別紙４

委託業者におけるセキュリティ対策について

既存のサービスデリバリーセンターにおける安全性

弊社サービスデリバリーセンターは、設備の安全対策のみならず、業務継続性を担保しますので、自然災害等による業務停止リスクを低減することが可能となります。

東西2拠点での運営のメリット

- **BCP対応**
  両拠点間でファシリティ及びオペレーション標準化、相互データバックアップを実施
  → **いずれかのセンターでBCPが発動された際、速やかな切り替えによる事業継続が可能**
- **生産キャパシティの柔軟な融通**
  各センターにおける処理要領の平準化が可能

既存のサービスデリバリー拠点における安全対策

- **頑強な建築構造と防火設備**
  関東大震災（M7～8）の地震に耐えられる建築構造かつ消防法を確実に満たす防災設備を完備
- **安定的な電源供給（自家発電設備の所有）**
  通常時は事業所が所有する変電設備（特高電源）から電源を供給し、一般の商用電源とは異なり安定供給を実現。計画停電時には自家発電装備の利用が可能。保全部隊も常駐しており、即時復旧が可能。
- **定期避難訓練の実施**
  有事に備え、年に1回の事業所全体の定期避難・消火訓練を実施
- **システムの二重化**
  他拠点とのネットワーク・サーバ機器持合いによる二重化
  プロセス管理システムはハードウェア・ソフトウェアの両面で二重化

既存のサービスデリバリーセンター

安全性／セキュリティ対策

認証資格

- BS7799-2:2002とISMS認証基準（Ver.2.0） 取得（2004年1月）
  ドキュメントアウトソーシングサービス事業領域として、日本で初めて取得
- ISO27001認定取得：登録NO：IC03J0033（2006年）

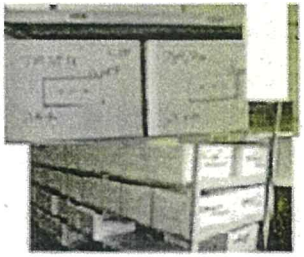
トレーサビリティカメラ

処理過程をすべてトレースすることで、万が一誤発送や紛失につながる作業ミスが発生したとしても、その原因追究が可能。

- 90台のトレーサビリティカメラ配備
- 撮影された内容は90日間保存

倉庫管理システム

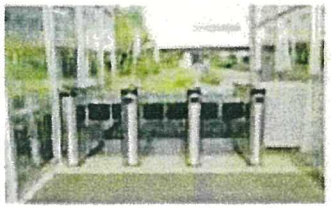
倉庫管理システムが、授受簿の箱・冊情報を抽出し、その内容をプロセス管理システムと連動させているため、ピッキングの情報等をすべてトレースし、書類紛失等を防止



プロセス管理システムと
連動した倉庫管理

入退室管理

従業員を含む全ての訪問者は、事業所の入退室管理で全て管理されているだけでなく、サービスデリバリーセンターエリアへの入室は、専用のICカード型装置によって制御

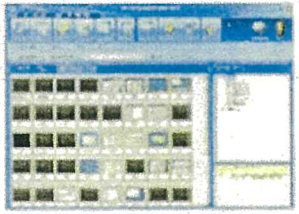


事業所入退出ゲート

ICカード型入退室
セキュリティ装置

システム・ネットワークからの不正アクセス防止

- クライアントPC管理ツール
  クライアントPC監視ツール（SKYSEA）により、不正アクセスや情報漏えいを防止し、ハード・ソフトウェアを防御
  - 不許可端末検知／遮断
  - 不許可のアプリケーションの無断インストール監視
  - 規定時間外端末機操作防止
  - 記憶媒体の使用および書込み制限
  - アクセスログの閲覧、収集
  - Windows パッチの配布と適用

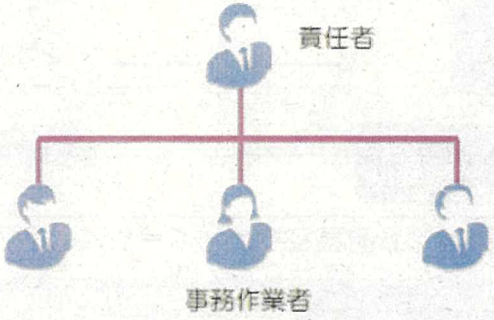


クライアントPC監視ツー（SKYSEA）

富士ゼロックスが考える安全管理措置①

弊社では、マイナンバーを取り扱うBPOサービスのご提供にあたり、「組織的」「人的」「技術的」「物理的」の四つの観点で安全管理措置の考え方を設定します。

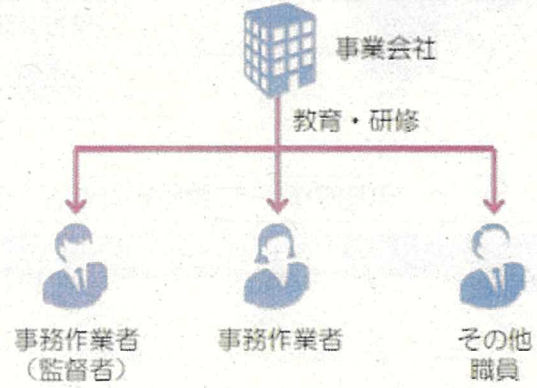
① 組織的安全管理措置　組織体制の整備



- 責任者・事務作業者※の明確化
  （部署・役職などの紐付けも可）
- 担当者が取扱う特定個人情報の範囲の明確化
- 取扱規程違反、情報漏えい時などの報告連絡体制の構築
- 複数部署で取扱う場合の役割分担・責任の明確化

※ 事務作業者：マイナンバーが付番された帳票を用いて事務を実施する担当者

② 人的安全管理措置　事務作業者の監督や教育

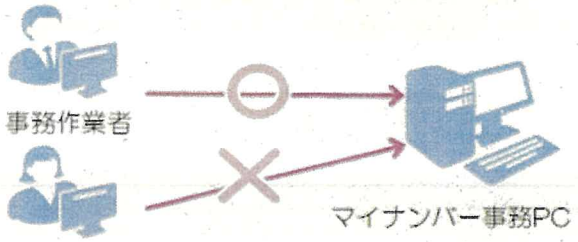


- トレーニングや研修の実施
- トレーニングを受講した専任者のみで対応
- 監督方法の設定
- 職員に対する周知徹底

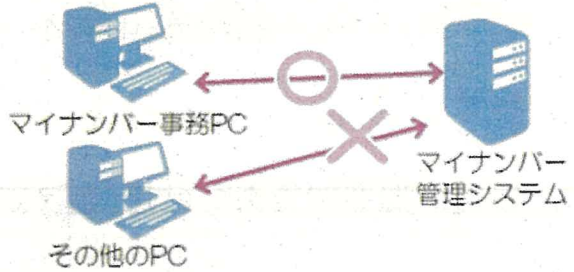
富士ゼロックスが考える安全管理措置②

③ 技術的安全管理措置　アクセス制御

① アクセス可能ユーザの限定

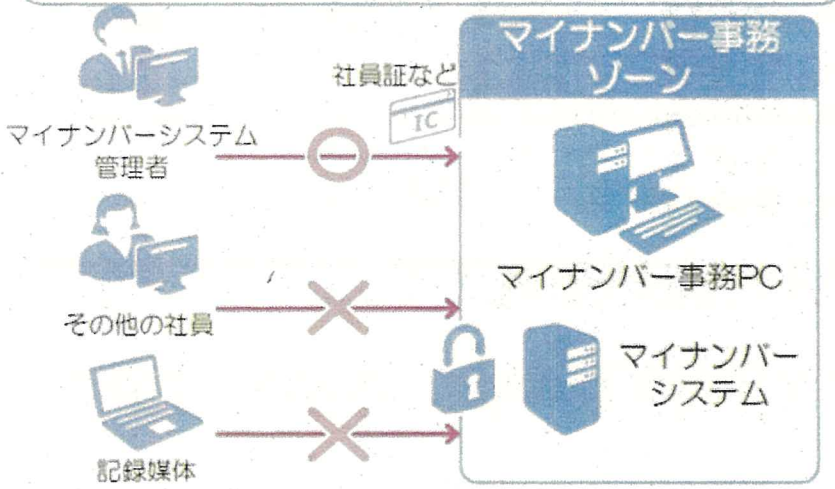


② アクセス可能システムの限定



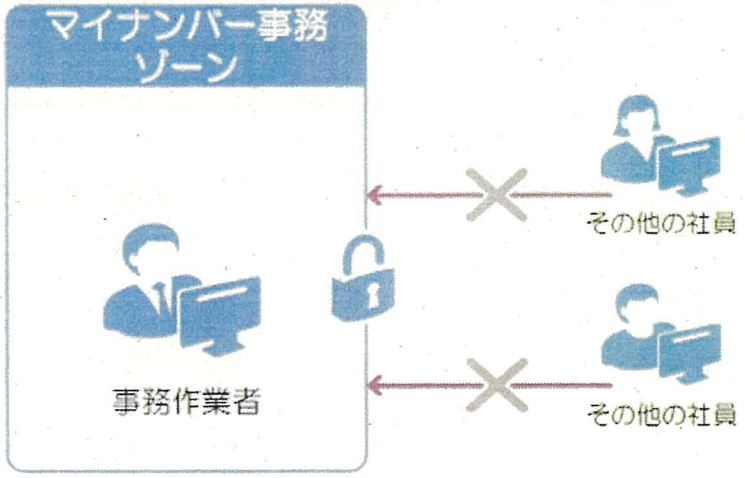
④ 物理的安全管理措置　特定個人情報などを取扱区域の管理

① マイナンバーシステムを管理する区域（管理区域）



- 社員証などによる入退室管理、記録媒体の持ち込み禁止・制限

② マイナンバーを扱う事務を実施する区域（取扱区域）



- 担当者以外の往来・覗き込みの防止

マイナンバー取り扱いサービスの安全管理措置（標準）①

安全管理措置項目		説明	対応
組織的安全管理措置	a.組織体制の整備	安全管理措置を講するための組織体制を整備する	責任者・担当者毎の役割や責任を明確にした組織体制の整備
	b.取扱規定等に基づく運用	取扱規定等に基づく運用状況を確認するため、システムログまたは利用実績を記録する	特定個人情報を取り扱う各機器のシステムログ、アクセスログ、操作ログを記録
	c.取扱状況を確認する手段の整備	特定個人情報ファイルの取扱状況を確認するための手段を整備する	特定個人情報ファイルごとの取扱台帳を整備する。 (ファイルの種類・名称/責任者、取扱い部署、利用目的、削除廃棄状況、アクセス権を有するもの)
	d.情報漏洩等事案に対応する体制の整備	情報漏洩等の事案の発生または兆候を把握した場合に、適切かつ迅速に対応するための体制を整備する	エスカレーション、および原因調査・対策検討体制の整備
	e.取扱状況の把握および安全管理措置の見直し	特定個人情報等の取扱状況を把握し、安全管理措置の評価、見直しおよび改善に取り組む	①ISMS（セキュリティ監査） 弊社内および外部機関による情報セキュリティリスクアセスメント、および改善計画の策定と実行 ②GSDM(富士ゼロックス標準の運営品質監査) 42のプロセス群におけるサイト運営の成熟度を判定、改善の方向性及び計画策定と実行
人的安全管理措置	a.事務取扱担当者の監督	事業者は、特定個人情報等が取扱規定等に基づき適正に取り扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行う	・担当者に対して、従業前に特定個人情報等の取扱いに関する教育受講とマイナンバー対応誓約書の提出を義務化 ・特定個人情報等の取扱いに関する留意事項等について、担当者に定期的な研修を実施
	b.事務取扱担当者の教育	事業者は、事務取扱担当者に、特定個人情報等の適正な取扱を周知徹底するとともに適切な監督を行う。	

マイナンバー取り扱いサービスの安全管理措置（標準）②

安全管理措置項目		説明	対応
物理的安全管理措置	a.特定個人情報等を取り扱う区域の管理	特定個人情報等を取り扱う情報システムを管理する区域(以下「管理区域」）と、特定個人情報等を取り扱う事務を実施する区域(以下「取扱区域」）を明確にし、物理的な安全管理措置を講する	＜管理区域および取扱区域＞ ・ICカードによる担当者の入退室管理、カメラ監視 ・PC、サーバのUSBポート使用不可制御 ・第三者の入室記録および作業時の管理者立ち会い ・私物（カメラつき携帯、かばん、雑誌等）の持込禁止 ＜取扱区域＞ ・作業スペースの物理的分離・・・取扱区域
	b.機器および電子媒体等の盗難等の防止		・可搬可能なPCはセキュリティワイヤー等で施錠 ・電子媒体や書類の施錠棚保管
	c.電子媒体等を持ち出す場合の漏洩対策	特定個人情報等が記録された電子媒体や書類等を持ち出す場合に、容易に個人番号が判明しない措置の実施、追跡可能な移送手段の利用等安全な方策を講する	・特定個人情報を含む書類の郵送時は、追跡が可能な書留を利用。 ・私書箱ー取扱区域間の郵送物輸送は、信書便対応業者によるセキュリティ便を利用して輸送。運搬用容器は施錠。
	d.個人番号の削除、機器および電子媒体等の廃棄	・保管期間経過後、速やかに復元できない手段で削除、廃棄する ・削除/廃棄の記録。委託する場合は証明書を取得する。	保存期間を経過した特定個人情報を含む情報は、媒体別に以下の方法で廃棄・削除 ・書類・・・溶解 ・データ・・・データ物理削除 ・機器/媒体廃棄・・・専用ツールを利用してダミーデータ上書き

マイナンバー取り扱いサービスの安全管理措置（標準）③

安全管理措置項目		説明	対応
技術的安全管理措置	a.アクセス制御	情報システムを使用して個人番号関係事務または個人番号利用事務を行う場合、事務取扱担当者および当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う。	アクセス可能ユーザ、付与するアクセス権の最小化
	b.アクセス者の識別と認証	特定個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有するものであることを、識別した結果に基づき認証する。	・PCは「ユーザID＋生体(指紋)」認証 ・サーバ、システム、NW機器等は「ユーザID＋パスワード」認証 ・ユーザIDは個人別に管理（ユーザIDの共用禁止） ・退職者のユーザＩＤは、速やかに削除 ・パスワード要件は以下のとおり。 ①8桁以上、英数混在 ②3ヶ月に一度のパスワード変更
	c.外部からの不正アクセス等の防止	情報システムを外部からの不正アクセスまたは不正ソフトウェアから保護する仕組みを導入し、適切に運用する。	・クラウド上のデータ授受用フォルダ(Working Folder)へのアクセスに対しては、ファイアウォールによりIP/ポートフィルタリングを実施 ・上記データ授受用フォルダへのアクセス許可PC、およびユーザは、必要最小限に限定 ・PCやサーバへのウィルス対策ソフト導入、および最新版パターンファイルの適用 ・OSやシステムの脆弱性確認時は、緊急度に応じて必要なパッチを適用
	d.情報漏えい等の防止	特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を講ずる。	・データ授受用フォルダ(Working Folder)への通信経路はSSLで暗号化 ・サーバ内に保存されたデータの暗号化