演習９　リスク対応として管理策の選定を行う

営業部の「IT 構築サポート課」でリスクアセスメントの結果から、脆弱性として残っている項目や、更なる改善点について、リスク値が受容可能レベル（リスク値≦９）を満たすように対応を検討することにしました。

すでに受容可能レベルを満たしているリスクに関する脆弱性・改善点は、客観的に保有するという判断をしています。

演習８の結果に対して、JIS Q 27001:2006 附属書 A から適切な管理目的と管理策を選び、リスク対応の４つの選択肢（最適化、回避、移転、保有）のどれを選択するかを考えます。

テストケースに示されている「リスクアセスメントマニュアル（抜粋)」の「（７）リスク対応」、「（８）リスク算定シートの作成」の手順に従い、「選択肢」、「管理目的」及び「管理策」の欄を記入し、「管理策に関する考察」の欄に、その管理策を選定した理由や関連する管理策の実施状況などの説明を記述して下さい。

※参考に、教材の「例：適切な管理策の選定」を参照してください。

本演習では、演習８の結果で残っている脆弱性や更なる改善点の関連行のみ、また、リスク算定シートの一部列（リスク対応に必要な部分のみ）を抜粋してあり、最後の２つの脆弱性・改善点については検討結果を記入してあります。

演習９－１．　リスク算定シートの「選択肢」、「管理目的」及び「管理策」の欄にリスク対応として検討した結果を記入し、「管理策に関する考察」の欄に、その管理策を選定した理由や関連する管理策の実施状況などの説明を記述して下さい。

＜リスク算定シート＞　資産 No.13 クライアント PC（ノート PC 本体)、管理組織名：IT 構築サポート課、管理責任者：営業部長

【機密性】　機密性の資産価値：４

脅威		脆弱性		リスク値	受容可能	残っている脆弱性・改善点等	選択肢	管理目的	管理策	追加対策後			管理策に関する考察
項目	レベル	項目	レベル							脅威	脆弱性	リスク	
盗難	１	取り外し可能な記憶媒体やシステム文書の保管、処分などの取り扱いが管理されていない。	２	８	○	PC を廃棄する手順が適切でない	保有						
持ち出し	２	取り外し可能な記憶媒体やシステム文書の保管、処分などの取り扱いが管理されていない。	２	１６	×	PC を廃棄する手順が適切でない	最適	９．２	９．２．６	２	１	８	PC を廃棄する手段が適切ではない課題に対応するため、A.9.2.6 を適用すれば、対応できると考えた。
情報への不正アクセス	２	利用者の責任(パスワード利用ルール、クリアスクリーンやクリアデスク)が果たされていない。	３	２４	×	パスワード利用ルールがない クリアスクリーン、クリアデスクの方針が明確でない	最適	A.11.3	A.11.3.1 A.11.3.3	２	１	８	利用者の責任において対処する場合、A.11.3.1 で言及されている正しいセキュリティ慣行でパスワードを選択、および利用することで対処できると考えた。 また、クリアデスク・クリアスクリーンについては

													A11.3.3 を直接適用することで対応できると考えた。
		OS のアクセス制御（識別認証、パスワード管理、管理ツールの制限、不要なセッションの切断、接続時間の制限等）が行われていない。	2	１６	×	パスワード管理ルールがない	最適	A.11.5	A.11.5.3	2	1	8	A.11.5.3 にあるパスワード管理システムにより良質なパスワードを強制することで管理ルールに替えて対応することができると考えた。
なりすまし	2	利用者の責任（パスワード利用ルール、クリアスクリーンやクリアデスク）が果たされていない。	3	２４	×	パスワード利用ルールがない クリアスクリーン、クリアデスクの方針が明確でない	最適	A.11.3	A.11.3.1 A.11.3.3	2	1	8	利用者の責任において対処する場合、A.11.3.1 で言及されている正しいセキュリティ慣行でパスワードを選択、および利用することで対処できると考えた。 また、クリアデスク・クリアスクリーンについては A11.3.3 を直接適用することで対応できると考えた

スタッフ不足 セキュリティ要求事項違反 職権乱用	1	情報セキュリティインシデントに対する効果的な取組み(責任の割り当て、インシデントからの学習、必要な証拠の収集など）が行われていない。	2	8	○	情報セキュリティインシデントに対する学習の仕組みがない 情報セキュリティインシデントに関する証拠の収集の仕組みがない	保有						クライアントPCとしてはリスク発生時の影響が大きくないため保有する。 サーバなど他の情報資産へのリスク対応で仕組みが構築されれば、対応する。
		セキュリティ方針やルール類が守られていることを点検できていない。	3	１２	×	情報セキュリティ運用を点検する仕組みがなく、点検されていない	最適	A.15.2	A.15.2.1	1	1	4	セキュリティ要求事項違反を防止するために、A.15.2.1（セキュリティ方針及び標準の順守）を適用すれば、手順の運用をチェックする仕組みを構築でき、対応できると考えた。