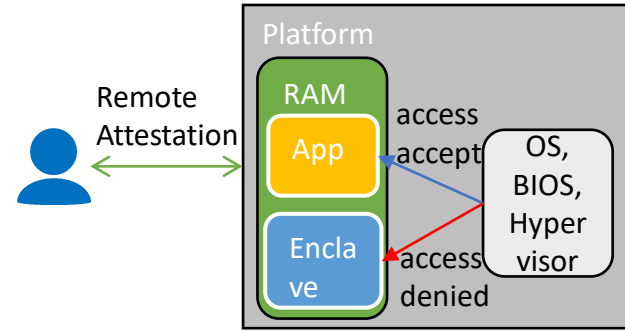



Intel SGX DCAPを利用したリモートアテステーションの特徴についての調査

矢川嵩(筑波大学, 産業技術総合研究所), 照屋唯紀(産業技術総合研究所), 須崎有康(産業技術総合研究所)

概要	Intel SGX	リモートアテステーション
<ul style="list-style-type: none">クラウドやIoTの普及に伴い、管理や操作を目的とした遠隔操作が増加リモートアテステーション：遠隔でデバイスとソフトウェアの健全性を確認隔離実行環境を提供するIntel Software Guard Extensions(SGX)は、2種類のリモートアテステーションに対応それらの仕様の違いによる利点と欠点は明確になっていない。 ↓ 調査段階として仕様を比較	 <ul style="list-style-type: none">TEEを提供するIntel CPUの拡張機能メモリの一部領域を暗号化(Enclave)リモートアテステーションによってプラットフォームとEnclaveの健全性を確認	<ul style="list-style-type: none">対象のEnclaveとプラットフォームの検証を含んだ独自プロトコルプラットフォームとEnclaveの健全性を示すのに必要な情報はまとめてQuoteと呼ぶQuoteには署名が付いており、この検証には外部サービスを利用 

2つのリモートアテステーションの比較

Enhanced Privacy IDベース 従来のリモートアテステーション	ECDSAベース Data Center Attestation Primitives(DCAP)を用いるリモートアテステーション
<ul style="list-style-type: none">Quote生成についての違い<ul style="list-style-type: none">信頼の鎖	<ul style="list-style-type: none">Quote検証についての違い<ul style="list-style-type: none">オフライン検証が可能

