資料４

宇宙システムの抗たん性に関する調査

宇宙システムの脆弱性評価の手法について

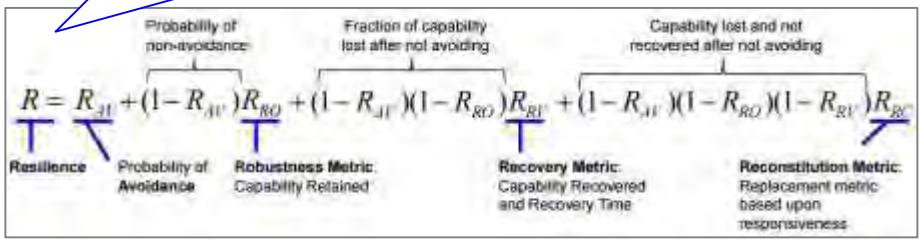
平成29年2月16日

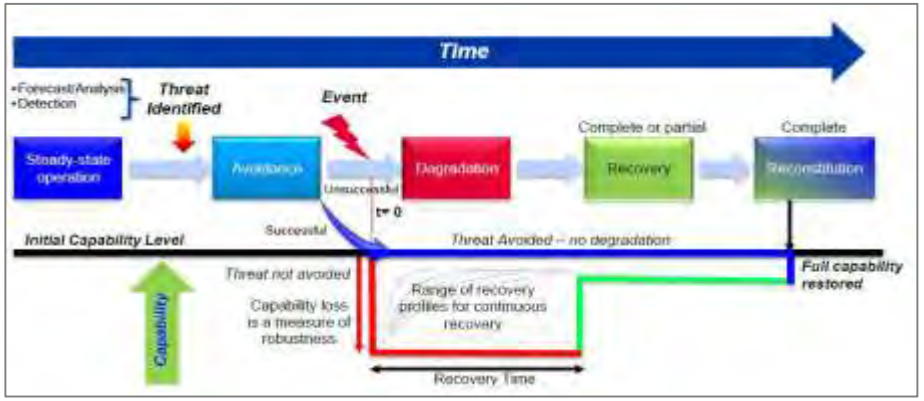
三井物産セキュアディレクション株式会社
有人宇宙システム株式会社

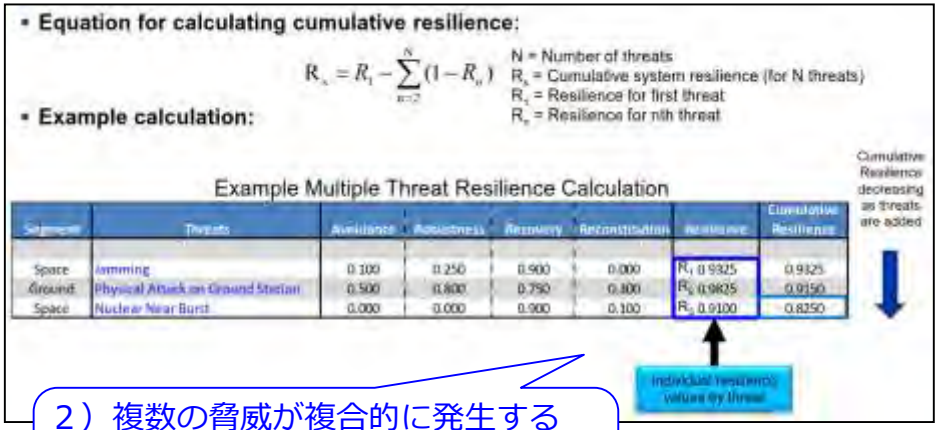
1．評価指標の事例
事例① 米国におけるSpace SystemsのResilience評価指標

- 米国では2011年におけるDoDのレジリエンスに関する定義を受け、宇宙システムについて”Capability Based” な指標について検討している。

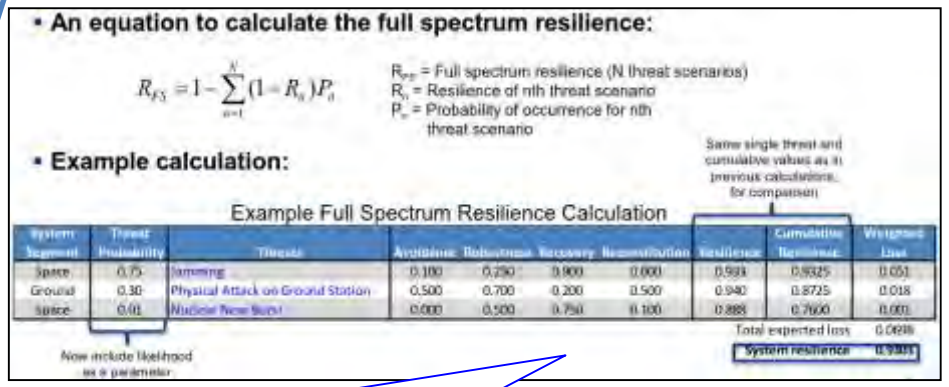
1）単一の脅威が発生した場合に、時系列に沿った４段階の対応毎の対応能力を考慮して抗たん性を計算







2）複数の脅威が複合的に発生するケースを想定した場合には、順に抗たん性の数値を差し引く



3）抗たん性指標に発生確率を掛け合わせることで、各システムのアーキテクチャを比較する

出所）米国NDIA(米国防衛産業協会) ワークショップ資料(Boeing) をもとに作成

1．評価指標の事例
事例② IT分野における共通脆弱性評価システム CVSS（ Common Vulnerability Scoring System)

- ソフトウェアや情報システムに存在する脆弱性の深刻度を評価する手法。システムの種類や開発元の違い、評価者の違い等に対して共通の尺度で深刻度を計測する。米国家インフラストラクチャ諮問委員会 (NIAC:National Infrastructure Advisory Council) のプロジェクトで 2004年10月に原案が作成された。
- 大きく分けて、以下の三種類の指標を0.0から10.0 までの得点で表す。

CVSS
共通脆弱性評価システム

CVSS基本値（base score）	その脆弱性によってどこからどのような攻撃が可能か、どのような影響が起こりうるかなど、脆弱性自体の性質に基づいて評価される指標
CVSS現状値（temporal score）	攻撃される可能性や、対応策や修正プログラムなどが利用可能か、脆弱性情報の信頼性など、その脆弱性の現在の状態によって評価される指標
CVSS環境値（environmental score）	攻撃を受けた際の二次被害の可能性や影響を受ける対象の範囲、対象システムの機密性などの要求度合いなどによって評価される指標

3.1 CVSS 基本値 (Base Score)

影響度 = 10.41×(1 - (1 - C)×(1 - I)×(1 - A)) …式(1)

攻撃容易性 = 20×AV×AC×Au …式(2)

f(影響度) = 0(影響度が0の場合) , 1.176(影響度が0以外の場合) …式(3)

基本値 = ((0.6× 影響度)+(0.4× 攻撃容易性)-1.5)×f(影響度) …式(4)
（小数点第 2 位四捨五入）

C：機密性への影響
I：完全性への影響
A：可用性への影響
AV:攻撃元区分
AC：攻撃条件の複雑さ
Au：攻撃前の認証要否

3.2 CVSS 現状値 (Temporal Score)

現状値 = 基本値 ×E×RL×RC （小数点第 2 位四捨五入） …式(5)

E：攻撃される可能性
RL：利用可能な対策のレベル
RC：脆弱性情報の信頼性

3.3 CVSS 環境値 (Environmental Score)

調整後影響度 =	min(10.0,10.41×(1-(1-C×CR)×(1-I×IR)×(1-A×AR))) …式(6)
調整後現状値 =	式(3)式(4)の影響度に、式(6)の調整後影響度の計算結果を代入し、基本値を再計算する。その基本値で式(5)の現状値を再計算する。 …式(7)

環境値 =(調整後現状値 +(10- 調整後現状値)×CD)×TD …式(8)
（小数点第 2 位四捨五入）

CR:機密性の要求度
IR：完全性の要求度
AR：可用性の要求度
CD：二次的被害の可能性
TD：影響を受ける対象システムの範囲

出所）IPA，共通脆弱性評価システムCVSS概説 http://www.ipa.go.jp/security/vuln/CVSS.html をもとに作成

1．評価指標の事例
事例③ 防災／事業継続計画(BCP)分野におけるチェックリスト

- 企業・組織の災害時における事業継続計画(BCP)の策定や平常時からの事業継続マネジメント(BCM)への取り組みに当たっては、その実施状況を日頃から確認していくことが重要である。
- 我が国でも内閣府 防災担当において平成17年に「事業継続ガイドライン –あらゆる危機的事象を乗り越えるための戦略と対応-」が策定され、その中で経営者自らがチェックリストを活用し、企業・組織の自主的な取り組みを把握・推進すべきとされている。

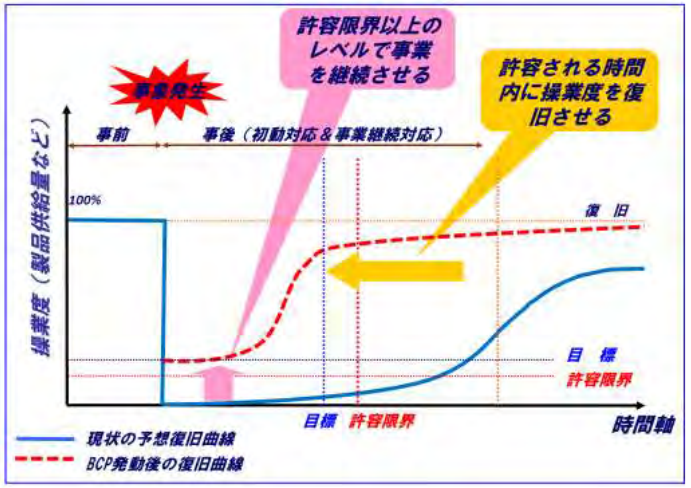


図 BCPの概念

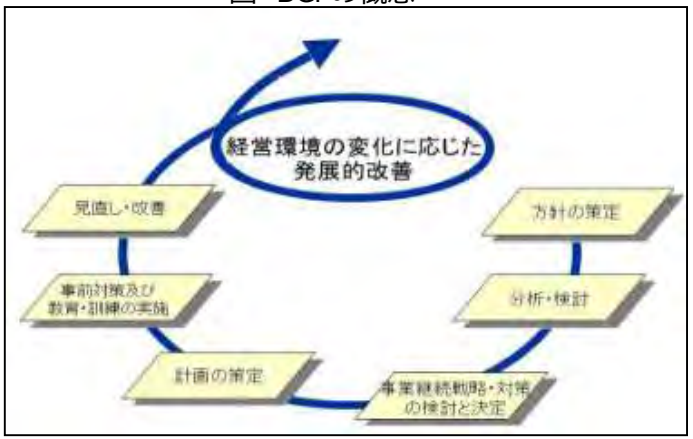


図 事業継続マネジメント(BCM)の流れ

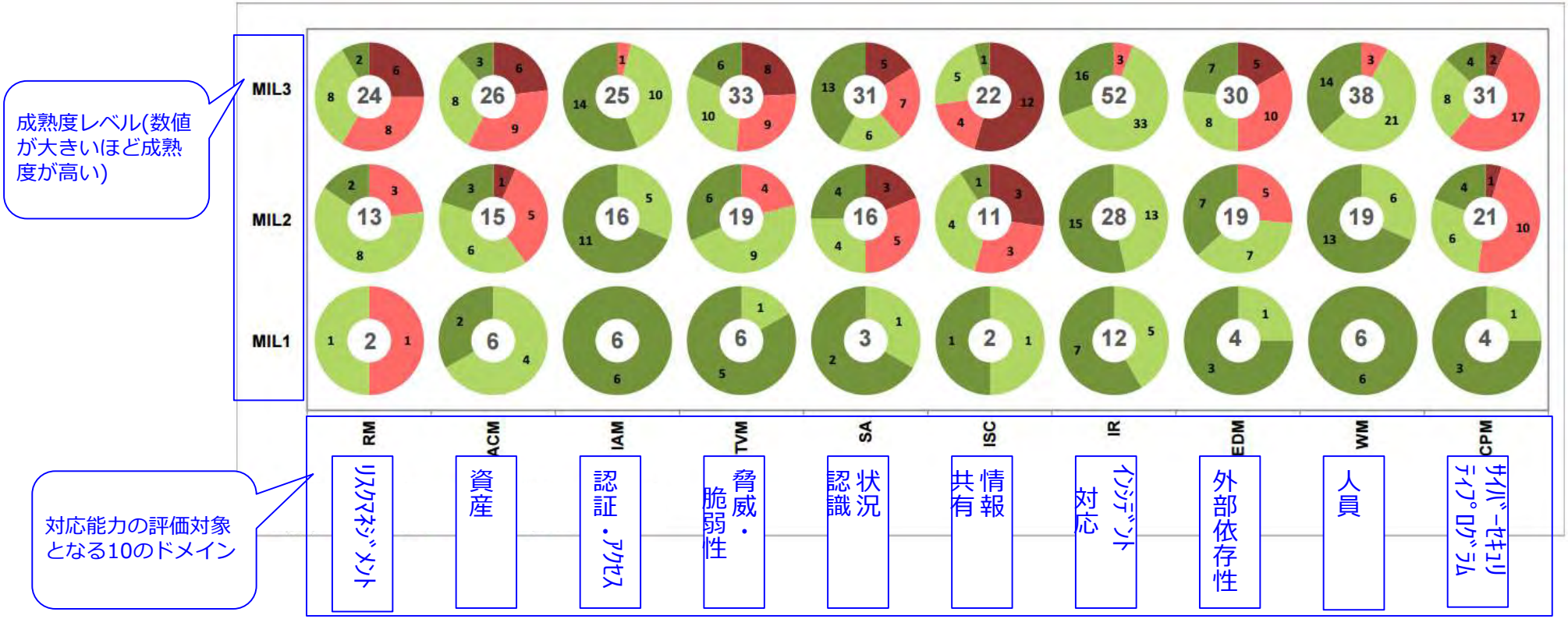
<事業継続ガイドライン チェックリスト>（ヘッダ項目のみ抜粋）

1. 経営者に求められる事項
2. 事業継続に対する基本方針を策定
3. 事業継続マネジメント（BCM）実施体制の構築
4. 事業中断による影響度の評価
5. 重要業務の決定と目標復旧時間、目標復旧レベルの検討
6. 重要な要素の把握とボトルネックの抽出
7. リスクの分析・評価
8. 事業継続戦略・対策の基本的考え方
9. 重要製品・サービスの供給継続・早期復旧
10. 企業・組織の中枢機能の確保
11. 情報及び情報システムの維持
12. 資金確保
13. 法規制等への対応
14. 行政、社会インフラ事業者の取組との整合性の確保
15. 地域との共生と貢献
16. 緊急時の体制
17. 緊急時の対応手順
18. 事前対策の実施計画
19. 教育・訓練の実施計画と実施
20. 見直し・改善の実施計画
21. 計画等の文書化
22. 事前対策の実施
23. 事業継続計画（BCP）が本当に機能するかの確認
24. 事業継続マネジメント（BCM）の点検・評価
25. 経営者による見直し
26. 是正・改善
27. 継続的改善

出所）内閣府防災，「事業継続ガイドライン –あらゆる危機的事象を乗り越えるための戦略と対応-」(平成25年8月改訂)をもとに作成

1. 評価指標の事例
事例④ 米国 CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)

- 組織内におけるサイバーセキュリティへの対応能力について成熟度を評価する指標。
- 2012年に作成された、電力業界を対象とするES-C2M2(Electricity Subsector Cybersecurity Capability Maturity Model)をベースに、様々な組織や業界で利用できるようC2M2として汎用化された。
- C2M2により自己評価を行うことでサイバーセキュリティの能力をベンチマークし、必要な投資の優先順位付けを行う。また組織においてNIST Cyber Security Frameworkの適用を支援するものである。



出所）米国エネルギー省(DOE)，CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2),
https://www.energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity

1．評価指標の事例
事例⑤ 米国におけるTarget Capability List (TCL)

- 2003年に米国大統領が発行した “Homeland Security Presidential Directive (HSPD-8)” を受け、米国におけるテロ攻撃、大規模災害、その他緊急事態へ備えるための「目標とする能力」とそれらの「優先順位」を示すもの。

Capability(能力)の定義：
厳しい条件のもと困難な達成目標レベルに対して、任務を遂行し求められる成果を獲得する手段。要素として、計画（情報収集・分析・手順・マニュアル）／組織（リーダーシップ）／人員確保／装備やシステム（任務・役割分担等）／トレーニング(演習・評価・改善活動)がある。

TCLには37のCore Capabilities(コア能力)が含まれている。
一例として、”Communication” では以下のようなタスクや指標が示されている。

15 の国家の計画策定上のシナリオ	
1. Improvised Nuclear Device	簡易核兵器（テロを想定）
2. Aerosol Anthrax	炭疽菌の空中散布
3. Pandemic Influenza	インフルエンザの大流行
4. Plague	ペスト
5. Blister Agent	びらん剤
6. Toxic Industrial Chemical	工業化学物質による中毒
7. Nerve Agent	神経ガス
8. Chlorine Tank Explosion	塩素タンクの爆発
9. Major Earthquake	大地震
10. Major Hurricane	大規模なハリケーン
11. Radiological Dispersal Device	放射性物質散布装置
12. Improvised Explosive Device	簡易爆弾
13. Food Contamination	食品への異物混入
14. Foreign Animal Disease	外来動物の疾病
15. Major Cyber Attack	大規模サイバー攻撃

Activity: *Develop and Maintain Plans, Procedures, Programs, and Systems*	
Critical Tasks	
ComC 1	Develop communication plans, policies, procedures, and systems that support required communications with all Federal, regional, State, local, and tribal governments and agencies as well as voluntary agencies
ComC 1.2.1	Develop procedures for the exchange of voice and data with Federal, regional, State, local, and tribal agencies, as well as voluntary agencies
ComC 1.6	Develop supplemental and back-up communications and information technology plans: procedures, and systems
Preparedness Measures	**Metrics**
Operable communications systems that are supported by redundancy and diversity, that provide service across jurisdictions, and that meet everyday internal agency requirements, are in place	Yes/No
Communication systems support on-demand, real-time interoperable voice and data communication	Yes/No
Plans and procedures are in place to ensure appropriate levels of planning and building public safety communication systems prior to an incident	Yes/No

出所）Target Capabilities List, https://www.fema.gov/pdf/government/training/tcl.pdf

1．評価指標の事例
事例⑥ 米国におけるIncident Management Capability Metrics (IMCM)

- 米国 国防総省 (DoD)、 国土安全保障省 (DHS)、およびUS-CERT等の機関によって作成された、組織におけるセキュリティ事案に対するインシデント管理手法（保護、検出、対処、改善）の基準を示したもの。
  セキュリティ事案が発生した際の対処よりも管理に重点を置く。
- Incident Management Capability Metrics (IMCM) では、インシデント管理能力を四つの主要な機能に分類するとともに、質問形式でのチェックリストを提供する。

Protect(予防)	Detect(検出)	Respond (対処)	Sustain(維持)
• リスクアセスメントのサポート • マルウェア保護のサポート • CNDの対処訓練 • 各部署における保護とトレーニング • 情報保証と脆弱性の管理	• ネットワーク・セキュリティのモニタリング • 検知・警報と状況の把握	• インシデント報告 • インシデント対処 • インシデント分析	• 契約・覚書 • プロジェクト／プログラム管理 • CNDの技術開発と適用 • 人事 • セキュリティ管理 • CND情報システム • 脅威レベルの適用

注) CND：Computer network defense（コンピュータ・ネットワーク防御）

出所）Incident Management Capability Metrix,
https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14873.pdf

Incident Management Capability Metrics

1.2 Malware Protection

1.2.1	Is there an institutionalized Malware/Anti-Virus (AV) Program?	Priority I	
Not observed ☐	Not applicable ☐	• There is an institutionalized Malware/Anti-Virus Program that includes installed AV software and automated updates, documented guidance for preventing, detecting, reporting, and handling malware activity.	Y ☐ N ☐

Prerequisites
- ☐ List of constituent critical assets and data [R]

Controls
- ☐ Documented policies and procedures exist that describe the process and method by which this program is provided to the constituents, including notifications, alerts, and remediation assistance [R]
- ☐ Documented policies and procedures exist that define reporting requirements when malware is discovered including working with vendors or other external entities
- ☐ Personnel are appropriately trained on the procedures, process and supporting technologies used to identify, analyze, and remediate malware [R]

Activity
- ☐ A current list of POCs for notifications and alerts is maintained
- ☐ Sources for information on emerging malware (e.g., FIRST, CERT/CC, vendor anti-virus sites, and other similar organizations) are reviewed
- ☐ The impacts of malware on constituent systems are analyzed
- ☐ Constituents are alerted to emerging or current malware threats [R]
- ☐ Remediation, response, and recovery solutions to malware occurrences and threats are provided [R]
- ☐ Documented anti-malware installation & update procedures are provided to appropriate personnel
- ☐ Constituents are advised of sources for anti-malware signature updates
- ☐ Malware outbreaks and remediation are tracked and recorded [R]
- ☐ US-CERT and other anti-malware organizations are coordinated with on the development of countermeasures

Supporting Mechanisms
- ☐ Available, approved anti-malware software is used in accordance with organizational requirements [R]
- ☐ Automatic update mechanisms for patch and remediation [R]
- ☐ Web site for posting anti-malware files for constituents to download
- ☐ Alerting and dissemination mechanisms such as email lists or web sites [R]

Artifacts
- ☐ Up-to-date POC list with individual names and phone numbers
- ☐ Example of virus infection reports and statistics [R]
- ☐ Recent email or web malware warnings and advisories [R]
- ☐ Recent information from vendors on products and/or services on file

Quality
- ☐ Personnel are aware of, knowledgeable of, and consistently perform the procedures, processes, methodologies, and technologies for performing this task [R]
- ☐ There is a process and criteria for evaluating the quality of performance and artifacts associated with this activity [R]
- ☐ The quality and effectiveness of this activity are periodically evaluated and appropriate improvements are made [R]
- ☐ Malware is reported to appropriate parties within required timeframe of discovery
- ☐ Malware incidents are handled in a timely manner

質問形式で提示

Ⅰ～Ⅳの優先度を明示

スコアとしてカウント

複数の観点からのチェックリストを提供

2. 抗たん性強化へ向けた対策オプションの視点

- 宇宙システム全体の抗たん性強化へ向けては、考えられる複数の対策オプションを列挙の上、システムの特性や対策の費用対効果等を考慮して適用していくことが必要ではないか。

＜抗たん性強化へ向けたチェックリストの視点例＞

✓ 対象システムは被害を受けても極力機能を継続できる能力を確保しているか
（分散アーキテクチャの採用、相互運用性の確保等）

✓ 対象システムは被害を回避・防護できるような能力を確保しているか
（耐妨害技術の採用、冗長構成、物理セキュリティ・サイバーセキュリティの確保等）

✓ 対象システムに関係するステークホルダー間にて、抗たん性能力を継続的に確保できる体制が整備されているか
（定期的な演習や訓練の実施、対応計画の策定や見直し、教育・訓練プログラムの実施等）