令和5年度
中小企業サイバーセキュリティ対策
継続支援事業

全体総括

サイバーセキュリティ
人材育成
社内体制整備支援

セミナー内容

回数	テーマ
第1回	サイバーセキュリティを取り巻く環境および中小企業に 求められるサイバーセキュリティ対策
第2回	これからの企業経営で必要な攻めと守りのIT活用および サイバーセキュリティ対策
第3回	サイバーセキュリティに関する国の方針・施策および サイバー脅威の動向
第4回	サイバーセキュリティ対策におけるフレームワークの体系
第5回	組織として策定すべき対策基準及び情報セキュリティの 三大要素【対策基準レベル①】

セミナー内容

回数	テーマ
第6回	セキュリティリスク評価及び対策基準に記載されるべき管理策【対策基準レベル②】
第7回	組織として実施すべき具体的な対策事項・手順【実施手順・実施者マニュアルレベル①】
第8回	組織的対策と人的対策【実施手順・実施者マニュアルレベル②】
第9回	技術的対策と物理的対策およびセキュリティ対策状況の有効性評価【実施手順・実施者マニュアルレベル③】
第10回	全体総括

１．総括編

全体概要

各章のポイント

読者に今後行ってほしいこと

テキストの活用

【参照：テキスト19-1-1.】
第19章 - 02

活用のポイント

1. 「DXの理解から対策の実践まで」のポイントを再認識する

2. 経営者を含めた関係者と共有する

3. 経営者のリーダーシップによって社内体制を確立する

4. 具体的なアクションを起こして一歩ずつ実践する

テキストの活用

【参照：テキスト19-1-1.】
第19章 - 03

1.「DXの理解から対策の実践まで」のポイントを再認識する

DXの推進の考え方の把握	
第1章	現代社会のITに関する情勢、Society5.0やDXについて紹介
第5章	政府が発表している国の基本方針や、国が目指している社会を実現するための計画を通じて、IT、デジタル、サイバーセキュリティの方向性・課題について紹介

セキュリティ対策の全容の認識	
第2章	近年のサイバー攻撃の傾向や手法を、実際のインシデント事例など通して把握し、それらの脅威に対する対策や、実際に被害にあってしまった際の対応方法を紹介
第3章	サイバーセキュリティの基本的な知識や対策や、自社のリスク状況や活用可能なリソースを考慮した、脅威に対する最適な対処方法を紹介
第4章	これからの企業経営で必要な観点となる社会の動向、「守りのIT投資」や「攻めのIT投資」などのIT投資、経営投資としてのサイバーセキュリティ対策の重要性を紹介
第6章	NISCによるサイバーセキュリティ戦略を通じて、DXとサイバーセキュリティの確保を同時に推進する重要性、サイバーセキュリティに関連する法令（個人情報保護法とGDPR）について紹介
第7章	ISMSをはじめとしたサイバーセキュリティ対策における代表的なフレームワークの特徴を紹介
第8章	ISMSを前提としたサイバーセキュリティ対策における基準を3段階にレベル分けし、各基準の手法を紹介
第9章	ISO/IEC 27002における管理策の分類と構成について紹介
第10章	ISO/IEC 27000に記述されている「リスク」、「脅威」、「脆弱性」、「管理策」といった用語の定義、それらの用語の関係性、脅威や脆弱性の識別方法を紹介

テキストの活用

【参照：テキスト19-1-1.】
第19章 - 03

1.「DXの理解から対策の実践まで」のポイントを再認識する

自組織でのセキュリティ対策の実施項目の認識	
第11章	リスクマネジメントの概要と、リスクマネジメントプロセスにおけるリスクアセスメントの手法やリスク対応の考え方を紹介
第12章	セキュリティインシデント事例を参考にするクイックアプローチと、ガイドラインやひな形などの資料を参考にするベースラインアプローチにおける対策基準・実施手順の策定方法を紹介
第13章	情報セキュリティマネジメントシステム（ISMS）のフレームワークを用いて、体系的・網羅的にセキュリティ対策基準、実施手順を作成する網羅的アプローチについて紹介

自組織として実践準備	
第14章	情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則として、組織的管理策を用いた「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について紹介
第15章	情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則として、人的管理策を用いた「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について紹介
第16章	情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則として、物理的管理策を用いた「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について紹介
第17章	情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則として、技術的管理策を用いた「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について紹介
第18章	セキュリティ対策をした結果、効果があったのか、目標に近づいているかを判断するための取組みである監査について紹介

テキストの活用

【参照：テキスト19-1-1.】
第19章 - 04

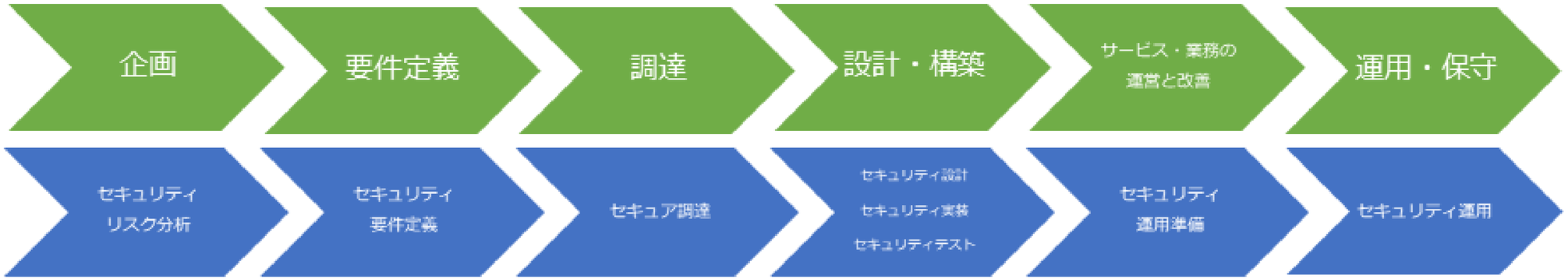
2. 経営者を含めた関係者と共有する

エグゼクティブサマリとしての活用（第19章 総括編）

3. 経営者のリーダーシップによって社内体制を整備する

デジタルスキル標準	DXリテラシー標準	ビジネスパーソン全体がDXに関する基礎的な知識やスキル・マインドを身につけるための指針 ※DXを利用する立場の方向け
	DX推進スキル標準	企業がDXを推進する専門性を持った人材を確保・育成するための指針 ※DXを推進する立場の方向け

4. 具体的なアクションを起こして一歩ずつ実践する



中小企業の情報セキュリティ対策

【参照：テキスト19-1-2.】
第19章 - 05

これまでの振り返り

テキストの概要	
第1回 （第1章～第3章）	情報セキュリティ白書、情報セキュリティ10大脅威、最近の事例、Security Actionについて紹介し、現代社会のIT情勢や、サイバー攻撃の傾向、脅威への対処方法について解説しました。
第2回 （第4章）	企業経営の観点で、ITの普及によるサプライチェーンの変化や、IT活用の課題、「守り」と「攻め」という2種類のIT投資、サイバーセキュリティ確保の重要性について解説しました。
第3回 （第5章～第6章）	日本政府がDXによってどのような社会を目指しているのか、サイバーセキュリティをどのように実現しようとしているのかについて解説しました。
第4回 （第7章）	サイバーセキュリティ対策におけるフレームワークについて、特にISMS、CSF、CPSF、サイバーセキュリティ経営ガイドラインについてピックアップして解説しました。
第5回 （第8章～第10章）	ISMSを前提に、セキュリティ対策基準とその策定方法、セキュリティ対策を示した管理策、「リスク」「脅威」「脆弱性」とは何かについて解説しました。
第6回 （第11章）	リスクを管理し、損失を回避、低減するためのリスクマネジメントに関して、その意義や、リスクアセスメントやリスク対応についてのプロセスを解説しました。
第7回 （第12章～第13章）	セキュリティ対策基準や、その具体的な実施手順を策定するにあたってのアプローチ方法として、クイックアプローチ、ベースラインアプローチ、網羅的アプローチを解説しました。
第8回 （第14章～第15章）	セキュリティ対策の具体的な規則としての「対策基準」と、その具体的な方法である「実施手順」について、組織的管理策、人的管理策をもとに解説しました。
第9回 （第16章～第18章）	セキュリティ対策の具体的な規則としての「対策基準」と、その具体的な方法である「実施手順」について、物理的管理策、技術的管理策をもとに解説し、対策状況の評価として監査についても解説しました。

第1章 デジタル時代の社会とIT情勢

【参照：テキスト19-2-1.】
第19章 - 06

内容

- デジタル時代の社会変革とIT情勢の関係性

主なキーワード

- Society5.0
- DX

全体概要

- 現代社会は技術革新とグローバル化で大きく変わっている。
- 日本政府は、Society5.0という新しい社会モデルを推進。
- Society5.0はデジタル技術を使って社会問題を解決し、生活を向上させることを目指す。
- AIやビッグデータを活用した効率的な社会システムと持続可能な産業構造を構築。
- 企業にはDXを推進し、データとデジタル技術を活用して新たな価値を顧客視点で創出することが期待されている。

第1章 デジタル時代の社会とIT情勢

【参照：テキスト19-2-1.】
第19章 - 06

訴求ポイント

章を通した気づき・学び

- 社会動向の情報収集が企業・組織には重要。
- ビジネス環境の変化への対応のためDX推進が必要。
- デジタル社会に適したビジネスモデル、組織、企業文化への変革が求められる。

認識していただきたい実施概要

- 中小企業はリソースが限られているため、ビジネス環境の変化に対応するためにDXの推進が重要。
- 最新技術に関する知識と精通した人材が要求される。
- データとデジタル技術の安全利用のためにセキュリティ対策が重要。

第2章 事例を知る：重大なインシデント発生から課題解決まで

【参照：テキスト19-2-2.】
第19章 - 07

内容

- 情報セキュリティの概要
- 重大インシデント事例から学ぶ課題解決
- 実際の被害事例からみるケーススタディ

主なキーワード

- 情報セキュリティ白書
- 情報セキュリティ10大脅威
- ランサムウェア
- サプライチェーン攻撃
- テレワーク
- 脅威
- インシデント
- サイバー被害

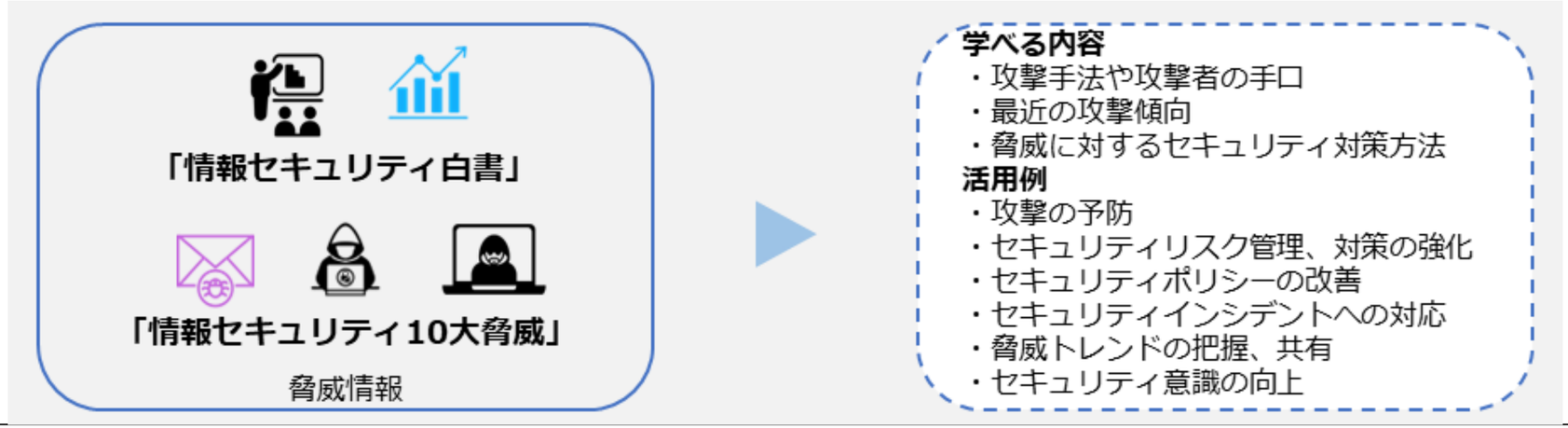
第2章 事例を知る：重大なインシデント発生から課題解決まで

【参照：テキスト19-2-2.】
第19章 - 07

全体概要

- 情報セキュリティ白書と10大脅威、インシデント事例を基に脅威を紹介。
- ランサムウェアとサプライチェーン攻撃が深刻。
- 攻撃は自社業務と取引先の信用に悪影響を与える。
- 攻撃は企業規模に関わらず発生。
- 中小企業もセキュリティ対策が不可欠。

情報セキュリティの概況



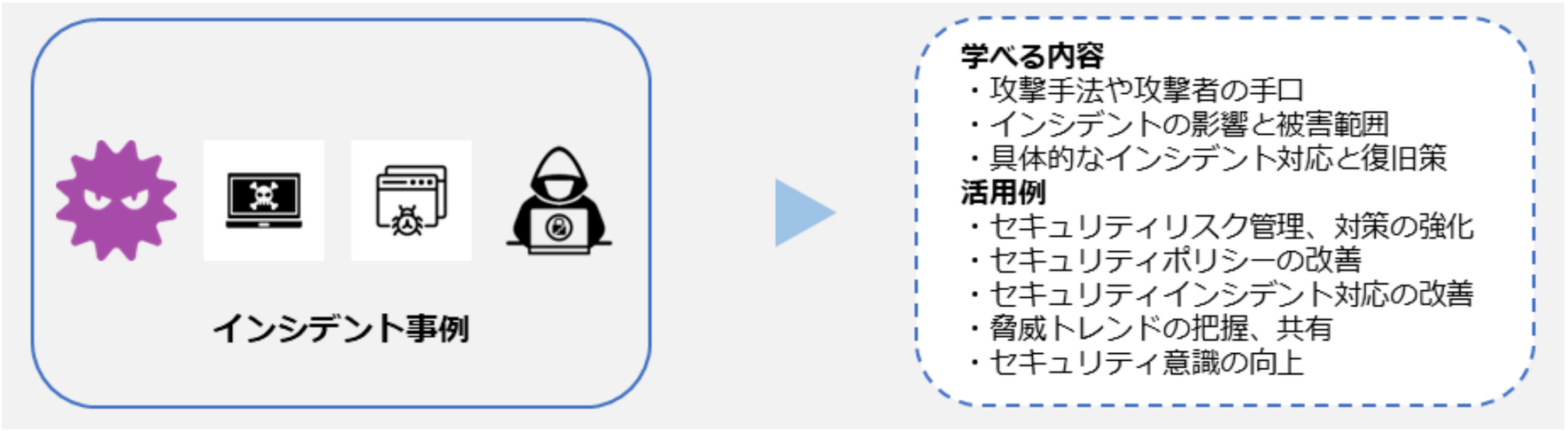
第2章 事例を知る：重大なインシデント発生から課題解決まで

【参照：テキスト19-2-2.】
第19章 - 08

重大インシデント事例から学ぶ課題解決

- 対応策の策定とリスク戦略の改善が必要。
- セキュリティ意識の向上が重要。
- IoTデバイス攻撃、サプライチェーンを介したメール攻撃、テレワークでの情報漏えい、ランサムウェア感染を含むインシデント事例を分析。
- 何が失敗したか、どの攻撃手法が用いられたか、どの脆弱性が標的になったかを理解することが大切。

実際の被害事例から見るケーススタディ



第2章 事例を知る：重大なインシデント発生から課題解決まで

訴求ポイント

【参照：テキスト19-2-2.】
第19章 - 08

章を通した気づき・学び

- 最新のセキュリティ脅威と脆弱性を理解する。
- 攻撃傾向を把握し、適切な予防と対策を実施。
- 過去のインシデントを分析し、対応策を強化。

認識していただきたい実施概要

- 脆弱性と脅威情報を最新の状態で把握する。
- セキュリティリスク評価には情報セキュリティ白書や10大脅威の情報が有効。
- 適切な予防策や対策の策定には過去のインシデント事例の分析が役立つ。
- リスク戦略の改善とセキュリティ意識の向上が必要。
- 未来のインシデントに備えるためには、原因とベストプラクティスを理解することが重要。

第3章 サイバーセキュリティの基礎知識

【参照：テキスト19-2-3.】
第19章 - 09

内容

- 導入済と想定するセキュリティ対策機能
- 各種資格試験から得るサイバーセキュリティの基礎知識
- Security Action（セキュリティ対策自己宣言）
- サイバーセキュリティアプローチ方法

主なキーワード

- UTM
- EDR
- 情報処理技術者試験
- SECURITY ACTION

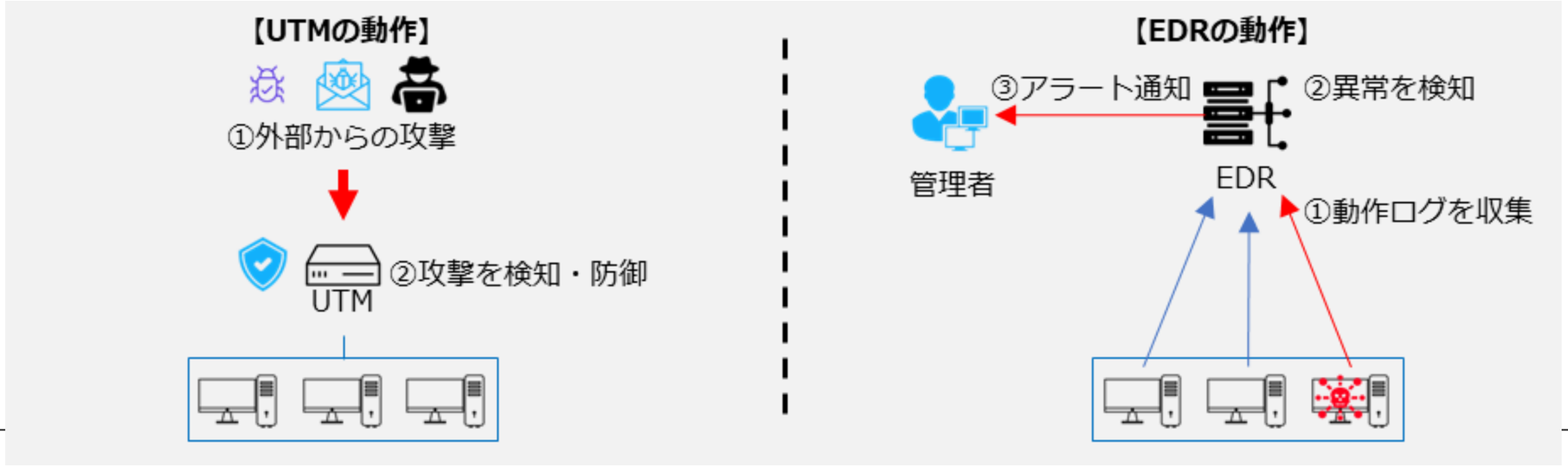
第3章 サイバーセキュリティの基礎知識

【参照：テキスト19-2-3.】
第19章 - 09

全体概要

- UTM、EDR機能とITセキュリティ知識の確認には、情報処理技術者試験が有効。
- 中小企業にはSECURITY ACTIONへの取り組みを推奨。
- サイバーセキュリティの脅威への対処には、3つの段階的アプローチが効果的。

導入済と想定するセキュリティ対策機能



第3章 サイバーセキュリティの基礎知識

【参照：テキスト19-2-3.】
第19章 - 10

各種資格試験から得るサイバーセキュリティの基礎知識

- ITパスポート試験（TP）
- 情報セキュリティマネジメント試験（SG）
- 基本情報技術者試験（FE）

SECURITY ACTION（セキュリティ対策自己宣言）

- 情報セキュリティ5か条
- 5分でできる！情報セキュリティ自社診断
- 情報セキュリティ基本方針

サイバーセキュリティアプローチ方法

- LV1. クイックアプローチ
- LV2. ベースラインアプローチ
- LV3. 網羅的アプローチ

第3章 サイバーセキュリティの基礎知識

【参照：テキスト19-2-3.】
第19章 - 10

訴求ポイント

章を通した気づき・学び

- ITと情報セキュリティの知識習得が重要。
- 社内外のセキュリティ専門家と協力する能力を持つことが必要。
- SECURITY ACTIONに取り組むことで従業員の意識を高め、信頼を向上。

認識していただきたい実施概要

- 情報処理技術者試験がITとセキュリティ知識の習得状況の確認に有効。
- 「SECURITY ACTION」制度は中小企業の情報セキュリティ対策に役立ち、従業員の意識と対外信頼を高める。
- サイバーセキュリティの脅威対処には効果的な3段階アプローチが存在。

第4章 企業経営で重要となるIT投資と投資としてのサイバーセキュリティ対策

【参照：テキスト19-2-4.】
第19章 - 11

内容

- これからの企業経営で必要な観点：社会の動向
- 守りのIT投資と攻めのIT投資
- 経営投資としてのサイバーセキュリティ対策

主なキーワード

- 守りのIT投資
- 攻めのIT投資

第4章 企業経営で重要となるIT投資と投資としてのサイバーセキュリティ対策

【参照：テキスト19-2-4.】
第19章 - 11

全体概要

- 社会動向に基づくセキュリティ対策とIT活用の重要性を説明。
- 守りのIT投資（業務効率化、コスト削減）と攻めのIT投資（DX）の特徴と違いを紹介。
- デジタル技術の主要な活用方法について説明。
- 経営者主体のサイバーセキュリティ対策の必要性と要点を強調。

これからの企業経営で必要な観点：社会の動向

- 社会動向と現実社会とサイバー空間の連携を説明。
- 現代は技術進化と競争激化により、革新的なアイディアと迅速な行動が必要。
- Society5.0が経済発展と社会課題解決のために提唱されている。
- 日本のデジタル化遅れの原因と現状のDX取り組みを米国と比較。

第4章 企業経営で重要となるIT投資と投資としてのサイバーセキュリティ対策

【参照：テキスト19-2-4.】
第19章 - 12

守りのIT投資と攻めのIT投資

「守りのIT投資」
（デジタルオプティマイゼーション）
目的：生産性向上

・業務の効率化
・コストの削減

「攻めのIT投資」
（デジタルトランスフォーメーション）
目的：ビジネス継続・競争力強化

・新たなビジネスの展開
・顧客視点で新たな価値の創造

経営投資としてのサイバーセキュリティ対策

ポイント①：ビジネスの継続・発展にはITの活用が不可欠
ポイント②：ITの活用にはサイバー攻撃への対策が必要
ポイント③：サイバーセキュリティ対策は経営者が自ら実行

第4章 企業経営で重要となるIT投資と投資としてのサイバーセキュリティ対策

【参照：テキスト19-2-4.】
第19章 - 12

訴求ポイント

章を通した気づき・学び

- Society5.0の提唱のもと、企業はデジタル技術を活用してビジネスモデルを変革。
- 顧客視点で新たな価値を創出するDXの推進には「攻めのIT投資」が重要。
- サイバーセキュリティ対策は経営者が主体となって指揮することが大切。

認識していただきたい実施概要

- 現実社会とサイバー空間の連携、Society5.0など社会動向の理解が企業経営で重要。
- 「攻め」と「守り」のIT投資を理解し、特に攻めのIT投資への取り組みが必要。
- DX推進とデータ・デジタル技術活用に伴い、サイバーセキュリティ対策が重要。

第5章 デジタル社会の方向性と実現に向けた国の方針

【参照：テキスト19-2-5.】
第19章 - 13

内容

- 国の基本方針および実施計画の要約
- 政府機関が目指す社会の方向性とサイバーセキュリティ課題

主なキーワード

- デジタル社会
- DX
- DXの推進
- サプライチェーン

第5章 デジタル社会の方向性と実現に向けた国の方針

【参照：テキスト19-2-5.】
第19章 - 13

全体概要

- 国のデジタル社会方針や政策、サイバーセキュリティの位置付けについて解説。
- Society5.0を目指すデジタル社会に言及。
- DXに関して、中小企業の優位性について事例を交えて説明。

国の基本方針および実施計画の要約

- IT・セキュリティ関連施策は「経済財政運営と改革の基本方針」に基づく。
- 2023年度の方針には「サプライチェーンの強靭化」と「DXの加速」が含まれる。

第5章 デジタル社会の方向性と実現に向けた国の方針

【参照：テキスト19-2-5.】
第19章 - 13

国の基本方針および実施計画の要約

- 国の基本方針に従い、IT・セキュリティ関連施策の実施計画が策定。
- 2023年度の方針には「サプライチェーンの強靭化」と「DXの加速」が含まれる。

政府機関が目指す社会の方向性とサイバーセキュリティ課題

- 政府は「経済財政運営と改革の基本方針」に基づく「デジタル社会の実現に向けた重点計画」を策定。
- 重点計画の「産業のデジタル化」部分には「中小企業のDX推進」と「中小企業のデジタル化の支援」が含まれる。

第5章 デジタル社会の方向性と実現に向けた国の方針

【参照：テキスト19-2-5.】
第19章 - 14

デジタル社会を実現していくための7つの戦略的な政策

1. デジタル社会の実現に向けた構造改革
2. デジタル田園都市国家構想の実現
3. 国際戦略の推進
4. サイバーセキュリティなどの安全・安心の確保
5. 急速なAIの進歩・普及を踏まえた対応
6. 包括的データ戦略の推進と今後の取組
7. Web3.0の推進

中小企業がデジタルトランスフォーメーション推進における優位な点

- 参考情報が豊富
- 環境が整備されている
- 環境の変化に素早く対応しやすい

第5章 デジタル社会の方向性と実現に向けた国の方針

【参照：テキスト19-2-5.】
第19章 - 14

訴求ポイント

章を通した気づき・学び

- デジタル活用進展に伴いサイバーセキュリティリスクが増加。
- 企業は自社のIT活用状況を認識する必要がある。
- 必要な知識・スキルを持った人材の育成・確保が重要。

認識していただきたい実施概要

- 国の基本方針と社会実現計画を通じて、IT、デジタル、サイバーセキュリティの方向性・課題を学ぶ。
- 中小企業の優位性を理解し、DXに積極的に取り組むことが組織成長に重要。

第6章 サイバーセキュリティ戦略および関連法令

【参照：テキスト19-2-6.】
第19章 - 15

内容

- NISC：サイバーセキュリティ戦略
- 関連法令

主なキーワード

- サイバーセキュリティ戦略
- DX with Cybersecurity
- 個人情報保護

第6章 サイバーセキュリティ戦略および関連法令

【参照：テキスト19-2-6.】
第19章 - 15

全体概要

- NISCの「サイバーセキュリティ戦略」の紹介とDX with Cybersecurityの解説。
- デジタル利用増加に伴いサイバーセキュリティリスクが高まる。
- 企業は自社のIT活用状況を把握し、必要な知識・スキルを持った人材を育成・確保する必要がある。
- 適切なサイバーセキュリティ対策の実施が重要。

第6章 サイバーセキュリティ戦略および関連法令

【参照：テキスト19-2-6.】
第19章 – 15, 16

NISC：サイバーセキュリティ戦略

- サイバーセキュリティ戦略
- 企業経営のためのサイバーセキュリティの考え方
- DX with Cybersecurity
- デジタルスキル標準（DSS）
- プラス・セキュリティ

関連法令

- 個人情報保護法
- GDPR（EU一般データ保護規則）

第6章 サイバーセキュリティ戦略および関連法令

【参照：テキスト19-2-6.】
第19章 - 16

訴求ポイント

章を通した気づき・学び

- 日本政府のサイバーセキュリティ戦略を理解することが重要。
- 関連する知識やスキルの習得が必要。

認識していただきたい実施概要

- 国家レベルでサイバーセキュリティを確保する方針や目標を理解する。
- サイバーセキュリティ対策を経営のための必要な投資と位置付ける。
- DX推進と同時にサイバーセキュリティ対策の重要性を認識し、必要なセキュリティ能力（プラス・セキュリティ）を身につける。
- 個人情報保護法やGDPRを含むサイバーセキュリティ関連法令の遵守と、個人情報の高レベル取扱いの重要性。

第7章 セキュリティフレームワーク

【参照：テキスト19-2-7.】
第19章 - 17

内容

- セキュリティフレームワークの概要
- 情報セキュリティマネジメントシステム（ISMS）[ISO/IEC27001:2022, 27002:2022]
- NIST サイバーセキュリティフレームワーク（CSF）
- サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）
- サイバーセキュリティ経営ガイドライン

主なキーワード

- セキュリティフレームワーク
- ISMS

第7章 セキュリティフレームワーク

【参照：テキスト19-2-7.】
第19章 - 17

全体概要

- セキュリティ対策関連フレームワークの特徴と概要、要素や要件を解説。
- 無計画なセキュリティ対策は複雑化や抜け漏れのリスクを招く。
- 企業はセキュリティフレームワークを用いて、自社に適した対策方針を選択することが重要。

セキュリティフレームワークの概要

- ISMS（情報セキュリティマネジメントシステム）[ISO/IEC27001, 27002]
- ISO/IEC27017
- CSF（サイバーセキュリティフレームワーク）
- CPSF（サイバー・フィジカル・セキュリティ対策フレームワーク）
- サイバーセキュリティ経営ガイドライン
- PCI DSS
- PMS（個人情報保護マネジメントシステム）
- CIS Controls
- ISA/IEC62443

第7章 セキュリティフレームワーク

【参照：テキスト19-2-7.】
第19章 – 17, 18

情報セキュリティマネジメントシステム（ISMS）

- ISMSは組織の情報セキュリティリスクを適切に管理するための仕組み。
- セキュリティフレームワークの中で代表的な存在。
- 目標はリスクマネジメントプロセスを通じて情報の機密性、完全性、可用性を維持・改善。
- リスクを適切に管理し、利害関係者に信頼を提供。

NIST サイバーセキュリティフレームワーク（CSF）

- サイバーセキュリティフレームワーク（CSF）はNISTが作成したサイバー攻撃対策のフレームワーク。
- 防御だけでなく、検知・対応・復旧のインシデント対応を含む。
- 多様な企業に適用可能な汎用性のある要求事項。
- CSFは①コア（対策一覧）、②ティア（成熟度評価基準）、③プロファイル（対策の現状と目標記述）の3要素で構成。

第7章 セキュリティフレームワーク

【参照：テキスト19-2-7.】
第19章 – 18

サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

- サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）は、ISMSとCSFを包含する。
- サイバー空間とフィジカル空間の両方のセキュリティ対策に対応したフレームワーク。

サイバーセキュリティ経営ガイドライン

- 経営者向けのサイバーセキュリティ対策指針。
- 経営者が認識すべき事項と、CISOなどの責任者に指示すべき事項を包括的にまとめている。
- 経営者がサイバーセキュリティ対策を実施する際の参考資料。

第7章 セキュリティフレームワーク

【参照：テキスト19-2-7.】
第19章 – 18

訴求ポイント

章を通した気づき・学び

- セキュリティ対策の漏れなく効果的な実施にはセキュリティフレームワークの使用が有効。
- 多様なフレームワークの中から自社の課題や目的に合ったものを選択することが重要。

認識していただきたい実施概要

- フレームワークに沿ってセキュリティ対策を進めることで、効果的な対策実施と信頼向上が可能。
- セキュリティ対策フレームワークは複数存在するが、ISMSを基本枠組みとして使用。
- 必要に応じて、業種や重点領域に特化したフレームワークで補完するのが有効。

第8章 セキュリティ対策基準の策定

【参照：テキスト19-2-8.】
第19章 – 19

内容

- 対策基準の策定

主なキーワード

- セキュリティ対策基準
- クイックアプローチ
- ベースラインアプローチ
- 網羅的アプローチ

第8章 セキュリティ対策基準の策定

【参照：テキスト19-2-8.】
第19章 – 19

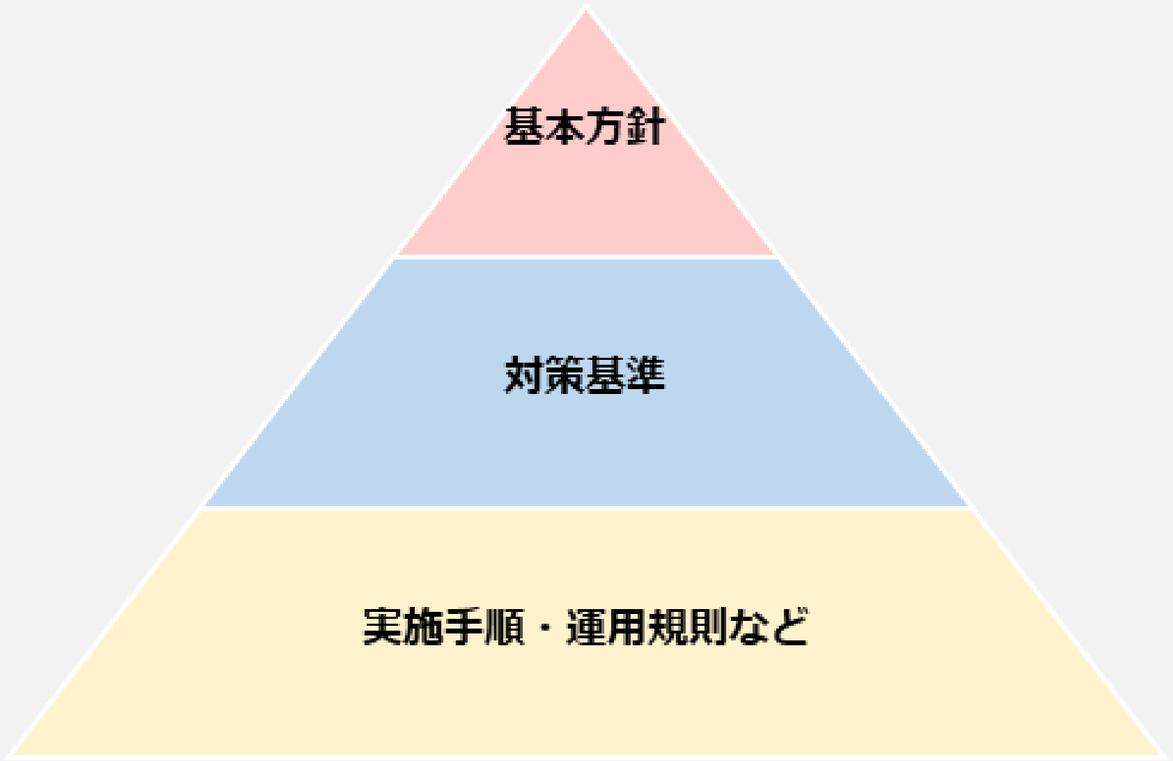
全体概要

- セキュリティポリシー構成（基本方針、対策基準、実施手順・運用規則など）について説明。
- 企業の現状や目標に応じた対策基準策定に3つのアプローチ手法を紹介
  - LV.1 クイックアプローチ
  - LV.2 ベースラインアプローチ
  - LV.3 網羅的アプローチ

第8章 セキュリティ対策基準の策定

【参照：テキスト19-2-8.】
第19章 – 19

対策基準の策定



基本方針
情報セキュリティに対する組織の基本方針・宣言を記述する。

対策基準
基本方針を実践するための具体的な規則を記述する。

実施手順・運用規則など
対象者や用途によって必要な手続を記述する。

第8章 セキュリティ対策基準の策定

【参照：テキスト19-2-8.】
第19章 – 20

対策基準策定のアプローチ方法

アプローチ手法	特徴	想定される適用ケース
LV.1 クイックアプローチ	インシデント事例内容を参考にして、対策基準を策定する方法。即時の対応や緊急事態への対処に適したアプローチ手法。	自社で発生する可能性が高い、または、発生したときの被害が大きいと考えられるインシデントに対処する場合。
LV.2 ベースラインアプローチ	ガイドラインやひな形を参考にして、対策基準を策定する方法。組織全体での一貫性を確保し、セキュリティの最低基準を満たすことを目指すアプローチ方法。	組織的に一定以上の対策基準を策定する場合。
LV.3 網羅的アプローチ	ISMSなどの既存のフレームワークを用いて、さまざまな脅威や攻撃手法に対して、網羅的な対策を講じることを目指すアプローチ手法。	ISMSの認証取得を目指す場合、あるいは、ISMSの認証取得が可能なレベルを目指す場合。

第8章 セキュリティ対策基準の策定

【参照：テキスト19-2-8.】
第19章 – 20

訴求ポイント

章を通した気づき・学び

- 状況に応じた適切なサイバーセキュリティ対策アプローチを選択することが重要。
- セキュリティ対策実施を内外に示すためには、対策基準の策定が必要。

認識していただきたい実施概要

- 対策基準を外部に公開し、セキュリティ対策の実施と説明責任を果たす。
- 実施手順を策定した対策基準に基づいて作成することが重要。
- 対策基準の策定には、「クイックアプローチ」「ベースラインアプローチ」が可能。
- 網羅的な対策にはISMSを参考にした「網羅的アプローチ」が推奨される。

第9章 管理策のテーマと属性

【参照：テキスト19-2-9.】
第19章 – 21

内容

- 管理策の分類と構成

主なキーワード

- 管理策
- ISO/IEC 27002

全体概要

- ISMSの管理策を示した規格のISO/IEC 27002についての説明。

第9章 管理策のテーマと属性

【参照：テキスト19-2-9.】
第19章 – 21

管理策の分類と構成

- 2013年版では管理策が14分野114項目だったが、2022年版では82項目に統合、新たに11項目が追加され、合計93項目に。
- 2022年版の管理策は「組織的管理策」「人的管理策」「物理的管理策」「技術的管理策」の4つのカテゴリに分類。
- 「属性（attribute）」という新概念が導入され、管理策のフィルタリング、並び替え、提示が容易に。
- ISMS構築時には、これらの管理策から自社に適したものを選択し、対策基準として採用。

第9章 管理策のテーマと属性

【参照：テキスト19-2-9.】
第19章 – 22

管理策のテーマと属性

第9章 管理策のテーマと属性

【参照：テキスト19-2-9.】
第19章 – 22

訴求ポイント

章を通した気づき・学び

- 企業や組織はISO/IEC 27002の管理策から、組織に必要なものを選択することが重要。

認識していただきたい実施概要

- ISMSにおいて、リスク対応の対策として管理策があり、ISO/IEC 27002:2022で93項目が示されている。
- ISO/IEC 27002:2022の管理策には4つのテーマと5つの属性があり、これらを参考に組織に必要なセキュリティ対策を選択することが重要。

第10章 脅威、脆弱性、リスクの定義と関係性

【参照：テキスト19-2-10.】
第19章 – 23

内容

- 用語の定義および関係性と識別方法

主なキーワード

- リスク
- 脅威
- 脆弱性

全体概要

- 「リスク」、「脆弱性」、「脅威」の定義とそれらの関係性についての理解。
- 「脅威」と「脆弱性」の識別方法についての詳細な説明。

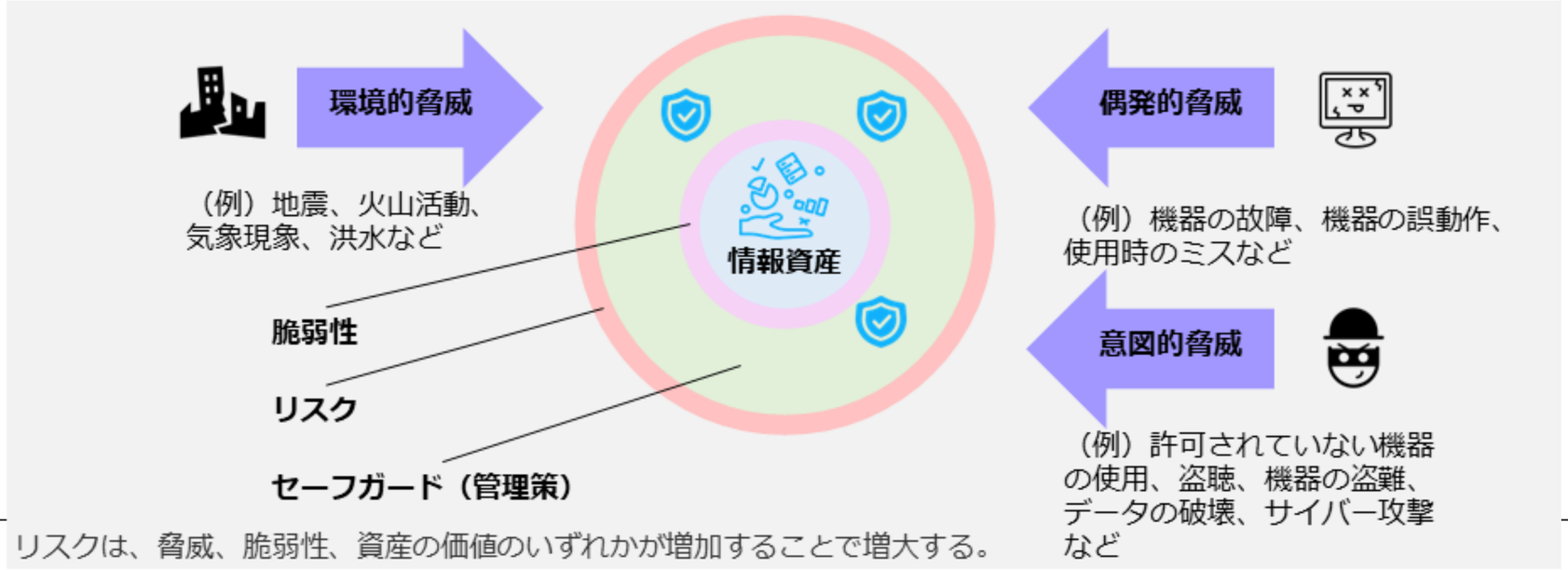
第10章 脅威、脆弱性、リスクの定義と関係性

【参照：テキスト19-2-10.】
第19章 – 23

用語の定義および関係性と識別方法

- 企業や組織にはセキュリティ上のリスクが存在する。
- これらのリスクを効率的に管理するためにはリスクマネジメントが必要。
- リスクマネジメントを理解するために、「脅威」、「脆弱性」、「リスク」という用語の定義と関係性を説明している。

（例）業務用ノートパソコンに関する脅威や脆弱性、管理策の関係



第10章 脅威、脆弱性、リスクの定義と関係性

【参照：テキスト19-2-10.】
第19章 – 24

脅威の識別

脅威の種類		想定される被害とセキュリティ対策
環境的脅威 (Environmental → E)		環境的脅威として地震や高潮がありますが、地震や高潮の発生そのものをコントロールすることはできません。従って、地震の発生可能性が低い場所を選択する、地震が発生した場合に素早く検知し、災害から回復する対策を検討して実施する、などのセキュリティ対策が選択されることになります。
人為的脅威	意図的脅威 (Deliberate → D)	悪意のある者によるサイバー攻撃（不正アクセスや標的型攻撃、DDoS攻撃など）があります。対策としては、OSやソフトウェアのアップデートを適宜実施する、EDRやUTMなどのセキュリティ製品を導入する、従業員へ教育の実施などがあげられます。サイバー攻撃により、個人情報や機密情報の漏えい、サービスの停止などの被害にあう可能性があるため、適切なセキュリティ対策を実施することが重要です。
	偶発的脅威 (Accidental → A)	「入力ミス」がありますが、入力ミスが生じないように、2回ずつ入力する、一定の範囲の値しか入力できないようにする、チェックデジットやチェックサムを設けるといった技術対策が有効となります。

脆弱性の識別

- 脆弱性があってもインシデントが発生するわけではないが、脆弱性は脅威を引き起こし、インシデントの発生確率を高める可能性がある。
- 脆弱性を減らすためには適切な管理策が必要であり、脆弱性は管理策の不足を示す。
- 脆弱性を識別することは必要な管理策を特定するのに役立つ。

第10章 脅威、脆弱性、リスクの定義と関係性

【参照：テキスト19-2-10.】
第19章 – 24

訴求ポイント

章を通した気づき・学び

- リスクマネジメントで使用される「脅威」、「脆弱性」、「リスク」という用語の定義や関係性を理解することの重要性。
- 「脅威」、「脆弱性」を識別する方法の理解の重要性。

認識していただきたい実施概要

- リスクは「脅威」「脆弱性」「資産の価値」のいずれかが増加することによって増大する。
- リスクを減少させるためには、「脅威」「脆弱性」「資産の価値」を識別し、保護要求事項を特定し、適切なセーフガードを実施する必要がある。

第11章 リスクマネジメント

【参照：テキスト19-2-11.】
第19章 – 25

内容

- リスクマネジメント：概要
- リスクマネジメント：リスクアセスメント
- リスクマネジメント：リスク対応

主なキーワード

- リスクマネジメント
- リスクアセスメント

第11章 リスクマネジメント

【参照：テキスト19-2-11.】
第19章 – 25

全体概要

- リスクマネジメントプロセスにはリスク基準の確立、リスクアセスメント、リスク対応が含まれる。
- リスクマネジメントはセキュリティ対策に必要であるが、顕在化していないリスクを考えるのは難しいことがある。
- リスクマネジメントプロセスの各段階で特定、分析、対応策の検討を円滑に行うための考え方と手法が存在する。

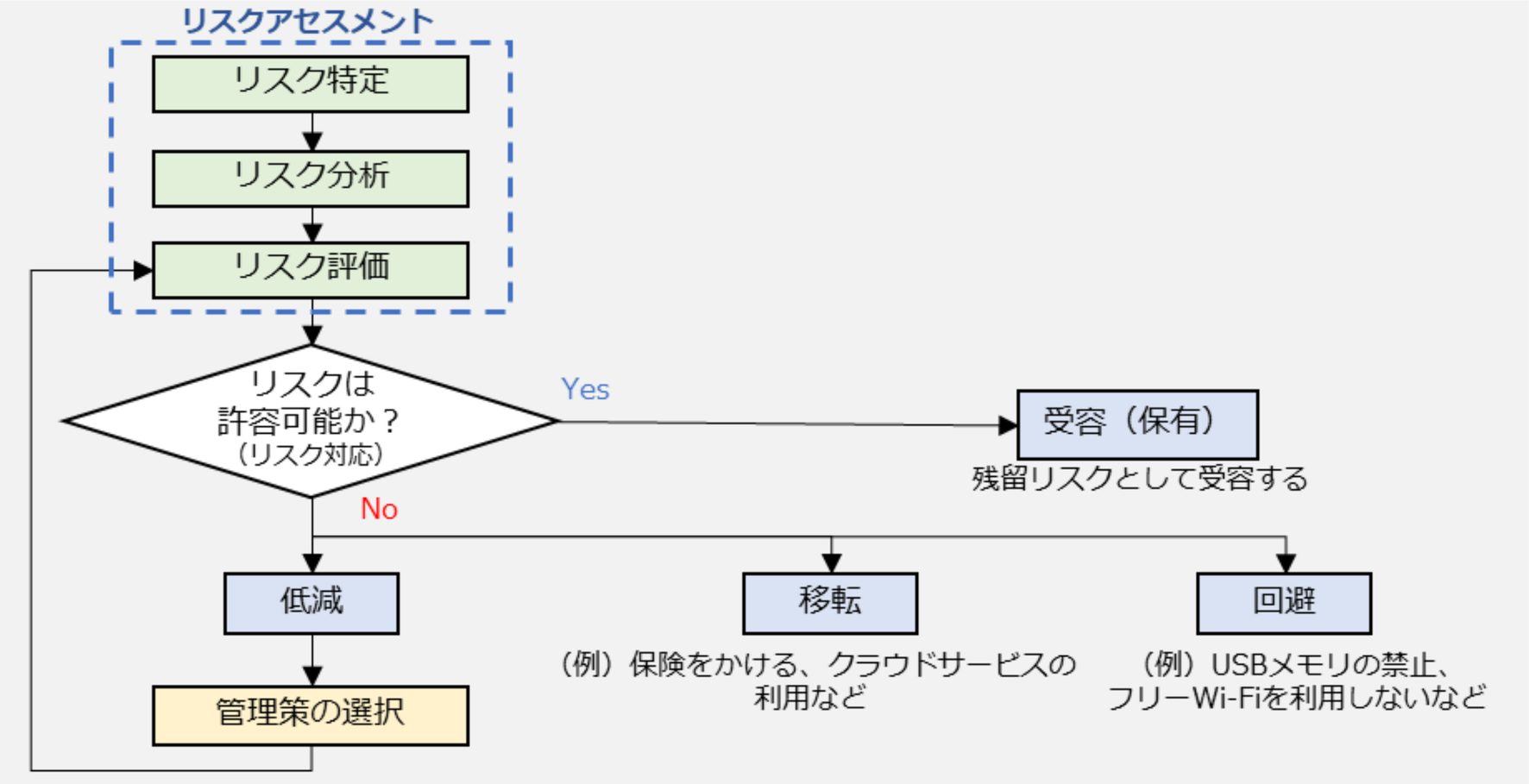
リスクマネジメント：概要

- リスクマネジメントプロセス（ISO 31000）
- 情報セキュリティリスクマネジメント（ISO/IEC 27005）
- ISO/IEC 27001におけるリスクマネジメント手順

第11章 リスクマネジメント

【参照：テキスト19-2-11.】
第19章 – 26

リスクマネジメント：リスクアセスメント
リスクマネジメント：リスク対応



第11章 リスクマネジメント

【参照：テキスト19-2-11.】
第19章 – 26

訴求ポイント

章を通した気づき・学び

- リスクマネジメントはセキュリティ対策に不可欠であるが、潜在的なリスクを考えるのが難しい場合がある。
- リスクマネジメントプロセスの各段階での考え方や手法を使用することで、リスクの特定、分析、対応策の検討を円滑に行うことができる。

認識していただきたい実施概要

- リスク対応にはリスクマネジメントプロセスにおけるリスクアセスメントが必要である。
- リスクアセスメントは「リスク特定」、「リスク分析」、「リスク評価」を実施する。
- リスク対応はリスクアセスメントの結果をもとに「リスク回避」、「リスク低減」、「リスク移転」、「リスク受容」から選択する。

第12章 具体的手順の作成 (LV.1 クイックアプローチ/LV2. ベースラインアプローチ)

【参照：テキスト19-2-12.】
第19章 – 27

内容

- 【LV.1 クイックアプローチ】【LV.2 ベースラインアプローチ】の概要
- 【LV.1 クイックアプローチ】セキュリティインシデント事例を参考とした実施手順
- 【LV.2 ベースラインアプローチ】ガイドラインを参考とした実施手順

主なキーワード

- クイックアプローチ
- ベースラインアプローチ

第12章 具体的手順の作成 (LV.1 クイックアプローチ/LV2. ベースラインアプローチ)

【参照：テキスト19-2-12.】
第19章 – 27

全体概要

- クイックアプローチ：実際のセキュリティインシデントの事例に基づいて対策基準や手順を策定するアプローチ。
- ベースラインアプローチ：既存のガイドラインやひな形を参考にして対策基準や手順を策定するアプローチ。
- クイックアプローチは社会的に影響の大きい事案に向いており、ベースラインアプローチは適切な参考元があれば簡易な手順で策定できる。

【LV.1 クイックアプローチ】 【LV.2 ベースラインアプローチ】の概要

- セキュリティ対策基準と実施手順の策定は情報漏えいなどのリスク対策に役立つ。
- LV.1 クイックアプローチ：緊急事態に対応するための即時の対策基準と手順を策定するアプローチ。
- LV.2 ベースラインアプローチ：既存のガイドラインを参考にして対策基準と手順を策定するアプローチ。

第12章 具体的手順の作成 (LV.1 クイックアプローチ/LV2. ベースラインアプローチ)

【参照：テキスト19-2-12.】
第19章 – 28

【LV.1 クイックアプローチ】セキュリティインシデント事例を参考とした実施手順

- メリット
  - 小規模な対策や修正を迅速に実施可能。
  - 低コストでリスクを軽減。
- デメリット
  - 短期的な解決策に偏りがちになる。
  - セキュリティインシデント事例ごとに策定するため、網羅性は低い。

【LV.2 ベースラインアプローチ】ガイドラインを参考とした実施手順

- メリット
  - 組織全体で一貫性を確保できる。
  - 最低限実施すべきセキュリティ対策を講じることができる。
- デメリット
  - セキュリティ対策やリスクに対する適切な対応策を検討する必要がある。
  - ガイドラインやひな形は一般的な組織を想定したもので、自社の状況に合わせて検討する必要がある。

第12章 具体的手順の作成 (LV.1 クイックアプローチ/LV2. ベースラインアプローチ)

【参照：テキスト19-2-12.】
第19章 – 28

訴求ポイント

章を通した気づき・学び

- 緊急性や即効性が必要な場合はクイックアプローチやベースラインアプローチが適している。
- 対策を検討する余裕がある場合、網羅的アプローチが重要である。

認識していただきたい実施概要

- クイックアプローチ：実際のセキュリティインシデントに基づいて発生可能性や被害規模を考慮し、社会的影響の大きいまたは緊急性の高い事象に対策を取りやすいアプローチ。
- ベースラインアプローチ：既存の手法を参考にして自社に適した対策基準や実施手順を簡易に策定できるアプローチ。

第13章 ISMSの要求事項と構築 (LV3. 網羅的アプローチ)

【参照：テキスト19-2-13.】
第19章 – 29

内容

- 【LV.3 網羅的アプローチ】の概要
- 【LV.3 網羅的アプローチ】フレームワークを参考とした実施手順

主なキーワード

- 網羅的アプローチ
- PDCAサイクル

第13章 ISMSの要求事項と構築 (LV3. 網羅的アプローチ)

【参照：テキスト19-2-13.】
第19章 – 29

全体概要

- 網羅的アプローチ：ISMSなどのフレームワークを使用して高いセキュリティ対策を策定する方法。時間がかかるが高いセキュリティレベルを確保できる。
- 緊急性や即効性が必要な場合はクイックアプローチやベースラインアプローチが適しているが、余裕がある場合は網羅的アプローチが推奨される。

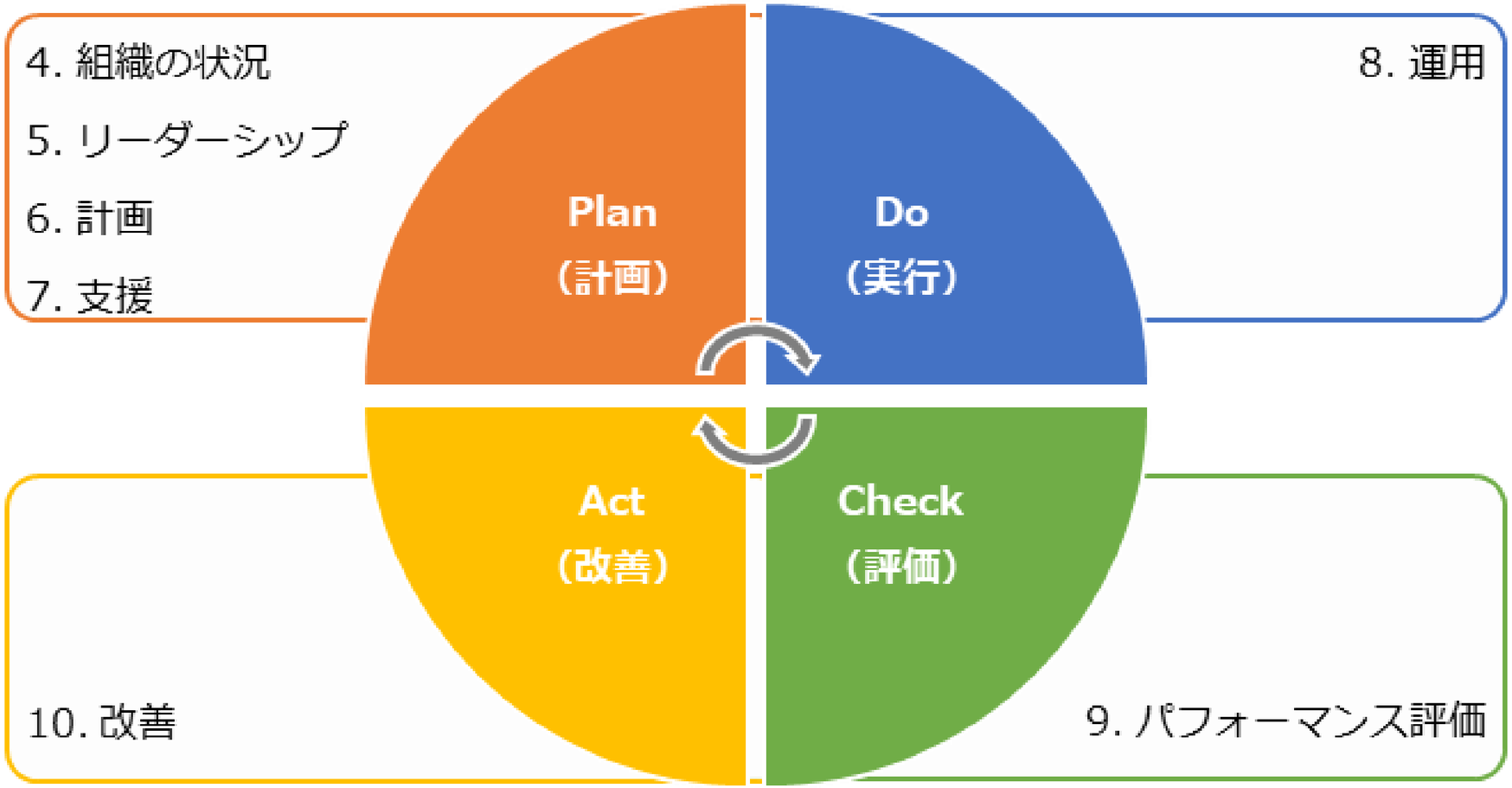
【LV.3 網羅的アプローチ】の概要

- 網羅的アプローチではISMSを使用してセキュリティ対策基準と実施手順を体系的に作成する。
- ISMSに従うため、技術的対策だけでなく運用や監査にも対策を含める。
- 網羅的アプローチのメリットはISMS要求事項の導入が可能で、デメリットは時間とコストがかかること。

第13章 ISMSの要求事項と構築 (LV3. 網羅的アプローチ)

【参照：テキスト19-2-13.】
第19章 – 30

【LV.3 網羅的アプローチ】フレームワークを参考とした実施手順



第13章 ISMSの要求事項と構築 (LV3. 網羅的アプローチ)

【参照：テキスト19-2-13.】
第19章 – 30

訴求ポイント

章を通した気づき・学び

- ISMSを使用した網羅的アプローチは、セキュリティ対策だけでなくISMS自体を改善し、自社に適した対策を継続的に検討することができる。

認識していただきたい実施概要

- 「4. 組織の状況」から「10. 改善」までの7項目で必要なドキュメントの作成手順を理解すること。
- ISMSマネジメントプロセスを取り込み、PDCAサイクルを回すこと。

第14～17章 ○○管理策

【参照：テキスト19-2-14～17.】
第19章 – 31～38

内容

- 4種類の管理策を参考とした対策基準・実施手順の策定

主なキーワード

- 組織的管理策
- 人的管理策
- 物理的管理策
- 技術的管理策

全体概要

- 対策基準の策定にはISO/IEC 27001:2022附属書Aの合計93項目の管理策を参考にできる。
- それぞれの管理策を参考に、対策基準を策定する手順と実施手順の例について説明。

第14～17章 ○○管理策

【参照：テキスト19-2-14～17.】
第19章 – 31～38

4種類の管理策を参考とした対策基準・実施手順の策定

対策基準の策定

- ISO/IEC 27001:2022附属書Aの管理策（93項目）を参考にして対策基準を策定する。
- リスクアセスメントの結果に基づいて適切な管理策を選択し、それを対策基準とする。
- 対策基準は基本方針と一緒に公開可能なものとして作成する。
- ISMSに基づく管理策を使用して対策基準を策定する際には、ISO/IEC 27001:2022の文献を参照する。

実施手順の策定

- 管理策（対策基準）に基づいてセキュリティ対策の実施手順の例を紹介。
- 実施手順は組織内の文書として作成され、具体的で理解しやすい内容である必要がある。
- ISO/IEC 27002の各管理策の手引きを参考に実施手順の例を紹介。自社に適した実施手順を策定することが重要。

第14～17章 ○○管理策

【参照：テキスト19-2-14～17.】
第19章 – 31～38

訴求ポイント

章を通した気づき・学び

- ISO/IEC 27002を参考にして管理策の対策基準と実施手順を決定することが重要。
- ドキュメントの作成と更新は大切だが、本来の目標は効果的な情報セキュリティ対策を計画し実行することである。

認識していただきたい実施概要

- リスクアセスメントの結果に基づいて管理策を選択し、対策基準を策定する。
- 対策基準は基本方針と一緒に公開可能なものとして作成する。
- 決定した対策基準に基づいて実施手順を策定する。
- 実施手順は従業員に対してわかりやすく内部文書として作成する。

第18章 セキュリティ対策状況の有効性評価

【参照：テキスト19-2-18.】
第19章 – 39

内容

- 内部監査・外部監査

主なキーワード

- 内部監査
- 外部監査

全体概要

- セキュリティ対策の有効性評価として、内部監査と外部監査が行われる。
- 内部監査は自社で規定した要求事項を満たし、業務がルールに従って実施されているかをチェックする。
- 外部監査は第三者が企業の情報資産を保護する体制や環境が整っているかをチェックする。

第18章 セキュリティ対策状況の有効性評価

【参照：テキスト19-2-18.】
第19章 – 39

訴求ポイント

章を通した気づき・学び

- 企業や組織はセキュリティ対策の有効性評価として内部・外部監査を定期的に実施する必要がある。

認識していただきたい実施概要

- 外部監査は第三者視点で情報資産の保護体制をチェックし、顧客や取引先にセキュリティ対策の信頼性を示す役割がある。
- 内部監査はセキュリティのルールや文書の適切性をチェックし、形骸化や目的の喪失を防ぐ役割がある。

今後のアクション

【参照：テキスト19-3-1.】
第19章 – 40

本テキストの内容を実践するために行うべき事項

**テキストに記載された各章の理解を深め、
経営者を含めた関係者と共有すること**

- 各章のポイントの理解
- DX推進の考え方の把握
- セキュリティ対策全容の認識
- 自組織でのセキュリティ対策の実施項目の認識

1. リスクアセスメントによって自組織の現状のリスクを把握する。
2. リスクアセスメントの結果を踏まえ、管理策の中から自組織として実施すべき項目を選定する。
3. 実施する管理策に関して、自組織としての実施手順を策定する。

今後のアクション

【参照：テキスト19-3-1.】
第19章 – 41

経営者のリーダーシップによって、社内体制を整備すること

- 実施手順の実践準備
- 実施手順の実践
  1. 組織体制と役割の決定
  2. 年間を通して実践すべき事項の例示

- リスクアセスメントの実施、リスク対応のための計画作成、管理策の検討
- 資産台帳の見直し
- 事業継続に関する試験
- 内部監査
- マネジメントレビュー
- 不適合及び是正処置のレビュー
- 定期教育
- 外部審査
- 情報セキュリティのための方針群のレビュー
- 秘密保持契約書の確認
- 「関係当局との連絡」体制の見直し
- 法令規制一覧表の確認
- 運用チェックリストによる確認
- 入退記録の確認
- など

実施するための年間計画を作成する

今後のアクション

【参照：テキスト19-3-1.】
第19章 – 43

管理策を実践するための参考となる情報

- ISO/IEC 27002:2022対応 情報セキュリティ管理策実践ガイド
- ISMS推進マニュアル – 活用ガイドブック ISO/IEC 27001:2022対応
- JISC「JIS Q 27000 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」
- ISO/IEC 27002:2022

取組み例

対策基準（例）	5.2 情報セキュリティの役割及び責任	5.5 関係当局との連絡	6.7 リモートワーク	8.15 ログ取得
実施手順（例）	情報セキュリティ委員会を設置する。	関係当局およびその連絡先を「連絡先一覧表」に特定し、必要時に容易に連絡がとれる体制を確立・維持する。	社内ネットワークへはVPNにて接続する。	バックアップが確実に行われており、障害時に復元が可能かどうかを月に1度チェックする。
トップマネジメント（経営層）	○	－	○	－
情報セキュリティ委員会	－	○	○	－
情報システム管理者	－	－	○	○
一般社員	－	-	○	－

今後のアクション

【参照：テキスト19-3-1.】
第19章 – 44

継続的な情報収集

- 国の方針、社会の現状と今後の動向
- IT活用事例
- セキュリティインシデント事例

人材育成

- DSSに基づく人材育成
- プラス・セキュリティ人材の育成

令和5年度
中小企業サイバーセキュリティ対策
継続支援事業