2012 年 8 月 1 日

ネットエージェント株式会社
フォレンジック調査部

個人所有パソコンの確保ガイドライン

情報漏洩の発生源が、従業員の個人所有パソコンや自宅にて利用中のパソコンである可能性が高い場合などに、それらの機器に対する確保ならびにフォレンジック調査を実施するには、以下の項目について確認を行う必要があります。

※下記内容はあくまで参考情報であり、実施するに場合には事前に法務部門または法律の専門家（弁護士など）に相談してください。

1. 同意書の取得

就業規則などにより、個人所有パソコンなどに対するデジタルデータのフォレンジック調査の実施を明確にしていない場合、事後の問題発生を避けるためフォレンジック調査に関する同意を事前に得る必要があります。調査の同意を得る場合、対象となる個人所有パソコンが家族などにより共同使用されている場合、基本的に家族全員の同意が必要となります。

また、対象者から「意味が分からずに署名させられた、よって同意書は無効だ」との抗弁が出ないためにも、何をしようとしているのか事前に十分説明する必要があります。

2. 確保方法

個人所有パソコンを調査対象として確保する場合、関連データの削除やフォーマット、機器の破壊などによる隠蔽工作を未然に防ぐ必要があります。

（1） パソコンの確保前に調査対象者への事情確認や連絡を行った場合、隠蔽工作を行う時間的余裕を発生させてしまい、結果的に調査対象者にとっても不利な状況を生み出す危険性があります。

過去の事例として、上司から事情確認が行われた後で、家人に携帯電話にて連絡を行いデータの削除を依頼したケースがあります。数分間で大量のデータを削除することが技術的に可能である点に注意してください。

（2） 個人宅にあるパソコンを確保する場合、個人宅に調査担当者（上司または責任者・2 名以上）が直接赴く、または調査対象者の帰社時に同行し、事情の説明と同意をその場で得

ます。
パソコンを確保するタイミングは、調査対象者の環境にも配慮し、事前に十分確認しておく必要があります。

(3) 調査対象者の自宅にてパソコンを確保する場合、調査対象者に電源断の作業を行わせるのではなく、調査担当者がシャットダウンする時刻を確認した上で電源を落とします。
パソコンが起動中の場合、可能であれば画面の内容をカメラなどで撮影しておきます。(確保時の作業内容はノートなどに記録しておくことをお奨めします。)
もし、すでにパソコンの電源が落ちている場合には、電源を入れずにそのまま電源ケーブルを抜きます。電源を入れた場合、ハードディスクへの書き込みが発生し、削除ファイルなどが失われる可能性や、タイムスタンプが変化してしまいます。

(4) 調査対象者の所有パソコンが 1 台とは限らないため、
①複数台のパソコンを所有していないか
②外付けのハードディスクや USB メモリの有無
③ネットワークに接続された共有ドライブ(ハードディスク)の有無
④SD カード・CF カードなどのメモリカードの有無
を確認し、未提出の機器がないことをその場で調査対象者に十分に確認します。
また、対象としない機器についても、調査終了までは使用を避けるように確認したほうがよい場合があります。

(5) パソコン本体以外に、外付けの機器(USB 接続のハードディスクなど)が接続されている場合、それぞれの接続ケーブルや電源ケーブルも確保します。特殊なインターフェイスを利用している機器などの場合には、ケーブル類の確保も重要です。

(6) 個人所有のパソコンなどを会社へ移動する際、精密機器であること、証拠データが保存されている可能性があることから、搬送途中に機器やデジタルデータが破損することがないように十分注意する必要があります。
また、搬送などに必要となる緩衝材やダンボール箱なども事前に用意が必要です。

3. 機器の記録

調査対象として個人より一時的に預かる機器は、機器の型番やシリアル番号などを記録しておきます。筐体内部のハードディスクなどを取り外す際は、どの機器に何がどのように取り付けられていたかを記録し、元の状態へ戻せるようにしておきます。

可能であればカメラで前面・背面・シリアル番号、筐体内部などを撮影しておきます。

4. 複製の作成

個人所有のパソコン内のデータを調査する場合、データの改変などを防ぐため、専用の書き込み禁止装置またはソフトウェアを利用して確認するか、専用の複製装置を利用してデジタルデータの完全な複製を作製し、複製したデジタルデータに対して調査を実施します。

これは、調査過程で意図的な改ざんや、捏造を会社が行ったのではないか？といった疑いを防ぐ目的で実施する必要があります。

個人所有のパソコンは、テレビ一体型などハードディスクを取り外すことが困難な機種を利用しているケースがあり、ハードディスクの取り外しにメーカーの保守を呼ぶ必要がある場合もあります。個人所有の機器を破損などから防ぐため販売元の保守を利用することをお奨めします。

5. 機器の保管

一時的に預かる個人所有パソコンなどの機器は、調査が完全に完了するまでは返却することができません。

長期間の保管を必要とすること、個人のデータが保存されている機器であることから預かっている期間中の機器管理は厳重に実施する必要があります。

デジタルデータは破損しやすいため、保管場所や環境としては、強力な磁気などを発生する機器がないかなどを注意する必要があります。

6. デジタルデータの確認

複製したデジタルデータには、個人のプライバシーに関する情報なども含まれるため、内容を閲覧・確認する場合は、調査員など職務上データの確認が必要な限られた人員のみでデータの内容を確認します。

※担当調査員を含む関係者の守秘義務を再確認しておくことをお奨めします。

以上