JSSEC スマートフォン利用ガイドライン 対策チェックシートⅡ【NIST-CSF対応版】 第1.0版

本シートは、「スマートフォン＆タブレット（以下スマートフォン）の業務利用に関するセキュリティガイドライン【第二版】」（2014年3月発行）に付属の「特性別／利用シーン別　対策チェックシート」のアップデート版である。スマートフォンの導入・運用・利用停止の各段階におけるセキュリティの考慮点を網羅的にまとめた項目を、NIST-CSFの体系に合わせ再点検し、使いやすく50項目に集約した。

表内の 「 新規・追加項目（■）」は、テレワーク や Webアプリ（サービス等） 活用の増加、経営層の視点、サプライチェーンへの配慮を念頭に、本シートで新たに追加した項目である。

初見でもすぐ理解できるよう、項目中に例や補足を記載しており、スマートフォンの新規活用時や情報セキュリティポリシー全体の見直しの際などに、効率的かつ手軽にご活用いただきたい。

【対象となる読者】

①企業や組織においてスマートフォンを導入する責任者・企画担当者
②企業や組織においてスマートフォンを導入する際にセキュリティポリシーを策定する責任者・担当者
③企業や組織におけるスマートフォン利活用の支援者・運用担当者
④企業や組織においてワークスタイル変革を推進する責任者・企画担当者

※NIST：National Institute of Standards and Technology（米国国立標準技術研究所）　引用先：NIST CSF1.1（IPA翻訳版2019年1月発行）

スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン【第二版】
https://www.jssec.org/dl/guidelines_v2.pdf

※PCからダウンロードしてください。
本チェックシート（Excel版）
https://www.jssec.org/dl/guidelines_checkSheet2_v1.0.xlsx

【チェックシートの活用方法】 ※検討内容が不明な場合はガイドラインを参照する。

①推奨項目を参考にし用途に合わせ検討内容を選択する（◎：採用／△：一部採用／×：不採用）
②採用/一部採用/不採用の理由を明確にする
③採用項目は、検討のポイントを明確にする
④自社の状況やビジネス用途に合わせ、検討項目を追加する

【補足：用途レベル毎の推奨項目】　※■：推奨項目

①簡易的な利用・・・・・ビジネスへ大きな影響を与えない
　例）情報収集や電話、短いコミュニケーションなど補助的な利用
②一般的な社内業務・・・影響は社内にとどまる
　例）日常のコミュニケーションツール、業務用資料の作成など、業務での継続的な利用
③重要な本業ビジネス・・社外のステークホルダーに影響を与える
　例）IoT関連の調査分析ツール、工場での活用など、本業を支える利用

NIST-CSF（Ver1.1）			JSSEC スマートフォン利用ガイドライン 対策チェックシートⅡ【NIST-CSF対応版】 第1.0版		用途レベル毎の推奨項目			自社の検討内容コメント欄	
	機能	カテゴリー	組織でスマートフォンを利用（導入）する時に検討すべき観点	新規・追加項目(■)	簡易的な利用	一般的な社内業務	重要な本業ビジネス	◎：採用 △：一部採用 ×：不採用	・採用/不採用などの理由 ・検討のポイント ・追加検討項目
平常時	識別（ID） ビジネス環境やIoT資産を把握し、リスクの想定と対応方針を定める	資産管理（ID.AM）	01）スマートフォンの盗難や紛失時に備え、守りたい情報と利用を制限する機能を明確にする						
			①重要なデータを明確にする	■		■	■		
			②利用されたくない機能（端末に搭載されている機能、SNSなどのサービス等）を明確にする	■					
			③情報やデータへのアクセスは、必要最低限、かつ、許可した範囲に制限する	■					
			02）スマートフォンの関係者の役割を把握し、周知する						
			①スマートフォンの管理責任者（利用者にルールなどを周知する担当）の役割について把握する	■		■	■		
			②スマートフォンメーカー、通信事業者、クラウドアプリ提供者、および、利用企業の役割を確認する	■					
			③スマートフォンの運用担当、保守担当の役割を策定する	■					
			④インシデント（紛失・盗難及び情報漏洩など）対応関係部署の定義と役割を策定する	■					
		ビジネス環境（ID.BE）	03)スマートフォンがどの業務に関係しているか調査し、守りたい環境を明確にする						
			①スマートフォンがどの業務に利用されているか把握する	■		■	■		
			②スマートフォンが重要な業務又は基幹業務に利用されているか確認する	■					
		ガバナンス（ID.GV）	04）スマートフォンを利用する際の対策を、方針として明確にする						
			①リスクを認識する（リスクアセスメントを実施する）	■					
			②セキュリティポリシーは、経営層に提言しながら随時見直しをする	■	■	■	■		
			③スマートフォンの利用シーンやスマートフォンの特性を考慮する	ー					
			④必要な運用体制を整備し、人材を確保して育成する	■					
			05）順守すべき法令などを把握し、想定された用途以外の利用を禁止する						
			①改正民法や、改正後の個人情報保護条例について、必要な項目を確認する	■					
			②許可するアプリケーションや機能を調査し、それだけを利用しているか確認する手段を用意する	■		■	■		
			③社員の位置情報など、個人情報を収集する場合は同意を得る	ー					
		リスクアセスメント（ID.RA）	06)想定された用途以外の利用リスクを想定する						
			①OSやアプリケーションの設定の不備（ミス）による外部からの攻撃を想定する	ー					
			②スマートフォンを可搬媒体とみなしたデータ持ち歩きのリスクを想定する（スマートフォンに持ち出しが禁止されているデータを保管しない等）	■	■	■	■		
			③不正な相手に接続するリスク（乗っ取りを含む）を想定する	■					
			07)スマートフォンの盗難・紛失などのリスクを想定する						
			①盗難・紛失時のリスクを評価し、対策が必要な場合には検討する	ー	■	■	■		
			08)スマートフォンの廃棄や転売時に情報を読み出されるリスクを想定する						
			①個人情報・秘密情報などが漏洩するリスクを想定する	ー	■	■	■		
		リスクマネジメント戦略（ID.RM）	09)リスク対応計画（方針）を策定する						
			①リスクアセスメントの結果を受け、自組織への影響と許容範囲から対応策を検討する（リスクの定期的な確認なども含めて検討する）	■			■		
			②マネージメントレビューを実施し計画を確定する（レビューのためにリスクを視覚化しておくことなども検討する）	■					
			10)重要な事項がWeb、マニュアル、契約書などに記載されているか確認する						
			①第三者アプリ利用時に個人情報やプライバシーを取り扱う場合は、保護規約などが記載されているかを確認する	ー					
			②アプリの動きが想定通りか確認し、利用許可するアプリを決める	ー	■	■	■		
			③サポート期間、問い合わせ先などを確認する	ー					
		サプライチェーンリスクマネジメント（ID.SC）	11) 作業委託先や発注先を管理する						
			①作業委託先や発注先の会社情報を確認する （開発元、保守委託業者、クラウド運営事業者、アプリ開発者　などが対象）	■					
			②作業内容を証明できる企業へ発注する	■			■		
			③作業終了後、委託先に対し、作業に関わる自社データが完全消去されたことを確認する	■					
			④作業委託先や発注先が、情報やデータへアクセスできる範囲は、必要最低限、かつ、許可した範囲とする	■					
			12) 作業委託先などビジネスパートナーのリスクを把握する						
			①情報セキュリティの推進体制が構築されており、運用されていることを確認する（必要に応じて、誓約書に同意させる）	■			■		
			②与信審査を行い、企業の健全性を確認する（作業者の状態、属性、作業環境、委託事業者社内セキュリティ体制にも留意する）	■					
			13) 業務の継続性を担保する　（バージョンアップ対応など継続提供できるかどうかのリスク判断）						
			①万が一の場合（倒産等）に備え、ソフトウェアの所有権、利用権を整理する（事業の持続が可能となるよう予め検討する）	■			■		
			②リスクの内容と対策について、ステークホルダーとコミュニケーションをとっておく	■					
			14) 利用するクラウドサービス/SaaSを精査する						
			①利用許可するクラウドサービスを明確にする	■		■	■		
			②利用許可するクラウドサービスの条件を明確にする	■					
			③利用禁止するクラウドサービスを明確にする	■					
	防御（PR） リスク対応方針に基き、物理面、人的面、技術面から防護策を実施する	アイデンティティ管理、認証／アクセス制御（PR.AC）	15) スマートフォンへのアクセス制限を適切に管理する						
			①パスワードやパスコードを複雑にする（例えばNISTのSP800-63Bや総務省、NISCの基準を参考にする） ※総務省「安全なパスワード管理」https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/01.html	ー	■	■	■		
			②生体認証の利用判断、設定、管理を適切に行う	■					
			16) 通信時のアクセスポイントを適切に管理する						
			①テザリング（ルータ機能）を利用許可する際は、機種名（ID）やパスワードを厳格に管理し、端末名は機種を推測されにくい名称に設定させる	ー					
			②利用可能なWi-Fiアクセスポイントを制限する（社内の正式なアクセスポイント、許可された公衆Wi-Fi、自宅、等、以外は利用禁止）	ー	■	■	■		
			③Bluetooth利用時、ペアリングの時に他の機器に接続しないよう注意させる（接続方式に注意する/関連製品増に伴うネットワーク混雑にも配慮する）	■					
			17) 組織契約のクラウドサービス（Webアプリ/SaaS（社内システム含む）/ASPサービス）の認証とアクセス制御を管理する						
			①ユーザ認証を行い、利用者を制限する	ー					
			②デバイス認証（二段階認証、二要素認証）等を行い、許可されていないスマートフォンからのサービス利用を禁止する	ー		■	■		
			③アクセスできる情報や利用できる機能を制限する	■					
			④サービスへアクセスできるネットワークを制限する（暗号化されていないネットワークの利用は不可など）	ー					
			18) 組織では許可していないクラウドサービス（Webアプリ/SaaS/ASPサービス）の利用ルールを作る						
			①特例申請のルールを作成する（基本的には利用禁止としておき、許可する条件を明確にする（定期的な利用申請、突発的な利用申請に備える）	ー		■	■		
			19) 社内ネットワーク（オンプレ）接続時の運用方法を策定する						
			①アクセスできるユーザとスマートフォンを制限する（ユーザ認証、デバイス認証）	ー					
			②アクセスできる社内システムを制限する（ネットワークを分離する、SSIDを分ける、アクセスポイントを分ける　など）	ー	■	■	■		
			③Wi-FiルータのSSIDは、組織名や機種を推測されにくい名称にする	ー					
			20) スマートフォンに標準搭載している機能を制限する						
			①スマートフォンで利用する機能を決め、不要な機能は無効にする（カメラ、マイク、NFC/FeliCa、Wi-Fi、Bluetoothなど）	ー					
			②利用不可としている機能を識別出来るようにする（無効化操作/ロック/セキュリティシール貼付など）	ー			■		
			③ブラウザなどにパスワードを保存させる場合のルールを決める	ー					
			21) アプリの利用範囲を制限する						
			①アプリが利用する機能を決め、利用出来るデータ・機能（住所録・画像データ・位置情報など）へのアクセス許可を最低限にする ※最新のアップデートにより利用可能となった機能に注意する	ー			■		
			②アプリが作成するデータから不要な情報（写真のExif、Information、プロパティ、属性情報　など）を排除する	ー					
			③データを保存する専用の保存場所を設けたり、保存場所を固定するなど、利用者に選択させないようにする	ー					
		意識向上およびトレーニング（PR.AT	22) 正しく利用するための手順書を作成する　（各項の内容はガイドライン参照）						
			①周辺の状況を考慮して利用することを指導する（覗き見防止シール貼付やショルダーハッキング対策など）	ー					
			②アプリを利用する時の注意事項を作成する（アドレス帳/電話帳/メール/スケジュール/Webブラウザ/各種アプリ） （アプリのプライバシーポリシーを確認する）	ー	■	■	■		
			③スマートフォンの機能を利用するときの注意事項を作成する（カメラ/マイク/位置情報/NFC/Ferica/生体認証など）	ー					
			④ネットワーク利用時の注意事項を作成する（Wi-Fi/Bluetooth）	ー					
			⑤データの取り扱いの注意事項を作成する（バックアップをとる/可搬媒体として利用する）	ー					
			23) 手順書に沿ってトレーニングする　（各項の内容はガイドライン参照）						
			①利用者の知識不足を補えるよう考慮する	ー					
			②利用者の誤操作防止を考慮する	ー	■	■	■		
			③盗難・紛失時の対応手順を考慮する	ー					
			24) 不正利用を防ぐための誓約書を作成する						
			①利用目的、管理方法、禁止事項、有効期間を定める	ー		■	■		
			②利用違反の罰則を定める	ー					
			25) 貸与したスマートフォンの私的利用を制限する						
			①電話やネット機能などの私的利用を禁止する	ー					
			②不適切なWebコンテンツ閲覧や許可されてないアプリを禁止する	ー	■	■	■		
			③通話料金や通話履歴、Web閲覧履歴を管理する	ー					
			26) BYOD利用時の環境を整備する						
			①利用者のプライバシーに配慮し（利用アプリやデータの分離、ログ収集方法、など）規定を策定する	ー					
			②利用者にルール順守の誓約書に同意させる	ー	■	■	■		
			③ログなどでプライベートなデータ混在する場合に、管理ルール（プライベートデータには関与しない、など）を定め、同意させる	ー					

NIST-CSF（Ver1.1）			JSSEC スマートフォン利用ガイドライン 対策チェックシートⅡ【NIST-CSF対応版】　第1.0版		用途レベル毎の推奨項目			自社の検討内容コメント欄	
	機能	カテゴリー	組織でスマートフォンを利用（導入）する時に検討すべき観点	新規・追加項目(■)	簡易的な利用	一般的な社内業務	重要な本業ビジネス	◎：採用 ・採用/不採用などの理由 △：一部採用 ・検討のポイント ×：不採用 ・追加検討項目	
平常時	防御（PR） リスク対応方針に基き、物理面、人的面、技術面から防護策を実施する	データセキュリティ（PR.DS）	**27) スマートフォン内のデータを保護する**						
			①スマートフォン内に保管するデータ、又は、スマートフォンの記憶領域（外部記憶媒体）を暗号化する ※最近のOSでは、データの記憶領域はデフォルトで暗号化されている	―	■	■	■		
			②スマートフォンのロックを設定し、ロック解除を複数回失敗した時に強制的にデータを消去する	―					
			③データを定期的にバックアップする（バックアップデータを、PCやクラウド、外部記憶媒体など別の場所で暗号化して保存する）	―					
			28) 通信時のデータを保護する						
			①通信や、通信時のデータを暗号化する ※Webアプリやクラウドサービスにてデータ授受を許可する場合、データ個別の暗号化などの保護が必要となる（TLSは通信経路の暗号化である）	―		■	■		
			②Webフィルタリングなどで不正サイトへのアクセス抑止を行う（フィッシング対策など）	―					
			③メールの誤送信対策を行う	―					
			④メールでファイルを授受できるよう、オンラインストレージを準備する（暗号化/パスワード付与）（本文へ添付しないことが望ましい）	■					
			⑤Webアプリ（外部運営のオンラインストレージやクラウドサービス）へアップロードするファイルを保護する（暗号化/パスワード付与）	■					
			29) スマートフォン落下時の保護対策を行う						
			①スマートフォンの損壊などによるデータ破損対策を行う（耐衝撃性ケースの利用、落下防止用ストラップや画面保護フィルムの装着）	―			■		
			30) 廃棄に備える						
			①廃棄時の手順を明確化する（端末やFeliCaの初期化など/　特に、Felicaを鍵として利用している場合には注意する）	―	■	■	■		
			②スマートフォンの廃棄や転売時には、業務データやログを完全消去しておく	―					
			31) BYOD利用時のデータを管理する						
			①退職時や利用終了時に業務データを削除したことを確認する	―	■	■	■		
			②データやアプリを区分する（プライベートと業務の保存場所の区分）	―					
		情報を保護するためのプロセスおよび手順（PR.IP	**32) インシデント発生時の対応計画と復旧計画を策定する**						
			①インシデントの基本的な対応手順を策定する（特に、インシデント時の初動計画を周知しておくことで、万が一の場合のダメージを最小限に抑える）	■		■	■		
			②インシデント対応後の基本的な復旧手順を策定する	■					
			③復旧のためのデータバックアップ計画を策定する	■					
			33) スマートフォンのライフサイクルに合わせ、手順を策定する						
			①スマートフォンの配布、再設定、ポリシー変更、買換え、機種変更、一時休止、廃止などの手順を明確にする	―		■	■		
		保守（PR.MA）	**34) OS・アプリを管理しスマートフォンの健康を維持する**						
			①各種情報（バージョンアップ、不具合、脆弱性など）を確認する ※スマートフォンやアプリ提供者のWebサイトやメール、および、IPAなどの機関から発信される情報を参照する	■	■	■	■		
			②提供者から通知が行われた脆弱性の影響（自社利用への影響）を特定し、必要に応じて対応する	■					
			③アプリは信頼できるマーケット（Google Play、Apple Store、キャリアマーケット）から入手する	―					
			35) アプリのアップデート手順を確認し策定する						
			①アップデート情報やアップデートファイルの入手方法、アップデート手順を確認する（特に、トラブルや不具合が起こった際の初動計画に留意する）	―		■	■		
			②アップデート後の動作検証を行い、アップデートする判断基準を定める	―					
			③アップデートの不具合があった時の復旧手順を策定する	■					
		保護技術（PR.PT）	**36) 必要なログが安全に保管されるか確認する**						
			①利用履歴（各種ログイン情報、サービス利用履歴、アプリ利用履歴など）、利用状況を取得する	―		■	■		
			②ログを安全に保管する（暗号化、アクセス権設定など）	■					
	検知（DE） 異常を検知するしくみの構築と継続的な監視を行う	異常とイベント（DE.AE）	**37）スマートフォンの異常な使われ方を検知する**						
			①利用者本人が、スマートフォンの異常な動きに気づくように手順書を作成し指導する ※異常は、利用者本人が気づいた場合に申告させ、それ以外を後述の項目「38」で検知する	■	■	■	■		
			②スマートフォンの異常に気づいたら、決められた手順に従って速やかに連絡先へ通知させる （落下、紛失、盗難、破損、水没、ウイルス感染、動きが異常、不用意に未知アプリを導入した、等）	―					
		セキュリティの継続的なモニタリング（DE.CM）	**38）スマートフォンの異常を継続的に監視する**						
			①利用者が気づきにくい異常な動きや不正を検知するしくみを検討する(マルウェア侵入、不正なアプリの導入など)	■		■	■		
			②利用者の不正な利用を検知するしくみを検討する(禁止アプリの導入など)	■					
		検知プロセス（DE.DP）	**39）検知した情報が異常か否か判断する**						
			①異常を判断するための閾値やルールを策定する	■			■		
			40）手順書やルール、連絡網を作る						
			①利用者から異常通知が受け取れるように、しくみを整備し、手順を策定する（特に、初動計画を対応担当者と共有し影響を最小限に抑える）	■	■	■	■		
			②利用者から第一報を受けた後の手順（紛失時における警察や鉄道への確認方法、電源を切るなど）を策定する	■					
非常時	対応（RS） 異常検知内容を分析し対応策と伝達計画を策定し、被害拡大を防止する	対応計画（RS.RP）	**41)スマートフォンのインシデントに対応する**						
			①速やかに発生事象を把握し、状況（影響など）、証拠（ログなど）を収集する	■					
			②インシデントの基本的な対応手順をもとに、発生した事象にあわせ対応手順を検討する	■					
			③インシデントの原因に対処し被害拡大を防止する（拡大防止策を検討する）	■					
			④利用者（個人）で対応することと、管理者（組織）が対応することを明確にする	■					
			⑤全ての対応活動を記録する	■					
		コミュニケーション（RS.CO）	**42) スマートフォンのインシデント情報を確実に収集できるようにしておく**						
			①盗難・紛失した場合は、事前に定めたルールに則り、盗難・紛失したことを利用者に通知させる（リモートワーク中のインシデントも想定する）	―	■	■	■		
			②連絡先変更時の改訂内容や、リモートワーク中/臨時の勤務体制時における対応方法は、確実に通達する	■					
			③遠隔でしか対応できないときの対処方法を検討する	■					
			43) スマートフォンのインシデント情報を関係部署へ通知する						
			①インシデントがサプライチェーンに及ぼす影響を確認し、必要に応じて対応する	■		■	■		
			②情報セキュリティ委員会、経営層、CSIRT等と連携しステークホルダーに報告する	■					
		分析（RS.AN）	**44) スマートフォンの利用状況を確認する**						
			①異常な利用履歴を確認する （紛失時刻から機能停止対応までの間の利用履歴、日頃の利用履歴との差異（利用時間帯、パケット数や通信量、費用の増減）など）	■			■		
			②ID、パスワードの利用、ログイン履歴を確認する（通常の履歴確認ではなく、異常か否かに留意して確認する（意図があったか））	■					
		低減（RS.MI）	**45)スマートフォンの盗難・紛失発生時の被害拡大を防止する**						
			①スマートフォンを探すサービスを利用して所在を確認し（GPS情報の一部活用など）、必要な対応を行う ※管理者および利用者の対応内容、通信事業者およびアプリ開発者への依頼事項などを整理する	■	■	■	■		
			②スマートフォンの利用を制限する（リモートロック、リモート消去、リモート電源OFFなど）	―					
			③スマートフォンからの通信を遮断する（VPNの利用停止、通信事業者へ回線停止依頼など）	―					
			④スマートフォンで使用していた認証機能を失効する（アカウントロック、パスワードの変更、証明書削除　等）	■					
			46) スマートフォンのマルウエアや不正アプリの被害拡大を防止する						
			①マルウエアの駆除又は不正アプリを削除する	■	■	■	■		
		改善（RS.IM）	**47)スマートフォンのインシデント事例から改善策を学習する**						
			①対応内容を分析し、手順の見直しを行う	■			■		
	復旧（RC） 事前に復旧計画を策定し、発生時には関係者と連携をとり復旧を行う	復旧計画（RC.RP）	**48) スマートフォンを通常の利用状況に戻す**						
			①復旧手順に従ってデータを含め、元の状態に戻す（スマートフォン本体、社内サーバ、クラウド上など）	■		■	■		
			②復旧したことを確認する（スマートフォン本体、社内サーバ、クラウド上など）	■					
		改善（RC.IM）	**49)スマートフォンのインシデントから再発防止策を検討する**						
			①インシデントから得た情報を再発防止策に活用する	■		■	■		
			②同じインシデントや異常が他のスマートフォンや利用者に起こっていないか確認する	■					
			③復旧計画の見直しや、改善を検討する	■					
		コミュニケーション（RC.CO）	**50) スマートフォンのインシデント情報と対応結果を通知する**						
			①発生したインシデントの最終的な影響範囲を確認する	■		■	■		
			②インシデントの対応結果や再発防止策を利用者や関係者に周知する	■					
			③重大な影響があった場合は、情報セキュリティ委員会、経営層、CSIRT等と連携しステークホルダーに報告する	■					

免責・注意事項	**※ JSSEC並びに執筆関係者は、チェックシートなどに関するいかなる責任も負うものではありません。全ては自己責任にて対策などをお願いします。** **※ 本チェックシートに登場する商品名・サービス名は、一般に各社の商標または登録商標です。** **※ 社内文書などに引用する場合、著作権法で認められた引用の範囲内でご利用ください。また、その際は必ず出典を明記してください。**
発行・著作権・連絡先	**発行者　：　2021年5月25日　　一般社団法人 日本スマートフォンセキュリティ協会（JSSEC）　利用部会** **著作権　：　一般社団法人日本スマートフォンセキュリティ協会** **連絡先　：　一般社団法人日本スマートフォンセキュリティ協会　事務局　TEL 03-6757-0159　　https://www.jssec.org/　（お問い合わせ先参照）**