JSSEC セキュリティフォーラム2021資料

NIST-CSF対応版
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
概説

～2021年リニューアルリリース～

2021年6月9日

日本スマートフォンセキュリティ協会（JSSEC）
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）

アジェンダ

JAPAN SMARTPHONE SECURITY ASSOCIATION

1. リリースの背景と狙い
2. チェックシートⅡ　概要
3. チェックシートⅡ　特長
4. 活用の手順と効果
5. まとめ

リリースの背景とねらい

JAPAN SMARTPHONE SECURITY ASSOCIATION

数年前から、急速に発展した**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が盛ん**になりました。
さらに昨年度以降は、テレワークの推進による働き方環境の激変に伴い、組織の規模を問わず、インフラ整備方針の見直しや、セキュリティポリシー上の課題検討が持ち上がっています。

そのような中、従来は電話とスケジュール管理での活用が主軸であったスマートフォンの**活用シーンも広がり**、また、タブレット導入も進んでいます。

そこで改めて、スマートフォン（タブレットを含む）を取り巻く環境と、国際的なセキュリティ対策の流れ、用途レベルや最近の社会情勢などを考慮し、安全な利活用を推進するための**セキュリティ要件を再検討することとしました。**

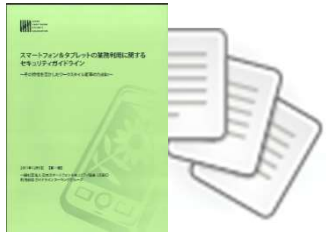
スマートフォンの利活用を立案する管理者や企画者の皆様には、ぜひ、新資料を、**現状に沿ったセキュリティポリシーを検討する**際のお役に立てていただきたいと考えています。

対策チェックシートⅡ　概要①

JAPAN SMARTPHONE SECURITY ASSOCIATION

■対策チェックシートⅡとは

「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】」
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」のアップデート版



付録：対策チェックシート

**チェックシートを
アップデート！
個別にリリース**

【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）⇒コロナ禍の収まりに比例して復調傾向あり

■リリース日～2021年6月3日

**リリースから二日間で、
約400件のダウンロード！**

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

対策チェックシートⅡ　概要②

JAPAN SMARTPHONE SECURITY ASSOCIATION

■アップデートのポイント：社会情勢の反映

・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

・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/

対策チェックシートⅡ　概要③

JAPAN SMARTPHONE SECURITY ASSOCIATION

■アップデートのポイント：社会情勢の反映（続き）

・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
②利用シーン毎に整理された各対策内容を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

対策チェックシートⅡ　概要④

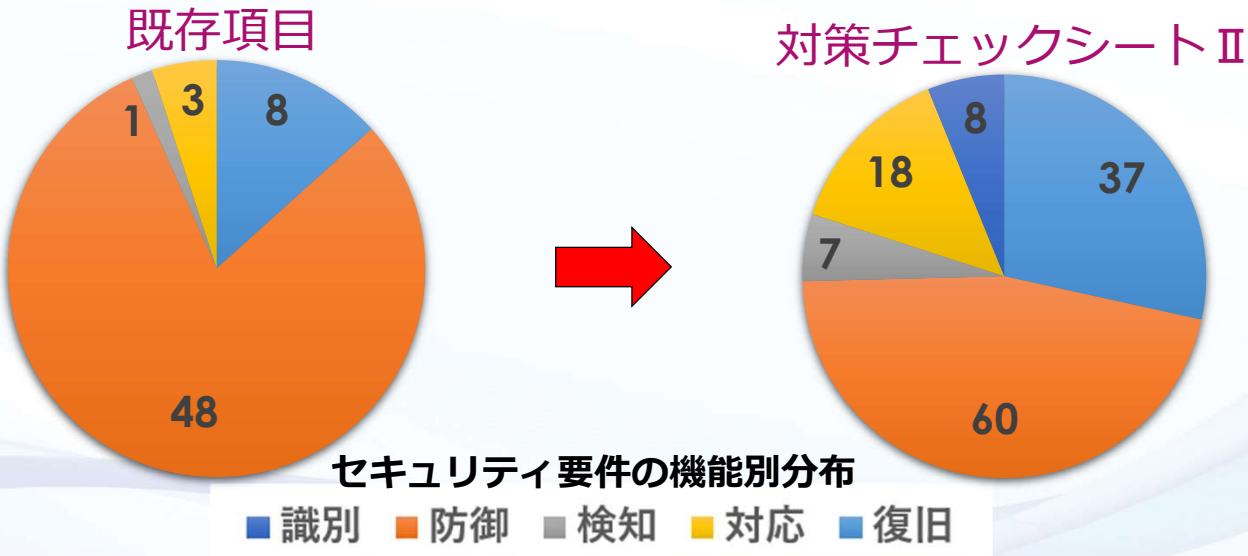
■既存チェックシートと新チェックシート(Ⅱ)の項目数比較

・前述のように、NIST-CSF 5機能に照合して過不足を検討した結果、
セキュリティ要件の機能別分布が、下記のように変化

既存項目数　：　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

見直し後の項目数：　識別37／防御60／検知７／対応18／復旧８



対策チェックシートⅡ　概要⑤

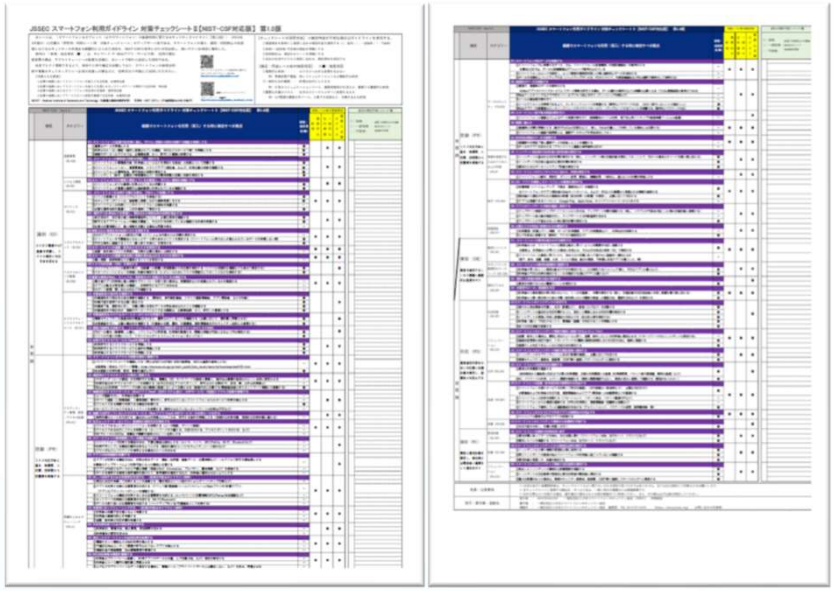
JAPAN SMARTPHONE SECURITY ASSOCIATION

■使いやすさの工夫

・A3両面に収めてコンパクトに！

・Excel版も配布、カスタマイズ可

・単独でも利用できるよう、項目中に例や補足を記載
  - 利用ガイドライン本体は、必要に応じて確認すればOK



※参考例：例や補足は以下の赤字部分

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）

対策チェックシートⅡ　概要⑥

JAPAN SMARTPHONE SECURITY ASSOCIATION

■対象となる読者

- 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
- 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
- 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
- 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

■活用シーン

- スマートフォンの新規活用開始時
- スマートフォンの活用範囲（対象業務・利用者・利用方法）の再検討時
- 情報セキュリティポリシー全体の見直し時

対策チェックシートⅡ　特長①

※下記①～⑤の色は次ページの表の説明と連動しています。

■ 5つのポイント

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

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

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

対策チェックシートⅡ　特長②

JAPAN SMARTPHONE SECURITY ASSOCIATION

■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。

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

対策チェックシートⅡ　活用手順

JAPAN SMARTPHONE SECURITY ASSOCIATION

■活用手順の例

Step1：表内①②の項目を参照し、自社のポリシーを照合

Step2：上記作業にて明確になった過不足項目を、
③を参照しながら整理

Step3：自社での用途を念頭に、④の推奨設定を
参照して採用/不採用を検討

Step4：採用/不採用の結果と理由を、⑤に記入

Step5：次回再検討時に、⑤欄を参照して見直し

■ご参考サイト

・経営層の視点：経産省/IPA「サイバーセキュリティ経営ガイドラインV.2.0」発行 等

https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf
https://www.ipa.go.jp/security/fy30/reports/ciso/index.html

・個人情報保護委員会サイト

https://www.ppc.go.jp/

対策チェックシートⅡ　活用の効果

JAPAN SMARTPHONE SECURITY ASSOCIATION

■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、経営層への報告時にも、**必要な要件の整理に役立ちます。**

まとめ～おわりに

JAPAN SMARTPHONE SECURITY ASSOCIATION

- NIST-CSFの「防御」における対策は、既存項目でもほぼカバーできていましたが、「検知・対応・復旧」の各項目は新設/追記が多いためぜひ一読してほしいと考えています。

- 多くの組織におけるセキュリティポリシーが、「防御」に偏っている可能性も否定できず、これを機にぜひ見直しをしてみていただきたいと思います。

- 「対策チェックシートⅡ」は、スマートフォンに係るセキュリティの項目を洗い出しています。
  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、それらを念頭に置いた上で、対策チェックシートⅡを有効に活用してください。**新資料が、皆様のお役に立てれば幸いです。**

制作

JAPAN SMARTPHONE SECURITY ASSOCIATION

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：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

ありがとうございました。

https://www.jssec.org/