bsi.

...making excellence a habit.™

ISO/IEC 27018

クラウドにおける個人情報の保護

ホワイトペーパー

はじめに

個人情報保護の重要性はかつてないほどに高まっています。
国際標準化機構 (ISO)、米国政府、欧州連合などの多くの国内組織および国際組織が
この課題を解決するための対策を講じています。
このような組織が共有するひとつの構想が国際規格の ISO/IEC 27018 です。

データ侵害の規模 [1]

3,046,456
– 1日あたり

2,116
– 1分あたり

126,936
– 1時間あたり

35
– 1秒あたり

ISO/IEC 27018 は、パブリッククラウドサービスにおいて個人の特定が可能な情報 (PII) を保護するための実施基準です。この規格は、情報セキュリティ管理策の実施基準として広く利用され順守されている ISO/IEC 27002 をベースに構成されています。ISO/IEC 27018 は、具体的にクラウドサービスの顧客に何を提供するのでしょうか。また、なぜこの規格が重要なのでしょうか。

個人情報の漏洩問題は、最上位の国際的議題です。非常に多数のセキュリティ侵害が明確になっていることから、どのように個人情報を保護すればよいのか人々の関心が高まっています。侵害とその影響を受けた人々の数を表示したリストを見ると、問題の大きさがわかります。米国人事管理局では、2100 万人以上の政府職員のデータが盗まれ、英国では、Carphone Warehouse が攻撃され、200 万人以上の同社の顧客が影響を受けました。これらは、2015 年の 3 か月間に発生した攻撃における氷山の一角に過ぎません。実際、Breach Level Index によると、2015 年には、7 億 750 万ドルのデータ記録が侵害されました [1]。

一方で、企業がセキュリティにかける費用はますます増加しています。IDC のデータによると、全世界の IT セキュリティにかかる費用は、2020 年までに 1016 億ドルに達するとされています [2]。

多くの人々にとって、ハッカーは社会の不適応者というイメージが強いですが、外部からの攻撃のほとんどは巧みな犯罪集団や国家的組織が行っているため、対抗措置を講じることが特に困難になっています。潜伏型のリスク、すなわち、内部関係者が故意または意図せずに、企業が攻撃を受けやすい状態にするというリスクが高まっています。

多くの場合、内部の脅威は報告されなかったり、隠ぺいされたりするため、危険度がより高くなります。Pricewaterhouse-Coopers の調査 [3] によると、従業員が犯したセキュリティ侵害の被害を受けた組織の 75% が、警察を介入させず、告発もしていません。これはすなわち、このような組織の顧客は攻撃を受けやすく、将来このような人材を雇用する企業はその人たちの過去を把握できないが故に、攻撃に対して無防備になるということです。

2016 年上半期のデータ侵害の 64% が個人情報の盗難で占められている [1] ことにより、個人情報保護の方法に強い懸念が寄せられることは当然のことであり、特に、クラウドコンピューティングを使用することとクラウドサービスプロバイダ (CSP) にデータ管理を委託することを恐れるのも当然と言えます。

このような背景から、たとえば、欧州連合は、ヨーロッパ全体の法的状況を統一するために、データ保護に関する新たな規則 (一般データ保護規則:GDPR) を導入しました。欧州に関して言えば、国ごとに異なるデータ保護法があることが、クラウドサービスプロバイダの運用を特に困難にしています。データセキュリティを管轄する法律は国ごとに異なりますが、クラウドコンピューティングを採用することで国々の間の境界がなくなります。

[1] http://breachlevelindex.com
[2] http://www.computing.co.uk/ctg/news/2474455/global-it-security-spending-to-top-usd100bn-by-2020
[3] http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

組織がデータを維持管理する状況も課題の1つです。クラウドサービスプロバイダとは法的責任に違いがあるためです。クラウドサービスプロバイダは顧客に代わってデータを維持管理しますが、そのデータに発生した事項の法的責任は顧客が負います。

実際、ここにクラウドサービスプロバイダに対する不安が集中しています。どのクラウドサービスプロバイダも、自社のセキュリティ技術、データ保護にかける費用、侵害を防止するために設置する物理的障壁について誇らしげに語りますが、クラウドサービスプロバイダが個人の機密データを顧客と同じように取り扱いを行うかという根本的な懸念は消えません。

欧州連合がデータ保護分野の統一を図っている一方で、米国ではまた異なる状況に対処する必要があります。

米国には、個人情報の取り扱い方法を規定する国内法がありません。州によって異なる方針があるため、混乱が生じやすくなっています。法規上の要求内容が、業界によってさまざまであることが、さらに事態を悪化させています。このような要素がすべて重なることで、一貫性のあるデータ方針を構築することがかなり困難になっています。このような不備な状況に対処する取り組みとして、2015 年 8 月、アメリカ国立標準技術研究所（NIST）は連邦機関に対して、「その理念及び方針策定活動において有効かつ適切である場合には、該当する国際規格をサイバーセキュリティに使用する」よう助言しました [4]。米国政府機関がこれらの規格を導入すると、契約業者やサプライチェーンにも順守が求められるようになります。

ISO/IEC 27000 ファミリー規格

ISO は国際的な視点から、情報セキュリティの規格ファミリーを開発してきました。これは、情報セキュリティに関する懸念事項への対処を目的としたプロセスと手順を開発するための枠組みを組織に提供するものです。

このファミリーの中心となる規格が ISO/IEC 27001 です。これは、重要な情報を意図しない配布及び権限のないアクセスから守るための規格として最も広く認められています。ISO/IEC 27001 及びこれに密接に関連する ISO/IEC 27002 には 114 の管理策があり、右記の事項によって、情報の収集、保管、及び流布に伴うリスクを軽減します。

- 有効な情報セキュリティマネジメントシステムの要求事項を提供する
- 組織が、増加する政府の規制と厳しい業界固有の要求事項を順守できるようにする
- 組織が、そのすべての機密情報の機密が保持されることを把握できるようにする

[4] http://csrc.nist.gov/publications/drafts/nistir-8074/nistir_8074_vol1_draft_report.pdf

ISO/IEC 27018 規格

クラウドコンピューティングを使用して個人情報を処理することに対する懸念がますます高まっている状況に対処するため、ISO は 2014 年秋に、新たな規格として ISO/IEC 27018 を策定しました。クラウドサービスプロバイダはこの規格を採用して、データのセキュリティに対する顧客の信頼を改めて確保しようとしています。ISO/IEC 27018 は、ISO/IEC 27001 と ISO/IEC 27002 をベースに策定されたもので、クラウドプロバイダが個人を特定できる情報（PII）をどのように取り扱うのか懸念する組織に対して指針を提供します。

これは、組織にとってやや法的に難しい分野であり、そのために EU GDPR の合意にも長い時間がかかりました。しかし、最初に一部の定義を策定する必要がありました。

最も重要なのは PII そのものであり、この定義によってすべての論議が左右されます。PII は、(a) この情報が関係する PII 主体を識別するのに使用できる情報、又は (b)PII 主体に直接的又は間接的に結び付けることができる情報、として定義されています。

ここで当然、別の疑問が生じます。PII 主体とは何か？という疑問です。一部の国では、これをデータ主体と呼んでいるため、少しわかりにくくなっていますが、個人データが関連する当該個人（本人）のことを指します。同様に、データコントローラとも呼ばれる PII コントローラという用語もややあいまいな用語です。ただ、ここで大事なのは、PII コントローラとは、個人情報が収集及び処理される目的を決定する個人又は組織であるという点です。

ISO/IEC 27018 の内容

この規格には複数の目的があります。ISO の記述に従って、以下にその目的を示します。

- パブリッククラウドサービスプロバイダが PII プロセッサとして機能する場合に、該当する義務に従うようにすること（該当する義務が PII プロセッサに直接課せられる場合も契約によって課せられる場合も含む）
- クラウドサービスカスタマが、適切に管理されたクラウドベースの PII 処理サービスを選択できるよう、関連する事項においてパブリッククラウドの PII プロセッサの透明性を確保すること
- クラウドサービスカスタマとパブリッククラウドの PII プロセッサが契約上の合意に至るのを支援すること
- 複数パーティの仮想サーバ（クラウド）環境で管理されているデータを個々のクラウドサービスカスタマが監査することが技術上現実的でなかったり、それによって設定されている物理的及び論理的ネットワークセキュリティ管理策へのリスクが高まったりする可能性がある場合に、クラウドサービスカスタマに、監査及び法令順守の権利及び責任行使の仕組みを伝えること

これらはまさに原則そのものですが、これらが何を意味するのか、これらが顧客にもたらすメリットは何かという具体的な視点から見ると、パブリッククラウドサービスにおける個人情報処理のための現実的な枠組みが提供されていることがわかります。

ISO/IEC 27018 では、ISO/IEC 27002 に記載されている広範にわたる一連のセキュリティ管理策をベースにして、これらを 2 つのポイントで拡大しています。1 つ目は、既存のセキュリティ管理策を多くの分野に拡大適用し、クラウドサービスカスタマとクラウドサービスプロバイダ間の責任の分担を処理できるようにした点です。2 つ目は、新しい一連のセキュリティ管理策を追加し、プライバシーの枠組みに関する規格である ISO/IEC 29100 で定義されているプライバシー原則を反映するようにした点です。拡大されたセキュリティ管理策の例を示します。

- 保管時及び着脱可能な物理的媒体での PII の暗号化に関する要求事項
- データが不要になった場合に、指定した期間内に PII を削除すること
- クラウドサービス契約に明示的に記載されている目的でのみ該当する PII を処理すること
- PII の検証及び修正における PII 主体の権利の行使に協力すること（多くの規制で規定されている）

ISO/IEC 27018 の採用によって、クラウドサービスプロバイダは、PII 処理に適切な手順を確実に導入することができます。また、より強固なクラウドサービス契約を策定するのにも役立ちます。この規格は、クラウドサービスプロバイダが PII に関して従業員をどのように教育訓練するか、どの文書の手順が必要かを規定し、順守すべき指針を提供します。

ISO/IEC 27018 の目的は、個人情報のセキュリティと保護に関してクラウドサービスプロバイダが行う内容を、クラウドサービスカスタマが明確に把握できるよう、顧客に対して真の透明性を確保することです。

この規格を導入する際に組織が特に留意すべき点は、下記の 3 点です。

- 業界固有の規則や規制など、組織が順守すべき既存の法的要求事項はないか
- ISO/IEC 27018 を順守することで組織のリスクが増大することはないか
- 規格を採用する場合に、組織の企業方針及び企業文化を変更する必要はないか

おわりに

クラウド業界が、適切かつ有効な情報セキュリティを提供するために標準化を必要としていることは疑いようのない事実です。2015 年の TrustE の調査によると、英国のオンラインユーザの 92% が自身のプライバシーに懸念を感じています[6]。最大の懸念は、オンラインで収集された自身に関する個人情報がどのように使用されるのか、複数の企業が個人情報を共有する可能性があるのかわからないということです。顧客の要求がますます増大する中で、企業はオンラインデータの収集、使用、及び保護おける透明性をさらに高めていく必要があります。

ISO/IEC 27018 の採用によって、業界は PII 保護のためのセキュリティ向上への取り組みを集中的に行うことができます。この規格はすでに一部の主要クラウドプロバイダに支持されています。Microsoft Azure、IBM Softlayer、Google Apps for Work、Amazon Web Services、Dropbox のすべてが ISO/IEC 27018 の認証を取得しています。さらに多くのクラウドサービスプロバイダがこれに続くと予想されます。組織は技術をより柔軟に活用し、資源の需要を抑えるというメリットを享受するために、情報処理のクラウドサービスへの移行をより一層進めていくと思われますが、セキュリティ、特にプライバシーに関する懸念への対処に際しては、組織の上層部での受入態勢が整うまでとなるでしょう。

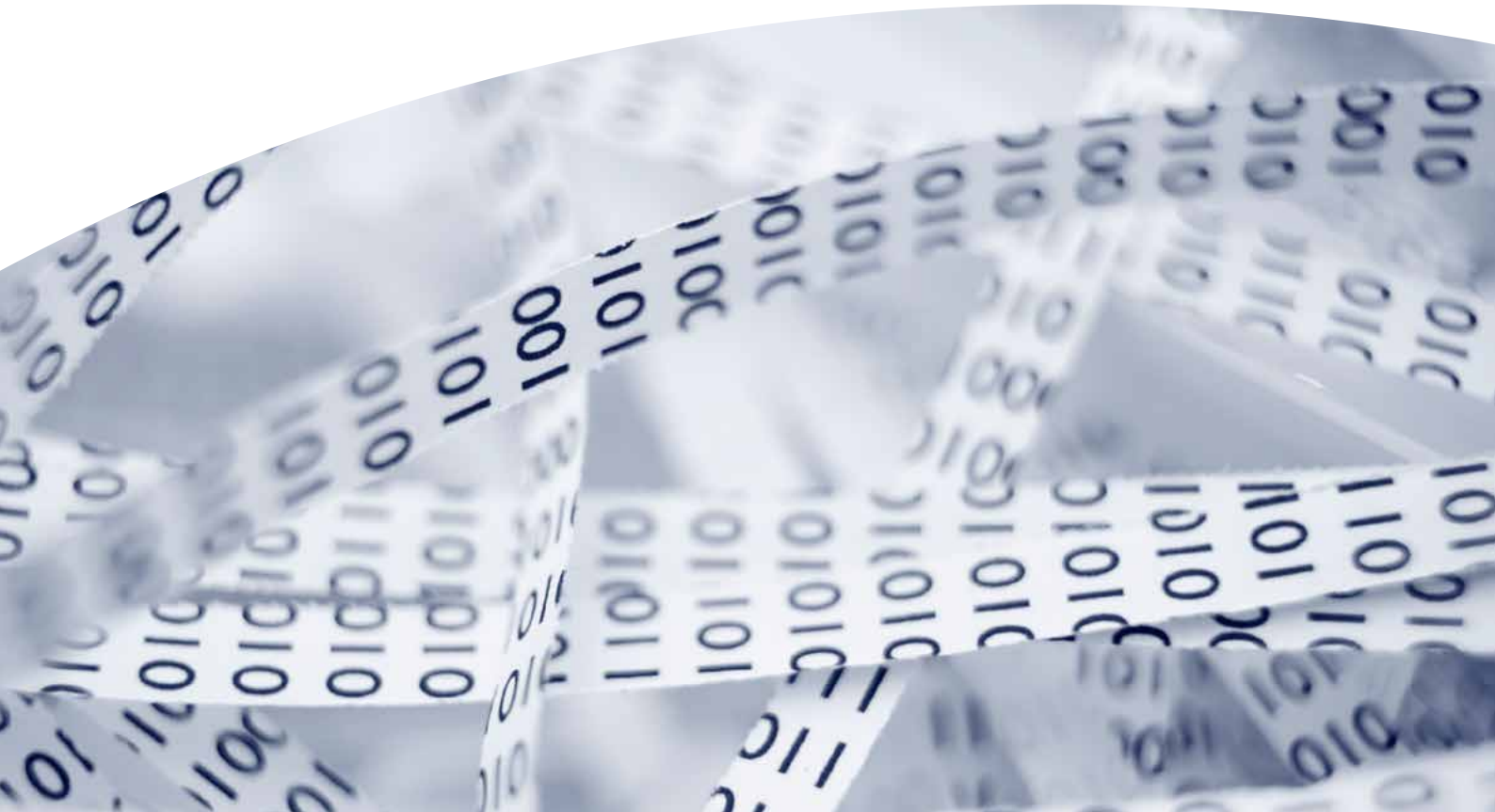
欧州 GDPR により、プライバシーに対する新たなアプローチが大きな関心事になると考えられます。

[6] https://www.truste.com/about-truste/press-room/british-customers-online-privacy-more-important/

ISO/IEC 27018 は、顧客の PII だけでなくクラウドサービスプロバイダの PII も適切に保護するための一連の指針を提供します。

ISO/IEC 27018 は、国内法規および国際法規に代わるものではありません。広く採用されますが、これによってプロバイダが自動的に法的事項を順守するということではなく、その行程の重要な一歩であることを意味しています。

データ保護支援に
関する BSI の
ソリューションについては
bsigroup.com/ja-JP を
ご覧ください。



Why BSI?

By Royal Charter

BSI は、常に ISO/IEC 27001 の最前線に立ってきました。
1995 年に BSI が開発した BS 7799 に基づいて、
BSI は ISO/IEC 27001 の開発と ISO 技術委員会に関与してきました。
また、とどまることなくサイバーセキュリティやクラウドセキュリティといった
新たな喫緊の課題に対して取り組んできました。
故に、BSI はお客様の新たな規格への移行を支援するにあたって、ベストパートナーに成り得るのです。
BSI は、規格を通じてお客様のビジネスの成功をけん引し、より卓越したビジネスの創造を目指しています。
私たちは、より良いパフォーマンス、リスクの管理、持続的な成長を後押しします。
BSI のエキスパートたちは、1 世紀以上に渡り、より卓越した方法を人々や製品に根付かせるため、
凡庸であることや現状への満足、自己満足に対して常に挑戦し続けています。

BSI の製品及びサービス

私たちは、サポート製品とサービスのユニークな組み合わせを、
知識、保証、コンプライアンスという 3 つの流れのなかでご提供しています。

知識

BSI は、ビジネスエキスパート、政府機関、事業者団体、
消費者グループと協力し、組織が成功するうえで必要な
ベストプラクティスを見つけ、知識を構築しています。
ISO 9001（品質マネジメント）及び ISO/IEC 27001
（情報セキュリティマネジメント）など、
広く利用され、実施されている国際規格の多くは、
もともと BSI が策定したものです。

コンプライアンス

お客様が実際に長期的なベネフィットを享受するためには、
法規制、マーケットニーズ、規格を順守する必要があり、
それを継続することで規格の順守は確固とした習慣になります。
付加価値及び差別化されたマネジメントツールを
提供するだけでなく、お客様が規格やその実施方法を
理解するのに役立つトレーニングも実施することで、
私たちは規格の継続的な順守プロセスをお手伝いしています。

保証

プロセスや製品が特定の規格に適合していることを
証明する独立した評価を通じ、
お客様のパフォーマンスの卓越性が保証されます。
私たちは、お客様が自らのパフォーマンスを
理解するお手伝いをすることで、
組織の内側からできる改善分野を洗い出します。

最新情報は下記Websiteをご覧ください。
www.bsigroup.com/ja-JP/

bsi.

BSI グループジャパン株式会社
T: +81 (0)3 6890 1172
www.bsigroup.com/ja-JP/