社会インフラシステムにおける
可用性維持に注力したセキュリティ対策立案手法の提案

松原 佑生子† 太田原 千秋† 熊谷 洋子†
甲斐 賢† 谷川 嘉伸†

†日立製作所 横浜研究所
244-0817 神奈川県横浜市戸塚区吉田町 292 番地
yukiko.matsubara.hq@hitachi.com

あらまし 本稿では，社会インフラシステム向けに，可用性の維持を重視したセキュリティ対策の立案手法を提案する．提案手法では，対象システムの業務フローと対策候補に付与する可用性の指標を新規に定義し，業務フローの可用性維持の条件と対策候補に見込める可用性の性能を評価した上で，実施すべき対策を選定する．これにより，定量的かつ客観的な評価が可能となり，より確実なシステムの可用性確保が可能となる．

A Proposal of Security Planning Method
in Social Infrastructure System

Yukiko Matsubara† Chiaki Otahara† Yoko Kumagai†
Satoshi Kai† Yoshinobu Tanigawa†

†Hitachi, Ltd., Yokohama Research Laboratory
292 Yoshida-cho, Totsuka-ku, Yokohama-shi, Kanagawa-ken, 244-0817 JAPAN
yukiko.matsubara.hq@hitachi.com

Abstract In this paper, we propose a method of planning security measures focusing on maintaining the availability for the social infrastructure system. In the proposed method, we define a new indicator of the availability and evaluate the required value of business flow of the target system and expected value of performance of measure candidate. This approach enables more quantitative and objective evaluation of the availability, and ensures more secure availability of the system.

1 はじめに

近年，社会インフラシステムの開発や保守の分野では，メーカーごとに独自仕様の機材やソフトウェアで構成されたシステムを，標準規格や業界標準に則り複数のメーカーの製品を組み合わせて構成し直すオープン化が進んでいる．一方，サイバー攻撃の報告数は年々増加しており[1][2]，北米の電力事業者向けセキュリティ基準である NERC CIP をはじめ様々な国際・業界標準規格においてリスクマネジメントが要求さ

れるなど，オープン化と共に社会インフラシステムへのセキュリティの意識は世界的に高まっている[3].

これを受け本稿では，制御セキュリティで最も重視される可用性の確実な維持を目的に，社会インフラシステムにおける新たな対策立案手法を検討した結果を報告する.

2 セキュリティ対策立案手法の現状と課題

本章では，社会インフラシステムにおける従来のセキュリティ対策立案手法とその問題点・課題について述べる．なお本稿では，これ以降'業務フロー'という言葉を，自動手動を問わず，業務を遂行するために必要なアクタ同士のやりとりや情報の流れ等を全て含んだ業務手続きの処理手順という意味で使用する.

2.1 セキュリティ対策立案の手順

従来のセキュリティ設計における，セキュリティ対策立案までの一般的な流れは以下の通りである[5].

S1 情報収集および評価対象の定義
S2 脅威分析・リスク評価
S3 対策立案（対策候補の列挙・選定）

まず，システム構成や前提条件など対象システムに関する必要な情報を収集し，機器やネットワーク，事業拠点などシステム構成要素におけるセキュリティ評価対象を定義する（S1）．次に，これらの間でやりとりされる資産のセキュリティ特性すなわち機密性・完全性・可用性を喪失させる脅威を抽出し，リスク発生時の影響の大きさを評価する（S2）．次にこの結果に基づきセキュリティ評価対象（対策実施箇所）ごとに対策候補を列挙し，対策の方針や要件を決定した上で，これらの選定を行う（S3）.

2.2 セキュリティ特性の優先順位

電子計算機により高速に情報処理を行うシステムには，大きく分けて情報システムと制御システムの二つの系統がある．情報システムは主に情報の収集・蓄積・処理・伝達・利用を行い，制御システムは主に他の機器やシステムの動作の管理・指示・制御を行う．列車運行管理システムやスマートグリッドシステムに代表される社会インフラシステムは，制御システムの性質を強く持っている.

二つの系統ではセキュリティ特性の優先順位も異なり，一般的に情報システムでは機密性が最も重視される一方，制御システムでは可用性，可用性，特に業務フローの可用性が最も重視される[4]．ここで，可用性とは要求された機能を常に提供できる状態であることから，業務フローの可用性が維持されている状態とは，業務フローの正常実行が可能な状態と捉えることができる.

2.3 従来手法の問題点

システムのセキュリティ対策立案は，2で述べた通り脅威分析・リスク評価の結果を元に行われる．しかし，制御システムにおける可用性重視の対策立案プロセスについては現在明確な基準やガイドライン等が存在せず，最終的に選定された対策について可用性維持に関する網羅性・確実性を客観的に評価することは難しい．このため，検討に見落としがあった場合にはシステムに大きな脆弱性を残してしまう可能性がある.

通常，セキュリティ設計ではシステム全体で複数の対策が立案される．これらの対策の間には，ある対策を実施すると，別の業務フローにおける対策や業務フローの実行そのものを妨害するといった矛盾する関係もある．一例として，ある業務フローに対して立案した対策が，フロー経路として一部の機器を共有する別の業務フローの可用性喪失を引き起こす事態が挙げられる．例えば，3 日に一度実行する業務フローⅠと連日 3 分に一度実

行する業務フローⅡが，共に機器 M をフロー経路に持っていたとする．このとき，業務フローⅠで扱う機器M内で処理される資産aの機密性喪失の脅威に対し，‘業務フローⅠの実行毎に，機器Aの稼働を5分間停止し資産aの情報を更新する’という対策を実施するとする．この場合，業務フローⅡの可用性は喪失する．

こういった事態の発生は，セキュリティ評価対象（対策実施箇所）ごとに対策立案を行った後，それらを実施した場合の他の機器や業務フローへの影響を充分に確認しないまま検討を終えてしまうことに起因する．しかし，現在一般的なセキュリティ評価基準にはそこまでの作業を明確に示したものは存在しない．加えて，特に可用性の点では，社会インフラシステムでは複雑にコンポーネントが絡むため対策同士の矛盾を解消することが難しく，結果として検討漏れを招きやすい状況となっている[6].

2.4　問題解消に向けた課題

2.3で述べた問題の解消には，可用性維持に関する定量的かつ客観的な評価方式およびこれを利用した対策立案手法の確立が課題となる．次章より，これらを解決する手法について述べる．

3　提案手法の基本方針

3.1　提案手法の手順概要

本稿で提案する手法の概要を述べる．本手法では可用性評価の指標を新たに定義し，対象システムの業務フローに必要とされる可用性の程度および立案候補に見込める可用性の程度を数値化する（それぞれ可用性要値，可用性期待値と呼ぶ）．この上で，同一の対策実施箇所を経路にもつ全ての業務フローの可用性要求値について，それらを上回る可用性期待値を持つ対策候補を選定する．

このような方法をとることで，実施される対策の影響を受ける全ての業務フローについて可用性の確保が可能となる．

3.2　可用性維持要件の考え方

本稿で提案する手法では，可用性の維持に関して「レジリエンス」という考え方を導入する．これは内閣官房における事前防災・減災の取組で，経済社会のシステムの在り方として推進されており，“国や地域の経済社会に関わる分野を幅広く対象にして，経済社会のシステム全体の「抵抗力」，「回復力」を確保”し，“いかなる事態が発生しても機能不全に陥らない経済社会のシステム”の実現を目的とした“国家のリスクマネジメントの基本”となる概念である[7].

本稿では，機能不全に陥らないという理念をシステムに適用させた場合，可用性維持と同様に捉えることが可能との考えの下に検討を進める．従って，システムの可用性維持の要件は“「抵抗力」と「回復力」”となる．次章で，可用性評価の指標の定義と共にこの要件の具体化を行う.

3.3　可用性評価の方針

防災・減災におけるレジリエンスでは，縦軸を社会機能の低下の度合い，横軸を時間にとったグラフにおいて，ハザードに対する社会の脆弱性を「被害の大きさ」と「復旧時間の長さ」に当たる辺から成る三角形で表すモデルがある[8][9]（図 1参照）．被害を抑止できるハザード前の備えを“抵抗力”，復旧時間を短縮できる早期復旧の体制整備を“回復力”として，「被害の大きさ」と「復旧時間の長さ」の辺を短くし三角形の面積を減らす取り組みが，レジリエンスの実現につながると考えられている．

本稿ではこのモデルを参考に，縦軸を業務フローの安全性の度合い（安全レベル），横軸を時間にとったグラフにおいて，以下の 2 つを図形で表現する．

A) 業務フローの可用性喪失（実行停止または異常実行）時の影響の大きさ
B) 業務フローにおいて実施されるセキュリティ対策（機密性・完全性・可用性用全て）に見込まれる効果

AとBの図形を構成する辺の設定についてはで4で詳しく述べる．なお，一つの業務フローに対して実施される対策は一つとは限らないため，1つのAに対しBは複数ある場合もある．

AにBを重ねた際，Bが覆うことのできるAの面積を3.2で述べた「回復力」，Aを覆っているB領域の総面積を「抵抗力」に相当する指標とする．

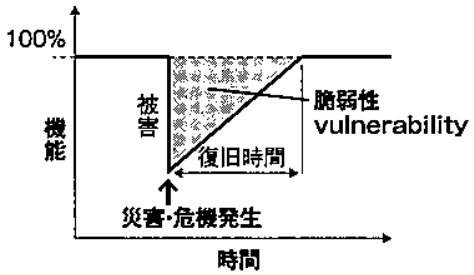

図 1：レジリエンスモデル（[8]より転載）

4 可用性の評価

本稿で提案する手法で用いる可用性の評価指標および評価方式について述べる．

4.1 可用性指標

本手法では，業務フローの可用性の評価指標として以下の2つを定義する．

R値（Required value of availability）：
業務フローに要求される可用性の程度を表す値．次の3つから成る．

- R_SL (Required Safety Level)：
  業務フローに要求される安全性の程度（異常稼働時や停止時の影響度または危険度）
- R_TP (Required Time to Prepare)：
  業務フローの一時停止が許される時間
- R_TO (Required Time of Operation)：
  業務フローに期待される継続稼働時間

E値（Expected value of availability）：
業務フローに対して実施されるセキュリティ対策が備える可用性に関する性能を表す値．次の3つから成る．

- E_SL (Expected Safety Level)：
  対策の実施によるR_SLの回復度
- E_TP (Expected Time to Prepare)：
  対策実施の準備に必要な時間
- E_TO (Expected Time of Operation)：
  対策の効果が持続する時間

4.2 システム状態図

本手法では，業務フローの可用性に関するシステムの状態をR値およびE値を用いたいくつかの図によって表現する．本節では，評価に用いる図で最小単位となる3つの図を定義する．

DS図（Dangerous State）：
ある対策の実施対象となる業務フローについて，セキュリティ対策が未実施である場合の危険な状態を表す図．3.3で述べたA)に該当する．縦軸をシステムの安全レベル(SL)，横軸を時間として R_SL×(R_TP＋R_TO)の四角形で表す．

図 2に，例として R_SL=6，R_TP=3，R_TO=8 であるDS図を示す．直観的には，黒く塗られた領域が危険な状態を表す．

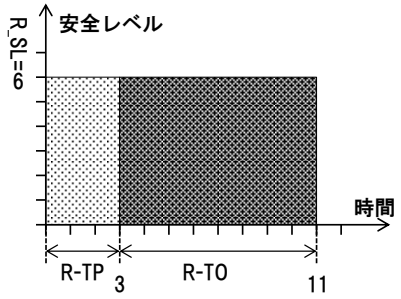

図 2： DS図の例

対策の実施対象となる業務フローが複数ある場合は，各業務フローのうち最大の

R_SL，最小の R_TP，最大の R_TO，つまりR値のうち最も厳しい値をとって作成する．例えば，R 値が {R_SL=2, R_TP=4, R_TO=8}，{R_SL=3, R_TP=3, R_TO=7}，{R_SL=5, R_TP=6, R_TO=6} である 3 つの業務フローを統合した DS 図の各値は R_SL=5, R_TP=3, R_TO=8 となる. なお，この値を以後統合 R 値と呼ぶ.

MS 図（Measure State）：

対象となる業務フローに対策を実施した場合に見込まれる安全性の程度を表す図. 3.3 で述べたB)に該当する．縦軸をシステムの安全レベル(SL)，横軸を時間として時間 0 から E_TP だけ経過した時点からはじまる E_SL×T_TO の四角形で表す.

図 3に，例として E_SL=7，E_TP=2, E_TO=10 である業務フローのMS図を示す. 直観的には，斜線の入った領域が安全状態を表す.

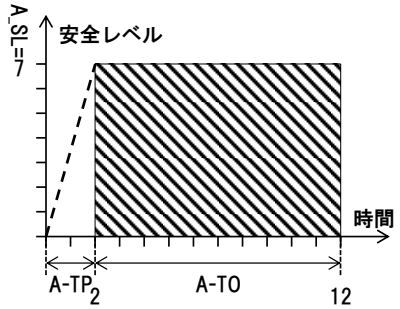

図 3： MS 図の例

DMS 図：

一個若しくは複数個の対策の MS 図と，対策の対象となる業務フローの DS 図を重ねた図．対策の評価に用いる.

システムの新規開発や刷新の際に配備する対策を評価する場合は，これらの効果の発揮開始時点が同じ（システム運用開始時点）であるため，各対策の MS 図および適用対象となる業務フローの DS 図は，R_TO および E_TO の表現が始まる時間を合わせた状態で重ねる（次節4.3の図 4参照）.

一方，システム運用中のアクシデント等による緊急対応用の対策を評価する場合は，システム障害発生（業務フローの異常実行または停止発生）時点より対策実施の準備が始められ，その完了時点で効果を発揮し始めるため，各対策の MS 図および適用対象となる業務フローの DS 図をそのまま重ね合わせる（次節4.3の図 5参照）.

4.3 対策評価値

本手法では，対策評価値として以下の２つを定義する.

MO 値（Maintain the system Operation）：

ある対策における，システム稼働（業務フローの正常実行）を維持できる力の大きさ. 本手法ではこれを，3における「回復力」を表す値とする.

EA 値（Endure an Attack）：

ある対策における，外部からの攻撃に耐え業務フローを正常実行できる力の大きさ．本手法ではこれを，3における「抵抗力」を表す値とする.

それぞれの算出方法は以下の通り.

MO 値の算出

DMS 図において，DS 図の R_SL×R_TO の範囲内で MS 図の E_SL×E_TO 部分が全体で占める領域（以後，MO 領域と呼ぶ）の面積を求める．MO 領域の例を図 4および図 5に示す.

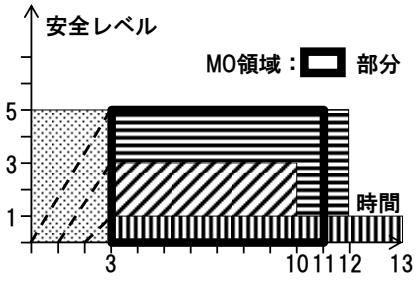

図 4：システムの新規開発や刷新時に配備する対策の評価向け DMS 図と MO 領域の例

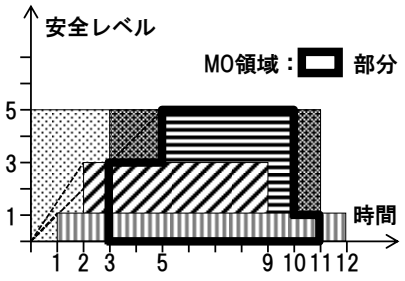

図 5： システム運用中の緊急対応で用いる対策の評価向け DMS 図と MO 領域の例

システムの新規開発や刷新時に配備する対策の評価を行う場合は，DMS 図において，DS 図の R_SL×R_TO の範囲内で各 MS 図の E_SL×E_TO 部分が占める領域（以後，EA 領域と呼ぶ）の総面積を求める（図 6参照）．また，システム運用中の緊急対応で用いる対策の評価を行う場合は，DMS 図において，DS 図の R_SL×(R_TP×R_TO)の範囲内で各 MS 図の E_SL×(E_TP×E_TO)部分が占める領域（以後，これも EA 領域と呼ぶ）の総面積を求める（図 7参照）．

EA 値の算出

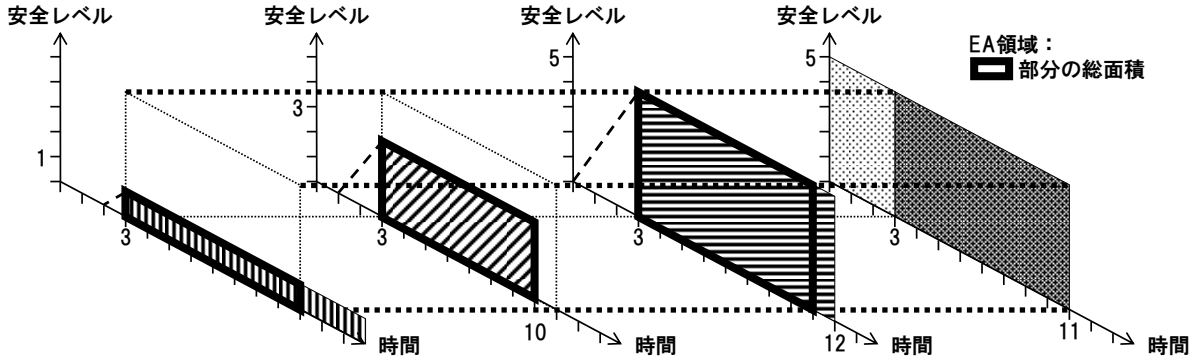

図 6：システムの新規開発や刷新時に配備する対策の評価向け EA 領域の例

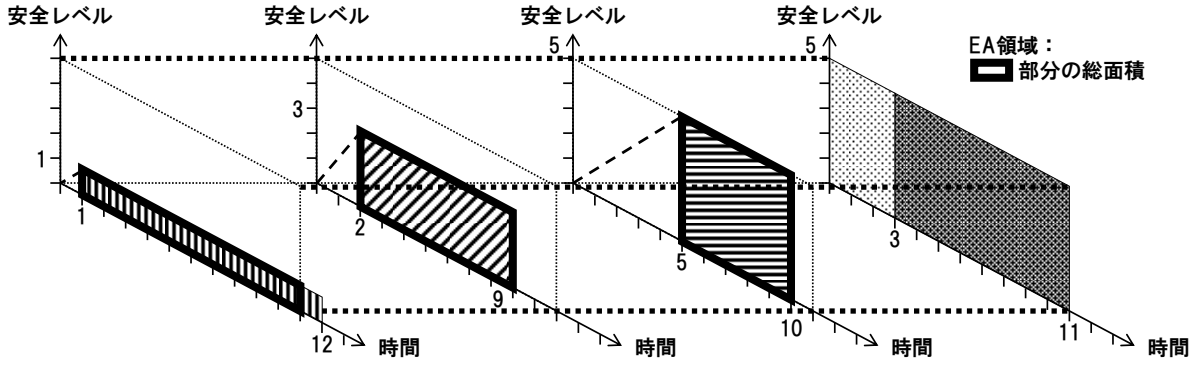

図 7：システム運用中の緊急対応で用いる対策の評価向 EA 領域の例

5 提案手法の詳細

以下に，本手法の手順と概要を示す．なお，手順番号の冒頭の S1,S2,S3 は2.1に記載の手順番号に対応している．脅威分析・リスク評価の実施手順については，本稿ではスコープ外のため割愛する．

S1-1. R 値付き業務フローを入手する．

S1 における情報収集時に，R 値を付与した業務フローを入手しておく．

なお，R 値と E 値付与の際には，図 8 のような各値の決定表を作成の上関係者間で共

有しておき，各業務フローや対策候補が決定表におけるどの部分に該当するかを検討の上決定する．

R_SL決定表

業務フローの停止または異常稼働時の影響	R_SL
人命・身体に危害を加える	7
電力の安定供給に支障あり（規模：地方、国単位）	6
電力の安定供給に支障あり（規模：県単位）	5
電力の安定供給に支障あり（規模：個人、市町村単位）	4
業務フローの実行期間が延びる（サービス影響なし）	3
社内業務の継続に支障があり	2
業務効率が低下する	1
影響なし	0

A_SL決定表

対策実施後の回復の程度	A_SL
100%	R_SL×1.0
90%	R_SL×0.9
80%	R_SL×0.8
70%	R_SL×0.7
60%	R_SL×0.6
50%	R_SL×0.5
40%	R_SL×0.4
30%	R_SL×0.3
20%	R_SL×0.2
10%	R_SL×0.1

※A_SLの計算には、実施の対象となる業務フローのR_SLを用いること

R_TP,A_TP決定表

業務フローに一時停止が許される時間　又は対策の実施準備時間	R_TP, A_TP
1ヶ月以上	10
2週間以上、4週間未満	9
1週間以上、2週間未満	8
3日以上、7日未満	7
1日以上、3日未満	6
18時間以上、24時間未満	5
12時間以上、18時間未満	4
6時間以上、12時間未満	3
3時間以上、6時間未満	2
3時間未満	1

R_TO,A_TO決定表

業務フローに要求される最低稼働時間　又は対策の効力の持続時間	R_TO, A_TO
10年以上	10
8年以上、10年未満	9
5年以上、8年未満	8
3年以上、5年未満	7
1年以上、3年未満	6
9ヶ月以上、12ヶ月未満	5
6ヶ月以上、9ヶ月未満	4
3ヶ月以上、6ヶ月未満	3
1ヶ月以上、3ヶ月未満	2
1ヶ月未満	1

図 8：R 値，E 値決定表の例

S2-1.　脅威分析・リスク評価を実施し，結果に R 値情報を追加する．

脅威分析・リスク評価を実施する．この際，結果をまとめた表に，各脅威の抽出元となった業務フローの R 値も記載しておく．

S2-2.　脅威ごとに対策候補を列挙し，各々に対し E 値を決定する．

S2-1 の結果を受け，抽出した脅威ごとに対策候補を列挙する．この際，対策の E 値も共に決定する．

S2-3.　脅威をグループ分けし，この統合 R 値を求める．

対策実施箇所（脅威の発生箇所）が同じである脅威ごとにグループ分けを行い，各グループごとに，各脅威の抽出元となった業務フローの R 値から統合 R 値を求める．

同じグループに属する脅威は対策を実施する箇所が同じであり，ある脅威への対策は，同じグループの別の脅威の抽出元となった業務フローの可用性を喪失させる可能性がある．従ってこれらの脅威に対する対策は，同じグループの他の脅威の抽出元となっている業務フローの R 値全てを上回る E 値を持っていなくてはならない．この評価を行うため，統合 R 値を設定する．

S3-1.　統合 R 値と E 値より，対策候補の MO 値と EA 値を求める．

対策方針や要件定義（例えば，4 つの種類の対策から最低 2 種類の対策を実施しなければならない，など）がある場合はそれに従い，対策実施箇所ごとに，列挙された対策候補の全ての組み合わせ（対策グループ）を作る．その上で，対策グループごとに，統合 R 値とグループを構成する各対策候補の E 値から，MO 値と EA 値を求める．

S3-2.　評価値に基づき対策を選定する．

対策実施箇所ごとに作られた対策グループ間で MO 値と EA 値の標準偏差を求め，この値が大きい対策グループを対策実施箇所ごとに選択し，立案する対策とする．

6　まとめと今後の課題

本稿では，社会インフラシステムのセキュリティ対策立案について，制御システムで最も重視される可用性維持に関する評価指標を新規に定義し，これを用いた対策立案手法を提案した．これを用いることにより，定量的かつ客観的な評価が可能となり，より確実なシステムの可用性確保が可能となる．

今後は，新規に提示した評価指標である R 値と E 値の決定方法についてさらに検討する必要がある．特に図 8に示した R 値，E 値

決定表の具体的な作成方法を確立し，本手法の実用性を高めることが重要である．

参考文献

[1] ICS-CERT, ICS-CERT Incident Response Summary Report (2009-2011), 2012. available at https://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT%20Incident%20Response%20Summary%20Report%20%282009-2011%29_accessible.pdf.

[2] ICS-CERT, ICS-CERT MONITOR, 2013. available at https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf.

[3] NERC-CIP Standards

[4] 情報処理推進機構, 重要インフラの制御システムセキュリティと IT サービス継続に関する調査, 2009. available at https://www.ipa.go.jp/files/000013981.pdf.

[5] 土居 範久, 佐々木 良一, 岡本 栄司ほか「情報セキュリティ事典」, 共立出版, pp.618-632. 2003.

[6] ISO. Information Technology - security evaluatin - Common Criteria for Information Technology - Part 2: Security functional components, 2012. available at http://www.ipa.go.jp/security/jisec/cc/documents/CCPART2V3.1R4.pdf.

[7] 内閣官房「国土強靭化(ナショナル・レジリエンス（防災・減災))推進に向けた考え方」, 2013. available at http://www.cas.go.jp/jp/seisaku/kyoujinka/pdf/kihon.pdf.

[8] 京大・NTT リジリエンス共同研究グループ「しなやかな社会への試練」, 日経 BP コンサルティング, 2012.

[9] 内閣府, 国土強靭化（ナショナル・レジリエンス）について(第 10 回経済財政諮問会議、資料 6), 2013. available at http://www5.cao.go.jp/keizai-shimon/kaigi/minutes/2013/0507/shiryo_06.pdf.