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 05

- 技術・運用管理

1. ネットワーク利用のための安全管理
   組織のネットワーク利用では、PC などの情報機器から重要情報が漏えいしないように、ファイル共有ソフトおよびソーシャルネットワークサービス(SNS)、外部のオンラインストレージなどの使用を制限して安全なネットワーク環境を整えなければならない。

2. どのようなリスクがあるのか？
   情報機器にファイル共有ソフトがインストールされていると、PC 内の重要情報が外部に意図せずに漏えいしてしまう恐れがある。ファイル共有ソフトで取得した外部のファイルを実行することでマルウェアに感染し、組織内の他の情報機器に感染を広げてしまう恐れもある。また、SNS および外部のオンラインストレージの利用並びに掲示板の書き込みが許可されていると、重要情報がアップロードされたり、書き込まれたりして漏えいする恐れがある。

3. 対策のポイント
   組織のネットワークから外部に重要情報が漏えいしないように、情報機器において対策を講じることが必要である。

   (1) PC などの情報機器には、組織内で許可されたソフトウェア以外のもの（例えば、ファイル共有ソフトなど）をインストールして利用することを禁止する。利用を許可するソフトウェアは、組織内で決定する。

   (2) Web アクセスに関しては、コンテンツフィルタを導入して、SNS およびアップローダー、掲示板などへのアクセスを制限することが望まれる。

   (3) 電子メールに関しては、業務のメールを個人のメールアドレスに転送する設定になっていないかを確認する。また、外部宛のメール送信を再確認する機能や上司に承認を要求する機能、および添付ファイルなどが暗号化されていないと送信できないメールシステムなどを導入することで、誤送信による情報漏えいの対策を講じることが望まれる。

(4) PC などの情報機器を守るために、ウイルス対策ソフトの導入やパッチ適用などの一般的なセキュリティ対策を実施する。

- 証拠確保

4. 情報システムにおけるログや証跡の記録と保存
内部不正の早期発見およびの事後対策の影響範囲の観点から、重要情報へのアクセス履歴および利用者の操作履歴などのログや証跡を記録し、定めた期間に安全に保存することが望ましい。

5. どのようなリスクがあるのか？
ログや証跡を記録し、定期的に確認していないと、ログや証跡から不正行為の前兆となる行為を知ることができないため、発見の遅れや、発見時に被害が大きくなっているといった恐れがある。また、ログや証跡が保存されていないと、内部不正が発生した場合に事後対応において、内部不正の原因特定および内部不正者の追跡、影響範囲などの調査が困難になる。さらに、処罰などの根拠や、法的紛争や訴訟になった場合の証拠として認められない場合もある。

6. 対策のポイント
内部不正の早期発見および事後対策の観点から、以下のようにログや証跡を記録して安全に保存する。

(1) ログは、重要情報へのアクセス履歴や、利用者の操作履歴（Web のアクセスログやメールの送受信履歴など）を取得する。

(2) 証跡は、設定したポリシに応じて、上記のログ以外の日時、利用者、操作端末、操作内容、送受信の内容などの情報を取得する。

(3) ログは定期的に確認します。多量なファイルへのアクセスや業務範囲外のファイルへのアクセスなどの通常の業務と異なる事象が発見された者に対して、事象確認または監視強化などの対策を行うことが望まれる。

(4) 利用者のプライバシーなどを考慮して、ログや証跡を収集することを労働組合などと合意をとることが望まれる。

(5) ログや証跡の保存を行っている事実を従業員に通知することは、内部不正の発生を抑止する上で効果的な方法と考えられるため、一般的には、通知することが望まれる。

(6) ログや証跡の保存期間は、リスクとコストのバランスによって決定する。保存期間は、内部不正の抑止の観点から内部者に知らせないことが望まれる。

(7) ログや証跡の確認には、改ざんおよび削除防止並びに特定のシステム管理者からのみアクセス可能などの措置が取られていることが望まれる。確認をする際には、総括責任者またはシステム管理者から許可を得ることが望まれる。

- コンプライアンス

7. 法的手続きの整備
内部不正を犯した内部者に対する解雇などの懲戒処分を考慮し、就業規則などの内部規程を整備して、正式な懲戒手続に備えなければならない。

8. どのようなリスクがあるのか？
内部不正を犯した内部者に対する懲戒処分が就業規則などの内部規程に盛り込まれてない場合や正式な懲戒手続きが整備されていない場合には、内部者から不当処分の訴えにより懲戒処分が無効となる恐れがある。

9. 対策のポイント
懲戒処分を行う場合には、内部規程において懲戒処分および秘密保持義務に関する項目を定めておくことが必要である。

(1) 内部規程には、懲戒処分の対象となる内部不正（例：営業秘密の侵害、個人情報の目的外利用など）に関する記載が必要である。

(2) 内部規程には、秘密保持義務の対象となる重要情報を客観的に特定できる記載が必要である。

(3) 解雇などの懲戒処分は、根拠となる内部規程に基づき、かつ労働法制を順守して処分をすることが必要である。

(4) 適切な懲戒処分を決定するために、査問委員会などによって事実関係を明らかにすることが必要である。

(5) 刑事告発および民事訴訟の法的な手続きに関する内部規程を整備することが必要である。

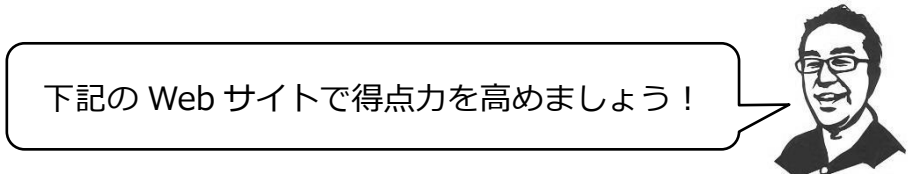
10. 内部不正に関わる事故
JNSA(特定非営利活動法人日本ネットワークセキュリティ協会)の調査報告によれば、2005 年～2010 年の内部犯罪・内部不正行為による個人情報漏えいの発生件数は全体のわずか 1%程度であるのに対して、漏えいした個人情報の数は約 25%程度(全体の 1/4 近く)となっている。

11. 情報の漏えい経路
経済産業省の調査において、営業秘密の漏えいがあった企業では漏えい経路が「中途退職者(正規社員)による漏えい(50.3%)」、「現職従業員などのミスによる漏えい(26.9%)」、「金銭目的などの動機をもった現職従業員などによる漏えい(10.9%)」と報告されている。

競争力につながる価値ある営業情報の漏えいは、内部の関係者によるものが多くを占める。

12. 内部統制との関連
内部不正対策は、会社法や金融商品取引法で求められている内部統制と、リスク管理の面から密接な関係があり、体制の面でも重なる部分もある。このため、既存の内部統制の体制を利用することで効率的かつ効果的な体制構築が可能となる。

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/