



ISO22320チェックリストの調査に 基づく組織の危機対応力について

2017.12.6

NTTセキュアプラットフォーム研究所 爰川 知宏

1. はじめに
2. 危機対応の標準化とISO22320
3. ISO22320簡易版チェックリスト
4. 調査と考察
5. おわりに

はじめに

組織をとりまく危機の甚大化・多岐化



- 気候変動による風水害の拡大、地震火山活動の活発化
- テロ攻撃の世界的広がり等による人為的災害の拡大
- サイバー攻撃の拡大、多岐化

自然災害

過去5年の激甚災害指定:22件

- 台風18号等 関東・東北被害 (2015.9)
- 熊本地震 (2016.4)
- 台風10号 北海道東北被害 (2016.9)
- 九州北部豪雨 (2017.6)

人為的災害

テロの世界的広がりによるCBRNE※
リスクの増大

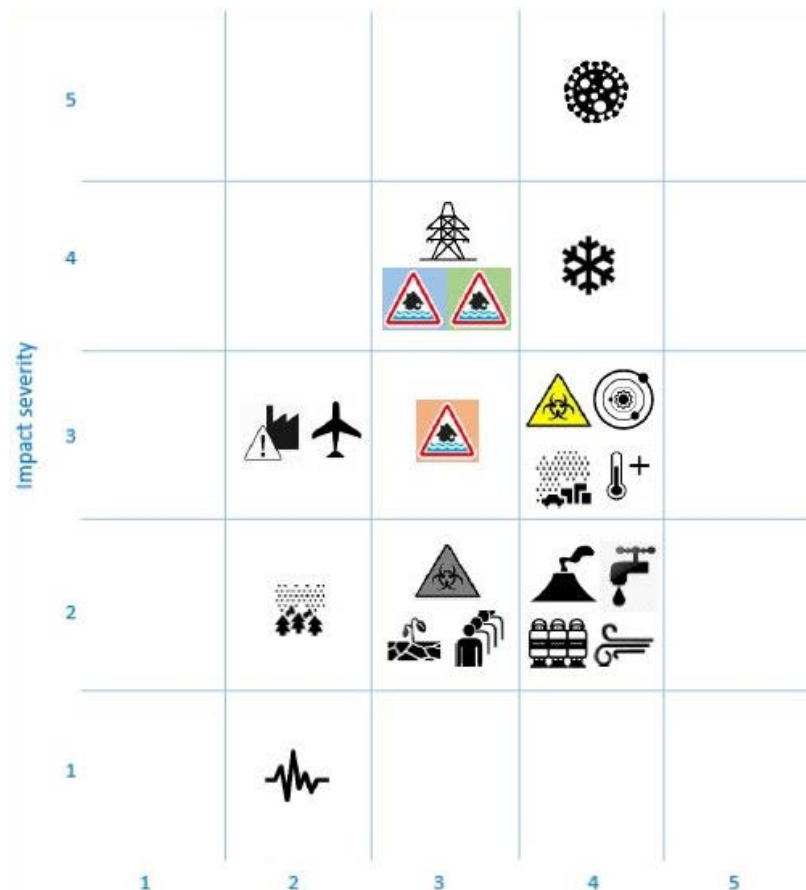
サイバー攻撃

- ・標的型攻撃、ランサムウェア等の拡大
 - 年金機構 (2015.5)、JTB (2016.6) 等での大規模個人情報流出
 - WannaCryの流行 (2017.5)
- ・IoTへの攻撃
 - Miraiマルウェアの拡散
- ・重要インフラを狙った攻撃
(サイバー・リアル複合危機)
 - ウクライナでの大規模停電 (2015.12) 等

様々なリスク: 自然災害・事故

英国政府発行「National Risk Register Of Civil Emergencies」より

影響の深刻さ



Likelihood of occurring in the next five years

今後5年間の発生可能性

KEY

自然災害

感染症

Natural hazards

Diseases

- Coastal flooding
- River flooding
- Surface water flooding
- Storms and gales
- Cold and snow
- Heatwave
- Drought
- Space weather
- Volcanic eruptions
- Poor air quality
- Earthquakes
- Wildfires

- Pandemic influenza
- Emerging infectious disease
- Animal disease

Major accidents

事故

- Widespread electricity failure
- Transport accidents
- Industrial and urban accidents
- System failures

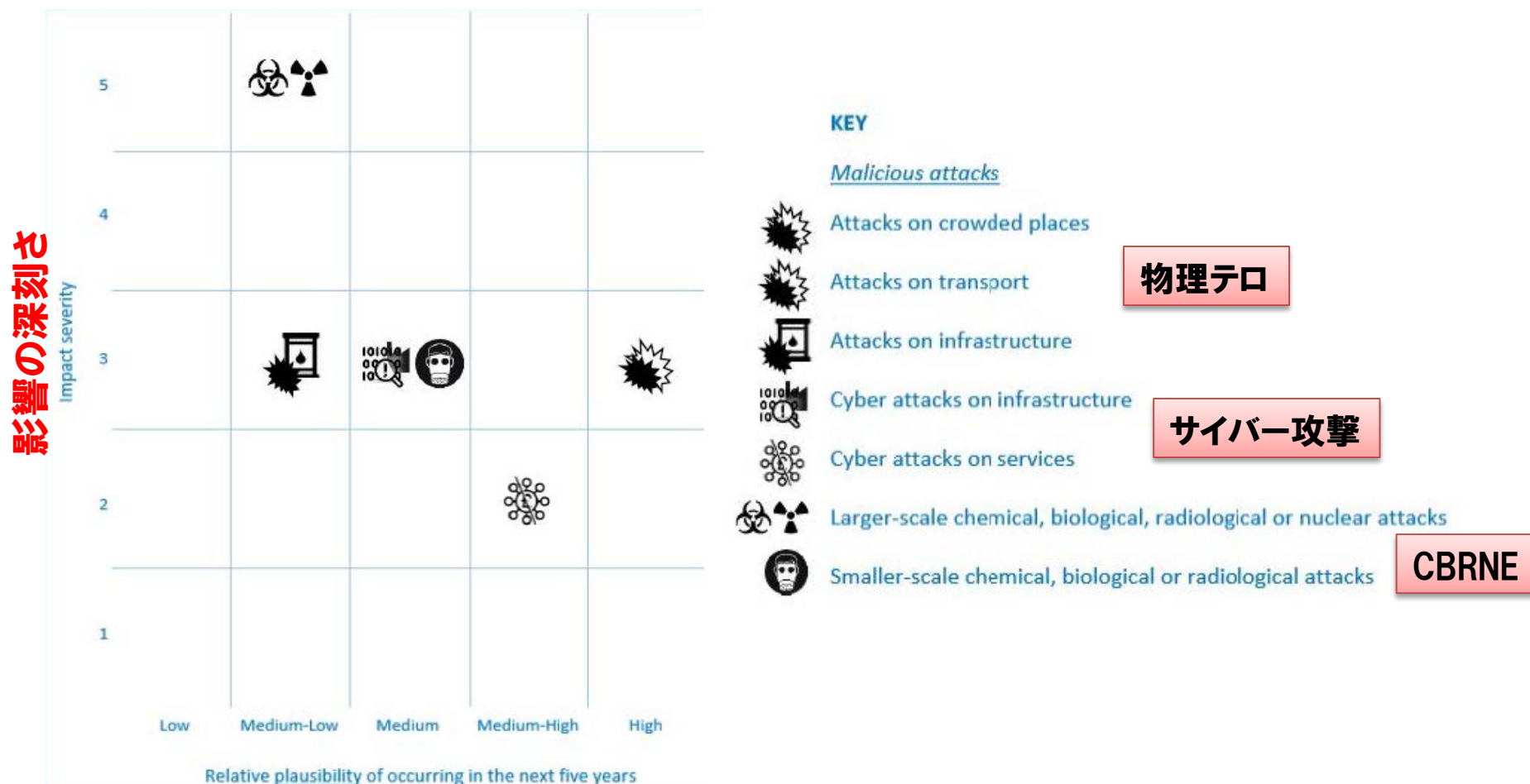
Societal risks

社会リスク

- Industrial action
- Public disorder

様々なリスク:悪意ある攻撃

英国政府発行「National Risk Register Of Civil Emergencies」より



今後5年間の発生の相対的可能性

防災からレジリエンスへ

- 予測・予防をいくら頑張っても、**リスクをゼロにすることはできない(防災の限界)**
- リスクが現実化(危機が発生)したときには「**対応力**」が重要となる
- 対応力によりすばやく立ち直ることでダメージを最小化⇒**レジリエンス**

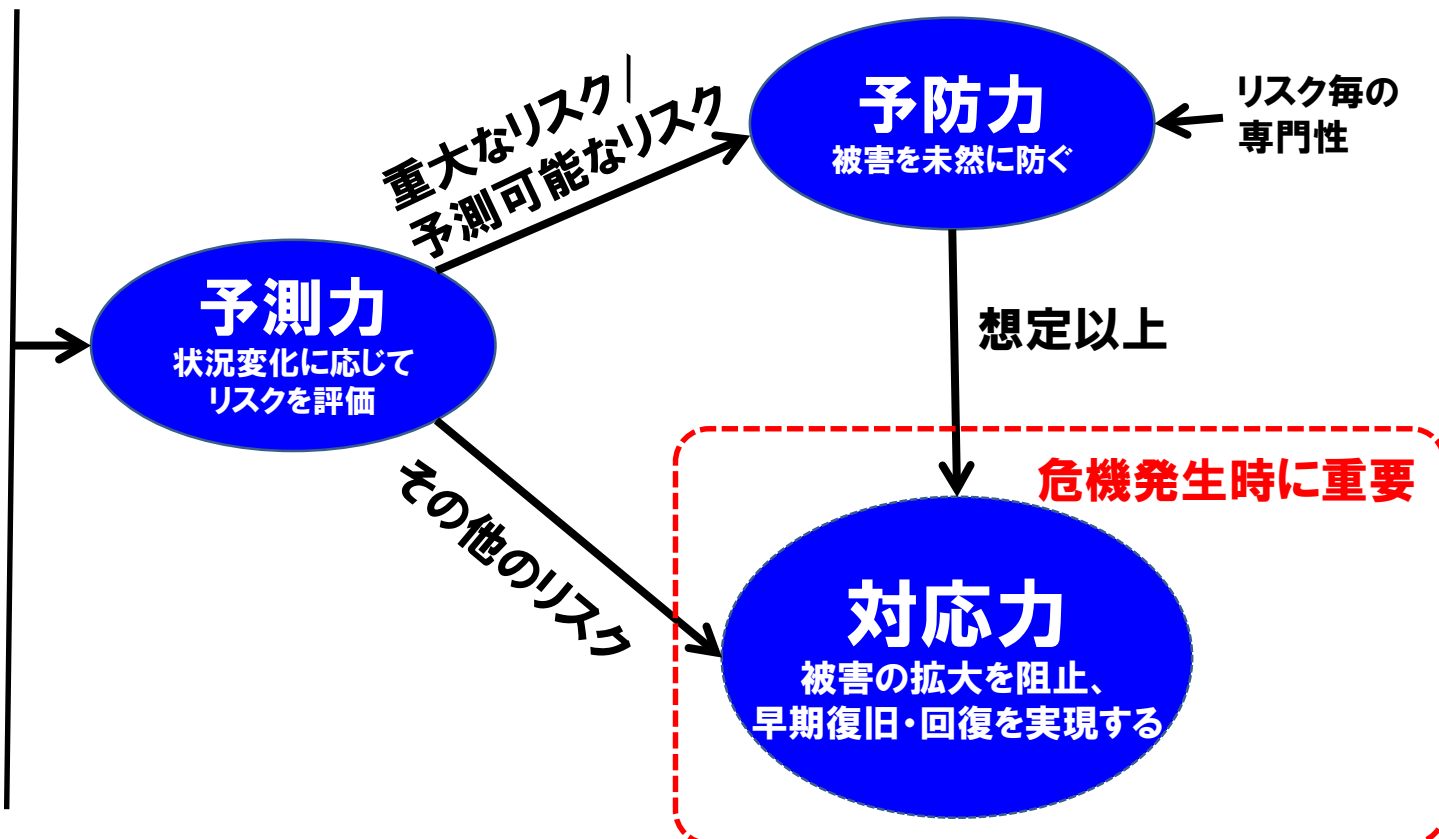
脅威

- ・CBRNE
- ・サイバー攻撃
- ・テロ
- ・事故
- ・犯罪
- ・地震
- ・風水害
- ・火災
- ・感染症 等
(受ける側の状況)

脆弱性

曝露量

- ・大都市の人口集積
- ・鉄道の相互乗り入れ
- ・制御システムNW化
- ・IoTの進展 等



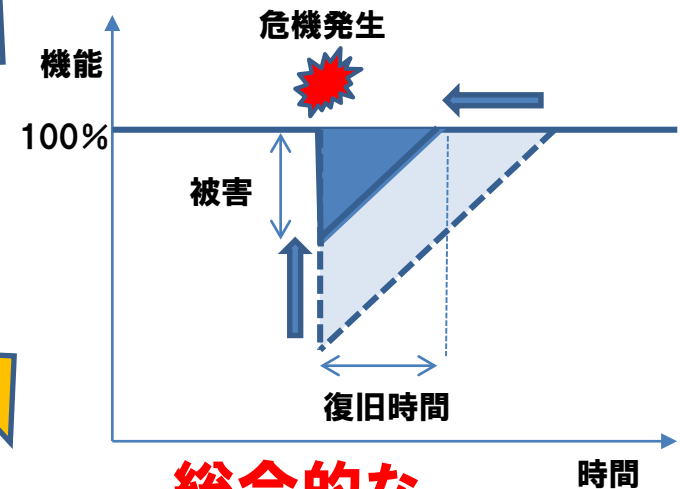
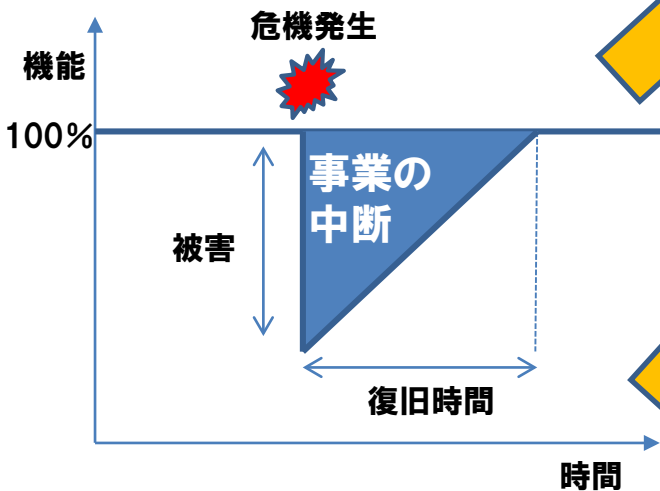
参考:レジリエンス社会をつくる研究会、「しなやかな社会の挑戦」、日経BPコンサルティング

レジリエンスの考え方

- リスクの種類に関係なく、**事業の中断による損失**(下図の三角形の面積)を減らすことが重要

抵抗力の向上
(被害を減らす)

予測力、予防力



総合的な
危機対応力の向上

回復力の向上
(復旧を早める)

対応力

危機対応はなぜ難しいのか？



- はるかに**仕事量が増える**
 - ✓ 平時にはない膨大な業務に振り回される
- **経験者・専門家がほとんどいない**(その場で一から考える)
 - ✓ やるべきことを決めるのに時間がかかる(意思決定できない)
 - ✓ やるべきと決めたことができない(統制できない)
 - ✓ やるべきだと決めたことが人によって異なる(言葉が合わない)

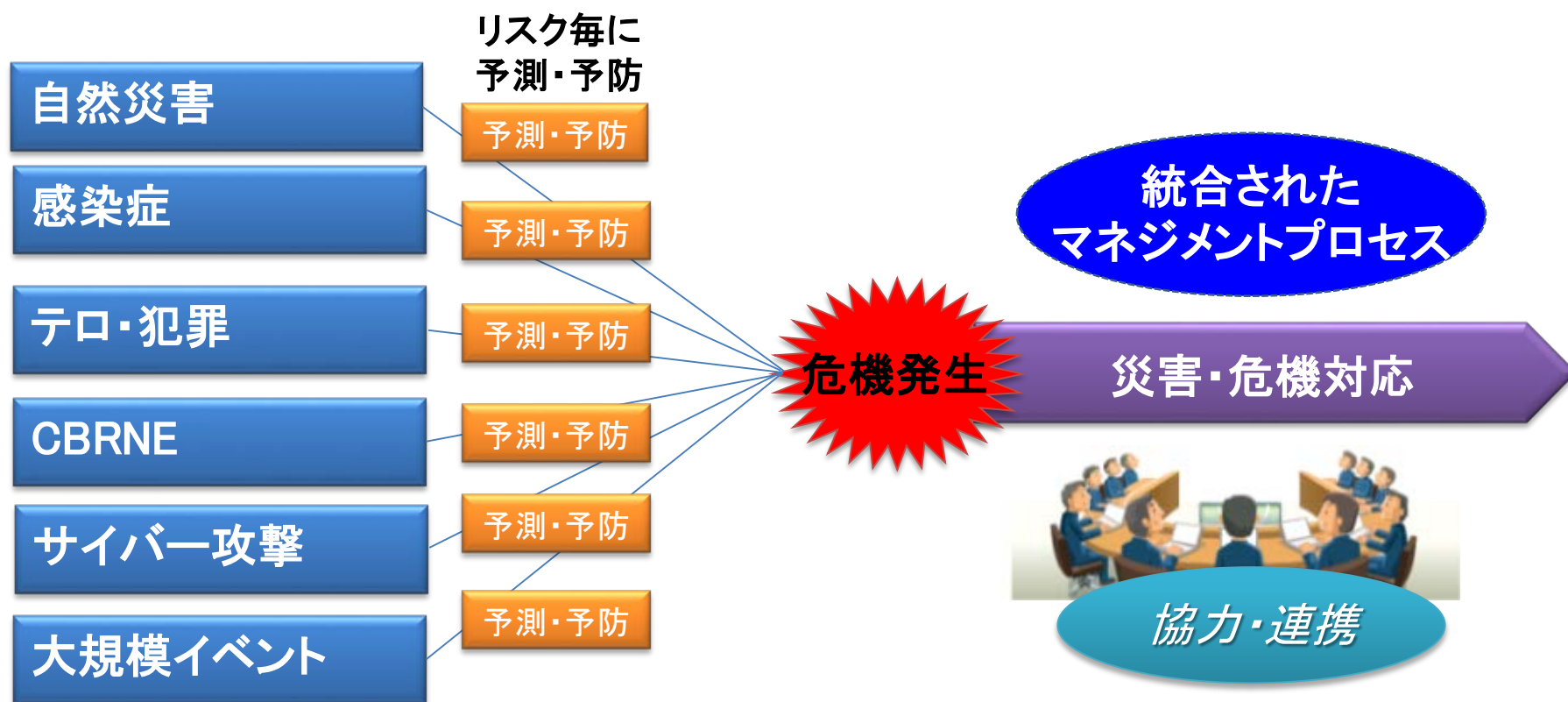
⇒ **応援が来ても活用できない**
- 曖昧な状況で**緊急性の高い意思決定**を迫られる
 - ✓ 情報がない/誤報多数。かといって何もしないと状況はさらに悪化
- 何をどこまでやればよいかの**指針がない**
 - ✓ 頑張った/想定外、は免罪符ではない。失敗すれば批判される

 **解決のためには、危機対応の標準化が必要**

危機対応の標準化とISO22320

危機対応のフレームワーク

- いかなるリスクに対しても、実際に危機が発生した際のマネジメントは共通
- そのためには、有事の際に関係組織が連携し業務を遂行できる**統一的なマネジメントフレームワーク**が必要

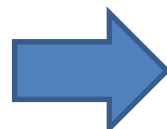


ICS (Incident Command System) とは

危機が発生した際に、警察・消防・軍などの制服組と、自治体・民間組織の非制服組を統合し運用する際の米国における標準。**あらゆる種類の危機に対して適用**

ICSの主な特徴

- ・共通の用語、情報管理様式
- ・目標による管理、プランニング
- ・指揮系統の統一と権限委譲

 ICSに沿って訓練プログラムやICTツールも整備

ISO22320 (JIS Q 22320)

- 効果的な危機対応を実現するための**必要最低限の要求事項**を規定
- **あらゆる種類の危機**への対応能力を高めることが目的
- 単一組織だけでなく、**組織・地域・国境を越えた連携**を想定
- 要求事項規格のみで、指針規格(ガイドライン)は定められていない
→ 第三者認証の仕組みを持たない(**評価基準がない**)

世界に通じる
危機対応

ISO 22320:2011
(JIS Q 22320:2013)

社会セキュリティ緊急事態管理
—危機対応に関する要求事項— 解説

編著者 林 春男
危機対応標準化研究会 編著

指揮・統制

活動情報

協力及び連携

世界に通じる危機対応
林春男、危機対応標準化研究会 編著
日本規格協会

序文

1章 適用範囲

2章 引用規格

3章 用語および定義

4章 **指揮・統制に関する要求事項**

5章 **活動情報に関する要求事項**

6章 **協力及び連携に関する要求事項**

附属書A(参考) 各要求事項の事例

附属書B(規定) 活動情報提供プロセスの評価基準

ISO22320の要点



章	概要	主な記載事項
4章：指揮・統制	人命を守り、負の影響を最小限にするためのあらゆる施策を行うための活動	・体制（権限、指揮レベル、指揮プロセス） ・地域社会との関係 ・必要な資源（ヒト・モノ・カネ・情報）の利用プロセス ・人的要因（文化的背景など、メンタル面）
5章：活動情報	危機対応活動を効果的に管理するための情報処理に関する活動	・情報処理（信頼性、信ぴょう性評価） ・情報分析（優先度、リスク分析、結果の推定） ・情報提供プロセスの評価
6章：協力および連携	共通の利害および価値観に基づいた効果的な危機対応を成し遂げるための協定に関する活動	・協力協定（専門家派遣など） ・連携プロセス（意思決定への寄与など） ・情報共有（環境、用語統一など）

レジリエンスに関する国際規格

- 適切なリスク管理を実施しても回避しがたい緊急事態が発生する場合がある。そのための国際規格として、ISO223シリーズ(社会セキュリティ)が策定されている
- 現在はISO292(セキュリティとレジリエンス)シリーズに統合

ISO31000:2009
(JIS Q 31000:2010)
リスクマネジメント
—原則および指針

ISO/IEC27005:2008
情報セキュリティの
リスクマネジメント

ISO22301:2012
(JIS Q 22301:2013)
事業継続マネジメントシ
ステム(BCMS)—要求事項

ISO22320:2011(JIS Q 22320:2013)
緊急事態管理—危機対応に関する要求事項

ISO22398:2013
(JIS Q 22398:2014)
演習の指針

ISO22325:2016
緊急事態管理能力
の評価

ISO22320簡易版チェックリスト

チェックリストの目的

- ISO22320に定められた要求事項をどの程度充足できているかを、担当者の主観により**危機対応力を可視化**
- (第三者認証ではなく)**セルフチェック**のためのツール
 - 自組織の強み・弱みの理解(**満点を取ることが目的ではない**)
 - トップ-担当間／部署間での意識違いの把握(**組織を代表したものではない**)

要件

- 要求事項を網羅したチェック項目の抽出
- チェック観点の明確化
- チェック結果のわかりやすい可視化

要求事項の評価(チェック)項目化

原文で助動詞に”**shall**”が使用された部分(63項目)に着目し、
以下の観点で不要と思われる部分を集約・統合

(ルール1) 階層関係にある要求事項(下位で詳細化、もしくは上位で絞り込み)

— 計8項目

(ルール2) 他の要求事項と補完関係(一方を満たせば自動的に満たされるもの)がある／統合が可能な要求事項

— 計18項目

(ルール3) ドキュメント化や実施レベルの評価が困難な要求事項(心得的なもの、担当者のスキル依存なもの)

— 計4項目

→精査の結果、33項目に集約

ルールに基づく精査例

ルール1

【5.3】組織は、活動情報提供プロセスの中で、次の評価基準を確実に満たすように検討しなければならない～詳細な事項および要求事項は附属書Bによる。

⇒附属書Bの各要求事項の上位階層である。

ルール2

【5.2.2】活動情報は、指揮・統制の一部として計画し、準備しなければならない（4.2.5参照）。

⇒4.2.5を満たせば自動的に満たされる。

ルール3

【6.3.2】連携の担当者は、他の関係者からの信頼を維持できるように行動しなければならない。

⇒担当者の心得であり、評価困難

(参考) 精査の詳細



節	要求 (shall)	推奨 (should)	ルール1	ルール2	ルール3	精査 結果
4.1	2	2	0	0	0	2
4.2.1	6	0	2	1	1	2
4.2.2	3	0	3	0	0	0
4.2.3	1	0	0	0	0	1
4.2.4	1	0	1	0	0	0
4.2.5	3	2	0	2	0	1
4.2.6	0	2	0	0	0	0
4.2.7	1	0	0	0	0	1
4.3	8	1	0	2	2	4
5.1	0	0	0	0	0	0
5.2.1	1	0	1	0	0	0
5.2.2	2	0	0	1	0	1
5.2.3	1	0	0	0	0	1
5.2.4	1	0	0	0	0	1
5.2.5	2	0	0	1	0	1
5.2.6	1	1	0	0	0	1
5.2.7	1	1	0	0	0	1
5.3	1	0	1	0	0	0

節	要求 (shall)	推奨 (should)	ルール1	ルール2	ルール3	精査 結果
6.1	1	1	0	0	0	1
6.2	1	0	0	0	0	1
6.3.1	3	2	0	1	0	2
6.3.2	11	0	0	6	1	4
6.3.3	3	0	0	1	0	2
6.4	2	0	0	0	0	2
6.5	1	0	0	1	0	0
B.1	0	0	0	0	0	0
B.2	2	1	0	1	0	1
B.3	0	0	0	0	0	0
B.4	2	1	0	1	0	1
B.5	1	0	0	0	0	1
B.6	0	0	0	0	0	0
B.7	0	1	0	0	0	0
B.8	1	0	0	0	0	1
B.9	0	1	0	0	0	0
B.10	0	1	0	0	0	0
B.11	0	1	0	0	0	0
計	63	18	8	18	4	33

	項目数
4章	11
5章	10
6章	12

※附属書Bは5章の補足資料のため、5章の項目としてカウント

チェックリストの構成

- 指針(ガイドライン)が存在しないため、充足レベルが答えづらい ⇒ **相対評価**
- すべての要求条件が必須なわけではない ⇒ **必要性と達成度**

ID	ISO項番	表題	項目	必要性		達成度		判断資料または根拠(任意)
				不要←	→必須	できていない←	→できている	
1	4.1	指揮・統制一般	危機対応にあたる組織・要員には必要な権限や資源を用意している。	○	○	●	○	
2	4.1	指揮・統制一般	地域社会が参画しやすいように関係を構築・維持している。	○	○	●	○	
3	4.2.1	指揮・統制システム一般	危機事象が発生した際には速やかに体制を立上げ(対策本部を設置し)、必要なプロセスを開始し、リーダを明確にしている。	○	○	●	○	
4	4.2.1	指揮・統制システム一般	初期の行動を迷わず迅速に行うために、文書化している。	○	○	●	○	
5	4.2.3	指揮・統制体制	判断の種類に応じて指揮レベルを分けている。例えば活動方針や目的・目標を決める戦略的役割、どのような資源を用いるか、どのような資源を活用するかを判断する戦術的役割など、	○	○	●	○	
ISO 22320の各節表題			下記に列挙した活動を含む計画を繰り返し実行していく仕組み					チェックに至る根拠(資料)を記述(任意)
			— 計画策定					
			— 意思決定及び決定事項の伝達					
			— 決定事項の実施					
			— 結果のフィードバック及び統制策					

チェック項目

必要性
自組織でこの項目が
どの程度必要かを
5段階で選択

達成度
自組織でこの項目が
どの程度できているか
を5段階で選択

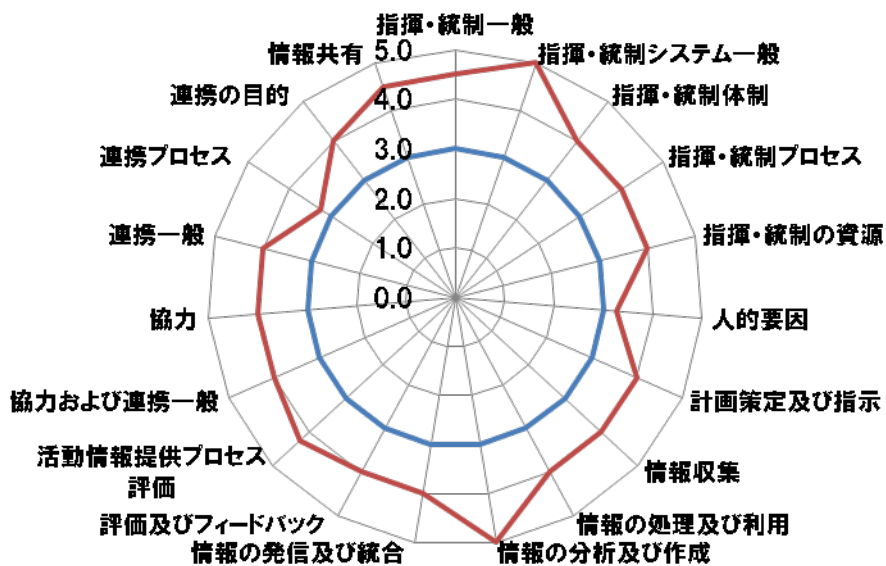
解説	適用しない場合のデメリット
【指揮・統制一般】 危機対応における指揮・統制全体を通じて念頭に置くべき要素である。危機対応組織を機能的に運営するためには、組織毎に適切な資源が用意されているだけでなく、より大規模な危機に対応するために、地域社会との連携が不可欠なることを理解すべきである。	現場単位で必要とする資源・権限を用意されていないければ、即時性を求められる対応が限定され、危機を拡大させる可能性が高くなる。また、広域対応を求められる場合には、地域社会との良好な関係が維持されていないければ、活動を制限される可能性も高い。

節単位に以下を記載
 ・簡単な解説
 ・チェック項目を適用しない場合のデメリット

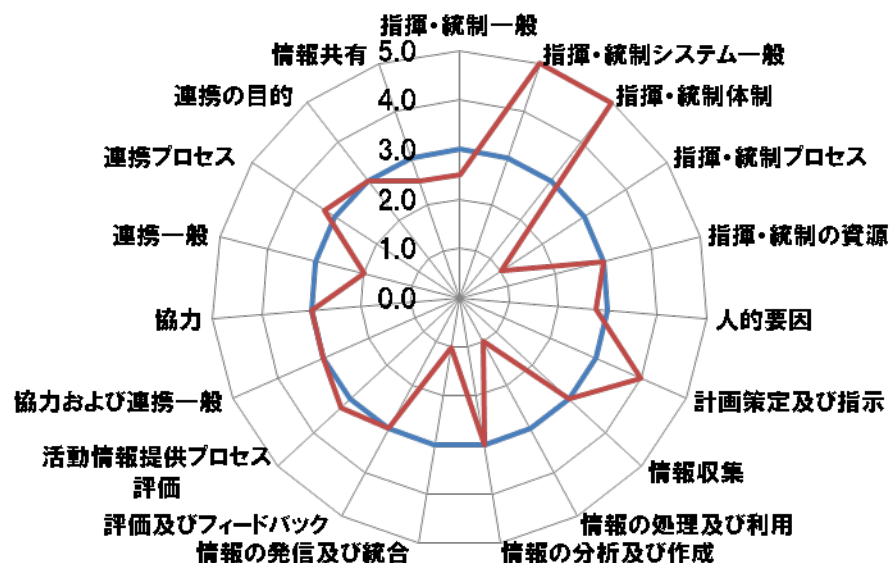
チェック結果の可視化

- 必要性、達成度それぞれを、各節単位の全19軸レーダーチャートで表示
(最低点は1、最高点は5)

必要性 5:高い(必須)～1:低い(不要)



達成度 5:できている～1:できていない



チェックリストの入手先

■ 本格活用に向け、引き続き調査への皆様のご協力をお願いします。

レジリエンス協会Webページ→社会セキュリティ研究会

<https://resiliencej.wordpress.com/research/society/>



2015年5月第1.0版発行
現在、第1.04版を公開中

2. 社会セキュリティ研究会

2017年1月11日更新

【ISO22320簡易版チェックリストについて】

ISO22320(JIS Q22320)は、組織があらゆる危機に対処するための能力を高めることを目的とした国際規格です。

本チェックリストは、皆様の組織の危機対応力を、ISO22320に記載の要求事項をどの程度必要とし充足できているかを簡易なチェックを通じて見える化するツールです。

- ・ISO22320のエッセンスを33個のチェック項目で網羅し、段階別でチェックできます。
- ・どの程度必要か（必要性）とどの程度できているか（達成度）の2つの観点で相対的に評価できます。
- ・レーダーチャートでの見える化により、強み・弱みを直感的に把握できます。

満点を取ることは目的ではなく、自組織の危機対応力の強み・弱みを把握して頂くことを主眼としています。

また、第三者認証規格ではなくセルフチェックとなりますので、組織を代表する見解を問うものでもありません。

むしろ、組織のメンバー間での意識の統一を把握して頂き、危機対応力の改善に役立てて頂くことを目的としています。

【調査へのご協力をお願い】

是非とも本チェックリストを貴組織にて実施して頂き、実施結果をフォームバックして頂ければ幸いです。

添付のチェックリストに必要事項を記入の上、societal-security@lab.ntt.co.jpまで、送信をお願い致します。

調査結果につきましては、匿名として統計的に処理を行った上で本ページにおいて公開させていただきます。

チェックリストはExcel版およびPDF版があります。

チェック項目自体は同一ですので、一方のみの実施で結構です。

Excel版で実施して頂くのが望ましいですが、紙に印刷して実施したい場合はPDF版をご利用ください。

その場合、スキャナ等で取り込んだファイルを上記アドレスまで送信をお願いします。

ご協力のほど、よろしくお願い申し上げます。

【チェックリスト、およびこれまでの調査結果はこちら】

ISO22320簡易版チェックリスト (Excel版) > [22320cl_excel_170110](#)
ISO22320簡易版チェックリスト (PDF版) > [22320cl_pdf_170110](#)
これまでの調査結果(2016年12月末現在) > [22320cl_result_20170110](#)

検索 ...

最近の投稿

2017年9月定例会資料

2017年6月定例会資料

2017年3月定例会資料

2017年1月定例会資料

定例会 2016年11月17日

アーカイブ

2017年10月

2017年8月

2017年4月

2017年2月

2016年12月

2016年10月

2016年8月

2016年3月

2016年2月

2016年1月

2015年11月

2015年9月

2015年7月

2015年6月

2015年4月

2015年1月

2014年11月

2014年6月

チェック結果の返送先
societal-security@lab.ntt.co.jp

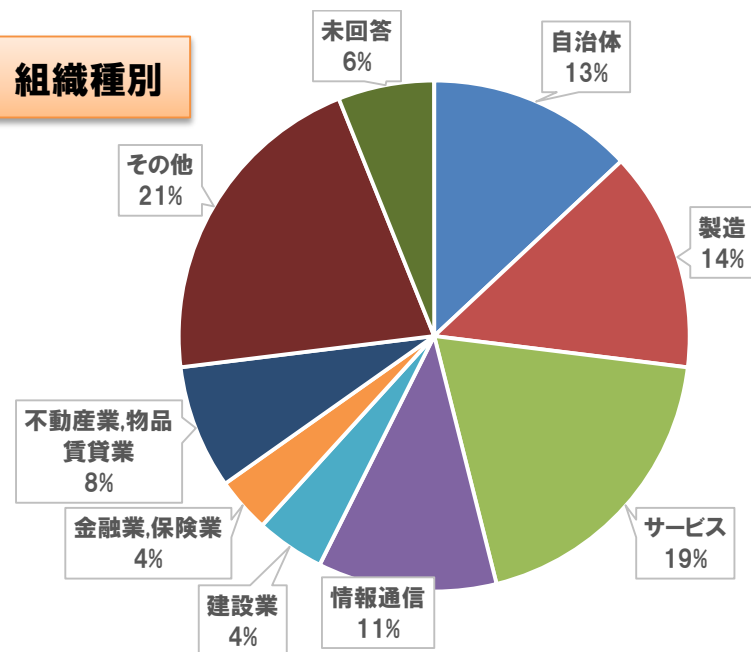
チェックリストのダウンロードリンク
Excel版 (推奨)
PDF版 (印刷実施の場合)

調査と考察

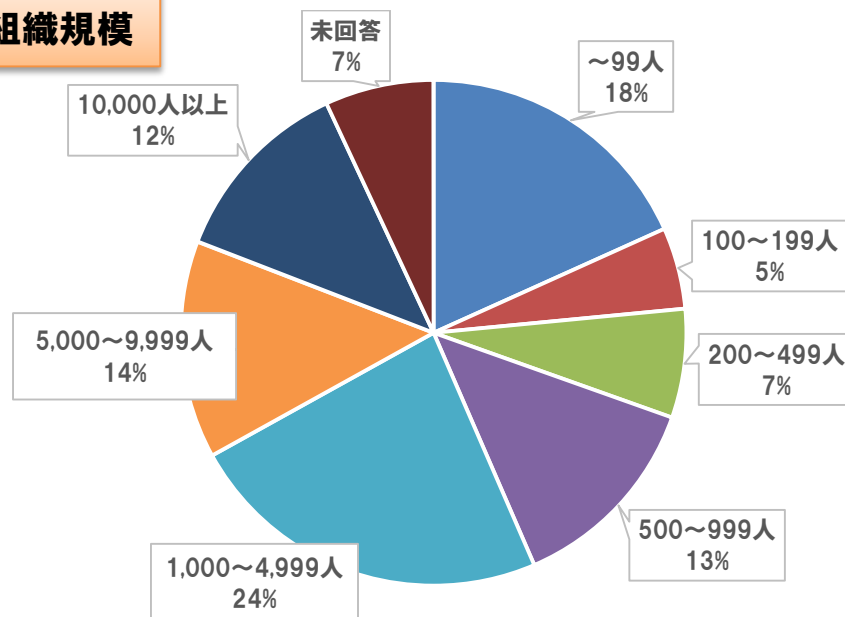
有効回答数: **115**組織
一般募集での回答: 45
各種セミナーで実施: 70

回答者プロフィール(1/2)

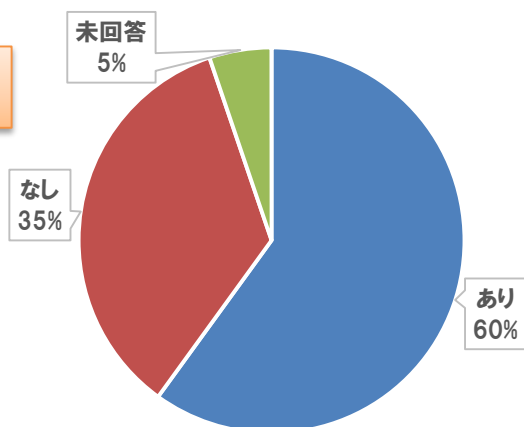
組織種別



組織規模



常設の危機対応部署

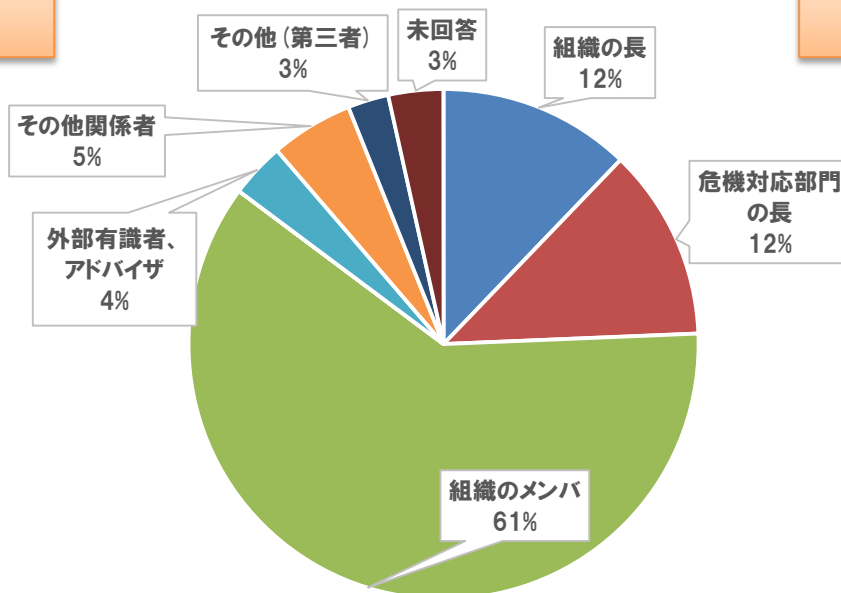


回答者プロフィール(2/2)

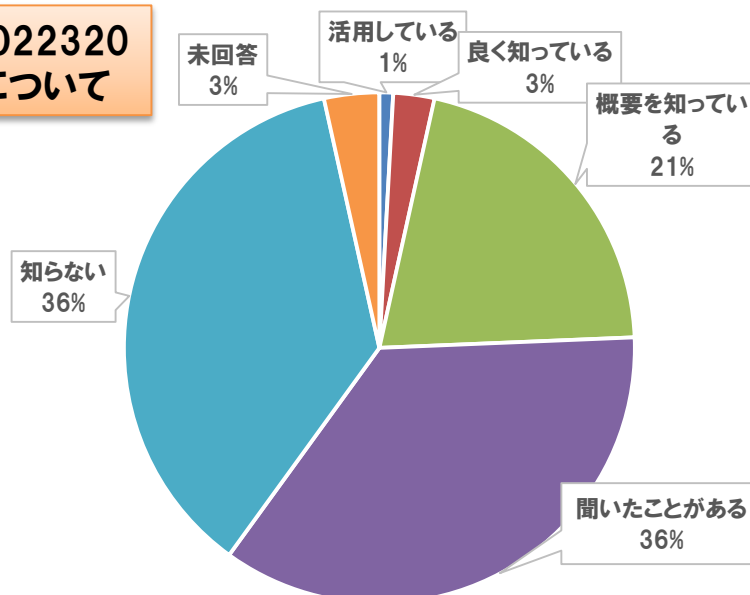
想定している危機・災害事象

項目	内訳	項目	内訳	項目	内訳
自然災害	95.6%	ICT	61.4%	労務	32.5%
感染症	72.8%	製品・サービス	18.4%	法務	31.6%
事故	71.9%	サプライチェーン	13.2%	社会	38.6%
インフラ	61.4%	交通	38.6%	環境	36.0%
テロ・犯罪	50.9%	人権	30.7%	地域	21.1%

チェック担当者の立場



ISO22320について



全体平均



■ 必要性、達成度の差＝組織の危機対応力の弱み

6章：協力および連携

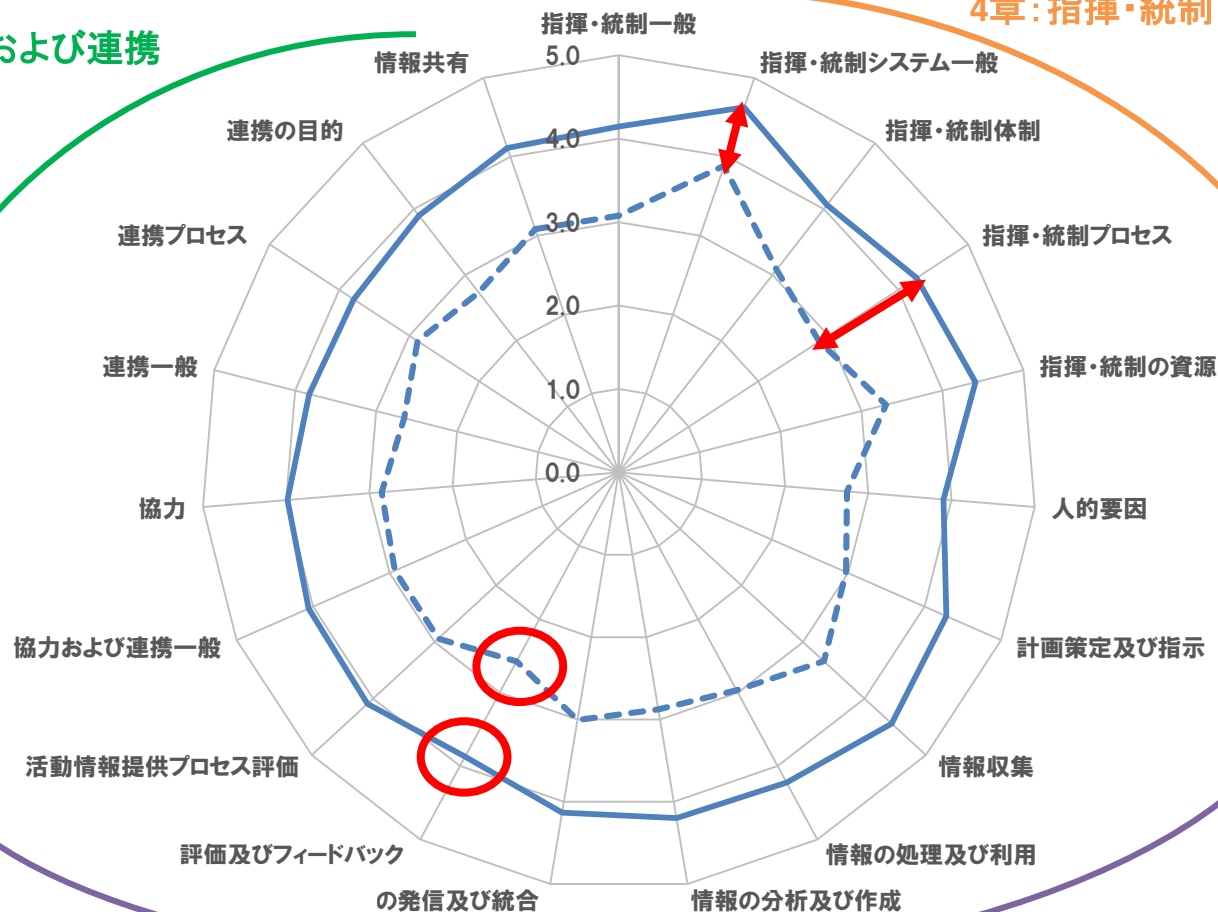
4章：指揮・統制

必要性

5:高い(必須)
～1:低い(不要)

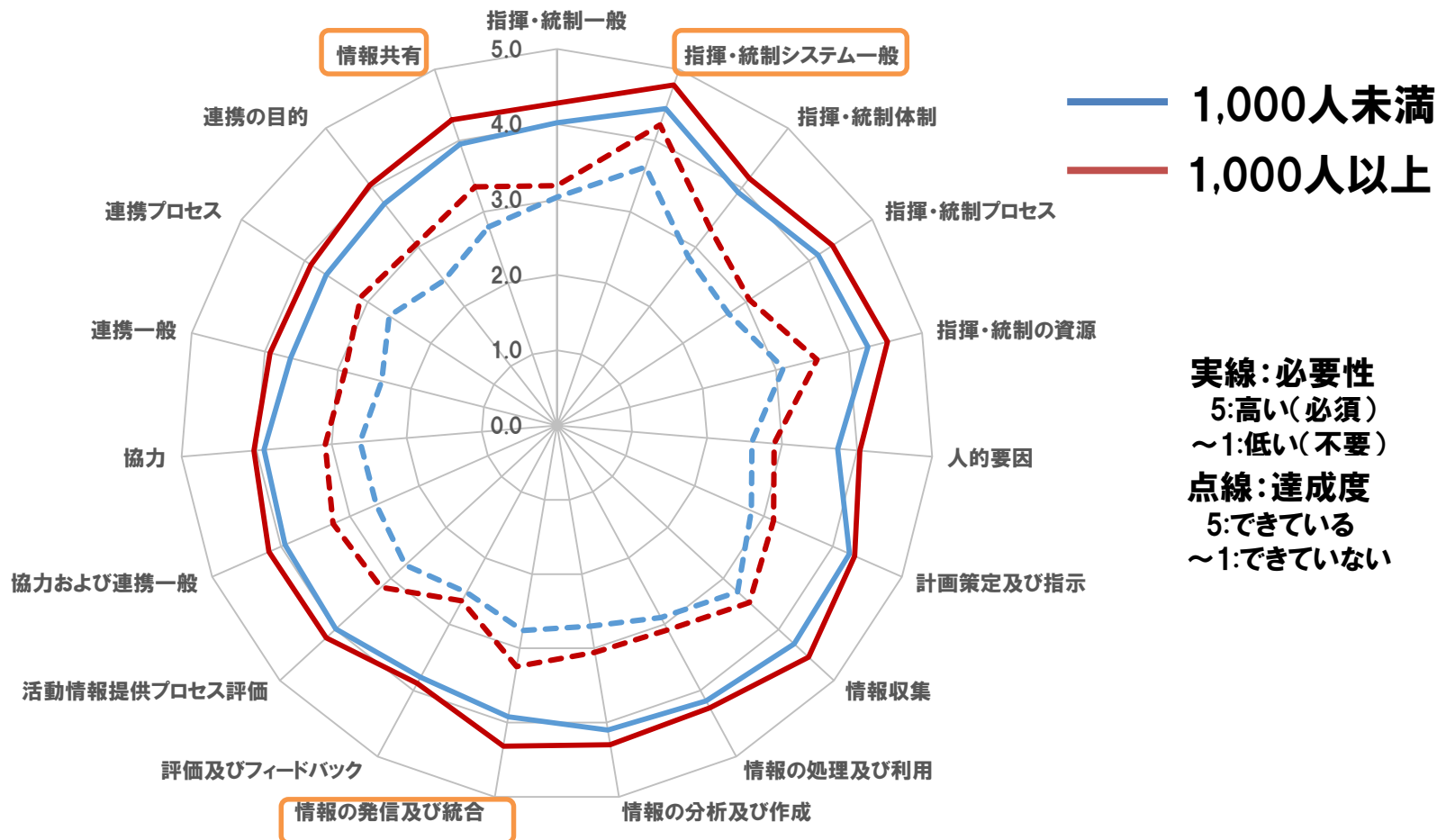
達成度

5:できている
～1:できていない



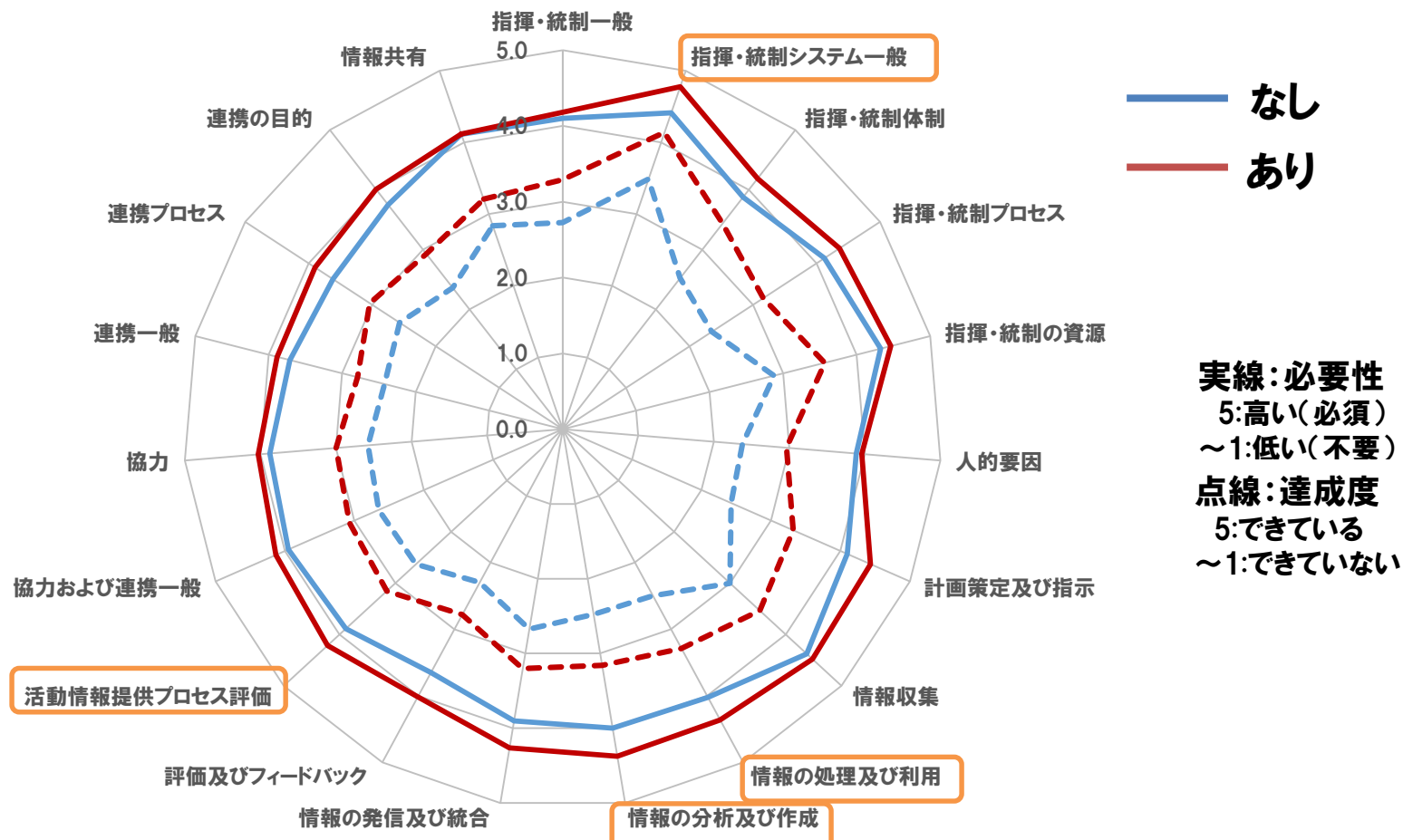
組織規模での比較

■ 協力・連携に関しては、達成度について有意差あり



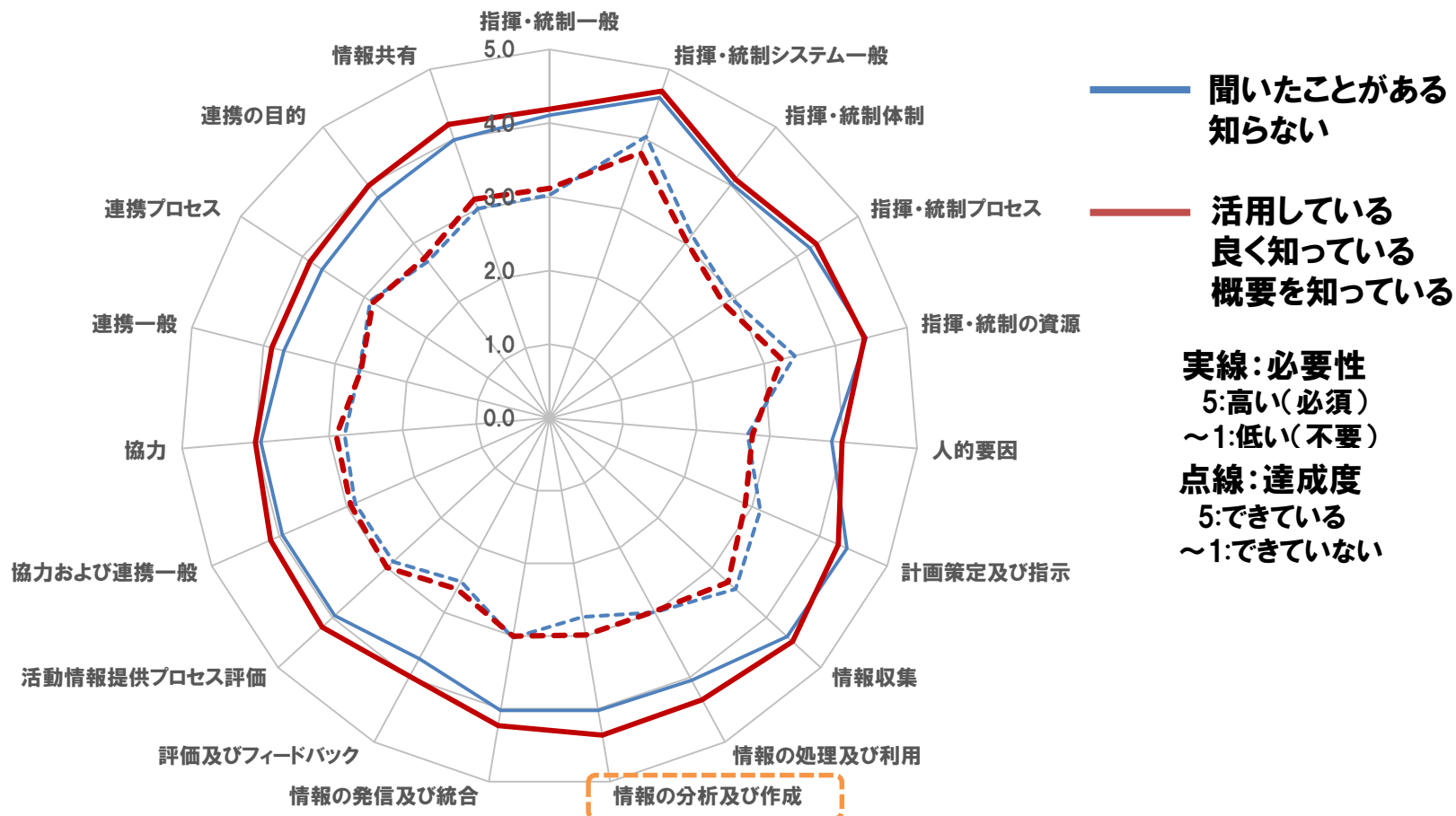
危機対応部署有無での比較

■ 情報処理・分析・評価を中心に有意差あり。達成度は全般に有意差あり



ISO22320に関する知識別比較

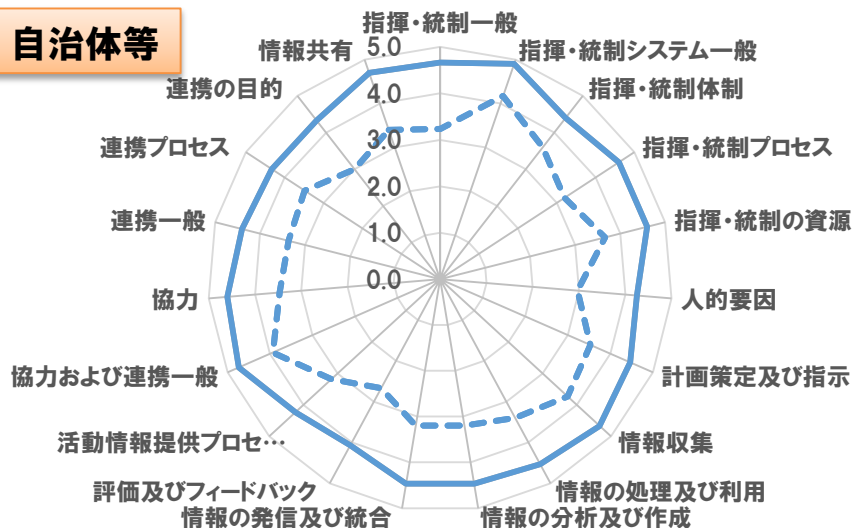
■ ISO規格への知識による有意差はほとんどなし



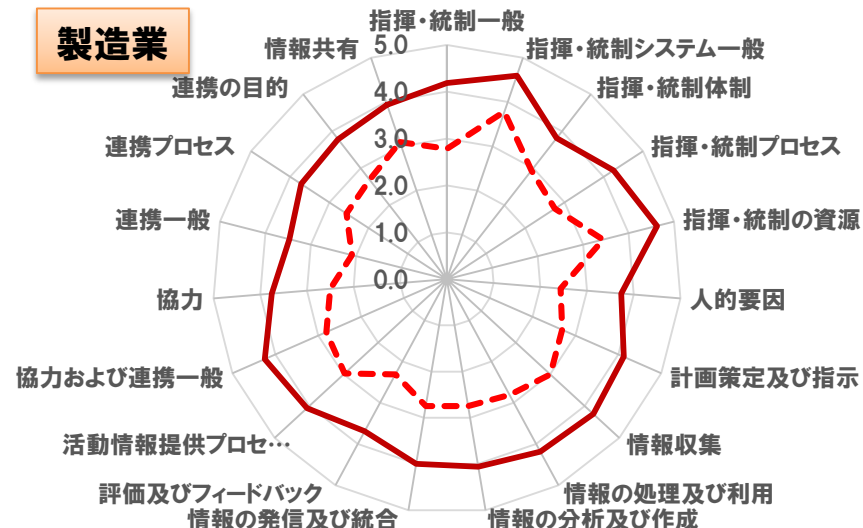
業種別比較



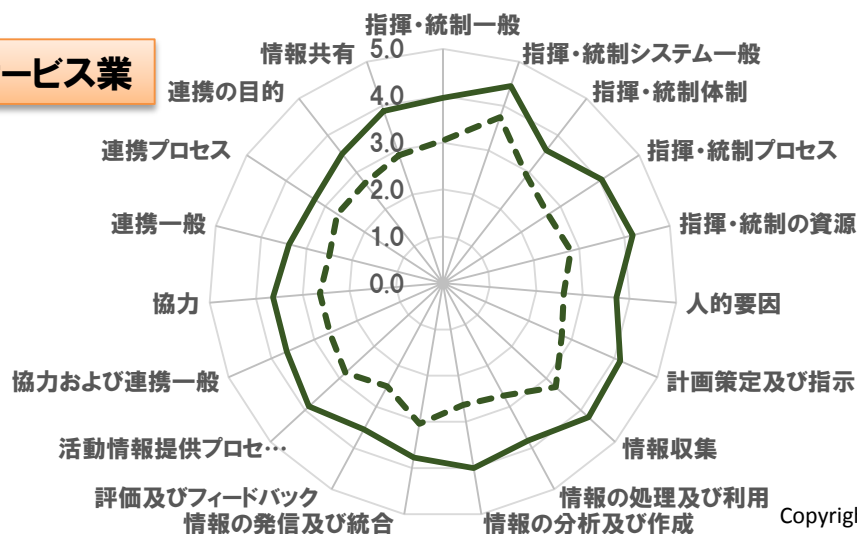
自治体等



製造業



サービス業



実線: 必要性
5: 高い(必須) ~ 1: 低い(不要)

点線: 達成度
5: できている ~ 1: できていない

チェックリスト自体の評価

- 項番1は評価が分散。(主なコメント)チェックする際の何らかの評価基準が欲しい
- 項番2は低評価が多め。(主なコメント)特に5章、6章がわかりづらい
- 項番3～5は概ね高評価。

No.	設問	回答平均	分散
1	必要性、達成度というチェック観点はわかりやすかったでしょうか？	3.4	1.15
2	各チェック項目の内容は理解しやすかったでしょうか？	2.8	1.00
3	本シートの操作は理解しやすかったでしょうか？	3.5	0.95
4	チェック作業そのものは容易だったでしょうか？	3.5	1.08
5	チェック結果のグラフは理解しやすかったでしょうか？	3.6	0.95

普及活動

- レジリエンス協会Webサイトで引き続き公開し、調査継続
 - ✓ 定例会での紹介・報告 (2015年6月、11月)
- メディア記事
 - ✓ リスク対策.comに紹介記事掲載 (2016年1月)
- 学会発表
 - ✓ 日本ファシリティマネジメント大会 (2017年2月、発表者:大成建設 天野)
 - ✓ 情報処理学会 グループウェアとネットワークサービス研究会 (2017年3月) →山下記念研究賞受賞

活用事例

- 本チェックリストを活用した危機対応組織作り
 - ✓ 2017年冬季アジア札幌大会の事例

まとめ

- 本チェックリストを活用することで、組織の危機対応力を可視化
- 全体的な傾向に加え、プロフィールに応じた傾向の違いも見えつつある

今後の予定

- 調査の継続
 - ✓ サンプル数を増やし、プロフィール毎の傾向を明確化
- チェックリストのブラッシュアップ
 - ✓ 項目、評価軸の精査
- 客観評価(評価基準策定)のためのガイドライン整備
 - ✓ ベストプラクティスの収集
- ICT支援に向けた要件抽出