●スマートフォンを安全に使うための企業のチェックリスト例

2012年4月20日　MCPCアプリケーションWG

	対策措置	Yes/No	備考
事前対策			
1	PINコードが設定されているか？		電源投入時の認証要求による盗難･紛失時の不正利用防止
2	電話帳バックアップサービスへ加入／設定されているか？		盗難･紛失時のデータ復元、情報把握、顧客対応等への備えとして
3	位置情報取得サービスへ加入しているか？		盗難･紛失時に端末の位置を探査できる場合がある。
4	リモートロック用アプリを使うよう設定されているか？		盗難･紛失時の第三者利用や情報流出防止のため
5	画面ロックの機能を使うよう設定されているか？		日常的な放置や盗難･紛失による第三者利用や情報流出防止のため
6	アクセス制限をかける（MDMやURLフィルタリングの活用）		業務に無関係なサイト利用と、それに伴う情報事故等を防止するため
7	セキュリティ対策ソフトがインストールされているか？		マルウエア等への感染を防止するため
運用中の対策			
1	画面ロックを常時使用する。		日常的な放置や盗難･紛失による第三者利用や情報流出防止のため
2	SDカードには電話帳等を保存しない。		SDカードを経由した情報流出を防止するため
3	端末の格納データを定期的に見直し、不要になった連絡先等は削除する。		紛失･盗難時に流出する情報を減少させるため
4	持ち歩くときはストラップを装着する。		日常的な放置や盗難･紛失を防止するため。
5	OS、アプリ、ウィルス対策ソフトのアップデートを欠かさない。		ソフトウエア的な脆弱性による情報事故を防止するため
6	業務に不必要なUSB機器、PC等を接続しない。		意図しない情報の拡散や流出を防止するため
7	業務に不必要なアプリをインストールしない。		意図しない情報の流出や悪意あるソフトウエアのインストールを防止するため
	･インストール時には、偽アプリをインストールしないよう、名称･バージョン･提供元を確認する。		悪意あるソフトウエアのインストールやフィッシング被害等を防止するため
8	私用PCに接続しない		意図しない業務情報の拡散や流出を防止するため
9	無線LAN接続時には、以下を確認する。		無線LAN環境を経由した情報事故を防止するため
	･通信路が暗号化されていること		第三者による通信傍受を防止するため
	･接続認証が行われていること		管理が不十分なNWによる情報事故を防止するため
	･社外の無線LANスポットではSSL暗号化通信やVPN通信を使う。		無線LAN区間及びインターネット区間での傍受を防止するため
	･オープンな無線LANネットワークは業務に利用しない。		管理が不十分なNWによる情報事故を防止するため
10	その他一般的な安全管理対策		不注意による情報漏えいに対する全般的な注意事項
	･基本的に身体から離さない。		紛失･置き忘れや第三者によるいたずらを防止するため。
	･不用意に机や椅子、棚、カウンター等に置いたり放置しない。		紛失･置き忘れや第三者によるいたずらを防止するため。
	･充電する時は置き忘れや盗難防止に十分配慮する。		紛失･置き忘れや第三者によるいたずらを防止するため。
	･背後からの覗き見に注意する。覗き見防止シール等を貼る。		覗き見による情報漏えい防止のため。
紛失･盗難時の事後対策			
1	通信会社に連絡し、利用を中断（通話を停止）する。		第三者による不正利用を防止するため。
2	警察へ紛失／盗難の届出をする。		紛失／盗難の事実があったことを証明するため。
3	リモートロックを実行する。		画面ロックによる情報保護を補強するため実施する。
4	社内システム側で、当該のアカウントの利用を停止する。		社内システムへの不正アクセスを防止するために実施する。
5	電話帳登録者へ連絡する。		情報漏えいの可能性があることを連絡し、二次被害を防止する。
6	情報セキュリティ管理部署へ連絡する。		社内での手続きや再発防止措置、監督官庁への報告等を依頼する。
ウイルス感染が疑われる場合の事後対策			
1	通信を遮断（電源OFFまたは機内モードに設定）し、情報管理責任者に連絡する。		ウイルスの拡散を防止し、対処を依頼する。
2	感染を発見したときは、その日時、場所、使用ソフトウエア、感染症状を情報管理責任者に報告する。		対処や拡散防止、今後の感染防止策策定のための情報として提供する。