

企業が個人所有パソコンの保全と調査を実施する場合のリスク

Winny など P2P アプリケーションを、従業員が自宅パソコンで利用中に誤ってウイルスへ感染した結果、企業の業務関連情報（顧客の個人情報・取引先の秘密情報）を P2P ネットワークへ流出させてしまったケースにおいて、企業側が個人所有パソコンのハードディスクを保全（複製）、調査することには以下のリスクを減らす意味があります。

□保全を実施しない場合のリスク

- 1.) 個人所有のパソコンであることから、企業側が長期にわたりパソコンを維持・管理することができません。
企業側が保全を実施し複製を作成していない場合、後日に何らかの争いが発生した際にあらためて調査などを実施することができません。
例えば、従業員が当初は情報流出を認めていたものの、後日になって否認に転じたケースなどにおいて企業側が証拠となるデータを確認できない可能性があります。
- 2.) デジタルデータは改ざんが容易であることから、適切な保全を実施しなかった場合に、意図的にデータを改変する、削除するなどの隠蔽工作をしたのではないかという疑いを持たれる可能性があります。
- 3.) 適切な保全を実施せず、原本のデジタルデータを不適切な状態（書き込みを禁止しない）で調査した場合、調査目的の操作により証拠となるデータの上書きによる消失、タイムスタンプが変化するなど、デジタルデータを改変してしまうことから、企業側が意図的にデータの操作を行ったのではないかという疑いを招く可能性があります。
この疑いは、従業員だけでなく被害者（顧客・取引先）からも向けられる可能性があります。不適切な調査を実施した理由を説明しなければいけなくなる可能性があります。

□調査を実施しない場合のリスク

- 4.) 従業員の説明が正しいかを、個人所有パソコン内のデジタルデータと比較して確認を行わなかった場合、従業員の記憶が曖昧な場合や、説明が誤っていた場合、最終的な報告内容が誤ったものとなり、結果として被害者（顧客や取引先）へ嘘の情報を伝えてしまう可能性があります。
後日、従業員の説明が正しくないことが判明した場合、報告した内容を訂正しなければならず、企業側の信用を低下させる可能性があります。
- 5.) 従業員が気付いてないウイルス感染による情報流出があった場合、企業側がデジタル

データの調査を実施しなかった場合には、結果的にそれを見逃すことになります。

後日、見逃した情報流出が確認された場合、何故その時点で流出範囲を確認しなかったのが問題となる可能性があります。

- 6.) 従業員が勘違いや知識不足などから、自分がウイルス感染し情報流出を発生させたと思い込んでいた場合、関係が無い従業員を犯人としてしまう可能性があります。

以上