デジタル庁
「デジタル化社会の中長期展望に係る調査研究」
有識者グループインタビュー
意見書

2023/10/24

登 大遊

添付資料

【資料 1】日本型組織 (政府・企業) を活かしたサイバー人材育成・技術研究の方法

第 1 節　アジェンダ 1: 2030･40 年においてメガトレンドはどのようになっているか ？

1　欧米で製品化された不完全な技術は、日本に 30 年以上遅れてやってきて開花し、高品質に大成する

欧米で製品化された不完全な技術は、日本に 30 年以上遅れてやってきて開花し、高品質に大成する。

> 半導体: 米国 1950s ⇒ 日本 1980s
> コンピュータハードウェア: 米国 1950s ⇒ 日本 1980s
> テレビゲーム: 米国 1960s ⇒ 日本 1990s
> より古くから、造船、鉄鋼、化学、家電、自動車等も同様であった。

現代型 OS 群 (モダン OS、クラウドシステム、ネットワークシステム、セキュリティシステム) が、2000 年代に米国で製品化された。

> ⇒ したがって、2030 年代に、モダン OS、クラウドシステム、ネットワークシステム、セキュリティシステムが、日本で開花し、高品質に大成する。

シリコンバレーの現代の技術者集団は、システムソフトウェア技術を強力な基礎として有していて、その上にアプリケーション層も立ち上げ、その二面で同時に活躍している。

> ⇒ したがって、2030 年代に、日本版シリコンバレーが誕生する。システムソフトウェア技術を強力な基礎とし、その上にアプリケーション層も立ち上げる。日本人技術者集団は、その二面ともに世界中で中心的責任を果たし、米国発祥のソフトウェア技術を安定的に完成させる。

2　日本が生み出すメガトレンド技術とは、どのようなものか

日本は、全く新しい技術を生み出すというよりも、どちらかというと、既存の外来技術を磨き上げ、高品質化・高信頼性を実現することが得意である。まあだいたいは地味な話である。日本人が生み出すものは、それほど、画期的という訳ではない。しかし、世界中で最も高品質で優れたなものとして、すすんで選択されるのである。

以下は、全世界的な爆発的需要の確実性が高いものの一例である。これらを日本人は作ることができるようになる。これらを作るための技術的基礎体力を、日本人集団は、実はすでに身に付けているのである。

ア. 新たな安全なパブリッククラウド技術

- 一極集中問題の解決
- マルチクラウドを安全簡単に分散利用できる仕組みの実現【第 3 章参照】
- 現在の外資系パブリッククラウドサービスと同等のサービスを誰でも構築できる技術
- 2030 年代までに発生し得る深刻なクラウド・ショックを予防・解決

イ. 重要システムにおけるシステムソフトウェアを数十年間安全に運用できる技術

- EoL となった古い Windows / Linux、データベース等を 40 年間保たせる技術
- 開発元がメンテナンスせず、ソースコードも非公開の購入済みソフトウェアを、ユーザーが自由・簡単に改造してゆく技術

ウ. 100 年間安定して使えるコンピュータネットワーク技術や装置

- PC における Windows のような存在、スマホにおける Android のような存在の、ネットワーク機器バージョン

今は、ネットワーク機器とソフトウェアは強度に結合してしまっている。どのベンダでもネットワーク機器に組み込んで出荷でき、アプリ・マーケットも有するネットワーク OS が日本から登場するであろう。

第 2 節　アジェンダ 2: 課題・機会の解決に向け、2030・40 年に向けデジタル分野で実施すべき取り組みは何か？

1　日本の役割

日本の役割は、せっかちで脆い不確実な現代世界の IT・デジタル環境を日本製技術によって改良し、長期的平和・安寧を実現することである。

これまでの IT・デジタル環境を支えるシステムソフトウェア技術は、実験的・短絡的に技術者の好奇心本位で生み出されている、未成年の不良学生のようなものである (攻撃的で短気的な米国 IT 事業者とその技術者集団の行動を見よ)。

これが、成人として安定成長し、やがて社会を真に安定して支える程度に至るには、日本が、米国由来の IT 技術を完成させ、平和・中立的な供給者として全世界に普及させ、世界の IT 化に貢献する必要がある。

日本人の IT 技術者集団と事業者集団は、未だその存在が世界的に認識されていないけれども、水面下で秘かに蓄積増大している、21 世紀最大の、驚異的な氷山下に韜晦(とうかい)する楽隊のようなものであり、世界中はその出現に震撼するであろう。

2　日本版シリコンバレーの出現（2030 年～）における行政機関の役割

既製品に頼らず、官僚と技術者たちが一生懸命問題解決・技術開発に取り組むことで、良い技術が埋まれ、これが世界を塗り替える。

(1)　米国の歴史

米国の歴史をみると、行政機関の課題である大規模計算処理・大規模通信処理を実現しようとして、既製品に頼らず、官僚と技術者たちが一生懸命技術開発に取り組んだ結果、現代型コンピュータシステム (ロスアラモス研究所でのノイマン型コンピュータの開発)、現代型インターネット (国防総省での研究用コンピュータ 3 台の接続が発端) が出現している。

その上で、巨大企業の課題である事務処理 (文書処理) を実現しようとして、既製品に頼らず、社員たちが一生懸命技術研究に取り組んだ結果、現代型 OS であ

る UNIX (AT&T 電話会社における文書処理システム開発が発端) が出現している。

さらに、その上で、巨大企業の課題である大量コンピュータリソース管理を実現しようとして、既製品に頼らず、社員たちが一生懸命技術研究に取り組んだ結果、現代型クラウドである AWS (Amazon Web Services) が出現している。

(2) 日本のこれからの現象

これと同じことが、日本でも発生する。

日本の行政機関は、巨大な情報処理の問題を抱え、大規模なコンピュータネットワークと優秀な人材を擁し、リソースに溢れ、これらを解決しなければならない状況にある。

よって、歴史の法則に基づき、既製品に頼らず、官僚と技術者たちが一生懸命問題解決・技術開発に取り組むことで、良い技術が埋まれ、これが世界を塗り替えるであろう。

(3) その後の歴史

日本人は、現在全世界で不足している、高品質なシステムソフトウェアの構築手法 (たとえば、どのようにすれば、Windows や AWS のような高度複雑なシステムソフトウェアの主要部分が作れるのか) を体系化し、日本語文献にまとめていく。これらは現在米国企業の現存技術者集団の頭脳に存在する秘伝のタレのようになっていて、彼らとしてもいまいち体系化していないから、大いに価値がある。日本人の作り上げた体系化文献群は、英語化・アジア語化され、アジアの国々の方々もやがて同じようなものを作り出すことができるようになる。

3 デジタル庁の役割

(1) **国の情シス ― 安全・確実なマイグレーション、アプリ開発 ―「厳格なシステム」**

これは、急ぎの仕事である。2030 年頃までに完成をさせることである。

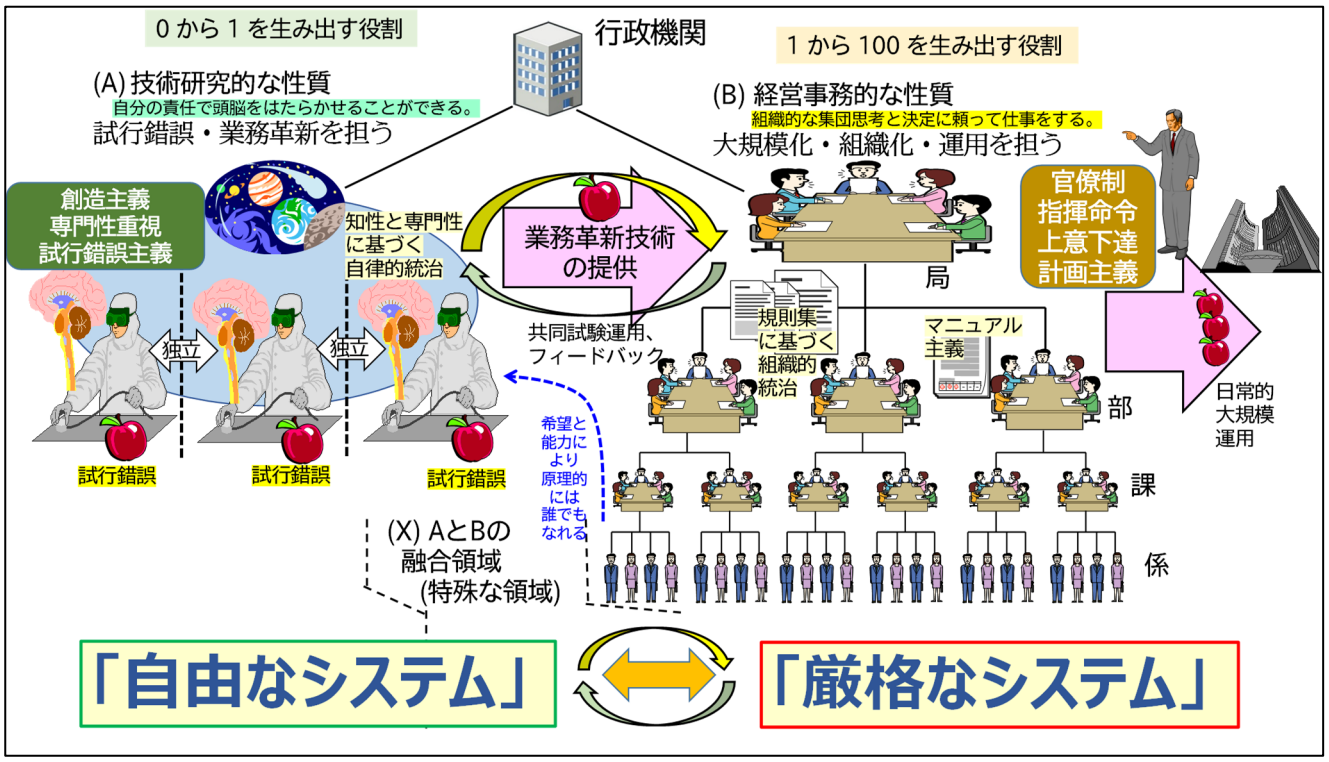
既存の省庁の NW、自治体の LGWAN を、安全確実に移行して延命させ

ることである。

(2)　**新技術の研究の土壌 ―「自由なシステム」**

これは、ゆっくりとした仕事である。2030 年以降に大いに発達をする日本版シリコンバレーの出現につながる土壌を作り始めるのである。

豊富なリソース、優秀な人材、多様な組織 (省庁・独法・地方自治体) において、米国の歴史上 IT 技術を生み出した程度の好事家を自由的秩序の元に活躍できるようにし、官民併せて、各種の技術開発が多様に並列して試行錯誤するようにして、日本版シリコンバレーの出現臨界点に足る技術をいくつか生み出す。具体的な方法の提案は、【資料 1】参照。



「自由なシステム」と「厳格なシステム」

上記 (1), (2) の役割は、時間軸・目的・価値・人材の水準が全然異なる。長期的には単一の目的であっても、当初は、異なるものである。(1), (2) を同一視して議論しようとする限り、前進は困難である。(1) は厳格な思想、(2) は自由な思想を基礎として、両方を同時並行に進めることになる。

「デジタル敗戦」という用語がしばしば政府関係者 (特に政治家)・報道機関によって用いられるが、上記 (1), (2) の概念が異なることを理解されていないようであり、混乱がみられる。米国・中国などの IT 技術立国に対比した遅れを意味する (2) を解決すること、日本版シリコンバレーの出現を願うことこそが、「デジタル敗戦」という言葉に集団的に込められている高水準の意義である。ところが、そのためにいくら (1) の方向性のみ考えても、これは、低水準の意味 (行政電子申請 Web アプリが貧弱等) だから、話が全然噛み合わないのである。これを理解した上で、的確な方向性を提示できた政治家は、日本中の技術系・人文系の両方の人材から評価され、トップクラスの支持を得られる。

われわれは、今や (1), (2) の 2 つの性質の違いを正しく認識するに至った。これから、(1), (2) の一方をもう一方に包含することなく、分散並行して両刀的に進めれば、必ず、日本は、すでに一位に輝いた各種の産業と同様に、IT 技術においても、再び世界一位の地位を譲り受けることができるのである。

第 3 節　【付録】クラウド・リスク ― クラウド・ショック

1　パブリッククラウドの有する未解決のセキュリティリスク

まず、現代型の大規模集約型パブリッククラウドサービスには、現在の技術水準の限界により、以下の未解決のセキュリティリスクが存在する。

(1)　可用性リスク ― 「クラウドサービスが壊れて、自社のデータが取り戻せない」

意外にも、データの所有権という法的概念は未だ存在しない。企業によるデータの権利を確実に保全するには、データを記録しているディスク装置という「物」の所有権を維持する必要がある。物の所有権は、「物権」と呼ばれる。物権は、大変強い。物が存在する限り存続する、絶対的な権利である。ディスク装置の物権としての所有権を確保しておくことが大切である。停電、災害、通信障害により、通常利用しているデータセンタが停止したとする。それでも、経営者は安心していられる。オンプレミス型システムでは、ディスクの所有権をユーザーが有しているからである。ユーザー企業は、堂々とデータセンタに入っていって (停電や認証システムが故障した場合なら、手動でドアを開けてくれるであろう)、自らのラックを開錠し、サーバーやディスクという「物」を取り出し、そのディスクを本社や庁舎に持ち帰ってデータを取り出したりして、業務継続が確実に可能である。極端には、データセンタ事業者がディスクを返してくれなければ、裁判所で返せという判決を得て、執行官を連れて行って、データセンタのドアをこじ開けてもらい、ディスクを取り返すこともできる。データセンタが倒産しても、ディスクは返ってくる。

これに対して、パブリッククラウドにおいては、ユーザーはデータをクラウドサービス事業者が所有権を有するディスク装置に書き込む。ユーザーはクラウドサービス事業者に対して、データを読み出しする権利を得る。これは物権ではなく、「債権」である。債権は、とても弱い権利である。履行してもらえるかどうか分からない。不履行があったら、裁判所に行って、履行せよという判決をもらうことはできる。しかし、それでも履行してくれない場合、現行法上、直接の強制をする手段がない。金銭による賠償か金銭制裁による間接強制で満足するしかない。クラウドサ

ービス事業者が破たんしたら、賠償も得られず、泣き寝入りになる。

パブリッククラウドにおいては、サービス障害時にはデータの所有者は、データが全然取り出せなくなる。データを書き込んでいるディスクの所有権はクラウド事業者にあり、他のユーザーを含めた複数ユーザーのデータが、1 台のディスクに、高度に重畳的に多重化されて記録されている。データセンタの障害のほか、クラウド事業者の認証システムやメタデータ管理システムのコードに誤りがあったり、障害が発生すると、「クラウドサービスが壊れて、自社のデータが取り戻せない」状態が発生する。

(2) 機密性リスク ― 「自社のデータが 10 年前から流出していた」

オンプレミス型システムでは、ユーザー企業が自らのコンピュータやディスクの所有権・支配権を有している限り、物理力 (例: データセンタへの設置と施錠) と自らの暗号化を用いて、自らの能力と責任で、確実に、機密性を維持できた。

パブリッククラウドにおいては、現在、同等の安全性は実現不能である。サーバーサイドで暗号化されて保管されているように見える全てのデータは、一見安全に見えても、クラウド事業者は、いつでも技術的に復号可能である。「毎回ユーザーが鍵を指定する方法で暗号化・復号化が行なわれる」という手法を用いても、データ暗号共通鍵そのものは一度クラウド事業者のサーバーのメモリに乗り、CPU で処理される以上、クラウド事業者は生データにアクセスできてしまう。復号化処理がクラウド事業者の有する CPU 上で行なわれる以上、クラウド事業者の最上位特権者 (基幹部分のプログラマ) は、データ暗号鍵 (これは共通鍵暗号で、ハードウェアセキュリティモジュール (HSM) を用いても保護不能である) にアクセス可能である。これを防ぐ技術的手段は、パブリッククラウドでは、実用化されていない。監査は、特権を有するプログラマに対して、ほとんど役に立たない。監査システムが監視できるのは、その監査システムの水準以下のオペレーションのみである。最上位特権者は監査システムをかわすことができる。これにより、クラウド事業者が暗号化されていないデータにアクセスことができる。また、認証部分の不具合により全世界にデータが公開されるリスクも存在する。クラウドサービス事業者の特権を有するプログラマが、過失または故意によりわずかな数ヵ所のコードの間

違いを注入しただけで、これが発生し得る。「自社の預かる顧客データが、クラウド事業者の故意又は過失により、10 年前から流出していた。」という事態が 10 年後にはじめて発見され、過去 10 年分の損害を顧客に賠償しなければならない事態が発生し得る。

上記 (1), (2) は、新規性のある話ではなく、クラウドサービス事業者や一定水準の技術者であれば誰でも知っている、既知の問題点である。しかし、ユーザー企業の経営者は知らない場合が多い。未だこの危険は現実化したことがないからである。これが現実化したときに多数のユーザー企業の経営者によって同時に発生するパニック的行動が、次の「クラウド・ショック」を引き起こす。

2 「クラウド・ショック」の発生リスクとそのメカニズム

大規模なパブリッククラウドにおいて、上記のリスクは、現在は幸運にも現実化していないが、2030 年・2040 年というような長い単位でみると、これらは現実に発生し得る。そのとき、きわめて危険な集団行動が発生する。上記のようなセキュリティ侵害が発生していることがついに表面化したとき、仮にその事件が小規模に発見された場合であっても、多くのユーザー企業は、できるだけそのパブリッククラウドから、いちはやくデータを避難させたいと考える。なぜならば、そのクラウド・スキャンダルはそのパブリッククラウド事業者に対して信用不安を引き起こすリスクが高いことは明らかで、信用不安が引き起こされたら、多数のユーザー企業がそのパブリッククラウドを利用しなくなるであろうことが各企業の経営者によって予測されるためである。それが発生すると、その大規模パブリッククラウド事業者の収入は激減し、事業継続の危機にさらされる。その大規模パブリッククラウド事業者は、データセンタの料金、電気代、回線費用、人件費を支払えなくなる。そうなると、サーバーが停止し、またメンテナンスが止まるので、データが取り出せなくなってしまう。支払困難になったパブリッククラウド事業者のサーバー群、ハードディスク群が、債権者に差し押えられるおそれもある。これは、最大限に深刻な事態である。前記のとおり、オンプレミス型システムであれば、データセンタ

が破たんしても、ユーザー企業は、所有権に基づいて自らのラックからハードディスクやサーバーを引き抜いて持ち帰ればよい (データセンタの物ではないので、債権者は、差押えできない)。しかし、パブリッククラウドの場合、ディスク装置やサーバーはパブリッククラウド事業者の所有物である。決してユーザー企業の所有物ではない。信用低下によって支払困難となったパブリッククラウド事業者に対する債権者 (たとえば、従業員や、賠償請求権を有する顧客) が差し押えたら、債権者はこれを競売にかけて換金・売却し、お金を取戻そうとする。それ以外でお金を取戻す方法がないためである。ここまでで指摘したようなことは、ユーザー企業の経営者であれば、利用しているパブリッククラウドにおいて、いざ危機が発生したとき、誰でも瞬時に思い付くに至るであろう。もしパブリッククラウド事業者が事業停止する前までにデータを取り出しできなければ、ユーザー企業自らが倒産の危機に陥る。そこで、パブリッククラウドを信用して重要な業務データ・機密データを預けてきたすべてのユーザー企業たちが、いっせいにデータを避難させようとする。他のパブリッククラウドにデータを移行したり、もうパブリッククラウドは使いたくないと考えて、オンプレミスシステムを急いで構築したりしようとする。そのためには、これまで何十年間も長い期間をかけてパブリッククラウドに少しずつ蓄積してきたデータを、すべて短時間でダウンロードしなければならない。そして、それは他のユーザー企業よりも早くダウンロードしなければならない。他のユーザー企業たちのダウンロードが終わり、契約を終了したら、パブリッククラウド事業者の収入が途絶え、そうするとダウンロード不能になる。このようなパニック状態では、一刻も早くダウンロードをして脱出をしたほうが良いという具合になる。

　このとき、何が発生するだろうか。パブリッククラウドの構造は、集約多重効果を前提に構築されている。CPU、ディスク、ネットワークなどのハードウェアリソースと、ノード管理システム、メタデータ処理システム群などのソフトウェア機構とは、いずれも、多数のユーザーが同時にフル回転させることがない前提で構築されている。CPU 消費率に対して追加課金をしたり、ディスクのリクエストに対して課金をしたり、長期保管データの読み出しに対して高額課金をしたり、データ転送リクエストに対して高額課金をしたりするのは、各ユーザーにできるだけリソー

スの回転率を低下させてもらい、ハードウェア購入コストを最小化して、大きな利益を得るためである。できるだけぎりぎりのところでこれらの装置群 (固定資産) 回転させて利益を挙げ、また、パブリッククラウド間の価格競争による値下げを耐え抜いているのである。このような、決して多数のユーザー企業が同時にリソースやシステムに負荷をかけないことが想定されているシステムにおいて、上記のような信用不安が発生し、突然に多数のユーザー企業が同時にデータを待避し始めると、コンピュータ用語でいう、スラッシングに似た現象が発生する。CPU のコンテキストスイッチの切り替え、ディスクの I/O 待ち時間の増大、ネットワークの帯域不足、認証システムやメタデータ管理システムの高負荷による不具合の発生やメモリ不足が発生する。この中で特に最初に限界点を迎えると想定されるのが、ネットワークの帯域である。パブリッククラウド事業者の弱点は、ネットワーク帯域不足である。これは、インターネット接続系でも、プライベート接続ポートでも、変わらない。ネットワークはバースト的にデータが流れるので、高帯域化を行なうと、使われていない時間のコストが増大する。また、イーサネットの技術やルーティングの技術は発展途上であり、パブリッククラウド上の多数のユーザーの本来需要を同時に収容するだけのキャパシティのあるネットワークを、現在の技術水準では、十分に分散して処理することが困難である。この制限は、光伝送の速度、装置のコスト、装置の集約率、発熱の具合、ハードウェアレベルのロードバランス技術や方式の限界によって生じる。これが原因で、集約率が高く大規模なパブリッククラウド事業者であればあるほど、ネットワーク伝送量単価が高額に設定されているのである。これは、ネットワーク通信量で利益を得たいから高額に設定されているのではない。多数のユーザーが本当に大量のネットワークを利用したら技術的に全然耐えられないので、高額な単価を設定することにより、ネットワーク帯域の消費を節約するように工夫させているのである。

ある程度の数の企業ユーザーが一刻もデータをダウンロードしようとして、ネットワーク帯域、CPU、ディスク、メタデータシステムに負荷がかかると、上記のようなリソース不足により、そのユーザーのダウンロード速度は低下する。ネットワークボトルネックが発生すると、TCP のレイヤにおける再送が発生し、速度は急

激に低下する。ディスクのボトルネックが発生すると、通常のディスクアクセスのソフトウェアの動作が遅くなったり、極めて不安定になり無応答に近くなる。この現象は、パニックを呼ぶ。さらに多くの企業ユーザーの経営者たちは、データを一刻も早く待避させるように指示をする。もはやこの状態の経営者の心理としては、そのパブリッククラウドの欠陥によるセキュリティ侵害などは、どうでも良い状態であると考えられる。それよりもパブリッククラウド事業者が破たんするより一刻も前に、データを待避させなければならない。他の企業ユーザーたちが待避させて解約する前に、自社のデータを全部待避させなければならない。しかし、数十年かけて溜め込んできたデータストレージに置いたデータの待避には、相当な時間を要する。途中で、どんどんとデータ転送速度が低下していく。これはおかしい具合だぞと考えたユーザー企業の技術者たちは、その旨をインターネットの SNS 上で周知する。これがさらなるパニックを引き起こし、いよいよ、ほぼすべてのユーザー企業がデータ待避を決意する。そうなると、もうデータ転送速度は 80kbps くらいに低下し、全然ダウンロードできなくなる。ネットワークのパケットロスによる再送と、高度密集された CPU のユーザー間の時間の奪い合い、ディスク I/O 能力不足により、システム全体の負荷は常に 100% となり、データ転送は、ほとんど停止した状態になる。この状態になると、そのパブリッククラウドサービスの復活は困難である。データはもはや永久に取り出せないか、配給制のようになり、随分先に自分の番が回ってきて初めて取り出せる。ユーザー企業は、データ取り出しに成功するよりも先にサーバー群、ディスク群を債権者が差押えられたり、従業員が給与不払いで離散したり、破産手続に移行して競売にかけられたりしないことを祈るしかない状態に陥る。長期間の停止により、社会は麻痺状態に陥る。

3 「クラウド・ショック」を解決する技術の必要性

われわれの社会は、いよいよパブリッククラウドシステムに依存しつつある。パブリッククラウドシステムは、クラウド・ショックの発生に対して大変脆弱である。したがって、われわれは、これを解決する技術を生み出す必要がある。