

## Spyrus 社 Hydra PC を認定 アメリカ国家安全保障局

アメリカ国家安全保障局は 2009 年 11 月 2 日 Spyrus 社の SuiteB 暗号の全てをサポートしている Hydra PC シリーズを機密データの暗号化メモリーとして認定した。

FIPS140-2 Level3 に加え“CNSS Instruction 4009 at the SECRET level”(米国 Committee on National Security Systems、<http://www.cnss.gov/>) の規定により、Hydra PC シリーズは世界で唯一の商業的製品 (COTS=Commercial-Off-The-Shelf) として認定された。

これまでは高価で取扱いが難しい Type-1 を使用しなければならないデータ携帯デバイスに替わり、非常に廉価な市販デバイスが登場したことになる。さらに CCI(Controlled Cryptographic Item)を必要としないため管理コスト、操作習熟度が通常の USB メモリー程度となった。商業利用が可能な SuiteB を搭載しているため、政府、企業に機密情報の携帯が簡単に安全に行われるようになった。ECC P-384, AES-256 and SHA-384 等の暗号アルゴリズムを使用可能なため高度なハッシュ、圧縮、暗号化、電子署名やシールに使用できる。FIPS 認定により個人鍵のインポート・エクスポート、破壊が不可能で高度なハッカー攻撃にも耐えられる。PIN の 10 回以上の入力暗号化鍵を削除して安全を確保するよう“brute-force”攻撃に備えており、その後の復号化は不可能になる。

それでも Hydra PC は管理者が指定したコンピュータ上で使用し、一定の境界内で使用することが望ましい。AES 暗号だけでは真のデータセキュリティは確保しきれない。Hydra PC は暗号化の鍵をも管理し FIPS、CNSS のセキュリティ要件を満たす世界唯一の USB メモリーデバイス・トークンである。

以上