サイバーセキュリティ経営ガイドライン解説セミナー

1．サイバーセキュリティ経営ガイドラインとその背景

株式会社ISO審査登録機構

サイバーセキュリティ経営ガイドライン

○サイバーセキュリティ経営ガイドラインとは

閣議決定された「サイバーセキュリティ戦略」を基に**経営責任**として
サイバーセキュリティ対策の必要性を示したもの。

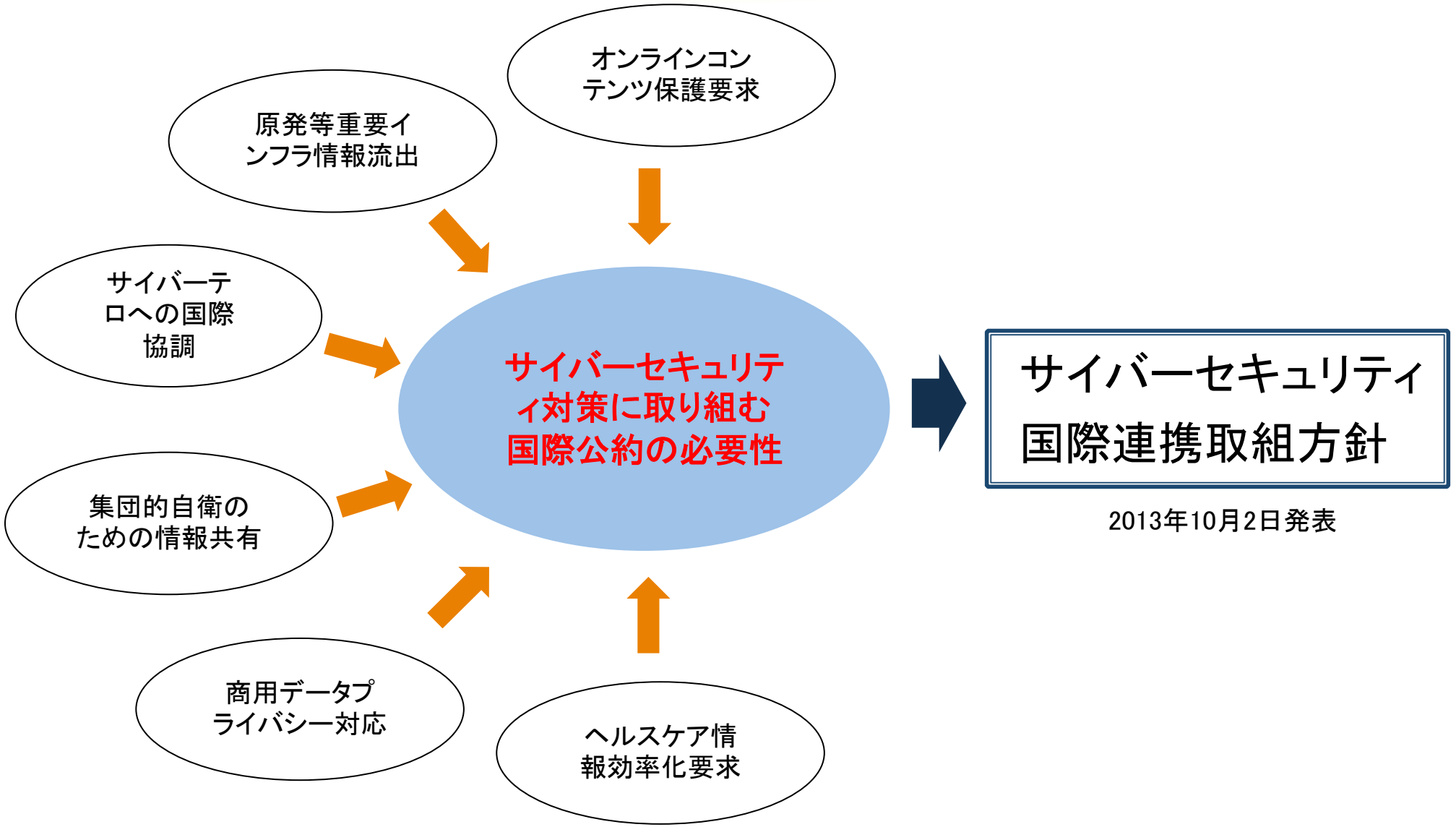
○経営者が認識する必要がある「**三原則**」
○情報セキュリティ対策を実施する上での責任者となる担当
幹部（CISO等）に指示すべき「**重要10項目**」
からなる。

○対象企業

大企業及び中小企業（小規模事業者を除く）のうち、ITに関するシステムやサービス等を供給する企業及び**経営戦略上ITの利活用が不可欠である企業**

➡ 実質、小規模事業者（20人以下、商業・サービス業は5人以下）を除く、**全企業対象**

ガイドライン成立の背景（国際環境）



ガイドライン成立の背景(社会環境)

サイバー攻撃の増加

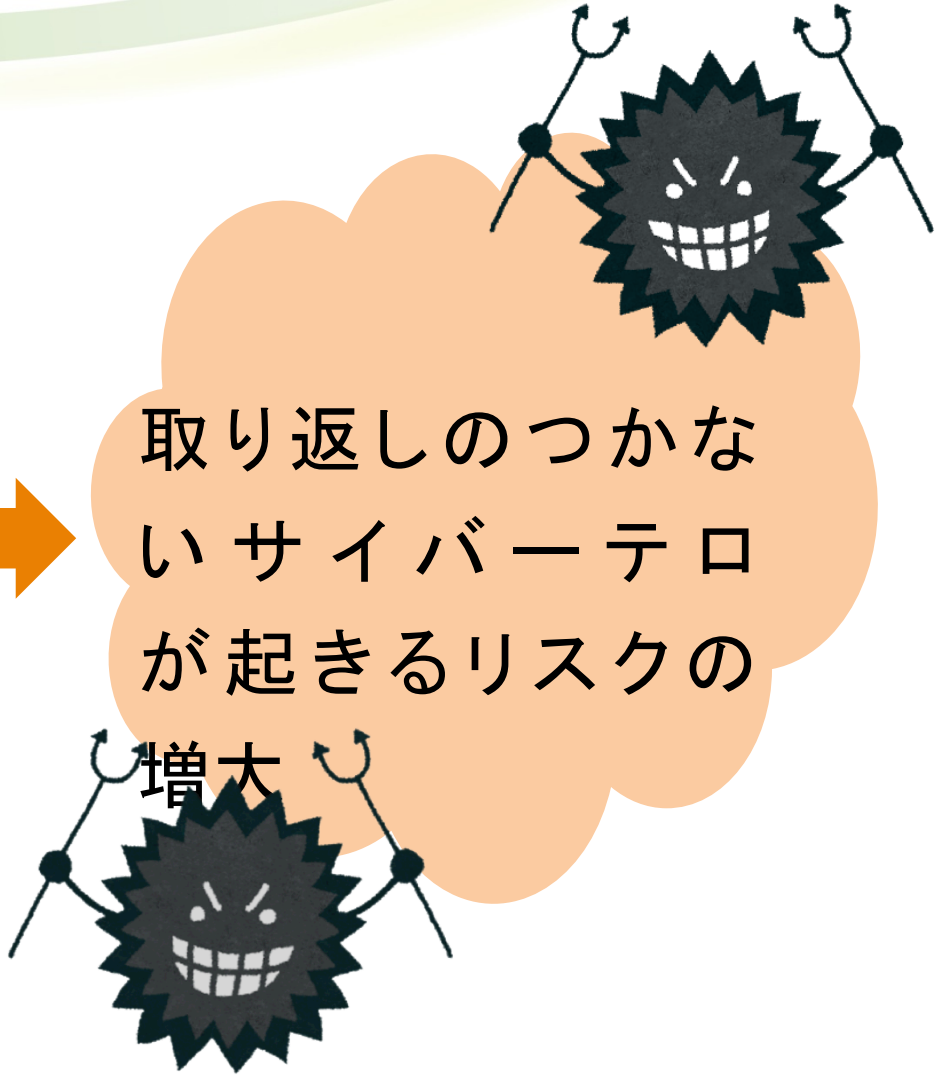
・年金機構への標的型攻撃
・国際組織アノニマス
・Webサイト改ざん多発　等

被害の大型化・深刻化

・ベネッセ個人情報漏洩事件
・原発システムへの侵入
・ビットコイン流出　等

経営層認識の後進性

・セキュリティ投資額の低さ
・CISOの不在　等



ガイドライン成立の背景（現状）

サイバーセキュリティ人材の“圧倒的”不足

政府機関ですら、人材の“圧倒的”不足を自覚した。

・各省庁のIT・セキュリティリテラシーの不足

弊害例：厚生労働省マイナンバー汚職事件

不足の人材

・橋渡し人材 ➡ 情報セキュリティマネジメント資格　新設
・高度専門人材 ➡ 情報処理安全確保支援士　創設
・突出した能力を有した人材 ➡ 未踏IT人材発掘・育成事業

ガイドライン成立の背景（サイバーセキュリティ基本法）

○サイバーセキュリティ基本法

省庁の縦割り対策から、NISC（内閣サイバーセキュリティセンター）が、各省庁全ての情報セキュリティ体制を監視できるようになる。

➡ 成果：年金機構標的型攻撃の発見

年金機構型の標的型攻撃では民間企業にも影響が出る。
⇒民間企業も情報セキュリティ体制の確立が不可欠

☆サイバーセキュリティ基本法改正案可決（2015.4.15）

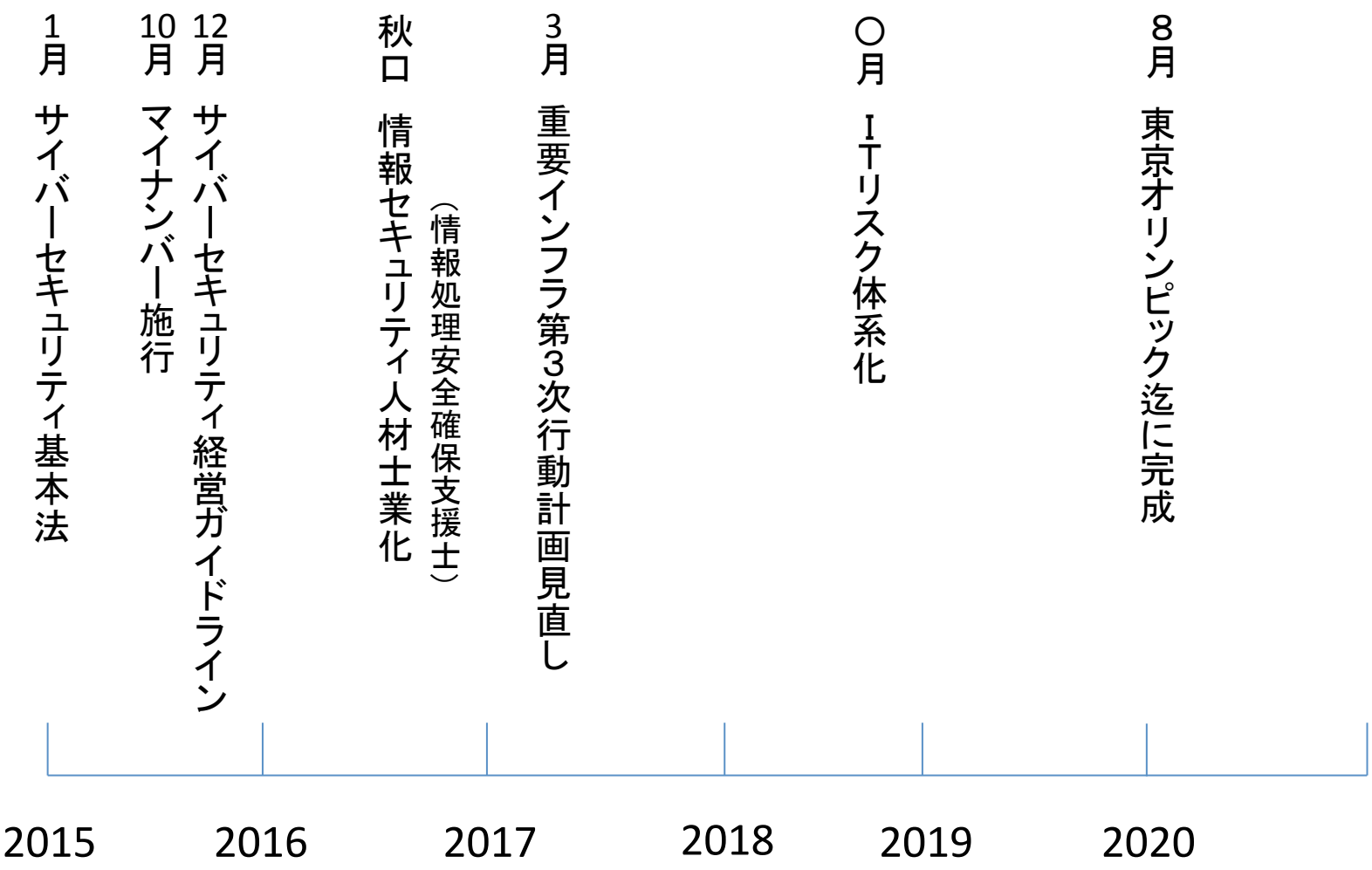
年金機構（特殊法人）の事件の経験から、NISCの監視対象が、特殊法人・認可法人にも広がる。

特殊法人：NTT、JR、NHK、日本郵政等
認可法人：日本商工会議所、全国商工会連合会、日本税理士会連合会、全国社会保険労務士会連合会等

◎監視業務の一部外部委託も可能となった

ガイドライン成立の背景（国のロードマップ）

日本を目指す
サイバーテロにも安心な
東京オリンピックまでに



重要インフラ13分野　第三次行動計画の見直し

○「重要インフラの情報セキュリティ対策に係る第3次行動計画」

IT障害が起きると、国民に多大な影響を与えるインフラに対し、情報セキュリティ対策を示したもの。

☆28年度末までに、**サプライチェーン等も含めた**リスク対策を実施するよう、見直しが為される予定。

兵庫県警HP「サイバーテロ対策」より

ガイドライン定着後の想定

○免責の基準

・「知らなかった」が通らない。既に、
セキュリティ対策を怠っていたことによる賠償判例（大阪地判平成18年5月19日等）
クラウド責任の線引きを怠っていたことによる賠償判例（東京地判平成25年3月19日等）
等、いくらでも存在する。

○取引条件

・委託先やパートナーの管理責任も問われるので、対策が取れていない企業と提携できなくなる。

○保険料率

・セキュリティ対策が取れていることにより、保険料の減額
（既にISMS取得等で対応済）

経営者が認識する必要のある三原則

- 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
  - 「知らない」「担当者に任せた」は通用しない
- 系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の委託先を含めたセキュリティ対策を実施すること
  - 「委託先の責任」「下請けのやったこと」「プロなのに裏切られた思い」は通用しない
- 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、対応に係る情報開示等、関係者との適切なコミュニケーションを行うこと
  - 根拠を説明できない「大丈夫」は通用しない

重要10項目
(リーダーシップの表明と体制の構築)

- サイバーセキュリティリスクの認識、組織全体での対応の作成

- サイバーセキュリティリスク管理体制の構築

重要10項目
(サイバーセキュリティリスク管理の枠組み決定)

- サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定

- 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

- 系列企業や、サプライチェーンのビジネスパートナー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

重要10項目
(リスクを踏まえた攻撃を防ぐための事前対策)

- 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
- ITシステム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保
- 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化活用のための環境整備

重要10項目
(サイバー攻撃を受けた場合に備えた準備)

- 緊急時の対応体制(緊急連絡先や初動対応、CSIRT)の整備、定期的かつ実践的な演習の実施

- 被害発覚後の通知先や開示が必要な書類の把握、経営者による説明のための準備

サイバーセキュリティ経営チェックシート（付録A）

○重要10項目をどこまで実施しているかのチェックシート

☆基本的な項目なので、状況に応じ、追加が必要。

今、「自社がどこまでできているか」のチェックに使う位置づけが良い

それでも・・・

- ・守るべき資産の特定
- ・CSIRTの設置
- ・IPAやJPCERTへの情報提供

等、多くの企業で実施して“いないであろう”項目を多く含んでいる

最大の課題

やはり、各階層における人材の絶対的不足が問題

・CISO、高度専門人材、橋渡し人材　⇒　多くの企業で社内に抱え込むことは実質不可能。

そもそものIT人材不足、それに加え、社内にIT人材を置く認識の薄さ

IT企業以外に属するIT人材　⇒　EU　52.4%　　日本　24.7%

（IPA 「IT人材白書2016」より）

どう対応するのか？

・外国人の活用

2020年までに、外国人IT人材を3万人から6万人に倍増。

（平成28年5月4日　対日投資セミナー安倍首相スピーチ）

➡ 実効性は？

・学校教育

小学校からプログラムを教える。

（サイバーセキュリティ2015　初等中等教育段階における教育の充実）

経営層が、人材確保と社内教育を指導することが不可欠

経営層の意識改革

早い段階での経営層の意識改革が成否を分ける

世間が動いてから対応しても、情報セキュリティ人材の枯渇は目に見えている。

第一、「情報セキュリティ人材の評価」は誰がするのか？
士業資格があっても、最近のテクニカルな情報を理解しているのか？

既に情報処理安全確保支援士は「数合わせ」の気配
2008年に廃止された資格試験の合格者も初回登録対象へ
（情報セキュリティアドミニストレータ、テクニカルエンジニア（情報セキュリティ））

信頼できる情報セキュリティ人材の確保が急務

➡ ここを間違うと、厚生労働省マイナンバー汚職のような事態が発生することになる。

サイバーセキュリティ経営ガイドライン解説セミナー

2. サイバーセキュリティ経営ガイドラインとISO27001

株式会社ISO審査登録機構

ISO27001（ISMS）の果たす役割

- そもそもISO27001を参考に作られている（付録C）

- ISMS取得促進が委員会で議論されている。

（第2回サイバーセキュリティリスクと企業経営に関する研究会要旨）

※第1回研究会でも、第三者評価の活用の重要性発言あり

サイバーセキュリティ経営ガイドライン　付録C

付録C　国際規格 ISO/IEC27001 及び 27002 との関係

	ISO/IEC 27001(●)、ISO/IEC 27002(・)
(1)サイバーセキュリティリスクの認識、組織全体での対応の策定	●5.1 リーダーシップ及びコミットメント ●5.2 方針
(2) サイバーセキュリティリスク管理体制の構築	●5.3 組織の役割、責任及び権限 ・6.1.1 情報セキュリティの役割及び責任
(3) サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定	●6.1 リスク及び機会に対処する活動 ●6.2 情報セキュリティ目的及びそれを達成するための計画策定 ・5.1.1 情報セキュリティのための方針群 ・5.1.2 情報セキュリティのための方針群のレビュー
(4) 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	●7.4 コミュニケーション ●8.1 運用の計画及び管理 ●8.2 情報セキュリティリスクアセスメント ●8.3 情報セキュリティリスク対応 ●9.1 監視、測定、分析及び評価 ●9.2 内部監査 ●9.3 マネジメントレビュー ●10.1 不適合及び是正処置 ●10.2 継続的改善 ・17.1.1 情報セキュリティ継続の計画 ・17.1.2 情報セキュリティ継続の実施 ・17.1.3 情報セキュリティ継続の検証、レビュー及び評価 ・18.1.1 適用法令及び契約上の要求事項の特定 ・18.2.1 情報セキュリティの独立したレビュー ・18.2.2 情報セキュリティのための方針群及び標準の順守 ・18.2.3 技術的順守のレビュー
(5) 系列企業や、サプライチェーンのビジネスパートナー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	●8.1 運用の計画及び管理
(6) 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	●7.1 資源 ●7.2 力量
(7) ITシステム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保	●8.1 運用の計画及び管理 ・15.1.1 供給者関係のための情報セキュリティの方針 ・15.1.2 供給者との合意におけるセキュリティの取扱い ・15.1.3 ICTサプライチェーン ・15.2.1 供給者のサービス提供の管理及びレビュー ・15.2.2 供給者のサービス提供の変更に対する管理
(8) 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のための環境整備	・6.1.3 関係当局との連絡 ・6.1.4 専門組織との連絡
(9) 緊急時の対応体制(緊急連絡先や初動対応マニュアル、CSIRT)の整備、定期的かつ実践的な演習の実施	・16.1.1 責任及び手順 ・16.1.2 情報セキュリティ事象の報告 ・16.1.3 情報セキュリティ弱点の報告 ・16.1.4 情報セキュリティ事象の評価及び決定 ・16.1.5 情報セキュリティインシデントの対応
(10) 被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備	・6.1.3 関係当局との連絡 ・6.1.4 専門組織との連絡

対策の進め方例　1

1. 方針の策定

自社が求められている周囲からのサイバーセキュリティに対する期待
（委託元の依頼、親会社の期待、世間の目等）を分析し、方針を定める。

2. 組織体制の構築

CISOの任命、システム対応の明確化等、組織体制の責任と権限を明確にする。

対策の進め方例　2

3. サイバーセキュリティリスクの特定と対策

（1）機密性・完全性・可用性を喪失したらどうなるか、の観点から、
「守るべき情報資産」を特定する。

- 機密性の喪失例・・・・・情報漏洩
- 完全性の喪失例・・・・・webサイト改ざん
- 可用性の喪失例・・・・・ランサムウェア

（2）「守るべき情報資産」に起こり得るリスクを特定し、対策を講じる。

例：社員による持ち出しを防止するため、データコピーを不可能にする、等

対策の進め方例　3

4. PDCAシステムの構築

（1）内部監査・マネジメントレビューの計画整備

（2）事故発生時の対応計画整備

5. 関係各所の状況把握

系列会社・パートナー等、自社が「守るべき情報資産」に影響を及ぼす可能性を持つ社外関係者を特定し、状況の把握と連携に努める。

6. 予算・人員等の確保

サイバーセキュリティ対策に必要な資源（予算・スキル等）を確認し、確保のための計画を検討する。

対策の進め方例　4

7. 委託先の特定とセキュリティ確保

ITシステム運用について、自社と委託先の切り分けを明確にし、委託先が攻撃を受けた場合にも自社がセキュリティを確保できることを確認する。

8. 情報の収集

常に最新のセキュリティホール・対策情報を把握するため、関係省庁との連絡体制、専門組織との連絡体制を構築する。

9. 緊急時の対応

※4－(2)　事故発生時の対応計画整備に関連

10. 被害発覚後の体制

※4－(2)　事故発生時の対応計画整備および8. 情報の収集に関連

サイバーセキュリティ経営ガイドライン解説セミナー

３．弊機関ISO27001審査の特色

株式会社ISO審査登録機構

国内のISO27001の問題点

1. 経営者の課題：**経営者が情報セキュリティ、ISMS推進などへの関心がない、または低い。**このため、推進事務局の努力が報われていない。経営者がISMSに関心を示さないケースは、営業上の目的などで形式的にISMSを取得する事業所等がある。

2. ISMSへの誤解：**管理策への誤解**が多い。管理策で必要ないものは適用除外したり、または追加の管理策で更に高度なセキュリティレベルを構築してもよいことを理解していない。ISMS導入前に**レベルの低いコンサルタントの利用**や**認証取得を優先**したのではないかと思われる面もある

3. コンサルタントの問題：認証取得のためにISMSへの支援を求めた**コンサルタントがISMSを理解**していないため、審査時に指摘事項の山となることもある

4. 審査機関･審査員の課題：**審査機関にも問題**がある可能性もあるが、**審査員がISMSの基本を理解していない**ために起こっている

情報セキュリティ大学院大学名誉教授　内田勝也先生
於：情報マネジメントシステム認証機関協議会2009　ISMSセミナー
（抜粋　赤字は当社）

いまだ状況は変わっていない？

原文に即した要求事項解釈

- 「ISO」の言語は英語・フランス語・ロシア語のみ

日本語版の「JIS　Q　27001」は誤訳と言わないまでも、誤解を受けそうなニュアンスが多い。

May be needed　⇒　～してもよい

Be　communicated　⇒　伝達する　　等

本来、規格が要求しているものと微妙に差があるため、誤解が生じている。

例）適用宣言書は、本来どんどん追加の管理策が加わるべき、
相手に伝わったことを確認するまでが、伝達者の役割、等

適用宣言書の確実な審査

○適用宣言書の内容確認はISO27001の有効性審査に必須！

ISO27001は他のISOマネジメントシステム規格と違い、
同じことをしていたら、確実に水準を維持できない。

外部要因でセキュリティ水準の維持を脅かす事象が次々発生している。
その対応や検討無しに、ISO27001の有効な活用などあり得ない。

➡ 100を超える事業所で審査員が適用宣言書を見ていない

内田勝也先生 「第4回ISMS調査の概要」より　http://www.uchidak.com/isms/

正しい情報セキュリティマネジメントシステム審査を定着させたい

JAB認定のISO27001

認定機関としてJABを選択した理由

1. 国際的に通用する審査を証明するため

ISO27001の国内認定機関は、未だ国際相互認証を受けておりません。JABなら他規格での実績があるため、国際相互認証を受けることが容易です。

2. プライバシーマークとの利害抵触を避けるため

プライバシーマークの審査指摘と齟齬がある場合でも、当方の指摘が正しいと堂々と主張できます。

※プライバシーマークの審査組織がISO27001の審査機関認定を行っていると、プライバシーマークの過誤指摘に躊躇する可能性が残ります。

ISO審査登録機構は“本来あるべき審査”を追及します。

ISOマネジメントシステムの
審査・社員教育のご用命は・・・

株式会社ISO審査登録機構

東京都渋谷区代々木1-32-11　Kビル5F
TEL:03-5333-7543　FAX:03-5333-7655