

脅威のタイプと一般的な脆弱性の例

※「脅威」のタイプは、ISO/IEC TR 13335-3:1998 附属書 C「考える脅威のタイプのリスク」を参考

※「脆弱性」の例は、ISO/IEC TR 13335-3:1998 附属書 D「一般的な脆弱性の事例」を参考

人為的脅威		環境的脅威
意図的脅威 (D : deliberate)	偶発的脅威 (A : accidental)	環境的脅威 (E : environmental)

一般的な脆弱性の事例

【災害】			
地震			○
洪水	○	○	○
台風			○
落雷			○
火事	○	○	

【故障】			
停電		○	
断水		○	
空調故障	○	○	
ハードウェアの故障		○	
電力の不安定		○	○
極端な温度及び湿気	○	○	○
ほこり		○	○
電磁波防放射	○		○
静電荷			○
記録媒体の劣化		○	○
ソフトウェアの故障	○	○	
ネットワーク構成要素の技術的障害		○	
送信エラー		○	
回線の損傷	○	○	
トラフィックのオーバーロード	○	○	
通信サービスのネットワークサービス障害	○		
故意の損害	○	○	

【人的】			
操作員のエラー	○	○	○
保守のエラー	○	○	
ユーザのエラー	○	○	
資源の誤用	○	○	
爆破行為	○	○	
武器の使用	○		
盗難	○		
記憶媒体の不正使用	○	○	
不正なユーザによりソフトウェアの使用	○	○	
不正な方法でのソフトウェア使用	○		
ユーザ ID の偽り	○	○	
ソフトウェアの違法な使用	○	○	
悪意のあるソフトウェア	○	○	
違法なソフトウェアの輸入・輸出	○		
不正なユーザによりネットワークへのアクセス	○		
不正な方法でのネットワーク設備の使用	○		
盗聴	○		
通信への進入	○		
争議行動	○	○	
ユーザのなりすまし	○		

【その他】			
トラフィック分析	○		
メッセージ経路選択の誤り		○	
メッセージの経路変更	○		
否認	○		
スタッフ不足		○	

洪水の影響を受けやすい地域への建物の配置

バックアップコピーの欠如

不適切なサービス保守の対応

不安定な電力配電網。ハードウェアの電圧変化に対する影響の受けやすさ。

ハードウェアの温度変化に対する影響の受けやすさ

ハードウェアの湿気、ホコリ、汚れに対する影響の受けやすさ

ハードウェアの電磁放射に対する影響の受けやすさ

定期的な交換計画の欠如

開発者のための不明確または不完全な仕様書。効果的な変更管理の欠如。

建物、部屋への物理的アクセス管理の不適当又は不注意な使用。不適切な採用手続。

ソフトウェアの複雑なユーザインタフェース。文書化の欠如。

不十分なセキュリティ訓練。ソフトウェアおよびハードウェアの正しくない使用。

ハードウェアの記憶媒体の不十分な保守／不適当な設置

不十分なセキュリティ訓練

建物、ドアおよびまどの物理的保護の欠如。保護されない文書の保管。

文書廃棄時の注意欠如。管理されない文書のコピー作成。

外部または清掃スタッフによる作業時の監督不在。

ソフトウェアのテストをしない、又は不十分なソフトウェアのテスト。

ソフトウェアの公知の欠陥。アクセス権の誤った割り当て。

ワークステーションから離れる際にログアウトしない。

適切に削除されていない記憶媒体の処理または再利用。

監査証拠の欠如。モニターのしくみの欠如。

ユーザの識別および認証メカニズムの欠如

管理されていないソフトウェアのダウンロードおよび使用。バックアップコピーの欠如。

平文でのパスワードの転送。ダイヤルアップ回線。

遠隔通信媒体およびメッセージ伝達の正しい使用のためのポリシー欠如

保護されていない通信回線。保護されていない重要度の高いトラフィック。

ケーブル接続の欠陥

保護されていないパスワードファイル。不十分なパスワード管理。

送信元および受信者の識別と認証の欠如。

メッセージ送受信の証明の欠如

要員の不在