

【マイナンバー時代のセキュリティ対策】：出典「MICROSOFT」を編集、文責：河東岩夫、作成日：平成28年1月18日
 マイナンバーのセキュリティ対策についての定期的な点検事項(実施日：平成 年 月 日)

分野	チェックの内容	✓確認
データ	① マイナンバーを含むファイルの取扱い者(責任者・担当者)が特定できる仕組みを用意しているか	□適□不
	② マルウェア対策ソフトを導入し、最新のパターンファいるかで定期的にチックを行うように構成しているか	□適□不
	② イナンバーを含むデータは使用しない時に暗号(電子割符を含む)化しているか	□適□不
	④ 法的な保存期間が終了したデータについて、決まった廃棄方法(記録を含む)を定めているか	□適□不
アプリ	⑤ マイナンバーを扱うアプリケーションを決めているか	□適□不
	⑥ 社内のみ /クラウドのみ等、マイナンバーの取扱い場所(サーバ：管理区域、事務処理：取扱区域)を定めているか	□適□不
	⑦ マイナンバーを含むメールの誤送信の対策を実施しているか	□適□不
	⑧ マイナンバーが含まれるファイルやメールを扱う時、そのことを取扱い者に意識させているか	□適□不
デバイス	⑨ マイナンバーを含むコンピュータを限定しているか、または紛失した時の対応方法を定めているか	□適□不
	⑩ マイナンバーの保存領域へのユーザ認証(二要素以上)方法を設定しているか	□適□不
ネットワーク	⑪ マイナンバーの保存領域に対する不正アクセスの検出方法を定めているか	□適□不
	⑫ マイナンバーをメールなど、ネットワーク経由で送受信する場合、その内容を暗号(電子割符を含む)化しているか	□適□不
組織のルール	⑬ マイナンバーの利用方法に関するルール(規定・記録等)を社内定めているか	□適□不

注) チェック内容の確認結果が全て“☒適”になる必要があります。