# 産業横断サイバーセキュリティ検討会（CRIC CSF）
# 活動概要

2024年11月14日

産業横断サイバーセキュリティ検討会

第５期 会長　土佐 泰夫

# 産業横断サイバーセキュリティ検討会について

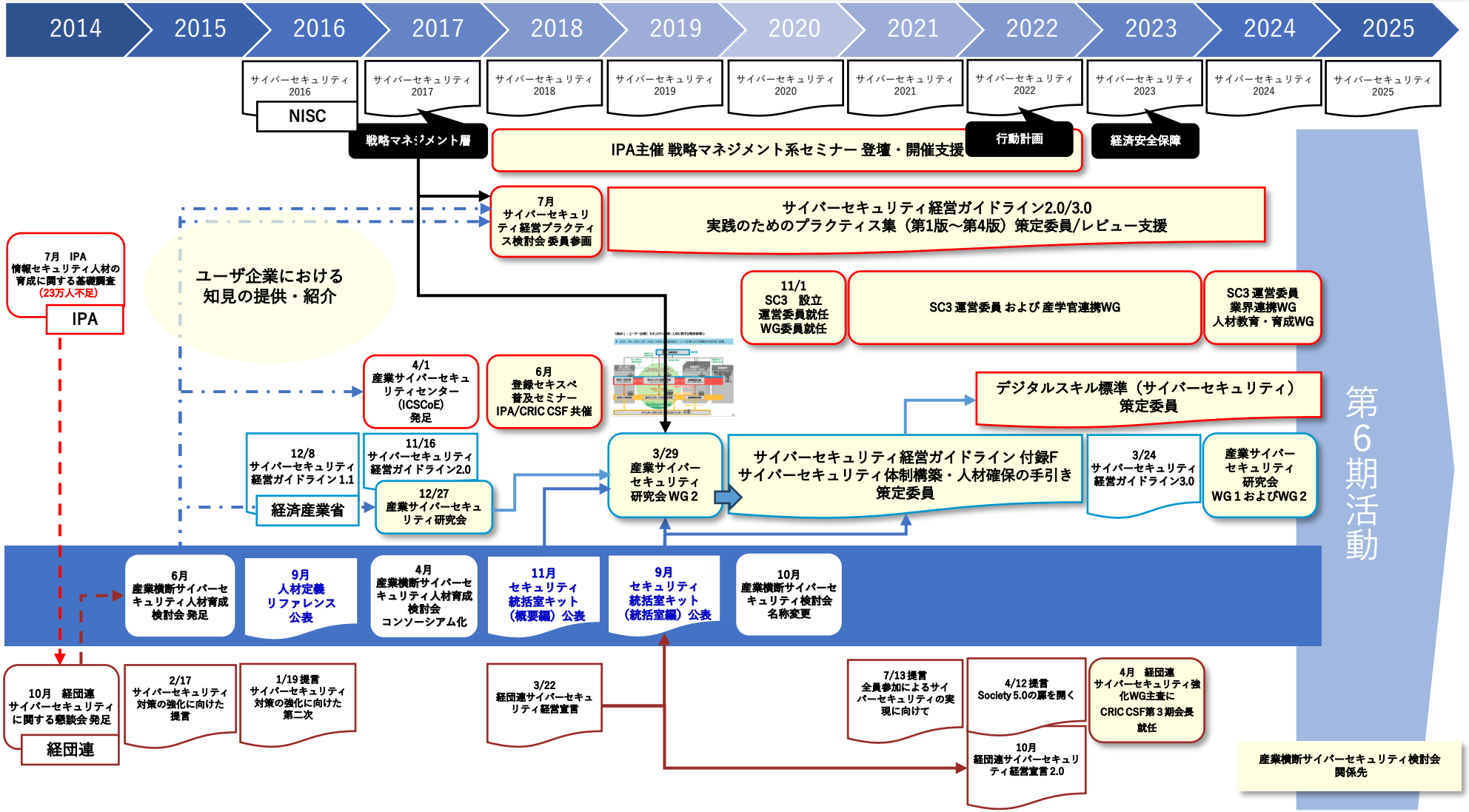
- 経団連傘下「サイバーセキュリティに関する懇談会」の有志企業により、2015年6月9日「産業横断サイバーセキュリティ人材育成検討会」として発足
- オリパラに向けたセキュリティ対応体制強化を目途に、産官連携による施策展開や、ユーザ企業視点でのセキュリティ人材活用のためのドキュメント等を策定し公開
- 2020年10月より、名称を「産業横断サイバーセキュリティ検討会」に改め、人材育成のみならずユーザ企業が直面するセキュリティ課題について幅広く対応

**業界の壁を越えた信頼の輪に基づく情報共有、及び産官学連携の活動を通じて得られたセキュリティ課題の解決を目指し、国内外で活発に活動を行っていく**

| | |
|---|---|
| 業界横断でのクローズドな情報交換 | ・平場では話せない事例/ナレッジの共有、議論<br>・有識者を交えたWGでのインテリジェンス勉強会 |
| 産業界代表として政府／経団連会合等へ参画 | ・産業サイバーセキュリティ研究会WG<br>・SC3、サイバーセキュリティに関する懇談会　他 |
| 公的機関にも採用・引用される成果物 | ・人材定義リファレンス<br>・セキュリティ統括室キット　他 |
| 国内外での積極的な活動実績 | ・米NISTカンファレンスでの講演<br>・IPAセミナーへの協力　他 |

# 産業横断サイバーセキュリティ検討会のあゆみ

## 発足から第５期まで活動状況



# 第５期 活動方針

■ **産業界ならではの知恵と知識と実行力を結集し、関係省庁・団体と連携しながら、我々にしか創りえない協創環境を維持発展させるとともに、様々な情報発信を行っていきます**

■ **第5期（2022年10月～2024年9月）の活動方針**

1. サイバーとフィジカルが融合していく中で、社会インフラおよびサプライチェーンを維持し産業界が発展していくための基盤となる**「信頼の輪」**の拡大
2. DXの推進と安全なサイバー空間の維持を実現するために必要な、最新技術から法規制国際情勢等に至る様々な情報、知見、対策、施策の**共有**
3. 産業界におけるセキュリティ人材のさらなる活躍に向けた、人材像、役割、機能の見直しと**産学官連携**による人材育成システムの確立

# 産業横断サイバーセキュリティ検討会　活動のスコープ

## サプライチェーン・サイバーセキュリティ

- ✓ **会員企業ごとにサプライチェーンが異なる産業横断の特徴**を生かしたサイバーセキュリティの検討
- ✓ **調達先や販売・提供先が国内に限定されない事業展開を前提**としたのサイバーセキュリティの検討

## 重要インフラ事業者のサイバーセキュリティ

- ✓ 省庁等による産業界への要求を確認し、**グループガバナンス及びサプライチェーンの観点**を踏まえた**効率的なセキュリティ運用**に関する情報共有。
- ✓ **重要インフラ事業者として求められるサイバーセキュリティ**と**デジタルトランスフォーメーション（DX）に求められるサイバーセキュリティ**の共通項目や差異についての意見交換。

## 経済安全保障及び各国サイバーセキュリティ動向

- ✓ 会員企業の約半数は、経済安全保障推進法第50条第１項及び第２項の規定に基づく**特定社会基盤事業者**であることから、法人組織としての実施事項及び対応実務に関する情報共有。
- ✓ 米国、欧州、中国等におけるサイバーセキュリティ関連法規制が実務レベルで運用されている現状に対して、**外部有識者を招聘した情報収集の機会**の定期開催。

## ユーザ企業の組織と事業を守るためのサイバーセキュリティ

- ✓ 上記、様々なセキュリティ課題に対して、**セキュリティ統括機能のあり方**を再整理し、**ユーザ企業におけるサイバーセキュリティ人材が活躍できる環境**の整備に関する情報発信を行う。
- ✓ 情報処理安全確保支援士の活躍など、**産学官連携による検討の機会への参画及び改善に向けた提言等**を行う。

# 第５期 活動体制

会長・副会長
運営会議

事務局

## WG1

**セキュリティ経営戦略検討WG**

主な活動内容
- セキュリティ統括室等の検討
- 人材定義リファレンスの改定
- サプライチェーン・セキュリティに関する討議

活動成果
- **サイバーセキュリティ経営ガイドライン 付録F** 策定支援
- **ITSS+(サイバーセキュリティ領域)** 策定支援
- **デジタルスキル標準（サイバーセキュリティ）** 策定支援
- 人材定義リファレンスの公表、NISTカンファレンス発表

## WG2

**Security Study Meetup**

主な活動内容
- 勉強会の企画・運営
- 懇親会の企画・運営
- 外部講師の選定・調整等

過去に開催した勉強会テーマ
- **EUサイバーレジリエンス法**
- **EU AI規制**
- **海外プライバシー法規制動向**
- **ランサムウェア被害対処**
- **DFFTとデジタルトラスト**
- **アタックサーフェスと格付け**
- **脅威インテリジェンス**

## WG3

**情報連携・ナレッジ共有WG**

主な活動内容
- インシデント事例に対する意見交換
- 各社の事例発表、対策共有

主な活動
- WG3の活動は会員企業限定としており、**内容は非公開**です。
- ユーザ企業が集まりサイバーセキュリティをテーマとして意見交換をする珍しい活動を行っております。

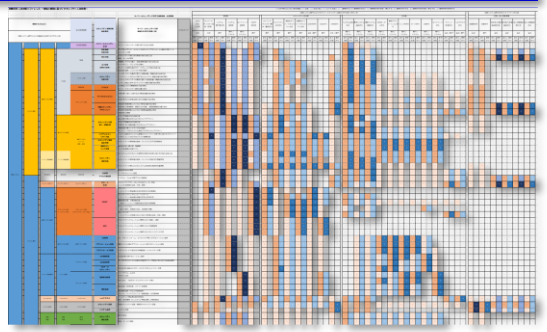
# 産業横断サイバーセキュリティ検討会　対外連携（第3期～第5期の主な活動）

**ユーザ企業による「現実的な課題検討」を通じて得られた知見を、政府省庁、他団体の取り組みに活用頂いております。**

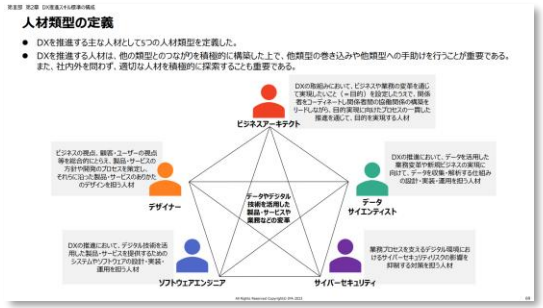
| 関係団体・省庁 | 関係組織 | 活動先 | 活動内容 |
|---|---|---|---|
| 経団連 | サイバーセキュリティ委員会 | サイバーセキュリティ強化WG | 共催：セキュリティ経営者サミット |
| 経済産業省 | サイバーセキュリティ課 | 産業サイバーセキュリティ研究会 | 研究会WG1 / 各種SWG |
| | | | 研究会WG2 / 非公式勉強会 |
| | | セキュリティ経営・人材確保の在り方検討TF | サイバーセキュリティ経営ガイドライン付録F |
| | | デジタル時代の人材政策に関する検討会 | デジタルスキル標準 |
| IPA | 産業サイバーセキュリティセンター | 中核人材育成プログラム | 登壇 / 情報提供 |
| | | 戦略マネジメント系セミナー | 登壇 / 情報提供 |
| | 社会基盤センター | | ITSS+（セキュリティ） |
| | SC3 | 運営委員会 | 団体新設時の活動支援（国際WG等） |
| | | 業界連携WG | サプライチェーンサイバーセキュリティ成熟度モデル検討SWG |
| | | 人材教育・育成WG | 共通語彙集/職務記述作成ツール |
| NISC | 基本戦略G | 普及啓発・人材育成専門調査会 | プラス・セキュリティ等の議論 |
| | サイバーセキュリティ協議会 | サイバー攻撃・・・ガイダンス検討会 | 情報共有・公表 |
| 総務省 | サイバーセキュリティ統括官室 | | （意見交換） |

# DX推進とサプライチェーンの維持のためのリファレンス改定

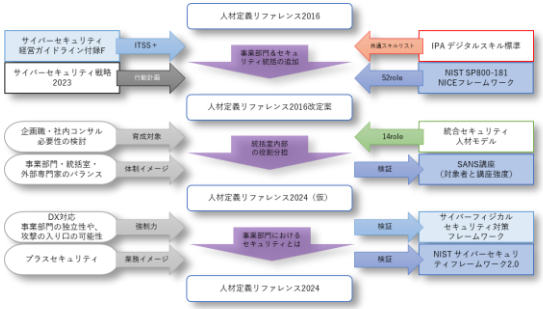
- ✓ 2016年、米国NIST Cybersecurity Framework1.1を活用し、日本企業の組織体制整備の考え方に基づく、**ユーザ企業のためのセキュリティ体制**をリファレンスとして公開しました。
- ✓ 現在、**サイバーセキュリティ経営ガイドライン3.0**が公表され、2024年には**NIST Cybersecurity Framework2.0**が重要インフラ事業者だけではなく全ての事業者を対象として公開されることが決定しており、**NIST公式WEBに紹介されている産業横断サイバーセキュリティ検討会**の取り組みも更新を検討する時期となっております。
- ✓ そこで、第五期後期の末を目指し、本紙の活動のスコープで紹介しました**様々なセキュリティ課題に取り組むために必要とされる組織体（セキュリティ統括室等）を再定義し、包括的な全社セキュリティ体制のモデル**として、新たなリファレンスの公開を目指すものです。
- ✓ 尚、検討にあたっては、様々な要素（サイバー空間におけるサプライチェーンや、ゼロトラストの取り組み等）を加味し、IPA デジタルスキル標準の共通スキルリストなどの国内で議論が進む枠組みを参考にしながら、**ユーザ企業が集まる産業横断らしいセキュリティ体制及び人材のあり方**を提示していく所存です。



CRIC CSF 人材定義リファレンス 2016年度版




IPA/METI　デジタルスキル標準 ver.1.1




人材定義リファレンス 改定プロセス

# 人材定義リファレンス改定に向けた課題認識

## ◘ 法人組織を守るためのサイバーセキュリティの取り組みは広がり続けている。

### 1. 国境を越えて広がる情報資産と国境を越えてアクセスされる情報資産に対する安全性の確保

- IT／OT／IoT ／AI それぞれに対するセキュリティ実装とルールの進化と深化が必要。

### 2. DX や AI に代表されるデジタル技術のビジネス利用拡大への対応

- ITガバナンスの強化と、社員によるデジタル技術の利活用の自由度のバランスの追求が重要。

### 3. 狙われるシステム管理者を守るための様々な取り組み

- 重要システムおよび重要データに対するサイバー空間を通じた侵害行為への対処に向けた知見共有。

### 4. 分業やAI活用により高度化する攻撃者への対応に求められる知見の集約

- 便利さを悪用される前提で考えるレジリエンスを追求したサプライチェーン・サイバーセキュリティ。

### 5. サプライチェーン全体での協調関係を構築するための法人としての責任体制

- 社内やグループ内に留まらないインシデント対応を効果的に進めるためのプロアクティブな信頼構築。

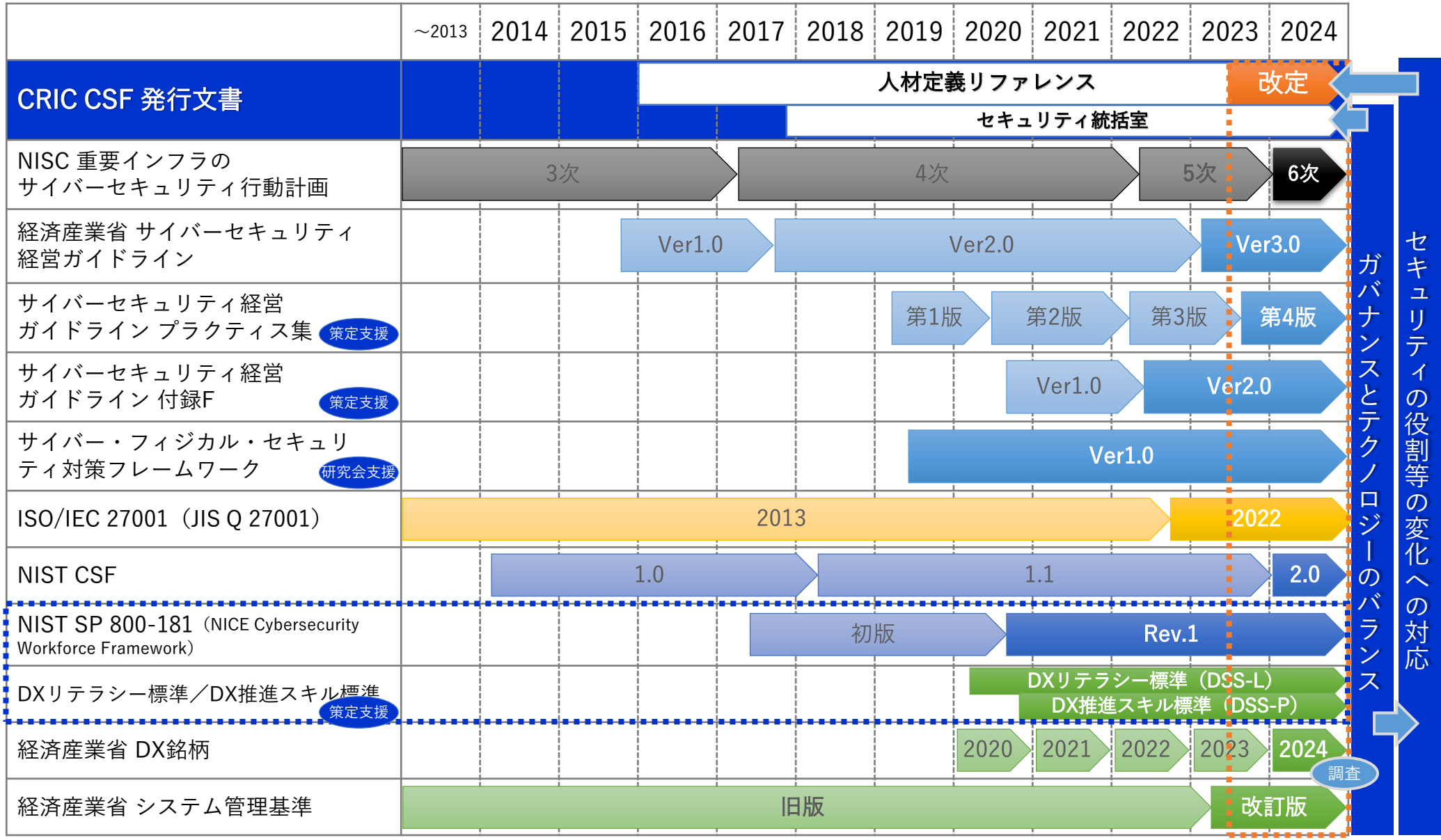
### 6. 取引先、政府省庁および投資家等との適切なリレーションとコミュニケーション

- 自助・共助・公助を意識し、説明責任を果たすことのできる情報共有のあり方。

### 7. 高度なセキュリティ要求にも耐えられる組織、役割、人材のあり方

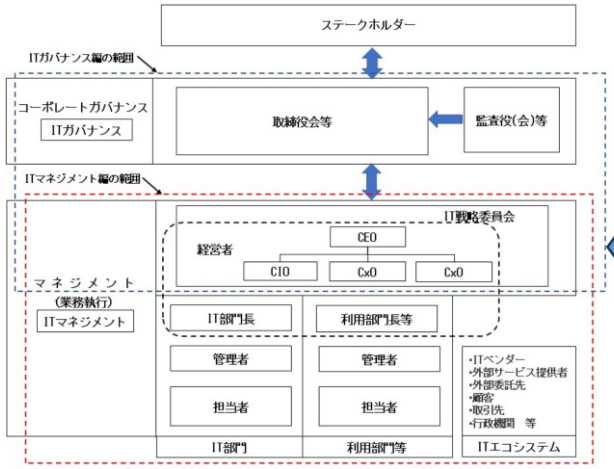
- 上場企業および重要インフラ事業者には強く要求されるデータの「機密性」の確保を多面的に検討。

# 人材定義リファレンス改定に向けた各種リファレンス

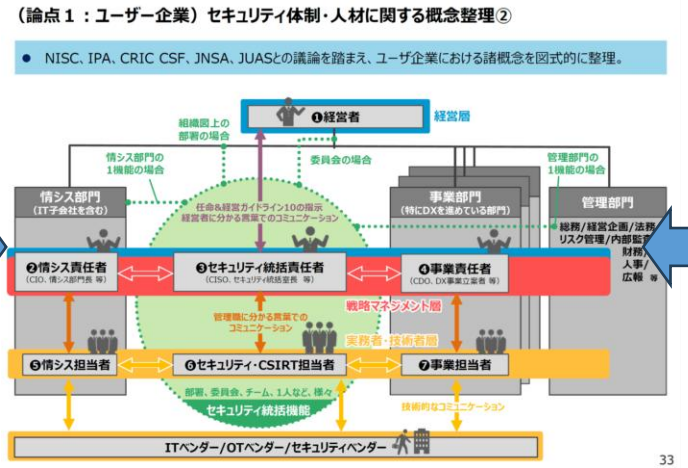


# 人材定義リファレンスの検討モデル①

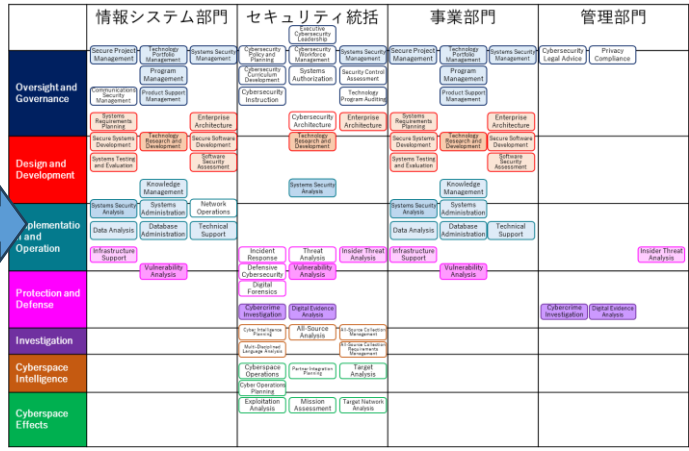
## ◘ 様々な体制モデル



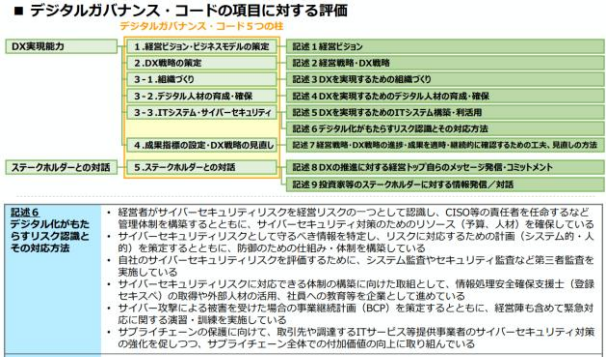

「システム管理基準」が想定する組織体の体制




第4回 産業サイバーセキュリティ研究会 ワーキンググループ2
（経営・人材・国際）資料3　事務局説明資料

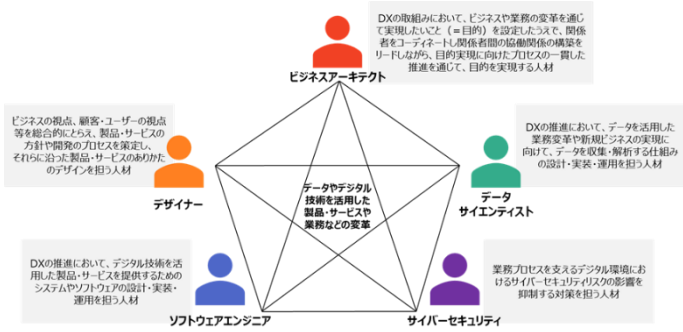



セキュリティ体制・人材に関する概念整理に基づく
NIST SP 800-181マッピング




デジタルトランスフォーメーション調査（DX調査）2025

**人材定義リファレンス**
**2024**




「DX推進スキル標準」の人材類型の定義

# 人材定義リファレンスの検討モデル②

Oversight and Governance | Implementation and Operation | Investigation
Design and Development | Protection and Defense | Cyberspace Intelligence | Cyberspace Effects

凡例：NICEフレームワークとの関係性

## ◘ 第6期 検討を進める体制モデルと役割分担（たたき台）


凡例：技術PF（技術ポートフォリオ）
Pg管理（プログラム管理）

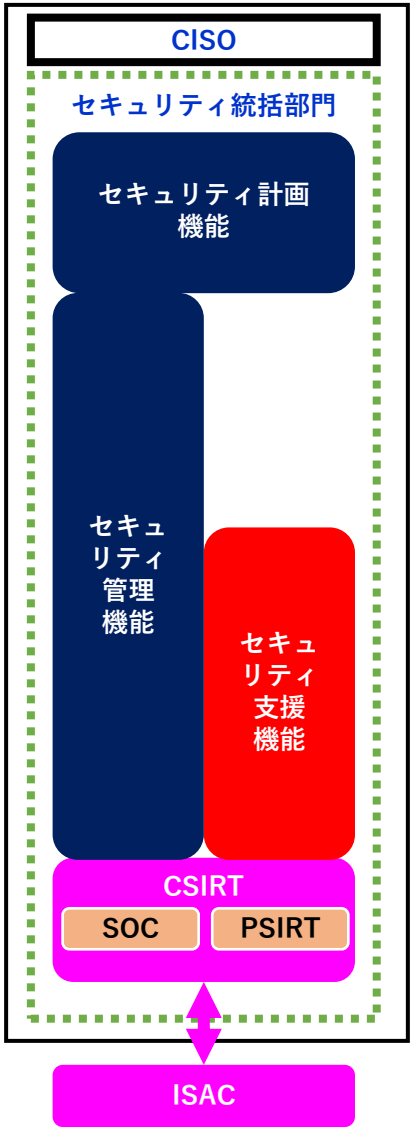
# 人材定義リファレンスの検討モデル③

Oversight and Governance | Implementation and Operation | Investigation
Design and Development | Protection and Defense | Cyberspace Intelligence | Cyberspace Effects

凡例：NICEフレームワークとの関係性

## ◘ 第6期 検討を進める体制モデルと役割分担（AI導入検討例）


要約例




凡例：技術PF（技術ポートフォリオ）
Pg管理（プログラム管理）

# お問い合わせ

当検討会へのご入会、ご意見、ご質問等がございましたら、以下よりお知らせください。

後日、事務局よりご連絡させて頂きます。

## ◘ お問い合わせ先

一般社団法人サイバーリスク情報センター

産業横断サイバーセキュリティ検討会　事務局

WEB　https://cyber-risk.or.jp/

Mail　office@cric-csf.jp