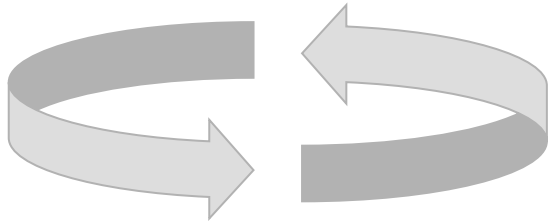
サイバーセキュリティ経営の実践と改善に貢献するセキュリティ監査の力

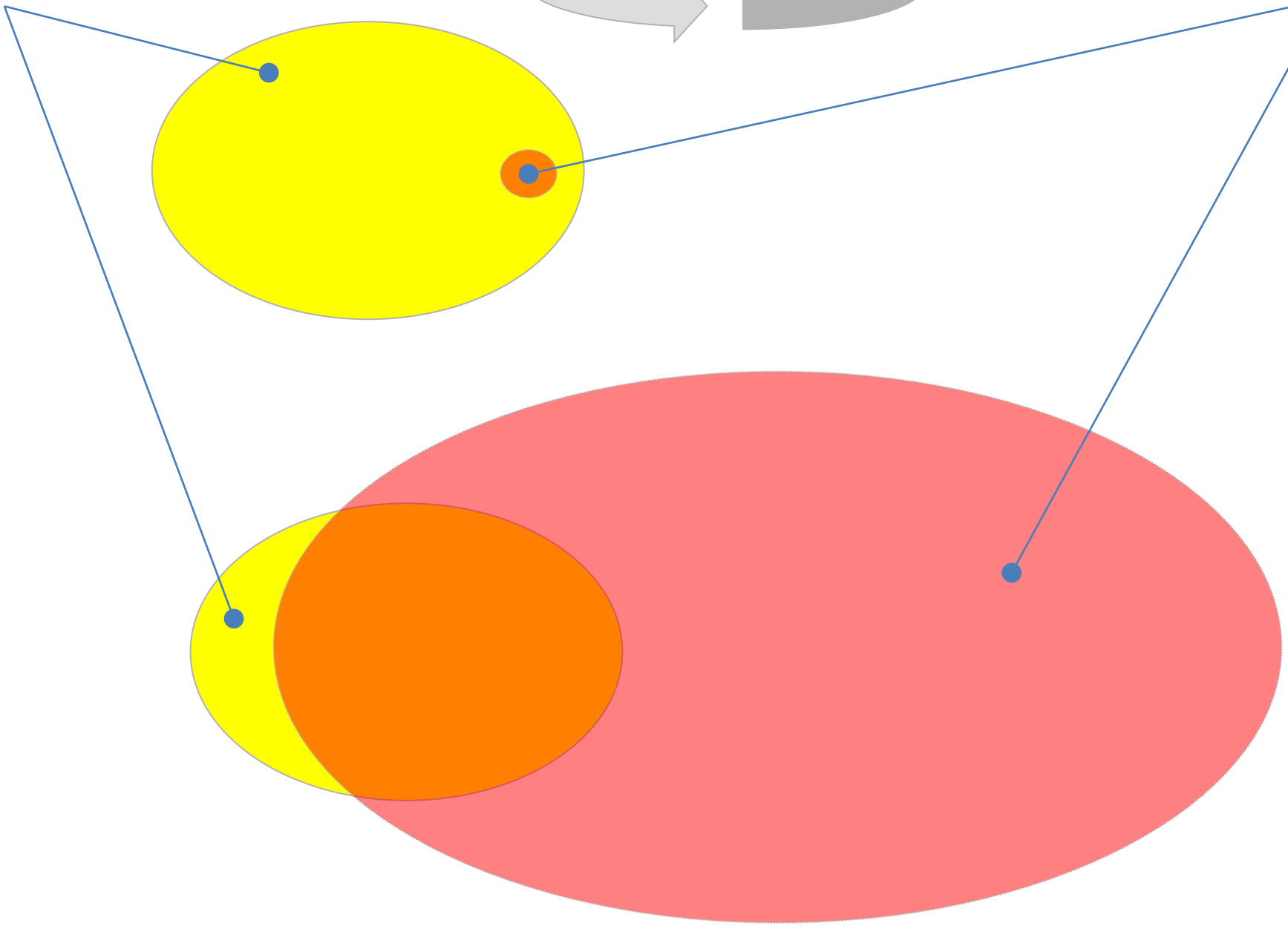
令和５年１０月１０日

上村　昌博
経済産業省
サイバーセキュリティ・情報化審議官

フィジカル空間



サイバー空間



事業活動の変化

フィジカル空間で資源を使い

＋ データを使い

ヒトが事業活動を行い

＋ AIも活動を行い

価値をつくり

反復継続的に客体へデリバリ

＋ 多様なチャネルでコミュニケート

サイバー空間とフィジカル空間の高度融合
～ Society5.0 ～

データ×IT･AI　～ イノベーション創出 ～

新たな付加価値の創出、様々な課題の解決

デジタル技術は経済社会に浸透
存在は当然　自然環境

かつて　自然環境や資源の利用・搾取
考慮せず　影響　相関　持続性
環境問題は、経済成長の制約となった

Society5.0、DX推進において
セキュリティ　意識　影響　対策　可視化
自らの制約となり、瓦解のおそれ

セキュリティ対策は経営マネジメント課題のひとつ

セキュリティは事業推進の大前提
適切なセキュリティ対策を遂行できる組織こそが
一層発展する

環境問題が、今日、GXとして、
成長の原動力となった様に

事業活動の多くはデジタル環境に依存

チャンスと共にリスクも潜む

サイバー空間とフィジカル空間との繋がりの緊密化とともに、セキュリティ事案は拡大、巧妙化、複雑化

IT分野だけでなく、工場等のOT分野でも、サイバー分野での脅威が顕在化

影響は一組織に留まらず、サプライチェーンを構成するあらゆる組織に及び得る
今や、いかなる組織でも被害者となる可能性

事業が提供する価値に影響を与え得るように

大事になる　情報の保全
デジタル環境に支えられたシステムの安定稼働

影響の極小化には、部門横断的な対応が鍵

組織の目的達成には、セキュリティリスクの、適確なマネジメントが重要

コーポレートガバナンスとして、セキュリティやサプライチェーン対策など事業環境の状況を、経営戦略に適切に反映させよう、との動き

「グループ・ガバナンス・システムに関する実務指針」、「投資家と企業の対話ガイドライン」、「デジタルガバナンスコード」

２０１９年　　２０２１年　　２０２２年

経営者のリーダーシップの下、セキュリティ対策を推進していくことが重要

「サイバーセキュリティ経営ガイドライン」を策定

（経済産業省・（独）情報処理推進機構(IPA)）

平成27(2015)年12月28日策定
平成28(2016)年12月　8日改訂(Ver1.1)
平成29(2017)年11月16日改訂(Ver2.0)
令和　5(2023)年　3月24日改訂(Ver3.0)

組織への社会的要請に応えるため、セキュリティに関する、適切な投資や対策の実践を促進

サイバーセキュリティ経営ガイドライン

Ver 3.0

経済産業省

独立行政法人　情報処理推進機構

目次

サイバーセキュリティ経営ガイドラインと支援ツールに係る情報掲載先

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

経営者が認識すべき３原則

（１）サイバーセキュリティリスクが**自社のリスクマネジメントにおける重要課題である**ことを認識し、自らの**リーダーシップのもとで対策を進める**

- 企業活動におけるコストや損失を減らすためにも必要不可欠な投資(事業活動、成長に必須な費用)
- サイバー分野の残留リスクを自社の許容水準以下まで低減することは経営者の責務

（２）責務を全うするには、自社のみならず、**国内外の拠点、ビジネスパートナーや委託先等、サプライチェーン全体にわたる目配りが必要**

- 従来の部品調達のかたちに止まらず、デジタルを介した外部との繋がり全てが含まれ、 時々刻々と変化
- 総合対策の徹底、顧客や社会からの信頼のため、全体のリスク低減が、参加する全ての経営層の責務

（３）平時及び緊急時のいずれにおいても、**関係者との積極的なコミュニケーション**が必要

- 不信感の抑制、緊急連絡の円滑化、初動体制を早め、円滑な対外説明を可能にする

経営者がCISO等に指示すべき１０の重要事項

リスク管理体制の構築	指示 1　組織全体での対応方針の策定 指示 2　管理体制の構築 指示 3　予算、人材の確保
リスクの特定と対策の実装	指示 4　リスクの把握と対応計画の策定 指示 5　リスクに対応する仕組の構築 指示 6　PDCAサイクルによる継続的改善
インシデントに備えた体制構築	指示 7　緊急対応体制の整備 指示 8　事業継続・復旧体制の整備
サプライチェーンセキュリティ	指示 9　サプライチェーン全体の状況把握と対策
関係者とのコミュニケーション	指示10　情報収集、共有及び開示の促進

サイバーセキュリティを巡る環境は常に変化
対応は不断の継続と進化・発展

組織の　経営リーダーシップ　その組織力は
価値の創出と　その持続可能化に　大きく寄与

- 自分ゴト化　　一人ひとりの責任感　参画と対応
- 新たな文化の創出　　価値観　信念　態度
- 集合知 複合的な力　　横断的な連携

サイバー空間の発展は、今後とも、多種多様な組織の力に大きく依拠
他方、サイバー脅威はますます増大

取組がきちんと機能するようにしていくことが大事
セキュリティ監査へのニーズと期待

セキュリティ監査へのニーズと期待

☆政府機関等のサイバーセキュリティ対策のための統一基準

独立性を有する者による**情報セキュリティ対策の監査**を実施することが必要

☆サイバーセキュリティ経営ガイドライン

指示６　PDCA サイクルによるサイバーセキュリティ対策の継続的改善

- ✓ **サイバーセキュリティに関する監査**を実施し、
  その結果を踏まえ、サイバーセキュリティ対策を適時見直している

- ✓ 必要に応じ・・・**情報セキュリティ監査等の外部サービス**を利用し、
  現状のシステムやサイバーセキュリティ対策の問題点を検出し、改善を行う

指示９　サプライチェーン全体の状況把握と対策

- ✓ 業界事情や役割分担、相手先の対応能力等の状況を踏まえつつ、参加企業の合意の下、
  各企業が実施すべき対策を定め、**監査**又は自己点検等の実施を通じ実効性担保

- ✓ 対策担保の手段として、第三者による評価検証結果の活用
  （認証制度の活用、**助言型外部監査**の実施等）。

☆デジタルガバナンスコード2.0

１．ビジョン・ビジネスモデル

２．戦略

2-1．組織づくり・人材・企業文化に関する方策

2-２．IT システム・デジタル技術活用環境の整備に関する方策

３．成果と重要な成果指標

４．ガバナンスシステム

- 経営者は、戦略実施に当たり、リーダーシップを発揮するべき
- 経営者は、DXにおける課題を把握・分析し、戦略の見直しに反映していくべき
- 経営者は、事業実施の前提となるサイバーセキュリティリスク等に対しても適切に対応すべき

→　戦略実施の前提となるサイバーセキュリティ対策の推進については、

✓ サイバーセキュリティ経営ガイドライン等に基づき対策を行い、**セキュリティ監査（内部監査を含む）を行っている**ことの説明文書等の提出をもって確認

☆工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン

セキュリティ対策企画・導入の進め方

ステップ1 **内外要件（経営層の取組や法令等）や業務、保護対象等の整理**

ステップ2 **セキュリティ対策の立案**

ステップ3 **対策の実行と見直し（PDCAサイクル）**

維持・改善面のセキュリティ対策

- 対策の実施・運用状況とその効果の確認
- 工場システムを取り巻く環境変化に関わる情報収集
- BC／SQDC 確保の観点も踏まえ、対策を評価、見直し、更新

→ **監査**の形で、独立した専門的な立場から、リスクマネジメントに基づき、セキュリティ対策の実施・運用状況を確認・評価する手法もあり、**見直しにおいて監査の手法を活用している企業もある**

サプライチェーン対策

- 取引先や調達先に対するセキュリティ対策の要請、対策状況の確認
- 工場システムの脅威、影響度、対応状況**（内部及び/または外部監査実施など）**を把握できている

☆ 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 2023年4月）

点検と改善：　計画した対策が、本当に実行されているか、見落としている対策はないか、対策がセキュリティ事故防止のために役立っているか確認・改善

営業秘密や個人情報等の特に十分な対策が必要な場合には、**第三者による情報セキュリティ監査の実施も検討**

付録6:クラウドサービス安全利用の手引き

【クラウドサービス選択時に参考となる制度例】

- **クラウド情報セキュリティ監査制度**
  （特定非営利活動法人日本セキュリティ監査協会）
- **ISMAP（イスマップ）**
  （政府情報システムのためのセキュリティ評価制度）

☆デジタルスキル標準（DSS） (経産省･IPA　2022.12 ver1.0, 2023.8 ver1.1)

全てのビジネスパーソン（経営層含む）

＜DXリテラシー標準＞

全ての人が身につけるべき知識･スキル

DXを推進する人材

＜DX推進スキル標準＞

DXを推進する人材類型の役割と習得すべきスキル

生成系AIについても新たに追加

Why
DXの背景

社会、顧客、
競争環境の変化

What
DXで活用される
データ･技術

データ、クラウド、
AI

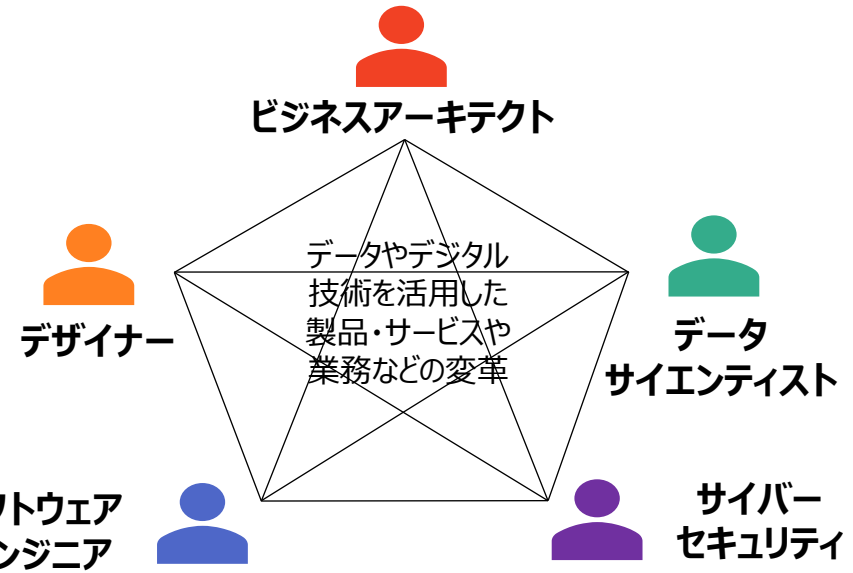
How
データ･技術の
利活用

利活用事例、
留意点

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

サイバーセキュリティマネジャーの役割のための
学習項目例の中に**「情報セキュリティ監査の手法」**



これから、を考える

Software Bill of Materials

IoT Security Label

SP800-171

Cyber Resilience Act

Secure by Design and Default

昭和５６年（１９８１年）
　安対制度　情報処理サービス業対象

平成１３年（２００１年）
　ISMS　全業種対象

平成１５年（２００３年）
　情報セキュリティ管理基準、監査基準　・・・・・　と始まり、
その後の色々な変化の中で・・・・・

そして、これからの時代の変化を見据えて・・・・・

いつ 何を どう みていくか
助言 と 保証
役割分担 と 連携
そして人

祝　情報セキュリティ監査制度　２０周年
これまでのご尽力に心から感謝します

セキュリティが適切に保たれた
透明性ある自由な経済社会を実現
一緒に歩を進めていければ幸い

セキュリティ監査は○○○○○