

DATA SECURITY ADDENDUM

データセキュリティ付属文書

In the event of any discrepancies between the English and the Japanese versions of this Addendum, the English version shall prevail.

本付属文書の英語版および日本語版に齟齬がある場合、英語版が優先するものとします。

1. SECURITY PROGRAM	1. セキュリティプログラム
While providing the Subscription Service, ServiceNow will ensure there is a written information security program of policies, procedures and controls aligned to the ISO27001 Series, or substantially equivalent standard, governing the processing, storage, transmission and security of Customer Data (the “ Security Program ”). The Security Program will include industry-standard practices designed to protect Customer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. ServiceNow updates the Security Program to address new and evolving security technologies, changes to industry standard practices, and changing security threats, provided that no such update will materially reduce the overall level of commitments or protections provided to Customer as described herein.	サブスクリプションサービスの提供中、ServiceNow は、顧客データの処理、保存送信およびセキュリティを管理する、ISO27001 シリーズまたは実質的に同等の標準に沿ったポリシー、手続ならびに管理についての書面による情報セキュリティプログラム（以下「セキュリティプログラム」という）が存在することを保証します。セキュリティプログラムには、偶然もしくは違法な破棄、損失、変更、権限のない開示またはアクセスから顧客データを保護するよう設計された業界標準の慣行を含みます。ServiceNow は、新規の、および発展するセキュリティ技術、業界標準の慣行の変化、ならびに変化するセキュリティ脅威に対応するため、セキュリティプログラムをアップデートします。ただし、いずれの当該アップデートも、DSA に記載に従って顧客に対して提供されるコミットメントまたは保護の全般的な水準を重大に低下させるものではありません。
1.1. SECURITY ORGANIZATION . There will be a Chief Information Security Officer, or equivalent executive, that is designated as responsible for coordinating, managing, and monitoring the information security function, policies, and procedures.	1.1. セキュリティ組織 最高情報セキュリティ責任者または同等の重役は、情報セキュリティ機能、ポリシーおよび手続の調整、管理および監視につき責任を負うそれらの責任者として指名されます。
1.2. POLICIES . The information security policies will be: (i) documented; (ii) reviewed and approved by management, including after material changes; and (iii) published, and communicated to personnel, and contractors, including appropriate ramifications for non-compliance.	1.2. ポリシー 情報セキュリティポリシーは、(i) 文書化され、(ii) 重大な変更を加えた後も含め、経営陣により精査および承認され、また(iii) 非遵守に対する適切な結果を含め、公表され、人員および請負人に対して伝達されます。
1.3. RISK MANAGEMENT . There will be information security risk assessments performed as part of a risk governance program that is established with the objective to regularly test, assess and evaluate the effectiveness of the Security Program. Such assessments will be designed to recognize and assess the impact of risks and implement identified risk reduction or mitigation strategies to address new and evolving	1.3. リスク管理 セキュリティプログラムの効果を定期的 に検証し、評価し、査定することを目的として設けられているリスクガバナンスプログラムの一部として、情報セキュリティのリスク評価が実施されます。当該評価は、リスクの影響を認識し、評価すること、ならびに新規の、および発展するセキュリティ技術、業界標準の慣行の変化、ならびに変化するセキュリティ脅威に対応するため、特定されたリスクの削減または緩和策を実行するよう計画されています。

security technologies, changes to industry standard practices, and changing security threats.	
2. CERTIFICATIONS AND AUDITS	2. 認証および監査
2.1. CERTIFICATIONS AND ATTESTATIONS. ServiceNow will establish and maintain sufficient controls to meet certification and attestation for the objectives stated in ISO27001, ISO27018, SSAE 18 / SOC 1 and SOC 2 Type 2 (or equivalent standards) for the Security Program. At least once per calendar year, an assessment against such standards and audit methodologies by an independent third-party auditor will be obtained for environments where Customer Data is stored.	2.1. <u>認証および認定</u> ServiceNow は、セキュリティプログラムのための ISO27001、ISO27018、SSAE18/SOC1、および SOC2 Type2（またはこれらと同等の規格）に規定された目的についての認証および認定を満たす十分な管理を確立し、維持します。少なくとも暦年に一度、独立した第三者監査人による当該規格および監査手法に対する評価を、顧客データが保存されている環境で入手します。
2.2. AUDIT. ServiceNow will allow for and contribute to audits that include inspections by granting Customer access to reasonable and industry recognized documentation evidencing the policies and procedures governing the security and privacy of Customer Data and the Security Program through a self-access documentation portal ("ServiceNow CORE") and at no additional costs ("Audit"). The information available in ServiceNow CORE will include documentation evidencing the Security Program, inclusive of the privacy policies and procedures regarding Personal Data Processed, as well as copies of certifications and attestation reports (including audits) listed above. To the extent that Customer has not reasonably been able to satisfy its audit requirements by following the procedure outlined in this Clause, ServiceNow will provide Customer with such further assistance as may reasonably be required (in accordance with the assistance obligations described herein) to substantially satisfy such requirements.	2.2. <u>監査</u> ServiceNow は、顧客が直接アクセスできる文書ポータル（以下「ServiceNow CORE」という）を通じて、追加費用なしで、顧客データのセキュリティおよびプライバシーならびにセキュリティプログラムについて規定するポリシーおよび手続を証する合理的かつ業界標準の文書に顧客がアクセスできるようにすることによる調査を含む監査（以下「監査」という）を認め、提供します。ServiceNow CORE で顧客が入手できる情報は、セキュリティプログラムを証する文書、ならびに処理される個人データに関するプライバシーポリシーおよび手続、認証書の写しおよび上記の認定報告書（監査を含む）を含みます。顧客が本条に概説されている手続をとって自らの監査要件を充足することが合理的に不可能である範囲に限り、ServiceNow は、(DSA に定められる支援義務に従い、) 合理的に要求され得る場合、顧客に対して、当該要件を実質的に充足するよう、かかる追加の支援を提供します。
2.3. OUTPUT. Upon Customer's request, ServiceNow and Customer may schedule a mutually convenient time to discuss the Audit. In the event the Audit has any findings of material noncompliance with the Data Processing Addendum or this Data Security Addendum ("DSA"), then ServiceNow will promptly address such findings of noncompliance. ServiceNow may, in its sole discretion and consistent with industry and ServiceNow's standards and practices, make commercially reasonable efforts to implement Customer's suggested	2.3. <u>アウトプット</u> 顧客からの要望がある場合、ServiceNow および顧客は、監査について議論するために互いに都合のよい時間を定めることができます。監査において、データ処理付属文書または本付属文書（以下「DSA」という）への重大な非遵守が発見された場合、ServiceNow は、速やかに当該非遵守の発見に対処します。ServiceNow は、その単独の裁量で、かつ業界および ServiceNow の標準および慣行に従い、ServiceNow のセキュリティプログラムを改善するために監査において言及された顧客提案の改善策を実行する商業的に合理的

improvements noted in the Audit to improve ServiceNow's Security Program. The Audit and the results derived therefrom are Confidential Information of ServiceNow.	な努力をします。監査およびそこから得られる結果は、ServiceNow の機密情報です。
3. PHYSICAL, TECHNICAL, AND ORGANIZATIONAL SECURITY MEASURES	3. 物理的、技術的および組織的セキュリティ対策
3.1. PHYSICAL SECURITY MEASURES.	3.1. 物理的なセキュリティ対策
3.1.1. <u>DATA CENTER FACILITIES.</u> The data center facilities will include: (1) physical access restrictions and monitoring that will include a combination of any of the following: multi-zone security, man-traps, appropriate perimeter deterrents (e.g. fencing, berms, guarded gates), on-site guards, biometric controls, CCTV, and secure cages; and (2) fire detection and fire suppression systems both localized and throughout the data center floor.	3.1.1. <u>データセンターの設備</u> データセンターの設備には、(1) 以下を組み合わせたものを含む物理的なアクセス制限およびモニタリング: マルチゾーンセキュリティ、マントラップ、適切な境界線上の妨害物(柵、盛り土、守衛門等)、現場の守衛、生体認証、CCTV、およびセキュアケージ、(2) データセンターフロアにおける局地的および全体的な火災感知および消火システムが含まれます。
3.1.2. <u>MEDIA.</u> For deletion of data, an industry standard such as NIST 800-88 (or substantially equivalent) will be used for the deletion of sensitive materials, including Customer Data, before final disposition of such media.	3.1.2. <u>媒体データの削除</u> に関しては、媒体の最終処分の前に、NIST 800-88 等(またはこれと実質的に同等)の業界標準を用いて、顧客データを含むセンシティブな資料を削除します。
3.2. TECHNICAL SECURITY MEASURES.	3.2. 技術的なセキュリティ対策
3.2.1. <u>ACCESS ADMINISTRATION.</u> Access by personnel to Customer Data will be conducted in a manner that: (i) is protected by authentication and authorization mechanisms; (ii) requires personnel to be assigned a unique user account; (iii) restricts the sharing of individual user accounts; (iv) requires strong authentication with complex passwords; (v) ensures accounts are lock-out enabled; (vi) requires access over a VPN; (vii) requires access privileges be based on job requirements limited to that necessary for the applicable personnel to undertake their duties; (viii) ensures access is revoked upon termination of employment or consulting relationships; and (ix) requires access entitlements be reviewed by management quarterly.	3.2.1. <u>アクセス管理</u> 人員による顧客データへのアクセスは、(i) 認証および認可メカニズムにより保護され、(ii) 人員に固有のユーザーアカウントが割り当てられるよう要求し、(iii) 個人ユーザーアカウントの共有を制限し、(iv) 複雑なパスワードによる強力な認証を要求し、(v) アカウント・ロックアウトの有効化を確実にを行い、(vi) VPN を経由したアクセスを要求し、(vii) アクセス権限が、該当する人員が職務を遂行するために必要とする程度に限定された、業務上の必要性に応じたものであるよう要求し、(viii) アクセスを保証し、雇用または委託関係の終了時に無効化され、かつ(ix) 経営陣が四半期ごとにアクセス権限を審査するよう要求する方法により、行われます。
3.2.2. <u>LOGGING AND MONITORING.</u> The production infrastructure log activities will be centrally collected, secured in an effort to prevent tampering, and monitored for anomalies by a trained security team.	3.2.2. <u>ロギングおよび監視</u> 本番環境のログのアクティビティは、中央で収集され、改ざんを防止すべく保管され、トレーニングを受けたセキュリティチームにより、異常がないか監視されます。
3.2.3. <u>FIREWALL SYSTEM.</u> Firewall technology will be installed and managed to protect systems and inspect ingress connections. Managed firewall	3.2.3. <u>ファイアーウォールシステム</u> 侵入経路を調査し、システムを保護するよう、ファイアーウォール技術がネットワーク上に導入され、管理されます。管理下にあるファイア

rules will be reviewed in accordance with then-current operating procedures, which will be reviewed no less frequently than quarterly.	一ウォール規則は、その時点で最新の運用手順に従って、検証され、当該手順は、少なくとも四半期ごとに検証されます。
3.2.4. <u>VULNERABILITY MANAGEMENT</u>. Vulnerability scans will be performed within the environment to determine potential vulnerabilities in accordance with then-current security operating procedures, which will be at least quarterly. When software vulnerabilities are revealed and addressed by a vendor patch, the patch will be obtained from the applicable vendor and applied within an appropriate risk-based timeframe in accordance with the then-current vulnerability management and security patch management standard operating procedure and only after such patch is tested and determined to be safe for installation in production systems.	3.2.4. <u>脆弱性管理</u> 潜在的脆弱性を判断するために、少なくとも四半期ごとに、その時点で最新のセキュリティ運用手順に従って、環境内において脆弱性検査が実施されます。ソフトウェア脆弱性がベンダーから提供されるパッチにより明らかとなり、対処された場合、当該パッチは、該当するベンダーから入手され、リスクに応じた適切な時間枠の中で、その時点で最新の脆弱性管理およびセキュリティ・パッチ管理標準運用手順に従い、テスト環境にて、本番環境へのインストールが安全だということを確認の上、本番システムに適用されます。
3.2.5. <u>ANTIVIRUS</u> . Antivirus, anti-malware, and anti-spyware software will be updated on regular intervals and centrally logged.	3.2.5. <u>ウイルス防止</u> ウイルス防止、マルウェア防止およびスパイウェア防止ソフトウェアは、定期的アップデートされ集約的に記録されます。
3.2.6. <u>CHANGE CONTROL</u> . Changes to the environment will be reviewed to minimize risk. Such changes will be implemented in accordance with then-current standard operating procedure.	3.2.6. <u>変更管理</u> リスクを最小限に抑えるために、環境への変更は審査されます。かかる変更は、その時点で最新の標準運用手順に従い実行されます。
3.2.7. <u>CONFIGURATION MANAGEMENT</u> . Standard hardened configurations for the system components within the environment will be maintained using industry standard hardening guides, such as guides from the Center for Internet Security.	3.2.7. <u>設定管理</u> 環境内のシステム要素についての標準的な堅牢性のある設定は、Center for Internet Securityからのガイド等、業界標準の堅牢性に関するガイドラインを使用して維持されます。
3.2.8. <u>DATA ENCRYPTION IN TRANSIT</u> . Industry standard encryption will be used to encrypt Customer Data in transit over public networks.	3.2.8. <u>移送中のデータの暗号化</u> 公共ネットワーク上で移送中の顧客データの暗号化には、業界標準の暗号化が使用されます。
3.2.9. <u>DATA ENCRYPTION AT REST</u> . The encryption of Customer Data at rest will be determined by Customer and, if encrypted, will be encrypted as determined by Customer according to the applicable offerings.	3.2.9. <u>保存中のデータの暗号化</u> 保存中の顧客データの暗号化については顧客が判断し、暗号化する場合は、提供されるもののうち、該当するものに応じて顧客が判断するおりに暗号化されます。
3.2.10. <u>ILLICIT CODE AND SECURE SOFTWARE DEVELOPMENT</u> . ServiceNow will follow the secure software development and code review practices described in this section to prevent harm from malware, such as from viruses, worms, date bombs, time bombs, or shut down devices. Software will be developed using secure application development policies and procedures aligned with industry standard practices such as the OWASP Top Ten (or a substantially equivalent	3.2.10. <u>不正コードおよび安全なソフトウェア開発</u> ServiceNow は、ウイルス、ワーム、デートボム、タイムボム、シャットダウン装置から等のマルウェアによる損害を防ぐため、本条に記載される安全なソフトウェア開発コード審査慣行に従います。ソフトウェアは、OWASP Top Ten(またはこれと実質的に同等の標準)等の業界標準の慣行に沿った安全なアプリケーション開発ポリシーおよび手順を用いて開発されます。安全なアプリケーション設計および

standard). Personnel responsible for secure application design and development will receive appropriate training regarding secure application development practices.	開発に責任を有する人員は、安全なアプリケーション開発慣行に関する適切なトレーニングを受けます。
3.2.11. <u>SECURE CODE REVIEW</u> . A combination of static and dynamic testing of code will be performed prior to the release of such code to Customers. Vulnerabilities will be addressed in accordance with the then-current software vulnerability management program. To address vulnerabilities where code has been made available to Customers, software patches will be regularly made available to Customers	3.2.11. <u>安全なコード検証</u> 顧客に対してコードをリリースする前に、静的および動的コードのテストを組み合わせで行います。脆弱性は、その時点で最新のソフトウェア脆弱性管理プログラムに基づいて対処されます。コードが顧客に対して入手可能となっている場合の脆弱性に対処するため、ソフトウェア・パッチを、顧客に対して定期的に入手することができるようにします。
3.3. <u>ORGANIZATIONAL SECURITY MEASURES</u> .	3.3. <u>組織的セキュリティ対策</u>
3.3.1. <u>PERSONNEL SECURITY</u> . Background screening will be performed on all employees and all contractors who have access to Customer Data in accordance with applicable standard operating procedure and subject to applicable Law.	3.3.1. <u>人的セキュリティ</u> 顧客データにアクセスするすべての従業員およびすべての請負人に対して、該当する標準運用手順および適用される法律に基づき、経歴のスクリーニングが行われます。
3.3.2. <u>SECURITY AWARENESS AND TRAINING</u> . Security and Privacy awareness training and education will be provided to employees and contractors who have access to Customer Data. Such training will be conducted at time of hire and at least annually throughout employment.	3.3.2. <u>セキュリティ啓発およびトレーニング</u> 顧客データへのアクセス権を有する従業員および請負人に対して、セキュリティおよびプライバシーに関する啓発トレーニングおよび教育が実施されます。かかるトレーニングは、採用時および雇用期間中少なくとも年 1 回行われます。
3.3.3. <u>VENDOR RISK MANAGEMENT</u> . Any vendor that accesses, stores, processes or transmits Customer Data will be assessed to ensure it has appropriate security and privacy controls.	3.3.3. <u>ベンダーリスク管理</u> 顧客データへアクセスし、これを保存し、処理し、または移転するあらゆるベンダーは、かかるベンダーが適切なセキュリティおよびプライバシー管理を有することを保証するため、査定されます。
3.3.4. <u>SOFTWARE AND ASSET INVENTORY</u> . An inventory of the software components (including, but not limited to, open-source software) used in the environment will be maintained.	3.3.4. <u>ソフトウェアおよび資産のインベントリ</u> 環境において使用されるソフトウェア部品（オープンソースソフトウェアを含むがこれに限らない）のインベントリは、維持されます。
3.3.5. <u>WORKSTATION SECURITY</u> . Security mechanisms on personnel workstations, including firewalls, anti-virus, and full disk encryption with a minimum of AES 128-bit encryption will be implemented and maintained. Personnel will be restricted from disabling security mechanisms.	3.3.5. <u>ワークステーションのセキュリティ</u> 最低でも AES128 ビットで暗号化されたファイアーウォール、アンチウイルスおよび完全なディスク暗号化を含む、人員のワークステーションのセキュリティの仕組みが、実装され、かつ維持されます。人員は、セキュリティの仕組みを無効化しないよう制限されます。
4. <u>SERVICE CONTINUITY</u>	4. <u>サービス継続性</u>
4.1. <u>DATA LOCATION</u> . ServiceNow will host the purchased instances in data centers located in the geographic region specified on the Order Form which have attained SSAE 18 Type 2 attestations or have ISO 27001 certifications (or equivalent or successor attestations or certifications) .	4.1. <u>位置データ</u> ServiceNow は、オーダーフォームに明記される地理的地域に位置しており、SSAE 18 Type 2 認定または ISO 27001 認証（または同等のもしくは承継の認定または認証）を有するデータセンターにおいて、購入されたインスタンスを保持します。

4.2. DATA BACKUP. Back-ups will be performed of all Customer Data in accordance with the then-current operating procedure available in the CORE Portal.	4.2. データバックアップ すべての顧客データのバックアップは、CORE ポータルにおいて実行可能な、その時点で最新の運用手順に従って、実施されます。
4.3. DISASTER RECOVERY. An Information Security Contingency Plan (ISCP) to address disaster recovery will be maintained that is consistent with industry standards for the environment and will: (i) test the ISCP at least once every year; (ii) make available summary test results that will include the actual recovery point and recovery times; and (iii) document any action plans within the summary test results to promptly address and resolve any deficiencies, concerns, or issues that prevented or may prevent the environment from being recovered in accordance with the ISCP.	4.3. 災害復旧 災害復旧に対処するための情報セキュリティ危機対策計画（以下「ISCP」という）は、環境についての業界標準に沿って維持され、(i) ISCP を少なくとも年 1 回の頻度で検証し、(ii) 実際の復旧地点および復旧時間を含む検証結果の概要を入手できるようにし、また、(iii) ISCP に基づく環境の復旧を妨げた、または妨げる可能性のある不具合、懸念または課題に速やかに対処しかつこれを解消するための行動計画を検証結果の概要内に文書化します。
4.4. BUSINESS CONTINUITY. A business continuity plan (“BCP”) will be maintained to minimize the impact from an event to ServiceNow’s provision and support of the Subscription Services. The BCP will: (i) include processes for protecting personnel and assets and restoring functionality in accordance with the time frames outlined therein; and (ii) be tested annually and updated based on any deficiencies identified during such tests.	4.4. 事業継続性 ServiceNow によるサブスクリプションサービスの提供およびサポートに対する事象の影響を最小化するため、事業継続計画（以下「BCP」という）が維持されます。BCP は、(i) かかる計画において概説されている時間枠に従った人員および資産の保護ならびに機能性の回復のための手順を含み、また(ii) 年 1 回の頻度で検証されかつかかる検証中に特定された不具合に基づいて見直されます。
5. MONITORING AND INCIDENT MANAGEMENT	5. モニタリングおよびインシデント管理
5.1. INCIDENT MONITORING AND MANAGEMENT. System events are monitored and analyzed in a timely manner in accordance with ServiceNow’s current standard operating procedures. Response teams will be escalated to and engaged as necessary to address a security incident.	5.1. インシデントのモニタリングおよび管理 システム事象は、ServiceNow の最新の標準運用手順に従って適時にモニターされ、分析されます。セキュリティインシデントに対処するために必要な場合、対策チームに上程され、対策チームは、これに従事します。
5.2. BREACH NOTIFICATION. 5.2.1 NOTIFICATION. ServiceNow will report to Customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure, of or access to Customer Data (“Breach”) without undue delay following determination by ServiceNow that a Breach has occurred.	5.2. 違反通知 5.2.1. 通知 ServiceNow は、顧客に対し、顧客データの偶然もしくは違法な破棄、損失、変更、権限のない開示またはアクセス（以下「違反」という）につき、違反が起きたと ServiceNow が判断した後、不当な遅滞なく報告します。
5.2.2. REPORT. The initial report will be made to Customer’s security or privacy contact(s) designated in ServiceNow’s customer support portal (or if no such contact(s) are designated, to the primary technical contact designated by Customer). As relevant information in relation to	5.2.2. 報告 最初の報告は、ServiceNow のカスタマーサポートポータルで指定された顧客のセキュリティまたはプライバシー担当者（担当者が指定されない場合、顧客によって指定された主な技術担当者）に対して行われます。違反についての関連情報が収集されるか、またはその他の方法により ServiceNow に対して入手可能となった場合、

the Breach is collected or otherwise becomes available to ServiceNow, it will provide such information without undue delay to Customer, to assist Customer to comply with its notification obligations under Data Protection Laws. In particular, to the extent reasonably possible and applicable, ServiceNow will provide Customer with the information described in Article 33 of GDPR.	ServiceNow は、顧客がデータ保護法に基づくその通知義務を遵守するよう支援するため、顧客に対して当該情報を不当な遅滞なく提供します。特に、合理的に可能かつ該当する場合に限り、ServiceNow は、顧客に GDPR の第 33 条に規定される情報を提供します。
5.2.3. DATA CONTROLLER OBLIGATIONS. Customer will cooperate with ServiceNow in maintaining accurate contact information in the customer support portal and by providing any information that is reasonably requested to resolve any security incident, including any Breaches, identify its root cause(s) and prevent a recurrence. Customer is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted Data Subjects in relation to any Breach and for providing such notice.	5.2.3. データ管理者の義務 顧客は、セキュリティインシデント(違反を含む)を解決し、根本原因を特定し、かつ再発を防ぐために合理的に要求された情報を提供することによって、ServiceNow と協力し、カスタマーサポートポータルにおいて正確な連絡先情報を維持します。顧客は、あらゆる違反に関連して、かつ関連する監督または規制官庁および影響を受けたデータ主体に通知するか否かの決定、ならびに当該通知の交付について単独の責任を負います。
6. PENETRATION TESTS	6. 侵入テスト
6.1. BY A THIRD-PARTY. For each family release, skilled third-party vendors will perform penetration testing on the applications on the ServiceNow platform to identify vulnerabilities. Executive reports from the penetration testing are made available to Customer in ServiceNow CORE.	6.1. 第三者によるテスト 各ファミリー・リリースに関しては、脆弱性を特定するために、技術を有する第三者ベンダーが、ServiceNow のプラットフォーム上のアプリケーションについて、侵入テストを実施します。侵入テストのエグゼクティブ・レポートは、ServiceNow CORE において顧客に提供されます。
6.2. BY CUSTOMER. Customer may request to perform, at its own expense, an application penetration test for applications in which Customer Data is stored; provided that Customer will: (i) notify ServiceNow and submit a request to schedule such a test using the Support Portal per ServiceNow's then-current penetration testing policy, and (ii) agree to ServiceNow's penetration test agreement prior to conducting such test. In the event Customer's authorized penetration testing identifies vulnerabilities that ServiceNow is able to reproduce, ServiceNow will, consistent with industry-standard practices, use commercially reasonable efforts to promptly make any necessary changes to improve the security of the Subscription Service.	6.2. 顧客によるテスト 顧客は、自己の費用で、顧客データが保存されているアプリケーションについて、アプリケーション侵入テストの実施を要求することができます。ただし、顧客は、(i) ServiceNow に通知し、サポートポータルを通して、その時点における最新の ServiceNow の侵入テストポリシーに従い、当該テストを予定するよう求める要求書を提出し、かつ (ii) 当該テストを実施する前に、ServiceNow の侵入テストに関する契約に同意します。顧客が承認した侵入テストによって ServiceNow が再現できる脆弱性が特定された場合、ServiceNow は、業界の標準的慣行に沿って、サブスクリプションサービスのセキュリティを向上させるために必要なあらゆる変更を速やかに行うため、商業的に合理的な努力を行います。
7. SHARED SECURITY RESPONSIBILITY	7. セキュリティ責任の共有
7.1. PRODUCT CAPABILITIES. ServiceNow provides a variety of security settings that allow Customer to configure security of the Subscription Services for their own use such as, but not limited	7.1. 製品の機能 ServiceNow は、顧客が、以下を含むが、以下に限定されない自らの使用のためにサブスクリプションサービスのセキュリティを設定することが可能となるよう、多様なセキュリティ設定を提供します。(i) 顧客インス

to: (i) authenticate users before accessing the Customer's instance; (ii) encrypt passwords; (iii) allow users to manage passwords; and (iv) access instance application logs. Customer will manage each user's access to and use of the Subscription Services by assigning to each user a credential and user type that controls the level of access to the applicable Subscription Services. Customer bears sole responsibility for reviewing the Security Program and making an independent determination as to whether it meets Customer's requirements, taking into account the type and sensitivity of Customer Data that Customer provides to ServiceNow. Customer bears sole responsibility for implementing encryption and access control functionalities within the instance to protect Customer Data and assumes all liability for damages directly resulting from any decision not to encrypt Customer Data. Customer bears sole responsibility for protecting the confidentiality of each user's login and password and managing each user's access to the Subscription Services. Customer will be solely responsible for implementing the documented best practices and hardening guidelines for securing its ServiceNow instances.	タンスにアクセスする前のユーザー認証、(ii) パスワードの暗号化、(iii) ユーザーによるパスワード管理、および(iv) インスタンスのアプリケーションログへのアクセス。顧客は、該当するサブスクリプションサービスへのアクセスレベルを制御する認証情報およびユーザータイプを各ユーザーに割り当てることによって、各ユーザーのサブスクリプションサービスへのアクセスおよび使用を管理します。顧客は、セキュリティプログラムを検証すること、ならびに、顧客が ServiceNow へ提供する顧客データの種類および機微性を考慮して、これが顧客の要求に見合ったものかどうか独自に判断することについて単独で責任を負います。顧客は、顧客データを保護するために、インスタンスの中で暗号化およびアクセス管理機能を実行することについて単独の責任を負い、顧客データを暗号化しないと判断した場合、それに直接起因する損害賠償金について全責任を負います。顧客は、各ユーザーのログインおよびパスワードの機密性の保護ならびに各ユーザーのサブスクリプションサービスへのアクセスの管理について単独で責任を負います。顧客は、自身の ServiceNow インスタンスの安全確保のために文書化されたベスト・プラクティスおよび堅牢性に関するガイドラインを実行することについて単独で責任を負います。
7.2. <u>SECURITY CONTACT.</u> In accordance with the Customer Support Policy (www.servicenow.com/upgrade-schedules.html), Customer agrees to identify and maintain appropriate security contact(s) for all information security incident and information security-related communication within the Support Portal.	7.2. セキュリティ担当者 顧客は、カスタマーサポートポリシー (www.servicenow.com/upgrade-schedules.html) に基づき、サポートポータル内で、すべての情報セキュリティインシデントおよび情報セキュリティ関連の連絡のための適切なセキュリティ担当者を特定し、かつ維持することに同意します。
7.3. <u>LIMITATIONS.</u> Notwithstanding anything to the contrary in this DSA or other parts of the Agreement, ServiceNow's obligations herein are only applicable to the Subscription Services. This DSA does not apply to: (i) information shared with ServiceNow that is not Customer Data; (ii) data in Customer's VPN or a third-party network; and (iii) any data processed by Customer or its users in violation of the Agreement or this DSA.	7.3. 制限 DSA または本契約のその他の部分に異なる定めがあろうとも、DSA に定める ServiceNow の義務は、サブスクリプションサービスのみには適用されます。DSA は、以下には適用されません。(i) 顧客データではない ServiceNow と共有された情報、(ii) 顧客の VPN または第三者のネットワークにあるデータ、および(iii) 本契約または DSA に違反して顧客またはそのユーザーが処理したあらゆるデータ。