情報セキュリティ事故から見る開発段階で求められること及びISMSから見た対応

2025年9月25日
一般財団法人日本科学技術連盟
ISO審査登録センター　審査部　情報セキュリティ審査室

目次

1. 昨今の情報セキュリティ事故
2. 現場と現況
3. 現況への取り組み
4. 日科技連　ISO審査登録センターが提供するサービス

1．昨今の情報セキュリティ事故

昨今の情報セキュリティ事故　①
（IPA　2025年 情報セキュリティ10大脅威）

情報セキュリティ10大脅威　2025

「情報セキュリティ10大脅威 2025」は、2024年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約200名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものです。

◢ 情報セキュリティ10大脅威 2025 [組織]

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

IPA（情報処理推進機構）「情報セキュリティ10 大脅威 2025」 https://www.ipa.go.jp/security/10threats/10threats2025.html

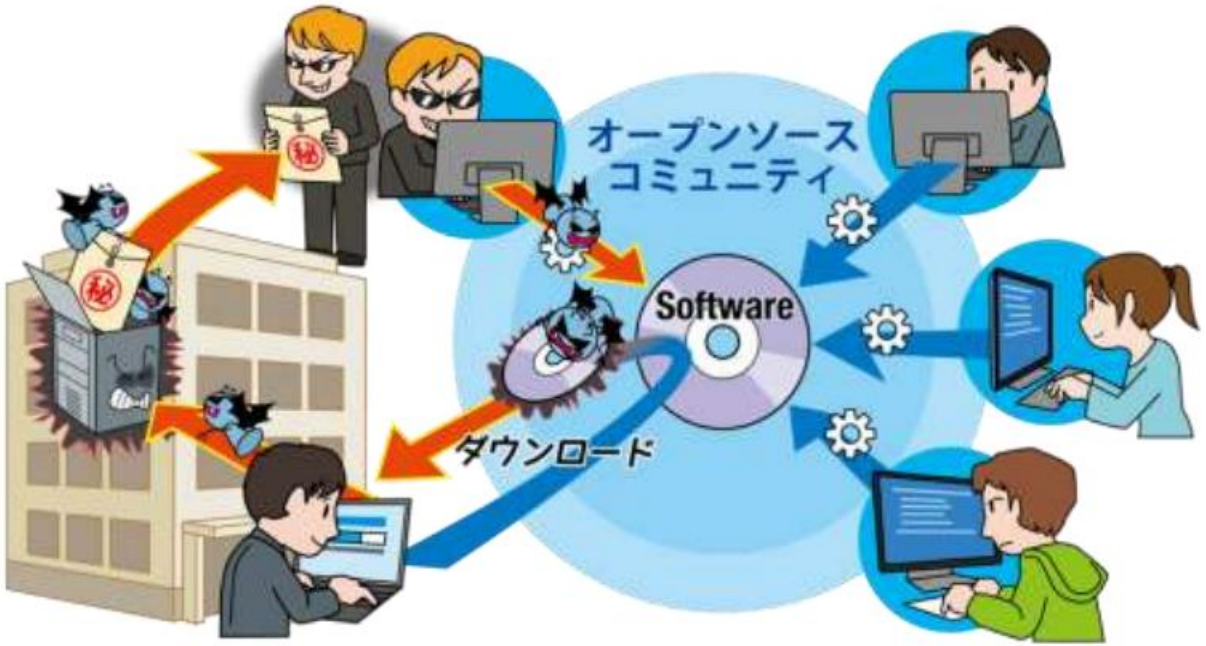
第1位　ランサム攻撃による被害

　ランサムウェアとは、PC やサーバーに感染後、端末のロックやデータの窃取、暗号化を行い、これらを取引材料とした様々な脅迫により金銭を要求するマルウェアの一種である。ランサムウェアを用いた攻撃をランサム攻撃と呼び、攻撃者は複数の脅迫を組み合わせて、被害組織が金銭の支払いを検討せざるを得ない状況を作り出そうとする。

IPA（情報処理推進機構）「情報セキュリティ10 大脅威 2025　組織編」 P.11～P.30より一部抜粋

第2位　サプライチェーンや委託先を狙った攻撃

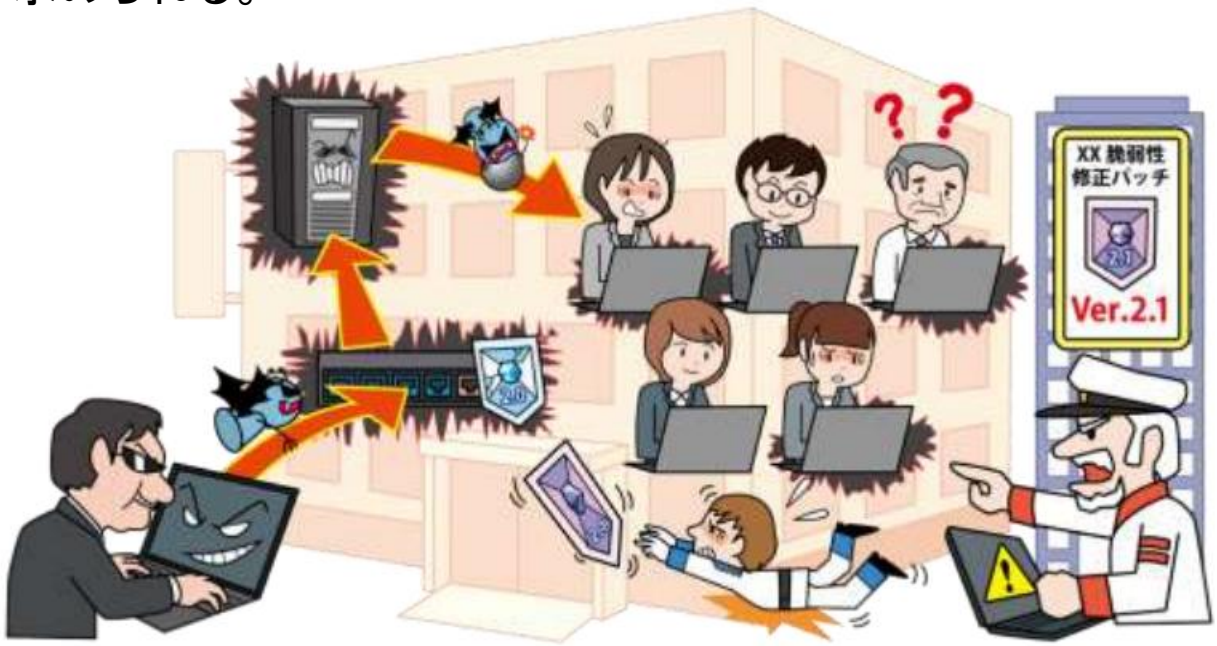
商品の企画、開発から、調達、製造、在庫管理、物流、販売までの一連のプロセス、およびこの商流に関わる組織群をサプライチェーンと呼ぶ。このような「ビジネス上の繋がり」を悪用した攻撃は、自組織の対策のみでは防ぐことが難しいため、取引先や委託先も含めたセキュリティ対策が必要な脅威と言える。また、ソフトウェア開発のライフサイクルに関与するモノ（ライブラリ、各種ツール等）や人の繋がりをソフトウェアサプライチェーンと呼ぶ。このような「ソフトウェアの繋がり」を悪用した攻撃もまた脅威であり、対策が求められる。



IPA（情報処理推進機構）「情報セキュリティ10 大脅威 2025　組織編」 P.11～P.30より一部抜粋

第3位　システムの脆弱性をついた攻撃

製品の開発ベンダー等による脆弱性対策情報の公開は、脆弱性の存在や対策の必要性を製品利用者に対して広く呼び掛けることができる。他方、攻撃者はその情報を悪用し、脆弱性対策が講じられていないシステムを狙って攻撃を行うことがある。なお、脆弱性対策情報を公開する前に行われる脆弱性を悪用した攻撃をゼロデイ攻撃と呼ぶ。脆弱性対策ができていない場合、マルウェア感染等に留まらず、事業やサービスの停止等に端を発し、甚大な被害に至ることもある。昨今、脆弱性が発見されてから、それを悪用した攻撃が発生するまでの時間が短くなっているため、脆弱性対策情報が公開された場合、早急な対策の実施が求められる。



IPA（情報処理推進機構）「情報セキュリティ10 大脅威 2025　組織編」 P.11～P.30より一部抜粋

第4位　内部不正による情報漏えい等

従業員や元従業員等、組織の内部関係者による意図的な機密情報の持ち出しや社内情報の削除等の不正行為が発生している。また、組織の情報管理規則に背き情報を持ち出し、不注意で情報を紛失し、情報漏えいになるケースもある。組織の内部関係者による不正行為は、社会的信用の失墜、損害賠償や業務停滞等による経済的損失を招く。また、不正に取得された情報を使用した組織や個人も責任を問われる場合がある。

IPA（情報処理推進機構）「情報セキュリティ10 大脅威 2025　組織編」 P.11～P.30より一部抜粋

第5位　機密情報等を狙った標的型攻撃

標的型攻撃とは、特定の組織（民間企業、官公庁、団体等）を狙う攻撃のことであり、機密情報等の窃取や業務妨害を目的としている。攻撃者は社会の動向や慣習の変化に合わせて攻撃手口を変える等、標的とする組織の状況に応じた巧みな攻撃手法で目的を果たそうとする。

IPA（情報処理推進機構）「情報セキュリティ10 大脅威 2025　組織編」 P.11～P.30より一部抜粋

第6位 リモートワーク等の環境や仕組みを狙った攻撃

リモートワークの浸透により、働き方の多様化が定着しつつある。しかし、リモートワークの実現に必要な環境や仕組みを狙ったサイバー攻撃が多発している。攻撃を受けるとマルウェア感染や情報漏えい等、様々な不正アクセスが行われ、組織の事業が停止するおそれがある。

IPA（情報処理推進機構）「情報セキュリティ10 大脅威 2025　組織編」 P.11～P.30より一部抜粋

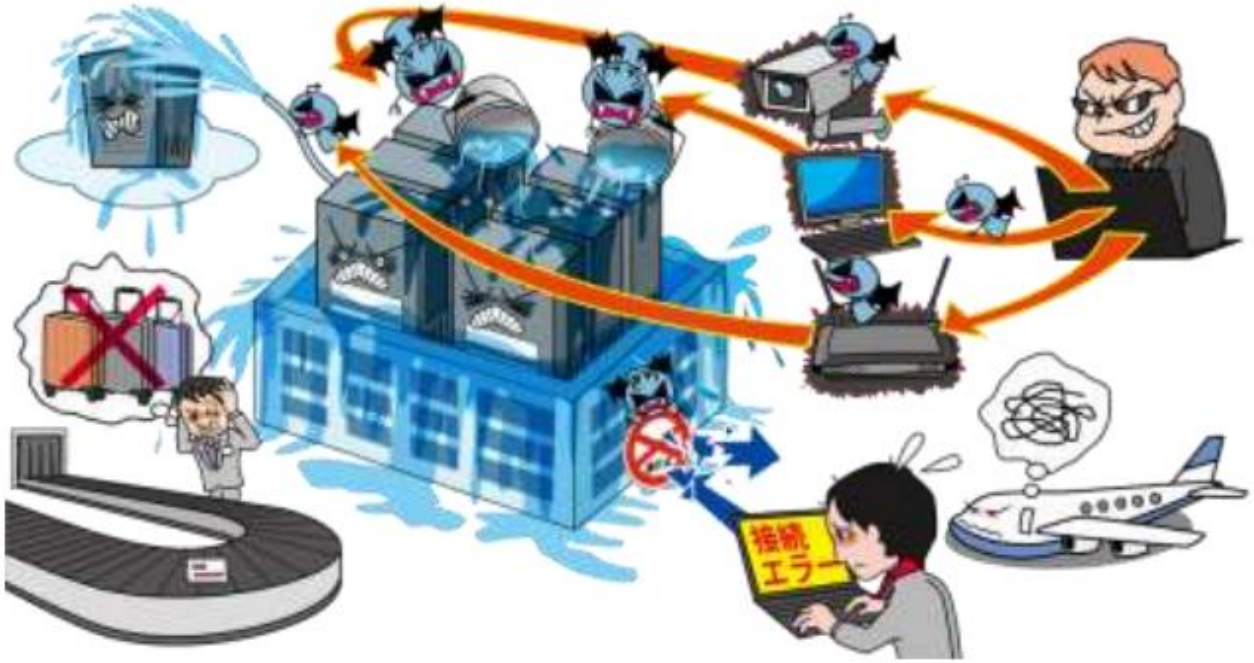
第7位　地政学的リスクに起因するサイバー攻撃

政治的に対立する周辺国に対して、社会的な混乱を引き起こすことを目的としたサイバー攻撃を行う国家が存在する。そのような国家は、外交・安全保障上の対立をきっかけとして、嫌がらせや報復のためにサイバー攻撃を行うことがある。また、自国の産業の競争優位性を確保するために周辺国の機密情報等の窃取を目的とした攻撃や、自国の政治体制維持のために外貨獲得を目的とした攻撃に手を染める国家もある。このような国家からの攻撃に備えて、組織として常にサイバー攻撃への対策を強化していく必要がある。

IPA（情報処理推進機構）「情報セキュリティ10 大脅威 2025　組織編」 P.11～P.30より一部抜粋

第8位　分散型サービス妨害攻撃（DDoS攻撃）

攻撃者に乗っ取られた複数の機器から構成されるネットワーク（ボットネット）から、企業や組織が提供しているインターネット上のサービスに対して大量のアクセスを一斉に仕掛けて高負荷状態にさせる、もしくは回線帯域を占有してサービスを利用不能にする等の分散型サービス妨害攻撃（DDoS 攻撃）が行われている。標的にされた組織・サービスは攻撃されると、Web サイト等の応答遅延や機能停止が発生し、サービス提供に支障が出るおそれがある。



IPA（情報処理推進機構）「情報セキュリティ10 大脅威 2025　組織編」 P.11～P.30より一部抜粋

第9位　ビジネスメール詐欺

悪意のある第三者が標的組織やその取引先の従業員等になりすましてメールを送信し、あらかじめ用意した偽の銀行口座に金銭を振り込ませるサイバー攻撃が行われている。この攻撃は、ビジネスメール詐欺（Business E-mail Compromise：BEC）と呼ばれ、組織の従業員を標的にした振り込め詐欺とも言われている。
そして、最近では生成 AI を利用した BEC が増加しているため、その対策が重要になってきている。

IPA（情報処理推進機構）「情報セキュリティ10 大脅威 2025　組織編」 P.11～P.30より一部抜粋

第10位　不注意による情報漏えい等

システムの仕様への認識不足、意図しない設定ミスによる非公開情報の公開、不注意による記録媒体の紛失等、個人情報等の漏えいが度々発生し、組織はその対応に追われている。ひとたび発生すると加害組織の信用、信頼に影響を与えるだけでなく、被害者への謝罪、補償等、事後対応に相応の負担がかかる。

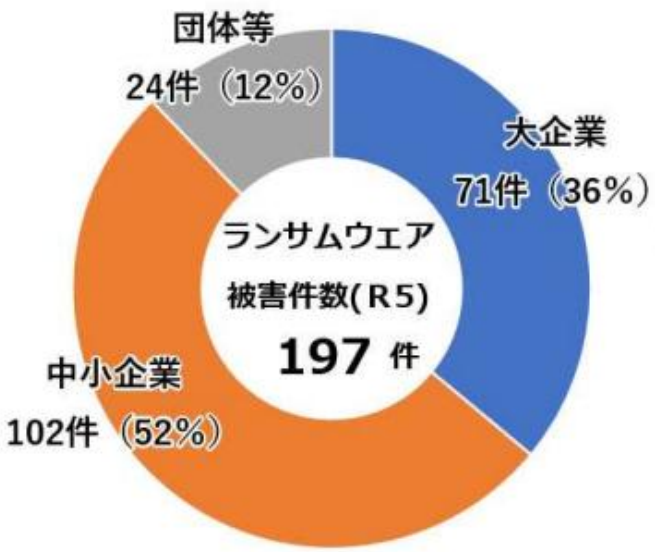
IPA（情報処理推進機構）「情報セキュリティ10 大脅威 2025　組織編」 P.11～P.30より一部抜粋

【補足】ランサムウェア

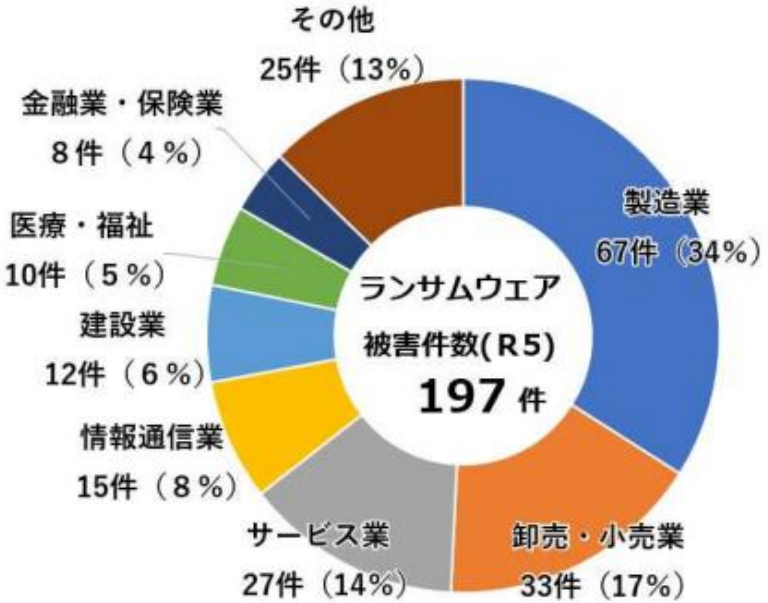
■　被害企業・団体等の規模

ランサムウェアによる被害（197件）の内訳を企業・団体等の規模別に見ると、大企業は71件、中小企業は102件であり、その規模を問わず、被害が発生した。また、業種別に見ると、製造業は67件、卸売・小売業は33件、サービス業は27件であり、その業種を問わず、被害が発生した。

【図表23：ランサムウェア被害の企業・団体等の規模別報告件数】



【図表24：ランサムウェア被害の企業・団体等の業種別報告件数】



注　図中の割合は小数第1位以下を四捨五入しているため、総計が必ずしも100にならない。

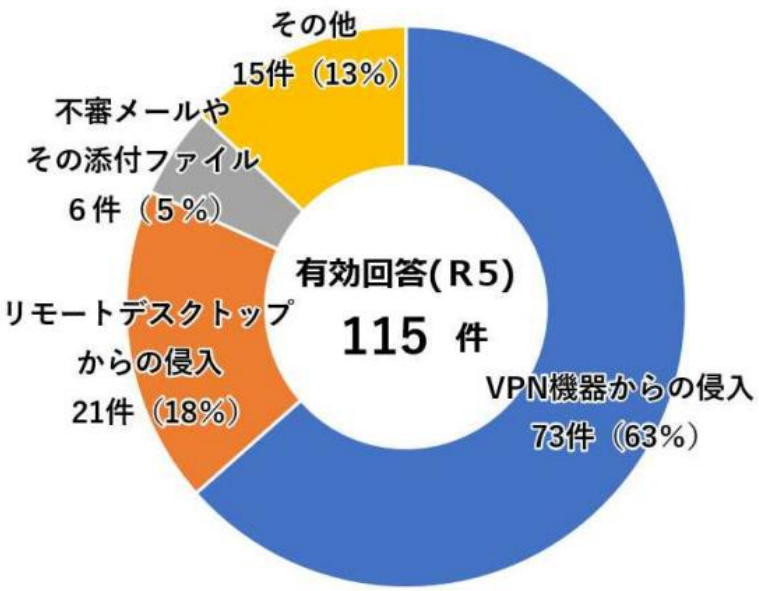
警察庁「令和5年におけるサイバー空間をめぐる脅威の情勢等について」 令和6年3月14日　P.25より抜粋

【補足】ランサムウェア

■　感染経路

ランサムウェアの感染経路について質問したところ、115件の有効な回答があり、このうち、VPN機器からの侵入が73件で63%、リモートデスクトップからの侵入が21件で18%を占め、テレワーク等に利用される機器等のぜい弱性や強度の弱い認証情報等を利用して侵入したと考えられるものが約82%と大半を占めた。

【図表25：感染経路】



注　図中の割合は小数第１位以下を四捨五入しているため、総計が必ずしも100にならない。

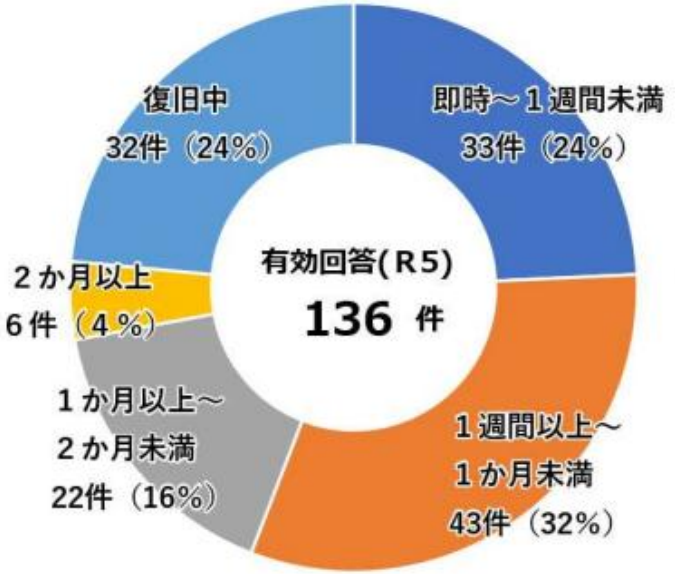
警察庁「令和5年におけるサイバー空間をめぐる脅威の情勢等について」 令和6年3月14日　P.26より抜粋

【補足】ランサムウェア

■　復旧等に要した期間・費用

復旧に要した期間について質問したところ、136件の有効な回答があり、このうち、復旧までに1か月以上を要したものが28件あった。また、ランサムウェア被害に関連して要した調査・復旧費用の総額について質問したところ、118件の有効な回答があり、このうち、1,000万円以上の費用を要したものが44件で37%を占めた。

【図表26：復旧に要した期間】



【図表27：調査・復旧費用の総額】

注　図中の割合は小数第1位以下を四捨五入しているため、総計が必ずしも100にならない。

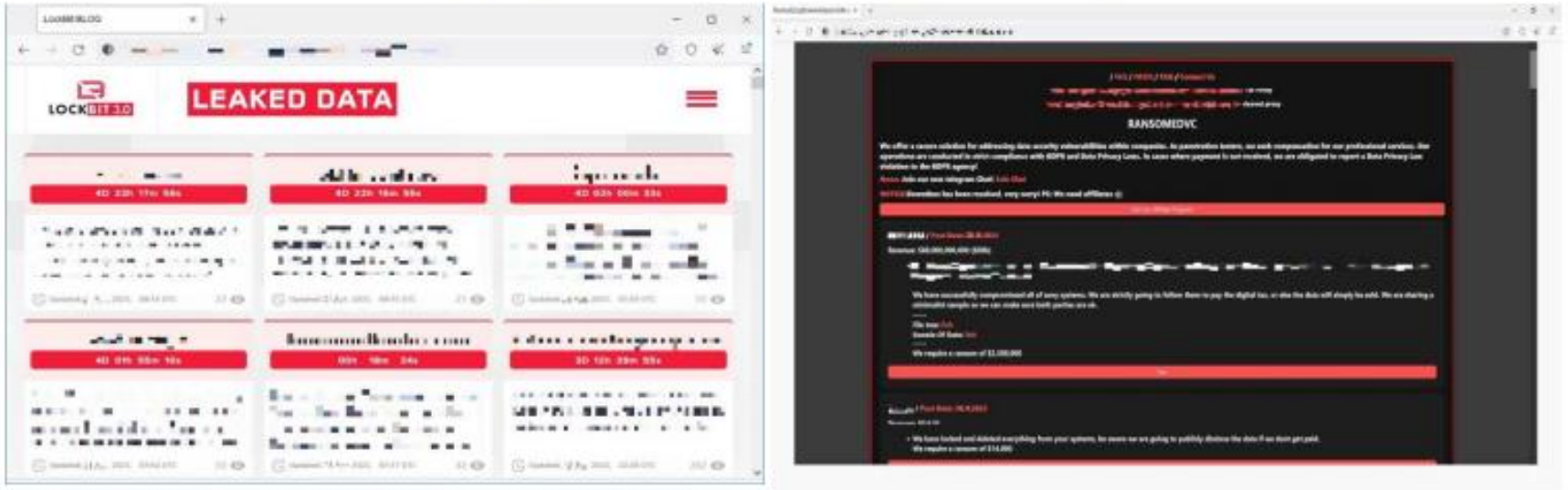
警察庁「令和5年におけるサイバー空間をめぐる脅威の情勢等について」 令和6年3月14日　P.26より抜粋

【補足】ランサムウェア

■　ランサムウェアと関連するリークサイトの状況

令和5年においても、ランサムウェアによって流出した情報等が掲載されているダークウェブ上のリークサイトに、国内の事業者等の情報が掲載されていたことを確認した。掲載された情報には、製品開発に関する情報や会計情報等が含まれていた。

【図表30：ダークウェブ上のリークサイト例】



警察庁「令和5年におけるサイバー空間をめぐる脅威の情勢等について」 令和6年3月14日　P.27より抜粋

昨今の情報セキュリティ事故　②
（訴訟に発展した開発・保守事例）

訴訟に発展した開発事例

■ セキュリティ要件、対応不備で訴訟に発展した事例

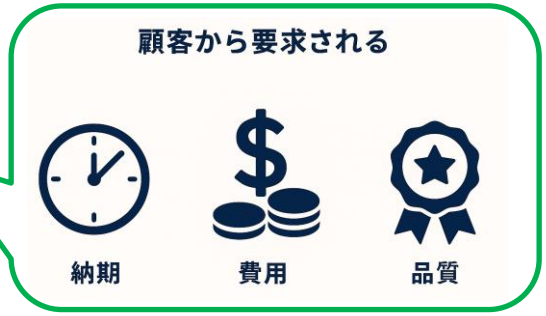
事案	
ECサイトのクレジットカード情報漏えい事件	
問題点	・セキュリティ要件（SQLインジェクション対策、暗号化など）が仕様書に明記されていなかった。 ・開発会社はオープンソース（EC-CUBE）をベースに構築したが、脆弱性対策が不十分
結果	・クレジットカード情報が漏えいし、発注企業が損害賠償請求（約1,100万円）を提起 ・裁判所は開発会社の重過失を認定し、約2,260万円の賠償命令
地方自治体のシステムで不正アクセスが発生（原因：セキュリティ設定の不備）	
問題点	・提案書には「強固なセキュリティ」と記載されていたが、実際には運用前試験も未実施
結果	・民間企業に約2億円の損害賠償請求
エステティックサロンの顧客情報が、Webサイトの制作・保守を受託した業者の過失により閲覧可能な状態	
問題点	・データ移管の際、誤った設定でデータ移管を行った。 ・2ちゃんねる上に閲覧可能なURLが公開される。
結果	・1 人当たり 3 万 5000 円（慰謝料 3 万円、弁護士費用 5000 円）

警察庁「令和5年におけるサイバー空間をめぐる脅威の情勢等について」 令和6年3月14日　P.28より抜粋

2. 現場と現況

ソフトウェア開発の現場と現況

現場：お客様から要求されること



~~セキュリティ要件~~

~~セキュリティ仕様~~

Pマーク/ISMSの
取得の有無確認

セキュリティ上の問題
が発生してしまった
場合の現況

・責任の追及
・損害賠償

プロとして整備すべきこと

セキュリティへの
考慮・対応

【補足】ランサムウェアの発生から

■　医療機関等との連携強化に向けた取り組み

医療機関におけるランサムウェアによる被害が発生していることを踏まえ、サイバー事案に係る被害の未然防止等を図る必要があることから、平時から緊密な連携を図り、事案発生時における警察への迅速な通報・相談を促進するため、令和５年４月、公益社団法人日本医師会と覚書を締結するとともに、令和５年５月、四病院団体協議会及び各国公私立大学病院に対して連携強化に関する依頼を行った。

【2024年、2023年に発生した事例】

- **QST病院（量子科学技術研究開発機構病院）　発生日**：2024年1月11日
- **岡山県精神科医療センター　発生日**：2024年5月19日
- **国分生協病院　発生日**：2024年2月27日
- **大阪府内の病院**（名称非公開）　**発生日**：2023年1月2。
- **大分県の市民病院　発生日**：2023年（詳細日不明）

これまで、閉域網で運用されていた業界にも影響を与えている。

警察庁「令和5年におけるサイバー空間をめぐる脅威の情勢等について」 令和6年3月14日　P.27より抜粋

利便性の向上：ネットワーク構成の変化による影響

■　利便性の向上

閉域網では外部連携が困難であったが、クラウド連携や遠隔診療が可能になり、業務の効率化と医療の質の向上につながりました。

ただし、リスクも増加します。

	閉域網時代	インターネット接続後の変化
外部アクセス	限定された内部アクセスのみ	外部からのアクセスが可能になり、攻撃対象が拡大
セキュリティ対策	物理的隔離が中心	ソフトウェアベースの対策が必要（IDS/IPS、ゼロトラストなど）
更新・パッチ管理	手動・限定的	自動更新が可能となる。だが、未管理だと脆弱性が残る

警察庁「令和5年におけるサイバー空間をめぐる脅威の情勢等について」 令和6年3月14日　P.28より抜粋

利便性の向上と広がるリスク

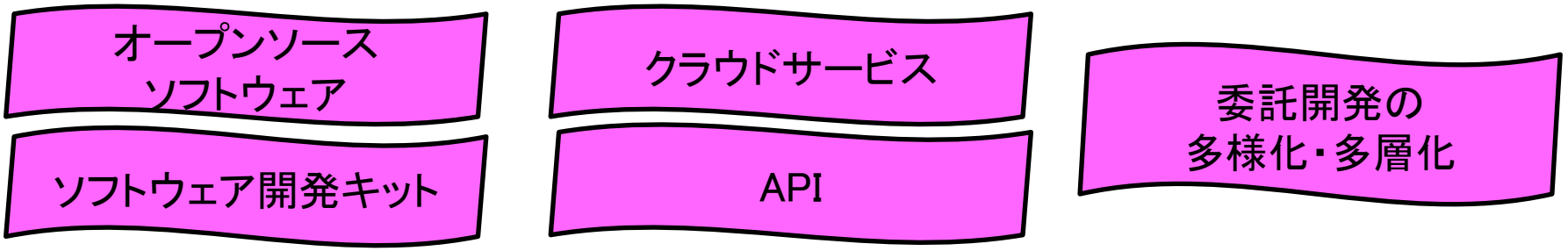
■ 利便性の向上：従来の自社内完結型からの進化

★外部のリソースの積極的な活用

オープンソースソフトウェア ソフトウェア開発キット	クラウドサービス API	委託開発の多様化
・開発期間とコストを大幅に削減 ・最新の技術、高度な機能を有したプラットフォームが利用可能 ・セキュリティと品質の向上	・自社のコア事業への集中化 ・初期投資を含めたコストの最適化 ・様々なサービスとの連携	・開発要員の育成のコスト削減 ・開発リソースの柔軟な確保 ・リスク分散

利便性の向上と広がるリスク

■ 広がるリスク：多層化と複雑化



- ・セキュリティの脆弱性
- ・ライセンス違反のリスク
- ・運用・継続性のリスク

- ・運用・継続性のリスク
- ・コンプライアンス・法的リスク
- ・ベンダーロックイン
- ・サービスの複雑化及び責任の所在の特定

- ・プロジェクト全体の管理と統制の複雑化
- ・進捗・品質の可視性の低下
- ・委託先のセキュリティ水準のばらつき
- ・責任の所在の特定

品質向上していく悪意

■　攻撃手法の標準化

現在、攻撃手順が詳細に記述されたマニュアルが存在する。（ターゲット組織の選定、業績や収益情報の分析、身代金の支払い能力の特定化など）

■　サイバー攻撃の請負（RaaS：Ransomware as a Service）

サイバー攻撃用のツールの販売・レンタル、委託開発や指南を受けることができる。（素人でも始められる。）

■　侵入しやすい箇所の高度な調査・情報収集の自動化（昔からありますが。。）

インターネット上では、常に侵入しやすい機器やシステムがないか高度な自動収集機能を有したロボットが調査しています。

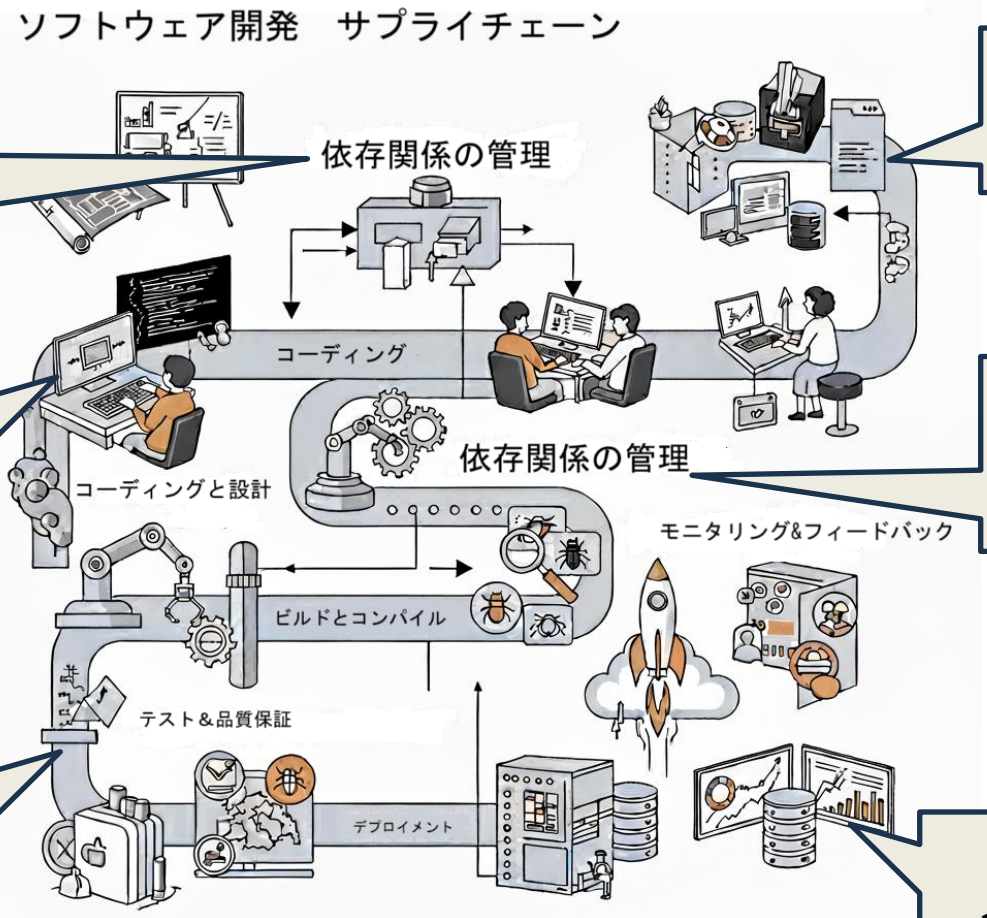
顧客が明示していない既知の要件　①

サプライチェーンを含むセキュリティが考慮された開発

ライブラリーの
バージョン管理

セキュアな開発環境
コーディングの原則
自動化ツール活用

セキュリティ検査
脆弱性診断
侵入テスト



ソフトウェア構成
の明確化

定期的な
監査とスキャン

運用対策
インシデント対策
脆弱性対策

顧客が明示していない既知の要件　②

セキュアな環境及び会社としての仕組みづくり
（ランサムウェアからの対策例）

識別・予防	目的：脅威を未然に防ぐ
	・ソフトウェアの更新（OS、アプリケーション、ネットワーク機器等） ・セキュリティソフトの導入 ・教育（不審なメールや添付ファイルの見分け方） ・最小権限の原則（アクセス権、ネットワーク等）
検知	目的：早期に異常を発見
	・振る舞い検知 ・ログの継続的な監視 ・リアルタイムアラート
対応・復旧	目的：被害を最小限に抑える
	・定期的なバックアップ ・迅速な隔離 ・復旧手順の確立

３．現況への取り組み

公開されているガイドラインを適用

公開されているガイドライン

デジタル庁　政府情報システムにおけるセキュリティ・バイ・デザインガイドライン
（URL　https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf）

防衛省　装備品等及び役務の調達における情報セキュリティ基準
（URL　https://www.mod.go.jp/atla/cybersecurity.html　防衛装備庁）

経済産業省　セキュア・ソフトウェア開発フレームワーク(SSDF)導入ガイダンス案（中間整理）
（URL　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/015_s01_00.pdf）

総務省　国民のための情報セキュリティサイト
（URL　https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/）

IPA　中小企業の情報セキュリティ対策ガイドライン
（URL　https://www.ipa.go.jp/security/guide/sme/about.html）

IPA　ランサムウェアの脅威と対策～ランサムウェアによる被害を低減するために
（URL　https://www.ipa.go.jp/security/anshin/measures/ug65p9000000njuc-att/000057314.pdf）

ガイドラインの構築・実装のメリット
（コンサル支援を含む）

・柔軟性と直接的な目的への適合性

ガイドラインは、ISMSのような厳格な認証規格と異なり、特定の目的や課題に焦点を当てた、より柔軟なアプローチを可能にします。組織は、自社のビジネスモデルやリスクに最も関連性の高い項目を選んで実装できます。

・迅速な導入

ISMSの認証取得には、多くの時間とリソース、そして専門的な知識が必要です。一方、ガイドラインの実装は、特定の目標に絞って進められるため、より迅速にセキュリティ体制を強化できます。また、認証費用が発生しないため、コストを抑えることが可能です。

・組織文化への浸透

ガイドラインは、従業員にとってより身近な課題や実践的な行動に焦点を当てていることが多く、理解と意識を浸透させやすいという利点があります。これにより、形式的なルールではなく、実質的な行動変容を促すことができます。

ISMS（ISO/IEC 27001）の実装
～認証取得はせずに～

ISMSとは

ISMS＝Information Security Management System

情報セキュリティのトータル的なリスクマネジメントシステムのこと。

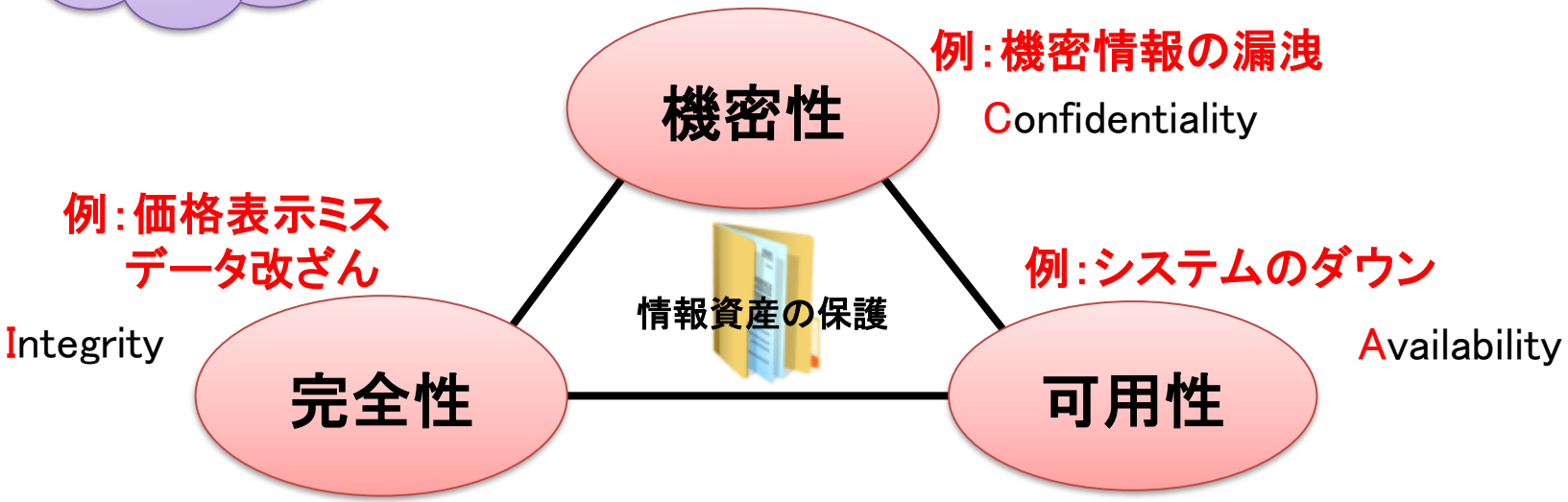
- ISO/IEC 27001の規格に基づき、情報セキュリティマネジメントシステムを構築し、組織の情報を適切に管理し、機密を守るための包括的な枠組み。
- コンピュータシステムのセキュリティ対策（技術的対策）だけではなく、情報を取り扱う際の基本的な方針、それに基づく具体的な計画の策定、計画の実施・運用、点検、見直しを行う。（PDCA）

情報セキュリティとは

情報セキュリティ＝情報の機密性、完全性、可用性を維持すること

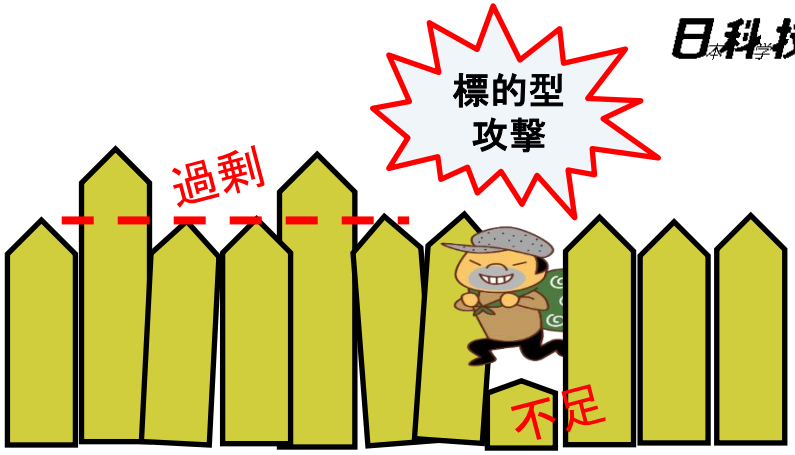
※JIS Q 27001より

情報のCIAを
維持すること



参考)「安全基準」

セキュリティ対策の安全性を
建物の塀に置き換えて…



- 高さ2mの塀であっても、1ヵ所10cmのところがあったら、そこから簡単に侵入されてしまう。
  - 情報セキュリティ対策も弱いところがあると攻撃されてしまうので、網羅的に対策を講じる。
- 高さが1.5mで安全性が保たれるのであれば、あるところは3m、あるところは5mにしても意味がなく、無駄な投資になるだけである。
  - 情報セキュリティ対策も必要な基準を決め、その基準に沿って対策を構築する。(コスト見直し)

ISMSで実現

ISMSの構成

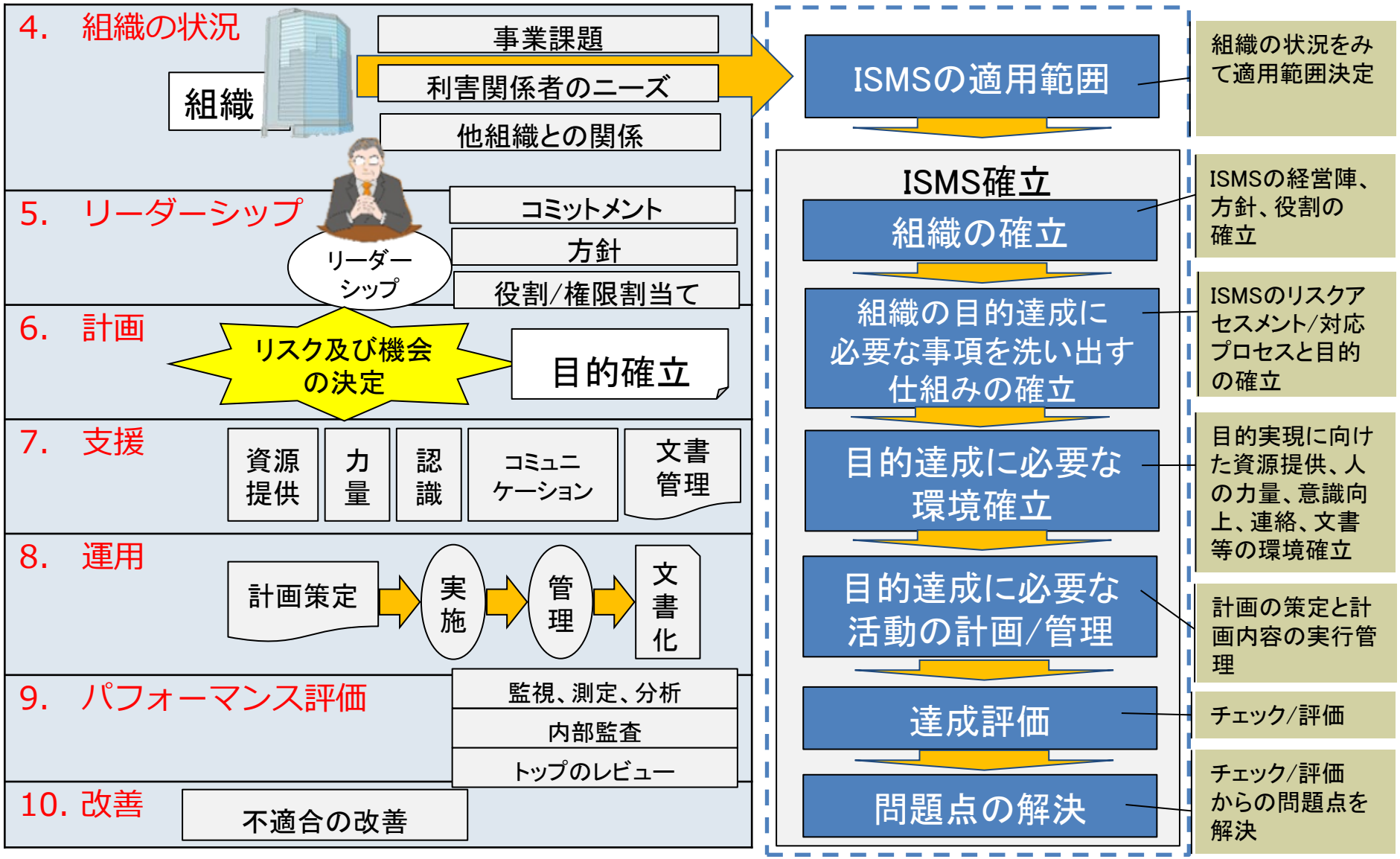
ISMSの認証を取得するための必要事項（要求事項）の構成は、次の通り。

要求事項

0. 序文
1. 適用範囲
2. 引用規格
3. 用語及び定義
4. 組織の状況
5. リーダーシップ
6. 計画
7. 支援
8. 運用
9. パフォーマンス評価
10. 改善

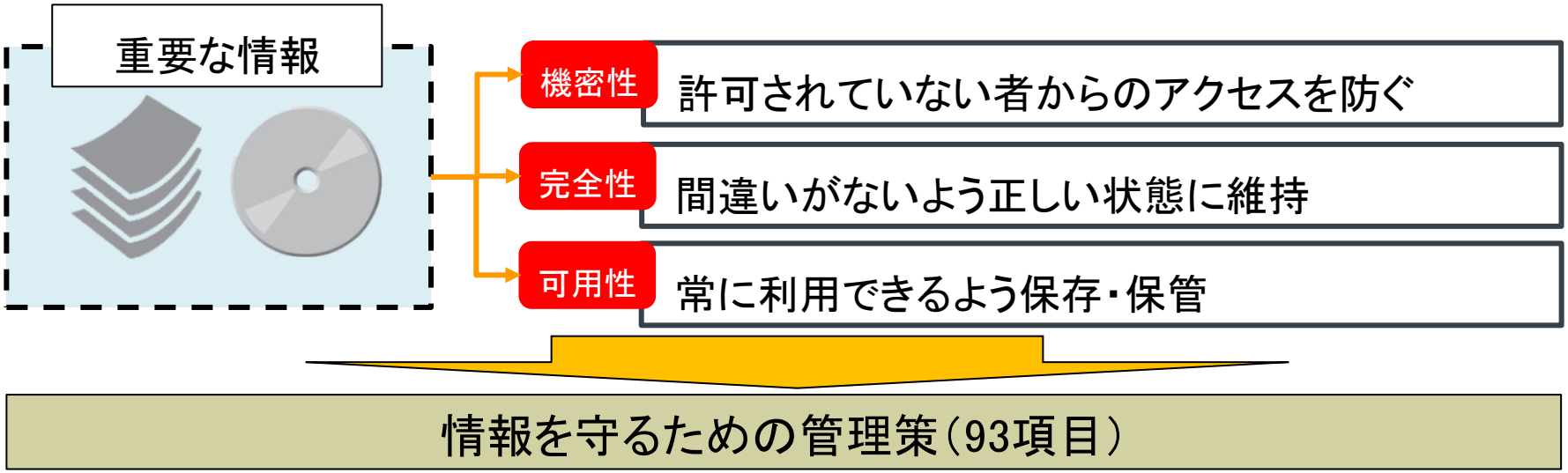
組織の中で、
規格要求事項の箇条4～10で要求されている内容を実現（ルール化、文書化、運用等）する。

ISMSのイメージ



附属書A：情報セキュリティ管理策

機密性、完全性、可用性の点で情報を守るための対策（管理策）が用意されています。



附属書A　情報セキュリティ管理策
5　組織的管理策：組織でみた適用すべき対策がまとめられている。
6　人的管理策　：人の管理において適用すべき対策がまとめられている。
7　物理的管理策：物理・環境面において適用すべき管理策がまとめられている。
8　技術的管理策：技術面において適用すべき管理策がまとめられている。

例：開発関連の管理策

サプライチェーンを含むセキュリティが考慮された開発

8.25 セキュリティに配慮した開発のライフライクル

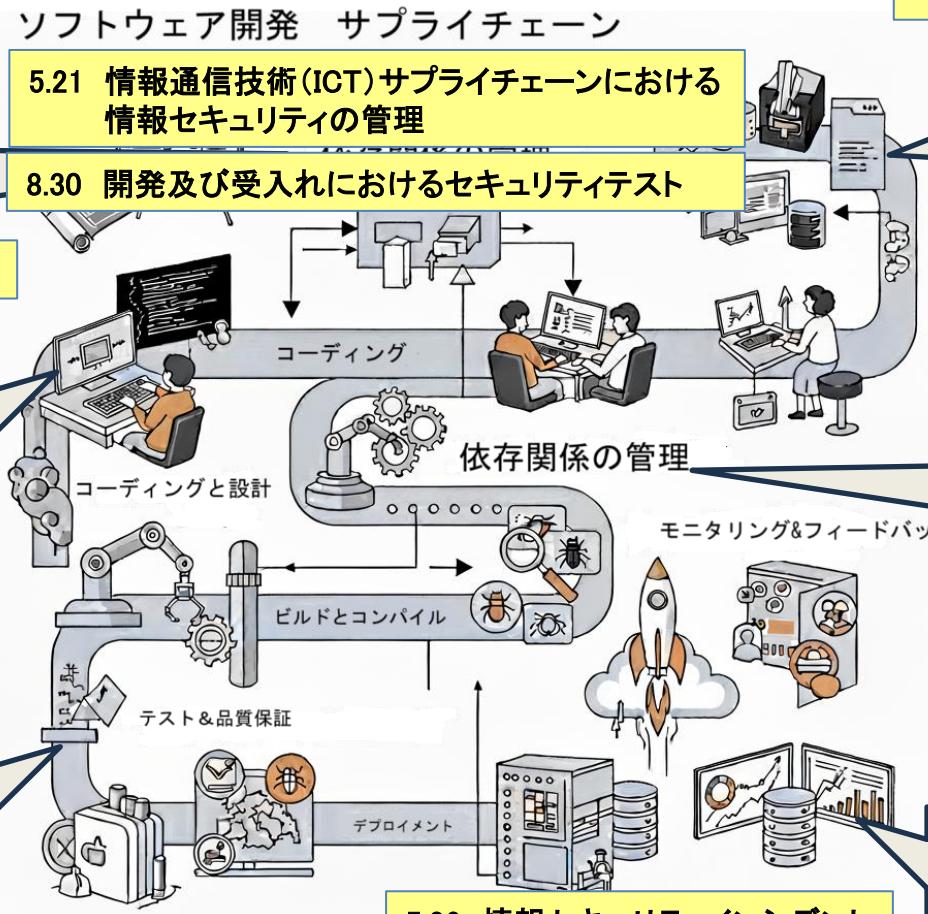
8.31 開発環境、テスト環境及び本番環境の分離

ライブラリーのバージョン管理

8.4 ソースコードへのアクセス

ソフトウェア構成の明確化

8.9 構成管理



セキュアな開発環境
コーディングの原則
自動化ツール活用

8.28 セキュリティに配慮したコーディング

定期的な監査とスキャン

8.34 監査におけるテスト中の情報システムの保護

セキュリティ検査
脆弱性診断
侵入テスト

8.8 技術的ぜい弱性の管理

8.29 開発及び受入れにおけるセキュリティテスト

5.26 情報セキュリティインシデントへの対応

6.8 情報セキュリティ事象の報告

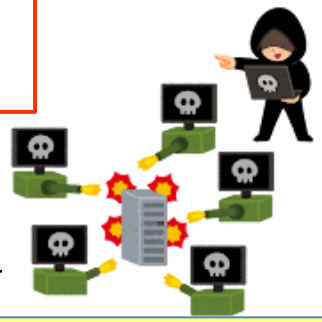
8.32 変更管理

運用対策
インシデント対策
脆弱性対策

8.8 技術的ぜい弱性の管理

例：セキュリティ環境のための管理策

セキュアな環境及び会社としての仕組みづくり
（ランサムウェアからの対策例）



識別・予防	目的：脅威を未然に防ぐ	
	・ソフトウェアの更新（OS、アプリケーション、ネットワーク機器） ・セキュリティソフトの導入 ・教育（不審なメールや添付ファイルの見分け方） ・最小権限の原則（アクセス権、ネットワーク等）	8.7 マルウェアに対する保護 8.8 技術的ぜい弱性の管理 8.12 データ漏洩防止 8.21 ネットワークサービスのセキュリティ
検知	目的：早期に異常を発見	8.15 ログ取得
	・振る舞い検知 ・ログの継続的な監視 ・リアルタイムアラート	8.16 監視活動 6.3 情報セキュリティの意識向上、教育及び教育 8.2 特権的アクセス権 8.3 情報へのアクセス権限
対応・復旧	目的：被害を最小限に抑える	
	・定期的なバックアップ ・迅速な隔離 ・復旧手順の確立	8.13 情報のバックアップ 5.26 情報セキュリティインシデントへの対応 6.8 情報セキュリティ事象の報告 5.30 事業継続のためのICTの備え 8.5 セキュリティを保った認証 8.20 ネットワークセキュリティ 8.22 ネットワークの分離 8.23 ウェブフィルタリング

ISMS（ISO/IEC 27001）の構築・実装のメリット

・世界標準の導入

ISO/IEC27001は、2005年の発行以来、社会環境の変化や技術の進化に合わせ、世界の専門家によって改訂・ブラッシュアップされてきた国際的な基準です。

・組織としての仕組みの構築

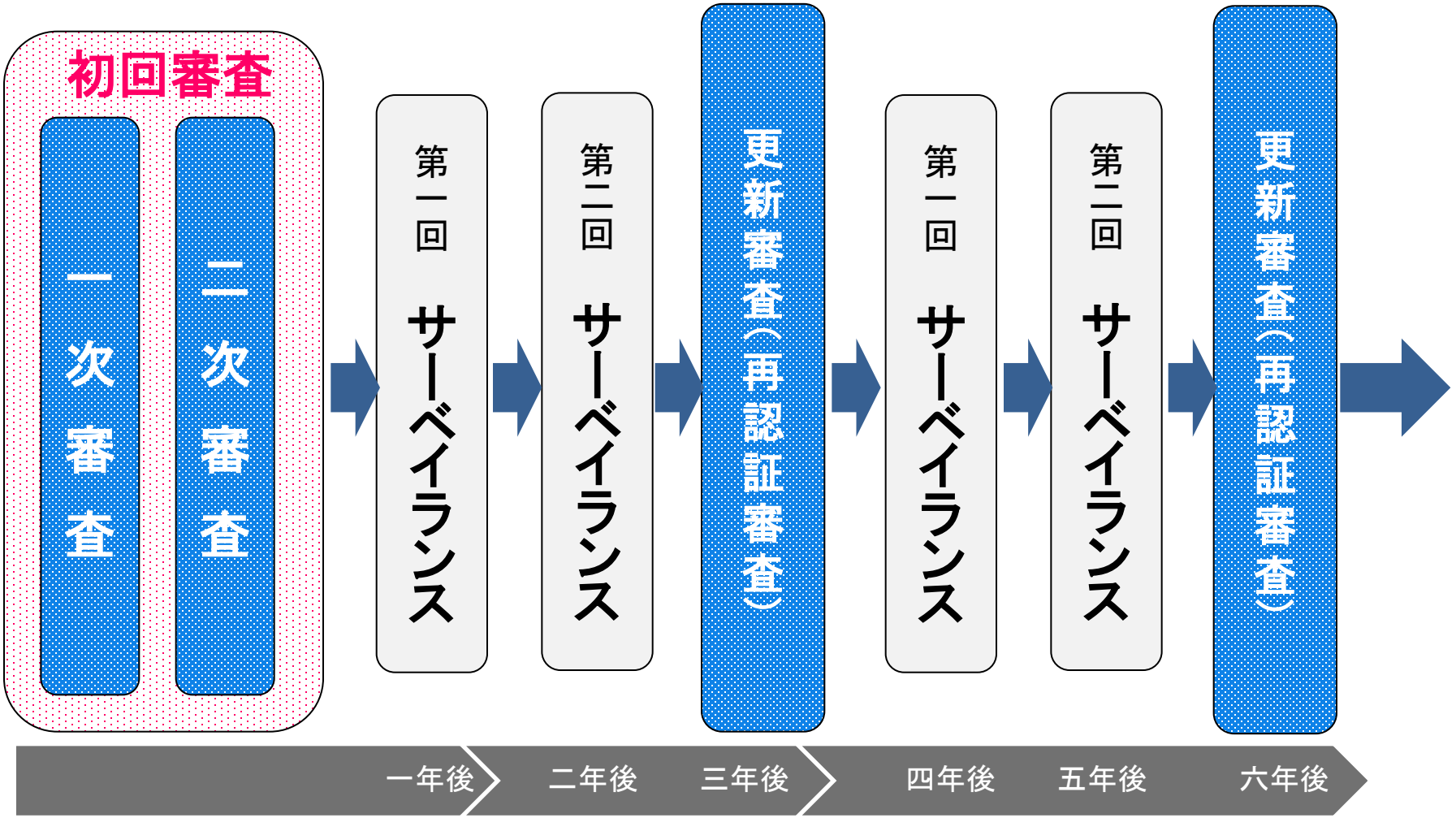
組織が情報セキュリティを維持するための仕組みを構築することを目的としています。リスク管理を含めたPDCAサイクル（Plan-Do-Check-Act）を適用し、組織の仕組みとして取り組むことができます。

・網羅的なセキュリティ対策

大企業から中小企業、業種を問わずあらゆる組織に適用できるよう設計された規格であり、組織として対応すべき網羅的な対策基準が用意されています。各項目をクリアしていくことで、漏れなく、かつ体系的に管理体制を確立することが可能です。

ISMS（ISO/IEC 27001）の
認証取得・維持

認証の維持



※ 認証の有効期間は3年間です。
※ サーベイランスは一年に一回、または半年に一回のどちらかを選択できます。
※ 初回審査後は、サーベイランス①→サーベイランス②→更新審査 の繰返しになります。

認証取得のメリット

・顧客や取引先へのアピール/ビジネス機会の拡大

組織が国際的な基準に準拠した情報セキュリティ管理を実践していることを、客観的に証明できます。これは、特にセキュリティを重視する顧客や取引先との関係構築において、大きな信頼獲得、入札案件への参加条条件を満たすことにつながります。

・組織文化と従業員の意識向上

情報セキュリティの維持には、従業員への継続的な教育と啓発が不可欠です。全従業員が情報セキュリティの重要性を理解し、日常業務におけるリスクを自律的に意識するようになるためには、組織が強い意志を持ち続ける必要があります。認証を取得・維持すると、定期的に外部の審査員が審査に入るため、組織及び従業員の順守への意識が継続されます。

・変化への対応

定期的な審査を通じて、客観的な視点から運用状況の評価し、改善が必要な点を検出することができます。特に、組織や外部環境の変化に伴う適合性や妥当性に関するコメント、他社事例、昨今の傾向等の情報を得ることが可能です。

各取り組みのメリットと注意点

	ガイドラインの構築	ISO/IEC27001の構築	認証取得・維持
メリット	・柔軟性と直接的な目的への適合性 ・迅速な導入 ・組織文化への浸透	・世界標準の導入 ・組織としての仕組みの構築 ・網羅的なセキュリティ対策	・顧客や取引先へのアピール/ビジネス機会の拡大 ・組織文化と従業員の意識向上 ・変化への対応
		一年後 → 二年後、三年後 → 四年後、五年後…	
注意点	・構築後の維持のための組織づくり、意識づくりをする。 -属人（部門）化してしまう。 -作業化してしまう。 -実態と合わなくなってしまう。	・規格表現と意図を理解する。 ・意識をもったcheckとactを実施する。 ・組織変化/環境変化への意識をもった対応をする。 ・具体的な対策の記載がない。	・規格表現と意図を理解する。 ・審査のための準備・負荷がかかる。 ・別視点での改善事項を得られるという意識で審査を受ける。

4. 日科技連 ISO審査登録センターが提供する認証サービス

JUSE-ISO CENTERとは

日本科学技術連盟　ISO審査登録センター
（以下、JUSE-ISO CENTER／略称：にっかぎれん ）は、1995年に審査機関としての活動をスタートしました。
2013年からは、認証審査を行なうだけでなく、登録組織様の**マネジメントシステム活用をサポートする**ことを目指し、無料セミナー・講演会サービスを拡充しています。

日本科学技術連盟（Union of Japanese Scientists and Engineers ）とは

1946（昭和21）年に創立。科学技術の進歩・発展をはかることを目的として、戦後日本のものづくりを支えてきました。「品質管理（QC）」や経営管理技術の普及拡大を中心に据え、調査・研究・開発、大会・シンポジウム、教育訓練・国際交流、QCサークル活動の全国的普及、技術相談および広報・出版など、企業の品質力向上に役立つ事業を幅広く展開。国内はもとより世界各国から高い評価を受けています。

JUSE-ISO CENTERのサービスの3つの柱

1. マネジメントシステム認証サービス

JUSE-ISO CENTERは、1995年にISO 9000シリーズ・品質システムの審査機関としてスタート。現在は多様な規格の審査に対応し、**認証登録件数は、2000社を超えます**。

2. 教育・講演サービス

2013年から、“単なる認証機関からの脱却”を目指し、登録組織限定の **「J-Club」サービス**を拡充。セミナー・講演会の提供を開始。 現在では、オンライン、会場参加型、アーカイブ等、多様な実施形式で

年間60種類130回以上開催

無料で利用でき、**社内教育にも活用いただいており、費用削減**にもつながるとのお声をいただいております。

3. 情報発信サービス

日科技連で開催している大会、シンポジウム、フォーラム等での発表**事例検索サービス「J-ナレッジ」**の提供や、**「J-Club NEWS」(年4回発行)**をはじめとした定期的な情報発信を行なっています。

JUSE-ISO CENTER　サービスその1

マネジメントシステム認証サービス

認証サービス(審査)の特長

1. QUALITYの高い審査員

組織の立場を理解できる豊富な知識・経験をもち、その業界・業界に精通した専門性の高い審査員が多数在籍しています。また、**定期的に審査員の教育**を実施し、**力量の維持・向上**を図っています。

2. 審査リーダーの固定による継続的な改善

初回審査～更新審査、更新審査～更新審査の**3年間(1サイクル)、審査リーダーを原則固定。**継続的にお客様と向き合うことで、製品やサービスを深く理解した質の高い審査を実現します。

3. 審査前の事前打合せ会の実施

審査の前に、受審側と審査リーダーとの事前打合せを実施。**業務内容や審査の目的を深く理解**した上で、課題や長所を顕在化し、審査へと進むことができます。

JUSE-ISO CENTER　サービスその2

教育・講演サービス

教育・講演サービス「J-Clubセミナー」

知識向上、人材育成、教育計画をサポート

★ガイドのダウンロード
J-Clubセミナーガイド

【J-Clubオンラインセミナー】（Zoom生中継）

①J-Clubマネジメント
→52コース／**要求事項の概要解説、内部監査員養成等のベースの教育からMS運用のレベルアップまで。**

②J-Clubアカデミア
→7コース／**経営戦略、経営とMSの融合、SDGs関連。**

③J-Club講演会
→最新トピックの紹介。適時開催。

④新入社員研修
→**社会人としての基本ビジネスマナーの習得。**

⑤J-Hiroba
→10コース／**コミュニケーションスキルの向上**

⑥J-Club：キッズプログラム
→登録組織様にご在籍の方のお子様（小学生）が対象。
夏休みの自由研究に（成果物あり）！

【J-Clubアーカイブ】【J-selectアーカイブ】

①J-Clubマネジメント
→30コース／いつでも・どこでも視聴可能！複数同時アクセス可

②J-select
→16コース／いつでも・どこでも視聴可能！複数同時アクセス可
品質管理・TQMのベース教育に最適！

「J-Clubセミナー」ラインナップ

2025 年度 セミナー開催一覧

アーカイブが1年間視聴可能！

セミナー名		カテゴリー	講師名	通算時間（※社会時間含まず）	2025年 4月	5月	6月
J-Club セミナー							
J-Club マネジメント							
M-1	ISO 9001（QMS）概要解説コース	ISO 9001関連	越山	5時間		14日（水）オンライン	
M-2	はじめてのISO 9001	ISO 9001関連	越山	1時間30分			
M-3	規格の意図と箇条間の関係性を理解する	ISO 9001関連	福丸	5時間			
M-4	内部監査報告書の書き方と調べ方［ISO 9001］	ISO 9001関連	国府	5時間			
M-5	「設計・開発」の捉え方と柔軟な運用	ISO 9001関連	越山	3時間			
M-6	実務者向けQMS短編集（その1）－製造－ NEW	ISO 9001関連	越山	1時間			
M-7	実務者向けQMS短編集（その2）－サービス－ NEW	ISO 9001関連	越山	1時間			
M-8	ISO 14001（EMS）概要解説コース	ISO 14001関連	高橋	5時間		21日（水）オンライン	
M-9	環境法規制管理のポイント	ISO 14001関連	高橋	5時間			
M-10	はじめてのISO 14001	ISO 14001関連	高橋	1時間30分			
M-11	自動車CSMS ISO/SAE 21434対応	自動車関連	村上	5時間			
M-12	ISO 22000・FSSC 22000概要解説コース	食品安全関連	島袋	5時間			
M-13	食品安全マネジメントシステム内部監査実践コース	食品安全関連	島袋	5時間			
M-14	どうされていますか？食品の微生物検査（初級編）～適切な検査計画のために～	食品安全関連	鈴木	3時間			
M-15	振り返ってみましょう！食品の微生物検査（中級編）～検査結果の正しい理解のために～	食品安全関連	鈴木	3時間			
M-16	食品工場の新人教育	食品安全関連	谷口	3時間			
M-17	初めて表示に携わる方の表示の見方・作り方	食品安全関連	見冨	3時間			
M-18	食品安全規格等の基礎知識：60分シリーズ　キホンの「キ」	食品安全関連	谷口 玉置	各1時間			
M-19	実務に取り込むISO 22000：2018	食品安全関連	渡辺	3時間			
M-20	HACCPの基礎知識	食品安全関連	玉置	3時間			
M-21	コンプライアンス担当が見た食品売り場（食品表示、栄養表示、優良誤認など）	食品安全関連	谷口	3時間			
M-22	必修！基礎から学ぶ食品衛生① 食品衛生責任者を超える力量が得られます！ ～公衆衛生から関連法規の理解まで～	食品安全関連	渡辺	3時間			
M-23	必修！基礎から学ぶ食品衛生② 食品衛生責任者を超える力量が得られます！ ～公衆衛生から関連法規の理解まで～	食品安全関連	渡辺	3時間			
M-24	ISO/IEC27001（ISMS）概要解説コース	情報セキュリティ関連	木村	5時間		15日（木）オンライン	
M-25	ISMSクラウドセキュリティ（ISMS-CS）概要解説コース	情報セキュリティ関連	吉田	3時間			
M-26	JIS Q 27001：2023に基づく　ISMS内部監査員研修	情報セキュリティ関連	村上	5時間			
M-27	QMS/EMS認証組織のための情報セキュリティ入門	情報セキュリティ関連	村上	3時間			
M-28	ISO/IEC27001：2022規格改正移行説明会	情報セキュリティ関連	吉岡	3時間			

11

2025 年度 セミナー開催一覧

セミナー名		カテゴリー	講師名	通算時間（※社会時間含まず）	2025年 4月	5月	6月
J-Club マネジメント							
M-29	ISO/IEC27002：2022情報セキュリティ管理策の解説	情報セキュリティ関連	村上	5時間			
M-30	プライバシー情報マネジメントシステム（ISMS－PIMS）について	情報セキュリティ関連	吉岡	3時間			
M-31	ISO 45001（OHSMS）概要解説コース	労働安全衛生	高橋	5時間			
M-32	わかりやすいプロセスアプローチ基礎解説コース	MS共通	横沢	5時間		23日（金）オンライン	
M-33	プロセス・マップの作成基礎コース	MS共通	横沢	5時間			12日（木）オンライン
M-34	内部監査員養成コース（MS共通）	MS共通	横沢	4時間	21日(月)~23日(水) 受講証明書付アーカイブ		
M-35	実のあるマネジメントシステム活動とするために	MS共通	国府	5時間			
M-36	「リスク及び機会」の正しい捉え方と「技術の伝承」の考え方	MS共通	国府	5時間			
M-37	形式的になりがちなマネジメントシステムの"3つのくせ者"実効性からの再考～力量、文書化、目標～	MS共通	国府	5時間			
M-38	1時間で分かる「業務内容とISO要求事項」購買・外注部門の主な機能とISO要求事項 NEW	MS共通	国府	1時間			
M-39	1時間で分かる「業務内容とISO要求事項」設計・開発部門の主な機能とISO要求事項 NEW	MS共通	国府	1時間			
M-40	1時間で分かる「業務内容とISO要求事項」営業・企画部門の主な機能とISO要求事項 NEW	MS共通	国府	1時間			
M-41	マネジメントシステムのスリム化セミナー	MS共通	国府	5時間			
M-42	経営管理とMS規格（箇条4：組織の状況）の本質	MS共通	福丸	3時間			
M-43	TQM視点でマネジメントシステム強化と内部監査コース	品質管理	丸山	3時間		30日（金）オンライン	
M-44	品質工学　パラメータ設計 ～効率の良い設計を実現するための手法～	品質管理	越山	3時間	アーカイブ		
M-45	新QC七つ道具概要解説コース	品質管理	高木	3時間			5日（木）オンライン
M-46	品質工学（タグチメソッド）概要解説コース	品質管理	越山	3時間			
M-47	新入社員2日間研修	人材育成	㈱インソース	1日目：6時間 2日目：7時間	10日（木）~11日（金）オンライン		
M-48	チームメンバーからチームリーダーへ （3～5年目社員研修）	人材育成	福島	5時間30分			
M-49	1on1ミーティングの進め方	人材育成	福島	3時間			19日（木）オンライン
M-50	日本型ワーク・エンゲージメントを考える	人材育成	福島	3時間			
M-51	今日作って、明日から使う カンタンすぎる人事評価制度セミナー	人材育成	山本	3時間			
M-52	サステナブルな人的マネジメント ～人手不足に対抗するISO 30414～	人材育成	三浦	3時間			
M-53	ハラスメント防止（全体向け） NEW	人材育成	福島	3時間		24日（木）オンライン	
M-54	ハラスメント防止（管理職向け） NEW	人材育成	福島	5時間			3日（火）オンライン
M-55	失敗学入門編	組織内リスク管理	岩松	2時間30分	15日(火)~17日(木) 日にち限定アーカイブ		
M-56	リスクマネジメントの基本	組織内リスク管理	村上	4時間			

13

「J-Clubセミナー」ラインナップ

2025 年度 セミナー開催一覧

セミナー名		カテゴリー	講師名	講義時間（休憩時間含まず）※講義時間は目安です。	2025年 4月	5月	6月
J-Club マネジメント							
M-57	BCPの基本	総合的リスク管理	村上	3時間30分			
M-58	効果的な是正処置方法とヒューマンエラー対策コース	総合的リスク管理	丸山	3時間			
M-59	有効な是正処置　具体事例をもとに考える	総合的リスク管理	横沢	5時間			
M-60	IEの基本 NEW	総合的リスク管理	木内	3時間			
M-61	VE研修（1日コース） NEW	総合的リスク管理	丹澤	5時間			
J-Club アカデミア							
A-1	戦略的リスクマネジメント概論	総合的リスク管理	神田	5時間			
A-2	戦略型リーダーになるための経営戦略論	リーダーシップ	神田	5時間			
A-3	マネジメントシステム運用に有効なKPIの設定とその管理	リーダーシップ	近藤	5時間			27日（金）オンライン
A-4	持続可能な調達に必要なマネジメント（入門編）	サステナビリティ	近藤	5時間			13日（金）オンライン
A-5	SDGs入門編：SDGsの概要を学ぶ	サステナビリティ	近藤	5時間	18日（金）オンライン		
A-6	持続可能なマネジメントシステムとバリューチェーン統合による気候変動対応	サステナビリティ	近藤	5時間			
J-Club講演会／キッズプログラム							
	J-Club講演会	J-Club講演会	未定	未定			
K-1	Kidsプログラム	キッズ対応	坂田	1時間30分			
J-Hiroba							
H-1	「聞き出す力（インタビュースキル）」養成基礎講座 ～内部監査の面談を想定した実践ロールプレイ～	コミュニケーション	浅川	5時間		28日（水）オンライン	
H-2	「伝達する力（プレゼンスキル）」養成基礎講座 ～プレゼンの3つの視点と自己紹介を題材にした実践演習～	コミュニケーション	浅川	5時間			25日（水）オンライン
H-3	「傾聴する力（アクティブリスニングスキル）」養成基礎講座 ～傾聴による関係の構築と基本技法の理解～	コミュニケーション	浅川	5時間			
H-4	「自己表現する力（アサーションスキル）」養成基礎講座 ～アサーティブなコミュニケーションの理解と実践～	コミュニケーション	浅川	5時間			
H-5	「論理的なコミュニケーション」養成基礎講座 ～ロジカルに話す力の基礎を学びフレームワークで強化する～	コミュニケーション	浅川	5時間			
H-6	「セカンドキャリアデザイン」養成基礎講座 ～人生100年時代における後半戦のキャリアデザイン～	コミュニケーション	浅川	5時間			
H-7	「セルフマネジメント」養成基礎講座 ～確実な成果を上げるために必要なこと～	コミュニケーション	浅川	5時間			
H-8	「アンガーマネジメント」養成基礎講座 ～心理学や心理療法等から学ぶ怒りのコントロール法～	コミュニケーション	浅川	5時間			
H-9	「フォローする力（フォロワーシップ）」養成基礎講座 ～フォロワーシップスタイル診断＆実践エクササイズ～	コミュニケーション	浅川	5時間			
H-10	「リードする力（リーダーシップ）」養成基礎講座 ～ヨコの関係強化と権限なき新たなリーダーシップ～	コミュニケーション	浅川	5時間			

15

2025年度 J-Clubアーカイブ一覧

視聴期間：2025年4月～2026年3月（1年間）

下記の複数のアーカイブセミナーを何種類でも、何回でも無料で視聴することができます。
※複数同時視聴可
※J-Clubアーカイブセミナーは、申込不要です。
※連絡担当者様宛に送付済のアーカイブ視聴用ID/PWでログインしてください。
※録画した内容をご視聴いただくため、若干映像の乱れ・音声の不具合がございますが、ご了承ください。

申込み不要 / 事前送付視聴用・ID・PW でご覧ください。

セミナー名		視聴時間（休憩時間含まず）※講義時間は目安です。	掲載頁
J-Club（アーカイブセミナー）			
M-1	ISO 9001（QMS）概要解説コース	5時間	22
M-2	はじめてのISO 9001	1時間30分	23
M-3	規格の意図と箇条間の関係性を理解する	5時間	23
M-4	内部監査報告書の書き方と調べ方［ISO 9001］	5時間	23
M-5	「設計・開発」の捉え方と柔軟な運用	3時間	24
M-6	実務者向けQMS短編集（その1）－製造－ NEW	1時間	24
M-7	実務者向けQMS短編集（その2）－サービス－ NEW	1時間	24
M-8	ISO 14001（EMS）概要解説コース	5時間	25
M-9	環境法規制管理のポイント	5時間	25
M-10	はじめてのISO 14001	1時間30分	26
M-11	自動車CSMS ISO/SAE 21434対応	5時間	26
M-12	ISO 22000・FSSC 22000概要解説コース	5時間	26
M-14	どうされていますか?食品の微生物検査（初級編）～適切な検査計画のために～	3時間	27
M-15	振り返ってみましょう！食品の微生物検査（中級編）～検査結果の正しい理解のために～	3時間	28
M-16	食品工場の新人教育	3時間	28
M-17	初めて表示に携わる方の表示の見方・作り方	3時間	28
M-18	食品安全規格等の基礎知識：60分シリーズ キホンの「キ」	各1時間	29
M-19	実務に取り込むISO 22000：2018	3時間	29
M-20	HACCPの基礎知識	3時間	29
M-21	コンプライアンス担当が見た食品売り場（食品表示、栄養表示、優良誤認など）	3時間	30
M-22	必修！基礎から学ぶ食品衛生① 食品衛生責任者を超える力量が得られます！～公衆衛生から関連法規の理解まで～	3時間	30
M-23	必修！基礎から学ぶ食品衛生② 食品衛生責任者を超える力量が得られます！～公衆衛生から関連法規の理解まで～	3時間	30
M-24	ISO/IEC27001（ISMS）概要解説コース	5時間	31
M-25	ISMSクラウドセキュリティ（ISMS-CS）概要解説コース	3時間	31

セミナー名		視聴時間（休憩時間含まず）※講義時間は目安です。	掲載頁
J-Club（アーカイブセミナー）			
M-26	JIS Q 27001：2023に基づくISMS内部監査員研修	5時間	32
M-27	QMS/EMS認証組織のための情報セキュリティ入門	3時間	33
M-28	ISO/IEC27001：2022規格改正移行説明会	3時間	33
M-29	ISO/IEC27002：2022 情報セキュリティ管理策の解説	5時間	33
M-30	プライバシー情報マネジメントシステム（ISMS－PIMS）について	3時間	34
M-31	ISO 45001（OHSMS）概要解説コース	5時間	34
M-32	わかりやすいプロセスアプローチ基礎解説コース	5時間	35
M-33	プロセス・マップの作成基礎コース	5時間	35
M-34	内部監査員養成コース（MS共通）	4時間	36
M-35	実のあるマネジメントシステム活動とするために	5時間	37
M-36	「リスク及び機会」の正しい捉え方と「技術の伝承」の考え方	5時間	37
M-37	形式的になりがちなマネジメントシステムの"3つのくせ者" 実効性からの再考～力量、文書化、目標～	5時間	38
M-38	1時間で分かる「業務内容とISO要求事項」購買・外注部門の主な機能とISO要求事項 NEW	1時間	38
M-39	1時間で分かる「業務内容とISO要求事項」設計・開発部門の主な機能とISO要求事項 NEW	1時間	38
M-40	1時間で分かる「業務内容とISO要求事項」営業・企画部門の主な機能とISO要求事項 NEW	1時間	39
M-41	マネジメントシステムのスリム化セミナー	5時間	39
M-42	経営管理とMS規格（箇条4：組織の状況）の本質	3時間	39
M-44	品質工学　パラメータ設計 ～効率の良い設計を実現するための手法～	3時間	40
M-46	品質工学（タグチメソッド）概要解説コース	3時間	41
M-52	サステナブルな人的マネジメント ～人手不足に対抗するISO 30414～	3時間	44
M-56	リスクマネジメントの基本	4時間	45
M-57	BCPの基本	3時間30分	46
M-59	有効な是正処置　具体事例をもとに考える	5時間	47

17

JUSE-ISO CENTER　サービスその3

情報発信サービス

情報発信サービス「J-ナレッジ」「J-Club NEWS」

【J-ナレッジ】
事例検索サービス
https://www.juse.jp/j-club/knowledge/

事例検索サービス（J-ナレッジ）2021年版の【ログインID･PW】は、
2021年4月1日よりJ-Clubサイトに掲載させていただきます。

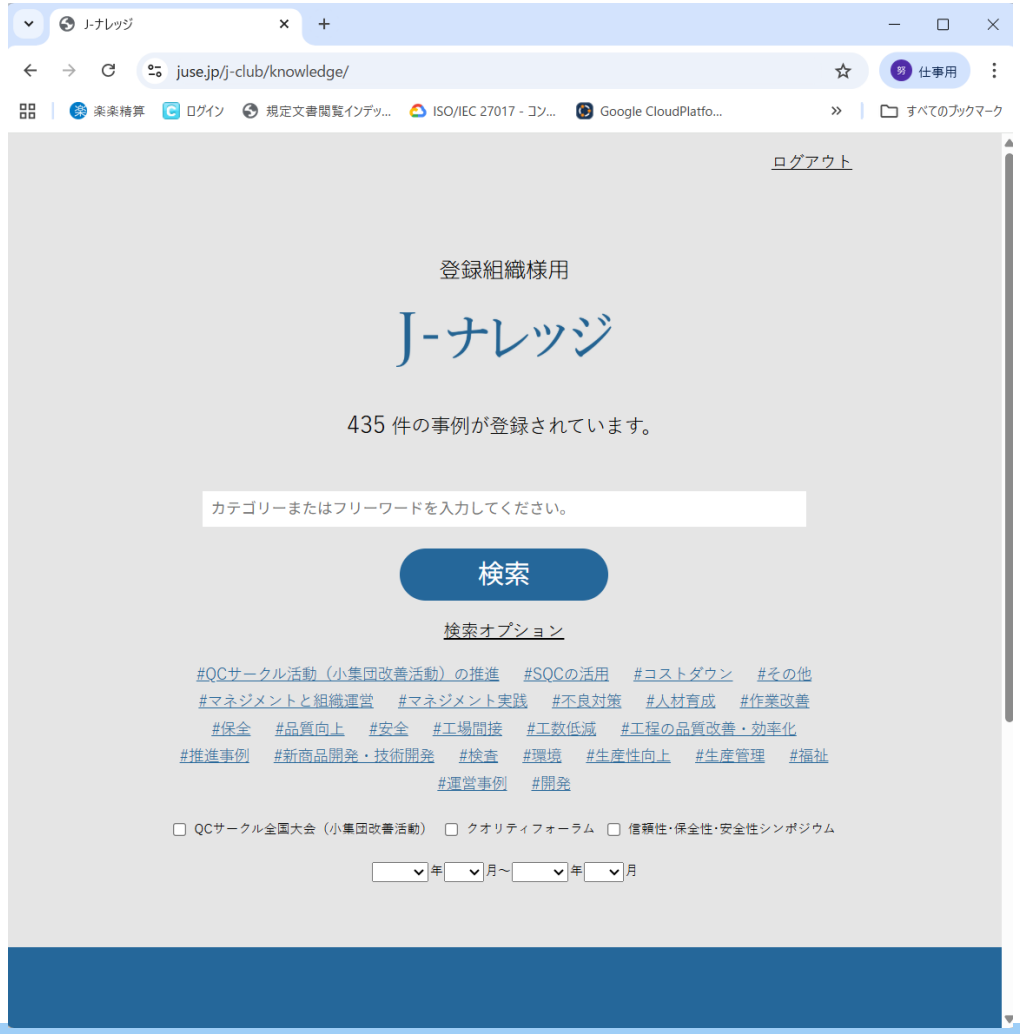
https://www.juse.jp/j-club/knowledge/

J-ナレッジは動画配信ではなく、PDFデータでのご提供となります。

【J-Club NEWS】
- **年4回（1月、4月、7月、10月）の定期発行**のほか、トピックスがある場合は臨時発行もいたします。
- **メールやJ-Clubサイト**（ログインID、PWが必要）**での情報発信**も行なっております。

J–ナレッジ

J–ナレッジでは、QCサークル、クオリティフォーラム、信頼性・保全性・安全性シンポジウムでの事例を検索し、情報収集できます。



ご清聴ありがとうございました。

― 品質経営で明るい未来を創る ―