「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

Supported by 日本財団 THE NIPPON FOUNDATION

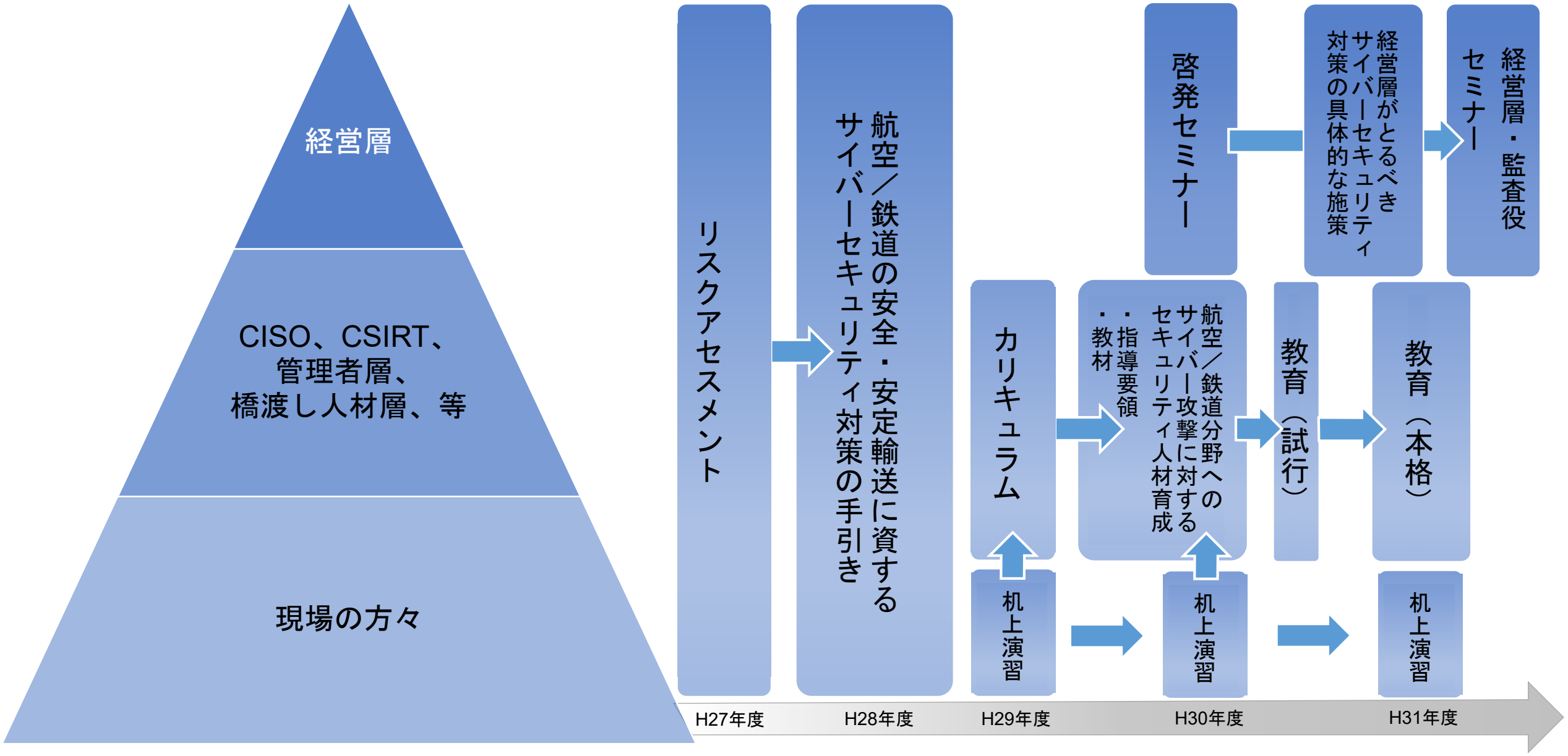
本日の内容

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．各施策案の説明
２−５．各施策の関係図
２−６．施策案のポイント
２−７．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．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

近年、情報セキュリティ対策の必要性に関する経営層の理解は高まっており、特にサイバーセキュリティに係るリスクへの必要な備えや有事の際の適切な対処等について、経営層が社内で指示すべき対策項目等に関する情報提供が進んできている。一方で、対策項目は一律に全企業で適用できるものではないため、経営層はその指示に苦慮しているのが現状と思われる。このため、サイバーセキュリティ対策を実施する上での指示を確たるものとするための施策が必要となってきている。

監査役セミナー開催について

監査役は、取締役とともに企業経営の両輪である。監査役の主な役割は、取締役の職務の執行を監査し、健全かつ適正な企業経営を実現することにある。

今日のサイバーセキュリティリスクは、現実に発生し得る重大な経営リスクとなっているが、例えば社内における予算措置等、対策の実行には様々な障壁が存在すると想定される。このような環境下、監査役には、健全かつ適正な企業経営を実現するため、取締役の良き助言者としての役割が求められている。

このため、経営層がとるべきサイバーセキュリティ対策について、監査役の理解が不可欠である。

２ － １．背景

◆経営層に更なる対策を促すための情報

〈 例 〉

・政府動向について

　サイバーセキュリティ対策の義務化の動きがある。

・事業被害について

　国内外とも事業被害額は拡大基調である。

２ － １．（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年をめどに内閣府の外局として設置するよう要請した。

出典：時事通信（2019年5月14日付）、
https://www.jiji.com/jc/article?k=2019051401171&g=pol

２ － １．（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

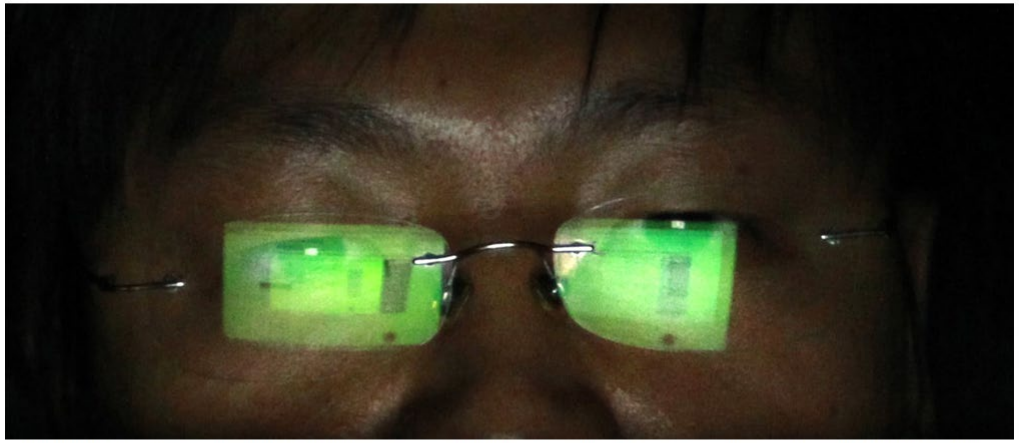
- 重大被害による年間平均被害総額（業種別）

※(　)内の数字はサンプル数

２ － １．（例）事業被害について②

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。

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

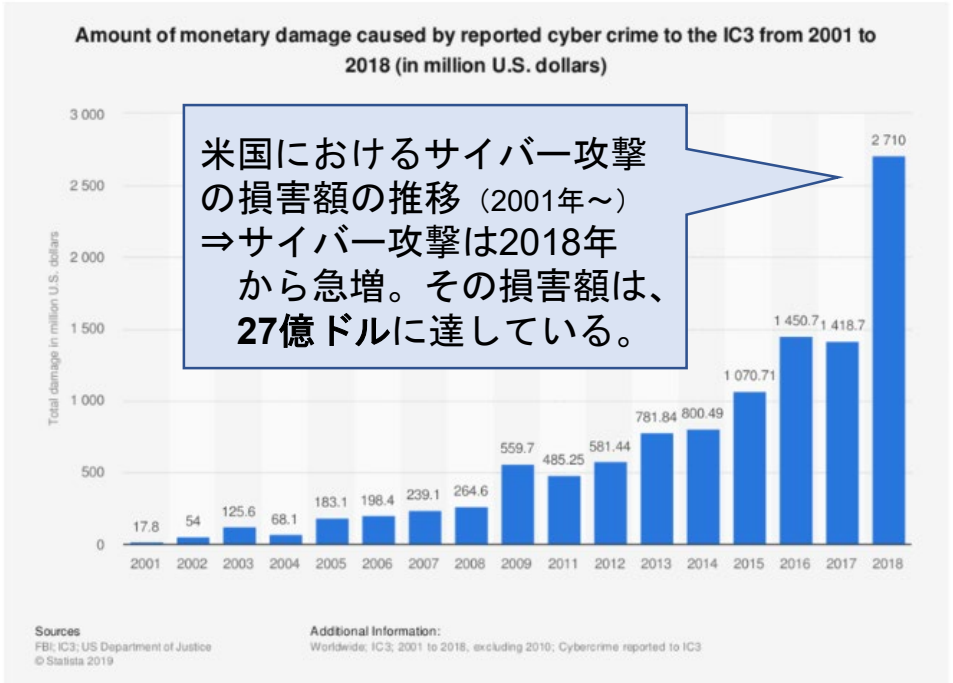
30 Sep 2019

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.

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。

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.

出典：WORLD ECONOMIC FORUM、
https://www.weforum.org/agenda/2019/09/our-cities-are-increasingly-vulnerable-to-cyberattacks-heres-how-they-can-fight-back/

２ － ２．目的

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。

２ － ４．各施策案の説明

◆各施策案の説明

以降から、１０の施策案の各施策について、
「施策例」と「施策を怠った場合のシナリオ」を挙げて説明する。

１０の施策案
1/１０

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、他の重大なリスクとともに対応状況を確認する。

○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、善管注意義務を問われる。

１０の施策案
2/１０

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。

１０の施策案
3/１０

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の仕組みを整備する。

○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、速やかに復旧するため、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。

１０の施策案
4/１０

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。

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る。
- 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。
- 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。

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関係する危機が発生した際に、助言を求める者が誰であるかを予め確認しておく。
- 既存のコンティンジェンシープラン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。

１０の施策案
7/１０

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。

１０の施策案
9/１０

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。

１０の施策案
１０/１０

施策９　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。

２ － ５． 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。

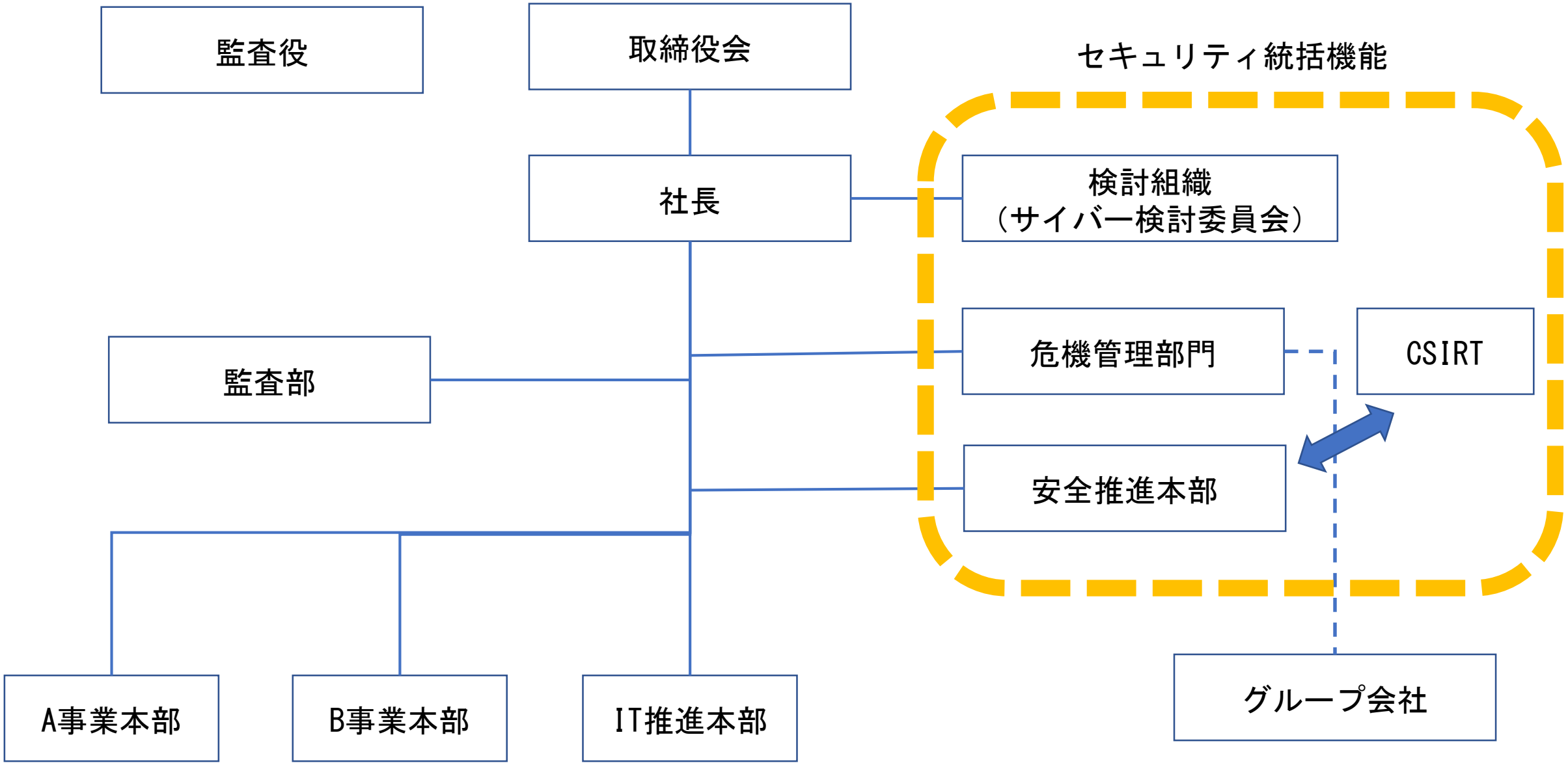
２－６．　施策案のポイント

- 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。

組織図例


監査役
取締役会
セキュリティ統括機能
社長
検討組織
（サイバー検討委員会）
危機管理部門
CSIRT
監査部
安全推進本部
A事業本部
B事業本部
IT推進本部
グループ会社

２ － ７．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。