別紙２　結果を生じ得る事象(脅威)の例

結果を生じ得る事象(脅威)			具体例
攻撃に起因する脅威	外部不正	標的型攻撃	アクセス権限のないポート、プロトコル、およびサービスを使用して、攻撃を実施する。
			ネットワーク境界を越えて許可されているトラフィック／データの移動を利用して、攻撃を実施する。
			重要な地位にいる職員の私有のデバイスを狙って侵害する攻撃を実施する。
			基幹業務に関わるハードウェア、ソフトウェア、ファームウェアを狙い、サプライチェーン攻撃を実施する。
		マルウェア	メールの添付ファイルからマルウェアを感染させる。
			ウェブサイトからマルウェアを感染させる。
			エクスプロイトキットを使って、ランサムウェアを拡散させる。
		情報窃取	SQLインジェクション等の情報漏えいにつながる脆弱性を悪用し、機微な情報を取得する。
			OSコマンドインジェクション等のソフトウェアの脆弱性を悪用し、機微な情報を取得する。
			外部ネットワークのネットワークスニッフィングを介して、機微な情報を取得する。
		サービス妨害攻撃	シンプルなサービス妨害(DoS)攻撃を実施する。
			分散型サービス妨害攻撃を実施する。
			標的型サービス妨害攻撃を実施する。
		ウェブサイト改ざん	開発時に作りこんだウェブアプリケーションの脆弱性を悪用して、サイトを改ざんする。
			ソフトウェアの脆弱性を悪用して、サイトを改ざんする。
			管理用サービスに侵入して、サイトを改ざんする。
		ウェブサービスへの不正ログイン	他のウェブサイトから漏えいしたIDとパスワードの組み合わせを利用して攻撃する。
			総当たりのログイン試行／パスワード推測攻撃を実施する。
		脆弱性を標的にした攻撃	公開された脆弱性情報を悪用して、対策をしていない利用者を攻撃する。
			パッチなどの修正手段が提供されていない脆弱性を狙って、非標的型ゼロデイ攻撃を実施する。
			IoT機器の脆弱性を悪用してウイルスを感染させる。
		金融情報の不正利用	インターネットバンキング詐欺ツールによって金融取引関連情報を窃取する。
			フィッシング詐欺をする。
		通信の盗聴・妨害	通信傍受攻撃を実施する。
			無線妨害攻撃を実施する。
			外部に設置された傍受用デバイスを使用して、無線ネットワークトラフィックを傍受する。
		データの改ざん	極めて重要なデータを汚染する、あるいは改ざんする。
			公的にアクセス可能な情報システム上にデータを作成・削除・変更する。
			もっともらしいが偽のデータを組織の情報システムに挿入する。
		ソーシャルエンジニアリング	不在時に他人の机の上にある資料やノートをのぞき見して、機密情報などを収集する。
			ゴミ箱をあさり、不用意に廃棄された資料やメモなどを収集し、目的の情報を取得する。
			機会をうかがって情報システム／コンポーネントを盗んだり、あさる。
		システム破壊	システムを破壊するマルウェアを不正にインストールする。
	内部不正	不正利用	データを不正に操作する。
			機密情報を不正に閲覧する。
			機微な情報を不正に取得する。
		不正持ち出し	機密情報を不正に持ち出す。
			データを意図的に外部に送信する。
		乗っ取り	内部の攻撃者が正規ユーザになりすましてウェブアプリケーションを操作し、セッションの乗っ取りを実施する。
			内部の攻撃者がネットワークトラフィックに侵入して、変更攻撃を実施する。
攻撃に起因しない脅威	自然現象	自然災害	地震が発生する。
			台風が発生する。
			温度・湿度異常が発生する。
			落雷が発生する。
			浸水が発生する。
		エネルギー不足	停電が発生する。
			水不足が発生する。
	障害	設備障害	火災が発生する。
			漏水が発生する。
			動植物害が発生する。
			施設が老朽化する。
			ビル付帯設備(空調機器、入退室管理装置、監視カメラ等)が故障する。
		ハードウェア障害	メモリ、ディスク、CPU、電源装置の障害が発生する。
			ディスクのエラーが発生する。
			機器・ケーブルが劣化する。
		ソフトウェア障害	OSやアプリケーションの潜在的なバグ・過負荷等による異常が発生する。
			資源(メモリやディスクの容量オーバー等)の枯渇により、処理性能が低下する。
		ネットワーク障害	通信の競合により、通信性能が低下する。
			回線(専用・公衆)、通信事業者(接続局、ISP、NOC、IDC等)、通信機器、構内配線の障害が発生する。
	人に起因する脅威	操作ミス	特権ユーザが、極めて重要な情報／機微な情報を誤って露出させる。
			特権ユーザが、他のユーザに例外的な権限を誤って付与する。
			メールを誤送信する／不要なメールを開封する／重要データを消去する。
		遺失・紛失	持ち出し媒体を置き忘れる／管理不備によって媒体を紛失する。
		不適切な廃棄	廃棄した媒体を復元する。
		無許可機器の持込	許可されていない機器、媒体、プログラムを社内ネットワークに接続する。
		無意図な情報公開	ウェブサーバの設定不備により重要データが流出する。
		任務怠慢	既定の操作の実行を忘れる。
		法令・政策の不認識	海外サーバにおいてデータ保管・処理等を行う場合において、認識していない当該地域の法令等による権限が行使される。