

「交通分野へのサイバー攻撃に対する セキュリティ人材育成に関する調査研究」

経営層がとるべきサイバーセキュリティ対策について

学校法人岩崎学園 理事
情報セキュリティ大学院大学 名誉教授
東京大学 名誉教授
田中 英彦

- 現状
 - 国際社会を跨るGAFA問題
 - 国間の攻撃が現実：物理攻撃の前にサイバー攻撃が日常
 - サイバーによるフェイクニュースと世論の制御
 - サイバー攻撃と被害の流布
 - 専守防衛の日本：牽制活動と陸海空に宇宙、サイバー・電磁波
- 情報共有の重要性
 - 情報寡占問題：便利の裏にある寡占の排除、連携による透明性確保
 - 企業間秘密とサイバー攻撃情報の共有問題
 - 情報共有に向けた法制度の担保：攻撃情報・マルウェア共有による対策向上の実施、対策実施及び研究の保護

経営者向けサイバーセキュリティ対策

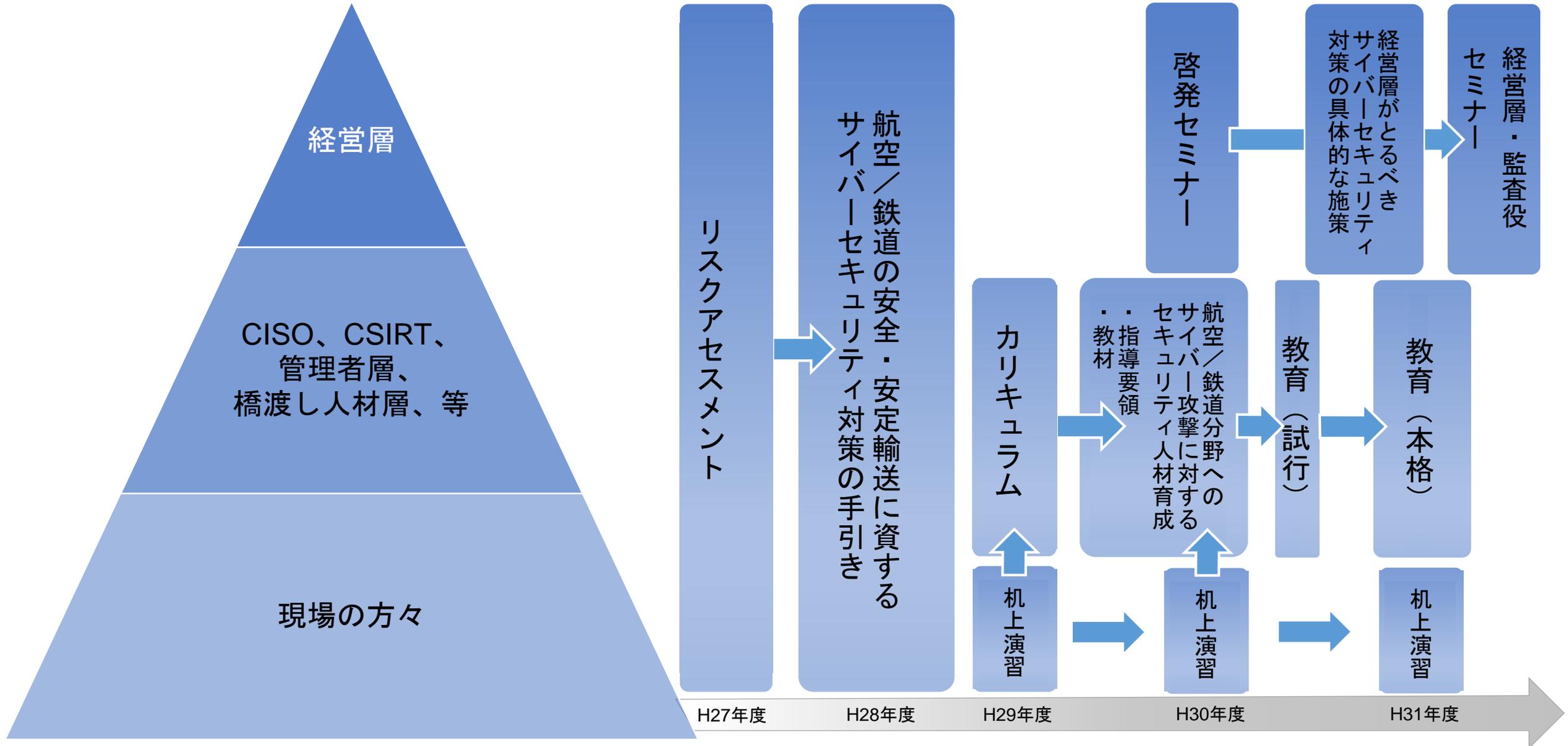
- 情報時代の認識
 - IoEverything, DX, データ/情報の力で経験を置き換える
- リスクの拡大に向けた経営の再考
 - 物理的リスク、論理的リスク（距離・時間・規模越え）
- 膨大な責任を負う経営者の実質的心構えと為すべきこと
 - 善管注意義務にセキュリティも含まれる
 - 必ず実施の最小限/チェック項目
- 目の前にあるオリンピック・パラリンピック
 - 攻撃は必至、既に織り込まれている

本日の内容

1. これまでの主な調査研究

2. 経営層がとるべきサイバーセキュリティ対策について
 - 2-1. 背景
 - 2-2. 目的
 - 2-3. 10の施策案
 - 2-4. 各施策の関係図
 - 2-5. 施策案のポイントと位置づけ
 - 2-6. オリンピック・パラリンピック対策に向けた施策

1. これまでの主な調査研究



2-1 背景

- サイバーセキュリティ対策の必要性：経営層の理解は高まり、経営層が社内で指示すべき対策項目の情報提供が進む
- 一方、対策項目は、全企業で一律に適用できず、対策を実施する上で分野に応じた現実的な心構えと施策を示す必要がある

(例) 政府動向について

インフラ事業者に対策義務付け＝サイバー攻撃、司令塔を新設—自民提言

自民党サイバーセキュリティ対策本部の高市早苗本部長らは14日、安倍晋三首相に首相官邸で会い、サイバー攻撃への対応に関する提言書を手渡した。**重要インフラ事業者に対して対策を義務付ける法律の制定**や、司令塔となる「サイバーセキュリティ庁」の新設を盛り込んだ。

国民生活や経済活動に大きく関わるとして政府が指定する**重要インフラ14分野のうち、現行法でサイバー対策を義務付けられているのは電気とガスの二つだけ**。提言書は、情報通信や金融など**他の分野でも対策**を取ることや、**重大事案が発生した際に遅滞なく政府に報告**することを求めた。

サイバーセキュリティ庁は、中央省庁のサイバー対策を担う内閣官房の「内閣サイバーセキュリティセンター（NISC）」を拡充するもの。大阪・関西万博が開かれる**2025年をめぐりに内閣府の外局として設置**するよう要請した。

(例) 事業被害について①

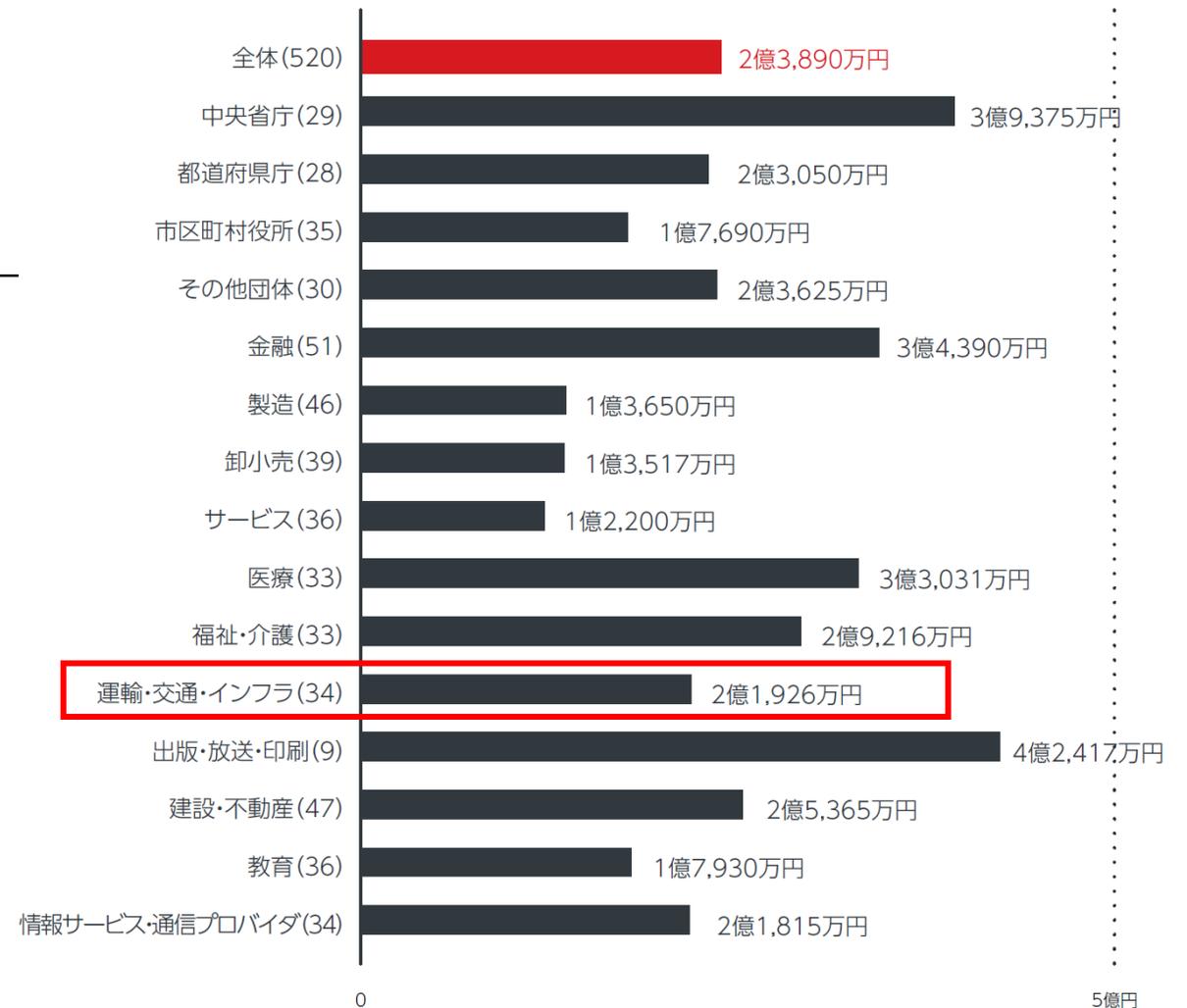
運輸・交通・インフラの年間平均被害総額は、
約2.2億円

トレンドマイクロが2019年6月、国内の民間企業や官公庁自治体を対象に行った「法人組織におけるセキュリティ実態調査2019年版」によると、セキュリティインシデントによる年間平均被害総額は約2.4億円、4年連続2億円を超える結果と発表した。

特筆すべき点として、重大被害発生率が業種全体で最も低い出版・放送・印刷の年間平均被害総額が、昨年調査の約1億円から約4.2億円と急増し、他業種よりも高い結果となっていること、重大被害発生率がそれほど高くない医療の年間平均被害総額が約3.3億円と全体平均を大きく上回る結果となっていることを挙げ、セキュリティインシデントによる被害の発生率が低い業種の場合でも、実被害額という観点では、事業を脅かす深刻な結果につながる可能性があることを示唆している。

出典：トレンドマイクロ株式会社、法人組織におけるセキュリティ実態調査2019年版

・ 重大被害による年間平均被害総額（業種別）



※ ()内の数字はサンプル数

(例) 事業被害について②

Cities are easy prey for cybercriminals.
Here's how they can fight back



Cities' digital infrastructure is often outdated and under-resourced - which makes them soft targets for cybercriminals. Image: REUTERS/Pichi Chuang

30 Sep 2019

Robert Muggah
Principal, SecDev Group

Marc Goodman
Founder, Future Crimes Institute

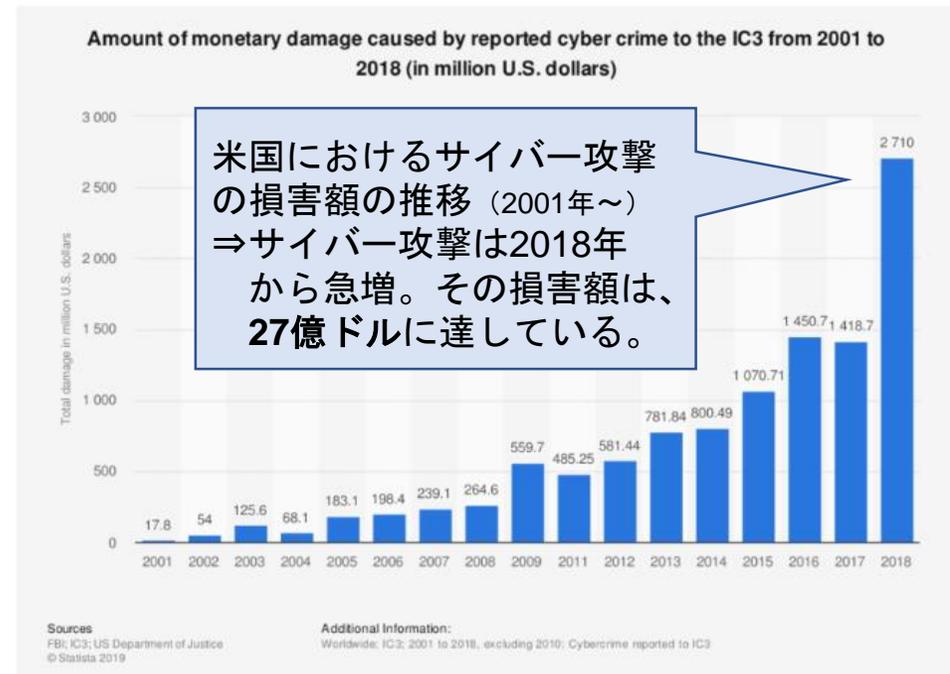
Make no mistake: the world is in the early stages of a techno-war against city governments and urban infrastructure. And while some cities have bolstered their capabilities to patch their vulnerabilities, they are entirely unprepared for the scale of cyberthreats that are coming.

The scope of the cyber threat to cities is becoming clearer. According to industry experts, more than 70 percent all reported ransomware attacks in the U.S. target state and local governments. At least 180 public safety call centers were also targeted in the last two years. (中略) The impacts of the cyber threat should not be taken lightly.

<https://www.weforum.org/agenda/2019/09/our-cities-are-increasingly-vulnerable-to-cyberattacks-heres-how-they-can-fight-back/>

ロイズは、ニューヨーク市だけでも2020年にサイバー関連の損失が23億ドルを超える可能性があると見積もっている。

Lloyds estimates that New York city alone could face over \$2.3 billion in cyber-related losses in 2020. Given their snowballing deficits, cities can ill afford the burgeoning costs of these digital incursions.



米国におけるサイバー攻撃の損害額の推移 (2001年～)
⇒サイバー攻撃は2018年から急増。その損害額は、27億ドルに達している。

出典：WORLD ECONOMIC FORUM、

2 - 2. 目的

◆目的：3月末に報告書提出予定

本研究では、2020年東京五輪大会に向け、経営者がとるべきサイバーセキュリティ対策についての具体的な施策の検討、ならびに過年度の成果物を総括したサイバーセキュリティ対策に関する提言のまとめを目的とする。

経営層の役割は、組織規模や置かれている環境に関わらず、リスクを回避して事業を継続するための経営判断を行うことである。今日では、サイバーセキュリティリスクが重要な経営リスクとなっていることから、経営層がサイバーセキュリティリスクの重要性を認識し、これを踏まえた上で経営判断を行うために必要となる施策について、具体的に示すことを目的とした。

なお、施策は、主として経営層が組織内において指示して実現すべき対策を指すが、本研究では、経営層が自ら実行することが望まれる行動指針についても施策に含めた。経営層がとるべきサイバーセキュリティ対策は、組織規模や組織が置かれている環境により千差万別であり、実現すべき対策を一律に定めることは難しい。このため、施策の具体化に際しては、これらの差異に配慮する記載に努めた。

2 - 3. 10の施策案

- 施策1 サイバーセキュリティリスクの重要性について経営会議において情報を分析する。
- 施策2 サイバーセキュリティリスクに関する検討組織を設置する。
- 施策3 危機管理を統括する既存部門とCSIRTの連携を強化する。
- 施策4 PDCAサイクルを実施する組織からリスク対応について定期的な報告を受ける。
- 施策5 経営層として情報共有に努める。
- 施策6 危機管理コミュニケーション力を高める。
- 施策7 有事に備えた現場担当者教育を強化する。
- 施策8 監査機能を積極活用する。
- 施策9 サイバーセキュリティリスクへの取り組みについて積極的な情報開示に努める。
- 施策10 自社のセキュリティ水準の将来目標を定め目標達成や進捗状況を管理する。

施策1 サイバーセキュリティリスクの重要性について 経営会議において情報を分析する。

分析結果に基づき、経営層が共通した認識の下で意思決定を行う。

○施策例

- 発生し得る重大なサイバーセキュリティリスク（例えば、サイバーテロによる業務妨害、経営戦略上において重要な営業秘密の流出による損害、ビジネスメール詐欺）を経営リスクとして認識する。
- 重大なサイバーセキュリティリスクについて、取締役及び監査役間において意見交換する等、経営層の間で日頃より**認識の共有**に努める。
- サイバーセキュリティリスクの重要性と対応について、取締役会等の経営会議における審議事項に含め、協議・分析を行う。年2回程度の**集中審議**を行い、対応状況を確認する。
- 情報セキュリティ対策の不備がサイバーセキュリティリスク発言の端緒となることを踏まえ、自組織における情報セキュリティ対策にも留意する。

○施策を怠った場合のシナリオ

- 経営層が自らの状況認識を高めることを放棄し、積極的に脅威情報を収集を怠ることにより、組織全体がサイバーセキュリティリスクに目を向けなくなり、**対策が停滞**する。
- サイバーセキュリティ対策などの実行が組織の方針と一貫したものとならない。
- サイバー攻撃による事故が発生した場合に、**善管注意義務違反を問われる**。

サイバーセキュリティ経営ガイドライン

経営者が認識すべき3原則

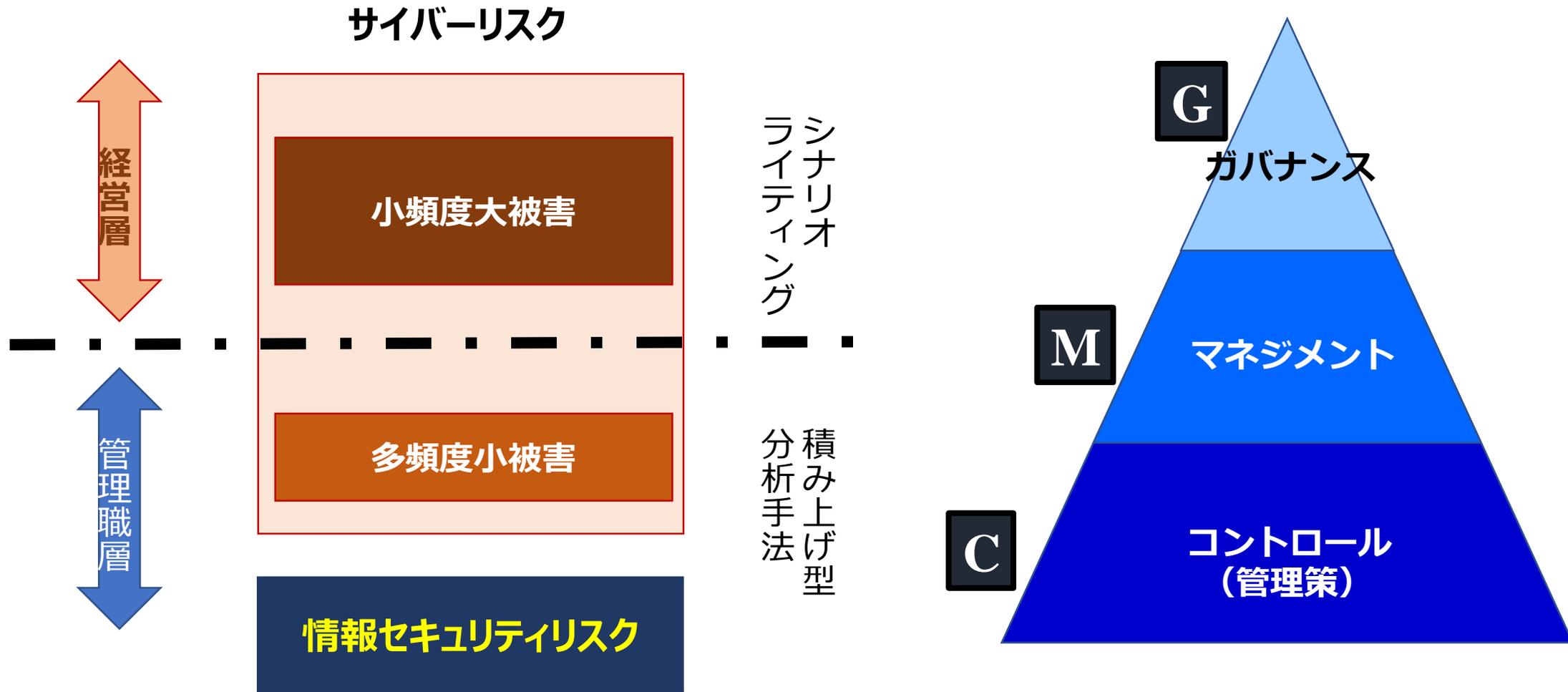
1. 経営者は、サイバーセキュリティリスクを認識しリーダーシップによって対策を進めることが必要

2. 自社のみならず、**ビジネスパートナーや委託先も含めた**セキュリティ対策が必要

3. **平時及び緊急時**のいずれにおいても、関係者との適切な**コミュニケーション**が必要

特徴

サイバーリスク判断における経営の役割



交通セキュリティセミナー 交通分野のサイバーセキュリティ対策における監査役の役割 (令和2年1月29日開催)

講演2 「サイバーセキュリティの監査」 NPO 日本セキュリティ監査協会 エグゼクティブフェロー 永宮直史氏 講演資料より

重要インフラ企業の経営者に求められる責任



経営リスクに占める、サイバーテロの位置づけ



善管注意義務を果たしているか



ちゃんとやったと、説明できるか



クライシスコミュニケーションの体制は

施策2 サイバーセキュリティリスクに関する検討組織を設置する

経営層が情報を分析して施策に反映させるために、専門の検討機能を組織する。

○施策例

- サイバーセキュリティリスクに関する検討組織を設置し、経営会議における協議・分析を支援する組織として活用する。
- 検討組織において以下を検討し、経営会議におけるインプット情報とする。
 - 重視すべきサイバーセキュリティリスクの選定と優先順位付け
 - リスクの発生確率や発生したときの損害試算
 - セキュリティポリシー策定あるいは修正方針の立案
 - リスクマネジメント、事業継続計画（BCP）とサイバーセキュリティリスクの関係
- 検討組織からのインプット情報をもとに、ヒト、組織、予算、等の社内資産を確保する。

○施策を怠った場合のシナリオ

- サイバーセキュリティリスクの管理体制を整備していない場合、組織としてサイバーセキュリティリスクの把握が出来ない。
- 適切な予算確保が出来ていない場合、組織内でのサイバーセキュリティ対策の実施や人材の確保が困難となるほか、信頼できる外部のベンダーへの委託が困難となる恐れがある。

施策3 危機管理を統括する既存部門とCSIRTの連携を強化する。

経営リスクとサイバーリスクを統括管理するために組織連携を強化する。

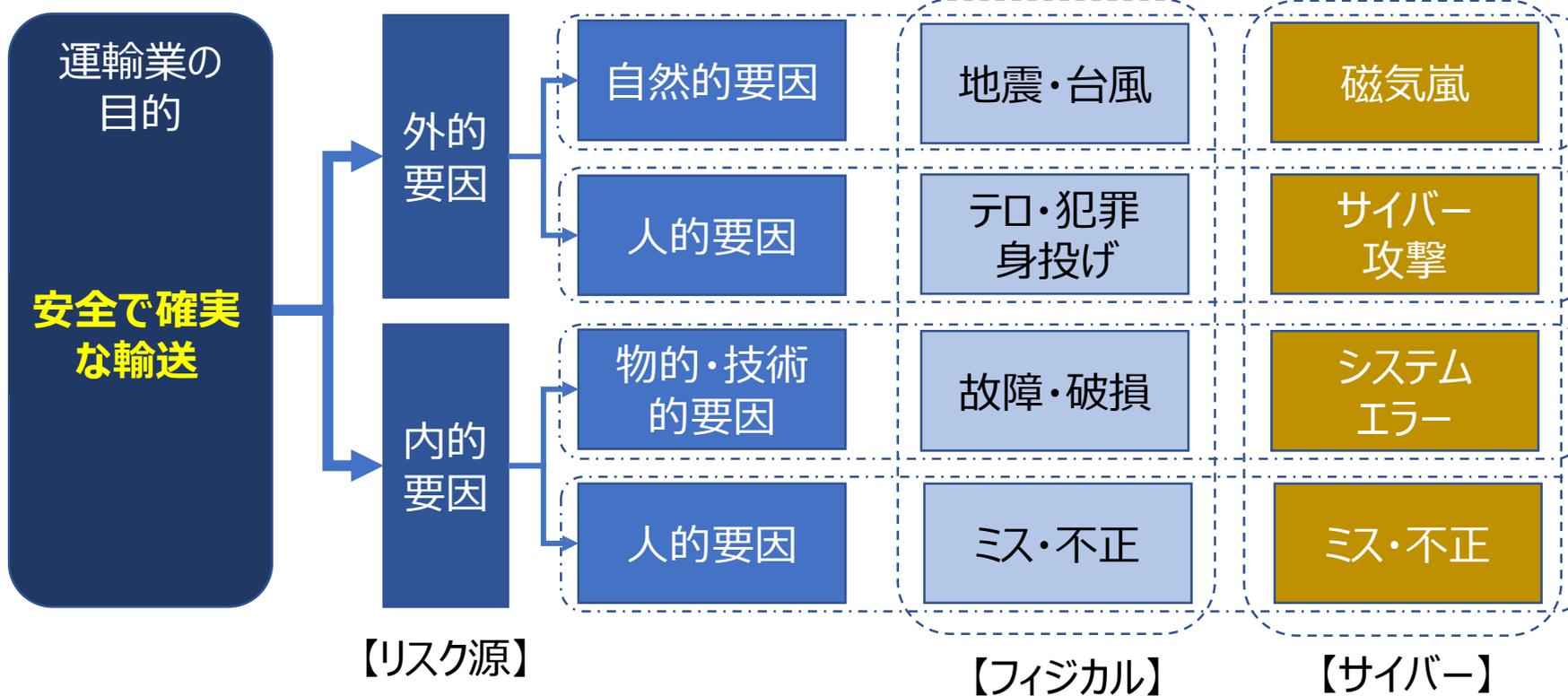
○施策例

- 事業部門におけるサイバー攻撃対応において、迅速にCSIRTと連携できるよう組織を整備する。
- サイバー攻撃の発生に備えて、危機管理を統括する部門とCSIRTが連携できるよう組織を整備する。
- サイバー攻撃により業務停止に至った場合、速やかに再開するため、関係機関との連携や復旧作業を実施できる管理体制を構築する。
- 構築した管理体制の下、重要な業務をいつまでに復旧すべきかの目標について、組織全体として整合をとる（例えばBCPで定めている目標との整合等）。
- 必要に応じて、速やかに安全推進を所管する部署と連携できる管理体制を構築する。

○施策を怠った場合のシナリオ

- 重要な業務が適切な時間内に復旧できず、企業経営に致命的な影響を与える恐れがある。
- サイバーセキュリティリスクに応じた適切な対策が行われていない場合、サイバー攻撃が発生した場合の被害が拡大する可能性がある。
- 事業部門を含む緊急時の対応体制を整備していないと、原因特定のための調査作業において、組織の内外の関係者間のコミュニケーションが取れず、速やかな対処ができない。

リスク：目的に対する不確かさの影響
(ISO31000)



サイバーセキュリティの要点

要点1

リスク評価

- 人的・物的被害に着目したリスク評価
 - ISO31000に基づくリスク評価を追加
 - ✓ めったに生じないが、甚大な被害が生じるリスク（想定外を想定する）

要点2

情報セキュリティ防御ができなかった場合の対策を強化

- 検知手順・インシデント判定手順の確立
- CSIRTの確立
- 事業継続：物理的対処チームや復旧プロセス等との連携及びサイバーレジリエンスの確立

※サイバーレジリエンス：
損害を被ったシステム部分を除いて、業務を継続する仕組みがあること

施策4 PDCAサイクルを実施する組織からリスク対応について定期的な報告を受ける。

報告をもとに、**経営層が重視するサイバーリスクへの対応状況**を定期的に確認する。

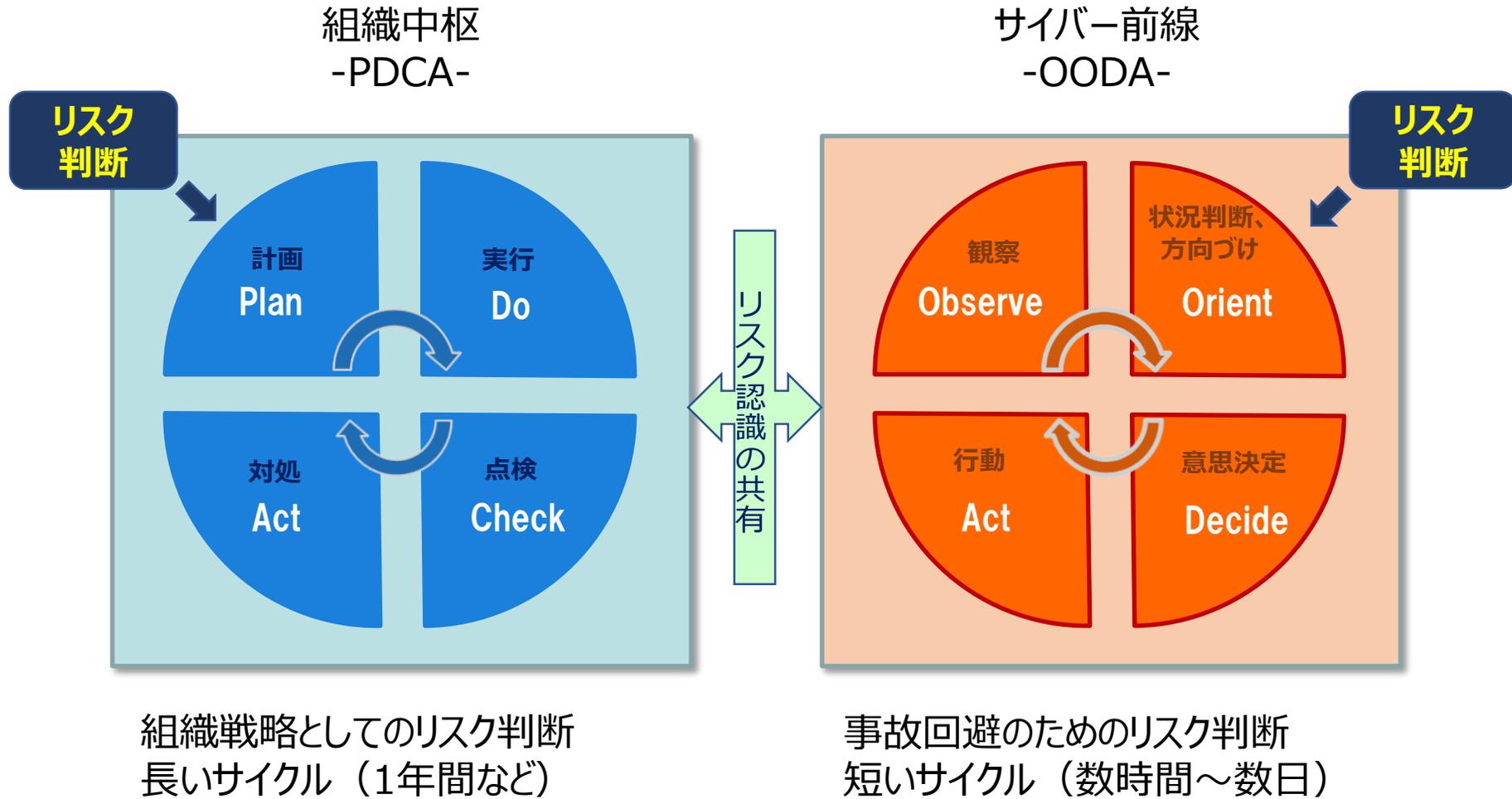
○施策例

- PDCAサイクルにおいて実施するリスク分析について、事業被害ベースのリスク分析手法を実施することを担当組織に指示する。
- 経営層として重視するサイバーセキュリティリスクについて、リスク分析に反映させる。
- 経営層として重視するサイバーセキュリティリスクについて、対応状況を報告させる。

○施策を怠った場合のシナリオ

- PDCA（Plan[計画]、Do[実行]、Check[実施状況の確認・評価]、Act[改善]）を実施する体制が出来ていないと、立てた計画が確実に実行されない恐れがある。
- 事業被害ベースのリスク分析を採用しないことにより、経営層として重視するサイバーセキュリティリスクの対策状況が十分なものか**判断できなくなる**。
- 最新の脅威への対応ができているかといった視点も踏まえて組織のサイバーセキュリティ対策を定期的に見直さないと、サイバーセキュリティを巡る**環境変化に対応できず**、新たに発生した脅威に対応できない恐れがある。

二つの活動とリスク判断



施策5 経営層として情報共有に努める。

経営層が関与することの組織的な効果を踏まえ、積極的な情報共有に努める。

○施策例

- サイバーセキュリティリスクに関する検討組織から情報を入手する。
- PDCAを実施する組織から**定期報告**を受け、社内の情報セキュリティ対策の現状を把握する。
- サイバーセキュリティに関する知見を有する者が誰であるか確認しておく。
- 経営層として認識する重要なサイバーセキュリティリスクについて**社内に周知**する。
- 現場に赴き、サイバーセキュリティリスクについて担当者と対話する。
- 経営層に向けたセミナー等に参加し、情報を収集する。
- 同業他社の経営層や所管省庁との間で、サイバーセキュリティリスクに係る**情報共有**に努める。

○施策を怠った場合のシナリオ

- 経営層としての重要情報を見落とすことにより、**経営判断を誤る**。
- 経営層としての情報共有を怠ることにより、社内のサイバーセキュリティ対策の方針が徹底しない。

重要なリスクコミュニケーション

組織全体でリスク認識が共有されていると、ガバナンスが利きやすい

- リスクコミュニケーション※の意義：
 - 組織内外の関係者が「リスク」「意思決定の根拠」「特定の活動が必要な理由」についての理解が容易になる
- リスクコミュニケーションの実施段階
 - リスクアセスメントのみではなく、リスク対策の実施、レビュー、記録等リスクマネジメントのあらゆるプロセスで行う
 - サイバーセキュリティ対策もリスクマネジメントプロセスとして行われる
- リスクコミュニケーションのねらい
 - プロセスの各段階で組織内外の専門家の知識を集める
 - リスク基準を定め、リスク評価の場合に異なる見解に考慮する
 - リスク監視及び意思決定を行うための十分な情報を提供する
 - **リスクの影響を受ける者たちの一体感と当事者意識を醸成する**

(注) ISO31000 : 2018に基づき加工

※ ISO31000では「リスクコミュニケーション及び協議」

オリンピック後も役立つ節目作戦



経営者が直接セキュリティの現場に行って、
毎月（6回）話を聞く



経営者がインシデント事例3つの訓練をする
（DDoS、平昌、三菱）



外部のプロに、穴を探してもらう。
（ペネトレーションテスト）

施策6 危機管理コミュニケーション力を高める。

経営層自身が適切な有事対応できるよう、平時より能力を高める。

○施策例

- 危機管理コミュニケーションの事例を集め、失敗事例の要因等を参考にする。
- 特にサイバー攻撃が発生した際に、**助言を求める者**が誰であることを予め確認しておく。
- 既存の事業継続計画にサイバー攻撃に起因するシナリオを追加する。追加シナリオに沿ってマニュアルを改定する。
- 経営層を含む関係者により、マニュアルに沿った**模擬訓練**を行う。

○施策を怠った場合のシナリオ

- 速やかな情報開示が行われない場合、**顧客や取引先等**にも被害が及ぶ恐れがあり、損害賠償請求など責任を問われる場合がある。
- 記者会見での**失言、情報を隠蔽**しているような誤解を与えてしまうことによって、事態が悪化してしまうことがある。
- ネガティブな印象によって企業**価値の低下**を招く恐れがある。

施策7 有事に備えた現場担当者教育を強化する。

攻撃を最初に検知するのは現場担当者であり、これを踏まえた教育を行う。

○施策例

- **現場担当者に対する教育**を行い、重大なサイバーセキュリティリスクが発生した際に迅速かつ適切な対応が行えるよう日頃から備える。
- サイバー攻撃が発生した際に適切に関係部門と連携ができるよう、現場担当者と関係部門を交えた演習・訓練を実施する。
- 体制について検証するために、**社外の演習**・訓練への参加を促進する。
- 現場担当者向け研修のための**予算**を確保し、継続的に役割に応じたセキュリティ教育を実施する。
- 経営層が重視するサイバーセキュリティリスクについて、**社内に積極的に発信**する。

○施策を怠った場合のシナリオ

- 現場担当者教育を怠ることにより、サイバー攻撃が発生した際の**初動対応**が遅れ、被害が拡大する。
- 経営層が重視するサイバーセキュリティリスクが現場担当者に周知されないことにより、サイバー攻撃**対策が徹底されない**。

施策8 監査機能を積極活用する。

監査を忌避する風潮を打破し、ガバナンス強化の仕組みとしての活用を図る。

○施策例

- 経営層が重視するサイバーセキュリティリスクに適切に対処しているかどうかを点検・評価・検証するよう、監査人に指示する。あるいは、経営層が重視するサイバーセキュリティリスクを**監査の観点に加える**よう、システム監査やセキュリティ監査を主管する部門に対して指示する。
- サイバーセキュリティ対策のチェックを実施することができる**内部監査人の育成**を行う。
- 系列企業、サプライチェーンのビジネスパートナーやシステム管理の委託先等のサイバーセキュリティ対策状況（監査を含む）の報告を受け、把握する。

○施策を怠った場合のシナリオ

- 経営層が重視するサイバーセキュリティリスクについての**対策が徹底されない**。
- 系列企業やサプライチェーンのビジネスパートナーにおいて適切なサイバーセキュリティ対策が行われていないことにより、これらの企業を**踏み台**にして自社が攻撃される。
- システム管理などの委託業務において、自組織で対応する部分と委託する部分の境界が不明確となり、対策漏れが生じる恐れがある。

サイバーセキュリティ監査の確認事項

- 企業がサイバーセキュリティに**的確に対応できているか**の確認
 - リスク認識の共有：組織末端までサイバーリスクの理解が共有できているか？
 - 組織態勢の確立：平時も異常時も円滑に全員が動けるか？
 - 事業継続：異常時に事業活動が途切れないか？
- **企業態勢がしっかりしているか**の確認
 - 経営者が役割を果たしているか
 - 企業存続に影響するサイバーリスクを常に見直しているか？
 - リスク認識の共有を図っているか？
 - 適切なガバナンスを行っているか？
 - 管理者が適切に管理しているか
 - PDCAがしっかり回っているか？
 - 技術者が適切に対処しているか
 - OODAによりインシデント検知が行われているか？
 - インシデント対応態勢が動くか？

基本となる情報セキュリティ監査

- 監査の目的
 - 情報セキュリティマネジメントが効果的か
- 監査の方法
 - 準拠性監査
 - ◆ 組織が定めたルールに準拠しているか
 - **有効性（妥当性）監査**
 - ◆ **リスク管理が有効か（管理策がリスクに対して妥当か）**

- **ISMS適合性評価制度の限界**
 - 監査の方法等は経営者が決める
 - ISO27006により審査工数の上限がある

~~自己流の監査~~



- 情報セキュリティ監査基準
- 情報セキュリティ管理基準

- 情報セキュリティサービス基準適合サービス

- 公認情報セキュリティ監査人
- 情報セキュリティ内部監査人能力認定

交通セキュリティセミナー 交通分野のサイバーセキュリティ対策における監査役の役割（令和2年1月29日開催）

講演2「サイバーセキュリティの監査」

NPO 日本セキュリティ監査協会 エグゼクティブフェロー 永宮直史氏 講演資料より

施策9 サイバーセキュリティリスクへの取組について積極的な情報開示に努める。

株主や投資家等を含め、多様な利害関係者に向けた積極的な情報開示を行う。

○施策例

- サイバーセキュリティリスクを考慮した**セキュリティポリシーを策定**する。その際、情報システムのみではなく、製造、販売、サービス等、**事業に応じた対応方針**を検討する。
- コーポレートガバナンス報告書にサイバーセキュリティリスクへの取り組みを記載することを検討する。
- サイバーセキュリティリスクへの**取り組みを一般公開**することでステークホルダーや社会に対する企業としての姿勢を示し、信頼性を高める。
- サイバーセキュリティ対策の状況について、サイバーセキュリティリスクの性質・度合いに応じて、情報セキュリティ報告書、CSR 報告書、サステナビリティレポートや**有価証券報告書等**への記載を通じて開示を検討する。

○施策を怠った場合のシナリオ

- 適切な開示を行わなかった場合、社会的責任の観点から、事業のサイバーセキュリティリスク対応について**ステークホルダーの信頼を失う**とともに、インシデント発生時に企業価値が大きく低下する恐れがある。

施策10 自社のセキュリティ水準の将来目標を定め、目標達成や進捗状況を管理する。

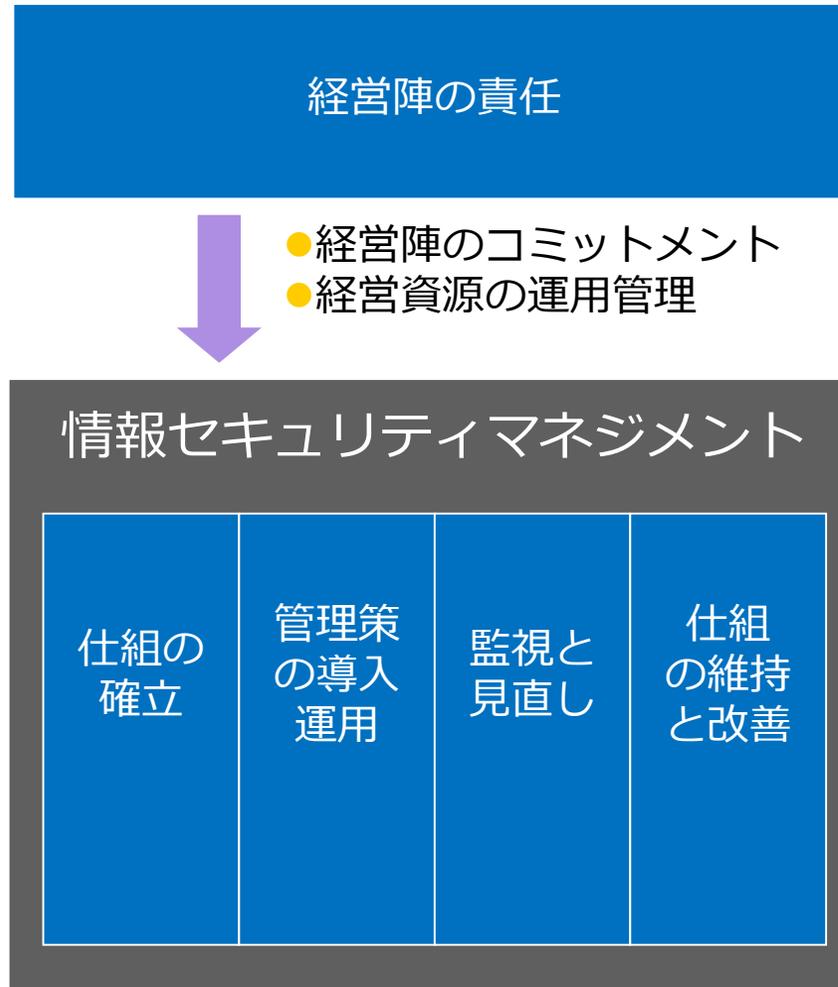
中長期の事業計画と整合したサイバーセキュリティ対策を計画し、実行する。

○施策例

- 中長期の事業計画において達成することが必要となる自社の**セキュリティ水準**（組織的、人的、技術的対策水準）を定める。
- 自社のセキュリティ水準の**将来目標**を定め、中長期の事業計画と整合させる。
- 対象となる事業計画には、新規事業も含まれる。
- 自社のセキュリティ水準については、組織的対策、人的対策、技術的対策が含まれる。
- 内部監査の実施に際して、目標とすべきセキュリティ水準の**達成度を確認**する。

○施策を怠った場合のシナリオ

- 企業の経営戦略に基づき、各企業の状況に応じた適切なリスク対応を実施しなければ、**過度な対策**により通常の業務遂行に支障をきたすなどの不都合が生じる恐れがある。
- 受容できないリスクが残る場合、想定外の損失を被る恐れがある。



- a. 基本方針を確立する
 - b. 目的を定め、計画の策定を指示する
 - c. 情報セキュリティに対する役割や責任を定める
 - d. 情報セキュリティの重要性を組織内に周知する
 - e. 必要な経営資源を提供する
 - f. リスク受容の基準、受容可能なリスクの水準を決める
 - g. 内部監査の実施を指示し支援する
 - h. 経営者の視点からレビューを実施する
- (ISO/IEC27001 : 2005による)

2 - 4 . 各施策案の関係図

(経営層からの)
アウトプットの観点

(経営層への)
インプットの観点

施策1 サイバーセキュリティリスクの重要性について経営会議において情報を分析する。

施策2 サイバーセキュリティリスクに関する検討組織を設置する。

施策3 危機管理を統括する既存部門とCSIRTの連携を強化する

施策4 PDCAサイクルを実施する組織からリスク対応について定期的な報告を受ける。

施策5 経営層として情報共有に努める。

施策6 危機管理コミュニケーション力を高める。

施策7 有事に備えた現場担当者教育を強化する。

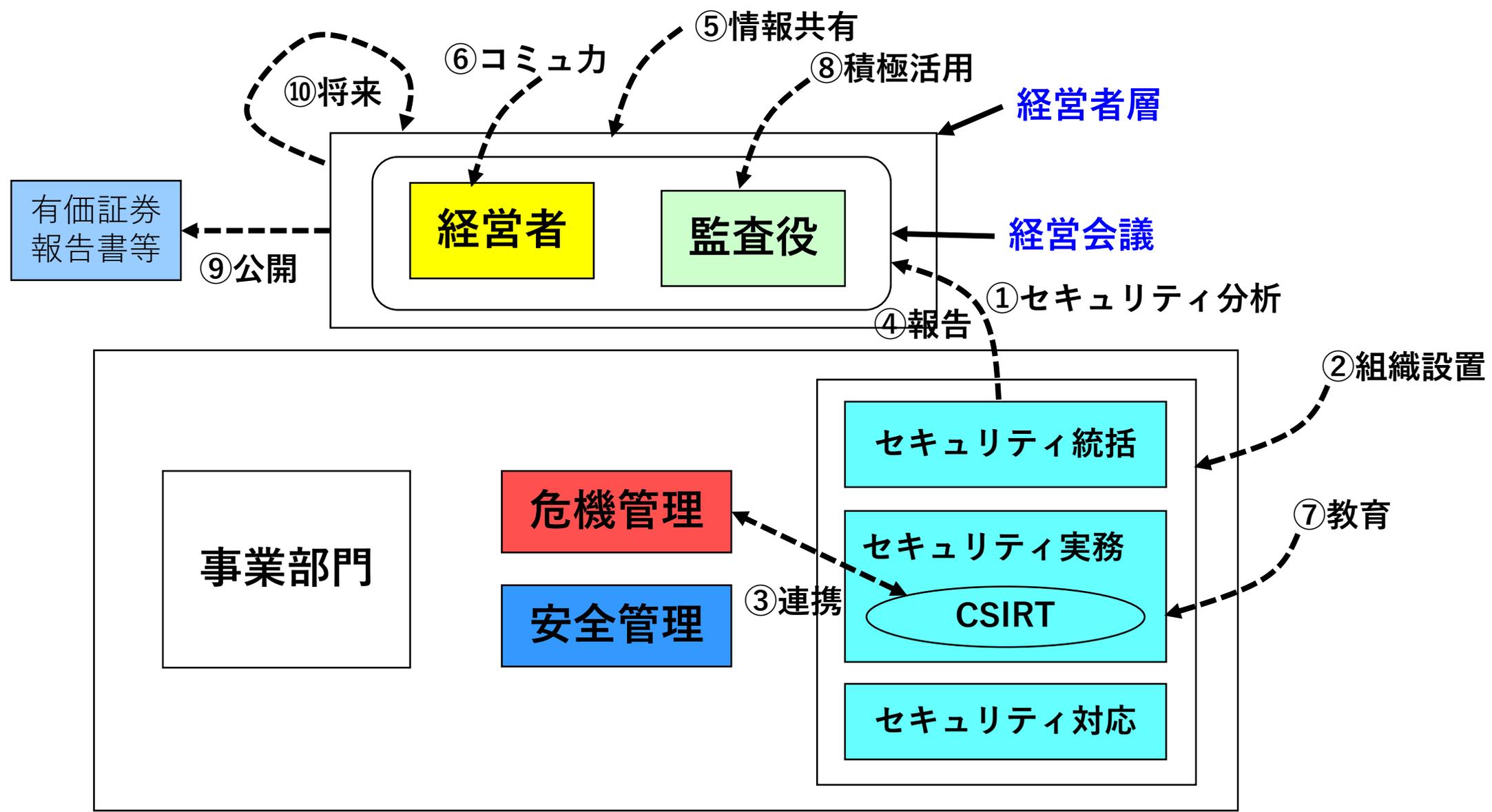
施策8 監査機能を積極活用する。

施策9 サイバーセキュリティリスクへの取り組みについて積極的な情報開示に努める。

施策10 自社のセキュリティ水準の将来目標を定め目標達成や進捗状況を管理する。

- 経営層（監査役を含む）は、サイバーセキュリティリスクを重要な事業リスクの一環として捉え、他の事業リスクとともに**危機管理の対象として認識**する必要がある。
- 経営層は、組織整備、情報把握、指示、確認、情報発信、といった一連の経営活動に即して、重大なサイバーセキュリティリスクに**対処するための施策を実施**する必要がある。
- 施策の実施に際しては、意思決定を支援する組織（検討組織）及び施策を徹底する組織（監査等）と**密に連携**することが望まれる。

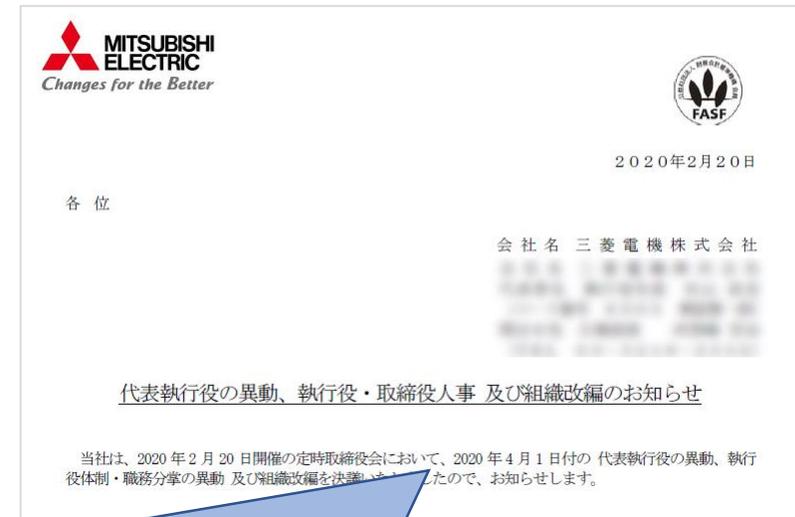
各施策の位置づけ



・事例①三菱電機

三菱電機がセキュリティ統括室、元エネ庁長官も迎える

三菱電機は20日、同社がサイバー攻撃を受けたことなどから、4月1日に「情報セキュリティ統括室」を新設すると発表した。今回の攻撃への対応の教訓を生かし、社長直轄で一元的に対策を担うようにする。渉外などを担当する常務執行役に、経済産業省の資源エネルギー庁長官を2018年に退官した日下部聡氏が同日付で就く人事も発表した。（日本経済新聞 2020/2/20付）



5. 組織改編（2020年4月1日付）

（1）情報セキュリティ統括室の新設

当社グループ全体の情報セキュリティ体制強化に向け、迅速な判断とインシデント発生時のお客様や関係機関との早期情報共有等を目的に、**情報セキュリティ全般の企画・構築・運営の機能を一元的に担う社長直轄の情報セキュリティ統括室を新設する。**

（三菱電機株式会社公式HPより）

今後：セキュリティ統括室における情報共有・情報連携機能の拡充

セキュリティ統括				
方針策定	セキュリティ戦略	法令対応（国内法対応、各国法対応） セキュリティポリシー 策定 リスクマネジメント・事業継続管理（BCM） 組織体制・職務権限・業務分掌 策定 セキュリティ基準・政府等ガイドライン対応		
	セキュリティ実務	規程・社則・技術的ガイドライン策定 構成管理指針策定・アセスメント実施 情報共有・情報連携 インシデント管理・CSIRT活動（SOC 含む）		
支援	セキュリティ対応	新規技術・サービス導入 データ管理		
実務支援	事業分野別セキュリティ対策	IoT	IT	OT
	企画	セキュリティ戦略 / 予算措置		
	設計	セキュリティバイデザイン		
	調達	選定基準（機器・サービス等）		
	運用	運用保守基準 / 品質管理		
	監査	アセスメント / 監査		
	調達先管理	サプライチェーンリスク管理		
	委託先管理			

セキュリティ統括室の機能

（産業横断サイバーセキュリティ人材育成検討会（CRIF CSF）資料より転載）



フュージョンセンターの概念図

（Citi の公開資料より和訳転載）

2 - 6. オリンピック・パラリンピック対策に向けた施策

- 施策1 サイバーセキュリティリスクの重要性について経営会議において情報を分析する。
- 施策2 サイバーセキュリティリスクに関する検討組織を設置する。
- 施策3 危機管理を統括する既存部門とCSIRTの連携を強化する。
- 施策4 PDCAサイクルを実施する組織からリスク対応について定期的な報告を受ける。
- 施策5 経営層として情報共有に努める。
- 施策6 危機管理コミュニケーション力を高める。
- 施策7 有事に備えた現場担当者教育を強化する。
- 施策8 監査機能を積極活用する。
- 施策9 サイバーセキュリティリスクへの取り組みについて積極的な情報開示に努める。
- 施策10 自社のセキュリティ水準の将来目標を定め目標達成や進捗状況を管理する。

おわり