ERICSSON

サプライヤー向け情報セキュリティ要件

ISRS

Security Requirements

はじめに

サプライヤー向けエリクソン情報セキュリティ要件（以下「要件」）は、サプライヤーとのあらゆる関係においてサプライヤーが以下を行う際に遵守する必要がある最低限の情報セキュリティ要件を規定するものです。

1. エリクソン情報の処理、保存、アクセスを行う。
2. エリクソンのネットワークやインフラストラクチャにアクセスする。
3. エリクソン向けのソフトウェアを開発またはカスタマイズする。
4. IT ハードウェアまたはソフトウェア製品を提供し、サポートサービスや保守サービスを実施する。

本要件は、情報セキュリティ要件の完全なリストを提供することを意図したものではありません。各サービス提供では、本要件に加えて、関連する契約で別途定義される適切な情報セキュリティ管理により対応する必要がある特別な要件が必要になる場合があります。

この文書は定期的に見直しが行われ、随時更新されます。

目次

1 情報セキュリティ要件

サプライヤーは、最新版の国際規格 ISO/IEC 27001 または書面による契約に基づいて同等の規格に準拠することにより、情報セキュリティ管理に対する体系的なアプローチを証明する必要があります。

1.1 情報セキュリティ管理

a. サプライヤーの経営陣は、情報セキュリティの方向性を定め、情報セキュリティに取り組む姿勢を示す必要があります。少なくとも、高いレベルの情報セキュリティポリシーと全社的に適用されるサポートプログラムが必要です。

b. 上記サブセクション a の情報セキュリティポリシーは、サプライヤーの経営陣によって承認され、サプライヤーの組織内で公開され、関連するサプライヤーの担当者に伝達される必要があります。

c. サプライヤーの情報セキュリティポリシーについては、サプライヤーが定期的にレビューする必要がありますが、適合性、妥当性、有効性を継続的に確保するために、少なくとも 24 か月に 1 回、または大幅な変更が発生した場合、レビューする必要があります。

d. 情報セキュリティプログラムを維持する責任者として、1 人以上の有資格者を任命する必要があります。

e. サプライヤーは、安全な職場環境の構築と維持に関して従業員責任を教育するため、情報セキュリティ啓蒙キャンペーンを定期的に実施する必要があります。

f. サプライヤーは、関連する職務の適切な職務分離を維持する必要があります。

1.2 リスク管理

サプライヤーは、情報セキュリティ上のリスクを特定し、対策を講じるリスク管理フレームワーク/プロセスを導入する必要があります。

1.3 人材のセキュリティ

a. サプライヤーは、適用法に従って、サプライヤーの全従業員に対して雇用前身元確認チェックを実施する必要があります。こうした身元調査の証拠は保管され、エリクソンの要求に応じてエリクソンに提供される必要があります。

b. サプライヤーの担当者は、エリクソン情報にアクセスする前に、サプライヤーとの書面による契約（雇用契約や NDA など）に基づく機密保持の制約に拘束される必要があります。これらの契約は、サプライヤーの担当者がエリクソン情報を第三者に開示することを禁止するものとし、契約に基づくサプライヤーのエリクソンに対する守秘義務と同等以上の制約を含むものでなければなりません。

c. エリクソンネットワーク インフラストラクチャ および/またはエリクソン情報 にアクセスできるサプライヤー担当者は、エリクソンの非開示およびアクセス指示文書 (NDI) に署名する必要があります。

d. サプライヤーは、情報セキュリティ違反に対処するための懲戒手続きを整備する必要があります。

1.4 資産管理

a. サプライヤーは、エリクソン情報を機密情報として取り扱い、この文書に記載されている要件に従ってこれを保護する必要があります。

b. サプライヤーは、サービスの一部である情報技術資産の一覧表を作成および管理する必要があります。

c. サプライヤーは、契約に基づく義務を履行する以外の目的で、エリクソン情報を保存、印刷、複製、開示、処理してはなりません。

d. サプライヤーは、サプライヤーの担当者の退職または雇用変更した場合に、エリクソンの資産を返却するためのプロセスを確立する必要があります。

e. サプライヤーは、業界のベストプラクティスに従ってエリクソン情報を安全に削除する手順を確立し、維持する必要があります（再利用できるようになる前に電子メディアからの情報の削除も含む）。

f. 契約の締結または終了時に、サプライヤーは、、サプライヤーが所有する電子形式または非電子形式のバックアップおよびアーカイブコピーを含むすべてのエリクソン情報を、業界のベストプラクティスに従って返却または安全に破棄する必要があります。サプライヤーは、要求に応じて、書面による確認、または該当する場合は破棄の証明書をエリクソンに提供する必要があります。

1.5 アクセス管理

a. エリクソンの管理外のネットワークからエリクソンに所属していない個人または組織がエリクソンの資産にアクセスすることは、承認されたエリクソンリモート アクセス ソリューションを通じてのみ許可されます。

b. エリクソン情報へのアクセスは、need to know の原則に基づき、特定の個人に限定し必要に応じてアクセスを制限する必要があります。

c. 共有アカウントは固く禁止されています。エリクソン情報にアクセスする各個人は、独自のアカウントを持っている必要があります。

d. 業界のベストプラクティスに従って、エリクソン情報を含むシステムおよびネットワークへのすべてのアクセスに多要素認証 (MFA) を実装する必要があります。

e. サプライヤーは、エリクソン情報にアクセスする際に、複雑なパスワードの使用、ログオンの最大許容失敗回数、すべてのパスワードに対する有効期限の設定など、業界のベストプラクティスに従ってパスワードの選択と管理を実施する必要があります。

f. サプライヤーは、エリクソン情報を処理、送信、または保存するネットワークやシステムへのユーザーの追加、変更、削除のために、承認が必要なプロセスを用意する必要があります。

g. サプライヤーは、解雇または雇用変更の場合にアクセスを取り消したり更新したりするプロセスを用意する必要があります。

h. サプライヤーは、エリクソン情報を処理するシステムおよびネットワークへのアクセス特権（管理アクセス特権を含む）をレビューする必要があります。定期的なレビューは少なくとも 12 か月ごとに実行し、特権ユーザーの場合は少なくとも 3 か月ごとに実行する必要があります。

i. サプライヤーは特権アカウントを管理するためのプロセスを備えている必要があります。

j. どのエリクソン情報がアクセス、変更、開示、または破棄されたかを示す記録は、監査可能な方法で保存する必要があります。

1.6 暗号化

a. 暗号化制御は、関連するすべての契約、法律、規制に準拠して実装する必要があります。

b. サプライヤーは、業界のベストプラクティスとなっている暗号化技術を使用して暗号化された電子メールを介してエリクソンと安全に通信できる必要があります。

c. エリクソン情報は、業界のベストプラクティスに従い、転送中および保存時に暗号化技術を使用して保護する必要があります。

d. 暗号キーは、業界のベストプラクティスに従い、キーの生成、更新、アクセス、配布、保管、アーカイブ、失効、破棄のプロセスを導入して一元管理する必要があります。

e. ルート証明書は運用環境で使用しないでください。

1.7 物理的及び環境セキュリティ

a. サプライヤーは、エリクソン情報の処理や保存が行われる施設およびデータセンターへの物理的なアクセスを、必要最小限の特定の個人に限定する必要があります。

b. エリクソン情報が処理される情報処理施設では、監視とアクセス制御が常時（24x7）実施される必要があります。

c. サプライヤーは、エリクソン情報が処理される情報処理施設を外的および環境的な脅威や危険から保護する必要があります。

d. エリクソン情報やエリクソンの資産を保護するために、クリアデスクとクリアスクリーンポリシーを適用する必要があります。

e. エリクソンのサービスが実行される場所への物理的なアクセスは、個別のスワイプ/近接カードまたはその他の同等のシステムを使用して制限する必要があります。

f. エリクソンのサービスが実行される場所への物理的なアクセスでは、日付、時刻、スワイプ/近接カード ID、ドア ID、アクセス拒否、アクセス許可などの物理的なアクセス関連のイベントを継続的に記録する必要があります。

1.8 運用セキュリティ

a. セキュリティインシデントや需要の増加が発生した場合でも継続的な可用性を確保するために、サプライヤーのシステムには十分な容量を用意する必要があります。

b. サプライヤーは、業界のベストプラクティスに従って、悪意のあるソフトウェアからの保護がシステムに導入され、最新の状態に保たれていることを確認する必要があります。

c. すべての特権ユーザーのアクションはログに記録する必要があります。システム、特権ユーザー、またはエンド ユーザーによるこれらのログへの変更は検出可能でなければなりません。ログ記録も定期的に個別にして確認する必要があります。

d. 重要なセキュリティ関連イベントに関する情報は、ログオン失敗、システムクラッシュ、アクセス権の変更などのイベントタイプや、日付、時刻、ユーザーID、ファイル名、ユーザーアクティビティの種類、IP アドレスなどのイベント属性を含めてログに記録する必要あります。

e. ログ記録は暗号化された状態で少なくとも 6 か月間保存され、要求に応じてエリクソンに提供できる必要があります。

f. 契約に基づく継続性と納入期限を確実に実現するために、バックアップを実施し、維持する必要があります。

g. 脆弱性の性質/重要性に基づいて脆弱性に優先順位をつけ、是正するための脆弱性管理プロセスを実施する必要があります。

h. 適時にパッチが適用されるように、パッチ管理プロセスを導入する必要があります。

i. サプライヤーは、業界のベストプラクティスを使用して、エリクソンのエンゲージメントをサポートするために使用されるシステムとインフラストラクチャの侵入テストを、少なくとも年に 1 回、実施する必要があります。

j. サプライヤーは、関連するすべての情報処理システムのクロックを単一の基準時間ソースに同期させる必要があります。

k. 攻撃対象領域を減らすために、現在の業界のベストプラクティスに従った強化をすべてのシステムに適用する必要があります。

l. サプライヤーは、エリクソンからの書面による事前許可なしに、エリクソン情報をポータブルデバイスに保存すること防止するための方針を導入するものとします。

m. サプライヤーは、適切な物理的、技術的、論理的手段によって、サプライヤー自身や他の顧客のシステムおよびデータからエリクソン情報およびエリクソンのアプリケーション/システムを分離する必要があります。

n. エリクソン情報を含む開発、テスト、および運用環境は、論理的および物理的に分離されている必要があります。

o. サプライヤーは、契約で特に合意していない限り、人工知能（AI）でエリクソン情報を使用してはなりません。

1.9 通信セキュリティ

a. エリクソン情報を含むシステムは、業界のベストプラクティスに従って強化する必要があります。これには、使用されてないソフトウェアや機能の削除または無効化が含まれますが、これらに限定されません。

b. サプライヤーは、エリクソン情報を保護するために、業界のベストプラクティスに従って、セキュリティが強化されたファイアウォール、侵入検知/防止システム、ネットワークセグメンテーション、およびその他の関連対策を活用した階層化セキュリティアプローチを導入する必要があります。

c. サプライヤーは、マルウェア、なりすましメール、フィッシング攻撃、スパムなどの悪意のある攻撃から保護するために、業界のベストプラクティスに従って、メールセキュリティソリューションを導入する必要があります。

1.10 下請業者との関係

a. エリクソン情報を下請業者に開示することは、エリクソンから書面による事前の同意がある場合に限り、契約に基づくサプライヤーの義務を履行する目的に限り許可されます。

b. 下請業者は契約上の義務を果たすために必要なエリクソン情報へのアクセス、使用、保存、開示のみに限定する必要があります。

c. サプライヤーは、本契約に記載されているものと同じ義務を書面による合意により下請業者に引き継ぐ責任があります。

d. サプライヤーは、新しい下請業者を受け入れる前に、その下請業者に関連するリスクを評価し、また、第三者によるリスク管理プロセスを導入する必要があります。

e. サプライヤーは、下請業者による本要件の遵守状況を定期的に監視、レビュー、監査する必要があります。

1.11 インシデント管理

a. サプライヤーは、インシデントを検出して処理するための文書化されたセキュリティ インシデント管理プロセスを備える必要があります。

b. サプライヤーは、エリクソン情報に影響を及ぼすインシデントを認識後速やかに、エリクソンに通知する必要があります。そのような通知は、インシデントの発生またはインシデントの疑いを認識した後、どのような場合でも、遅くとも 24 時間以内または同意した時間内に、以下の者に対して行う必要があります。

   i. 契約に定められたエリクソンの連絡先、および

   ii. gs.sim.dispatch@ericsson.com

c. セキュリティ関連のインシデントに関するすべての報告は機密情報として扱い、業界のベストプラクティスの暗号化方法を使用して暗号化するものとします。

d. サプライヤーは、これらの報告への対応においてエリクソンに全面的に協力する必要があります。協力には、フォレンジック評価のためのコンピューターベースの証拠データへのアクセスの提供が含まれる場合があります。

e. サプライヤーは、サービスやエリクソン情報に影響を及ぼすセキュリティインシデントや脆弱性に対する是正措置の一環として、相互に同意できる適切なセキュリティ対策と手順が確実に実施されるようにエリクソンと協力するものとします。

1.12 事業継続性管理

a. サプライヤーは、少なくとも毎年事業継続および災害復旧計画を文書化およびテストし、エリクソンの要求に応じてコピーを提供する必要があります。

b. サプライヤーは、情報セキュリティと ICT 準備要件が事業継続および災害復旧計画に組み込まれていることを確認する必要があります。

c. サプライヤーは、エリクソンの要請に応じて、エリクソンが指定する相互の事業継続や災害復旧活動に貢献する必要があります。

1.13 システムの取得、開発及び保守

以下の情報セキュリティ要件は、エリクソン情報の処理を含むソフトウェアやハードウェアの開発またはカスタマイズサービスを提供するサプライヤーに適用されます。

a. サプライヤーは、文書化されたソフトウェア開発ライフサイクル (SDLC) 方法論を備えている必要があります。

b. システムのソース/オブジェクト コードは、不正アクセスから保護する必要があります。ソースコードリポジトリへのアクセス権限については、定期的にレビューを行い、許可された従業員にのみに限定する必要があります。

c. 実稼働システムからのエリクソン情報は、テストおよび開発システムでは使用しないでください。

d. サプライヤーは、エリクソン情報を処理するソフトウェアおよび/またはその他の製品に、既知のセキュリティ上の脆弱性やその他のセキュリティ上の欠陥が一切ないことを保証する必要があります。

e. エリクソンの要求に応じて、サプライヤーは、エリクソン情報を処理をサポートするソフトウェアの開発に使用した第三者のソフトウェア/プラグイン（独自開発されたものまたはオープンソース）を開示する必要があります。

f. サプライヤーは、アプリケーションおよびインフラストラクチャ関連の変更を要求、テスト、承認するための文書化された変更管理手順に従う必要があります。

1.14 ソフトウェア サプライチェーン セキュリティ

サプライヤーは、使用した第三者ソフトウェアコンポーネント（オープンソースおよび独自開発コンポーネントの両方）とそれぞれのバージョン番号を特定して文書化する必要があります。また、エリクソンに納品される、またはエリクソンが利用できるすべてのソフトウェア（スタンドアロンで提供されるか、ハードウェアに組み込まれて提供される）について、SPDX 仕様 V2.2.1/ISO 5962:2021 およびサプライヤー向け SBOM 仕様（条件とガイドライン – サプライヤーとパートナー – エリクソンを参照）に準拠したソフトウェア部品表（SBOM）をエリクソンに提供する必要があります。

2 コンプライアンス

a. 情報セキュリティに関するサプライヤーの内部監査および/または評価は、訓練を受けたサプライヤー担当者、またはサプライヤーが指定した第三者によって定期的に実施され、発見された事項は速やかに修正されなければなりません。

b. エリクソンの要求に応じて、サプライヤーは 10 日以内に、要件およびエリクソンと合意したその他の情報セキュリティ要件への遵守を証明できなければなりません。特定された不遵守は、エリクソンに追加費用をかけずに直ちに修正する必要があります。

c. サプライヤーは、エリクソンの要求に応じて、下請業者による本要件の遵守に関する証拠をエリクソンに提供するものとします。

d. サプライヤーは、エリクソンの要求に応じて、ペネトレーションテストや脆弱性テストのすべての結果をエリクソンに提供するか、エリクソン情報の処理や保存が行われる、サプライヤーが管理またはホストするシステムまたは環境でエリクソンがペネトレーションテストや脆弱性テストを実施するのを許可する必要があります。

e. サプライヤーは、要件への遵守を証明するために必要なすべての記録を保持し、保護する必要があります。

3 定義

本書では、文脈によって明らかに意味が異なる場合を除き、以下の用語及び表現は、以下の意味を有するものとします。

契約	サプライヤーとエリクソンの間の契約。これに従ってエリクソンは、本要件が適用される、サプライヤーからの製品（IPR で保護されているソフトウェアやその他の製品を含む）、サービス、またはその他の成果物の購入、ライセンスイン、またはリースを行います。
身元確認チェック	身元確認チェックは、ISO/IEC 27001/27002 に規定されているものと同じ意味を持ちます。
エリクソン情報	エリクソン、エリクソンの顧客、またはエリクソンとビジネス関係にある他の第三者に所有権がある情報、およびサービスの一部を構成するその他の情報。エリクソン情報には個人情報が含まれます。
業界のベストプラクティス	同じまたは類似の状況下で、サービス受領者または請負業者(該当する場合)と同種の事業に従事する熟練した適格なサービス提供者に合理的かつ通常期待されるスキル、注意、配慮、および運用慣行を意味します。
情報処理施設	エリクソン情報を処理または保存するシステムを収容する物理的な場所。
個人情報	個人情報とは、特定された、または特定可能な人物（「データ主体」）に関連する可能性のある情報、または法律、規制、契約上の合意によって別途定義される情報を意味します。識別可能な人物とは、特に名前、識別番号、位置データ、オンライン識別子などの識別子、またはその人の身体的、生理的、精神的、経済的、文化的、または社会的アイデンティティに固有の 1 つ以上の要素を参照することにより、直接的または間接的に識別できる人物です。
サービス	契約に基づきサプライヤーがエリクソンに提供するサービス、製品、その他の成果物。
単一の基準時間ソース	時計と時間を調整するために世界中で使用されている主要な時間標準である UTC（協定世界時）の信頼できるソースに直接リンクされているタイムサーバーソース（つまり、Stratum1）。
サプライヤー	エリクソンと契約を締結し、サービスを提供する会社。この文書において「サプライヤー」という用語を通じてサプライヤーに義務または要件を課す場合、その用語にはサプライヤーの関連会社、下請業者、および担当者も含まれます。