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 03

- 秘密指定

1. 情報の格付け区分
   重要情報を把握して重要度に合わせて格付け区分し、その区分に応じて取り扱い可能な役職員の範囲(例:職位、職種など)を定めなければならない。

2. どのようなリスクがあるのか?
   顧客名簿や技術ノウハウなどの重要情報とそれ以外の情報を区別しないと、役職員は保護する必要のある重要情報が分からず、重要情報を知らずに漏らしてしまう恐れがある。

   また、重要情報を格付け区分して区分に応じた適切な管理をしないと、対策が不十分であったり、対策にコストをかけすぎたりすることがある。これらの管理ができていないと、不正を犯した内部者の責任を追及できないことがある。また、企業や団体の管理責任を問われることもある。

3. 対策のポイント
   重要情報を把握し、適切に管理するために、以下のことを定める。

   (1) 重要情報の取り扱いを定める。三つ以上に重要度を格付け区分した場合は、重要度ごとに取り扱いを定める。定めた重要情報の取り扱いは、定期的に見直す必要がある。

   (2) 重要情報の管理者を定める。例えば、部門責任者または部門責任者から割り当てられた担当者を管理者とする。また、大規模な組織では、部門ごとに管理者を定める。

- アクセス権指定

4. 情報システムにおける利用者のアクセス管理
   重要情報を把握して重要度に合わせて格付け区分し、その区分に応じて取り扱い可能な役職員の範囲(例:職位、職種など)を定めなければならない。

5. どのようなリスクがあるのか？

情報システムにおいて利用者 ID やアクセス権が適切に設定されないと、本来アクセス権のない役職員に重要情報のアクセスを許してしまい、重要情報を不正に利用される恐れがある。また、逆に業務上アクセス権を必要とする役職員が権限のないために業務を遂行できなくなる。

異動または退職によって不要となった利用者 ID が削除されていないと、役職員および元役職員によって不正に利用されて、重要情報にアクセスされる恐れがある。これらの管理ができていないと、不正を犯した役職員および元役職員の責任を追及できないことがあり、企業や団体の管理責任を問われることもある。

6. 対策のポイント

情報システムにおいて、利用者 ID およびアクセス権を誤りなく設定するために、以下の対策を実施する。

(1) 利用者 ID およびアクセス権の登録・変更・削除に関する承認手順や設定終了報告などの手続きを定めて運用する。

(2) 情報システムには、格付け区分の適用とラベル付けで定めた取扱範囲に基づいて重要情報へのアクセス権が利用者 ID に設定されるようにする。もし、取扱範囲によるアクセス権の設定ができない場合は、格付け区分の適用とラベル付けの見直しまたは情報システムの機能変更を行って対処する。

(3) 重要情報へのアクセス権限を付与すべき者を必要最小限とする。また、アクセス権限を持つ者に付与する権限を必要最小限とし、権限を付与する期間も必要な時期に限って行うこととする。特に、委託先の従業員などに権限を付与する場合は、契約上の措置が必要である。

(4) 利用者 ID およびアクセス権の登録・変更・削除の手続きに漏れがないように、人事異動に関連する人事手続きなどと連携した運用とする。

(5) 利用者 ID およびアクセス権が適切に付与されているかを確認するために、定期的にアクセス権の要件を見直す。例えば、人事異動の時期に一斉に見直すなどを行うことが望まれる。特に、アクセス権限が集中している者に対しては、適切性を確認し、不必要なアクセス権限は削除を行う。

(6) 重要情報を格納している情報システムでは、時間およびアクセス数や量などのアクセス条件による制御を行うことが望まれる。

例えば、時間であれば夜間に重要情報にアクセスすることを制限する。また、アクセス数・量であれば重要情報を一括してダウンロードすると上司などに通知されるようにする。

7. システム管理者の権限管理
システム管理者が複数人いる場合は、システム管理者 ID ごとに適切な権限範囲を割り当てシステム管理者が相互に監視できるようにしなければならない。

8. どのようなリスクがあるのか？
権限範囲を適切に割り当てていないと、例えば、利用者 ID の不正登録および削除が起こることで、不正登録による重要情報の不正使用や、不正な削除による業務妨害などの恐れがある。

一人の管理者に権限が集中している場合は、情報システムの破壊および重要情報の削除などの妨害によって事業継続が不可能となる恐れがある。

9. 対策のポイント
システム管理者による内部不正を防止するために、以下のようにシステム管理者 ID ごとに適切な範囲の権限を割り当て、運用されていることを確認する。

(1) システム管理者を決める際には、高い規範意識などの適性を満たす者を任命する。複数の管理者を任命し、相互に監視できることが望まれる。

(2) 一人のシステム管理者に権限が集中しないように権限を分散する。

(3) 相互に監視するために、作業内容や作業日時などが記載された作業報告を作成して残す。この作業報告を別のシステム管理者が確認することが望まれる。

(4) システム管理者は、特権を必要とする操作以外では特権を用いて操作を行わないようにする。

10. 情報システムにおける利用者の識別と認証
情報システムでは、利用者およびシステム管理者の識別において、共有 ID および共有のパスワードや IC カードなどを使用せず、個々の利用者 ID またはシステム管理者 ID を個別のパスワードや IC カードなどで認証しなければならない。

11. どのようなリスクがあるのか？
情報システムで共有 ID および共有のパスワード・IC カードなどを使用していると、内部不正発生の際に重要情報にアクセスした利用者が識別できないため、内部不正者の特定が困難となる。また、内部不正者の特定が困難なことから心理的に重要情報を持ち出しやすい環境となる。これらの管理がされていないと、不正を犯した内部者の責任を追及できないことがある。また、企業や団体の管理責任を問われることもある。

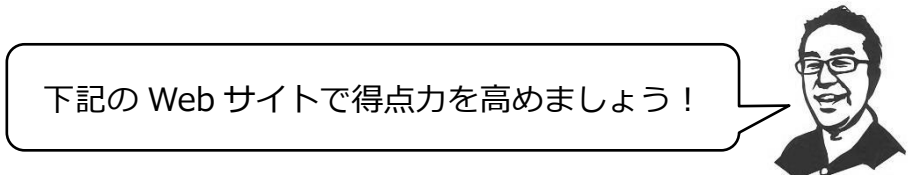
12. 対策のポイント
情報システムでは、利用者の識別と認証を適切に行うために、以下のように利用者 ID やシステム管理者 ID を管理する規程を整備し、運用することが必要である。

(1) 利用者とシステム管理者を識別するために、利用者ごと、システム管理者ごとに利用者 ID、システム管理者 ID を割当てる。そして、利用者 ID およびシステム管理者 ID はパスワードなどで認証する。

(2) 利用者自身の利用者 ID を他の利用者に不正使用されないように、パスワードについては、単純な文字列を設定しないことおよびできれば定期的に変更することなどの管理事項を定めて利用者に実施させる。

(3) 他の利用者に ID およびパスワード・IC カードなどを貸与することを禁止する。

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）



- ✓ **翔泳社「情報セキュリティマネジメント要点整理＆予想問題集」**
- ✓ **情報セキュリティマネジメント試験合格講座** http://rakupass.com/security/