準備ガイド

2018 年 9 月版

目次

1. 概要

EXIN Privacy & Data Protection Practitioner (PDPP.JP)

要約

EXIN プライバシーとデータ保護　プラクティショナ (PDPP)は、欧州のプライバシー(データ保護)法令とその国際的な影響についての専門家の知識と理解、さらに、その知識と理解を日々の専門的実務に適用する能力があることを認証する資格です。

試験サマリー

インターネットに氾濫する情報の爆発的な増加に伴い、すべての企業が人々のプライバシーやデータをどのように管理して保護するかを考えなければなりません。データの管理と保護を規制するための多数の新たな法律が、欧州連合(EU)に加えて米国や他の多くの地域で制定されつつあるのには理由があります。

先般、欧州委員会は EU 一般データ保護規則 (GDPR) を発表しました。これは、すべての関連する組織が具体的な規則を順守しなければならないことを意味します。PDPP は、既存及び新規法令、プライバシーとデータ保護のガイドラインやベストプラクティスの適用を順守するためのポリシーと手続を設計し実装することに重点を置き、データとプライバシーの保護マネジメントシステムを構築することによって、ファンデーション資格で網羅した項目をさらに発展させたものです。

背景

EXIN プライバシーとデータ保護　プラクティショナ (PDPP)資格は、プライバシー及びデータ保護に関する、EXIN の資格プログラムの一部です。

対象グループ

プラクティショナレベルの本資格は、特にデータ保護責任者(DPO)、プライバシー責任者、法務責任者／コンプライアンス責任者、セキュリティ責任者、ビジネス継続マネージャ、データ管理者（コントローラ）、データ保護監査人（内部および外部）、人事マネージャの役割を担う方に役立ちます。
本資格は上級レベルであるため、EXIN プライバシーとデータ保護 ファンデーション (PDPF)資格を所有していることを強く推奨します。

認定のための要件

- プライバシーとデータ保護　プラクティショナ認定講習の受講。実践課題の完了を含みます。
- EXIN プライバシーとデータ保護　プラクティショナ試験の合格。

試験の詳細内容

試験の形式:	コンピュータベースまたは紙ベースの多肢選択形式
問題数:	40
合格点:	65%
参考書やノートの持ち込み:	不可 文献 C のみがすべての試験項目の付録として提供され、適用可能な場合、使用することができます。
電子機器の持ち込み:	不可
試験時間:	120 分

EXIN の試験規則はこの試験に適用されます。

ブルームレベル

EXIN プライバシーとデータ保護　プラクティショナ試験では、改訂版ブルームの分類法に基づき、ブルームレベル 2、レベル 3 およびレベル 4 の受験者をテストします。

- ブルームレベル２：「理解」　「記憶」よりも上のステップです。「理解」することにより、受験者は提示された内容を理解していることを示し、学習教材が受験者の環境でどのように適応できるかを評価することができます。
- ブルームレベル 3：「応用」　学習した時とは違う環境で知識を利用する能力が受験者にあることがわかります。質問の目的は、受験者が獲得した知識、事実、技法、規則を異なる方法または新たな方法で応用して、新しい状況での問題を解決できるのを実証することです。質問には通常短いシナリオが含まれます。
- ブルームレベル 4：「分析」　学習した情報を分解して理解する能力が受験者にあること示します。このブルームレベルでは、主に実践課題でテストされます。実践課題の目的は、受験者が動機または原因を識別することによって情報を検査し分解できること、推論を立てられること、また、総括するためのエビデンスを見つけられることを実証することです。

教育・訓練

授業時間

この教育コースの推奨受講時間は 21 時間です。（グループ）課題、試験準備、休憩が含まれます。宿題、実践課題、試験時間、昼休みはこの時間に含まれません。実践課題の推奨受講時間は最大 8 時間です。実践課題は受講時間外に完了することが可能です。また、コース時間を延長し、コース時間内に実践課題の完了を含めることができます。
教育事業者が、国内のプライバシーとデータ保護法案に時間を割り当てたい場合には、推奨受講時間の 21 時間とは別にコース時間を追加する必要があります。

学習時間の目安

120 時間を推奨しますが、個人が習得している知識によります。

教育事業者

認定教育事業者のリストを www.exin.com で参照できます。

2. 試験要件

試験要件は、試験仕様に明記されています。以下の表にモジュールトピック（試験要件）とサブトピック（試験仕様）の一覧を示します。

試験要件	試験仕様	配分
1. データ保護ポリシー		**10%**
	1.1 受験者は組織におけるデータ保護／プライバシーポリシーの目的を理解している	5%
	1.2 受験者はデータ保護バイ・デザインおよびデータ保護バイ・デフォルトを理解している	5%
2. データ保護の管理と構成		**35%**
	2.1 受験者はデータ保護管理システム(DPMS)を段階的に適用することができる	35%
	2.2 受験者はデータ保護意識を高める行動計画の理論を適用することができる[1]	0%
3. 管理者（コントローラ）、処理者/取扱者（プロセッサ）、データ保護責任者(DPO)の役割		**15%**
	3.1 受験者は管理者（コントローラ）及び処理者/取扱者（プロセッサ）の役割を実装することができる	7.5%
	3.2 受験者はデータ保護責任者(DPO)の役割及び責任を規定できる	7.5%
4. データ保護影響評価(DPIA)		**30%**
	4.1 受験者はデータ保護影響評価(DPIA)の基準を適用できる	15%
	4.2 受験者はデータ保護影響評価(DPIA)のステップを適用できる	15%
5. データ侵害、通知及びインシデント対応		**10%**
	5.1 受験者は個人データ侵害に関する GDPR 要件を適用することができる	5%
	5.2 受験者は通知要件を適用することができる	5%
	合計	100%

[1] 試験仕様 2.2 は参考文献が不十分なため、現行の試験には含まれません。今後のバージョンで追加される予定です。

試験仕様

1 データ保護ポリシー

1.1 受験者は組織におけるデータ保護／プライバシーポリシーの目的を理解している
次のことが行える。
- 1.1.1 データ保護法令を順守するために組織において必要なポリシーと手続について説明ができる
- 1.1.2 ポリシーの内容について説明ができる

1.2 受験者はデータ保護バイ・デザインおよびデータ保護バイ・デフォルトを理解している
次のことが行える。
- 1.2.1 データ保護バイ・デザインおよびデータ保護バイ・デフォルトの概念について説明ができる
- 1.2.2 データ保護バイ・デザインおよびデータ保護バイ・デフォルトの 7 つの原則について記述ができる
- 1.2.3 データ保護バイ・デザインおよびデータ保護バイ・デフォルトの原則をどのように実施するかを具体例で説明できる

2 データ保護の管理と構成

2.1 受験者はデータ保護管理システム(DPMS)を段階的に適用することができる
次のことが行える。
- 2.1.1 DPMS の第 1 段階「データ保護とプライバシー：準備」をどのように適用するかを具体例に説明できる
- 2.1.2 DPMS の第 2 段階「データ保護とプライバシー：組織」をどのように適用するかを具体例に説明できる
- 2.1.3 DPMS の第 3 段階「データ保護とプライバシー：構築と実施」をどのように適用するかを具体例に説明できる
- 2.1.4 DPMS の第 4 段階「データ保護とプライバシー：ガバナンス」をどのように適用するかを具体例に説明できる
- 2.1.5 DPMS の第 5 段階「データ保護とプライバシー：評価と改善」をどのように適用するかを具体例に説明できる

2.2 受験者はデータ保護意識を高める行動計画の理論を適用することができる[2]
次のことが行える。
- 2.2.1 特定の状況におけるデータ保護意識のための行動計画を作成できる

3 管理者（コントローラ）、処理者/取扱者（プロセッサ）、データ保護責任者(DPO)の役割

3.1 受験者は管理者（コントローラ）及び処理者/取扱者（プロセッサ）の役割を実装することができる
次のことが行える。
- 3.1.1 管理者の責任を規定できる
- 3.1.2 処理者の責任を規定できる
- 3.1.3 特定の状況における管理者と処理者の関係について説明できる

3.2 受験者はデータ保護責任者(DPO)の役割及び責任を規定できる
次のことが行える。
- 3.2.1 データ保護責任者(DPO)が GDPR の下でいつ義務化されたか説明できる
- 3.2.2 データ保護責任者(DPO)の役割を規定できる
- 3.2.3 データ保護責任者(DPO)の監督機関との関係における立場について説明できる

[2] 試験仕様 2.2 は参考文献が不十分なため、現行の試験には含まれません。今後のバージョンで追加される予定です。

4　データ保護影響評価(DPIA)

4.1　受験者はデータ保護影響評価(DPIA)の基準を適用できる

次のことが行える。

4.1.1　データ保護影響評価(DPIA)を実施するための基準を適用できる

4.1.2　データ保護影響評価(DPIA)の目的と結果について記述できる

4.2　受験者はデータ保護影響評価(DPIA)のステップを適用できる

次のことが行える。

4.2.1　データ保護影響評価(DPIA)のステップについて記述できる

4.2.2　特定の状況においてデータ保護影響評価(DPIA)を実施できる

5　データ侵害、通知及びインシデント対応

5.1　受験者は個人データ侵害に関する GDPR 要件を適用することができる

次のことが行える。

5.1.1　　データ侵害が GDPR の観点から発生しているかどうか評価できる

5.2　受験者は通知要件を適用することができる

次のことが行える。

5.2.1　個人データ侵害を監督機関に通知できる

5.2.2　個人データ侵害をデータ主体に通知できる

5.2.3　GDPR の文書化義務の要素について記述ができる

3. 基本概念の一覧

この章では、認定候補者が習熟しておく必要がある用語と略語を示します。

これらの用語の知識だけでは試験に十分ではないことに注意してください。受験者は、その概念を理解し、例を提示できる必要があります。

英語	日本語
adequate	十分な
appropriate technical and organizational measures	適切な技術及び組織的な対策
audit • initial data (protection) audit • internal and external data (protection) audit	監査 • 初期データ（保護）監査 • 内部及び外部データ（保護）監査
authenticity	真正性
availability	可用性
awareness	意識
benchmark	ベンチマーク
binding	拘束
binding corporate rules	拘束的企業準則(BCR)
biometric data	生体認証データ
Bring Your Own Device (BYOD)	個人デバイスの持ち込み(BYOD)
certification	認証
certification bodies	審査機関
child's consent	子供の同意
cloud computing	クラウドコンピューティング
codes of conduct	行動規範
collection of personal data (verb.)	個人データを収集する（動詞）
commission reports	欧州委員会報告書
complaint	苦情
compliance	コンプライアンス
conditions for consent	同意の条件
consent	同意
consistency	一貫性
consistency mechanism	統一する仕組み（一貫性メカニズム）
constitution	憲法
contract	契約
controller	管理者（コントローラ）
cross-border processing	国境を越えた処理（越境的取扱い）
data accuracy	データの正確性
data breach	データ侵害
data classification system	データ分類システム
data concerning health	健康に関するデータ
data controller	データ管理者（コントローラ）
data lifecycle management (DLM)	データライフサイクルマネジメント（DLM）
data mapping	データマッピング

data portability	データポータビリティ
data protection	データ保護
(data privacy) breach response plan / data privacy incident response plan	（データ　プライバシー）侵害対応計画／データ　プライバシーインシデント対応計画
data protection authority (DPA)[3]	データ保護機関(DPA)
data protection by default / privacy by default	データ保護バイ・デフォルト / プライバシーバイ・デフォルト
data protection by design / privacy by design	データ保護バイ・デザイン / プライバシーバイ・デザイン
data protection impact assessment (DPIA) / privacy impact assessment (PIA)	データ保護の影響評価(DPIA) / プライバシー影響評価(PIA)
Data Protection Management System (DPMS) / Data Protection and Privacy Management System (DPMS)	データ保護マネジメントシステム(DPMS) /データ保護及びプライバシーマネジメントシステム(DPMS)
data protection officer (DPO) • designation • position • tasks	データ保護責任者(DPO) • 指名 • 地位 • 役割
data protection policy	データ保護ポリシー
data protection program	データ保護プログラム
data protection provisions	データ保護条項
data subject	データ主体
data subject access (facilities)	データ主体のアクセス（設備）
data transfer	データ移転
declaration of consent	同意の宣言
delegated acts and implementing acts • committee procedure	委任法及び施行法 • 委員会手続
documentation obligation	文書化の義務
derogation	免除（除外）
enforcement • administrative fines • administrative penalties • criminal penalties • dissuasive penalties • effective penalties • proportionate penalties	執行 • 過料（制裁金） • 行政罰 • 刑事罰 • 抑止的な罰 • 効果的な罰 • 均衡がとれた罰
enterprise	事業者または企業
European Economic Area (EEA)	欧州経済領域　(European Economic Area (EEA))
EU types of legal act • decision • directive • opinion • recommendation • regulation	EU の法令（法律・規制類）の体系 • 決定 • 指令 • 意見 • 勧告 • 規則

[3] GDPR が導入される前は、「*データ保護機関*」がデータ保護に関する規制の施行を担う国家機関でした。GDPR では、現在「*監督機関*」と呼びます。

European Data Protection Board • chair • confidentiality • independence • procedure • reports • secretariat • tasks	欧州データ保護評議会 • 議長 • 機密性 • 独立性 • 手続き • 報告書 • 事務局 • 役割
European Data Protection Supervisor (EDPS)	欧州データ保護監督官 (EDPS：European Data Protection Supervisor)
European Union legal acts on data protection	データ保護に関する EU 法令
exchange of information	情報交換
exemption	除外（免除）
explicit consent	明確な同意
filing system	ファイリングシステム
General Data Protection Regulation (GDPR)	一般データ保護規則（GDPR）
genetic data	遺伝子データ
governing body	運営組織
group of undertakings	事業体グループ
incident response	インシデント対応
independent supervisory authorities • activity reports • competence • establishment • powers • tasks	独立監督機関 • 活動報告書 • 管轄 • 創設・設置 • 権限 • 役割
Information Security Management System (ISMS)	情報セキュリティマネジメントシステム (ISMS)
information society service	情報社会サービス
international organization	国際組織
Internet of Things (IOT)	モノのインターネット(IoT)
joint controllers	共同管理者
judicial remedy	司法的救済
lawfulness of processing	適法な取扱い
legal basis	法的根拠
legitimate ground (GDPR article 17/1c, article 18/1d, article 21/1) and legitimate basis (GDPR article 40)	正当な事由（GDPR 17 条 1c、 18 条 1d、21 条 1）及び法的根拠（GDPR 40 条）
legitimate interest	正当な利益
liability	法的責任
main establishment	主たる事業所
material scope	実体的範囲
measures based on DPIA results	DPIA の結果に基づく対策
National Identification Number	国民識別番号
non-repudiation	否認防止
notification obligation	通知義務
opinion of the board	欧州データ保護会議の意見
personal data	個人データ
personal data breach	個人データ侵害

personal data relating to criminal convictions and offences	有罪判決及び犯罪に関する個人データ
principles relating to processing of personal data	個人データの取扱いに関する原則
• accountability	• 説明責任（アカウンタビリ ティ）
• accuracy	• 正確性
• confidentiality	• 機密性
• data minimization	• データの最小化
• fairness	• 公正性
• integrity	• 完全性
• lawfulness	• 適法性
• purpose limitation	• 目的の制限
• storage limitation	• 保存の制限
• transparency	• 透明性
policy	ポリシー/方針
policy rule(s)	ポリシー規定
prior consultation	事前協議
privacy	プライバシー
privacy analysis	プライバシー分析
privacy officer/chief privacy officer	プライバシー責任者／主任プライバシー責任者
processing	処理（取扱）
processing (of personal data)	処理（取扱）（個人データの）
processing agreement	同意の取扱
processing situations	取扱い状況
• data protection rules of churches and religious associations	• 教会及び宗教組織のデータ保護規則
• employment	• 雇用
• for archiving purposes in the public interest	• 公共の利益における保管目的
• for scientific or historical research purposes	• 科学的若しくは歴史的研究の目的
• for statistical purposes	• 統計目的
• freedom of expression and information	• 表現及び情報の自由
• National Identification Number	• 国民識別番号
• obligations of secrecy	• 守秘義務
• public access to official documents	• 公式文書へのパブリック・アクセス
processing which does not require identification	識別を要求しない取扱い
processor	処理者/取扱者
profiling	プロファイリング
proportionality, the principle of	比例性の原則
pseudonymization	仮名化
quality cycle	品質サイクル
recipient	取得者
relevant and reasoned objection	適切及び合理的な不服
repealed	無効化された、破棄された
representative	代表者
restriction of processing	取扱いの制限
retention period	保存期間

right to compensation	賠償請求権
rights of the data subject	データ主体の権利
• automated individual decision-making	• 自動化された個人意思決定
• data portability	• データ・ポータビリティ
• information and access	• 情報及びアクセス（情報及び認証手続）
• modalities	• 手続
• notification obligation	• 通知義務
• rectification and erasure	• 訂正若しくは消去
• restriction of processing	• 取扱いの制限
• restrictions	• 制限
• ‘right to be forgotten’	• ‘忘れられる権利’
• right to objection	• 不服申立ての権利
• transparency	• 透明性
risk management	リスク管理
rules of procedure	手続規定
security breach (security incident)	セキュリティ侵害（セキュリティ　インシデント）
security of personal data	個人データの保護
security of processing	取扱いの保護
sensitive data	機微データ
service provider	サービスプロバイダ
seven principles for privacy by design (Lit. A Chapter 5, paragraph Privacy by design and by default)	プライバシーバイ・デザインの７つの原則（参考文献　A　Chapter 5, paragraph Privacy by design and by default))
Social, Mobile, Analytics, Cloud, Things (SMACT)	ソーシャル、モバイル、分析、クラウド、モノ(SMACT)
special categories of personal data	特別な種類の個人データ
• biometric data	• 生体データ
• data concerning health	• 健康に関するデータ
• genetic data	• 遺伝データ
• political opinions	• 政治的思想
• racial or ethnic origin	• 人種的または民族的素性
• religious or philosophical beliefs	• 政治的または宗教的信条
• sex life or sexual orientation	• 性生活または性的指向
• trade union membership	• 労働組合員資格
subsidiarity, the principle of	補完性の原則
supervisory authority	監督機関
supervisory authority concerned	関係監督機関
suspension of proceedings	訴訟の一時停止
territorial scope	地理的範囲
third party	第三者
threat	脅威

transfer of personal data to third countries and to international organizations • adequacy decision • appropriate safeguards • binding corporate rules • derogations • disclosures • international protection of personal data	第三国または国際機関への個人データの移転 • 十分性の決定（十分性認定） • 十分な保護措置 • 拘束的企業準則(BCR) • 逸脱 • 開示 • 国際的な個人データ保護
unified communications and collaboration (UCC)	統合コミュニケーション及びコラボレーション(UCC)
vulnerability	脆弱性

4. 参考文献

試験の参考文献

試験に必要な知識は、次の文献に記載されています。

A. IT Governance Privacy Team
EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide
IT Governance Publishing, Cambridgeshire (2016)
ISBN 978-1-84928-8354 (paperback)
ISBN 978-1-84928-8378 (e-book)

B. Kyriazoglou, J.
Data Protection and Privacy Management System. Data Protection and Privacy Guide - Vol. 1
bookboon.com 1st edition (2016)
ISBN 978-87-403-1540-0

C. European Commission
General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) Regulation of the European Parliament and the Council of the European Union. Brussels, 6 April 2016, available at http://eur-lex.europa.eu
PDF:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN
HTML:
http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=EN

D. Article 29 Data Protection Working Party
Guidelines on Data Protection Officers ('DPOs'), wp 243rev.01, 5 April 2017 available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

E. Article 29 Data Protection Working Party
Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248, 4 April 2017 available at
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

コメント

試験要件は試験の参考文献に基づきます。GDPR に関する十分な内容が他の参考文献に含まれているため、文献 C は主要参考文献ではありません。受験者は、他の参考文献で参照された内容の範囲内で文献 C について精通しておく必要があります。文献 C はすべての試験項目の付録として提供され、適用可能な場合は参照可能です。

追加文献

F. Example of Privacy by Design Framework
https://www.privacycompany.eu/files/DPbD_Framework.pdf

コメント

追加の参考文献は、参考として知識を深めるためのものです。

参考文献と試験仕様

試験要件	試験仕様	参考文献
1. データ保護ポリシー		
	1.1 受験者は組織におけるデータ保護／プライバシーポリシーの目的を理解している	A: Chapter 16 paragraph Using policies to demonstrate compliance
	1.2 受験者はデータ保護バイ・デザインおよびデータ保護バイ・デフォルトを理解している	A: Chapter 5 paragraph Privacy by design and by default
2. データ保護の管理と構成		
	2.1 受験者はデータ保護管理システム(DPMS)を段階的に適用することができる	A: Chapter 12 paragraph Records of processing A: Chapter 14 introduction + paragraph Notification B: Chapter 2, paragraph 2 DP&P System Phases
	2.2 受験者はデータ保護意識を高める行動計画の理論を適用することができる	*No literature yet*
3. 管理者（コントローラ）、処理者/取扱者（プロセッサ）、データ保護責任者(DPO)の役割		
	3.1 受験者は管理者（コントローラ）及び処理者/取扱者（プロセッサ）の役割を実装することができる	A: Chapter 12
	3.2 受験者はデータ保護責任者(DPO)の役割及び責任を規定できる	A: Chapter 2 B: Chapter 2 paragraph 2 Phase 4 D: Chapter 2 paragraph 1 Mandatory designation D: Chapter 4 Tasks of the DPO D: Chapter 5 paragraph 1 Which organizations must appoint a DPO?
4. データ保護影響評価(DPIA)		
	4.1 受験者はデータ保護影響評価(DPIA)の基準を適用できる	A: Chapter 5 introduction, paragraph Privacy Impact Assessments and paragraph When to conduct a DPIA A: Chapter 6 paragraph DPIA’s as part of risk management A: Chapter 8 paragraph Objectives and outcomes E: Chapter 3 DPIA: the Regulation explained

	4.2 受験者はデータ保護影響評価(DPIA)のステップを適用できる	A: Chapter 5 paragraph Privacy Impact Assessments A: Chapter 7 A: Chapter 8 paragraph Five key stages in a DPIA and paragraph Consultation E: Chapter 3 DPIA: the Regulation explained
5. データ侵害、通知及びインシデント対応		
	5.1 受験者は個人データ侵害に関するGDPR要件を適用することができる	A: Chapter 3 paragraph Personal data breaches, Anatomy of a data breach, Sites of attack
	5.2 受験者は通知要件を適用することができる	A: Chapter 14 paragraph Notification, paragraph Events vs incidents, paragraph Types of incidents

コメント

文献C、‘GDPR’は、詳細には参照されません。

EXIN の連絡先

www.exin.com

YOUR ICT COMPETENCE PARTNER