JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

中小企業向け個人情報保護対策WG
チェックシート集計結果

2006 年 12月

はじめに

10月26日に開催した西日本支部主催 NSF2006 in Osaka において中小企業向け個人情報保護WGから個人情報保護対策ﾁｪｯｸｼｰﾄの紹介、および来場者の皆様にはご自身や所属される組織のコンプライアンス並びに安全対策の現状を『認識度』『実践度』を対象にご確認戴きました。

その結果の整理、分析ができましたので、ご報告します。

なお、本報告は本ｾﾐﾅｰに参加して頂いた方の範囲での分析結果であり、世の中の一般動向、状況を表すものではありません。また回答して頂いた方もご自身の組織の全ての状況を把握できているわけではないと思われます。

しかし、JNSAのｾﾐﾅｰに参加されるｾｷｭﾘﾃｨ意識の高い皆さんの結果である、という点でみると、ひとつの目安になるところもあると思われます。

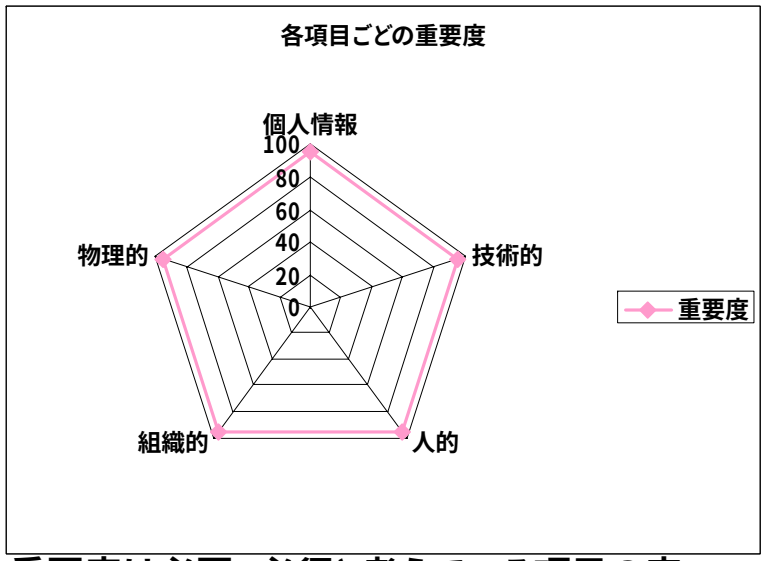
最後に, NSF2006 in Osakaにおいてﾁｪｯｸｼｰﾄの体感にご協力して頂いた来場者の皆様方に御礼を申し上げます。

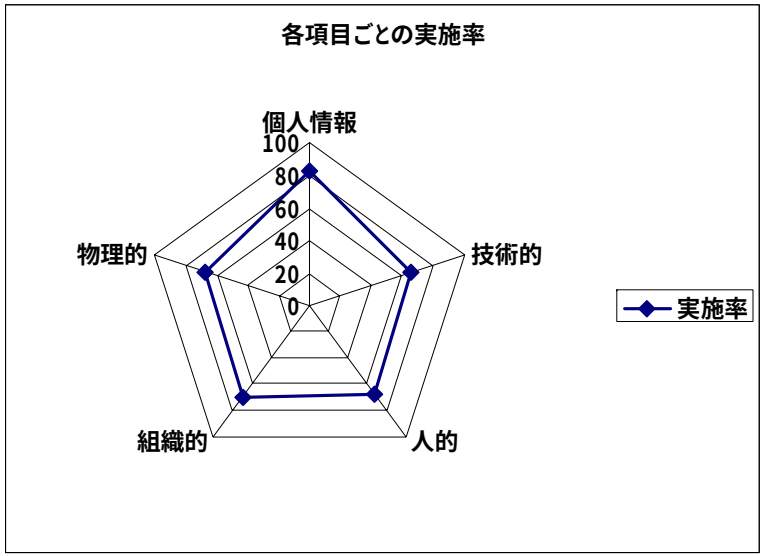
本資料をご覧戴き、感想、要望等を下記ﾒｰﾙｱﾄﾞﾚｽまでお送りください。

その際、入手したメールアドレス,お名前,所属する組織名などの個人情報に関しましてはJNSAの研究活動以外で利用することはなく一切開示いたしません。

送り先 ： sec@jnsa.org

全体の傾向





重要度は必要、必須と考えている項目の率

コメント

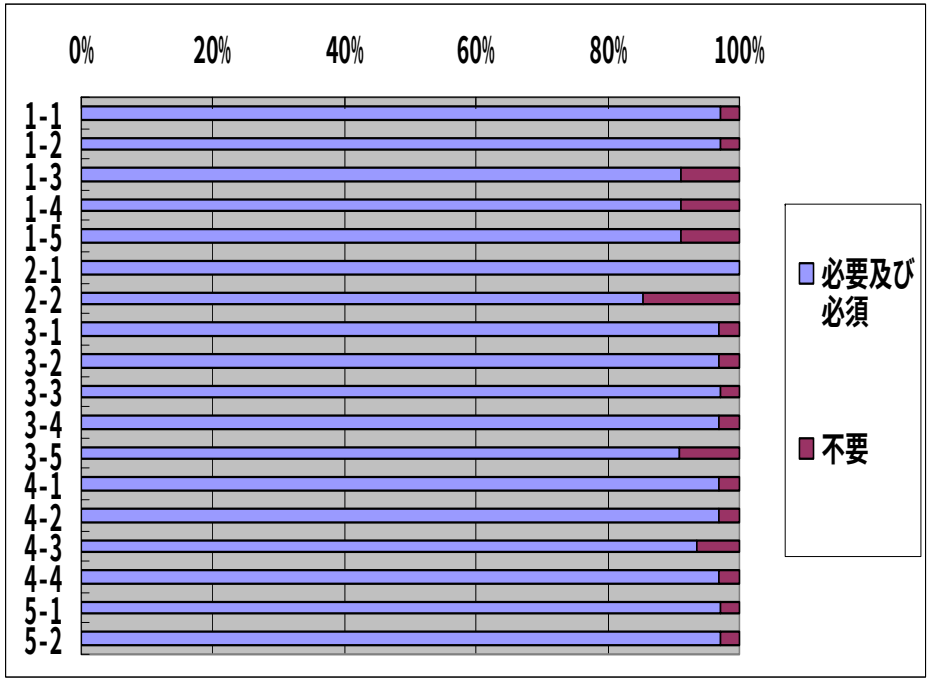
全般的にみてチェック項目の重要性については95%が必要･必須との判断となっており、重要度の認識が高い。
個人情報保護にはコンプライアンスプログラムの要求事項（JisQ15001）と全般統制としての情報セキュリティマネジメントシステム（ISMS)への準拠という二面性が求められているが、この内、コンプアライアンスに対する重要度認識は高く、実践度面においても浸透していると認識される。
しかし、マネジメントの実施度については未だ対策しきれていない部分や対策を逡巡している部分が見られる。

①本人確認のため認証やウイルス対策、FW･ルーターの整備、シュレッダーの設置については１００%対策済みとなっており、まず、やれるところから実施するアプローチは着実に浸透している。

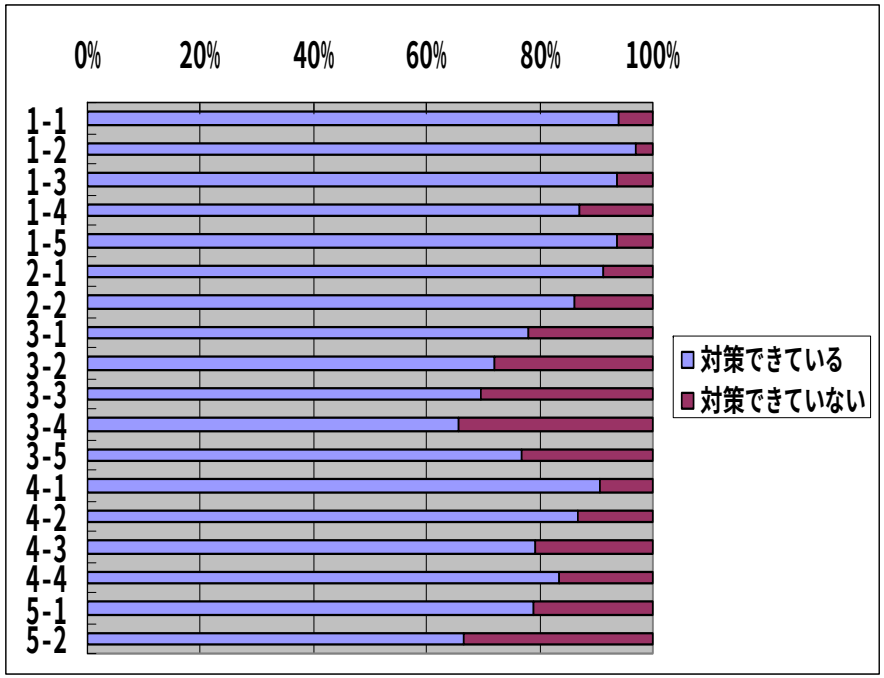
②反面、「費用対効果が見えにくい」、「コストがかかりすぎる」と言った経済的要因から、一過性の措置に比して、予算化、コストのかかる技術対策、長期的･継続的な対応の実施度が低い結果となって現れている。

③また、中小企業特有の傾向とも思慮されるが、業務遂行上の必要から来る利便性重視から業務時間外でのアクセス禁止、ソフトウェアの無断使用、ＦＤＤ、ＣＤ等の電磁記録媒体の使用制限、出力制限に対しては、実施度は低い。更に、人的関係では信頼関係を基調とするために、性悪説を肯定出来ず個人の行動を監視･牽制･評価、賞罰実施すること、及び業務委託先を点検･監査する実施には「逡巡」からか、規定化に比して実施度は低い。

個人情報取扱措置の詳細



※重要度の必要、必須をまとめ、不要と分類

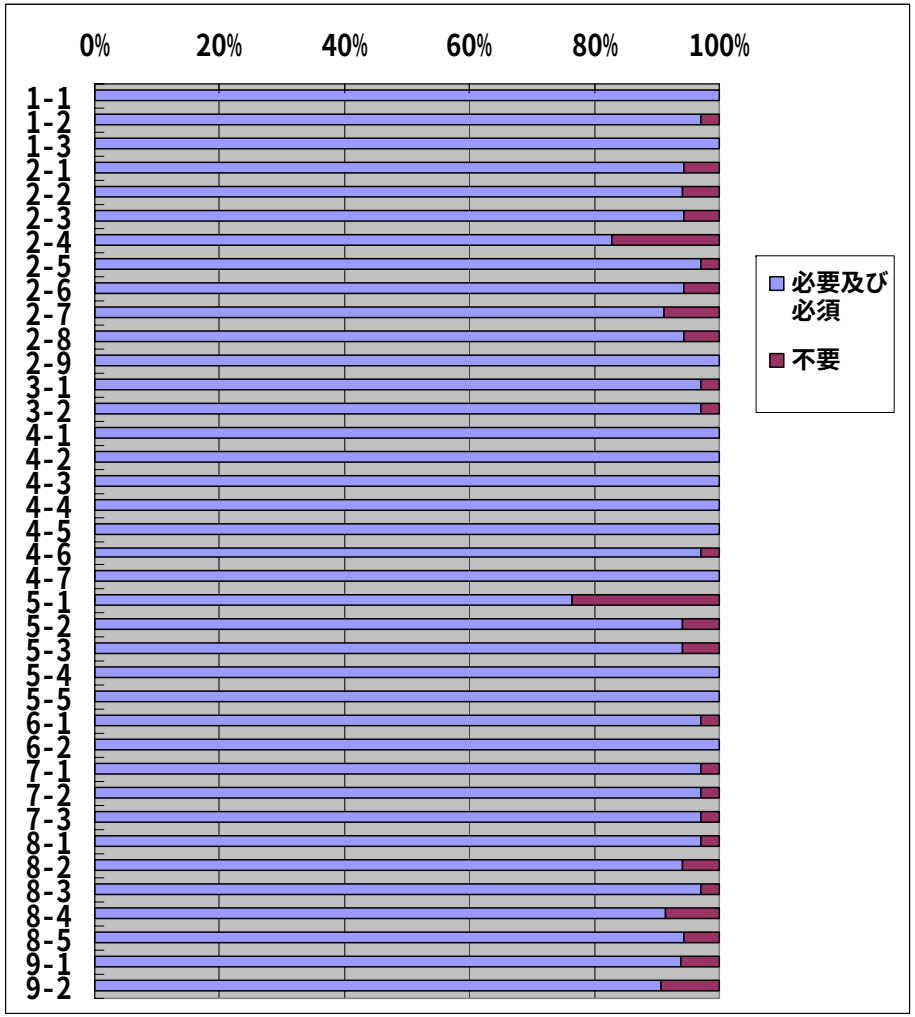


※重要度を必要もしくは必須と回答している方に限定し、実践度3,4を対策できているとし、実践度0,1,2を対策できていないに分類

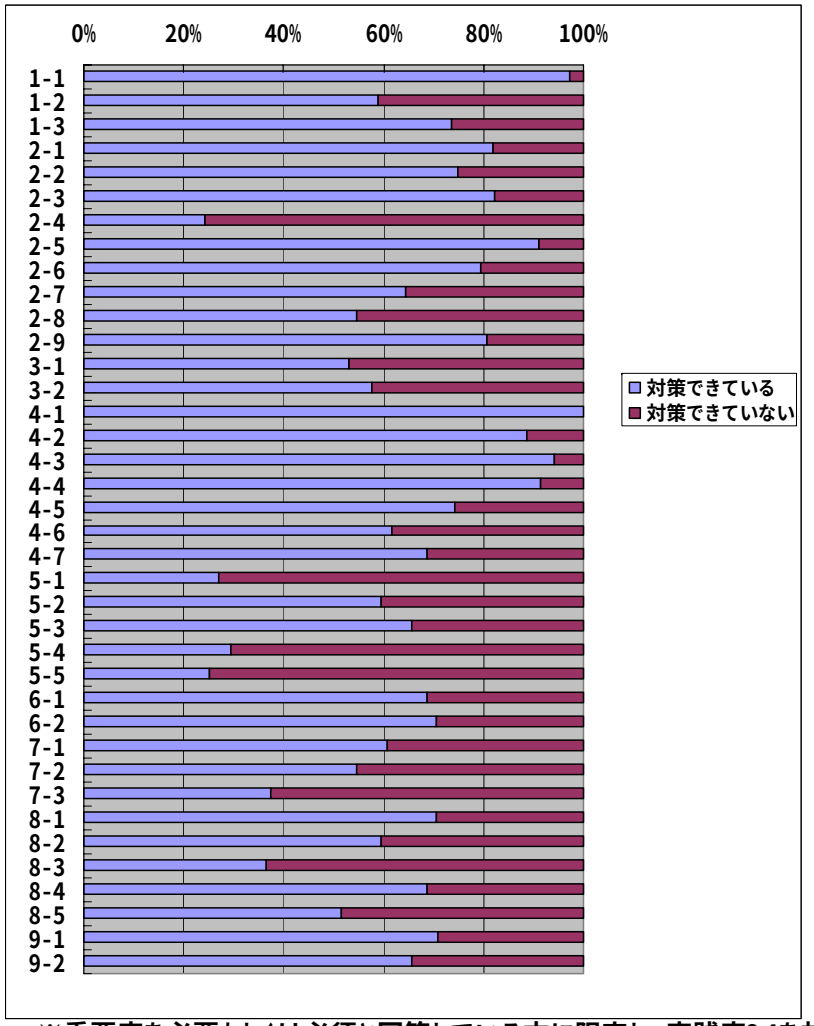
コメント

重要度に対する認識度は高く、実施度の面においても浸透度は高い。ただし、3-1～5の適正管理に関する措置では、他の技術的対策、物理的対策などの安全管理措置との関連もあり、明確化に回答ができない傾向が伺える。

個人情報技術的安全管措置の詳細



※重要度の必要、必須をまとめ、不要と分類



※重要度を必要もしくは必須と回答している方に限定し、実践度3,4を対策できているとし、実践度0,1,2を対策できていないに分類

個人情報技術的安全管措置の詳細

コメント

技術的安全管理措置のうち以下の項目については実践度が80%以上であり、対策の浸透度が高い。

- ユーザ認証(1-1)

  なお、ユーザ認証の実施率に比べ接続端末の認証の実践度は低く、端末認証まではまだ浸透していないことが伺える。
- アクセス権限を必要最小限に設定(2-1)
- ユーザ認証に基づくアクセス制御(2-3)
- ファイアウォール、ルータなどのインフラ整備(2-5)
- ユーザ認証機能、ユーザ権限設定機能をもつアプリケーションの利用
- スクリーンセーバの設定など覗き見対策
- ウィルス対策ソフトの導入(100%の導入回答)
- Windowsアップデートやアンチウィルスソフトのパターンファイル更新、定期的なウィルススキャンなど日常におけるウィルス対策(4-2,3,4)

上記の実践度が80%以上を超えるものに対し、逆に50%以下(ほぼ50%近辺のものを含めて)のものは以下のとおり。

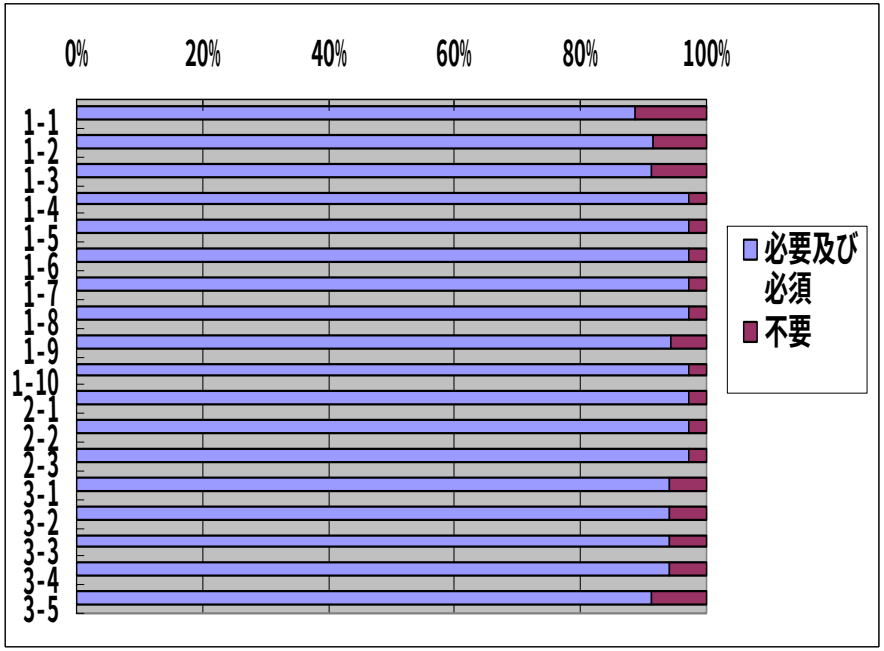
- 業務時間外のﾃﾞｰﾀアクセス制限(2-4)
- USBやCD-Rの使用制限(2-8,5-1)
- アクセス記録の採取、保存、定期的な検査(3-1.2,7-2)
- 印刷可能なデータは業務遂行上、必要最小限としている(5-4)
- システムの脆弱性の定期的な検査(7-3)
- バックアップ媒体の正常性確認(8-3)
- バックアップデータの暗号化(8-5)

さらに70%程度以下の実践度まで広げてみると1-2,4-6,4-7,5-2,5-3,6-1,6-2,7-1,8-2,8-4,9-1,9-2が該当する。

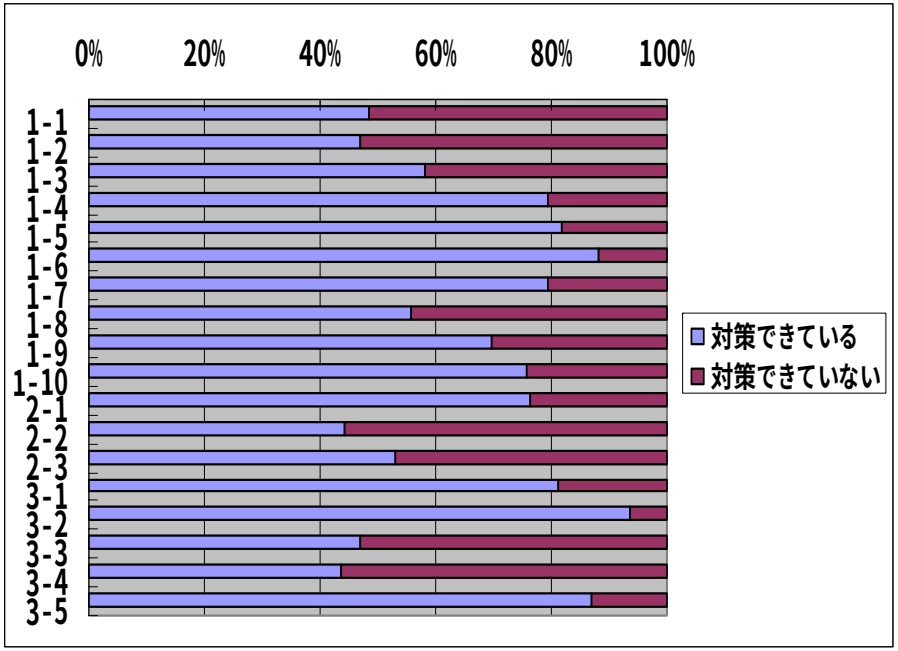
これらの実践度が70%以下の各項目に対して必要性をどう感じているか、という問いに2-4,5-1以外は全て90%以上が必須･必要と捉えており、業務遂行上の必要から来る利便性とのバランス感覚から、これらの対策については逡巡が見られる。

なお、システムの脆弱性の定期的検査、バックアップの正常性確認については、何処まで実施すれば対策済みかの具体例の明示がないために、判断が困難となり対策出来ていないが６０%を超えたものと見られる。

個人情報人的安全管措置の詳細



※重要度の必要、必須をまとめ、不要と分類

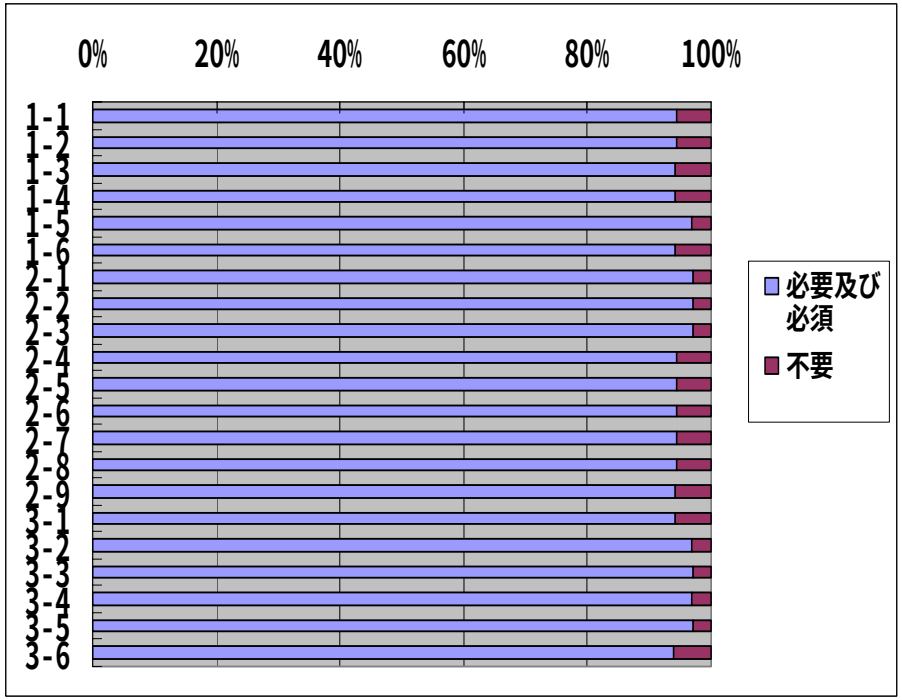


※重要度を必要もしくは必須と回答している方に限定し、実践度3,4を対策できているとし、実践度0,1,2を対策できていないに分類

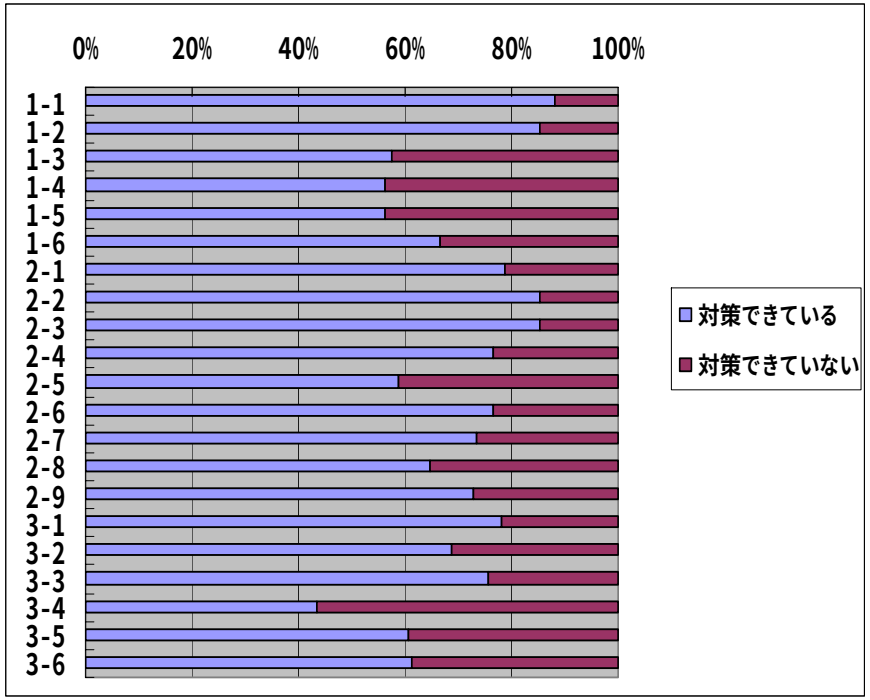
コメント

規定に盛り込む事で対策済みと認識できる対策（1-4,1-5、1-6,1-9,1-10）ならびに業務委託における基準(3-1,3-2)、法的対応(3-5)の実施度は80%を超える。
それに対し、1-1,1-2,2-2,2-3,3-3,3-4といった人的信頼関係が及ぶ対策については、実践度が50%以下である。
1-8については、業務遂行上の必要性から来る利便性とのバランス感覚からの逡巡が見られ、実施度が６０%を下回っている。

個人情報組織的安全管理措置の詳細



※重要度の必要、必須をまとめ、不要と分類



※重要度を必要もしくは必須と回答している方に限定し、実践度3,4を対策できているとし、実践度0,1,2を対策できていないに分類

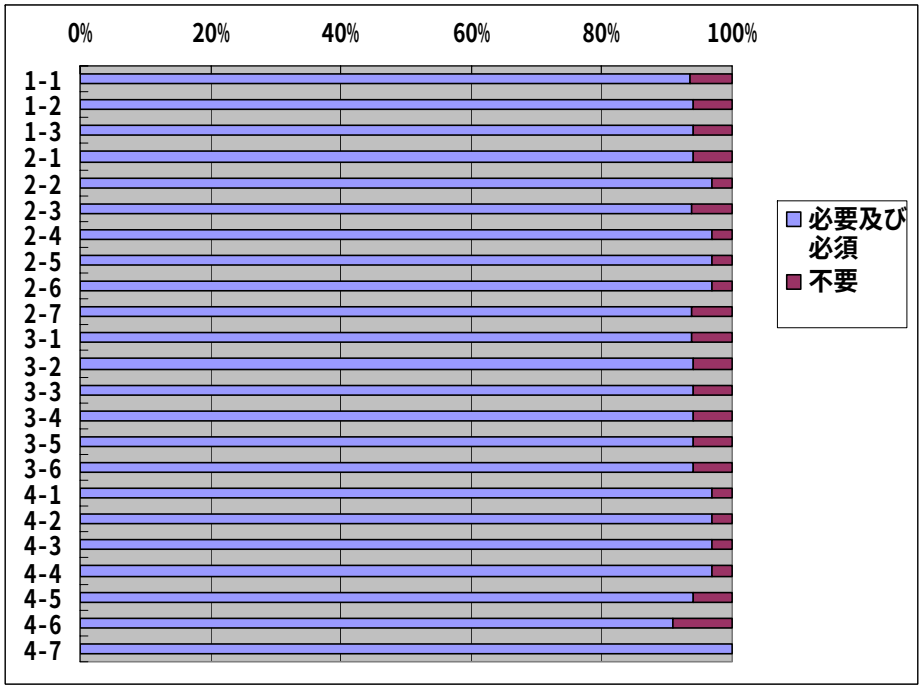
コメント

やや強引にではあるが、2つに分類した場合、①一度の対策で完結するもの：1-1,1-2,2-1,2-2,2-3,2-6,3-1,3-2,3-3,②定期・長期的対策が必要なもの:1-3,1-4,1-5,1-6,2-4,2-5,2-7,2-8,2-9,3-4,3-5,3-6となる。①の実施率の平均80%、②の実施率の平均62%となり、定期・長期的対策が必要な項目の実施率が低いことがわかる。

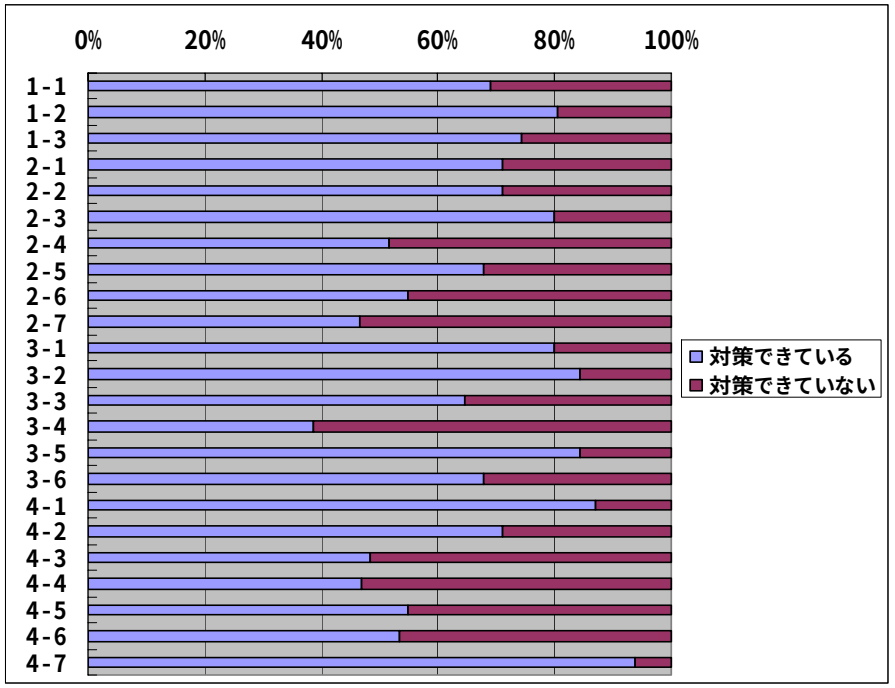
状況の定期的なチェック(1-6)、監査(2-8)、見直し(2-9)がそれぞれ65%を超えているものの、計画・予算化(1-3,4,5)の実施率が低い。その結果、チェック、監査及び見直しは2/3程度ができているものの、投資の必要な技術的安全管理措置が適切に行われていない可能性が伺える。それを反映してか、組織的安全管理措置だけでは実施が難しい、アクセス記録(3-4)の実施率が著しく低い。

アクセス記録(3-4)の実施率が低い理由として、次の2点が考えられる。1)技術的安全管理措置のアクセス記録の措置(技術的安全管理措置3-1)ができていないために低い可能性。2)”他の人に開示されているか”の解釈が分かれた可能性。技術的安全管理措置3-1の実施率53%を鑑みると、①の理由が大きい可能性がある。

個人情報物理的安全管措置の詳細



※重要度の必要、必須をまとめ、不要と分類



※重要度を必要もしくは必須と回答している方に限定し、実践度3,4を対策できているとし、実践度0,1,2を対策できていないに分類

コメント

入退室管理および媒体管理について、十分に対策が出来ていない傾向がみられる。

入退室管理においては、特に定期的な運用が必要になる部分 (2-4, 2-6) で実践度が低く、また、人の動線管理 (2-7) についても、実践できていない状況がみられた。

媒体管理については、外部記憶媒体の管理 (4-4, 4-5, 4-6) について実践度が低く、利便性とリスクのどちらを取るかの逡巡を示すものと思われる。

その他、災害対策 (3-3, 3-4, 4-3) においても実践度が低い傾向がみられるが、これは建物の基本構造に関わる部分もあるため、対策のしにくさを表すものと思われる。

付　録

チェックシート

チェックシートの項目
(個人情報取扱措置)

個人情報取扱措置	
1	収集に関する措置
1-1	個人情報の収集は、収集目的を明確に定め、その目的の達成に必要な限度において行われているか
1-2	個人情報の収集は、適法、かつ公正な手段によって行われているか
1-3	業務上必要としない（法により禁止されている場合を含む）機微な個人情報の収集、利用又は提供を行っていないか (1) 思想、信条及び宗教に関する事項 (2) 人種、民族、門地、本籍地（所在都道府県に関する情報を除く）、身体・精神障害、犯罪歴、その他社会的差別の原因となる事項 (3) 勤労者の団結権、団体交渉及びその他団体行動の行為に関する事項 (4) 集団示威行為への参加、請願権の行使及びその他の政治的権利の行使に関する事項 (5) 保健医療及び性生活に関する事項
1-4	業務に必要の無い情報を所持していないか 本人から直接に個人情報を収集する場合、担当者は本人に対して、次に示す事項を記載した書面若しくはこれに代わる方法によって通知し、本人の同意を得ているか (1) 個人情報に関する問合せ部署名及び連絡先 (2) 収集目的 (3) 個人情報を第三者に提供することが予定される場合には、その目的、当該情報の受領者及び個人情報の取扱いに関する契約の有無 (4) 個人情報をデータ処理等のために第三者に預託することが予定される場合には、その旨 (5) 本人が個人情報を与えることの任意性及び当該情報を与えなかった場合に本人に生じる結果 (6)個人情報の開示を求める権利及び開示の結果、当該情報が誤っている場合に訂正、追加、削除を要求する権利の存在並びに本人が当該権利を行使するための具体的な方法
1-5	本人以外から間接的に個人情報を収集する場合、担当者は本人に対して、1-4に示す事項を記載した書面若しくはこれに代わる方法によって通知し、本人の同意を得ているか
2	利用及び提供に関する措置
2-1	個人情報の利用及び提供は収集目的の範囲内で行われているか
2-2	本人が同意を与えた収集目的の範囲外で利用及び提供を行う場合、担当者は本人に対して、1-4に示す事項を記載した書面若しくはこれに代わる方法によって通知し、本人の同意を得ているか

チェックシートの項目
(個人情報取扱措置)

3	適性管理に関する措置
3-1	個人情報を収集目的に応じ必要な範囲内において正確かつ最新の状態で管理しているか
3-2	保有するすべての個人情報を特定し、特定するための手順を確立しているか
3-3	個人情報へのリスク(不正アクセス、紛失、破壊、改ざん及び漏えい)に対して合理的な安全策を講じているか
3-4	個人情報へのリスクに対する安全策を定期的に見直しているか
3-5	情報処理を委託するなどのために個人情報を預託する場合、十分な個人情報の保護水準を満たしている者を選定する基準を確立しているか、また保護水準を明記した契約を締結しているか
4	情報主体の権利保全に関する措置
4-1	本人(本人)からの苦情及び相談窓口を設け適切に対応しているか
4-2	本人(本人)から自己の情報について開示を求められた場合、合理的な期間内に応じているか
4-3	本人(本人)から自己の情報について訂正又は削除を求められた場合、合理的な期間内に応じているか、また訂正又は削除を行った場合は通知を行っているか
4-4	本人(本人)から自己の情報について利用又は第三者への提供を拒まれた場合、これに応じているか
5	教育・監査
5-1	役員及び従業員に個人情報を適切に取り扱うための適切な教育を行っているか
5-2	個人情報が適切に取り扱われているか運用状況を定期的に監査しているか

チェックシートの項目
(個人情報技術的安全管理措置)

個人情報技術的安全管理措置	
1	アクセス権限の管理
1-1	アクセス権限を有するユーザ本人であることの識別と認証(例えば、IDとパスワードによる認証)の実施をしているか
1-2	アクセス権限を有する端末の識別と認証(例えば、MACアドレス認証、電子証明書等)の実施をしているか(端末認証をする場合でも1-1ユーザ認証は必要である)
1-3	IDとパスワードを利用する場合、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等のポリシーを設けているか 例) - システム的にポリシー違反のパスワード設定を不可としている - 教育を行い、ポリシー違反しないように指導、徹底している
2	アクセス制御
2-1	アクセス制御を付与すべきユーザを必要最小限にしているか
2-2	アクセス制御を付与すべき端末数を必要最小限にしているか
2-3	ユーザ認証に基づいたアクセス制御をしているか
2-4	業務時間外は個人データにアクセスできないような措置を講じているか
2-5	ファイアウォール、ルータ等を設定して、個人データを格納したシステムを無制限アクセスから保護しているか
2-6	個人データにアクセス可能なアプリケーションに、ユーザ認証機能、ユーザ権限設定機能を持たせているか
2-7	個人データにアクセス可能なアプリケーションは必要最低限のコンピュータにしかインストールしていないか
2-8	個人データにアクセス可能なコンピュータに、不必要なモデム、USBメモリ、CD-R等のデバイスの使用を許可していないか 例) - システム的に使用を制限する仕組みを導入している - 教育を行い、不必要なモデム、USBメモリ、CD-R等のデバイスを使用しないように指導、徹底している
2-9	離席時におけるのぞき見に備え、何らかの対策(例えば、パスワード付きスクリーンセイバー)により見えないようになっているか

チェックシートの項目
(個人情報技術的安全管理措置)

3	アクセスの記録
3-1	個人データへのアクセスの記録 (例えば、ファイルの場合、誰が=ユーザID、何時、何を=個人データID、何処から=端末ID、どうしたか=作成、保存、移動、複製、参照、修正、削除等を成功したか失敗したか)を残しているか
3-2	アクセス記録を漏洩、滅失及び毀損から適切に保護すると共に一定期間保管しているか
4	不正プログラム対策
4-1	ウイルス対策ソフトウエアを導入しているか
4-2	OS、アプリケーション等に対するセキュリティパッチを適用しているか 例) - 自動的にセキュリティパッチの適用が行われる設定にしている - 教育を行い、セキュリティパッチの適用を行うよう指導、徹底している
4-3	ウィルス対策ソフトのパターンファイル更新をしているか 例) - 新しいパターンファイル更新を自動的に行う仕組みを導入している - 教育を行い、新しいパターンファイル更新を行うよう指導、徹底している
4-4	周期的にウィルススキャンを行っているか 例) - スキャンは自動的に行う仕組みを導入している - 教育を行い、周期的にスキャンを行うよう指導、徹底している
4-5	危険性のあるインタネットサイトへのアクセスを制限しているか 例) -システム対策している -教育を行い、危険性のあるインタネットサイトにはアクセスしないよう指導、徹底している
4-6	危険性のあるインタネットサイトからのソフトウエアのダウロードを禁止しているか 例) -システム対策している -教育を行い、危険性のあるインタネットサイトからのソフトウエアのダウロードをしないよう指導、徹底している
4-7	許可していないソフトウエアのインストールを禁止しているか 例) -アクセス権限による制限などシステム対策している -教育を行い、許可していないソフトウエアのインストールをしないよう指導、徹底している

チェックシートの項目
(個人情報技術的安全管理措置)

5	出力制限
5-1	部署内ではＦＤＤドラブ、ＣＤＷドライブ等を物理的に除去する等、電磁記録媒体を必要としない環境としているか
5-2	持ち出し端末での個人データの使用を禁止しているか
5-3	持ち出し端末で個人データを使用する場合には、ディスクの暗号化等の情報漏洩・端末紛失対策を行うと共に、持ち込時には最新のウイルス検知ソフトの検査を実施しているか
5-4	印刷可能なデータ項目は業務遂行上の必要最小限としているか
5-5	印刷可能なデータ項目は業務遂行上の必要最小限としているか
6	移送・送信時の対策
6-1	移送時における紛失・盗難に備え、個人データを格納したコンピュータ、媒体に何らかの対策(例えば、個人データの暗号化、輸送業者選択（セキュリティ便等）)をおこなっているか
6-2	通信時における盗聴に備え、個人データを通信するネットワークに何らかの対策(例えば、通信の暗号化、https)をおこなっているか
7	情報システムの監視・監査
7-1	個人データを取り扱うシステムの使用状況の監視・監査をしているか
7-2	個人データへのアクセス記録の監視・監査をしているか
7-3	個人データを取り扱うシステムの脆弱性有無の検証を定期的におこなっているか
8	バックアップ・保管
8-1	個人データのバックアップは定期的に行っているか
8-2	バックアップは数世代前まで遡って復元可能なように、複数世代で管理しているか
8-3	定期的にリストア確認を行い、バックアップの正常性を確認しているか
8-4	個人データを消去する場合には適切な措置を講じているか(例えば、専用のソフトウエアを利用する)
8-5	万一の盗難や紛失の事態に備えて、外部保管用のデータは暗号化しているか
9	開発環境の分離
9-1	個人データを取り扱うシステムの動作確認のテストデータとして実際の個人データを使用していないか（もしくはマスクをかけてもらう）
9-2	個人データを取り扱うシステムの変更時に、変更によりシステム又は本番の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か

注：5-4,5-5は編集時の誤りで同一項目となっています

チェックシートの項目
(個人情報人的安全管理措置)

個人情報人的安全管理措置		
1	不正予防対策	
1-1		特定の組織、個人に権限が集中する事の無い様に役割･責任の明確化に配意した職務分掌となっているか
1-2		組織間、個人間で、業務の相互牽制が行われているか
1-3		個人の行動（アクセス、接待など）ができるだけ、他の人に開示されているか
1-4		規程等を周知徹底し、行動に組み込むとともに、繰り返し注意喚起しているか
1-5		入社、異動、退職などが発生した場合には、システム管理、機密保持など関して、説明、引継、返却等を規程により実施し、管理者が確認しているか
1-6		機密情報については、在職中、退職後を問わず開示、漏洩しないよう、社員に対して誓約書などを取り交わしているか
1-7		個人識別のための社員証やIDカードの発行･管理が適切に行われると共に、退職者等のパスワードは遅滞無く無効化しているか
1-8		フロッピーデスク、ＣＤ等の電磁記録媒体の私物持込み制限が行われているか
1-9		机の上を退社時にはきれいにするクリアデスクポリシーやが離席時におけるディスプレイを見えなくするクリアスクリーンポリシーが採用されているか
1-10		書損印刷物溶解処理（もしくは類似した外部業者への廃棄処置）は実行されているか

チェックシートの項目
(個人情報人的安全管理措置)

2	教育	
2-1		個人情報の取り扱いに関する従業者の役割及び責任を定めた内部規程等についての社員教育を定期的に行っているか
2-2		個人情報保護レベルが目標に達しない場合の対応措置を講じているか ・チェックリストによる効果測定や賞罰の実施 ・プライバシーリーダ制度の導入
2-3		個人情報保護レベルの均質化を図る為の対策を講じているか ・個人情報保護週間や個人情報保護強化月間の推進 ・Webによるトレーニングや個人情報保護試験の実施 ・個人情報保護啓発セミナーやグッズの配布
3	業務委託	
3-1		業務委託先の選定基準が整備されているか
3-2		委託先と締結する契約書に以下のような要求事項が記載されているか ・ 機密保持や知的財産権についての取り決め ・ 再委託の禁止または書面による事前許可 ・ 事故発生時の立ち入り検査や損害賠償 ・ 業務終了後の情報の返却や廃棄
3-3		業務委託先の点検や監査を実施しているか
3-4		委託先の点検や監査の結果に基づいて、委託先の見直しを行っているか
3-5		下請代金支払遅延等防止法(下請法)の遵守はできているか

チェックシートの項目
(個人情報組織的安全管理措置)

個人情報組織的安全管理措置		
1	組織・体制	
1-1		情報セキュリティポリシーの策定の下、個人情報を管理・統制する仕組みがつくられているか
1-2		個人情報保護の管理体制を全社的に構築・整備されているか ・個人情報管理委員会等
1-3		個人情報保護の為の中長期及び年間の計画が立てられているか
1-4		個人情報が漏洩した場合等の対処策として、危機管理計画を策定しているか
1-5		個人情報保護の施策を実施する予算が確保されているか
1-6		個人情報保護の状況(規定等の遵守状況等)をチェックする仕組があるか
2	規程・マニュアル・ルール	
2-1		個人情報を取り扱う業務内容や個人情報の特性、リスクに応じて、必要な規程、マニュアル、ルール等を文書化しているか
2-2		規定等の内容は、以下に例示する関連法規を遵守しているか ・刑法・民法 ・不正アクセス行為の禁止等に関する法律 ・不正競争防止法・公益通報者保護法 ・著作権法 ・個人情報の保護に関する法律 ・プライバシーマーク制度
2-3		規定等の運用者を特定すると共に、対象者に周知しているか
2-4		教育・啓発により規定類の周知徹底が図られると共に、必要な時に確実な運用が出来る手順が整備されているか
2-5		事故または違反が発生した場合に、迅速な原因究明等による再発防止手順が整備されているか
2-6		漏洩の原因が故意または過失による手順違反の場合、別に定める就業規則等に罰則規定がある
2-7		規定等に定めた事項に基づいて確実に運用されているか
2-8		規定等が遵守されている事を検証する為、定期的にチェック(監査等)を実施しているか
2-9		運用・監査・経営環境の変化に対応して、規定類等を適切に見直しているか

チェックシートの項目
(個人情報組織的安全管理措置)

3	取扱台帳の整備･管理	
3-1		個人情報を洗い出して、個人情報管理台帳(利用目的、保管場所、保管方法、アクセス権限者、利用期限等)を作成しているか
3-2		洗い出された個人情報には重要性の評価が行われているか
3-3		保有管理者及び管理責任者を明確にした台帳管理をしているか
3-4		個人データへのアクセスは記録されると共に、出来るだけ他の人に開示されているか
3-5		入社、異動、退職などが発生した場合には、システム管理、機密保持など関して、説明、引継、返却等を規程により実施し、管理者が確認しているか
3-6		台帳の更新は内容に変更がある都度、また、定期的(3ヶ月、半年等)に見直しをしているか

チェックシートの項目
(個人情報物理的安全管理措置)

個人情報物理的安全管理措置		
1	セキュリティ区画	
1-1		個人情報のある場所（保管、格納形態がサーバ,紙を問わず）を特定すると共に、セキュリティ区画として識別しているか
1-2		セキュリティ区画の出入口は、不特定多数の人が行き交わないような場所にあるか
1-3		セキュリティ区画外に個人情報の無断、持ち出しを制限しているか
2	入退室管理	
2-1		個人情報を保管する場所の入退館及び入退室に関する管理責任者を定めているか
2-2		個人情報を保管する場所の出入口で（社員通用、お客様用、搬入用などそれぞれで）入退管理を行っているか 例）-入退室時にICカードによる個人認証を行い、履歴を保管している -入退室時に監視を行い（カメラ･警備員など）、履歴を保管している
2-3		個人情報を保管する場所へ第3者が入室する時は社員が立ち会っているか
2-4		個人情報を保管する場所の入退室時の履歴に関して、定期的に確認しているか
2-5		個人情報を保管する場所の入退館及び入退室に関する管理規程はあるか
2-6		個人情報を保管する場所の入退館及び入退室に関する運用を定期的に見直ししているか
2-7		個人情報を閲覧する機会のある場所を社外、社内を問わず閲覧権限のない人間が通ることがないよう、人の動線管理をしているか
3	設備	
3-1		個人情報を保管する場所の出入口には（社員通用、お客様用、搬入用などそれぞれに）入退管理設備を設けているか 例）-個人識別ICカードによる施錠設備がある -常時警備員を配置している -監視カメラがある
3-2		個人情報を保管する場所に外部からの侵入による盗難、破壊等を防止する措置をしているか 例）-建屋の低層階の窓のある部屋に個人情報を置かない -施錠管理可能なキャビネット内に保管している
3-3		個人情報を保管する場所は火事、水害、停電などの対策はできているか 例）-個人情報は火の気のない場所に保管する -サーバルームには可燃物を置かない -建屋の低層階に個人情報を保管しない -無停電装置を設置している
3-4		個人情報を保管する建屋は免震構造など、災害対策が充分か
3-5		個人情報を格納するサーバへの電源供給は、停電時においても確保する予備電源をもつ、もしくは速やかに自動的にサーバをシャットダウンさせ個人データの破壊、棄損が生じない設備を設けているか
3-6		個人情報にアクセス可能なノートPCにはチェーンロック等で盗難防止措置を実施しているか

チェックシートの項目
(個人情報物理的安全管理措置)

4	媒体管理	
4-1		個人情報を含むバックアップ媒体(DAT,MOなど) は施錠可能な場所で保管しているか
4-2		複数世代のバックアップ媒体を整理整頓して保管しているか
4-3		バックアップ媒体の保管場所は、火事、水害などへの対策がとられているか 例) -火の気のない場所に保管する -建屋の低層階に保管しない -複数のバックアップを別々の場所 (遠隔地) に保管する
4-4		個人情報にアクセス可能なサーバ・PCでのFD,CD,DVD,USBメモリー等、外部記憶媒体の使用を制限しているか
4-5		FD,CD,DVD,USBメモリー等の外部記憶媒体の所在、管理者が明確であり、周期的に管理状況を確認しているか
4-6		個人所有のPC,PDA,携帯電話、デジタルオーディオプレーヤーやFD,CD,DVD,USBメモリー等の外部記憶媒体の持込みを禁止あるいは制限しているか
4-7		個人情報を含む媒体 (紙に印刷されたものを含む) の破棄に対して対策がとられているか 例) -シュレッダーで裁断後に破棄している -専門の廃棄業者に委託している