システム監査学会
２０１８年度「情報セキュリティ対策の診断」研究プロジェクト

ＥＵ一般データ保護規則(GDPR)対応研究
成果物集

目次

はじめに
１．ＧＤＰＲの対象企業チェックリスト
２．ＧＤＰＲへの対応策
2.1.対応策に向けての考え方
2.2.ＥＵ域内事業所での対応
2.3.日本国内事業所での対応
3.4.補完的ルールへの対応
2.5.標準的契約条項の利用
３．制裁金の仕組み
3.1.制裁金に関する規定
3.2.GDPR が制裁金を科す原則
3.3.GDPR の制裁金の設定
４．ＧＤＰＲの違反可能性チェックリスト
4.1.違反可能性チェック
５．同意書の重要さ
5.1.同意書の位置づけ
5.2.同意書上の表現
5.3.多種類の個人データの取得
６．ＰＭＳやＩＳＭＳの内容を強化
6.1.ＧＤＰＲと日本の個人情報保護法との関係
6.2.GDPRと個人情報保護法との相違点
6.3.ＧＤＰＲとＰマークとの関係
6.4.GDPR とISMSとの関係
おわりに
参考資料

研究期間　2018 年 7 月～2019 年 5 月
報告書作成　2019 年 5 月 22 日

研究プロジェクト主査　木村裕一
研究メンバー　尾崎孝章、赤尾嘉治、鈴木淳哉
オブザーバー　久山真宏

ご質問、お問い合わせは、システム監査学会経由でチーム主査までご連絡ください。
問合せフォーム　→ https://www.sysaudit.gr.jp/toiawase/index.html
連絡先:システム監査学会　→ https://www.sysaudit.gr.jp
〒106-0032　東京都港区六本木 1 丁目 9-9　六本木ファーストビル　JIPDEC 内

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

はじめに

この成果物集は初めてGDPR(General Data Protection Regulation)に接した方への分かりやすい説明・対応を試みたものです。

グローバルなビジネス展開をしている企業なら、GDPRは好むと好まざるとに関わらず、知っておかなければならないルールだと考えます。そのため、何時、何処で、誰が、何を、なぜ、どのように、と5W1H的に考えやすいように構成しています。一先ずこの資料を理解した上で、更に上級の対応へステップアップして、企業リスクの低減を試みることを期待します。

1．GDPRの対象企業チェックリスト

(1)対象企業チェックリスト

企業とすれば、まず、第一に我が社がGDPRの対象となるかどうかの心配がある。

そのため、対象企業チェックリストを作成したのでセルフチッェクをして欲しい。

対象企業チェックリスト(CL)

質問	チェック項目	チェック内容	GDPR条文	判断の結果	備考
A	EU域内拠点有無	EU域内に管理者または処理者の拠点がある。	3	YES／NO	
B	データ移転	EU所在のデータ主体の個人情報を日本に移転している。	44	YES／NO	
C	データ移転	EU所在のデータ主体の個人情報を移転元より受け取っている。	44	YES／NO	
D	収集場所	EU域内の市場では活動しておらず、EU域内データ主体が日本滞在時にのみ個人情報の収集している。	3	YES／NO	
E	サービス内容	EU域内データ主体に対し日本国内からネットワーク経由で、EUの言語、通貨等によるサービス・商品を提供している。	3	YES／NO	

この対象企業チェックリストでチッェクした結果、YES が一つでもあれば、念のため本資料に沿って、対応作業を行っていただきたい。

(2)対象企業の内、どのパターンか

今回のGDPRのケースではEU域内と日本との2拠点での事象に対しての対応であるので幾つかのパターンに分けて説明した方が分かりやすいと判断した。

①資料図:GDPR対象企業のフローに基づき、質問A～Eまでを辿り、自社がパターンの「**1～5**」のどのパターンに該当するか確認する。

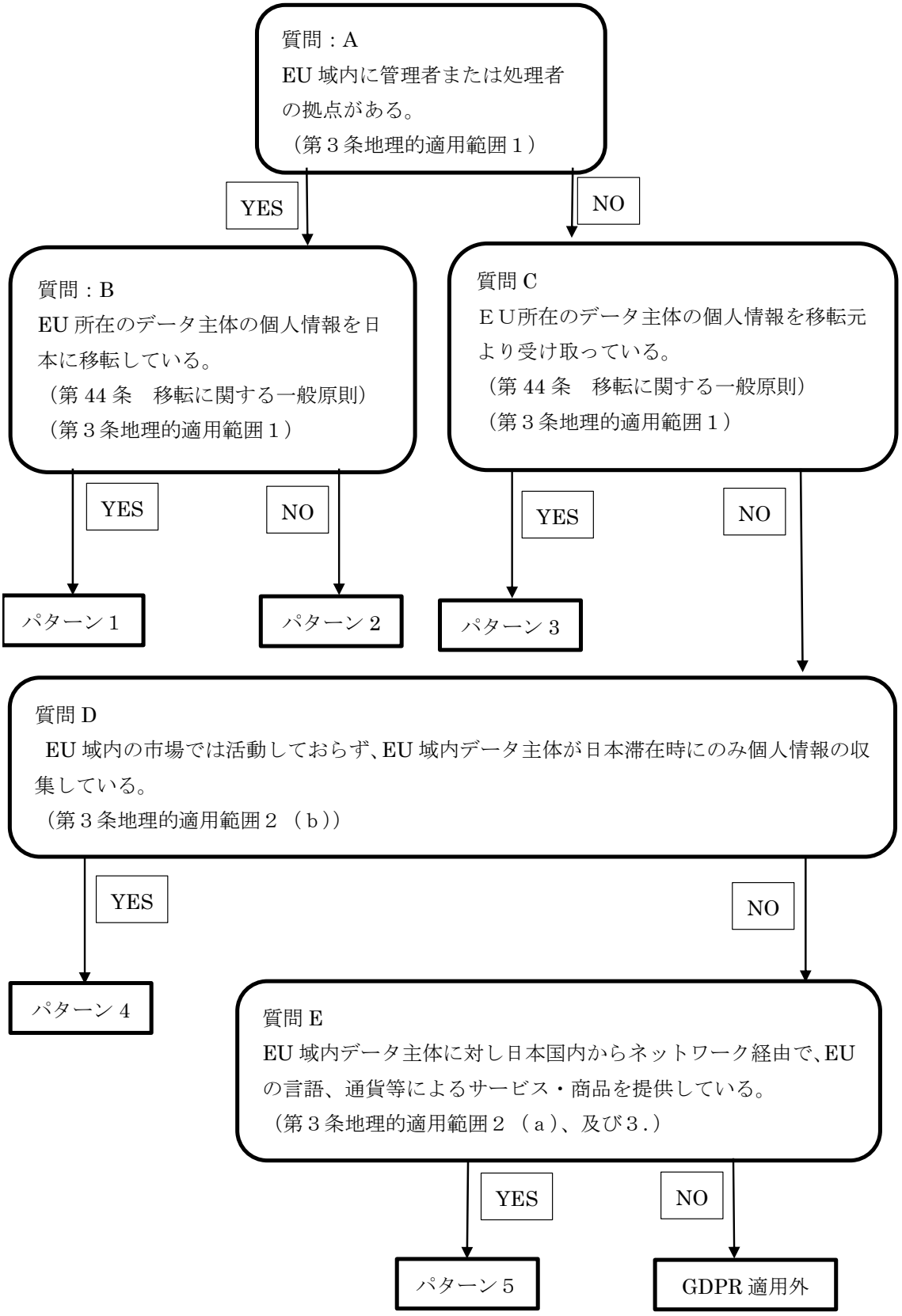
②パターンが決まったら、各パターンの詳細が書かれている内容で、質問A～Eの選択の正しかったことの確認

③EU域内と日本との2拠点での状況を図示した画像で地理的適用範囲の関係をイメージする。

④更に各パターンの「観点」、「法令」、「認定」、「同意」、「制裁」の内容を把握し、自社の置かれている環境、管理するべき状況を確実にし、取るべき対策の主要な観点を理解していただきたい。

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

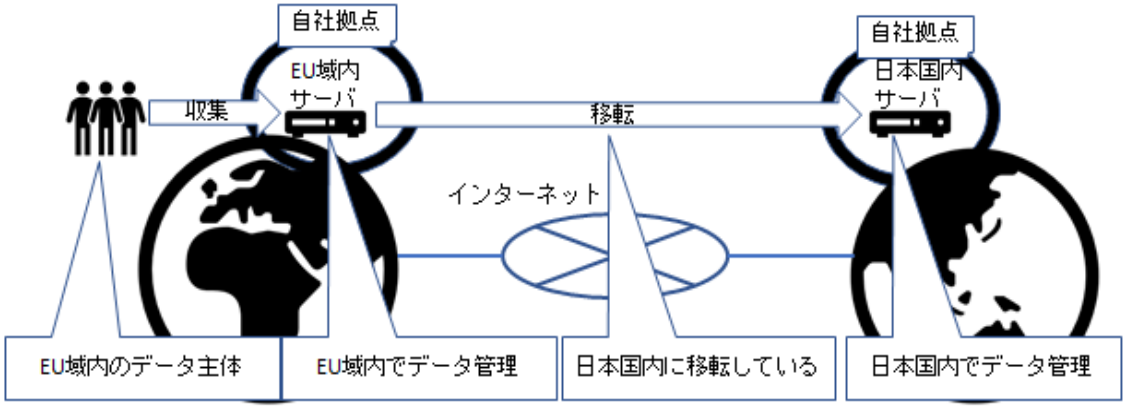
資料図：GDPR 対象企業



©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

パターン１：ＥＵ域内に管理者または処理者の拠点があり、個人情報を日本に移転している。

質問	チェック項目	チェック内容	GDPR条文	判断の結果	備考
A	EU域内拠点有無	EU 域内に管理者または処理者の拠点がある。	3	YES	
B	データ移転	EU 所在のデータ主体の個人情報を日本に移転している。	44	YES	
C	データ移転	EU 所在のデータ主体の個人情報を移転元より受け取っている。	44	不問	
D	収集場所	EU 域内の市場では活動しておらず、EU 域内データ主体が日本滞在時にのみ個人情報の収集している。	3	不問	
E	サービス内容	EU 域内データ主体に対し日本国内からネットワーク経由で、EU の言語、通貨等によるサービス・商品を提供している。	3	不問	

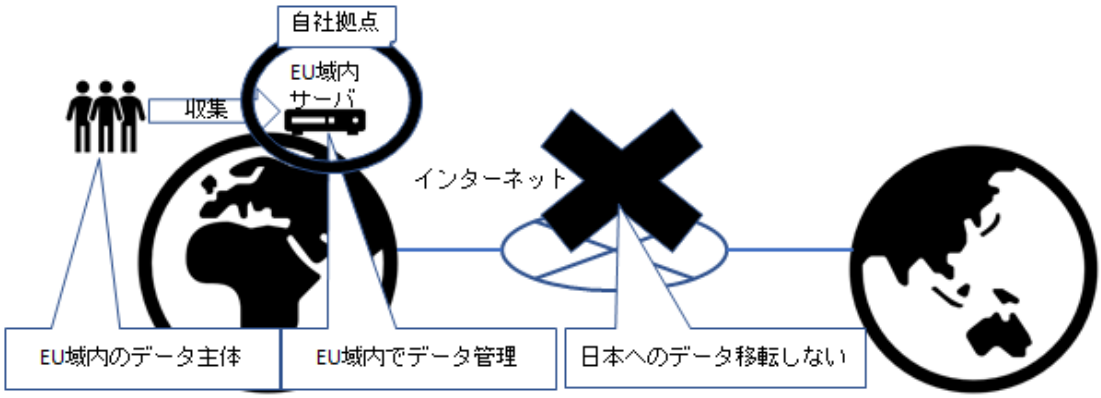


観点	EU 域内事業所	移転に関する統治（本社→事業所への指示）	日本国内事業所
法令	・ＧＤＰＲ遵守	・ＧＤＰＲ遵守指示	・個人情報保護法遵守 ・十分性認定遵守
認定	・ＩＳＭＳの取得	―	・ＩＳＭＳ又はＰマークの取得 ・補完的ルールの順守
同意	・データ主体からの同意書の取得 ・データ主体からの移転の同意取得	・同意書の取得指示 ・同意書の内容確認	・EU 域内の事業所が同意書の取得済確認
制裁	・制裁金の対象		・制裁金は受けないが、契約の関係に基づき影響を受ける。

パターン２：ＥＵ域内に管理者または処理者の拠点があり、個人情報を日本に移転していない。

質問	チェック項目	チェック内容	GDPR条文	判断の結果	備考
A	EU域内拠点有無	EU 域内に管理者または処理者の拠点がある。	3	YES	
B	データ移転	EU 所在のデータ主体の個人情報を日本に移転している。	44	NO	
C	データ移転	EU 所在のデータ主体の個人情報を移転元より受け取っている。	44	不問	
D	収集場所	EU 域内の市場では活動しておらず、EU 域内データ主体が日本滞在時にのみ個人情報の収集している。	3	不問	
E	サービス内容	EU 域内データ主体に対し日本国内からネットワーク経由で、EU の言語、通貨等によるサービス・商品を提供している。	3	不問	

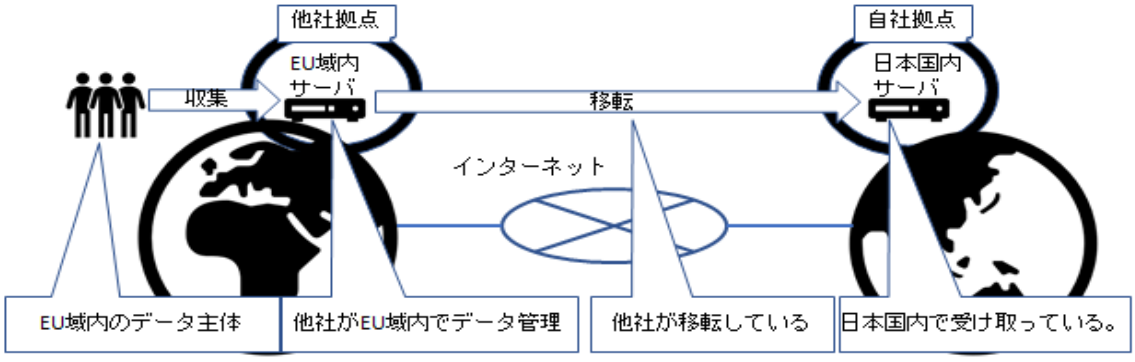
©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.



観点	EU 域内事業所	移転に関する統治 （本社→事業所への指示）	日本国内事業所
法令	・ＧＤＰＲ遵守	・ＧＤＰＲ遵守指示	―
認定	・ＩＳＭＳの取得	―	―
同意	・データ主体からの同意書の取得 ・データ主体からの同意書の取得済確認	・同意書の取得指示 ・同意書の内容確認	―
制裁	・制裁金の対象		―

パターン３：ＥＵ域内に拠点がなく、個人情報を移転元より日本国内で受け取っている。

質問	チェック項目	チェック内容	GDPR条文	判断の結果	備考
A	**EU域内拠点有無**	**EU 域内に管理者または処理者の拠点がある。**	**3**	**NO**	
B	データ移転	EU 所在のデータ主体の個人情報を日本に移転している。	44	不問	
C	**データ移転**	**EU 所在のデータ主体の個人情報を移転元より受け取っている。**	**44**	**YES**	
D	収集場所	EU 域内の市場では活動しておらず、EU 域内データ主体が日本滞在時にのみ個人情報の収集している。	3	不問	
E	サービス内容	EU 域内データ主体に対し日本国内からネットワーク経由で、EU の言語、通貨等によるサービス・商品を提供している。	3	不問	

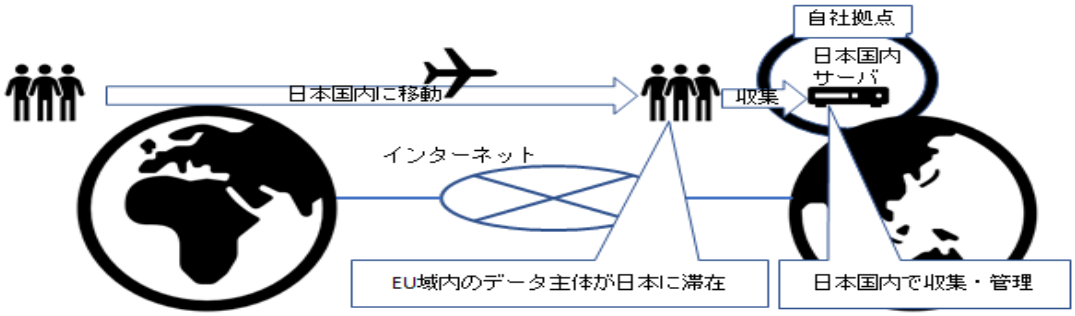


©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

観点	EU 域内事業所	移転に関する統治 （自社→他社への指示）	日本国内事業所
法令	・ＧＤＰＲ遵守	・ＧＤＰＲ遵守指示	・個人情報保護法遵守 ・十分性認定遵守
認定	・ＩＳＭＳの取得	―	・ＩＳＭＳ又はＰマークの取得 ・補完的ルールの順守
同意	・データ主体からの同意書の取得 ・データ主体からの移転の同意取得	・同意書の取得指示 ・同意書の内容確認	・EU 域内の事業所が同意書の取得済確認
制裁	・制裁金の対象		・制裁金は受けないが、契約の関係に基づき影響を受ける。

パターン４：ＥＵ域内に拠点がなく、データ主体が日本に滞在時のみ個人情報を収集する。

質問	チェック項目	チェック内容	GDPR 条文	判断の結果	備考
A	EU域内拠点有無	EU 域内に管理者または処理者の拠点がある。	3	NO	
B	データ移転	EU 所在のデータ主体の個人情報を日本に移転している。	44	不問	
C	データ移転	EU 所在のデータ主体の個人情報を移転元より受け取っている。	44	NO	
D	収集場所	EU 域内の市場では活動しておらず、EU 域内データ主体が日本滞在時にのみ個人情報の収集している。	3	YES	
E	サービス内容	EU 域内データ主体に対し日本国内からネットワーク経由で、EU の言語、通貨等によるサービス・商品を提供している。	3	不問	



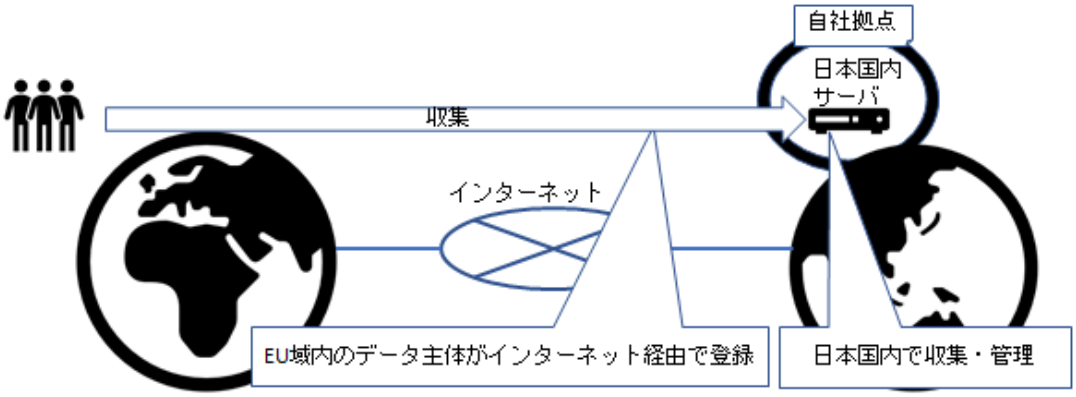
観点	EU 域内事業所	移転に関する統治	日本国内事業所
法令	―	―	・個人情報保護法遵守 ・十分性認定遵守
認定	―	―	・ＩＳＭＳ又はＰマークの取得 ・補完的ルールの順守
同意	―	―	・データ主体からの同意書の取得
制裁			・日本国内の法制度に従う。

※ＧＤＰＲの地理的適用範囲（第３条）に関するガイドラインより、ＥＵ市場で活動していない企業にたいするＧＤＰＲの適用は対象外となるが、国内の個人情報保護法の範囲での対応は必要。

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

パターン５：

質問	チェック項目	チェック内容	GDPR条文	判断の結果	備考
A	EU域内拠点有無	EU 域内に管理者または処理者の拠点がある。	3	NO	
B	データ移転	EU 所在のデータ主体の個人情報を日本に移転している。	44	不問	
C	データ移転	EU 所在のデータ主体の個人情報を移転元より受け取っている。	44	NO	
D	収集場所	EU 域内の市場では活動しておらず、EU 域内データ主体が日本滞在時にのみ個人情報の収集している。	3	NO	
E	サービス内容	EU 域内データ主体に対し日本国内からネットワーク経由で、EU の言語、通貨等によるサービス・商品を提供している。	3	YES	



観点	EU 域内事業所	移転に関する統治（自社→他社への指示）	日本国内事業所
法令	—	—	・個人情報保護法遵守 ・十分性認定遵守
認定	—	—	・ＩＳＭＳ又はＰマークの取得 ・補完的ルールの順守
同意	—	—	・データ主体からの同意書の取得 ・データ主体からの移転の同意取得
制裁	—	—	・制裁金の対象。

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

2. GDPR への対応策

GDPR の内容に該当する場合、企業としての対応を進める必要がある。特長として、条文は組織と外部（個人データの本人、企業の対応責任、監督機関、社会など）との関わりについて重点が置かれた規則になっている。組織が、組織内でマネジメントシステムをどの様に構築するのかについては、記述の対象になっていない。データの海外（域外）への移転が大きなテーマで、莫大な制裁金を科すことを規定している。データ移転の詳細な規程、取扱いの法的根拠（同意書など）の要求、PIAの実施要求など説明責任に重点が置かれていることが特徴といえる。これらについて、対象企業から見ると対応すべき規則の内容が具体的に分かりにくいことが懸念される。

2. 1. 対応策に向けての考え方

GDPR で要求されている内容に対して取るべき対応策を以下のように考えることにします。

①対象となる企業は日本に帰属することから、先ず我が国の「個人情報保護法」を確実に遵守している必要がある。

②そのため、現時点では、「PMS」、「ISMS」の認証制度を受審して、客観的であり第三者的な観点からの保証を取得しておくことが有効と考えます。

③「PMS」、「ISMS」の認証を取得する方法は別途ご相談ください。

④ただし認証取得した上でも幾つかの課題があります。

◆「EU 域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」への対応について、 2019 年 1 月 23 日、個人情報保護委員会より発表がありましたとおり、日本も“十分性認定”を受けることになり、日本国内法「個人情報保護法」と「補完的ルール」を遵守すれば、EU 域内の事業者から個人データの移転を受けることが可能となりました。

◆従って「PMS」、「ISMS」の認証取得時に「個人情報保護法」と「補完的ルール」を遵守していることが保証されていることが条件です。

◆Pマークの審査においては、EU 域内から十分性認定により移転を受けた個人データを取扱う事業者は、補完的ルールの遵守が必要になります。対象になる場合に審査では「十分性認定に関する補完的ルール」への適合状況を H31 年 1 月から確認している。事業者はその項目に対応をする必要がある。

◆このためには「PMS」、「ISMS」の認証機関による保証の声明が公表されていなければならないと考えます。

⑤上記の考え方以外に、「3. 対象企業の内、どのパターンか」の観点に従って、EU 域内事業所と日本国内事業所の取るべき主要な対応を紹介します。

2. 2. EU 域内事業所での対策

日本の企業として EU 域内事業所に関して次の事項を実施する。

①法令ではGDPR遵守する「方針」を打ち出す。

②認定では「PMS」又は「ISMS」の認証を取得する。

③同意では

・データ主体からの同意書の取得

・データ主体からの同意書の取得済確認

・データ主体からの移転の同意取得

④制裁では制裁金の目的の理解と周知徹底

2. 3. 日本国内事業所での対策

日本国内の事業所に関して次の事項を実施する。

①法令では「個人情報保護法」と「補完的ルール」を遵守する「方針」を打ち出す。

②認定では「PMS」又は「ISMS」の認証を取得する。

③同意では

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

・EU 域内の事業所が同意書の取得済確認
・データ主体からの同意書の取得
④制裁では
・制裁金は受けないが、契約の関係に基づき影響を受ける。
・日本国内の法制度に従う。
・制裁金の対象となったときの対応のシミュレーション

2．4．補完的ルールへの対応

個人情報保護委員会が補完的ルール「EU 域内から十分性認定により移転を受けた個人データの取扱い編」を公開している。また、個人情報保護委員会では、日本の十分性認定に向け、補完的ルールを 2018 年 4 月 25 日にパブリックコメントに付していたが、その結果がまとまり 8 月 24 日に公表された。内容は、大きく次の 5 点についてである。

①要配慮個人情報（法第 2 条第 3 項関係）
②保有個人データ（法第 2 条第 7 項関係）
③利用目的の特定、利用目的による制限（法第 15 条第 1 項・法第 16 条第 1 項・法第 26 条第 1 項・第 3 項関係）
④外国にある第三者への提供の制限（法第 24 条・規則第 11 条の 2 関係）
⑤匿名加工情報（法第 2 条第 9 項・法第 36 条第 1 項第 2 項関係）。

なお、欧州委員会司法総局からの示唆により、EU域内の関係者に容易に理解できるよう、本案の表題を「個人情報の保護に関する法律に係るEU域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」に修正したとのことである。

また、本補完的ルールは、欧州委員会が日本の十分性決定が効力を生ずる日（2019年1月 23 日、日本と EU 間で十分性認定が発効）から施行することになる。補完的ルールの公開資料の別紙2には、寄せられた意見に対する個人情報保護委員会の見解が示されており理解の参考になる。

個人情報の保護に関する法律に係るEU域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール
https://www.ppc.go.jp/files/pdf/Supplementary_Rules.pdf

2．5．標準的契約条項の利用

2018 年 5 月 25 日から適用が開始される EU の「一般データ保護規則（General Data Protection Regulation：GDPR）」では、EEA 内から日本を含む EEA 外への個人データの移転は原則として違法とされるが、データ輸出者とデータ輸入者との間で標準的契約条項（Standard contractual clauses：SCC）を締結することが、移転が適法と認められるためのひとつの手段とされている。

SCC のひな型として欧州委員会が公開している 3 つの資料（仮訳したもの）のダウンロード先：
https://www.jetro.go.jp/world/reports/2018/01/8d894f365ea5c3a7.html
欧州委員会決定 2001/497/EC（Commission Decision 2001/497/EC ）
欧州委員会決定 C（2004）5271 （Commission Decision C(2004)5271）
欧州委員会決定 C(2010)593（Commission Decision C(2010)593）

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

3. 制裁金の仕組み

3. 1. 制裁金に関する規定

制裁金は、各監督機関が科すものであり、そのきっかけには、①顧客の苦情、②個人データの漏えい、③データ処理での違反、④データ移転での違反が考えられる。GDPR の第 58 条で監督機関の権限として制裁金が規定され、第 83 条で制裁対象が規定されている。

制裁金の額を判定する要素として、①事業者(組織体)が個人データを扱う際に対応すべきと GDPR が規定した以下の対処が実現されていないこと、②またその結果、個人データの侵害が発生し、個人データ本人に損害が及ぶこと、などである。制裁金を理解しやすいよう表Ⅲ－1でそれを示す。

なお、制裁金と表現しているが、警告、懲戒、命令、取扱い禁止などの措置も第 58 条2に含まれている。

表Ⅲ－１「制裁金に関わる GDPR 管理項目－事業者が行うべき対処」

	GDPR の仕組みへの対応(例)	個人データの取扱いへの対応(例)	備考
前提事項	＜1－1枠＞ ・個人情報保護方針の公開 ・管理者の指名(24 条) ・DPO の指名	＜1－2枠＞ ・個人データの漏れのない洗出し ・同意書を準備し取得する手順がある ・同意書は撤回する権利など明記し条件を満たしている(7 条)	
運用事項	＜2－1枠＞ ・個人データ侵害発生の 72 時間以内の報告(33 条、34 条) ・加盟国の国内法を遵守する(9 条) ・監督機関の命令等に違反していない((58 条 2) ・	＜2－2枠＞(欄外参考事項を参照) ◎データ保護原則の義務を遵守(総括) ・ﾃﾞｰﾀ主体から同意(目的を含む)を取得していること(6 条、7 条)(9 条) ・管理者は個人データ取得時に、必要な情報(目的を含む)を提供する(13 条) ・データ主体の権利に対する対応不足・誤り(12 条~22 条)がないこと ・リスクに応じた取扱いの安全性を確保する(32 条)(安全性を確保しても発生した侵害あり) 個人データの漏えい他の侵害の発生なし ・個人データの移転の条件を遵守している(44 条～49 条)	「データ保護原則の遵守」は総括的な表現 ＊詳細は別紙「制裁金に関する 83 条記述（4a、5a、5b，5c、5d)」参照
共通事項	＜3－1枠＞ ・侵害行為が故意 or 過失か(故意の侵害は論外) ・管理者・処理者が講じた軽減措置 ・管理者・処理者の責任程度	＜3－1枠＞ ・過去の措置命令の遵守状況 ・管理者・処理者の過去の違反	＜3－1枠＞は評価時の考慮事項である

ここで上記の内容は制裁金の軽重の判断材料であるが、枠は、次の意味をもつ。
＜1－1枠＞:個人情報保護のマネジメントシステムとして、必要な仕組み。個人データ取得前に対応可能な事項
＜1－2枠＞:個人データを取扱うことに関して、あらかじめ準備する、対応することが可能な仕組み事項
＜2－1枠＞:個人データの取扱う際に、実施する仕組みを用意して運用にあたる事項
＜2－2枠＞:個人データの取扱う際に、日々の運用で実現させる事項
＜3－1枠＞:マネジメントシステムの運用にあたって、発生する状況であり、制裁金の軽重の評価項目
上記色付の□＜2－2枠＞は、顧客の個人データの侵害を発生させ、顧客に損害を与えることに関する項目の区分けである。事業者が一番注力するべき部分と考える。

3. 2. GDPR が制裁金を科す原則

制裁金を科す狙いとして、次の原則をうたっている(第 83 条、第 58 条、第 70 条、ガイドライン)

①均等な制裁(一貫性)　　GDPR 全体を通じた考え方
②効果的、比例的かつ抑止的　　第 83 条 1 項、ガイドライン
③個々の事案の事情に応じて評価　　第 83 条、ガイドライン
④制裁金　調和のとれたアプローチ　　ガイドライン

3. 3. GDPR の制裁金の評価

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

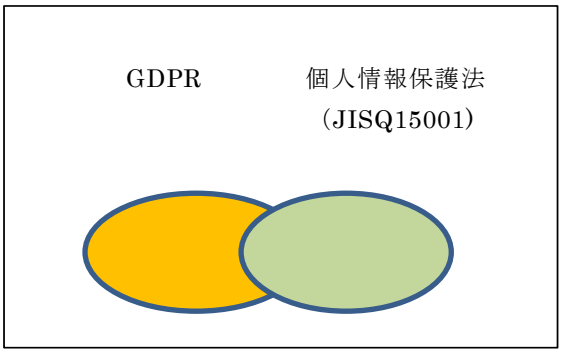
制裁金は制裁金の上限を定めて、違反の性質により、違反を第 83 条 2 項の評価基準 a)～k)により評価する。
制裁金の狙いは懲罰的な意味というより、(きれいごとの表現だが)是正措置を通じて、法令順守の回復を図る狙いがあり、監督機関には、そのための最適な手段を選択することが義務付けられる。

表Ⅲ－2:評価基準のあらまし(第 83 条 2 項から抽出)

	項目	制裁金額を評価する際の考慮の内容
a)	違反の性質、重大さ及び期間	制裁金の代わりに注意処分を行う場合がある
b)	違反の故意又は過失	違反が過失によるものか、故意によるものか(故意は重大)
c)	損失低減のための措置	データ主体の損失軽減のために管理者、処理者が講じた措置
d)	管理者、処理者の責任の程度	個人情報保護バイデザインや、安全管理などで実装した措置を考慮した、管理者、処理者の責任
e)	管理者、処理者による過去の違反	管理者、処理者による過去の違反
f)	悪影響低減のための監督機関との協力	違反の解消、違反の悪影響低減のための、監督機関との協力の程度
g)	影響を受ける個人データの種類	関係する個人データの種類(重大な侵害をもたらすものか、否か)
h)	違反を通知したか	監督機関が違反を知ることになった態様、事業者による通知であるか否か
i)	事前に命令された措置への対策の遵守	同じ事項に関して過去に命じられた措置が遵守されているか、状況
j)	行動規範、認証メカニズムの固守	管理者の団体や組織が定める行動規範、承認されたデータ保護マークの認証取得方法を遵守しているか
k)	違反から得られた利益、損失	違反行為による直接、間接の利益、若しくは回避された損失などの要素

研究部会としてのコメント
GDPR 規則は、正面から適切な保護の取扱いに向き合う必要があることを求めている。(当然であるが)
企業としては、PMS、ISMS の認定遵守にまじめに取り組むこと。更に GDPR 対応として追加する点(図Ⅲの橙色部分)については留意する。

図Ⅲ　個人情報保護法の対応範囲と、GDPR の対応範囲



©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

4. GDPRの違反可能性チェックリスト

GDPR におけるプライバシー違反時の対応は次のように定められています。

表Ⅳ－1　GDPR における侵害発生時の対応要求

	GRPR の特徴	日本企業としての対応
侵害発生時の対応	プライバシー違反時の報告が義務化され、侵害を認識してから可能な 72 時間以内に GDPR の管轄監督機関への報告が必要である。(第 33 条)	万が一、データ侵害が発生した際には、その事実を検知して適切な対応ができるようにする体制が必要である。例えば GDPR の管轄監督機関との窓口となる「DPO」(Data Protection Officer)を選任し、その氏名と連絡先を明示する。※個人情報保護法では、事故時の個人情報保護委員会等への速やかな報告は努力義務であり、マイナンバーについてのみ、特定個人情報の安全の確保に係る「重大な事態」が生じたときに、個人情報保護委員会に報告することが法令上の義務である。

4. 1違反可能性チェック

GDPR は世界で最も厳しいデータ保護規則の 1 つと見なされており、EU 市民の個人データを一貫して保護することを目的としています。この規則により、EU 市民のデータをインタラクティブに操作および保管するすべての組織には、違反時に制裁金が科されることになります。このため、違反可能性チェックリスト(違反深刻度評価)を作成したので、転ばぬ先の杖と考えて、チッェクしてみてください。

表Ⅳ－2　違反可能性チェックリスト(違反深刻度評価)

No	チェック項目	チェック内容	GDPR 条文	判断の結果	注
1	同意書	同意目的は「具体的、かつ十分な情報開示に基いており、明確でわかりやすく表示されているか	6.4		1-2 2-2
2	記録	この同意書に基づいて同意を取った記録が残してあるか	7		2-2
3	廃棄	同意書のない個人データは適切に廃棄されているか			2-2
4	変更	同意目的が変更された場合は速やかに、新しい同意を得ているか			2-2
5	撤回	同意の撤回が、同意をしたときと同様に簡単にいつでも可能であることを確保しているか、実施できているか	17		1-2 2-1
6	個人データの侵害	個人データの侵害が発生していないか 個人データの侵害が発生する可能性の状況にもない	多数		2-2
7	侵害発覚時の対処	個人データの侵害発覚から 72 時間以内に日本の個人情報保護委員会と EU の当局に通知しなければならない	33		2-1
8	管理者	管理者責任が強化され、仮に外注先(処理者)でのミスが原因で情報流出が発生していないか。あればそのデータを委託している「管理者」も GDPR 違反に問われます。	24		1-1 2-1
9	Cookie	「Cookie および類似のテクノロジ」のセクションで、当社 が使用する Cookie に関する説明を明示している			1-1

注欄は、表Ⅲ－1の枠の位置づけを表示したもの。

上記の表は違反可能性チェックの大枠を示したもので、GDPR 条文での最終的な確認をする場合は下記リストを参照する。

表Ⅳ－3　違反可能性　評価チェックリスト

No	チェック項目	チェック内容		判断の結果	備考
	GDPR 条文	項目	評価事項		
1	83 条 2 58 条 2 a)～h)、j)に規定する是正権限の措置に加えて、又は代えて	58 条 2　a)～k)の規定項目: a)違反行為の性質、重大性、持続期間、被害の人数、損害の程度。b)違反行為の故意または過失。c)損失の軽減のための措置。d)管理	個人データ侵害に関する左記内容の状況により制裁金を判断される 個人情報保護に関して組織の行う努力が評価され、制裁金の		

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

	制裁金を科す。制裁金を科す判断、額の判断においての考慮事項 a)～k)に規定	者又は処理者の責任の程度。e)管理者又は処理者の過去の違反。f)違反解消のための監督機関との協力。g)違反の個人データ種類。h)違反が判明した経緯。i)過去の経緯。j)行動規範の遵守。k)その他の要素。	低減に反映される。努力は見えるように(記録を残して)実施しているか		
2	83 条4 管理者及び処理者の義務 8 条、11 条、25 条～39 条、による	左記各条の義務に違反することがない行為を実施する必要がある。	遵守しているか (以下に個別に展開)		
3	8 条 情報社会サービスとの関係において子供の同意に適用される要件	対象となる子供の要件。子どもからの同意取得要件	・親権者などからきちんと同意を取得しているか		
4	25 条 データ保護バイデザイン及びデータ保護バイデフォルト	・データ保護義務のための(仮名化のような)技術的・組織的措置を実装する。必要なデータのみが取り扱われる措置を実装する	実装し機能させているか		
5	26 条 共同管理者	定義。ﾃﾞｰﾀ主体の権利保証 共同利用責任の明確化	遵守しているか		
6	28 条処理者	管理者が処理者に個人データを取り扱わせる条件、処理者の管理者との取扱いの契約等	遵守しているか		
7	29 条 管理者又は処理者の権限下での取扱い	個人データのアクセス者は管理者からの指示がない限り取扱いは不可	遵守しているか		
8	30 条 取扱い活動の記録	記録すべき項目の列挙	遵守しているか (注)中小零細企業への適用例外(記録免除)あり		
9	31 条 監督機関との協力	管理者、処理者の職務遂行で監督機関との協力を要す	遵守しているか		
10	32 条 取扱いの安全性(4－2安全性)	安全措置の実装 仮名化暗号化／機密性完全性可用性、回復	安全性を確保しているか		
11	33 条 監督機関に対する個人データ侵害の通知	管理者、処理者の義務内容	遵守しているか		
12	34 条 データ主体に対する個人データ侵害の連絡	ﾃﾞｰﾀ主体に対する侵害の連絡	遵守しているか		
13	35 条 データ保護影響評価 DPIA＝データ保護影響調査	管理者による評価を要す。また、その実施方法。監督機関の措置。評価の内容。新たな技術採用時にリスク発生の恐れに対して実施	必要に応じて(リスクが高い個人データ処理の場合)DPIA を実施し評価を実施しているか		
14	83 条4 制裁金は1000 万ユーロ以下または売上総額2%以下	左の制裁金の対象として、83 条4a～83 条4c が該当する	―		
15	83 条4a 8 条、11 条、25 条～39 条、42 条、43 条	8 条子供の同意、11 条識別を要しない取扱い、25 条～39 条管理者、処理者による取扱い等、 ただ 43 条 43 条は認証機関な関するもので企業には該当しないと判断した	―		
16	83 条 5	83 条 5 は 83 条 4 より重い制裁。	⇒83 条 5a)～5e)項		

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

	違反制裁金の対象 制裁金区分:2000万ユーロ以下、売上総額4%以下	特に 5a)は簡単な記述であるが内容は広く重い。			
17	83条5a 同意、基本原則 同意の条件、基本原則 5条、6条、7条、9条 注 5条:適法であり、公正であり、透明性のある態様の取扱い。目的の限定、データの最小化、正確性、記録保存の制限、完全性及び機密性	5 条個人データの取扱いと関連する基本原則 6条取扱いの適法性 7条同意の要件 9 条特別な種類の個人データの取扱い (注)7条同意に関しては、当資料5項を参照	5 条の原則は、制裁金の評価に規則をどのようにでも適用できる表現。 基本原則の遵守しているか 同意の条件遵守として、ﾃﾞｰﾀ主体との約束を満たしているか		
18	83条5b ﾃﾞｰﾀ主体の権利 ﾃﾞｰﾀ主体の権利条項 12条～22条	ﾃﾞｰﾀ主体の権利条項として、透明性及び手順(12条)、情報及び個人データへのアクセス(13 条～15条)、訂正及び消去(16 条～20条)、異議を述べる権利及び個人に対する自動化された意思決定(21条、22条)を含む。	個人データの運用に関する規定事項である。実際運用において管理策の遵守しているか		
19	83条5c 個人データの移転 第三国内又は国際機関内の取得者に対する個人データの移転 44条～49条	以下の条項による規定 44条移転に関する一般原則 45条十分性認定に基づく移転 46適切な保護措置に従った移転 47条拘束的企業準則 48 条 EU 法によって認められない移転又は開示 49条特定の状況における例外	原則規定の遵守 個人データの移転により自然人の保護のレベルが低下しないことを確保できているか		
20	83条5d 9 条 加盟国の国内法	加盟国の国内法による義務を果たさないことが違反	国内法を遵守しているか		
21	83条5e 監督機関からの命令等 58 条 2 による監督機関からの命令、取扱の制限、停止の不服従、58条1に違反のアクセスの不提供	監督機関からの命令とは58条2に規定する是正権限への不服従 58条1の規定(監督機関の調査権限)に対するアクセスの不提供	状況確認、対応見直し 左記に相当する行為は制裁金に該当する		
22	83条6 58条2 監督機関からの命令、取扱の制限、停止の不服従等	監督機関からの命令とは58条2に規定する是正権限への不服従 2000 万ユーロ以下、(事業の場合)売上総額 4%以下の高額の制裁金	監督機関による命令に不服従は制裁金に該当する		
23	83条7～9 加盟国の制裁金法令の制定、法制度	権利行使は加盟国の国内法に従う	ー		
24	84条 制裁	加盟国は制裁に関する法整備をし、措置を講ずる。	ー		
25	前文146 管理者又は処理者の責務	管理者又は処理者は違反する取扱いの結果の損害の賠償をしなければならない	制裁金を科せられ評価される根拠となる		

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

26	前文 148 本規則の違反に対して制裁が加えられる	軽微な場合注意が与えられる、違反行為の性質、重大性、持続期間などを考慮	ー 制裁金を科せられる根拠となる		

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

5. 同意書の重要さ

5. 1. 同意と同意書の位置づけ

GDPR の定義(第 4 条)では、データ主体の「同意」とは、自由に与えられ、特定され、事前に説明を受けた上での、不明瞭ではない、データ主体の意思の表示を意味し、それによって、データ主体が、その陳述又は明確な積極的行為により、自身に関連する個人データの取扱いの同意を表明するものを意味する、としている。

また、個人データを GDPR で規定した明確な法的根拠が適用される場合にのみ、取り扱いを適法としている(第 6 条)。その中で個人情報を取扱う有効な法的根拠として同意を表明する文書:同意書を位置付けている。

同意について、条文第 7 条で次を規定している。

表Ｖ－１　GDPR の同意に関する条文（第 7 条を（抜き書き）示す）

No	GDPR 条文	同意についての規則　　記述内容 （抜き書き）
1	第 7 条 同意の要件	1. 取扱いが同意に基づく場合に、管理者は、ﾃﾞｰﾀ主体が自己の個人データの取扱いに同意していることを証明
2		2. 同意の要求は、別の事項と明確に区別でき、理解しやすく容易にアクセスできる方法で、明確かつ平易な文言を用いて、表示されなければならない
3		3. ﾃﾞｰﾀ主体は、自己の同意を、いつでも、撤回する権利を有する。 同意の撤回は、同意を与えるのと同じように、容易なものでなければならない
4		4. 同意が自由に与えられたか否かを判断する場合、契約の履行に必要のない個人データの取扱いの同意を契約の条件としているか否か、が重要

企業は同意書によってデータ主体から個人データ取得の同意を得ることが重要となる。当然、個人データの取扱いの目的に応じて同意書を GDPR に適合した表現にする必要がある。上記表Ｖ－1には同意の要件が規程され、同意の定義は冒頭に記載しているが、その具体的な記述については、「同意に関するガイドライン」が公表されているので、それを基に GDPR において同意書が満たすべき要件を、検討した。

同意書の運用に関する留意事項は以下のとおりである。

①同意目的は「具体的、かつ十分な情報開示に基いており、明確でわかりやすく表示されているか

②この同意書に基づいて同意を取った記録があるか

③同意書のない個人データは適切に廃棄されているか

④同意目的が変更された場合は速やかに、新しい同意を得ているか

⑤同意の撤回が、同意をしたときと同様に簡単にいつでも可能であることを確保しているか

「同意に関するガイドライン」に記述されている内容を見ると、同意に関する解説と、同意で満たさなければならない事項が読み取れる。これらをガイドラインの項目で展開した。

同意書で同意を必要とする内容は、日本の企業が現時点で個人情報保護方針やプライバシーポリシー等によって記述している内容と、GDPR で要求する内容が異なる。

実際の同意書の記載内容に関する留意事項は以下のとおりである。

表Ｖ－２　同意のガイドラインと同意の留意事項

網掛け部分：同意書で表現する内容への要求事項。右欄に〇記載で表示

No	同意ガイドライン 番号	ガイドライン項目 小見出し	ガイドラインの記述内容を想起する記述 (ガイドラインの記述の一部抜き書き) ガイドラインの内容の要約ではない(要約はできない)	GDPR との対応 条項: 〇条 前文: 〇項	ﾎﾟﾘｼｰへの要求事項 要求 ｶﾞｲﾄﾞﾗｲﾝの事例番号

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

1	1	はじめに 同意の概念について詳細な分析 同意が適切な法的根拠となる条件 データ主体が自分の同意を制御	実用的なガイダンス 同意はデータ主体のデータを取扱う根拠の一つ。同意書は支配権限をデータ主体に与えるツール。(支配権限をデータ主体に与えるツールでなければ違法) データ主体が不利益を被らずに拒否でき、支配権限をデータ主体に与える	5 条	解説
2	2	GDPR 第 4 条(11)における同意 同意を定義している	定義を満たす同意は個人データの取扱いが基礎にしなければならない法的根拠の一つ。 第 7 条及び前文第 32 項、第 33 項、第 42 項、第 43 項追加 同意の撤回について:データ主体に一定程度の支配権限が残されている 同意はデータ主体が撤回可能な判断であること	4 条 (11)	解説
3	3	有効な同意の要素	①自由に与えられ②特定され③説明を受けた④不明瞭でない⑤データ主体の意思の表示		解説
4	3.1	自由 / 自由に与えられた	データ主体に真の選択と支配権限がある 撤回できない場合は自由ではない		○ 事例1
5	3.1.1	力の不均衡、管理者が「公的機関」である場合	公的機関の活動によるものは力の不均衡があり、同意に依拠できそうにない。承諾に代わる代案はないが、他の法的根拠があり、適切であると考える	4 項	○ 事例2 ～4
6	3.1.1	雇用の場(職場)での監視カメラによるモニター導入	雇用条件、何らかの同意圧力を感ぜずに不同意にできることは少ない。この同意を根拠として使うのは問題あり		○ 事例 5
7	3.1.1	同意しない場合	同意しない場合に(＝場合であっても)ごまかし、脅迫、強制又は重大なネガティブな結果を受けない場合に、同意は有効である		○
8	3.1.2	条件性	契約条件の承諾と同意の「抱き合わせる」 同意と契約を融合させて曖昧にできるものではない	7(4)	○
9	3.1.2	この場合「契約の履行に必要な」は、厳密に解釈することを要す	オンラインで購入された商品が配達できるようにデータ主体の住所を取り扱うこと、又は支払いを迅速化するためにクレジット・カードの内容を取り扱うこと	7(4)	○
10	3.1.2	抱き合わせの評価	賃金支払いのために給与の情報と銀行口座内容を取り扱うことは容認できる ＊10	7(4) 43 項	事例 6 ○
11	3.1.2	追加目的のための個人データ利用についての同意を含んだサービス	左のサービスと同等のサービスを本人の同意なしに提供すれば、管理者は選択肢を提供していると主張できる		○
12	3.1.3	粒度	一つの業務で複数の目的がある場合の同意	ー	解説
13	3.1.3	サービスが複数の目的のためにいくつもの取扱業務を行う	ひとまとまりの取扱いの目的に同意しなければならないのではなく、 取扱いが複数の目的をもつ場合、同意は、それらの全ての目的に対して与えられなければならない		○ 事例 7
14	3.1.4	不利益	管理者は同意を不利益無しで拒否又は撤回できることを示す必要がある その同意撤回により明確な不利がないことを証明する必要があ	42 項	○ 事例 8 ～10
15	3.2	特定の ＜内容をはっきり理解できない、分らない＞	機能の隠れた拡張(function creep)に対する保護措置としての目的の詳述 同意要求についての粒度、また データ取扱活動についての同意取得に関係した情報を、他の事項についての情報から、明確に分離すること	6 条(1) (a)	解説 事例 11
16	3.2	特定の	同意のメカニズムは、「自由」の要件、各目的に		解説？

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

			ついて個別のオプトインを提供すべき		
17	3.3	説明を受けた	同意の取得に先立ってデータ主体に情報を提供し、データ主体が何について承諾しているかを理解できるようにすること 同意を撤回する権利を行使できるようにするため	5 条 6 条	○
18	3.3.1	同意が「説明を受けた」上でのものとなる最小限の要件 第 29 条(作業部会の見解)では 右は、データ主体が選択を行うために提供すべき要素である、とする	「説明を受けた」の最小限の要件 (ⅰ)管理者の身元 (ⅱ)同意が求められるそれぞれの取扱業務の目的 (ⅲ)収集され利用されるデータ(そのタイプ) (ⅳ)同意を撤回する権利の存在 (ⅴ)関連する場合、第 22 条(2)(c)に従い自動化された意思決定のためのデータ利用についての情報 (ⅵ)十分性認定及び第 46 条で述べられる適切な保護措置がないことによるデータ移転で起こりうるリスク について	13 条 14 条 22 条 46 条	○
19	3.3.2	情報を提供する在り方	同意という要件を満たす書式又は形式を規定していない 「説明を受けた」の要件について記述あり 法律家だけでなく標準的な人にも容易に理解できるようにすべきことを意味 明確かつ平易な用語で説明 管理者がだれか データ取扱いの目的を明確にする 同意が電子的手段の場合 明確かつ簡潔要す	13 条 14 条 7 条(2) 32 項	○
20	3.3.2	ターゲットにする人々に未成年のデータ主体が含まれる場合	ターゲットにする人々を確認した後、管理者はどのような情報を提供すべきか、またそれに続いてどのようにデータ主体に情報を提示するかを決定 子どもの場合、平易な表現のこと		○
21	3.3.2	同意が(紙の)契約書の一部として要求される場合	同意の問題ははっきり目立った形で又は別の文書で扱われるべきである		○
22	3.3.2	同意が電子的な手段によって求められる場合	同意の要求は分離され区別されたもの		○ 事例 12 事例 13
23	3.4	不明瞭でない意思表示 同意の明確化	・同意したことが明らかでなければならない。 ・不明瞭でない意思の表示 ・データ主体の同意意思が明らか(チェック入りボックスは不可)	4 条(11) 7 条 32 項	○ 事例 14 ～16
24	4.	明示的な同意の取得 明示的な同意	・明示的な同意は、重大なデータ保護のリスクが出現する状況において必要 ・書面の同意など(電子的方法もあり限定ではないが)。2 段階の同意もよい ・“明示的な”は同意が表現される方法にも係る	9条 49 条 22 条	○ 事例 17 ～20
25	5.	有効な同意に必要な追加的条件	・同意の記録を取ること、データ主体が同意を容易に撤回する権利を持つ ・これは 8 条(子ども)、9 条(特別な・・)にも適用される	7 条 8 条 9 条	○
26	5．1	同意の証明	・同意を証明するのは管理者側の義務 (同意取得を証明できないデータは使用できない、廃棄すべきと考える) (廃棄する指示と考えるべきか？)	7条(1) 42 項	解説
27	5．1	最低限の収集	・必要以上に多くの情報を収集すべきではない。 (注)3.1. 2 項の抱き合わせの評価と内容が重なる。	5条(c)	○
28	5．1	同意の証拠保持	・取り扱いが終了した後も、同意の証拠は保持すべき。	17 条 3 (b)17 条	解説 事例 21

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

			・GDPR では同意がどのくらい期間継続するか、特定の期間を示していない	3(e)	
29	5．2 ＊7	同意の撤回 同意の容易な撤回 消去要求の無い場合の評価 取り扱い変更の通知	・同意の撤回が、同意をしたときと同様に簡単にいつでも可能であることを確保する。 ・不利益を被ることなく同意を撤回できること。 ・消去要求の無い場合でも、問題のデータの取り扱いが適切かを評価しなければならない。 ・取り扱いについての法的根拠の変更は、データ主体に通知されなければならない。	7条(3) 13 条 14 条	○ 事例 22
30	6	同意と GDPR 第 6 条(適法性)における他の法的根拠との関係 (適法なデータの取扱いの条件)	適法なデータの取扱いの条件 6 件の法的根拠(同意、ﾃﾞｰﾀ主体の契約履行、管理者の法的義務、生命に関する利益を保護、管理者に与えられた職務の遂行、正当な利益の目的のために必要) 取扱の根拠を“同意”とすれば、同意を撤回した時はその取扱いを中止できるように用意する 管理者は同意を他の法的根拠に置き換えることはできない	6 条	
31	7	GDPR における特定の問題領域	GDPR は立場の弱い自然人(特に子ども)に追加的保護レイヤーを設けている		○
32	7．1	子ども(第 8 条) (8 条の適用)	GDPR は立場の弱い自然人(特に子ども)に追加的保護レイヤーを設けている。子どもに関する個人データの収集も対象に含む 年齢に関する議論がある 同意のためには、子供に対して明快で平易な文言で説明	8 条 38 項	○
33	7.1．1	情報社会サービス	「情報社会サービス」の定義 オンライン締結され、又は伝送された契約及びその他のサービスを含む。 商品の物理的配達又は物流の要素は含まない	4 条(25)	解説
34	7.1．2	子供に対する直接の提供	定義 8 条は「情報社会サービスの一部に適用される」意味	8 条	？適用不明
35	7.1．3	年齢	加盟国は 13 歳を下回らない限り、子どもの年齢を定めることができる 子どもであることの適切なチェック 親権の保有者であることの証明	8 条	○ 適用
36	7.1.4	子供の同意と親の責任 未成年への措置 未成年が成年に達した場合	親であることの確認におけるリスク 適切な措置は管理者の責任 同意の扱い	7 条	○ 適用 事例 23
37	7.2	科学研究	科学的研究の定義 GDPR にはない 望ましい慣行に従う 匿名化は個人データの取扱いなしに研究が実現できるときは望ましい 透明性は特定の同意を認める状態にない場合、保護措置となる 同意が取扱いの法的根拠である場合、同意の撤回は原則ただちに個人データを消去しなければならない	6 条 89 条 9 条(2) 33 項	解説
38	7.3	ﾃﾞｰﾀ主体の権利	同意が取扱いの法的根拠である場合、個人の権利に影響するデータポータビリティの権利を持ちうる	20 条	○
39	7.3	ﾃﾞｰﾀ主体の権利 (撤回)	同意が撤回されたとき、訂正及び消去の権利がある	16 条 17 条 18 条 19 条 20 条	不適用
40	8	指令 45/46/EC により取得された同意	既存の同意の全てを更新することを求めていない。これまでの同意も GDPR の条件に沿ってい		解説

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

			れば有効である。管理者が有効な同意を得たことを証明できなければ、更新が必要。チェックボックスに予めチェックが入ったものによる同意はGDPR の基準を満たさない。		
41			同意の法的根拠を別の法的根拠に置き換えることはできない 管理者は、適法であり、公正であり、かつ透明性のある取扱いの原則を遵守する必要がある	13 条 14 条	解説

表Ｖ－2　注記

＊1:利用は自由意思に基づくものであるので、強制とは言えない。ただし、利用したいものと抱き合わせになっているので、サービスで不要のものがあっても便利さとの引き換えで承知するしかないものがある。便利さとのバランスで判断することになる。（この解釈で良いのか？）

＊2:プライバシーポリシーを印刷した場合のページと項目見出しを表示する。

＊3:利用規約を印刷した場合のページと項目見出しを表示する。

＊4:個人情報保護方針は、方針項番、個人情報保護への取り組みはページと項目番号を表示する。

＊6:「個人情報保護方針」「個人情報の取扱いについて」

＊7(5.2 項):撤回と情報の開示とは異なるので、下線部が有効であることは「不利益を被ることなく同意撤回」には反しない。
本人確認の書類（住民票、運転免許証などのコピー）は必要である、は当然。

＊8:(3.1 項)同意の撤回と個人情報の削除とは、意味が同じようで異なる。ここでは同一とみなした。

＊10:サービス提供に伴う、契約の履行に必要のない個人データの取扱いの同意を求めることについて
企業には取扱うデータ項目を増やして、多くのデータ項目を正当に集めることができるようにして、自社に有利にするようとする狙いがある。そのため、企業は「データ主体に様々なサービスを提供するとして、その契約の履行に必要な情報であることを主張したい。」と働きかけている。

＊5、9:欠番

5. 2. 同意書上の表現

ガイドラインの、同意文に関する“要求事項”について、研究会では、上記表Ｖ－2により、いくつかの企業の例（グーグルジャパン、Facebook、ジャパネットたかた、オリオンツアー、ショップジャパン）についてプライバシーポリシー、個人情報保護方針などで実際にどのような表現がなされているか、項目ごと対比で調査した。＜注:現在この別紙は、内容が詰め切れておらず、成果物集に収録していない。＞

その表現は、ガイドラインの項目ごとに個別の（1）収集する個人データ項目と、利用目的の対応は、どの企業においても、個人データのいくつかをくくりで利用目的を記述している。利用目的を 1 つ 1 つ分けて記述することは利用者に取り分り易いか、便利か検討の余地がある。ただ、規則をそのまま読むと、そのように細かく記述するべきと読める。しかし、利用者の立場からそれが便宜を図られたものであるかどうか、検討の余地がある。

5. 3. 多種類の個人データ項目の取得

GDPR では、「契約の履行のために取扱いが必要となる場合」は、個人データを正当に取扱える根拠(6 条 1 項)となる。事業者は正当な法的根拠の下で多くの種類の個人データを、多くの者から収集して、情報保有で優位に立つことを考えているので、利用者に多くのサービスメニューを提示し、それについて同意を得るようにしている。Google やFacebook、通販企業、Web サービス企業などのプライバシーポリシーでは、利用者に便宜を図る多くのサービスを提供しているが、その背景には、多くの利用目的をサービスメニューの契約に含め同意を得て、多種類の個人データ項目を取得し扱えるようにしていることがある。これは法的根拠としては、同意の取得と正当な利益のためが該当するようである。5.2 項の企業の意図である。

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

6. PMSやISMSの内容を強化

6．1　GDPRと日本の個人情報保護法との関係

「EU 域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」への対応について 2019 年 1 月 23 日、個人情報保護委員会より発表がありましたとおり、この度、日本も“十分性認定”を受けることになり、日本国内法と「補完的ルール」を遵守すれば、EU 域内の事業者から個人データの移転を受けることが可能となりました。

これを受け、EU 域内から十分性認定により移転を受けた個人データを取扱う事業者は、個人情報保護法に加え、「補完的ルール」の遵守が必要となります。

○十分性認定に関する補完的ルールへの対応について

⇒ https://privacymark.jp/system/operation/suppl_rules/index.html

⇒ https://www.ppc.go.jp/files/pdf/310118_siryou1-1_betten2.pdf

⇒ https://www.ppc.go.jp/files/pdf/310118_siryou1-2.pdf

第二十四条（外国にある第三者への提供の制限）

第七十八条（外国執行当局への情報提供）

6．2 「GDPR」と「個人情報保護法」との相違点

個人情報の取扱いにおいて、GDPRと個人情報保護法には内容に差がある。日本企業が GDPR 対応を考える際の主要な事項を表Ⅵ－1 に表わす。これはこれはイメージ図(図Ⅲ)の橙色の部分である。

表Ⅵ－1 「GDPR」と「個人情報保護法」との相違点

	項目	GDPR の内容	日本の企業が留意すべき事項	GDPR 条文
1	個人データの定義	個人データの定義の相違(GDPR では幅広い)	日本では意識されていない情報が個人情報保護の対象になる	4 条
2	取扱の適法性	個人情報の取扱いの適法性として法的根拠を明確に求める	根拠とするべき事項を認識し、記録などを残す等の対処をする	6 条
3	同意の重視	データ主体による同意は法的根拠の 1 つとして重視。同意の明確化、任意性、撤回などの要件が重要	同意があいまいな表現や同意の撤回が容易に行えないことは制裁要件になる	7 条
4	個人情報保護に関する権利	個人情報保護に関する権利項目が厳重に定められている	個人情報保護法の規定と比べると、項目は存在するが個々の内容で GDPR ではﾃﾞｰﾀ主体の権利が大きくなっている	12 条～20 条
5	説明責任は管理者の責任	管理者が遵守すべき義務を遵守しているとの説明責任は、管理者にある	管理者が説明責任を果たせよう、重要事項の記録を残すなどの措置を行う	24 条
6	プライバシーバイデザインの導入	デザインとデフォルトの考えを基本として保護のしくみを確立させる	PMS 構築の基本が、個人情報保護を実現するものになっていること	25 条
7	侵害発生時の届け出	個人データ侵害発生時の 72 時間以内の届け出の義務	侵害の状況把握のために記録を残し、侵害を発見した後の情報収集や報告方法を構築する	33 条
8	データ保護影響評価(DPIA)による評価	高いリスクの個人データの扱いの前にデータ保護影響評価(DPIA)による評価が必要	該当する扱いにおいては、DPIAを実施するか、それと同様のリスク分析を実施することと、それと同様の対策の検討をする	35 条
9	データ保護オフィサー(DPO)の指名	データ保護オフィサー(DPO)の指名	自社に取りDPOの必要性を確認し、それをどのように実現するか検討する	37 条～39 条
10	個人データの EU 域外への移転	個人データの EU 域外への移転に関する規制が決められた	まず自社の業務での該当状況を確認する	44 条～

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

11	第三国との十分性認定制度	第三国との十分性認定制度	EU からの移転個人データの処理に伴う条件を明らかに自然人対処する	45 条
12	高額な制裁金の仕組み	高額な制裁金の仕組み	高額な制裁金が科せられる項目を確認し、それらへの対策をMSとしてPMSに組み込む	83 条

6．3　GDPR とPマークとの関係

(1)PMS の見直し

P マークを取得した企業が、自社の個人情報保護マネジメントシステム(PMS)を見直しし、GDPR に対応したものとするために、PMS を構築したステップに沿って見直し、GDPR の必要な事項を取り込む対応を検討した。ここで紹介するPMS構築ステップは、「個人情報保護ﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑ導入・実践ガイドブック」　(一般財団法人日本情報経済社会推進協会　プライバシーマーク推進センター　編)の　“基本的なPMS構築のステップ(例示)”であり、それに基づいて表Ⅵ－１　「GDPR」と「個人情報保護法」との相違点を取り込んだものである。

なお、　PMS構築のステップは、ここにあげたステップに限定されないので、マネジメントシステム構築段階の内容に相応してGDPRの要求項目を、検討に含めて行えばよい。

表Ⅵ－２　PMS 構築ステップ＊において行う GDPR 対応の例

(個人情報保護法、JISQ15001 と GDPR の相違点対応)

PMS 構築のステップ　＊			このステップで行う GDPR への対応		
ステップ No	ステップの名称	ステップの内容	該当する GDPR の条文番号	対応する内容	チェック
ステップ1	個人情報保護の目的と方針を定める	個人情報保護方針と個人情報保護目的を確立する	データ保護方針 5	基本的考え方の確認 適法性、公正性、透明性、目的の限定、ﾃﾞｰﾀ最小化	
			データ保護オフィサーの任命 37-39	日本企業(ここでは中小企業)としては DPO が持つ機能を自社として既存の組織・規程の中で個人情報保護管理者などが果たすことができるか、検証し対処する	
			管理者、処理者の関与 24,28	GDPR の管理者、処理者に相当する者の業務遂行要件が日本企業で MS として規定されていること	
ステップ2	個人情報保護の目標を定める	個人情報保護目的を達成させるために、誰が、何を、いつまでに実現させるか指標を示す	取扱い 5	方針で述べられた考え方の基本事項が、PMS で実現できるように具体的に規定されていること、を確認する。特に説明責任が企業側にあることに留意する	
			処理者による取得 13,14,26	個人データの取得に際し、GDPR が要求する要件を PMS として規定して満たしているか。ここでは個人データのアクセス、訂正、消去、ポータビリティに留意する	
			データ保存 5,13,32,15	取扱いの法的根拠を明確にし、保存期間などを適正に規定し通知すること	
			ﾃﾞｰﾀ主体の権利 1,15,16,17,18,20	第 1 条の規定に基づき、データ主体の権利に関しての要件一訂正、消去(忘れられる権利)、ﾃﾞｰﾀﾎﾟｰﾀﾋﾞﾘﾃｨに留意して PMS に規定されていることを確認	
			データ影響評価 DPIA 35，36 基本的なプライバシー影響評価 (PIA) 運用に関する PIA	ある条件にある個人データの取扱いは、GDPR では DPIA を実施することを要求している。日本企業としてはこれに該当するか否か、該当する場合に、その求めるリスク評価など適正に実施する体制にしていることを確認する。	

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

ステップ3	保護の対象となる個人情報を特定する	個人情報の特定方法を定め、取扱の詳細分析を行い、管理台帳とする 個人情報を取扱いを業務フローで表す	説明責任 5,12,24,39,40	日本企業として EU 等の個人データを取扱うことに関して、管理者はﾃﾞｰﾀ主体に対して情報提供し、説明すること。ﾃﾞｰﾀ取扱いの責任者が明確になっており、これらが適正に運用されることが PMS で規定されていること。	
			個人データの明確化 1,4,5,(9,10)	個人データを明確にしていること。個人データの定義範囲が異なるので、留意する 個人データの特定と管理要件を明確にする	
			取扱い原則 5,6	データが必要以上でないこと、目的の限定、最小化、記録保存の制限などの条件が、PMS で満たされるようにすること。その説明責任を果たせること	
			同意の管理 7.8.9.17	同意が重要な位置づけになり、その内容、利用、取得の説明、特別な種類の場合、子供の場合について、PMS で適合しているようにする	
ステップ4	法令、国が定める指針その他の規範を特定する	特定した法令、国が定める指針その他の規範等を明確にする	説明責任 5,12,24,39,40	法令並びに GDPR の関連規程などに基づく運用を PMS で満たしていること	
			データ移転に対する規制への対応、十分性認定など 44,45,46～	第三国への個人データの移転について、原則、十分性認定による移転などの対応を定める	
ステップ5	個人情報保護リスクを認識し特定する	個人情報保護リスクを業務、個人情報、ライフサイクルごとに把握する	DPIA 35,36	実際の取扱いにおいて、DPIA を実施して保護対策を必要とするような場合に、取扱が評価され、関係機関と協議して運用されること	
ステップ6	個人情報保護リスクを分析し対策を検討する	個人情報保護リスクに対する対策を、人的、物理的、技術的面から検討し、リスク分析表、リスク優先順位、リスク対応策をまとめる	リスク対策 24-28	リスク対策の見直し(十分な検討を行ったか、内容を示せること) 、安全管理体制、共同利用の責任、データ移転に関する契約(SCC)の締結などの確認、記録保存と消去	
			リスク分析 35,36	安全確実なデータ保管 基本的なプライバシー影響評価(PIA) 運用に関する PIA	
ステップ7	個人情報保護リスク対応計画を策定する	実際の業務プロセスと結合した個人情報保護リスク対応計画を策定する	データ侵害の対応 33,34	監督機関へのデータ侵害発生時の通知、ﾃﾞｰﾀ主体へのデータ侵害発生時の連絡、対応	
			安全性確保 24-28	安全確実なデータの保管	
ステップ8	計画を具体化する（文書化し、システムを構築する）	資源を確保し、計画を文書化し、システムを構築する	同意の管理 7,8,9,17	同意取得の内容と取得の記録、説明の容易性、など(別項参照)	
			データの保存 5,6,13,32	目的限定の保存、データ主体への情報提供がより明確に運用されること	
			ﾃﾞｰﾀ主体の権利 1,16,17,18,20	法律、規定を遵守し、取扱を記録し保管することの徹底（PMS もこの点は同じ）	
			安全確実なデータの取扱い 24-28	安全性確保のリスク対応の具体化の組み込み	
			研修 28,29,39	法律、規定を遵守し、取扱を記録し保管することの徹底（PMS もこの点は同じ）	
			詳細な処理記録の維持 30	記録の要求項目は GDPR では広い	

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

（2）プライバシーマークの審査においては、「補完的ルール」の対象となる事業者については、当該事業者の個人情報保護マネジメントシステムが「補完的ルール」にも対応していることを確認する。

「補完的ルール」の対象となる事業者におかれましては、下記の JIPDEC 公表資料等に示す事項をご参照の上、ご対応をお願いします

補完的ルールの対象となるかご判断が難しい場合等、ご不明な点がありましたら、JIPDEC もしくは審査機関までご相談ください。

〇JIPDEC 公表資料「EU 域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」への対応について

⇒https://privacymark.jp/system/operation/suppl_rules/pdf/supplrules_kaisetsu_190122.pdf

日本の企業が GDPR に取り組む場合のステップは、PMS のアプローチで行った方法を再度 GDPR の対応事項を含めた内容でトレースする方法を検討し、表Ⅱ－2として掲載する。

6．4　GDPR とISMSとの関係（検討中）

GDPRに該当する企業のISMSでの対応は下表の要修正と要検討に基づいて追加の作業が必要となる。作業に当たるものには GDPR とISMS両方の要求事項を精査するスキルが要求される。

表Ⅵ－3　ISMSの要求に対する GDPR の追加対応の必要性の例

要求項目	要修正	要検討
1　適用範囲	◎	―
2　引用規格	―	〇
3　用語及び定義	◎	―
4.1　組織及びその状況の理解	―	◎
4.2　利害関係者のニーズ及び期待の理解	―	◎
4.3　情報セキュリティマネジメントシステムの適用範囲の決定	―	〇
4.4　情報セキュリテイマネジメントシステム	―	〇
5.1　リーダーシップ及びコミットメント	―	―
5.2　方針	―	―
5.3　組織の役割，責任及び権限	◎	―
6.1　リスク及び機会に対処する活動	―	―
6.1.1　一般	―	〇
6.1.2　情報セキュリティリスクアセスメント	◎	―
6.1.3　情報セキュリティリスク対応	◎	―
6.2　情報セキュリティ目的及びそれを達成するための計画策定	―	―
7.1　資源	―	〇
7.2　力量	〇	―
7.3　認識	◎	―
7.4　コミュニケーション	◎	―
7.5　文書化した情報	―	―
7.5.1　一般	―	―
7.5.2　作成及び更新	―	―
7.5.3　文書化した情報の管理	◎	―
8.1　運用の計画及び管理	―	―
8.2　情報セキュリティリスクアセスメント	◎	―
8.3　情報セキュリティリスク対応	◎	―
9.1　監視，測定，分析及び評価	◎	―
9.2　内部監査	◎	―
9.3　マネジメントレビュー	◎	―
10.1　不適合及び是正処置	―	〇
10.2　継続的改善	―	―
	―	―
A.5.1　情報セキュリティのための経営陣の方向性	◎	―
A.6.1　内部組織	◎	―
A.6.2　モバイル機器及びテレワーキング	―	〇
A.7.1　雇用前	―	〇
A.7.2　雇用期間中	―	〇
A.7.3　雇用の終了及び変更	―	―

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

A.8.1 資産に対する責任	◎	ー
A.8.2 情報分類	◎	ー
A.8,3 媒体の取扱い	ー	ー
A.9.1 アクセス制御に対する業務上の要求事項	◎	ー
A.9.2 利用者アクセスの管理	◎	ー
A.9.3 利用者の責任	ー	○
A.9.4 システム及びアプリケーションのアクセス制御	○	ー
A.10.1 暗号による管理策	ー	ー
A.11.1 セキュリティを保つべき領域	○	ー
A.11.2 装置	◎	ー
A.12.1 運用の手順及び責任	ー	ー
A.12.2 マルウェアからの保護	◎	ー
A.12.3 バックアップ	ー	○
A.12.4 ログ取得及び監視	○	ー
A.12.5 運用ソフトウェアの管理	ー	ー
A.12.6 技術的ぜい弱性管理	ー	ー
A.12.7 情報システムの監査に対する考慮事項	ー	ー
A.13.1 ネットワークセキュリティ管理	ー	ー
A.13.2 情報の転送	◎	ー
A.14.1 情報システムのセキュリティ要求事項	ー	ー
A.14.2 開発及びサポートプロセスにおけるセキュリティ	ー	ー
A.14.3 試験データ	ー	ー
A.15.1 供給者関係における情報セキュリティ	○	ー
A.15.2 供給者のサービス提供の管理	○	ー
A.16.1 情報セキュリティインシデントの管理及びその改善	◎	ー
A.17.1 情報セキュリティ継続	○	ー
A.17.2 冗長性	ー	ー
A.18.1 法的及び契約上の要求事項の順守	◎	ー
A.18.2 情報セキュリティ,のレビュー	○	ー

修正例

「A.13.2 情報の転送」で、「1．GDPRの対象企業チェックリスト(2)対象企業の内、どのパターンか」確定し、それにより各パターンの「観点」、「法令」、「認定」、「同意」、「制裁」の取るべき対策を選択しなければならない。

「A.16.1 情報セキュリティインシデントの管理及びその改善」で、プライバシー違反時の報告が義務化され、侵害を認識してから可能な 72 時間以内に GDPR の管轄監督機関への報告の追加等が必要となる。

「A.18.1 法的及び契約上の要求事項の順守」で情報セキュリティに関連する法的，規制又は契約上の義務に対する違反，及びセキュリティ上のあらゆる要求事項に対する違反を避けるため、要求事項の特定としては、最低限でも**参考資料**にある一般データ保護規則と補完ルールは選択しなければならない。

おわりに

GDPR 対応はITやSNSの普及に伴う管理・責任への要求です。この資料に従って対応を検討・実施をしてください。このような要求は今後ますます拡大していくものと思われますので、これを機会にグローバルな環境におけるルールについて企業として認識・習熟しておくことが望まれます。

また、更に理解を深めることをお考えの方は、下記の具体的な行動を実践することをお勧めします。

①「**参考資料**」の GDPR について、日本語仮訳を読むこと、

②同業他社の対応状況等、情報収集すること、

③もし違反した場合の自社のダメージ、制裁金をシミュレーションすること、

④疑問に答えてもらえる専門家との連絡網を構築すること

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

参考資料

個人情報保護委員会

個人情報の保護に関する法律（平成 15 年法律第 57 号）
https://www.ppc.go.jp/files/pdf/290530_personal_law.pdf
補完的ルール(個人情報の保護に関する法律に係るEU域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール(平成 30 年9月)
https://www.ppc.go.jp/files/pdf/Supplementary_Rules.pdf

EU 一般データ保護規則（GDPR） 原文・和訳

EU一般データ保護規則の関係文書の原文は英文で、その日本語訳として以下の組織が対応している。
個人情報保護委員会、https://www.ppc.go.jp/enforcement/cooperation/cooperation/GDPR/
GDPR について、日本語仮訳

文書名	ファイル名	頁
一般データ保護規則の前文（PDF：654KB）	gdpr-preface-ja.pdf	62
一般データ保護規則の条文（PDF：1230KB）	gdpr-provisions-ja.pdf	108
データポータビリティの権利に関するガイドライン（PDF：1105KB）	dataportability_guideline.pdf	43
データ保護オフィサー（DPO）に関するガイドライン（PDF：906KB）	dpo_guideline.pdf	54
管理者又は処理者の主監督機関を特定するためのガイドライン（PDF：596KB）	kanrisya_guideline.pdf	26
データ保護影響評価（DPIA）及び取扱いが 2016/679 規則の適用上、「高いリスクをもたらすことが予想される」か否かの判断に関するガイドライン（PDF：1152KB）	dpia_guideline.pdf	49
規則における制裁金の適用及び設定に関するガイドライン（PDF：304KB）	seisaikin_guideline.pdf	25
規則に基づく個人データ侵害通知に関するガイドライン（PDF：521KB）	tsuuchi_guideline.pdf	67
自動化された個人に対する意思決定とプロファイリングに関するガイドライン（PDF：493KB）	profiling_guideline.pdf	77
同意に関するガイドライン（PDF：487KB）	doui_guideline.pdf	71
透明性に関するガイドライン（PDF：573KB）	toumeisei_guideline.pdf	83
規則第 49 条の例外に関するガイドライン（PDF：427KB）	article49reigai_guideline.pdf	35
GDPR の地理的適用範囲（第 3 条）に関するガイドライン- 意見募集版	chiritekitekiyouhanni_guideline.pdf	52
Infographic（外部サイト（欧州委員会）） 日本語仮訳付 PDF（PDF：1090KB）（中小企業向けの、簡単にまとめられた GDPR 説明）	EC-Infographic.pdf	18
Fact Sheet ″Questions and Answers - Data protection reform package″（外部サイト（欧州委員会）） 日本語仮訳付 PDF（PDF：318KB）（GDPR によるデータ保護改革案についての質疑応答概略）	Factsheet-20170524QandA.pdf	18

GDPR 参考リンク、書籍集

GDPR 日本語訳、GDPR の原文、ハンドブック、ガイドラインの和訳 等
https://xn--gdpr-ev9g41r.net/reference/japanese.html

ハンドブック、ガイドライン

★「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック by JETRO
入門編
https://www.jetro.go.jp/ext_images/_Reports/01/dcfcebc8265a8943/20160084.pdf
実践編

©2019JSSAシステム監査学会－「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.

https://www.jetro.go.jp/ext_images/_Reports/01/76b450c94650862a/20170058.pdf
★「EU 一般データ保護規則(GDPR)」に関わる実務ハンドブック(第 29 条作業部会ガイドライン編) by JETRO
☆データ保護責任者
https://www.jetro.go.jp/ext_images/_Reports/01/28dd771ad2a2c020/20170094.pdf
☆データポータビリティの権利
https://www.jetro.go.jp/ext_images/_Reports/01/2d8d30044cc65583/20170096.pdf
☆管理者および処理者の主導監督当局の特定
https://www.jetro.go.jp/ext_images/_Reports/01/9a90f1003bc16515/20170095.pdf
☆データ保護影響評価(DPIA)の実施)
https://www.jetro.go.jp/ext_images/_Reports/01/4d53cce1193597c7/20170117.pdf
★「個人情報保護ﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑ導入・実践ガイドブック」
一般財団法人日本情報経済社会推進協会 プライバシーマーク推進センター 編
―――

概要・解説
★NTTデータ先端技術株式会社
EU 一般データ保護規則(GDPR)の概要(前編・後編)
http://www.intellilink.co.jp/article/column/security-gdpr01.html
http://www.intellilink.co.jp/article/column/security-gdpr02.html
―――

欧州委員会決定
★標準的契約条項(Standard contractual clauses:SCC)
SCC の仮日本語訳 by JETRO
SCC についての説明は、こちらをご覧ください。
★欧州委員会決定 2001/497/EC(Commission Decision 2001/497/EC
https://www.jetro.go.jp/ext_images/_Reports/01/8d894f365ea5c3a7/20170116_2001_497_EC.pdf
★欧州委員会決定 C(2004)5721(Commission Decision C(2004)5721)
https://www.jetro.go.jp/ext_images/_Reports/01/8d894f365ea5c3a7/20170116_2004_5721.pdf
★欧州委員会決定 C(2010)593(Commission Decision C(2010)593)
https://www.jetro.go.jp/ext_images/_Reports/01/8d894f365ea5c3a7/20170116_2010_593.pdf
★欧州委員会
(インフォグラフィック)の仮訳 by 個人情報保護委員会
https://www.ppc.go.jp/files/pdf/EC-Infographic.pdf
中小企業向けの、簡単にまとめられた GDPR 説明、ということでとても読みやすいですよ。
「infographic(インフォグラフィック)」は"information(情報)"と"graphic(図版)"を組み合わせた造語です。
★欧州委員会 GDPR の Q&A の仮訳 by 個人情報保護委員会
https://www.ppc.go.jp/files/pdf/Factsheet-20170524QandA.pdf
GDPR による変更点や、利点、忘れられる権利やデータポータビリティについての説明などがあります。
―――

©2019JSSAシステム監査学会 – 「情報セキュリティ対策の診断研究プロジェクト」 All right reserved.