

ISACA東京支部CISMカンファレンス

# 経営戦略としてのセキュリティマネジメント

2025年2月15日

日本電気株式会社 Corporate Executive CISO

兼 サイバーセキュリティ戦略統括部長

兼 NECセキュリティ株式会社 取締役

淵上 真一, CISSP

## 淵上 真一



日本電気株式会社

Corporate Executive CISO

兼 サイバーセキュリティ戦略統括部長

兼 NECセキュリティ株式会社 取締役

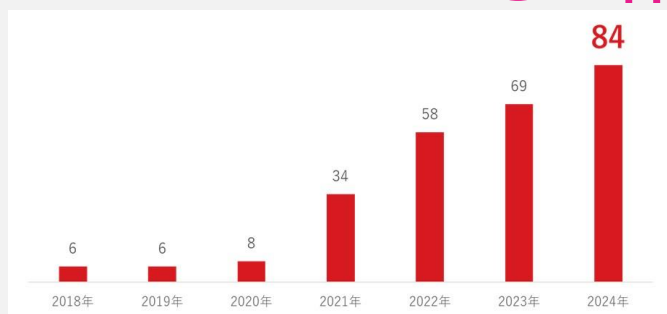
ベンチャー系システムインテグレータでのネットワークエンジニアを経て、専門学校グループを運営する学校法人に転職  
教員経験を経て、セキュリティ担当の役員として経営に参画  
社外では司法、防衛関連のセキュリティトレーニングを手掛ける  
2018年よりNEC NECグループ全社セキュリティ統括を担当

- ISC2 認定主任講師
- Cisco Networking Academy Instructor Trainer
- 情報処理安全確保支援士 集合講習認定講師
- 北海道大学 客員研究員
- サイバー安全保障人材基盤協会 理事
- 日本情報経済社会推進協会(JIPDEC) 評議員
- 警察大学校 嘱託講師
- Hardening Project 実行委員

# サイバーセキュリティ動向

## 2024年に国内組織が公表したランサムウェア被害件数

84件



「RansomHub」をはじめとした、新興ランサムウェアグループによる被害が2024年下半年から急速に拡大。

(2025/01/08、TrendMicro)

## 2024年12月のフィッシング報告数が過去最多23万超

日本国内のフィッシング報告数・URL件数がともに過去最多を更新。URL件数は約12万件。  
なりすまし送信の割合は大きく減少したものの、適切なDMARC構成でないドメインへのなりすまし報告が続いている。



## 2023年1月以降のフィッシング報告推移

画像引用: SecurityNEXT

(2025/01/17、フィッシング対策協議会)

## ランサムウェア被害経験企業の過去3年間の平均累積被害額




2.2億円



(2025/01/08、TrendMicro)

# サイバー攻撃は経済利得を目的とした犯罪に

## 2023年 名目GDP

1位		27.4兆ドル
2位		17.7兆ドル
3位		4.5兆ドル
4位		4.2兆ドル

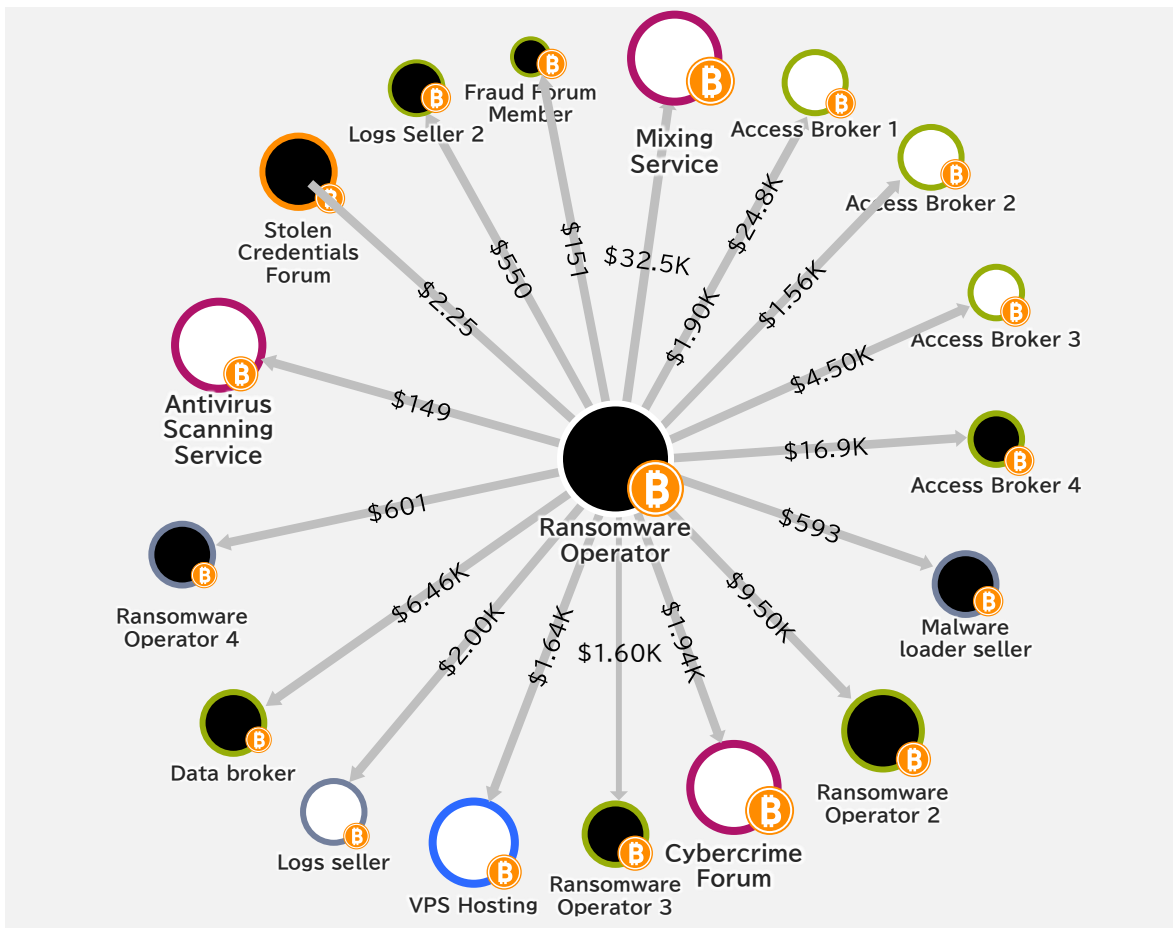


サイバー攻撃による被害額は  
2023年 名目GDP比較で  
世界3位規模  
8.0兆ドル

各国GDPIは内閣府発表 サイバー攻撃による被害額  
<https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/>

# ランサムウェアの資金の分析

## 複数の初期アクセスブローカー等を活用するRaaSのエコシステムが確立



Ransomware Payments Exceed \$1 Billion in 2023, Hitting Record High After 2022 Decline  
<https://www.chainalysis.com/blog/ransomware-2024/>

## ランサムウェアエコシステム

### あるランサムウェアオペレーター(アフィリエイト)の送金先は20か所近くに

初期アクセスブローカー(IAB)4人、マルウェアローダーの販売者他のランサムウェアオペレーター3人、暗号資産ミキシングサービスデータブローカー、VPSホスティング業者、犯罪フォーラムなど

資金洗浄には集中型取引所のほか、ミキサー、ブリッジ、インスタントエクスチェンジャー、ギャンブルサービス等を使用

# サイバー脅威予測



攻撃の成功確率を高めるための**手間**を惜しまない



**創造性**をもって業務プロセスの中に自然な形で入り込む

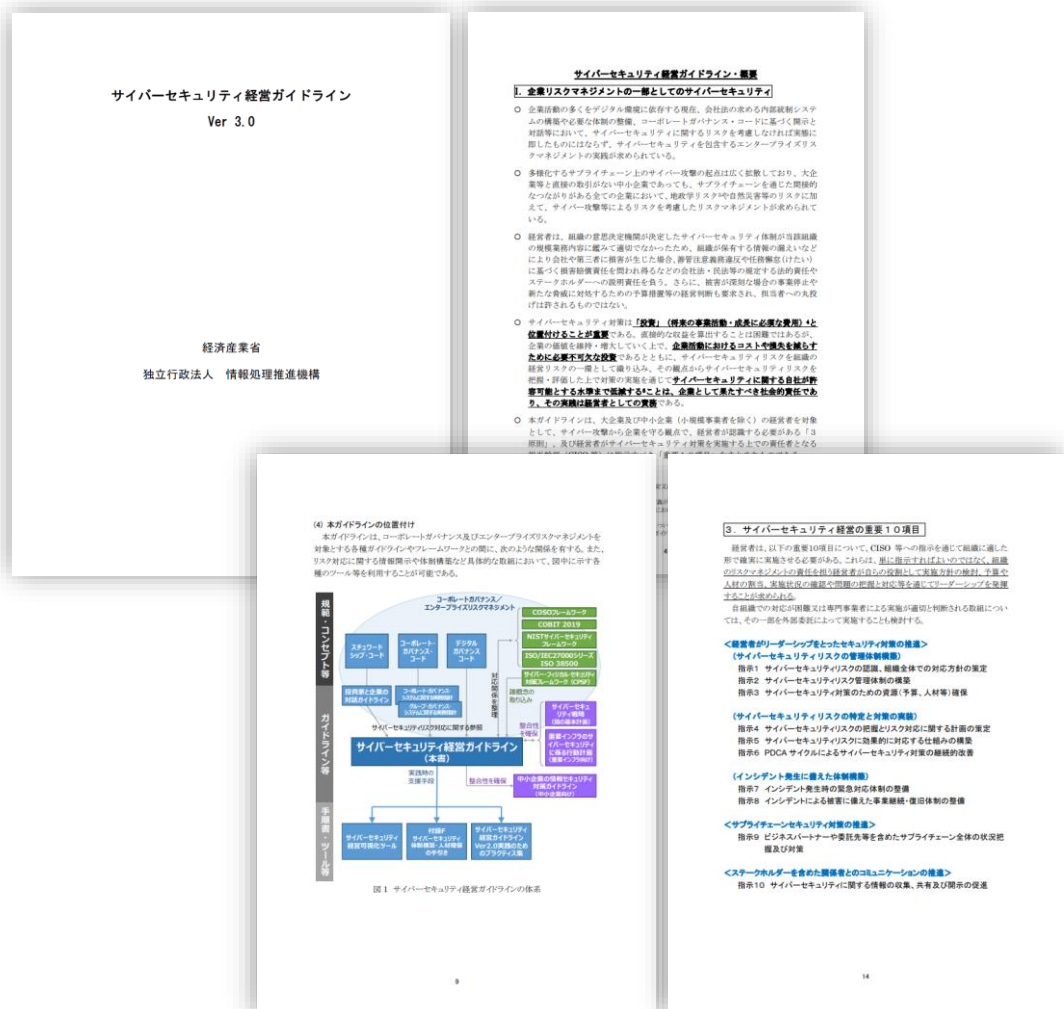


生成AIを悪用した攻撃の**底上げ**が進み、AIエージェントによる効率を高める工夫も



攻撃者サイドの活動や主張を**検証・追求**し、信頼を低下させる

# サイバーセキュリティ経営ガイドライン ver3.0 2023年3月23日



[20230324002-1.pdf](https://www.meti.go.jp/20230324002-1.pdf)  
([meti.go.jp](https://www.meti.go.jp/))

## 概要

経済産業省とIPAが共同で策定した  
企業向けのセキュリティガイドライン

国内企業において経営者の主導のもとで  
組織的なサイバーセキュリティ対策を  
実践するための指針

## 構成

国内企業間でサイバーセキュリティ対策を  
行う際の共通言語

- 「経営者が認識すべき3原則」
- 「サイバーセキュリティ経営の重要 10 項目」

2015/12/28 サイバーセキュリティガイドライン ver1.0  
2016/12/08 サイバーセキュリティガイドライン ver1.1  
2016/11/16 サイバーセキュリティガイドライン ver2.0

# サイバーセキュリティ経営ガイドライン概要改訂ポイント

## Ver2.0

セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必要なものと位置づけて「投資」と捉えることが重要

セキュリティ投資は必要不可欠かつ経営者としての責務

経営責任や法的責任が問われる可能性がある

## Ver3.0

サイバーセキュリティ対策は「投資」(将来の事業活動・成長に必須な費用)と位置付けることが重要。企業活動におけるコストや損失を減らすために**必要不可欠な投資。**

サイバーセキュリティリスクを把握・評価した上で、対策の実施を通じてサイバーセキュリティに関する**自社が許容可能とする水準まで低減する**ことは、企業として果たすべき社会的責任であり、その実践は経営者としての責務。

善管注意義務違反や任務懈怠に基づく**損害賠償責任を問われ得る**などの会社法・民法等の規定する法的責任やステークホルダーへの説明責任を負う。



# 重要インフラのサイバーセキュリティに係る行動計画 改訂

## サイバーセキュリティ体制の構築・運用について経営層の責任を明確化

重要インフラの防護を目的に、以下の項目に関する取り組みを示している

1. 「重要インフラ防護」の目的
2. 関係主体の責務
3. 基本的な考え方
4. 障害対応体制の強化

### 重要インフラ分野

情報通信	金融	航空
空港	鉄道	電力
ガス	政府行政サービス	医療
水道	物流	化学
クレジット	石油	

2022年6月17日に5次計画が公表

### ②サイバーセキュリティと取締役等の責任

組織の意思決定機関が決定したサイバーセキュリティ体制が、当該組織の規模や業務内容に鑑みて適切でなかったため、組織が保有する情報が漏えい、改ざん又は滅失(消失)若しくは毀損(破壊)されたことにより会社に損害が生じた場合、体制の決定に関与した**経営層は、組織に対して、任務懈怠(けたい)に基づく損害賠償責任を問われ得る。**また、決定されたサイバーセキュリティ体制自体は適切なものであったとしても、その体制が実際には定められたとおりに運用されておらず、経営層(・監査役)がそれを知り、又は注意すれば知ることができたにも関わらず、長期間放置しているような場合も同様である。個人情報情報の漏えい等によって第三者が損害を被ったような場合、経営層・監査役に任務懈怠につき悪意・重過失があるときは、第三者に対しても損害賠償責任を負う。

IV. 計画期間内の取組/1. 障害対応体制の強化/1.1 組織統治の一部としての障害対応体制  
2. 安全基準等の整備及び浸透

# NIST サイバーセキュリティ フレームワーク



Fig. 3. Steps for creating and using a CSF Organizational Profile

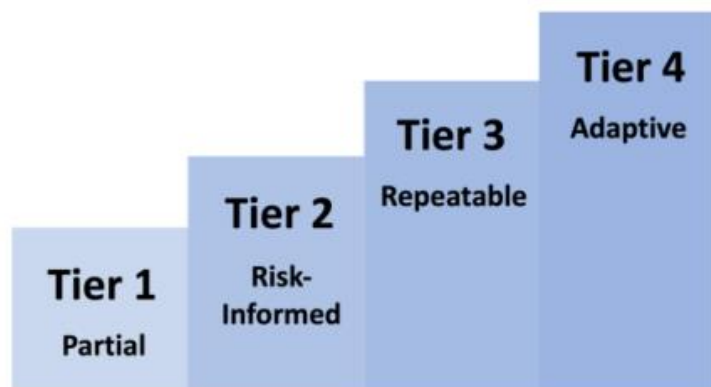


Fig. 4. CSF Tiers for cybersecurity risk governance and management

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

組織がサイバーセキュリティリスクを理解、評価、管理、改善するためのガイドライン、汎用的なフレームワーク

フレームワークコア (Framework Core):

サイバーセキュリティ活動を5つの機能(識別、防御、検知、対応、復旧)に分類し、それぞれに具体的なカテゴリとサブカテゴリを定義。組織が達成すべきサイバーセキュリティの成果を示しています。

フレームワーク実装ティア (Implementation Tiers):

組織のサイバーセキュリティリスク管理の成熟度を4つの段階(部分的、リスク情報に基づく、反復的、適応的)で評価し、組織が目指すべきレベルを明確にする。

フレームワークプロファイル (Framework Profiles):

組織が、ビジネス要件やリスク許容度に基づいて、フレームワークコアのカテゴリやサブカテゴリを優先順位付けし、現状のプロファイルと目標のプロファイルを定義するための手法を提供。

# NIST サイバーセキュリティフレームワーク改訂

NIST サイバーセキュリティフレームワークが10年ぶりの改訂(2024年2月26日)

## 改訂の ポイント

### 適用範囲の拡大

#### 正式名称の変更

変更前

Framework for Improving Critical Infrastructure Cybersecurity



変更後

Cybersecurity Framework

新規機能 Govern(統治)が追加

サプライチェーンマネジメントの強化

# Govern(統治)



Fig. 2. CSF Functions

図: The NIST Cybersecurity Framework (CSF) 2.0

Govern  
機能とは

サイバーセキュリティを  
より広い企業リスク管理(ERM)戦略に  
組み込むために重要

組織の使命や利害関係者の期待をふまえ、  
対策の優先順位をつけ、意思決定を導く

6つの  
カテゴリ

- GV.OC(組織のコンテキスト)
- GV.RM(リスクマネジメント戦略)
- GV.RR(役割、責任及び権限)
- GV.PO(ポリシー)
- GV.OV(監督)
- GV.SC(サイバーセキュリティサプライチェーン  
リスクマネジメント)

## Governが果たす役割:

- ✓ 組織のビジネス目標、ステークホルダーの期待、法的・規制要件を理解し、それらに基づいてサイバーセキュリティ戦略を策定する。
- ✓ サイバーセキュリティリスクを特定、評価、管理、監視するためのプロセスを確立し、組織全体で一貫したリスク管理を実施する。
- ✓ サイバーセキュリティの役割と責任を明確化し、組織全体で説明責任を果たす体制を構築する。
- ✓ サプライチェーン全体のリスクを管理するためのプロセスを確立する。
- ✓ サイバーセキュリティプログラムの有効性を継続的に監視、評価、改善する。

# Governの実現するもの:

## ✓ リスク管理の強化:

組織全体のリスク管理戦略にサイバーセキュリティを組み込み、リスクの特定、評価、および軽減を体系的に実施する。

## ✓ セキュリティ文化の醸成:

セキュリティポリシーの策定、役割分担の明確化、従業員への教育などを通じて、組織全体でセキュリティ意識を高め、セキュリティ文化の醸成。

## ✓ コンプライアンスの遵守:

関連する法令や規制、業界標準への準拠を徹底し、法的リスクやレピュテーションリスクを低減。

## ✓ 事業継続性の確保:

サイバー攻撃による事業中断のリスクを最小限に抑え、事業継続性を確保。

## ✓ ステークホルダーからの信頼獲得:

顧客、取引先、株主など、様々なステークホルダーからの信頼を獲得し、企業価値を高める。

# Governの機能

## 1. ID.GV-1: 組織的背景の理解 (Organizational Context)

### 目的:

サイバーセキュリティ戦略を組織のビジネス戦略と整合させ、適切なリスク判断を行うための基盤を構築する。

### 内容:

組織のミッション、ビジネス目標、ステークホルダーの期待、法的・規制要件、およびサイバーセキュリティリスクとの関係を理解する。

### 具体的な活動例:

ビジネス環境、ステークホルダー、およびその期待の文書化  
法的・規制要件の特定と文書化  
サイバーセキュリティリスクとビジネス目標との関連付け

# Governの機能

## 2. ID.GV-2: リスク管理戦略の確立 (Risk Management Strategy)

### 目的:

組織全体で一貫したリスク管理アプローチを確立し、リスクに基づいた意思決定を行う。

### 内容:

リスク許容度を含む、組織のリスク管理戦略を確立する。

### 具体的な活動例:

リスク許容度の定義と文書化/役割と責任の明確化

リスク評価、リスク対応、リスク監視のためのプロセスの確立

## 3. ID.GV-3: 役割、責任、権限 (Roles, Responsibilities, and Authorities)

### 目的:

サイバーセキュリティプログラムを効果的に運用し、責任の所在を明確にする。

### 内容:

サイバーセキュリティの役割、責任、権限を確立し、組織全体で説明責任を果たす体制を構築する。

### 具体的な活動例:

サイバーセキュリティの役割と責任の定義と文書化

役割と責任を組織全体に伝達/適切な権限の付与



# Governの機能

## 4. ID.GV-4: 方針 (Policy)

### 目的:

サイバーセキュリティに関する組織の基本的な考え方やルールを明確化し、一貫した運用を促進する。

### 内容:

組織のサイバーセキュリティリスクに対応するための、組織全体の方針を確立する。

### 具体的な活動例:

情報セキュリティポリシーの策定と文書化

ポリシーの定期的なレビューと更新/ポリシーの組織全体への周知徹底

## 5. ID.GV-5: サプライチェーンリスク管理 (Supply Chain Risk Management)

### 目的:

サプライチェーンを経由したサイバー攻撃のリスクを低減する。

### 内容:

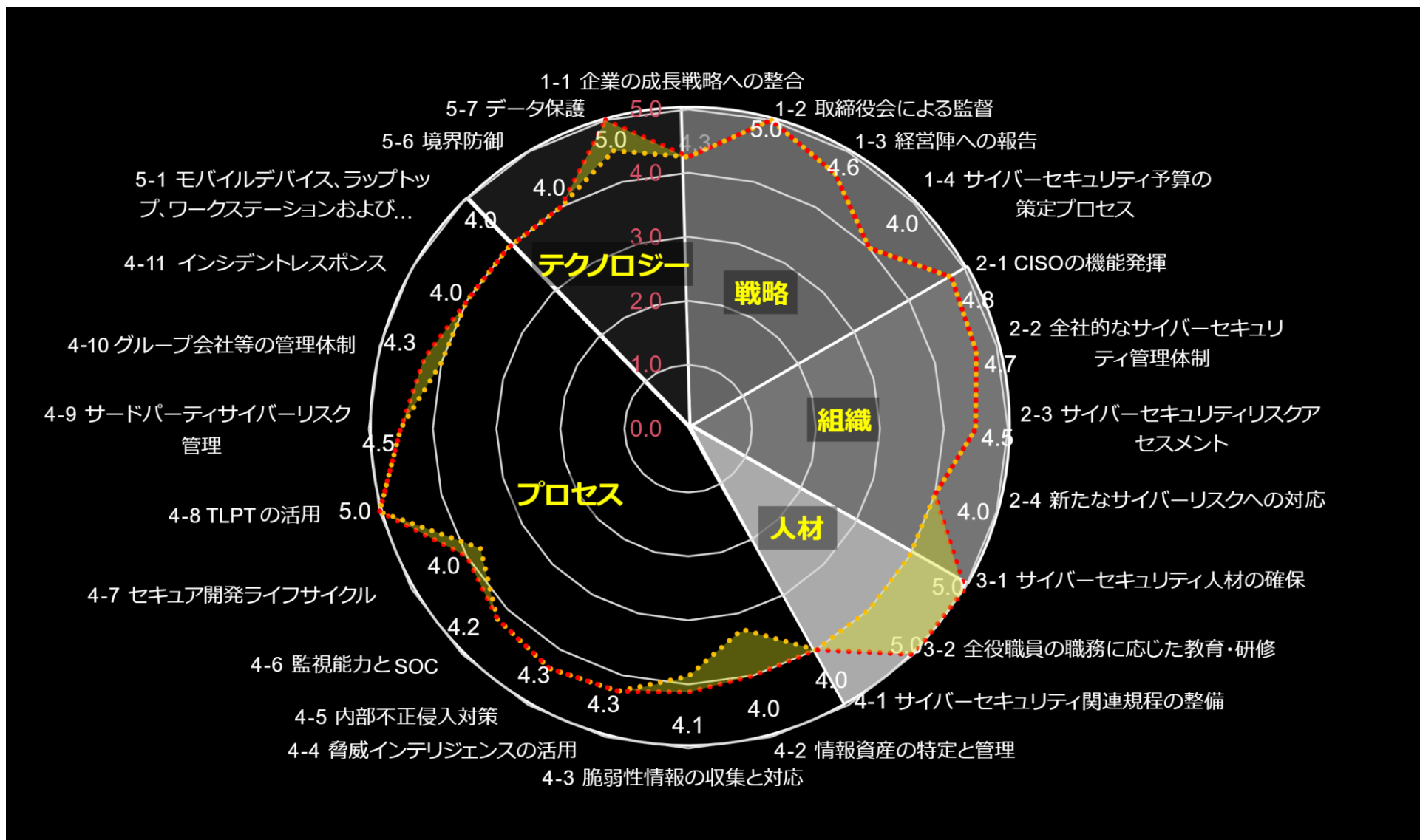
サプライチェーン全体のリスクを特定、評価、管理、監視するためのプロセスを確立する。

### 具体的な活動例:

サプライヤーのセキュリティリスク評価/サプライヤーのセキュリティ対策の監視

サプライヤーとの契約におけるセキュリティ要件の定義

# NIST CSFを利用した評価の事例



An aerial photograph of Tokyo, Japan, featuring the Tokyo Skytree tower prominently in the center. The city is densely packed with buildings, and a river is visible on the left side. The sky is filled with soft, golden light from a setting sun, with scattered clouds catching the light. The overall mood is serene and expansive.

# 成功のカギは組織のサイロ化からの脱出

**NEC**

\Orchestrating a brighter world