個人情報保護法のチェックシート

出展： 神奈川県中小企業団体中央会 （2005.8.25）　　CXMedia Inc. 2005.8.28

ch		項目	備考
		１．個人情報保護法	
	1	個人情報の利用目的を明確にしているか	
	2	個人情報提供者の権利を理解しているか	
	3	第三者提供は本人の同意がなければ認められないのを知っているか	
	4	苦情対応の窓口を設置しなければならないのを知っているか	
	5	本人の求めにより、保有個人データを開示しなければならないのを知っているか	
	6	個人情報を不正に取得してはいけないことを知っているか	
	7	利用目的を変更する場合は、本人の了承を得なければいけないのを知っているか	
	8	自社が個人情報取扱事業者であるか否か知っているか	
	9	従業員及び委託先の管理監督責任があるのを知っているか	
	10	本人の求めにより、保有個人データを訂正しなければならないのを知っているか	
		２．個人情報保護／情報セキュリティポリシー	
	1	個人情報保護基本方針を定めているか	
	2	個人情報保護基本方針を社内外に公表しているか	
	3	個人情報保護管理規程を定めているか	
	4	個人情報保護管理規程を社内に周知徹底しているか	
	5	個人情報保護手引書を作成しているか	
	6	情報セキュリティ基本方針を定めているか	
	7	情報セキュリティ基本方針を社内外に公表しているか	
	8	情報セキュリティ管理規程を定めているか	
	9	情報セキュリティ管理規程を社内に周知徹底しているか	
	10	機密情報取扱手引書を作成しているか	
		３．組織セキュリティ	
	1	個人情報保護推進体制を持っているか（委員会等）	
	2	情報セキュリティ推進体制を持っているか（委員会等）	
	3	推進体制に経営者が参画しているか	
	4	個人情報保護責任者を設置しているか	
	5	個人情報保護監査責任者を設置しているか	
	6	個人情報を扱う業務を外部に委託する場合、契約に個人情報保護の条文を入れているか	
	7	外部委託先の選定基準を持っているか	
	8	定期的に監査責任者による監査を実施しているか	
	9	Ｐマークまたはそれに準ずる認証の取得をしているか（取得しようとしているか）	
	10	個人情報漏えい対策保険に加入しているか	
		４．人的セキュリティ	
	1	採用時に個人情報保護／情報セキュリティの教育を行っているか	
	2	採用時に誓約書を取り交わしているか	
	3	従業員・パート社員に対する定期的な個人情報保護／情報セキュリティの教育を行っているか	
	4	従業員・パート社員と誓約書を取り交わしているか	
	5	納入業者等、出入りを行う業者に個人情報保護／情報セキュリティ遵守の指示を出しているか	
	6	事故の際の報告義務が徹底されているか	
	7	事故の際の報告手順が明確になっているか	
	8	事故の際の各自の役割が明確になっているか	
	9	パスワード管理が徹底されているか（類推されやすい内容の禁止やディスプレイに貼り付けられていない）	
	10	パスワードを定期的に変更しているか	
	11	公益通報者保護法の支持を宣言しているか	
		５．物理的セキュリティ	
	1	会社の入口にて入退出管理を実施しているか	
	2	社員証の携行を常に行っているか	
	3	区画に対してセキュリティレベルの設定を行っているか	
	4	セキュリティレベルの高い場所への入退出管理を実施しているか	
	5	区画のセキュリティレベルにより、持ち出し可能な書類が決められているか	
	6	機密情報を施錠ができる保管場所に保管しているか	
	7	機密情報が放置されないような仕組みになっているか	
	8	重要なサーバは、施錠された部屋に設置されているか	
	9	ＵＳＢメモリ等の大容量記憶装置の持込、使用を制限しているか	
	10	ＣＤ-Ｒ等の利用の制限を物理的に行っているか	
		６．技術的セキュリティ	
	1	システムの運用手順が決定されているか	
	2	勝手なソフトウェアのインストールは制限されているか	
	3	業務に関係ないメール、インターネットの利用を禁止しているか	
	4	モバイルパソコンの利用に際して注意事項を決めているか（社内放置、盗難、紛失）	
	5	モバイルパソコン内の機密情報は暗号化されているか	
	6	ウイルス対策ソフトウェアをすべてのパソコンに入れているか	
	7	ＯＳの最新アップデートが正しく行われているか	
	8	利用者の権限に沿ったアクセス制限が設定されているか	
	9	社内システムをインターネットから隔離しているか（ファイアウォールの設置）	
	10	アクセスログを一定期間、保管しているか	

○個人情報保護法対応度チェックシートの解説

１．個人情報保護法は個人情報保護法の理解度のチェックである。すべて「はい」ではない場合は、再度個人情報保護法を勉強すべきである。

２．個人情報保護／情報セキュリティポリシーは、会社によって違いが出てくる部分である。すべて「はい」でなくて構わないが、自信を持って答えることができたかが重要である。

３．組織セキュリティ以降は、安全管理のチェック項目である。個人情報を会社の機密情報として、如何に安全に管理しているかをチェックしている。安全管理には「組織的」、「人的」、「物理的」、「技術的」がある。個人情報保護において特に重要なのは「人的」部分である。漏えい原因の半分以上がここに起因している。「物理的」側面は、社員が日々の業務で個人情報保護及び情報セキュリティを強く意識する部分である。会社の姿勢を示す意味でもしっかりと対応したい。「技術的」のチェック項目は、自社でシステムを運用し個人情報を管理している会社が強く意識しなければならない項目である。いずれの項目も社内でよく検討し、かつ判断されていなければならない。