

システム構築・運用事業者 セキュリティ評価ガイドライン概要

サイバーセキュリティ委員会
DX with Cybersecurity分科会



はじめに ― 本ガイドラインの目的と位置づけ

ランサムウェア被害はサプライチェーンを構成する中小企業へ拡大。EUサイバーレジリエンス法、米国のSBOM義務化、経済産業省のSCS評価制度・サイバーインフラ事業者ガイドラインなど、事業者責任を具体化する動きが国内外で加速している。

① 目的

- ・ ユーザー組織がセキュリティ対策と運用に配慮したSI事業者を選ぶ際の確認ポイントを示す
- ・ SI事業者にとっては、質の良い提案・サービス提供のあるべき姿を示す自己点検や顧客への説明にも活用できる
- ・ セキュア・バイ・デザインが競争優位を生む市場環境の醸成を目指す

② 想定読者

- ・ 調達時にSI事業者・構築内容へ十分なセキュリティ要件を定義・明示できていないユーザー組織
- ・ セキュリティのスキル／人的リソースに課題を抱える組織（中小企業、小規模自治体、病院など）
- ・ 自社の体制やサービスを自己点検・説明したいSI事業者自身

③ 適用範囲

- ・ 対象：ネットワーク・サーバー等のインフラ構築から手がけるSI事業者
- ・ 対象外：WEB／ソフトウェア開発事業者、IaaS・PaaS上での開発事業者、SaaSカスタマイズ提供事業者
- ・ SES（準委任）で契約上セキュリティ要件が定義済みの場合は契約条件が優先し対象外

④ 原則

- ・ ISMS・プライバシーマーク等の認証要求を網羅するものではなく、適合を保証するものでもない
- ・ 記載要件は一例。代替の取り組みも許容され、100点満点を目指すものではない
- ・ ユーザーの想定リスクとSI事業者の取り組みレベルが合致しているかを判断するフレームワーク

第二章

SI事業者を選定する上でユーザーが考慮すべき要素

信頼できるSI事業者を見極めるための「2つの軸」と、それを構成する「4つの要件」。

【ユーザーに提供される価値】

① 構築

リスクを事前に十分に予測し、それを前提にした提案ができるリスクの全体像を可視化し、何を許容したかを共有する姿勢

② 運用

平時の運用だけでなく障害発生時にも柔軟に対応できる。対策強化・脆弱性管理・ログ監視など継続的運用で担保する。

【SI事業者によるコミットメント】

③ 企業の体制

高い意識で提案する文化があり、サービスレベルを維持できる体制がある。経営層主導でポリシー徹底と人材投資を継続している。

④ 契約・責任分界の明確化

リスクとコストのバランスを率直に伝え、ユーザーと合意する。責任分界点を明確にし、残存リスクを契約で明らかにする。

第三章で用いる確認記号

I-V1~V5

構築業務
(Implementation-Value)

O-V1~V3

運用業務
(Operation-Value)

C1~C4

SI事業者の体制
(Company / Commitment)

A1

契約・責任分界の明確化
(Agreement)

第三章

詳細要件 ①構築業務（I-V1～V5）

構築フェーズで確認すべき5つの要求事項。各要件はSI事業者の体制（C1～C4）と契約（A1）の観点で確認する。

I-V1

セキュリティリスク評価

どこにどのようなリスクがあるかを可視化し、文書として提案・合意の中で共有する姿勢。有資格技術者の確保とリスクコミュニケーションのプロセス化。

A1：リスク分析の実施を説明・明記

I-V2

品質維持

完成時だけでなく作業工程の適切なタイミングでセキュリティチェックを実施。ポリシー・手順書を整備し、技術者の能力に過度に依存しない。

A1：完了報告書に品質管理者の承認

I-V3

完成検査

脆弱な初期設定を残さない。管理者パスワード、最新バージョン、IPアドレス・共有設定、パターンファイル等をチェックリストで検証。

A1：完成検査の実施と、その限界を明記

I-V4

構成管理

ネットワーク構成図・IT資産リストを提供し、顧客の資産台帳整備を支援。インシデント時の侵入経路調査・影響範囲特定的前提となる。

A1：IT資産管理の必要性和責任範囲を合意

I-V5

サプライチェーン管理

自社ポリシーを外部認証（ISMS、Pマーク、ISMAP等）で担保し公表。二次委託先を含む教育・監査・更新確認を継続的に実施。

A1：委託契約での遵守宣言と取り決め

詳細要件 ②運用業務（O-V1～V3）

セキュリティは構築時点で終わらない。稼働期間全体を通じた継続的な運用によって担保される。

O-V1

インシデント対応

- ・ 対応窓口の設置、エスカレーションフローの文書化、FAQ等の開示
- ・ インシデントレスポンス能力を持つ技術者の育成、公的機関・団体の勉強会への参加
- ・ 自社能力を超える場合の外部委託先・ベンダーへのエスカレーション先を紹介できる

A1：無償対応範囲と有償サービス範囲を文書化（SLA／SLO、対応時間帯の明示）

O-V2

脆弱性対応

- ・ 納入システムの機器名称・バージョンを記録し、的確な情報提供ができる体制
- ・ 最新の攻撃情報を提供するプロセス、脆弱性診断サービスの提供（外部委託も可）
- ・ 早期警戒情報を入手できる情報流通網を持ち、入手先を定期的に見直している

A1：脆弱性情報の入手先提供と、納品時のベンダーサポート窓口登録の徹底

O-V3

保守・保全

- ・ 構築した製品のサポートを自社で提供できる能力を有している
- ・ ベンダー資格取得の教育機会の提供、情報セキュリティ資格取得の推奨
- ・ 顧客サポート満足度の評価基準を持ち、可視化して継続的に改善している

A1：サポート条件の明示、無償／有償範囲の文書化と顧客合意プロセスの徹底

チェックリストの使い方

付録のチェックリストは、ある意味「理想を並べた要望リスト」。すべてを網羅するには相応のコスト負担が必要となる。

1

投資判断は リスクの重要度で

- 重要システムには経営層が覚悟を決めて投資する
- 資産価値が低いシステムはリスクを許容する保険等へ移転するという考え方もある
- 侵害時の事業インパクトは投資額をはるかに超える事案が多数報告されている

2

自社のリスクを 確認してから使う

- 委託先に求める範囲と、その確認方法を決める
- 何を重視しリスクをどこまで許容するかを経営層も含めて確認する
- その結果を意識して委託事業者を選定する

3

濃淡をつけて 対話の起点に

- 概念的な内容のため教科書的な使い方はできない
- 業種・業態・取引先からの要求によって求められる濃淡は変わる
- セキュリティに関するコミュニケーションが文化として根付くことを目指す

「ここで書かれた考え方を元に、セキュリティに関するコミュニケーションが文化として根付いていく事を願う」

当分科会では本ガイドラインを継続的に改善し、皆様にお届けしていくことを目指しています。

SUMMARY

全体まとめ

システム構築・運用事業者セキュリティ評価ガイドライン Ver.1.0（日本IT団体連盟 サイバーセキュリティ委員会 DX with Cybersecurity分科会）

目的

セキュリティに配慮したSI事業者を選ぶための確認ポイントを示し、ユーザーが安心できるシステムの構築・運用を支援する。

構造

「提供価値（構築・運用）」と「コミットメント（企業の体制・契約）」の2軸4要件で評価する。

構築

I-V1～V5：リスク評価／品質維持／完成検査／構成管理／サプライチェーン管理。

運用

O-V1～V3：インシデント対応／脆弱性対応／保守・保全。稼働期間全体を通じた継続性が鍵。

確認軸

各要件をC1整備・C2強化定着・C3補強代替・C4継続改善と、A1契約・責任分界の明確化で確認する。

活かし方

認証ではなく、リスクとコストの対話のためのフレームワーク。100点ではなく自社のリスクとの適合を見る。

リスクに見合ったコストを、事業者とユーザーが率直に語り合うために。

EOF