以下の翻訳は情報提供のみを目的として提供されるものです。この翻訳と最新の英語版との間に（翻訳の遅れによるものも含め）不一致、矛盾、抵触がある場合は、英語版が優先されます。

Amazon ベンダーセキュリティポリシー

最終更新日：2024 年 9 月 11 日

1. **対象範囲** サプライヤーは、このセキュリティ要件（「本セキュリティポリシー」）を遵守するものとします。本セキュリティポリシーは、サプライヤーの他の契約上又は法律上の義務を制限するものではありません。本セキュリティポリシーとサプライヤー及び Amazon 間の他の契約との間に矛盾がある場合、サプライヤーはその範囲で、Amazon 情報の保護を強化するより制限の厳しい要件を遵守するものとします。

2. **更新**

2.1 Amazon は、随時、本セキュリティポリシーに対し商業上合理的な更新を行うことができます。更新は、本セキュリティポリシーの「最終更新日」から 30 日後に発効します。サプライヤーは、更新が発効した時点で、更新後のセキュリティポリシーに拘束されることに同意します。

2.2 サプライヤーは、これらの更新について発効前に事前通知を受けることを希望する場合、本セキュリティポリシーのウェブページに掲載されている申込書式を利用して更新通知の受信を申し込むことができます。サプライヤーは、更新通知の申込みの際に提供されたサプライヤーのすべての連絡先情報を常に正確かつ最新の状態に保つようにします。更新通知は、サプライヤーが実際に受領したか否かにかかわらず、電子メールで送信された時点で、サプライヤーがこれを受信したものとみなされます。

3. **許可された目的**

3.1 **明示的な許可** サプライヤーは、本件契約に基づき明示的に許可された Amazon 情報のみを、本件契約に基づき製品又はサービスを提供する目的（「許可された目的」）に限り処理することができます。

3.2 **データ保持** サプライヤーは、許可された目的のためにのみ、必要とされる期間に限り、Amazon 情報を保持します。

3.3 **明示的な制限** サプライヤーは、別途以下のとおりとします。匿名化されている場合でも、(a) Amazon 情報を処理しないこと、(b) Amazon 情報を譲渡、賃貸、交換、取引、販売、貸与、リース、その他の方法で第三者に配布し、又は利用可能にしないこと、(c) Amazon 情報を使用して人工知能（AI）又は機械学習（ML）モデルを開発、訓練又は改善しないこと。

4. **最低セキュリティ要件** サプライヤーは、業界のベストプラクティス（国際標準化機構（「ISO」）の 27001 及び 27002、米国国立標準技術研究所（「NIST」）のサイバーセキュリティフレームワーク、その他の同様の規格を含みます。）に則った物理的、管理的及び技術的な保護措置を維持します。サプライヤーが維持する保護措置には、以下の第 4.1 項から第 4.18 項に記載する最低限の要件を含めるものとします。

4.1 **書面による情報セキュリティプログラム** サプライヤーは、以下に該当する書面による情報セキュリティプログラムを実施します。(a) 本セキュリティポリシーに定める要件を満たす適切なポリシー、手順及び基準を含み、(b) セキュリティ問題（セキュリティインシデントを含みます。）の連絡及び管理につき責任を負うセキュリティ担当窓口を指定し、(c) 少なくとも年 1 回見直しを行い、必要に応じて更新し、(d) 人員に適用されるもの。サプライヤーは、情報セキュリティプログラムを監視及び実施して、違反に対処します。

4.2 **パッチ管理** サプライヤーは、最新のアップグレード、アップデート、バグフィックス及び新バージョンにより、対象情報システムを最新の状態に保ちます。サプライヤーは、パッチ適用不可能なアセットに対する緩和策を実施します。

4.3 **ロギング** サプライヤーは、監査、イベント及びセキュリティログを収集、管理及び保持します。例えば、(a) 許可された目的のためにサプライヤーに提供された Amazon のアカウント又はクレデンシャルのすべての使用（許可されたもの及び許可されていないものの両方）に関するログデータ、並びに (b) Amazon 情報又は対象情報システムにアクセスできる Amazon

以下の翻訳は情報提供のみを目的として提供されるものです。この翻訳と最新の英語版との間に（翻訳の遅れによるものも含め）不一致、矛盾、抵触がある場合は、英語版が優先されます。

の人員又は本人員のなりすまし、又はなりすましの試みに関するログデータが含まれます。当該ログには、ログに記録された各イベントについて、(i) イベントを開始した本人員又はアカウント、(ii) イベントの発生時刻、(iii) 影響を受けたシステム、データ、その他のリソースを特定するのに十分なデータが含まれます。サプライヤーは、不正行為の検出、調査及び復旧に役立てるため、当該ログを定期的に分析します。

4.4 **マルウェアからの防御** サプライヤーは、(a) すべての対象情報システムにマルウェア対策ソフトウェア又は同等のセキュリティ制御を導入し、(b) マルウェア対策ソフトウェア又は同等のセキュリティ制御のアップデート、シグネチャ及び設定を維持し、(c) 悪意のあるコード又は不正なコードのインストール、拡散及び実行を検出、防止及び是正するシステムを設定します。

4.5 **リスク管理プログラム** サプライヤーは、リスク分析、リスク処理、リスク受容、例外処理のプロセスを定義した書面による情報セキュリティリスク管理プログラムを実施します。

4.6 **セキュリティ意識向上トレーニング** サプライヤーは、採用時及びその後少なくとも年 1 回、本人員を対象として、情報セキュリティ及びデータプライバシーに関するトレーニングを行います。サプライヤーはまた、サプライヤーのセキュリティ及びデータプライバシーポリシーの更新について、本人員に適時に通知するようにします。

4.7 **データインベントリ** サプライヤーは、(a) 自らが処理している Amazon 情報の種類並びに (b) 当該 Amazon 情報が処理されている方法及び場所に関する情報を（例えば、最新のアーキテクチャ図などに）文書化し、維持します。Amazon の要求に応じて、サプライヤーは、この情報を Amazon に提供します。

4.8 **セキュリティテスト**

4.8.1 サプライヤーは、本セキュリティポリシーの要件を確実に満たすため、毎年テストを実施します。

4.8.2 サプライヤーは、少なくとも年 1 回、サプライヤーのセキュリティ防御の侵入テストを実施します。侵入テストには、(a) サプライヤーのネットワーク内外からのテスト、(b) ソーシャルエンジニアリング（フィッシングシミュレーションなど）、(c) 無線ネットワークのセキュリティテストが含まれます。サプライヤーは、脆弱性管理プログラムの一環として、特定された脆弱性に対処します。Amazon の要求に応じて、サプライヤーは、そのような侵入テストの結果及び脆弱性修復を Amazon に提供します。

4.9 **ネットワークセキュリティ** サプライヤーは、特に外部ネットワークからの不正なネットワークアクセスを制限することにより、対象情報システムを保護します。サプライヤーは、システムを不正アクセスから保護するため、ファイアウォールその他の同等のセキュリティ制御を維持、設定し、少なくとも年 1 回、ファイアウォールルールセットを見直し、すべてのルールについて文書化された有効なビジネスケースが存在するよう徹底します。

4.10 **適切な環境** サプライヤーは、その目的に適した環境でのみ Amazon 情報を処理し、本件契約に基づき許容されていない限り、テスト環境で Amazon 情報を処理しないものとします。

4.11 **暗号化** サプライヤーは、業界のベストプラクティスに従い、静止時及び外部ネットワーク経由時のすべての Amazon 情報を暗号化します。Amazon 情報がサプライヤーの内部ネットワークで送信される場合、業界のベストプラクティスに適合する暗号化されたプロトコルを介して送信されます。サプライヤーは、業界のベストプラクティスに従って暗号鍵を管理し、保護します。

4.12 **管理者特権の使用制御** サプライヤーは、NIST サイバーセキュリティフレームワーク又は ISO 27002 に従い、管理者機能を管理します。サプライヤーは、最低限、管理者アカウントを標準アカウントから分離し、管理者アカウントを管理機能の実行に必要な機能にのみ制限します。サプライヤーは、個々のユーザーに帰属する方法で、すべての管理者アカウントの操作を記録します。標準アカウントに付与される管理者機能は、最小特権ベースであり、個々のユーザーに帰属する方法で記録されます。

以下の翻訳は情報提供のみを目的として提供されるものです。この翻訳と最新の英語版との間に（翻訳の遅れによるものも含め）不一致、矛盾、抵触がある場合は、英語版が優先されます。

4.13 **アクセス制御**

4.13.1 **一意の ID** サプライヤーは、Amazon 情報又は対象情報システムにアクセスできる本人員に対し、管理者アクセス権を有するアカウントを含め、個別の一意の ID を付与します。

4.13.2 **「知る必要」がある場合に限定** サプライヤーは、Amazon 情報及び対象情報システムへのアクセス許可を、許可された目的のために「知る必要」がある本人員のみに限定します。

4.13.3 **ユーザーアクセスレビュー** サプライヤーは、少なくとも 90 日に 1 度、Amazon 情報及び対象情報システムにアクセスできる本人員及びサービスのリストを見直し、アクセスする必要がなくなったアカウントからアクセス権を削除します。

4.13.4 **Single Sign-On（SSO）** Amazon の人員認証を必要とするサプライヤーサービスは、そのような認証を提供する際に、Amazon ID プロバイダー（Amazon Federate など）と統合する必要があります。このようなサービスは、認証のためにサプライヤーが提供する、又はサプライヤーが管理するクレデンシャルを使用してはなりません。

4.14 **パスワードの管理**

4.14.1 **強力なパスワード** サプライヤーは、対象情報システムのシステムパスワードその他のセキュリティパラメーターにおいて、メーカーが提供するデフォルト値を使用しないものとします。サプライヤーは、すべての対象情報システムにおいて、NIST SP 800-63B に記載されているベストプラクティスに従い、システムで強制される「強力なパスワード」の使用を義務付け、徹底します。サプライヤーは、すべてのパスワード及びアクセスクレデンシャルの秘密保持を義務付けるものとし、これらを本人員間で共有しないものとします。

4.14.2 **ロックアウト** サプライヤーは、アカウントについて連続 10 回不正確なパスワードの入力を試みた場合、Amazon 情報又は対象情報システムにアクセスできるアカウントを無効にすることで、「アカウントのロックアウト」を維持し、実施します。

4.15 **リモートアクセス、多要素認証** サプライヤーは、サプライヤーのネットワーク、システム、アプリケーション、その他のアセットへのリモートアクセスについて、多要素認証（すなわち、ユーザーを認証するために少なくとも 2 要素を必要とするもの）を導入します。

4.16 **「一括」アクセス** 本条において、「一括」アクセスとは、データベースクエリ、レポート作成その他データの大量転送によってデータにアクセスすることを意味します。

4.16.1 本件契約に明示的に定める場合、又は Amazon が書面で別途定める場合を除き、サプライヤーは、Amazon 情報が Amazon 又はサプライヤーが制御するデータベース内にあるか、ファイルベースのアーカイブ（フラットファイルなど）への保存を含むその他の方法を用いて保存されているかにかかわらず、Amazon 情報に「一括して」アクセスせず、またそのようなアクセスを許可しません。

4.16.2 Amazon が「一括」アクセスを許可する場合、サプライヤーは、(a) 当該アクセス許可を「知る必要」がある指定された本人員のみに制限し、(b) 第 4.3 項の要件に従い、当該アクセスの明示的な許可及びロギングを要求します。第 10 条のセキュリティレビュー又は第 11 条のセキュリティインシデントに伴う Amazon の要求に応じて、サプライヤーは、本条で言及される「一括」アクセスに関するすべてのログを Amazon に提供します。

4.17 データの分離 サプライヤーは常に、Amazon 情報をサプライヤー及び第三者の情報から物理的又は論理的に分離します。分離が不可能な場合、サプライヤーは、ロギング、削除、インシデントへの対応の目的で、Amazon 情報を他の情報と区別できるようにします。

4.18 **サプライヤーの本人員のセキュリティ**

以下の翻訳は情報提供のみを目的として提供されるものです。この翻訳と最新の英語版との間に（翻訳の遅れによるものも含め）不一致、矛盾、抵触がある場合は、英語版が優先されます。

4.18.1 サプライヤーは、Amazon 情報へのアクセス権を付与された本人員がその秘密性を保持し、許可された目的のみにこれを使用させるよう、あらゆる合理的な予防措置を講じます。これらの予防措置には、秘密保持契約やサプライヤーポリシーを通じて秘密保持の要件を課すことも含まる必要があります。

4.18.2 (a) Amazon 情報へのアクセスを必要としなくなった本人員、又は (b) サプライヤーの本人員としての資格を失った本人員については、サプライヤーは、24 時間以内に Amazon 情報及び対象情報システムへのアクセスを終了します。(a)又は(b)のいずれかが発生してから 24 時間以上経過した後も、いずれかの本人員が Amazon 情報又は対象情報システムへのアクセス権を保持する場合、サプライヤーは、サプライヤーがこの継続的なアクセスに気づいてから 24 時間以内に、Amazon に電子メール（security@amazon.com）で通知します。

5. **支払セキュリティ要件** サプライヤーは、ペイメントカード会員データにアクセスできる場合、又はこれを処理する予定である場合、ペイメントカード業界データセキュリティ基準（PCI DSS）の最新版を遵守します。

6. **下請業者**

6.1 サプライヤーは、Amazon の書面による事前の同意を得ずに、本セキュリティポリシーに基づく義務を第三者（総称して「下請業者」）に再委託又は委任しないものとします。下請契約又は委任の存在又は条件にかかわらず、サプライヤーは、本セキュリティポリシーに基づく義務の完全な履行について引き続き責任を負います。本セキュリティポリシーの条件は、サプライヤーの下請業者及び下請業者の本人員に対して拘束力を有します。

6.2 サプライヤーは、下請業者の対象情報システムを使用する場合、下請業者の対象情報システム及びそのセキュリティ制御についてセキュリティレビューを実施し、Amazon の要求に応じて、下請業者の対象情報システムのセキュリティ制御に関する定期的な報告を Amazon が要求する形式（保証業務基準書（Statement on Standards for Attestation Engagements）（SSAE）16 など）にて提出します。

7. Amazon が管理する情報システムへのアクセス Amazon は、許可された目的に限り、ウェブポータルその他の非公開ウェブサイト又はエクストラネット（それぞれ、「Amazon が管理する情報システム」）を介して Amazon 情報を処理する権利をサプライヤーに付与することができます。Amazon がサプライヤーに対し、Amazon が管理する情報システムを使用して Amazon 情報を処理することを許可する場合、サプライヤー及びその本人員は、以下の要件に従わなければなりません。

7.1 **アカウント** サプライヤーは、サプライヤーの本人員が、Amazon により各個人に指定された Amazon が管理する情報システムアカウントのみを使用するよう徹底するほか、サプライヤーの本人員に対し、アクセスクレデンシャルを秘密にすること及びこれを共有しないことを義務付けるものとします。

7.2 **システム** サプライヤー及びその本人員は、(a) サプライヤーが管理し、フルディスク暗号化を使用するオペレーティングシステムを実行し、(b) 第 4.2 項（パッチ管理）、第 4.4 項（マルウェアからの防御）及び第 4.9 項（ネットワークセキュリティ）の要件を満たすコンピューティングシステム若しくは処理システム又はアプリケーションを通じてのみ、Amazon が管理する情報システムを使用します。

7.3 **制約** Amazon が事前に書面で承認しない限り、サプライヤーとその本人員は、Amazon が管理する情報システムから Amazon 情報をいかなる媒体にもダウンロード、ミラーリング、又は永久保存しないものとします。

7.4 **アカウントの終了** (a) Amazon が管理する情報システムへのアクセスが不要になった、又は (b) サプライヤーの本人員としての資格を失った本人員（サプライヤーを退職した者など）について、サプライヤーは、直ちに（遅くとも 24 時間以内に）Amazon が管理する情報システムへの当該本人員のアクセスを終了するか、又は Amazon への通知をもって当該アクセス権の削除を要請します。

8. **Amazon のドメイン又は URL** サプライヤーは、Amazon の単独使用のために提供するドメイン又は URL について、本件契約終了後少なくとも 5 年間、これを第三者に発行してはならず、第三者がこれを再利用してもなりません。

以下の翻訳は情報提供のみを目的として提供されるものです。この翻訳と最新の英語版との間に（翻訳の遅れによるものも含め）不一致、矛盾、抵触がある場合は、英語版が優先されます。

9. データの返却と削除、メディアのフォレンジック破壊

9.1 **データの返還及び削除** Amazon の要求があった場合、サプライヤーは、返還及び／又は削除を要求する Amazon の通知に従い、速やかに（ただし 72 時間以内に）すべての Amazon 情報を Amazon に返還し、永久的かつ安全に削除します。サプライヤーはまた、許可された目的の達成、又は本件契約の解除若しくは満了のうちいずれか早く到来した日から 30 日以内に、Amazon 情報のすべてのライブ（オンライン又はネットワークからアクセス可能な）インスタンスを永久的かつ安全に削除するものとします。Amazon の要求を受けた場合、サプライヤーは、すべての Amazon 情報が削除されたことを書面で証明します。明確にするために付言すると、本条は、第 9.3 項に基づくアーカイブコピーには適用されません。

9.2 **データサニタイゼーション** サプライヤーにより削除されたすべての Amazon 情報は、該当する種類のデバイスをパージするために、NIST SP 800-88 Rev 1「メディアサニタイゼーションガイドライン（Guidelines for Media Sanitization）」（2014 年 12 月 18 日、付録 A）に含まれる最小限のサニタイゼーションの推奨に従って消去されます。該当するタイプのデバイスに関して NIST SP 800-88 にガイドラインがない場合、サプライヤーは、以下のいずれかの方法により Amazon 情報を含むデバイスを破棄します。(a) NIST の SP800-88 で定義されたパージ、(b) NIST の SP800-88 で定義された破棄、(c) その他 Amazon 情報の分類と機密性に基づいて Amazon が要求することのある基準。

9.3 **アーカイブコピー** サプライヤーは、法により Amazon 情報のアーカイブコピーの保持を義務付けられる場合、アーカイブされた Amazon 情報を他の目的で使用してはならず、引き続き、本セキュリティポリシーに基づくすべての義務を負います。アーカイブされた Amazon 情報は、暗号化したうえで、暗号化された Amazon 情報をホスト又は保存する対象情報システムが、暗号化の際に使用された鍵のコピーにアクセスできない場所に保存しなければなりません。オフラインバックアップ又は「コールド」バックアップ（即時に又はインタラクティブに使用できないバックアップ）は、物理的に安全な施設に保存する必要があります。

9.4 **メディアのフォレンジック破壊** Amazon 情報が保存されている、又はいずれかの時点で保存されていたハードウェア、ソフトウェア、その他の媒体を廃棄する前に、サプライヤーは、NIST SP 800-88 付録 A に従い、かかるハードウェア、ソフトウェア、その他の媒体の完全なフォレンジック破壊を行います。この破壊要件は、サプライヤーが物理的なアクセス権を有しない又は制御していない記憶媒体には適用されません。このような場合、サプライヤーは、業界のベストプラクティスに従い、不要になった Amazon 情報が安全に削除されるよう徹底します。

> 9.4.1 サプライヤーは、Amazon から書面による明示的な事前の承諾を得ない限り、本条に従ってフォレンジック
> 破壊されていない限り、Amazon 情報が保存されていたハードウェア、ソフトウェア、その他の媒体をいつでも販売、再販売、寄付、改修、その他の方法で譲渡しないものとします。

10. **セキュリティレビュー** Amazon の要求に応じて、サプライヤーは、以下を行うものとします。(a) Amazon リスク評価を完了させる。(b) サプライヤーによる本セキュリティポリシーの遵守状況を確認するために Amazon が要求する証拠書類を提出する。(c) Amazon 又はその代理人に指名された第三者が、サプライヤーにおける本セキュリティポリシーの遵守状況を審査することを許可する。(d) オープンサイバーセキュリティスキーマフレームワーク（Open Cybersecurity Schema Framework、OCSF）フォーマット第 4.3 項で言及されるすべてのログを Amazon に提供する。サプライヤーは、いずれかの証拠書類について、Amazon に提供して遠隔での審査を受けるのではなく、対面で又は現場で当該証拠書類を閲覧するよう求める場合、当該現場での閲覧に要する移動費その他の経費を負担します。評価又は審査によって何らかの所見が認められた場合、サプライヤーは、自らのみの費用負担で、Amazon が合理的に満足するよう、合意された期間以内にかかる所見を是正するために必要とされる合理的なあらゆる措置を速やかに取るものとします。

11. **セキュリティインシデント**

以下の翻訳は情報提供のみを目的として提供されるものです。この翻訳と最新の英語版との間に（翻訳の遅れによるものも含め）不一致、矛盾、抵触がある場合は、英語版が優先されます。

11.1 **セキュリティインシデント通知** サプライヤーは、Amazon 情報又は対象情報システムへの不正アクセス、その収集、取得、使用、送信、開示、破損又は紛失（「セキュリティインシデント」）が生じたことをサプライヤーが知った後、又はサプライヤーが合理的にそのように考えた後、可能な限り速やかに（ただし遅くとも 24 時間以内に）Amazon に通知します。サプライヤーは、セキュリティインシデント通知を security@amazon.com 宛に送信します。

11.2 **インシデント対応計画** サプライヤーは、書面によるインシデント対応計画を維持し、要請に応じてその写しを Amazon に提供します。サプライヤーは、サプライヤーの書面によるインシデント対応計画及び業界のベストプラクティスに従い、各セキュリティインシデントを適時に是正します。サプライヤーは、少なくとも年 1 回、計画を見直し、テストし、（必要であれば）更新します。

11.3 **Amazon との協力関係** サプライヤーは、(a) Amazon によるセキュリティインシデントの調査を支援し、(b) セキュリティインシデント又は対応に関与した本人員その他の者との面談を促進し、(c) サプライヤーのセキュリティインシデントの調査及び対応の詳細を書面で保管し、(d) Amazon が要求するすべての関連記録、ログ、ファイル、データ報告、フォレンジックレポート、調査報告書、その他の資料を Amazon に提供します。

11.4 **第三者通知** 法により別途義務付けられる場合を除き、サプライヤーは、(a) 第三者（規制当局若しくは顧客を含みます。）にセキュリティインシデントを通知する前、又は (b) セキュリティインシデントに関する通知若しくは公的声明で Amazon を特定する前に、Amazon の書面による事前の承諾を得ます。法により別途義務付けられる場合を除き、Amazon は、セキュリティインシデントの通知を第三者に提供するかどうか、並びに当該通知の形式、時期及び内容を決定する権利を有します。

12. **法的手続きの通知** 法的手続きの通知 法により禁止される場合を除き、Amazon 情報が法的手続きその他適用法への対応を求められる場合、サプライヤーは、Amazon が秘密保持命令その他適切な救済を求めることができるよう、十分な通知を Amazon に提供します。

13. **定義**

13.1「**本件契約**」とは、本セキュリティポリシーに言及する契約を意味します。

13.2「**Amazon**」とは、Amazon.com, Inc.及びその関係会社を意味します。

13.3「**Amazon 情報**」とは、匿名化されている場合を含め、(a) すべての Amazon 秘密情報（当事者間の他の契約において定義されます。）、(b) サプライヤー又はその関係会社が、Amazon から、Amazon のために、その他本件契約に関連して、取得、アクセス、収集、受領、保存又は維持するあらゆる形式のすべてのデータ、記録、ファイル、コンテンツ又は情報、及び (c) (a)又は(b)から派生する情報を意味します。

13.4「**匿名化**」とは、あらゆるデータ又は情報（Amazon 情報を含みます。）について、Amazon、又はそのユーザー、デバイス識別子、ソース、製品、サービス、コンテキスト若しくはブランドを特定しない、特定を許可しない、その他それらに帰属させない方法又は形態でこれらを処理することを意味します。

13.5「**対象情報システム**」とは、サプライヤーが Amazon 情報を処理する際に使用するシステムを意味します。

13.6「**本人員**」とは、サプライヤー又は下請業者の従業員、代理人、下請先、並びにそのシステム及びネットワークリソースの他の正規ユーザーを意味します。

13.7「**処理**」とは、アクセス、使用、収集、受領、保管、変更、送信、普及、その他の方法での提供のほか、消去又は破棄など、データに対して何らかの操作を実行することを意味します。

13.8「**サプライヤー**」とは、本件契約に定義されている各供給者、ベンダー又は請負業者及び本件契約の対象となる他のプロバイダーを意味します。