

# IoT情報をどうやって保護する？ 最後の砦を守る、 次世代暗号プラットフォーム ～ データベース/インフラに求めること

株式会社アメニディ  
代表取締役 CEO 山下 祥宏  
CTO 鴨志田 達朗

2019.8.6



# アジェンダ

1. AMENIDYとは
2. AMENIDY Suiteを動かすために必要なこと
3. AMS for IoT(RT-Connecting)
4. AMENIDY Suiteの製品・サービスのご紹介
5. AMENIDY Suite サービス外観
6. AMENIDY Suite Core  
Oracle Cloud上での動作・パフォーマンス検証  
インフラ編、データベース編
7. デモ





# AMENIDYとは

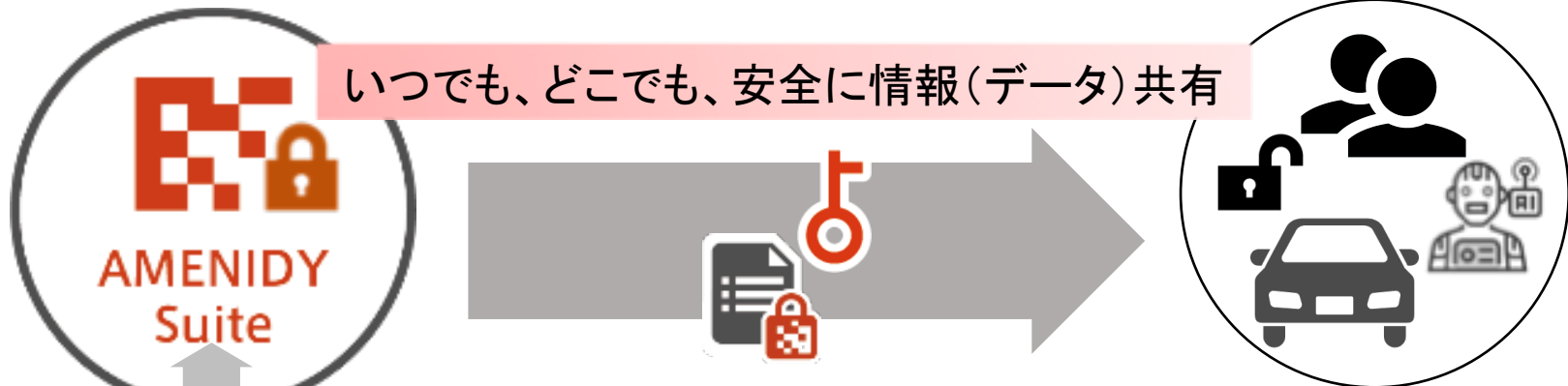
SECURITY



# 次世代暗号技術を活用した 【プラットフォーム】を ビジネス展開する企業です

自社次世代暗号技術  
プラットフォーム  
「AMENIDY Suite\*」

閲覧権限を  
持っている人・モノ



\*AMENIDY Suiteを以降AMSとも表記します



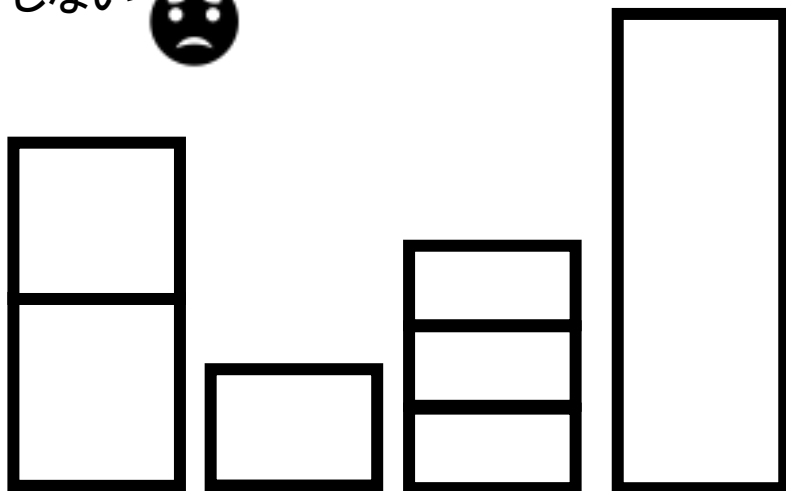
# AMENIDY Suiteはプラットフォーム技術です

## 従来ケース

個別開発によっても、課題は100%解決しない



個別開発による サービス群



暗号技術



汎用(標準)暗号技術

データ

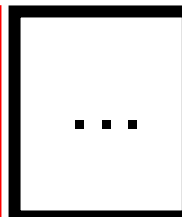


IoT/ビッグデータ

## 自社プラットフォームでのケース

サービス群

自社  
サービス



これまで難しかったインテリジェンスなファイル共有やIoT機器、車などのM2M認証サービスが作れます



自社次世代暗号技術  
プラットフォーム



PAT.

## API連携

- ・スマートアクセス(即時共有、停止)
- ・利用追跡機能提供
- ・ピアtoピアでの相互認証機能
- ・先端暗号技術でのデータ保護

暗号技術



先端暗号技術(利用技術)

データ



IoT/ビッグデータ






# 機密情報利用時のお決まり事

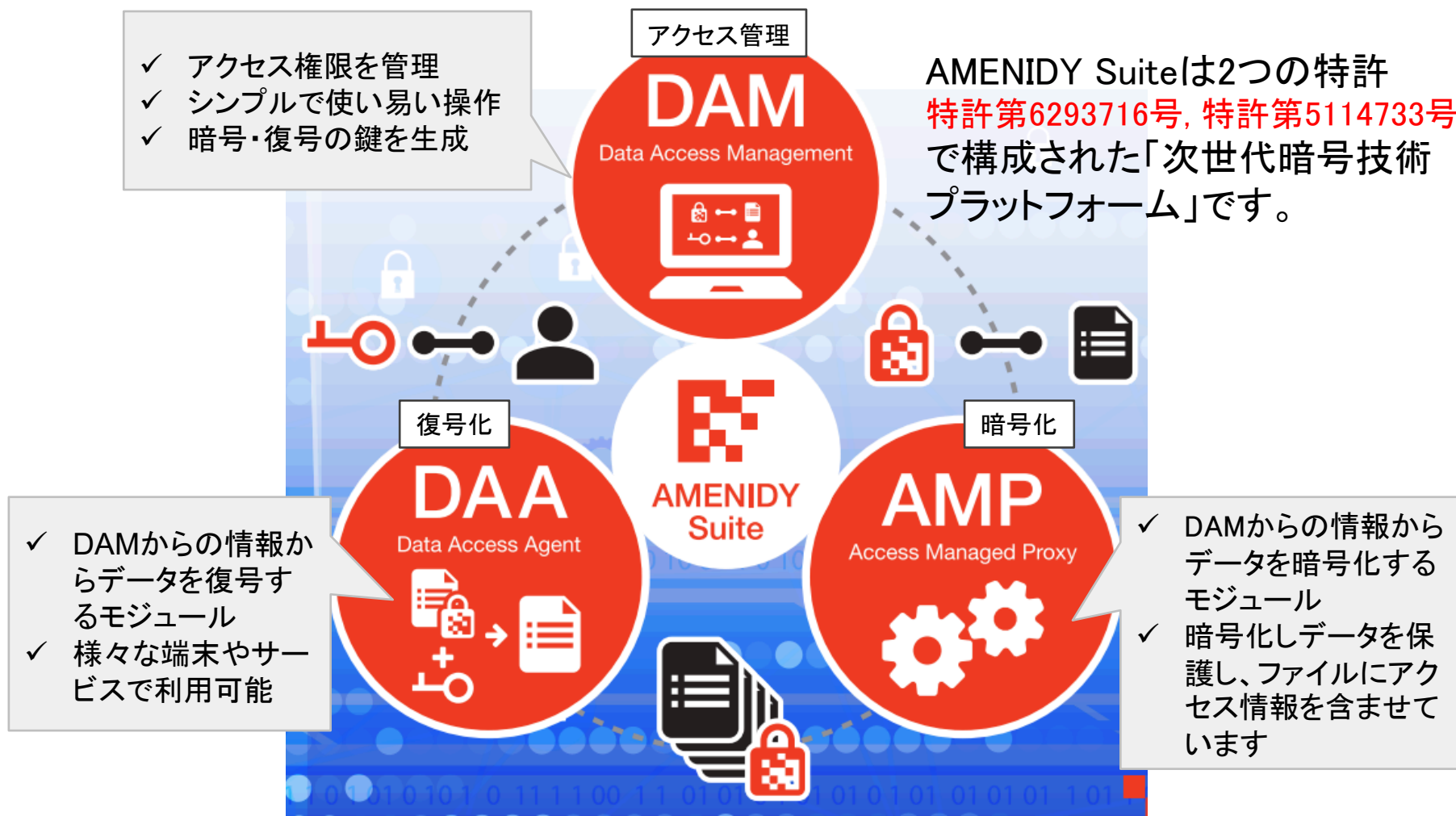
1. ユーザー権限に合わせた綿密なデータアクセスの仕組みを必要
2. ネットワークセキュリティを保つことでのデータ保護が必要
3. 利用ユーザーへ利用場所の制限を課す必要

## 課題

「使う環境はいまひとつ」  
ビッグデータの活用は進みません



# AMENIDY Suiteの3つの技術で達成します

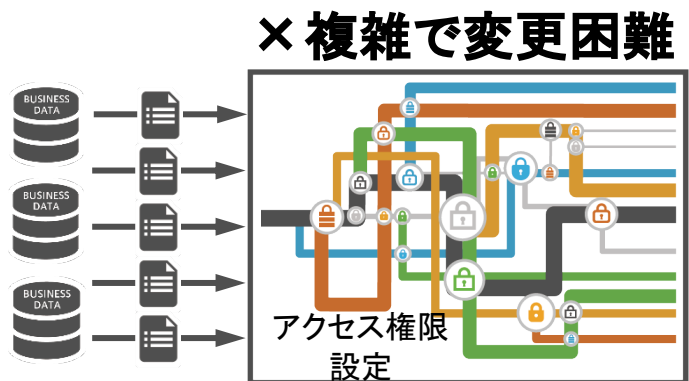


当社技術の根幹: 1つの公開鍵: 1つの秘密鍵ではなく、**1つの公開鍵: n個の秘密鍵**

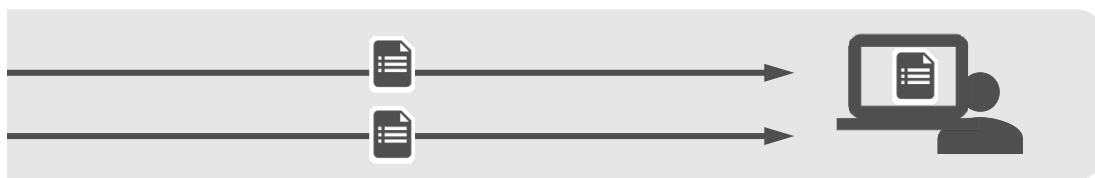


# AMENIDY Suiteの特徴 ①「アクセス制御は簡単」

## 従来方式



△ネットワークセキュリティでデータ保護



× データは保護されていない △利用場所が限定

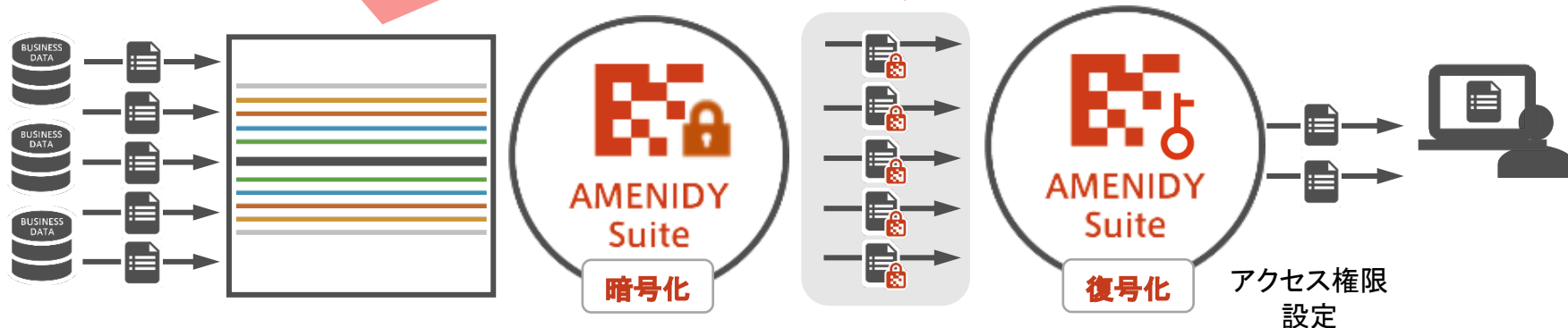
## AMS方式

× 多大な工数を消費

○シンプルかつ即時変更可能

○データ暗号化保護

○利用場所を限定しない



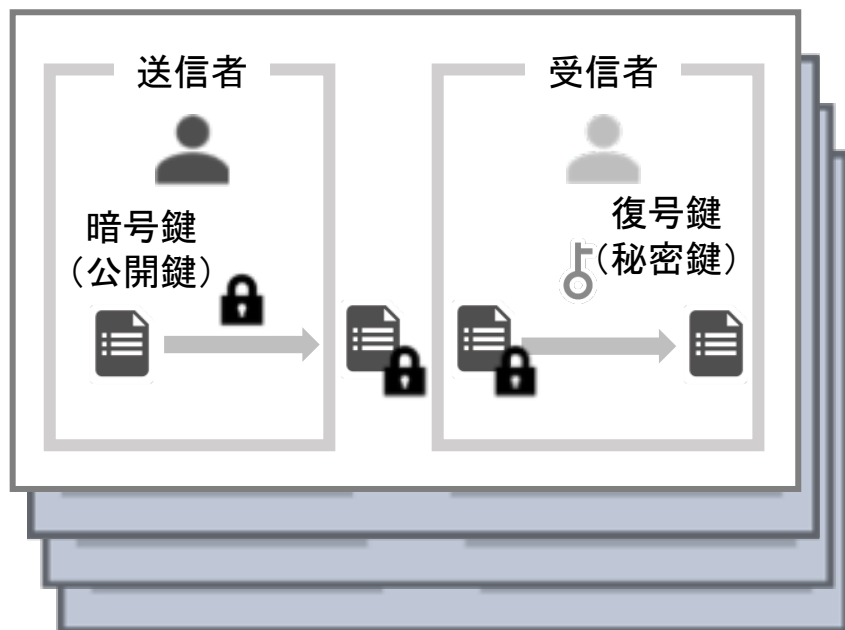


## AMENIDY Suiteの特徴 ②「暗号鍵は1つ」



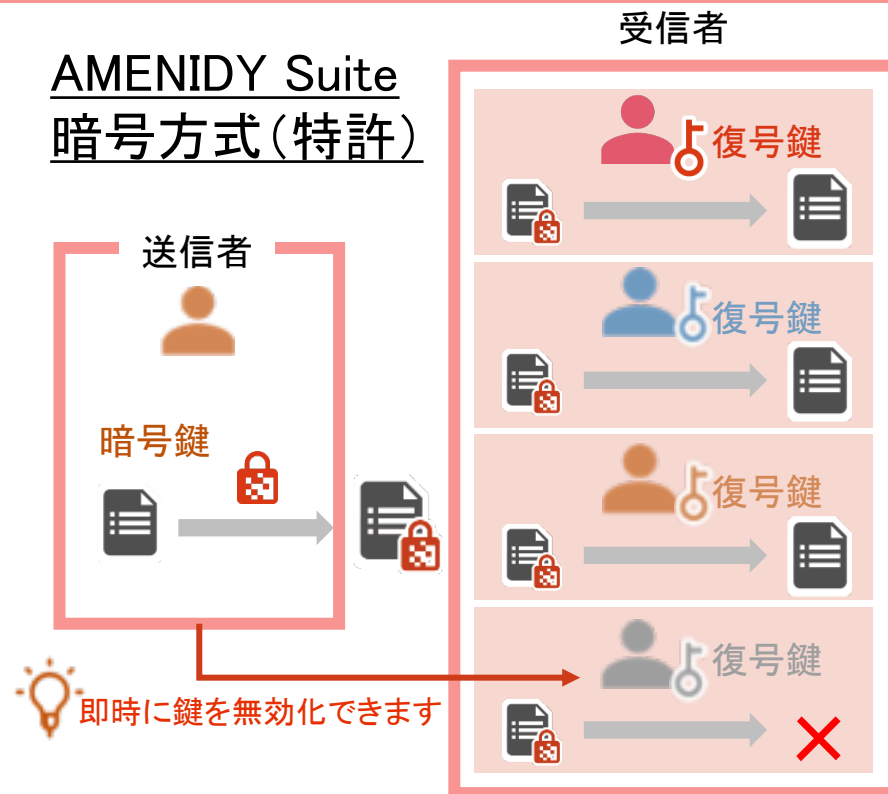
「膨大な鍵の管理(既存のPKI基盤)」はいずれ破綻します

### 公開鍵暗号方式



一つの暗号鍵に対して一つの復号鍵  
(復号鍵は厳重に管理)

### AMENIDY Suite 暗号方式(特許)



**1つの暗号鍵**で複数の復号鍵  
アクセス権は、柔軟に変更・破棄可能



# AMENIDY Suiteの特徴 ③「簡単に権限設定ができます」

AMENIDY, Inc. Master administrator

ユーザーリスト 組織図

所属名の入力...

ドラッグ・アンド・ドロップで権限変更が即時できます

(株) amtwostech セキュリティ事業本部

yamashita@amtwostech.co.jp  
012e44a7a50c9c44

(株) amtwostech x セキュリティ事業本部 x

前田 勝之  
maeda@amtwostech.co.jp  
012e44a7a50b9796

IoTコンサル事業部 x

IoT事業本部

IoTコンサル事業部

「x」をクリックで権限が即時削除され、以降ファイルは見れません

複雑な構成にも即時、権限設定が可能

研究開発本部

セキュリティ技術研究所

IoT技術研究所

AI技術研究所

経営企画部

AMENIDY Suite for Cloud Storage

利用ユーザーへの権限付与状況

権限構造(組織図など)

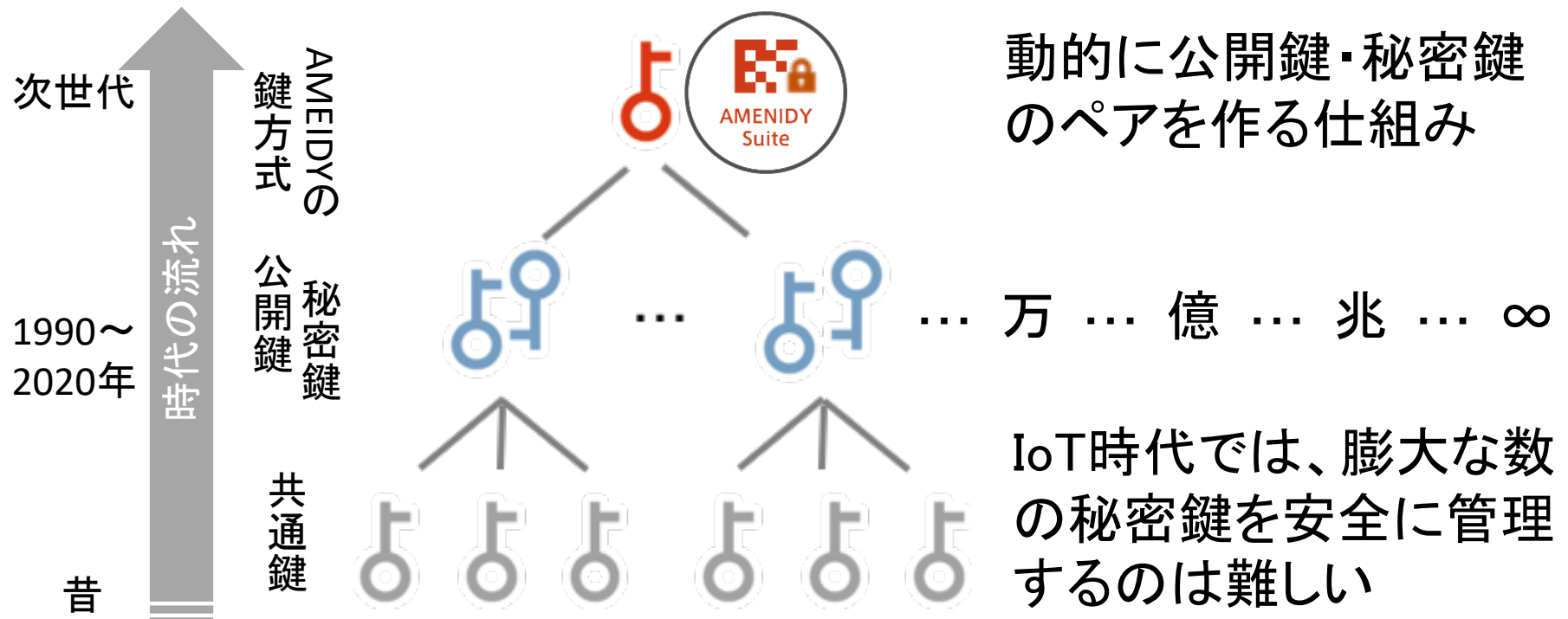




# AMENIDY Suite を動かすための必要なこと



# IoT時代の鍵管理の問題から



AMENIDY Suiteは鍵管理の優位さで、受け入れられると考える一方、「動的な鍵発行」のために必要となる、**クラウド基盤で「高い計算処理能力」を必要**とします



# 使いやすいアクセス権限設定の実現に向けて

権限構造と連携した  
暗号ファイル



AMENIDY Suiteの  
権限設定画面



権限構造の柔軟な設定、変更  
ができること



AMENIDY Suiteは柔軟なアクセス権限設定を可能とするために、  
自社特許の「権限チェーン」をグラフ構造を得意とするデータベー  
ス技術で実現しています。このためクラウド基盤に対して**「洗練さ  
れた優秀なグラフ型DB」**を備えていることを必要とします





基本機能の達成のため

優秀な処理能力を  
持ったクラウド

UX向上のため

洗練されたグラフ型DBを  
持ったクラウド





The background of the slide is a grayscale photograph of several toy cars on a light-colored surface. In the center, a silver hatchback is shown from a rear three-quarter view. To its right, the front wheel and part of a larger, darker toy vehicle are visible. On the left, another smaller toy car is partially seen. The overall scene is slightly out of focus, emphasizing the text overlay.

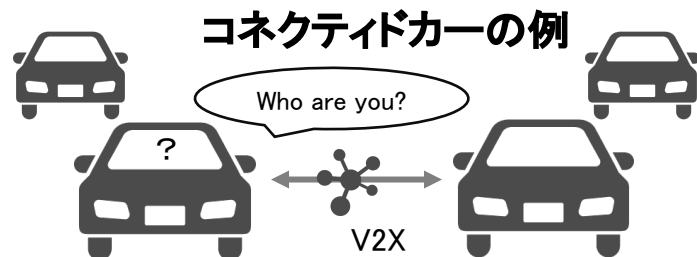
# ご参考(研究開発中) AMS for IoT(RT-Connecting)



# 参考) AMS for IoT <膨大な量のIoTデバイス向け>

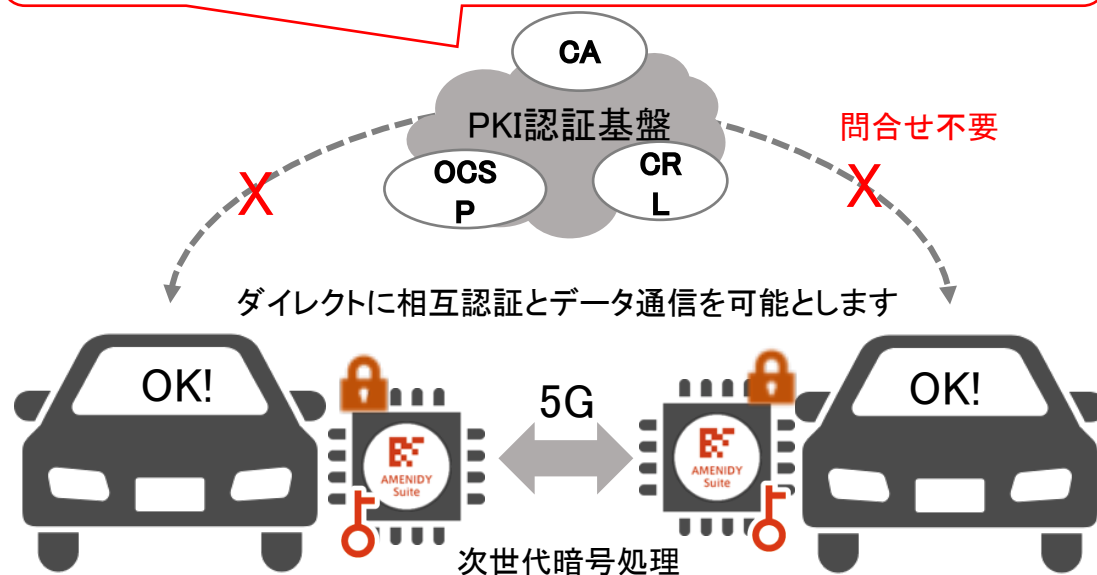
## AMS for IoT(RT-Connecting)

組込ソリューションによるライセンス販売を想定



AMSでリアルタイムに莫大な車車間通信の相互認証を解決

V2Xの世界では、信頼ある車車間通信が大前提とされているが、PKI認証に委ねた仕組みは膨大な車数に対して限界あり



### 提供機能

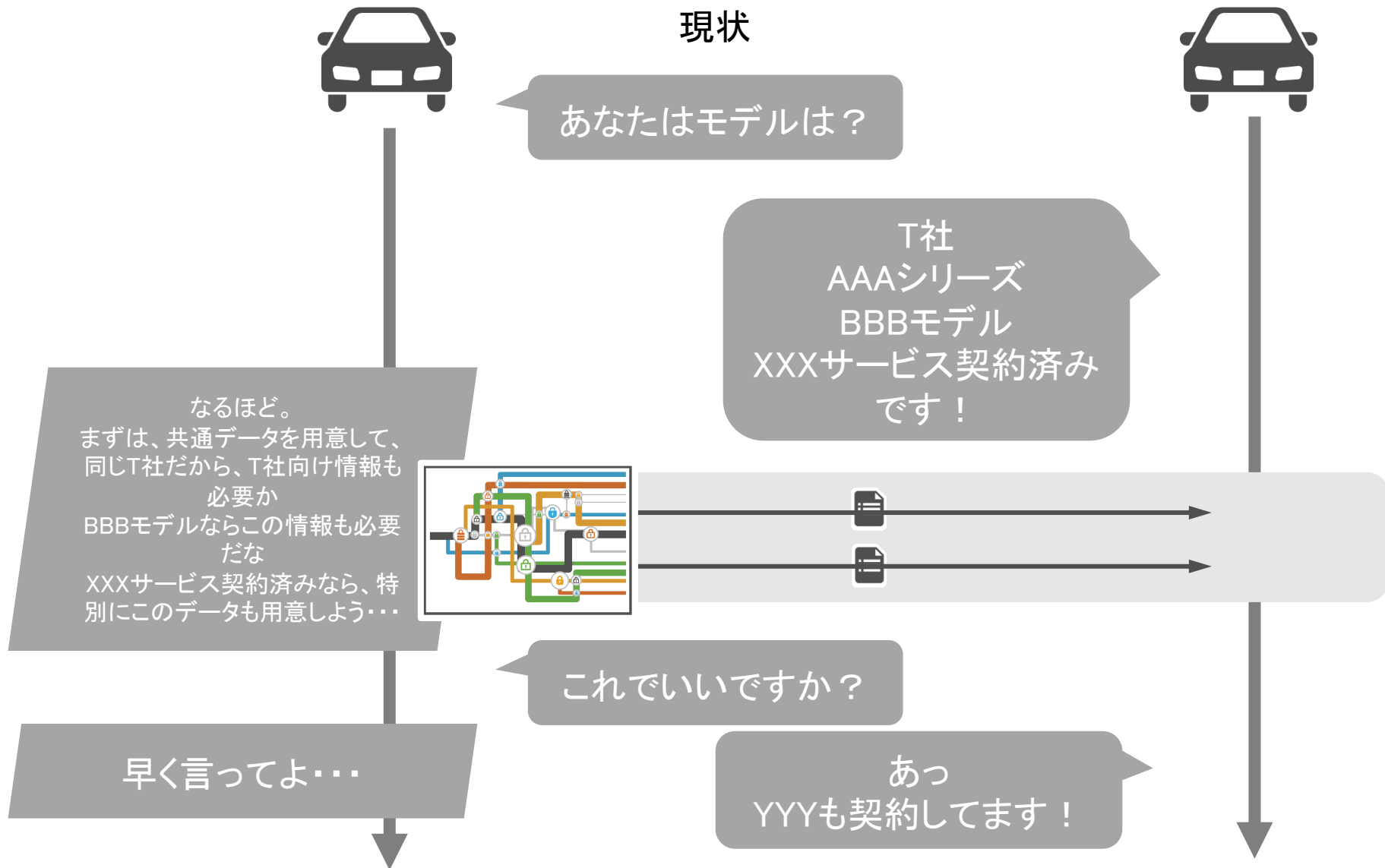
- PKI認証基盤に依存せず相互認証機能をP2PTポロジで提供可能
- リアルタム、大量のIoTノードの相互認証が可能
- 自社特許技術に基づく耐タンパデバイスへ実装による堅牢性、他IoTデバイスへの移植性
- SDKおよびデバイスへのデプロイ支援SaaSサービスを提供予定

### ターゲットユーザー

- コネクティッドカーメーカー
- オンプレネットワーク下でのシンプルな相互認証機能を要する医療・工場分野

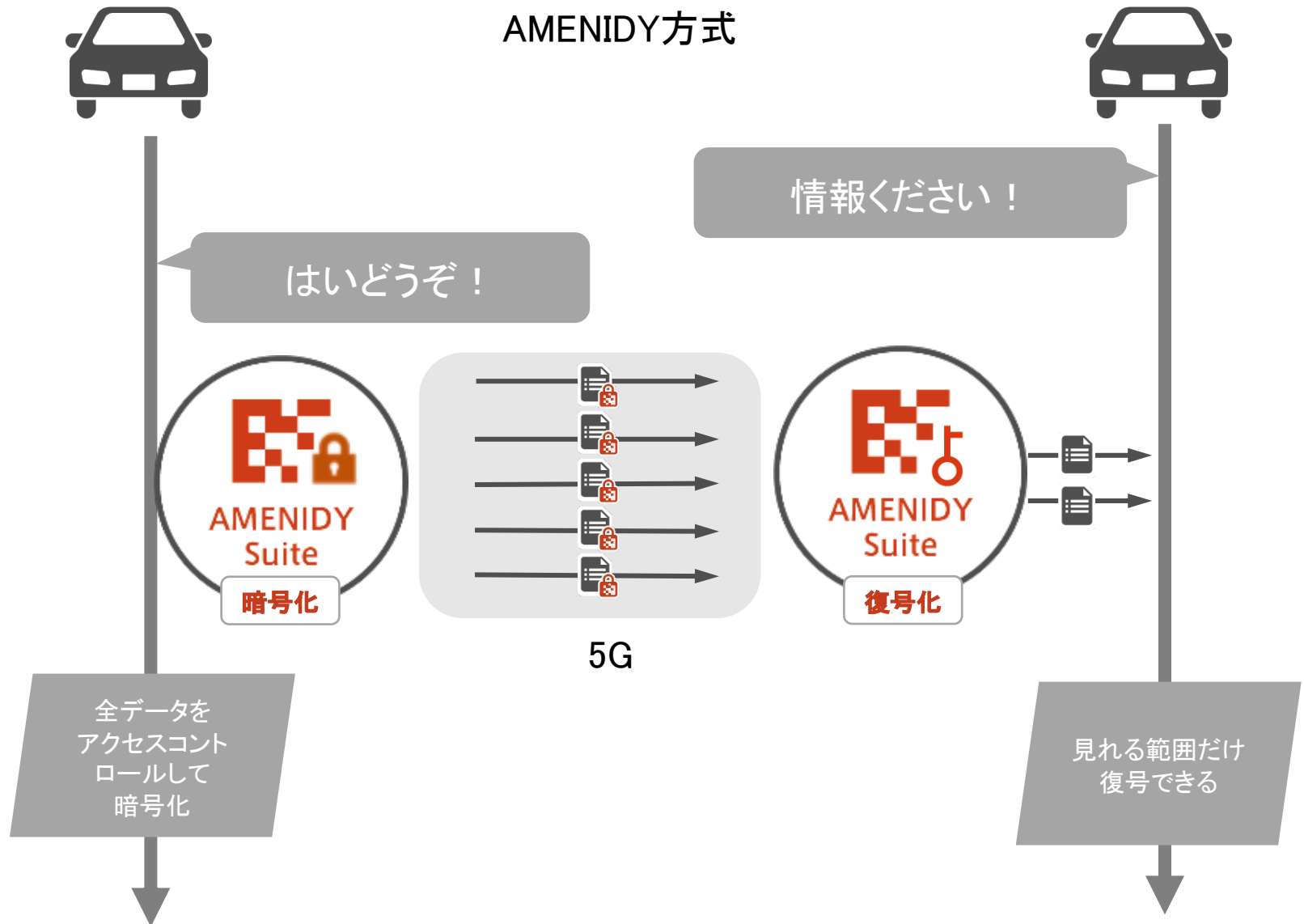


# ご参考: AMS for IoT <膨大な量のIoTデバイス向け>





# ご参考: AMS for IoT <膨大な量のIoTデバイス向け>







# AMENIDY Suiteの 製品・サービスのご紹介

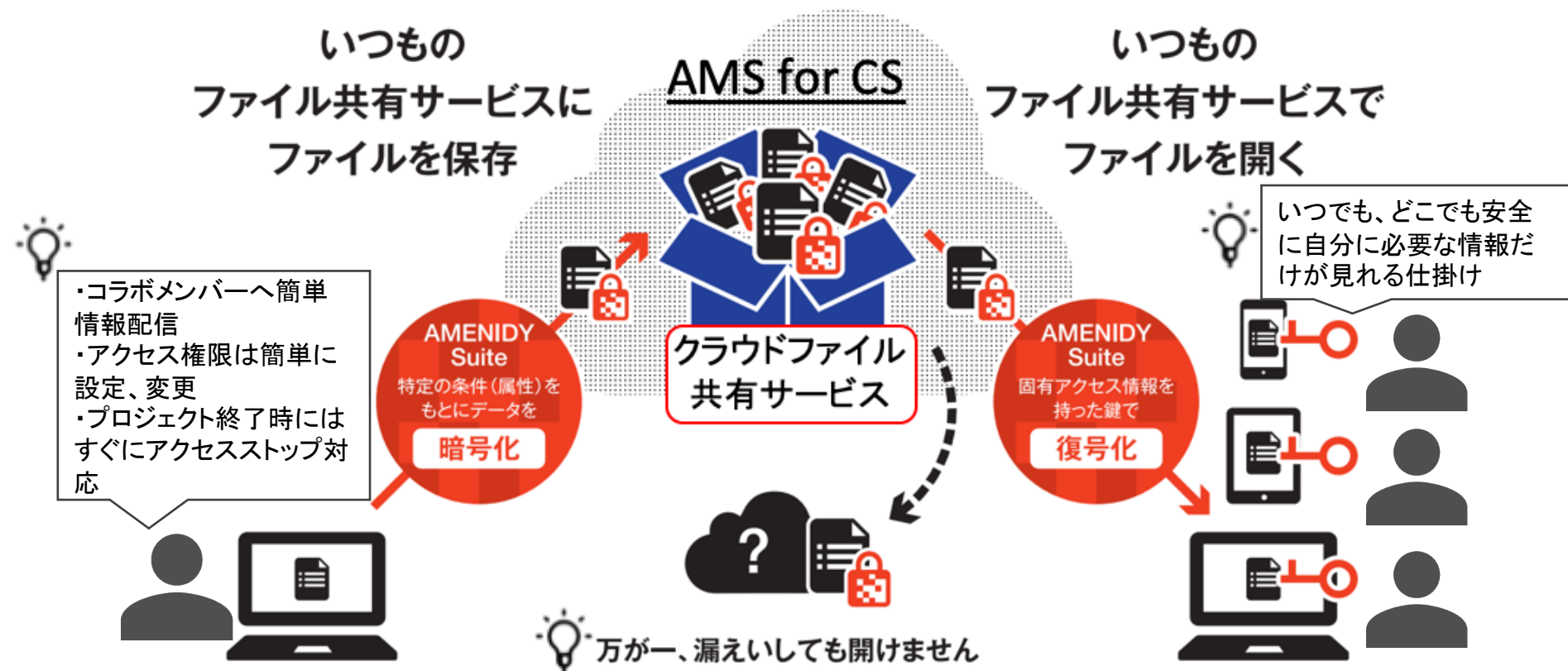




## AMS for CS PCアプリの使い方イメージ



クラウドの箱を利用して、「いつでも、どこでも、誰でも情報共有」  
クラウド事業者は一切ファイルの中身を知られることはありません。  
共有設定はAMENIDY Suiteによって簡単かつ即時可能です

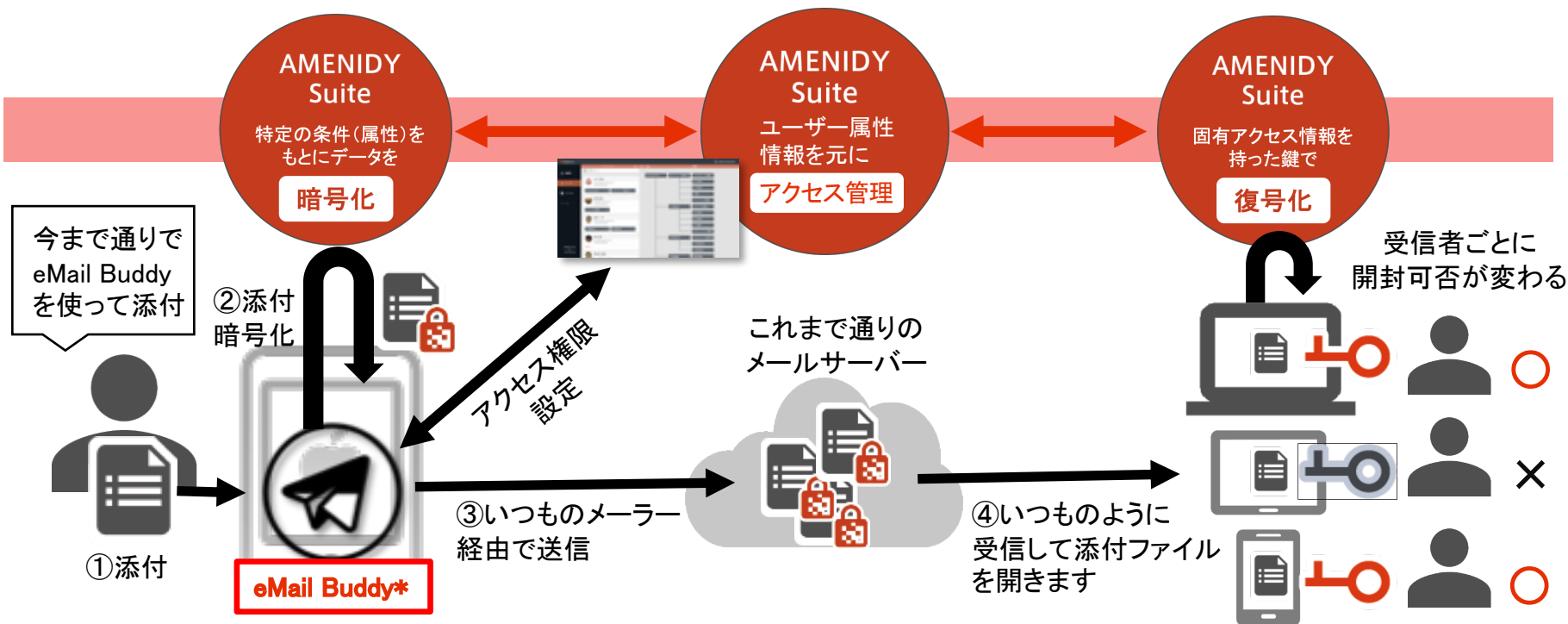




# AMS for CS iOSアプリ(eMail Buddy)使い方イメージ

💡 形骸化したパスワードZIP添付メールの時代は終わります！

eMailでのパスワード付き圧縮添付ファイル送信の世界を変えます。  
ファイル添付時にeMail Buddyを使って、いつものメーラーで送信するだけ。開封許可のある受信者は、それを開くだけ。  
後日、送信者が受信者の許可変更(＝取り消し)も可能です。





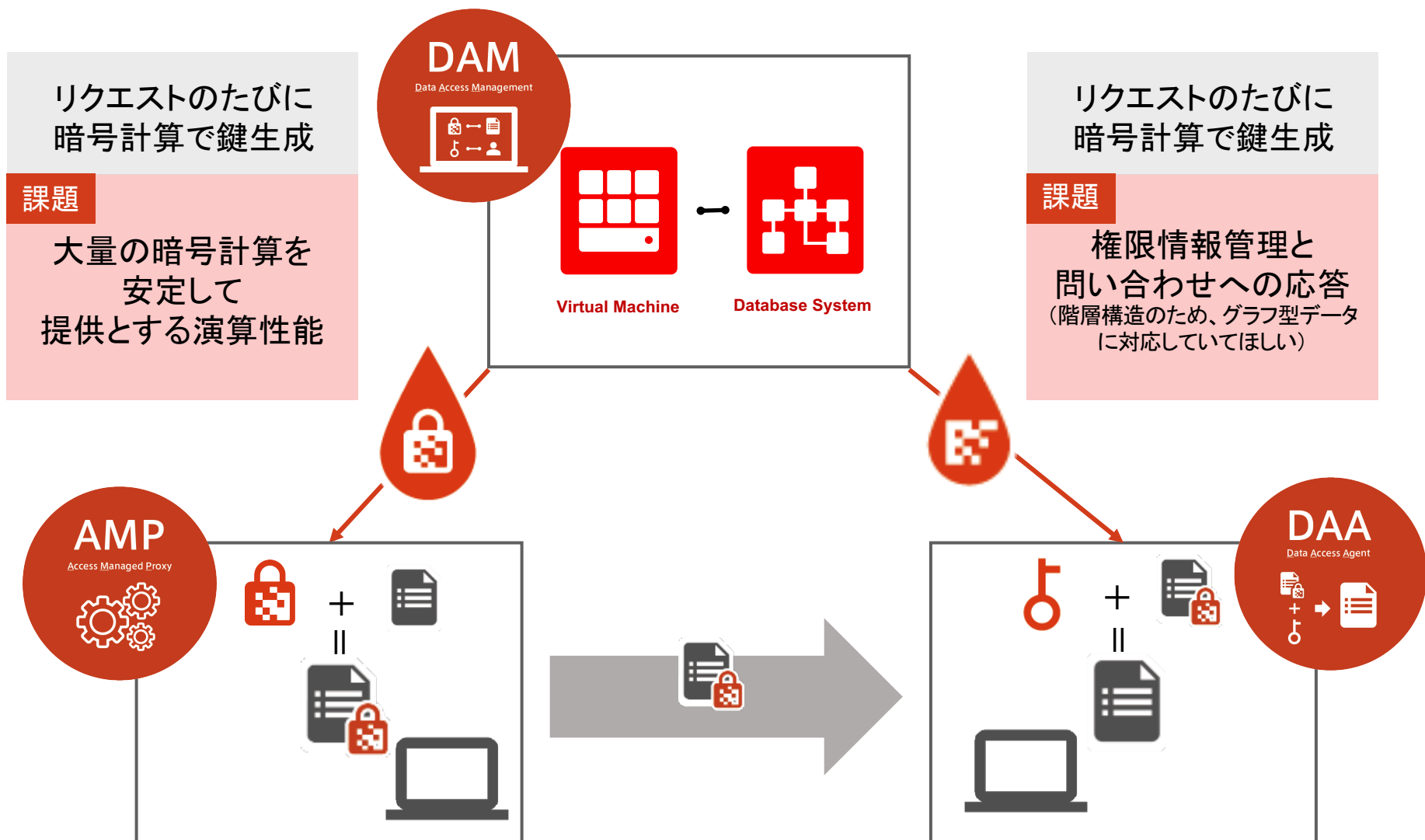


# AMENIDY Suite

## サービス外観



# AMENIDY Suite システム構成図



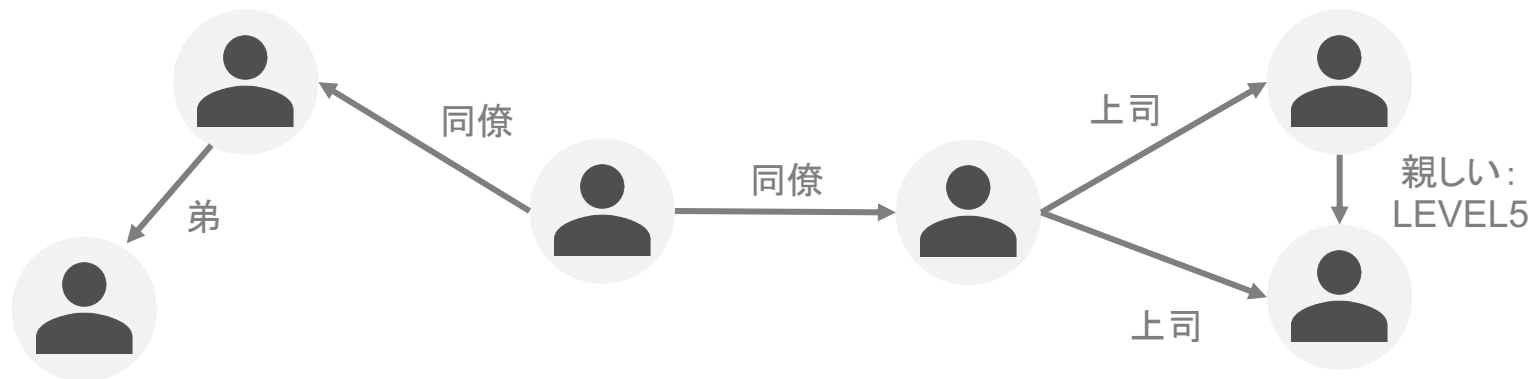


# グラフ型DBを活用したAMENIDY Suiteの情報管理

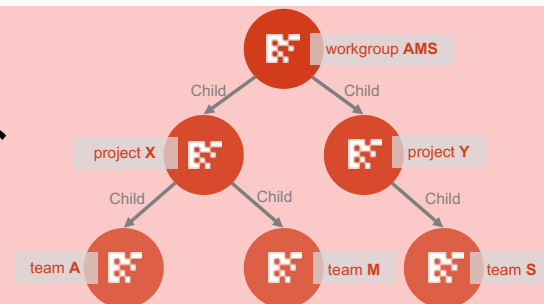
## グラフ型データベースとは・・・

FacebookやTwitterなどのSNSが利用している繋がりを高速に管理するデータベース  
「グラフデータ」を格納でき、演算できる

### グラフデータ: 点と線で表現されるデータの集合



AMSは、グラフ型データベースの特徴を利用し、  
アクセス情報やユーザー情報を  
柔軟・高速に管理可能としています。



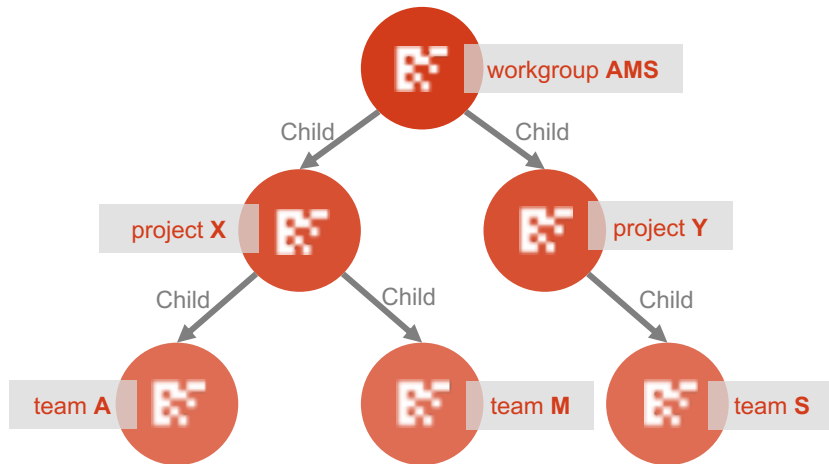





# AMENIDY Suite Core Oracle Cloud上での 動作・パフォーマンス検証 ～インフラ編～



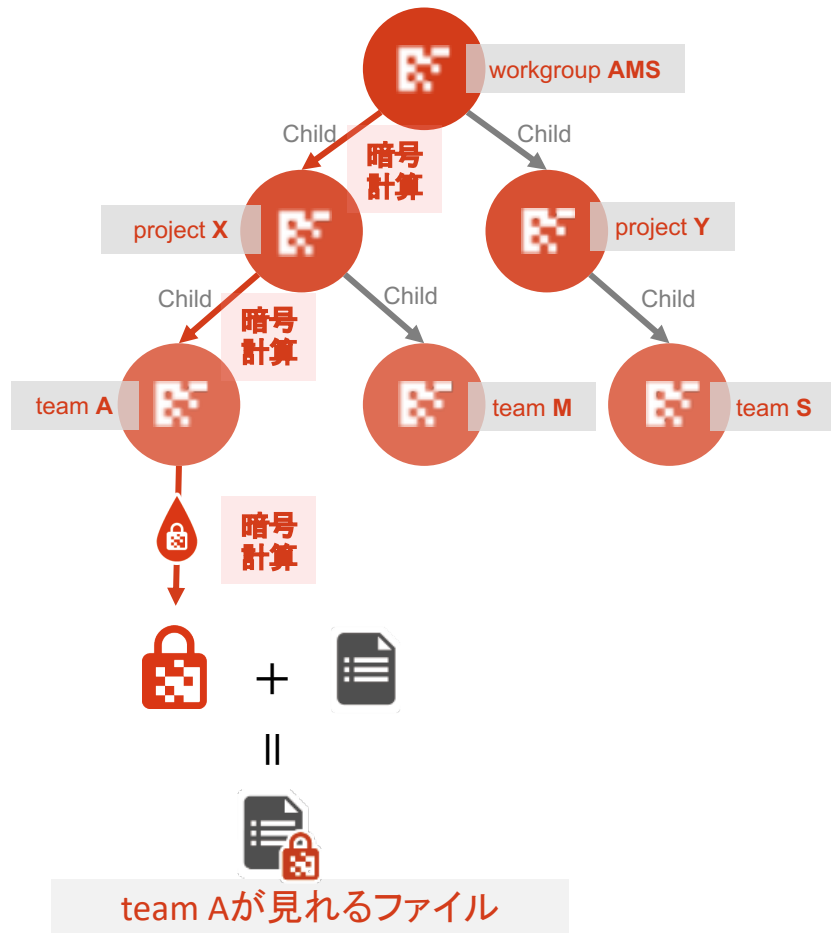
## AMENIDY Suiteの技術的特徴




 アクセス権限は、階層構造で管理



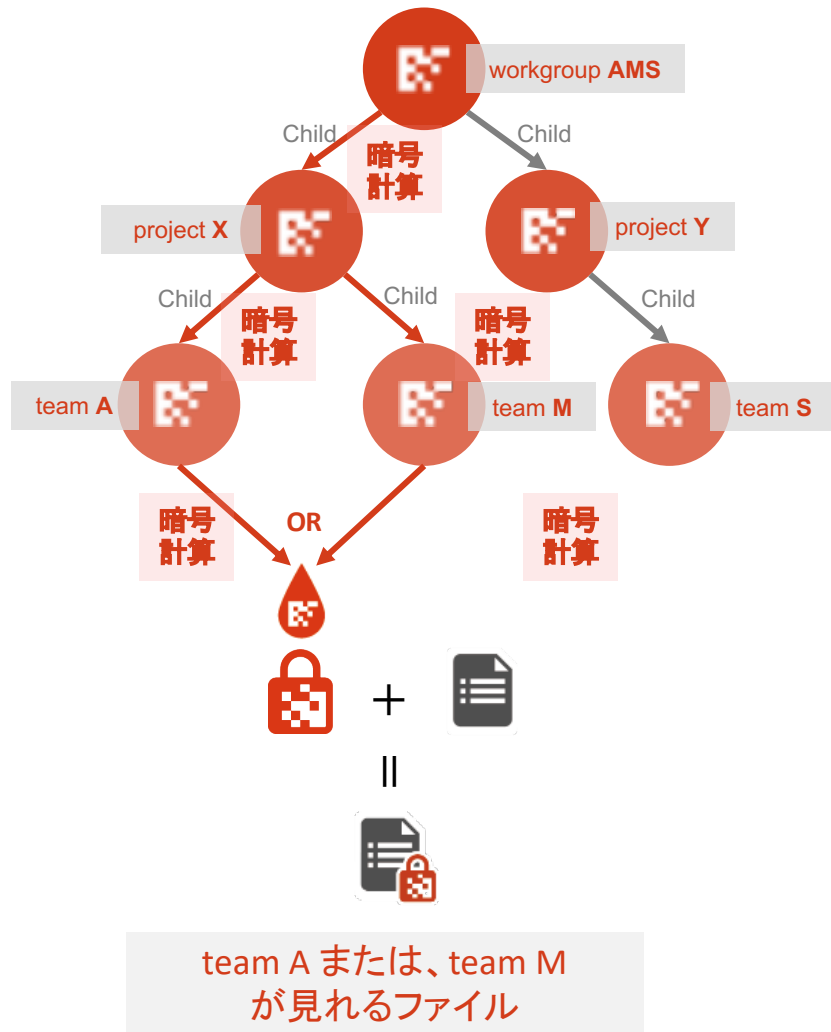
# AMENIDY Suiteの技術的特徴



 暗号化の鍵は、計算で都度生成  
暗号化鍵を管理は不要



# AMENIDY Suiteの技術的特徴

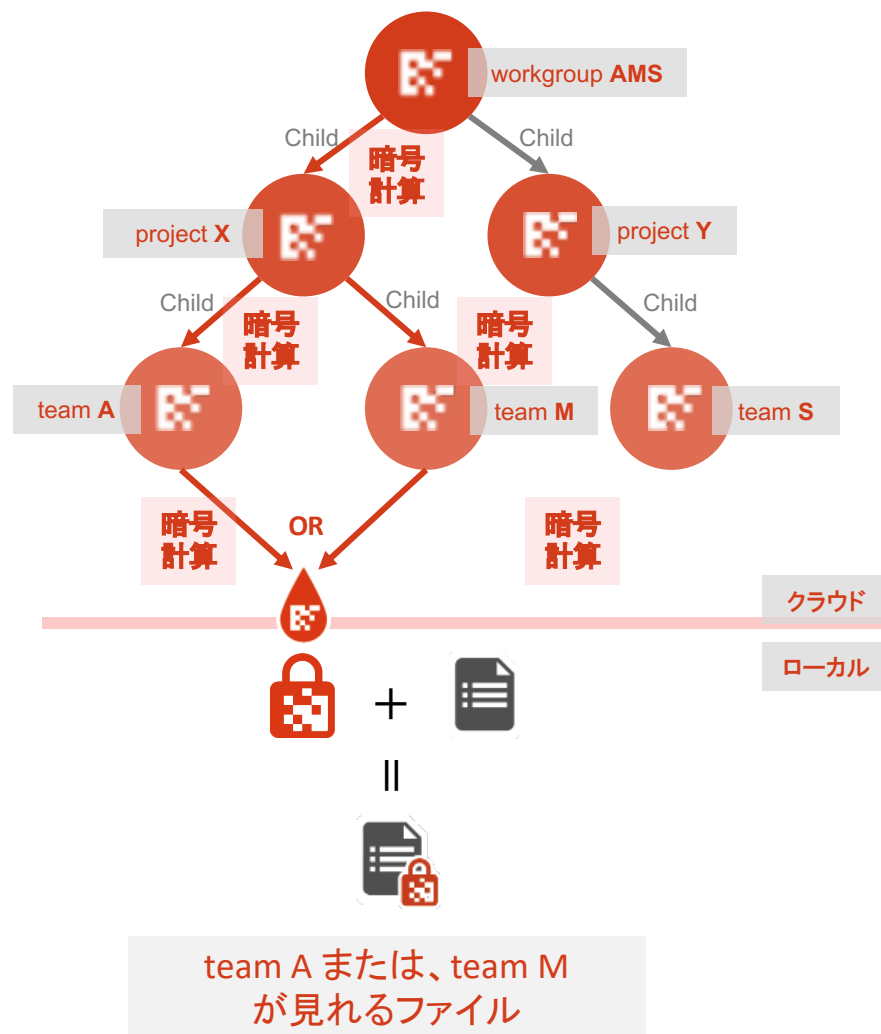


複合的なアクセス権限設定も可能

if...then.. 処理は暗号技術で代行



# AMENIDY Suiteの技術的特徴

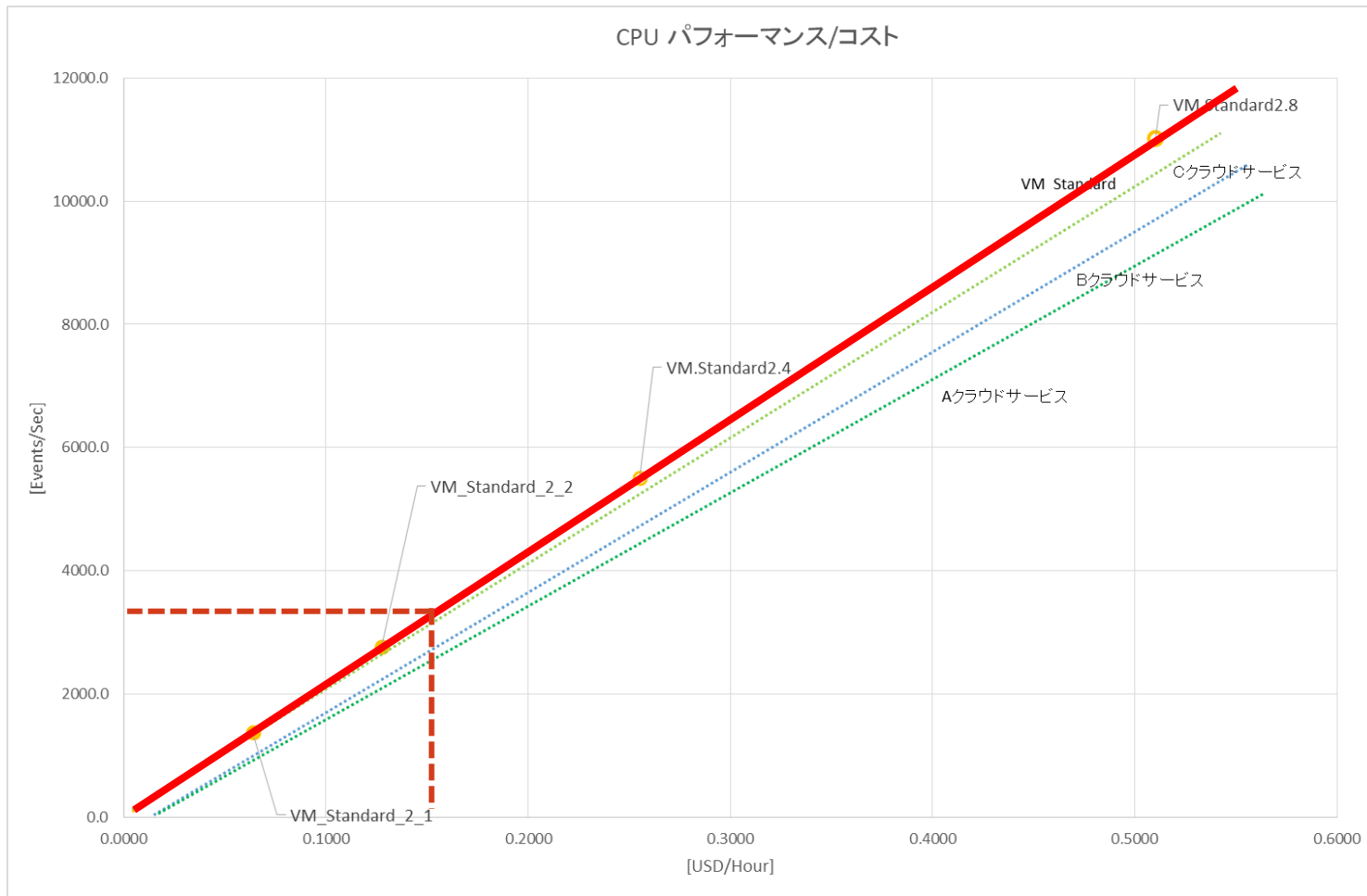


AMSがクラウドに求める事①  
大量の暗号計算を安定して  
可能とする演算性能

AMSがクラウドに求める事②  
柔軟にスケールしつつ、  
コストパフォーマンス



## sysbench※による、パフォーマンス計測



※ sysbench: Scriptable database and system performance benchmark

広く用いられているベンチマークソフトウェアの一つ。Linux, macOS, Windows 上で、CPU, メモリ, ファイルシステム等のパフォーマンスを計測することができるツール



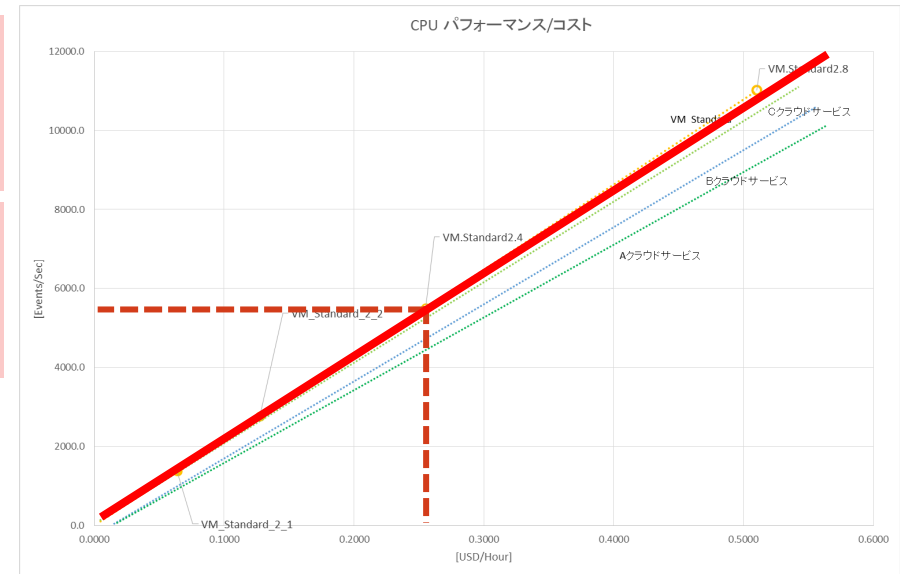
# Oracle Cloud Infrastructure 調査

## AMSがクラウドに求める事①

大量の暗号計算を安定して  
可能とする演算性能

## AMSがクラウドに求める事②

柔軟にスケールしつつ、  
コストパフォーマンス



1. CPU処理という面では、サービスに大きな差はなかった。
2. 同じ性能でのコスト比較をすると、他のサービスよりコストパフォーマンスが高い

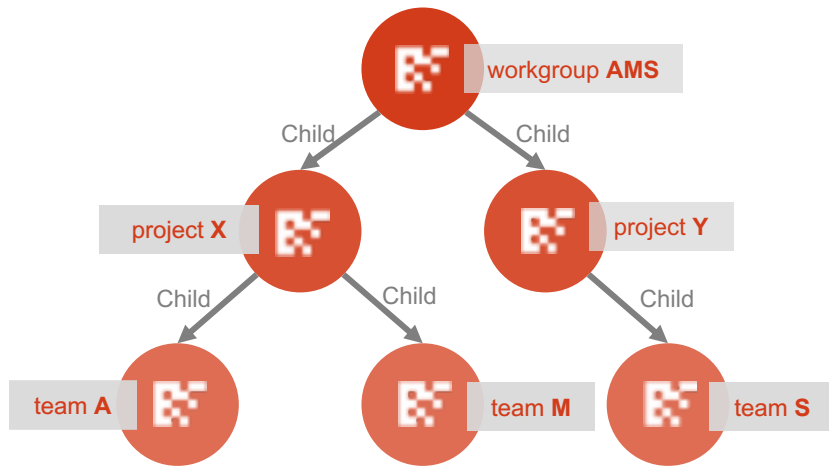




# AMENIDY Suite Core Oracle Cloud上での 動作・パフォーマンス検証 ～データベース編～



# AMENIDY Suiteの技術的特徴



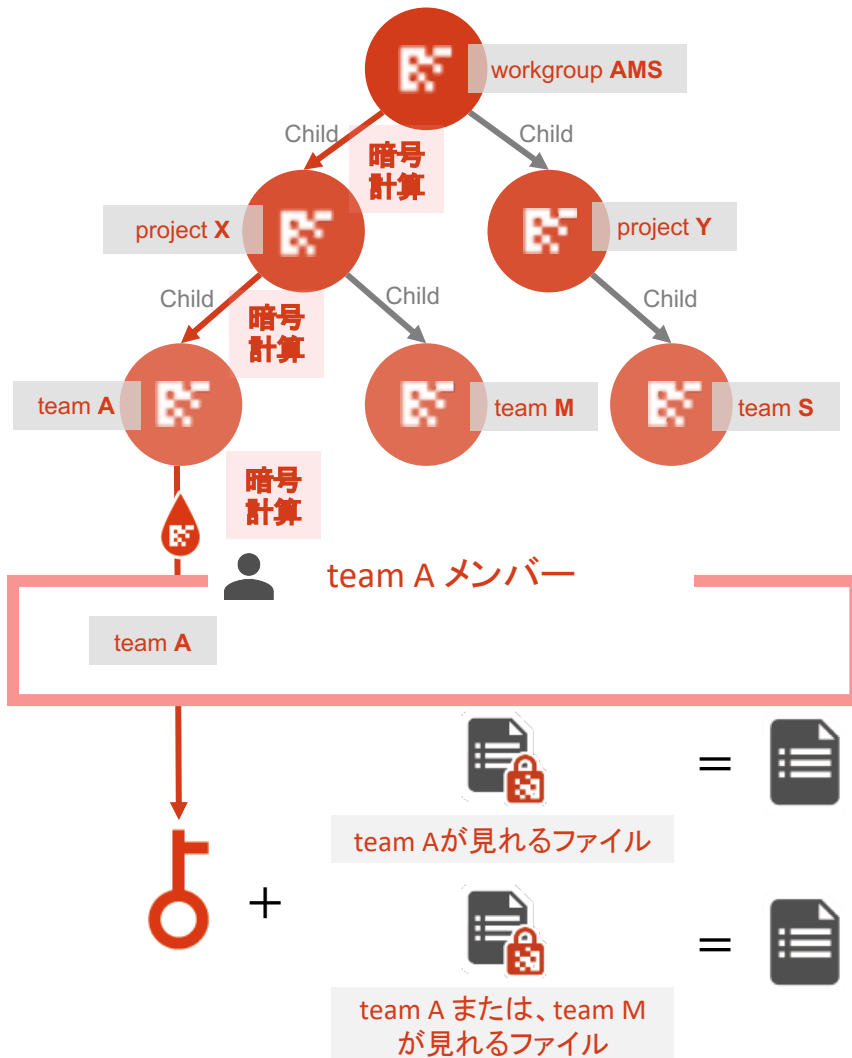
ユーザーの権限は、  
コンテキストに応じて柔軟に設定



project X リーダー



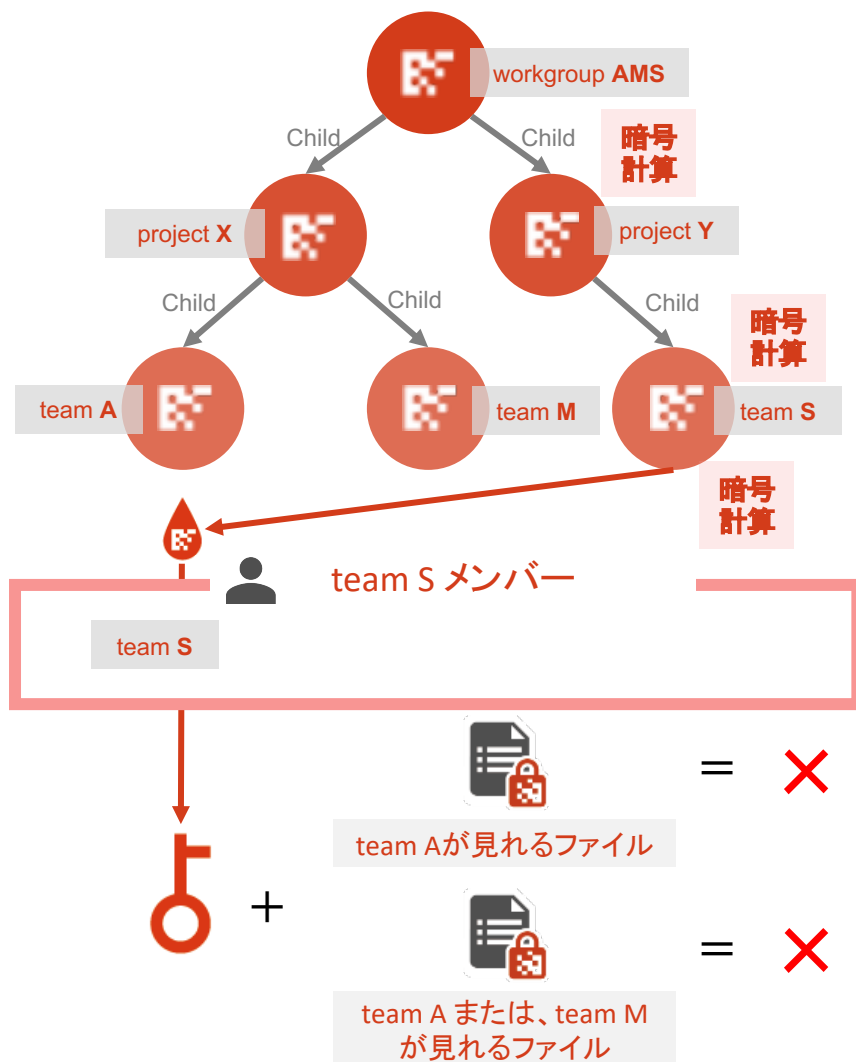
# AMENIDY Suiteの技術的特徴



復号の鍵は、計算で都度生成  
鍵の管理は不要



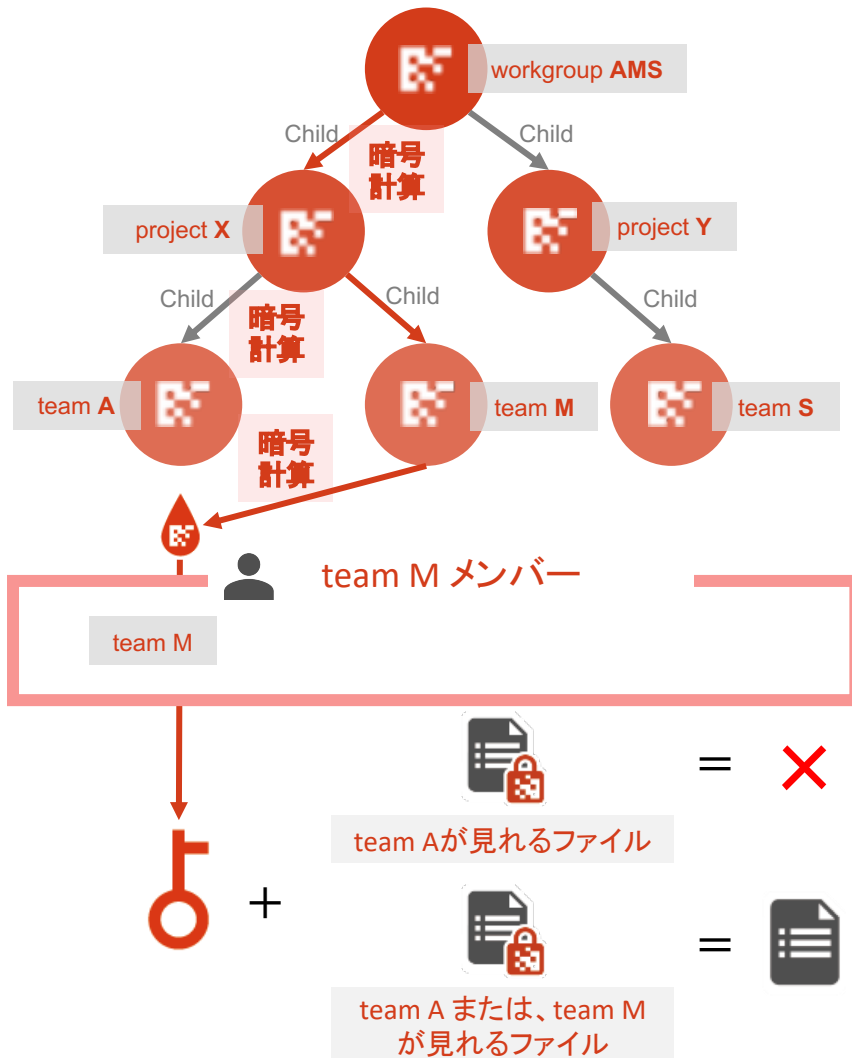
# AMENIDY Suiteの技術的特徴



復号の鍵は、計算で都度生成  
鍵の管理は不要



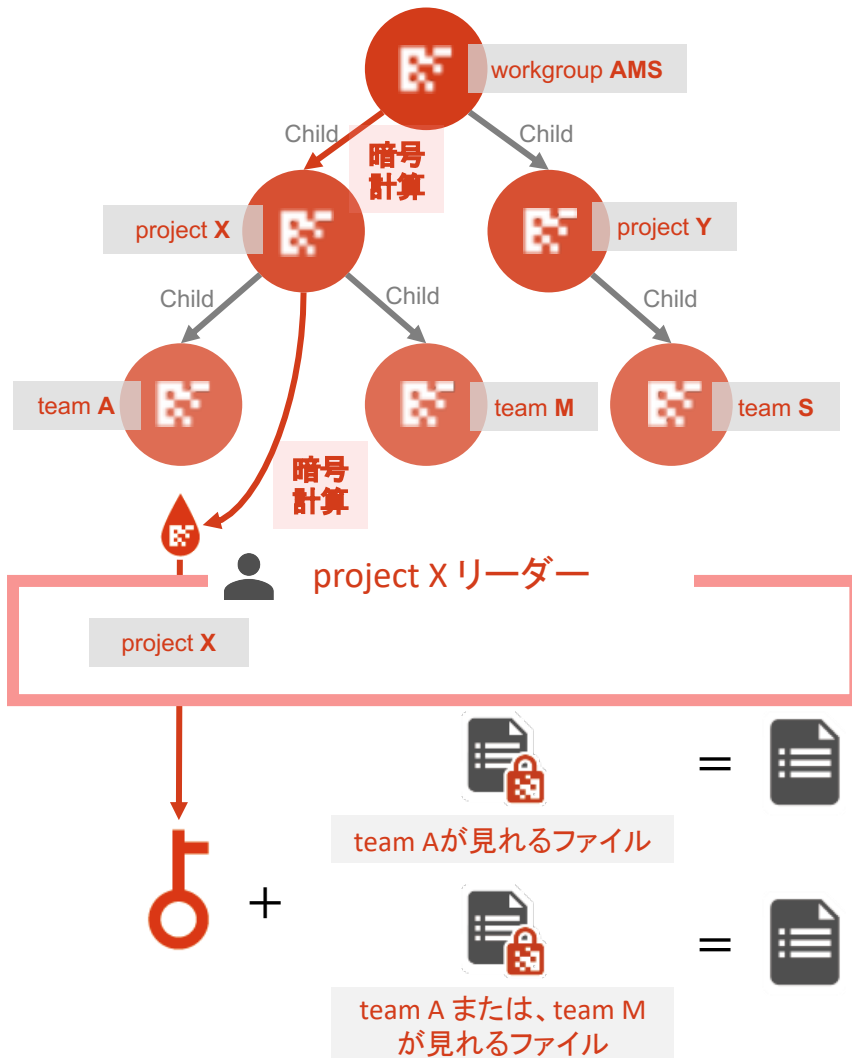
# AMENIDY Suiteの技術的特徴



復号の鍵は、計算で都度生成  
鍵の管理は不要



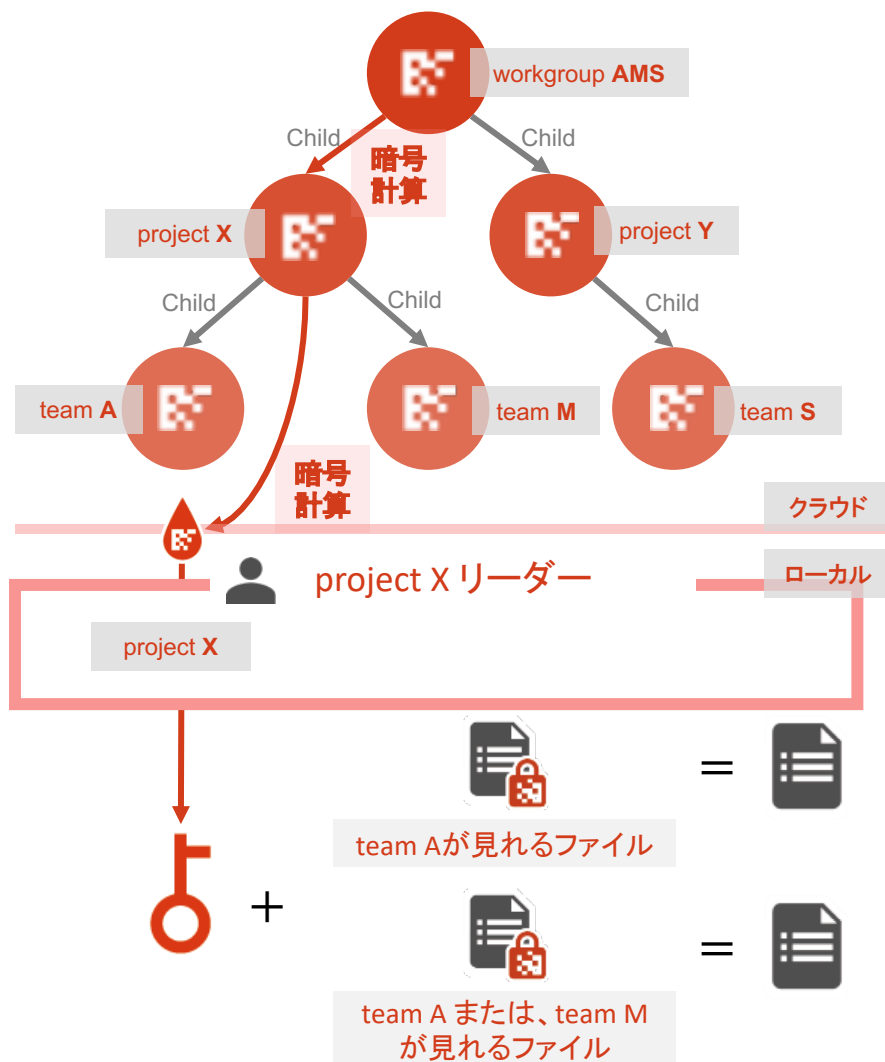
# AMENIDY Suiteの技術的特徴



復号の鍵は、計算で都度生成  
鍵の管理は不要



# AMENIDY Suiteの技術的特徴

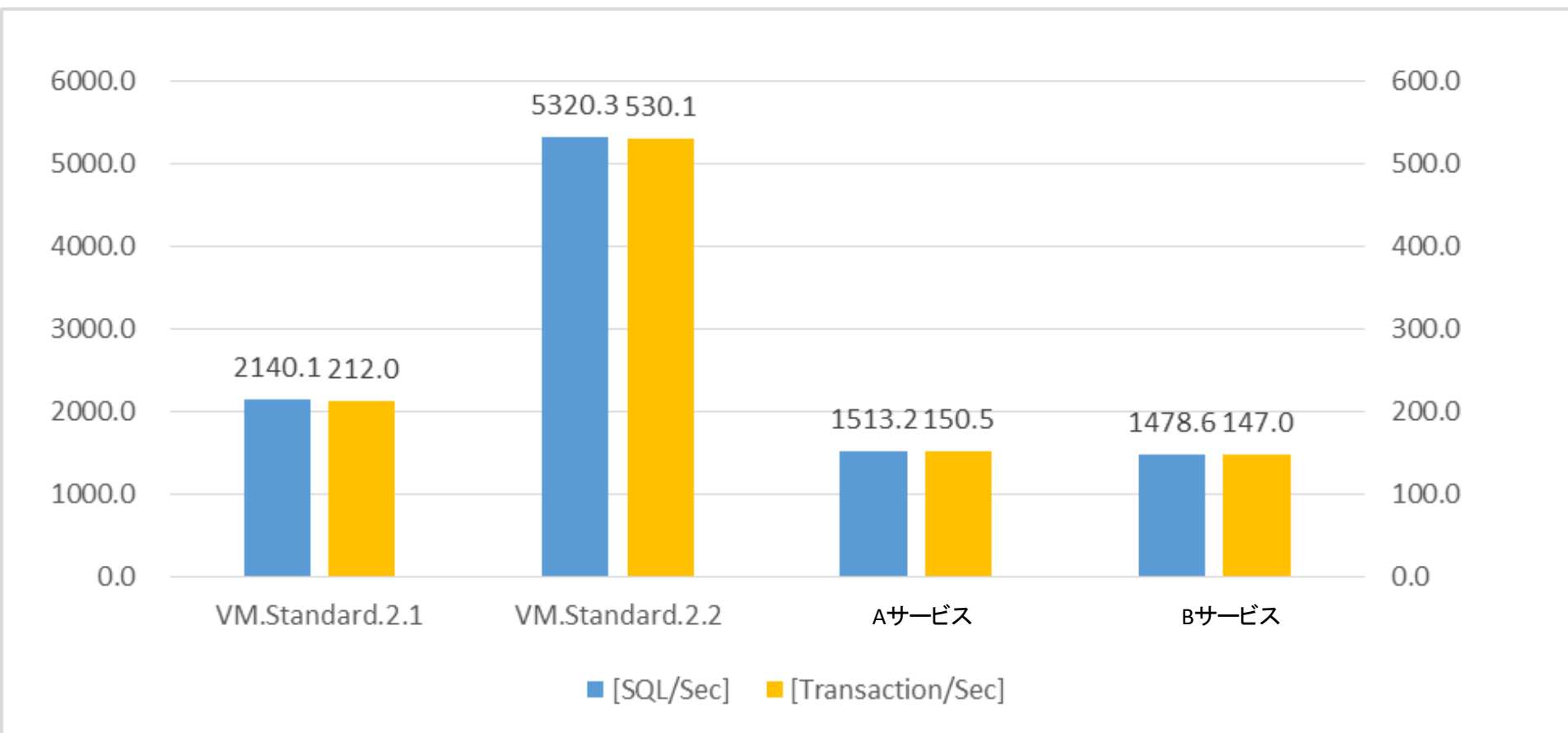


## AMSがクラウドに求める事③

データへの安定したクエリー性能  
(階層構造のため、グラフ型データに対応してほしい)



# SLOB※ を用いて Oracle データベース稼働環境のパフォーマンス評価

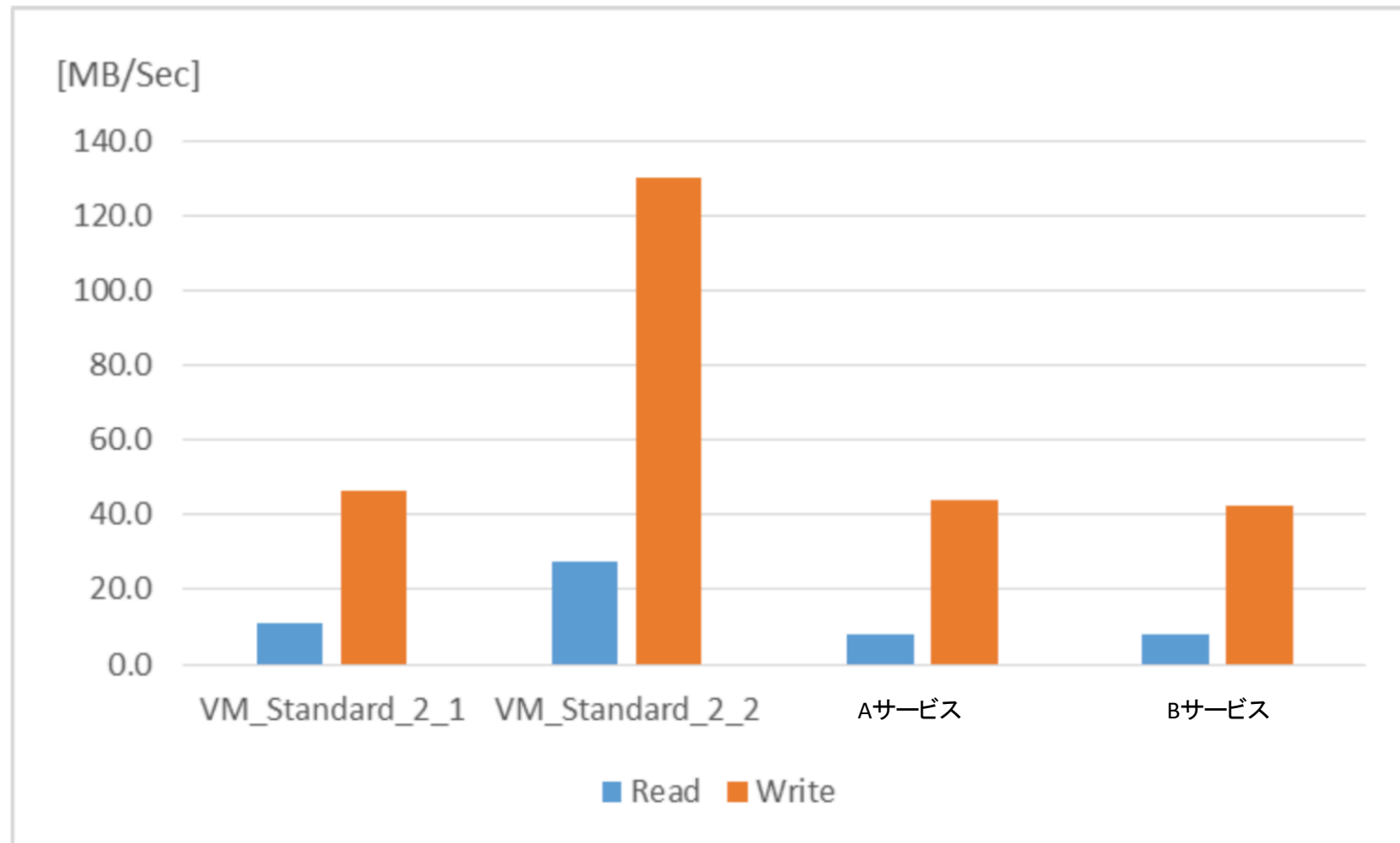


SQLExecute, Transaction のパフォーマンス

※ SLOB: 稼働状況のスナップショットをを利用した稼働環境のベンチマークツール



## SLOB※ を用いて Oracle データベース稼働環境のパフォーマンス評価



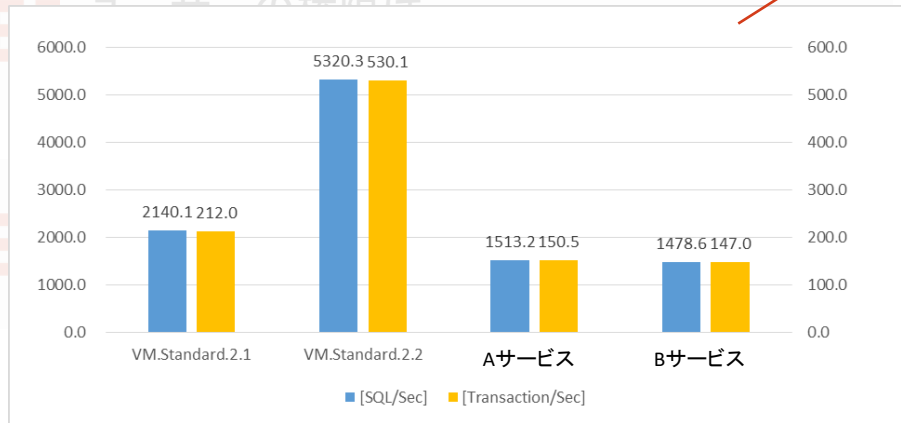
SLOB 実行時の I/O スループット

※ SLOB: 稼働状況のスナップショットをを利用した稼働環境のベンチマークツール

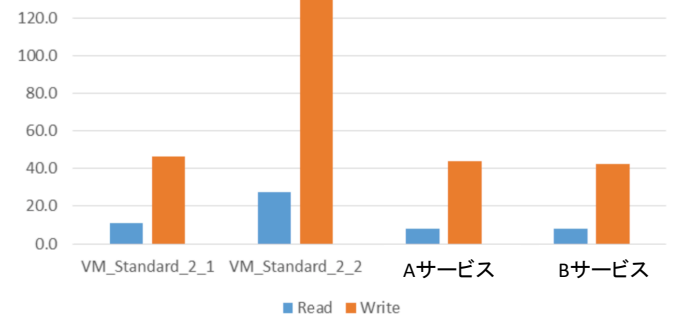


# Oracle Cloud Infrastructure 調査

## 1. データベースの性能を比較すると他のサービスを圧倒している



SQLExecute, Transaction のパフォーマンス



SLOB 実行時の I/O スループット

### AMSがクラウドに求める事③

データへの安定したクエリー性能  
(階層構造のため、グラフ型データに対応してほしい)

Oracle Database なら、グラフをサポートし、  
PGXが未来を見せてくれる！



# AMENIDY Suiteの技術的特徴



インフラ

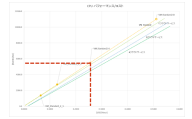
## AMSがクラウドに求める事①

大量の暗号計算を安定して  
可能とする演算性能

## AMSがクラウドに求める事②

スケールアウトした場合の  
コストパフォーマンス

安定した演算性能と  
コストパフォーマンス



加えて...

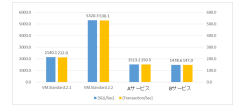
Outbound Data Transferは魅力的

データベース

## AMSがクラウドに求める事③

データへの安定したクエリー性能  
(階層構造のため、グラフ型データに対応してほしい)

確かなクエリー性能



加えて...

Autonomous Database活用で  
DBメンテナンス(コスト削減)に期待

BtoB向けで多数のユーザー、アクセス情報を安定して管理する基盤とし、  
そのデータを自律的にメンテ可能なデータベースを考慮すると  
Oracle Cloud Infrastructure上でのサービス構築が最適





# デモ **SECURITY**



## 権限の設定(デモ向け)

The screenshot displays the AMENIDY, Inc. interface with a sidebar on the left and a main content area on the right.

**Sidebar (Left):**

- 組織図 (Organizational Chart)
- ユーザー (User)
- ファイル (File)
- 設定 (Settings)

**Main Content Area (Right):**

The main content area is divided into two sections: "ファイルリスト" (File List) and "組織図" (Organizational Chart).

**ファイルリスト (File List):**

- サービス\_紹介資料.pptx
  - (株) amtwostech | x
- ビジネスエコシステム概観(案).xlsx
  - セキュリティ事業... | x
- ロードマップ.docx
  - (株) amtwostech | x

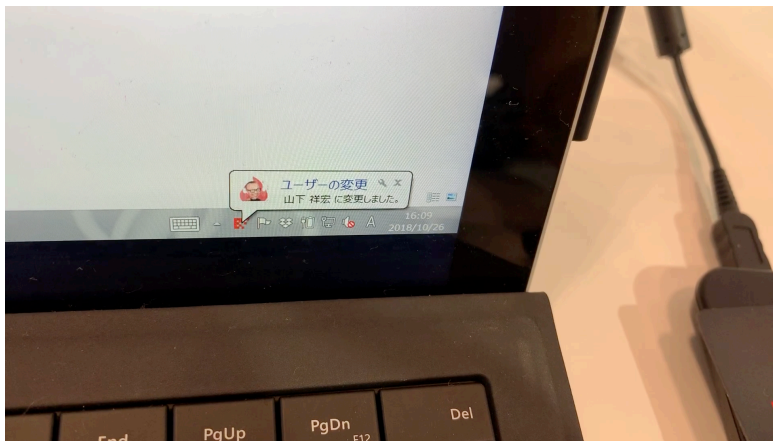
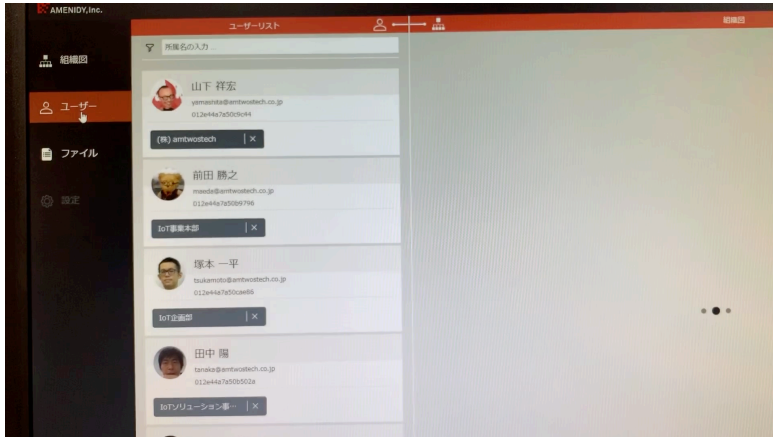
**組織図 (Organizational Chart):**

The organizational chart shows the hierarchy of the company:

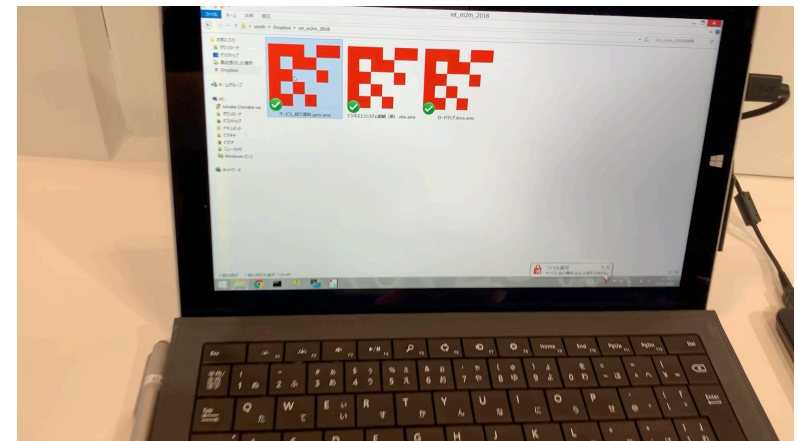
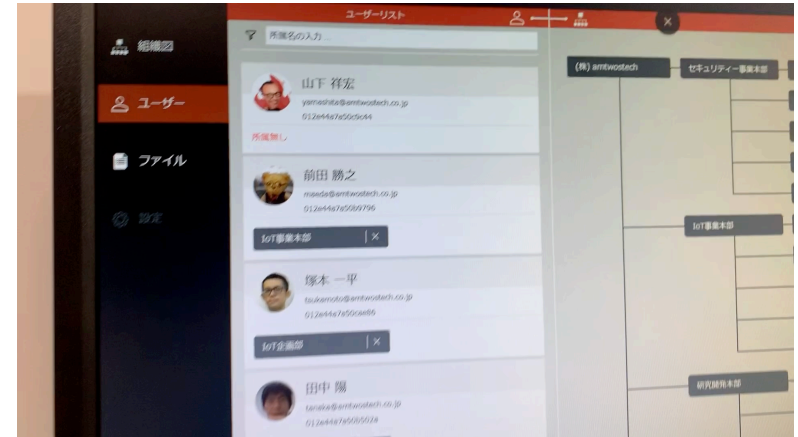
- (株) amtwostech
  - セキュリティ事業本部
    - コンサルティング事業部
    - 第一営業部
    - 第一開発部
    - 企画部
    - ソリューション事業部
  - IoT事業本部
    - IoTコンサル事業部
    - 第二営業部
    - 第二開発部
    - IoT企画部
    - IoTソリューション事業部
  - 研究開発本部
    - セキュリティ技術研究所
    - IoT技術研究所
    - AI技術研究所



## 権限をなくす



## 権限をつける





	事象	システム/サービス外観	要望とキーワード
1990年代	WWW登場	すべてのデータを集めて サーバーで処理  データを利用する主役は ユーザーであり、ユーザー の役割に応じた権限管理で システムを構築	すべての情報を どこでもやり取りできるように  WWW
	Windows95登場		
	Yahoo Japanサービス開始		すべての情報を安全にやり取りできる ように( <b>安全な通信</b> )  TLS  PKI基盤
	ECサイト続々オープン		
	企業業務のITC化		
2000年代	SSL、TLSなどが 安全な通信の規格が 標準化		個々の情報を どこでもやり取りできるように  スマホ  IoTデバイス
	スマホ登場 インターネットの急激な普及		
	ブロックチェーン登場		
2010年代	SNS拡大	様々な場所でデータが生成 される 情報は分散され、サービス も小さいサービスを組み合 わせて構築されるように  [世論] 個人情報の扱いなどにつ いて問題にあげられる  GAFAが大量の個人情報を 保持している事が 問題になる	個々の情報を安全にやり取りできる ように( <b>安全なデータ</b> )  ブロックチェーン (改ざん不可チェーン)  権限チェーン (情報閲覧権限チェーン)  認証チェーン (匿名での信頼チェーン)
	IoT ブーム		
	個人情報が特定の企業に集まる (GAFA)		
	AI ブーム		
	EU GDPR		
	全サイトHTTPS化		

安全な通信の上に流れるデータも管理する(ソフトウェアで安全を定義する)時代へ





Have a good trip  
with AMENIDY !