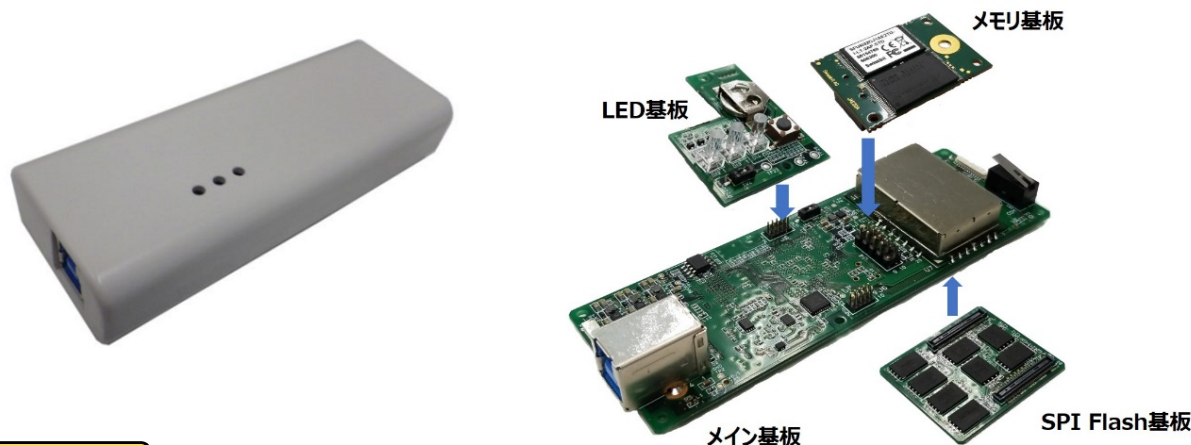


物理乱数ドングル



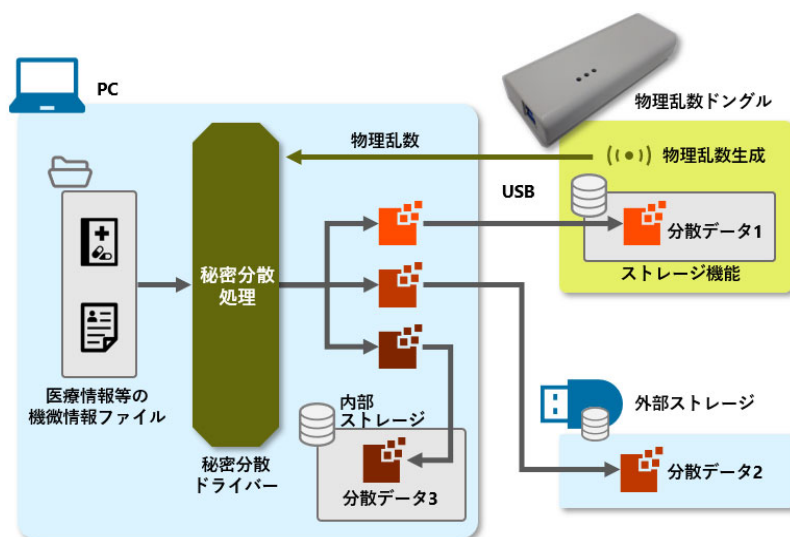
○ 特徴

- ・持ち運び可能な物理乱数源
120mm × 45mm × 21mm、重さ 120g
- ・生成した物理乱数を保存し、利用時にまとめて使用することが可能
物理乱数保存容量: 16Gbit
- ・秘密分散された1片を格納し、持ち運びするストレージとして使用することが可能
分散データ保存容量: 32GB
- ・乱数出力(PC接続)インターフェースはUSB3.0により、1Gbps以上の転送が可能
- ・乱数生成には物理乱数チップを搭載
生成性能: 10Mbps以上、NIST Special Publication 800-22/-90Bをパス
- ・乱数データ形式: API側で、バイナリー、整数、浮動小数点を選択可能
- ・セキュリティー機能
 - a) ワンタイム組立により容易に解体出来ない仕組み
 - b) 解体時には、認証用鍵ペアを消去する
 - c) ECDSAによる個体認証

○ 運用例

株式会社ZenmuTechが提供する秘密分散技術と組み合わせて、下記の機能を提供する。

- ・秘密鍵用の物理乱数
- ・秘密分散後のデータストレージ機能



※ 分散データ1~3のいずれか2つにより元のデータを復元可能

仕様は予告なく変更することがあります