ビジネス向けPCのセキュリティ技術

Security Technologies for Business Notebook PCs

松岡　義雄　　上田　国生
■MATSUOKA Yoshio　■UEDA Kunio

昨今，特に日本国内においては個人情報の保護に関する法律が施行されたこともあり，情報セキュリティが注目を浴びている。企業内パソコン（PC）の中の個人情報量は膨大であり，その情報が漏えいした場合の賠償などのリスクは企業の存在をも危うくさせるほどに高くなっている。ビジネス向けノートPCにおいては，可搬性を向上させるというメリットを生み出すと同時に，盗難の容易性，置忘れなどのリスク要素を増加させるため，顧客に対してその情報を守る手段と守られている安心感，つまり“安心と安全”を提供することが必須となっている。

東芝は，長年培ってきた自社製BIOS（Basic Input Output System）と自社製ソフトウェアの技術の組合せにより，使い勝手を考慮しつつセキュリティ強化を積極的に図ってきた。BIOS改ざん防止技術やBIOSパスワード・HDD（磁気ディスク装置）パスワード認証，SD（Secure Digital）カードトークン認証，デバイスロック，指紋認証，“東芝サインログオン”の実装がその取組みの一例である。

Information security is currently attracting considerable attention, especially in Japan with the recent enactment of the Personal Information Protection Law. PCs used in the corporate environment contain huge volumes of personal information. As a result, the risks of the leakage of such information have become so high that the existence of the corporation itself may be threatened, through having to pay compensation for damages, for example. In the case of business notebook PCs, it has therefore become mandatory to provide customers with the security of having clear ways to protect information, because the greater portability of these PCs also increases their vulnerability to theft and loss.

Utilizing its long-accumulated in-house technologies in both BIOS and application software, Toshiba has been aggressively strengthening information security while taking ease of use into consideration. Among the information security technologies that we have developed are protection against malicious alteration of a computer's BIOS, BIOS password, hard disk drive password, secure digital (SD) card token, device lock, fingerprint authentication, and handwritten signature log-on.

1　まえがき

PCのセキュリティ機能としては，基本ソフトウェア（OS）が持つ機能や社外から導入したアプリケーションにおいて実現されるものもあるが，ここでは主に，東芝として独自の特長を持つ自社製BIOS（Basic Input Output System）及び自社製ソフトウェアによるセキュリティ機能差異化技術について述べる。なお，これらの技術は過去1～2年間の当社PCに順次搭載され，かつ強化されて現在に至っている。

2　BIOSセキュリティポリシーの強化

BIOSにセキュリティ機能を持たせる場合，そのセキュリティ機能が信頼できるものであるためには，BIOS自体が容易に改ざんできない仕組みが必要である。

PC起動時のBIOSの実行は**図1**に示すとおりブートブロック処理，起動時のハードウェア初期化とテストのためのIRT（Initial Reliability Test）処理，オプションROM処理，OS起動前処理に大きく分けられる。従来のBIOSでは，起動時に実行される各コードにおいてチェックサム（コードバイナリ値の単なる加算）確認は行っていたものの，それはセキュリティ

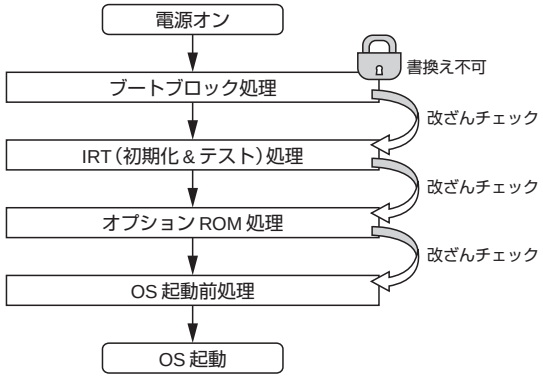

図1．起動時のBIOSシーケンス ― 電源オン後からOSが起動するまでの間に各種の初期化処理が行われる。各ブロック実行前に改ざんチェックが行われることで，OS起動前のシステム安全性を保証する。

Flowchart of BIOS boot sequence

的な観点の確認ではなく，BIOSコードの内容が何らかの原因（ROM破壊など）で壊れたことをチェックするためであった。

そこで当社のBIOSでは，ハッシュ関数を利用した改ざん検出機能を実装することにした。BIOSの各ブロックに対するハッシュ値を計算し，そのハッシュ値が正当なものかどうかを独自設計のセキュリティ用ハードウェアで検証する仕組みを作り込んだ。

具体的には図1のように，マシン電源オン直後はブートブロックと呼ばれるROM領域が最初に実行されるが，ブートブロックは書換えができないようにハードウェア的にロックされており容易に改ざんできない。ブートブロックは次に実行されるIRTコードのハッシュ値を検証し，改ざんされていないことを確認してからIRTコードを実行する。同様にIRTコードは次にオプションROMコードを実行する前にオプションROMコードのハッシュ値を検証し，改ざんされていないことを確認してからオプションROMコードを実行する。このように次のコードを実行する前に必ずそのハッシュ値を検証して，正しく検証された実行コードだけを実行が許可されるようにした。すべてのBIOS実行コードが改ざんされていないことを保証するこのリンク構造のことを“Chain of Trust（信頼の鎖）”と呼んでいる。

当社の新BIOSでは起動の高速性を損なわずにChain of Trustの基礎技術を確立したことで，BIOSパスワード，HDDパスワードなどの各種セキュリティ機能の全体的な信頼性を向上させることができた。

3 BIOSのセキュリティ機能

次に，当社のBIOSが提供する主なセキュリティ機能について述べる。

3.1 BIOSパスワード認証

これは，電源オン後，OS起動前にパスワードロックをかける機能で，OS非依存でシステムを保護できる利点がある。パスワードは，HDDやRTC（Real Time Clock）内のRAMなどの一般に仕様公開されたエリアではなく，独自設計のセキュリティ用ハードウェア内の秘匿エリアに保存し，安全性を高めた。

更に，BIOSパスワードを忘れてしまったユーザーに，パスワード解除を行う仕組み（迂回（うかい））を必ず提供する必要があるが，その部分にもセキュリティ強化を実施した。従来のBIOSでは，あるハードウェアモジュールを接続することによってパスワードを解除する仕組みを用意していたが，そのモジュールを悪意のある人間が作成し，パスワードを無効にしてしまうことが懸念された。

このため，現行BIOSでは保守部門でのパスワード解除方法に“チャレンジ・レスポンス”という新しい方式を導入した。これはユーザーがパスワードを解除できなくなった場合，まず当社の保守窓口へPCを持ち込み，正当な所有者であることの確認を行う。そこで，保守担当がこのPC上で特別な操作を行うことにより，使い捨てのチャレンジコードが得られる。安全な場所に設置されている専用サーバにて，保守担当の認証とチャレンジコードの検証が行われ，対となるレスポンスコードが発行される。保守担当が，レスポンスコードをこのPCへ与えることにより，パスワードの代わりとして認証される。こうして保守担当はパスワードを迂回してPCを起動したり，パスワードを解除したりすることができる。チャレンジコードから不正にレスポンスコードを得ることはたいへん困難なので，容易にパスワードを無効化できてしまうというぜい弱性はなくなった。

3.2 HDDパスワード認証

これは，HDD内部機能として用意されているHDDパスワード機能をBIOSで完全サポートするものである。HDDの内部ROMにパスワードを保持するため，システムからHDDを物理的に取り外して別のマシンに接続されても，HDDパスワード認証が行われない限りHDDにはアクセスできない。

3.3 SDカードトークン認証

BIOSパスワードを入力する際，キーボード入力に代わる認証方式として，市販のSDメモリカードを使った物理的な認証鍵（トークン）を作成することができる。これは，SDメモリカード一枚一枚がハードウェア的に固有に持つID（IDentification）を鍵の一部として利用している。ユーザーがSDカードトークンをスロットに挿入するだけで本人認証が完了し，BIOSパスワードの入力が不要なため，ユーザーの使い勝手も向上した。

3.4 指紋認証

当社PCでは，指紋センサデバイスを2005年の春モデルから採用した。OSのログオンだけでなくBIOSパスワードに代わる認証方法として，BIOSレベルでも指紋認証サポートを始めている。PC本体に組み込まれた指紋センサを指で軽くなぞるだけで，指の表面より深い層にある真皮の部分のパターンを読み取り，登録データと照合して本人認証を行える（**図2**）。BIOSパスワードを覚えておく必要がないため，セキュリティ強化とともに使い勝手を高めている。指紋認証プログラム起動時も，そのプログラム自体が改ざんされないよう，暗号化や実行コードハッシュ値検証によるチェックシーケンスを組み込んだ。

3.5 デバイスロック機能

当社BIOSと自社製のユーティリティの組合せにより，ほぼすべての外部入出力ポート及びブートデバイスのロック機能をサポートした。例えば，USB（Universal Serial Bus）ポートやPCカードなどにはフラッシュメモリが接続され，PC内部の情報が流出する可能性がある。これを防ぐために，

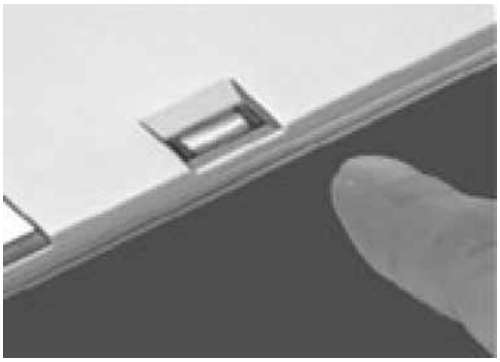

図2．指紋認証動作 ― 指紋認証デバイス上で指を滑らせることで，OSログインなどの個人認証が行える。
Operation of fingerprint authentication

図3．デバイスロックユーティリティ設定画面 ― ロック可能なすべての設定項目を表示している。
Setting of device lock utility

管理者がスーパバイザパスワードでシステムを保護している状態からデバイスロックユーティリティを起動し，禁止したいポートをロック指定してPCを再起動することで次回からポートは動作しなくなる（デバイスマネージャ上からも消える）。ロック情報は，独自設計のセキュリティ用ハードウェア内の秘匿エリアに保存され，いったん設定後はOSを差し替えてもそのロック機能は継続できる。また，例えば外部FDD（Floppy Disk Drive）などからブートされ，別のOSを起動されて情報が盗まれる場合も考慮し，ブート機能のロックもサポートしている（**図3**）。

4 “東芝サインログオン”

東芝サインログオンは，ユーザーがあらかじめ登録しておいたみずからのサインを手書き入力することで，自動的にWindows®（注1）にログオンすることができるユーティリティである。当社のタブレットPC dynabook R10などに搭載されている。

このユーティリティは，最近注目を浴びている生体情報を用いた個人認証の一実施例である。一般に生体情報を用いた認証は，認証のための鍵となるデバイスなどを持ち歩く必要がなく，また個人に特有の情報であるので，悪意の第三者が不正アクセスのための偽データを準備することが困難である，などの利点があると言われている。

ここでは，このユーティリティの機能と技術的な背景について述べる。

4.1 機能

このユーティリティは大きく分けると，サイン登録機能と，認証及び自動ログオン機能の二つを提供する。

ユーザーはあらかじめサイン登録機能を使い，ログオンに使用するユーザー名やパスワードなどの情報とともに，自分のサインを登録しておく必要がある。サイン登録時には複数回の入力を行わせ，更にその後の1回の入力により模擬認証を行うことで，登録データの信頼性を確保している。非常に単純なパターンのサインは，セキュリティの観点から問題があるので，この段階で登録を拒否する。

1個以上のサインが登録された状態では，Windows®のログオン画面においてサイン入力のための入力枠が表示される（**図4**）。ユーザーは自分のユーザー名をコンボボックスから選択し，枠内にサインを入力する。入力されたサインが後述の認証エンジンにより登録データと照合され，認証を通れば自動的にログオンする。

この画面をキャンセルして，通常のWindows®のログオン画面からパスワードによりログオンすることも可能である。

4.2 認証エンジン

このユーティリティはサインの認証処理を行うもので，当社が開発した“東芝サイン認証エンジン”を使用している。

このエンジンは，ユーザーが入力したサインから座標や速度などの運筆情報を取り出し，これらをあらかじめ登録さ

図4．サイン認証のための入力画面 ― Windows®のログオン画面で入力枠が表示される。
Input box for signature log-on

（注1），（注2） Windows，Microsoftは，米国Microsoft Corporationの米国及びその他の国における登録商標。

れたサインの運筆情報と照合し，その相違度を見ることで本人か否かを判断する。運筆情報の照合には，DP（Dynamic Programming）マッチングを用いている。単純な軌跡（筆跡）情報だけでなく，速度，加速度，筆圧を含んだ7次元ベクトルの時系列データを照合対象としているので，かりになんらかの方法で見本（本人のサイン）を入手してそれをまねて書いても，他人が不正に認証を通すことは困難である。

5 今後の技術動向

セキュリティの新技術や応用技術は，以下のように各種の方式が候補として考えられている。

5.1 TPM

既に一部の当社PCにも搭載されているセキュリティチップTPM（Trusted Platform Module）は，TCG（Trusted Computing Group）が策定した仕様に準拠したチップの名称で，ハードウェア及びソフトウェアの改ざんチェック，暗号鍵の安全な保管，RSA（Rivest-Shamir-Adleman）暗号やハッシュの暗号処理などのコアとなる。今年後半にはチップ仕様がバージョン1.2に更新され，Windows®などのソフトウェアと親和性がいっそう高くなる。将来的にはPCシステムに必須のハードウェアになり一般化する可能性が高く，今後はTPMを活用しかつ当社先行技術との組合せにより，特長のある商品を提供していく計画である。

5.2 NGSCBとLT

Microsoft®（注2）は新しいPCセキュリティアーキテクチャとしてNGSCB（Next Generation Secure Computing Base）を開発中である。これはLonghornと呼ばれる次期OSでも一部機能しか間に合いそうにないが，Intel®（注3）のLT（LaGrande Technology）及びTPMと組み合わせることで，PC内部に強力な秘匿領域を作り出すものである。これまでのOSカーネルとは別にセキュリティカーネルを用意し，そのカーネルで管理される情報（メモリやHDD上のデータを含む）及び外部接続ケーブルに入出力されるデータを暗号化するため，認証されていないユーザーが外部から情報をのぞき見したり改ざんすることができない。例えば，外部ディスプレイケーブルや外部キーボードケーブルも暗号化された情報をやりとりするため，悪意のある人間がキー入力の生情報を盗むことができない。次期OSについてはFull Volume Encryption（HDD内容の丸ごと暗号化）やSecure Start-up（BIOS，OS，アプリケーションまでのすべてのソフトウェア実行コードを改ざんチェックする仕組み）と呼ばれる技術を組み込むことが発表されており，当社もそれらに対応した技術開発を進めている。

5.3 生体認証

生体認証とは人体が持つ固有の情報を使って認証を行う仕組みで，多方面で研究が進んでおり，虹彩，指や手のひらの静脈，顔，声紋などが脚光を浴びている。当社は現在指紋認証とサイン認証を製品化しているが，ユーザーがパスワードやトークンを管理する必要がない運用性の良さが魅力である。当社内でも顔認証や声紋認証のほか先行的技術を研究しており，積極的にPC差異化に結びつけていく予定である。

5.4 近接認証

近接認証とは，固有のIDを持つ無線認証デバイスを持っているユーザーが，その無線を受信可能なターゲットPCに一定距離近づくことで認証が行われる方式である。例として，ユーザーがPCから離れると自動的に画面にロックをかければ第三者からデータを見られることがない。近接認証は基本的にコネクタ接続でないため，使い勝手や耐久性の点からも有利である。当社は，既に自社ノウハウが培われているBluetooth™（注4）ワイヤレス技術を応用した近接認証システムを検討中である。

5.5 防犯・追跡システム

これは，PCを物理的に盗難から未然に防ぐ，あるいは盗まれてしまったPCを取り返すシステムである。盗まれないようにすることもセキュリティを考えるうえで重要な要素であり，当社のPCで実現している“加速度センサを応用した移動警報機能”はその一例である。また，PC盗難後にネットワーク経由でPCを追跡し，見つかればBIOSがPCを二度と起動できなくさせる技術も考案されている。

6 あとがき

現在は強力と思われるセキュリティ機能でも，時間がたつと解析され破られる可能性がある。例えば，指紋認証センサが一般化すると指紋複製技術が進んでしまうことも想定される。当社は，最新技術を積極的に応用し，各種脅威に対抗しかつ使い勝手のよいセキュリティ技術商品を，自社製BIOSと自社製ユーティリティの強みを生かしてタイムリーに市場に提供していきたい。

（注3） Intelは，米国又はその他の国における米国Intel Corporation又は子会社の登録商標又は商標。

（注4） Bluetoothは，Bluetooth SIG, Inc.の商標。

松岡　義雄　MATSUOKA Yoshio

PC&ネットワーク社 PC開発センター PC設計第一部主務。PCのBIOS開発に従事。

PC Development Center

上田　国生　UEDA Kunio

PC&ネットワーク社 PC開発センター PCソフトウェア設計第一部。PCのソフトウェア開発に従事。

PC Development Center