経済産業省

資料４

経営リスクとしてのサイバーセキュリティ対策
～サイバーセキュリティ経営ガイドラインのポイント解説～

経済産業省

商務情報政策局

サイバーセキュリティ課

１．サイバーセキュリティ経営ガイドライン概要

２．ガイドライン改訂のポイント

サイバーセキュリティ対策における経営者の役割

- 企業戦略として、どの程度ITに対する投資やセキュリティ投資を行うかは経営判断。
- 場合によっては経営者責任を問われる恐れ。

経営判断が必要

- 企業戦略として、どの程度IT投資を行うか
  （生産性向上、ビジネス拡大）
- その中で、どの程度セキュリティ投資を行うか
  （企業価値向上）

経営者のリスク対応の是非、経営者責任について社会から問われる恐れ

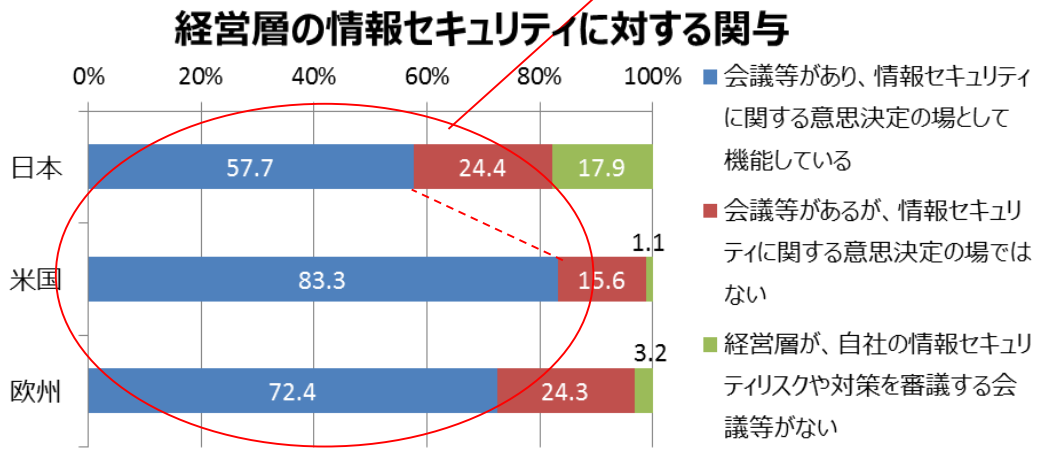
例えば、以下のような時に問われる恐れがある

- サイバー攻撃により個人情報や秘密情報が漏洩した場合
- インフラの供給停止など、社会に損害を与えてしまった場合

サイバーセキュリティ対策の現状（経営者の意識）

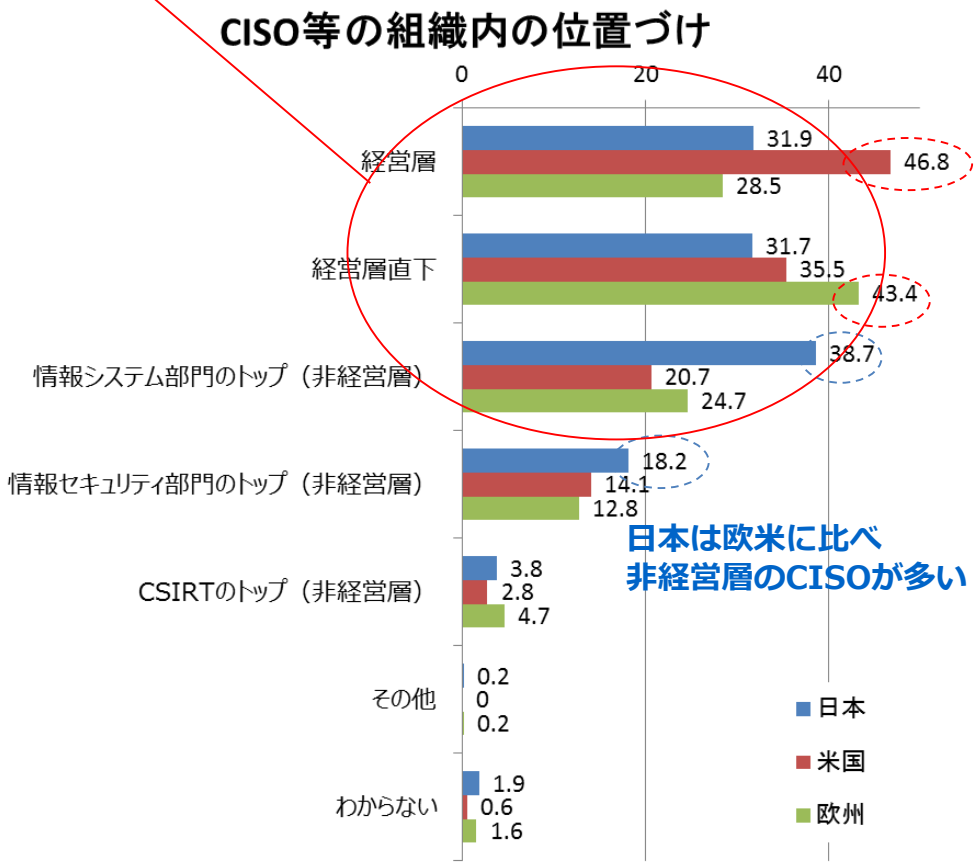
- 日本では、サイバーセキュリティ対策において、経営者が十分なリーダーシップを発揮していない可能性がある。

情報セキュリティの意思決定に経営層が関わるのは米国の2/3

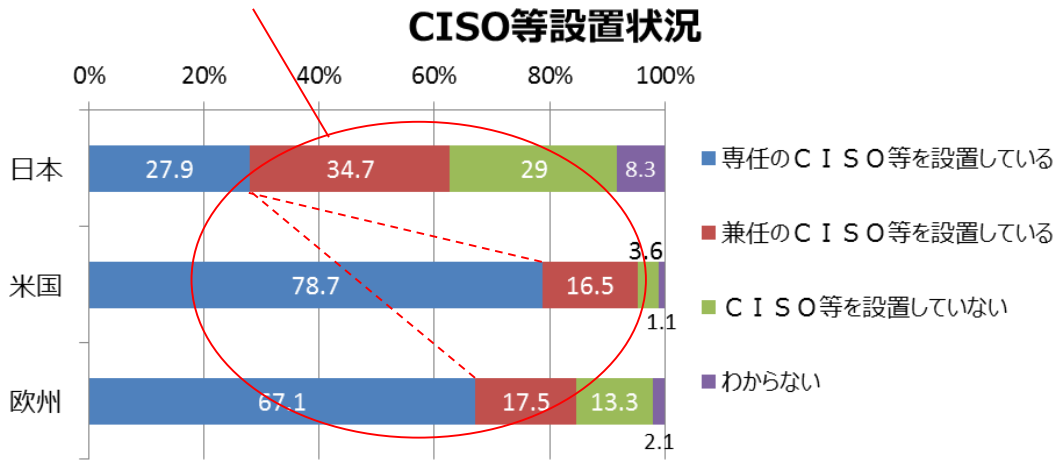


欧米は経営層に紐づくCISO※が多い

※Chief Information Security Officer（シーアイエスオー、シーソ）



日本の専任CISOは欧米の半分以下



日本は欧米に比べ非経営層のCISOが多い

出典：独立行政法人情報処理推進機構「企業のCISOやCSIRTに関する実態調査2017-調査報告書-」（2017年4月13日）

＊日本・米国・欧州（英・独・仏）の従業員数300人以上の企業のCISO、情報システム／情報セキュリティ責任者／担当者等にアンケートを実施（2016年10～11月）

＊回収は日本755件、米国527件、欧州526件

サイバーセキュリティ経営ガイドライン

- 経営者のリーダーシップによってサイバーセキュリティ対策を推進するため、**経営者が認識すべき3原則**と、**経営者がセキュリティの担当幹部（CISO等)に指示すべき重要10項目**を提示。

1．経営者が認識すべき３原則

（１）経営者が、**リーダーシップを取って対策**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を含めた対策**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

2．経営者がCISO等に指示すべき１０の重要事項

リスク管理体制の構築

（１）組織全体での対策方針の策定
（２）方針を実装するための体制の構築
（３）予算・人材等のリソース確保

リスクの特定と対策の実装

（４）リスクを洗い出し、計画の策定
（５）リスクへの対応
（６）PDCAの実施

インシデントに備えた体制構築

（７）緊急対応体制の構築
（８）復旧体制の構築

サプライチェーンセキュリティ

（９）サプライチェーンセキュリティの確保

関係者とのコミュニケーション

（10）情報共有活動への参加

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３原則）

① 経営者は、IT活用を推進する中で、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 自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の**委託先を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**、サイバーセキュリティリスクや対策、対応に係る情報の開示など、**関係者との適切なコミュニケーション**が必要

経営者がCISO等に指示をすべき１０の重要事項 －全体像－

経営者

【３原則】
１．経営者のリーダーシップが重要
２．自社以外（ビジネスパートナー等）にも配慮
３．平時からのコミュニケーション・情報共有

ACT

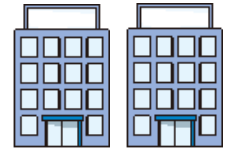
指示

報告

①サイバーセキュリティ対応方針策定

PLAN

内外に宣言・開示



ステークホルダー
（株主、顧客、取引先等）

②リスク管理体制の構築

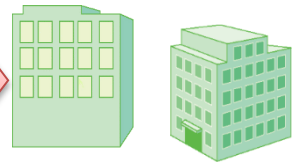
サイバーセキュリティリスク管理体制

◆経営リスク委員会等
他の体制と整合
（ex.内部統制、災害対策）

CISO等の担当幹部

③資源(予算、人材等)の確保

⑨サプライチェーンセキュリティ対策



ビジネスパートナー

DO

セキュリティ担当、CSIRT等

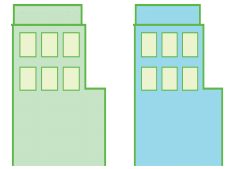
④リスクの把握と対応計画策定

⑤保護対策(防御・検知・分析)の実施

⑦緊急対応体制の整備

⑧復旧体制の整備

⑩情報共有活動への参加



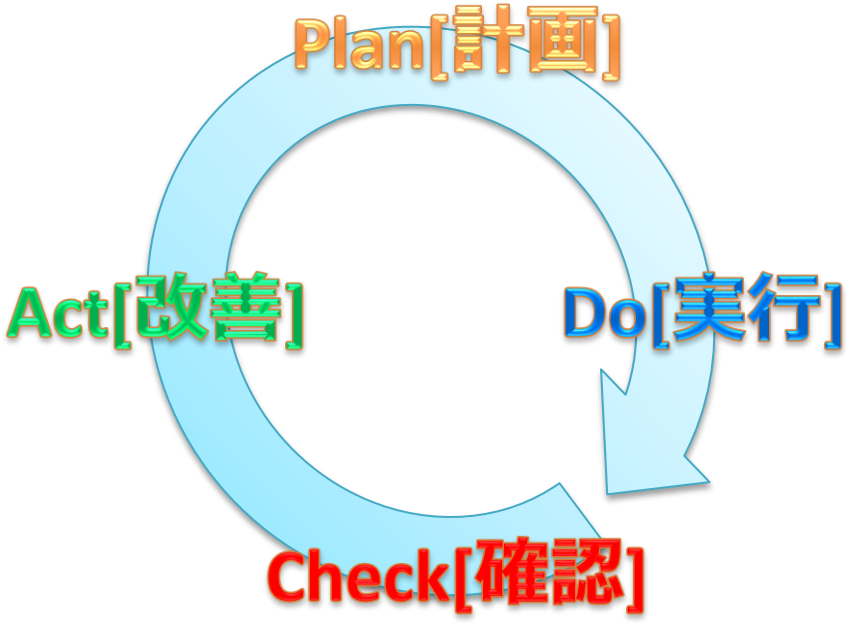
情報共有団体・コミュニティ

CHECK

⑥PDCAの実施

（参考）経営者がCISO等に指示をすべき１０の重要事項
(6)サイバーセキュリティ対策フレームワーク構築(PDCA)と対策の開示

計画が確実に実施され、改善が図られるよう、PDCAを実施させること。



計画の確実な実施と、改善

経営者への報告

KPIの設定など、
経営者が把握できるよう
可視化して報告

KPIの例

- セキュリティ投資額
- リスク分析の実施回数
- リスクアセスメントの指摘事項数
- セキュリティ教育受講率

情報開示に関する言及（ガイドラインの対策例より該当箇所抜粋）

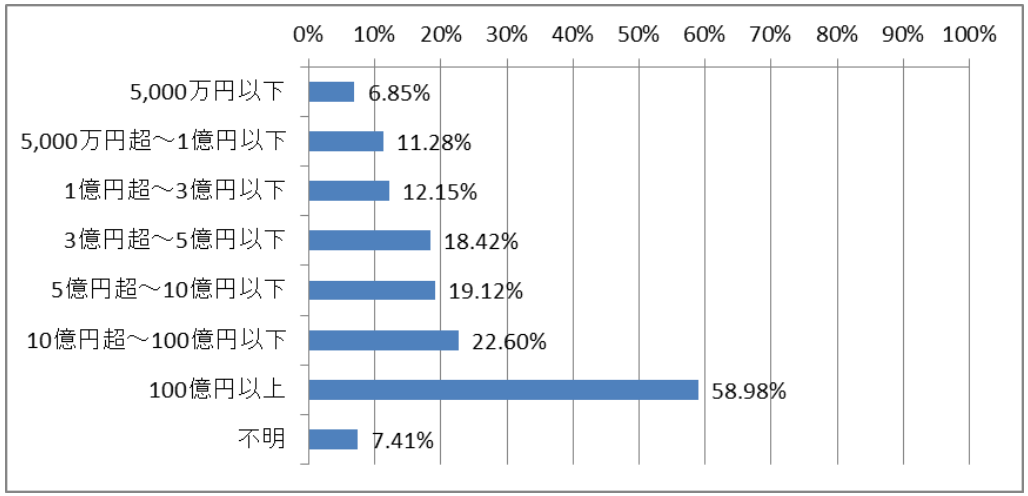
- サイバーセキュリティ対策の状況について、サイバーセキュリティリスクの性質・度合いに応じて、情報セキュリティ報告書、CSR報告書、サステナビリティレポートや有価証券報告書等への記載を通じて開示を検討する。

（参考）企業における経営ガイドラインの活用状況

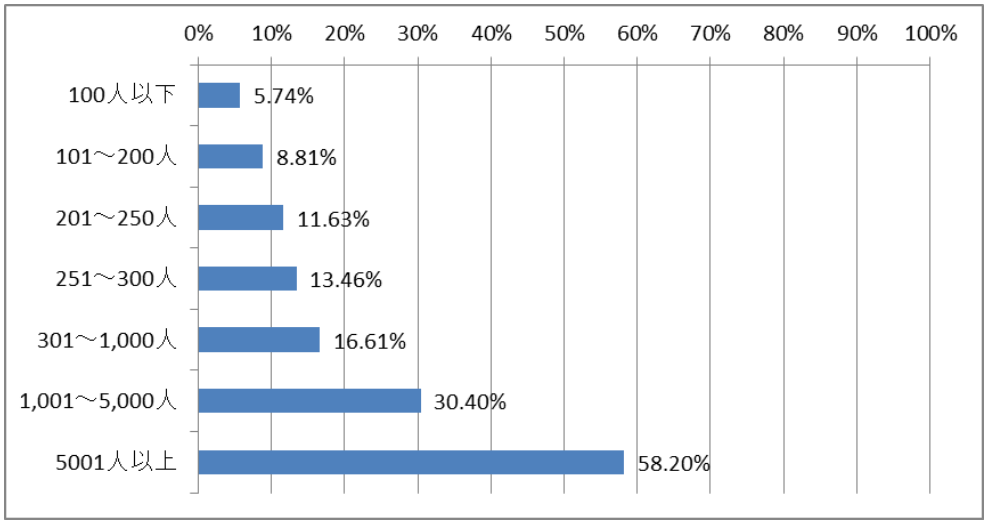
- 企業規模が大きくなるにつれて経営ガイドラインの実施率が高くなっている。
- 特に資本金100億円以上、従業員数5,001人以上の企業においては60%近くが当該ガイドラインを活用している。

経営ガイドラインの参照状況（全体）

経営ガイドラインの参照状況（資本金別）



経営ガイドラインの参照状況（従業員数別）



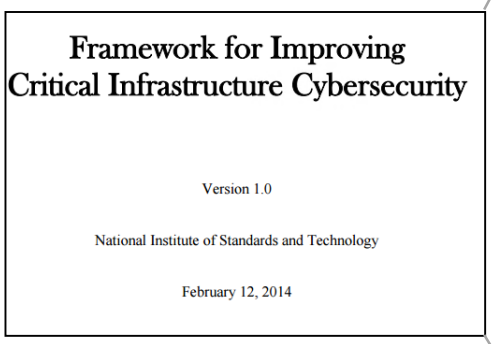
(*)平成28年度我が国におけるデータ駆動型社会に係る基盤整備（情報処理実態調査の分析及び調査設計等事業）調査報告書（経済産業省）のデータを元に作成
http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/pdf/H28_report.pdf

１．サイバーセキュリティ経営ガイドライン概要

２．ガイドライン改訂のポイント

ガイドライン改訂前の主な課題

- 昨今のサイバー攻撃の巧妙化により事前対策だけでは対処が困難。
- 米国のサイバーセキュリティフレームワークでも事前対策だけでなく、事後（**検知、対応、復旧**）対策を要求。
- 一方で従来のガイドラインは**国際的な状況を踏まえるとガイドラインとの整合性が不十分**。



	重要10項目の項番（Ver1.1）
特定	1、2、3、5、7、8
防御	3、6
検知	–
対応	9、10
復旧	–

重要１０項目の整理

- 新規に２項目（(5)対策実施と(8)復旧）追加するとともに、既存の項目を再整理した。
- 重要１０項目の並びについても、３原則、及び作業の時系列を意識して再整理した。
- (7)の参考資料として付録C「インシデント発生時に組織内で整理しておくべき事項」を新規に追加した。

1.リーダーシップの表明と体制の構築	
(1)	セキュリティポリシーの策定
(2)	サイバーセキュリティリスク管理体制の構築
2.サイバーセキュリティリスク管理の枠組み決定	
(3)	リスクの把握、対策目標と計画の策定
(4)	PDCAの実施と対策の開示
(5)	サプライチェーンセキュリティ対策の実施
3.サイバー攻撃を防ぐための事前対策	
(6)	セキュリティ対策のための資源確保
(7)	ITシステム管理の委託範囲の特定
(8)	情報共有活動への参加
4.サイバー攻撃を受けた場合に備えた準備	
(9)	緊急時の対応体制の整備
(10)	被害発覚後の準備

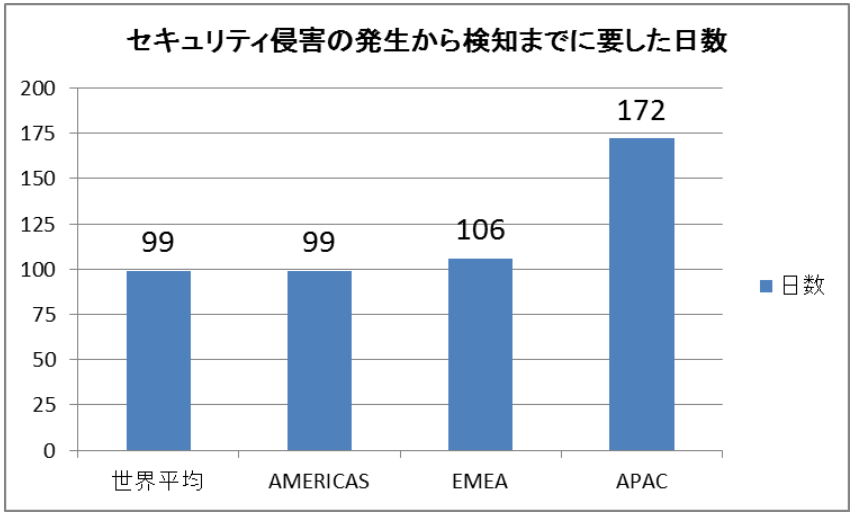
＜経営者がリーダーシップをとった対策の推進＞	
セキュリティマネジメント体制の構築	
(1)	セキュリティポリシーの策定
(2)	サイバーセキュリティリスク管理体制の構築
(3)	セキュリティ対策のための資源確保
セキュリティリスクの特定と対策の実装	
(4)	リスクの把握、対策目標と計画の策定
(5)	リスク対応策（防御・検知・分析）の実施
(6)	PDCAの実施と対策の開示
サイバー攻撃を受けた場合に備えた体制構築	
(7)	緊急時の対応体制の整備
(8)	復旧体制の整備
＜サプライチェーンセキュリティ対策の推進＞	
(9)	サプライチェーンセキュリティ対策の実施
＜関係者とのコミュニケーションの推進＞	
(10)	情報共有活動への参加

新規追加項目　類似項目をマージ

事後対策の強化　～検知･復旧対策の実施～

- 重要項目　指示5として「攻撃の検知」に関する、「サイバーセキュリティリスクに対応するための仕組みの構築」を追加

- サイバー攻撃による被害を最小限にするためには早期に検知することが重要。
- 約半数の企業が外部からの指摘によりサイバー攻撃による被害が発覚している状況であり、**<u>サイバー攻撃を自分たちで気づけていない</u>**ケースが多い。



APAC（アジア太平洋）
EMEA（欧州、中東及びアフリカ）

（出典）FireEye. Inc.
「M-trends2017：セキュリティ最前線からの視点」より経済産業省作成

- 重要項目　指示8 として「復旧」に関する、「サイバーセキュリティリスクに対応するための仕組みの構築」を追加

企業においてBCPの策定・訓練の実施が進んでいるが、自然災害対策等を想定しており、**<u>サイバー攻撃についての復旧が意識されていない</u>**ケースが多い。

サプライチェーン対策の強化

- 重要項目　指示9の「サプライチェーンのビジネスパートナーや委託先等を含めたサイバーセキュリティ対策の実施及び状況把握」において、委託先におけるリスクマネーの確保や委託先の組織としての活用の把握（ISMSやSECURITY ACTION）等の留意点を追記

日本企業の自社のセキュリティ点検は欧米にやや遅れる程度だが、委託先等へのケアは大幅に遅れている。

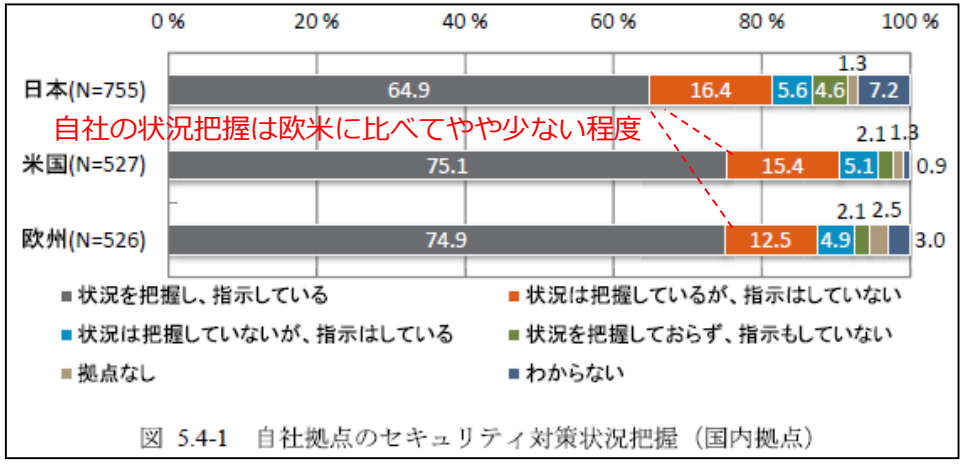


図　5.4-1　自社拠点のセキュリティ対策状況把握（国内拠点）

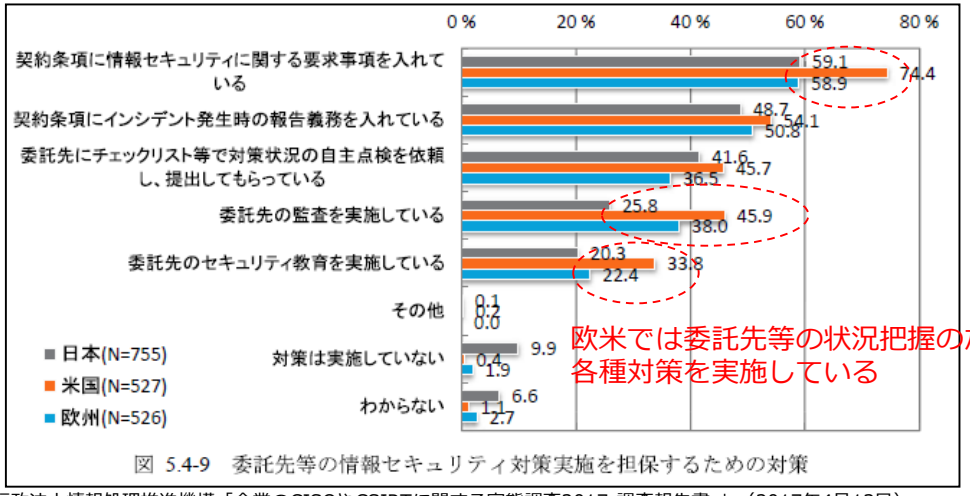


図　5.4-9　委託先等の情報セキュリティ対策実施を担保するための対策

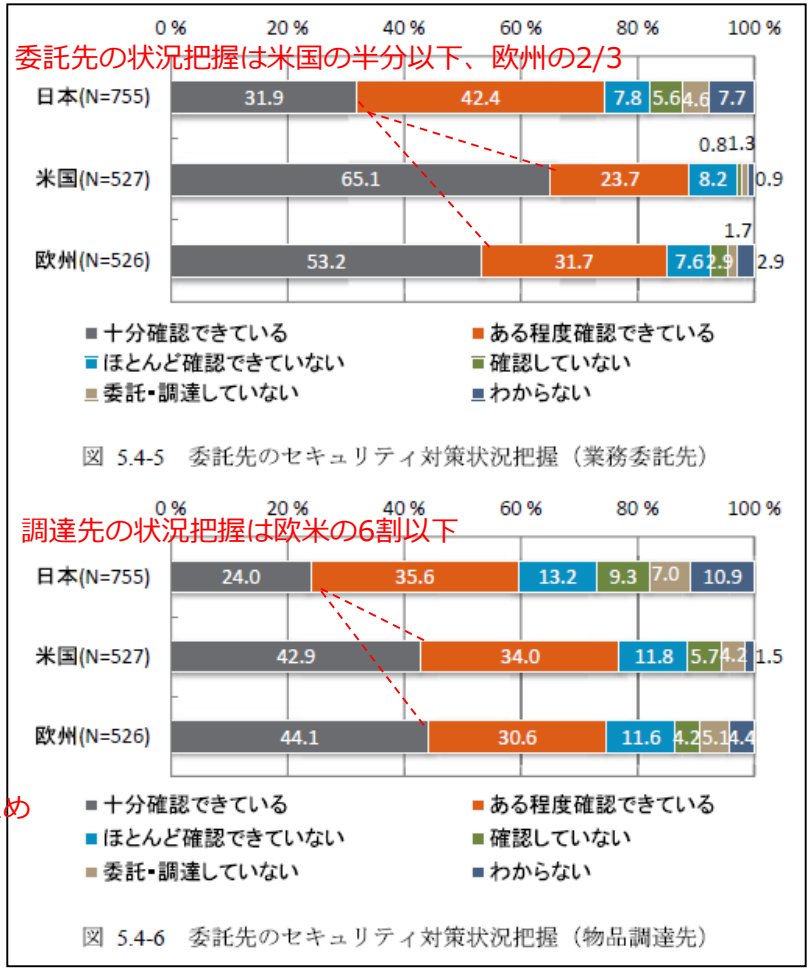


図　5.4-5　委託先のセキュリティ対策状況把握（業務委託先）

図　5.4-6　委託先のセキュリティ対策状況把握（物品調達先）

出典：独立行政法人情報処理推進機構「企業のCISOやCSIRTに関する実態調査2017-調査報告書-」（2017年4月13日）

＊日本・米国・欧州（英・独・仏）の従業員数300人以上の企業のCISO、情報システム／情報セキュリティ責任者／担当者等にアンケートを実施（2016年10～11月）＊回収は日本755件、米国527件、欧州526件

（参考）欧米において強化される『サプライチェーン』サイバーセキュリティへの要求

- **米国、欧州は、サプライチェーン全体に及ぶサイバーセキュリティ対策を模索。**
- 国内でも、**Connected Industriesの進展、ボットネット対策から、製品・サービスに対する、より一層のサイバーセキュリティ対策の推進が求められる。**

【米国】

- **サイバーセキュリティフレームワーク（NIST策定のガイドライン）に、『サイバーサプライチェーンリスクマネジメント』を明記へ**
- **防衛調達に参加する全ての企業に対してセキュリティ対策（SP800-171の遵守）を義務化**

【欧州】

- **単一サイバーセキュリティ市場を目指し、ネットワークに繋がる機器の認証フレームの導入を検討**
- 既に、**エネルギー等の重要インフラ事業者は、セキュリティ対策が義務化（NIS Directive）**

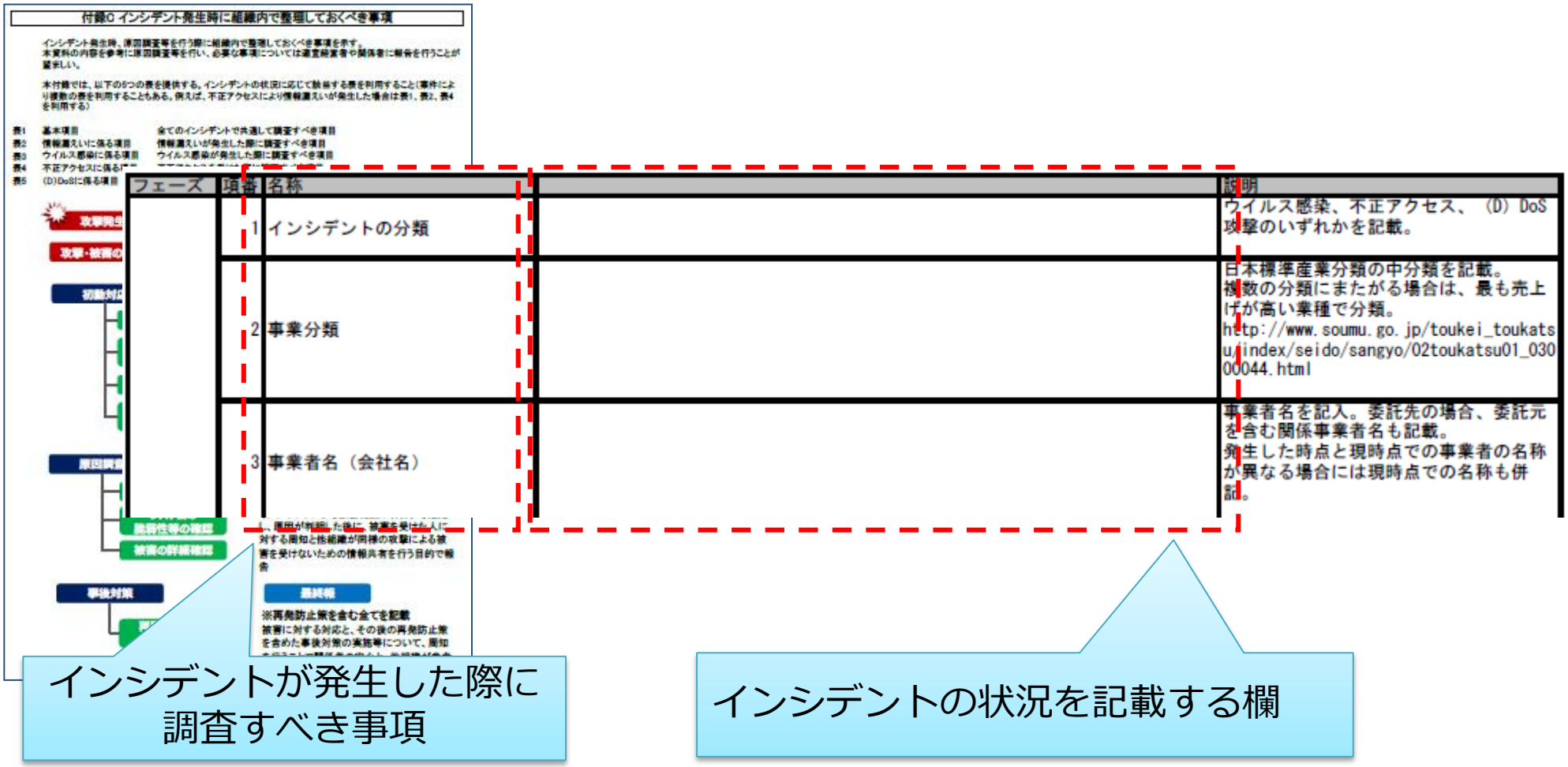
セキュリティ要件を満たさない事業者、製品、サービスはグローバルサプライチェーン、国内サプライチェーンからはじき出されるおそれ

【国内】Connected Industriesの推進、ボットネット対策

- 「つながる」ことを前提とするコネクテッドインダストリーにおいて、サイバーセキュリティの確保は必要条件
- 2020年東京オリパラに向けて、ボットネット撲滅の推進を決定

（参考）付録C インシデント発生時に組織内で整理しておくべき事項

- 事後対策の対応力を強化するために、インシデント発生時に組織として整理しておくべき事項を付録Cで提示。



その他の改訂ポイント

＜NISTのサイバーセキュリティフレーワークとの対応関係の提示＞

- 付録Aの各チェック項目について、NISTのサイバーセキュリティフレームワークと対応する項目を提示。

＜冒頭の説明の見直し＞

- 「サイバーセキュリティ経営ガイドライン・概要＞の説明を全体的に修正。
- IoTやAIの活用といった最近の情勢をふまえるとともに、サプライチェーンセキュリティの必要性が高まっていることや、セキュリティ対策を怠ると他社に迷惑をかけることもある等についても言及。

＜統計データのアップデート＞

- １．１節「サイバーセキュリティ経営ガイドラインの背景と位置づけ」で参照している統計データをアップデート。それに伴い説明文も修正。

＜情報共有活動における情報提供の記載を強調＞

- 重要１０項目の（１０）において、従来は「情報の入手とその有効活用」となっていた部分を「情報の提供、及び入手とその有効活用」に修正。

＜その他＞

- 経営者、CISOを対象読者としていることから、全体のボリュームを減らすために冗長な表現の見直し、及び記載を簡素化。