情報システムセキュリティのこれまで
と
制御システムセキュリティのこれから

平成25年5月28日

慶應義塾大学名誉教授

土居範久

謝辞

資料を作成するにあたっては多くの方々の協力を得た.

とりわけ次の方々には貴重な資料をご提供頂いた:

・(一財) 日本情報経済社会推進協会情報マネジメント推進センター
・経済産業省 商務情報政策局 情報セキュリティ政策室
・(独)情報処理推進機構 セキュリティセンター
・NPO法人　日本セキュリティ監査協会
・(株)三菱総合研究所
・防衛庁 管理局 航空機通信電子課 (当時)
・(独)製品評価技術基盤機構

土居範久（どい　のりひさ）

慶應義塾大学名誉教授，　科学技術振興機構 社会技術センター 参与

日本学術会議 副会長
文部科学省 科学技術･学術審議会 情報科学技術委員会 委員長
文部科学省 次世代スーパーコンピュータ戦略委員会 主査
総務省 情報通信審議会会長代理･ 情報通信技術分科会 会長
総務省 電波利用料制度に関する専門調査会 座長
経済産業省 産業構造審議会 臨時委員（情報セキュリティ部会委員）
経済産業省 情報セキュリティガバナンス研究会 座長
宇宙航空研究開発機構　情報化評価委員会　委員長　　などを歴任

現在
文部科学省 HPCI計画推進委員会 主査
防衛省 情報流出対策会議　有識者委員
科学技術振興機構 社会技術センター「サービス科学研究開発プログラム」プログラム総括
NPO法人 日本セキュリティ監査協会　会長
情報セキュリティガバナンス協議会　会長
ブロードバンドワイヤレスフォーラム　会長　など.

専門はソフトウェアを中心とした計算機科学および情報セキュリティ

情報セキュリティ認証制度関連など

- 情報マネジメントシステム（IMS）運営委員会 委員長
- 制御システムセキュリティマネジメントシステム（CSMS）評価認証制度
  有識者委員会 委員長
- ITセキュリティ評価・認証プログラム運営委員会 委員長
- 暗号モジュール試験及び認証制度運営委員会 委員長

・独立行政法人 情報処理推進機構 :
情報システム等の脆弱性情報の取扱いに関する研究会 座長
・JPCERT/CC:
制御システム用製品の脆弱性情報の取扱に関する研究会 座長

情報システムセキュリティのこれまで

情報セキュリティの重要性 ①
（情報セキュリティとは？）

情報セキュリティとは、守るべき情報の機密性、完全性、
可用性を維持すること。

・**機密性**：アクセスを認可された者だけが情報をアクセスできることを確実にすること。
・**完全性**：情報及び処理方法が、正確であること及び完全であることを保護すること。
・**可用性**：認可された利用者が、必要なときに、情報及び関連する資産にアクセス
できることを確実にすること。

脅威

情報の機密性、完全性、可用性に危害を与える要因

・外部からの不正行為
・内部での操作・処理ミス
・内部からの不正行為
・偶発的に起きる事故

情報セキュリティの重要性②
（脅威：外部からの不正行為）

●**サイバー攻撃**

不正アクセス、コンピュータウィルス等情報通信ネットワークや情報システムを利用した電子的な攻撃（サイバー攻撃）による情報漏えい、情報消去、改ざん

・電力供給、交通、電子政府等重要インフラや公共の安全確保等の産業や政府の活動の多くは、情報システムに依存。基幹となる情報システムに対してサイバー攻撃が行われた場合には、国民生活や社会経済活動の混乱、国民の生命の危険などの重大な被害が発生。
・他の物理的攻撃と異なり、技術を有する者が一台のコンピュータによって行うことが可能であり、国民生活や社会経済に混乱を引き起こすこと等を目的として組織的に大規模な攻撃（サイバーテロ）を行うことも可能。

●**物理的破壊、盗難**

外部から侵入し、書類、コンピュータ等を盗難、破壊することによる情報漏えい及び情報消去

・大規模な破壊を伴うテロが発生するおそれもある。

情報セキュリティの重要性 ③
（脅威：内部での不正行為、誤操作、事故等）

●**内部での不正行為**

内部関係者（社員、派遣社員、元社員、非常勤職員、下請会社社員等、情報資産に対する正当なアクセス権を有する者）による意図的な情報漏えい、情報消去、改ざん

・情報漏えいの大部分が内部での不正行為だと言われている。
・情報システム及び記録媒体の発達により、情報を外部に持ち出すことが容易となったこと、終身雇用制の崩壊等により、内部での不正行為の危険性が増大。

●**内部での操作・処理ミス**

内部関係者の誤操作等（メールの送信ミス、添付ファイルの間違い、施錠忘れ、PC画面放置、机上の資料放置、ファイルの誤削除、火の不始末による書類焼失、コンピュータシステムの誤設定・誤操作等）による情報漏えい、情報消去、改ざん

●**偶発的に起きる事故**

地震、洪水、台風等の自然災害による停電、破壊、浸水等被害
機器、ソフトウェアの故障

情報セキュリティの重要性 ④
（対応策：技術的措置）

●技術基準（ISO15408（CC: Common Criteria））を用いた対応策

ISO15408（CC: Common Criteria）
：情報技術を用いた製品やシステムの開発、製造、運用に係る情報セキュリティ確保（製品の信頼性保証）に関する基準

対象：OS、コンピュータネットワーク、アプリケーション、ICカード、通信機器、情報家電、モジュール等

Part 1 ： 概要、一般モデル、基本設計書及び要求仕様書の規定
Part 2 ： 情報セキュリティ機能カタログ（機能要件）
Part 3 ： 情報セキュリティ機能評価基準、評価保証レベル（EAL）（保証要件）

機能要件（11項目）

- 監査
- 暗号
- 識別／認証
- プライバシー
- 可用性とリソース管理
- アクセス制御
- 通信
- 利用者データ保護
- セキュリティ管理
- セキュリティ機能保護
- 高信頼性通信路

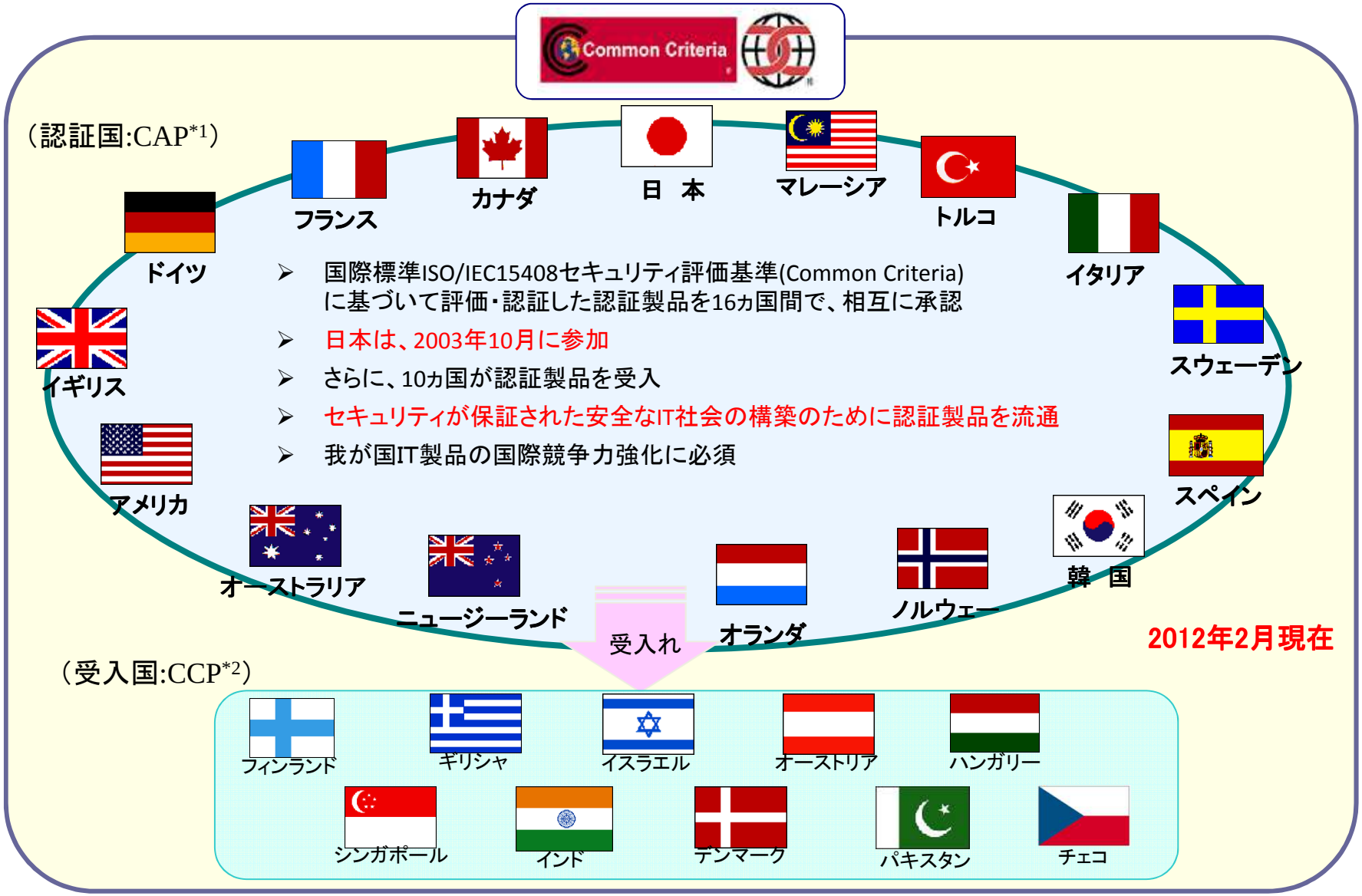
保証要件（10項目）

- 基本設計書の評価
- 構成管理
- 開発と実装
- ライフサイクルサポート
- テスト
- 保守保証
- 要求仕様書の評価
- 配布と運用
- ガイダンス文書
- 脆弱性評価

EAL1～7で規定

EAL: Evaluation Assurance Level

国際的な相互認証制度



*1 CAP ： Certificate authorising participants

*2 CCP : Certificate consuming participants

プログラムの対象

JISEC

- **IT製品**：
  単独で使用又は様々なシステム内への組み込みを目的に設計された機能性を提供するITのソフトウェア、ファームウェア、及び／又はハードウェアの集まり。
- **ITシステム**：
  特定の目的及び運用動作環境を伴う特定のIT設備。
- **プロテクションプロファイル(PP)**：**セキュリティ要求仕様書**
  あるTOEの分野に関して、特定の利用者の要求を満たす実装に依存しないセキュリティ要件を記述した文書のセット。
- **セキュリティターゲット(ST)**：**セキュリティ設計仕様書**
  識別されたTOEの評価に用いられるセキュリティ要件及び仕様を記述した文書。

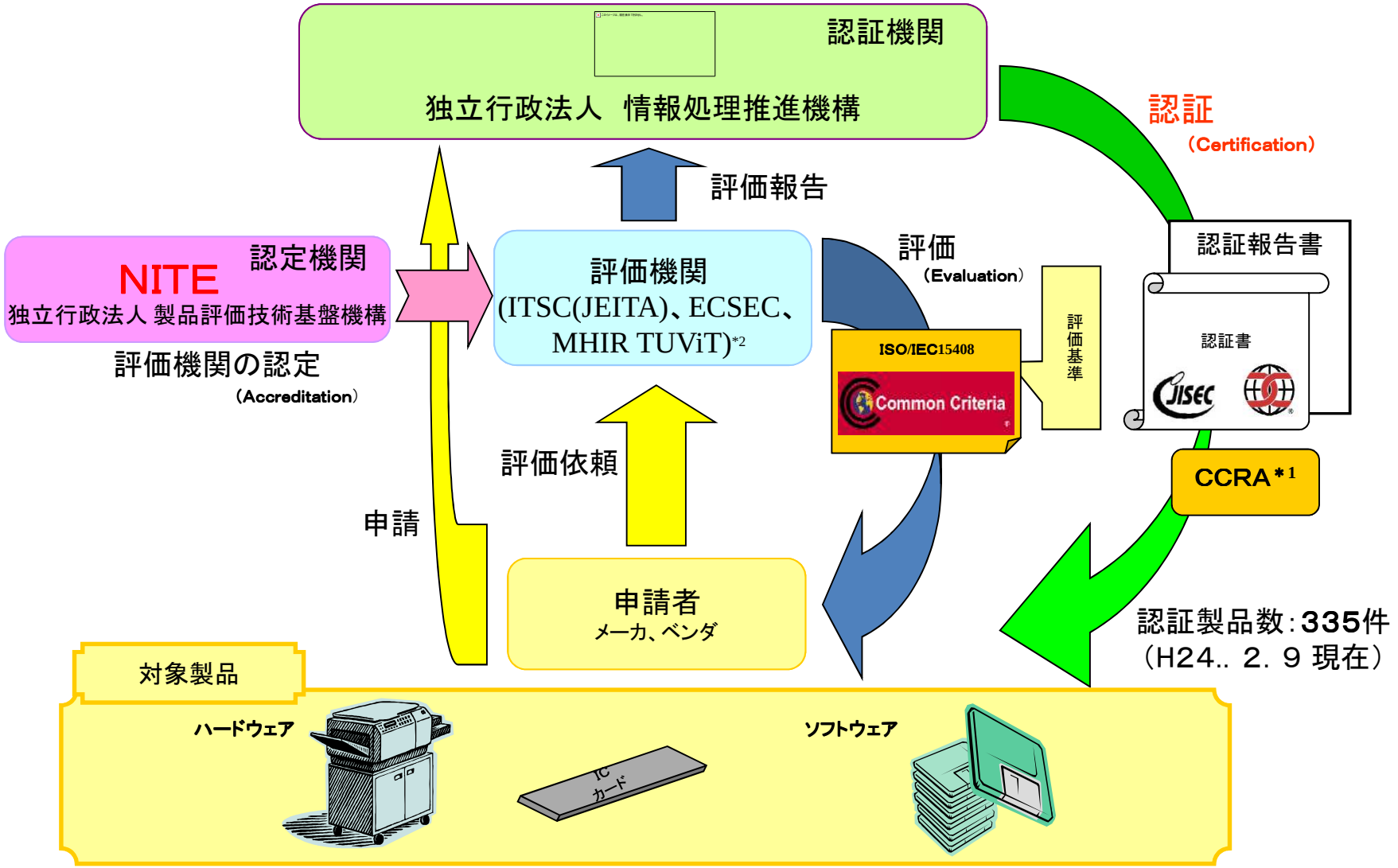
TOE : Target of evaluation

NITE

ITセキュリティ評価及び認証制度
（IT製品等の安全性に係る国際的な評価認証制度）

国際基準（ISO/IEC15408）に基づき、IT製品等の安全性を評価・認証する制度

http://www.ipa.go.jp/security/jisec/index.html



*1：Common Criteria Recognition Arrangement

*2 ITSC:一般社団法人ITセキュリティセンター、ECSEC：株式会社電子商取引安全技術研究所、MHIR：みずほ情報総研株式会社、TUViT:TÜV Informationstechnik

情報セキュリティの重要性 ⑤
（対応策：管理的措置）

●管理基準（BS7799、ISO17799）を用いた対応策

BS7799

：組織が保有する情報資産の情報セキュリティ確保のための組織のマネジメントに関する基準

Part 1 ： 情報セキュリティマネジメントの実戦のための規範（ガイドライン）（→ISO17799）
Part 2 ： 情報セキュリティマネジメントの仕様（要求事項）

Part 1 の構成

1. 適用範囲
2. 用語及び定義
3. セキュリティ基本方針
4. 組織のセキュリティ
5. 資産の分類及び管理
6. 人的セキュリティ
7. 物理的及び環境的セキュリティ
8. 通信及び運用管理
9. アクセス制御
10. システム開発及び保守
11. 事業継続管理
12. 適合性

3．～12．の10マネジメント領域について、全部で36項目の目的、127項目の詳細指針を規定

Part 2

セキュリティマネジメントシステムの構築に当たっての要求事項

情報セキュリティ管理（監査・認証等）の進展（ISMS適合性評価制度の普及）

●ISMS適合性評価制度とは

・組織が行う情報セキュリティマネジメントに対して、ISMS認証基準（ISO/IEC17799及びBS-7799 Part2に基づいた基準）への適合性を第三者が評価する制度。

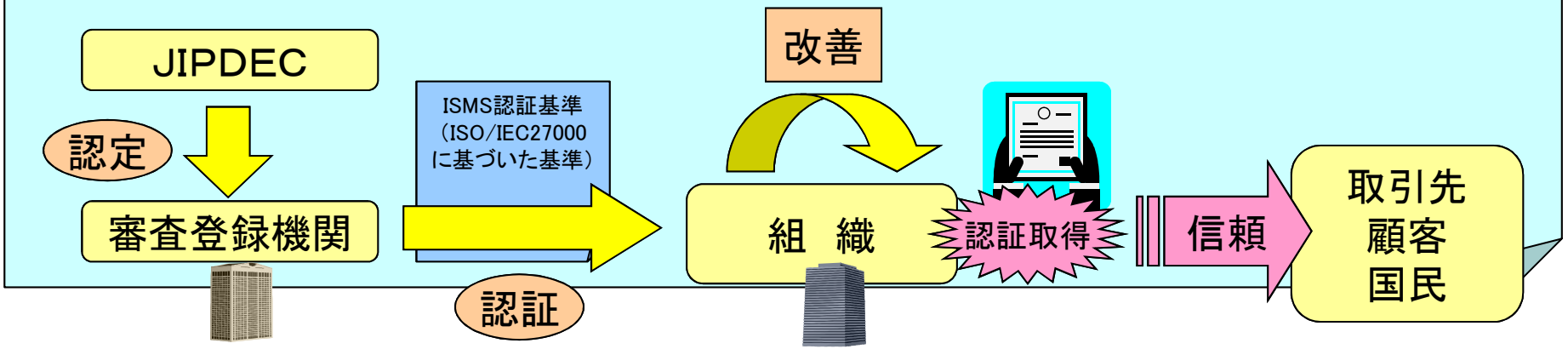
・2002年4月より財団法人日本情報処理開発協会（JIPDEC）によって本格運用開始。
→ISMS認証の取得数の伸び（企業への浸透）

・2006年よりISO27000へ移行

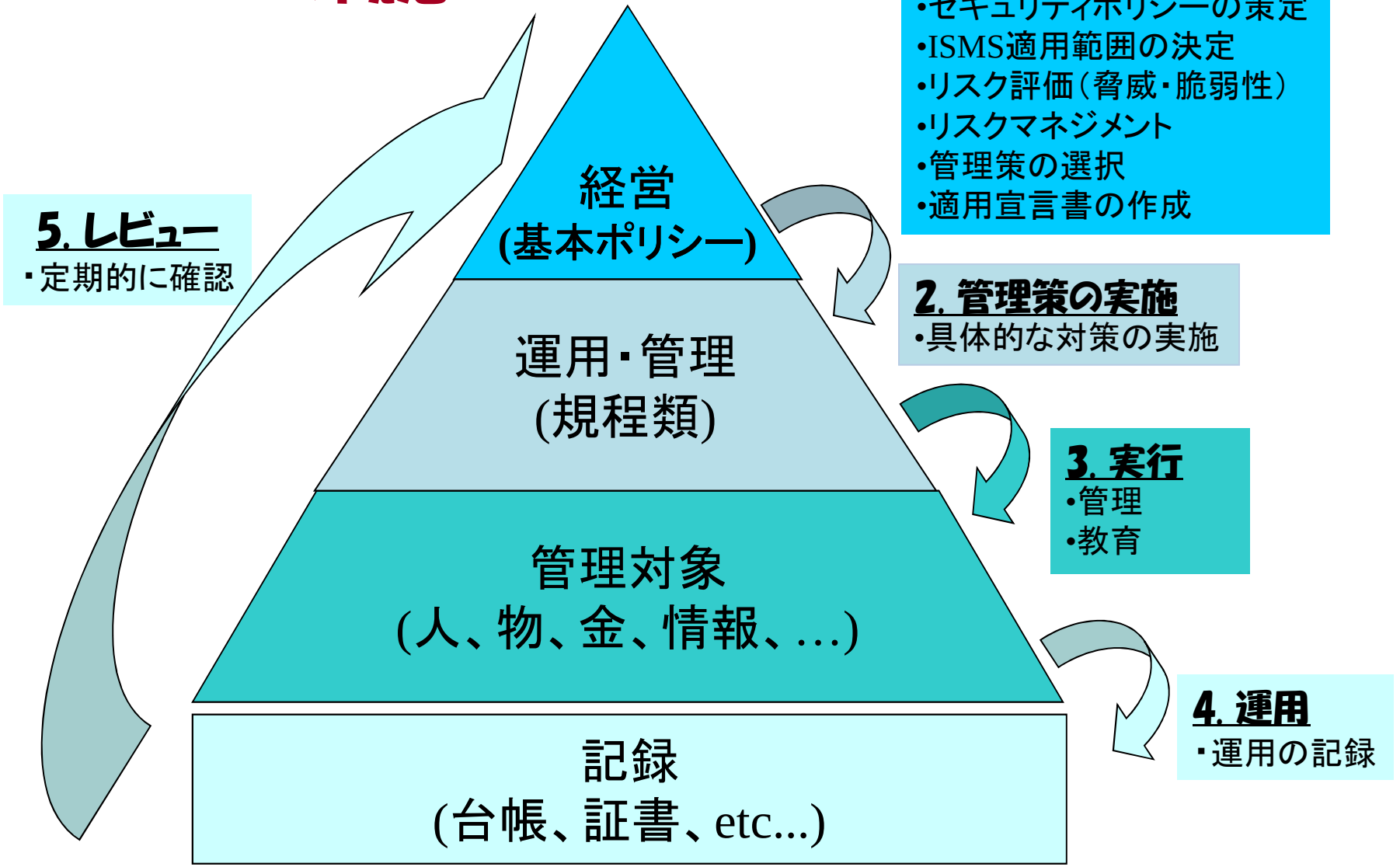
（制度活用のメリット）

・内部監査では発見困難な情報セキュリティ上の欠陥を把握し、改善することが可能

・対外的に、組織としての情報セキュリティ対策の信頼性を確保することが可能



ISMSの概念



1. マネジメント枠組み
- セキュリティポリシーの策定
- ISMS適用範囲の決定
- リスク評価（脅威・脆弱性）
- リスクマネジメント
- 管理策の選択
- 適用宣言書の作成

2. 管理策の実施
- 具体的な対策の実施

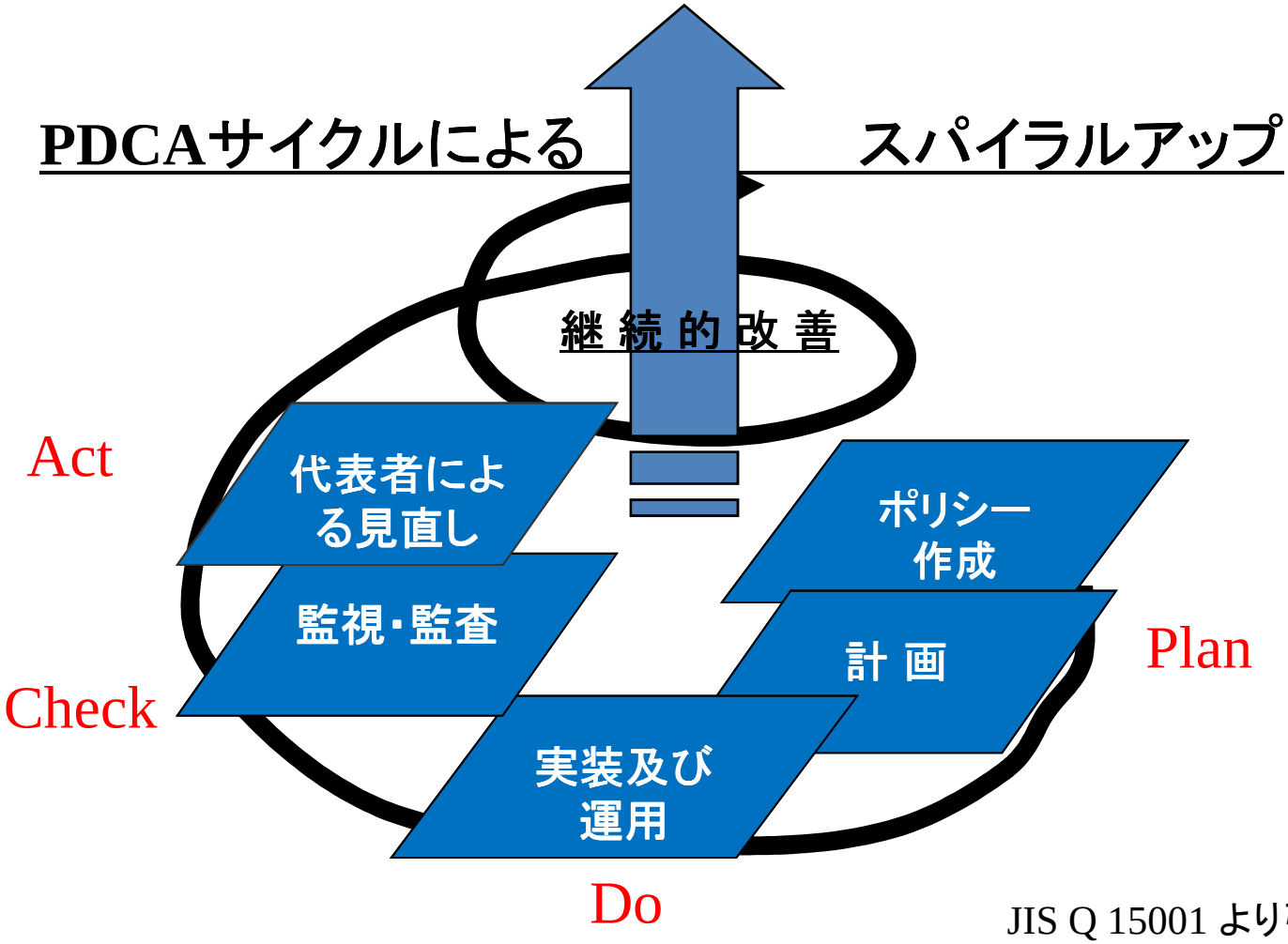
3. 実行
- 管理
- 教育

4. 運用
- 運用の記録

5. レビュー
- 定期的に確認

*セキュリティポリシー：　基本方針（ポリシー）、対策基準（スタンダード）、実施手順（プロシージャ）

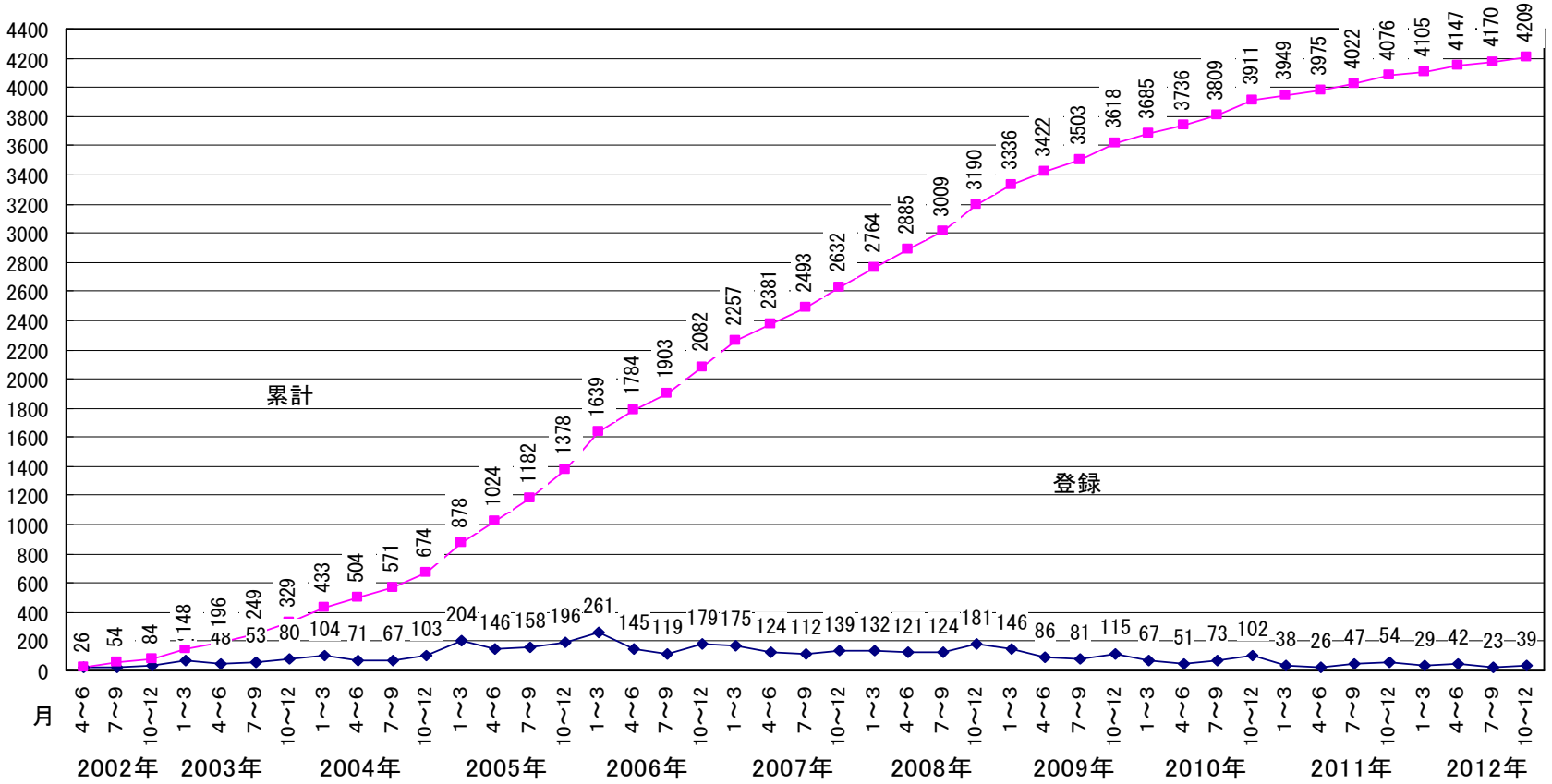
マネジメントシステム(PDCA)
[継続的なマネジメントレビュー]



JIS Q 15001 より引用・加筆

ISMS認証取得組織数の推移

2012年12月25日現在



各国のISMS認証取得登録発行数

出典：http://www.iso27001certificates.com/

(Version 215 August 2012)

2012年11月現在

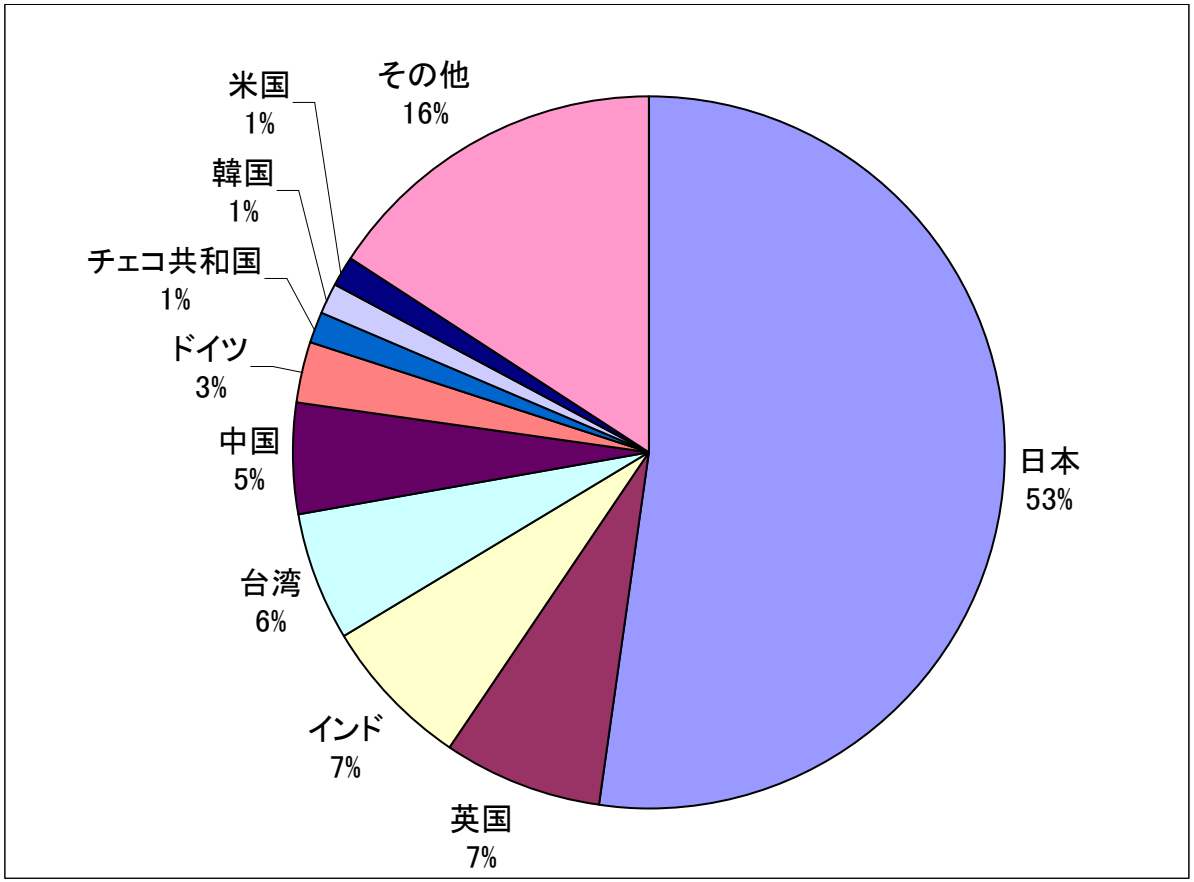
日本	4152	オーストラリア	30	カナダ	10	ジャージー	2
英国	573	シンガポール	29	ノルウェー	10	カザフスタン	2
インド	546	クロアチア	27	スウェーデン	10	ルクセンブルク	2
台湾	461	スロベニア	26	スイス	9	マケドニア	2
中国	393	メキシコ	25	バーレーン	8	マルタ	2
ドイツ	228	スロバキア	25	ペルー	7	モーリシャス	2
チェコ共和国	112	ブラジル	24	チリ	5	ウクライナ	2
韓国	107	オランダ	24	エジプト	5	アルメニア	1
米国	105	サウジアラビア	24	オマーン	5	バングラディシュ	1
イタリア	82	アラブ首長国連邦	19	カタール	5	ベラルーシュ	1
スペイン	72	ブルガリア	18	スリランカ	5	ボリビア	1
ハンガリー	71	イラン	18	南アフリカ共和国	5	デンマーク	1
マレーシア	66	ポルトガル	18	ドミニカ共和国	4	エストニア	1
ポーランド	61	アルゼンチン	17	モロッコ	4	キルギスタン	1
タイ	59	フィリピン	16	ベルギー	3	レバノン	1
ギリシャ	50	インドネシア	15	ジブラルタル	3	モルドバ	1
アイルランド	48	パキスタン	15	リトアニア	3	ニュージーランド	1
オーストリア	42	コロンビア	14	マカオ	3	スーダン	1
トルコ	35	ロシア連邦	14	アルバニア	3	ウルグアイ	1
トルコ	35	ベトナム	14	ボスニア・ヘル	2	イエメン	1
フランス	34	アイスランド	13	キプロス	2		
香港	32	クウェート	11	エクアドル	2	**Total**	**7940**

各国のISMS認証取得登録発行数

出典：http://www.iso27001certificates.com/
2012年11月現在

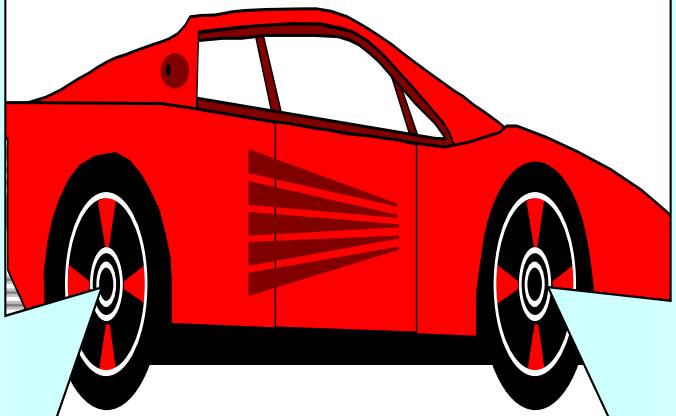
(Version 215 August 2012)

国	組織数
日本	4152
英国	573
インド	546
台湾	461
中国	393
ドイツ	228
チェコ共和国	112
韓国	107
米国	105
その他	1263
計	7940



情報セキュリティにおける技術とマネジメント

情報セキュリティの確保には、
①技術的対応
②マネジメント的対応
が車の両輪



技術的な対応

・IT製品・システムの安全性について客観的な基準（ISO/IEC 15408）に基づいて評価する制度。

・日本では、2001年4月より独立行政法人製品評価技術基盤機構を中心とし、政府利用のIT関連製品のための評価・認証体制の創設。

・2003年に国際相互承認の枠組み（CCRA）への参加。

・欧米では既に10年以上の評価実績があり、相互承認のスキーム (Common Criteria Scheme) が1998年から存在。

マネジメント的な対応

・組織における情報安全対策のあり方を客観的な基準（ISO/IEC 27000）に基づいて評価する制度。組織において、必要な安全性のレベルの決定、プランの作成、自らの評価、定期的な見直し等のマネジメントを求めている。

・日本では、2002年4月より運用開始。情報処理開発協会（JIPDEC）による認証制度（ISMS認証制度）が開始されている。

・国際相互承認をにらんだガイドラインを提示。

・海外では英国を中心に認定制度が運用されてきた。

製品からプロセスへ

機器・ソフトウェアに関する
情報技術セキュリティ評価・認証制度

情報セキュリティマネジメントに関する
適合性評価制度

情報セキュリティ監査

情報セキュリティ監査制度

http://www.meti.go.jp/policy/netsecurity/is-kansa/index.html

- 「**情報セキュリティ監査制度**」とは、(1)企業等の情報セキュリティ対策（外部からの不正アクセス防止の設定をしているか、情報管理責任者を任命しているか等）について、(2)客観的に定められた国の基準に基づいて、(3)独立した専門家が(4)評価（保証または助言）する制度。
  - 2003年4月、「情報セキュリティ管理基準」及び「情報セキュリティ監査基準」を、経済産業省告示により公表。これに基づき、制度運用開始。
  - 監査主体は「情報セキュリティ監査企業台帳」に登録され（約500事業主体）、公表。毎年7月に更新。「日本セキュティ監査協会」（JASA）にて、監査の質の向上のための取り組み。

客観的に定められた国の基準

- 「改善のプロセス」までを包含した「管理項目」を定めた基準（監査の際の判断の尺度）

⇒ 情報セキュリティ**管理**基準

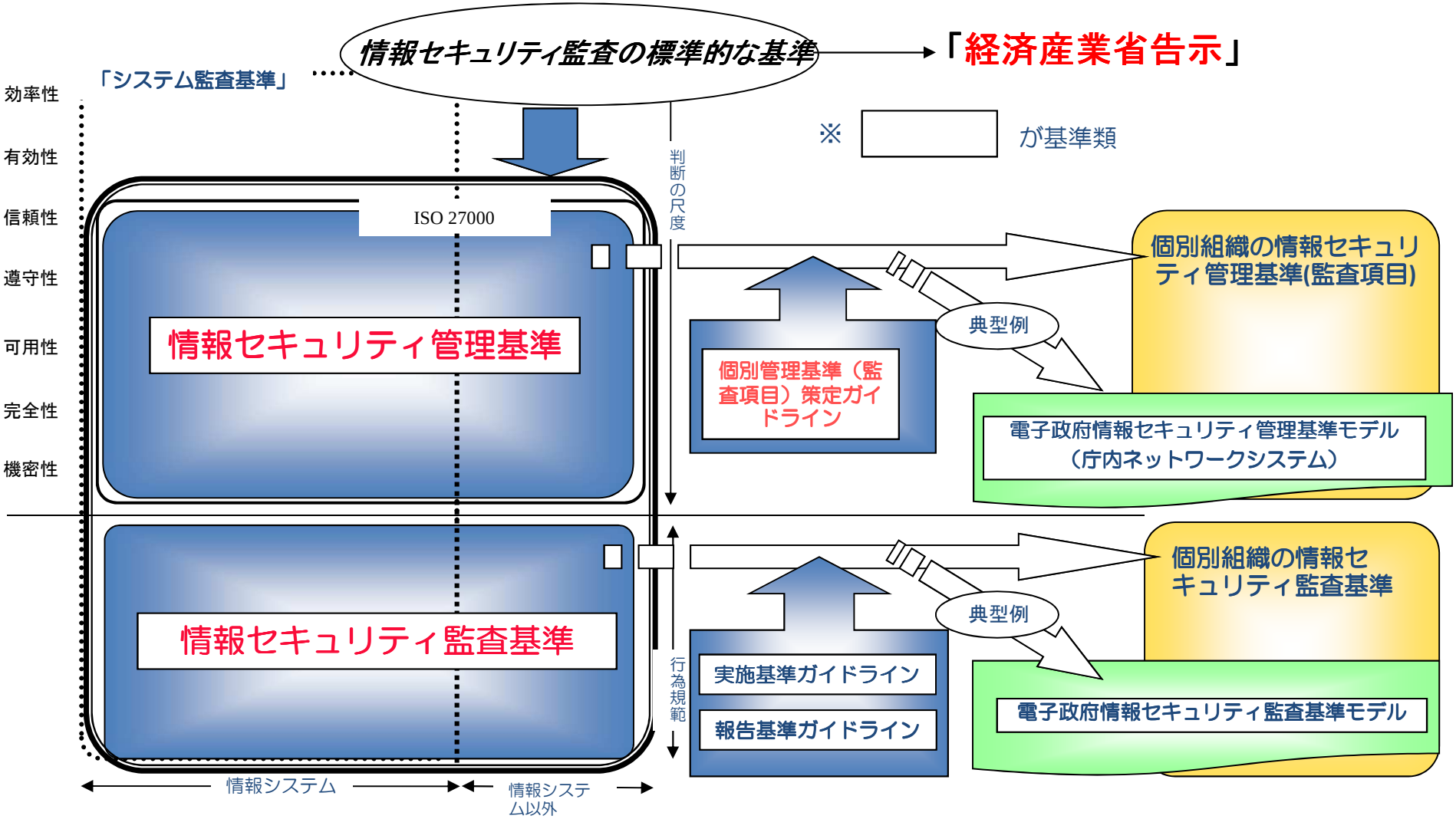
- 監査主体の行為規範を定めた基準

⇒ 情報セキュリティ**監査**基準

- 会計監査のような法定監査ではないものの、これらの基準を国が標準として示すことで、監査結果に対する「**公定力**」や「**信頼**」を付与。
- 事例の蓄積も容易となり、法的責任の分担も明確化の方向へ。

客観的に定められた国の基準

（全体像～2つの基準・3つのガイドライン・2つのモデル）



http://www.meti.go.jp/policy/netsecurity/index.html 「情報セキュリティ監査制度」より入手可能

ISMS認証との関係

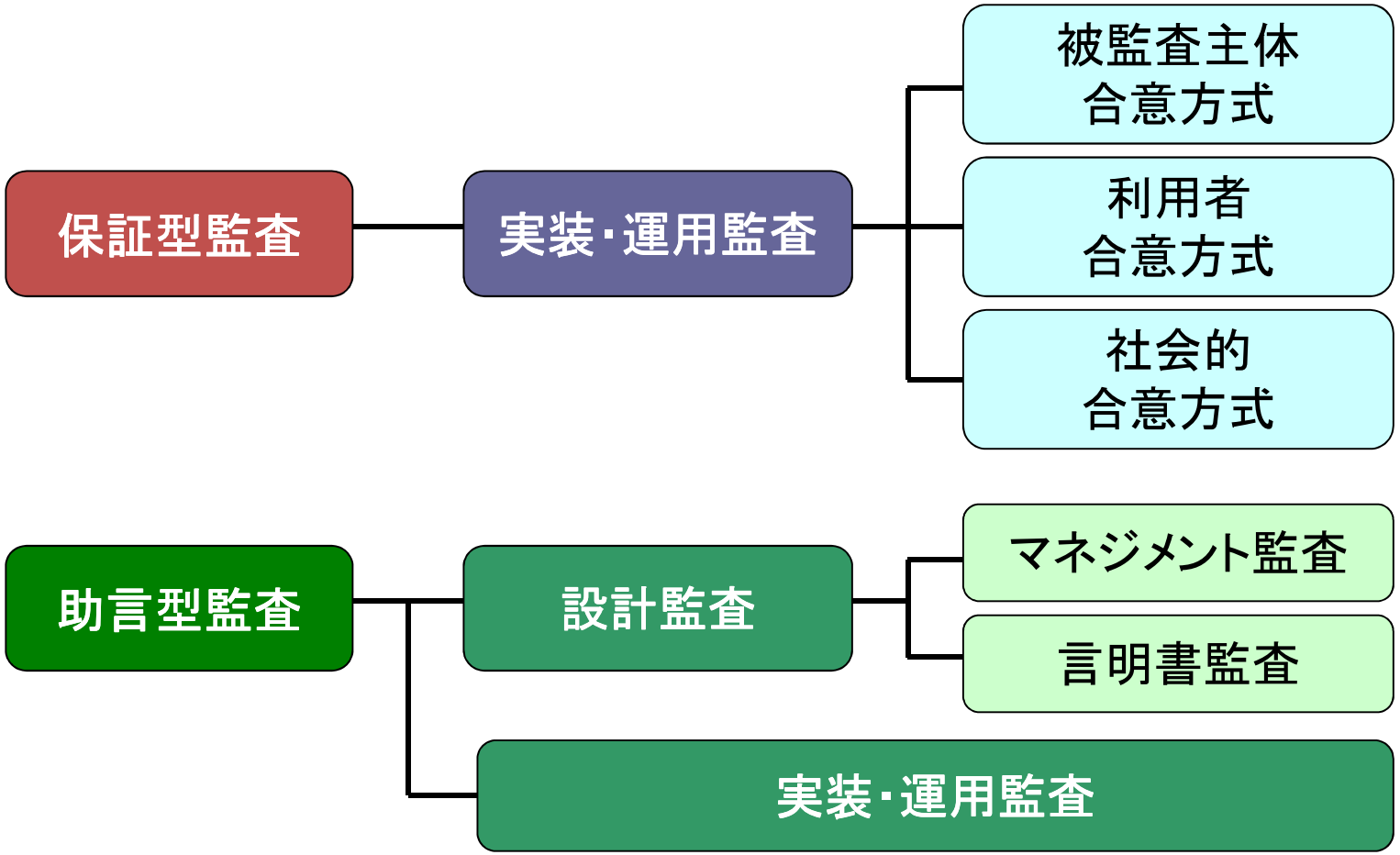
委託先がISMS認証を取得していれば、委託先において的確な情報セキュリティのマネジメントが行われていると期待できるので、一応安心と考えることができる。

しかし、ISMS認証取得は、自社とのリスク認識が同じことを保証してくれるわけではない。

つまり、委託先がISMS認証を取得しているだけでは、トータルのリスク対応コストが最適化されていることにはならない。

重要な情報を委託先に委ねるなどの場合は、委託先の条件としてISMS認証取得を求めることが有効だが、さらに保証型情報セキュリティ監査でリスク認識を共通にすることが最善の対策といえる。

情報セキュリティ監査の種類



＊設計監査　　組織が定めた（設計した）情報セキュリティ対策が第三者から求められているレベルに達していることを保証の内容とする。

＊実装監査　　組織が定めた（設計した）情報セキュリティ対策と組織の現在の情報セキュ リティ対策に乖離がないことを保証の内容とする。

特定非営利活動法人 日本セキュリティ監査協会

会　長

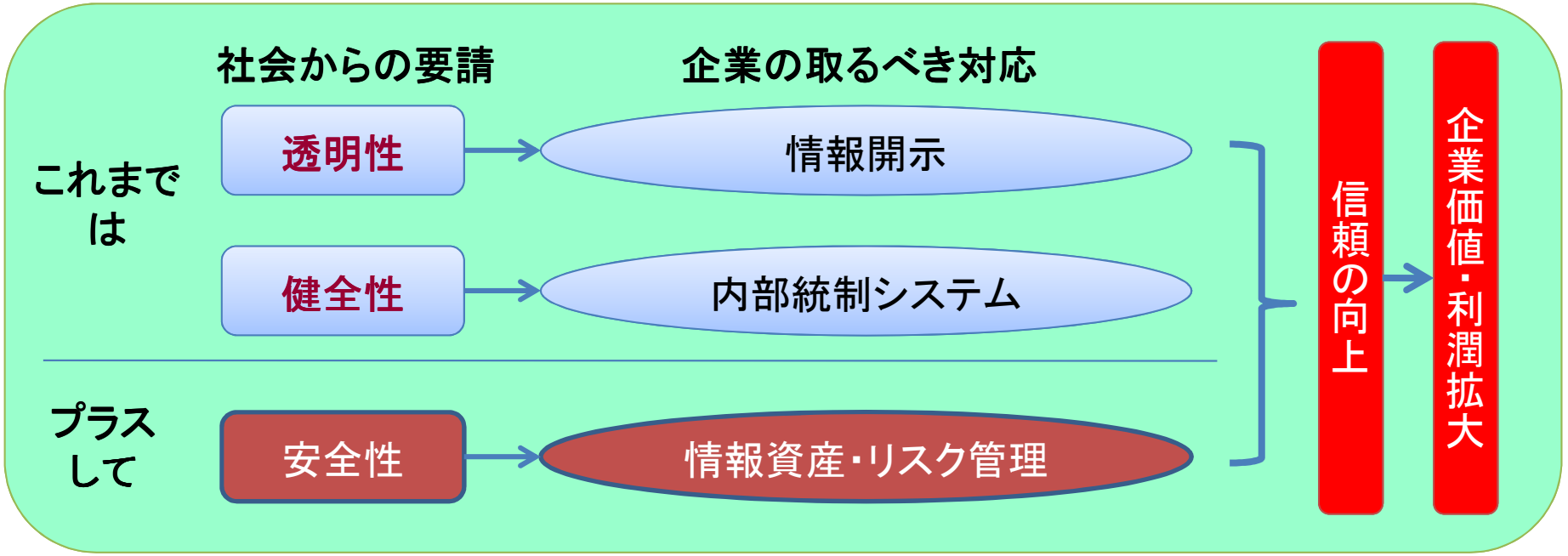
土居範久　　慶應義塾大学名誉教授

副会長

増谷洋　　NRIセキュアテクノロジーズ株式会社代表取締役社長
長尾 慎一郎　新日本有限責任監査法人

情報セキュリティガバナンス

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**」としてまとめることが急務

情報セキュリティガバナンスの確立とは

確立プロセス例

すべての企業には守るべき情報資産、対処すべきリスクがある

↓

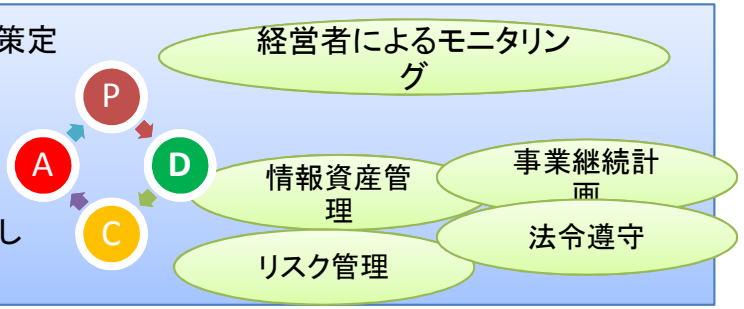
リスクを低減して情報資産を守ることが情報セキュリティの確保である

↓

適切に評価を行わずに情報セキュリティ対策を施し続けていても投資対効果（ROI）を評価できない

経営者が自身の経営課題として捉え

① 情報資産の価値、リスクの大きさの判断を行う指標の策定
② 指標に基づく情報資産評価、リスクアセスメント
③ アセスメント結果に基づく情報セキュリティ対策の立案
④ 情報セキュリティ対策の実施
⑤ 対策効果のアセスメント
⑥ アセスメント結果に基づく情報セキュリティ対策の見直し
⑦ 情報セキュリティ対策の実施



↓

企業の活動目的（利潤確保、社会貢献等）を支援する適切な情報セキュリティ対策を実現

↓

情報セキュリティへの取組、ROI等を公開することで投資市場、取引先企業からの評価が向上

↓

リスクを減らし、情報資産を守り、利潤を上げ、社会貢献を果たす、理想的な企業へ

情報セキュリティガバナンス　2005.3

問題点

(1) IT事故発生のリスクが明確でなく、適正な情報セキュリティ投資の判断が困難

✓ **投資判断のための指標**が求められているのではないか。

(2) 既存の情報セキュリティへの「対策」「取組」が企業価値に直結していない

✓ 情報セキュリティに係る取組みが、**企業価値向上**に寄与する仕組みが必要ではないか。

(3) 事業継続性確保の必要性が十分に認識されていない

✓ IT事故発生時の対応手続きを**事業継続の観点**から定めておくことが必要ではないか。

問題点を克服し、企業が情報セキュリティガバナンスの確立を促進するツール

情報セキュリティ対策ベンチマーク

- 情報セキュリティ対策のセルフチェック等に有用なベンチマークの指標を開発
- さらに、IT事故データ収集のあり方や被害想定額算出手法について調査し、ベンチマークデータと連動したリスク評価の可能性を模索

情報セキュリティ報告書モデル

- 企業のコンプライアンスや社会的責任を説明するIRの一環として、自らの情報セキュリティポリシーやそれを実現する対策の実施状況について対外的に公表する「情報セキュリティ報告書」を提唱し、そのモデル案を策定

事業継続計画策定ガイドライン

- 企業がIT事故発生時にも事業運営を継続的に維持するための事業継続計画（BCP）について、その策定手順や検討項目、事例等を紹介する「事業継続計画策定ガイドライン」を策定

企業・社会への普及方策

・情報セキュリティ格付け
・政府調達への活用
・損害保険との連携　　等

既存施策との連携

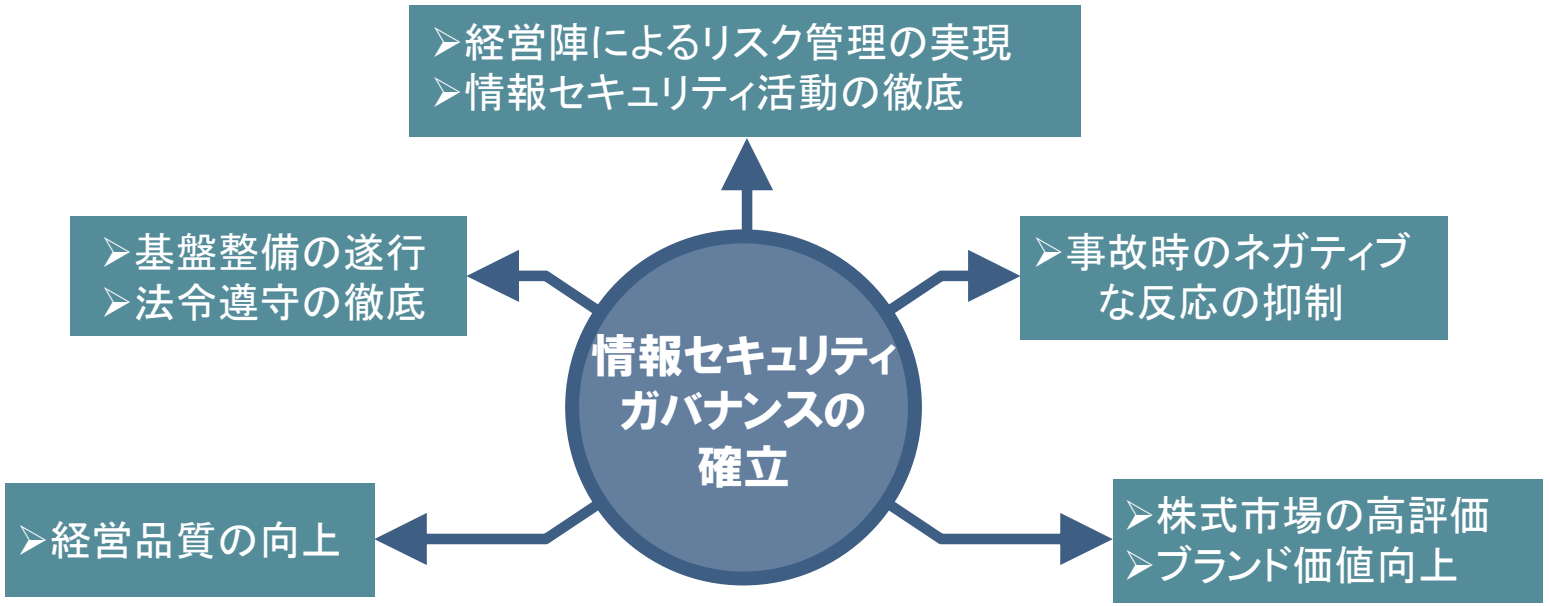
・ISMSや情報セキュリティ監査の「入口」としての活用
（セルフチェック→第三者認証・評価へ）　等

企業における情報セキュリティガバナンスの確立

情報セキュリティガバナンスの期待される効果

■ 情報セキュリティガバナンスに取り組むことで、情報セキュリティが経営陣に「見える」ようになり、適切なリスク管理の実現が期待できる。

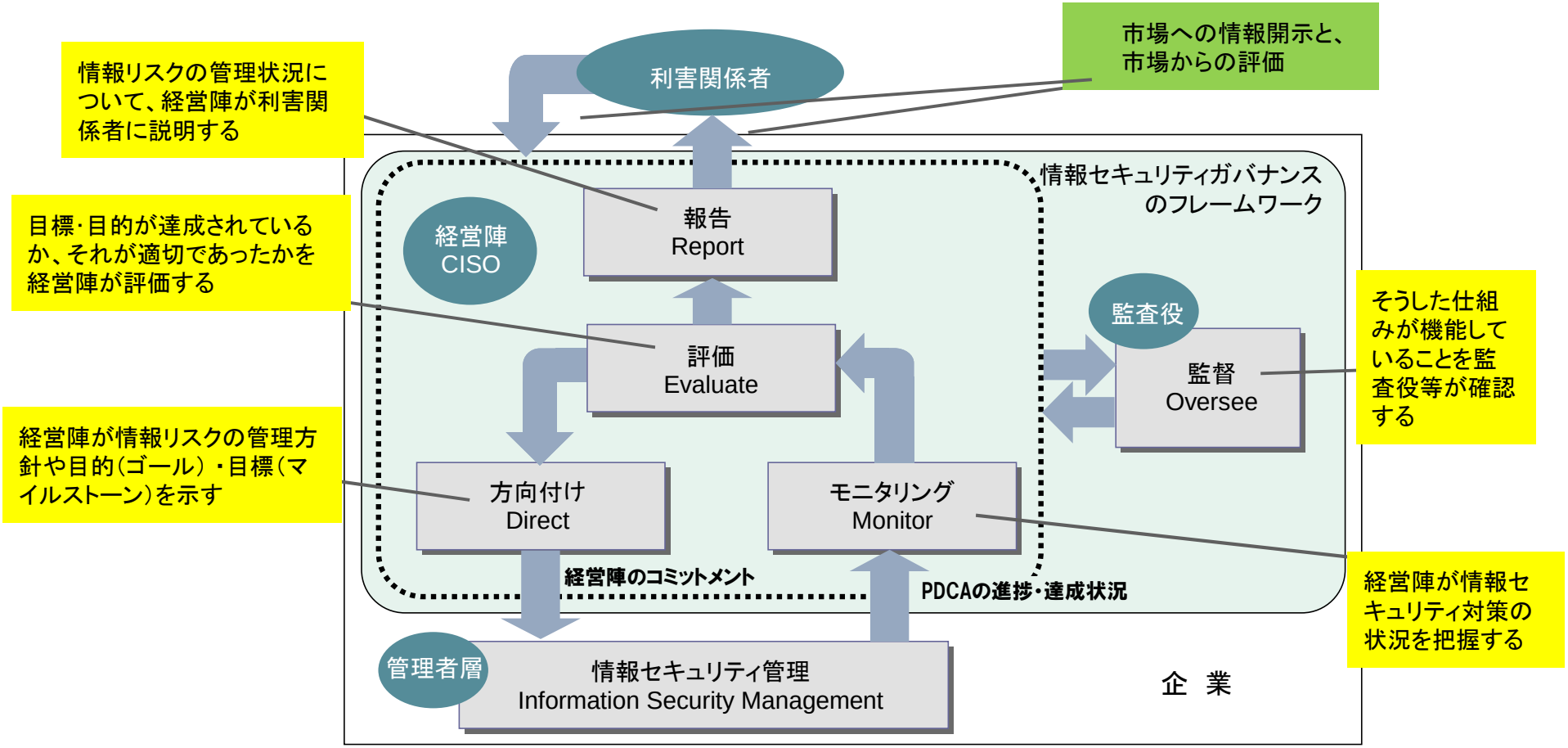
■ また、品質の向上はもちろん、コンプライアンスの徹底や経営品質の向上、さらに企業価値向上、事故時のネガティブな反応を抑制する効果も期待できる。



企業が情報セキュリティガバナンスに取り組むことで得られる効果

経営陣に求められる5つの活動

■ 経営陣が主体的かつ適切に情報リスクを管理し、利害関係者に説明する仕組みを構築・運用
→ 方向付け、モニタリング、評価、監督、報告の5つの活動を実施



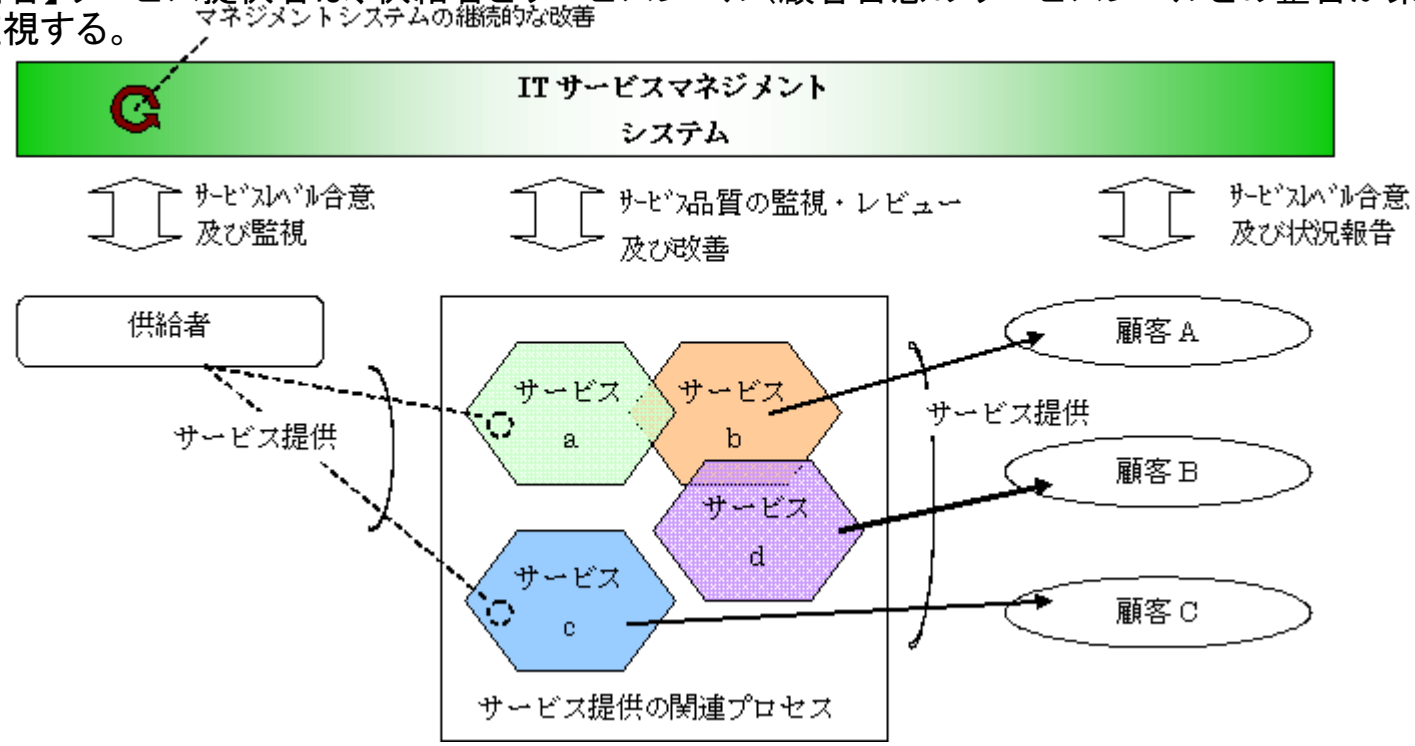
情報セキュリティガバナンスのフレームワーク

（出典：経済産業省「情報セキュリティガバナンス」, 2009/08を基に作成）

ITSMS

サービス提供者が、提供するITサービスのマネジメントを効率的、効果的に運営管理するための仕組み（ISO/IEC 20000に基づく制度。 2007年4月より運用開始）

【対顧客】サービス提供者は、提供のサービスレベルを顧客と合意し、合意に基づいたサービス品質を管理し、サービスレベル状況を顧客に報告する。
【対サービス提供の関連プロセス】サービスマネジメントは、顧客との合意のサービスレベルを含む各種要求を満たすよう、サービス提供の関連プロセスを統制する。
【対供給者】サービス提供者は、供給者とサービスレベル（顧客合意のサービスレベルとの整合が条件）を合意し、監視する。



IMS運営委員会

委員長　　土居　範久（慶應義塾大学　名誉教授）
副委員長　大木　榮二郎（工学院大学　教授）
副委員長　島田　洋之（大同火災海上保険株式会社）
委員　　稲垣　隆一（稲垣隆一法律事務所）
委員　　榎木　千昭（慶應義塾大学　教授）
委員　　大畑　毅（日本電気株式会社）
委員　　熊谷　堅（KPMGビジネスアドバイザリー株式会社）
委員　　小林　憲明（日本マネジメントシステム認証機関協議会）
委員　　駒瀬　彰彦（株式会社アズジェント）
委員　　小山　條二（特定非営利活動法人itSMF Japan）
委員　　笹岡　賢二郎（独立行政法人　情報処理推進機構）
委員　　塩田　貞夫（洛ITサービス・マネジメント株式会社）
委員　　杉浦　昌（日本電気株式会社）
委員　　田原　幸朗（一般社団法人情報サービス産業協会）
委員　　出口　幹雄（富士通株式会社）
委員　　中尾　康二（KDDI株式会社）
委員　　藤本　正代（富士ゼロックス株式会社）
委員　　八木　隆（株式会社日立製作所）

制御システムセキュリティのこれから

制御システムセキュリティ上の脅威事例

米国 *1997年*	***米国の重要インフラに直接的な被害を与えた最初の事例*** 10代の若者がダイアルアップモデムを使って、マサチューセッツ州ウォーセスター空港の設備にサービスを提供していた通信事業者NYNEXのデジタル・ループ・キャリア・システムを停止させ、空港の管制塔、セキュリティ、消防署、気象サービス及び空港を利用する航空会社の電話サービスを利用不能にした。さらに、管制塔に設置してある滑走路のライトを制御する送信機をシャットダウンしたため、6時間にわたって同設備が使えなくなった。
豪州 *2000年*	***SCADA※システムへの攻撃の事例*** オーストラリアのSCADAソフトウエアを開発する企業の元従業員が、上下水処理場の運営会社の職に応募したものの不採用とされたことに恨みを抱き、2カ月間の間46回にわたって同社の下水処理の制御システムに侵入し、下水排水施設のデータを書き換えたりオペレーションを妨害し、結果として264,000ガロンもの未処理の下水を河川や公園に放出した。
米国 *2005年*	***ウィルス感染により制御システムが停止する事例*** 米国のダイムラー・クライスラー（現ダイムラー）の 13の自動車工場が単純なインターネットワームにより操業停止となった。情報ネットワークと制御ネットワークの間にはファイアウォールが設置されていたにもかかわらず、Zotobワームが制御システム内に入り込み、プラント中に広がった（外部から持ち込まれ、制御システムに接続されたノート PC 経由の可能性も指摘されている）。自動車生産は50 分間停止する状態となったほか、部品サプライヤへの感染も疑われて部品供給の懸念も生じ、およそ 1,400 万ドルの損害をもたらした。

※SCADA（Supervisory Control And Data Acquisition）：コンピュータによるシステム監視とプロセス制御を行う制御システム

制御システムへのウィルス感染事例はインシデントとして最も多く、事例のような持込みPC経由の感染、中央監視室からのインターネット接続による感染などの事例が報告されている。特に近年USBメモリによりウィルス感染する事例は頻発している。

スタックスネット（Stuxnet）

・Windowsで感染するコンピュータウイルス

・シーメンス社が遠隔監視制御・情報取得（SCADA）システムにおいてプログラマブルロジックコントローラ（PLC）に対するWindows側のインタフェースソフトウェアとして採用しているWinCC/PCS7を攻撃目標としている

・2010年9月に、イランの核燃料施設のウラン濃縮用遠心分離機を標的として、スタックスネットを使ったサイバー攻撃が実施された

・インターネットから隔離されたスタンドアローンの産業用制御システムにおいても感染し、かつ実害を生じるという特徴がある

・2011年秋に出現したトロイの木馬型マルウェアであるドゥークーは、スタックスネットから派生したものと考えられている

・シマンテックは「USBメモリで媒介される」として不用意な接続をしないよう呼びかけている

出典：Wikipedia

現実的な脅威

USBメモリ

- Stuxnet等USBメモリからのマルウェア感染事例がある
- 制御システムではUSBメモリデバイスが膨大であり、なくすことは不可能

リモートメンテナンス回線

- 某社は、米国アトランタの中央監視室からリモートメンテナンス回線により世界中のタービンをリアルタイム監視
- リモートメンテナンス回線の先の端末からの不正アクス
- 端末からのマルウェア混入

操作端末の入れ替え

- 日本の自動車会社では、ベンダが入れ替えた端末にウィルスが混入していた事例あり
- 操作端末は、Windows等汎用パソコンであることが一般的

内部犯行

- 内部犯行者は物理的セキュリティをすり抜ける
- スイッチに直接PCを接続すると、不正パケット送信や盗聴可能

制御システムにおける脆弱性

（独）情報処理推進機構では「JVN iPedia」という脆弱性対策情報データベースを運営している。このデータベースに登録された産業用制御システムの脆弱性対策情報は、2010年（21件）、2011年（89件）、2012年（162件）と大幅な増加傾向にある（PCソフトウェアの2012年登録脆弱性件数は528件）。

また、脆弱性対策情報全体と比較して深刻度レベルIII（危険）と評価された脆弱性対策情報が相当に多い。

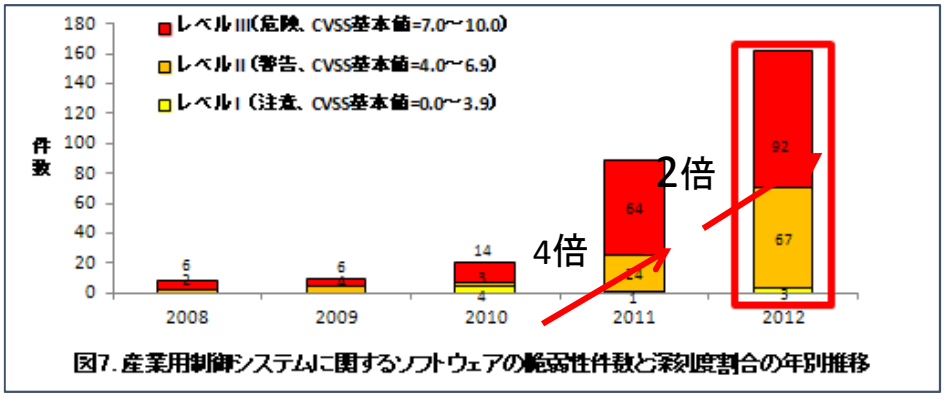


図7. 産業用制御システムに関するソフトウェアの脆弱性件数と深刻度割合の年別推移

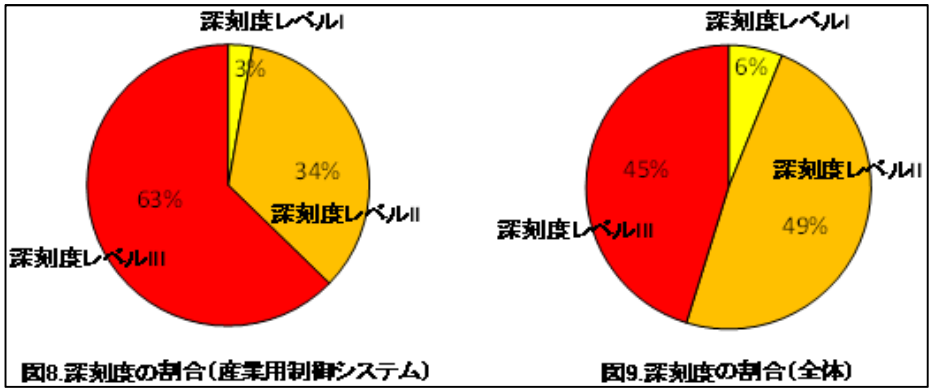
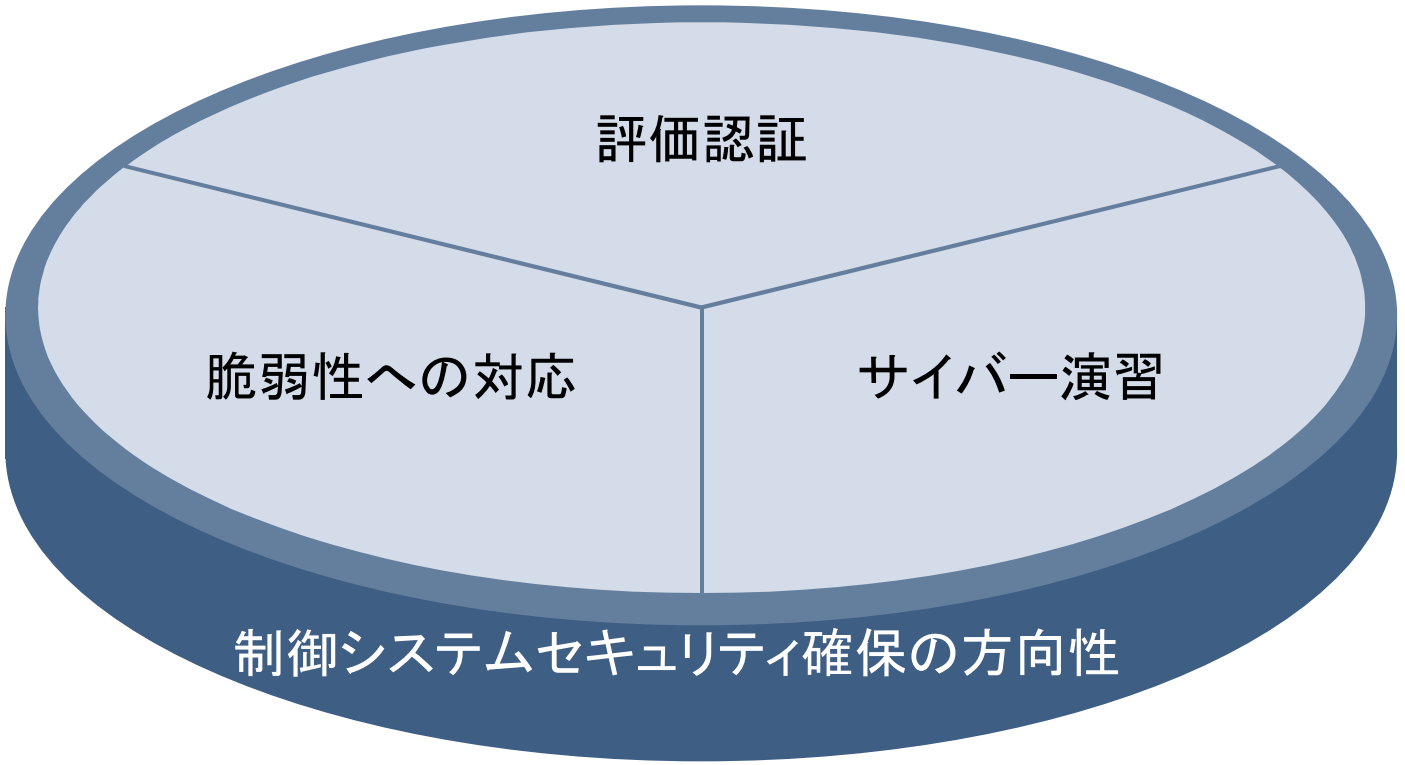


図8.深刻度の割合（産業用制御システム）

図9.深刻度の割合（全体）

出典：IPA脆弱性対策情報データベースJVN iPediaの登録状況 [2012年第4四半期（10月～12月）]

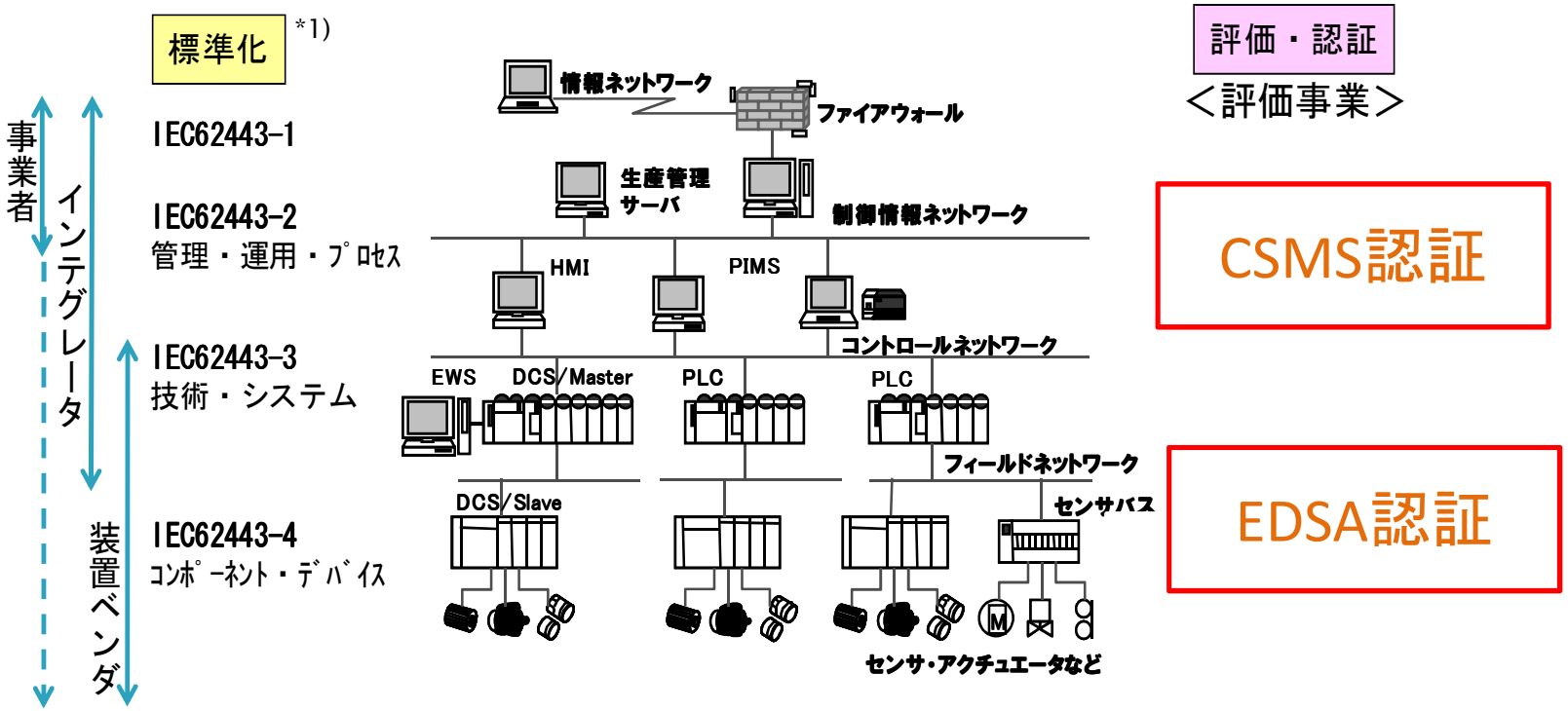
制御システムセキュリティ確保の方向性



制御システムセキュリティ
における評価認証

制御システムセキュリティにおける評価認証

■IEC62443は制御システムセキュリティの全レイヤ/プレイヤーをカバーした規格
■先行する評価認証の規格（EDSA認証等）がIEC62443に採用される方向



*1) IEC62443のCyber securityの標準化作業は、IEC/TC65/WG10が担当（日本国内事務局はJEMIMAが対応）
*2) Cyber Security Management System：ISMSを制御システム関連組織向けに特化した要求事項を規定（認証スキーム開始予定）
*3) EDSA：Embedded Device Security Assurance：制御機器（コンポーネント）の認証プログラム→IEC62443-4に提案されている
*4) ﾈｯﾄﾜｰｸ接続装置（ｺﾝﾄﾛｰﾗ等）の認証（ﾍﾟﾈﾄﾚｰｼｮﾝ、ﾌｧｼﾞﾝｸﾞﾃｽﾄ）　調達要件に指定されている（EDSA要件としても引用）
*5) DCS: Distributed Control System　PLC: Programmable Logic Controller　PIMS: Process Information Management System

CSMS認証

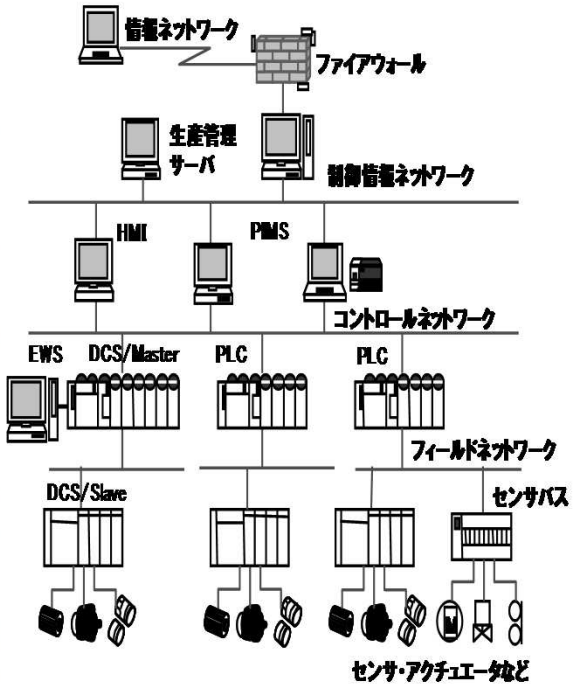
CSMS規格とIEC62443の対応関係

CSMS規格(126要件)

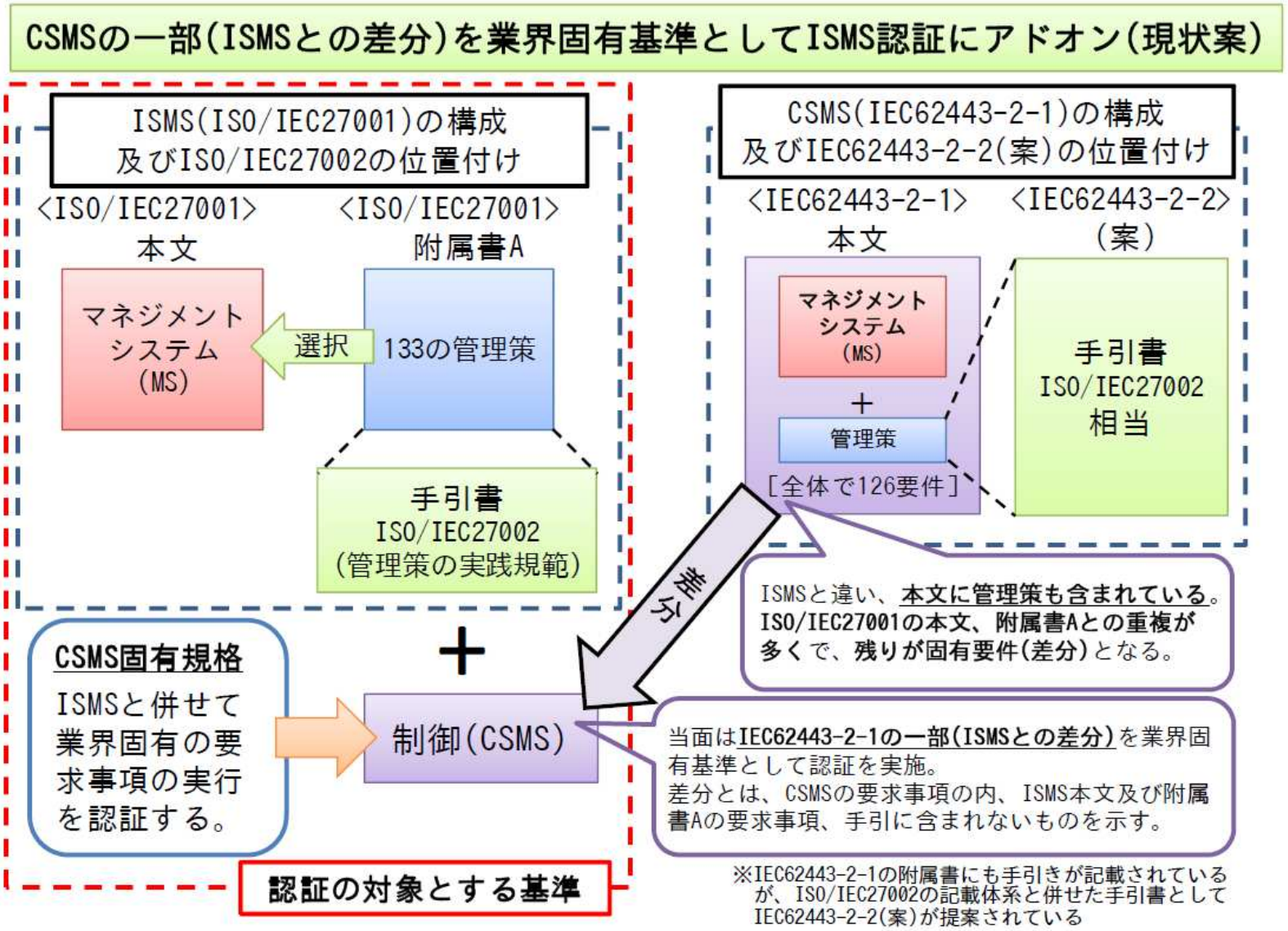
- リスク分析
- リスク対応
- 維持・改善

・ISMSの要求事項をベースとした規格
・本規格を用いた日本発の認証スキームを構築予定

IEC	主対象者	区分
62443-2-1	事業・運用者	セキュリティプログラム
62443-2-2		
62443-2-3		
62443-2-4		
62443-3-1	構築事業者・SIer	システム
62443-3-2		
62443-3-3		
62443-4-1	装置ベンダ	部品
62443-4-2		



CSMSの認証の対象とする基準案



CSMS評価認証制度確立計画

・2013年度：パイロットプロジェクトにより、認証基準、スキームを立ち上げ

・2014年度：認証事業の開始。先行事業者によるノウハウの蓄積

・2015年度：業界別のガイドライン策定。事業メリット明確化、認証取得拡大

2013 年　　2014 年　　2015 年

認証取得の試行

・先行的な評価・認証によるノウハウの蓄積(2件程度)

・効果的な試行者の選定

・パイロットプロジェクト国家施策による立上げ支援

評価認証の拡大

・一般認証事業開始

・業界固有の特徴分析、ノウハウの蓄積（業界毎に1件程度）

認証の本格的普及

・蓄積されたノウハウに基づくガイドラインの策定（各業界向けガイドライン公開）

・ガイドラインを活用した評価・認証の実施

・認証取得の事業メリットの明確化、活用

出典：IPA　CSMS説明資料

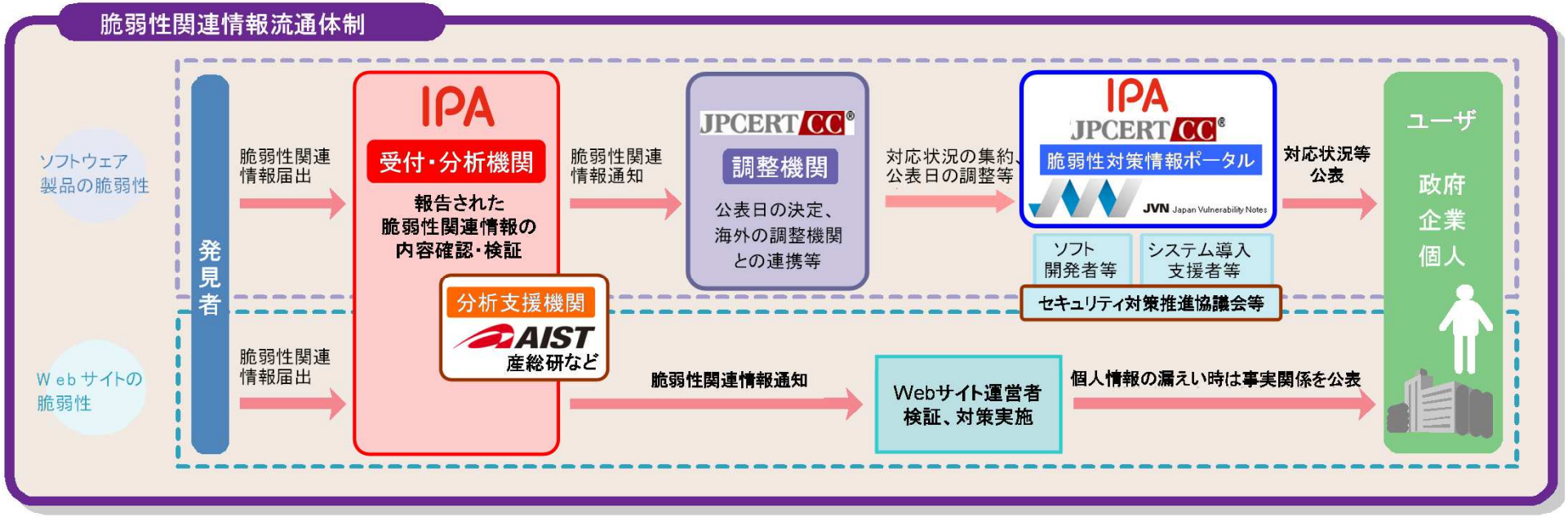
有識者委員会

氏名	会社・機関名
委員長 土居　範久	慶應義塾大学
大木　榮二郎	工学院大学
織茂　昌之	株式会社日立製作所
小林　偉昭	技術研究組合　制御システムセキュリティセンター（CSSC）
金野　千里	独立行政法人情報処理推進機構(IPA)
佐々木　良一	東京電機大学
鈴木　剛	東洋エンジニアリング株式会社
武部　達明	横河電機株式会社
藤巻　慎二郎	公益財団法人日本適合性認定協会(JAB)
宮地　利雄	一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）

役割：CSMS技術専門部会で作成されたCSMS認証・認定基準、ユーザーズガイドを承認し、CSMSパイロット認定・認証制度の制度運用について諮問し、パイロット事業成果を踏まえて制度開始を承認する。

制御システムセキュリティにおける脆弱性対策

情報セキュリティ早期警戒パートナーシップ



※JPCERT/CC：一般社団法人 JPCERT コーディネーションセンター、産総研：独立行政法人 産業技術総合研究所

【期待効果】

①製品開発者及びウェブサイト運営者による脆弱性対策を促進
②脆弱性関連情報の放置・危険な公表を抑制
③個人情報等重要情報の流出や重要システムの停止を予防

脆弱性関連情報の届出件数

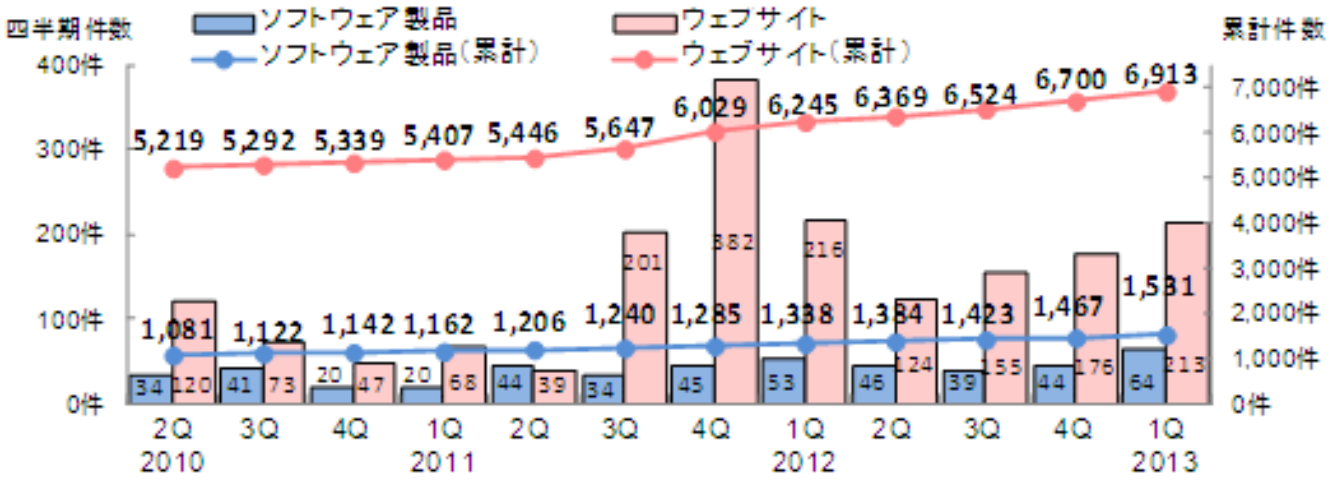


図 1−1. 脆弱性関連情報の届出件数の四半期別推移

表 1−2. 届出件数（過去 3 年間）

	2010 2Q	3Q	4Q	2011 1Q	2Q	3Q	4Q	2012 1Q	2Q	3Q	4Q	2013 1Q
累計届出件数[件]	6,300	6,414	6,481	6,569	6,652	6,887	7,314	7,583	7,753	7,947	8,167	8,444
1就業日あたり[件/日]	4.32	4.22	4.10	4.01	3.92	3.91	4.01	4.03	3.99	3.96	3.95	3.97

制御システムセキュリティの早期警戒パートナーシップ

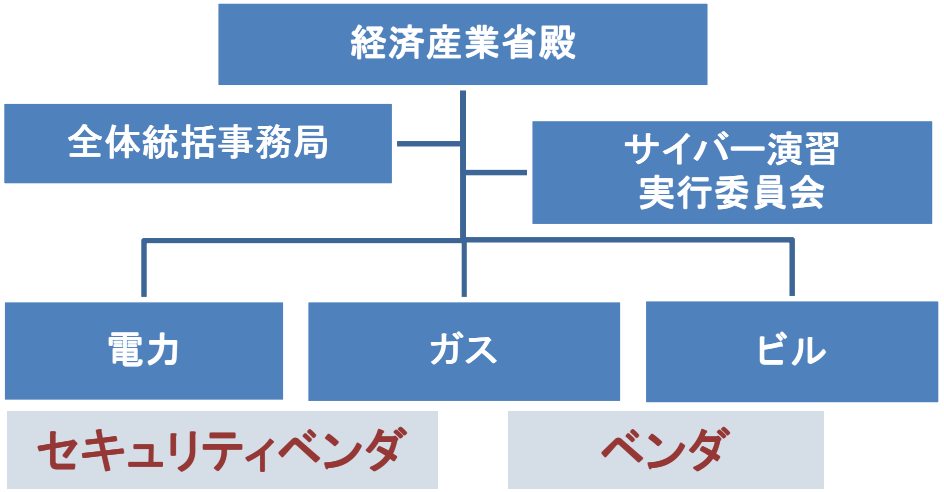
- 経済産業省、IPA、JPCERT/CCを中心に、CSSCおよび制御システム関係者とともに、制御システムにおける脆弱性対応を検討中
  - 告示およびガイドラインへの反映に関して、制御システム関係者の意見を聞きつつ検討
  - 制御システム用製品の脆弱性情報の取扱に関する研究会

制御システムにおける
サイバー演習

平成24年度経済産業省サイバーセキュリティ演習

制御システムを対象	模擬システムを構築	本格的な機能演習を実施
■セキュリティ対策の必要性が増している制御システムを対象 ■制御システムの関係者（今年度は電力、ガス、ビル）の協力を得て実施	■継続的に利用可能な模擬システムを構築 ■初年度は、模擬システムを用いて脅威と対策の体感を通じて課題を抽出 ■次年度以降は、CSSC東北多賀城技術研究センターに移設して運用	■模擬システムを用いた制御システムセキュリティにおける対策実装の課題抽出 ■攻撃守備演習による課題抽出

平成24年度サイバーセキュリティ演習の実施体制



各組織の役割分担	
経済産業省	• 意思決定
全体統括事務局	• 全体スケジュール調整 • 全体進捗管理 • 脅威特定 • 報告書とりまとめ
各分野 （各分野毎に事務局を設置、以下分野事務局）	• シナリオ作成 • 演習実施方法検討 • 演習実施 • 報告書作成

分野	関係者と役割
電力	業界団体（電力業界窓口）、電力事業者（演習主体）、日立製作所（模擬システム構築）、三菱総合研究所（事務局）
ガス	業界団体（ガス業界窓口）、ガス事業者（演習主体）、アズビル（模擬システム構築）、セキュリティベンダ（事務局）
ビル	ビル事業者等（演習主体・模擬システム構築）、学識経験者（模擬攻撃者）、三菱総合研究所（事務局）
全体統括事務局	三菱総合研究所

サイバーセキュリティ演習の成果

- 各分野関係者における制御システムセキュリティに係わる意識啓発
- 今後の制御分野のサイバー演習のインフラとなる模擬システムの構築
- サイバー演習のためのコンテンツ作成

CSSCへの期待

CSSCへの期待

- 製造業の中核となる制御システムの競争力の厳選であるセキュリティ機能の強化
- セキュリティ機能の強化のために評価認証、脆弱性対応、サイバー演習（普及啓発・人材育成）、研究開発の推進
- 上記を通した東北と多賀城における復興への貢献

以上