講ずべき安全管理措置の内容			ガイドラインにおける手法の例示	Dellの対応ソリューション	内容
A	－	基本方針の策定	特定個人情報等の適正な取扱いの確保について組織として取り組むための、基本方針を策定	Dell SecureWorks セキュリティ&リスクコンサルティングサービス	マイナンバーに関する特定個人情報保護の 方針・規程の整備サポート サービス
B	－	取扱規程等の策定	特定個人情報等の具体的な取扱いを定める取扱規程等の策定	Dell SecureWorks セキュリティ&リスクコンサルティングサービス	マイナンバーに関する特定個人情報保護の 方針・規程の整備サポート サービス
講ずべき安全管理措置の内容			ガイドラインにおける手法の例示	Dellの対応ソリューション	内容
C	－	組織的安全管理措置	事業者は、特定個人情報等の適正な取扱いのために、次に掲げる組織的安全管理措置を講じなければならない。		
C	a	組織体制の整備	安全管理措置を講ずるための組織体制を整備する。 ≪手法の例示≫ ＊ 組織体制として整備する項目は、次に掲げるものが挙げられる。 1・ 事務における責任者の設置及び責任の明確化 2・ 事務取扱担当者の明確化及びその役割の明確化 3・ 事務取扱担当者が取り扱う特定個人情報等の範囲の明確化 4・ 事務取扱担当者が取扱規程等に違反している事実又は兆候を把握した場合の責任者への報告連絡体制 5・ 情報漏えい等事案の発生又は兆候を把握した場合の従業者から責任者等への報告連絡体制	1,2,3,4,5,6 Dell SecureWorks セキュリティ&リスクコンサルティングサービス	1,2,3,6 は、マイナンバーに関する特定個人情報保護の 方針・規程の整備サポートサービスに包含可能(オプション) 4,5 は、CSIRP(Computer Security Incident Response Plan)策定支援サービスに包含可能
C	b	取扱規程等に基づく運用	取扱規程等に基づく運用状況を確認するため、システムログ又は利用実績を記録する。 ≪手法の例示≫ ＊ 記録する項目としては、次に掲げるものが挙げられる。 1・ 特定個人情報ファイルの利用・出力状況の記録 2・ 書類・媒体等の持出しの記録 3・ 特定個人情報ファイルの削除・廃棄記録 4・ 削除・廃棄を委託した場合、これを証明する記録等 5・ 特定個人情報ファイルを情報システムで取り扱う場合、事務取扱担当者の情報システムの利用状況(ログイン実績、アクセスログ等)の記録	1,5 Dell SecureWorks マネージド セキュリティサービス	1,5 ログ保管サービスにて、Syslogを保管 2,3,4 に関してファイルを特定して記録(デジタル、アナログ両方)するソリューションは未提供
C	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。 なお、取扱状況を確認するための記録等には、特定個人情報等は記載しない。 ≪手法の例示≫ ＊ 取扱状況を確認するための記録等としては、次に掲げるものが挙げられる。 1・ 特定個人情報ファイルの種類、名称 2・ 責任者、取扱部署 3・ 利用目的 4・ 削除・廃棄状況 5・ アクセス権を有する者	1,2,3,4,5 Dell SecureWorks セキュリティ&リスクコンサルティングサービス	1,2,3,4,5 マイナンバーに関する特定個人情報保護の方針・規程の整備サポートサービスに包含可能(オプション)
C	d	情報漏えい等事案に対応する体制の整備	情報漏えい等の事案の発生又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。 情報漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、事案に応じて、事実関係及び再発防止策等を早急に公表することが重要である。 ≪手法の例示≫ ＊ 情報漏えい等の事案の発生時に、次のような対応を行うことを念頭に、体制を整備することが考えられる。 1・ 事実関係の調査及び原因の究明 2・ 影響を受ける可能性のある本人への連絡 3・ 委員会及び主務大臣等への報告 4・ 再発防止策の検討及び決定 5・ 事実関係及び再発防止策等の公表	1,2,3,4,5 Dell SecureWorks セキュリティ&リスクコンサルティングサービス	1,2,3,4,5 CSIRP(Computer Security Incident Response Plan)策定支援サービスに体制整備のドキュメントを包含可能
C	e	取扱状況の把握及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、見直し及び改善に取り組む。 ≪手法の例示≫ 1＊ 特定個人情報等の取扱状況について、定期的に自ら行う点検又は他部署等による監査を実施する。	1,2 Dell SecureWorks セキュリティ&リスクコンサルティングサービス	1,2 セキュリティ安全管理措置アセスメントサービス

講ずべき安全管理措置の内容			ガイドラインにおける手法の例示	Dellの対応ソリューション	内容
D	－	人的安全管理措置	事業者は、特定個人情報等の適正な取扱いのために、次に掲げる人的安全管理措置を講じなければならない。		
D	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程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。	未対応	非IT項目
D	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いを周知徹底するとともに適切な教育を行う。 ≪手法の例示≫ 1＊ 特定個人情報等の取扱いに関する留意事項等について、従業者に定期的な研修等を行う。	1,2 Dell SecureWorks セキュリティ&リスクコンサルティング サービス	1,は、セキュリティ各発レポートに含有可能(オプション) 2,は、マイナンバーに関する特定個人情報保護の 方針・規程の整備サポートサービスに包含可能(オプション)
講ずべき安全管理措置の内容			ガイドラインにおける手法の例示	Dellの対応ソリューション	内容
E	－	物理的安全管理措置	事業者は、特定個人情報等の適正な取扱いのために、次に掲げる物理的安全管理措置を講じなければならない。		
E	a	特定個人情報等を取り扱う区域の管理	特定個人情報等の情報漏えい等を防止するために、特定個人情報ファイルを取り扱う情報システムを管理する区域（以下「管理区域」という。）及び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」という。）を明確にし、物理的な安全管理措置を講ずる。 ≪手法の例示≫ 1＊ 管理区域に関する物理的安全管理措置としては、入退室管理及び管理区域へ持ち込む機器等の制限等が考えられる。 2＊ 入退室管理方法としては、ICカード、ナンバーキー等による入退室管理システムの設置等が考えられる。 3＊ 取扱区域に関する物理的安全管理措置としては、壁又は間仕切り等の設置及び座席配置の工夫等が考えられる。	未対応	非IT項目
E	b	機器及び電子媒体等の盗難等の防止	管理区域及び取扱区域における特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的な安全管理措置を講ずる。 ≪手法の例示≫ 1＊ 特定個人情報等を取り扱う機器、電子媒体又は書類等を、施錠できるキャビネット・書庫等に保管する。 2＊ 特定個人情報ファイルを取り扱う情報システムが機器のみで運用されている場合は、セキュリティワイヤー等により固定すること等が考えられる。	未対応	非IT項目
E	c	電子媒体等を持ち出す場合の漏えい等の防止	特定個人情報等が記録された電子媒体又は書類等を持ち出す場合、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、安全な方策を講ずる。 「持出し」とは、特定個人情報等を、管理区域又は取扱区域の外へ移動させることをいい、事業所内での移動等であっても、紛失・盗難等に留意する必要がある。 ≪手法の例示≫ 1＊ 特定個人情報等が記録された電子媒体を安全に持ち出す方法としては、持出しデータの暗号化、パスワードによる保護、施錠できる搬送容器の使用等が考えられる。ただし、行政機関等に法定調書等をデータで提出するに当たっては、行政機関等が指定する提出方法に従う。 2＊ 特定個人情報等が記載された書類等を安全に持ち出す方法としては、封緘、目隠し	1, Dell DDP|Encryption	1,の電子媒体持ち出しに対して、様々な形式の媒体に暗号化を実施することが可能 2,は非IT項目
E	d	個人番号の削除、機器及び電子媒体等の廃棄	個人番号関係事務又は個人番号利用事務を行う必要がなくなった場合で、所管法令等において定められている保存期間等を経過した場合には、個人番号をできるだけ速やかに復元できない手段で削除又は廃棄する。 個人番号若しくは特定個人情報ファイルを削除した場合、又は電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存する。また、これらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて、証明書等により確認する。 ≪手法の例示≫ 1＊ 特定個人情報等が記載された書類等を廃棄する場合、焼却又は溶解等の復元不可能な手段を採用する。 2＊ 特定個人情報等が記録された機器及び電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等により、復元不可能な手段を採用する。 3＊ 特定個人情報ファイル中の個人番号又は一部の特定個人情報等を削除する場合、容易に復元できない手段を採用する。 4＊ 特定個人情報等を取り扱う情報システムにおいては、保存期間経過後における個人番号の削除を前提とした情報システムを構築する。 5＊ 個人番号が記載された書類等については、保存期間経過後における廃棄を前提とした手続を定める。	未対応	1,5 は非IT項目 2,3,4 はソリューション未対応
講ずべき安全管理措置の内容			ガイドラインにおける手法の例示	Dellの対応ソリューション	内容
F	－	技術的安全管理措置	事業者は、特定個人情報等の適正な取扱いのために、次に掲げる技術的安全管理措置を講じなければならない。		
F	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又は個人番号利用事務を行う場合、事務取扱担当者及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。 ≪手法の例示≫ ＊ アクセス制御を行う方法としては、次に掲げるものが挙げられる。 1・ 個人番号と紐付けてアクセスできる情報の範囲をアクセス制御により限定する。 2・ 特定個人情報ファイルを取り扱う情報システムを、アクセス制御により限定する。 3・ ユーザーIDに付与するアクセス権により、特定個人情報ファイルを取り扱う情報システムを使用できる者を事務取扱担当者に限定する。	Active Directory等	弊社グローバルサービスによる導入支援サービスにて、Active Directory 等の機能を活用したアクセス制御環境の構築支援を提供
F	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者であることを、識別した結果に基づき認証する。 ≪手法の例示≫ ＊ 事務取扱担当者の識別方法としては、ユーザーID、パスワード、磁気・ICカード等が考	DDP|ST	指紋およびFelicaの多要素認証で対応
F	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又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。 ≪手法の例示≫ 1＊ 情報システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する。 2＊ 情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入する。 3＊ 導入したセキュリティ対策ソフトウェア等により、入出力データにおける不正ソフトウェアの有無を確認する。 4＊ 機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。 5＊ ログ等の分析を定期的に行い、不正アクセス等を検知する。	1, Dell SonicWALL 4, Dell KACE 3.5 Dell SecureWorks マネージド セキュリティサービス	1,は、Dell SonicWALL 次世代ファイアウォールによる保護を提供 2, ソリューション未対応 3, Dell SecureWorks マネージド セキュリティサービスによる監視で不正ソフトウェアの有無を確認 4, Dell KACE による、様々なソフトウェア更新の自動適用 5, Dell SecureWorks マネージド セキュリティサービスによるログの常時監視もしくは、コンサルティング サービスによる定期分析
F	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。 ≪手法の例示≫ 1＊ 通信経路における情報漏えい等の防止策としては、通信経路の暗号化等が考えられる。 2＊ 情報システム内に保存されている特定個人情報等の情報漏えい等の防止策として	1, Dell SonicWALL 2, Dell DDP|Encryption	1, Dell SonicWALL のSSL/VPN 機能により、通信経路の暗号化 2, Dell DDP|Encryption によるデータの暗号化