重要インフラ事業者向け情報セキュリティセミナー

IT障害に対して配慮すべき法的事項

内部統制と責任論からみた「重要インフラの情報セキュリティ対策に係る基本的考え方」

独立行政法人 情報処理推進機構 (IPA)
有限責任中間法人 JPCERT コーディネーションセンター
(JPCERT/CC)

稲垣隆一法律事務所

弁護士 稲 垣 隆 一

IT障害に関連する事件　何が起きているのか

- 航空
  - 2003年3月21日　ANAシステムダウンにより羽田始発から発着遅れ150便欠航300便遅れ。１０万2000人に影響
  - 2006年2月17日　国土交通省東京航空管制部　フライトプラン転送システムがダウン。羽田、成田、中部、関西などへのフライトプランの転送不能。7分間で復旧し、ダイヤへの影響なし。
  - 2006年1月3日　日本航空運行管理システムＪＡＬＦＯＳがダウン。出発便の重量･重心の自動計算不能に。国内線９便，国際線１便が最大53分遅れ，２２００人に影響。
- 通信
  - 2005年10月13日　兵庫県西宮市の加入電話の電話番号が1日近く入れ替わる事故。
  - 2005年11月2日　ドリーム･トレイン･インターネット（東電系IP電話グループ）のプロバイダ統合に際してのシステムトラブルで，電話回線業者に契約者のデータ送信不能に。新規契約者８００件に影響。
- 証券
  - 2003年10月3日　東証システム障害　1128株のみずほファイナングループ株の売り注文に対して買い注文がないのに取引を誤って成立させ，約定代金3億3千万円を支払い。
- 金融
  - 2002年　みずほシステム統合に伴うＡＴＭ障害。振込不能による代金回収の遅れ，再請求費用などの賠償請求（東京都水道局　１６９７万円、ＮＴＴ東日本、西日本、ＮＴＴドコモ、ＮＴＴコミニュケーション合計約2億７０００万円、東京電力５０００万円。九州電力６００万円などが報じられている）
  - 2006年1月　三菱東京ＵＦＵ銀行　システム統合検査間に合わず合併御業務開始期日を延期。
  - 2005年　富士火災海上保険会社　プログラムの欠陥やチェックシステムの不備のため過去3年間に4827件合計約1億2914万円の保険金不払発生。過去６年ないし９年間に約２５万件４１９４万円の保険料を違法徴収
  - 2005年10月７日　ソニー生命02年における変額保険，変額個人年金保険の解約返戻金，積立金計算プログラムの修正時のミスにより，過去3年間に解約返戻1119件約144万円の支払い不足。
- 首都高
  - 2006年１月12日午後８時から８時間首都高ＥＴＣに障害。約６万台に影響。時間帯割引が不能となったため、希望者からの料金後払いで対応。
- 損害賠償約款
  - 独立行政法人通関情報処理センター　「システム障害に係る利用者への損害賠償について」‥‥連続してシステム全部停止の障害が発生した場合、センターは臨時開設手数料のうち利用者の申請に基づきセンターが認定した損害を賠償する。（http://www.naccs.go.jp/unkyou/unkyou/29data/songaibaisho.pdf）

重要インフラ　IT障害の際の法的根拠は何か

- 責任を負う相手との主たる法律関係
  - 商品市場
    - 大規模取引先･･･個別契約
    - 大衆取引先･････約款契約
    - 不法行為法制
    - 会社法
  - 株式市場
    - 会社法
    - 証取法
    - 証券市場のルール
  - 株主･その他の利害関係者
    - 会社法･不法行為法
  - 社会･国
    - 事業法
    - その他の項法的規制

- 責任の根拠
  - なすべきことをなしていたか

IT障害防止のために「なすべきこと」をどう把握するのか

内部統制　大和銀行代表訴訟事件判決(平成12年9月20日大阪地方裁判所判決)

■　**リスク管理体制＝内部統制の整備が必要**

「健全な会社経営を行うためには、目的とする事業の種類、性質等に応じて生じる各種のリスク･･･の状況を正確に把握し、適切に制御すること、すなわちリスク管理が欠かせず、会社が営む事業の規模、特性等に応じたリスク管理体制（いわゆる内部統制システム）を整備することを要する。」

■　**リスク管理体制＝内部統制の大綱決定は取締役会の職務**

「重要な業務執行については、取締役会が決定することを要する（商法二六〇条二項）から、会社経営の根幹に係わるリスク管理体制の大綱は、取締役会で決定することを要し、業務執行を担当する代表取締役及び業務担当取締役は、大綱を踏まえ、担当する部門におけるリスク管理体制を具体的に決定するべき職務を負う。

■　**リスク管理体制＝内部統制の構築は取締役の善管義務の内容をなす**

取締役は、取締役会の構成員として、また、代表取締役又は業務担当取締役として、リスク管理体制を構築すべき義務を負い、さらに代表取締役及び業務担当取締役がリスク管理体制を構築すべき義務を履行しているか否かを監視する義務を負うのであり、これもまた、取締役としての善管注意義務及び忠実義務の内容をなすものと言うべきである。

■　**取締役のリスク管理体制の整備は監査役によって監査される**

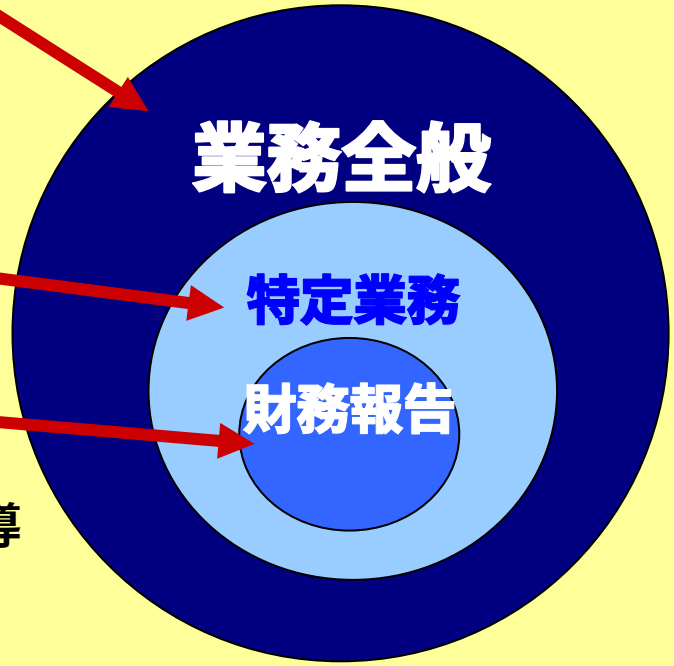
監査役は、商法特例法二二条一項の適用を受ける小会社を除き、業務監査の職責を担っているから、取締役がリスク管理体制の整備を行っているか否かを監査すべき職務を負うのであり、これもまた、監査役としての善管意義務の内容をなすものと言うべきである

大和銀行事件　リスク管理体制とコンプライアンス体制整備

- 問われているのは、主として、被告らのうち、大和銀行の代表取締役･･･及び取締役在任中にニューヨーク支店長の地位にあった者が、同支店における財務省証券取引及びカストディ業務に内在する、･･･事務リスクを適切に管理する仕組み、すなわちリスク管理体制を整備していたか否か、また、その余の被告らに、取締役又は監査役としての監視義務違反又は監査義務違反が認められるか否かである。
- ところで、取締役は、自ら法令を遵守するだけでは十分でなく、従業員が会社の業務を遂行する際に違法な行為に及ぶことを未然に防止し、会社全体として法令遵守経営を実現しなければならない。
- しかるに、事業規模が大きく、従業員も多数である会社においては、効率的な経営を行うため、組織を多数の部門、部署等に分化し、権限を部門、部署等の長、さらにはその部下へ委譲せざるを得ず、取締役が直接全ての従業員を指導･監督することは、不適当であるだけでなく、不可能である。
- そこで、取締役は、従業員が職務を遂行する際違法な行為に及ぶことを未然に防止するための法令遵守体制を確立するべき義務があり、これもまた、取締役の善管注意義務及び忠実義務の内容をなすものと言うべきである。
- この意味において、**事務リスクの管理体制の整備は、同時に法令遵守体制の整備を意味する**ことになる。

内部統制　対象領域に応じて基準はさまざま

- 業務･財務･コンプライアンス情報など
  - 会社法
  - 監査役監査基準
  - その他のガイドライン･指針
- 特定業務情報など
  - 業務検査基準
- 財務報告･会計情報など
  - 証取法･企業内容等の開示に関する内閣府令
  - 有価証券報告書の提出に関する財務局の指導
  - 証券市場による誘導
    - 「適時適切な情報開示に関する宣誓」
    - 「有価証券報告書等の適正性に関する確認書」
  - 会計監査基準
  - Ｊ－Ｓｏｘ



新会社法の内部統制の内容は何か

基本方針の決定と整備　　内部統制システムの整備は取締役会・取締役の責務

取締役会非設置会社

第三百四十八条　取締役は、定款に別段の定めがある場合を除き、株式会社（取締役会設置会社を除く。以下この条において同じ。）の業務を執行する。

2　取締役が二人以上ある場合には、株式会社の業務は、定款に別段の定めがある場合を除き、取締役の過半数をもって決する。

3　前項の場合は、次に掲げる事項についての決定を各取締役に委任することができない

四　取締役の職務の執行が法令及び定款に適合することを確保するための体制その他株式会社の業務の適正を確保するために必要なものとして法務省令で定める体制の整備

取締役会設置会社

第三百六十二条

2　取締役会は、次に掲げる職務を行う。

一　取締役会設置会社の業務執行の決定

4　取締役会は、次に掲げる事項その他の重要な業務執行の決定を取締役に委任することができない。

六　取締役の職務の執行が法令及び定款に適合することを確保するための体制その他株式会社の業務の適正を確保するために必要なものとして法務省令で定める体制の整備

委員会設置会社

第四百十六条　委員会設置会社の取締役会は、第三百六十二条の規定にかかわらず、次に掲げる職務を行う。

一　次に掲げる事項その他委員会設置会社の業務執行の決定

ロ　監査委員会の職務の執行のため必要なものとして法務省令で定める事項

ホ　執行役の職務の執行が法令及び定款に適合することを確保するための体制その他株式会社の業務の適正を確保するために必要なものとして法務省令で定める体制の整備

大会社

第三百四十八条　4　大会社においては、取締役は、前項第四号に掲げる事項で定める体制の整備）を決定しなければならない。

大会社

第三百六十二条　5　大会社である取締役会設置会社においては、取締役会は、前項第六号に掲げる事項を決定しなければならない。

第四百十六条

2　委員会設置会社の取締役会は、前項第一号イからホまでに掲げる事項を決定しなければならない。

監査　　取締役による内部統制システムの整備は監査役によって監査される

■ 監査役設置会社、会計監査人設置会社の監査役は、事業報告に内部統制の基本方針の決定・内部統制整備の決議が記載されているときは、定款で監査役の監査権限を会計に限定しているときをのぞき、、その事項の内容が相当でないと認めるときはその旨と理由を監査報告書に記載(第四百三十六条1項、2項、施行規則第百二十九条1項五号、2項)。取締役会ではこれらの監査を受けたものは取締役会の承認を得なければならない(法第四百三十六条3項)

事業報告による開示　　内部統制システムは株主・会社債権者に開示・報告される

■ 内部統制の基本方針の決定・内部統制整備の決議は事業報告書に記載(第四三五条2項、施行規則百十八条2号)

■ 事業報告及び事業報告に係る監査役(監査役会設置会社の監査役会委員会設置会社では監査委員会)の監査報告における監査報告の意見)は招集通知に添付、本店・支店への備置などの方法により株主・会社債権者及び親会社社員に開示する(法第四百三十七条、施行規則第四款、第百三十三条以下、法第四百四十二条)

新会社法の内部統制　具体的には　施行規則98条

整備すべき内部統制システムとは

法第三百四十八条第三項第四号に規定する法務省令で定める体制は、次に掲げる体制とする。

一取締役の職務の執行に係る情報の保存及び管理に関する体制

二損失の危険の管理に関する規程その他の体制

三取締役の職務の執行が効率的に行われることを確保するための体制

四使用人の職務の執行が法令及び定款に適合することを確保するための体制

五当該株式会社並びにその親会社及び子会社から成る企業集団における業務の適正を確保するための体制

2 取締役が二人以上ある株式会社である場合には、前項に規定する体制には、業務の決定が適正に行われることを確保するための体制を含むものとする。

3 監査役設置会社以外の株式会社である場合には、第一項に規定する体制には、取締役が株主に報告すべき事項の報告をするための体制を含むものとする。

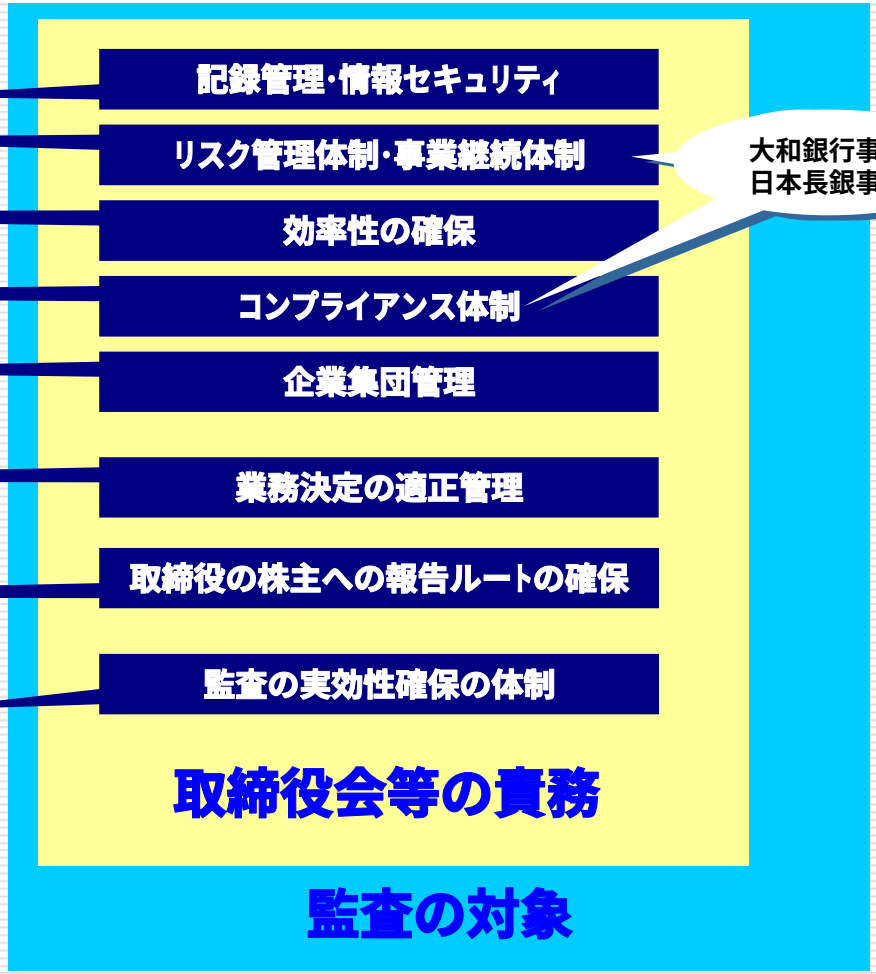
4 監査役設置会社（監査役の監査の範囲を会計に関するものに限定する旨の定款の定めがある株式会社を含む。）である場合には、第一項に規定する体制には、次に掲げる体制を含むものとする。

一監査役がその職務を補助すべき使用人を置くことを求めた場合における当該使用人に関する事項

二前号の使用人の取締役からの独立性に関する事項

三取締役及び使用人が監査役に報告をするための体制その他の監査役への報告に関する体制

四その他監査役の監査が実効的に行われることを確保するための体制



内部統制はどのようにして整備するのか
大和銀行代表訴訟判決(平成12年9月20日大阪地方裁判所判決)

行為のときを基準として判断
整備すべき内部統制の内容については経営裁量が認められる。

- **行為の時を基準に判断する**
  - 整備すべきリスク管理体制の内容は、リスクが現実化して惹起する様々な事件事故の経験の蓄積とリスク管理に関する研究の進展により、充実していくものである。 したがって、・・・現時点で求められているリスク管理体制の水準をもって、本件の判断基準とすることは相当でない

- **内部統制の内容の選択には経営裁量が認められる**
  - どのような内容のリスク管理体制を整備すべきかは経営判断の問題で・・会社経営の専門家である取締役に、広い裁量が与えられていることに留意しなければならない。

裁量権の逸脱　判断の指標は何か
日本長期信用銀行プロジェクト融資事件判決(平成１４年４月２５日東京地裁判決)

適切な事実認識と判断の推論過程･判断内容の合理性がポイント

- **取締役の判断に許容された裁量の範囲を超えた善管注意義務違反があるとするためには**
  - 判断の前提となった事実の認識に不注意な誤りがあったか否か、又は判断の過程･内容が取締役として著しく不合理なものであったか否か、すなわち、当該判断をするために当時の状況に照らして合理的と考えられる情報収集･分析、検討がなされたか否か、これらを前提とする判断の推論過程及び内容が明らかに不合理なものであったか否かが問われなければならない。

大和銀行代表訴訟事件判決にみる内部統制の整備

脅威とリスクの把握

- 財務省証券取引には、取引担当者が自己又は第三者の利益を図るため、その権限を濫用する誘惑に陥る危険性があるだけでなく価格変動リスク（市場リスク）が現実化して損失が生じた場合に、その隠ぺいを図ったり、その後の取引で挽回をねらいかえって損失を拡大させる危険性（事務リスク）を抱えている。また、カストディ業務には、保管担当者が自己又は第三者の利益を図って保管物を無断で売却して代金を流用する等、権限を濫用する危険性（事務リスク）が内在している。

リスク対処方針決定
最小限に食い止める

- 「このような不正行為を未然に防止し、損失の発生及び拡大を最小限に止める」必要がある。
- 「そのリスクの状況を正確に認識・評価し、これを制御するため、様々な仕組みを組み合せてより効果的なリスク管理体制（内部統制システム）を構築する必要がある。」

「財務省証券の保管残高の確認は、カストディ業務に内在する事務リスクを適切に管理するため、最も基本的かつ効果的であり、欠くことのできない仕組みである。他にどのような仕組みを組み合せようとも、適切な残高確認を欠いたリスク管理体制は十全とは言い難い。」

「事務リスクを適切に管理するためには、預かり保管する証券の性質に応じた適切な方法によって保管残高を検査することが必要である。」

対処策の選択
リスク対処方針との合理的関連性が必要

- 「残高確認を行うに当たって、預かり保管する証券の性質に応じた適切な方法を採り、いわば現物確認を行うことが必要である。証券が発行されているのであれば、現金の残高を確認する際実際に現金を数えて帳簿上の金額と照合するように、証券の現物と帳簿上の記載とを突合することが必要であり、証券が発行されない登録債であり、かつ、バンカーズ・トラストにその保管を再委託している場合には、カストディ業務の担当者を介さず、直接バンカーズ・トラストに対して保管残高の照会を行うことが必要となる。

実行と責任

- にもかかわらず、ニューヨーク支店では、毎月の店内検査、随時実施されていた内部監査担当者による監査、二年に一回の臨店検査、米州企画室による検査、三年に一回の会計監査人による監査のいずれにおいても、検査対象であるニューヨーク支店あるいはカストディ係にバンカーズ・トラストから財務省証券の保管残高明細書を入手させ、その保管残高明細書と同支店の帳簿とを照合するという確認方法を採用していた。

そのため、井口に保管残高明細書を改ざんする機会を与える結果となり、本件無断売却及び虚偽のバンカーズ・トラストの保管残高明細書の作成及び虚偽の保管残高明細書のファクシミリ送信を発見、防止することができなかった。

大和銀行のリスク管理体制は、この点で、実質的に機能していなかったものと言わなければならない。

裁量権逸脱の判断　下部組織の検討への信頼が許される場合とは
日本長期信用銀行プロジェクト融資事件判決(平成１４年４月２５日東京地裁判決)

専門知識と能力ある職員が重畳的に情報収集･分析･検討を加える手続きの整備が必要

- **取締役の行なった情報収集･分析、検討などに不足や不備がなかったかどうかについては**
  - 分業と権限の委任により広汎かつ専門的な業務の効率的な遂行を可能とする大規模組織における意思決定の特質が考慮に入れられるべきであり
  - 下部組織が求める決裁について、意思決定権者が、自ら新たに情報を収集･分析し、その内容をはじめから検討し直すことは現実的でなく
  - 下部組織の行った情報収集･分析、検討を基礎として自らの判断を行なうことが許されるべきである。
- **特に、原告のように専門知識と能力を有する行員を配置し、融資に際して、営業部店、審査部、営業企画部などがそれぞれの立場から重畳的に情報収集、分析及び検討を加える手続が整備された大銀行においては、**
  - 取締役は、特段の事情のない限り、各部署において期待された水準の情報収集･分析、検討が誠実になされたとの前提に立って自らの意思決定をすることが許されるというべきである。
  - そして、上記のような組織における意思決定の在り方に照らすと、特段の事情の有無は、当該取締役の知識･経験･担当職務、案件との関わり等を前提に、当該状況に置かれた取締役がこれらに依拠して意思決定を行なうことに当然に躊躇を覚えるような不備･不足があったか否かにより判断すべきである。

重要インフラのIT障害に関する法的課題

- **法的責任の根拠はなにか**
  - 関係者の意思の自由の確保
  - 具体的には・・・・・想定した価値を想定したリスク内で得られること
  - 法的責任が発生するのは
    - 得られた価値が想定より低いとき
    - 現実化したリスクが想定より高いとき
  - 組織が関係者の意思の自由を確保するためになすべきことは
    - コンプライアンス
    - 情報開示
    - 確実な価値の移転と現実化したリスクの想定内への封じ込め
- **IT障害との関係における論点**
  - コンプライアンス
    - ルールの正統性をどう確保するか=どのような内容のルールを誰がどのようにして作るか
  - 情報開示
    - 開示すべき情報は何か、これを可能とする条件は何か、情報開示をどのようにして確保するか
  - 確実な値の移転と現実化したリスクの想定内への封じ込め
    - 事業継続のレベルをどう措定するか、事業継続をどのように確保するか

重要インフラのIT障害に関する法的課題

- **重要インフラの機能と特性**
  - 他に代替することが著しく困難なサービスを提供する事業
  - 国民生活及び社会経済活動の基盤
  - その機能が停止、低下又は利用不可能な状況に陥った場合に、我が国の国民生活または社会経済活動に多大なる影響を及ぼすおそれが生じる

従って

- 重要インフラのIT障害に関するコンプライアンスと情報開示の確保は国民生活と社会経済活動の基盤

しかし

- **IT障害に対する責任の原則**
  - IT障害に対する重要インフラの法的責任は各重要インフラ自身にある
  - 所管官庁は各重要インフラのIT障害対処を支援する責任を負う
- **その意味を具体的に捉えると**
  - ルールと責任の範囲の決定、脅威の把握、対処方針の決定、対処策の選定、実行が各重要インフラ自身の責任。その担保は各重要インフラの資産と所管官庁による業法規制

- **新たな枠組みの必要・・・「重要インフラの情報セキュリティ対策に係る基本的考え方」**

平成17年9月15日情報セキュリティ政策会議決定「重要インフラの情報セキュリティ対策に係る基本的考え方」の意義

- **意義**
  - 平成12年12月「重要インフラのサイバーテロ対策に係る特別行動計画」の見直しと新視点の導入
  - **見直し**
    - **重要インフラの範囲、対象分野の拡大と継続的な見直し**
      - 重要インフラの範囲
        - 他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状況に陥った場合に、我が国の国民生活または社会経済活動に多大なる影響を及ぼすおそれが生じるもの
      - 重要インフラの対象分野
        - 重要インフラのうち、そのサービスの提供が情報システム委大きく依存しているため、IT障害についての総合的な取り組みが必要と考えられる分野。 情報通信、金融、航空、鉄道、電力、ガス、政府・業精査^ビス(地方公共団体を含む)、医療、水道、物流の10分野。
    - **想定する脅威の見直し**
      - 「サイバー攻撃等の意図的要因」に止まらず「人為的ミス、外部委託等の情報技術の適用方法の変化に伴う構造的な脅威などの非意図的要因」や「地震・津波などの自然災害」など多種多様な脅威のすべて。
  - **新たな視点**
    - **「個別の取り組みを政府が支援する」から「我が国全体としてセキュリティ水準を向上させてゆく」という観点**
      - 重要インフラの相互依存性解析
        - 重要インフラに起こりうる脅威の把握
        - ある重要インフラのIT障害が他のどのインフラに影響するかの相互依存性の把握
      - 分野横断演習などの重要インフラ横断的な総合的対策の強化
    - **重要インフラ防護の一層の強化**
      - 分野毎の安全基準・ガイドラインの作成・評価
      - 官民の連絡・連携、情報共有体制の強化とその実効性の確保
      - 情報セキュリティ基盤の強化
      - 詳細検討の実施

平成17年9月15日情報セキュリティ政策会議決定「重要インフラの情報セキュリティ対策に係る基本的考え方」実現にむけた期待

- コンプライアンスの確保の視点から
  - 「分野毎の安全基準・ガイドラインの作成・評価」について
    - 基準の策定の責任は依然として各重要インフラに委ねられている
    - 重要インフラの機能、IT障害の社会的影響、防護目的からして各事業法による担保との連携をどのように図るかが今後の課題
- 情報開示の視点から
  - 「官民の連絡・連携、情報共有体制の強化とその実効性の確保」について
    - その重要インフラが対策を講じる視点からのもの
    - 開示すべき情報の範囲の決定
      - 相互依存する相手方のリスク把握の視点からも検討されることが望まれる
    - 開示を可能とする条件整備
      - 免責・守秘の保障についても検討が望まれる
- 事業継続確保の視点から
  - 事業者による事業継続を支援する主体と責任、行動計画の検討が望まれる

ISMS認証取得

稲垣隆一法律事務所

弁護士　稲　垣　隆　一

〒104-0028
東京都中央区八重洲2-10-10ムラキビル6階
PHONE:03-3279-0300/FAX:03-3279-0301
Bengoshi_inagakimail@alpha.ocn.ne.jp

日本弁護士連合会　コンピュータ委員会副委員長・情報問題対策委員会委員・消費者問題対策委員会(電子商取引・ネットワーク部会)　外

学 会 等　法とコンピューター学会・情報ネットワーク法学会・日本刑法学会・システム監査学会　外

公　務　法制審議会刑事法部会(ハイテク犯罪関連)幹事・警察庁「総合セキュリティ対策会議」・経済産業省「情報セキュリティ監査研究会」・「情報セキュリティ教育研究会」、JIPDEC「システム監査基準検討委員会」「ＩＳＭＳ運営委員会」・総務省「地方公共団体におけるシステム監査のあり方に関する調査研究会」,「地方公共団体の情報セキュリティレベルの評価に係る制度の在り方に関する検討会専門委員」,「地方公共団体の各種インシデントの適切な予防及び復旧に役立てる仕組みの具体化のための調査研究会委員」,内閣官房「IT戦略本部情報セキュリティ基本問題委員会第1,第2分科会」「内閣官房「情報セキュリティ政策会議セキュリティ文化専門委員会」「重要インフラ専門委員会」委員外を歴任

著書・論文　サイバースペースと法規制（日本経済新聞社・平成9年）
持株制度の運用と実務（新日本法規出版・平成10年）
情報ネットワークの法律実務（第一法規出版・平成11年）
法律実務のためのコンピュータ徹底活用ブック（トール・平成11年）
ビジネスマンのためのインターネット法律辞典（日経BP社・平成13年）
個人情報保護法Ｑ＆Ａ（中央経済社・平成13年）
情報セキュリティ監査と管理の法的問題（日本内部監査協会）
個人情報保護法と企業対応（清文社・平成15年　新版・平成16年）
いやでもわかる法律（日経ビジネス人文庫）外

IJ 01378　ISMS認証基準(Ver.2.0)
IS 92993　ＢＳ7799：Pert2:2002

業務　企業の業務上組織上のリスク対策・商品開発や契約における法規適合性確保の取り組み・顧問業務・内部統制構築
ＩＳＭＳ構築・プライバシーマーク取得支援・継続のための教育・システム監査・セキュリティ監査
個人情報保護法適合性監査・継続教育