Snowflake セキュリティ追補条項
Snowflake Security Addendum

更新日：2022 年 5 月 6 日
LAST UPDATED: MAY 6, 2022

本セキュリティ追補条項[1]は、この書面を参照する Snowflake とお客様との間の契約書（以下「基本契約」といいます）に援用され、その一部となります。本追補条項で用いられている大文字で始まる定義のない用語は、基本契約と同じ意味を有します。基本契約の条件と本追補条項との間に不一致がある場合には、本追補条項が優先します。本追補条項の言語は、英語及び日本語です。英語と日本語の間に齟齬がある場合は、日本語の文章が優先されます。
This Security Addendum [1] is incorporated into and made a part of the written agreement between Snowflake and Customer that references this document (the "**Agreement**") and any capitalized terms used but not defined herein shall have the meaning set forth in the Agreement. In the event of any conflict between the terms of the Agreement and this Security Addendum, this Security Addendum shall govern. The language of this Security Addendum is English and Japanese. In the event of a conflict between the English and Japanese text, the Japanese text shall govern.

Snowflake は、基本契約、ドキュメンテーション又はその双方に記載する IaaS クラウドプロバイダー（以下「クラウドプロバイダー」といいます）を利用し、当該クラウドプロバイダーがホスティングする VPC/VNET 及びストレージ（以下「クラウド環境」といいます）を使用するお客様に本サービスを提供します。
Snowflake utilizes infrastructure-as-a-service cloud providers as further described in the Agreement and/or Documentation (each, a "**Cloud Provider**") and provides the Service to Customer using a VPC/VNET and storage hosted by the applicable Cloud Provider (the "**Cloud Environment**").

Snowflake は、NIST 800-53（又は業界で確立されたその後継フレームワーク）に基づき、文書化された包括的なセキュリティプログラムを整備し、これに基づき、本サービス及び顧客データの秘密性、完全性、可用性及びセキュリティ保護のために設計される、以下をはじめとする物理的及び技術的な安全対策並びに管理運用上の安全対策（以下「セキュリティプログラム」といいます）を実施します。Snowflake は定期的にセキュリティプログラムのテスト及び評価を行った上で、セキュリティプログラム及び本セキュリティ追補条項を見直し、改訂します。ただし、改訂はセキュリティプログラムの質の向上を目的とするものであり、実質的に低下させるものではありません。
Snowflake maintains a comprehensive documented security program based on NIST 800-53 (or industry recognized successor framework), under which Snowflake implements and maintains physical, administrative, and technical safeguards designed to protect the confidentiality, integrity, availability, and security of the Service and Customer Data (the "**Security Program**"), including, but not limited to, as set forth below. Snowflake regularly tests and evaluates its Security Program, and may review and update its Security Program as well as this Security Addendum, provided, however, that such updates shall be designed to enhance and not materially diminish the Security Program.

1. Snowflake の監査及び認証
1. Snowflake's Audits & Certifications

1.1 本サービスを提供するために使用される情報セキュリティ管理システムは、年に 1 回以上、次の監査及び認証に記載されているとおり、独立した第三者監査人による審査（以下「第三者監査」といいます）を受けます。

[1] 明確性を期すために付言すると、お客様の基本契約において「セキュリティ方針」という用語が用いられている場合には、この別紙のことを意味するものとします。For clarity, where Customer's Agreement refers to the defined term "Security Policy", such reference shall be interpreted to refer to this exhibit.

The information security management system used to provide the Service shall be assessed by independent third-party auditors as described in the following audits and certifications ("**Third-Party Audits**"), on at least an annual basis:

- ISO27001
  ISO27001
- SOC 2 タイプ II
  SOC 2 Type II
- SOC 1 タイプ II
  SOC 1 Type II
- Snowflake の Business Critical Edition 及び Virtual Private Snowflake Edition のみに関しては、以下の認証：
  For Snowflake's Business Critical Edition and Virtual Private Snowflake Edition only:
  - PCI-DSS サービスプロバイダーレベル 1 認証
    PCI-DSS Service Provider Level 1 Certification
  - 米国の一部地域では FedRAMP Moderate Authorized（ドキュメンテーションにて記載されているとおりとします）
    FedRAMP Moderate Authorized in certain U.S. Regions (as described in the Documentation)
  - HITRUST CSF 証明書（AWS 又は Microsoft がクラウドプロバイダーの場合）
    HITRUST CSF Certification (where AWS or Microsoft are the Cloud Provider)
  - オーストラリアの一部地域では IRAP プロテクティッドレベル（ドキュメンテーションにて記載されているとおりとします）
    IRAP at the Protected Level in certain Australian Regions (as described in the Documentation)
  - HIPAA 業務委託先コンプライアンスレポート（Google がクラウドプロバイダーの場合）
    HIPAA Compliance Report for Business Associates (where Google is the Cloud Provider)

1.2 第三者監査は、第 9.2.1 条に従い、お客様の閲覧に供されます。
Third-Party Audits are made available to Customer as described in Section 9.2.1.

1.3 Snowflake は、第三者監査を中止することを決定した場合には、業界で確立されたこれと同等のフレームワークを採用することとします。
To the extent Snowflake decides to discontinue a Third-Party Audit, Snowflake will adopt or maintain an equivalent, industry-recognized framework.

1.4 FedRAMP、IRAP、PCI-DSS に関し、お客様が責任を負う Snowflake が特定したコントロールに関連する情報は、お客様からの書面による要請により入手可能です。お客様は、前述のいずれかに基づく責任について、独立した評価を行う責任を負うものとします。
Information related to Snowflake-identified controls for which Customer is responsible in connection with FedRAMP, IRAP, and PCI-DSS is available upon written request by Customer. Customer is responsible for performing an independent assessment of its responsibilities under any of the foregoing.

2. 顧客データのホスティング地域
2. Hosting Location of Customer Data

2.1 ホスティング地域　顧客データのホスティング地域は、Snowflake が提示しお客様が注文申込書で選択するか又は本サービスを通じて設定した地域における本稼働クラウド環境とします。
Hosting Location. The hosting location of Customer Data is the production Cloud Environment in the Region offered by Snowflake and selected by Customer on an Order Form or as Customer otherwise configures via the services.

3. 暗号化
3. Encryption

3.1 顧客データの暗号化　Snowflake は、AES 256 方式又はこれより高水準の暗号化方式を用いて顧客データの保存データ（data at rest）を暗号化します。信頼性の低いネットワーク上での顧客データ送信には、トランスポートレイヤセキュリティ（TLS）1.2 又はこれより高水準の方式を使用します。

Encryption of Customer Data. Snowflake encrypts Customer Data at-rest using AES 256-bit (or better) encryption. Snowflake uses Transport Layer Security (TLS) 1.2 (or better) for Customer Data in-transit over untrusted networks

3.2 暗号化キーの管理　Snowflake の暗号化キー管理は NIST 800-53 に準拠したものとし、暗号化キーは定期的にローテーションされます。ハードウェアのセキュリティモジュールが、トップレベルの暗号化キーの保護に用いられます。Snowflake は、暗号化キーと顧客データを論理上分離します。

Encryption Key Management. Snowflake's encryption key management conforms to NIST 800-53 and involves regular rotation of encryption keys. Hardware security modules are used to safeguard top-level encryption keys. Snowflake logically separates encryption keys from Customer Data.

4. システム及びネットワークのセキュリティ

4. System & Network Security

4.1 アクセス面でのセキュリティ対策（Control）Access Controls.

4.1.1 Snowflake の担当者によるクラウド環境へのアクセスは、必ず固有ユーザーID を用いて最小権限の原則（principle of least privilege）に従って行い、アクセスの際には必ず VPN 接続を使い、多要素認証方式と、少なくとも PCI-DSS に定める長さ及び複雑性の要件を充たしたパスワードを利用します。

All Snowflake personnel access to the Cloud Environment is via a unique user ID, consistent with the principle of least privilege, requires a VPN, as well as multi-factor authentication and passwords meeting or exceeding PCI-DSS length and complexity requirements.

4.1.2 Snowflake の担当者は、以下の場合を除き、顧客データにアクセスしません。(i) 基本契約に基づくサービスを提供するために合理的に必要な場合、又は (ii) 法律又は政府機関の拘束力のある命令を遵守する場合。

Snowflake personnel will not access Customer Data except (i) as reasonably necessary to provide Snowflake Offerings[2] under the Agreement or (ii) to comply with the law or a binding order of a governmental body.

4.2 エンドポイントでのセキュリティ対策　クラウド環境へのアクセスのため、Snowflake 従業員は社内支給のノートパソコンを利用します。このノートパソコンには、次のようなセキュリティ対策が施されています（これらに限られません）。(i) ディスクの暗号化、(ii) 疑わしいアクティビティや悪質なコード（以下に定義する）をモニターし、警告を発するエンドポイント検出・対応（EDR）ツール、及び(iii) 第 4.7.3 条（脆弱性対策）に従った脆弱性対策。

Endpoint Controls. For access to the Cloud Environment, Snowflake personnel use Snowflake-issued laptops which utilize security controls that include, but are not limited to, (i) disk encryption, (ii) endpoint detection and response (EDR) tools to monitor and alert for suspicious activities and Malicious Code (as defined below), and (iii) vulnerability management in accordance with Section 4.7.3 (Vulnerability Management).

4.3 環境の分離　Snowflake は、生産環境と開発環境とを論理上分離します。クラウド環境は、Snowflake の法人オフィス及びネットワークと理論上も物理的にも分離されます。

[2] Snowflake Offering(s)が基本契約で定義されていない場合、「Snowflake Offering(s)」とは、Snowflake が提供するサービス、テクニカルサービス（いかなる提供物を含む）、サポート及びその他の付帯するサービス（サービス又は技術的な問題を防止又は対処するサービスを含むが、これらに限定されない）を意味するものとします。If Snowflake Offering(s) is not defined in the Agreement, "Snowflake Offering(s)" means the Service, Technical Services (including any Deliverables), and any support and other ancillary services (including, without limitation, services to prevent or address service or technical problems) provided by Snowflake.

Separation of Environments. Snowflake logically separates production environments from development environments. The Cloud Environment is both logically and physically separate from Snowflake's corporate offices and networks.

4.4 ファイアウォール／セキュリティグループ　Snowflake は、業界水準のファイアウォール又はセキュリティグループのテクノロジーを利用してクラウド環境を保護します。この際には、業務に必要な範囲以上のネットワーク内トラフィック・プロトコルの送受信を防ぐため、「Deny-all」のデフォルトポリシーが適用されます。

Firewalls / Security Groups. Snowflake shall protect the Cloud Environment using industry standard firewall or security groups technology with deny-all default policies to prevent egress and ingress network traffic protocols other than those that are business-required.

4.5 ハードニング　クラウド環境は、脆弱性からの保護のため、業界水準の方法を利用してハードニングが施されます。これには、デフォルトのパスワードの変更、不必要なソフトウェアの削除、不必要なサービスの無効化又は削除、さらに、本セキュリティ追補条項に定める定期的なパッチ適用などが含まれます。

Hardening. The Cloud Environment shall be hardened using industry-standard practices to protect it from vulnerabilities, including by changing default passwords, removing unnecessary software, disabling or removing unnecessary services, and regular patching as described in this Security Addendum.

4.6 モニタリング及びログ作成 Monitoring & Logging

4.6.1 インフラストラクチャー・ログ　ホストベースの侵入検知ツールをはじめとするモニタリングツールやサービスを利用して、クラウド環境内の一定のアクティビティと変化を示すログを作成します。このログはさらに、異変がないかを確認するためにモニター及び分析がなされ、変造防止対策が施された安全な方法によって 1 年以上保存されます。

Infrastructure Logs. Monitoring tools or services, such as host-based intrusion detection tools, are utilized to log certain activities and changes within the Cloud Environment. These logs are further monitored, analyzed for anomalies, and are securely stored to prevent tampering for at least one year.

4.6.2 ユーザー・ログ　ドキュメンテーションにてさらに詳細に説明する通り、Snowflake は、アカウント内の一定のアクティビティと変化を示すログも把握し、お客様の保存及び分析用に提供します。

User Logs. As further described in the Documentation, Snowflake also captures logs of certain activities and changes within the Account and makes those logs available to Customer for Customer's preservation and analysis.

4.7 脆弱性の検知及び対策 Vulnerability Detection & Management

4.7.1 ウィルス対策及び脆弱性検知　クラウド環境では、高度な脅威検知ツールを利用します。このツールは、シグネチャの更新が毎日行われ、疑わしいアクティビティ、潜在的なマルウェア、ウィルス、悪質なコンピュータコード又はそれらの一部若しくは全部のモニタリング及び警告（以下「悪質なコード」と総称します）に利用されます。Snowflake は、顧客データに悪質なコードが含まれていないか調べるためのモニタリングは行いません。

Anti-Virus & Vulnerability Detection. The Cloud Environment leverages advanced threat detection tools with daily signature updates, which are used to monitor and alert for suspicious activities, potential malware, viruses and/or malicious computer code (collectively, "**Malicious Code**"). Snowflake does not monitor Customer Data for Malicious Code.

4.7.2 侵入テスト及び脆弱性検知　Snowflake は、年間を通じて侵入テストを定期的に行います。また、1 年に 1 回以上、外部第三者に依頼して本サービスの侵入テストを行います。Snowflake は、更新された脆弱性データベースを利用して、クラウド環境の脆弱性スキャンを毎週行います。

Penetration Testing & Vulnerability Detection. Snowflake regularly conducts penetration tests throughout the year and engages one or more independent third parties to conduct penetration tests of the Service at least annually. Snowflake also runs weekly vulnerability scans for the Cloud Environment using updated vulnerability databases.

4.7.3 脆弱性対策　定義されたリスク基準に該当する脆弱性が発生すると、警告が発せられ、本サービスに及ぼす影響の程度に応じて対応策の優先度が決定されます。Snowflake がこのような脆弱性を認識した場合には、民間機関及び公的機関（米コンピュータ緊急事態対策チーム（US-CERT）等）の基準で「非常に危険（critical）」「高度（high）」に該当するものについては 30 日以内に、「中程度（medium）」に該当するものについては 90 日以内に対処するよう商業的に合理的な努力を払います。脆弱性が「非常に危険」「高度」又は「中程度」のいずれに該当するかを決定するため、Snowflake はアメリカ国立標準技術研究所の脆弱性情報データベース（NVD）の共通脆弱性評価システム（CVSS）、また該当する場合には US-CERT の格付を利用します。

Vulnerability Management. Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on their potential impact to the Service. Upon becoming aware of such vulnerabilities, Snowflake will use commercially reasonable efforts to address private and public (e.g., U.S.-Cert announced) critical and high vulnerabilities within 30 days, and medium vulnerabilities within 90 days. To assess whether a vulnerability is 'critical', 'high', or 'medium', Snowflake leverages the National Vulnerability Database's (NVD) Common Vulnerability Scoring System (CVSS), or where applicable, the U.S.-Cert rating.

5. 管理運用上のセキュリティ対策

5. Administrative Controls

5.1 人事面でのセキュリティ対策　Snowflake は、人事採用の際に、法令上許容される範囲内で従業員の前科調査を義務付けています。

Personnel Security. Snowflake requires criminal background screening on its personnel as part of its hiring process, to the extent permitted by applicable law.

5.2 社員研修　Snowflake は、新人研修及び継続研修など、従業員向けの書面化されたセキュリティ意識向上・研修プログラムを整備します。

Personnel Training. Snowflake maintains a documented security awareness and training program for its personnel, including, but not limited to, onboarding and on-going training.

5.3 従業員による合意書差し入れ　Snowflake 従業員は、秘密保持合意書への署名が義務付けられます。また、Snowflake 情報セキュリティ方針への署名も求められ、これには従業員が顧客データ関連セキュリティインシデントの報告責任を負うことを了解する旨の規定が含まれています。

Personnel Agreements. Snowflake personnel are required to sign confidentiality agreements. Snowflake personnel are also required to sign Snowflake's information security policy, which includes acknowledging responsibility for reporting security incidents involving Customer Data.

5.4 従業員のアクセス権限の見直し及び退職時の取扱い　Snowflake は、四半期に 1 度以上、従業員のクラウド環境へのアクセス権限を見直し、退職した従業員のアクセス権限は速やかに取り消します。

Personnel Access Reviews & Separation. Snowflake reviews the access privileges of its personnel to the Cloud Environment at least quarterly, and removes access on a timely basis for all separated personnel.

5.5 Snowflake のリスクマネジメント及び脅威評価　Snowflake のリスクマネジメントのプロセスは、NIST 800-53 及び ISO 27001 に準拠しています。Snowflake のセキュリティ委員会は、脅威環境のレポート及び重大な変化について検討し、セキュリティ対策の潜在的欠陥を把握するために定期的にミーティングを行い、セキュリティ対策及び脅威対処戦略の新規導入又は強化に関する提案を行います。

Snowflake Risk Management & Threat Assessment. Snowflake's risk management process is modeled on NIST 800-53 and ISO 27001. Snowflake's security committee meets regularly to review reports and material changes in the threat environment, and to identify potential control deficiencies in order to make recommendations for new or improved controls and threat mitigation strategies.

5.6 外部機関の脅威情報のモニタリング　Snowflake は、US-CERT の脆弱性情報その他の信頼できるソースの脆弱性報告など、外部機関の脅威情報を検討します。US-CERTにより公開された、

「非常に危険」又は「高度」と評価された脆弱性については、第 4.7.3 条（脆弱性対策）に従って優先的な是正措置を講じます。

External Threat Intelligence Monitoring. Snowflake reviews external threat intelligence, including US-Cert vulnerability announcements and other trusted sources of vulnerability reports. U.S.-Cert announced vulnerabilities rated as critical or high are prioritized for remediation in accordance with Section 4.7.3 (Vulnerability Management).

5.7 変更の管理　Snowflake は、本サービスに関する変更管理プログラムを文書で整備します。

Change Management. Snowflake maintains a documented change management program for the Service

5.8 委託先リスクマネジメント　Snowflake は、顧客データ処理を依頼した業務委託先が本セキュリティ追補条項に定める Snowflake の義務に沿ったセキュリティ対策を講じるよう確保するため、業務委託先用のリスクマネジメントプログラムを整備します。

Vendor Risk Management. Snowflake maintains a vendor risk management program for vendors that process Customer Data designed to ensure each vendor maintains security measures consistent with Snowflake's obligations in this Security Addendum.

6. 物理的及び環境面でのセキュリティ対策

6. Physical & Environmental Controls

6.1 クラウド環境のデータセンター　クラウド環境をホスティングするデータセンターに関して、クラウドプロバイダーが物理的及び環境面での適切なセキュリティ対策を講じるよう確保するため、Snowflake は、そのクラウドプロバイダーの第三者審査及び認証を受けたセキュリティ対策を、定期的に審査します。各クラウドプロバイダーは、SOC 2 タイプ II 年間審査及び ISO 27001 認証を受けているか、またはそれに相当する業界基準を充たしたものでなければなりません。これらのセキュリティ対策には、以下のようなものが含まれます（これらに限られません）。

Cloud Environment Data Centers. To ensure the Cloud Provider has appropriate physical and environmental controls for its data centers hosting the Cloud Environment, Snowflake regularly reviews those controls as audited under the Cloud Provider's third-party audits and certifications. Each Cloud Provider shall have a SOC 2 Type II annual audit and ISO 27001 certification, or industry recognized equivalent frameworks. Such controls, shall include, but are not limited to, the following:

6.1.1 施設への立ち入りは建物の入口で規制する。
Physical access to the facilities are controlled at building ingress points;

6.1.2 訪問者には、ID の提示と入館記録への署名を求める。
Visitors are required to present ID and are signed in;

6.1.3 サーバーへの物理的アクセスを、アクセス制御装置により規制する。
Physical access to servers is managed by access control devices;

6.1.4 物理的アクセスの権限を定期的に見直す。
Physical access privileges are reviewed regularly

6.1.5 施設ではモニタリング・警告システムを利用する。
Facilities utilize monitor and alarm response procedures;

6.1.6 CCTV を利用する。
Use of CCTV;

6.1.7 火災検知及び防止システム
Fire detection and protection systems;

6.1.8 電源バックアップ及び冗長性システム
Power back-up and redundancy systems; and

6.1.9 空調システム
Climate control systems.

6.2 Snowflake 法人オフィス　Snowflake の法人オフィスでは顧客データのホスティングは行いませんが、Snowflake の法人オフィスにおける ISO 27001 に準拠した物理的、技術的及び管理運用上のセキュリティ対策には以下のものが含まれるものとします（これらに限られません）。

Snowflake Corporate Offices. While Customer Data is not hosted at Snowflake's corporate offices, Snowflake's technical, administrative, and physical controls for its corporate offices covered by its ISO 27001 certification, shall include, but are not limited to, the following:

6.2.1 法人オフィスへの立入りはオフィスの入口で規制する。
Physical access to the corporate office is controlled at office ingress points;

6.2.2 スタッフ全員に入館証を携行させ、入館証の有効性を定期的に見直す。
Badge access is required for all personnel and badge privileges are reviewed regularly;

6.2.3 訪問者には入館記録への署名を求める。
Visitors are required to sign in;

6.2.4 建物の入口には CCTV を設置する。
Use of CCTV at building ingress points;

6.2.5 Snowflake 社内支給のノートパソコン及びネットワーク設備のタグ付け及び管理リスト作成。
Tagging and inventory of Snowflake-issued laptops and network assets;

6.2.6 火災検知及び防止システム
Fire detection and sprinkler systems; and

6.2.7 空調システム
Climate control systems.

7. インシデントの検出及び対応
7. Incident Detection & Response

7.1 セキュリティインシデント報告　Snowflake は、顧客データの事故又は違法行為による破壊、紛失、改変若しくは無断開示又はアクセスの原因となるセキュリティ違反（以下「セキュリティインシデント」といいます）を把握した場合には、お客様に不当な遅延なく（可能であればその発生を知ったときから 72 時間以内に）連絡するものとします[3]。適時な通知を行うために、お客様は、このような通知のために本サービスに最新の電子メールを登録し、維持する必要があります。このような電子メールが登録されていない場合、お客様は、通知の手段は Snowflake の合理的な裁量によるものとし、Snowflake の適時通知能力にネガティブな影響を及ぼすことを認識します。
Security Incident Reporting. If Snowflake becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data (a "**Security Incident**"), Snowflake shall notify Customer without undue delay, and in any case, where feasible, notify Customer within 72 hours after becoming aware.[2] To facilitate timely notification, Customer must register and maintain an up-to-date email within the Service for this type of notification. Where no such email is registered, Customer acknowledges that the means of notification shall be at Snowflake's reasonable discretion and Snowflake's ability to timely notify shall be negatively impacted.

7.2 調査　前項に定めるセキュリティインシデントが発生した場合には、Snowflake はその対処、調査及び影響軽減のための合理的な措置を速やかに取るものとします。セキュリティインシデントに関連があると思われるログはすべて、1 年以上保存します。
Investigation. In the event of a Security Incident as described above, Snowflake shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident. Any logs determined to be relevant to a Security Incident, shall be preserved for at least one year.

7.3 連絡及び協力　Snowflake は、お客様に対して、把握している範囲のセキュリティインシデント情報をタイムリーに提供するものとします。これには、セキュリティインシデントの性質及び影響、Snowflake が軽減又は解決のために実施し又は実施しようとする措置、Snowflake による調査状況、追加情報の問い合わせ先、さらに、影響を受けるデータ記録の種類及びおおよその件数を含みますが、これらに限られません。上記の規定にもかかわらず、お客様は、

[3] 明確性を期すために付言すると、お客様の基本契約において「セキュリティ違反（Security Breach）」という用語が用いられている場合には、本追補条項にて定義するセキュリティインシデントを意味するものとします。For clarity, where Customer's Agreement refers to the defined term "Security Breach", such reference shall be interpreted to refer to Security Incident, as defined herein

Snowflake 従業員が顧客データの内容を見ることができないかもしれないため、Snowflake が顧客データの具体的な性質に関する情報、又は影響を受けるデータ主体の身元、件数又は種類に関する情報を提供できる可能性は非常に低いかもしれないことを了解します。Snowflake がお客様にセキュリティインシデントに関連する連絡をしたこと又は Snowflake のためにそのような連絡がされたことをもって、Snowflake がそのセキュリティインシデントに関する過失又は責任を認めたものとは解釈されないものとします。

Communication and Cooperation. Snowflake shall provide Customer timely information about the Security Incident to the extent known to Snowflake, including, but not limited to, the nature and consequences of the Security Incident, the measures taken and/or proposed by Snowflake to mitigate or contain the Security Incident, the status of Snowflake's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. Notwithstanding the foregoing, Customer acknowledges that because Snowflake personnel may not have visibility to the content of Customer Data, it may be unlikely that Snowflake can provide information as to the particular nature of the Customer Data, or where applicable, the identities, number, or categories of affected data subjects. Communications by or on behalf of Snowflake with Customer in connection with a Security Incident shall not be construed as an acknowledgment by Snowflake of any fault or liability with respect to the Security Incident.

8. 顧客データの消去
8. Deletion of Customer Data

8.1 お客様による消去　本サービスはお客様に顧客データを削除する権限を付与します（詳細はドキュメンテーションに記述されます）

By Customer. The Service provides Customer controls for the deletion of Customer Data, as further described in the Documentation.

8.2 Snowflake による消去　基本契約の適用のある条件を遵守することを条件として、Snowflake は、(i)本契約の期間満了又は解除、及び(ii)基本契約に規定される終了後の「回収の期間」のいずれか遅い方が到来したときは、速やかに、残存する顧客データを消去するものとします。

By Snowflake. Subject to applicable provisions of the Agreement, upon the later of (i) expiration or termination of the Agreement and (ii) expiration of any post-termination “retrieval period” set forth in the Agreement, Snowflake shall promptly delete any remaining Customer Data.

9. お客様の権利及びセキュリティに関する責任共有
9. Customer Rights & Shared Security Responsibilities

9.1 お客様による侵入テスト　お客様は、自らのアカウントの侵入テスト（以下「侵入テスト」といいます）を、サポートチケットにより書面で申し込むことができます。Snowflake が申し込みを受けた後、Snowflake 及びお客様は、侵入テストの開始日、範囲及び期間、さらに、秘密保持若しくはセキュリティへの潜在的リスク又はその他本サービス若しくは Snowflake 業務の中断による影響の軽減のための合理的な条件など、侵入テストの詳細条件を事前に合意するものとします。侵入テスト及びそれにより得られた情報は Snowflake の秘密情報とみなされます。お客様が侵入テストに関連して脆弱性又はその疑いを発見した場合には、直ちに Snowflake に開示し、第三者には開示しないものとします。

Customer Penetration Testing. Customer may provide a written request for a penetration test of its Account ("**Pen Test**") by submitting such request via a support ticket. Following receipt by Snowflake of such request, Snowflake and Customer shall mutually agree in advance on details of such Pen Test, including the start date, scope and duration, as well as reasonable conditions designed to mitigate potential risks to confidentiality, security, or other potential disruption of the Service or Snowflake's business. Pen Tests and any information arising therefrom are deemed Snowflake's Confidential Information. If Customer discovers any actual or potential vulnerability in connection with a Pen Test, Customer must immediately disclose it to Snowflake and shall not disclose it to any third-party.

9.2 お客様による監査の権利 Customer Audit Rights.

9.2.1 Snowflake は、書面による合理的な要請に応じて、お客様及び・又は正当に授権された第三者である代理人（以下「監査人」と総称します）に対し、必要に応じて、本セキュリティ追補条項に基づく Snowflake の義務遵守に関する以下の証明書類へのアクセスを、お客様の追加費用なしで提供します。(i) Snowflake の ISO 27001、HITRUST CSF 及び PCI-DSS のサードパーティ認証、(ii) Snowflake の SOC 2 タイプ II 監査レポート、SOC 1 タイプ II 監査レポート及び HIPAA 業務委託先コンプライアンスレポート、(iii) Snowflake の最新の業界標準セキュリティ調査（SID、CAIQ 等）、並びに(iv) 本サービスのデータフロー図（以下、第三者監査と併せて「監査報告」といいます）。

Upon written request and at no additional cost to Customer, Snowflake shall provide Customer, and/ or its appropriately qualified third-party representative (collectively, the "**Auditor**"), access to reasonably requested documentation evidencing Snowflake's compliance with its obligations under this Security Addendum in the form of, as applicable, (i) Snowflake's ISO 27001, HITRUST CSF, and PCI-DSS third-party certifications, (ii) Snowflake's SOC 2 Type II audit report, SOC 1 Type II audit report, and HIPAA Compliance Report for Business Associates, (iii) Snowflake's most recently completed industry standard security questionnaire, such as a SIG or CAIQ, and (iv) data flow diagrams for the Service (collectively with Third-Party Audits, "**Audit Reports**").

9.2.2 お客様は、Snowflake 施設への検査も含む、Snowflake の適切な管理の監査を書面で申し込むことができます。Snowflake が申し込みを受けた後、Snowflake 及びお客様は、監査の合理的な開始日、範囲及び期間、さらに監査に適用されるセキュリティ及び秘密管理対策を含めた詳細について事前に合意するものとします。Snowflake は、監査料金を請求することができ、その金額は Snowflake が費消するリソースを考慮した上で合理的な金額とします。監査報告、監査及びこれらから得られた情報はすべて、Snowflake の秘密情報とみなされます。

Customer may also send a written request for an audit of Snowflake's applicable controls, including inspection of its facilities. Following receipt by Snowflake of such request, Snowflake and Customer shall mutually agree in advance on the details of the audit, including the reasonable start date, scope and duration of and security and confidentiality controls applicable to any such audit. Snowflake may charge a fee (rates shall be reasonable, taking into account the resources expended by Snowflake) for any such audit. Audit Reports, any audit, and any information arising therefrom shall be considered Snowflake's Confidential Information.

9.2.3 監査人が第三者である場合（すなわち、お客様が第三者に依頼して第 9.1 条に基づく承認を受けた侵入テストを行わせる場合）には、当該第三者が監査、侵入テスト又は監査報告の検討を行う前に、Snowflake との間で別途秘密保持契約書の締結を求めることがあります。当該第三者が適切な資格を備えていないか又は Snowflake の直接の競合業者であると合理的に判断する場合には、Snowflake はその第三者に関して書面で異議を述べることができます。Snowflake が異議を述べた場合には、お客様は、別の第三者を選任するか、自ら監査、侵入テスト又は報告書の検討を行わなければなりません。監査報告の審査、監査又は侵入テストに関して監査人に発生したいかなる費用は、すべて監査人の負担とします。

Where the Auditor is a third-party (or Customer is using a third-party to conduct an approved Pen Test under Section 9.1), such third party may be required to execute a separate confidentiality agreement with Snowflake prior to any audit, Pen Test, or review of Audit Reports, and Snowflake may object in writing to such third party if in Snowflake's reasonable opinion the third party is not suitably qualified or is a direct competitor of Snowflake. Any such objection by Snowflake will require Customer to appoint another third party or conduct such audit, Pen Test, or review itself. Any expenses incurred by an Auditor in connection with any review of Audit Reports, or an audit or Pen Test, shall be borne exclusively by the Auditor.

9.3 センシティブな顧客データ　PCI-DSS、HIPAA、FedRAMP、又は同等の高度な基準の要件を満たすために、本サービスを使用する場合は、お客様が実施する追加の管理が必要です。これには、かかる要件の対象となるお客様のデータは、 かかる要件についてドキュメンテーションで特に指定された本サービスの Edition 及び地域にのみアップロードできることが含まれます。

さらに、お客様は、そのようなデータを保護するために、お客様側で設定可能でかつ適切なセキュリティ対策をすべて実施しなければなりません。これには、すべてのユーザーの対話型ログオン（本サービスへの認証接続を行う個人等）の際の IP ホワイトリスティング及び二段階認証（MFA）などが含まれます。

Sensitive Customer Data. Use of the Service to meet requirements of PCI-DSS, HIPAA, FedRAMP, or similar heightened standards, require additional controls which shall be implemented by Customer, including that Customer Data subject to such requirements may only be uploaded to Editions and Regions of the Service specifically designated in the Documentation for such requirements. Additionally, Customer must implement all appropriate Customer-configurable security controls, including IP whitelisting and MFA for all User interactive logins (e.g., individuals authenticating to the Service) to protect such data.

9.4 セキュリティに関する責任共有　お客様は、以下のことに同意するものとします。これらは、本セキュリティ追補条項に基づく Snowflake の義務を軽減するものではありません。

Shared Security Responsibilities. Without diminishing Snowflake's commitments in this Security Addendum, Customer agrees:

9.4.1 Snowflake が、特定の法令、規制その他の要件が課される情報がないか調べることを含め、顧客データの内容、正確性又は適法性を審査する義務を負うものではないこと。お客様は、本サービスを適切に利用し（第 1.1 条で特定されていない認証及び/又は認可を必要とするデータをアップロードしないことを含む）、顧客データの内容に応じた水準のセキュリティを確保する責任を負います。これには、Tri-Secret Secure（ドキュメンテーションにて説明されます）などの暗号化機能の実行、顧客データの匿名化及び本サービスをバックアップされた顧客データに設定することなどが含まれます。

Snowflake has no obligation to assess the content, accuracy or legality of Customer Data, including to identify information subject to any specific legal, regulatory or other requirement and Customer is responsible for making appropriate use of the Service (including not uploading data that requires a certification and/or authorization which is not identified in Section 1.1) to ensure a level of security appropriate to the particular content of Customer Data, including, where appropriate, implementation of encryption functionality, such as the "tri-secret secure" feature (as described in the Documentation), pseudonymization of Customer Data, and configuration of the Service to back-up Customer Data;

9.4.2 お客様は、ユーザーのロール及び認証情報の管理及び保護について責任を負うこと。これには、以下の責任が含まれますが、これらに限られません。(i) すべてのユーザーに対して、認証情報を秘密情報として扱い、無権限者と共有しないよう確かにすること。(ii) お客様のアカウントに関して疑わしいアクティビティが把握された場合（例えば、ユーザーの認証情報が流出した場合）は、迅速に Snowflake に報告すること。(iii) 顧客データの性質を勘案した上で、ユーザーによるアクセスの範囲及び時間など、ユーザー及びロールに応じたアクセス制御を適切に設定すること。(iv) パスワードの適切な一意性、長さ、複雑さ及び有効期限を維持すること。

Customer is responsible for managing and protecting its User roles and credentials, including but not limited to (i) ensuring that all Users keep credentials confidential and not share such information with unauthorized parties, (ii) promptly reporting to Snowflake any suspicious activities related to Customer's Account (e.g., a user credential has been compromised), (iii) appropriately configuring User and role-based access controls, including scope and duration of User access, taking into account the nature of its Customer Data, and (iv) maintaining appropriate password uniqueness, length, complexity, and expiration;

9.4.3 お客様の管理下にある暗号化キーを適切に管理及び保護し、キー及びそのキーにより暗合化された顧客データの完全性、可用性及び秘密性を確保すること。

to appropriately manage and protect any Customer-managed encryption keys to ensure the integrity, availability, and confidentiality of the key and Customer Data encrypted with such key; and

9.4.4 Snowflake がアップデートを公表した場合には速やかにクライアントソフトウェアを更新すること。

to promptly update its Client Software whenever Snowflake announces an update.