Computer Security Symposium 2018
22 - 25 October 2018

「サイバーセキュリティ能力成熟度モデル」を一部改良して使用した国レベルの能力測定の提案

森 滋男[†1]　　後藤 厚宏[†1]

概要：サイバー攻撃による被害が，甚大化，深刻化しており，電力という国民生活に直接影響を及ぼすものまでサイバー攻撃の脅威に晒される事態となっている．一部のサイバー攻撃は，国家の関与も疑われている．このような状況下，もはや企業や個人によるサイバー攻撃対策だけで被害を防げるとは言い難く，国によるプロアクティブなサイバーセキュリティ能力の醸成が不可欠であると見られる．では，国レベルではどのようなサイバーセキュリティ能力を持つ必要があるのであろう．国が持つべき，多岐に渡るサイバーセキュリティ能力について，強いところ弱いところを明確にし，それに基づいて強化施策を策定することは重要である．本ペーパーでは英国オックスフォード大学を中心に設立されたグローバル・サイバーセキュリティ能力センターが開発した「国家のためのサイバーセキュリティ能力成熟度モデル」を，一部改良したうえで使用した国レベルのサイバーセキュリティ能力測定を提案する．

キーワード：サイバーセキュリティ，能力成熟度

Assessment of National Capabilities Using the Modified 'Cybersecurity Capacity Maturity Model'

Shigeo Mori[†1]　Atsuhiro Goto[†1]

Abstract: The damages caused by cyber-attacks are becoming larger, broader and more serious. Now, even the essentials for daily life of citizens, for example electricity, are exposed to cyber threat. Some cyber-attacks are arguably suspected to be parts of national campaigns. Under such circumstances, the countermeasures by enterprises and individuals cannot sufficiently prevent cyber-attacks from causing damages, and enhancement of proactive cybersecurity capabilities initiated by nations is needed. Then, what capabilities does a nation have to have? It is important that a nation plans the political approaches for enhancing its cybersecurity capabilities based on the recognition of strong and weak points in the various capabilities that nations must have. In this paper, the authors propose the assessment of national cybersecurity capabilities using the Cybersecurity Capacity Maturity Model for Nations developed by the Global Cyber Security Capacity Centre established around Oxford University in the UK with the modification to the method.

Keywords: Cybersecurity capacity maturity

1. はじめに

サイバー攻撃のニュースが毎日のように報道されている．それらサイバー攻撃の標的，攻撃手法，損害，推定される攻撃者と攻撃者の目的は様々であるが，ひとつ共通しているのは，サイバー攻撃による被害が，甚大化，深刻化しているように見られるという点である．2017 年 10 月には，Yahoo!が 30 億件の顧客情報が流出していたと発表した[1]．2016 年 2 月にはバングラデシュの中央銀行がサイバー攻撃により SWIFT という国際的な銀行間の資金決済の仕組みを通じて約 951 百万米ドルを盗まれた[2]．2015 年 12 月と 2016 年 12 月にはウクライナにてサイバー攻撃による広域停電が発生した[3][4]．このように，サイバー攻撃は，今や甚大なる被害，巨額の金銭的損害や，停電などの国民生活に直結する被害までも，引き起こすことができるようになった．一部のサイバー攻撃については，国家の関与も疑われている[5]．

このような状況にあって，企業や個人はサイバー攻撃対策を行うわけであるが，最早それだけでサイバー被害を防ぐことは難しいと思われ，国民の安全安心な生活を守るため，国が主体的にサイバーセキュリティを向上させる必要があるのではないかと考える．

田川および林[2017]は，「今後は（中略）英知を結集して国全体のサイバーセキュリティ対策の強化を図るべきであると考える．具体的には，民間主導で事後対応を中心にした，従来のサイバーセキュリティ対策を基盤とし，それを維持した上で，国全体としての proactive（事前配慮的）な要素を上乗せすることである．」と述べ，国としてのサイバーセキュリティ能力醸成の必要性を主張している[6]．

では，国レベルにて持つべきサイバーセキュリティ能力とはどのようなものであろうか．企業や組織が持つべきものと同様であろうか．田川および林[2017]は「国全体として（中略）上乗せ」[6]と言っているのだから，国レベル独自

†1 情報セキュリティ大学院大学
Institute of Information Security

の能力は必要であろう．具体的に考えてみても，例えば，企業等はサイバー攻撃を受けた際に証拠保全に留意する必要があるが，国の場合は法執行や司法に関わる能力が求められるなど，企業等では求められない，国レベルだからこそ必要となる能力が存在することは明らかである．

では，具体的にどのようなサイバーセキュリティ能力が国レベルで求められるのかを示したガイドラインのようなものはあるのであろうか．例えば，企業や組織が拠り所とすることの多い，アメリカ国立標準技術研究所（NIST）による重要インフラのサイバーセキュリティを向上させるためのフレームワーク[7]の，国家版のようなものである．

筆者らが調査した限りでは，国家版のサイバーセキュリティガイドラインは存在しないが，国のサイバーセキュリティ能力を測定しようという試みは存在する．能力上の弱点を補う，あるいは，強い部分をさらに伸ばすのが施策であるから，どのようなサイバーセキュリティ能力を強化するべきか，どのような施策でそれを実現するかを検討するにあたって，まず能力を測定することは必須である．よって，国レベルのサイバーセキュリティ能力を測定する試みについて，次項にて紹介する．

2. 国のサイバーセキュリティ能力測定の試み

2.1 ITU GCI

2017 年 7 月，国際電気通信連合（International Telecommunication Union（略称：ITU））のサイバーセキュリティチームは，各国のサイバーセキュリティへの取組み度を表す指標として「世界サイバーセキュリティ指数（Global Cybersecurity Index（略称：GCI））」を調査し公表した[8]．GCI は 2014 年にも発表されており，2017 年のものが 2 回目である．

GCI は，法体系，技術，組織，能力醸成，協力の 5 つの区分に分類される 25 個の指標に基づく複合指数である．ITU は，各国に 157 項目からなる質問書を送付し，回収した回答から「スコア」を計算し，公表している．2017 年の上位国と，そのスコアは表 1 のとおりである．

表 1　GCI2017 結果（上位国）

順位	国	GCI総合指数
1	シンガポール	0.925
2	アメリカ合衆国	0.919
3	マレーシア	0.893
4	オマーン	0.871
5	エストニア	0.846
6	モーリシャス	0.830
7	オーストラリア	0.824
8	ジョージア	0.819
	フランス	0.819
10	カナダ	0.818
11	ロシア	0.788
12	日本	0.786
	ノルウェー	0.786

GCI は ITU の加盟国 193 ヶ国をカバーしている．

質問書は，比較的シンプル，かつ，分かりやすいものであり，例えば，以下のような内容である．

・サイバー犯罪に関わる実体法はあるか？
・不正アクセスに関する項目はあるか？
・法執行機関要員に対するサイバーセキュリティ訓練は行われているか？
・訓練は定期的に実施されているか？

分かりやすい点は評価できるが，これを以って，サイバー攻撃から国民の安心安全を守る，国レベルでの総合能力を示しているとは言い切れないという印象である．

2.2 Cybersecurity Capacity Maturity Model

英国オックスフォード大学を中心に設立された，グローバル・サイバーセキュリティ能力センター（Global Cyber Security Capacity Centre）は，2014 年 12 月，サイバーセキュリティ能力成熟度モデル（Cybersecurity Capability Maturity Model）1.2 版を公表した[9]．その後，いくつかの国家における試行的評価を行ったうえでアップデートし，2017 年 2 月に，国家のためのサイバーセキュリティ能力成熟度モデル（Cybersecurity Capacity Maturity Model for Nations）改訂版として再リリースした[10]．

このモデルは，国家が自国のサイバーセキュリティ能力を，システマティック，かつ，実質的な方法で改善することを支援することを目的としている．サイバーセキュリティ能力は，5 つの要素からなると考えられており，それらを「Dimension」と呼んでいる．5 つの dimension は，以下のとおり．

1. サイバーセキュリティポリシー，および，戦略
2. サイバー文化と社会
3. サイバーセキュリティ教育，訓練，スキル
4. 法，および，規制体系
5. 標準，組織，および，技術

各 dimension は，いくつかの「Factor」に分類され，さらに factor は「Aspect」に分類されている．Factor は全部で 24 個，aspect は全部で 53 個ある．

また，成熟度合いに応じた段階が設けられており，本モデルではこれを「Stage」と呼ぶ．Stage は 5 段階あり，下から「Start-up」「Formative」「Established」「Strategic」「Dynamic」である．

各 aspect の stage 毎に，「Indicator」と呼ぶ達成要件が定義されている．Indicator は殆どのケースで複数あり，全てを満たしていないと，当該 stage を達成しているとは見なされない．

Dimension，factor，aspect，stage，indicator の関係を図示すると，図 1 のようになる．

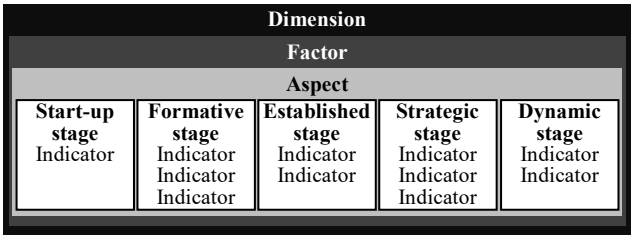

図 1　モデル構成要素の関係

1.2 版を使用して，これまでに，ウガンダ，セネガル，ブータン，コソボ，英国がアセスメントを実施している[11][12][13][14][15]. 改訂版を使用したアセスメント事例は，まだ発表されていない．他に，ラテンアメリカ，および，カリブ諸国が米州機構，および，米州開発銀行のイニシアチブで, 1.2 版とも改訂版とも若干異なるバージョンのモデルを使用してアセスメントを実施し，結果を公表している[16]. 日本は，まだ公式なアセスメントは実施していない．

本モデルは，53 個の aspect に 500 個を超える indicator が示されている．オックスフォード大学をはじめとする世界中の研究者や実務者が参加して策定したものであり，国レベルで求められるサイバーセキュリティ能力を広範囲にカバーしているものと考える．

3. サイバーセキュリティ能力測定方法の提案

3.1 サイバーセキュリティ能力測定の必要要件

1. はじめに で述べたとおり，筆者らの目的は，国が持つべきサイバーセキュリティ能力，および，それを強化するための施策に関してガイドを得ること，である．そのために国レベルのサイバーセキュリティ能力を測定することが必須であると述べたが，その測定は，国が持つべきサイバーセキュリティ能力の全般に渡って，強いところと弱いところが分かるようになっていなければならない．それが分かったうえで, どこをどの程度強化するのか方針を定め，さらにはそれを実現するための具体的方策を策定するわけである．図示すると，図 2 のようになる．

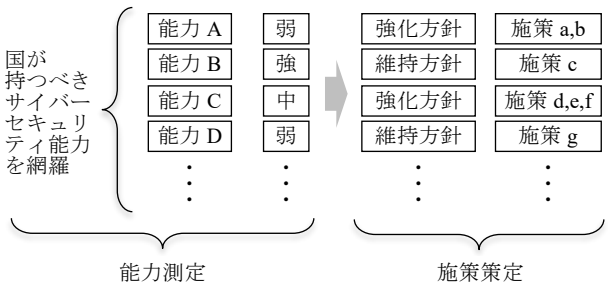

図 2　能力測定と施策策定の関係

この観点で見ると, 2.2 で紹介した国家のためのサイバーセキュリティ能力成熟度モデルは，53 個という多岐に渡る aspect において，5 段階の成熟度水準を設定しており，好都合である．すなわち，本モデルがサイバーセキュリティ施策を策定する上での良きガイドとなるかどうかは措いておいて，その前段階の，どの能力が強く，どの能力が弱いかを把握するための測定ツールとしては，非常に優れていると考えられる．

よって，本モデルを用いて，国レベルのサイバーセキュリティ能力の測定を実施することは有用であると考える．

ただし，どの能力が強くどの能力が弱いかを見極め，適切なサイバーセキュリティ施策の策定に貢献することを主目的とした場合，本モデルをそのまま使用し，本モデルの既定の方法に従って測定を行うのではなく，測定方法を一部改良したほうが，測定後の施策策定の議論に繋げやすいと考える．次項にて，その改良案について述べる．

3.2 測定方法改良の概要

測定方法を改良する目的は，本モデルによる能力測定結果を，サイバーセキュリティ施策の策定に，より活用しやすくすることである．そのためには，測定した結果，どの能力が強く，どの能力が弱いかが明確になること，また，何ができていないために弱いと判定されているのかが容易に分かること，が必要であると考える．

よって，測定方法の改良を，以下の観点から検討した．

・各 stage で要求している事項の細分化，明確化
・Stage 判定の詳細化

以下，それぞれについて詳細に述べる．

3.3 要求事項の細分化，明確化

国家のためのサイバーセキュリティ能力成熟度モデルは，基本的に文章で記述されている．例えば，最初の aspect である「Strategy Development」における「Dynamic」stage の記述は以下のとおりである．

Continual revision and refinement of cybersecurity strategy is conducted proactively to adapt to changing socio-political, threat and technology environments.

The country is a leader within the international community and the debate shaping the development of global cybersecurity strategy.

このように，各文がそれぞれ 1 つの indicator，すなわち達成要件を示している．一方,「Incident Response」factor の「Coordination」aspect における「Established」stage は以下のように書かれている．

Routine and coordinated national incident response is established and published between public and private sectors, with lines of communication prepared for times of crisis.

International cooperation for incident response between organisations exists to resolve incidents as they occur.

ここで，最初の文の national incident response が establish されていることと，with 以下の communication line が用意

されていることは，明らかに 2 つの異なる要件である．したがって，このケースでは，以下の 3 点を全て満たさないと，当該 stage を達成できない．

・国レベルのインシデント対応が官民間で確立している
・危機下で使用できる通信網が確保されている
・国際協同体制が確立している

そこで，筆者らは，文章で書かれているものを個々の indicator に分解する作業を行った．各 stage を達成しているか否かを判定するだけであれば，必ずしもこのような作業は必要ではないのだが，判定したのち，施策検討の議論に貢献するためには，どの indicator を達成していて，どの indicator が未達なのか明確にする必要があるためである．

また，書かれているものの中に，要件とは呼べないもの，すなわち，ネガティブな内容であり，それを満たしている必要はないと考えられるものがある．例えば，「Organisation」aspect の「Formative」stage は以下のように書かれている．

A coordinated cybersecurity programme is being developed through a multistakeholder consultative process.

However, budgets reside in disparate public departments without a discrete cybersecurity budget line.

However 以下は，予算がバラバラの省庁で所管されていて，サイバーセキュリティ専用の予算ではないということを述べている．ここで，仮に予算が集中管理されていたら，この indicator を満たさないので「Formative」stage とは見なされないかというと，当然そんなことはない．したがって，however 以下は indicator とは見なさないこととした．

同じような理由で，「Start-up」stage の記述も indicator とは見なさないこととした．本モデルにおける一番下の段階である「Start-up」stage にも indicator が記述されているが，仮にそれらの indicator を達成していなくても，「Start-up」と見なされる．「Start-up」より下には stage はないからである．したがって，これらの indicator は，要件というより，状態の説明であって，達成しているか達成していないかを検討する必要がないと判断した．

3.4 Stage 判定の詳細化

Stage 判定を行うにあたって，まず，indicator 毎に，達成しているか達成していないかを判定していくわけであるが，いくつかの indicator では，全くできていないわけではないが，完全にはできていない，すなわちできている部分もあればできていない部分もある，と判断せざるを得ない状況にある．例えば，「ICT Security Standards」aspect の「Strategic」stage では，次のようなことが求められている．

Government and organisations promote adoption of standards and good practices according to assessment of national risks and budgetary choices.

リスクベースで標準やベストプラクティスへ導入を決めているということであるが，先進的な組織においては実施していると思われるものの，実施していないところも多いであろう．このように，部分的にできているという状態は，本モデルの判定方法に従えば「未達」であるが，前述のように，判定したのちの改善を目指すことを想定し，「部分達成」という判定を許容することとした．

もう一点，実施しているか実施していないかと聞かれたら実施していないが，その段階は過ぎていて実施する必要がない，という indicator がある．例えば，先にも引用した「Organisation」aspect の「Formative」stage では，以下のように書かれている．

A coordinated cybersecurity programme is being developed through a multistakeholder consultative process.

我が国では既にサイバーセキュリティプログラムが確立されており，策定途上にはない．「対象外」という判定を作ることも考えられるが，「達成」とすることとした．

また，本モデルの正式なアセスメント方法としては，各 stage の全ての indicator を達成している場合に，当該 stage を達成と見なす（したがって，aspect 毎に，どの stage にあるかという判定が出る）．それを factor 毎に集計し，各 factor の stage を判定することになっている．

筆者らが提案する改良方法では，factor 毎の集計は行わず，aspect 毎の stage 判定を行うにとどめることとした．これによって，極力詳細化された能力単位での強い弱いが判別できる．

また，indicator 毎の「達成」「部分達成」「未達」の判定を見れば，何ができていないために弱いと判定されたのかも分かる．

3.5 測定方法改良案のまとめ

国家のためのサイバーセキュリティ能力成熟度モデルを用いて国レベルのサイバーセキュリティ能力を測定するにあたって，その測定結果をサイバーセキュリティ施策の策定に活用することを念頭に置いた場合の測定方法の改良案を述べた．改良ポイントは以下の 5 点である．

① モデルでは文章で書かれているものを，個々の indicator に分解
② 要件でないものは indicator から除外
③ 各 indicator に対して「達成」「未達」に「部分達成」を加えた 3 種類で判定
④ 要件で求めている段階を超過している場合は「達成」で判定
⑤ Aspect 毎の stage 判定にとどめ，factor 毎の stage 判定は行わない

4. 我が国サイバーセキュリティ能力の仮測定

本ペーパーは，国のサイバーセキュリティ施策策定に貢献することを目的として，グローバル・サイバーセキュリティ能力センターが開発した，国家のためのサイバーセキュリティ能力成熟度モデルを，測定方法に改良を加えたうえで使用して，国レベルのサイバーセキュリティ能力を測定することを提案するものである．

しかし，それを我が国に適用した場合に，概ねどのような結果が出てくるのかを示すことは，提案の有効性に一定の支持を与えるものと考える．そこで，あくまでも筆者らによる仮の測定であるが，測定結果を以下に示す．

仮測定に際し，我が国の現状を把握するには，「サイバーセキュリティ戦略」（平成 27 年版）[17]，「同」（平成 30 年版）[18]，「サイバーセキュリティ 2015～2018」[19][20][21][22]等を参考にした．

サイバーセキュリティ能力成熟度モデルを使用した正式な測定プロセスについては，5. まとめ の中で紹介する．

Indicator 毎の判定結果を表 2 に，判定結果の集計を表 3 に，aspect 毎の stage 判定を表 4 に示す．表 2 はスペースの関係で dimension 1 のみ記載した．また，各 indicator はキーワードのみ記載している．詳細については国家のためのサイバーセキュリティ能力成熟度モデル原文[10]を参照願いたい．

表 2　Indicator 毎の我が国の判定結果（抜粋）

#	Dimension	Factor	Aspect	Formative		Established		Strategic		Dynamic	
				y/n	Keywords	y/n	Keywords	y/n	Keywords	y/n	Keywords
111	Cybersecurity Policy and Strategy	National Cybersecurity Strategy	Strategy Development	y	Outline of strategy	y	Strategy established	y	Reviewing process of strategy	y	Continual revision of strategy
				y	Development process of strategy	y	Stakeholders' consultation in strategy	y	Cyber exercises considered in strategy	n	Contributing to international debate of strategy
				y	Stakeholders involved in strategy development	y	Implementation of strategy	y	Measurement of cybersecurity defined in strategy		
								y	Capacity building & investment considered in strategy		
112			Organisation	y	Cybersecurity programme under development	y	Cybersecurity programme agreed	y	PDCA processes of cybersecurity programme	n	Reassignment & reallocation of resources for cybersecurity programme
						y	Coordinating body of cybersecurity programme	y	Consolidated budget for cybersecurity	n	Dissemination & feedbacks about cybersecurity programme
						y	Goals & measurement of cybersecurity programme				
						y	Discrete budget for cybersecurity				
113			Content	y	Risk priorities of cybersecurity defined in strategy	y	National objectives of cybersecurity defined in strategy	y	Measurement of cybersecurity defined in strategy	y	Continual revision of strategy
						y	Minimum coverage of strategy contents	y	Protection of critical infrastructures defined in strategy	n	Contributing to international cooperation
121		Incident Response	Identification of Incidents	y	Recording incidents	y	Central registry of incidents	n	Regular revision of incident registry	n	Adapted analysis of incidents
								p	Incident analysis		
122			Organisation	y	Key incident response organisations in private sector identified	y	National CSIRT	y	Formal roles & responsibilities allocated	n	Sustainability of incident response capability
				y	Ad-hoc responses	y	Roles & responsibilities of national CSIRT	n	Adequate resources for incident response	n	Early warning capability
										n	Capability to manage threat landscape
123			Coordination	y	Leading incident response organisation designated	y	Coordination established	y	Subnational / sectorial incident response organisations	n	Coordinating all levels / sectors
						y	Communication lines for crisis	n	International coordination	n	Regional coordination
						n	International cooperation in incident response	p	Information sharing across sectors		
124			Mode of Operation	y	Key incident response processes	y	Incident response processes & tools established	y	Training & accreditation for CSIRT members established	n	Scenario testing of incident response processes
				y	CSIRT member training	y	Regular training for CSIRT members	p	Sophisticated incident analysis	n	Evaluating effectiveness of CSIRT members training
						y	Limited response to national level incidents	y	Regular review of incident response processes	n	Tools against zero-day vulnerabilities
								p	Forensics	n	Regional coordination
								n	International coordination		
131	Cybersecurity Policy and Strategy	Critical Infrastructure (CI) Protection	Identification	y	List of CI assets	y	Audit of CI assets	p	Priority of CI risks	n	Regular review of CI risk priorities
						y	CI assets audit list	n	Vulnerability & asset management of CI assets		

注）y：達成　p：部分達成　n：未達

#	Dimension	Factor	Aspect	Formative y/n	Formative Keywords	Established y/n	Established Keywords	Strategic y/n	Strategic Keywords	Dynamic y/n	Dynamic Keywords
132	Cybersecurity Policy and Strategy	Critical Infrastructure (CI) Protection	Organisation	y	Informal information sharing between CI & government	y	Information sharing established between CI & government	n	Centralised management of CI protection	n	Ability to adjust of CI protection
						y	Formal & consistent information sharing between CI & government	p	Public awareness campaign of CI protection	p	Trust between CI & government
						y	Point of contact	n	Supply chain management of CI		
						y	Government engagement in CI protection				
133			Risk Management and Response	y	Access control implemented in CI	p	Standards & best practices in CI	p	Cybersecurity oriented risk management in CI	p	Regular audit of CI
				y	Basic capacity against cyber threat in CI	p	Risk management processes in CI	p	Regular review of impact analysis of CI	p	Indirect costs inclusive in impact analysis of CI incidents
				y	Data security policy in CI	p	National CI incident response plan	p	Regular review of CI incident response plans		
								n	Regular review of resource allocation for CI protection		
								p	Insider threat detection in CI		
141		Crisis Management	Crisis Management	y	Assessment of exercise of national incident	y	National incident exercise done	n	High-level scenario of national incident exercise	n	Peer observance of national incident exercise
				y	Exercise planning organisation designated for national incident	y	Appropriate resources for national incident exercise	p	Trust between participants of national incident exercise	n	National incident exercise contributing to international challenges
				y	Stakeholders' participation in national incident exercise	y	Roles in national incident exercise defined	n	SMART objectives & KPI of national incident exercise	n	Internationally shared result of national incident exercise
						y	Incentives to participate in national incident exercise	p	Evaluation of national incident exercise informing investment	n	National crisis management established
						y	Trained monitors of national incident exercise	p	National crisis management aligned with international best practices		
						y	Evaluation of national incident exercise	y	Tailored reports of national incident exercise		
151		Cyber Defence	Strategy	n	National-level threats identified	n	Cyber defence strategy exists	n	Dedicated resources for cyber defence	n	Rules of engagement in cyberspace
								n	Capturing landscape of national-level threat	n	Military doctrine in cyberspace
								n	Cyber defence strategy meets objectives		
152			Organisation	y	Dispersed cyber operations	y	Defined responsibility of cyber defence organisation	n	Advanced capabilities & situational awareness	n	Cross-border response ability
153			Coordination	n	Cyber defence capability requirements agreed	n	Coordination between CI & defence	p	Analytical capability in cyber defence	n	Leading international debate about cyber defence
						p	Intelligence sharing between CI & defence	p	Strengths & weaknesses of cyber defence understood	n	Intelligence shared with allies
161		Communi-cations Redundancy	Communi-cations Redundancy	y	Gaps in emergency communication identified	n	Emergency response assets hardwired	n	Redundant communications for key stakeholders	n	Optimised for extended outages
				y	Emergency procedures established	n	Communication between emergency response functions distributed	n	Interoperability & functionality under compromised situation	n	Assisting neighbours
						n	Testing, training, drills of emergency response	p	Evaluation of national incident exercise informing investment		
								n	Contribution to international communications' redundancy		

（Dimension 2 以降は省略）

表 3　「達成」「部分達成」「未達」の集計

Dimension \ Stage	Formative			Established			Strategic			Dynamic			合計			総計
	達成	部分	未達	達成	部分	未達	達成	部分	未達	達成	部分	未達	達成	部分	未達	
1 Cybersecurity Policy and Strategy	22	0	2	30	4	6	13	16	17	2	3	27	67	23	52	142
2 Cyber Culture and Society	19	0	0	19	3	1	9	9	6	2	4	11	49	16	18	83
3 Cybersecurity Education, Training and Skills	13	1	1	16	1	4	5	7	11	0	7	9	34	16	25	75
4 Legal and Regulatory Frameworks	24	1	1	21	0	9	12	0	19	6	3	20	63	4	49	116
5 Standards, Organisations, and Technologies	27	0	0	24	4	7	8	15	6	2	10	18	61	29	31	121
合計	105	2	4	110	12	27	47	47	59	12	27	85	274	88	175	
Indicator 数合計	111			149			153			124			537			

「Formative」stage では「達成」が 105/111（9.6%），「Established」stage では 110/149（73.8%）と高いが，「Strategic」stage では 47/153（30.7%），「Dynamic」stage では 12/124（9.7%）と低くなり，全体では 274/537（51.0%）と約半分の達成である．

Dimension 別に見ると，「達成」の比率は dimension 1 から

順に，47.2%，59.0%，45.3%，54.3%，50.4%となっており，dimension による大きな差異は見られない．

表 4　Aspect 毎の stage 判定

Dimension	Factor	Aspect	S-u	F	E	S	D
Cybersecurity Policy and Strategy	National Cybersecurity Strategy	Strategy Development					■
		Organisation					■
		Content					■
	Incident Response	Identification of Incidents				■	■
		Organisation				■	■
		Coordination			■	■	■
		Mode of Operation				■	■
	Critical Infrastructure (CI) Protection	Identification				■	■
		Organisation				■	■
		Risk Management and Response			■	■	■
	Crisis Management	Crisis Management				■	■
	Cyber Defence	Strategy		■	■	■	■
		Organisation				■	■
		Coordination		■	■	■	■
	Communications Redundancy	Communications Redundancy			■	■	■
Cyber Culture and Society	Cybersecurity Mind-set	Government				■	■
		Private Sector				■	■
		Users				■	■
	Trust and Confidence on the Internet	User Trust and Confidence on the Internet				■	■
		User Trust in E-government Services			■	■	■
		User Trust in E-commerce Services			■	■	■
	User Understanding of Personal….	User Understanding of Personal Information Protection Online			■	■	■
	Reporting Mechanisms	Reporting Mechanisms			■	■	■
	Media and Social Media	Media and Social Media				■	■
Cybersecurity Education, Training and Skills	Awareness Raising	Awareness Raising Programmes		■	■	■	■
		Executive Awareness Raising				■	■
	Framework for Education	Provision				■	■
		Administration				■	■
	Framework for Professional Training	Provision				■	■
		Uptake		■	■	■	■

Dimension	Factor	Aspect	S-u	F	E	S	D
Legal and Regulatory Frameworks	Legal Framework	Legislative Framework for ICT Security					■
		Privacy, Freedom of Speech & Other Human Rights Online					■
		Data Protection Legislation				■	■
		Child Protection Online			■	■	■
		Consumer Protection Legislation					■
		Intellectual Property Legislation					■
		Substantive Cybercrime Legislation				■	■
		Procedural Cybercrime Legislation				■	■
	Criminal Justice System	Law Enforcement			■	■	■
		Prosecution			■	■	■
		Courts			■	■	■
	Formal and Informal….	Formal Cooperation		■	■	■	■
		Informal Cooperation		■	■	■	■
Standards, Organisations, and Technologies	Adherence to Standards	ICT Security Standards			■	■	■
		Standards in Procurement			■	■	■
		Standards in Software Development			■	■	■
	Internet Infrastructure Resilience	Internet Infrastructure Resilience					■
	Software Quality	Software Quality			■	■	■
	Technical Security Controls	Technical Security Controls				■	■
	Cryptographic Controls	Cryptographic Controls				■	■
	Cybersecurity Marketplace	Cybersecurity Technologies			■	■	■
		Cyber Insurance			■	■	■
	Responsible Disclosure	Responsible Disclosure			■	■	■

S-u：Start-up，F：Formative，E：Established，
S：Strategic，D：Dynamic
□：達成
■：未達

5. まとめ

本ペーパーでは，昨今のサイバー攻撃から国民の安全安心な生活を守るために国のサイバーセキュリティ能力を向上させることが必要であることを述べ，その能力向上を図るための施策を適切に策定するために，国家のためのサイバーセキュリティ能力成熟度モデルを，測定方法を一部改良したうえで，国レベルのサイバーセキュリティ能力の測定に使用することを提案した．

筆者らは，2016 年に，サイバーセキュリティ能力成熟度モデルを使用しての正式な能力測定について，グローバル・サイバーセキュリティ能力センターにヒアリングした．その結果は以下のとおりであった．なお，同センターではこのプロセスを「アセスメント」と呼んでいるので，以下それに従う．

まずアセスメントを実施しようとする国は，アセスメント実施にあたるチームを組成しなければならない．このチームは，国内の利害関係者に当たって各 aspect 毎にどの stage に該当するのかを判定するとともに，その判定を立証できる証拠を集めなければならない．当然，然るべき権限が与えられなければならない．この利害関係者には，政府の各機関だけでなく，民間部門も含まれる．組成後，チームは，能力センターから，本モデルを使用したアセスメントを行うためのトレーニングを受ける．このトレーニング期間は，チームメンバーの能力，経験等によって異なる．また，トレーニングが完了し，アセスメント作業が始まって以降の支援については相談に応じる，というものであった．

すなわち，正式に実施するためには，相応のリソースと，強いコミットメントが必要である．

筆者らは，本ペーパーで提案する測定方式を我が国に適用し，仮測定してみた．その結果は 4. に示したとおりであるが，「達成」の比率が約半分（51.0%）で，残りの半分は「部分達成」もしくは「未達」であったこと，いくつかの aspect では最も初歩の「Start-up」stage と判定せざるを得なかったこと，など注目すべき結果であったと考える．

一方，すでに正式アセスメントを実施済みの国，例えば英国においても，昨今の状況を考えると，再アセスメントが必要である可能性がある．すなわち，現状把握にあたっ

て参照した「サイバーセキュリティ戦略」（平成 30 年版）[18]にも述べられているとおり，サイバー空間と実空間の一体化が加速的に進展しているほか，サプライチェーンも従来の概念を超えた多様性と流動性を持つに至るなど，様々な変化が起こっている．このような中，例えば標準の適用状況においても，従来のように IT のみにおいて標準化が進んでいても不十分で，IoT 等にも標準の適用が進展していないと，達成と見なすべきではない．サプライチェーンマネジメントにしても，従来よりもはるかに拡大したマネジメントが必要である．経営層の意識改革などは，例えば製品担当役員など，従来よりも対象者、対象とすべき領域ともに拡大が必要である．そのような変革期だからこそ，国レベルでのサイバーセキュリティ能力の測定の重要性は高まっているものと考える．

なお，本ペーパーでは，サイバーセキュリティ施策策定に資するための，国レベルでのサイバーセキュリティ能力測定について提案したが，実際のところ，我が国をはじめ多くの国において，すでに積極的にサイバーセキュリティ施策が展開され，能力向上に努力が払われている．それらが適切に策定されているものかどうか，当然気になるところであろう．そのような観点からサイバーセキュリティ施策を点検する方法について筆者らが論じた論文が，Journal of Disaster Research Vol.13 No.5（富士技術出版株式会社）に掲載される予定である．

参考文献

[1] Oath Inc. news release on 3 Oct. 2017 “Yahoo provides notice to additional users affected by previously disclosed 2013 data theft” https://www.oath.com/press/yahoo-provides-notice-to-additional-users-affected-by-previously/, (参照 2018-08-11).

[2] The New York Times article on 30 Apr. 2016 “Hackers’ $81 Million Sneak Attack on World Banking” https://www.nytimes.com/2016/05/01/business/dealbook/hackers-81-million-sneak-attack-on-world-banking.html, (参照 2018-08-11).

[3] SANS ICS Defense Use Case March 18, 2016 “Analysis of the Cyber Attack on the Ukrainian Power Grid” https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, (参照 2018-08-11).

[4] SANS ICS Defense Use Case No.6 August 2, 2017 “Modular ICS Malware” https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_6.pdf, (参照 2018-08-11).

[5] Executive Order 13687 of January 2, 2015 “Imposing Additional Sanctions With Respect To North Korea” https://www.federalregister.gov/documents/2015/01/06/2015-00058/imposing-additional-sanctions-with-respect-to-north-korea, (参照 2018-08-11).

[6] 田川義博, 林紘一郎. サイバーセキュリティのための情報共有と中核機関のあり方 —3 つのモデルの相互比較とわが国への教訓—. 情報セキュリティ総合科学. 情報セキュリティ大学院大学, 2017, vol. 9, p. 17-44.

[7] National Institute of Standards and Technology “Framework for Improving Critical Infrastructure Cybersecurity” https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity, (参照 2018-08-11).

[8] International Telecommunication Union “Global Cybersecurity Index (GCI) 2017” https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf, (参照 2018-08-11).

[9] Global Cyber Security Capacity Centre “Cyber Security Capability Maturity Model (CMM) –V1.2” https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf, (参照 2018-08-11).

[10] Global Cyber Security Capacity Centre “Cybersecurity Capacity Maturity Model for Nations (CMM) Revised Edition” https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf, (参照 2018-08-11).

[11] Global Cyber Security Capacity Centre “Cybersecurity Capacity Review of the Republic of Uganda” https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Uganda%20CMM.pdf, (参照 2018-08-11).

[12] Global Cyber Security Capacity Centre “Cybersecurity Capacity Review of the Republic of Senegal” https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Senegal-Report-v4%20.pdf, (参照 2018-08-11).

[13] Global Cyber Security Capacity Centre “Building Cyber-security Capacity in the Kingdom of Bhutan” https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM_Review_Report_Bhutan_September_2015.pdf, (参照 2018-08-11).

[14] Global Cyber Security Capacity Centre “Cybersecurity Capacity Assessment of the Republic of Kosovo” https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM_Review_Report_Kosovo_June_2015.pdf, (参照 2018-08-11).

[15] Global Cyber Security Capacity Centre “Cybersecurity Capacity Review of the United Kingdom” https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity%20Capacity%20Review%20of%20the%20United%20Kingdom.pdf, (参照 2018-08-11).

[16] Inter-American Development Bank “Cybersecurity: Are We Ready in Latin America and the Caribbean?” https://publications.iadb.org/handle/11319/7449, (参照 2018-08-11).

[17]サイバーセキュリティ戦略本部 “サイバーセキュリティ戦略” https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf, (参照 2018-08-11).

[18]サイバーセキュリティ戦略本部 “サイバーセキュリティ戦略” http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf, (参照 2018-08-11).

[19]サイバーセキュリティ戦略本部 “サイバーセキュリティ 2015” https://www.nisc.go.jp/active/kihon/pdf/cs2015.pdf, (参照 2018-08-11).

[20]サイバーセキュリティ戦略本部 “サイバーセキュリティ 2016” https://www.nisc.go.jp/active/kihon/pdf/cs2016.pdf, (参照 2018-08-11).

[21]サイバーセキュリティ戦略本部 “サイバーセキュリティ 2017” https://www.nisc.go.jp/active/kihon/pdf/cs2017.pdf, (参照 2018-08-11).

[22]サイバーセキュリティ戦略本部 “サイバーセキュリティ 2018” https://www.nisc.go.jp/active/kihon/pdf/cs2018.pdf, (参照 2018-08-11).