CLOUD SECURITY ALLIANCE

GDPR 準拠の為の行動規範

CSAJC cloud security alliance SM Japan Chapter

CSA cloud security alliance®

ABOUT & ACKNOWLEDGMENTS

The Cloud Security Alliance (CSA) Code of Conduct (CoC) for GDPR Compliance has been developed within CSA by an expert Working Group (WG) chaired by Prof. Dr. Paolo Balboni (Founding Partner of ICT Legal Consulting; Professor of Privacy, Cybersecurity, and IT Contract Law at the European Centre on Privacy and Cybersecurity within the Maastricht University Faculty of Law; President of the European Privacy Association) and Francoise Gilbert (Partner, Greenberg Traurig; co-chair PLI Privacy and Security Law Institute; author and editor of Global Privacy and Security Law). Prof. Dr. Paolo Balboni is also the
main author of the PLA. Daniele Catteddu and Eleftherios Skoutaris greatly contributed to the document creation.

The PLA WG is composed of representatives of cloud service providers, local supervisory authorities and independent security and privacy professionals.[1]

We would also like to thank CSA staff, Hillary Baron, Daniele Catteddu, Damir Savanovic, Kendall Scoboria, and Eleftherios Skoutaris for their support and contribtion.

Our sponsors Gemalto and Shellman have also greatly contributed to the publication of this document.

[1] Part 3 of this document, i.e. PLA CoC Governance, has been developed thanks to the contribution of the European Commission-funded project European Security Certification Framework (EU-SEC).

COPYRIGHT NOTICE

日本語版提供に際しての告知及び注意事項

本書「GDPR 準拠の為の行動規範」は、Cloud Security Alliance (CSA)が公開している「CODE OF CONDUCT FOR GDPR COMPLIANCE」の日本語訳および一般社団法人日本クラウドセキュリティアライアンス（CSAジャパン）が解説を加えたものです。本書は、CSAジャパンが、CSAの許可を得て翻訳し、公開するものです。原文と日本語版の内容に相違があった場合には、原文が優先されます。
翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSAジャパンは何らの保証をするものではありません。
この翻訳版は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください(文中で記載したURLは2017年12月25日現在で確認されたものです)。

変更履歴

日付	バージョン	変更内容
2018 年 8 月 1 日	日本語版 1.0	初版発行

日本語版作成に際しての謝辞

「GDPR 準拠の為の行動規範」の日本語訳は、CSAジャパンの「クラウドプライバシー・ワーキンググループ」に参加するメンバーを中心とした、CSAジャパン会員の有志により行われました。
作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。
以下に、翻訳に参加された方々の氏名および所属先（企業会員からの参加の場合のみ）を記します。（氏名あいうえお順・敬称略）
笠松 隆幸
柏浦 謙一
勝見 勉
小貝 隆
サルギシャン・アレクサンドル： ファイルフォース株式会社
新貝 知晃： 株式会社日立システムズ
谷本 茂明
羽田野尚登
守屋 有晶
諸角 昌宏
山崎 万丈

目次

本書で使用されている用語の説明

原文	日本語訳および注釈
CoC	行動規範
CoP	実践規範
Subcontractor	契約先
subprocessor	再委託先処理者
Cloud Provider, Provider	CSP に統一する
CSP	英語のまま（ただし、内容により事業者とする）
customer	利用者
PLA	英語のまま（Privacy Level Agreement）
PLA CoC	PLA 行動規範
PLA CoP	PLA 実践規範
CSA CoC	CSA CoC(PLA [V3])に統一
EU 内	EEA の範囲で使用する（EU＋ノルウェー、アイスランド、リヒテンシュタイン）を意味する

I. 序論

データ保護のコンプライアンス(法令順守)は、リスクベースになってきている。データの管理者(Controller)および処理者(Processor)は、彼らが処理する個人データの適切な保護レベルを組織内で決定し実施する責任を負う。その決定においては、最先端技術、実装費用、データ処理の性質、範囲、内容および目的を勘案し、また自然人の権利及び自由に対する主張の可能性および深刻さが変動するリスクを考慮する必要がある。その結果、クラウド事業者（CSP）は、彼らが処理する個人データに求められる保護レベルを自ら決定する責任を負う。

このようなことから、クラウドセキュリティアライアンス（CSA）は、欧州の一般データ保護規制（GDPR）準拠のためのCSA行動規範（CoC）を作成した。

CSA GDPR準拠の為の行動規範(CSA CoC(PLA[V3])は、CSPとクラウド利用者にGDPR準拠のためのソリューションを提供し、CSPが提供するデータ保護レベルに関する透明性ガイドラインを提供することを目指している。

CSA GDPR準拠の為の行動規範(CSA CoC(PLA[V3])は、実質的に以下を提供するものである:

- あらゆる規模のクラウド利用者向けの、異なる複数のCSPによって提供される個人データ保護レベルを評価するツール（それゆえ、情報に基づく意思決定を支援）
- あらゆる規模および所在場所のCSPにとっての、欧州連合(EU)の個人データ保護の法令に遵守し、利用者に提供している個人データ保護レベルを、体系化された方法で明示するためのガイダンス。

CSA GDPR準拠の為の行動規範(CSA CoC(PLA[V3])は、GDPRに含まれる要件を規定する技術標準であるプライバシーレベル契約実践規範（PLA CoP）と、それに関連する認証スキームおよび遵守メカニズムの2つの主要コンポーネントに基づいている。

CSA GDPR準拠の為の行動規範(CSA CoC(PLA[V3])は、主に法的要件に重点を置いているため、Cloud Control Matrix（CCM）やSTAR認証（またはSTAR評価証明またはSTARセルフアセスメント）などの他のCSA作成の実践規範および認証と組み合わせてこの規範を採用することを提案し、情報セキュリテ

ィの技術的な制御と目的に関する追加ガイダンスを提供する。

このような状況において、Cloud Control Matrixまたはそれと同等のもの（例えば、ISO 27017またはISO 27018による補完を伴うISO 27001、またはAICPAのTRUSTサービス基準）といった情報セキュリティの技術標準の採用や、それらに関連する認証スキーム（例えば、STAR認証、STAR評価証明、STARセルフアセスメント、ISO 27001、またはSOC2）は、CSPがセキュリティプログラムまたは情報セキュリティ管理システム（ISMS）を実装し、これらのリスクアセスメントおよびデータ保護影響評価（DPIA）で概説された脅威から利用者のデータを適切に保護している証拠を提供する。

CSA GDPR準拠の為の行動規範(CSA CoC(PLA[V3])は、GDPRのクラウド分野に関連する要件を反映し、CSA Security, Transparency and Assurance Registry（STAR）の一部を構成する。

CSA GDPR準拠の為の行動規範(CSA CoC(PLA[V3])の対象読者には、 CSP、クラウド利用者と潜在利用者、クラウド監査者、およびクラウドブローカーのように、クラウドコンピューティングおよびEUの個人データ保護法制に関心のあるすべての利害関係者が含まれる。

最後に、CSA GDPR準拠の為の行動規範(CSA CoC(PLA[V3])に対するいかなる認証も、管理者（Controller）または処理者（Processor）がGDPRを遵守する責任を軽減するものではなく、国のデータ保護機関（DPA）の任務および権限を損なうものではないことに注意することが重要である。

II.背景

“Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union (PLA [V1]”（EU内のクラウドサービス販売用PLA枠組み）は2013年2月に自主規制の調整用ツールとして発表され、クラウドサービス事業者（CSP）が得意先および潜在顧客に対して個人データの保護レベルを伝達するための体系化された方法を提供するものであった。PLA [V1]は、EUの法的要請のみならず実践規範や推奨事項をベースとしていた。

PLA [V1]は多数のEUの監督当局からお墨付きを得、クラウドコンピューティングにおける個人データ保護に関するEUの研究、実践規範、実施項目の開発作成に際して活用され参照された。

しかし、PLA [V1]のリリース後、PLAのワーキンググループは、CSPもその顧客も潜在顧客も依然として、EU全体にわたる個人データ保護に必要なベースラインを探り当てるための模索を続けているとの認識に至った。

その結果、PLAワーキンググループはPLA [V2]を作成し、クラウドコンピューティング市場への様々な参加者に対して、単なる「見える化」の仕組みを用意するだけでなく、法令順守のためのツールを提供することにした。

PLA [V2]は実在するEU個人データ保護指令準拠法令（すなわちDirective 95/46/ECとそれのEU参加国における実適用）のみをベースとしたものとした。

2016年5月にREGULATION (EU) 2016/679 ("GDPR”)が発効し、2018年5月25日以降すべてのEU参加国において直接適用されることになった。PLAワーキンググループとしては、CSP、その顧客および潜在顧客がクラウド環境において新しい法を遵守するための新しいガイダンスを必要とすることは自明のことであった。従い、PLAワーキンググループはGDPRに盛り込まれた新しい義務を反映した、順守のためのツールであるPLA [V3]を開発した。

PLAはプライバシーとデータの保護が目に見える形で保証され、法令が順守されていることを担保するためのCode of Practice（実践規範）と理解すべきである。

PLAの実践規範の現行のバージョン、すなわち[V3]は、権限を有する公的機関が法規制、意見、ガイドライン、推奨事項等を発行した場合に、それらに基づいて必要となるのに応じて改訂される予定である。

したがって、PLA [V3]はその設計上、現行のEU個人データ保護指令の要件（即ちDirective 95/46/ECとそのEU参加国における実適用）にPLA [V2]の構成を生かすことで対応し、同時にGDPRによって規定される将来の法的要求事項との継続性を持たせている。

PLA は、CSP、その顧客および潜在顧客が新旧のEUデータ保護体系の間での移行に対応し、GDPRをクラウドの世界に適切に適用することを支援する構成となっている。

PLA [V3]は、クラウド環境に対するGDPRの適用に関して、主として以下の項目について規定している:

1. 公正で透明なデータ処理;
2. 公開向けおよびデータ主体向けの情報提供（GDPR4章(1)の規定による）;
3. データ主体の権利行使;
4. GDPR第24、25条の規定に対応した手段と手続きならびにGDPR第32条に規定された処理のセキュリティを確保するための手段;
5. 個人データ漏えいに際しての監督当局への通知（GDPR4章(21)の規定による）およびデータ主体への連絡
6. 第三国への個人データの移転。

更に、PLA [V3]は、GDPR第41(1)に定める組織が、データ管理者または準拠を請け負ったデータ処理者がその規定を順守していることを監視する義務を、GDPR第55、56条に基づいて所管の監督当局が行う業務とその強制力を損なうことなく、果たすための仕組みも盛り込んでいる。

これらのことから、PLA 実践規範（本書第2部）およびガバナンスの章（本書第3部）は、GDPR第40条（“PLA Code of Conduct” または "PLA CoC”）に基づく”Code of Conduct”のドラフトの要件を満たしている。

III. CSA CoC for GDPR Compliance(PLA[V3])の構造

CSA GDPR準拠の為の行動規範(CSA CoC(PLA[V3])（この文書では、「CSA行動規範」、「CoC」または「規範」とも呼ばれる）は、次の3つの部分で構成されている:

- 第1部では、範囲、目的、範囲、方法論、前提条件について説明する。解説を提供する。
- 第2部では、CSA PLAワーキンググループによって策定されたPLA実践規範[V3]とその主要な規定について、説明する。
- 第3部では、ガバナンスの構造とCSA行動規範の遵守の仕組みを概説する。

第1部

CSA行動規範の目的、対象範囲、方式、想定、解説

1. CSA CoCの目的

1. CSAのCoCはクラウドサービス契約の付録として参照および使用し、CSPが提供するプライバシー保護のレベルを記述したものである。サービスレベルアグリーメントは一般的に、サービスのパフォーマンスに関する計測手段およびその他の情報を提供するために使用されるが、一方CoCは、情報のプライバシーおよび個人データ保護の実施事項に対応する。
2. CoCによって、CSPは、データ処理について維持することを請け負っている、プライバシーやデータ保護のレベルを明確に記述できる。
3. CoCが世界的に採用されることで、強い影響力を持つ世界的な業界標準を推進し、協調を高め、適用されるEU内のデータ保護に関する法律への順守を実現することができる。
4. 結局のところ、CoCは、次の事を提供することを意図している:
    - クラウド利用者や潜在的な利用者に対して（規模の如何によらず）：異なるCSPによって提供される個人データ保護のレベルを評価するツールであること（それゆえ、情報に基づく判断を支援できる）
    - CSPに対して（規模の如何によらず）：EU個人データ保護法令に準拠するためのガイダンスであり、CSPが顧客へ提供する個人データ保護レベルを構造化した方法で開示できること。

2. 範囲及び方法

本規範はクラウド利用者が個人より企業であることを勘案し（企業対消費者間取引（BtoC）ではなく）企業間取引（BtoB）のみを取り扱う。本規範は利用者の状況について2つのケースを対象とする:

- クラウド利用者がデータ管理者であり、CSPがデータ処理者であるケース
- クラウド利用者とCSPの両者が管理者であるケース

[解説]

CSPがSaaS事業者の場合は、データ主体との同意の取得等で直接的にBtoCの取引を行う場合、2章を参照して戴きたい。

本規範の開発者として、PLAワーキンググループは、複合的/ハイブリッドな状況（例えば、CSPが共同のデータ管理者である、あるいはクラウド利用者およびCSPがどちらもデータ処理者である場合）は本規範の対象外であると認識しているので、行動規範の利用者が、ケースバイケースベースで関係者のそれぞれのプライバシー上の役割を慎重に評価し、関連する義務を明確に特定することを推奨する。複合的/ハイブリッドな場合には、PLAの実践規範 (CoP）（すなわち、本規範の元となる技術基準）は付録１のPLA[3]テンプレートの“CSPがデータ管理者”あるいは“CSPがデータ処理者”の欄にすでに明確に識別された関係者のそれぞれの義務を具体的に割り当てるために有効なツールである。

本行動規範は以下のガイドライン等を考慮対象としている：29条データ保護作業部会のデータ移転（データ・ポータビリティ）権利（A.29WP242/16-rev.01）に関するガイドライン、データ保護オフィサーに関するガイドライン（A.29WP243/16-rev.01）、データ保護影響評価(DPIA)および2016/679[16] (A.29WP248/17-rev.01)規制に照らして「処理が高いリスクをもたらす可能性」があるかどうかの判断に関するガイドライン、主な監督機関に関するガイドライン (A.29WP244/16-rev.01)、行政罰金の適用お

よび決定に関するガイドライン(A.29WP253/17)、2016/67919の規則の下での個人データ侵害通知に関するガイドライン (A.29WP250/17-rev.01)、2016/67920の規則の目的のための個人の自動的な意思決定およびプロファイリングに関するガイドライン(A.29WP251/17-rev.01)、2016/67921の規則の下での透明性に関するガイドライン(A.29WP260/17-rev.01)、クラウドコンピューティングについての意見05/2012 (A.29WP05/2012)、デジタルサービス事業者のための最低限のセキュリティ対策を実施するためのENISA技術ガイドライン (ENISA Guidelines February 16, 2017)。したがって、本行動規範は該当するEU個人データ保護フレームワークの法規定に基づいているだけでなく、欧州監督当局による関連する解釈ならびに関連する機関が作成した実践規範も反映している。本規範は、異なるセクターやドメインに渡りEU内個人データ保護に関する法律に準拠するために利用できる汎用的なツールを目指している。PLAワーキンググループは、EU参加国がGDPRに対して除外または減免、より具体的な規制、追加の要求条件を加える可能性を理解し、また特定サービス向けのEU内個人データ保護規定（すなわち、プライバシーと電子通信に関する指令およびネットワーク・情報システムズ指令）が存在することを知っている。そのために、PLAワーキンググループは、本規範の利用者が参加国/業界特有の追加要件を付加することを勧めている。本行動規範はISO/IEC 27018,クラウドサービスレベルアグリーメント標準化ガイドライン、行動規範に関するクラウド事業者団体（Cloud Select Industry Group）による活動成果、欧州クラウドインフラサービス事業者(CISPE)により開発された資料、クラウド説明責任プロジェクトを考慮しながら作成された。

本規範は、クラウド分野に関するGDPRの要求条件を反映しており、GDPRの地理的適用範囲を対象にしつつも、PLA CoPはEUの地域を超えて適用できる。

本CoCのターゲット層は　クラウドコンピューティングと欧州個人データ保護法制の領域のすべての関係者（ステーク・ホルダー）であり、そこにはCSP、クラウド利用者および潜在的利用者、クラウド監査人、クラウドブローカーなどが含まれる。

3. 推奨

クラウドサービスの提供に関する契約を締結する前、あるいはGDPR要件に照らしてそのような契約を見直す必要がある場合、すでにクラウドを利用している利用者および潜在的なクラウド利用者は、内部および外部のデューディリジェンスを実施することが推奨される。たとえば、以下のような内容になる:

- 内部デューディリジェンスは、クラウドサービスを利用することに伴って起きる、またはその利用を妨げる、制限や制約（たとえば、データ主体がクラウド上で処理したいデータタイプのために、クラウドは価値のあるソリューションであるか？）を発見することができる
- 外部デューディリジェンスは、クラウド事業者の提案内容が利用者の内包するニーズとコンプライアンス義務を満たしているかどうかを判定する。CSPが提供する個人データ保護のレベルを評価するのに役立つ。たとえば、提案してきたCSPの水準が、企業自身が決定したものであれ、または適用法で要求されているものであれ、企業が必要とするプライバシーおよびデータ保護のレベルおよび適用されるEU法に対するコンプライアンスの水準を提供しているか？について。

3.1 クラウド利用者の内部デューディリジェンス

内部デューディリジェンスの一環として、個人データをクラウドに移行しようとするデータ主体は、とりわけ次のことを考慮する必要がある:

1. セキュリティ、データ保護、コンプライアンス要件の定義.
2. どのデータ/プロセス/サービスをクラウドに移行するかの特定
3. 既存の契約、適用される法律、規制、ガイドライン、ベストプラクティスなどの、独自の内部セキュリティおよびプライバシー/データ保護ポリシーおよび個人データの使用に関するその他

の制限のレビュー

4. リスクの分析と評価（例えば、GDPR第35条で要求される範囲でデータ保護の影響の評価を実施する）
5. クラウド内での処理における、従業員または顧客の個人データの適切な保護のために必要な、または有益なセキュリティ管理策と認証の特定
6. セキュリティ管理策を実装する責任とタスクの決定（つまり、どのセキュリティ管理策が組織の直接のガバナンス下にあり、どのセキュリティ管理策がCSPの責任であるかの把握）
7. クラウド利用者がモニタの対象とすべきクラウド事業者の行為とその方法（たとえば、オンサイト訪問が必要か、または第三者からの証明書または評価証明に依拠できるか）

3.2 クラウド利用者の外部デューディリジェンス

クラウド利用者は、提案されたCSPの実践についてデューディリジェンスの実施を検討する。これは、とりわけ次のことを含む:

1. PLA 実践規範を使用して、クラウド事業者-（再）委託先/処理者を含む-が、プライバシーおよびデータ保護に関してクラウド利用者の要件を満たすかどうかの評価
2. CSPが、独立した第三者評価に基づく、適用すべき認証または評価証明を保持しているかどうかの判断
3. CSPによって実装されたセキュリティ管理および実践規範に対する可視性の有無、モニタリング能力およびそれらを実施する方法の把握

4. 解説

CSPは、提供するサービスの種類、異なる製品や、異なる慣習または参入している市場に応じて様々な行動規範を提供することができる。

さらに、本行動規範は、提供されるクラウドサービスが特定する対象と時間枠、クラウド事業者による個人データの処理の方法と目的、および処理される個人データの種類を明確にするために、尤度を持たせ、または他の文章にて言及することがある。そのような情報は、とりまとめてクラウド利用者との間で合意されなければならない。

重複を避けるため、マスターサービス契約、サービスレベルアグリーメント（SLA）またはクラウドサービスのための契約の一部であるその他の文書の適切な規定への参照を行うこともできる。例えば、通常、SLAにはデータセキュリティに関する情報が含まれている。文書間の相互参照を利用することは、クラウド利用者とCSPの双方にとって物事をシンプルにすることを意図している（クラウド利用者を迷わせるということではなく）。明瞭性と透明性が重要である。

第2部

PLA実践規範

本書の第2部は、付属書1:PLA[V3]テンプレートと合わせて利用されたい。

PLA実践規範の要求事項の記述においては、それがデータ管理者としてのクラウド事業者に適用される場合は[C]で示し、データ処理者としてのクラウド事業者に適用されるときは[P]で示し、その両方に適用される場合は[C&P]でしめす。

データ処理者がデータ処理の目的と手段を選ぶ場合には、データ処理者はその処理に関してはデータ管理者とみなされることに注意。

1. コンプライアンスと説明責任についてのCSPの言明

CSPはクラウド利用者に対し以下のことを言明する:

1. 適用されるEU内のデータ保護法ならびに技術的・組織的セキュリティの条項を遵守する。また、データ主体の権利をセーフガードにより保護する; **[C & P]**
2. 適用されるEU内のデータ保護法を順守していることを示すことができる（説明責任）。**[C & P]**

[解説]
説明責任（accountability）とは、データ管理者が幅広く管理を行い、データ保護原則が実践として順守されていることを確保する立場にあることを確かめることを目的とした原則である。説明責任は、データ管理者が、内部メカニズムとコントロールシステムを導入してコンプライアンスをするとともに、監査レポートなどのエビデンスを提供することで、監査当局を含む外部ステークホルダーに対して法令順守を実証することを要求している。（引用: European Data Protection Supervisor (EDPS) (2012), Glossary of terms, https://edps.europa.eu/data-protection/ data-protection/glossary_en#accountability.）

CSPはクラウド利用者に以下の事項を文書で示す:

3. CSP自身、再委託先(Section 3.3, “委託先事業者” 参照)、または事業場の連携先がコンプライアンスを示し保証するために、クラウド事業者がどんなポリシーや手順を設定しているか。 **[C & P]**

CSPは以下を明示する:

4. 上記の法令順守を証明する証拠となる事項。証拠となる事項は、様々ない形式をとる：自社による認証/評価証明、第三者監査（例：認証、評価証明、シール）、ログ、監査証跡、システム保守記録、より一般的な運用に関するシステム記録や、責任範囲下にある全ての処理操作の記録文書など。これらの事項は、以下のレベルにおいて提供する必要がある:
   i. 組織的ポリシーのレベルにおいて、ポリシーが適正で適切であることを示す;
   ii. ITコントロールのレベルにおいて、適切な管理策が展開されていることを示す；
   iii. 運用レベルにおいて、計画通りにシステムが稼働していることを示す。

異なるレベルに対応する証拠となる事項の例は、データ保護に関する認証、シール、マークである。
[C & P]

2. CSPに関する接触の窓口とその役割

CSPは、クラウド利用者に次の事項を明確にする:

1. CSPの身元及び窓口の詳細（例：名前、住所、電子メールアドレス、電話番号、及び拠点の場所）; **[C & P]**
2. CSPの知識における代理人（例：EU域内の代理人）の身元及び窓口の詳細（例：例：名前、住所、電子メールアドレス、電話番号、及び拠点の場所） **[C & P]**
3. 関連する処理におけるデータ保護のための役割（例：管理者、共同管理者、処理者、又は処理者の再委託先）**[C & P]**
4. データ保護責任者（DPO）の連絡先の詳細、または、DPOがいない場合は、利用者が要請を行うプライバシー問題の管理責任者の窓口の詳細; **[C & P]**
5. 情報セキュリティ責任者（ISO）の連絡先の詳細、または、ISOがいない場合は、利用者が要請を行う、セキュリティ問題の管理責任者の窓口の詳細 **[C & P]**

【備考】

- EU域内の代理人の必要性については、GDPR 第27条「EU 域内に拠点のない管理者又は取扱者の代理人」を参照。
- データ保護オフィサー（DPO）については、GDPR 第4節「データ保護オフィサー」（第37条～第39条）に、データ保護オフィサーの指名、地位、及び業務について規定されている。

3. データを処理する方法

3.1 一般的な情報

データ管理者であるCSPは、次の点についてクラウド利用者に詳細情報を提供する:

1. 処理に関連する個人データのカテゴリ; **[C]**
2. データ処理の意図した目的と、合法的な方法でそのような処理を実行するために必要な法的根拠 **[C]**
3. データの取得者または取得者のカテゴリ; **[C]**
4. 個人データへのアクセスおよび修正または削除を要求する権利、データ主体に関する処理の制限を要求する権利、またはデータ処理に反対する権利、そしてデータの可搬性の権利を有すること **[C]**
5. 該当する場合には、CSPが第三国または国際組織に個人情報を移転しようとしている状態において欧州委員会からの妥当であるとの判断が得られていないという事実、もしくは十分もしくは適切な保護が行われているという情報と、そのコピーを入手する手段もしくはその情報が得られる場所に関する情報; **[C]**
6. 個人データが保管される期間、または期間の明示が不可能な場合は、その期間を決定するために使用される基準; **[C]**
7. 処理が同意に基づいている場合、撤回前の同意に基づく処理の合法性に影響を与えることなく、同意を取り消す権利の存在;**[C]**
8. 監督機関（GDPR第4条（21）に定義されている）に苦情を提出する権利; **[C]**
9. 個人データの提供が、法的または契約上の要件であるか、契約を締結するために必要な要件であるかについて。併せて、データ主体が個人データの提供を義務づけられているかどうかと、個人データを提供できない場合に生じうる結果; **[C]**
10. プロファイリングを含め自動化された判断が行われること、およびそのロジックに関する意味

のある情報、ならびにデータ主体にとってのそのような処理の影響度合いと想定される結果; **[C]**

11. 個人データが収集されている目的以外の目的のためにクラウド事業者が個人データをさらに処理しようとする場合、当該の更なる処理に先立って提供される、その別の目的のための情報; **[C]**

12. 個人データがデータ主体から得られたものではない場合には、その情報の入手源、そして該当する場合には、公開の情報源から得られたものかどうか。 **[C]**

13. 合意されたクラウドサービスの提供のためにとられた行為（例えば、データストレージ）、クラウド利用者の要求で行われた行為（例えばレポート作成）、CSPのイニシアチブで行われた行為（バックアップ、災害復旧、不法行為モニタリングなど）。 **[C]**

【備考】

- 提供すべき情報については、GDPR第13条及び第14条等に規定されている。
- GDPR第9条においては、特別な種類（カテゴリ）の個人データの取り扱いが規定されていて、当該データを取り扱う場合には同意が必要になるなど、注意を要する。

データ処理者であるCSPは、次のような情報をクラウド利用者に提供する:

14. クラウド利用者であるデータ管理者が、CSPであるデータ処理者に拘束力のある指示をすることができる範囲と様式。 **[P]**

CSPは、クラウド利用者に以下を示す:

15. 関連するクラウドサービスに関する、機能の実装や削除などの関連する変更について、クラウド利用者にどのように通知するか。 **[C & P]**

3.2 個人データの所在場所

CSPは、以下をクラウド利用者に示す:

1. 個人データが処理されるすべてのデータセンターまたはその他のデータ処理の場所（国単位）および、特に、データの保存、ミラーリング、バックアップ、および復元が行われうる場所（これはデジタル手段と非デジタル手段の両方を含む）。 **[C & P]**

3.3 委託先事業者

CSPは以下を明示する:

1. データ処理に参加する契約者および再委託先処理者。データ保護要件が満たされていることを確実にするための説明責任と実施責任の連鎖についての情報を含む。 **[C & P]**

CSPはクラウド利用者に以下を宣言する:

2. CSPは、クラウド利用者の特定の又は包括的な書面による許諾なしに、別の処理者を使用しないこと。 **[P]**

CSPはクラウド利用者にCSPが以下であることを宣言する:

3. 契約（または他の拘束力のある法的行為）により、CSPとクラウド利用者の間で定められたのと同等のデータ保護義務を他の処理者にも課す。特に、EU内の適用法の要件を満たすような方法で適切な技術的および組織的措置を実施することの十分な保証の提供を含めて; **[P]**

4. 他の処理者がデータ保護義務を履行しない場合、当該他の処理者の義務の履行について、クラウド利用者に完全に責任を負う。 **[P]**

CSPは以下を明示する:

5. 委託先事業者または再委託先処理者の追加または変更について、クラウド利用者に通知するための手順。クラウド利用者は、変更の拒否や、契約を終了する権利を常に保持すること。**[C & P]**

3.4 クラウド利用者のシステムへのソフトウェアのインストール

CSPはクラウド利用者に以下を示す:

1. サービスの提供にあたって、クラウド利用者のシステムにソフトウェア（ブラウザプラグインなど）のインストールを必要とするかどうか。**[C & P]**
2. データ保護およびデータセキュリティの観点からの当該ソフトウェアの影響。 **[C & P]**

3.5 データ処理契約（またはその他の拘束力のある法的行為）

CSPはクラウド利用者と以下を共有する:

1. クラウド利用者に代わってCSPによって実行される処理を規定し、処理の目的および期間を定め、個人データおよびデータ主体のカテゴリのタイプを規定し、クラウド利用者の義務および権利を定めたモデルデータ処理契約（またはその他の拘束力ある法的行為）。**[P]**

契約またはその他の法律では、特にCSPが以下を行うことを規定している:

2. クラウド利用者からの文書化された指示があった場合のみ、個人データを処理すること。それには、第三国または国際機関への個人データの移転を含む。ただしCSPが規制対象となるEUまたは加盟国の法律によって要求されていない場合に限る。そのような場合、CSPは、その法律が重要な公益上の根拠に基づき情報提供を禁止する場合を除き、処理前に当該法的要請をクラウド利用者に通知すること。**[P]**
3. 個人データを処理する権限を与えられた人物が、EUまたは加盟国の法律で要求されている秘密保持の適切な法的義務を遵守していること、およびクラウド利用者からの指示を除いて個人データを処理しないこと。**[P]**
4. 適用されるEU法で要求されるすべての措置をとること。**[P]**
5. 他の処理者を使用する条件を尊重すること。（上記の3.3「委託先事業者」を参照 **[P]**
6. データ処理の性質を考慮して、クラウド利用者がデータ主体の権利行使要求に応える義務を履行するために、可能な範囲で、適切な技術的および組織的措置によってクラウド利用者を支援すること。**[P]**
7. データ処理の性質とデータ処理者が利用可能な情報を勘案して、クラウド利用者が以下の行為を行うことを助けること：データ処理のセキュリティに関する義務の遵守を確実にすること、監督当局への個人データ侵害の報告、データ主体への個人データ侵害の通知、データ保護影響評価。**[P]**
8. クラウド利用者の選択により、データ処理に関連するサービスの提供が終了した後、すべての個人データを削除または返却すること。またEUまたは加盟国の法律が当該個人データの保管を要求しない限り、既存のコピーを削除すること。 （下記の第2部11章「データの留保、返却、および削除」を参照） **[P]**
9. 関連するデータ保護義務の遵守を示すために必要なすべての情報をクラウド利用者に提供すること。クラウド利用者またはクラウド利用者が指定する監査人が実施する調査を含め、監査を受け入れ、監査に協力すること。**[P]**

4. 記録の保持

4.1 CSPのデータ管理者のための記録の保持

CSPのデータ管理者は、クラウド利用者に対して以下を確認する:

1. CSPの責任において、データ処理作業の記録を保持し、関係当局の要請に応じて提供できるようにすること。 **[C]**

記録は以下の情報を含む:

2. データ管理者の名前および連絡先の詳細、また該当する場合には、共同データ管理者、データ管理者の代理人、データ保護責任者の名前および連絡先の詳細。**[C]**
3. データ処理の目的; **[C]**
4. データ主体のカテゴリと個人データのカテゴリの記述; **[C]**
5. 個人データの開示先または開示予定先のカテゴリ。第三国または国際組織の開示先を含む。**[C]**
6. 該当する場合には、第三国または国際組織への個人データの移転。第三国または国際組織の識別情報と適切な予防措置を記載した文書を含む。**[C]**
7. 可能であれば、各種カテゴリのデータを削除するのに要する最大時間。 **[C]**
8. 可能であれば、技術的、組織的なセキュリティ対策の総合的な記述。**[C]**

4.2 データ処理者であるCSPのための記録の保持

データ処理者であるCSPは、クラウド利用者に対して以下を確認する:

1. データ管理者に代わって実施するデータ処理作業のすべてのカテゴリの記録を保持し、関係当局の要請に応じて提供できるようにすること。 **[P]**

記録は以下の情報を含む:

2. データ処理者およびデータ処理者を代行するデータ管理者の名前と連絡先の詳細。あるいは、該当する場合には、データ処理者の代理人、データ保護責任者の名前と連絡先の詳細; **[P]**
3. データ管理者に代わって行われるデータ処理のカテゴリ; **[P]**
4. 該当する場合には、第三国または国際組織への個人データの移転。第三国または国際組織の識別情報と適切な予防措置を記載した文書を含む。 **[P]**
5. 可能であれば、技術的、組織的なセキュリティ対策の総合的な記述。 **[P]**

5. データの移転

CSPは次のことを明示する:

1. 通常の稼働状態または緊急時にデータの移転、バックアップおよびリカバリが、国境を越えて行われるのか。 **[C & P]**

もし、このようなデータ移転がEU内の適用法令により制限されているなら、次のことを明示すること:

2. データ移転（何段階かの下請け業者への再移転も含む）を行う法的根拠。例えば、欧州委員会による十分性認定や、モデル契約／標準データ保護条項、承認済の行動規範もしくは認証メカニズム、拘束力のある企業の内部規定（BCR）、プライバシーシールドへの参加、など。**[C & P]**

「解説」
個人データが欧州経済領域の域外へ移転される場合、移転先の第三国が十分な個人データ保護レベルを有することを求めていることから（欧州委員会による十分性認定）、CSPとして個人データをどの第三国へ移転させるのか示すことは非常に重要である。
移転とは明確に定義されていないものの、欧州経済領域域外への第三国への第三者に対して、個人データを閲覧可能にするためのあらゆる行為をさす。移転が制限される個人データの例は次の通り

- 自然人の氏名
- 識別番号
- 所在地データ
- メールアドレス
- オンライン識別子(IPアドレス/クッキー識別子)
- 身体的、生理学的、遺伝子的、精神的、経済的、文化的、社会的固有性に関する要因

欧州経済領域域外への個人データ移転は原則として違法であるが、移転先が条件を満たしている場合は例外的に適当になる。移転が適法な例は次の通り。

- データ主体による移転の同意
- 十分性認定を受けた国や地域に加え、プライバシーシールドを締結した米国への移転
- 標準契約条項（Standard Contractual Clauses: SCC）や拘束的企業準則（Binding Corporate Rules: BCR）の整備による適切な保護措置の実施

「補足」
欧州委員会は2016年7月12日に欧米プライバシーシールドにおいて次の決定を採択した：
「Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 」は、欧州議会および理事会の「EU指令（95/46/EC）」や欧米プライバシーシールドによって提供されている「データ保護の十分性」に準じている（「 C(2016) 4176」により文書化されている）。2015年10月6日欧州司法裁判所は、セーフハーバー協定によって提供される保護の十分性に基づいたEU指令（95/46/EC）準じている、2000年7月26日付の「Commission Decision 2000/520/EC」が無効である立場を表明、関連したFAQ(OJ 2000 L 215, p. 7)が米国商務省発行されている（Judgment of the Court - 6 October 2015 Schrems Case C-362/14）

6. データセキュリティ措置

CSPは「最近採択されたEU全域においてネットワークおよび情報システム安全性の高い共通水準のための措置に関する2016年7月6日付け欧州議会および理事会の(EU) 2016/1148指令の関連でクラウドコンピューティングサービスはデジタルサービス事業者として扱われている」ことを予め留意すべきである。A.29WP05/2012に基づいている本セクションを完成させるにあたって、CSPは2016年2月16日付けENISAガイドラインを考慮し、または、ガイドラインに従うように奨励されている。さらに、データセキュリティ遵守の証拠は、関連する行動規範および認証メカニズムに沿って実施する中でクラウド利用者に提出されることが期待される。

最先端技術、実装費用、データ処理の性質、範囲、内容および目的を勘案し、また自然人の権利及び自由に対する主張の可能性および深刻さが変動するリストを考慮し、CSPは:

1. 偶発的または違法な破壊、偶発的紛失、改変、不正使用、不正改造・不正開示・不正アクセス、その他違法な手段によるデータ処理から個人データを守るための技術的措置、物理的措置、組織的措置をクラウド利用者に明示する。**[C & P]**

「考察」
個人情報の保護に関する法律の第二十条には“個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失またはき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない”と記載されている。

2. 以下の防御を確実にするための具体的な技術的、物理的、組織的対策（保護型、検出型、是正型の措置）をクラウド利用者に対して示す。**[C & P]**

「考察」

個人情報保護委員会のガイドラインによると安全管理措置には“技術的措置”、“物理的措置”、“組織的措置”に加えて、主に教育を課題にする“人的安全措置”がある。

i. **可用性**：インターネット接続のバックアップ、冗長ストレージ、効果的なデータバックアップ、リストアの仕組み、パッチ管理など、中断リスクの管理およびインシデントの防止、検出、対応のための手順および対策。**[C & P]**

「解説」

ISO/IEC 13335-1 2004 (JIS Q 13335-1 : 2006) では、「可用性」が次のように定義する。“認可されたエンティティが要求したときに、アクセス及び使用が可能である特性”、言わば、認可を受けた人や組織、団体あるいは機械が必要な時に情報やシステムにアクセスし利用できる状態を確保できる能力である。

「ユースケース」

事業継続計画の一部としての可用性：災害などの緊急事態によって多くの民間企業や政府および公的機関、医療機関は個人データ紛失やデータアクセス不能の事態が発生する可能性があります。この事態を回避対策として複数データセンターへのデータ分散やデータレプリケーション機能を有するクラウドサービスが挙げられる。

ii. **完全性**：CSPが完全性をどのように保証するかの方法（たとえば、メッセージ認証あるいは電子署名といった暗号メカニズムによる個人データの改ざん検出、誤り修正、ハッシュ化、ハードウェアの放射線や化学的変化への対策、物理的なアクセス・侵害・破壊＜対策＞、ソフトウェアのバグ、設計上の欠陥、人的ミス＜への対策＞など。）**[C & P]**

「解説」

ISO/IEC 13335-1 2004 (JIS Q 13335-1 : 2006) では、「完全性」を次のように定義する。“資産の正確さ及び完全さを保護する特性”、言わば、保有および取り扱っている情報の正確さおよび完全さを確保できる能力である。

iii. **機密性**：CSPが、契約的観点から機密性を確保し認可された人物のみがデータにアクセスできることを確実にするためにとる方法。特に、通信中および保存中の個人データの仮名化および暗号化、承認メカニズムおよび強力な認証。また契約の視点からは、CSPとその全ての従業員（正社員、パートタイム、契約社員）ならびにデータにアクセスできる委託事業者を拘束する秘密保持契約、秘密保持条項、ポリシーや手順などの手段。**[C & P]**

「解説」

ISO/IEC 13335-1 2004 (JIS Q 13335-1 : 2006) では、「機密性」を次のように定義する。“認可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性”、言わば、認可を受けたもののみが情報にアクセスしたり、情報を利用したりすることができる状態を確保できる能力である。

「考察」
「機密性」の定義において、PLAでは人物のみを対象にしている。一方、ISO/IEC 13335-1 2004 (JIS Q 13335-1 : 2006)では、「人物」だけではなく「エンティティ」という用語を加えることによって、組織、団体あるいは機械も対象にしている。

iv. **透明性**：透明性を維持し、利用者による監査を可能にするためにCSPが適用した技術的、物理的、組織的措置。（セクション7“モニタリング”を参照）**[C & P]**

「解説」
透明性は、法的、技術的、組織的背景を含み、プライバシー関連のデータの処理を随時に理解および再構成できることを確保する。情報は処理前、処理中、処理後に利用可能な状態でなければならない。したがって、透明性は処理自体だけではなく、予定されている処理（事前透明性）および正確に事情を分かるために処理後（事後透明性）の期間もカバーしなければならない。提供する情報の量や伝達方法に関してはターゲット層、たとえば、データ管理者、利用者、内部監査人　監督当局の能力に合わせて調整しなければならない。
透明性は開放性の原則に関連し、責任追跡性の前提条件である。透明性を達成あるいはサポートするメカニズムは、ロギング、レポーティング、技術、組織、責任、ソースコード、プライバシーポリシー、通知をカバーする理解可能なドキュメント、および、データ処理されている人とその人とのコミュニケーションに関する情報を含む。

出典：
G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. L. Métayer, R. Tirtea and S. Schiffner, “Privacy and Data Protection by Design - from policy to engineering,” European Union Agency for Network and Information Security (ENISA), December 2014. P.7
https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

v. **隔離**（目的制限）：CSPが個人データに対する隔離をどのように確保するか；（たとえば、個人データにアクセス権限と役割の適切なガバナンス（定期的に見直す）、最小権限の原則を基にしたアクセス管理；　ハイパーバイザのハードニング（要塞化）；　異なるクラウド利用者の間に物理リソースをシェアするために仮想マシンが使用される場合は、共有資源の適切な管理）**[C & P]**

「解説」
クラウドインフラストラクチャーにはストレージ、メモリー、ネットワークなどのリソースがクラウド顧客間によりシェアされている。こういう状況が、非正当な目的のためにデータ開示およびデータ処理の新しいリスクを生み出す。保護目的の“隔離”はそのリスクに対処し、本来の目的外に利用されないようにする保証や“機密性”および“完全性”維持に貢献する。

出典：
01037/12/EN WP 196 P.15
http://ec.europa.eu/justice/data-protection/index_en.htm

「ユースケース」
複数のクラウド利用者の間にストレージなどのリソースの物理的な分離管理によって、標的攻撃や法執行機関の法的な装置に対しての対応性を向上できる。さらに、クラウド環境においてのアクセス制御はデータの漏洩や不正利用の基本対策として挙げられている。

「考察」
隔離の保護目的は利用目的制限と見なされている。

vi. **介入性**　：クラウド事業者がデータ主体のアクセス権、異議の権利、忘れられる権利、処理を制限する権利、データ移転先の十分性を確実にする方法。それにより、データが委託先によって更に処理される場合を含め、これらの要件に対する技術的および組織的な支障がないことを証明する（関連事項：セクション9“データの移植性、移行および転送”）。**[C & P]**

「解説」
介入性はプライバシー関連の進行中あるいは計画中のすべての処理に、特にデータ主体による介入の可能性を確保する。介入性の目標は、改善装置及び必要な場合はカウンターバランスである。
介入性はデータの訂正、データ削除、同意の取り消し、申し立て、救済を達成するために紛争を起こすことなどの個人の権利の原則に関連している。さらに、介入性はその他の関係者に重要であり、たとえばデータ管理者がデータ処理者を効率的に管理したり　ITシステムを利用しデータ処理を影響あるいは中止させたりすることができる。介入性を達成あるいはサポートするメカニズムは、一部あるいはすべてデータ処理を影響あるいは中止する定着されたプロセス、自動決定を手動でくつがえすこと、データ処理者にロックインされることを防ぐためのデータ移植性の予防装置、ブレークグラスポリシー、個人介入要求用の単一の連絡先、設定変更ためのユーザ切り替え（たとえば、非個別化、空プロファイル設定）、一時的に自動運用及び監視システムを非アクティブ化するなどを含む。上記のメカニズムは事業者の協力が求められる（honest-but-curious (正直・好奇心)攻撃者のモデルと呼ばれている）。

出典：
G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. L. Métayer, R. Tirtea and S. Schiffner, “Privacy and Data Protection by Design - from policy to engineering,” European Union Agency for Network and Information Security (ENISA), December 2014 P.7.
https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

「考察」
介入性は処理されている情報に対してのデータ主体の権利行使を可能にする要素であり、部分的にはOECD8原則の個人参加の原則と一致している。

vii. **ポータビリティ（移植性）**：後述のセクション9 “データの移植性、移行および転送”を参照 **[C & P]**

viii. **説明責任（責任追跡性）**：前述のセクション1 “コンプライアンスと説明責任についてのCSPの言明” を参照 **[C & P]**

7. モニタリング

CSPはクラウド利用者に次のことを明示すること:

1. PLAが規定する適切なセキュリティ・プライバシー施策が継続的に順守されていることを確実にするために、利用者がモニタリングと監査を行う権利を有すること（例：CSPまたはその下請けが実施する該当の処理作業に対するロギング、報告実施、第一者および第三者監査90）。**[C & P]**

[解説]
6. 2. iv.「透明性」を参照。
クラウド環境の中で、利用者の資産に対するセキュリティとプライバシーが担保されていることの保障の一手段として、利用者が事業者に対して「監視」＝モニタリングを行うことの規程である。
最終的に記述形式としては、クラウド事業者が、利用者に対してモニタリングを許すことを明示すること、という形になっている。としつつ、適用対象は事業者・利用者双方という表示はそのまま残ってい

る。

モニタリングの方法としては、
ロギング、
レポーティング、
第一者監査（すなわち自己評価結果）、
第三者監査
の4項目を挙げている。

第三者監査については、脚注で参考情報として「CNILの2014年8月25日付決定：セキュリティ監査の不実施に関する注意喚起」を示している。CNILは”Commission nationale de l'informatique et des libertés”の略称で、フランスの情報処理および自由に関する全国委員会を指す。注意喚起の内容については、二つのURLを掲げている。どちらもCNILによるある一つの文書（2014年）を指すようであるが、フランス語のテキストしか提供されておらず、残念ながら内容の確認はできない。

また、モニタリング方法の例示全体に対しても脚注が付されている。そこには3つの参照先が示されている。
①GDPR第28.3条(h)および本PLA第1章“CSP declaration of compliance and accountability”
②29条作業部会2012年5月発行の13ページSection3.4.2および11ページSection3.4.1.2
③ICOガイドライン13,14ページ　（ICO：英Information Commissioner’s Office The UK’s independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.）

①はデータ管理者のコンプライアンス確認または第二者もしくは第三者監査のためにprocessorが情報提供することを義務付けている。
②はクラウドサービス／利用契約に盛り込むべきデータ保護のための条項（3.4.2）と、目的外利用禁止のためのクラウド事業者に対する監査（3.4.1.2）について規定している。
③はタイトルからは”Guide to Data Protection” “GDPR Consent Guidance” などが該当しそうだが、いずれも13, 14ページはconsentに関する記述であり、監視・監査に関する記述を見出すことはできなかった。ICOのサイトで探す限り、他に該当しそうな文書は見つからない。

8. 個人データ侵害

「個人データ侵害」とは、CSPによって提供されるサービスに関連して、送信や保管その他処理された個人データの偶発的または不法な破壊、紛失、改ざん、無断開示、アクセスにつながるセキュリティ違反を意味する。

CSPはクラウド利用者に以下のこと明示する:

1. CSPおよび/またはその再委託先によって処理されたクラウド利用者のデータに影響する個人データ侵害を決められた時間内に利用者に通知する方法。**[C & P]**

その際、情報は以下に示すように、少なくとも可能な限り最大限の情報を通知する:

2. 可能であれば、関連する個人データレコードのカテゴリとおおよその数を含む個人データ違反の内容を記述する; **[C & P]**
3. より多くの情報を入手できるデータ保護責任者またはその他の窓口の名前と連絡先の詳細を通知

する（第2章「CSP関連窓口とその役割」を参照）; **[C & P]**
4. 個人データ侵害によって起こりうる継続事象を記述する；**[C & P]**
5. 必要に応じて起こり得る悪影響を軽減するための措置を含め、個人データ侵害に対処するために取られる（取られることを提案する）措置を記載する；**[C & P]**

CSPは併せて次のことも明示する:

6. 個人データ侵害に気づいてから72時間以内に監督機関に個人データのセキュリティ侵害を通知する方法。**[C]**

7. 個人データ違反が自然人の権利および自由に高いリスクをもたらす可能性がある場合、遅滞なくデータ主体に通知する方法。**[C]**

[解説]
GDPR 第4条：「定義」
12. 「個人データ違反」とは、送信や保管その他処理された個人データの偶発的または不法な破壊、紛失、改ざん、無断開示、アクセスにつながるセキュリティ違反を意味する。

GDPR 第33条：「監督当局に対する個人データ違反の通知」
1. 個人データの違反があった場合、データ管理者は過度の遅滞なく、可能な場合にはそれを認識してから72時間以内に第55条に従って管轄する監督当局に個人データ違反を通知する。監督当局への通知が72時間以内に行われない場合は、遅滞理由が付随していなければならない。
2. データ処理者は、個人データ違反を認識した後、過度の遅延なしにデータ管理者に通知しなければならない。
3. 本条第1項の通知は、以下の通りとする。
（a）対象となるデータ主題のカテゴリーおよび概数、および関連する個人データ記録のカテゴリーおよびおおよその数を含む、個人データ違反の性質を記述する。
（b）データ保護責任者またはより多くの情報が得られる他の連絡先の名前と連絡先の詳細を伝える。
（c）個人データ違反の可能性のある結果を記述する。
（d）個人データ違反に対処するために、データ管理者が取るべき措置または取られた措置を記述する。
4. 同時に情報を提供することができない場合は、過度の遅れなく段階的に提供する。
5. データ管理者は、個人データ違反、その影響および取られた是正措置に関連する事実を含む、あらゆる個人データ違反を記録しなければならない。

GDPR 第34条:「個人データ違反とデータ主体との通信」
1. 個人データ違反が自然人の権利と自由に高い危険をもたらす可能性が高い場合、データ管理者は、過度の遅滞なく個人データ違反をデータ対象に伝達する。
2. 本条第1項に規定するデータ主体とのコミュニケーションは、個人データ違反の性質を明確かつ簡潔に記述する（少なくとも第33条第3項の（b）、（c）および（d））。
3. 第1項に規定するデータ主体との通信は、以下のいずれかの条件が満たされた場合には必要ない。
（a）データ管理者は、適切な技術的（暗号化など）および組織的保護措置を実施し、アクセスを許可されていない人に対し、特に、個人データ違反の影響を受けた個人データを理解させないようにした場合
（b）データ管理者は、第1項で言及されたデータ主体の権利と自由に対する高いリスクがもはや実現しないことを確実にする措置をとった場合
（c）不均衡な努力を伴う場合には、その代わりに意見広告または同様の措置を講じてデータ主体に同様に効果的な方法で通知する場合
4. データ管理者が個人データの違反をデータ主体に伝達していない場合、監督官庁は、個人データ違反のリスクが高いと判断した場合、データ主体に伝達することを要求するか、または、第3項の条件が満たされているか判断する。

さらに、ドイツでは、2009年9月1日に施行された法律上のデータ違反通知要件がある。ドイツ連邦データ保護法のセクション42（a）を参照。「ドイツの法律上のデータ違反通知要件に関するよくある質問」も参照。

http://www.datenschutz-berlin.de/content/themen-a-z/informationspflicht-nach-42-a-bdsg.

オランダでは、2016年1月1日、データ違反通知義務が発効しました。A.29WP05 / 2012、第3.4.2項、p.13も参照のこと。

https://autoriteitpersoonsgegevens.nl/en/news/data-breach-notification-obligation」.

[参考]
１）GDPR の第 33 条および第 34 条に関して
　データ管理者は、過度の遅滞なく、可能であれば違反の発見から72時間以内に、個人データの違反を監督当局に報告することを要求している。さらに、違反が彼らの「権利と自由」に影響を及ぼすリスクが高い場合、影響を受けるEU市民にデータ管理者が連絡しなければならない。
　強固な違反対応は明らかに重要だが、最高の罰則は良い防御である。理想的には、組織は最初にこれらのプロセスを呼び出さない方が望ましい。また、明らかに違反を通知するには、適切な人材、プロセス、技術を持っている必要がある。

[引用-1] rapid 7, SOLUTION BRIEF General Data Protection Regulation (GDPR) Articles 33 & 34, How to expedite compliance with Rapid7 solutions
https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-solution-brief-gdpr-article-33-34.pdf

２）罰則に関して
　GDPR違反の場合の制裁金の上限額には次の2 とおりある。
* 1,000 万ユーロ以下または、企業の場合には前会計年度の全世界年間売上高の2%以下のいずれか高い方
- 安全管理策を取らなかった場合
- 義務付けられた記録を保持していなかった場合
- 個人データに対する侵害発生時に報告しなかった場合
- DPO（データ保護責任者）を任命していなかった場合

* 2,000 万ユーロ以下または、企業の場合には前会計年度の全世界年間売上高の4%以下のいずれか高い方
- データ処理に関する原則や同意の取得・センシティブ情報の取り扱いを遵守しなかった場合
- 個人データの域外転移に関するルールを守らなかった場合
- 監督機関からの命令を守らなかった場合

[引用-2] 山崎万丈、CSA の考える プライバシー保護の在り方について、CSA Japan Congress 2017講演資料
http://www.cloudsecurityalliance.jp/newsite/wp-content/uploads/2017/11/PLA%E3%81%A8GDPR%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6.pdf

[引用-3]日本貿易振興機構（ジェトロ）、「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（入門編）、2016 年11 月
https://www.jetro.go.jp/ext_images/_Reports/01/dcfcebc8265a8943/20160084.pdf

9. データの移植性、移送および返送

CSPはクラウド利用者に対して以下を明確にする:

1. CSPが、個人データを、構造化され、共通性があり、機械で判読可能で、相互運用可能な形式で、以下のものに対して送信することができるかという意味で、データの移植性を保証する方法 **[C & P]**
    i. クラウド利用者に対して（‘返送’、例えば社内IT環境への）; **[C & P]**
    ii. 直接、データ主体に対して; **[C & P]**
    iii. 他の事業者に対して（‘移送’、例えばダウンロードツール、API, またはAPIの組合せによる） **[C & P]**

【解説】

データ移植の権利は、GDPRによって導入された新しい法令上の権利である。GDPRのデータ移植の権利は、PII主体が、CSPの不意な契約解除によりPIIを失うことを回避するためのものであると考えられる。ISO/IEC27018附属書A9.3“PIIの返却、転送、廃棄”に同様の説明があるが、CoC(仮)の本規定と同様の主旨であると考えられる。

ISO/IEC27018附属書A9.3“PIIの返却、転送、廃棄”

（管理策）

パブリッククラウドPIIデータ処理者（PIIを扱うCSP）は、返却、転送、廃棄に関するポリシーを持つ必要がある。このポリシーをクラウドサービスの顧客に提供する必要がある。

（実施の手引）

ある時点で、PIIは何らかの方法で廃棄される必要があると思われる。廃棄とは、クラウドサービス顧客へのPIIの返却、他のパブリッククラウドPIIデータ処理者や（例えば合併の結果として）他のPIIデータ管理者への転送、安全な削除あるいは破壊、匿名化又は保管を意味すると考えられる。（以下省略）

【ユースケース】

① データを預けていた事業者が財政的困難に直面していることが利用者に知られ、全利用者が不意のサービス停止に備え、PIIデータを一斉にエクスポートしようと試みたが、事業者の回線帯域制御により、意図通りのデータ保全が困難となった。

② SaaSサービスを利用する利用者が、他のSaaSサービスに移行しようとしたが、データをエクスポートするためのAPIが提供されておらず、また、利用者がアドオン開発したアプリケーションを移行するための新たなAPIの開発コストが膨大であるため、PIIデータを移行することが著しく困難となる。

CSPはクラウド利用者を以下のように記述する:

2. データを他の事業者、あるいは、社内のIT環境へ移行できるかについて、CSPが、どのようにして、また、どのようなコストで、顧客を支援するか。**[C & P]**

10. 処理の制限

CSPは、クラウド利用者に、次の事項を説明する:

1. 個人データの処理を制限する可能性が、どのように認められているか； 処理が制限された場合、当該個人データは、保存を除きデータ主体の同意に基づくか、法法的主張時の立証、行使若しくは抗弁のため、又は他の自然人若しくは法人の権利を保護するため、若しくはEU 若しくは加盟国の重要な公共の利益のためだけに取り扱われなければならない。**[C & P]**

【備考】

CSPは、クラウド利用者に対して、個人データの処理に制約を課せられる可能性があることを説明しておくことが必要である。

GDPR 第18条では、データ主体が管理者に取扱いの制限をさせる権利を有することが規定されており、そのような処理に制限が課せられた場合には、上記本文のような条件の場合にのみ処理が認められる。また、GDPRの備考（Recital 67）では、次のような説明がある。

個人データの処理を制限する方法は、とりわけ、選択されたデータを別の処理システムに一時的に移動させ、選択された個人データを利用者が利用できないようにするか、またはウェブサイトから公開データを一時的に除去することを含む。 自動ファイリングシステムでは、処理の制限は、原則として、技術的手段（個人データはそれ以上の処理操作を受けず変更することができないといった手段）によって保証されるべきであり、個人データの処理が制限されているという事実は、システムに明確に示されなければならない。

11. データの留保、返却、および削除

11.1 データの留保、返却、および削除のポリシー

CSPはクラウド利用者に次を説明すること:

1. CSPのデータ留保のポリシーとタイムライン、およびサービスが終了した後の個人データ返却、またはデータ削除の条件。 **[C & P]**
2. 同様に、委託先事業者のこれらのポリシー、タイムラインおよび条件。 **[C & P]**

11.2 データ留保

CSPは以下のことを示すこと:

1. 個人データが留保される、または留保される可能性がある期間、またはそれが不可能な場合は、その期間を決定するために使用される基準。 **[C & P]**

11.3 特定のセクターの法的要件を満たすためのデータ留保

CSPはクラウド利用者に以下のことを示すこと:

1. クラウド利用者がCSPに特定のセクターの法律や規制を遵守するように要求することができるかどうか、どのように要求できるか。 **[C & P]**

11.4 データの返却および/または削除

CSPはクラウド利用者に以下のことを示すこと:

1. データの移植性（上記9章「データの移植性、移行、転送バック」も参照）を担保する形式で個人データをクラウド利用者に返却する手順; **[C & P]**
2. データ削除に利用できる、または使用される方法; **[C & P]**
3. クラウド利用者がデータを削除（または削除要求）した後、または契約終了後にデータが留保されるかどうか; **[C & P]**
4. データを留保する特定の理由; **[C & P]**
5. CSPがデータを留保する期間。 **[C & P]**

【解説】
「個人データの消去」とは、GDPRでは、その管理者は、当該個人データを取り扱っている管理者たちにデータ主体が当該個人データのあらゆるリンク又はコピー若しくは複製の消去を要求している旨を通知するために、技術的措置を含む合理的手段をとらなければならないと規定されている（参照：GDPR第17条）。
一方、日本の個人情報保護法では、当該個人データを個人データとして使えなくすることであり、当該データを削除することのほか、当該データから特定の個人を識別できないようにすること等を含むとしており(参照：「個人情報保護法ガイドライン（通則編）3-3」)、その方法についての違いがある。

12. クラウド利用者との協力

CSPにおける明示:

1. クラウド事業者は、適用されるデータ保護条項の遵守を確実にするために、クラウド利用者と協力する。例えば、アクセス権、異議の権利、忘れられる権利、処理を制限する権利、データ移転先の十分性などデータ主体の権利行使を効果的に保証するため。セキュリティ侵害やデータ侵害に際してのインシデント（フォレンジック分析を含む）を管理するため。6章「データセキュリティ措置」および8章「個人データ違反」も併せて参照のこと。 **[C & P]**

2. コンプライアンスを証明するために必要な情報をクラウド利用者および管轄の監督当局に対して提供する（「コンプライアンスと説明責任についてのクラウド事業者の言明」も併せて参照のこと）。 **[C & P]**

13. 法的な開示要求

クラウド事業者は以下のことをクラウド利用者に明示する：

1. 法執行当局による個人情報の開示要求を管理し対応するためのプロセス。刑法における法執行のための操作の秘密保持など、特に禁止されていない限り、関心のある顧客（本人）への通知手続きに特に注意を払うこと。**[C & P]**

14. クラウド利用者の救済措置

クラウド事業者は以下のことをクラウド利用者に明示する：

1. CSPおよび/またはCSPの委託業者（3章「データを処理する方法」、より具体的には3.3「委託先事業者」を参照）においてPLAに基づく契約上の義務違反が発生した場合、クラウド利用者が利用できる救済策。救済には、クラウド利用者へのサービスクレジットおよびCSPに対する契約上の補償金が含まれる。**[C & P]**

15. CSP保険の方針

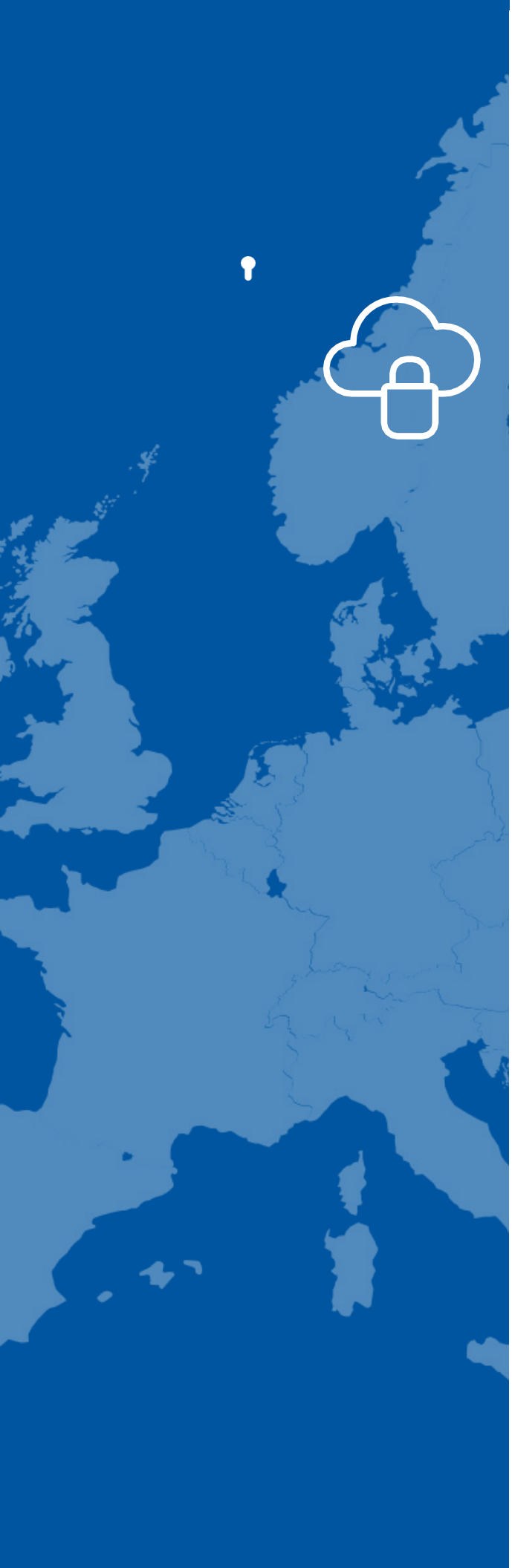
CSPは以下のことをクラウド利用者に明示する：

1. CSPの事業に関連する保険契約の範囲（例えば、データ保護遵守保険：データ保護義務を履行しない再委託先処理者のカバーを含む、およびサイバー保険：セキュリティ侵害・データ侵害に対する保険を含む）。**[C & P]**

「考察」

CSPは、SLAという形でクラウド利用者へ提供するサービスの品質保証をしている。SLAに違反した場合の損害補償は、一般的に契約金額を上限とすることが多いがが、その違反によりクラウド利用者が被るビジネス面での損害は補償されることは少ない。

仮にCSPが上記ビジネス面の損害を補償するための、保険契約等を備えているなら、クラウド利用者はその内容を把握し、万が一の場合の対応に不足が想定されるならば、クラウド利用者自身が情報漏えい保険やサイバーセキュリティ対策保険等の備えを行うことが望ましい。



第3部

CSA 行動規範の
ガバナンスと適
用の仕組み

クラウドセキュリティ認定の状況は静的ではなく急速に変わる可能性がある。クラウド事業者とクラウド利用者は個人データ保護に関連する新しい法律や規制や要求事項などに即時に対応をしなければならない。関係者や既存認証スキームは、適応することで実施中のセキュリティとプライバシー対策が進化すること、ならびに、新しい規制要件に継続的に対応していることを確実にしなければならない。

本行動規範(CoC)は、前述のように進化を続けるべきものである。したがって、ガバナンス体制を整備して、必要な変更の一貫性、管理、適切な実施を確保するとともに、行動規範と関連の文書の変更に関する「条件」、「時期」、「方法」、「主体」を正確に定義することが必要である。

行動規範のガバナンス体制に関して、次の重要な要素を考慮しなければならない;

1. **技術要素**：法令、規制、技術環境の経時変化、または、CSA内部の変化により影響を受ける要素
2. **ガバナンスの体制**：鍵となる**ガバナンス**の体制、役割、責任
3. **プロセス**：本規範の構成部分の定義、改定、実行に関する**ガバナンス**プロセスおよび活動

1. 技術構成要素

行動規範のガバナンス構造の構成要素:

1. PLAの行動規範
2. 行動規範の認証制度と準拠の仕組み;
3. 倫理規範;
4. PLAとOCFワーキンググループの趣意書。

1.1 PLAの実践規範

本文章の第2部に掲載されているPLAの実践規範（CoP）は、欧州連合における関連する個人データ保護のコンプライアンス要件を特定する技術標準であり、これらの要件への準拠を管理するための条項と管理策を定義している。PLAの行動規範は、この行動規範（CoC）の基本的な技術要件を構成するものである。

1.2 認証スキーム/規範遵守の仕組み

PLA CoPの要件に準拠したCSPおよびクラウド利用者は、本書で確立した原則、方針とガイドラインに従い、遵守宣言書（附属書2参照）をCSAに提出しなければならない。さらに、CSA OCFワーキンググループによって開発されCSAによって発行されたCoC認証制度の更新にも対応しなければならない。

遵守宣言書には、会社/組織の法律上の代表者または指定されたデータ保護責任者（DPO）の署名が必要であり、セルフアセスメント（自己評価証明）または第三者認証の形式によるPLA [3]テンプレート（附属書1参照）が付属されなければならない。

GDPR遵守テンプレート（GDPR Compliance Adherence Template）のためのCSA CoCは、PLA CoPに含まれる要件をテーブル構造でまとめている。

CSPおよびクラウド利用者は、すべてのPLA CoPを考慮対象としなければならず、選択されたサブセットのみを遵守する宣言は出来ないということを常に明確にしておかなければならない。

CoC認証スキームは、この行動規範を遵守するための目的、方針、仕組み、範囲、規則、要件、およびプロセスを定義すると共に、以下を定めている:

(a) 認証の範囲と目的;

(b) 監査ルールと仕組み;
(c) 審査員資格手順;
(d) 失効および苦情処理の条件;
(e) 認証料。

CoC認証スキームは、CSA認証フレームワークの構成要素であり、STARプログラム/ Open Certification Framework（OCF;下記の附属書3参照）である。このスキームは、2つのレベルの保証に基づいている:

1. 行動規範の自己評価証明;
2. 行動規範の第三者認証。

以下に報告するものは、CSA PLAワーキンググループがCSA OCFワーキンググループにCoC認証スキームの策定のために提供するものである。

1.2.1 CoCの自己評価証明

CoCの自己評価証明は、クラウド事業者またはクラウド利用者がCSA STARレジストリ（附属書3参照）に自発的に公表するもので、その組織がCoCに適応したことを示す。CoCの遵守宣言書（附属書2）およびPLAテンプレート（附属書1）をCSAへ提出し、STARレジストリへアップロードし公開する。自己評価証明プロセスでの行動規範は、独立した資格のある第三者による審査は行われない。PLAテンプレートとCoC遵守宣言書は、CSAに提出され、行動規範の全ての項目を満たしていることを検証し、PLA CoP要件に完全に対処するための「誠実な」努力が行われたことが確認される。CSAは、また提出者が自らのウェブサイト上で行動規範への遵守を公開したことを確認する。一旦、必要な条件がすべて満たされていることが確認されると、CSAは、申請者に対して自己評価証明の適合マークを付与する。

行動規範の自己評価証明を示す適合マークは、発行日から12ヶ月間有効で、その後更新する必要がある。さらにCoCの自己評価証明は、事業者の関連する方針や実施事項が変更されるたびに改訂する必要がある。

認証マークを取り消すための条件と苦情の仕組みについては、3.3「CoCマークの発行、遵守宣言書の発行および苦情管理」に記載されている。

CSA STARレジストリへの公表と認証マークの発行は、管理手数料の対象となる可能性があることに注意すること。

1.2.2 CoCの第三者認証

行動規範の第三者認証は、PLA CoP要件への遵守を認定した行動規範の監査パートナー（以下に詳述）の検証を経て取得される。検証プロセスは、以下を確認することを目的としている:

- 行動規範の正しい使用（例えば、データ管理者/データ処理者が PLA CoP 内のすべてのセクションを完了したか、すべてのセクションに含まれるコンテンツがデータ処理および処理に関する必要な情報を提供しているか？）;
- コードに含まれる情報の正確性（例えば、提出物に含まれている情報は真実か、証拠によって裏付けられているか？）。

上記のように、検証は、CSAとの「認定CoC監査パートナーシップ契約（Qualified CoC Auditing Partnership Agreement）」に署名した組織である認定CoC監査パートナーによって実行されなければならない。パートナーシップ契約の注意すべき要件は次のとおりである:

- パートナーは、少なくとも1人の認定CoC審査員を採用する
- パートナーは、監査契約期間の関連部分について少なくとも1人の認定CoCセキュリティ専門家を採用しているか、委託している。（この人物はCoCの認定資格者でもある）

注意：CoC監査パートナーの資格のあるCSA企業会員は、CSAのWebサイトに無償で掲載される。

認定CoC審査員は、次の要件を満たす専門家である:

1. データ保護の法的遵守に関する2年以上の経験、または関連する専門資格（例えば、IAPP CIPP/E、ECPC-B DPO Certification, CSA CoC training and certification）を所持している。

認定CoCセキュリティエキスパートは、以下の要件を満たす専門家である（要件は、監査対象会社の情報セキュリティ認証状況によって異なる）:

1. 監査対象会社が関連する情報セキュリティ認証（例えば、CSA STAR 認証/評価証明、ISO 27001）を持っている場合：
   クラウドセキュリティに関わる法規制への準拠に対する最低1年以上の経験、または関連する専門資格（例えば、CSA CCSK、(ISC)2 CCSP）を所持していること。
2. 監査対象会社が関連する情報セキュリティ認証（例：CSA STAR 認証/評価証明、ISO 27001）を持っていない場合：
   関連する情報セキュリティ認証（例えば、ISACA CISA, CSA STAR Certification Auditor, ISO 27001 Lead Auditor）に応じた物理的・組織的・技術的な最低3年以上の経験、または関連する証明書（例えば、ISACA CISA、CSA STAR認証審査員、ISO 27001審査員）を所持していること。

必要な条件がすべて満たされたことが確認されると、CSAは、行動規範の第三者認証マークをその認定された者に付与する。

行動規範の第三者認証マークは、発行日から12ヶ月の有効期間を有し、この期間後に更新する必要がある。さらに、行動規範の第三者認証マークは、事業者の方針や実務が変更されるたびに改訂する必要がある。

認証マークを取り消すための条件と苦情の仕組みについては、3.3「CoCマークの発行、遵守声明（Statement of Adherence）の発行と苦情管理」に記載されている。

CSA STARレジストリへの公開と認証マークの発行は、管理手数料の対象となる可能性があることに注意しなければならない。

1.3 倫理規定

倫理規定の記述については、下記の附属書4を参照のこと。

1.4 PLAおよびOCFワーキンググループの趣意書

PLAおよびOCFワーキンググループの趣意書については、それぞれ下記の附属書5および附属書6を参照のこと。

2. ガバナンスの体制、役割、責任

PLA CoCおよびそのコンポーネント（PLA 実践規範（Code of Practice）、認証体系、倫理規定（Code of Ethics）の統制管理はPLAワーキンググループ、OCFワーキンググループとCSAの共同責任である。

2.1 PLAワーキンググループ（WG）

PLAワーキンググループ(WG)は、技術基準/実践規範、すなわちPLA Code of Practise (現在バージョン3、PLA[V3])の定義、承認、更新に対して責任を負う。このチームはまた、CoC自己評価やCoC認証に関する苦情がCSAに提起された場合、専門家としての意見を提供する。PLA WGの趣意書には、WGの目的、対象範囲、メンバーシップ、構成と責任、関連するCSAのWGとの関係、対外活動、運営、コミュニケーションの方法、意思決定プロセス、活動、生成物、活動期間、知的財産権ポリシーを規定している。各メンバーはCoCの変更を提案する権利を有する。

PLA WGへの参加はボランタリベースで、貢献したい人は自由に参加できる。

2.2 OCFワーキンググループ

このチームはCSA STARプログラムに組み込まれた認証スキームの策定に対して責任を負っている。OCF WGはCSA OCF/STARプログラム内の既存の認証スキームに対して設計、見直し、更新の承認を行い、新しい認証スキーム（すなわちCoC認証スキーム）に対しても設計、見直し、承認を行う。

OCF WGの趣意書（附属書6参照）は、WGの目的、対象範囲、メンバーシップ、構成と責任、関連するCSAのWGとの関係、対外活動、運営、コミュニケーションの方法、意思決定プロセス、活動、生成物、活動期間、WGの知的財産権ポリシーを規定している。各メンバーはCSA STARプログラムに組み込まれた認証スキームの変更を提案する権利を有する。

2.3 クラウドセキュリティアライアンス(CSA)

CSAは、STARプログラムの一部であるCoC認証スキームを実施に移すことの支援と監視を行う。その活動には以下の事項があるが、これに限る訳ではない：

- 発行されたPLA認証書の公開された登録情報の維持管理。登録に際しては最低限以下の情報が必要である：(i)組織の名称と説明、(ii) PLAの対象となるサービスの名称と説明、(iii) PLAの登録、(iv)適用したPLA CoCのバージョン（現行V3）、(v)証明書の有効期限、(vi)監査した組織または審査員の名称；
- 公認PLA審査員の公開された登録情報の維持管理；
- PLAのコンセプト、アプローチ、技術標準に関する情報とガイドライン、および認証スキームの要件プロセス、費用が記載されたWebサイトの維持管理；
- PLA自己評価証明（self-attestations）をチェックして最小要件を満たしていることを確認すること；
- 苦情を受け付ける仕組みの維持管理；
- 苦情の確認と必要な措置の実施（例：レジストリからのPLA登録および証明書の削除、レジストリからの公認PLA監査機関の削除など）；
- 紛争の取扱いに関するガイダンスの提供；
- アドバイザー組織（例えば欧州プライバシー協会（European Privacy Association(EPA)）といった組織で構成）を組成し、CSAに対して認証スキームの実施と監督について支援する（例：PLA監査の要件に対する定期的監査、監査結果に対する定期的チェック、苦情処理など）；
- 標準の開発や認証スキームの実施と管理に関して、透明性と完全性を保持すること；
- OCF趣意書の改訂と追記の承認；
- PLA趣意書の改訂と追記の承認；
- 認証費用の決定と見直し；
- PLA公認審査員教育機関の承認；
- 本プログラムの運営に伴う全ての手数料その他の収入とその処理に関する公認会計報告の提供。

2.4 データ保護監督当局との協調および支援活動

PLA CoCガバナンスチームは、以下の条件のもとに、クラウド上の個人データ保護に関する事項について、国のデータ保護監督機関(SA)に対して協調および支援を行うものとする。

協調に関しては、国のSA、29条データ保護作業部会、欧州データ保護委員会の求めに応じ、PLA CoCガバナンスチームは、以下のことを提供する：

- クラウドコンピューティングサービスの利用者である企業及び個人向けのガイドラインおよび啓発活動；

- 関連するデータ保護法制に対する意見（例：国のSAが行う国会その他の公的権威機関への法定の意見表明）についてのアドバイス。

支援に関しては、国のSA、29条データ保護作業部会、欧州データ保護委員会の求めに応じ、PLA CoCガバナンスチームは、以下のことを提供する：

- PLA自己評価およびPLA認証を取得した企業に対して、国のSAが行う施策（PLA自己評価およびPLA認証を取得した企業に対して適用された一般条項や特定条項）に関する啓発活動；
- 国のSAがPLA認証企業に対して検査を行う場合には、当該企業に関してCSAが保有する情報と証拠を国のSAに提供する。この場合、CoCガバナンスチームはCSAにおける連絡窓口となる。
- 国のSAによりペナルティが課された場合には、見直しを行い、必要な場合にはPLA認証を取り消す。

3. ガバナンスプロセス及び関連活動

行動規範のガバナンスプロセスは、すべての行動規範コンポーネントの一貫した管理プロセスを維持するために、統制機関とそれに準拠する必要がある一連の活動との関係を定義する。

3.1 PLA 実践規範のレビュープロセス

PLA実践規範は、欧州連合（EU）の個人情報保護に関連する法的枠組みの変更を受ける可能性があるため、定期的なレビューの対象となる。 PLA 実践規範のレビュープロセスは、PLA WGの責務に該当する。

PLA実践規範のレビュープロセスは、PLA実践規範の要件を最新の関連する法令に合わせる必要性に基づいて、CSAコミュニティの任意のメンバー（ボランティア、企業メンバー、PLA WGのメンバーなど）によって始動される。

PLA実践規範 [V3]の更新要請は、PLA WGメンバーによって評価され、決定されるものとする（参照下記の附属書5のPLA趣意書に記載）。

SAおよびPLA WGのメンバーは、不完全な要件に従っている組織のリスクを制限するために、PLAの更新がタイムリーに行われるようにする。

現行バージョンのPLA実践規範 [V3]は、実際の（EU指令95/46 / ECとEU加盟国における実施）および今後の欧州連合（EU）の個人情報保護に関する法律（EU規則/ 679、GDPR）に焦点を当てている。

PLA WG趣意書には、PLA実践規範の現在の地理的範囲の拡張も含まれている。PLA WGはまた、グローバルレベルでのプライバシー/データ保護要件に対応する行動規範の開発も想定している。

3.2 行動規範認証レビュープロセス

OCF WGは、行動規範認証スキームの審査を開始するとともに、審査要求の評価と承認、提案された変更の実施を担当している。

OCF WGメンバーは、行動規範認証を含むCSA STARプログラムの認証スキームの変更を提案する権利を有する。

3.3 CoCマークの発行、遵守声明の発行および苦情管理

CSAは、CoC自己評価証明および第三者認証の発行、遵守申告書の提出手続および関連する苦情の審査、

承認および管理を担当している。 以下に詳しく説明する；

(i) CoC自己評価証明
CSAは、第三者から提出されたCoC自己評価証明および関連する苦情を審査する責任がある。前者の場合、CSAは最小要件が満たされていることを確認するものとする。後者の場合、CSAは苦情の正当性を検証し、PLA WGからの情報に基づいて、適切な措置を取るものとする。

妥当性確認が行われると、CSAはCoC自己評価証明がオンラインCSAレジストリに公開されることを保証するものとする。最低要件が満たされない場合、または苦情が有効であるとみなされる場合、CSAは次のいずれかの行動を取る：

a） CoC自己評価証明の修正を要求する、

または

b） CSAレジストリから自己評価証明を削除し、（付与した）マークを取り消す。

(ii) CoC 認証
CSAは、認定審査員が行動規範の審査に合格したことを通知すると、STARレジストリへのCoC認証の発行を担当する。

CSAは、関連する苦情申請書が提出された場合には、CoC認証を発行した認定審査員に通知する責任も負っている。その場合、CoC認証を発行した認定審査員は、苦情の正当性を検証し、CSAに報告しなければならない。

苦情が有効であるとみなされた場合、CoC認証を発行した認定審査員は、一時的に認証を停止するか、または取り消さなければならない。したがって、CSAは、レジストリから認証証明を削除し、マークを取り消さなければならない。

3.4 倫理規範レビュープロセス

倫理規範の声明文は、CSA取締役会によって毎年レビューされ、更新される。声明文の変更は、すべてのCSA関係者に伝達されるものとする。

3.5 PLAとOCF WG趣意書レビュープロセス

CSAは、OCFとPLA趣意書の改定や追加要求を承認する責任がある。

附属書 1: PLA [V3] テンプレート

要求事項	要求事項 ID	コントロール	コントロール ID	詳細	CSPがデータ管理者	CSPがデータ処理者
1. コンプライアンスと説明責任についてのCSPの言明	DCA	1. コンプライアンスと説明責任についてのCSPの言明	DCA-1.1	*1. 適用されるEU内のデータ保護法ならびに技術的・組織的セキュリティの条項を遵守する。また、データ主体の権利をセーフガードにより保護する*	適用可能	適用可能
			DCA-1.2	*2. 適用されるEU内のデータ保護法を順守していることを示す（説明責任）。*	適用可能	適用可能
			DCA-1.3	*3. CSP自身、再委託先(セクション3.3, "委託先事業者"参照)、または事業場の連携先がコンプライアンスを示し保証するために、クラウド事業者がどんなポリシーや手順を設定しているかを言明する。*	適用可能	適用可能
			DCA-1.4	*4. 上記の法令順守を証明する証拠となる事項。証拠となる事項は、様々ない形式をとる：自社による認証/評価証明、第三者監査（例：認証、評価証明、シール）、ログ、監査証跡、システム保守記録、より一般的な運用に関するシステム記録や、責任範囲下にある全ての処理操作の記録文書など。これらの事項は、以下のレベルにおいて提供する必要がある:* *(i) 組織的ポリシーのレベルにおいて、ポリシーが適正で適切であることを示す;* *(ii) ITコントロールのレベルにおいて、適切な管理策が展開されていることを示す；* *(iii) 運用レベルにおいて、計画通りにシステムが稼働していることを示す。異なるレベルに対応する証拠となる事項の例は、データ保護に関する認証、シール、マークである。*	適用可能	適用可能
2. CSPに関する連絡先とその役割	CAR	1. CSPに関する連絡先とその役割	CAR-1.1	*1. CSPの基本情報と連絡先の詳細を明示すること。（例：社名、住所、eメールアドレス、電話番号、設立地）；*	適用可能	適用可能
			CAR-1.2	*2. CSPの当該地域における代理店（例：EU内の代理店）について、その基本情報と連絡先の詳細を明示すること。（例：社名、住所、eメールアドレス、電話番号、設立地）；*	適用可能	適用可能
			CAR-1.3	*3. Sデータ取扱いにおけるCSPのデータ保護に関する役割を明確にすること。（すなわち、コントローラ、共同コントローラ、プロセッサまたはサブプロセッサの別）；*	適用可能	適用可能
			CAR-1.4	*4. データ保護責任者(Data Protection Officer, DPO)の連絡先の詳細を明示すること。DPOが存在しない場合は、顧客が要求を提出する先となるプライバシー問題の責任者について実施すること;*	適用可能	適用可能

			CAR-1.5	*5. 情報セキュリティ責任者(Information Security Officer, ISO)の連絡先の詳細を明示すること。ISOが存在しない場合は、顧客が要求を提出する先となるセキュリティ問題の責任者について実施すること。*	適用可能	適用可能
3. データ処理の方法.	**WWP**	**1. 一般的情報**	**WWP-1.1**	*データ管理者であるCSPは、次の点についてクラウド利用者に詳細情報を提供する:* *1. 処理に関連する個人データのカテゴリ;*	適用可能	適用不可能
			WWP-1.2	*2. データ処理の意図した目的と、合法的な方法でそのような処理を実行するために必要な法的根拠*	適用可能	適用不可能
			WWP-1.3	*3. データの取得者または取得者のカテゴリ*	適用可能	適用不可能
			WWP-1.4	*4. 個人データへのアクセスおよび修正または削除を要求する権利、データ主体に関する処理の制限を要求する権利、またはデータ処理に反対する権利、そしてデータの可搬性の権利を有すること*	適用可能	適用不可能
			WWP-1.5	*5. 該当する場合には、CSPが第三国または国際組織に個人情報を移転しようとしている状態において欧州委員会からの妥当であるとの判断が得られていないという事実、もしくは十分もしくは適切な保護が行われているという情報と、そのコピーを入手する手段もしくはその情報が得られる場所に関する情報*	適用可能	適用不可能
			WWP-1.6	*6. 個人データが保管される期間、または期間の明示が不可能な場合は、その期間を決定するために使用される基準*	適用可能	適用不可能
			WWP-1.7	*7. 処理が同意に基づいている場合、撤回前の同意に基づく処理の合法性に影響を与えることなく、同意を取り消す権利の存在*	適用可能	適用不可能
			WWP-1.8	*8. 監督機関（GDPR第4条（21）に定義されている）に苦情を提出する権利*	適用可能	適用不可能
			WWP-1.9	*9. 個人データの提供が、法的または契約上の要件であるか、契約を締結するために必要な要件であるかについて。併せて、データ主体が個人データの提供を義務づけられているかどうかと、個人データを提供できない場合に生じうる結果*	適用可能	適用不可能
			WWP-1.10	*10. プロファイリングを含め自動化された判断が行われること、およびそのロジックに関する意味のある情報、ならびにデータ主体にとってのそのような処理の影響度合いと想定される結果*	適用可能	適用不可能
			WWP-1.11	*11. 個人データが収集されている目的以外の目的のためにクラウド事業者が個人データをさらに処理しようとする場合、当該の更なる処理に先立って提供される、その別の目的のための情報*	適用可能	適用不可能
			WWP-1.12	*12. 個人データがデータ主体から得られたものではない場合には、その情報の入手源、そして該当する場合には、公開の情報源から得られたものかどうか*	適用可能	適用不可能
			WWP-1.13	*13. 合意されたクラウドサービスの提供のためにとられた行為（例えば、データストレージ）、クラウド利用者の要求で行われた行為（例えばレポート作成）、CSPのイニシアチブで行われた行為（バックアップ、災害復旧、不法行為モニタリングなど）*	適用可能	適用不可能

		WWP-1.14	*データ処理者であるCSPは、次のような情報をクラウド利用者に提供する* *14. クラウド利用者であるデータ管理者が、CSPであるデータ処理者に拘束力のある指示をすることができる範囲と様式*	適用不可能	適用可能
		WWP-1.15	*15. 関連するクラウドサービスに関する、機能の実装や削除などの関連する変更について、クラウド利用者にどのように通知するか。*	適用可能	適用可能
	2 個人データの所在場所	WWP-2.1	*1. 個人データが処理されるすべてのデータセンターまたはその他のデータ処理の場所（国単位）および、特に、データの保存、ミラーリング、バックアップ、および復元が行われうる場所（これはデジタル手段と非デジタル手段の両方を含む）。*	適用可能	適用可能
	3 下請事業者	WWP-3.1	*1. データ処理に参加する契約者および再委託先処理者。データ保護要件が満たされていることを確実にするための説明責任と実施責任の連鎖についての情報を含む。*	適用可能	適用可能
		WWP-3.2	*2. CSPは、クラウド利用者の特定の又は包括的な書面による許諾なしに、別の処理者を使用しないこと。*	適用不可能	適用可能
		WWP-3.3	*3. 契約（または他の拘束力のある法的行為）により、CSPとクラウド利用者の間で定められたのと同等のデータ保護義務を他の処理者にも課す。特に、EU内の適用法の要件を満たすような方法で適切な技術的および組織的措置を実施することの十分な保証の提供を含めて; [P]*	適用不可能	適用可能
		WWP-3.4	*4. 他の処理者がデータ保護義務を履行しない場合、当該他の処理者の義務の履行について、クラウド利用者に完全に責任を負う。*	適用不可能	適用可能
		WWP-3.5	*5. 委託先事業者または再委託先処理者の追加または変更について、クラウド利用者に通知するための手順。クラウド利用者は、変更の拒否や、契約を終了する権利を常に保持すること。*	適用可能	適用可能
	4 クラウド利用者のシステム上へのソフトウェアのインストール	WWP-4.1	*1. サービスの提供にあたって、クラウド利用者のシステムにソフトウェア（ブラウザプラグインなど）のインストールを必要とするかどうか。*	適用可能	適用可能
		WWP-4.2	*2. データ保護およびデータセキュリティの観点からの当該ソフトウェアの影響。*	適用可能	適用可能
	5 データ処理契約（またはその他の法的拘束力を伴う行為）	WWP-5.1	*1. クラウド利用者に代わってCSPによって実行される処理を規定し、処理の目的および期間を定め、個人データおよびデータ主体のカテゴリのタイプを規定し、クラウド利用者の義務および権利を定めたモデルデータ処理契約（またはその他の拘束力ある法的行為）。*	適用不可能	適用可能
		WWP-5.2	*契約またはその他の法律では、特にCSPが以下を行うことを規定している*	適用不可能	適用可能

				2. クラウド利用者からの文書化された指示があった場合のみ、個人データを処理すること。それには、第三国または国際機関への個人データの移転を含む。ただしCSPが規制対象となるEUまたは加盟国の法律によって要求されていない場合に限る。そのような場合、CSPは、その法律が重要な公益上の根拠に基づき情報提供を禁止する場合を除き、処理前に当該法的要請をクラウド利用者に通知すること。		
			WWP-5.3	*3. 個人データを処理する権限を与えられた人物が、EUまたは加盟国の法律で要求されている秘密保持の適切な法的義務を遵守していること、およびクラウド利用者からの指示を除いて個人データを処理しないこと。*	適用不可能	適用可能
			WWP-5.4	*4. 適用されるEU法で要求されるすべての措置をとること。*	適用不可能	適用可能
			WWP-5.5	*5. 他の処理者を使用する条件を尊重すること。（上記の3.3「委託先事業者」を参照）*	適用不可能	適用可能
			WWP-5.6	*6. データ処理の性質を考慮して、クラウド利用者がデータ主体の権利行使要求に応える義務を履行するために、可能な範囲で、適切な技術的および組織的措置によってクラウド利用者を支援すること。*	適用不可能	適用可能
			WWP-5.7	*7. データ処理の性質とデータ処理者が利用可能な情報を勘案して、クラウド利用者が以下の行為を行うことを助けること：データ処理のセキュリティに関する義務の遵守を確実にすること、監督当局への個人データ侵害の報告、データ主体への個人データ侵害の通知、データ保護影響評価。*	適用不可能	適用可能
			WWP-5.8	*8. クラウド利用者の選択により、データ処理に関連するサービスの提供が終了した後、すべての個人データを削除または返却すること。またEUまたは加盟国の法律が当該個人データの保管を要求しない限り、既存のコピーを削除すること。（第11章「データの留保、返却、および削除」を参照）*	適用不可能	適用可能
			WWP-5.9	*9. 関連するデータ保護義務の遵守を示すために必要なすべての情報をクラウド利用者に提供すること。クラウド利用者またはクラウド利用者が指定する監査人が実施する調査を含め、監査を受け入れ、監査に協力すること。*	適用不可能	適用可能
4. 記録の保持	**REC**	**1.CSPのデータ管理者のための記録の保持**	**REC-1.1**	*1. CSPのデータ管理者はクラウド利用者に対して、CSPの責任において、データ処理作業の記録を保持し、関係当局の要請に応じて提供できるようにすること。*	適用可能	適用不可能
			REC-1.2	*記録は以下の情報を含む:* *2. データ管理者の名前および連絡先の詳細、また該当する場合には、共同データ管理者、データ管理者の代理人、データ保護責任者の名前および連絡先の詳細。*	適用可能	適用不可能
			REC-1.3	*3. データ処理の目的;*	適用可能	適用不可能
			REC-1.4	*4. データ主体のカテゴリと個人データのカテゴリの記述;*	適用可能	適用不可能

			REC-1.5	*5. 個人データの開示先または開示予定先のカテゴリ。第三国または国際組織の開示先を含む。*	適用可能	適用不可能
			REC-1.6	*6. 該当する場合には、第三国または国際組織への個人データの移転。第三国または国際組織の識別情報と適切な予防措置を記載した文書を含む。*	適用可能	適用不可能
			REC-1.7	*7. 可能であれば、各種カテゴリのデータを削除するのに要する最大時間。*	適用可能	適用不可能
			REC-1.8	*8. 可能であれば、技術的、組織的なセキュリティ対策の総合的な記述。*	適用可能	適用不可能
		2 4.2 CSPのデータ処理者のための記録の保持	REC-2.1	*1. CSPのデータ処理者はクラウド利用者に対して、データ管理者に代わって実施するデータ処理作業のすべてのカテゴリの記録を保持し、関係当局の要請に応じて提供できるようにすること。*	適用不可能	適用可能
			REC-2.2	*記録は以下の情報を含む:* *2. データ処理者およびデータ処理者を代行するデータ管理者の名前と連絡先の詳細。あるいは、該当する場合には、データ処理者の代理人、データ保護担当者の名前と連絡先の詳細；*	適用不可能	適用可能
			REC-2.3	*3. 3. データ管理者に代わって行われる処理のカテゴリ;*	適用不可能	適用可能
			REC-2.4	*4. 該当する場合には、第三国または国際組織への個人データの移転。第三国または国際組織の識別情報と適切な予防措置を記載した文書を含む。*	適用不可能	適用可能
			REC-2.5	*5. 可能であれば、技術的、組織的なセキュリティ対策の総合的な記述。*	適用不可能	適用可能
5. データ移転.	**DTR**	**1. データ移転**	**DTR-1-1**	*1. 通常時／緊急時に関わらず、バックアップおよびリカバリを含め欧州経済領域（EEA（EU加盟国28カ国+アイルランド、リヒテンシュタイン、ノルウェー））を越えてデータが移転するか否かを示す。*	適用可能	適用可能
			DTR-1-2	*もしこのようなデータ転送がEU内の適用法令により制限されている場合:* *2. データ転送を可能とする法的根拠を明確にする（このデータ転送には、複数の下請け業者・協力企業を通して行われる転送も含む）。例えば、欧州委員会による十分性認定や、モデル条項／標準データ保護条項、承認済の行動規範もしくは認証メカニズム、拘束力のある企業の内部規定（BCR）、プライバシーシールドへの参加、などに基づくことを根拠にする。*	適用可能	適用可能
6. データセキュリティ措置	**SEC**	**1. データセキュリティ措置**	**SEC-1.1**	*1. 偶発的または違法な破壊、偶発的紛失、改変、不正使用、不正改造、不正開示、不正アクセス、その他違法な処理から個人データを守るために技術的措置、物理的措置、組織的措置をクラウド利用者に明示する。*	適用可能	適用可能

			SEC-1.2	*2. 以下の防御を確実にするための具体的な技術的、物理的、組織的対策（保護型、検出型、是正型の措置）をクラウド利用者に対して示す。*	適用可能	適用可能
			SEC-1.2.i	*(i) 可用性：インターネット接続のバックアップ、冗長ストレージ、効果的なデータバックアップ、リストアの仕組み、パッチ管理など、中断リスクの管理およびインシデントの防止、検出、対応のための手順および対策。*	適用可能	適用可能
			SEC-1.2.ii	*(ii) 完全性：CSPが完全性をどのように保証するかの方法（たとえば、メッセージ認証あるいは電子署名といった暗号メカニズムによる個人データの改ざん検出、誤り修正、ハッシュ化、ハードウェアの放射線や化学的変化への対策、物理的なアクセス・侵害・破壊＜対策＞、ソフトウェアのバグ、設計上の欠陥、人的ミス＜への対策＞など。）*	適用可能	適用可能
			SEC-1.2.iii	*(iii) 機密性：CSPが、契約的観点から機密性を確保し認可された人物のみがデータにアクセスできることを確実にするためにとる方法。特に、通信中および保存中の個人データの仮名化および暗号化、承認メカニズムおよび強力な認証。また契約の視点からは、CSPとその全ての従業員（正社員、パートタイム、契約社員）ならびにデータにアクセスできる委託事業者を拘束する秘密保持契約、秘密保持条項、ポリシーや手順などの手段。*	適用可能	適用可能
			SEC-1.2.iv	*(iv) 透明性：透明性を維持し、利用者による監査を可能にするためにCSPが適用した技術的、物理的、組織的措置。（セクション7“モニタリング”を参照）*	適用可能	適用可能
			SEC-1.2.v	*(v) 隔離（目的制限）：CSPが個人データに対する隔離をどのように確保するか；（たとえば、個人データにアクセス権限と役割の適切なガバナンス（定期的に見直す）、最小権限の原則を基にしたアクセス管理； ハイパーバイザのハードニング（要塞化）； 異なるクラウド利用者の間に物理リソースをシェアするために仮想マシンが使用される場合は、共有資源の適切な管理）*	適用可能	適用可能
			SEC-1.2.vi	*(vi) 介入性：クラウド事業者がデータ主体のアクセス権、異議の権利、忘れられる権利、処理を制限する権利、データ移転先の十分性を確実にする方法。それにより、データが委託先によって更に処理される場合を含め、これらの要件に対する技術的および組織的な支障がないことを証明する（関連事項：セクション9“データの移植性、移行および転送”）。*	適用可能	適用可能
			SEC-1.2.vii	*(vii) ポータビリティ（移植性）： 後述のセクション9 “データの移植性、移行および転送”を参照*	適用可能	適用可能
			SEC-1.2.viii	*(viii) 説明責任（責任追跡性）： 前述のセクション1 “コンプライアンスと説明責任についてのCSPの言明” を参照*	適用可能	適用可能
7. モニタリ	**MON**	**1. モニタリ**	**MON-**	*1. PLA[V3]が規定する適切なプライバシー・セキ*	適用可能	適用可能

ング		ング	1.1	*ユリティ施策が継続的に順守されていることを確実にするために、利用者はモニタリングと監査（例：CSPまたはその下請けが実施する該当の処理作業に対するロギング、報告実施、第一者および第三者監査）を行わなければならない場合があることをクラウド利用者に示すこと。*		
8. 個人データ違反.	PDB	1. 個人データ違反	PDB-1.1	*CSPはクラウドの顧客に次のように明示する:* *1．決められた時間内に、CSPおよび/またはその下請け業者によって処理される顧客データに影響する個人データ違反の顧客への通知方法を指定する。*	適用可能	適用可能
			PDB-1.2	*2．可能であれば、関連する個人データレコードのカテゴリーとおおよその数を含む個人データ違反の内容を記述する;*	適用可能	適用可能
			PDB-1.3	*3．より多くの情報を入手できるデータ保護責任者またはその他の連絡先の名前と連絡先の詳細を通知する（第2章「CSP関連窓口とその役割」を参照）;*	適用可能	適用可能
			PDB-1.4	*4．個人データ違反の可能性がある結果を記述する;*	適用可能	適用可能
			PDB-1.5	*5．必要に応じて起こり得る悪影響を軽減するための措置を含め、個人データ違反に対処するために取られる（取られることを提案する）措置を記載する。*	適用可能	適用可能
			PDB-1.6	*6．個人データ違反に気づいてから72時間以内の監督機関への個人データのセキュリティ違反の通知方法を明示する;*	適用可能	適用不可能
			PDB-1.7	*7．個人データ違反が自然人の権利および自由に高いリスクをもたらす可能性がある場合、過度の遅滞なくデータ主体への通知方法を明示する。*	適用可能	適用不可能
9. データの移植性、移行および転送	PMT	1. データの移植性、移行および転送	PMT-1.1	*CSPはクラウドカスタマに対して以下を明確にする:* *1. CSPが、個人データを、構造化され、一般的に使用されている機械で判読可能で、相互運用可能な形式で送信する能力の点で、データの移植性を保証する方法：*	適用可能	適用可能
			PMT-1.1.i	*(i) クラウド顧客に対して（'転送'、例えば社内IT環境への）;*	適用可能	適用可能
			PMT-1.1.ii	*(ii) 直接、データ主体に対して;*	適用可能	適用可能
			PMT-1.1.iii	*(iii) 他のサービスプロバイダに対して（'移行'、例えばダウンロードツール又はAPI, APIsによる）*	適用可能	適用可能
			PMT-1.2	*2. データを他のプロバイダ、あるいは、社内のIT環境へ移行できるかについて、CSPが、どのようにして、また、どのようなコストで、顧客を支援するか。*	適用可能	適用可能

10. 処理の制限	**ROP**	**1. 処理の制限**	**ROP-1.1**	*1. 個人データの処理を制限する可能性が、どのように認められているか； 処理が制限された場合、当該個人データは、保存を除きデータ主体の同意に基づくか、法法的主張時の立証、行使若しくは抗弁のため、又は他の自然人若しくは法人の権利を保護するため、若しくはEU 若しくは加盟国の重要な公共の利益のためだけに取り扱われるかについて、クラウド利用者に説明する。*	適用可能	適用可能
11. データの留保、返却、および削除	**RRD**	**1.データの留保、返却、および削除のポリシー**	**RRD-1.1**	*1. クラウド利用者に、CSPのデータ留保のポリシーとタイムライン、およびサービスが終了した後の個人データ返却、またはデータ削除の条件を説明すること。*	適用可能	適用可能
			RRD-1.2	*2. クラウド利用者に、CSPの委託先事業者のデータ留保のポリシーとタイムライン、およびサービスが終了した後の個人データ返却、またはデータ削除の条件を説明すること。*	適用可能	適用可能
		2. データ留保	**RRD-2.1**	*3. 個人データが留保される、または留保される可能性がある期間、またはそれが不可能な場合は、その期間を決定するために使用される基準を示すこと。*	適用可能	適用可能
		3. 特定のセクターの法的要件を満たすためのデータ留保	**RRD-3.1**	*1. クラウド利用者がCSPに特定のセクターの法律や規制を遵守するように要求することができるかどうか、どのように要求できるかを示すこと。*	適用可能	適用可能
		4. データの返却および/または削除	**RRD-4.1**	*1. データの移植性（上記のセクション9'データの移植性、移行、転送バック'も参照）を担保する形式で個人データをクラウド利用者に返却する手順、*	適用可能	適用可能
			RRD-4.2	*2. データ削除に利用できる、または使用される方法、*	適用可能	適用可能
			RRD-4.3	*3. クラウド利用者がデータを削除（または削除要求）した後、または契約終了後にデータが留保されるかどうか、*	適用可能	適用可能
			RRD-4.4	*4. データを留保する特定の理由、*	適用可能	適用可能
			RRD-4.5	*5. CSPがデータを留保する期間を示すこと。*	適用可能	適用可能
12. クラウドカスタマとの協力	**CPC**	**1. クラウドカスタマとの協力**	**CPC-1.1**	*1. CSPがクラウドカスタマと協力して、適用可能なデータ保護条項（例えば、アクセス権、訂正、消去「忘れられる権利」、処理の制限、移植性）、セキュリティ/データ侵害の場合のフォレンジック分析を含むインシデント管理に使用する。また、セクション6「データセキュリティ対策」およびセクション8「個人データの侵害」も併せて参照のこと。*	適用可能	適用可能
			CPC-	*2. コンプライアンスを示すために必要な情報をク*	適用可能	適用可能

			1.2	*ラウドカスタマおよび管轄の監督当局に提供すること。また、セクション1「コンプライアンスと説明責任に関するCSP宣言」も併せて参照のこと。*		
13. 法的な開示要求	**LRD**	**1. 法的な開示要求**	**LRD-1.1**	*1. 法執行当局による個人情報の開示要求を管理し対応するためのプロセスは、法執行機関の調査の守秘義務を守るための刑法上の禁止など特に禁止されていない限り、関心のある顧客への通知手順に特に注意を払うこと。*	**適用可能**	**適用可能**
14. クラウドカスタマの救済措置	**RMD**	**1. クラウドカスタマの救済措置**	**RMD-1.1**	*1. CSPおよび/またはCSPの下請け業者（セクション3「データが処理される方法」、より具体的にはセクション3.3「下請け業者」を参照）においてPLAに基づく契約上の義務違反が発生した場合、クラウド顧客が利用できる救済策を示す。救済には、クラウド顧客のサービスクレジットおよび/またはCSPに対する契約上の罰金が含まれる可能性があります。*	**適用可能**	**適用可能**
15. 15. CSP保険の方針	**INS**	**1. 15. CSP保険の方針**	**INS-1.1**	*1. 保険証券に記載されているCSP事業に関連する補償範囲を明示すること（例えば、委託先の事業者によるデータ保護義務違反まで補償範囲として含むデータ保護遵守保険や、セキュリティ侵害や情報漏えい保険までを含むサイバー保険についてである）。*	**適用可能**	**適用可能**

附属書 2: STATEMENT OF ADHERENCE TEMPLATE

CSA Code of Conduct (CoC): Statement of Adherence Self-Assessment

1. Name and URL/Address

Name	
URL/Address	

2. Services covered by the PLA Code of Practice (CoP)

Please provide a list with the name(s) of the service(s) covered by the PLA CoP will be provided in the table below.

Service 1 name	
Service 2 name	
…	
Service *n* name	

3. Means of Adherence

Self-Assessment

4. Scope of Adherence

~~Please provide a description of the assessment scope for each of the s~~ervices listed in (2) with regards to the PLA Code of Practice.

Description

5. PLA Code of Practice version used

Version ID	(e.g., v.3.0)

6. Issue/Expiry date

Issue Date	
Expiry Date	

7. Legal representative/DPO signed by

By signing this statement of adherence, the organization/company confirms that:

a. As of this date, the services listed in (2) adhere to the CSA CoC requirements (see CSA CoC section 3.3, “CSA CoC Marks issuing, Statement of Adherence publication and complaints management”).

b. The CSA CoC self-attestation mark will have a validity of 12 months from the day of their issuance and should be renewed after this period. Moreover, the CSA CoC self-attestation must be revised every time there’s a change in the company’s relevant policies or practices.

Name	
Title	
Date	

CSA Code of Conduct (CoC): Statement of Adherence 3rd Party Certification

1. Name and URL/Address

Name	
URL/Address	

2. Services covered by the PLA Code of Practice (CoP)

Please provide a list with the name(s) of the service(s) covered by the PLA CoP will be provided in the table below.

Service 1 name	
Service 2 name	
…	
Service *n* name	

3. Means of Adherence

3rd Party Certification

4. Scope of Adherence

Please provide a description of the assessment scope for each of the services listed in (2) with regards to the PLA Code of Practice.

Description

5. PLA Code of Practice version used

Version ID	(e.g., v.3.0)

6. Certification Body

Name	

7. Country of issuing

Name	

8. Certificate number

Name	

9. Issue/Expiry date

Issue Date	
Expiry Date	

10. Legal representative/DPO signed by

By signing this statement of adherence, the organization/company confirms that:

a. As of this date, the services listed in (2) adhere to the CSA CoC requirements (see CSA CoC section 3.3, “CSA CoC Marks issuing, Statement of Adherence publication and complaints management”).

b. The third-party certification compliance marks will have a validity of 12 months from the day of their issuance and should be renewed after this period. Moreover, third-party certification must be revised every time there’s a change in the company’s relevant policies or practices.

Name	
Title	
Date	

附属書 3：CSA STARプログラムとオープン認証フレームワーク (OCF)

CSAは、2011年にCSA Security Trust and Assurance Registry（STAR）を開始し、
透過的な情報セキュリティ保証を提供することにより、クラウド市場における信頼を獲得している。

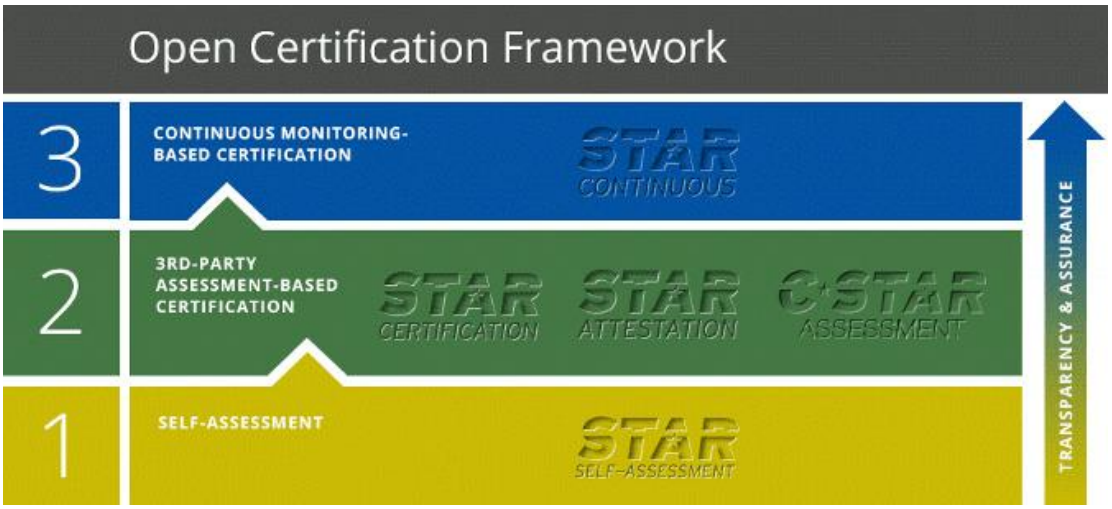
CSA STARは、クラウド利用者（CSC）、クラウド事業者（CSP）、クラウド監査人などのクラウドステークホルダーに、CSAのベストプラクティスであるクラウドコントロールマトリックス（CCM）とコンセンサスアセスメントイニシアチブ（CAI）に基づく内部デューディリジェンスの結果に関する情報を公表できる公開リポジトリ（STARレジストリ）を提供する。

CSA STARをサポートするために必要な技術能力を開発することを目的として、2012年にCSA オープン認証フレームワーク（OCF)ワーキンググループ（WG）が開始された。

OCF WGは、CSAセキュリティ認証フレームワークと、フレームワークに含まれている認証スキームを定義している。

WGは、オープン認証フレームワークを3つのレベルの信頼に基づいた多層構造として定義した：

- レベル1、自己評価：STAR自己評価
- レベル2、第三者評価：STAR認証、STAR評価証明、C-STAR評価
- レベル3、継続的モニタリング/監査：STAR継続型



2012年に、CSA STARプログラムは、CSA STARの取り組みを支援し、OCFの実施を管理する手段として立ち上げられた。

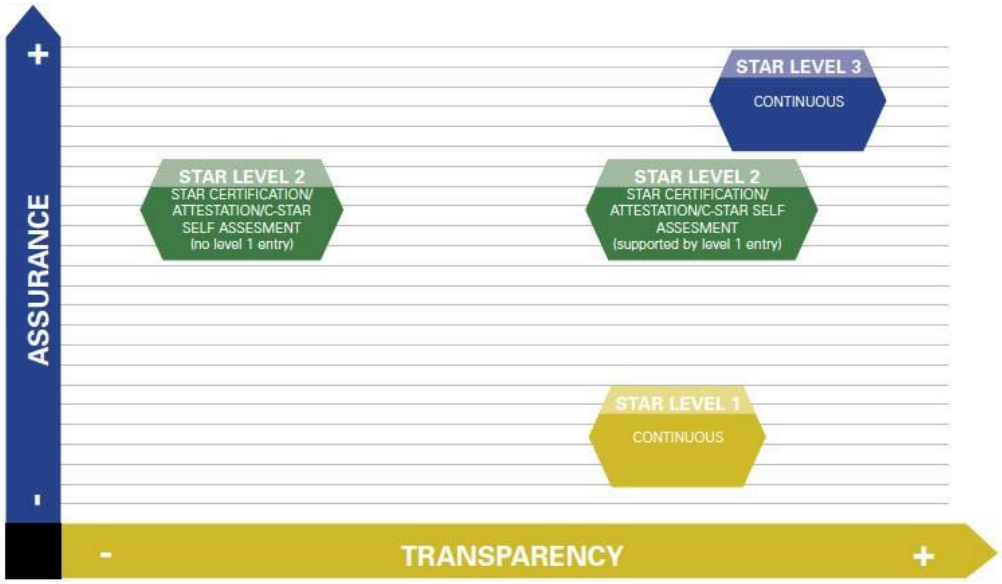
現在、STARプログラムは、自己評価（レベル1）および第三者評価ベースの認証/評価証明（レベル2）を提供している。

継続的モニタリング/監査ベースの認証が開発中です。

OCFレベル間の関係は次のとおりです。

「保証」の観点からは、OCFレベル1は適度な保証を提供し、OCFレベル2は高い保証を提供し、OCFレベル3は非常に高い保証を提供する。

「透明性」の観点から、OCFレベル1は良好な透明性を提供し、OCFレベル2は低い透明性から高い透明性を提供し、OCFレベル3は非常に高い透明性を提供する。



3つのOCFレベルによって提供される透明性は、必ずしも3つのレベルの保証に対応するとは限らない。例えば、OCFレベル1は、OCFレベル2よりも優れた透明性を提供することができる。なぜなら、OCFレベル2のSTAR認定スキームもSTAR評価証明スキームも、組織がセキュリティ管理策を公的に利用可能にすることを要求していないからである。

CSAは、OCFレベル2での認定を目指す組織が、OCFレベル1で最初に自己評価することを奨励する。

附属書 4: CODE OF ETHICS

1. Scope

This Statement of Ethics applies to all Board Members, officers, full-time and part-time employees, contractors, or volunteers of the Cloud Security Alliance ("CSA Parties").

2. Definitions

Board Member: a member of the Board of Directors of the Cloud Security Alliance in office.
CSA Party: a Board Member, officer, full-time or part-time employee, contractor, or volunteer of the Cloud Security Alliance.
Volunteer: an individual who spends significant time advancing the mission of the Cloud Security Alliance as a member of its Board of Directors or through service on an advisory committee to the Board of Directors.

3. Ethics Principles

The CSA Parties, by virtue of their roles and responsibilities within the Cloud Security Alliance, represent the Cloud Security Alliance to the larger society. They have a special duty to observe the highest standards of personal and professional conduct.

The Cloud Security Alliance requires all CSA Parties to comply with the following Ethics Principles:

- our words and actions embody respect for truth, fairness, free inquiry, and the opinions of others;
- we respect all individuals without regard to race, colour, sex, sexual orientation, marital status, creed, ethnic or national identity, handicap, or age;
- we uphold the professional reputation of others and give credit for ideas, words, or images originated by others;
- we safeguard privacy rights and confidential information;
- we do not grant or accept favours for personal gain;
- we do not solicit or accept favours where a higher public interest would be violated;
- we avoid actual or apparent conflicts of interest and, if in doubt, seek guidance from appropriate authorities;
- we follow the letter and spirit of the laws and regulations affecting the Cloud Security Alliance;
- we actively encourage colleagues to join us in supporting these laws and regulations and the standards of conduct in these Ethics Principles.

4. Review and Acknowledgment of Statement of Ethics

Upon the entry into force of this Statement of Ethics, and thereafter for each calendar year before the last day of January, each CSA Party shall be provided with and asked to review a copy of this Statement of Ethics and to acknowle.g.,in writing that he/she has read, understood and agreed to abide by this Statement of Ethics.

5. Entry into Force and Implementation

This Statement of Ethics is approved by the Board of Directors of the Cloud Security Alliance. This Statement of Ethics will enter into force as of January 1, 2012. The Board of Directors directs the Cloud Security Alliance Executive Director to ensure that this Statement of Ethics is given to and acknowledged by all CSA Parties.

6. Oversight

The Board shall have direct responsibility for the oversight of this Statement of Ethics and for the establishment of procedures to support this Statement of Ethics.

7. Review and Changes

This Statement of Ethics shall be reviewed and updated as necessary, annually by the Board of Directors. Any changes to the Statement of Ethics shall be communicated to all CSA Parties.

附属書 5: PRIVACY LEVEL AGREEMENT WORKING GROUP CHARTER

EXECUTIVE OVERVIEW

Data protection compliance is becoming increasingly risk-based.[1] Data controllers and processors are accountable for determining and implementing in their organisations appropriate levels of protection of the personal data they process. In such decision, they have to take into account factors such as state of the art of technology; costs of implementation; and the nature, scope, context and purposes of processing; as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.[2] As a result, Cloud Service Providers (CSPs) will be responsible for self-determining the level of protection required for the personal data they process.

In this scenario, the PLA Code of Conduct gives guidance for legal compliance and the necessary transparency on the level of data protection offered by the CSP.

Privacy Level Agreements (PLAs) are essentially intended to provide:

- Cloud customers of any size with a tool to evaluate the level of personal data protection offered by different CSPs (and thus to support informed decisions)[3]
- CSPs of any size and geographic location with a guidance to comply with European Union (EU) personal data protection legislation and to disclose, in a structured way, the level of personal data protection they offer to customers.

PLA Code of Conduct is designed to meet both actual, mandatory EU legal personal data protection requirements (i.e., Directive 95/46/EC and its implementations in the EU Member States), by leveraging the PLA [V2] structure, and the forthcoming requirements of the GDPR. This specific feature makes PLA [V3] a unique tool that helps CSPs, cloud customers and potential customers manage the transition from the old to the new EU data protection regime, and contributes to the proper application of the GDPR into the cloud sector. PLA [V3] specifies the application of the GDPR in the cloud environment, primarily with regard to the following categories of requirements:

- fair and transparent processing of personal data;
- the information provided to the public and to data subjects (as defined in Article 4 (1) GDPR);
- the exercise of the rights of the data subjects;
- the measures and procedures referred to in Articles 24 and 25 GDPR and the measures to ensure security of processing referred to in Article 32 GDPR;

[1] See, e.g., Preamble 83 and Articles 25, 32, 33, 34 and 35 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR)

[2] See, e.g., Articles 24, 25, 32, 35 and 39 of the GDPR.

[3] "All cloud providers offering services in the European Economic Area (EEA) should provide the cloud client with all the information necessary to rightly assess the pros and cons of adopting such services. Security, transparency, and legal certainty for the clients should be key drivers behind the offer of cloud computing services." Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing ("A.29WP05/2012"), p. 2; "A precondition for relying on cloud computing arrangements is for the controller [cloud client] to perform an adequate risk assessment exercise, including the locations of the servers where the data are processed and the consideration of risks and benefits from a data protection perspective." p. 4 id. (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf).

- the notification of personal data breaches to supervisory authorities (as defined in Article 4 (21) GDPR) and the communication of such personal data breaches to data subjects; and
- the transfer of personal data to third countries.

Additionally, PLA [V3] contains mechanisms that enable the body referred to in Article 41 (1) GDPR to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors that undertake to apply it, without prejudice to the tasks and powers of competent supervisory authorities pursuant to Article 55 or 56 GDPR.

BACKGROUND

The Cloud Security Alliance ("CSA") published in 2013 the "Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union" (PLA [V1]) and in 2015 the "Privacy Level Agreement [V2]: A Compliance Tool for Providing Cloud Services in the European Union" (PLA [V2]).

Based on the work already created by the, i.e. PLA V1 and PLA V2, the CSA PLA WG will develop "Privacy Level Agreement [V3] Code of Conduct. A Compliance Tool for Providing Cloud Services in the European Union" (PLA [V3]) to address the upcoming change to the data protection laws of the European Union and Europe Economic Area Member States to the General Data Protection Regulation, Regulation (EU) 2016/679 also known at the GDPR.[4]

PRACTICAL USE

The PLA CoC is intended to be used as the structure for the creation of an appendix to a Cloud Services Agreement that would describe the level of privacy and data protection that the CSP undertakes to commit to provide and maintain with respect to the personal data that its customer will provide to the CSP and process through the CSP's service(s).

The PLA Code of Conduct provides a structure for CSPs to register the completed Privacy Statement developed in accordance to the PLA Code of Practice [V3] with the CSA STAR Service that will be used as a custodian.

The adoption of the PLA CoC worldwide can promote a powerful global industry standard, enhance harmonization and facilitate compliance with applicable EU data protection law.

[4] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=it.

WORKING GROUP SCOPE AND OBJECTIVES

The working group is chartered to research in the area of privacy and data protection compliance for cloud computing services at global scale and will pursue the following three goals.

Objective 1: Define a Privacy Level Agreement Code of Practice that addresses the requirements set forth in the GDPR, based on the experience of PLA [V2].

Objective 2: Define a Governance Structure and mechanisms of adherence to the PLA CoC.

Objective 3: Participate in the implementation and management over time of the PLA CoC.

Objective 4: Monitor the legal and regularly landscape so to be able to update the PLA Code of Practice.

Objective 5: Provide expert opinion to CSA when complaints about PLA Self Attestation or Certification are submitted.

Objective 6: Provide expert opinion to CSA Open Certification Working Group on the PLA CoC third party certification scheme.

WORKING GROUP STRUCTURE AND FUNCTIONING

Co-Chairs

The working group will be led by co-chairs in addition to the selected leadership. The co-chairs will assist with the leadership responsibility of the working group. The co-chairs may appoint others as necessary to assure the effective execution of the defined research.

Sub-Work Groups

Ad hoc sub-working groups comprised of subject matter experts may be formed to plan or execute any related outreach, awareness, or research opportunities. Such sub-working groups shall report directly to the PLA Working Group.

The Working Group may also choose to allow resource sharing between cloud communities and other CSA working groups to assist in the timely completion of projects, programs and other activities needed to support/enable the working group's defined body of work.

Membership

Any individual with the appropriate expertise can participate to the activities of the working group. The table below provides an example of the organizations that CSA encourages to join the PLA Working Group.

Community	Purpose	Example
International, Regional, National Regulatory Bodies, Agencies, Supervisory Authorities, and Institutions	Policy makers and supervisory authorities who can ensure appropriate alignment with legal and regulatory requirements	· European Commission · European Data Protection Board · EDPS · National Supervisory Authorities · ENISA · METI · IDB - IDA · USA FTC · Etc.
CSA OCF Co-Chairs	To maintain the alignment with OCF and assess the feasibility of the introduction of a privacy module / seal in the OCF.	· OCF Co-chairs
CSA GRC Stack WG Co-Chair	Maintain alignment GRC Stack research initiatives	· Cloud Controls Matrix (CCM) · Consensus Assessment Initiative (CAI) · CloudAudit · Cloud Trust Protocol (CTP)
CSA International Standardization Council	Maintain alignment with ISC work	· ISC Co-chairs
Internal Auditors/Consultants	Lead representatives from organization who provides internal auditing services and consultancies.	· Big Four (PwC, E&Y, Deloitte, KPMG) · Representatives of smaller Auditing and consulting firms
Other research effort	Representatives from ongoing research project with similar scope to maintain alignment and consistency between projects	· A4Cloud · Internet2

CSA Corporate Members (Cloud Service Providers	Representatives from cloud service/solution providers to validate applicability of the PLA4EU Compliance and the feasibility of the introduction of privacy certification	·
Independent Subject Matter Expert	Independent Subject Matter Expert	· European Privacy Association (EPA) · International Association of Privacy Professionals (IAPP)
Cloud Users/Consumers	Representatives from corporate cloud provider and/or representatives of users/consumers organization to ensure alignment with user requirements and needs	· EuroCio · etc.

Alignments with Other Groups

The working group will share research and align with other CSA Working Groups, advisory groups, and industry partners such as SDO's.

Operations

Advisory
The PLA Working Group will be advised by the CSA Subject Matter Expert (SME) Advisory Council, International Standardization Council (ISC), and CSA Executive Team to ensure that the research under the working group is within the scope of the CSA and aligns with other industry partner research. The research will remain unique to industry and make reference to any redundant or replicated works.

Research Lifecycle
The PLA Working Group will follow the development of the CSA research lifecycle for all projects and initiatives.

Peer Review
The PLA Working Group will seek CSA's help in reaching out to peers for reviewing our charter, publications, and other documented activities of the working groups.

Communications Methods

Infrastructure & Resource Requirements
The PLA Working Group will be composed of CSA volunteers; it will have co-chairs and/or committee(s). The working group will require typical project management, online workspace and technical writing assistance.

Working Group Meetings

The PLA Working Group will hold periodic conference calls. Attendance or participation in the online workspace by the Principal or Alternate is required. The Alternate must have full authority to act on behalf of the Principal if the Principal is absent. In-person meetings will happen in a location to be determined**.**

Decision-making Procedure

Decision shall be made by simple majority of the PLA Working Group members (including the Co-Chairs).

Definition of a majority

1. A majority shall consist of more than half the members participating in person or by phone, and voting
2. In computing a majority, all members casting a vote for, against or abstention) shall be counted and taken into account.
3. In case of a tie, a proposal or amendment shall be deemed rejected.
4. For the purpose under this Charter, a "member present and voting" shall be a member voting for, against, or "no opinion" a proposal, including proxy representative. Proxy where authority is delegated through a written statement or non-repudiated email will be declared and inspected for validity by a co-chair before voting starts.

Abstentions of more than fifty per cent

When the number of abstentions exceeds half the total number of votes cast (for, against, abstentions), consideration of the matter under discussion shall be postponed to a later meeting, at which time the matter shall be further discussed, any documentation or decision reviewed and amended, and the revised proposal shall be submitted again to a vote by the Working Group.

Voting procedures

The voting procedures are as follows:

1. By email sent to the co-chairs unless a secret ballot has been requested;
2. By a secret ballot, sent by mail to a trusted third party, if at least 20% of the members present and entitled to vote so request before the beginning of the vote (online voting is applicable)

Before commencing a vote, the Chair(s) shall review any request as to the manner in which the voting shall be conducted, and then shall formally announce the voting procedure to be applied and the issue to be submitted to the vote. The Chair(s) shall then declare the beginning of the vote and, when the vote has been taken, shall announce the results.

In the case of a secret ballot, the secretariat shall at once take steps to ensure the secrecy of the vote.

Deliverable approval and endorsement process

PLA Working Group deliverables are subject to the approval and endorsement of CSA. The decision is based on the advice of the SME Advisory Council.

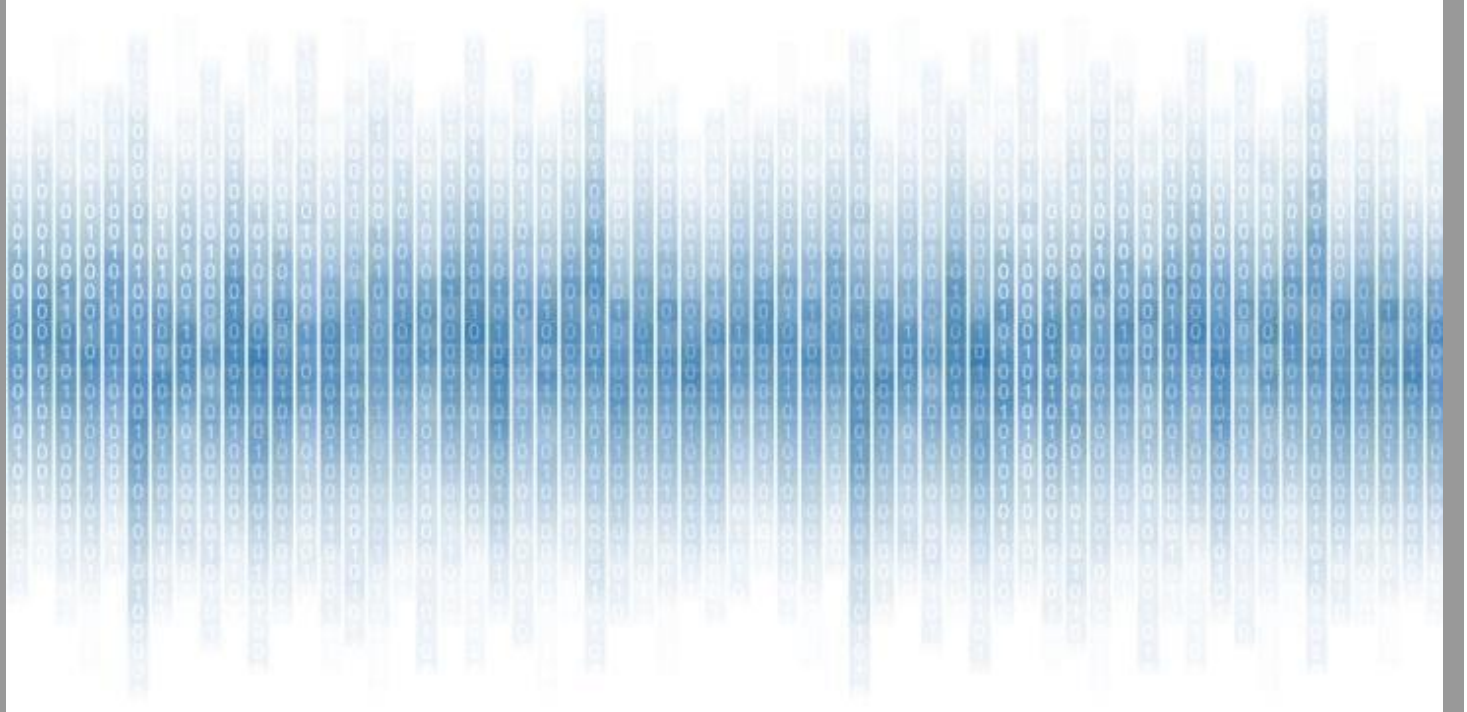
DELIVERABLES

1. PLA CoC objectives, scope, methodology, assumptions and explanatory notes
2. Privacy Level Agreement [V3] Code of Practice
3. PLA Code of Conduct (CoC) Governance and adherence mechanisms
4. The PLA Template
5. The PLA Statement of Adherence template
6. Presentations and other awareness material
7. Procedure for complain management
8. PLA Code of Practice change management process

DURATION

This charter will be valid until 31 March 2019

附属書 6: OPEN CERTIFICATION FRAMEWORK WORKING GROUP CHARTER



Open Certification Framework Working Group

Charter

2017

TABLE OF CONTENTS

WORKING GROUP EXECUTIVE OVERVIEW

Mission

The mission of the Open Certification Framework Working Group is to develop, maintain, review, update, support the implementation of all the certification schemes included in the CSA Security Transparency Assurance Registry (STAR) Program. The OCF WG focuses on information security and privacy certification schemes for processes and product in the areas of cloud computing and mobile.

Working Group Scope and Responsibilities

The Cloud Security Alliance has identified gaps within the IT ecosystem that are inhibiting market adoption of secure and reliable cloud services. Consumers do not have simple, cost effective ways to evaluate and compare their providers' resilience, data protection and privacy capabilities and service portability.

The CSA Open Certification Framework (OCF) is an industry initiative to allow global, trusted certification of cloud providers. It is a program for flexible, incremental and multi-layered cloud provider certification according to the Cloud Security Alliance's industry leading security guidance and control framework.

The objective of the program will be to harmonize with existing third-party certifications and audit standards to avoid duplication of effort and cost.

The CSA OCF is based upon the control capabilities achieving maturity through continuous assurance as defined within the CSA Governance, Risk and Compliance (GRC) Stack and Privacy Level Agreement research initiatives.

The CSA OCF will support several tiers, recognizing the varying assurance requirements and maturity levels of providers and consumers. These will range from the CSA Security, Trust and Assurance Registry (STAR) self-assessment to high-assurance specifications that are continuously monitored.

Discussions and decisions/changes proposed by the OCF and its working groups are considered privileged and confidential and are not to be made public until either the proposed changes have been finalized or a vote has been taken and so documented.

Working Group Membership

Eligible members are of the OCF WG

- CSA enterprise customer corporate members (Enterprise Users)
- CSA solution provider corporate members (CSPs)
- International, Regional, National Regulatory Bodies, Agencies and Institutions (European Commission, Article 29 Working Party, ENISA, METI, IDB – IDA, NIST, FedRAMP, USA DoD, USA FTC, etc)
- SDOs and other organizations (e.g. ISO/IEC / JTC 1 / SC27, SC38, ITU-T, ETSI, W3C, ISACA, AICPA, JIPDEC, JASA, etc)
- Representatives of relevant research project not directly run under the auspices of the CSA, but relevant to the activities of the OCF WG (e.g. Accountability for Cloud, CUMULUS, SLA Ready, SPECS, Internt2/NET+, Cloud for Europe, etc.)
- Representative of trade and users associations (e.g. EuroCIO, etc.)

Working Group Structure

Co-Chairs

The working group will be led by co-chairs in addition to the selected leadership. Co-chairs must be members of CSA, unless the CSA Executive Team has granted an exception. The co-chairs will assist with the leadership responsibility of the working group. The co-chairs may appoint others as necessary to assure the effective execution of the defined research. Responsibilities of the co-chair include:

- Define the work plan for each year (e.g., meetings and expected deliverables)
- Ensure progress of work according to the work plan
- Report to the CSA Executive Team on execution risks and suggest possible solutions
- Convene meetings when necessary and act as Chairperson of OCF.
- Lead the preparation of draft deliverables, or identify a suitable person within the OCF who will take the role of main editor/rapporteur of the deliverable
- Ensure that guidance provided in the current OCF charter is followed
- Ensure that relevant documents are circulated to OCF members

Committees

The working group may designate and organize subcommittees to aid in research with the initiatives pertaining to the subject matter of the working group.

Sub-Work Groups

Ad hoc sub-work groups comprised of subject matter experts may be formed to plan or execute any related outreach, awareness or research opportunities. Such sub-working groups shall report directly to the main working group.

Alignments with Other Groups

The OCF working group may also choose to allow resource sharing between cloud communities and other CSA working groups to assist in the timely completion of projects, programs and other activities needed to support/enable the working group's defined body of work, on demand basis. The list other groups that the OCF working group will be working closely with includes, but is not limited to:

- CSA Cloud Trust Working Group:
  - Specifically collaborating on the implementation of the OCF Level 3.
- CSA GRC Stack Working Group:
  - Specifically collaborating on…
    - defining "OCF compliance profiles" (e.g. subsets and addendum of CCM relevant to a certain sector, service offering)
    - ensure the controls and measures relevant to accountability are specified and integrated
- CSA PLA Working Group:
  - Specifically collaborating on the development of a scheme to certify organization against the requirements included in the PLA Code of Conduct v3.
- CSA MAST Initiative Working Group:
  - Specifically collaborating on development of a scheme (tentatively named CSA STAR Mobile) to certify mobile applications against the requirements to be developed from the MAST whitepaper
- Additional groups:
  - CSA Cloud Audit Working Group
  - EC C-SIG
  - ENISA
  - ISO SC 27
  - NIST
  - AICPA
  - The German Federal Office for Information Security (BSI)
  - and other (e.g. ANSSI)

Operations

Advisory

The CSA Working Group will be advised by the CSA Subject Matter Expert (SME) Advisory Council, International Standardization Council (ISC), and CSA Executive Team to ensure that the research under the working group is within the scope of the CSA and aligns with other industry partner research. The research will remain unique to industry and make reference to any redundant or replicated works.

Research Lifecycle

The CSA Working Group will follow the development of the CSA research lifecycle for all projects and initiatives: https://downloads.cloudsecurityalliance.org/initiatives/general/CSA_Research_Lifecycle_FINAL.pdf

Peer Review

We will seek CSA's help in reaching out to peers for reviewing our charter, publications, and other documented activities of the working groups.

Communications Methods

Infrastructure & Resource Requirements

The working group will be composed of CSA volunteers; it will have co-chairs and/or committee(s). The working group will require typical project management, online workspace and technical writing assistance.

Work Group Conference Calls and In-person Meetings

The working group will hold conference calls no less than bi-monthly. Attendance or participation in the online workspace by the Principal or Alternate is required. The Alternate must have full authority to act on behalf of the Principal if the Principal is absent. In-person meetings will happen in a location to be determined.

Decision-Making Procedures

A. Definition of a majority

1. A majority shall consist of more than half of the members present and voting.
2. In computing a majority, members abstaining shall not be taken into account.
3. In case of a tie, a proposal or amendment shall be considered rejected.
4. For the purpose under this Charter, a "member present and voting" shall be a member voting "for" or "against" a proposal, including proxy representative.
5. Proxy where authority is delegated through a written statement or non-repudiated email should be declared and inspected for validity by the working group leadership before voting starts.

B. Abstentions of more than fifty percent

1. When the number of abstentions exceeds half the number of votes cast (for votes, plus against votes, plus abstention votes), consideration of the matter under discussion shall be postponed to a later meeting, at which time abstentions shall not be taken into further account.

C. Voting procedures

1) The voting procedures are as follows:
    a) By a show of hands as a general rule, unless a secret ballot has been requested; if at least two members, present and entitled to vote, so request before the beginning of the vote and if a secret ballot under b) has not been requested, or if the procedure under a) shows no clear majority
    b) By a secret ballot, if at least five of the members present and entitled to vote so request before the beginning of the vote (online voting is applicable)

2) The Chair(s) shall, before commencing a vote, observe any request as to the manner in which the voting shall be conducted, and then shall formally announce the voting procedure to be applied and the issue to be submitted to the vote. The Chair(s) shall then declare the beginning of the vote and, when the vote has been taken, shall announce the results.
3) In the case of a secret ballot, the working group leadership shall at once take steps to ensure the secrecy of the vote.

Deliverables/Activities

The tentative deliverables include:

- Alignment of OCF Level 2 (STAR Certification) with ISO/IEC 27017 and 27018.
- Amendment of the STAR Certification scheme to better align with ISO/IEC 27006 current version.
- Amendment of the STAR Attestation certification scheme (STAR Attestation Type 1 based on SOC 2 Type 1).
- Definition and implementation of the OCF Level 3 – STAR Continuous.
- Whitepaper outlining the benefits of CSA STAR Program.
- Definition and implementation of the PLA Code of Conduct Certification scheme based on the recommendation of the PLA WG.
- Definition and implementation of the STAR Mobile Certification scheme based on the input of the MAST WG.

Deliverables will be governed by CSA's intellectual property rights policy.

Duration

This charter will be valid until 31 March 2019

Charter Revision History

November 2015	March 2016	Sept 2017