保障するための仕組みが求められている

暗号技術

B5G/6Gに向けた暗号技術検討の要約

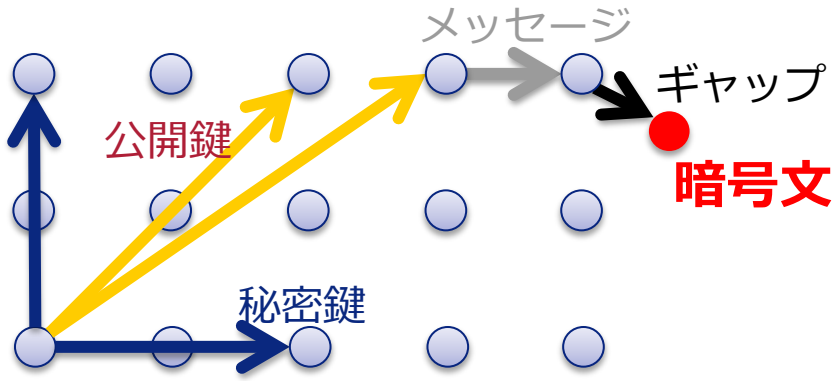
要件	対応方法	2023年度活動
量子コンピュータ出現への対応	量子暗号通信（QKD：量子鍵配送）技術の展開	ITU-Tへの展開
	耐量子計算機暗号アルゴリズム（PQC）の開発と応用	
超高速、大容量、低遅延通信への対応	高速暗号アルゴリズムの開発	3GPPへの展開

QKD: Quantum Key Distribution



- 量子力学の性質を利用し、攻撃者による盗聴や改ざんを検知できる鍵共有方式。

Post-Quantum Cryptography



- 量子コンピュータでは解けない数学的問題に基づく公開暗号システム

QKDに関わるITU-Tへの貢献（寄書入力）

2023年度は、下記の勧告策案作成に貢献（寄書8件）。ITU-TにおけるQKDセキュリティの議論をリード。

勧告案タイトル、概要	寄書提出機関
X.sec_QKD_profr: Framework of quantum key distribution (QKD) protocols in QKD network 2023年度開始案件。本勧告は、QKDネットワークの量子レイヤにおけるQKDリンクで接続されたQKDモジュール間で情報理論的安全性に基づいて共通鍵暗号に利用する共通鍵を共有するための量子鍵配送ロトコルの枠組みを規定する。	**NICT、NEC、東芝**
X.sec_QKDN_tn: Security requirements and designs for the protection of quantum key distribution node X.1713として勧告発行承認済み（2024/03）。鍵配布距離を拡大することを目的にQKDネットワークに導入されるQKDノードの信頼性を確保するために、QKDノードの安全な実装と運用のためのガイダンスを提供する。	**NICT、NEC、東芝**
X.sec_QKDN_CM: Security requirements and measures for quantum key distribution networks - control and management ITU-T Y.3804で定義されたQKDNの制御と管理のための機能アーキテクチャに基づき、QKDNにおける制御と管理のためのセキュリティ要件と対策を規定する。	**NICT、NEC、東芝**
X.sec_QKDN_AA: Authentication and authorization in QKDN. QKDネットワーク内で利用される認証と認可について規定されている。QKDノード間で利用するIDとその管理、PKIによる公開鍵認証の利用等が説明されている。	**NICT、NEC、東芝**
X.1715: Security requirements and measures for integration of quantum key distribution network and secure storage network 2022年に発効した勧告の修正提案。2022/09会合で提案し、2023/03会合で承認済み。主に、説明が分かりにくい部分を補足し、編集上のミスを修正している。	**NICT、NEC、東芝**

PQC、暗号応用に関わるITU-Tへの貢献（寄書入力）

2023年度は、日本から下記のワークアイテムに関して寄書を提出し、文書作成に貢献。

略称	種類	タイトル	提案国
TR.ba-iot	技術 レポート	Broadcast authentication scheme for IoT system	日本
状況：　2023年9月に発行合意 要約：　IoTシステムにおいて多数のデバイスを一括して認証するブロードキャスト認証（BA）方式を規定するために、対象となるBAシステムの概念モデルを提供し、そこで要求されるセキュリティ特性と要件を明らかにしている。また、セキュリティ要件を実現する方式として、MAC（Message Authentication Code）ベースのBA認証方式とDS（Digital Signature）ベースのBA認証方式を規定し、それぞれの利便性と利用方法を示している。			
TR.au-pqc	技術 レポート	Guidance on use of advanced cryptography based on PQC	日本
状況：　2024年3月に作業開始を合意 要約：　最新の暗号アルゴリズムを利用するためのガイドラインを提供する。代表的な最新の暗号を抽出し、その特徴やPQCベースの構成に関する議論・提案の種類を紹介する。その上で、5G/B5Gなどの環境での活用が期待されるPQCベースの高度暗号の構築・実装方法についてガイダンスを示す。本資料は、5G/B5Gなど今後の新たな環境におけるビジネスやアプリケーションの設計・運用において、PQCに基づく高度暗号の実装・実現を支援するものである。			

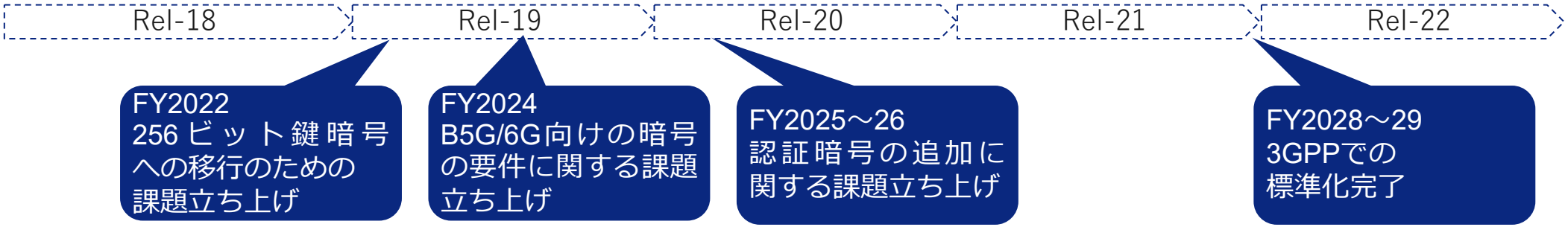
- **特定のサービスやアプリケーションにおける暗号化や認証を効率化する暗号アルゴリズムの提案と適用（PQCの最適化を含む）**
- **暗号アルゴリズムの危殆化に対応したシステム、サービスの更新**

開催日： 2023年11月9日（木） URL: https://www.ttc.or.jp/seminar/rep/rep20231109

講演内容	講演者
開会挨拶	TTC Network Vision専門委員会 委員長 後藤 良則 氏（NTTアドバンステクノロジ株式会社）
ITU－T SG13におけるネットワーク技術の最新動向	TTC Network Vision専門委員会 SWG1104リーダ 谷川 和法 氏（国立研究開発法人情報通信研究機構）
Q-STARの取り組みと量子インスパイアードコンピューティングの産業活用状況	Q-STAR 最適化・組合せ問題に関する部会 部会長 岩井 大介 氏（富士通株式会社）
Beyond 5G/6G時代に向けたセキュリティ検討について	TTC セキュリティ専門委員会 委員長 三宅 優氏（KDDI株式会社）
量子暗号の最新動向と量子技術プラットフォーム構想について	量子ICTフォーラム・技術担当理事 佐々木 雅英 氏（国立研究開発法人情報通信研究機構）
パネルディスカッション 『ネットワーク×コンピューティング×セキュリティがもたらす新たなサービス基盤について』	モデレーター ：佐々木 雅英氏 パネリスト •谷川 和法 氏 •岩井 大介 氏 •三宅 優 氏 •花井 克之 氏（Q-STAR 量子暗号・量子通信部会 部会長）
閉会挨拶1	一般社団法人情報通信技術委員会 代表理事専務理事 岩田 秀行
閉会挨拶2	量子ICTフォーラム 代表理事 富田 章久 氏

3GPPにおける暗号関連検討の調査（国際展開に向けた取り組み）

- 256ビット鍵に対応した暗号方式への移行（PQC対応）
  - 準備（2018年）
    - TR 33.841: Study on the support of 256-bit algorithms for 5G
    - 鍵長を長くした暗号アルゴリズムの検討が推奨されており、ETSI SAGEでSNOW-5G、ZUC-256、AES-256の評価を実施
  - 実用化に向けた課題の整理と対応策を検討（2022年）
    - 128/256混在のリスク、256統一に向けた課題、影響を受けるエンティティの整理、等
  - 256ビット暗号アルゴリズムの検討（2023年）
    - 暗号アルゴリズムAES, SNOW, ZUCの256ビット版仕様の作成
  - 256ビット暗号アルゴリズム以降に向けた課題の検討（2023年）
    - 端末-ネットワーク間の鍵長のネゴシエーション
    - MAC長の延長とMAC長のネゴシエーション
  - その他
    - 認証暗号（AEAD: Authenticated encryption with associated data）利用の検討を開始
      - 認証暗号：データの秘匿性、完全性、および認証性を同時に提供する暗号利用モード
  - ロードマップ（案）



AIセキュリティ

OECD Global ForumでのAIセキュリティに関する企業としての取り組み紹介

イベント名： 4th OECD Global Forum on Digital Security for Prosperity
日時： 2023年3月13～14日

Theme 2: How can a 'secure by design' approach be embedded within Artificial Intelligence policies?

14:30 – 15:45: Security risks in Artificial Intelligence

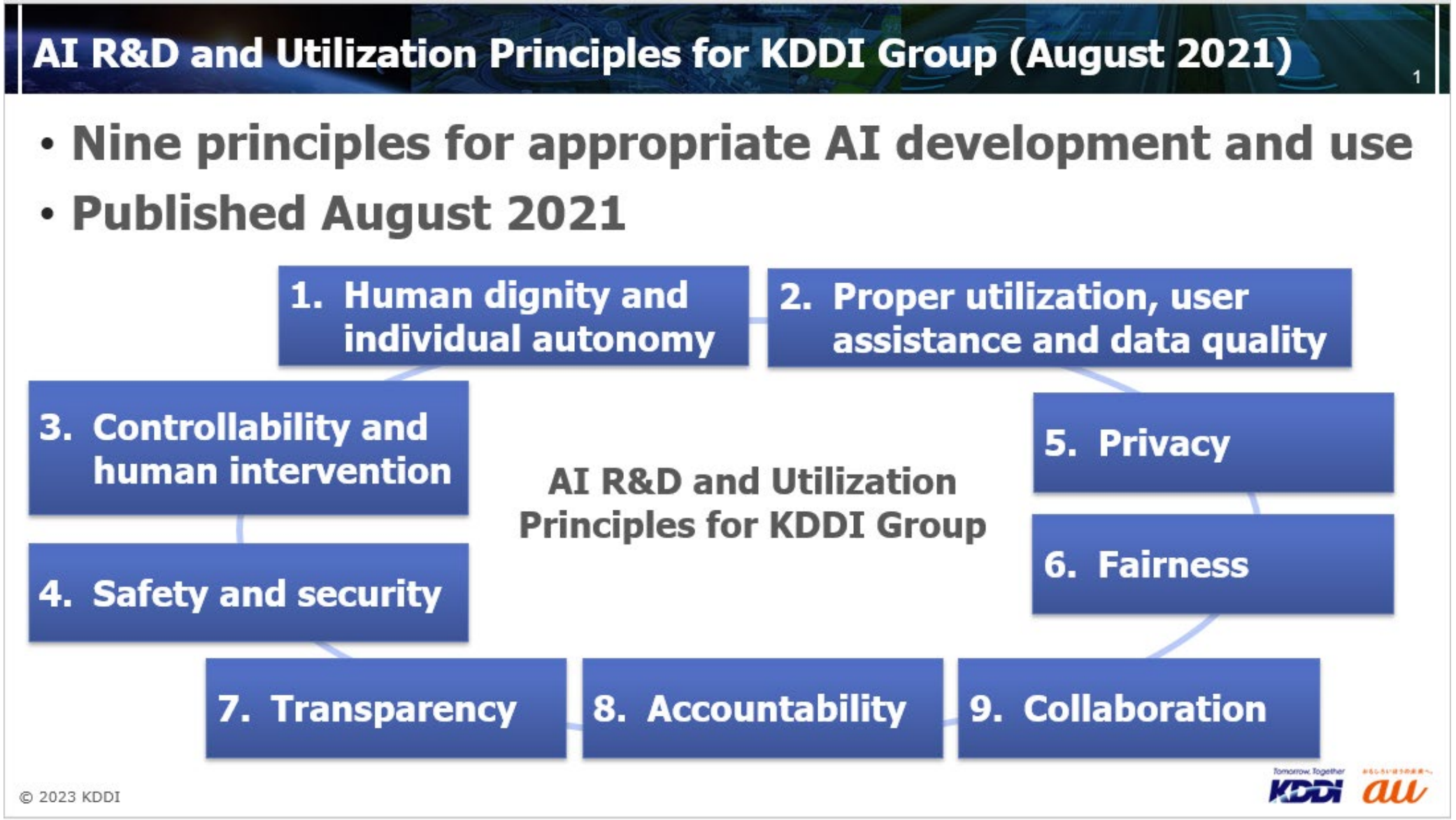
This session will share insights from across the public and private sectors to highlight the challenges of security within Artificial Intelligence, with risks including lack of transparency and explainability, bias and discrimination, vulnerability to attacks, lack of human oversight, and privacy concerns. These risks can lead to flawed decisions negatively impacting individuals or groups. In addition, the safety of AI is interlinked with other digital security matters. For example, security risks in AI can affect product safety if connected products such as driverless cars or AI-powered home appliances are not sufficiently secure.

Moderator: **Sebastian Hallensleben,** Chair, CEN CENELEC JTC21
Proposed speakers:

- **Dan Fagella,** Head of Research, Emerj
- **Poppy Gustafsson,** Chief Executive Officer, Darktrace
- **Victoria Krakovna,** Research Scientist, Deepmind
- **Yutaka Miyake,** Director, Information System and Security Department General Affairs Division KDDI Research, Inc
- **Clara Neppel,** Senior Director, IEEE
- **Taylor Reynolds,** Technology Policy Director, MIT Internet Policy Research Initiative (IPRI)

OECD Global ForumでのAIセキュリティに関する企業としての取り組み紹介

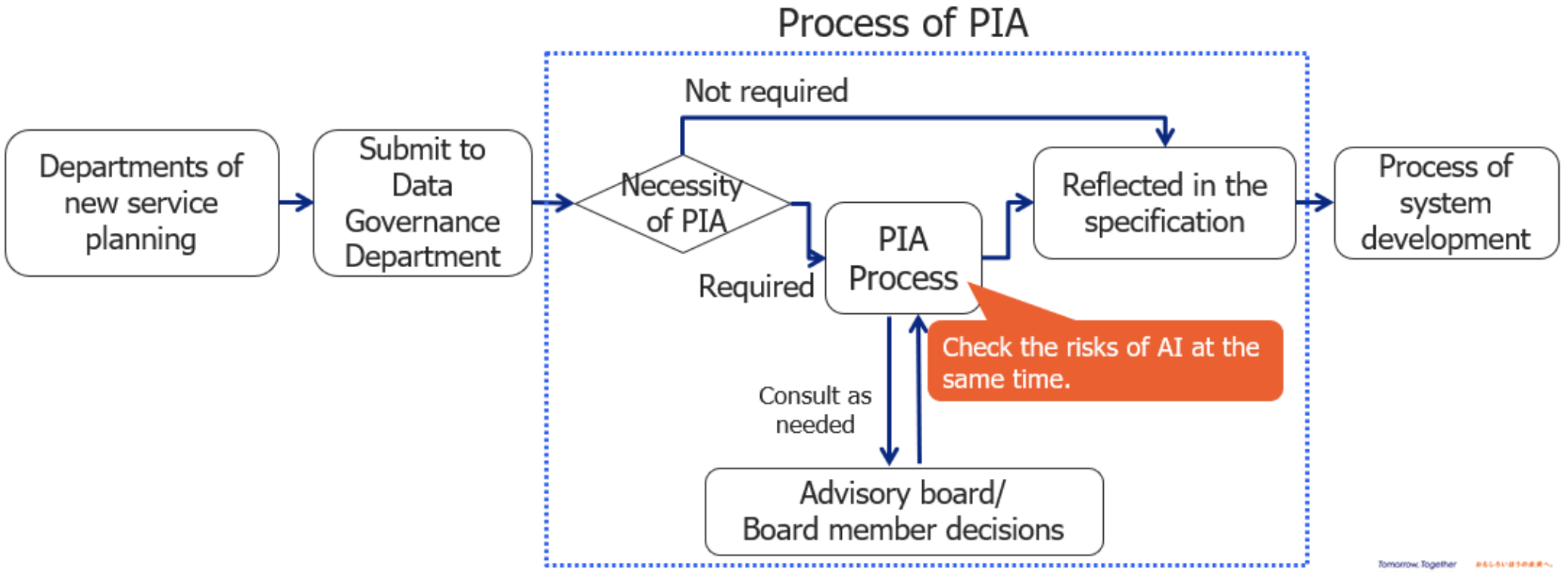
KDDIグループのAI利用における基本原則



AI技術利用におけるアセスメント実施

3) Internal operational arrangements

- **Risk assessment and countermeasures are carried out prior to the start of services through PIA (Privacy Impact Assessment)**
- **The same flow applies to AI related services.**




ITUEvents
Workshop on generative AI: Challenges and opportunities for security and privacy
19 February 2024
Geneva, Switzerland
itu.int/go/SP4GAI
ITU

ITUワークショップのセッション構成と発表者

Session	タイトル、内容
Session 1	Understanding the benefits and concerns to security and privacy
	生成AIは、セキュリティ機能を強化する可能性を秘めているが、逆に、ハッカーの参入障壁を下げることにより、攻撃者を強化することにもなる。本セッションでは、生成AIのこの二重の側面を検証し、生成AIを含むAIにまつわるセキュリティとプライバシーへの懸念、リスク、脅威に焦点を当てる。
Session 2	Security and privacy controls (Part 1)
	生成AIにまつわるセキュリティとプライバシーの懸念を軽減するためのコントロールを特定することに焦点を当て、セキュリティとプライバシーを維持するために効果的なコントロールを調整する方法についての知見を共有する。
Session 3	Security and privacy controls (Part 2)
	（Session 2と同じ）
Session 4	Panel discussion - Future directions
	将来の標準化の可能性を探り、ITU-T Study Group 17に対し、この分野での今後の取り組みに関する提言を行う。

発表者：　米国　6名、中国　4名、韓国　3名、英国　2名、南アフリカ　2名、オランダ　2名、フランス　1名、エジプト　1名、カナダ　1名

ITU-T SG17でのAIセキュリティに関する活動状況

- Workshopを踏まえた検討課題の整理（ITU-T SG17での検討対象候補）
  - 生成AIのセキュリティ、PII保護、信頼性
  - 生成AIの好ましくない結果を軽減するためのコントロール
  - 生成AIの倫理に関する共通用語
  - 生成AIのためのデータガバナンス
- ITU-T SG17で議論中のワークアイテム

略称	種類	タイトル	提案国
X.sr-ai	勧告	Security requirements for AI systems	韓国
X.sr-da-gai	勧告	Security threats and requirements for data annotation service of generative artificial intelligence	中国
X.sgGenAI	勧告	Security Guidelines for Generative Artificial Intelligence Application Service	中国
X.srm-fml	勧告	Security requirements and measures of federated machine learning	中国
TR.se-ai	技術レポート	Security Evaluation on Artificial Intelligence Technology in ICT	中国

サプライチェーンセキュリティ

ITUEvents

Workshop on

Zero trust and software supply chain security

28 August 2023
Goyang, Republic of Korea

itu.int/go/ZeroTrust_SSCS

Ministry of Science and ICT

ITUワークショップのセッション構成と発表者

Session	タイトル、内容
Session 1	Need, security issues, threats and controls for zero trust
	ゼロ・トラストに関する様々な側面や見解に注目し、ゼロ・トラストの必要性を特定し、セキュリティ上の問題、脅威、コントロールについて議論する。
Session 2	Need, security issues, threats and controls for software supply chain security
	ソフトウェア・サプライチェーン・セキュリティの必要性を特定し、セキュリティ問題、脅威、管理策について議論することに焦点を当てる。
Session 3	Implementation of zero trust and software supply chain security
	ゼロ・トラストとソフトウェア・サプライチェーン・セキュリティの実施、国や地域の戦略・政策の策定に焦点を当てる。
Session 4	Panel discussion – Future directions for Study Group 17
	SG17の今後の活動について提言を行うことに焦点を当てる。

発表者：　米国　8名、韓国　8名、英国　3名、日本　2名、中国　2名、フランス　1名、カナダ　1名、
ロシア　1名、ドイツ　1名

ITU-T SG17でのサプライチェーンセキュリティに関する活動状況

- Workshopを踏まえた検討課題の整理（ITU-T SG17での検討対象候補）
  - ソフトウェアサプライチェーンに関するサイバーセキュリティの脅威とリスク
  - ソフトウェアサプライチェーンセキュリティの実装を可能にするガイドラインと推奨事項
  - ソフトウェアサプライチェーンセキュリティの基盤技術の研究
    - SBOMのためのX.509属性証明書の新しいユースケース
    - 商用ソフトウェアや自社開発ソフトウェアなどに必要なSBOM構成単位のガイドライン
    - サプライチェーンを横断して保証証明を取得・伝達するための自動化ガイドライン
    - ソフトウェアの開発者検証の最低基準に関するガイドライン
- ITU-T SG17で議論中のワークアイテム

略称	種類	タイトル	提案国
TR.x509ac4sc	技術レポート	A use case of ITU-T X.509 attribute certificates for supply chains（2023/09発行承認、発行済み）	日本
X.st-ssc	勧告	Security threats of software supply chain	韓国
X.ssc-sa	勧告	Guidelines for Software Supply Chain Security Audit	中国
X.rm-sup	勧告	Risk management on the security of software supply-chain for telecommunication organizations	中国
X.sc-sscti	勧告	Guidelines on Security Capabilities for Software Supply Chain in the Telecommunications Industry	中国

まとめ

まとめ

- B5G/6G時代に向けて注目されている以下の3つの分野について、調査、展開活動を実施
  - 暗号技術
  - AIセキュリティ
  - サプライチェーンセキュリティ
- 暗号技術
  - 量子コンピュータの性能向上に伴うセキュリティ対策強化が必要
  - システムの大規模化、複雑化や通信速度の高速化・大容量化に伴うセキュリティ処理の軽量化・効率化が求められている
- AIセキュリティ
  - プライバシーやセキュリティの懸念から、各国政府や標準化団体が各種のガイドライン文書等を作成
  - AI活用の技術が進む中で、セキュリティ面では多くの課題あり
- サプライチェーンセキュリティ
  - サプライチェーンセキュリティのための共通基準（標準化）が必要とされている
  - サービスを提供する会社が出てきており、今後の普及が期待されている


B5GPC