

BSI PCI DSS文書テンプレート の取扱いについて

2018年 9月 28日

BSI Professional Services Japan株式会社
グローバルセキュリティエキスパート株式会社



By Royal Charter

目次

1. はじめに
2. 著作権
3. ご利用条件
4. 動作環境
5. ご提供文書
6. ご使用方法
7. ご使用上の注意点
8. 文書変更履歴

1. はじめに (1/2)

- 当商品は、PCI DSS準拠（PCI DSS v3.2に対応）に必要な方針、規程類、手順書等を編集可能なMicrosoft Word、Excel形式で提供した文書テンプレート集です。
- ご提供した文書はPCI DSS準拠のための文書テンプレートですので、貴社の現状に合わせてご自由にカスタマイズしてご使用下さい。

1. はじめに (2/2)

- ご提供した文書の中の以下4点は、付録という位置付けです。
※特に、1)、2)については各事業者様によって個別に定める性質のものであるため、あくまでも付録という位置付けで提供させていただきます。
- 1)「手順」フォルダの中の文書
 - 2)「記録フォーム」フォルダの中の文書
 - 3)PCI DSS 文書提供テンプレート一覧
(今回提供する文書テンプレートの一覧となります)
 - 4)PCI DSS 文書化チェックシート
(PCI DSSの文書化要件を確認するためのチェックシートとなります)

2. 著作権

- 当商品は共同著作物であり、著作権はBSI Professional Services Japan株式会社（以下当社とよぶ）とグローバルセキュリティエキスパート株式会社に帰属します。

3. ご利用条件

- 当商品は、ご購入者または所属組織内でのご使用を条件とします。
- 当商品に記載された目的で、加工・修正して使用することが可能です。
- 当商品は、使用者が次の事項に関する行為を行うことを禁止します。
 - 1)ご購入者または所属組織以外でのファイル及び印刷物の複製及び使用。
 - 2)当商品に記載された使用目的以外のデータファイル内容の改変・結合等。
 - 3)ファイル及びその複製物の譲渡・貸与・販売。

4. 動作環境

- Microsoft Office2010以降がインストールされている環境

5. ご提供文書 (1/2)

分類	提供文書名
方針・憲章	情報セキュリティ基本方針.docx PCI DSS憲章.docx
規程	PCI DSS運用規程.docx
基準・ポリシー	PCI DSS運用ポリシー.docx 脆弱性管理基準.docx 構成管理基準.docx
手順	PCIDSS_システム変更管理手順.docx PCIDSS_セキュリティパッチ適用手順.docx PCIDSS_暗号鍵管理手順.docx PCIDSSアクセスログ監視手順.docx PCIDSSアクセスログ監視手順別紙1 (監視対象機器ログ一覧) .docx PCIDSSアクセスログ監視手順別紙2 (調査指示書) .xlsx PCIDSSアクセスログ監視手順別紙3 (調査状況管理台帳) .xlsx PCIDSS_データ廃棄手順.docx PCIDSS_ウイルス対応手順.docx PCIDSS_ログ管理手順.docx PCIDSS_インシデント対応手順.xlsx PCIDSS_アクセス制御手順.docx

5. ご提供文書 (2/2)

分類	提供文書名
記録フォーム	PCIDSS運用会議記録.xlsx 入退室記録表.xlsx システム開発標準.xlsx
	PCI DSS 文書提供テンプレート一覧.xlsx PCI DSS 文書化チェックシート.xlsx

(ご注意)

上記の「PCI DSS 文書提供テンプレート一覧」の中の、ピンク色のセルが今回提供対象となります。

それ以外の無色のセルの文書は、今後、ご購入者に限り提供予定です。

その場合のご連絡は、別途メールにてお伝えいたします。

6. ご使用方法 (1/6)

1. まず、貴社がQSA（訪問審査）、SAQ（自己問診）のどちらの対応が必要かご確認ください。

その判断基準は以下の各カードブランドのWebサイトで確認できます。

<各カードブランドのPCI DSS準拠対応の判断基準>

VISA

http://www.visa-asia.com/ap/jp/merchants/riskmgmt/ais_how.shtml

JCB

<http://www.global.jcb/ja/products/security/data-security-program/>

MasterCard

<http://www.mastercard.co.jp/merchants/security-what-can-do-sdp-levels.html>

AMEX

https://merchant-channel.americanexpress.com/merchant/ja_JP/data-security?inav=jp_merch_security

6. ご使用方法 (2/6)

SAQの場合、カード会員データの取扱い方によって変わり、全部で9種類あります。どのSAQ（自己問診）を適用するかご確認下さい。

その判断基準はJCDSC（日本カード情報セキュリティ協議会）のWebサイトで確認できます。

<各 SAQ (v3.2 版)を適用すべきカード情報取扱い形態の説明 JCDSC>

http://www.jcdsc.org/topics/pdf/SAQ-type-20170701_Ver3.2.pdf

6. ご使用方法 (3/6)

2. 貴社がどのSAQを適用すればよいかご確認されましたら、該当のSAQの日本語訳版をダウンロードし、準拠に必要な要件を確認してください。

SAQ日本語訳版は以下のWebサイトでダウンロードできます。

<PCI SSC ドキュメントライブラリ 日本語訳版>

<https://ja.pcisecuritystandards.org/minisite/env2/>

6. ご使用方法 (4/6)

3. SAQ日本語版のドキュメントをご確認いただき、PCI DSS文書テンプレート（PCI DSS運用規程、PCI DSS運用ポリシー）の中で不要な要件を削除してください。
（もし削除しない場合、本来準拠しなくてもよい要件を守らなければいけなくなります。）

削除すべき要件は以下の文書で確認することができます。

文書テンプレートチェックシートのF～M列で該当するSAQを選び、「○」だけをフィルタしてください。

<SAQごとに準拠が必要な要件を確認できる文書>
PCI DSS 文書化チェックシート

6. ご使用方法 (5/6)

4. 貴社がQSAの対応が必要である場合、SAQではないので文書テンプレートチェックシートのF～M列でフィルタしない状態でご使用ください。
5. PCI DSS運用規程の文中に”【関連文書】TBD”と記載がある部分は、貴社の文書整備状況に合わせてご修正下さい。例えば関連文書がない場合、”【関連文書】TBD”の部分は削除してください。もしくは貴社が作成した文書で関連文書がある場合は、その文書名をご記入下さい。

6. ご使用方法 (6/6)

6. 当文書テンプレートでは、共有ホスティングプロバイダ、サービスプロバイダに対する追加要件も含んでおります。文書テンプレートの中で、共有ホスティングプロバイダ、サービスプロバイダに対する追加要件に該当する箇所を削除してください。

(もし削除しない場合、本来準拠しなくてもよい要件を守らなければいけなくなります。)

削除すべき要件は以下の文書で確認することができます。こちらのチェックシートのO,P列で「○」だけをフィルタしてください。

<共有ホスティングプロバイダ、サービスプロバイダに対する追加要件を確認できる文書>
PCI DSS 文書化チェックシート

※ただし、要件11.3.4と11.3.4.1については判別しにくいいため、サービスプロバイダに対する追加要件をあえて分けて表記しております。(該当文書名：PCI DSS脆弱性管理基準「表7.1 ペネトレーションテストの実施タイミング」)

7. ご使用上の注意点 (1/2)

- 以下の文書の表紙の日付、変更履歴は貴社にてご記入下さい。
 - PCI DSS運用規程
 - 情報セキュリティ基本方針
 - PCI DSS憲章
 - PCI DSS運用ポリシー
 - PCI DSS構成管理基準
 - PCI DSS脆弱性管理基準
 - システム開発標準

7. ご使用上の注意点 (2/2)

- 今後、PCI DSS要件がバージョンアップした場合、当文書テンプレートもバージョンアップした形であらためてご提供する予定ですが、その場合には、別途追加料金が必要となりますのであらかじめご了承下さい。
- 当文書テンプレートに関する内容についての質問は、コンサルティングの範疇になるためお答え致しかねます。
- 万が一、ダウンロード後ファイルがどうしても開けない場合は下記のメールアドレスまでお問い合わせください。他の方法でご提供いたします。

BSI Professional Services Japan へのお問い合わせ先

BSI.PSJ@bsigroup.com

8. 文書変更履歴

- 前回より更新があった文書、新規追加文書は以下の通りです。

分類	更新文書	新規文書
方針・憲章	—	—
規程	PCI DSS運用規程.docx	—
基準・ポリシー	PCI DSS運用ポリシー.docx	—
手順	—	PCIDSS_データ廃棄手順.docx PCIDSS_ウィルス対応手順.docx PCIDSS_ログ管理手順.docx PCIDSS_インシデント対応手順.xlsx PCIDSS_アクセス制御手順.docx
記録フォーム	—	—
その他	—	BSI PCI DSS文書テンプレートの取扱いについて.pdf

(ご注意) 文書内の変更箇所は、変更履歴付きの文書をご確認下さい。

「BSI PCI DSS文書テンプレートの取扱いについてpdf」は、前回readme.txtで提供しておりました。

bsi.

...making excellence a habit.™