

Acompany

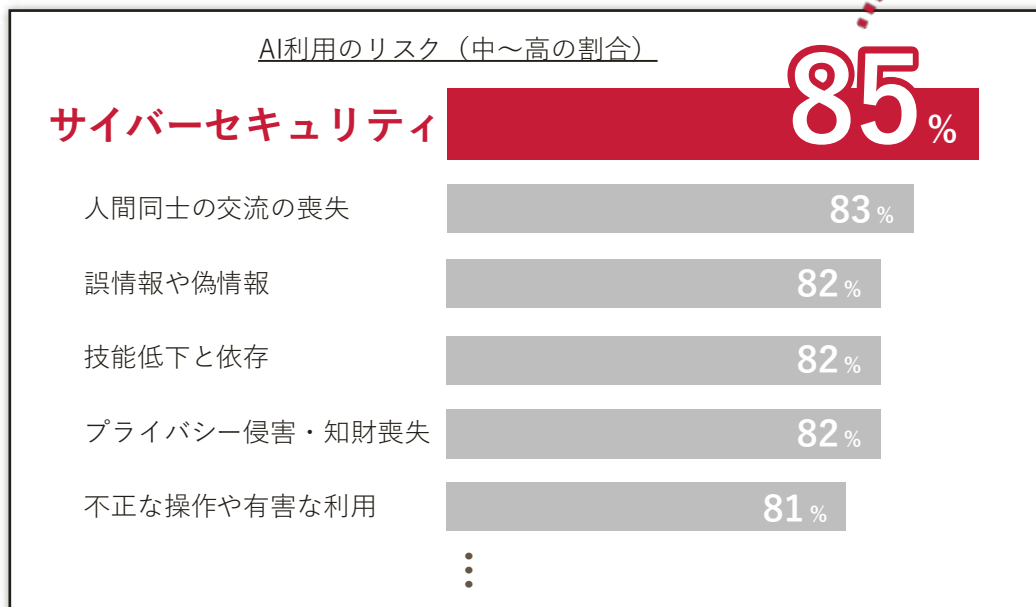
機密情報ですら安全に活用可能にする 次世代の安全性を有するAIサービス

株式会社 Acompany

セキュリティはAI推進における最大のボトルネック

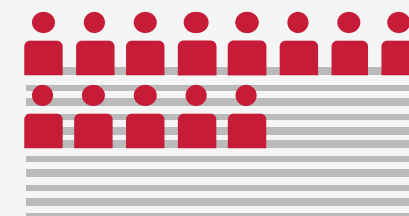
AI・データ活用による社会的インパクトは大きいですが、情報漏洩がリスク

セキュリティが最大のAI阻害要因



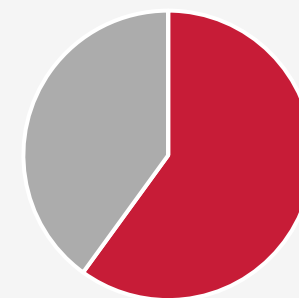
汎用AIは業務知見が不足

48% の従業員が機密データを外部AIに



マスキングの手間と人的ミス

60% が人的要因のインシデント



「安全で秘密を守れるAI」で、 生成AIの「機密データ入力禁止」を過去に変える



複数のLLMモデルを
シームレスに切り替えできる



機密/個人情報をAIによって
自動的に無害化できる



すべてのAI利用ログを記録し
ダッシュボードで監査できる



Acompany Secure Chat

新しいチャット

機密情報保護ウィザード

プレビュー 各項目をクリックしてマスキング適用を切り替え すべてマスキングを適用

マスキング後

以下のメールを要約してください

件名: 【機密】Q4売上報告書とクライアント契約更新について - 至急確認要

田中 PERSON_1806496bcb753c28 様

お疲れ様です。営業部 I I G E I H E I H I L N C C C N D D D M D M D N D N の長谷部 PERSON_0b8acbc8ff7418f3 です。

第4半期の売上実績がまとまりましたので、ご報告いたします。今期の総売上は1億5000万円となり、前年同期比105%を達成しました。

主要クライアントの契約更新状況は以下の通りです:

- Acompany Inc ORGANIZATION_16e95757bb8fcf01

担当者: 佐藤健一 PERSON_c35c7d6506bc47ff 様 (携帯: 090-1234-5678 PHONE_522d69851a96e960)

キャンセル

設定

ChatGPT Gemini Claude Grok LLaMA Qwen

Gemini 3 Flash

安全機能と使い勝手に加え、「コストメリット」を実現

- 複数の最新モデルを即座に利用可能な自動マスキング機能付きチャットサービス
- 個別AIサービスへの契約不要のため、コストを抑えながらも利便性と安全性を実現したAI活用が可能



複数のLLMモデルをシームレスに切り替えできる

機密/個人情報をAIによって自動的に無害化できる

すべてのAI利用ログを記録しダッシュボードで監査できる

利用するAI例



5,500円/人

4,500円/人

55~64%の
コストダウン

2,000円/人

※ChatGPT Plus + Claude Pro

※Copilot for Microsoft365

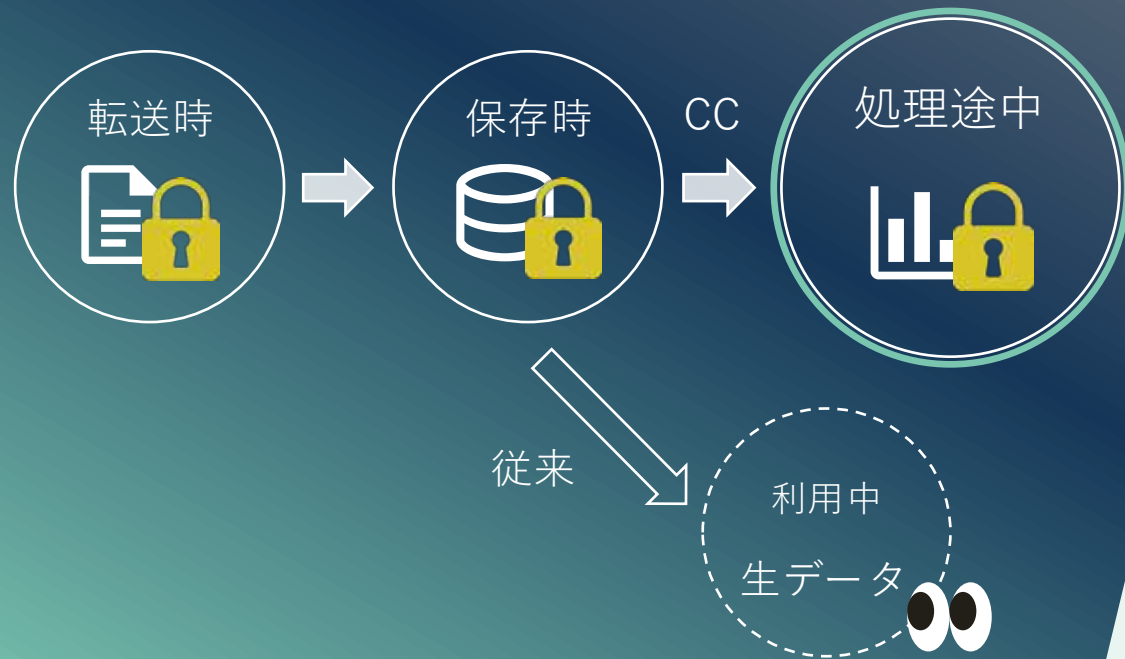


コア技術：Confidential Computing（秘密計算）

例えば、Acompanyですら中身を見ることができない強固な金庫の中でデータ処理を実現する技術

コア技術：Confidential Computing（CC）

全プロセスを暗号で保護したままデータ処理が可能



世界水準での研究開発を実現

Intelとの共同研究



自社特許
(申請中)

Securing Nested Attestation of Confidential Serverless Computing without Intra-Enclave Isolation

Atsuki Momose
Acompany Co., Ltd.
atsuki.momose@acompany-ac.com

Ao Sakurai
Acompany Co., Ltd.
ao.sakurai@acompany-ac.com

Kailun Qin
Intel & Shanghai Jiao Tong University
kailun.qin@intel.com

Mona Vij
Intel Labs
mona.vij@intel.com

ABSTRACT

Confidential Computing-as-a-Service has gained significant attention in recent years, driven by rapid advances in Trusted Execution Environment (TEE) technology. Among various architectures, confidential serverless computing has emerged as a promising model. A common approach to designing confidential serverless computing involves decoupling the client workload from the initial enclave image and dynamically provisioning the workload at runtime. This enables both offloading the costly enclave bootstrapping and maintaining a fixed reference measurement for attestation. This decoupling necessitates nested attestation, where the client's workload is attested via a custom attestation module embedded in a platform-attested enclave established at boot time. The challenge in designing nested attestation, however, is to distinguish fresh

1 INTRODUCTION

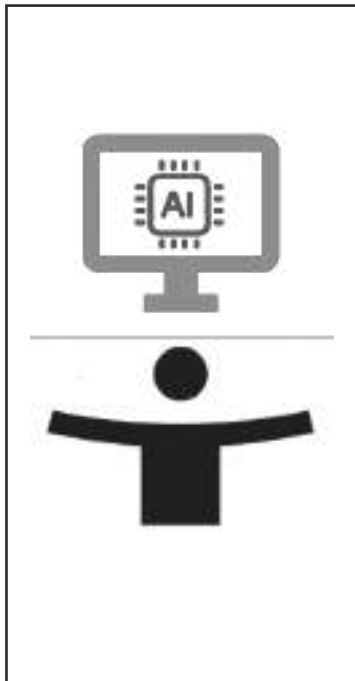
Confidential Computing-as-a-Service (CCaaS) [7, 44] is a form of cloud service model where the cloud service provider (CSP) offers secure enclaves, typically backed by hardware-assisted Trusted Execution Environment (TEE) technology, allowing users to run workloads in an isolated execution environment that remains protected from system software, hypervisors, and even cloud administrators. Common TEE technologies include Intel SGX [11, 24] and Intel TDX [17], AMD SEV [3], and ARM CCA [24]. These technologies typically provide tamper-proof attestation features, allowing remote clients to verify both the hardware specifications and the exact software running within the enclave. This ensures remote clients can securely execute their workloads even against a potentially malicious CSP.

Confidential AIを含む2つのプランでニーズを実現

「AIによる自動無害化」と、追加オプションで「秘密計算環境での丸ごと保護」も実現



AI利用企業



目指すのConfidential Computingのプラットフォーマー

「SaaS」だけでなく「PaaS (Platform as a Service)」へと展開する



SAM

Acompany
セキュアチャット
Confidential 生成AI SaaS

2,232億円

今

2026

2032

TAM

Confidential Computing
プラットフォーム

52.5兆円

(Fortune business insights 2032年予想)

事例

△company

高い技術レベルを求められる領域での実績を有する

KDDI様と業務提携

防衛プロジェクトの受注

KDDI

約4,000万人データを
安全にAI利活用へ

詳細非公開

事業化の加速

日本代表として世界大会へ出場し、10傑入り
世界30,000社からTOP10へ

年間平均契約額（上位3社）

4,830万円

年間平均契約額（全体）
2,560万円+

収益源

- ・ライセンス提供
- ・導入サポート

KDDI TOPPAN

AISIN **関西電力**

HakuhodoDY holdings
など

資金調達額

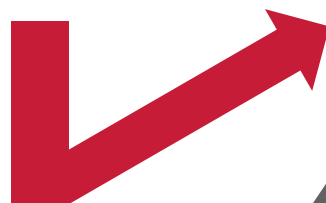
21億円

世界
6位
★★★

東京予選優勝



日本代表



スタートアップワールドカップ 2025

@サンフランシスコ



卓越したメンバーが集まる本領域の国内トップチーム

代表

業界団体会長も務め 市場を作る

#プライバシーテック協会会長
#アジアを代表する30代未満の30人

Forbes
Asia



代表取締役 CEO
高橋 亮佑

政策/法律

Confidential Computing (秘密計算)の第一人者

#デジタル庁 データセキュリティWG委員
#OECD国際会議にて日本代表として提言



執行役員 VP of Public Affairs
竹之内 隆夫

卓越したチームメンバー

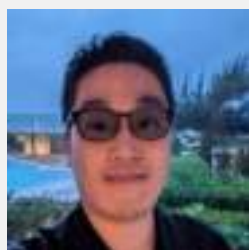
AIセキュリティ・プライバシーの
世界トップ研究者



プリンシパルリサーチャー
高橋 翼



Confidential Computingの
国内トップ技術者



シニアリサーチャー
櫻井 碧



株主 & アドバイザー

日本を代表する 経営コンサルタント

#元BCG日本代表



元BCG 日本代表
杉田 浩章

他メンバー出身例

