日銀マンのＩＴ企業見聞録

第４回
端末のシンクライアント化

日立製作所 情報・通信システム社
経営戦略室 担当本部長
岩下 直行

84年日本銀行入行。日銀金融研究所で金融分野における情報セキュリティ技術研究に従事し、同研究所・情報技術研究センター長、下関支店長を歴任後、現在は日立製作所に出向中。

出向してきた初日、一台の端末装置を渡された。ノートパソコンにしてはずいぶん軽い、不思議な端末だ。これは画面表示と文字入力の役割のみを果たすもので、シンクライアント端末と呼ばれる。ハードディスクは装備しておらず、メモリーも最低限しか積んでいない。いわゆるパソコンの本体部分の機能は、社内のネットワークを経由した先、遠く離れたデータセンターのサーバーのなかにおかれている。

日立では、ほぼ全員が、この端末を利用している。金融機関でも、大手を中心に情報漏洩対策として導入している先があるが、これだけ大規模かつ実直にシンクライアント化を徹底している企業もめずらしい。

この端末を使用している限り、ソフトウェアのバージョンアップやウィルスチェックの操作は不要だ。サーバー側で自動的に実施されるからである。文書データもすべてサーバー内に格納されていて、ＵＳＢメモリーなどに吸い上げることは不可能なつくりだ。

メール、スケジューラ、ブラウザ、ワード等を含む自分の作業環境はサーバー上に存在する。社員は個人端末を持ち運んで会社からも自宅からもアクセスできるし、ＵＳＢ型の認証キーさえあれば会議室の共用端末で自分の作業環境を呼び出すこともできる。万一災害等で在宅勤務が必要になっても、普段と変わらない環境で作業できるのは大きい。

ただし、端末とサーバーとの間は、ある程度高速の回線で接続していることが必要だ。たとえば、出張先からモバイル接続すると反応の遅さにイライラするし、滞在したホテルで提供される通信サービスの品質が低いと使い勝手が悪くなる。そんなリスクを抱えつつも、全員でシンクライアント端末を利用し続けているのは、情報漏洩対策のためである。かりに端末を外部に持ち出した際に盗まれてしまったとしても、サーバー側に格納されている情報が漏洩することはないからだ。

一方、ちょっとした外出の際には、スマートフォンに持ち替えて業務データにアクセスしている。会社支給のスマートフォンには、万一紛失したときに情報を消去したり、イントラネットに暗号通信でアクセスするための機能が組み込まれている。携帯電話の３Ｇ回線を通じて、社内メールの添付書類を閲覧したり、自分や同僚のスケジュールを確認することも容易だ。イントラネットで社内専用のＳＮＳを閲覧することもできる。シンクライアント端末と同様に、スマートフォンも端末に情報を残さない運用となっている。

社内システムへの多様なアクセス手段を提供している企業は多いが、セキュリティと使い勝手を両立させることは容易ではない。日立の社内環境は、標準的なサービスとして社員に提供されており、複雑な操作なしに高いセキュリティを実現できている事例として参考になると思う。

※本稿は筆者の個人的見解であり、所属企業その他とはいっさい関係がない。