

セキュアなUSBメモリを社内で作れる



InterSafe SecureDevice

USBメモリによる情報漏えいやウイルス感染は、多くの企業の悩みの種だ。これに対して、ALSIの「InterSafe SecureDevice」は、汎用のUSBメモリを専用アプリケーションによりセキュア化することで、情報漏えいを防止する。

アルプスシステムインテグレーション (ALSI)
<http://www.alsi.co.jp>

セキュアなUSBメモリを作れる InterSafe SecureDevice

大容量化・低価格化するUSBメモリはモバイルユーザーに高い利便性を提供してくれるが、一方で情報漏えいの危険性を秘めている。紛失や盗難などにより、顧客データや業務機密が漏えいしてしまうことも多く、大きな問題となっている。USBメモリの利用自体を禁止する会社もあるほどだ。

これに対しては、セキュアUSBメモリの導入が効率的だ。データの暗号化やパスワード認証、書き込みやコピーの制御を行なえるセキュアUSBメモリを社員に貸与し、利用を徹底すれば、情報漏えいのリスクを低減することができる。

こうしたセキュアUSBメモリを汎用USBメモリから作れるのが、今回紹介するALSIの「InterSafe SecureDevice」(以下、SecureDevice)である。具体的には汎用USBメモリをSecureDeviceのコンソール上からフォーマットすることで、暗号化や読み書き制御、ログ管理などが可能なセキュアUSBメモリに仕立て上げられるというものだ。

SecureDeviceには、Standard、Professional、Ultimateという3つのライセンスがあるが、今回はStandardの最新版1.5を試用した。

管理コンソールの導入と セキュアUSBメモリの登録

SecureDeviceにおけるセキュアUSBメモリの生成と管理には、専用の管理コンソールとデータベースであるPostgreSQLのインストールが必要になる。インストール終了後は、デスクトップにできたショートカットから管理コンソール

を起動する。初期パスワードでログインし、発行されたライセンスを登録し、再起動を行なうと利用可能になる。

SecureDeviceの管理コンソールの上部には、各種メニューが並んでいる。USBメモリを登録する「デバイス」、セキュリティポリシーの「テンプレート」、ログの取得と検索を行なう「ログ」、パスワード管理やフォーマットなどを行なう「管理ツール」、権限の異なる管理者を登録できる「管理者設定」ライセンスやマスターキーなどの環境を設定する「環境設定」などだ。このうちUSBメモリ登



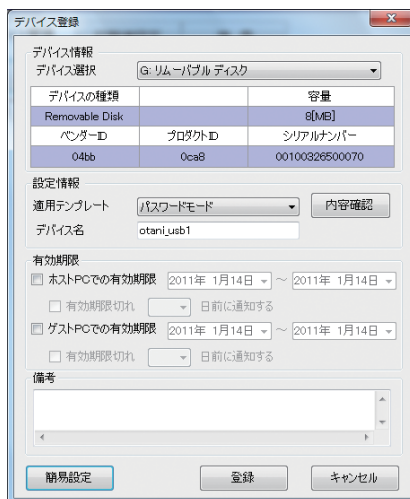
画面1 管理コンソールの「テンプレート」メニューで、各モードを選択する

録の前にチェックしておきたいのが、テンプレートである。

デフォルトでは、パスワードモード、情報漏洩対策モード、ウイルス対策モードの3つが用意されており、それぞれアクセス制御のポリシーが異なっている。最も緩いパスワードモードは、PCとUSBメモリ間でのデータのコピーや移動、クリップボード、印刷なども可能だが、情報漏洩対策モードではPCからUSBメモリへのデータ書き込みのみ許可される。もちろん、ウイルス対策モードでは、すべてのやり取りが禁止となっており、USBメモリ内のファイルは読み出しと編集のみ可能となる。USBメモリの登録時は、このテンプレートを選択することになるので、ポリシーについてチェックしておこう。もちろん新規で作成することも可能だ。

実際のUSBメモリ登録を見ていこう。登録したいUSBメモリを差し込み、デバイスタブで「登録」ボタンを押す。すると「デバイス登録」のダイアログが表示されるので、ここではパスワードモードを選択し、デバイス名を入力する。デバイス名は検索の時のキーになるので、企業で統一したルールで入力しておいたほうがよいだろう。また、詳細設定ボタンを押すと、有効期限も設定できる。「登録」ボタンをフォーマットが実行され、セキュアUSBメモリへの変換が完了する。USBメモリは複数まとめてグループ化できるので、部署ごとにグループ化しておくともよいだろう。

フォーマットが完了したら、できたUSBメモリをエンドユーザーに渡し、エンドユーザーは自身のPCに登録する。SecureDeviceでは、最初に登録したPCをホストPCとみなし、そのほかはアクセスが限定されたゲストPCとして



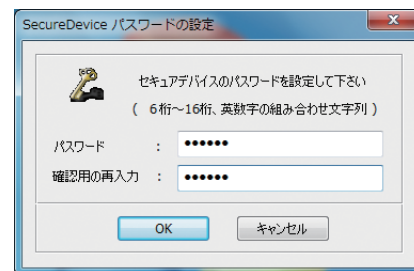
画面2 「内容確認」のボタンを押すと、モードの中身が表示される。有効期間の設定も可能

扱われる。ホストPCではUSBメモリを通常どおり使えるが、それ以外のゲストPCにおいてはポリシーに応じて編集や移動などの操作が制限される。

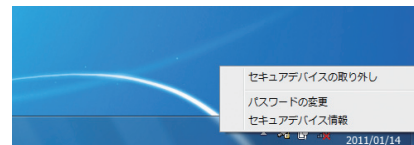
なお、ProfessionalやUltimateではUSBメモリ1本につき複数のPCを登録できるほか、利用期間を超過したデータを自動的に削除する機能もある。

セキュア化されたUSBメモリを渡されたユーザーが、PCにそのUSBメモリを差し込むと、ホストPCとして登録するかどうかのダイアログが表示される。OKを押すと、パスワードの設定を求められ、SecureDeviceが起動。これにより、以降はホストPCとして動作することになり、「SECUREDRIIVE」というユーザー用に割り当てられたボリュームを自由に利用することができる。認証を通らないと、そもそもSECUREDEVICEというボリューム自体が見えないので、紛失や盗難が起っても情報漏えいの危険性は低い。

なお、SecureDeviceは接続されている間タスクバーに常駐しており、外す際にはここから行なう。右クリックメニューから「セキュアデバイス情報」を



画面3 ホストPCの登録の際には、パスワードを設定する必要がある



画面4 取り外す際には右のタスクバーの常駐メニューから操作を行なう

選択すると有効期限やパスワード、アクセス制御のポリシーなどを確認できる。

導入が容易な USBメモリセキュリティ製品

ここまでSecureDeviceを試用してきたが、インストール作業でつまづかなければ、実際の利用までは比較的容易だと感じられた。あらかじめテンプレートが用意されているので、ポリシーの割り当ても簡単。フォーマットも時間を要さず、軽快に利用できる。とはいえ、製品の特性上、セキュアUSBメモリを1本ずつ作る必要があるため、手間がかかるのは覚悟すべきだろう。あとは登録時のフローや紛失時の手続きなどは必要になる。

一方、エンドユーザーの立場からすると、SECUREDRIIVEがマウントされたり、取り外しが完了するまで、一瞬時間がかかるので、せっかちなユーザーは慣れる必要がある。とはいえ、操作はおおむねスムーズで、通常のUSBメモリの使用感と特に変わらない。パスワードでデータが守られているというのは、やはり使っている側の立場でも安心感が得られると感じられた。