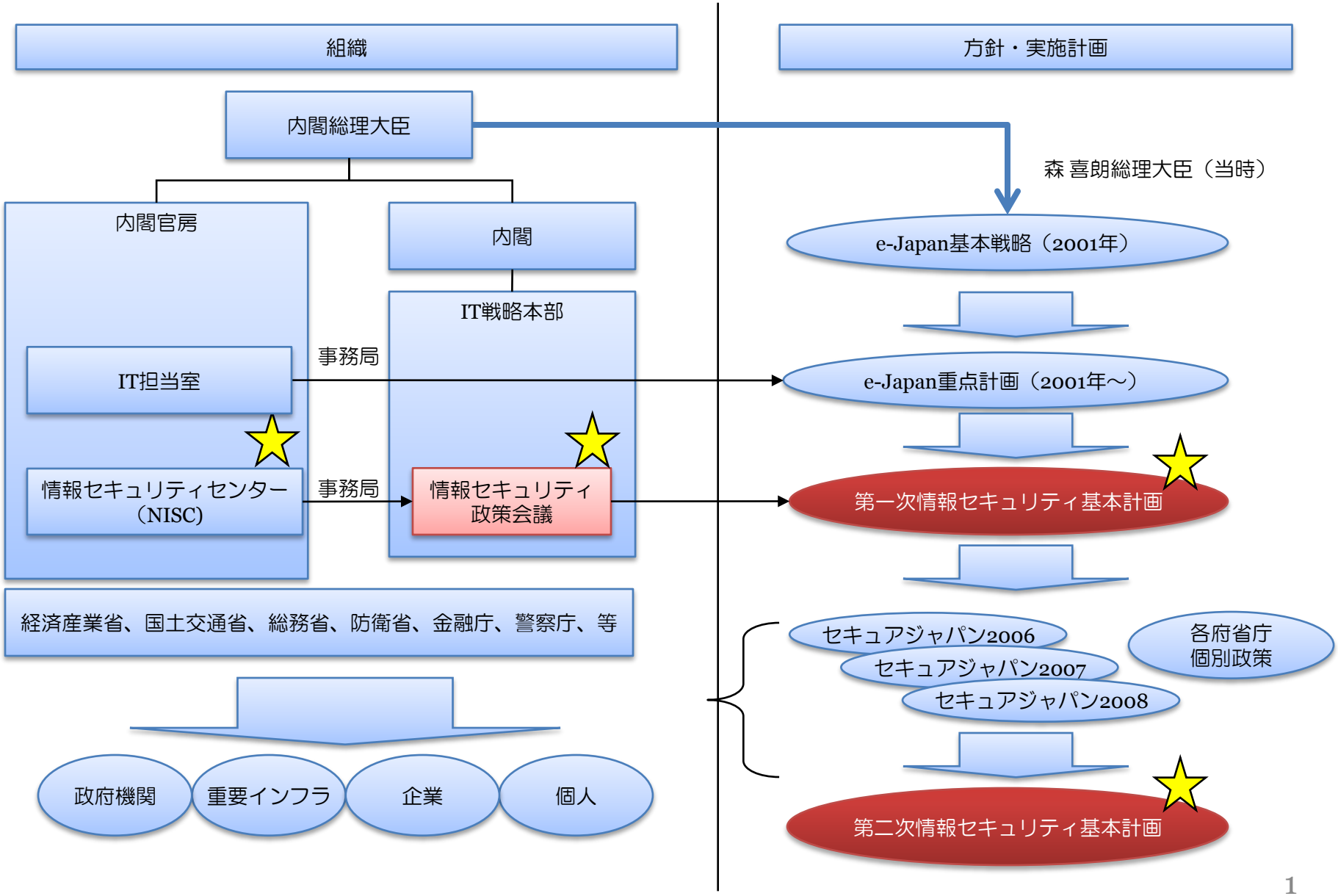
経済産業省
Ministry of Economy, Trade and Industry

情報セキュリティ政策について

経済産業省 商務情報政策局
情報セキュリティ政策室
課長補佐 清水 友晴

情報セキュリティ政策の概略



情報セキュリティ基本戦略（政府方針）

高度情報通信ネットワーク社会推進戦略本部（ＩＴ戦略本部）設置の情報セキュリティ政策会議で決定された情報セキュリティ基本戦略にもとづき、各府省庁は所管領域の情報セキュリティ政策を立案、実施する

政府として情報セキュリティ対策を行うことの根拠法と考えられる

経緯

年次	事象	概要
2000年	高度情報通信ネットワーク社会形成基本法	IT基本法、第二十二条（高度情報通信ネットワークの安全性の確保等）高度情報通信ネットワーク社会の形成に関する施策の策定に当たっては、高度情報通信ネットワークの安全性及び信頼性の確保、個人情報の保護その他国民が高度情報通信ネットワークを安心して利用することができるようにするために必要な措置が講じられなければならない。
2001年	IT本部情報セキュリティ専門調査会設置	官民における情報セキュリティ対策の推進に係る事項の調査のため、情報セキュリティ専門調査会を設置。2004年までに6回開催。
2005年	IT本部情報セキュリティ政策会議設置	「わが国の情報セキュリティに関する問題の根幹に関する事項を決定する母体」となる。二ヶ月に一度、現在（平成２１年６月２２日）までに２２回開催
	内閣官房情報セキュリティセンター設置	情報セキュリティ政策会議で決定された基本戦略の遂行機関として設置される。情報セキュリティ政策に関する中長期計画や年度計画の立案、政府機関・重要インフラの情報セキュリティ対策、情報セキュリティ政策に関する国際連携の窓口機能等を受け持つ。
2006年	第１次情報セキュリティ基本計画	2006年から2008年における情報セキュリティ政策の基本方針を定義。
2006年	セキュア・ジャパン2006	情報セキュリティ基本戦略にもとづき、各府省庁で実施する施策を年次ごとにまとめたもの。
2007年	セキュア・ジャパン2007	
2008年	セキュア・ジャパン2008	
2009年	第２次情報セキュリティ基本計画	2009年から2011年における情報セキュリティ政策の基本方針を定義。

第１次情報セキュリティ基本計画

経済産業省
Ministry of Economy, Trade and Industry

「第1次情報セキュリティ基本計画」（２００６年2月2日　情報セキュリティ政策会議）

2006～2008年度の3ヵ年計画。全主体が適切な役割分担を果たす「新しい官民連携モデル」の構築を目指す。

	政府機関・地方公共団体	重要インフラ	企　業	個　人
目標	２００９年度初めには すべての政府機関が 「政府機関統一基準」が 求める水準に	２００９年度初めには ＩＴ障害を限りなくゼロに	２００９年度初めには 対策の実施状況を 世界トップクラスの水準 に	２００９年度初めには 「IT利用に不安を感じる」 個人を限りなくゼロに
各重要政策領域の実施	◆ 政府機関統一基準に基づく各省庁の評価 ◆ サイバー攻撃等への緊急対応能力の強化	◆ 情報共有・分析機能の整備 ◆ 連絡協議会の設置 ◆ 分野横断的な演習、相互依存性解析の実施	◆ 政府調達における入札条件の整備 ◆ 第三者評価制度の活用 ◆ ウィルス等への体制強化	◆ セキュリティ教育の推進 ◆ 広報啓発の強化 ◆ ユーザーフレンドリーなサービスの提供等

横断的な重要政策

- 情報セキュリティ技術戦略の推進
- 情報セキュリティ人材の育成確保
- 国際連携・協調の推進
- 犯罪の取締り、権利利益の保護救済

2005年度 → 2006年度 → 2007年度 → 2008年度 → 2009年度

「セキュア・ジャパン２００６」

① ２００６年度の実施計画　（１３３施策）
～「官民におけるセキュリティ対策の体制の構築」

② ２００７年度の重点施策の方向性　（２６施策）
～「官民におけるセキュリティ対策の底上げ」

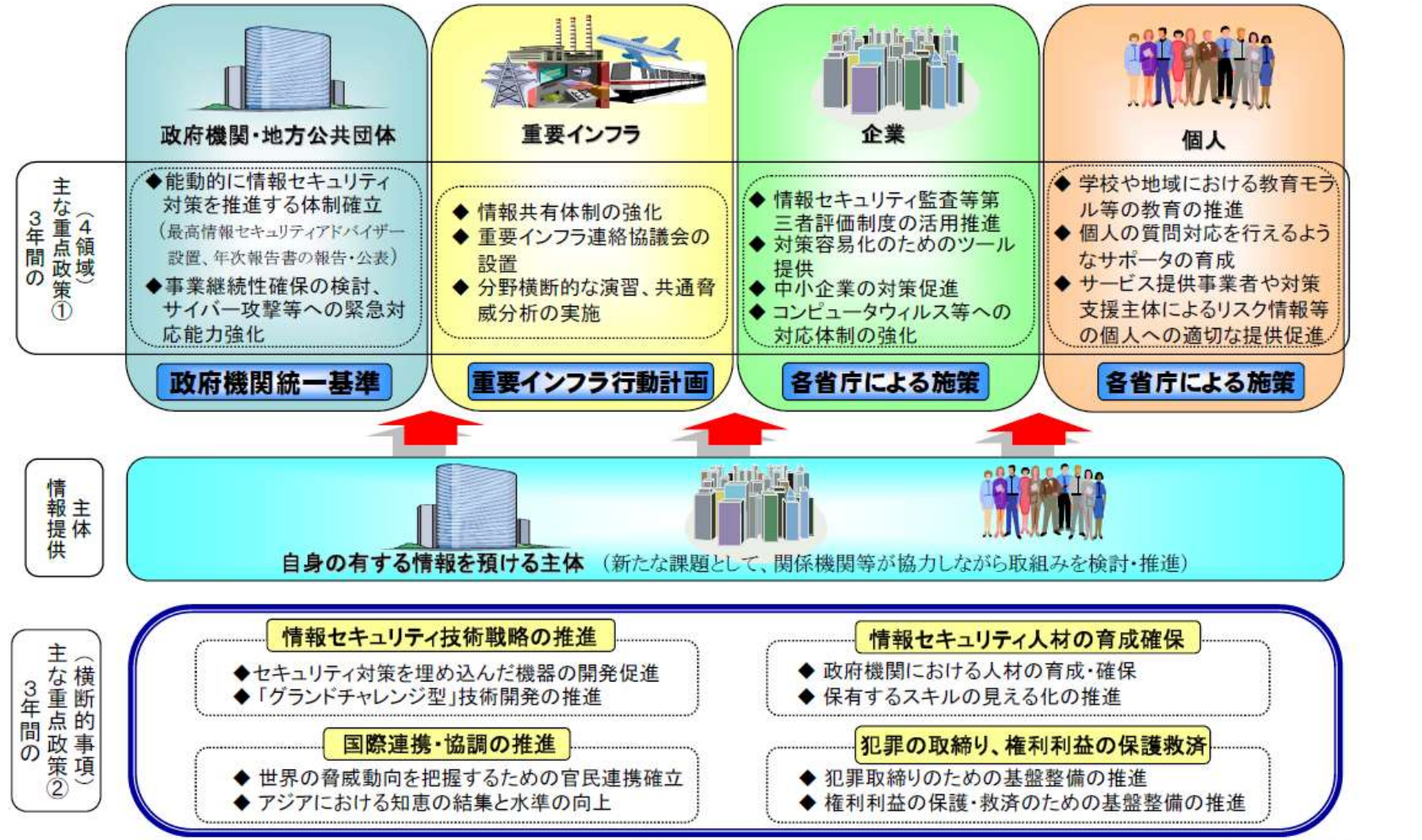
セキュア・ジャパン２００７

セキュア・ジャパン２００８

第２次情報セキュリティ基本計画

経済産業省
Ministry of Economy, Trade and Industry

「第２次情報セキュリティ基本計画」（２００９年２月３日　情報セキュリティ政策会議）



※その他、対策支援主体（「情報セキュリティ対策を実施する主体」の取組みを支援する主体）の取組みも促進する。

具体的施策（抜粋）

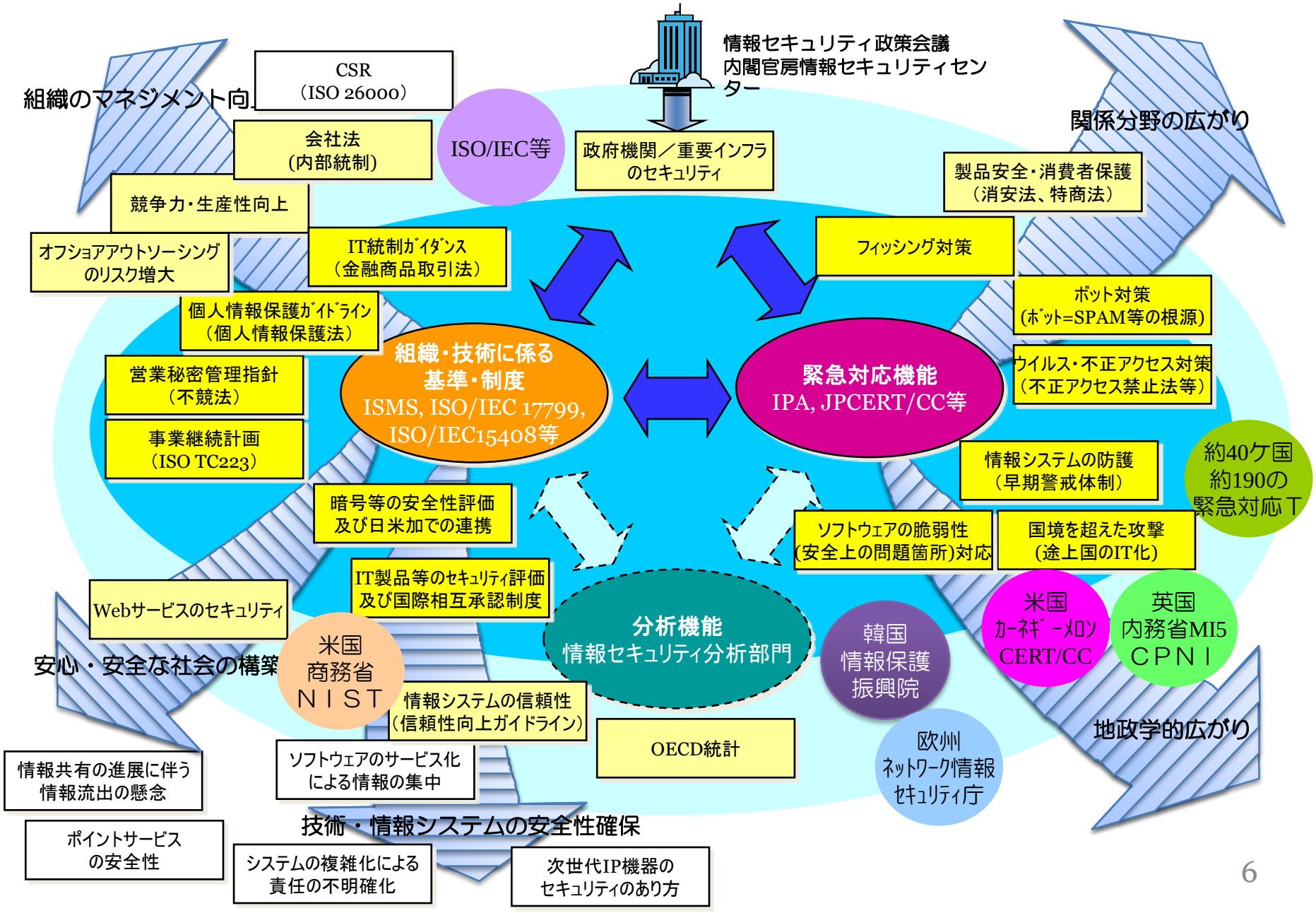
経済産業省
Ministry of Economy, Trade and Industry

政府における
情報セキュリティ
マネジメント

- 政府機関・公共団体
  - 政府機関統一基準の策定と評価・勧告によるPDCAサイクルの構築
    - 各省庁及び関連機関のセキュリティレベルを改善しつづける取組
  - サイバー攻撃等に対する政府機関における緊急対応能力の強化
    - GSOC（Government Security Operation team：政府横断的な情報収集解析部門）
  - 地方公共団体における情報セキュリティ確保に係るガイドラインの見直し
- 重要インフラ
  - 重要インフラにおける情報セキュリティ確保に係る「安全基準等」の整備
  - 情報共有体制の強化
    - CEPTOAR-Council（重要インフラ連絡協議会、仮称）
  - 分野横断的な演習の実施
- 企業
  - 企業の情報セキュリティ対策が市場評価につながる環境の整備
    - 情報セキュリティガバナンス確立の促進
  - 質の高い情報セキュリティ関連製品及びサービスの提供促進
    - 情報セキュリティマネジメントシステム適合性評価制度の普及促進（ISMS）
    - 情報セキュリティ監査制度の普及促進
  - コンピュータウイルスや脆弱性などに早期に対応するための体制の強化
- 個人
  - 情報セキュリティ教育の強化・推進
    - インターネット安全教室、e-ネットキャラバン
  - 広報啓発・情報発信の強化・推進
    - CheckPC！、情報セキュリティの日、NISCメールマガジン

企業における
情報セキュリティ
マネジメント関連

経済産業省の情報セキュリティ対策と裾野の広がり



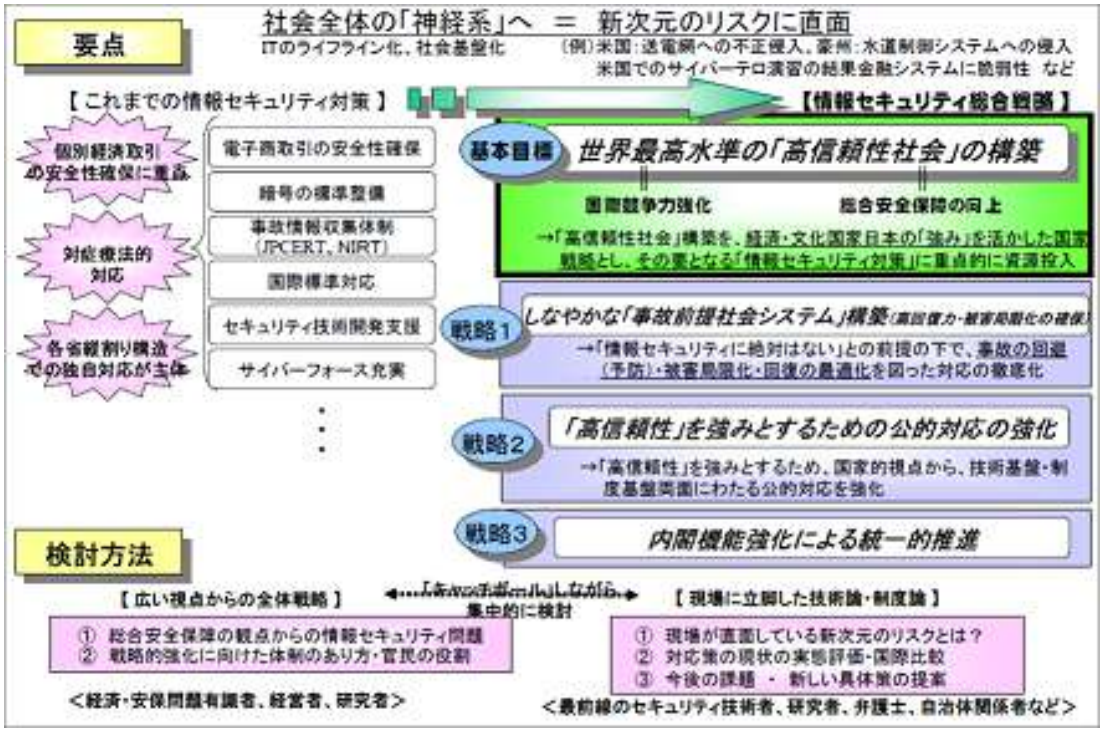
経済産業省「情報セキュリティ総合戦略」

経済産業省
Ministry of Economy, Trade and Industry

- 2003年制定
- 「我が国で初めて策定された総合的な情報セキュリティに関する戦略」
- 「戦略」の基本目標を、経済・文化国家日本の強みを活かした「世界最高水準の「高信頼性社会」の構築」と位置付け
- その要となる「情報セキュリティ対策」について、３つの戦略と４２の施策項目を提言。

セキュリティマネジメントによる事前予防策

- 情報セキュリティ監査の実施やISMS 認証取得の促進
- 情報セキュリティ格付けのあり方の検討



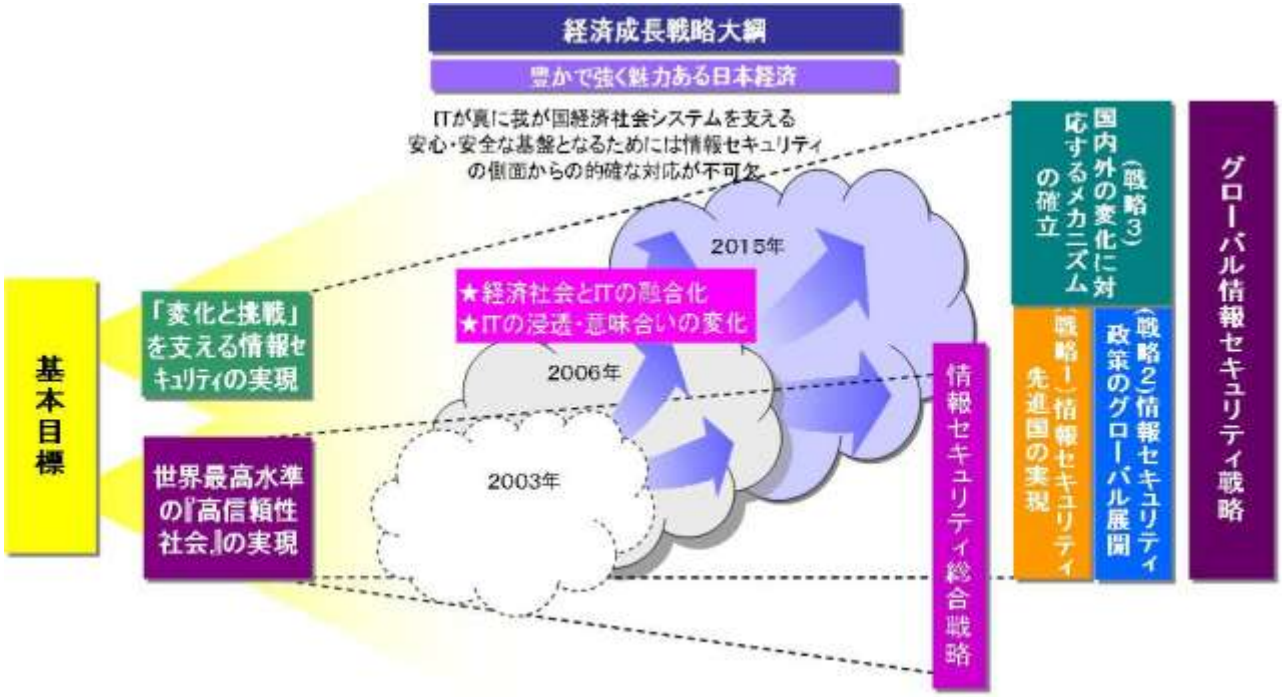
経済産業省「グローバル情報セキュリティ戦略」

経済産業省
Ministry of Economy, Trade and Industry

- 2007年制定
- ITが国内外の経済社会システムに融合化し、情報セキュリティに関する脅威も国際化傾向にある中、産業構造審議会情報セキュリティ基本問題委員会にて、次の３つの戦略からなる「グローバル情報セキュリティ戦略」を取りまとめた。
  - 戦略１ 我が国を真に「情報セキュリティ先進国」とするための取組み
  - 戦略２ 国際化する脅威に対応し、我が国の国際競争力を強化していく観点からの情報セキュリティ政策のグローバル展開
  - 戦略３ 国内外の変化に対応するためのメカニズムの確立

セキュリティマネジメントによる事前予防策

- 情報セキュリティ対策状況に係る情報開示を通じた民間格付けの促進等
- 企業等の情報セキュリティ対策に係るベストプラクティス事例集等の提供
- 情報セキュリティ対策実施状況確認のための標準フォーマットの策定
- 企業や製品・サービス等に係る情報セキュリティ関連評価制度の拡充・強化
- オフショア・アウトソーシングに係る情報セキュリティリスク等の検討
- 保証型情報セキュリティ監査の普及



企業に対する情報セキュリティ政策の背景

経済産業省
Ministry of Economy, Trade and Industry

我が国産業の競争力強化

- ＩＴを基盤とした情報の利活用は競争力の源泉

↓

競争力強化を阻害する情報セキュリティに係る要因

しかし、**企業の情報資産に対する脅威は増大の一途**　⇒　事件・事故が多数発生

↓

情報セキュリティ基本計画に位置づけ

- 第二次情報セキュリティ基本計画にて「情報セキュリティガバナンス」を位置づけ［２００９年２月　情報セキュリティ政策会議（議長：内閣官房長官）で決定］

※　**情報セキュリティガバナンス**：情報セキュリティの観点からガバナンスの仕組みを構築・運用

【発生している事件・事故の具体例（2006年～）】
- 元A証券社員が全個人口座148万6651件の情報を無断で持ち出し一部を売却
- 金融機関多数において伝票、名簿等の顧客情報を誤廃棄・紛失　（都市銀行、地方銀行 等）
- ファイル共有ソフト（Winny 等）による情報漏えい事件の多発　（ITベンダ、通信事業者、学校法人 等）

【コンプライアンス問題の例】
- インサイダー（情報漏えい）　（印刷業者、放送事業者 等）

【膨大な被害額】
- 国内個人情報漏えい事件の想定損害賠償総額：２兆円超（2007年）　[日本ネットワークセキュリティ協会調べ]
- 不正アクセスによる被害規模（事例）：数億円～数十億円／一件あたり（2006年）[（独）情報処理推進機構調べ]

【第二次情報セキュリティ基本計画】（計画期間　2009年度～2011年度）

- **企業における情報セキュリティ対策の推進は、政府、重要インフラ、個人における対策とともに４本柱の一つ。**
- 「**政府**は**企業における情報セキュリティ対策**の実施状況を**世界トップクラスの水準**にすることを目指して最大限の努力を行う」
- 企業に係る**第一の情報セキュリティ政策**として「**情報セキュリティガバナンスの経営の一環としての認識の定着とそれに応えられるツールの存在**」を**位置づけ**。

情報セキュリティ確保のための施策

経済産業省
Ministry of Economy, Trade and Industry

情報セキュリティの確保（＝情報セキュリティガバナンスの確立）を実施する上で、企業経営者の抱えている課題を解決するための施策を実施

これまでの経緯

企業の情報セキュリティに関する制度等

- 2001年 情報セキュリティマネジメントシステム（ISMS）適合性評価制度」開始 （（財）日本情報処理開発協会（JIPDEC））
- 2003年 情報セキュリティ監査制度開始（NPO日本セキュリティ監査協会（JASA））
- 2005年 情報セキュリティ対策ベンチマークのサービス開始（（独）日本情報処理推進機構（IPA））
- 2008年 民間の情報セキュリティ格付機関設立

制度・規定・ガイダンス等

- 2001年 ISMS国際標準規格 ISO/IEC 17799:2000 に対応したISMS認証基準策定（JIPDEC）
- 2003年 情報セキュリティ管理基準、監査基準（経済産業省告示）
- 2005年 情報セキュリティ報告書モデル、事業継続計画（BCP）策定ガイドライン（書籍化）
- 2006年 財務報告書に係るＩＴ統制ガイダンス　（J-SOX対応版）
- 2008年 情報セキュリティ管理基準、監査基準（改正）、ITサービス継続ガイドライン
- 2009年 中小企業の情報セキュリティガイドライン（IPA）

今回の取組

企業の情報セキュリティを確立する上で解決されていない課題

（１）経営層が情報セキュリティの観点から何をすべきか不明確
（２）ＩＳＭＳを実装しようとしても法令との関係が分からない
（３）業務委託先での情報漏えい対策等の実施方策が分かりにくい
（４）実施状況の「見える化」のため信頼できる民間格付け機関が必要

課題に対応して今回策定したガイダンス類

（１）情報セキュリティガバナンス導入ガイダンス
（２）情報セキュリティ関連法令の要求事項集
（３）アウトソーシング・セキュリティ対策ガイダンス
（４）情報セキュリティ格付機関の規律に関する基準

企業のセキュリティガバナンスに関する一連のガイダンス類の普及展開フェーズへ

情報セキュリティガバナンス関連ガイドライン等の体系

経済産業省
Ministry of Economy, Trade and Industry

目的／担当	機密性の確保（情報漏洩対策等）	完全性の確保（情報改ざん対策等）	可用性の確保（IT障害への対策等）
経営者	**情報セキュリティガバナンス導入ガイダンス（＊１）** 情報セキュリティの観点からガバナンスの仕組みを構築・運用		
	情報セキュリティ報告書モデル（2005年）		
管理者	情報セキュリティマネジメントシステムの国際標準（ISMS）（2001年～） 自社の情報セキュリティ対策の適正な改善メカニズム（PDCAサイクル）の構築		
	情報セキュリティ関連法令の要求事項集（＊２） 情報セキュリティ対策に必要な法令を遵守するための情報提供		
			情報セキュリティ対策ベンチマーク（2005年）
	アウトソーシング・セキュリティ対策ガイダンス（＊３）	財務報告に係るIT統制ガイダンス（2006年）	事業継続計画（ＢＣＰ）策定ガイドライン（2005年）、ITサービス継続ガイドライン（2007年）
外部機関	情報セキュリティ監査（2003年）等		
	情報セキュリティ格付（情報セキュリティ格付機関の規律に関する基準（＊４））		

（1）経営層が情報セキュリティの観点から何をすべきか不明確

（2）ISMSを実装しようとしても法令との関係が分からない

（3）業務委託先での情報漏えい対策等の実施方策が分かりにくい

（4）企業の情報セキュリティ対策実施状況の「見える化」が不十分

（＊ 今回策定した文書、１～４企業経営者の抱える課題）

競争力強化に向けた情報セキュリティ確立の必要性

経済産業省
Ministry of Economy, Trade and Industry

① 情報資産の利活用と管理

ビジネス分野では、ＩＴを活用した自社内の「縦割り」を排除し、積極的な情報共有、情報の可視化による「全体最適」を目指した「マネジメント改革」が本格化しつつあるが、全体的に見ると、約７割が「部分最適」にとどまっている。全体最適のステージに進むためには情報資産の管理、すなわち情報セキュリティを確立する必要があるのではないか。

② 適法性と適正性

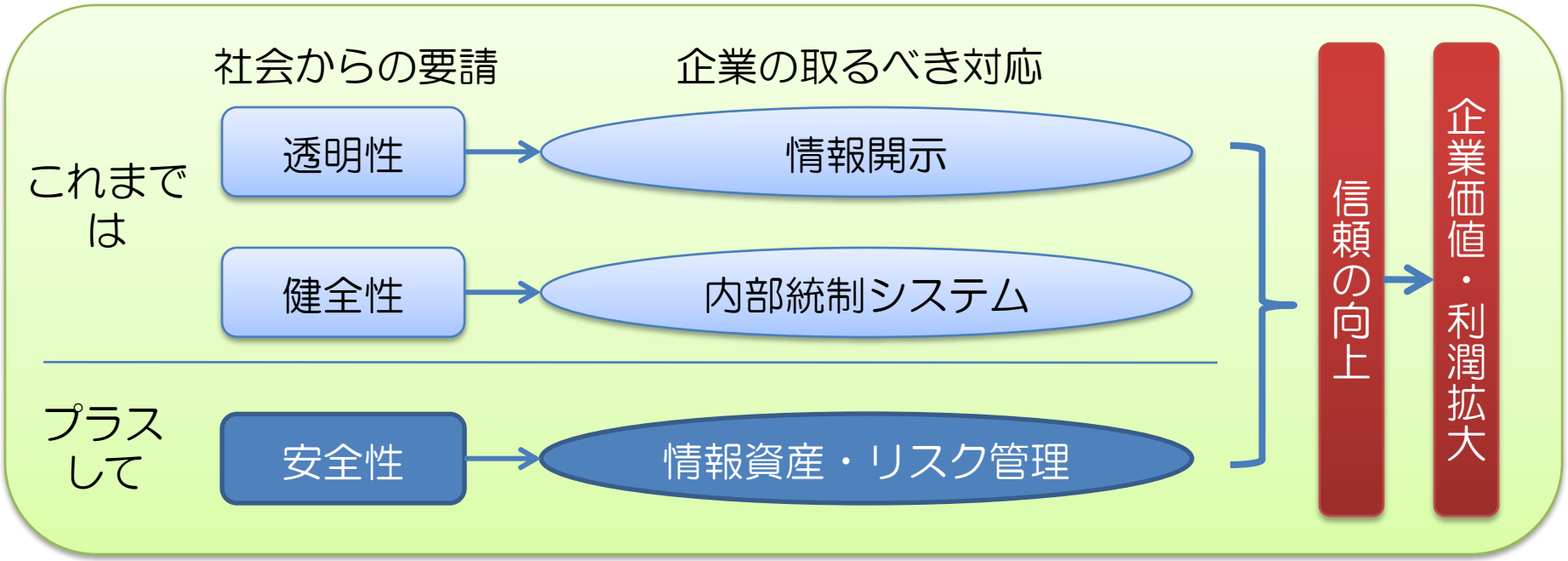
個人情報保護法、金融商品取引法、会社法等、法的要求に対応する適法性と、社会や顧客からの適正性の要求についてバランスをとらなければならないが、過剰な法令対応、あるいは過少対応が散見され、適正性が守られていないのではないか。

③ 企業の社会的責任

コーポレートガバナンス、社会的責任（CSR）の観点から顧客・社会に対して企業の透明性を提供することは常識化したといえる。同じように、情報セキュリティ向上に努めること、事業継続性を確保することも社会的責任の一つであり、企業は責任を以って取り組まなければならないのではないか。

一般的に企業利益に結び付かないと考えられている情報セキュリティへの取り組みを、企業戦略と整合性ととるかたちで見つめ直し、「攻めの情報セキュリティ投資」、すなわち、情報セキュリティ対策を企業価値を高めるための投資対象として位置づけるべきではないか

企業に必要なガバナンス活動



財務リスク、労務リスク、法令リスク、
情報セキュリティ上のリスク、
ITシステム上のリスク、等を
経営者が常時、把握できるように
企業のビジネスプロセス全体の
リスクマネジメント、
つまりERM体制を確立する必要がある

経営者による情報セキュリティ上のリスクマネジメント及び改善活動を
「情報セキュリティガバナンス」としてまとめたガイダンスを策定

情報セキュリティガバナンス導入ガイダンス

経済産業省
Ministry of Economy, Trade and Industry

本ガイダンスが必要となる背景

- 経営者は、情報資産の管理が経営戦略そのものであり、それを支えるリスク管理の一環としての情報セキュリティ対策こそ、**正面から対峙しなければならない経営課題**であることを認識する必要がある
- 情報資産に係る機密性、完全性、可用性の観点からのリスク管理として**情報セキュリティガバナンスの確立**に取り組むべきである。

ガイダンスの目的と内容

【情報セキュリティガバナンスの確立のためのモデルを提示 】

- 経営者が情報セキュリティに係る**全体方針を決定**し実施責任者として**CISO（＊）を任命**
- CISOは組織内の情報セキュリティの状況を**モニタリング・報告する仕組みを構築**
- **監査役は情報セキュリティガバナンス体制の機能状況を確認**、状況に応じて経営者に改善を促す
- 経営者は情報セキュリティの取組を利害関係者に開示、評価を受ける仕組みを構築（**報告書**）

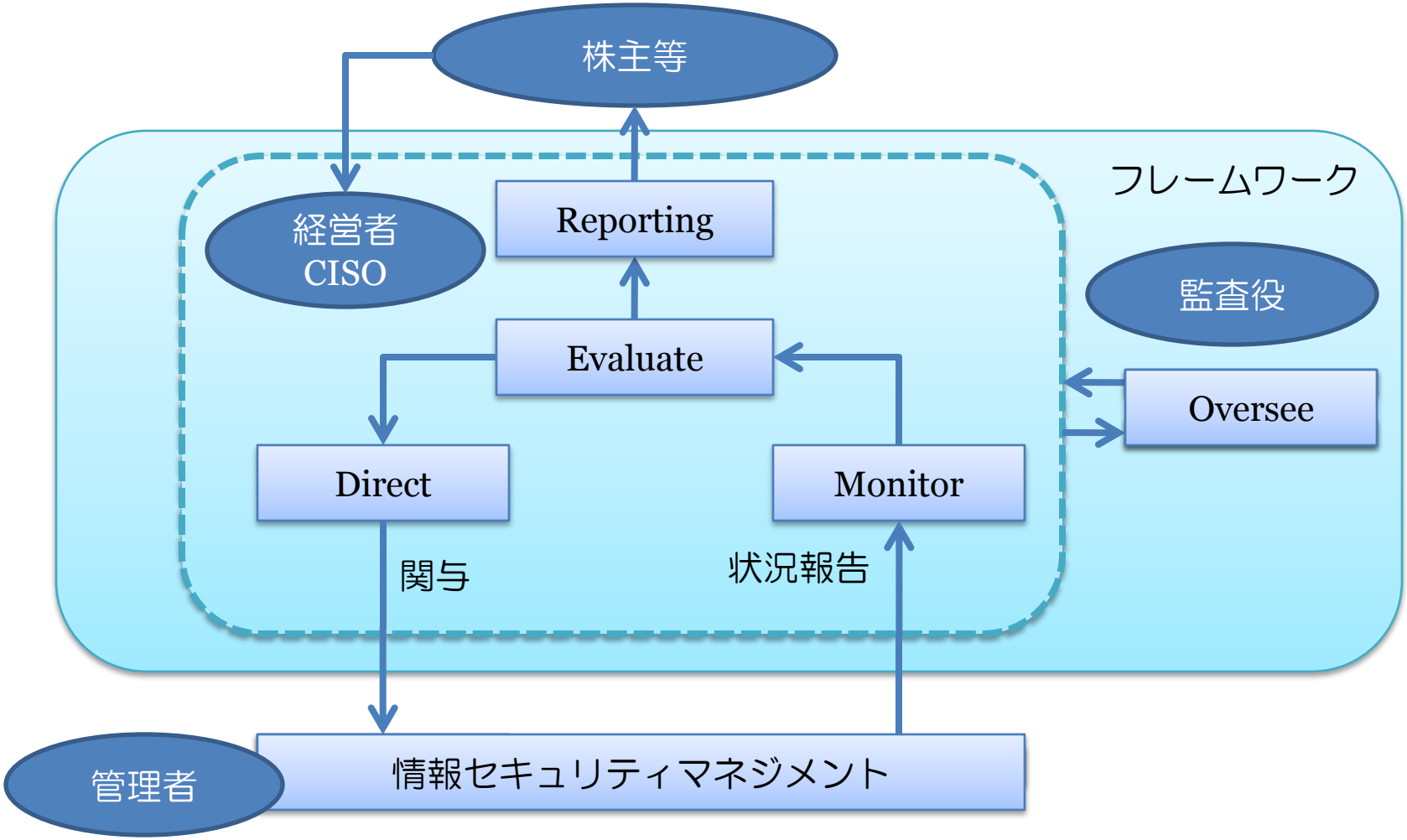
確立プロセス	監査役（監査役会）	経営者	CISO	管理者
情報セキュリティガバナンス体制の確立	情報セキュリティガバナンス体制が機能していることを確認 必要に応じて問題の改善を促す （指摘）	CISOを任命	各部門、事業者等に情報セキュリティ管理者を配置 （指名）	（配置される） （指名）
リスク管理方針、情報セキュリティに関する目標、対策の決定		リスク評価を行い、リスク管理方針を決定する	リスク管理方針に基づいて情報セキュリティ目標を定める （指示）	情報セキュリティ目標をブレークダウンした情報セキュリティ対策を決定する （指示）
モニタリング＆報告		（報告を受ける） （報告）	情報セキュリティ対策の実施状況、目標の達成状況をモニタリング 全体の状況を総括して経営陣に報告 （報告）	担当部門、事業所等の情報セキュリティ対策実施状況について把握 CISOに報告を行う

（＊CISO＝情報セキュリティ最高責任者）

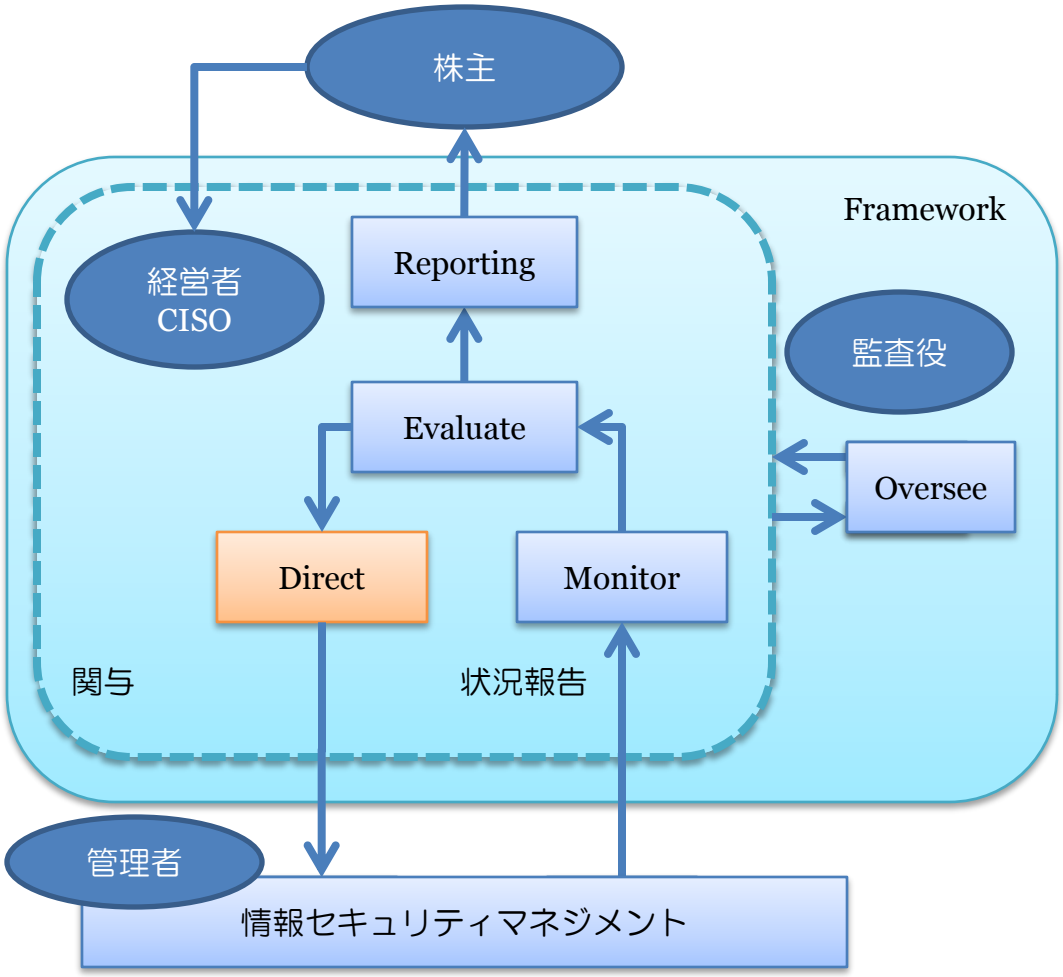
情報セキュリティガバナンスフレームワーク

経済産業省
Ministry of Economy, Trade and Industry

- 情報セキュリティガバナンス導入ガイダンスを原案とした国際標準規格 ISO/IEC 27014として策定プロセス進行中

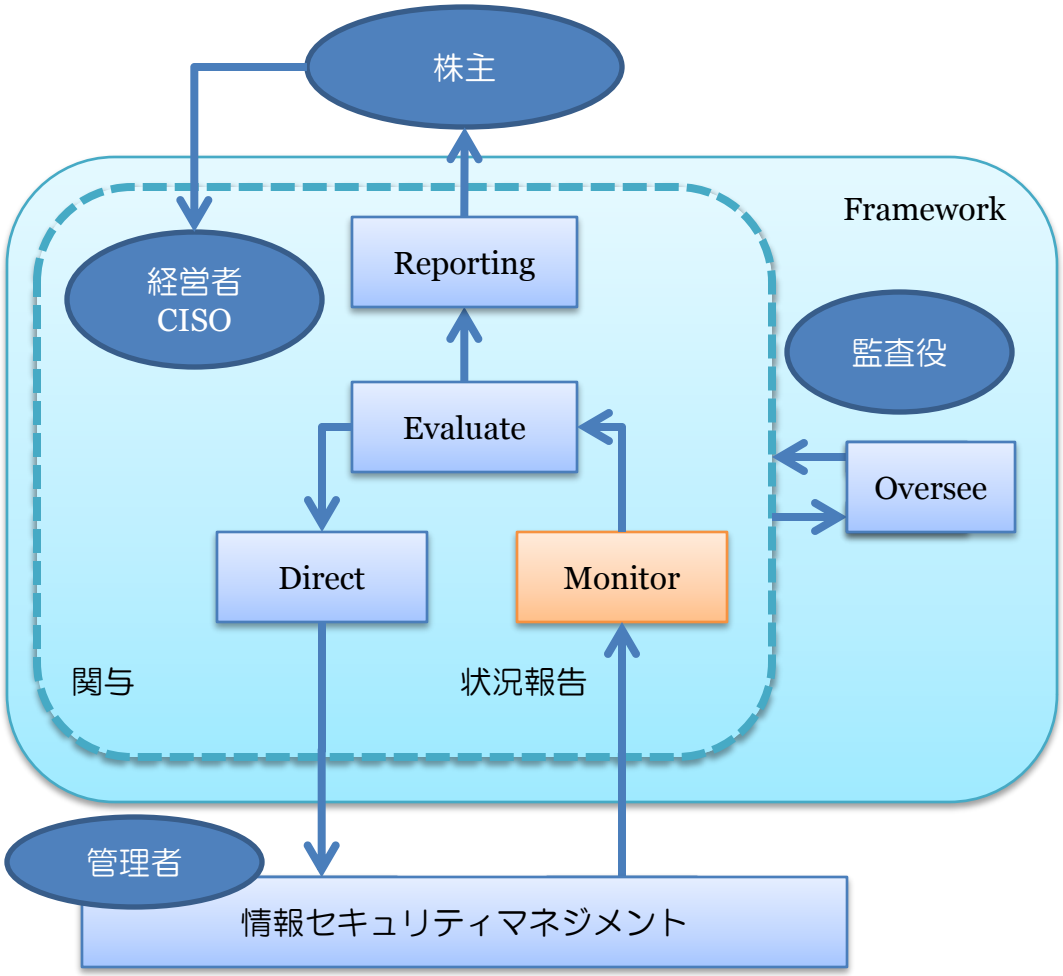


Direct



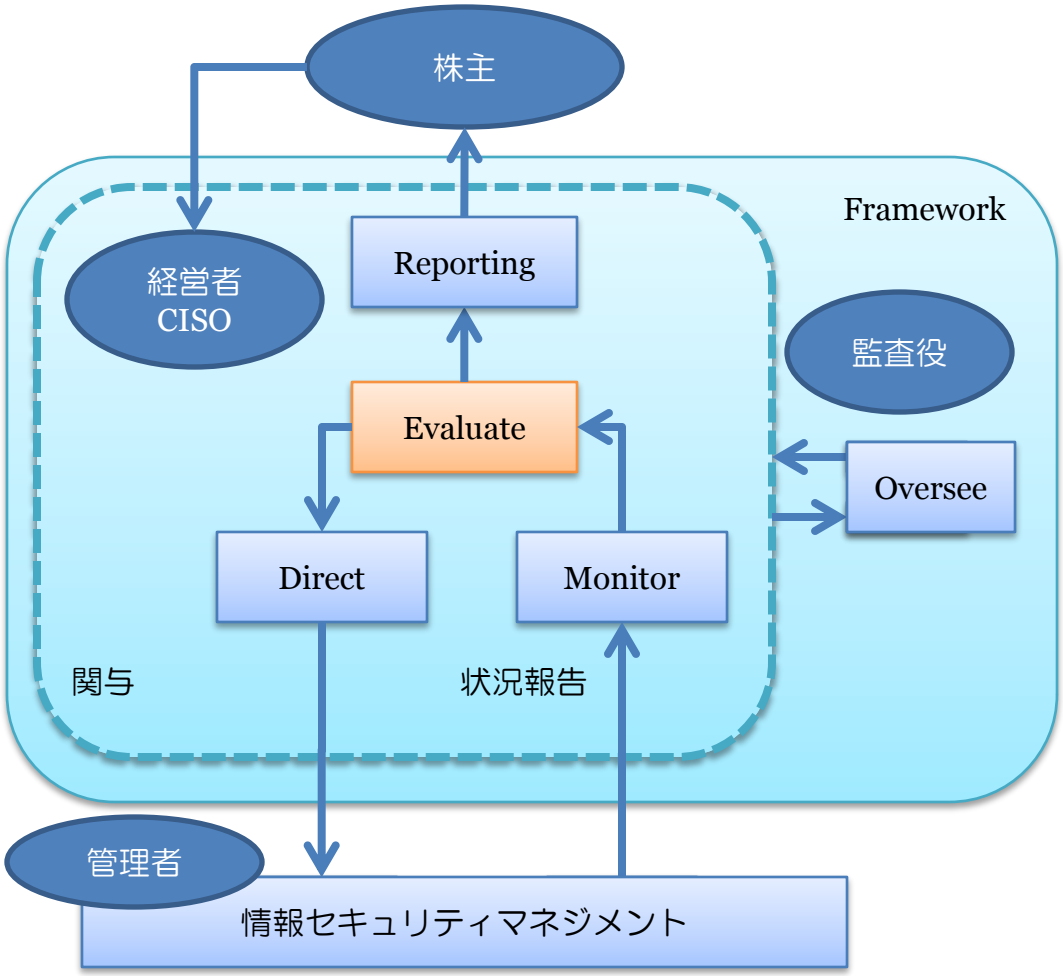
- Direct（方向付け）
  - 経営者はリスク管理方針に基づき情報セキュリティ目的と目標を決定する
  - 経営者は最高情報セキュリティ責任者（CISO）を任命する
  - CISOは各部署に情報セキュリティ管理者を配置する

Monitor



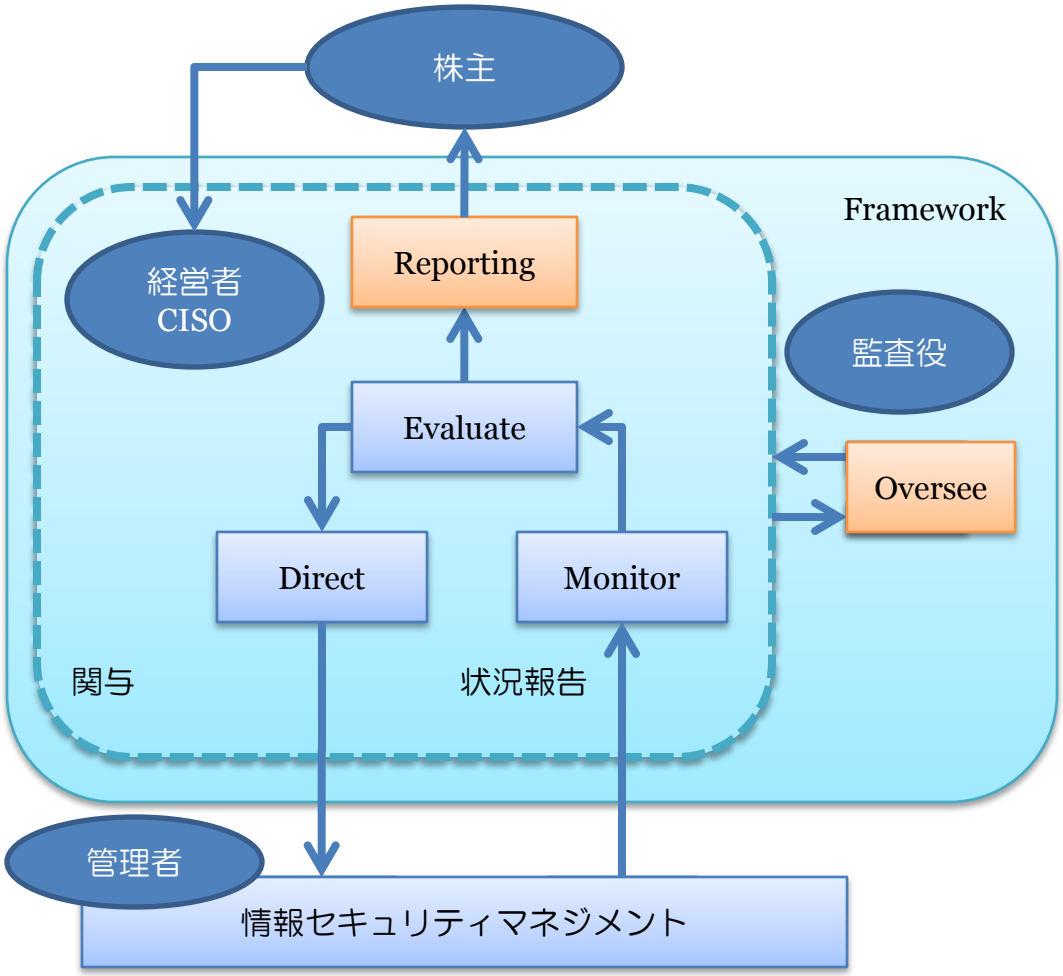
- Monitor（モニタリング）
  - モニタリングメカニズムの確立
    - 測定指標を定め、測定を可視化する

Evaluate



- Evaluate（評価）
  - 経営者は情報セキュリティ目標の達成状況を評価する
  - CISOは各部署のKPI（Key Performance Indicator）を評価する

Oversee & Reporting



- Oversee（監督）
  - 監査役又は監査委員会はガバナンスの改善プロセスを監督する
- Report（報告）
  - 情報セキュリティガバナンス活動の状況を株主等に開示する

御清聴ありがとうございました