別紙4　リスク源の例

分類		リスク源の例	該当する「結果を生じ得る事象(脅威)」の例
ハード	システム	システムのバグ放置 機器のリプレース未実施 メンテナンス不足 冗長化の不採用	ハードウェア障害、ソフトウェア障害、ネットワーク障害
		データバックアップの不備 非常用エネルギー設備の未設置	ハードウェア障害、ソフトウェア障害、ネットワーク障害、エネルギー不足、自然災害
		耐震化・耐水化の不備 バックアップサイトの未設置 設備のリプレース未実施	自然災害、設備障害
	セキュリティ	DoS対策の不備 (装置／設定)	サービス妨害攻撃
		不正検知システムの未導入・不備	標的型攻撃、マルウェア、サービス妨害攻撃、ウェブサービスへの不正ログイン
		防犯カメラの未設置	ソーシャルエンジニアリング
		保護されていない通信経路	通信の盗聴・妨害
ソフト	脆弱性対策	修正プログラムの未適用 既知の脆弱性の放置 サポート終了したソフトウェアの継続使用	情報窃取、ウェブサイト改ざん、脆弱性を標的にした攻撃
	接続環境	USB、外部媒体が接続できる環境有	マルウェア、不正利用、不正持ち出し
		誰でもアクセスできる環境有 外部ネットワークへの接続環境有 インターネットへの接続環境有 周辺システムとの連携有 誤操作・意図的な操作ができる環境有 外部からの不正情報を受信できる環境有	標的型攻撃、マルウェア、情報窃取、サービス妨害攻撃、ウェブサイト改ざん、 ウェブサービスへの不正ログイン、データの改ざん、システム破壊、 不正利用、不正持ち出し、乗っ取り
	ルール	不要な人へのアクセス権限の付与 不要アカウントの放置 作業できるオペレーターのID管理不備 パスワード変更の放置	標的型攻撃、情報窃取、ウェブサイト改ざん、ウェブサービスへの不正ログイン、 不正利用、不正持ち出し、乗っ取り
		ネットワーク通信の暗号化不徹底	通信の盗聴・妨害
		廃棄承認ルールの未整備・不徹底	不適切な廃棄
		入退室管理の不備	不正利用、不正持ち出し、ソーシャルエンジニアリング
		機器や情報の不適切な保管 外部業者の本人確認の未徹底 施錠未実施	ソーシャルエンジニアリング
スキル・人材	組織共通	長時間労働	操作ミス、任務怠慢
		社内セキュリティ教育が不十分 セキュリティ意識の欠如	不正利用、不正持ち出し、操作ミス、遺失・紛失、無許可機器の持込、任務怠慢
		安易なパスワード設定 パスワードの使いまわし	ウェブサービスへの不正ログイン、金融情報の不正利用
		機密・重要書類の放置 不在時のPCログイン未設定	ソーシャルエンジニアリング
		不正アプリケーションのインストール 更新・保守作業時にウィルスチェックをしていない	マルウェア、情報窃取、ウェブサイト改ざん、脆弱性を標的にした攻撃
	セキュリティ部門	メンテナンス時の確認漏れ	マルウェア、システム破壊
		情報セキュリティ要員のスキル不足 セキュリティ要件を満たさないコーディング	脆弱性を標的にした攻撃、ウェブサイト改ざん、操作ミス、無意図な情報公開
		情報セキュリティ要員の要員不足 不十分なセキュリティ訓練	標的型攻撃、マルウェア、サービス妨害攻撃、脆弱性を標的にした攻撃