マイナンバーの安全管理措置チェックシート

マイナンバー対応情報セキュリティ検討 WG
情報セキュリティ検討チーム

2016 年 1 月 1 日より全ての企業にてマイナンバーの取り扱いが必須となり、業務検討・構築だけでなく、マイナンバーの漏洩を防止するための安全管理措置を取る必要があります。

この安全管理措置に関しては、2014 年 12 月 14 日に特定個人情報委員会がリリースした「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」に記載がありますが、マイナンバーを取り扱う際、どこまで対策すればいいか分からないと多くお聞きします。

そこで、JNSA マイナンバー対応情報セキュリティ検討 WG では、どの程度対策を取ればいかを確認できる「マイナンバーの安全管理措置チェックシート」を作成・公開しました。

◆「マイナンバーの安全管理措置チェックシート」の概要

○　上記「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」の安全管理措置に基づき、作成しています。

○　「最低限取るべき措置」と「オプションとして取るべき措置」に分け、チェック項目をまとめています。

※どこまで対策を取るべきか、具体的な指針は法律上ありません。本リストの「最低限取るべき措置」は JNSA の検討チームの視点で最低限対策が必要と判断したものです。

※「オプションとして取るべき措置」は、サイバー攻撃が高度化する中、できればここまで対策をとった方がより安全であろうと判断したものです。

○　対象はガイドラインに記載されている以下 4 項目です。

C　組織的安全管理措置
D　人的安全管理措置
E　物理的安全管理措置
F　技術的安全管理措置

各社においては、A 基本方針の策定、B 取扱規程等の策定が必要となりますが、その際に自社の安全管理措置に漏れがないか、このチェックシートをご利用頂ければと思います。

以　上

JNSA

マイナンバーの安全管理措置チェックシート

Ver.2（2015/11/12）

C　組織的安全管理措置　※特定個人情報の適正な取扱いに関するガイドライン（事業者編）を参照ください。（http://www.ppc.go.jp/files/pdf/261211guideline2.pdf）

P51　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。

a 組織体制の整備

P51　安全管理措置を講ずるための組織体制を整備する。

	最低限取るべき措置	コメント			プラスα（オプションとして取るべき措置）	コメント	
1	【前提条件】事業者は、安全管理措置を講ずるための取扱規程等を作成する。		□				□
2	事務における責任者の設置および責任と権限を明確にする。		□	①	個人情報保護管理者（いわゆる、チーフ・プライバシー・オフィサー（CPO））を設置する。		□
3	監査責任者を設置する。		□	②	特定個人情報管理者の任命および「特定個人情報の利用者の識別および認証」として「本人確認に関する情報」の管理者を任命する。		□
4	特定個人情報を取扱う情報システム運用責任者の設置および担当者（システム管理者を含む）を限定する。		□	③	特定個人情報の安全管理に関する従業者の役割・責任を職務分掌規程、職務権限規程等の内部規程、契約書、職務記述書等に具体的に定める。		□
5	事務取扱担当者の明確化およびその役割を明確にする。		□	④	事務取扱担当者が複数いる場合、責任者と事務取扱担当者を区分する。		□
6	個人番号関係事務担当者の明確化のために部所名（○○課、△△係）、事務名（××事務担当者）等を定める。		□				
7	特定個人情報の取扱い（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄等の作業）における作業責任者の設置および作業担当者を限定する。		□				
8	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にする。		□				
9	個人番号関係事務の範囲を明確にする。		□				
10	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を整備する。		□				
11	特定個人情報の取扱いに関する規程等に違反している事実、又は兆候があることに気づいた場合の、代表者等への報告連絡体制を整備する。	おかしいなと感じたら直ぐ窓口（社内担当者や弁護士等専門家）へ連絡・相談することが重要。	□				
12	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を整備し、周知する。		□				
13	監査実施体制を整備する。		□				
14	特定個人情報等を複数の部署で取り扱う場合の各部署の任務分担および責任を明確にする。		□				

b 取扱規程等に基づく運用

P51　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。

	最低限取るべき措置	コメント			プラスα（オプションとして取るべき措置）	コメント	
1	特定個人情報ファイルの利用・出力状況を記録する。		□	①	管理区域・取扱区域外への個人番号および個人情報を含む書類、媒体、携帯可能なコンピュータ等に関する持ち出しについて、持出管理記録簿で以下項目を管理する。 □日時 □担当者 □持ち出しデータ □利用目的（相手先） □移送経路 □返却日時 □データ消去等		□
2	個人データの取扱いを委託する場合における受託者の選定基準、委託契約書のひな型等の整備とそれらに従った運用を行う。		□				
3	就業規則等における安全管理措置を整備する。		□				
4	特定個人情報の安全管理に関する規程および委託先の選定基準の承認および周知徹底する。		□				

c 取扱状況を確認する手段の整備

P52　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。

	最低限取るべき措置	コメント		プラスα（オプションとして取るべき措置）		コメント	
1	特定個人情報ファイルの種類、名称を記載した台帳を作成する。		□				
2	特定個人情報ファイルの記載内容に対する定期的な確認と台帳を最新状態に維持する。		□				
3	特定個人情報ファイルの台帳へ各ファイルの責任者、取扱部署を明記する。		□				
4	特定個人情報ファイルの台帳へ各ファイルの利用目的を明記する。		□				
5	特定個人情報ファイルの台帳へ各ファイルの削除・廃棄状況を記載管理を		□				
6	特定個人情報ファイルの台帳へ各ファイルに対するアクセス権を有する者の記載管理をする。		□				
7	特定個人情報等の取扱状況の分かる記録を保存する。		□				

d 情報漏えい等事案に対応する体制の整備							
P53	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。						
最低限取るべき措置		コメント		**プラスα （オプションとして取るべき措置）**		コメント	
1	事実関係の調査および原因を究明する。	情報漏えいに関する報告窓口には、様々なレベルの報告が行われると考えられる。特定個人情報に限らず、個人情報全般における情報漏えいが起きた可能性がある状況について、報告された内容の事実関係および原因の究明を知見のある担当使者によって行うことが求められる。	□	①	事故対応に必要な技術的支援、ノウハウ、関連情報の入手を支援する人／チーム／部署の設置をする。		□
2	自社のマイナンバー関連ネットワークおよびシステムを把握する。	この機会に情報の取扱および情報漏えい対策を見直しましょう！	□	②	特定個人情報の漏えい等についての情報は代表窓口、苦情処理窓口を通じ、外部からもたらされる場合もあるため、苦情の処理体制等との連携を図る。		□
3	事故対応の担当者と責任者を明確にする。		□				
4	外部組織に依頼する場合の、外部の対応能力の把握と適切な報告をす		□				
5	影響を受ける可能性のある本人へ連絡をする。		□				
6	委員会および主務大臣等へ報告をする。		□				
7	事故発生時の報告窓口を一元化する。		□				
8	再発防止策の検討および決定をする。		□				
9	事実関係および再発防止策等を公表する。		□				
10	事故対応に必要なポリシーおよびマニュアル等を整備する。		□				
11	情報漏えい等の事案の発生等に備え、従業者から責任ある立場の者に対する報告連絡体制等をあらかじめ確認しておく。		□				
12	自社内外への報告体制を整備する。		□				

e 取扱状況の把握及び安全管理措置の見直し							
P53	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。						
最低限取るべき措置		コメント		**プラスα （オプションとして取るべき措置）**		コメント	
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（内部監査）を実施する。	外部主体による他の監査活動と合わせて、監査を実施することも有効。	□	①	新たなリスクに対応するための、安全管理措置を評価し、見直しおよび改善を行う。	次の項目を評価することを推奨 □特定個人情報保護対策および最新の技術動向を踏まえた社内の対応 □情報セキュリティ対策に十分な知見を有する者による（必要に応じ、外部の知見を有する者を活用し確認させることを含む）社内の対応 □同業他社で発生している事故の把握及び発生可能性の分析 □自社/他社で発生した事故傾向・原因を分類検証	□
2	これまで発生した事故の把握および傾向を分析をする。		□	②	定期的および臨時の点検を実施。また、点検の実施後において、規程違反事項等を把握したときは、その改善を行う。		□
3	特定個人情報を取り扱う部署において、点検計画を策定することにより点検体制を整備する。		□				
4	事故対応に必要なポリシーおよびマニュアル等を適宜改訂する。		□				
5	予測される事故発生場所の把握および傾向を分析する。		□				
6	責任ある立場の者が、特定個人情報等の取扱状況について、定期的に点検を行う。		□				

JNSA

マイナンバーの安全管理措置チェックシート

Ver.2（2015/11/12）

D	人的安全管理措置　※特定個人情報の適正な取扱いに関するガイドライン（事業者編）を参照ください。（http://www.ppc.go.jp/files/pdf/261211guideline2.pdf）
P54	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。

a 事務取扱担当者の監督

P54　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。

	最低限取るべき措置	コメント			プラスα（オプションとして取るべき措置）	コメント	
1	事務取扱担当者と特定個人情報等に関する非開示契約（誓約書）の締結する。	非開示契約（誓約書）：別途文書を作成する必要はなく、現在実施している秘密保持契約書などがあれば、追記する方が最適。	□	①	非開示契約（誓約書）の表現は、退職・契約解除後も一定期間有効とする。		□
2	違反した場合の罰則規定を整備する。	罰則の記載箇所として以下などがある。 □就業規則（従業員10名以上の事業者で就業規則を変更した場合は労基署への届出が義務となる） □マイナンバー等取扱規程（取扱数101名以上の事業者は作成義務がある（届出の必要は無し））	□	②	委託先の選定基準を元に、委託先（再委託先も含む）を定期的に評価し、継続有無を決定または適切な指導をする。		□
3	事務を委託する場合、委託元と委託先間での非開示契約（誓約書）を締結する。	非開示契約（誓約書）：別途文書を作成する必要はなく、現在実施している秘密保持契約書などがあれば、追記する方が最適。（無ければ作成する必要あり。） ・再委託先が発生する場合には、再委託先にも同様とする旨の文言を記載することが必要。	□	③	委託先に依頼をする場合には、委託先選定基準を設け、調査を実施した上で、基準値に満たした委託先に依頼をする。	委託先選定基準は以下などがある。 □委託元と同等レベルの安全管理措置をしているか否か。 □PマークやISMSを取得しているか否か。 □再委託をしているか否か。（している場合は、同様の管理かどうか）	□
				④	委託先の選定基準を元に、委託先（再委託先も含む）を定期的に評価し、継続有無を決定または適切な指導をする。		□

b 事務取扱担当者の教育

P54　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。

	最低限取るべき措置	コメント			プラスα（オプションとして取るべき措置）	コメント	
1	事務取扱担当者へ内部規程・手順書等の周知、教育・訓練を実施する。	教育内容には、マイナンバー対応以外に、以下を含めることが重要。 □標的型攻撃等のセキュリティインシデントの理解 □インシデントが発生した場合の連絡体制 □再発防止対応方法 □マイナンバーに関する最新情報（事件・事故も含む）	□	①	関与する者の役割と責任を定めた内部規程等について周知徹底をする。		□
2	全従業員へマイナンバーを収集する範囲・利用目的等を周知し、2015年10月以降に通知カードが届いた後の対応（収集等の手順等）について教育をする。	・手元に届かなかった場合や住民票を移せない場合など、ケーススタディ教育をすることも有効。 ・事業者は、従業者にカード本来の利用価値を理解してもらった上で、通知カードではなく、個人番号カードへの切替を促進することが重要。	□	②	事務取扱担当者以外のシステム（DB）管理者や関連従事者へも内部規程等の周知と教育・訓練を実施する。	社内従業員と同等の教育・訓練をする必要がある。（特にシステムに関しては、セキュリティインシデント教育は重要）	□
3	新入社員・中途社員の入社時にマイナンバーを収集できる仕組み作り（運用手順書・マニュアル整備など）と入社時教育（安全管理に関する内容も含む）を行う。	収集等は、その時期で方法が変わる可能性もあるため、手順書やマニュアルなどはその都度見直しをすることが重要。	□	③	教育・訓練を定期的に計画し、実施する。		□
4	全従業員へマイナンバーに限らず個人情報漏洩事件が起きた際の事業者への影響等を周知、教育する。		□	④	関与する者の教育実施記録、教育受講記録を取り、適切なフォローや見直しを実施する。（評価分析や力量管理など）	PDCAの活用が有効	□
				⑤	マイナンバー法のみならず、個人情報保護法の内容についても周知、教育を行う。		□
				⑥	マイナンバーに関する資格取得の促進や、資格取得のバックアップ体制を整備する。	マイナンバーについての資格（2015年9月現在） □マイナンバー実務検定：1級～3級（全情協主催） □マイナンバー管理士：マイナンバー実務検定１級と、全情協主催の個人情報保護士の双方資格保持者からの申請により付与される資格	□

JNSA

マイナンバーの安全管理措置チェックシート

Ver.2（2015/11/12）

E	物理的安全管理措置　※特定個人情報の適正な取扱いに関するガイドライン（事業者編）を参照ください。（http://www.ppc.go.jp/files/pdf/261211guideline2.pdf）
P54	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。

a 特定個人情報等を取り扱う区域の管理

P54　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。

	最低限取るべき措置	コメント			プラスα（オプションとして取るべき措置）	コメント	
1	個人情報を取り扱う情報システム機器等を施錠可能な室内等への設置および、記録簿による入退館（室）管理をする。	小規模組織であっても、最低でも1年は記録を保管しておき、定期的に毎月1回以上チェックするのが妥当。	□	①	独立した管理区域への担当者以外の立入禁止とICカード等による入退館（室）記録と施錠管理をする。		□
2	個人情報を取り扱う業務を施錠可能な室内もしくは間仕切り等によって仕切られた区域にて実施、および記録簿による入退館（室）管理をする。		□	②	独立した取扱区域へのICカード等による入退館（室）管理をする。		□
3	管理区域および取扱区域への災害対策*を実施する。	*災害対策：消火設備、地震対策（備品の固定や転倒防止等）、漏水・浸水対策（なるべく上方に置く等）、停電対策（UPS等）など	□	③	管理区域への、社外（個人所有）の電磁記録装置類（USBストレージ、スマホ、カメラ機能を有する機器類、デジタルオーディオ等）の持込を禁止とする。		□
4	取扱区域における端末画面への覗き見防止フィルタや机の向きを工夫するなど、漏えい事故防止策を講じる。		□				

b 機器及び電子媒体等の盗難等の防止

P54　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。

	最低限取るべき措置	コメント			プラスα（オプションとして取るべき措置）	コメント	
1	離席時の特定個人情報を記した書類、媒体、携帯可能なコンピュータ、情報システムの操作マニュアル等の机上等への放置を禁止する。		□	①	個人番号・個人情報を記した書類、媒体、情報システム機器を取り扱うエリア（取扱区域）および保管するエリア（管理区域）への防犯カメラや侵入監視装置等を設置する。		□
2	離席時のパスワード付きスクリーンセイバー等の起動を徹底する。		□	②	施錠可能な専用の書庫・キャビネット等を管理区域内に設置し、全てをそこに保管する。	特定個人情報を含む各種媒体は、複数個所に分散させずに一元管理できる方が望ましい。	□
3	特定個人情報を含む書類、外部記録媒体、携帯可能なコンピュータ等の持ち出し可能な各媒体を、施錠可能な書庫・キャビネット等にて保管、施錠管理をする。		□	③	個人情報と個人番号の分離保管をする。		□
4	個人番号、個人情報を取り扱う情報システム機器への盗難防止用ワイヤーロック設置、施錠管理をする。		□				

c 電子媒体等を持ち出す場合の漏えい等の防止

P55　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。

	最低限取るべき措置	コメント			プラスα（オプションとして取るべき措置）	コメント	
1	特定個人情報を含む電子媒体を持ち出す場合は、データの暗号化およびパスワード設定を実施する。 　また電子媒体が共用機器であれば利用履歴を残す。	強度の高い暗号アルゴリズム（AES-128以上）にすることが望ましい。	□	①	持ち出し制御機能として、USBメモリなど記録メディアへの書込み規制、プリントアウト規制等を行う。また、暗号化して廃棄されるまでの間のファイルアクセス履歴をログにて記録する。		□
2	書類（紙媒体）の持ち出し時は、中身が見えないよう封筒に入れるか目隠しシールを貼付、施錠可能な鞄等にて運搬し、置いたりせず常に携行する。 　また郵送する場合は簡易書留など送達過程が記録される手段を利用する。		□	②	管理区域・取扱区域外への個人番号および個人情報を含む書類、媒体、携帯可能なコンピュータ等に関する持ち出しについて、持出管理記録簿で以下項目を管理する。 □日時 □担当者 □持ち出しデータ □利用目的（相手先） □移送経路 □返却日時 □データ消去等		□
3	個人番号および個人情報を含む電子データを管理区域および取扱区域の外にネットワーク経由で送付する必要がある際は、通信の暗号化およびファイルのパスワード設定を行う。 　ただし、行政機関等に法定調書等を電子データで提出する必要がある場合には、当該行政機関等が指定する提出方法に従う。		□	③	個人番号および個人情報出力用プリンターの取扱区域内への設置と記録簿による出力管理、もしくは出力時にICカード等による認証を要するシステムの導入による出力履歴管理をする。		□

d 個人番号の削除、機器及び電子媒体等の廃棄

P55　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。

	最低限取るべき措置	コメント			プラスα（オプションとして取るべき措置）	コメント	
1	書類、メディア等の廃棄はシュレッダー、焼却または溶解等の復元不可能な手段を用いる。		□	①	シュレッダーはDIN規格レベル６以上など、復元が極めて困難な製品を使用する。		□
2	廃棄管理記録簿による、削除または廃棄の記録（委託の場合は証明書）作成（取得）、保管をする。		□				
3	電子データの廃棄時は、復元不可能な専用の削除ソフトウェア等を利用する。 　外部記憶装置自体の廃棄時は、装置そのものにデータの復元が不可能な物理的破壊を行う。		□				
4	特定個人情報から一定の保存期間経過後に個人番号が削除される前提での情報処理システム、管理マニュアルを作成する。	個人番号について、所管法令により一定期間の保存が義務付けられているものについて、当該期間が経過するまで保管が義務付けられる一方、法令上の保存期間を経過した際には可及的速やかに廃棄または削除しなければならない、という時限管理が必須となっている。	□				

5	個人番号が記載された書類が一定の保存期間経過後に廃棄される前提での保管手続きを作成する。	同上。 個人番号はあくまで個人番号関係事務又は個人番号利用事務に必要な範囲で保管できるものであって、原則として所管法令に定められた保存期間を超えて保存することはできない。 　例えば、扶養控除等申告書では所得税法施行規則で、当該申告書の提出期限の属する年の翌年1月10日の翌日から7年を経過する日まで保存すると規定されているが、この場合は当該期限まで保存義務があり、また当該期限を超えて保存することはできないということ。	□				

JNSA

マイナンバーの安全管理措置チェックシート

Ver.2（2015/11/12）

F	技術的安全管理措置　※特定個人情報の適正な取扱いに関するガイドライン（事業者編）を参照ください。（http://www.ppc.go.jp/files/pdf/261211guideline2.pdf）
P54	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。

a アクセス制御

P56　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。

	最低限取るべき措置	コメント			プラスα（オプションとして取るべき措置）	コメント	
例示	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。						
1	C.組織的安全管理措置、E.物理的安全管理措置において特定した特定個人情報を取り扱う人と機器に対するアクセス権限、権限設定の管理を情報システムに実装することで、個人番号と紐付けてアクセスできる情報の範囲を制限するために、データ自体もしくは保管機器にアクセス権限を付与する。		□	①	人事異動や担当変更によるアクセス権限の変更を、迅速かつ確実に行うためにActive Directory*等アクセス権限設定管理機能を活用し、管理者・取扱担当者・利用者など当該者に対して、個人番号と紐付けてアクセスできるシステムに対する適切な編集・参照などのアクセス権限の付与状態を維持する。	*Active Directory＝マイクロソフト社の製品	□
2	C.組織的安全管理措置、E.物理的安全管理措置において特定した特定個人情報を取り扱う人と機器に対するアクセス権限、権限設定の管理を情報システムに実装することで、個人番号と紐付けてアクセスできる情報の範囲を制限するために、ユーザー制御機能（ユーザーアカウント制御）により、情報システムを取り扱う事務取扱担当者を限定する。		□	②	個人番号と紐付けてアクセスできるシステムへのアクセスログを記録・保存することで、故意の漏洩抑止と迅速な侵害発生時の原因究明を実現する。		□
例示	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。						
1	C.組織的安全管理措置、E.物理的安全管理措置において特定した特定個人情報を取り扱う人と機器に対するアクセス権限、権限設定の管理を情報システムに実装することで、特定個人情報ファイルへのアクセスを制限するために、ユーザーＩD/パスワード管理(発行/更新/廃棄)を徹底する。		□	①	人事異動や担当変更によるアクセス権限の変更を、迅速かつ確実に行うためにActive Directory*等アクセス権限設定管理機能を活用し、管理者・取扱担当者・利用者など当該者に対して、特定個人情報ファイルへのアクセスに対する適切な編集・参照などのアクセス権限の付与状態を維持する。	*Active Directory＝マイクロソフト社の製品	□
2	C.組織的安全管理措置、E.物理的安全管理措置において特定した特定個人情報を取り扱う人と機器に対するアクセス権限、権限設定の管理を情報システムに実装することで、特定個人情報ファイルへのアクセスを制限するために、送信元IPアドレスによる制限で利用端末を制限する。		□	②	C.組織的安全管理措置、E.物理的安全管理措置において特定した特定個人情報を取り扱う人と機器に対するアクセス権限、権限設定の管理を情報システムに実装することで、特定個人情報ファイルへのアクセスを制限するために、MACアドレス、クライアント証明書による制限で利用端末を制限する。		□
				③	特定個人情報ファイルを取り扱う情報システムとの通信に必要な通信（IP,ポート）のみをゲートウェイ機器（ファイアウォール等）で許可する。		□
				④	ゲートウェイ機器の設定により、特定個人情報ファイルへのアクセス承認、および承認後の当該システムへのアクセス可能時間帯の制御を行う。		□
				⑤	特定個人情報ファイルへのアクセスログを記録・保存することで、故意の漏洩抑止と迅速な侵害発生時の原因究明を実現する。		□
				⑥	情報システムエリアとその他ネットワーク接続エリアを独立させる。		□
例示	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						
1	C.組織的安全管理措置、E.物理的安全管理措置において特定した特定個人情報を取り扱う人と機器に対するアクセス権限、権限設定の管理を情報システムに実装することで、特定個人情報ファイルへのアクセスを制限するために、ユーザー制御機能（ユーザーアカウント制御）により、情報システムを取り扱う事務取扱担当者を限定する。		□	①	特定個人情報ファイルへのアクセスをより厳密に事務取扱担当者に限定するために、当該情報システムへのアクセスを複数の要素認証を用いて制限する。		□
2	アクセス制御のポリシー運用の手順・方法を決定し、内容を記録する(マニュアル化など)		□	②	特定個人情報ファイル1つ1つに対し、適切なアクセスコントロールを設定する。		□
				③	DB 管理者による特定個人情報へのアクセスを制御する製品を導入する。		□
				④	管理者権限等、厳密に管理すべきサーバーやネットワーク機器の特権IDの管理ポリシーや管理体制を明確にし、管理を徹底する。		□
				⑤	アクセス権が適正がどうかについて、監査など定期的に見直しを行う。		□
				⑥	監視カメラ・端末操作監視など物理・システム双方の監視対象・方法及びその必要性を検討もしくは実施する。		□

b アクセス者の識別と認証

P57　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。

	最低限取るべき措置	コメント			プラスα（オプションとして取るべき措置）	コメント	
例示	1）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カード等が考えられる。						
1	C.組織的安全管理措置、E.物理的安全管理措置において特定した特定個人情報を取り扱う人と機器に対するアクセス権限、権限設定の管理を情報システムに実装することで、特定個人情報ファイルへのアクセスを制限するために、ユーザー制御機能（ユーザーアカウント制御）により、事務取扱担当者が特定個人情報を取り扱う情報システムへのアクセスを行う際には、ID、パスワードによる主体認証を行う機能を設ける。		□	①	特定個人情報ファイルへのアクセスをより厳密に事務取扱担当者に限定するために、当該情報システムへのアクセスを複数の要素認証を用いて制限する。要素としては、通常のユーザーＩDおよびパスワードの他に、ワンタイムパスワード、担当者の携帯物（ＩＣカード等）や担当者自身の生体認証等を利用する。		□
2	特定個人情報等を取り扱う情報システムにアクセスする事務取扱担当者に付与しているパスワードの複雑性・有効期限・履歴などの運用ポリシーを設定し、確実に運用する。		□	②	リスクベース認証（通常と異なる端末からのアクセス拒否、同じIDでのアクセスにおいて物理的に離れた場所から短時間でアクセスされた場合拒否等）の導入。		□
3	IDの同時使用（使い回し）を禁止する。		□	③	内部犯行を想定した特権管理措置として、ユーザIDの権限付与承認者と登録実施者を分離し、それぞれの職権ごとに異なるユーザIDを付与する（職権分離）し、IDの共用を禁止する。		□

c 外部からの不正アクセス等の防止							
P57	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。						
	最低限取るべき措置	コメント			プラスα （オプションとして取るべき措置）	コメント	
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。						
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/プロキシを設置し分離し、通信フィルタを記述することで、最小限のアクセスのみ有効とする。		□	①	情報システムと外部ネットワークとの接続箇所にゲートウェイ/リバースプロキシ、高度なマルウェア対策製品を導入する。		□
				②	情報システムと外部ネットワークとの接続箇所に、IDS/IPSを導入し、不正アクセスの検知及び遮断を実施する。		□
				③	情報システムと外部ネットワークとの接続箇所に次世代ファイアウォールを導入		□
				④	ファイアウォール/プロキシを設置する際に定義ファイルを明確化する。		□
				⑤	情報システムと外部ネットワークとの接続箇所に、WAF(Webアプリケーションファイアウォール）を導入し、アプリケーションの脆弱性を突いた攻撃の遮断を行う		□
				⑥	危険なメールの受信を排除する製品を導入する。		□
例示	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。						
1	情報システムにアクセスする端末機器にウイルス・マルウェア対策ソフトウェアを導入し、パターンファイルの更新を適切に行うことで、最新状態を維持し、定期的な調査を実施する		□	①	情報システムを取り扱うサーバーにマルウェア対策製品等を導入し、パターンファイルの更新を適切に行うことで、最新状態を維持し、定期的な調査を実施する。		□
2	不要なソフトウェアを導入しない。不要なサービスを停止・削除する。		□	②	情報システムを取り扱うサーバー、およびクライアント機器に振る舞い検知型のマルウェア対策製品等の導入を行い、未知のマルウェアの防御を行う。		□
				③	通信経路において、異なる定義ファイルを用いるマルウェア対策製品等を組み合わせる。または定義ファイルパターンマッチングや振る舞い検知等の異なる技術を用いる製品を組み合わせる。		□
例示	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。						
1	ウイルス・マルウェア対策ソフトウェアによるリアルタイム分析を行い、削除・防御等を行う。		□	①	アラート・通知などリアルタイムに気付ける仕組み(製品)を導入する。		□
例示	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にするよう努める。						
1	Windows Update等OSを最新状態にするよう努める。		□	①	NIST、IPA、ベンダー等から発信される脆弱性情報を定期的に収集し、OS、利用機器の更新プログラムを適用して最新状態を維持する。		□
2	利用しているソフトウェアを最新状態にするよう努める。		□	②	脆弱性情報をPush通知で受け取れる仕組みを導入し、素早く脆弱性を認知、対応する(脆弱性情報提供サービスの利用)		□
3	セキュリティ対策製品を最新状態にするよう努める。		□	③	OS、利用機器、ソフトウェアのＩＴ資産管理を自動化するシステムを利用し、更新プログラムの確実な自動適用や許可しないソフトウェア・サービスの導入防止、運用ポリシーに沿わない端末のアクセスを許可しない等の措置を講じる。 自動更新が望ましいが、難しい場合は運用フローを策定し、定期的な見直しを実施する		□
				④	システムに対し定期的な脆弱性診断を実施し、対策を講じることでセキュリティ侵害のリスクを軽減する。		□
例示	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	FWやウイルス対策ソフトウェア等のログを保存し、確認を行う。		□	①	ネットワークログやデータ操作ログ、オペレーション操作ログ等、複数のログを取得し、管理するシステムを導入する。保存するログの対象・期間・方法と確認ポイント及び対応手順など運用を決め、実施する		□
				②	改ざん検知・ログ収集など多層的なセキュリティ対策機能の利用するとともに、これらの対策を統合的に監視できるSIEM等を導入する。		□
				③	通信、サーバのログを常時監視し、不正アクセスを検知したらアラートを通知する仕組みを導入する。 アラート・通知などリアルタイムに気付ける機能が望ましい。		□
				④	自社内での専門部隊や外部の監視サービスなども含め、SOC/CSIRTといった体制化ができる事が望ましい。		□
				⑤	採取したログに対しても完全性維持が必要となるため、不正なログの改ざんや消去を防止の為に厳密なアクセス制御を行う。		□
				⑥	各サーバ等の時刻合わせを行う		□
				⑦	サーバー上にて動作させるプログラムをホワイトリストとして登録しておき、ホワイトリストに登録されていない不正なプログラムの起動を防止する。		□
				⑧	フィッシングを行う標的型メールの検知を実施するメールゲートウェイ装置の導入を行う。		□
				⑨	外部公開するサーバーにて、改ざんの検知・防止を行うシステムの導入を行う。		□
				⑩	不正アクセスや災害等で個人番号を含むデータベースが破壊された時のため、定期的なバックアップの取得ならびに保全を行うと共に、破壊されたときに正常にリストアできるよう定期的なリストア・テストを実施する。		□

d 情報漏えい等の防止							
P57	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。						
	最低限取るべき措置	コメント			プラスα （オプションとして取るべき措置）	コメント	
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。						
1	特定個人情報等を含んだデータを外部に送信する場合はSSL(TLS)、IPSec等による通信経路の暗号化を行う。また、通信経路の暗号化を実施する場合、危殆化した暗号化アルゴリズムは使用しない。該当環境がない場合は物理的輸送手段を取る。		☐	①	アプリケーション間、DB 間の通信の経路暗号化を実施する。		☐
2	特定個人情報にアクセスできる端末には、USB メモリ、外付けドライブ等の接続を管理する。		☐	②	特定個人情報に関しては、メールの使用は推奨しない。		☐
3	物理媒体（USBメモリ、外部記憶媒体など）やメールを使う場合は暗号化を実施する。特定個人情報にアクセスできる端末からは印刷は管理する。		☐	③	特定個人情報データ保存領域もしくは特定個人情報データ自体に暗号化を実施する。		☐
4	特定個人情報にアクセスできる端末からは印刷は管理する。		☐	④	特定個人情報を取り扱う端末、サーバーのHDDの暗号化を実施する。		☐
5	特定個人情報ファイルにパスワードをかける等アクセス制限を行う。		☐	⑤	特定個人情報データファイルの秘密分散を行う。		☐
6	不要になった特定個人情報のデータは完全消去が必要となる。 社内規定で復元が困難な消去ルールを決め、そのルールにより速やかに消去する。		☐	⑥	DLP(Data Loss Prevention) 対策製品を利用する。		☐
7	IPアドレス等により、特定のネットワークからの接続に限定する		☐	⑦	特定個人情報を含んだデータベースの暗号化を実施する。 例：特定のテーブルに対する参照範囲を列レベルで制御、データをマスキングする製品の導入等		☐
				⑧	持ち出し時の強制暗号を実現するソリューション(製品)を利用する。		☐
				⑨	ゲートウェイにおけるWeb/Mail経由での持ち出し制御を実装する。		☐
				⑩	拠点間をつなぐ仮想LANを構築する。		☐
				⑪	特定個人情報の取扱情報システムへのアクセスを行う端末と、業務で利用する端末を物理的に分ける。 ハイパーバイザによって、情報システムエリアとその他ネットワーク接続エリアを独立させる。		☐
				⑫	フォワードプロキシにてホワイトリストを登録し、登録されたアクセス以外の通信は遮断を行う。		☐