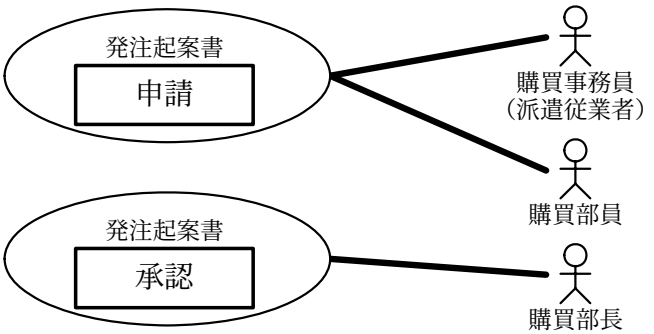
平成 21 年度　秋期　情報セキュリティスペシャリスト試験　解答例

午後 II 試験

問１

出題趣旨
情報システムの構築において，情報セキュリティ技術者は，企業の経営戦略に適した技術を選択するとともに，内部統制の観点も併せもって情報セキュリティを確保するための検討を行うことが求められている。 本問では，経営統合に伴うシステム連携を状況として設定し，認証・認可基盤の構築計画策定を題材に，ロールベースのアクセス制御や ID 連携技術の基本的な理解を問うとともに，ID 管理を検討する際に求められる技術及び運用プロセスの両面から総合的に判断し，適切な構築計画を策定する能力を問う。

設問		解答例・解答の要点		備考
設問１		**a**	・認証アサーション ・認証トークン	
		b	サインオフ	
		c	リダイレクト	
設問２	**(1)**	業務システムごとに拡張属性を定義して使用しており，スキーマが異なるから		
	(2)	・業務システムへのアクセスが本来許されない利用者が，アクセス可能な状態になる。 ・退職や異動で権限がなくなったはずの者が業務システムにアクセスできてしまう。		
設問３	**(1)**	**業務対象**	顧客情報	
		業務操作	閲覧	
	(2)	**分離すべき理由**	発注起案書申請と発注起案書承認が同一人物によって行われ，架空発注などの不正を発見できないおそれがあるから	
		分離後		
	(3)	① ②	・職掌変更などで役職に対する役割に変更が発生した場合に，容易に対応できるから ・申請と承認のような分離されるべき責務が，同じ権限として定義されていないから	
	(4)	**追加される管理項目**	・ロールに関する情報 ・職掌に関する情報	
		運用見直しの内容	人事部あるいは管理者によって，従業者の所属組織や職掌の変更の都度，遅滞なく，情報を更新する。	
設問４		①	・認証方式をアプリ認証方式からプロキシ認証方式に変更する。	
		②	・認可ロジックをロールベースのアクセス制御に対応した実装にする。	

問2

出題趣旨
情報セキュリティの実現に当たっては，取り扱う情報の機密性に応じて適切なセキュリティ対策を講じるとともに，環境の変化に対応して継続的に改善を図る必要がある。 本問では，内線電話の IP 電話化と情報連携の迅速化という課題への取組みを状況として設定し，ネットワークの統合を含む社内 LAN の見直しを題材に，ファイアウォールによるアクセス制御や無線 LAN の認証技術の基本的な理解を問うとともに，機密性の高い情報を保護するための対策を講じる能力を問う。

設問		解答例・解答の要点		備考
設問1		**a**	開発 LAN の IP 電話　又は　設計エリアの IP 電話	
		b	SIP サーバ	
設問2		DoS 攻撃のパケットを遮断できる可能性が高くなる。		
設問3	**(1)**	**接続箇所**	(r)	
		接続すべきでない理由	極秘情報が保存された開発サーバや製造サーバが接続された開発 LAN 及び製造 LAN に，営業担当者がアクセスすることを許可すべきではないから	
	(2)	**保存前対策**	・共有データを保存する際に責任者が内容を確認して承認する。 ・共有データの作成者とは別の担当者が内容を確認して保存する。 ・極秘情報と機密情報の区別を明確にして設計部員に周知徹底する。	
		保存後対策	・極秘データが情報共有サーバに保存されていないことを定期的に検査する。	
設問4	**(1)**	・ネットワークケーブルへの PC の不正接続 ・ネットワーク上を流れる特注品に関する極秘情報の盗聴		
	(2)	情報セキュリティポリシに従い，機密区画にある SPC から極秘情報を保存することになった製造サーバにアクセスする場合には，FWx によるアクセス制御を行う必要があると判断したから		
設問5	**(1)**	SSL　又は　TLS		
	(2)	・PEAP 方式は EAP-TLS 方式に比べて利用者を特定できる利点があるから ・EAP-TLS 方式はクライアント証明書を組み込んだ PC を認証するので利用者を特定できないから		
	(3)	NPC の持出しと返却の日時及び使用者に関する記録を残すこと		