FM実践講座 オフィス改革⑤

ワークスタイル変革を可能とする情報セキュリティ対策

●文●ワークプレイス・リサーチ・センタ　代表　小田 昆古氏

新聞紙上を賑わす個人情報漏洩事件。一度でも起きれば損失は計り知れず、結果、PCの社外持ち出しを禁止するなど、過剰とも言える対策を講じる企業が増えている。一方で、時間や場所に縛られない新しい働き方、“どこでもオフィス”を積極的に推進し、生産性を高める企業もある。今号では、情報セキュリティの在り方、考え方について、ワークプレイス・リサーチ・センタ代表 小田 昆古氏に先進的事例を紹介していただいた。

はじめに

FM実践講座

“どこでもオフィス”という言葉が最近はやっている。情報化が進み、ノートブックPCを持っていれば、街中では無線LAN、家ではADSLや光ファイバーで高速な通信やデータ処理が可能な時代となった。

企業も生産性の観点から、フリーアドレスや在宅勤務などで、従業員の仕事の内容や生活に合わせた働き方を推進している。次世代育成支援法も、このようなフレキシブルな働き方を積極的に採用することを勧めており、官民あげて支援している。

反面、最近のウィニーのウイルス問題や、企業の機密情報・個人情報の漏洩など、PCを媒体とした犯罪やトラブルも増加している。このため、ノートブックPCの社外持ち出しを禁じ、会社の仕事はオフィス内に限定する企業も現れている。

しかし、この流れは時代に逆行している。

一方で、長年、モバイルワーク（どこでもオフィス）を積極的に推進して、業績を上げている企業がある。また、ワーク／ライフ・バランスの観点から、在宅勤務やフレキシブルな働き方がこれからの経営に重要であるととらえ、生産性と社員のモチベーションアップにつなげている企業もある。

このような企業では、ウイルスや情報漏洩の問題にどう対処して、どうクリアしているのか検証してみたい。

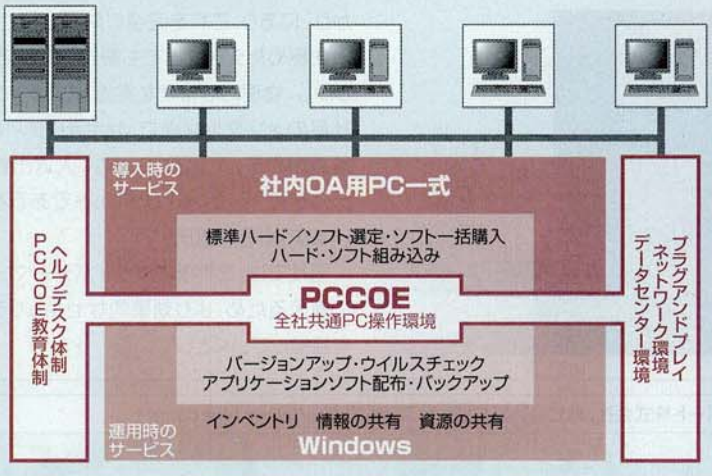
日本HPの例

FM実践講座

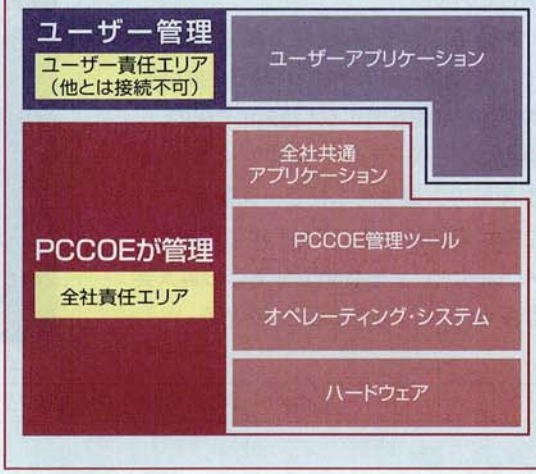
日本ヒューレット・パッカード（日本HP）は、1990年代からモバイルワークに取り組み、フリーアドレスも1995年に採用した。しかし、当時はLAN環境の未整備などもあって、一度は失敗を経験している。

2000年に営業、サービスサポート部門を中心に、「Next Generation Workplace(NGW:次世代ワークプレイス)コンセプト」を前面に押し出し、モバイルワークを全社的に導入した。現在は、全社員固定席なしを前提に、ハンディキャップやコールセンターなど例外的に固定席を必要とする人を特定するという方法にして、フリーアドレスを推し進めている。もちろん、ここではノートブックPCは必須である。

■図表1／PCCOEの仕組み（日本HP）



■図表2／PCCOEの管理する内容（日本HP）



90年代にPCCOE導入

FM実践講座

まだデスクトップPCが主流だった1990年の初期、"PCCOE(PC Common Operating Environment)"という「全社共通PC操作環境」が米国のHPで始まり、日本HPには1993年に導入された(図表1)。

この仕組みが、ウイルス対策や情報漏洩防止に効果的だということは、当初あまり予想していなかった。しかし、数年後から始まったNGWの展開において、これが大きな支えとなった。今では、大企業を中心に同様のシステムが普及しつつあるが、十数年前には画期的な仕組みであったと言えるだろう。

PCCOEとは、PCを使うユーザーに提供される共通の標準環境。アプリケーションソフトは会社が推奨するものを、本部がネットワーク経由で配布・管理し、適切なバージョンアップも本部からまとめて行われる。ハードウェアであるPCも、PCCOE標準環境が装備されたものが提供される。これによって、特殊なアプリケーションソフトは排除され、ウイルス対策も、本部によって全HPに対し一括して行われるので、対策も迅速、効果的。個人が対策し忘れたため蔓延するという心配もない。また、社員が使っているPCは特定されているので、ネットワークにつながっているPCをチェックすることによって、不適切な使い方やアクセスをしている人には即、注意を促すなどの対応もとれる(図表2)。

情報を守るために、PCを立ち上げるときのパスワード、社外から社内ネットワークにつなぐときに必要な暗証番号がアトランダムに変わるワンタイムパスワード、その先の機密情報や人事情報にアクセスを許された人を特定する認証機能と、セキュリティチェックにも厳しい。ノートブックPC内部のハードディスクに入っているデータを守るためには、ドライブロックというガードシステムがあり、ハードディスクに暗号がかかっていて、他人は中身を見られないようになっている。万一、PCが紛失または盗難されても、パスワードを知らなければデータ漏洩はないので安心だ(写真1)。

「性善説」に立った社員教育

FM実践講座

社外へ、そして社外からのガードは万全としても、内部の人間がその気になれば、USBスティックなどを用いて、ある程度の機密情報を持ち出すことは可能だ。これをどう防ぐか。日本HPでは、性善説に立った社員教育に重点を置いている。ここには、「人は良い環境に置かれれば、良い仕事をする」という"HP Way"が貫かれている。

従来からあったStandard Business Conduct(SBC:企業倫理教育)に加えて、「情報セキュリティ eラーニング」で、年に

■写真1／ドライブロックされたPC

数回以上の頻繁な教育を実施している。受講したか、理解したかのチェックはもちろん、定期的に社内監査があり、教育する側もされる側も、その状況を評価され、プロセス不備の場合は社長までレポートされる仕組みにもなっている。

ここで言う「性善説」、「良い環境に置く」とは、放任することではない。きちんとマネージする仕組みがあってこそ、成り立つ言葉なのだ。

同社は、これまで10年以上にわたりモバイルワークを実践しているが、セキュリティ上のトラブルは、PCそのものの紛失以外にはないという。きちんとした管理体制と社員教育がなされれば、新しい働き方を進められる好例である。

日本テレコムの例

FM実践講座

日本テレコムは、2005年にそれまで分散していた本社オフィスを統合して、汐留に移転した(写真2)。1984年創業、旧国鉄の鉄道電話網を一般の通信回線に利用する新しい通信システムをビジネスの主眼に据えた、古くて新しい会社だ。今はソフトバンク・グループの企業として、「21世紀のネットワーク社会におけるライフスタイル、ワークスタイル、ビジネスモデルを提案し、最先端の技術を使い、その実現を推進する」ことを事業ビジョンに掲げている。

ここで働く人は、これからの知識社会にふさわしい、創造的かつ効率的なワークスタイルを実践することを求められている。時間や場所の制約がなく、ワーク／ライフ・バランスをベースとした、社員の自立した働き方ができる会社でもある。在宅勤務を中心とした仕事と生活のバランスの中で、何がメリットで何が障害となるか、"ライフスタイリスト"という実験も行っている。最近の社員調査によれば、汐留移転後の働き方変革に伴い、「大幅な効率アップが実現している」と実感している社員も多く、モチベーションも高まっている。

日本テレコムでは、ノートブックPCが仕事の唯一のツールと言ってもよく、書類の保管はすこぶる少なく、個人の文書キャビネットもない。仕事上のデータはすべてサーバもしくはPCの中。こ


■写真2／日本テレコムのモバイルワーク・オフィス（汐留本社）

れが無くなったらおしまいである。当然、それぞれのデータのバックアップシステムもきちんと整備されている。

このような環境の中で働く社員にとって、社外から会社の情報システムにアクセスすることは日常茶飯事である。情報漏洩や機密情報保護には、どのような工夫がなされているのだろうか?

機密情報は完璧にブロック
FM実践講座

日本テレコムは、日本HPと同様、アプリケーションソフトの標準化、標準PCの提供を行っている。特別なアプリケーションソフトを部門が要求する場合は、情報管理部門が評価したうえ、標準ソフトに加えるか否かを判断する。同時に、社内外からサーバへの接続はVPN（Virtual Private Network:インターネット上の拠点間を専用線のように接続し、のぞき見や改ざんなどの不正アクセスを防ぎ、安全な通信を可能にする技術）を導入し、検疫装置を使ったウイルスチェックを定期的に行っている。

そして、日本テレコムのセキュリティ対策の特徴として挙げられるのが、守るべき情報を物理的に強固にガードしていることだ。経営活動と情報管理を両立させるために、「守秘義務がシステム的に遵守」され、さまざまなインシデント（不測事態）から来る「業務活動の停止を最小限」に抑え、さらに「スタッフの能力が最大限に発揮」されることをコンセプトとしている。そこで、機密情報をレベル分けすることによって、何もかも「機密」扱いにする傾向に歯止めをかけている。

レベル1と2はオープンな情報を取り扱う「OAクライアント・ネットワーク」と名づけられたエリアで、ここまでは、社員証と一体となったICカードをノートPCに挿入し、必要な認証をとって、VPN経由で入ることができる。このエリアのデータで大半の仕事は可能だ。

レベル3以上は、高セキュリティエリアになる。この対象となるのは、顧客に影響のある機密情報（通信の秘密や顧客の個人情報に関するデータ）などである。これらのデータは隔絶された部屋の中に保管され、ガードマンが監視しており、部屋の中のネットワークは、レベル1と2から完全に独立している。当然のことながら、この部屋ではインターネット不可、社外メール不可、あらゆる物の持ち込み・持ち出し不可であり、強固な入退室管理がなされ、万全な情報管理の仕組みが構築されている（図表3）。

ワークスタイルを守るためのセキュリティ
FM実践講座

社内外の場所、時間を問わず、ワークプレイスを自由に選べる働き方の裏には、守秘義務を徹底的に追求した究極の管理体制がある。「社員が自立したワークスタイルを守る」ために、セキュリティ対策を活用しているとも言えるだろう。

日本テレコムでも、社員の情報管理教育には力を入れている。「守るべき情報を扱うのは最終的には人」であり、「人は往々にして迷う」こともあるという「性弱説」を前提に、年4回以上のeラーニング中心の研修を行い、性弱になりがちな人間を正しい軌道にのせる後押しをしている。

社員のモチベーションを高める働き方の改革により、会社へのロイヤリティも高まり、また、オープンにする環境とクローズする環境を分けることによって、リスクマネジメントを進めている同社のやり方は、これからの日本企業にとって参考となるだろう。

全社IT標準管理・社員を信頼・情報活用
FM実践講座

リスク管理の仕組みには違いがあるものの、日本HP、日本テレコムに共通することも多い。まとめてみよう。

①ITをガバナンス（統治）する

アプリケーションソフトの標準化、セキュリティ対策など、情報の保護と管理を、全社統一した仕組みで徹底的に行い、会社としての社会的信頼を維持している。これによって、ウイルス被害、情報漏洩などの被害を未然に防いでいる。

②社員を信頼する「性善説」「性弱説」

情報漏洩を恐れるあまり、PCを持ち出し禁止にするやり方は、「性悪説」に立った考えであり、社員を信頼していないと言っても過言ではない。このような企業は、社員の働き方を活性化させる施策も乏しく、旧態依然とした管理手法をとっているところが多い。性善説も性弱説も「人は良い者、弱い者」と、社員を暖かく見る視点から情報管理教育を考えている。働くための施策も、社員の視点に立っている。

③ビジネスプロセスでの情報「活用」

情報の「保護」に走りすぎると、情報を個別に保持しているだけで活用されず、"活きた"情報にならない。会社全体でIT環境を標準化して管理することは、「使える情報」を見極めることにつながる。バラバラだった情報も一括管理されることにより、「役立つ情報」となる。

オープンにする環境とクローズする環境をきちんと見極め、情報や働き方にやみくもに制約をかけないことが、これからの時代に生き残る企業のやり方であろう。そのためには、全社的に統一したIT環境を構築することがまず第一歩。その結果、現在起こっている情報管理に伴うトラブルを、かなりの確率で防止することが可能になる。

次のシステム"シンクライアント"

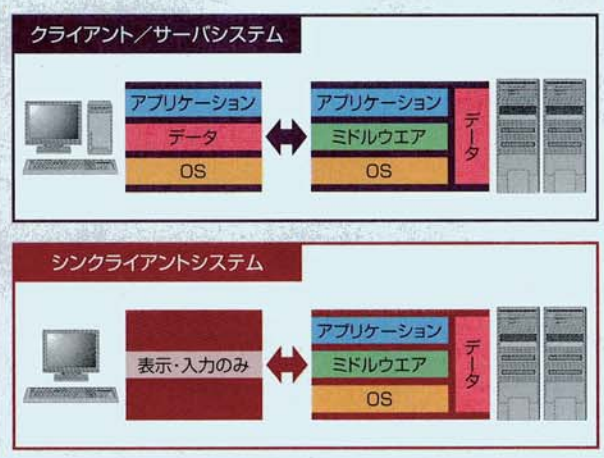
FM実践講座

シンクライアントという情報システムが、いま脚光を浴びている。これまでのPCには、情報処理、データの入出力に必要なWindowsなどのOSやExcel、Word、Outlookなどのアプリケーションソフト、そしてデータ格納のハードディスクが装備されており、ネットワークでサーバと接続して使う。これをクライアント／サーバシステムPCという。

しかし、情報漏洩は、クライアントPCからUSBやハードディスクで持ち出されるケースが多くなっている。一方で、データ処理やメール処理は、自分のPCでないとやりにくい。

これらの問題を解決する方式が、シンクライアント(Thin Client)である。文字どおり、うすっぺらなクライアント端末ということになる。この端末は、表示機能と入力機能しかなく、ハードディスクなどの記録装置も出力装置もないので、USBなどによるデータの持ち出しは一切できない。データは、すべてサーバ側にストレージされている。WindowsなどのOSもアプリケーションソフトもサーバ側にあり、ネットワーク回線でサーバの情報を読み、データ処理を行う。作成し、変更したデータはサーバに保存される。手元にあるのは端末のみ、プレイステーションのコントローラーのような存在だ。電源を切れば単なる端末装置で、盗難されてもデータ流出などの心配はない**(図表4)**。

■図表4／シンクライアント・システム



サン・マイクロシステムズの例

FM実践講座

サン・マイクロシステムズは、1990年代後半から、「Sun Ray」というシステムで、シンクライアント情報システムに取り組んできた先駆的企業である。同社のオフィスには、シンクライアントのマシンが設置され、Sun Ray社員証カードを持った社員なら、誰でもどの端末マシンでも、社員証を端末に挿入することによって、自分の仕事環境を簡単にそのマシン上に実現できる。Sun Rayが設置されている所なら、まさに公衆電話の要領で使うことができる。もちろん、情報漏洩の心配もない。

無線LAN環境が課題

FM実践講座

シンクライアントは、安全性、セキュリティの面からみても、理想的なシステムと思われる。しかし現在は、デスクトップPCかつ有線LAN環境で有効に機能しているという制約がある。ノートブックPCでも可能ではあるが、モバイルワークを考えたとき、無線LAN環境では作業性に難がある。スピードが遅く、この点ではクライアント／サーバシステムPCに軍配があがる。

「どこでもオフィス」は、文字どおり場所を選ばず、が売り物だ。無線LANかつノートブックPCのシンクライアント端末が実用的になったとき、モバイルワークの情景も大きく変わってくるであろう。

筆者プロフィール

小田 昆古(おだ ひこ)

早稲田大学第一商学部卒業。日本ヒューレット・パッカード㈱で、不動産部長、ワークプレイス・ソリューション部門長を、2001年まで12年間歴任。この間、オフィス改革に取り組み、通産大臣賞を含む日経ニューオフィス賞を5回受賞。現在は、ワークプレイス・リサーチ・センタ代表を務めるとともに、BPIA(ビジネスプロセス革新協議会)の「ライフスタイルとワークプレイス研究会」座長として活動。㈳日本ファシリティマネジメント推進協会(JFMA)の前ベンチマークデータセンター長。また、シービー・リチャードエリス㈱FMコンサルティング部のFM戦略顧問も務めている。

○取材・写真協力／日本ヒューレット・パッカード株式会社、日本テレコム株式会社