ゼロトラスト　プライバシー評価とガイダンス

CSAJC cloud security alliance℠ Japan Chapter

CSA cloud security alliance®

The permanent and official location for the CSA PLA and Zero Trust Working Group is respectively:
https://cloudsecurityalliance.org/research/working-groups/privacy-level-agreement
https://cloudsecurityalliance.org/research/working-groups/zero-trust

Acknowledgments

Lead Authors

Diego Diviani Marina
Bregkou Isabella Oldani
Martim Taborda Barata
Jacopo Dirutigliano

Contributors

Steve Foster Kevin
Dillaway

Reviewers

Aparna Achanta
Faizan Ali
Sami Al-Shaheri
Songbo Bu
Aditya Garg
Shamik Kacker
Rahul Kalva
Sujay Kulkarni
Gurunadha Mangalampenta
Ana-Maria Matejic
Usman Mustafa
Mudussar Nazir
Joseph Ohaeche
Emmanuel Ogunwobi
Govindaraj Palanisamy
Mithilesh Ramaswamy
Ramesha Reddy
Nirupam Samanta
Alex Sharpe
Amit Singh
Ashish Vashishtha

CSA Global Staff

Marina Bregkou
Erik Johnson
Alex Kaluza
Stephen Smith

日本語版提供に際しての告知及び注意事項

本書「ゼロトラスト　プライバシー評価とガイダンス」は、Cloud Security Alliance (CSA)が公開している「Zero Trust Privacy Assessment and Guidance」の日本語訳です。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。

変更履歴

日付	バージョン	変更内容
2025年04月02日	日本語版1.0	初版発行

CSAジャパン成果物の提供に際しての制限事項

日本クラウドセキュリティアライアンス（CSAジャパン）は、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

１．　責任の限定
CSAジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。
(1)　本書の内容の真正性、正確性、無誤謬性
(2)　本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと
(3)　本書の内容に基づいて行われた判断や行為がもたらす結果
(4)　本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

２．　二次譲渡の制限
本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。
ただし、以下の場合は本項の例外とします。
(1)　本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明

記してください。
(2)　本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。
(3)　CSAジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。
(4)　転載、再掲、複製の作成と配布等について、CSAジャパンの書面による許可・承認を得た場合。この許可・承認は、原則として文書単位で得るものとします。

３．　本書の適切な管理
(1)　本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。
(2)　本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守させるものとします。また、当該責任者は、本書の電子ファイルを適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する（組織内の利用者に順守させることを含む）ようにしなければなりません。
(3)　本書をダウンロードした者は、CSAジャパンからの文書（電子メールを含む）による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。
(4)　本書を印刷した者は、CSAジャパンからの文書（電子メールを含む）による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

４．　原典がある場合の制限事項等
本書がCloud Security Alliance, Inc.の著作物等の翻訳である場合には、原典に明記された制限事項、免責事項は、英語その他の言語で表記されている場合も含め、すべてここに記載の制限事項に優先して適用されます。

５．　その他
その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSAジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、info@cloudsecurityalliance.jp までお願いします。

日本語版作成に際しての謝辞

「ゼロトラスト　プライバシー評価とガイダンス」は、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を記します。（氏名あいうえお順・敬称略）

石井　英男
井上　尚人
笠松　隆幸
土肥　千明
諸角　昌宏
山﨑　英人
山下　亮一

目次

要旨

データがサーバー、ノートパソコン、クラウド環境などの資産にデジタル形式で保存されている場合、鍵のかかったオフィスビルの物理的なキャビネットに保存されている紙の記録とは対照的に、悪意のある行為者がデータにアクセスする手段は広がります。

個人を特定できるデータへの不正アクセスは、個人のプロファイリングにつながる可能性があり、また、影響を受けた人々の移動や自由に影響を与える可能性があります。このような侵害は、権限のない外部エンティティによって実行されるだけでなく、内部エンティティによっても実行され、アクセス制御の誤りまたは悪意のある行為によって、個人を特定できるデータにアクセスできる可能性があります。アクセス権の取得方法にかかわらず、このような侵害の影響はプライバシーの侵害につながります。個人データの保護を確実にするために、さまざまなプライバシー保護法が存在します。プライバシー法はその保護について詳しく説明していますが、保護そのものは、サーバー、ノートパソコン、クラウド環境などのデジタル機器上で実施します。

ゼロトラスト（ZT）が保護メカニズムを強化できるのは、個人データへのアクセス要求の真正性を検査し、その要求が認可されたエンティティからのものであると判断された場合にアクセスを許可するようにすることです。

本書では、「データ保護」の代わりに「データプライバシー」と「データセキュリティ」という用語を採用し、（欧州における）データ保護の概念を「プライバシー」と呼ぶことにします。

対象読者

本書の対象読者は以下の通りです：

- 主なターゲットオーディエンス；データプライバシーおよび保護アーキテクト、リスクマネージャー、法律顧問、データガバナンスオフィサー
- 第二のターゲットオーディエンス；データセキュリティアーキテクト、ゼロトラストプログラムおよびプロジェクトチーム、CISO、CIO

スコープ

本書の目的は、プライバシーの実装においてゼロトラストを使用するためのガイダンスを提供することです。本書では、プライバシーの基本原則、プライバシーの原則とゼロトラストの実施との整合性、プライバシーの影響評価について説明しています。GDPRは、プライバシー規制と要件の例証として使用されています。これは、世界のさまざまな地域で現在使用されている可能性のあるすべてのプライバシー規制を含むものと解釈すべきではありません。本書では、ゼロトラストの実装／アーキテクチャの詳細については触れません。また、プライバシー規制だけに焦点を当てているわけでもありません。

はじめに

人々がゼロトラスト（ZT）の原則について議論するとき、多くの場合、ZTが組織全体のデータ保護能力を高めるのにどのように役立つかに焦点が当てられていますが、ZTが規制を遵守して組織内のデータプライバシーの実現能力を高めるのにどのように役立つかは忘れられがちです。

急速に変化する今日のコンプライアンスの世界におけるプライバシーは、ZTに活用されているのと同じコントロールと思考プロセスのすべてを活用すべきです。このようにすることで、データプライバシーは次のようなアーキテクチャの原則を活用することができます：

- データにアクセスするアイデンティティ、特にプライバシーが懸念される機密データにアクセスするアイデンティティの管理を改善する。
- アプリケーションレベルでのアクセス管理により、よりきめ細かな管理を可能とする。
- 変化するビジネスシナリオやユースケースに迅速に適応する能力を持つ。

本書では、プライバシー評価と5段階のZT実施プロセスを使用することにより、プライバシーと規制の観点から、ZTの方法論とコントロールを活用する際のいくつかの課題を克服する必要性を取り上げています。

さらに、ZTとプライバシーがどのように共存し、互いの成功を支援する方法として、強固な基盤となるようなトピックも取り上げています。

1. ゼロトラストとは何か？

1.1 なぜゼロトラストが重要なのか？

国家安全保障電気通信諮問委員会（NSTAC）による「セロトラストと信頼されるID管理に関する大統領への報告書」では、ゼロトラスト（ZT）を*「いかなるユーザーや資産も暗黙的に信頼してはならないという考えを前提としたサイバー セキュリティ戦略です。侵害がすでに発生しているか、発生すると想定し、組織の境界で1回検証するだけでエンティティに機密情報へのアクセスを許可すべきではありません。代わりに、各ユーザー、デバイス、アプリケーション、トランザクションを継続的に検証する必要があります。」と定義しています。*

分散型/分散クラウドコンピューティングとリモート ワーカーの時代では、「城」の内に組織の資産やユーザーがほとんど存在しないため、従来の集中型の「城と堀」セキュリティモデルは、現代の分散型環境では効果がありません。

インターネット接続を多用する、高度に分散した現代の企業ネットワークにおいて、技術的または人的な脆弱性を悪用することに、洗練された脅威行為者はますます習熟しています。成功するサイバー攻撃は、一般的に何らかの方法で信頼を悪用します。信頼は、それが誤った相手に向けられている場合、脆弱性となり、積極的に管理し、最小限に抑える必要があります。ゼロトラストでは、すべてのネットワーク接続とパケッ

トは信頼されていないとみなされ、同じように厳格な検証プロセスが適用されます。信頼レベルはゼロと定義され、これがゼロトラストという用語の由来となっています。

ゼロトラストは、クラウド／マルチクラウド（すべてのサービスモデル）、オンプレミス／ハイブリッド・システム、社内外のパートナー／利害関係者、ユーザー・エンドポイント（組織が管理するエンドポイント、BYOD）を包含し、運用技術（OT）、産業用制御システム（ICS）、IoTを含む、総合的な企業セキュリティ戦略です。その結果、ゼロトラストは、一歩ずつ登っていかなければならない山に例えられてきました。これらの原則は、CSAのZTガイダンスに共通するテーマです。

ゼロトラストの企業導入は幅広く、拡大しています[1]。Venture Beatのレポートによると、クラウドに移行する企業の90%がゼロトラスト戦略を採用しており[2]、Gartnerは、2026年までに大企業の10%が成熟した測定可能なゼロトラストプログラムを導入すると予測しています[3]。

1.2 ゼロトラスト実装

ゼロトラストの伝道者である John Kindervag が定義したプロセスは、5段階の実装プロセスです。このプロセスを使うことをお勧めします。これらのステップは、コントロールの実装を扱うセクションでさらに参照されます。

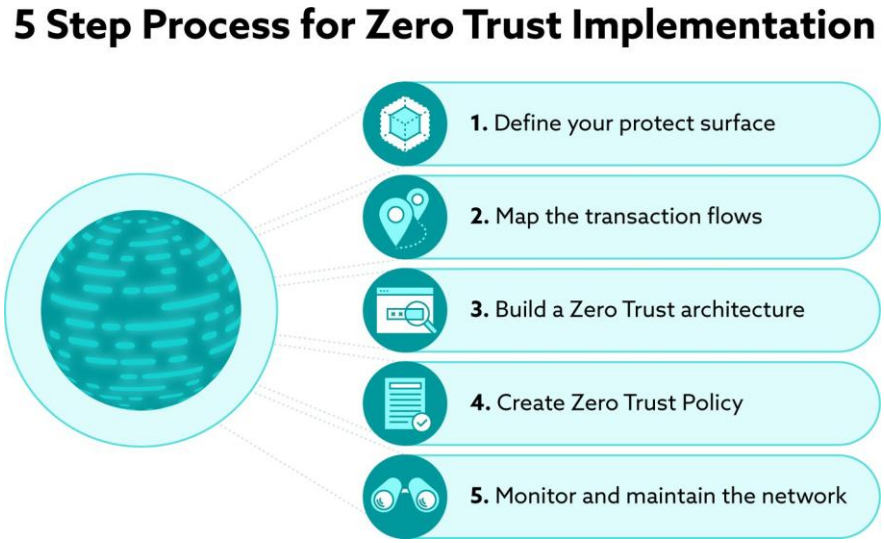

図1: ゼロトラスト実装の5つのステップ

[1] 例えば、金融機関は機密性の高い金融データを保護するためにゼロトラストを使用し、厳格なアクセス制御とネットワークセグメンテーションを適用して内部脅威を軽減しています。同様に、医療プロバイダーは、HIPAAのコンプライアンスを確保しながら、不正アクセスから電子カルテ（EHR）を保護するために使用しています。

[2] https://venturebeat.com/security/why-90-of-enterprises-migrating-to-the-cloud-are-adopting-zero-trust/

[3] https://www.gartner.com/en/newsroom/press-releases/2023-01-23-gartner-predicts-10-percent-of-large-enterprises-will-have-a-mature-and-measurable-zero-trust-program-in-place-by-2026

2. プライバシーを理解する

2.1 プライバシーとは何か？

世界人権宣言（1948年）第12条と欧州人権条約（1950年）第8条で初めて認められた「プライバシー権利」は、一般的に私生活を尊重する権利と理解されてきました。

他方、ヨーロッパでは「データ保護」と言う概念（「プライバシー」と言う概念と関連しているものの、それとは異なる）は、個人情報の処理の保護と規制を目的としたさまざまな法律の制定とともに発展し始めました[4]。 例えば、データ保護分野における唯一の法的拘束力のある国際文書である「個人データの自動処理に関する個人の保護に関する欧州評議会条約（108号条約）」や、「個人データの処理に関する個人の保護および当該データの自由な移動に関する指令95/46/EC」（現在は「個人データの処理に関する自然人の保護および当該データの自由な移動に関する規則（EU）2016/679」（一般データ保護規則（GDPR））によって廃止されている）の場合です。

この2つの概念に対処する為、欧州連合基本権憲章（2000年）（以下「憲章」）は、私生活と家族生活の尊重の権利だけでなく、個人データの保護の権利も定められています。特に、憲章第7条が「すべての人は、自己の私生活、家庭生活、住居および通信を尊重される権利を有する」と規定しているのに対し、第8条は「すべての人は、自己に関する個人データを保護される権利を有すると規定しています。このようなデータは、特定の目的のために、関係者の同意または法律で定められたその他の正当な根拠に基づいて、公正に処理されなければなりません。すべての人は、自己に関して収集されたデータにアクセスする権利と、それを修正させる権利を有する」と規定しています。

ヨーロッパにおいて、「プライバシー」とは異なる「データ保護」（よって、データ保護への権利）の概念が発展したのは、主に技術革新の急速なペースと、そのような変化（およびグローバル化）が個人情報の保護にもたらす課題によって促進されたものです[5]。実際、デジタル技術の浸透とグローバリゼーションは、現代の情報社会の中心であるデータを混乱させる社会的変化を引き起こしています[6]。そのため、個人データの保護は極めて重要になっています[6]。

このような背景から、EU内外でさまざまな法律が制定されてきました。前述の通り、2018年5月までのEUにおける主要な法制度は指令95/46/ECであり、この指令は異なるEU加盟国がすでに採用していたデータ保護法を調和させる手段として採択されたため、EUにおける包括的なデータ保護制度システムを確立する手段として採用されました。この指令はその後、GDPRの採択によって近代化され、データ保護の権利が今日の世界で果たすべき役割を欧州の視点から定めています。この文脈において、（GDPRで定義される）個人データにまつわる権利の強化は、基本的人権と自由を保護する枠組みを定めると同時に、（少なくとも欧州経済領域内では）それらのデータの自由な移動と関連する経済発展の促進を目指しています。

---

[4] 欧州連合基本権機関 欧州データ保護法ハンドブック 2018 年, https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf, P.18

[5] これは例えば、GDPR 前文 6 および 7 によって示唆されています。

[6] Durante, M. (2021). Computational Power: The Impact of ICT on Law, Society and Knowledge (1st ed.). Routledge. https://doi.org/10.4324/9781003098683

EU域外でも、個人情報（それぞれの法律で定義されている）の収集、アクセス、処理の方法を規制する目的で、いくつかの法律が採択されています（または現在策定中です）。これには、カリフォルニア州消費者プライバシー法（「CCPA」）、カナダの個人情報保護および電子文書法（「PIPEDA」）、オーストラリアのプライバシー法、南アフリカで制定された個人情報保護法（「POPOIA」）、ブラジルの一般データ保護法（GDPRをほぼモデルとしている）など、数多くの法律が含まれます[7]。
絶え間なく進化するプライバシーの状況を考慮し、本書では特定のデータ保護法に焦点を当てるのではなく、ゼロトラストに関する考察を行うために、世界の法律に共通するプライバシーの一般原則を検討することを目的としています。

このように常に進化し続ける状況において、「プライバシー」の概念は一般的に私生活を尊重する権利として理解される一方で、国際的に認められた（データ保護）基準がない場合、異なる（法的拘束力のある）データ保護要件が、適用される様々な国内またはEU域内のような超国家的な規範的枠組みから生じる可能性があることを思い出す価値があります。

これは、世界中で採用されている用語にも影響し、国によって異なる場合があります。従って、用語の一貫性を保つため、**本書では「データ保護」の代わりに「データプライバシー」と「データセキュリティ」という用語を採用し、欧州のデータ保護の概念を「プライバシー」と呼ぶことにします。**

また、本書を通じて表現される概念を明確に理解できるようにするため、「個人データ」、「データサブジェクト」、「個人データ侵害」、およびその他の関連用語への言及は、GDPRの下で提供される定義に基づいて解釈する必要があります（本書で使用されるすべての関連定義については、用語集を参照）。この選択は、GDPRがデータ保護の世界的な最高基準の1つであり、その主要用語に広範な定義を提供し、技術的に中立な方法で作成されているため、GDPRが意図している保護レベルが損なわれないことを保証するためです[8]。その結果、GDPRは世界中の他の多くのデータ保護法制の開発の基礎として機能し（GDPRの原則および中核規定といくつかの類似点を共有しています）、データ保護の定義に関する主な参照としてGDPRを使用することをさらにサポートしています。

2.2 プライバシーを追求することが重要な理由

私生活尊重の権利と個人情報の保護の権利は、個人が自由に個性を発展させ、考え、意見を形成できる個人的な領域を与えることによって、個人の自律性と人間としての尊厳を保護することを目的としています[9]。この意味で、これらの権利は「表現の自由、平和的集会と結社の自由、宗教の自由など、他の基本的自由の行使に不可欠な前提条件」[10]です。

さらに、特定のプライバシー原則（以下のセクション3.3.でさらに詳しく説明するセキュリティ原則など）に違反することは、人々の安全と健康を危険にさらす可能性があります。例えば、個人データの違法な開示（「個人データ侵害」に相当）は、関係するデータサブジェクトにとって、克服できないかもしれない重大な結果（例えば、多額の負債や就労不能などの経済的困窮、長期にわたる精神的・身体的

[7] 国際的な基準がないため、多くの国がデータ保護法に関する独自の基準を定めようとしています。したがって、世界中の企業は、事業を展開するそれぞれの地域で適用される基準を満たしていることを確認する必要があります。例えば、現在アメリカには12以上の州でプライバシーに関する法律が制定されており、他の州ではプライバシーに関する法律が提案され、承認待ちの状態です。
[8] GDPR 前文 15を参照
[9] 欧州連合基本権機関 欧州データ保護法ハンドブック 2018 年, https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf, P.19
[10] 欧州連合基本権機関 欧州データ保護法ハンドブック 2018 年, https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf, P.19

疾患、死亡など）をもたらす可能性があり、深刻な困難（資金の不正流用、銀行によるブラックリスト登録、財産的損害、失職、召喚、健康状態の悪化など）を伴わなければ克服できないかもしれません。このことは、プライバシー要件の遵守が、「個人データ」を、そのデータが関係する個人の保護を目的としていることを示しています。

参照する特定の法的枠組みによっては、適用されるプライバシー要件に違反すると、行政制裁（管轄の監督当局によって組織に課される可能性があります）やデータサブジェクトからの賠償請求（データサブジェクトが被ったと主張する損害に対するもの）につながることもあります。例えば、GDPRの規定の一部に違反した場合、最高20,000,000EUR（2,000万ユーロ）以下の行政制裁金、または事業者の全世界年間総売上高の4%以下のいずれか高い方が科される可能性があります。

さらに、例えば、技術的・組織的なセキュリティ対策が十分でなかったために重大なセキュリティインシデントが発生したことが判明した場合や、適用されるプライバシー要件不遵守に起因する複数かつ反復的な行政処分を受けた場合には、組織は風評被害を被るリスクに直面する可能性があります。このようなインシデントや制裁金は、顧客の信頼にも影響を及ぼし、既存顧客と潜在顧客の双方が、より安全でコンプライアンスが遵守されていると認識される競合他社に流れてしまう可能性があります。[15]

23 中核となるプライバシー原則および要件

様々なプライバシー法制の枠組み（GDPR、CCPA/CPRA、PIPEDAなど）に見られる主要な共通原則／規則には、例えば、以下のような原則があります：

- 個人情報の収集および利用を特定の合法的な目的に限定する制限の目的；
- 組織は、特定された目的のために厳密に必要な個人データのカテゴリーのみを収集するものとするデータの最小化；
- 個人データは、特定された目的を達成するために必要な期間のみ保持されるべきであるというデータの保持；
- 組織が保有する個人データを不正使用、盗難、紛失、その他の不正な干渉のリスクから確実に保護されるための措置を講じることを求めるセキュリティ；

個人はまた、自分の個人データにアクセスする権利、自分の個人データがどのような目的で使用され誰に開示されたかを知る権利、自分のデータを削除してもらう権利、自分のデータを訂正／更新してもらう権利など、さまざまな権利をいくつかの司法管轄で与えられています。GDPRは、自己に関する法的効果を生じさせるか、または同様に重大な影響を及ぼす自動化された処理（プロファイリングを含む）のみに基づく決定を回避する権利を個人に付与しており[11]、CCPAは、個人（またはCCPAで定義されるより優れた「消費者」）は、自己について収集された機密情報の使用と開示を制限し[12]、個人データの販売または共有からオプトアウトする権利を有する[13]と規定されています。

[11] GPRR 第22条を参照

[12] CCPA第1798.121条。「機微情報（Sensitive infromation）」は、1798.140条（ae）に定義されており、特に、社会保障番号、金融口座情報、正確な位置情報、遺伝情報が含まれます。特に、社会保障番号、金融口座情報、正確な位置情報、遺伝情報）が含まれます。

[13] CCPA第1798.120条。「販売（Sell））」とその派生語は、1798.140条（ad）で以下のように定義されています：「販売（Sell,

本書では、セキュリティの概念を掘り下げ、「データセキュリティ」と「プライバシー」の違いを分析します。データ保護法制に関連する「セキュリティ」への言及は、一般的に、処理中の個人データを保護することを目的とした技術的・組織的対策の実施に関連します[14]。さまざまなデータ保護法に反映されているこれらの対策の例としては、仮名化、処理システムのレジリエンスを向上させる対策、バックアップ手順、災害復旧プロトコルなどがあります。世界の大企業の89%以上がDXとAIによる変革を進めていると報告されており[13]、個人データを含む紙文書のアーカイブとは対照的に、個人データのデジタル保存が増加していることを考慮すると、情報セキュリティ／サイバーセキュリティは、個人データの保護と本質的に結びついています。しかしながら、個人データが関与していない場合、「プライバシー」は何の役割も果たしません。一方、「データセキュリティ」は機密性の高いビジネス情報を含む他の種類の情報が、データサブジェクトの個人の権利と自由とは無関係に保護を必要とする限りにおいて、依然として関連しています。

今日の社会では、デジタル・セーフティーとは、保護対象がデータだけでなく、そのデータに関連する人々であることを認識することです。これによりセキュリティがプライバシーとデータ保護が本質的に結びついている理由と、セキュリティ対策を強化することが後者の2つの権利の保護にいかに役立つかの理由を説明するものです。

3. プライバシーの目標達成にゼロトラストはどう役立つのか？

プライバシー保護にはデータ中心の保護が求められる為、ゼロトラスト・コントロールは、組織にとって重要なデータや、情報の性質上機密性の高いデータの保護を強化することを目的としています。データの分類は、プライバシーの実践に共通するタスクであり、保護対策の強化が正当化される可能性のある情報を特定します。データ分類が早期に適用できればできるほど、ゼロトラスト・アプリケーションはより成熟したものになります。

作成時またはインポート時にデータにタグを付けることで、組織はデータを分類して、データ入力からプライバシーを保護できます。分類されたデータ属性に基づく論理アクセス制御は、属性ベースアクセス制御[1]（ABAC）と呼ばれ、ゼロトラスト環境内で機密データに対するプライバシー固有の制御をさらに可能にします。

ABACのコンセプトは、コンテキストベースアクセス制御(Context-Based Access Control ; CBAC）を含むことでさらに拡張され、ネットワークからの様々な信号、時間帯、アプリケーションの状態、ユーザーの詳細情報などを使用して計算されたコンテキストに基づいてアクセスを許可します。CBACは、ゼロトラストの原則と組み合わせることで、フィードバックループとアクセスの改良によって、さらに強化および改善することができます。

selling）」、「販売」、「売却」、または「売却された（sold）」とは、販売することを意味します。「販売」、「売却」、または「売却された」とは、金銭的またはその他の価値ある対価のために、事業者が消費者の個人情報を第三者に、販売、貸与、解放、開示、流布、提供、譲渡、またはその他の方法で口頭、書面、電子的またはその他の手段で伝達することを意味します。

[14] 例えばGPPR第32条を参照

ABAC/CBACを使用することは、組織のプライバシーニーズに特化したデータ著作権管理（DRM）とデータ損失防止（DLP）ソリューションをさらに促進するプライバシーデータの属性ポリシーを適用できます。

ゼロトラストの原則は、自動化とAI駆動型分析をABACとCBACに統合することで、さらに最適化できます。例えば、機械学習モデルは、ユーザーの行動を分析し、異常に基づいてアクセス許可を動的に適応させ、プライバシー保護をさらに強化することができます。このアプローチにより、プライバシーポリシーのリアルタイムの準拠を確保しながら、人間の介入を最小限に抑えることができます。

ゼロトラストは、アクセス要求を許可する前に認証を行うことを推奨しています。これは、権限のないエンティティが資産にアクセスするのを防ぐためです。

プライバシーの重要な要件のひとつは、権限のないエンティティが個人データにアクセスできないようにするアクセス制御です。

ゼロトラストは、トランザクションの流れをマッピングし、組織が情報経路（内部／外部）を可視化して管理できるようにすることを重視しています。この原則は、プライバシー要件があるデータの場所、プライバシーデータを取得する情報フローとプロセス、および地理的かどうかにかかわらず、その他の外部の場所への情報フローを組織が理解するのに役立ちます。

これらのステップは、以下の方法でプライバシー要件をサポートします：

- 組織内のプライバシーを特定するためのプロテクトサーフェスを定義する。
- トランザクションをマッピングし、プライバシーデータの入出力を特定する。
- ゼロトラストアーキテクチャー（ZTA）により、セキュリティ制御をプロテクトサーフェスと入出力フローに近づける。
- 許可されたアイデンティティからのアクセス要求が受け入れられ、 許可されていないアイデンティティからの要求が拒否されるようにポリシーを追加する 。
- 技術資産を監視し、必要なセキュリティポスチャを維持する。

4. ゼロトラスト実装におけるプライバシー原則と要件の整合

プライバシー原則は、個人データの合法的、倫理的かつ責任ある処理を保証するための重要な基盤として機能します。GDPRやその他の関連する世界のデータ保護法に反映されている原則のうち、セキュリティ原則は、情報セキュリティを個人データの保護に本質的に結びつけるものです（上記セクション参照）。この原則に準拠するために、組織は適切な技術的および組織的セキュリティ対策を実施し、その処理に内在するリスクに見合ったレベルの個人データのセキュリティを確保しなければなりません[15]。

この要件をどのように満たすかの方法を理解するには、GDPR（およびGDPRをモデルとする他のデータ保護法）が、セキュリティ対策の実施を含め、コントローラに義務を課す際に「リスクベースのアプ

[15] GDPR第32条

ローチ」を採用していることを念頭に置くことが重要です。このアプローチは、コントローラが実施する特定の個人データ処理活動から生じる可能性のある「自然人の権利と自由に対する様々な可能性と重大性のリスク」を含む幾つかの要因を考慮して、GDPRに準拠する技術的および組織的対策を決定することが求められます。このアプローチは、GDPRにおいて、説明責任の原則（コントローラがその状況に適したコンプライアンス対策を自律的に決定し、実施した対策を実証し、その決定に責任を負うことを求める）の導入だけでなく、そのさまざまな条項を通じて「リスク」という言葉が頻繁に使用されていること（75回）からも明らかです。

当然のことながら、急速な技術発展とグローバル化（例えば、クラウドベースのデータ処理技術の台頭、個人がオンラインで自身の個人データを共有する可能性の増大、個人に関するプロファイリングや意思決定を行うために膨大な個人データを分析する人工知能の利用など）も、個人データ保護に新たな課題を提起しています。したがって、デジタル経済が安定的に発展していくために必要な信頼の風土を作り出すためには、合法的で倫理的かつ責任ある個人データ処理を保証するための、強固で安全なアプローチが必要です。こうした背景から、ZTは重要な役割を果たすことができます。

4.1 ゼロトラストのコンテキストにおけるプライバシーリスク

ZTの実装には、ZTのメカニズムやシステムを使って個人データが処理されることになる個人の基本的権利（特に、プライバシー権とデータ保護権）に対する、その潜在的な利益と潜在的なリスクや影響との間で、バランスを取る作業が伴わなければなりません。

このバランス調整は、GDPRのリスクベースアプローチを実際に実装するための方法であり、セキュリティ対策の最大化（すなわち、可能な限り最も効果的かつ徹底的な方法でセキュリティを追求すること）と、個人のプライバシーや権利への潜在的な悪影響（例えば、特定のネットワーク上での個人の活動を過度に細かく監視することで、セキュリティとは無関係ですが、それにもかかわらず個人の観点からは機微な個人の側面が明らかになる可能性があること）とを比較検討することを中心に行うことになります。要するに、ZTを通じて達成されるセキュリティ強化は、関連するデータサブジェクトへの悪影響を最小限に抑えつつ、対処しようとする特定されたセキュリティリスクに比例したものでなければなりません。

このシナリオでは、プライバシーリスクアセスメントと、必要に応じて、より徹底的なデータ保護影響アセスメント（DPIA）を実施することが、データ保護要件に準拠してZTを実装しようとする組織が取るべき最初のステップです。

これにより、組織は、意図しているZTの実装が、個人に関連するリスクを発生させる可能性があるかどうかを理解し、必要な場合には、それらのリスクに対処するために実装できる緩和策を特定することができます。

DPIAは、分析された処理活動（データ処理中のプロファイリング、自動化された処理など）が、自然人の権利と自由に対して高いリスクをもたらす可能性がある場合に、一定の条件の下で法的に義務付けされている包括的なリスクアセスメントです。

実際には、プライバシーリスクアセスメントを実施することで、個人に対する高いリスクが検出された

場合には、DPIAを実施することによってプライバシーリスクアセスメントを深める必要性が明らかになる場合があります。組織がDPIAを実施することを法的に義務付けられているかどうかにかかわらず、プライバシーリスクアセスメントを実施することは、組織が実施するすべての処理活動に関する重要な作業であることに変わりはありません。これなしでは、組織の活動が伴う可能性のある個人に対するリスクの全体的なレベルを適切に理解し、それに応じて対応することができない可能性があります。ZTの実装は、特定または識別可能な個人（ネットワークユーザーなど）に関する情報の処理を伴う限りにおいて、この例外ではありません。

4.2 プライバシーリスクアセスメント（ISO PIAおよびGDPRに基づくDPIA）

プライバシーアセスメントは、プライバシーリスクアセスメント（PRA）、データ保護影響アセスメント（DPIA）、プライバシー影響アセスメント（PIA）などの方法論を採用し、個人データ管理のガバナンスの要となるものです。これらの用語は、プライバシー関連のリスクを特定し、効果的に軽減するために設計されたプロセスを説明するためによく使用されています。

プライバシーアセスメントの目的は、個人データがどのように処理されているかを分析し、関連するプライバシー要件への準拠を確認し、プライバシー関連のリスクを軽減することです。

PRA、DPIA、PIAは類似していますが、これらのアセスメントは異なる目標に焦点を当てています。

4.2.1 プライバシーリスクアセスメント（PRA）

プライバシーリスクアセスメント（PRA）は、個人データ処理活動から生じる個人の権利と自由に対するリスク、特に物質的または非物質的な損害を引き起こす可能性のあるリスクを評価します。その目的は、(i)処理による悪影響の可能性、(ii)個人への潜在的影響を評価することによって、これらのリスクを特定することです。重要なのは、組織ではなく影響を受ける個人に焦点が当てられていることです。たとえば、機密性侵害によるリスクを評価する場合、評価では組織自体ではなく、データサブジェクトへの損害を考慮します。PRAの目的は、特定されたリスクを許容レベルまで軽減するための技術的または組織的な対策を提案することです。リスクが「高い」（可能性が非常に高い、重大な影響がある、またはその両方）と判断された場合、データ保護影響アセスメント（DPIA）などのより詳細な分析が開始される可能性があります。

DPIAが法的に義務付けられている場合、または自主的に実施される場合、PRAはより深い分析の基盤となります。

4.2.2 データ保護影響アセスメント（DPIA）

GDPRの下では、データ保護影響アセスメント（DPIA）は、組織が個人データの処理に関連するデータ保護リスクを特定し、軽減することを可能にするプロセスです。DPIAは、GDPRの要件へのコンプライアンスを確保し、データサブジェクトのプライバシーと権利を保護するための重要なツールです。これは、データ処理活動を分析し、その必要性と比例性を評価し、差別、なりすまし、データ侵害など、個人の権利と自

由に対するリスクを特定するための体系的なアプローチを提供するものです。

GDPR DPIAの主要な側面には以下が含まれます：

- **処理活動の特定**：
  - 処理活動の性質、範囲、文脈、および目的を決定する。
- **必要性と比例性の評価**：
  - 意図された目的に照らして、処理活動の必要性を評価する。
  - データサブジェクトの権利に関連して、処理の比例性を評価する。
- **リスクの特定と評価**：
  - 処理活動から生じる個人の権利と自由に対するリスク（差別、なりすまし、データ侵害、不正アクセスなど）を特定し、評価する（規則2018/1725 第39条第1項）。
  - 潜在的なリスクの可能性と重大性を考慮する。
- **リスクの軽減と協議**：
  - GDPRデータ保護影響アセスメント（DPIA）の原則および要件に沿って、特定されたリスクを軽減するための具体的な技術的および組織的対策を定義する。
  - データ保護責任者（DPO）の助言を求め、場合によってはデータサブジェクトまたはその代理人と協議する。
- **監督当局との協議**：
  - DPIAにより、その処理が、組織が軽減できない高いリスクをもたらすことが示された場合、処理を進める前に、関連する監督当局に相談すること。
- **文書化と記録管理**：
  - 評価、講じられた措置、協議の結果を含むDPIAプロセスの文書を維持すること。

GDPRの遵守を証明するための記録を保管し、必要に応じてDPIAを定期的に見直し、更新します。

DPIAを実施することで、組織はデータ保護への考慮事項をプロセスに確実に組み込むことができ、プライバシー侵害の可能性を低減し、GDPRへの全体的なコンプライアンスを強化することができます。[3]

ZTの実装に焦点を当てた、PRAとDPIAのパフォーマンスに従う可能性のある方法論の概要は、これらの評価が実際にどのように実行されるかを示すものとして、以下のセクション4.3で提供されています。

4.2.3 プライバシー影響アセスメント（PIA）

ISO/IEC 29134で定義されているプライバシー影響アセスメント（PIA）は、個人情報の処理に関連するプライバシーリスクを評価するために使用される方法論です。PIAの主な目的は、特に機密データが関係する場合、潜在的なプライバシーリスクを軽減するための適切な制御と対策を特定することです。これは通常、新しいサービス、製品、プロジェクトで機密性の高い個人情報を処理する必要がある場合に適用され、プロセスの早い段階でプライバシーリスクが特定され、対処されるようにします。

PIAは、様々な規制の枠組みによって義務付けられています。例えば2002年の米国電子政府法は、政府機関が個人を特定できる情報（PII）を収集する際にPIAを実施することを義務付けています。コロラド州、バージニア州、コネチカット州を含むいくつかの州法も、リスクの高いデータ処理や個人情報の販売などの活動に対してPIAを義務付けています。カリフォルニア州では、カリフォルニア州消費者プライバシー法（CCPA）はまだPIAを明確に要求していませんが、カリフォルニア州プライバシー保護庁（CPPA）は、PIAが必要とされる時期を明確にする規制を発表する予定です。

ゼロトラスト・プロジェクトの文脈では、早い段階でPIAを実施することで、プライバシー要件がシステムの機能要件に組み込まれていることを確認できます。

4.2.4 まとめ

PRA、DPIA、PIAの各方法論を組み合わせることで、プライバシーリスクを管理するための包括的で多次元的な枠組みが実現します。これらの方法論により、組織はプライバシー侵害の可能性を減らしながら、法的および規制要件の複雑な状況を乗り切ることができます。そうすることで、信頼を醸成し、データ管理業務のあらゆる面において最高水準のデータ保護と組織の説明責任を堅持するという確固としたコミットメントを示すことができます。さらに、これらの方法論は将来を見据えたアプローチを具現化するものであり、組織が将来のプライバシー規制の進展や技術の進歩を予測し、それに適応できるようにするものです。厳格な適用と継続的な改善を通じて、PRA、DPIA、PIAは、個人と組織の双方に利益をもたらす強固なプライバシー・ガバナンスの枠組みの構成要素として機能します。

4.3 NIST プライバシーリスクアセスメント方法論の要約

NISTプライバシーリスクアセスメント手法（PRAM）は、PIAモデルを適用したプライバシーリスク管理のフレームワーク／ツールです。

NISTのプライバシーリスクアセスメント手法（PRAM）には、4つのステップで説明されています：

- ステップ1：ビジネス目標の策定と組織のプライバシー・ガバナンス[16]
- ステップ2：システム設計の評価、データマップのサポート
- ステップ3：リスクの優先順位付け
- ステップ4：コントロールの選択

ステップ1：ビジネス目標の策定と組織のプライバシー・ガバナンス

「プライバシー ガバナンス」という用語は、通常、ビジネス目標と要件、およびデータプライバシーの管理を導くプライバシー法と規制を定義します。

- **ビジネス要件：**ビジネス目標の説明は、 リスクを軽減し、ビジネス目標をサポートすることができる**基本的なプライバシー・コントロール**を特定し、選択するのに役立ちます。
- **規制要件：**プライバシーに関する法律、規制、基準、フレームワークを特定することで、法的要件と技術的要件を理解し、プライバシー問題の管理指針とすることができます。

ステップ2：システム設計の評価、データマップのサポート

データマップまたはデータフローマップは、データフロー環境を図示し、個人データが処理されるシステムコンポーネントを示します。このマップは、収集から使用、保存、移転、削除に至るまで、データのライフサイクルの全過程を通じたPIIの工程を詳述しています。

[16] 「プライバシー・ガバナンス」という用語は、通常、ビジネスの目的と要件、およびデータプライバシー管理の指針となるプライバシー法および規制を定義する。データプライバシー管理の指針となる法規制を定義しています。

データマッピングは重要です：

- どのようなデータが処理されているのか、*誰が*アクセスできるのか、データはどこにあるのかを理解する。
- 言いきりにしても良いかも「処理されるデータ、アクセス権を持つユーザー、およびデータの保存場所を理解する」
- PII j 処理のプライバシーリスクを特定する
- GDPR 第30条、第35条、第36条に記載されているGDPRの主要な要件に準拠していることを証明する。

ステップ3：リスクの優先順位付け（リスクアセスメントフレームワーク）

データサブジェクトのプライバシーに対する潜在的な脅威を特定します。これには、個人データの機密性、完全性、または可用性を損なう可能性のある、不正アクセス、データ侵害、または悪意のある攻撃など、内部および外部の脅威の分析が含まれます。

特定された脅威の可能性と影響を評価します。これには、データサブジェクトのプライバシーに対する潜在的な損害を見積もり、影響の重大性や既存の管理の有効性などの要因に基づいて、全体的なリスクレベルを評価することが含まれます。

その目標は、規制要件や組織の目標に沿って、リスクを許容可能なレベルまで確実に低減することです[4] [5]。

ステップ4：コントロールの選択

このステップでは、ステップ2と3から導き出されたPRAMプロセスの前のステップで優先されたプライバシーリスクを管理するための対策を特定し、実施します。組織は、特定された特定のリスクと影響に基づいて適切なプライバシー・コントロールを選択し、プライバシーイベントの可能性を低減し、またはその結果を軽減することを目指すべきです。これには、技術的、管理的、物理的なコントロールを考慮し、より広範な組織の方針およびリスク管理戦略と整合させることが含まれます。選択プロセスでは、選択されたコントロールが、ビジネス機能およびコンプライアンス要件を実現しながら、プライバシーの目的をサポートすることを保証します。

追加的なフレームワークとして、欧州連合サイバーセキュリティ機関（ENISA）が概説する5つのステップも、プライバシーリスク評価を実施するための包括的なアプローチを提供し、組織がプライバシーリスクを体系的に特定、評価、軽減することを保証します。

NISTとENISAのステップをゼロトラストフレームワークに統合することで、組織は規制要件とプライバシー管理のベストプラクティスの両方を順守しながら、強固なプライバシーポスチャを維持することができます。

4.4 定義されたプライバシー要件をZT の実装に統合する方法

4.4.1 プライバシー要件と管理

要件とコントロールの相関関係を理解することは極めて重要です。コントロールは、プライバシーリスクアセスメント（PRAM）手法で定義されたプライバシー目標を達成するために、プライバシー要件を満たすために組織が実装する保護対策の説明とみなすことができます。

4.4.2 プライバシー・コントロールの実装に関する考慮事項

PII処理に関連するリスクを分析するプライバシーリスクアセスメント（PRA）の実施により、プライバシー・コントロールの選択と、管理の実施に必要な調整フェーズを導くことができます。

調整プロセスは、NIST SP 800-53B [14]で提供されるプライバシー・コントロールの選択されたベースラインセットのカスタマイズを可能にし、4.3 章で詳述されているように、特定され優先順位付けされたプライバシーリスクを軽減するためのインフラストラクチャのセーフガード保護のニーズに対応します。

期待されるセーフガードを保証するためには、コントロールが正確に実施され、システムの機能コンポーネントと、調整および統合されていることが重要です。プライバシー・コントロールは、ISO27701規範付属書A/Bに従い、GDPR第25条、第32条に準拠して、デフォルトでのデータ保護とデータ処理の適切なセキュリティレベル（例：仮名化、個人データの暗号化）を確保するために、適切な技術的（プライバシー強化技術（PET））および組織的対策を使用して実装されなければなりません。

4.4.3 5ステップモデルにおけるコントロールの統合と調整

プライバシー要件をZTの実装に組み込むには、次のような方法があります：

- **プロテクトサーフェスの定義：**データを保護するためには、データの所在を把握することが重要です。プロテクトサーフェスを定義する検出フェーズでは、プライバシーに関わるデータを含めます。例えば、名前、住所、生年月日、パスポート番号のような機密データの組み合わせです。このフェーズでは、発見され文書化されたプライバシーデータに関するメタデータを含めます。活動の全容を理解するには、ZTワーキンググループのデータ・ピラーが開発・展開した「Defining the Zero Trust Protect Surface」を参照ください。
- **トランザクションフローのマッピング：**トランザクションフローのマッピング中に、PII をホスト及び／又は送信するコンポーネントを含めます。一般的に、以下の質問に答えることが役立ちます：
    - 誰がデータにアクセスするのか？
    - システムは、外部ソースからデータを取得するか？
    - システムは、データを外部ソースの下請けに送信するか？
    - PIIをホストする独立した資産はあるか？
    - PIIで構成される定期的なバックアップはあるのか？
    - 第三者と共有されるPIIは？
    - スタンドアロンサーバーを含むPIIの永続性、PIIにアクセスできるユーザー、およびアクセスのためにどのような認証方法が導入されているか。
    - さらに、システムからのPIIの外部へ流れる通信。

  これらのマッピング活動は、プライバシー要件の準拠を確実にするために不可欠です。先のセクションで説明したように、トランザクションフローを文書化することに重点が置かれており、データ

プロセッサがシステム内でどのようにPIIを処理するかの方法を理解するための基礎となります。

- **ゼロトラスト・アーキテクチャー（ZTA）の構築：**ZTAは、セキュリティーコントロールをプロテクトサーフェスに近づけることを目的としています。この点に関して、PIIのプロテクトサーフェスと、PIIの永続化と送信を伴うトランザクションフローを使用して、PIIと関連するプロテクトサーフェスへのアクセスを要求するエンティティが、アクセスを許可される前に認証されることを保証するために、ポリシー定義ポイント（PDP）、ポリシー実施ポイント（PEP）、ポリシー管理者（PA）を設計します。
- **ゼロトラストポリシーの作成：ZT**ポリシーは、ZTAの中核を形成します。このステップではアクセスを要求するエンティティへのアクセスの許可／拒否、許可されたポートやプロトコルなどのネットワーク層のアクセスに関するポリシーを設計します。
- **ネットワークの監視と保守：**ネットワークの監視と保守は、重要ですが、その他の資産を監視と保守、PIIの取得、処理、保持、転送、送信するプロテクトサーフェスも同時に重要です。このステップを達成するために、PIIの検出時に特定されたプロテクトサーフェスを、組織内の既存の監視と保守プロセスに追加し、すでに存在する技術やノウハウを活用して、無駄な作業を避けること。ただし、欠落しているプロセスという形でギャップが特定された場合は、ぜひそのプロセスを設計し、実施してください。

5. 結論

本書は、プライバシー要件に対応し、PIIを保護するためにゼロトラスト原則をどのように使用するかについてのガイダンスを提供します。テクノロジーが進歩し世界のデジタル化の進展に伴い、プライバシーデータの保護だけでなく、関係者や機密性の高い重要な仕事に従事する人々のデータを保護することが、ますます重要になっています。ゼロトラスト原則は、そのようなデータが適切なセキュリティレベルで適切に識別、特定、処理、廃棄されることを保証します。

本書のプライバシーセクションは、プライバシー要件のニュアンスや特殊性を確実に把握されるように、プライバシー専門の弁護士によって執筆されています。

本書が、組織のプライバシー要件とゼロトラスト原則との整合に着手する一助となれば幸いです。

6. 参考文献

[1] NIST Special Publication 800-162. (2019). Guide to Attribute-Based Access Control (ABAC) Definition and Considerations.
Guide to Attribute Based Access Control (ABAC) Definition and Considerations

[2] Department of Defense (DoD). (2022). Zero Trust Reference Architecture (Version 2.0) Department of Defense Zero Trust Reference Architecture

[3] European Union (EU). EUROPEAN DATA PROTECTION SUPERVISOR. Data Protection Impact Assessment (DPIA).
Data Protection Impact Assessment (DPIA)

[4] ENISA (European Union Agency for Cybersecurity). (2023). Interoperable EU Risk Management Toolbox. Available at:
Interoperable EU Risk Management Toolbox — ENISA.

[5] ENISA (European Union Agency for Cybersecurity). (2023). Updated Risk Analysis Methodology. Available at: https://www.sk-cert.sk/en/enisa-updated-the-risk-analysis-methodology.

[6] National Institute of Standards and Technology (NIST). (2021). Privacy Risk Assessment Methodology (PRAM). Available at:
NIST PRAM (NIST Computer Security Resource Center) (NIST).

[7] National Institute of Standards and Technology (NIST). (2020). Implementing a Zero Trust Architecture. Special Publication 800-207. Gaithersburg, MD: U.S. Department of Commerce. Available at:
SP 800-207, Zero Trust Architecture | CSRC.

[8] European Union Agency for Cybersecurity (ENISA). (2013). Recommendations for a Methodology of the Assessment of Severity of Personal Data Breaches. Available at:
https://www.enisa.europa.eu/publications/recommendations-for-a-methodology-of-the-assessment-of-severity-of-personal-data-breaches.

[9] International Association of Privacy Professionals (IAPP). Privacy Program Management. Portsmouth, NH: IAPP, 2021.

[10] European Union Agency for Cybersecurity (ENISA). (2018). Privacy Enhancing Technologies (PETs) - Current Tools and Techniques. Available at:
https://www.enisa.europa.eu/publications/privacy-enhancing-technologies-pets.

[11] ENISA. (2017). Guidelines for SMEs on the security of personal data processing.
https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

[12] ENISA. (2023). Interoperable EU Risk Management Framework.

https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework

[13] Lamarre, E., Chheda, S., Riba, M., Genest, V. and Nizam, A. (2023). 'The value of digital transformation', *Harvard Business Review*, 31 July.
The Value of Digital Transformation

[14] National Institute of Standards and Technology (NIST), 2020. *NIST SP 800-53B: Control Baselines for Information Systems and Organizations*. Gaithersburg, MD: NIST. Control Baselines for Information Systems and Organizations.

[15] Adams, M., 2023. Non-GDPR compliant? Understanding the risks of failing to comply with GDPR. *Business Tech Weekly*, 24 August.
Non-GDPR Compliant? Understanding the Risks of failing to comply with GDPR - Businesstechweekly.com
and
Lomas, D., 2019. Could the biggest risk from GDPR be to your reputation? *Business Aspects Magazine*.
Could the Biggest Risk from GDPR be to Your Reputation? - Business Aspects Magazine

用語集と用語

CSA用語集へのリンク：https://cloudsecurityalliance.org/cloud-security-glossary/

CSA Code of Conduct for GDPR Compliance：用語

- **自動化された意思決定**とは、データ対象者に関する法的効果を生じさせるか、または同様に データ対象者に重大な影響を与える、プロファイリングによるものを含む自動化された処理のみに基づく意思決定を行うことを意味します。
- **CJEU**とはEU司法裁判所のこと。
- **クラウド利用者**とは、消費者とは対照的に、企業、組織、法人など、クラウドサービスプロバイダー（CSP）が提供するサービスの企業間取引（B2B）顧客を意味します。
- **CNIL**とは、フランス情報自由委員会（Commission Nationale de l'Informatique et des Libertés）を意味し、フランスの監督官庁です。
- **同意**とは、自由に与えられた、具体的で、十分な情報を与えられた、明確な意思表示であり、データ対象者が声明または明確な肯定的行動によって、自分に関する個人データの処理に同意することを意味します。
- **コントローラ**とは、個人データ処理の目的および手段を決定する自然人または法人、公的機関、代理店またはその他の団体を意味します。このような処理の目的および手段がEUまたは加盟国の法律によって決定される場合、コントローラまたはその指名のための特定の基準は、EUまたは加盟国の法律によって規定される場合があります。
- **CSP**とはクラウドサービスプロバイダーの略で、クラウドベースのサービス（SaaS、IaaS、PaaS）のプロバイダーを意味します。
- **データサブジェクト**とは、識別された、または識別可能な自然人を意味します。また、「特定可能な自然人」とは、直接または間接的に、特に、氏名、識別番号、位置情報、オンライン識別子などの識別子、またはその自然人の身体的、生理的、遺伝的、精神的、経済的、文化的、社会的アイデンティティに固有の1つ以上の要素を参照して特定できる者をいいます。
- **DPA**とは、Art. 28 GDPRの下で、データ処理契約を意味し、コントローラに代わってプロセッサが行う個人データの処理を規制するために、コントローラとプロセッサの間で締結される契約を意味します。
- **DPIA**とは、35 GDPRで定義された、データ保護影響アセスメント（Data Protection Impact Assessment）のことであり、意図された処理活動について説明し、その必要性と比例性を評価し、個人データの処理に起因する自然人の権利と自由に対するリスクを評価し、それらに対処する措置を決定することにより、管理を支援するために設計されたプロセスを意味します。。
- **DPO**とはデータ保護責任者を指し、データ保護法およびその運用に関する専門知識を有する者を意味し、コントローラまたはプロセッサの補助者として、GDPRの社内コンプライアンスを監視し、Arts.GDPRの37から39に定められたその他のすべての任務および義務を独立した立場で

遂行します。

- **EDPB**とは、欧州データ保護委員会のことで、EU全域におけるデータ保護規則の一貫した適用に貢献し、EUのデータ保護当局間の協力を促進する欧州の独立機関です。EDPBは各国のデータ保護当局とEDPSの代表で構成されます。

- **EDPS**とは、EUの独立したデータ保護当局である欧州データ保護監督機関のことで、EUの機関や団体が個人データを処理する際に、個人データの保護とプライバシーの保護を監視・確保すること、およびその他の関連業務を行うことを任務としています。

- **EEA**とは、欧州経済領域（European Economic Area）のことです。

- **ENISA**とは、欧州連合サイバーセキュリティ機関（European Union Agency for Cybersecurity）のことで、加盟国、EUの機関、機関、事務所、機関に対し、サイバーセキュリティの向上を積極的に支援するなど、EU全体でサイバーセキュリティの高い共通レベルを達成することを使命とするEUの機関であり、EUの機関、機関、事務所、機関、その他関連するEUの利害関係者に対し、サイバーセキュリティに関する助言と専門知識の参照先として機能しています。

- **EU**とは欧州連合のことです。

- **Garante**とは、Garante per la Protezione dei Dati Personaliのことで、イタリアの監督官庁です。

- **ICO**とは、英国の監督官庁である情報コミッショナー事務局を指します。

- **ISO**とは、国際標準化機構（International Organization for Standardization）のことで、各国の標準化団体の代表で構成される国際標準化機関として活動する独立した非政府組織です。

- **共同コントローラ**とは、個人データの処理の目的および手段を他のコントローラ（1人または複数）と共同で決定するコントローラを意味します。

- **個人データ**とは、データサブジェクトに関するあらゆる情報を意味します。

- **個人データの侵害**とは、送信、保存、またはその他の方法で処理された個人データの偶発的または違法な破壊、紛失、改ざん、不正な開示、または個人データへのアクセスにつながるセキュリティ違反を指します。

- **処理**（個人データに関連する場合は、ProcessおよびProcessedなどの変形も含む）とは、収集、記録、整理、構造化、保管、適応または変更、検索、相談、使用、送信、普及またはその他の方法による開示、利用可能化、整列または組み合わせ、制限、消去または破壊など、自動化された手段であるか否かを問わず、個人データまたは個人データの集合に対して実行されるあらゆる操作または一連の操作を意味します。

- **プロセッサ**とは、コントローラに代わって個人データを処理する自然人または法人、公的機関、代理店またはその他の機関を意味します。

- **プロファイリング**とは、自然人に関連する特定の側面を評価するため、特にその自然人の仕事上のパフォーマンス、経済状況、健康状態、個人的嗜好、関心、信頼性、行動、場所、または移動に関する側面を分析または予測するために個人データを使用することからなる、あらゆる

形態の個人データの自動処理を意味します。

- **仮名化**とは、追加情報を使用することなく個人データを特定のデータ対象者に帰属させることができなくなるように個人データを処理することを意味します。ただし、そのような追加情報は別個に保管され、個人データが特定または識別可能な自然人に帰属しないことを保証するための技術的および組織的措置が講じられることを条件とします。

- **受領者**とは、第三者であるか否かを問わず、個人データが開示される自然人または法人、公的機関、代理店、その他の団体を意味します。ただし、EU法または加盟国の法律に基づき、特定の問い合わせの枠内で個人データを受領する可能性のある公的機関は、「受領者」とはみなされません。これらの公的機関による個人データの処理は、処理の目的に応じて適用されるデータ保護規則を遵守するものとします。

- **処理の制限**とは、将来の処理を制限する目的で、保存されている個人データにマークを付けることを意味します。

- **特別カテゴリーの個人データ**とは、人種的または民族的出身、政治的意見、宗教的または哲学的信条、または労働組合への加盟を明らかにする個人データ、遺伝データ、バイオメトリクスデータ（自然人を一意に識別する目的で処理される場合）、健康に関するデータ、または自然人の性生活または性的指向に関するデータを意味します。

- **サブプロセッサ**とは、コントローラに代わって個人データの処理を支援するために、プロセッサに従事する自然人または法人、公的機関、代理店、その他の団体を意味します。

- **監督機関**とは、GDPR第51条に基づきEU加盟国が設置する独立した公的機関を意味します。

- **第三国**とは、EUまたは欧州経済地域以外の国を意味します。

- **WP29**とは、第29条データ保護作業部会のことであり、2018年5月25日（GDPRの適用開始）までプライバシーと個人データの保護に関する問題を扱っていた欧州の独立作業部会です。