（JSSM公開討論会）

情報セキュリティの「実効性あるガバナンス」は可能か？

2008年2月24日

林　紘一郎 Ph.D., LL.D.
情報セキュリティ大学院大学　副学長・教授

Institute of Information Security
14-1, 2 chome, Tsuruya-cho, Kanagawa-ku,
Yokohama, JAPAN
e-mail hayashi@iisec.ac.jp
URL http://lab.iisec.ac.jp

問題意識として

責任の希釈化と厳罰化

← 希釈化

・法的責任を問われる
取締役・監査役は稀

・法的責任を問われる
監査法人・公認会計士も稀

・法的責任を問われる公務員も稀

・個人情報漏洩で損害賠償訴訟に
いたるのは稀、賠償額も少額

→ 厳罰化

・情報漏洩に対する
マスコミのパッシング

・企業不祥事に対する
一般の過剰な反応

・漏洩を起した個人や
下請けに対する厳しい懲戒

・中には損害賠償額を
予定した契約も

情報資産の法的保護の類型
（有体物に体現されない場合）

	公開情報		非公開（秘匿）情報
法人等に帰属する情報	特許発明	著作物	営業秘密に係る情報 通信の秘密に係る情報
個人に帰属する情報	特許発明	個人情報	営業秘密に係る情報 通信の秘密に係る情報 プライバシーに係る情報

出典：林・鈴木[2008]

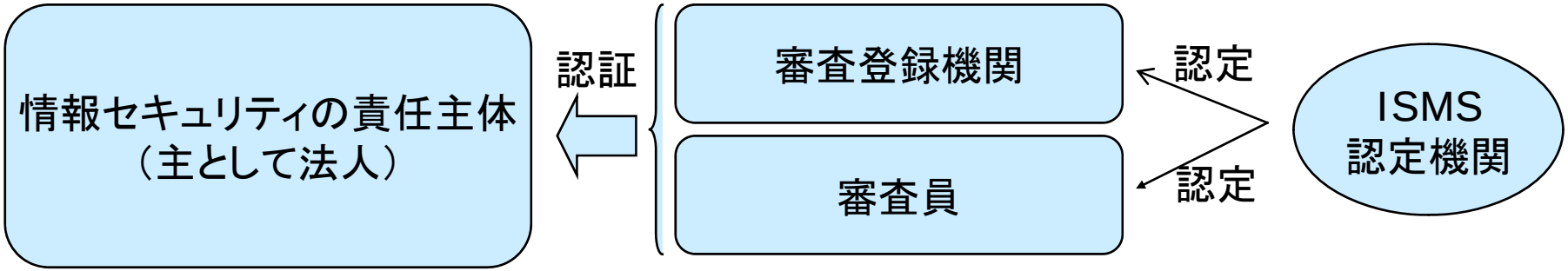
ISMSとは何か？

- 品質管理を「モノ」から「サービス」へ、さらには「経営」へと適用範囲を拡大していこうとする**運動論**
- 最終製品ではなく、そのプロセスを制御することで、「目に見えない」品質を担保する**仕組み**
- 前項を実効性あらしめるため、国際的な標準的枠組みを用意する**制度**（グローバル・スタンダード）
- 法的な効力とは切り離し、民間ベースのデ・ファクト標準を志向する**制度間競争**

ISMSの規範力（秘密の保護という観点から）

原子力安全基準	比較項目	ISMS
原子力基本法	基本法	なし
情報セキュリティ関連では、核原料物質、核燃料物質及び原子炉の規制に関する法律	根拠法	（JISになっている範囲で工業標準化法）
防護対象特定核燃料物質の輸送に係る核物質防護に関する情報の取扱いについて	政・省令	（個人情報保護法のガイドラインに組み込まれた範囲で省令と同等）
1年以下の懲役若しくは100万円以下の罰金に処し、又はこれを併科する	違反に対する罰則	特になし （個人情報保護法の間接罰）
「原子力事業者等」 製錬事業者、加工事業者、原子炉設置者、外国原子力船運航者、使用済燃料貯蔵事業者、再処理事業者、廃棄事業者及び使用者	適用される事業者	適用事業者は広く一般企業全体
原子炉の設置、運転等に関する規制	許認可	許認可とは無関係

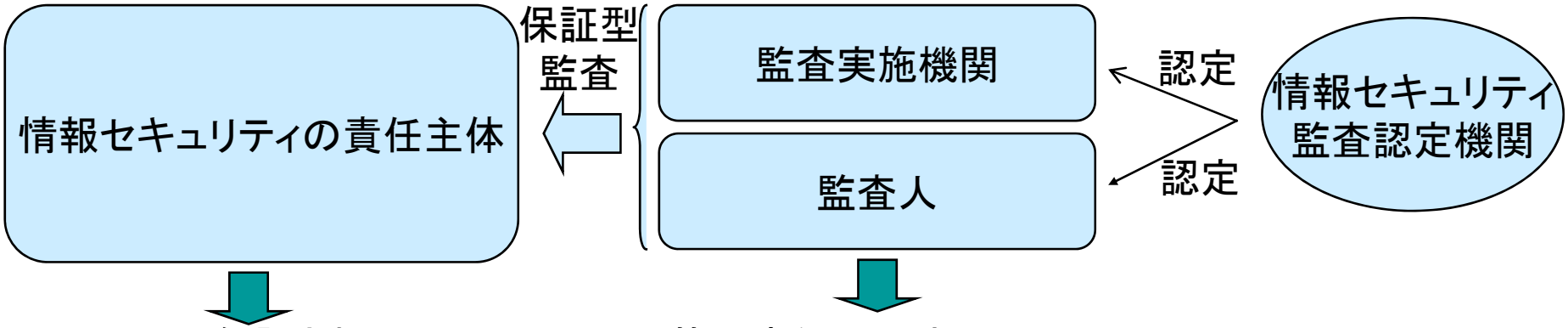
コミットメント責任の原点



Plan-Do-Check-Act
のうち主としてP-D

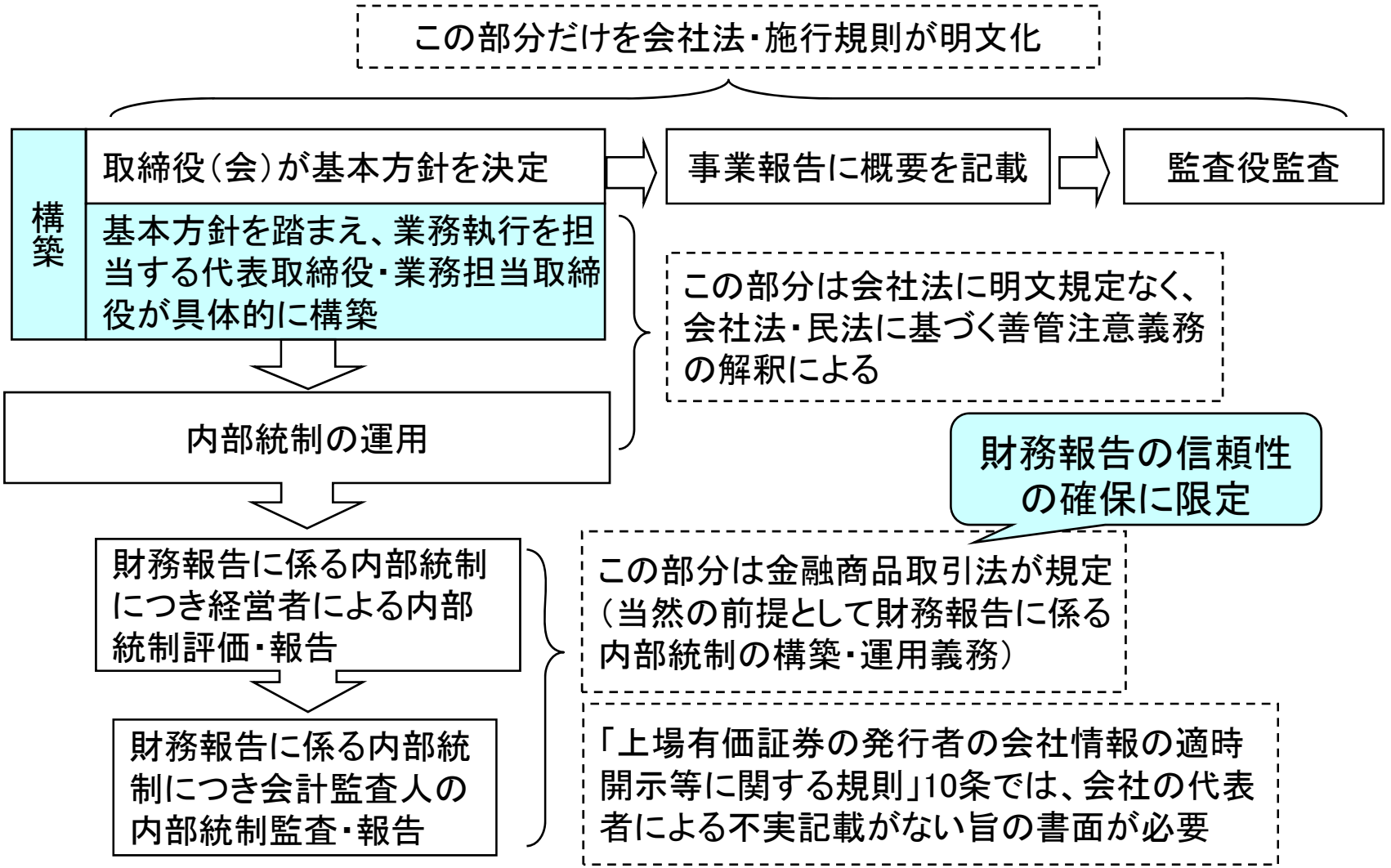
実際にはつながっていない

（Checkの実施後ー将来的には情報セキュリティ会計報告書に対して）



保証された（した）レベルの管理責任の発生

内部統制とコミットメント責任？



出典：岡村久道『内部統制―会社法と金融商品取引法』（富士通総研特別企画カンファレンス「内部統制とIT」2006.9.28.）に一部加筆

「賞味期限」というコミットメント

平成20年 1月1日 火曜日 朝日新聞

信 偽 模 正 造 作 誤 真 偽 造 歴 正 似

ニセモノ社会 真 1

鹿児島県霧島市内で食品会社を営んできた木吉純孝さん(68)は、苦い思いで新年を迎えた。

創業70年、「鹿児島漬物」の2代目社長だったが昨秋、産地を偽っていたことが発覚した。たくあんなど漬物に中国産の大根を使いながら「鹿児島産」と表示していた。

中国産の大根を扱い始めたのは十数年前。名古屋のスーパーからの依頼で始めた。「産地・中国」と表示していた。

ところが06年春ごろから、「中国産」の食品は敬遠されるようになった。在庫を抱えても、工場には契約通り、中国産大根800㌧入りの木箱が次々と運び込まれた。それから2カ月ともたずに倒産した。

「偽装している間はびくびくして不安で仕方がなかった。本当は全部しっかりと鹿児島産でやればよかった。でもお金もなかったし、調達もできない。最初はだます気などなかったのに」

「つけ込みの容器の後ろに、まるで隠すようにして置かれていた」と、元従業員は説明した。

「仕入れた物を全部捨てるわけにもいかない。会社がつぶれちゃうから。良心の呵責はあったけど、お金にしなければとやってしまった」。社長は悔いを口にした。

「中国産大根が鹿児島産か、漬物で見極めることは到底むり。消費者は素人だけど、こっちは曲がりなりにも玄人ですから。結局は売り手のモラルが問われる」

1年前とは違って人影の絶えた工場には、まだ漬物のにおいが濃く立ちこめていた。

食品偽装が起きているのは日本だけではない。

モスクワでは昨秋、野良犬の肉を「羊の肉」と偽っていた中華料理店が警察に摘発された。まさに「羊頭狗肉」だ。

昨年春れ、記者が訪ね

値段も同じ 本物の食品と見まがう食品サンプル。かつてはろうで作られていたが、今は塩化ビニルや合成樹脂製が多い。業界大手「まいづる」によると、最も高価なのは10㌔を超えるマグロの切り身で29万4千円。「本物のマグロと同じ値段」という。飲食業界のほか、神社や寺院、画家も顧客だという＝東京都台東区で、江口和裕撮影

あふれる裏切りの味

食の偽装が次々に発覚するのはなぜか。経済評論家江坂彰さん(71)は「最高の時期に食べたい」と賞味期限にこだわる消費者心理と、「少しでも利益を上げようとメーカーの思惑が期限の偽装を生んだ」とみる。鮮さを強調したい

偽装や欠陥が明らかになった品々

食

- 北海道銘菓「白い恋人」
- 伊勢名物「赤福餅」
- 名古屋コーチン

局の通知文が玄関扉に貼られていた。テーブルいすなどは片づけられ、店内は無人だった。

すぐそばで料理店を営む男性(40)は、「ロシアの人々にとって犬はペット。犬料理など受け入れられないのに。うちは生肩のお墨付きの肉や旬の幸しか使わない」と胸を張った。

中国・安徽省の高級

と、「営業していい」と手書きした行政

出典:『朝日新聞』2008年1月1日号

環境法からの教訓

- precautionary principle
  （事前抑止原則、予防原則と訳されることもある）

- adaptive　principle
  （化学者の中西準子さんが提唱する「順応的管理」という漸進的方法）

- pledge and review
  （地球温暖化枠組条約の交渉に際して、日本が提案した方法）

CIAでは不十分

- Confidentiality
- Integrity
- Availability

① Confidential でない情報資産の保護が不可欠
- 個人情報は保護と利用のバランスが重要だが、前者のみが強調されやすい。
- 知的財産は総じて「情報を公開しつつ権利は守る」もの。

② これらは情報セキュリティの目標ではあり得ても、実効性を担保するものではない。
- Plan-Do寄りでCheck-Actが薄い。
- 責任（あるいはsanction）の要素が必要。

PAIRS

- Proper Protection of Eligible Information
- Availability
- Integrity（含Authenticity）
- Risk Inclusion
- Sanction

- Plan-Do段階に焦点
- 情報の秘匿性のみならず利活用も視野に
- リスクへの対応を勘案
- 結果への対応を意識

MoRALE

- Monitoring
- Response
- Accountability
- Liability
- Externality and Learning

- Check-Act の段階に焦点
- 監査を重視
- 責任論を3分
  (Response/Accountability/Liability)
- 責任を問い難い部分を、とりあえず外部性とする

PAIRS-MoRALEの問題点（外延）

1. 情報サービスの品質そのものは問題にしなくて良いのか。
   - たとえばソフトウェア・バグを製造物責任法の対象にするなどの視点。
   - ISO9000/14000/27000と並べることができる（あるいはそのように位置づける）なら、品質管理は不可欠。
   - しかし安全対策とセキュリティ対策は別、との考えもあり得る。

2. ユニバーサル・アクセスは考慮しなくて良いか。
   - 情報化社会の大目標ではあっても、情報セキュリティの目標ではない？

3. Reliabilityは入っているのかいないのか。

4. COSOフレームワークにある「業務の効率化」を入れなくて良いのか。
   - 業務を遂行する以上、当然のことで省略して良い？

PAIRS-MoRALEの問題点（内包）

1. P （Proportion）の内容と妥当性
2. A の内容と妥当性
3. I の内容と妥当性
4. R (Risk) の内容と妥当性
5. S (Sanction) の内容と妥当性
6. Mo（Monitoring）の内容と妥当性
7. R (Response) の内容と妥当性
8. A (Accountability) の内容と妥当性
9. L (Liability) の内容と妥当性
10. E (Externality)の内容と妥当性

（蛇足）学会とは

- 学者相互の連絡、研究の促進、知識・情報の交換、学術の振興を図る協議などの事業を遂行するために組織する団体（『広辞苑』（第5版）2007年）

- 学問や研究の従事者らが、自己の研究成果を公開発表し、その科学的妥当性をオープンな場で検討論議する場である。また同時に、査読、研究発表会、講演会、学会誌、学術論文誌などの研究成果の発表の場を提供する業務や、研究者同士の交流などの役目も果たす機関でもある（『ウィキペディア（Wikipedia）』）

日本学術会議協力学術研究団体

「日本学術会議協力学術研究団体」は、日本学術会議と各団体との間で緊密な協力関係を持つことを目的とし、従来の登録学術研究団体及び広報協力学術研究団体に代わって、平成17年10月に設けられました（日本学術会議会則第34条）。日本学術会議からは、広報刊行物、ニュースメール等の配布・配信、会議の共催や後援などを行っています。

（注）日本学術会議協力学術研究団体としての要件

①学術研究の向上発達を図ることを主たる目的とし、かつその目的とする分野における学術研究団体として活動しているものであること、②研究者の自主的な集まりで、研究者自身の運営によるものであること、③「学術研究団体」の場合は、その構成員（個人会員）の数が100人以上であることです。

出典：http://www.scj.go.jp/ja/info/dantai/index.html