

令和6年度 中小企業サイバーセキュリティ 社内体制整備事業

第1回

第1編：サイバーセキュリティを取り巻く背景

第2編：中小企業に求められるサイバーセキュリティ対策



講師紹介



氏名	星野 樹昭（ほしの しげあき）
業務経歴	26年（セキュリティ経験：20年）
専門分野	ITインフラ設計 / 構築 / テスト 移行設計 セキュリティ製品導入支援 ISMS導入支援
保有資格	情報処理安全確保支援士（登録番号 第002047号） CISSP MCP
コメント	官公庁や金融機関などの大規模環境から、中小零細企業規模まで、オンプレ/クラウド問わず様々な環境のITインフラ環境導入・移行の経験あり。 セキュリティ製品の導入支援では、DB暗号化ソフトウェアやWeb Application Firewall、クライアントPCのセキュリティ対応など、実績豊富。 現在はISMSコンサルも実施しており、活動は多岐にわたる。

目的

- 継続的なセキュリティ対策の実施を支援する。
- 人材の育成と実践的な課題解決を通じて、サプライチェーン全体のセキュリティ強化を図る。

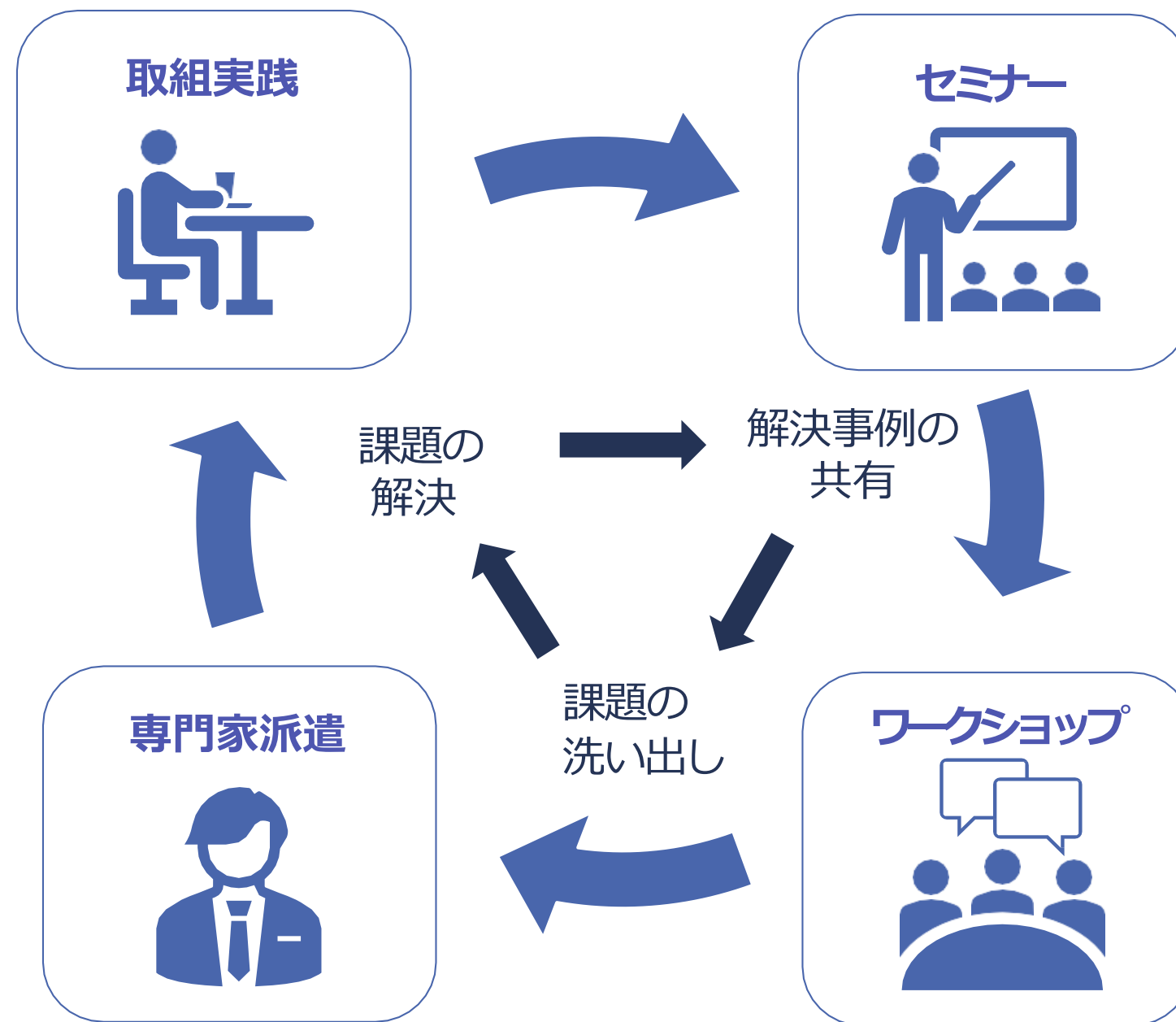
東京都他事業と本事業の位置づけ

成熟度レベル ※COBITを援用し設定	0	1	2	3	4	5
事業と主な支援領域 ステータス	セキュリティ意識もなく、対策等も考えていない状態	セキュリティ対策をしたいが、何から始めたらよいかわからない状態	基本的な対策をしているが、次に何をしたらよいかわからない状態	セキュリティマネジメント計画や行動を決め、実践している状態	リスクを分析し、方針・ルール・対策の見直しを行っている状態	常に改善と効果の最大化に取り組んでいる状態
中小企業サイバーセキュリティの極意	→					
中小企業サイバーセキュリティ普及啓発事業	→					
中小企業サイバーセキュリティ基本対策事業	→					
中小企業サイバーセキュリティ社内体制整備事業 (本事業)	→					
中小企業サイバーセキュリティ特別支援事業	→					
Tcyss (東京中小企業サイバーセキュリティ支援ネットワーク)	→					
サイバーセキュリティ対策促進助成金	→					

支援内容

セミナーで得た知見やワークショップの事例を参考に、専門家と決めた取組を実践します。不明点や不安点などは、コミュニティを通して質問を行い、専門家だけでなく、参加企業同士でフォローします。

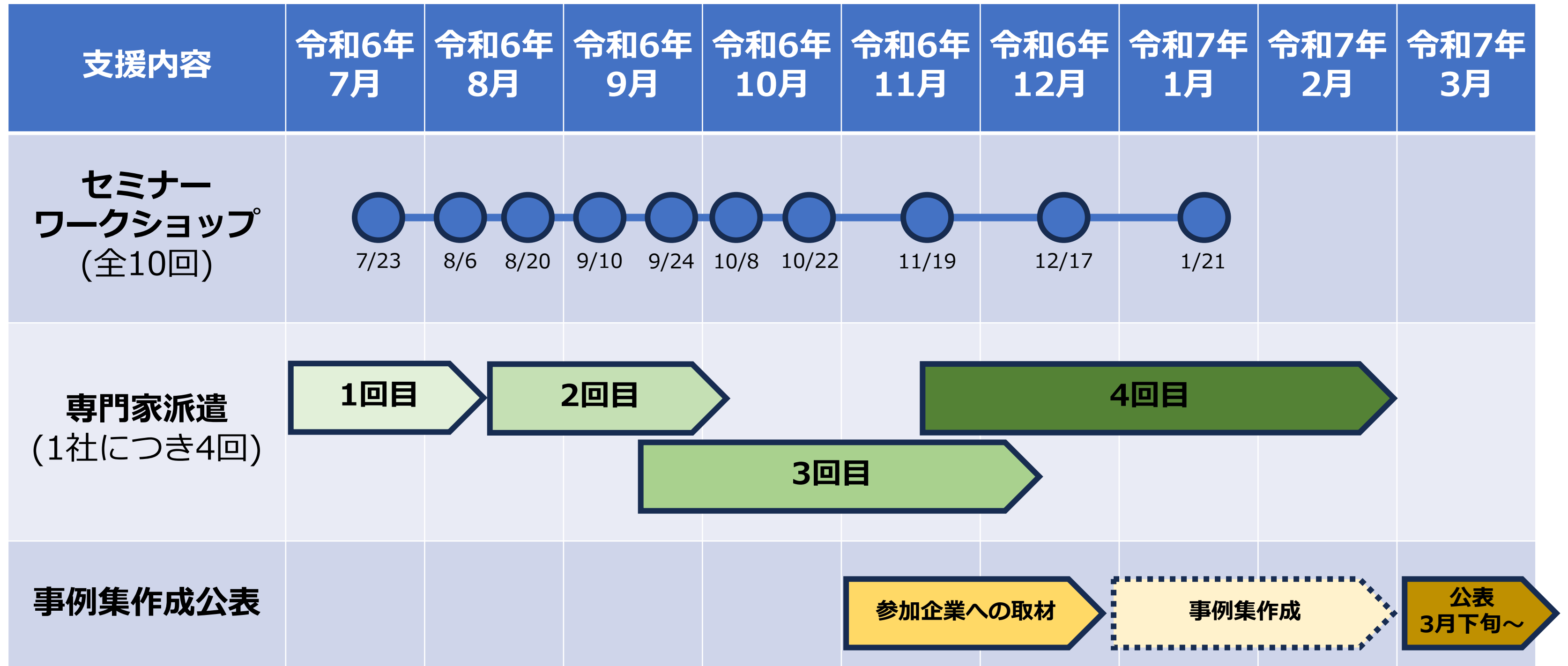
ワークショップで洗い出した課題やセミナー・ワークショップの気づきをもとに、企業が直面しているセキュリティ上の問題点解決や、社内体制構築へ向けた支援を行います。



導入済みのセキュリティ機器の日常的な運用方法や、業務内容に沿ったセキュリティルールの策定方法など、中小企業の皆様が自主的にセキュリティ対策業務を運営する上で生じる疑問点の解決に直接役立つ、実践的な知識・ノウハウを講義形式でお伝えします。

参加企業の皆様同士で、それぞれの課題と一緒に取組み、解決策を考えます。自社の問題だけでなく、他社の事例に触れることで、様々な課題の解決に向けた引き出しとなる知識を得られます。

スケジュール



セミナー内容

編	テーマ
第1編	サイバーセキュリティを取り巻く背景
第2編	中小企業に求められるデジタル化の推進とサイバーセキュリティ対策
第3編	これからの企業経営で必要なIT活用とサイバーセキュリティ対策
第4編	セキュリティ事象に対応して組織として対策すべき対策基準と具体的な実施
第5編	各種ガイドラインを参考にした対策の実施

セミナー内容

編	テーマ
第6編	ISMS等のフレームワークの種類と活用法の紹介
第7編	ISMSの構築と対策基準の策定と実施手順
第8編	具体的な構築・運用の実践
第9編	中小企業が組織として実践するためのスキル・知識と人材育成
第10編	全体総括

セミナー内容

第0章. テキストの活用

第1章. デジタル時代の社会とIT情勢

第2章. サイバーセキュリティの基礎知識

第3章. デジタル社会の方向性と実現に向けた国の方針

第4章. サイバーセキュリティ戦略及び関連法令

第5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

**第6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**

第0章. テキストの活用

テキストの目的、想定読者、全体構成、テキストの利用方法など

テキストの目的、想定読者、全体構成、テキストの利用方法など

【参照：テキスト0-1-1.】
P5

テキストの目的、想定読者

- 目的
中小企業がサイバーセキュリティの重要性と対策について理解を深めるための情報を提供します。
- 中小企業の現状
 - セキュリティ対策のリソースが限られ、大企業よりもサイバー犯罪者に狙われやすい。
 - フィッシング攻撃やランサムウェア攻撃の頻度が増加している。
 - 攻撃により業務停止や経済的損失、企業の信頼・ブランド価値への影響が懸念される。
- 想定読者
中小企業の経営者やIT担当者。

テキストの目的、想定読者、全体構成、テキストの利用方法など

【参照：テキスト0-1-2.】
P5

全体構成

- 本書の構成
 - サイバー攻撃の脅威や実際の被害事例を通じてリスク認識を深める。
 - ITおよびセキュリティの基礎知識と対策の要点を解説。
 - 政府や業界団体の取組、最新の技術やトレンドについて詳しく解説し、対応力を向上させる。
 - 中小企業におけるIT・セキュリティの課題に焦点を当て、具体的な解決策を提示。
 - ISMS認証などのフレームワークの習得、組織内でのセキュリティ管理体制の構築や認証取得の手順を解説。

テキストの目的、想定読者、全体構成、テキストの利用方法など

【参照：テキスト0-1-2.】
P5

全体構成

- 第4章以降では、セキュリティ対策をレベル分けして説明。
 - レベル1：緊急性の高い事例への対処法を解説。
 - レベル2：ガイドラインを用いて、組織全体で最低限実施すべきセキュリティ対策を解説。
 - レベル3：セキュリティフレームワークを用いて、より多くの攻撃手法に網羅的に対応するための事項を説明。
- セキュリティ対策を実施するための知識やスキル、人材の育成や確保について実践的な知識を提供。

テキストの目的、想定読者、全体構成、テキストの利用方法など

【参照：テキスト0-1-3.】
P6, P7

テキストの利用方法

経営層

- 組織として実践すべき事項と概要を知りたい。

システム管理担当者層

- セキュリティに関する動向を知りたい。
- 中小企業に必要な事項を知りたい。
- セキュリティ対策の具体的な手順を知りたい。

現在の対策状況

- 緊急に、大きなセキュリティホールを塞ぎたい。
- 素早く、多くのセキュリティホールを塞ぎたい。
- じっくり、小さなセキュリティホールも残さないように塞ぎたい。

第1章. デジタル時代の社会とIT情勢

デジタル時代の社会変革とIT情勢の関係性

デジタル時代の社会変革とIT情勢の関係性

【参照：テキスト1-1】
P9

社会の現状と今後の動向

- Society5.0とは
「サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）」

内閣府. “Society 5.0” https://www8.cao.go.jp/cstp/society5_0/, (参照 2023-07-06)

- Society1.0 : 狩猟社会
- Society2.0 : 農耕社会
- Society3.0 : 工業社会
- Society4.0 : 情報社会
- Society5.0 : 未来社会

https://wwwc.cao.go.jp/lib_006/society5_0/society5_0_mirai1.html

Society5.0 ビックデータ連携がもたらす未来社会像

https://wwwc.cao.go.jp/lib_006/society5_0/society5_0_bigdata1.html

デジタル時代の社会変革とIT情勢の関係性

デジタルトランスフォーメーション(DX)とは

【参照：テキスト1-1】
P10

定義

「DXとは、企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること。」

経済産業省. “デジタルガバナンス・コード2.0” https://www.meti.go.jp/policy/it_policy/investment/dgc/dgc2.pdf , (2023-07-06)

概要

- DXは、データやデジタル技術を使って新たな価値を生み出すこと。
- DXには、ビジネスモデルや企業文化の変革が必要。
- DX戦略では、経営ビジョンを描き、関係者を巻き込んで課題を解決する。
- DXは「知識」、「人材」、「**セキュリティ**」が重要な要素。

デジタル時代の社会変革とIT情勢の関係性

デジタルトランスフォーメーション(DX)とは

【参照：テキスト1-1】
P10

DXに必要な3要素

知識

- ITの基礎知識
- データサイエンスの知識
- AI・ブロックチェーンなどの最新の知識

人材

- 業務内容に精通
- 要件を実現させるために、新たな技術・手法を用いることができる

セキュリティ

- リモートワークのためのセキュリティ
- クラウドサービスを利用するためのセキュリティ

デジタル時代の社会変革とIT情勢の関係性

【参照：テキスト1-1】

P10, P11

生成AIとは

概要

- 既存のデータを解析・学習して新しいコンテンツを生成するAI。
- ディープラーニングを用いてテキスト、画像、音楽、映像などを作り出す。
- 従来のAIは大量の学習データをもとに結果を予測し行動を自動化していた。
- 新しい情報やデータから独自のコンテンツを生み出すことができる。

活用

- 生成AIを用いたチャットボットが24時間365日対応している。
- 広告制作では、バナーやプロモーション用のビジュアルを迅速に、かつ短時間で何種類も生成できる。
- 多くの業務プロセスを効率化できる。

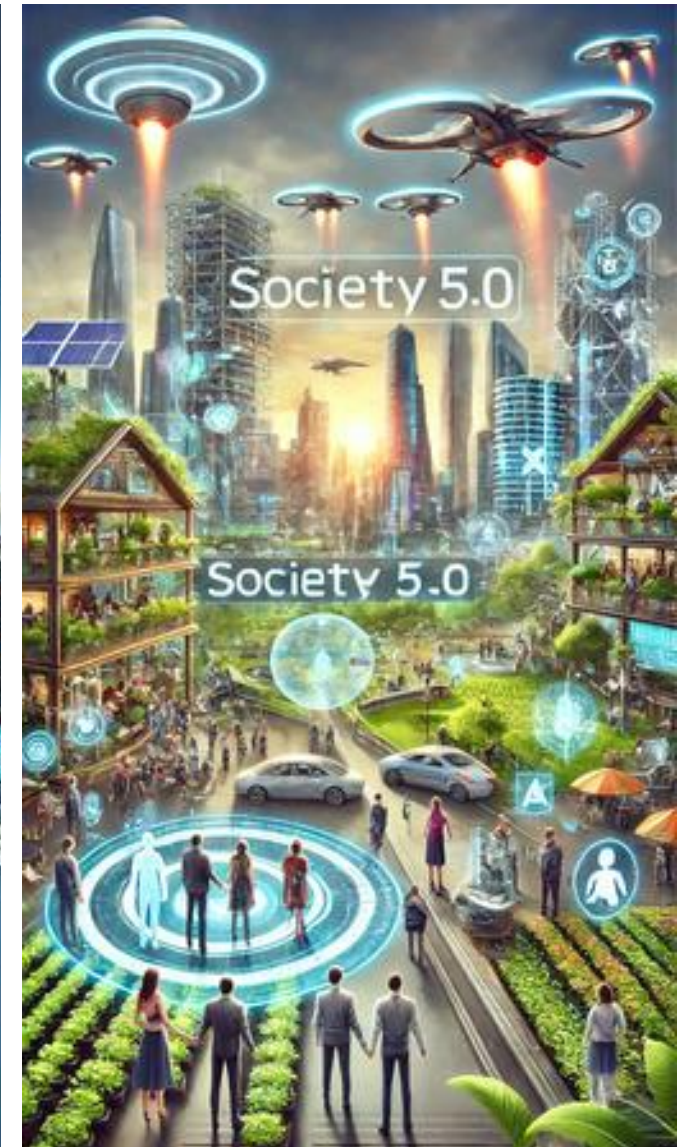
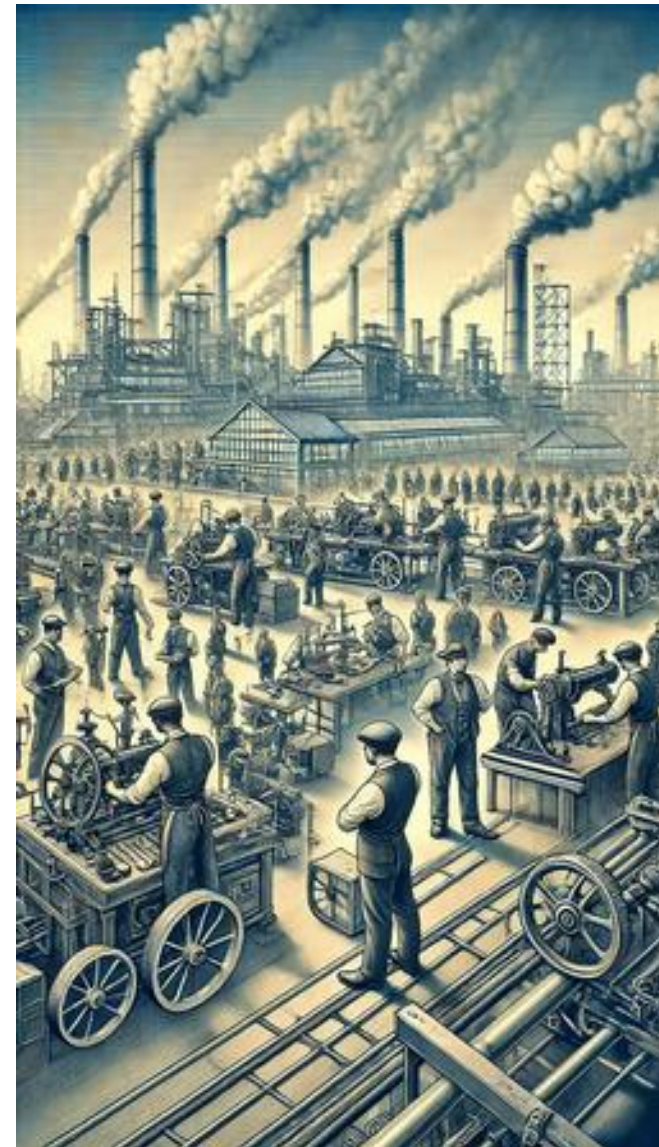
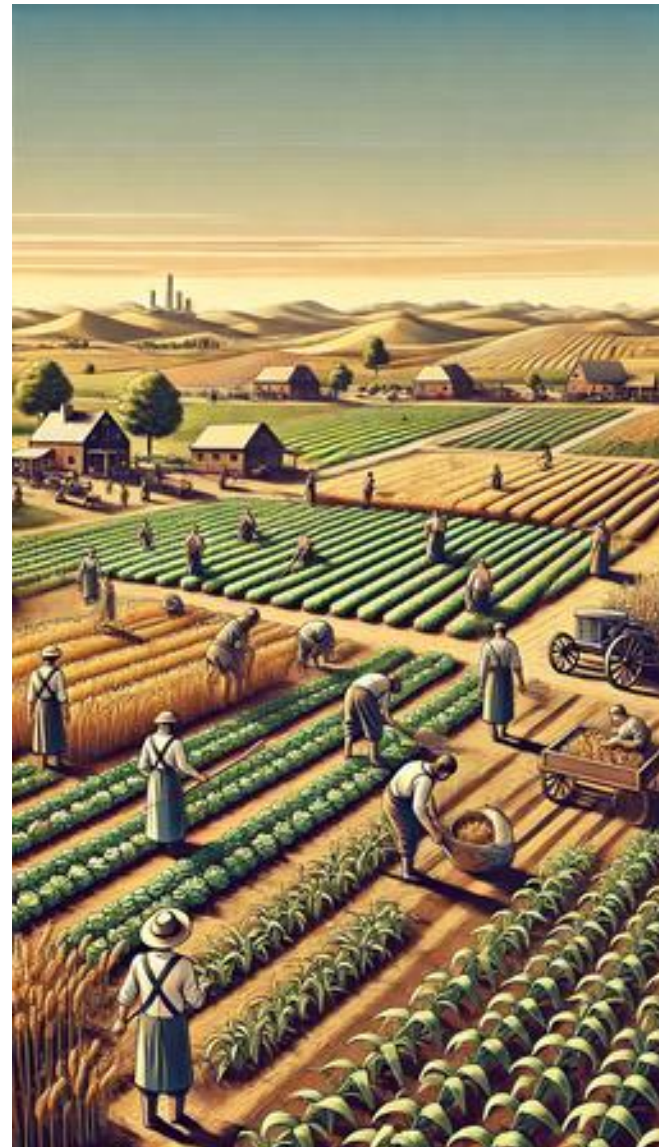
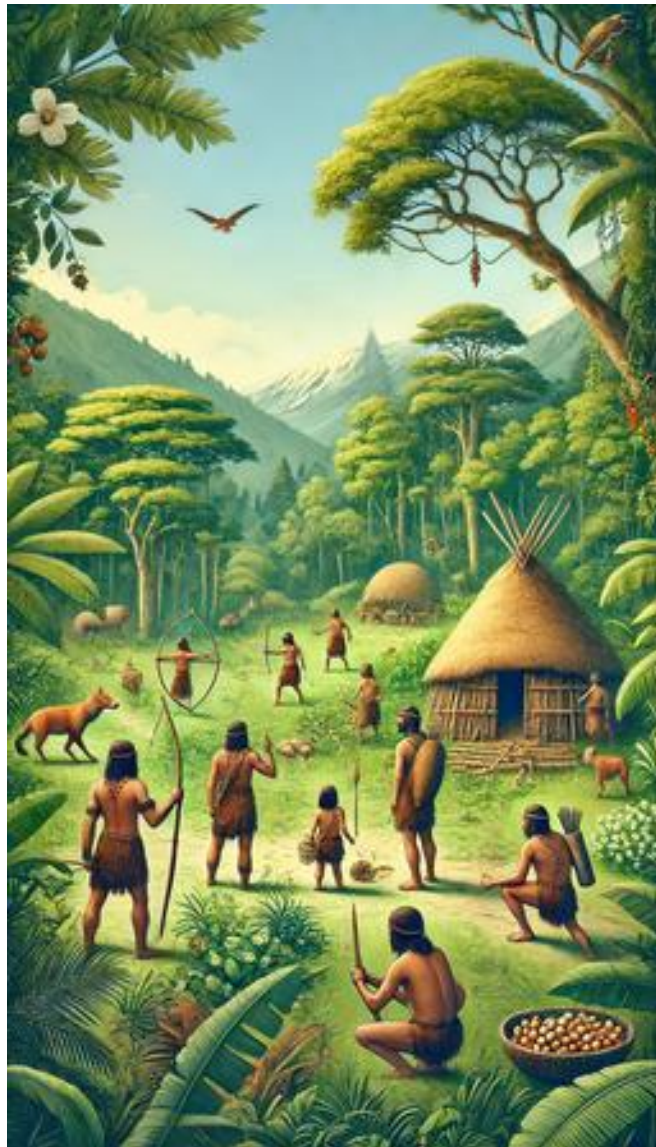
デジタル時代の社会変革とIT情勢の関係性

【参照：テキスト1-1】
P10, P11

生成AIとは

使用例

例えば、Society1.0~5.0のイメージを描かせると、こんな感じ。



第2章. サイバーセキュリティの基礎知識

導入済みと想定するセキュリティ対策機能

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

導入済みと想定するセキュリティ対策機能

【参照：テキスト2-1.】
P13

UTMとEDRについて

UTM (Unified Threat Management)

- UTM (統合脅威管理) は複数のセキュリティ機能を一つの機器に集約するシステム
- ネットワーク全体のトラフィックを監視・管理する
- ファイアウォール、侵入検知システム、ウイルス対策などが統合されている
- 外部からの侵入や攻撃を防御する
- 企業や組織内のネットワークセキュリティ対策として有効

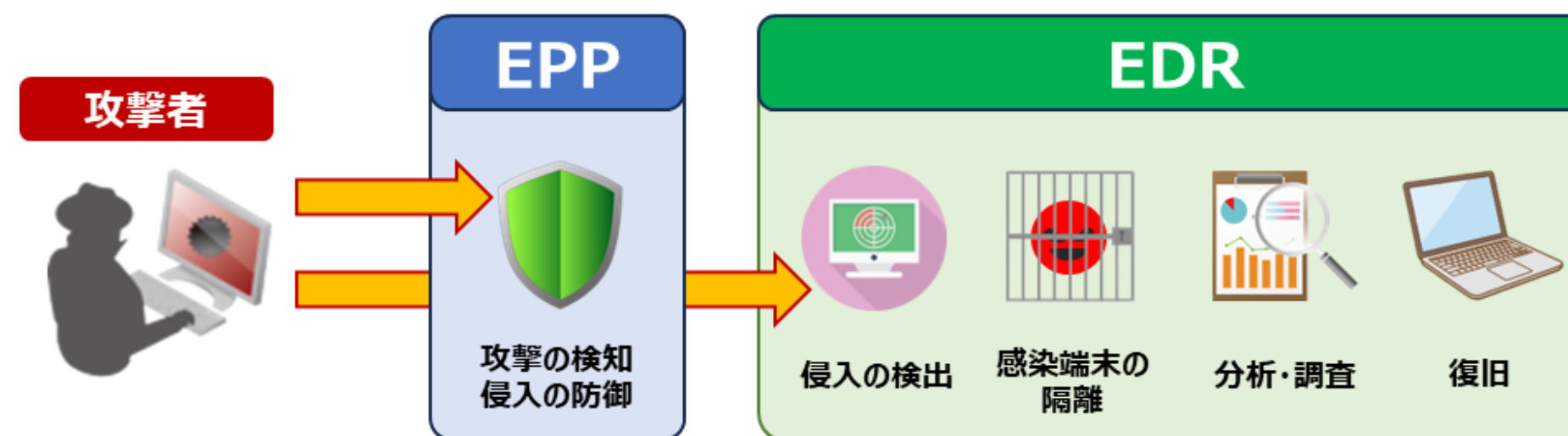
導入済みと想定するセキュリティ対策機能

【参照：テキスト2-1.】
P13

UTMとEDRについて

EDR (Endpoint Detection and Response)



- EDRはエンドポイント（PC、サーバなど）での脅威の検知と対応を可能にする
- 従来のアンチウイルスソフトでは検知できないマルウェアも検知可能
- エンドポイント上の不審な動作を検知する
- 検知した脅威に対して、悪意のあるプロセスの終了や感染したエンドポイントの隔離などの対応を行う
- EDRを活用することでセキュリティインシデントの早期発見と迅速な対応が可能になる



SECURITY ACTION 二つ星レベル

【参照：テキスト2-2-1.】
P14

レベルごとの宣言内容

レベル	宣言内容	ロゴマーク
★ 一つ星	「情報セキュリティ5か条」に取り組むことを宣言する	 <p>サンプル SECURITY ACTION ★ セキュリティ対策自己宣言</p>
★★ 二つ星	<ol style="list-style-type: none"> 「5分でできる！情報セキュリティ自社診断」で自社のセキュリティ対応状況を把握する 情報セキュリティ方針を策定する 外部に公開したことを宣言する 	 <p>サンプル SECURITY ACTION ★★ セキュリティ対策自己宣言</p>

IPA. "SECURITY ACTION セキュリティ対策自己宣言". <https://www.ipa.go.jp/security/security-action>

SECURITY ACTION 二つ星レベル

宣言プロセス

【参照：テキスト2-2-1.】
P14

概要	詳細
1. 使用規約を確認	「ロゴマーク使用規約確認」にて規約を確認する。
2. 必要事項を入力	「事業者情報入力」、「自己宣言入力」それぞれの画面で必要事項を入力する。
3. 確認メールを受信	「自己宣言受付確認のお知らせ」メールを受信する。 メール本文中のURLをクリックする。
4. 自己宣言IDのお知らせ	「自己宣言完了のお知らせ」メールにて、ログインに利用する自己宣言IDが通知される。
5. ロゴマークダウンロード	自己宣言完了後、1～2週間程度でロゴマークのダウンロードに必要な手順が、メールで通知される。

SECURITY ACTION 一つ星

情報セキュリティ5か条

【参照：テキスト2-2-2.】
P15

1. OSやソフトウェアは常に最新の状態にしよう！
2. ウイルス対策ソフトを導入しよう！
3. パスワードを強化しよう！
4. 共有設定を見直そう！
5. 脅威や攻撃の手口を知ろう！

SECURITY ACTION 二つ星

【参照：テキスト2-2-3.】
P16

情報セキュリティ自社診断

自社のセキュリティ対策がどれくらい実施できているかを把握するための診断ツール。25項目の設問に答えるだけで診断できる。

分類

パート	内容
Part1 基本的対策	No.1~5は企業の規模や形態を問わず、必須の5項目。
Part2 従業員としての対策	No.6~18は従業員として注目すべき項目。
Part3 組織としての対策	No.19~25は組織としての方針を定めた上で、実施すべきセキュリティ対策。

SECURITY ACTION 二つ星

情報セキュリティ自社診断

【参照：テキスト2-2-3.】
P16

診断方法

- 経営者またはシステム担当や部門長など、実施状況を把握している人が記入する。
- 一人で記入が難しい場合は、事業所、部署ごとに記入し、責任者・担当者が集計する。

点数

項目	点数
実施している	4点
一部実施している	2点
実施していない	0点
わからない	-1点

情報セキュリティ自社診断

5分でできる！情報セキュリティ自社診断とは 判定

【参照：テキスト2-2-3.】
P16, P17

合計得点	現在の状況	次の対策
100 点満点	入門レベルのセキュリティ対策は達成	さらに強化
70～99点	部分的に対策が不十分	100点満点への挑戦
50～69点	対策が不十分	低い項目から改善
49点以下	事故がいつ起きても不思議ではない	早急に改善

情報セキュリティ基本方針

【参照：テキスト2-2-4.】
P18

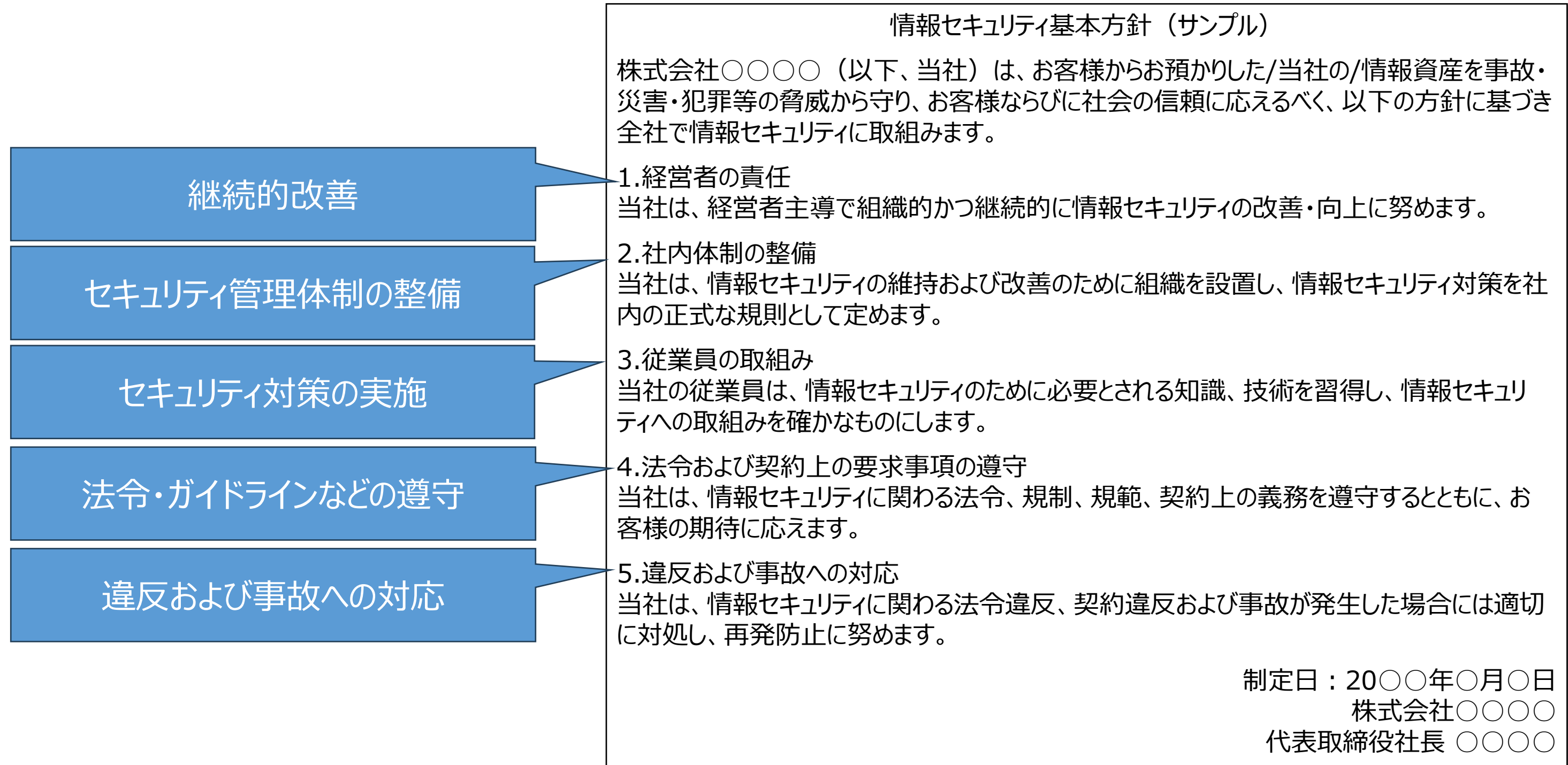
情報セキュリティ基本方針とは

- 経営者が情報セキュリティに関する基本方針を策定する。
- 従業員や関係者に基本方針を伝達するため、簡潔な文書を作成する。
- 基本方針の作成には特定の書き方が定められていない。
- 事業の特徴や顧客の期待を考慮して基本方針を策定する。
- 経営者と連携し、自社に適した基本方針を策定する。

情報セキュリティ基本方針

記載内容

【参照：テキスト2-2-4.】
P18, P19



サイバーセキュリティアプローチ方法

対策基準レベルの概要

【参照：テキスト2-3.】
P20

レベル	概要
Lv.1 クイック アプローチ	緊急に、狙われやすい大きな穴（セキュリティホール）を塞ぐ
Lv.2 ベースライン アプローチ	素早く多くの穴を塞ぐ
Lv.3 網羅的 アプローチ	じっくりと、小さな穴を残さないように確実に塞ぐ

第3章. デジタル社会の方向性と実現に向けた国の方針

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

国の基本方針および実施計画の要約

【参照：テキスト3-1.】
P23

5つのAction

1. 物価上昇を上回る賃上げの定着
2. 構造的価格転嫁の実現
3. 成長分野への戦略的な投資
4. スタートアップネットワークの形成
5. 新技術の徹底した社会実装

5つのVison

1. 社会課題解決をエンジンとした生産性向上と成長機会の拡大
2. 誰もが活躍できるWell-beingが高い社会の実現
3. 経済・財政・社会保障の持続可能性の確保
4. 地域ごとの特性・成長資源を活かした持続可能な地域社会の形成
5. 海外の成長市場との連結性向上とエネルギー構造転換

国の基本方針および実施計画の要約

IT戦略に関係する施策例

- デジタル技術の活用
- デジタル・ガバメントの強化
- サイバーセキュリティの強化

【参照：テキスト3-1.】
P23, P24

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

デジタル社会の実現に向けた重点計画

【参照：テキスト3-2-1.】

P25, P26

デジタル社会で目指す6つの姿

1. デジタル化による成長戦略
2. 医療・教育・防災・こどもなどの準公共分野のデジタル化
3. デジタル化による地域の活性化
4. 誰一人取り残されないデジタル社会
5. デジタル人材の育成・確保
6. DFFT（Data Free Flow with Trust）：
「信頼性のある自由なデータ流通」の推進を始めとする国際戦略

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

デジタル社会の実現に向けた戦略・施策

【参照：テキスト3-2-1.】

P26, P27

目指す姿を実現する上で有効な戦略的取組（基本戦略）

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

サイバーセキュリティなどの安全・安心の確保

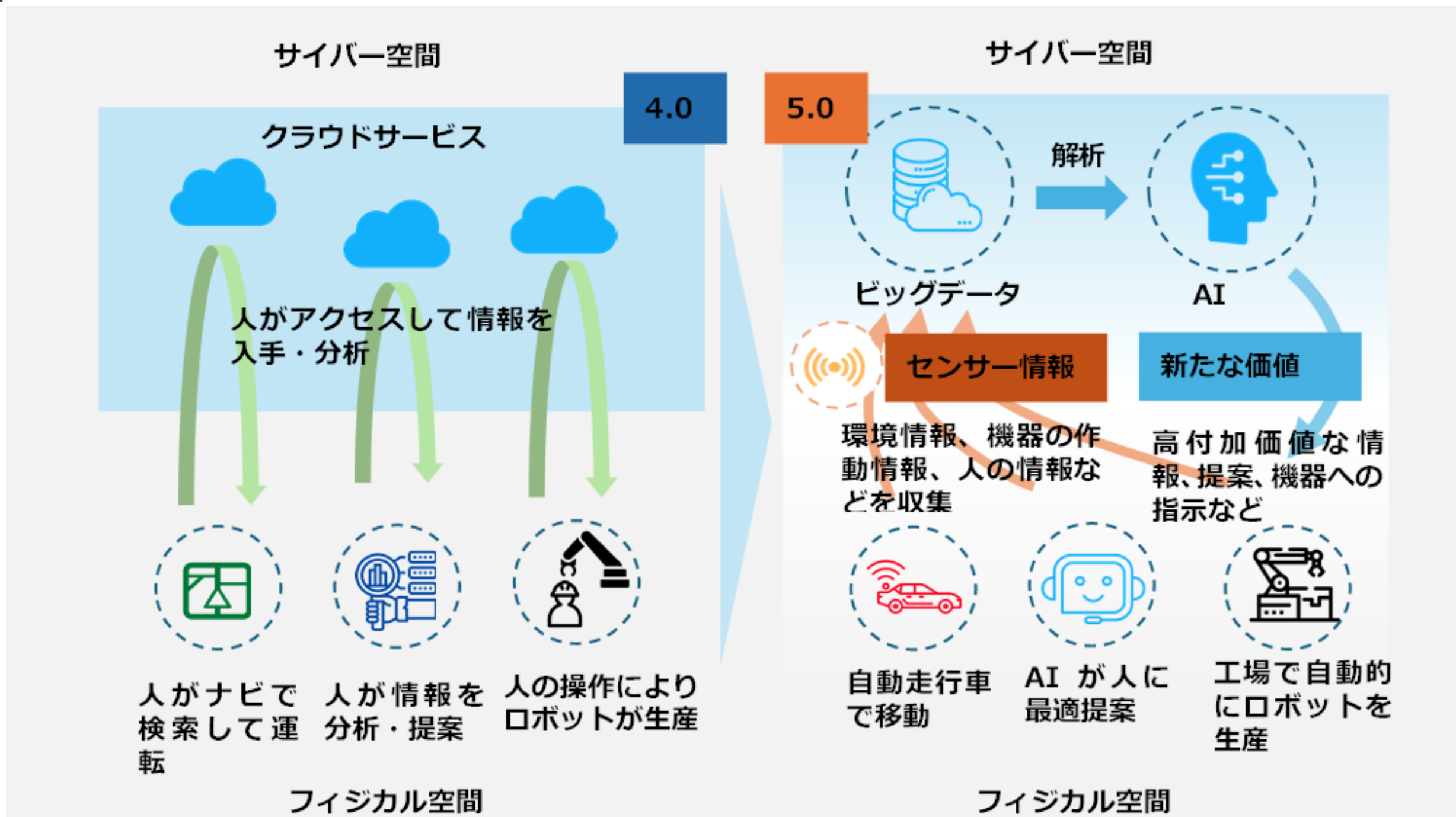
1. サイバーセキュリティの確保
2. 個人情報などの適正な取扱いの確保
3. 情報通信技術を用いた犯罪の防止
4. 高度情報通信ネットワークの災害対策

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

【参照：テキスト3-2-2.】
P27

Society 5.0

Society 4.0と5.0の比較



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

【参照：テキスト3-2-2.】
P28

Society 5.0

社会の変化に対するセキュリティ上の脅威

Society5.0における社会の変化	社会の変化に対するセキュリティ上の脅威
大量データの流通・連携	<ul style="list-style-type: none"> データの性質に応じた適切な管理の重要性が増大
フィジカル空間とサイバー空間の融合	<ul style="list-style-type: none"> サイバー空間からの攻撃がフィジカル空間まで到達 フィジカル空間から侵入してサイバー空間へ攻撃を仕掛けるケース フィジカル空間とサイバー空間の間における情報の転換作業への介入
複雑につながるサプライチェーン	<ul style="list-style-type: none"> サイバー攻撃による影響範囲が拡大

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

【参照：テキスト3-2-3.】
P29

DXの推進

中小企業がDX推進における優位な点

優位点	理由
参考情報が豊富	<ul style="list-style-type: none"> DXを既に手掛けている中小企業や、DXを順調に進めている企業のやり方を参考にすることができる
環境が整備されている	<ul style="list-style-type: none"> 先行者や大企業などにより既に整備されたプラットフォームを利用し、新たなビジネスに取り組むことができる
環境の変化に素早く対応しやすい	<ul style="list-style-type: none"> 経営者が即断即決し、新しい取組に臨みやすい利点がある。そのため、変革のスピードにおいて優位性を持つことができる

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

【参照：テキスト3-2-3.】
P30

DXの推進

データ活用の流れ

手順	概要
1. データの収取	IoTやセンサー、カメラなどの機器を用いて情報を収集する。
2. データの蓄積	収集した膨大なデータ（ビッグデータ）を集積する。
3. データの解析	AIを用いてデータを解析する。
4. 解析結果の反映	解析の結果を基に改革を進める。

DX with Cybersecurityの概要

- デジタル技術の利用拡大に伴い、セキュリティリスクが増大するため、セキュリティ対策の強化が求められる。
- セキュリティ対策はコストではなく、企業価値や競争力の向上に不可欠な要素として重要である。

第4章. サイバーセキュリティ戦略および関連法令

NISC : サイバーセキュリティ戦略

※NISC

(National center of Incident readiness and Strategy for Cybersecurity)

企業経営に重要なDX推進とセキュリティ確保の両立

関連法令

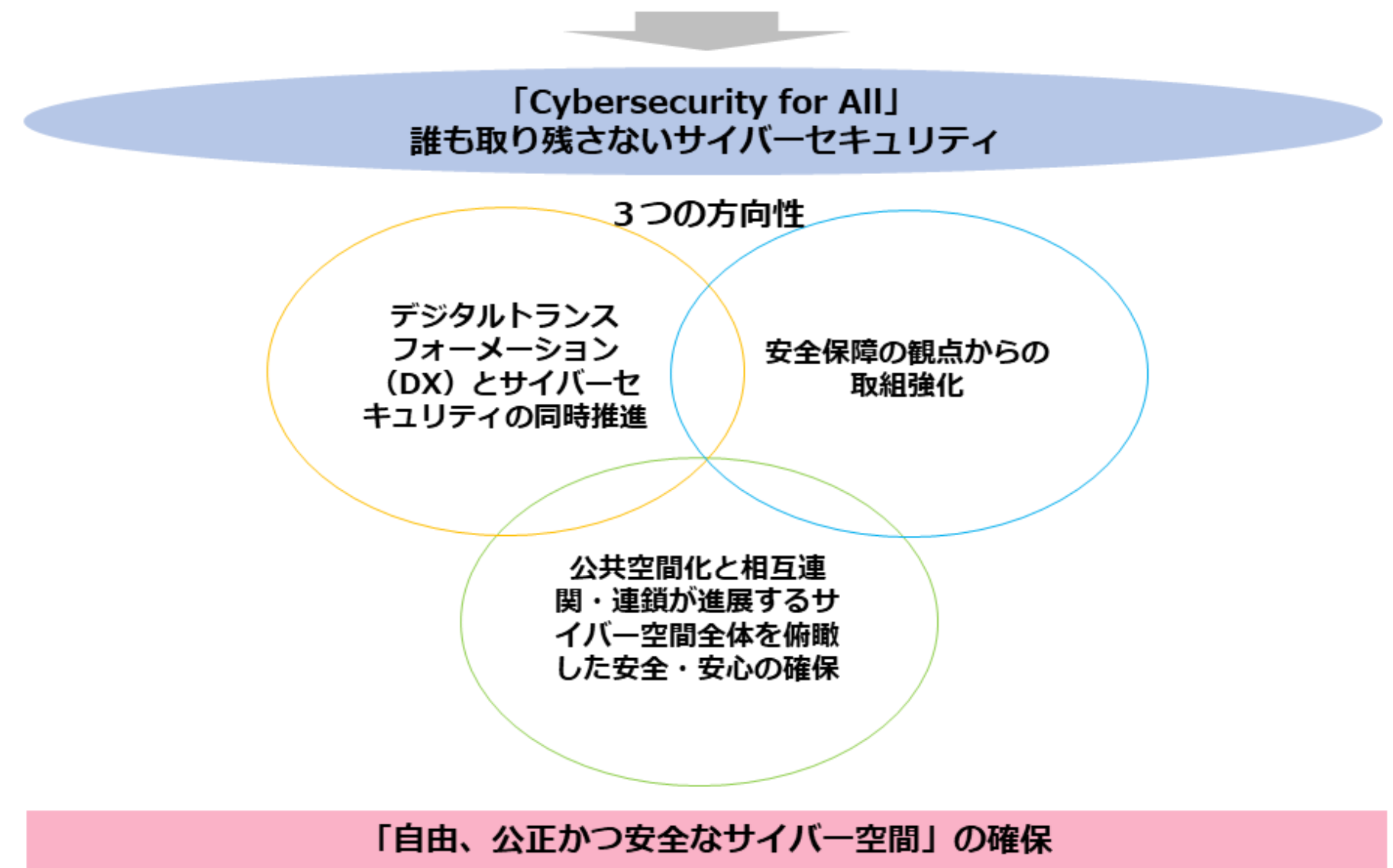
NISC : サイバーセキュリティ戦略

サイバーセキュリティ戦略の課題と方向性

【参照：テキスト4-1-1.】
P34

- サイバーセキュリティ戦略は、国家レベルでのサイバーセキュリティ確保の方針・目標を示す。
- デジタル化の進行とともに、すべての主体がサイバー空間に参加する動きがある。
- 「誰一人取り残さない」セキュリティ確保が必要。
- 戦略では、「自由、公正、かつ安全なサイバー空間」確保のため、3つの方向性をベースに施策推進の方針が示されている。

2020年代を迎えた日本を取り巻く時代認識：「ニューノーマル」とデジタル社会の到来
(デジタル改革の推進、新型コロナウイルスの影響、SDGsなど)
サイバー空間をとりまく課題認識：国民全体のサイバー空間への参画
(サイバー攻撃の巧妙化、サイバー空間の公共化、現実世界との相互連関など)



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の課題と方向性

【参照：テキスト4-1-1.】
P35, P36, P37, P38

3つの政策目標

「経済社会の活力の向上及び持続的発展」

「国民が安全で安心して暮らせるデジタル社会の実現」

「国際社会の平和、安定及び我が国の安全保障への寄与」

横断的施策

- 人材育成・確保・活躍推進
- 研究開発の推進
- 全員参加による協働・普及啓発

NISC : サイバーセキュリティ戦略

【参照：テキスト4-1-1.】
P38, P39

横断的施策

3つの政策目標を達成するために、横断的・中長期的な視点で取り組む施策。

研究開発

- 国際競争力の強化・産学官エコシステムの構築
- 実践的な研究開発の推進
- 中長期的な技術トレンドを視野に入れた対応

人材の確保・育成・活躍促進

- DX with Cybersecurityの推進
- 巧妙化・複雑化する脅威への対処
- 政府機関における取組

全員参加による協働・普及啓発

- ガイドラインやさまざまな解説資料などの整備の推進

NISC : サイバーセキュリティ戦略

【参照 : テキスト4-1-2.】
P39, P40

サイバーセキュリティ2023

サイバー空間を巡る状況変化と情勢、及び政策課題

- 昨今の状況変化
- サイバー空間の現下の情勢 ～サイバー攻撃の深刻化・巧妙化～
- 昨今の状況変化を踏まえた政策課題

今後の取組の方向性

1. 経済社会の活力の向上及び持続的発展
2. 国民が安心して暮らせるデジタル社会の実現
3. 国際社会の平和・安定及び我が国の安全保障への寄与

企業経営に重要なDX推進とセキュリティ確保の両立

企業経営のためのサイバーセキュリティの考え方

【参照：テキスト4-2-1.】
P41, P42

2つの基本的認識

1. 挑戦

サイバーセキュリティは、ビジネスの革新や新しい製品・サービス創出の一環として、利益を生み出す戦略として考慮すべきである。

2. 責任

つながる社会でのサイバーセキュリティへの取組は、社会の要求であり、自社だけでなく、全体の発展にも寄与する。

3つの留意事項

1. 情報発信による社会的評価の向上

2. リスクの一項目としてのサイバーセキュリティ

3. サプライチェーン全体でのサイバーセキュリティの確保

企業経営に重要なDX推進とセキュリティ確保の両立

サイバーセキュリティ対策の取組レベル

【参照：テキスト4-2-1.】
P42

レベル	分類	概要
理想的に	1	ITの利活用を事業戦略上に位置づけ、サイバーセキュリティを強く意識し、積極的にITによる革新と高いレベルのセキュリティに挑戦する企業
もっと積極的に	2	IT・サイバーセキュリティの重要性は理解しているものの、積極的な事業戦略としての組み込みはできていない企業
無駄な投資	3	過剰なセキュリティ意識により、ITの利活用を著しく制限し、競争力強化に活用させていない企業
危険	4	サイバーセキュリティ対策の必要性は理解しているが、必要十分なセキュリティ対策ができていないにもかかわらず、ITの利活用を進めている企業
	5	サイバーセキュリティの必要性を理解していない企業や、自らセキュリティ対策を行う上で事業上のリソースの制約が大きい企業
対象外	6	ITを利用していない企業

企業経営に重要なDX推進とセキュリティ確保の両立

【参照：テキスト4-2-2.】
P43

DX with Cybersecurity

DX with Cybersecurityの推進に向けた主な施策

分類	課題	施策
経営層の意識改革	経営層が主体性を持ってDXとサイバーセキュリティ対策に取り組むためには、専門家とのコミュニケーションが重要	経営者がITやセキュリティに関する専門知識を持っていない場合でも、セキュリティ専門家と協力し、「プラス・セキュリティ」知識を習得する環境を整備
地域・中小企業におけるDX with Cybersecurityの推進	中小企業は、セキュリティ対策に予算を割くことの必要性を理解する	中小企業が利用しやすい安価かつ効果的なセキュリティサービス・保険の普及など、中小企業向けセキュリティ施策を推進
新たな価値創出を支えるサプライチェーンなどの信頼性確保に向けた基盤づくり	サイバー攻撃の起点となり得る箇所拡大に伴う、リスク管理が重要	産業分野別、または産業横断的なガイドラインの策定や活用促進を通じて、産業界におけるセキュリティ対策の具体化・実装を促進

関連法令

個人情報保護法

【参照：テキスト4-3-1.】
P45

個人情報保護法とは

- インターネット普及や情報技術の進歩を背景に、「個人情報保護法」が2005年4月に施行。
- デジタル技術の進展や社会情勢の変化を受けて、法律は3度の改正を経ている。
- この法律では、何が個人情報とされるかや、その取り扱い方法を規定。

個人情報の定義

- 「個人情報」は生存する個人に関する情報。
- 氏名、生年月日、住所、顔写真などで個人を特定できる。
- 他の情報と照合し特定可能なものも含む。

関連法令

個人情報を取扱う時の基本ルール

【参照：テキスト4-3-1.】
P45

項番	取扱い種別	ルール
1	取得・利用	<ul style="list-style-type: none"> ・ 利用目的を特定して、その範囲内で利用する ・ 利用目的を通知又は公表する
2	保管・管理	<ul style="list-style-type: none"> ・ 漏えいなどが生じないように、安全に管理する ・ 従業者や委託先にも安全管理を徹底する
3	提供	<ul style="list-style-type: none"> ・ 第三者に提供する場合は、あらかじめ本人から同意を得る ・ 第三者に提供した場合、提供を受けた場合は一定事項を記録する
4	開示請求などへの対応	<ul style="list-style-type: none"> ・ 本人から開示などの請求があった場合はこれに対応する ・ 苦情に適切かつ迅速に対応する

個人情報保護法の罰則規定

- ・ 2022年4月の法改正で、罰則強化。
- ・ 個人情報保護委員会の命令違反や不正流用で、1億円以下の罰金。
- ・ 報告義務違反の場合、50万円以下の罰金。

関連法令

【参照：テキスト4-3-2.】
P46

GDPR

GDPR（一般データ保護規則）とは

起源: 欧州連合（EU）で策定された新しい個人情報保護の枠組み。

目的: 個人のプライバシー権を強化し、個人データの処理に関する組織の透明性を増すことを目的としている。

適用範囲: 欧州経済領域（EEA）内で活動するすべての組織に適用され、EEA外の組織もEEAの市民のデータを処理する場合にはこの規則の対象となる。

内容: 個人データの「収集」、「処理」、「保存」、「移転」など、あらゆる側面に関してのルールが定められており、ユーザーには自らのデータに対するアクセス、修正、削除などの権利が保障されている。

罰則: 違反組織には、全世界の年間売上の最大4%以下、または2,000万ユーロ以下（いずれか高い方）の罰金が課せられることが規定されている。 ※2,000万ユーロ：約34億円

関連法令

GDPRと日本企業の関係

【参照：テキスト4-3-2.】
P46, P47

- EU内に物理的拠点が無い企業も対象となる可能性
インターネットを利用してEU域内に商品やサービスの提供、情報収集を実施
EU域内からのアクセスを持つターゲティング広告を配置した自社サイトを保有
- GDPR違反時には重い制裁金が課せられる

対策例

- GDPRにおいて、Cookieは「個人情報」として扱われる
- WebサイトでCookieを使用する場合、閲覧者からの同意取得が必須
- 個人データの利用同意の管理のため、ツール（CMP）の導入が推奨される

関連法令

【参照：テキスト4-3-3.】
P47

その他関連法令

- 不正競争防止法
- 著作権法
- 電気通信事業法
- 電子証明および認証業務に関する法律
- 情報処理の促進に関する法律
- 国立研究開発法人情報通信研究機構法
- 刑法
- 不正アクセス行為の禁止などに関する法律

第5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

情報セキュリティの概況

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見るケーススタディ

情報セキュリティの概況

情報セキュリティの脅威を学ぶ

【参照：テキスト5-1-1.】
P51, P52

目的

- 適切な予防策や対策を講じること

内容

- 攻撃手口の**傾向**を把握する
- 脅威に対する対策方法を理解する

活用すべき代表的な刊行物

- 情報セキュリティ白書
- 情報セキュリティ10大脅威



情報セキュリティの概況

情報セキュリティ白書

【参照：テキスト5-1-2.】
P52

記載内容

- セキュリティインシデントの事例
- セキュリティ対策強化の取組
- サイバーセキュリティ経営ガイドライン
- 国内外のセキュリティの動向
- セキュリティ人材の育成
- 中小企業のセキュリティ対策
- 個別テーマ（IoT、インフラシステム等）のセキュリティ動向
- セキュリティツールの紹介

情報セキュリティの概況

情報セキュリティ10大脅威 2024[組織編]

【参照：テキスト5-1-3.】
P53, P54, P55, P56, P57

順位	組織向け脅威	概要
1	ランサムウェアによる被害	システムを人質に取り、身代金を要求するマルウェア
2	サプライチェーンの弱点を悪用した攻撃	取引先や供給業者を通じて攻撃する手口
3	内部不正による情報漏えい等の被害	従業員や関係者が内部から情報を漏らす行為
4	標的型攻撃による機密情報の窃取	特定の企業や組織を狙った攻撃で機密情報を盗む
5	修正プログラムの公開前を狙う攻撃	ソフトウェアの脆弱性が修正される前に攻撃する手法
6	不注意による情報漏えい等の被害	ヒューマンエラーによる情報の漏えい
7	脆弱性対策情報の公開に伴う悪用増加	公開された脆弱性情報を悪用する攻撃の増加
8	ビジネスメール詐欺による金銭被害	ビジネスメールを装った詐欺によって金銭をだまし取る手口
9	テレワーク等のニューノーマルな働き方を狙った攻撃	テレワーク環境を狙った攻撃
10	犯罪のビジネス化	犯罪行為をサービスとして提供するビジネスの存在

重大インシデント事例から学ぶ課題解決

【参照 : テキスト5-2-1.】
P58

インシデント事例から学ぶ

目的

- 具体的な知識をもとに実践的なアプローチ手法を習得すること。

学べる内容

- 攻撃手法や攻撃者の手口
- インシデントの影響と被害範囲
- 具体的なインシデント対応と復旧策

活用例

- リスク管理、対策の強化、ポリシーの改善、インシデント対応の改善
- 脅威トレンドの把握、共有
- セキュリティ意識の向上

重大インシデント事例から学ぶ課題解決

【参照 : テキスト5-2-2.】
P59

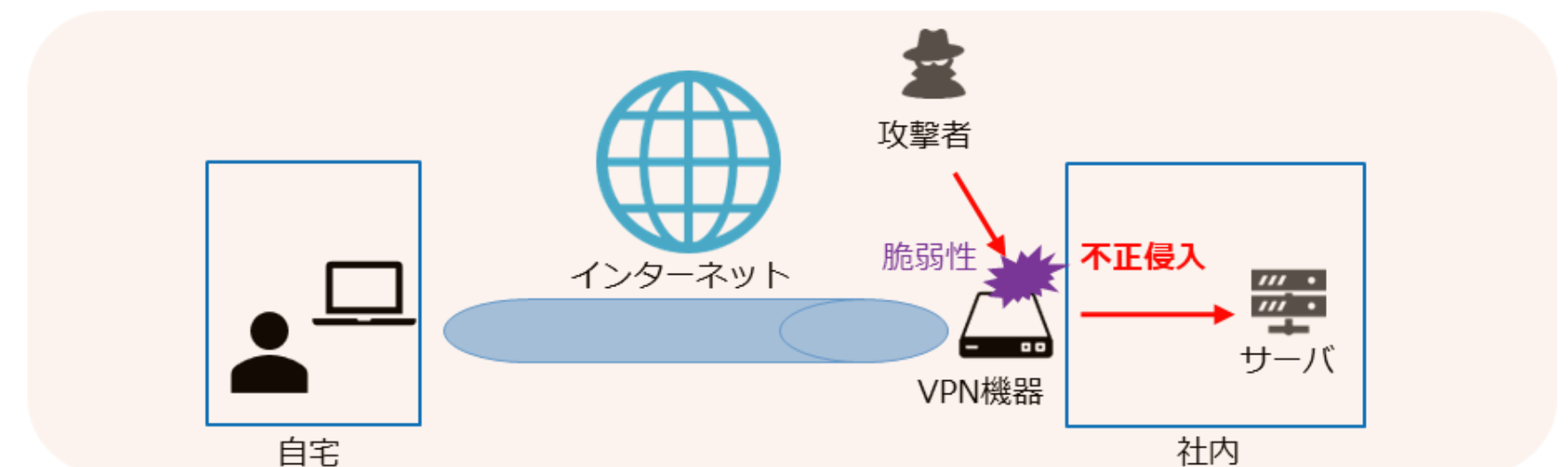
テレワークによるサイバー被害

事例概略

- テレワーク導入のために、社外からVPN接続できるようにした。
- VPN機器の脆弱性対応を実施した。
- すでに接続アカウントは抜かれた後で、そのアカウントを悪用された。

対処ポイント

- 脆弱性を悪用されることで、何が起こるのかを理解する。
- すでに攻撃を受けていることを前提とする。



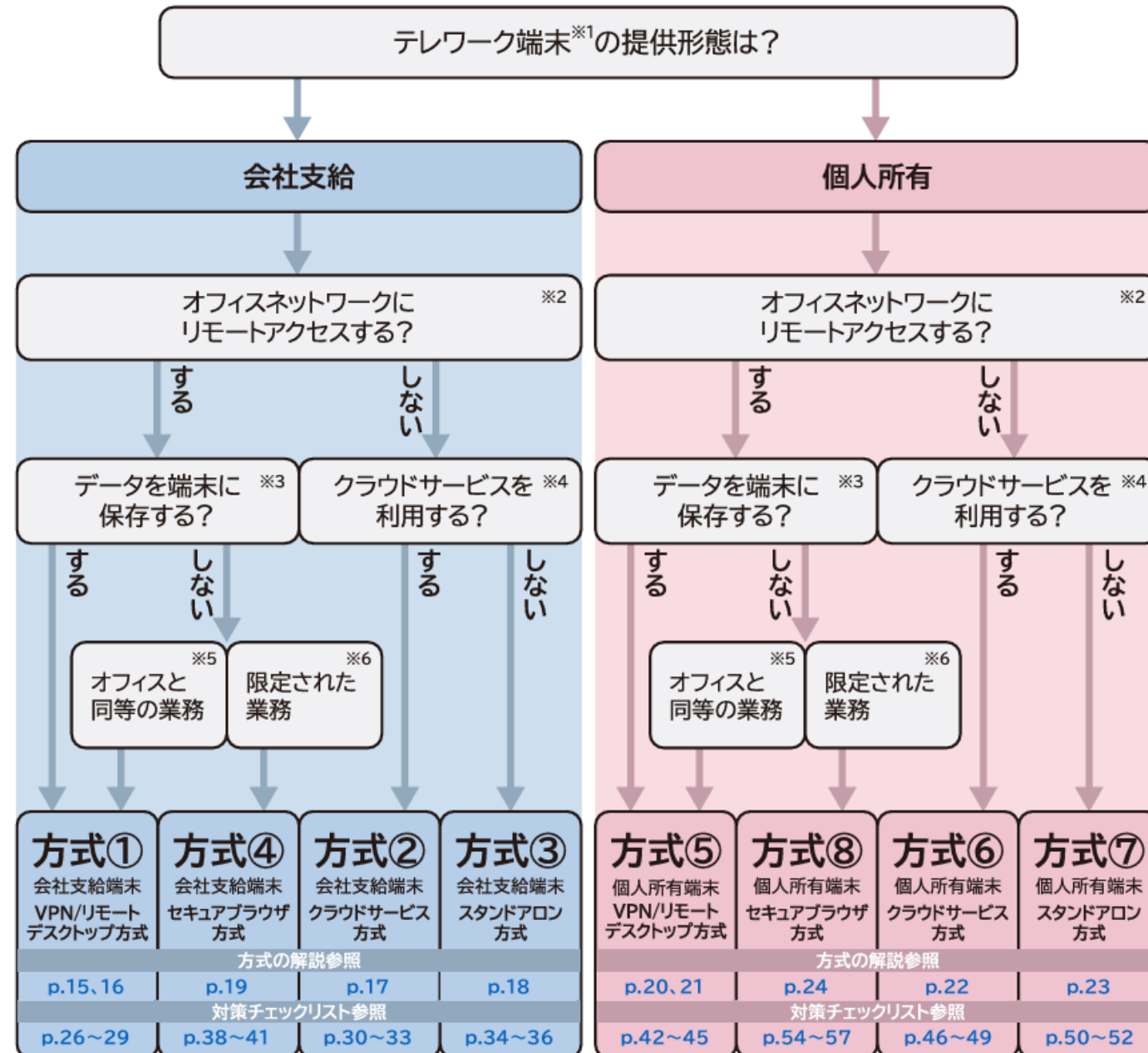
重大インシデント事例から学ぶ課題解決

テレワークのセキュリティ対策

【参照 : テキスト5-2-2.】

P59, P60

テレワーク方式概要



No	方式名
方式1	会社支給端末・VPN/リモートデスクトップ方式
方式2	会社支給端末・クラウドサービス方式
方式3	会社支給端末・スタンドアロン方式
方式4	会社支給端末・セキュアブラウザ方式
方式5	個人所有端末・VPN/リモートデスクトップ方式
方式6	個人所有端末・クラウドサービス方式
方式7	個人所有端末・スタンドアロン方式
方式8	個人所有端末・セキュアブラウザ方式

総務省. "中小企業等担当者向けテレワークセキュリティの手引き". https://www.soumu.go.jp/main_content/000816096.pdf

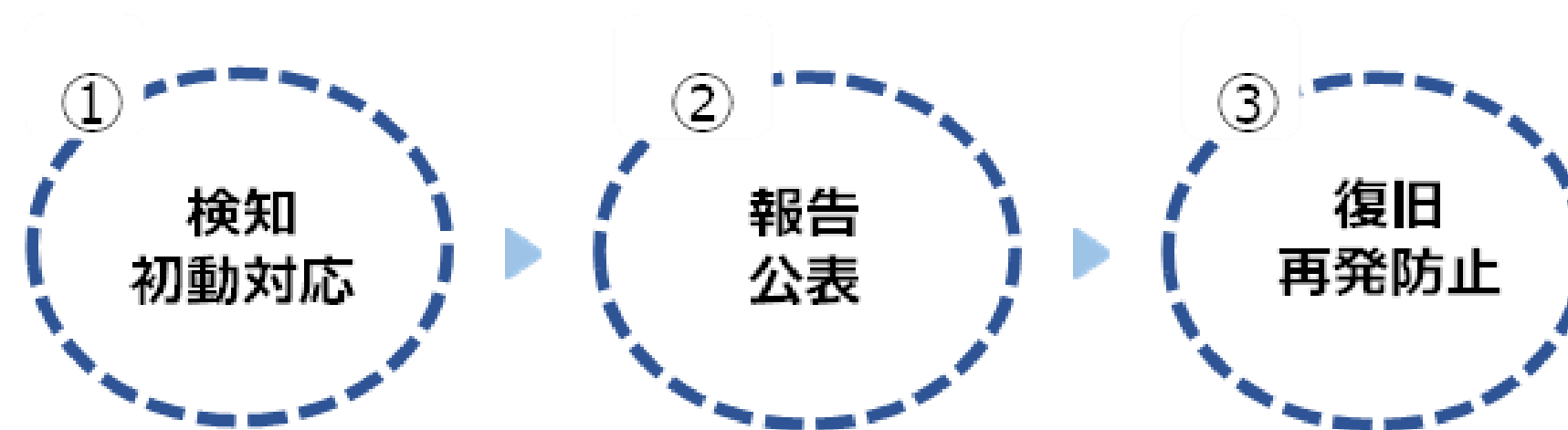
重大インシデント事例から学ぶ課題解決

【参照：テキスト5-2-3.】
P60, P61

インシデント対応の流れ

手順概要

1. 検知・初動対応
2. 報告・公表
3. (調査・対応) 復旧・再発防止



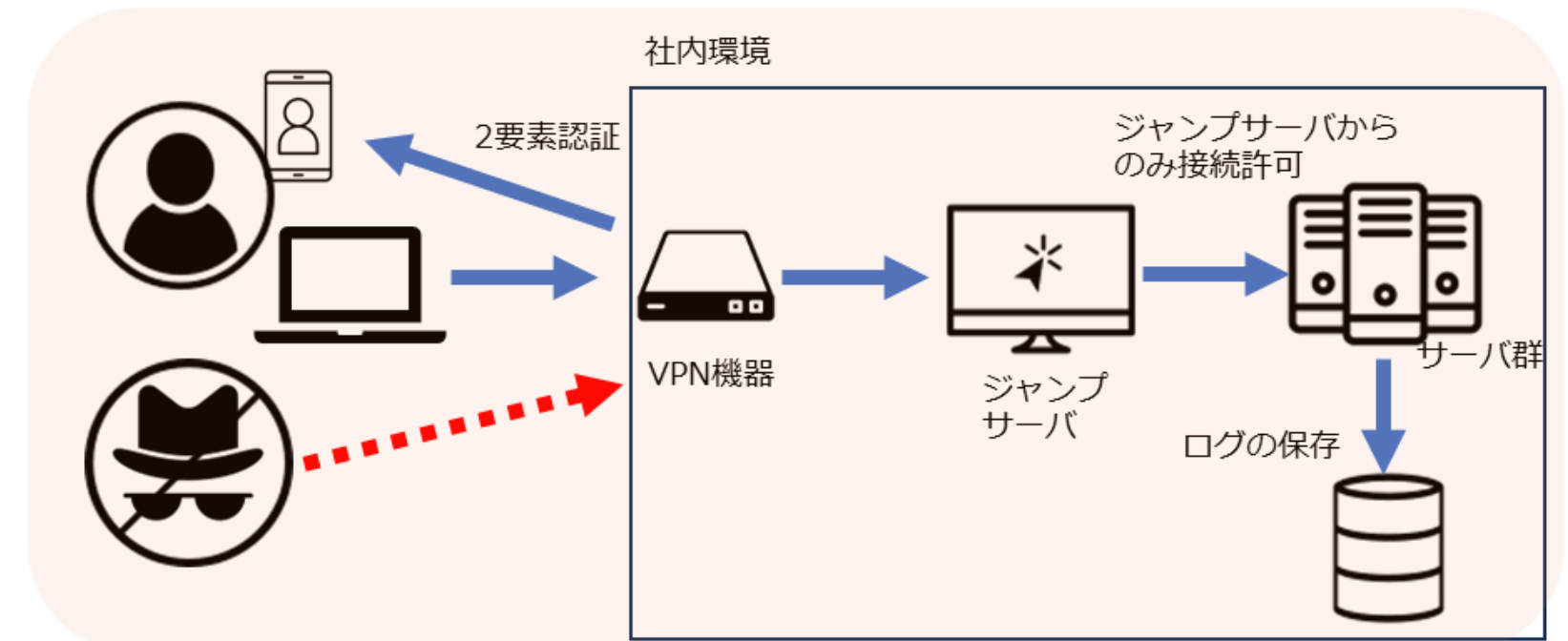
重大インシデント事例から学ぶ課題解決

【参照 : テキスト5-3-3.】
P67

具体的な対応策

実施するべき技術的対策

- VPN機器への接続に多要素認証を導入し、接続元の信頼性を上げる。
- 外部から中枢のサーバに対し、VPN経由での直接接続をさせない。
- サーバやPCの特権アカウントのパスワードを定期的に変更する。
- OSのファイアウォール機能を有効にし、接続元を限定する。
- サーバやネットワーク機器のログを取得し、定期的を確認する。
- 脆弱性情報を高い頻度で確認する。
- パッチマネジメントを実施する。
- EDRなどの製品を導入する。



第6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

これからの企業経営で必要な観点：社会の動向

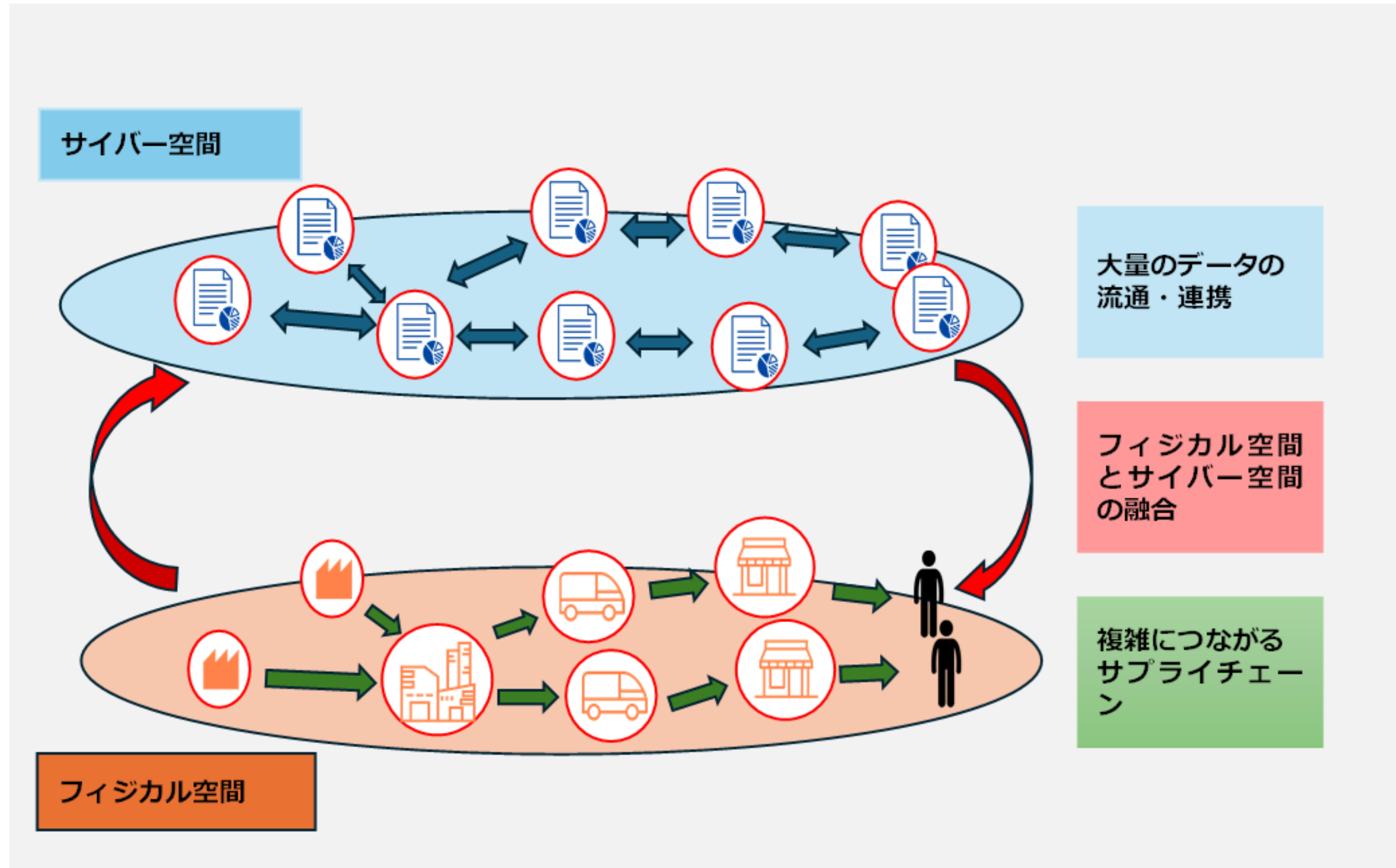
守りのIT投資と攻めのIT投資

経営投資としてのサイバーセキュリティ対策

これからの企業経営に必要な観点：社会の動向

現実社会とサイバー空間のつながり

【参照：テキスト6-1-1.】
P69, P70, P71, P72



これからの企業経営で必要な観点：社会の動向

IT活用における課題

【参照：テキスト6-1-2.】
P72, P73



我が国がデジタル化で後れを取った6つの理由

1. ICT投資の低迷
2. 業務改革等を伴わないICT投資
3. ICT人材不足・偏在
4. 過去の成功体験
5. デジタル化への不安感・抵抗感
6. デジタルリテラシーが十分ではない

守りのIT投資と攻めのIT投資

守りのIT投資、攻めのIT投資の概要

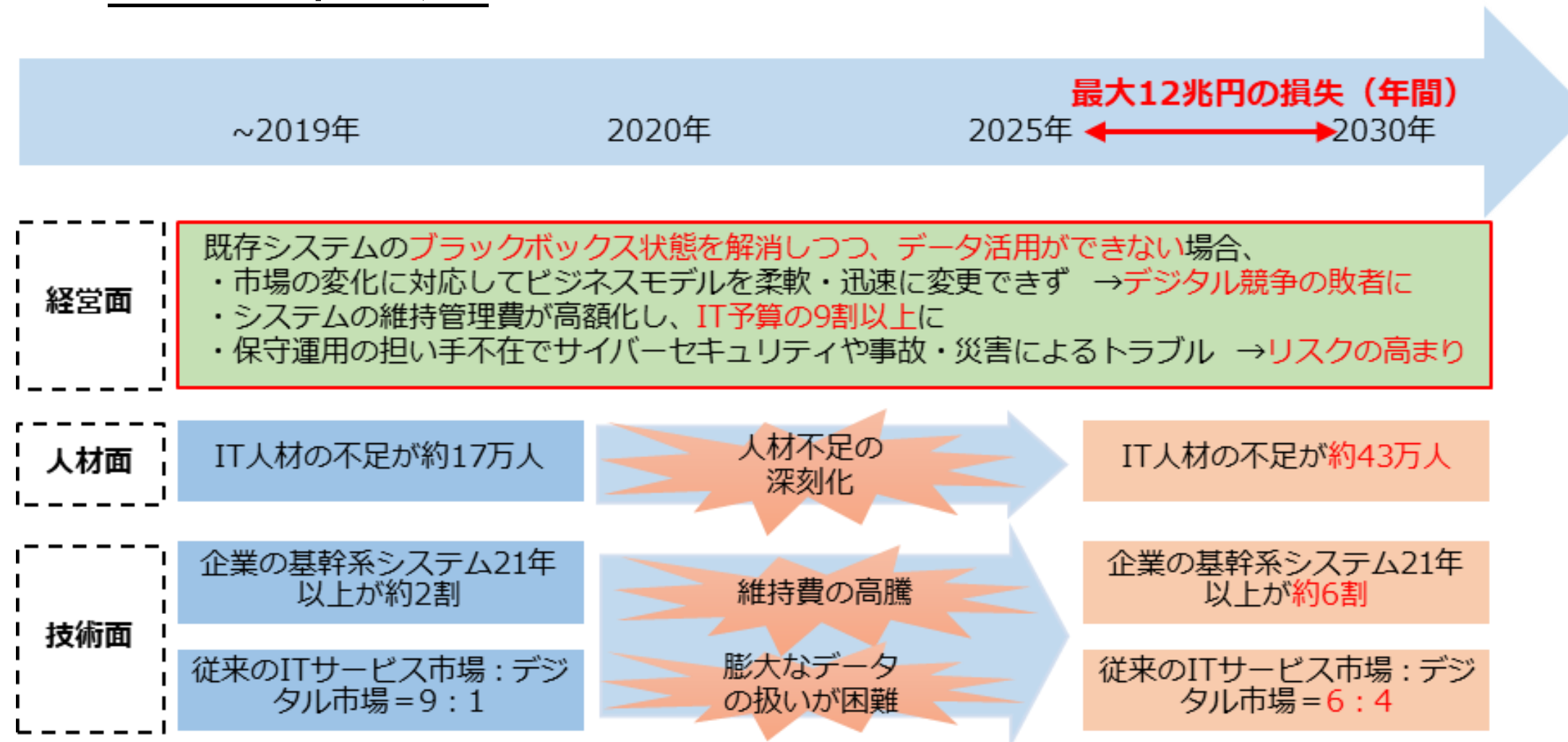
【参照：テキスト6-2-1.】
P75

<p>「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</p>  <ul style="list-style-type: none">● 業務の効率化● コストの削減	<p>「攻めのIT投資」 (DX) 目的：ビジネス継続・競争力強化</p>  <ul style="list-style-type: none">● 新たなビジネスの展開● 顧客視点で新たな価値の創造
---	---

守りのIT投資と攻めのIT投資

「攻めのIT」に取り組む方針について 2025年の崖

【参照：テキスト6-2-2.】
P76



「2025年の崖」の概要図

(出典) 経済産業省「DXレポート～ITシステム「2025年の崖」の克服とDXの本格的な展開～」をもとに作成

項番	課題
対策1	「見える化」指標、診断スキームの構築
対策2	DX推進ガイドラインの策定
対策3	ITシステムの刷新
対策4	ユーザー企業・ベンダー企業との新しい関係性構築
対策5	DX人材の育成・確保

守りのIT投資と攻めのIT投資

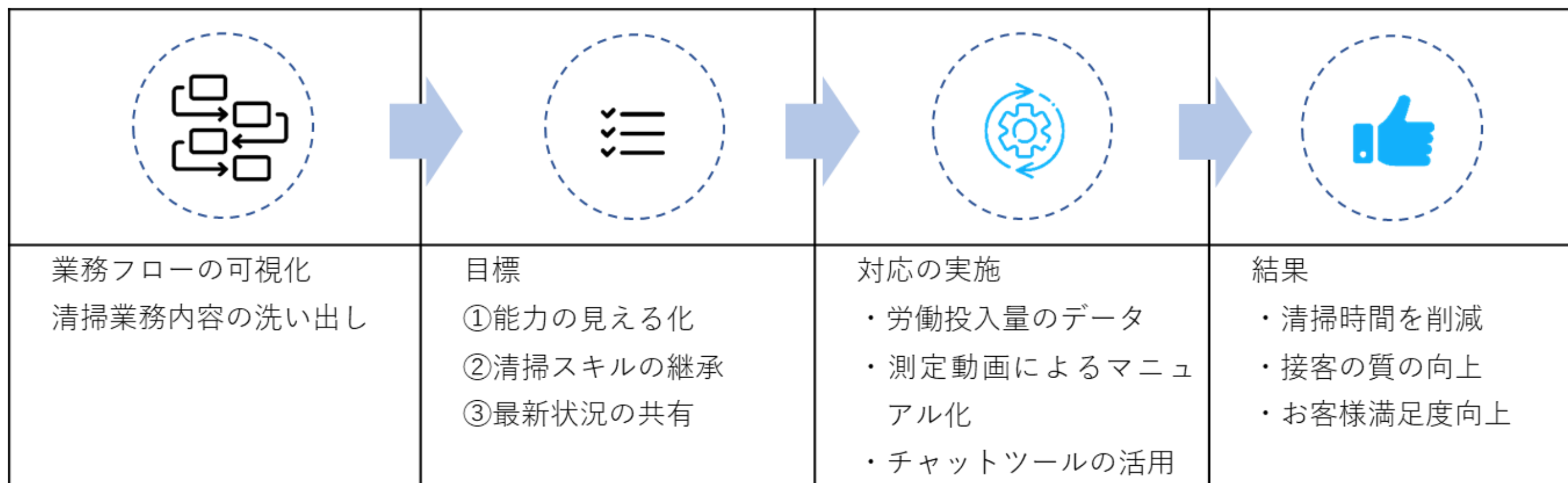
ITを活用した生産性の向上

【参照：テキスト6-2-3.】
P77, P78

「守りのIT投資」：デジタルオプティマイゼーション

- 業務効率化・コスト削減
- デジタル活用するための環境整備

事例：某旅館



守りのIT投資と攻めのIT投資





ITを活用した新たなビジネスの展開

【参照：テキスト6-2-4.】
P79, P80

「攻めのIT投資」：DX

- ビジネス環境の急激な変化に対応するため
- 多様化する顧客ニーズに応えるため

事例：某ワイン製造会社

			
<p>実現したこと</p> <p>付加価値が高い「産地細分化ワイン」を増産・安定供給すること</p>	<p>課題</p> <p>アナログ作業（口頭伝達、手書き記帳など）の改善</p>	<p>対策</p> <p>「ブドウ受入演算システム」を構築</p>	<p>結果</p> <p>産地細分化ワインの増産・安定供給実現</p>

守りのIT投資と攻めのIT投資

次世代技術を活用したビジネス展開

【参照：テキスト6-2-5.】
P81

活用する技術

技術	概要	活用方法例
AI	膨大な情報を処理し、判断や予測を行うことができる。	<ul style="list-style-type: none"> • 需要の予測や在庫の最適化 • 不良品の自動検出 • 対話型AIによる、問い合わせ対応の自動化 • コンテンツの生成
IoT	現実世界のさまざまなモノが、インターネットと繋がる。収集したデータが、インターネットに送信・蓄積され、データを分析・活用することで、新たな価値の創出につながる。	<ul style="list-style-type: none"> • 生産設備にセンサーを設置し、振動データを取得し分析することで、部品の故障予知や性能維持が可能 • 生産設備の稼働状況を可視化したことで、全ての拠点での生産状況をリアルタイムに把握可能
クラウドサービス	自社で機器やシステムを保有しなくても、インターネット経由で様々なサービスを利用できる	<ul style="list-style-type: none"> • 社内情報の一元管理 • システムを開発・実行するためのツールや環境構築作業の省略 • 場所やデバイスに依存せずに作業の継続が可能

経営投資としてのサイバーセキュリティ対策

経営者が重要視すべき3つのポイント

【参照：テキスト6-3-1.】
P84



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



ITの活用とサイバーセキュリティ対策の関係性

(出典) 東京都産業労働局 「MISSION 3-1 サイバーセキュリティ対策が経営に与える重大な影響」

経営投資としてのサイバーセキュリティ対策

【参照：テキスト6-3-2.】
P84, P85

経営者が重要視すべき3つのポイント

ポイント1：ビジネスの継続・発展にはITの活用が不可欠

【中小企業の重要課題】

- 業務や生産の効率化
- 人材確保

ポイント2：ITの活用にはサイバー攻撃への対策が必要

DX推進のためにはIT活用は必須

IT活用のためにはインターネットの活用は必須

インターネットの活用にはサイバーセキュリティ対策は**最優先事項**！

経営投資としてのサイバーセキュリティ対策

経営者が重要視すべき3つのポイント

【参照：テキスト6-3-2.】
P85, P86

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

- 経営者による経営判断が必要
- セキュリティインシデントが発生した際に、経営者が責任を負う

法令	条項	要約
民法	第415条 債務不履行による損害賠償責任	サイバー攻撃により仕事が停滞した場合、会社および第三者に対する、契約違反による賠償義務を負う。
	第644条 取締役の善管注意義務違反	企業のセキュリティ体制が規模や業務内容に鑑みて適切でなく、サイバー攻撃により企業や第三者に損害が発生した場合、取締役は会社に対して、善管注意義務違反による賠償義務を負う。
会社法	第330条 取締役の善管注意義務違反 第423条 1項 任務懈怠による損害賠償責任 第429条 1項 第三者に対する注意義務違反	企業のセキュリティ体制が規模や業務内容に鑑みて適切でなく、サイバー攻撃により企業や第三者に損害が発生した場合、取締役は会社に対する、善管注意義務違反による任務懈怠（けたい）に基づく損害賠償義務を負う。

情報セキュリティ対策が不備の場合に責任追及の根拠とされる主な法律
(出典) IPA 「中小企業の情報セキュリティ対策ガイドライン 第3.1版」から抜粋



**令和6年度
中小企業サイバーセキュリティ社内体制整備事業**