情報セキュリティマネジメント試験合格講座 午後試験対策 04

- 物理的管理

1. 物理的な保護と入退管理
   許可された者以外の重要情報の格納場所や取り扱う領域などへの侵入などを物理的に保護する境界を定めて、重要情報や情報システムを壁や入退管理策によって保護しなければならない。

2. どのようなリスクがあるのか？
   重要情報を格納する装置や重要情報を扱う PC などの情報機器に許可のない者が触れることができると、それら情報機器が破壊されて業務を妨害されたり、重要情報が盗まれて漏えいしたりする恐れがある。また、それらの情報機器を操作されることで重要情報の漏えいまたは消去の恐れがある。特に、重要情報の格納装置および記録媒体は、破壊されると業務が継続できなくなる恐れがあるため、入退室管理が厳しいサーバルームなどで厳重に保護することが必要である。

3. 対策のポイント
   例えば、重要情報の格納場所や取り扱う領域などを明確にし、これらの領域に入ることができる役職員や運送業者などの外部者を制限するために、物理的に保護することが必要である。

   (1) セキュリティを強化すべき物理的領域を定め、領域ごとに管理する情報資産の重要性に応じて順守すべきセキュリティ上の規程を整備する。例えば、サーバルームへの入室の際に IC カードやバイオメトリクスによる認証を行うようにする。

   (2) 役職員や運送業者などの外部者によって、重要情報が不正に持ち出されないように出入り可能な領域を決めて領域ごとに入退出管理をする。例えば、運送業者はロビーまで、取引先は応接室まで、役職員は共用エリアと業務フロアまでというようなセキュリティポリシを策定する。また、サーバルームなどへの入室はシステム管理担当者などの資格のある者だけが必要な場合のみ、サーバルームの管理者（責任者などを含む）の許可を事前に得て入室するものとする。

(3) 各入退出管理ポイント(各管理エリアの境界)では、内部不正の防止および発生後の犯人追跡のために、入退出の記録を取ることが必要である。また、入退出の証跡を残すことを目的とし、顔写真などの「個人を特定するための記録」を取ることで、より高い内部不正抑止効果が期待できる。この場合、「入退出の記録」と「個人を特定するための記録」は、定期・不定期に監査を行って照合する。

(4) 重要情報にアクセス可能な物理的領域については、無人時における不正侵入も考慮することが必要である。例えば、機械警備システムや監視カメラを導入し、建物の開錠(最初入場時)・閉錠(最終退出時)における警備システム操作者の記録については、顔写真などの個人を特定するための記録も取ることが望まれる。

(5) 重要情報を格納する装置は、必要に応じてネットワークから隔離された環境を用意するなども考慮することが必要である。

4. 情報機器および記録媒体の資産管理および物理的な保護
PC などの情報機器および携帯可能な外部記録媒体は、盗難や紛失などがないように管理・保護しなければならない。また、不要になった情報機器や記録媒体を処分する際には重要情報が完全消去されていることを確認しなければならない。

5. どのようなリスクがあるのか？
情報機器および記録媒体が管理されていないと、盗難や紛失をしやすい環境であるだけでなく、盗難や紛失を発見でない。また、情報機器を物理的に保護していないと、盗難によって重要情報が漏えいしてしまう恐れがある。

6. 対策のポイント
保護すべき重要情報を扱う情報機器および記録媒体に求められる対策を規定し、情報機器および記録媒体の盗難および紛失、並びに、処分を考慮して管理や保護を行うことが必要である。

(1) 情報機器の紛失などを発見できるようにするために、台帳などで設置場所や使用者を管理し、定期的に棚卸(資産の有無の確認)を実施する。

(2) 情報機器はセキュリティワイヤーなどで机などに固定することが望まれる。また、携帯可能なモバイル機器や、USB メモリなどの携帯可能な記録媒体は棚や机などに施錠保管する。

(3) 重要情報の格納サーバやアクセス管理サーバなどの情報機器は、管理者以外が触れられないように、入退出管理が厳しいサーバルームなどの場所に設置する。

(4) 情報機器および記録媒体を処分する際は、HDD や USB メモリなどの記録媒体から重要情報を復元できないように完全消去する。さらに、CD-R、DVD-R などの記録媒体は破砕機などを用いて物理的に破壊することが必要である。

7. 個人の情報機器および記録媒体の業務利用および持込の制限
個人のノート PC やスマートデバイスなどのモバイル機器および携帯可能な USB メモリなどの外部記録媒体の業務利用および持込を適切に制限しなければならない。

8. どのようなリスクがあるのか？
個人の情報機器および記録媒体を業務利用すると、個人の情報機器および記録媒体の組織による管理が困難であることや、個人と組織の情報がともに扱われることから、ウイルス感染や操作ミスなどによって重要情報が漏えいする可能性が高くなる。

また、内部不正の発生後の調査において、個人の情報機器および記録媒体の提供を承諾してもらえずに、調査が困難になる場合がある。重要情報を取り扱う業務フロアなどの領域に個人の情報機器および記録媒体を持ち込まれると、個人の情報機器や記録媒体に重要情報を格納して持ち出される恐れがある。

また、カメラ付きの情報機器であれば、重要情報を写真に撮って持ち出される恐れもあり、通信可能な情報機器であれば、重要情報を外部に送信される恐れもある。

9. 対策のポイント
個人の情報機器および記録媒体の業務利用および持込を制限する場合、その場所で扱う重要情報の重要度および情報システムの設置場所などを考慮することが必要である。具体的には、以下の内容を定めて運用する。

(1) 個人の情報機器および記録媒体の業務利用を許可するか否かを検討する。

(2) 業務利用を許可する場合には、利用する業務範囲および順守事項などのルールを整備する。また、業務利用にあたって順守事項などの承諾書をとっておくことが望まれる。

(3) 個人の情報機器を組織ネットワークへ接続することを許可する場合には、情報セキュリティ対策を実施した機器のみ許可する。

(4) 個人の情報機器において重要度の高い情報を扱う場合には、必要に応じて重要情報を管理できるソフトウェアなどを導入して組織側で重要情報を管理できることが望まれる。

(5) 重要情報の重要度により重要情報格納サーバやアクセス管理サーバなどが設置されているサーバルーム、および重要情報を取り扱う業務フロアなどには、個人所有のノート PC やタブレット端末、スマートデバイスなどのモバイル機器、その他の携帯可能な情報機器の持込や利用を厳しく制限する必要がある。

(6) 情報機器の持込を禁止する場所では、持込禁止のポスターなどを貼って警告することが望まれる。

(7) 個人所有の USB メモリなどの携帯可能な記録媒体などの持込を制限する。記録媒体などの利用は会社貸与品のみとする。

(8) スマートデバイスなどのモバイル機器や携帯可能な USB メモリなどの外部記録媒体の利用を制限するソフトウェアを導入することで、個人の情報機器および記録媒体による情報漏えいの対策を講じることが望まれる。

出典:IPA「組織における内部不正防止ガイドライン」 2017 年 1 月改訂(第 4 版)