様式4

個人情報セキュリティー評価チェックシート

※貴法人記入欄　ご担当者様にご署名・ご捺印願います。

貴法人名	
店舗名・医院名	
個人情報管理責任者	

実施日	年　　月　　日

各該当項目に対し、〇を記入してください。

判定基準	確認内容	取得済 取得予定	未取得 取得予定なし
A	プライバシーマークまたはISMSの認定/認証を持っているか。		
B	プライバシーマーク認証取得予定事業者・その他のISO認証取得予定事業者であるか。		

各該当項目に対し、〇を記入してください。

判定基準		確認内容	実施済	未実施	該当なし	未実施の場合、改善措置
1	1	担当者が知りうる範囲で、過去2年以内に情報漏洩の事故を起こしていないか。				
	2	情報資産全般（個人情報含む）の保護方針を定めているか。（ホームページ上やパンフレットなどで）				
	3	情報資産全般（個人情報含む）の保護に関する教育を行っているか。				
	4	個人情報を取り扱うに当たって、その利用の目的をできる限り開示しているか。（ホームページ上やパンフレットなどで）				
	5	個人情報の取扱いに関する苦情は、適切かつ迅速に対応しているか。				
2	1	出入り口はすべて施錠タイプか。				
	2	すべての端末（パソコン）にウイルス検知ソフトウェアを導入しているか。				
	3	情報資産全般（個人情報含む）に関する教育実施はされているか。				
	4	社内規則（就業規則）として「個人情報や機密漏洩に関する罰則規定」があるか。				
	5	退社時や外出時に、机上などに個人情報を放置しないようにしているか。				
	6	個人情報を取り扱う場所や部屋は、施錠管理が行われているか。				
	7	個人情報管理責任者が任命されているか。				
	8	情報資産全般（個人情報含む）の保護のために管理策を選定、実施しているか 。				
	9	退職後に効力のおよぶ守秘義務条項の入った誓約書を従業員と取りかわしているか。				
	10	納品業者など、来訪者について入退室記録を取っているか。				
	11	事故・不正アクセス・脆弱性の指摘等が発生した場合の対応手順を定めているか。				
	12	ウィルス検知ソフトウェアのパターンファイルは自動的に最新版に更新されるようになっているか。				
	13	個人情報に対する質問窓口とその連絡先を設けているか。				
	14	個人携帯電話で個人情報に関するやり取りをしていないか。また、社用パソコン宛のメールを個人携帯電話に転送していないか。				
	15	個人情報を受け渡しする時、面識のある双方の担当者立会いのもと、行っているか。				
	16	個人情報含むを配送する時、記録簿もしくは代替となる記録物に記録しているか。 「OK」の場合、記録の方法は 〔　　〕				
	17	個人情報を記載・記録した書類や電子媒体は、就業時間外等に施錠したキャビネット、保管庫に保管しているか。				
	18	収集した個人情報を保管・管理する担当者に付与されるログインIDは業務上必要な権限のみ（閲覧権限、保存権限、編集権限等）を付与し管理しているか。				
	19	情報は適切な時期に適切な方法で処理されているか。				
	20	例外的に個人情報を電子メールで送信するときは、あらかじめ指定されたあて先に対して、所定の方式で「パスワードを付与する」か又は「暗号化して」送信しているか。				
	21	個人情報を含むファイルをパソコン、または可搬媒体（USBメモリ等）に保管する場合、適切な方法でパスワードロックをかけているか。				
	22	個人情報管理責任者の許可を得て、外部委託情報（個人情報含む）を複製（コピー）しているか。				
	23	個人情報を保管もしくは使用するサーバは、WEBサーバ等の公開用サーバと区別するなどして、外部ネットワークと完全に分離されているか。				
	24	サーバの管理は、管理責任者を置き、常時セキュリティ情報を入手して必要な措置を講じているか。				
	25	サーバ上の個人情報データは、他のサーバから利用できないようになっているか。				
	26	バックアップは上記システム管理者だけが行い、バックアップ媒体はシステム管理者が施錠できる保管場所にある所定の保管庫に保管しているか。				
3	27	個人情報の出力は、責任者もしくはシステム管理者が立会いのもとに行っているか。				
	28	ID・パスワードは個人毎に与えられ管理されているか。				
	29	個人情報をPCで見るときやパスワードを打つときは、背後に人物がいないなど確認を行うよう、周知徹底されているか。				
	30	離席する際にPCのロックまたはスクリーンセーバーをかけるなど、第三者が勝手にPCを使用できないよう、周知徹底されているか。				
	31	パスワードは定期的に変更されているか。				
	32	個人情報へのアクセス権限は、責任者及び必要最小限の人だけが行っているか。（グループ単位に権限を付与し、権限が不要な人にも権限が与えられていないか等）				
	33	個人情報データの内容に関して、定期的に検査を行い、記録として残しているか。				
	34	定期的に、個人情報データベースに対するアクセスの記録（ログ）を調べ記録に残しているか。				
4	35	権限者以外からのアクセス、成りすましのアクセス等の異常が発見されたとき、情報資産全般（個人情報含む）保護とリスク対応の為の委員会を設置し対策検討などを行う措置を講じているか。				
	36	教育を受けた参加者の出欠確認（日付、本人の署名（または押印））と参加者名簿等の記録を保管しているか				
	37	会社のコンピュータは、業務遂行のためのものであり、コンピュータに関する社員や関係者個人のプライバシーの保護は保証されないことを説明しているか。				
	38	個人情報を扱う場所には、関係者以外のものが出入りできないようになっているか。				
	39	個人情報を扱う場所への入退室を記録し、場所への最初の入室者および最後の退室者がわかるように記録簿に記録しているか。				
	40	個人情報を扱う場所への入退者に対して、目視で身分を証明できるもの（社員証、補助社員証、入館証）を着用させているか。				
	41	個人情報を廃棄する場合、媒体に応じシュレッダーにかけたり、破壊したりして読み取り不能にした上で信頼できる廃棄物処理業者に廃棄を依頼しているか。				
	42	情報資産全般（個人情報含む）を破棄する場合、廃棄作業は責任者もしくは権限主の立会いのもとに行っているか。				
	43	廃棄に際して、全て廃棄記録簿もしくは、それに代替する方法にて記録を残しているか。 「OK」の場合、記録の方法は （　　）				
合　　計（JBRS記載）						

JBRS記載欄
改善指導項目
改善結果についての評価