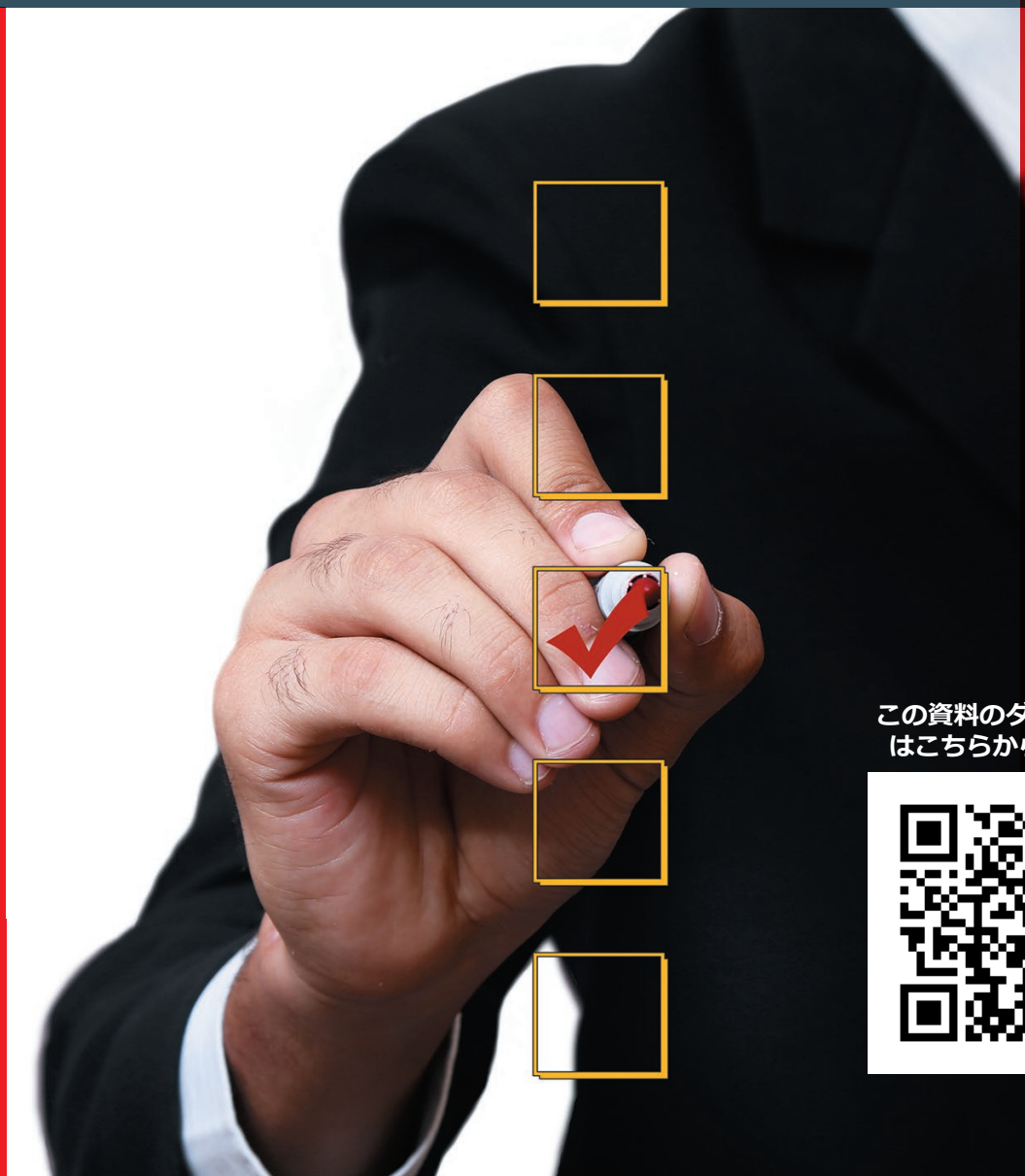
GDPR対応のポイント

―明示的同意取得とデータセキュリティ対策について―

2018年5月に施行されるEUのGDPR（一般データ保護規則）は、EU居住者の個人情報を扱うすべての組織が適用対象とされる。すなわち、EU居住者が利用可能なサービスを提供している企業は、たとえ国内にしか事業所を持たないとしても、GDPRへの対応が必須となる。そこで本文書では、情報セキュリティ・コンサルタントの佐藤慶浩氏に、GDPR対応におけるポイントを解説していただく。万全な体制でGDPR施行を迎えるために、本文書をご活用いただきたい。



この資料のダウンロード
はこちらからできます

GDPR対応のポイント
―明示的同意取得とデータセキュリティ対策について―

1. GDPR対応 ―日本の企業もGDPRへの対応が求められる

EUでは、2016年にGDPR（General Data Protection Regulation：一般データ保護規則）が制定され、2018年5月からの施行により、EU域内の居住者の個人情報を取り扱う各国の事業者への対応が求められている。

GDPRの目次を、本文書巻末の**表1**に示した。

GDPRへの対応では、表1の各項目に準拠する必要があり、特に域外移転などの個人情報の保管と移転についての要件がたびたび取り上げられているが、それ以外にも特徴的な要件が含まれている。本文書では、そうした特徴的な要件として、明示的同意取得とデータセキュリティ対策について解説する。

2. GDPRの特徴的要件 ―明示的同意取得

GDPRには、ご本人から同意を得るための方法において、他国の規制などよりも厳しい特徴的な要件があるので、それを紹介する。

日本の個人情報保護法では、個人情報を取得する際に、取得する個人情報の利用目的を通知する義務があるが、多くの国では、通知だけではなく同意を得ること（以後、「同意取得」と言う）も求められている。日本においても、個人情報保護マネジメントシステムの工業規格であるJIS Q 15001は同意取得を求めており、同規格に基づくプライシーマーク認証や、筆者が理事を務める一般社団法人 日本個人情報管理協会のJAPiCOマーク認証においては同意取得が求められる。ただし、諸外国の規制やJIS規格においても、同意取得の方法については詳細を定めていない。それに対して、GDPRでは、同意取得の方法を明示的な方法に限ると定めた。これは諸外国の既存規則にない特徴的な制限である。

2.1 明示的同意とは？

明示的な同意取得とは、同意するための行為をご本人に示し、その行為をご本人が実行した場合に限って、同意したものと判断することを求めるものである。

たとえば、ウェブ画面で個人情報を入力してもらい、利用目的を記載し、**図1**のように表示した上で、ご本人がチェックマークを記入した場合に限って、同意したこととすることが、明示的な同意取得となる。

一方で、明示的な同意取得にならないものは、**図2**のような表示である。

図2の例1は、チェックがあらかじめ選択されていることが、図1との違いである。図2の例2は、同意しない場合にはチェックしてくださいという文章にすることで、これにチェックしないのであれば、同意していると取り扱うというものである。

図1：明示的な同意取得となる例

例）個人情報の利用目的に同意していただける場合には、以下のチェックボックス（□）をクリックして、チェック（✓）を選択してください。

□利用目的に同意します

図2：明示的な同意取得とならない例

例1）個人情報の利用目的に同意していただける場合には、以下のチェックボックス（□）で、チェック（✓）を選択してください。

☑利用目的に同意します

例2）個人情報の利用目的に同意していただけない場合には、以下のチェックボックス（□）をクリックして、チェック（✓）を選択してください。

□利用目的に同意しません

図3：同意しているように見える画面表示

例1）

☑利用目的に同意します

例2）

□利用目的に同意しません

図2のような表示をした上で、ご本人が何もしなかった場合には、図3のような状態になる。

図3の状態は、表示上は、同意しているように解釈できるが、このような方法では、同意を得たことにならないということが、GDPRで制限されている。

つまり、ご本人による行為を伴わないような指示をした上で、そのような行為をしなかったことをもって、同意として取り扱うことは認めないということである。同意には、ご本人による行為が必要であるというのが、明示的な同意取得の制限である。

このように同意取得の方法を明示的か、そうではないかを区別することについては、経済産業省「オンラインサービスにおける消費者のプライバシーに配慮した情報提供・説明のためのガイドライン」（http://www.meti.go.jp/press/2014/10/20141017002/20141017002.html）でも示されている。同ガイドラインでは、明示的ではない同意取得を暗黙的同意取得と呼んでいる。また、現在、国際規格として、ISO/IEC 29184-Guidelines for online privacy notices and consentでも作成が進められており、それぞれ、Explicit consent（明示的同意）とImplicit consent（暗黙的同意）としており、それらを区別することは国内外を問わないことであるが、同意取得の方法を明示的な

ものに制限するというのは、GDPRが初めてであり、それが求められていることに事業者は注意しなければならない。

2.2 明示的同意取得の不備は、すぐに発覚する!

データセキュリティ対策の不備は、データ流出などの事故があった場合に、個人情報のご本人や規制当局に、その不備が発覚することになる。それと異なり、この同意取得の制限は、図2のような表示をしていることがわかった時点で、即座にGDPR違反であることが発覚する。すわなち、個人情報を取得すらしていない時点でも問題視されることについて、事業者は留意することが重要である。

そのため、従来は、JIS Q 15001規格による個人情報保護マネジメントシステムを構築していれば、利用目的の同意取得については、海外でも各国法令を遵守できることになったが、GDPRにおいては、明示的同意取得を確実にする必要がある。

ここでは、個人情報の利用目的についての同意取得について紹介したが、GDPRでは、第三者へ個人情報を提供することの同意取得や、EU域外に個人情報を移転することの同意取得についても、同様に、明示的な同意取得が求められている。

なお、同意取得状態をグローバルにデータ管理する方法については、拙著の論文「データプライバシー対策をグローバル対応するための顧客情報管理データベースの設計と運用のプラクティス」(https://ipsj.ixsq.nii.ac.jp/ej/?action=repository_uri&item_id=112548)に詳しく書いてあるのでご参照いただきたい。

3. GDPRの基本的要件 ―データセキュリティ対策は基本から

ご本人や当局に気づかれやすい同意取得の要件をまず先に紹介したが、当然、保管時の要件としてのデータセキュリティ対策についても対応が必要である。これについては、既に多くの解説があるが、GDPRの要件に個別に対応するよりは、データセキュリティ対策の基本に戻って、システム全体を見直す機会にするのがよい。

3.1 ITセキュリティ対策の基本は、4A+E対策

データセキュリティ対策の基本は、認証(Authentication)※、認可(Authorization)※、管理(Administration)、監査(Audit)の4つとされており、それらの英語の頭文字をとって4A対策としても知られている。これら4つのAに暗号化(Encryption)を加えて、**図4**のように4A+E対策として、ITシステム全体を検証するとよい。

4A+E対策について、順番に説明する。

図4:4A+E対策

A1 : 認証(Authentication)の厳格化:
アクセス者の特定
- 共用アカウントの利用の原則禁止

A2 : 認可(Authorization)の厳格化:
アクセス権の最少化
- ロール・ベース・アクセス制御による認可の運用

A3 : 管理(Administration)の厳格化:
認証と認可の適切な維持
- 管理作業の定型化ツールによる運用
- 特権アカウントの運用時凍結

A4 : 監査(Audit)の厳格化:
認証・認可・管理の証跡の保全
- 追記と読み出しだけに限定し、運用から独立した保全
- アノマリアクセスの監視

E : データ自身の保護:暗号化(Encryption)
- データアクセス経路の遮断/データファイルの暗号化

A1 認証(Authentication)の厳格化:アクセス者の特定

● 共用アカウントの利用の原則禁止

データへのアクセス主体が個人として識別される必要がある。これは、共用アカウントの利用を禁止することを意味する。データへのアクセスに、データベース等を使用している場合には、前段のアプリケーションでユーザー管理をしている場合であっても、データベースへのアクセスに共用アカウントを使わないようにすべきである。

図5の○で示すような適切な認証をすることによって、データベース製品が装備しているセキュリティ機能を最大限に活用することができるという利点もある。

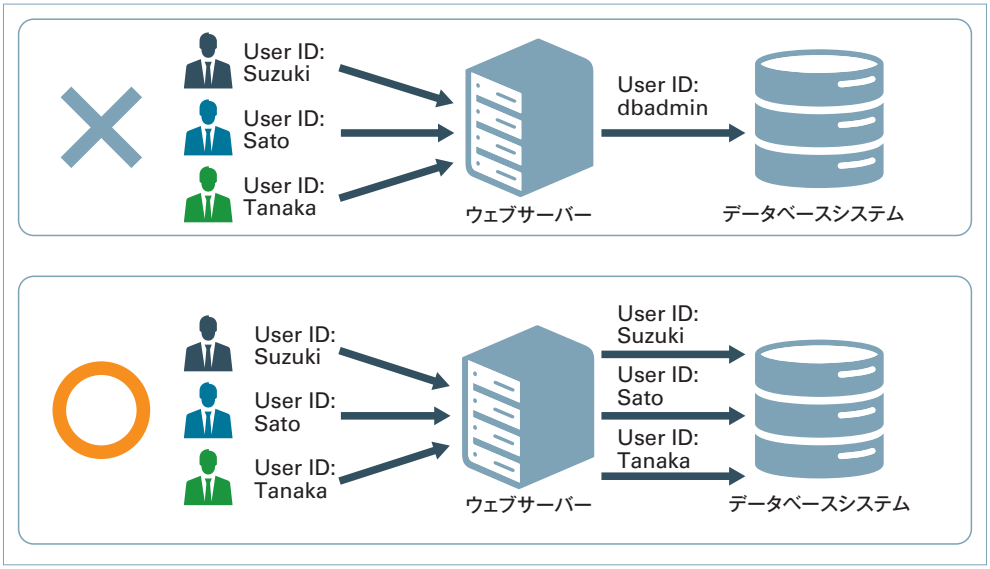
A2 認可(Authorization)の厳格化:アクセス権の最少化

● ロール・ベース・アクセス制御による認可の運用

各アクセス主体に対するアクセス権の付与については、業務上必要最低限にする必要がある。この最少化には、5W1H観点(いつ、どこで、誰が、何を、どの目的で、どのようにしての観点)で細密に検討するべきである。たとえば、深夜にアクセスすることが想定されないならば、その時間帯のアクセスが制限されるべきである。そのような運用を適切にするには、各人の職責と連携するようなロール・ベースでのアクセス制御が現実的である。

※:AuthenticationとAuthorizationをそれぞれ認証と認可と呼ぶことが一般的だが、どちらも日本語の本来の意味のとおり第三者による行為に限定されるものではない。そのため、第三者に限る認証と認可よりも、それに限らない検証と許可が日本語としては正確であるが、本文書では、なじみやすさを優先して認証と認可を用いる。

図5：データベースアクセスにおける適切な主体認証



特に重要なのは、システムの管理運用業務をロールとして正しく制御することである。

たとえば、すべてのデータのバックアップを作成する業務を、データアクセスのあらゆる権限を与えて実行させることがあってはならない。その業務の担当者は、バックアップを作成できればよいのであって、データを参照できてはならないからである。その担当者には、最少の権限として、バックアップ開始の指示だけを認可すべきであり、そのようなシステムの構築が必要である。

A3 管理（Administration）の厳格化：認証と認可の適切な維持

● 管理作業の定型化ツールによる運用

利用者のアカウントの新規作成には、デュアルロック機能を装備しなければならない。デュアルロック機能とは、行為に対して、少なくとも2名の者が操作しなければ、その行為を完遂できないようにする方式のことである。

また、利用者のアクセス権限の更新については、業務システムとの連携を図り、無人化すべきである。たとえば、担当業務の異動によるロールの変更については、人事管理システムと連携したり、ITシステム開発業務におけるロールの変更については、プロジェクト管理システムと連携させたりすることによる自動化が考えられる。

● 特権アカウントの運用時凍結

管理作業の定型化を徹底することにより、管理のためのアカウントによるログインを凍結することができる。逆に、そのアカウント凍結ができないということは、管理の厳格化が不十分であるとみなすべきである。

A4 監査（Audit）の厳格化：認証・認可・管理の証跡の保全

● 追記と読み出しだけに限定し、運用から独立した保全

監査証跡とアクセスログの違いを認識し、証跡（trail）として保全し、保護対象のシステム管理者によっても単独では保護機構を回避できないようにすることが重要である。そのためには、追記しかできない仕組みをシステム的に構築する必要がある。

データベースへのアクセスについては、認証で紹介したように、データベースの認証を適切に使うことにより、データベース製品による厳格な監査証跡の保全機能を使うこともできるようになる。

● アノマリアクセスの監視

アクセスログについては、アノマリアクセス（非通常行動）の監視を行うことが望ましい。アノマリアクセスを検知するためには、通常の行動も把握する必要があるため、収集したログの定期的な監視が必要となる。

E データ自身の保護：暗号化（Encryption）

● データアクセス経路の遮断／データファイルの暗号化

データベースとしての4A対策を十分に実施したとしても、データファイルそのものへの直接的なアクセスによって、すべてのデータを参照できてしまっては、データ自身が保護されない。これを防ぐには、データファイルの暗号化が必須である。このことは、ディスク装置の故障時の交換修理などにおいても、データ自身を保護するためにも必須の対策である。

3.2 GDPRが求めているのは基本的なこと

4A+E対策のうち、特徴的なことを紹介した。これを検証した上で、GDPRのデータセキュリティ要件を確認すると、その多くが基本を踏まえることを求めているだけであることがわかるはずである。そのように検討すれば、GDPRへの個別対応というよりは、この機会にシステムの基本的なことの再確認だと思って前向きに取り組むことができるはずである。

4A+E対策について、すべての機能を確認したければ、国際規格であるISO/IEC 15408（https://www.ipa.go.jp/security/jisec/about_cc.html）を参考にするとよい。この規格は「コモンクライテリア」と呼ばれ、本来は、ソフトウェア製品のセキュリティ認証を取得するための規格であり、WindowsやLinuxなどのOS製品の他、データベース製品などが同規格に基づく認証を取得している。しかし、認証を得る目的ではなく、自社で構築した社内システムに対して、規格に示された機能要件を満たしているかを検証してみることは、システム全体のセキュリティ機能の網羅性を確認するために有用な内容である。

これは、ISO/IEC 15408に示されている機能をすべて網羅すべきということではない。それらの機能を対象のシステムで装備していないことのリスクを認識することに役立てることができる。装備しない機能については、技術的に対応しなくとも、そのリスクを認識できれば、運用方法で対応することによってリスク軽減することについて検討するきっかけにすることができるので有用である。

4. まとめ

GDPRについて、明示的同意取得とデータセキュリティ対策について紹介した。2018年5月には、ここで紹介したことの他に、表1の要件すべてについて対応する必要がある。しかし、GDPRが求めていることは、事業者が消費者に対して行うべきことの基本的なことであると考えることもできる。もしも、GDPR対応をするにあたって、これまで自社で行なっていたことに追加的な対応が必要になるとしたら、それは、これまで消費者目線での対応ができていなかったことの戒めとして受け止めてもよいかもしれない。

つまり、GDPR対応をEU規制へのコンプライアンス対応と考えるよりは、お客様対応意識の再確認として取り組むことが、事業者にとって健全である。経営層は、各事業部門がGDPRの要件をそのように受けとめられるかで、各事業部の取り組みがお客様目線になっているかを認識する機会にするべきである。

［著者プロフィール］
佐藤慶浩（さとうよしひろ）
オフィス四々十六・代表（https://office4416.com/resume）
アポロコンピュータ、ヒューレット・パッカードでソフトウェア及びハードウェアの開発を経て、ISP、インターネットバンキング、インターネットトレーディングなどの国内での立ち上げにおいて、それぞれ、高可用性、セキュリティ、スケーラビリティの高度化のためのITアーキテクトを担当。それらと併行して情報セキュリティ規程策定の方法論を開発及びコンサルティングして国内に展開。民間組織以外に政府機関についても内閣官房NISCに併任して政府機関統一基準を設計した。
ヒューレット・パッカード社セキュリティソリューション事業アジア地域統括マネージャ、内閣官房情報セキュリティ参事官補佐・情報セキュリティ指導専門官、HP社アジア地域プライバシー・オフィサーを歴任した後、現在はフリーランス・コンサルタントをしている。

この資料のダウンロード
はこちらからできます

表1：GDPRの目次（「EU一般データ保護規則（仮訳）」https://www.jipdec.or.jp/library/archives/gdpr.htmlから抜粋）

第 1 章　総則

第 2 章　諸原則
- 個人データの取扱いに関する原則
- 適法な取扱い
- 同意の条件
- 情報社会サービスに関する子どもの同意に対して適用される条件
- 特別な種類の個人データの取扱い
- 有罪判決及び犯罪に係る個人データの取扱い
- 識別を要求しない取扱い

第 3 章　データ主体の権利
- データ主体の権利行使のための透明性のある情報、通知及び手続
- データ主体から個人データを収集する場合に提供される情報
- データ主体から個人データを取得しない場合に提供される情報
- データ主体のアクセス権
- 訂正の権利
- 消去の権利（忘れられる権利）
- 取扱い制限の権利
- 個人データの訂正若しくは消去又は取扱いの制限に関する通知義務
- データポータビリティーの権利
- 異議を唱える権利
- プロファイリングを含む自動化された個人意思決定

第 4 章　管理者及び取扱者
- 一般的義務
- 個人データの保護
- データ保護影響評価及び事前協議
- データ保護オフィサー
- 行動規範及び認証

第 5 章　第三国又は国際機関への個人データ移転
- 移転に関する一般原則
- 十分性決定に基づく移転
- 適切な保護措置に従った移転
- 拘束的企業準則
- EU 法によって認められていない移転又は開示
- 特定の状況における例外
- 個人データ保護に関する国際協力

第 6 章　独立監督機関

第 7 章　協力及び一貫性

第 8 章　救済、法的責任及び制裁

第 9 章　特別な取扱い状況に関する条項

第 10 章　委任行為及び実施行為

第 11 章　最終条項

日本オラクル株式会社
〒107-0061 東京都港区北青山2-5-8 オラクル青山センター
oracle.com/jp

お問い合わせ窓口
Oracle Digital
TEL 0120-155-096
URL oracle.com/jp/contact-us