clearswift
RUAG Cyber Security

# EU GDPR（一般データ保護規則）に備える

## よくあるご質問とその答え

ホワイトペーパー

# 目次

## 背景

EUの新しい一般データ保護規則（GDPR）（EU 2016/679）が2018年に施行されることになっています。この新規則では、現在多くの組織で講じられているものを超えるデータのプライバシーとセキュリティが求められています。EU内でビジネスを行っている企業は、たとえEU内に拠点を持たずとも、所定のコンプライアンス措置を講じなければ、莫大な制裁金に直面することになります。

クリアスウィフトは、新規則の理解と準備の効率化のための資料として、クリアスウィフトのホワイトペーパー『EU一般データ保護規則（GDPR）に備える ― 新規則の概要と技術戦略』を提供しております。これに加え、本書ではGDPRに関してよくあるご質問とその答えをまとめました。

## よくあるご質問とその答え

1. なぜ今になってGDPRが導入されようとしているのですか？

   EUにはデータ保護[1]とプライバシーのための指令が20年以上前から存在しています。これはEUにおけるプライバシーと人権保護のための法の土台となるもので、その多くの規定はGDPR（一般データ保護規則）に盛り込まれたものと同じものです。しかし、指令自体には法的拘束力がないため、この法の執行は各加盟国に委ねられていました。しかも、この20年間で情報の価値や、情報の共有と管理の方法が大きく様変わりしています。　それゆえに、EU全体で一貫した法的拘束力のある規則が、指令に代わって必要となったのです。

   GDPRは、ビジネスに足枷をはめるために制定されたものではありません。規則の順守が各国でまちまちな現状を、統一された規則に置き替えるためのものであり、それによって年間20億ユーロ以上の費用削減が見込まれています。

2. GDPRが施行されるのはいつからですか？

   新規則は2018年5月に施行される予定です。これはかなり先のことのように思えるかもしれませんが、大規模なコンプライアンスプロジェクトにとっては目の前に迫ったのも同然です。設備投資を伴うような場合には、期限内に調査、購入、導入までを完了するのに残されているのは、わずかに1会計年度のみです。

3. 保護する必要があるのはどのような情報ですか？

   GDPRは、EU市民の個人データを保護するためのものです。しかし、この個人データの定義に関しては、しばしば議論の対象となっています。欧州委員会では、個人データを　「私的、職業的、または公的な個人に関する情報であり、氏名、写真、電子メールアドレス、銀行口座情報、ソーシャルメディアへの投稿、医療記録、またはコンピュータのIPアドレスなどあらゆるものを含む」と定義[2]しています。

   また、国家安全保障や児童保護、医療、歴史的/科学的調査に関するデータの処理については、特別な条件が設けられている点に注意を払う必要があります。

4. 提案された制裁金は企業を廃業に追いやるものではないのですか？

   コンプライアンス違反に対する制裁については、たしかにメディアの注目を集めています。全売上高の4%という額は、確かに企業を廃業に追いやる可能性があります。しかしながら、制裁金は支払わせるのが目的ではなく、コンプライアンスの達成に意識を向けさせるために設けられたものです。巨額の制裁金については先例があり、近いものではフォルクスワーゲンの排ガス不正についてのアメリカでの和解がそのひとつです。

   サイバーセキュリティについては、役員レベルで関心を持つ必要があります。このような巨額の制裁金は、それを単なる話題として終わらせず、実際の行動を起こさせる刺激となるでしょう。

[1] https://en.wikipedia.org/wiki/Data_Protection_Directive

[2] http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en

5. 制裁金が実際に課せられることはあるのでしょうか?

制裁金が課せられた例はまだありませんが、ある程度の憶測は流れています。これまでに、データ侵害に対して制裁金が課せられた国がいくつかあり、その多くは規則で決められた範囲の最高額でした。一般に理解されているところでは、コンプライアンスを助長するために、早い段階でかなり大きな額の制裁金が課せられるだろうと言われています。

もちろん、コンプライアンスの目的は制裁金を回避することにあります。制裁金を課せられる可能性を思い悩んで時間を潰してしまうと、コンプライアンスを実現するために必要な時間がなくなってしまいます。

6. 承諾書用紙自体など、 個人の明確な同意表明は、保管して利用可能な状態にしておくことが求められていますか?

要求に応じるにはいくつかの方法があります。紙の書式によることもできますし、Webページでのオンラインによるものもあるでしょう。同意のあることを証明する義務は企業側にありますので、コンプライアンスを達成するためにベストな方法を決めるのも企業に任されます。多くの場合、同意が得られた日時を記録することが求められますので、紙の書式だけでは十分ではありません。紙の書式を使用する場合は、後で要求された場合に検索できるよう、スキャンして保存することになるでしょう。

また、16歳以下の未成年との取引を行う場合には、親または保護者（検証可能な人物）の同意が必要であることに留意するべきです。

7. 電子メールの保管義務はありますか?

いいえ、規則では特に定められていません。しかし、他の規則では、特に企業の記録に関して電子メールを一定期間保存するように定めているものがあります。

パートナーと電子メールでデータ共有を行っている場合は、電子メールを保管することで誰に何を送ったか、あるいはパートナーから何を受け取ったかを追跡するのに利用できます。この種類の情報は、「忘れられる権利」と呼ばれる同意の撤回など、規則中の特別な要求に応じる際に必要となります。

8. 「プライバシー バイ デザイン」とは実際どのような意味なのですか?

「プライバシー バイ デザイン」は、GDPRの重要な要素のひとつです。一般的に言って、セキュリティやプライバシーといった側面は、製品やアプリケーションが作られた後に考慮され、後に改良が加えられる傾向にあります。最初から設計にそれらを組み込んでおけば、改良時にしなければならない妥協をする必要がなくなります。

ヤン フィリップ アルブレヒト欧州議員[3]は、プライバシー バイ デザインだけでなく、実施についても語っています。今のところ、これを容易に評価するための基準は存在しておらず、したがって、コンプライアンスのためにどれほどのことをする必要があるかを経営陣が判断するのが難しい状況にあります。

9. 企業にとっては、GDPRを順守するとサイバーセキュリティリスクの軽減に役立つのでしょうか?

もちろんです。GDPRは、世界中で百以上存在するデータ保護とプライバシーに関する規則と異なるものではありません。GDPRが適用される範囲は他の規則よりも広く、影響もより大きなものですが、本質的には同じものです。情報の内容とその保管場所、そしてアクセスできる者が誰かを理解して、保護を施します。それらをコントロールできるほど十分に理解し、削除するように求められたときには、それができなければなりません。GDPRを順守するということは、実質的には、順守すべき他の規則すべてを順守するということになります。

10. GDPRには他の規則と相反する部分がありますか?

多くの企業にとって、規則の順守とは規則間の相反部分のバランスを取る作業であり、GDPRも例外ではありません。自分と組織が順守すべき規則を理解することで、相反する点を浮き彫りにすることができます。簡単な例が、GDPRにある「忘れられる権利」です。表面だけを見れば、それは単に要求を提出した個人に関連する情報を削除するというものです。しかしながら、それが商品やサービスを購入した顧客に関するものである場合、その種の記録を一定期間保存するように定めた他の規則によって、GDPRの規則は覆される可能性があります。

[3] http://www.europarl.europa.eu/meps/en/96736/JAN+PHILIPP_ALBRECHT_home.html

### 11. GDPRでは、暗号化はどのように扱われていますか？

GDPRでは暗号化について特に言及されてはいません。しかし、暗号化はセキュリティとプライバシーのためには価値のある技術です。クレジットカード番号のような情報は、PCIデータ　セキュリティ　スタンダード(PCI DSS)に準拠した処理を行う際のさまざまなポイントで暗号化することが求められており、これはコンプライアンス計画の中で暗号化をどのように利用できるかを示したものとも言えます。

暗号化については、その解読において、個人のプライバシーの尊重と、インサイダー取引や市場操作、贈収賄、汚職、マネーロンダリングなどの法的監視義務履行との間で、規制順守上の難問となる可能性があります。

今日の暗号化ソリューションは、企業業務のプライバシー的側面とコンプライアンス順守をサポートするよう設計されています。GDPRは、このバランスを脅かすために制定されたものではありません。多くの組織にとっては、容認可能な使用法を取り決めた明確な定義のポリシーを持つことが、適切なソリューションを導入する鍵となるでしょう。金融サービス市場においては、許容できるものとできないものの厳格なガイドラインが存在しており、それらをポリシーに組み込み、その上で個人、部門、あるいはテクノロジーによって執行されることになります。

### 12. イギリスのEU離脱は、イギリス内にあるデータにどのような影響を及ぼすでしょうか？

本書の執筆時点（2016年7月）においては何の影響もありません。EU離脱には最低でも2年かかる見通しであり、イギリスが実際に離脱するまでは、それらのデータは「EU内」にあることになります。現時点では、イギリス内のデータの保存方法とアクセス方法にはいくつかの異なったルールが存在しています。セーフハーバー協定[4]はEU-USプライバシーシールド[5]によって置き換えられましたが、その適用外であっても、数年の間はモデル契約条項[6]や拘束的企業準則[7](BCR)を利用可能です。

またEU離脱後であっても、EU市民と取引を行うイギリス国内企業は、やはりGDPRを順守する必要があります。

### 13. プライバシー保護のために当社が監督すべきサードパーティのプライバシー規則のバランスはどうなっていますか？

GDPRは実現手段として捉えるべきものですが、どうもこれは難しいようです。多くの人がこれを「もうひとつの規則」としてしか見ていないためです。GDPRの及ぶ範囲はこれまでの規則よりも広いため、企業や組織はパートナー、サプライヤー、請負業者、コンサルタントなどについて、自社の顧客や市民のプライバシー権が適切に保護されているかどうか、調査を開始する必要があります。聞かねばならない種類の問いかけを発することで、必然的に抵抗に合うことが予想されます。たとえば、パートナーがサイバーセキュリティに真剣に取り組んでいるかどうかを判断するための侵入テストや脆弱性テストを行って、結果が悪かったことを相手に伝えると、相手は侮辱と受け取るかもしれません。

今は、難しい時代です。コンプライアンスに取り組む上では、他社が個人情報をどのように扱っているのかを知らなければなりません。他社が個人情報を売ったり、うっかり漏らしたり、第三者に譲渡したりということがないことを誰もが願うでしょうが、実際のところは分かりません。他社も自社と同じように重要情報を保護していると信じたいものですし、実際そうだとは思いますが、聞いてみなければ知ることはできないのです。どのような組織であっても、孤立しているわけではありません。上流と下流には必ず誰かがいます。相手のサイバーセキュリティ対策について質問するのは気が進まないかもしれませんが、自社については聞かれても大丈夫なように準備しておくべきです。

他社と協力し、インフォメーションチェーン全体に適切な保護を施すことが、全員にメリットをもたらすことになるのです。

### 14. GDPRを順守した企業が、順守しない他社に対して不利になることはありませんか？

EU域内で取引を行うのであれば、GDPRを順守する必要があります。現行の制度においては、EU内に拠点を持つ組織は罰せられ、そうでなければ罰則を逃れられるということがあり得ます。しかし、新規則の下では、どちらにも同じ罰則が適用されます。同様に、現行の制度下では、国によってEUのガイドラインの解釈が異なるために国による違いが生じていますが、新規則の下では域内が統一されます。順守がデメリットではなく、メリットを生じるのです。

[4] https://en.wikipedia.org/wiki/Safe_harbor_(law)
[5] https://en.wikipedia.org/wiki/EU-US_Privacy_Shield
[6] http://www.out-law.com/en/topics/tmt--sourcing/data-protection-and-privacy/model-clauses-for-transferring-personal-data-overseas-an-overview/
[7] https://en.wikipedia.org/wiki/Binding_corporate_rules

15. データ保護官（DPO）は本当に雇用する必要があるのですか？

簡単に言ってしまえば、「イエス」です。詳しくお答えするためには、データ保護官(DPO)を他社と共有するのか、または、社員の誰かを任命することができるか、という点を考慮する必要があります。DPOの役目は、市民の情報保護を真剣に懸念している政策制定者の立場から組織を眺めることにあります。DPOの役割を、「コンプライアンスを推進し、コンプライアンスを通した競争力を生み出す者」と考えることができれば、組織にとって必要な役割であるとポジティブに捉えることができるでしょう。

16. 当社にはCISO（あるいはCIO）がいますが、その人物をデータ保護官(DPO)とすることは可能ですか？

同じように、簡単な答えは「イエス」です。中小規模組織の多くにおいては、一人の役員がいくつもの役割を兼務する必要があります。CISOかCIOの役割は、DPOの役割になじみます。さらに小規模な組織では、IT部長やITセキュリティマネージャーにDPOの責務を与えることが検討されています。いずれの場合においても、この役割を担う人物には規則の詳細を理解するためのトレーニングを受けさせる必要があります。GDPRには、IT専門家が持つスキルを必要とする部分と、規則のニュアンスを理解するために別種のトレーニングが必要な部分があるためです。大規模な組織においては、DPOは兼務としない方が、利害の衝突が起きない分だけコンプライアンス推進上有利となるでしょう。

## どこから手を付けたらよいでしょうか

GDPRに向かって全力投入する前に、教育と啓蒙活動が必要です。事業部横断のワーキンググループを立ち上げ、GDPRとその要求事項について議論を行いましょう。その結果に応じて、アクションプランをまとめていきます。また、クリアスウィフトのウェブサイトには準備に役立つ資料を掲載しておりますので、そちらもご参照ください。

17. 実際にどこから手を付ければ良いのでしょうか？

表面的にはGDPR順守はとてつもない課題に見えますが、基本から始めて、アクション可能な部分に切り分ければ、容易に進められます。既にいくつかの法令順守を行っているのであれば、そこを始点とし、類似点と相違点を明らかにして行くのが良いでしょう。アメリカにはいくつもの侵害報告を義務付ける法令があります。GDPRでも、侵害報告が義務付けられています。ですから、アメリカの企業にとっては、現在行っていることとそれほど大きな違いはないかもしれません。

GDPRとは要は情報とその保護に関するものであり、それがどこにあるかは関係ありません。したがって、自分が持つ情報を理解することが重要な第一歩となります。

- 今保持している情報で新規則の対象となるものはどれか
- その情報は、どこに保存されているか（データベース内だけでなく、レポートやファイル、クラウドストレージ、USBなどを含める）
- その情報にアクセスできるのは誰か（社員だけでなく、社内にいる部外者や、その情報を送付した社外の人間も含める）
- その情報の処理目的は何か、そして入手済みの同意レベルはどの程度のものか
- その情報が不注意や悪意によって組織外に流出してしまう可能性のある経路にはどのようなものがあるか（電子メール、FTP、クラウドストレージ、クラウドコラボレーション、ソーシャルメディア、企業Webサイト上での公開など）

情報とその流れを理解することで、コンプライアンス計画の作成が可能になります。既存のポリシーやプロセス、さらにはセキュリティソリューションの見直しも必要です。それらはコンプライアンスのために利用できるものもありますし、強化や拡張が必要なものもあるでしょう。

### 18. GDPRの中で、順守が最も難しいのは何ですか?

難しい質問です。あえて言えば、「忘れられる権利」が最も難しいものかも知れません。これは、「同意の撤回」、または「削除権」とも呼ばれているもので、個人が自身に関するすべての個人情報の削除（消去）を要求できる権利です。

組織側としては、そういった情報がどこにあろうが見つけ出し、削除する必要があります。ただし、それは他の規則に抵触または違反しない場合に限ります。データベース内の情報を検索することは、比較的容易です。しかし、電子メールやレポート、文書中にも存在するかもしれない情報のコピーも見つけなければなりません。GDPRの効力が到達する距離は長く、削除要求は該当する情報を共有しているサードパーティにも伝えなければなりません。

これは、今日のテクノロジーを利用すれば完全に可能なことです。しかし、多くの企業では削除要求に応えるためのプロセスや技術を備えていないのが現状です。

### 19. GDPRは、捕まりさえしなければ問題ないのではないですか?

EUで取引を行い、規則の適用対象となる情報を保持している場合には、コンプライアンスを達成していることと、そのために用いた戦略を文書化することが求められます。また、政策制定者は、いつでもその情報の提出を求めることができます。そういった情報を持っていなければ、それは既に規則違反とみなされます。

GDPRは一つの組織に止まらず、そのサプライヤーをはじめ情報サプライチェーンに含まれるすべての組織に対して適用されます。他の組織からの要求を受けることが当たり前のこととなり、また、ビジネスを行う上での必要条件となるでしょう。結局のところ、GDPRの対象となる情報を、それを適切に管理できないような相手と共有する気になれますか?

### 20. GDPRを順守するには多大なコストがかかるのでしょうか?

これは、難しい質問です。貴社の今日のコンプライアンスレベルが高ければ、新規則による影響は最小となるでしょう。新たなプロセスを設ける、あるいは新しいポリシーやプロセスを実行するために新規の技術ソリューションが必要になるかもしれませんが、その必要すらないこともあり得ます。

しかし、ほとんどの組織にとっては、規制順守は費用と時間のかかるものとなるでしょう。それでも、規制順守に必要なコストは、制裁金やコンプライアンス違反発生の際の緊急処理に伴うコストよりも少ないものです。たとえばソニーは2011年の違反事案を解決するために1億7100万ドルを支出しなければならなかったと見積もられています。[8]当時はGDPRによる制裁金はまだありませんでしたが。別の味方をすれば、これは特に初期段階においては、競争力を高めるためのチャンスとして利用できるでしょう。消費者の33%が、プライバシーの懸念から取引をキャンセルしたという事実があります[9]。競合他社よりも優れたプライバシー保護方針を持つことで、お客様を自社に引き寄せることが可能なのです。

[8] http://www.darkreading.com/attacks-and-breaches/sony-data-breach-cleanup-to-cost-$171-million/d/d-id/1097898

[9] Forrester North American Consumer Technology Survey, 2014

clearswift
RUAG Cyber Security

**クリアスウィフトについて**

ククリアスウィフトの製品、ソリューション、サービスはGDPR遵守のための様々な手助けをいたします。

クリアスウィフトは、ビジネスクリティカルなデータを保護して安全なコラボレーションとビジネスの成長を実現することで、世界中のお客様に信頼されている情報セキュリティ企業です。クリアスウィフト独自の技術は、直接的で「適応型」の情報漏洩防止をサポートし、業務の中断を防ぎ、クリティカルな情報に対する完全な可視性の常時確保を可能にします。

クリアスウィフトおよび製品、サービスに関する詳しい情報は以下のホームページをご覧ください。
www.clearswift.co.jp

**クリアスウィフト株式会社**

〒163-1030
東京都新宿区西新宿3-7-1
新宿パークタワーN30階

Tel :03-5326-3470
Fax: 03-5326-3001
Email: sales.jp@clearswift.co.jp
Website: http://www.clearswift.co.jp