FORXAIパートナー-アメニディ技術紹介：属性ベース暗号

2023-12-15 09:00　Masaaki Suzuki
IoT, Tech

株式会社アメニディの鈴木です。

IT技術が普及している現在、それを安全に利用するために暗号技術は身近な多くのところで活用されています。例えばスマートフォンでのWi-Fi通信や、様々なWebのサービス、クレジットカード等。そして、その暗号技術は日々進化しています。

本記事では、FORXAIパートナーとしてコミュニティに参画させて頂いているアメニディの保持技術である次世代暗号技術の属性ベース暗号について紹介すると共に、その技術をコニカミノルタ様の画像IoT技術や他FORXAIパートナー様の技術と組み合わせて描ける未来について述べていきたいと思います。

目次 [非表示]

現代暗号技術の紹介

まず、現代の暗号技術として広く利用されている共通鍵暗号と公開鍵暗号を紹介します。

共通鍵暗号とは

共通鍵暗号とは暗号化と復号化を同じ鍵を使用して暗号化する暗号方式であり、秘密鍵暗号や対象鍵暗号とも呼ばれています。共通鍵暗号にはDES、AES、RC4といった様々なアルゴリズムがあります。

利点としては、暗号化と復号化の計算がシンプルであり、処理速度が速い点があげられます。
また、活用例としては無線LANに多く活用されています。無線LANの通信は傍受されるリスクがあるため暗号化が必須となっており、現在無線LANの暗号化規格の主流となっているWPA2ではAESというアルゴリズムが活用されています。

公開鍵暗号とは

共通鍵暗号では暗号化する人と復号化する人が同一の鍵を利用するため、鍵の受け渡しが必要となり、その受け渡し時に鍵が漏洩するリスクがありました。そこで、暗号化する鍵と復号化する鍵を分けようと考えられた方式が公開鍵暗号となります。誰にも教えない秘密鍵と皆に教える公開鍵を作り、その2つの鍵を利用して暗号化と復号化をします。公開鍵暗号にはRSAや楕円曲線暗号等のアルゴリズムがあり、広く利用されているRSAは素因数分解問題の困難性に基づくアルゴリズムとなっています。

利点としては、共通鍵暗号と比較すると公開鍵は公開しているため管理が楽になることや、秘密鍵を他者に共有する必要がないため、その漏洩リスクが下げられる点があげられます。

また、活用例としては、暗号通信や電子署名に広く活用されています。暗号通信はWeb上で個人情報やパスワードを通信にて送る際によく使われており、これは公開鍵によりデータを暗号化し、送りたい相手に送った後に秘密鍵により復号化することで、秘密鍵を持つ人しかデータを閲覧出来なくしています。反対に秘密鍵でデータを暗号化して公開鍵で復号化することで電子署名としても使われており、そのデータを作成した人が秘密鍵を持つ本人であることや、データが改ざんされていないことなどを証明することに活用されています。

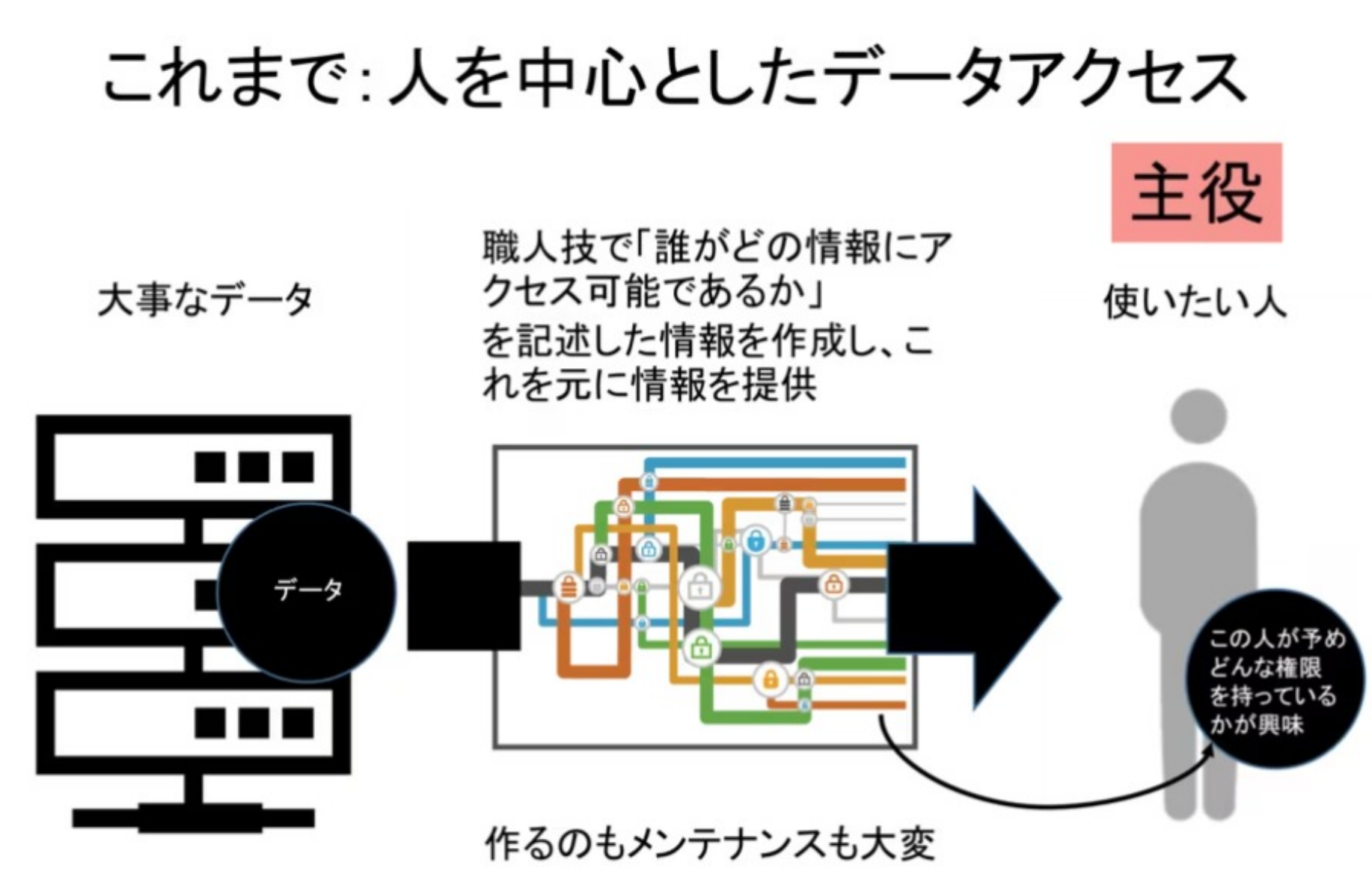
現代暗号技術の課題

広く普及して利用されている現代暗号技術にも、鍵の管理という課題があります。

共通鍵暗号はその仕組み上、鍵を自身と他者で共有する必要があり、その上でその鍵を秘密にしておく必要があり、厳重な管理が必要になります。

また、公開鍵暗号においても、公開鍵の管理は楽ですが、秘密鍵は変わらず適切な管理が必要となります。さらに公開鍵暗号を暗号通信で活用する場合、秘密鍵を復号化に利用するため、暗号データを復号化する必要のあるデータ受信者毎に、秘密鍵とそれに対応した公開鍵のペアが必要となります。そのため多くの人が暗号通信をしたい場合、多数の鍵のペアが必要となってしまい、その管理が非常に困難となります。

これはデータへアクセスする相手に応じて逐次データを暗号化し、誰がどの情報にアクセス可能かを人毎に制御する、人を中心としたデータアクセスともいえます。

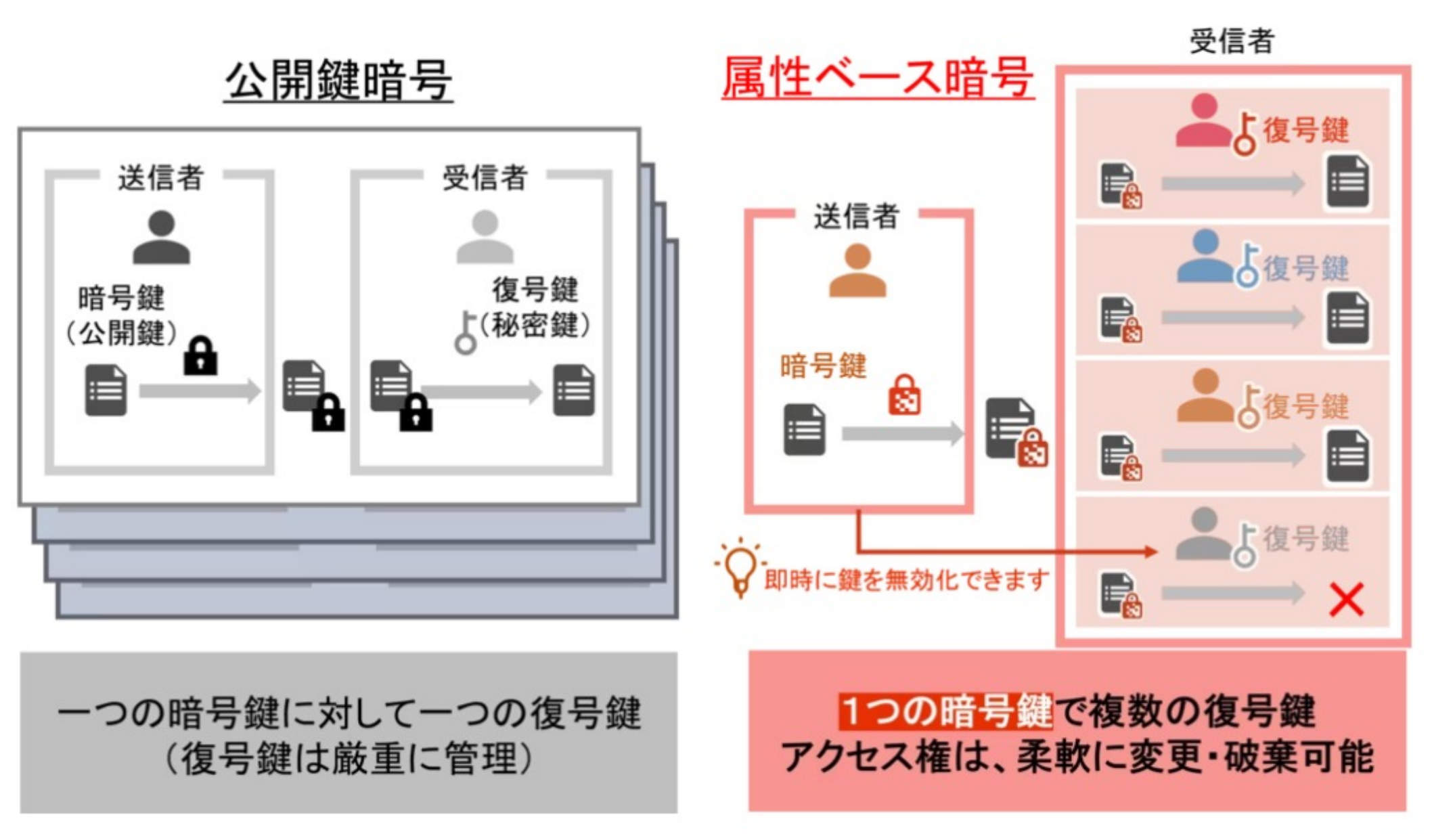


課題に対応した次世代暗号技術：属性ベース暗号

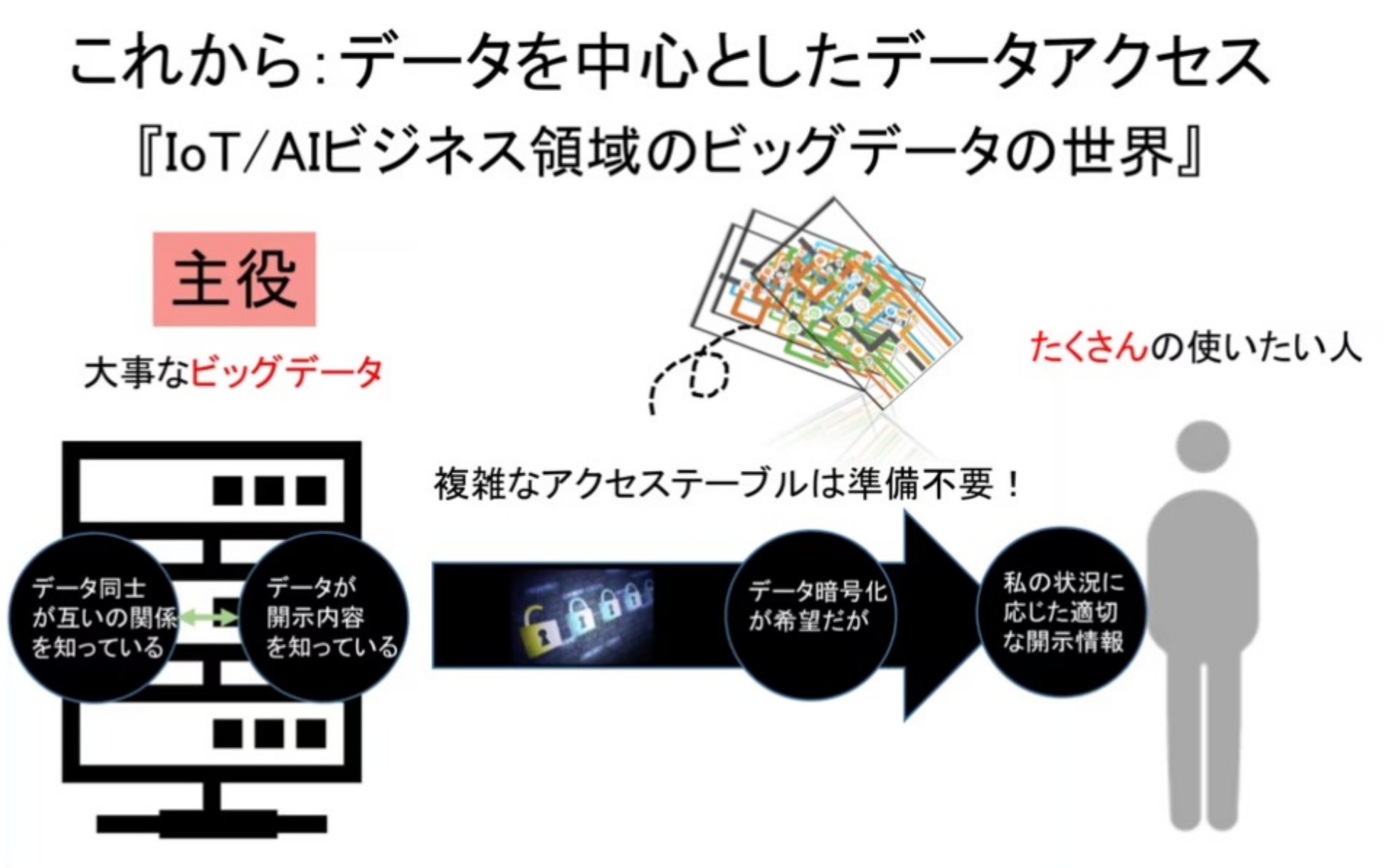
鍵の管理という課題に対応した次世代暗号技術として、属性ベース暗号という暗号技術が開発されています。

属性ベース暗号は、データの解読に必要な条件を属性として定義して暗号化し、その条件を満たす受信者だけがデータを解読できるようにすることで、指定した属性に基づいてアクセス制御する暗号方式となります。

そのため、属性を定義した暗号化のための公開鍵は1つ生成すれば良く、さらにデータ受信者毎の復号のための秘密鍵はその受信者の属性に応じて都度、自動で生成すれば良くなります。そのため、鍵管理が非常に容易となります。



これはデータ自体に、アクセスして良い人の属性を定義する暗号化となるため、データを中心としたデータアクセスともいえます。



このように次世代暗号技術である属性ベース暗号は鍵管理の課題をクリアにすることが出来るため、DXで要求される「セキュリティと利便性」の両立が可能となり、広く活用されることが出来る技術であると考えられます。

次世代暗号技術が普及した未来

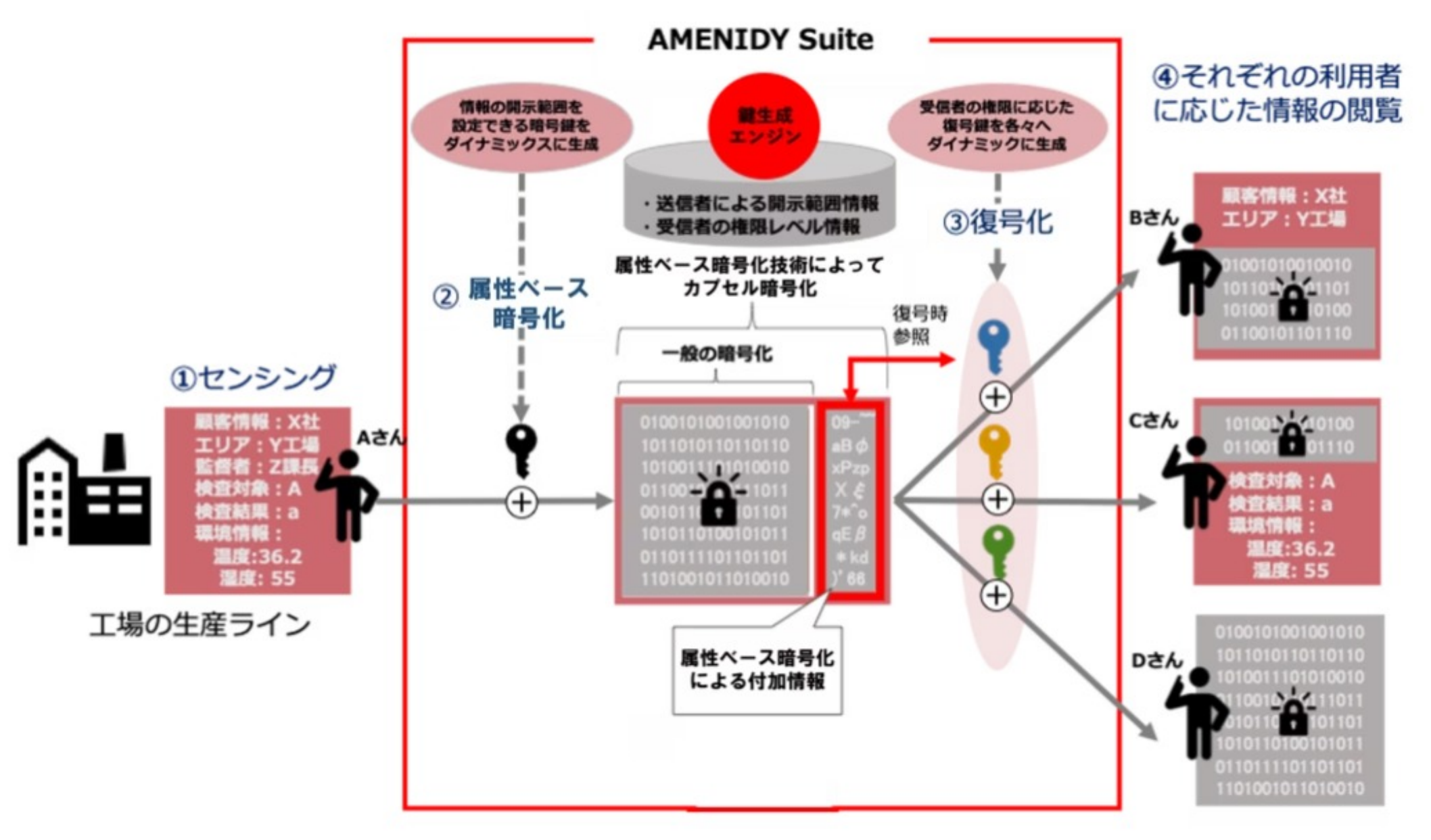
次世代暗号技術である属性ベース暗号を活用すると何が出来るのか、そしてそれが普及するとどんな未来が描けるのかについて触れていきます。

属性ベース暗号の活用例

属性ベース暗号により、暗号技術がより安全により容易に使えるようになれば、データの活用が促進されます。特に医療分野、金融分野、防衛分野など、より秘匿性の高いデータを取り扱う業界・分野や、データの種類や属性に応じて解読・活用可能な人や組織を細かくコントロールしたいシーン等で、さらにデータが積極的に活用されていくと考えられます。

例えば、ネットワークカメラで取得出来る画像データを元にAIで認識・解析した人の情報（性別、年齢、服装、挙動等）を、閲覧・活用権限保持者のみが柔軟かつ安全にアクセス可能とすることが出来ます。

例えば、製造業の工場にてセンシングにより取れる様々データを、部門に応じて部門毎に必要としているデータのみを共有することも出来ます。

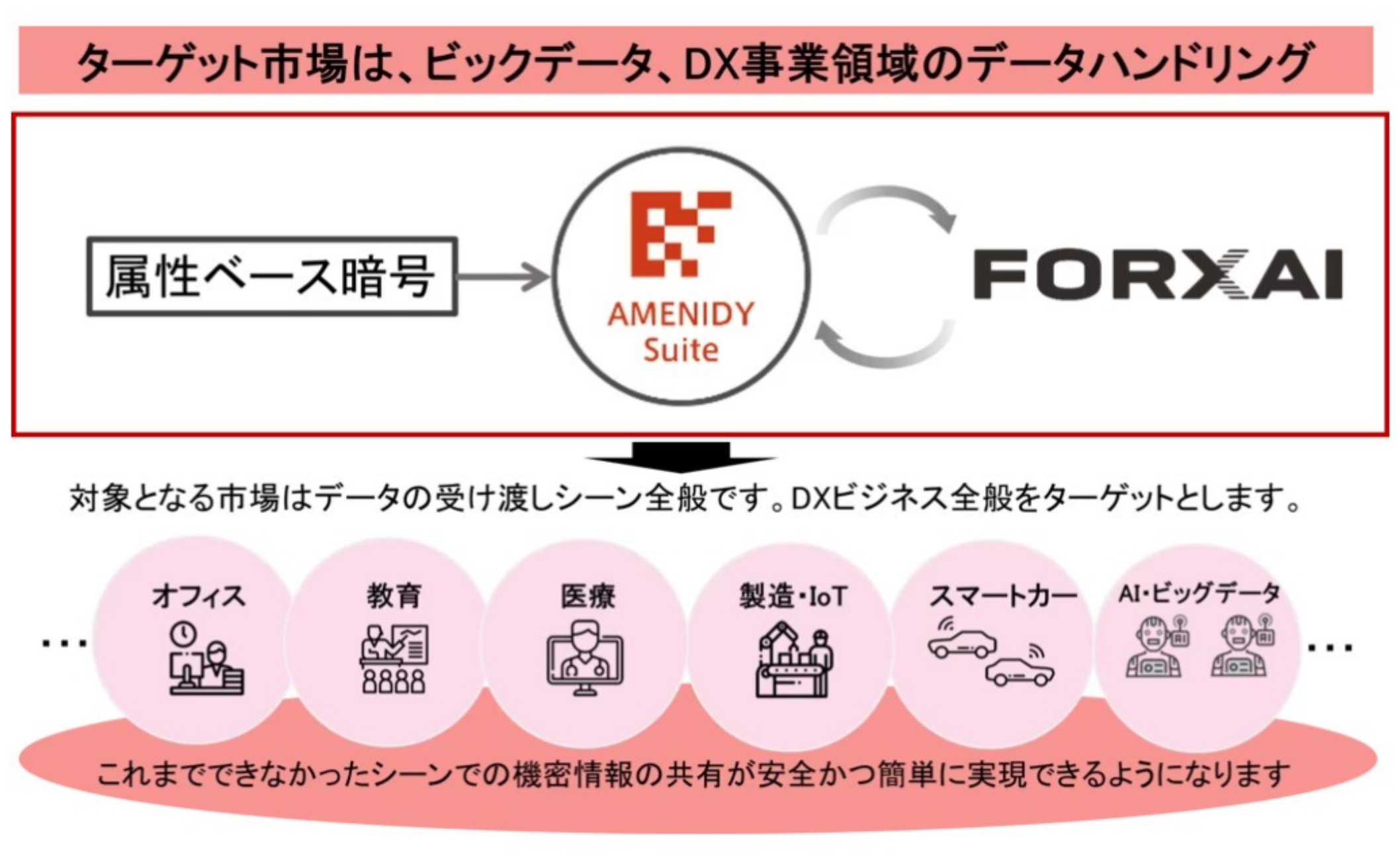


株式会社アメニディではこの属性ベース暗号技術を搭載したプラットフォームであるAMENIDY Suiteを開発・リリースしており、FORXAI上でも活用可能となっております。そのため、コニカミノルタ様の画像IoT技術や他のFORXAIパートナー様の技術等と組み合わせて新たなサービスやソリューションが開発可能となっております。

- AMENIDY,Inc.
- AMENIDY Suite

属性ベース暗号が普及した社会

属性ベース暗号にて安全かつ容易に共有可能となるデータは、画像データはもちろん、個人情報、金融関連情報、センシングデータ、購入した音楽や映像コンテンツ等、どのようなデータでも対象となり、それらのデータが適切な相手およびシステムだけが活用出来るようになります。



そのため、この暗号技術が普及することにより、現在世の中にあふれているほぼ全てのデータが安全で気軽に活用可能となり、そのデータにより個々人に最適化されつつ，社会全体でも無駄のないサービスや機能が多数創出され，その価値を享受出来るようになると思われます。

例えば、どこかに行きたい時、行きたい場所を選ぶだけで最適な手段、コスト、時間で移動出来る。

例えば、日々の日用品が意識することなく適切なタイミングで配送され、常に必要な時必要な物が手に入る。

例えば、重い病気等になる前に、個々人に適切な食事、運動、早期治療が提案されて健康が維持される。

例えば、仕事において事務作業等が最小化されて本来やるべき業務に集中できる。

そのような社会が来るのではと考えられます。

そして、人が本当にやりたい事だけに集中出来る未来がもうすぐ来るかもしれません。

コニカミノルタは画像IoTプラットフォームFORXAIを通じて、お客様やパートナー様との共創を加速させ、技術・ソリューションの提供により人間社会の進化に貢献してまいります。

新卒採用については以下の採用情報ページをご覧ください。

新卒採用情報 – 採用情報 | コニカミノルタ

コニカミノルタの新卒採用サイトです。募集要項や募集職種などの採用情報から、プロジェクト紹介、社員インタビューなどを掲載しています。ぜひご覧ください。

KONICA MINOLTA

中途採用に関する情報については以下の採用情報ページをご覧ください。

キャリア採用情報 – 採用情報 | コニカミノルタ

コニカミノルタキャリア採用情報　現在の募集職種にはこちらからエントリー可能です。募集要項、先輩インタビュー、人事部からのメッセージなど掲載。

KONICA MINOLTA

Masaaki Suzuki

株式会社アメニディ 執行役員。 大手SIerにて多様なシステムやサービスの開発に従事した後、コニカミノルタにてグローバルクラウドサービスの開発や画像IoT向けAIの研究・サービス開発に従事。その後、大手IT企業にて金融向けデータプラットフォームサービスの開発・提供を実施。そして、現職アメニディにて次世代暗号技術を用いたセキュアITサービス事業の戦略立案、事業開発、サービス開発・提供と、組織開発、組織構築業務を担当。

前の記事

第2回 AI品質マネジメントシンポジウム・登壇レポート

次の記事

Google Next Tokyo 2023に参加しました。

シェアする　ポスト　B! ブックマーク 0　Pocket 0　いいね　LINEで送る