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。(特に翻訳の遅れを原因として)当該翻訳と英語版との間に矛盾、不統一、不一致が認められる場合、英語版を優先するものとします。

ベンダーセキュリティ規約

最終改定日:2022 年 1 月 28 日

1. 対象範囲および定義

1.1 セキュリティ規約 サプライヤーは本規約(「**本セキュリティ規約**」)に定める Amazon の情報セキュリティ要件を全ての点で遵守するものとします。本セキュリティ規約は、サプライヤーによる関連契約上の履行行為およびサプライヤーによる Amazon 情報へのアクセス、Amazon 情報の収集、使用、保存、転送、開示、破棄または削除の全てに適用するほか、Amazon 情報に関するセキュリティインシデントに適用します。それ以外のサプライヤーの義務については本セキュリティ規約による制限を加えません。そのような義務としては、Amazon との他の契約に基づく義務のほか、サプライヤーを拘束する法令に基づく義務、Amazon との他の契約をサプライヤーが履行する場合に当該履行を拘束する法令に基づく義務、または Amazon 情報もしくは許可目的に適用される法令に基づく義務を含みます。本セキュリティ規約が両当事者間の非開示契約または両当事者を拘束するその他の契約と齟齬を生じている場合、サプライヤーは直ちに当該齟齬について Amazon に通知した上で、それらのうち Amazon 情報の保護をより厳重に義務付けている方の規定に従うものとします。ただし、保護の厳重度が低い方の規定が厳重度の高い方の規定に優先する旨が明示されている場合(Amazon がそのように指定することがあります)はその限りでありません。Amazon は、本セキュリティ規約を任意に随時改定することができます。ただし、当該改定が商慣習上不当である場合、Amazon は、要請があれば、協議を行って適当な料金の追加につき合意を図るものとします。

1.2 定義

1.2.1 「**集約**」とは、Amazon 情報をサプライヤーもしくは第三者のデータもしくは情報と結合すること、または Amazon 情報をサプライヤーもしくは第三者のデータもしくは情報と併せて保存することをいいます。

1.2.2 「**関連契約**」とは本セキュリティ規約に言及する契約をいいます。

1.2.3 「**Amazon**」とは Amazon.com, Inc.およびその関連会社をいいます。

1.2.4 「**匿名化**」とは、データまたは情報(Amazon 情報を含みます)の使用、収集、保存、転送または変換を行う場合に、Amazon、Amazon のユーザー、Amazon のデバイス識別子、Amazon のソース、Amazon の製品、Amazon のサービス、Amazon のコンテキストまたは Amazon のブランドについて、それらを特定しないような方法や形式、それらの特定を可能にしないような方法や形式、およびそれらに遡及しないようなその他の方法や形式により、当該使用、収集、保存、転送または変換を行うことをいいます。

1.2.5 「**Amazon 情報**」とは次の (a) から (c) までの各々または全部をいいます。(a) 全ての Amazon 秘密情報(両当事者間の非開示契約またはその他の契約の定義に準じます)。(b) サプライヤーまたはその関連会社が、Amazon から、もしくは Amazon に代わって、またはその他の形で本セキュリティ規約もしくはサービスに関係して、または関係契約に由来もしくは関係する権利を両当事者が履行もしくは行使することに関係して、何らかの形式またはフォーマットにより、取得、アクセス、収集、受領、保存または維持管理を行うその他全てのデータ、記録、ファイル、コンテンツまたは情報。(c) 上記 (a) または (b) に由来する情報(匿名化されたものを含みます)。

1.2.6 「サプライヤー」とは関係契約で各々定義するサプライヤー、ベンダーまたは契約業者、および関連契約に拘束されるその他のプロバイダーをいいます。

1.3 許可目的 サプライヤーは、関連契約で明示的に許可されている場合かつ関連契約に基づく製品またはサービスの提供を目的とする場合に限り、本セキュリティ規約で付与されるライセンス(もしあれば)の規定に従って、Amazon 情報に係るアクセス、収集、使用、保存および転送を行うことができます(Amazon 情報のそのような用途を「**許可目的**」といい

ます）。サプライヤーは、関連契約で明示的に許可されている場合を除き、Amazon 情報に係るアクセス、収集、使用、保存または転送を行わないものとし、かつ、Amazon 情報が匿名化されているかどうかによらず、Amazon 情報の集約を行わないものとします。サプライヤーは、Amazon から事前に書面で明示的に承諾を得ている場合を除くほか、次の (a) または (b) を行わないものとします。(a) Amazon 情報を第三者に譲渡、賃貸、交換、売買、売却、貸付けもしくはリースし、またはその他の形で配布もしくは提供すること。(b) Amazon 情報が匿名化されているかどうかによらず、Amazon 情報をその他の情報またはデータと集約すること。

2. Amazon セキュリティ規約

2.1 基本的セキュリティ要件 サプライヤーは、最新の最高業界標準および Amazon が Amazon 情報の種別および機微性を基準として指定するその他の要件に準じて、物理的保護措置、管理上の保護措置および技術的保護措置ならびにその他のセキュリティ保護措置を実施することにより、次の (a) および (b) を図るものとします。(a) サプライヤーがアクセス、収集、使用、保存または転送する Amazon 情報のセキュリティおよび機密性を維持すること。(b) Amazon 情報のセキュリティおよび完全性に対する既知の脅威もしくは危険または通常予想しうる脅威もしくは危険、Amazon 情報の不慮の漏洩、改ざんおよび開示、ならびにその他全ての不正な形式による処理から Amazon 情報を保護すること。サプライヤーは、Amazon 情報の処理に使用するシステムまたは Amazon 情報にアクセスしうるシステム（「**Amazon 情報システム**」）について、次の要件を例外なく遵守するものとします。

2.1.1 ネットワークセキュリティ サプライヤーは、特に外部のインターネット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 Amazon 情報システムを保護するものとします。サプライヤーは、Amazon 情報を常時保護するために、ファイアーウォールなど実効性のあるネットワーク・セキュリティ・ソリューションをインストールして維持管理するものとします。

2.1.2 アップデート サプライヤーは、米国国立標準技術研究所（National Institute of Standards and Technology：「NIST」）の特別刊行物（Special Publication：「SP」）800-40 Revision 3 の記載内容に従って、Amazon 情報のセキュリティ確保に必要な最新のアップグレード、アップデート、バグ修正および新バージョンならびにその他の修正を適用し、Amazon 情報システムを最新の状態に保つものとします。

2.1.3 マルウェア対策 サプライヤーはマルウェア対策ソフトウェアまたは同様のセキュリティ管理手段を常時使用してマルウェアによる侵害およびマルウェア拡散のリスクの低減を図るものとします。サプライヤーがマルウェア対策ソフトウェアを使用する場合は常に最新の状態に保つものとします。

2.1.4 暗号化 サプライヤーは業界最良慣行に従って保存データおよびオープンネットワーク上で送信するデータを暗号化するものとします。

2.1.5 テスト サプライヤーは、セキュリティシステムおよびセキュリティプロセスの定期的なテストを実施して、同システムおよびプロセスが本セキュリティ規約またはサプライヤーと Amazon とが最も直近に合意したセキュリティ規約の要件を充足していることを確認するものとします。Amazon が第 1.1 項に従って本セキュリティ規約の改定を行った場合、本項に関しては、サプライヤーと Amazon とが合意（電子メールによる合意で足りるものとします）に達するまで当該変更は効力を生じないものとします。

2.1.6 アクセス制御 サプライヤーは次の要件を遵守するなどの方法により Amazon 情報のセキュリティを確保するものとします。

2.1.6.1 サプライヤーはコンピューター上で Amazon 情報または Amazon 情報システムにアクセスしうる各人員に一意の ID 番号を割り当てるものとします。

2.1.6.2 サプライヤーは、許可目的上の「知る必要（Need To Know）」を有する者以外には Amazon 情報へのアクセスを許可しないものとします。

2.1.6.3 サプライヤーは Amazon 情報にアクセスしうる人員およびサービスのリストを定期的に見直し、Amazon 情報システムへのアクセスが不要となったアカウントを削除するものとします。この見直しは 90 日に 1 回またはそれ以上の頻度で実施する必要があります。

2.1.6.4 サプライヤーは、Amazon 情報システムで、メーカーが提供する既定のシステムパスワードおよびその他のセキュリティパラメーターを使用しないものとします。サプライヤーは、NIST SP 800-63B に記載された最良慣行に従って、全ての Amazon 情報システムで「強いパスワード」の使用をシステム的に強制するように設定を行うものとします。サプライヤーは全てのパスワードおよびアクセス認証情報について秘密保持を義務付け、かつ人員相互間での共有を禁止するものとします。

2.1.6.5 サプライヤーは、あるアカウントで不正なパスワードによるログイン試行が連続 10 回を超えた場合に当該アカウントによる Amazon 情報または Amazon 情報システムへのアクセスを禁止する「アカウントロックアウト」を実施および強制適用するものとします。

2.1.6.6 サプライヤーは、Amazon が書面で明示的に許可した場合を除くほか、Amazon 情報をサプライヤーの情報および第三者の情報から物理的または論理的に常時（保存、処理、転送の実施時を含みます）隔離するものとします。

2.1.6.7 Amazon が物理的なアクセス制御措置を追加するようサプライヤーに書面で要求した場合、サプライヤーはそれらの物理的アクセス制御措置を導入して使用するものとします。

2.1.6.8 サプライヤーは、Amazon が正当に要求した場合、次の (a) および (b) を Amazon に提出するものとします。(a) 許可目的を用途として Amazon がサプライヤーに提供したアカウントまたは認証情報の全使用状況（許可の有無は問いません）に関するログデータ。(b) Amazon 情報へのアクセス権を有する Amazon の人員またはサプライヤーの人員になりすます行為が行われた場合（未遂の場合を含みます）は当該行為に関する詳細なログデータ。

2.1.6.9 サプライヤーは悪意のある行為または不正なアクセスが行われた形跡がないかどうかにつきアクセスログを定期的に確認するものとします。

2.1.7 サプライヤーの規約 サプライヤーは、従業員、下請業者、代理店および供給業者を対象として、本セキュリティ規約に定める基準と一致する情報およびネットワークセキュリティ規約（規約の違反を発見して記録する手続きを含むものとします）を制定して実施するものとします。サプライヤーの情報およびネットワークセキュリティ規約に対する違反が発生し、それがセキュリティインシデント（以下で定義します）に該当する恐れがあるとの疑義をサプライヤーまたは Amazon のいずれかが正当に抱いた場合、サプライヤーは Amazon の要求に応じて当該違反に関する情報を Amazon に提供するものとします。

2.1.8 外部委託 サプライヤーは、Amazon から事前に書面で承諾を得ることなく、本セキュリティ規約上の自己の義務を下請業者または代理人（「**下請人**」と総称します）に委託または委任しないものとします。委託または委任が行われている場合であっても、その条件にかかわらず、サプライヤーは引き続き本セキュリティ規約上の自己の義務を完全に履行する責任を負うものとします。本セキュリティ規約の規定の拘束力はサプライヤーの下請人および人員にも及ぶものとします。サプライヤーは、(a) 自己の下請人および人員に本セキュリティ規約を遵守させるものとし、かつ (b) サプライヤーの下請人および人員の全ての行為、不作為、過失および不正について責任を負うものとします。

2.1.9 リモートアクセス サプライヤーは Amazon 情報システムにアクセスする者に多要素認証を義務付けるものとします（例えばユーザー認証に 2 つ以上の別個の要素を義務付けるなど）。

2.1.10 大量アクセス 本項において「大量アクセス」とは、データベースクエリ、レポート生成またはその他の大量データ移転手段によりデータにアクセスすることをいいます。サプライヤーは、Amazon が書面で明示的に許可した場合を除くほか、Amazon 情報への大量アクセスを行わず、かつ他者にも大量アクセスを許可しないものとします。この場合、Amazon 情報がサプライヤーもしくは Amazon が管理するデータベース上にあるか、またはファイルベースのアーカイブ（例えばフラットファイル）への保存などその他の形で保存されているかは問いません。具体的には、許可目的により個別の記録へのアクセスが必要となる場合以外における Amazon 情報へのアクセスは本項により禁止されます。サプライヤーは Amazon 情報への大量アクセス（成功しなかった試行を含みます）に関する詳細なログデータを保持するとともに、第 2.5 項（セキュリティレビュー）に基づくサプライヤーの義務の一部として、そのログから作成したレポートを提出するものとします。Amazon が、Amazon 情報への大量アクセスをサプライヤーに書面で許可した場合、サプライヤーは (a)「知る必要」を有する指定従業員以外の者

には当該アクセスを行わせないものとし、かつ (b) アクセスを制限するツールを使用し、明示的な認証および全てのアクセスの記録を義務付けるものとします。

2.1.11 サプライヤーの人員　Amazon は、サプライヤーの人員が Amazon 情報にアクセスする条件として、Amazon が指定する様式の非開示契約を個別に締結して Amazon に交付することをそれらの人員に要求することができます。サプライヤーの人員は、Amazon からの要求があった場合、個別に非開示契約を締結するものとします。サプライヤーは（サプライヤーの人員にアクセス権を付与する前または情報を提供する前に）、Amazon 情報へのアクセス権を有するサプライヤーの人員が個別に署名した非開示契約を取りまとめて Amazon に交付するものとします。また、サプライヤーは、Amazon 情報システム上で Amazon 情報にアクセスした人員または Amazon 情報を受領した人員全員のリストを作成し、Amazon からの要求があった場合はそのリストを速やかに提出するものとします。サプライヤーは、(a) Amazon 情報へのアクセスが不要となったサプライヤーの人員、または (b) サプライヤーの人員としての資格を喪失した者（例えばサプライヤーによる雇用を離れる者）について、Amazon 情報および Amazon 情報システムへのアクセス権を直ちに（最長で 24 時間以内に）停止するものとします。サプライヤーは、それらの人員に Amazon 情報システム上での Amazon 情報へのアクセスを許可する場合も、24 時間以内に Amazon に通知するものとします。

2.2 Amazon のエクストラネットおよびサプライヤーのポータルへのアクセス　Amazon は、ウェブポータルもしくはその他の非公開ウェブサイト経由、または Amazon もしくは第三者のウェブサイトもしくはシステム上のエクストラネットサービス（各々を「**エクストラネット**」といいます）経由で、許可目的により Amazon 情報にアクセスする権限をサプライヤーに付与することができます。Amazon がエクストラネットを使用して Amazon 情報にアクセスすることをサプライヤーに許可する場合、サプライヤーは次の要件を遵守する必要があります。

2.2.1 許可目的　サプライヤーおよびサプライヤーの人員は、許可目的以外の目的ではエクストラネットにアクセスしないものとし、かつ、許可目的以外の目的では Amazon 情報に係るアクセス、使用、表示、検索、ダウンロードまたは保存をエクストラネットから行わないものとします。

2.2.2 アカウント　サプライヤーは、Amazon が各個人に指定したエクストラネットアカウント以外のアカウントを使用しないようにサプライヤーの人員に指示するとともに、アクセス認証情報の秘密保持を行うことをサプライヤーの人員に義務付けるものとします。

2.2.3 システム　サプライヤーがエクストラネットにアクセスする場合は、サプライヤーが管理するオペレーティングシステムを実行している計算システムや処理システムまたはアプリケーションを必ず経由してアクセスするものとし、かつ、そのシステムには次の (a) から (d) までを全て含むものとします。(a) 第 2.1.1 項（ネットワークセキュリティ）に準ずるシステム・ネットワーク・ファイアーウォール。(b) 第 2.1.2 項（アップデート）に準ずる集中的なパッチ管理。(c) オペレーティングシステムに適したマルウェア対策ソフトウェアであって第 2.1.3 項（マルウェア対策）に準ずるもの。(d) 携帯デバイスについての完全なディスク暗号化。

2.2.4 制限　サプライヤーは、Amazon が事前に書面で許可した場合を除くほか、Amazon 情報についてエクストラネットから何らかの媒体（機械、デバイス、サーバーを含みます）へのダウンロード、ミラーリングまたは永久的な保存を行わないものとします。

2.2.5 アカウントの停止　サプライヤーは、エクストラネットへのアクセスを許可したサプライヤーの人員であって次の (a) または (b) に該当する人員について、アカウントの停止および Amazon への通知（24 時間以内）を行うものとします。(a) Amazon 情報へのアクセスが不要となった人員。(b) サプライヤーの人員としての資格を喪失した者（例えばサプライヤーによる雇用を離れる者）。

2.2.6 第三者のシステム

2.2.6.1　サプライヤーが、第三者のシステムを使用して Amazon 情報を保存しようとする場合、または第三者のシステムを使用してその他の形で Amazon 情報にアクセスしようとする場合は、事前に Amazon に通知した上で Amazon から事前に書面で承認を得るものとします。ただし、次の (a) かつ (b) に該当するときはその限りでありません。(a) データが本セキュリティ規約に従って暗号化されている。(b) 当該第三者のシステムが暗号化キーまたは暗号化されていない「プレーンテキスト形式」のデータにアクセスできない。

Amazon は、当該第三者のシステムを承認する前に、第 2.5 項（セキュリティレビュー）に準じた Amazon セキュリティレビューを要求する権利を有します。

2.2.6.2 サプライヤーが、第三者のシステムを使用して暗号化されていない Amazon 情報を保存しようとする場合、または第三者のシステムを使用してその他の形で暗号化されていない Amazon 情報にアクセスしようとする場合は、当該第三者のシステムおよび当該第三者のシステム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するものとし、かつ、当該第三者のシステムのセキュリティ制御について、Amazon が要求する様式（例えば米国監査基準書（SAS）第 70 号もしくはその後継である報告書、または一般に認められた業界標準的なその他の報告書であって Amazon が承認したもの）により Amazon に対して定期的な報告を行うものとします。

2.3 データの保管および破棄

2.3.1 保管 サプライヤーは、許可目的のために行う場合に限り、かつ許可目的のために保管が必要な期間に限り、Amazon 情報の保管を行うものとします。

2.3.2 返却または削除 サプライヤーは、Amazon 情報について Amazon から返却または削除の要求があった場合、当該要求の通知に従って、全ての Amazon 情報を直ちに（ただし 72 時間以内に）Amazon に返却または削除するものとします。また、サプライヤーは、許可目的が完了した時点または本セキュリティ規約の解除もしくは満了時点のうち早い方の時点から 30 日以内に、Amazon 情報の全てのライブインスタンス（オンラインまたはネットワークでアクセス可能なもの）を永久的かつ安全な形で削除するものとします。サプライヤーは、Amazon から要求があった場合、全ての Amazon 情報を破棄した旨の証明書を Amazon に提出するものとします。なお、第 2.3.3 項の保存用コピーには本項を適用しません。

2.3.3 保存用コピー サプライヤーが、税務または同様の規制により、Amazon 情報の保存用コピーを保管する法律上の義務を負っている場合、当該 Amazon 情報の保管は次の方法のうちいずれか一つにより行う必要があります。

2.3.3.1 コールドバックアップまたはオフラインバックアップ（つまり即時使用または双方向的使用を行えないもの）として物理的に安全な施設に保存する。

2.3.3.2 暗号化ファイルをホスティングまたは保存するシステムが暗号化キーのコピーにアクセスできない場合は暗号化して保存する。

2.3.4 復元 サプライヤーが災害復旧の目的で復元（つまりバックアップへの復帰）を実行する場合、サプライヤーは、関係契約もしくは本セキュリティ規約または Amazon とのその他の契約により削除する必要がある全ての Amazon 情報を、復元の実行から 24 時間以内に、第 2.3 項に従って再削除または上書きするプロセスを策定して実施するものとします。サプライヤーが何らかの目的で復元を実行する場合、Amazon から事前に書面で承諾を得ることなく、Amazon 情報を第三者のシステム上またはネットワーク内に回復することはできません。Amazon は、当該第三者のシステムまたはネットワークへの Amazon 情報の回復を許可する前に、第 2.5 項（セキュリティレビュー）に準じた第三者のシステムまたはネットワークの Amazon セキュリティレビューを要求する権利を有します。

2.3.5 データ無害化（サニタイズ）の基準 サプライヤーが Amazon 情報を削除する場合は、該当デバイス上のデータの抹消に関して、NIST SP 800-88 Revision 1、Guidelines for Media Sanitation（2014 年 12 月 18 日）（http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf で入手可能）の別紙 A に記載された無害化の最小推奨事項に従って全て削除するものとします。該当の指針が NIST SP 800-88 の別紙 A に記載されていない場合、Amazon 情報を格納するデバイスは次の (a) から (c) のいずれか一つの方法により破壊するものとします。(a) 1 万ガウス以上の電磁束場で磁気メディアを消磁する。(b) 2 mm×2 mm 未満の細片となるように粉砕または機械的に分解する。(c) Amazon 情報の種別および機微性を基準として Amazon が要求するその他の基準に従って破棄する。

2.4 フォレンジック調査を不可能とする破壊 サプライヤーは、何らかのハードウェア、ソフトウェアまたはその他のメディアであって Amazon 情報を格納しているものまたはいずれかの時点で Amazon 情報を格納していたものを処分する前に、どのような形式によっても Amazon 情報を復旧できないように、当該ハードウェア、ソフトウェアまたはその他のメディア

をフォレンジック調査が不可能となるまで完全に破壊するものとします。サプライヤーは、該当デバイスの破壊に関して、NIST SP 800-88 別紙 A に記載された無害化の最小推奨事項に従って、フォレンジック調査不可能な破壊を実施するものとします。

2.4.1 サプライヤーは、本第 2.4 項により義務付けられているフォレンジック調査不可能な破壊をまだ実施していない、Amazon 情報を格納しているハードウェア、ソフトウェアまたはその他のメディアについて、売却、再販売、寄付、修理再生またはその他の移転（それらのハードウェア、ソフトウェアその他メディアの販売もしくは譲渡、サプライヤーの事業の清算に関連する処分またはその他何らかの処分を含みます）を行わないものとします。

2.5 セキュリティレビュー

2.5.1 Amazon はサプライヤーに対して Amazon リスク評価への参加を定期的に要求する権利を有します。

2.5.2 証明書 サプライヤーは、Amazon から書面で要求があった場合、リスク評価の一環として提出した情報が、サプライヤーと Amazon とが最も直近に合意した本セキュリティ規約に準拠していることを証明する証明書を Amazon に提出するものとします。Amazon が第 1.1 項に従って本セキュリティ規約の改定を行った場合、本項に関しては、サプライヤーと Amazon とが合意（電子メールによる合意で足りるものとします）に達するまで当該変更は効力を生じないものとします。

2.5.3 その他のレビュー Amazon は Amazon 情報システムのセキュリティについて定期的なレビューを実施する権利を有しますが、次の (a) または (b) の場合を除くほか、当該要求は 1 年につき 1 回を限度とします。(a) 過去 1 年（暦年）以内に重大な問題が発生したことが発見された場合。(b) Amazon が政府機関またはその他の規制機関からそのようなレビューの実施を義務付けられている場合。サプライヤーは、要求された全ての情報を、相当の期間内（ただし、Amazon による要求があった日から暦日 20 日を超えない期間とします）に Amazon に提出するものとします。

2.5.4 問題の解消 セキュリティレビューにより何らかの問題が発見された場合、サプライヤーは、費用および経費を全面的に負担して、双方が合意した期間内に当該問題を解消するために必要な相当の措置を全て講じるものとします。

2.6 セキュリティインシデント

2.6.1 Amazon 情報に係る不正なアクセス、収集、取得、使用、転送、開示、毀損もしくは消失、または Amazon 情報システムの侵害（「**セキュリティインシデント**」）が実際に発生したこと、または発生した疑いがあることをサプライヤーが把握した場合は、可能な限り速やかに（ただし、遅くとも 24 時間以内に）Amazon に通知するものとします。サプライヤーは各セキュリティインシデントを適時に是正した上で、サプライヤー社内で実施した各セキュリティインシデントの調査について詳細を記載した書面を Amazon に提出するものとします。サプライヤーは、適用法令上許可されている場合に限り、Amazon に代わって規制機関または顧客に通知することを行いません。ただし、Amazon がサプライヤーに対して、そのような通知を行うように書面で個別に要求した場合はその限りでなく、Amazon はサプライヤーが当該通知を発する前にその形式および内容を確認する権利を有します。サプライヤーは Amazon に協力し、発生が確認されたセキュリティインシデントを是正する計画を Amazon と共同で策定および実行するものとします。

2.6.2 サプライヤーが政府機関からの請求または命令（召喚状、裁判所の命令、捜索令状など）により Amazon 情報を含むデータの提出を要請された場合、サプライヤーは、適用法令上許可されている範囲で、Amazon が秘密保持命令またはその他の適切な救済手段を要求するために十分な通知を Amazon に交付するものとします。

2.7 一般条項 Amazon は本セキュリティ規約に基づく全ての決定を任意に行う裁量権を有します。「を含みます」の前または「例えば」の後に挙げた項目は例示にすぎず、全ての項目を漏れなく列挙したものではありません。本セキュリティ規約でセキュリティ要件の基準に言及している箇所は、Amazon が別段に定めた場合を除くほか、具体的な基準およびその後継版または同等版（基準の改定が行われた場合は改定後のもの）に言及しているものとします。