CITP 認定情報技術者
Certified IT Professional

CITP コミュニティ
アニュアルレポート 2017

超スマート社会を牽引する実践的IT人材が創る社会価値

平成 30 年 3 月

一般社団法人 情報処理学会
CITP フォーラム

一般社団法人 日本情報システム・ユーザー協会
アドバンスド研究会

特別寄稿

CITP 制度の IFIP IP3 認定について

旭　寛治（一般社団法人 情報処理学会）

このほど、CITP*1 制度が国際認定を取得した。これによって、CITP はグローバルに通用する資格となった。本稿では、情報処理学会で同認定の取得に携わった者の立場から、認定の意義や取得の経緯等について述べる。

■ CITP 制度創設の経緯

情報処理学会が情報技術者の資格制度創設の検討を始めたのは 10 年ほど前のことである。WG が設けられ、筆者が主査を仰せつかった。情報技術の世界では「プロフェッション」が確立していない、つまり、IT の仕事というのは専門技術者でなくても誰でもできることになっている。とりわけ日本の情報産業は、過度のアウトソーシングによって労働集約型産業となり、技術者の専門性が生かされる環境となっていない[1]。社会インフラを支える情報産業がそのような状態にあることは看過できないというのが筆者の問題意識であった。

検討の結果、「プロフェッション」を確立するために資格制度を導入することにした。これが CITP である。制度設計に当たっては、IPA と協議の上、国内標準である ITSS に準拠した資格とすると同時に、グローバルに通用する資格とするため国際標準と整合を取ることなどを基本方針とした。[2] [3] [4]

ちょうどその頃、IFIP*2 で情報技術者の国際相互認証を推進するプロジェクト IP3*3 が立ち上がった。IFIP は約 50 ヵ国が加盟する情報処理の国際連合であるが、情報処理学会は IFIP と密接な関係がある。1960 年にユネスコの提案によって IFIP が設立された時、日本の代表組織として誕生したのが情報処理学会なのである。その IFIP が IP3 を立ち上げたことを知り、CITP 制度は早期に IP3 の認定を取得することを目標に掲げた。IP3 設立の目的は、グローバルな IT プロフェッションの確立であり、筆者らの意図と一致した。情報処理学会は 2009 年に IP3 に参加し、翌年からはボードメンバーとして活動してきた。

■ IP3 の要件

IP3 のフレームワークは、各国の資格制度に一定の要件を課すことにより国際的な同等性を確保し、認定国間での相互認証を実現するというもので、IFIP が各国のメンバー学会を資格認証機関として認定する。情報処理学会はこの認定を目指した。

IP3 の資格水準には IP3P（Professional）と IP3T（Technologist）の二つのレベルがある。上位の IP3P は SFIA*4 のレベル 5 以上の能力が要求されるが、これは ITSS のレベル 4 以上に相当する。CITP は IP3P の要件を満たすようにした。

IP3 の制度は、情報技術者資格の国際標準である ISO/IEC 17024（適合性評価：要員の認証を実施する機関に対する一般的要求事項）および同 24773（ソフトウェア技術者認証）に基づいている。これらの国際標準の主要な要件の一つに、更新制がある。資格には有効期間を設定し、期間終了後も資格を継続するためには更新審査を受けなければならない。また、更新には所定の CPD*5 が必要である。CITP は有効期間を 3 年とし、更新には 150 ポイント以上の CPD を要件とした。国際標準という点では、倫理綱領や行動規範の順守も非常に重視される。CITP 制度の設計に当たっては、当初からこれらの要件を組み入れたものとした。

---

*1) Certified IT Professional、認定情報技術者

*2) International Federation for Information Processing、情報処理国際連合

*3) International Professional Practice Partnership

*4) Skills Framework for the Information Age、英国の IT スキル標準

*5) Continuing Professional Development、継続研鑽

■ IP3 認定の取得

CITP 制度は 2014 年に本運用を開始し、昨年 3 月に最初の資格更新を実施した。IP3 の認定を取得するためには一定の運用実績のあることが条件となるので、3 年あまりの実績を踏まえて昨年 7 月に IP3 に認定の申請書を提出した。

これに先立ち 2016 年 4 月、情報処理学会に WG を設置し、申請書類を作成する作業を開始した。申請書類の本体は、IP3 が提示するガイドラインにしたがって、認定の要件となっている項目ごとに CITP 制度の実施内容を記述する。制度の詳細を記述するのでかなりの量となるが、本体よりも問題となるのは、CITP 制度に関連する各種規程や様式等の attachments（添付書類）である。これらの原本は、当然ながらすべて日本語で書かれている。申請書の attachments とするためには、英訳が必須である。これは大量のため、翻訳業者に委託することした。委託に当たっては、用語の対訳集を作成し、英訳結果は WG の委員が分担してレビューした。CITP 制度のベースとなっている ITSS については、すでに IPA が海外展開のために英語版を作成済みであったので、それを借用できたのが幸いであった。

申請書の提出から約半年にわたって書類審査が行われ、その間に何件かの Q&A が行われた後、本年 2 月に審査チームによる site visit（現地視察）が実施された。アメリカ、オーストラリア、南アフリカから計 3 名の審査員が来日し、東京御茶ノ水の情報処理学会で 3 日間にわたって審査が行われた。審査に際しては、プロの通訳を同席させた。大きなカンファレンス等を除いて通常の学会の会議では通訳を置くことはないが、今回は学会関係者外の人々も参加することから、通訳の同席が効率的と判断された。

審査結果は直ちに IP3 の理事会に提出され、審議の結果、CITP 制度は認定された。IP3 から送られてきた認定書を図 1 に示す。

■ CITP コミュニティの貢献

CITP 制度創設の目的が「情報技術者のプロフェッションの確立」にあったことは上に述べたが、筆者らの真の狙いは、CITP の有資格者によるプロフェッショナルコミュニティの形成であった。コミュニティが情報産業の発展に貢献し、その結果、現在は決して高いとは言えない情報技術者の社会的地位が向上することを期待した。幸い、2014 年 11 月に CITP コミュニティの第 1 回会合が開かれ、その後コミュニティ活動が徐々に広がりつつあるのは、筆者らにとって真に喜ばしいことである。

このコミュニティの存在が IP3 の認定審査にも大きな役割を果たした。審査チームによる site visit では、主として筆者ら CITP 制度の運営関係者が対応したのはもちろんであるが、同時に CITP 制度のステークホルダーに対するインタビューが重要な審査項目であった。CITP 制度を利用して資格を取得された方々が、この制度を appreciate しているのか、つまり、この制度の意義を認めているのかという点が、審査の合否を決定する上で大きな要素であった。CITP コミュニティで熱心に活動されている方々の中から何人かにインタビューを受けていただいたが、CITP 資格取得の目的や活用状況などを適切に述べていただき、審査員から高評価を得ることができた。

CITP 制度には、企業の社内資格制度を認定するという仕組みがあるが、その認定企業の関係者の方にもインタビューを受けていただいた。こちらも会社としての認定のメリットを具体的に述べていただき、同じく高評価を得た。

■ IP3 認定の意義

IP3 による認定を取得した意義は大きい。これまでは、情報処理学会という日本の一組織の定める資格に過ぎなかった CITP が、グローバルに通用する資格となり、その価値が向上した。今回の認定により、学会の Web サイトには早速 IP3P のロゴマークが表示された。CITP 制度で認定された企業にとっても、社内資格制度が国際的に認められた CITP 制度に基づく制度となることの意義は大きい。

一方、IP3 としても、日本が認定国の仲間入りをしたことは意義がある。これまで IP3 の認定を取得したのはすべて英語圏の国だった。IP3 Chair の Moira de Roche 氏は、CITP 制度の認定によって“The IP3 program has become truly global.”と述べている。[5]

CITP 認定情報技術者
Certified IT Professional

ACCREDITED IP3P

■ 今後の展望

上述のように、IP3 の認定を取得することは、CITP 制度創設を検討した当初からの目標であった。目標達成によって、CITP 制度は次のフェーズに入ったということができる。IP3 認定を機会に、CITP 制度の認知度の向上と一層の普及に弾みをつけたい。その一環として、まず日経 BP 社の取材を受け、IP3 認定に関する記事が同社の Web サイト「日経 xTECH」に掲載された。3 月に開催された情報処理学会の全国大会では、CITP セッションでの発表とともに参加者全員に CITP のリーフレットを配布した。広報活動の継続によって、CITP 有資格者および認定企業の増大を図る予定である。[6]


IP3 International Professional Practice Partnership
Partnering for Trust in Digital

The International Professional Practice Partnership certifies that the

Information Professionals Society of Japan (IPSJ)

Certified Information Technology Professional (CITP) Scheme

CITP 認定情報技術者
Certified IT Professional

has been examined and is accredited as meeting the standards set down by the International Federation for Information Processing IP3

Dated this 26th day of February 2018

Adrian Schofield FIITPSA
Chief Assessor
Chairman Standards and Accreditation Council

Moira de Roche FIITPSA
Chair IP3 Board

Valid for period 26 February 2018 to 25 February 2023

ifip

図 1　IFIP IP3 認定書

＜参考文献＞

[1]松田信之「CITP 制度を活用した高度 IT 人材の育成～超スマート社会を支える実践的技術者育成～」平成 28 年度 CITP フォーラム/JUAS アドバンスド研究会 活動報告書(2017)
[2]旭寛治「認定情報技術者制度(1)－制度の概要－」『情報処理』第 55 巻第 8 号(2014)
[3]IT エンジニアの新しい認定制度が始動､大手 6 社が主導するプロの免許､日経 SYSTEMS 2014.5
[4]IT 技術者を「社会から尊敬される職業に」､情報処理学会が“高度”新資格を開始､日経
コンピュータ (2014.9.4)
[5]IFIP IP3 Accredits First Non-English ICT Certification、IFIP News(2018.3.15)
https://www.ifipnews.org/media-release-ifip-ip3-accredits-first-non-english-ict-
certification/
[6]「日本発 IT 資格が国際資格に、高まる期待と 2 つの課題」日経 xTECH(2018.3.9)
http://tech.nikkeibp.co.jp/atcl/nxt/column/18/00001/00138/?P=1

旭　寛治
（株式会社日立製作所／情報処理学会 資格制度運営委員会 前委員長）
【略歴】(株) 日立製作所基本ソフトウェア本部長、ストレージ
ソリューション本部長、(株) 日立テクニカルコミュニケーションズ
代表取締役社長等を歴任。1999 年本会理事、2005 年副会長。
IT プロフェッショナル委員長。情報処理学会名誉会員。

目次

CITP フォーラムの活動

～社会に求められる高度IT人材像と CITP の活動の方向性～

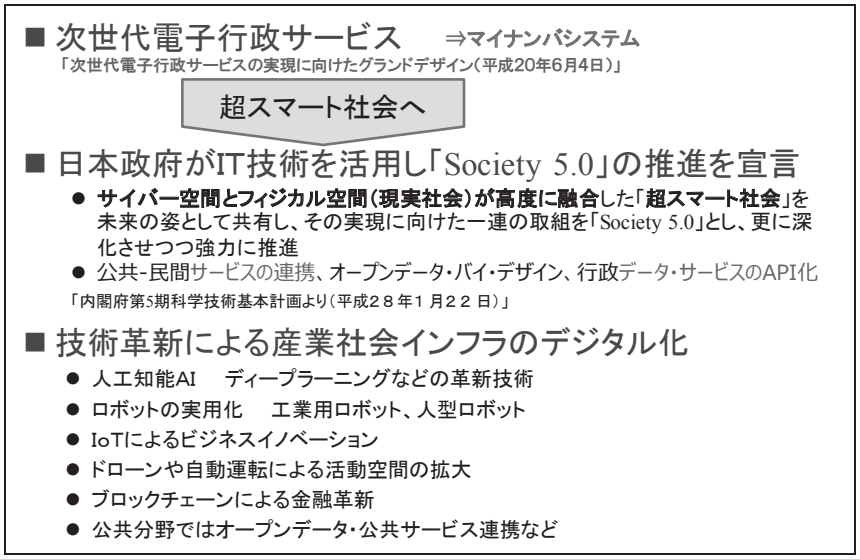
平林　元明
情報処理学会 CITP フォーラム 代表

超スマート社会を実現するという国家的取組が始まっている。超スマート社会を実現するためには、それを担う実践的 IT 人材が必要となる。情報処理学会の認定情報技術者（CITP：Certified IT Professional）制度によって認証された実践的 IT 人材とはどのような人材なのか。本論では、社会に求められるその人材像を俯瞰するとともに、CITP のコミュニティである CITP フォーラムの活動内容を紹介する。CITP フォーラムでは、5 つの専門部会（SIG）と 3 つの委員会を設置し、社会貢献活動、人材育成活動、社会提言などを行っている。これらの活動を実践し、運営してきた経緯や課題対応についても述べる。

Ⅰ　社会に求められる人材像

1．IT 人材が求められる社会

今から 10 年前、次世代電子行政サービスという構想[1]があった。これは政府のシステムを横連携していくというものであるが、今のマイナンバーシステム[2]に繋がっている。完成したのは昨年であるが、構想から 9 年掛っている。そして今度は Society 5.0[3]が進められている。超スマート社会を実現するという構想で、官民のサービスの連携をしていくものである。このためデータ公開やサービスの API 化などもしていく予定となっている。このような IT 化は世界全体としての流れであり、社会インフラのデジタル化が進み、AI やロボット、IoT といった技術を使いこなす人材がますます必要になってきているのが現状である。



2．IoT・AI 技術を活用したフォーメーション

今まではユーザ企業が発注したシステムを IT 企業が作るというのが日本では一般的であったが、IPA(独立行政法人 情報処理推進機構)の人材白書[4]には、ユーザ企業と IT 企業が協働してサービスを創る時代に変わってくると謳われている。IT 人材も単に IT の専門家としてだけでなく、エンドユーザに対するサービスの価値を意識したシステム開発をしないといけない時代になってきている。

●受発注の関係から協働・協創の関係へ

●システムを作るからサービスを創る時代へ

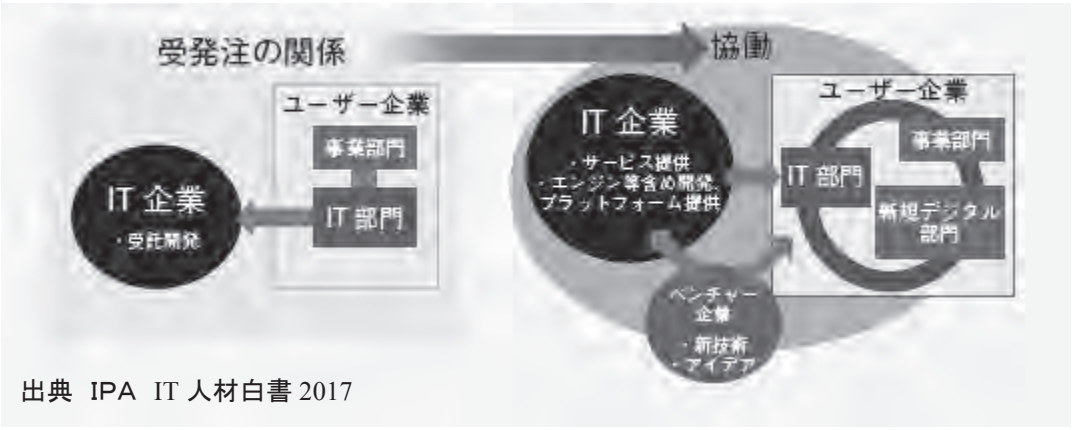


図 1 デジタル化によるユーザ企業と IT 企業の関係性の変化

3．IoT やビッグデータ・AI に携わる人材の育成・獲得・確保方法

IoT やビッグデータ・AI に携わる人材をどのように確保するかというアンケート調査結果がある。1 番目は社内の人材を再教育するというもの、2 番目は外部人材の中途採用となっている。つまり AI で仕事がなくなると言われているが、変化に対応できる人材や専門分野を持つ人材が生き残っていくということを物語っている。

1 位　社内の人材を再教育
2 位　外部人材の中途採用
3 位　新卒の育成や他社の活用

⇒

求められる人材
・変化に対応する人材
・専門分野を持つ人材

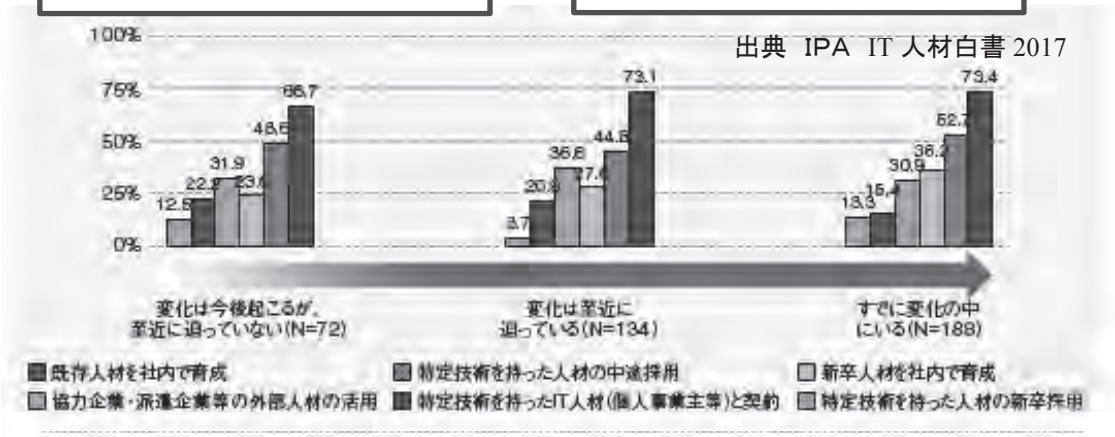
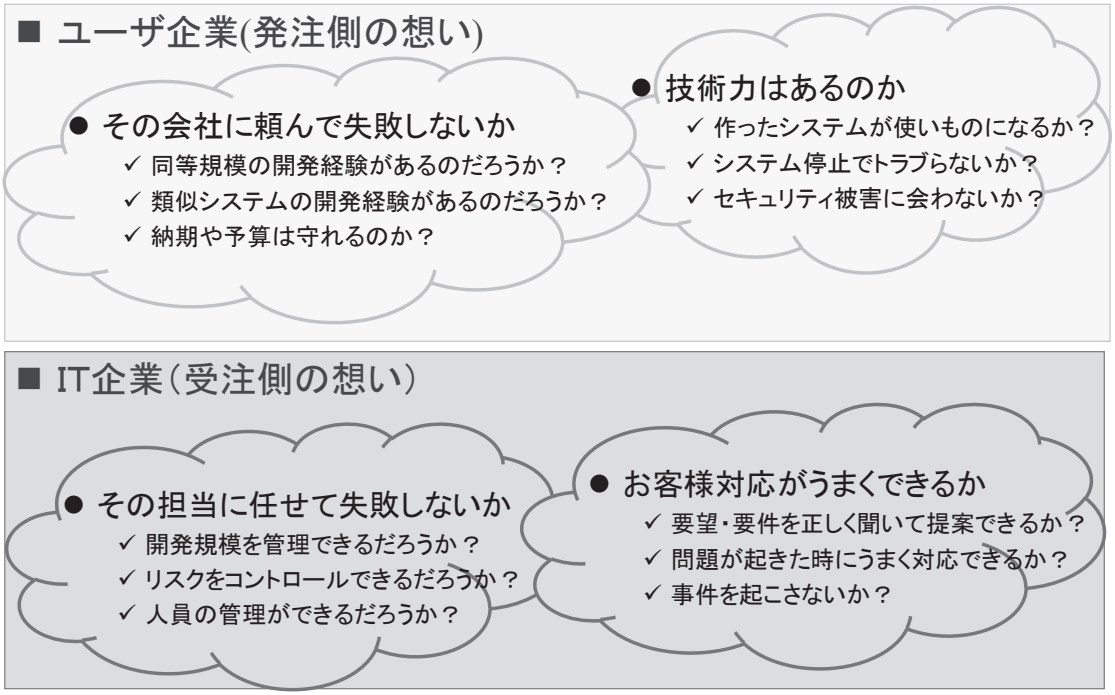


図 2 IT 企業の IoT やビッグデータ、AI 等に携わる人材の育成、獲得、確保

４．人財に対する期待

日本では欧米に比べ IT 技術者が IT 企業に集中し、ユーザ企業に少ない傾向がある。ユーザ企業と IT 企業は受発注の関係にあるわけであるが、双方の期待は人材の経験と企業の信頼にある。つまり実行力があるかどうかが採用のポイントになる。



５．求められる行動特性

高度 IT 人材に求められる行動特性をまとめると「**５つの力と３つの価値**」に整理することができる。これらの行動特性はシステムに求められる要件を正しく理解し、チームの総力を結集し、必要なタイミングでシステムをリリースするために必要なものである。

① 実行力　実績を残す実行力
② 判断力　完遂に導く使命感と判断力
③ 予測力　課題やリスクに対応する予測力
④ 適用力　スキルを生かす適用力
⑤ 管理力　部下を育成・指導する管理力
⑥ 自分の価値　を認識したプロジェクトへの貢献と責任感
⑦ 顧客の価値　を認識した顧客対応力
⑧ 社会の価値　を認識したプロフェッショナルとしての自覚
⑨ コミュニケーション力　理解する・伝わる・意欲がある
⑩ 職業倫理 信頼できる

６．IT 技術者の方向性

社会の将来の方向性、将来の新しい技術を担う人材、企業で求められる人材や行動特性など、高度 IT 技術者の向かうべき方向性をまとめると以下のようになるであろう。

- **■ 高度な技術を使いこなせる人材に**
  - **● IT を作るから IT を使いこなす　⇒IT は体の一部**
  - **● IT そのものの知識は当然　⇒IT による価値創造へ**
  - **● より上位のレベルを目指す　⇒高度 IT 人材**
- **■ これから社会で求められる人材**
  - **● IT 技術力（実行力のある人）　⇒CITP**
  - **● IT を活用した新しい技術　⇒人工知能など**
  - **● 社会的価値の創造　⇒ビジネスモデル**

CITP とは「実行力のある高度 IT 人材」を認証された人材である。この技術力を生かし、新しい技術を活用して、社会が必要とする価値を創造することによって、その力を発揮することができるであろう。

技術力×活用力×創造力

II　CITP フォーラム 活動状況

この章では、CITP フォーラムの活動状況を紹介する。

1．CITP フォーラム 活動状況

CITP フォーラムの活動拠点および活動実績は次のようになる。

- 2014 年末活動開始

  2018 年 3 月までに定例会　20 回　(2 ヶ月に 1 回)
- 活動拠点

  東京・神奈川地区、名古屋地区、大阪地区
- 合宿

  湯河原(2016 年)、石巻シビックテック(2017 年)
- 分科会

  定例会の他、専門部会や個別チーム会合多数
- 情報発信・共有・コミュニケーション
  ホームページ、メーリングリスト、掲示板、FIT、全国大会、ワークショップ、
  アニュアルレポートを発行（2016 年度は約 70 ページ）、外部委員会参加、
  社会提言、政府パブコメ、政府 CIO 補佐官との意見交換　等

2．CITP コミュニティの構成

CITP フォーラムは情報処理学会の IT フォーラムのひとつであるが、CITP 自身による自主運営組織として CITP コミュニティを運営している。[5][6]

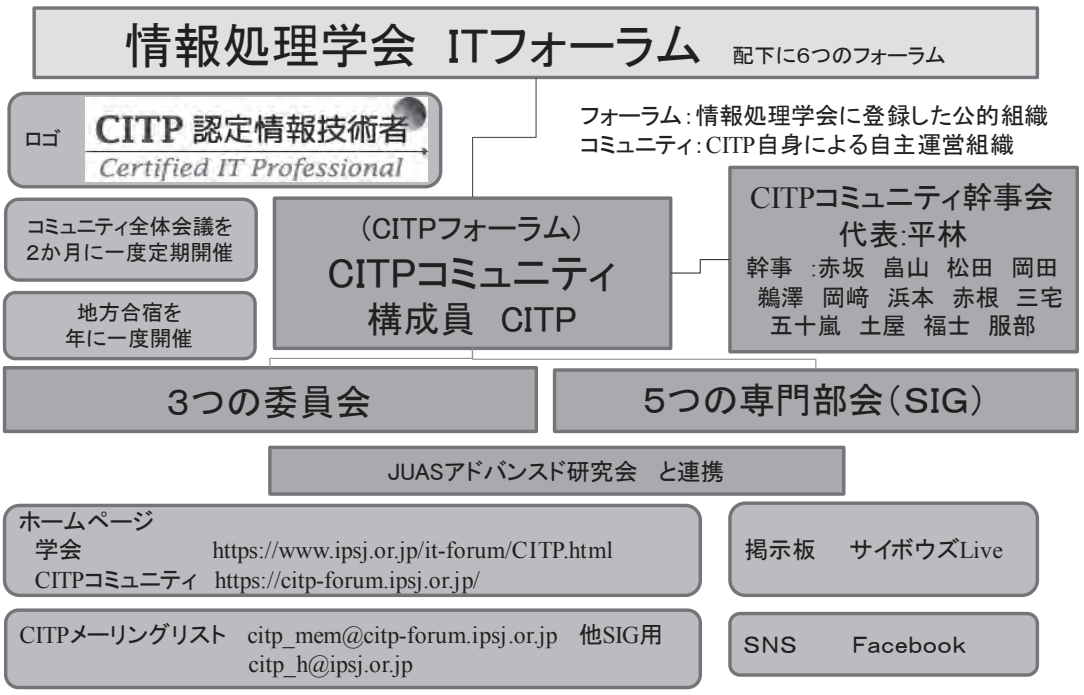


図 3 CITP コミュニティの構成

３．CITP コミュニティの構成

（１）CITP コミュニティの全体フレーム

CITP コミュニティはコミュニティの運営を行う幹事会、技術者の交流を行う定例会、有志による特別活動を行う専門部会から構成される。

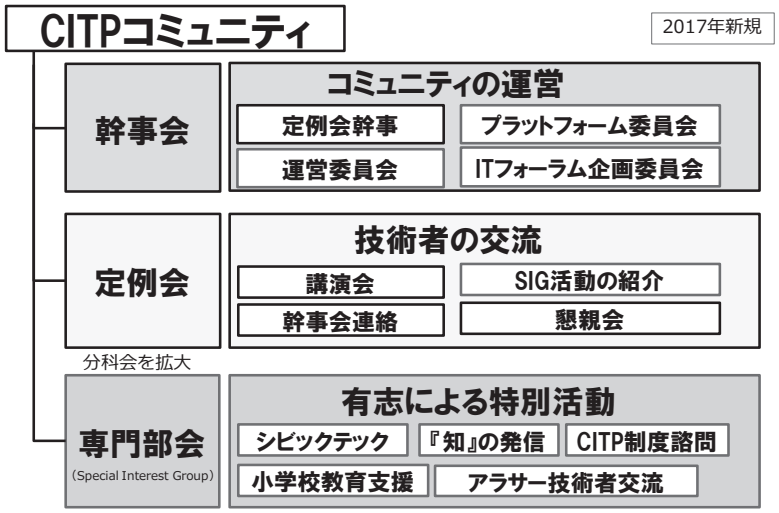


図 4 CITP コミュニティの全体フレーム

（２）幹事会　-コミュニティの運営-

幹事会は、意思決定を行う組織であり、委員会などから構成される。

	活動概要	委員長	メンバー（※：賛助会員）
幹事会	コミュニティの運営全般に関する意思決定	幹事会は新しい幹事を適宜募集・選任することができる	
幹事会 定例会 担当幹事	・幹事会・定例会の開催日時、議題（講演会含む）、ｽｹｼﾞｭｰﾙの決定と場所の確保 ・幹事会・定例会の司会進行	開催場所を提供できる幹事で持ち回り	
運営 委員会	CITP コミュニティの運営に関する企画・改善検討	松田 （中電シーティーアイ）	森田（NRI） 服部（NEC） 旭※（情報処理学会）
プラットフォーム 委員会	ホームページ、メーリングリスト等コミュニティの連絡および広報の IT インフラの構築・運営	岡田（NEC）	赤根 (デジタルフィールド) 森田（NRI）
IT フォーラム 企画 委員会	情報処理学会 IT フォーラム（ソフトウェアジャパン、全国大会等）に関する企画・運営	平林（日立）	三宅 （NEC ソリューションイノベータ） 福士（LAC） 松田(中電 CTI) 林※（情報処理学会） 旭※（情報処理学会）

（３）コミュニティ会議(定例会)　-技術者の交流-

コミュニティ会議(定例会)は CITP 全員を対象とした集まりで、定例議題などの他に講演会や専門部会の報告などを開催している。

	活動概要	委員長	メンバー (※：賛助会員)
講演会	CITP や産・学・官の有識者/キーマンによる講演会	開催場所を提供できる幹事で持ち回り	
幹事会連絡	幹事会で議論・決定した内容を必要に応じて説明	開催場所を提供できる幹事で持ち回り	
SIG 活動の紹介	専門部会の活動状況の報告(必要に応じて)	SIG 部会長	SIG メンバー
懇親会	コミュニティメンバー、賛助会員、ゲスト等による懇親会	開催場所を提供できる幹事で持ち回り	

（４）専門部会（SIG）　-有志による特別活動-

有志による特別活動で、CITP なら誰でも参加でき、自分の関心のあるテーマで新しい部会の設立も提案できる。また、部会長が認めれば CITP 以外も参加できる。

	活動概要	部会長	メンバー　(※：賛助会員)
シビックテック	IT を活用し、被災地をはじめとする地域社会の課題解決に取り組む	赤坂（日本 IBM)	土屋（ハイマックス） 鵜澤（日立） 三宅(NEC ソリューションイノベータ) 福士（LAC）他
小学校教育支援	小学校のプログラミング教育における CITP の活用を検討	五十嵐（NRI)、 （赤根 部会長代理)	赤根 (デジタルフィールド) 松田、青木、宮下 (中電シーティーアイ)他
『知』の発信	CITP が持つノウハウや活動成果を『知』としてまとめ、エッセイや論文などで公開・発信する	松田 (中電シーティーアイ)	岡崎 (住友電工情報システム) 赤根 (デジタルフィールド) 井川（NEC)、 久保、宮下、豊田 (中電シーティーアイ)他
アラサー技術者交流	若手（30～40 代）CITP 同士の交流	服部（NEC)	森田（NRI) 鵜澤（日立）他
CITP 制度諮問	CITP 制度に関する改善点・要望やレベル５認証等に関して情報処理学会に諮問する	平林（日立)	林※（情報処理学会） 旭※（情報処理学会）

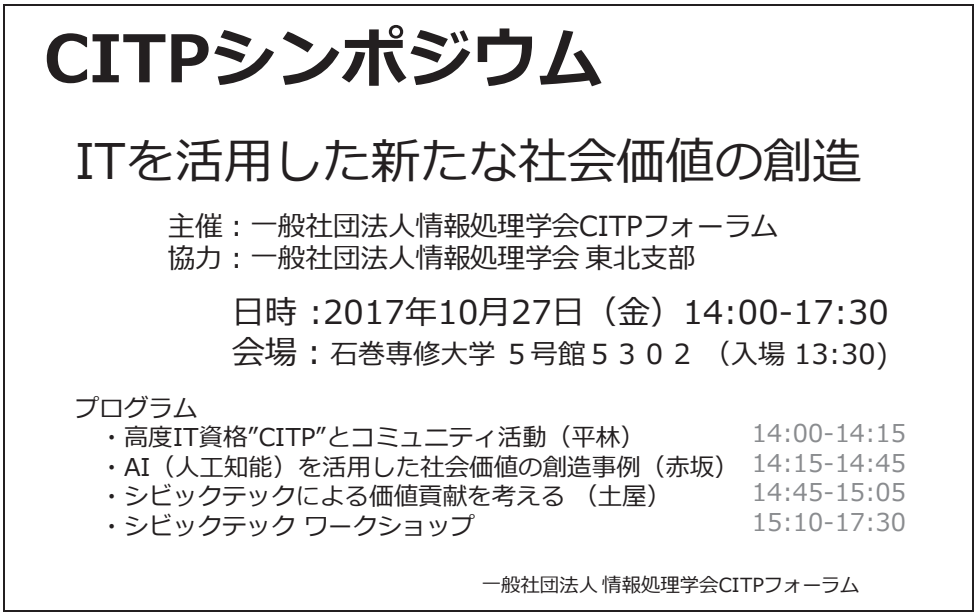
４．専門部会の紹介

（１）シビックテック専門部会

IT を活用し、被災地をはじめとする地域社会の課題解決に取り組む部会。

コーディネータ：　日本 IBM　赤坂　亮　／　ハイマックス　土屋 俊樹

2017 年度は下記シンポジウムを開催した。



（２）「知の発信」専門部会

CITP が持つノウハウや活動成果を『知』としてまとめ、エッセイや論文などで公開・発信する部会である。

① 定例会での発表や企業間コミュニティの交流

- 第 19 回 CITP コミュニティ inNAGOYA（H29.12.6 定例会）では日立製作所 HPM プロフェッショナルコミュニティと中電シーティーアイ CITP コミュニティの活動を紹介
- **活動成果の発表**
  - 夏休みの宿題でプログラミングをやらせてみた

    株式会社中電シーティーアイ　宮下修
  - 中国のインターネット事情

    株式会社中電シーティーアイ　久保壮一郎
  - 合格者が作る「認定情報技術者(個人認証)申請の手引き」

    住友電工情報システム株式会社　岡﨑四郎

② アニュアルレポートの発行

- 2016 年のコミュニティ分科会（IT 人材育成分科会、社会価値創造分科会）の活動成果を論文集「超スマート社会をリードする実践的ＩＴ人材の育成と潜在的社会価値を持つサービスの創出」にまとめ発行した。

■ アニュアルレポート　全 71 ページ

【IT 人材育成分科会/JUAS 実践的IT人材の評価・育成研究会】

①CITP 制度を活用した高度 IT 人材の育成

～超スマート社会を支える実践的技術者育成～

中電シーティーアイ　松田信之

②ソフトバンク（IT 統括）の人財育成について

ソフトバンク　鈴木忠之

③人工知能時代の IT 人材育成

デジタルフィールド　赤根大吾

④小学校段階におけるプログラミング教育と CITP との連携

株式会社野村総合研究所　五十嵐智生

⑤人財能力を実務ベースで可視化する

住友電工情報ｼｽﾃﾑ株式会社　岡崎四郎

【社会価値創造分科会/JUAS 潜在的ニーズを持つサービスの社会価値創出の研究会】

⑥CITP による社会価値創造の取組み

日本 IBM（株）　赤坂亮

⑦日本を元気にする攻めの IT

-組み合わせ型のビジネス課題解決-

中電シーティーアイ　荒木岳文

⑧映画鑑賞における視覚障碍者の QoL（Qualityof Life）

日本電気株式会社　岡田克彦

⑨初中級プロマネのための現場で活かせ！統計情報

ハイマックス　土屋俊樹

■ 合格者が作る「認定情報技術者(個人認証)申請の手引き」 全 23 ページ

第 1 章　IT 技術者のスキル・能力を
　　どのように可視化するの？

第2章　申請書の書き方のポイントは？

　　提出書類の概要と作成順

　　業務経歴書

　　認定情報技術者申請書

　　主要業務・研修・プロフェッショナル貢献の記録

　　達成度指標チェックシート

　　スキル熟達度チェックシート

第3章　合格者からのアドバイス

（３）小学校教育支援専門部会

小学校のプログラミング教育における CITP の活用を検討する専門部会である。パブリックコメントを発信した。

ALT(外国語指導助手)制度を参考に民間の現役 SE や退職者 SE などをプログラミング教育助手（TA）として全国の小学校に派遣することを提案

「学校教育法施行規則の一部を改正する省令案並びに幼稚園教育要領案、小学校学習指導要領案及び中学校学習指導要領案」に関する意見

文部科学省初等中等教育局教育課程課 御中　2017 年 3 月 15 日　一般社団法人　情報処理学会

意見：

情報処理学会では、IT スキル標準レベル 4 以上の上級技術者を対象に IT スキル標準で定められたスキル評価方法に基づき、所定のレベルに相当する能力を有すると判定された技術者を「認定情報技術者（CITP)」として認証する制度を実施しています。現在 6,000 名を超える技術者が CITP に認定されています。この度、プログラミング教育が義務化されることが小学校学習指導要領案で明示されたことは、情報リテラシーの裾野を広げるという意味で大変評価しています。情報教育を伴う今次改定に、CITP が有志を募り、民間人として小学生のプログラミング教育に貢献ができないか、ワーキンググループを作り具体策を検討しています。

小学校学習指導要領案を拝見しましたが、算数と理科に関しては、具体的な一方で、算数と理科以外の科目に関しては、「指導に当たっては、コンピュータや情報通信ネットワークを積極的に活用して、情報の収集・整理や、実践結果の発表などを行うことができるように工夫すること」としか記載がなく、今次改定で示されているプログラミング的思考の教育を、小学校現場の創意工夫だけで進めることは無理がある印象を受けました。また、小学校教諭は担当する教科が幅広いことに加え、英語の教科化に伴う負担増などを考慮すると、教科化されていないプログラミング教育を同時に進めなければならない教諭の負担が大きすぎると認識しています。

CITP 有志は、検討を進める中で、外国語指導助手（ALT）制度のプログラミング教育版を整備することができないかと考えています。ALT 制度を参考に自治体国際化協会に準じたプログラミング教育の受け皿を設けることで、民間の現役 SE や退職者 SE などを訓練し、プログラミング教育助手（TA）として全国の小学校に派遣できないかを考えています。今回の答申では、プログラミング教育の実現化のために、国、教育委員会、小学校現場、関係団体、民間や学術機関が連携すると記載されています。私たちは、民間や学術機関の一員として、今次改定の実現を望んでいます。小学生のプログラミング教育の円滑な実現のためにも、是非、具体的な推進に向けて、民間などの関係団体との連携もご検討下さい。

（４）アラサー技術者交流専門部会

若手（30～40 代）CITP 同士の交流をする専門部会である。

- CITP メンバーが提供する、この活動だけの特別講演の開催
- SIG メンバー同士の自発的なビジネスアイディア検討会
- 講演／セミナー後の技術座談会開催＋懇親会

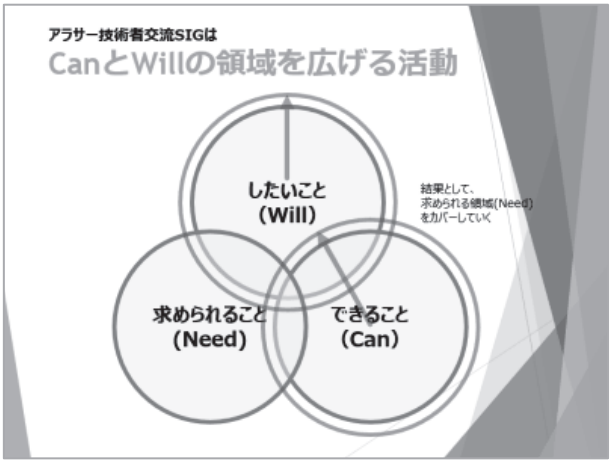


図 5 アラサー技術者交流専門部会の活動イメージ

（５）CITP 制度諮問専門部会

CITP 制度に関する改善点・要望やレベル５認証等に関して情報処理学会に諮問する。

■活動その１　CPD[7]登録の正しい書き方検討プロジェクト

- CITP の実際の活動例を収集した

  ⇒内容を精査し、分析した

- 正しい書き方を CITP 定例会議にフィードバック

  ⇒CITP 制度の委員会を通して CPD 申請案内にも反映された

取得日	開催地	証明書用タイトル	活動形態 活動内容	数量 単位表記	取得 単位
2016.3.28	情報大学(情報学部)	論文誌（情報学01）第99巻（2015年）; 事例分析に基づく情報システム開発のリスク対策方法; 担当分2ページ	[2-1] 業務上の成果を発信する活動 6-論文掲載（査読付き論文）	2ページ	60.0
2016.2.4	情報処理学会(一橋大学)	ソフトウエアジャパン2016; 人工知能は世の中をどう変えるか; Robot of Everything; オープン・サービス・イノベーションで加速するKNOWLEDGE INTEGRATION; 質問応答システムWatsonとその実用化; IoTビジネスの過去・現在・未来; パネル討論「人工知能は2020年の世界をどう変えるのか？」; 誰でも使える自然言語処理技術を目指して; 受賞スピーチ2	[1] 能力を磨く活動 2-集合研修（テスト、演習等なし）	4.8時間	4.8
2014.12.10	CITP コミュニティ(CD社/東京)	第1回CITPコミュニティ; 日本や社会全体のIT技術関連の問題についてディスカッションを行った	[1] 能力を磨く活動 3-見学会、ワークショップ、コミュニティ活動への参加	2時間	2.0
2015.4.13	AB社	特開2015-069999; 情報識別システム; 貢献3割	[2-1] 業務上の成果を発信する活動 24-技術的成果(特許　発明者に限る）公開時	0.3件	3.0
2014.11.6	情報処理学会(御茶ノ水)	実務家コミュニティイベント; システムの課題と実践	[2-1] 業務上の成果を発信する活動 4-研究会発表（登壇あり）	1.5時間	15.0

図 6 CPD(Continuing Professional Development)実績登録の正しい書き方の例

CPD 実績記入上の留意点　(一部抜粋)

- ✓ 社内研修など社外秘の内容の場合、CITP の資質向上にふさわしい内容であることがわかる注記を具体的内容に記載する。講演名などの一部を伏せ字(■)にしたものでもよい。エビデンスとしては上長等の確認資料または参加したことがわかる資料を準備すること。
- ✓ メンター・後進の指導など月単位の場合、対象日には月の最初の日付を登録する。登録できる活動は、新人指導 (報告書や日誌がある)、中堅のOJT指導(指導計画がある)、師弟関係にある指導者、などで、職制上の部下やプロジェクトチームの部下、など立場上の管理者による場合は含まない。また、具体的内容には指導した各人に対する指導概要を一人一行程度で記述すること。

・　・・

■活動その 2　CPD 対象範囲の見直しプロジェクト

- CITP の実際の活動例を分析し貢献活動を整理した

  ⇒所属する企業に対する貢献や社会に対する技術的貢献の他に、業務とは直接連動しない支援活動に対する CPD 登録の定義が無いことが判明した

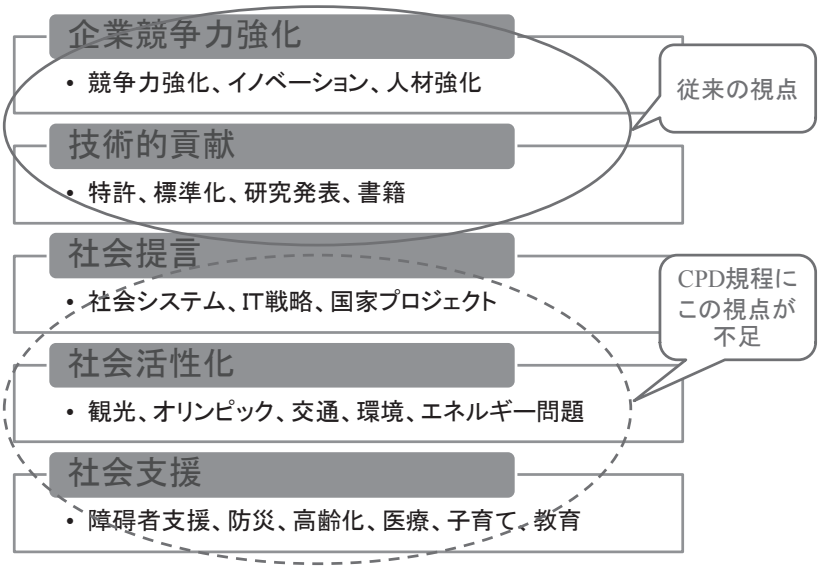


図 7 社会貢献の種類(CITP の活動スコープ)

- CPD 規程に追加すべき活動を委員会に提案

  ⇒CITP 制度の委員会を通して CPD 規程に反映された

CPD区分		実施形態・活動内容	ベース	重み	上限	注
① 能力を磨く活動	①	1-集合研修（テスト、演習等あり）	受講時間	2		A
		2-集合研修（テスト、演習等なし）		1		A, 1
		3-集合研修（見学会、ワークショップ、コミュニティ活動）	参加時間	1		
	⑧	4-自己学習(資格取得)	件	20		3
		5-自己学習(エビデンスが合格証などの場合)	履修時間	1	20/年	
		6-自己学習(エビデンスが自分でまとめた学習成果資料の場合)	ページ数	1	10/年	
②-1 業務上の成果を発信する活動	②	7-研究会発表（登壇あり）	発表時間	10		B, 1
		8-研究会発表（ポスタ）		2		B
	③	9-論文掲載（査読付き論文）	ページ	30		C, 2
		10-論文掲載（査読なし論文）		10		D, 1, 2
	④	11-著作（技術図書（原著）刊行）	ページ	10		2
		12-著作（技術図書（翻訳）刊行）		5		2
	⑤	13-研修会講師（社内；初回）	講演時間	3		
		14-研修会講師（社内；同一内容2回目以降）		2		
		15-研修会講師（メンター、後進の指導など；月単位）	人数×月	2		
	⑦	16-技術的成果(社内外での著しい技術的成果；単独/共同)	件	20		E, 2
		17-技術的成果(特許 発明者に限る；公開時)		10	20/年	2
		18-技術的成果(特許 発明者に限る；権利化時)		20		2
		19-技術的成果(組織内での技術的成果の共有；単独/共同)		10		2
		20-技術的成果(組織内の審査、査読)		5		F
②-2 社会貢献活動	⑤	21-研修会講師（社外；初回）	講演時間	3		G
		22-研修会講師（社外；同一内容2回目以降）		2		G
	⑥	23-公的団体への貢献(各種委員)	所要時間	3		H
		24-公的団体への貢献(国際、国内、業界標準の作成)		4		
		25-公的団体への貢献(裁判等での技術鑑定)		4		
		26-公的団体への貢献(JABEE審査)		3		
		27-公的団体への貢献(論文などの査読)	件数	10		
		28-公的団体への貢献(CITPの審査　個人認証)	審査件数	6		
		29-公的団体への貢献(CITPの審査　企業認定)	所要時間	3		
		30-公的団体への貢献(初中等教育における技術指導)	所要時間	2		
		31-公的活動への貢献(パブリックコメント)	件数	5		
		32-公的活動への貢献(ワークショップ、コミュニティ活動：資料提出あり)	参加時間	2		I
		33-公的活動への貢献(ワークショップ、コミュニティ活動：資料提出なし)	参加時間	1		I

業務外の自主的活動

パブコメ プロボノ等

（注）　プロボノ：プロによる社会貢献ボランティア活動

図 8 CPD 規程の改定内容

Ⅲ　今後に向けて

１．運営上の課題と対応

３年間の CITP フォーラムの活動を通して発生した運営上の課題に対して工夫した主なものを整理する。

■ **参加者をどのように増やすか**

- 企業認定制度の無い会社は認定制度を作るのは大変なので、社外の制度を利用するメリットがある　－　会社として CITP 制度を推奨して申請を社員に促す
- 専門部会を増やし興味のある部会を作る　－　一般の技術者の取り込みを図る
- 幹事を増やすことで運営負担を分散
- 専用ホームページや個別メーリングリストの設置など PR の機会を増やす

■ **定例会議の場所の問題**

- 各社持ち回りで開催し会議室を提供することで負担を分散

■ **予算の問題**

- 会議室は各社提供
- 講演者は CITP を中心とし、外部講演者は人脈を活用

■ **実務で忙しい CITP**

- 土日にやると会社会議室が使えない、旅費が自腹となるなど、孤立して会社から見えなくなるので、できるだけ会社の理解をもらう
- 幹事が忙しい時は相互バックアップ

■ **ボランティアに関心がある人が参加する傾向**

- プロボノも CPD カウント可能とし、モチベーションアップ

2．CITP フォーラムの実績評価

CITP フォーラムの設立目的に照らして３年間の活動を評価する。主なものとして、社会提言については、パブコメを発信している。教育人材育成活動については、石巻を始め教育関係機関との連携を始めている。学会以外の委員会活動や情報技術者の評価などはこれからという状況である。

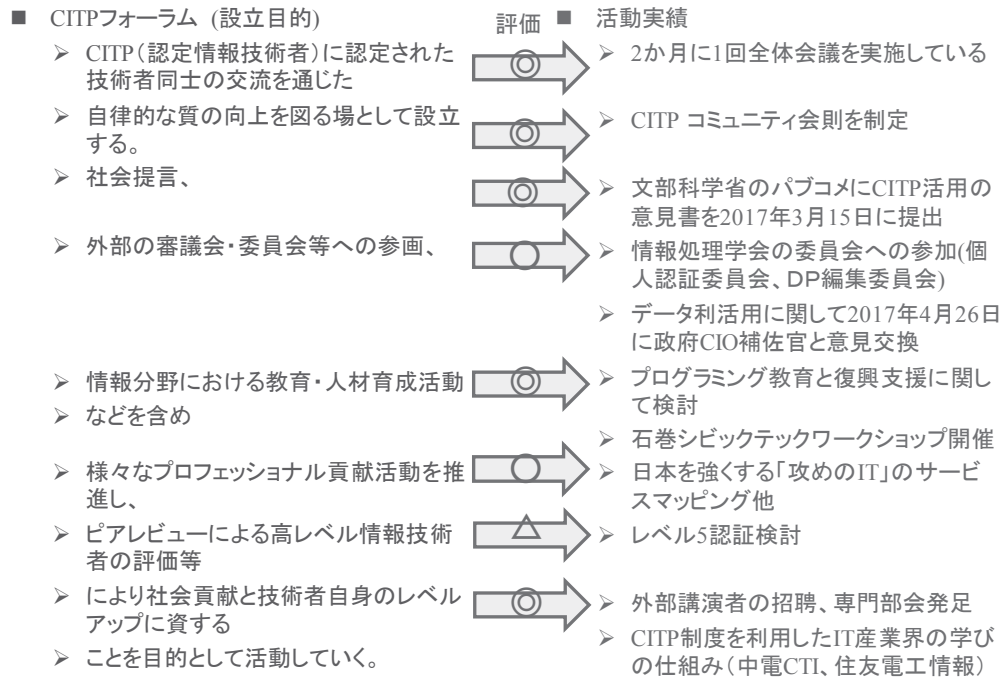


図 9 CITP フォーラムの実績評価

3．CITP 活動の方向性

本論の 1 章から 3 章までの視点・評価をまとめ、進むべき CITP 活動の今後の方向性を示す。

■ 社会に求められる人材像の視点

技術力×活用力×創造力

- CITP の専門分野を生かした勉強会
- 社会貢献活動を生かした社外の知見と理解

■ CITP フォーラム 活動状況の視点

- 認定者/参加者の増加
- 専門部会の活性化
- 一般の技術者の取り込み

■ 実績評価の視点

- 対外的な連携の推進
- より上位の技術者を目指す仕組み作り

【著者】平林　元明（ひらばやし　もとあき）
情報処理学会 CITP フォーラム 代表

（株）日立製作所で OS や運用管理ミドルウェアを開発。内閣府情報化参与 CIO 補佐官として政府情報システムの最適化を推進。CIO 補佐官連絡会議情報技術 WG リーダ、経済産業省文字情報基盤推進委員会、IPA TRM 検討 WG 主査、文字情報基盤運用検討 WG 委員長等の政府関連委員会に参画、静岡大学情報学部客員教授、JEITA IT サービス調達政策専門委員会委員長を経て、情報処理学会 CITP フォーラム代表。

参考文献

[1] 次世代電子行政サービスの実現に向けたグランドデザイン　2008 年 6 月 4 日
http://www.kantei.go.jp/jp/singi/it2/nextg/index_before090916.html#jisedai
[2] マイナンバーシステム　2016 年 12 月 5 日
https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/detakatsuyokiban/kiseiseidokaikaku_dai2/siryou1_2.pdf
[3] 内閣府 第 5 期科学技術基本計画 Society 5.0　2016 年 1 月 22 日
http://www8.cao.go.jp/cstp/kihonkeikaku/index5.html
[4] (独)情報処理推進機構 IT 人材白書 2017　2017 年 4 月 25 日
https://www.ipa.go.jp/jinzai/jigyou/about.html
[5] 学会ホームページ
https://www.ipsj.or.jp/it-forum/CITP.html
[6] CITP コミュニティ
https://citp-forum.ipsj.or.jp/
[7] CPD 規程
https://www.ipsj.or.jp/13CITP/CITP_CPD_kitei20170731v6a.pdf

以　上

デザイン思考を流用した地域復興アイデアソン

㈱ハイマックス　土屋俊樹

概要 : 2017 年 10 月 27 日 宮城県石巻市の石巻専修大学にて、CITP 社会価値創造分科会他有志メンバーにより、CITP シンポジウムを開催した。シンポジウムでは石巻市オープンデータを題材に、同大大学生と CITP メンバーによる地域活用アプリ作成のシビックテック（アイデアソン）を実施した。その活動内容をレポートする。

1. シビックテックの概要

2017 年 10 月宮城県石巻市の石巻専修大学にて CITP シンポジウムを開催した。シンポジウムの中で、石巻市オープンデータ[1]を活用したアイデアソンを大学生中心に実施し、ワークショップ自体は盛況のうちに終えることができた。

取組み内容については、2 月のソフトウエアジャパン、3 月の情報処理学会全国大会にて発表した。発表の際に使用した資料を元にその概略を本書向けにレポートする。

2. 取組みの背景

CITP コミュニティ内の社会価値創造分科会（その後、シビックテック SIG へ改編）にて、デザイン思考[2]を活用した社会価値問題解決の取組みの一環として、IT による震災復興支援ができないか討議を重ねた。

そして被災地である石巻現地視察を経て、シビックテックを兼ねたシンポジウムを現地開催する運びとなった。

3. 実施概要

シンポジウムは 4 部構成とし、前半 3 部は CITP メンバーによる講演、後半 1 部をシビックテック（アイデアソン）とした。石巻専修大学の教室を間借りし、大学生や CITP メンバー他を交えて 4 グループに分かれてアイデアソンを実施した。

4. 実施結果

短い時間ではあったがグループディスカッションは盛り上がり、全グループがアイデア発表までたどり着けた。終了後の大学生のアンケート結果も約 9 割有用との評価を得た。

また CITP メンバー自身も若い大学生とのディスカッションを大いに楽しみ、かつ刺激を受けた。

5. 今後の展望

今後は、アイデアソンの手法をさらにブラッシュアップし、実用に耐えるアイデア出しを行い、実際のアプリリリースまで結び付けたい。ゆくゆくはマネタイズできることが理想だが、まずは継続して実施できる体制作りを目指す。また当取組みを他大学へも横展開していきたい。

6. 補足

参考として実際の発表内容を次頁以降に添付する。本書向けに縮小しているので、読みにくい点はご容赦願いたい。通常カラー版は下記 URL を参照願いたい。

＜通常版 URL＞
http://www.ipsj.or.jp/event/sj/sj2018/download/citp/Session2.pdf

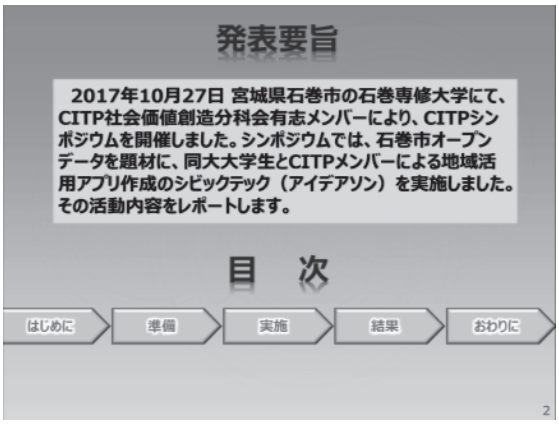
【著者略歴】土屋　俊樹（つちや　としき）
CITP 認定番号 15000003
シビックテック SIG メンバー
㈱ハイマックスにて、主に流通、小売業のシステム開発にプロジェクトマネジャーとして従事。またユーザー企業情報システム部門向け講座の企画・講師を担当。
高度情報処理(ST、PM、AE、DB、SM、SC)

ソフトウエアジャパン、および第 80 回情報処理学会全国大会発表資料（右側に簡単なコメントを追記）

1

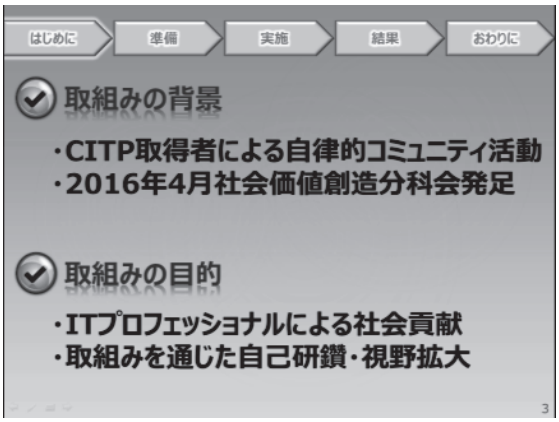
表紙。

2



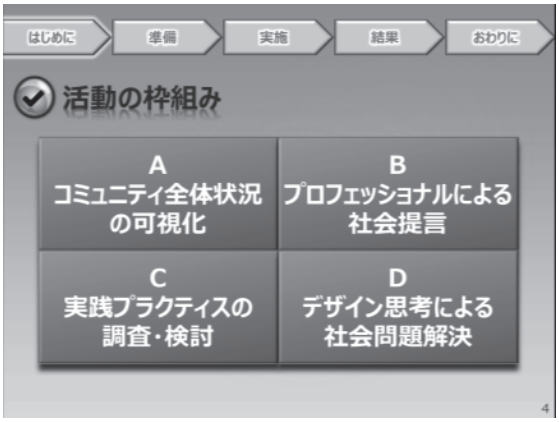
発表要旨と目次。

3



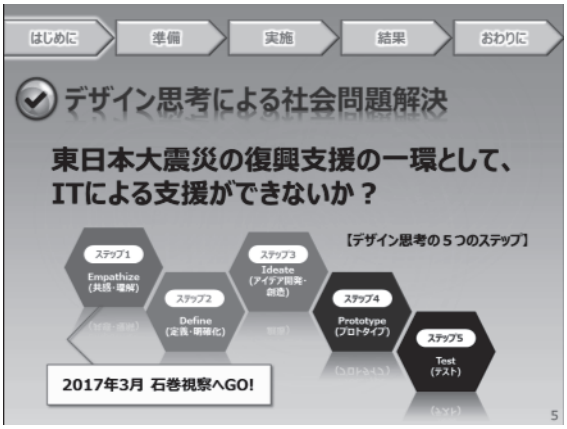
シビックテック取組みの背景と目的を説明。

4



CITP コミュニティは、主に４つの枠組みに沿って取り組んでいる。

5



有名なスタンフォード大学のデザイン思考フレームワークを用いて課題を検討。
まずは、「共感＝考えるより感じよう」ということで、CITP メンバーの出身地でもあった宮城県石巻市へ現地視察に出かけた。

6

石巻市現地の震災情報館にて、現地 NPO の館長さんから現地の復興の模様を教えていただいた。

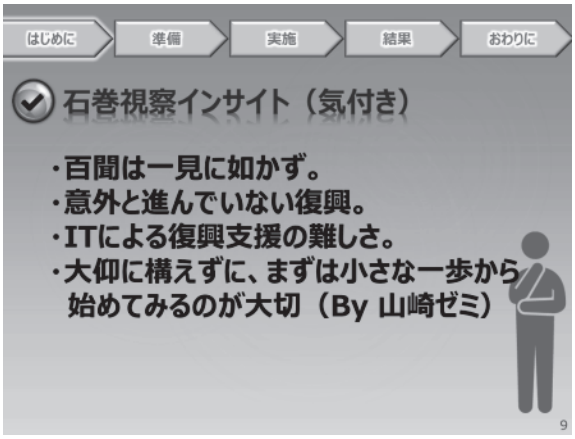
7

多数の児童と先生が亡くなった大川小学校跡を見学。遺構として残る建物が痛々しい。津波の凄さを改めて実感。

8

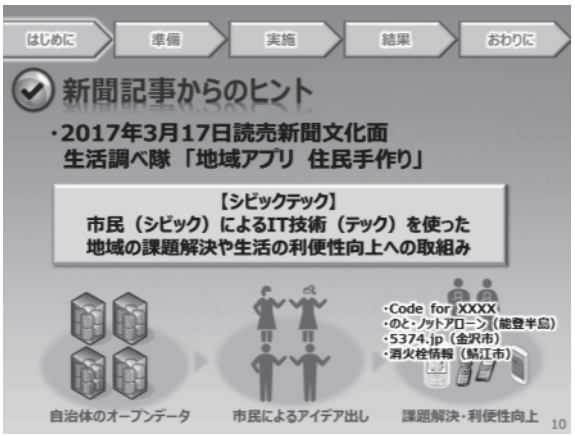
視察の最後に石巻市にある石巻専修大学にて、山崎教授の震災復興ゼミを受講。大学生とともにワークショップを開催していただいた。復興支援への気付きを得る。

9



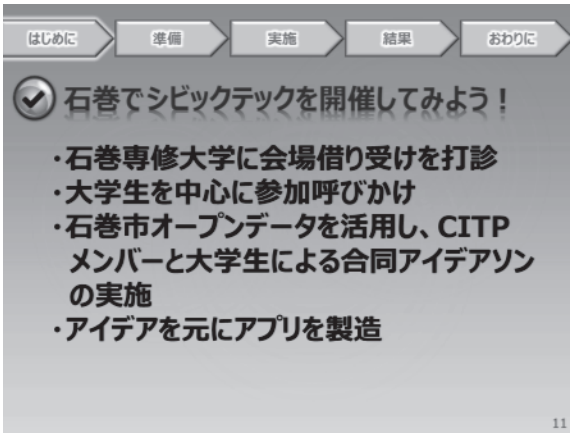
石巻視察結果の取りまとめ。
この時点で今後の具体的な取り組みは模索状態であった。

10



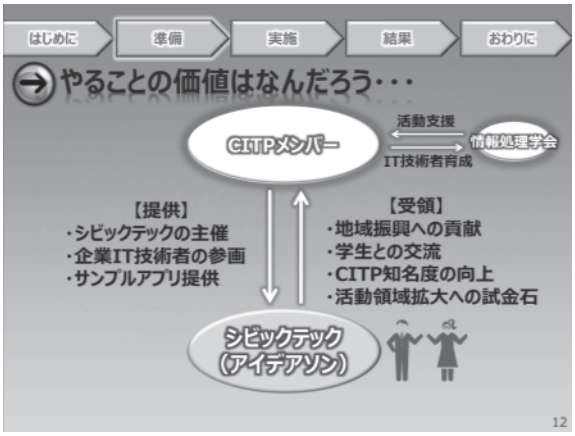
ちょうどその頃、新聞記事より今後の取組みのヒントを得る。
→現地のオープンデータを活用した現地課題解決のアプリを作れないか？

11



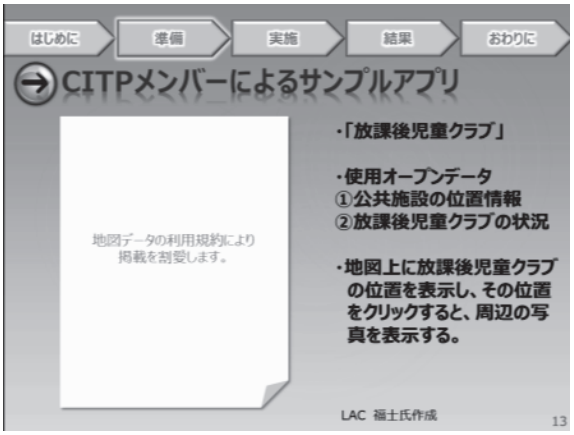
石巻でシビックテックの開催を検討。
アイデアを出し合い、実際に開催してみることに決定した。

12



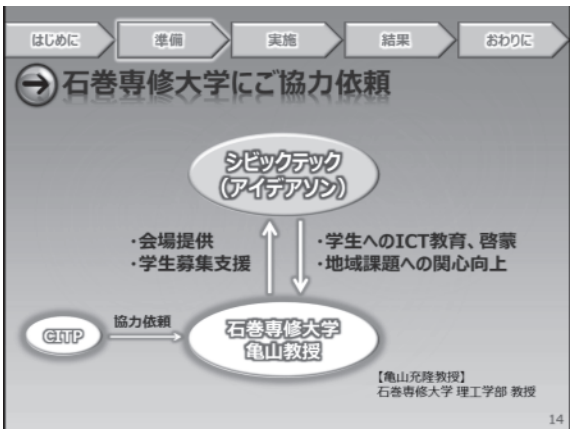
＜準備段階の説明＞
実際の開催にあたって、取組みの「価値」（＝実行する意味）を図解してみた。

13



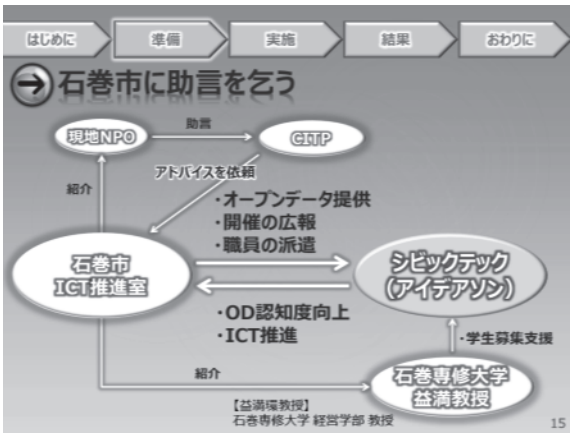
LAC 福士氏が作成したサンプルアプリ。
（規約の関係上、掲載を割愛します）

14



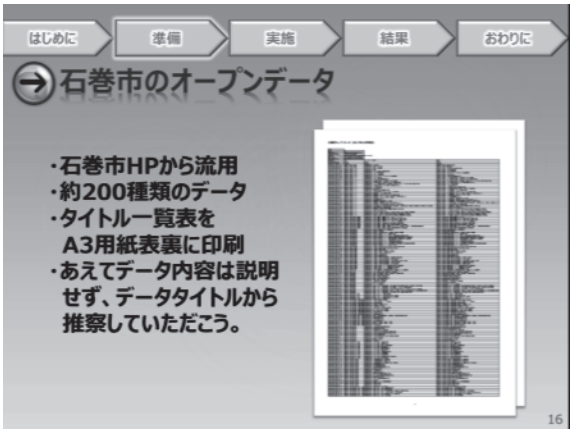
まずは石巻専修大学に協力を打診した。
取組みの価値を説明し、亀山教授より前向きな返事をいただけた。

15



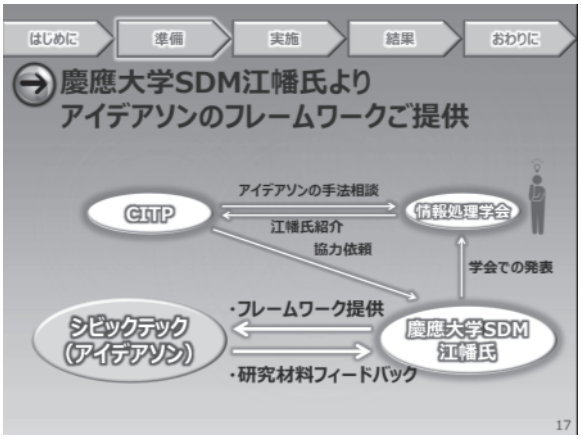
次にオープンデータの提供元である石巻市 ICT 推進室にアドバイスをいただけないか打診した。
協力する旨の返信をいただけた。

16



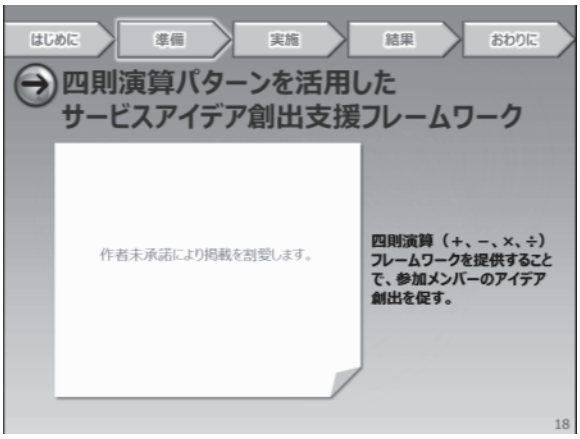
石巻市のオープンデータの説明。
約 200 種類、公開されている。

17



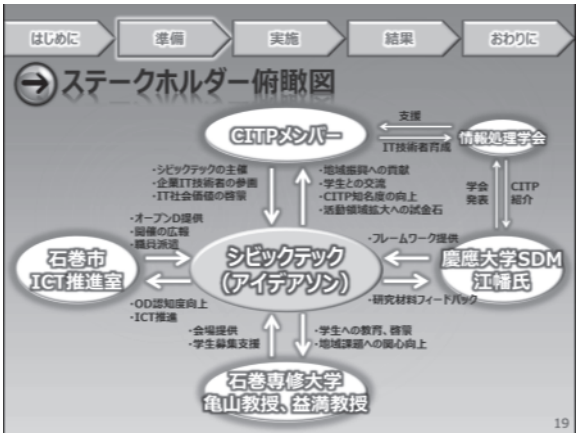
情報処理学会旭氏の推薦により、アイデアソン実施のフレームワークを、慶應大学 SDM の江幡氏よりご提供いただく。

18



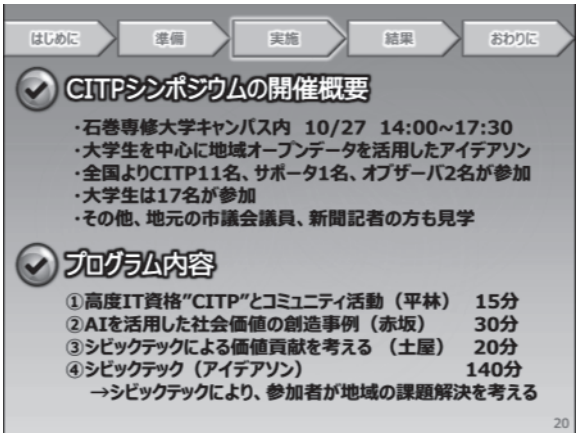
四則演算パターンを活用したサービスアイデア創出支援のフレームワーク。
（作者都合により掲載は割愛します）

19



まとめ：ステークホルダー全体を俯瞰。
それぞれ一方的な価値提供になっていないことに注目。

20



＜実施段階の説明＞
開催概要とプログラム内容を説明。金曜日の午後を使って石巻シンポジウムを開催した。

21

No.	タスク	内容	時間	累計時間
1	チーム分け	チーム分けを行う	5分	5
2	自己紹介	チーム内で自己紹介（各自30秒以内）	5分（30秒×4名）	10
3	チーム名決定	チームリーダー決定と、チーム名決定	5分	15
4	個人ワーク（用紙に記入）	フレームワークを使用して、可能な限りアイデアを出す。	20分	35
5	休憩	（個人ワークは継続可）	10分	45
6	グループワーク	一人ずつアイデアをチーム内で発表する。	30分	75
7	アイデアまとめ	模造紙（orパワポ）にアイデアを書き出す。	15分	90
8	発表	・チーム毎に発表	20分（5分×4チーム）	110
9	休憩	（この間に審査員による審査実施）	10分	120
10	表彰	優秀チームを表彰＆賞品（東京みやげ）授与	5分	125
11	感想戦	各チーム内で反省会	5分	130
12	講評	有識者より講評（2名）	10分（3分×2名）	140
13	（終了後アンケート記入）	アンケート用紙に記入してください	（時間外）	
		小計	**140分（2時間20分）**	**140**

実際の時間割。

22

ここからは、写真で実施状況を説明。
石巻専修大学キャンパス現地到着の様子。

23

キャンパス内の教室を借りて実施。
開始直前の様子。大学生が集まりはじめた。

24

１４時、シンポジウム開始。
総合司会：日立鵜澤氏。

25

講演１：
「高度 IT 資格と CITP コミュニティの活動」
講演者：日立　平林氏。

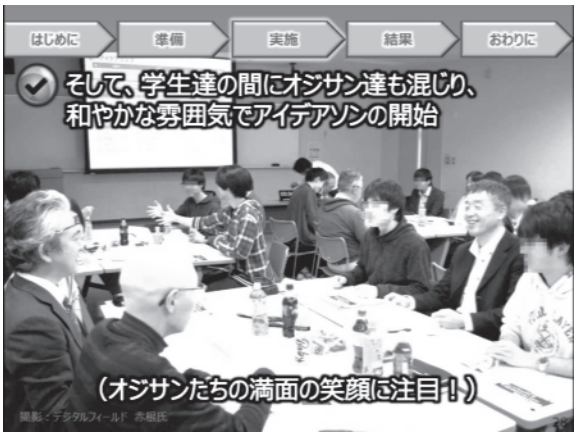
26

講演２：
「AI を活用した社会価値の創造事例」
講演者：日本 IBM　赤坂氏

27

講演３：
「シビックテックによる価値貢献を考える」
講演者：ハイマックス　土屋

28



しよいよシビックテック開始。
大学生の間に CITP メンバーが挟まり、４グループに分かれてディスカッション開始。
大学生に挟まれている CITP メンバーの笑顔がステキ。

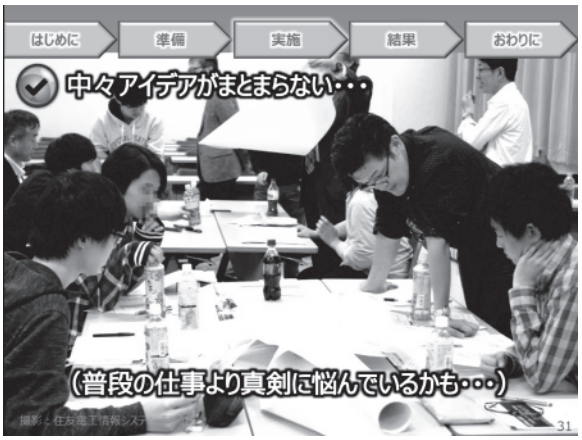
29

まずは個人ワーク実施。江幡氏ご提供フレークワークを使用してアイデア出し。なかなか手強い。

30

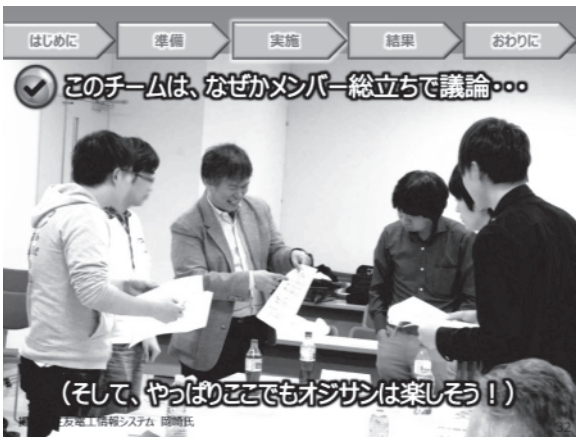
その後、グループワーク開始。
石巻専修大学　亀山教授も、机の間を徘徊しながら覗き込んでいます。

31



グループワークの様子。
かなり真剣に議論中。脳に汗かいています。

32



グループワークの様子。
このグループは全員総立ちで議論白熱中。（でも笑顔）

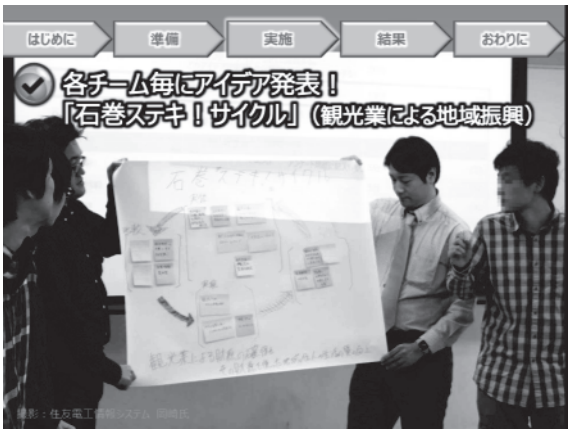
33

石巻市役所、ICT 推進室の高橋様も大学生達の間はさまり一緒に議論中。

34

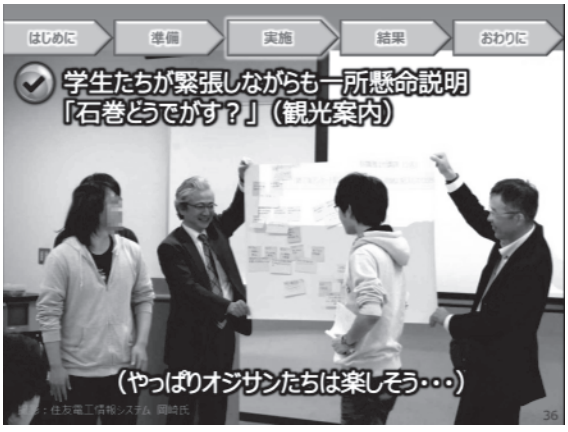
発表直前の様子。最後の追い込み中。

35



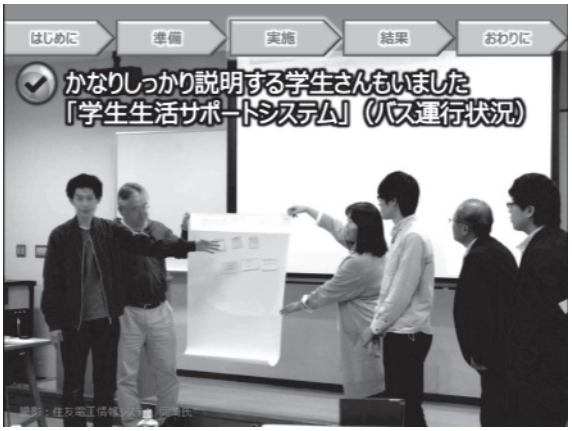
そしてグループ発表。
アイデアタイトル「石巻ステキ！サイクル」
（観光業による地域振興）

36



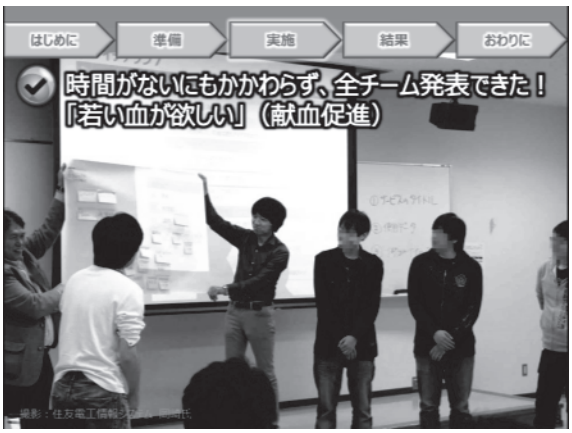
アイデアタイトル「石巻どうでがす？」
（観光案内）

37



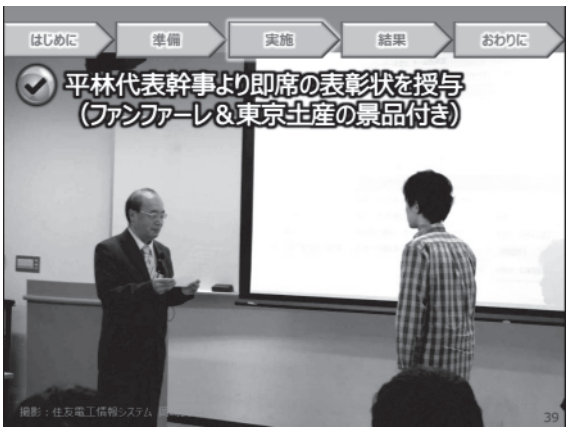
アイデアタイトル「学生生活サポートシステム」
（バス運行状況）

38



アイデアタイトル「若い血が欲しい」
（献血促進）

39



最後に各アイデアについて表彰式。
CITP コミュニティ代表幹事平林氏より表彰状授与。

40

講評：亀山教授
「この取り組みは、ぜひ継続してほしい」

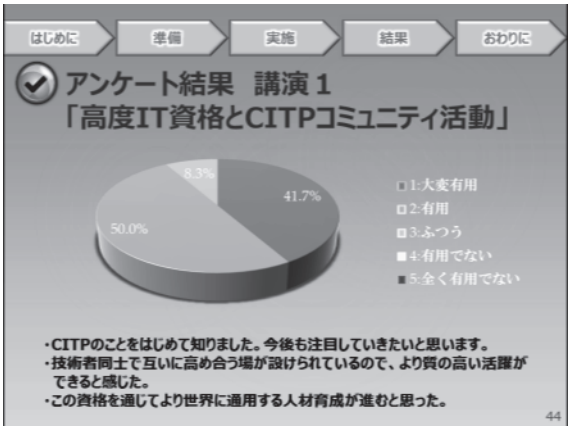
41

講評：情報処理学会オブザーバ 林氏
「楽しい取組みでした」

42

講評：上表処理学会オブザーバ 旭氏
「非常に有意義な取組みでした」

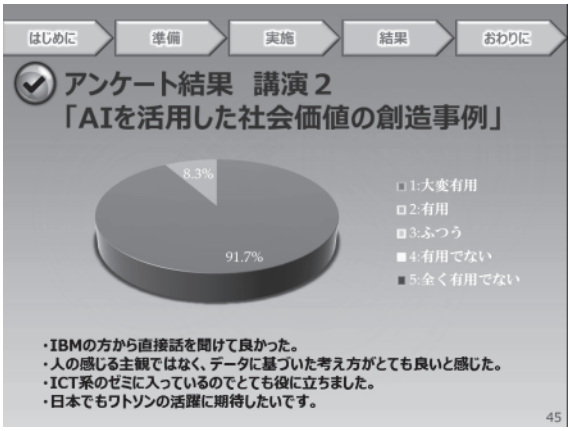
43



大学生達のアンケート結果取りまとめ。

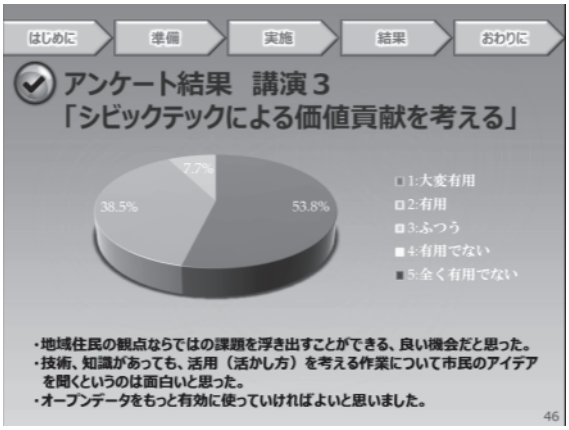
講演１：約９割有用。
主な感想：
・CITP のことをはじめて知りました。今後も注目していきたいと思います。
・技術者同士で互いに高め合う場が設けられているので、より質の高い活躍ができると感じた。
・この資格を通じてより世界に通用する人材育成が進むと思った。

44



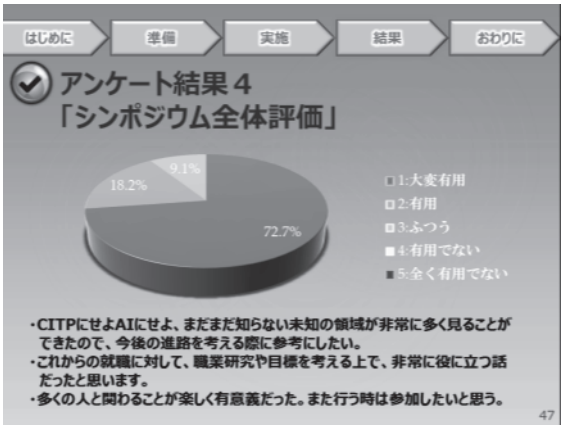
講演２：約９割非常に有用。
主な感想：
・IBM の方から直接話を聞けて良かった。
・人の感じる主観ではなく、データに基づいた考え方がとても良いと感じた。
・ICT 系のゼミに入っているのでとても役に立ちました。
・日本でもワトソンの活躍に期待したいです。

45



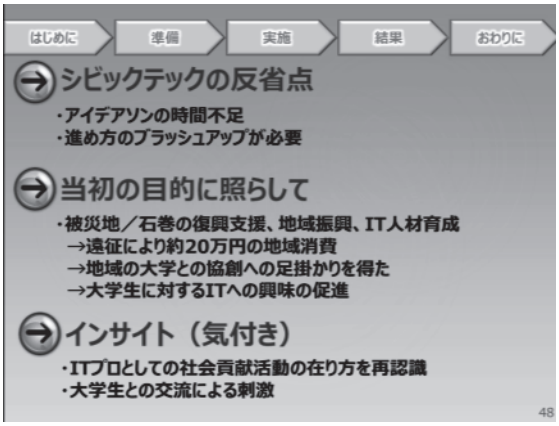
講演３：約９割有用。
主な感想：
・地域住民の観点ならではの課題を浮き出すことができる、良い機会だと思った。
・技術、知識があっても、活用（活かし方）を考える作業について市民のアイデアを聞くというのは面白いと思った。
・オープンデータをもっと有効に使っていければよいと思いました。

46



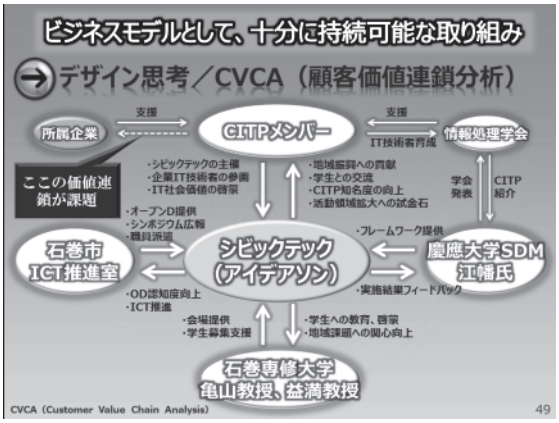
シンポジウム全体：約９割有用。
主な感想：
・CITPにせよAIにせよ、まだまだ知らない未知の領域が非常に多く見ることが　できたので、今後の進路を考える際に参考にしたい。
・これからの就職に対して、職業研究や目標を考える上で、非常に役に立つ話だったと思います。
・多くの人と関わることが楽しく有意義だった。また行う時は参加したいと思う。

47



<おわりに>
シビックテックの反省点・振り返りと気づき。

48



最後にあらためて全体ステークホルダー俯瞰図を説明。
これはデザイン思考的には、CVCA（顧客価値連鎖分析）に該当する。マネタイズまでにはたどりついていないが、取組みとしては十分に持続可能であることを説明した。

＜注釈＞

[1]　石巻市オープンデータ
http://www.city.ishinomaki.lg.jp/cont/10182000/20161007130030.html

[2]　デザイン思考についての参考書籍
- 「デザイン思考が正解を変える」　ティム・ブラウン
  重要キーワード :「変化しつづける外的要因（新技術、顧客基盤の変化、戦略的な脅威やチャンス）にもっともさらされている人々こそ、それに対するのにもっとも適していて、さらに対応する意欲を持っている」
- 「デザイン思考の道具箱」奥出直人
  重要キーワード :「デザインを専門としていない人にデザイン手法を教えて、コラボレーションによって分析的には不可能な問題を解いてみせる。それがデザイン思考だ。」
- 「システム×デザイン思考で世界を変える」前野隆司
  重要キーワード :「CVCA は、スタンフォード大学の故石井浩介教授らによって提唱されました。検討の対象となる会社や組織が「誰」と「どんな価値」をやり取りしているかというバリューチェーンの視点で、ある製品やサービスをめぐるステークホルダー間の関係を可視化する手法です」
- 「エンジニアのためのデザイン思考入門」東京工業大学エンジニアリングデザインプロジェクト

以上

中国のインターネット事情

～ キャッシュレス化がもたらす超スマート社会 ～

情報処理学会　CITP コミュニティ
株式会社中電シーティーアイ　久保　壮一郎

1. はじめに

筆者は 2009 年頃から、担当業務であるアプリケーション開発において中国オフショアを活用してきた。その経緯で毎年中国を訪れているが、特に 2015 年以降、中国の人々の生活が大きく変わっていく様子に驚いていた。

変化の中心にあるのがスマホ決済である。中国ではスマートフォンによる決済（スマホ決済）が普及し、キャッシュレス社会が到来している。従来、コンビニなどで買い物をすると、手垢にまみれた紙幣を渡し、店員はめんどくさげに透かしをチェックすることがおきまりの風景であったが、それはもはや過去の話である。現在、上海では支払い時に現金を出す人間は外国人くらいだといって過言ではない。つり銭が無いという理由で商品購入を拒否された経験は一度や二度ではない。

スマホ決済は支払い行為を簡素化しただけでなく、決済、個人認証、信用のプラットフォームとして機能している。このプラットフォームにより、企業家たちはアイデアのマネタイズをすることが容易となった。このことが、シェア自転車や無人コンビニなどのさまざまな新サービスを生む土台となっている。

本稿では、キャッシュレス化とは単に決済を効率化させるだけでなく、新たなサービスや商品を生み出す効果があり、最終的には超スマート社会の実現につながるということを主張する。第 1 章では中国のインターネット事情を概観する。その後、第 2 章にてスマホ決済によるキャッシュレス化の背景を明らかにし、さらに第 3 章でスマホ決済を土台として生み出された様々なサービスについて紹介したい。

2. 中国のインターネット概要

2-1. 世界一のインターネット人口

中国は世界一のインターネット人口を持っている。その人数は 2017 年 6 月末時点で 7.3 億人といわれており、ヨーロッパの総人口に匹敵するものだ。

さらに、スマートフォンからの利用は 90%を占める。これは日本やアメリカとは異なり、

パソコンによるインターネットの時代を経由せずに、直接モバイルインターネットの時代に突入したという事情による。中国の人々にとってインターネットは常に手のひらにある身近な存在であり、このことが、スマートフォンやインターネットを使用した新しいサービスが抵抗なく受け入れられる下地となっている。

2-2. 規制されたインターネット環境

このような多くの顧客を擁する巨大 IT 市場であるが、残念なことに海外企業は直接に参入することはできない。中国では政府によるインターネット空間の強い統制が行われているためである。ネット上のニュースやアプリ、SNS の書き込み内容は厳しく検閲され、中国共産党や国家、政府要人に不都合のある内容は逐一削除される。最近では、「熊のプーさん」や「ジャイアン」が習近平国家主席に似ているということで規制対象になったことで話題になった。

こうした統制は「グレートファイヤーウォール」と呼ばれている。この統制により中国共産党の「指導」が及ばない海外企業が運営するサービスは、基本的には中国国内では利用することはできない状態にある。そのため、中国の各種インターネットサービスは、中国国内の IT 企業が海外でヒットしたサービスを中国向けにローカライズして提供している。筆者も中国出張中は、日本で常時利用している Google 検索や Google Map、LINE など利用できないため、上述した中国版アプリで代替している。

2-3. 中国 IT 企業の成長

政府によるこうした「ネット鎖国」により、膨大な利用者を取り込むことに成功した中国の IT 企業は世界レベルの大企業として成長を遂げている。中でも、アリババとテンセントという 2 大ネット企業は、2017 年末にそれぞれ時価総額が 50 兆円を超えており、時価総額の世界ランキングでもトップ 10 位以内にランクインしている。

アリババはネット通販最大手で、淘宝網や T モールなどを運営しており、E コマースの分野にて中国でトップシェアを占めている。ソフトバンクも早い段階から出資をしており、2015 年にはニューヨーク市場に史上最大規模で上場を果たしたことも話題となった。

一方のテンセントは、中国版 LINE と呼ばれている微信を運営している。微信は全世界で 10 億人を超えるユーザーを抱える超巨大 SNS である。企業公式アカウントは 2000 万社を超えており、豊富な資金力で多くの事業領域に投資先を広げている。

2-4. スマホ決済分野での競争

アリババとテンセント、ネット通販と SNS と、業態が異なる 2 社が現在熾烈な競争を繰り広げているのが、スマホ決済の分野である。

先行したのはアリババである。もともとはネット通販における決済手段として開発した決済システムをリアルの店舗にも展開した。テンセントは後発ながら、10 億人という巨大

SNS を背景にシェアを一気に伸ばしている。

次章にて、このスマホ決済の概要と、その覇権をめぐる 2 大ネット企業の競争がもたらした結果について詳述したい。

3. スマホ決済の普及

3-1. スマホ決済とは

本稿では、スマートフォンによる決済を総称してスマホ決済と呼んでいる。スマホ決済には二つの側面がある。一つは、スマートフォンからネット通販を利用する際の決済機能、もう一つは、リアル店舗での決済機能だ。リアル店舗では、専用アプリに表示される QR コードを店舗側が読み取ることで決済が完了する。

利用シーンがネットかリアルか、言い換えると、オンラインかオフラインかに関係なく、スマートフォンがあれば同じ仕組みで決済ができる。このことがスマホ決済の本質であり、日本の電子マネーとの最も大きな違いであるといえる。日本では、例えば交通系 IC カードなど、リアル店舗を前提に設計されており、チャージした金額をネットでの商品購入やサービス利用に使用することはできない。

3-2. ネット通販の決済手段

かつて中国では、信用を前提とした商慣習が確立されていないため、ネット通販は普及しないと言われていた。中国にネット通販を根付かせるには、偽物と不払いを防ぐ安全な取引方法を確立する必要があった。

そこでアリババが自社ネット通販サイトで導入したものが、いわゆるアリペイである。アリペイは、第三者決済という仕組みで安全な取引を実現している。顧客と店舗はそれぞれアリペイ口座を持つところから始まる。アリペイ口座は銀行口座と紐づいており、自由に資金をチャージできる。顧客が商品を購入した際の代金はすべてアリペイで支払う。アリペイでの支払いが完了すると、店舗に連絡が行き、店舗はそれを受けて商品を発送する。商品を受け取った顧客は中身を確認し、問題がないことが確認できたらその旨をアリババに通知する。この段階で店舗に代金が届き、決済が完了する。この仕組みにより、顧客は偽物をつかまされる確率が減り、店舗側も遅滞なく支払いを受けることができる。取引中に発生した決裁上の損失は、基本的にはアリババが保証する。

2003 年、中国には eBay が進出しており、アリババとネット通販のシャアをめぐり激しい競争を繰り広げていた。アリババは、この中国の商慣習にフィットした決済の仕組みにより競争に勝利し、ネット通販事業のトップの座を確立することができた。

3-3. スマホ決済普及の背景

さて、リアル店舗に目を向けてみると、中国における決済手段は、従来は現金とデビッ

トカード（銀聯カード）が主流であった。クレジットカードは現在も普及していない。審査に通るだけの収入を持つ国民の絶対数がまだまだ少ない上に、手数料も高額であることが普及を妨げる原因である。

銀聯カードは銀行口座に紐づけて発行されるデビットカードである。中国政府の後押しもあり、多くの店舗で使用できるが、認証手続きが煩雑で使い勝手が悪い。現金は偽札が横行しており信頼性が低く、汚れも目立つ。さらに、最高紙幣が 100 元と低く、日常の買い物に際しても多額の紙幣を持ち歩く必要があり、煩雑であった。

このような決済事情のなか、2011 年にアリペイはオフラインの決済手段にも対応した。スマートフォンと QR コードで決済ができる手軽さは、従来の煩雑な決裁に悩む人々からの指示を受け、一気に普及することとなった。

店舗側にとってもクレジットカードに比べて格段に手数料が低いことが大きな魅力であった。小規模飲食店や露天商、果物店、雑貨店などは店頭に支払い用の QR コードを掲示するだけでよいので設備投資は一切不要。さらに帳簿の作成も自動化されるなどの管理上の手間も軽減されるため、さまざまな業態に広まっていった。

3-4. アリババとテンセントの競争

このように、アリババのアリペイが中国の決済環境を作りかえる中、テンセントは 2013 年に SNS 機能の一部としてスマホ決済サービスに参入した。大規模 SNS と圧倒的なユーザー数を強みに決裁取引数を一気に拡大した。正月時期にリリースした、個人間の送金サービスである「お年玉機能」のヒットも、テンセントのシェア拡大を後押しした。

アリババはアリペイをプラットフォームとし、金融サービスやシェアサービスなどを展開する戦略をとっている。対してテンセントは、SNS がプラットフォームとなる。

取引数から見ればテンセントはすでにアリババを抜いている。しかし、決済金額では、アリババが上回る。ユーザーからみると、テンセントはゲーム会社というイメージが強く、高い金額の決済を行うことに抵抗感があるようだ。対してアリババは金融業の参入を正式に表明していることがユーザーから一定の評価を得ていると思われる。

3-5. スマホ決済がもたらしたもの

スマホ決済は支払い行為を簡素化しただけでなく、決済、個人認証、信用のプラットフォームとして機能している。この決済プラットフォームにより、企業家たちはアイデアのマネタイズが容易となった。このことが、シェア自転車や無人コンビニなどのさまざまな新しいサービスや商品を生む土台となっている。

スマホ決済のシェアを拡大するには、まずはユーザー数を増やすことであり、そのために魅力的な新しいサービスや商品を次から次へとリリースしていく必要がある。その成長戦略から、アリババとテンセントは豊富な資金力により、新しい事業領域に投資先を広げ、収益を得ているだけでなく、決済プラットフォームを中心としたエコシステムを成長させ

ている。特に最近は両社とも小売り分野にて、新たな競争を繰り広げている。

いずれにしても、アリババとテンセントというネット巨大企業の競争が、新しいサービスや商品の開発を促進し、結果として人々により便利な暮らしをもたらしているといえる。次章より、スマホ決済を土台として生み出された様々なサービスについて紹介する。

4. スマホ決済がもたらす新しいサービス

4-1. シェアサービス

シェアサービスとは遊休資産の貸し出しを仲介するサービスと一般的に定義されている。シェアサービスを構築する上で、相手方の認証や信用確認、安全な決済は欠かせない要件である。したがって、これまで見てきたスマホ決済のプラットフォームは、シェアサービスとの親和性が高い。そのため、中国ではさまざまなシェアサービスが展開している。

4-2. シェア自転車

シェアサービスの事例として、日本でも話題になっているシェア自転車を取り上げたい。シェア自転車は専用のスマホアプリから解錠から支払い、施錠をすべて行うことができる。自転車は目的地についたら乗り捨てても構わない。別の人がその自転車で好きな場所まで移動する仕組みだ。自転車がどこにあるかも、アプリから探すことができる。とはいえ、自転車は大量にあふれているので、見つからないということはまずない。

ところで、日本でもレンタル自転車というサービスは観光地を中心に広く展開されている。ただし、返却スタンドが少なかったり、支払い時の小銭が必要だったりなど、使いやすいとは言い難い。中国でも同様の問題があり、観光客以外には利用されていない事情があった。このレンタル自転車の課題を IT 技術により解決したサービスがシェア自転車である。

もともとは、学生起業家が大学構内の移動を便利にするサービスとして立ち上げたものだ。それが社会に広まるまで、さほど時間がかからなかった。

ヒットの要因は、価格や利便性はさることながら、自転車のデザインに気を配っているからだとも言われている。中国人はメンツを気にする。従来は自転車、電動バイク、自動車と、より高価なモノを所有することがメンツであった。これに対し、あえて自転車をスタイリッシュなデザインにすることで、シェア自転車に乗るコトはカッコいいというイメージを作り上げたのである。

一時期は 50 社以上がシェア自転車事業に参入していたと言われている。そのため、街には自転車が溢れかえり、また、競争に敗れた企業からはデポジットが戻らないなどの社会問題を生みつつも、後追いで規制や対策が行われ、現在は秩序を保っている。このように、まずはやってみて問題が出たら対策するという発想は、新しいサービスを実施する上で見習うべき姿勢であると考えられる。

4-3. 新しい小売り体験

アリババは新しい小売り体験という概念を提唱している。いわば、買い物をコト消費とする発想だ。人々の消費が店舗からネットに推移する中で、ネットとリアルを融合した店舗を開発することで、消費を促進させようという戦略である。

4-4. 無人コンビニ

2017 年 7 月、上海で無人コンビニがオープンした。Amazon Go が話題となったわずか半年後に、商用ベースで店舗展開を始めるという、おそるべきスピード感である。技術的には Amazon Go がカメラによる画像認識によるものだが、中国のそれは、各商品に IC タグをつけることで実現している。

店舗に入るには専用のスマホアプリが必要だ。あらかじめユーザー登録をしておき、アプリにて店舗のドアを開く。顧客は商品を選び、IC タグを近づけて代金を集計する。支払いはもちろんスマホ決済で行う。支払いが済んでいない商品を持っていると、外に出ることはできない。店舗内はリアルタイムで自動監視がされていて、不審な行動をした場合は、すぐに気づくことができる。

ちなみに無人コンビニを運営している起業家は、過去 2 回、事業に失敗している。それでもなお、再チャレンジできる社会が後押ししている。

4-5. ネットと連動した生鮮食品スーパー

上海ではネットと連動した生鮮食品スーパーが広がっている。アプリで商品を選択すると、近隣店舗から商品が配達されてくる。3 キロ圏内であれば、30 分以内かつ配送料無料のサービスを実現している。

このサービスでは、店舗はネット通販の倉庫であると同時に、ショーウィンドウの役割も果たしている。実際に店舗を訪れてみると、中央に大きな生け簀があり、生きている魚や貝をそのまま購入することができる。また、調理を依頼し、店内で食事をすることもできる。

値段は比較的高めの設定だが、人々は「新しい小売り」を体験することができる。

5. おわりに

キャッシュレス化とは単に決済を簡素化するだけでなく、新たな商品やサービスを生み出す効果がある。中国では、巨大 IT 企業が、スマホ決済によるキャッシュレス化を推進している。彼らが提供する決済、個人認証、信用のプラットフォームを土台に、企業家たちはさまざまなアイデアを実現して世の中にリリースしている。これらのサービスはネットとリアルが融合したものであり、それはまさに超スマート社会の実現に他ならない。

IoT（Internet of Things）は「モノのインターネット」と訳されることが多いが、「コトのインターネット」という側面がある。中国では決済という「コト」をネットにつなげることで、お金の流れというビックデータを得ており、今後はそれを利活用するために AI 分野の投資に力を入れている。中国の超スマート社会に、日本は大きく水をあけられている。

2017 年 8 月にはシェア自転車が日本の一部地域でサービスを開始した。2018 年春には、アリペイが日本で正式にサービスを開始するという。中国発祥のインターネットサービスが続々と日本市場に進入しきている中で、中国勢の勢いに脅威を覚えつつも、彼らがどのようにして硬直化した日本市場で新たなサービスを浸透させていくのか、今後注目したい。

久保 壮一郎　（認定番号：16006336）
（株）中電シーティーアイ

株式会社中電シーティーアイにて、インターネット関連サービスの開発・保守および、超高速開発基盤ソフトウェアの開発に従事。2009 年度より、継続的に中国オフショア開発を経験してきた。高度情報処理技術者（エンベデッド、セキュリティ、データベース、ネットワーク）、情報処理安全確保支援士

【参考文献】

[1] ダイヤモンド社『週刊ダイヤモンド』 2017 年 7 月 5 日号
[2] 毎日新聞出版『週刊エコノミスト』 2017 年 8 月 8 日号
[3] 毎日新聞出版『週刊エコノミスト』 2018 年 3 月 6 日号
[4] 株式会社文藝春秋『文藝春秋』2017 年 10 月 10 日号
[5] 日本経済新聞 2018 年 2 月 2 日朝刊　「中国 SNS 発 小売り革命狙う」
[6] 日本経済新聞 2017 年 12 月 27 日朝刊　「中国小売り　無人化の波」
[7] 日本経済新聞 2017 年 12 月 22 日朝刊　「中国ネット 2 強時価総額」
[8] 日本経済新聞 2017 年 12 月 21 日朝刊　「スマホが生む新たな消費」
[9] 日本経済新聞 2017 年 12 月 12 日朝刊　「検閲 vs. 隠語 やまぬ戦い」
[10] 日本経済新聞 2017 年 8 年 9 日朝刊　「止まらない中国ネット 2 強」
[11] 中国互聯網絡信息中心『中国互聯網絡発展状況統計報告』(2017)
[12] 天下文化『穿布鞋的馬雲』王利芬，李翔 (2015)

小学校プログラミング教育への考察
～夏休みの宿題で感じたこと～

宮下　修
株式会社中電シーティーアイ

小学校のプログラミング教育が 2020 年度から必修化される。最近のプログラミング教育の関心の高まりからか、テレビ、インターネット、書籍等いろいろな場面で見聞きすることが多くなってきている。本稿は、筆者の小学生の子供に初めてプログラミング（Scratch[1]）を触れさせたときの状況や、そこで感じた気づきを紹介し、教育制度や教育現場の現状、環境整備の必要性など、各種情報を基に考察する。

なお、本稿中の意見や、特に注釈の無い状況説明は筆者の個人的見解、および筆者の家族から伝え聞いた内容であり、所属元や CITP コミュニティの見解を代表して表明するものではないことを予めご了承いただきたい。

＜キーワード＞プログラミング教育、新学習指導要領、Computational Thinking、習い事

はじめに

小学生を子に持つ親として、毎年夏休みになると頭を悩ますものに「自由研究」がある。64.4%という数値は何であるか想像が付くだろうか。株式会社オークローンマーケティングが 2017 年 6 月にインターネット調査した「子どもの夏休みの宿題」を親が手伝っている割合（9～12 歳）である。[2]

ここで子供の名誉の為に断っておくが、筆者の家庭では「自由研究」のヒントは与えるが、やる内容は本人の判断に委ね、創作活動自体には無用な口出しはしないことにしている。

先の調査結果から見て、夏休みの宿題に関与する親は意外に多いと感じるのではないだろうか。筆者は IT 関連の仕事をしているが故、プログラミング教育というキーワードに職業柄敏感に反応したこともあり、小学生の子供にやらせてみたいと常々考えていた。NHK E テレでプログラミング番組[3]を既に視聴し興味を持っていたこともあり、筆者の提案はあっさり受け入れられた。

今回の取り組みで、自らの創造力を発揮し、目的に向かって努力する子供の姿を間近に見ることが出来た。プログラミング教育の目的は何であるか、子供は何を得ることが出来るのか、経験を通して得た内容、親が取り組むべき内容も併せて述べていく。

1. プログラミング教育とは

1-1 新学習指導要領

2017 年（平成 29 年）3 月、文部科学省は新学習指導要領[4]を公示した。2020 年度（平成 32 年度）から開始される小学校段階におけるプログラミング教育の必修化が盛り込まれた内容である。公示に至る過程では、「小学校段階における論理的思考力や創造性、問題解決能力

等の育成とプログラミング教育に関する有識者会議」[5]での検討を行い、2016 年（平成 28 年）6 月 16 日、「小学校段階におけるプログラミング教育の在り方について（議論の取りまとめ）」[6]を公表した。その後、2016 年（平成 28 年）12 月 21 日、中央教育審議会による「幼稚園、小学校、中学校、高等学校及び特別支援学校の学習指導要領等の改善及び必要な方策等について（答申）（中教審第 197 号）」[7]に組み込まれてきた。

このように専門家らにより議論が進められ、プログラミング教育制度の仕組みが作られていく訳であるが、「プログラミング教育」を単純に捉えることはなかなか難しい。新学習指導要領にはどのような定義がされているのだろうか。

以下は、小学校学習指導要領解説 総則編[8]からの抜粋である。

> 子供たちが将来どのような職業に就くとしても時代を越えて普遍的に求められる「プログラミング的思考」（自分が意図する一連の活動を実現するために，どのような動きの組合せが必要であり，一つ一つの動きに対応した記号を，どのように組み合わせたらいいのか，記号の組合せをどのように改善していけば，より意図した活動に近づくのか，といったことを論理的に考えていく力）を育むため，小学校においては，児童がプログラミングを体験しながら，コンピュータに意図した処理を行わせるために必要な論理的思考力を身に付けるための学習活動を計画的に実施することとしている。その際，小学校段階において学習活動としてプログラミングに取り組むねらいは，プログラミング言語を覚えたり，プログラミングの技能を習得したりといったことではなく，論理的思考力を育むとともに，プログラムの働きやよさ，情報社会がコンピュータをはじめとする情報技術によって支えられていることなどに気付き，身近な問題の解決に主体的に取り組む態度やコンピュータ等を上手に活用してよりよい社会を築いていこうとする態度などを育むこと，さらに，教科等で学ぶ知識及び技能等をより確実に身に付けさせることにある。

間違ってもプログラミング言語を習得し、コーディングを行い、アプリやゲームを作成することを目的としている訳では無い。プログラミング教育の重要なキーワードは、やはり「プログラミング的思考」や「論理的思考力」を育むことであろう。この２つの言葉から連想するのは、いわゆる「コンピュテーショナル・シンキング／Computational Thinking」の考え方である。今後 IT に携わっていくかどうかに関わらず、この考え方を習得する意義は大変大きく、仕事のみならず普段の生活においても「よりよい社会を築いて」いく為の重要なファクターとなるであろう。

1-2 コンピュテーショナル・シンキング／Computational Thinking

「小学校段階におけるプログラミング教育の在り方について（議論の取りまとめ）」[6]には、『「コンピュテーショナル・シンキング」の考え方を踏まえつつ、プログラミングと論理的思考との関係を整理しながら提言された定義である』とある。新学習指導要領のプログラミング教育を制定する上で参考にした重要な考え方であることが分かる。

Computational Thinking（以後 CT と略す）について、イギリスの Computing At School（以後 CAS と略す）が公開している解説書を参考に内容を見てみることにする。

※本稿では CT の起源や CAS に関する内容は省略する。本家 Web サイトを参照されたし https://www.computingatschool.org.uk/

CT は 5 つの概念からなるが、CAS computational thinking - A Guide for teachers[9]には次のように記載されている。（誤訳があるといけないため原文を併記する）

Computational thinking is a cognitive or thought process involving logical reasoning by which problems are solved and artefacts, procedures and systems are better understood.
コンピュテーショナルシンキングは、問題が解決され、人工物、手順、およびシステムがより良く理解されることによる、論理的な推論を伴う認知もしくは思考プロセスである。
It embraces:
それは次を含む：
the ability to think **algorithmically**; the ability to think in terms of **decomposition**; the ability to think in **generalisations**, identifying and making use of **patterns**; the ability to think in **abstractions**, choosing good **representations**; and the ability to think in terms of **evaluation**.
・**アルゴリズム的**に考える能力 ・**分解**の観点で考える能力 ・**一般化**で考える能力、パターンを識別し利用する ・**抽象化**で考える能力、良い表現を選択する ・**評価**の面で考える能力

5 つの概念（concepts）：能力（ability）の集合として表現されている。筆者も含めた IT 技術者ならば、これら 5 つの要素は理解に容易いものであるはずだが、はたしてこの内容を意識して教育論が確立されるのか、そして実際に教育がなされるのか、今後の整備にかかっている。

また、コンピュータ教育におけるレベル（Progress：上達）と 6 つのカテゴリ（Algorithms/Programming & Development/Data & Data Representation/Hardware & Processing/Communication & Networks/Information Technology）で構成された学習体系マトリクスである Computing Progression Pathways[10]には、5 つの能力のどれに該当するかが示されている。（紙面の関係上一部抜粋のみとし日本語訳は省略する）

＜表 1＞ Computing Progression Pathways（抜粋）

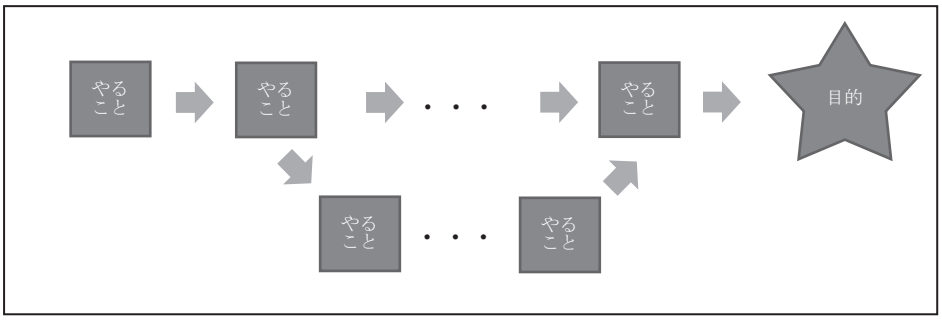
	Algorithms	Programming & Development	Data & Data Representation	Hardware & Processing	Communication & Networks	Information Technology
1	·Understands what an algorithm is and is able to express simple linear (non-branching) algorithms symbolically. (AL) ·Understands that computers need precise instructions. (AL) ·Demonstrates care and precision to avoid errors. (AL)	·Knows that users can develop their own programs, and can demonstrate this by creating a simple program in an environment that does not rely on text e.g. programmable robots etc. (AL) ·Executes, checks and changes programs. (AL) ·Understands that programs execute by following precise instructions. (AL)	·Recognises that digital content can be represented in many forms. (AB) (GE) ·Distinguishes between some of these forms and can explain the different ways that they communicate information. (AB)	·Understands that computers have no intelligence and that computers can do nothing unless a program is executed. (AL) ·Recognises that all software executed on digital devices is programmed. (AL) (AB) (GE)	·Obtains content from the world wide web using a web browser. (AL) ·Understands the importance of communicating safely and respectfully online, and the need for keeping personal information private. (EV) ·Knows what to do when concerned about content or being contacted. (AL)	·Uses software under the control of the teacher to create, store and edit digital content using appropriate file and folder names. (AB) (GE) (DE) ·Understands that people interact with computers. ·Shares their use of technology in school. ·Knows common uses of information technology beyond the classroom. (GE) ·Talks about their work and makes changes to improve it. (EV)
2	·Understands that algorithms are implemented on digital devices as programs.(AL) ·Designs simple algorithms using loops, and selection i.e. if statements. (AL) ·Uses logical reasoning to predict outcomes. (AL)	·Uses arithmetic operators, if statements, and loops, within programs. (AL) ·Uses logical reasoning to predict the behaviour of programs. (AL) ·Detects and corrects simple semantic errors i.e. debugging, in programs. (AL)	·Recognises different types of data: text, number. (AB) (GE) ·Appreciates that programs can work with different types of data. (GE) ·Recognises that data can be structured in tables to make it useful. (AB) (DE)	·Recognises that a range of digital devices can be considered a computer. (AB) (GE) ·Recognises and can use a range of input and output devices. ·Understands how programs specify the function of a general purpose computer. (AB)	·Navigates the web and can carry out simple web searches to collect digital content. (AL) (EV) ·Demonstrates use of computers safely and responsibly, knowing a range of ways to report unacceptable content and contact when online.	·Uses technology with increasing independence to purposefully organise digital content. (AB) ·Shows an awareness for the quality of digital content collected. (EV) ·Uses a variety of software to manipulate and present digital content: data and

	·Detects and corrects errors i.e. debugging, in algorithms. (AL)					information. (AL) ·Shares their experiences of technology in school and beyond the classroom. (GE) (EV) ·Talks about their work and makes improvements to solutions based on feedback received.(EV)
3:7	・・・	・・・	・・・	・・・	・・・	・・・
8	·Designs a solution to a problem that depends on solutions to smaller instances of the same problem (recursion). (AL) (DE) (AB) (GE) ·Understands that some problems cannot be solved computationally. (AB) (GE)	·Designs and writes nested modular programs that enforce reusability utilising sub-routines wherever possible. (AL) (AB) (GE) (DE) ·Understands the difference between 'While' loop and 'For' loop, which uses a loop counter. (AL) (AB) ·Understands and uses two dimensional data structures. (AB) (DE)	·Performs operations using bit patterns e.g. conversion between binary and hexadecimal, binary subtraction etc. (AB) (AL) (GE) ·Understands and can explain the need for data compression, and performs simple compression methods. (AL) (AB) ·Knows what a relational database is, and understands the benefits of storing data in multiple tables. (AB) (GE) (DE)	·Has practical experience of a small (hypothetical) low level programming language. (AB) (AL) (DE) (GE) ·Understands and can explain Moore's Law. (GE) ·Understands and can explain multitasking by computers. (AB) (AL) (DE)	·Understands the hardware associated with networking computer systems, including WANs and LANs, understands their purpose and how they work, including MAC addresses. (AB) (AL) (DE) (GE)	·Understands the ethical issues surrounding the application of information technology, and the existence of legal frameworks governing its use e.g. Data Protection Act, Computer Misuse Act, Copyright etc. (EV)

※AB=Abstraction; DE=Decomposition; AL=Algorithmic Thinking; EV=Evaluation; GE=Generalisation

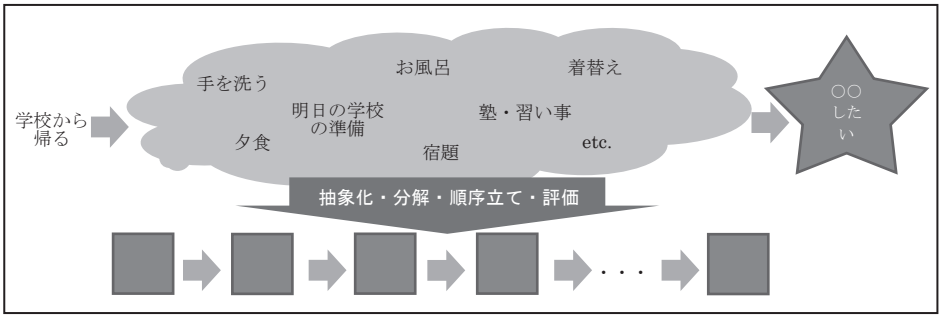
具体的かつ体系的に整理されており、我が国もプログラミング／コンピュータ教育をリードするイギリスの例を参考にすることは非常に意義があると考える。ただ、子供たちが理解し、楽しんで教育を受けるためには、このような概念を前面に出すことはせず、容易く理解できるレベルのものを準備することが望ましいと考える。

ではどのようなことか。問題解決を行う上で至極単純な例として次のようなものがある。



＜図 1＞単純なフロー図（概念）

具体的には次のような例題であれば論理的思考も理解し易いのではないだろうか。



＜図 2＞単純なフロー図（具体例）

おそらく子供たちは無意識に行っているようなことでも、きちんと論理立てて説明出来る

ようになることが重要である。このように子供たちにとって身近な題材から論理的思考を学び、ステップアップしていくカリキュラムが必要ではないかと考える。

1-3 STEM 教育との関わり

ここで近年、国内、海外問わず注目されている STEM 教育について取り上げたい。

STEM とは、"Science, Technology, Engineering and Mathematics"のそれぞれ頭文字で表される言葉である。科学、技術、工学、数学を重視した教育方針とされ、アメリカで始まった教育モデルと言われている。[11]

イギリスとアメリカの教育の違いを本稿で述べることはしないが、CT と同様に初等教育からの実践により、論理的思考力の醸成、延いては科学技術人材の育成を行うというシナリオを想定したとき、STEM 教育は大きな意義を持つものだと見えてくる。

世界最先端 IT 国家創造宣言・官民データ活用推進基本計画について（平成 29 年 5 月 30 日閣議決定）[12]、Ⅱ－１－(9) 人材育成、普及啓発等【基本法第 17 条、第 18 条関係】、① 分野横断的な施策のうち重点的に講ずべき施策、若年層に対するプログラミング教育の普及推進　にある、「将来の我が国の社会経済を支える人材を育成」にも基本的な考え方は合致する。

また、民間企業でも STEM 教育を謳う教育サービスの提供が開始されており、今後の盛り上がりが期待される。

1-4 プログラミング教育の副産物

プログラミング教育の効果として、「プログラミング教育」の実施状況に関する現状調査_調査報告書（詳細版）[13]には次の効果があるとする有識者の意見がある。

- 創造力の向上
- 課題解決力の向上
- 批判的思考力の向上
- 合理性、論理的思考力の向上
- 表現力の向上
- 意欲の向上（内発的な動機づけ効果）
- コンピュータの原理に関する理解
- 情報活用能力

今回の取り組みで筆者が特に感じた副産物は三つある。一つ目は「問題解決力」である。ある時子供が真剣な眼差しでパソコンに向かいバグ取りをする姿があった。自分の思い描いている動きと違うらしく、問題箇所を探し、本や筆者からヒントを得、改善策を試行錯誤しながら見つけていた。思い通りに動いた時の表情が印象的であった。二つ目は「自発的学習力」である。学校や塾の宿題を早々に済ませたり、小説を読んだりゲームする時間を削ってパソコンを使用することが多くなった。プログラミング本も数冊購入し、時間を見つけては読み返しているようだ。夏休みの自由研究をきっかけに、明らかに興味の質が変化している。三つ目は「創造力と自己実現・表現力」である。自由研究では Scratch でゲームを作った。何を作りたいかデザインを考え、どうすれば実現できるのか、悩みながら取り組んでいた。さらに、どうすれば面白くなるか、もっと高度なことを組み入れたいなど、一歩踏み込んだ

考えも芽生えてきている。

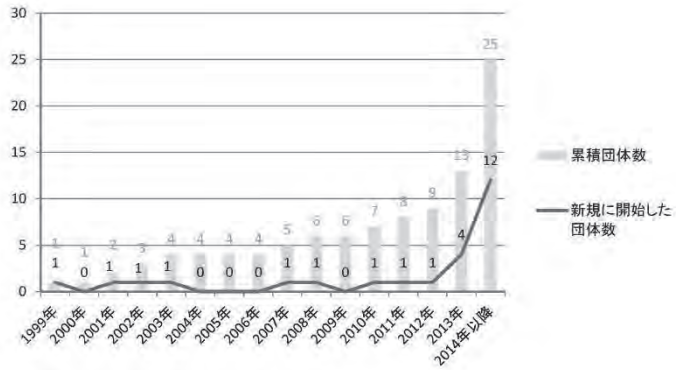
有識者の意見にあるような効果が、すべての子供たちに当てはまるとは断言出来ないが、新しい学びにおける知的好奇心を駆り立て、プログラミングスキルのみに留まらない多様な能力の向上へと導いてあげるのがこれからの教育制度の課題であるように思う。

2. プログラミングに触れる

プログラミングに触れる機会はいろいろ存在する。今回の筆者の取り組みでは、テレビ、書籍、インターネット、そして筆者自身の知見による子供への提供であった。世間に目を向けると多様な機会を見つけることが出来る。

2-1 プログラミング教室

近年、プログラミング教育の関心の高まりから、インターネットや雑誌の記事、フリーペーパーの習い事欄など多く目にするようになり、プログラミング教室が広まっていると実感する。若干古い情報となるが、平成 27 年に総務省が公表した「プログラミング人材育成の在り方に関する調査研究　報告書」[14]では、2013 年（平成 25 年）あたりからプログラミング教室・講座の開始が増加し始め、翌年 2014 年（平成 26 年）には倍増している。（図 3）



＜図 3＞プログラミング教室・講座の開始時期

ただしこの調査報告書は、プログラミングに関わる教育を実施している教育関係団体計 43 団体を対象とし、有効回答を得られた 25 団体のアンケート結果である。そのため、全国に存在する実際の数、および増加傾向が必ずしも一致しているとは限らない点に注意が必要である。本稿執筆時点（2018 年 2 月）でより新しい調査結果は公表されていないが、インターネットで「プログラミング教室」を検索すると数多くヒットすることから、ロボット教室も合わせると実際には非常に多く、増加傾向もしばらく続くのではないかと推測される。

一般社団法人情報処理学会の 2017 年 10 月号「情報処理」の特集「情報教育とワークショップ」[15]に、子供たちのプログラミング学習にワークショップの形態を採用した取り組みの実践例が紹介されている。先生が生徒に一方通行で教えるのではなく、子供たち同士が影響し合い、興味・創造力を膨らませて取り組んでいく。従来の教科にある学校授業とは一線を画すものである。

小学校のプログラミング教育においては、特集記事のような実践例や、一部の学校でのプログラミング教育の試行結果など事例を収集・整理し、授業のやり方に創意工夫が必要となるであろう。また、一般のプログラミング教室では、特集記事のワークショップの好事例のように、実施内容の「質」が今後求められるようになると思われる。

2-2 モデル校での試行

試行実施の一例として総務省の調査研究報告書がある。平成 29 年 7 月、総務省は「若年層に対するプログラミング教育の普及推進に向けた調査研究」報告書[16]を公表した。総務省は、プログラミング教育の低コストかつ効果的な実施手法や指導者の育成方法等を実証し、全国に普及させるための事業に取り組んでいる。この実証では、全国から選定された 11 団体が中心となり、全国 11 ブロックで地域のメンター（指導者）を育成し、地域の子供たちを対象としたプログラミング講座を実施している。（表 2）なお、対象の学校は小学校のほか中学校・高等学校も一部含まれる。

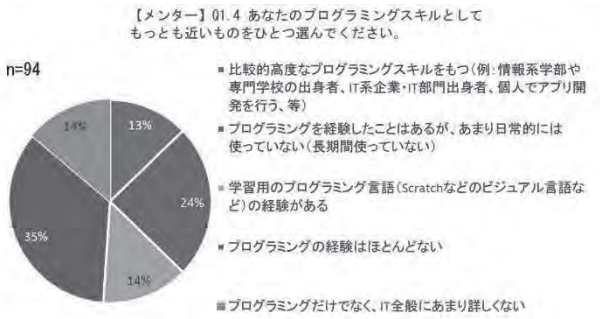
＜表 2＞全国 11 ブロックの概要（一部抜粋）

教材タイプ	ブロック（団体）	会場 受講者数	講座実施環境	教材
ロボット教材	北海道 (LITALICO)	1 校 (1 年生～6 年生 42 名＋特別支援学級 3 名)	・デスクトップPC1人1台（コンピュータ教室）ペア同士隣り合わせて着席。 ・レゴ® WeDo2.0 のスマートハブと Bluetooth 接続が必要。	・Scratch(スクラッチ) ・レゴ®WeDo2.0
	東北 (奈良女大附中)	4 校 (小学校高学年 53 名、中学校 30 名超)	・ノートPCグループに1台 グループごとに固まって着席。	・National Instruments「LabVIEW」(ビジュアル言語) ・python(テキスト言語) ・教育版レゴマインドストーム EV3(ロボット)
	近畿 (NTT 西日本)	1校 (5年生 62名)	・タブレット（Windows OS）及びロボット（Ozobot）は1人1台ずつ配布学校の教室にて、班ごとに固まって着席。 学校内に整備された無線 LAN 環境を活用。	・Ozobot(ロボット) ・OzoBlockly(ビジュアル言語)
	中国 (ファブラボ鎌倉)	1校 (高学年20 名)	デスクトップPC1人1台（コンピュータ教室。PCは壁際にレイアウトされ、中央にスペースあり。）	・Scratch(ビジュアル言語)
	四国 (TENTO)	2校 (6年生12名、3-5年生8名)	ノートPC1人1台 （コンピュータ教室） ※必要な設定を済ませたスティック型 PC（Ubuntu）を学校ノート PC で起動させて利用。	・ScratchX(ビジュアル言語) ・AruduinoX(サーボモーター)
	九州 (アーテック)	6校 (小学校高学年36名) (高等学校 26 名)	ノートPC1人1台（普通教室）	・Audiuno(テキスト言語) ・アーテックロボ(ロボット)
学習用ビジュアル言語	沖縄 (学情研)	2校 (高学年 65 名)	デスクトップPC1人1台 （コンピュータ教室）	・Scratch(ビジュアル言語)
	信越 (スタープログラミング)	3校 (高学年27名＋特別支援6名) (中学校32名)	・デスクトップPC（Windows） ・児童の座席配置（コの字型） ・有線LANで接続。 ・その他必須の機器や環境(プロジェクター2 台)	・Scratch(ビジュアル言語)
ドリル教材	関東 (グリコ)	1校 (低学年 195 名、保護者 136 名)	タブレットPC1人1台 （一部団体が貸与した端末を含む）	・GLICODE(お菓子を用いるプログラミング体験ツール)
	北陸 (みんなのコード)	5校 (高学年98名)	1,2,5コマ目：コンピュータ不使用（普通教室） 3,4コマ目：デスクトップまたはタブレット型PC1人1台 （コンピュータ教室または普通教室。）	・Hour of Code(ビジュアル言語) ・ルビィのぼうけん(アンプラグド)
開発系言語	東海 (D2C)	複数校 (中学校38名)	Macbook1人1台 ※団体が端末とネットワーク環境を持ち込み、設定。グループごとに固まって着席。	・Swift、Xcode(iPhoneアプリ開発) ・Gamesalad(テキスト言語) ・HTML/CSS、Brackets・Mozer(テキスト言語)

この報告書[16]で触れられている内容で、筆者が特に興味深いと感じたのがメンター育成、受講者の反応である。

＜メンター育成＞

各地域での実施に際し、メンターを募集し、研修会を実施している。メンターは地域の学生（大学生・専門学校生など）、社会人・地域住民、教員が候補となるが、半数近くがプログラミング未経験者であった。（図 4）

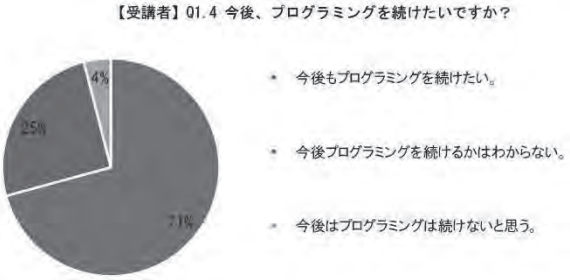


＜図 4＞研修受講前のメンターのプログラミングスキル

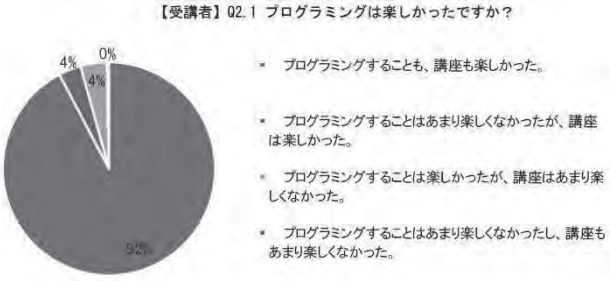
研修では IT スキルを一定レベルに向上させることの他に、答えを教えるのではなく子供の主体性を伸ばすようなコーチングスキルや子供同士の話し合いをファシリテートするスキルなどの教育スキルを向上させることを重視している、とある。これは小学校の先生たちへの教育に大いに参考になる手法ではなかろうか。教育のプロである先生たちは必ずしも IT スキルに長けているとは限らないため一定レベルへの引き上げは必要であるが、新しいプログラミング教育の準備をする上で、従来の教育方法が足枷となってはならない。2-1 で述べたワークショップの形態がプログラミング教育の手法として脚光を浴びるのも頷ける。

＜受講者の反応＞

講座終了後に受講した子供たちへのアンケートでは、プログラミングの継続希望は 7 割以上、プログラミングが楽しかったとする割合も 9 割を超えている。（図 5,6）



＜図 5＞受講者のプログラミング継続希望



＜図 6＞受講者の講座満足度

大多数の子供がプログラミングに関心を持ち、楽しむことが出来たようである。また、論理的思考力に関しては、「半数近い受講生は論理的にプログラムを見直すことが出来るようになっているといえる。また、プログラミングによって日常生活の課題（家事、忘れ物、ペンのインク切れ、教師の負担・・・等）を解決するためのアイディアが多数挙がっており、課題解決力醸成に繋がる取組みになっていたと推察される」とある。この調査からも、プログラミング教育の目的の一つである論理的思考力の育成は、継続していくことが重要であるが、達成できるものと考えられる。1-2 で述べたように、やはり身近な題材から論理的なものの考え方を学ぶことは、子供たちがイメージし易く適しているのかも知れない。

2-3 ３０年以上前にもあった

近年のプログラミング教育の盛り上がりから遡ること 30 年以上前、PC が家庭にあまり普及していない頃、主にホビー向け用途の PC として MSX[17]や、当時大流行していたファミリーコンピュータの周辺機器ファミリーベーシック[18]が存在した。詳しい仕様は本稿では省略するが、BASIC の文法に基づいた簡単なゲームプログラムを自作することができるとさ

れている。筆者がまだ小学生であった時期であるが、実際に MSX やファミリーベーシックを所有する友人もいて、プログラミング教室に通われていたことを記憶している。2020 年の小学校プログラミング教育の必修化は当時では考えられなかったであろうが、その時と違い、現代の子供たちが学ぶプログラミング環境はより高度化され整いつつある。子供たちが担うこれからのコンピュータ社会に一層期待したい。

3. 世間と学校現場の実情

夏休みが終われば自由研究の発表があるのはどの学校でも同じであろうが、子供が通う小学校での発表では意外な反応があったようだ。「自由研究でプログラミングをやったのはクラスの中で自分一人」「すごい！（友達）」「スクラッチって聞いたことあるけど何？（先生）」「えっ！プログラミングやったの？（ママ友）」など。他に気になることも聞いた「学校の PC が新しくなったけど動きが遅い」。どうやら、情報処理の特集記事[15]や、プログラミング教育試行実施校[16]に比べ、学校の対応状況の遅れや、周囲のプログラミングに対する意識がそれほど高くないように感じた。実際はどうであろうか。

3-1 小学校の ICT 整備状況

2017 年（平成 29 年）12 月、文部科学省は平成 28 年度学校における教育の情報化の実態等に関する調査結果[19]を公表した。小学校での ICT 環境の整備状況について 3 つの項目に注目した。（表 3）

＜表 3＞小学校の主な ICT 環境の整備状況（抜粋）

	1 台当たりの児童数	（参考）政府の目標値[20] 1 台当たりの児童生徒数
教育用コンピュータ	6.7 人	3.6 人

	無線 LAN 整備率(%)	有線 LAN 整備率(%)
普通教室の LAN	31.8 %	87.9 %

	100Mbps 以上の割合(%)	30Mbps 以上の割合(%)
超高速インターネット	46.4 %	86.9 %

教育用コンピュータに関して、第 2 期教育振興基本計画（平成 25 年 6 月 14 日閣議決定）[20]、基本施策 25-2 教材等の教育環境の充実　には、教育用コンピュータ 1 台当たりの児童生徒数の目標を 3.6 人としているが、調査結果では 6.7 人であり、教育用コンピュータの普及がまだ進んでいないことが分かる。

普通教室の無線 LAN に関して、同政府目標では整備率 100%を目指しているが 1/3 にも満たない状況である。ノート型やタブレット型の可動式コンピュータによる自由度のある授業形態を想定した場合には無線 LAN の方が良く、今後の環境整備が急務である。

インターネット接続速度に関して、今後教育用コンピュータの普及が進み、授業等でインターネットコンテンツの利用が増加し大量のデータ通信が発生すると、より帯域のあるインターネット環境が必要となるはずである。100Mbps 以上の割合が半分以下であるため、通信環境についても今後の環境整備が必要である。

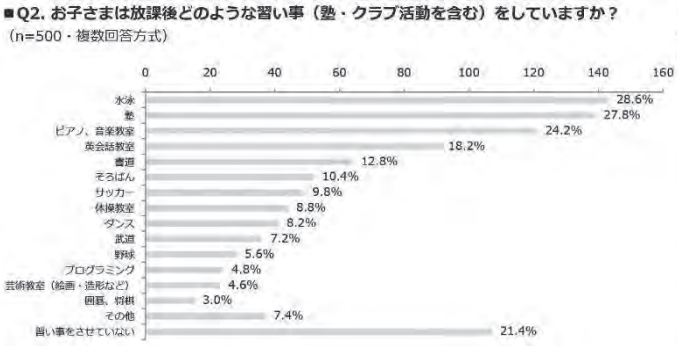
3-2 教員向け教育

学校教員へのプログラミング研修が進められているようだ[21]。記事にある参加者によると「大人が触っても楽しい。理科や社会の授業に使えそうだ」と話す一方、プログラミングへのなじみが薄い教師は「楽しく学べそうだが、自分が指導するとなると、より深く勉強をして臨まないといけない」と困惑している様子が窺える。

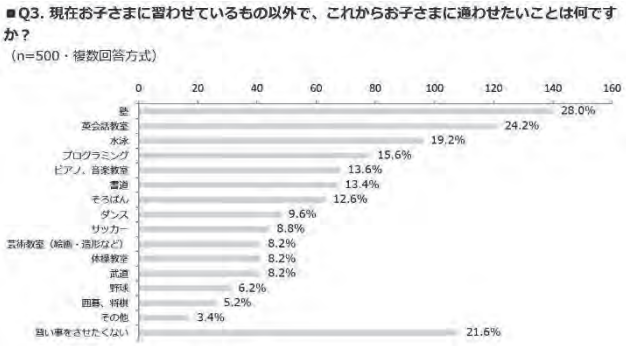
全国でどの程度教員向けプログラミング研修が行われているかの統計情報が見当たらなかった。学校における教育の情報化の実態等に関する調査結果[19]には、ICT 活用指導力の状況の各項目に関する研修を受講した教員数、および割合は存在するが、これは平成 19 年 2 月に策定・公表された「教員の ICT 活用指導力」のチェックリストをベースにしており、プログラミングに関する内容は含まれていない。毎年実施される実態調査も、今後の教育制度に合わせて見直されるべきと思われる。

3-3 習い事事情

プログラミング教育が注目されていることがわかる興味深いデータがある。株式会社明光ネットワークジャパン／明光義塾が実施した、放課後の習い事に関する小学生の子供を持つ保護者へのアンケート調査結果である。[22]



＜図 7＞放課後の習い事ランキング



＜図 8＞これから通わせたい習い事

現在通っている習い事（図 7）は、水泳やピアノなど昔から定番のものが上位を占めており、プログラミングは 4.8%で少数派である。これから通わせたい習い事（図 8）ではプログラミングが 15.6%となり上位に浮上している。英会話も上位に浮上しているのは、新学習指導要領で英語教育が強化される影響であろうか。多くの保護者が新しい教育制度を見据えて、子供の習い事を考えていることが見て取れる。

3-4 さまざまなギャップ

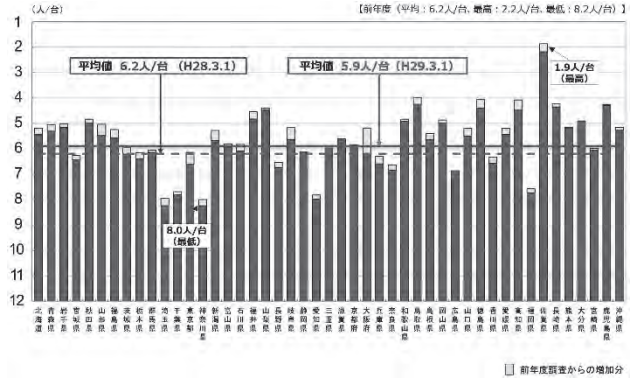
プログラミング教育の話題から少し逸れるが、筆者が最近感じた学校間のギャップについて紹介したい。先日、筆者の所在地で小中学校の美術展示会が文化センターで開催されたため参観してきた。展示品は図画工作や美術の授業、クラブ活動で作成した絵や工作物、書道などあり、学校間各学年共通したテーマで制作された作品である。学校間の作品を見比べてみるとあることに気付いたのだが、それは作品の“傾向”と、“デキ”が学校間で異なることである。個人的私見でうまく言い表せないが、色合いや表現方法、全体の印象が学校ごとに揃っている印象を受けた。これは、子供たちは千差万別でありながら各学校の担当教員の指導方法によって枠に入れられてしまうことにより“傾向”が生まれ、子供たちの創造力・表

現力などを伸ばせるかどうかで“デキ”が異なってくるのではないだろうか。

プログラミングでも同様なことが起きる可能性がある。プログラミング教育の目的は論理的思考力を育むことであるが、枠にはめた指導では本来の目的を果たすことは難しいはずである。ワークショップ形態の授業を積極的に活用するなど、従来とは異なる授業で個性を引き出し、能力を伸ばすことを前提としたカリキュラムが必要になってくると考える。

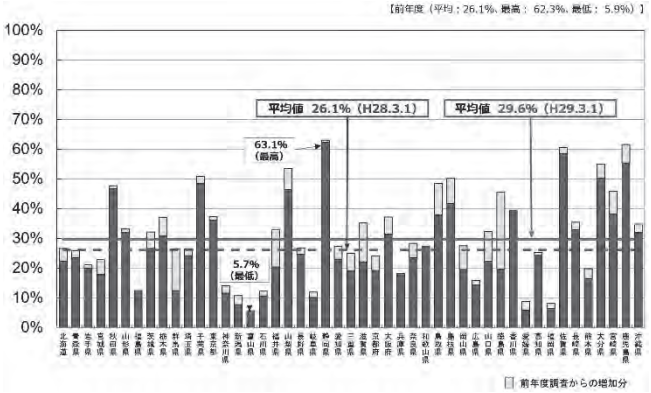
上記は学校間ギャップの一例を述べたが、少し視野を拡げて都道府県別の違いとして、学校の主な ICT 環境の整備状況と、プログラミング教室展開状況を見てみることにする。
なお、図 9,10,11 のデータは、都道府県ごとの整備状況を把握するため、小学校のみのデータではなく、学校教育法にて定義されている学校種である小学校、中学校、義務教育学校、高等学校、中等教育学校、特別支援学校の合算データである。[19]

＜学校の ICT 環境＞



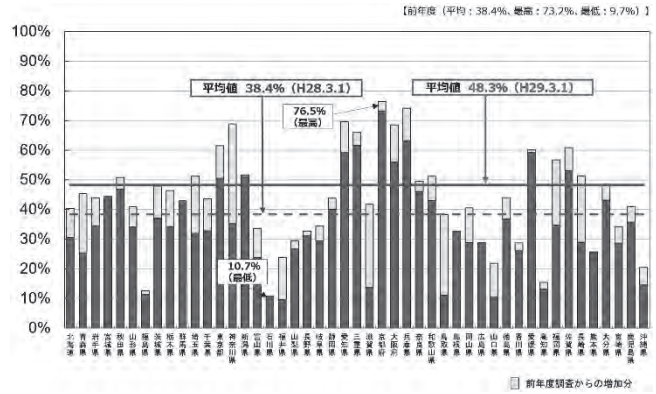
教育用コンピュータ 1 台当たりの児童生徒数の都道府県間のバラつきがあるのが分かる。

＜図 9＞教育用コンピュータ 1 台当たりの児童生徒数



普通教室の無線 LAN 整備率は都道府県間で大きく差が開いているのが分かる。

＜図 10＞普通教室の無線 LAN 整備率



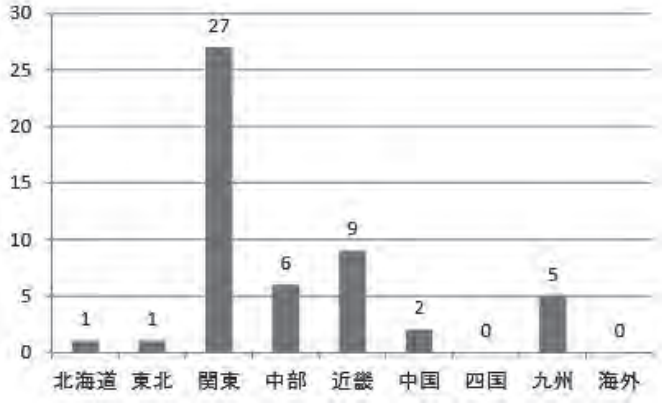
100Mbps 以上のインターネット接続状況は都道府県間で大きく差が開いているのが分かる。

＜図 11＞インターネット接続 100Mbps 以上整備率

都道府県間の ICT 整備状況の違いが把握でき大きな差も確認できる。本稿では割愛するが、市区町村別のデータも公表されており、整備率の高い都道府県であっても市区町村間では大きな差も見受けられる。地域により子供たちの学校教育環境に違いがあってはならないため、早急な整備が必要である。

＜プログラミング教室＞

総務省の「プログラミング人材育成の在り方に関する調査研究　報告書」[14]によると、プログラミング教室・講座の開催地の多くは関東に集中している。（図 12）また、都市の規模でみた場合、多くが大都市での開催であり、中都市・小都市は事例も少なく、プログラミング教育の認知度が低いと考えられる、とある。



注）2-1 で述べた通り、この調査報告書[14]は、平成 27 年に公表されており、プログラミングに関わる教育を実施している教育関係団体計 43 団体を対象とし、有効回答を得られた 25 団体のアンケート結果である。そのため、全国に存在する実際の数ではないことに注意が必要である。

＜図 12＞プログラミング教室・講座の地域別教室数

本稿執筆時点（2018 年 2 月）でより新しい調査結果の公表が存在しないが、学校数、児童生徒数の多い地域で開催される傾向があるように見えるため、今後も人口集中地区で多く開催されていくものと推測される。ただ、地域によって教育を受ける機会が損なわれるのは望ましいことではないため、自治体による誘致を積極的に行うなどの方策が必要である。

4. 取り組むべき事柄

プログラミング教育必修化に向けた準備として、これまでに学校の ICT 環境や、教育制度の整備が必要であることを述べてきた。これらは当然ながら今後の課題として位置付けられるものである。ハード面の ICT 環境整備は順次整備範囲を拡大していくことになるが、ソフト面の制度整備に関しては、課題や制約が多いと考えられ慎重に進める必要があろう。

4-1 教育現場の現実問題

学習指導要領の今回の改訂では、プログラミング教育は既存の科目の中で実施されるため教科としては存在せず、授業時間は単独で確保されることはない。（外国語の授業時間以外は増えない）[6][8]（表 4）

また、幼稚園、小学校、中学校、高等学校及び特別支援学校の学習指導要領等の改善及び必要な方策等について（答申）[7]には、「各小学校には、その実情等に応じて、プログラミング教育を行う単元を位置付ける学年や教科等を決め指導内容を計画・実施していくことが求められる。」とあり、カリキュラムの作成は学校側に委ねられている。また、同別紙 3-2[23]にはプログラミング教育の実施例（表 5）もあるが、より具体的な指導内容を創意工夫して

立案していかなければならないと考えられる。

＜表 4＞小学校標準授業時数の現行との比較

新							
	学年						計
	1	2	3	4	5	6	
国語	306	315	245	245	175	175	1461
社会	-	-	70	90	100	105	365
算数	136	175	175	175	175	175	1011
理科	-	-	90	105	105	105	405
生活	102	105	-	-	-	-	207
音楽	68	70	60	60	50	50	358
図画工作	68	70	60	60	50	50	358
家庭	-	-	-	-	60	55	115
体育	102	105	105	105	90	90	597
特別の教科である道徳	34	35	35	35	35	35	209
特別活動	34	35	35	35	35	35	209
総合的な学習の時間	-	-	70	70	70	70	280
外国語活動	-	-	35	35	-	-	70
外国語	-	-	-	-	70	70	140
合計	850	910	980	1015	1015	1015	5785

現行							
	学年						計
	1	2	3	4	5	6	
国語	306	315	245	245	175	175	1461
社会	-	-	70	90	100	105	365
算数	136	175	175	175	175	175	1011
理科	-	-	90	105	105	105	405
生活	102	105	-	-	-	-	207
音楽	68	70	60	60	50	50	358
図画工作	68	70	60	60	50	50	358
家庭	-	-	-	-	60	55	115
体育	102	105	105	105	90	90	597
道徳	34	35	35	35	35	35	209
特別活動	34	35	35	35	35	35	209
総合的な学習の時間	-	-	70	70	70	70	280
外国語活動	-	-	-	-	35	35	70
-	-	-	-	-	-	-	-
合計	850	910	945	980	980	980	5645

※授業時数の 1 単位時間は 45 分

※下線部が変更となった対象

＜表 5＞プログラミング教育の実施例

総合的な学習の時間	自分の暮らしとプログラミングとの関係を考え、そのよさに気付く学び
理科	電気製品にはプログラムが活用され条件に応じて動作していることに気付く学び
算数	図の作成において、プログラミング的思考と数学的な思考の関係やよさに気付く学び
音楽	創作用の ICT ツールを活用しながら、音の長さや高さの組合せなどを試行錯誤し、音楽をつくる学び
図画工作	表現しているものを、プログラミングを通じて動かすことにより、新たな発想や構想を生み出す学び
特別活動	クラブ活動において実施

小学校は基本的に担任が全ての教科を担当するケースが多いはずである。効率的な授業を計画したとしても､忙しいとされる教員たちにさらなる負担となることが容易に想像される。

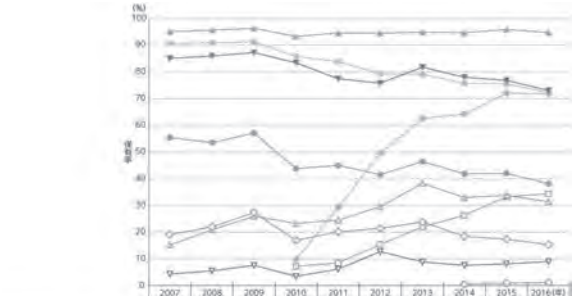
プログラミング教育必修化に向けた制度整備において、教員の負担軽減となる方策として五十嵐智生氏の提案[24]がある。英語教育で既に導入されている「外国人指導助手（ALT：Assistant Language Teacher)」の仕組みと同じように、プログラミング教育に対してシステムエンジニアによる「指導補助員（TA：Teaching Assist)」の仕組みを整備するというものである。TA 制度の実現に向けては、政府、自治体、各種団体、および民間企業との連携が重要であり協議を重ねていかなければならない。また､TA の確保や研修の方法論として、

2-2 で述べたモデル校での実証結果[16]も参考に出来るのではないだろうか。メンターの確保や育成を各地域にて継続させるために、実証で得られた知見が具体例としてまとめられておりヒントを得ることが出来る。

4-2 家庭で出来ること

2020 年の必修化はすぐそこまで迫ってきている。不安を煽る訳ではないが、プログラミングを始める良い機会であり、早く始めるに越したことはない。ただ、これまでに述べたようにプログラミング言語を学び、コーディングをすることが目的ではないことを念頭に、まずは軽い気持ちでパソコンに触れることから始めるのが良いだろう。スマホやタブレットではなくパソコンである。コーディングをすることが目的ではないものの、ステップアップしていく上でより高度なことを行うにはやはりパソコンでないと支障をきたす場面が出てくるはずだ。さらに、可能であれば子供専用のパソコンを与えることが理想だと考える。所有することの喜びや、物を大切にすることも学び、何よりも自発的学習に目覚めることが期待出来るのではないだろうか。

総務省による情報通信端末の世帯保有率調査[25]では、スマホやタブレットの世帯保有率が年々増加しているが、パソコンは逆に減少をしている。（図 13）プログラミング教育の必修化に伴い、パソコンが見直され、家庭での普及が上昇に転じるかもしれない。



	2007 (n=3,640)	2008 (n=4,515)	2009 (n=4,547)	2010 (n=22,271)	2011 (n=16,530)	2012 (n=20,418)	2013 (n=15,599)	2014 (n=16,529)	2015 (n=14,765)	2016(年) (n=17,040)
固定電話	90.7	90.9	91.2	85.8	83.8	79.3	79.1	75.7	75.6	72.2
FAX	56.4	53.5	57.1	43.8	45.0	41.5	46.4	41.8	42.0	38.1
モバイル端末全体	95.0	95.6	96.3	93.2	94.5	94.5	94.6	94.6	95.8	94.7
スマートフォン	–	–	–	9.7	29.3	49.5	62.6	64.2	72.0	71.8
パソコン	85.0	85.9	87.2	83.4	77.4	75.8	81.7	78.0	76.8	73.6
タブレット型端末	–	–	–	7.2	8.5	15.3	21.9	26.3	33.3	34.4
ウェアラブル端末	–	–	–	–	–	–	–	0.5	0.9	1.1
インターネットに接続できる据置用テレビゲーム機	15.2	20.8	25.9	23.3	24.5	29.6	38.3	33.0	33.7	31.4
インターネットに接続できる携帯型音楽プレイヤー	19.1	22.0	27.3	17.0	20.1	21.4	23.8	18.4	17.3	15.3
その他インターネットに接続できる家電（携帯電話）等	4.3	5.5	7.8	3.5	6.2	12.7	8.8	7.6	8.1	9.0

＜図 13＞情報通信端末の世帯保有率の推移

筆者の今回の取り組みで気付いたことの一つは、子供が例年になく自由研究を楽しんでいたことである。プログラミングは楽しいと感じてくれたことが、IT の仕事をする筆者にとって一番の収穫であったかもしれない。冒頭で、ヒントは与えるが無用な口出しはしないと述べた。言い換えると、「一緒になって考える」ことをし、「教えない」ことを実践したまでである。子供のやる気が起こるのは、やること自体が楽しくなければならず、自らやったことの成果が見え、それを認めてもらえることが必要ではないだろうか。ぜひ親も一緒に楽しみ、成果を出すために取り組み、笑顔にさせてあげてほしい。

そして何はともあれ、子供のやる気と取り組みを支えるためには環境を整えることが必要だ。学校、習い事、家庭、いずれも大人・親の役目である。子供は勝手に学び、勝手に成長していくことを筆者は肌で感じたが、その過程を大人・親が止めることのないようにしていかなければならない。

おわりに

これから 2020 年の必修化に向けてハード・ソフトの環境整備は徐々に整っていくものと思われる。小学生の子供を持つ親たちは、世間の動向にはアンテナを張って乗り遅れないようにしていかなければならない。ただし、あまり気負う必要はなく、とりあえず何かやり始めてみることだ。遅すぎることはない。そして、プログラミング教育は将来プログラマを目指すための英才教育ではないが、積極性・習熟度によって、より高度なものへと発展し導いてあげることも必要になる。筆者も含め、IT 技術者は自身を活かせることに気づき、スマホアプリや電子工作、ロボット、AI など、得意分野で知識を提供し、社会への貢献を果たしていく義務があろう。高度情報通信社会の主役となっていく子供たちのために、プログラミング教育のこれからの成熟を目指し、官民協力のもと環境を整備していくことが急務である。そのための努力を惜しんではならない。

著者紹介

宮下　修（CITP 認定番号：16006339）
株式会社中電シーティーアイ
顧客のシステム提案、開発、構築のプロジェクト管理に従事。現在は主に大規模なストレージシステムの構築案件を担当。
高度情報処理技術者（プロジェクトマネージャ、セキュリティ、ネットワーク）、PMP。

参考文献

[1] Scratch, https://scratch.mit.edu/（参照 2018.02.10）
[2] 株式会社オークローンマーケティング, 【子どもの夏休みの宿題に関する調査結果】,
http://www.oaklawn.co.jp/news/20170724post-62.html（参照 2018.02.10）
[3] NHK E テレ, Why!?プログラミング
[4] 文部科学省, 新学習指導要領（平成 29 年 3 月公示）,
http://www.mext.go.jp/a_menu/shotou/new-cs/1383986.htm（参照 2018.02.10）
[5]文部科学省, 小学校段階における論理的思考力や創造性、問題解決能力等の育成とプログラミング教育に関する有識者会議,
http://www.mext.go.jp/b_menu/shingi/chousa/shotou/122/index.htm（参照 2018.02.10）
[6]文部科学省, 小学校段階におけるプログラミング教育の在り方について（議論の取りまとめ）,
http://www.mext.go.jp/b_menu/shingi/chousa/shotou/122/attach/1372525.htm（参照 2018.02.10）
[7]文部科学省, 幼稚園、小学校、中学校、高等学校及び特別支援学校の学習指導要領等の改善及び必要な方策等について（答申）（中教審第 197 号）,
http://www.mext.go.jp/b_menu/shingi/chukyo/chukyo0/toushin/__icsFiles/afieldfile/2017/01/10/1380902_0.pdf（参照 2018.02.10）
[8]文部科学書, 小学校学習指導要領解説 総則編,
http://www.mext.go.jp/component/a_menu/education/micro_detail/__icsFiles/afieldfile/2017/07/12/1387017_1_1.pdf（参照 2018.02.10）
[9]Computing At School, CAS computational thinking - A Guide for teachers,
https://community.computingatschool.org.uk/resources/2324/single（参照 2018.02.10）
[10]Computing At School, CAS Computing Progression Pathways KS1 (Y1) to KS3 (Y9) by topic,
http://community.computingatschool.org.uk/resources/1692/single（参照 2018.02.10）
[11]Wikipedia, STEM 教育,
https://ja.wikipedia.org/wiki/STEM%E6%95%99%E8%82%B2（参照 2018.02.10）
[12]首相官邸, 世界最先端 IT 国家創造宣言・官民データ活用推進基本計画について（平成 29 年 5 月 30 日閣議決定）,
https://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20170530/siryou1.pdf（参照 2018.02.10）
[13]首相官邸, 「プログラミング教育」の実施状況に関する現状調査　調査報告書（詳細版）,
https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/pdf/chosashosai.pdf（参照 2018.02.10）
[14]総務省, プログラミング人材育成の在り方に関する調査研究　報告書,
http://www.soumu.go.jp/main_content/000361430.pdf（参照 2018.02.10）
[15]久野 靖・苅宿 俊文・石戸 奈々子・原田 康徳・渡辺 勇士・阿部 和広・宮田 義郎・竹林 暁・本多 展幸・石原 淳也・伊藤 一成（分担執筆者順）(2017) 特集 情報教育とワークショップ, 情報処理 Vol.58, No.10, pp.882-912.
[16]総務省, 若年層に対するプログラミング教育の普及推進に向けた調査研究 報告書,
http://www.soumu.go.jp/main_content/000532006.pdf（参照 2018.02.10）
[17]Wikipedia, MSX, https://ja.wikipedia.org/wiki/MSX（参照 2018.02.10）
[18]Wikipedia, ファミリーベーシック,
https://ja.wikipedia.org/wiki/%E3%83%95%E3%82%A1%E3%83%9F%E3%83%AA%E3%83%BC%E3%83%99%E3%83%BC%E3%82%B7%E3%83%83%E3%82%AF（参照 2018.02.10）
[19]文部科学省, 平成 28 年度学校における教育の情報化の実態等に関する調査結果,
http://www.mext.go.jp/component/a_menu/education/micro_detail/__icsFiles/afieldfile/2018/02/20/1399330_01_1.pdf（参照 2018.02.25）
[20]文部科学省, 第 2 期教育振興基本計画（平成 25 年 6 月 14 日閣議決定）,
http://www.mext.go.jp/a_menu/keikaku/detail/__icsFiles/afieldfile/2013/06/14/1336379_02_1.pdf （ 参 照 2018.02.25）
[21]毎日新聞デジタル版, 小学校プログラミング 教師も未経験 必修化控え指導準備（2017 年 8 月 29 日）,
https://mainichi.jp/articles/20170829/k00/00e/040/186000c（参照 2018.02.25）
[22]株式会社明光ネットワークジャパン／明光義塾調べ, お子さまの放課後の過ごし方に関する実態調査,
http://www.meikonet.co.jp/news/detail/year/2017/id/622（参照 2018.02.25）
[23]文部科学省, 幼稚園、小学校、中学校、高等学校及び特別支援学校の学習指導要領等の改善及び必要な方策等について（答申）（中教審第 197 号）別紙,
http://www.mext.go.jp/component/b_menu/shingi/toushin/__icsFiles/afieldfile/2016/12/27/1380902_2.pdf（参照 2018.02.10）
[24]五十嵐 智生（2017）, 小学校段階におけるプログラミング教育と CITP との連携 ソフトウェアジャパン 2017 IT フォーラムセッション資料,
https://www.citp-forum.ipsj.or.jp/wp-content/uploads/2017/02/sj5.pdf（参照 2018.02.25）
[25]総務省, 平成 29 年版情報通信白書　情報通信端末の世帯保有率の推移,
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/html/nc262110.html（参照 2018.02.25）

ビットコインをきっかけに学ぶ暗号技術入門

赤根大吾[†1]

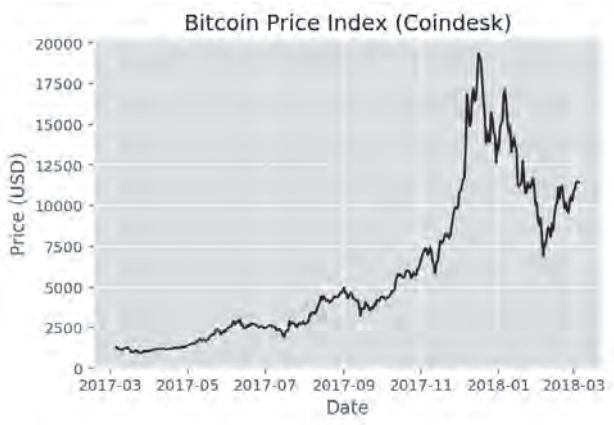
概要：ビットコインをはじめとする暗号通貨は、デジタル署名や一方向ハッシュ関数など、コンピュータを使った暗号技術によって支えられています。何かと話題の多い暗号通貨を題材にして、暗号技術を学んでみてはいかがでしょうか。基本的な近代暗号の用語から、ビットコインで使われている楕円曲線暗号、特に、秘密鍵から公開鍵を導くスカラー倍算について詳しく解説します。

キーワード：暗号通貨、暗号技術、ビットコイン、楕円曲線暗号、有限体、スカラー倍算、ECDSA、ECDH、公開鍵暗号、ブロックチェーン、ハッシュ関数

1. 暗号通貨の「暗号」とは

1.1 2017 年は暗号通貨元年？

2017 年はビットコインをはじめとする暗号通貨が大変話題になった一年でした。特に、日本円や米ドルなどの法定通貨（fiat currency）に対する価値の上昇はめざましく、年始には 1000 ドル程度だった 1BTC の価格は 12 月には一時 20000 ドル近くまで上昇しました。所有する暗号通貨の価格上昇により資産が億の単位になった「億り人」などのバズワードがニュースを賑わせ、改正資金決済法の施行や、暗号通貨の売買による収益を税法上どのように取り扱うかなど、法律面での整備も進みました。



1.2 「暗号通貨」か「仮想通貨」か

日本では「仮想通貨」という呼称が一般的ですが、英語圏では、「crypto currency＝暗号通貨」と呼ばれます。本稿でも「暗号通貨」を使いたいと思います。その方が、Suica など発行・管理を行う主体が存在する既存の「電子マネー」に対して、ビットコインをはじめとする非中央集権型の貨幣システムの新規性を区別しやすいと思うからです。

1.3 暗号通貨の技術を理解するメリット

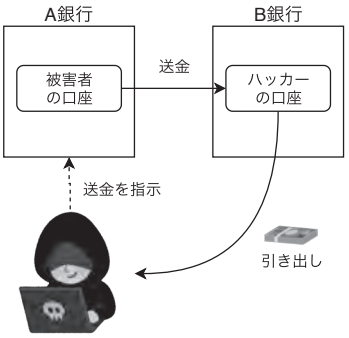
暗号通貨を所有する人が、そこで使われている技術を理解するのは当然のことでしょう。「Gox」やa、「セルフ Gox」bを防ぐため、正しい知識を身につけておく必要があります。また、暗号通貨に興味がない人でも、暗号通貨に使われている技術を学ぶ意味はあると考えます。暗号通貨は、コンピュータを用いた近代的な暗号技術に支えられており、その殆どは 2009 年の暗号通貨の登場以前から、毎日の暮らしの中で使われているものだからです。[1] 暗号通貨そのものが、今後どれだけ普及するかはわかりませんが、暗号通貨で使われている暗号技術そのものは、コンピュータにおける基礎知識なのです。

1.4 Coincheck 事件に学ぶブロックチェーン技術の概要

2018 年 1 月に Coincheck 社から 580 億円相当の NEM(XEM) cが流出するという事件がありました。このような暗号通貨の資金流出問題と、旧来のインターネットバンキングのハッキング被害との違いを見て見ましょう。インターネットバンキングのハッキングでは、大まかには以下の流れで被害が発生します。

1. ハッカーは、パスワードを不正に入手、またはマルウェアで振込の宛先を自分の口座に書き換えるなどして、自分の口座への送金指示する
2. 自分の口座から現金を引き出す

図 1: インターネットバンキングのハッキング被害



一方、暗号通貨では「口座」の代わりに「ウォレット＝財布」で資産を管理します。ウォレットには「アドレス」と、それに対応する「秘密鍵」が存在します。簡単に特徴を書

†1 (株)デジタルフィールド　東京都羽村市

a 取引所に預けた暗号通貨が消失することを、2014 年に発生した Mt.Gox 事件になぞらえ、「Gox する」と言われます。

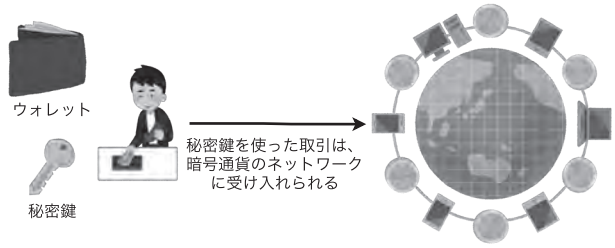
b 機器の故障や取り扱いの不備など、自分の過失によって暗号通貨を失うことを「セルフ Gox」と呼びます。

c NEM（ネム）の技術によって実現される代表的な暗号通貨とその単位を、XEM（ゼム）といいます。

き出すと以下のようになります。

- 「ウォレット」には「アドレス」と「秘密鍵」が存在する
- 「アドレス」と「秘密鍵」はペアである
- 「アドレス」は世界中に公開して良い
- 「秘密鍵」は絶対に公開してはいけない
- 「秘密鍵」を知っていれば、「アドレス」の残高を自由に使える

「秘密鍵」は「アドレス」を使った取引を通算した残高の正しい所有者の証明となり、「秘密鍵」を使った取引は世界に繋がった暗号通貨のネットワークに受け入れられます。



アーシュラ・K・ル＝グウィンの「ゲド戦記」には、対象を意のままに操ることができる「まことの名」が登場します。[2] これを喩えに使うのであれば、「通り名＝ハイタカ」が「アドレス」、知られてはいけない「まことの名＝ゲド」が「秘密鍵」に対応します。

Coincheck の場合、今回の事件で引き出された XEM のアドレスは、

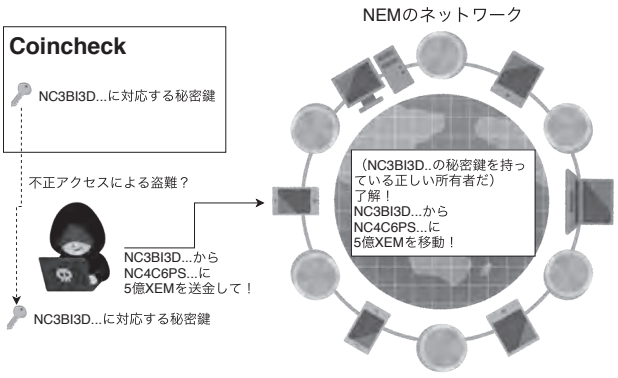
NC3BI3DNMR2PGEOOMP2NKXQ
GSAKMS7GYRKVA5CSZ

であるとわかっています。一方、秘密鍵は、私たちが知ることはできません。本来 Coincheck だけが知っているはずですが、流出がハッカーの仕業だとすると、ハッカーが何かしらの手段で秘密鍵を入手したことになります。

また、送金先のアドレスは

NC4C6PSUW5CLTDT5SXAGJDQJ
GZNESKFK5MCN77OG

でした。



ハッカーは「NC3BI3D...」の秘密鍵を用いて、「正しい」所有者として、「NC3BI3D...」から「NC4C6PS...」へ約 5 億 XEM の送金を行ったことになります。暗号通貨の世界では、秘密鍵の持ち主はアドレスの所有者の証明なので、この取引は正常に完了します。また、この取引は世界中に分散した NEM のネットワークを構成するコンピュータ群に記録されるため、取り消すことはできません。

さて、ここでこのような疑問を持つ方はいないでしょうか。

「暗号通貨というけれど、どこに暗号が使われているのだろう。暗号って、何かを暗号化して誰かから読めなくするように、秘密を守るためにあるのではないの？」

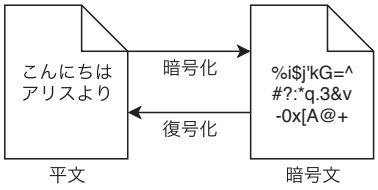
この疑問に答えるためには、少しコンピュータで使う暗号技術についての説明が必要です。

2. コンピュータで使う暗号技術

このセクションでは、コンピュータで使う暗号技術を代表して、「共通鍵暗号」「公開鍵暗号」「一方向ハッシュ関数」「デジタル署名」の 4 つを解説します。ただし、その技術をどのように実現しているか、深くは扱いません。興味のある方は「暗号技術入門」[3]「暗号がわかる本」[4]、「現代暗号入門」[5]などを参考にしてください。

2.1 秘密を守る暗号技術

暗号といえば、秘密を守るためにあります。メールの添付ファイルを zip ファイルで圧縮する際に暗号化する、というのが一番身近な例でしょうか。ここで、用語を定義します。**暗号化**されていない素のドキュメントを**平文**（ひらぶん）、暗号化したドキュメントを**暗号文**と言います。また、暗号文を平文に戻すことを**復号化**と言います。



2.1.1 共通鍵暗号

共通鍵暗号は、「暗号化するための鍵」と、「復号化する（＝暗号を解く）ための鍵」が同じ暗号です。

zip ファイルを暗号化してメールに添付する場合、暗号化する時のパスワードと、復号化するためのパスワードは同じですが、このパスワードが「共通鍵」となります。

共通鍵暗号として、最もよく使われている方式として AES (Advanced Encyption Standard) があります。無線 LAN の設定などで目にしたことがある人も多いのではないでし

ょうか。

図 2: 共通鍵暗号でメッセージを送信

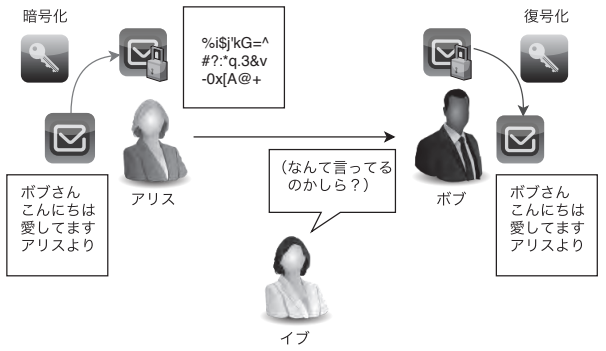


図 2 では、アリスが共通鍵暗号を用いてボブにメッセージを送信しています。イブが盗聴していますが、メッセージは暗号化されているのでイブには内容が理解できません。

2.1.2 鍵配送問題

これでアリスの秘密は守られました。めでたしめでたし…、とはなりません。共通鍵暗号には「鍵配送問題」が付きまといます。

図 3: 鍵配送問題

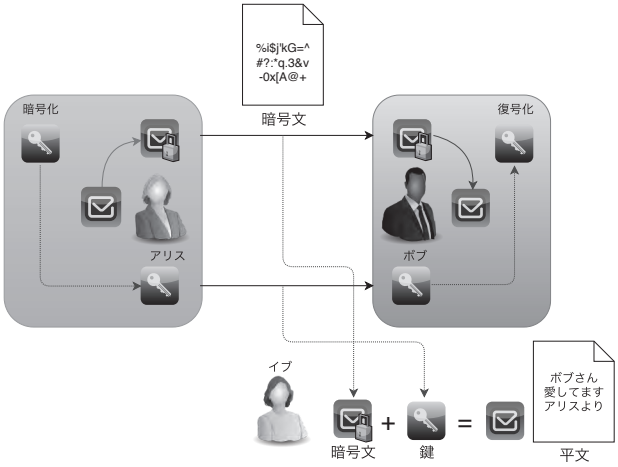


図 3 でボブは共通鍵を使って復号化していますが、アリスはボブにどのように鍵を渡せばよいでしょうか。イブが通信内容を盗聴できるのであれば、アリスからボブに鍵を送る時に、イブは鍵を入手できることになります。そして、暗号文もイブの手によって復号化されてしまいます。

日本のビジネスの現場では、パスワードで暗号化したメールを添付して、その前後のメールで鍵であるパスワードを送付するという慣習が見られますが、セキュリティ的にはあまり意味がないと言えるでしょう。d

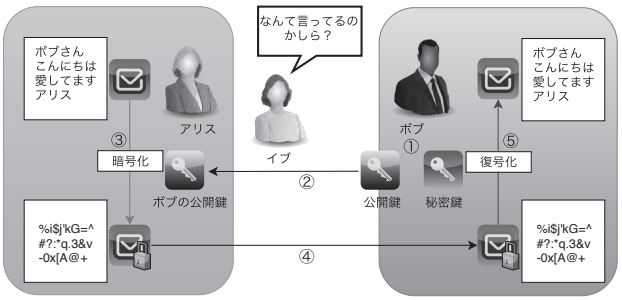
2.1.3 公開鍵暗号

鍵配送問題を解決する手段の一つとして、公開鍵暗号があります。先ほどの共通鍵暗号では一つの鍵を暗号化と復号化で使いましたが、公開鍵暗号では「公開鍵」と「秘密鍵」の 2 つが登場します。

- ペアとなる「公開鍵」と「秘密鍵」がある
- 「公開鍵」は持ち主以外に知られても良い
- 「秘密鍵」は持ち主以外に知られてはいけない
- 「公開鍵」を使って暗号化する
- 「秘密鍵」を使って復号化する

公開鍵暗号を使ってアリスがボブにメッセージを送る手順を示します。

図 4: 公開鍵暗号でメッセージを送信



1. ボブは自身の「公開鍵」と「秘密鍵」のペアを作成する
2. ボブはアリスに「公開鍵」を送付する
3. アリスは「ボブの秘密鍵」を使ってメッセージ（平文）を暗号化する
4. アリスは暗号化したメッセージ（暗号文）をボブに送付する
5. ボブは受け取った暗号文を、「ボブの秘密鍵」で復号化し、平文のメッセージを得る

盗み見しているイブは「ボブの公開鍵」と「暗号化されたメッセージ」を入手できますが、メッセージを復号化するのに必要な「秘密鍵」はないので、メッセージの内容を知ることはできません。

公開鍵暗号方式として、RSA、ElGamal、楕円 ElGamal などが挙げられます。PGP（GPG）や S/MIME など、公開鍵暗号方式を使ってメールや添付ファイルを暗号化する手段も提供されています。

2.2 ごまかしを防ぐ暗号技術

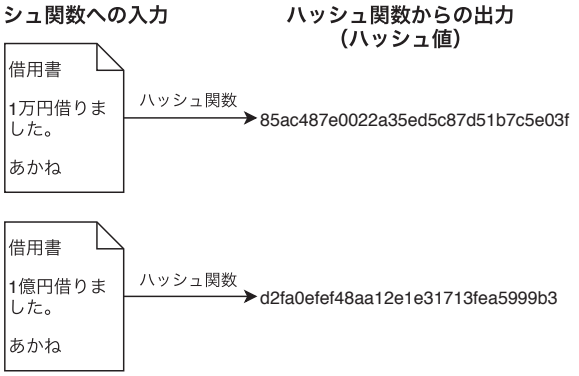
ここまでは秘密を守るための暗号技術を見てきましたが、少し違う目的のための暗号技術を紹介します。一言でいう

d　パスワードは暗号文とは別の手段で受け渡しを行うことが推奨されます。内閣官房情報セキュリティセンターの「庁舎内におけるクライアント PC 利用手順」では「保護に用いたパスワードについては、あらかじめ受信者と合意した文字列を用いるかあるいは、電子メールで送信せずに電話などの別手段を用いて伝達すること」とあります。

と、「ごまかし」を防ぐために暗号技術を使う方法です。

2.2.1 一方向ハッシュ関数

一方向ハッシュ関数は、入力された内容に応じて、決められたルールに従った出力を返す関数で、内容に変更があったかを判断するために使われます。ハッシュ関数の出力を「ハッシュ値」とも呼びます。次の例は、MD5 という一方向ハッシュ関数に、2 つのテキストファイルを入力し、その出力結果を比較したものです。



上の文書では「一万円」となっている箇所が、下の文書では「一億円」となっています。ただの 1 文字しか違いがないのに、ハッシュ値は大きく異なります。

この例では、内容が簡単だったため、目視でも違いがわかりました。これが 1 万文字を超えるような契約書が 2 部あり、その 2 部に違いがあるか、急いで確認しないといけない場合を想像すると、ありがたみがわかるでしょう。それぞれのデータを一方向ハッシュ関数に入力し、同じハッシュ値が出力されたら、内容は同じだと判断できます。

重要なことをまとめると：

- ハッシュ関数は入力が同じであれば同じハッシュ値を返す
- ほんの少しでも異なる入力であれば、（例外が無視できる確率で）異なるハッシュ値を返す

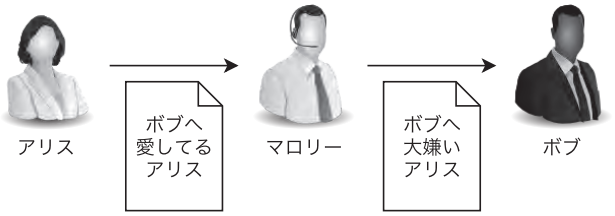
ハッシュ関数は、ビットコインのマイニング[e]にも使われています。簡単にいうと、「それまでの取引の履歴」＋「ランダムな文字」をハッシュ関数の入力として、あるルールを満たすハッシュ値が得られた場合にマイニングの成功となり、ブロックチェーンに新しいブロックが追加され、マイナー[f]に報酬が支払われます。

ビットコインでは SHA256 というハッシュ関数が使われています。

2.2.2 デジタル署名

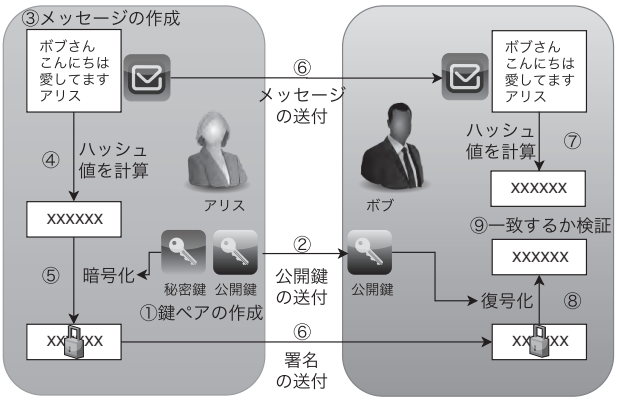
デジタル署名は、メッセージの内容が改ざんされていないと保証するための手段です。「公開鍵暗号技術」と「ハッシュ関数」を使います。

デジタル署名の必要性を認識するために、メッセージの内容を盗み見するだけだったイブではなく、メッセージの内容を改ざんできるマロリーに登場してもらいましょう。アリスはボブに「愛してる」というメッセージを送ったのに、マロリーが「大嫌い」と書き換えてしまいました。



デジタル署名を使えば、このような状況でも、受け取ったメッセージが、本当にアリスが書いたものかどうかを判断できます。デジタル署名にもいくつかの方法が存在しますが、ここでは RSA をデジタル署名に使った場合の手順を紹介します。先ほど、公開鍵暗号によるメッセージ送付の例では「公開鍵」で暗号化したメッセージを「秘密鍵」で復号化しました。RSA は「秘密鍵」で暗号化したものを「公開鍵」で復号化するという逆の使い方も可能で、その特性を署名に利用しています。

図 5: RSA を用いたデジタル署名



1. アリスは自身の「公開鍵」と「秘密鍵」を作成する
2. アリスは「公開鍵」をボブに送付する（この公開鍵の受け渡しは確実に行えたと仮定する）
3. アリスはボブ宛てのメッセージを作成する
4. 作成したメッセージのハッシュ値を計算する
5. 作成したハッシュ値を、アリスの秘密鍵で暗号化する。これを「デジタル署名」という
6. アリスは、「メッセージ」と「デジタル署名」をボブに送付する
7. ボブは受け取ったメッセージからハッシュ値を計算する
8. ボブは受け取ったデジタル署名を「アリスの公開鍵」で復号化する
9. ボブは「メッセージから計算したハッシュ値」と「デ

e ビットコインの取引を分散台帳（ブロックチェーン）に記録する作業です。マイニングに成功すると報酬として、一定量の新規発行されるビットコインと、送金者がトランザクションに含めた手数料を入手できます。

f マイニングを行う人のことです。

ジタル署名を復号化して得られたハッシュ値」とを比較する。一致した場合は、メッセージは改ざんされていない、一致しない場合は、メッセージが改ざんされた、と判断する

公開鍵暗号で暗号化したときと同様、秘密鍵は持ち主以外に知られてはいけません。アリスの公開鍵で復号化できるデジタル署名を作成できるのは、公開鍵に対応する秘密鍵を持ったアリスだけなので、9 の「ハッシュ値」の比較が一致するのであれば、アリスがメッセージを作成した時点から、メッセージは全く同じ内容であると言えます。

デジタル署名によって、秘密鍵の持ち主は、メッセージの内容に責任を持つことができます。逆にメッセージの内容が誰かによって改ざんされたものだと言い逃れはできません。

2.2.3 ハッシュ値だけでは、何故ダメか

メッセージを改ざんされたことはハッシュ値を比較すればわかるのだから、メッセージとハッシュ値を常にセットで送付すれば、ボブは改ざんに気づけるのでは？と考えるかもしれません。しかし、それではダメなのです。アリスやボブがハッシュ値を計算できるのと同様に、マロリーもハッシュ値を計算できるため、マロリーが「改ざんしたメッセージ」と「改ざんしたメッセージから計算したハッシュ値」を一緒に渡せば、ボブは改ざんに気づけません。

2.2.4 ECDSA による署名の作成と検証のデモ

ビットコインでも使われている ECDSA (Elliptic Curve Digital Signature Algorithm)というデジタル署名のアルゴリズムがあります。Elliptic Curve というのは「楕円曲線」という意味です。この ECDSA を使って、ボブに届いたメッセージが、アリスから送られたものかを確かめる手順を、Python のプログラムで示します。なお、本稿で使用するプログラムは Jupyter notebook 形式で github に公開しています。

https://github.com/dgakane/citp-report2017/

```
from ecdsa import SigningKey, VerifyingKey,¥
    SECP256k1, BadSignatureError
sk = SigningKey.generate(curve=SECP256k1)
```

アリスは作成した秘密鍵を使って、メッセージに署名をします。

```
msg_alice="""ボブへ
愛してる
アリス"""
vk = sk.get_verifying_key()
signature = sk.sign(msg_alice.encode())
```

ここで、sk が秘密鍵、vk が公開鍵、signature が署名となります。ボブのところに、アリス名義の、全く逆の内容のメッセージが 2 通届いたとします。このうちのどちらをアリスが書いたものか（署名したものか)、公開鍵（vk）と署名（signature）で検証します。

```
msg_mallory="""ボブへ
大嫌い
アリス"""

# マロリーのメッセージを検証
print("===========")
print(msg_mallory)
print("===========")
try:
    vk.verify(signature, msg_mallory.encode())
except BadSignatureError:
    print("↑アリスが署名したものではない")
else:
    print("↑アリスが署名したもの")

# アリスのメッセージを検証
print("===========")
print(msg_alice)
print("===========")
try:
    vk.verify(signature, msg_alice.encode())
except BadSignatureError:
    print("↑アリスが署名したものではない")
else:
    print("↑アリスが署名したもの")
```

このプログラムの実行結果は、以下のようになります。

```
===========
ボブへ
大嫌い
アリス
===========
↑アリスが署名したものではない
===========
ボブへ
愛してる
アリス
===========
↑アリスが署名したもの
```

どうやら、どちらがアリスが書いたメッセージなのか、判別できたようです。

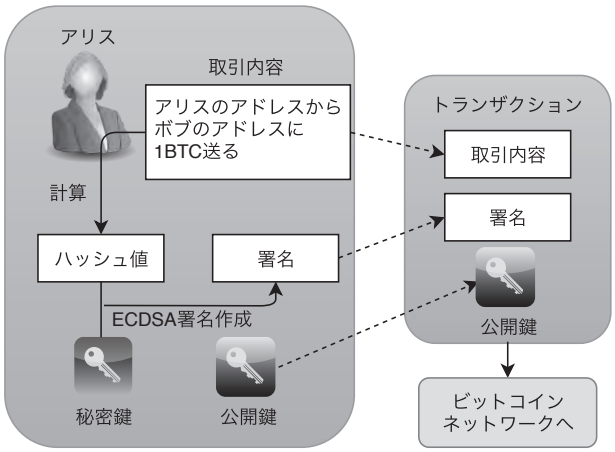
2.3 ビットコインのトランザクション（取引）の仕組み

アリスがボブにビットコインを使って送金するという例で、これまで紹介した暗号技術が暗号通貨にどのように使われているかを見てみましょう。

1. アリスは「アリスからボブに 1BTC を送金」という取引内容のハッシュ値を計算する

2. 「ハッシュ値」と「アリスの秘密鍵」を用いて、ECDSA で署名を作成
3. 「取引内容」＋「署名」＋「公開鍵」からなるトランザクションを作成。ビットコインネットワークに送信する

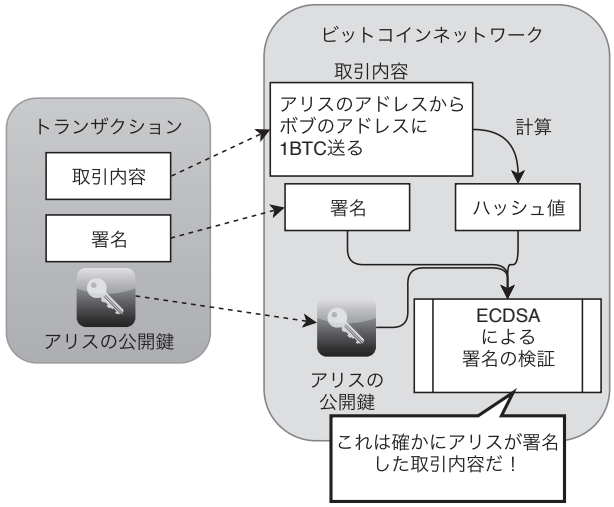
図 6: トランザクションの作成



アリスからのトランザクションを受け取ったビットコインネットワークでは、トランザクションが本当にアリスから送信されたものかを検証します。

1. トランザクションに含まれる「取引内容」から、「ハッシュ値」を計算する
2. 計算した「ハッシュ値」と、トランザクションに含まれる「署名」「アリスの公開鍵」を ECDSA に従い検証する

図 7: トランザクションの検証

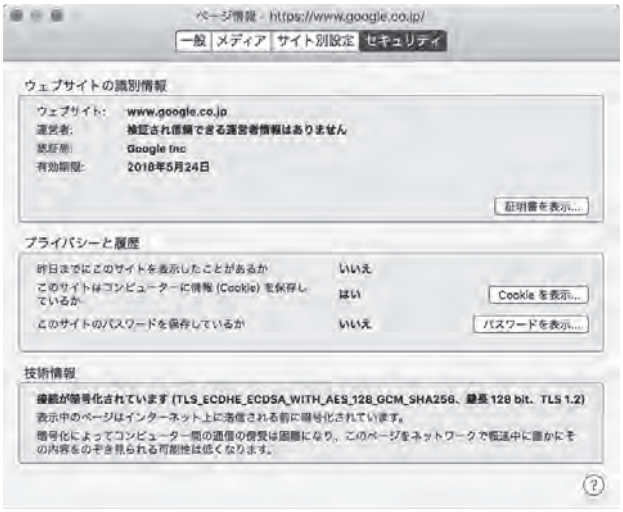


このように検証が完了したトランザクションは、ビットコインネットワークを構成する他のノード（コンピュータ）に伝播し、アリスから送信された正当な取引としてブロックチェーンに繰り込まれることになります。

ノードが検証している項目はもっと多岐に渡りますが、さらに詳しく知りたい方は「ビットコインとブロックチェーン 暗号通貨を支える技術」[6]を参照してください。

2.4 実は日常的に使っている暗号技術

ここまで見てきた暗号技術は、普段あまり意識しないのですが、実は日常的に使っているものです。下は、著者の Mac の Firefox で、Google にアクセスした際に、どのような暗号を使っているかを表示したダイアログです。



「 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256」という文字列が読み取れます。詳しい説明は省きますが、Web ブラウザと Web サーバとの通信の中で、いくつかの暗号技術を組み合わせて使っていることを示しています。

目的	方式
鍵交換に使っている方式は	ECDHE g
署名に使っている方式は	ECDSA
暗号化に使っている方式は	AES 128 GCM
メッセージ認証に使っている方式は	SHA256

共通鍵暗号で挙げた AES、ビットコインも使っている署名のアルゴリズム ECDSA やハッシュ関数 SHA256 が使われていることがわかります。

日常的に使われている暗号技術と、ビットコインなどの暗号通貨が繋がっていることが、おわかりいただけたでしょうか。

3. 楕円曲線暗号入門

さて、ここまで登場してきた「アドレス」「公開鍵」「秘密鍵」「ECDSA」などをより深く理解するためには、楕円曲線暗号について解説が必要です。正確には有限体上で定義された楕円曲線暗号といい、数学的な内容も出てきますが、プログラムによるスニペットとグラフによる可視化で、できるだけイメージしやすい説明に挑戦します。

g ECDHE に関しては、セクション 3 の最後にアルゴリズムを紹介します。

3.1 ビットコインで使われる楕円曲線

3.1.1 「アドレス」「公開鍵」「秘密鍵」の関係

「アドレス」「公開鍵」「秘密鍵」が具体的にどのようなものか例を見てみましょう。

ビットコインの**アドレス**は、以下のように 1 で始まる文字列です。

12noHBPojYCYtEPaXGeLAY8ExyXJRC7uq8

公開鍵は（あとで説明しますが）平面上の点なので、x 座標と y 座標を表す 2 つの値で構成されます。[h]

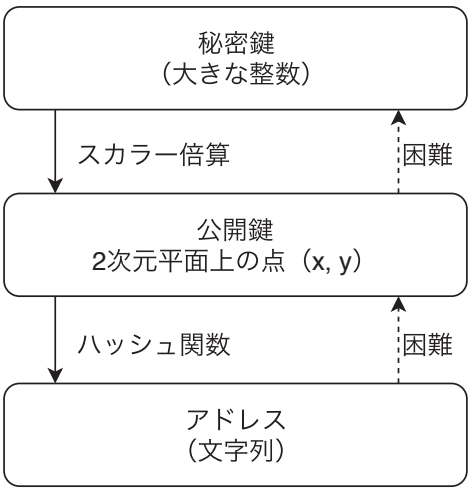
(x, y)=
(59657349624863415277140746483024327429760811273444096062005870676035102190933,
57361002836192819049676076242901405112088254166527378116283440525442954582659)

秘密鍵は一つの値で、大きな整数です。

57625604009098861386593689532106037116306023484397133537612206883757739966481

公開鍵は、秘密鍵から「スカラー倍算」という計算で作られます。逆に、公開鍵から秘密鍵を求めることは困難です。

アドレスは、公開鍵から「ハッシュ関数」で作られます。アドレスから公開鍵を求めることは困難です。図にまとめます。



ハッシュ関数は、先ほどのセクションで紹介したものです。そして、新たに「スカラー倍算」というものが出てきました。**このセクションは、「スカラー倍算」の説明をゴールとします**。

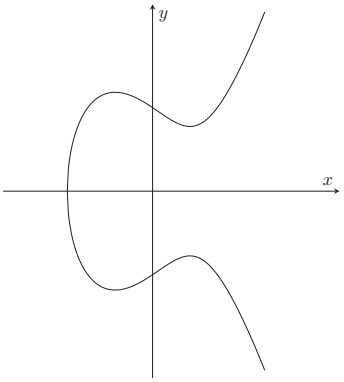
3.2 実数平面上の楕円曲線

楕円曲線は以下のような方程式で与えられます

$$y^2 = x^3 + ax + b$$

グラフで描画すると以下のようになります。

図 8: 楕円曲線



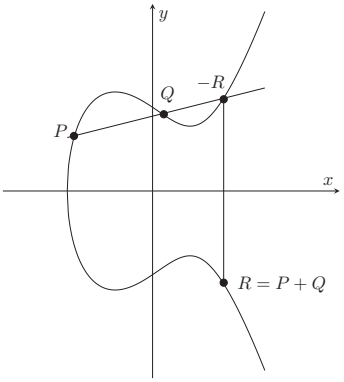
3.2.1 楕円曲線上の点の加法（実数バージョン）

この楕円曲線上で、以下のように点と点の加法（足し算）を定義します。

楕円曲線E上の 2 点の和$P+Q=R$を以下のように定義する:

- PとQを通る直線が、再びEと交差する点を$-R$
- $-R$と x 軸に関して対称な点をRとする

図 9: 楕円曲線上の加法（$P \neq Q$の場合）



この定義に従い、具体的な座標の計算も可能です。

$P=(x_P, y_P)$、$Q=(x_Q, y_Q)$、$R=(x_R, y_R)$と書くとき、

$$x_R = \lambda^2 - x_P - x_Q$$

$$y_R = \lambda(x_P - x_R) - y_P$$

ここでλは、点P, Qを通る直線の傾きで、

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}$$

とする。

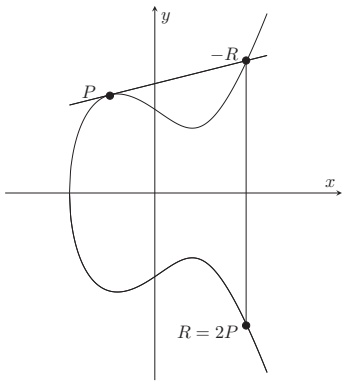
PとQがどんどん近づいて、一つの点となった場合（$P=Q$）は、楕円曲線上の点の 2 倍と考えることができます。

楕円曲線E上の点Pの 2 倍$P+P=2P=R$を以下のように定義する:

- EのPにおける接線が、再びEと交差する点を$-R$
- $-R$と x 軸に関して対称な点をRとする

h ビットコインの公開鍵は、02 または 03 から始まる「圧縮された形式」の文字列で表現されることもあります。どちらにしても、平面上の点であることに変わりはありません。

図 10: 楕円曲線上の加法（$P = Q$の場合）



この場合も、以下のように座標を求めることができます

$P = (x_P, y_P)$、$R = (x_R, y_R)$と書くとき、

$$x_R = \lambda^2 - 2x_P$$

$$y_R = \lambda(x_P - x_R) - y_P$$

ここでλは、点P, Qを通る直線の傾きで、

$$\lambda = \frac{3x^2 + a}{2y}$$

とする。

3.3 コンピュータで楕円曲線を扱う

ここまで楕円曲線を我々にとって普通の数＝実数上で考えてきました。グラフに書いたり、慣れ親しんだ方法で座標を計算したりできるのでイメージしやすいのですが、実際にコンピュータで楕円曲線を扱う場合と大きな乖離があります。実数には、無限に大きな数が存在したり、どれだけ小さな数と数との間にも無限の数が存在するといった特徴があり、有限の桁数（ビット）しか持たないコンピュータには扱いづらいのです。コンピュータでは実数上ではなく、有限体（ゆうげんたい）上で定義された楕円曲線を使います。

3.3.1 体（Field）とは？

体（たい）とは、四則演算（足し算、引き算、かけ算、割り算）が行える集合です。その集合の要素を使って四則演算を行えば、演算の結果もまたその集合に含まれます。この性質を「四則演算で閉じている」と言います。例えば、実数の集合ℝは体となります。「実数」同士で四則演算を行った結果は必ず「実数」になるからです。

$1 + 2 = 3 \cdots 3$ は実数

$1 - 2 = -1 \cdots -1$ は実数

$1 \times 2 = 2 \cdots 2$ は実数

$1 \div 2 = 0.5 \cdots 0.5$ は実数

「四則演算が行えるなんて当たり前では？」と思うかもしれません。「四則演算が行えない」例としては、整数全体の集合ℤでは、その要素同士での割り算の結果が整数にならないことがあります。

$1 \div 2 = 0.5 \cdots 0.5$ は整数ではない

そのため、整数全体の集合ℤは体ではありません。

3.3.2 有限体（Finite Field）とは？

有限体は、有限の要素からなり、四則演算で閉じている集合です。要素の数が無限に存在するℝなどと異なり、コンピュータでの演算が容易です。口で言うのは簡単ですが、本当にそのような集合は存在するのでしょうか。pを素数として、0から$p-1$までの整数で構成される集合$\mathbb{F}_p = \{0,1,\cdots,p-1\}$に、私たちが普段使っているものとは、少し違った四則演算を定義して、有限体とすることができます。pが小さい場合で例を作ってみます。$p = 5$の場合、つまり$\mathbb{F}_5$での四則演算を見ていきます。

3.3.3 有限体$\mathbb{F}_5$の足し算

基本的には普通の足し算と同じですが、計算の結果 5 を超えた場合は、その結果を 5 で割った余りを答えとします。$a + b$の結果を以下にまとめます。

a＼b	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Python の関数として書くと、このようになります。

```
def add(a, b): # F5 での足し算
    return (a + b) % 5
```

引き算は、このコード例で b がマイナスになった場合ですので、割愛します。

3.3.4 有限体$\mathbb{F}_5$のかけ算

かけ算も同様に、「普通のかけ算」の結果を 5 で割った余りとなります。

a＼b	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

```
def multiply(a, b): # F5 でのかけ算
    return (a * b) % 5
```

3.3.5 有限体$\mathbb{F}_5$の割り算

割り算に関しては、少し工夫が必要です。$1 \div 2$など、通常の割り算では結果が整数にならず、そのままでは計算結果が$\mathbb{F}_5$に含まれません。ここで少し割り算の意味を考えてみると、「割り算」は「かけて 1 になる数＝逆数」をかけていると言えます。例えば、「普通の」かけ算や割り算で考える

と 2 の逆数は$\frac{1}{2}$となります。$\mathbb{F}_5$の世界で「かけて 1 になる組み合わせ」をかけ算の表の中ではグレーの網かけで表しました。これによると、2 の逆数は 3 となります。なので、$\mathbb{F}_5$の世界では、$1 \div 2 = 1 \times 3 = 3$となります。かけ算の表で、かけたら 1 になる数を探しながら、割り算の表を作れます。

b

a ÷	0	1	2	3	4
0	-	0	0	0	0
1	-	1	3	2	4
2	-	2	1	4	3
3	-	3	4	1	2
4	-	4	2	3	1

しかし、いちいちかけ算の表を確認しないと割り算ができないのでしょうか。$p = 5$の場合なので、なんとかできますが、pの値が大きくなった場合には大変そうです。ここは数学の力を借りることにします。「ユークリッドの互除法」や「フェルマーの小定理」を利用して、「かけて 1 になる数＝逆数」を求めることができます。[7]

フェルマーの小定理より
任意の素数pと、0 ではない$n \in \mathbb{Z}_p$について

$$n^{p-1} = 1 \bmod p$$

が成り立つ。ここから

$$n^{p-2} = n^{-1} \bmod p$$

と変形でき、nの逆数「n^{-1}」は、「n^{p-2}のpの剰余」と等しい

次のコードでは、フェルマーの小定理を使って逆数を求めています。Python でべき乗を行う pow 関数は第 3 引数を受け取ることができ、pow(x, y, z)は x の y 乗に対する z の剰余を返します。

```
def inv(n, p): # 剰余 p の世界で逆数を求める関数
    return pow(n, p-2, p) # フェルマーの小定理より
def div(a, b): # F5 での割り算
    return (a * inv(b, 5)) % 5
```

このように、$\mathbb{F}_5$に（少し変わった）四則演算を定義することができました。一般に、pが素数の場合は、$\mathbb{F}_p$は有限体となり、素体とも言われます。

3.3.6 有限体$\mathbb{F}_p$上の楕円曲線

有限体$\mathbb{F}_p$での楕円曲線を以下のように定義します。

$y^2 \equiv x^3 + ax + b \pmod{p}$を満たす 2 次元平面$\mathbb{F}_p \times \mathbb{F}_p$上の点$(x, y)$

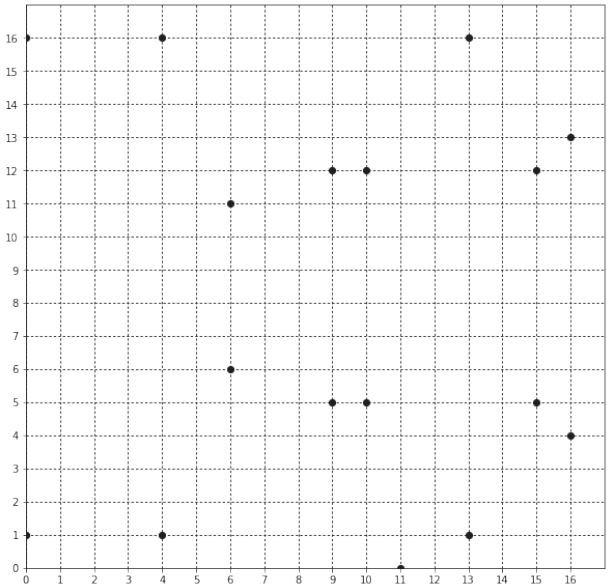
$s \equiv t \pmod{p}$と言うのは、「sをpで割った余りと、tをpで割った余りは等しい」という意味です。$0 \equiv t - s \pmod{p}$と変形すれば、「$t - s$をpで割った余りは0である」と読み替えられます。なので、有限体$\mathbb{F}_p$での楕円曲線は、「$x^3 + ax + b - y^2$をpで割った余りが0となるような(x, y)の集合」となります。式や文章だと分かりにくいですが、コードとグラフで確認すると意外と簡単です。$\mathbb{F}_{17}$上での$y^2 = x^3 + x + 1$をグラフにプロットする Python のプログラムを以下に示します。

```
def plot_ec(a, b, p):
    import matplotlib.pyplot as plt
    xlist = []
    ylist = []
    for x in range(p):
        for y in range(p):
            if((x**3 + a * x + b - y**2) % p == 0):
            # 方程式を満たす x,y の組をリストに格納
                xlist.append(x)
                ylist.append(y)
    #以下は表示のため
    plt.figure(figsize=(10,10))
    plt.axis([0,p,0,p])
    if(p < 55):
        point_style = 'o'
        plt.grid(which='major',linestyle=':'
                 , color="black")
        plt.yticks( [i for i in range(p)] )
        plt.xticks( [i for i in range(p)] )
    else:
        point_style = '.'
    plt.plot(xlist, ylist, point_style , color="black")
    plt.show()

plot_ec(1, 1, 17)
```

実行結果はこうなります。

図 11: $\mathbb{F}_{17}$上での楕円曲線$y^2 = x^3 + x + 1$

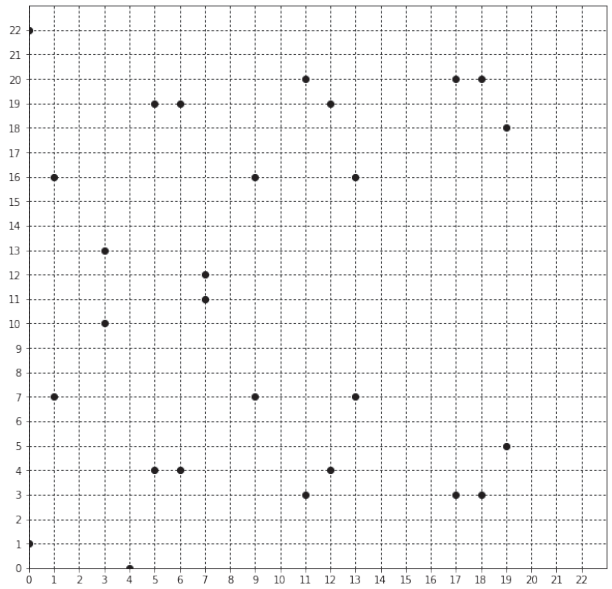


plot_ec の第 3 引数を変更することで、異なるpでの楕円曲

線をみることができます。pをもう少し大きくして見ましょう。$p = 23$の場合：

```
plot_ec(1, 1, 23)
```

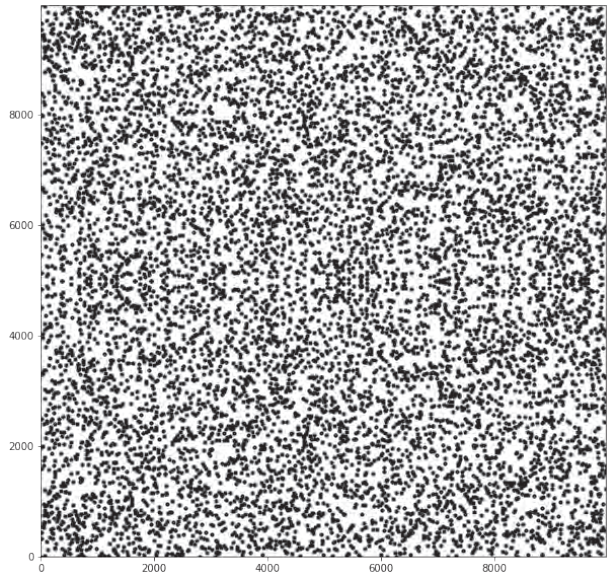
図 12: $\mathbb{F}_{23}$上での楕円曲線$y^2 = x^3 + x + 1$



$p = 9973$の場合：

```
plot_ec(1, 1, 9973)
```

図 13: $\mathbb{F}_{9973}$上での楕円曲線$y^2 = x^3 + x + 1$



いかがでしょうか。楕円曲線と言う割に、楕円でも曲線でもありません。よく観察すると以下のような特徴があります。

- とびとびの値を取っている
- $y = 0$上の点を除いて、$y = \frac{p}{2}$を挟んで線対称に点が分布している
- 対称な点同士は奇数と偶数に分かれている

3.3.7 楕円曲線の点の加法（有限体$\mathbb{F}_p$バージョン）

実数の時と同様に、楕円曲線上の点の加法を定義します。

$\mathbb{F}_p$上の楕円曲線$y^2 = x^3 + ax + b$上の点P, Qの和$R = P + Q$を以下のように定める:

$P = (x_P, y_P)$、$Q = (x_Q, y_Q)$、$R = (x_R, y_R)$と書くとき、

$$x_R = \lambda^2 - x_P - x_Q$$

$$y_R = \lambda(x_P - x_R) - y_P$$

ここでλは、

$$\begin{cases} P \neq Q \text{ の時: } \lambda = \dfrac{y_Q - y_P}{x_Q - x_P} \\ P = Q \text{の時: } \lambda = \dfrac{3x_P^2 + a}{2y} \end{cases}$$

とする。[i]

式自体は実数の時と同じですが、ここでの四則演算は全て$\mathbb{F}_p$における四則演算だということに注意が必要です。分数＝割り算は、普通の割り算ではなく、有限体における逆数のかけ算です。

3.3.8 具体的にやってみる

ここで具体的に、楕円曲線上の点の足し算を行なって見ます。$(x, y) = (0,1)$は$y^2 = x^3 + x + 1$上の点です。この点をGと名付けます。$\mathbb{F}_{23}$上で$(0,1) + (0,1) = G + G = 2G$を計算します。

$(0,1) + (0,1) = G + G = 2G$の計算：

まずλを計算する。

同じ点同士の足し算なので、「$P = Q$の時」に該当する。

$$\lambda = \frac{3x_P^2 + a}{2y} = \frac{3 \cdot 0^2 + 1}{2 \cdot 1} = \frac{1}{2} = 2^{-1} = 2^{23-2} \bmod 23 = 12$$

（逆数の計算にはフェルマーの小定理を利用した。）

$$x_R = \lambda^2 - x_P - x_Q = 12^2 - 0 - 0$$

23を超える計算結果は、23で割った余りなので、

$$= 144 \bmod 23 = 6$$

$$y_R = \lambda(x_P - x_R) - y_P = 12(0 - 6) - 1$$

$$= 12 \cdot 17 - 1$$

$$= 203 \, mod \, 23 = 19$$

$$\therefore 2G = (0,1) + (0,1) = (6,19)$$

これらの計算を ec_double という関数にまとめてプログラムにすると以下のようになります。

```
# F_p 上の y^2=x^3+ax+b での p, a, b
p, a, b = 23, 1, 1
G=(0,1)
def inv(n, p):
    return pow(n, p-2, p)
def ec_double(A):
    l = (((3 * A[0] **2) + a) * inv(2*A[1], p)) % p
    x = (l ** 2 - A[0] - A[0]) % p
    y = (l * (A[0] - x) - A[1]) % p
```

i 不完全な定義です。無限遠点に関する定義を省略しています。

```
    return x, y
G2=ec_double(G)
print(G2) # (6, 19)
```

このようにして計算してできた$2G = (6,19)$にもう一度Gを足して$3G$を作って見ましょう。今度は異なる点の足し算なので、ec_add という関数を作ります。

```
def ec_add(A, B):
    l = ((B[1] - A[1]) * inv(B[0] - A[0], p)) % p
    x = (l ** 2 - B[0] - A[0]) % p
    y = (l * (A[0] - x) - A[1]) % p
    return x, y
G3 = ec_add(G2, G)
print(G3) # (3, 13)
```

できた点に繰り返しGを足していくと、次から次へと楕円曲線上の点が現れます。自作の関数でも良いのですが、Python の ecdsa ライブラリを使って同じことをしてみます。すでに自作関数を使って計算した$2G$と$3G$の検算にもなります。

```
from ecdsa.ellipticcurve import CurveFp, Point
# F_p 上の y^2=x^3+ax+b の意味での p, a, b
p, a, b = 23, 1, 1
c = CurveFp(p,a,b)
# G を c 上の点(0,1)とする
G = Point(c, 0, 1)
current = G
for i in range(1,28):
    print("{}G:¥t{}".format(i,current))
    current = current + G
```

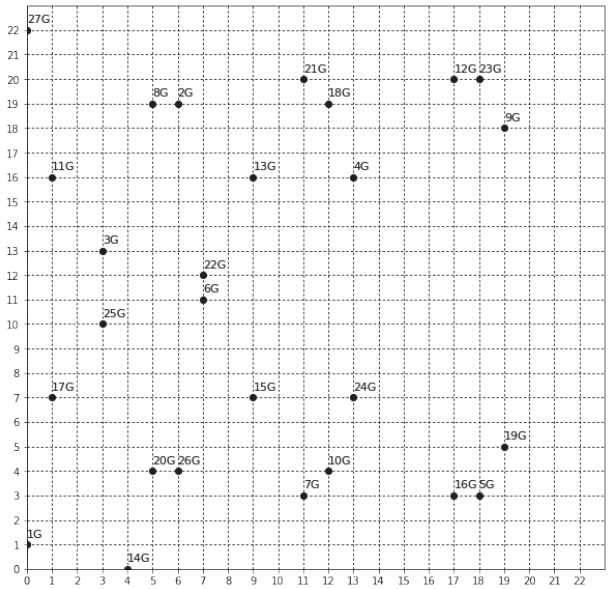
このプログラムの実行結果は以下のようになります。

表 1: Gを足し合わせた結果

```
1G:     (0,1)
2G:     (6,19)
3G:     (3,13)
   (略)
23G:    (18,20)
24G:    (13,7)
25G:    (3,10)
26G:    (6,4)
27G:    (0,22)
```

これを座標にプロットすると図 14 のようになります。図 12 と同じグラフが得られました。

図 14: $\mathbb{F}_{23}$上での楕円曲線$y^2 = x^3 + x + 1$



3.3.9 楕円曲線上の点のスカラー倍

このように点Gをd回足して得られる点を**スカラー倍点**といい、スカラー倍点を求める計算を**スカラー倍算**と言います。

スカラー倍算

$$dG = \underbrace{G + \cdots + G}_{d\text{個}}$$

dGの座標を具体的に求めるための方法として、定義通りに、GからスタートしてGを$d-1$回足していく素朴な方法があります。

スカラー倍算（素朴な方法）

$$dG = \underbrace{G + \cdots + G}_{d\text{個}}$$

$$= G + \underbrace{G + \cdots + G}_{d-1\text{ 個}}$$

$$= 2G + \underbrace{G + \cdots + G}_{d-2\text{ 個}}$$

$$\vdots$$

$$= (d-1)G + G$$

このように逐次計算を行うのではなく、もっと直接的に求めることはできないのでしょうか。

3.3.10 スカラー倍算の高速化（バイナリ法）

直接的、とは言えないかもしれませんが、もっと効率よく計算するアルゴリズムとして**バイナリ法**を紹介します。以下は、スカラー倍算を用いて楕円曲線上の点Pをd倍する手順です。

スカラー倍算（バイナリ法）

- スカラーdの２進数表現を$(1, d_{n-2}, \cdots, d_1, d_0)$とする
  例: d = 129の場合(1,0,0,0,0,0,0,1)
- 開始する点をPとする

1. $Q \leftarrow P$
2. $i = n-2, n-3, \cdots, 1,0$に対して以下を行う
   2-1: $Q \leftarrow 2 \times Q$
   2-2: $d_i = 1$ならば$Q \leftarrow Q + P$
3. Qを返す

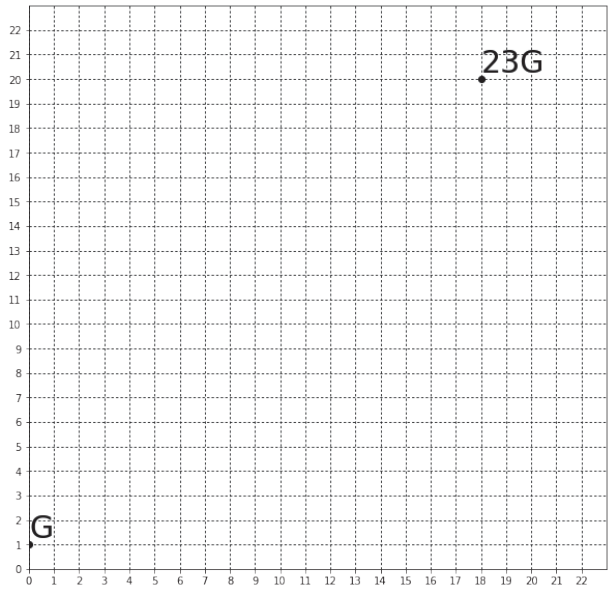
これはプログラムで見た方がわかりやすいかもしれません。ここで使っている関数 ec_double と ec_add は、3.3.8 で作成したものです。

```
def binary_method(P, d):
    Q = P
    bin_str = format(d, 'b') # d の二進数表現文字列
    for bit in bin_str[1:]:
        Q = ec_double(Q)
        if bit == "1": Q = ec_add(Q, P)
    return Q
```

この関数を使って$23G$を計算してみましょう。表 1 ならびに図 14 から、$23G$が(18,20)であることがわかっています。binary_method を使っても同じ結果が得られます。

```
G23 = binary_method(G,23)
print(G23) # (18, 20)
```

図 15: $23G$をいきなり求める



3.3.11 スカラー倍算に必要な計算量

スカラー倍算の方法として、順番に点を足し合わせていく「素朴な方法」と、効率的な「バイナリ法」を紹介しました。しかし、バイナリ法は本当に効率的なのでしょうか？この 2 つを比べると、どのくらい計算量に違いがあるのでしょうか。計算量を式として表してみます。

「素朴な方法」の計算量：

Gから$2G$を計算…ec_double を使用
$2G$から$3G$を計算…ec_add を使用
$3G$から$4G$を計算…ec_add を使用
：
$(d-1)G$からdGを計算…ec_add を使用

つまり、dG まで至るまでに、
ec_double を 1 回、ec_add を$(d-2)$回使う。
ec_double と ec_add の計算量が同程度とすると、

$$\textit{素朴な方法の計算量} = d - 1$$

バイナリ法は、dを二進数で表現した桁ごとに手順 2-1 と手順 2-2 を行なっています。また、ある数nを二進数で表した場合の桁数は約$\log_2 n$になることを利用します。

バイナリ法の計算量：

手順 2-1 の ec_double は必ず実行される

手順 2-2 の ec_add は$\frac{1}{2}$の確率で実行される

ec_double と ec_add の計算量が同程度とすると、
$\textit{バイナリ法の計算量} = (1 + 0.5) \times$「$d$の二進数での桁数」と書けます。ここで

$$d\text{の二進数での桁数} \cong \log_2 d$$

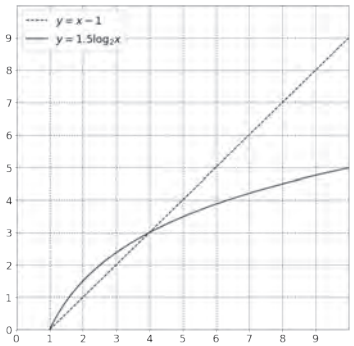
なので、

$$\textit{バイナリ法の計算量} \cong 1.5 \log_2 d$$

※≅は「おおよそ等しい」

$d-1$と$1.5\log_2 d$では、どちらが大きいのでしょうか？グラフを書いて確認します。最初のうちこそいい勝負に見えますが…

図 16: 計算量の比較（10 まで）



dが大きくなるに従って、徐々に差が大きくなって来ます。

図 17: 計算量の比較（100 まで）

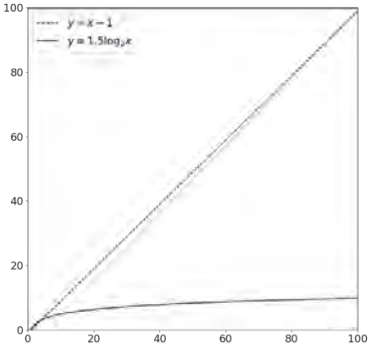
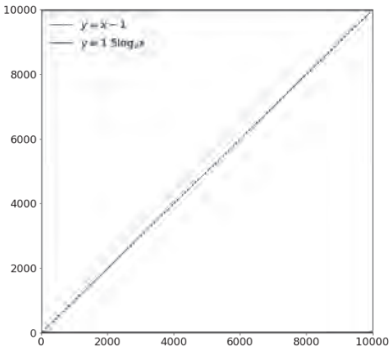


図 18: 計算量の比較（10000 まで）



「素朴な方法」での計算量は一定の割合で増加し続けるのに比べ、「バイナリ法」では増加の仕方が減っていき、dが十分に大きな数になると「素朴な方法」と比べて無視できる計算量であることがわかります。

3.4 楕円曲線暗号における「鍵」

実は、楕円曲線暗号における「秘密鍵」と「公開鍵」は、それぞれdと、dGになります。

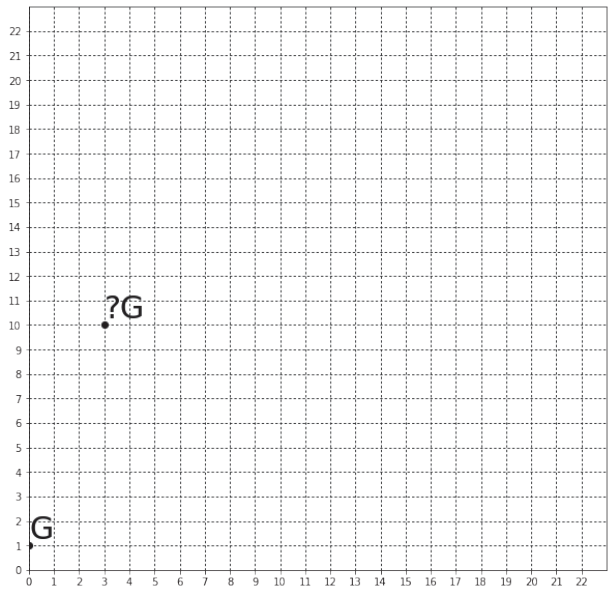
秘密鍵	公開鍵
d	dG

以下のような情報をあなたが知っていたとします。

知っている情報	例
有限体$\mathbb{F}_p$の標数p	$p = 23$
楕円曲線の方程式	$y^2 = x^3 + x + 1$
ベースポイントG	$G = (0,1)$
公開鍵dG	$dG = (3,10)$

さて、ここで$dG = (3,10)$はGを何回か（d回）足し合わせたものであることはわかっています。このとき、dの値がわかりますか？少し考えてみてください。

図 19: (3,10)はGを何倍したもの？



実は、私たちは$\mathbb{F}_{23}$上の$y^2 = x^3 + x + 1$の点を、図 14 で全て計算済みです。そのため、図を見比べることでdが 25 であることを知ることができます。ですが、それは点を一つずつ足していった「素朴な方法」で求めたものでした。$?G = (3,10)$となるような?を知るためには、Gを足してできる点を一つ一つ、しらみつぶしに試していくしかないのです。このように、

- 秘密鍵（$= d$）を知っていれば、公開鍵（ $= dG$）を計算するのは（計算量的に）容易
- 一方、秘密鍵を知らない攻撃者が公開鍵から秘密鍵を求めようとしても、総当たり、この場合は順番に試していくしか方法がない

という性質を、楕円曲線暗号は利用しています。スカラー倍算によって、秘密鍵から公開鍵を求めることはできるのに、公開鍵から秘密鍵を求めることはできないというのは、ここで挙げた計算量の違いによるものです。

3.5 楕円曲線上の点の位数

ところで、楕円曲線上の点Pを足し合わせていくと、いつかPとx座標が等しい点が出現します。これを$-P$とし、$-P$にさらにPを足した点を無限遠点$\mathcal{O}$と定義します。すると、楕円曲線上の点の足し算は以下の様に巡回します。

$$\underbrace{P \to 2P \to 3P \to \cdots \to -P \to \mathcal{O}}_{r\text{個}} \to P \to \cdots$$

この様に$rP = \mathcal{O}$となるような最小の自然数を「Pの点位数」と言います。楕円曲線暗号で使う場合、点位数rが素数となるようなベースポイントGを選びます。

ここまで見てきた、「有限体での四則演算」や「スカラー倍算」「点位数」がわかれば、楕円曲線を使った暗号方式（楕円曲線 ElGamal）や、署名（ECDSA）のアルゴリズムを自分で計算してみることが可能になります。これらのアルゴリズムについて、詳しくは「楕円曲線暗号入門」[8]や「暗号理論と楕円曲線」[9]などをご参照ください。

3.6 ビットコインに使われる楕円曲線のパラメータ

ビットコインは米国国立標準技術研究所（NIST）が策定した secp256k1 という楕円曲線と定数を使用しています。以下の情報は、誰でも知ることが可能な公開情報です。

有限体$\mathbb{F}_p$の標数p:

$$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$$

楕円曲線の方程式:

$$y^2 = x^3 + 7$$

スカラー倍のベースポイント:

$$G = (G_x, G_y)$$

G_x =55066263022277343669578718895168534326250603453777594175500187360389116729240

G_y =32670510020758816978083085130507043184471273380659243275938904335757337482424

ベースポイントGの点位数r:

r =115792089237316195423570985008687907852837564279074904382605163141518161494337

秘密鍵は、1 からrの範囲で、ランダムに選ばれます。このrは、10^{77}くらいの値です。「観測可能な宇宙に存在する素粒子の数」が、10^{80}くらいと言われていますので、とても大きな選択肢の中から秘密鍵を選んでいるわけです。公開鍵dGに対応する秘密鍵dを、しらみつぶしに探すことがいかに無謀か、おわかりいただけるでしょうか。

3.7 楕円曲線 Diffie-Hellman 鍵共有

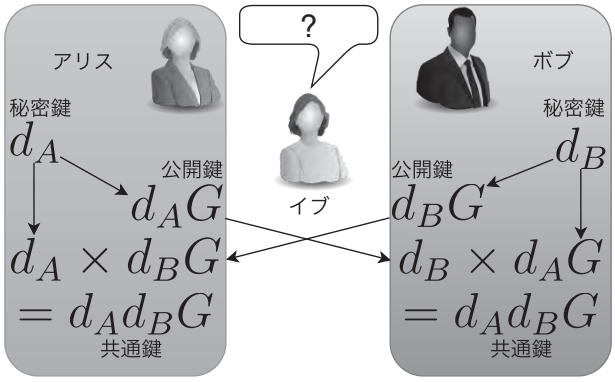
最後に、スカラー倍算を使ったアルゴリズムの例として、ここでは楕円曲線を使った鍵共有の方式、ECDH (Elliptic-curve Diffie–Hellman)について紹介します。

「2.1.2 鍵配送問題」では、盗聴者がいる場合、共通鍵暗号を使おうにも、鍵が盗聴者に知られてしまう問題を取り上げ、その解決策の一つとして公開鍵暗号を紹介しました。ここで、もう一つの解決策として、盗聴者のいるところでも、楕円曲線を使って安全に鍵を受け渡しできる方法を紹介します。

楕円曲線 Diffie-Hellman (ECDH)
有限体$\mathbb{F}_p$、楕円曲線の方程式、ベースポイントG、Gの点位数rはアリス、ボブ、イブに既知とする。

1. アリスは$1 < d_A < r$となるd_Aを選び、秘密鍵とする。またd_AGを公開鍵とする。
2. ボブは$1 < d_B < r$となるd_Bを選び、秘密鍵とする。またd_BGを公開鍵とする。
3. アリスとボブはお互いの公開鍵を交換する。公開鍵は盗聴されても構わない。
4. アリスはボブから入手したd_BGと自分の秘密鍵d_Aで、d_Ad_BGを計算する。
5. ボブはアリスから入手したd_AGと自分の秘密鍵d_Bで、d_Ad_BGを計算する。
6. d_Ad_BGをお互いの共通鍵として使う。j

図 20: 楕円曲線 Diffie-Hellman



イブは公開鍵であるd_AGやd_BGを入手することはできますが、公開鍵から秘密鍵であるd_Aやd_Bを知ることはできません。一方、アリスとボブは自身の秘密鍵と相手の公開鍵からd_Ad_BGを計算することが可能です。このd_Ad_BGを共通鍵として、安心して使うことができます。

4. 社会とつながる暗号技術

2018 年 3 月 8 日の参議院予算委員会、浅田均議員の質問の中で、公文書の管理にハッシュ関数やブロックチェーンを活用してはどうかという趣旨の発言がありました。

国会は約 1 年にわたり「森友学園問題」に揺れており、国有地の売却についての「決裁文書」に、「国会に提出されたもの」と「詳細が記された売却契約当時のもの」が存在する―つまり決裁文書の改ざんの疑惑で、佐川国税庁長官の辞任に発展しました。

浅田議員の発言、「公文書の管理にハッシュ関数やブロックチェーンを利用すること」のメリットを著者なりに解釈すると、

- ハッシュ値により、「決裁文書」が決裁時点から変更されていないことを保証できる
- ブロックチェーンに記録することで、決済文書をハッシュ値ごと「なかったこと」にできない

ということだと思います。k

暗号通貨には少しいかがわしいイメージがつきまとっていますが、使われている技術そのものは、民主的な国家を維持する上で必要不可欠な「国民の知る権利」や「正しい情報公開」のために使われるかもしれません。[10]

暗号通貨以外へのブロックチェーン技術の活用の取り組みは世界中で行われており、特にエストニアでは、登記や納税など、多くの公的サービスでブロックチェーンが利用されています。

暗号通貨に対しては、投機の対象として価格のボラティリティ（変化の激しさ）に一喜一憂するか、いかがわしいものだと無視するか、どちらかの立場となることが多いと感じています。しかし、そこで使われている暗号技術をできるだけ正確に、冷静に知ることは、間違いなく暗号通貨以外のところでも役に立つことでしょう。本稿がそのきっかけになれば、幸いです。

j d_Ad_BGはGのスカラー倍であり、Gと同様に平面上の点です。通常、d_Ad_BGのx座標が共通鍵として使われます。

k 改ざん防止、削除防止のためにブロックチェーンも使えますが、ブロックチェーンでないと実現できないわけではありません。タイムスタンプ、ヒステリシス署名など、既存の技術が存在します。ただし、改ざんや削除を防ぐ原理は共通であると考えます。

謝辞

本稿の作成にあたり、「知の発信」SIG のメンバをはじめとする CITP フォーラムの方々、またデジタルフィールドの同僚にレビューをいただきました。特に青木伸輔さん（中電 CTI）、服部智明さん（NEC）から多くのアドバイスを頂戴しました。貴重な時間を割いていただき、本当にありがとうございました。ただし、本稿に残った誤りとレビュー結果の未反映は、全て赤根の責任です。

参考文献・資料

[1]木下宏揚. サトシ・ナカモトは現代のマルコーニか？. 情報処理学会 連続セミナー2016 第 6 回 :「フィンテック～ブロックチェインの理解と応用～」資料. 情報処理学会 (2016)
http://www.ipsj.or.jp/event/seminar/2016/program06.html
[2]アーシュラ・K. ル=グウィン (著), 清水真砂子 (翻訳). 影との戦い ゲド戦記 I, 岩波書店 (1999)
https://www.iwanami.co.jp/book/b260752.html
[3]結城浩. 暗号技術入門 第 3 版 秘密の国のアリス. SB クリエイティブ株式会社 (2015)
http://www.hyuki.com/cr/
[4]神保雅一, イオタゼミ. なるほどナットク！ 暗号がわかる本. オーム社 (2004)
http://shop.ohmsha.co.jp/shopdetail/000000002099/
[5]神永正博. 現代暗号入門　いかにして秘密は守られるのか(ブルーバックス). 講談社 (2017)
http://bookclub.kodansha.co.jp/product?isbn=9784065020357
[6]アンドレアス・M・アントノプロス（著）, 今井崇也,鳩貝淳一郎（訳）. ビットコインとブロックチェーン 暗号通貨を支える技術. NTT 出版 (2016)
http://www.nttpub.co.jp/search/books/detail/100002391
[7]萩田真理子. 暗号のための代数入門. サイエンス社. p87 (2010)
http://www.saiensu.co.jp/?page=book_details&ISBN=ISBN978-4-7819-1268-4&YEAR=2010
[8]伊豆哲也. 楕円曲線暗号入門. (2013)
https://researchmap.jp/mulzrkzae-42427/
[9]辻井重男, 笠原正雄(編著), 有田正剛, 境隆一,只木孝太郎, 趙晋輝, 松尾和人(共著). 暗号理論と楕円曲線, 森北出版 (2008)
http://www.morikita.co.jp/books/book/2213
[10]野口悠紀雄. 森友問題の公文書改ざんはブロックチェーン技術で防げる. ダイヤモンド・オンライン (2018)
http://diamond.jp/articles/-/163327

著者紹介

赤根大吾（認定番号：14000022）
（株）デジタルフィールド
取締役
情報処理安全確保支援士
（登録番号 第 002400 号）

ソフトウェア開発インフラの構築、継続的インテグレーションの導入に従事。高度情報技術者（テクニカルエンジニア（情報セキュリティ）、ネットワークスペシャリスト、プロジェクトマネージャ、IT ストラテジスト）。TOEIC 885 (2015 Apr)。@dgakane on Twitter

認定情報技術者（個人認証）申請の手引き

CITP コミュニティ

CITP 認定情報技術者
Certified IT Professional

はじめに

認定情報技術者(CITP：Certified IT Professional)は平成 26 年度より情報処理学会が創設したプロフェッショナル IT 人材認証制度である。

CITP 制度の目的は第一に「高度な能力を持つ情報技術者を可視化し、その社会的地位の確立を図ること」である。つまり IT 技術者に対し自発的に技術向上を促すともに、IT 技術者の能力を客観的に評価する尺度を提供することにある。

IT 分野の技術進歩の速さはこれまでもドッグイヤーと呼ばれてきたが、シリコンバレーがもたらす破壊的なビジネス変化のスピードはさらに速い。このような業界で必要とされるプロフェッショナル IT 人材には、モチベーションが高く、自らアンテナを立て自ら学び常に変化に追随してゆく、“トップガン”が必要となる。

本書は CITP に挑戦し、学び続ける技術エリートの道を歩み始めるための手引きとして、CITP コミュニティがまとめたものである。

CITP コミュニティ　「知」の発信専門部会
2017 年 12 月

第 1 章

IT 技術者の
スキル・能力をどのように可視化するの？

人間の能力を可視化しレベルに応じて認証することは一般的には非常に難しい。

幸い、IT 技術者の場合、国際標準に準拠した IT スキル標準（ITSS）が策定されており、これにより可視化するようになっている。その概要を説明する。

1.1　認定の 4 つのポイント

認定情報技術者（CITP）の申請案内には下記のように解説されている。

> 「CITP とは、IT スキル標準（ITSS）のレベル 4 以上に相当する知識とスキルを保有し、それを業務で発揮していると共に、技術の発展や後進の育成などの社会貢献を行っていると認定を受けた技術者です。

この説明から

①知識を保有

②スキルを保有

③業務で知識・スキルを発揮している(ビジネス貢献)

④技術の発展や後進の育成などの社会貢献を行っている（プロフェッショナル貢献）

の４つの観点で、レベル 4 以上が必要ということになる。

ではレベル 4 以上とはどういうことか？　同じく申請案内では、

> IT スキル標準のレベル 4 とはプロフェッショナルとしてスキルの専門分野が確立し、自らのスキルを活用することによって、独力で業務上の課題の発見と解決をリードするレベル。社内において、プロフェッショナルとして求められる経験の知識化とその応用（後進育成）に貢献しており、ハイレベルのプレーヤとして認められる。スキル開発においても自らのスキルの研鑽を継続することが求められる（IT スキル標準より)」

となっており、

・独力で業務上の課題の発見と解決をリードできる

・社内においてプロフェッショナルとして求められる経験の知識化とその応用（後進育成）に貢献

・自らのスキルの研鑽を継続している

ことが求められる。

これらをまとめると、CITP の認定には以下の 4 つがポイントになる(図１)。

①知識

②専門分野のスキル

プロフェッショナルとしてスキルの専門分野が確立している

③ビジネス貢献

プロジェクトの成功の経験と実績などのビジネス成果に対する貢献。独力で業務上の課題の発見と解決をリードできる。

④プロフェッショナル貢献

専門技術の向上による社内外への貢献、後進育成や技術の継承などのプロフェッショナルとしての貢献。自らのスキルの研鑽を継続することができる。

この 4 つのポイントについてその意味と申請書での対応項目を順に解説する。

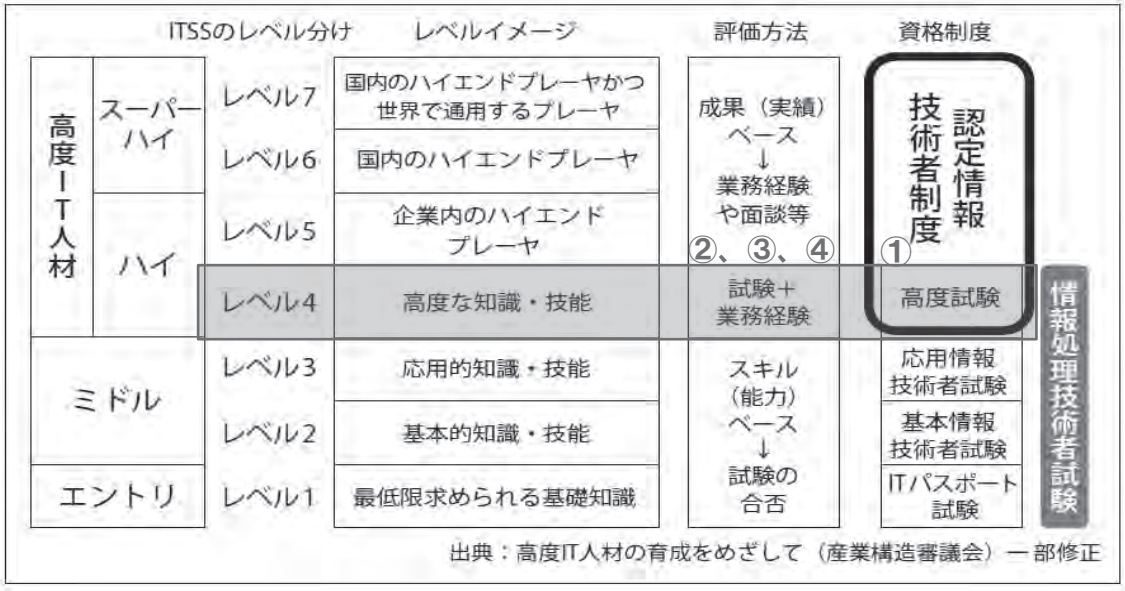


図１　ITSS と認定情報技術者の関係

1.2　知識

ITSS の知識レベルと情報処理試験は連携しており、レベル４の知識は高度情報処理試験の合格により証明できる。申請職種に必要な高度情報処理試験は図２の通り。

CITP職種	専門分野	情報処理技術者試験（高度試験） ※いずれかに合格していること
ITアーキテクト	アプリケーションアーキテクチャ	システムアーキテクト試験
	インテグレーションアーキテクチャ	ITストラテジスト試験
	インフラストラクチャアーキテクチャ	（旧試験）アプリケーションエンジニア
		（旧試験）システムアナリスト
		（旧試験）上級システムアドミニストレータ
プロジェクトマネジメント	システム開発	プロジェクトマネージャ試験
	ネットワークサービス	（旧試験）プロジェクトマネージャ
	ソフトウェア製品開発	
ITスペシャリスト	ネットワーク	ネットワークスペシャリスト試験
		（旧試験）テクニカルエンジニア：ネットワーク
	データベース	データベーススペシャリスト試験
		（旧試験）テクニカルエンジニア：データベース
	セキュリティ	情報処理安全確保支援士試験
		情報セキュリティスペシャリスト試験
		（旧試験）テクニカルエンジニア：情報セキュリティ
		（旧試験）情報セキュリティアドミニストレータ試験
アプリケーションスペシャリスト	業務システム	システムアーキテクト試験
	業務パッケージ	（旧試験）アプリケーションエンジニア
ソフトウェアデベロップメント	応用ソフト	システムアーキテクト試験
		（旧試験）アプリケーションエンジニア
カスタマサービス	ハードウェア	ITサービスマネージャ試験
	ソフトウェア	（旧試験）テクニカルエンジニア：システム管理
	ファシリティマネジメント	
ITサービスマネジメント	運用管理	ITサービスマネージャ試験
	システム管理	（旧試験）テクニカルエンジニア：システム管理
	オペレーション	
	サービスデスク	

図２　CITP 職種と申請に必要な情報処理技術者試験・情報処理安全確保支援士試験

1.3　専門分野スキル、ビジネス貢献、プロフェッショナル貢献の表現方法

4 つのポイントの内、残りの 3 つ（②専門分野のスキル、③ビジネス貢献、④プロフェッショナル貢献）は ITSS の基準で表現する。ITSS は 3 部構成となっており、③ビジネス貢献・④プロフェッショナル貢献は 2 部キャリア編の**達成度指標**として定義されている。また、②専門分野のスキルは 3 部スキル編の**スキル熟達度**として定義されている(図 3)。

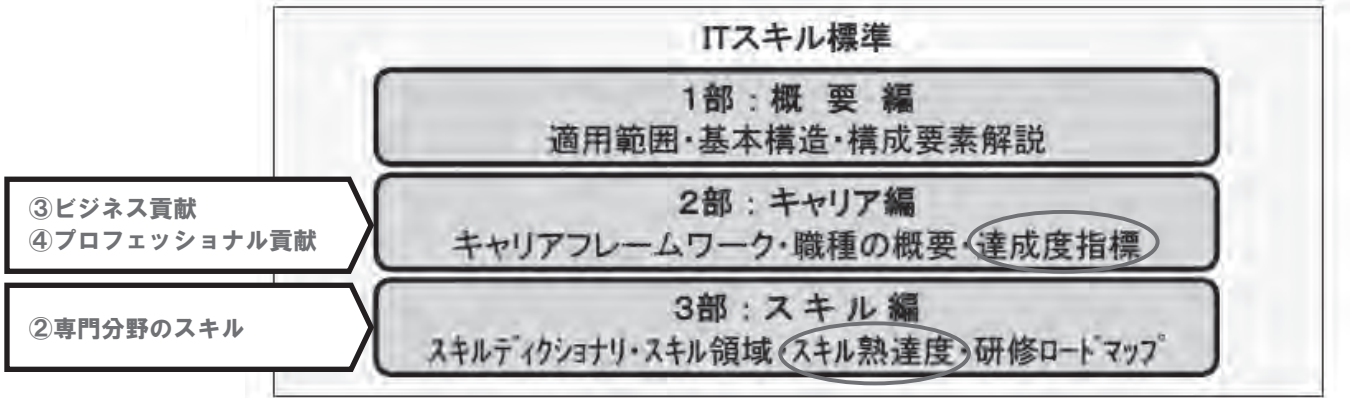


図 3　ITSS の構成

申請者は**「キャリア⇒達成度指標」**と**「スキル⇒スキル熟達度」**の基準を満たすことが求められる。理解を助けるため、アプリケーションスペシャリスト・レベル 4 の具体的な基準を図 4 に示すが、次ページからより詳しく解説する。

キャリア（達成度指標）	スキル（スキル熟達度）
責任：開発チームリーダとして 実績：至近 5 年以内のプロジェクトを 2 回以上 複雑性：8 つの複雑性要件の中から 2 項目以上 サイズ：3 人以上 を成功裏に達成した経験を有する	開発チームリーダとして 共通スキル（業務分析、テクノロジ、デザイン等）および固有スキル（業務システム構築等） を発揮できる

図４ アプリケーションスペシャリスト（レベル４）の達成度指標とスキル熟達度

1.4　達成度指標とは

(1) ビジネス貢献とプロフェッショナル貢献

達成度指標は、ビジネスを成功させる人材を可視化するために２つの貢献に焦点をあてている。第一はプロジェクトの成功の経験と実績などビジネスに対する貢献を示すビジネス貢献、第二は専門技術の向上による社内外への貢献や後進育成や技術の継承といったプロフェッショナルとしての貢献を示すプロフェッショナル貢献である(図 5)。

この２つの貢献の具体的内容は職種によって異なっており、詳細は「IT スキル標準 V3 2011　２部キャリア編」補足 B（ページ 17～56）を参照のこと。

以降、アプリケーションスペシャリストを例に説明する。

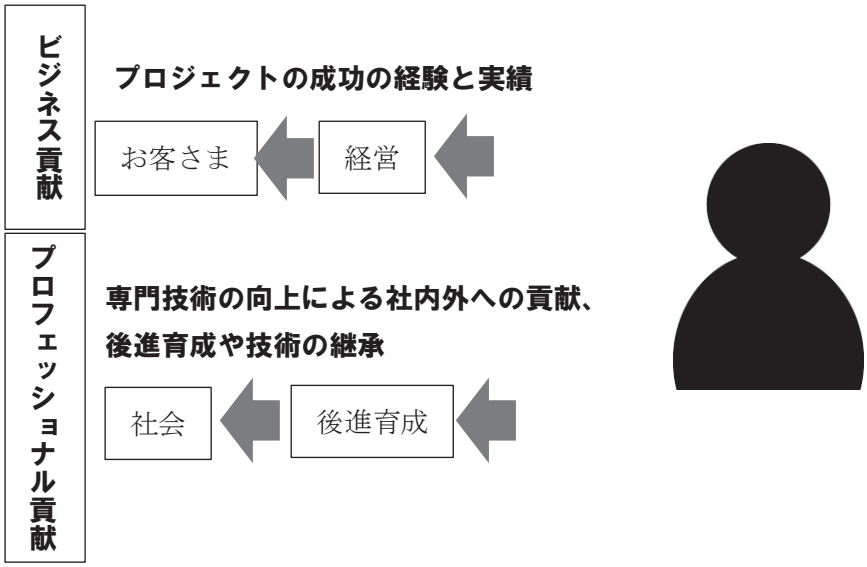


図５　ビジネス貢献とプロフェッショナル貢献

(2) ビジネス貢献の指標

ビジネス貢献は、担当したプロジェクトにおける責任の重さを示す責任性、プロジェクトの難易度を表す複雑性、およびサイズという３つの指標で評価する(図６)。

ITスキル標準V3 2011 2部:キャリア編_20120326

B．7 アプリケーションスペシャリスト

■達成度指標のレベル記述の違い（ビジネス貢献）　専門分野「業務システム」

レベル	ビジネス貢献						
	責任性				複雑性		サイズ
	活動局面	役割・責任範囲	品質条件	実績回数	複雑性要件	必要条件数	開発チームのピーク時要員数
6	アプリケーションの開発、設計、構築、導入、テスト及び保守における	開発チーム責任者として、開発チームをリードし、業務開発全局面に責任を持つ。	顧客の環境に最適な品質（機能性、回復性、利便性等）を満足するアプリケーションの設計、開発及び導入を	３回以上（内１回以上はレベル６、他はレベル５以上の複雑性、サイズ相当）成功裡に達成した経験と実績を有する。	□複雑な業務要件が多岐に亘り存在し、幾つかの特殊な業務要件が含まれる □新技術で大手企業で実績のないもの、あるいは事例が見当たらない使用実績の少ないテクノロジを使用 □複数のシステム形態が共存（トランザクション処理、クライアントサーバ、Web 等） □ミッションクリティカルなシステムであり高品質を要求 □各業種代表的、業種横断的又は国内有数規模のシステム □クロスプラットフォームでのアプリケーション □２４時間３６５日の連続稼動が要求され、変更、保守、障害回復に高度な設計が必要 □限られた期間内で要求される業務形態の変更度合いが大きい	２項目以上	５０人以上
						４項目以上	１０人以上５０人未満
5				３回以上（内１回以上はレベル５、他はレベル４以上の複雑性、サイズ相当）成功裡に達成した経験と実績を有する。		２項目以上	１０人以上５０人未満
						４項目以上	３人以上
4		開発チームリーダとして、業務開発全局面において、	担当するアプリケーションの成果物に責任を持ち、	プロジェクトを２回以上（内１回以上はレベル４、他はレベル３以上の複雑性、サイズ相当）成功裡に達成した経験と実績を有する。		２項目以上	３人以上
3	アプリケーションの開発、設計、構築、導入、テスト及び保守において、	既存の作業標準やガイダンスに従い、開発チームメンバとして、	担当する成果物の実施責任を持ち、	プロジェクトに１回以上（レベル３の複雑性、サイズ相当）参画した経験を有する。		２項目以上	特定せず

図６　ビジネス貢献の３つの指標（ｱﾌﾟﾘｹｰｼｮﾝｽﾍﾟｼｬﾘｽﾄ）

・責任性

プロジェクト全体の責任者として、あるいはサブプロジェクトの責任者として、もしくはメンバとして対応したかによって責任の重さが違う。その対応すべき立場の責任性をレベルごとに設定している(図７)。

レベル４はチームのリーダとしてプロジェクトを２回以上成功させた実績が必要。

（内１回以上はレベル４、他はレベル３以上の複雑性、サイズ相当）

・複雑性

プロジェクトの難易度を表す要素である。新規性、ミッションクリティカル性、国際的認知性等８つの項目を定義しており、レベルごとに必要な複雑性の数を設定している。レベル４は２項目以上となっている。

・サイズ

プロジェクトの規模を表す要素である。プロジェクト規模（例：必要とする要員の数が 10 人か 50 人か 100 人か？)、あるいはビジネス規模（例：必要とされる予算金額が 1 億円か、10 億円か、50 億円か？）をレベルごとに明示している。

レベル４は３人以上となっている。

(3) プロフェッショナル貢献の指標

プロフェッショナル貢献は、技術者の保有する専門性（専門分野別主要テーマ)、貢献度合い、技術継承実績（技術の継承に関する実績度)、後進の育成の４つの指標で評価する（図７)。

ITスキル標準V3 2011 2部:キャリア編_20120328

■達成度指標のレベル記述の違い（プロフェッショナル貢献）

レベル	プロフェッショナル貢献					
	専門分野別主要テーマ		貢献度合い	技術の継承に対する実績度		後進の育成
	業務システム	業務パッケージ		活動分野	必要条件数	
6	□アプリケーション開発領域における技術要素(ツール、標準、メソドロジ等) □アプリケーション部分のコスト、スケジュール、リスクのアセスメント	□業務パッケージを活用した適用導入および関連するアプリケーション開発領域における技術要素(ツール、標準、メソドロジ等) □業務パッケージを活用した適用導入および関連するアプリケーション部分のコスト、スケジュール、リスクのアセスメント	他を指導することができる高度な専門性を保有し、業界に貢献している。	□学会、委員会等プロフェッショナルコミュニティ活動 □著書 □社外論文掲載 □社内論文掲載 □社外講師 □社内講師 □特許出願	４項目以上	必須
5	□アプリケーション部分のコスト、スケジュール、リスクの管理	□業務パッケージを活用した適用導入および関連するアプリケーション部分のコスト、スケジュール、リスクの管理	他を指導することができる高度な専門性を保有し、社内に貢献している。		３項目以上	必須
4	□アプリケーション部分のコスト、スケジュール、リスクの管理	□業務パッケージを活用した適用導入および関連するアプリケーション部分のコスト、スケジュール、リスクの管理	高度な専門性を保有し、後進を指導している。		１項目以上	必須
3	□アプリケーションの設計、開発、導入	□業務パッケージを活用した適用導入および関連するアプリケーションの設計、開発、導入、カスタマイズ	専門性を保有し、独力で実践している。	－	－	－

図７　プロフェッショナル貢献の４つの指標（ｱﾌﾟﾘｹｰｼｮﾝｽﾍﾟｼｬﾘｽﾄ）

・専門性（専門分野別主要テーマ）

各専門分野ごとの主要テーマを例示し、それらの専門性の影響度合をレベルごとに定

義している。主要テーマは職種によって異なるため、「IT スキル標準 V3　2011　2 部キャリア編」補足 B（ページ 17～56）を参照のこと。

・貢献度合い

レベル 6 は業界に貢献、レベル 5 は社内に貢献、そしてレベル 4 は「高度な専門性を有し、後進を指導している」ことが求められる。

・技術継承実績

下記 7 つの活動分野（全職種共通）の内、レベルごとに必要条件数を明示している。レベル 4 の場合少なくとも一つの項目が必要である。

□学会, 委員会等プロフェッショナルコミュニティ活動　□著書

□社外論文掲載　□社内論文掲載　□社外講師　□社内講師　□特許出願

・後進の育成

レベル 4 は「後進の育成（メンタリング、コーチング等）を必須としている。

1.5　スキル熟達度とは

『専門分野のスキル』を表現する指標が「スキル項目」、「スキル熟達度」である（図 9）。

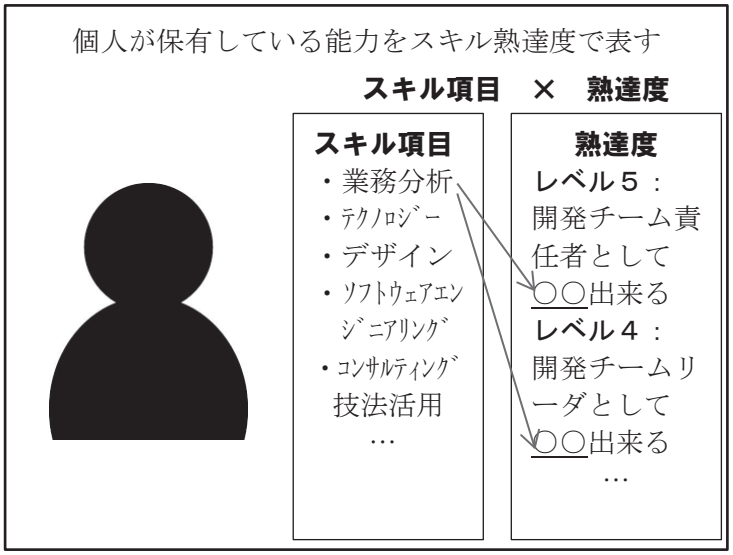


図９　スキル項目とスキル熟達度

(1) スキル項目

「スキル項目」は、技術者が持つ専門分野のスキルを定義したもので、職種共通スキル項目と専門分野固有スキル項目がある(表 10)。

表 10　ITSS で定義されているスキル項目（ｱﾌﾟﾘｹｰｼｮﾝｽﾍﾟｼｬﾘｽﾄ）

共通スキル項目	スキル熟達度に関する自己申告
業務分析	開発／適用のチームリーダとして、業務要件、技術要件分析を行うことができる。
テクノロジ	開発／適用のチームリーダとして、複雑性の高い技術的問題解決を実践するとともに全開発局面を遂行することができる。※複雑性の高い技術的問題を具体的に明記すること
デザイン	開発／適用のチームリーダとして、開発環境要件、データベース要件を満たすアプリケーションデザインを実施することができる。
ソフトウェア エンジニアリング	開発／適用のチームリーダとして、最適開発手法、開発支援ツール、テスト技法等のソフトウェアエンジニアリング技術に関して経験の浅いメンバに対してアドバイスを与え、システム開発を遂行することができる。
コンサルティング 技法の活用	開発／適用のチームリーダとして、コンサルティング技法を適用し、プロジェクトを実施することができる。
知的資産管理 活用	開発／適用のチームリーダとして、知的資産のデータベース化、活用、維持、管理を行い、プロジェクトを効率的、高品質に実施することができる。
プロジェクト マネジメント	開発／適用のチームリーダとして、プロジェクトマネジメント職種と協業し、プロジェクト計画策定と実施、変更管理等のプロジェクトマネジメントを遂行できる。
リーダシップ	開発／適用のチームリーダとして、指揮、命令しプロジェクトを遂行することができる。
コミュニケーション	開発／適用のチームリーダとして、プロジェクトメンバとのチームコミュニケーションを図りプロジェクトを遂行することができる。
ネゴシエーション	開発／適用のチームリーダとして、プロジェクトチームメンバと技術的課題に関する合意を形成できる。
専門分野固有スキル：業務システム	
業務システム構築	開発のチームリーダとして、プロジェクトを遂行することができる。

(2) スキル熟達度

スキル熟達度は技術者が各スキル項目をどのレベルで保有しているかを表現するもので、「～することができる」という能力表現で定義している。熟達度は役割とレベルが対応しており、レベル 4 はリーダとしてそのスキルを発揮できること求められる(表 11、12)。

表 11　スキル熟達度のレベルと役割

レベル	責任
レベル 7 ～ 5	責任者として
レベル 4	リーダとして
レベル 3 ～ 1	メンバとして

表 12　レベル 4 のキャリア（達成度指標）（アプリケーションスペシャリスト）

スキル項目と知識項目	スキル熟達度	
【職種共通スキル項目】 ●業務分析 【知識項目】 －業務要件分析 －技術要件分析 －インダストリ知識 －システム化戦略策定 －プラットフォーム要件定義 －システム価値の検証 －情報化と経営 －汎用業務内容 －汎用業務最新動向	レベル7	
	レベル6	ピーク時の要員数50人以上のアプリケーション開発プロジェクトにおいて、開発チーム責任者として、経営戦略・システム化戦略との整合性を保ち、業界や技術動向の先見的見地に基づき複雑高度な業務要件、技術要件分析を行うことができる。
	レベル5	ピーク時の要員数10人以上50人未満のアプリケーション開発プロジェクトにおいて、開発チーム責任者として、業務要件、技術要件分析を行うことができる。
	レベル4	ピーク時の要員数3人以上のアプリケーション開発プロジェクトにて、開発チームリーダとして、業務要件、技術要件分析を行うことができる。
	レベル3	アプリケーション開発プロジェクトの開発チームメンバとして、担当する領域における業務要件、技術要件分析を行うことができる。

第２章

申請書の書き方のポイントは？

申請には多くの書類を作成しなければならない。筆者も経験したが、優先順位を付けないと途中でエネルギーを使い果たしてしまう。的確かつ効率的な書き方の例を紹介する。

2.1　提出書類の概要と作成順

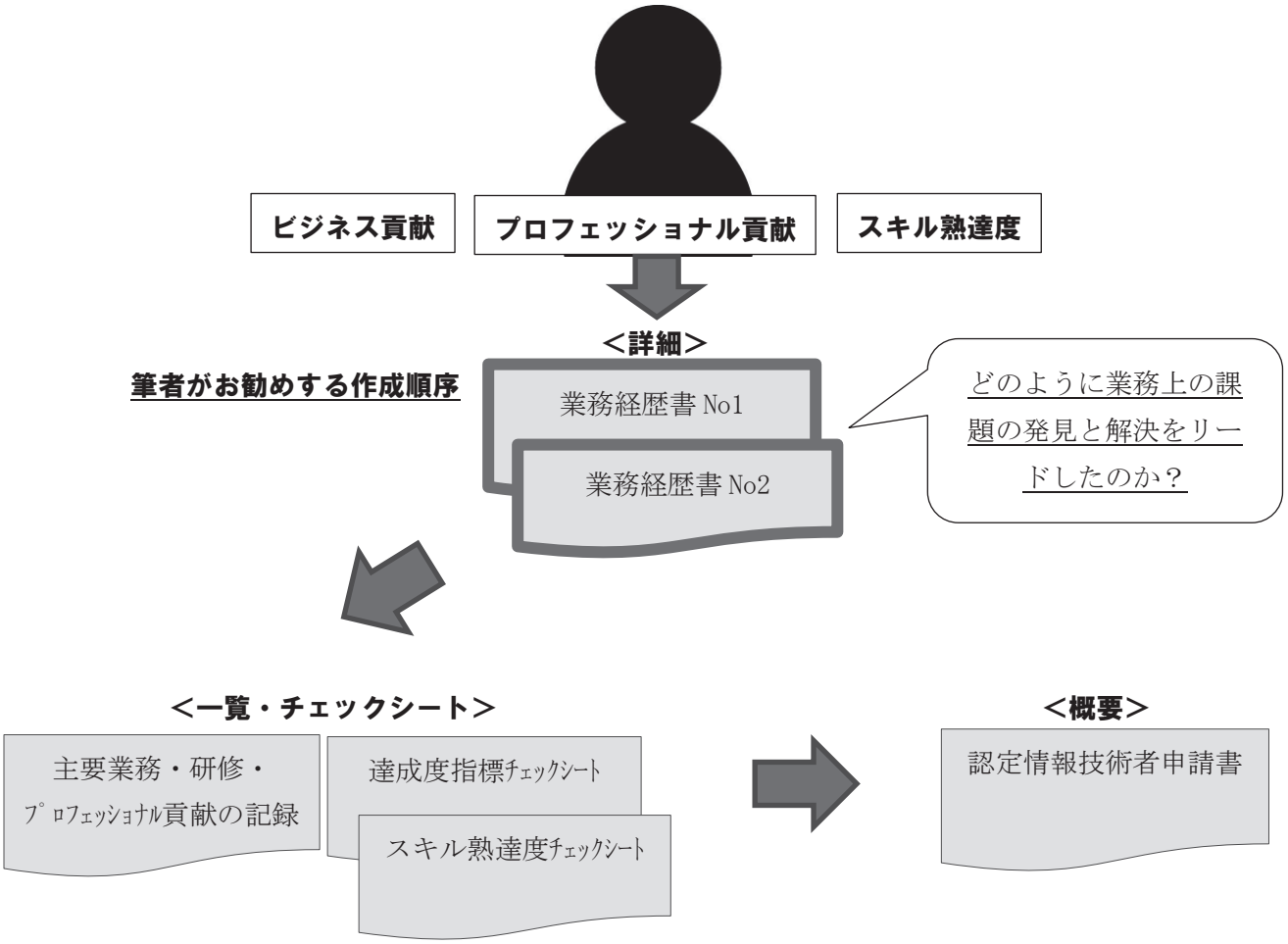
作成する提出書類は下記の 5 種類がある。

a. 認定情報技術者申請書
b. 主要業務・研修・プロフェッショナル貢献の記録
c. 業務経歴書 No1, No2
d. 達成度指標チェックシート
e. スキル熟達度チェックシート

このうち最も重要なのが『c. 業務経歴書』である。採点者はこれに書かれている具体的な内容で申請者のスキル・能力を判断する（と思われる）。

また、『a. 認定情報技術者申請書』は概要をまとめたもの、『b. 主要業務・研修・プロフェッショナル貢献の記録』、『d. 達成度指標チェックシート』、『e. スキル熟達度チェックシート』の３つは一覧によるチェック用である。

したがって『c. 業務経歴書 No1, No2』に最もエネルギーを使い、これが完成したら概要編やチェックシート系を作成するのが良い。次ページから書き方のポイントを解説する。



2.2. 業務経歴書

採点者に如何に申請者の実力を分かり易く伝えるかがポイントである。採点者への印象を高めるために、以下の項目に留意して記載してほしい。

なお、実績は自身で評価が高いものから順に 2 件だけを選んで記載するとよい。

○一般的な内容ではなく、実際に実施した内容を具体的に記載する

○高度情報処理試験に出てくる専門用語を出来るだけ使う

○『独力で業務上の課題の発見と解決をリードできる』ことを示す

・どのような課題を、誰が、どう解決し、どのような結果・評価を得たか

・チームリーダとしてのスキルを発揮したか

○後進育成への貢献

以下に合格例を紹介する。

(1) 一般的な内容ではなく、実際に実施した内容を具体的に記載する

申請者が活用した技術やその背景を具体的に記載することにより採点者がイメージしやすくなる。

【ITS(NW)職種の合格例】

プロジェクト要件	• 新拠点に構築済みのリバースプロキシが存在し、将来的に社外公開サーバはそちらへ移行することが決まっている為、・・・新拠点のリバースプロキシを経由する経路へ変更する方式で移行作業を行う。 • 社外公開サーバが接続している LAN セグメントを、新拠点まで L2延伸することで・・・。 • 新拠点のリバースプロキシはファームウェアのバージョンが異なることから・・・を移行作業日までに実施する。

(2) 高度情報処理試験に出てくる専門用語を出来るだけ使う

CITP には高度情報処理試験の合格が前提となっているが、それぞれの職種に対応する知識ドメインの用語を適切に使うことで所有する知識とその理解度をアピールできる。

【PM 職種の合格例】

業務概要	活用した専門技術	• PMBOK のプロジェクトマネジメント・プロセス全般を活用しているが、特に高度な対応を必要とした技術は以下 WBS 作成、アクティビティ資源・所要時間見積り、コスト見積り、スケジュールコントロール

自らのスキルを発揮した課題と解決	［解決・結果］ 私はプロジェクトマネージャとして、漏れのない移行を行うため、以下事項を特に重視し作業を進めた。 • 作成した WBS をアクティビティに要素分解する際、・・・・を実施し、作業項目漏れのないことを確認した。 • 若手メンバをアクティビティ定義の作業に参加させることにより、・・・という教育的効果もあった。 • アクティビティ順序設定、所要期間見積りをベースに、クリティカル・チェーン法により所要期間バッファの追加を考慮して移行対象ごとの移行準備スケジュールを作成しコントロールすることで、・・・、クラッシングや、ファスト・トラッキングを行う必要なく順調に進捗した。

(3)『独力で業務上の課題の発見と解決をリードできる』ことを示す
・どのような課題を、誰が、どう解決し、どのような結果・評価を得たか

『どのような課題』は『業務概要・複雑性要件』欄の中で該当項目を□から■に変え、そのあとに具体的内容を記述する。2 件以上必要。

『誰が』は例えば『申請者自ら』というように、自らが解決をリードしたことをアピールする。

『どのような結果・評価』は『自らのスキルを発揮した課題と解決』欄に、『業務概要・複雑性要件』欄の該当項目を再掲するとともに、 [課題]と[解決・結果]を整理して記載する。

【ITS (SC) 職種の合格例】

業務概要	複雑性要件	■複雑、高度なアクセスコントロール要求 【保守者・管理者のアクセスコントロール】 機密情報を取り扱うため保守者・管理者に対して厳密なアクセス制限が求められる。

項目を一致させる

自らのスキルを発揮した課題と解決	■複雑、高度なアクセスコントロール要求 【保守者・管理者のアクセスコントロール】 [課題] • 1)機密情報を扱うため保守者アカウントは厳密に管理し、万一の事故に備え作業履歴を残す必要があった • 2)各社の管理者は自社の情報にしかアクセスできないようにし、権限の付与は各社が管理できるようにする必要があった [解決・結果] • 課題 1 については申請者自ら以下のようなポリシーを制定し、運用設計に盛り込んだ。 • 1-1)・・・ • 1-2)・・・ • 1-3)・・・ • 課題 2 については申請者が要件定義の段階でアクターを整理しユースケース設計を実施した。その結果、・・・を用意することで課題を解決した。・・・

・チームリーダとしてのスキルを発揮したか

レベル 4 はリーダとしてそのスキルを発揮できること求められるため、役割を明確に記述する。PM や責任者でもさらに上のレベルとなるのでＯＫ（スキル熟達度参照)。

【PM 職種の合格例】

自らのスキルを発揮した課題と解決	**※どのような課題を、誰が、どう解決し、どのような結果・評価を得たかに加えて、レベル 4 の実績ではチームリーダとしてのスキルを発揮したことが明確になるよう記述して下さい。** • 当プロジェクトは短納期であり、かつ、顧客担当者が十分な打ち合せ時間を確保する事が困難であるという課題があった。そのため、私は PM としてプロトタイプモデルを採用する事とした。なぜならば、・・・、短納期にも対応可能と考えたからである。 • 設計工程以降に仕様変更が発生する事が確定的であるが、変更内容が決まらず納期直前に変更を依頼される可能性があるという課題があった。私はマスタスケジュール作成時に、考えられる仕様変更毎に変更にかかる日数を設定し納期と品質を守る事を前提とした仕様変更可能最終日を設定した。その日付を顧客に説明し合意したことで、・・・。

(4) 後進育成への貢献

CITP はプロフェッショナル貢献として「高度な専門性を有し、後進を指導している」ことが求められているため、『後進育成への貢献』欄は必須である。

なお、8 ページ図 7 に規定されている技術継承実績では一つ以上が求められるが、『後進育成への貢献』欄は「社内講師」に該当する。そのため『主要業務・研修・資格・プロフェッショナル貢献の記録』申請書の＜後進の育成＞欄には本欄に記載した以外の活動を記載するが、なければ空白でもよい。

【ITS (SC) 職種の合格例】

後進育成 への貢献	• プロジェクトメンバー（入社 3 年目）をスマートフォンアプリ開発の主担当として、委託先の管理全般を任かせた。積極的に情報を吸い上げ、プロジェクト完了時にはスマートフォンアプリ開発の第一人者と呼べるまでに成長した。・・・技術面についても、APS のレベル 3 まで成長できたと評価する。 • また、もう一人のプロジェクトメンバー（入社 4 年目）をバックエンド開発の主担当にすえ、前述した通りテストケースの洗い出しを実施させた。・・・彼も今回のプロジェクトを通じて APS のレベル 3 まで成長できたと評価する。

【ITS (NW) 職種の合格例】

後進育成 への貢献	• 本プロジェクトでは少人数のチームであったため、メンバは一人何役もこなす必要があった。担当メンバは・・・業務分野の専門家としてチームに加わったが、改修における要件定義、設計のフェーズではネットワークやセキュリティについてもディスカッションを重ねて知見を共有し、構築についても web アプリ部分のコーディングを行ってもらうことで経験を蓄積し、ITS（ネットワーク）レベル3相当の能力を身につけた。現在は運用保守におけるトラブル発生時に、申請者に代わってどちらでも対応できる体制を取っている。

2.3　認定情報技術者申請書

認定情報技術者申請書は、『業務経歴書』などで記載した適格性をまとめたものである。実績 No1, No2 を記載してから記述すると記載し易い。

(1) 申請理由

申請理由はレベル 4 に該当することを示すためにビジネス貢献およびプロフェッショナル貢献の要約を 4～5 百字内で簡潔に記述することが求められている。

【PM 職種の合格例】

申請理由	・・・のシステム開発を過去5年間に2件経験し、どちらもプロジェクトマネージャとしてメンバーを率いて、・・・プロジェクトを完遂した。また、開発時以外でも保守チームのチームリーダとしてマネジメントに従事し、不具合対応や改修作業を滞りなく実施している。 業務経歴書の実績 No.1 に関しては、開発のプロジェクトマネージャとして、短納期かつ仕様変更の可能性が高いプロジェクトを納期通りに完成させた。実績 No.2 では、・・・のプロジェクトマネージャとして、処理時間に課題を抱えたシステムを無事想定時間内に収め完成させた。 実績 No.1 では若手を中心にプロジェクトを実施し、自信を付けさせると同時に技術力の向上にも貢献したほか、社外のPMコンテストにPMとして参加し、プロジェクトマネジメント部門で優勝した。 以上のビジネス貢献、プロフェッショナル貢献によりレベル4のプロジェクトマネジメントの条件を満たしていると考え認定を申請する。

上記例では、アンダーライン部にビジネス貢献として PM の達成度指標を簡潔に記している（スキル項目・熟達度は詳細にわたるため省略している)。また、　部にプロフェッショナル貢献として後進の育成と社外コミュニティ活動が記されている。

下記例は 5 百文字を超えるが貢献項目毎にまとめた合格例である

【PM 職種の合格例】

申請理由	【ビジネス貢献】 • 責任性　・・・ • 複雑性　・・・ • サイズ　・・・ 【プロフェッショナル貢献】 • 専門性　・・・ • 技術の継承　・・・ • 後進の育成　・・・ これらのビジネス貢献、プロフェッショナル貢献から、IT スキル標準レベル 4 のプロジェクトマネジメントの条件を満たしていると考え、認定を申請する。

(2) 得意分野

申請者の得意分野としてスキル熟達度チェックシートに記載した内容の要約を含めて、2～3 百字程度に具体的かつ簡潔に記載する必要がある。そのためこれも先にスキル熟達度チェックシートを完成させ、その要約を記載するようにするとよい。

【PM 職種の合格例】

得意分野	入社以来、大手会社向けのミッションクリティカルな基幹系システムの構築・開発に携わっており、オープン系のシステム構築・開発を得意分野としている。特に・・・に精通している。また、システム開発だけでなく、顧客企業に求められる競争力強化に必要なコストダウン施策や新規システムの企画・提案も行っている。 ・・・・・・・ ・・・・・・・ 新技術の情報収集を重ね、システム刷新の際にコスト削減だけでなく、運用、将来性、システムライフサイクルなどの観点も踏まえソリューション提案を実践しており、最新の技術動向、業界動向にも長けている。

2.4　主要業務・研修・プロフェッショナル貢献の記録

記入要領・記入例をみて記載する。

＜著作・論文＞　、＜講演・講師＞　、＜特許出願＞、＜学会・コミュニティ活動＞の４つについては、少なくとも一つ書くのが望ましい。どれもハードルが高そうに見えるが、業務経歴書で述べた後進育成への貢献は「社内講師」に該当するため、＜講演・講師＞でそれを記載するとよい。

また、＜後進の育成＞欄には業務経歴書で述べた『後進育成への貢献』欄に記載した以外の活動を記載する。それがなければ空白でもよい。

【ITS(SC)職種の社内講師事例】

発表年月	講演タイトル名	主催・イベント名	具体的内容	社内/外区分
yyyy 年 m 月 ～ 継続中	・・・・・ ・・・・・ ・・・・・ ・・・・・ ・・・・・ 開催毎にホットな話題を取り上げる。	（自らが主催） 社内セキュリティ勉強会	年に数回程度、セキュリティトピックスに関する社内勉強会を主催。 **発表者を有志で募るが、自らも、毎回発表**している。 参加者は XX 人～X 人。 ・・・・・・ ・・・・・・ ・・・・・・	社内

2.5　達成度指標チェックシート

達成度指標チェックシートは詳細に記述した 2 件の業務経歴書について、ビジネス貢献、プロフェッショナル貢献をクリアしているかをマーク方式でチェックするもの。
ビジネス貢献（責任性・複雑性・サイズ）、プロフェッショナル貢献（専門性・技術の継承・後進の育成）の計 6 項目について、業務経歴書を読み直しながらチェックするとよい。

2.6　スキル熟達度チェックシート

スキル熟達度チェックシートは全項目について、具体的に記載する必要がある。この書類になってくるとかなり疲れが溜まってくると思うが、全項目について手を抜かずしっかり記載してほしい。

第３章　合格者からのアドバイス

【計画的に準備する】

・請書に記入する内容が多いため、作成に時間がかかることと、資格の合格証書や研修の受講記録など用意する資料が多く、探すのに手間取って、時間をかけて準備を進める必要がありましたので、締め切りまでの時間に余裕を持って準備をする必要があると思います。（ITS　F 氏）

・申請書の作成には非常に時間がかかったため、シナリオ作成から素案作成、本書作成、校正、他者チェックなど、　計画的に進めていく必要があった。(PM　M 氏）

・書き始めてみて思った以上に時間がかかるとわかったこと。(複雑性要件の項目が固定のため、それに当てはまる事例を考え、さらに自身の実績がアピールできるようまとめる点に時間がかかりました)、あとは締切日が IPA 試験の翌日だったためです。言葉にすると言うまでもないことですが、計画的に執筆にとりかかることをアドバイスしたいです。（ITS　M 氏）

【IT スキル標準を熟読する】

・業務経歴書、チェックリストを作成する前に、「IT スキル標準」を熟読し、自分が申請する業種に求められているスキルレベルを理解することが大切だと思います。私はこれをしっかり行わない状態で、業務経歴書、チェックリストの記載を始めてしまったので、一通り記載した後に、大量の修正を行うことになりました。(ITS　T 氏）

・社内標準での表現ではなく、「IT スキル標準」の用語で表現する事を意識しました。一旦、文章を作成した上で、使用した用語が「IT スキル標準」で定められているか、意味が同じであるかという点を意識して加筆修正を行いました。(ITA　O 氏）

【社外活動への取り組み】

・IT スキルを客観的に評価できる社外論文やフォーラム講演などは、エビデンス含め提出することができるため、合格に有利に働くと思います。申請者(予定者含む)は、特に意識した社外活動の取り組みが必要と考えます（PM S 氏）

・プロフェッショナル貢献の記載内容に書けることが少なく、記載内容も妥当であるか不安でした。また、具体的な活動のエビデンスを求められるので、計画的に記録を残していないと難しいと感じました（ITS　M 氏）

【職種を意識する】

・職種を意識するようにしました。私は、セキュリティで申請しましたが、ついついアプリケーションスペシャリスト寄りになってしまいました。

・役割＝リーダーを意識しました。「〇〇した」だと、担当者になってしまうので、「〇〇するよう指示した」や「〇〇に気を付けるよう指導した」のような表現を用いました。(ITS K 氏)

・求められるものが職種によって違うということです。私は ITS(SC)ですが、求められるのはあくまで「技術」なのだと面接で強く感じました。日常業務でプロジェクトマネージャーを行っていると、どうしてもマネージメントの実績をアピールしがちだと思うので、職種で求められるスキルを意識して執筆することが大事だと思いました。(ITS　M 氏)

【記入方法の注意書き/サンプルの熟読】

・記入方法の注意書きやサンプルを熟読し、 要求されている記載方法を順守するようにしました。形式不備で不合格になってしまうのはとても残念なので。例えば、「2.6　スキル熟達度チェックシート」では、スキル項目ごとに、実績 1 か実績 2 かを明記し、とあるので、以下のように記述をしました。

「実績 1 では、〇〇をした。実績 2 では、〇〇をした。」(ITS K 氏)

執筆者・ノウハウ提供者

【本篇担当】

中電シーティーアイ　取締役人財開発センター長　松田信之（ITA）

住友電工情報システム株式会社　岡崎四郎（ITA）

【申請書ノウハウ提供】

中電シーティーアイ　インフラユニット　基盤システム部　ITデバイスG　GL　茶野木　孝宏(PM)

同　インフラユニット　プラットフォームセンター　ｽﾄﾚｰｼﾞG ｽﾄﾚｰｼﾞT　主査　宮下　修(PM)

同　ビジネスユニット　エネルギーシステム部　ITシステムG　火力T　TL　石黒　俊幸(PM)

同　インフラユニット　基盤システム部　ｲﾝﾌﾗｺﾝｻﾙﾃｨﾝｸﾞG　GL　池田　佳裕(ITS(NW))

同　電力MSユニット　解析エンジニアリング部　流体G　解析T　専門係長　藤木　一雄(ITS(NW))

同　インフラユニット　プラットフォームセンター　ネットワークG　専門係長　豊田　太司(ITS(NW))

同　インフラユニット　ｲﾝﾌﾗ･ｾｷｭﾘﾃｨｻｰﾋﾞｽ部　情報基盤Gお客さまｻﾎﾟｰﾄT主査　水野　剛(ITS(SC))

同　インフラユニット　ｲﾝﾌﾗ･ｾｷｭﾘﾃｨｻｰﾋﾞｽ部　ｾｷｭﾘﾃｨ基盤G　SOTC　TL 中田　圭亮(ITS(SC))

同　ビジネスユニット　ﾋﾞｼﾞﾈｽｼｽﾃﾑ部　ｲﾝﾀｰﾈｯﾄｻｰﾋﾞｽGｻｰﾋﾞｽ開発T　TL　久保　壮一郎(ITS(SC))

同　インフラユニット　ｲﾝﾌﾗ･ｾｷｭﾘﾃｨｻｰﾋﾞｽ部　情報基盤Gお客さまｻﾎﾟｰﾄT　専門係長　宮部　麻里子（ITS（SC））

注）GL:グループリーダ　TL：チームリーダ

パブリッククラウドの本格利用に伴うネットワークの課題と対策

豊田　太司
(株)中電シーティーアイ

【概要】
企業ネットワークが変革の時期を迎えている。
SaaS（Software as a Service）に代表されるパブリッククラウドサービスの利用拡大に伴い、イントラネット内で処理されていたトラフィックがインターネットへ流出している。このネットワークの変化がもたらす課題はいくつかあり、既存ネットワークに何も対策を行わない状態でパブリッククラウドの利用を始めると、基幹システムが長時間停止する、レスポンスが非常に悪くなる等の思わぬトラブルにつながることがある。
本論文では、インターネット上のパブリッククラウドを本格的に利用する際に、多数の企業が直面する課題について説明すると共に、その対応例について解説する。

キーワード（パブリッククラウド、インターネット、ADC、キャパシティ管理）

１．はじめに

基幹システムをパブリッククラウドへ移行する企業が飛躍的に増えており、イントラネット内で処理されていたトラフィックがインターネットへ流出している。基幹システムをパブリッククラウドへ移行する場合、インターネットという外部ネットワークの集合体がシステムの通信経路の一部となるため、インターネットもシステムの一要素と捉えなければならない。その場合、対応しなければならないネットワークの課題が大きく分けて２つあり、何も対策を行わないまま既存ネットワーク上でパブリッククラウドを利用すると、基幹システムが長時間停止する、基幹システムのレスポンスが非常に悪くなり業務に支障をきたす等の想定外のトラブルにつながる可能性がある。

最初に考えなければならない課題としては、インターネット接続の可用性確保である。2017 年 8 月に起こった、米 Google 社の作業ミスによるインターネットの通信障害を始め、インターネット全体に及ぶネットワーク障害は定常的に発生している。インターネットは自社でのコントロールが不可能な箇所も多く、とりわけ万能なネットワークではない。それゆえに、自社で対応出来る範囲で可用性を高める対策をとらなければならない。

もう一つの課題として考えなければならないのは、インターネットへ流出する大量トラフィックへの対応である。この課題に対して何も対策を行わない状態で、パブリッククラウドの本格利用を開始すると、当該システムのみならず、他の業務システムへ影響を与えてしまう結果となる。こちらについても、現状のネットワークトポロジーにとらわれることなく、事前に対策を講じる必要がある。

本論文では、この２つの課題について、内容を説明するとともに、筆者が考える対応策について解説する。

２．インターネットを利用する際の課題

前章で触れたパブリッククラウドを利用する際に考慮が必要となる、「インターネット接続の可用性確保」、「インターネットへ流出する大量トラフィックへの対応」の２つの課題について、それぞれ内容を説明する。

２．１　インターネット接続の可用性確保

基幹システムの通信経路としてインターネットを利用する以上、インターネット接続の可用性確保は誰もが考える課題である。繰り返しとなるが、インターネットを始めとするネットワークは万能ではない。インターネットは ISP（インターネットサービスプロバイダー）が構築するネットワークの集合体であり、個々のネットワークは一企業が設計し、運営するネットワークシステムである以上、設計ミス、作業ミス等によるネットワークの停止は決してゼロにはならない。この状況を踏まえると、インターネットを通信経路の一部として利用する、ミッションクリティカルなシステムは、インターネット接続を担う ISP が長時間停止することを想定し、事前に対策を講じておく必要がある。

2017 年 8 月 25 日に、米 Google 社の作業ミスにより、インターネット全体を巻き込んだ通信障害が発生し、とりわけ日本国内の ISP は大きな影響を受けた。日本の大手プロバイダ（OCN、KDDI）でもネットワーク障害が発生し、JR 東日本、楽天証券などが影響を受けるなど、全国規模のネットワークトラブルとなった。（表 1 参照）[1]

表 1　2017 年 8 月 25 日に発生した主なトラブルの一覧

Web サイト	発生時間	障害内容
JR 東日本	12 時 30 分頃	モバイル Suica、Web サイトにつながりにくい状態
楽天証券	12 時 30 分頃	ログインしづらい状況
三重県	午後から	入札サイトが利用しづらい状況
徳島市	12 時 30 分頃	Web サイトが閲覧できない事象
GMO クリック証券	12 時 30 分頃	ログインしづらい状況
SB 証券	不明	断続的にアクセスしづらい状況
じぶん銀行	12 時 30 分頃	ログインできない事象
ジャパネット銀行	午後から	ログインしづらい状況

翌日（2017 年 8 月 26 日）、米 Google 社が作業ミスを認めて謝罪を行ったが、作業ミスの詳細な内容については公表されていない。このように、一企業の作業ミスが、日本全国規模のネットワーク障害につながってしまうこともある。また、世界規模で見ても、インターネット上においてこのような通信障害が発生している頻度は決して少なくない。[2]

このような状況のインターネットに対して、インターネット接続の可用性を高める対策を取ることは必須であり、自社で対応できる範囲で対策することが重要である。

２．２　インターネット向け大量トラフィックへの対応

もう一つの課題であるインターネット向け大量トラフィックへの対応は、パブリッククラウドを本格的に利用することで新たに発生する課題であり、対応できている企業は少ないと思われる。

これまでの一般的なインターネット接続の形態は、インターネットとの接続ポイントを１カ所に集中させる形が主流である。この形態を取ることでインターネット向けトラフィックの管理が容易になる。また、ファイアウォール、プロキシサーバ、その他情報漏洩対策等のセキュリティ機器といった、インターネット接続時に経由する機器を１カ所に集約することで、初期導入コスト、および運用コストの削減にもつながる。この従来の１極集中型のインターネット接続構成を変えない状態で大量のトラフィックがインターネットへ流出した場合、想定外の問題が発生する恐れがある。

真っ先に考えられる問題としては、トラフィック量の増加に伴うレスポンスの悪化である。この問題の原因は、インターネット接続時に経由する機器（プロキシサーバ、ファイアウォールなど)、もしくはインターネット接続回線のいずれかが性能限界となっていることが多く、既存システムも含めて影響を受けてしまう。(図１参照)

他に考えられる問題として、インターネット向けセッション数の増加が、同じ経路を利用している既存システムへ悪影響を及ぼすことがある。こちらは、セッション数が増えるにつれて、徐々に業務システムのレスポンスが悪化していき、利用者からの苦情によって気づくといったケースが多い。また、対処が必要となった場合、TCP/IP 関連のパラメータの一部に原因が潜んでいるなど、調査および対応に時間がかかることも多い。

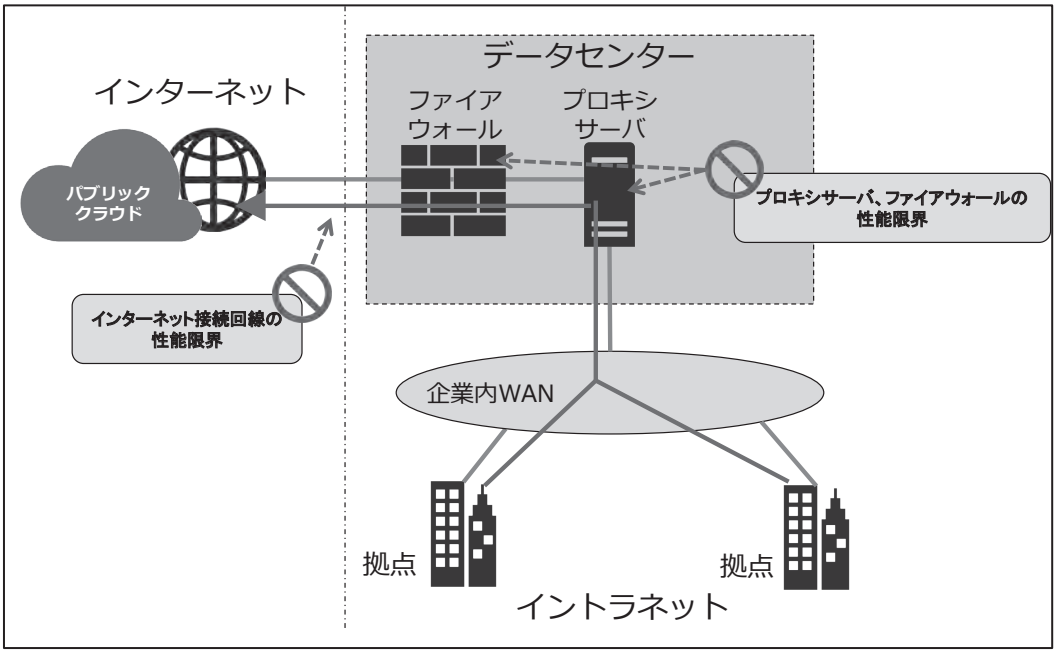


図１　従来の１極集中型のインターネット接続

これらの問題を放置したまま、パブリッククラウドの本格利用を進めてしまうと、遅かれ早かれ、前述した問題に直面し、右往左往することになる。そのような事態になる前に、増加するトラフィック量、セッション数の試算を行った上で、対策を講じる必要がある。

３．課題への対応方法

前章で述べた「インターネット接続の可用性確保」、「インターネットへ流出する大量トラフィックへの対応」の２つの課題に対する対応方法について表にまとめる。（表 2 参照）

どちらの課題についても対応の流れとしては、「インターネット回線の冗長化」、「アプリケーションごとの経路制御」、「インターネット接続回線のキャパシティ管理」という順序で対応を行うことになる。

これらの３つの対応方法について、事項から順に説明する。

表 2　対応方法と課題に対する効果

No	対応方法	課題に対する効果		具体的な対策
		インターネット接続の可用性確保	インターネット向け大量トラフィックへの対応	
1	インターネット接続回線の冗長化	インターネット接続の可用性向上	負荷分散によるボトルネックの緩和	信頼できる複数の ISP へ接続する
2	アプリケーションごとの経路制御	トラブル発生時の影響範囲を局所化	トラフィックの分散によるボトルネック箇所のコントロール	ADC 等の機器を用いて、アプリケーションごとに経由機器、接続回線をコントロールする
3	インターネット接続回線のキャパシティ管理	プロアクティブな対応による障害の未然防止	性能データに基づく適切な機器増強判断	アプリケーションごとのトラフィック量、セッション数を定期的に取得・分析する

３．１　インターネット接続回線の冗長化

対応済みの企業が多い対策となるが、インターネット回線を複数準備し、回線の冗長化を行うことが必要となる。こうすることで、トラフィックの負荷分散が可能となり、1 カ所にトラフィックが集中することを回避できる。インターネット回線を選択する際は、接続する ISP や接続する地域を分けることで、さらに効果が大きくなる。ただし、インターネット回線の冗長化を行うためには、何らかの手段でインターネット接続回線の振り分けを行う必要があり、ネットワーク設計が複雑になる。それが起因して別のトラブルにつながるといったデメリットもあるため、できるだけ設計をシンプルにすることも重要になる。

また、接続する ISP を決める際の判断材料の一つとしては、２．１項で述べた通信障害のような、想定外の事象を考慮した機器構成となっているかを、ISP の担当へ確認すればよい。具体的には、「インターネット全体を巻き込んだ通信障害の発生に備え、御社ではどのような対策を行っていますか？」という質問を ISP の担当へ投げかけ、その回答の納得度を判断材料にするという方法も考えられる。

３．２　アプリケーションごとの経路制御

アプリケーションごとに経由させる機器、およびインターネット接続回線を分ける対策を行うことも重要になる。この対策を行うためには、トラフィックの可視化、すなわちアプリケーションごとにトラフィックの流れを把握する作業を行った上で、ADC（Application Delivery Controller）等の機器を用いて、アプリケーション層のデータによって、通信経路を決定するといった対応が必要となる。トラフィック種別ごとにインターネット接続経路をコントロールすることで、インターネット向けに大量トラフィックを発生させる通信については、通常の通信が経由する機器をバイパスさせ、インターネット接続時にボトルネックとなるポイントを減らすと共に、トラフィックの集中によるレスポンス低下が発生しない構成とする。（図 2 参照）

この対策に加えて、トラフィックの帯域制御を行うことも有効である。専用の機器が必要となるが、回線を流れるトラフィック種別、およびその必要帯域をあらかじめ把握していれば、最優先すべき業務トラフィックに必要帯域を割り当てることで、最も優先させる業務のトラフィックを保証するといった対応も取れる。

これらの対策は、継続的に機能していることが重要である。帯域制御の設定について言えば、対象のシステムに仕様変更が入り、必要帯域の増減があった場合は、変更内容に合わせた設定修正が必要になる。せっかく設定した帯域制御の設定も、システムが撤去されているにもかかわらず、帯域制御の設定が残っている場合などは、ただ無駄に帯域を確保しているだけの設定である。そのようなことにならないように、定期的な棚卸、設定の見直しが重要となる。

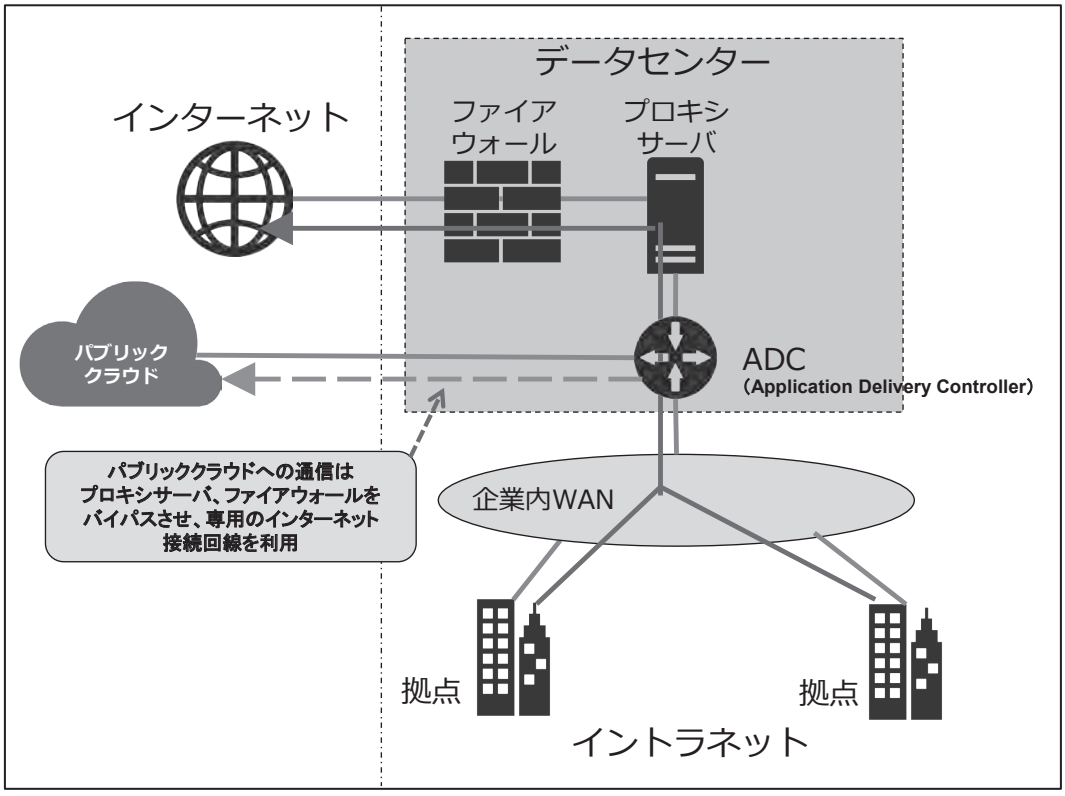


図 2　ADC を用いたトラフィックコントロール

３．３　インターネット接続回線のキャパシティ管理

ネットワーク性能データ（トラフィック量、セッション数など）を長期的に記録し、プロアクティブな対応を取ることによる障害の未然防止、およびネットワーク性能データに基づく適切な機器増強判断を行うことも重要である。

どのシステムが、どこの回線を、どの程度利用しているかを把握し、トラフィックを可視化することが最終的な目標となるが、そこまでの対応を短期間で行うことは困難である。最初のステップとしては、既存のネットワーク機器で取得できる MIB（Management Information Base）情報の範囲で、ネットワーク性能データを定期的に取得し、過去のデータを調査できるようにしておくことができれば十分である。

最近のネットワーク機器であれば、通信する TCP ポート番号ごとに、ネットワーク性能データを取得できる機器もあるため、該当するネットワーク機器の MIB 情報を調査し、既存の性能管理システムに登録することで、即座に対応することが可能である。

定常的にネットワーク性能データを収集することで、ベースラインとなる平常時の状態を数値で把握することができる。また、大量に増えるトラフィック量、セッション数を踏まえ、定期的なデータの確認を行い、必要であれば機器の増強などの対応を取ればよい。

本章では、「インターネット接続の可用性確保」、「インターネットへ流出する大量トラフィックへの対応」という２つ課題に対して、「インターネット接続回線の可用性確保」、「アプリケーションごとの経路制御」、「インターネット接続回線のキャパシティ管理」という３つの対策を順に説明してきた。これらの一連の対策は、一度対応したら終わりではなく、定期的に対策内容の評価、見直しを行うことも重要となる。

４．まとめ

本論文では、パブリッククラウドの本格利用を開始する際に考慮が必要となるネットワークの課題、およびその対応方法について解説を行ってきた。

パブリッククラウドの利用拡大に伴い、企業ネットワーク設計を根本から見直す時期に来ているが、対応出来ている企業は少ない。これは既存システムへ影響を与えないことを最優先に考え、10 年以上も前に設計したネットワークトポロジーをなるべく維持し、企業ネットワークの根本的な見直しを先延ばしにしてきた結果である。

しかし、トラフィックの流れが、大きく変わろうとしている今、企業ネットワークを根本的に見直す以外に、利用者全てが幸せになる選択肢は見つからない。ネットワークのトポロジーを見直すと、既存システムへ大きな影響を与える結果につながることがあるため、足踏み状態になりがちであるが、長期的なシステム導入計画を考慮した移行設計を行うことで、システム側への影響を最小限にすることはできる。この機会をチャンスと捉え、一歩を踏み出すことにより、利用者満足度の高いネットワーク環境の構築を目指すべきである。

これまでのネットワークエンジニアは、共通インフラのエンジニアとしてサポート役に徹し、表舞台に立つことは少なかったように思うが、現在のシステムはネットワークなしでは考えられず、システムの構築プロジェクトにおいて重要な役割を果たすことも少なくない。AI（人工知能）やビッグデータといった最新技術の活用についても、ネットワークの信頼性に依存するところが

大きいと思われ、ネットワークエンジニアの仕事は、ますます忙しくなっていくと予想される。

最後に、これからネットワークエンジニアが学ぶべきスキルについて考えてみた。SDN（Software Designed Network）や、API（Application Programming Interface）を利用したネットワーク機器の運用管理などの普及により、プログラミング技術が重要になることは誰もが想像する所であるが、トラフィックの流れが大きく変わり、インターネット上で論理的なイントラネットの構築が始まろうとしている今、一般企業においても、ISP 事業者のネットワークエンジニアが持っているような、インターネットルーティング等の知識の習得も重要になると考える。

このような時代のニーズを素早く読み取り、どの部門に、どのような知識を優先的に学ばせるかといった戦略についても、これからの IT 企業では必要になってくると思う。

以上

著者紹介

豊田　太司（CITP 認定番号：16006338）
株式会社中電シーティーアイ
情報システムの提案、開発、構築のプロジェクトに従事。現在は主に大規模なネットワークの構築案件を担当。
高度情報処理技術者（ネットワーク、セキュリティ、IT サービスマネージャ）

参考文献

[1]http://d.hatena.ne.jp/Kango/20170825/1503655538
[2] http://www.geekpage.jp/blog/?id=2017-9-13-1
[3] BGP によるドメイン間経路制御の現状と将来：障害事例と対策
[4] 平成 29 年 8 月に発生した大規模なインターネット接続障害に関する検証報告
[5] これまでの常識は捨てるべし！ クラウド時代の理想の企業ネットとは 2017/09/26 businessnetwork.jp
[6]CITP 制度を活用した高度 IT 人材の育成 ～超スマート社会を支える実践的技術者育成～
[7]ソフトバンク（IT 統括）の人財育成について

ITSS レベル判定からの脱却
iCD と PBL を活用した IT 技術者育成体系の再構築

高綱理恵† 伊藤秀行 † 宮田利昭† 松田信之 ††

要旨

・日本のソフトウェア業界の人材育成は 2002 年に IT スキル標準（ITSS[1]）が発表されるまで、プログラミング言語を教えた後は OJT（On-the-Job Training）でカバーするという非体系的な教育がなされてきた。
・大手 SIer 向けに作られた ITSS は大企業を中心に導入が進んだが、中小のソフトウェアハウスや情報子会社の多くは自社業務との不適合を理由に導入を断念しており、現在でも体系的な人材育成が図られていないと推測される。
・情報子会社である弊社でも ITSS 自社業務に合うように改変し導入してきたが（CPSS[2]）、「レベル判定の仕組み」が心理的な反発や見做し判定などを招き活用度が高まらなかった。
・そこで「人財育成のしくみ」として再構築するために現場技術者を中心とした CPSS 改訂プロジェクトを発足させ 3 年に亘り検討をおこなってきた。そこから見えてきた課題と改訂の方向性を報告する。

1．日本の IT 教育

日本の IT 産業に詳しい同志社大学中田喜文教授[1]から戴いた古い日経新聞の記事がある。1992 年 6 月 6 日に慶應義塾大学大岩元教授の「日本のソフト技術者　専門教育充実の必要」という記事で下記要旨が書いてある。

- *日本のソフトウェア業界の教育は最低限必要な PG 言語の文法のみを教えそれ以降は OJT に頼ったが、これは日本語が話せない外国人に最低限の日本語文法を教え新聞記事を書かせるようなものである。*
- *日本の大学では体系的なコンピュータ科学を教えられる教官が育っていない。*
- *CMMI を開発したカーネギーメロン大学のハンフリー教授は日本の IT 業界を視察し、少数大企業のソフトウェア品質は良いがそのほかのソフトウェアハウスの殆どは最低品質のプロセスだと指摘。*

経済産業省は 2002 年に IT プロフェッショナル人材育成を目的とした ITSS を公開[2]、以降大手 SIer を中心に ITSS の導入が進んだが、IT 企業全体としては 28%に留まっている。約 40%の企業がその理由として「ITSS が自社の業務と不適合」を挙げている[3]。SI ビジネスにより発展した日本のソフトウェア産業は、大手 SIer をトップに子会社、孫会社に下流工程をアウトソースする下請け階層型構造が形成されてきた[1]。また、ユーザ企業も情報子会社を設立し IT 業務のアウトソース化を進めた。こうした子会社や中小のソフトウェアハウスでは、小規模の開発や保守・運転業務が中心となり、大手 SIer を中心に作られた ITSS では業務自体が合わなかったのである。

†㈱中電シーティーアイ　人財開発センター　名古屋市
†† 同上　CITP
1) Information Technology Skill Standard
2) Chuden CTI Professioinal Skill Standard

２．中電シーティーアイにおけるスキル標準導入の経緯

弊社においても 2006 年に社外サービスを用いた ITSS 診断で技術者のレベル把握を開始したが、実業務（システム保守、解析業務）とのギャップ等から活用が滞っていた。そのため 2010 年より**現場の実業務に合わせたスキル標準（初版 CPSS）**を作成し運用してきたが、これも現場の活用意欲は高まらなかった。CPSS を**「技術力の共通のものさし」**として導入したため、測ること、つまり社員のレベル判定ばかりに労力を割いてしまい、肝心な研修体系の整備が行われなかった。また、現場からすると「レベル判定の仕組み」とみなされ心理的な反発や見做し判定などを招き信頼を得られなくなってしまった。そのため、2015 年の電力自由による経営環境の変化を契機とした長期ビジョンの策定を機に、**「人財育成の体系的な仕組み」**としての**改訂版 CPSS** の策定プロジェクトを開始した。ビジョン達成に必要なタスク、そのタスクを実行できる高度 IT 人材と必要数などを改めて洗い出し、現場技術者と膝を詰めて 3 年に亘り検討をおこなってきた。そこから見えてきた課題と改訂の方向性を以下に整理する。

３．CPSS の課題

（１）コンサル委託…＞現場自らが策定

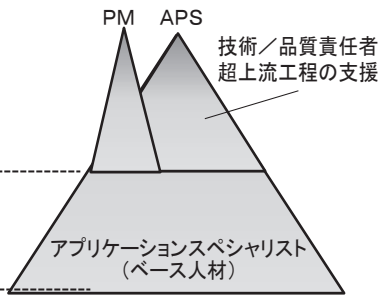
初版 CPSS は現場の負担軽減と短期に全社展開するため、策定をコンサル会社に依頼した。現場ヒアリングをベースにコンサル側で原案を策定し、現場代表者会議で承認するという形をとったが、社員自らが作業や検討を行っていないため、「与えられた基準」という感がぬぐえなかったことも活用を阻害する一因であった。

そこで今回は試行部署を決め、現場の技術者自らが **i コンピテンシディクショナリ（iCD）**[4]を基に必要なタスクを洗い出し、必要スキルを定義していった。そのため作成に 2 年余の歳月を要したが、「自らが作った基準」として納得感を得られることができた。

（２）開発・保守全てを経験できない…＞職種から専門分野へ細分化

当社は保守・運用をベースに再開発を担うことがコアビジネスであり、アプリケーションの開発・保守の上流から下流までを主導的に担うアプリケーションスペシャリスト（ＡＰＳ）をベース人材として位置づけている。技術／品質の責任者やお客さまの超上流工程（企画、要件定義工程）を支援する人材をＡＰＳのハイレベル人材（シニア、エグゼクティブ）として位置づけ、プロジェクトマネージャ（ＰＭ）はＡＰＳの中からＰＭ適性に優れた人材を育成するキャリアフレームワークを設定している。また、レベルはﾍﾞｰｼｯｸから ｴｸｾﾞｸﾃｨﾌﾞの 5 段階に設定され、中核的人財として入社 10 年を目安にアソシエイトが設定されている(図 1)。**図１　初版 CPSS の概要**

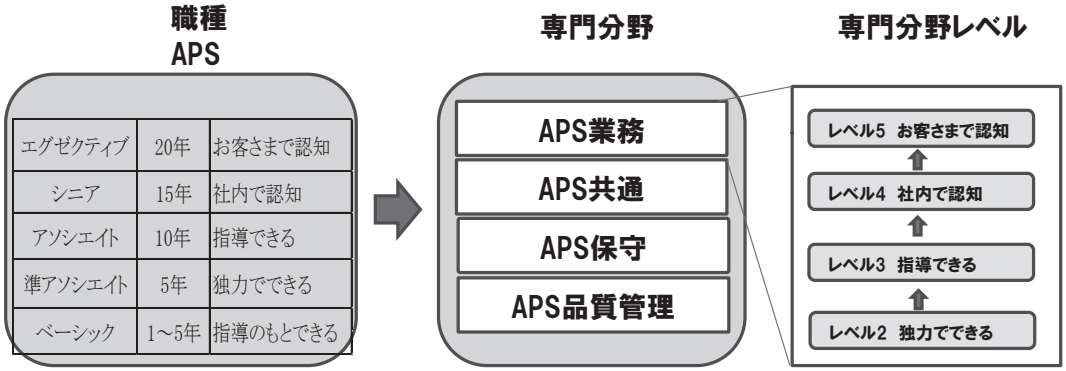
レベル名	位置づけ	入社経年（標準目安）	能力概要	ITSS
エグゼクティブ	ハイレベル人材（CCP認定）	20年	お客さま(中部電力等)で認知されている	L6
シニア		15年	社内で認知されている	L5
アソシエイト	中核的人材	10年	指導できる	L4
準アソシエイト	キャリア育成期間	5年	独力でできる	L3
ベーシック	基本育成期間	1～5年	指導のもとできる	L2 L1



しかしながら、情報子会社として開発より保守件名が圧倒的に多い中、上流工程（要件定義）やプロジェクトマネジメントを経験できる社員は限られ、開発・保守両方を全て経験することは現実的には不可能に近かった。そのため一部に経験できていないスキルがあるにも拘わらず、入社年数を目安としたレベル認定には必要なため、上司が「総合的に勘案し経験あり」として判定するようになった。初版 CPSS が育成ではなくレベル判定の制度と見做されれば、このような事態は避けられず、制度設計自体に問題があったといえる。

この反省を踏まえ現場技術者を中心とした今回の改定プロジェクトでは、開発・保守全ての業務経験を問うのではなく、有期で経験できかつ専門性がある業務群に分解した**専門分野**を定義し、それを難易度に応じた**レベル**で診断するようにした(図２)。

図２　職種から専門分野への細分化



（３）診断項目として iCD を採用…＞スキル・経験の標準化より正確な把握が可能に

専門分野のスキルレベルの把握には、最新の iDC を採用した。初版 CPSS では PM 経験のない技術者が保守の「要件定義」や「時間管理」を PM の「ｽｺｰﾌﾟﾏﾈｼﾞﾒﾝﾄ」や「ﾀｲﾑﾏﾈｼﾞﾒﾝﾄ」と解釈する例が多かった。しかし技術者自らが iCD をベースに専門分野基準を策定していく中で、**用語の意味の理解とその共通認識**ができるようになり、保守業務における「要件定義」や「時間管理」が PMBOK で定義される「ｽｺｰﾌﾟﾏﾈｼﾞﾒﾝﾄ」や「ﾀｲﾑﾏﾈｼﾞﾒﾝﾄ」とは異なるという理解が共有された。iCD を利用することでプロジェクトマネジメントや要件定義でのスキル把握がより正確に把握できるようになった（図 3)。

図３　iCD によるスキル診断項目とスコア定義

カテゴリー	タスク大項目	タスク中項目	APS業務 レベル5	APS業務 レベル4	APS業務 レベル3	APS業務 レベル2
開発工程	企画	現行業務の調査・分析	7	4	1	
		新業務モデルの作成	7	4	1	
		システム化方針の検討	7	4	1	
		システム化方針の立案	7	4	1	
		レビュー	7	4	1	
		まとめ	7	4	1	
	要件定義	業務要件	7	7	4	1
		機能要件	7	7	4	1
			7	7	4	1
		非機能要件				
		システム構成				
		費用見積	7	7	4	1
		レビュー	7	7	4	1
		まとめ	4	4	4	1
	基本設計	システム方式設計	1	1	1	1
		ソフトウエア要件定義	7	7	7	4
			7	7	7	4
			7	7	7	4
			1	1	1	1
			1	1	1	1
			1	1	1	1
			1	1	1	1
		費用再見積り	1	1	1	1
		レビュー	4	4	4	1

スコア
０：経験なし
１:指導の下実施した経験あり
４：独力で実施した経験あり
７：指導した経験あり

４．CPSS 改訂の方向性

（１）職種としてのレベル判定より専門分野／レベルの可視化

先ほども述べたように、開発より保守件名が圧倒的に多い情報子会社では上流工程（要件定義）やプロジェクトマネジメントを経験できる社員は限られている。また、共通班（標準化やデータ管理等）も専門性が必要であり、経験豊かな技術者に固定することでリスクを低減する傾向がある。こうした技術者個人の特性により専門性を積んでいくことは、すべての技術者が平等により深く、より広く経験を積んでいくことより現実的である。会社にとって重要な事は、**①将来必要な技術者の目標を大まかに把握し、②現在の技術者レベルの可視化を行い、③目標に向けて計画的に育成する**ことである。

これまで初版 CPSS では入社 10 年後の中核人財としての「アソシエイト」診断が重要な位置づけと認識されていた。筆者らはこれが逆に正確な診断と計画的な育成を阻んできたと推測する。**「アソシエイト」のような呼称を廃止し、技術者の専門分野／レベル管理を充実する**ことも改定のひとつのオプションである。

（２）モチベーション向上のための社外認定制度の活用

レベル呼称を廃止する場合、モチベーション対策はどうすべきだろうか？　筆者らは情報処理学会が平成 26 年度に創設した認定情報技術者（CITP）をその代替とすることを提案したい。CITP 制度は「高度な能力を持つ情報技術者を可視化し、その社会的地位の確立を図ること」[5]であり、以下の特徴を持つ。

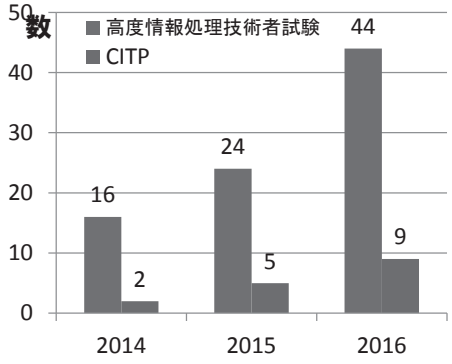
・IFIP-IP3より国際的な高度IT人材プロフェッショナル資格制度の認定取得(2018年2月)。

・継続的研鑽（CPD: Continuing Professional Development）による資格の3年更新

特に継続的研鑽は、これからの超スマート社会において最も重要な能力となり、CDP ポイントによる 3 年更新は学ぶモチベーション維持に役立つ。

弊社では平成 27 年度より CITP 取得支援制度を創設し、これまでに 21 名が個人認証されており、自社内のコミュニティ活動も活発に行われている(図 4)。

図４　中電シーティーアイ　CITP 認証数



４．体系的な研修の整備

（１）PBL をベースとした体系的な IT 実践研修の整備

冒頭に述べたように日本のソフトウェア業界では非体系的な OJT ベースの研修が長く続いてきたが、当社でも初版 CPSS 導入時に研修体系が整備されず同様な状態にあった。

OJT は重要であるがそれだけでは進化の激しい IT 業界では取り残されてしまう。特にソフトウェア工学に関する研究組織をもたない企業では現場で使われている技術の可視化や向上は難しい。そこで当社では業界最新の**プロジェクトベースドラーニング（PBL**: Project-Based Learning）研修を取り入れた**「IT スキル系研修受講モデル」**（図 5）を体系化し、下記を狙いとして平成 30 年度より提供開始する予定である。

①最新 IT 知識･スキルの体系的習得（OJT の補完・支援）

②学び･考え続けることの習慣化

③入社 3 年間で共通的に必要な基礎実践力を習得

④大学教育のプロジェクト疑似体験が低いための補強

図５　IT スキル系研修受講モデル

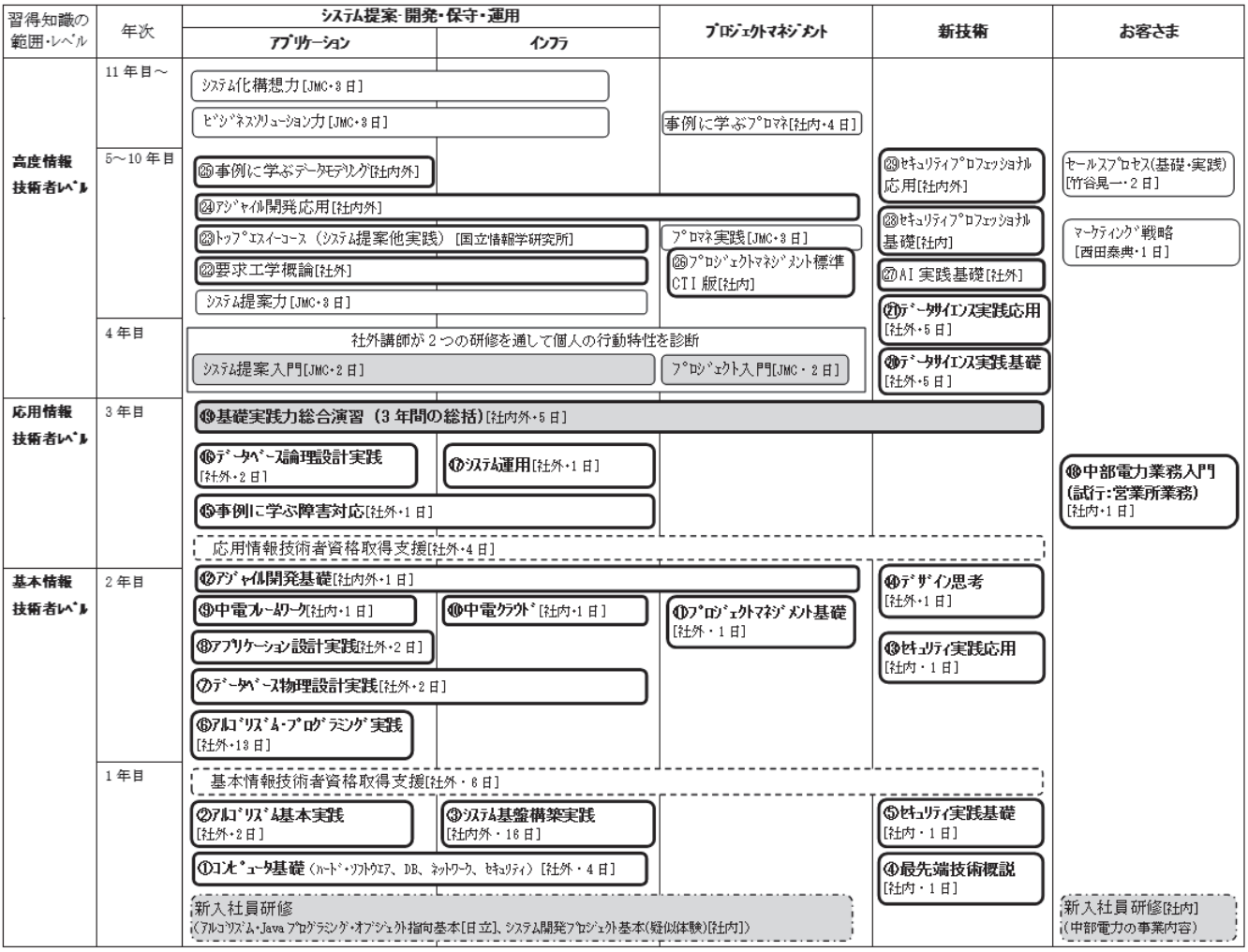


図６　基礎実践力総合演習のカリキュラム

概要	項目	ポイント（演習カリキュラム）
入社3年間で学んだ知識･スキルの総括(プログラミングは対象外)	機能設計	要件定義との整合性･画面･機能･データ･条件/動作テーブル
	方式設計	アプリ形態･オンライン処理･バッチ処理･共通処理
	結合テスト	プロセス単体･システム間連携
	総合テスト	機能要件･非機能要件

（２）ビジネススキル系研修体系

当社ではコンサルティング業務などより付加価値の高いビジネスの拡大を目指しており、それに必要なビジネススキル体系を下記の考え方で整備している。(図 7)。

・入社 3 年目までにビジネススキル基礎（文書表現力、論理的思考、問題解決）を学ぶ

・重要なビジネススキルは基礎から応用までを段階的に繰り返し学ぶ

図７　ビジネススキル研修体系

年齢		文章力	論理的思考	問題解決	コミュニケーション
C級			論理の構造化（上級）	問題解決（課題設定型）	ネゴシエーション
S級	4年目～	文章表現力向上	論理の構造化（中級）	問題解決（問題発生型）	プレゼンテーション
	2～3年目	文書作成個別指導		問題解決（初級）	
	新入社員	文章表現力向上	論理的思考		

（３)情報学の必要スキルをカバー

平成 28 年日本学術会議は学問として「情報学分野」を策定し情報学に必要なジェネリックスキルとして**論理的思考、問題発見、課題解決、コミュニケーション、リーダーシップ**などを挙げ、従来の講義・演習に加え**プロジェクト学習（PBL：ProjectBasedLearning）**も必要と提言している[6]。今回作り上げた IT スキル研修体系とビジネススキル研修体系は情報学の要求を満たしている。

おわりに

平成 27 年度から専属要員 2 名を充て CPSS 改訂のプロジェクトを進めてきた。2017 年 4 月 1 日には IPA より iCD 活用ゴールド企業認証を戴いたが、それ以上に手ごたえを感じるのは現場技術者と一体で 3 年間にわたり育成体系の基礎を作り上げてきたことである。詳細な制度はこれからになるが骨格は納得いくものであり、実践的な研修体系と合わせ高い活用が期待される。改めて試行部署のみなさんには感謝を申し上げたい。

以上

[1] Yoshifumi Nakata
http://www.haas.berkeley.edu/groups/online_marketing/facultyCV/papers/Cole_Robert_The_Japanese_Software_Industry.pdf
[2] https://www.ipa.go.jp/jinzai/hrd/index.html
[3] IT 人材白書 2012 独立行政法人情報処理推進機構（IPA）2012 年 5 月
[4] https://www.ipa.go.jp/jinzai/hrd/i_competency_dictionary/index.html
[5]旭寛治(2014)「認定情報技術者制度(1)－制度の概要－」『情報処理』第 55 巻第 8 号
[6]大学教育の分野別質保証のための教育課程編成上の参照基準　情報学分野
平成 28 年 3 月 23 日　日本学術会議情報学委員会情報科学技術分科会

CITP 制度とは

2014 年に情報処理学会が創設した高度ＩＴ資格制度で、「高度な能力を持つ情報技術者を可視化し、その社会的地位の確立を図ること」を目的にしています。具体的にはITSS（IT スキル標準）レベル 4 以上の上級技術者を認証します。また 2018 年 2 月にIFIP（情報処理国際連合）の高度 IT 人材相互資格認証組織である IP3 の認定を非英語圏で初めて取得しグローバルに通用する資格になりました。個人を対象とする個人認証と企業を対象とする企業認定があります。

https://www.ipsj.or.jp/citp.html

CITP コミュニティ

CITP 認証者有志によりかねてより経済産業省産業構造審議会等で提言されていた高度 IT 人材育成のためのプロフェッショナルコミュニティが形成されました。CITP 同士の交流を通じた自律的な質の向上や社会提言、外部の審議会・委員会等への参画、情報分野における人材育成や地域活動などの社会貢献を目的に活動しています。

https://www.citp-forum.ipsj.or.jp/

CITP 資格取得者　約 7,500 名

取得者一覧　https://www.ipsj.or.jp/CITPholders.html

CITP 認定企業

エヌ・ティ・ティ・コミュニケーションズ株式会社およびそのグループ会社
エヌ・ティ・ティ・コムウェア株式会社
ニッセイ情報テクノロジー株式会社
日本電気株式会社およびそのグループ会社
株式会社日立製作所およびそのグループ会社
富士通株式会社およびそのグループ会社
三菱電機インフォメーションシステムズ株式会社
NTT テクノクロス株式会社

一般社団法人　日本情報システム・ユーザー協会（JUAS）

ホームページ　https://www.juas.or.jp/

アドバンスド研究会　http://www.juas.or.jp/activities/outline/advanced/

表紙絵　古澤優子　「**草原の家**」
１９６８　埼玉県生まれ
１９８８　東京芸術大学美術学部日本画専攻卒業　安宅賞受賞
１９９２　東京芸術大学美術研究科修士課程絵画専攻日本画修了
２００２　上野の森美術館大賞展　一次賞候補
　　第２回トリエンナーレ豊橋　星野眞吾賞展
２００６　第 17 回臥龍桜大賞展（岐阜県美術館、他）
２００７　「福」屏風展　SAKURA FESTIBAL(サンフランシスコ)
　　第 18 回臥龍桜大賞展（岐阜県美術館、他）
その他、多数
（ハイマックス　土屋俊樹氏推薦）