（4）ノートPCの安全対策

本節では、特に本体そのものが盗難・紛失に遭遇するリスクが高いノート PC について、個人情報保護のためにどのような対策を講じているのか、ということについて取り上げている。

例えば、最も徹底した方法としては、ノート PC そのものの台数を相当程度限定して、ごく一部の従業者にしか認めないような事例（③）を紹介している。

また、万が一盗難・紛失等に遭遇しても、個人情報へのアクセスを許さないために、パスワード等による多重ロックを掛けている事例（①）なども紹介しているほか、さらに携帯電話と同じように、ノート PC に遠隔消去システムを導入して、紛失・盗難時には中の情報を全て消去できるようにしている事例（⑤）も紹介している。

さらに、そもそもノート PC を事業所外で利用することについて、可能な限り限定し、管理を徹底している事例として、データを暗号化済みのノート PC のみに「持ち出し OK」を示すシールを貼ることで誰が見てもチェックができるようにしている事例（②）や、ノート PC 持ち出し時には毎日でも台帳に記入させているような徹底した事例（④）も紹介している。

本節で紹介している取組事例

4-(4)-①：**アクセスロックを多重にかけることで対応**
4-(4)-②：**持ち出し禁止シールを貼って対応**
4-(4)-③：**ノート PC の配布は特定の従業者に限定**
4-(4)-④：**ノート PC の外部持ち出し時は台帳に必ず記載。会社では専用ロッカーに保管**
4-(4)-⑤：**ノートPCに遠隔消去システムを導入**

4-⑷-①【アクセスロックを多重にかけることで対応】

（情報サービス業（ソフトウェア）：約 400 人）

・N 社ではノート PC へのログインには ID とパスワードが必要である。パスワードは英数字 8 文字以上としており、40 日間隔で更新が必要になっている。

・ノート PC には BIOS ロック、HDD ロックが義務付けられている。また、ノート PC には外部との連絡のための電子メールアドレス程度の情報しか入れないようにしている。

4-⑷-②【持ち出し禁止シールを貼って対応】（複合（情報システム／製造）：約 500 人）

・R 社ではハードを暗号化しているパソコンには「持ち出し OK」シールを、そうでないものには「持ち出し禁止」シールを貼付し、注意を喚起している。

・800 台あるノート PC のうち 300 台が持ち出し可能である。これらは HDD の暗号化、BIOS ロック、OS、システムで 4 つの ID、パスワードが必要となっている。4 つの ID、パスワードは月に 1 度変更を求めている。パスワードを紙などに記載することは禁止されている。

4-⑷-③【ノート PC の配布は特定の従業者に限定】

（その他サービス業（教育、学習支援）：約 1,200 人）

・S 社では地区統括の責任者、エリアマネージャーなどの一定レベル以上の者に限定してノート PC を配布し、かつ個人情報保護管理者の許可を得て持ち出している。

4-⑷-④【ノート PC の外部持ち出し時は台帳に必ず記載。会社では専用ロッカーに保管】

（その他サービス業（情報提供サービス業）：大企業）

・β 社ではノート PC を社外に持ち出す際には、持ち出し台帳に必ず記載するようにしており、外勤従業者は、持ち出す度に記帳している。

・ノート PC は外勤従業者のほぼ全員が保有している。

・ノート PC を自宅に持ち帰らない場合には、社内の専用ロッカーに保管するように義務付けている。

4-⑷-⑤【ノート PC に遠隔消去システムを導入】（製造業：約 26,000 人）

・サ社では 2009 年 10 月から、社員にハードディスクの内容を遠隔操作で消去できるノート PC を支給している。

・この仕組みは、暗号化したハードディスクを復号するための鍵を記録しているメモリー部分を遠隔操作で消去することができるというもの。

・消去されると、その旨のレポートが管理部門に送信でされる仕組みになっている。同レポートには最終アクセス日が記載されており、不正アクセスがなかったか確認できる。

・この PC は誤作動が最も危惧されるため、2 重 3 重の保護対策を図っている。