〈研 究 論 文〉

サイバーセキュリティ人材育成施策に関する動向と考察

大　手　英　明

Trends and considerations regarding measures for development of Cybersecurity Human Resource

Hideaki Ohte

Abstract

In recent years, the threat of cyberattacks is expanding both in quality and quantity, and their impact on society have been more and more serious as digitization spreads throughout society. As these recent trends, in order to create new value, we need cyber human resources who can ensure cyber security while advancing digitalization and innovation. It is expected that the demand for such cybersecurity human resource will show a significant increase in the future.

In Japan, especially since the large-scale leakage of personal information held by government-related entities occurred in 2015, the Japanese government has promoted various measures by formulating “Cybersecurity strategy” according to the Basic act on Cybersecurity and amending related laws. In particular, with regard to measures for development of cybersecurity human resource, the government have been executing measures such as “Cyber Defense Exercise with Recurrence” and the establishment of a national certification system.

While reviewing the historical background of cybersecurity policies to date, this paper analyzes the implementation status of these projects in light of the social impact of Novel coronavirus infection（COVID-19）and changes in the national security environment.

Based on the above, this paper considers what kind of initiatives are necessary for development of cybersecurity human resource in the future.

KeyWords

cybersecurity human resource, cyber defense exercise, national certification system

目　　次

はじめに

近年，サイバー攻撃の脅威は質量ともに高まっており，その社会への影響は，社会全体のデジタル化の浸透に伴ってますます深刻化してきている．こうした近年の潮流に伴い，新たな価値を生み出すためにはデジタル化を進めると同時にサイバーセキュリティの確保も行うことができる人材が必要であり，その需要はますます拡大すると想定される．

我が国では，特に 2015 年の政府関係機関が保有する個人情報の大規模な流出事案が発生して以来，サイバーセキュリティ基本法（以下「CS 基本法」という）に基づくサイバーセキュリティ戦略[1]（以下「CS 戦略」という．）の策定や関連法の改正を行って様々な人材育成施策を強化してきた．本稿では，新型コロナウイルス感染症（COVID-19）による社会的影響や安全保障環境の変化も踏まえ，人材育成に関する実施状況を分析し，今後の人材育成に向けてどのような取組が必要なのか考察する．

なお，本稿の寄稿にあたっては，筆者が 2017 年から 2 年間内閣官房内閣サイバーセキュリティセンター（NISC）で勤務するとともに，2021 年から 2022 年 3 月までの間，国立研究開発開発法人情報通信研究機構ナショナルサイバートレーニングセンターで人材育成関連施策に直接携わった経験を基に，これまでの歴史的経緯や基本方針などの全体的な潮流を俯瞰したうえで，状況の整理と考察を行うこととする．

1） 2015 年 9 月 4 日閣議決定．以下，2 度改定（2018 年 7 月 27 日閣議決定，2021 年 9 月 28 日閣議決定）

1. 施策の背景

1.1 黎明期（2002 年以前）

（1） 黎明期の取組

情報セキュリティ関連施策は，当初，1987 年郵政省告示[2]等の民間における対策を進めるための基準・指針等の策定や 1987 年刑法改正による電子計算機使用詐欺罪等の創設など[3]各省庁において各々行われていた．インターネットの商用化以降，その普及が 1990 年代後半に進展し，これに伴い，不正アクセス，コンピュータウイルスなどの問題がいわゆる 2000 年問題[4]とも関連して我が国全体で取り組むべき課題となった．また，OECD（経済協力開発機構）が 1986 年「コンピュータ犯罪―立法政策の分析」を公表して 1992 年には「情報セキュリティガイドライン」を策定するとともに，1998 年バーミンガム・サミットにおいてハイテク犯罪に対する法制度の見直しを進める等の声明が公表されるなどの国際的な潮流もあり，1999 年 8 月に不正アクセス禁止法が成立し[5]，同年 9 月に「情報セキュリティ関係省庁局長等会議」（議長：内閣官房副長官（事務））[6]が設置された．

翌 2000 年 1 月，政府関係機関のホームページ改

2） 情報通信ネットワーク安全・信頼性基準（昭和 62 年郵政省告示第 73 号）https://www.soumu.go.jp/menu_seisaku/ictseisaku/net_anzen/anshin/

3） 「ハッカー対策等の基盤整備に係る行動計画」（2000 年 1 月 21 日情報セキュリティ関係省庁局長等会議決定）参照 https://warp.ndl.go.jp/info:ndljp/pid/8295038/www.nisc.go.jp/active/sisaku/0121actionplan.html

4） ハッカー・サイバーテロ対策に関する体制の整備について（2000 年 2 月 22 日（火）内閣総理大臣発言要旨（抜粋）「今後，ハッカー・サイバーテロ対策について，コンピュータ西暦二千年問題における経験も活かしながら，抜本的な対策強化を図りたいと考えます．」https://warp.ndl.go.jp/info:ndljp/pid/8295038/www.nisc.go.jp/active/sisaku/0222souri.html

5） 不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）
（参照）不正アクセス対策法制研究会「逐条不正アクセス行為の禁止等に関する法律補訂第 2 版」立花書房，2008.10，pp.1-10

ざん事案[7]の発生を契機に，同年2月に同会議が「情報セキュリティ対策推進会議」[8]に改組され，事務局として，政府全体の総合調整を担う内閣官房情報セキュリティ対策推進室[9]も設置され，この下で各府省庁が対策を推進する形となった[10]．これが同年中の政府機関のポリシー及び重要インフラの計画の策定につながった[11]．人材育成の観点では，いずれにも職員等への「教育・訓練」との文言が盛り込まれた．

(2)　初期のIT戦略での位置づけ

セキュリティ確保の基本方針は，法律レベルでは，旧IT基本法（2000年11月成立）[12]で「高度情報通信ネットワークの安全性及び信頼性の確保」などと明記された．

戦略レベルでは，翌2001年1月策定の基本戦略であるe-Japan戦略[13]においては「知識創発型社会」実現に向けたIT整備と活用に重点が置かれ，4つの重点政策分野の一つの「超高速ネットワークインフラ整備及び競争政策」の項目中に「安心」・「安全確実」との文言が点在し，また，「プライバシーとセキュリティの保護がしやすいIPv6」との文言が入って脚注でセキュリティの解説がなされていたという程度にとどまった[14]．

単年度計画レベルでは，この後，e-Japan戦略に基づく2001年3月策定の「e-Japan重点計画」[15]

---

6)　情報セキュリティ関係省庁局長等会議の設置について（1999年9月17日内閣官房長官決裁）https://warp.ndl.go.jp/info:ndljp/pid/8295038/www.nisc.go.jp/active/sisaku/0917kyokutyou.html

7)　園田寿，野村隆昌，山川健「ハッカーvs.不正アクセス禁止法」日本評論社，2000.6，参照pp.8-26

8)　情報セキュリティ対策推進会議の設置について（2000年2月29日高度情報通信社会推進本部長決定）（議長：内閣官房副長官（事務））．同日，民間有識者で構成される「情報セキュリティ部会」も設置された．https://warp.ndl.go.jp/info:ndljp/pid/8295038/www.nisc.go.jp/conference/suisinkaigi/dai1/1kaigi.html
なお，この2機関は2001年1月22日に高度情報通信社会推進本部（以下「IT戦略本部」という．）の下におく組織として改組され，民間有識者の会議は「情報セキュリティ専門調査会」となった．https://warp.ndl.go.jp/info:ndljp/pid/8295038/www.kantei.go.jp/jp/singi/it2/dai1/pdfs/s3.pdf

9)　情報セキュリティ対策推進室の設置に関する規則（2000年2月29日内閣総理大臣決定）https://warp.ndl.go.jp/info:ndljp/pid/8295038/www.nisc.go.jp/conference/suisinkaigi/dai1/0229kisoku.html

10)　IT戦略本部情報セキュリティ専門調査会情報セキュリティ基本問題委員会第1次提言（2004年11月16日），p.20参照 https://www.nisc.go.jp/pdf/policy/kihon-s/teigen/1teigen_hontai.pdf

11)　IT戦略本部の情報セキュリティ対策のページ https://warp.ndl.go.jp/info:ndljp/pid/8295038/www.kantei.go.jp/jp/it/security/index.html
情報セキュリティポリシーに関するガイドライン（2000年7月18日）https://warp.ndl.go.jp/info:ndljp/pid/8295038/www.kantei.go.jp/jp/it/security/taisaku/pdfs/ISP_Guideline.pdf
重要インフラのサイバーテロ対策に係る特別行動計画（2000年12月15日）https://warp.ndl.go.jp/info:ndljp/pid/8295038/www.kantei.go.jp/jp/it/security/taisaku/2000_1215/pdfs/txt3.pdf

12)　高度情報通信ネットワーク社会形成基本法（平成12年法律第144号）第22条及び第36条第2項第6号参照（以下，「IT基本法」という．以下のURLは制定当時の旧IT基本法（2000年11月29日成立）のもの）https://warp.ndl.go.jp/info:ndljp/pid/8295038/www.kantei.go.jp/jp/singi/it2/hourei/honbun.html

13)　e-Japan戦略（2001年1月22日高度情報通信ネットワーク社会推進戦略本部（以下「IT戦略本部」という）決定）．なお，同戦略は，サイバーセキュリティ基本法に策定義務等が定められている「サイバーセキュリティ戦略」とは異なり，IT基本法に特別の根拠規定は存在しない．https://warp.ndl.go.jp/info:ndljp/pid/8295038/www.kantei.go.jp/jp/singi/it2/kettei/010122honbun.html

14)　脚注13「e-Japan戦略」における脚注では，「セキュリティ：情報セキュリティ．情報通信を利用する上での安全性．」と記載されていた．
また，関啓一郎「サイバーセキュリティ基本法の成立とその影響」（知的資産創造/2015年4月号，以下URL，pp.82参照）で「総合的な戦略は不在のままであった」と総括されている．https://www.nri.com/-/media/Corporate/jp/Files/PDF/knowledge/publication/chitekishisan/2015/04/cs20150408.pdf?la=ja-JP&hash=D5363AF4094C814F3F06FDB395323E824825A182

15)　e-Japan重点計画（2001年3月29日IT戦略本部決定）https://warp.ndl.go.jp/info:ndljp/pid/8295038/www.kantei.go.jp/jp/singi/it2/kettei/3siryou46.html

（以下「重点計画 2001」という.）において，ようやくセキュリティに関する具体的な記載が盛り込まれた．ここでは，「高度情報通信ネットワークにおける脅威に起因するサービス提供機能の停止をゼロとすることを目標とする.」とされ，重点計画 2001 における具体的施策については，すでに触れた政府部内の対策と重要インフラ等民間部門の対策に加え，「研究開発」，「人材育成」，「国際連携」など横断的施策の記載もあり，後の戦略の骨格となる要素が抽出されていた点は着目される．

本稿の主題である人材育成に関しても，同計画において「研修事業，資格制度の導入等を通じ，高いレベルの情報セキュリティ技術を有する人材を十分に確保するための多面的な育成を行う.」とされ，教育と資格という二本柱の下地ができていたといえよう．翌年の重点計画 2002[16]では，2001 年 11 月 23 日に我が国も署名した「サイバー犯罪に関する条約」という国際的潮流があったものの，人材育成に関しては試験科目の追加や新たな試験の導入[17]など前年度成果と「IT セキュリティ技能標準の策定・普及」等の新規施策の記載もなされたが，全体で 600 字程度でありボリュームがあるものではなく，基本方針の記載に変化はなかった．

1.2 安心（リスクゼロ）志向の戦略（2003 ～ 2008 年）

（1） 元祖の戦略（2003 年）

情報セキュリティに関して，戦略レベルで初めて策定されたのが翌 2003 年の e-Japan 戦略Ⅱ[18]である．Ⅰ～Ⅳの柱のうち「Ⅲ.新しい IT 社会基盤の整備」中，「2. 安全・安心な利用環境の整備」との項目が新設された．e-Japan 戦略Ⅱのこの部分は元祖の戦略と捉えることもできる．

ここでは，「実現したいこと」として「情報セキュリティを確保し，安心してインターネット等を利活用できる環境を構築することが必要である」と記載され，「安心」に重点が置かれている．重点計画 2001 にあった「ゼロにする」とまでは記載されていないが，「不正アクセス等による被害を最小限にするための（中略）体制を確立する」（同戦略 p.27 参照）としており，安心志向と整理できる．

人材育成面では，「政府職員等の教育訓練を推進するほか，資格制度の有効活用等に努める」（同戦略 p.27 参照）とされ，その後に引き継がれる「教育訓練」と「資格制度」という 2 本柱が掲げられた．加えて，民間を含む啓発を意図し「情報セキュリティ文化」[19]の定着を目指すとした点は，後述する「サイバー空間の衛生」や「サイバー空間における新たな公衆衛生活動（New Cyber Hygiene）」等にも通ずる面があり興味深い．

その後，e-Japan 戦略Ⅱに基づき策定された重点計画 2003，2004 では，各省庁の施策が数多く盛り込まれたものの基本方針に変更を及ぼすようなものはなかった．

（2） 旧 NISC の設置（2005 年）

2004 年 11 月の IT 戦略本部情報セキュリティ専門調査会情報セキュリティ基本問題委員会「第 1 次提言」[20]を踏まえ，2005 年 4 月，内閣官房情報セキュリティ対策推進室が改組・拡充され，情報セキュリティセンター（旧 NISC[21]）が設置された．また，同年 5 月に IT 戦略本部の下，内閣官房長官を議長とし関係大臣と有識者 6 名を構成員とす

16） e-Japan 重点計画 2002（2002 年 6 月 18 日 IT 戦略本部決定）https://warp.ndl.go.jp/info:ndljp/pid/8295038/www.kantei.go.jp/jp/singi/it2/kettei/020618-2-5.html

17） 電気通信主任技術者試験に情報セキュリティに関する試験科目を追加（総務省）（2001 年 4 月），情報処理技術者試験に情報セキュリティアドミニストレータ試験を導入（経済産業省）（2001 年 10 月）

18） e-Japan 戦略Ⅱ（2003 年 7 月 2 日 IT 戦略本部決定）https://warp.ndl.go.jp/info:ndljp/pid/8295038/www.kantei.go.jp/jp/singi/it2/kettei/030702ejapan.pdf

19） 2002 年に勧告された OECD の「情報システム及びネットワークセキュリティのガイドライン」で「セキュリティ文化の実装」が示されていた．（脚注 10「IT 戦略本部情報セキュリティ基本問題委員会第 1 次提言」，p.3 参照）

20） 脚注 10「IT 戦略本部情報セキュリティ基本問題委員会第 1 次提言」

21） National Information Security Center の略

る「情報セキュリティ政策会議」[22]が設置された．トップが政務レベルに引き上げられており，重みが全く異なるためその訴求力は大幅に向上したと評価できる．

この格上げされた体制の下，情報セキュリティ政策会議で2006年，2009年，2010年，2013年の計4回[23]，セキュリティ単独の中長期計画である基本戦略が策定された．これらを本稿では便宜上，各々「○年戦略」と呼称することとする．

(3) 2006年戦略（第1次情報セキュリティ基本計画）

2006年戦略[24]の志向としては，重要インフラについて「IT障害の発生を限りなくゼロにすることを目指し」（p.17参照），個人に関し「「IT利用に不安を感じる」とする個人を限りなくゼロにすることを目指し」（同戦略p.20参照）と掲げ，重点計画2001や2003年のe-Japan戦略Ⅱの安心志向の潮流を引き継いでいる．この点，2009年の第2次情報セキュリティ基本計画で「現実には容易ではない」（同p.26）と指摘されており，一般論としても心の不安をゼロにするというのは困難であるが，ブロードバンド・スマートフォン普及以前のインターネットは大衆化したとまではいえない状況であり，利用者側の一定のリテラシーの確保の下で，システム・技術的なアプローチによりリスクを限りなくゼロにできるのではないかとの期待が存在したのではないかとも考えられる．

次に，2006年戦略では実現すべき基本目標を定めているが，「事前に考えられる対策が十分に施されていること」，「その対策が施された環境を（中略）十分に理解したうえで使いこなしていること」，「対処方針があらかじめ検討されており，被害の局限化や救済等がなされ，事業の継続性が確保されること」の3条件（同戦略，p.5参照）とされた．3条件の3つ目は事後対処のための事前対策といえるものであり，また，4つの基本方針（同戦略，p.7参照）の3つ目で「安全保障・危機管理的な側面から（中略）公的部門の対応能力を戦略的に強化」が明記されたが，総じて事前対策に重点が置かれていると考えられる．

人材育成について「教育訓練」と「資格制度」という2本柱との関連では，教育訓練に関しては重要インフラにおける「分野横断的な演習の実施」や企業の情報システム担当者等に対する広報啓発など，各主体に応じた施策が盛り込まれた（同戦略p.19参照）．また，「多面的・総合的能力を有する実務家・専門家の育成」が必要とされ，従来から指摘されていた情報セキュリティ技術者に加えて「最高情報セキュリティ責任者（CISO）」，「各組織の情報システム運用担当者」などが例示された．また，資格制度に関しては「資格制度の体系化」が掲げられ，各主体それぞれに応じた適切なスキルを確定するとされた（同戦略p.22参照）．

1.3 深刻化するリスク前提の戦略（2009～2012年）

(1) 2009年戦略（第2次情報セキュリティ基本計画）

ブロードバンドの契約数は2003年度末時点で1,367万契約だったが，2009年度末時点で3倍弱の3,171万契約[25]となり当時の世帯の6割を超える状況となっていた．こうした中，2009年戦略[26]では，高齢化社会において，いわゆる情報弱者を

22）「情報セキュリティ政策会議の設置について」（平成17年5月30日報道発表）https://warp.ndl.go.jp/info:ndljp/pid/8295038/www.nisc.go.jp/conference/seisaku/pdf/050530seisaku-press.pdf

23）NISC主要公表資料 https://www.nisc.go.jp/policy/materials/index.html　第1次情報セキュリティ基本計画（2006.2.2），第2次情報セキュリティ基本計画（2009.2.3）及び国民を守る情報セキュリティ戦略（2010.5.11）は「基本計画関連」を参照．サイバーセキュリティ戦略（2013.6.10）は「サイバーセキュリティ戦略」を参照

24）第1次情報セキュリティ基本計画（2006年2月2日情報セキュリティ政策会議決定）https://www.nisc.go.jp/pdf/policy/kihon-s/bpc01_ts.pdf

25）平成22年版 情報通信白書図表4-1-1-5　ブロードバンド契約数の推移 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h22/html/me411200.html

含めて利用の裾野が拡大することなどを背景に「事故前提社会」が掲げられた．

事前対策について最大限の努力を行うとしながらも，事態の認知・分析，情報連絡，迅速な対応・復旧などの事業継続性を確保する観点からの事後対応に重点が置かれた．リスクの扱いについて，2006 年戦略にあった「ゼロにすることを目指す」のではなく，2009 年戦略では「客観的に許容可能な範囲内で管理できる水準」の対策を実施するとされた（同戦略 pp.27-28 参照）．この基本的な考え方は表現に差異はあるにせよ，後の CS 戦略で引き継がれており[27]，この時期に示された点は興味深い．

人材育成については，基本的な考え方として「情報セキュリティ人材の重要性が社会で十分認識され，（中略）優秀な人材が官民を問わず（中略）すすんで集まることを目指す」（同戦略 p.42 参照）とあり，逆にいえば，当時は社会的理解が十分に得られていなかった状況[28]を示しており，いわゆる好循環が起きていなかったことを示している．これに対応して，政府機関と民間企業における対応に加え，「情報セキュリティに関する能力向上に係る環境整備の進展」として「資格保有者等によるキャリアアップの道筋が見えやすくすること」を例示として掲げられている（同戦略 p.42-43 参照）が，これは現在においても課題であると考えられる．

各主体の取組としては，政府機関における緊急対応能力の強化等に係る記載として，2008 年度に本格運用を開始した GSOC[29]を核として緊急対応能力を向上させるとした（同戦略 p.50-51 参照）．また，地方公共団体が活用できるよう参考資料等を作成・紹介することとされており，対応を強化する方向となっている点も特筆される（同戦略 p.53 参照）．

なお，同戦略で事後対策の流れとして示された「事態の認知・分析」，「情報連絡」，「迅速な対応・復旧」という一連の手順が 2013 年から開始された「実践的サイバー防御演習（以下「CYDER」（サイダー）という．）」[30]の流れと概ね合致[31]しており興味深い．また，横断的なセキュリティ基盤として「設計段階からセキュリティを作り込む開発手法の普及と定着」が掲げられて設計・開発側の視点が入った．2013 年戦略において「政府機関の情報システムについて，その設計，製造，設置等の段階において情報セキュリティの技術標準化やその適合性の評価結果の活用が必要」としているが，その後，2015 年以降の CS 戦略に盛り込まれた「セキュリティ・バイ・デザイン」の原点となったと思われる点も着目される．

26） 第 2 次情報セキュリティ基本計画（2009 年 2 月 3 日情報セキュリティ政策会議決定）https://www.nisc.go.jp/pdf/policy/kihon-s/bpc02_ts.pdf

27） 「サイバーセキュリティ戦略（2015 年 9 月 4 日閣議決定），p.8」では「セキュリティリスクを許容し得る程度まで低減していくことが，今後の社会全体としての課題（チャレンジ）となる．」，「サイバーセキュリティ戦略（2018 年 7 月 27 日閣議決定），p.11」では「セキュリティリスクを許容し得る程度まで低減していくという課題への対処が求められる．」，「サイバーセキュリティ戦略（2021 年 9 月 28 日閣議決定），p.6」では「不確実性をできる限り制御していくアプローチが重要である．」としている．

28） いわゆる事業仕分け等に見られるように，コンピュータを含む ICT の利活用促進自体が広範な社会的理解を得られていたとはいえない状況であった．

29） Government Security Operation Coordination team の略 https://www.nisc.go.jp/policy/group/toukatsu/index.html

30） 2013 年に総務省の実証実験としてスタートし 2022 年現在も継続している．（参照）「ナショナルサイバートレーニングセンターにおけるセキュリティ人材育成の取組について」02 参考資料 p.3 参照 https://nct.nict.go.jp/file/national_cyber_training_center_20220805_reference.pdf

31） 以下のような対応関係になると考えられる．
「事態の認知・分析」≒ CYDER「検知・連絡受付，トリアージ（優先順位付け）」
「情報連絡，迅速な対応・復旧」≒ CYDER「インシデントレスポンス（対応：証拠保全，封じ込め，根絶，復旧措置），報告・公表，事後対応」
※なお，事態の分析や対応，情報連絡の中身が CYDER で明確化された．

（2）　2010年戦略（国民を守る情報セキュリティ戦略）

2010年戦略[32]では，2009年7月の米韓における大規模サイバー攻撃事態の発生等を踏まえ，大規模サイバー攻撃事態への対処に関する記載として「初動対処に係る訓練を実施する」とされたことや，前述したGSOCについて「政府横断的な情報収集・分析システムの充実・強化」として掲げられ，事前・事後という捉え方に加え，「能動的な」対策について明記された点が特筆される．

人材育成については「産学連携による実践的な人材育成手法等に基づく高度な情報セキュリティ人材を育成する」（同戦略 p.15 参照）とされ，産学連携の視点が入った．

（3）　深刻化するリスク前提の戦略のまとめ

以上のように，2009年及び2010年において策定された2つの戦略では，サイバー空間におけるリスクを正視し，米韓における大規模サイバー攻撃事態等の国際潮流を含めた時代の要請に応じて，「事故前提社会」という発想の転換を図り，事前対策に加えて事後対策の強化を打ち出すとともに，能動的な対策や連携についても言及し，先見性を持った基本方針を示すこととなった．

1.4　次元を変えた取組を加えた戦略（2013年～2017年）

（1）　2013年戦略（サイバーセキュリティ戦略）

2013年戦略[33]は，CS基本法に基づくCS戦略ではないため，閣議決定ではなく従来の情報セキュリティ政策会議決定であったが，現在に至るCS戦略の原点となったというべき戦略である．

まず，その証左として，「情報セキュリティ」に代わり「サイバーセキュリティ」という用語が初めて用いられた点がある．対策初期から言及されている不正侵入や不正プログラム（いわゆるコンピュータウイルス）に加え，情報システムの作動停止や誤作動が脅威としてあげられ，情報資産に対するセキュリティだけでなく，コンピュータと各種ネットワークで構成される仮想空間全体のセキュリティという視点に視野が拡大された．

IoT時代を迎え，広くサイバー空間に係る取組を推進する観点とされた．この点，「ソフトウェアの脆弱性等を狙うサイバー攻撃により，通信障害，交通混乱やブラックアウトといった事態が発生し大規模な社会的混乱や人の生死に直接的な影響をもたらすことも可能性として想定される」（同戦略，pp.7-8 参照）としており，社会インフラとしてのサイバー空間が意識されていたといえる．

また，2013年は，移動系ブロードバンドの契約数が固定系を超えた[34]年であり，主にスマートフォンを通じてサイバー空間が急速に日常の中に浸透していった時期でもあり，情報流出に限らず，社会インフラとしてのITサービス停止等の影響が大きくなることが予見されていたと考えられる．

さらに，この時期，国際潮流としても，米国，EU等が包括的な戦略を策定していた[35]ことも刺激となったと考えられ，「サイバー空間の持続性，発展性を確保する」といった目指すべき社会像や，現在に至るまで西側諸国の共通の価値である「情報の自由な流通の確保」という理念が基本的な考

32）　2010年戦略（2010年5月11日情報セキュリティ政策会議決定）https://www.nisc.go.jp/pdf/policy/kihon-s/senryaku.pdf

33）　2013年戦略（2013年6月10日情報セキュリティ政策会議決定）https://www.nisc.go.jp/pdf/policy/kihon-s/cyber-security-senryaku-set.pdf

34）　平成26年度情報通信白書（図表5-5-2-4）参照
なお，平成25年度末（2013年度末），3.9世代携帯電話（LTE）のブロードバンド契約数に占める契約数の割合は51.7％と示されている．https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/html/nc255210.html

35）　米国「National Security Strategy」（White House, May2010）「Cybersecurity, Innovation and the Internet Economy」（The Department of Commerce Internet Policy Task Force, June 2011）
EU「Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace（European Commission & High Representative of the Union for Foreign Affairs and Security Policy, Feb. 7, 2013）.

え方として謳われたことも着目される．

こうした国内外の状況を踏まえ，「次元を変えた取組が必要との認識」[36]が示された．「平時からの能動的な対策」や「共助」の取組を「サイバー空間の衛生」と呼称し，明記したのもこの戦略の先進的な特徴である．この概念は，2003年のe-Japan戦略Ⅱで定められた「情報セキュリティ文化」を発展させたものと思われ，その後のCS基本法に基づくCS戦略の原点となったといえる．

具体的には，事前のポリシー策定や事後の対処訓練などの受動的な対策に加え，平時からの能動的な対策として「認知解析機能の向上」や「情報共有の促進」，「脆弱性への対処」などを行うとされた．また，各主体が個別の対策に加えて各主体の連携，「共助」で行っていくという方針も示された．

対象がサイバーセキュリティに拡大されたという点ですでに次元を変えているともいえるが，このような対策面での「次元を変えた取組」の考え方は，例えば，左右の軸をそれぞれ従来の事前対策と事後対策とし，新たに上下の次元を設けてそれぞれ「受動」と「能動」の取組を置くとすると，下の次元にある能動的な取組を進めることと捉えることができる．実際に，この後のCS戦略やCS基本法改正，関連法改正に基づき，多様な主体が相互に連携し早期の段階で情報を迅速に共有するための「サイバーセキュリティ協議会」[37]やIoT機器の脆弱性調査及び注意喚起を行う「NOTICE」[38]などがこの領域の取組として行われるようになった．

2018年CS戦略[39]において「サイバー攻撃に対して能動的に防御していく取組のこと」を「積極的サイバー防御」と呼称することとなったが，その対象は主に左（事前段階）から真ん中（予兆段階）における，下（能動）の領域が中心の取組と考えられる．

人材育成についても，こうした大きな潮流を受けて，扱う領域や役割が拡大した中，これに応じる必要が生じたことも踏まえ，サイバーセキュリティ人材不足を受けた量的な観点で教育・トレーニングの必要性に加え，IoT時代における新たな課題への対応の必要性を踏まえて「教育だけでは得られない突出した能力を有する人材の確保」が大きな課題であるとされ，「優れた個人を発掘育成するための合宿研修や情報セキュリティ人材が実践的技能を競うコンテスト等を官民で連携し，実施する」とされた．また，「サイバーセキュリティ従事者の能力の底上げと，突出した人材の発掘・育成を図っていくためには，社会全体で育成し活用するための仕組みが必要である」とし，「公的資格・能力評価の改善や新設の必要性も含め（中略）ニーズの多様化に応じた検討を行う」とされた（2013年戦略，p.37参照）．これらの考え方は，2015年のCS戦略に基づく施策の前提となったと考えられる．

このように，2013年戦略は「情報」だけでなく，重要インフラサービス等の提供の前提となっている「情報システム」を含め，サイバー空間全体を明確に対象として視野に入れ，現在に至る施策の基盤となった．また，同戦略では，政府の体制について「NISCについては（中略）2015年度を目途として「サイバーセキュリティセンター」（仮称）

36） 脚注33「2013年戦略」，p.3参照

37） サイバーセキュリティ協議会 https://www.nisc.go.jp/council/cs/kyogikai/index.html

38） National Operation Towards IoT Clean Environmentの略 https://notice.go.jp/

39） サイバーセキュリティ戦略（2018年7月27日閣議決定），p.20参照 https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2018.pdf

「サイバーセキュリティ2019」，pp.20-21参照，以下抜粋 https://www.nisc.go.jp/pdf/policy/kihon-s/cs2019.pdf

「英国でも，ACDは平素からのISPと協力したネットワーク防御を意味しており，Offensive Cyber（サイバー攻撃能力）やhack back（逆ハック，サイバー反撃）のような取組とは明確に区別されており，新戦略で掲げる積極的サイバー防御にもこれらが含まれないことに留意が必要である．」なお，これらに関連し，松村（2021）において，サイバー攻撃阻止や被害限定といった拒否的抑止に加え，日本国憲法下における懲罰的抑止についても考察がなされている．

に改組する」とされ，司令塔の機能強化が謳われ，CS 基本法制定以降の体制の原点にもなった．

(2)　CS 基本法の制定（2014 年）

2014 年にいわゆる議員立法により CS 基本法が制定された．この経緯については，関（2015）[40]に詳述されているが，与野党合意の下で政治的リーダーシップがとられて制定されたことが特徴である．また，提案者の一人（平井卓也議員）が「サイバーセキュリティに関しては，国家の安全保障，危機管理にも関する分野であり，国と民間の役割を明確化した上で，国が主導的立場を果たしながら，官民の緊密な連携により取り組みを着実に進めていかなければならない」と答弁[41]しているように，安全保障・危機管理という要素が前面に出てきた．また，「国が主導的立場を果たす」ことが意図されていた点も重要である．

さらに，「サイバーセキュリティ」という用語を法令上定義した[42]ことも歴史的な意義を有する．情報の漏洩，滅失又は毀損の防止といういわゆる情報の CIA[43]に対応する規定が設けられるとともに，「情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置」と明記され，「情報」だけでなく，情報システムとネットワークのセキュリティ確保が射程に入ることが法令上明らかにされた．

人材育成については，2003 年の e-Japan 戦略Ⅱで示された二本柱（「教育訓練」と「資格制度」）のうち，「教育訓練」については国の行政機関，独立行政法人等の「サイバーセキュリティに関する演習及び訓練」が CS 基本法第 13 条で規定され，重要インフラ事業者についても「演習及び訓練（中略）その他の自主的な取組の促進その他必要な施策を講ずる」と同法第 14 条で規定され，「演習及び訓練」を進めることが法律で明記された．

また，「資格制度」に該当する部分については，同法第 22 条第 2 項で「国は，大学，高等専門学校，専修学校，民間事業者等と緊密な連携協力を図りながら，サイバーセキュリティに係る人材の確保，養成及び資質の向上のため，資格制度の活用，若年技術者の養成その他の必要な施策を講ずる」とされ，様々な主体の連携を図りながら，資格制度の活用を進めることが明記された．

(3)　NISC 設置と年金機構情報流出事案（2015 年）

2014 年の CS 基本法の制定後，2015 年 1 月に内閣官房組織令の改正により現・NISC[44]（内閣官房内閣サイバーセキュリティセンター）が発足した．CS 基本法第 26 条，第 28 条及び第 32 条等により，サイバーセキュリティ戦略本部長が関係行政機関の長に対しサイバーセキュリティに関する情報やデータの提出を求める権限や勧告する権限等が定められた．そのうえで，同本部の事務局を NISC が担うことを想定して内閣官房組織令で規定整備がなされた．同組織令に基づく GSOC 機能などその他の権限については，関（2015）[45]に詳述されているが，NISC の体制強化が法令上も図られたといえる[46]．

40）脚注 14「関啓一郎（2015）」，pp.84-87 参照

41）第 186 回国会　衆議院　内閣委員会　第 23 号　平成 26 年 6 月 11 日

42）サイバーセキュリティ基本法（抜粋）
第二条　この法律において「サイバーセキュリティ」とは，電子的方式，磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という．）により記録され，又は発信され，伝送され，若しくは受信される情報の漏えい，滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という．）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む．）が講じられ，その状態が適切に維持管理されていることをいう．

43）情報の機密性，完全性，可用性（それぞれ英語の Confidentiality, Integrity, Availability）

44）National center of Incident readiness and Strategy for Cybersecurity の略

45）脚注 14「関啓一郎（2015）」，pp.101-103 参照

46）谷脇康彦「サイバーセキュリティ」岩波書店，2018.10，pp.102-104 参照

このような体制の下，CS 基本法第 26 条第 1 項に基づく初めての CS 戦略の策定作業が本格化し，その策定過程であった 5 月，いわゆる年金機構情報流出事案が発生した．本事案は，日本年金機構において，外部からの標的型メールに添付されたウイルスに感染したことにより不正アクセスが行われ，個人情報約 125 万件が流出した事案である．

その原因については，検証委員会報告書[47]や原因究明調査書[48]によれば，個人情報等の重要情報を共有フォルダに保管しないというルールが徹底されていなかったことや，標的型メール攻撃の疑いについて組織内で情報共有が行われなかったことなどが指摘された．

この事案は，前述した権限行使の有効な先例となり，有事における具体的な対処能力を有する体制（CSIRT = Computer Security Incident Response Team）とそれを支える実践的な人材育成の重要性を改めて認識させ，政府関係機関に深く浸透させることとなったと考えられる．

（4） 2015 年 CS 戦略

このような経緯を踏まえ，サイバーセキュリティ戦略本部による検討が行われたうえで，2015 年 9 月にサイバーセキュリティ戦略（以下「2015 年 CS 戦略」[49]という．）が閣議決定された[50]．

その理念や内容については，三角（2021）[51]に詳述されているが，そのポイントは 2013 年戦略の基本的な潮流を引き継ぎつつ，基本認識と基本原則の確立，主体別ではなく CS 基本法の戦略目的[52]別に施策の方向性をまとめたものとなった点である．

人材育成施策を含む各施策の土台となる基本認識については，サイバー空間を経済成長のフロンティア[53]と捉え，「実空間とサイバー空間の融合が高度に深化した社会」（連接融合情報社会）が実現しつつあるとした．また，目指すサイバー空間を「自由，公正かつ安全なサイバー空間」とし，基本原則は 2013 年戦略にもあった「情報の自由な流通の確保」に加え，「法の支配」，「開放性」，「自律性」，「多様な主体の連携」の計 5 原則を掲げ，西側諸国の共通の価値観である自由，民主主義，法の支配と併せて，インターネットの基本思想（自律・分散・協調）を反映したものとなった．

サイバー空間を経済成長のフロンティアとして捉えるという基本認識はサイバーセキュリティ対策を「費用」ではなく積極的な経営への「投資」であるとの記載につながり，これは後の CS 戦略においても引き継がれた．また，従来からの重要インフラ，政府関係機関等対策の考え方として「機能保証（任務保証）」（同戦略 p.15 参照）の考え方が盛り込まれ，これも引き継がれることになった．また，戦略目的の 3 つ目に当たる「国際社会の平和・安定及び我が国の安全保障」の項目には，国際的な法の支配に向けた各国との連携などが盛り込まれた．さらに，これらを支える横断的施策として「研究開発の推進」に加えて「人材の育成・確保」が盛り込まれた．

47） 日本年金機構における不正アクセスによる情報流出事案検証委員会報告書（平成 27 年 8 月 21 日厚生労働省）https://www.mhlw.go.jp/stf/shingi2/0000095311.html

48） 日本年金機構における個人情報流出事案に関する原因究明調査結果（平成 27 年 8 月 20 日サイバーセキュリティ戦略本部）https://www.nisc.go.jp/pdf/council/cs/dai04/incident_report.pdf

49） サイバーセキュリティ戦略（2015 年 9 月 4 日閣議決定）https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku.pdf

50） なお，本稿では，法律に基づかない戦略と差別化する観点から，CS 基本法に基づく戦略を「○年 CS 戦略」と呼称している．

51） 三角育生「我が国のサイバーセキュリティ戦略策定の背景」日本セキュリティ・マネジメント学会誌 34（3），39-46，2021 https://www.jstage.jst.go.jp/article/jssmjournal/34/3/34_39/_pdf/-char/ja

52） 「経済社会の活力の向上及び持続的発展」，「国民が安全で安心して暮らせる社会の実現」，「国際社会の平和・安定及び我が国の安全保障」
（参照）サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 1 条

53） 脚注 49「2015 年 CS 戦略」，pp.1~2「サイバー空間は（中略）無限の価値を産むフロンティア」である人工の空間である．」との記載もある．

人材育成については，「サイバーセキュリティは，同分野の専門家はもちろん，一般的な情報通信技術者，ひいてはIoTシステムの利用者に至るまで，程度に差はあるものの様々な層の人材に必須の素養である」（同戦略p.35参照）とし，IoTにまで裾野が拡大することを示したうえで，演習・訓練については「サイバー演習の環境をクラウド環境で整備するとともに，産学官共同による教材開発を支援するなど，人材育成のための実践的な演習の取組を推進する」（同戦略p.35参照），「組織のサイバー対処に必要な能力を体系化するとともに，それらの能力を向上させるための実践的演習の取組を充実させる」（同戦略p.37参照）とされ，実践的なサイバー演習の環境整備が求められることとなった．また，資格に関しては，「サイバーセキュリティに従事する者の実践的な能力を適時適切に評価できる資格制度の創設」（同戦略p.37参照）などが盛り込まれた．

さらに，「実務の現場から経営までの各層において，それぞれのニーズに応じたサイバーセキュリティの知見を有する又は理解し判断できる人材が必要となる．（中略）サイバーセキュリティに特化して突出した能力のある人材に加え，こうした人材をリードしていく人材も必要となる．」とされた．サイバー空間を「経済成長のフロンティア」と捉える同戦略の考え方を踏まえれば，これは経営ニーズに応じて専門家をリードしてイノベーションにつなげることができるといった人材像を想定していたと考えられ，これも後の事業の下地にもなったと考えられる．

また，これらのまとめとして，「こうした取組等を通じ，人材の需要と供給の好循環を創出していく．」との記載もされており，2018年CS戦略で提示されたエコシステム（生態系）の前提となったと考えられる．

(5)　CS基本法改正と関連法の改正（2016年）

2015年CS戦略に基づき，翌2016年には年金機構等を監査・監視の対象とするのための規定整備等を内容とするCS基本法等の改正[54]が行われ，同法でいわゆるIPA[55]法も同時に改正され，最新のセキュリティに関する知識を備えた高度かつ実践的な人材に関する国家資格として「情報処理安全確保支援士」制度が創設されることとなった．

また，サイバー演習の環境をクラウド環境で整備する主体としては，国立研究開発法人情報通信研究機構（以下「NICT」という．）がその役割を担うこととなり，同年にNICT法の改正[56]も行われ，その業務の範囲に「その研究等に係る成果の普及として行うサイバーセキュリティに関する演習その他の訓練」を追加すること等が明記された．これを受けて，2016年度，NICTは「演習その他の訓練」を実施する組織としてセキュリティ人材育成研究センターを設置[57]し，演習・競技用模擬ネットワーク環境を提供し[58]，CYDER（2013年度から総務省事業として開始され実施されていた．）を継承・拡充した[59]．

2017年1月，総務省は「セキュリティ人材育成のスピードアップ」などの5項目を盛り込んだ「IoTサイバーセキュリティアクションプログラム

54)　サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律（2016年4月15日成立）https://www.shugiin.go.jp/internet/itdb_housei.nsf/html/housei/19020160422031.htm　https://www.sangiin.go.jp/japanese/joho1/kousei/gian/190/meisai/m19003190011.htm

55)　独立行政法人情報処理推進機構

56)　国立研究開発法人情報通信機構法及び特定通信・放送開発事業実施円滑化法の一部を改正する法律（2016年4月20日成立）https://www.shugiin.go.jp/internet/itdb_housei.nsf/html/housei/19020160427032.htm　https://www.sangiin.go.jp/japanese/joho1/kousei/gian/190/meisai/m19003190038.htm

57)　国立研究開発法人情報通信研究機構平成28年度事業報告書，p.12参照 https://www.soumu.go.jp/main_content/000496945.pdf

58)　脚注57「国立研究開発法人情報通信研究機構平成28年度事業報告書」，p.4参照

59)　脚注57「国立研究開発法人情報通信研究機構平成28年度事業報告書」，p.6参照
なお，総務省事業については以下，p.3参照 https://www.soumu.go.jp/main_content/000209377.pdf

2017」を公表した[60].

これを受け，同年4月にNICTはセキュリティ人材育成研究センターを改組してナショナルサイバートレーニングセンターを設置し，これまでのCYDERに加え，東京2020オリンピック・パラリンピック競技大会に向けた演習「サイバーコロッセオ」を引き継ぐとともに，若手セキュリティエンジニアの育成を目的とした「セキュリティイノベーター育成事業（以下「SecHack365」という.）」を新たに創設し，プレスリリースがなされ[61]，3つの人材育成事業を推進することとなった.

1.5 サイバーセキュリティ戦略の改定（2018年以降）

以上から，本稿で取り上げるこれらの人材育成事業の発端となった戦略は2015年CS戦略であるといえるが，CS戦略は現在に至るまで2度改定されており，人材育成事業に関して今後の潮流を検討するうえで特筆すべき点を整理することとする.

（1） 2018年CS戦略

2018年7月，2015年の時と同じくサイバーセキュリティ戦略本部での検討を経て，2018年CS戦略[62]が閣議決定された．その基本理念や原則は2015年CS戦略を踏襲したが，基本認識については，AIなど計算機科学の知見の更なる進展が期待されることを背景に「サイバー空間と実空間の一体化が進展」，「情報社会からSociety 5.0へのパラダイムシフトが生じつつある」とさらに踏み込んだ．サイバー空間を前提とするAIの実用の拡がりを想定し，脅威が一気に高まる可能性を示した.

こうした脅威に対する対処として，2009年戦略で示した「事故前提社会」の下でリスクを制御する考え方や2013年戦略で示した「サイバー空間の衛生」として各主体が共助で取り組むこと等のこれまでの考え方を整理・統合し，サイバーセキュリティの基本的な在り方として「サービス提供者の任務保証」，「リスクマネジメント」，「参加・連携・協働」という3つの観点から取り組み，サイバー空間が自律的・持続的に進化・発展する生態系「サイバーセキュリティエコシステム」（2018年CS戦略 pp.10-12参照）を目指すとした．このうち，「参加・連携・協働」については「サイバー空間における新たな公衆衛生活動（New Cyber Hygiene）」と捉えて基本的な取組と位置付ける必要があるとされた．これは2013年戦略にある「サイバー空間の衛生」をさらに発展させたものと捉えられる.

リスクの捉え方としては，リスクマネジメントとして「完全なリスクの除去は不可能であることから，リスクの性格や影響の現れ方に応じて適切に対処し，その効用と比較してセキュリティリスクを許容し得る程度まで低減していく」（2018年CS戦略 p.11参照）とされ，2009年戦略以来の潮流を引き継ぐものとなっている.

エコシステムの考え方は，人材育成にも反映され，「教育等を通じ，資格・評価基準等によって可視化された確かな知識と実践力を備えた人材が，適切な処遇を受け，更に実務経験を積み重ねることにより，人材の需要と供給が相応されるといった好循環の形成」（2018年CS戦略 p.37参照）とされ，持続可能性を含む循環が意識された.

人材育成施策については，「戦略マネジメント層の育成・定着」，「実務者層・技術者層の育成」，「人材育成基盤の整備」など5項目に分けて方向性が整理された．「戦略マネジメント層の育成・定着」はサイバー空間の利用が経営戦略や事業戦略と直結してくるという状況を踏まえ経営層と実務

60）「IoTサイバーセキュリティ アクションプログラム2017」の公表（2017年1月17日）https://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000115.html

61）「ナショナルサイバートレーニングセンター」の設置等のプレスリリース（2017年4月3日）https://www.nict.go.jp/press/2017/04/03-1.html
なお，同プレスリリースで，NICT理事長に対し助言を行う「ナショナルサイバートレーニングセンター・アドバイザリーコミッティー」の設置も発表された．2021年8月18日現在の委員は以下のとおり．https://www.nict.go.jp/nct/nct-advisory-committee-members.html

62） 脚注39「サイバーセキュリティ戦略（2018年7月27日閣議決定）」

者の間でリスクマネジメントを支える役割の重要性を提起したものであり，IPA の産業サイバーセキュリティセンターにおけるプログラムの開始につながった．また，「実務者層・技術者層の育成」では資格・試験，演習の実施などを引き続き強化を図っていく必要があるとし，「チームの一員として対処ができるようにすること」や「戦略マネジメント層が示す概念的・抽象的な考えを理解し，それを具体化」を重要な点として掲げ（同戦略 p.38 参照），CYDER などを念頭に，実践的な演習が引き続き必要とされた．さらに，「人材育成基盤の整備」において SecHack365 を念頭に「将来，高度なサイバーセキュリティ技術を持つ人材となることが期待される若年層向けに，（中略）自由にサイバー関連ツール，機器を用いて興味を持って学べる機会が豊富に用意されるような環境整備」との記載もされた．

（2） 2021 年 CS 戦略

2021 年 CS 戦略[63]は，2021 年 9 月，サイバーセキュリティ戦略本部での検討を経て閣議決定された．同戦略では，過去 2 回の CS 戦略で示した「自由，公正かつ安全なサイバー空間」や基本原則といった「基本的な立場」を堅持する（同戦略，p.4 参照）としたことが重要なポイントである．

そのうえで，時代認識として新型コロナ禍の影響による不連続な変化と安全保障環境の変化により，サイバー空間をとりまく不確実性（リスク）が変容し，増大しているとした．リスクへの対処については 2009 年戦略以来の立場を踏襲し，「不確実性をできる限り制御していくアプローチが重要である」とした．

また，新型コロナ禍への対応としてテレワークや教育における ICT 活用等のデジタル技術の活用が加速し，サイバー空間の「公共空間化」が進展したとした．これは「連接融合情報社会」や「サイバー空間と実空間の一体化」といった記載より，サイバー空間での活動が公的なものとして扱われることが一般的になるという意味で別の次元でより踏み込んだ表現になったと捉えられる．

こうした認識の下，「あらゆる国民，セクター，地域等において，サイバーセキュリティの確保が必要とされる時代（Cybersecurity for All）」が到来したとされた．これを踏まえ，諸施策の目標や実施方針として，今後，デジタル化の動きと呼応し「誰一人取り残さない」サイバーセキュリティの確保に向けた取組を進める必要があるとされた．

なお，デジタル庁を司令塔とする社会全体のデジタル化の動きと呼応していくという基本方針の一方で，同戦略では，2020 年の国際連合の宣言を引用し，サイバー空間の利用に関し「不適切に悪意をもって利用されれば，国家間における分断や危険を増大させ，人権を阻害し，不公平を拡大し得る」とし，また，国際社会の現状から，「自由，公正かつ安全なサイバー空間」の確保は危機に直面していると警鐘をならすものとなっている．また，「サイバー空間が公共空間へと変貌を遂げつつある一方で，このような状況により，国民がサイバー空間に対する不安感を完全に払拭できていないことも事実」，「中長期的にはその前提も大きく変わり得ることも同時に意識することが重要」（2021 年 CS 戦略，p.6 参照）とも明記しており，黎明期の戦略のような安心志向の潮流が強まる可能性にも触れているように思われる．

施策の方向性としては，これまでの戦略でも掲げられた自律的な取組（「自助」）や多様な主体の緊密連携（「共助」）に加え，それらの基盤となる「公助」の役割をはじめとした多層的な取組強化に加え「国がインシデント対応とその後の再発防止や改善に向けた政策措置を一体的に推進するための総合的な調整を担うナショナルサート（CSIRT/CERT）の枠組みの強化を図り」との記載がなされたことも特筆される．

人材育成の観点では，「質」・「量」両面での官民の取組を一層継続深化させていくとしたうえで，経営層をはじめ必ずしも専門知識などを有していない人材に社内外のセキュリティ専門家と協働す

63） サイバーセキュリティ戦略（2021 年 9 月 28 日閣議決定）https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf

るにあたって時宜に応じて「プラス・セキュリティ」知識が補充され，社会全体で「DX with Cybersecurity」を推進していくことが重要とした．また，実践的な対処能力を持つ人材育成の重要性は一層増しているとし，「資格制度の整備・改善」，「若年層向けのプログラム」，「演習環境の提供」を例示しつつ，「取組を一層強化し，コンテンツの開発・改善を図っていく」とされた．また，「講師の質の担保等に留意」などきめ細かな記載が盛り込まれた（同戦略 pp.38-40 参照）．

2. 各人材育成施策の状況

人材育成施策については，2003 年 e-Japan 戦略Ⅱで「教育訓練」と「資格制度」という 2 本柱が挙げられ，2009 年戦略や 2013 年戦略で示された基本的な考え方をベースに，2015 年 CS 戦略に基づき強化されて推進されている．

主な事業として，IPA の「産業サイバーセキュリティセンター中核人材育成プログラム」や「セキュリティ・キャンプ」，「未踏 IT 人材発掘・育成事業」，NICT が構築を進め民間事業者等へのオープン化に向けたトライアル等が開始されたサイバーセキュリティ統合知的・人材育成基盤「CYNEX（Cybersecurity Nexus）」などもあるが，本稿では筆者が直接関わった施策を取り上げ，その実施状況の整理と考察を行う．

2.1 演習その他の訓練

（1） 実践的サイバー防御演習（CYDER）

CYDER は，国の行政機関，地方公共団体，重要インフラ等を対象として，NICT が有するサイバーセキュリティの技術的知見等を最大限に活かした実践的なサイバー防御演習である．その特徴は，インシデント発生から解決，事後対応までを実機を使って体験できる点である．事前オンライン学習も準備しており，NICT の公表資料[64]によれば「「ベンダーお任せ」では済まない，インシデント発生時の即応的な対処のために最低限必要なスキルを厳選して凝縮し，1 日程度のコンパクトで効率的な実機演習できる」としている．また，大規模高性能サーバー群「NICT 北陸 StarBED 技術センター」のクラウド環境を活用できる点も特筆される．

集合演習の流れとしては，「検知・連絡受付」，「トリアージ（優先順位付け）」，「インシデントレスポンス（対応：証拠保全，封じ込め，根絶，復旧措置）」，「報告・公表」，「事後対応」となっており，中でも，トリアージについては，委託しているセキュリティベンダや専門家だけでは判断が難しい，経営層の立場に立ち前述した「任務保証」の観点からの判断が必要なものである．また，報告・公表についても対外的に非常に重要であり，いずれも実践的な演習となっている．

受講者の実績としては，総務省事業として 2013 年度より開始され，2015 年度までの 3 年間は 292 人，507 人，715 人であり計 1,500 人程度であったが，2016 年度は NICT（セキュリティ人材育成研究センター）が事業を引き継いで 1 年間で 1,539 人[65]の受講を実現した．その後，2017 年 4 月の「ナショナルサイバートレーニングセンター」の設置の際[66]に，「CYDER の開催規模の大幅な拡充（47 都道府県で 100 回 3000 人実施予定）」が掲げられた．

具体的な演習の受講人数は，2017 年度は計 3,009

64） ナショナルサイバートレーニングセンターお知らせ https://nct.nict.go.jp/#news
「ナショナルサイバートレーニングセンターにおけるセキュリティ人材育成の取組について」01 説明資料 https://nct.nict.go.jp/file/national_cyber_training_center_20220805.pdf
02 参考資料 https://nct.nict.go.jp/file/national_cyber_training_center_20220805_reference.pdf

65） 内訳（国の機関等：420 人，地方公共団体向け：1,119 人）https://cyder.nict.go.jp/about/report/2016/index.html

66） 脚注 61「ナショナルサイバートレーニングセンター」の設置等のプレスリリース（2017 年 4 月 3 日）（1 ①）参照．なお，この前提として，総務省「IoT サイバーセキュリティ アクションプログラム 2017」（2017 年 1 月）（脚注 60 参照）において，「官公庁，地方公共団体，独立行政法人及び重要インフラ企業等に対する実践的なサイバー防御演習⇒ 47 都道府県で演習を実施し，演習規模を 3000 人まで拡大」として公表されている．

人[67]，2018 年度は計 2,666 人[68]，2019 年度は計 3,090 人[69]が受講した．2020 年度は，相次ぐ，新型コロナウイルス感染症緊急事態宣言やまん延防止等重点措置の発令で主な対象である地方公共団体の受講キャンセルが多数発生したことなどにより伸び悩み，2020 年度の受講は計 2,648 人[70]となり，2021 年度も同様の要因により集合演習の受講は計 2,454 人[71]となった．なお，2021 年度は，新設されたオンライン演習に 641 人が受講しており，演習の性質は異なるがこれを合わせれば 3,095 人[72]が受講したことになる．事業が開始された 2013 年度からの集合演習の受講者の累積数については，オンライン演習の受講者を除き，計 16,121 人となった．

新型コロナの影響も受け，当初掲げた受講者目標に達さない年もあったが，「受講勧奨に向けた周知広報や新型コロナ対策」[73]の着実な実施や，オンライン事前学習と 2021 年度開始のオンライン演習を含めたオンラインの活用なども通じて，サイバー攻撃に対応する実践的な演習を受けた者は着実に蓄積されたと評価できる．

(2) セキュリティイノベーター育成事業（SecHack365）

SecHack365 は，世界のセキュリティソフトウェア市場における我が国の存在感が決して大きくないなど，欧米等海外に比べ遅れているとの認識を背景に，既存のセキュリティソフトウェア等を単に「ユーザー」として利用するだけではなく，新たに自ら「研究・開発」していくことができる人材の育成が必要との問題意識から，「自ら手を動かし，セキュリティに関わる新たなモノづくりができる人材（セキュリティイノベーター）」[74]を育成するための事業[75]として 2017 年度より開始された．

この考え方については，2009 年戦略にある「設計段階からセキュリティを作り込む開発手法の普及と定着」以来の「セキュリティ・バイ・デザイン」を実現する突出した専門家の発掘・育成という問題意識に加え，2015 年戦略で示された専門家

67) サイバーセキュリティ政策に係る年次報告（2017 年度），p.112 参照 https://www.nisc.go.jp/pdf/policy/kihon-s/jseval_2017.pdf
内訳　A：1,477 人，B-1：649 人，B-2：883 人 https://cyder.nict.go.jp/about/report/2017/index.html

68) サイバーセキュリティ 2019，p.183 参照 https://www.nisc.go.jp/pdf/policy/kihon-s/cs2019.pdf
内訳　A：1,389 人，B-1：708 人，B-2：303 人，B-3：266 人 CYDER 過去の開催実績：https://cyder.nict.go.jp/about/report/2018/index.html

69) サイバーセキュリティ 2020，p.161 参照 https://www.nisc.go.jp/pdf/policy/kihon-s/cs2020.pdf
内訳　A：1,949 人，B-1：593 人，B2：548 人 CYDER 過去の開催実績：https://cyder.nict.go.jp/about/report/2019/index.html

70) サイバーセキュリティ 2021，p.173 参照 https://www.nisc.go.jp/pdf/policy/kihon-s/cs2021.pdf
内訳　A：2,036 人，B-1：391 人，B2：221 人 CYDER 過去の開催実績：https://cyder.nict.go.jp/about/report/2020/index.html

71) サイバーセキュリティ 2022，p.183 参照 https://www.nisc.go.jp/pdf/policy/kihon-s/cs2022.pdf
内訳　A：1,656 人，B-1：411 人，B2：315 人，準上級 C：72 人 CYDER 過去の開催実績：https://cyder.nict.go.jp/about/report/2021/index.html

72) 国立研究開発法人情報通信研究機構令和 3 年度の業務実績に関する項目別自己評価書，p.95 参照 https://www.soumu.go.jp/main_content/000828659.pdf

73) 周知広報（基礎情報提供（動画，パンフ等）：https://cyder.nict.go.jp/about/index.html
イベント・セミナー：https://cyder.nict.go.jp/event/index.html#old
メールマガジン：https://cyder.nict.go.jp/mailmagazine/index.html
新型コロナ対策（脚注 72「国立研究開発法人情報通信研究機構令和 3 年度の業務実績に関する項目別自己評価書」，p.96．以下抜粋 「新型コロナウイルス感染症対策を徹底した．CO_2 センサーでの換気状況監視，サーキュレータによる換気を実施すると共に会場内でのマスク着用の徹底（講師，チューター，現場スタッフは，マスクとフェイスシールドを併用）し，参加人数が会場の収容人数（定員）の 50％未満となる会場を確保した．」

74) 脚注 64「「ナショナルサイバートレーニングセンターにおけるセキュリティ人材育成の取組について」01 説明資料」p.19 にも同様の表現がある．

75) 脚注 61「ナショナルサイバートレーニングセンター」の設置等のプレスリリース（2017 年 4 月 3 日）

をリードしてイノベーションにつなげる起業家的な人材像も踏まえたものであると考えられる[76]．

この取組の概要は，毎年度40名程度の受講生を選抜し，NICTの持つ長年の研究開発のノウハウや，実際のサイバー攻撃関連データとそれらを安全に利用して研究開発が行える環境を活かし，年6回のイベントを軸とした，いわゆるハッカソンと呼ばれる訓練を行っている．その特徴はコースごとに研究開発・セキュリティのスペシャリストからなるトレーナー陣[77]が指導に当たる点である．

修了生の数については，2017年度は39人[78]，2018年度は3コース制（表現駆動・思索駆動・開発駆動）を導入し46人[79]であった．2019年度からは育成プログラムを5コース（学習駆動・研究駆動を追加）に細分化し，45人が修了した[80]．2020年度は41人[81]が修了し，2021年度は41人が修了した．これにより，2021年度までの累計で，事業開始から212人が修了した状況[82]となっている．

また，国際協力・連携に資する修了生の海外派遣として，米国での世界最大級のハッカソンへの派遣や2018年11月に総務省及びイスラエル国家サイバー総局においてMoC（サイバーセキュリティ分野における協力に関する覚書）が締結されたことを受けグローバルイベントへの参加が2019年度まで行われた[83]．

2020年度及び2021年度は，新型コロナの影響で，年間プログラムを再検討してイベント等をオンラインやチャットツールでの指導を実施し，成果発表会もオンラインで実施するなど全プログラムをオンラインで実施することとなった[84]．なお，筆者も本事業に一部関わったが，後述するCYDERのオンライン演習においても共通する課題があるが，完全オンラインで効率化する面は当然あるものの，現行のツールにより制約された視覚と聴覚のみを用いるコミュニケーションではその量と質の不足が生じざるを得ない面があり，協創機会という観点で不足が生じたとも考えられる．

他方，本事業の成果としては，修了生が情報処理学会の優秀論文賞や情報危機管理コンテストの文部科学大臣賞・経済産業大臣賞などを受賞し，起業を行うなど，各方面での活躍が報告されている．2021年度における「SecHack365」修了生の主な成果としても，学会・研究会等の活動において執筆した論文が受賞した[85]とされ，成果は着実に蓄積されている．

76） 脚注67「サイバーセキュリティ政策に係る年次報告（2017年度）」，pp.111-112参照．SecHack365は，「(4) 人材が将来にわたって活躍し続けるための環境整備」の項目に分類されている．
脚注49「サイバーセキュリティ戦略（2015年9月4日閣議決定）」p.37参照

77） SecHack365のHP　https://sechack365.nict.go.jp/　ページ最下部のパンフレット参照

78） 脚注67「サイバーセキュリティ政策に係る年次報告（2017年度）」，p.112

79） 脚注68「サイバーセキュリティ2019」，p.185

80） 脚注69「サイバーセキュリティ2020」，p.163

81） 脚注70「サイバーセキュリティ2021」，p.175

82） 脚注71「サイバーセキュリティ2022」，p.183

83） 脚注64「「ナショナルサイバートレーニングセンターにおけるセキュリティ人材育成の取組について」02参考資料」，pp.26-27
国立研究開発法人情報通信研究機構平成30年度の業務実績に関する項目別自己評価書，p.146　https://www.soumu.go.jp/main_content/000647336.pdf
国立研究開発法人情報通信研究機構令和元年度の業務実績に関する項目別自己評価書，p.169　https://www.soumu.go.jp/main_content/000704859.pdf

84） 国立研究開発法人情報通信研究機構令和2年度の業務実績に関する項目別自己評価書 p.173　https://www.soumu.go.jp/main_content/000763048.pdf
脚注72「国立研究開発法人情報通信研究機構令和3年度の業務実績に関する項目別自己評価書」pp.97-98

85） 脚注72「国立研究開発法人情報通信研究機構令和3年度の業務実績に関する項目別自己評価書」，p.98.以下抜粋
「CSS2021最優秀論文賞「接触確認フレームワークに対する陽性者特定攻撃の評価と対策」コンピュータセキュリティシンポジウム2021，筆頭著者：令和2年度SecHack365優秀修了生
CSS2021優秀論文賞「Androidアプリの自動リンクにおける悪意のあるリンク生成リスクの検討」コンピュータセキュリティシンポジウム2021，筆頭著者：令和2年度SecHack365修了生」

2.2　2021 年度新規の取組

（1）　CYDER 関連の新規の取組

① オンライン演習

2021 年 11 月，時間的・地理的要因で参加が困難な者を対象とする個人演習としてオンライン演習が開始され，報道発表された[86]．事前学習は 1 時間程度で演習 1 日間という枠組みは集合演習と同様である．同報道資料において「個人学習向けに最適化したもので，自習形式でありながら，相応の学習効果が得られるように設計されています.」とされているように，チームで行う演習ではなく，個人学習向けのものになっているのが特徴である．

NICT 自己評価書[87]によれば，オンライン演習開講に向けて，2 カ月間，約 300 名の受講者に対してテストを実施し，その結果を踏まえて改修するなど準備万端に進められた．同評価書によれば，「個人受講においても，集合演習のグループ発表を疑似体験できる課題を含むシナリオ構成とした.」としている．

筆者は，集合演習を複数回視察し，オンライン演習を 2022 年 2 月に受講しているが，自分のペースを行うことができるという利点があり，知識修得という点で大きな支障はないものの，集合演習では配備されているチューター等にちょっとした疑問を聞くことができないため時間を浪費してしまう場合があることを実感した．これに加え，同演習の肝である「トリアージ」（優先順位付け）や「報告・公表」に至る場面においてグループワークができない点がチームとしての対応能力の育成の観点でどうしても劣ってしまうとの印象を持った．

こうした点は NICT においても当初より認識されており，同報道資料でも「グループメンバーと協調しながら課題に取り組む集合演習と両方受講いただくことで，相乗効果が得られ，一層理解が深まるように設計されています.」とされている．

86）　報道資料 CYDER「オンライン A コース」の提供を開始 https://www.nict.go.jp/press/2021/11/09-1.html

87）　脚注 72「国立研究開発法人情報通信研究機構令和 3 年度の業務実績に関する項目別自己評価書」，p.96 参照

時間的・地理的要因で集合演習への参加が困難な者への対応を優先した形となったと考えられる．この点，ICT サイバーセキュリティ総合対策 2022[88]において「地理的・時間的要因等により CYDER が受講できない者への最低限の対応としてオンライン演習のコースを追加した」との認識が示されている．受講者については，前述したとおり，2021 年 11 月から 2022 年 3 月までの間，641 人が受講し，一定の成果があがった．

2022 年度においては，標準コース（5/24 ～ 7/19）に加え，入門コース（2023 年 1 月～ 2 月予定）を新設することとされている[89]．これは，集合演習に参加できない初学者向けという趣旨をより一層明確にしようという取組であると考えられる．

ただし，時間的・地理的な制約については構造的な問題であり，オンライン上で円滑なグループワークができるようにするという課題については，テレワークにおける課題とも共通であると考えられ，いわゆる「メタバース」なども含め，これを解決する新たな技術，ツールの可能性，その活用の在り方について引き続き検討することが重要であると考えられる．

② CYDER 準上級 C コースの新設

2021 年度，NICT はサイバーコロッセオ事業（2020 年度限りで終了[90]）で蓄積した演習ノウハウを生かし，より高いレベルを目指した C コースを新

88）　ICT サイバーセキュリティ総合対策 2022（2022 年 8 月総務省 サイバーセキュリティタスクフォース）（令和 4 年 8 月 12 日報道発表）p.33 参照．https://www.soumu.go.jp/main_content/000829941.pdf

89）　脚注 64「ナショナルサイバートレーニングセンターにおけるセキュリティ人材育成の取組について」01 説明資料，p.7 参照

90）　脚注 88「ICT サイバーセキュリティ総合対策 2022」p.34 参照．以下抜粋．

「同演習は（中略）2020 年度で目標とする人材育成を完了した（実機演習を伴った演習（コロッセオ演習）で延べ 571 名，講義演習形式による演習（コロッセオカレッジ）で延べ 1717 名の人材を育成）.」

脚注 64「ナショナルサイバートレーニングセンターにおけるセキュリティ人材育成の取組について」02 参考資料，pp.31-38 参照

設した．攻撃者の攻撃手法やその痕跡に対する高いレベルで取り組み，受講者がしっかりと技術を習熟できるように工夫し，2日間の演習コースとして開催し受講者は109人であった．

本コースについては，サイバーコロッセオ事業がレガシーとして活用されていることを踏まえ，今後も2025年日本国際博覧会（以下「大阪・関西万博」という．）をはじめサイバー攻撃の可能性が高まる世界規模のイベントが開催されることも想定されるため，こうしたイベントにおけるレガシーを着実に反映していく取組が求められると考えられる．

(2)　実践サイバー演習（RPCI）と関連制度

「情報処理安全確保支援士制度」は，2015年CS戦略の「サイバーセキュリティに従事する者の実践的な能力適時適切に評価できる資格制度」として，2016年10月に「サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律」が施行され，開始された．

制度趣旨を踏まえた特徴として，同資格は3年ごとの更新制が採られていたが，この更新講習については，2020年のIPA法の改正（2021年5月15日施行）により，目指すキャリアパスに応じて知識・技能の実践的な活用力を修得することを目的として，IPAが行う汎用的な講習以外の一定の条件を満たした講習も「特定講習」として認められるようになった．これを踏まえ，2021年度より，この特定講習の一つとしてNICTが行う実践サイバー演習（以下「RPCI」（リプシイ）という．）が選定された（2021年3月31日）．NICTは同年7月にRPCIの報道発表[91]を行い，募集を開始し演習を同年8月から9月までの間，計10回開催して57名が受講した．

受講者アンケート[92]では，56％が5段階評価の5と回答し，3（普通）以下の評価はなかったとされ，高い評価が得られたといえる．特に，「グループワークで活発な意見を交わすことで，自分にはない考え方や気づきを習得でき」や「適切なタイミングでチューターからのコメントやアドバイスがあるので進むべき方向性などが確認できる」というコメントがあったとされ，他の特定講習がオンライン演習も多かったことと比較し，集合演習の利点が示された形となった．

今後，「実践的な能力を適時適切に評価できる」という制度趣旨に沿って，情報処理安全確保支援士制度の発展によるサイバーセキュリティ人材の育成の好循環に貢献すべく，RPCIの更なる改善と着実な実施を図っていくべきであると考えられる．

3. 今後に向けた考察

サイバー空間とそれを取り巻く状況の変化に伴い，様々な戦略策定とこれらに基づく施策が講じられてきた．今後，ロシアによるウクライナ侵略等の国際社会における安全保障を巡る状況の緊迫化[93]に伴う世界的なサイバーセキュリティの脅威への対応に加え，メタバース等のサイバー空間の新たな潮流[94]への目配りも必要であり，対策を強化していく必要がある．人材育成については，演習基盤の民間事業者等へのオープン化などを含め

91)　公的機関初の情報処理安全確保支援士向け特定講習実践サイバー演習「RPCI」の受付開始（2021年7月14日）https://www.nict.go.jp/press/2021/07/14-1.html

92)　脚注64「ナショナルサイバートレーニングセンターにおけるセキュリティ人材育成の取組について」01説明資料，p14参照

93)　脚注88「ICTサイバーセキュリティ総合対策2022」，p.9参照

94)　「経済財政運営と改革の基本方針2022（令和4年6月7日閣議決定）」，p.17参照．以下抜粋

「ブロックチェーン技術を基盤とするNFTやDAOの利用等のWeb3.0の推進に向けた環境整備の検討を進める．さらに，メタバースも含めたコンテンツの利用拡大に向け，2023年通常国会での関連法案の提出を図る．」https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/2022/2022_basicpolicies_ja.pdf

総務省「Web3時代に向けたメタバース等の利活用に関する研究会」（令和4年7月13日報道発表）https://www.soumu.go.jp/menu_news/s-news/01iicp01_02000109.html

た多様なニーズに対応しつつ，地道な取組を蓄積し，全体のサイバーセキュリティ対策の基盤となる取組を「質」・「量」ともに強化していく必要がある．

本稿で取り上げた事業については，これまで触れてきたとおり一定の成果を出しつつあるが，関係の当初予算は横ばいからやや減少傾向[95]となっており，継続事業に対する厳しい視線が感じられる．他方，CYDER については未受講の地方公共団体があることも指摘[96]されており，オンライン演習の背景であった地理的・時間的要因等の解決など多様なニーズに応えること[97]や新たな技術・ツールの活用等の模索なども引き続き求められる．加えて，2025 年開催の大阪・関西万博など大規模国際イベントは攻撃インセンティブが高まるおそれがある[98]ため十分な対策が必要である．

なお，オンラインの活用については，制約された視覚と聴覚に依存する現状のオンライン演習では，特に，各種戦略でも示された「共助」の根幹であるグループワークに関して時間的な面，コミュニケーションの面で限界があることが実証された．逆に，集合演習でのグループワークに高評価が得られたが講師に依存する面があると考えられるため質の高い講師の確保は課題である．また，指導方法によってはオンラインでも効果をあげることができる可能性もあり，さらなる取組の蓄積が求められると考えられる．

また，全体としてサイバー空間の安全性及び信頼性を確保するためには，既存のサイバー攻撃事例の分析対処に加え，想像力を働かせた対処や柔軟な思考による「セキュリティ・バイ・デザイン」が重要なことに変わりはない．これを実現するには，2021 年 CS 戦略で示された，同時に DX を推進する視点「DX with Cybersecurity」が必須である．DX によりコスト削減に加え収益増が得られて初めて，セキュリティ対策が「投資」として機能する．

今後も引き続き，関係予算を確保し，社会インフラとなる機関における地道な演習・訓練の実施等により社会全体の実践的な対処能力の強化を図るとともに，新たな価値を創造する際には同時にセキュリティを組み込むという「DX with Cybersecurity」に向けて，資格制度による人材育成の好循環を維持しつつ，突出した専門能力に加えてイノベーションを引き起こす力を持つ若手人材の発掘・育成が不可欠であると考えられる．

おわりに

以上，サイバーセキュリティの政策全体の方針に関するこれまでの歴史的経緯について，実施体制ではなくリスクに対する考え方などその内容ごとに整理しつつ人材育成施策を関連させて論じてきたが，これらをまとめると以下のとおりである．

95）行政事業レビューシートによれば，ナショナルサイバートレーニングセンター関連の予算は，2017 年度：14.99 億円，2018 年度：15.07 億円，2019 年度：14.87 億円，2020 年度：15 億円，2021 年度：11.99 億円，2022 年度：11.87 億円となっている．なお，2021 年度の減少はサイバーコロッセオ事業が 2020 年度（令和 2 年度）で終了となった影響と思われる．

令和 2 年度行政事業レビューシート https://www.soumu.go.jp/main_content/000721476.pdf

令和 3 年度行政事業レビューシート https://www.soumu.go.jp/main_content/000767808.pdf

令和 4 年度行政事業レビューシート https://www.soumu.go.jp/main_content/000834445.pdf

なお，令和 3 年度（2021 年度）補正予算として「サイバーセキュリティ演習環境の拡充」（11.7 億円）が計上されており，前述（脚注 73）の新型コロナ対策への対応も含め，演習環境の改善が期待される．以下「令和 3 年度総務省所管補正予算（案）の概要」p.6 参照 https://www.soumu.go.jp/menu_news/s-news/01kanbo04_02000173.html https://www.soumu.go.jp/main_content/000779895.pdf

また，令和 5 年度（2023 年度）予算概算要求（2022 年 8 月）では 13.0 億円となっている．以下資料 p.19 参照 https://www.soumu.go.jp/main_content/000834260.pdf

96）脚注 88「ICT サイバーセキュリティ総合対策 2022」p.34 参照

97）脚注 88「ICT サイバーセキュリティ総合対策 2022」p.34 では，オンライン演習のほか，「出前講習，サテライト講習の試行」が挙げられている．

98）脚注 68「サイバーセキュリティ 2019」p.11 参照

2000年の省庁HP連続改ざんを機に開始された全政府的なセキュリティ対策の基本方針については2003年e-Japan戦略Ⅱに始まったが，当時はIT利活用に重点を置き，リスクゼロ・最小限化といった安心志向の事前対策が重要視された．他方，人材育成面では，「教育訓練」と「資格制度」という2本柱が挙げられた．

2009年戦略（第2次情報セキュリティ基本計画）では，ブロードバンドの普及に伴う利用者の裾野拡大を背景に，事故前提社会を掲げ，リスクを客観的に許容範囲内で管理することを目指し事後対策に重点が置かれた．人材育成に関しては事案対処能力や設計・開発側の視点が入ることとなった．

2013年戦略（サイバーセキュリティ戦略）は，スマートフォンの普及，IoT等に伴う更なる裾野拡大の潮流と，安全保障・危機管理の観点からの対応の必要性が生じたことを背景に，情報セキュリティからサイバーセキュリティに対象を拡大し，能動的な取組を含む次元を変えた対策が必要とされた．人材育成面でも教育訓練の量的な拡充に加え，突出人材の必要性やセキュリティ人材のニーズの多様化が謳われ，後の施策の原点となった．

2015年の年金機構情報流出事案は実践的な人材の必要性の認識を深く浸透させることとなり，これを反映した2015年CS戦略を踏まえ，2017年度からNICTによる実践的な人材育成事業が本格化し，2020年度以降は新型コロナの影響を受けながらも着実に実施されてきており，その裾野を広げるために実施したオンラインの活用については様々な課題も見えてきている状況である．

昨今，昨年5月の米最大の石油パイプライン停止[99]や同年10月徳島県つるぎ町の病院機能が麻痺する事態[100]などサイバー攻撃により実際に重要インフラサービスに障害が生じる事例が出ている．

また，前述したロシアによるウクライナ侵略に関連して本年9月にはサイバー攻撃集団「キルネット」による「DDoS[101]攻撃」と呼ばれるサイバー攻撃が報じられ[102]，e-Govや地方税共同機構が運営するeLTAXに障害生じる[103]など，国家の関与が疑われるものを含む攻撃によるサービス障害も顕在化している[104]．こうした中，これまでも触れてきたとおり，ヒトとモノ両面の脆弱性の完全除去は困難でサイバー攻撃を完全に避けることは難しいため，攻撃後を想定してチームで的確に対処する能力養成の重要性は増すばかりであり，グループワークのあるリアルな演習の繰り返しが求められると考えられる．

この点，筆者は，サイバー攻撃への対処そのものではないが新型コロナ等の危機管理対応を経験した際，チームにおける立場により視野が異なることを理解したうえで，各々の役割を意識しながら適時に情報共有及び意思決定していくプロセスの困難さを実感したところである．こうした感覚を机上の学習だけで養うことは難しいと考えられ，情報システム担当者などはグループワークのあるリアルな演習を受講することが望ましい．他方，遠方の演習会場に実際に参集することが難しい場合も多く，オンライン活用のニーズは高いが，前述のとおり，現行のオンラインツールにおいて制約された視覚と聴覚の下でのグループワークは，メンバーのスキルや信頼関係による面はあるもののどうしてもリアルな演習に質的に劣ってしまい十分なものにならないという現状があり，今後の

99） 脚注71「サイバーセキュリティ2022」，p.6（脚注5），p.19

100） 時事メディカル 医療ニュース トピックス 特集 病院機能を麻痺させないために～サイバー攻撃の経験から～ （2022/09/19 05:00）https://medical.jiji.com/topics/2741

101） Distributed Denial of Serviceの略．分散型サービス不能攻撃

102） 2022年9月7日6時37分NHKニュース https://www3.nhk.or.jp/news/html/20220907/k10013806691000.html

103） 寺田総務大臣閣議後記者会見の概要（令和4年9月9日）参照 https://www.soumu.go.jp/menu_news/kaiken/01koho01_02001168.html

104） サイカル journal by NHK（2022.07.27）https://www3.nhk.or.jp/news/special/sci_cul/2022/07/special/cyber-ukraine-0728/，脚注71「サイバーセキュリティ2022」，p.4参照

課題として残る．一般的に人はすぐに忘れ，飽き，楽をしようとしがちであり，こうした視点を踏まえ，主体的に関わって実感を持てるような演習方法に関して引き続き試行錯誤が求められると考えられる．

今後，2018 年 CS 戦略で記載された AI の進展や 2021 年 CS 戦略で示された「サイバー空間の公共空間化」など，サイバー空間の社会への浸透がさらに進み，安全保障環境の悪化に伴う脅威はますます深刻化することも想定される．また，メタバースなどサイバー空間が拡張する潮流も顕在化してきている．これらに対する国際的な潮流も踏まえつつ，我が国が目指すサイバー空間[105]とそれが持続的に発展する「生態系」を創出していくため，社会インフラとなる機関における地道な演習・訓練の実施，好循環をもたらす資格制度の運用，若手人材の発掘・育成を粘り強く続けるとともに，守るべきサイバー空間の変化に伴うニーズに応じた事業の多様化や新たな技術の活用等も模索していくことが求められると考えられる．

＜参考文献一覧＞

園田寿，野村隆昌，山川健「ハッカー vs. 不正アクセス禁止法」日本評論社，2000.6.
NTT データ技術開発本部システム科学研究所「サイバーセキュリティの法と政策」NTT 出版，2004.3.
不正アクセス対策法制研究会「逐条不正アクセス行為の禁止等に関する法律補訂第 2 版」立花書房，2008.10.
土屋大洋「サイバーセキュリティと国際政治」千倉書房，2015.4.
関啓一郎「サイバーセキュリティ基本法の成立とその影響」知的資産創造 /2015 年 4 月号
谷脇康彦「サイバーセキュリティ」岩波書店，2018.10
瀬戸洋一「情報セキュリティ概論」日本工業出版，2019.3.
長谷川長一「実践的サイバーセキュリティ人材の育成」日本セキュリティ・マネジメント学会誌 33 (1)，37-42，2019-05-31
塩原俊彦「サイバー空間における覇権争奪」社会評論社，2019.8.
塩崎彰久［ほか］サイバーセキュリティ法務研究会「サイバーセキュリティ法務」商事法務，2021.2.
羽室英太郎「サイバーセキュリティ入門第 2 版」慶應義塾大学出版会，2022.5.
岡嶋裕史「絵でわかるサイバーセキュリティ」講談社，2020.6
三角育生「我が国のサイバーセキュリティ戦略策定の背景」日本セキュリティ・マネジメント学会誌 34 (3)，39-46，2021
松村昌廣「我が国のサイバーセキュリティ戦略の欠点と展望」総務省 学術雑誌『情報通信政策研究』第 5 巻第 2 号，2021
※なお，脚注にある URL は 2022 年 9 月 23 日参照時点で全て有効であった．

105）自由，公正かつ安全なサイバー空間（free, fair and secure cyber space）