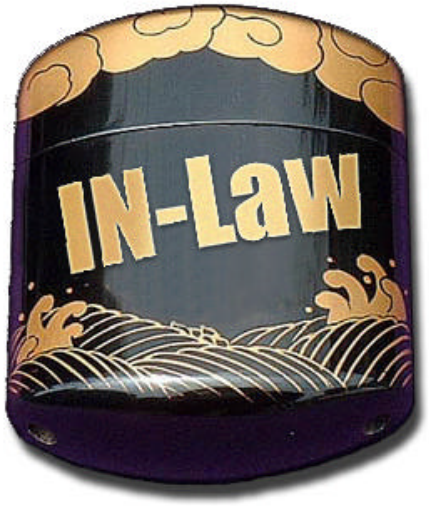
企業における
情報セキュリティリスクマネジメント



IN-Law
情報ネットワーク法学会
The Information Network Law Association
佐藤　慶浩

講演者

佐藤　慶浩　　(さとう　よしひろ)

情報ネットワーク法学会　セキュリティ技術研究部会　部会長

日本ヒューレット・パッカード株式会社　個人情報保護対策室　室長
現在、内閣官房情報セキュリティセンター内閣参事官補佐を併任。

その他に、27000シリーズなどを規格するISO/IEC JTC1/SC27委員会の国際委員、国内ISMS認証の技術専門部会委員、プライバシーマーク認証の判定委員を務めている。

詳細は、http://yosihiro.com/profile/　に掲載。

講演内容

- リスクマネジメントとは
- リスクマネジメントと業務の関係
- リスクマネジメントの集中管理
- リスクマネジメントとしての情報セキュリティ
- 情報セキュリティの傾向と課題

- すぐに使える推奨資料

リスクマネジメントとは？

資産
assets

脅威
threat

脆弱性
vulnerability

分析
analysis

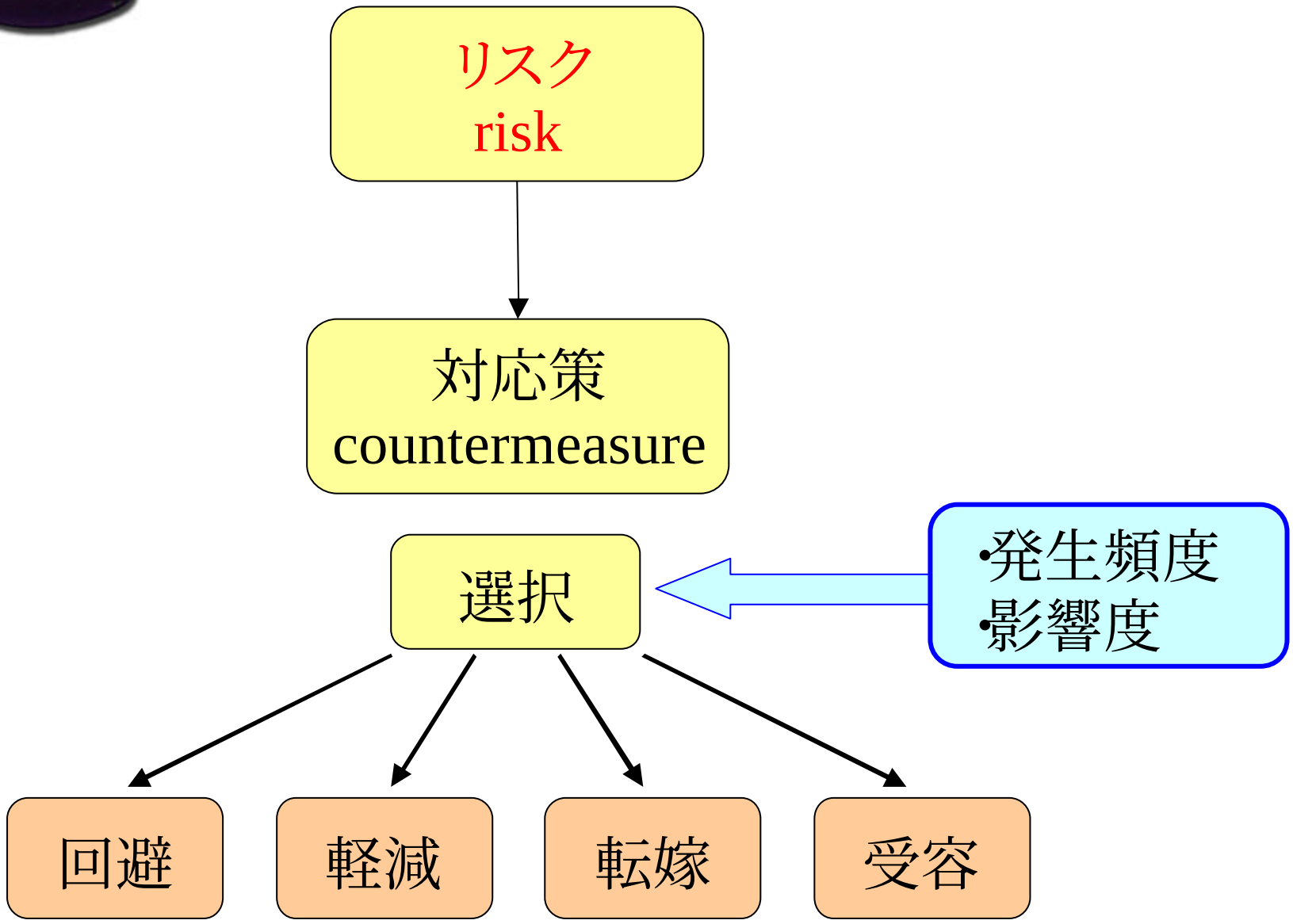
リスク
risk

マネジメント
management

対応策
countermeasure

出典：CRAMM(CCTA Risk Analysis and Management Method)

リスクマネジメントとは？



リスクマネジメントと業務の関係

脅威と脆弱性によりリスクが生まれる

脅威や脆弱性を生じる事象の分類：

- 業務によらない事象
  - 人為的な事象　→無許可のアクセス・・・
  - 人為的ではない事象　→自然災害・・・
- 業務による事象
  - 業務の不作為による事象　→注意不足・・・
  - 業務の作為による事象　→故意、過失・・・

リスクマネジメントと業務の関係

・業務の作為による事象」以外は、
　リスク対応策は、本来業務と独立又は区別できるリスク対応業務となる。

・業務の作為による事象」は、
　リスク対応策は、業務そのものに内在する。
　当該業務手順が標準化されていれば、その標準にリスク対応策を適用することができる。・・・はず。

リスクマネジメントと業務の関係

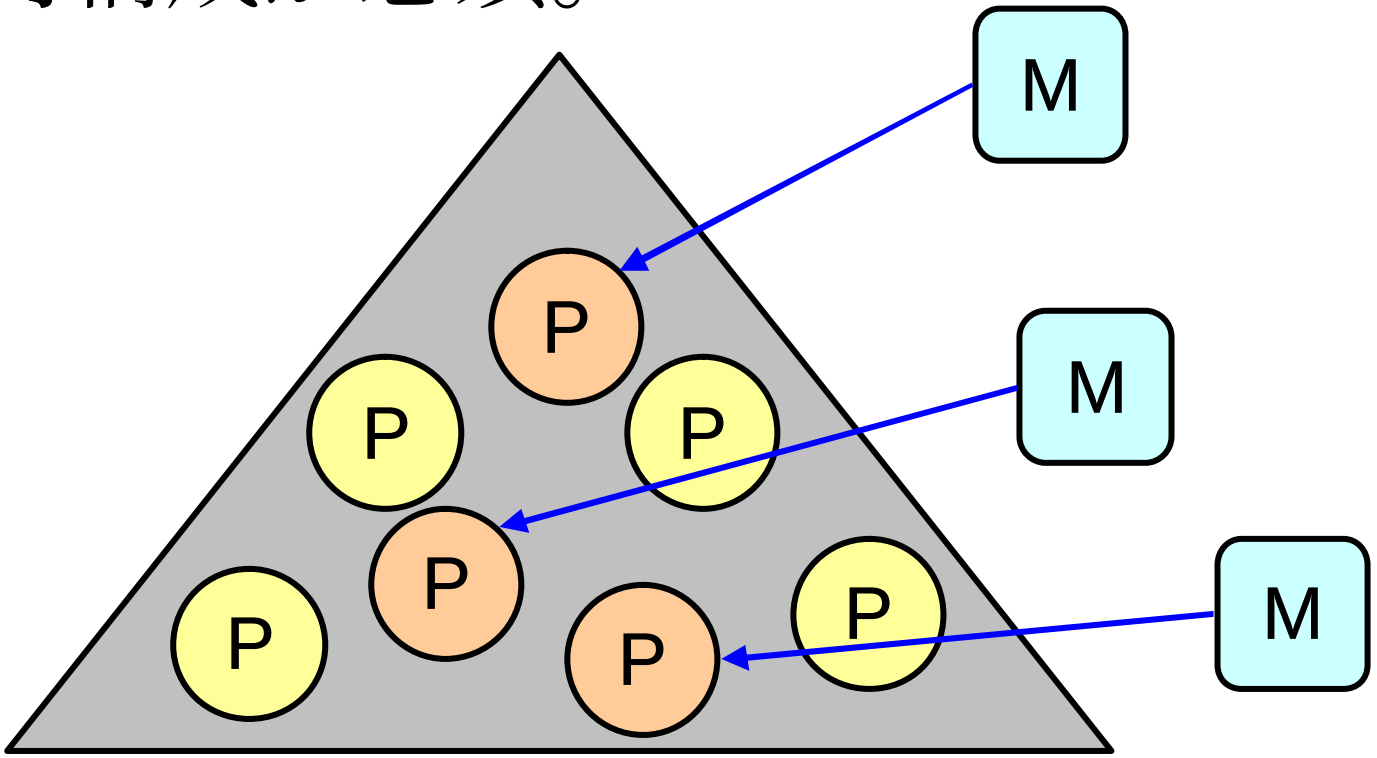
当該業務手順が標準化されていれば、その標準にリスク対応策を適用することができる。・・・はず。

一方で、非標準化手順、すなわち、裁量業務については、リスクマネジメントの集約が困難である。と考えるべき。

なぜなら、手順を裁量しているのが業務担当者である限り、業務担当者がリスクの分析やリスク対応策の選択をする部分があるため。

リスクマネジメント
集中管理できるのか？

マネジメントのプロセスを集約化することは可能。
マネジメントするプロセスを集約化することは、
プロセス再構成が必須。



リスクマネジメント
リスクは細部に宿りたもう

■リスクマネジメントの手続きを一元化しつつ、分析と判断を現場に任せることは現実的であると考えられる。

□判断基準の標準化を志してもよいが慎重にすべき。その場合、例外承認手続きとともに導入するのがよい。
□判断基準の標準化を現場が要望するのは注意信号である。

リスクマネジメント

JIS Q 2001「リスクマネジメントシステム構築のための指針」より

発生場所、原因、損害を受ける対象などによってリスクをグループとして扱うことが適切と判断できる場合には、そのグループごとに部門、部署、委員会などの形式でリスクマネジメントシステム担当者を定めてもよい。」

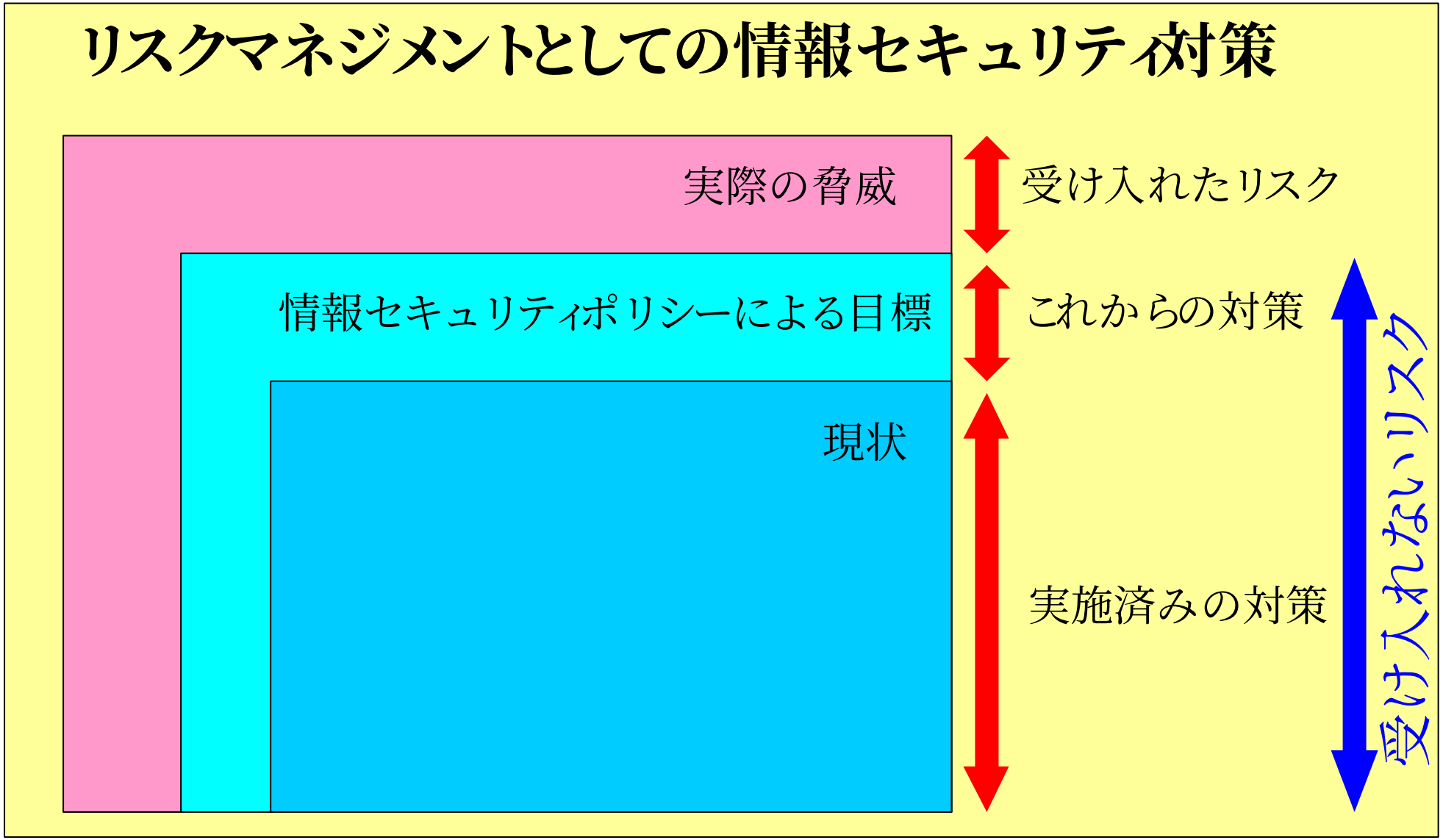
拙著 参考記事：

翔泳社Webサイト IT Compliance Web 内部統制と情報セキュリティ

リスクは集中管理できるのか　～企業における法対応とITのバランス～

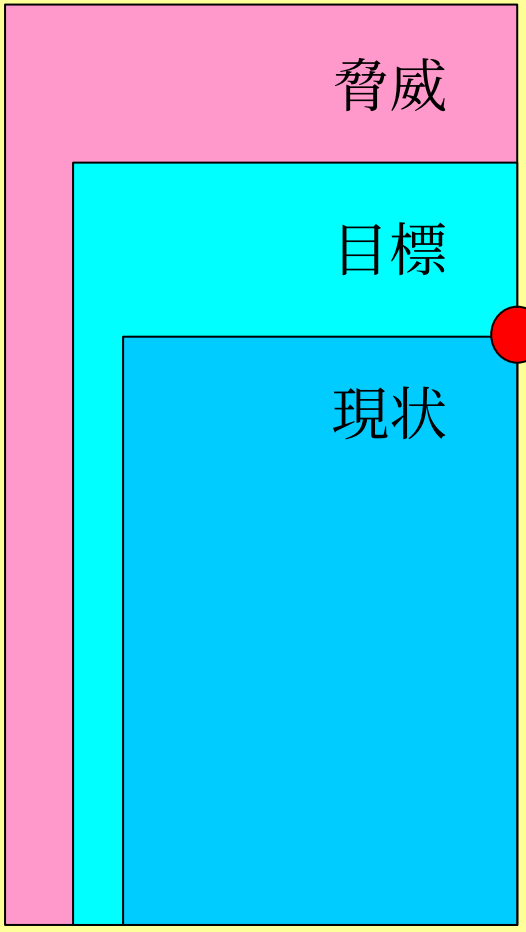
http://www.itcomp.jp/a/article.aspx?aid=153

リスクマネジメントとしての情報セキュリティ対策



最低基準ではなく適正基準
何ができるかより、何をしないか」

リスクマネジメントとしての情報セキュリティ対策



?

チャンスとリスクの トレードオフ

変化＝チャンス＋リスク

柔軟性のある作業手順　業務）

非正社員との協業　人）

インターネット接続　技術）

情報セキュリティ
従来の傾向

情報セキュリティとは、機密性、完全性、可用性を確保すること。

機密性 C: Confidentiality
完全性 I: Integrity
可用性 A: Availability

■従来の情報セキュリティ対策は、C:機密性に偏っている傾向がある。

情報セキュリティ
今後の方向性

CIAからAICへ

□実際には、Cに加えて+Iさらに+A

□しかし、CとIとAの要求が相反する場合にトレードオフを図る必要に迫られる。

□情報セキュリティを直接トレードオフすることはできない。リスクのトレードオフとなる。

■情報セキュリティマネジメントシステムにおいては、+I&+Aによって、対策そのものに加えてリスク評価が重要になる。

情報セキュリティ再確認すべき事項

■委託先における情報セキュリティマネジメントシステムについて、リスクマネジメントの視点で再確認することが重要である。

□委託先におけるISMS認証の取得を義務付けることの意味。

講演内容

- リスクマネジメントとは
- リスクマネジメントと業務の関係
  - 非標準手順による業務
- リスクマネジメントの集中管理
  - リスクは細部に宿りたもう
- リスクマネジメントとしての情報セキュリティ
  - 最低基準ではなく適正基準
- 情報セキュリティの傾向と課題
  - ＣＩＡからＡＣＥへ
  - 委託先におけるマネジメント

すぐに使える推奨資料

「先進企業から学ぶ事業リスクマネジメント実践テキスト」
平成17年3月　経済産業省
（事業リスク評価・管理人材育成システム開発事業）

情報セキュリティに限らない、企業におけるリスクマネジメント全般について検討すべきことを紹介している。
300ページと分量が多いが、図を多用し、企業事例にも具体的にふれてわかりやすく解説しているため、読むのにストレスはない。

以下のWebから無償ダウンロード可能
http://www.meti.go.jp/policy/economic_industrial/report/downloadfiles/g50331i00j.pdf

すぐに使える推奨資料

先進企業から学ぶ事業リスクマネジメント実践テキスト」
平成17年3月　経済産業省
（事業リスク評価・管理人材育成システム開発事業）

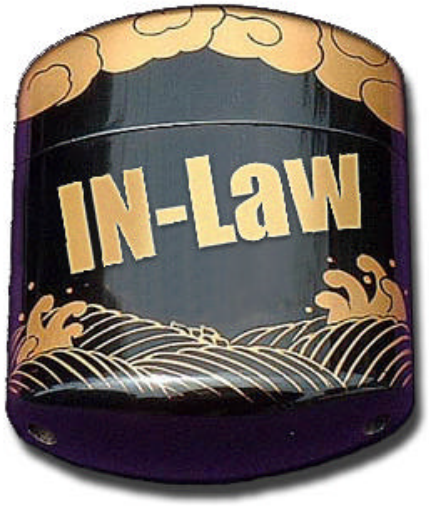
目次

1. リスクマネジメントとは
2. 事業リスクマネジメントシステム構築及び維持のための体制
3. リスクマネジメント方針
4. リスクマネジメント計画の策定
5. リスクマネジメントの実施
6. リスクマネジメントシステムに関する評価、是正・改善

情報ネットワーク法学会

http://in-law.jp/

随時、入会受付中



発表資料のダウンロード

http://yosihiro.com/go/2008-02-21-inlaw