課題 202

超長期セキュア秘密分散保管システム技術の研究開発

物理乱数源と秘密分散ソフトウェアを開発し、超長期データ保管を実現することによって、
ネットワークテストベッド上での超長期セキュア秘密分散保管システム構築のための基盤技術を獲得する。

背景と課題

重要情報、特に生命に関わる重要な医療情報やビジネス価値の高い機密情報が近年急速に増え、その超長期間にわたる機密性・完全性確保の機運は各国で高まっている。またこのような重要情報は災害やサイバー攻撃があった場合でも減失や棄損があってはならず、必要なとき常に利用できる必要がある（可用性の保証）。しかし、これらを実現する技術を本格的に実用化するには至っていない。そこで、物理乱数源により生成した真性乱数を秘密分散によるデータ保管に利用することで、機密性、完全性及び可用性の高いデータ保管を超長期にわたって実現する。

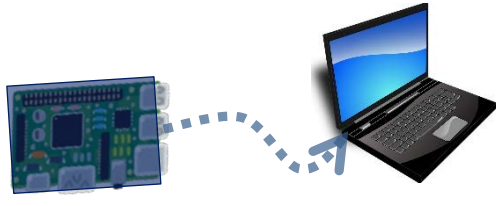
研究開発の目的

上記の機密性、完全性及び可用性の高い超長期データ保管を、機構やその協力機関と共同で実施するネットワークテストベッド上で実現するために基礎となる技術を開発することを目的とする。

研究開発の概要

課題A 物理乱数源の研究開発 (1) 小型の物理乱数チップを開発したうえで、(2)物理乱数ドングルの開発と製品プロトタイプの作製を実施、更に上述のネットワークテストベッド上で超長期データ保管を実現するため、大量の真性乱数を必要とするサーバ等での秘密分散処理に対応可能な (3)高速物理乱数装置の研究開発にも取り組む。

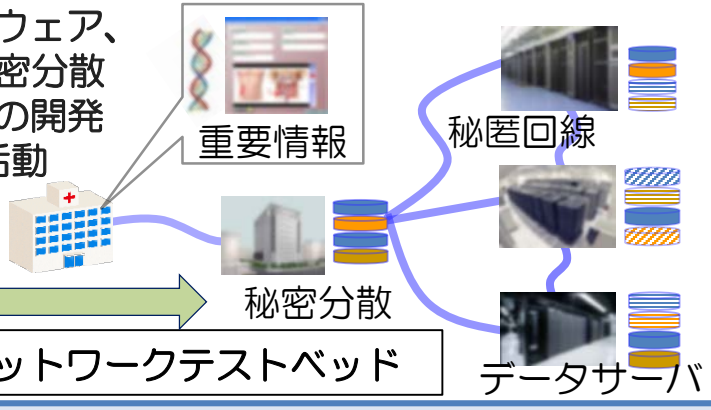
課題B 秘密分散ソフトウェアの研究開発 (1) 課題Aの物理乱数ドングルまたは高速物理乱数装置とインテグレートした秘密分散ソフトウェア及び(2)超長期セキュア秘密分散保管システム技術を開発し、(3)その標準化に向けた活動を行う。



課題A (1)小型物理乱数チップの開発
(2) 物理乱数ドングルの開発、
製品プロトタイプの作製
(3)高速物理乱数装置の研究開発

課題B (1)(2)秘密分散ソフトウェア、
超長期セキュア秘密分散
保管システム技術の開発
(3)標準化に向けた活動

真性乱数の提供



研究開発期間：2018年度（契約締結日）から2020年度末までの3年間（第1期）
2021年度から2022年度までの2年間（第2期）については、次期中長期目標の状況等も踏まえ、継続について検討する。
2018年度予算：課題A 15百万円（上限）、課題B 25百万円（上限）　　採択件数：課題A、課題B　各1件