コンフィデンシャル・コンピューティング およびインテル® SGXについてのご紹介

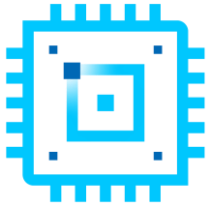
小佐原 大輔
インテル株式会社
新規事業推進本部

エンド・トゥ・エンドのデータ保護実現の為の最後の砦 ＝アプリケーション実行時のデータ保護

従来技術で保護が可能

保管時
データの暗号化による保護

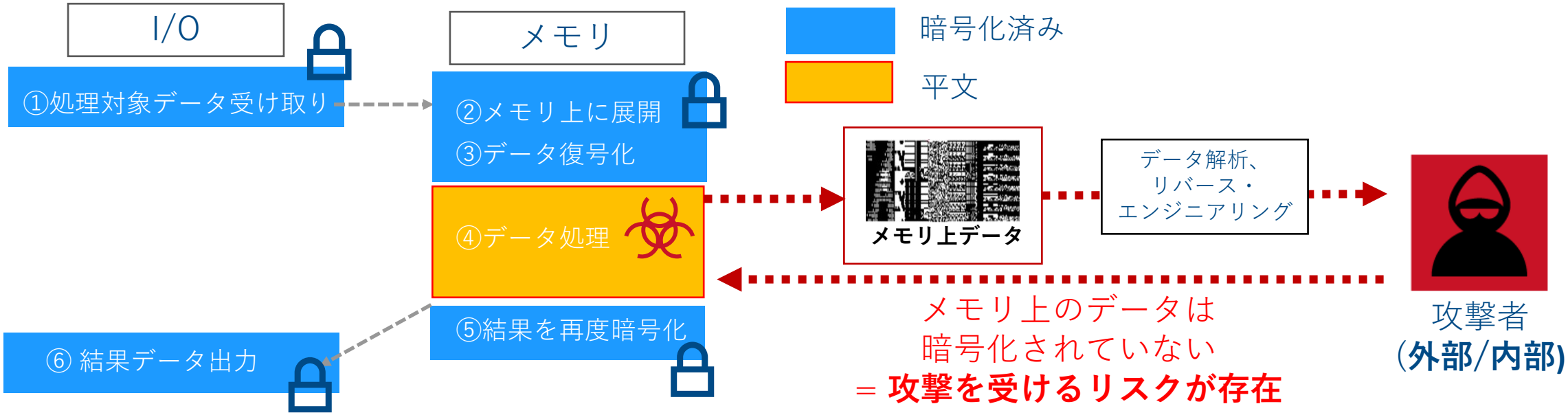
転送時
通信経路でのデータの暗号化
(例：SSL/TLS, IPsec 等



実行時
ソフトウェアがデータ処理時に
メモリ上に存在しているデータの保護

アプリケーション実行時のデータ保護が必要な理由

機密データを処理するときの一般的な流れ



メモリへの主な攻撃手法

- バッファオーバーフロー等といったソフトウェアの脆弱性を利用した権限昇格攻撃
- 不正に改ざん等された OS/仮想マシンモニタによるメモリダンプ
- コールドブート攻撃
- 権限を持つ内部のシステム管理者によるメモリダンプ

アプリケーション実行時のメモリ上のデータ保護が必要不可欠

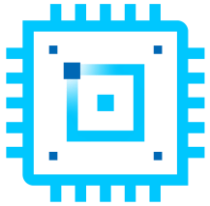
エンド・トゥ・エンドのデータ保護実現の為の最後の砦 ＝アプリケーション実行時のデータ保護

従来技術で保護が可能

保管時
データの暗号化による保護

転送時
通信経路でのデータの暗号化
(例：SSL/TLS, IPsec 等

秘密計算によって保護



実行時
ソフトウェアがデータ処理時に
メモリ上に存在しているデータの保護

秘密計算を実現するための主な手法

1. アーキテクチャ的な手法： 秘密分散(sMPC) など
2. メモリ上のデータを暗号化する手法
   2-1: **ソフトウェアによる手法**: 準同型暗号 など
   2-2: **ハードウェアによる手法**: **ハードウェア TEE** (通称：**コンフィデンシャル コンピューティング**), TME など
   - 主なハードウェア TEE 方式： インテル® SGX など

コンフィデンシャル・コンピューティング (HW TEE 技術)

プライバシー保護とセキュリティの技術革新

- **IT 業界全体での取組み**
  - コンフィデンシャル コンピューティング・コンソーシアムという様々なIT関連企業によって構成されているコンソーシアムによって推進
- **コンフィデンシャル コンピューティングの市場について**
  - 2026年までに最大 90-95% の年間成長率が見込まれる (Everest Group 調べ)

CONFIDENTIAL COMPUTING CONSORTIUM

参加企業

https://confidentialcomputing.io

プレミアム・メンバー

intel, Microsoft, accenture, Meta, 蚂蚁集团 ANT GROUP, Google, Red Hat, arm, HUAWEI

一般メンバー

AMD, anjuna, Anqlave, Baidu 百度, ByteDance, cosmian, decentriq, Fortanix, KINDITE, NVIDIA, OASIS LABS, swissCom, r3, Tencent 腾讯, vmware, iExec, and growing...

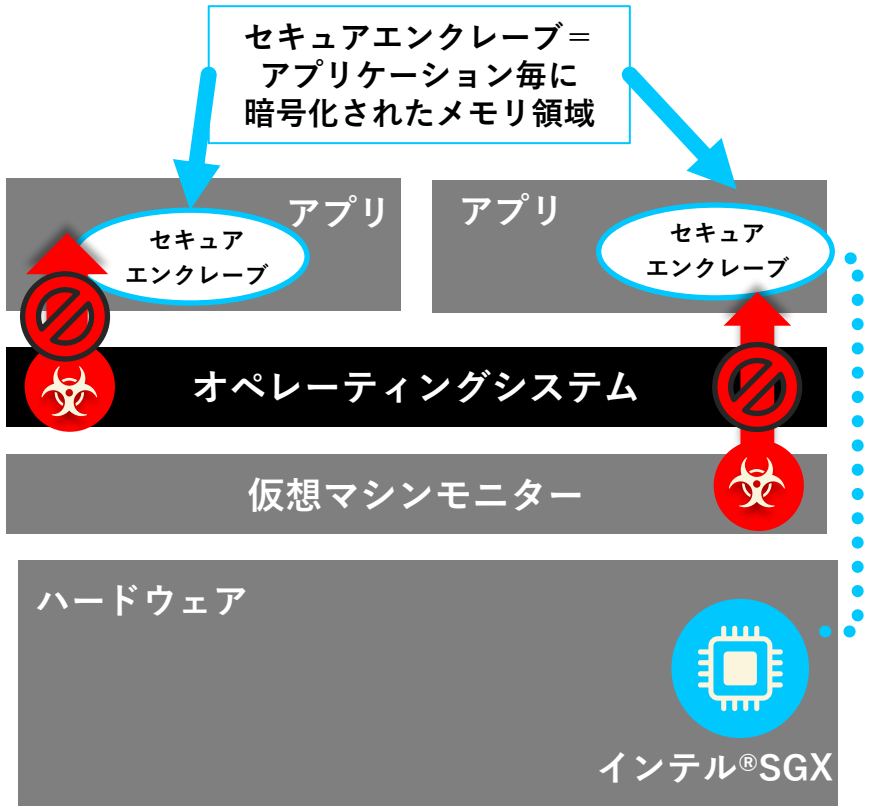
The CC market is poised for exponential growth

- The Total Addressable Market (TAM) for confidential computing in 2021 is **US$ 1.9-2.0 billion**
- The CC market is expected to grow at a **CAGR of 90-95%** in the best-case scenario and **40-45%** in the worst-case scenario through 2026
- Cyber risks, regulations, and avenues for incremental revenue position CC for hyper growth

出典：https://confidentialcomputing.io/wp-content/uploads/sites/85/2021/10/Everest_Group_-_Confidential_Computing_-_The_Next_Frontier_in_Data_Security_-_2021-10-19.pdf

インテル® ソフトウェア・ガード・エクステンションズ (通称：インテル® SGX)

コンフィデンシャル コンピューティングを実現する技術(**HW TEE**)のひとつ
アプリケーション毎に隔離、暗号化されたメモリ領域を作成



- **ソフトウェア攻撃からの保護**
  OSや、デバイスドライバ、BIOS や VMM 等が危険に晒された状態でも、アプリケーションのデータを保護可能
- **より強固な秘密保護**
  攻撃者がシステム全体のコントロールを持っている状態でも有効
- **様々なメモリ攻撃からの防御**
  メモリバススニーピング、メモリタンパリング、コールドブート攻撃への耐性
- **ハードウェアベースの認証(アテステーション) を提供**
  TEE の適切さ(CPU の真贋性、FW の状態)と、エンクレーブ上で動作するコードの改ざんが無いことを検証

他の HW TEE 技術では権限付きソフトウェアによって攻撃を受けてしまうリスクが存在

最小サイズのトラステッド・コンピューティング・ベース (TCB: 攻撃可能領域) を実現

防御が難しい領域や攻撃手法からのデータ保護を強化

透明性の確保、
説明責任の徹底

主な HW TEE の実装方式

メモリの隔離を実現する技術はインテル® SGX 以外でも存在

PROTECT THE DATA
IN-USE

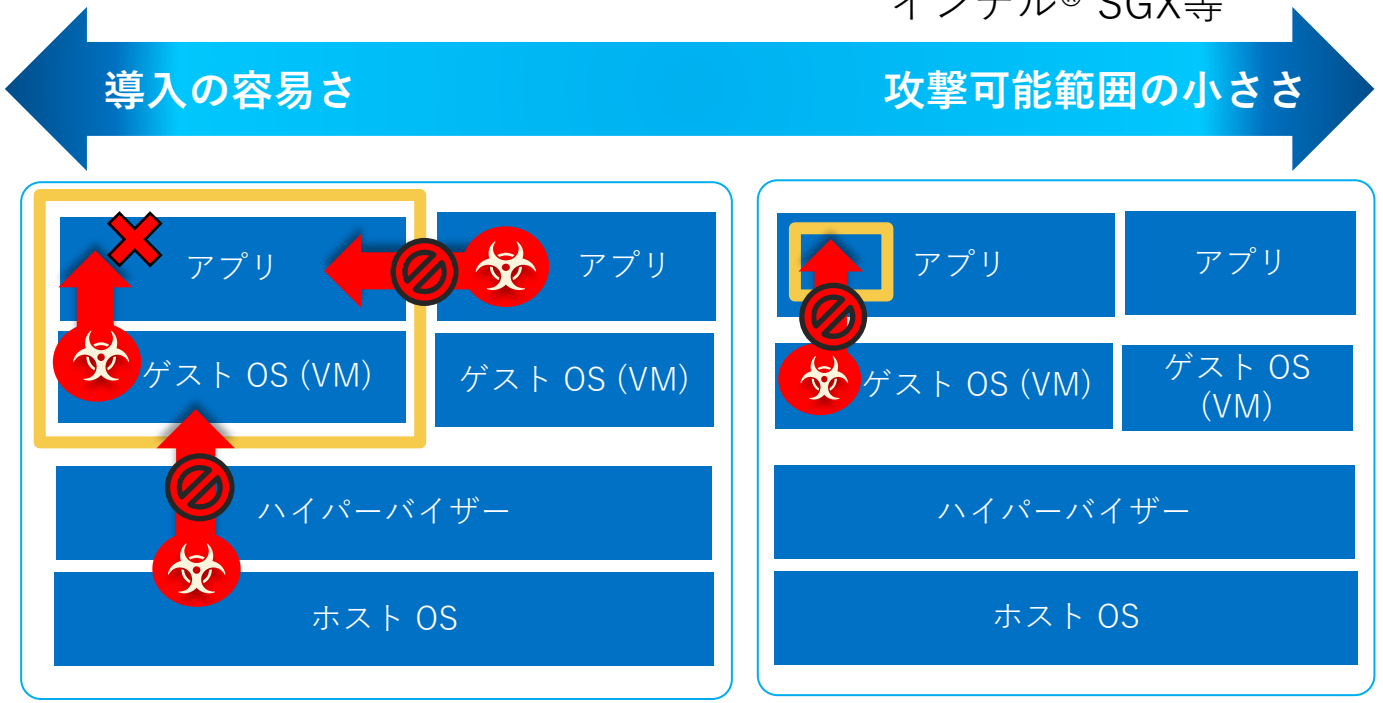
隔離されている領域

VM 単位の隔離

インテル® TDX
AMD SEV-SNP 等

アプリケーション単位の隔離

インテル® SGX等



メリット：導入の容易さ
アプリケーション・コードの改変が不要なため手軽に導入できる

主な利用用途：
クラウドでのテナント隔離
クラウド事業者やハードウェアを共有しているほかのテナントから、自分の仮想マシン上のメモリを秘匿化できる

防げない脅威：OS からのアプリのメモリへのアクセス

- ゲスト OS の脆弱性を利用した攻撃
- ゲスト OS 管理者からのアクセス

等

メリット：セキュリティの強固さ

VM単位の隔離で防げない攻撃(OSの脆弱性を利用した攻撃や、OS管理者からの不正アクセス)を防ぐことが可能

主な利用用途：内部関係者/パートナーに対しても処理中のデータを秘匿したいケース

例： 秘密鍵の管理、ブロックチェーン、顧客プライバシー情報等の処理、電子投票、連合学習、マルチ・パーティ計算　等

インテルのサーバー向けCPUにおける SGX 拡張の歴史

EPC: Enclave Page Cache = SGX で隔離可能なメモリ

Intel® Xeon® E3
128MB EPC

Intel® SGX カード
3 x 128MB EPC

Intel® Xeon® E
2000 シリーズ
256MB EPC

SGX2 世代

第3世代 Intel® Xeon® SP
1 CPU あたり最大
512GB のEPC

2018 2019 2020 2021

現在

世代が進むことによってより大きなサイズのメモリの隔離が可能
＝AIやML 等メモリを大量消費する用途への適用も容易に

インテル® SGX ：多様なパートナーからのサポート[1,2]

ソリューション & サービス

Fortanix, CONSILIENT, decentriq, LayerX Labs, Microsoft SQL Server, r3, SAP, Aggregion, secretarium, Riddle & Code, enigma, ERICSSON, intellect EU, eperi (Your Key to your Cloud Data Protection), VENAFI, anjuna, secunet, TALIUM, MADANA, HYPERLEDGER FABRIC, SILENTDATA, (ONE)FACTOR, ARMO, cosmian, NEC, CYSEC, iExec, Anqlave, accenture, LOCKHEED MARTIN, edgeless systems, T-Systems, ami (power • manage • secure), appliedblockchain, edgeless systems, CYBERNETICA

開発環境

Microsoft Open Enclave SDK, Fortanix Enclave Development Platform (EDP), intel SGX, Baidu 百度 RUST-SGX, r3, edgeless systems

クラウド・サービス・プロバイダー

Microsoft Azure, IBM Cloud, swisscom, Alibaba Cloud, EQUINIX, OVHcloud, PhoenixNAP SecuredCloud, 百度网盘, G-CORE LABS, QCT

OS / VMM

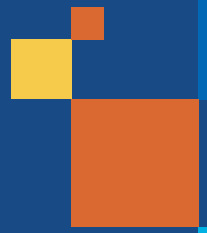
vmware, Microsoft, Red Hat, CentOS, ubuntu, SUSE

ランタイム環境

Occlum (Empowering everyone to run every app in enclaves), GRAPHENE, SCONTAIN, Fortanix, SGX-LKL

1 . Not an exhaustive list; ecosystem is growing all the time. 2. Majority in production; see vendors for specific readiness timelines.

インテル® SGX のユースケース



intel®

インテル® SGX の主な利用シーン

クラウド環境
マルチテナントなパブリッククラウド環境でのデータ保護を実現

機械学習
顧客のプライバシー情報や自社が持つIP情報等の秘匿性を担保した状態での機械学習処理を実現

連合学習
分散された環境にてデータを集約せずに機械学習を実行。学習アルゴリズムと処理データの秘匿性を担保

セキュアな鍵管理
従来専用 HW で実現をしていた HSM の機能を汎用サーバー上で実現。より柔軟かつスケーラブルな分散アーキテクチャでの鍵管理を実現

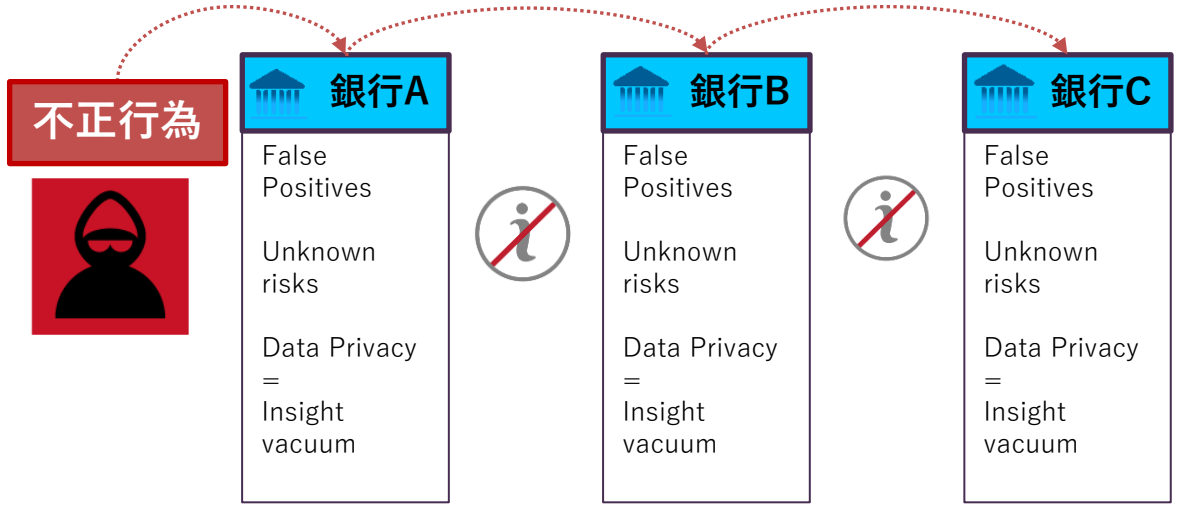
ブロックチェーン
オフチェーン処理の秘匿化、改ざん防止(あてステーション機能を利用) など

マルチパーティー計算
100%の信頼が担保されない相手とのデータ連携をセキュアに実現

インテル® SGX の 金融向けユースケース

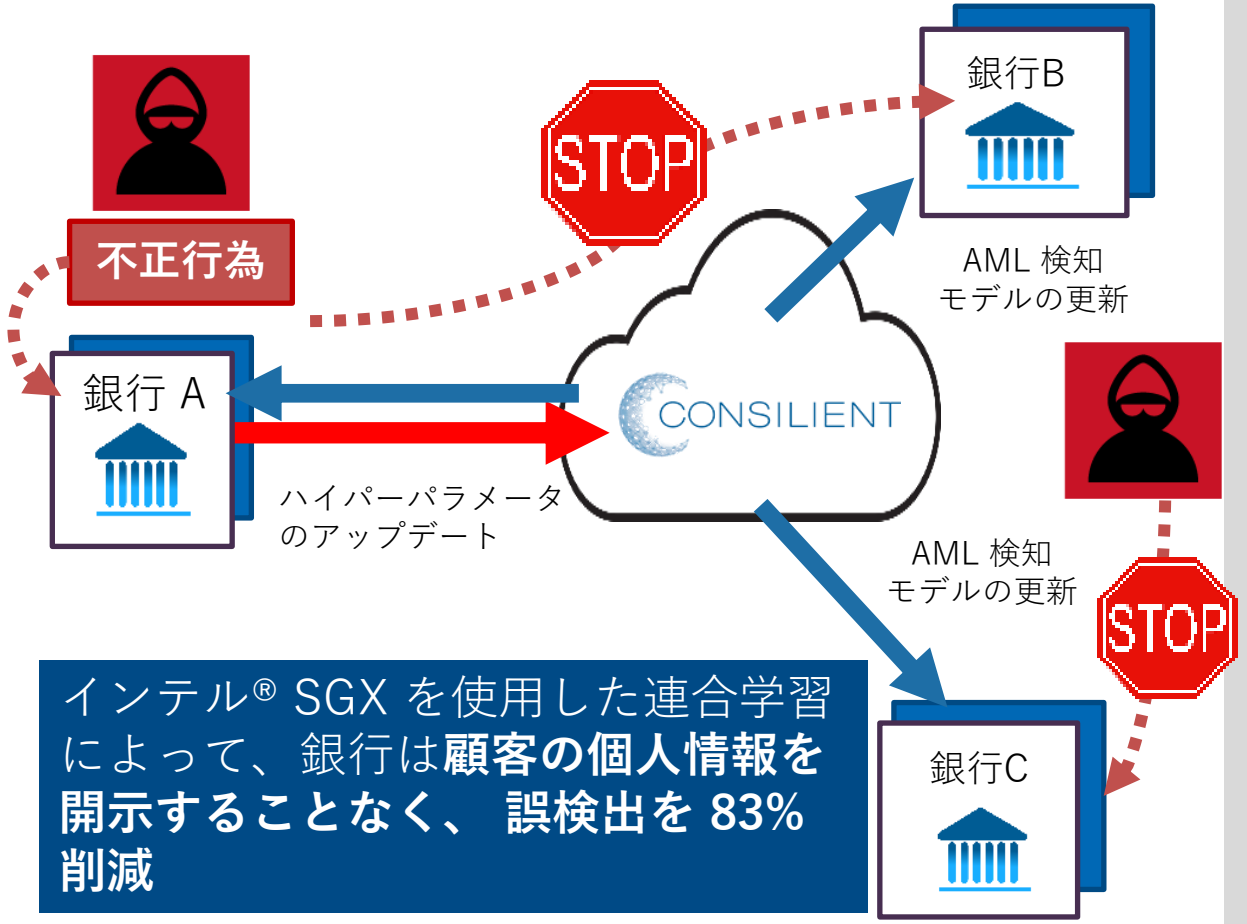
連合学習によるマネーロンダリングおよびテロ資金対策手法

現在の対策手法



- 現状のAML/CFT システムのトランザクション監視によって生成されるアラートのうち、95% 以上は誤検知[1]
- 不正検知の為の機械学習では高度な秘匿データを取り扱うため、複数銀行間でのデータ連携を行っての機械学習をとることが難しく、複数の銀行で同様の手口を実行されてしまう

Consilient の連合学習によるアプローチ

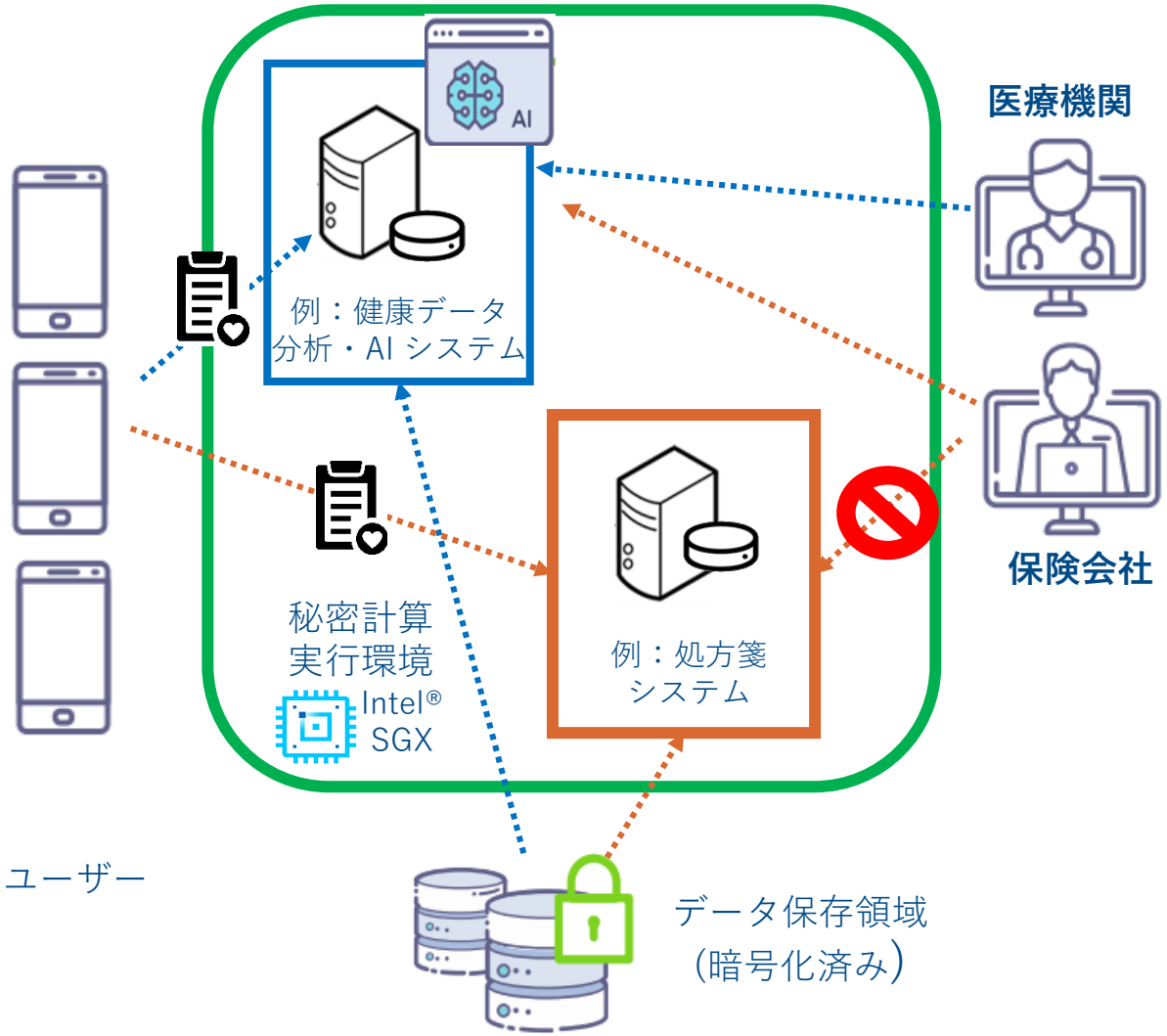


インテル® SGX を使用した連合学習によって、銀行は**顧客の個人情報を開示することなく、 誤検出を 83% 削減**

[1] 参照元: https://www.unodc.org/unodc/en/money-laundering/globalization.html

Intel® SGX の ヘルスケア向けユースケース

ドイツでの電子健康記録（eHR）データの利活用



背景：

ドイツでは患者の所見、 診断、治療方法、治療手段、治療報告書、予防接種などのデータは電子健康記録(eHR)に保存されている

そのような eHR データをセキュアに利活用できるシステムをインテル® SGX 上で実装

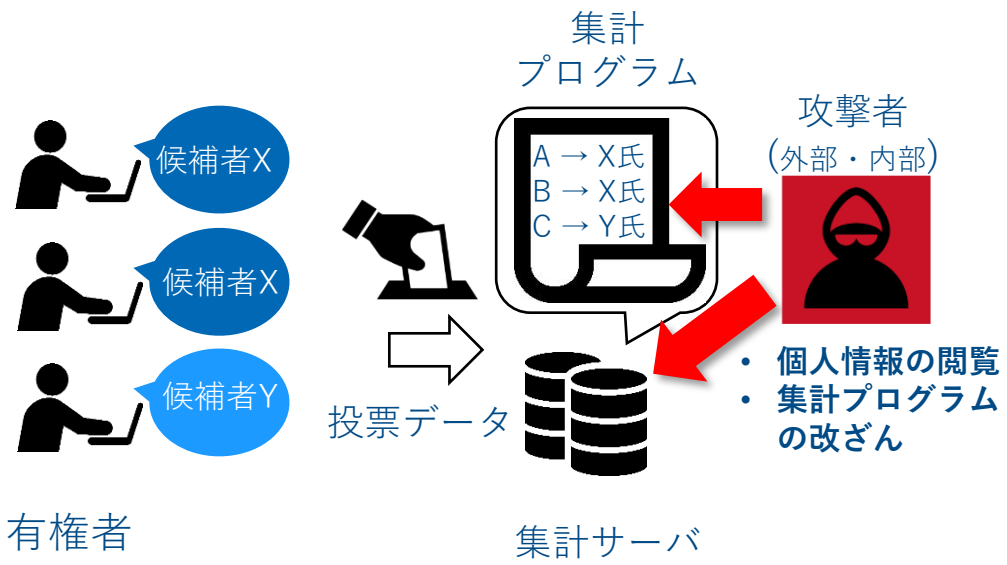
- 目的：より優れた医療、保険の提供
- 秘密計算環境には認められた医療機関、保険会社のみがアクセス可能だが、参加者にも計算途中のデータ(患者のプライバシー情報など)は取得できない
- データ利用にあたってはユーザの同意が必須

現在の状況

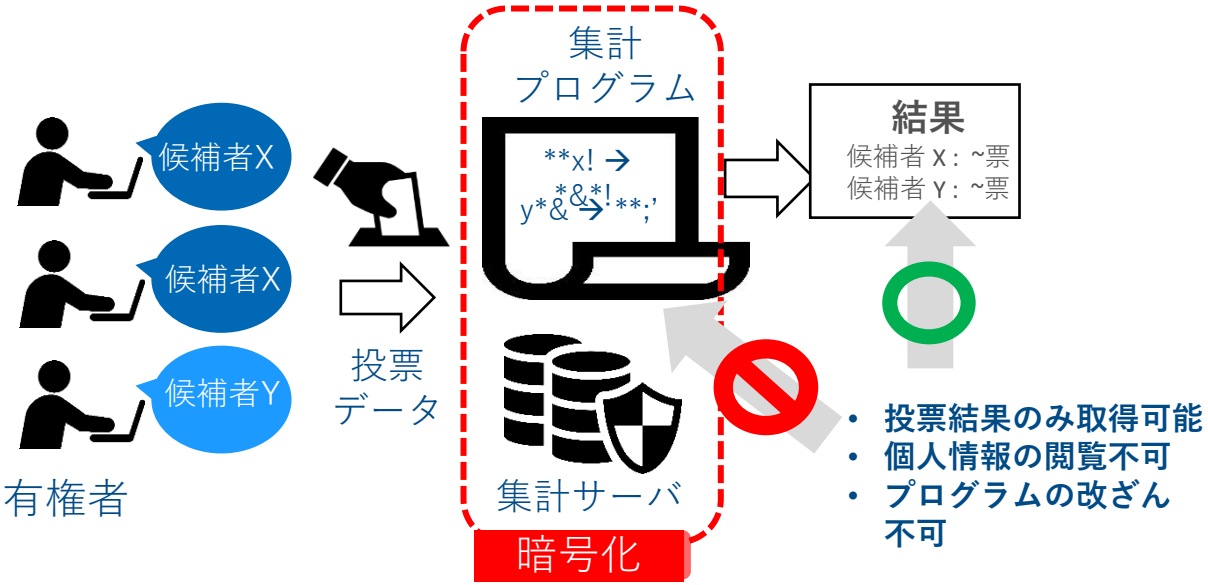
- 2021年1月より運用開始：7500万人の被保険者の電子健康記録を実装
- 5つの医療保険会社が参加 (2300万人をカバー)
- 既に 100万人のユーザが利用
- 2021年7月より、電子処方箋システムの運用を秘密計算実行環境で実装 – 年間 8億件の医薬品取引を想定

日本国内でのインテル® SGX のユースケース

インターネット投票システム実証実験 （LayerX 様事例）



Anonify・SGX<u>なし</u>の場合



Anonify・SGX<u>あり</u>の場合

- 株式会社LayerX 様が提供する、Intel™ SGXを活用した秘匿化ソリューションである「Anonify」を活用した電子投票システムの実証実験
- 将来のインターネット投票を見据え、高い秘匿性と非改ざん性を備えた市民意見収集システムをつくば市で実証(協力会社：株式会社VOTE FOR様、株式会社LayerX様)

まとめ

- コンフィデンシャル・コンピューティング(HW TEE) およびインテル® SGX のご紹介
  - コンフィデンシャル・コンピューティングはIT業界全体での取り組みで、今後大きな市場の成長が見込まれている
  - インテル® SGX ：最も歴史と実績のある HW TEE 技術
    - アプリケーション単位の隔離を実現している技術で、VM単位の実装と比較して強固なセキュリティを提供
    - SGX 対応プロセッサの進化により、より高速に、より多様な用途にも対応
    - 数々の導入実績と様々なパートナー様からのソリューションが提供済み。
      代表的な例として
      - いますぐにインテル® SGX を使えるクラウド環境としてのマイクロソフト様の
        「**Azure Confidential Computing**」 → この後のマイクロソフト 佐藤様のセッション
      - SGX に対応したソフトウェアを簡単に開発するためのソリューションとしての
        「**Conclave**」 → この後の SBI R3 堀田様のセッション


intel