演習１０　管理策の実装を検討する

営業部・IT サポート課でリスク対応を検討し、「適切な管理策を適用してリスクを最適化（低減）する」という選択肢を選んだリスクについて、選択した管理目的/管理策は、以下の表のものです。この結果に基づいて、「リスク対応計画書」を作成することにしました。

関連する脅威	対応前リスク値	選択した管理目的 選択した管理策		対応後リスク値
持ち出し	１６	A.9.2	装置のセキュリティ	８
		A.9.2.6	装置の安全な処分又は再利用	
なりすまし	２４	A.11.3	利用者の責任	８
		A.11.3.1	パスワードの利用	
情報への不正アクセス	２４	A.11.3	利用者の責任	８
		A.11.3.3	クリアデスク・クリアスクリーン方針	
情報への不正アクセス	１６	A.11.5	オペレーティングシステムへのアクセス制御	８
		A.11.5.1	セキュリティに配慮したログオン手順	
セキュリティ要求事項違反 職権乱用	１２	A.15.2	セキュリティ方針及び標準の順守、並びに技術的順守	４
		A.15.2.1	セキュリティ方針及び標準の順守	

演習１０－１．　選択した管理策のうち、一部の管理策については、どのように実現するか検討した具体策を記入済です。
テストケースに示された「リスクアセスメント（９）リスク対応計画書の作成」に手順に従って、残りの管理策について、どのように実現するか具体策を検討し、「リスク対応計画書」に書いてください（完了実績、効果確認方法の確認者と期日は実績記入欄なので記入不要)。
尚、ひとつの管理策につき、具体的に実施する項目が２つ以上ある場合は、１つの実施項目毎に１行の計画を記入してください。

初版作成　平成１７年１１月２０日
最新更新日　平成１７年１１月２０日
承認：営業部・IT サポート課 セキュリティ管理者
作成：営業部・IT サポート課 セキュリティ担当者

リスク対応計画書（営業部・IT サポート課）

No.	関連する脅威	対応前リスク値	選択した管理策	リスク対応実施項目	対応後リスク値	優先度	責任者	必要な資源	完了予定	見直予定	完了実績	効果確認方法 確認者（期日）
1	持ち出し	１６	A.9.2.6	廃棄担当部門が、PC や電子媒体処分前のクリアを全点検するように、管理表に確認欄を追加し、運用する。	８	B	△課長	管理表追加の工数：1 人・H	5/25	—		No.6 のチェック実施によって確認する 目標は適用率 100%
2	なりすまし	２４	A.11.3.1	パスワード選択と利用の正しいセキュリティ慣行について、定期的な教育と理解度チェックを実施する	８	A	△課長	教育プログラウ受講：２日・H	12/5	—		定期的なセキュリティポリシーの理解度確認をすべての社員に実施する。 目標は理解度 100%
3	情報への不正アクセス	２４	A.11.3.3	クリアデスク・クリアスクリーンのチェックリストを作成し、定期確認を行う。	８	A	△課長	チェック実行の工数:10 人･H*対象業務数	12/5	—		チェックリストの集計を行い確認する。 目標は 100%

No.	関連する脅威	対応前リスク値	選択した管理策	リスク対応実施項目	対応後リスク値	優先度	責任者	必要な資源	完了予定	見直予定	完了実績	効果確認方法 確認者（期日）
4	情報への不正アクセス	１６	A.11.5.1	ログインするユーザあてにメールの送信されるログインアラートの仕組みを導入する。	8	B	△課長	ログインアラートの仕組みを導入する工数：5人/日	12/5	—		ログインアラートの設定を完了した端末の割合を100%にする。
5	セキュリティ要求事項違反 職権乱用	１２	A.15.2.1	各種ルールの運用状況確認のためのチェックリスト作成と定期的確認を手順化する	4	B	△課長	手順書作成の工数：10人・H	5/10	—		翌年度計画作成の予定と実績で確認する 目標は実施率100%
6	セキュリティ要求事項違反 職権乱用	１２	A.15.2.1	各種ルールの運用状況確認のためのチェックリストを使って、確認をさせる	4	B	△課長	チェック実行の工数：5人・H*対象業務数	6/10	—		目標は各種ルールの運用率100%