Centrino の登場と重要視されるセキュリティ

～高まる secure な PC の要求～

冨岡 弘志，福永 隆宏
Hiroshi TOMIOKA，Takahiro FUKUNAGA

1　はじめに

現在，国内におけるノート PC のシェアは PC マーケット全体の約 50 %にまで拡大している．そのため，ユーザのよりハイパフォーマンスなノート PC の要求に対し，Intel 社はモバイルに特化した新たな CPU である「Pentium-M」，それを含めたモバイルプラットフォームの新ブランド「Centrino」を発表した．これにより更なるノート PC のシェア増加が見込まれる．しかし，ノート PC が普及していくことにより，今まで以上にセキュリティの重要性が高まってくる．本稿ではノート PC におけるセキュリティについて，Centrino の登場により重要視すべき問題点を述べ，それに対する現在の技術を紹介し，ノート PC を含め PC 全体におけるセキュリティの展望について述べる．

2　次世代ワイヤレスコンピューティング技術

CPU の開発はクロック数を増加させることが重要視されていた．しかし，2002 年に登場した Mobile Pentium-4-M プロセッサはクロック周波数は高いが，パフォーマンスや消費電力面ではノート PC には向いていないものであった．そこで，Intel 社は開発コード「Banias」という名で，モバイル専用の CPU の開発に取り組んでいた．これまでと大きく異なる点は，従来のようにデスクトップ PC 用の CPU を低電圧化させて搭載するというアプローチではないということである．そこで，Intel 社は以下の 4 つの指針を掲げ，ノート PC 専用 CPU「Pentium-M」を発表した．

- 高い処理性能
- 長いバッテリ持続時間
- 小型軽量化
- 安全なワイヤレス接続性

Fig. 1　ロゴ

そして Intel 社は，この Pentium-M に加え，統合された無線 LAN[1]，Pentium-M 専用に設計された低消費電力チップセット「Intel855PM，855GM」の 3 つの技術を合わせて「Cetrino プラットフォーム (Fig. 1)」を発表した [1)]．

このような技術によりノート PC のシェアは格段に増加するため，セキュリティ問題がより重要な課題となる．

3　ノート PC のセキュリティ問題

3.1　ノート PC 自体の盗難による情報の漏洩

PC の盗難，すなわち情報の盗難である．ノート PC は携帯性に優れているので，それだけデスクトップ PC よりも盗難される可能性が高い．PC 内に保存していた機密情報が漏洩し，企業の経営等に被害が出ることは防ぐべき問題である．

3.2　リモート環境でのインターネット接続

近年，ホットスポットの増加により，無線 LAN 内蔵のノート PC なら簡単にインターネットに接続できるという環境が広がっている．しかし，このホットスポットはクライアントとアクセスポイント間が暗号化されていない場合が多く，盗聴される可能性がある．WEP（暗号化キー）で無線 LAN の内容を暗号化することも可能だが，安全であるとは言い切れない．

4　セキュリティ テクノロジ

本章では，前章で述べた問題点を解決するためのセキュリティ技術について説明する．

4.1　TPM(Trusted Platform Module)

TPM は secure PC の規格団体「Trusted Computing Platform Alliance(TCPA)[2]」により策定された，秘密鍵を持った小型のチップ仕様であり，暗号処理専用のマイクロプロセッサと EEPROM [3]が内蔵されている．TPM は直接アクセスする方法を提供していないため暗号処理もチップ内部で行われ、結果だけをシステムに返す．

TPM 搭載のノート PC は，本体が起動されるとシステムのハードウェア情報が TPM に読み込まれる．それにより TPM がシステムを特定し，メトリクスと呼ばれる評価付けの値を更新する．ストレージ・キーによりデータが TPM 内に格納されると，このプラットフォーム構成以外のハードドライブからは格納されたデータにアクセスできなくなる．

[1]Centrino^{TM} は IEEE802.11b WLAN 規格をサポート，11g への対応にも動き始めている

[2]Trusted Computing Group（TCG）として再編成された

[3]RSA 暗号鍵を保管する専用の不揮発性メモリ

もし，保護されたデータがTPMを搭載した他のノートPCにコピーされても，TPMが異なるプラットフォームであることを認識しアクセスを拒否する．また，盗んだデータにアクセスしようと，盗んだノートPCをフロッピーからブートすると，TPMが異なるOSからブートされることを認識し，プラットフォーム構成が異なるためにデータへのアクセスを拒否される．これにより，データの安全性が保障される．

4.2 Microsoft 社の Palladium

セキュリティの問題を解決するため，新たな技術も現在開発されている．例えば，Microsoft 社の secure OS「Palladium[4]」が挙げられる．これは，従来と同じ機能を持つPCの内部に別の secure な PC を作るというものである [2]．以下に Palladium の機能を紹介し，Fig. 2 に Palladium のセキュリティの概念図を示す．

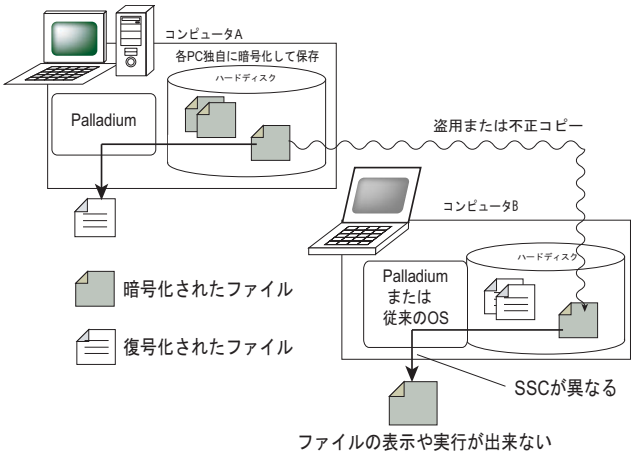

Fig. 2　Palladium のセキュリティ

SSC（Security Support Component）

従来の暗号化などの処理では，鍵を作り，暗号化・復号化を行うのはソフトウェアであるため，ハッキングされる可能性がある．そこで Palladium では，秘密鍵を SSC というハードウェア内に格納し，暗号化・復号化の処理をハードウェア内のメモリ空間だけで行う．これは TPM 技術とほぼ類似したものである．

Sealed Storage

ソフトやデータのディスク上での改竄などができないようにするために，ディスク上でデータがすでに暗号化されている．データは SSC で暗号化されているので，仮にハードディスクを持ち出して，異なる SSC を持った PC でデータを閲覧しようとしても，SSC 内に格納されているシステム識別データが異なっているために鍵が一致せず，ハードディスク内のデータを閲覧できない．

このような技術が実装された Palladium は対応する CPU が必要である．Microsoft 社は 2004 年後半に市場に提供することを目標としている [3]．

4.3 Intel 社の LaGrande テクノロジ

他社のセキュリティ技術として，Intel 社の「La Grande」テクノロジが挙げられる．この技術はプロセッサに実装され，暗号化はプロセッサレベルで行われる．そしてハードディスクにデータが格納されるときにはすでに暗号化が終了している．メモリは他から完全に隠されたメモリ領域に記入されるので，他のプロセスからデータが盗まれることはない．ただし，BIOS は La Grande に対応する必要がある．これは，secure にブートアップできる BIOS でなければならないからである．

LaGrande は Palladium に対応しており，導入時期は 2005 年頃と報告されている．しかし，これはデスクトップ PC のみでノート PC への搭載予定はまだない [4]．

5　今後の展望

Centrino は TPM を搭載した，secure なノート PC と言える．現在，各メーカは Centrino プラットフォームのノート PC を次々発売している．このことより 1 年後，国内では Centrino 搭載 PC が 7〜8 割を占めると予想する．しかし，世界的にみると Centrino の無線 LAN 規格に準じない国もあるため，全世界に完全に浸透しきれないのではないかと考える．一方，Transmeta 社のノート PC 向け CPU「Crusoe」にもセキュリティ技術が搭載され，今年の下半期に製品を発表するとの報告がある [5] が，ノート PC 市場での Crusoe のシェアは小さく，Intel 社が大幅に占めているため，CPU にセキュリティ技術を搭載したノート PC は Crusoe のシェア程度にとどまるのではないかと考えられる．

また，デスクトップ PC では，ノート PC と比較して secure な PC の登場は多くないと思われる．それは，セキュリティ機能を備えた Palladium・LaGrande の登場が 2004 年後半以降と発表されており，各メーカもそれに合わせて PC の製造を行うと考えられるからである．ただし，その間に secure な PC が全く登場しないわけではなく，TPM を搭載したデスクトップ PC が市場に投入されると考えられる．

参考文献

1) 【IDF Spring 2003 レポート】明らかになった Centrino の性能と 802.11g への対応．
http://pcweb.mycom.co.jp/news/2003/02/22/21.html.

2) 後藤弘茂の Weekly 海外ニュース.
http://pc.watch.impress.co.jp/docs/2002/0911/kaigai01.htm.

3) MS の Palladium は，PC の守護者かプライバシーの破壊者か？
http://www.zdnet.co.jp/news/0206/25/ne00_palladium.html.

4) Intel Developer Forum Conference Fall 2002 基調講演レポート.
http://pc.watch.impress.co.jp/docs/2002/0910/idf02.htm.

5) Transmeta，crusoe にセキュリティ機能搭載.
http://www.zdnet.co.jp/news/0301/15/nebt_05.html.

[4] 1 月に Next-Generation Secure Computing Base と開発コードネームが変更された