



欧州委員会

ブリュッセル, 17.10.2024 C(2024)  
7151 final

附属書

## 附属書

### 欧州委員会施行規則

に対して、次のようになる。

サイバーセキュリティリスク管理措置の技術的および方法論的要件に関する指令 (EU) 2022/2555 の適用に関する規則を定め、DNS サービス・プロバイダ、TLD ネーム・レジストリ、クラウドコンピューティング・サービス・プロバイダ、データセンターサービス・プロバイダ、コンテンツ配信ネットワークプロバイダ、マネージドサービス・プロバイダ、マネージドセキュリティサービス・プロバイダ、オンラインマーケットプレイス、オンライン検索エンジン、ソーシャルネットワーキングサービス・プラットフォームに関して、重要インシデントとみなされる場合のさらなる詳細を規定する、

## 附属書

### 本規則第 2 条に言及する技術的および方法論的要件

1. ネットワークと情報システムのセキュリティに関する方針（指令（EU）2022/2555 第 21 条（2）項（a））
  - 1.1. ネットワークと情報システムのセキュリティに関する方針
    - 1.1.1. 指令(EU)2022/2555 の第 21 条(2)項(a)については、ネットワークと情報システムのセキュリティに関する方針を定める：
      - (a) 関連システムおよび情報システムを定める；
      - (b) 関連する戦略と目標に適切であり、それを補完するものでなければならない；
      - (c) ネットワークと情報セキュリティの目標を定める；
      - (d) には、ネットワークと情報システムのセキュリティの継続的改善へのコミットメントを含む；
      - (e) 必要なスタッフ、財源、プロセス、ツール、テクノロジーなど、その実施に必要な適切なリソースを提供することを約束する；
      - (f) 関連する従業員および関連する外部関係者に伝達され、認知される。
      - (g) 1.2.に従い、役割と責任を明確にする；
      - (h) 保管すべき文書とその保管期間を記載する；
      - (i) トピック固有のポリシーを列挙する；
      - (j) ネットワークと情報セキュリティの成熟度の現状と、その実施状況を監視するための指標と対策を策定する；
      - (k) は、関連事業体のマネジメント陣（マネジメント陣）による正式承認の日付を示す。
    - 1.1.2. ネットワークと情報システムのセキュリティ・ポリシーは、少なくとも年 1 回、また、重要インシデントが発生したとき、または、運用やリスクに重要な変更が生じたときに、経営陣によりレビューされ、必要に応じて更新されるものとする。レビューの結果は文書化するものとする。

## 1.2. 役割、責任、認可

- 1.2.1. 1.1.で言及したネットワークと情報システムのセキュリティに関する方針の一環として、関連事業体は、ネットワークと情報システムのセキュリティに関する責任と権限を定め、役割に割り当て、関連団体に従って割り当てるものとする。
- 1.2.2. 関連事業体は、すべての従業員及びサードパーティに対し、関連事業体の確立されたネットワークと情報セキュリティポリシー、トピック別ポリシー及び手順に従い、ネットワークと情報システムのセキュリティを適用することを要求しなければならない。
- 1.2.3. 少なくとも1名は、ネットワークと情報システムのセキュリティに関する事項について、マネジメント陣に直接報告する。
- 1.2.4. 関連事業体の規模に応じて、ネットワークと情報システムのセキュリティは、専用の役割または既存の役割に加えて遂行される職務によってカバーされなければならない。
- 1.2.5. 矛盾する職務および矛盾する責任範囲は、該当する場合、分離されなければならない。
- 1.2.6. 役割、責任、権限は、計画された間隔で、また、重要インシデントや業務またはリスクに重要な変更が生じた場合に、マネジメント団体により見直され、必要に応じて更新されるものとする。

## 2. リスクマネジメント方針（指令（EU）2022/2555 第 21 条 2 項(a)）

### 2.1. リスクマネジメントの枠組み

- 2.1.1. 指令(EU)2022/2555 の第 21 条(2)項(a)を目的として、関連事業体は、ネットワークと情報システムのセキュリティにもたらされるリスクを特定し、対処するための適切なリスクマネジメントの枠組みを確立し、維持しなければならない。関連事業体は、リスクアセスメントを実施・文書化し、その結果に基づき、リスク処理計画を策定・実施・監視するものとする。リスクアセスメントの結果および残存リスクは、関連事業体がマネジメント団体への適切な報告を確保することを条件として、マネジメント団体、または、該当する場合には、説明責任を有し、リスクを管理する認可を有する者によって受け入れられなければならない。
- 2.1.2. 2.1.1.の目的のために、関連事業体は、リスクの特定、分析、アセスメント及び処置のための手順（サイバーセキュリティ・リスクマネジメント・プロセス）を確立しなければならない。サイバーセキュリティ・リスクマネジメント・プロセスは、該当する場合には、関連事業体の全体的なリスクマネジメントプロセスの不可欠な一部でなければならない。サイバーセキュリティ・リスクマネジメント・プロセスの一環として、関連事業体は以下のことを行わなければならない：

- (a) リスクマネジメントの方法論に従う；
- (b) 関連事業体のリスク選好度に従って、リスク許容度を設定する；
- (c) 関連するリスク規準を設定し、維持する；
- (d) オール・ハザード・アプローチに従い、ネットワークと情報システムのセキュリティ、特にサードパーティに 関連するリスク、および単一障害点の特定を含むネットワーク と情報システムの可用性、完全性、識別性、機密性の中断 につながるリスクを特定し、文書化する；
- (e) サイバー脅威インテリジェンスと脆弱性を考慮し、脅威、可能性、影響、リスクレベルなど、ネットワークと情報システムのセキュリティにもたらされるリスクを分析する；
- (f) 識別されたリスクをリスク規準に基づいて評価する；
- (g) 適切なリスク治療の選択肢と対策を特定し、優先順位をつける；
- (h) リスク処理措置の実施を継続的に監視する；
- (i) リスク処置の実施責任者と実施時期を特定する；
- (j) 選択したリスク処理策をリスク処理計画に文書化し、残存リスクを受け入れることを正当化する理由を理解しやすい方法で文書化する。

2.1.3. 適切なリスク処理の選択肢及び対策を特定し、優先順位を決定する際、関連事業体は、リスクアセスメントの結果、サイバーセキュリティリスクマネジメント対策の有効性を評価する手続きの結果、期待される便益に対する実施コスト、12.1.に言及する資産格付け、及び 4.1.3 に言及するビジネスインパクト分析を考慮しなければならない。

2.1.4. 関連事業体は、リスクアセスメント結果及びリスク処置計画を、計画された間隔で、少なくとも年 1 回、また、業務又はリスクに重要な変更が生じたとき、又は重要インシデントが発生したときに、見直し、必要に応じて更新しなければならない。

## 2.2. コンプライアンス・モニタリング

2.2.1. 関連事業体は、ネットワークと情報システムのセキュリティに関する方針、トピック固有の方針、規則、標準の遵守状況を定期的にレビューする。管理団体は、定期的な報告によって、遵守状況のレビューに基づくネットワークおよび情報セキュリティの状況を通知されるものとする。

- 2.2.2. 関連事業体は、その構造、事業環境及び脅威の状況に適した効果的なコンプライアンス報告システムを導入しなければならない。コンプライアンス報告システムは、関連するリスク管理の現状について、情報に基づく見解をマネジメント団体に提供できるものでなければならない。
- 2.2.3. 関連事業体は、計画された間隔で、また、重要インシデントまたは業務もしくはリスクに重要な変化が生じた場合に、コンプライアンス・モニタリングを実施しなければならない。

### **2.3. 情報およびネットワーク・セキュリティの独立審査**

- 2.3.1. 関連事業体は、ネットワークと情報システムのセキュリティを管理するためのアプローチと、人、プロセス、技術を含むその実施方法を独自に見直さなければならない。
- 2.3.2. 関連事業体は、適切な監査能力を有する個人によって実施される独立レビューを実施するためのプロセスを開発し、維持しなければならない。独立したレビューが関連事業体のスタッフによって実施される場合、レビューを実施する者は、レビュー対象分野の担当者の職権ライン上にはならない。関連事業体の規模がそのような権限ラインの分離を許さない場合、関連事業体は、レビューの公平性を保証するための代替措置を講じなければならない。
- 2.3.3. 2.2.に従ったコンプライアンス・モニタリングおよび 7.に従ったモニタリングと測定の結果を含む独立したレビューの結果は、管理団体に報告されなければならない。関連する規準に従い、是正措置を講じるか、または残存リスクを受け入れるものとする。
- 2.3.4. 独立したレビューは、計画された間隔で、また、重要インシデントが発生したとき、または、業務やリスクに重要な変更が生じたときに実施されるものとする。

## **3. インシデントハンドリング (指令 (EU) 2022/2555 第 21 条 (2) 項 (b))**

### **3.1. インシデントハンドリング方針**

- 3.1.1. 指令(EU)2022/2555 の第 21 条(2)項(b)を目的として、関連事業体は、インシデントの検知、分析、封じ込め又は対応、回復、文書化及び報告を適時に行うための役割、責任及び手順を定めたインシデントハンドリングポリシーを策定し、実施するものとする。
- 3.1.2. 3.1.1 の方針は、4.1 の事業継続及び災害復旧計画と首尾一貫していなければならない。方針には以下を含むものとする：
  - (a) 3.4.1.に従って実施された事象のアセスメントおよび分類と一致する、インシデントの分類システム；

- (b) エスカレーションや報告など、効果的なコミュニケーション計画を立てる；
- (c) インシデントを検知し、適切に対応するための役割を、有能な従業員に割り当てる；
- (d) インシデント対応マニュアル、エスカレーションチャート、連絡先リスト、テンプレートなど、インシデントの検知と対応の過程で使用される文書。

3.1.3. 本方針に定められた役割、責任、手続きは、計画された間隔で、また、重要インシデントが発生した後や、業務やリスクに重要な変更があった後に、テスト、見直しを行い、必要に応じて更新するものとする。

## 3.2. モニタリングとロギング

3.2.1. 関連事業体は、インシデントとみなされる可能性のある事象を検知し、影響を緩和するために適宜対応するための手順を定め、ネットワークと情報システム上の活動を監視し、ログに記録するためのツールを使用しなければならない。

3.2.2. 実行可能な範囲で、モニタリングは自動化され、業務能力に応じて継続的または定期的に実施されなければならない。関連事業体は、偽陽性及び偽陰性を最小化する方法でモニタリング活動を実施しなければならない。

3.2.3. 3.2.1.で言及した手続きに基づき、関連事業体は、ログを維持し、文書化し、レビューしなければならない。関連事業体は、2.1.に従って実施されたリスクアセスメントの結果に基づき、ログの記録対象となるアセスメントのリストを確立しなければならない。適切な場合、ログは以下を含むものとする：

- (a) 関連するアウトバウンドおよびインバウンドのネットワークトラフィック；
- (b) 関連情報システムのユーザーの作成、変更、削除、および権限の拡張；
- (c) システムやアプリケーションにアクセスする；
- (d) 認証関連イベント；
- (e) システムおよびアプリケーションへのすべての特権アクセス、および管理者アカウントによって実行される活動；
- (f) 重要な設定ファイルやバックアップファイルへのアクセスや変更を行う；
- (g) イベントログや、アンチウイルス、侵入検知システム、ファイアウォールなどのセキュリティツールからのログ；

- (h) システムリソースの使用と、そのパフォーマンス；
- (i) 施設への物理的アクセス；
- (j) ネットワーク機器やデバイスにアクセスし、それを使用する；
- (k) 各種ログの起動、停止、一時停止
- (l) 環境イベント。

3.2.4. ログは、異常または望ましくない傾向がないか定期的にレビューされなければならない。適切な場合、関連事業者はアラームしきい値に適切な値を設定するものとする。アラームしきい値の設定値を超えた場合、必要に応じて自動的にアラームを作動させなければならない。関連事業者は、アラームが発生した場合、適時に適格かつ適切な対応が開始されるようにしなければならない。

3.2.5. 関連事業者は、予め定義された期間、ログを維持し、バックアップし、不正アクセスまたは変更履歴から保護しなければならない。

3.2.6. 実行可能な範囲で、関連事業者は、イベントアセスメントのためにシステム間のログを関連付けることができるように、すべてのシステムが同期された時間ソースを有することを保証しなければならない。関連事業者は、ログを記録するすべての資産のリストを確立し、保管し、監視及びロギングシステムが冗長であることを保証しなければならない。監視および記録システムの可用性は、それらが監視しているシステムから独立して監視されるものとする。

3.2.7. 手順ならびに記録される資産のリストは、定期的に、また重要なインシデントが発生した後に、見直され、必要に応じて更新されるものとする。

### **3.3. イベント報告**

3.3.1. 関連事業者は、従業員、サプライヤー、顧客が疑わしい事象を報告できるような簡単な仕組みを導入しなければならない。

3.3.2. 関連事業者は、適切な場合、事象報告の仕組みをサプライヤーや顧客に伝え、その仕組みの利用方法を従業員に定期的に教育しなければならない。

### **3.4. イベントのアセスメントと分類**

3.4.1. 関連事業者は、疑わしい事象をアセスメントし、インシデントに該当するかどうかを判断し、該当する場合はその性質と重要性を判断しなければならない。

3.4.2. 3.4.1 項の目的のため、関連事業者は次のように行動しなければならない：

- (a) 事前に定めた規準に基づきアセスメントを実施し、トリアージによってインシデントの封じ込めと根絶の優先順位を決定する；
- (b) 四半期ごとに、本規則第 4 条にいう再発インシデントの有無をアセスメントする；
- (c) イベントの評価と分類のために、適切なログをレビューする；
- (d) ログの相関と分析のプロセスを導入する。
- (e) 新たな情報が入手可能になった場合、または既に入手可能な情報を分析した後、事象を再評価し、再分類する。

### **3.5. インシデント対応**

3.5.1. 関連事業者は、文書化された手順に従い、適時にインシデントに対応しなければならない。

3.5.2. インシデント対応手順は、以下の段階を含むものとする：

- (a) インシデント封じ込め、インシデントの影響が広がるのを防ぐ；
- (b) インシデントの継続や再発を防ぐために、根絶を図る、
- (c) 必要に応じて、インシデントからの回復を図る。

3.5.3. 関連事業者は、コミュニケーション計画及び手順を確立しなければならない：

- (a) インシデント通知に関して、コンピュータ・セキュリティ・インシデント対応チーム（CSIRT）、または認可されている場合は所轄当局と連携する；
- (b) 関連事業者のスタッフ間のコミュニケーション、および関連事業者の外部の関連利害関係者とのコミュニケーションに使用する。

3.5.4. 関連事業者は、3.2.1.で言及した手順に従ってインシデント対応活動を記録し、証拠を記録しなければならない。

3.5.5. 関連事業者は、インシデント対応手順を計画された間隔でテストしなければならない。

### **3.6. インシデント後のレビュー**

3.6.1. 適切な場合、関連事業者は、インシデントからの回復後、ポストインシデントレビューを実施しなければならない。インシデント後のレビューは、可能であれば、インシ

デントの根本原因を特定し、将来のインシデントの発生と結果を低減するための教訓を文書化するものとする。

3.6.2. 関連事業体は、インシデント発生後のレビューが、ネットワーク及び情報セキュリティ、リスク処理措置、並びにインシデントハンドリング、検知及び対応手順へのアプローチの改善に資することを確実にしなければならない。

3.6.3. インシデントがインシデント後のレビューにつながった場合、関連事業体は計画された間隔でレビューを行わなければならない。

#### **4. 事業継続と危機管理（指令（EU）2022/2555 第 21 条 2 項(c)**

##### **4.1. 事業継続と災害復旧計画**

4.1.1. 指令(EU)2022/2555の第21条(2)項(c)を目的として、関連事業体は、インシデント発生時に適用する事業継続計画および災害復旧計画を策定し、維持するものとする。

4.1.2. 関連事業体の業務は、事業継続及び災害復旧計画に従って復旧されなければならない。この計画は、2.1 に従って実施されたリスクアセスメントの結果に基づくものとし、適切な場合には以下を含むものとする：

- (a) 目的、範囲、読者；
- (b) 役割と責任
- (c) 主要な連絡先と（社内外の）コミュニケーション・チャネル；
- (d) プランの有効化と無効化の条件
- (e) 手術の回復順序
- (f) 復旧目標を含む、特定の業務に関する復旧計画；
- (g) バックアップや冗長性など、必要なリソースを確保する；
- (h) 一時的な措置から活動を回復し、再開する。

4.1.3. 関連事業体は、事業運営に対する深刻な中断の潜在的影響を評価するために事業影響分析を実施し、事業影響分析の結果に基づいて、ネットワークと情報システムの継続性要件を確立しなければならない。

4.1.4. 事業継続計画及び災害復旧計画は、計画された間隔で、かつ、重要インシデント又は業務若しくはリスクの重要な変化の後に、テストし、レビューし、必要に応じて更新

しなければならない。関連事業体は、かかるテストから得られた教訓を計画に盛り込むことを確実にしなければならない。

## 4.2. バックアップと冗長性管理

4.2.1. 関連事業体は、適切なレベルの冗長性を確保するために、データのバックアップコピーを維持し、設備、ネットワークと情報システム、スタッフを含む十分な利用可能なリソースを提供しなければならない。

4.2.2. 2.1 に従って実施されたリスクアセスメントの結果及び事業継続計画に基づき、関連事業体は、以下を含むバックアップ計画を策定しなければならない：

- (a) 回復には時間がかかる；
- (b) クラウドコンピューティング・サービス環境に保存されている構成データおよびデータを含め、バックアップコピーが完全かつ正確であることを保証する；
- (c) バックアップ・コピー（オンラインまたはオフライン）を、システムと同じネットワーク内になく、メイン・サイトでの災害による損害を免れるのに十分な距離にある安全な場所に保管する；
- (d) 資産の格付けレベルに従い、バックアップ・コピーに対する適切な物理的・論理的アクセス管理を行う；
- (e) バックアップ・コピーからデータを復元する；
- (f) ビジネスおよび規制要件に基づく保存期間。

4.2.3. 関連事業体は、バックアップコピーの完全性チェックを定期的実施しなければならない。

4.2.4. 2.1 に従って実施されたリスクアセスメントの結果及び事業継続計画に基づいて、関連事業体は、次の少なくとも部分的な冗長化によって、資源の十分な可用性を確保しなければならない：

- (a) ネットワークと情報システム；
- (b) 施設、設備、備品などの資産を含む；
- (c) 必要な責任、認可、能力を持つ人員；
- (d) 適切なコミュニケーション・チャンネルを持つ。

4.2.5. 適切な場合、関連事業者は、施設、システム及び要員を含む資源の監視及び調整が、バックアップ及び冗長性要件から正当に情報を得ていることを確実にしなければならない。

4.2.6. 関連事業者は、バックアップコピー及び冗長化の復旧テストを定期的実施し、復旧状況において、バックアップコピー及び冗長化が信頼でき、効果的な復旧を行うためのコピー、プロセス及び知識を網羅していることを確認しなければならない。関連事業者は、テストの結果を文書化し、必要に応じて是正措置を講じなければならない。

### 4.3. 危機管理

4.3.1. 関連事業者は、危機管理のためのプロセスを整備しなければならない。

4.3.2. 関連事業者は、危機管理プロセスが少なくとも以下の要素に対処していることを保証しなければならない：

(a) 要員、および必要に応じてサプライヤーやサービスプロバイダの役割と責任について、具体的な手順を含め、危機的状況における役割分担を明記する；

(b) 関連事業者と所轄官庁との間の適切なコミュニケーション手段；

(c) 危機的状況において、ネットワークと情報システムのセキュリティを確実に保守するための適切な手段を適用すること。

(b)の目的上、関連事業者と関連主管庁との間の情報の流れには、インシデント報告や関連するタイムラインなどの認可を要するコミュニケーションと、認可を要しないコミュニケーションの両方が含まれるものとする。

4.3.3. 関連事業者は、インシデント、脆弱性、脅威、又は可能な軽減策に関して、CSIRT又は、認可されている場合、管轄当局から受領した情報を管理し、利用するためのプロセスを実施しなければならない。

4.3.4. 関連事業者は、定期的に、または重要インシデントが発生した後、あるいは業務やリスクに重要な変化が生じた後に、危機マネジメント計画をテストし、見直し、必要に応じて更新しなければならない。

## 5. サプライチェーンの安全保障（指令（EU）2022/2555 第 21 条 2 項（d））

### 5.1. サプライチェーンのセキュリティ方針

5.1.1. 指令(EU)2022/2555 の第 21 条(2)の(d)項を目的として、関連事業者は、ネットワークと情報システムのセキュリティに対する特定されたリスクを軽減するために、直接のサプライヤー及びサービスプロバイダとの関係を規定するサプライチェーン・セ

セキュリティポリシーを確立し、実施し、適用しなければならない。サプライチェーン・セキュリティポリシーにおいて、関連事業体は、サプライチェーンにおける自らの役割を特定し、それを直接のサプライヤー及びサービスプロバイダに伝えなければならない。

5.1.2. 5.1.1 で言及したサプライチェーン・セキュリティポリシーの一環として、関連事業体は、サプライヤー及びサービスプロバイダを選定し、契約するための規準を定めなければならない。これらの規準には、以下を含むものとする：

- (a) 安全な開発手順など、サプライヤーやサービスプロバイダのサイバーセキュリティ慣行；
- (b) サプライヤーやサービスプロバイダが、関連事業体によって設定されたサイバーセキュリティ仕様を満たす能力；
- (c) ICT 製品および ICT サービスのリスクおよび格付けレベルを含め、ICT 製品および ICT サービスの全体的な品質およびレジリエンス、ならびにそれらに組み込まれたサイバーセキュリティリスク管理対策；
- (d) 該当する場合は、関連事業体が供給源を多様化し、ベンダーの囲い込みを制限する能力。

5.1.3. サプライチェーン・セキュリティポリシーを確立する際、関連事業体は、該当する場合、指令 (EU) 2022/2555 の第 22 条(1)に従って実施された重要サプライチェーンの協調セキュリティリスクアセスメントの結果を考慮しなければならない。

5.1.4. サプライチェーン・セキュリティポリシーに基づき、かつ、附属書 2.1.に従って実施されたリスクアセスメントの結果を考慮し、関連事業体は、サプライヤー及びサービスプロバイダとの契約において、適切な場合にはサービスレベル合意を通じて、次の事項を明記することを確実にしなければならない：

- (a) 6.1.に定める ICT サービス又は ICT 製品の取得におけるセキュリティに関する要件を含む、供給者又はサービスプロバイダに対するサイバーセキュリティ要件；
- (b) サプライヤーに求められる意識、スキル向上およびトレーニング、そして適切な場合には認証に関する要件。
- (c) サプライヤーおよびサービスプロバイダの経歴検証に関する要件

- (d) サプライヤーとサービスプロバイダは、関連事業体のネットワークと情報システムのセキュリティにリスクをもたらすインシデントが発生した場合、不当な遅滞なく関連事業体に通知する義務を負う；
- (e) 監査権または監査報告を受ける権利；
- (f) 関連事業体のネットワークと情報システムのセキュリティにリスクをもたらす脆弱性に対処する義務を、サプライヤーとサービスプロバイダに課す；
- (g) 下請けに関する要件、及び、関連事業体が下請けを認めている場合には、(a)で言及したサイバーセキュリティ要件に従った下請け業者に対するサイバーセキュリティ要件；
- (h) 契約終了時にサプライヤーおよびサービスプロバイダに課される義務、例えば、サプライヤーおよびサービスプロバイダがその業務を遂行する上で入手した情報の回収および廃棄など。

5.1.5. 関連事業体は、新たな供給者及びサービスプロバイダの選定プロセスの一環として、また、6.1.項で言及する調達プロセスの一環として、5.1.2 項及び 5.1.3 項で言及する要素を考慮しなければならない。

5.1.6. 関連事業体は、サプライチェーン・セキュリティポリシーを見直し、サプライヤ及びサービスプロバイダのサイバーセキュリティ慣行の変化を、計画された間隔で、また、ICT サービスの提供に関連する又はサプライヤ及びサービスプロバイダからの ICT 製品のセキュリティに影響を及ぼす業務又はリスク又は重要インシデントに重要な変化が生じたときに、監視し、評価し、必要に応じて対応しなければならない。

5.1.7. 5.1.6.の目的のため、関連事業体は次のことを行わなければならない：

- (a) 該当する場合は、サービスレベル協定の実施に関する報告書を定期的に監視する；
- (b) サプライヤーおよびプロバイダからの ICT 製品および ICT サービスに関するインシデントを検証する；
- (c) 予定外のレビューの必要性をアセスメントし、その結果をわかりやすく文書化する；
- (d) サプライヤーおよびサービスプロバイダからの ICT 製品および ICT サービスに関連する変更をもたらすリスクを分析し、適切な場合には、適時に低減措置を講じる。

## 5.2. サプライヤーとサービスプロバイダのディレクトリ

関連事業体は、以下を含む、直接のサプライヤーおよびサービスプロバイダの登録簿を維持し、最新の状態に保たなければならない：

- (a) 各直接サプライヤーおよびサービスプロバイダの連絡先；
- (b) 直接のサプライヤーまたはサービスプロバイダが関連事業体に提供する ICT 製品、ICT サービス、および ICT プロセスのリスト。

## 6. ネットワークと情報システムの取得、開発、保守におけるセキュリティ（指令（EU）2022/2555 第 21 条 2 項（e））

### 6.1. ICT サービスまたは ICT 製品の取得におけるセキュリティ

6.1.1. 指令(EU)2022/2555 の第 21 条 2 項(e)項を目的として、関連 事業体は、第 2.1 項に従って実施された リスク アセスメントに基づき、関連事業体のネットワークおよび情報システムのセキュリティにとって 重要なコンポーネントの ICT サービスまたは ICT 製品を、そのライフサイクルを通じて 供給者またはサービス提供者から 取得することから生じるリスクを管理するためのプロセスを設定し、実施しなければならない。

6.1.2. 6.1.1.の目的上、6.1.1.で言及されるプロセスには、次のものを含むものとする：

- (a) 取得する ICT サービスまたは ICT 製品に適用されるセキュリティ要件；
- (b) ICT サービスまたは ICT 製品の全使用期間を通じて、またはサポート期間終了後の交換期間を通じて、セキュリティ更新に関する要件を満たすこと；
- (c) ICT サービスまたは ICT 製品に使用されるハードウェアおよびソフトウェア・コンポーネントを説明する情報；
- (d) ICT サービス又は ICT 製品の実装されたサイバーセキュリティ機能及びそれらの安全な運用に必要な構成を記述する情報；
- (e) ICT サービスまたは ICT 製品が(a)に従ったセキュリティ要件に準拠していることを保証する；
- (f) 提供された ICT サービス又は ICT 製品が規定のセキュリティ要件に適合していることを妥当性確認するための方法、及び妥当性確認の結果の文書化。

6.1.3. 関連事業体は、計画された間隔で、また、重要インシデントが発生したときに、プロセスを見直し、必要に応じて更新しなければならない。

## 6.2. 安全な開発ライフサイクル

6.2.1. 関連事業体は、ソフトウェアを含むネットワークと情報システムを開発する前に、ネットワークと情報システムのセキュリティ開発に関する規則を定め、ネットワークと情報システムを自社で開発する場合、またはネットワークと情報システムの開発を外部に委託する場合に適用しなければならない。ルールは、仕様、設計、開発、実装、テストを含むすべての開発フェーズを対象とする。

6.2.2. 6.2.1.の目的のために、関連事業体は次のことを行わなければならない：

- (a) 関連事業体又は関連事業体に代わって行う開発又は取得プロジェクトの仕様及び設計段階において、セキュリティ要件の分析を実施する；
- (b) サイバーセキュリティ・バイ・デザインやゼロ・トラスト・アーキテクチャの推進など、あらゆる情報システム開発活動にセキュアシステムエンジニアリングの原則やセキュアコーディングの原則を適用する；
- (c) 開発環境に関するセキュリティ要件を定める；
- (d) 開発ライフサイクルにおけるセキュリティテストプロセスを確立し、実施する；
- (e) セキュリティテストデータを適切に選択し、保護し、管理する；
- (f) 2.1に従って実施されたリスクアセスメントに従い、検査データをサニタイズし、匿名化する。

6.2.3. ネットワークと情報システムの開発を外部に委託する場合、関連事業体は、ポイント5と6.1で言及した方針と手順も適用しなければならない。

6.2.4. 関連事業体は、計画された間隔で安全開発規程を見直し、必要に応じて更新しなければならない。

## 6.3. コンフィギュレーション管理

6.3.1. 関連事業体は、ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティ設定を含む設定を確立し、文書化し、実施し、監視するために適切な措置を講じなければならない。

6.3.2. 6.3.1.の目的のために、関連事業体は次のことを行わなければならない：

- (a) ハードウェア、ソフトウェア、サービス、ネットワークのコンフィギュレーションを構築し、セキュリティを確保する；

(b) ハードウェア、ソフトウェア、サービス、ネットワークについて、新しくインストールされたシステムだけでなく、運用中のシステムについても、その耐用期間を通じて、定められた安全な設定を実施するためのプロセスとツールを策定し、実施する。

6.3.3. 関連事業者は、計画された間隔で、又は重要インシデント若しくは業務若しくはリスクに重要な変更が生じたときに、コンフィグレーションを見直し、必要に応じて更新しなければならない。

#### **6.4. 変更管理、修理、保守**

6.4.1. 関連事業者は、ネットワークと情報システムの変更を管理するために、変更管理手順を適用しなければならない。該当する場合、その手順は、関連するマネジメントと整合していなければならない。

6.4.2. 6.4.1.で言及された手順は、運用中のソフトウェア及びハードウェアのリリース、修正及び緊急変更、並びに構成の変更に適用されるものとする。その手順は、それらの変更が文書化され、2.1.に従って実施されたリスクアセスメントに基づき、実施される前に潜在的な影響を考慮してテストされ、評価されることを保証するものとする。

6.4.3. 緊急事態のために通常の変更管理手順に従えなかった場合、関連事業者は、変更の結果及び手順に従えなかった理由の説明を文書化しなければならない。

6.4.4. 関連事業者は、計画された間隔で、また、重要インシデントが発生したとき、又は業務若しくはリスクに重要な変化が生じたときに、手順を見直し、必要に応じて更新しなければならない。

#### **6.5. セキュリティテスト**

6.5.1. 関連事業者は、セキュリティテストの方針及び手順を確立し、実施し、適用しなければならない。

6.5.2. 関連事業者は、次のことを行わなければならない：

(a) ポイント 2.1 に従って実施したリスクアセスメントに基づき、セキュリティテストの必要性、範囲、頻度及び種類を設定する；

(b) リスク分析で安全な運用に関連すると特定された構成要素を対象とし、文書化されたテスト方法に従ってセキュリティテストを実施する；

(c) テストの種類、範囲、時間および結果を文書化し、各発見に対する重要性のアセスメントおよび低減措置を含む；

(d) 重要な発見があった場合は、低減措置を適用する。

6.5.3. 関連事業体は、計画された間隔でセキュリティテスト方針を見直し、必要に応じて更新しなければならない。

## 6.6. セキュリティ・パッチ管理

6.6.1. 関連事業体は、6.4.1.で言及した変更管理手順、並びに脆弱性マネジメント、リスクマネジメント及びその他の関連する管理手順と首尾一貫した、次のことを確実にするための手順を規定し、適用しなければならない：

(a) セキュリティパッチが利用可能になった後、妥当な時間内に適用される；

(b) セキュリティパッチは、本番システムに適用する前にテストされる；

(c) セキュリティパッチは信頼できるソースから提供され、完全性がチェックされる；

(d) 6.6.2に従ってパッチが利用できない、または適用されない場合には、追加的な対策を実施し、残存リスクを受け入れる。

6.6.2. 6.6.1.(a)の適用除外として、関連事業体は、セキュリティパッチを適用することによる不利益がサイバーセキュリティ上の利益を上回る場合、セキュリティパッチを適用しないことを選択することができる。関連事業体は、そのような決定の理由を正当に文書化し、立証しなければならない。

## 6.7. ネットワーク・セキュリティ

6.7.1. 関連事業体は、サイバー脅威からネットワークと情報システムを保護するために適切な措置を講じなければならない。

6.7.2. 6.7.1.の目的のため、関連事業体は次のことを行わなければならない：

(a) ネットワークのアーキテクチャを、理解しやすく最新の方法で文書化する；

(b) 関連するドメインを不正アクセスから保護するための防御管理を決定し、適用する；

(c) へのアクセスやネットワーク通信を防止するためのアクセス管理を設定する。

関連事業体の運営に必要なものである；

(d) サービスプロバイダによるアクセスを含め、ネットワークと情報システムへのリモートアクセス管理を決定し、適用する；

- (e) セキュリティポリシーの実施管理に使用されるシステムを、他の目的で使用しない；
- (f) 不要な接続やサービスを明示的に禁止または停止する；
- (g) 適切な場合には、事業体によって許可された機器による関連システムおよび情報システムへのアクセスのみを許可する；
- (h) サービスプロバイダの接続は、認証要求の後、保守作業期間など設定された期間のみ許可する；
- (i) 他の通信チャネルから論理的、暗号的または物理的に分離され、エンドポイントの確実な識別とチャネルデータの改ざんや開示からの保護を提供する信頼されたチャネルを通じてのみ、異なるシステム間の通信を確立する；
- (j) 安全で適切かつ段階的な方法で、最新世代のネットワーク層通信プロトコルに完全移行するための実施計画を採択し、その移行を加速させる方策を確立する；
- (k) 電子メール関連の脅威に関連する脆弱性を軽減するために、電子メールコミュニケーションの安全性を確保するための、国際的に合意され相互運用可能な最新の電子メールコミュニケーション標準の展開のための実施計画を採択し、その展開を加速するための措置を確立する；
- (l) DNS のセキュリティ、インターネット・ルーティングのセキュリティ、およびネットワークから発信され、ネットワークに向かうトラフィックのルーティングの衛生に関するベストプラクティスを適用する。

6.7.3. 関連事業体は、計画された間隔で、また、重要インシデントや業務またはリスクに重要な変化が生じた場合に、これらの対策を見直し、必要に応じて更新しなければならない。

## 6.8. ネットワーク・セグメンテーション

6.8.1. 関連する事業体は、2.1 で言及したリスクアセスメントの結果に従って、システムをネットワーク又はゾーンに区分しなければならない。当該事業体は、自己のシステム及びネットワークを第三者のシステム及びネットワークからセグメント化しなければならない。

6.8.2. そのために、関連事業体は次のことを行わなければならない：

- (a) 信頼できるシステムとサービス間の機能的、論理的、物理的関係（場所を含む）を考慮する；
- (b) セキュリティ要件のアセスメントに基づいて、ネットワークまたはゾーンへのアクセスを許可する；
- (c) 関連事業体の運営や安全確保に不可欠なシステムを、保護区域に置く；
- (d) 通信ネットワーク内に非武装地帯を展開し、自国のネットワークから発信される、あるいは自国のネットワークに向けられる安全な通信を確保する；
- (e) ゾーン間およびゾーン内でのアクセスおよび通信を、関連事業体の運営に必要なもの、または安全のために必要なものに制限する；
- (f) ネットワークと情報システムを管理するための専用ネットワークを、関連事業体の運用ネットワークから分離する；
- (g) ネットワーク管理チャンネルを他のネットワークトラフィックから分離する；
- (h) バックアップを含め、開発およびテストに使用する関連システムと本番システムを分離する。

6.8.3. 関連事業体は、計画された間隔で、また、重要インシデントが発生したとき、または業務やリスクに重要な変化が生じたときに、ネットワーク・セグメンテーションを見直し、必要に応じて更新しなければならない。

## 6.9. 悪意のある不正ソフトウェアからの保護

6.9.1. 関連事業体は、悪意のある無許可のソフトウェアからネットワークと情報システムを保護しなければならない。

6.9.2. そのために、関連事業体は特に、悪意のあるソフトウェアまたは未承認のソフトウェアの使用を検知または防止する措置を実施しなければならない。関連事業体は、必要に応じて、そのネットワークと情報システムに検知・対応ソフトウェアが装備されていることを保証しなければならない。このソフトウェアは、2.1 に従って実施されたリスクアセスメントおよびプロバイダとの契約合意に従って定期的に更新される。

## 6.10. 脆弱性の取り扱いと開示

6.10.1. 関連事業体は、ネットワークと情報システムの技術的脆弱性に関する情報を入手し、当該脆弱性へのエクスポージャーを評価し、脆弱性を管理するための適切な措置を講じなければならない。

6.10.2. 6.10.1.の目的のため、関連事業体は次のことを行わなければならない：

- (a) 脆弱性に関する情報を、CSIRT や所轄当局の発表、サプライヤやサービスプロバイダから提供される情報など、適切なチャネルを通じて監視する；
- (b) 必要に応じて脆弱性スキャンを実施し、計画された間隔でスキャン結果の証拠を記録する；
- (c) 事業体にとって重要であると識別された脆弱性については、過度の遅滞なく対処する；
- (d) 自社の脆弱性ハンドリングが、自社の変更管理、セキュリティパッチ管理、リスクマネジメント、インシデントマネジメントの手順と適合していることを確認する；
- (e) 適用される国別脆弱性開示ポリシーに従って、脆弱性を開示する手順を定める。

6.10.3. 脆弱性の潜在的な影響によって正当化される場合、関連事業体は脆弱性を低減する計画を作成し、実施しなければならない。その他の場合、関連事業体は、脆弱性の是正を必要としない理由を文書化し、立証しなければならない。

6.10.4. 関連事業体は、脆弱性情報の監視に使用するチャネルを計画された間隔で見直し、適切な場合には更新しなければならない。

## **7. サイバーセキュリティリスクマネジメント対策の有効性を評価するための方針および手順（指令（EU）2022/2555 の第 21 条 2 項（f））**

**7.1. 指令(EU)2022/2555 の第 21 条(2)の(f)項を目的として、関連事業体は、関連事業体が講じたサイバーセキュリティリスクマネジメント対策が効果的に実施され維持されているかどうかを評価するための方針および手順を確立し、実施し、適用しなければならない。**

**7.2. 7.1.で言及された方針及び手順は、2.1.に従ったリスクアセスメントの結果及び過去の重要インシデントを考慮しなければならない。関連事業体は決定しなければならない：**

- (a) どのようなサイバーセキュリティリスクマネジメントを監視・測定するのか（プロセスや統制を含む）；
- (b) モニタリング、測定、分析、評価の方法（該当する場合）
- (c) 監視と測定が実行される時；

- (d) サイバーセキュリティリスクマネジメント対策の有効性を監視・測定する責任を負う；
- (e) モニタリングや測定から得られた結果を分析し、評価する場合である；
- (f) この結果を分析し、評価しなければならないのは誰なのか。

**7.3. 関連事業体は、計画された間隔で、また、重要インシデントが発生したときや、業務やリスクに重要な変化が生じたときに、方針と手順を見直し、必要に応じて更新しなければならない。**

## **8. 基本的なサイバー衛生の実践とセキュリティ研修（指令（EU）2022/2555 の第 21 条(2)項(g)**

### **8.1. 意識向上と基本的なサイバー衛生の実践**

8.1.1. 指令(EU)2022/2555 の第 21 条(2)の(g)項を目的として、重要事業体は、マネージド団体メンバーを含む従業員、ならびに直接のサプライヤーおよびサービスプロバイダがリスクを認識し、サイバーセキュリティの重要性を知らされ、サイバー衛生慣行を適用することを確実にしなければならない。

8.1.2. 8.1.1.の目的のため、関連事業体は、マネジメント陣の構成員を含む従業員、及び 5.1.4.に従って適切な場合には直接の供給者及びサービスプロバイダに対し、意識向上プログラムを提供しなければならない：

- (a) 活動を繰り返し、新入社員をカバーできるよう、時間をかけてスケジュールを組む；
- (b) ネットワークおよび情報セキュリティポリシー、トピック別ポリシー、ネットワークおよび情報セキュリティに関する関連手続きに沿って制定される；
- (c) は、関連するサイバー脅威、実施されているサイバーセキュリティ・リスクマネジメント対策、サイバーセキュリティに関する追加情報やアドバイスのための連絡先やリソース、ユーザーのためのサイバー衛生習慣をカバーしている。

8.1.3. 意識向上プログラムは、必要に応じて、有効性の観点からテストされなければならない。意識向上プログラムは、サイバー衛生慣行の変化、関連事業体にもたらされる現在の脅威の状況及びリスクを考慮して、計画された間隔で更新され、提供されなければならない。

## 8.2. セキュリティトレーニング

- 8.2.1. 関連事業体は、セキュリティに関連するスキルセット及び専門知識を必要とする役割を担う従業員を特定し、当該従業員がネットワークと情報システムのセキュリティに関する定期的な訓練を受けることを確保する。
- 8.2.2. 関連事業体は、ネットワーク・情報セキュリティポリシー、トピック別ポリシー、及び規準に基づき特定の役割や役職に対するトレーニングの必要性を定めたネットワーク・情報セキュリティに関するその他の関連手順に沿ったトレーニングプログラムを確立し、実施し、適用する。
- 8.2.3. 8.2.1.で言及された訓練は、従業員の職務に関連したものでなければならず、その有効性がアセスメントされなければならない。研修は、実施されているセキュリティ対策を考慮し、以下を対象とするものとする：
- (a) モバイルデバイスを含むネットワークと情報システムのセキュリティ設定と操作に関する指示；
  - (b) 既知のサイバー脅威に関するブリーフィングを行う；
  - (c) セキュリティに関連する事象が発生したときの行動を訓練する。
- 8.2.4. 関連事業体は、セキュリティに関連するスキルセット及び専門知識を必要とする新たな職位又は役割に異動するスタッフに対し、訓練を適用するものとする。
- 8.2.5. プログラムは、適用されるポリシーや規則、割り当てられた役割、責任、また既知のサイバー脅威や技術開発などを考慮し、定期的に更新され、実行されなければならない。

## 9. 暗号技術（指令(EU)2022/2555 の第 21 条 2 項(h)

- 9.1. 指令(EU)2022/2555 の第 21 条(2)項(h)を目的として、関連事業体は、関連する資産格付及び第 2.1 項に従って実施されたリスクアセスメントの結果に沿って、データの機密性、真正性及び完全性を保護するための暗号の適切かつ効果的な使用を確保することを目的として、暗号に関連する方針及び手順を確立し、実施し、適用するものとする。
- 9.2. 9.1.で言及された方針と手続きは、以下を定めるものとする：
- (a) を保護するために必要な暗号化手段の強度と品質に従うものとする；

(b) (a)に基づき、採用するプロトコルまたはプロトコルファミリー、ならびに暗号アルゴリズム、暗号強度、暗号ソリューションおよび使用方法を承認し、適切な場合は暗号アジリティアプローチに従って関連事業体で使用することを要求する；

(c) 適切であれば、以下の関連する方法を採用する：

- (i) 暗号システムやアプリケーションのさまざまな鍵を生成する；
- (ii) 公開鍵証明書を発行し、取得する；
- (iii) 鍵の配布を意図した事業体に行う。鍵の受け取り時に鍵を有効にする方法を含む；
- (iv) 権限のあるユーザーが鍵にアクセスする方法を含め、鍵を保管する；
- (v) いつ、どのようにキーを変更するかについてのルールを含む；
- (vi) 漏洩した鍵に対処する；
- (vii) 鍵の失効には、鍵の撤回または無効化方法も含まれる；
- (viii) 紛失または破損したキーを復元する；
- (ix) キーのバックアップやアーカイブを行う；
- (x) キーを破壊する；
- (xi) 主要な経営関連活動の記録と監査を行う；
- (xii) 鍵の有効期限と無効期限を設定し、鍵管理に関する組織の規則に従って、鍵が指定された期間のみ使用できるようにする。

**9.3. 関連事業体は、暗号技術の最新状況を考慮に入れて、計画的な間隔でその方針及び手順を見直し、必要な場合には更新しなければならない。**

**10. 人的資源の安全保障（指令（EU）2022/2555 第 21 条 2 項(i)**

**10.1. 人材確保**

10.1.1. 指令(EU)2022/2555 の第 21 条(2)の(i)項を目的として、関連事業体は、その従業員、直接の供給者及びサービスプロバイダ（該当する場合）が、提供されるサービス及び

職務に適切であり、ネットワークと情報システムのセキュリティに関する関連方針に沿って、セキュリティ責任を理解し、コミットすることを確実にしなければならない。

10.1.2. 10.1.1.で言及した要求事項には、次の事項を含めなければならない：

- (a) すべての従業員、直接の供給業者、サービスプロバイダ（該当する場合）が、8.1.に従って関連事業体が適用する標準的なサイバー衛生慣行を理解し、これに従うことを保証するための仕組み；
- (b) 管理者または特権的アクセス権を持つすべてのユーザーが、それぞれの役割、責任、権限を認識し、それに従って行動することを保証するための仕組み；
- (c) 管理団体の構成員が、ネットワークと情報システムのセキュリティに関する自らの役割、責任および権限を理解し、それに従って行動することを確保するための仕組みを構築する；
- (d) 身元確認、審査手続き、資格の妥当性確認、筆記試験など、それぞれの役割にふさわしい人材を採用するための仕組み。

10.1.3. 関連事業体は、1.2.で言及された特定の役割への要員の割り当て、及びそれに関する人的資源のコミットメントを、計画された間隔で、少なくとも毎年見直さなければならない。必要な場合は、配置を更新しなければならない。

## 10.2. バックグラウンドの検証

10.2.1. 関連事業体は、その役割、責任及び権限に必要な場合、従業員、及び該当する場合には5.1.4 項に従って直接の供給者及びサービスプロバイダの経歴の検証を、実行可能な範囲で確実に行わなければならない。

10.2.2. 10.2.1.の目的のため、関連事業体は次のことを行わなければならない：

- (a) どのような役割、責任、権限を、経歴が確認された人物にのみ行使させるかを定めた規準を設ける；
- (b) この検証は、ビジネス要件、12.1.で言及されている資産格付け、アクセスされるネットワークと情報システム、および認識されるリスクに比例して、適用法、規制、および倫理を考慮するものとする。

10.2.3. 関連事業体は、計画された間隔で方針を見直し、必要に応じて更新しなければならない。

### 10.3. 解雇または転職の手続き

10.3.1. 関連事業体は、従業員の解雇または雇用の変更後も妥当性を確認できるネットワークと情報システムのセキュリティ責任と義務が、契約によって定義され、実施されることを確実にしなければならない。

10.3.2. 10.3.1.の目的のため、関連事業体は、雇用条件、契約条件又は合意条件において、秘密保持条項など、雇用又は契約の終了後も妥当性を確認できる責任及び義務を規定しなければならない。

### 10.4. 懲戒プロセス

10.4.1. 関連事業体は、ネットワークと情報システムのセキュリティポリシー違反に対処するための懲戒プロセスを確立し、コミュニケーションし、維持しなければならない。このプロセスは、関連する法律、法令、契約及び事業上の要件を考慮しなければならない。

10.4.2. 関連事業体は、計画された間隔で、また、法改正または業務もしくはリスクの重要な変化により必要な場合には、懲戒プロセスを見直し、必要に応じて更新しなければならない。

## 11. アクセス管理（指令（EU）2022/2555 第 21 条 2 項(i)および(j)）

### 11.1. アクセス管理ポリシー

11.1.1. 指令(EU)2022/2555 の第 21 条(2)項(i)を目的として、関連事業体は、ネットワークと情報システムのセキュリティ要件だけでなく、ビジネス要件に基づき、ネットワークと情報システムへのアクセスのための論理的・物理的アクセス管理ポリシーを確立し、文書化し、実施するものとする。

11.1.2. 11.1.1.で言及された方針は、以下のとおりとする：

- (a) 従業員、訪問者、サプライヤーやプロバイダなどの外部事業体を含む人によるアクセスに対処する；
- (b) ネットワークと情報システムによるアクセスに対処する；
- (c) 適切に認証されたユーザーにのみアクセスが許可されるようにする。

11.1.3. 関連事業体は、計画された間隔で、また、重要インシデントや業務またはリスクに重要な変化が生じたときに、方針を見直し、必要に応じて更新しなければならない。

## 11.2. アクセス権の管理

11.2.1. 関連事業者は、11.1.で言及したアクセス管理ポリシーに従って、ネットワークと情報システムへのアクセス権をプロバイダ、変更、削除及び文書化しなければならない。

11.2.2. 関連事業者は、次のことを行わなければならない：

- (a) 知る必要性、最小権限、職務分掌の原則に基づき、アクセス権を割り当て、取り消す；
- (b) 雇用の終了または変更に伴い、アクセス権が適宜変更されるようにする；
- (c) ネットワークと情報システムへのアクセスが、関係者によって承認されていることを確認する；
- (d) アクセス権は、特にアクセス権の範囲と期間を制限することで、訪問者、サプライヤー、サービスプロバイダなどのサードパーティからのアクセスに適切に対応するようにする；
- (e) 付与されたアクセス権の登録簿を保持する；
- (f) アクセス権の管理にロギングを適用する。

11.2.3. 関連事業者は、計画された間隔でアクセス権を見直し、組織の変更に基づいてアクセス権を修正しなければならない。関連事業者は、アクセス権の必要な変更を含む見直しの結果を文書化しなければならない。

## 11.3. 特権アカウントとシステム管理アカウント

11.3.1. 関連事業者は、11.1 項で言及したアクセス管理ポリシーの一部として、特権アカウント及びシステム管理アカウントの管理ポリシーを維持しなければならない。

11.3.2. 11.3.1.で言及された方針は、以下のとおりとする：

- (a) 多要素認証のような強固な本人確認、認証、および特権アカウントとシステム管理アカウントの承認手順を確立する；
- (b) インストール、設定、管理、保守など、システム管理業務のみに使用する特定のアカウントを設定する；
- (c) システム管理権限を可能な限り個別化し、制限する、
- (d) プロバイダは、システム管理アカウントがシステム管理システムに接続するためだけに使用されるようにする。

11.3.3. 関連事業体は、特権アカウント及びシステム管理アカウントのアクセス権を計画された間隔で見直し、組織の変更に基づいて修正し、必要なアクセス権の変更を含め、見直しの結果を文書化しなければならない。

#### 11.4. 管理システム

11.4.1. 関連事業体は、11.1.で言及したアクセス管理方針に従って、システム管理システムの使用を制限及び管理しなければならない。

11.4.2. そのために、関連事業体は次のことを行わなければならない：

- (a) システム管理システムはシステム管理の目的にのみ使用し、それ以外の業務には使用しない；
- (b) このようなシステムは、システム管理目的に使用されないアプリケーション・ソフトウェアから論理的に分離する、
- (c) 認証と暗号化によって、システム管理システムへのアクセスを保護する。

#### 11.5. 識別

11.5.1. 関連事業体は、ネットワークと情報システムおよびその利用者の ID の全ライフサイクルを管理しなければならない。

11.5.2. そのために、関連事業体は次のことを行わなければならない：

- (a) ネットワークと情報システム、およびそのユーザーに固有の ID を設定する；
- (b) ユーザーの ID を一人の人物にリンクする；
- (c) ネットワークと情報システムのアイデンティティを確実に監視する；
- (d) アイデンティティの管理にロギングを適用する。

11.5.3. 関連事業体は、共有 ID のような複数の人物に割り当てられた ID を許可する場合、それが事業上または業務上の理由により必要であり、明確な承認プロセスおよび文書化の対象となる場合に限るものとする。関連事業体は、2.1.で言及したサイバーセキュリティリスクマネジメントの枠組みにおいて、複数の者に割り当てられた識別子を考慮しなければならない。

11.5.4. 関連事業体は、ネットワークと情報システム及びその利用者の ID を定期的に見直し、不要となった場合には、遅滞なくその ID を無効化しなければならない。

## 11.6. 認証

11.6.1. 関連事業体は、アクセス制限及びアクセス管理ポリシーに基づいて、安全な認証手順及び 認証技術を実装しなければならない。

11.6.2. そのために、関連事業体は次のことを行わなければならない：

- (a) 認証の強度が、アクセスする資産の格付けに適切であることを確認する；
- (b) 認証情報の適切な取り扱いについて要員に助言することを含め、情報の機密性を確保する プロセスによって、秘密認証情報のユーザへの割り当ておよび管理を管理する；
- (c) 認証クレデンシャルは、当初はもちろん、あらかじめ定義された間隔で、またクレデンシャルが危殆化した疑いがある場合にも変更する必要がある；
- (d) 認証情報をリセットし、あらかじめ定義された回数ログインに失敗したユーザーをブロックする必要がある；
- (e) あらかじめ定義された非アクティブ期間の後、非アクティブなセッションを終了する。
- (f) 特権アクセスや管理アカウントにアクセスするには、別の認証情報が必要である。

11.6.3. 関連事業体は、実行可能な範囲で、関連するリスクアセスメント及びアクセスされる資産の格付けに従って、最先端の認証方法及び固有の認証情報を使用しなければならない。

11.6.4. 関連事業体は、計画された間隔で認証手順および技術を見直すものとする。

## 11.7. 多要素認証

11.7.1. 関連事業体は、アクセスされる資産の格付けに従って、当該資産にアクセスするための複数の認証 要素又は継続的な認証メカニズムによって利用者が認証されることを確保しなければならない。

11.7.2. 関連事業体は、認証の強度がアクセスされる資産の格付けに適切であることを保証しなければならない。

## 12. 資産管理（指令（EU）2022/2555 第 21 条 2 項(i)）

### 12.1. 資産格付け

12.1.1. 指令(EU)2022/2555 の第 21 条(2)項(i)を目的として、関連事業体は、必要な保護レベルについて、ネットワークと情報システムの範囲内にある情報を含むすべての資産の格付けレベルを定めなければならない。

12.1.2. 12.1.1.の目的のため、関連事業体は次のことを行わなければならない：

- (a) 資産の格付けレベルを定める；
- (b) 機密性、完全性、真正性、可用性の要件に基づき、すべての資産に格付けレベルを関連付け、その機密性、重要性、リスク、ビジネス価値に応じて必要な保護を示す；
- (c) 資産の可用性要件を、事業継続計画および災害復旧計画で定めた提供目標および復旧目標と整合させる。

12.1.3. 関連事業体は、資産の格付けレベルの定期的なレビューを実施し、適切な場合には更新しなければならない。

### 12.2. 資産の取り扱い

12.2.1. 関連事業体は、ネットワーク及び情報セキュリティ方針に従って、情報を含む資産の適切な取扱いに関する方針を確立し、実施し、適用しなければならず、資産の適切な取扱いに関する方針を、資産を使用する者又は資産を取扱う者に伝達しなければならない。

12.2.2. 本方針は、以下のとおりとする：

- (a) 取得、使用、保管、輸送、廃棄を含む、資産のライフサイクル全体を対象とする；
- (b) 資産の安全な使用、安全な保管、安全な輸送、回復不能な削除と破棄に関する規則を提供する；
- (c) 譲渡は、譲渡される資産の種類に従い、安全な方法で行われるものとする。

12.2.3. 関連事業体は、計画された間隔で、また、重要インシデントが発生したとき、または業務やリスクに重要な変化が生じたときに、方針を見直し、必要に応じて更新しなければならない。

### 12.3. 可搬媒体ポリシー

12.3.1. 関連事業体は、可搬保存媒体の管理に関する方針を確立し、実施し、適用し、可搬媒体が関連ネットワークと情報システムに接続される関連又はその他の場所で可搬保存媒体を取り扱う従業員及びサードパーティに伝達しなければならない。

12.3.2. 本方針は、以下のとおりとする：

- (a) 可搬媒体の使用に組織的な理由がない限り、その接続を技術的に禁止する；
- (b) このようなメディアからの自己実行を無効にし、関連メディアで使用される前に悪意のあるコードがないかスキャンする。
- (c) 輸送中および保管中にデータを含む可搬保存媒体を制御および保護するための手段を提供する；
- (d) 必要に応じて、可搬保存媒体上のデータを保護するために暗号化技術を使用するための手段を提供する。

12.3.3. 関連事業体は、計画された間隔で、また、重要インシデントや業務またはリスクに重要な変化が生じたときに、方針を見直し、必要に応じて更新しなければならない。

### 12.4. 資産目録

12.4.1. 関連事業体は、完全、正確、最新かつ一貫性のある資産目録を作成し、維持しなければならない。また、インベントリの記載事項の変更を追跡可能な方法で記録しなければならない。

12.4.2. 資産のインベントリの粒度は、関連事業体のニーズに適したレベルでなければならない。インベントリには以下を含むものとする：

- (a) 業務とサービスのリストとその説明、
- (b) ネットワークと情報システム、その他の関連資産のリスト。

12.4.3. 関連事業体は、インベントリおよびその資産を定期的に見直し、更新し、変更履歴を文書化しなければならない。

### 12.5. 解雇時の資産の預託、返却、削除

関連事業体は、従業員が保管する資産が雇用終了時に預託、返却又は削除されることを確実にする手順を確立、実施及び適用しなければならない。また、これらの資産の預託、返却及び削除

を文書化しなければならない。資産の寄託、返却又は削除が不可能な場合、関連事業体は、12.2.2.項に従い、資産 CA システムを確保しなければならない。

## **13. 環境および物理的安全保障（指令（EU）2022/2555 第 21 条 2 項（c）、（e）および（i））**

### **13.1. ユーティリティのサポート**

13.1.1. 指令(EU)2022/2555の第21条(2)(c)の目的のため、関連事業体は、ネットワークと情報システムの損失、損傷、危殆化、またはサポートユーティリティの障害と中断による業務の中断を防止しなければならない。

13.1.2. そのために、関連事業体は、適切な場合、次のことを行わなければならない：

- (a) 電気、通信、水道、ガス、下水、換気、空調などのユーティリティ設備の故障による停電やその他の障害から施設を守る；
- (b) 公共サービスにおける冗長性の利用を検討する；
- (c) データを伝送したり、ネットワークと情報システムに供給したりする電力や電気通信のユーティリティ・サービスを保護し、傍受や損害から保護する；
- (d) (c)のユーティリティ・サービスを監視し、ユーティリティ・サービスに影響する 13.2.2(b)に言及した最小及び最大管理閾値外の事象を、管轄の内部又は外部要員に報告する；
- (e) 非常用電源の燃料など、非常用電源とそれに対応するサービスの契約を結ぶ；
- (f) 提供されるサービスの運営に必要なネットワークと情報システム、特に電気、温湿度管理、通信、インターネット接続の供給が継続的に有効であることを確認し、監視し、維持し、テストすること。

13.1.3. 関連事業体は、定期的に、又は重要インシデント若しくは業務若しくはリスクの重要な変化の後に、保護手段をテストし、見直し、及び必要に応じて更新しなければならない。

### **13.2. 物理的・環境的脅威からの防御**

13.2.1. 指令(EU)2022/2555の第21条(2)(e)の目的のため、関連事業体は、2.1項に従って実施されたリスクアセスメントの結果に基づき、自然災害及びその他の意図的又は非意図的な脅威など、物理的及び環境的脅威に起因する事象の結果を防止又は軽減しなければならない。

13.2.2. そのために、関連事業体は、適切な場合には、次のことを行わなければならない：

- (a) 物理的・環境的脅威に対する保護手段を設計し、実施する；
- (b) 物理的・環境的脅威の最小・最大管理閾値を決定する；
- (c) 環境パラメータを監視し、(b)で言及された最小および最大管理閾値外の事象を、内部または外部の担当者に報告する。

13.2.3. 関連事業体は、物理的及び環境的脅威に対する保護手段を、定期的に、又は重要インシデント若しくは業務又はリスクの重要な変更後に、試験し、見直し、及び必要に応じて更新しなければならない。

### **13.3. 境界および物理的アクセス管理**

13.3.1. 指令(EU)2022/2555の第21条(2)(i)の目的のため、関連事業体は、ネットワークと情報システムへの無許可の物理的アクセス、損傷、干渉を防止し監視するものとする。

13.3.2. そのために、関連事業体は次のことを行わなければならない：

- (a) 2.1に従って実施されたリスクアセスメントに基づき、ネットワークと情報システムのセキュリティエリアおよびその他の関連資産を保護するために、セキュリティ境界を設定し、使用する；
- (b) 適切な進入管理とアクセスポイントにより、(a)の区域を保護する；
- (c) オフィス、部屋、施設の物理的セキュリティを設計し、実施する、
- (d) 無許可の物理的アクセスがないか、敷地内を継続的に監視する。

13.3.3. 関連事業体は、物理的アクセス管理手段を定期的に、または重要インシデントもしくは業務またはリスクの重要な変更後に、テストし、レビューし、必要に応じて更新しなければならない。