

脅威		脆弱性
環境および物理的管理		
①	情報処理施設に不正アクセスされる	部屋への物理的なアクセス制御が不十分
②	不正侵入、情報漏えい	情報処理施設や機器及びオフィス内に対する物理的セキュリティ対策に不備がある(扉が開放) 物理的境界線が不明確。レベル分けが不十分 重要な施設について、フロア内を監視する手段がない 不必要な情報資産や物品が存在している
③	原因追求が困難	サーバ室への入退室のログが取得されていない
④	緊急時避難通路をふさいでしまう	ロッカー、本棚等の耐震設備がなされていない
⑤	機器障害、通信障害	ケーブルや通信機器に対するセキュリティ対策に不備がある(ケーブルの保護、ハブ等の管理)
ハードウェア		
①	情報漏えい	ノートPCがダンボール箱に放置。PCの保管がなされていない(帰宅)
②	PC盗難による情報漏えい	ノートPCが固定されていない
③	機器障害に陥る	重要サーバに対する定期点検が行われていない
④	情報漏洩の危険性がある	重要サーバ・コンソール・PC等やが安全な場所に設置されていない(誰でもアクセス可能な場所にある)
⑤	機器障害に陥る	湿気、ほこり、汚れに対する影響の受けやすさ
⑥	機器障害や情報が漏洩する	サーバ等の設置が強固になっていない
ソフトウェア		
①	立証能力が不足する。許可されていない方法によるソフトウェアの使用	セキュリティ監査・追跡の欠如 アクセス権の誤った設定や設定ミスがある
②	ユーザのなりすまし	保護されていないパスワードファイル 貧弱なパスワード管理(簡単に推測できる、生データのまま保存、不十分な変更頻度)
③	不正アクセスによる情報漏洩、システム障害の危険性がある	アクセス権の定期的な見直しがなされていない
④	セキュリティホールを利用した攻撃を受ける。不正侵入やウイルス感染の危険性がある	セキュリティホールが存在する セキュリティパッチプログラムを適用していない
⑤	新種のウイルス感染の可能性がある	ウイルス対策ソフトが導入されていない、もしくは常駐使用されていない 最新版のウイルスパターンファイルを更新していない
⑥	悪意のソフトウェア	ソフトウェアの管理されていないダウンロードや使用
⑦	オペレーションスタッフエラー	ドキュメントがない。整備されていない
⑧	不許可ユーザによるソフトウェアの使用	適切な消去をしていないサーバやストレージ媒体の廃棄/再利用
通信		
①	盗聴およびネットワーク及びネットワークサービスに不正アクセスされる	保護されていない通信回線
②	情報漏えい	許可されていないモデム使用
③	盗聴、情報の漏洩	無線LANを使用している
④	不許可ユーザのソフトウェア使用	保護されていない公衆網接続
文書管理		
①	窃盗、盗難	保管場所に対して窃盗防止や施錠などの対策ができていない ファイルが棚に無施錠のまま保管されている
②	法令の適用が受けられない。情報の管理がずさんのため、情報漏えいが発生する	重要度に応じた情報資産の廃棄、複写、配布等のルールが明確でない 重要度に応じた情報の分類分けがなされていない 重要度に応じた情報の管理がなされていない
人的管理		
①	不正に撤去もしくは持ち出されることによって情報資産が紛失・改ざん	机上に書類が放置されている
②	セキュリティ対策等が適正に運用されない。	管理者によるチェックがなされていない、もしくは不十分である
③	窃盗、盗難	監督・監視されていない外注業者/清掃業者等の作業
④	情報が漏洩してしまう	セキュリティ教育やトレーニングが行われていないか不十分である
⑤	故意、過失等によりデータや文書を削除、廃棄する	セキュリティ遵守性の認識の欠如
⑥	管理策の実行が不正確か、もしくは管理策が実行されていない	セキュリティに対する責任体制が不明確である
⑦	損害及び被害等が拡大する恐れがある	連絡体制に不備がある
⑧	過去に発生したセキュリティ事故と同じ事故が発生する	情報セキュリティポリシー違反時の罰則規定が不明確
⑨	不許可ユーザによるソフトウェアの使用	離席時にログアウトしない
⑩	不許可ユーザによる情報漏洩および不正使用	スクリーンセーバーが設定されていない。
⑪	ユーザのなりすまし	パスワードの運用が不十分である
⑫	立証能力が不足する。管理責任及び監督責任が十分に果たせない	ユーザIDを複数人が共有使用している。システム利用者本人を特定(確認)できない
⑬	媒体等から情報が漏洩する。ウイルス感染の危険性がある	PC等を外部から持ち込むもしくは持ち出す FD,DVD,USBフラッシュメモリー等を許可なく利用している 記憶媒体の廃棄が不十分である
⑭	プログラムやデータの消失や不正なプログラムが組み込まれる可能性	システム等の変更管理手順が確立されていない
その他		
①	立証能力が不足する。原因分析が行えない	記録類、ログ情報などの収集・保管方法に不備がある
②	情報が漏洩する	委託先の管理があいまいであるか十分でない