

SMS活用した紛失・盗難対策ソリューション

「ノートPC持ち出し禁止」は不要に

盗難にあったノートPCを3G携帯電話のSMSネットワークを介して使えなくしてしまうサービスをドコモなどがスタートさせる。3G内蔵ノートPCを本格普及させるトリガーにもなりそうだ。

文 藤井宏治 (IT通信ジャーナリスト)

盗難・紛失による情報漏洩の懸念から、多くの企業でノートPCの社外持ち出しが厳しく制限されている。HDDに大量のデータが蓄積されるノートPCでは、万一事故が発生した場合のリスクが非常に大きくなるからだ。

とはいえ、オフィスのコンピューティング環境をそのまま出先でも利用できるノートPCは、業務効率化の有効な手段でもある。処理能力やバッテリー稼働時間の向上、WiMAXや3G/LTEなどの新たなモバイルデータ通信サービスの登場により、社外での利用価値はますます高くなっている。盗難・紛失によるリスクを回避し、社外でも安心してノートPCを利用できる環境の整備が企業から強く求められているのである。

この問題の突破口となり得るサービスが、2011年秋にも登場する。

今年2月にNTTドコモがセキュリティアベンダーの米シマンテックとの共同開発を発表したもので、3G携帯電話のショートメッセージサービス(SMS)を介して、盗難等にあったPCに命令を送り、使えなく(ロック)してしまう機能が売り物だ。ドコモ以外の通信事業者やPCメーカーなどにも同様のソリューションを提供する動

きがあり、今年から来年にかけて普及が本格化するものと見られる。

ノートPCを再びオフィスの外へ解き放ち、モバイルデータ通信市場の活性化にもつながると期待される、このソリューションの実像を探ってみた。

PC内蔵の盗難対策機能を活用

ドコモなどが実用化を進めているこの情報漏洩対策ソリューションには、インテルの「Intel Anti-Theftテクノロジー(以下ATと表記)というプラットフォームが用いられている。

インテルはCore i5/i7などのPC向けチップセットに「vPro(ヴィープロ)」と呼ばれるクライアント管理機能の搭載を進めている。ATはその機能の1つで、PCのハードウェアに文字通り「盗難対策」機能を実装したものだ。ビジネス仕様のノートPCを中心に搭載が進んでおり、すでに国内で出荷されるPCの約2割がAT対応機となっているという。

ATは盗難や紛失などが発生した際に、該当するPCを遠隔からロックして情報の流出を防ぐ役割を果たす。この機能は大きく3つのパターンで実行される。

その1つが、PCがインターネットな

どのIP網に接続されている場合に、管理サーバーからネット経由で命令を送ってPCを起動できなくするものだ。この命令は「ポイズンピル(毒薬)」と呼ばれている。

2つ目が設定時間によるロックだ。AT搭載PCと管理サーバーとの間では定期的に通信を行っており、一定時間このやりとりが途絶えた場合にロックがかかる。盗難にあったPCがインターネットに接続される確率は高くないので、それを補完する役割を担う。

ATのシステムはCPUコアとは独立したハードウェアモジュール上に実装されているため、PCの電源が入ってなくても時間が来ればロックをかけることができる。

ロックの処理は、このモジュールにより、OS起動のブロック、HDDが暗号化されている場合、そのデータを読み取れなくする形で実行される。実行されると、クライアントPC側だけでは復旧できなくなる。

盗難・紛失したPCが発見された場合は、管理サーバーで生成した復旧用の暗証番号を入力するなどの処置を行うことで容易に復旧させることができる。これがATの大きな特徴となっている。

ATで特に注目されているのが3番目の3G携帯と連携するパターンだ。新たにATに追加された機能で、管理サーバーから3G携帯電話のSMS