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/解説編」の活用法

～ 2022年初夏リリース予定の解説編ご紹介 ～

2022年3月24日

JSSEC 一般社団法人 日本スマートフォンセキュリティ協会
利用部会 副部会長 兼 利用ガイドラインWGリーダー 松下綾子
（アルプスシステムインテグレーション株式会社）

部会紹介：目的とめざす成果

https://www.jssec.org/activities

利用部会	**利用者視点**の活動	安心・安全なスマートフォン利用のために情報収集と課題を整理し、情報発信を行う。 又、近年のスマートフォン利用形態の変化に合わせ、たとえば、IoTの導入など利用企業の共通的 な経営課題を中心にテーマを選定し、利用事例の調査や新しい技術の調査・研究の成果 を発信する。
技術部会	**提供者視点**の活動	スマートフォンを安全に利用するための技術的な調査・研究・議論を行う。 具体的には4ワークグループで構成し成果物を公開する事で、日本における スマートフォン利用の安全性向上に寄与する。
啓発事業部会	**学生への啓発**活動	JSSECがスマートフォンの安全利用を推進し広く社会に貢献するため、積極的に啓発活動展開を行うことを目的とする。 特に、中高生など学生向けの啓発活動に注力する。
ＰＲ部会	JSSECの**PR活動**	JSSECが行うすべての活動について普及啓発するための情報配信を行う。 例）・メディア対応/各種成果物、JSSEC活動に関する情報配信 ・イベント・セミナーの企画・運営 ・他団体との連携

もくじ

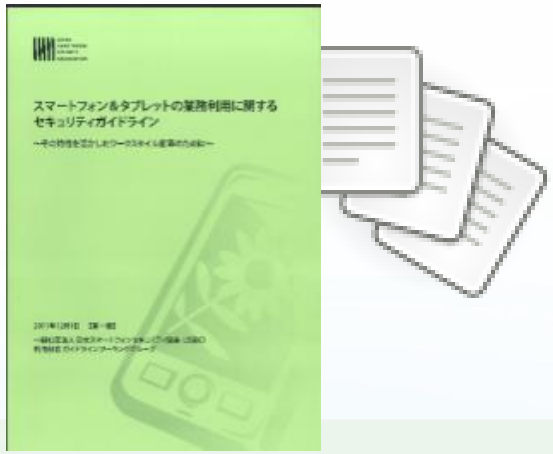
JAPAN SMARTPHONE SECURITY ASSOCIATION

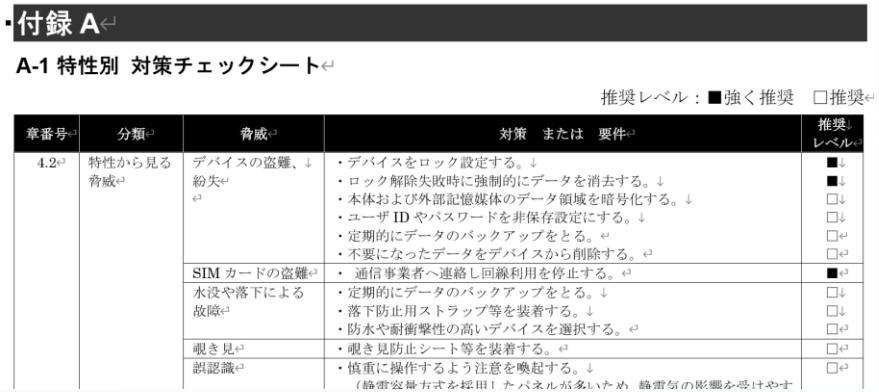
スマートフォン利用ガイドライン　「対策チェックシートⅡ」

対策チェックシートとは

2014年に発行したスマートフォン（タブレット含む）利活用のための

セキュリティガイドライン冊子に付属している「特性別／利用シーン別 対策チェックシート」





付録 A

A-1 特性別 対策チェックシート

推奨レベル：■強く推奨　□推奨

章番号	分類	脅威	対策　または　要件	推奨レベル
4.2	特性から見る脅威	デバイスの盗難、紛失	・デバイスをロック設定する。 ・ロック解除失敗時に強制的にデータを消去する。 ・本体および外部記憶媒体のデータ領域を暗号化する。 ・ユーザ ID やパスワードを非保存設定にする。 ・定期的にデータのバックアップをとる。 ・不要になったデータをデバイスから削除する。	■ ■ □ □ □ □
		SIM カードの盗難	・　通信事業者へ連絡し回線利用を停止する。	■
		水没や落下による故障	・定期的にデータのバックアップをとる。 ・落下防止用ストラップ等を装着する。 ・防水や耐衝撃性の高いデバイスを選択する。	□ □ □
		覗き見	・覗き見防止シート等を装着する。	□
		誤認識	・慎重に操作するよう注意を喚起する。 （静電容量方式を採用したパネルが多いため、静電気の影響を受けやす	□

付録：対策チェックシート

【ご参考】　**『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**
～その特性を活かしたワークスタイル変革のために～ 【第二版】』<2014年3月25日発行>

https://www.jssec.org/report/20140417.html

■2019年度のDL数：3538件（294件/月）
■2020年度のDL数：　985件 (　82件/月）

対策チェックシートⅡ リリースの背景

1．Web系サービスやクラウドストレージ（Webアプリ）の活用に向けた、
社内インフラ再構築の増加

2．テレワークの推進など働く環境の激変に伴う、セキュリティポリシーの再検討

3．スマートフォン活用シーンの広がりとタブレット導入の増加

スマートフォン（タブレット含む）を取り巻く環境と、国際的なセキュリティ対策の流れ、用途レベルの変化や最近の社会情勢などを考慮し、セキュリティ要件を見直して、2021年6月、別資料「チェックシートⅡ」としてリリースしました。

「対策チェックシートⅡ」概要①

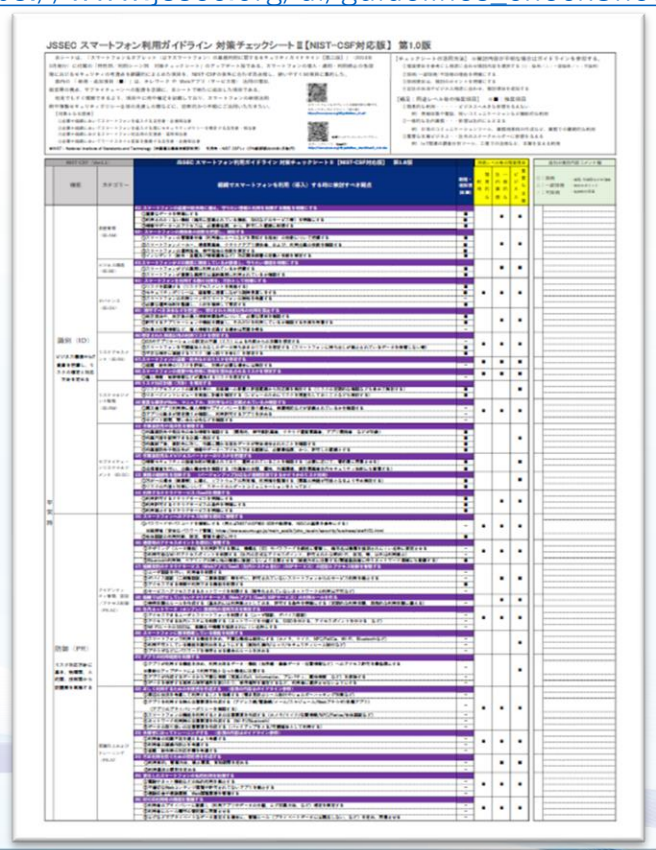
■2014年発行の「特性別／利用シーン別 対策チェックシート」をアップデートした資料

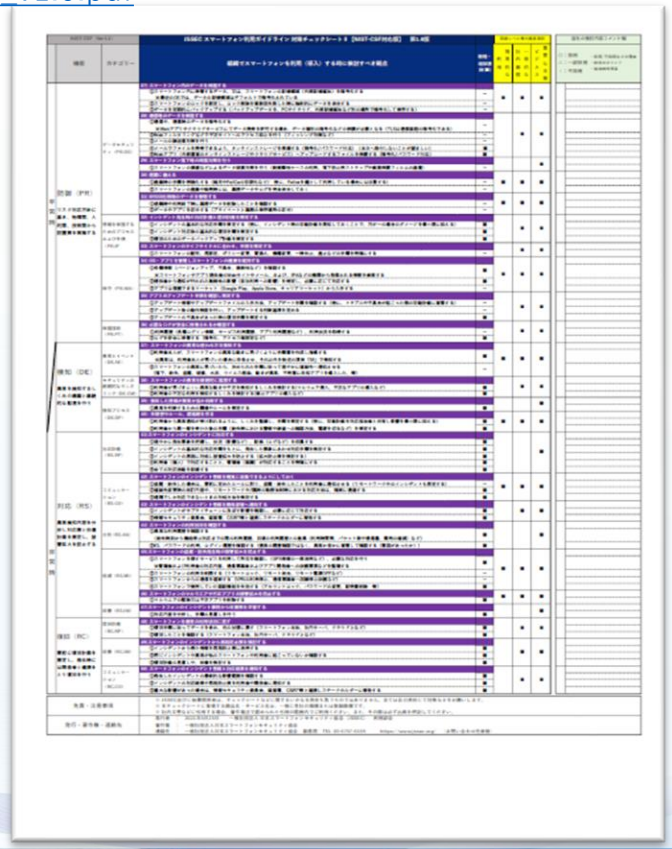
■2021年6月3日発行

「対策チェックシートⅡ」概要②

このようなA3資料（両面1枚）がダウンロードできます。

- **Excel版 ：**https://www.jssec.org/dl/guidelines_checkSheet2_v1.0.xlsx
- **PDF版 ：**https://www.jssec.org/dl/guidelines_checkSheet2_v1.0.pdf





特長：社会情勢の反映①

■働き方改革＋オープンイノベーション対応の考慮

- **利用者や利用シーンの変化**（社内事務系での利活用に加え、社外とのコミュニケーションや、本業を支える利用への変化）を考慮し、過不足を追加修正

1)サテライトオフィス/工場/仕事の現場/在宅勤務/BYOD/介護/育児/定年再雇

- ●仕事をするための敷居を下げ、より快適な環境で創造性の高い付加価値のある仕事を行うツールとしての活用
- ● BCP対策のための整備の一環としての活用

2)社内外のコミュニケーション/音声・静止画・動画・作業の共有

- ●より付加価値の高い成果を目指して、
  多くの関係者の知見を集める活動を支援するためのツールとしての活用
- ●社内外を問わず、コミュニケーションの機会と対象を拡大するための活用

※JSSECで2020年7月に行ったアンケートでは、緊急在宅勤務において重要書類の持ち出しが一時的に認められたこと、在宅勤務は製造・研究職の現場でも取り入れられたことなどが分かり、それらも念頭におきました。
https://www.jssec.org/dl/telework_research_20200722.pdf

■個人情報の取り扱いに対する注意喚起

- **個人情報保護の意識**についての記載　　※個人情報保護委員会- https://www.ppc.go.jp/

特長：社会情勢の反映②

■NIST-CSF* の活用

- セキュリティフレームワーク **5機能（識別/防御/検知/対応/復旧）** と、
  既存の対策チェックシートを照合し、過不足を追加修正

・National Institute of Standards and Technology（NIST） ：米国国立標準技術研究所
・Cybersecurity Framework（CSF） ：サイバー攻撃を防止、検出および対応する能力を、評価および改善する方法に関するコンピューターセキュリティガイダンスのポリシーフレームワーク https://www.nist.gov/cyberframework
・**IPAの情報サイトはこちら：https://www.ipa.go.jp/security/publications/nist/**

- 手順 ①既設のセキュリティ要件の洗い出し ➡ガイドライン本体とチェックシートの再照合
  ②**利用シーン毎**に整理された各対策内容 ➡**セキュリティ要件毎**に再整理

A-1 特性別 対策チェックシート
A-2 利用シーン別 対策チェックシート
手順書の例
誓約書の例
BYODの留意点
ライフサイクルにおける留意点（管理面）

NIST-CSFの５機能に 合わせて、
統合・分離・追加

アップデートの際の気付き

JAPAN SMARTPHONE SECURITY ASSOCIATION

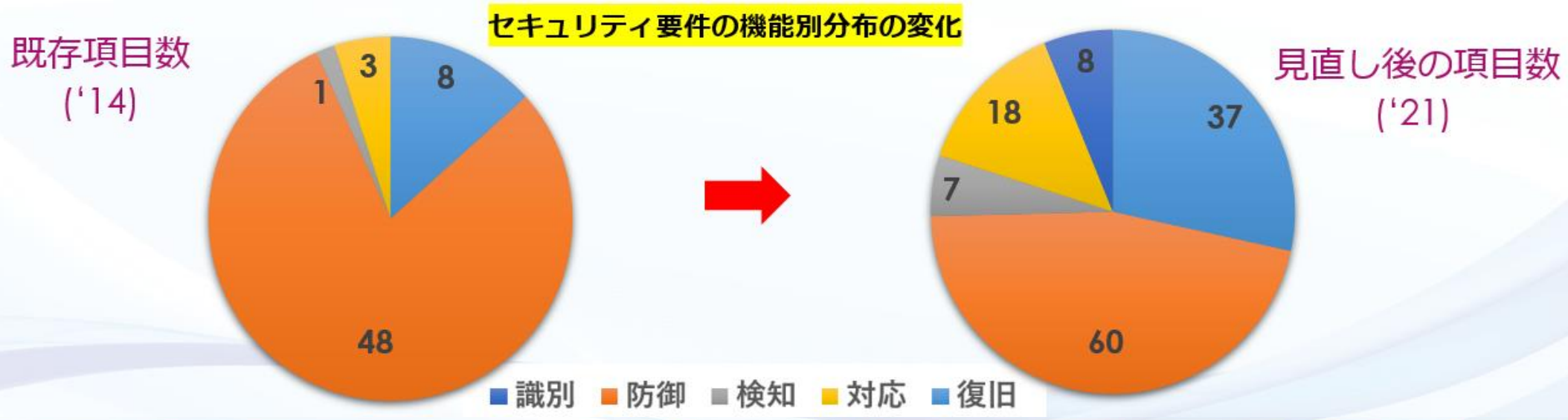
■旧チェックシート(‘14年版）と新チェックシート(‘21年版)の項目数比較

既存チェックシートを新チェックシートの項目に照合した結果

‘14年版項目数　：　識別８　／防御48／検知１／対応３　／復旧０

追記・新設数　：　識別29／防御12／検知６／対応15／復旧８

‘21年版の項目数　：　識別37／防御60／検知７／対応18／復旧８



特長：網羅的＆コンパクト

■ 5つのポイント

※下記①～⑤の色は次ページの表の説明と連動しています。

①すぐに読める＝**50項目**（A3両面、1枚）で簡潔

② セキュリティの対策項目をNIST-CSF 5機能分類で、**網羅的にチェック可能**

③ 従来チェックシートの**過不足項目を追加／補充**

・項目見直し時のキーワード：テレワーク、Webアプリ、クラウドサービス活用の増加、経営層の視点、
サプライチェーンへの配慮、法整備、社内外のステークホルダー（例：CSIRT）との関係性 等

④ 3種の用途レベル毎に、セキュリティ対策の**推奨項目を設定**

・用途レベル **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

・用途レベル **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

・用途レベル **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

⑤ すぐ使える＝**自社の状況も記入可能**

・特に、この項目を「なぜ採用したのか/しなかったのか」(理由)の記載が重要

特長：網羅的＆コンパクト②

■チェックシート表の構成

・対策チェックシートⅡは、前ページ①～⑤の説明に合わせ、以下のような構成になっています。

② NIST-CSF（Ver1.1）		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	③	④ 用途レベル毎の推奨項目			⑤ 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
識別（ID）	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	－				
		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	－				
		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	－	■	■	■	

- **Excel版** ：https://www.jssec.org/dl/guidelines_checkSheet2_v1.0.xlsx
- **PDF版** ： https://www.jssec.org/dl/guidelines_checkSheet2_v1.0.pdf

解説編について①

■**チェックシートⅡを読み解くための資料**

■**2022年初夏リリース予定**

■**特長：4つの視点でコンパクトに要点を掲載**

①なぜ検討するのか（検討の理由、背景、目的）
②なにを検討するか（検討の対象）
③注意点や考慮点
④事例や補足説明（理解が難しい部分のワンポイント解説）

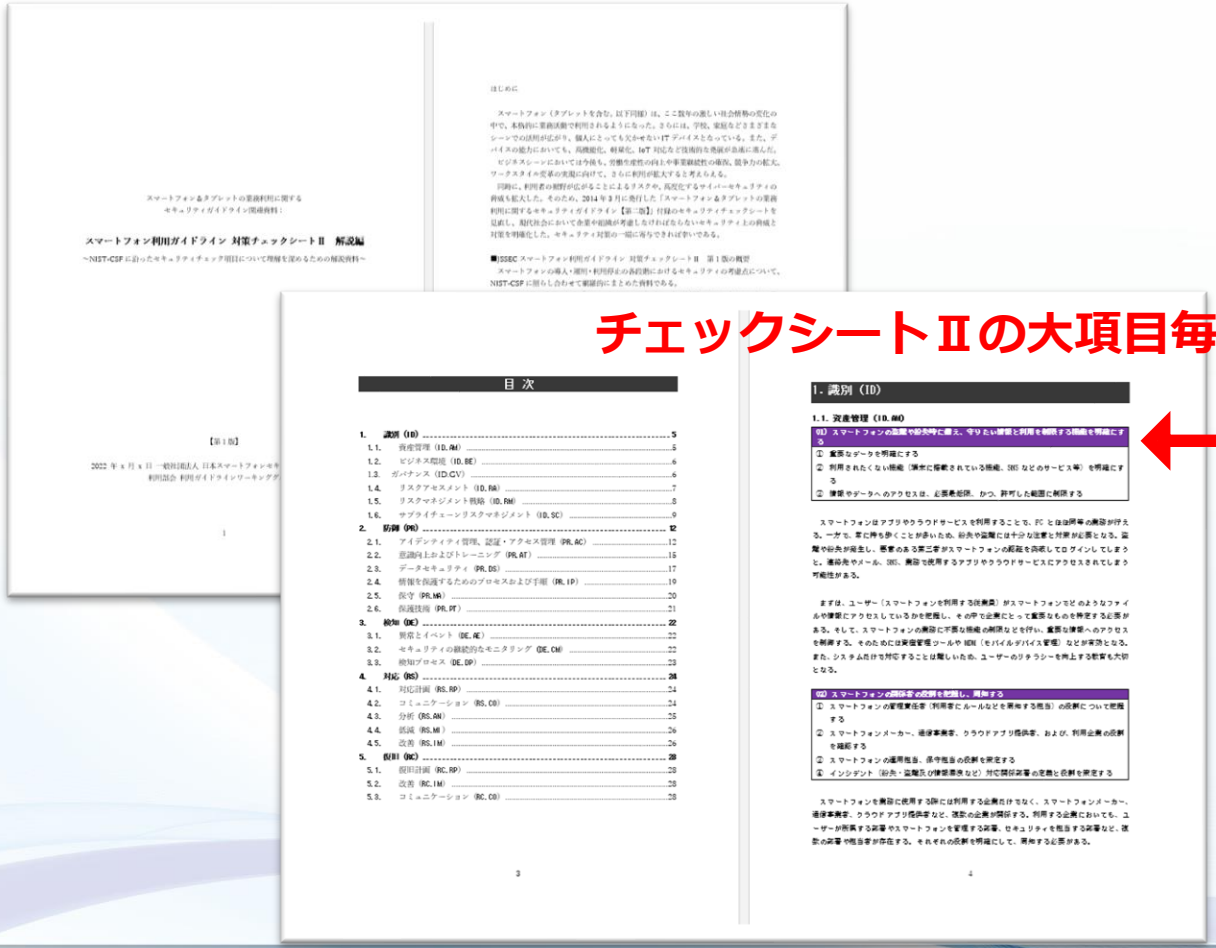
■**参考**

チェックシートⅡの表内に掲載している参考例や補足と合わせて確認すると効果的

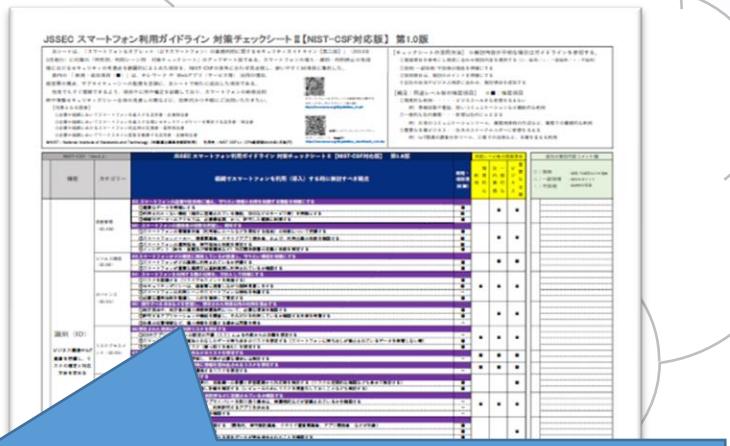
15) スマートフォンへのアクセス制限を適切に管理する
①パスワードやパスコードを複雑にする（例えばNISTのSP800-63Bや総務省、NISCの基準を参考にする）
※総務省「安全なパスワード管理」 https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/01.html
②生体認証の利用判断、設定、管理を適切に行う
16) 通信時のアクセスポイントを適切に管理する
①テザリング（ルータ機能）を利用許可する際は、機種名（ID）やパスワードを厳格に管理し、端末名は機種を推測されにくい名称に設定させる
②利用可能な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）
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）

解説編について②

■A4、30ページ程度（予定）



チェックシートⅡの大項目毎に解説



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
- 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

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

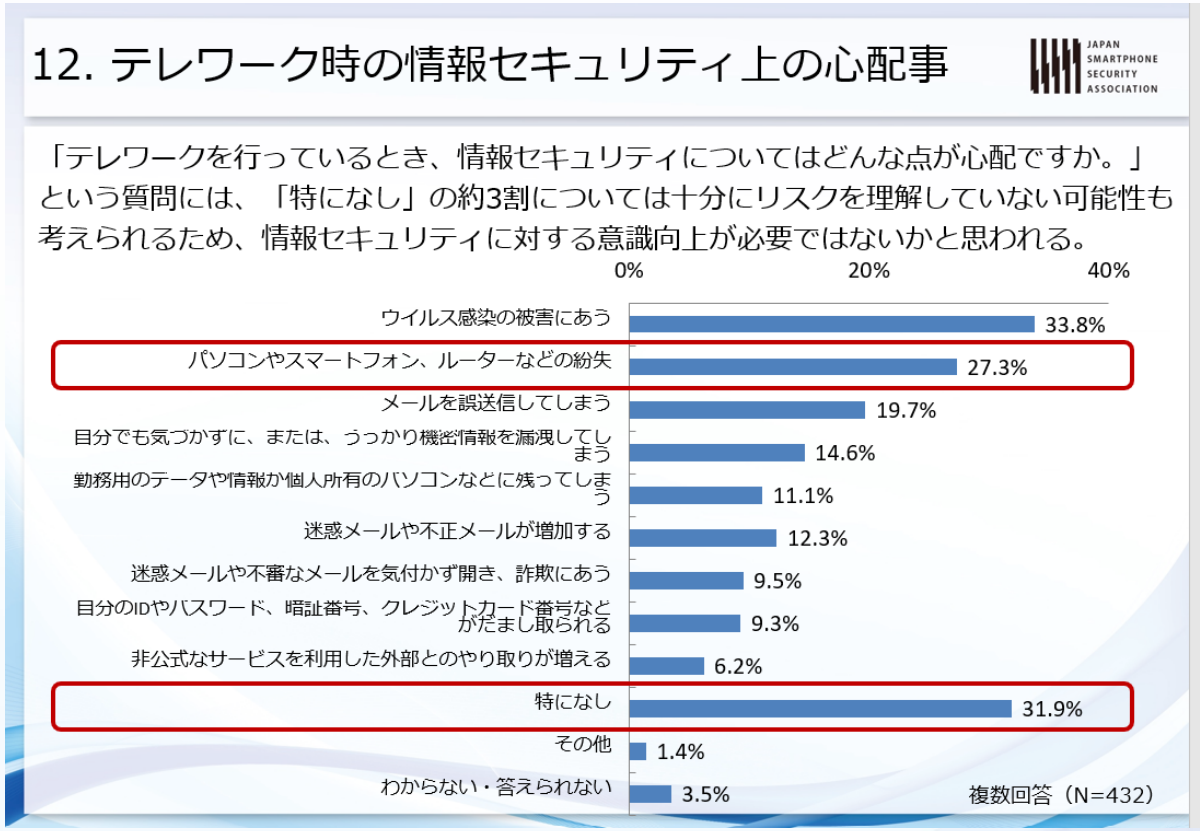
04）スマートフォンを利用する際の対策を、方針として明確にする
- ①リスクを認識する（リスクアセスメントを実施する）
- ②セキュリティポリシーは、経営層に提言しながら随時見直しをする
- ③スマートフォンの利用シーンやスマートフォンの特性を考慮する
- ④必要な運用体制を整備し、人材を確保して育成する

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

解説編について③

■ワーキンググループでの議論の例

- 「スマートフォンの利活用で特に心配な点は、『紛失すること』」※右図参照
  - **➡パソコンとは違う紛失対策の重要性**
- 「意識せずに、いつのまにか、多様なアプリを業務で使っているのではないか？」
  - **➡ビジネスパートナーのリスク分析の必要性**
- 「インシデントの事前・事後対策や、万が一の場合のリスク低減対策に課題はないのか？」
  - **➡テレワーク中の関係者との連絡方法や、リスク低減のための初動対応の準備**



[出典] JSSECテレワーク状況とセキュリティに関するアンケート調査レポート(2020年7月)

活用の効果

■スマートフォンの新規活用開始において

1. セキュリティ要件として**検討すべきことが網羅できます。**
2. 検討が必要な要件について、**見落としやミスを防げます。**

■情報セキュリティポリシー全体の見直しにおいて

1. 自社の状況を照らし合わせてみることで、**現行のセキュリティポリシーの課題や、時代に合わせて新しく対応すべき点に気づくことができます。**
2. 各項目に対する「採用/一部採用/不採用」を考え、その理由を明確にしておくことで、**将来の点検時に役立てられます。**
3. ベンダーやSI業者との打ち合わせ時や、経営層への報告時、**必要な要件の整理に役立ちます。**

まとめ

■**対策チェックシートⅡ**は、NIST-CSFに沿ってまとめた**コンパクト**な資料であり、セキュリティ対策の**網羅性が高く**なっています。

■**解説編**は、チェックシートⅡの**読み解きや知識を深める**ために役立ちます。

■セキュリティ対策は、守る対象となる情報や、対応業務、デバイス、人、利用シーンなどについて、システム全体を通して総合的に検討する必要があります。
対策チェックシートⅡ＆解説編は、スマートフォンに係るセキュリティ項目ですが、全体を見直す際の項目としても参考になると思いますので、ぜひご活用ください。

利用部会ガイドラインワーキンググループタスクフォース

リーダー	松下 綾子	（アルプスシステムインテグレーション株式会社）
メンバー	北村 裕司	（サイバートラスト株式会社）
	後藤 悦夫	（株式会社ラック）
	本間 輝彰	（KDDI 株式会社）
	三池 聖史	（ユニアデックス株式会社）

※氏名五十音順

ご参考： **IoTセキュリティチェックシート**と**説明動画**(You Tube)

利用部会では、IoTを導入する場合の検討事項をまとめ、
「IoTセキュリティチェックシート」と「説明動画」(You Tube) を公開しています。
このあと15:30から説明させていただきますので、ぜひご覧ください。

JSSEC IoTセキュリティチェックシート	□NIST-CSFの分類：5機能23カテゴリ(識別/防御/検知/対応/復旧) □企業のIoT推進者や管理者の視点で検討すべき点：60項目 □IoT用途レベル毎の推奨項目：3つの重要度に分類 □各社の検討内容　採用理由／追加項目：検討結果の見える化 □検討主体（IT又はOT）及び、連携（ITとOT）が重要な項目を明記

動画セミナー公開中

第1回　セミナーの構成と受講の進め方
第2回　チェックシートの特徴とセキュリティの重要性
第3回　「識別」の解説
第4回　「防御」の解説
第5回　「検知・対応・復旧」の解説
第6回　チェックシートの活用例

https://www.jssec.org/iot-youtube

ありがとうございました。

ぜひ、ワーキンググループの活動に参加してみませんか。
メールお待ちしております。

JAPAN SMARTPHONE SECURITY ASSOCIATION

https://www.jssec.org/

Mail：sec@jssec.org

matsushita@alsi.co.jp