物理的安全管理措置

目的

物理的安全管理措置は、以下の点を目的として対処をするものです。

- 物理的区画への不正アクセスによる情報漏えいの防止
- 情報および情報機器の紛失・盗難による情報漏えいの防止

本項では、目的ごとに、概要、求められる要件と手法をご紹介します。

1 物理的区画への不正アクセスによる情報漏えいの防止

自宅の玄関に鍵が無い家はないでしょう。空き巣被害に遭うリスクがあるため、外出する際は鍵をかけるはずです。大切な書類やPCなどがある書斎を考えましょう。夫妻は出入りできて良いでしょうが、子供や子供の友達が勝手に出入りできると、大切な書類が無くなったりするかもしれませんので、できるだけ鍵をかけたいところです。

上の例では、家の中で、家族みんなが入れる場所（書斎以外の場所）、夫妻だけしか入れない場所（書斎）を考えました。そして、書斎を鍵で施錠することを考えました。つまり、区画、アクセス可能者、アクセス制御方法を考えたわけです。これが物理的区画への不正アクセスによる情報漏えいの防止です。事務所でも対処をする必要があることは常識的に理解できるでしょう。

例を加えます。

夫妻の友人が訪問した場合はどうでしょう。やはり夫妻だけしか入れない場所（書斎）は、夫妻の友人も入れないでしょうが、それ以外の場所を自由に入らせて良いか、というと、なかなか難しい問題があるでしょう。もしかすると、親しい友人の場合には「ちょっと見せて」という依頼に、案内という形でならば対応できるかもしれません。友人ではなく、知人、近隣の人という関係人が訪問した場合であるなら、玄関だけで対応することにするかもしれません。つまり、家族以外の人の場合は、その人との関係性をもとに、アクセス権限、アクセス制御方法を決めているのです。事務所でも同様に、外部の様々な関係者が訪問しますので、その際のアクセス権限、アクセス制御方法を決める必要があるのです。

物理的区画への不正アクセスによる情報漏えいの防止では、リスクを低減するため、以下の2点の要件を満たす対処をする必要があります。

- 個人情報の管理区域、取扱区域を定める
- 個人情報の管理区域、取扱区域への入室を制御する

なお、本項では、区画の表記と定義を以下のようにしています。

表記	定義
管理区域	個人情報を保管管理する区域
取扱区域	個人情報を取り扱う事務を行う区域
事務所	当該組織が業務を実施し、訪問者の応対も行う区域

求められる要件と手法

1 個人情報の管理区域、取扱区域を定める

この要件は、物理的な区画に対して、事務所内を業務や業務で取り扱う情報の観点で区分し、適切なアクセス制御を実施することができるようにするためのものです。
管理区域、取扱区域の定義を前述しましたが、実務上、所長および税理士、従業者それぞれの取り扱う情報を区別することは難しいと考えられますので、応接スペース以外の部分を取扱区域と定めて良いでしょう。また、管理区画は必ずしも執務可能な空間（サーバ室など）とする必要はなく、個人情報を保存するサーバを、管理区域と設定してもよいでしょう。
対処の手法と取得できる記録をご紹介します。

手法の例	取得できる記録の例
オフィスマニュアル、取扱規程上に明示する	-
オフィスのレイアウト図や建築図面を利用して明示する	-
オフィスの床、壁などに明示する	-

管理区域、取扱区域は、フロアの床や壁に明示して定義することもできます。ビニールテープで区画を明示しても良いでしょう。ただし、定義をして、後述する入室制御の対処を講じ、全員が理解できるように周知を行うことが必要です。

2 個人情報の管理区域、取扱区域への入室を制御する

この要件は、誰が、どこに、どのような方法で入るのかという点を決め、入ることができる権限を持つ人だけを入室させることで、不正なアクセスを防止できるようにするためのものです。
この要件で重要なのは、制御する仕組みが機能することです。扉は必須ではありません。「外部の人が事務所に来訪した際には従業者が声をかけること」というルールを徹底すれ

ば、不正にアクセスすることは難しくなります。大規模な組織では、声をかけるルールの徹底は難しいかもしれませんが、小規模の事務所であれば可能でしょう。
対処の手法と取得できる記録をご紹介します。

手法の例	取得できる記録の例
従業者証（入館証)、来訪者証での識別	来訪者証の貸出管理簿
有人での監視 - 警備員による監視 - 従業者、所長による監視	来訪者管理簿
施錠扉の設置 - 物理的鍵の扉 - ICカード認証式の扉 - 暗証番号式の扉 - 生体認証式の扉	入室記録 鍵の貸出記録
情報システムのサーバ室への格納、サーバラックへの格納　など	入室記録 鍵の貸出記録

誰が、どこに入れるのか、という点を管理するために、特に従業者の多い事務所では、管理簿などでアクセス権限を設定することが必要になるでしょう。管理簿を作成する場合は、従業者の配属や異動等を反映するとともに、定期的に棚卸を実施し、管理簿を維持してください。

なお、入室の制御が十分でない場合には、盗み見を防止するために、以下の手法を加えることも有効です。

- フロアレイアウトの見直しによる導線の変更
- ディスプレイフィルタの設置
- パーテーションの設置

2 情報の紛失・盗難による情報漏えいの防止

懇親会の幹事役になったと仮定しましょう。懇親会費用を集める場合には会費が間違いなく受領できるように、保管する時は人目に触れないように、使う場合には持ってくる時に落とさないように、気を使うはずです。
「金庫内に入れていれば何の問題もない。」と考える方はいないでしょう。集めるときも、持ち出す時も注意をする必要があり、清算が終了するまで安心できないからです。
情報も同じです。集める、使うまたは渡す、保管する、廃棄する、というプロセスがあります。（これを情報のライフサイクルと呼びます。）情報が紛失したり、盗難に遭ったりすることを避けるためには、保管だけではなく、集める場合、使う場合などを考慮して、対処を考える必要があるのです。

上の例では現金を使いました。他の例として、会社のクレジットカードを預かることになった場合はどうでしょう。小切手を顧問先から預かることになった場合はどうでしょう。もちろん注意はすると思いますが、持ち運ぶ方法や、無くした場合に備えて実施すること、無くした場合に実施することなどは同じではないでしょう。形態に応じて注意すべき点が異なるからです。

情報も同じです。情報は、紙、サーバ、PC、記憶媒体などの形態をとっており、それぞれの形態で保管、持出し、廃棄などの際の注意すべき点が異なります。先ほどの金庫の例と同じように、情報がサーバの中に記録されている状態だけを考えて対処しても、持出し時や廃棄時等の対処が考慮されていなければ、情報が漏えいするリスクは低減できないのです。

情報の紛失・盗難による情報漏えいの防止では、ライフサイクルの段階（取得、流通、利用、保管、廃棄）と、対象（サーバ、PCなどの情報機器、記憶媒体、紙など）とを考慮して、リスクを低減するため、以下の6点の要件を満たす対処をする必要があります。

- 情報の取得時に情報の保有期間を定める
- 情報の流通、利用時に使用する情報機器、媒体を明確にする
- 情報の流通（持出し）時に容易に個人情報が見えない仕組みを整備する
- 情報の流通（移送）時に委託する場合に追跡可能な仕組みを整備する
- 情報の保管時の紛失・盗難防止の仕組みを整備する
- 情報の廃棄時に容易に個人情報が見えない仕組みを整備する

求められる要件と手法

1 情報の取得時に情報の保有期間を定める

この要件は、個人情報が利用目的を限定して取り扱うものであるため、利用目的を達成した個人情報は、削除または廃棄を行うことが妥当なことから求められます。個人情報保護法では明確に定められていませんが、マイナンバー法では、明確に利用目的を制限していますので、提供者との契約事項または所管法令に準じて必ず設定をしましょう。

手法の例	取得できる記録の例
個人管理台帳等を整備して、所有する情報資産を把握する	個人情報管理台帳

2 情報の流通、利用時に使用する情報機器、媒体を明確にする

この要件は、業務で使用するPCやUSBメモリ、CD-Rなどを洗い出し、利用する機器、媒体の意図しない増減の把握、紛失時の早期発見、媒体に応じた適切な対処などを実施することができるようにするためのものです。

必ずしも管理簿を新たに作成する必要はなく、固定資産の管理、備品管理などの管理簿が存在していれば、それを利用することで問題はありません。どのような管理簿を利用する場合でも、PCや媒体の購入、廃棄などを反映するとともに、定期的に棚卸を実施し、管理簿を維持する必要があります。

手法の例	取得できる記録の例
機器管理簿等を整備して、所有する機器を把握する	機器管理簿
記憶媒体管理簿等を整備して、所有する媒体を限定、把握する	記憶媒体管理簿

3 情報の流通（持出し）時に容易に個人情報が見えない仕組みを整備する

この要件は、情報を情報機器、記憶媒体、紙などの形態で持出した際に、紛失しても、それを拾った人によって中身を確認されないようにするためのものです。
情報が入った情報機器、記憶媒体、紙などを持ち出す場合には、相応の注意をして持ち出すと思いますが、それでも電車内に置き忘れたり、ひったくりや置き引きにあったりすることがあります。この場合も含めて、中身の情報を守る対処をする必要があります。
情報機器、紙など形態毎の対処の手法をご紹介します。

形態	手法の例
情報機器 記憶媒体	情報にパスワードを設定、もしくは暗号化する
	情報機器にパスワードを設定、もしくは記憶領域を暗号化する
	生体認証装置付の情報機器、記憶媒体を利用する
紙	外から中身が透けて見えない封筒を利用する
	個人情報に該当する箇所に目隠しシールを張る
	紛失、盗難にあった場合でも、中身が取られないようにするために施錠できる鞄を利用し、鍵は鞄とは別に保持しておく

本手法は、実施した記録を正確に取得することが難しいため、運用をチェックする際には、持出管理表等やヒアリングや目視確認などを実施するようにしてください。

4 情報の流通（移送）時に委託する場合に追跡可能な仕組みを整備する

この要件は、移送の途中で紛失、盗難が発生した場合でも、被害にあったことを早期に検知し、責任の所在を明確にするためのものです。
対処の手法と取得できる記録をご紹介します。

手法の例	取得できる記録の例
セキュリティ便を利用する	配送記録（配送伝票）
書留郵便を利用する	配送記録（配送伝票）

5 情報の保管時の紛失・盗難防止の仕組みを整備する

この要件は、事務所内のサーバや情報機器、記憶媒体、紙が、無くなったり、盗まれたりしないようにするためのものです。また、情報機器、記憶媒体の場合は、記録されている情報が盗まれないようにすることも必要です。
紙や記憶媒体などが盗まれることを防ぐためには、施錠保管することが一般的に採られる手法です。施錠保管できない情報機器が盗まれることを防ぐためには、情報機器を固定することが考えられます。監視カメラを設置して記録を取得することも有効です。
情報機器、紙など形態毎の対処の手法と取得できる記録をご紹介します。

形態	手法の例	取得できる記録の例
情報機器	情報機器をセキュリティワイヤ等で固定する	-
	施錠保管する	-
	私物、情報機器、記憶媒体の持ち込みを制限する - 荷物検査の実施 - 私物保管ロッカーの設置	-
	不要なUSBポート、ディスク挿入口を物理的に封鎖して、媒体、情報機器への書き出しを制限する	チェックリスト 点検票
	書き出しを制御するソフトを利用して、媒体、情報機器への書き出しを制限する	ソフトのログ
	監視カメラを設置する	監視カメラの記録
記憶媒体	施錠保管する	-
	監視カメラを設置する	監視カメラの記録
紙	施錠できる書庫等に保存する	-
	監視カメラを設置する	監視カメラの記録
	クリアデスクを徹底する	-

監視カメラや、書き出し制御のソフトを利用するといった機器やソフトなどを利用する手段以外では、実施した記録を取得することは難しいでしょう。運用をチェックする際に、ヒア

リングや目視確認などを実施するようにしてください。

6 情報の廃棄時に容易に個人情報が見えない仕組みを整備する

この要件は、廃棄した情報機器、記憶媒体、紙などから情報が漏えいしないようにするためのものです。
PCの中に記録された情報は、通常の方法でゴミ箱から削除しても、情報を復元できます。また、紙データはシュレッダーでの裁断処理や焼却処理を行わなければ、情報を見ることができる状態にあります。廃棄をする予定の機器や紙は、特に注意が緩んでしまいがちになりますので、廃棄予定のもの、廃棄後のものから情報が漏えいしないように、適切に対処をしてください。
対処の手法と取得できる記録をご紹介します。

形態	手法の例	取得できる記録の例
情報機器 記憶媒体	ソフトウェアを利用して削除した後に廃棄する	削除記録
	物理的に破壊した後に廃棄する	廃棄物の受領記録 廃棄記録
紙	シュレッダーの利用による廃棄	-
	溶解、焼却などの処理を委託する	受領記録

紙の焼却、溶解などは各事務所で実施できない手段であるため、廃棄の委託をすることとなります。安全に廃棄することを宣言し、記録を残すことができる廃棄業者に委託することを確実にしてください。