SANS SECURITY AWARENESS

コンピュータ利用者のためのマンスリー・セキュリティ・アウェアネス・ニュースレター

GDPR

はじめに

新しく制定された法律であるGDPR、あるいはGeneral Data Protection Regulationについて聞いたことはあるでしょうか。欧州連合によって立案されたこの法律は、2018年5月25日に施行されます。この法律は、世界のどこに所在しているかに関わらず、欧州連合（EU）圏内の全ての住民の個人情報を扱う、全ての企業や団体に適用されます。GDPRはEU圏内の全住民の個人情報について、プライバシーとセキュリティを確保することを企業や団体に要求しています。GDPRへのコンプライアンスを守るためには、重要な原則を理解し導入する必要があります。

誰であれ人はプライバシーの権利を有します。企業や団体は、どの個人データを収集し利用するのか制限を設け、集めたデータを保護することにより、顧客のプライバシーを守る必要があります。プライバシー保護の義務は、欧州連合圏内に住む個人を特定し得るものであれば、単独で、あるいは他の情報と組み合わせて利用される、あらゆる情報に適用されます。そうした情報には、住所、パスポート番号、運転免許証の番号、財政状況、生体認証に利用できる情報、組合加入の有無、既往歴、位置情報、もしくは性的、宗教的、政治的指向に関する情報が含まれるでしょう。規制は「自然人」つまり生存する個人に適用されます。遵守が必要となるGDPRの主な原則のうちいくつかを、次に紹介します。

- 一人一人の個人データは法律に従って、公正に、わかりやすい形で処理されるべきである。
- 個人はどの情報がどのような目的で収集されているのかを、知らされる必要がある。
- 個人データは特定の、明確な、合法な目的で収集されるべきである。個人データはそうした目的以外の、いかなる理由においても利用されるべきではない。
- 個人データは、そのデータが必要とされる期間においてのみ、保管および利用されるべきであり、その期間を過ぎてはならない。
- 個人データは最新および正確な状態で保管されなければならない。

個人は自身のデータのコピーを受け取る権利を持ち、これ以上自身の個人データが利用されないよう、もしくは場合によっては完全に削除されるよう要請することができる。

企業や団体は、偶発的あるいは非合法的な破壊、紛失、改ざん、漏洩から個人データを保護するための適切なセキュリティ対策を導入しなければならない。

また、企業や団体は個人データを扱う全職員が、そのようなデータを安全な状態に保ち、保護するための適切な訓練を受けていることを保証する必要がある。

個人データを安全な状態に保つために導入した対策には、このようなデータがもつ機微な性質に適切な保護レベルが確保されていなければなりません。データに関わるリスクの増大にともない、そのデータを保護する対策にかかる労力や費用は増加するのが当然です。これらの対策は、適切であることを確認するため、定期的に評価、アップデートされるべきです。しっかりと資料化された、プライバシーやセキュリティの決定、対策に関する記録は、GDPRの要求事項へのコンプライアンスを証明することに役立つでしょう。さらに企業や団体は、個人データを外部のサードパーティや、特に欧州連合圏外の第三者に渡す際、その個人データを保護するための、契約やデューデリジェンスの調査といった対策を導入することが法的に義務付けられています。最後に、個人データが漏洩した場合、企業や団体は漏洩を認識してから72時間以内に、漏洩の事実を報告する必要があります。企業や団体がGDPRに従わない場合、最大で世界的に得た利益の4%が科される可能性があり、これによりGDPRは世界で最も財政的なコストが大きい規制の一つとなっている。

日本語版翻訳チーム

日本語版翻訳ーNRIセキュアテクノロジーズ株式会社

NRI セキュアテクノロジーズは、国内でも有数の情報セキュリティ専門企業です。マネージドセキュリティサービス、コンサルティング、ソフトウェアソリューションなどの提供を通じて、情報セキュリティのあらゆる視点からお客様をサポートします。http://www.nri-secure.co.jp

ゲストエディタ

ブライアン・ホナン氏は、アイルランドのダブリンに事業所を構え、サイバーセキュリティとデータ保護を得意とする独立コンサルティング企業BH　CONSULTINGのCEOです。ブライアンは欧州サイバー犯罪センター（EC3）の特別顧問を務めた経歴をもち、アイルランド初のCERTを設立した後、現在は革新的なセキュリティ企業数社において、諮問委員会のメンバーを務めています。また、LINKEDIN (www.linkedin.com/in/brianhonan)やTWITTER（@brianhonan）からも情報を発信している。

リソース

GDPR 個人と企業、団体向け概要:	http://gdprandyou.ie
GDPR規制:	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679
OUCH! Translations and Archives:	https://www.sans.org/u/D88

OUCH!はSANS Security Awareness プログラムによって発行され、Creative Commons BY-NC-ND 4.0 licenseに従って配布されます。 このニュースレターを再配布し、もしくは啓発資料としてご利用いただけますが、コンテンツの改変は認められません。 翻訳その他に関しては、www.sans.org/security-awareness/ouch-newsletter までお問合せください **Editorial Board:** Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | **Translated By:** 内山　貴之, 時田　剛