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

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

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およ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およ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．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

経済財政運営と改革の基本方針2023

【参照：セミナーテキスト5-1-1.】

経済財政運営と改革の基本方針

- 国の基本的な政策方針を示すもので、通称「骨太の方針」と呼ばれる
- 官邸主導での改革を目的とし、内閣総理大臣が議長を務める経済財政諮問会議で毎年策定される
- ITとセキュリティ関連の施策もこの方針に基づいて計画される
- 2023年の方針では、「デジタル」が50回以上使用され、デジタル技術の活用とデジタル社会構築が協調される

経済財政運営と改革の基本方針2023

【参照：セミナーテキスト5-1-1.】

新しい資本主義の取組み

- 官民連携による国内投資拡大と**サプライチェーンの強靭化**
- グリーントランスフォーメーション（GX）、デジタルトランスフォーメーション（DX）などの加速
- スタートアップの推進と新たな産業構造への転換、インパクト投資の促進
- 官民連携を通じた化学技術・イノベーションの推進
- インバウンド戦略の展開

経済財政運営と改革の基本方針2023

【参照：セミナーテキスト5-1-1.】

官民連携による国内投資拡大とサプライチェーンの強靭化

1. 新しい資本主義の下の変化
2. 挑戦と方針
3. 日本経済の再生のための方針
4. 投資拡大の方策
5. 雇用と人材の課題への対応
6. 強靭な経済構造の構築
7. 国際協力と投資拡大の推進

経済財政運営と改革の基本方針2023

【参照：セミナーテキスト5-1-1.】

GX、DXなどの加速

GXの加速

1. 日本の脱炭素政策
2. エネルギー政策の推進
3. 環境友好的な輸出と生活の推進

DXの加速

1. デジタル行政の実現
2. 市場環境の整備
3. 先進技術と国際連携

経済財政運営と改革の基本方針2023

【参照：セミナーテキスト5-1-1.】

スタートアップの推進と新たな産業構造への転換、インパクト投資の促進

スタートアップの促進と新たな産業構造への展開

1. 参入と再チャレンジの際の障壁を低くする
2. 「スタートアップ育成5か年計画」を通じて、参入・退出の円滑化

インパクト投資の促進

1. インパクトスタートアップへの支援を強化
2. 社会的起業家の認証制度の設立

経済財政運営と改革の基本方針2023

【参照：セミナーテキスト5-1-1.】

官民連携を通じた科学技術・イノベーションの推進

1. 科学技術・イノベーションの推進
2. 高等教育と研究の強化
3. 教育の国際化と人材の育成

経済財政運営と改革の基本方針2023

【参照：セミナーテキスト5-1-1.】

インバウンド戦略の展開

1. 持続可能な形での観光立国の復活
2. 高度人材の受入れ
3. 技能実習制度および特定技能制度の在り方の検討
4. 資産運用立国・国際金融センター等の実現

デジタル社会の実現に向けた重点計画

【参照：セミナーテキスト5-2-1.】

重点計画とは

1. データの重要性増大
2. デジタル社会実現の必要性
3. 重点計画の策定
4. 計画の役割
5. PDCAサイクルの徹底
6. 施策の進捗公開

デジタル社会の実現に向けた重点計画

【参照：セミナーテキスト5-2-1.】

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」の推進をはじめとする国際戦略

デジタル社会の実現に向けた重点計画

【参照：セミナーテキスト5-2-1.】

デジタル社会の実現に向けた戦略・施策

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み
7. Web3.0の推進

デジタル社会の実現に向けた重点計画

【参照：セミナーテキスト5-2-1.】

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

デジタル社会の実現に向けた重点計画

【参照：セミナーテキスト5-2-1.】

各分野における基本的な施策

1. 国民に対する行政サービスのデジタル化
2. 安全・安心で便利な暮らしのデジタル化
3. アクセシビリティの確保
4. **産業のデジタル化**
5. デジタル社会を支えるシステム・技術
6. デジタル社会のライフスタイル・人材

デジタル社会の実現に向けた重点計画

【参照：セミナーテキスト5-2-1.】

産業のデジタル化

1. デジタルによる新たな産業の創出・育成
   クラウドサービス産業の育成／ITスタートアップなどの育成
2. 事業者向け行政サービスの質の向上に向けた取組み　【別ページで解説】
3. 中小企業のデジタル化の支援　【別ページで解説】
4. 産業全体のデジタルトランスフォーメーション

デジタル社会の実現に向けた重点計画

【参照：セミナーテキスト5-2-1.】

事業者向け行政サービスの質の向上に向けた取組み

1. 電子署名、電子委任状、商業登記電子証明書の普及
2. 法人共通認証基盤（GビズID）の普及
3. 事業者に対するオンライン行政サービスの充実
4. レベルに応じた認証の推進
5. eKYCなどを用いた民間取引などにおける本人確認手法の普及促進

デジタル社会の実現に向けた重点計画

【参照：セミナーテキスト5-2-1.】

中小企業のデジタル化の支援

1. 中小企業の事業環境デジタル化サポート
   ・IT専門家との相談を受けられる体制の整備、IT導入補助金　など

2. 中小企業のサイバーセキュリティ対策の支援
   ・「サイバーセキュリティお助け隊サービス」の普及促進
   ・相談体制の強化、情報集約、共有促進機能の強化　など

Society5.0

【参照：セミナーテキスト5-2-2.】

Society5.0の特徴と期待される未来

1. IoTを利用
   ・全ての人とモノが繋がり、知識や情報を共有する
   ・新たな価値の創出や社会の課題の解決が可能となる

2. AI、ロボット、自動走行車を利用
   ・少子高齢化、地方の過疎化、貧富の格差などの課題への対応が期待される
   ・希望を持てる社会や、世代間で互いに尊重し合う社会、個人が快適に活躍できる社会の実現が期待される

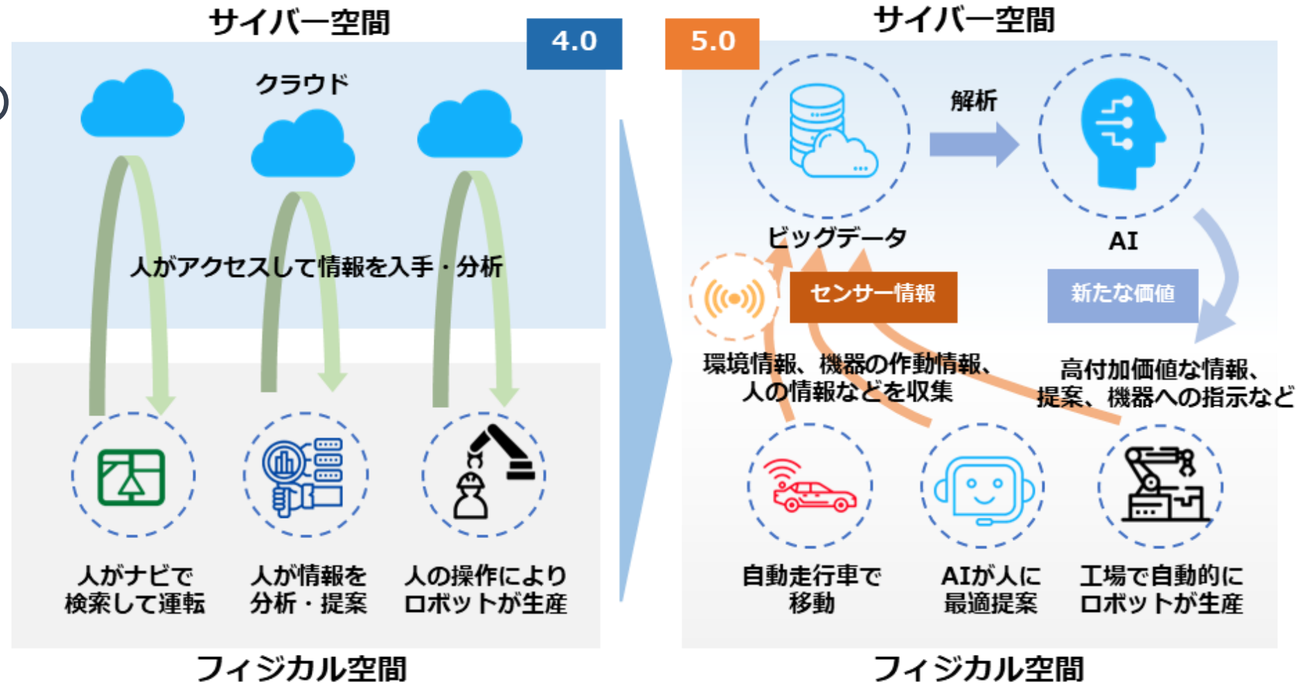
Society5.0

【参照：セミナーテキスト5-2-2.】

Society5.0とこれまでの情報社会（Society4.0）の違い

- Society4.0：
  人がクラウドサービスにアクセスし、情報やデータを取得・分析
- Society5.0：
  フィジカル空間のセンサーから取得した膨大な情報がサイバー空間に集積

※ Society4.0では人間が情報の解析で価値を生んでいたが、Society5.0ではAIによる解析結果が人間にフィードバックされ、新しい価値が産業や社会にもたらされる



Society4.0とSociety5.0の比較
（出典）内閣府.”Society5.0”.https://www8.cao.go.jp/cstp/society5_0,（2023-08-03）.

Society5.0

【参照：セミナーテキスト5-2-2.】

社会の変化に対するセキュリティ上の脅威

1. サイバー攻撃によりサービス利用の中断または利用不可能
2. データがサイバー空間で改ざんされ、偽情報が拡散されるリスク
3. 情報の漏えいや改ざんによるプライバシー侵害や知的財産権侵害のリスク増加
4. サイバー空間とフィジカル空間の融合による新たな処理がサイバー攻撃の新しい対象となる
5. サプライチェーンの変化に伴うサイバー攻撃の影響範囲が拡大するリスク

DXの推進

【参照：セミナーテキスト5-2-3.】

中小企業がDX推進における優位な点

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

DXの推進

【参照：セミナーテキスト5-2-3.】

データ活用の流れ

1. データの収集
   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（ビックデータ）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。

2．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）

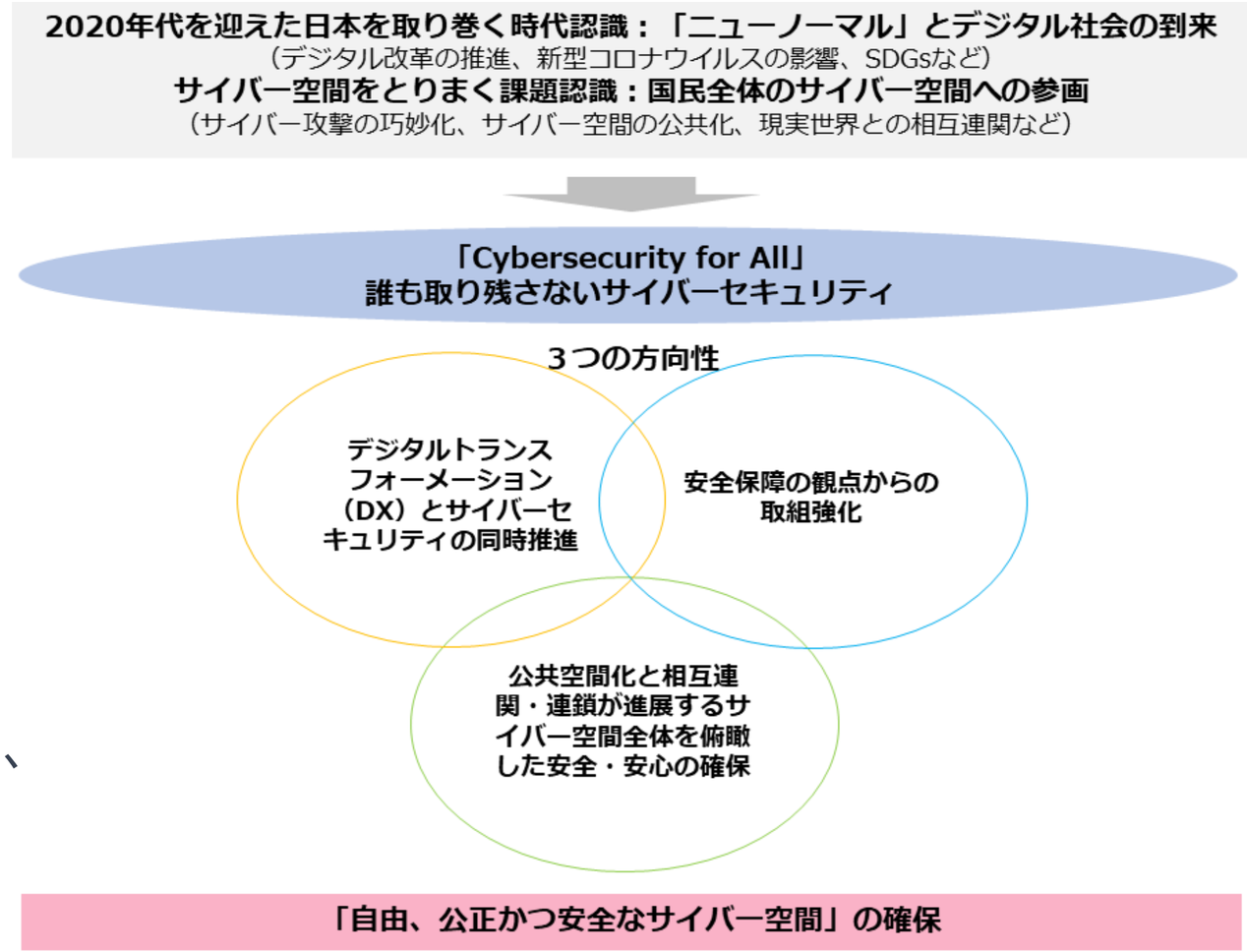
関連法令

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-1.】

サイバーセキュリティ戦略の課題と方向性

- 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。



サイバーセキュリティ戦略の課題と方向性の概要
（出典）NISC「 サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ」を基に作成

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-1.】

3つの政策目標と横断的施策

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

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-1.】

経済社会の活力の向上及び持続的発展

方向性

DXとサイバーセキュリティの同時推進

課題

- DXの進行中、サイバーセキュリティの意識と技術・データへの信頼が不足すると、表層的なデジタル化のリスクが高まる
- デジタル化が進展しているが、セキュリティ確保は企業価値にリンクし、「セキュリティ・バイ・デザイン」の考慮と、デジタルとセキュリティの投資が同時に必要である

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-1.】

経済社会の活力の向上及び持続的発展

主な具体的施策

1. 経営層の意識改革
2. 地域・中小企業におけるDX with Cybersecurityの推進
3. 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
   - ➢ サプライチェーン、データ流通、セキュリティ製品・サービス、先端技術
4. 誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-1.】

国民が安全で安心して暮らせるデジタル社会の実現

方向性

　公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保

課題

- サイバー空間の公共空間化、相互連関、連鎖の深化
- サイバー攻撃の組織化、洗練化

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-1.】

国民が安全で安心して暮らせるデジタル社会の実現

主な具体的施策

1. 国民・社会を守るためのサイバーセキュリティ環境の提供
2. デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保
3. 経済社会基盤を支える各主体における取組み
4. 多様な主体による情報共有・連携と大規模サイバー攻撃事態などへの対処体制強化

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-1.】

国際社会の平和・安定及びわが国の安全保障への寄与

方向性

安全保障の観点からの取組み強化

課題

- 我が国の安全保障環境が厳しく、中国・ロシア・北朝鮮がサイバー能力を増強し、情報窃取を試みるサイバー攻撃を行っているとの認識がある。
- 同盟国や同志国はサイバー脅威への対応を強化しており、サイバー空間のルールに関する対立に連携して立ち向かっている。
- 安全保障の範囲が経済や技術分野にも広がっているため、同盟国や同志国と連携し、自由で公正なサイバー空間の確保と国際ルールの形成が必要である。

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-1.】

国際社会の平和・安定及びわが国の安全保障への寄与

主な具体的施策

1. 自由・公正かつ安全なサイバー空間の確保
   - サイバー空間における法の支配の推進
   - サイバー空間におけるルール形成

2. 我が国の防御力・抑止力・状況把握力の強化
   - サイバー攻撃に対する防御力の向上
   - サイバー攻撃に対する抑止力の向上
   - サイバー空間の状況把握力の強化

3. 国際協力・連携
   - 知見の共有・政策調整
   - サイバー事案などに係る国際連携の強化
   - 能力構築支援

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-1.】

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み

全員参加による協働・普及啓発
- ガイドラインや様々な解説資料などの整備の推進

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-1.】

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
  - ➢ サイバー空間への依存度の高まり/情報システムの利用拡大/サプライチェーンの多様化・複雑化の進展/生成AIなどの新たな技術普及　など

- 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～
  - ➢ ランサムウェアが依然とした脅威、不正プログラムEmotetが活動と停止の繰り返し/暗号資産交換業者もサイバー攻撃の対象　など

- 昨今の状況変化を踏まえた政策課題
  - ➢ 政府による「国家安全保障戦略」の策定　など

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-1.】

サイバーセキュリティ2023

今後の取組みの方向性

1. 経済社会の活力の向上及び持続的発展
   - **ICTの利活用に積極的ではなかった地域・中小企業における対策の促進**
   - **サプライチェーンリスクの増大を踏まえたソフトウェアセキュリティの高度化に関する取組み強化**
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

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-1.】

サイバーセキュリティ2023

今後の取組みの方向性

1. 中小企業のサイバーセキュリティ対策促進
   - 「サイバーセキュリティお助け隊サービス」の普及
   - サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）との連携

2. サプライチェーンリスクを踏まえたソフトウェアセキュリティの高度化に関する取組強化
   - 脆弱性情報とSBOMの紐付けを機械的に行う手法の実証
   - 通信分野でのSBOM導入に向けた取組

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-2.】

企業経営のためのサイバーセキュリティの考え方

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みは、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。

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-2.】

企業経営のためのサイバーセキュリティの考え方

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

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-2.】

サイバーセキュリティ対策の取組みレベル

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付け、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

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-3.】

DX with Cybersecurity

DX with Cybersecurityの推進に向けた主な施策

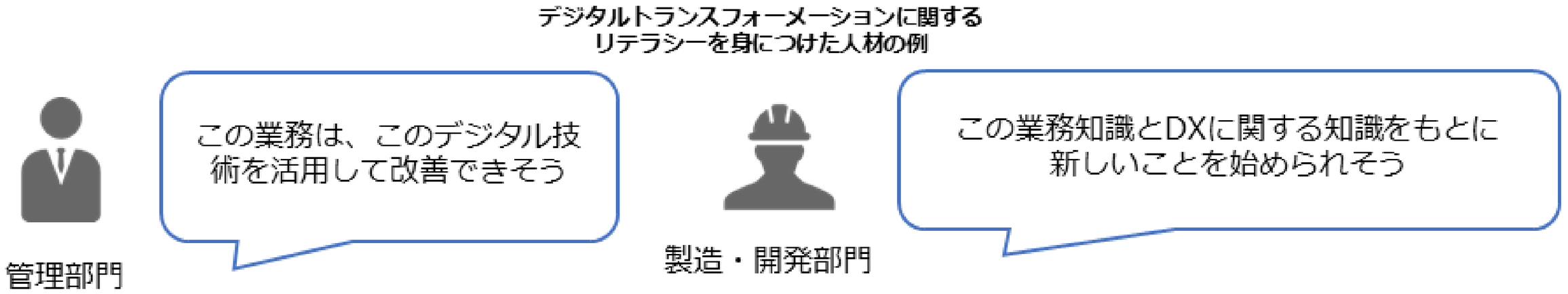
分類	課題	施策
経営層の意識改革	経営層が主体性をもってDXとサイバーセキュリティ対策に取組むためには、専門家とのコミュニケーションが重要	経営者がITやセキュリティに関する専門知識を持っていない場合でも、セキュリティ専門家と協力し、「プラス・セキュリティ」知識を習得する環境を整備
地域・中小企業におけるDX with Cybersecurityの推進	中小企業は、セキュリティ対策に予算を割く事の必要性を理解する	中小企業が利用しやすい安価かつ効果的なセキュリティサービス・保険の普及など、中小企業向けセキュリティ施策を推進
新たな価値創出を支えるサプライチェーンなどの信頼性確保に向けた基盤づくり	サイバー攻撃の起点となり得る箇所の拡大に伴う、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

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-3.】

DXに関するリテラシーを身につけたことによる効果（個人）

- 世の中のDXと最新技術にアンテナを広げる
- 新技術やキーワードに興味を持つ
- 知らない内容に遭遇した時、自ら調査しDXの知識を深める



サイバーセキュリティ戦略

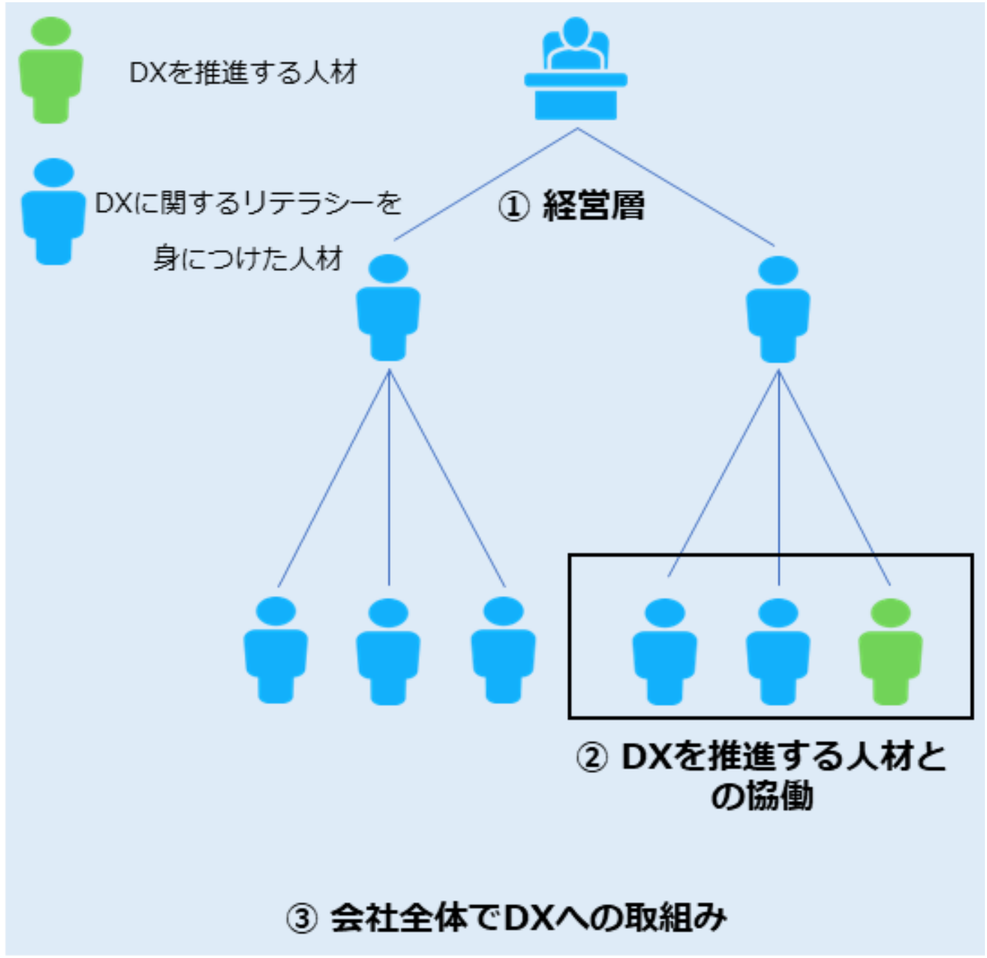
【参照：セミナーテキスト6-1-3.】

DXに関するリテラシーを身につけたことによる効果（会社）

経営層
- 社会・ビジネス環境の変化を把握
- 有益な技術・考え方を獲得
- 自社のDXの方向性を社員に示す

DXを推進する人材との協働
- 事業知見を持つ人材との協力
- DX専門の人材との連携
- これにより企業のDXが進展しやすくなる

会社全体でDXへの取組み
- 社員全員がDXリテラシーを習得
- 組織内の変化に対する理解が増加
- DXの推進が受け入れられやすくなる



DXリテラシー標準に沿った学びによる効果の概要
（出典）IPA、経済産業省「デジタルスキル標準ver.1.0 」を基に作成

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-3.】

デジタルスキル標準（DSS）

「DXリテラシー標準」は、自身が属する産業や事業の方向性に合わせる必要がある

標準策定のねらい

ビジネスパーソン一人ひとりがDXに関するリテラシーを身につけることで、
DXを自分事ととらえ、変革に向けて行動できるようになる

Why
（DXの背景）
DXの重要性を理解するために必要な、社会、顧客・ユーザー、競争環境の変化に関する知識を定義

→ DXに関するリテラシーとして身につけるべき知識の学習の指針とする）

What
（DXで活用されるデータ・技術）
ビジネスの場で活用されているデータやデジタル技術に関する知識を定義

→ DXに関するリテラシーとして身につけるべき知識の学習の指針とする

How
（データ・技術の利活用）
ビジネスの場でデータやデジタル技術を利用する方法や、活用事例、留意点に関する知識を定義

→ DXに関するリテラシーとして身につけるべき知識の学習の指針とする

マインド・スタンス

社会変化の中で新たな価値を生み出すために必要な意識・姿勢・行動を定義

→個人が自身の行動を振り返るための指針かつ、組織・企業がDX推進や持続的成長を実現するために、構成員に求める意識・姿勢・行動を検討する指針とする

DXリテラシー標準の全体像
（出典）IPA、経済産業省「デジタルスキル標準ver.1.1 」を基に作成

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-3.】

デジタルスキルの学習方法

マナビDXとは

- DXに関する講座を案内するサービス
- https://manabi-dx.ipa.go.jp/

取り扱い講座

- 経済産業省の審査基準を満たしたDXに関するもの
- 掲載講座数：457件
  有償：360件　無償：97件　（2023/8/27現在）

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-3.】

プラス・セキュリティ

プラス・セキュリティとは
自らの業務遂行にあたって
セキュリティを意識し、
必要かつ十分なセキュリティ
対策を実現できる能力を身に
つけること、あるいは身に
つけている状態のこと。

クラウドを活用した
新規プロジェクトの担当者

組み込みソフトウェアの
機能を設計する担当者

自社の電話、
インターネット、複合機な
どの保守契約を扱う担当者

サイバーセキュリティの知識が不十分な
場合の問題例

目的にそぐわないクラウドを選定することや、自社のサイバーセキュリティ担当者が把握していないクラウドの導入により、情報漏洩などのリスクが高まる恐れがあります

ソフトウェアにサイバー攻撃に対する脆弱性が生じる恐れがあります

不適切な設定で運用することで、機器を介した情報漏えいの原因となる恐れがあります

サイバーセキュリティ戦略

【参照：セミナーテキスト6-1-3.】

プラス・セキュリティ人材の育成

試験・資格の活用

- 各分野の人材がセキュリティ知識を習得する手段として、資格や試験がある。
- 資格の利点は、特定の業務に必要なスキルを効率的に学べること。

情報セキュリティマネジメント試験

対象：企業の戦略マネジメント層や実務者層のサイバーセキュリティ担当者
内容：組織の情報セキュリティを確保し、脅威から保護するための計画・運用・評価・改善のスキルを認定する。

教育プログラム・コミュニティ活動の活用

NISCでは、経営層、管理職、一般社員ごとにそれぞれ初級、中級、上級で難易度が分けられたプラス・セキュリティ知識を補充できる研修、セミナー、講義などが紹介されています。
https://security-portal.nisc.go.jp/#strategiclist

関連法令

【参照：セミナーテキスト6-2-1.】

個人情報保護法

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

【参照：セミナーテキスト6-2-1.】

個人情報を取り扱う時の基本ルール

項番	取扱い種別	ルール
1	取得・利用	・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	・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	・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	・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

<u>個人情報保護法の罰則規定</u>

- 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：セミナーテキスト6-2-2.】

GDPR

GDPR（一般データ保護規則）とは

起源: EU（欧州連合）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。

※1ユーロ：¥158.09（2023/8/27日現在）
2,000万ユーロ：約31.6億円

関連法令

【参照：セミナーテキスト6-2-2.】

GDPRと日本企業の関係

- EU内に物理的拠点がな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

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