

■ご参考資料 Pマーク取得におけるLucida SecurOfficeの対応範囲

Pマーク取得時に審査項目の基準となる「JISQ15001:2006をベースにした個人情報保護マネジメントシステム実施のためのガイドライン-第1版-」よりシステム対応に関連する「3.4.3.2安全管理措置」の項目へのLucida SecurOfficeの網羅状況。

「JISQ15001:2006をベースにした個人情報保護マネジメントシステム実施のためのガイドライン-第1版-」より抜粋

安全管理措置	チェック項目	Lucida SecurOfficeでの適用範囲
1. 物理的安全管理措置		
1.1 入退館(室)管理	① 建物、室、マシン室、個人情報の取り扱い場所への入退の制限機構がある ② 建物、室、マシン室、個人情報の取り扱い場所への入退が制限されている ③ 建物、室、マシン室、個人情報の取り扱い場所への入退の記録が取られ、保管されている ④ 建物、室、マシン室、個人情報の取り扱い場所への入退の記録は定期的にチェックされている	
1.2 盗難等の防止	① 離席時に個人情報を書類、媒体、携帯可能なコンピュータ等を机の上に放置していない。 ② 個人情報を取り扱うPCの操作において、離席時は、パスワード付きスクリーンセーバーの起動又はログオフを実施している。 ③ 個人情報を記録した媒体(記録媒体、紙)は施錠保管され、あるべきものが全てあることが把握されている。 ④ 個人情報を記録した媒体(記録媒体、紙)の保存場所の鍵は特定者が管理している。 ⑤ 個人情報を記録した媒体(記録媒体、紙)の廃棄は、再利用できない措置を講じている。 ⑥ 個人情報を記録した携帯可能なPC等の盗難防止措置が施されている。 ⑦ FD、MO、CD、USBフラッシュメモリ等の外部記憶媒体の利用はルールに従っている。 ⑧ 個人情報を取り扱う情報システムの操作マニュアルを机の上に放置していない。	暗号化機能、外部媒体書出し禁止機能 外部媒体書出し禁止機能
1.3 機器・装置等の物理的な保護	① 個人情報を取り扱う機器・装置等について、安全管理上の脅威(盗難、破壊、破損等)や環境上の脅威(漏水、火災、停電、地震等)からの物理的な保護装置がある。	
2. 技術的安全管理措置		
2.1 個人情報へのアクセスにおける識別と認証	① 個人情報へのアクセスにおいて、識別情報(ID、パスワード等)による認証が実施されている。 ② 個人情報を格納した情報システムは、デフォルトの設定を残していない。 ③ 識別情報の発行・更新・廃棄は、ルールに従っている。 ④ 識別情報は平文で記録していない。 ⑤ パスワードの有効期限の設定、同一又は類似パスワードの再利用の制限、最低パスワード文字数の設定、一定回数以上ログインに失敗したIDの停止等の措置が講じられている。 ⑥ 個人情報へのアクセス権限を有する従業者が使用できる端末又はアドレス等は、MACアドレス認証、IPアドレス認証、電子証明書や秘密分散技術を用いた認証等により、制限されている。	
2.2 個人情報へのアクセス制御	① 個人情報にアクセスできる従業者の数は必要最小限である。 ② 個人情報にアクセスできる識別情報を複数人で共有していない。 ③ 従業者に付与するアクセス権限は必要最小限である。 ④ 個人情報を格納した情報システムの同時利用者数は制限されている。 ⑤ 個人情報を格納した情報システムの利用時間を制限している。 ⑥ 個人情報を格納した情報システムを無制限アクセスから保護している。 ⑦ 個人情報にアクセス可能なアプリケーションの無権限利用を防止している。 ⑧ 個人情報を取り扱う情報システムに導入したアクセス制御機能の有効性を検証している。	
2.3 個人情報へのアクセス権限の管理	① 個人情報にアクセスできる者を許可する権限管理を適切かつ定期的実施していること。 ② 個人情報を取扱う情報システムへのアクセスは必要最小限であるよう制御している。	
2.4 個人情報へのアクセス記録	① 個人情報へのアクセスや操作の成功と失敗の記録を取得し、保管している。 ② 取得した記録について、漏えい、滅失及びき損から適切に保護している。	ファイルアクセス履歴による履歴管理 漏えい→Lucida SecurOfficeのセキュアOSIによる対応 滅失、き損→Lucida SecurOfficeバックアップ機能
2.5 個人情報を取扱う情報システムに関する不正ソフトウェア対策	① ウイルス対策ソフトウェアが導入され、常に最新版が適用されている。 ② OSやアプリケーション等に対するセキュリティ対策用修正ソフトウェア(いわゆるセキュリティパッチ)を適用している。 ③ 不正ソフトウェア対策の有効性・安定性を確認している。 ④ 個人情報にアクセスできる端末にファイル交換ソフトウェア(WinnyやShareなど)をインストールしていない。	アプリケーション禁止機能 アプリケーション一覧機能による確認
2.6 個人情報の移送・通信時の対策	① 個人情報の受渡しには授受の記録が残されている。 ② 個人情報を媒体で移送する時に、移送時の紛失・盗難が生じた際の対策が講じられている。 ③ 盗難される可能性のあるネットワーク(例えばインターネットや無線LAN等)で個人情報を送信(例えば本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等)する際に、個人情報の暗号化又はパスワードロック等を実施している。	パソコン操作レポート、ファイルアクセスレポート等 暗号化機能 暗号化機能
2.7 個人情報を取扱う情報システムの動作確認時の対策	① 情報システムの動作確認時のテストデータとして個人情報を利用していない。 ② 情報システムの変更時に、それらの変更によって情報システム又は運用環境のセキュリティが損なわれていないことを検証している。	
2.8 個人情報を取扱う情報システムの監視	① 個人情報を取扱う情報システムの使用状況を定期的にチェックしている。 ② 個人情報へのアクセス状況(操作内容を含む。)を定期的にチェックしている。	週次レポート等(各種レポート) 週次レポート作成通知メール(運用面での支援)