別添資料

研修資料コンテンツ一覧

研修資料一覧
　情報セキュリティポリシー研修に係る下記研修に使用する教材のコンテンツは本書のとおり定めるものとする。
　なお「動画時間」は動画教材の時間をいい、スライド教材は十分充実した分量で作成したうえで、動画教材においては、その内容につき解説が不要な個所の説明を一部省いても構わない。

記

１　動画研修用教材
　⑴　外部ホームページ担当者向け研修用教材
　⑵　病院局向け研修用教材

２　e-ラーニング研修用教材
　⑴　一般職及び係長職向け研修用教材
　⑵　役職者及びセキュリティ担当者向け研修用教材

以上

1(1) 外部ホームページ担当者向け研修用教材

動画時間：合計90分

No.	単元タイトル	No.	章分類	No.	コンテンツ	備考・備忘
1	目次と目的	(1)	研修の目的	ア	外部HPを安全に管理する	
		(2)	目次			
2	導入	(1)	大規模なサイバーテロへの備え		直近の具体的事例	
3	情報セキュリティとは	(1)	情報対策の必要性	ア	三要素の説明	
				イ	三要素が欠けると何が起こるか	
				ウ	札幌市又は自治体の事故事例	
		(2)	情報セキュリティポリシー			
4	HP管理について	(1)	HP管理とは		ポリシーを遵守しない管理	←担当者責任を問われる。危機感の発揚
		(2)	あるべき管理とは	ア	認証・アクセス権の管理	
				イ	パスワードの設定	
				ウ	データの暗号化	各通信区間ごとの暗号化手法について整理する。 利用者→Webサーバ：SSL（Webサーバに電子証明書導入）による通信 管理者→Webサーバ：SSH接続による通信 ファイル転送：SCP，SFTPによる通信 Webサーバ内：暗号化ソフトの導入 Webサーバ⇔管理者：VPN及びVPNソフトウェア VPN⇔VPN：通信の暗号化機能のあるVPNの利用
				エ	ソフトウェア管理	更新遅れは1日でも致命的、サポート終了ソフトの使用禁止 契約不備による不正アクセス事例
				オ	サーバの脆弱性診断（年1回）	ポリシー上の義務。委託業者にも順守させる 検出された課題は必ず対処する。しなければ無意味。 XSSについて
				カ	ログの管理	設定方法は技術対策基準5(5)ア
5	DC、委託業者選定	(1)	種類と特徴	ア	①公式HP、②情シスのサーバー、③外部サーバ	
				イ	それぞれのメリットデメリット	
				ウ	リージョンによる注意	
		(2)	外部サーバ使用時の注意点	ア	CISO承認	システム調整課に連絡
				イ	技術対策基準P70	
				ウ	事故事例	
		(3)	委託業者との契約	ア	事前確認事項	対応時間、バックアップやサーバ構成、故障時の対応内容
				イ	契約時の注意点	技術対策基準に定める内容の解説
				ウ	開発時の管理事項	
				エ	運用保守時の管理事項	
6	内部監査結果	(1)	実際に対策の弱いところを確認する		ルールの形骸化に注意！	
		(2)	日本年金機構の実例			
		(3)	監査結果			←昨年の監査結果を確認してコンテンツ作成
7	セキュリティ事故対応	(1)	連絡経路			
		(2)	事前に定めておくべきこと	ア	緊急時の連絡	委託先、他部局関係者が漏れやすい。特に土日の連絡について
				イ	責任権限の明確化	形骸化させないこと。情報収集、各所への連絡、意思決定、公開停止の決定権を決めておく
		(3)	万が一の際の対応ポイント	ア	電源は切らずにネットワークから隔離	状況把握と証拠保全のため電源はオン
				イ	バックドア対策	被害にあったすべてのソフトウェアの再インストール
8	クラウド・SNSの利用	(1)	CISO承認	ア	広報課との事前協議	札幌市ソーシャルメディア活用ガイドライン
				イ	副市長決裁	
		(2)	利用上の注意点	ア	信用失墜行為（バカッター）	
				イ	職務専念義務	
				ウ	守秘義務違反	職場で撮影した写真に重要書類が写り込んでいた事例。鏡、金属、窓などに移り込んでいる場合も
				エ	公私混同	公共SNSアカウントを個人アカウントと取り違えた事例
		(3)	事故事例			
9	不正アクセスへの備え	(1)	連絡体制の整備		特に夜間休日が手薄	
		(2)	不正アクセスの多い時期			
		(3)	情報セキュリティクラウドについて	ア	情報セキュリティクラウドとは	概要図があるとイメージしやすい
				イ	外部ホームページが利用できる機能	リバースプロキシ、WAF、ログ分析機能

その他、内容の加除修正については、本市と協議の上で調整及び決定することとする。

1⑵ 病院局向け研修用教材

動画時間：合計20～長くて25分

No.	単元名	No.	章分類	No.	コンテンツ
1	情報セキュリティ対策の必要性	⑴	セキュリティ対策の必要性		
		⑵	病院総合版評価、機能別版評価に含まれている		
2	情報セキュリティ対策の実施	⑴	USBメモリの取り扱い		
		⑵	私用機器の接続禁止		充電目的のスマホ利用も禁止
		⑶	個人情報の持ち出し・目的外利用禁止	ア	電子カルテ情報の持ち出しなどは処分の対象
				イ	自宅PCへのメール転送は原則行わない
		⑷	ハードディスク等の廃棄の方法		
		⑸	ID認証		認証カードの共有禁止
		⑹	暗号化		Officeの暗号化手順について
		⑺	パスワードの設定		英数混合ランダム16桁以上を
3	情報セキュリティ上の脅威	⑴	ウイルス対策		
		⑵	標的型攻撃メール	ア	定義
				イ	種類
				ウ	対策・対応
		⑶	外部クラウドサービス利用上の注意		
		⑷	SNS利用上の注意		
4	医療機関の事故事例	⑴	USBメモリ紛失		
		⑵	個人情報を口外		
		⑶	個人情報紛失		
		⑷	情報資産不正持出		
		⑸	情報資産目的外利用		
		⑹	電子カルテの取り扱いによる事故		
		⑺	アカウント共有		
		⑻	病院を狙ったサイバーテロ		
		⑼	医療関係詐欺		
		⑽	SNSの不適切な使用		

その他、内容の加除修正については、本市と協議の上で調整及び決定することとする。

2(1) 一般職及び係長職向け研修用教材

動画時間：合計60分（延長可）

教材No.	単元タイトル	No.	章分類	No.	コンテンツ	備考・備忘
1	本研修の目的	(1)	目次			テストなし
		(2)	本研修の目的			
2	情報セキュリティ対策の必要性	(1)	情報セキュリティ対策の意義			
		(2)	情報セキュリティ対策の定義	ア	三要素＝完全性、可用性、機密性の説明	
		(3)	セキュリティ要素別の事故事例			
		(4)	実施すべきセキュリティ対策の一覧			
3	情報セキュリティポリシー	(1)	情報セキュリティポリシーとは			
		(2)	緊急事態の報告経路	ア	報告の必要な緊急事態	
				イ	報告経路	
				ウ	情報システム部の相談先一覧と 情報セキュリティ危機管理マニュアル（参考）	
		(3)	ログ管理	ア	アクセス状況の記録とは	
				イ	ログ管理の目的	
				ウ	ログは管理されている	職員向け研修では、ログが監視されていることによる警鐘を鳴らす
		(4)	ポリシー違反の場合の懲戒	ア	ログ監視と懲戒処分	
				イ	懲戒実例	
		(5)	ポリシーの非公開			
		(6)	セキュリティ内部監査の実施			
4	情報資産の管理	(1)	情報資産とは		定義の説明	
		(2)	情報資産の重要性分類			
		(3)	重要性1を扱う場合に関わるルール一覧 ※あくまで重要性1の重要度を伝える目的 各項目の解説はここではせず、各単元に譲る	ア	重要性1を取り扱うシステムに関するルール	ICカード等による二要素認証
						通信及びデータの暗号化機能
						インターネット上への公開にはCISO承認（副市長決裁）が必要
				イ	重要度の高い情報資産の運用ルール	のぞき見防止策の実施義務
						記憶媒体廃棄時の手順
						利用できる職員の範囲を定める必要有り
						在宅勤務における持出禁止
						重要性2以上の情報資産の無線LAN使用禁止
		(4)	マイナンバーの取扱上の注意			
		(5)	情報資産の把握・整理	ア	情報資産は管理が必要＝一覧の作成	
				イ	新しい業務ができたら、必ず情報資産一覧に追加	新規事業の開始と情報資産一覧の作成はセットと心得る
				ウ	業務を廃止したら、必ず情報資産一覧から削除	
		(6)	その他注意事項	ア	目的外利用の禁止	
				イ	デスクトップ、ローカルディスクに保存しない	
				ウ	異動時の返却	
5	情報資産の持ち出し	(1)	執務室外への持ち出しの禁止			他部局へのメールでの送信も持ち出しに含まれる。
		(2)	持出許可と管理簿の作成	ア	課長への許可申請	メールの場合も必要

				イ	管理簿の作成	
		⑶	持ち出しの方法	ア	原則として外部記憶装置を用いない	SDカード、USB、CD、DVD、ノートPC、タブレット等
				イ	推奨される具体的な方法	ファイルサーバ、データ交換フォルダ、暗号化したファイルのメール添付
				ウ	やむを得ない場合に外部記憶装置を用いる	
		⑷	公用USBメモリ等の使用上の注意	ア	個人所有の記憶媒体の使用禁止	スマホ・タブレット等の充電目的の接続も禁止
				イ	暗号化機能必須	
				ウ	パスワードの設定	
				エ	使用記録簿の作成	
6	セキュリティ脅威への具体的対応	⑴	電子化によって増えるリスク			
		⑵	SNSアカウントの適切な利用	ア	やってはいけないこと	
				イ	事故事例	
		⑶	ウイルス対策	ア	ウイルス対策ソフト	
				イ	外部ファイル取り込み時のウイルススキャン	
				ウ	感染時対応	
				エ	事故事例	
		⑷	標的型攻撃メール対策	ア	とは	
				イ	パターン（種類）	
				ウ	対策	
				エ	事故事例	
		⑸	「かも」と思ったら即行動	ア	結果的に問題なしでもOK	
				イ	いつ、どこで、だれが、何をして、どうなったかを整理	セキュ担⇒情シスに報告
7	パソコン等の使用とICカードの管理	⑴	パソコンやシステムの使用上の注意	ア	不正改造や設定の変更禁止	ハンドブック引用
				イ	周辺機器の増設には課長の許可が必要	
				ウ	パスワード付きスクリーンセーバーの使用	
				エ	物理的なのぞき見の防止	
				オ	離席・業務終了時のICカードの抜き取りと保管	
				カ	イントラ以外のネットワークへの接続禁止	
				キ	許可のないソフトウェアインストールの禁止	情報システム部及び所属長の許可が必要
		⑵	認証機能	ア	認証の必要性と種類	IDパスワードが基本で、重要性1取り扱う場合は二要素認証＝ICカード＝職員証
				イ	ICカード（職員証）の役割と重要性	PCだけではなく、イントラネットや、各種システムへのログインにも使われている
				ウ	ICカードの取り扱い	紛失時の報告、離席時に外す（監査）、貸与・共有禁止
				エ	ID・パスワードについて	英数混合８文字以上、定期的な変更、紙に書かない、人に教えない
8	パソコン等及びネットワーク機器の廃棄方	⑴	廃棄・転用時の注意点 ※通知内容の説明	ア	導入：事故事例	神奈川県の事故
				イ	重要性分類に応じた分類	特1、１＆2、3の3段階。物理的、磁気的、ソフトウェアによる消去の説明
				ウ	特1の扱いについて特に説明	対象になるかどうかの判断基準を、わかりやすく説明する
				エ	リースの場合の対応	
		⑵	執務室外の修理時の注意点			
9	在宅勤務と個人所有PCの使用	⑴	在宅勤務時の個人所有PCの使用	ア	課長の許可を得ること	
				イ	使用可能端末の条件	最新OS、ウイルス対策、設置場所
				ウ	情報の持ち出しの方法と制限	重要性１以上は個人PC使用禁止。持出はUSB、メール、データ交換ファイルのみ

その他、内容の加除修正については、本市と協議の上で調整及び決定することとする。

2(2) 役職者及びセキュリティ担当者向け研修用教材

動画時間：合計30分（情報セキュリティ担当者のみ受講する部分は除く）

No.	単元タイトル	No.	章分類	No.	コンテンツ	備考・備忘	
1	役職者の役割 受講対象：役職者、情報セキュリティ担当者	(1)	部長の役割				
		(2)	課長の役割				
		(3)	情報セキュリティ担当者の役割				
		(4)	情報セキュリティ内部監査について				
2	緊急事態における対応 受講対象：役職者、情報セキュリティ担当者	(1)	課長の対応			ハンドブック引用	
		(2)	部長の対応			ハンドブック引用	
		(3)	セキュリティ担当者の対応			ハンドブック引用	
3	セキュリティリスクの類型と対策 受講対象：役職者、情報セキュリティ担当者	(1)	職員の振る舞いによる人的リスク（仮）			この章に関しては、業務開始後に受託者と本市で協議し、業務責任者及び講師の有する最新の知見を踏まえて、構成及び詳細な内容を検討すること。	
		(2)	ランサムウェア（仮）				
		(3)	セキュリティ攻撃（仮）				
		(4)	必要な対策				
4	平常時の管理業務 受講対象：役職者、情報セキュリティ担当者	(1)	情報資産一覧表の作成	ア	作成と更新	新規資産作成時の追加、不要なものの削除も必要	
				イ	年に一度の突合検査	情報資産一覧と、管理簿等を突合し、抜け漏れを更新する	
				ウ	リスク管理		
		(2)	周辺機器の増設許可				
		(3)	稼働状況の監視と障害の早期発見				
		(4)	インターネット接続サーバの脆弱性診断（年1回）				
5	ソフトウェア利用の注意点 受講対象：情報セキュリティ担当者	(1)	業務目的外のソフトウェアのインストール禁止				
		(2)	脆弱性対策プログラムの迅速なアップデート				
		(3)	サポート終了ソフトウェアの使用禁止	ア	サポート終了済み、終了間近のソフト		
				イ	サポート切れのソフトウェアを使用している場合	直ちにシステム調整課まで連絡を	
		(4)	ライセンスのないソフトウェアの使用禁止				
		(5)	ソフトウェアのインストール手順	ア	SWS配布		
				イ	フリーソフトの注意点	ウイルスチェック必要＆手順	
		(6)	重要性1を含む記憶媒体の秘匿化				
6	システム改修・開発、ファイルサーバ設置等 受講対象：情報セキュリティ担当者	(1)	情報システム部への事前報告と技術審査			新規システム開発時	
		(2)	管理区域の策定と施錠等				
		(3)	CISO承認	ア	CISO承認とは		
				イ	CISO承認の必要な場合4種及び例外		
				ウ	手続と提出書類		
				エ	相談先		
		(4)	システムに備えるべきセキュリティ対策	ア	重要性1を取り扱う場合に特に必要な対策	高度な認証機能	要二要素認証
						情報資産の暗号化	要実施手順策定
				イ	すべての情報システムに必要な対策	バックアップ対策	要実施手順策定
						アクセス権の付与とID管理	要実施手順策定
						アクセス状況等の記録	
						ウイルス対策	
						仕様、構成図等の文書化	要更新
		(5)	開発及び運用保守における修正、更新、障害対応等の作業の記録				
		(6)	実施手順の策定		実施手順の作成が必要な場合の列記		
		(7)	情報セキュリティ技術対策基準について			参考資料として（イントラ内の掲載場所を）紹介、非開示情報であることを注意	
7	委託業者管理 受講対象：役職者、情報セキュリティ担当者	(1)	契約書上のセキュリティ順守事項の明記				
		(2)	入退室管理				
		(3)	ID・パスワードの付与・削除				
		(4)	アクセスログの収集				
		(5)	委託作業時に漏れがちなこと				
		(6)	委託先で順守されにくいこと				
8	部内研修・訓練の実施 受講対象：役職者、情報セキュリティ担当者	(1)	部内セキュリティ研修				
		(2)	訓練の実施				
		(3)	提供可能な教材と連絡先				

その他、内容の加除修正については、本市と協議の上で調整及び決定することとする。

※受講対象者に名前がなくても任意受講として受講は可能なものとする。