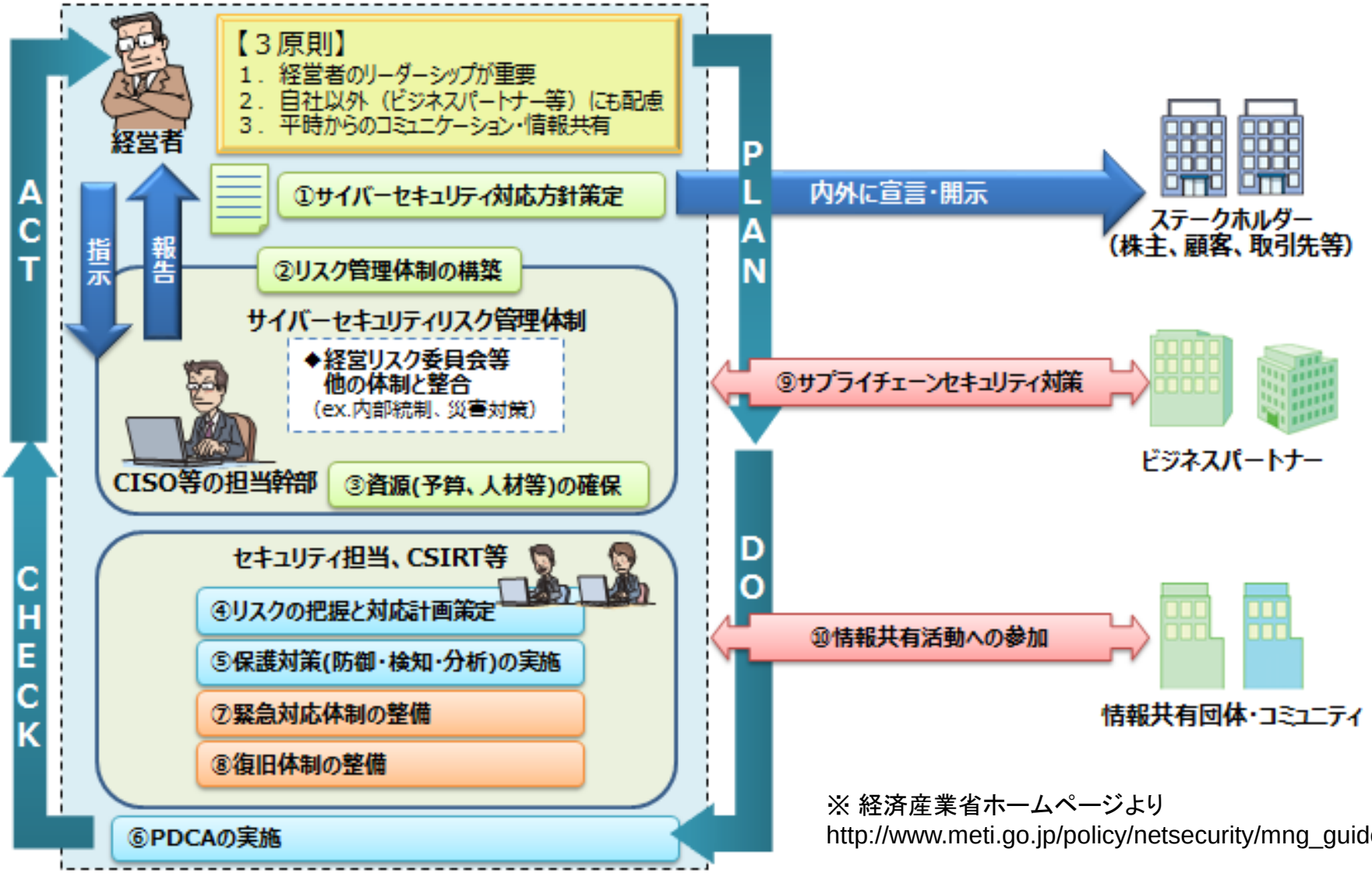
IPA Better Life with IT

サイバーセキュリティ経営ガイドラインを実践するための経営プラクティス

2019年4月23日

情報処理推進機構　セキュリティセンター
セキュリティ対策推進部　セキュリティ分析グループ
小川　隆一

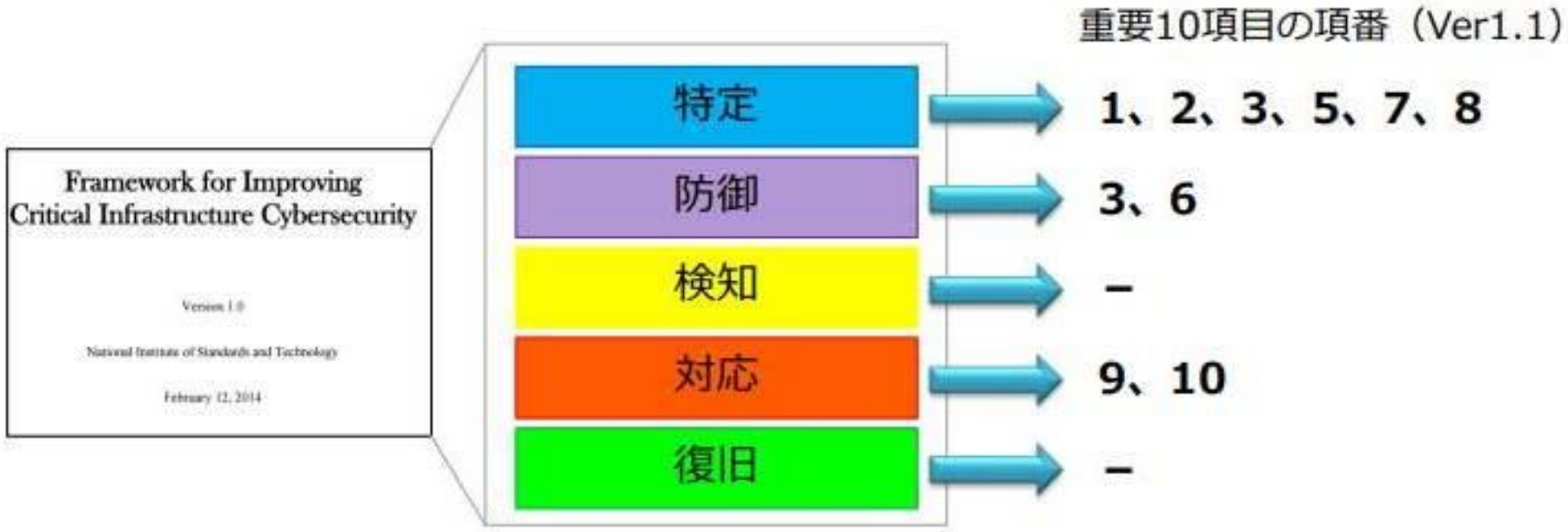
おさらい：サイバーセキュリティ経営ガイドラインの3原則と重要10項目



※ 経済産業省ホームページより
http://www.meti.go.jp/policy/netsecurity/mng_guide.html

V2.0改訂の背景

- 海外のガイドライン・規格に基づく見直し
  - **検知・対応・復旧**の強化
  - **サプライチェーン**対応の集約



NIST サイバーセキュリティ経営ガイドラインとの比較

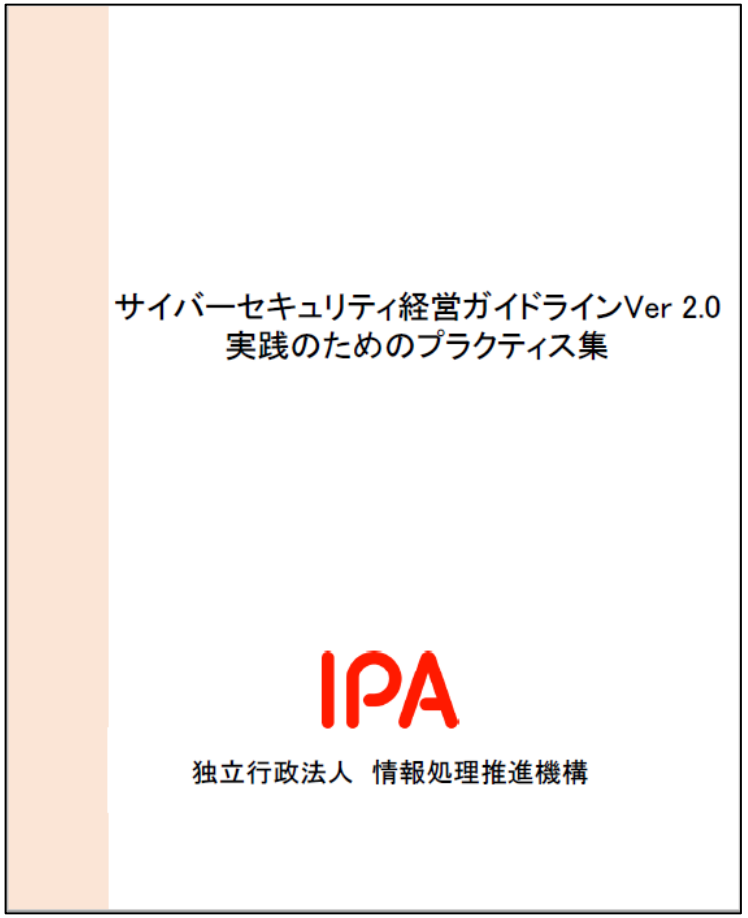
出典：サイバーセキュリティ経営ガイドラインの改訂ポイント
http://www.meti.go.jp/policy/netsecurity/downloadfiles/overview.pdf

経営ガイドラインの反響（2018年4月時点）

- 評価点
  - 政府がそれを言ったこと
- 課題
  - 人材・スキルの不足
  - 事業におけるサイバーセキュリティの優先度
- 要請
  - 方向性
  - どう使えばいいのか
  - 実戦事例

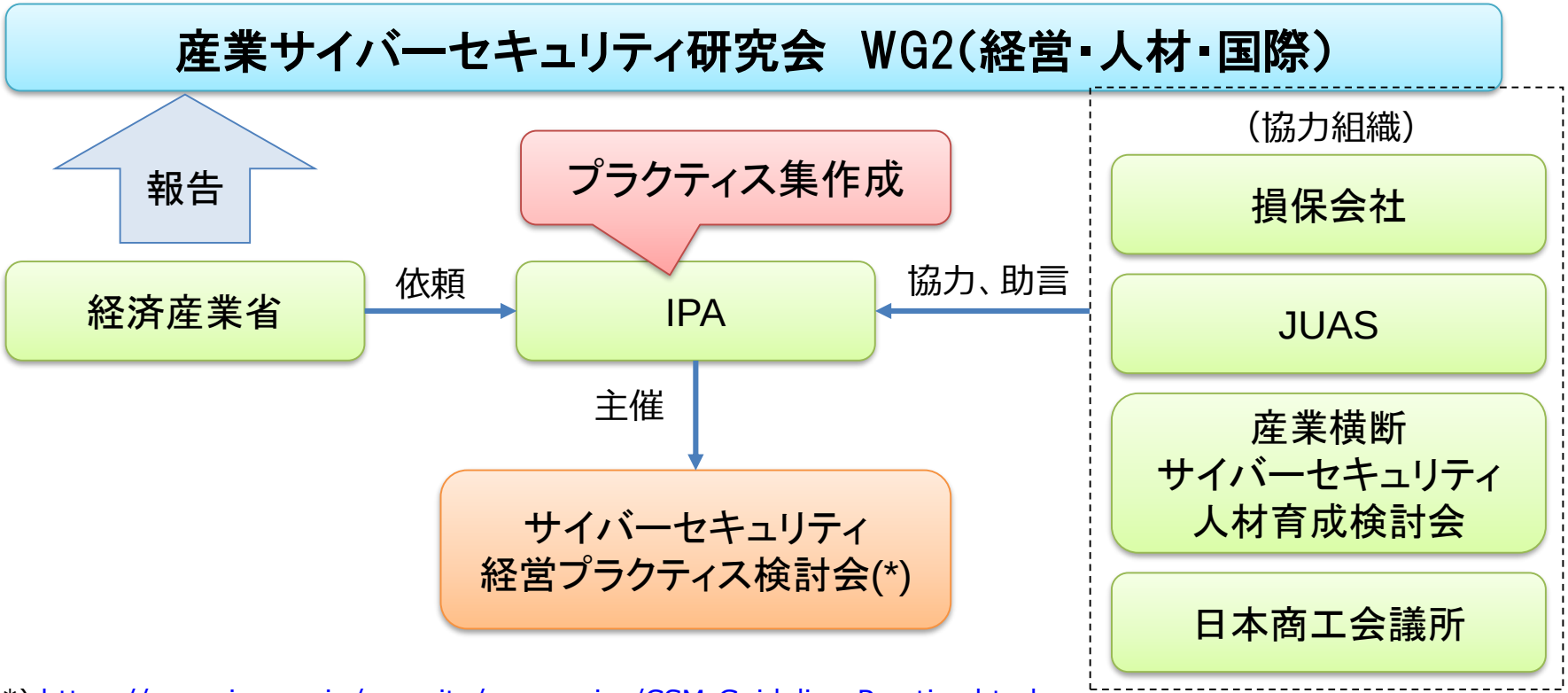
経営ガイドラインプラクティス集策定の狙い

- **事例を求める声**にこたえる
- 重要10項目の具体的**実践事例**、実践上の**悩みと解決策**
- 自社の状況を踏まえて対策を検討いただく



サイバーセキュリティ経営プラクティス検討・作成のスキーム（2018年4月～2019年2月）

- サイバーセキュリティ経営ガイドラインのプラクティスと、セキュリティ対策の実施状況を可視化するツールを作成するためにサイバーセキュリティ経営プラクティス検討会をIPAに設置し、全5回開催。



(*) https://www.ipa.go.jp/security/economics/CSM-Guideline-Practice.html

プラクティス集の想定読者

- 中堅企業
- ある程度の情報セキュリティ対策は実施
- 全社システムは一応対策、事業部門の対策はこれから
- サイバー攻撃対策、インシデントレスポンスに不安

⇒ サイバーセキュリティ **はじめの一歩**が知りたい

プラクティス集の構成

- 特徴
  - 簡潔・ビジュアル。仮想企業のプラクティスだが、すべて実例に基づく
- 構成

第一章：経営とサイバーセキュリティ

＜経営者、CISO等向け＞
なぜサイバーセキュリティが経営課題となるのか等を解説

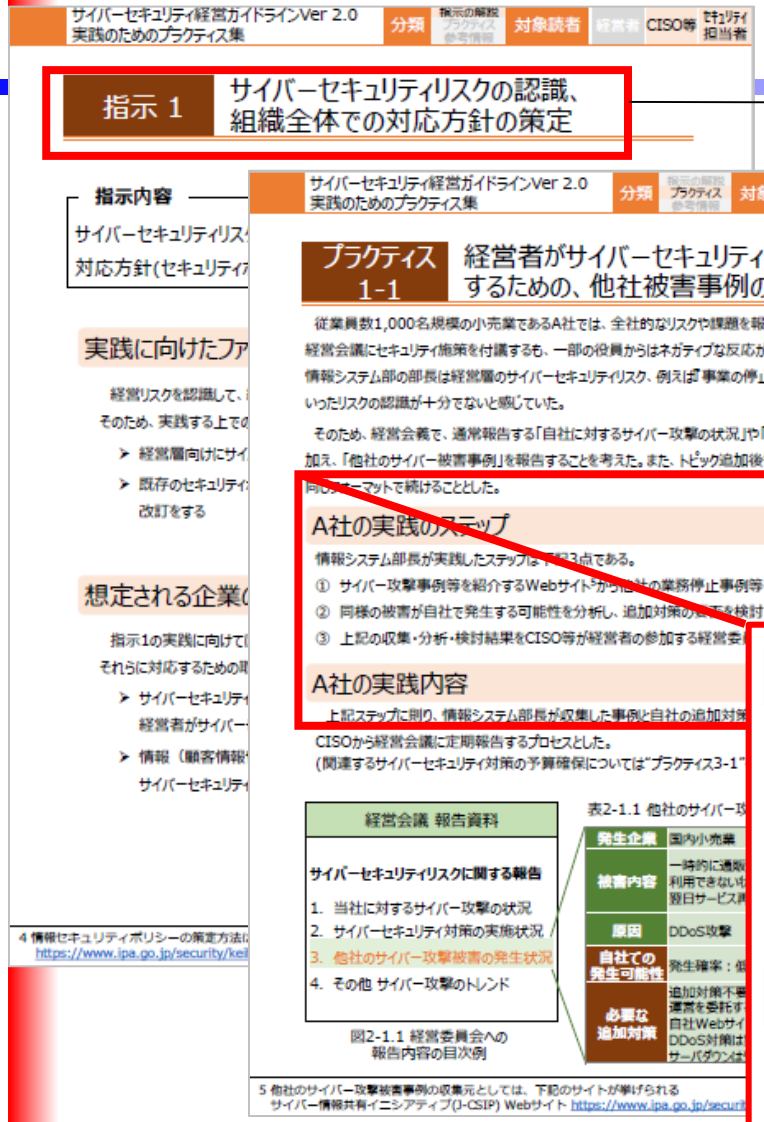
第二章：サイバーセキュリティ経営ガイドライン実践のプラクティス

＜CISO等、セキュリティ担当者向け＞
事例をベースとした重要10項目の実践手順、実践内容、取り組む際の考え方を解説

第三章：サイバーセキュリティ対策を推進する担当者の悩みと解決のプラクティス

＜CISO等、セキュリティ担当者向け＞
サイバーセキュリティ対策を実践する上での悩みに対する取組事例を紹介

第二章（重要10項目、まずここから）



サイバーセキュリティ経営ガイドラインの重要10項目毎に章立てを整理

企業の具体的取組をベースに
重要10項目の実践内容を説明

A社の実践のステップ

情報システム部長が実践したステップは下記3点である。

① サイバー攻撃事例等を紹介するWebサイト[5]から他社の業務停止事例等を収集する

② 同様の被害が自社で発生する可能性を分析し、追加対策の要否を検討する

③ 上記の収集・分析・検討結果をCISO等が経営者の参加する経営委員会で定期報告する

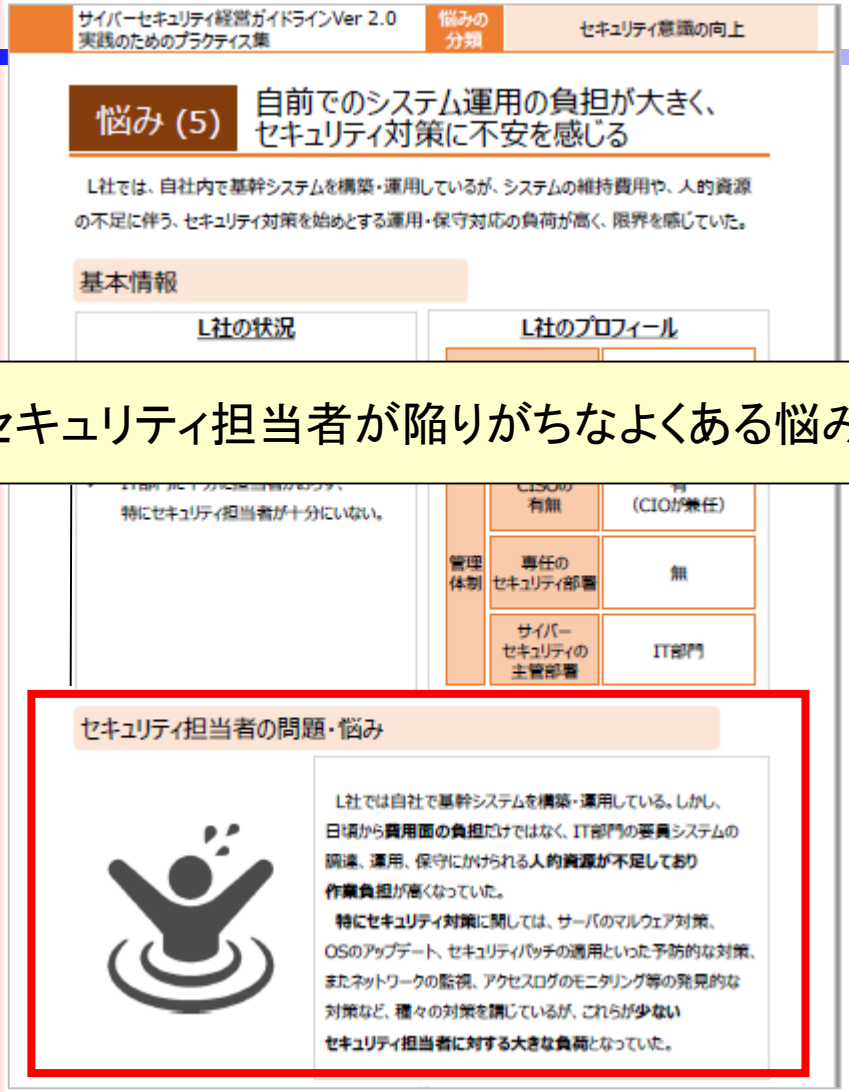
A社の実践内容

上記ステップに則り、情報システム部長が収集した事例と自社の追加対策要否をCISO等に説明し、CISOから経営会議に定期報告するプロセスとした。
(関連するサイバーセキュリティ対策の予算確保については"プラクティス3-1"を参照)

第二章（重要10項目、まずここから）

	サイバーセキュリティ経営の重要１０項目	実践のプラクティス
1	サイバーセキュリティリスクの認識、 組織全体での対応方針の策定	1-1.経営者がサイバーセキュリティリスクを認識するための、他社被害事例 の報告 1-2.セキュリティポリシーの改訂・共同管理
2	サイバーセキュリティリスク管理体制の構築	2-1.サイバーセキュリティリスクに対応するための、 兼任のサイバーセキュリティ管理体制の構築
3	サイバーセキュリティ対策のための資源 （予算、人材等）確保	3-1.サイバーセキュリティ対策のための、予算の確保 3-2.サイバーセキュリティ対策のための、必要な サイバーセキュリティ人材の定義・育成
4	サイバーセキュリティリスクの把握と リスク対応に関する計画の策定	(参考資料の提示)
5	サイバーセキュリティリスクに対応するための仕組み構築	5-1.多層防御の実施 5-2.アクセスログの取得
6	サイバーセキュリティ対策における PDCAサイクルの実施	(参考資料の提示)
7	インシデント発生時の 緊急対応体制の整備	7-1.旗振り役としてのCSIRTの設置 7-2.従業員の初動対応の定義
8	インシデントによる被害に備えた 復旧体制の整備	8-1.インシデント対応時の危機対策本部との連携 8-2.組織内外の連絡先の定期メンテナンス
9	ビジネスパートナーや委託先等を含めた サプライチェーン全体の対策及び状況把握	9-1.サイバーセキュリティリスクのある委託先の特定と 対策状況の確認
10	情報共有活動への参加を通じた 攻撃情報の入手とその有効活用及び提供	(参考資料の提示)

第三章（担当者の悩みと取り組み）


サイバーセキュリティ経営ガイドラインVer 2.0 実践のためのプラクティス集
悩みの分類 セキュリティ意識の向上

悩み (5) 自前でのシステム運用の負担が大きく、セキュリティ対策に不安を感じる

L社では、自社内で基幹システムを構築・運用しているが、システムの維持費用や、人的資源の不足に伴う、セキュリティ対策を始めとする運用・保守対応の負荷が高く、限界を感じていた。

基本情報

L社の状況

特にセキュリティ担当者が十分にいない。

L社のプロフィール

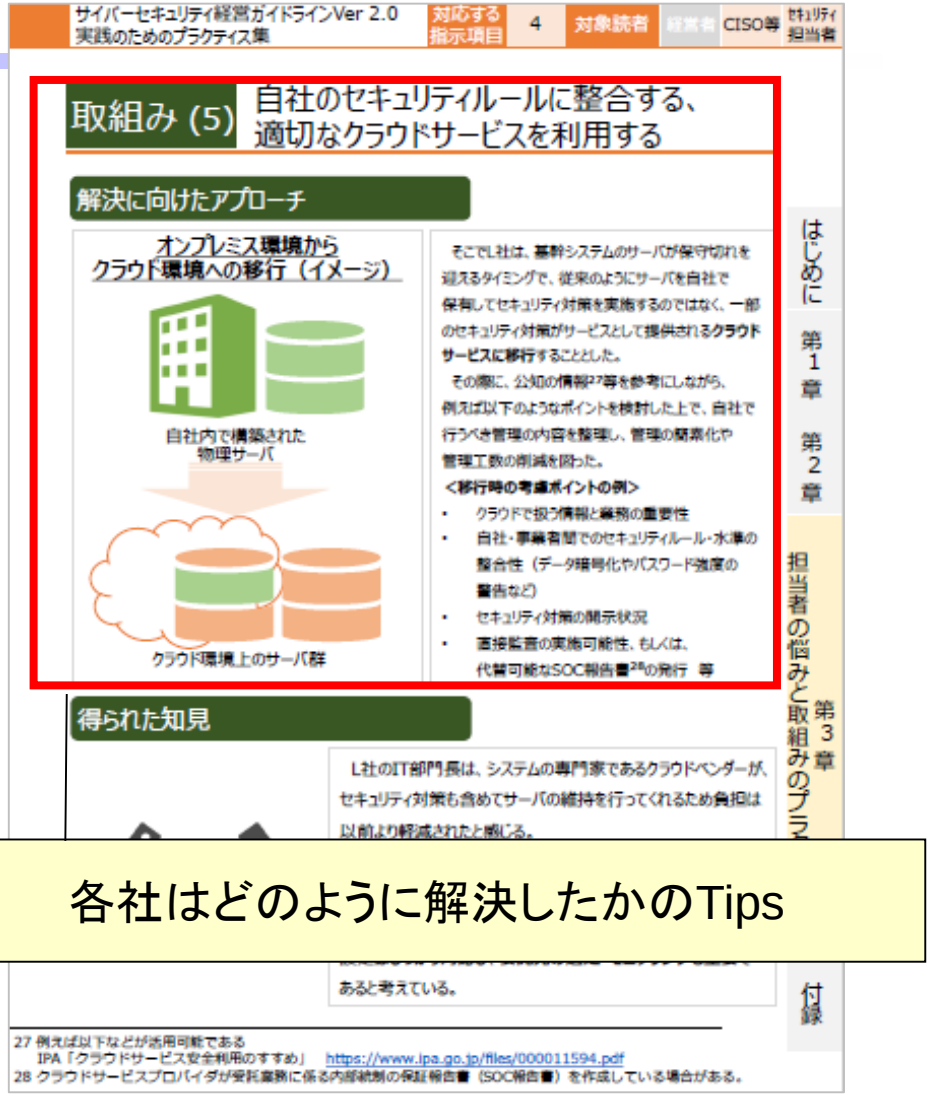
管理体制	CISOの有無	有（CIOが兼任）
	専任のセキュリティ部署	無
	サイバーセキュリティの主管部署	IT部門

セキュリティ担当者の問題・悩み

L社では自社で基幹システムを構築・運用している。しかし、日頃から**費用面の負担**だけではなく、IT部門の要員システムの調達、運用、保守にかかられる**人的資源が不足しており作業負担**が高くなっていた。

特にセキュリティ対策に関しては、サーバのマルウェア対策、OSのアップデート、セキュリティパッチの適用といった予防的な対策、またネットワークの監視、アクセスログのモニタリング等の発見的な対策など、種々の対策を講じているが、これらが**少ない**セキュリティ担当者に対する大きな負荷となっていた。

セキュリティ担当者が陥りがちなよくある悩み


サイバーセキュリティ経営ガイドラインVer 2.0 実践のためのプラクティス集
対応する指示項目 4 対象読者 経営者 CISO等 セキュリティ担当者

取組み (5) 自社のセキュリティルールに整合する、適切なクラウドサービスを利用する

解決に向けたアプローチ

オンプレミス環境からクラウド環境への移行（イメージ）

自社内で構築された物理サーバ

クラウド環境上のサーバ群

そこでL社は、基幹システムのサーバが保守切れを迎えるタイミングで、従来のようにサーバを自社で保有してセキュリティ対策を実施するのではなく、一部のセキュリティ対策がサービスとして提供される**クラウドサービスに移行**することとした。

その際に、公知の情報[27]等を参考にしながら、例えば以下のようなポイントを検討した上で、自社で行うべき管理の内容を整理し、管理の簡素化や管理工数の削減を図った。

<移行時の考慮ポイントの例>

- クラウドで扱う情報と業務の重要性
- 自社・事業者間でのセキュリティルール・水準の整合性（データ暗号化やパスワード強度の要件など）
- セキュリティ対策の開示状況
- 直接監査の実施可能性、もしくは、代替可能なSOC報告書[28]の発行 等

得られた知見

L社のIT部門長は、システムの専門家であるクラウドベンダーが、セキュリティ対策も含めてサーバの維持を行ってくれるため負担は以前より軽減されたと感じる。

あると考えている。

27 例えば以下などが活用可能である
IPA「クラウドサービス安全利用のすすめ」 https://www.ipa.go.jp/files/000011594.pdf
28 クラウドサービスプロバイダが受託業務に係る内部統制の保証報告書（SOC報告書）を作成している場合がある。

はじめに 第1章 第2章 第3章 担当者の悩みと取組みのプラ 付録

各社はどのように解決したかのTips

第三章（担当者の悩みと取り組み）

	セキュリティ担当者の悩み	取組みのプラクティス	関連する重要10項目
(1)	インシデント対応経験がない要員でCSIRTを組成したが対応に不安がある	社外専門家を活用しながら自社でサイバーセキュリティ人材を育成する	2
(2)	インシデント対応の初動における情報共有に不安がある	標的型メール訓練で開封したかではなく報告したかを意識させる	7
(3)	インシデントが起きた際の財務面でのリスクヘッジが十分ではない	初動対応のリスクを減らすサイバー保険の活用を検討する	4
(4)	IoT機器が「シャドーIT」化している	製造部門とIT部門が連携し、不正接続機器や不適切な設定を排除する	3
(5)	自前でのシステム運用の負担が大きく、セキュリティ対策に不安を感じる	自社のセキュリティルールに整合する、適切なクラウドサービスを利用する	4
(6)	全国各地の拠点におけるセキュリティ管理状況に不安がある	拠点におけるセキュリティの取組みを把握し、対面で対話する	6
(7)	外部サービスの選定でIT部門だけでは対応が困難である	社内の関連部門と連携して外部サービスの選定を行う	2
(8)	IT部門のみで経営層のセキュリティ意識を向上させることに限界を感じている	外部講師による経営層向けの研修会を実施する	1
(9)	従業員に対してセキュリティ教育を実施しているが効果が感じられない	特定の部署・役職等に向けたフォローアップの仕組みを企画し、試行する	3
(10)	スタートアップ企業のセキュリティ管理体制に不安を感じ、取引先として推奨できない	セキュリティ対策の取組み、セキュリティ認証の取得状況を確認する	9

悩み事例1： インシデント対応経験がない要員でCSIRTを組成したが対応に不安がある

サイバーセキュリティ経営ガイドラインVer 2.0 実践のためのプラクティス集

悩みの分類：セキュリティ意識の向上

悩み（1） インシデント対応経験がない要員でCSIRTを組成したが対応に不安がある

H社では、インシデント発生時に対応体制が明確でなく対応に時間を要した反省から、CSIRTを設置することとなった。しかし、自社にセキュリティ専門家が十分にいない状況であった。

基本情報

H社の状況

- ✓ 現在、セキュリティ委員会、CSIRTといったセキュリティ管理体制を構築している段階である。
- ✓ IT部門がセキュリティを主管しているが、セキュリティ専門家が十分にはいない。
- ✓ 外部ネットワークに接続していない制御システムを扱う製造部門では、セキュリティ意識が定着していないという課題がある。

H社のプロフィール

業種		製造業
規模		500人
管理体制	CISOの有無	有（CROが兼任）
	専任のセキュリティ部署	無
	サイバーセキュリティの主管部署	IT部門

セキュリティ担当者の問題・悩み

H社では、最近、ビジネスメール詐欺に遭った経験がある。

しかし、インシデント対応体制が整備されておらず、インシデント発生時の社内外への連絡体制が不十分であった。

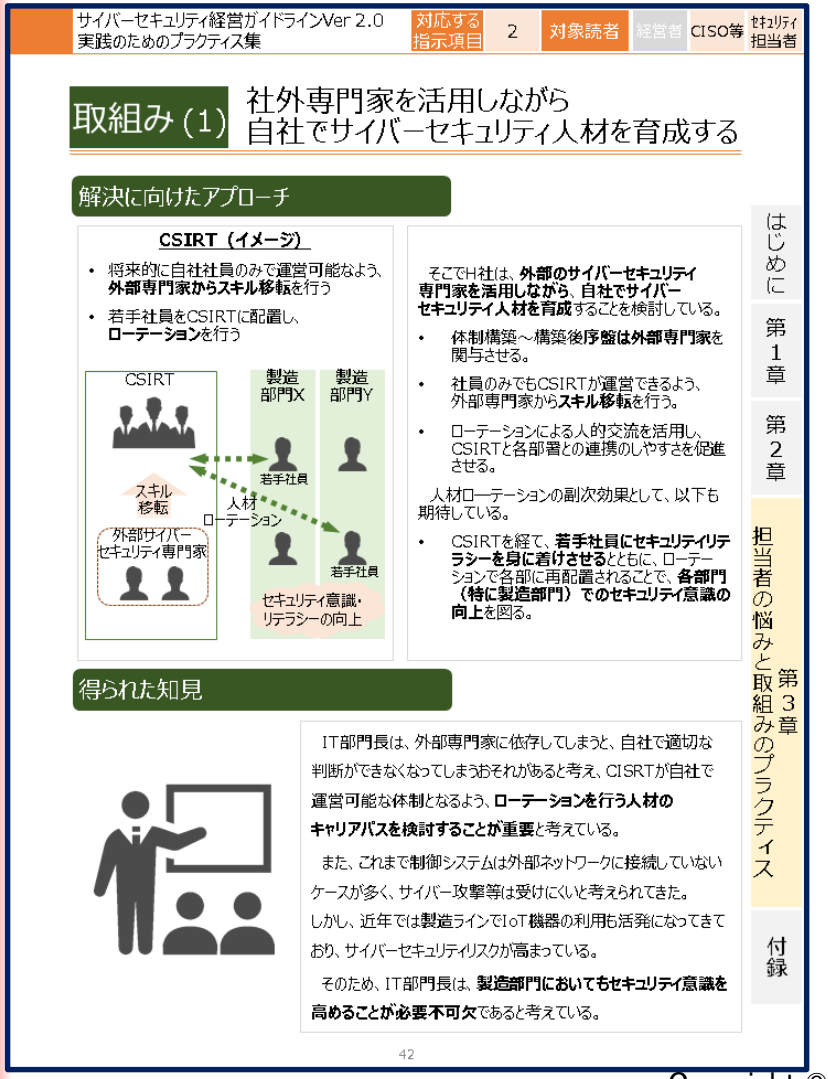
そのため、社内の関連部署や外部機関と円滑に連携できず、対応完了までに約1ヶ月もの時間を要した。

この件を受けて、IT部門長を筆頭に、**CSIRTを設置することになったが、社内にセキュリティ専門家が十分にいない**ことが問題となっていた。

41

インシデントが発生したが体制整備・経験が不足対応完了まで1か月かかった

取り組み事例1： 社外専門家を活用しながら自社でサイバーセキュリティ人材を育成



- 「**若いうちに**」セキュリティの「肌感覚を身につけさせる」
- 必要なのは「**消防団**」（プロの消防士ではない）

悩み事例2： インシデントが起きた際の財務面でのリスクヘッジが十分ではない

サイバーセキュリティ経営ガイドラインVer 2.0 実践のためのプラクティス集 | 悩みの分類 | リスク対策費用の確保

悩み (3) インシデントが起きた際の財務面でのリスクヘッジが十分ではない

J社は顧客情報を活用する業態であり、個人情報漏えい保険に加入している。しかし、サイバー攻撃等については加入している個人情報漏えい保険では補償されないケースがあると聞き、インシデント発生時の特に財務面でのリスクヘッジについて検討していた。

基本情報

J社の状況

- ✓ 製造業であり、ECサイト経由で、消費者向けに製品の販売を行っている。
- ✓ 顧客情報を活用する業態である。
- ✓ 個人情報漏えい保険に加入している。

J社のプロフィール

業種		製造業
規模		4,000人
管理体制	CISOの有無	有（CIOと兼任）
	専任のセキュリティ部署	有
	サイバーセキュリティの主管部署	セキュリティ部門

セキュリティ担当者の問題・悩み

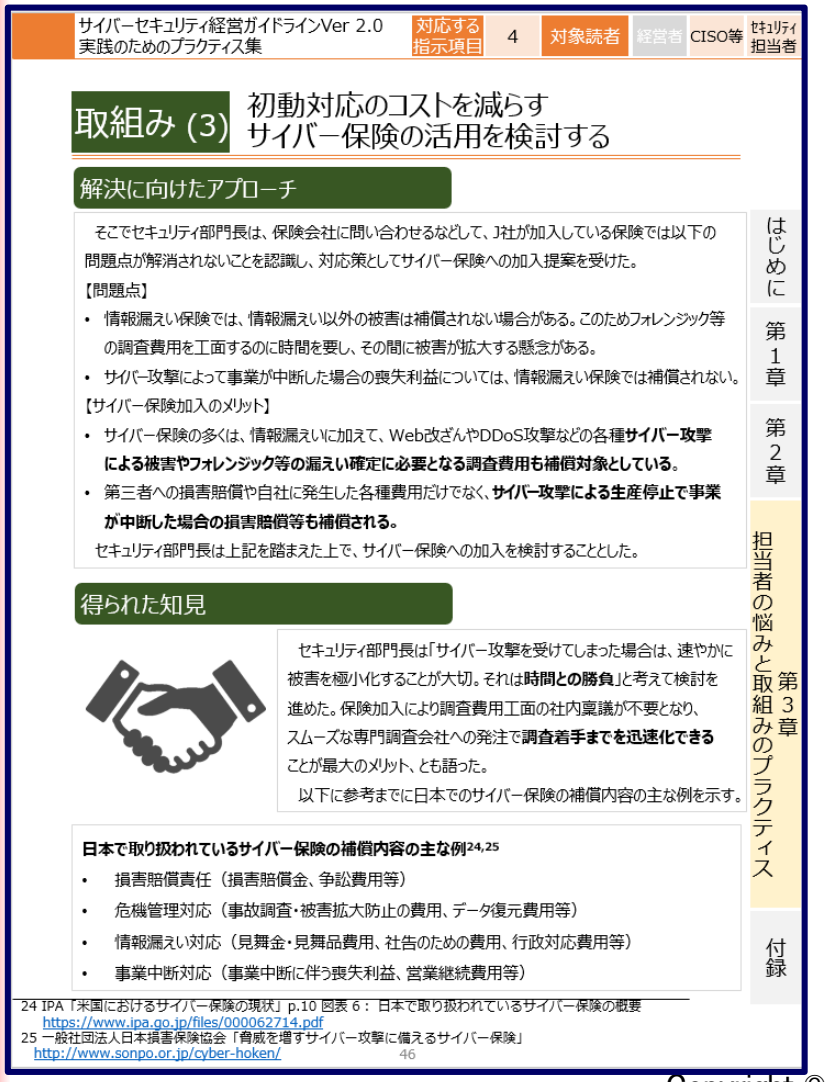
J社のセキュリティ部門長は、既存の個人情報漏えい保険ではサイバー攻撃を受けた際に生じた被害の一部や調査費用は補償されなかった、という他社事例を聞いた。

そこで、現状の個人情報漏えい保険をこのまま契約し続けるべきか、インシデント発生時のリスク対策費用確保に係る経営リスクをよりヘッジする策は他にないか、を検討すべきと感じていた。

45

個人情報漏えい保険だけで大丈夫なのか

取り組み事例2：初動対応のコストを減らす サイバー保険の活用を検討する


サイバーセキュリティ経営ガイドラインVer 2.0 実践のためのプラクティス集

対応する指示項目 4　対象読者 経営者 CISO等 セキュリティ担当者

取組み (3) 初動対応のコストを減らす サイバー保険の活用を検討する

解決に向けたアプローチ

そこでセキュリティ部門長は、保険会社に問い合わせるなどして、J社が加入している保険では以下の問題点が解消されないことを認識し、対応策としてサイバー保険への加入提案を受けた。

【問題点】

- 情報漏えい保険では、情報漏えい以外の被害は補償されない場合がある。このためフォレンジック等の調査費用を工面するのに時間を要し、その間に被害が拡大する懸念がある。
- サイバー攻撃によって事業が中断した場合の喪失利益については、情報漏えい保険では補償されない。

【サイバー保険加入のメリット】

- サイバー保険の多くは、情報漏えいに加えて、Web改ざんやDDoS攻撃などの各種**サイバー攻撃による被害やフォレンジック等の漏えい確定に必要となる調査費用も補償対象としている。**
- 第三者への損害賠償や自社に発生した各種費用だけでなく、**サイバー攻撃による生産停止で事業が中断した場合の損害賠償等も補償される。**

セキュリティ部門長は上記を踏まえた上で、サイバー保険への加入を検討することとした。

得られた知見

セキュリティ部門長は「サイバー攻撃を受けてしまった場合は、速やかに被害を極小化することが大切。それは**時間との勝負**」と考えて検討を進めた。保険加入により調査費用工面の社内稟議が不要となり、スムーズな専門調査会社への発注で**調査着手までを迅速化できる**ことが最大のメリット、とも語った。

以下に参考までに日本でのサイバー保険の補償内容の主な例を示す。

日本で取り扱われているサイバー保険の補償内容の主な例[24,25]

- 損害賠償責任（損害賠償金、争訟費用等）
- 危機管理対応（事故調査・被害拡大防止の費用、データ復元費用等）
- 情報漏えい対応（見舞金・見舞品費用、社告のための費用、行政対応費用等）
- 事業中断対応（事業中断に伴う喪失利益、営業継続費用等）

はじめに　第1章　第2章　第3章 担当者の悩みと取組みのプラクティス　付録

24 IPA「米国におけるサイバー保険の現状」p.10 図表 6： 日本で取り扱われているサイバー保険の概要 https://www.ipa.go.jp/files/000062714.pdf

25 一般社団法人日本損害保険協会「脅威を増すサイバー攻撃に備えるサイバー保険」 http://www.sonpo.or.jp/cyber-hoken/

46

- **調査費用を保険でカバー**
- **初動対応の迅速さを確保**

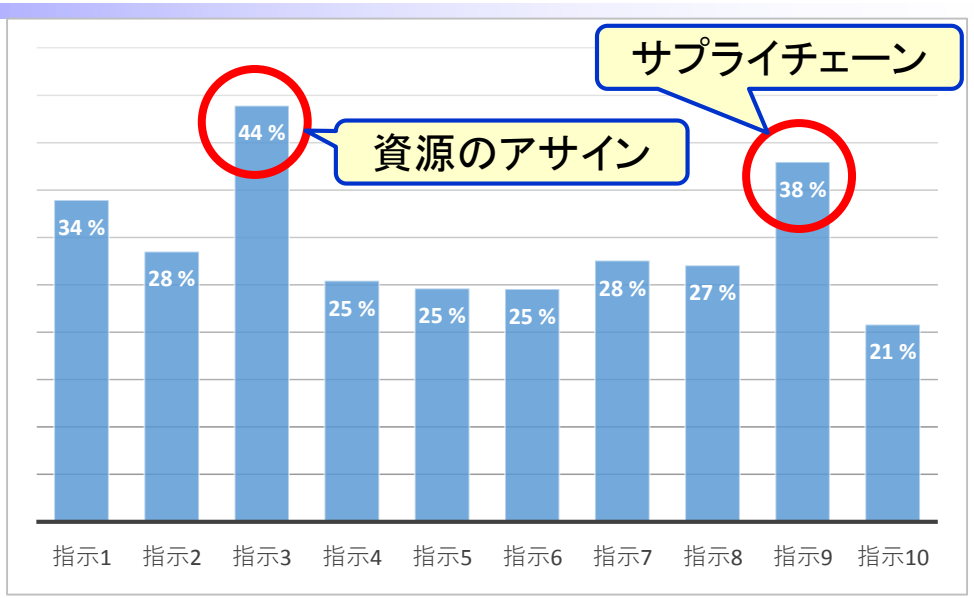
反響

- 3月25日～4月23日のプラクティス集ダウンロード数＝2639

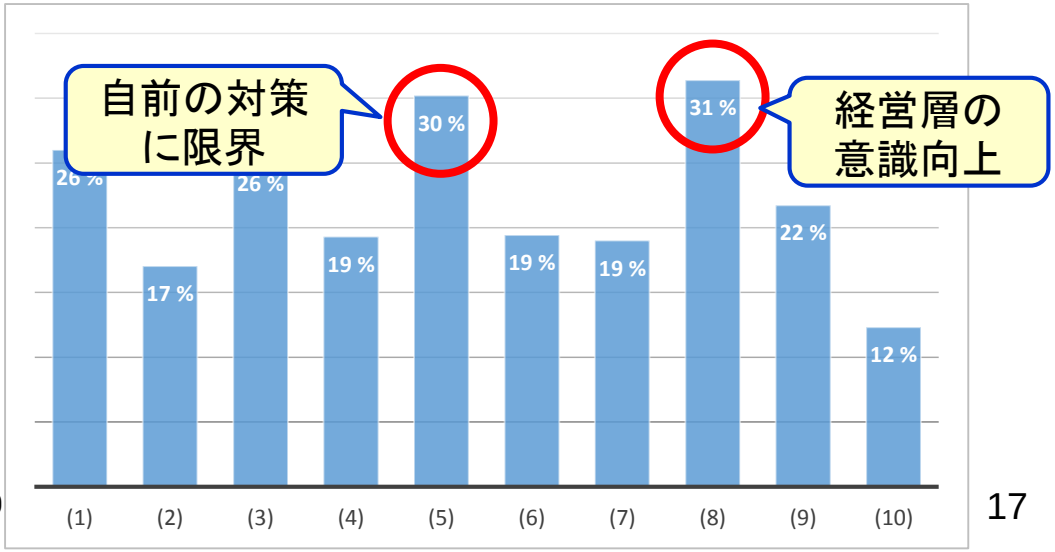
- ブログ等からのコメント
  - 実践する内容やステップ、得られた知見、アウトプットの例などが記載されており、必ずしも記載の方法に沿う必要はないが、計画・実行上の参考になる内容が多く記載
  - ゼロから考えるよりもこのような資料を参考にし、実現段階で詳細を決める際には専門家の力を借りるのがスムーズに進める方法になると考えられる
  - 担当者の悩みに注目したのはいいと思う

プラクティス集ダウンロード時のアンケート結果（2019/3/25～4/23, N=2639）

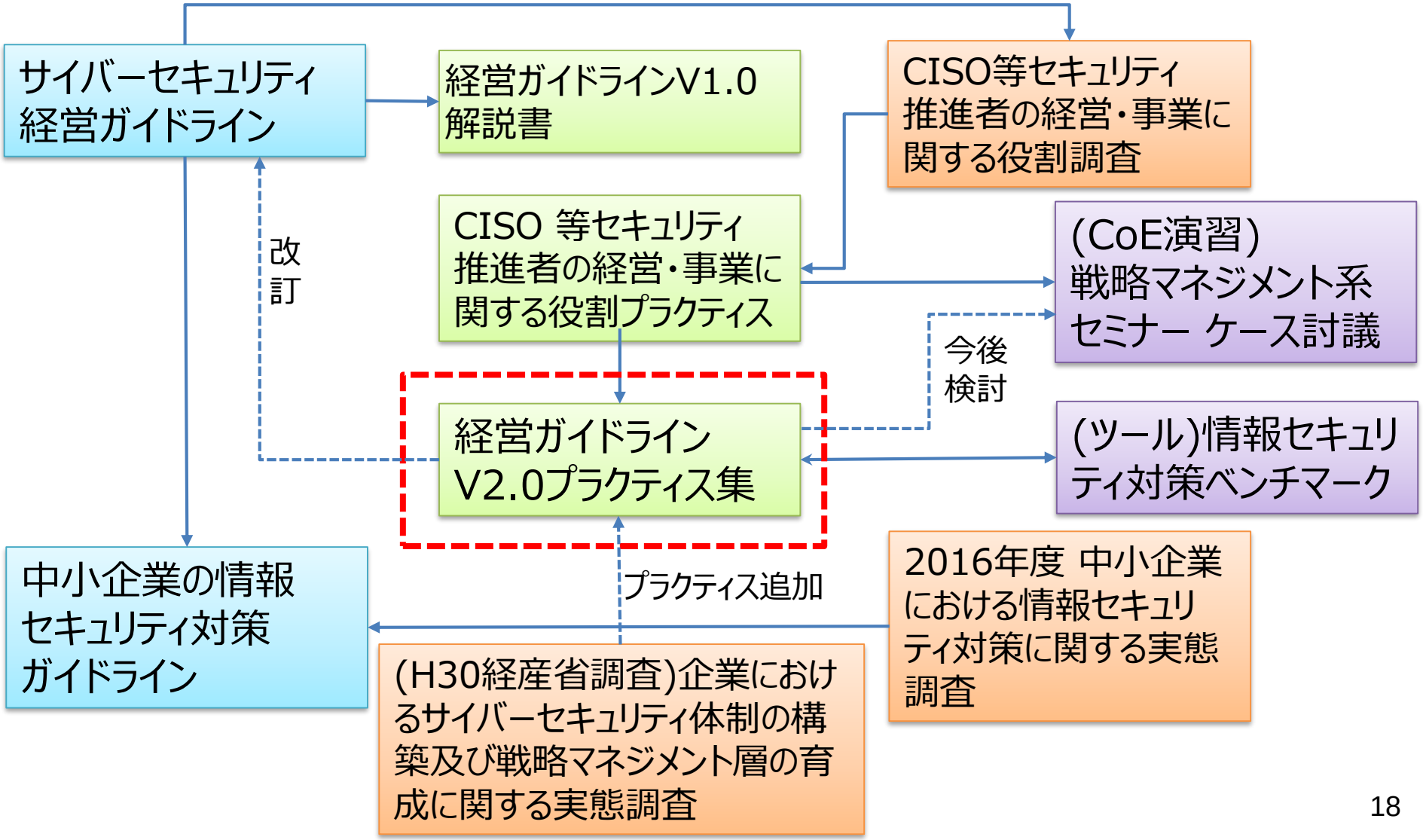
Q1.　サイバーセキュリティ経営ガイドラインに記載の重要10項目について、あなたもしくはあなたの組織で実践に困っていると思われる項目はありますか？



Q2.　あなたもしくはあなたの組織において、困っていることや共感できる課題はありますか？



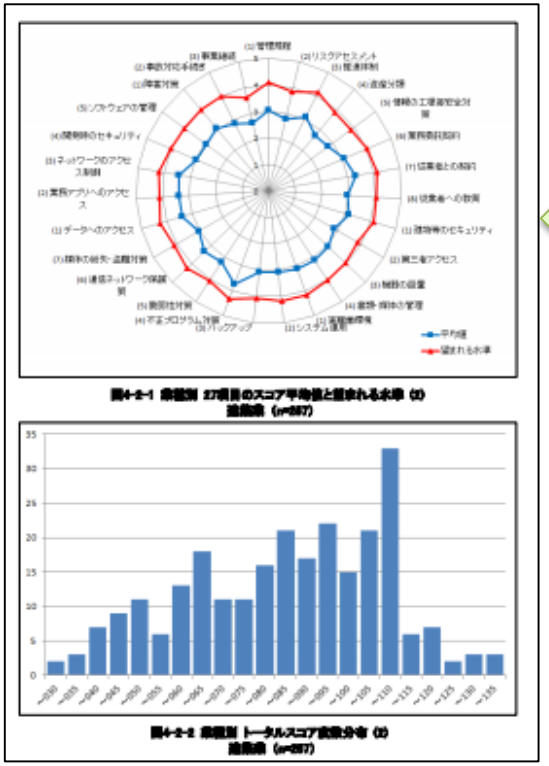
参考：ガイドライン・プラクティス・ツール等の関係



参考：ガイドライン実践の可視化検討状況

- Cybermaturity Platform（ISACA）、CAT(*)（FFIEC）等の可視化ツールを調査。情報セキュリティベンチマーク（IPA）の拡張可能性を検討。

情報セキュリティベンチマーク



項目追加・見直し

整合性を考慮すべきガイドライン

- サイバーセキュリティ経営ガイドライン（METI、IPA）
- サイバーセキュリティフレームワーク（NIST）
- サイバー・フィジカル・セキュリティ対策フレームワーク（METI）

ベンチマークの評価項目と経営ガイドラインを比較し、不足している項目の例

- 経営者がサイバーセキュリティ対策の報告を受けていること
- サイバーセキュリティに関する注意喚起情報等の情報共有、提供を行っていること

(*)FFIEC CAT（FFIEC（米国連邦金融機関検査協議会）が公開するCybersecurity Assessment Tool）

Thank you！