クラウド サブスクリプション スケジュール

情報セキュリティ対策に関する補遺

サプライヤーは、以下に掲げるセキュリティ対策を導入しており、今後もこれらを維持するものとします。これらのセキュリティ対策は、該当するサブスクリプション仕様書で概説しているセキュリティ対策とともに、サプライヤー提供サービスのセキュリティに関してサプライヤーが負う唯一の責任です。本補遺において別段の定義を記載していない限り、本補遺で用いている「」により定義されたすべての用語の意味は、クラウド サブスクリプション スケジュールに定めるとおりとします。

機能	対策
情報セキュリティ プログラム	サプライヤーは、次の目的のために設計された情報セキュリティ プログラム（社内ポリシーおよび社内基準の採用を含みます）を導入しており、今後も当該プログラムを維持するもの とします。 （a）サプライヤー提供サービスを提供するために使用され、サプライヤーが管理しているデータ センター、サーバー、ネットワーク機器、ファイアウォールおよびホストソフトウェア システム（以下、「サプライヤー ネットワーク」といいます）の該当箇所に対する合理的に予見可能なセキュリティ リスクを特定すること。そして （b）適切であるとみなした場合に、定期的なリスク アセスメントおよびテストなどにより特定されたセキュリティ リスクを低減すること。 サプライヤーは、情報セキュリティ プログラムの調整、監視および実行を担当する 1 人以上のセキュリティ責任者を任命しています。 サプライヤーは、サプライヤー ネットワーク内の脆弱性を継続的に監視する脅威・脆弱性管理プログラムを維持するものとします。脆弱性は、さまざまな情報源および方法を活用して特定しています。かかる情報源および方法には、ベンダー、セキュリティ研究者、脆弱性診断、レッドチームの活動、ペネトレーション テストおよび従業員による報告が含まれることがあります。また、公表された第三者の脆弱性がサプライヤーの環境において適用されるか否かを確認しています。さらに、サプライヤーのアプリケーション インフラストラクチャ上において脆弱性診断および脆弱性評価を日常的かつ定期的に行っています。これらのプロセスは、脆弱性の先を見越した特定と修復を可能にするためだけではなく、サプライヤーのコンプライアンス上および規制上の要件を満たすために設計されています。

セキュアな開発ライフサイクルおよび脆弱性対応	サプライヤーは、サプライヤーの販売物が、公式のガバナンスプログラム体制の下で、適切に設計、開発、パッケージ化されていることを確実にするために実行しなければならない手順を定義することを目的として、セキュアな開発ライフサイクル プログラムを導入・維持しています。このプログラムは、サプライヤーの情報セキュリティ プログラムとともに、サプライヤー提供サービスの開発ライフサイクルおよび保守ライフサイクル全体におけるセキュリティに対処する際に役立っています。サプライヤーは、セキュアな開発および脆弱性対応に関する自らの慣行を継続的に評価および改善するための厳格なプロセスを採用しています。また、サプライヤーは、かかる自らの慣行と業界標準の慣行を定期的に比較しています。 報告されたサプライヤー提供サービス内の脆弱性を調査および検証した後に、サプライヤーは、公開済みのサプライヤーの脆弱性対応ポリシー（現時点において、Supplier Vulnerability Response Policy | Supplier US に掲載されています）に従って、適切な救済措置の特定、開発および適正化を試みるものとします。サプライヤーは、必要に応じて、セキュリティ上の注意喚起を通じて救済措置を顧客にお知らせしています。 また、サプライヤーは、商業上合理的な期間内にその救済措置を提供するよう努めています。なお、対応スケジュールは、脆弱性の重大度、救済措置の複雑度、影響を受けたコンポーネントなどの多くの要因によって異なります。
資産管理	サプライヤーはサプライヤー ネットワークを構成する物理的資産および論理的資産を追跡しています。サプライヤーが追跡する可能性のある資産および導入し得る管理策の例は次のとおりです。 （a）ソフトウェア資産（アプリケーションおよびシステム ソフトウェアなど） （b）物理的資産（サーバー、デスクトップ/ノートパソコン、バックアップ/アーカイブ用テープ、プリンターおよび通信機器など） そして （c）情報資産（データベース、ディザスター リカバリー計画、ビジネス継続計画、データの区分、アーカイブした情報など） サプライヤーは、事業上の重要性もしくはデータ区分上の機密性またはその両方に基づいて資産を分類しています。このように分類することで、上記の資産へのアクセスを適切に制限および管理することが可能になります。

人的セキュリティ	雇用プロセスの一環として、サプライヤーの従業員は、採用時に機密保持契約（NDA）に署名する義務および適用法に沿った人事調査を受ける義務があります。サプライヤーは、自らの単独の裁量の範囲内で、自らのポリシーを見直し、人的セキュリティを導入する権利を留保していますが、最新のポリシーに基づき、現地の法律および現地における実行可否に従って、サプライヤーは、次の雇用調査の１つ以上を実施しています：薬物検査、社会保障番号に基づく調査、犯罪歴の調査、学歴および職歴の検証、ならびに雇用資格の検証。また、サプライヤーは、サプライヤーの業界における類似企業の最新の業界基準を満たすよう努めていますが、サプライヤーは、自らの人的セキュリティおよび人事調査を特定のお客様の具体的な要望に沿うように計画することはできません。 第三者または外部契約者は、サプライヤーによる調査、契約条件としての調査、サプライヤーが認めた調査プロセスに従った請負業者による調査としての検証のいずれかを受けています。 サプライヤーは、サプライヤーの情報セキュリティ プログラムの要求事項を遵守していない要員に対する措置を講じるための懲戒プロセスを維持しています。かかる要求事項には、サプライヤーのセキュリ　ティ、可用性、および機密保持に関する確約と要件を達成するために整備された要求事項が含まれますが、これに限定されません。 サプライヤーは、該当するすべての要員に対し、セキュリティ意識向上トレーニングを毎年実施しています。また、該当する下請け業者には、当該下請け業者の要員に対し同一のトレーニングを実施することを義務付けています。
物理的セキュリティ	サプライヤー ネットワークの物理的な構成要素をハウジングしている施設（例：データ センター）では、リスク ベースの管理策を整備しています。アクセス制御の手法には、警備員の配 置、セキュリティ ログの取得、監視、警報装置の設置、セキュリティ区域への立ち入り制限、アクセス経路の保護、監視カメラの使用、キー カード、二要素認証などがあります。 この規定は、サプライヤーが管理するコロケーション サイト、およびパブリッククラウド サービスをホスティングするベンダーが管理するデータ センターに適用されます。
ネットワーク セキュリティ	サプライヤーの要員は、サプライヤー提供サービスを提供するために必要なときに、サプライヤーネットワークに電子的手段によりアクセスすることができます。サプライヤーは、ファイアウォールの使用や認証による制御を含め、各接続におけるサプライヤーが許可したサプライヤー ネットワークへのアクセスを管理するためのポリシーおよびアクセス制御策を維持するものとします。

	サプライヤーは、リスクに応じて管理策を導入することにより、サプライヤー ネットワーク内における資産の悪意ある使用を防止し、悪意あるソフトウェアから保護しています。Dell が導入している管理策には、セキュリティ ポリシー、アクセス制限、開発環境およびテスト環境の分離、サーバー、デスクトップおよびノートパソコン上のマルウェアの検知、E メールに添付されたマルウェアのスキャン、システム適合状況の確認、侵入防止モニタリングおよび侵入時対応、主要な疑わしいイベントに関するログの取得およびアラートの発信、データの種類、EC アプリケーションおよびネットワーク セキュリティに応じた情報取り扱い手順、外部資産の使　用、システムおよびアプリケーションの脆弱性診断が含まれることがありますが、これらに限定されません。 サプライヤーは、サプライヤーの情報セキュリティ プログラムに従って、かつ、必要に応じて、送信中および保存中のデータを暗号化することを要求しています。サプライヤーは、お客様の環境にリモートでアクセスするとき、またはオープン ネットワーク上でお客様のデータを送信するときに、暗号化技術および適切なプロトコル（例：TLS）を使用しています。サプライヤーは、業界で受け入れられている鍵管理の慣行を実行するように設計された承認済みのソリューションに、使用していないサプライヤーの暗号鍵を保管しています。
アクセス制御	サプライヤーは、サプライヤー ネットワークへの不正アクセスを防止するために設計された適切なアクセス制御策を導入しています。また、故意によるものであるかその他の理由によるものであるかを問わず、サプライヤー ネットワークの誤用のリスクを低減するために、「最小特権の原則」および「知る必要性の原則」に従って、アクセスを制御しています。サプライヤーが活用する可能性があるアクセス制御策には、アクセス レビュー、サービス アカウントおよびアプリケーションへの特権アクセスの維持管理、システム レベルでのアクセス権の設定、アクセスに関連するレポートの生成が含まれます。 サプライヤーは、サプライヤー ネットワークのユーザーを識別および認証するために、業界標準の慣行（該当する場合には、二要素認証を含みます）を実行しています。また、サプライヤーは、サプライヤー ネットワーク全体において強固なパスワードの使用を要求しています。さらに、サプライヤーは、（a）サプライヤー ネットワークのユーザーがパスワードを共有すること、メモすること、E メールで送信すること、インスタント メッセンジャーで送信すること、およびいずれかのシステム上で暗号化せずに保存することを禁止し、（b）誤ったパスワードが連続して複数回入力された後に該当するアカウントをロックしています。 サプライヤーがアクセス制御を強化するために必要に応じて実行している業界標準の慣行の例は次のとおりです。 （a）操作がないまま放置されているユーザー セッションの自動的なタイムアウト （b）ユーザー セッションを再開する際の ID とパスワードの要求

	（c）インターネットに接続することがある場合に VPN 接続による保護が実装されており、受け入れられている業界標準のファイアウォールによる外部アクセスからの保護 （d）パスワードを表示または入力する際のパスワードのマスキング（状況に応じて） （e）パスワードを送信する際の、適切かつ業界標準であるパスワードの暗号化
インシデント管理	サプライヤーは、セキュリティ イベントに対する段取りを整備し、セキュリティ イベントに対応し、セキュリティ イベントの影響を管理および最小化するためにインシデント対応フレームワークを活用しています。このフレームワークには、セキュリティ インシデントが発生したときに従うべ き手順が含まれています。かかる手順の内容は次のとおりです。 （a）対応リーダーを配置した社内のインシデント対応チームの設置 （b）調査チームによる根本原因分析の実施と影響を受けた当事者の特定 （c）社内の報告プロセスおよび通知プロセス （d）対応措置および修復計画の文書化 そして （e）インシデント解決後のイベントのレビュー
ビジネス継続性管理	サプライヤーは、合理的に実務上可能な限りすみやかにビジネスの中断から回復し、通常のビジネスの運営を再開するためのビジネス継続計画（以下、「**BCP**」といいます）を維持しています。 サプライヤーは、サプライヤーのお客様に重大な影響が及ぶビジネスの中断が発生した際に、そのような状況下において合理的かつ適時にお客様に連絡することを試みます。