2507ConfidentialComp.pdf
2025.7 ブログ：「Confidential（機密）Computing の概要と動向」を読んで、の詳細
（→ http://www.1968start.com/M/blog/index4.html#2507 ）

「Confidential（機密）Computing の概要と動向」を読んで

中所武司

■このエッセイのきっかけ
情報処理学会誌の最新号の下記の解説論文について、個人情報保護の観点で読んでみた。

・情報処理 Vol.66 No.7 (July 2025) p.e1-e7
特集：AI 時代の安全なデータ処理「Confidential Computing」
Confidential Computing の概要と動向
-AI 時代に急速に普及する機密コンピューティング-

■内容の要約とコメント（→★）

Confidential Computing の普及

・近年の生成 AI の活用進展に伴い，データを秘匿したまま処理できる技術として「Confidential Computing」（以下，CC）や TEE（Trusted Execution Environment）が注目されている．

・すでに Apple の iPhone では，この技術が適用されている．生成 AI の処理は重たく，一部の処理は iPhone 端末内では処理が間に合わないため，プライバシーにかかわる機密情報を暗号化してサーバーに送り，サーバーでも秘匿化された状態で処理する．サーバーのデータは Apple にも見られず，利用者は安心して生成 AI を利用できる．

→★分野は異なるが、小生の下記の特許では、電子文書の公平な公開を必要とする場合，システム内に保存された電子文書が、将来の指定時刻まで，**システム管理者などの内部の関与者からも閲覧ができないことを保証する**ことを特徴としている．

（参考）特許：時刻認証方法：特許番号＜3577704 3572576＞ 登録日：2004.7
https://www.1968start.com/M/patent/index.html
https://www.1968start.com/M/patent/comment.html

・プライバシーを重視する Apple がこの技術を大規模に採用したことで，この技術の普及が確固たるものになった．

・Web ページの通信に HTTP でなく暗号化された HTTPS を使うのが普通になったように，今後はほぼすべての処理が CC で処理されるようになる．

→★私のホームページは昨年 4 月に HTTPS 化済み

・本稿では，実務者や初学者に本技術について、データ活用・連携の重要性を説明し、
この技術を解説し，市場動向や国内外の事例を紹介する．
個人情報保護法や安全保障関係との関係についても説明する．

CC の普及の背景・期待

企業間データ連携の実現

・AI の進展によりデータが重要となる中，一部の巨大企業は戦略的にデータを収集し、
活用する一方，一般の企業の今後の成長戦略は，データの囲い込みではなく，
データの連携と言われている．

・しかしデータが競争力の源泉である以上，データを容易に外部に出すことは難しい．
データを出さずに企業間で連携するという要件を満たせる技術の 1 つが，CC である．

Confidential AI の実現

・さらに期待されるのが AI を機密性高く安全に実行する Confidential AI である．
機密性が高いデータを生成 AI に入力して，活用するニーズが高まっているが，
処理が重いので，PC やモバイル端末ではなく、サーバーの GPU での処理が期待される．
しかし，特にクラウドでの処理はデータの安全管理が問題なので，GPU にも対応する
CC が期待されている．

→★サーバにある個人情報をサーバの管理者から秘匿する技術は重要と思う。
これは、私がクラウドを個人情報の保管用に利用していない理由である。

CC/TEE の技術概要

CC/TEE とは

・CC は，ハードウェアを用いた TEE と呼ばれる安全な実行環境で処理され，
以下の 2 点の特徴がある．
- 処理途中のデータを暗号化などして秘匿化したまま処理できる
- 処理が正しく動いていることを確認（リモートアテステーション）できる

処理中のデータの保護

・一般的なコンピュータ処理では，メモリ内のデータや処理途中のデータは保護されず、
コンピュータウイルスなどに管理権限を奪取され，メモリ内や処理中のデータが
不正者に盗まれる恐れがある．

→★かつて、私も共用のコピー機やプリンタからの情報漏洩を心配したことがある。
また、昭和の時代の写真屋へのフィルムの現像、焼き増し依頼などを思い出す。

・CC を用いたシステムでは，暗号化されたデータも処理回路では復号された生データで
処理されるため，「暗号化したまま処理する」という表現は若干誤解を生む．
管理権限を持つ不正者にメモリ内を見られてしまうリスクは一定程度あり，
そのリスクや影響度などに対する CC の導入コストなどを勘案した判断が望ましい．

リモートアテステーション

・もう１つの特徴が「Remote Attestation（リモートアテステーション）」である．
これは，CC の TEE 実行されるコードが，事前に認証された安全なものであることを第三者が検証できる仕組みで、以下のような流れで実施される：

1. 事前に，コードのハッシュ値を保存
2. 実行時に TEE から，ハードウェア製造企業の電子署名付きのハッシュ値を取得
3. それを比較・検証することで安全性を確認

→★以前、アプリの中に余計なコードを作りこみ、特定条件で実行させる犯罪があった。
この検証方法なら、実行コードのローディング後にパッチをあてるのも検出可能？

CC が満たす性質と価値

・上記のような特徴は技術的には以下のような性質を満たすと表現される．
- データの機密性（Data Confidentiality）
- データの完全性（Data Integrity）
- コードの完全性（Code Integrity）

・つまり、処理中のデータは，OS の管理権限を保有する不正者でも，閲覧ができず，データの改ざんも防ぎ，実行時には処理コードが改ざんされてないことを確かめられ，データを不正にどこかに送信するなどもできないのである．

→★現在、ブラウザを利用して何かを検索すると、その直後から、関連するバナー広告がブラウザに表示される。この機能を適用すれば、検索に関する「データの機密性」が守られ、このようなバナー広告を防げるのだが・・・。

・この特徴により，複数の企業が持つ機密データや個人情報を開示して流通せずに，データを連携して分析した結果であるデータの価値だけを流通させることもできる．

さまざまな TEE と安全性

・TEE は，Intel、AMD、NVIDIA などがチップを提供しており，Microsoft Azure や GoogleCloud Computing や Amazon Web Service などが関連する機能を提供している．
これらの TEE は TCB（Trusted Computing Base）と言われる，

秘匿したまま処理できる「秘密計算」との関係

・CC は日本では「秘密計算」の一種とも分類される．秘密計算は，処理中のデータを秘匿化したまま処理する技術の総称である．実現方法は，CC のようにハードウェアを用いた方式もあれば，ソフトウェア的に実現する方式も存在する．

・ソフトウェア的に実現する方式の代表的なものは，鍵で暗号化したまま処理したり，秘密分散という手法を用いたりして，暗号化／秘匿化したまま処理する技術である．

・CC は，安全性がハードウェアのメーカーに依存することや，サイドチャネル攻撃（例：処理時間の若干の差から秘密情報を推測する）には対応していないため，ソフトウェア型の秘密計算と比較して，安全性についての注意が指摘される．

GPU 対応の CC
・AI 処理を CC で行いたいという需要があり，現在は GPU も CC に対応している．

CC の市場規模予測
・CC の市場調査では，年平均の市場成長率は約 50%という結果になっている．

CC の事例

海外の事例
・最も象徴的な Apple の事例で、Secure Enclave という TEE が導入され，
TEE 動作するソースコードが一部開示され、暗号研究者が安全性の検証なども行える．

・Google も TEE の処理環境を提供し，組織間で突合分析する広告分析に適用．
Amazon も広告分析の環境に Nitro Enclave という技術を適用．
米国海軍は 2024 年 5 月に軍事用 AI の演算環境に CC 技術を適用と発表．
米国陸軍は 2024 年 7 月に同様の技術提供を受けると発表．
米国以外では，イスラエルが同様の技術を導入．

国内の事例
・NTT ドコモと JAL らは企業間で個人データを突合分析する処理に TEE を用いている．
リモートアテステーション機能を活用して，データ削除を確認する良い事例である．
三井物産の子会社のゼウレカは，GPU の CC を用いての創薬研究を進めている．
NEC もサプライチェーンの最適化を目指し，物流データの秘匿処理に CC を導入．
異業種間での安全なデータ連携基盤として構築された．

CC のインフラ提供動向

海外のインフラ提供動向
・TEE 対応のチップは Intel，AMD，NVIDIA が提供し，クラウドインフラは
Amazon Web Service や Google Cloud Platform や Microsoft Azure が提供し、
ミドルウェアは，Fortanix や Anjuna や Enveil のスタートアップが提供．米国が強い．

→★本機能は、クラウド利用の企業アプリでは必須と思われる。

国内のインフラ提供動向
・政府向けクラウド環境の「ガバメントクラウド」では，「機密コンピューティング」が
必須機能となっており，さくらインターネットは本技術の導入準備を進めている．
NTT Data も経済安全保障やソブリンクラウド（国家・企業が主権を保持し，
コントロール可能なクラウドサービス）のために CC の導入を目指している．

・IPA（情報処理推進機構）は，通信や電力などの重要情報を扱うシステムの安全性要求を
記載したガイドラインを 2023 年に発行しており，「計算途上のデータ暗号化」という
CC 相当の機能を記載し，技術成熟度なども検討した導入検討を推奨している．

・ハードウェアのチップは、富士通が TEE の CPU を 2027 年にリリース予定.
ミドルウェアは，Acompany が GPU の TEE にも対応したミドルウェアをリリース済み.
CC については，政府が進める K Program（経済安全保障重要技術育成プログラム）で，
TEE がテーマの１つとなっている．経済安全保障の観点では，技術ベンダーの選択肢が
狭いことは好ましくないので，国内では，急速に技術開発が進んでいる.

CC と法制度との関係

・CC に関連する法制度の議論も活発で，個人情報保護法の改正に向けた議論では，
個人情報保護委員会から，統計目的で個人データを第三者提供し，複数企業から第三者
提供されたデータを突合して統計的に集計し，統計情報を得るような処理については，
個人の権利利益を害する恐れが低いため同意を不要とする件について議論されている.

・デジタル庁の「データセキュリティ WG」や DFFT（Data Free Flow with Trust）でも
CC を含む PETs（Privacy Enhancing Technologies）が論点となっており，
技術を用いた信頼できる安全なデータ活用が検討されている.

→★GAFA が得ている膨大な個人情報の扱いについての規制も必要と思われるが・・・
以前、薬局やコンビニの POS 端末からの情報収集が話題になった時代もあった。

今後の期待

・CC は生成 AI の適用拡大とともに急速に注目され，特に海外での導入が進んでいる.
今後は国内でも導入が進んでいくことが予想され，関係する環境整備が必要である.

・特に日本は企業間でのデータ連携によるデータ活用の推進が，産業競争力を高める
基本的な戦略となっている．ぜひ CC 技術をそのためのキーとなる技術と捉え，
制度整備が進みつつある今，新たなビジネスの検討に着手されることに期待したい.

以上