重要インフラにおける情報システムリスクマネジメント

～事業継続マネジメントの観点から考える現状と今後の課題～



重要インフラ情報セキュリティフォーラム2008

2008年2月20日

渡辺　研司

WATANABE, Kenji

watanabe@kjs.nagaokaut.ac.jp

長岡技術科学大学大学院技術経営研究科

アジェンダ

1. 現代社会において増加するICT依存性と情報システムリスク
2. 重要インフラにおける論点整理
3. 重要インフラ防護（CIP）と情報システムリスクマネジメント
   ～最近の米国動向と日本の取組み～
4. 今後の方向性と残された課題

1．現代社会において増加するICT依存性と情報システムリスク

情報システムにおけるリスク要因・脆弱性の増加

情報システムに求められる要件と新たな脆弱性要因

- 高速/大量処理
- 24時間365日運用
- リアル・タイム処理
- ネットワーク化
- 分散処理
- マルチ・プラットフォーム
- マルチ・ベンダー
- 社会基盤相互依存

- マニュアル・リカバリーの限界
- 復旧作業タイミングの減少
- 障害時の経済的損失の増加
- 障害伝播速度の高速化
- 障害伝播到達範囲の広域化
- 他者からの影響の可能性
- 障害原因特定の遅延
- プロジェクト管理のスキル不足
- 社会インフラ間の連鎖障害

ネットワーク型社会における脆弱性増加の背景

相互依存性の範囲・レイヤーの拡大

- サプライチェーン、ネットワーク経由の障害伝播（スピード、範囲、影響度の増大）
- 『広域』連鎖障害・災害の増加
- 『他者リスク』の増大
- 複雑性、階層性に起因する原因究明の遅延

2. 重要インフラにおける論点整理

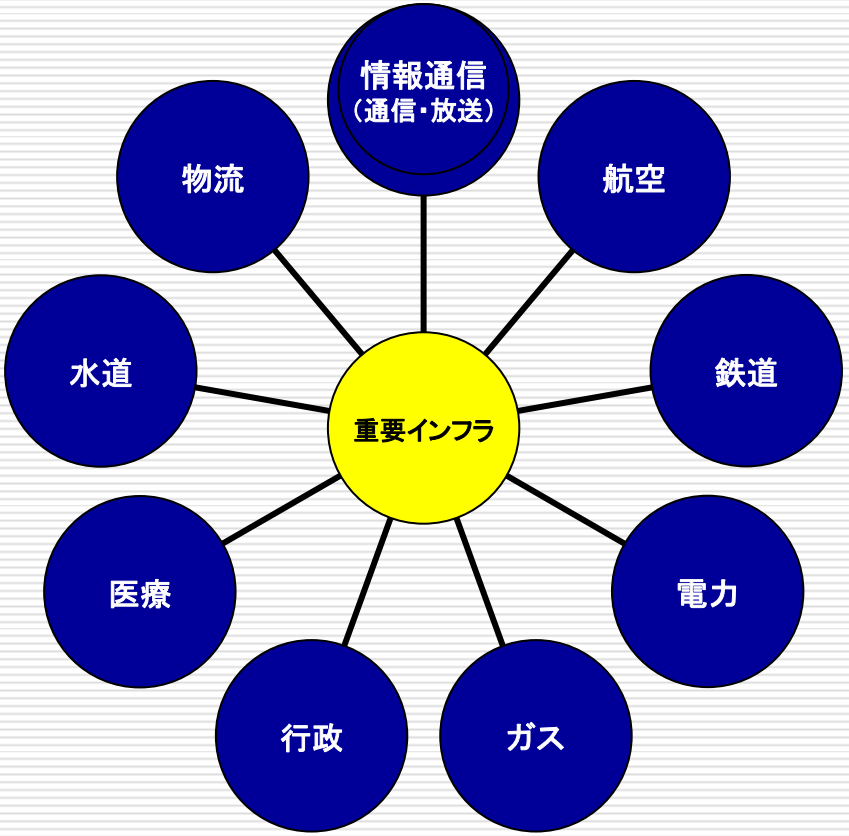
システム障害事例(2002～)

発生分野・パターンの多様化

- ダム異常放流(2002)
- 銀行システム統合障害(2002)
- 航空管制システム障害(2003,2008)
- 全国銀行ATMネットワーク障害(2004)
- IP電話不通(2004)
- 消防局119番通報制御停止(2004)
- 血液検査肝炎ウィルス感染誤判定(2005)
- 航空チェックインシステム障害(2007)
- 鉄道自動改札障害(2007)
- 証券取引売買システム障害(2005,2006,2008)
- 新聞制作システム障害(2007)
- 鉄道の進路制御装置誤動作(2008)
- 公衆電話通信障害(2008)　　など

我が国の重要インフラを取巻く状況

ICT導入加速の背景とそれに伴う脆弱性の台頭



- ICT（情報通信技術）の発展と依存
- 民営化など経済性・効率性の観点
- 重要インフラ間の相互依存性
- 「想定外」事案の発生
- 事業者の業態と所管省庁の乖離

など

重要インフラにおけるICT関連脆弱性

ICT（情報通信技術）に関わる脆弱性の具体的例示

- アウトソーシング、業務委託など外部業者との接続形態の多様化
- 自動化、リモートコントロール化、標準化などによる情報システムへの依存性増加と運用形態の多様化・複雑化・ブラックボックス化
- ICT障害発生時の復旧の長期化
- 基本設計時の想定と現在の運用上の潜在リスクとの乖離（技術構成、運用方法など）
- ICT運用方法の多様化による複合的なリスクの台頭
- 重要社会インフラ間の相互依存性の発生（障害連鎖の可能性）
- 事業者 / 所管省庁間の連絡体制の整備未了

重要インフラにおけるICT関連脆弱性

金融業界における事例（平成20年版金融システム情報白書より抜粋）

- 日本の約700の金融機関（銀行、証券、保険、ノンバンク） を対象に調査

- 情報システム障害件数：
  - 2006年：　183件@109機関
  - 2007年：　196件@111機関

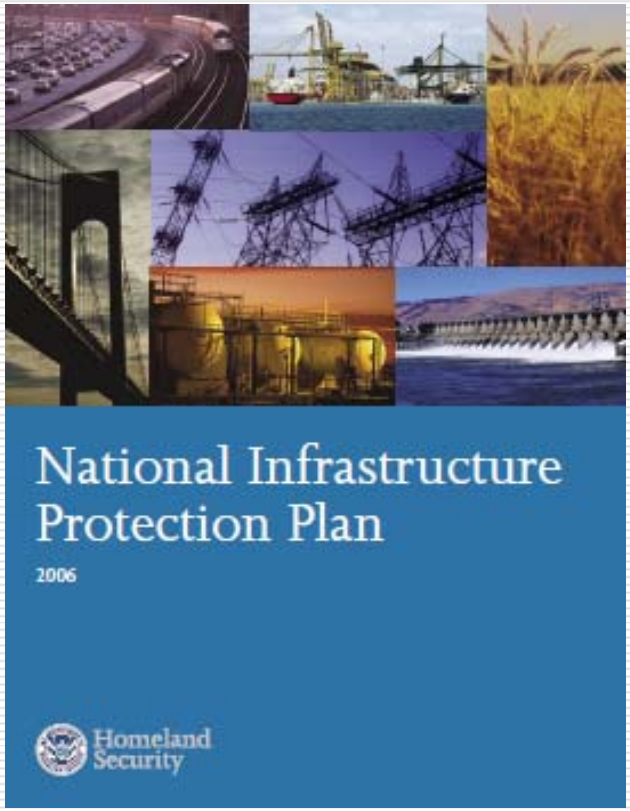
- 2007年の情報システム障害要因
  - 最も多い要因：　電力系
  - 急増中：　オペレーション障害、落雷、導入障害

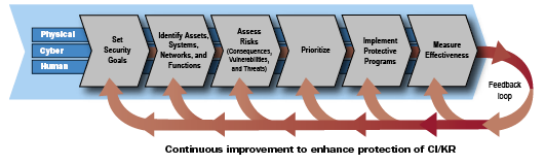
- 情報システム障害要因の多様化
  - 共同事務センター、共同データセンターにおける情報システム障害
  - アウトソーサー・外部委託先における情報システム障害
  - アウトサーサー・外部委託先のオペレーションミス
  - システム開発外部委託先のプログラミングミス
  - 旧システムから新システムへの移行失敗　など

3. 重要インフラ防護（CIP）と情報システムリスクマネジメント
～最近の米国動向と日本の取組み～

米国のCIP:国家重要インフラ防護計画(2006)

National Infrastructure Protection Plan (NIPP)





リスクアセスメントのアプローチは、**PDD63(Presidential Decision Directive 大統領令、1997)を踏襲する、HSPD-7(国土安全大統領令、2003)の枠組みを採用:**

- 個人の生命及び生活への影響
- 経済的な影響
- 社会的なモラル・自信への影響
- 国家機能への影響

重要インフラにおける情報システム防護

米国におけるCIIP（重要情報インフラ防護）の考え方　①

（1）重要情報インフラ防護の要素

- システムの接続性と可用性：Access & Availability
- 人的（知識・スキル）要素：Human Factors
- 組織責任：Organizational Responsiveness
- 自発的・能動的な取組み：Proactive Abilities

重要インフラにおける情報システム防護

米国におけるCIIP（重要情報インフラ防護）の考え方　②

（2）重要情報インフラの脅威（直接 / 間接、途絶 / 攻撃）

- **脅威の主体：Who ？**

自然災害、内部関係者、関係者（出入りの業者、ベンダー）、外部関係者（競合者、敵）

- **脅威の方法：How ？**

ヒューマン・エラー（開発時 / 運用時）、気づきの失敗（Failure of awareness）、
意図的な / 故意の行為

- **脅威の内容：Why ？**

偶発事故・災害、重要インフラ運営における損害、重要インフラに依存する組織への損害、
窃盗・強奪、社会・経済における損害

重要インフラにおける情報システム防護

米国におけるCIIP（重要情報インフラ防護）の考え方　③

（3）研究・開発のハードル（克服すべき困難性）

- **物理的要因**：Physical factors

重要社会インフラの情報システムの複雑性、相互接続（依存）性、広範な範囲と規模

- **知的要因**：Intellectual factors

動的（dynamic）な攻撃手法の進化、未集約の専門的知識と散在 / 散逸する専門家

- **感情的要因**：Emotional factors

大規模障害時の官・民・個人間の「すくみ」、未調整の官民間の意思決定プロセス、官民対応における中長期的観点の欠如

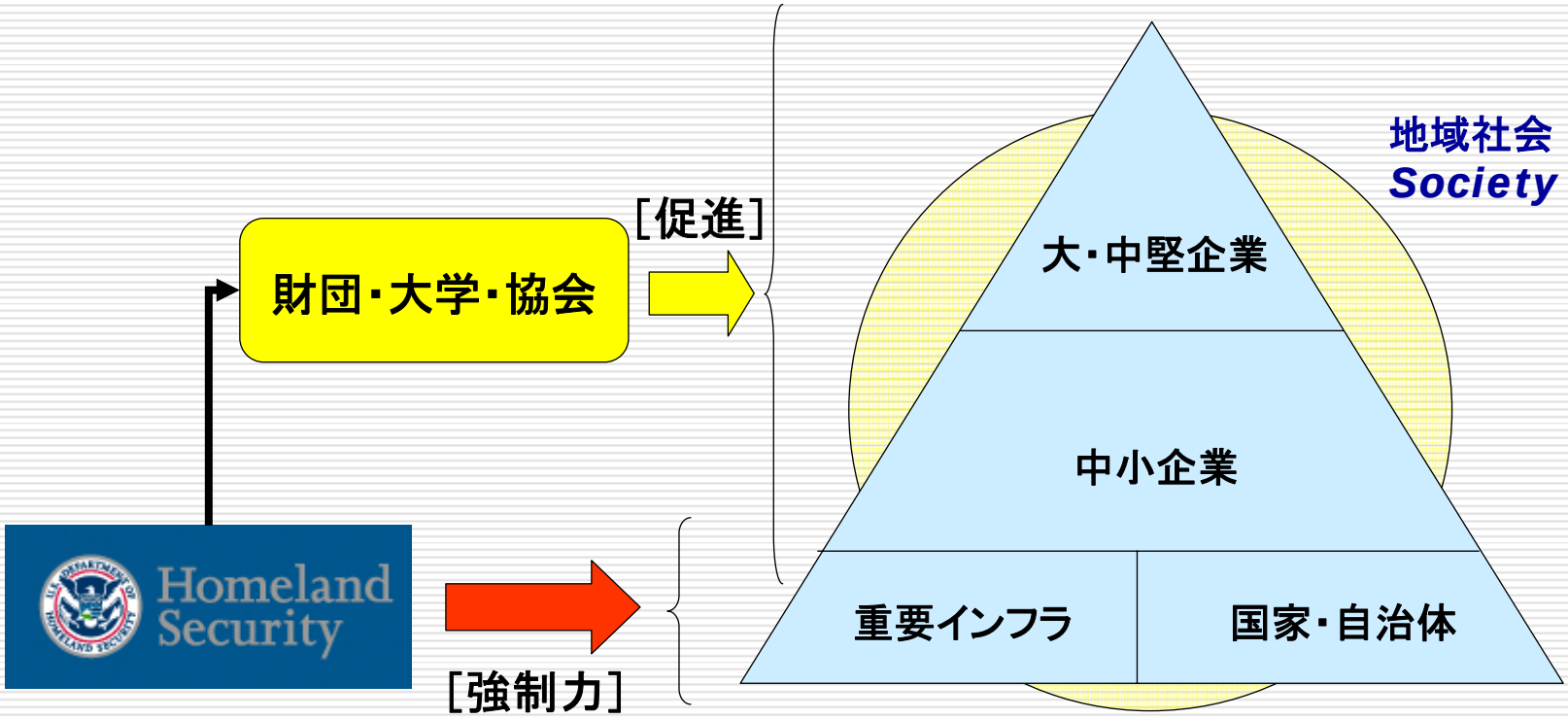
- **法的要因**：Legal factors

未調整の国内組織間、国際間の法的側面

国家全体のレジリエンシー強化

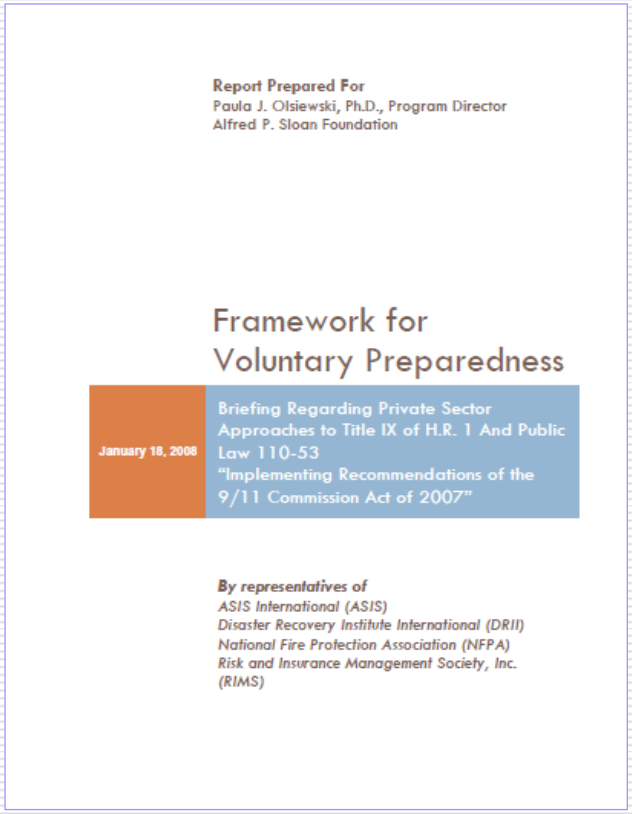
米国政府の取組み［概念図］

2008年2月現在



企業の自発的な備えに関する枠組み（2008）

民間企業にも自主的な自助努力を示唆：多様な選択肢



Report Prepared For
Paula J. Olsiewski, Ph.D., Program Director
Alfred P. Sloan Foundation

Framework for
Voluntary Preparedness

January 18, 2008

Briefing Regarding Private Sector Approaches to Title IX of H.R. 1 And Public Law 110-53
"Implementing Recommendations of the 9/11 Commission Act of 2007"

By representatives of
ASIS International (ASIS)
Disaster Recovery Institute International (DRII)
National Fire Protection Association (NFPA)
Risk and Insurance Management Society, Inc. (RIMS)

ASIS INTERNATIONAL
Advancing Security Worldwide

セキュリティ
Security

DRI
the institute for continuity management

事業継続
Business Continuity

NFPA

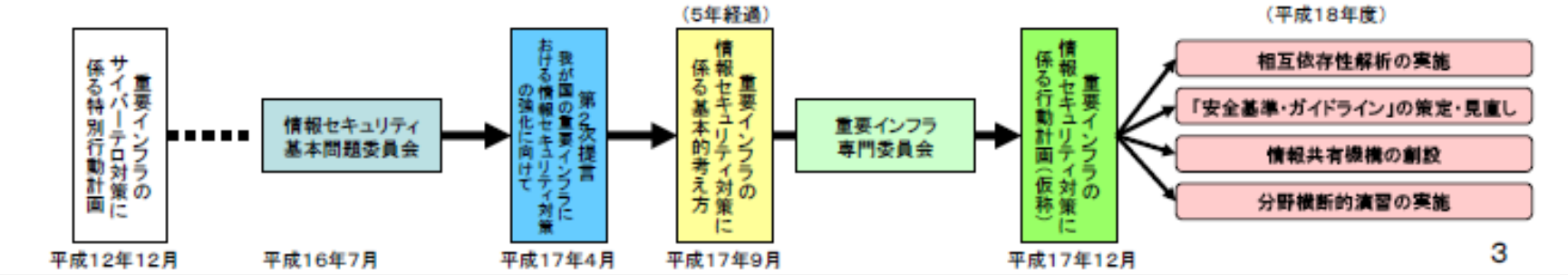
緊急時マネジメント
Emergency Management

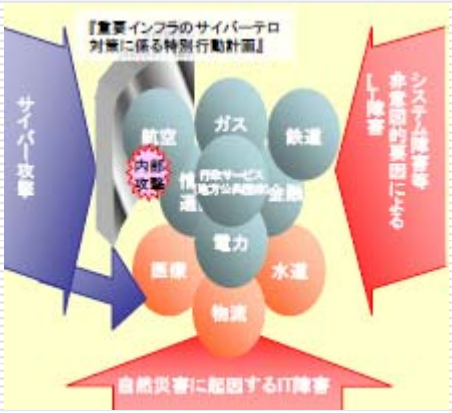
Risk and Insurance Management Society, Inc.

リスクマネジメント
Risk Management

我が国のCIP/CIIP

内閣官房主導で所管省庁・業者・業界の協力を得ながら推進中





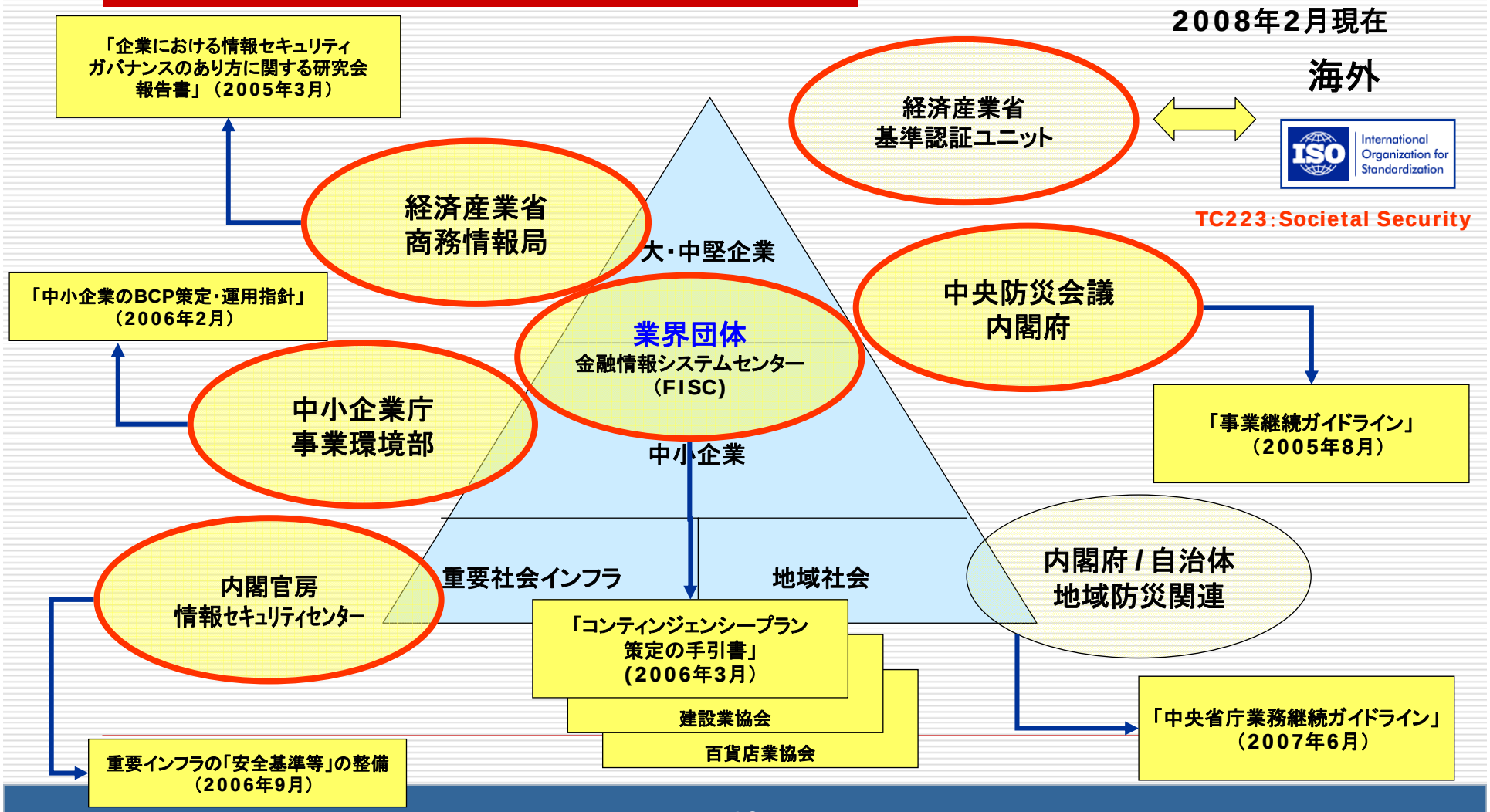
第1次情報セキュリティ基本計画（2006～2008年度）

- 政府、重要インフラ、企業、個人を視野

第2次情報セキュリティ基本計画（2009年度～）[策定中]

国家全体のレジリエンシー強化の動き

日本政府の取組み[概念図]



4. 今後の方向性と残された課題

今後の方向性と残された課題

適度な情報開示、「自助」部分の拡大、専門人材の集約が鍵

- 重要インフラ防護（CIP）の合理性に関する基本的な考え方
- CIPとCIIPそれぞれの定義・役割分担と推進体制
- 物理的な防護と電子的な防護の融合
- 情報・知見共有の体制とリスクコミュニケーション（対企業・国民）
- 社会経済活動・個人生活における「自助」意識の醸成・拡大
- 情報システムリスクの分析・モニタリング手法の開発
- 高い信頼性の重要情報インフラのモニタリング（監視）の仕組みと早期警戒システム
- 専門人材の育成　　など

CIIPへの経営資源投資のインセンティブ

情報セキュリティの観点からの概念的な議論

■ OECD「情報システムのセキュリティのためのガイドライン」

（1） 守秘性（Confidentiality）
（2） 可用性（Availability）
（3） 完全性（Integrity） の確保

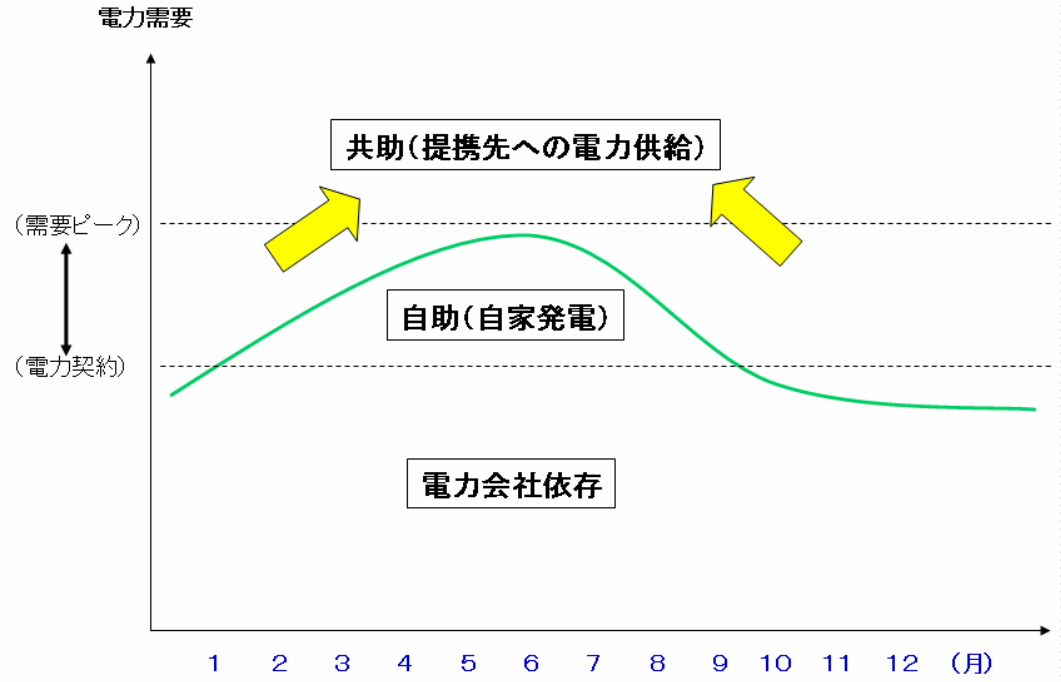
■ WEIS（Workshop on the Economics of Information Security）での議論

信頼性（Dependability / Reliability）の確保

重要インフラ利用者としての企業のBCM

重要社会インフラにおける事故前提シナリオと自助/共助の取組み

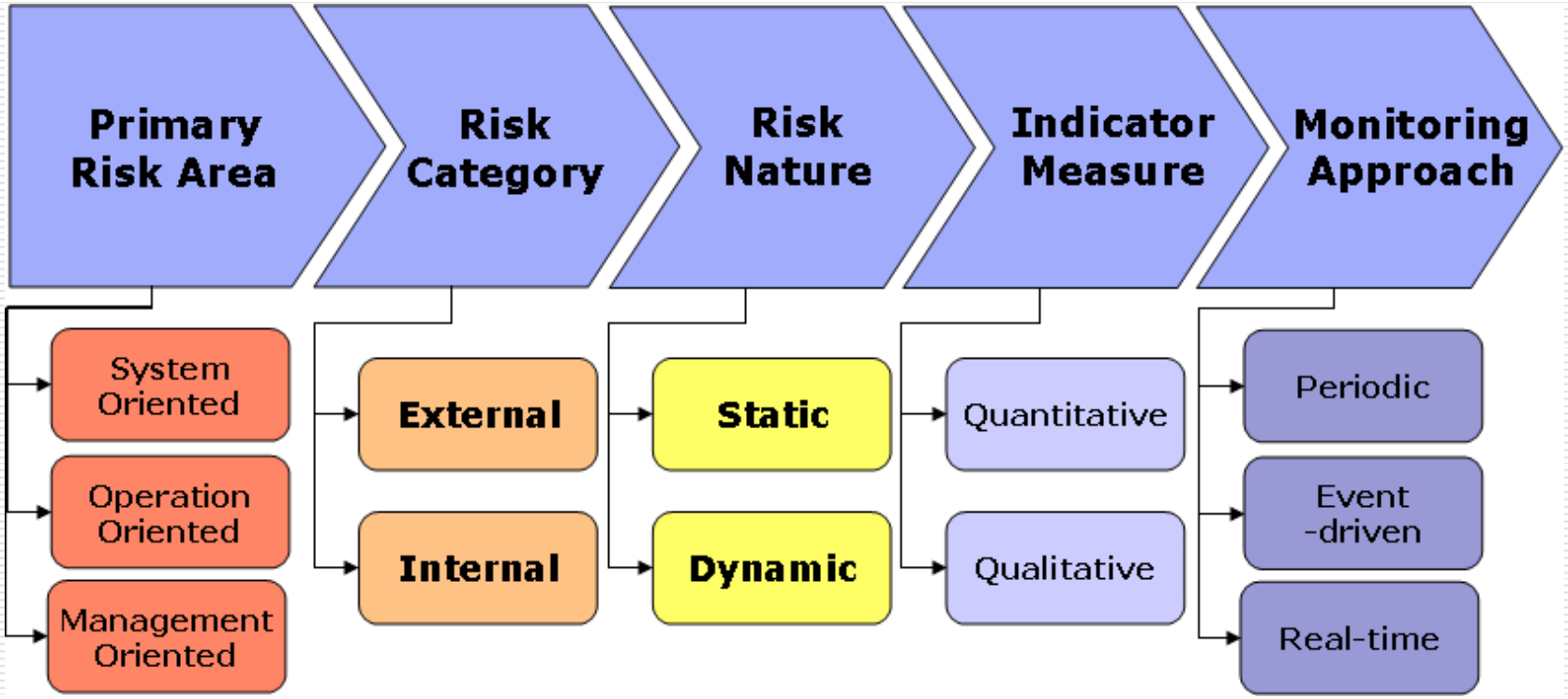
- 重要社会インフラのICT障害によるサービス機能不全を前提としたBCM
- 「自助」のための設備投資、業務プロセス変更によるレジリエンシーの確保
- 他社との相互バックアップ（共助）



契約電力量と自助/共助の仕組みのバランス［概念図］

情報システムリスクマネジメントの要素

情報システムリスク・マネジメント：モニタリング指標の開発



情報システムリスクマネジメント

早期警戒を目的とした先行指標の開発（例示）

Primary Risk Area	Risk Category	Incident Area	Potential Risk (Example)	Nature	Indicator	Monitoring Approach
System	Internal	Hardware	Hard disk failure	Static	Qualitative	Event-driven
		Software	Critical bug realization	Dynamic	Quantitative	Periodic
		Network	Network down	Dynamic	Quantitative	Real-time
		Infrastructure	Power failure	Dynamic	Quantitative	Real-time
	External	Hardware	Stop running with overcapacity	Dynamic	Quantitative	Real-time
		Software	Program version unmatch	Static	Qualitative	Event-driven
		Network	Slow communication	Dynamic	Quantitative	Real-time
		Infrastructure	Closed traffic (no access to office)	Dynamic	Qualitative	Event-driven
Operation	Internal	Human resource	Regional -wide epidemics	Dynamic	Quantitative	Event-driven
		Transaction	Unexpected irregular transactions	Dynamic	Quantitative	Real-time
	External	Human resource	Decrease in skill level	Static	Quantitative	Real-time
		Transaction	Unexpected slow performance	Dynamic	Quantitative	Real-time
		Contract	Very limited SLA	Static	Qualitative	Event-driven
Management	Internal	Staff skill	Lack of necessary skills	Static	Qualitative	Periodic
		Staff availability	Unexpected high turnover	Dynamic	Quantitative	Real-time
		Compliance	Criminal fraud	Dynamic	Qualitative	Real-time
	External	Vendor	Multi-vendor management failure	Static	Qualitative	Periodic/Event-driven
		Project	Project management failure	Dynamic	Qualitative	Periodic
		Other banks	System integration failure	Dynamic	Quantitative	Real-time
		Natural disasters	Earthquake	Dynamic	Quantitative	Real-time
		Human disasters	Terro-attack	Dynamic	Qualitative	Real-time

情報システムリスクの関与範囲の拡大

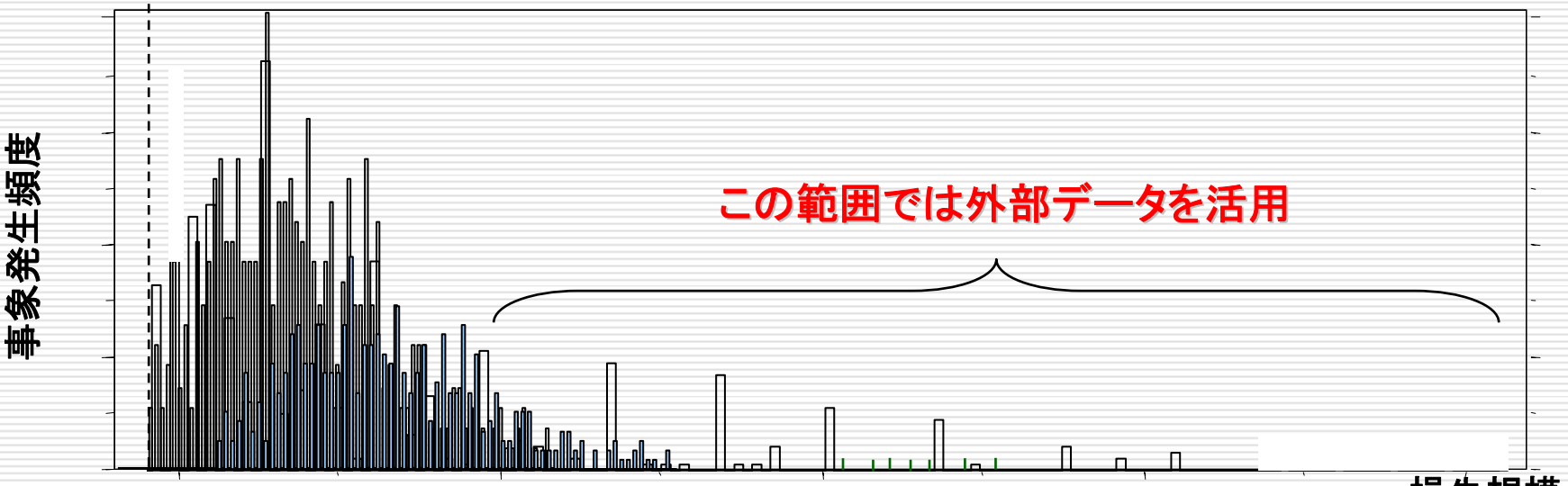
金融分野におけるオペレーショナルリスクのファクター分類に基づく考察

大分類	中分類	情報システム関連リスク
人	従業員の詐欺、悪意(犯罪)	○
	権限外の行為、違法取引、従業員の不正	○
	雇用法	
	労働の中断	
	キーパーソンの喪失、不在	
プロセス	支払・決済のデリバリーリスク	○
	文章または契約書のリスク	
	査定・価格設定	
	内部・外部報告	○
	コンプライアンス	
	プロジェクトリスク、経営戦略の変更	
	販売リスク	
システム	技術投資リスク	◎
	システム開発と実装	◎
	システムキャパシティ	◎
	システム停止	◎
	システムセキュリティの突破	◎
外部	法的・公的責任	
	犯罪行為	
	アウトソーシング・サプライヤーリスク	○
	インソーシングリスク	○
	災害と社会インフラの停止	○
	規制リスク	
	政治・行政リスク	

(財)金融情報システムセンター、「統合リスク管理研究会」報告書(BBA:英国銀行協会のリスクファクター分類)をもとに作成

オペレーショナルリスクマネジメント方法論の適用

事故・障害に伴う損失に関わる外部データの活用可能性



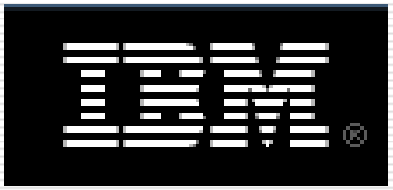
発生頻度（大）/損失規模（小）- 内部データが多く存在

発生頻度（中）/損失規模（中）- 内部データが一部存在

発生頻度（小）/損失規模（大）- 内部データは殆どなし

情報システムのレジリエンシー成熟度指標

ICTの観点から評価する組織の回復力



① 米国カーネギーメロン大学：**RMM (Resiliency Maturity Model)**

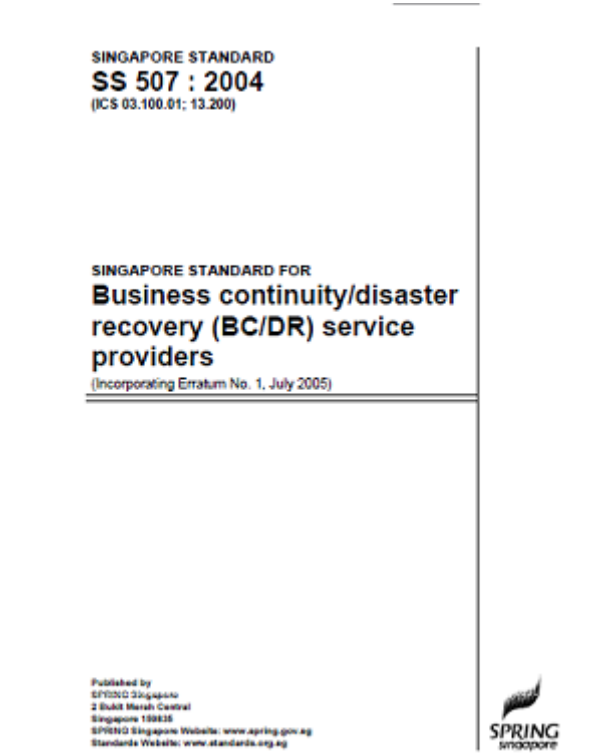
- 同大ソフトウェア工学研究所、金融業界、主要ベンダーなどがコンソーシアムを組成
- テロ・災害・サイバー攻撃対応、制度対応、重要インフラ障害対応、サプライチェーン途絶対応などの能力についての成熟度指標を開発
- 現在フェーズ3－Bに入り、他業界も含めてベンチマーキングを試行中

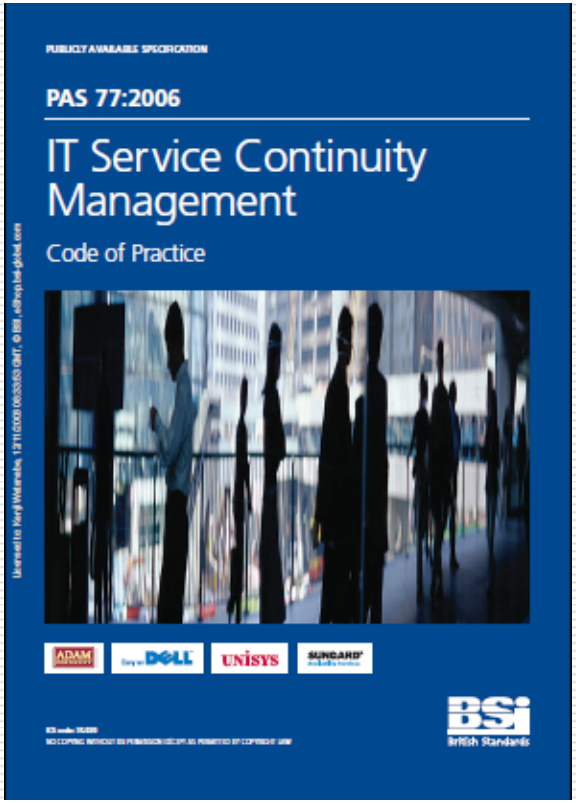
② **IBM**インド基礎研究所：**RMI (Resiliency Maturity Index)**

- 情報システム関連の故障や機能停止が組織に及ぼす影響を数値化
- 情報システムのコンポーネント毎に異なる回復力（レジリエンシー）を評価、総合的に組織全体の回復力にどのように影響するかを把握する
- 対象は社内業務評価のみならず外部アウトソーシング移行の判断支援に用いられる

IT継続性（内部・外部）に関する標準・ガイドライン

ITサービス供給側・利用側のIT継続性確保の規格が出現中

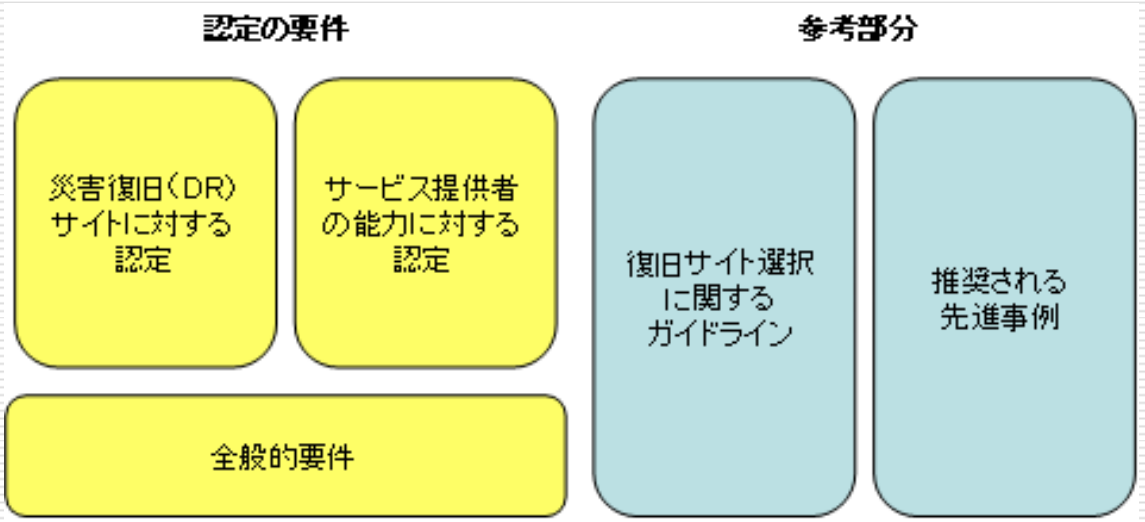




IT継続性に関わる規格・ガイドライン

シンガポール・SS507（DR／BCサービス供給業者向け基準）

1. 情報通信開発庁（IDA：Infocomm Development Authority of Singapore）が2004年に策定
2. 事業継続や災害復旧に関する業界の標準（資格制度）
3. 政府のバックアップにより国内の事業継続や災害復旧に関する業界の競争優位性の確保を目的とする
4. 業者間の品質格差が広がり、業界全体の信用力が落ち始めたことを懸念した政府が、産官学で連携
5. 実際にこの規格をクリアした業者は政府系や大手の7社程度



長岡技術科学大学
大学院技術経営研究科
渡辺　研司
watanabe@kjs.nagaokaut.ac.jp