HULFT Newton IT

White Paper

「データ移転」だけが問題じゃない? IT で実現すべき GDPR 対策

― 4 つのポイントと IT ソリューション ―

Newton Information Technology Ltd.

株式会社セゾン情報システムズ　HULFT 事業部

15 May 2018

はじめに

2014 年 4 月 14 日に欧州議会で制定された GDPR（General Data Protection Regulation / EU 一般データ保護規則）が 2018 年 5 月 25 日より適用開始となります。

European Economic Area / 欧州経済領域（EEA）域内の企業及び、EEA 域内に存在する個人データを処理している域外の企業は、法務、データ管理、IT の三視点からの対応が必要となり、日本企業においても、EEA 域内拠点のみならず、本社や EEA 域外拠点での対応が必要な場合もあり、ビジネス上の重要課題の一つでもあります。そのため、前述の三視点を踏まえ、法務、人事、情報システム、内部統制等の関連部署が連携し対処することが必要になります。

このホワイトペーパーでは GDPR が生まれた背景、主に IT 面から気を付けるべきポイントについて株式会社セゾン情報システムズと、Newton Information Technology Ltd.がその知見に基づき概説し、対応する IT ソリューションに関してご紹介します。

GDPR 誕生の背景

GDPR の源流は、1995 年に採択されたデータ保護指令（The European Data Protection Directive (Directive 95/46/EC) ）に遡ることができ、この指令に基づき、EU 加盟国は各国法を整備し、英国では Data Protection ACT 1998 が制定され、2000 年から適用されました。当時の状況を振り返ると、電子商取引、オンラインバンキング、スマートフォン、アナリティクス、SNS、ビッグデータ、AI 等、個人データが電子的に処理、保存され、多方面で利用されるようなテクノロジー、プラットフォーム、システム等、現在とは比ぶべくもありません。

デジタルトランスフォーメーション時代を迎え、新たな個人データ保護の枠組みが必要となり、また、企業活動がグローバル化する中、EU 加盟国間で非整合な個人情報保護法制への対応労力が増大していることも含め、GDPR は正に時代の変化に対応することへの必要性から生まれたと言えます。

規制強化された点

GDPR は、EEA 域内での個人データ保護法制の統一を目指すもので、規制項目は大別すると、取得、処理、域外移転の 3 点になります。

■ 取得

データ取得者たる企業は、データ主体（個人）に取得目的、第三者への開示有無、データ主体の権利等を分かり易く説明し、明確な方法で同意を得、かつ同意を撤回できるようにしておかなければならない等、個人データ取得の為の処理手順の確立が必要になります。

■ 処理

取得した個人データを安全かつ正しく処理する為の仕組みの構築に加え、従業員数が 250 名を超える企業や、センシティブデータ（第 9 条で規定されている信仰や政治信条等のデータ及び、刑事有罪判決、犯罪行為に関するデータ）を処理する場合には、データ処理の履歴を記録することが求められています。また、データポータビリティの権利や削除権（忘れられる権利）、DPIA（データ保護影響評価）への対応等も必要になります。これに加え、大量の個人データを定期的かつ体系的に処理する場合には、DPO(Data Protection Officer / データ保護責任者)の配置も必要です。

■ 域外移転

EEA 域内から EEA 域外への個人データの移転については、原則禁止されていますが、第 45 条に基づき、EC（European Commission / 欧州委員会）が個人データ保護についての十分性認定（Adequacy Decision）を行った国々（アンドラ、アルゼンチン、カナダ、フェロー諸島、ガーンジー、イスラエル、マン島、ジャージー、ニュージーランド、スイス、ウルグアイ）についてはデータ管理者または処理者への移転が認められています。また、米国についてはプライバシーシールドフレームワークに加入している 2,723 の企業、団体への移転が可能になっています。日本、韓国は協議中の状況（2018 年 4 月 30 日現在）です。
十分性認定が得られていない国々の企業・団体等へのデータ移転については、適切なセーフガードが構築されていることを前提（第 46 条）に、BCR（Binding Corporate Rules /拘束的企業準則 - 第 47 条）または SCC（Standard Contractual Clauses /準契約条項）を締結することにより認められます。

尚、違反時の過料は以下のとおり規定されています。

- 1,000 万ユーロ、または、前会計期間の全世界の売上高の 2%のうち、いずれか高い方の過料
- 2,000 万ユーロ、または、前会計期間の全世界の売上高の 4%のうち、いずれか高い方の過料

上記のとおり、EEA 域内に拠点を置く多くの日本企業の連結売上高を考えると、最悪の場合、非常に高額な過料を課せられることになります。それでは実際に GDPR に準拠した事業を運営して行く上で、どのような対策を考えて行けば良いかを次の章で説明いたします。

対応のポイント

英国の ICO（Information Commissioner's Office / 個人データ保護機関） は、Preparing for the General Data Protection Regulation (GDPR) - 12 steps to take now「GDPR 対応準備 - 今、行うべき 12 ステップ」として、以下の点を考慮した対応を推奨しています。

ICO は英国機関ですが、GDPR 対応に立脚した視点から策定されている当該 12 ステップは、英国企業のみならず、在 EEA の企業おいても指針策定の軸になり得るとの考えから、本資料において参考にしています。

1. Awareness（認識）
2. Information you hold (保持している情報)
3. Communicating privacy information（適切なプライバシー通知の適用）
4. Individuals' rights（個人の権利）
5. Subject access requests（アクセス権）
6. Lawful basis for processing personal data（個人データの処理の法的根拠）
7. Consent（同意）
8. Children（16 歳以下のデータ主体の個人データ取得）
9. Data breaches（データ侵害への対応）
10. Data Protection by Design and Data Protection Impact Assessments (法令遵守の為の仕組みの構築及びデータ保護影響評価)
11. Data Protection Officers（DPO、データ保護責任者の任命）
12. International（域外移転）

本資料では、12 ステップの中から、IT ソリューションでの対応という視点から、4 点に焦点を当てて解説します。

対応ポイントと IT ソリューション

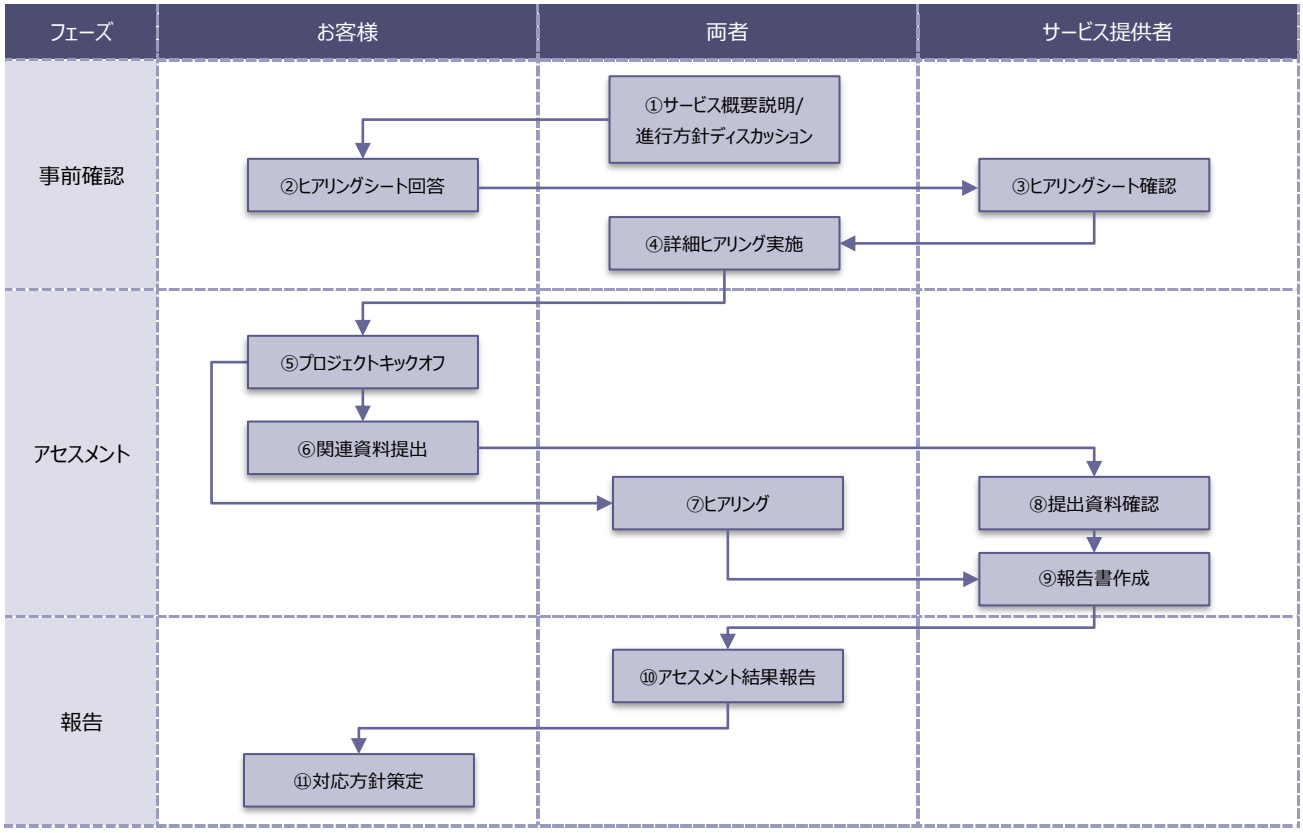
ポイント	企業における課題点	要実施事項	IT ソリューション
Information you hold (保持している情報)	• 現行の個人データ移転・処理状況の未把握 • GDPR 違反有無の未把握 • 不要個人データの保持	• データマッピング • サードパーティアセスメント	• GDPR アセスメント
Individuals' rights (個人の権利)	• 「データ主体の権利の尊重」に対応するための仕組みの未整備 • 保持個人データの所在の未把握	• データ所在把握の仕組みの導入 • データ管理体制導入	• 個人データの所在検索
Data breaches (データ侵害への対応)	• 個人データ侵害が発生した際の検知の仕組みの未整備 • 監督機関/データ主体への報告体制の未整備	• データ侵害検知の仕組みの導入 • ログ取得	• 情報漏洩検知・防止 • データ抽出 • データ正確性実証
Data protection (データ保護)	• 情報セキュリティに対する考慮が不足した IT インフラ環境の利用	• IT インフラ環境の精査 • 脆弱性への対策実施	• IT インフラ環境監査 • レイヤー毎の情報セキュリティ対策適用

■ Information you hold(保持している情報)

GDPR の初期対策としては、以下 2 点の実施が推奨されており、この 2 つを包含した対応が、通常、「GDPR アセスメント」と呼ばれています。

1. データマッピング
   企業が保持する個人データについて、その種別、格納場所、処理内容、データ量、移転の状況等を明確化する
2. 課題点抽出
   上記データマッピングを基に、GDPR に違反すると考えられる点を抽出する

本アセスメントのプロセスの例としては以下の通りです。



アセスメントにより抽出された課題に関して、優先順位を付けて対応して行くことになります。

■ Individuals' rights（個人の権利）

GDPR には、「忘れられる権利」に関わる 17 条、個人の自己データ利活用と保護を両立させる為のデータポータビリティを規定している 20 条、今後進展すると思われる AI やアナリティクスによるプロファイリングに基づく決定への懸念を反映した 22 条等が定められており、データ主体の権利の行使への対応が必要になります。例えば、ビジネス向け SNS のような企業が参照できる個人データと、個人の履歴書情報には最新の情報を反映する際にタイムラグが発生する可能性があります。それを企業が参照すると、誤った情報が伝わる可能性があり、このような情報を訂正できるようにしなければなりません。

データ主体から削除、提供、変更といった要請があった場合には、適時性をもって対応しなければならず、対象となる個人データの所在を効率良く特定するシステムを構築する対応が効果的です。マニュアルで社内システムから個人データを探し出して更新するのは限界があるため、データ連携ツールを利用した自動監視が効果的と考えられます。

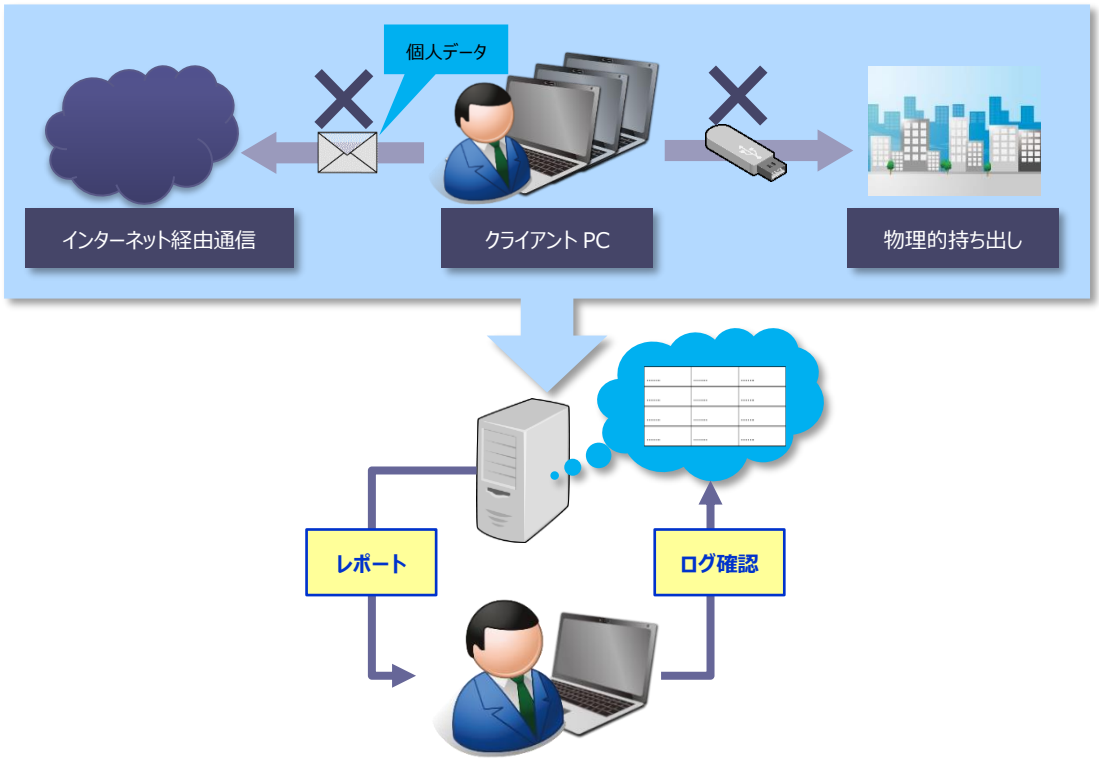
例えば、セゾン情報システムズのデータ連携ツール「DataSpider Servista」では、データベースの特定テーブルを監視するデータベーストリガーがあり、変更が発生した際に、リアルタイムで他のシステムに存在する情報を更新するといった運用が可能です。

Data breach（データ侵害への対応）

改ざん、漏洩を含む個人データの侵害が発生した際は、これを検知してから 72 時間以内に、以下をはじめとする項目を各国の監督機関に通知することが求められます。

- データ侵害の内容
- 個人データのカテゴリー
- 対象となるデータ主体/データの数

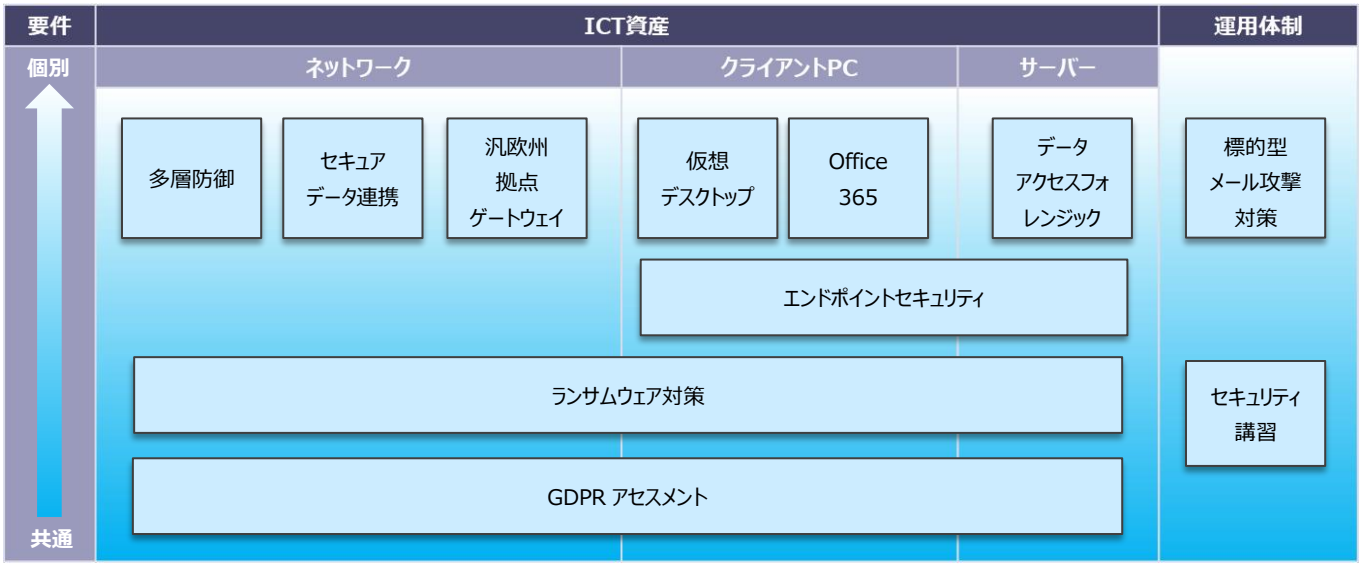
過去、2011 年に日系企業より、クレジットカード情報を含む大量の個人データ漏洩が発生しましたが、規模の大小にかかわらずこのようなケースに備えることが重要となります。
以下にデータ侵害検知ソリューションの概要を示します。



本ソリューションでは、クライアント PC 経由での特定の個人データの通信について、検知・ブロックを行うと共に、この内容を管理者にレポートし、ログの蓄積を行います。これにより、万が一の漏洩が発生した場合にも GDPR が定める通知要件に対応することが可能になります。

■ Data protection（データ保護）

GDPR 関連アセスメント、またはセキュリティ監査実施の後、その結果を基に、課題点に対する対策を講じる必要があります。特に、IT 視点にて対応可能、かつ有効と想定されるソリューションは以下となります。



1） 多層防御

侵入対策（ファイアウォール、不正侵入検知システム-IDS、不正侵入防御システム-IPS）、エンドポイント対策、重要サーバーの隔離対策、漏洩対策（持ち出しの制御、データの暗号化）等セキュリティ対策を多層化することで、強固な防御網を構築し、情報資産に対する不正アクセス、窃取等のリスクに対応することができます。

2） セキュアデータ連携

EEA 域内・外でのシステム間のデータ交換にも漏えいのリスクは存在するため、高セキュリティ、高信頼性、万が一の際の履歴保全などを備えた堅牢なデータ連携基盤を構築する必要があります。例えば、セゾン情報システムズのファイル転送ツール「HULFT」を使えば、AES 暗号、再転送機能、履歴保全機能などをパッケージとして導入することができます。

3） 仮想デスクトップ

データセンターに仮想デスクトップ環境を構築し、集中管理を行うことにより、クライアント環境のセキュリティを強化します。これにより、ユーザー毎のアプリケーション利用可・不可の設定や、セキュリティパッチ適用を一元的に行うことができ、均一的なセキュリティレベルの維持が可能になります。また、ローカル端末にデータを保持させないことにより、PC 紛失等の事故による情報漏洩を防ぐことができます。

4） ランサムウェア対策

ランサムウェアにデータを暗号化させない仕組みと、バックアップ対策で万が一の事態に備えます。

ランサムウェア被害は最悪の場合、PC を一から再構築し直す等、手数のかかる作業が発生する可能性があり、復旧を迅速に行う為の仕組み作りが有効な対策の一つになります。

5) 汎欧州拠点ゲートウェイ
クラウドベースのプロキシサービスにより、インターネットアクセスの際のセキュリティを強化します。ウェブサイトの閲覧を制限し、組織のセキュリティポリシーに基づく安全なインターネット接続環境を構築することで、悪意のあるウェブコンテンツの脅威を軽減します。

6) Office 365
クラウド型メールセキュリティサービスによるスパムメール検知、防御の仕組みでセキュリティを強化します。

7) データアクセスフォレンジック
ファイルサーバ、アクティブディレクトリサーバ、データベースサーバへのデータアクセスログ取得、分析を行います。セキュリティ対策要件の一つとしてログ管理が必要な場合、その対応が可能になります。また、データアクセスログを分析可能な仕組みを持つことにより、内部不正行為の抑止効果が期待できます。

8) エンドポイントセキュリティ
アンチウィルスソフト、資産管理ソフトの組み合わせでエンドポイントのセキュリティを強化します。また DLP（Data Loss Prevention）機能の利用により、エンドポイントに保存されたデータの外部への漏洩を監視・抑止することができます。

9) 標的型メール攻撃対策
不審なメールに対するセキュリティ意識を高めることを目的とし、ユーザーに標的型メール攻撃を疑似的に体験していただくことにより、知識・理解向上を促進します。

10) セキュリティ講習
企業をとりまく脅威の最新状況等を踏まえ適切な講習を行うことで、ユーザーのセキュリティ意識向上を促進します。

おわりに

GDPR 対応全般に言えることですが、対策と仕組み作りは、各企業のビジネスモデル、取り扱う個人データの利用目的、種類、移転範囲等により対応が異なります。重要なポイントは、それらに照らし合わせて対策や仕組みの実効性が実証可能で、合理性があることです。
このホワイトペーパーでは、GDPR の概要と IT 視点からの対応ソリューションについて記述してまいりました。今後もこのホワイトペーパーを、GDPR 施行後のトピックを交えて発行してまいります。

免責事項

本資料記載の内容は現時点で株式会社セゾン情報システムズと、Newton Information Technology Ltd.が入手可能な情報に基づいて作成しておりますが、GDPR への対応、及び施行後の業務負荷削減を考える上でのご参考という位置付けであり、規則の解釈、適用に関する法的助言を示すものではありません。個人データの取得、処理、移転に関し、いかなるソリューション、サービスの利用も含め、適用される可能性のあるあらゆる法律や規制を、弁護士事務所等の専門家にご相談の上、各企業が理解する必要がございます。

商標関連

- 「Office 365」は、米国 Microsoft Corporation の、米国およびその他の国における商標または登録商標です。
- 「HULFT」その他 セゾン情報システムズの商品またはサービスの名称等は、セゾン情報システムズの商標または登録商標です。
- 「DataSpider」、「DataSpider Servista」、「DataSpider Cloud」は株式会社アプレッソの商標です。
その他の会社名、製品名、サービス名は、各社の登録商標または商標です。

Newton IT Newton Information Technology Ltd.

・電話番号　　：+44 (0)20 8782 1920
・URL(JP)　　：http://www.newtonit.com/ja/
・E メールアドレス：sales@newtonit.com

HULFT
株式会社 セゾン情報システムズ
HULFTフリーダイヤル 0120-80-8620
※利用時間 9:30～17:00(土・日・祝日および年末年始を除く)
URL www.hulft.com e-mail info@hulft.com

HULFT事業部
〒107-0052 東京都港区赤坂1-8-1
赤坂インターシティAIR 19F
TEL 03-6370-2310

中部事業所
〒450-0003 愛知県名古屋市中村区名駅南2-14-19
住友生命名古屋ビル 21F
TEL 052-588-5591 FAX 052-588-5592

HULFT Pte. Ltd.
7 Temasek Boulevard #32-51, Suntec Tower 1
Singapore 038987
TEL +65 6678 6566 FAX +65 6678 6501

Saison Information Systems CO., LTD
EMEA Office
5th Floor, First Central 200, 2 Lakeside Drive
London, NW10 7FQ, United Kingdom

西日本事業所
〒550-0002 大阪府大阪市西区江戸堀1-5-16
肥後橋MIDビル 4F
TEL 06-6479-1151 FAX 06-6479-1152

九州サテライトオフィス
〒812-0011 福岡県福岡市博多区博多駅前2-19-27
九勧博多駅前ビル
TEL 092-434-4527 FAX 092-434-4528

HULFT, Inc.
1820 Gateway Drive,
Suite 120 San Mateo, California 9440480
TEL +1-650-393-4930

世存信息技術(上海)有限公司
中国上海市长宁区天山西路1068号D栋3楼B单元
TEL +86-21-6239-9201 FAX +86-21-6239-9321