

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

2026 年 10 月 1 日

一般社団法人日本 IT 団体連盟

サイバーセキュリティ委員会

DX with Cybersecurity 分科会

目次

第一章：はじめに.....	2
目的.....	2
想定読者.....	3
適用範囲.....	3
原則.....	4
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.....	5
構成の理解.....	5
ユーザーに提供される価値.....	5
SI 事業者によるコミットメント.....	6
第三章：詳細要件.....	7
①構築業務.....	7
セキュリティリスク評価（I-V1）.....	7
品質確保（I-V2）.....	10
完成検査（I-V3）.....	12
構成管理（I-V4）.....	15
サプライチェーン管理（I-V5）.....	18
②運用業務.....	21
インシデント対応（O-V1）.....	21
脆弱性対応（O-V2）.....	24
保守・保全（O-V3）.....	27
第四章：チェックリストの使い方.....	29
第五章：附則.....	30
関連資料:.....	30
改訂履歴:.....	31
執筆者.....	32

第一章：はじめに

【目的】

近年のサイバーセキュリティにおける脅威は、ランサムウェア被害の拡大に伴って、大手企業をターゲットとしていた従来のサイバー攻撃からすそ野を拡げ、サプライチェーンを構成する中小企業に対する攻撃が日々激化してきています。これは、大手企業に対するサプライチェーン攻撃の起点として比較して脆弱と思われる取引先の中小企業がターゲットにされるだけでなく、RaaS¹のようなランサムウェア攻撃を成功に至らしめるビジネスモデルの定着により、ツールや攻撃インフラの開発コストが低下し、中小企業そのものを攻撃対象としてもビジネスとして成立する環境の変化に伴うものと言えます。

またEUではソフトウェアサプライチェーン攻撃の観点からサイバーレジリエンス法が採択され、セキュリティ・バイ・デザインに対する要求が対応必須の要件となっています。加えて米国でも大統領令でSBOMの提出を義務付けるなど、世界的に事業者の責任を具体的に規定する法制化が進められています。これを受けて日本でもIoT機器のセキュリティ要件適合評価及びラベリング制度であるJC-STAR²の★1、★2の申請受付が2025年3月に開始されました。今後政府調達や重要社会インフラ事業者での調達を前提とした第三者認証付の★3の要件も2026年の4月以降申請受付を開始する見込みです。

ここ数年のいくつかの病院におけるランサムウェア被害の報告書では、エンドユーザーを支える専門事業者のセキュリティの取り組みの改善の必要性を指摘しています。加えて、経済産業省では「サプライチェーン強化に向けたセキュリティ対策評価制度」、「サイバーインフラ事業者に求められる役割等のガイドライン」がパブリックコメントを経て制度化が進んでいます。これらの取り組みはユーザー企業のセキュリティ対策を推進するだけでなく、そのユーザー企業のシステムを構築することに携わっている事業者に対しても影響が及ぶものであると考えられます。このため、ユーザー組織がどのようなシステムインテグレーター（以下S I事業者と呼ぶ）からシステムのセキュリティ構築やサービスの提供を受けるかが、セキュリティの強度や安定運用に大きな影響を与えると言う社会的要求が高まっていると言えます。

本文書では、ユーザー組織がセキュリティ対策と運用に配慮したSI事業者を選ぶうえで留意すべき

¹ Ransomware as a Service の略、ランサムウェア本体や身代金要求のためのインフラなどランサムウェア攻撃に必要な一式を「サービス」として提供するものであり、サイバー犯罪のビジネスモデルの1つです。

² JC-STARとは、ETSI EN 303 645 や NISTIR 8425 等の国内外の規格とも調和しつつ、独自に定める適合基準（セキュリティ技術要件）に基づき、IoT製品に対する適合基準への適合性を確認・可視化する、我が国の制度です。

<https://www.ipa.go.jp/security/jc-star/index.html>

確認ポイントを示すことを目指しています。それによって、ユーザー組織がより安心できるシステムを構築し、運用を実現する事が出来るように支援する事を目的としています。また SI 事業者にとっても、質の良い提案やサービス提供のあるべき姿を示すことで、セキュア・バイ・デザインに根差した製品やサービスの提供が、顧客満足度の向上を通して競争優位を生み出す価値の連鎖を生み出していく、そういった市場環境の醸成に繋がる事を期待しております。

【想定読者】

本ガイドラインは、情報システムの調達に際して取引 SI 事業者及び構築作業内容に対する十分なセキュリティ要件を定義せず、調達要件としても契約上明示していない取引の場面を想定しています。また、セキュリティに関するスキルないしは人的リソースに課題を抱えているユーザー組織での利用を想定して記述しています。多くの場合このような組織は、中小企業と呼ばれる規模の組織と定義が重なる場合が多く、同時に大手企業のサプライチェーンを構成する企業である可能性も高いと言えます。加えて比較的小規模な自治体や病院なども同じような課題を共有している可能性があるため、利用することが出来るかもしれません。

また、上記のような顧客のスキルやリソースの課題をシステム構築や運用の外部委託という形で支援している SI 事業者自身が、お客様に信頼をいただける体制やサービスを自己点検したり、お客様に説明したりするために本ガイドラインを利用することも可能です。

【適用範囲】

本ガイドラインで対象とする SI 事業者は、顧客の課題解決のために IT システムを構築する事を主たる生業としている事業者です。その場合、ネットワークやサーバーを含むインフラ構築から行うものと、既に構築されたインフラの上でソフトウェア開発を行うものに分けられます。

- 本ガイドラインは、セキュアなシステムの構築に際しての課題解決を主眼とするため、後者の WEB ページ開発を含むソフトウェア開発事業者は対象にしません。また、IaaS³や PaaS⁴の上でシステムを開発する事業者や SaaS⁵としてサービスをカスタマイズして提供する事業者も対象とはしていません。
- 一方大手システムベンダーから委託を受けて、ネットワーク構築やセキュリティデザインのみを提供するシステム事業者は、課題解決のための IT システムそのものを提供しているわけではありませんが、システムのセキュリティ構築の上では重要な役割を果たすことが多く、元受け

³ IaaS (Infrastructure as a Service : イアス/アイアス) とは、サーバー、ストレージ、ネットワークなどの IT インフラ (基盤) をインターネット経由で提供するクラウドサービスで、ユーザーは物理的なハードウェアを持たずに、必要な分だけ仮想化されたリソースを柔軟に利用・構築・拡張できるモデルです。

⁴ PaaS (Platform as a Service : パース) とは、アプリケーションを開発・実行するための基盤 (プラットフォーム) をインターネット経由で提供するクラウドサービスです。

⁵ SaaS (サース/サーズ) とは「Software as a Service」の略で、インターネットを通じてソフトウェアをサービスとして利用する形態です。

システムベンダーに対する外部委託の上でこのガイドラインを参考にする事は想定されます。

- 準委任契約の形で SES⁶（System Engineering Service）を提供している事業者が構築や運用を請け負う場合、業務委託契約の中でセキュリティ要件を定義している場合があります。その場合は契約条件が上位の概念になるため、本ガイドラインの適用の対象外になります。

【原則】

本ガイドラインは ISMS⁷やプライバシーマーク⁸のような既存の認証制度の要求を網羅するものではありません。従って本ガイドラインに適合している事をもって、何らかの認証要件への適合を保証するものでもありません。網羅性を高め、要件を厳しくすることにより、寄り高いレベルの安心と品質を担保することは出来ます。しかしながら、そのためには継続的な監査や客観的な評価基準、評価を行うものの信頼性の確保といった条件が必須になってきます。こういった網羅性の高い信頼性を保証する認証は、既に実績のある取り組みが存在している為、そちらを活用することを勧めます。

本ガイドラインの使い方としては、日々の SI 事業者との見積もり交渉、業者選定において、或いは公的な認証を持たない SI 事業者間の比較選定に際して、最低限考慮すべき要件を抜き出し、セキュリティへの取り組みを評価する為のものです。また必要に応じて、別紙チェックリストを使用する事で価値を提供できることを目指しています。

基本的な考え方として、本ガイドラインに記載されている要求事項は、あくまでもあるべき姿とそれを実現する為の詳細要件のほんの一部を例として示しているにすぎません。従ってここに記載されていない取り組みであっても、顧客が要求するリスクレベルに合致していれば、それを代替する取り組みを許容する事も、要求事項そのものを無視する事も、使い方として問題が有りません。

さらに言えば、ここに書かれている全ての要求事項を網羅し、100 点満点を目指すことを求めているわけでもありません。あくまでもユーザー企業が想定するリスクレベルと SI 事業者の取り組みレベルが合致しているのか、という判断と確認の為のフレームワークを提供しているわけです。これまで、セキュリティはコストであるという判断は有りつつも、リスクに見合ったコストという考え方が置き去りにされてきたという課題意識から、本ガイドラインは作られています。

⁶ SES（System Engineering Service）とは、IT 業界でエンジニアの技術力や労働力を期間契約で提供するサービス形態で、クライアントの要望に応じてシステム開発や運用をサポートします。

⁷ ISMS は、情報セキュリティの個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用するものです。JIS Q 27001（ISO/IEC 27001）は、ISMS の要求事項を定めた規格であり、組織が ISMS を確立し、実施し、維持し、継続的に改善するための要求事項を提供することを目的として作成されています。

⁸ プライバシーマークは、「個人情報適切に管理している」と評価された事業者が使用できるマークです。個人情報保護の管理レベルの向上やお客様からの信頼獲得のため、現在、約 17,700 社以上の事業者がこのマークを取得しています。

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

【構成の理解】

安定稼働が出来、セキュリティ強度の高いシステムを継続的に利用可能であることを担保出来、必要な情報をコミュニケーションできる SI 事業者を選定する為には、大きく分けて 2 つの軸とそれを構成する 4 つの要件があります。

ユーザーにとって最も重要な一つの目の軸は【ユーザーに提供される価値】です。そして SI 事業者が提供する価値は、「①構築」と「②運用」の二つの要件によって構成されます。セキュリティ面で十分に考慮されたシステムを構築し、継続的に安定運用する事を可能にする SI 事業者こそが信頼できるパートナーです。

もう一つの軸は【SI 事業者によるコミットメント】です。優れた価値を提供する SI 事業者は、それを実現する為に企業としての投資や経営判断を行い、ユーザーとの信頼関係の構築の努力をしているはずです。これは「③企業の姿勢」と「④契約・責任分界の明確化」という二つの要件によって構成されるものです。表面的な謳い文句は素晴らしいが、それを実現するための体制の維持や契約条件による責任の明確化が出来ていない SI 事業者は、安価で構築し、無償のサービスで見積もりを提示してくるかもしれません。しかしながら、セキュリティは継続的な運用が重要です。本当に価値を継続的に提供できる SI 事業者であるか慎重な見極めが必要です。

		SI事業者による コミットメント	
		③SI事業者の体制	④契約・責任分界 の明確化
ユーザーに 提供される価値	①構築業務		
	②運用業務		

図 1：要求のフレームワーク

【ユーザーに提供される価値】

- ① 構築業務：リスクを事前に十分に予測し、それを前提にした提案が出来る。

提案をする前にセキュリティリスクを考慮し、必要とされる対策のあるべき姿を語る SI 事業者の提案は信頼が出来ます。当然ながら投資自体は掛けられるコストと得られるメリットのトレードオフによって顧客が判断するものになります。しかしながら、リスクの全体像を可視化し、何をリスクとして許容したのかが判れば、提案自体の納得性も高まります。

- ② 運用業務：平時の運用を提供するだけでなく、障害発生時にも柔軟に対応できる。

セキュリティは構築をした時点で終わるわけではなく、攻撃手法の変化に伴う対策の強化や脆弱性管理、セキュリティログの監視といった継続的な運用によって担保されるものです。継続的な運用を可能にする知見や体制、サービスの建付けなどを見る事によって、安心して任せられる事の出来る SI 事業者なのかを判断することが出来ます。

【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。

受託業務に対するセキュリティの重要性を認識して業務を遂行することを徹底している事がユーザー企業の求める価値として最も重要です。

その価値提供を実現するためには、経営層が主体となって社内のセキュリティポリシーの徹底と見直しを推進し、人材やセキュリティ対策に継続的に投資する事が担保されている事が求められます。このような SI 事業者から提供されるサービスにおいては、セキュリティを真摯に提案する姿勢が期待できます。

- ④ 契約・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。

セキュリティ対策には 100% の正解は無く、その時点の環境でギャップがどの程度あり、どの程度のリスクを許容しているのかの率直なコミュニケーションが必要です。調達に際してはコストの制約の中で何をどこまで誰が責任を負い、その前提要件で発生しうるリスクを契約の中で明らかにすべきです。

ユーザーが運用するために必要な原則や内容について一定の基準を示すことにより、SI 事業者とユーザーにおける責任分界点を明確化する事が重要です。また、それによって事前に想定すべき脆弱性対応を含む安定的運用をユーザーに定着させ、可能な限りセキュリティインシデントの被害にあわないで済む継続的な取り組みの定着も目指します。

第三章：詳細要件

ここでは、それぞれの業務で要求される詳細要件を説明します。

また、提供される価値を支える SI 事業者の体制と契約の在り方についても同時に説明をします。

以下に示された確認すべき要求事項と実現すべき詳細要件を参考に、構成を捉えながら読み進めてください。

構築業務については I-V1~V5 で確認します。(Implementation-Value の省略)

運用業務については O-V1~V3 で確認します。(Operation-Value の省略)

SI 事業者の体制については C 1~C 4 で確認します。(Company と Commitment の両方の意味)

契約については A1 で確認します。(Agreement の省略)

■ 構築業務：セキュリティリスク評価（I-V1）

大項目	中項目	内容	要求事項（確認事項）
①構築業務	セキュリティリスク評価（I-V1）	リスク分析に基づいてセキュリティ要件を決定する	構築完了時のセキュリティリスクを理解し、顧客に説明できること。

【解説】

- ・ システムを構築する際にセキュリティ対策が後付けになる、あるいは部分的に構築を委託するという事は一般的にあり得ると思います。その場合、システム全体のリスクを全て可視化する事は難しく、導入するソリューションによっては全てのリスクを低減することが出来ない場合も少なくは有りません。
- ・ 重要なのは、どこにどのようなリスクがあるのかを可視化しようとする姿勢と、それを文書などの目に見える記録として提案やコミュニケーションの中で共有しようとする姿勢です。このような姿勢が良い SI 事業者を評価する一つの基準となります。
- ・ 提案時に構築するシステムが実現するセキュリティ強度と期待値とのギャップを認識する事が、構築されるシステムのリスク評価のスタートラインになります。

SI 事業者の体制

事業者への要求	分類	取り組み例
③SI事業者の体制	整備(C1)	下記資格を参考に同等レベルのセキュリティ技術者を確保している ・ 情報処理安全確保支援士 ・ 公認情報セキュリティ監査人 ・ CISSP、CISM、CISA等 ・ ISO27001主任審査員
	強化・定着(C2)	リスクコミュニケーションをプロセス化している。 ・ チェックリストの整備 ・ 説明フォーマット整備 ・ 完了報告書での実施確認
	補強・代替(C3)	リスク評価とその説明能力を補う体制を確保している。 ・ 定期的に内部または外部の研修による技術力の向上を図っている ・ 外部委託による技術力の補完
	継続・改善(C4)	整備・強化・定着及び補強・代替の取り組みを定期的に見直し、改善している。 ・ 導入時には想定外の環境の変化に伴うリスク分析 ・ 上記分析に基づくチェックリストの見直し

整備(C1) : 下記資格を参考に同等レベルのセキュリティ技術者を確保している

- ・ 情報処理安全確保支援士⁹
- ・ 公認情報セキュリティ監査人¹⁰
- ・ CISSP¹¹
- ・ CISA¹²
- ・ CISM¹³
- ・ ISO27001 主任審査員¹⁴

⁹ 情報処理安全確保支援士（通称：登録セキスペ）は、IPA（情報処理推進機構）が実施するサイバーセキュリティ分野の国家資格です。高度な技術・知識で組織の情報システムを攻撃から守り、安全な企画・設計・運用を支援する専門家です。合格率は20%前後、IT系初の登録制士業（試験合格後に登録が必要）として知られます。

¹⁰ 公認情報システム監査人（CISA：Certified Information Systems Auditor）は、ISACAが認定する、情報システムの監査、セキュリティ、統制（コントロール）に関する高度な知識・技能・経験を有するプロフェッショナルを証明する国際的な資格です。ITガバナンスやリスク管理の観点から企業のシステムを評価し、世界的にも高く評価されています。

¹¹ CISSP（Certified Information Systems Security Professional）は、ISC2（国際情報システムセキュリティ認証コンソーシアム）が認定する、国際的に最も権威ある情報セキュリティ・プロフェッショナル認証資格です。セキュリティの技術的知識と経営・管理面を網羅する8分野（CBK）で高い専門性を証明し、世界的に「最強レベル」のセキュリティ資格として高く評価されています。

¹² ISACA（情報システムコントロール協会）が認定する世界共通の国際資格です。ITガバナンス、リスク管理、情報システムの監査・セキュリティに関する高度な専門知識の証明として、監査法人や金融機関などで高く評価されています。

¹³ CISM（Certified Information Security Manager：公認情報セキュリティマネージャー）は、ISACAが認定する、情報セキュリティの戦略、リスク管理、ガバナンスに特化した国際的な上級資格です。セキュリティ管理者（CISOやマネージャー）を対象とし、技術より経営視点での統制力を証明する、セキュリティ分野で特に高い信頼を持つ資格の一つです。

¹⁴ ISO27001（ISMS）主任審査員は、情報セキュリティマネジメントシステムの適合性を評価し、認証機関の審査チームを指揮する専門資格です。

強化・定着(C2)：リスクコミュニケーションをプロセス化している。

- ・チェックリストの整備
- ・説明フォーマット整備
- ・完了報告書での実施確認

補強・代替(C3)：リスク評価とその説明能力を補う体制を確保している。

- ・定期的に内部または外部の研修による技術力の向上。
- ・外部委託による技術力の補完

継続・改善(C4)：整備・強化・定着、及び補強・代替の取り組みを定期的に見直し、改善している

- ・導入当時には想定外の環境の変化に伴うリスク分析
- ・上記分析に基づくチェックリストの見直し

【解説】

- ・ リスク評価を行う上で SI 事業者セキュリティに関して十分な知見を持った技術者が居ないという事は提案や説明そのものの信頼性を大きく損なうものです。
- ・ また、技術者が居ても提案のプロセスの中でチェックし、それを説明する仕組みが無い SI 事業者は結局取り組みが無いのと変わりが有りません。
- ・ ただし、SI 事業者が自社でそのような体制が実現できない場合は、人材の採用、教育によって補強するまでの間、外部委託等によって補完する事も許容されます。
- ・ また、想定するリスクは AI の利用等、技術の進化や攻撃手法の変化に伴って見直される必要があり、その点でもスキルの向上や情報の更新への SI 事業者の取り組みが必要です。

契約・責任分界の明確化(A1)

リスク分析を行うことを説明している（または、明記している）

【解説】

- ・ 宅地建物取引法において重要事項説明書を使用して注意を要する不動産の実態や災害のリスク、未整備な部分の説明が義務化されています。システム構築の際にも、評価したリスク、構築によって低減できたリスク、許容したリスクなどについて、真摯なコミュニケーションを文書ベースで実施し、記録に残すことが合意においては重要です。このような姿勢の SI 事業者は信頼ができます。

■ 構築業務：品質維持（Ⅰ－Ⅴ２）

大項目	中項目	内容	要求事項（確認事項）
①構築業務	品質確保 （Ⅰ－Ⅴ２）	システムのセキュリティの品質確保とは、構築完了時において、セキュリティリスクを最小限にすることである。	構築業務の工程ごとにセキュリティチェックポイントを定め、チェックを実施している。

【解説】

- ・ セキュアなシステム構築は、それぞれの作業の工程における適切なタイミングで行われるセキュリティチェックによって品質を維持する事が必要です。完成時にチェックするだけでなく、作業工程の中で適切なタイミングでセキュリティチェックを行うことを手順化されていることが必要であり、技術者の能力に過度に依存しないSI事業者は高い構築能力を保持していると評価できます。

SI事業者の体制

事業者への要求	分類	取り組み例
③SI事業者の体制	整備(C1)	セキュリティチェックの為にポリシー文書・プロシジャの整備をしている。
	強化・定着(C2)	品質管理責任者の任命をしている。
	補強・代替(C3)	情報処理安全確保支援士等の在籍、ないしは外部委託先の確保をしている。
	継続・改善(C4)	最新の脅威動向に沿ったセキュリティチェック手順の更新をしている。

整備(C1) : セキュリティチェックの為にポリシー文書・プロシジャの整備をしている。

強化・定着(C2) : 品質管理責任者の任命をしている。

補強・代替(C3) : 情報処理安全確保支援士等の在籍、ないしは外部委託先の確保をしている。

継続・改善(C4) : 最新の脅威動向に沿ったセキュリティチェック手順の更新をしている。

【解説】

- ・ セキュアな構築のあるべき姿を示すポリシー文書とそれを確実に実行する手順書を持っている SI 事業者は信頼が出来ます。
- ・ また、品質管理責任者を置いて目を行き届かせている SI 事業者は、構築作業全般にわたって高いレベルの品質を維持する事が可能です。
- ・ また、その作業レベルの信頼性を担保する資格を有している技術者がいるか、または外部委託契約をしている SI 事業者であれば安心ができます。
- ・ そして、その手順書が陳腐化されることなく、適時更新されていく事が重要です。

契約・責任分界の明確化(A1)

完了報告書において品質管理者の承認がある。

【解説】

- ・ 手順通りにセキュリティチェックを行い、作業完了に至ったことを品質管理者が承認し、顧客に提示することができる。

■ 構築業務：完成検査（Ⅰ－Ⅴ３）

①構築業務	完成検査 (Ⅰ－Ⅴ３)	納品時の脆弱性低減 を目指す。	構築完了時のセキュリティチェックリストを整備し、それを顧客に説明できること。
-------	----------------	--------------------	--

【解説】

- 機能要件としてのシステム完成検査は一般的に行われ、想定した機能が実現されている事の判断の方法は確立されていますが、非機能要件であるセキュリティ機能は攻撃を再現する事は容易ではなく、ペネトレーションテストをすべてのシステムに対して行う事はコスト的にも難しい場合があります。
- そのため、セキュリティにおける完成検査では攻撃に対して脆弱な設定を残さないことが重要です。必要なセキュリティの機能を最新のものにアップデートし、機能が可能な限り有効な設定になっているか、管理者パスワードがデフォルトのまま、あるいは安易に予想のつくものになっていないか、不必要に権限共有されているリソースや不必要に露出している IP アドレスが無いかな等の考慮が必要です。
- 最新の攻撃に対応するために IPA¹⁵ や総務省等監督省庁¹⁶ や業界団体等¹⁷ が提供するガイドラインを参照する事が望ましく、取引する構築 SI 事業者がそういった姿勢をもって報告するかが重要です。

IPA¹⁵、総務省¹⁶、業界団体¹⁷

¹⁵中小企業の情報セキュリティ対策ガイドライン

<https://www.ipa.go.jp/security/guide/sme/about.html>

¹⁶ 「地方公共団体における 情報セキュリティポリシーに関する ガイドライン(令和 8 年 3 月版)」

https://www.soumu.go.jp/main_content/001068239.pdf

「医療情報システムの安全管理に関するガイドライン 第 7.0 版 (令和 8 年 6 月)」

https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

¹⁷ 「自動車産業サイバーセキュリティガイドライン」

https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html

SI 事業者の体制

事業者への要求	分類	取り組み例
③SI事業者の体制	整備(C1)	検収完了報告書における設定情報の記載と変更すべき初期値の記載を徹底している。 ・管理者パスワード：初期パスワードのまま使わず、強固なパスワードを使用する ・最新バージョンへ：OSやソフトウェアは常に最新の状態にする ・IPアドレス及び共有設定：不必要に外部に公開されたり、容易にアクセス出来ないか確認する ・セキュリティソフト：パターンファイルは常に最新の状態になるように設定する
	強化・定着(C2)	設定チェックリスト通りになっているかのテストを行うことが出来る。 ・簡易ペネトレーションツールの利用 ・脆弱性診断サービスの提供
	補強・代替(C3)	外部委託先やベンダーとのエスカレーションプロセスを構築している。
	継続・改善(C4)	利用している製品やサービスの脆弱性情報や攻撃手法の変化に対応するために、これらの最新情報を入手しチェックリストへ反映している。
④契約	責任分界の明確化(A1)	完成検査を行うこと、ならびに、完成検査の限界を明記している。

整備(C1)：検収完了報告書における設定情報の記載と変更すべき初期値の記載を徹底している。

- ・管理者パスワード - 初期パスワードのまま使わず、強固なパスワードを使用する
- ・最新バージョンへ - OS やソフトウェアは常に最新の状態にする
- ・IP アドレス及び共有設定 - 不必要に外部に公開されたり、容易にアクセス出来たりしないか確認する
- ・セキュリティソフト／パターンファイルは常に最新の状態になるように設定する

強化・定着(C2)：設定チェックリスト通りになっているかのテストを行うことが出来る。

- ・簡易ペネトレーションツール¹⁸の利用
- ・脆弱性診断サービスの提供"

補強・代替(C3)：外部委託先やベンダーとのエスカレーションプロセスを構築している。

継続・改善(C4)：利用している製品やサービスの脆弱性情報や攻撃手法の変化に対応する為にこれらの最新情報を入手し設定チェックリストへ反映している。

¹⁸ 簡易ペネトレーションツール（簡易侵入テストツール）は、Web アプリケーションやネットワークのセキュリティ上の脆弱性を、自動スキャンや基本的な模擬攻撃（ブルートフォース攻撃など）で手軽に診断するツールです。本格的な手動ペネトレーションテストよりも迅速かつ安価に実施でき、初期段階の脆弱性発見や「ファストペネトレーションテスト」のようなサービスで活用されます。

【解説】

- ・ 近年のセキュリティ事故においては、基本的な設定のミスがなければ防げていた事案も少なくありません。こういった初歩的な見落としを無くすチェックリストの整備とユーザーへの説明の徹底は、信頼できる SI 事業者の判断基準になります。
- ・ そのうえで完成時の脆弱性診断サービスや事後的に発生する脆弱性を発見する為のペネトレーションテストを SI 事業者が提供しているとさらに安心が出来ます。その際には情報セキュリティサービス基準適合サービスリスト¹⁹なども参考に選定をするとさらに安心してサービスを受けることが出来ます。
- ・ また、ベンダーサポートを受けるための基本契約の締結やエスカレーション窓口の明確化など、SI 事業者の対応体制も事前に確認しておくべきです。
- ・ さらに、こういった内容は常に最新の情報に更新されているかを確認することで、信頼できる事業者を確認する事ができます。

セキュリティサービス基準適合サービスリスト¹⁹

契約・責任分界の明確化(A1)

完成検査を行うこと、ならびに、完成検査の限界を明記している。

【解説】

- ・ 完成検査の中で初期設定におけるリスクを排除し、構築における残存リスクの低減を目指しているかどうかを確認することが重要です。また引き渡し後の運用変更や設定変更でリスクが作りこまれる可能性について説明し、完成検査の限界について顧客に説明を行う姿勢を持つ SI 事業者はより信頼できます。

¹⁹ 経済産業省が策定した「情報セキュリティサービス基準」への適合性を審査されたサービス、IPA のサイトで確認が出来ます。

https://www.ipa.go.jp/security/service_list.html

■構築業務：構成管理（Ⅰ－Ⅴ４）

大項目	中項目	内容	要求事項（確認事項）
①構築業務	構成管理 （Ⅰ－Ⅴ４）	IT資産を可視化することでセキュリティリスクの低減をしている	提供する製品やサービスの顧客ネットワークやデータアクセスへの影響度の確認をしている。

【解説】

- ・ 本来的にはネットワーク構成図や IT 資産台帳の整備はユーザーの責任範囲です。しかしながら、人的リソースや能力・知識の問題で情報のメンテナンスが行えていないケースは少なくありません。また、これらの場合、インシデントなどが発生した場合、侵入経路の調査、暫定的対処の策定、影響範囲の特定を難しくします。
- ・ 少なくとも構築または変更されたシステムのネットワーク構成や既存ネットワーク環境との接続状況、新規に追加された IT 資産のリストが提供されなければ、ユーザー自身が資産管理台帳やネットワーク構成図を最新に保つことが難しくなります。
- ・ また、侵入経路や手法から攻撃が成立した原因を特定することが出来なければ、最終的な終結宣言にたどり着くことが出来ない為、SI 事業者の協力体制が不可欠です。

SI 事業者の体制

事業者への要求	分類	取り組み例
③SI事業者の体制	整備(C1)	導入製品の構成情報を提供し、顧客の重要IT資産台帳への情報の記載を支援するプロセスを整備している。
	強化・定着(C2)	ネットワーク構成におけるリスクコンサルティングができる体制の整備をしている。 ・ 情報処理安全確保支援士の在籍、ないしは同等の資格の保有
	補強・代替(C3)	顧客に対して継続的なIT資産の管理を可能にするツールの提供やサービスを提供できる ・ 資産管理ツールの提供及びセキュリティコンサルティングサービスへの外部委託
	継続・改善(C4)	公的機関やセキュリティ団体加盟等による情報の継続的更新をしている。 ・ IPA、JPCERT/CC、JNSA、ISOG-J、Software-ISACなど

整備(C1) : 導入製品の構成情報を提供し、顧客の重要 IT 資産台帳への情報の記載を支援するプロセスを整備している。

強化・定着(C2): ネットワーク構成におけるリスクコンサルティングができる体制整備をしている。
・ 情報処理安全確保支援士の在籍、ないしは同等の資格の保有

補強・代替(C3): 顧客に対して継続的な IT 資産の管理を可能にするツールの提供やサービスを提供できる
・ 資産管理ツール²⁰の提供及びセキュリティコンサルティングサービスへの外部委託

継続・改善(C4): 公的機関やセキュリティ団体加盟等による情報を入手し継続的に更新をしている。
・ IPA²¹、JPCERT/CC²²、JNSA²³、ISOG-J²⁴、Software-ISAC²⁵など

²⁰ 資産管理ツール (IT 資産管理ツール) とは、企業が保有するパソコン、サーバー、ソフトウェア、ライセンスなどの IT 資産を自動で収集・一元管理するシステムです。Excel での手動管理に比べ、情報の更新手間を削減し、資産の「どこに」「何が」あるかを可視化することで、セキュリティ強化、コスト最適化、コンプライアンス遵守を強力に支援します

²¹ 独立行政法人情報処理推進機構 (IPA: Innovation Platform Agency, Japan) 独立行政法人 情報処理推進機構 (IPA) : 経済産業省所管の公的機関。IT パスポートや基本情報技術者などの国家試験の実施、情報セキュリティ対策の普及などを行っています。

²² (一般社団法人 JPCERT コーディネーションセンター) 国内で発生するサイバーセキュリティインシデント (不正アクセスや情報漏えいなど) の被害拡大防止や、脆弱性情報の提供を行う中立的な専門組織です。日本の代表的な CSIRT として、海外機関との連携や注意喚起の発信などを行っています。

²³ NPO 日本ネットワークセキュリティ協会は、ネットワーク社会の情報セキュリティレベルの維持・向上及び日本における情報セキュリティ意識の啓発に努めるとともに、最新の情報セキュリティ技術および情報セキュリティへの脅威に関する情報提供などを行うことで、情報化社会へ貢献することを目的としております。

²⁴ 日本セキュリティオペレーション事業者協議会 (Information Security Operation providers Group Japan 略称: ISOG-J) は、セキュリティオペレーション技術向上、オペレータ人材育成、および関係する組織・団体間の連携を推進することによって、セキュリティオペレーションサービスの普及とサービスレベルの向上を促し、安全で安心して利用できる IT 環境実現に寄与することを目的として設立されました。

²⁵ Software ISAC は一般社団法人ソフトウェア協会のセキュリティ委員会が母体となり、2018 年からセキュリティに関する情報共有、PSIRT の設置推進などの活動をソフトウェア協会会員向けに行っています。

【解説】

- ・ 構築したシステムのネットワーク構成図、IT 資産のリストをユーザーに提供するプロセスが SI 事業者にあることが大前提になります。
- ・ またデータを提供する事だけでなく、リスク面での十分な説明がされたうえで引き渡しされる事が求められます。そのためには十分な知見を持った技術者が SI 事業者にいることがより望ましいです。
- ・ IT 資産の管理を台帳管理で行うことはメンテナンス性や実態との乖離などの面で様々な課題があります。そういった場合、資産管理ツールやセキュリティコンサルティングサービスによって、運用の精度や実効性を担保することが可能になりますので、こういったサービスの提供が出来るないしは紹介が出来る SI 事業者を選ぶと安心が出来ます。
- ・ より効率的で安全性の高い資産管理の在り方についての情報は、経済産業省と Software-ISAC が継続的に議論しており、ISOG-J では実用性の高いベストプラクティスを提供しており、SI 事業者はこういった情報に常に触れている事が求められます。

契約・責任分界の明確化(A1)

導入した IT 資産の管理の必要性和責任の範囲を説明・合意をしている。

【解説】

- ・ 安定したシステム運用において資産管理は基本中の基本です。しかしながら、導入済みのシステムの資産台帳を事後的に作成する事は非常に工数がかかり、多くの企業 IT 部門の課題となっています。少なくとも新しく導入するシステムの資産管理から整備していく事で資産管理の網羅性は高まっていくはずです。そういった意味で導入構築時に資産管理の重要性を理解し、必要な情報を提供する姿勢がある SI 事業者であるかどうかは重要な確認ポイントです。
- ・ また、導入後の管理情報の更新はユーザーの責任で行う必要であることが原則ですが、マネージドサービスのような外部委託の形態をとった際に責任の範囲が曖昧になることがあります。そういった際に責任の範囲を明確に伝え、必要な管理体制を顧客に説明する姿勢も重要な確認ポイントとなります。

■ 構築業務：サプライチェーン管理（Ⅰ－Ⅴ５）

大項目	中項目	内容	要求事項（確認事項）
①構築業務	サプライチェーン管理 （Ⅰ－Ⅴ５）	委託先を起点とした 顧客データの漏洩リ スクを低減している	取引先との情報セキュ リティ対策の合意をし ている。

【解説】

- ・ 昨今の情報漏洩事案の一つの特徴として、IT サービスを提供する外部委託先に預けた情報が漏洩する事案が増加する傾向が有ります。自社内に IT システムを運用する十分なリソースが無い企業においては、そのリスクが高くなる可能性があります。
- ・ また、委託先のさらに先で二次委託されている場合、二次委託先が不正アクセスの被害にあう事で情報が漏洩する場合は有り、プライムに立つ事業者とのセキュリティ合意だけでは不十分な状況が有ります。
- ・ こういった中、政府においてはサプライチェーンセキュリティに対する取り組みが結果として、産業全体のセキュリティ強度を高め、事業継続性に寄与すると考え、サプライチェーンセキュリティ評価制度を 2027 年度を目途にスタートさせる予定です。
- ・ また、システムサポートの為、SI 事業者からのリモートアクセスを常時許可した事による間接的侵入や、システム連携の為に常時接続を許可していた委託事業者が脆弱性を突かれてランサムウェアの侵害の起点になった事案は記憶にも新しく、サプライチェーン全体における情報セキュリティの確認が不可欠になってきています。

SI 事業者の体制

事業者への要求	分類	取り組み例
③SI事業者の体制	整備(C1)	自社の情報セキュリティポリシーを外部認証等により担保し、公表している。 ・ISMS、プライバシーマーク、ISMAP等
	強化・定着(C2)	外部委託先を含めた情報セキュリティポリシーの教育、周知の徹底をし、定期的に確認を行っている。
	補強・代替(C3)	外部委託先に情報セキュリティ監査を実施、または、情報セキュリティ監査報告書の提示など、外部委託先の第三者監査を受けている
	継続・改善(C4)	外部委託先の認証の更新確認の実施、ないしは外部委託先に対する継続的実地監査の実施をしている。

整備(C1)：自社の情報セキュリティポリシーを外部認証等により担保し、公表している。

・ISMS²⁶、プライバシーマーク²⁷、ISMAP²⁸、ISMS クラウドセキュリティ認証²⁹等"

強化・定着(C2)：外部委託先を含めた情報セキュリティポリシーの教育、周知の徹底をし、定期的に確認を行っている。

補強・代替(C3)：外部委託先に情報セキュリティ監査を実施、または、情報セキュリティ監査報告書の提示など、外部委託先の第三者監査を受けている

継続・改善(C4)：外部委託先の認証の更新確認の実施、ないしは外部委託先に対する継続的監査の実施をしている。

²⁶ ISMS (Information Security Management System：情報セキュリティマネジメントシステム) とは、企業が保有する情報を「機密性」「完全性」「可用性」の3要素を保ち、情報漏洩や改ざん、紛失といったリスクから守るための総合的な管理体制・仕組みのことです。国際規格 (ISO/IEC 27001) に基づいて構築・運用されます。

²⁷ プライバシーマーク (P-Mark) は、JIS Q 15001 (個人情報保護マネジメントシステム) に準拠し、個人情報を適切に管理・保護している企業を第三者機関が認定し、その証として付与するマークです。一般財団法人日本情報経済社会推進協会 (JIPDEC) が運用し、取得企業はウェブサイトやパンフレットに掲示して信頼性をアピールできます。

²⁸ ISMAP (イスマップ：Information system Security Management and Assessment Program) は、政府が求めるセキュリティ基準を満たしたクラウドサービスを事前に評価・登録する「政府情報システムのためのセキュリティ評価制度」です。2020年に運用が開始され、政府機関は原則としてこのリストに掲載されたサービスから調達することで、安全かつ円滑なクラウド導入を実現しています。

²⁹ ISMS クラウドセキュリティ認証 (ISO/IEC 27017) は、クラウドサービス特有のセキュリティリスク (データ共有、責任分解など) に対応した国際的な管理規格。従来の ISO/IEC 27001 (ISMS) にアドオン (追加) する形で、クラウドの提供側 (CSP) と利用側 (CSC) 双方の安全性を第三者機関が認定し、信頼性を担保します。

【解説】

- ・ 委託先のセキュリティの取り組み状況を個別具体的に評価する事は工数的にも負担が大きく、知見の無い中で実施しても実効性の伴わないものになる可能性が高くなります。その場合、既存の ISMS や P-Mark のような第三者認証の取得状況を確認する事を推奨します。また、クラウドサービスを利用している場合には、ISMAP や ISMS クラウドセキュリティ認証なども参考にすると良いでしょう。
- ・ また、先に述べたサプライチェーン強化の為にセキュリティ対策評価制度(SCS 評価制度³⁰、2027 年度より開始)は、SI 事業者も取得が推奨されるため、今後はこういった制度を参考にすることも出来るようになるでしょう。
- ・ 外部委託先の情報セキュリティ合意については上記認証の中で管理策として網羅されていますが、実効性を担保するためには外部委託先に対しての合意したセキュリティポリシーや監査の状況を追加で確認する事も可能です。
- ・ また、外部アドバイザーによるサプライチェーンセキュリティ対策の見直しや自社では気づかない情報漏洩のリスクや兆候をいち早く察知する通報窓口の設置なども設置されている事は安心材料になります。
- ・ 契約時点での外部委託先の取り組みが運用期間にわたって実施されている事を継続的に担保する事業者の取り組みが有る事がより望ましい姿です。

SCS 評価制度³⁰

契約・責任分界の明確化(A1)

業務委託契約における情報セキュリティポリシー遵守の宣言、及び外部委託先との間の情報セキュリティに関する取り決めがある。

【解説】

- ・ 業務委託契約を行う際に第三者認証を取得している事が確認できる事が最も信頼性が高いですが、IPA プラクティス・ナビ³¹などを参考に独自にチェックし判断することも出来ます。

ベストプラクティスナビ³¹

³⁰ 委託先へのサイバー攻撃等を起因とした自社事業・サービスの提供途絶／機密情報の漏えい、改ざんや委託先等を踏み台とした不正侵入等のリスクに対する適切なセキュリティ対策の実施を促し、サプライチェーン全体でのセキュリティ対策水準の向上を図ることを目的とし 2 社間の取引契約等において、委託元が、委託先に適切な段階（☆3，☆4）を提示し、示された対策を促すとともに実施状況を確認することを想定

³¹ 「プラクティス・ナビ」は、企業が「サイバーセキュリティ経営ガイドライン」の内容を実践する際の、実際に行われている事例に基づく実践手順や取組の例を検索するためのサイトです。カテゴリやトピックを選択することで、知りたいプラクティスを見つけることができます。

<https://www.ipa.go.jp/security/economics/practice/>

■ 運用業務：インシデント対応（O－V1）

大項目	中項目	内容	要求事項（確認事項）
②運用業務	インシデント対応 （O－V1）	インシデントにおけるログ分析の重要性を認識し、分析を元に判断している	インシデント対応窓口の設置及び対応能力の維持をしている。

【解説】

- ・ システムは構築が終わった時点で運用開始を迎えますが、実際にはシステムが業務で使用される期間にわたって安定稼働の為の運用が必要になります。
- ・ 特にセキュリティに関しては、ランサムウェアのようにある日突然システムが暗号化され使用できなくなる場合もあれば、機能としては正常に動作しているものの、知らないうちに重要な情報が外部に流出し、風評被害や取引先からの損害賠償リスクなどに巻き込まれる場合もあります。
- ・ このような運用上のリスクに備えるためには、いずれのケースにおいてもセキュリティにおける監視が欠かせません。直近の事例では EDR³² のような最新の技術を導入していても監視が十分ではなく、ランサムウェア被害にあった事案も存在しています。
- ・ 自社で監視やインシデント対応が出来ない場合、運用事業者に依存するほかなく、マネージドサービスという形で運用をアウトソースする必要が発生し、実インシデント対応の為には別途インシデントレスポンスサービスを提供する企業と個別契約を締結する必要が有ります。
- ・ いずれにしても監視を平時からしっかりと行い、調査の際に遡って調査が出来るように十分な期間ログを保持出来ている事を常に確認しておく必要が有ります。

EDR³²

³² EDR（Endpoint Detection and Response）は、エンドポイント上の不審な振る舞いを継続的にスキャンし、潜在的な脅威を検知するセキュリティソリューションです。これにより、攻撃の早期発見と迅速な対応が可能になり、サイバー攻撃による被害を効果的に軽減します。従来のセキュリティ対策では、マルウェアなどの侵入を防ぐことに主眼が置かれてきましたが、EDR は侵入されることを前提に、異常をいち早く発見して対処するという考え方に基づいています。侵入を完全に防ぐことが難しくなった今日では、万が一のすり抜けに対して、被害を最小限に抑えるために EDR のような検知・対応型のソリューションが不可欠です。

SI 事業者の体制

事業者への要求	分類	取り組み例
③SI事業者の体制	整備(C1)	インシデント対応窓口の設置、エスカレーションフローの文書化、FAQ等の開示をしている。
	強化・定着(C2)	SI事業者においてインシデントレスポンス能力を持った技術者の育成を行っている。 ・ベンダーの実施するトレーニングへの技術者派遣 ・公的機関やセキュリティ団体における勉強会への積極的参加
	補強・代替(C3)	自社の能力を超える場合の外部委託先（インシデントレスポンス、マネージドサービス含む）、ベンダーエスカレーション先の紹介をできる。
	継続・改善(C4)	情報セキュリティサービス基準審査登録制度の適合基準を参考に、社内リソースの拡充と継続的な育成を実施している。

整備(C1)：インシデント対応窓口の設置、エスカレーションフローの文書化、FAQ 等の開示をしている。

強化・定着(C2)：SI 事業者においてインシデントレスポンス能力を持った技術者の育成を行っている。

- ・ベンダーの実施するトレーニングへの技術者派遣
- ・公的機関やセキュリティ団体等における勉強会への積極的参加

補強・代替(C3)：自社の能力を超える場合の外部委託先（インシデントレスポンス、マネージドサービス含む）、ベンダーエスカレーション先の紹介をできる。

継続・改善(C4)：情報セキュリティサービス基準審査登録制度の適合基準を参考に、社内リソースの拡充と継続的な育成を実施している。

【解説】

- ・ インシデントの発生の際にその窓口で受け付けられるのか、対応できる時間帯は明示されているか、対応が有償か無償かなどが明確になっている必要が有ります。
- ・ また、インシデントレスポンスの対応スキルを持っている技術者がいるのかも確認しておくとい良いでしょう。
- ・ 運用事業者そのものがインシデント対応の能力を持っていない場合は、対応可能なベンダーやインシデントレスポンスサービスを提供する企業へ相談できるルートを確認しているかどうかを確認しましょう。
- ・ 質の高いインシデントレスポンスサービスを運用事業者が提供する際には、「情報セキュリティサービス基準」への適合性を審査された情報セキュリティサービス基準適合サービスリストへの登録ないしは、それと同等の能力をもっているかどうかなどを確認すると良いでしょう。

契約・責任分界の明確化(A1)

インシデント発生時、無償サービスで対応できる範囲、有償サービスで提供できる範囲の文書化をしている。

【解説】

- ・ 製品やシステムのサポートサービスにはインシデント対応は含まれていない事がほとんどです。一般的にセキュリティインシデントは、悪意のある第三者の不正な行為や運用の不備に起因するものであると考えられている為です。
- ・ このような責任範囲の明確化や有事の際にかかるコストの想定を平時から認識し、判断をスムーズに行うことは難しいため、見積もり段階から明確にする事業者は信頼が出来ます。(JCSSA の情報機器販売時のガイドライン³³)
- ・ また、窓口の対応可能時間、SLA³⁴ や SLO³⁵ などの対応時間の目安についても確認をしておくが良いでしょう。

JCSSA 情報機器販売時のガイドライン³³、SLA³⁴、SLO³⁵

³³ JCSSA（一般社団法人日本コンピュータシステム販売店協会）セキュリティ委員会では販売店が情報機器の販売時の責任範囲を明確にし、必要な原則や内容について一定の基準を示すことにより、販売店と利用者間における責任分界点を明確化することを目的とした、《情報機器販売時のガイドライン》をリリースいたしました。

https://www.jcssa.or.jp/backing_index/guideline_securityservice/

³⁴ SLA（Service Level Agreement：サービス品質保証）は、通信やクラウドサービスなどの事業者と利用者の間で、提供するサービスの品質（可用性、応答時間、速度など）に関する目標水準と、それを下回った場合のペナルティ（返金など）を明確に定めた契約のことです。主に IT 分野でトラブルを避け、信頼性を担保するために用いられます。

³⁵ SLO（Service Level Objective：サービスレベル目標）は、システムやサービスの信頼性を担保するため、稼働率や応答速度などについて提供者側が設定する「具体的な目標値」のことです。SLA（契約）とは異なり、未達成でも法的罰則はないが、安定的な運用のための内部目標として利用されます。

■ 運用業務：脆弱性対応（O－V2）

大項目	中項目	内容	要求事項（確認事項）
②運用業務	脆弱性対応 （O－V2）	脆弱性情報を速やかに入手し業務に反映している	脆弱性情報の継続的入手体制が構築され、適時顧客に提供するプロセスを構築している

【解説】

- ・ システムの脆弱性を悪用した攻撃は IPA が発表する情報セキュリティ 10 大脅威に直近 6 年連続 9 回もランクインしており、中でもコロナ禍のテレワークの活用を機に広がった SSL-VPN³⁶ や RDP³⁷ の利用とその脆弱性を突く攻撃は、ランサムウェア被害では侵入の手法として常態化して居る状況です。
- ・ 昨今のサイバー攻撃は脆弱性を利用して基盤を構築し、より高い権限を奪取したうえでセキュリティ機能を無効化するというのが一般的になっています。境界型防御を突破され、アンチウィルス機能の無効化をされてしまうと、侵害に気づくことは非常に難しく、より高度なセキュリティ監視を行っていない限り攻撃を防ぐことは出来ません。従って脆弱性情報を積極的に入手し、対処していく運用が必要です。
- ・ また、近年の AI の急激な能力の向上により、セキュアコーディングを実現する事が可能になっているのと同時に、脆弱性の発見数と攻撃に悪用されるまでの時間も大幅に短縮されています。以前はパッチ適用による影響度調査の為に十分に時間をかける事が可能でしたが、例え重要なシステムがシステム停止するリスクを負ってでも、攻撃が成立する前にパッチ適用をしなければならない時代が来た、と、NCO を始め金融庁などからも発信を始めています。

SSL-VPN³⁶、RDP³⁷

³⁶ SSL/TLS 技術を用いてインターネット上に安全な暗号化通信路（トンネル）を構築し、社内ネットワークへリモートアクセスする技術です。Web ブラウザ（HTTPS）を利用するため専用ソフトが不要で、導入コストが低く、テレワークや出張時の社内システム接続に広く利用されています。

³⁷ Microsoft が開発した、Windows PC やサーバーに遠隔地からネットワーク経由でアクセスし、画面操作やデータ編集を行うための通信プロトコル（規約）です。主に Windows の「リモートデスクトップ」機能で使用され、安全な通信のために暗号化に対応しています。

SI 事業者の体制

事業者への要求	分類	取り組み例
③SI事業者の体制	整備(C1)	顧客納入システムの機器名称、バージョンなどの情報を記録し、顧客への的確な情報提供が出来る体制の確保をしている。
	強化・定着(C2)	最新の脆弱性に対する攻撃情報を提供するプロセスの構築をしている。 ・パッチ情報や攻撃情報（注意喚起）などを提供。 ・定期的に学ぶ機会の提供。 ・脆弱性診断サービス等の提供。
	補強・代替(C3)	外部委託による脆弱性診断サービスの提供。 セキュリティ団体を通じて早期警戒情報を入手することが出来る情報流通網を持っている。
	継続・改善(C4)	ベンダーからの情報提供窓口が常に更新され、情報の入手に問題が無いかを定期的に見直ししている。

整備(C1):顧客納入システムの機器名称、バージョンなどの情報を記録し、顧客への的確な情報提供が出来る体制の確保をしている。

強化・定着(C2):最新の脆弱性に対する攻撃情報を提供するプロセスの構築をしている。

- ・定期的に学ぶ機会の提供。
- ・脆弱性診断サービス等の提供。

補強・代替(C3):外部委託による脆弱性診断サービスの提供。

- ・公的機関やセキュリティ団体等を通じて早期警戒情報を入手することが出来る情報流通網を持っている。

継続・改善(C4):ベンダーからの情報提供窓口が常に更新され、情報の入手に問題が無いかを定期的に見直ししている。

【解説】

- ・脆弱性管理の為に情報資産台帳の作成が必要ですが。製品やバージョンの情報を正確に把握し、タイムリーに提供されない限り、計画的な運用は難しくなります。
- ・脆弱性管理は対応の緊急度と緩和策の容易さに依存する為、そういった周辺情報を提供できる能力の有無がユーザーの運用の上では重要な確認ポイントになります。
- ・自社に十分なリソースを持たない運用事業者は、外部委託によって脆弱性診断サービスやペネトレーションテストを提供できるようにする。ソフトウェア協会、JNSA や ISOG-J などの団体に加盟し、脆弱性管理に関する最新の情報を入手しているかを確認してください。
- ・常に最新の情報提供に問題が無いかのチェックをしているかを確認してください。
- ・また今後はソフトウェアの構成管理を可能にするために開発元からの SBOM の提供が推奨されていく事が世界的な動きになっているので、こういった情報を理解しているかどうか良い SI 事業者を選定する一つの判断基準になるかもしれません。

契約・責任分界の明確化(A1)

脆弱性情報の入手先情報の提供および、納品時におけるベンダーサポート窓口の登録の徹底をしている。

【解説】

- ・ 脆弱性情報の提供がサポート契約の中で明記されているかを確認しましょう。
- ・ またパッチの適用に伴う検証や作業の実施が運用契約の中に含まれているかどうかを確認しましょう。
- ・ 有償・無償の範囲を明確にし、文書化しているかも確認が必要です。
- ・ ユーザーが脆弱性情報を自分で情報を入手するのか、サポートニュースとして受信するのかを確認しましょう。その際、ベンダーのサイトに登録をしなければ情報が配信されない、閲覧することが出来ないなどの条件があるかどうかを確認する必要が有ります。

■ 運用業務 ：保守・保全（O－V3）

大項目	中項目	内容	要求事項（確認事項）
②運用業務	保守・保全 （O－V3）	サポート範囲、条件 を顧客と合意してい る	サポート範囲、条件を 合意する手続きがある

【解説】

- ・ サポート範囲について契約の中で合意する事はごく当たり前のように行われていますが、セキュリティは契約内で想定していない事象に対処する事が求められる為、事後的に対処する際の対応と責任範囲を事前に把握しておく必要が有ります。
- ・ システムすべてを構築から運用まで提供する場合にはサポート範囲や条件を明文化する事は容易ですが、システムのセキュリティ部分のみを二次委託されて構築・運用する場合、責任範囲の切り分けが非常に難しくなります。
- ・ システム間連携によって互換性の問題が発生したり、複数の異なるダッシュボードをまたがる監視を行ったりする事で責任の所在が曖昧になり、運用の精度を落とすことも考えられます。コストに見合うセキュリティレベルの差が明確に出るわけではないので投資判断が難しく、ベネフィットの大きさとバランスする運用上のリスクの許容が必要になってきます。

SI 事業者の体制

事業者への要求	分類	取り組み例
③SI事業者の体制	整備(C1)	構築した製品に関するサポートを自社で提供できる能力を有している。
	強化・定着(C2)	ベンダーが提供する資格を取得するための教育の機会を技術者に提供している。あるいは一般的な情報セキュリティ資格の取得を推奨している。
	補強・代替(C3)	ベンダーとの間でサポート契約を締結しており、エスカレーションや支援を受ける体制が構築されている。
	継続・改善(C4)	顧客サポート満足度に関する評価基準を持ち、顧客に高い品質のサポートを提供出来ているかを可視化し、継続的に改善している。

整備(C1) :構築した製品に関するサポートを自社で提供できる能力を有している。

強化・定着(C2):ベンダーが提供する資格を取得するための教育の機会を技術者に提供している。

あるいは一般的な情報セキュリティ資格の取得を推奨している。

補強・代替(C3):ベンダーとの間でサポート契約を締結しており、エスカレーションや支援を受ける体制が構築されている。

継続・改善(C4):顧客サポート満足度に関する評価基準を持ち、顧客に高い品質のサポートを提供出来ているかを可視化し、継続的に改善している。

【解説】

- ・ ソリューションを安定して運用する為には、きちんとした知見を持ったサポートが提供できる体制のある事業者からサービスを受けるようにしましょう。
- ・ ベンダー依存ではなく、スキルを常に向上させ自社で切り分けが出来る体制を持つ運用事業者を選びましょう。そのためには会社として技術者に投資し、日々研鑽を促す企業かどうかを見極めていく事が大切です。資格者の数や研修の頻度などでそれを知ることができます。
- ・ 団体に加盟し、WG 活動に積極的に参加する企業は情報の鮮度にこだわり、最新の技術動向や脅威に基づいた運用提案が期待できます。
- ・ 顧客満足度に対する KPI を持ち、課題をヒアリングし改善していく体質のある SI 事業者であれば、安心して運用サービスを受けることができます。

契約・責任分界の明確化(A1)

サポート受付時間などのサポート条件の明示。無償サポート範囲と有償サポート範囲の文書化及び顧客説明の徹底、合意のプロセスの徹底をおこなっている。

【解説】

- ・ 製品サポートと運用業務支援、運用コンサルティング、インシデント対応などセキュリティ運用の中には多くの要求があります。
- ・ しかしながら、インシデント発生の際には緊急性を要するが余り、これらの境が曖昧になり、過大な要求を求める事になるのが一般的です。
- ・ 普段から起こり得る事態をシュミレーションし、必要なアクションを文書化し、事業者と事前に対応を合意する事が重要です。
- ・ また、経営層の有事の意思決定は、緊急の投資コストや事業判断を得る際にも必ず必要になってきますので、経営層も交えてシュミレーションし文書化していく事を推奨します。

第四章：チェックリストの使い方

本ガイドラインに付録としてついてくるチェックリストは、ある意味理想を並べた要望リストです。実際の提案の中で、このすべてを網羅した体制と提案を提供してもらう為には、それなりのコスト負担をユーザーは覚悟しなければなりません。それでも事業継続性の上で重要なシステムがセキュリティ侵害に見舞われて事業継続性に影響を与える事になれば、ビジネスインパクトはその投資をはるかに超える甚大なものになる、という事案が数多く報告されています。

重要なシステムに対しては、経営層が覚悟を決めて投資をしていく事を求められますが、資産価値がそれほど高くないシステムにはリスクを許容したり、リスクを保険等に移転したりするという考え方もあると思います。

システムを構築や運用を外部事業者へ委託する場合において、委託する外部事業者へ何をどこまで求めるか、そして、それを確認する必要があります。この時、自社が何を重視して、何を重視しないかなど自社のリスクを確認し、そのリスクをどこまで許容するかについて、経営層も含め確認・許容することが必要です。その結果を意識して委託する事業者を選定するために、このチェックリストを活用してください。

概念的な内容が並んでいるので教科書的に使う事は出来ないかもしれませんが、個々の会社の業種、業態、取引先からの要求によって求められるものの濃淡は変わってくると思います。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って、本ガイドラインの結びとさせていただきたいと思います。

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事を目指しております。

第五章：附則

■ 関連資料

中小企業の情報セキュリティ対策ガイドライン

<https://www.ipa.go.jp/security/guide/sme/about.html>

5分でできる！情報セキュリティ自社診断

<https://www.ipa.go.jp/security/guide/sme/5minutes.html>

情報セキュリティ 10 大脅威

<https://www.ipa.go.jp/security/10threats/index.html>

サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針（案）

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/20251226_report.html

サイバーインフラ事業者に求められる役割等に関するガイドライン案

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/cyber_infrastructure/202503_guidelines.html

セキュリティ要件適合評価及びラベリング制度（JC-STAR）

<https://www.ipa.go.jp/security/jc-star/index.html>

情報セキュリティサービス基準適合サービスリスト

https://www.ipa.go.jp/security/service_list.html

■ 改訂履歴:

日付	バージョン	変更箇所	承認者
2026-10-1	V1.0	初版	下村正洋

■ 執筆者

氏名	所属	役職
下村正洋	一般社団法人日本IT団体連盟理事・サイバーセキュリティ委員会	委員長
立石聡明	一般社団法人日本インターネットプロバイダー協会	副会長
原 洋一	一般社団法人ソフトウェア協会	前事務局長
田上利博	一般社団法人ソフトウェア協会・サイバーセキュリティ委員会 サイバートラスト株式会社	副委員長
尾崎嘉一	日本コンピュータシステム販売店協会・セキュリティ委員会 株式会社ソフトクリエイト	委員
持田啓司	日本ネットワークセキュリティ協会 株式会社ラック	幹事
谷 建志	サイバーセキュリティ委員会 DX with Cybersecurity 分科会 大日本印刷株式会社	委員
日向 亨	サイバーセキュリティ委員会 DX with Cybersecurity 分科会 トレンドマイクロ株式会社	主査