第 1 回 TCG Virtual CodeGen Developer Challenge

応募概要

開催期間：2021 年 10 月 18-22 日 PDT　（Kick-off 会議：10 月 18 日 PDT)
審査会：10 月 22 日 PDT

テーマ	Pervasive Security and Application of TCG standards in SW and HW development （SW 及び HW 開発においての TCG 標準規格とセキュリティの普及を目指す）
応募対象	テクノロジーやイノベーションに興味をお持ちの 18 歳以上の方（チーム or 個人）※ ※TCG 会員企業に所属される方で、技術委員会の Work Group の会員専用サイトにアクセスされたことがある方は、応募対象となりませんので、予めご了承ください。
プレエントリー/ 応募概要締切	2021 年 10 月 12 日 03:59PM JST / 10 月 11 日 11:59PM PDT プレエントリーフォーム　;　応募概要提出フォーム
応募内容	未応募（他のコンテストを含む）の以下の内容を含むオリジナル作品※ ※TCG の規格を利用した実際に動作が確認できるプログラムのほか、TCG の規格の拡張への提案、TCG の規格を利用したアイディア。
応募部門	TSS and TPM、DICE、Storage、FIM and RIM
各賞・副賞	ファイナリスト/Challenge Area Winner (4 部門):　各 1,000 米ドル グランプリ/Finals Winner: さらに、4,000 米ドル（総額 5,000 米ドル） 特別賞/Honorable Mention: 1,000 米ドル
応募作品の著作権	本コンテストに参加する応募者が作成・提出した作品の知的財産権は、応募者に帰属するものとします。ただし、TCG が、当該作品の使用、公表、発信することについては、一切制限がないものとします。また、応募作品には、互換性のある他のオープンソースライセンスが指定されていない限り、BSD 2-clause ライセンスが適用されるものとする。
備考	• 提出書類、応募内容のプレゼンはすべて英語で準備をお願いします。 • 応募部門が特定できない場合は、概要ご提出の際にお知らせください。主催者側で特定します。 • 審査会でのプレゼンは、時差の関係で Live 参加が難しい場合は録画でのご提出も可能です。 • キックオフ会議や審査会の時間などの詳細については、後日ご案内します。
詳細 URL	https://trustedcomputinggroup.org/work-groups/regional-forums/japan/tcg-codegen-developer-challenge
問い合わせ先	CodeGen@trustedcomputinggroup.org（英語；日本語可）

応募内容詳細

下記の４つの部門を設けており、応募作品の種類は、下記を例に幅広い作品のご応募をお待ちしております。

- **実際に動作が確認できるプログラム**
- **TCG の規格の拡張への提案**
- **TCG の規格を利用したアイディア**

TSS and TPM

TPM 仕様および TSS 仕様は、TPM を様々なプラットフォームに実装する方法を詳述し、TPM の機能にアクセスするための標準 API を提供しています。アプリケーション開発者は、これらの仕様を利用して、より耐タンパ性の高いコンピューティングのための相互運用可能なクライアントアプリケーションを開発することができます。

Trusted Platform Module Library Specification

(Family "2.0", Level 00, Revision 01.59, November 2019)

https://trustedcomputinggroup.org/work-groups/trusted-platform-module/

DICE

DICE のリソースは、TPM を搭載したシステムを強化するだけでなく、TPM を搭載していないシステムやコンポーネントに対しても、実行可能なセキュリティとプライバシーの基盤を提供します。この研究の焦点は、最小限のシリコン要件でセキュリティとプライバシーを強化する新しいアプローチを開発することにあります。

Trusted Platform Architecture Hardware Requirements for a Device Identifier Composition Engine

(Family "2.0", Level 00 Revision 69, December 16, 2016, Committee Draft)

https://www.trustedcomputinggroup.org/wp-content/uploads/Device-Identifier-Composition-Engine-Rev69_Public-Review.pdf

Storage

Storage 仕様は、既存の TCG 技術をベースに、専用ストレージシステムのセキュリティサービスに焦点を当てています。目的の一つは、ATA、シリアル ATA、SCSI、FibreChannel、USB Storage、IEEE 1394、Network Attached Storage (TCP/IP)、NVM Express、iSCSI を含むがこれらに限定されない、専用のストレージコントローラインターフェイス間で、同じセキュリティサービスを定義するための標準と手法を開発することでです。ストレージシステムには、ディスクドライブ、リムーバブルメディアドライブ、フラッシュストレージ、マルチプルストレージデバイスシステムなどがあります。

Storage 関連リソース：https://trustedcomputinggroup.org/work-groups/storage

FIM and RIM

FIM と RIM の仕様は、PC クライアントの取り組みの一環として、TPM や Opal などの TCG 技術の機能と動作を、クライアントのエンドポイントコンピュータのコンテキストで定義するものです。

TCG PC Client Platform Firmware Integrity Measurement

（*Version 1.0 Revision Specification 43, Family 2.0, May 7, 202*）

https://trustedcomputinggroup.org/wp-content/uploads/TCG-PC-Client-FIM_v1p0_r0p43_pub.pdf

TCG Reference Integrity Manifest (RIM) Information Model

(Version 1.01, Revision 0.16, November 12, 2020)

https://trustedcomputinggroup.org/wp-content/uploads/TCG_RIM_Model_v1p01_r0p16_pub.pdf

参照リソースページ：https://trustedcomputinggroup.org/resources/