データ処理契約

最終更新日: 2023 年 12 月 15 日

本データ処理契約 (以下「本 DPA」) は、本規約に準拠し、本規約の一部を構成するものであり、Stripe およびその関連会社による個人データの処理について規定しています。

1. 構成

お客様の Stripe アカウントが北米または南米に所在する場合、お客様は本 DPA を Stripe, Inc. (以下「SINC」) との間で締結します。お客様の Stripe アカウントがそれ以外の地域に所在する場合、お客様は本 DPA を Stripe Payments Europe, Limited (以下「SPEL」) との間で締結します。したがって、本 DPA において「Stripe」とは、文脈に応じて SINC または SPEL のことをいいます。

2. データ処理者およびデータ管理者としての Stripe

データ処理上の役割

データ処理者としての Stripe	Stripe はデータ処理者として個人データを処理する場合、データ管理者であるお客様に代わってデータ処理者として行動します。
データ管理者としての Stripe	Stripe はデータ管理者として個人データを処理する場合、 - お客様から、またはお客様を通じて受領した個人データの処理の目的と手段を決定できる単独の排他的権限を有します。また、 - (a) 認定サービスを提供する共同管理者、および (b) 認定サービス以外のサービスを提供するデータ処理者としての役割を、Stripe 関連会社に委託する場合があります。

データ処理の目的

データ処理者としての Stripe	Stripe がデータ処理者としての立場で個人データを処理する目的は次のとおりです。 - Stripe プラットフォームによるサービスを提供する - Stripe のプロダクトおよびサービスを提供し、これらを利用できるようにする

データ管理者としての Stripe	Stripe のプロダクトおよびサービスの提供にあたって、Stripe が データ管理者としての立場で個人データを処理する目的は次のとおりです。 - サードパーティー (銀行および決済手段プロバイダー) を決定し、これらを利用する - Stripe プラットフォームにおける不正取引などの不正行為を監視、防止、検知する - 金銭的損失、セキュリティリスク、その他の損失を監視、防止、軽減する - Stripe のプロダクトおよびサービスの提供を可能にする内部プロセス (取引関係管理、課金、請求書発行など) を実施、維持、遂行する - 法令を遵守する (適用されるマネーロンダリング防止スクリーニング、本人確認義務、金融パートナーおよび政府当局の要件や要求事項の遵守を含む) - Stripe のプロダクトおよびサービスを分析し、開発する

データ主体と個人データの分類: データ処理者**およびデータ管理者としての Stripe**

データ主体	Stripe は、Stripe アカウントにアクセスまたは使用するユーザー、代理人、および自然人の個人データを処理することがあります。
個人データ	該当する場合、Stripe は、決済アカウントの詳細、銀行口座情報、請求/発送先住所、氏名、注文内容 (日時、金額、プロダクトまたはサービスの説明を含む)、デバイス ID、メールアドレス、IP アドレス/所在地、注文 ID、決済カードの詳細、納税者 ID/ステータス、固有の顧客識別情報、政府発行の書類 (国民 ID、運転免許証、パスポートなど) を含む本人確認情報を処理することがあります。
センシティブデータ	必要に応じて、Stripe はセンシティブデータ (顔認識データなど) を処理することがあります。

処理の期間

データ処理者としての Stripe	契約期間、および契約終了後の当事者の義務履行に必要な期間。

データ

セキュリティ	
データ処理者およびデータ管理者としての Stripe	Stripe は、本 DPA の別紙に記載するデータセキュリティ対策を含む、書面による情報セキュリティプログラムを実施し、維持します。

3. Stripe がデータ処理者として行動する場合に負う義務

3.1 義務

Stripe がお客様のデータ処理者として行動する場合、Stripe は次のことを行います。

(a) お客様に代わり、お客様の指示に従って個人データを処理します。Stripe は、指示がデータ保護法に違反または抵触すると判断した場合、お客様に通知します。

(b) Stripe によって個人データの処理を許可されたすべての人が、知る必要のある場合に限り個人データへのアクセス権を与えられ、その個人データの機密性に配慮するよう努めることを保証します。

(c) データ保護法により義務付けられている範囲内で、Stripe がデータ主体から受けた、データ保護法に基づく (i) 収集された個人データにアクセスする権利 (CCPA に基づく知る権利など)、(ii) 収集された個人データを訂正もしくは消去させる権利、(iii) Stripe による処理を制限する、もしくはその処理に異議を唱える権利、または (iv) データポータビリティー権を行使する各請求 (CCPA に定義されている「検証可能な消費者の請求 (verifiable consumer requests)」を含む) (以下、総称して「データ主体の請求」といいます) を通知します。より詳しい情報を求め、データ主体を特定し、該当する場合はデータ主体をデータ管理者であるお客様に案内する以外に、Stripe は、お客様が書面で Stripe に指示した場合を除き、これらの請求に応じることはありません。処理の性質を考慮し、Stripe は、データ主体の請求に応じる義務を果たせるよう、可能な限り、適切な技術的および組織的手段によりお客様を支援します。

(d) データ保護法により義務付けられている範囲内で、個人データの開示を Stripe に求める、または Stripe による個人データの開示を必要とする調査に参加するよう求める、政府機関からの法執行上の各要求を Stripe が受けた場合に、法律で禁止されていない限りその旨をお客様に通知します。

(e) データ保護法により義務付けられている範囲内で、お客様からの書面による要請に従い、お客様が データ保護法に基づく義務を遵守するための合理的な支

援を提供します。Stripe はまた、処理の性質および Stripe が利用可能な情報を考慮したうえで、お客様がデータ保護影響評価を実施したり、監督機関に相談したりするのに役立つ合理的な情報も提供します。お客様が Stripe に要請する支援が、データ保護法または本規約の下で Stripe が負う義務の範囲を超えるものである場合、Stripe は合理的な料金をお客様に請求できるものとします。

(f) Stripe でデータインシデントが発生した場合に、不当な遅滞なくお客様に通知します。GDPR または英国 GDPR の対象となる個人データに影響を及ぼすデータインシデントについては、そのデータインシデントに気付いてから、いずれの場合も 48 時間以内に通知します。Stripe によるお客様への通知には、Stripe が把握している範囲内で、(i) データインシデントの対象となった個人データの種類、(ii) 影響を受けた個人または記録の分類と潜在的な数 (その所在国を含む)、および (iii) Stripe による調査の状況と、現在のまたは計画中の是正措置について、合理的な範囲で詳細な説明が記載されます。通知後、Stripe はお客様が データ保護法に基づく義務を遵守できるよう支援するため、関連する最新情報を提供します。

(g) データ保護法により義務付けられている範囲内で、かつお客様からの書面による請求に応じて、監査報告書をお客様に提供することで、監査または調査をサポートします。この請求を受けた後、Stripe は年 1 回を超えない頻度で、Stripe

およびその関連会社による個人データの処理に関する合理的な範囲および期間を対象として、速やかに文書を提供するか、データセキュリティ質問票を作成します。提供するすべての報告書および文書は、セキュリティ質問票への回答を含め、Stripe の機密情報となります。

(h) 本規約の終了後、お客様の選択に基づき、本サービスに関連して処理されたすべての個人データを削除するかお客様に返却し、既存のコピーを削除します。ただし、Stripe によるその個人データまたは既存のコピーの保管が、(i) Stripe が本規約に基づく権利の行使と義務の履行のために必要である場合、または (ii) より長期の保管が データ保護法により義務付けられているか許可されている場合には、Stripe はその個人データの削除または返却も、既存のコピーの削除も行う必要はありません。

3.2 復処理者

(a) Stripe は、本サービスを実施するうえでの必要性に応じて、復処理者に業務を委託します。Stripe の復処理者の一覧 (Stripe 関連会社も含まれる場合があります) は stripe.com/service-providers/legal に掲載されています (以下、「Stripe 復処理者リスト」といいます)。お客様は、Stripe が自らの既存の復処理者を利用することに同意するとともに、Stripe に対し、本サービスを実施するうえでの

必要性に応じて復処理者に業務を委託する一般的権限を書面により付与するものとします。Stripe 復処理者リストのメール通知に登録している場合、Stripe は、Stripe が同リストに復処理者を追加する予定であるとき、その変更が有効になる少なくとも 30 日前までにメールでお客様に通知します。お客様は、変更の通知を受け取ってから 30 日以内であれば、正当な根拠に基づき、変更に対して正当な異議を唱えることができます。お客様は、Stripe の復処理者が本サービスを提供するために不可欠であること、およびお客様が Stripe による復処理者の利用に異議を唱えた場合、本規約 (本 DPA を含む) に別段の規定があったとしても、Stripe は、Stripe がその復処理者を利用している本サービスをお客様に提供する義務を負わないことを了承するものとします。

(b) Stripe は、各復処理者との間で、適切なデータセキュリティ対策を講じる義務を含む、本 DPA の下で Stripe に課される義務と同等の義務を復処理者に課す書面契約を締結します。その契約に基づくデータ保護義務を復処理者が履行しない場合、Stripe は、本 DPA における該当する本サービスを直接履行したときに Stripe が負う責任と同じ範囲で、復処理者の作為・不作為についてお客様に対し引き続き責任を負うものとします。

3.3 CCPA

CCPA が適用され、Stripe がデータ処理者として行動する場合、Stripe は、(a) (CCPA で定義されているところの) 個人データを販売または共有せず、(b) Stripe のプロダクトおよびサービスの提供を目的とするとき、ならびに法令を遵守するために必要とされるときを除き、お客様との直接の取引関係の範囲を超えて個人データを保持、使用または開示せず、また (c) Stripe のプロダクトおよびサービスの提供を目的とするとき、および法令で認められている場合を除き、お客様から、またはお客様を通じて受領した個人データを、他のユーザーから、もしくは他のユーザーに代わって受領した個人データ、または Stripe 自身による他のユーザーとのやり取りから収集した個人データと組み合わせることはありません。Stripe は、自らが CCPA に関連する本 DPA の要件を理解しており、これを遵守し、また CCPA が義務付けているものと同じ水準のプライバシー保護を個人データに適用することを認証します。Stripe は、自らが CCPA に基づく義務を履行できなくなったと判断した場合、お客様に通知し、個人データの不正な処理を是正するための合理的かつ適切な措置を講じます。

3.4 免責

本 DPA を含む本規約に別段の規定があったとしても、Stripe およびその関連会社は、Stripe がお客様の指示に従って行動していた限りにおいて、Stripe または

その関連会社の作為または不作為に起因または関連するデータ主体による請求について責任を負いません。

4. お客様がデータ管理者として行動する場合に負う義務

お客様は、次の要件を満たすものとします。

(a) 適法である指示のみを Stripe に対して行います。

(b) データ主体の権利、データセキュリティ、秘密保持に関するものを含め、データ保護法に基づく義務を遵守し、履行するとともに、本 DPA を含む本規約に記載する個人データの処理について、適切な法的根拠に基づくものとします。

(c) 本 DPA を含む本規約に記載する目的のための Stripe およびお客様による個人データの処理に関して、データ主体に対し、必要なすべての情報を (透明性が高く簡単にアクセスできる、プライバシーに関する公開通知を提供するなどして) 提供し、データ保護法で義務付けられている場合は、必要なすべての同意を得ます。

5. Stripe がデータ管理者として行動する場合に負う義務

Stripe は、個人データを処理する際に、データ保護法に基づく義務を遵守し、履行しなければなりません。

6. データ移転

6.1 お客様による越境データ移転

お客様は、Stripe が本サービスを提供できるようにするため、個人データを米国の Stripe, Inc. (「SINC」) に移転することを了承するものとします。この移転に、データ移転メカニズムを必要とする個人データが伴う場合、本 DPA に組み込まれるデータ移転に関する補遺が適用されます。

6.2 Stripe による越境データ移転

Stripe およびその関連会社は、本サービスを提供するために必要な場合、個人データをグローバルに移転することがあります。特に、個人データは、米国の SINC や、他の国における Stripe の関連会社および復処理者に移転されることがあります。

7. 規定間の矛盾

規定間に矛盾がある場合は次のとおりとします。

(a) 本 DPA の規定と、個人データの処理に関する本規約の規定との間に矛盾がある場合は、本 DPA の規定が優先されます。

(b) 本 DPA の規定と、データ移転に関する補遺の規定との間に矛盾がある場合は、データ移転に関する補遺の規定が優先されます。

8. 定義

本 DPA で定義されていない、英語版において大文字で始まる用語はすべて、本規約で定義されている意味に従います。

「本規約」は、お客様と Stripe との間の Stripe 利用規約 (www.stripe.com/[countrycode]/legal/ssa に記載) で与えられた意味を有します。

ここで、「[countrycode]」とは、お客様の Stripe アカウントが所在する国を表す 2 文字の略語を意味するか、当事者間で別途合意されたものを意味します。

「認定サービス」とは、政府機関が認可、許可、または規制する本サービスを意味します。

「CCPA」とは、2018 年カリフォルニア州消費者プライバシー法 (カリフォルニア州民法第 1798.100 条 ~ 第 1798.199 条) およびその施行規則を意味します。

「データ管理者」とは、単独で、または他者と共同で、個人データの処理の目的および手段を決定する事業体を意味し、これには、該当する場合、CCPA で定義されている「事業者」が含まれることがあります。

「データインシデント」とは、当事者もしくはその関連会社、または当事者もしくはその関連会社の下請業者、代理人もしくは代表者の所有下もしくは管理下にある個人データに関して、そのデータの不正または違法な処理、使用、アクセス、紛失、開示、破壊または改変を意味します。

「データプライバシーフレームワーク」とは、該当する場合、米国商務省が運営する EU と米国間、スイスと米国間、または英国と米国間のデータプライバシーフレームワークの自己認証制度を意味します。

「データ処理者」とは、データ管理者に代わって個人データを処理する事業体を意味し、これには、該当する場合、CCPA で定義されている「サービスプロバイダー」が含まれることがあります。

「データセキュリティ対策」とは、個人データをその処理のリスクに見合ったセキュリティ水準で保護することを目的とした、技術的および組織的な対策を意味します。

「データ主体」とは、個人データに関連する、識別された、または識別可能な自然人を意味します。

「データ移転メカニズム」とは、データ保護法の下で個人データの適法な越境移転を可能にする移転メカニズムを意味します。これには、データプライバシーフレームワーク、EEA SCC、英国国際データ移転に関する補遺、本 DPA に組み

込まれる データ保護法の下で利用可能なデータ移転メカニズムなど、EEA、スイス、および英国の データ保護法の下で必要とされる移転メカニズムが含まれます。

「データ移転に関する補遺」とは、www.stripe.com/legal/dta に記載されているデータ移転に関する補遺を意味します。

「データ保護法」とは、プライバシー、データ保護またはデータセキュリティに何らかの点で関連のある国際法、連邦法、州法および現地法を含む、本規約および本 DPA に基づく個人データの処理に適用される法令を意味します。

「EEA」とは、欧州経済領域を意味します。

「EEA SCC」とは、個人データを GDPR に従って第三国に移転するための標準契約条項に関する欧州委員会実施決定 (EU) 2021/914 内に定められた標準契約条項のモジュール 1 (移転: 管理者から管理者) およびモジュール 2 (移転: 管理者から処理者) を意味します。

「GDPR」とは、一般データ保護規則 (EU) 2016/679 を意味します。

「指示」とは、Stripe API、Stripe ダッシュボード、またはお客様と Stripe との間の書面による合意を通じて示されるものを含む通信または文書であって、それを通じて、データ管理者がデータ処理者に対し、自己のために個人データの特定の処理を実行するよう指示するものを意味します。

「共同管理者」とは、他のデータ管理者と個人データの処理の目的および手段を共同で決定するデータ管理者を意味します。

「個人データ」とは、本サービスに関連して処理される、識別可能な自然人に関するあらゆる情報を意味し、これには、GDPR で定義されている「個人データ」および CCPA で定義されている「個人情報」が含まれます。

「処理」とは、1 件の個人データまたは個人データの集合に対して単一の操作または一連の操作を実行することを意味し、ここでいう操作には、データ保護法で説明されているとおり、収集、記録、編集、構造化、保存、適合または改変、検索、参照、使用、送信による開示、配布その他の方法により利用可能にすること、整合または結合、制限、消去または破棄などが含まれます。

「センシティブデータ」とは、そのデータが データ保護法の下で個人データの特別な分類として他の個人データとは明確に区別されて取り扱われている限りにおいて、(a) 遺伝子データ、生体データ、健康状態、もしくは自然人の性生活や性的指向に関するデータである個人データ、(b) 人種的もしくは民族的出自、政治的見解、宗教的もしくは哲学的信条、もしくは労働組合への加盟に関するデータ、(c) 地理位置情報データ、または (d) CCPA で定義されているセンシティブな個人情報を意味します。

「復処理者」とは、データ処理者が、本サービスに関連して自己に代わり個人データを処理するよう委託する事業体を意味します。

「監督機関」とは、(i) 欧州連合加盟国により GDPR 第 51 条に基づいて設立された独立の公的機関、または (ii) お客様に対する監督権限および管轄権を有しデータ保護を管理する公的機関を意味します。

「英国 GDPR」とは、2018 年欧州連合 (離脱) 法第 3 条の運用により英国国内法に移管され、2019 年データ保護、プライバシーおよび電子通信 (改正等) (EU 離脱) 規則により改正された GDPR を意味します。

「英国国際データ移転に関する補遺」とは、英国の個人情報保護監督機関 (Information Commissioner's Office) が発行する EEA SCC の国際データ移転に関する補遺を意味します。

別紙: Stripe のデータセキュリティ

セキュリティプログラムとポリシー	Stripe は、セキュリティ管理手段を含め、Stripe におけるセキュリティ管理方法に対応したセキュリティプログラムを維持し、実施します。セキュリティプログラムには以下が含まれます。 - Stripe が正式に承認し、社内で公表し、適切な人員に伝達し、少なくとも年次で見直す文書化されたポリシー - セキュリティプログラム活動に対する責任と権限の文書化された明確な割り当て - 該当する場合、許容されるコンピューターの使用、データ分類、暗号化管理、アクセス管理、リムーバブルメディア、およびリモートアクセスに関するポリシー - 主要な管理手段、システムおよび手順の定期的なテスト プライバシープログラム。Stripe は、個人データの収集、使用、共有の方法を取り扱うプライバシープログラムおよび関連ポリシーを維持し、実施します。

リスク管理と資産管理	Stripe は、リスク評価を実施するとともに、リスクの特定、分析、監視、報告および是正措置のための管理手段を取り入れ、維持します。 Stripe は、ハードウェア資産およびソフトウェア資産を、それらのライフサイクル全体を通して適切に分類し管理する資産管理プログラムを維持し、実施します。
人員の教育と管理手段	すべての (a) Stripe の従業員、および (b) Stripe の独立請負業者であって、個人データを処理する者を含む、データにアクセスする可能性のある者 ((a) と (b) を総称して、以下「人員」といいます) は、Stripe のポリシーに基づくデータセキュリティおよびプライバシーに関する自己の責任について了承するものとします。 人員について、Stripe は、自ら、または第三者を通じて、次のことを行います。 - 雇用前の身辺調査およびスクリーニングを実施する - セキュリティおよびプライバシーに関するトレーニングを実施する

	- データセキュリティまたはプライバシーに関する要件の違反に対する懲戒プロセスを実施する - 解雇または該当する役割の変更があり次第、人員のアクセス権を速やかに削除または更新し、人員に個人データの返却または破棄を求める
	認証。Stripe は、各人員の身元を、強力なパスワード、トークンデバイス、生体認証などの適切な認証資格情報を通じて認証します。
トレーニングと意識向上	セキュリティおよびプライバシーに関する年次トレーニング。Stripe の従業員は、Stripe のデータセキュリティおよび機密保持に関するポリシーと実践について、セキュリティおよびプライバシーに関する年次の意識向上トレーニングを受講します。

ネットワーク管理と運用管理	ポリシーと手順。Stripe は、ネットワーク管理と運用管理のためのポリシーおよび手順を実施します。これらのポリシーおよび手順は、ハードニング、変更管理、職務分掌、開発環境と本番環境の分離、技術アーキテクチャ管理、ネットワークセキュリティ、マルウェアからの保護、転送時および保管時のデータ保護、データの完全性、暗号化、監査ログ、ネットワーク分離を取り扱っています。
	脆弱性評価。Stripe は、個人データを処理するシステムとアプリケーションなど、運用するシステムとアプリケーションの脆弱性評価および侵入テストを定期的に実施しています。脆弱性は、Stripe の脆弱性管理基準に従って管理、是正されます。

	アクセス制御。Stripe は、データ処理システムが無許可の者に使用されないようにするため、次の対策を実施しています。 - ユーザーの識別および認証手順 - MFA など NIST 800-63B に基づくより強固なデジタル認証手段を含む ID/パスワードによるセキュリティ手順 - 自動ブロック (パスワードやタイムアウトなど) - 侵入試行に対する監視
技術的アクセス制御	データアクセス制御。Stripe は、データ処理システムを使用する権限のある者が、そのアクセス権に基づき許可された個人データのみにアクセスできるようにし、許可なく個人データの読み取り、コピー、変更または削除をできないようにするために、以下のような対策を実施しています。 - 内部ポリシーおよび手順 - 管理権限スキーム - 分化型アクセス権 (プロファイル、ロール、アクション、目的) - アクセスの監視と口ギング

- アクセスレポート

- アクセス手順

- 変更手順

- 削除手順

物理的アクセス制御	Stripe は、信頼できるサードパーティーのサービスプロバイダーを利用して本番環境のインフラをホストしています。Stripe は、これらのサードパーティーを活用して、自社が管理するデータセンター施設への物理的なアクセス制御を管理しています。Stripe のサービスプロバイダーは、個人データが処理されている施設および設備で使用可能なデータ処理システム (データベース、アプリケーションサーバー、関連ハードウェアを含む) に、権限のない者が物理的にアクセスできないようにするための対策を提供しています。このような対策には、たとえば以下のようなものがあります。 - Stripe の施設に設置された物理的アクセス制御システムおよびプログラム - 物理的セキュリティシステムを監視する年中無休のグローバルセキュリティオペレーションセンター - セキュリティビデオとアラームシステム - アクセス制御のロールおよび区域ゾーン - アクセス管理監査対策

- 鍵の電子追跡および管理プログラム

- 従業員および第三者に対するアクセス許可プロセス

- ドアの施錠 (電気錠など)

- 訓練を受けた制服着用の警備スタッフ

Stripe は、サードパーティーによる監査報告書を確認して、Stripe のサービスプロバイダーが管理対象のデータセンターにおいて適切な物理的アクセス制御を維持しているか検証します。

可用性制御	Stripe では、物理的または技術的なインシデントが発生した場合に、可用性および個人データへのアクセスを適時に復旧できる能力を確保するための対策を実施しています。このような対策には、たとえば以下のようなものがあります。 - データベースのレプリケーション - バックアップ手順 - ハードウェアの冗長性 - 災害復旧計画
開示制御	Stripe は、(a) 電子的伝送、転送、ストレージメディアへの (手動または電子的) 保存中に、認可なく個人データを読み取り、コピー、変更または削除できないようにすること、および (b) ロギング、転送セキュリティ、暗号化を含め、個人データがどの企業やその他の法人に開示されているかを確認できるようにすることを徹底するための対策を講じています。

入力制御	Stripe は、ロギングおよび報告システム、監査証跡、文書化を含め、データ処理システムからデータが入力、変更または除去 (削除) されたかどうか、また誰によってなされたかを監視するための対策を実施しています。
分離制御	Stripe は、それぞれ異なる目的で収集された個人データが確実に個別に処理されるようにするために、以下を含む対策を実施しています。 - 内部サービスによるデータへのアクセスの「最小権限」制限 - 機能分離 (本番/テスト) - それぞれ異なる目的でのデータの保存、修正、削除、送信の手順 - 個人データの分離を管理するための論理セグメンテーションプロセス

	PCI 準拠。本サービスに該当する範囲において、Stripe は本サービスを、PCI-DSS 要件で規定されている最高認定レベル (PCI レベル 1) に合致した方法で提供する責任を負います。Stripe の認定は、認定セキュリティ審査機関 (QSA) による確認を毎年受けています。
認定とレポート	SOC レポート。Stripe は、AICPA の下で発行されるサービス組織に対する監査基準である Service Organization Controls (以下「SOC」) を維持しています。SOC 1 レポートと SOC 2 レポートは毎年作成され、請求に応じて提供されます。 Stripe は基準や認定をいつでも追加することがあります。

暗号化	Stripe は、Stripe のサービスにおける複数のポイントでデータ暗号化メカニズムを適用することで、保管時および転送時の Stripe データへの不正アクセスが発生するリスクを軽減させています。Stripe の暗号鍵の資料へのアクセスは、許可のある限られた数の人員に制限されています。 転送時の暗号化。転送時のデータを保護するため、Stripe ではすべての送受信データ接続に、TLS 1.2 プロトコルを使用した暗号化を義務付けています。Stripe の社内本番ネットワークを経由するデータについては、Stripe は mTLS により本番システム間の接続を暗号化します。 保管時の暗号化。保管時のデータを保護するため、Stripe では、業界標準の暗号化 (AES-256) により、サーバーインフラに保存されるすべての本番データを暗号化します。 決済カードと銀行口座データのトークン化。決済カード番号と銀行口座番号は、データレベルで業界標準の暗号化 (AES-256) を使用して個別に暗号化され、高度に制限された別個のデータボールトに保管されます。復号鍵は別のマシンに保存されます。トークンは、Stripe のデータ処理をサポートするために生成されます。

データセキュリティインシデントの管理と通知	Stripe は、Stripe がデータインシデントを管理する方法に対応したデータセキュリティインシデント管理プログラムを実施しています。 影響を受ける Stripe ユーザーおよび政府機関 (該当する場合) に対し、Stripe は データ保護法の定めるところに従って適時にデータインシデントを通知します。
審査、監査報告書、セキュリティ質問票	Stripe は、書面による要請を受けた場合、年 1 回を超えない頻度で、個人データの処理に関する Stripe のビジネス慣行およびデータ技術環境について、合理的な範囲および期間に関するデータセキュリティ質問票に回答します。このセキュリティ調査票に対する Stripe の回答は、Stripe の機密データとなります。

システム構成	Stripe は、社内 IT および IT セキュリティガバナンスのためのデフォルト構成措置など、システム構成を確保するための措置を実施しています。 Stripe は基本的に、インフラとシステム構成をデプロイするうえでデプロイメント自動化ツールを使用しています。自動化ツールは、Stripe のインフラ構成を活用しています。この構成はコードで管理されており、変更管理プロセスを経て進行します。Stripe の変更管理プロセスにおいては、本番環境へのリリースに先立ち、正式なコードレビューと 2 者の承認が必要です。 Stripe は監視ツールを使用して本番インフラを監視し、既知の構成ベースラインからの変更がないか確認します。
データポータビリティー	Stripe API を使用すると、PCI の範囲に含まれるデータを除き、Stripe ユーザーはプログラムを使って、転送用に保存されたデータにアクセスできます。PCI-DSS レベル 1 に準拠している他の決済代行業者へ移行する場合の PCI データのポータビリティープロセスについては、https://stripe.com/docs/security/data-migrations/exports をご覧ください。

データの保持と削除	Stripe は、個人データに関するデータ保持ポリシーおよび手順を実施、維持し、これらのポリシーと手順の見直しを適宜行っています。