

サプライヤーの情報セキュリティ管理要件

目次

1.	はじめに	1
2.	定義	2
3.	情報セキュリティポリシー	3
4.	注意義務	4
5.	個人データの保護および取り扱いの要件	5
6.	人的資源のセキュリティ	6
7.	責任ある人工知能の使用	6
8.	システムの取得、開発および保守	7
9.	資産管理	8
10.	アクセス制御	9
11.	暗号化	10
12.	物理的および環境的セキュリティ	10
13.	運用セキュリティ	11
14.	事業継続性	12
15.	情報セキュリティインシデント管理	12
16.	データインシデントまたは侵害の通知	13
17.	通信のセキュリティ	14
18.	サプライヤーリレーションシップ	14

1. はじめに

マイクロンでは、IT 資産およびマイクロンデータ（後述の定義参照）のセキュリティ確保に力を注いでいます。

適用範囲

サプライヤーの情報セキュリティ管理要件（以下「**情報セキュリティ管理要件**」）は、IT 資産およびマイクロンデータの取り扱い、処理、または提供に携わるすべてのサプライヤー、ならびに IT 資産およびマイクロンデータを取り扱いまたは処理するソリューションもしくはプラットフォームを提供する、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、IT 資産およびマイクロンデータを、不正なアクセス、取得、開示、破壊、改変、偶発的損失、誤用、または毀損から保護するための、管理上および物理的、技術的な対策を講じ、国際標準化機構（ISO）27001「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」の規格、またはその後継規格に準じた、業界標準以上に厳格な最善の手段を用いるものとします。

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代わるものではなく、サプライヤーの標準的なポリシーや手順の一部として実施すべき最低限の管理要件となるものです。以下に詳述するとおり、サプライヤーは、本要件に従って複数の管理領域を維持するものとします。

本書は、マイクロンとマイクロンのサプライヤーとの間における情報セキュリティおよびリスク管理についての合理的期待と要件をまとめたものです。重要な点として、国際規格（具体的には ISO 27001 および SOC 2 Type II）の遵守が本書に記載の要件を満たす実際的な方法になることが挙げられます。これらの公認された認証や評価フレームワークは、第三者プロバイダーが関与する場合も含め、マイクロンのデータを保護する盤石なセキュリティ対策、リスク管理手法、データ保護措置が整備されていることを示すものです。さらに本書は、現行のセキュリティ評価についてのプロトコルを掘り下げ、特定のリスクまたは不備に対処し、これを是正するための協調的なアプローチに力点を置くことで、マイクロンの情報セキュリティ基準との完全な整合性を確保しています。マイクロンのより機密性の高い情報に関わる状況においては、同社の裁量により、追加のセキュリティ要件が課される場合もあります。

2. 定義

a) **インシデント**：情報システムまたは情報システムが処理するマイクロンデータ（マイクロンの業務に不可欠なデータを含みます）の機密性、完全性、可用性を実際に侵害する、または侵害する可能性のある事象を指します。これには、マイクロンデータへの不正なアクセス、その使用、開示、妨害、改変、または破壊、およびマイクロンのセキュリティポリシー、手順、利用規定の違反または差し迫った違反の恐れがある場合が含まれます。

b) **IT 資産**：コンピューター機器（ノートパソコンやデスクトップ等）、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

ス、ID（E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の提供等）、およびマイクロンが自社の事業を行う目的でその取締役、役員、チームメンバー、請負業者またはその他の第三者に使用させ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、バックアップアプリケーション環境等）を含み、かつこれらに限定されるものではありません。

c) **マイクロンデータ**：マイクロンが所有するか、またはマイクロンが第三者から委託された知的財産およびその他の機密・専有データを含みます。

d) **個人データ**：マイクロン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指します。つまり、特に氏名、識別番号、位置データ、オンライン識別子、または当該人物の物理的、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ひとつもしく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ものを意味します。また、個人データは適用されるデータ保護法によっても定義されます。

e) **処理**：マイクロンデータの生成、収集、保有、廃棄、操作、処理、受領、送信、保管、保持および開示の総称です。

3. 情報セキュリティポリシー

有効な ISO/IEC 27001 認証および/または SOC 2 Type II 保証書を保持するサプライヤーは、かかる認証が以下の条件を満たす場合、マイクロンの一定のセキュリティ要件を満たすものとみなされる場合があります。

- 公認かつ認定された機関によって発行されていること
- 有効かつ最新であること
- マイクロンのサービスまたはデータに実質的に関連する対象範囲のシステム、プロセス、および管理を網羅していること

マイクロンは、その単独の裁量により、かかる認証の妥当性を評価する権利を留保します。該当する場合、サプライヤーはマイクロンのセキュリティ評価プロセスにおいて、重複する証拠の提出を免除されることがあります。

上記の代わりとして、サプライヤーはマイクロンデータ、IT資産、ならびに自社が提供する関連サービスの受領、送信、処理、保管、アクセスおよび保護について規定する文書に基づき、セキュリティポリシーおよび手順を維持し、実施する必要があります。サプライヤーのポリシーおよび手順は、NIST サイバーセキュリティフレームワーク、ISO 27001/27002、または業界で認定され、これらに代わる標準もしくはフレームワークに準拠していなければなりません。

これらのポリシーは、少なくとも以下の管理領域に対応している必要があります。

- 情報セキュリティガバナンスおよび説明責任
- 情報の分類、ラベリング、および取り扱い（データ分離を含みます）
- 許容される IT システムの利用（技術的、管理的制御を伴う合意された目的に限ります）
- インシデントの検知、対応、および違反通知（決められた役割、エビデンスの保全、マイクロンとの協カプロトコルを含みます）
- ネットワークおよびホストのセキュリティ（マルウェア対策、ファイアウォール、IDS/IPS、システム強化、等）
- 認証およびアクセスの管理（定期的なユーザーアクセスレビューを含みます）
- マイクロンデータを処理するシステムのロギングおよびモニタリング（物理的、論理的）
- 従業員向けのセキュリティおよびプライバシー意識向上トレーニング
- 暗号化によるデータ保護（保存時、転送時、使用時）
- 施設の物理的および環境的セキュリティ
- データ保持、廃棄、およびライフサイクルポリシー（要望に応じて提供）

4. 注意義務

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データを作成し、受領し、またはこれにアクセスする必要があることを認識し、これに同意します。サプライヤーは、本書に定める条件を遵守し、サプライヤーまたはそのサードパーティーの不正または違法な処理について責任を負うものとします。

サプライヤーは、マイクロンデータにアクセスする権限を有するユーザー、従業員、請負業者および／またはデータ処理業者の作為および不作為について、マイクロンに対して道義的かつ法的に責任を負うものとします。また、マイクロンデータまたは IT 資産にアクセスする権限を有するすべての関係者との間で、書面による契約を結ばなければなりません。上記の点を認識し、サプライヤーは以下の内容に同意し、誓約するものとします。

- a) マイクロンデータはすべて極秘扱いとし、不正なアクセス、使用または開示の防止に適切な注意を払うこと。
- b) 法律に違反する形でマイクロンデータの作成、収集、受領、使用、またはそれへのアクセスをしないこと。
- c) マイクロンデータの使用および開示は、本書の条件に従ったマイクロンデータまたはそれへのアクセスが提供される目的に限り、かつ排他的に行うこと。マイクロンの書面による事前の同意を得ることなく、サプライヤー自身の目的またはマイクロン以外の者の利益のためにマイクロンデータを使用、販売、貸与、譲渡、配布、またはその他の方法で開示を行ったり、その利用を可能にしたりしないこと。

- 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、マイクロンの書面による事前の同意なく、マイクロンデータをサプライヤーの従業員、請負業者、および／またはデータ処理業者以外の者に開示しないこと。また、マイクロンデータを取り扱うすべてのサプライヤーの請負業者またはデータ処理業者に対して、本書に定める義務を遵守するように書面で要求すること。
- f) サプライヤーの従業員または下請業者に対して、マイクロンのシステムもしくは施設、マイクロンデータ、または IT 資産へのアクセスを付与する場合、マイクロンがサプライヤーに通知するすべての適用方針および手順を該当事業者が遵守し、具体的にサービス提供に必要とされるものを除いて、マイクロンのコンピューターシステム、電子ファイル、ソフトウェア、その他の電子サービスへのアクセスまたはアクセスの試みを行わないように保証すること。サプライヤーの従業員もしくは請負業者が解雇される場合、またはそれらの者がマイクロンへのサービス提供を終了する場合、サプライヤーは当該従業員または請負業者のマイクロンデータおよび IT 資産へのアクセス権限（例：バッジによるアクセス、ログイン等）を停止するために、少なくとも 24 時間前までにマイクロンに通知すること。

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 回はこれを見直すものとします。サプライヤーは、リスク管理プロセスを維持し、マイクロンデータおよび IT 資産のリスクを定期的に特定、評価、管理するものとします。

5. 個人データの保護および取り扱いの要件

- a) **個人データの機密性。** サプライヤーは、マイクロンとの業務の過程において収集したすべての個人データの機密性を保持するものとします。
- b) **データの最小化と目的の限定。** サプライヤーは、個人データの収集および利用については、マイクロンに製品またはサービスを提供するサプライヤーの役割に関連した権利および義務の履行のために合理的に必要かつ正当な事業目的がある場合に限るものとします。マイクロンの書面による事前の許可がない限り、それ以外の個人データの利用は一切認められません。
- c) **守秘義務の徹底。** サプライヤーは、個人データの機密性を維持し、その収集および使用をマイクロンへの製品およびサービスの提供に必要なプロセスに限る義務について、個人データを取り扱う従業員、請負業者およびその他の第三者に定期的に指導するものとします。サプライヤーは、個人データを取り扱うすべての下請業者あるいは下請処理業者について、契約によって同様のデータ保護義務を課すものとします。

- d) **プライバシー**。サプライヤーは、データ主体のプライバシー権に関する適法な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に協力するものとします。サプライヤーは、マイクロンの書面による指示に基づき、サプライヤーの履歴およびデータリポジトリ内の個人データの写しを提供、修正、削除します。ただし、かかる個人データを原型で保持する法的義務がある場合に限り、そのような保持の期間は法律上の要件が存続する限りとし、その後は削除するものとします。サプライヤーは、マイクロンの書面による事前の承諾を得ることなく、個人データを共有または販売しないものとします。
- e) **プライバシーに関するインシデント発生の通知および協力**。サプライヤーは、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、破壊があった場合は速やかにマイクロンに通知し、マイクロンの調査に協力するものとします。個人データ情報に関わるインシデントの通知は、security@micron.com に送付しなければなりません。
- f) **コンプライアンスの証明**。サプライヤーは、マイクロンの求めに応じて、本項（「個人データの保護および取り扱いの要件」）の遵守を示す適切な書面による保証を速やかに提出するものとします。個人データの保護義務は、現時点でサプライヤーがマイクロンに製品またはサービスを提供しているか否かに関わらず、サプライヤーまたはその代理人が個人データを保有している限り有効でなければなりません。

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維持するものとします。従業員は、固有の身分証明書（バッジ等）を携行し、守秘義務契約に署名し、サプライヤーの倫理規定またはそれに相当する規定を毎年確認して、これに同意する必要があります。さらに従業員は、包括的な身元調査を完了する必要があります。これには、法律が認める範囲において、指紋の採取、犯罪歴照会、信用履歴照会、薬物スクリーニング、身元照会を含む場合があります。

サプライヤーは、すべての従業員に対して、機密情報および顧客データの適切な使用および取り扱いに関する情報セキュリティトレーニングを年 1 回受講するよう求め、かかるトレーニングを完了した従業員の記録を維持するものとします。サプライヤーは、サプライヤーの情報セキュリティポリシーの理解およびその遵守を、すべての従業員に確認させるものとします。

7. 責任ある人工知能の使用

マイクロンの事業運営における人工知能（以下「AI」）の責任ある導入および使用を確保するため、サプライヤーはマイクロンへのサポートに関連して AI を使用する場合、以下の事項を遵守するものとします。

- a) 透明性のある AI の使用に努めること。これには、マイクロンに提供する AI 生成資料または制作物について、ラベル付けまたはその他の明確な表示を含む場合があります。
- b) マイクロンの人的資源業務に関する個人データの処理に AI を使用する場合は、マイクロンに通知すること。
- c) サプライヤーまたはその請負業者の AI モデルのトレーニング、またはサプライヤーもしくはその請負業者のデータセット強化のためにマイクロンデータを使用する場合は、マイクロンの書面による事前の同意を得ること。
- d) マイクロン向け、またはマイクロンデータを用いた業務もしくはサービスの分析、処理、開発に際して、データの処理および取り扱いについてはマイクロンが承認した AI ツールのみ使用すること。また、サプライヤーはマイクロンの機密データまたは非公開データについて、未承認または公開の AI ツールおよび／または言語モデルを利用しないこと。承認済みのマイクロンツールの最新リストについては、AI_OPS_CORE@micron.com お問い合わせください。
- e) サプライヤーまたはその請負業者の AI 品質、規制、コンプライアンス管理については透明性を確保すること。サプライヤーは、マイクロンの合理的な求めに応じて、バイアス試験、検証バイアス管理、パフォーマンス管理、および適用される法令または規制の遵守に必要なその他の管理を含む、サプライヤーの AI 品質、規制、およびコンプライアンス管理に関する情報をマイクロンに提供すること。

8. システムの取得、開発および保守

サプライヤーは、開発ライフサイクル全体を通じてセキュリティ対策を講じた安全な開発手法を維持するものとします。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、以下のことを行うものとします。

- a) マイクロンデータの機密性、完全性、および可用性を保護するように設計された方法で、アプリケーションおよびデータベースを開発し、構成すること。
- b) セキュリティのベストプラクティス（OWASP Top 10 等）に従ってウェブアプリケーションを開発し、かかるウェブアプリケーションが OWASP Top 10 の脆弱性に対して保護される設定になっ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、テスト環境を個別に実装すること。
- d) 自動スキャンツールおよび手動分析を用いて、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、リスクに基づく是正の優先順位を定めた文書化されたポリシーに従い、特定された脆弱性が確実に是正されることを保証すること。
- e) アクセスを制限し、デプロイ前にコードの完全性を検証する文書化された手順に従ってソースコードを管理すること。
- f) サプライヤーは、サプライヤーまたはサプライヤーの下請業者がウェブサイト、ポータル、および／またはその他のテクノロジーを用いてサービスを提供する場合、自己の負担により独立した第三者機関にペネトレーションテストを毎年実施させること。サプライヤーは、かかる第三者機関による重大な指摘事項について、速やかに是正すること。マイクロンは、当該テストが完了し、指摘事項が是正されたか否かを検証する権利を有します。

9. 資産管理

サプライヤーは、データライフサイクル全体を通じて、情報の分類、ラベリング、取り扱い、および廃棄方法について、従業員を教育するための情報セキュリティプログラムを実施するものとします。

サプライヤーは従業員に対して、情報の種類別に配布、協議、郵送、複写、ファクシミリ送信、保管等についての適切な取扱方法を指導するものとします。

サプライヤーは、以下のことを実施するものとします。

- a) IT 資産の在庫を管理するとともに、関連する資産ライフサイクルを管理する。
- b) IT 資産が合意された目的にのみ使用されていることを確認する。
- c) 個人データを含むマイクロンデータの取り扱い、処理、保管については、業界標準および適用される規制に従う。

- d) ISO 27001、CMMC Level 2、またはそれらに代わる標準など、現行の業界標準に従った手順でメディアの消去または安全な破壊を行う。
- e) マイクロンに関するサプライヤーの業務が完了もしくは終了した場合、またはマイクロンが要請した場合、サプライヤーは電子的形式または非電子的形式を問わず、バックアップコピーおよびアーカイブコピーを含むマイクロンデータのすべてのコピーを消去し、安全に破壊する（マイクロンの要請があった場合はマイクロンに返却する）。また、サプライヤーの役員が署名し、マイクロンが受諾可能な詳細な内容で当該返却または廃棄について証明する証明書を提出するものとする。

10. 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 およびアクセス管理システムならびに認証メカニズム）を維持し、許可された従業員のみがマイクロンデータへのアクセスを付与されることを確認するものとします。アクセス要求は、正規のアクセス管理システムを通じて追跡し、承認しなければなりません。アクセスは、最小権限および職務分掌の概念に基づいて付与し、業務上の必要がある者に限定し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実施するものとします。

- a) 識別子を利用し、サプライヤーの他の顧客がマイクロンデータを閲覧したりアクセスしたりできないように、論理的にアクセスを制限すること。
- b) 従業員または契約社員の離職後、またはサプライヤーの従業員が当該アクセスを必要としない職務へ内部異動した場合、商業上合理的な期間内に速やかにアクセスを無効化すること。
- c) ユーザーアカウントおよびその特権を定期的に見直し、職務に照らしてアクセスが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、システム管理または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) マイクロンデータへのアクセスを追跡できるように、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、ユーザーからの対話型ログインを防ぐように設定すること。

- g) IT 資産へのリモートアクセスについては、権限を有する個人のみを制限し、安全かつ暗号化されたソリューションを導入すること。

11. 暗号化

サプライヤーは、連邦情報処理規格（FIPS）140 の現行改訂版に準拠し、マイクロンデータおよび IT 資産の保護に使用するすべての暗号技術に適用される暗号化ポリシーを維持するものとします。これには業界標準のアルゴリズムおよび鍵長、鍵のライフサイクル管理の要件、鍵および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、転送中および保存中のマイクロンデータを暗号化するためのポリシー、プロセス、技術を維持するものとします。これにはテープ、リムーバブルメディアデバイス、ノートパソコン、ネットワークファイル転送、およびウェブ取引が含まれます。暗号化は、商用グレードの業界標準の暗号アルゴリズム、プロトコルおよび鍵強度によって提供しなければなりません。

サプライヤーは、マイクロンの要件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するため、マイクロンと協力するものとします。

12. 物理的および環境的セキュリティ

サプライヤーは、以下のことを維持するものとします。

- a) IT 資産への物理的なアクセスを管理、制限する物理的なセキュリティ対策。これには常勤の専門警備員、マイクロンデータの処理および保管専用に確保された安全区域および制限／重要区域へのアクセスポイント、および駐車場をカバーするカメラが含まれます。
- b) 侵入検知および警報機能。
- c) 適切なアクセス制御システム、訪問者管理、および記録。
- d) 人的ミス、火災や水害などの潜在的な環境的危険、または技術的不具合による IT 資産の破壊、紛失、損傷から保護するためのインフラおよび環境的な制御。これには、電力、温度、湿度の監視、消火システム、ユニバーサル電源（UPS）、現地法および業界基準に沿った緊急システムまたはバックアップシステム等が含まれ、かつこれらに限定されません。

- e) サプライヤーは、少なくとも、常時監視、施錠メカニズム、およびデスク整理ポリシーによって物理的資産が保護されていることを保証するものとします。

マイクロ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だけにのみ設置しなければなりません。サプライヤーとマイクロンとの間で締結された契約の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、生産サポートを含み、かつこれらに限定されない技術サポートサービスは北米以外の地域から行うことができます。サプライヤーは、アメリカ合衆国外での業務について、現地の規制と同等またはそれ以上に厳格な管理を維持するものとします。

13. 運用セキュリティ

サプライヤーは、マイクロンデータおよび IT 資産を保護するように設計されたセキュリティ運用プログラムを維持するとともに、これをテストし、継続的に改善するものとします。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維持するものとします。

- a) データ損失、マルウェア、悪意のある侵入、または悪意のあるダウンロードからの保護。
- b) マルウェア対策およびウイルス対策のシグネチャの適宜更新。
- c) 侵入検知システム (IDS) および侵入防止システム (IPS) 。
- d) 不正なアクセス、接続、デバイス、ソフトウェアの監視。
- e) セキュリティ脆弱性プログラム (定期的なネットワーク脆弱性スキャン、パッチ管理、リスクに基づき優先順位付けされた特定のセキュリティ脆弱性の是正を含みます) 。
- f) 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相関分析によるセキュリティイベントの検知および対応 (セキュリティインシデントおよびイベント管理 [SIEM] 等) 。
- g) 標準化および強化されたビルドを使用したシステムおよびデバイスの実装。
- h) サプライヤーの従業員のインターネット接続の監視および管理。

- i) テスト済みのバックアップおよび復元手順に従った、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なマイクロンデータのバックアップ、ならびにバックアップデータの紛失、損傷、および不正アクセスからの保護。
- j) マイクロンデータおよび IT 資産を保存する情報システム（ワークステーション、サーバー、ネットワーク、アプリケーション等）のインストール、設定、運用、維持を行うための安全な変更管理プロセスの運用。

14. 事業継続性

サプライヤーは、技術や業務の復旧を含む包括的な事業継続および災害復旧用プログラムを維持するものとします。サプライヤーは、通信、システム、業務運営の冗長による停止の防止、および損失発生時の復旧戦略の両方に注力するものとします。事業継続および災害復旧用プログラムは、物品またはサービスのプロバイダーとしてサプライヤーに適用される法的および規制上の要件を遵守しなければなりません。

災害復旧プロセスには、少なくとも年 1 回、重要な技術および業務運営の復旧に関する訓練、計画、およびテストを行うことが含まれなければなりません。ビジネスインパクト分析を必ず実施するほか、施設、人員、技術、サプライチェーンの喪失を含むさまざまな脅威を想定した復旧戦略を策定する必要があります。サプライヤーは、イベント発生中または発生後に実行可能な復旧計画を維持し、要求があった場合は当該復旧計画が存在する証拠を提示するものとします。

15. 情報セキュリティインシデント管理

サプライヤーは、潜在的な脅威の特定、リスクの影響評価、経営陣へのリスクの報告、および事業運営の保護のために設計され、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、定期的にテストするものとします。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、以下のことを行うものとします。

- 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めおよび軽減化による対処。
- c) 同種のインシデントの再発リスクを最小化する対策の特定。
- d) 証拠保全に関する法的要件に従った調査の実施。
- e) 全体的なインシデント管理能力の向上に向けた教訓の特定。

16. データインシデントまたは侵害の通知

サプライヤーは、マイクロンデータの紛失、破壊、損傷、破損、使用不能に至る脆弱性が生じた場合、または許可のない個人または団体のアクセス（閲覧、複製、改変、開示、送信等）があった場合、適用される契約上または法的な要件に従い、マイクロンの security@micron.com に速やかに通知するものとします。サプライヤーは、当該マイクロンデータを自己負担によって復元するものとします。サプライヤーは、適用される法令または規制に従い、遅滞なく、かついかなる場合でも、何らかのインシデント、マイクロンデータの不正または違法な処理を認識してから 72 時間以内にマイクロンに通知するものとします。不正または違法なマイクロンデータの処理が行われた場合、当事者は直ちに相互に協力し、かかる事態の調査を行わなければなりません。

サプライヤーは、かかる事態へのマイクロンの対応に協力するものとします。それには以下のことが含まれます。

- a) 調査に協力すること。
- b) マイクロンに対して、影響を受けた施設および業務への論理的、物理的、および遠隔によるアクセスを適宜提供すること。
- c) すべてのプライバシーおよびデータ保護要件の遵守に必要な場合、またはマイクロンの合理的な要求に応じて、関連する記録、ログ、ファイル、データ報告、およびその他の資料を提供すること。

サプライヤーは、法令に別段の定めがある場合を除き、マイクロンの書面による事前の同意を得ることなく、いかなるインシデントについても第三者に通知してはなりません。さらにサプライヤーは、法律もしくは規制の要求またはマイクロンの裁量により、影響を受けた個人、規制当局、法執行機関、その他に対してインシデントの通知を行うか否か（通知内容および送達方法を含みます）、またはインシデントの影響を受けた個人に対して何らかの形での救済措置を行うか否か（かかる救済措置の性質および範囲を含みます）の決定について、マイクロンが単独の権限を有することに同意します。

サプライヤーは、本項に基づく義務の履行に関連するすべての合理的な費用を負担するものとします。またサプライヤーは、作為不作為を問わず、サプライヤーが引き起こしたインシデントに関して、本項に定める通知および何らかの救済措置の費用を含む損害への対応およびその軽減について、マイクロンが負担した合理的な費用をマイクロンに対して補償するものとします。サプライヤーは、インシデントに関わるすべての文書、記録、その他のデータを維持し、保存することに同意します。さらにサプライヤーは、マイクロンデータの使用、開示、保護、および維持に関わ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、またはその他の措置について、自己の費用負担により、マイクロンに全面的に協力することに同意します。紛失または破壊され

たマイクロンデータについて、マイクロンが合理的に設定した期間内にサプライヤーが修正または再生成できない場合、マイクロンは第三者によるデータ復元サービスを受けることができます。サプライヤーはマイクロンの要請に応じて、当該第三者に協力するものとします。サプライヤーは、マイクロンデータの損失がマイクロンの事業またはサプライヤーが提供するサービスに悪影響を及ぼさないように、優先的にこれに取り組むものとします。

17. 通信のセキュリティ

サプライヤーは、公衆ネットワークまたは無線ネットワーク上を経由するデータの機密性および完全性を確保し、IT 資産（ファイアウォール、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を含みます）を確実に保護するように設計された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するものとします。

サプライヤーは、以下の措置を講じるものとします。(i) リスクに基づき、仮想プライベートネットワーク (VPN) へのリモートアクセスおよび特定の基幹インフラコンポーネントの管理に多要素認証を使用すること。(ii) ネットワークの完全性を保護し、許可された業務トラフィックに限定するために、すべてのネットワークについてファイアウォールまたはこれと同等の手段でネットワークゾーンを分離するように設計すること。(iii) ファイアウォールポリシーを年 1 回見直すこと。

18. サプライヤーリレーションシップ

サプライヤーは、サプライヤーのセキュリティポリシー、ISO 27001、およびその他の業界標準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データを取り扱う下位サプライヤーに対する定期的な審査等を行うサードパーティリスク管理プログラムを維持するものとします。

マイクロンは、サプライヤーとマイクロンと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ます。

サプライヤーは、マイクロンからの要求に応じて、ISO 27001 の認証書、SOC 2 Type II 報告書、またはそれらと同等かそれ以上の基準を有する年次報告書において、適切な情報セキュリティの保護および管理対策が実施されていることを保証するものとします。

サプライヤーは、適用される法律および業界標準に加えて本基準の遵守を確認するため、マイクロンからの書面による要求に応じて、本基準に基づいてサプライヤーが取り扱うマイクロンデータ、または同社がマイクロンに提供するサービス、またその両方に関連するサプライヤーの業務慣行および情報技術環境について、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ーによる情報セキュリティ質問票に、迅速かつ正確に回答するものとし

ます。サプライヤーは、かかる照会に全面的に協力するものとします。マイクロンは、セキュリティ質問票を通じてサプライヤーが提供する情報を、サプライヤーの機密情報として取り扱うものとします。

マイクロンが、サプライヤーのサイト、施設、システム（インフラ、ソフトウェア、人員、手順、データを含みます）、およびサービス提供の起点または経由地点であるシステム構成要素（サプライヤーのすべての供給業者、下請業者、下請サービス業者を含みます）についてオンサイトまたは遠隔によるセキュリティ評価（以下「**セキュリティ評価**」）を行う場合、マイクロンはサプライヤーの業務の支障および混乱を最小限に抑えつつ、通常の営業時間内に、年 1 回を超えない頻度により、また少なくとも 90 日前までに書面による通知を行った上で、当該のセキュリティ評価を行うものとします。サプライヤーが負担するセキュリティ評価の時間は、無償でマイクロンに提供されるものとします。マイクロンは、サプライヤーのその他の顧客もしくはクライアントに関するデータもしくは情報、サプライヤーの専有データ（サプライヤーおよびサプライヤーのクライアント双方のデータを保護する管理体制を損ない得る情報）、またはセキュリティ評価の目的に関係のないその他の機密情報を閲覧することはできません。また、管理のテストもしくは実行を再実施または観察することはできません。

セキュリティ評価は、合理的な長さおよび相互に合意した範囲でなければなりません。マイクロンは、まず既存の SOC 2 Type II サービス監査報告書、ISO 27001 認証書、またはそれらと同等かそれ以上の基準による報告書を参照し、マイクロンデータの保護に関する管理体制についての合理的な保証を得るために、適切な情報セキュリティ保護策および管理が実施されていることを確認するものとします。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への論理的なアクセスならびにサプライヤーの施設および人員への無制限な物理的アクセスを行ってはなりません。サプライヤーは、マイクロンの合理的な質問に対応するためにセキュリティ担当者を設置するものとします。マイクロンは、かかる評価の実施において、サプライヤーの競合他社（またはサプライヤーとマイクロンとの間の契約に基づくサプライヤーの主要な下請業者）、サプライヤーの第三者サービス監査人、または ISO27001 監査人を使用しません。マイクロンのサードパーティー代表者は、いずれも機密保持契約および非開示契約を締結し、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、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ぐために、少なくとも自社の情報、データ、記録の保持に用いる措置と同様の保護措置を維持するものとします。マイクロンは、法律で要求される場合を除き（そのような場合、マイクロンはかかる要求についてサプライヤーに書面で通知するものとします）、サプライヤーの書面による事前の許可なしに、サプライヤーから得たセキュリティ情報をいかなる第三者にも開示しないものとします。セキュリティ評価でマイクロンが重大なリスクまたは欠陥を特定し、かかるリスクの是正が必要だと両当事者が合意した場合、マイクロンおよびサプライヤーは迅速かつ相互に、時間枠を含む是正計画に合意するものとします。サプライヤーは、発見された欠陥または重大なリスクを是正するために、商業的に合理的な努力を行うものとします。

さらに、マイクロンの要請があった場合、サプライヤーは SOC 2 報告書（または機能的にそれと同等のもの）の完成からマイクロンの会計年度末までの期間に、当該報告書の対象となる管理体制、手順、システムについて

当該期間中に実施した変更内容（もしあれば）を記載した書面による証明書を提出し、マイクロンが当該報告書によって自社の監査およびコンプライアンス要件を満たすことができるようにします。

本書に定めるいずれかの要件の遵守をサプライヤーが怠っているとマイクロンが判断した場合、またはサプライヤーが本書の条件について遵守を確認するための監査報告書もしくはその他の要求に応じなかった場合、マイクロンは違約金および費用を負担することなく以下の権利を有するものとします。(i) 追加のセキュリティ評価を実施し、サプライヤーがこれらの情報セキュリティ管理要件を遵守していることを確認する、および／または (ii) サービスを停止もしくは解除する、またはマイクロンの選択によって支払いを保留する。サプライヤーは、当該停止または解除に関連して適用される解約手数料または未払料金の請求を放棄します。