シンクライアント方式（TBSラジオ「日本全国8時です」2005．3．10）

今年１月に札幌市の保健所でノートパソコンが１台盗まれて、その中に２万９５００人分の出生、死亡、婚姻、離婚などの情報が入っていたとか、２月には京都大学の大学病院で９台のノートパソコンが盗まれて、その中に２４９名分の患者の情報が入っていたとか、２月には近江鉄道グループの自動車教習所からノ−トパソコンが盗まれて４０００人分の個人情報が流出したとか、さらに３月には茨城県の中学校で６台のノートパソコンが盗まれ生徒１３０名分の成績が紛失したなど、ノートパソコンの盗難が頻繁に起っています。

これらは氷山の一角で、国内には６５００万台ほどのパソコンがあり、そのうち３８００万台ほどは家庭にあると推定されていますが、仮に０・１%が盗難に会ったとしても６万５０００台になり、それによって漏れる情報は膨大なものになります。

これらは数年前から騒がれている「住民基本台帳ネットワーク」のように、氏名、性別、年齢、住所という基礎的な情報だけではなく、成績とか病歴とか離婚とか、個人のプライバシーに関わる情報が含まれていますから深刻な問題です。

先日、タクシーに乗ったときに、座席にライターが落ちていたので、運転手さんに渡したら、ライターの忘れ物も多いが、携帯電話の忘れ物のほうが多いということでした。日本には現在７５００万台ほどの携帯電話が普及していますが、これも盗難や紛失が続出しており、情報が漏れる可能性があります。

４月から個人情報保護法も施行されるので、この情報の漏洩や盗難は慎重に考える必要があります。

様々な対策がありますが、まず原始的な方法はノートパソコンと机を針金で結ぶというものです。ご存知の方も多いかと思いますが、ノートパソコンの側面には電源用や通信用など様々なコネクターが付いていますが、小さな穴だけ空いていて利用方法が分からないものがあります。これはセキュリティホールといわれ、盗難防止用の針金を固定するためのものです。しかし、これではレンチなどで切られてしまえば効果はないし、持ち運ぶときには役に立ちません。

そこで、次の方法は情報を記録しているハードディスクの内容を暗号にして、本体が盗まれても情報を読み取ることは簡単にできないようにするということです。このようなソフトウェアはいくつも販売されていますが、利用が意外に面倒でなかなか普及しないのが実情です。

そこで登場した究極の対策が、パソコンのなかに情報を入れておかないという方法です。空の財布であれば、盗まれても財布の損失だけで、お金やクレジットカードの被害はないということになります。

このようなコンピュータが今年の２月に日立製作所から発売されました。これは簡

単にいえば、通信機能だけをもった端末装置から通信回線を経由して会社などにあるコンピュータやサーバーを操作するという仕組みです。専門用語では「シンクライアント」方式といわれ、以前から存在しているのですが、商品として発売されたのです。

これは通信回線がブロードバンドになり、大量の情報を迅速にやり取りできる状態になったために実用になってきたのですが、色々な利点があります。

第一は、もちろん盗難に対する対策ですが、第二に、端末のコンピュータのメンテナンスが簡単になることです。最近の複雑なソフトウェアの調子が悪くなると、素人では簡単には回復できあせんが、この方法であれば、会社にあるコンピュータを専門の人間がメンテナンスしていればいいということになります。

第三に、ソフトウェアのバージョンアップも簡単になります。例えば、何百台ものノートパソコンを使用している会社では、一台一台のソフトウェアを変更しようとすると面倒ですが、この方法であれば、親元のコンピュータのソフトェアを変更するだけでいいのです。

第四に、ハードディスクのデータの破壊や消滅も防ぐことができます。私もノートパソコンのハードディスクが壊れて苦労したことがありますが、親元のコンピュータでバックアップをしていれば、このような問題も防げます。

そして、ウィルス対策やハッカー対策もまとめてすればいいということになります。すでに数年前からＡＳＰ（アプリケーション・サービス・プロバイダ）という名前で、このようなサービスを提供する会社が増えてきていますが、通信回線の容量が増大する一方、コンピュータに詳しくない一般の人々がコンピュータを利用する社会には、このシンクライアント方式が重要になると思います。