情報セキュリティ管理要件

1. はじめに

マイクロンの経営陣はマイクロンのデータのセキュリティ確保に努めています。

適用範囲
ここに挙げられる情報セキュリティ管理要件は、マイクロンのデータを扱う、処理する、または提供するすべてのサプライヤーに適用されます。

マイクロンのサプライヤー（以下、「**サプライヤー**」）は、マイクロンに代わってアクセスする、提供を受ける、または保管する有形無形のマイクロンの所有物および提供物（以下、「**IT 資産およびマイクロンのデータ**」）を許可されていないアクセス、取得、開示、破壊、改変、偶発的な損失、誤用、毀損から保護しなければなりません。そのためには、情報セキュリティ環境やガバナンスアプローチを含む情報に対して、国際規格である ISO27001 が定める「情報セキュリティ、サイバーセキュリティおよびプライバシー保護 - 情報セキュリティマネジメントシステム - 要求事項」の沿った、またはそれに代わる規格に準じた、業界標準以上に厳格な最良の方法で管理的、物理的、技術的な対策を講じる必要があります。

本情報セキュリティ管理要件は、サプライヤーの標準的なポリシーや手順に取って代わるものではなく、それらの一部として実施すべき最低限の管理要件を定めることを目的としています。サプライヤーはこの要件に従い、以下に詳述される様々な領域で継続的なセキュリティ管理を実施しなければなりません。

2. 定義

IT 資産：コンピューター機器（ラップトップやデスクトップ等）、モバイル機器（携帯電話・スマートフォン、タブレット等）、ハードウェア、ソフトウェア、オペレーティングシステム、ストレージメディア、ネットワークリソース、ID（電子メール、オンラインブラウジング、ファイル転送プロトコルおよびその他の IT サービスへのアクセスに必要となるもの等）、マイクロンの事業を行う目的でマイクロンの取締役、役員、チームメンバー、請負業者またはその他のサードパーティが利用できるコンピューティング環境（開発、テスト、ステージング、本番、バックアップのアプリケーション環境等）が含まれ、かつこれらに限定されません。

マイクロンのデータ：マイクロンが所有する、またはマイクロンがサードパーティから委託された知的財産およびその他の機密・専有データを指します。

個人データ：上述のマイクロンのデータの一部であり、特定された、または特定可能な自然人に関するあらゆる情報を意味します。特定可能な自然人とは、特に氏名、識別番号、位置データ、オンライン識別子、または当該自然人の物理的、生理的、遺伝子的、精神的、経済的、文化的もしくは社会的アイデンティティに特有な一つまたは複数の要素を参照することによって、直接的または間接的に識別され得る者のことです。個人データは適用されるデータ保護法によって定義されます。

マイクロンのインシデント：情報システムもしくは当該システムが処理、保存、送信する情報（マイクロンのデータ）の機密性、完全性、可用性を実際もしくは潜在的に脅かす事象、またはセキュリティに関するポリシーや手順もしくは許容される利用方針に違反するか、違反につながる差し迫った脅威をもたらす事象を指します。

処理：マイクロンのデータの生成、収集、保有、廃棄、操作、加工、受領、送信、保管、保持および開示を「処理」と総称します。

3. 情報セキュリティポリシー

サプライヤーは、マイクロンの情報、資産および関連サービスの受領、送信、加工、保管、管理、配布、読み出し、アクセス、提示、保護を規定する、文書化されたセキュリティポリシーならびに手順一式を管理、維持しなければなりません。

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、ISO27001/27002、あるいはこれらに代わる業界公認の規格またはフレームワークに準拠する情報セキュリティポリシーの枠組みを通じて、IT 資産を包括的な保護するとともにそれに対する責任を明確に負わなければなりません

サプライヤーの情報セキュリティポリシーおよび手順は、少なくとも以下の点を網羅してください。

a) 情報セキュリティに対するサプライヤーのコミットメント

b) 情報の区分、ラベリングおよび操作（マイクロンのデータをサプライヤーまたはサプライヤーの他のクライアントの情報から分離する等）

c) コンピューティングシステム、ネットワーク、メッセージング等の IT 資産の許容可能な利用（同意された目的のみに、規制ができる形で利用する等）

d) 情報セキュリティインシデント管理（侵害の通知、証拠収集への協力やその手順等）

e) ホストおよびネットワークベースのセキュリティ管理（アンチウィルス、IDS：侵入感知システム、IPS：侵入防止システム、ファイヤーウォール、システムハードニング要件等）

f) エンドユーザー、管理者およびシステムの認証要件

g) アクセス制御（リモートアクセスの管理、アクセス権の定期的な見直し等）

h) サプライヤーの本番環境のログ取得および監視（個人データを処理、保管する IT 資産への物理的および論理的アクセス等）

i) 従業員へのプライバシーおよび情報セキュリティに関する適切なトレーニングの提供

j) エンドポイントセキュリティ、保存時、伝送時、使用時のデータを保護するために使用される暗号技術

k) 物的資産を保護するための物理および環境セキュリティの管理

l) データライフサイクル管理、記録維持、要請があった場合のこれらのポリシーおよびその実践を示す書類のマイクロンへの提供

サプライヤーへ合理的な通知を行った後、マイクロンはサプライヤーの情報セキュリティポリシーおよび手順に対して要求、見直し、調査を行うことができるほか、これらの計画に対して合理的な変更を求めることができます。

4. 注意基準

サプライヤーは、マイクロンとの契約期間中、個人データを含むマイクロンのデータを作成、受領したり、これらにアクセスしたりする可能性があることを認識し、これに同意します。サプライヤーは、本マイクロンデータ処理基準に定める内容を遵守し、管理するマイクロンのデータをサプライヤーまたは第三者が不正または違法に処理した場合はこれに責任を負うものとします。

マイクロンのデータにアクセスできる自社のユーザー、請負業者、データ処理業者の作為および不作為について、サプライヤーはマイクロンに対して法律上の責任を含む責任を負わねばならず、また、少なくともサプライヤーが自らのデータを保護するのと同程度に保護しなければなりません。以上を認識した上で、サプライヤーは以下の事項について同意し、誓約するものとします。

a) マイクロンのデータはすべて極秘扱いとし、不正なアクセス、使用、開示の防止に必要な適切な注意を払うこと。

b) マイクロンのデータを法律に違反して作成、収集、受領、アクセス、使用しないこと。

c) マイクロンのデータの使用および開示は、本基準の条件に従ってマイクロンのデータまたはそれらへのアクセスが提供される場合に限り行うものとする。サプライヤー自らの目的やマイクロン以外の者の利益のためにマイクロンのデータを使用、販売、貸与、譲渡、配布、開示したり、利用できるようにしたりする場合は、必ずマイクロンから事前に書面での同意を得ること。

d) AI チャットボット、検索エンジン、不正開示の原因になる可能性のあるツールでのマイクロンのデータの使用を制限すること。

e) 直接間接を問わず、マイクロンのデータをサプライヤー以外の者に開示する場合は、必ずマイクロンから事前に書面での同意を得ることとし、マイクロンのデータを取り扱うサプライヤーのすべての請負業者またはデータ処理業者に対して、本文書に定める義務に従うよう書面により要求すること。

サプライヤーは、テクノロジーおよびサイバーセキュリティのリスク管理プログラムを維持し、少なくとも年 1 回の見直しを行わなければなりません。また、リスク管理プロセスを常に改善し、マイクロンのデータおよび IT 資産のリスクを定期的に特定、評価、管理できるようにしてください。

5. 個人データの保護および取り扱いに関する要件

a) **マイクロンの個人データの機密性**：サプライヤーは、マイクロンとの取引プロセスにおいて収集されるすべての個人データを常に機密情報として扱わなければなりません。**「個人データ」**とは、それ自体または他の情報との組み合わせによって特定の個人を合理的に識別できる情報（氏名、連絡先、勤務地、購買履歴、記述、嗜好、写真、音声記録等）を指します。これらの情報を**「マイクロンの個人データ」**と総称します。

b) **データの最小化と目的の限定**：サプライヤーは、マイクロンに製品またはサービスを提供する自らの役割に関わる権利や義務の遂行に合理的に必要な、合法的な事業目的にのみ、マイクロンの個人データを収集および利用することができます。それ以外の目的でマイクロンの個人データの使用する場合は、必ずマイクロンから事前に書面による許可を得なければなりません。

c) **守秘義務の徹底**：サプライヤーは、マイクロンの個人データを機密情報として扱い、その収集や使用をマイクロンに製品およびサービスを提供するために必要なプロセスのみに限定する義務について、これらのデータを取り扱う従業員、請負業者およびその他のサードパーティに定期的に指導しなければなりません。サプライヤーは、マイクロンの個人データを取り扱う下請け業者あるいはサブプロセッサーに対しても、同様のデータ保護義務を契約により義務づけなければなりません。

d) **プライバシー**：サプライヤーは、法律で認められたデータ主体のプライバシー権に関する要求に適時かつ透明性のある方法で対応するために、マイクロンと協力しなければなりません。サプライヤーは、マイクロンの書面による指示に従い、サプライヤーの履歴やデータリポジトリにあるマイクロンの個人データの写しの提供、修正、削除を行いますが、これはそのデータを元の形式で保持する法律上の義務がある場合にのみ制限されます。そうした保持は法律上の要件が存続する限り行うものとし、その後は削除するものとします。サプライヤーは、マイクロンから事前に書面による承諾を得ずに、マイクロンの個人データを共有あるいは販売してはなりません。

e) **プライバシーに関するインシデント発生時の通知と協力**：サプライヤーは、マイクロンの個人データ情報に対する不正なアクセス、収集、使用、改変、共有、複製、破壊があった場合には速やかに通知し、マイクロンの調査に協力しなければなりません。マイクロンの個人データ情報に関わるインシデントの通知は、security@micron.com に送付してください。

f) **コンプライアンスの証明**：サプライヤーは、マイクロンからの求めに応じて、個人データの保護および取り扱いに関する要件を遵守していることを示す適切な保証書を速やかに提出しなければなりません。マイクロンの個人データを保護する義務は、サプライヤーが現在マイクロンに製品またはサービスを提供しているかどうかに関わらず、サプライヤーあるいはその代理店がマイクロンの個人データを保有する限り効力を有します。

6. 人的資源のセキュリティ

サプライヤーは、多層的な人的資源セキュリティ対策を講じなければなりません。従業員は、個別に本人確認ができるもの（社員証等）の携行、守秘義務契約への署名、サプライヤーの倫理規定またはそれに相当するものの年 1 回の確認が求められます。さらに、指紋、犯罪歴、信用履歴、薬物スクリーニング、リファレンスチェック等法律上認められている範囲内の包括的なバックグラウンドチェックを受けなければなりません。

サプライヤーは、機密情報や顧客データの適切な使用と取り扱いに関する情報セキュリティ研修を年 1 回受講することを従業員に義務づけ、受講を完了したことを記録してください。また、すべての従業員に対して自社の情報セキュリティポリシーの理解と遵守を義務づけてください。

7. システムの取得、開発、保守

サプライヤーは、開発ライフサイクル全体にセキュリティ対策を講じた安全な開発方法を維持しなければなりません。これにはアプリケーション開発方針、アプリケーション開発者向けセキュリティ研修、外部向けウェブアプリケーションのセキュアコードレビューおよびペネトレーションテストが含まれます。
サプライヤーは、システムの取得、開発、保守プロセスの一環として以下のことを行ってください。

a) 開発、設定するアプリケーションおよびデータベースを、マイクロンのデータの機密性、完全性、可用性を保護できるように設計すること。

b) OWASP（The Open Web Application Security Project）Top 10 等のセキュリティのベストプラクティスに準拠するウェブアプリケーションを開発し、それが OWASP Top 10 で指摘されている脆弱性への対策が講じられていることを検証する合理的な手順を踏むこと

c) 本番、開発、テストそれぞれに個別の環境を用意すること。

d) 自動スキャンツールおよび手動分析を使用し、オープンソースレビューを含むセキュアコードレビュー、ペネトレーションテストまたは同等のテストを少なくとも年1回実施すること。サプライヤーは、リスクに応じて修正の優先順位を定めた文書化されたポリシーに従い、特定された脆弱性に確実に対処しなければなりません。

e) 文書化されたアクセス制限の手順に従ってソースコードを管理し、デプロイ前にコードの完全性を検証すること。

8. 資産管理

サプライヤーは、情報およびあらゆるタイプのメディアの作成から処理、保管、廃棄に至るまで、その分類、ラベリング、取り扱い、廃棄方法について従業員に教育するための情報セキュリティプログラムを実施しなければなりません。

情報の種類ごとに配布、言及、メール送付、コピー、ファックス送付、保管等における適切な取扱方法を指示してください。

サプライヤーは以下のことを行ってください。

a) IT 資産の棚卸しと関連する資産のライフサイクル管理を継続的に実施する。IT 資産が合意された目的以外に使用されないようにする。

b) 個人データを含むマイクロンのデータの取り扱い、処理、保管を行う際には、業界標準および適用される規制に従う。

c) 米国国防総省、NIST の 800-88 またはこれと同等の規格、その他の後継規格等、最新の業界標準に従った手順でメディアをサニタイズし安全に破壊する。

d) サプライヤーのマイクロンとの業務が完了もしくは終了した場合、またはマイクロンの要求により、サプライヤーは電子的または非電子的形式のいずれかを問わず、バックアップコピー、アーカイブコピー等マイクロンの情報を複写したものをす

べてサニタイズし、安全に破壊（もしくは要求によりマイクロンに返却）し、返却や破壊についてマイクロンが許容できるだけの詳細を記した証明書を、サプライヤーの担当者の署名を付して提出する。

9. アクセス制御

サプライヤーは、合理的なアクセスポリシーおよびアクセス制御（ID およびアクセスを管理、認証するメカニズム）を維持し、許可された者のみがマイクロンのデータにアクセスできるようにしなければなりません。正規のアクセス管理システムを通じてアクセス要求を監視、承認してください。また、アクセスは最小権限と職務分掌の考え方に基づいて付与され、業務上必要な者に限定されなければなりません。

サプライヤーはアクセス制御の一環として以下のことを行ってください。

a) 識別子を利用してアクセスを論理的に制限し、サプライヤーの他のクライアントがマイクロンのデータを閲覧したり、これにアクセスしたりできないようにすること。

b) アクセスできる者が退職した場合は速やかに、またアクセスが不要な職務に社内異動した場合は商業上合理的な期間内に、そのアクセスを無効化すること。

c) ユーザーアカウントとその特権の定期的な見直しによってアクセスが職務内容に照らして適切であることを確認し、不要となったアクセスを削除すること。

d) 特権アカウントの使用をシステムおよびセキュリティ管理業務を行う権限のある従業員に限定すること。

e) マイクロンのデータへのアクセスが追跡できるようにログを収集、監視、保持すること。

f) システムアカウントはシステム間通信にのみ利用し、ユーザーからのインタラクティブなログインができないように設定すること。

g) IT 資産へのリモートアクセスにはセキュアで暗号化されたソリューションを導入し、権限を与えられた者以外はアクセスできないようにすること。

h) マイクロンのデータへのアクセスが追跡できるようにログを収集、監視、保持すること。

10. 暗号化

サプライヤーの暗号化ポリシーは、最新版の FIPS（Federal Information Processing Standards：連邦情報処理規格）140 に準拠し、マイクロンのデータおよび IT 資産を保護するために使用するあらゆる暗号技術に適用されなければなりません。これには業界標準のアルゴリズムと鍵の長さ、鍵のライフサイクル管理要件、鍵と証明書の検証に関する要件が含まれます。

サプライヤーはマイクロンのデータを保存、伝送時に暗号化するためのポリシー、処理、技術を維持しなければなりません。これにはテープ、リムーバブルメディア、ラップトップ、ネットワークファイル転送、Web トランザクションが含まれます。暗号化は、商用グレードで業界標準の暗号アルゴリズム、プロトコルおよび鍵の強度を用いて行われなければなりません。

サプライヤーはマイクロンと協力し、マイクロンの要望を満たす信頼性の高い、安全な電子データの転送方式を導入してください。

11. 物理および環境セキュリティ

サプライヤーは、IT 資産への物理的なアクセスを管理、制限する物理セキュリティ対策を講じなければなりません。これにはセキュリティを専門とする専任スタッフ、マイクロンのデータの処理および保管専用に確保された安全な制限（重要）区域へのアクセスポイントや駐車エリアを監視できるカメラ、侵入検知および警告機能、適切なアクセス制限システム、訪問者管

理および記録が含まれます。インフラおよび環境管理には電力、温度および湿度のモニタリング、消火システム、無停電電源装置（UPS）、現地の法律および業界標準に従った緊急システムまたはバックアップシステムが含まれ、かつこれらに限定されません。

マイクロンのデータを保管するすべてのデータセンターは、マイクロンが承認した地域のデータセンター内にのみ設置されなければなりません。サプライヤーとマイクロンの間で締結された契約にある他のいかなる規定にも関わらず、ソフトウェア開発、バックオフィス業務、品質保証、生産サポート等技術サポートサービスは北米以外の地域で行うことができます。但し、サプライヤーが米国外で業務を行う場合のセキュリティ管理は現地の規制以上に厳格なものでなければなりません。

12. 運用のセキュリティ

サプライヤーは、マイクロンのデータおよび IT 資産を保護できるように設計されたセキュリティ運用プログラムを検証し継続的に改善することで、これを常に適切な状態に保たなければなりません。サプライヤーはこの運用プログラムの一環として以下のセキュリティ管理を行ってください。

a) データ損失、マルウェア、悪意のある侵入、悪意のあるダウンロードからの保護

b) アンチマルウェアおよびアンチウィルスのシグネチャの適時アップデート

c) 侵入検知システム（IDS）および侵入防止システム（IPS）

d) 許可されていないアクセス、接続、機器、ソフトウェアの監視

e) セキュリティ脆弱性対策プログラム（定期的なネットワーク脆弱性スキャン、パッチ管理、特定されたセキュリティ脆弱性の修正に対するリスクベースの優先順位づけ等）

f) セキュリティイベントを検知し対処するための IT 資産およびセンサーからのセキュリティイベントの収集とその相関分析（シーム：SIEM、Security Incident and Event Management 等）

g) 標準化され、堅牢に構築されたシステムおよびデバイスの実装

h) 従業員のインターネット接続の監視と管理

i) マイクロンのデータのバックアップ（検証済みのバックアップおよび復元手順に従ってサプライヤーの事業継続要件および復旧時間目標を満たすために必要となります）、バックアップされたデータの紛失、損傷、不正アクセスの防止

13. 事業のレジリエンス

サプライヤーは、事業継続性および災害復旧に関する包括的なプログラムを常に準備しておかなければなりません。これには技術や業務の復旧が含まれます。サプライヤーは、電気通信、システム、業務の冗長性による機能停止の防止だけでなく、損失イベントの復旧戦略にも重点を置く必要があります。事業継続および災害復旧プログラムは、サービスプロバイダーとしてサプライヤーに適用される法律上および規制上の要件を遵守していなければなりません。

災害復旧プロセスには訓練、計画、少なくとも年 1 回の重要な技術および業務の復旧の検証が含まれなければなりません。また、事業インパクト分析を行い、施設、人員、技術、サプライチェーンの喪失等の脅威を想定した復旧戦略を策定してください。サプライヤーは、イベント発生中および発生後の復旧計画を維持し、それをマイクロンと共有しなければなりません。その際、システムがイベントの継続的な影響を受けても復旧が可能であることを証明しなければなりません。サプライヤーの事業継続および災害復旧プログラムの成果として、サプライヤーの RTO（Recovery Time Objective：目標復旧時間）および RPO（Recovery Point Objective：目標復旧時点）がマイクロンの RTO および RPO と合致し、両者間のサービスレベル合意書の基本として機能しなければなりません。

14. 情報セキュリティインシデント管理

サプライヤーは文書化された、包括的なサイバーインシデント対応計画を策定し、定期的に検証しなければなりません。この計画は潜在的な脅威の特定、リスクの影響の評価、経営陣へのリスクの報告、事業運営の保護のために設計されるものです。サプライヤーは、情報セキュリティインシデント管理計画の一環として以下のことを行ってください。

a) セキュリティイベントおよび疑わしいインシデントの評価

b) インシデントの封じ込みおよび影響の低減による対応

c) 同様のインシデントの再発リスクを最小化するための対策の特定

d) 証拠保全に関する法的要件に従った調査の実施

e) インシデント管理能力の向上につながる教訓の確認

15. データインシデントもしくは侵害の通知

マイクロンのデータが消失、破壊、損傷、破損したり使用不可能になったりした場合、あるいは許可されていない個人または法人・団体からのアクセスがあった場合（閲覧、複写、改変、開示、送信等）、サプライヤーは適用される契約上あるいは法律上の要件に従い、脆弱性をマイクロンの security@micron.com 宛てに速やかに通知しなければなりません。サプライヤーは、そのようなマイクロンのデータを自ら費用を負担して復元しなければなりません。サプライヤーにおいてセキュリティインシデント、マイクロンのデータに対する不正もしく違法な処理が発覚した場合、サプライヤーは適用される法律、規則、あるいは規制に従い、最長でも 72 時間以内の妥当な時間内にマイクロンにその旨を通知しなければなりません。マイクロンのデータに対して何らかの不正または違法な処理が行われた場合は、その直後から両者が相互に協力して調査を行う必要があります。サプライヤーは、事態の対応にあたるマイクロンに協力しなければなりません。具体的には以下のことが含まれます。

a) 調査に協力すること。

b) 必要に応じて、マイクロンが関連する施設や業務に論理的、物理的、あるいはリモートでアクセスできるようにすること。

c) 事態に関与するサプライヤーの従業員、元従業員、請負業者、サブプロセッサー等との面談を設定すること。

d) 関連する記録、ログ、データ報告の他、すべてのプライバシーおよびデータ保護要件に準拠するために必要な、またはマイクロンが合理的に要求する資料をすべて提供すること。

サプライヤーは、法律または規則に別段の定めがある場合を除き、いかなるセキュリティインシデントもマイクロンの書面による事前の同意なしに第三者に通知してはなりません。サプライヤーはさらに、法律や規制の定めにより、あるいはマイクロンの裁量で、影響を受けた個人、規制当局、法執行機関等にインシデントの通知を行うかどうか（通知の内容や送付方法に関する判断を含む）、インシデントの被害に遭った個人に何らかの救済措置を行うかどうか（救済措置の性質および範囲に関する判断を含む）について、マイクロンのみが決定できることに同意します。

サプライヤーは、本項目に記載のある義務の遂行に関連する妥当な費用をすべて負担しなければなりません。また、作為不作為に関わらず、サプライヤーは自らが引き起こしたインシデントによる損害への対応やその軽減のためにマイクロンが負担する妥当な費用を補填しなければなりません。これには本項目で定めるすべての通知や救済措置の費用が含まれます。サプライヤーは、セキュリティインシデントに関連するすべての文書、記録、その他のデータを維持、保存することに同意します。さらに、マイクロンのデータの使用、開示、保護、維持に関係するマイクロンの権利を保護するためにマイクロンが必要とみなす訴訟、調査、その他の措置において、サプライヤーが費用を負担してマイクロンに全面的に協力することに同意します。

16. 通信のセキュリティ

サプライヤーは、公衆ネットワークおよび無線ネットワーク上を通過するデータの機密性および完全性を確保し、IT 資産を確実に守ることのできる合理的で適切なネットワークセキュリティおよび情報転送管理を維持しなければなりません。これにはファイヤーウォール、侵入検知および防止システム、マルウェア対策、プロキシサーバー、安全なファイル転送技術が含まれます。

サプライヤーは、リスクに応じて VPN へのリモートアクセスおよび特定の基幹インフラストラクチャーコンポーネントの管理に多要素認証を使用してください。また、すべてのネットワークの完全性を保護し、トラフィックを許可された業務関連のものに限定するために、ファイヤーウォールまたはそれと同等のものでネットワークゾーンを分割し、ファイヤーウォールポリシーの年1回の見直しを行ってください。

17. サプライヤーリレーションシップ

サプライヤーは、自社のセキュリティポリシー、ISO 27001 およびその他の業界標準の慣行に基づく包括的なリスク評価を用いて、個人データを含むマイクロンのデータを取り扱うサプライヤーの供給元の定期的な見直し等、サードパーティのリスク管理プログラムを維持しなければなりません。

マイクロンは、サプライヤーとマイクロンの間で締結された契約に基づいて提供されるサービスに関連して、サプライヤーがクラウドサービスプロバイダーを利用する場合があることを認めています。このようにマイクロンのデータを処理、保存するサプライヤーの供給元が提供するサービスについても、サプライヤーは自社でそのサービスを提供した場合と同程度の責任を負います。供給元が提供するサービスがこれに該当する場合、サプライヤーは自社の情報セキュリティに関する義務と整合性のある契約を当該供給元と締結しなければなりません。

18. セキュリティの保証と評価

サプライヤーは年1回、マイクロンからの要求により、ISO27001 の証明書、SOC2 Type2 レポート、またはそれに代わる、もしくは同等の報告書において、適切な情報セキュリティ保護および管理対策が実施されていることを保証しなければなりません。

サプライヤーは、マイクロンからの書面での求めにより、本基準および適用される法律や業界標準への準拠を裏付けるために、マイクロンまたはマイクロンの代理であるサードパーティから提供される情報セキュリティに関する質問票に速やかに、かつ正確に回答する必要があります。この質問票は、本基準に基づいてサプライヤーが取り扱う、またはサプライヤーからマイクロンに提供されるすべてのマイクロンのデータに関連するサプライヤーの業務および情報技術環境を確認するものです。サプライヤーはこのような照会に全面的に協力しなければなりません。マイクロンは、セキュリティに関する質問票においてサプライヤーから提供される情報をサプライヤーの機密情報として取り扱います。

マイクロンは、サービスが提供されるサプライヤーのサイト、施設、システム（インフラストラクチャー、ソフトウェア、人員、手順、データ等）およびシステムコンポーネントに関してオンサイトあるいはリモートでセキュリティ評価（以下、「**セキュリティ評価**」）を行います。その場合、対象にはサプライヤーのすべての供給元、下請業者、再受託会社が含まれます。このセキュリティ評価で、マイクロンはできる限りサプライヤーの業務を妨げたり中断させたりしないようにし、年1回に限り実施し、少なくとも 90 日前までに書面で通知をした上で通常の業務時間中に行うものとします。サプライヤーがセキュリティ評価および監査のために費やす時間は無償でマイクロンに提供されなければなりません。マイクロンは、サプライヤーの他の顧客やクライアントのデータまたは情報、サプライヤーの専有データ（サプライヤーとそのクライアント双方のデータ保護のための制限を侵害する可能性のある情報）、本セキュリティ評価の目的と無関係のその他の機密情報を閲覧することはできません。また、セキュリティ管理の検証または実行を再実施したり、監視したりすることもできません。

セキュリティ評価は合理的な長さで、対象範囲について相互に合意したものでなければなりません。マイクロンは、自社のデータ保護のための管理手段全体を合理的に保証する適切な情報セキュリティの保護や管理が実施されているかどうかを示すものとして、まず既存の SOC2 Type2 のサービス監査人レポート、ISO27001 の証明書、それに代わるか同等の規

格のレポートを参照します。マイクロンは、サプライヤーのネットワークおよびシステムに論理的にアクセスしてはなりません。また、自由にサプライヤーの施設に入ったり人員に接触したりすることもできません。サプライヤーは、マイクロンの合理的な質問に回答できるセキュリティ担当者を確保してください。マイクロンは、サプライヤーの競合他社（もしくはサプライヤーとマイクロンとの契約に基づくサプライヤーの重要な下請業者）、サプライヤーの第三者サービス監査人または ISO27001 監査人を当該評価の実施に使用してはなりません。マイクロンのサードパーティの代表者はいずれも機密保持および守秘義務契約を締結し、サプライヤーのセキュリティ要件および機密保持要件に従わなければなりません。マイクロンは、自社の情報、データ、記録を維持するために実施する予防措置と少なくとも同様の措置を講じることで、サプライヤーから得たセキュリティ情報の不適切な開示を防止しなければなりません。マイクロンは、法令に定めのある場合を除き、サプライヤーから得たセキュリティ情報をサプライヤーの書面による事前の許可なしに第三者に対して開示してはなりません。セキュリティ評価において重大なリスクまたは欠陥が発見され、マイクロンとサプライヤーの双方が是正の必要性を認めた場合、両者は是正計画に速やかに合意しなければなりません。その際、サプライヤーは発見された欠陥や重大なリスクを是正するために商業上合理的な努力を払うものとします。