

# デジタル技術解説記事の サンプル記事執筆結果について

— オンライン受験システム (CBT) 技術の検証と評価手法 —

2023年2月9日(木)  
登 大遊

【背景】 2022/12/06 に、デジタル庁より以下の依頼をいただきました。

登様、1点ご相談です。年明け以降、調達なども交えて技術解説記事の検討を進めていきたいと考えておりますが、その意思決定のため、**具体的イメージが一つ必要**と考えております。ついては、もし可能であれば、御提案頂いた、**意思決定層と技術者層のどちらにも魅力がある記事**というイメージを伝えるべく、先行公募を行った講習・試験の製品を題材に、**記事のサンプル作成**をご検討頂くことは可能か、実現性をご教示頂けないでしょうか。1月中旬以降に予定される次回テクノロジー改革委にて、サンプルを交えてプロトタイピングの方向性について説明の上、記事編集を本格化する手順を考えております。進め方、必要なもの等含め、是非ご意見頂戴できましたら幸いです。

そこで、以下の目的で1本記事を書いてみましたので、大変拙劣な出来で申し訳ありませんが、サンプルとして共有いたします (この PDF の P.3 以降)。

- 対象技術の検証、実験のためのプログラムの作成、記事の執筆を、1人で約1週間の工数で書くとしたら、だいたいどの程度の分量や内容の記事になるのか測るために、自ら、実際に1本書いてみることにしました。
- サンプルなので、対象デジタル技術としては、何でも良かったのですが、ちょうどデジタル庁では、「講習・試験のデジタル化」に必要な技術から技術カタログを整備する流れになっているので (下図)、CBT 試験システムを1つ選び、これを対象としてデジタル技術解説記事を1本書いてみることにしました。

**テクノロジーマップに係る技術カタログの先行公募について**

「講習や試験のデジタル化」に必要な技術から技術カタログの整備を開始

**公募対象** 講習・試験のデジタル化を実現するための製品・サービス

**スケジュール** 9/30 (金) 公募開始 (10/21 (金) 締切)、10月下旬以降試行版として公表予定

**募集・公表方法** デジタル庁HPからフォームで応募を受け付け、デジタル庁HPでカタログ公表  
URL <https://www.digital.go.jp/policies/digital-extraordinary-administrative-research-committee/>

**ポイント** 規制所管省庁との調整を通じて明らかとなった、講習・試験のデジタル化を実現する上での様々な課題に対して、どのようなソリューションがあるか、技術保有企業からの積極的な提案を求める。

**留意事項** 技術カタログは、あくまで講習実施者がデジタル化を検討する上での参考情報を提供するものであり、カタログに掲載する個別技術について、国が認証・認可等を行うものではない。

**カタログ掲載項目のイメージ** カタログ掲載項目のイメージは以下のとおり。  
(以下は、修了試験の不正受験対策に関するカタログ掲載項目のイメージ)

不正受験対策	離席検知	<input checked="" type="checkbox"/>	一定時間以上の離席を検知する仕組みがある	比較が可能となるような主な機能について共通項目を設定
	なりすまし検知	<input checked="" type="checkbox"/>	受講者以外の人間が受講していることを検知する仕組みがある	
	解答作成以外の操作の検知	<input checked="" type="checkbox"/>	解答作成以外のPC操作を検知する仕組みがある	
	カンニング対策	<input checked="" type="checkbox"/>	視線の動きをモニタリングするなど、カンニング行為を検知する仕組みがある	
	音声の検知	<input checked="" type="checkbox"/>	第三者が口頭で回答を伝達するような行為を検知する仕組みがある	
	テスト内容による不正対策	<input checked="" type="checkbox"/>	設問を複数パターンで設定できる、設問の順番をランダムに設定するなどの仕組みがある	
	その他	<input checked="" type="checkbox"/>	.....	
不正受験対策に関する詳細	個別の不正受験対策技術の詳細な仕様 (例: どの程度の視線の不自然な動きを検知できるか) 不正受験対策に係る技術に関するエビデンス等について記載を求める			個別の技術の詳細については自由記述欄で積極的にアピールを求める

- 記事の構成は、
  - 第1章 総論 — そもそも試験とは何であるか、なぜ不正防止が必要か、不正防止の観点で従来の紙試験と CBT との違いの本質は何か、インターネット通信を経由する場合の限界は何か、なぜそのような限界が生じるのか等を記述。
  - 第2章 不正防止技術の評価 — 例えば、以下の公募文書における「不正受験対策」に対する評価を主目的として、不正受験者の立場を想定した上で、半日くらいで自作できる SSL 中間者攻撃などのプログラムを自作して在宅型 CBT 試験における監視カメラの映像等の改ざん等の攻撃を加える実験手法等の検証結果を多数述べ、解決方法を提案。
  - 第3章 完全性・機密性・可用性の評価 — 技術限界と解決手法を提案。
  - 第4章 考察とまとめ
 というものになっています。意思決定層と技術者層の両方に魅力があるかどうかは怪しいのですが、少しは読んでもらえそうな内容にするよう努力しました。
- ほとんど他の業務の合間に走り書きでやっており、かなりのやっつけ仕事で、不満足な点が多いと思いますが、技術記事として最低限満たすべき内容や品質をひとまずは示すという面で、一応の参考として活用いただければ幸いです。

デジタル技術解説記事 サンプル

# CBT 試験システム技術の 検証と評価

不正受験行為防止と機密性・完全性・可用性の実現

Ver 0.4 (2023/02/09)

登 大遊

## この記事について

本記事は、各種試験実施主体の経営者や職員の視点を想定し、CBT (Computer Based Testing: コンピュータを用いた試験) システムを評価するものである。すなわち、「試験システムを試験する」という、心躍る内容である。対象読者は、各種試験実施主体の経営者、職員、および試験システムを開発する事業者の経営者および技術者等である。

本記事は、コンピュータやネットワーク技術を基礎として、さまざまな不正行為を行なおうとする不正受験者の視点に立ち、懸命に試験システムによる不正監視をかいくぐろうとすることにより、試験システムの不正行為防止機能を試すものである。また、試験システムに要求される機密性・完全性・可用性に係る耐性と脅威を、かなり真剣に、評価検討するものである。そして、試験実施者や、CBT 試験システムの開発者の視点に立ち、これらの問題を解決する方法を考えるものである。

本記事は、ある企業のある1つの在宅型 CBT 試験システム製品をお借りして、様々な角度から検証した結果を参考にしたものである。しかし、当該特定製品固有の事柄について色々述べたとしても、さほど汎用的でない記事が出来上がってしまう。そこで、本記事においては、他の任意の CBT 試験システム (在宅型であっても、集合型であっても) について考える際もほとんど共通となるような事柄を対象として、できるだけ本質的評価と考察を行なうように努めた。試験という社会的行事の意義や、不正防止を行わなければならない理由等の本質的な原理にできるだけ近付いて議論をするように試みた。本システム以外の他の CBT 試験システム (在宅型であっても、集合型であっても) を利用しようとする試験実施主体にとって有用な情報を提示できることを目指した。

本記事は、サンプル記事として依頼されたものなので、対象システムの評価に 2.5 日間 (試験システムを欺くための SSL 中間者攻撃等の必要な自作プログラムの開発を含む)、記事の執筆に 5.0 日間程度しか費やしていない、ほとんど走り書きであり、内容は全く校正しておらず、未だ満足なものにはなっていない粗末なものであるが、このような技術記事として最低限満たすべき内容や品質をひとまず示すという面で、一応の参考としてご活用いただければ幸いである。

# 目次

<b>第 1 章</b>	<b>総論—CBT 試験システム</b>	<b>7</b>
第 1 節	はじめに	7
1	試験とは何か	8
2	試験に対する脅威	9
3	脅威 (a) と脅威 (b) は一体何が違うのか	10
4	人類社会の発展・存続は、公平公正な試験の実現にかかっている	13
5	そのため、「試験システムに対する試験」はさらに重要である	13
6	紙を用いた集合型試験では、数々の工夫により、不正防止が実施されてきた	14
7	CBT 試験システムでも従来の紙試験と同等の水準での不正防止対策が必要である	19
8	「試験システムに対する試験」の実施のためには試験システムの内側や開発業者に対する奥深い検証と試問が必要不可欠である	21
9	試験システムに対する検証は、試験実施主体自らが、不正受験者の立場で考えられるさまざまな不正を試してみることによって実施する必要がある	23
10	試験システムの検証作業は、いざ始めてみると、創造的で楽しい作業となる	24
第 2 節	CBT 試験における重要な課題	29
1	課題 1. CBT 試験システム (在宅型) の不正防止機能の実効性に関する問題 (紙ベースの従来型試験と比較してより容易に不正が可能になってしまわないか)	29
2	課題 2. CBT 試験システム (在宅型であっても、集合型であっても) の運営者 (業者) が不正に荷担する可能性の問題	30
3	課題 3. (主に在宅型の) CBT 試験システム運営者 (業者) がパブリッククラウドを用いる場合におけるパブリッククラウド運営業者が不正に荷担する可能性の問題	32
4	課題 4. 可用性および完全性の問題 (紙ベースの従来試験よりも受験者の不利益やリスクが増えないか)	39
<b>第 2 章</b>	<b>各論 I—在宅型 CBT 試験システムの不正防止機能の検証</b>	<b>65</b>
第 1 節	なぜ不正対策が重要か	65
第 2 節	本システムの不正行為検出機能の仕組みの評価	68
1	概要	68
2	カメラ映像から AI で検出可能な不正被疑行為	72
3	検出された不正被疑点の確度の数値化	73
第 3 節	本システムで想定される不正行為とその実験評価	81
1	カメラ妨害 (遮断)	83
2	カメラ妨害 (映像劣化)	93
3	カメラ映像改ざん (平穏な映像のループ再生等)	103
4	タブまたは別ウインドウを用いた不正情報摂取	112
5	重なり合った 2 枚のモニタによる不正情報摂取	121
6	その他の替え玉的受験の手法	127
7	全問題文閲覧後のブラウザ異常終了の偽装と試験再開	131

## 第 3 章 各論Ⅱ—CBT 試験システムの公平性 (完全性・機密性・可用性) の検討 135

第 1 節	可用性に対するリスク (在宅型).....	135
1	在宅型 CBT 試験システムにおける可用性とは .....	135
2	本システムにおける通信経路の可用性の検討.....	135
3	本システムにおける試験サーバー動作の可用性の検討 .....	154
第 2 節	機密性に対するリスク (在宅型・集合型の両方).....	159
1	試験システムにおける機密性とは.....	159
2	システム運業者の関係者による不正のリスク.....	159
3	パブリッククラウド運業者の関係者による不正のリスク .....	163
第 3 節	完全性に対するリスク (在宅型・集合型の両方).....	164
1	試験システムにおける完全性とは.....	164
2	システム運業者の関係者による不正のリスク.....	164

## 第 4 章 考察とまとめ..... 171

第 1 節	試験における不正行為の防止の重要性 .....	171
第 2 節	不正防止機能の必要性和本システムに対する考察.....	172
1	CBT 試験における集合型紙試験と同等程度の不正防止機能の必要性.....	172
2	CBT 試験システム (在宅型・集合型の両方) の試験問題の機密性と答案データの完全性に関する関係者による不正防止の必要性.....	173
3	在宅型 CBT 試験システムにおける試験中の受験者による不正情報摂取や替え玉受験等の不正防止の必要性 .....	175
4	インターネットやクラウドサービスを用いる場合の CBT 試験システムの可用性の実現の必要性.....	179
第 3 節	まとめ .....	181

このサンプル記事は、「デジタル技術解説記事を書くための参考に資するサンプル記事」として、「記事の見本」(記事の書き方の一提案)を作成する目的で執筆したものであり、特定の事柄に関する専門の書物のような正確性と品質を有するものではない。内容の正確性について、著者および配布主体は、一切の責任を負わない。このサンプル記事は、技術者・経営者としての視点で、自らの経験を元に執筆した。必要最小限の法的事柄にも言及している箇所があるが、著者は法律の専門家ではないので、その部分に誤りがある可能性は、技術部分のそれに比べて大きい。

# 第1章 総論—CBT 試験システム

## 第1節 はじめに

CBT 試験システム、特に在宅型 CBT 試験システムは、素晴らしいソフトウェア技術である。在宅型 CBT 試験システムにより、受験者は、自宅で入社試験や資格試験を受験できるようになる。本文書でサンプルをお借りして試すことにしたある製品システム（「本システム」という。）のような在宅型の CBT 試験システムは、在宅の受験者の Web カメラの様子（目線の動き等）をセンターに送付し、センター側でその映像データを AI 分析し、不正行為（カンニング）の可能性を自動検出して、これを試験実施主体に報告するという、画期的な、優れた不正防止機能を有している。このような AI を用いた試験不正防止機能は、無限の可能性を有している、素晴らしい機能である。単なる試験以外にも、社会の様々な場面で、広く活用できる豊富な可能性を秘めている。

また、AI を使用しない在宅型 CBT 試験システムも存在する。これは、人間がすべての映像をチェックし不正を発見するというものである。これはさらなる厳格性を求める場合に利用可能である。

そして、集合型 CBT システムも存在する。これは、従来の紙試験における集合型試験で、媒体（問題表示、答案作成）について、紙の代わりにコンピュータを利用するようにしたものである。

これらの CBT 試験システムにおいて評価する際には、不正防止機能の評価と、試験システムそのものがどの程度の水準の信頼性（試験問題が漏れないという面での機密性、答案データが不正に書き換えられないという面での完全性、試験前および試験中にすべての受験者がインターネット経由で確実に試験サーバーにアクセスすることができるという面での可用性）を有しているかが問題となる。そこで、本文書では、これらの点を評価することを主眼として、CBT 試験システムの分析を行なった。

本記事における本文中のスクリーンショットは、ある評価対象システム（本シス

テム) の評価のために提供されたデモアカウントで実際の試験システムに接続した際の実行画面結果を、そのまま撮影したものである。ただし、一部の試験画面の本文と選択肢は、臨場感を出すために、デモアカウント用のサンプル試験問題を、本場の資格試験の過去問に入れ換えてある。また、本記事は CBT 試験システムの評価方法を示すサンプル的な記事であり、たまたま対象とした本システムについて宣伝したり言及したりするためのものではないので、システムの固有名詞や URL 等は、スクリーンショット中からすべて削除させていただいた。

本記事においてこれから述べるさまざまな事柄や分析結果は、在宅型 CBT システムかつ AI 支援型の不正自動検出システムを元に記述しているが、大半の部分は、AI 支援がなく、人力によるカメラ監視を行なう仕組みでも妥当する。また、機密性・完全性に関する議論は、インターネットを用いた在宅型 CBT システムのみでなく、集合試験型の CBT システムにも妥当する。

## 1 試験とは何か

そもそも、試験とは何だろうか。

試験といっても、様々なものがあるが、ここでは、人物を選抜したり、評価したり、資格を与えたり、修了を認定したりするような考査試験について考えてみることにしよう。この目的においては、試験というものは、試験実施主体の視点から、特定の受験者が、試験の対象分野について、高い能力・性能を身に付けているかどうかを知るため、受験者にあれこれと試問をしてみて、その能力を測るプロセスであるということができる。

試験は、実施する側も、受講する側も、一定のコストや時間を費やす。それでは、そもそも、なぜ試験が必要なのだろうか。それは、対象者の身心 (特に頭脳) の内部状態 (記憶内容と、形成された思考ルーチン) の価値・状態を、外部から見極める必要があるためである。それらは人間の頭脳の神経回路として形成されており、外部から観測することは、今のところ技術的に困難である。そこで、代わりに、外部から言語を用いて色々なテスト (試問) をして (試験問題の提示)、その挙動・応答を観測し (答案容易への記入)、結果を試験実施主体が読み取って (採点)、対象

者の内部状態のレベルをある程度正確に推測する試験プロセスが必要となるのである。

そして、複数回繰り返される試験においては、試験問題の出題の傾向が如実に受験者に把握されてしまうと、多くの受験者は表面的対策（過去問の暗記等）を行なうことで真の実力を水増ししようとしてしまうことになる。そのため、試験実施主体の視点においては、単に表面的な試問だけでなく、かなり深いところを見極めることにより、対象受験者の真の能力レベルを測定することができる試問をあれこれと行なうことが不可欠となる。

## 2 試験に対する脅威

前述した試験の性質から、試験に対する下記 2 点の本質的脅威が導出される。

### 脅威 (a): 受験者によって表面的な受験対策を施されてしまう可能性

第一に、試験実施者が表面的な試験を作ってしまう、受験者による表面的な受験対策を施されてしまうという可能性が存在する。

受験者の内部状態が対象物事の本質的理解に近付いていないのに、受験者の側で対策を施されれば（例えば、過去問集の丸暗記等）、受験者は、試験実施主体に対して、あたかも自らが本質的理解を成し遂げているように粉飾することが、簡単にできてしまう。

そこで、実際の能力を測定するためには、粉飾可能な表面的な試問だけでなく、奥深くまで準備してはじめて答えられるような、対象領域に関する本質や知見の限界にまで接近した試問を、あれこれと行なわなければならない。

このことから、試験実施主体自ら（試問を行なう側）は、試験の対象領域に対する、並外れた水準の知見を有する必要があることになる。

### 脅威 (b): 不正行為（カンニング）の可能性

第二に、不正行為（カンニング）の可能性がある。替え玉受験、試験時間中における助言者からの情報の不正摂取、試験中の参考書（最近では、インターネットサ

イト等を含む。)に記載されている情報の不正閲読、試験後の採点前における内通者を通じた答案用紙の不正書き換えなどの手法が、古来より存在する。

### 3 脅威 (a) と脅威 (b) は一体何が違うのか

上記で検討した脅威 (a) は、通常の実験対策方法として知られている。(a) のような実験手法が、試験の実効性を損なうとして批判されることはあっても、これが不正として取り締まられることはなく、社会的に一応許容されている。

他方で、脅威 (b) のような不正行為は、わずかな不正行為 1 回限りであっても、直ちに失格処分等のペナルティが課されることが通常である。

それでは、なぜ、(a) は社会的に許容され、(b) は社会的に許容されないのだろうか。今一度、深く考えてみよう。

#### 試験対策 (a) の丸暗記対策を行なう受験者は、一応は試験の価値そのものと同じ方向を向いているので、不正ではない

まず、どのような試験でも、ある程度の傾向が存在し、受験者側として、安易な試験対策を行なうことができってしまうことは避けられない。受験者がその安易な試験対策を行ない、高得点を得ることは、外形的に何らかの試験中のルールに外形的に違反している訳でない。試験実施主体がルールを課することができるのは、原則として、試験時間中の行為に限られる。試験時間が到来する前における受験者の勉強の方法は完全に自由であり、それについてルールを課することはできないのである。このように、(a) を禁止するルールを制定することは不可能であることを理由に、(a) を取り締まることは、そもそも不可能である。

次に、(a) の手法は、実は、勉強として一応効果的であるという側面も存在する。受験者が、確かに (a) のような安易な試験対策を施すつもりで、例えば過去問の丸暗記を行なうにしても、それには、実際相当の時間をかける必要がある。その暗記を繰り返す過程で、単なる暗記データとしての記憶に留まらず、そのような暗記データを自動的に導出するための頭脳内部の思考回路が、自然に自らの頭脳内部に形成されるという効果が、われわれ人類の経験則上、明らかに存在する。よって、

(a) の単なる安易な丸暗記勉強法であっても、それがかなりの回数繰り返されれば、丸暗記受験者の頭脳は、試験そのものが測定を目指している、対象領域に関する高い水準の本質的理解を有する状態（すなわち、試験が誘導しようとしている価値の高い状態）に近付くのである。言い換えれば、試験の対象領域に対する本質的理解の度合いと、表面的対策に費やした努力の総量とは、一般に、正の相関関係が見られると期待できる。

このように、試験が目指すべき価値と、表面的対策の努力によって自然に向かう先とは、ほとんど同一の方向を向いているので、(a) は社会的に許容されるし、場合によっては、(a) は、正しい努力的行為であるともみなされる。

**不正行為 (b) を行なう受験者は、受験の時点で試験の実現価値を否定していることになるから、試験結果判定以前において、失格として取り扱うことが正当化される**

他方、(b) の不正行為は、(a) と全く異なる。(b) のような不正行為を行なうことと、試験の対象領域に対する本質的理解を深めることとは、方向性が真逆である。そもそも、不正行為を行なえば良いのではないかという (b) のような者の内面で生じるよこしまな誘惑は、(a) のようなたとえ表面的であっても一応の努力を費やして受験対策を行なう際に必要な努力をしなくてもそのような努力をした者と同じの成績結果を是非とも得たいという衝動によって、ついに実行されるに至るものと考えられる。すなわち、不正行為を行なう主要な動機は、(a) のような表面的努力にかかるコストを節約したいというものである。(a) の表面的努力は、一応は対象領域の本質的理解に近づくための努力であると考えることができるが、(b) のような不正行為を行なう行為は、まさにその対象領域の本質的理解を否定するという行為に他ならないことになる。すなわち、(b) のような不正行為を実行することは、その試験が実現しようとする価値そのものを、完全に否定していることと同値である。そこで、(b) のような不正行為を実施する者は、最初からその試験の実現価値を自ら否定してしまっているのだから、その試験を受験する資格がなく、よって、結果を判定することなく最初から失格としても差し支え無い、ということになるのであろう。

👉 ところで、上記の議論には穴がある。例えば、試験問題または試験の模範正答を予め不正入手した上で受験する行為が存在する。この手の情報不正入手型の不正行為は、そのことを勉強法の工夫の延長であると形式的にみなせば、これは (a) に該当するので取り締まることができないということになってしまうのである。われわれは、これに対する反論を用意しなければならない。

一般的に (a) のような丸暗記勉強法が一応正当であるとみなされる理由は、たとえば丸暗記であっても、試験の対象領域に対する多種多様な分野の事柄を次々に暗記していけば、その対象領域の本質を形作る形状がある程度暗記者の頭脳内に形成されると考えて、形成された価値のある思考能力の量と、暗記等の表面的勉強に費やす勉強量との間に、一定の比例関係があるとみなすことができるためである。われわれの社会の経験則上、その比例関係が通常生じているということの推定が働くので、その推定が覆らない限り、(a) によって勉強を行なった結果の成績は、社会的には、一応正しいものとみなしてよい。

ところが、試験問題または試験の模範解答を予め不正入手した上で受験するような行為は、受験者は、その出題される問題または正答「だけ」を一生懸命勉強して暗記していることになる。これにより、形成された価値のある思考能力の量がわずかであるにもかかわらず、膨大な量を形成しているというように粉飾している状態となっている。すなわち、粉飾率が (a) の平均的粉飾量と比類にならない程高くなっていて、前記の比例関係を満たさない状態となっている。

このような行為は、確かに受験時間中には何ら不正行為を行っていないようではあるが、不正に試験問題または試験の模範解答を予め入手していたという事実が証明されれば、前記の比例関係の推定が覆され、不正入手した情報を元に有利に受験をしたのではないかと、合理的にみなせる状態に陥る。この状態に陥った受験者は、不正入手した情報を何ら有利に活用していないという旨を逆に証明しなければならないことになるが、それは、証明不能である。よって、その受験者は、不正行為とみなされて、(b) と同様に試験価値を否定したとして失格にされることが許容されるのであろう。

ただ、この理論を突き詰めて考えてみると、境界値付近で、色々な疑問が生ずるものである。例えば、客観的に、試験のために正しく勉強努力をして必要な知識知恵を有する状態になった受験者が、誤って試験の前日に試験問題または試験の模範

解答が道路に落ちていて (またはインターネット上の掲示板にアップロードされていて)、拾ってそれをついっかり読んでしまった場合を考えてみよう。その場合、その受験者も不正行為として失格にしなければならないのかどうかという問題があり得る。誠に興味深い難題である。

われわれは、試験というものについて、このようなさまざまなケースを評価し議論することにより、初めて、試験システムが保護しようとしている価値について考えることができるのである。

#### 4 人類社会の発展・存続は、公平公正な試験の実現にかかっている

試験は、重要な社会的行事である。人類社会の発展・存続は、できるだけ多くの人々の頭脳が、できるだけ多くの、世界に存在する物理的・社会的および論理的な問題を解けるか、そして、その水準を人類が存続・発展可能な程度の一定の高いレベルに維持することができるか否かにかかっている。頭脳水準の維持は、各人の勉学の成否にかかっている。各人の勉学の成否は、勉学結果を評価する試験システムにかかっている。したがって、各種の試験システム上、公平公正で良い試験が実施されることが真に保障されるか否かは、人類社会の存続・発展の可能性を決定的に左右する重大問題である。

公平公正で良い試験が実施されることを前提として、試験で良い成績を得られたときは受験者に何らかのインセンティブが生じる状態を作り出せば、各受験者は自らの頭脳を駆使して勉強に励み、よって人類の存続に必要なだけの知恵が生じる思考回路が人々の間で自然に形成されることになる。このことを実現するため、われわれは、公平公正な試験の実現のために、全力を注ぐ必要性が肯定される。

#### 5 そのため、「試験システムに対する試験」はさらに重要である

試験システムによる公平・公正な試験の実施が極めて重要な課題であるとするならば、それらの「試験システムそのもの」が、公平・公正な試験の実施を担保することができる程度の手続きを保障し、不正を防止することができる仕組みを具備し

ているかどうかを「試験すること」、すなわち、「試験システムを試験すること」は、さらに重要であるといえる。

特に、近年は効率化のために、少数の共通的な試験システムによって、複数の試験実施主体による多数の試験が実施・運用されることがあり得る状態となっている(本書において評価対象としている本システムのような製品等である。)

この場合、そのような一つの共通的試験システムには、多数の試験が寄りかかり、当該システムを共有利用することになる。そのため、このような共通的な試験システム一つを特に取り上げて試験することは、その試験システムに対する試験を実施するためにかかるコストに比べて、その試験システムに依存しているすべての試験の公平性・公正性といった質を大幅に高めることができるという利益が生じるので、極めて重要な作業であるということになる。

したがって、共通的試験システムを試験するという試験は、社会の中のすべての試験の中でも、最も重要な試験であるといえる。

## 6 紙を用いた集合型試験では、数々の工夫により、不正防止が実施されてきた

試験システムは、短期的にみても多くの受験者の人生にそれなりの重要な影響を及ぼす。また、長期的には人類の生存・発展に極めて重大な影響を及ぼすものである。したがって、各種の試験は、権威・価値・信頼を有する者によって実施される必要がある。これまで長い間、権威・価値のある試験を実施してきた試験実施主体たちの公正・公平性は、その長年の間に、重大な不正疑惑または不正防止責務に対する懈怠の疑惑がないことをもって、社会的に担保されてきた。特に、その実施主体が公的機関である場合は、主権者たちの判断と支持を背景として、その試験実施主体の正当性が、いわば政治責任的に担保されてきた。

さまざまな重要な試験実施主体は、これまで、長年手慣れた手法である「紙を用いた集合型試験」を実施してきた。試験実施主体たちは、紙を用いた集合型試験という「試験システム」に不正が入り込む余地について、数々の不正防止および公平性担保のノウハウの蓄積を用いてこれを運用することで、そのリスクを最小化する

ことができてきた。後に詳しく述べるとおり、紙を用いた集合型試験では、物理的に一箇所の室に多数の受験者を集合させて実施していたので、多人数の受験者が、1つの空間を、いわば「受験者集団が個々の受験者や試験実施関係者（試験監督たち）を逆に監視する」ことができることが、光学的（視覚的）および音響的（聴覚的）に、保障されてきた。これに関連して、紙の問題用紙の印刷・配布のいずれのプロセスにおいても、試験委託業者・印刷業者の役員や被用者誰1人に対しても決して事前に問題用紙の内容が読み取られることがないように、最新の注意を払い、当日朝まで確実に封印して保管し、当日試験代行業者にこれを手渡す際においても、講堂において試験日当日に一齐に受験者たちの目前で封筒開封させるなどの、公平・公平性を最大限視覚的・聴覚的に全受験者に対して証明するための手続き的保障がなされていた。

1つの受験会場で、何十名もの受験者が集まって緊張状態で座しているとき、いわば受験者たちが現場において公平・公正な受験体制の監視員・証人の役割を果たしているのである。このことによって自然に生じる強力な不正防止効果については、在宅型 CBT 試験システムとの対比の関係で極めて重要であるから、ここで、もう少し詳しく分析してみよう。

#### **(a) 集合型試験では、受験者たちは物理的に他の受験者たちの不正を監視できる物理的状态にあった**

紙を用いた集合型試験では、試験実施主体が試験を実施する際にすべての受験者に対して公平・公正に接しているかどうか、ある受験者があからさまに自席で不正行為を行なっているのにそれを過失により見逃すことがないか、といった点が、全受験者たちの共通の関心事であった。善良な受験者としては、不正な受験者の存在により、自らの相対評価が下がるので、不正な受験者がいればこれを検出・排除したいという集団的インセンティブが、試験会場の現場で常に働く。

集合型試験においては、受験者全員が試験会場の他の受験者たちの受験の様子や、試験実施主体の関係者たち（実際には、試験実施主体の被用者である試験監督員たち）の誠実な働きの様子を、目視で監視しようとするれば監視できる状態になっており、いわば、全受験者が会場の公平・公正性に対する目撃証人の役割を果たしてき

た。

すなわち、集合試験型においては、不正行為を行なおうとする者は、試験監督員たちだけでなく、それに加えて、なんと、周囲にいる全受験者の目を盗んで、不正行為を行なう必要があったのである。100名の受験者がいて、仮に90名くらいの受験者は善良な受験者であるとする、それらの善良な受験者たちは、仮に同じ試験会場に不正行為を行なう受験者がいるのを見とめたならば、それを放置すると自らの善良な努力による試験結果が、不正者によって不公正に価値低下させられるリスクを痛感する。そこで、善良な受験者としては、そのような場合は、付近の試験監督員に対して、すぐさま、その不正受験者を指差しするなどして、不正を公正に見咎めるべきであると指摘したくなるかも知れない。そういう個人的インセンティブを、各受験者たちは、常に有していることになる。

このような自然発生的な監視関係は、不正行為の実施を検討している者によっても容易に予想がつくので、周囲の受験者に不正行為を発見されて吊し上げられるおそれを警戒して、不正行為をしづらくなるという、一応好ましい状態が、会場で形成されていたのである。これは、集合型試験の場合、原理的に、必ずみられる現象であるといってもよい。

#### **(b) 集合型試験では、試験会場提供者（会場ホスト組織）であっても不正に関与する余地がなかった**

試験会場は、多くの場合、大型の堅牢な建物所有者等（大規模な民間のセミナー会場ビル所有者、大学、高校など）が所有・管理し、これを試験の際に1、2日間の期間を定めて、試験実施主体に有償又は無償で貸し出される。

このように、試験場所をホストする側の、広大な建物を所有する者（法人等）またはその管理者たちは、社会的にはそれなりに地位が高く（大抵、大きな資本を有している）、一般的な一市民の人脈と比較すると、かなり多くの人的つながりを有していることになる。

そして、これらの施設管理者たちは、試験実施会場そのものに物理的に手を加えることができってしまう。試験実施中でも、施設管理権と称して、何かと理由を付けて、試験教室に自ら入っていくこともできるのである。

このように、社会的に多くの人的つながりを有しているこれらの会場ホスト組織の有力者たちは、受験者またはその関係者から、受験にあたっての便宜を依頼される可能性が、その有している人的つながりの本数に比例して多いことになる。そこで、これら施設管理者（ホスト組織）が不正行為への加担を囑託されてしまう可能性も高い。

しかし、会場ホスト組織の有力者たちは、仮に自身の有する施設を貸し出して行なわれる重要な試験実施において、依頼された特定の受験者に対して、その会場ホスト組織としての地位を濫用して、その試験結果を左右することができるような何らかの有利な取扱いを行なうことは、ほとんど不可能であった。その理由は、(a)で分析した理由とよく似ている。

すなわち、受験者たちが全員を相互証人のように監視し牽制し合っているので、会場ホスト組織の有力者といえども、不正な挙動を物理的に行執りづらかったのである。また、試験実施主体たちは紙の問題用紙を、封筒などで封印した状態で当日会場に持ち込む。試験実施主体たちは、公平・公正性を受験者たちに一生懸命にアピールする目的で、試験開始直前に、試験会場の一番前で、目立つように、受験者の面前で封を切るような動作を行なうこともある。会場ホスト組織は、試験実施主体とは異なる主体であるため、いかに会場ホスト組織の有力者であっても、貸出先の試験実施主体が試験会場に持ち込む問題を、試験開始前に盗み見ることは、このような物理的な封印システムと、試験会場における集団監視の下では、ほとんど不可能であった。

会場ホスト組織の有力者が、仮に特定の受験者から不正を囑託されていたとして、出来ることといえば、せいぜい、(a) 特定の受験者に、試験の途中で模範解答やアドバイスの紙を手渡しする等の情報提供行為、(b) 特定の受験者に、エアコンの風をよく当ててあげるといった施設管理権を濫用した行為、くらいしかない。

(a) のような物理的な行為に及んだならば、周囲の受講者によって直ちに見抜かれてしまう。

(b) の行為は、有利な効果がたいして無い。それに、大抵の場合、どの受験者がどの座席に座るのかは、試験当日の入場時まで、試験実施主体の側が管理しており、

会場ホスト組織の有力者としては事前に予測する方法はなく、当日行ない得る物理的な不正便宜供与行為の範囲は、著しく限られている。

これらを原因として、集合型試験における会場ホスト組織が主体となった不正は、かなりの水準で抑制・予防されてきたといえる。

### (c) 集合型試験では、試験代行業者や印刷業者であっても不正に関与する余地がなかった

大型の試験においては、試験代行業者や印刷業者が活用されるケースが多い。これらの業者の経営者や被用者たちは、試験の代行または問題用紙の印刷業務において、相当に高額な報酬と引き換えに不正行為を囑託されれば、発覚のリスクが低ければ、これに応じる可能性が発生する。しかしながら、物理的な集合型紙試験においては、試験実施主体の側における各種の秘密保持の手法に工夫が凝らされていて、不正の発覚のリスクを高い状態に維持することができていた。

加えて、(a), (b) で述べたような試験会場における受験者相互の監視体制も自然に形成されていたことも相まって、これらの受注業者の経営者や被用者であっても、試験問題を事前に入手したり、試験中または試験後に特定の受験者に有利な便宜を図ったりするといったことは、ほとんど不可能であった。

不正防止のための具体的方法としては、紙試験に長けた試験実施主体によるノウハウにより千差万別であった。

一般的な手法としては、例えば、試験代行業者と問題用紙印刷業者を分離し、両方を一つの業者に決して委託しないという手法がある。

問題用紙の印刷も、デジタル・データとして印刷業者に送付するのではなく、印刷現場まで、試験実施主体の委員複数名が共同で物理媒体に格納してこれを持っていき、これらの委員の注意深い監視のもと、印刷工場で決してデータが複製されることがない形で、その場で印刷・製本がなされ (ただし、印刷・製本中に、委託先印刷作業員がその内容を注視していないことの確認は必要であった。)、その結果数量 (印刷・製本された冊数) を厳密に確認した上で、その場で輸送用の封筒に入れ、封筒を封印して試験実施主体の事務所の金庫室に再度複数の委員が合同で持ち帰ることが可能であった (ただし、この工程において、アナログ輪転機であっても、

デジタル印刷機であっても、印刷内容が印刷機に残存する可能性はある。そこで、これを印刷業者に目前で確実に破棄させるという追加的作業を忘れずに実施する必要がある。これらすべての作業の完了を見届けるのは、一見、比較的容易なことであるように見える。しかし、厳密には印刷機の内部構造まで点検しなければならないので、本質的には、かなり難しい作業であるといえる。)

このようにして嚴重に数量カウントされ封印された問題用紙を入れた封筒は、試験当日まで試験実施主体自ら（委嘱した信頼できる試験委員たちを含む。）が金庫等で物理的に保管しておき、試験当日の、試験時刻の 15 分前等に、試験会場の現場における試験代行業者の被用者たちに引き渡すのである。

試験問題を入れた封筒は、試験代行業者によって、前記 (b) に述べたように、試験開始直前に、試験会場の一番前で、目立つように、受験者の面前で封を切るような動作で開封することができるし、その際に、数量を再度確認することもできる。

この手法により、試験代行業者や印刷業者に試験業務を委託している場合でも、これらの業者の経営者や被用者たちが不正に問題用紙を事前に読み取るという、最も防がなければならない最大の不正の脅威を、十分に回避することができてきた。

## 7 CBT 試験システムでも従来の紙試験と同等の水準での不正防止対策が必要である

ところが、本記事で触れるような CBT 試験システムのようなコンピュータ技術を活用した試験システムは、その主要部分がコンピュータ空間上で動作するものになってしまう。そのため、試験実施主体は、従来の紙ベースの試験不正防止ノウハウを用いても、公平性の担保や、不正防止が確実になされているかの担保を、容易に確保することができない。

試験実施主体は、CBT 試験システムを用いる場合は、従来の紙試験と比較して、試験代行業者が提供する CBT 試験システムに基づく試験を実施させるという、契約上の関係でのみ、試験の公平性と不正防止措置の実際の実現を期待することができる。契約上の関係にのみ頼る場合、従来の紙試験と比較して、試験の公平性および不正防止の実現という面で見るときには、どうしても、実効性が弱いものとな

ってしまう。このことは、従来の紙試験の場合と比較してイメージすれば、容易にその違いが理解できる。この 2 つは、債権的効力と物権的効力との強さの違いに似ている。

従来の紙試験であれば、仮に試験代行業者を使うとして、確かにその契約関係上に公平性の担保や不正防止の措置を受託者に義務付けている。その義務付けは、単に契約上の義務付けである。これで主催者は一応安心できる気もするけれど、それだけでは確実とはいえない。契約上の義務は、実際に確実に履行される保証がないからである。そこで、試験実施主体またはその指名する信頼できる職員、委員等が、実際に試験会場に分散して出向き、物理的に、委託者による試験代行実施が公平性および不正防止措置を確実に実現しているかどうか、目視をもって確認することができていたし、ほとんどの場合は、重要な試験では、そのように行なわれてきたのである。仮に現場でこれらの措置が不十分であるという懷疑が生じたならば、試験実施主体は、直ちに代行業者に対して是正をしよう求めることができるし、場合によっては、その場においては、代行業者に頼らず、自ら試験を実施することもできた。つまり、従来手法では、単なる契約上の関係に基づく強制力・抑制力という弱い力に加えて、試験実施主体自らが現場で確認をし、必要に応じて是正をさせるというかなり強い強制力・抑制力が働き、そのような力関係があることは試験関係者全員に予測されるので、委託先の代行業者の被用者を含めた試験関係者全員が、神経を集中させて試験運営に挑む状態が常に維持されるという、公平性の担保および確実な不正防止措置の実現という目的のために、誠に最良の状態が、長年、維持されてきたのである。

しかし、CBT 試験システムでは、すべてコンピュータやネットワーク上で試験が実施される。特に、在宅型 CBT 試験システムの場合、従来方式のように、試験実施主体自らがその公平性と不正防止措置の確実性を、試験実施中に自ら確認しに行くことが、時間的・距離的制約により、不可能となる。そこで、試験実施主体としては、試験実施中にこれらを確認するのではなく、事前に、使用しようとする CBT 試験システムについて、自ら、かなり強力・過酷に試験を施す必要が生じる。

すなわち、当該試験システムが、公平性及び不正防止措置を常に確実に実現でき

るものであるか、予期せぬ不正が入り込む余地はないかといった点を、相当の力強さをもって、テストしなければならない。

これまで全国各地の試験会場に委員・職員等を出向かせて試験当日の前述のような現場確認を行ない試験の公平性を維持するのに、かなりのエフォートをかけていた試験実施主体としては、それらの物理的・当日確認作業のためのエフォートが、CBT 試験システムでは、かなり、または、すべて不要になる。そこで、それによって節約されたエフォート（空いた優秀な組織職員たちの時間）のうち相応の部分を、CBT 試験システムを事前にかなり過酷に試験するというためのエフォートに振り分け、CBT 試験システムに生じるかもしれない不公平の余地や不正が入り込む余地を、徹底的に洗い出さなければならない。

試験実施主体は、仮にこれらの事前検証を尽くさなかったとき、その懈怠が原因で後に不正行為が発生してしまった（不正行為を見抜くことができなかった）ことが分かれば、コスト削減目的で CBT 試験システムを用いたことによるその削減したコストの一部を用いて万全の不正対策をすべきであったのに、その責務を怠っていたということになり、これは、強い社会的非難にさらされるおそれがある。

## 8 「試験システムに対する試験」の実施のためには試験システムの内側や開発業者に対する奥深い検証と試問が必要不可欠である

このように考えると、CBT 試験システムという「試験システムに対する試験」の質は、試験実施主体にとって、経営上の重要な死活問題であるということができる。そこで、どうにかして、利用しようとする CBT 試験システムを深く試験する必要がある。

ところが、CBT 試験システムは、多くの場合、その実装がブラックボックス化されており、そのプログラムのソースコード群も、サーバーシステムの構築・運用に関する手順書類も、すべて、代行業者の手中にある。そして、これらは、企業秘密であるとして開示してもらえないことが多い。たとえ開示されたとしても、試験実施主体の職員におけるコンピュータやネットワークに関する技術力は発展途上であるので、その開示された実装を分析しても、それが適切・妥当な水準の能力を

維持しているかどうか、なかなか分からない。それを検証するためには、代行業者において当該システムを開発したプログラマーよりもさらに高いレベルを有する職員を育成する等して、長時間かけて分析しなければならない。それは、近い将来、すべての試験実施主体において必要になることである。しかし、その人材育成には、これから、少なくとも数年間の時間を要する。従って、内部実装を技術的に調べ尽くすという手法は、本日時点では、まだ現実的ではない。

それでも、試験実施主体としては、代行業者の手中にある CBT 試験システムのブラックボックス的実装の安全性・確実性を、確実に検証しなければならない。このような「試験システムに対する試験」について考えるとき、われわれは、このことが、第 1 章第 1 節 1 で前述した「試験とは何か」における、受験者の頭脳の内部状態を外から知る方法がないので、代わりにあれこれと試問をしてみて、その反応（回答）を読み取り、内部状態の質を推定するというモデルに、とても的確にあてはまることに気付く。すなわち、真の内部状態を知り得ないのであれば、試験実施主体は、ブラックボックスである試験受験者（本件の場合は、CBT 試験システムおよびその業者）に対して、あれこれと過酷な試問をして、さまざまな反応をみて、これをよく整理し、対象の試験システムの質が果たしてどの程度の水準であるのか、試験する必要がある。これが、今のところ、「試験システムに対する試験」を実現するための唯一の方法であるということになる。

それでは、CBT 試験システムに対する試験として、われわれは、どのように試験を行えば良いのであろうか。

まず、試験業者に、単に表面的質問をするだけでは、全く意味がない。「あなたのシステムには、十分な措置が講じられているのか。」と質問をして、肯定回答があったからといって、それを信用してはならないのは、試験の本質をよく知る試験実施主体として、最も良く了解されていることである。

それでは、試験業者に対して、セキュリティ・チェック・シート等といった Excel シートを手渡して、すべての項目を満たしているかどうか自主チェックせよという風に指示すれば良いだろうか。これは、試験したことにはならない。まんべんなく全項目について「自主チェックいたしました。問題はありませんでした。」という

回答が来る可能性が高い。これでは、試験としては、意味がない。

その他の手法として、試問シートのようなものを作り、自由回答文で記入せよという方法にすれば、試問の内容をある程度のコンピュータセキュリティ専門家が考えるならば、最初は効果がある。ただ、その試問の内容はそのうち試験代行業者内で出回り、「こう聞かれたら、こう答えれば良い。」という過去問丸暗記受験者的なノウハウが蓄積されてしまい、意味がない。

加えて、第三者による監査に頼るという方法も、たいてい無意味である。その第三者の監査者は、単に上記のようなことをほとんどそのまま行なって、監査の仕事を完遂したことにするのである。それよりも深く検証すべきというインセンティブが、第三者監査人には存在しないからである。

## 9 試験システムに対する検証は、試験実施主体自らが、不正受験者の立場で考えられるさまざまな不正を試してみることで実施する必要がある

それでは、このように、CBT 試験システムに対する試験をするとき、業者に対する表面的試問、Excel シートや試問シートへの回答要求、第三者監査人の監査等の 3 つの方法の、いずれも意味をなさないとしたら、残された手法は、唯一、試験実施主体自らが、その CBT 試験システムをあれこれといじり回って、また必要に応じて可能な範囲で技術的分析を加え、そのシステムが、(a) 確かに公平・公正で、(b) 業者等関係者による不正が入り込む余地がなく、(c) 受験者たちの手によっても、少なくとも集合型紙試験と比較して容易に不正を行なうことが困難であり、(d) 試験で求められる可用性の点でも問題がない、ということ、自ら検証するという方法が存在するのみである。

この自ら検証する作業においては、自らがいわばカンニングをこれから是非とも意欲的に行なおうとする一人の悪い不正受験者であるというような想定で、色々な手を尽くして、検出されない方法でカンニングができるか否かを試してみるとか、業者の関係者としてシステム上の操作や脆弱性を突いてみて、色々不正なことができないか試してみるというようなとても面白い作業に他ならない。

このような作業は、試験実施主体の組織の職員などの信頼できるメンバーの能力

を駆使して、ある程度の時間、実際に試してみる必要がある。

## 10 試験システムの検証作業は、いざ始めてみると、創造的で楽しい作業となる

ところで、そのような検証作業を任せられた試験実施主体の職員としては、最初は嫌な仕事であるような気分になるかも知れないが、実際に試してみると、すぐさま、これはとても創造的で楽しいものであるということが分かるであろう。

なぜならば、その過程は、表面的には対象システムを検証し、さまざまな点でそれを鍛えるという地味で単調な作業であるものの、その途中で、そのような検証作業を行なう検証者自らがその能力を鍛えられるという作用が生じ、これが、極めて心地良いものとして、すぐさま感じられるためである。

そして、単にその娯楽的感覚のみならず、それによって得られる、検証者側の価値の向上が、長期的資産として、検証者の側に個人的および組織的にどんどんと蓄積されていくという実感が、感じられるのである。

この際の職員の心境の変化は、面白い。最初は、試験実施主体の職員は、利用しようとしている CBT 試験システムを色々と検証し、あれこれと懐疑点を見つけ出しては、試験の公平性や不正防止の点に対してその懐疑点がどのような脅威となるのかを理論付け、これを評価するという、あたかも、「本来この CBT 試験システムの開発元業者が十分にそれを行なわなければならなかったはずなのに、それが不十分であるから、それを代わりに客のほうが行なわさせられておるのだ。」という、かなり理不尽な仕事を担っている気分になる。これは、いわば、旅館の修繕を、旅客がやっているようなものである。

しかし、この滑稽な仕事がさらに進行すると、次第に、CBT 試験システムの素人であるはずの試験実施主体の職員たちは、CBT 試験システムの内部実装の様子や不正防止のポイント等について、CBT 試験システムの玄人であるはずの開発元業者と同じくらいに、だんだんと詳しくなってくる。

これがさらに進歩すると、ついには、試験実施主体の職員たちの側のほうが、CBT 試験システム開発業者よりも、CBT 試験システムの内部実装や不正防止の

仕組みについて相当詳しいという、誠に心躍る状態に達することになるのである。

現在、市場には、CBT 試験システムには、複数の業者・製品が存在する。精力的な試験実施主体であれば、一者の CBT 試験システムに限らず、多数者の CBT 試験システムをそれぞれ比較検討するであろう。その結果、試験実施主体は、それら検討対象システムすべてについて、本文書で述べるような様々な検証を実施することになる。これと比較して、すべて競争関係にある CBT 試験システム開発業者間は、互いに、相手のシステムは見せてもらえないことが多い。しかし、試験実施主体であれば、比較検討をするためにすべての業者の CBT 試験システムを色々と深くまで触ってみることができるのである。そして、各社のシステムのそれぞれの長所と弱点とをまんべんなく把握した上で、さまざまな不正行為の試みを、色々な角度から試してみることができる。

このような精力的な試験実施主体（その組織の職員）は、この進歩的作業を継続的行なえば、ついには、互いに隔離・断絶されている複数の CBT 試験システム開発業者では到達し得なかった、極めて高い知見・能力のレベルに、到達することができる。これは、素晴らしいことである。この原理により、優れた試験実施主体は、本来、すべての市場に存在する CBT 試験システム開発業者のレベルよりも高いレベルに常に立ち、すべての業者を指導監督し、すべての業者の CBT 製品の質を引き上げるといふ、最も重要な社会的仕事を、本来の職務範囲外として、自然に担うことになるためである。それは、前記のように各社のシステムを比較検討分析することで、自らの力を鍛え、次第に成長し、ついには最上の能力を有する状態になった試験実施主体しか担えない。

前にも述べたとおり、「試験」が人類の発展・存続に重要で、「試験システム」に対する試験は極めて重要であることから考えれば、試験システムが CBT に移行しつつあるこれからの社会において、CBT システムに対する最上級の試験を施すことができる試験実施主体は、まさしく、人類の発展・存続のために最も重要な役割を担う存在であるということになる。これが仮に試験実施主体の所掌業務以外であったとしても、その重要性と社会的必要性は、必ず社会的に肯定される。これにより、その試験実施主体の組織は繁栄し、有能な人材が集まり、社会の信頼を集め

て事業の多角化が可能となり、存続可能性が高まる。その過程で、試験実施主体の経営上のさまざまな多数の課題が自己解決できるようになり、組織の経営目的が達成できる。

という訳で、すべての試験実施主体たちは、これから CBT 試験システムを利用しようとするのであれば、それを良い契機として、その対象 CBT 試験システムについて、色々な角度から検証をすることが有利である。これは、試験実施主体でなければ行ない得ない、特権的行為である。その入口においては、全く闇雲に手を動かして触ってみるよりは、一応の方向性を決めてシステムを試してみるのが良い。一応の方向性を考えるときは、試験システムが実現しなければならない価値を思い出すとよい。試験システムの実現しなければならない最も重要な価値というのは、受験者および運営関係者による不正・不公正な行為を系統的に防止することにある。また、それに付随して、試験の公平性・公正性を担保するために、機密性・完全性・可用性を実現することにある。したがって、CBT 試験システムを利用しようとする試験実施主体としては、いかなる点で、CBT 試験システムに、これらの不正・不公正の脅威があるか、機密性・完全性・可用性に対するリスクがあるのか、検討する必要がある、ということになる。

試験実施主体が自ら少し探索をしてみれば、従来の紙ベースの試験にはなかったようなさまざまな脅威を、自然に見つけることができる。それらは、従来の紙ベースの試験に長けた試験実施主体にとって一見未知の脅威で、対処ノウハウがほとんどないように見えるかも知れない。しかし、実はそれらは物理的な試験でも存在し得た脅威が、異なる空間上にその形を変形して出現しているものである。したがって、長年の歴史を有する試験実施主体は、自らのこれまでの経験を十分に活かして、新たな CBT 試験における脅威に対処する方法を着実に考案することができるのである。

#### 👉【コンピュータを用いた試験 (CBT) の歴史】

試験は、古くから、特定の施設に受験者を集合させ、主に紙により試験を実施する方式で行なわれてきた。最近では、コンピュータおよびインターネット技術の進歩

に伴い、利便性が高くコストの低い手法が、次々に生み出されている。これらは、CBT (Computer Based Testing: コンピュータを用いた試験) と総称される。日本では、1990 年代頃から、コンピュータに関する資格試験を中心として、コンピュータを用いて試験が行なわれる例が、複数出現し出した。コンピュータ業界の試験であるので、コンピュータを利用しようとするのは、自然なことであった。これらが、CBT の草分け的存在であると考えられる。

CBT の存在意義は、紙の試験と比較して試験実施主体と受験者の双方のコストを低下させることにある。しかし、いざ CBT を確実に実現しようすると、案外大変な作業であることが分かる。1990 年当時、CBT が登場した頃をみると、インターネットは一般に普及しておらず、信頼性もあまり高くはなかった。そのため、試験代行業者が設置する全国のテストセンターに受験者が集合して受講する必要があった。テストセンターには受験者の台数分のパソコンが設置され、パソコン間は LAN 配線が行なわれていた。試験が開始されると、センター内に設置されている問題配信サーバーから各パソコン画面に問題文が配信され、各受験者は各自の答案を現在の会場貸与パソコンで入力し、結果がまた問題配信サーバーに集約され記録されるというものである。

このようなテスト会場は、一体どのように運営されてきたのであろうか。試験代行業者は全国各地に、コンピュータを必要な台数並べたテストセンターを設置する必要がある。しかし、彼らは、不動産を自前で所有または長期間賃借していないことが多い。コストがかかるためである。そこで、試験代行業者は、テストが実施される日の前日等から当日夜までの間、臨時的に、会議室等のセミナー会場を一時的に借りて、そこに前日にコンピュータを持ち込んで設置し、LAN 配線を行ない、サーバーのセットアップを行なって、試験当日に備えるのである。これは比較的単純な作業であるが、それなりの人的コストと、パソコンや LAN を設置したりセットアップしたりするコストが必要である。そして、これらの事前作業に誤りがあつたり、機器の主要部分に不具合があつたりすると、当日来場した受験者たちの努力は水泡に帰すことになり、大問題に発展することもあり得る。これを回避するために、試験代行業者は、準備作業を確実に完了させる対策を講じる必要があつた。例えば、良い現場手順説明書を作る、訓練を受けた専門家によるセットアップを実施する、機器や LAN の主要部分を冗長化する等である。これらの業務を間違いなく完了す

るための多額のコストがかかってきた。

本文書の後半で実際の評価の対象としているような在宅型 CBT 試験システムが実現されれば、上記のような集合型の CBT 試験よりも、試験実施業者たちは、さらにコストを大幅に削減することができる。そして、受験者にとっても、会場への往復が不要になり、自宅で試験を受けることができることから、試験に集中することができるという利益がある。加えて、従来型集合試験で発生していた試験会場への交通や会場での待ち行列等によるストレス等に左右されない、受験者の普段の真の能力の測定を、高精度で行なうことも可能になるのである。

しかし、試験の実施というのは、単にコストを削減し、試験が形式的に無事に完了すれば良いというものではない。試験実施の完遂という仕事それ自身よりも、さらに重要なこととして、受験者たちによるさまざまな不正行為を防止し、不正行為が行なわれた場合はこれを確実に検知して証拠を掴み、場合によっては試験実施主体の判断として、試験中の退場または不合格等の処分を課すという仕事が、試験実施主体および試験代行業者に課せられている。また、試験の公平性・公正性が保たれる必要がある。そのためには、在宅型であっても、集合型であっても、CBT 試験システムには、必ず、機密性 (試験問題が事前に流出しないこと)、完全性 (答案データが試験後に秘かに変更されることがないこと)、可用性 (試験の開始時に試験システムに正しくアクセスでき、そのアクセス可能な状態が試験終了後まで確実に持続すること) が重要である。これらを、CBT 試験システムにおいて、従来の紙方式の集合試験と同等かそれ以上の水準で実現しなければならない。なかなか難しい課題である。そのためには、各種の仕組みや技術上の工夫が必要となる。そこで、試験実施主体の立場においてこれを確実に実現させるためには、試験実施主体が自らの頭脳を用いて様々な検討を施し、これを、CBT 試験システムの開発会社に試問したりフィードバックしたりする必要がある。

そのため、試験実施主体やその職員におかれては、いよいよ、コンピュータやネットワーク、ソフトウェアに関する基本的知識を、最低限度、身に付ける必要が生じたのである。

## 第 2 節 CBT 試験における重要な課題

CBT 試験システムには、以下の 4 つの重要な課題が存在する。

### 1 課題 1. CBT 試験システム (在宅型) の不正防止機能の実効性に関する問題 (紙ベースの従来型試験と比較してより容易に不正が可能になってしまわないか)

CBT を用いた「試験システム」は、コンピュータ・プログラムやネットワークシステムを駆使して実装されている。紙や講堂における従来の試験と比較して、実装の技術的難易度が高く、実装されたシステムは、高度・複雑となる。現時点では、試験実施主体自らがこれらのシステムを開発・構築・運用することが困難であるから、民間企業が開発したものを利用せざるを得ない状態である。

そこで、当該システムについて営業上・仕様上宣伝広報されている不正防止機能が、本当に、従来の紙ベースで実施していた試験と比較しても、十分なものであるか、という問題を検証する必要がある。従来の紙ベース試験における不正行為と比較して、簡単・低コスト・発見可能性が低い形で、一部の不正受験者によって出し抜かれ、不正受験者の不正行為を見抜けない状態が生じているならば、その問題が解決されるまでの間、当該 CBT 技術を活用することは困難となるためである。

一般に、紙ベースの集合試験でも、集合型 CBT 試験システムを用いた集合型試験であっても、在宅型 CBT 試験システムを用いたオンライン試験であっても、懸念されるリスクは、ほとんど同一であり、列挙すると、次のとおりとなる。

- (a) 替え玉受験
- (b) 支援者への相談と助言の受領  
(音声、モールス信号、イヤホンや電話等)
- (c) 紙情報の摂取  
(カンニング・ペーパー、参考書籍等)
- (d) オンライン情報の摂取  
(スマートフォン等によるインターネットアクセス)

これらの脅威が、紙ベースの集合試験と比較して、特に、在宅型 CBT 試験システムを用いる場合に、高難易度となるのであれば良い。しかし、逆に低難易度になってしまう自体が生じるとしたら、従来型の集合型紙試験から在宅型 CBT 試験への切り替えは、許容されなさそうである。

よって、これらの受験者による不正行為を防止できる仕組みを、従来型試験と同等の水準で実現する技術的方策が重要となる。

## 2 課題 2. CBT 試験システム (在宅型であっても、集合型であっても) の運営者 (業者) が不正に荷担する可能性の問題

CBT を用いた「試験システム」(在宅型であっても、集合型であっても) の問題文配信機能は、紙と異なり、業者の所有するコンピュータ・プログラムやネットワークシステムによって形作られるコンピュータ空間上で、試験直前まで管理される。答案内容も、同様に、コンピュータ空間上に蓄積される。

従来型の集合試験会場において視覚的に実行が可能であった、各種不正行為防止のための試験監督作業も、受験者の宅内の PC に接続されている Web カメラの録画と、その録画データが、サイバー空間上に蓄積された結果の録画データの分析に取って代わられる。

すなわち、CBT 試験においては、コンピュータ空間上 (在宅型においては、インターネット上) に試験会場や答案データ保管・採点施設が存在する状態になるといえる。

そこで、サイバー空間上の性質をあわせて考えると、公平・公正な試験の実施に関して、以下のような脅威が存在することが分かる。

### (a) 問題文の不正読み出しリスク

問題文配信機能については、事前に問題文が試験業者によって読み出され不正利用されないことのシステム上の保証が必要である。

ところが、コンピュータ空間上で、システム全体を自ら完全にコントロールでき

るシステム提供業者が、果たして自らでも試験問題を見ることができない試験問題の事前登録方法を、システム上の実装・運用し得るのだろうか。これは、最大の懸念事項である。

すなわち、紙の試験問題であれば、試験会場で試験開始 1 時間前くらいに業者の誰かがルールを破って事前に封印を開封すれば、その証跡が物理的に確実に残る。試験実施主体は、業者に対して責任追及したり、試験そのものを全部無効にして後日やり直したりできる（やり直しの費用も、業者に賠償請求できるであろう）。

これと比較して、CBT を用いた試験システム（在宅型であっても、集合型であっても）では、プログラムを自由自在にコントロールすることができる業者（極論をいえば、その業者の代表取締役等の経営者たち）は、試験問題を容易に事前に読もうとすれば読めてしまい、そのことが試験実施主体に気付かれることもなくなる状態が存在し得るのではないか、という問題である。

## **(b) 答案データの改ざんリスク**

試験終了後、不正な囑託を受けた試験業者が、特定の受験者の答案データを修正するなどの不正行為ができる状態になっていないか、という問題がある。

この問題も、業者内の最高レベルの技術者や代表取締役等の経営者たちは、絶大な権力・能力を有しており、自らの支配するシステムや生データベースを、監査ログを含め、すべて改変することができる可能性がある。

すなわち、前述の (a) の問題文配信機能において問題文を、試験実施主体がオンラインで登録した、またはオフラインで事前送付した問題文を、業者が盗み出したことが気付かれないのと同様に、不正な答案データの書き換えについても、業者内部の行為として、試験実施主体に全く気付かれることなく、実行可能なのではないか、それを防ぐ技術的手立ては、果たして存在するだろうかといった問題が生じてくる。

### (c) AI 検出アルゴリズムやパラメータの不正調整リスク

特に在宅型 CBT 試験システムにおいては、試験中の不正行為防止の能力が、ほとんど Web カメラの録画データおよびその AI 検出手法の保存や精度にかかっている。

ところが、これらは業者のブラックボックスの中にある。そこで、業者が特定の受験者から囑託を受けて、AI 検知のアルゴリズムやパラメータをその受験者に対してのみ変更し、または録画データを差し替えて、不正を隠してしまうことが可能なのではないか、という問題が生じてくる。

## 3 課題 3. (主に在宅型の) CBT 試験システム運営者 (業者) がパブリッククラウドを用いる場合におけるパブリッククラウド運営業者が不正に荷担する可能性の問題

### (1) 利用システムがパブリッククラウド上で稼働している場合、直接契約関係がないクラウド事業者に命運を握られる

前記の課題 2 では、CBT 試験システム運営者が当該システムを完全にコントロールできることから生じる CBT システム業者が引き起こせる不正行為について述べた。

ところが、在宅型 CBT 試験システム運営者のシステムは、さらに、パブリッククラウド上に存在する場合も多い。仮にそのシステムがパブリッククラウド上に存在するとしたら、パブリッククラウド運営者のレイヤにおいても、この問題と全く同一の脅威が生じる。

すなわち、パブリッククラウド運営者の有力な経営者あるいはパブリッククラウド運営者の社内で権力と能力を有する一部の技術者たちは、当該パブリッククラウド上のすべてのシステムおよびデータの挙動を、完全にコントロール (読み書き) することができる能力を有している。この種のコントロール能力は、監査システムをも上書きすることが理論上・技術上可能である。

すると、パブリッククラウドの契約者に気付かれることなく、パブリッククラウド運営者自らは、契約者のサーバー上のメモリやストレージ等に蓄積されたデータ

の読み書きが可能である（読み取る難易度はかなり低い。書き込み難易度は、不整合を発生させないように書き込む必要があるので、それなりに高い。）。

例えば、試験実施主体が在宅型 CBT 試験システム A を利用し、システム A がパブリッククラウド B を利用しているとする。試験実施主体としては、A の所有者（試験代行業者）と、B の所有者（パブリッククラウド事業者）の両方による不正を、常に警戒しなければならない。この 2 層の不正リスクは、重なり合って生じる。そのいずれか一方の者が不正を行なうと、試験の公平・公正が失われるという、かなり高いリスクである。

そして、このような 3 者間関係においては、A または B のシステム層よる不正の疑惑があった場合、試験実施主体からの責任追及上、厄介な問題が発生し得る。試験実施主体が在宅型 CBT 試験システム A を利用するならば、試験実施主体と在宅型 CBT 試験システム運営者とは契約関係にあるが、この時、実はシステム A がパブリッククラウド B 上で動作していたとすれば、試験実施主体とパブリッククラウド B の運営者との間には、契約関係が存在しないことになる。ところが、パブリッククラウド B が不正なことをしないかどうかは、当該試験の公平・公正さを、直接左右する状態になっている。すなわち、試験実施主体からみると、自らと直接契約関係がない、知らない第三者に、自らの命運を握られているという、経営的にみて極めて高いリスクを押し付けられる状態が発生している。

ここで契約関係を今一度分析してみよう。試験実施主体と在宅型 CBT 試験システム運営者とは、当然直接契約関係にあり、報酬対価を授受している関係にあるので、在宅型 CBT 試験システム運営者が裏切る可能性は、比較的少ない。

また、契約内容にもよるが、在宅型 CBT 試験システム運営者は、試験実施主体からいつでも報告を求められたら、すぐに報告する義務を負っていることが普通である。

さらに、在宅型 CBT 試験システム運営者は日本企業であることも多く、同じく日本の組織である試験実施主体にとって、ひいては日本国民に対して不利益な行為をとる可能性は、外国企業と比較すると、相応に低い。

加えて、試験実施主体は、在宅型 CBT 試験システム運営者に対して、直接質問

し報告を求める権利を行使し、契約で定められている範囲で、一応、直接監査を行なうこともできるであろう。

そして、在宅型 CBT 試験システム運営者に何か不正な行為があれば、これは、試験実施主体に対する債務不履行責任として、試験実施主体は、容易に在宅型 CBT 試験システム運営者を責任追及して賠償請求できる。

このような契約上および国籍上の仕組みにより、在宅型 CBT 試験システム運営者が、あからさまな不正を行なう可能性は、こういった契約がなかったり、外国企業であったりする場合と比較して、もともと、ある程度、抑制されていると期待し得る。

## (2) 直接契約関係にない第三者であるパブリッククラウド事業者の不法行為の責任追及は、相当ハードルが高い

ところが、これと比較して、前述のとおり、試験実施主体は、CBT システムが動作しているより下位のレイヤであるパブリッククラウドとは何の契約関係もない。それなのに、すべてのシステム上の権限を、すなわち不正が発生するか否かの命運を、見ず知らずの第三者である、パブリッククラウド運営業者によって支配されてしまっている構造になっている。

試験実施主体は、何の契約もないパブリッククラウド運営業者に対して、直接報告を求めることも、直接監査を行なうことも、直接質問を行なうこともできない。

そして、パブリッククラウド運営業者が何らかの不正な行為を行なったとしても、試験実施主体としては、その不正行為は、契約関係がないことから、債務不履行責任として追及できずに、不正行為責任としてしか、責任追及できない。

債務不履行責任の立証ハードルはとても低く、債務を履行したことの証明がされなければ不履行だと主張できる。これと比較して、不正行為責任の立証ハードルはとても高く、不法行為があったことの証明に試験実施主体の側が成功しなければ、パブリッククラウド運営業者を訴えて、不法行為で発生した損害を賠償してもらえないのである。

これは、すなわち、不正な行為があったことの立証責任が試験実施主体の側に転

換されてしまっていることになる。パブリッククラウド運営業者側は、自らに不利な証拠を出すことはないので、不法行為の証明はほとんど不可能である。

加えて、パブリッククラウド運営業者は、われわれ日本人との間で共同の利益を共有する関係にない、異国の企業であるケースも多く、その場合、日本の組織である試験実施主体にとって、ひいては日本国民に対して不利益な行為をとる可能性は、日本企業と比較すると、相応に高いといえる。

このように、在宅型 CBT 試験システム運営者がパブリッククラウドに依存し、パブリッククラウド上でシステムを稼働させてしまっている場合、在宅型 CBT 試験システム運営者すら与り知らないところで、いつの間にか、パブリッククラウド運営業者により、試験システムのデータの不正な読み出し (例えば、登録問題文の事前読み出し行為) がなされるリスクは、相応に存在すると考えることができる。

👉 下位レイヤのクラウドサービス事業者の不法行為責任を追及できなくても、直接契約先である試験代行業者 (CBT 試験システムを構築・運営する事業者) に対して債務不履行責任を追及すればよいのではないかという反論があり得る。しかし、3 つの点で限界がある。

第一に、試験代行業者に債務不履行があっても免責となり、同時に、その原因を作り出したクラウドサービス事業者の不法行為は (仮に立証できれば) 免責とされない場合があり得る。このように、試験実施主体がクラウドサービス事業者に対してしか責任追及できない場合があり得る。

第二に、試験実施主体—試験代行業者間の関係と、試験実施主体—クラウドサービス事業者間の関係とは、異なる関係なので、それぞれの関係における責任追及では、法的に異なる判断がなされる可能性がある。そのため、前者の関係とは別の問題として、後者のクラウドサービス事業者の責任追及が、技術的に可能か否かは、重大な問題である。

第三に、クラウドサービス事業者が過失または故意 (システム権限の悪用等) して引き起こすことができる損害の大きさは、試験代行業者のそれと比較して極めて大きい場合があり得る。このとき、試験実施主体は、試験代行業者の資力の見積りにおいて、試験代行業者が引き起こす可能性がある損害の額とちょうど同じ資力が

あると信用して契約したとする。クラウドサービス事業者のそのシステム特権上の立場が原因となり引き起こされた損害が、その性質上、より大きい金額となった場合、たとえ試験代行業者に債務不履行責任を追求できるとしても、試験代行業者が無資力に陥る可能性があり（試験代行業者がクラウドサービス事業者の責任追及に成功するか否かは別の問題なので）、この場合、試験実施主体は、別途クラウドサービス事業者を責任追及できなければ、無資力部分の損害を負うことになる。

よって、いざというときに、下位レイヤのクラウドサービス事業者に対する直接の責任追及ができるかどうかは、試験実施主体の命運を左右する、極めて重要な経営上の問題であることに変わりはない。

### (3) 集合型 CBT 試験システムでも、サーバーがパブリッククラウド上であれば、同じリスクが発生する

上記の脅威は、在宅型のみならず、集合型の CBT 試験システムであっても、試験処理を担うサーバーがパブリッククラウド上に存在する場合は、全く同じように存在する。

### (4) パブリッククラウドを利用せざるを得ない場合は暗号化等の最大限の追加的工夫が必要となる

このように、パブリッククラウドを利用することには、機密性・完全性に関してかなりのセキュリティ・リスクがあり、これは重要な未解決問題である。ところが、残念ながら、日本のコンピュータ業界は、この 20 年間でシステムソフトウェア領域の人材育成に失敗してしまっており、パブリッククラウドに依存しないセキュアなシステムを自らの組織で構築することができる若手人材が、圧倒的に不足してしまっている。そのため、日本企業であることが多い CBT 試験システム運営者としては、いわば緊急避難的に、パブリッククラウドを利用せざるを得ない状態となっている。

このような日本のコンピュータ業界の能力の弱体化を考えると、パブリッククラ

ウドを利用している CBT 試験システムを、リスク対策の観点から排除するとなれば、優れた CBT 試験システムの多くが排除されてしまい、むしろ試験実施主体にとって不利益な結果になりかねない。

そこで、試験実施主体としては、現在は、CBT 試験システム運営者が緊急避難的にパブリッククラウドを利用せざるを得ない状態にあるとしてこれを許容する必要がありそうである。しかし、その場合であっても、ソフトウェア・プログラムやサーバー運用方法に最大限に工夫を施すことを CBT 試験システム運営者に対して常に求める必要が生じる。

すなわち、たとえパブリッククラウド運営者の経営者または技術者たちが、不正なユーザーデータの読み書きを行なおうとしても、容易にそれができないようにするために、各種の暗号化技術や難読化技術等の予防策を駆使した対策を施す必要があるということである。

データをパブリッククラウド上に保存したり、メモリ上で一時的に処理をしたりする場合においても、パブリッククラウドを利用する上では、パブリッククラウド事業者によってもそれらのデータが盗み見られないように、機密保持の工夫を実装する必要がある。

そして、これらの暗号化手法においては、パブリッククラウド側の提供する適切な表面的暗号化手法（たとえば、ユーザー提供の復号化キーを、データの読み書きの都度、パブリッククラウドの提供する API 窓口に対して、都度指定するような手法）等に決して頼ってはならない。パブリッククラウド側の提供する表面的暗号化手法は、仮に不正を画策するパブリッククラウド側技術者が存在するとして、その不正侵害者の立場からみると、あたかも、被害者が金庫を施錠しているけれどもその金庫の上にキーを置いておくこととほとんど同一の無意味な結果を作り出すことができるためである。

そのため、パブリッククラウド側の提供する表面的暗号化手法に頼ることなく、CBT 試験システム運営者自らが、自前の責任・コントロール範囲内における実装方式として、安全確実に暗号化を施し、不正を画策するパブリッククラウド側技術者に対抗できる状態にしておく必要がある。

ただし、こういった一見十分な暗号化も、パブリッククラウド上のすべてのプロセスのメモリを自由に参照できてしまうという（したがって、プロセスメモリ上の秘密鍵も読み出すことができる）パブリッククラウド運営者の絶大なシステム特権からみると、実は、究極的には無力である。

それでも、このような暗号化対策を万全に施すことは、不正が行なわれるコストをある程度引き上げることを可能とするので、一定の効果がある。

その他、パブリッククラウド事業者が「耐タンパ性が存在する」と主張するハードウェアを用いた暗号化メカニズムを利用するという方法もあるかも知れない。しかし、この物理的実装が本当に耐タンパ性を有するのかどうかの保証があるか、言い換えれば、実はパブリッククラウド事業者だけは、機密鍵に何らかの方法でアクセスできるのではないかという懸念を払拭することができないケースも、豊富に相当し得る。これも、金庫を施錠して、その金庫の上にキーを置いておくことと理論上ほとんど同一の無意味な結果になる。

重要なのは、これらの色々なケースを想定して、多重のレイヤで暗号化を施し、パブリッククラウド事業者の不正侵害者が不正な復号化や書き換えを実行しようとしても、極めて困難である（たとえば、不正侵害者によるリバースエンジニアリングや不正読み出しの後の復号化のためのコストがかかり、このコストが、不正に読み出される試験問題がブラックマーケットで販売される場合における価値を大幅に上回る）というような状態を、常に維持する必要があることになる。

#### (5) 試験実施主体は、パブリッククラウドを利用している CBT 試験システム運営者に、機密性保持の対策をあれこれと技術的に試問しなければならない

ところが、CBT 試験システム運営者においては、パブリッククラウド運営者が、一切その低レイヤにおける権限を悪用した不正を実行することはあり得ないといういわば盲信の元で、システムを設計・開発して、パブリッククラウド上でこれらアプリケーションを動作させているケースも、おおいに存在し得る。

したがって、重要な試験を担う試験実施主体の立場としては、パブリッククラウ

ド運営者によるより低レイヤの不正を想定し、その不正に対する防護手段を講じているかどうかを、CBT 試験システム運営者に対して、必ず確認しなければならない。確認としては、上記のような、パブリッククラウド運営者が最大限の権限を活用してもなお機密データが読み書き困難となる状態を維持するような工夫の有無を、実際にソースコードの提出を受けるなどして、試験実施主体自ら、その対策を確認しなければならない。

このことから、パブリッククラウドを利用している CBT 試験システムを利用する場合は、試験実施主体の側に、相当の技術能力とリテラシーが求められることになる。そのような一定水準の能力を有する職員人材の育成・獲得が、ますます、各試験実施主体における急務となってくるのである。

#### 4 課題 4. 可用性および完全性の問題 (紙ベースの従来試験よりも受験者の不利益やリスクが増えないか)

試験というものは、必ず、受験者の人生に何らかの影響を与えるものである。そこで、特に重要な試験においては、試験実施主体は、試験中に試験が中断してしまうことがないように、試験システムの可用性 (試験が滞りなく実施できること) および完全性 (試験の答案内容が変質・滅失しないこと) について、万全の対策を施す必要がある。

従来の集合型の紙の試験においては、一度物理的に印刷した紙の問題用紙が試験中に突然読めなくなる事態 (印字されたインクが突然全部消えるなど) は、まず発生しない (せいぜい、落丁・乱丁・印刷ミスがある程度であり、その場合は、問題用紙を交換すれば対応可能である。)。そこで、従来型試験の可用性に対する脅威は、おおむね、天災等の発生、会場における停電、会場付近における音響的じょう乱の発生 (例えば、試験会場付近の道路での街宣車などによる演説行為)、試験会場への不審者の乱入等、試験会場付近における物理的事象に限定されてきた。そして、試験の完全性について考えると、試験の最後に受験者が答案用紙を提出したならば、その答案用紙も紙であったので、その文字が勝手に消えてしまうという心配も、ほとんど考えられなかった。試験実施主体または代行業者による答案用紙の紛

失・滅失が、ほとんど唯一の脅威であった。これらのリスクを軽減させるための各種の措置は、いずれも物理的なもので足りるので、試験実施主体自らリスク対策することが可能であった。

試験実施主体に対する契約上の責任として、試験代行業者ももちろん責任を有しているが、重要な試験は、失敗が許容されず、一年に一回限りのものであることも多く、このような場合は、失敗時に回復不可能な損害が発生するので、これを予防するために、試験実施主体は、代行業者の手中における対策を盲目的に信頼することでは足りず、自ら試験代行業者と一体となって、自ら現場に出向き、物理的なリスク対策を講じることで、ほぼ完全な脅威への対処を行なってきた。その結果、これらの可用性・完全性に対する脅威が発生するリスクは、これまで、かなり低い状態で維持されてきたのである。

このような確実な実施のためのノウハウが、物理空間・物理法則に基づいて積み重ねられてきた従来の紙による試験と比較して、CBT 試験システムはコンピュータ空間上で動作するものであるという特徴を要する。そのため、試験中および試験完了後における、可用性・完全性の保障は、コンピュータ空間上の各種セキュリティ措置 (サイバーセキュリティ) によって講じる必要がある。

ところが、CBT 試験システムの実装 (プログラム) およびその実装を稼働させるサーバーコンピュータならびに関係するサービス・コンポーネント (データベース等) は、試験実施主体の手元を離れ、CBT 試験システム提供業者 (試験代行業者) の手中にある。

そこで、試験実施主体としては、従来行なってきたような確実なリスク対策をどのようにして代行業者に講じさせることができるのか、その実効的手法を知る必要がある。そのためには、試験代行業者の運営するシステムにおいて、どのような可用性および完全性上の問題が存在するか、確実に理解した上で、それについて試験代行業者を厳しく試問することで、対策を確実化する必要がある。

CBT 試験システムにおける可用性および完全性に対する課題は、おおよそ、以下のような点に存在する。

(1) 在宅型 CBT 試験システムでは、通信にインターネットを利用しているが、インターネットの特性上、受験者と在宅型 CBT 試験システムサーバーとの間の通信はいつでも突然切れてしまう可能性がある

インターネットは、複数のネットワーク運営主体を数珠つなぎにうまく接続した、性善説に基づく、本質的に不安定なネットワークの上で、かろうじて確立されるので、安定性は保証されていない

受験者と、在宅型 CBT 試験システムのサーバーとの間の通信は、試験実施主体に対して確実な責任を果たすことができる単一の通信事業者によって処理される訳ではない。受験者とサーバーとの間の通信は、「インターネット」と呼ばれる、相互に独立した直接の契約関係がない複数のネットワーク運営主体を数珠つなぎにうまく接続した、性善説に基づく、本質的に不安定なネットワークの上で、かろうじて確立される。したがって、インターネットを利用して通信を実現しようとする行為そのものが、試験に求められる水準の可用性の実現という目的と、本質的に相反するのである。

近時のインターネットは、それなりに安定してきているので、多くのインターネットユーザーは、あたかも、インターネットにいったん接続さえすれば、自らと、インターネット上の任意のサーバーとの間の通信が、常時保証されるというような認識的誤解を有している。しかし、これは、全くの誤りである。そのような安定性の保証は、インターネットの構造上、不可能である。

### インターネットの動作原理の簡単な解説

このことを理解するためには、インターネットの本質について、若干の深い理解が必要不可欠である。そこで、インターネットの動作原理について、簡単に解説をする。

インターネットの本質は、複数のネットワーク運営主体が、互いに自らのネットワーク・リソース (通信経路) を、世界に対して開放・共有する (持ち寄る) ことを宣言し、BGP (Border Gateway Protocol) というかなり自律的で自由なプロトコルで、通信経路を持ち寄った無数の主体同士が、手を取り合って世界をいくつもの輪で囲むようにして包み込んだ上で、その包み込みの網の目のいずれか一点と、

別の一点との間で、通信が試行されたとき、電光石火のごとくその通信をうまく二点間で伝送するよう努力するという仕組みで構成されている点にある。現在のインターネットの仕組みは、1960年代～1980年代、当初かなり局所的な行政的目的（たとえば米国政府の国防総省内のある行政部署と、共同研究をしている大学間の、合計3個のホストコンピュータ間の相互接続の需要を満たすためであった）のために実験的に作られた数々の通信の方式や規約が、後に大変に人気となって、その方式や規約に沿った通信システムのソフトウェアをさまざまな主体が自作して接続し合い、それが結果としてうまく動作している、というものである。

インターネットを支えている各種方式、規約、運用方法は、法令等で定まっているわけではない。これらは、ボランティア精神が溢れる大学や行政や企業の研究者や技術者たちの自由な発想と試行錯誤によって事実上支持されているに過ぎず、また、動的なものであり、日々進化をしている。

インターネット全体は、時々深刻な不具合が発生するものの、技術者たちは、その時々々の知恵に応じてうまく問題を回避し、回復を試みているのである。このように、まず、インターネットというのは、その全体的動作の安定性について何者かが責任を有している訳ではなく、インターネット内の任意のPCとサーバーとが正しく通信できることについては、何らの物的担保も、法的担保も存在しないことに注意する必要がある。

インターネット上で、2つの通信主体（試験システムにおいては、受験者のPCと、試験サーバーの2者である）が相互に通信しようとするとき、4パターンが存在する。

#### **ア. 当事者間で単一のネットワーク運営者に閉じた折返し通信がなされるパターン**

偶然、仮にこの2つの主体が同じネットワーク運営者と契約関係にあれば、この2つの主体の間の通信の可用性は、その契約によって保証され得る。つまり、当該ネットワーク運営者一者だけの設備だけで、確実に当事者間の通信ができることになる。もし通信ができなければ、それは、当該ネットワーク運営者の責任となり、責任追及し得る。

## イ. 当事者がそれぞれ契約する両端のネットワーク運営者間が相互接続契約を締結しているパターン

2 つの主体が異なるネットワーク運営者とそれぞれ契約関係にあるときでも、その 2 つのネットワーク運営者の間で、相互接続契約が存在していることがある。相互接続契約に基づき、それらの 2 つのネットワーク同士は、直接接続されている。両方のネットワーク運営者は、その相互接続契約に基づいて互いに自らの利用者の通信を相手方に伝送するべき旨を請求できる。そのため、この場合、2 つの主体の間の通信の可用性は、これらの契約関係の連結によって、保護され得る。

この関係は、電話網をイメージすると分かりやすい。例えば、日本には、複数の電話会社が存在する (NTT、KDDI、ソフトバンク、ケーブルテレビ会社、携帯電話会社等である。)。それらの電話会社間では、必ず、相互に、「相互接続契約」が締結されている。これにより、自社の電話会社の顧客の通信は、他の電話会社の顧客と必ず通話することができる。もし通話に何か問題があれば (つながらない、音質が不良である等)、その原因は、(i) 一方 (自身) の電話会社の不具合か、(ii) もう一方 (相手方) の電話会社の不具合か、あるいは、(iii) その相互接続点の不具合かのいずれかの 3 点のうち 1 点に、確実に定まる。(i) 自身の電話会社に問題があれば、契約関係に基づいて、直接修理を請求すればよい。(ii) 相手方の電話会社に問題がある場合は、2 つの電話会社は相互契約関係にあるので、相互接続契約に基づいて相手方の責任を追及することで、自己の電話会社は、顧客に対する責任を果たすことができる。(iii) 相互接続点に問題があれば、そこは共同部分なので、顧客に対してはそれぞれ自らの電話会社が修理する義務がある。すなわち、顧客に対する電話会社の関係としては双方が連帯債務関係となる。そして、電話会社同士の関係としては、隣接電話会社に責任がある部分については隣接電話会社に責任追及できる。これらの責任の連結により、電話会社は、必ず、顧客に対する責任を果たすことができる。電話網は、品質保証がなされているネットワークであるということができる。

## ウ. 当事者がそれぞれ契約する両端のネットワーク運営者間の間に共通のトランジット事業者が存在するパターン

上記のイのパターンだけでは、遠く離れた異国の電話会社同士でも、相互に契約を締結する必要があり、国際電話網の発達において不便であった。そこで、国際電話に代表されるような接続形態において、特定の宛先の集団の電話会社宛の通信を全部請け負う形の中間トランジット事業者が出現した。

当事者がそれぞれ契約する両端のネットワーク運営者間は、同一の中間トランジット事業者と接続契約関係にあるので、一旦のネットワーク運営者は、もう一旦のネットワーク運営者を宛先とした通信を、当該単一の中間トランジット事業者に託送して（伝送業務を請け負いさせて）届けてもらうことができる。

これは、電力事業における、電力自由化制度の託送契約と同じようなものである。この際、両端のネットワーク運営者間と中間トランジット事業者との間では、必ず契約が存在し、その契約に基づいた義務の履行として、託送がなされる。よって、中間トランジット事業者の設備不具合があった場合でも、顧客に対する責任としては、顧客が契約する電話会社が、託送を担っている中間トランジット事業者に責任追及すればよく、これにより、電話会社は、顧客に対する責任を必ず果たすことができる。

このように、インターネットが登場する前の電話会社のネットワークである電話網においては、基本的に、上記の ア、イ、ウ のパターンいずれかしか存在しなかった。いずれのパターンも、通信を行なう当事者 2 者間の通信の可用性に対する責任は、事業者間の契約関係によって、何らかの形で担保されていることが分かる。契約関係上どこかに穴があるというような例外的場合を除き、いずれの場合も、無責任状態に陥ることはない。したがって、電話網の可用性は、制度上担保されてきたといえる。

ところが、インターネットが画期的だったのは、その動作原理上、以下の エ のパターン（素晴らしい無責任パターン）を積極的に容認したことにある。

## エ. 当事者がそれぞれ契約する両端のネットワーク運営者間との間の通信を 1 個または複数の契約関係のないネットワーク運営者たちが数珠つなぎ方式で送り届けるパターン（素晴らしい無責任パターン）

インターネットの革命性は、当事者がそれぞれ契約する両端のネットワーク運営者間が直接接続されておらず、その間に、全く契約関係のない複数のネットワーク運営者間が「トランジット」として介在し、そのトランジット経路を経由して通信が流れるという形態を、通信の仕組み上、積極的に許容した点にある。

この、インターネットにおける独特のトランジット通信は、ウ のパターンような単一の間トランジット事業者と両当事者とが接続契約を締結していることを全く要しない。間にトランジットを提供するネットワーク運営者が複数存在するパターンも豊富に存在する。それらの間で連鎖的契約関係、言い換えれば、通信に不良が生じた場合に顧客に対してその不良を修理する責任を果たすことを確実化する制度的な関係が存在しない。

このかなり自由で自律的なトランジットの仕組みにより、直接契約関係なく、また品質について何ら保証をすることもなく、実験的に自作したネットワークや機器、通信ソフトウェア等を持ち寄って、次々につないでいき、世界全体を網の目で覆うことに成功したのが、現代のインターネットである。通信経路上において連鎖的契約関係を必要としないことから、誰でも、ボランティア的に自分のネットワーク通行権を、全く見ず知らずの人たちのネットワーク同士の通信経路として、世界中の通信ユーザーに対して、無償で差し出すことができるようになっているのである。

物理社会におけるイメージで考えると、インターネットとは、互いに独立関係にある領主が無数に存在する大陸のようなものである。このイメージの世界において、各領主は、自らの領有地を、通行人との直接契約関係がなくても自由に誰でも通行してよいと宣言して開放する、気前の良い領主達の任意の隣接地域間の接続同盟のようなものに参加している。従来、領主達が隣接地域との間で関所のようなものを設置して、許可を得ないと通過させないとか、税金を支払えというような形で収入を得ていたのを、全体的利益を優先して考えて同盟を組み（しかも、その同盟は何ら法的に担保されている同盟ではなく、明文化もされておらず、事実上のムー

ブメントに過ぎないボランティア精神的なものである)、一々通行チェックしないことにしてみたら、その領主達が存在する大陸全体が大いに発展して、すべての領主たち (インターネットの運営組織達) は、大いなる共同の利益を受けた、というものである。

上記のような領主たちの例において考えると、インターネットでは、各領主は、隣接する領主との間でだけ、契約を締結している (していない場合もある) のである。隣接地点においては、通行する人を妨げないとか、我が方からの通行人が多ければ我が方は相手方に差額の料金を支払うというような最低限の契約があり得る (契約がろくに無い場合も多い)。ここで極めて重要なことは、各領主は、世界中に存在する直接隣接関係にない他の領主たちとの契約関係が全くなく、そもそも会ったことすらなく、互いの存在すら、個別具体的に意識していないということである。間接的につながっている少し離れた別の領主のところからきた通行人を、自らの領域を通過させる際、領主とその通行人との契約関係も、また、領主とその通行人の出発元の領主との契約関係も、一切存在しない。契約関係がないので、領主は、通行人に対して、原則として、品質維持責任を果たす義務がない。何か聞かれたら、領主は、「貴殿が、通過したければ、我が領土を自由にかつ無許可で通過してもよいが、我が領土は最近結構混み合っており、スムーズに通過できるかどうかは、保証しない。嫌ならば、通過しなければよいであろう。」と宣明するくらいであろう。もちろん、領主が意図的に自領土を通過する通行人に対して、加害をした (たとえば、通信内容を勝手に書き換える) とか、領土に危険なものを放置してそれが原因で通行人が死傷した (たとえば、落とし穴のようなものができていて、それをあえて放置し、全通行人がそこに落ち込んで地面の底に吸収されてしまう) とかであれば、それは別の次元の問題で、そのような領土を管理する領主には、加害者として、大いなる責任が生じる。しかし、そういった意図的な加害でない限り、領土の中が最近ある程度混雑しているとか、または、大雨で地面がぬかるんでいて、いまいちスムーズに前進できないということがあっても、その領土の領主としては、その状況を意図的に作り出して通行人に対して加害しているという訳ではなく、ボランティア的に自分の領土の通過を許容しているだけに過ぎないから、高い品質を

常時保証する責任が生じない。

インターネットにおいては、上記のような各通過地における領主の責任のイメージをもとに、「ベストエフォート」（できるだけ努力する）という品質概念が形成された。すべてのインターネットアクセスを提供するネットワーク運営主体は、ユーザーに対して、決して通信品質を保証しない。仮に品質を保証せよとしたならば、上記のイメージにおける世界中の領主は、他の全領主と契約を締結する必要があることになってしまう。しかし、領主の数は数万にもものぼるし、毎日のように増加したり離脱したりするので、全員と契約することはできないのである。

インターネットへのアクセスを提供する典型的なネットワーク運営主体は、商用ISP（インターネット・サービス・プロバイダー）であるが、ユーザーの通信相手先が偶然自らのISP内の他の顧客のサーバーであるとか、直接接続契約を締結している他のISP上のサーバーであるというような稀な場合を除き、ISPは、通信品質は保証しない。品質保証をしないという意味は、速度が低下したり、通信内容が欠落したりすることがあるというだけでなく、そもそも、特定の通信相手との間で、全く通信ができない場合もあり得るという意味である。

通信をしようとする通信当事者間を偶然に結ぶ経路の間のいずれか1点の領主の設備に問題があり（たとえば、ルータと呼ばれる装置のメモリの特定一ビットが故障していてビット反転が起きる等）、そこで一定の条件を満たした通信内容が、常に損傷して、パケットが滅失しまう問題も、容易に発生し得る。

通信パケットの長さや性質によってだけ通信切断の問題が発生するようなことも多く、なかなか気付かれない。善意に満ちたプロバイダーが、その原因を究明しようとしても、途中の領主の土地に立入って管理者として色々調査しなければ分からないことが多い。ところが、それは、他の領主の主権を侵害することになるので、できないのである。

このように、インターネットは、かなり自由奔放な相互独立した領主たちの自主的同盟によって互いに連結され、何か不具合があってもどこが原因でそれが生じているのなかなか分からず、さらに意図的に発生させた加害行為でもない限り、不具合を生じさせている途中通過点の領主に対して責任追及ができないという、良い

意味で、かなりいい加減な仕組みで成立している。

言ってみれば、インターネットは結構無責任な世界最大のネットワーク相互接続連邦である。したがって、インターネットの黎明期（1960年代以降）においては、こんなものがうまく成立する訳はないという主張がなされた。電話会社はインターネットに懐疑的であった。さらに、このようないい加減なネットワークが万一それなりにうまく成立してしまったならば、品質保証で高い対価を得てきた電話会社の課金ビジネスが、すべて崩壊するリスクがある。そこで、電話会社は、インターネットの成立にかなり抵抗してきた。ところが、そのような抵抗に遭っても力強く前進し続けた全世界のインターネット研究者たちの努力により、実際のインターネットが形成されてきた結果、その無責任性とトレードオフの関係として、ほとんど無料同然で、全世界の通信相手と、それなりに良い性能で通信ができているという利点を実証された。そして、実際にインターネットはそれなりに安定してきたので、商用でも利用できるようになり、現代社会において、大いに普及したのである。

そこで、昔は声を大にしてインターネットに反対していた電話会社たちも、現在は、何食わぬ顔をしてインターネットへのアクセス回線を提供し、大きな利益を挙げているのである。

このようなインターネットにおいて、仮に品質を担保するために契約の締結をし始めると、現在のような全世界的通信機能は、現在のような月額数百円～数千円の安価な価格では、決して実現されなくなってしまう。

このように、インターネットの無責任性は、それによって得られる利益のほうが桁違いに大きいので、全世界のインターネットユーザーおよび運営関係者集団によって、今のところ、支持・承認されてきているのである。

👉 インターネット経由の通信の多くが、ユーザーが所属している ISP とサーバーの接続している ISP のいずれの直接的契約先からもコントロール外にあり、通信の可用性が保証されていないのではないかという問題提起については、インターネット事業者たちから、次のような反論が予想される。すなわち、理論上は確かにそ

うかも知れないが、実際には多くのケースでは、商用 ISP には上流トランジット事業者があり、またその上のトランジット事業者があり、これを順に辿れば、Tier1 という最上流のトランジット事業者に行き着き、これらのトランジット事業者間は、上流が下流に対する契約上の履行責任が必ず存在し、そこに品質保証が付随しているから、全体として、ユーザーとサーバーとの間の通信は、必ず保証されているはずである、という反論である。

しかし、その反論は成り立たない。たとえ事実上そのような場合が多いとしても、必ずすべての場合で、上記のような契約ベースのトランジットを経由することは保証されていないが、それを無視して考えて、仮にすべての経路が契約ベースのトランジット回線を通る場合であったとしても、以下のようなさまざまな穴が存在する。

第一に、契約ベースのトランジット回線は、市場で手に入る大手の最も高品質なトランジット回線契約条件 (SLA: サービス品質保証約款) を確認しても、実は、可用性は保証されていないのである。たとえば、IIJ 社やソフトバンク社の専用線トランジットでは 30 分以下の、NTT PC コミュニケーションズ社の専用線トランジットでは 1 時間以下の完全通信断が起こっても、これらは、契約上完全に免責される契約になっている<sup>①②③</sup>。また、保証というからには、いわば担保のようなもの (保証違反が発生した場合の損害賠償 = 違約金の支払義務) が必要であるが、仮に 1 時間もの完全通信断が起こったとしても、月額料金のわずか約 3% ~ 20% しか賠償 (返金) されない。このように、かなり少ない金額の賠償額の制限が契約上規定されてしまっている。これでは、重要な試験時間内の多くの時間 (30 分 ~ 1 時間程度) の通信障害が発生しても、それはトランジット事業者によって免責されてしまうのである。これらは、前記で述べた IIJ、ソフトバンク、NTT の 3 社の品質が低いという意味ではない。むしろ、これら 3 社の品質は日本国内でも世界中でも最上級である。それでも、前述の水準しか実現しておらず、30 分以内、または 1 時間以内の故障が発生しないということは、契約上、保証されていないのである。

第二に、商用 ISP というものは複数の上流 BGP トランジットを束ねているの

① <https://www.ij.ad.jp/svcsol/agreement/pdf/REG002.pdf>

② [https://www.softbank.jp/biz/nw/internet/lineup/ether\\_access/sla/](https://www.softbank.jp/biz/nw/internet/lineup/ether_access/sla/)

③ <https://www.nttpc.co.jp/service/product/mastersone/#contents--sla>

で、上流 1 社で 30 分 ~ 1 時間の通信断が発生しようとも、BGP の仕組みで瞬時に他の正常な上流に切り替わり、影響はないはずだという反論が考えられる。しかしながら、ある商用 ISP が、たとえ複数の上流回線を束ねて万全の体制を整えていても、上流 ISP との BGP リンクが完全に切れるようなきれいな障害は別として、上流 ISP のバックボーン部分の故障の様態によっては、BGP リンク (制御用通信) は切れずに、通信パケット本体 (実際のユーザーの通信) だけ消失するという障害が発生し得る。この場合、他の正常な上流に自動的に切り替わらないので、結局、通信障害の継続時間は、故障時間と同じだけ生じる。

第三に、上記の点をいずれも無関係に考えても、そもそもトランジット契約が保証するのは、そのトランジット事業者が隣接する接続先 (対等なピアと呼ばれる接続先、または上流の接続先) との接続点までであり、それより先の部分で、特定の相手先と何らかの理由で通信ができなかったとしても、それはコントロール範囲外の無関係部分なので、修理せよという責任追及ができない。

第四に、これは技術的な点を超えて、実際の可用性の「保証」というものの本質に関わるものであるが、上記の点をいずれも無関係に考えても、通信経路を辿ると、外国の通信事業者を経由している場合が生じ得るが、仮にその外国事業者に過失または故意があったとして、外国事業者は日本国の法律に従っておらず、その外国の通信事業者を責任追及するには、当該外国の裁判所に訴える必要がある (なぜならば、たとえ日本の裁判所に訴えてもし勝訴したとしても、当該外国の事業者は日本に資産を有しておらず、当該外国の事業者に対して物理的に執行できない場合が多いため、意味がないからである。)、世界には無数の異なる法や習慣が存在するので、例外的な場合を除き、ほとんどの国の事業者に対して、事実上責任追及ができない場合が多い。

第五に、たとえすべての上流トランジット事業者が正常でも、インターネットに BGP 接続している全世界中の任意の第三者は、通信をしているユーザーとサーバーの 2 つのグローバル IP アドレスを包含する /24 という細かい単位 (256 個単位) の IP アドレス群をインターネット上でいつでも誤って、または故意に広報することが可能であり、この場合は、BGP のレイヤの正常な動作として、トラフィックはその誤った第三者のルータに向けてすべて吸い寄せられてしまう。このような事故または不正は、しばしば発生している。インターネット上では、他人の IP ア

ドレスは、簡単に乗っ取られるのである<sup>①②</sup>。これは、いずれの上流 ISP にも責任がなくとも、無関係の第三者の加害者による不法行為によって、突然自分の IP アドレスが通信できなくなってしまうことを意味する。この問題が発生した場合は、人間的プロトコル (電子メールや電話などの他の手段) で、さまざまな関係者に連絡して、過失または不正行為を行なっている当該第三者をインターネット全体から切り離してもらわなければならないが、それには 1 時間以上かかるので、その間に、試験時間は終わってしまう。この BGP 経路ハイジャックという手法の興味深い点は、「大半のユーザーは通信ができるが、一部のユーザーは通信ができない。」という、試験において致命的な、受験者間で不公平な状態が、世界中のわれわれと全く無関係の第三者によっていつでも発生させられてしまうという点にある。今のところ、インターネットにおけるこの BGP ハイジャック問題に対する現実的に有効な技術的解決策がないので、これは、困った問題である (BGP 経路情報をデジタル署名するという規格は策定されたが、ほとんど普及していない)。

よって、仮に商用 ISP の上流を含めた全体をみて商用トランジット契約が成立していたとしても、ユーザーとサーバーとの間の通信の可用性は保証されない。

そして、われわれが注意しなければならないのは、「通信の可用性が保証されている。」という状態と、「通信の可用性が保証されているような気分になることができ安心である。」状態とは、全く異なるということである。本文書で指摘しているのは、インターネットでは、原理的に、前者の保証は成り立たないのではないかという点にあり、後者の話題ではない。インターネットに関する検討を行なう場合、この 2 つの話を決して混合しないように注意することが重要である。

インターネットの本質と制約を理解した上で、ようやく本題の、在宅型 CBT 試験システムの話に戻ろう。在宅型 CBT 試験システムは、各自宅の受験者との間の通信については、専用の通信網を構築することはコスト的に不可能なので、通信経路は、インターネットを利用せざるを得ない。インターネットを利用する以上、受

<sup>①</sup> <https://xtech.nikkei.com/it/article/COLUMN/20090225/325481/>

<sup>②</sup> <https://gigazine.net/news/20180425-amazon-route-53-hacked/>

験者の自宅のコンピュータと、在宅型 CBT 試験システムのサーバーとの間の通信が確実に維持される責任は、前述のとおり、誰も有していないことになる。したがって、受験者は、在宅型 CBT 試験システムに自宅から接続しようとする際に接続できない場合もあるし、試験中に突然試験サーバーとの間の通信が完全または不完全に切断される場合もある。実際、インターネット上では毎時間のようにこのような障害が発生している。さまざまなインターネット上のネットワークの運営主体の障害情報をみると、頻繁にインターネット内の各所の通信は切れたり復旧したりしていることが分かる。

問題は、受験者と在宅型 CBT 試験システムとの間の通信が切れてしまう場合、大抵は、その原因は、受験者側の責任にもよらず、また在宅型 CBT 試験システム運営者側の責任（受験者との関係上は、試験実施主体の責任）にもよらず、むしろ、その二者の間の通信を経由・媒介する、契約上の責任関係が全くない第三者のネットワークが原因によるものである、という点にある。

インターネットでは、前述のように、自宅のユーザーが接続しているネットワーク運営者（領主）と、そのユーザーがアクセスする際のサーバーが接続しているネットワーク運営者（領主）とが異なり、その間に多数の知らないネットワーク運営者たち（多数の領主たち）が介在して、2 者間の通信を実現している。途中のトランジット状の通信経路の領主たちは、2 者のいずれとも契約関係がないので、責任を負ってくれない。また、実際に切れた原因がどのネットワーク運営者に存在するかも分からない場合も多い。よって、通信が切れたときに、その責任は誰にも無いということになる。

在宅型 CBT 試験システムを利用しようとする試験実施主体は、前記のようなそもそも保証がないインターネットというものを利用しようとする以上、受験者に対して、「自己の責任で、試験中に絶対試験サーバーとの間で切れないインターネット事業者と契約せよ」と要求することは、無意味である。仮にインターネット回線事業者がいかに高品質であって、また回線が切れなくても、そのインターネット回線事業者と、在宅型 CBT 試験システムのサーバーが設置されているネットワーク事業者との間には、インターネット上で数珠繋ぎになった複数の仲介者が存在

するので、それらの仲介者のうち 1 点で通信の不具合が発生するリスクはいつでもあり、それについて、受験者の契約するインターネット事業者は、責任を負ってくれない。試験サーバーとの間の通信が切れないことが契約上保証される (切れた場合に責任を負ってもらえる) インターネット回線は市場に 1 つも存在せず、受験者は、それを調達することは不可能である。受験者に対して不可能を強いることはできないので、そのような要求はできない。

試験実施主体からの視点でみると、インターネットというものは、従来の集合型紙試験において、受験者が試験当日の朝、自宅から道路や利用する通行手段を受験者の責任で任意に選択して、試験会場に時間通りに来る際の、その交通経路に似ていると考えれば良い。試験実施主体としては、試験会場と集合時刻だけを定めておけば良いのであり、その時刻までに受験者が試験会場にアクセスできれば、受験ができ、できなければ失格 (棄権) ということにできる。試験会場と接続する道路は何本も存在し、また、複数の交通手段 (最悪は、自転車や徒歩) が存在するので、受験者の自由なリスク判断で、当日の朝、試験会場に到達できればよいのである。何か不測の事態が生じて (たとえば、電車不通、道路工事)、そのリスクを含めて受験者はより早い時刻から出発することもできたので、大災害のような全員が会場に来られなくなった場合でなければ別として、単に特定の試験会場アクセス経路で障害が発生したことは、不運にもその障害によって受験できなかった受験者のリスク管理不足であるとして、切り捨てるという選択肢である。これと同様に、インターネットを用いた在宅型 CBT 試験においても、受験者側に対して、「結果的に在宅型 CBT 試験のシステムへのアクセスに成功するインターネット回線を、自分のリスクで用意せよ。したがって、もし、1 本の回線では不安があるとしたら、全く異なる運営主体が提供する 2 本以上のインターネット回線を自費で確保せよ。」と要求すればよいという考え方もできる。

ところが、さらに深く考えると、インターネットを用いた在宅型 CBT 試験と、前記の道路の例における集合型紙試験との間では、重大な違いが 1 つ存在する。

従来の集合型紙試験においては、受験者は複数存在している道路を色々と検討し、自らのリスクで利用する経路を選択して、試験会場に時間までに辿り着きさえすれ

ば、それで良かった。いったん試験会場の施設に足を踏み入れて自席に無事に着席したならば、大安心である。その時点以降は、自己の体調不良等を別として（それは受験者自らのリスクである。）、何か不測の自らに責任がない事態が発生して自分だけが不運にも試験の途中で受験を中断させられるリスクというものは、決して存在しないはずである（大地震等の場合は、受験は中断させられるが、これは全受験者にとって発生する不利益なので、一部の受験者だけが不利益を被ることはない）。

ところが、インターネットを用いた在宅型 CBT 試験の場合、一度試験システムへのアクセスに成功して試験が開始されても（これは、先の比喻において、物理会場の自席に無事に座れたことと等価である。）、全く安心することはできないのである。なぜならば、試験が開始されてから終了するまでの間に、いつでも通信不具合が発生する可能性があるためである。このような通信不具合が発生したら、不具合が発生した受験者だけが、試験が続行できなくなってしまう。このような場合に備えて、受験者側のリスクで、長い試験時間の途中で通信が切れずに確実に可能なインターネット回線を自ら選定して用意せよという要求で、受験者側に責任を押し付けることは、不可能な要求であり、極めて酷である。なぜならば、前記のように、そのようなことが保証されるインターネット回線など市場に存在しないためである。

仮にそのようなことを要求したとすれば、受験者としては、確率的に最も良い回線を選択する必要性が生じる。いずれのインターネット回線事業者が、今回受験する在宅型 CBT 試験のサーバー設備がたまたま設置されているネットワークまでの間の通信が最も切れにくい回線事業者であるかを事前に吟味して、契約をしなければならなくなる。しかし、実際にいずれの回線が CBT 試験のサーバー設備がたまたま設置されているネットワークとの間で通信障害が発生する確率が低いかは、いかに努力をしてコストをかけたとしても、各受験者は、事前に予測することは不可能である（CBT 試験サーバーとの間のインターネット接続経路は、インターネット上の BGP と呼ばれる経路自動形成システムによって決定されるが、これは複雑系システムであり、試験当日の経路は、事前に予測することが不可能であるため

である。) 。不可能なことを、受験者の責任として強いることは、不合理である。在宅型 CBT 試験システムの導入により、受験者に大きな不利益や不安を与えることになるためある。

結論として、在宅型 CBT 試験システムにおいては、試験中に受験者の PC と試験サーバーとの間のインターネット通信が絶対切れないことが確実な回線を自ら用意することを受験者に求めることはできない、ということになる。

## (2) そうすると、CBT では試験中に通信が切れることを許容する必要があるが、そのことにより、逆に公平・公正性が犠牲になってしまう

前記 (1) により、在宅型 CBT 試験では、インターネットにまつわる上記の特性上、試験中に通信が切れてしまうことを、一応は許容しなければならないことになる。

これは、技術的には一見簡単に見える。試験再開機能、すなわち、仮に途中で通信が切れても、切れたところから再開できるようにする機能を実現すればよい。在宅型 CBT 試験システムの中には、そのような機能が実装されているものが多い。

ところが、この通信エラー時の試験中断・再開機能により、公平・公正の問題や、不正行為を助長する問題が生じることになる。

まず、通信エラー時の試験中断・再開機能によって生じる、公平・公正の問題に対するリスクについて考える。

在宅型 CBT 試験システムにおいては、在宅型 CBT 試験システムのサーバーと受講者のコンピュータとの間の通信エラーが発生すると、自動的に試験を中断し、画面を消した上で、再度ログインすると試験が続行できる仕組みが実装されている。

ところが、この再開までに要する時間分だけ、試験の制限時間が延長されるとしたら、通信エラーが発生した受験者のほうが、エラーが発生せずスムーズに受験した受験者よりも、難問を考えることができる時間が追加で与えられるので、かなり有利な結果となってしまう。

一方で、仮に再開までに要する時間分の試験の制限時間の延長はしないというこ

とにするならば、通信エラーが回復するまで時間が長ければ、自己の責任によらず発生した通信エラーに遭遇した受験者は、自らの責任によらずに、試験時間を大きくロスすることになり、かなり不利な結果となってしまふ。

さらに、仮に通信エラーが発生したら直ちに画面を消すという処理があっても、通信エラーというものの定義は、受験者のコンピュータと在宅型 CBT 試験システムのサーバーとの間の通信が失敗したということの意味するので、通信エラーを検出するためには、タイムアウトの発生を検出する必要があることになる。TCP/IP というインターネット上のパケット通信の仕組みの限界として、実際の障害が発生してから、通信エラーが検出されるまでは、タイムアウト時間だけの時間 (ソフトウェアの設定にもよるが、一般的に 10 秒程度 ~ 数 10 秒程度) かかってしまふ。その後、エラーが画面に表示され、クライアント PC 上でのシステムは終了するが、この場合、余分に画面に表示されていた時間は何秒間であったのか、在宅型 CBT 試験システムのサーバーはその余分な秒数を正確に知る手段がない。これにより、通信エラー発生時から画面が消去されるまでの秒数だけ、受験者は得をすることになってしまふ。

さらには、通信エラーが発生してから、再度通信が復旧し、受講者側のパソコンで受験システムを再立ち上げするまでの間は、在宅型 CBT 試験システムの売りである監視カメラによる不正行為の監視もできないので、受験者は、任意の方法で不正な調べ物をする事ができてしまふ。

このように、試験中に通信が切れることを許容すると、公平・公正性が犠牲になってしまうのである。

### **(3) CBT の試験中の通信エラーを意図的に発生させると不正行為が容易に可能となる**

さらに、通信エラーというものは、本来正常になされるべき 2 点間の通信 (CBT システムの場合は、在宅受験者の PC と、在宅型 CBT 試験システムのサーバー) とがタイムアウトすることによって発生するが、通信エラーは、受験者が自ら意図的に容易に引き起こすことが可能である。(2) で述べたように、通信エラーが発生

したほうが自己に有利な結果を引き起こすことができるならば、有利な結果を得たい不正受験者の中には、自己と CBT システムサーバーとの間の通信を意図的に引き起こす者も多く発生すると思われる。

ここで、通信エラーに関わる本質的問題がわれわれの前途の道に大きく手を広げて姿を現わす。通信エラーが発生したとき、その通信エラーを、受験者が自ら意図的に引き起こしたものであるか、それとも、その責任によらず発生したのかを識別する確実かつ現実的な方法が、インターネットの仕組み上、存在しないのである。

インターネット上では、通信はパケットと呼ばれる最小単位に分割して送付される。通信エラーとは、そのパケットが途中経路上のいずれかの地点（前述 (1) で詳しく述べたような、隣接する数珠つなぎの領主ネットワーク間のいずれかの領土上）で消失してしまった場合に発生する。この場合、なぜそのパケットが消失してしまったのかは、いくつかの例外的場合を除いて、通常は、理由の把握がシステムの的に不可能である。このことを知っている不正受験者は、自らのコンピュータと、在宅型 CBT 試験システムのサーバーコンピュータとの間で、通信パケットを消失させることにより、かなり自然な形で、通信エラーが発生したことを両端のコンピュータ・プログラムに誤認させることができる。具体的な最も簡単な方法としては、通信経路上に、パケットフィルタ等を挿入すればよい。試験実施主体や在宅型 CBT 試験システムを運用する試験代行業者は、仮に意図的な通信妨害を受験者自ら行なっていたとしても、それを検出・証明する手段が存在しない。

そして、もちろん、受験者は、自らが不利になった場合だけ、通信エラーを意図的に引き起こすことができる。そういった目的で通信エラーを引き起こすことができることも、不正受験者にとって利益となる。しかし、より大きな脅威は、不正受験者は、不正行為防止のための監視システム（監視カメラ等）を、通信エラーを引き起こして麻痺させることができるという点にある。

不正受験者は、わずかな通信の知識を有するだけで、通信エラーを用いて監視カメラの監視データを、ちょうどやむを得ない回線不具合によって時々映像が欠落してしまっただかのように見せかけることが可能になる。これにより、不正受験者は、AI や人間に基づく監視カメラによる遠隔での不正行為の検出を回避することが

できるのである。

その具体的な方法と検証結果については、本文書で詳しく後述する。

試験サーバーの側からみて、通信エラーが意図的であるかどうかを検出する方法がない以上は、これらの意図的な通信エラーに基づく利益を得ようとする不正受験者を排除するためには、通信エラーが発生したときは必ずその受験者を失格としなければならない。

しかし、それは前述のとおり受験者に不可能を強いることになり、公平・公正ではない。

すなわち、この問題は、公平・公正を担保し、かつ、不正行為を防止することを、品質保証の実現手段がない安価なインターネット上で実現しようとするものの両立の原理的な困難さによって生じている。

この問題を緩和するためのさまざまな進歩的な手法を、これから次々と試行錯誤と技術的創造性の発揮により発明していくことが、試験実施主体たちおよび在宅型 CBT 試験システム提供業者たちに対して、社会的に期待されている責務である。

#### (4) CBT 試験システムサーバーの保存データにおけるビットエラー

紙の試験の答案用紙やマークシート用紙を思い出してみよう。これらは、鉛筆またはボールペンで記入がなされる。たとえば、選択肢 1 ~ 4 をいずれか選択する問題であれば、「1」、「2」、「3」、「4」などという文字が記入される。このような答案用紙上の 1 文字は、紙の上に、相応の大きさを物理的に筆記される（目に見えないほど小さい文字を書くと、何も書かれていないとみなされ、得点にならず不利であるため、受験者たちは、皆、相応の大きさの文字を書くのである。）。

この際、鉛筆であれば答案用紙の表面に大量の黒鉛の粒子が力強く付着する。ボールペンであればインクが紙面に強く染みこむ。マークシートを塗りつぶす方式でも、同様に、四角形の枠の内側の相応の面積を塗りつぶす。いずれの方式でも、たとえば、一度「2」と書いた文字が、後から勝手に「3」に変化してしまうことは、物理的にあり得ない。

もし、受験者は、自らが「2」と書いたはずで、正答も「2」であるのに、その間

題が不正解にされていたことが原因で試験に不合格になったら、試験実施主体に対して、答案用紙またはマークシートに自身は確かに「2」と書いたはずだと申立てればよい。試験実施主体は、そのような場合に備えて、1年間くらいは、答案用紙やマークシート用紙をどこかの倉庫に保管しているものであるから、それを申立者と一緒になって、目視して確認すればよい（一緒になって確認する際には、申立者がその用紙を触れて悪さをしないように物理的によく警戒する必要があることは、もちろんである。）。大抵は、申立者の記憶違いであるが、稀に読み取りミス、採点ミスも有りうるので、受験者の申立てが客観的に正しい場合もあるかも知れない。いずれであるかを客観的に判定する証拠として、紙に付着した鉛筆の大量の黒鉛粒子やボールペンインクの染み込みは、動かぬ証拠として利用できる。

このことの本質は、ある情報を記録する記録媒体におけるビット数の問題として考えることができる。筆記された紙というものは、試験においては、答案データの記憶媒体として機能しているが、「1」、「2」、「3」、「4」などという情報を最小ビットで記録するのではなく、その情報を、本来必要な情報量と比較して、極めて冗長なビット数で保持している。黒鉛の粒子の一部が欠落したり、一部の黒炭粒子が少しくらい紙の上を風化により移動したりしたとしても、紙媒体は、全く揺るがない程度の冗長性を、物理的に保証しているのである。紙媒体は、なかなか優秀な冗長化されたストレージであるといえる。

これと比較して、CBT 試験システム（在宅型であっても、集合型であっても）において受験者からの送付を受けた答案データは、どのように保存されているのだろうか。答案データ（特にマークシートに代わるチェックボックス式またはラジオボタン式の選択肢に基づく「1」、「2」、「3」、「4」等の選択結果のデータ）は、すべて、在宅型 CBT 試験システムのサーバー側のストレージシステムに保存される。このストレージへの保存形式（フォーマット）は様々であるが、最終的には、受験者から送付を受けた「1」、「2」、「3」、「4」等の選択結果データは、それを示す数ビット（せいぜい 1 バイト。すなわちコンピュータ上の 1 文字）の整数データまたは文字データとして、ファイルやデータベース上に保存されることになる。この保存されるデータが、さらにこの世界の物理空間上のいずれの部分に保存されるか

を突き詰めて考えてみよう。これは、ハードディスクや SSD 等のストレージ装置の上の特定の磁気データまたは静電データとして保存されている。ここで、ハードディスク上に一度保存されたデータは、まず変質することはないと誤解している人は多い。多くの IT 人材も、若干高価なエンタープライズ向けのデータセンタ用ハードディスクに保存したデータであれば、絶対に安心であると考えている。これらのハードディスクには、「Enterprise」等と誇らしげな文字が入っていて、購入者は、大いに安心できる気分になるものである。ところが、そのような安心は、少しハードディスク製品の仕様書を確認してみれば、直ちに、糠喜びに変わるであろう。仕様書を確認すれば分かるように、実際には、高品質のエンタープライズ向けハードディスクでも、約 100TBytes に 1 バイト程度のデータ化けが発生し得る。例えば、東芝の 2023 年の時点で現役のエンタープライズ HDD 製品のスペックシートにも、125TBytes あたり 1 ビット程度の回復不能なデータ化けが存在し得るという旨の記載がある<sup>①</sup>。このデータ化けは、極めて恐ろしい。データの管理者は、データが化けていることすら気付かなくなるのである。これは、HDD よりも発生頻度は低いが、SSD でも発生する。なお、ビット化けは、メモリやネットワーク上でも発生することがある。

本当に HDD のビット化けは発生するのだろうか。実際に試してみなければならぬ。そこで、評価者は、最近、実際に 16TB の HDD を 25 台用意し、これに合計 400TB 分もの大量の疑似乱数データを書き込んで、後に読み出しを行ない、ハッシュと呼ばれる計算式を用いて、書き込み時と読み出し時のデータが変わっていないか検証してみた。すると、25 台のうち 1 台について、確かに、少なくとも 1 ビットのデータ化けが、実際に発生したのである。このことから、確かに HDD におけるデータ化けは、スペック値よりももう少し低い確率であるものの、ある確率で本当に発生し得ることが分かった。

これは、次のことを意味する。受験者が苦勞して試験問題を解いて、「2」という選択肢を書いた答案を CBT 試験システム (在宅型であっても、集合型であっても)

---

<sup>①</sup> [https://storage.toshiba.com/docs/enterprise-hdd-documents/ehdd\\_mg08\\_product-manual\\_rev-3.pdf](https://storage.toshiba.com/docs/enterprise-hdd-documents/ehdd_mg08_product-manual_rev-3.pdf)

のサーバーに送付したとする。これを数値の「2」としてサーバーが記録するとする。「2」は、2進数であれば、1バイト表記で「00000010」である。このデータの末尾1ビットが化けたとする。すると、2進数で「00000011」となり、「3」を選択したものと記録される。在宅型 CBT 試験システムは、その結果に基づいて採点を行なう。採点結果で、本来正解になっているはずの問題が不正解にされ、その結果、試験が不合格となった受験者は、おかしいと思い、試験実施主体に異議を申し出るであろう。ところが、CBT 試験システムサーバーに受験者から送付された答案データは、この時点ですでに「2」から化けていて、誤って「3」と記録されている。受験者は「2」を選択したはずだと訴えるであろうが、何度確認しても、ハードディスクに記録されている答案データが「3」である以上、そのような異議申し出は斥けられる。これにより、何ら責任がない受験者が不公平な不利益を被ることになる。

ただし、125TB あたり 1 ビット程度が化ける可能性があるというのは、ある1人の受験者の視点としては、不運にも自らの答案がそのビット化けの対象となってしまう可能性は、確率的には、それなりに低い。単純計算で、一生に 1,000 回の試験を受け、それらが、1つの試験について 1,000 問くらいのマークシート方式で、選択肢が「1 ~ 8」(3 ビット) と仮定しても、自らの答案データがそのビット化けの直撃を受けるのは、一生涯で 3.3 億分の 1 くらいの確率である。しかし、実際にはよくビット化けを起こすストレージとそうでないストレージに偏りがあることが考えられる。CBT 試験システムのサーバーとして動的に割当てられた自前サーバーまたはクラウド事業者のストレージを構成する HDD または SSD の当該ファイルが保存される特定の物理的なセクタ領域の付近が、運悪くビット化けを多発させる場所であった場合は、より高い確率で、受験者の答案データのビットが化けることになる。

なお、ストレージ上のデータを管理するファイルシステムのチェックを行ったとしても、この問題を修正することはできない。たとえば、データは現実的には PC サーバー上の NTFS や ext4 といったファイルシステムで記録されているとする。NTFS や ext4 のチェックプログラムを用いたとしても、これらのチェック

プログラムは、ファイルシステムの構造をチェックすることができるだけで、保存されているデータをチェックすることはできない。RAID を用いて冗長性を高め、物理的な HDD 上のデータ化けの問題は解決しない場合が多い。RAID は、いずれかの HDD が故障した場合にパリティまたはミラービットを用いてデータを復旧可能であるが、HDD の正常稼働中には、読み出しは、高速化のために、ストライプと呼ばれる塊を最小読み出し量で読み出すためである。この際には、1 台の HDD におけるビット化けが検出されない (検出するためには、複数の HDD からのデータを読み出して整合性を比較しなければならない)。よって、たとえば RAID による冗長化を用いていたとしても、HDD 上に実際に記録されている 1 ビットが化けてしまったとすると、化けているデータがそのまま読み出されてしまう可能性がある。

この問題は、従来の紙を用いた試験では、長年、最重要の情報である答案用紙に記入された 1 つの問題の選択肢という、極めて貴重な、容易に化けることが許されない 1 つの情報量を保存するのに、大量の黒鉛の粒子やボールペンのインクを紙に付着させて、ビット化けを防止してきたという配慮の存在にもかかわらず、CBT 型試験を導入した時に、従来と同等程度の配慮を怠っていることによって発生する。

受験者としては、これまでの紙方式であれば、突然のビット化けが発生する可能性は皆無なレベルが物理的に保証され、安心して試験を受けることができていたのである。ところが、CBT 方式になり、突然に、冗長性が失われた形で、最小のビット数だけでストレージ上で自己の大切な人生がかかった答案データが保存されるようになり、そして、その保存されるデータは受験者自らの手中を離れて試験代行業者の運営する CBT サーバーのストレージ (または、さらにそこから外部委託されるパブリッククラウド事業者のストレージ) に保存される。

これらの物理的ストレージについて、一体どの程度の品質の HDD が採用されており、どのような形でビット化けを防いでいるのか、情報は全く不透明であり、すべて、ブラックボックスの内側に隠されている。そこで、受験者としては、上記のようなエンタープライズ HDD におけるビット化けエラー率を元に、自らの答案

データがビット化けの被害を受ける可能性を計算し、これに加えて、HDD ごとの偏り等の存在も考慮して、ある程度不運な場合の自己が被害を受ける確率を想定することになる。これらの知識に基づき、そのような十分な確率計算を行なった受験者は、その結果、相当な不安を感じるであろう。自らの人生を賭けて今まさに受験しようとするこの目前の CBT 試験の自らの答案データが、もしかすると、試験実施代行業者のサーバー上では、冗長化されていない最小ビット量でのみ保存され、それが不運にもビット化けするも知れないという確率は、紙の従来試験の場合と比較して、比べものにならないほど高い確率であるということになり、大きな不安となり得る。

この受験者の不安は、確率的に考えても、過小評価できず、正当で合理的なものであるといえる。もともと、試験実施主体としては、受験者の利益のために、従来型の紙試験を、CBT 試験に変更するのであるという建前を謳っている。そうである以上、受験者が新しい方式において新たに生じる正当で合理的な不安を解消する方法が容易に採り得るのであれば、その容易な方法により、ビット化けに対する冗長化対策を、確実に講じるべきである。

そこで、答案データ保存時におけるビット化けを防止するために、比較的簡単かつ確実に実施できる手法としては、以下のようなものがある。

#### (1) 複数データへの書き出し方式

複数のデータ（できれば複数の異なる形式のデータ）として書き出す方法。データベース上のデータ等の正規の処理を行なう上でのデータは 1 つで良いが、それとは全く別のログファイルのようなデータファイルとして、デバッグ的なデータとして、できれば複数のログファイルに、受験者から受信したデータを次々に追記していき、そのログファイル群は、受験者からの異議申立てに備えて、一定期間保存する。

#### (2) 一度書き込んだデータに基づく受験者への提示方式

試験の最後に、サーバーに保存された答案データを再度読み出して、そのデータを受験者に提示し、受験者に確認させ、それらのサーバー

上の答案データが、意図したものになっていることに明示的に同意してもらった上で、確定ボタンをクリックさせる。ただ、この方法でも、結局その後にサーバーに保存されたデータがビット化けする可能性もあるので、結局、前記のログファイルへの書き出しも併用しなければならない。

### (3) 受験者の側の画面のスクリーンショットも保存する方式

紙の答案用紙やマークシートでは、構造上、1文字の答案筆記が無数の数の黒鉛粒子またはボールペンの付着として記録されていた。CBT 試験において、このビット冗長に相当するものとしては、受験者の回答画面のチェックボックスまたはラジオボタン等の画面上のコントロールボタンに黒いチェック点等が描画されている様子であろう。そこで、受験者側の画面のキャプチャ等を行ない、回答時における物理的な画面の様子を撮影して、それを画像データとして CBT サーバ側にも伝送してこれを保存しておけば、万一受験者から懐疑による申立が生じたときに、その画像データを答案用紙原本と同じ程度の価値がある最終的白黒判定証拠として利用可能である。

## 第2章 各論 I —在宅型 CBT 試験システムの不正防止機能の検証

ここまでは、CBT 試験システムにおいて試験を実施する場合における、不正行為や機密性・完全性・可用性等を含めたさまざまな試験に対するリスクとその緩和方法について分析をした。

ここからは、実際に CBT 試験システムの 1 つである、ある民間企業のシステム製品 (在宅型 CBT 試験システムであり、クラウド型で利用できるものである) に含まれている各種の不正行為防止機能について、その動作を実際に検証し、これらの機能が受験者による不正行為をどの程度効果的に防止することができるかどうかを、確認していく。そして、これらの不正行為防止機能の現段階における本システムの限界を分析するとともに、今後どのような技術的進歩が、これらの限界をどのように解決していくべきであろうかという点について、試験運営主体の立場および CBT システムのソフトウェア開発者の視点を想定して解説をする。

以下でみる不正対策機能に対する各種の検証結果は、上記製品を対象としたものであるが、他のほとんどの在宅型 CBT 試験システムを検証するときにも、ほぼ同じ形で検証をすればよく、汎用的に役立つ情報であると思われる。

### 第1節 なぜ不正対策が重要か

本システムの不正防止機能の検証を行なう前に、なぜ、試験においては、不正防止が重要であるかを深く考えてみよう。

その直接の理由は、試験システムにおける不正の発生が、試験実施主体に対して致命的な経営上の打撃を与えるおそれがあるためである。試験実施主体が不正行為を防止することができない場合、試験実施主体に対して、直接的に、次の 4 つの損害が生じる。そして、この損害は、間接的には受験者たちおよび社会全体に生じるのである。

## (1) 試験による高能力保有者の選抜が困難となり、試験目的の実現が不能となることを防止するため

不正行為が容認・放置されれば、勉強・研鑽を行なった結果として高レベル能力を獲得した善良受験者と、勉強・研鑽を行なっておらず高いレベルの能力獲得を経していない不正粉飾受験者とを区別することができなくなる。

そもそも、試験というものは、人材間の能力を絶対的あるいは相対的に区別または比較することで、一定の水準を超える者や、特に能力の高い者を抽出するために、実施されるものである。不正行為が容認・放置されている場合、その結果は信頼することができなくなり、試験を実施する意味が損なわれてしまう。

たとえば、試験実施主体が会社や官庁等の組織であり、入社試験等を実施するとする。入社試験で、高い業務能力を有する人材を選別しようとして試験を実施したところ、不正が容易であれば、実際には、高い業務能力ではなく、高い不正行為能力を有する人材ばかりが選抜されて入社してくることになる。その組織は、その後、大きな損害を受け、それらの人材による組織内不正行為が多発し、やがて、存続の危機に瀕するであろう。

したがって、これを防止する必要がある。

## (2) 不正行為が長年一定割合で発生することによる合格者集団の社会的価値の低下を防止するため

加えて、試験の不正行為が容易である状態で一定年数が経過すると、当該試験の合格者等の集団の中には、不正行為を行なった者が、相当な確率で入り交じることとなる。その結果、合格者集団の能力（当該試験によって測られたはずの能力）の実際の平均値が、名目上の能力平均値よりもかなり低下してしまうことになる。そうすると、ある試験の合格者集団に実施されることが期待されていた社会的価値のある活動の質が低下する。

たとえば、資格試験で、一定の対象領域の能力水準を有する者だけに資格を授与しようとしたところ、対象領域の能力水準が低く、不正行為能力が高い人材もそれに混じってしまう。すると、有資格者たちの平均能力水準は低下してしまい、試験

が正しく実施されていた場合は比較して、社会的損失が発生する。

したがって、これを防止する必要がある。

### (3) 予見可能性の高い不正行為手法の場合の主催者に対する強い社会的非難を避けるため

ある試験について、不正行為が実際に放置・容認されてしまったことが 1 例でも発覚したならば、それが試験にとって致命的となる場合もあり得る。

その不正行為が、試験実施主体による対策が可能であったにもかかわらず、不正行為が 1 件でも発生したとする。その原因が、試験実施コストを無理に下げることにより熱中する余り（例えば、安易な在宅型 CBT 試験の導入等）、本来対策すべき点について手を抜いたとか、試験実施方法について不正の余地があることを知っているにもかかわらず対策をしなかったというような、意図的な不作為があったとする。

この場合、合理的・定量的な評価とは別に、社会現象として、試験実施主体が強い非難にさらされてしまう現象が存在する。特にそれが公的な試験（国家資格試験、大学入学試験等）であれば、なおさらである。

したがって、これを防止する必要がある。

特に、公的な試験実施主体は、私企業と比較して、常に社会からの非難の声によって自らの命運が左右されるリスクが高いため、特に十分に注意して防止する必要がある。

### (4) 善良な努力によって試験を受験した者が損害を被ることを避けるため

最後に、試験において、不正行為を行なった者が 1 人でも存在するならば、善良な努力によって試験を受験した者は、ちょうど不正行為があった分量だけ、損害を被ることになる。

不正行為が存在しただけで、善良な受験者は、自らの試験結果に対する社会的価値がそれだけ低下したことになり、損失が発生する。特に、上位何名を選抜すると

というような相対評価の場合は、不正行為実施者と全く同じ人数の善良な受験者が、選抜から漏れてしまい、個人的な損失が発生する。

したがって、これを防止する必要がある。

上記をまとめると、(1) は試験実施主体自らが被る損害 (自業自得)、(2) は社会的責任、(3) は政治的責任、(4) は善良な受験者に対する責任 (不正に試験を受験する者を見抜くべき義務を怠った責任) ということになる。そして、不正行為が生じたならば、この (1) ~ (4) の問題が、その試験の性質に応じて多少大小は異なるものの、一度に 4 つとも発生してしまう可能性がある。

そこで、試験実施主体が在宅型 CBT 試験を使用する場合、自らが実施する試験における上記のような損害の発生を防止するためには、在宅型 CBT 試験における不正対策が、経営上の課題として、極めて重要となる。

いかなるシステムも、不正行為に対して 100% の耐性を実現することは、不可能である。必要な不正耐性の度合いは、程度問題であるといえる。そして、一般的な試験実施主体が在宅型 CBT 試験システムに要求するのは、通常の水準の不正耐性であると想定される。こういった不正な行為が、従来の集合型紙試験よりも、低コストで、容易に、かつ発覚する可能性が低い状況で、簡単に実現できるかどうか重要となる。

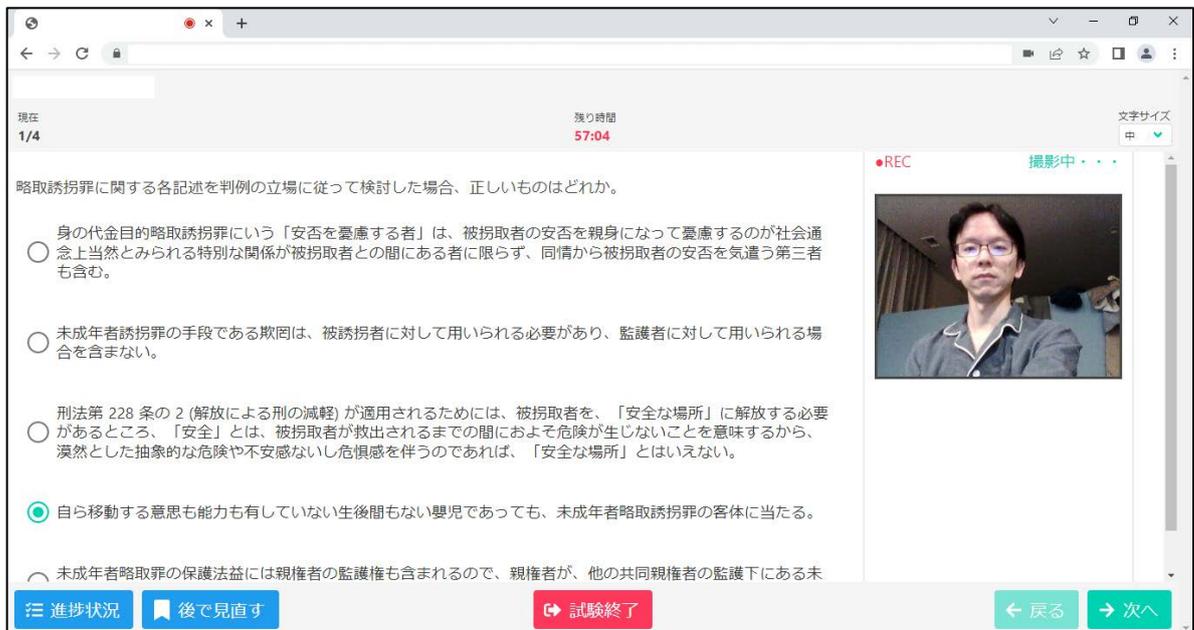
## 第 2 節 本システムの不正行為検出機能の仕組みの評価

### 1 概要

本システムに搭載されている不正行為防止機能は、受験者の様子をカメラで撮影し、撮影された映像データをインターネット経由でセンターサーバーに送付し、センターサーバーでその映像データを AI 分析した上で、不正行為である可能性が高い部分があれば、これをマーキングして試験実施主体に対して知らせることにより、試験実施主体の判断を仰ぐ仕組みを備えることにより、不正行為を防止しようとしている。

本システムは、各受験者の受験ごとに、以下の流れによって、不正行為の有無を判定しようとする。

- (1) 在宅受験者は、自宅で、自分自身が所有・支配・管理するパソコンで試験を受験する。試験の受験は、Web ブラウザによって行なう。本システムの試験の基本的機能は、試験問題を画面上部に表示し、選択肢または自由入力欄を画面下部に表示し、試験者によるキーボードまたはマウスを用いた選択肢の選択または自由入力結果のテキストデータを、試験サーバーに送付することによって行なわれる。



本 CBT システムの受験画面（これは、択一型の画面のサンプルである）

- (2) (1) で述べた試験の基本的機能に付随して、カメラを用いた受験様子の撮影が実施される。受験者のパソコンに USB 等で取り付けられている（ノートパソコンの場合は、液晶モニタ付近に内蔵され、内部的に USB 接続されている場合もある。）受験者側が所有する Web カメラを用いて、受験者の受験中の容姿およびその周囲の様子を視覚的に撮影し、これが、プログラムにより、常時 CBT システムのサーバーに送付される。本システ

ムの受験者側の PC で動作する部分は、JavaScript と呼ばれるプログラム言語で実装されている。JavaScript のプログラムが、Web ブラウザに内蔵されているカメラ撮影機能および動画圧縮機能 (H.264 と呼ばれる、最近オンラインテレビ会議等のソフトウェアでも活用されている高性能な映像圧縮技術である) を呼び出し、常時映像を撮影・圧縮し続けるとともに、10 秒ごとに、映像圧縮結果を、インターネット経由で試験サーバーに送付する。

- (3) 試験サーバー側では、10 秒ごとに受験者の映像が次々に届く。これは、サーバーですぐには AI 処理せず、一度、単純にサーバー側でデータとして保存する。たとえば、60 分の試験を受験する人が 1 名いれば、60 分間分の映像データがサーバーに溜まっていく。100 人もいれば合計 6,000 分間分の映像データが溜まっていくことになる。
- (4) 本システムは、(3) で溜まったデータを、順次 AI で処理し、不正行為の可能性が高い被疑点を発見する。多数の受験者が一度に試験を受験すると、(3) のデータが一時に大量に蓄積される。これを AI が遅延処理で全部確認するので、多くの受験者がいる場合は、すべての映像データの分析が完了するには結構時間がかかる。大量の受験者がいる場合は、延々と何日間も処理時間がかかるかも知れない。ただ、AI 処理は多数のコンピュータで分散することができる。そこで、本システムの運営会社は、大量の処理を一時的に必要とする場合は、並列 AI 処理をするサーバーコンピュータの台数を一時的に増やして、全部の AI 処理が完了するまでの時間を高速化することができる。このような処理能力の引き上げのために、本システムの運営会社は、クラウドコンピューティング基盤を活用しているものと推測できる。
- (5) (4) の結果、各受験者の映像データについて、被疑点の一覧が生成される。

たとえば、受験時間が 60 分間の映像データがあるとする。その中で、その受験者が、合計 3 回くらい、あくびをしたり、ついうっかりと、視線を大きく左右に動かしたりしてしまったとする。それらの瞬間は、せいぜい数秒程度、長くて 10 秒程度である。この場合、60 分間の映像の中で、これらの被疑点 3 回分 (1 回あたり 10 秒程度) が、目立つようにマークされる。その結果は、受験者ごとに、試験実施主体がログインできる試験結果管理画面上に、わかりやすく表示される。

- (6) 試験実施主体は、試験結果管理画面上にログインして、(5) の被疑点の一覧を確認できる。被疑点は、あくまでも、AI が人間の目線などをもとに判断して被疑点であるとマークしたに過ぎない。これが試験上の不正行為であるかどうかの判断は、試験実施主体のみが有する裁量権である。したがって、試験実施主体は、事後的に、各被疑点を実際に本画面から目視で確認し、不正行為があったとみなすかどうかを決定することになる。どのような場合に不正行為があったとみなすべきかは、試験実施主体それぞれが自ら基準を定めるであろうから、その一定の基準に基づいて、被疑点を次々に確認していけば良い。一般的には、試験中に数回程度目線が動いたとか、よそ見をしたとかいうような被疑点があっても、受験者の緊張や精神の集中が一時的に切れて休養をするためにそのような動きがあることは自然なことであるから、多くの試験実施主体のポリシーとしては、その程度の頻度や回数の被疑点があっても、これらを不合格であるとみなすことはしないであろう。一方で、1 人の受験者が、その試験中の大半の時間でこういった被疑点を見せる様子が多数記録されており、それが客観的にも明らかに不正行為をしている証拠であると認定され得る程度に、その不正の可能性の水準が極めて高い場合は、試験実施主体としては、これを不正行為であるとみなすことを決心し、失格とすればよい。後は受験者がその判定に異議を申し出て争ってくることがあれば、試験実施主体は、被疑点の一覧の映像を証拠として保存しておき、万一争いになった場合は、公

平・中立・客観的な第三者の判断者（例えば、裁判所）による判断を仰ぐことになるであろう。

- (7) 試験時間の最初から最後まで録画データを AI が分析した結果、1 つでも被疑点が存在する受験者については、(6) の仕組みにより、本システムは、試験実施主体に対して、すべての被疑点を手動検査すべき旨を表示する。これらの手動検査がなされるまでは、その受験結果は「保留」状態となっている。検査を行なう試験実施主体は、検査結果として「正常受験」とか「不正行為」というように、判定結果を本システムに入力していくことになっている。
- (8) 他方で、試験時間の最初から最後まで録画データを AI が分析した結果、1箇所も被疑点が検出されなかった場合は、その受験者の結果は、最初から、自動的に「正常受験」として設定される。
- (9) このように、本システムの AI を用いた不正行為自働検出機能は、不審な目線や身体の動きに基づいて、不正の可能性が高い部位を特にマーキングし、そのマーキング一覧を試験実施主体に対して提示することにより、試験実施主体が、すべての受験者のすべての映像を最初から最後まで神経を集中させて確認する必要をなくし、真に確認すべき部分のみを確認することで足りるようにすることにより、映像確認と不正発見のために必要な時間、すなわち人的コストを、著しく節約することに貢献する。

## 2 カメラ映像から AI で検出可能な不正被疑行為

### (1) 替え玉受験および不正援助者の出現の検出

本システムでは、受験者は、受験開始前に、カメラを用いて 1 枚の顔写真を撮影する。この最初の 1 枚の顔写真は、本システムの受験中における替え玉受験検

出のための基準写真となる。

試験中には、常に受験者の顔が撮影されるが、その受験中の顔と、最初に撮影した基準写真の顔とが同一人物であるかどうか、受験終了後に、AI によって判定される。

異なる人物の顔が、録画データ中に 1 箇所でも検出されると、替え玉の可能性または第三者（協力者）による受験者への不正援助の可能性であるとして、被疑点としてその瞬間の映像部分がマークされる。

## (2) 不自然な目線の移動の検出

本システムでは、受験者の受験中の目線が AI によって検出される。わき見が発生すると、その瞬間の映像部分が、被疑点としてマークされる。

## (3) 受験者の身体の大規模な移動の検出

本システムでは、受験者の受験中の大きな移動（画面から大きくはみ出た、画面外に一時退席した等）も AI によって検出され、その瞬間の映像部分が、被疑点としてマークされる。

## (4) 様々な物体の出現の検出

本システムでは、受験者の受験中に、最初はカメラの視線内になかったような物体（電話機、参考書等）が新たに出現する等、受験者の周辺環境に視覚的に大きな変化があった場合も、AI によってこれが検出され、その瞬間の映像部分が、被疑点としてマークされる。

## 3 検出された不正被疑点の確度の数値化

AI が、受験者の受験中の映像中から、上記で述べたような被疑点をマークした場合、そのマークされた被疑点ごとに、その水準（怪しさ）を示す「不正確度」および「別人確度」という数値（0 ～ 100）が表示される。

この 2 つの種類の数値は、実は AI が処理したすべての対象映像の全部の部分について計算されている。これらの数値のいずれかが、一定の閾値を超えた部分が、試験実施主体がログイン可能な管理画面において被疑点として出現し、手動で人間が判定することを促される仕組みになっている。

## (1) 不正被疑行為検出時の画面例

実際に、本システムを用いて受験を行ない、カメラの面前で不正行為を行なってみた際の、試験実施主体がログイン可能な管理画面における被疑点検出結果を、サンプルとして示す。

項目	ピックアップ動画
検知人数	1
AI判定	
不正確度	83%
別人確度	100%

試験中に参考書閲読や電話をかけて試験を受験するという不正行為の実験を行なった結果、きちんと、不正被疑行為として多数のモーションが自動検出された。これは素晴らしい。

この例では、受験者は、過去問集を左手に、電話機を右手に持って、試験を受験している。このような試験受験を始終行なってみたところ、その結果の映像は、本システムの AI によって検査され、「不正確度」の結果がおおむね 70% ~ 80% 程度の水準で推移した。

試験実施主体は、これらの「不正確度」が高い点を集中的に再生して、試験実施主体としての不正行為の有無の決定を下し、「失格」等として、本システムに判定結果を投入する。なお、その判定についてコメント文字列を入力することも可能である。

## (2) 本システムの AI 支援型カメラ映像不正行為検出システムの概念は素晴らしいものである

### 紙試験 → 集合型 CBT 試験の技術進化

試験実施においては、前述のとおり、不正行為防止は、何よりも重要である。そこで、従来から、試験実施主体たちは、物理会場を開設し、複数人数による巡視を行なう等の手法により、不正防止を膨大なコストをかけて実施していた。大学入試や各種資格試験の受験会場を思い出してみるとよい。これには、かなりの人件費と設備費がかかっている。受験者の側も、自らが不正をせず合格できる受験者であることを証明するためには、自ら会場へ出頭する必要があった。そして、会場では、伝統的には紙による試験が実施されてきた。次に、会場集合型 CBT 試験が出現した。

しかし、会場集合型 CBT 試験は、単に紙がパソコンになっただけであり、用意すべき会場の広さや不正監視の人的コストはさほど変わらないか、むしろ、パソコンのセットアップの作業分だけ増加する場合もあり得る。よって、会場集合型 CBT 試験は、コスト削減効果が薄かった。

### 集合型 CBT 試験 → 在宅型 CBT 試験（人間監視型）の技術進化

そこで、インターネットの発達により、その後、在宅型 CBT 試験方式というのが発明された。在宅型 CBT 試験では、受験者は自宅の自分のパソコンで受講ができるので、前記のような集合型紙試験または集合型 CBT 試験にまつわるコストの大半が削減できる。これは、まさに画期的な発明であった。

ところが、在宅型 CBT 試験方式では、受験者が手元資料（過去問集）や Web ブラウザ等で試験中に調べ物をしたり、試験中に友人や家族に相談をしたり、替え

玉受験を利用したりすることが、容易に懸念された。

これを防止するため、在宅型 CBT の場合、在宅者の PC に付いている Web カメラやマイクを用いて、受験者の周囲の映像の様子を、主催者側（主催者本人か、主催者から委託を受けた試験実施代行業者）が常時監視するという手法も実用化された（本システムと同系列の別製品は、そのような人間による常時監視サービスを提供している。）。

ところが、この手法は、人間が人間を監視する訳であるから、前記の会場集合型の紙試験または集合型 CBT 試験と比較して、本質的に、監視コスト構造（監視に要する監視作業員の拘束時間）はほとんど変わらず、コスト削減効果に乏しい。

もちろん、監視作業員は、リモートから監視できるので、作業員自らも在宅ワークが可能である。また、録画データを監視することでもよいので、時間に拘束されない働き方ができる。しかし、この 2 点は、神経を集中して対象受験者の映像を監視するために要する時間に、それほど影響を与えない。よって、1 受験者あたりの監視コストにかかる人件費は、同一の神経の集中度合いを前提とすると、一定であるといえる。

もし、1 受験者あたりの監視コストにかかる人件費を無理に削減すると（すなわち、1 人が同時に監視する受験者の数を増やしたり、早送りをしたりする等、神経の集中度合いを緩和すると）、不正行為の見落としのリスクが増加する。不正行為の見落とし頻度がある一定許容量を超えて品質低下した場合には、試験実施主体（および試験実施代行業者）は、大きな損害リスクと前述したような社会的非難を受けるリスクにさらされるので、おいそれと監視コストを削減することもできない。

これが、従来の在宅型 CBT 試験方式の限界であった。

前述のように、従来の在宅型 CBT 試験においては、PC に付いている Web カメラやマイクを用いた監視コストにかかる人件費と、不正行為の実行容易性とは、長年、固定的なトレードオフの関係にあった。不正行為の実行容易性を高いレベルで容認・放置することは、試験実施主体の視点からは、極めて大きなリスクとなるから、在宅型 CBT 試験を利用するとしても、監視のための人件費コストを削減す

ることはできなかつた訳である。そして、コスト削減効果が薄いのであれば、不確実で回線トラブルや受験者側 PC に起因する相性問題といった不具合が発生する可能性の在宅型 CBT 試験でなく、従来通りの集合型の紙試験または CBT 試験のほうがむしろ安全確実で良いのではないかと、という経営判断が生じ得る。

以上でみてきたような、従来の集合型の紙ベースの試験から、在宅型 CBT 試験におけるカメラ監視型試験まで、いずれの段階でも、試験実施主体（というよりも、むしろ試験実施代行業者）の経営上の悩みは、受験者数とコストが比例関係にあり、その比例関係を越えてスケールしないという点にあった。

試験実施代行業者としては、受験者数によって売上を得ることができるけれども、受験者数に応じて監視人件費を支出する必要がある、利益のスケラビリティには一定の限界があった。社会における試験の数は有限であるため、多数存在する試験実施代行業者は、常に値下げ競争にさらされることになるが、前記のスケラビリティの面で限界がある（すなわち、支出人件費が受注受験者数に応じてかかってしまう）ので、収益性の面で限界があるというのが、競争上、いずれの業者にも残された不可避のボトルネック・ポイントとなってしまうのである。

既存の技術的水準を前提とした市場競争が一定時間継続すると、当事者によって、競争の次元を変化させるための、新たな技術的進化が試みられる。

## 在宅型 CBT 試験（人間監視型）→ 在宅型 CBT 試験（AI 監視型）の技術進化

この在宅型 CBT 試験におけるカメラ監視人件費にまつわる固定的状況を打開するための革新的技術が、カメラ監視における AI の導入であった。

これは、在宅型 CBT 試験において、受験者のカメラ監視（前述のように、これは、受験者のノートパソコンの Web カメラで行なわれる）における不正行為の検出のうち大半の作業を、人間ではなく、AI が実施するというものである。

AI がある受験者の映像（たとえば 60 分の試験であれば 60 分間すべて）を分析し、受験者の目線の動きが怪しいとか横を向いている（情報の不正摂取）とか、電話をかけている、スマートフォンで調べ物をしている、または替え玉が登場した等の、映像上の特徴的な変化を検出したら、その点を、被疑点としてマークする。

AI はあくまで被疑点を抽出するのみであり、その被疑点を人間である試験実施主体がピンポイントで目視し、不正行為であるかどうかを判定する。

この AI 支援型の不正行為検出・判定手法の登場は、AI 登場以前の、前述のような、受験者の数に応じた膨大な監視人件費の問題を解決する、決定的に重要な技術革新といえる。これは、まさに注目すべき、素晴らしい技術である。

この AI 技術の効果は、少し計算してみれば、絶大であることが分かる。たとえば、60 分間の試験時間のうち、AI 支援型により不正行為の被疑点がだいたい 1 分間分のカメラ映像として検出されたら、その部分を確認する工数は、1 人あたりわずか 1 分で済む。ほとんどの受験者は善良な受験者なので、試験実施主体がそれを少し確認して、問題でないと判断すれば、1 人あたり平均 1 分くらいでチェックが完了することになる。

他方、不正な受験者は、情報を何度も不正摂取したり、電話をかけたり、スマートフォンで調べ物をしたり、同室の支援者に助力を求めたり、または替え玉が画面内に出現したりするであろう。すると、不正な受験者の録画データには、60 分間の映像のうち、たとえば 30 分間分も、AI によって被疑点として検出されたマークが付く。被疑点マークが付いた部分を、主催者が次々に確認していくと、これらの不正行為が実施されている確証に至る映像 (すなわち、不正行為の証拠) をいくつか発見できる。不正受験者を不合格としても抗弁を受けない程度の証拠が固まれば、試験実施主体の不正検知の仕事は完了である。

この手法による時間削減効果を算出してみよう。例えば、60 分間の受験時間で、1,000 名の受験者が存在するとしよう。そして、10 名の不正受験者が存在するとしよう。

- (a) まず、AI 導入前の従来の在宅型 CBT 試験において実施されていた手法について、監視コストを計算してみよう。監視者が神経を十分集中させてすべての映像を確認するとしたら、それにかかる人件費は、映像全部であるから、1,000 時間分である。1 時間の人件費が仮に 3,000 円とすると、300 万円のコストがかかることになる。

ところで、この従来型の人間によるリモートカメラの監視手法は、単にコストの問題だけでなく、作業員（被用者）に過酷な作業を押し付けるといった問題がある。これらの監視者たちが見せられる映像 1,000 時間分のほとんどは、善良な受験者の何の変哲もない無味乾燥な映像であり、それを見続ける精神的な疲労は、あたかも昔の深夜テレビの停波後の「砂嵐」の中に（アナログ地上波放送のテレビの場合は、毎晩深夜に「砂嵐」という現象があった。知らない新世代型読者たちは、YouTube 等で「砂嵐」を検索してみるとよい。）、異星人からの突然のメッセージ信号を見出すことができるかも知れないという期待を信じて（そのような噂が一時期小中学生の間にあった。確かにそれは、原理上あり得ることである。しかし、その当時、これを信じた者たちは、皆深夜テレビの砂嵐に見入って、寝不足となり、翌日学校で居眠りしていた。）、「砂嵐」を見続けるようなもので、極めて大きな疲労である。常に作業椅子に座してこれを行なわなければならない。これは、たとえば報酬と引き換えであったとしても、過酷な非人間的な作業である。これと比較すると、集合型試験会場で紙の試験を実施している現場を、受験者の集中の妨げにならないように工夫して静かに歩き回って巡視するような、従来型試験監督の作業のほうが、大いに人間的であり、全身をかなり精密にコントロールしながら行なうことから、自らの頭脳の働きも活性化し、精神の健全性も十分に維持されるのであった。

- (b) 次に、AI 技術を導入した本システムのような在宅型 CBT 試験において、監視コストを計算してみよう。監視者が神経を十分集中させて確認すべき映像は、全体の 1,000 時間分でなく、うち 990 人の善良受験者のそれぞれ 1 分 ~ 5 分程度の AI が検出した被疑点部分だけで済む。仮に 1 人 5 分くらいの被疑点 AI 検出されるとして、990 人の善良受験者を合計しても、その分量の合計は、わずか 80 時間で済む。他方で、10 名の不正受験者の映像データについては、たとえば

1 人あたり 30 分間分、AI が検出した被疑点部分を確認し、容易に不正と思われる行為を発見することになる。不正受験者の検出と映像の吟味に時間を十分かけることは、目的に適った有益なことであるから、コスト計算上さほど問題としなくても良いが、一応 1 人あたり 2 時間かけてこれらを吟味するとしても (この吟味にかかる時間は、AI 未導入の場合でも変わらないはずである)、合計 20 時間である。したがって、全部合計で 100 時間の確認時間かかる。1 時間の監視者の人件費が仮に 3,000 円とすると、理想的には、全体で、わずか 30 万円の監視コストで、(a) の 300 万円をかけていた監視コストと同じだけの不正受験者を発見することができる。

そして、この AI 支援を受けて被疑点だけを次々と確認していく (b) の手法は、(a) のすべての映像を人間が目視する手法と比較して、監視従事者の精神的負担を、相当和らげることができる。

なぜならば、監視従事者の画面には、特に不正の疑いがある点ばかりが次々に表示されるので、監視従事者は、それが不正か否か、それぞれ、かなり創造的な考え方を巡らして検討し、主催者に報告すべきか否かを判断するという比較的变化に富んだ仕事を、単位時間あたり、(a) の約 10 倍程度の密度でこなすことになるので、(a) と比較して、退屈をすることがない。

人間としていちばん精神的に辛いのは、常に一点の見落としも許されない神経の集中を長時間要求されるけれども、検出しなければならぬ特異な現象が稀にしか生じないような場合における、その監視作業である。AI 支援によって検出された不正行為の場面の映像は、監視者にとっても、それぞれが特異で創造的なもので、次々に興味深い映像を見て判断するという仕事は、少なくとも、(a) のような、干し草の中から針を見つけるような過酷な作業と比べて、相応な楽しみを見出すことができる生産的・人間的な作業である。加えて、AI が判定してもなお白黒つけ難いような被疑点の映像のみを、より高度な役割を持った人間が判断するというときのその判断が自らに今まさに委ねられているという重要な責任感によっても、肯定

的・健全な精神を持続することができる。よって、(a) の方法よりも、(b) の AI を活用した方法が、人間的である。

そして本システムのような AI 支援型被疑点検出システムの、素晴らしい点は、もう 1 つ存在する。従来の (a) 型であれば膨大な監視時間を要するので、ほとんど試験実施代行業者の被用者たちが、前記 (a) のような過酷な監視作業を強いられていた。他方、本手法では、AI が被疑点の映像だけをまとめて抽出してくれるので、確認すべき映像の総時間はかなり短縮され (前記の計算であれば、約 10 分の 1 に削減できている)、本システムを利用する主催者自らの側の人員でも、全部の被疑映像を検証可能になるという点である。すなわち、(a) の手法では、年中、様々な試験実施主体の代行者として大量の映像を一日中監視するような過酷な労働を行なう人員を、試験実施代行業者が確保し続ける必要があったが、(b) の手法では、監視すべき映像の時間が短くなったことから、様々な試験実施主体自らの社員・職員たちが、その執務時間を用いて検証することが可能になったのである。

前述のように、一年中監視カメラの映像を監視専門家たちが監視する仕事は、大変過酷で退屈なものであるが、試験実施主体の職員たちが AI が抽出した被疑点のみの検証を自ら行なうのであれば、それは、同じ監視作業であっても、その負荷が社会のさまざまな人員に分散したことになり、固定的な人材たちに集中する場合のそれらの方々の精神的な疲労という弊害が解消されるのである。

さらに、一般に試験実施主体の社員・職員のほうが、精神をより集中させてでも不正行為を見抜こうという真剣さが、代行業者の社員たちによるそれよりも、いっそう増すとしたら、本システムによる AI 支援の効果は、誠に良いことづくめであるということができる。

### 第 3 節 本システムで想定される不正行為とその実験評価

前述のように、本システムの有する AI 支援型の不正行為検出機能は、大変画期的であると言える。しかし、それはもちろん、本試験システムの有する在宅型 CBT における不正行為監視・検出機能が、有効に機能する場合に限定される。仮に AI

支援型の不正行為検出機能をうまく出し抜いたり、麻痺させたりする手法が、従来の集合型紙試験と比較して容易に行えるようになってしまったならば、本末転倒な結果となる。

いかなる場合でも、不正行為を 100% 発見・防止することはできない。従来型の集合型紙試験の実施においても、不正行為者が十分なコストをかければ、検出されない不正行為は可能であろう。そこで、すべての不正を防止することを要求する必要はなく、社会通念上許容される水準まで不正を防止すれば良いであろう。

従来の集合型紙試験と比較して、(a) 容易に、(b) 発覚のリスクが低く、かつ、(c) 低コストで不正ができる手法が存在するかどうか、重要な点であるといえる。(a) + (b) + (c) のいずれも成り立つ不正手法が存在するか否かの探求は、本システムや、同等の技術を用いた他製品の、集合型試験と比較した限界を明確にすることに他ならない。

本システムのような在宅型 CBT 試験システムの有する前記のような映像録画と AI による分析を用いた不正行為防止機能は、受験者の PC のカメラを用いて録画される映像を元に行なわれるものである。

不正受験者は、さまざまな方法で在宅型 CBT 試験システムの不正行為防止機能をかいくぐり、検出されることなく不正行為を成功させようと努力すると考えられる。その際、不正受験者は自己の PC のカメラで撮影される映像の撮影を妨害したり、そのサーバーへの送信を妨害したり、サーバーにインターネット経由で送信される際に映像をすり替えたりすることを画策したりすることが想定される。

そこで、在宅型 CBT 試験システムにおいては、このような不正行為がなされた場合を検証し、システムがどのような反応をするか、そういった行為を被疑として正しく試験実施主体に検出・通報する能力を有するかが、最重要の問題点となり、これを重点的に検証する必要がある。

そのため、まず、本システムを代表とした各種在宅型 CBT 試験システムにおいて想定される不正行為の典型例を考えてみる。これには、主に、以下のようなものが挙げられる。

## 1 カメラ妨害 (遮断)

最も簡単な不正行為として、撮影の妨害・遮断がある。不正受験者は、本システムが自らの受験中の様子を撮影することを妨害した上で、妨害中に不正行為を行なうことが想定される。

妨害には、2 種類の種類があると考えられる。

### (1) Web カメラによる撮影そのものに対する妨害

これは、最も簡単な妨害方法である。例えば、受験中に Web カメラを抜去する方法が考えられる。試験開始時には Web カメラによる撮影およびサーバーへの送付が成功する必要があるため (成功しなければ、試験が開始されない為)、試験開始後に Web カメラを抜去する行為が想定される。

#### 検証: カメラ抜去実験

試験を開始した後に、Web カメラを抜去したところ、カメラ読み取りが異常である旨のエラーメッセージが表示され、試験問題の表示が消え、試験は途中で中断された。

なお、その後に Web カメラを再度取り付けて試験ページにアクセスすると、試験は再開された。

したがって、本システムは、Web カメラそのものを抜去することによる撮影妨害に対する耐性は有していると考えられる。

### (2) 撮影されたデータがサーバーに送付される際の送付経路上での通信妨害

これは、受験中に通信の内容を色々と書き換えたり遮断したりして、撮影された動画データがサーバーに送付されることを妨げる手法である。

第一の手法と同様に、試験開始時にはカメラ映像の送信と AI 検出のテストが行なわれるので、当初は通信妨害をしてはならないが、試験開始後の任意のタイミ

ング（不正行為をいよいよ行なおうとするタイミング）で通信の妨害を開始すればよい。

これらの撮影妨害があった場合において、本システムがどのような挙動を示すかが、重要な問題となる。すなわち、何らかの方法で撮影妨害が成功したときに、本システムが、その受験者の受験全体を「正常受験」として判定してしまうと、もはや試験実施主体は、「なぜカメラ映像の撮影または送付が妨害されたのか」と真実を問うことの契機としての疑問すら生じなくなり、その不正受験者をみすみす見逃してしまうことにつながるためである。

### 検証その 1: SSL 中間者攻撃によるカメラ映像送付通信の妨害実験

本システムにおいて、Web ブラウザが試験サーバーに対してカメラ映像を送付する通信経路を妨害することは、それなりに手間がかかる。通常、特定のインターネット通信を妨害するためには、「パケットフィルタ」と呼ばれる、通信経路上のパケット遮断装置を設定し、特定の IP アドレスやポート番号と呼ばれる宛先宛の通信を指定して遮断する方法が簡単かつ確実である。ところが、不正受験者が本システムのカメラ映像の送付のみを遮断しようとするときに、パケットフィルタは利用できない。

パケットフィルタが妨害のために利用できない理由は、本システムの Web サーバーは、「〇〇〇.com」という名前のホスト名で示される HTTPS エンドポイントに集約されており、試験システムの Web ページや、試験中の試験問題の配信（ページ送り）や、受験者が選択または入力した回答データ（選択肢や自由入力欄）は、カメラ映像送付先と全く同一の宛先である、当該「〇〇〇.com」という名前のホスト名に対して、「HTTPS プロトコル」で送付されることに由来する。試験中に常時送付される受験者のカメラ映像は、10 秒毎に、H.264 形式（動画圧縮の規格）のデータとして、「HTTP POST」と呼ばれるプロトコルによって送付される。

「HTTPS プロトコル」は、「HTTP」という Web サイト接続用のプロトコルを、「SSL (TLS)」という暗号化プロトコルで包み込んだものである。HTTPS プロト

コルは、共通の宛先ポート番号「TCP 443」を使用する。SSL で包み込まれた通信内容は暗号化されており、すべて同一の IP アドレスの「TCP 443」というポート宛であるので、パケットフィルタによって内容を検査することができない。そのため、不正受験者は、自らのコンピュータのファイアウォールプログラムや、インターネット接続用ルータ等のセキュリティシステムの「パケットフィルタ」機能を用いて、カメラ映像のみを遮断することができない。不正受験者は、仮にカメラ映像をパケットフィルタで遮断しようと試みると、直ちに、試験そのものの表示や操作に必要な通信まで遮断してしまい、試験が続行できなくなってしまうのである。

これは、封筒のイメージで考えると、嚴重に封印されている封筒の中に色々なメッセージ（試験問題、答案データ、カメラの撮影データ）が入っているが、封筒の宛先は全部同じ住所が書かれているので、外から触っても中身がいずれであるか分からないという状況である。このイメージにおいて、パケットフィルタとは、不正郵便局員のような立場にある。カメラの撮影データのみを送付妨害したいのだから、いずれの封筒にカメラの撮影データが入っているのか、封筒の外からは分からないから、全部を送付妨害することしかできない。

そこで、不正受験者としては、SSL 中間者攻撃と呼ばれる手法を用いて、自らの Web ブラウザと試験サーバーとの間の通信を一度復号化してから、再度暗号化する必要に迫られることとなる。

SSL 中間者攻撃の手法は、先の不正郵便局員のイメージで表現すると、郵便局員が一度封筒を開封して、中身を確認し、中身がカメラの撮影データ以外の内容であれば、再度ほとんど似たような封筒に封入して送付するような盗聴行為に似ている。中身がカメラの撮影データであれば、その郵便物をさっと破棄してしまうのである。

この手法を用いれば、封筒の宛先だけでなく、中身に着目して、カメラの映像のみを破棄することが可能となる。

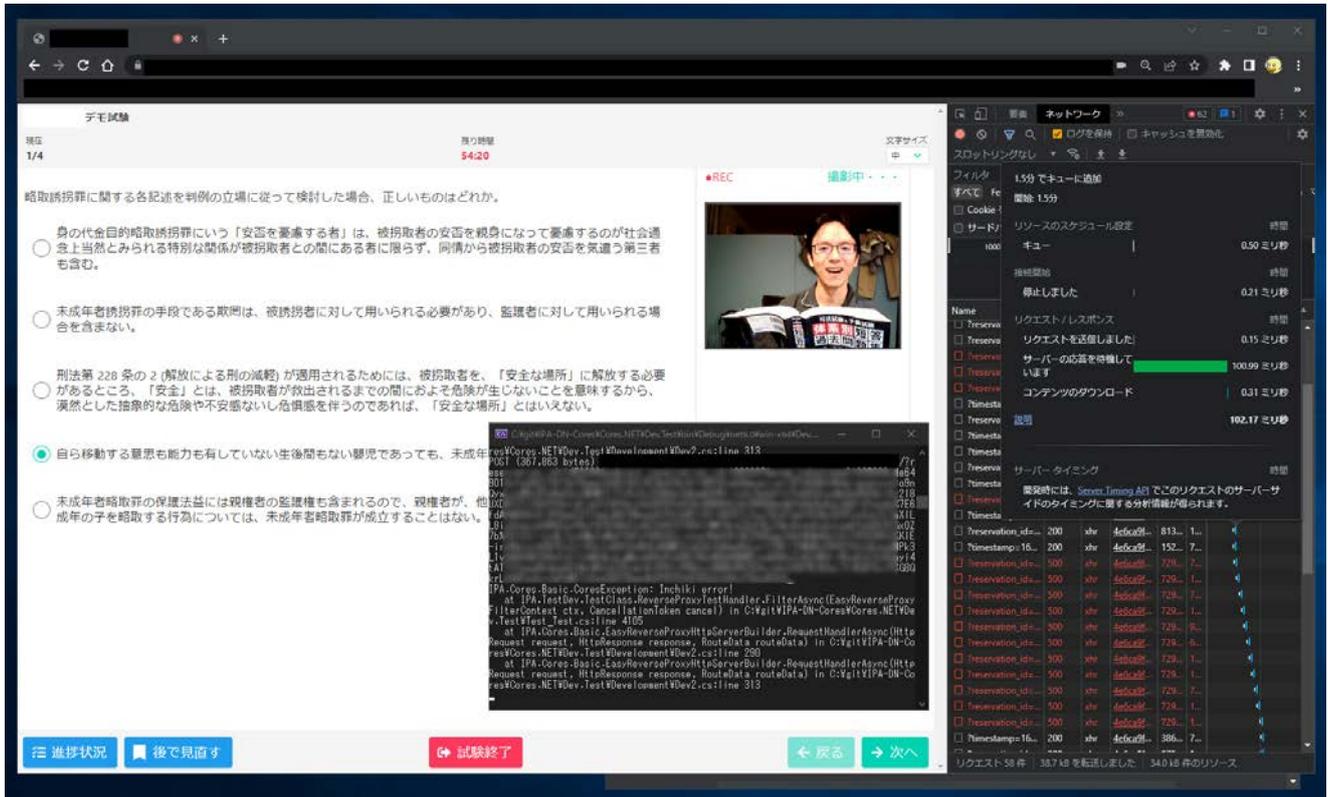
SSL 中間者攻撃の手法は、通常は第三者の通信内容を解読する際に利用される。他人の電気通信を無断で復号化して再暗号化する盗聴行為は、犯罪行為（電気通信事業法違反）である。しかし、今回は、受験者が、他人ではなく、自らが当事者と

なる通信を一度復号化して再暗号化する行為なので、電気通信事業法上は、違法ではない。

SSL 中間者攻撃は、簡単なプログラムを書くだけで実現することができる。実際に本システムと Web ブラウザとの間で SSL 中間者攻撃を行ない、カメラ映像の遮断を行なう実験を行なってみた。この自作プログラムでは、試験開始後、最初の 1 分間だけ、カメラ映像を遮断せずにそのまま送付する。1 分間が経過したら、それ以降のカメラ映像はすべて遮断する。

結果は、図のとおり、意図通りにカメラ映像のみを送信妨害することが容易にできた。この結果、試験サーバーには試験開始後のカメラ映像のうち最初の 1 分間くらいのデータが送付され、それ以降のデータは送付されない。不正受験者として、図のカメラ映像のように過去問集を悠々と読みながら試験を受験したが、結果として本システムのサーバーにはその間の録画データが一切蓄積されず、試験開始後 1 分間の録画データのみを対象として AI 分析がなされた。その結果、「正常受験」として判定がなされた。

よって、SSL 中間者攻撃によるカメラ映像送付経路の妨害により、不正行為を行なうことが可能であることが分かった。



SSL 中間者攻撃プログラムを自作して Web ブラウザと試験サーバーとの間の HTTPS 通信を書き換えることにより、カメラ映像の試験サーバーへの送付を妨害でき、カンニングを行なっても「正常受験」と判定されることに成功した。

## 検証その 2: パケットロス偽装方法によるカメラ映像送付通信の妨害実験

前記の「検証その 1」で実施した SSL 中間者攻撃手法は、簡単なプログラムを書けば、誰でも、確実に実行が可能である。そして、この中間者攻撃は透過的に行なわれるので、試験サーバー側は、中間者攻撃を受けたことを知る手段がない。

しかしながら、これはかなり積極的な不正行為であるので、不正受験者としては、不正行為を行なった証拠が何らかのミスによって掴まれてしまった場合は、相当不利な立場に立たされることになる。そしてまた、SSL 中間者攻撃手法を利用する際には、一応プログラムツールを介在させる必要があるもので、若干技術力が必要である (といっても、本システムが重要な試験で利用されるようになったとしたら、カメラ映像遮断にとっても有効な SSL 中間者攻撃プログラムが出回るのは時間の問題であるから、不正受験者としては、単にそういったプログラムを入手すれば良く、それほど高度な技術力は不要であろう)。

そこで、不正受験者としては、より消極的・受動的な方法で、カメラ映像送付を

妨害することができれば、リスクが低く、尚良いということになる。すなわち、何ら高度・複雑なプログラムツールを内部的に介在させることなく、何らかの事象を外部的・環境的に引き起こし、その事象が不運にも試験システムにおけるカメラ映像の送付の妨げとなってしまったというように外形上見える工夫を実現できれば、不正受験者として、不正が発覚し追求されるリスクを下げるができる。

このような軟派な不正受験者として利用できる手法には、どのようなものがあるだろうか。容易に思い付くのは、受験者の PC からインターネットを経由して試験サーバーに向けた通信がなされる通信回線上の通信品質を意図的に劣化させる手法である。Web ブラウザからは、同一の通信先である「〇〇〇.com」という HTTPS サーバーに対して、外形的には同一のプロトコルにより、(a) 試験問題の要求、(b) 答案の送付、(c) カメラ映像の送付、の 3 つの種類通信が送付される。ここで、(a) は単なる要求文であり、また、(b) も短い分量のデータであることが推測される。(a), (b) はいずれも数百バイトから 1 キロバイト程度であろうと予想可能である。これと比較して、(c) のデータは、映像データであるから、かなり大きなデータになると推測可能である。実際に、(c) のデータは 10 秒間に 0.25Mbytes、1 分間に 1.5Mbytes 程度の分量となる。60 分間の試験であれば、90Mbytes 程度である。かなり大きいデータ量である。

ここで、インターネット通信に関する基礎知識を有すると想定される不正受験者の立場で、少し戦略を練ってみよう。(a), (b), (c) のいずれも、HTTPS という手法でサーバーにデータを送信する。HTTPS とは、HTTP を SSL で包んだものであるが、そのデータ量は、暗号化される前のデータ量におおむね比例する。そして、インターネットでは、ある程度大きなデータを送付するときは、TCP のパケット分割の仕組みにより、そのデータを複数のパケットに分割して送付することになる。インターネット上の送付データは、おおむね 1,460 バイトまたはそれ以下のデータに分割され、分割されたデータが次々に連続して送付される。TCP の特性上、次々に連続して送付する際には、スロースタートおよび輻輳制御という少し複雑なメカニズムが働き、通信回線が混雑している場合はゆっくりと、通信回線が空いている場合は素早くデータが送付される。(a), (b) のデータ送付は、ほとんど 1

または 2 個のパケットで完結しそうである。他方で (c) のデータ送付は、1 回の送付 (10 秒分のデータ) あたり 0.25 Mbytes (250,000 バイト) 程度の塊であるから、これを 1,460 で割ると、約 170 個のパケットとなる。すなわち、1 つのカメラ映像が送付される際は、約 170 個のパケットに分割される。このような通信の基本的知識を利用すれば、不正受験者は、自らの PC からインターネットに対して送付されるパケットについて、(a), (b) のパケットの送付は完了するものの、(c) のパケットはなかなか送付されない状態を、確率的に作り出すことができる。

具体的手法としては、インターネットの出口において、アップロード (送信) 方向の回線を混雑させたり、意図的にパケットの破棄を作り出したりして、ちょうど良い具合に (a), (b) のみを通過させ、(c) が遮断されるような状態を成立させれば良いのである。

そこで、著者が色々と試行錯誤をしてみた結果、おおむねパケットロス率が 65% 程度に通信回線が劣化したときに、(a), (b) すなわち試験問題の要求と答案データの送付のための通信はすべて成立し、(c) の通信すなわち監視カメラの送付通信は途中でタイムアウトになる状態を作り出すことができることが分かった。

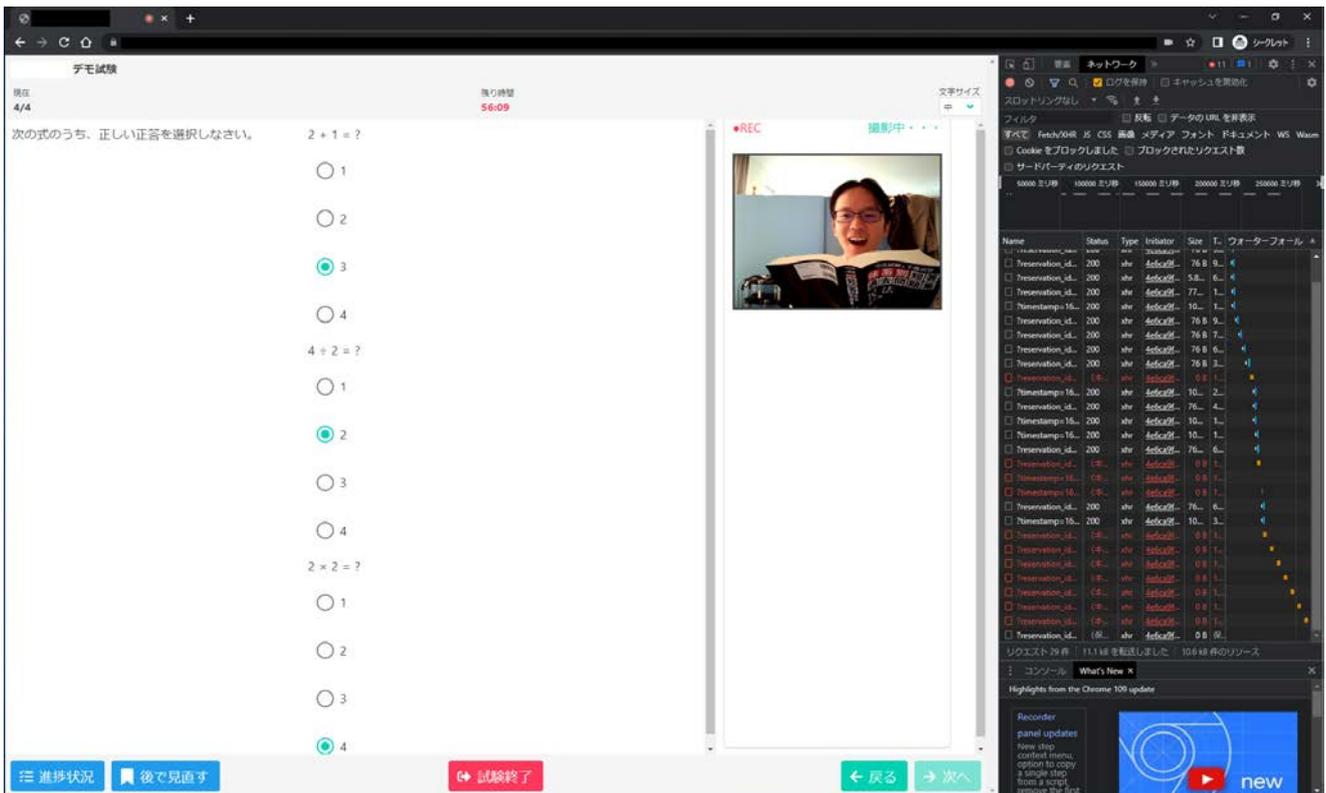
```
管理者: コマンド プロンプト - ping
からの応答: バイト数 =32 時間 =5ms TTL=118
からの応答: バイト数 =32 時間 =5ms TTL=118
要求がタイムアウトしました。
からの応答: バイト数 =32 時間 =5ms TTL=118
からの応答: バイト数 =32 時間 =5ms TTL=118
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。
からの応答: バイト数 =32 時間 =5ms TTL=118
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。
からの応答: バイト数 =32 時間 =5ms TTL=118
からの応答: バイト数 =32 時間 =5ms TTL=118
要求がタイムアウトしました。
からの応答: バイト数 =32 時間 =5ms TTL=118
要求がタイムアウトしました。
要求がタイムアウトしました。
からの応答: バイト数 =32 時間 =17ms TTL=118
要求がタイムアウトしました。
からの応答: バイト数 =32 時間 =5ms TTL=118
要求がタイムアウトしました。
要求がタイムアウトしました。
```

試験サーバーとの間のインターネット通信に対して、約 65%のパケットロスを意図的に引き起こしている様子 (ping コマンドによる通信状態の確認画面)。

本システムの監視カメラの送付通信は、10 秒ごとの H.264 形式の映像録画データを送信待ち行列に入れて、これを順次サーバーに HTTPS で送信していく手法によって実現されている。この送信は 10 秒間のタイムアウトが設定されている。10 秒以内に送信に失敗すれば、一旦諦めた上で、再度、送信を一から再試行するようになっている。約 170 個のパケットに分割された 0.25Mbytes のデータを送信しようとするとき、約 65% のパケットロスがあると、一部のパケットが、TCP/IP の通信上、何度も再送を繰り返すことになり、なかなか送信が終わらない。その間に 10 秒間が経過してしまうと、再度一から送信を再試行し直す。この無限の繰り返しにより、(c) のカメラ映像は、全くサーバー側に到達しない結果となる。そのうちに試験は終了してしまい、答案データが送付され成績が確定した後に、受験者は Web ブラウザを閉じる。閉じた瞬間、これまでメモリ上に蓄積・記録されてきた未送付の監視カメラの映像データは、永久に失われる。

図は、パケットロスを発生させた結果、カメラ映像の送付が妨害された様子を示している。評価者は、試験問題を、過去問集等を読みながら悠々と解いているので

あるが、その際の映像は、自らの PC 上で撮影・圧縮はされるものの、ついに、試験終了時までサーバーに 1 枚も送付されることなく、試験は無事にすべて完了した。結果として本システムのサーバーにはその間の録画データが一切蓄積されず、試験開始後 1 分間の録画データのみを対象として AI 分析がなされた。その結果、「正常受験」として判定がなされた。



約 65%のパケットロスを引き起こすと、CBT の不正防止用の Web カメラの映像送付の通信をちょうど良い具合に妨害できた。他方で試験そのものの進行の通信は可能であり、SSL 中間者攻撃を用いることなく、AI による「正常受験」判定を AI によって得ることに成功した。単に通信が混雑しているように見えるので意図的な不正通信妨害であることが証明されてしまうリスクは、極めて低い。

よって、単なるパケットロスを発生させるだけの手法によっても、カメラ映像送付経路の妨害により、不正行為を行なうことが可能であることが分かった。この手法の不正受験者にとってのメリットは、(1) 検証その 1 で述べた方法と比較して、特殊な通信内容介入ソフトウェアを利用する必要がなく、(2) 発覚しづらいこと、(3) 単に通信経路上の混雑によって問題が引き起こされたのであるという抗弁が容易であること、(4) 試験実施主体の側がその抗弁を覆して、通信経路上の混雑が不正受験者によって意図的に引き起こされていることを証明することは容易では

なく、実際問題としてほとんど不可能であること、等が挙げられる。さらに、特殊なソフトウェアを用いる必要がないので、心理的な抵抗（罪悪感等）も、その 1 の手法よりも薄まることから、その 1 の手法に出る硬派な不正受験者と比較して、より軟派な不正受験者は、本手法を是非利用したいと思うであろう。

## 問題の本質

上記の検証結果は、在宅型 CBT 試験におけるカメラ映像の監視の仕組みの本質的問題を浮き彫りにする。

善良な受験者が本システムを使用する場合、様々な通信経路上の不具合や混雑が一時的に発生したり、試験サーバー側における映像受信能力・容量不足が一時的に発生したりしたとき、特定の受験者による試験途中のカメラ映像の一部または全部が試験サーバー側に送付・蓄積されない事象が発生し得る。

このようなカメラ映像の欠落事象は、ほとんどの場合、受験者の責任外で発生するものである。したがって、カメラ映像が多少欠落しているからといって、その受験者を失格にすることはできない。受験者を失格にするためには、カメラ映像の欠落が意図的に引き起こされたということの証明が必要である。

ところが、前記のそれぞれの手法は、いずれも、受験者の側のネットワーク環境上で通信経路に対する妨害が行なわれたものであり、受験者が完全に管理・支配する領域（宅内のネットワーク）において実施された不正行為である。そのような不正行為を、外部に存在する試験実施主体やシステムを運営する代行業者が見抜くことは、ほとんど不可能である。

## 解決策

これが、本システムのような、現在の一般的な在宅型 CBT 試験システムにおける監視カメラ方式の限界である。これを解決するためには、技術的な工夫・進化が必要である。どのような工夫が考えられるであろうか。

例えば、複数のカメラにおける監視を要求するという手法が考えられる。近年は

スマートフォンが普及しているので、受験者に対して、受験用 PC の他に、少なくとも 1 台のスマートフォンでも、違う角度から試験中の受験者の映像を撮影させるという手法である。そして、そのようなスマートフォンにおける第二のカメラの撮影映像送信機能は、スマートフォンのアプリとして実装し、十分なバッファを有した状態で、試験終了後もゆっくりと送付させるようにするのである。

そのような第二のカメラによる映像データを要求することにより、第二のカメラの映像データがない場合は、第一のカメラにおける映像欠落時は不正行為ありと見なす旨の試験ポリシーを定めることができるようになる。

ただし、この手法は、受験者に対して余分なスマートフォンの供用を義務付けることになる。また、スマートフォンを適切な角度で立て掛けておくスタンド等の準備も義務付けることになる。スマートフォンのアプリも必ずしも安定して動作するとは限らない点も問題となる。

また、スマートフォンのアプリに対する改造や SSL 中間者攻撃が可能となり、スマートフォンで撮影した映像の改ざんや録画データに対する差し替えも可能となる。ただし、映像改ざん・差し替えについては、たとえば受験の様子を受験中のディスプレイ画面を含めて背後から撮影させるようにし、受験中のディスプレイ画面の一部にワンタイムパスワード的な文字列や QR コード等を表示させる方法によって、かなり防ぐことができると考えられる。

## 2 カメラ妨害 (映像劣化)

次に簡単な不正行為として、不正受験者による映像の意図的劣化がある。映像の劣化にも様々な手法がある。評価方法としては、ある程度の不鮮明な動画データを送付したり、試験の冒頭と試験中とであえてピントをぼかす度合いを変更したり、また、映像をキャプチャする間隔をととても長くする等して、不正目線検知がされず、結果として AI による正常性判定を獲得することが容易に可能かどうかの検証が必要である。

想定される手法としては、以下のようなものがある。

## (1) 解像度の低下（安価な西暦 2000 年代の 10 万画素の中古 Web カメラをあえて利用する等）

録画映像を元に、受験者の眼球の動きを、AI または人力で検出する方式の不正行為検出手法で検出されないようにする程度に解像度の低い映像を送付するという不正手法が存在する。

不正受験者の視点としては、どのようにして解像度の低い映像を送付すれば良いかが問題となる。これは、意外にも簡単である。極めて安価な 2000 年頃に発売された Web カメラを利用すれば良いのである。20 年以上前に発売されていた Web カメラは、10 万画素等の現代の水準から比較すると想像できない程度の品質の低いものであった。これらを堂々と利用して、不正目線の検出が困難な程度の画質低下を作り出せば良い。

この方法は、心理的障壁が低い。万一、試験実施主体から、なぜこのような画質の悪いカメラを利用するのかと聴取を受けた不正受験者は、「私は、この安価な Web カメラしか持っていないから、これを利用しているのである。」と堂々と答えることができるためである。ただし、後述のような検証方法で、そもそも AI の判定において「正常受験」と自動判定されることを実現できれば、試験実施主体は、解像度の低いカメラの映像すら一度も確認することなく、見逃されることになるであろう。

さらに、このような古い Web カメラの中には、焦点距離 (ピント) を手動で調整することができるものがある。そこで、ある程度不鮮明な映像を送付することで、視線の動きがはっきりとわからないようにする方法が考えられる。また、試験の最初 (写真の撮影や AI による顔検出等の動作テストが行なわれる) は鮮明な映像を送付しておいて、後から不鮮明な映像に切り替えるような、工夫を凝らした不正手法も考えられる。

### 検証: 2000 年頃発売された 10 万画素のカメラの利用

そこで、評価者は、わざわざ、本記事による評価のためだけに、2002 年頃に発売されたと思われるサンワサプライ社の「CMS-USBV10」という非常に古い Web

カメラを、インターネットオークションで、わずか数百円で落札・購入し、このカメラを用いて AI による不正目線検出をすり抜けることができるかどうか確認をした。



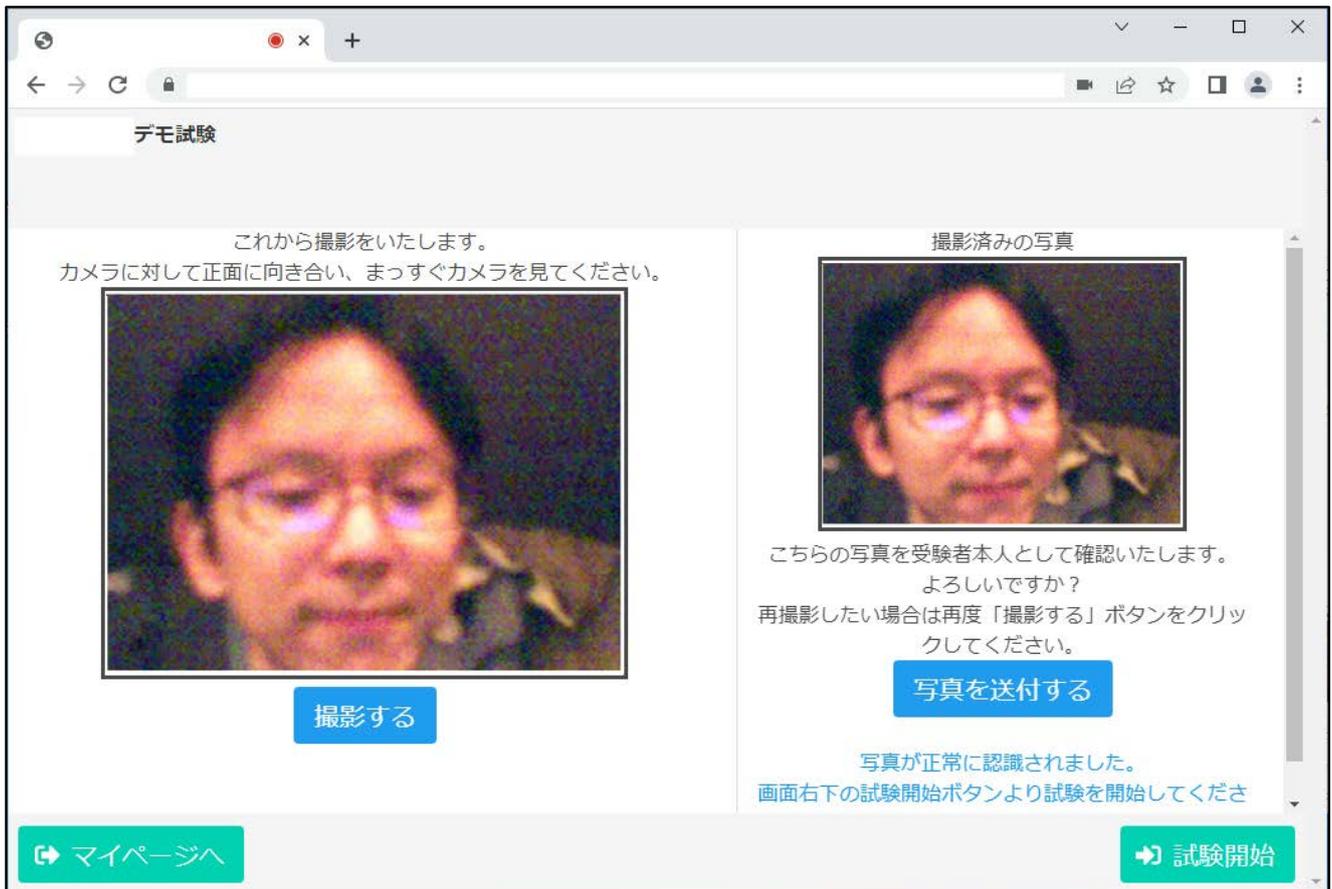
2002年に発売された10万画素の骨董品的価値を有するCMOS Webカメラの新品パッケージ。著者は、本実験のためだけにわざわざYahoo!オークションでこれを購入したのである。

この Web カメラのパッケージには、「Windows 98 対応」、「10 万画素 CMOS センサー」などの、心躍る特徴が記載されている。さて、これを最新の Windows 10 のコンピュータで動作させるには、一苦勞を要した。まず、32bit ドライバが存在しないので、Windows 10 の 32bit を手元のノートパソコンにクリーン・インストールした。次に、カメラ用のドライバが Windows XP や Windows 2000 までの形式しかなく、ドライバの「inf ファイル」と呼ばれる定義ファイルの書式が Windows 10 ではうまく読み込めなかったため、inf ファイルに加工を施して、無理矢理 Windows 10 で認識させた。



「Windows 98 対応」、「10 万画素 CMOS センサー」等の懐かしい記載があるパッケージ。ドライバが Windows 2000 / XP (32bit 版) までしかなく、現代的な Windows 10 の PC に認識させるためには、若干の苦労を必要とした。しかし、本実験のためならその苦労は厭わない。

この大変解像度の低い安価な Web カメラを用いて、本システムによる試験を受験してみた。受験中においては、視線を部屋の中で上下左右大きく動かしてわき見をした。手元の参考書を読んだり、近くのモニタの文字を見たりするといった具合である。その結果、本安物 Web カメラにおいては、不正視線が被疑点として検出される精度は、最近のパソコンに搭載されている通常の画質の Web カメラと比較して、著しく低下することが確認できた。何度か検証を実施した結果、全く不正視線が検出されないこともあった。



20年前の10万画素のCMOS Webカメラの画質は、この程度である。とても懐かしい画質である。20年前は皆この画質でNetMeeting等を楽しんでいたのである。

さらに、本 Web カメラのピント調整機能を操作して、さらに不正が容易に可能となるかどうかを検証した。試験の開始時における顔写真の撮影においては、ピントは、ある程度合わせておく必要がある。そうしなければ、試験実施主体が顔写真を事前送付している証明書等の顔写真と一致するか否かを確認する際に、ピントをあえてぼかしていることが発覚してしまい、不正行為が疑われて、不正受験者にとって不利益であるためである。

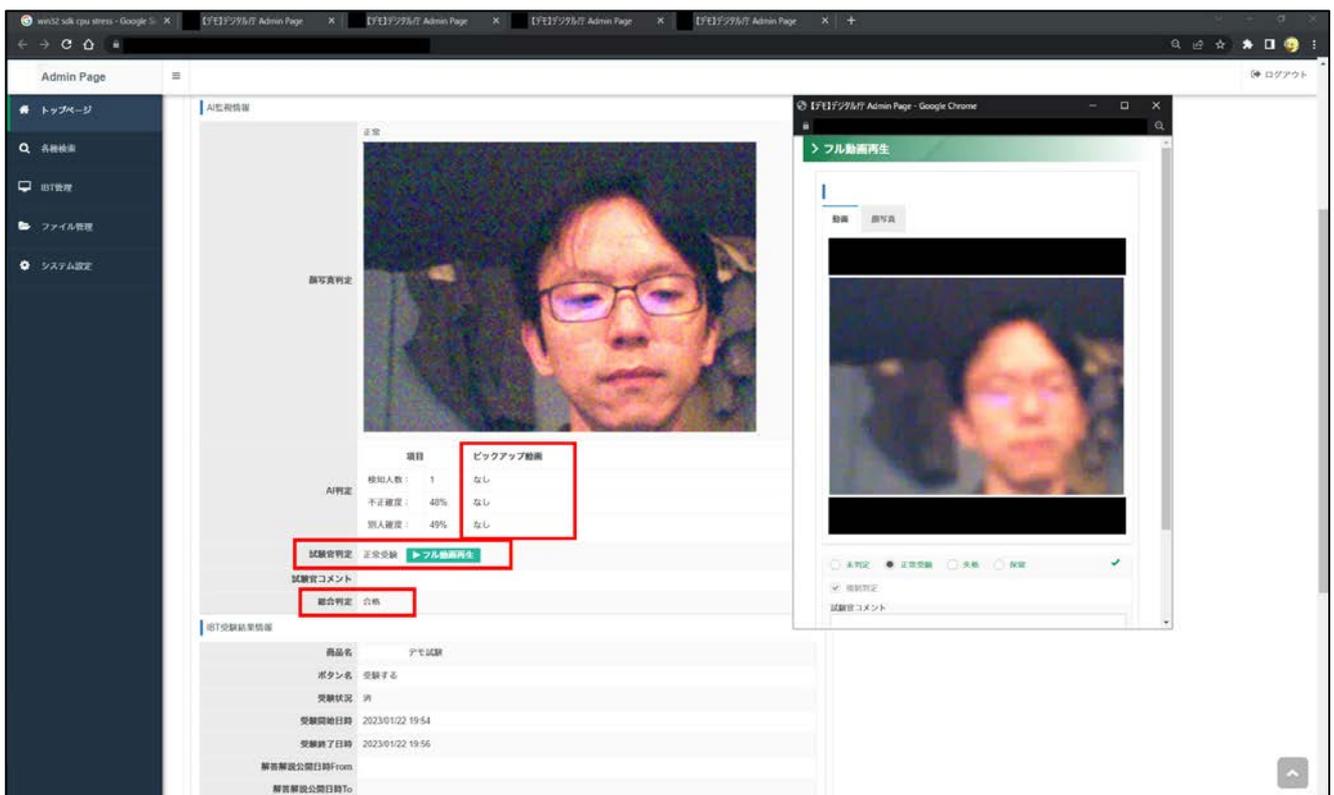
そこで、試験開始後に、改めてピントを操作して、ある程度ぼかした状態にしてみた。うまくやれば、ある一定レベルのピントぼかし度合いまでは、AI は、最初にある程度鮮明なピントで撮影した静止画と、ピントぼかしがなされた際の撮影データとの間で、「別人確度」（すなわち、試験の途中で受験者が入れ替わっていないかどうかを示す AI 判定の確度数値）が一定の閾値以下（すなわち、別人であるという被疑点が生じないレベル）に保てることが判明した。

下図において、左側の顔写真が、試験開始前に Web カメラで撮影させられる顔

写真である。この左側の写真を撮影する際には、Web カメラのピントは、それなりに合った状態にしておいた（そうしないと、試験実施主体によって、顔写真一覧を検査された際にピントぼかしが発覚し、これに引き続く試験時間全体のピントぼかしが発覚する可能性があるためである）。そして、試験開始後は、ピントを操作して、この右側の映像のような程度にぼかした。

その結果、(1) AI は、左側の写真と、右側の映像とを、同一人物であるとみなした。そして、(2) AI は、右側の映像のすべてのコマを判定したが、右側の映像はピントがぼかしてあるので、目線が写っておらず、目線の不正な動き（カンニング）を検出できなかった。

これにより、試験システム上の受験者一覧画面において、自らの映像について、AI による「正常受験」という自動判定結果が得られることに成功した。



左側の写真が、試験開始時の写真撮影（本人確認用）である。これはピントをあわせてそれなりに鮮明に撮影する。次に、試験が開始されたら、いよいよ、カメラのピントをぼかすのである。すると、右側の写真のような具合になる。ここで、AI は左側と右側を同一人物であると判定し（実際に同一人物であるから、この点は正しい）、一方、右側の目線はほとんどピンポイントで写っているため、不正目線検出可能は働かず、カンニングし放題な状態となったのである。

よって、不正受験者の視点としては、古い 10 万画素程度のカメラを活用し、か

つピントをちょうど程良く調整することにより、AI による別人検出アルゴリズム上は正常であるという結果を生じさせ、かつ、試験中は、不正目線の動きの部分、ピントぼかしによって不正検出されないような状態を維持することが可能である。

## 問題の本質

この問題の本質は、在宅型 CBT 試験におけるカメラのハードウェアとして、受験者自ら提供のものを利用せざるを得ないことに由来している。すなわち、カメラの調子や具合は、受験者の有する資産・物品に依存するのである。

カメラは、もともと、製品間で性能差があり、同一型番であっても個体差がある。また、受験者は多種多様な PC を用いて試験に臨む。カメラで受験者の映像が一応映っている限り、AI はこれを正常とみなしてしまう。また、たとえ人間によって検査を行なう場合であっても、カメラの画質がある程度低いことをもって、直ちに失格であると宣言することは、かなり困難である。カメラの画質だけでなく、部屋の環境 (例えば、室内照明の明暗、逆光等の差し込み具合、メガネのブルーライトレンズの反射の具合等) で受験者の目線をどれだけ鮮明に撮影できるかが、AI 検出の精度を大きく左右する。試験開始時および試験中に特に警告を受けずに試験を最後まで受験し、答案を提出したのであれば、後から、目線部分の撮影がぼやけていたということを理由に失格にすることは、不正行為の確証がない限り、極めて難しい。正当な受験者からの強い非難を浴び、場合によっては争いにまで発展する可能性があるためである。

## (2) CPU 負荷の意図的増大によるカメラ監視フレームレートの低下

在宅型 CBT 試験システムのクライアントアプリは、受験者の PC 上で動作する。受験者の PC 上では、他にも様々なアプリが動作している可能性があり、これらの他のアプリは、試験実施主体のコントロールの範囲外である。

そこで、不正受験者としては、受験中に、特に CPU 負荷を高負荷とするようなストレスの高いアプリを同時に稼働させて、在宅型 CBT 試験システムのクライ

アントアプリのプロセス (Web ブラウザ型の場合は、Web ブラウザプロセス) に割当てられる CPU の処理時間を減殺するという手法が可能である。

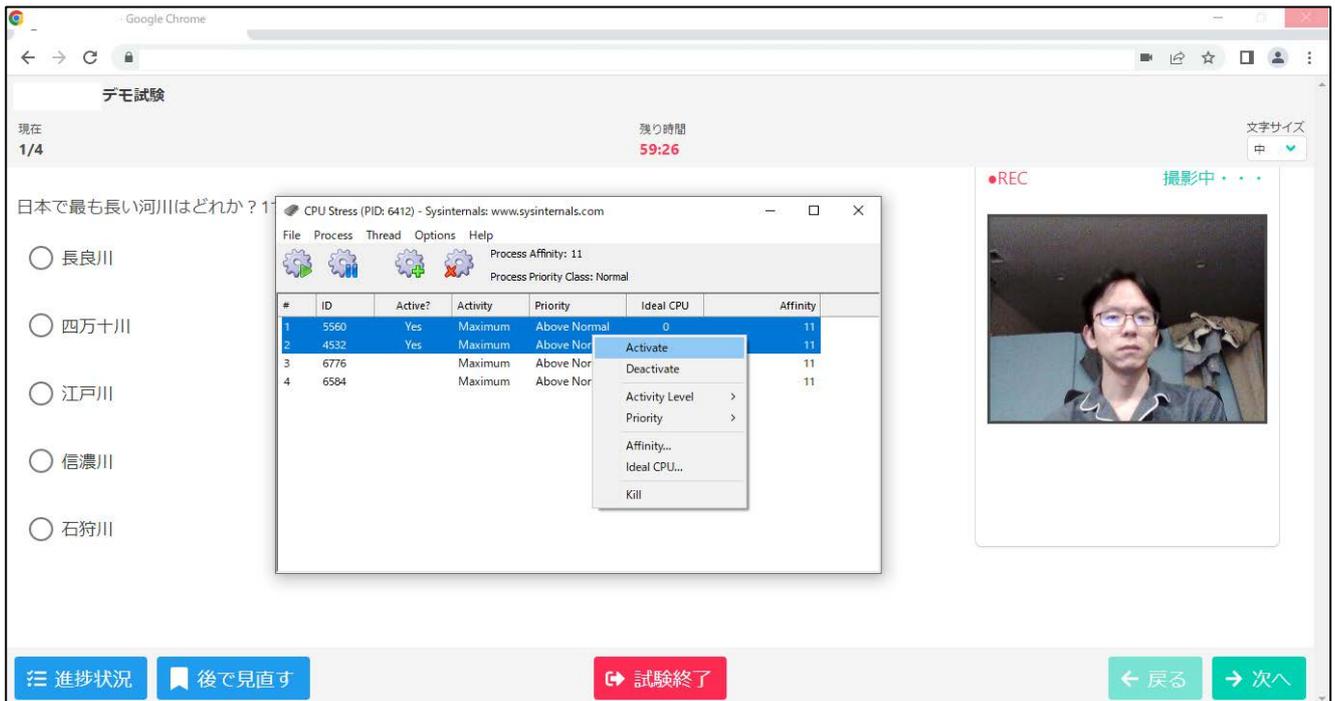
そうすれば、在宅型 CBT 試験システムのクライアントアプリは Web カメラからの映像キャプチャ、キャプチャ映像のエンコード (圧縮)、および圧縮結果のインターネット経由での CBT サーバーへの送付等のいずれのプロセスの動作を鈍くすることができる。

平常時であれば、毎秒 5 枚くらいの静止画が連なった映像データがスムーズに送付されるべきところ、数秒に 1 枚くらいのデータしか送付されなくなる現象を、意図的に作り出すことができる。CBT サーバーが受け取る映像データのフレーム (コマ) が、かなり間引かれるので、その間に物理的にちらちらと不正行為 (たとえば、目線の不正移動) が行なわれても、気付かれることがなくなる。

### 検証: Microsoft 「CPU Stress」ツールを用いた試験中の CPU 負荷の急上昇

試験中の CPU 負荷の急上昇を実行するには、C 言語などで作成した自作のツールを用いてももちろん良いが、Microsoft 社が Windows 用のツールとして配布しているフリーウェア「CPU Stress」が存在するので、これを利用すれば手抜きの楽である。そこで、このツールを用いて、本システムにおける試験中に CPU 負荷の意図的増大によるカメラ監視フレームレートの低下を引き起こし、不正が可能かどうかを検証した。

これはとても簡単であり、試験中に不正をしたい状態になったときを見計らって、「CPU Stress」ですべての CPU 時間を全く無駄に消費するように操作すればよい。その際の CPU 優先度は、「通常以上」がちょうど良いことが分かった。それよりも低い CPU 優先度にとすると、Web ブラウザによる撮影データのキャプチャや圧縮、送付がそれほど妨害されない。それよりも高い CPU 優先度にとすると、逆に、試験画面における選択肢のチェックやボタンのクリックが大変遅くなり、不正受験する際の実質的な試験時間 (答案を考えるための時間) が、極端に短くなってしまう。



このけしからん受験者は、試験が開始されると、さっそく、自分の PC の CPU 負荷を無意味に高揚させるのである。すると、カメラの映像キャプチャや H.264 圧縮ののコマ数が直ちに低下し、間引かれた状態で試験サーバーに送付される。その結果、AI 型監視検出であっても、人間型監視であっても、映像が間引かれているので、不正行為を見抜くことが困難となる。

検証結果として、試験中の CPU 負荷の急上昇中は、動画データはスムーズに送付されず、かなり細切れに送付される状態を作り出すことができた。これにより、目線を大きく動かすなどの不正行為を行なっても、AI によって検出されることを防止でき、不正受験の目的が達成可能であることが分かった。

## 問題の本質

この CPU 負荷の意図的増大による映像送信妨害という不正手法の優れている点は、不正受験者の側において、試験実施主体からの事情聴取に対して、「意図的な不正はしていない。」「たまたま、PC の調子が悪かったようだ。」、あるいは、「この程度の CPU 負荷で動作がおかしくなる本 CBT システムのクライアントアプリの出来が悪いのである。」などというように、否認の主張が簡単に行える点にある。

最近の PC は、様々な真に信頼できないアンチウイルスソフトウェア等がイン

ストールされ、ますます高度・複雑となっており、色々なバックグラウンドタスクが並行して稼働している。そのため突然 CPU 負荷が上がり通常のアプリの CPU 動作が圧迫されたり、またそれによって生じる廃熱が、高度な CPU の動作速度の調整機能を動作させて CPU クロック数 (計算の速度) がダイナミックに乱高下したりすることは、通常 of 自然な事象である。そのような最近の PC の複雑な事情にうまく紛れて、コンピュータの調子を程良く狂わせ、映像送付のコマ数を少なくしてしまえば、このような不正行為が用意になるのである。

試験実施主体が、そのような CPU 負荷の増大による映像の欠落が受験者によって意図的に引き起こされたことを証明することは、極めて困難である。

## 解決策

CPU 負荷の意図的増大による映像送信妨害という不正手法の検出や予防を実現するのは、Web ブラウザ型のアプリでは、かなり困難である。Web ブラウザは、ユーザーのプライバシーを保護するために、アプリに対して、同一のコンピュータ上で他にどのようなプログラムが動作しているかを知る手段を与えていないためである。

一方で、仮にネイティブアプリ方式であれば、他にどのようなプログラムが動作しているのか、各プログラムの現在の CPU 使用率はどの程度かといった情報を OS から取得することができる。これを試験サーバーに送付することにより、不正受験者が意図的に他のプログラムの CPU 使用率を増大させている事実を捕捉することはできるかも知れない。ただし、それでも送付できるのはせいぜいプログラムファイルのファイル名や消費 CPU 使用率、メモリ容量程度である。不正受験者はプログラムファイル名を怪しくない名前に変更するなどして、不正行為の発覚を妨げることが可能である。

より完全な対処方法としては、後に述べるように、第二の監視カメラアプリを設置させ、これを、スマートフォン等の、アクティブなアプリケーションが CPU をほとんど占有することができることを保証したプラットフォーム上で動作させる

ことが挙げられる。

### 3 カメラ映像改ざん (平穏な映像のループ再生等)

もう少し高度な不正行為として、不正受験者がカメラ映像を差し替えるといった手法が考えられる。これは、試験前に予め録画しておいたカメラ映像を試験中のものとして流す方法のほか、試験開始後一定時間 (例えば数分間程度) の何の変哲も無い平穏なカメラ映像をループ再生したり、これを短時間に分割したものをランダムに結合したりして、残り時間 (例えば 55 分程度) 分の映像データを作り出す方法が挙げられる。

何の変哲も無い平穏なカメラ映像を、長々とループ再生すれば、AI による検知であっても、人手による検知であっても、いずれの検査者も偽の平穏映像を見せられることになり、その間に、不正受験者は映像で監視されていないこととなり、いかなる物理的な不正でも可能となる。前記のカメラ妨害の手法では、システム側が妨害されたことを認識し得るので、不正受験者は、後で事情聴取を受けたり、場合によっては失格とされたりするリスクがある。しかし、カメラ映像を改ざんする手法では、そのリスクがなくなるので、不正受験者にとって有利である。

このカメラ映像改ざんの手法は、大きく分けて 2 つの方法が想定される。

#### (1) カメラの映像ソースの入れ換え

在宅型 CBT 試験システムのクライアントアプリを受験者の PC 上で動作させる際、そのアプリは、Web ブラウザ型であっても、ネイティブ型であっても、PC 上で認識される Web カメラのデバイスドライバから、映像信号を常時受け取る。システムがデバイスドライバから受け取る映像信号が、すでにその時点で書き換えられていれば、システムは、書き換えられた映像データを受け取ることになり、すでに映像データが書き換えられているか否かの見分けを付けることは困難である。

この映像ソースの入れ換え手法は、さらに細分化して説明すると、3 つの方式が存在する。

## (a) キャプチャデバイスに映像入力信号として録画データを入力する手法

PC の Web カメラは、ソフトウェア的には、ビデオキャプチャデバイスとして認識される。そこで、すでに任意のカメラ (Web カメラでも良いし、ハンディカム等でも良い) で撮影した、正常な 60 分間分の映像データを編集・生成し、これを試験中には外部機器から再生して、ビデオキャプチャデバイスを通じて PC に入力すれば、在宅型 CBT 試験システムのクライアントアプリが、これを Web カメラのものと誤認して、試験中の映像としてサーバーに送付する。

なお、在宅型 CBT 試験システムのクライアントアプリは、キャプチャデバイスの USB 上のベンダ ID やデバイス ID 等の製品固有の識別子も、サーバーに対して報告するが、この際の識別子は、クライアント PC 上のデータである。在宅型 CBT 試験システムでは、不正受験者がクライアント PC の OS 全体を含めたシステムを完全に支配しているため、OS やデバッグの知識を有していれば、自由にこれらを書き換えることが可能である (逆に、Web ブラウザのプログラムの側を書き換えても良い。Chrome 等の Web ブラウザはオープンソース実装であるため、自由にその挙動を改造することができる。)

在宅型 CBT 試験システムのクライアントアプリが知り得るキャプチャデバイスの USB 上のベンダ ID やデバイス ID 等の製品固有の識別子は、すでに信頼できないものであるため、これらを在宅型 CBT 試験システムのサーバー側で確認することで、不正なデバイスにより再生がなされていることを確認することは不可能である。

## (b) 仮想デバイスドライバを用いて画像データを入力する方法

PC の Web カメラと同様に見せかけた仮想デバイスドライバを用いて画像データを入力する手段が考えられる。

OS やプログラミングに関する基礎レイヤの知識があれば、仮想デバイスドライバを作成することができ、PC の Web カメラに見せかけて、すでに録画済みの映

像データファイルをそのまま再生したものを在宅型 CBT 試験システムのクライアントアプリに流入させることができる。

### (c) Web ブラウザまたはネイティブクライアントアプリを改造する方法

Web ブラウザまたはネイティブクライアントアプリを改造することにより、実際には録画済みの映像データを、あたかも Web カメラからのリアルタイム入力データとして見えるように、在宅型 CBT 試験システムのクライアントアプリに入力させることが可能である。

この問題の原因は、在宅型 CBT 試験システムの弱点として、クライアント側のコンピュータおよびその OS 環境が受験者の完全な所有・支配下にあることにある。この問題の本質については、後に詳しく解説する。

## (2) 受験者 PC からサーバーに送付される映像データのすり替え

仮に在宅型 CBT 試験システムのクライアントアプリが PC を介して Web カメラから受け取る映像データが本物であっても、これをサーバーに送付する際の映像データが不正受験者によって容易にすり替えられてしまうことが可能とすれば、在宅型 CBT 試験システムのサーバーはそのすり替えられた映像データのみを受信することになってしまう。

この映像のすり替えにも、大きく分けて、以下の 3 つの手法が存在する。

### (a) 通信データを変更する方法

在宅型 CBT 試験システムのクライアントアプリは、在宅型 CBT 試験システムのサーバープログラムと通信を確立し、リアルタイムで、クライアント側で録画された映像データを送付する。

この送付の際の通信経路上で、通信内容をうまく改ざんすれば、映像データをすり替えることが可能である。

## (b) クライアントアプリの挙動を変更する方法

在宅型 CBT 試験システムのクライアントアプリは、受験者の PC 上 (Web ブラウザで実装されている場合は、PC 上の Web ブラウザ内) で動作する。

このアプリのコードは、受験者の PC 上で動作しているため、不正受験者はそのコードまたはコードが参照するメモリを書き換えて、送付するデータをすり替えることが可能である。

## (c) クライアントアプリの挙動とほとんど同じ通信上の挙動を行なう別のアプリを作成する方法

これは、(b) と原理的には類似した手法であるが、既存の在宅型 CBT 試験システムの正規クライアントアプリそのものの挙動を改造するのではなく、その挙動とほとんど同じ通信上の挙動を示すアプリを新たに作成して、在宅型 CBT 試験システムのサーバーに対してデータを送付する手法である。

新たに実装した偽アプリは、正規アプリと同様の通信方式で在宅型 CBT 試験システムのサーバーと対話する。偽アプリの通信部分における再現度合いは、正規アプリと全く同一である必要はなく、在宅型 CBT 試験システムのサーバーが、これを正規のアプリからの通信であると認識して正常に処理を行なう程度の精度で足りる。

## 検証: SSL 中間者攻撃を用いた送付映像データのすり替え

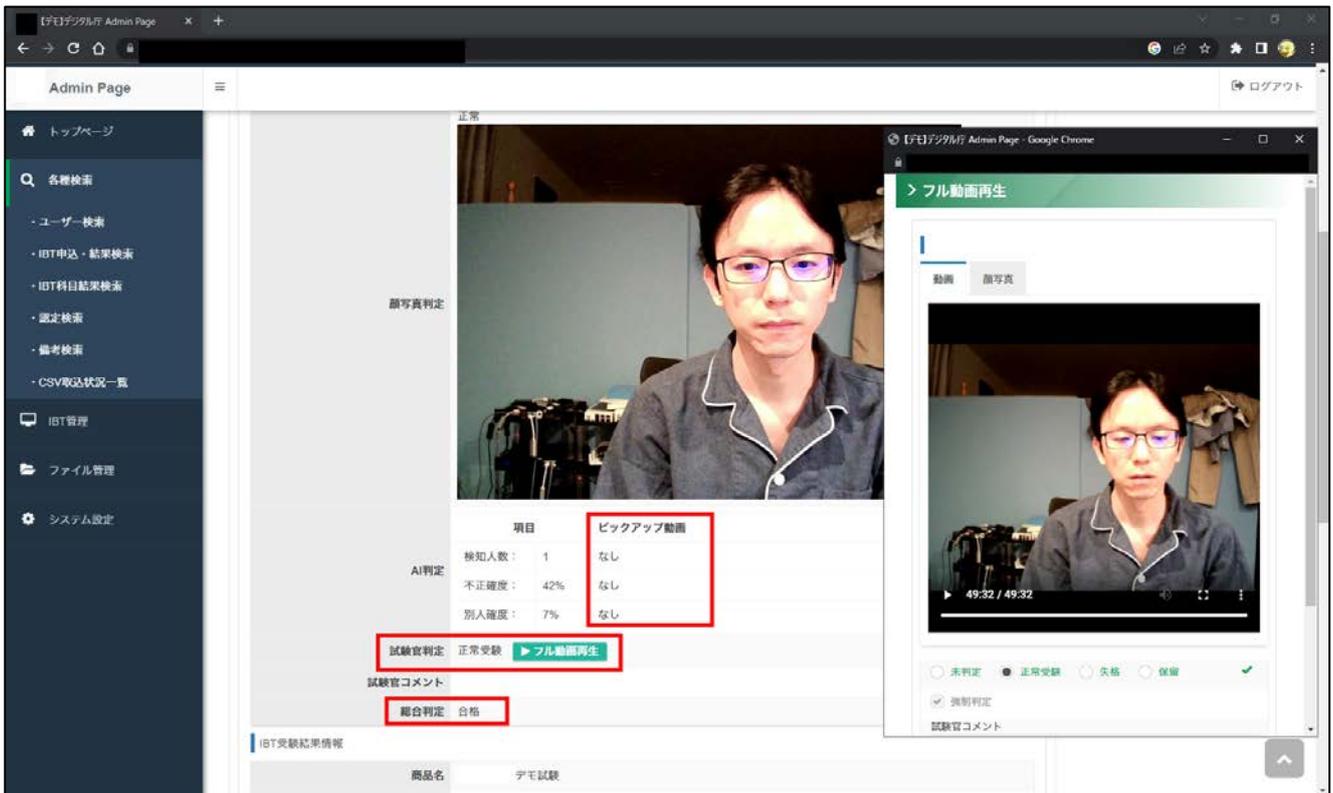
先に、SSL 中間者攻撃を用いて送付されるカメラ映像データの送付を妨害するという手法とその検証結果を解説した。

この SSL 中間者攻撃手法を、そのまま発展させ、さらに工夫して不正に用いると、単に特定の種類の試験のための通信データの送信を遮断 (妨害) するだけでなく、データが送信される際に、その内容を自由に書き換えることが可能である。先に述べた不正郵便局員のイメージで示すと、郵便局員が、封筒の封を開き、中の手紙の筆跡を真似て新たな手紙に書き換えて、また封筒に封入してそのまま宛先に送

付するという行為と同等である。

送付される映像データのすり替え行為については、誰でも、そのロジックのプログラムを書けば、自己の PC が送付するデータを、任意の映像データにすり替えることが可能である。すり替え先は、事前録画したデータでもよい。また、試験開始後の最初の数分間を録画した 10 秒間隔の映像データをランダムに結合して残りの試験時間分ループ送付したデータでもよい。すなわちアメリカのハリウッド映画のスパイ等が監視カメラの映像を守衛に対して誤魔化するために延々と正常時の同じカメラの映像をループするような攻撃を仕掛けることがあるが、それと同等のことが、SSL 中間者攻撃を用いれば可能である。

まず、不正受験者は、SSL 中間者攻撃を行なうことにより、通信プロトコルを分析し、本システムにおいて、Web ブラウザがどのようなデータ形式で試験サーバーにカメラ映像を送付しているかを明らかにする。分析結果として、本システムでは、10 秒に 1 回、過去 10 秒間のカメラ映像を HTTP POST と呼ばれるコマンドによって送付していることが分かる。HTTP POST におけるデータには、映像データ本体（これは H.264 という圧縮形式で構成されている）と、映像データの最終フレームをそのまま JPEG 形式に変換した画像、および当該映像が試験開始後何秒後から何秒後までのものであるかを示す数値が含まれる。この 3 つのデータの意味を理解した上で、送付されるデータを差し替えるプログラムを作成することは、さほど難しくくない。本評価では、実際にそのようなプログラムを 1 時間くらいで作成してみた。



SSL 中間者攻撃プログラムを改造し、CBT 試験サーバーに送付するカメラ映像をすり替えて、最初の 3 分間の映像を延々とループ再生した結果を残りの 47 分間にランダム再生し続け、その間に悠々とカンニングを実施する大変悪い受験者。試験サーバーや試験官は、映像すり替えに原理的に気付けないので、AI が判定しても、人間が判定しても、正常受験となってしまふ。

その結果は、図のとおり、不正効果てきめんである。試験時間は約 50 分であるが、試験開始後 3 分間だけ、受験者は、真剣にカメラのほうを注視して目線をほとんど動かさない姿勢を維持した。この最初の 3 分間分のデータが、10 秒 × 18 個の映像データ (180 秒分) としてサーバーに送付された。自作の SSL 中間者攻撃プログラムは、この 180 秒分のデータを覚えておき、181 秒目以降の 10 秒毎の映像データの送付時には、180 秒分のデータのうちランダムな 10 秒間の映像を選び出して、その選んだランダムデータと置換した上で送付をするようにした。試験サーバーは、データが書き換えられていることに気付かない。

この約 50 分間の試験中、3 分経過後に、評価者は参考書を読んだり、電話をかけたりして、多数の不正を実行した。しかし、その映像は送付されず、最初の 3 分間の真面目な受験風景だけが繰り返し送付された。その結果、AI は全体を正常受験とみなした。人間による検査者が録画データを確認しても、不審な点は見あたらない。

## 問題の本質

この問題の本質は、監視カメラにおける映像のキャプチャも、そのキャプチャされた映像データの送信も、すべて受験者側のシステムによって実施されていることに由来する。受験者は自らのシステムが送付するデータを自由に書き換えられる。この書き換えは、通常の Web ブラウザの操作のみではできないが、SSL 中間者攻撃等の一般的な手法を用いれば容易に可能である。

在宅型 CBT 試験システムの弱点は、クライアント側のコンピュータおよびその OS 環境が受験者の完全な所有・支配下にあることである。Web ブラウザを用いている在宅型 CBT 試験システムの場合は、Web ブラウザのオープンソースのコードを改造することにより、Web ブラウザそのものの挙動を自由自在に変更できてしまう。

実際には録画済みの映像データを、あたかも Web カメラからのリアルタイム入力データとして見えるように、在宅型 CBT 試験システムのクライアントアプ

りを実装している JavaScript と呼ばれるプログラムに入力させることが可能である。

JavaScript のプログラムは、Web ブラウザの手のひらの上で動いているので、Web ブラウザから供給される映像キャプチャ API から渡されるデータ配列が、本当に物理的に PC に取り付けられた Web カメラからリアルタイムで供給される映像であるか、それとも偽の録画映像であるか、識別が困難である。

仮に、Web ブラウザを用いたアプリではなく、ネイティブクライアントアプリであっても、難易度は若干高くなるものの、カメラ映像の差し替え等の不正行為は同様に可能である。ネイティブクライアントアプリは、Windows や macOS 等の OS の有する API を直接呼び出して Web カメラからのデータを受け取る。しかし、OS そのものや、さらには、コンピュータそのものは、最初から、受験者の完全な支配下にあり、不正受験者は、デバッガや逆アセンブラ等を用いて、その動作を完全にリアルタイムに制御可能である。ネイティブクライアントアプリそのものの挙動を書き換えることも可能である。これらの防止のために、ネイティブクライアントアプリに何らかの改造防止手法が搭載されていても、その改造防止手法を実装するプログラムコードも不正受験者が支配するコンピュータや OS の手のひらの上で動作するので、結局はそのコードも無効化され、改造され得る。

改造された場合は、その動作はもはや一切信頼できない。

## 解決策

この問題を解決するためには、技術的進歩が必要である。それでは、どのような手法が有効であろうか。

- (1) 受験者にスマートフォン等で特定の Web ページを開かせて、そこに次々に表示されるワンタイムパスワードのようなもの（これは時刻同期がなされている。）を、監視カメラの画面内に写り込ませる方法が考えられる。この手法により、映像の事前録画やループ再生といった映像差し替えの不

正行為を防止することが可能である。ただし、スマートフォンを試験中にカメラに写るようにうまく立て掛けてもらう必要があり、スタンド等の追加の出費を受験者に強いることになる。さらに、スマートフォンを持っていない受験者に対応することができない。

- (2) 画面に時々表示されるメッセージを時々読み上げてもらう方法が考えられる。この手法でも、録画データへの差し替えやループ再生を防止・検出することができる。ただし、受験者の集中が阻害されてしまう。試験中に、試験と無関係なことに頭脳を使うことを強いることは、不正防止の対策強化の観点では正しくても、受験者の不利益となってしまうことは明らかである。従来型の紙による試験では、そのような集中阻害がなかった。在宅型 CBT 試験を採用したいという試験実施主体の側の都合に合わせて、受験者に従来方式よりも集中阻害を強いることは、避けなければならないであろう。
- (3) 画面に色鮮やかな塗り潰し描画物体を大きな面積で時々表示し、その色が受験者の顔面に反射する際の顔面の色を AI によって確認するという手法が考えられる。これは、既存の eKYC (スマートフォン等を用いた本人確認手段) におけるカメラ映像の真正性を担保する手段としてすでに存在するようである。ただし、この手法では、受験者の顔面の色が変わる程度に、画面に色鮮やかな塗り潰し描画物体を大きな面積で時々表示する必要があり、(2) と同様に集中阻害が懸念される。
- (4) 最後に、前記の「撮影されたデータがサーバーに送付される際の送付経路上での通信妨害」で述べたようなスマートフォンを用いた第二カメラによる監視手法を受験者に要求する手法が考えられる。

## 4 タブまたは別ウィンドウを用いた不正情報採取

### (1) 概説

上記で述べてきた各不正手法は、不正防止のために撮影されている映像データのキャプチャや送付をうまく妨害するか、すり替えるといったものであった。すなわち、堂々と不正行為を行なうために、カメラ映像の側をごまかすというものである。しかし、これらの手法は、不正受験者の側にも、最低限のスキルが必要であった。

そこで、より怠惰な不正受験者は、前記で述べたスキルを身に付けることなく、より安易な方法で不正ができないかということに精力を傾けるに違いない。

まず、誰でも思い付く方法は、タブまたは別ウィンドウを用いた不正情報採取であろう。すなわち、試験中に分からない問題が生じたら、その問題について、Webブラウザ上のタブや別ウィンドウで、こっそりと Web 検索をしたり、参考書の PDF を開いたりして、不正に情報を採取するのである。

Web を用いた不正情報採取の例としては、従来型の Google 等の Web 全文検索の他に、2022 年 11 月頃に世界に突然登場して大変話題となっている ChatGPT 等の驚異的な汎用質問回答型 AI に質問文をペーストし、AI がその答えを教えてくれるまで数秒待つといった、AI 活用型の手法が想定される。また、LINE や Slack 等のメッセージングアプリを立ち上げておいて、友達等に不正に援助を求める手法も考えられる。

ただし、不正行為者がこっそりとこれらの Web 検索または AI を用いた質問を行なう際、またはメッセージングアプリを用いて他人に質問をする際には、キーボードでの入力に神経を集中させる必要がある。この場合、キーボードを操作する際に、AI にカメラの録画データを分析され、被疑点として検知されるリスクがある。特に、選択肢を選択する形式の試験の場合、キーボードを触れる必要がないはずなので、キーボードに触れているというだけで、不正行為であるとみなされるリスクがある。

そこで、不正受験者の視点では、カメラ録画映像上は自然な体勢を維持したまま、いかに、キーボードを触らずに、こっそりと開いた Web 検索キーワードボックスまたは AI 質問入力ボックス、チャットボックス等に、設問のキーワードを投入で

きるかが重要となる。不正受験者の視点としては、そのために一番簡単かつ重要で、是非とも実現したいと思うことは、在宅型 CBT 試験システムの画面上の文字をクリップボードにコピーする手法であろう。

## (2) 問題文の抽出とコピペによる他ウィンドウでの情報摂取

本システムのクライアント画面は、Web ブラウザを用いている。本システムのクライアント画面上は、質問の文字列は選択してコピーすることは一見できないように工夫されている。しかし、受験者は、Web ブラウザ上でキーボードの F11 キーを押す等して、Web ブラウザの開発者モードに入ることができる（試験開始時に F11 キーを 1 回だけ押せば、開発者モードとなり、試験時間中、常時 ON になっているので、キーボードに触れる必要があるのは 1 回だけである）。

ここで、試験画面中の HTML タグを辿っていけば、容易に試験の問題文や選択肢が、テキストデータとして、HTML タグ中に出現する。

よって、受験者は、マウスクリックだけで、試験中に、すべての問題文と選択肢をコピーして、別のウィンドウやタブ上の Web 検索や AI 質問のテキストボックスまたはチャットアプリにペーストし、情報を不正摂取することが可能である。



この受験者は、またしても悪さを行なっている。マウスのクリック操作だけで、うまく問題文のテキスト情報を抽出し、別のタブで開いた Google 検索や ChatGPT 等の AI 問答ソフトにより、答えを悠々と検索しているのである。目線が自然であれば、Web カメラの映像からではなかなか不正が分からない。

### (3) 問題文と選択肢を画像データにすれば若干抽出を難しくできる

このような不正行為は、本システムに若干の改良を施すだけで、ある程度は、実行を難しくすることができるであろう。

先のコピー & ペーストができてしまう問題の原因の本質は、サーバーからクライアントに対して文字データとして試験問題文および選択肢データが送付されてきているので、クライアント PC が受験者の所有でかつ完全な支配下にある以上、クライアントアプリが受信したテキストデータを受験者自らが取り出すことが可能であることに所在する。

したがって、受験者がいかなる状態でも問題文および選択肢をテキストデータで取り出すことが不可能な状態を維持すれば、前記のような安易なコピー & ペーストは不可能となる。

そのために有効な方法は、サーバー側でのテキストデータの画像へのレンダリングである。すなわち、サーバー側で、画像として問題文および選択肢を生成し、こ

れをクライアントに送付すれば、クライアント側で不正受験者がいかように操作しても、テキストデータがそもそも送付されてきていないので、テキストデータを取り出すことはできなくなる。

#### (4) 画像データであっても OCR 処理によるテキスト読み取りが可能である

ところが、仮にサーバー側でのテキストデータの画像へのレンダリング手法によって、テキストデータを取り出すことができなくても、不正受験者は、画面に表示された問題文や選択肢の文字列を、OCR (画像からの文字認識) 技術を用いて抽出することが可能である。

試験時間中に、画面のスクリーンショットを撮影してその静止画データを OCR プログラムにかけることができる。また、自作プログラム等を用いて現在マウスカーソルがある近くの文字列を自動的に OCR 処理することもできる。その結果を一度クリップボードに入れてから、Web 検索または AI 質問のテキストボックスに貼り付けすることができてしまう。さらに、そもそもメッセージングアプリを用いて友達等に質問をする場合は、画像で貼り付けても構わない。

不正行為のための、こういった試験中の問題文からのテキスト抽出に要する時間は、前記の HTML タグ等からテキストデータを抽出する方法とほとんど変わらない。あるいは、プログラミングで、便利な簡易ツールを作れば、より簡単なマウス操作だけですべて完結させることもできてしまう。よって、単にテキストデータを画像データに置換するというだけでは、OCR を用いた問題文・選択肢のテキストデータ化による安易な Web 検索等による情報摂取や、メッセージングアプリによる不正援助を他人に求めることを防止することはできなさそうである。

#### (5) もう少し工夫すればキャプチャ禁止 (OCR 禁止) の画像描画も可能である

不正防止の観点において、今われわれが是非とも実現したいことの本質は、Web ブラウザまたはネイティブアプリ上で表示される問題文および選択肢を、コピー

& ペーストであっても、または画面キャプチャによる OCR 処理であっても、試験時間中に簡単にテキストデータ化して別ウィンドウで検索されることを避けることであるといえる。

ところが、在宅型 CBT 試験システムの性質上、クライアント PC は受験者が完全に所有・支配しているため、受験者によって画面のキャプチャができてしまう以上は、不正受験者によって自動的にキャプチャまたは OCR をかけられることは防止できなさそうにも思える。

これを防止する技術的手法は、果たして存在するだろうか。それなりに効果がありそうなのは、著作権保護技術の活用である。Web ブラウザや DVD ビデオ再生アプリ等で映画を鑑賞したことがある方は、その映画の映像を、画面のスクリーンショット機能で撮影しようとしても、うまく撮影できなかった経験をお持ちかも知れない。PC の画面上に描画されたデータは、自由にキャプチャ (スクリーンショットの撮影) ができるが、映画の映像等の著作権保護対象部分だけは、キャプチャ機能がうまく働かないように、特殊な処理がなされているのである。具体的には、Web ブラウザや DVD ビデオ再生アプリは、著作権保護された映像データを画面上に表示する際、その領域を処理するウィンドウ (画面上の四角形の枠の領域) を OS に対してキャプチャ禁止指定ウィンドウとして指定している。在宅型 CBT 試験システムでも、この仕組みを利用して、試験問題や選択肢部分をキャプチャ禁止にすることは可能である。Web ブラウザを用いる試験システムの場合は、サーバーからクライアントに配信する試験問題や選択肢を、テキストデータにも、静止画データにもせずに、著作権保護された映像データの形式 (これは、EME: Encrypted Media Extensions と呼ばれている。) をリアルタイムで生成し、これを配信すればよい。そうすれば、Web ブラウザ上の HTML5 ビデオ領域として表示される試験問題は、不正受験者によって、容易にキャプチャされ OCR 処理の対象とされることはなくなる。

ネイティブアプリであれば、この処理は、より簡単である。著作権保護された映像データの形式などを使用しなくても、単に、OS のキャプチャ禁止領域指定の API を呼び出せば良い。たとえば Windows では、かなり具体的なことで恐縮で

あるが、一応紹介をすると、「SetWindowDisplayAffinity」という名前の API の WDA\_EXCLUDEFROMCAPTURE フラグを設定すればよい<sup>①</sup>。そうすれば、当該領域のキャプチャが禁止される。

ところが、実は、これらのキャプチャ禁止手法も万能ではなく、抜け道が存在する。

まず、これらのキャプチャ禁止手法は、所詮は、結局は受験者が完全な物理的支配を有しているコンピュータと、その中で動作する OS によって、プログラムコードとして実装されているものである。したがって、そのキャプチャ禁止の挙動は、PC の所有者自らがソフトウェア的に無効化することが可能である。

たとえば、前記の 「SetWindowDisplayAffinity」 という API の WDA\_EXCLUDEFROMCAPTURE フラグがアプリによって設定される点を変更し、フラグを設定しないように挙動を書き換えてしまう手法が利用可能である。

また、より簡単な抜け穴としては、VM (仮想マシン) 内で OS 環境を動作させるという手法がある。VM 内ではキャプチャができなくとも、VM の外側に描画される外側の画面上ではキャプチャが可能である。VM 内には手元の物理的な Web カメラの USB デバイスを内部的に接続しておけば、VM 内での試験受験も可能である。受験中に、VM の外側で調べ物をすれば良いのである。

その他にも、モニタで表示されている HDMI 信号を分岐した上で、著作権保護信号を外し (そのようなデバイスは、安価に販売されている)、これを別の PC でキャプチャしてリアルタイムで OCR をかけてキーワードベースで Web 検索または AI 質問を行なうというような不正手法も考えられる。

## (6) タブまたはウィンドウの切り替えの検出手法による対策とその限界

そもそも、タブまたはウィンドウの切り替えがなされたときに、どのようなタブまたはウィンドウがアクティブになったのかを、試験システムが知ることができれば、大抵の不正行為の兆候は検出できそうである。そこで、その方法が採り得るか

---

<sup>①</sup> <https://learn.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-setwindowdisplayaffinity>

どうか検討してみよう。

本システムは、在宅型 CBT のクライアント側のアプリを Web ブラウザで実装している。これは、JavaScript と呼ばれるプログラミング言語によってプログラミングされている。このプログラムに改良を追加すれば、Web ブラウザ上で別のタブが開かれ、当該別のタブがアクティブタブとなったり、OS 上の別のアプリがアクティブウィンドウとなったりした場合に、JavaScript のイベントを受信することができる。そのようなイベントを受信したら、JavaScript によって、その旨を CBT システムのサーバーに通報することは、技術的に可能であると考えられる。仮にそのようなアクティブ解除通知機能を実装したならば、試験実施主体は、ある受験者が受験中に他のタブをアクティブにしたり、他のアプリをアクティブにしたりしたことを知ることができる。

ところが、本システムは Web ブラウザ上でアプリとして動作している。Web ブラウザは、ユーザーのプライバシーを保護するため、あるアプリに対して、他のアプリの情報を完全に隔離している。したがって、他のタブやアプリがアクティブになったとしても、その他のタブやアプリの名称は、本システムのクライアント側アプリが知る手段が存在しない。

そこで、試験実施主体としては、他のタブまたはアプリがアクティブになった事実だけを知ることになる。それが一体何であったのかを受験者に対して事情聴取することは、可能である。

ただ、他のウィンドウがアクティブになったことだけを捉えて、直ちに不正行為がなされたと断定することはできない。受験者がうっかりクリックを間違えて他のタブやデスクトップをアクティブにしてしまったのかも知れない。

また、最近のコンピュータの OS では、さまざまなプリインストール・ソフトウェア (アンチウイルスソフトウェア等) が搭載されており、頻繁に自らをポップアップする。それにより、アクティブタブが解除されることもある。このような背景がある以上、受験者としては、詰問されても、「不正などしていない。」と否認ができてしまうので、単にアクティブ状態の解除の事実だけをもって、受験者を詰問することには、あまり意味がない。

## (7) 受験者側のデスクトップ画面の監視手法による対策とその限界

そこで、在宅型 CBT のクライアント側のアプリが Web ブラウザで実装されている場合、単にタブまたはウィンドウの切り替えの検出を行なうだけでなく、受験者のデスクトップ全域をキャプチャして監視してしまうという手法も有効である。

これは、近年の Web ブラウザにおいて Web 会議システムを実現するために、手元のパワーポイント等の画面を Web 会議に対して送付して画面共有することを主目的として Web ブラウザに用意された API である。

これを活用すれば、在宅型 CBT 試験システムにおける受験者のデスクトップ画面を記録・監視することも可能である。

実際に、本システムの開発元が提供している在宅型 CBT 試験システムの上位製品 (AI ではなく人力で監視を行なう種類のもの) においては、受験者のデスクトップ全体をキャプチャし、これを、カメラ映像の録画データと併せて録画して、CBT サーバーに送付・記録する機能が付随している。

しかしながら、仮に受験者の受験中のデスクトップ監視を行なったとしても、以下のような 3 つの限界がある。

### (a) キャプチャ禁止ウィンドウ領域の内容はキャプチャできないので、監視されない領域を作り出すことができる

スクリーンショットの撮影や OCR 等による問題文の簡単な抽出等の不正防止のために、OS の提供するキャプチャ禁止指定機能を指定したウィンドウを作成する手法 (API) があることは、前述した。

このキャプチャ禁止ウィンドウ領域は、キャプチャすることができないので、デスクトップ画面監視手法によってキャプチャされない。したがって、不正行為者は、デスクトップ画面が監視されている場合でも、決してキャプチャされることがない秘密のウィンドウを自らのデスクトップ上に作成し、その中で情報摂取等を行なう

ことが可能となる。これは、不正防止のためのキャプチャ禁止の仕組みが、逆に、受験者の画面を試験実施主体が監視しようとする局面において、不正な情報摂取ウインドウのキャプチャの妨げとなるという、興味深い検証である。不正を防止するための機能を用いて、不正が行えるということである。

#### **(b) VM の内部で受験をして VM の外側で不正を行なう場合、VM の外側は監視できない**

不正受験者が VM を作成し、VM の内側で在宅型 CBT のクライアント側のアプリを起動して、それを用いて受験を行なうとする。その表示画面は、VM の外側に伝達される。不正受験者は、VM の外側で各種の情報摂取等の不正行為を行ない、その結果知った正答を、VM の内側の画面に入力する。

この場合、受験者側のデスクトップ画面の監視手法でどれだけ監視をしたとしても、それは結局 VM の内側に終始するものであり、VM の外側に表示されている不正画面 (Web 検索や AI を用いた情報摂取、メッセージングアプリを用いた友人への質問等) の存在を知ることは、決してできない。

#### **(c) コンピュータ上で動作するアプリの挙動はコンピュータの所有者が自由自在に変更可能である**

受験者側のデスクトップ画面の監視手法は、プログラムで実装されている。そして、そのプログラムは、不正受験者が完全な支配を有する受験者側の PC 上で動作しており、任意に挙動の変更が可能である。したがって、前述した Web カメラの映像差し替えや送付時の通信の差し替えが可能である。

### **(8) 問題の本質と限界**

これらの問題は、在宅型 CBT 試験システムの本質から生じる技術的制約の限界を示している。従来の集合型試験であれば、紙ベースのものであっても、CBT であっても、物理的な装置や施設は、試験実施主体または試験代行業者のほぼ完全な

支配下にあった。不正受験者は、その間隙を突いて不正行為を行なう必要があった。

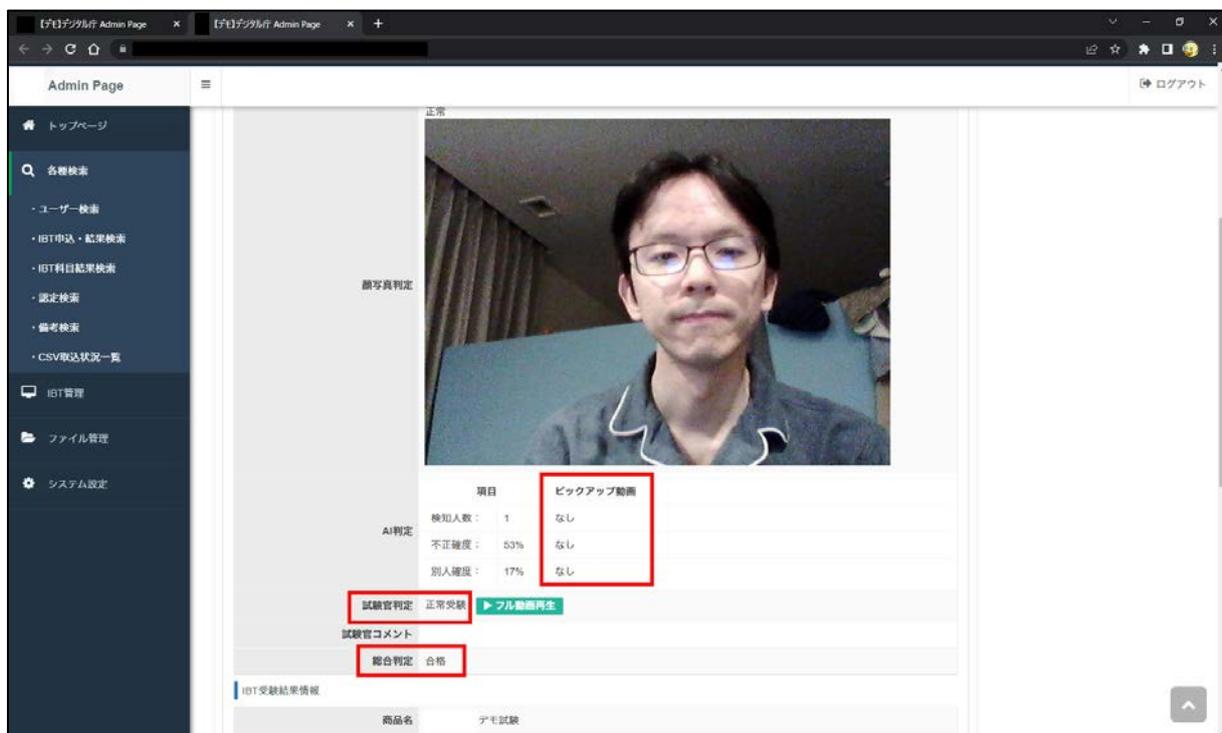
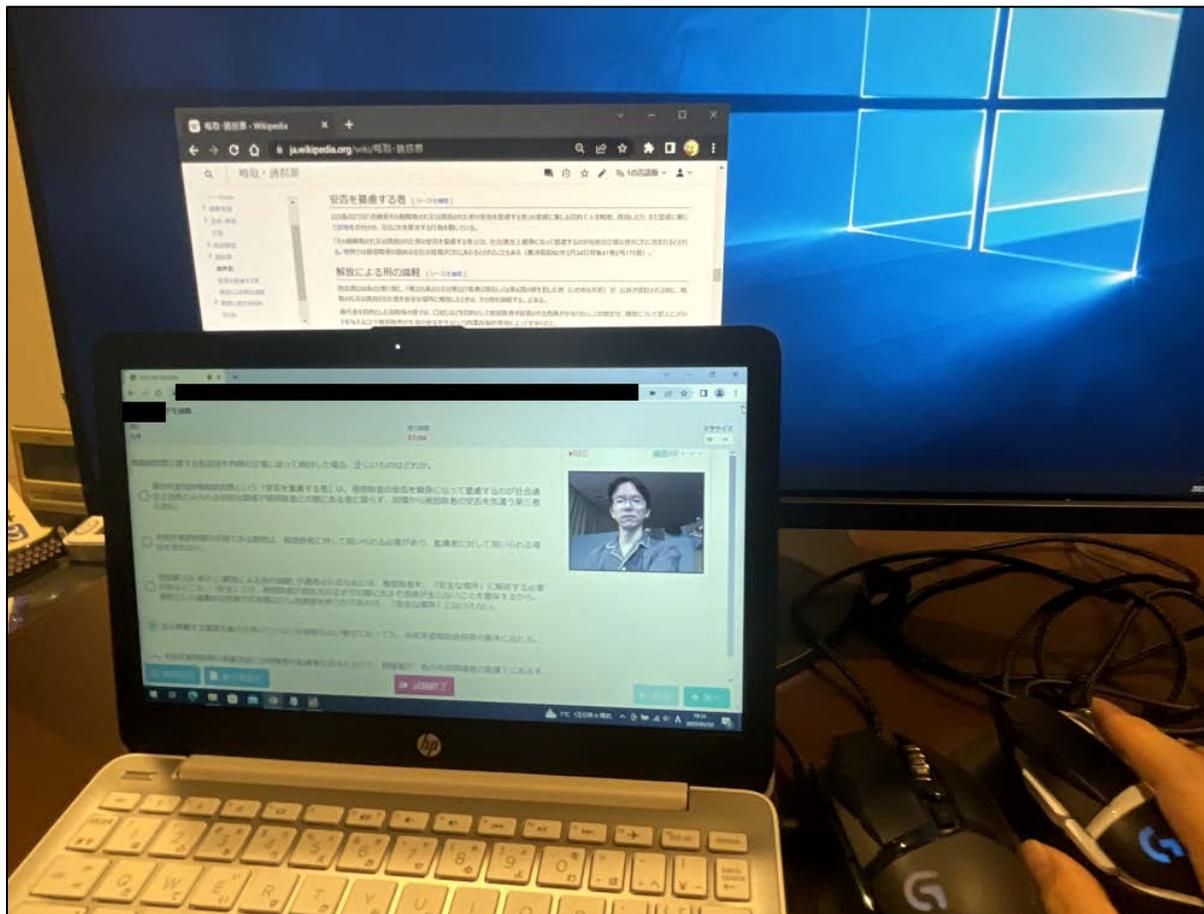
ところが、在宅型 CBT 試験システムにおいては、AI を使用するか否かにかかわらず、監視システムや不正防止のシステムの主要な部位と情報の経路が、不正受験者の手中にある各種装置の内部に存在する。これらの自宅側装置は、PC、OS、Web ブラウザ、カメラ、モニタ、マウス、キーボードといった汎用部品やソフトウェアのみで構成されており、内部の改造や特殊な接続方法等を防止することは、原理的に不可能である。そこで、原理的に不正行為の防止・検出が不可能であることをいったん認めた上で、検出されない不正行為を実行するために不正受験者側に要求されるスキルのレベルをできるだけ高める方法が重要であるといえることができる。

## 5 重なり合った 2 枚のモニタによる不正情報摂取

不正受験者によって実行可能な、極めて安易な不正情報摂取方法は、在宅型 CBT 試験システムによる試験を受ける PC のモニタのすぐ裏面に、別の 1 枚のモニタを用意しておき、その別の 1 枚のモニタの中に、参考書 PDF や Web 百科事典等のウィンドウを表示しておく手法である。

この不正情報摂取用のモニタは、別の PC でも良いし、同一の PC をマルチモニタで利用してもよい。別の PC を用いる場合は、手元に情報摂取用のマウスと、受験用のマウスの、合計 2 つのマウスを用意しておく必要があることに注意する。

この手法により、不正受験者は、ほとんど視線を上下左右に動かすことなく、裏側のモニタ内の参考書 PDF や Web 百科事典等のモニタ内の情報をマウスによって必要に応じて検索し、結果を用いて答案を作成することができる。



この受験生は、懲りずにまた悪さを行なっている。受験用コンピュータのモニタとほとんど同じ焦点距離上に、別のモニタを重ね、そこでWikipedia等を読んで情報を不正摂取している。

これにより、目線は自然となり、AIも人間も、不正を検出することができない。コツは、2枚のモニタを重ね合わせること、2個のマウスを手元に置き、目線を自然にすることである。

## 検証

実際にこの手法を実験してみたところ、かなり簡単に、AI 検知を回避しつつ、不正情報摂取を行なうことができた。

本システムで撮影される Web カメラの視点からは、視線はかなり安定して試験画面だけを注視しているように見えるのだが、実際には、その画面のすぐ裏にある不正な情報摂取ウィンドウからの情報を得て、試験問題に不正に回答しているのである。本システムの AI は、これを見抜くことはできず、自動判定で「正常受験」という結果が得られてしまった。

## 問題の本質

本手法は簡単に実行でき、発覚する危険もかなり低い。

本システムその他、他の在宅型 CBT 試験システムにおいても、試験開始前などに、試験代行業者のオペレータが受験者に対して Web カメラを 360 度周囲を回転させるように指示し、自室に他に人がいないか、不正な物 (参考書等) が置かれていないか等を一瞥して確認するフローとしている場合も多い。

しかし、本不正手法では、単にモニタが 1 枚写るだけであるため、不正な物としてなかなか認識されない。

さらに万全な不正受験者 (ノート PC を用いているものとする) は、そのような確認フェーズのために、モニタには最初には実際の受験画面 (CBT システムのクライアント画面) を表示しておき、単に「これは、本 PC に接続され、本受験画面が表示されているモニタである」と説明し、実際にその様子をカメラで映すと良い。そうすれば、事前の検証は難無く通過できる。

その後、試験が始まれば、その不正受験者は、試験そのものはノート PC の内蔵モニタで行ない、背後モニタで不正情報摂取に勤しむことになるのである。

このような方法の他にも、様々な事前検証をうまく通過する方法は、容易に思い付くであろう。

## (2) PC 操作代行型替え玉受験

在宅型 CBT 試験システムにおいて替え玉受験を行なう場合、受験を行なう自室に替え玉を予め呼び寄せておけば、前記のようなカメラ撮影妨害や送信妨害、または送信映像のすり替えを開始した後に、悠々と、替え玉受験が可能となる。しかしながら、これらの手法は、前記のようないくつかのツールを用いる必要があり、一定の不正受験スキルが必要であった。

これとは別に、より簡単な方法として、在宅型 CBT 試験システムにおいては、リモート型替え玉受験が成立し得る。リモート型替え玉受験とは、試験が正常に開始した後に、受験者本人の PC に表示される画面の内容を替え玉にリモート送付し、替え玉が受験 PC をリモートから遠隔操作して、答案の入力 (選択肢の選択、自由入力テキストの入力) を代行するという手法である。

この手法の驚異的な点は、一切の映像のすり替えが不要であるという点にある。受験者本人は、自分の PC の前に単に座していればよい。なお、リモートの替え玉が、実際の回答を選択・入力する操作を行なっている間も、受験者本人はカメラに写る必要があるため、ある程度真剣に問題文を読んで答えを練っている様子が一応撮影される程度に演技 (というよりも、画面を注視するという我慢) をすることは、必要である。

リモート替え玉においては、受験者本人の PC と、替え玉との間の距離は、近くても離れていてもよい。

それぞれの場合に実行可能な不正手法を以下で述べる。

### (a) 近距離替え玉受験

近距離のほうが、不正替え玉受験の実現は簡単である。

たとえば、本人と替え玉が友人関係である場合等は、替え玉が本人の自宅に来訪して、近距離型の替え玉受験を行なえば良い。その場合、以下のように、自宅には、2 つの部屋が必要になる。

まず、第一の部屋には、本人の試験用 PC があり、本人が座っている。すぐ隣の第二の部屋に替え玉が座っていて、その替え玉が、本人の試験用 PC を遠隔操作する。これはかなり簡単で、2 つの部屋の間 (自宅であれば、数メートル ~ 10メートル程度であろう。) に HDMI ケーブルと USB ケーブルを 1 本ずつ敷設すれば良い。

まず、表示系について述べる。これは、替え玉の部屋にもモニタを置き、本人の PC のディスプレイ信号を HDMI で複製・分岐して (分岐する小型の装置が市販されている。)、本人と替え玉の両方の部屋で同じ画面が見えるようにする。

次に、入力系について述べる。これは、替え玉の部屋にはキーボードとマウスを置き、これは USB ハブで 1 本にまとめた状態で、少し長い USB ケーブルを用いて、本人の PC と直接接続するのである (なお、USB ハブで 1 本にまとめることは必須ではなく、2 本の長い USB 延長ケーブルを用意してもよい。)。このような原始的な方法で、隣接替え玉受験が可能になる。

これらのケーブル類や分岐装置は、極めて一般的な外観をしており、また、分岐装置等は PC 裏面等の延長コードやネットワーク機器等 (ルータ等) が一箇所に固まっている部分に格納することもできるので、仮に試験開始前にカメラを 360 度ぐるりと回転させて室内を検査するプロセスがあっても、それによって不正が検出される可能性はほとんど存在しない。

そして、これらのケーブル類により表示画面が隣接替え玉のために分岐され、また、隣接替え玉によるキーボードやマウス入力により PC が操作される状態になっていることは、本システムの CBT クライアントアプリからは、検出不能である。

## (b) 遠距離替え玉受験

前記 (a) の方法は、直接知らない人に替え玉を囑託したり、遠距離の友人や親族等に替え玉を依頼したりする場合には、利用できない。

そこで、このような場合は、代わりに、本人の PC を替え玉がインターネット経由でリモート操作する方法が利用できる。

その手法では、インターネット経由で PC 画面をそのまま遠隔操作できるテレワークツール等が利用されると考えられる。PC の遠隔操作ツールには 2 種類あり、遠隔操作中には手元の PC の画面がロックされてしまう方式と、手元の画面が表示されたままの方式とが存在する。遠距離替え玉事件に適した遠隔操作ツールは、後者のものである。たとえば、無償で利用できる「NTT 東日本 - IPA シン・テレワークシステム」<sup>①</sup> の「ユーザーモード」を利用すれば、後者のような遠隔操作が可能となる。

本不正手法も、基本的な原理は、(a) 近距離替え玉受験の手法と同様である。ただし、(a) の手法は、ハードウェア的に表示画面を分岐し、また、替え玉からの入力を受験者本人の PC に伝達していたが、本手法は、これをソフトウェア的にインターネット経由で実現しているという点が異なる。

これは、不正受験者の視点からみて、若干リスクが異なる。(a) の手法は、ハードウェア分岐であるので、CBT システムの視点からみても、ソフトウェア的に別室への分岐や別室からのリモート入力を検出する方法は存在しない。他方で、本手法では、仮に在宅型 CBT 試験システムのクライアントアプリが様々な OS 上の技巧的な手法 (たとえば、動作中のプロセス一覧を列挙する、通信中の相手一覧を列挙する等) を駆使すれば、リモート管理ツールを起動している事実を検出することが、もしかすると、可能な場合があるのではないか、という心理的不安が生じる。ただし、本システムは Web アプリ型であり、Web ブラウザのプライバシー保護機能により、そのような動作中の他アプリの一覧や他の通信の状況を知る方法がないから、おそらく、結局検出されないであろう。仮に CBT クライアントアプリがネイティブアプリであれば、これらを検出することは、OS に対するプロセス一覧列挙命令 (API) を用いれば、可能である。

なお、不正受験者がこのようなネイティブアプリによる監視から確実に解放されることを欲する場合、(a) の亜種として、(a) のハードウェア型画面分岐の結果を、受験者本人の自宅からインターネット経由で遠方に伝送し、遠方からのキーボード

---

<sup>①</sup> <https://telework.cyber.ipa.go.jp/>

またはマウス操作入力を、同様にインターネット経由で受験者本人の自宅に伝送して受験者 PC にハードウェア的に入力する手法も考えられる。

この場合、この手の込んだ仕組みはハードウェア的に実装されていることから、ソフトウェアによる検出は、(a) と同一に、極めて困難となる。そのため、不正受験者としては、かなり安全に替え玉受験を他人に依頼することができる。

## 6 その他の替え玉的受験の手法

在宅型 CBT 試験システムにおいて、現実的に容易に想定される替え玉的受験の方式を色々と考えた結果は、次のとおりである。

### (1) 画面内容の支援者への伝送と、正答の本人への秘かな伝達

前記の「PC 操作代行型替え玉受験」は、画面内容を替え玉受験者が読み、問題を解いて、その結果を替え玉受験者が直接受験者本人の PC に入力・回答していた。この方法の亜種として、画面内容は替え玉受験者に伝達されるものの、替え玉受験者からの正答の伝達は別の経路で行なわれ、不正受験者本人が正答を画面入力するという手法が想定される。

この手法は、実際に本人が答えを入力するので、「PC 操作代行型替え玉受験」において発生するリスク（監視カメラをごまかすための手元動作や神経の集中や我慢等の必要性）が不要となる。

画面内容を替え玉受験者に伝達する方法は、もともと、「PC 操作代行型替え玉受験」で述べた (a) ハードウェア的方法、または (b) ソフトウェア的方法のいずれか方法で可能であった。

新たに問題となるのは、替え玉受験者が不正受験者本人に秘かに正解を伝達する方法である。これには、以下のような方法が考えられる。

### (1) 音や振動などにより伝達を受ける方法

音や振動などによる正答の不正伝達受領方法は、従来型の紙ベースの集合試験で

も存在した平凡な不正手法であり、新規性のあるものではない。

しかしながら、在宅で受験を行なう以上、たとえば別室等から、または携帯電話等から、受験者本人に対して音や振動などによる不正伝達がなされていることを検出することは、かなり困難であろう。

仮に在宅型 CBT 試験システムが、監視カメラのほか、マイクの音を録音していたとしても、それで判別不能な振動（音波としては検出が困難な振動等）を受信する装置を不正受験者本人が足元などに取り付けていた場合、これを検出することはほとんど不可能である。

## (2) 受験 PC と同一の画面上で別ウィンドウ上で伝達を受ける方法

受験者本人の PC 上の別ウィンドウやブラウザ上の別タブ上で、メッセージングアプリやその他の任意のアプリで正答が流れてくるという手法である。

ここで、PC 上の画面が完全に監視されてしまうタイプの在宅型 CBT 試験システムのクライアントアプリが動作している場合は、そのままでは、このような不正が検知・記録されてしまう。

そこで、前述したように、著作権保護機能のために用意されている OS のキャプチャ禁止対象の特別フラグを指定したウィンドウ領域を作ることにより、当該特殊ウィンドウを、PC 上の画面が完全に監視されてしまうタイプのアプリによる監視から免れることが可能な場合がある。

ただし、この手法が効果的に機能しなかった場合等、不慮の事態が発生したならば、不正行為が発覚するリスクがある。

## (3) 受験 PC と同一の画面上で HDMI 映像合成により伝達を受ける方法

そこで、もう少し手の込んだ手法として、受験用 PC が接続されているモニタに映像が入る前に、HDMI のリアルタイム編集装置を間に挿入し、特定の大きさで特定の文字または画像をモニタに送り込む方法が存在する。

これは、受験用 PC からの出力 HDMI 信号のさらに先で、ハードウェア的に

画面上の一部分に情報を埋め込むので、受験者 PC 上でいかなる監視ソフトウェアが動作していたとしても、その監視ソフトウェアによって、このような情報の画面への埋め込みが検出されてしまうリスクは存在せず、絶対安全に不正行為を実施することができる。

#### (4) 受験 PC と物理的に重なり合った他の画面上で伝達を受ける方法

上記の (3) のさらなる亜種として、受験 PC のモニタと物理的に重なり合った他のモニタ上で不正な情報伝達を受ける方法がある。

受験 PC のモニタと物理的に重なり合った他のモニタが存在する場合、これを注視する際の目線の動きは、受験 PC のモニタを注視する場合とほとんど同じになり、不正な目線として検出されないことは、前に述べたとおりである。

これを利用すれば、重なり合った背後のモニタを用いて、替え玉受験者からの不正情報摂取を受けることが可能である。

#### (2) 替え玉受験者もまた正規の受験者であるケース

上記で述べた各種手法は、替え玉受験者について、正規の受験者ではなく、正規の受験者本人から問題文および選択肢の情報を画面分岐等の手法により伝達され、本人に代わって問題を解くという存在を想定している。

しかしながら、替え玉受験者自らも同じ在宅型 CBT 試験に出願し、同一時刻に試験を受けることも可能である (本人と不正支援者とは交換されないことになるので、「替え玉」と呼称するのはおかしい。そこで、以下では、「不正支援受験者」と表現することにする。 )。

この場合、受験者本人の画面または表示される試験問題の内容を不正支援受験者に複製・転送する必要はなくなり、不正支援受験者は、単に問題を解けば良いことになる。そして、不正支援受験者が解いた結果を、前記のような何らかの方法 (画面、音、振動等) で、受験者本人に伝達すればよい。

この手法は、もちろん、従来の集合型の紙ベースの試験会場でも可能であった。

そこで、従来の試験では、試験実施主体は受験者たちをランダムに並び替えて、受験者本人とその本人を支援する意図を有して試験を出願している不正支援受験者が近くの座席に配置されないように工夫を講じていた。また、遠隔の無線を用いた不正情報伝達は、イヤホンに付けている受験者がいれば不正行為とみなす方法で排除できた。

物理的集合試験の会場では、昔から、このような対策がなされていることが周知の事実であったので、そもそもこの方式で不正を実施しようとする者はほとんど出現しなかったのである。

ところが、在宅型 CBT 試験システムでは、何ら対策をしない限り、これらの不正行為が極めて容易に完遂できるようになる。受験者が宅内等自由な場所で受験することができることから、試験実施主体は、その受験者周辺環境から不正につながる余地がある物を排除したり、物理的に不正支援者を近接させることを防止したりすることが極めて困難となるのである。

この手法に対する不正防止対策方法としては、比較的簡単であり、出題される問題文や選択肢を受験者ごとにランダムに並び替えればよい。これは、多くの在宅型 CBT 試験システムで利用可能である。

### (3) 問題の本質

上記のさまざまな手法でみたように、替え玉受験者は、問題を表示した画面の分岐・複製を受けることにより、受験者本人と全く同じ状態で、問題を解いてしまえる。問題を表示した画面の分岐・複製が、受験者の宅内で物理的に可能である以上、これを禁止する手立てはない。

そして、替え玉受験者が問題を解いてしまえば、それを不正受験者本人に伝達する手段は色々なものがあり、そのような不正情報伝達を系統的に防止することは、在宅型 CBT 試験システムの特長上、ほとんど困難であるといつてよい。

この問題は、在宅型 CBT 試験システムを用いる場合、試験実施主体による五感による不正発見のための巡回・監視活動が不可能であることから、監視を受験者の宅内に受験者が自ら所有し設置する Web カメラの撮影データに頼らざるを得な

いという状況と、この監視手段のハードウェア的な技術上の制約によって生じているのである。

## 7 全問題文閲覧後のブラウザ異常終了の偽装と試験再開

### (1) 概説

在宅型 CBT 試験システムでは、Web ブラウザを用いて試験ページに接続し、試験を開始する。試験開始で制限時間のカウントダウンが開始される。一度試験を開始すると、受験者は、ページを次々にめくっていき、すべての問題を目にすることができる。試験中は試験者の全容が Web カメラにより撮影、記録され、サーバーに送信されて、試験実施主体または代行業者によって、AI または人力でチェックされる。

ところで、試験開始後に、PC の OS や Web ブラウザが異常終了したり、通信回線が切れたりすると、試験は途中で中断する。受験者は再起動後に再度試験ページに接続すると、試験が再開される。この間の動きは、当然、カメラにより一切撮影されていない。

したがって、受験者は、任意の方法で、分からなかった試験問題の正答を調べることができる。調べたい事柄を記憶していても良いし、本文書で前述した各種の方法で試験問題をメモしておいてもよい。試験中断中に悠々と調べ物を行なった不正受験者は、その後試験が再開したら、何食わぬ顔で、先ほど分からなかった問題の答えを入力する。この方法により、不正受験者は、満点を取ることができてしまう。

### (2) 問題の本質

この問題の本質は、CBT システムにおいては、従来型の紙試験と比較して、試験開始後に問題文および答案用紙の代替として機能する媒体である PC の OS や Web ブラウザが、突然異常で終了してしまう可能性を事前に排除することができないという点に帰着する。

すなわち、紙や鉛筆を用いる従来型の試験では、試験中に突然問題用紙や答案用

紙が消滅するという可能性は、物理的に、まず存在しない。せいぜい問題用紙を床に落としてしまって、目前から問題文がなくなってしまう程度である。この場合は、床に落ちてしまった問題用紙を、自ら拾い上げるか、または試験監督に拾ってもらえば、問題は短期間 (数秒 ~ 十数秒) でたちまち解決する。

ところが、CBT システムでは、紙よりもかなり複雑・高度・不安定な媒体であるコンピュータを使用している。コンピュータそのものは不安定で、メモリ上の素子の 1 ビットでも反転すると、動作がおかしくなるのである。

コンピュータの上で動作する OS はさらに不安定で、バグが満載である。OS の内部で動作するデバイスドライバ、OS の上で動作する API ライブラリ、Web ブラウザプログラム、Web ブラウザ内の JavaScript 実行エンジン、HTML レンダリングエンジン、Web ブラウザと並行して全く対等に動作する他のアプリケーション (アンチウイルスソフトウェア等) といった、有機生命体によく似た大量のプログラムコードが、1 つのコンピュータの中で共存している。

これら受験者 PC の内側のソフトウェア部品には、無数の不具合や相性問題が存在する。さらに、受験者 PC と CBT サーバーとの間の通信を実現するためのインターネットや、インターネットに接続するための経路上にも、本文書で前述したように、無数のソフトウェア的またはハードウェア的な障害点が存在する。

これらのうち 1 点でも動作がおかしくなると、たちまち Web ブラウザ経由の CBT 試験は中断してしまう。そして、そのような中断のほとんどの要因は、受験者にとって全く責任がない原因で発生する。そもそも原因が不明となる可能性のほうが、原因が明瞭となる可能性よりも高いであろう。

そのため、CBT システムでは、一度試験画面が異常中断してしまった場合のために、試験を再開可能とすることが必須となる。その際に、Web ブラウザや PC が異常終了してしまった原因が、自然発生的なものであるのか、それとも、不正受験者が不正のために意図的に異常終了させたのか、いずれかであるかを確実に区別する方法は存在しない。不正受験者が不正のために意図的に異常終了させたとしても、試験実施主体は、その意図的な異常終了の事実の証拠を得ることができない。よって、試験実施主体としては、受験者に責任のない何らかの不具合で画面が終了

し、その後再接続され、再開がなされたとみなすしかないのである。

### (3) トイレ退席を装った不正情報摂取

このような、CBT 試験途中での異常中断による情報の不正摂取と類似の不正手法として、かなり原始的ではあるが、CBT 試験途中において問題文を読んだ後に、トイレに行きたくなったとして退出し、Web カメラの視界外でスマートフォンや PC で正解を調べ、トイレから戻ってきて悠々と受験を続行するという不正手法が考えられる。

トイレで離席する際は、Web カメラの監視映像からは離席の様子が鮮明に記録されるので、その後の AI または人力によるカメラ映像の分析結果で、離席している様子が記録される。しかし、受験者にその離席の事情を聴取しても、「トイレ退席であった。」と主張されてしまうと、試験実施主体としては、もはやそれ以上真実を追求する手段がない。短時間の試験であれば、トイレ退席等を一切認めないすることも可能であるが、60 分程度かそれ以上に及ぶ可能性がある重要な試験においては、トイレ退席を認めないことは、人権問題となるから、それは困難であろう。

このトイレ問題の本質について、従来型集合型試験との対比で考察してみよう。集合型試験においても、もちろん、受験者はトイレのためにいつでも離席する可能性がある。この際、離席の際に受験者が不正情報摂取に利用可能なデバイス (スマートフォン等) を所持していないかどうか、試験実施主体が外形的に一応確認可能である (もともと、試験開始時に、これらのデバイスはポケットに入れずに鞆の中に収納するべき旨の指示がなされる。)。そして、試験会場となる教室と、最寄りのトイレとの間の廊下は一続きになっており、廊下にも大抵試験実施主体側の職員や代行業者の被用者が 1 人くらい立っていて、最寄りのトイレへ行くように促される。この状態で、あえて遠方の他の階や建物のトイレへ行こうとすれば、試験を辞退する意思あり (失格) とみなされるであろう。また、最寄りのトイレへ向かう場合であっても、スマートフォン等の不正通信デバイスは、それなりの容積と重量があるので、これがポケット内に入った状態で歩行すると、監視者から結構容易に

判別され得る。少しでも疑わしければ、監視者によって臨時検査を要求されるであろう。検査を不当に拒否すると、失格とみなされるであろう。そのような発覚リスクがあるので、不正受験者はスマートフォン等をポケットに入れた状態で試験を受け、その途中でトイレへ行き、スマートフォンで不正情報撮取をすることは、大変困難である。

そこで、トイレの戸室内等に予めスマートフォンや参考書等を隠しておく手法が考えられる。しかし、トイレ内も試験実施主体による全面的支配が及んでいる。事前にトイレの個室は点検され、隠しデバイス等が設置されていないことが注意深く確認されている。このように、集合型試験においては、試験会場のトイレ設備を含めて、試験実施主体の責任と権限で、受験者に対して物理的な支配を及ぼすことができてきたのである。何と素晴らしいことであろうか。

ところが、在宅型 CBT 試験では、この試験実施主体の責任と権限で見張ることができるのは、Web カメラが写っている範囲に限定されてしまう。その視界外で何が起きているのかは、もはや、物理的に認知不可能である。

これが、現在の在宅型 CBT 試験における現在の技術水準上の限界である。われわれは、これから、在宅型 CBT 試験をより公平・公正なものにするために、技術を進歩させ、このような技術上の限界を突破するさまざまな手法を、試行錯誤により考案しなければならない。

# 第3章 各論Ⅱ—CBT 試験システムの公平性（完全性・機密性・可用性）の検討

前章では、在宅型 CBT システムの不正防止機能に関する検証を行なった。ここからは、本システムについて、CBT 試験システムにおいて試験の公平性・公正性を実現するために重要な、完全性・機密性・可用性に関する検討を行なう。完全性及び機密性については、在宅型 CBT 試験システムおよび集合型 CBT 試験システムの両方に妥当する事柄を検討し、可用性については、インターネットを用いる在宅型 CBT 試験システムに限定した事柄を検討する。

## 第1節 可用性に対するリスク（在宅型）

### 1 在宅型 CBT 試験システムにおける可用性とは

在宅型 CBT 試験システムにおける可用性とは、受験者が試験の開始前に試験にアクセスすることができる状態を維持し、試験の開始後は、試験の終了時に受験者から送付される答案内容を確実に試験サーバーが受信し終えるまでサーバーを稼働させ続け、また、受験者の PC と試験サーバーとの間の通信が途切れないように維持する能力を指す。

受験者の PC と試験サーバーとの間の通信経路の可用性と、試験サーバーそのものの可用性の 2 つの可用性の問題が存在する。

試験時間中に両方の可用性が維持されて初めて、試験を公平・公正に完了することができる。

### 2 本システムにおける通信経路の可用性の検討

#### (1) 概説

本システム（本文書でサンプル的に評価した対象製品）に代表される、すべての在宅型 CBT 試験システムは、各受験者の PC と試験サーバーとの間で、インタ

一ネットを介して、それぞれ、1組ずつの通信が成立する。たとえば、受験者が100名いれば、100組の通信が成立する。この場合、在宅型 CBT 試験を用いる試験実施主体は、100名の受験者それぞれに対して、100組の通信経路の可用性を維持する責任が発生することになる。

在宅型 CBT 試験システムの通信はインターネットを経由するが、インターネットというものは何か固定的な実体がある訳でなく、いわば抽象的な存在に近いダイナミックなネットワークであり、極めて不安定なものである。インターネットは、多数の互いに契約関係のない（従って、可用性を互いに維持し合う責任のない）ネットワーク運営者同士が、領主間の同盟のように、数珠つなぎになって、広い大陸を覆うようなイメージのネットワークである。1つの単一の具体的なインターネットおよびその運営主体が存在する訳ではない。このようなインターネットの仕組みと、随時の通信障害の発生の可能性については、すでに、第1章第2節4(1)で詳しく述べた。

そうすると、試験開始前のアクセスの段階と、試験開始後の試験中の段階のいずれの時点においても、インターネットの様々な部分で、試験実施主体の責任でも受験者の責任にもよらない通信不具合が発生し、受験者が試験サーバーとの間で正常に通信ができない状態が発生し得ることになる。

また、インターネットは多数の独立能力を有する運営主体が自律的・連合的に連結したネットワークであるので、全体が麻痺する不具合が発生する頻度はかなり低く、他方で、個別的・局所的な不具合は極めて頻繁に発生するという特徴を有する。

すなわち、試験実施前または実施最中において100名の受験者が存在するとして、インターネット上のある1点で不具合が生じたときは、そのうち例えば30名の受験者のみ通信が突然異常となり、残り70名の受験者は通信が正常なままである、というような事象が発生し得る。このようなインターネットの通信上の不具合が発生する原因は、様々なものがある。

たとえば、インターネット上において、第1章第2節4(1)で述べた BGP (Border Gateway Protocol) という仕組みで数珠つなぎになっている AS (インターネット上の独立ネットワーク運営主体) のうち一部の BGP を司るルーティン

グソフトウェアと呼ばれるプログラムに不具合があった場合や、いずれかの AS の BGP 運営者が操作ミスで誤った設定をインターネットに流してしまった場合などは、あたかも生体組織の特定の部位が損傷を受けた時のように、局所的な不具合や麻痺が発生し、その不具合が解消されるまで何時間または 1 日程度かかる可能性がある。

インターネットは全世界的に形成されているので、全世界の AS のうち 1 箇所の BGP ルータのソフトウェアのプログラムの不具合、または 1 人の運営者の操作ミスによって、このような局所的麻痺が日常的に発生するのである。

試験は、受験者の人生がかかっている重要な社会的行事である。そこで、試験実施主体には、たとえインターネット上の局所的な不具合が発生しても、このような不公平が発生しないように、事前に措置・対策を講じる責任がある。

したがって、試験実施主体（または外注業者）が在宅型 CBT 試験システムの試験サーバーを運営する場合においては、インターネット上の局所的な不具合が発生して、100 名の受験者の一部が通信できなくなった場合に備えて、当該局所的な不具合の箇所を通過することがない別の安定した通信経路を用いて試験サーバーの運営を続行することができる体制を整えておく必要がある。

これは、従来型の紙ベースの集合試験においては、常に実現されていたことである。集合試験の会場は、周囲に少なくとも数本程度の道路が存在して、試験会場に 2 つ以上の入口があり、それぞれ、異なる道路に接続されてきた。朝、受験者たちの一部が試験会場に到着した後に、その来場経路の主要な一部の道路で局所的な不具合（たとえば交通事故）が発生して、試験会場の入口の 1 つの部分を含めて、通行不能になったと想像しよう。それ以降にアクセスする受験者たちは、その交通事故の道路を避けて、他の道路から試験会場に接近し、もう 1 つの入口から入場することが可能である。このように、受験者の人生がかかっている試験においては、試験実施主体は、試験会場入口付近の道路における局所的な不具合が発生した場合にも受験者によるアクセスに支障がないように、別の道路に面したもう 1 つの入口を用意しておく等の、周到な障害リスク管理の対策を施している。

そこで、在宅型 CBT 試験システムにおいても、従来の紙ベースの試験と同等程

度の可用性を実現しているといえる状態を維持するためには、インターネット上の局所的通信不具合に対応するために、同様に、試験システムへの 2 つ以上の入口を用意しておく必要がある。

## (2) 本システムの試験サーバーのインターネット接続経路は複数組織に冗長化されておらず、全断が発生し得る

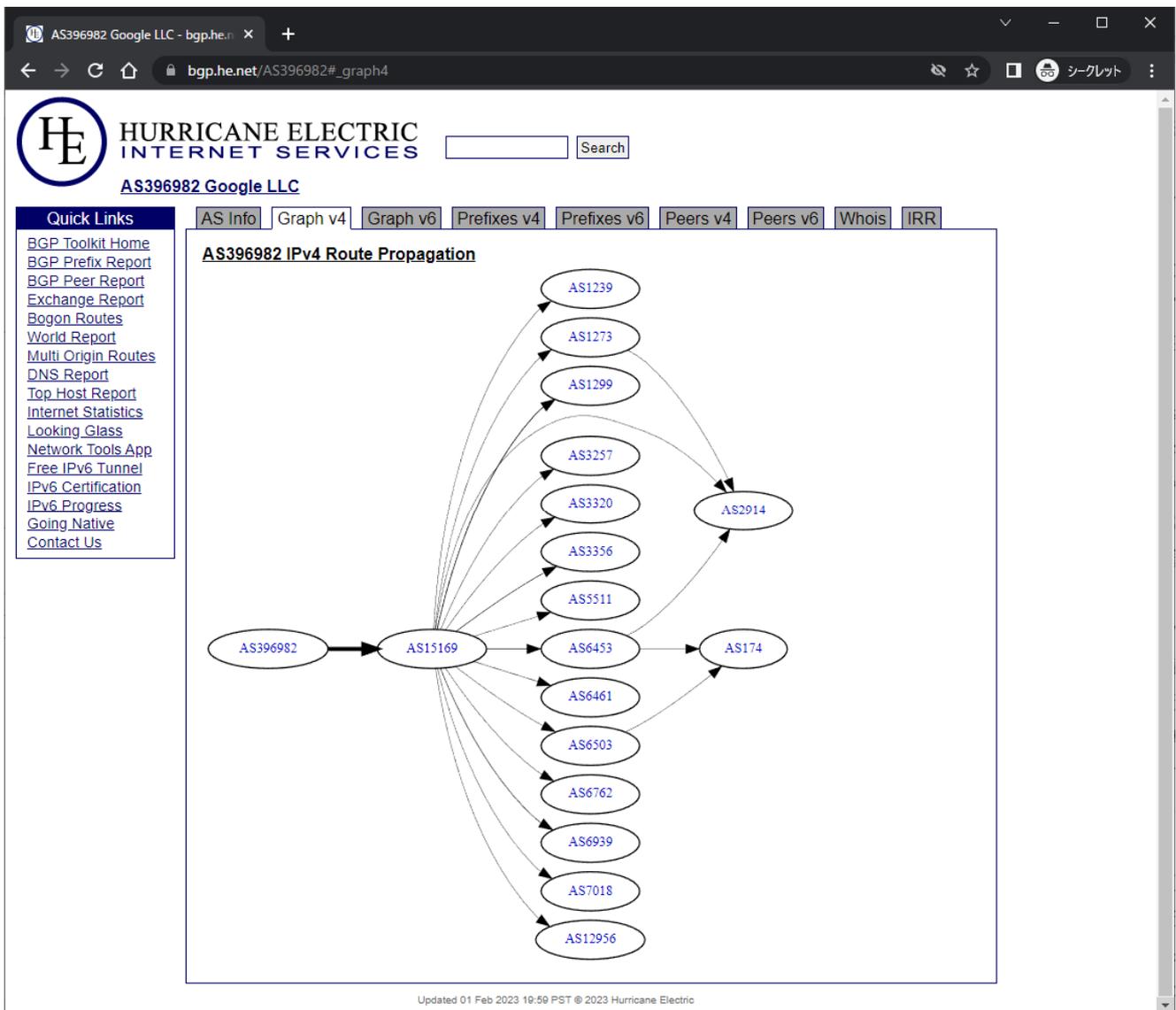
ところが、本システム (本文書でサンプル的に評価した対象製品) を実際に検証すると、本システムのサーバーは、インターネット上で 1 つの入口しか設けていないことが分かるのである。

これをもう少し詳しく検討しよう。本文書の執筆時において、本システムのサーバーは、「〇〇〇.com」という名前のホスト名で示される HTTPS エンドポイントに存在している。本文書の執筆時におけるこの「〇〇〇.com」というホスト名に対応する IP アドレスは、固定的に、「〇〇.〇〇〇.〇〇〇.〇〇」となっている (なお、この IP アドレスはリバースプロキシである可能性が存在する。その場合は、実体のサーバーはさらなる背後に存在する。)。この固定 IP アドレスは、インターネット経路上における「〇〇.〇〇〇.0.0/14」というサブネットと呼ばれるネットワーク上に属し、AS396982 (GOOGLE-CLOUD-PLATFORM) という米国の単一の AS (インターネット上の独立ネットワーク運営主体) の BGP ルータと呼ばれる通信装置を用いて、インターネットに接続されている。

仮にこの AS396982 (GOOGLE-CLOUD-PLATFORM) が、インターネットに対して、複数の異なる組織を経由して、複数の経路 (出入り口) を有して接続されていれば、一部の出入り口で障害が発生しても、通信は別の経路に自動的に迂回される可能性が高い。先の物理的な集合型試験会場のイメージでいうと、2 つ以上の出入り口で異なる道路に接続されていれば、いずれの道路で交通事故があっても、会場には迂回して出入りできるが、それと同一のことは、インターネット上で BGP の仕組みを用いれば、容易く実現できる。

しかし、本原稿の執筆時点において、この AS396982 (GOOGLE-CLOUD-PLATFORM) というネットワークは、なんと、単一の上流 ISP である AS15169

(GOOGLE) というネットワークとしか接続していない。インターネットから見れば、「〇〇〇.com」のサーバーをホストしているネットワークは、袋小路になっていて、その 1 本の道路で (すなわち単一の上流である AS15169 で) 不通が発生すれば、もはやインターネットとの間で全く通信をすることができなくなる。



インターネット上のすべての IP アドレスは、AS と呼ばれる独立組織によって BGP と呼ばれる仕組みで広報され、AS 間は数珠つなぎ的かつ冗長的に連なっている。AS396982 (GOOGLE-CLOUD-PLATFORM) はかなり特異で、上流が AS15169 (GOOGLE) のみである。今回評価対象となった試験システムのサーバーは AS396982 (GOOGLE-CLOUD-PLATFORM) に完全に依存してしまっており、AS396982 または AS15169 のいずれかの AS がダウンしてしまった場合、直ちに可用性の問題が生じる。

インターネットがかなり柔軟で自律的な仕組みで低コストに安定して動作している理由は、1 つのネットワーク (AS) は、必ず 2 つ以上の複数のネットワーク (AS) と相互に接続されていることの原則が保たれているためである。ところが、

「〇〇〇.com」が AS396982 のみに依存し、AS396982 が AS15169 のみに依存するという二箇所の点で単一組織への依存が発生しており、いずれかの組織で不具合が発生すると、一部または全部の受験者の PC との通信が全部止まってしまうことになる。

このように、本システムのサーバー「〇〇〇.com」は、本原稿執筆時点では、インターネット上でも、かなり特殊なネットワーク（上流ネットワークが 1 つしかない）に接続されており、ネットワーク経路的にみて、一般的な冗長体制が実現されていないといえる。たった 1 つのネットワーク経路上の組織の不具合（本サーバーを収容している AS396982、またはその単一上流の AS15169 のいずれかの組織で発生した不具合）によって、全断が発生し得る。

👉 AS396982 (GOOGLE-CLOUD-PLATFORM) と AS15169 (GOOGLE) とは、同一の Google 社が運営しているようなので、この 2 つの AS は完全に同視できるのではないかと（すなわち、特殊なケースとして考えるのではなく、単に 1 つの AS としてみるべきである。実際にはこの 2 つの AS は全く同一の管理システムで運営されているのではないかと）、という考え方があり得る。

しかしながら、仮に「完全に」同視できるとなると、AS 番号を取得する要件である「必要性」が存在しないことになってしまい、AS 番号の取得ができないはずなので矛盾が生じる。したがって、この 2 つの AS は、何らかの理由で正当な必要性があり、確かに、2 つに分離しているということになる。2 つに分離しているのであれば、管理体制や管理ポリシーが、内部的関係上、別々であることになり、例え同一の法人の Google 社が運営していたとしても、可用性の面で考察するときは、これらは、別々のものであると考えなければならない。

なお、本記事で述べている問題は、本試験サーバーを収容している AS396982、またはその単一上流の AS15169 のいずれかの組織で発生した不具合で、本試験サーバーが全断してしまうということであるので、上記の 2 つの AS が同視できるか否かは、本質的な問題ではない。しかし、できるだけ正確性を期すために、このように解説を記述することにした。

### (3) 単一の他社ネットワーク設備に依存していることで局所的不具合が発生し得る

本システムのサーバー「〇〇〇.com」は、本原稿執筆時点では、単一の他社ネットワーク設備 (GCP: Google Cloud Platform サービスの設備) に依存しているように見える。この状態で、インターネット上に、局所的な不具合が発生したと仮定しよう。

たとえば、米国の AS396982 (GOOGLE-CLOUD-PLATFORM) の運営主体がインターネットに出る際の複数の経路のうち 1 箇所では不良が発生したとする。米国の AS396982 (GOOGLE-CLOUD-PLATFORM) は、別の AS15169 (GOOGLE) というネットワークを経由して、インターネットに対して、少なくとも、合計 495 本の論理的なリンクを通じて接続されている (フルルート情報による。)①。これらの 495 本の論理的なリンクのうち、いずれか 1 箇所では、前記の交通事故のような局所的な不具合が発生したとする。完全にリンクが切れて、かつ、関連する BGP ルーティングソフトウェアと呼ばれるプログラムの動作も仕様通りであれば、その部分は自動迂回されることが期待できる。ところが、問題となる多くのケースでは、リンクの故障は、とても中途半端に発生するのである。完全に切れてはいないが、通信が時々おかしくなるというような故障方法である。このような中途半端な通信不良が発生したとき、経路としては、その故障経路は維持されているが、いざ通信が流れようとする、うまく通信できないという事象に遭遇することになる。これは、AS15169 (GOOGLE) の側の不具合の可能性だけでなく、接続している対向側のネットワーク運営主体の側に不具合がある場合もある。可能性は、ちょうど半々である。この種の問題は、AS15169 (GOOGLE) に隣接しているネットワークで発生するだけでなく、さらにもう 1 つ受験者に近い側のネットワークで発生することもあり得る。また、ネットワーク同士を接続するための共用のデータリンク設備 (IX: Internet Exchange と呼ばれる。) や、データリンク

---

① [https://bgp.he.net/AS15169#\\_peers](https://bgp.he.net/AS15169#_peers)

を構成するための専用線設備の故障で発生することもあり得る。

このような様々な点で突然発生し得る中途半端な局所的な不具合は、全断ではないので、なかなか治らない場合が多い。全体的な不具合で、かつ、完全に通信が切れるといった類のものは、ルーティングプログラムが自動的に検出して、その不良点を迂回する通信経路が自動形成されるのであるが、中途半端かつ局所的な不具合の場合は、そのような迂回のトリガーが引かれず、いつまでも中途半端かつ局所的な不具合点を通じてデータが流れることになる。

この場合でも、しばらく時間が経つと、その経路を通じて通信を行なっているユーザーたちから不具合の申告がユーザーと直接契約関係にある ISP に寄せられる。ISP は、その苦情の数が一定数になったら調査に乗り出し、原因がインターネット側にあると判断すれば、直接契約関係がある隣接する ISP に苦情を申し出る。このように隣接関係をずっと辿って苦情がバケツリレー的に伝播していけば、いずれは、不具合がある点の設備を管理している責任者に辿り着くことが可能である。そうして、ようやく、不具合の原因組織によってその不具合が認識され、その後、その組織の技術者によって、ソフトウェアの設定を修正したり、ハードウェアを交換したりして、不具合が解消される。これらはすべて人間が介在するプロセスなので、数時間以上を要することが多い。

つまり、インターネット上の通信経路の不具合は、プログラムが自動的に修復可能なケースは一瞬で修復されるが、そうでない様々な故障ケースは、人間が修理しなければならないのであり、回復までに、かなりの時間を要するという性質を有するといえる。

重要な試験時間中に、受験者の PC と受験サーバーとの間のインターネット上の経路上で生じる特定の通信不具合が回復しない現実的可能性が存在することになる。

#### (4) 本システムのサーバー「〇〇〇.com」のインターネットとの出入り口が単一の他社ネットワーク設備に依存してしまっていることを示す根拠

前述のように、本システムのサーバー「〇〇〇.com」は、少なくとも、外形的に

は、単一の他社ネットワーク設備 (GCP: Google Cloud Platform サービスの設備) に依存しているように見える。

実は、本記事は、外部から本システムのサーバー「〇〇〇.com」との通信経路等の挙動を観測して得られた情報をもとに執筆していることから、真にサーバー「〇〇〇.com」のネットワークが GCP 設備のみに依存しているか否かは確認できていない。実際には GCP の不具合時に発動される隠された優れた切り替えの仕組み (たとえば、GCP と一部の受験者との間において通信の局所的な不具合が発生した場合等に、DNS 側のレコードが書き換えられて、他の経路でインターネットに接続されている別の IP アドレスが当該ホスト名に関連付けられる等の仕組み) が存在するのかもしれない。しかし、本システムの開示情報からは、そういった冗長化機能の存在がうかがえなかった。

かえって、本システムに、そういった冗長化機能の存在がなさそうであるという推測を補強する根拠が、本システムのドメインの DNS 権威サーバーの設定に存在する。以下、これについて、解説をする。

本システムのサーバー「〇〇〇.com」の DNS 権威サーバーの設定を、外部から可能な範囲で検証してみたところ、「〇〇〇.com」の IP アドレス情報の TTL (Time To Live: 情報の有効期限、すなわちキャッシュされることが許容される最大時間を示す) が 3,600 秒 (60 分) として設定されていることが分かった。

```
C:\WINDOWS\system32\cmd.exe - nslookup

> set debug
> [redacted].com.
サーバー: 01.dnsv.jp
Address: 157.7.32.53

-----
Got answer:
HEADER:
opcode = QUERY, id = 3, rcode = NOERROR
header flags: response, auth. answer, want recursion
questions = 1, answers = 1, authority records = 4, additional = 0

QUESTIONS:
[redacted]. type = A, class = IN
ANSWERS:
-> [redacted].com
internet address = [redacted].[redacted].[redacted].[redacted]
ttl = 3600 (1 hour)
AUTHORITY RECORDS:
-> [redacted].com
nameserver = 01.dnsv.jp
ttl = 86400 (1 day)
-> [redacted].com
nameserver = 02.dnsv.jp
ttl = 86400 (1 day)
-> [redacted].com
nameserver = 03.dnsv.jp
ttl = 86400 (1 day)
-> [redacted].com
nameserver = 04.dnsv.jp
ttl = 86400 (1 day)

-----
Got answer:
HEADER:
opcode = QUERY, id = 4, rcode = NOERROR
```

評価対象の CBT 試験システムのサーバーの IP アドレス情報は、DNS 上で TTL（キャッシュ時間）が 3,600 秒（1 時間）に設定されている事実（公開情報）から、本システムは、サーバーをクラウド間で冗長させていないこと（ダウン時に他に切り替える仕組みがないこと）を知ることが出来る。

仮に、DNS を用いてサーバー側のネットワーク障害に対応した冗長（切り替え）を実現する場合、TTL は、1 分とか 5 分程度の短い長さに設定されているはずである。なぜならば、TTL が 60 分間などの長時間に設定されている場合、いざ DNS サーバー側で切り替えを実施しても、すでに障害発生中にアクセスを試みた受験者 PC 等のクライアント PC や、自宅のルータの DNS 機能、ISP の DNS サーバー等に、最大 60 分間分の古い情報が残存してしまっていて、結局試験が受験できないという状態になってしまうためである。今、本システムの DNS のレコードの TTL が 3,600 秒（60 分）と設定されていることから合理的に観測できることからしても、本システムのサーバー「〇〇〇.com」は、設計上、インターネ

ットとの経路としては、単一の他社ネットワーク設備 (GCP) に完全に依存した設計になってしまっている (単一のネットワーク設備への依存を完全に前提として運用されている) ように推定できる。本システムの実装が、この推定を覆すに足る、複数の主体のネットワーク設備に冗長化されて接続されているという外部への情報の現われは、検証した範囲では、見あたらなかった。

## (5) どのようにサーバー収容ネットワークの冗長化を確実化すべきか

そこで、本システムのような在宅型 CBT 試験システムを利用しようとする試験実施主体においては、本システムの提供者に対して、試験サーバーを収容しているネットワークが複数ネットワーク組織にまたがって (すなわち、GCP クラウド設備以外を通して) 正しく冗長化されてインターネットに接続されているかどうか、あるいは、仮に固定的に単一の組織の設備 (GCP 設備) の経路のみを經由してインターネットに接続されている場合であっても、局所的な不具合を含めた通信不良が発生したならば、すぐさま、他の経路を通してインターネットに接続し直す仕組みが具備されているかどうか (例えば、DNS レコードを自動的に書き換えることにより、障害のない側のネットワークの IP アドレスを返すようにする等の体制が具備されているか)、よく聴き取りをして確認しておく必要がある。

聴き取りの結果、業者から、「万全の体制です。」という回答があったとしても、試験実施主体は、それを鵜呑みにしてはならない。試験実施主体は、試験の性質からしても、代行業者を最も厳しく「試験」しなければならない。あれこれと質問を試みたり、前記のようなインターネット接続経路の状態を確認したり、DNS レコードの TTL の値を確認すること等により、初めて、代行業者の真の技術能力と具備している障害耐性を知ることができるのである。

また、本システムのような在宅型 CBT 試験システムのサーバーを構築・運営する試験代行業者においては、試験サーバーを必ず 2 つの経路 (異なるネットワーク運営組織、すなわち異なる AS 番号) を通ってインターネットに接続した状態とするか、または、常に単一のネットワークを經由するようになっていたとしても、必要な場合には、DNS のレコードの切り替え等の仕組みにより、予備のネットワ

ークを經由できるようにする等の対策を施しておく必要がある。

DNS による切り替えを実施する方式の場合は、プログラムで自動化をすることもできるし、場合によっては、試験時間中にオペレータが待機しておき、決められた簡単な操作を実施する (DNS ゾーン情報の書き換えを行なう) だけで切り替えることができる体制を構築しても良いであろう。

いずれの方法にもリスクが存在するが、比較的 low コストで実現することが可能である。重要なのは、真に万全の体制を具備しているといえるだけの技術的知識を、組織的に、常時維持・研鑽し、それに裏付けられたサーバーやネットワークを構築・運用することである。これが、試験実施主体 (発注者) からの信頼を確立することができる、唯一の方法である。

## (6) 本システムの試験サーバーの DNS サーバーは複数組織に冗長化されていない

次なる問題は、本システムのサーバー「〇〇〇.com」の DNS 権威サーバーと呼ばれる重要な情報配信サーバーが、インターネット上で適切に冗長化されていないという可能性である。DNS 権威サーバーの冗長化が不完全であるとき、それは、前述した、試験サーバーのネットワークが GCP に単一依存してしまっている状態と同等程度か、それ以上に危険な、試験の可用性に対するとなるリスクになる。

DNS 権威サーバーというものは、インターネット上でホスト名 (〇〇〇.com 等) を IP アドレス (〇〇. 〇〇〇. 〇〇. 〇〇 等) に変換する役割を果たす、重要なサーバーである。DNS 権威サーバーは、伝統的には、ドメインの所有者が自ら構築するものであったが、最近では、共有の DNS 権威サーバー機能をレンタルする形で DNS 権威サーバーを稼働させる方式も、一般的にみられる。これは、どちらでも良い。自前で構築する方法が最も安定して動作する上に、技術力研鑽にもなるので、長期的利益は大きいですが、レンタルサービスを利用すれば、そのような技術力不要で DNS 権威サーバーを立ち上げることができるという短期的利益が得られる。レンタル DNS 権威サーバーであっても、それなりに安定して動作すると期待できる。

問題は、自前で DNS 権威サーバーを構築する方法でも、レンタルサービスを利用する方法でも、それらの DNS 権威サーバーの運営基盤およびインターネットとの接続経路を、単一組織に依存させてはならないという点にある。仮に DNS 権威サーバーそのもの、または、インターネットから DNS 権威サーバーに至るまでのネットワーク経路で障害が発生してしまった場合、たとえ試験サーバーそのもの（本システムの例においては、サーバー「〇〇〇.com」）がその意図した IP アドレスで正常に稼働していたとしても、試験システムにアクセスしようとする受験者は、サーバーの IP アドレスを知る手段がなくなり、結果として、試験を受験することが全くできなくなってしまうためである。

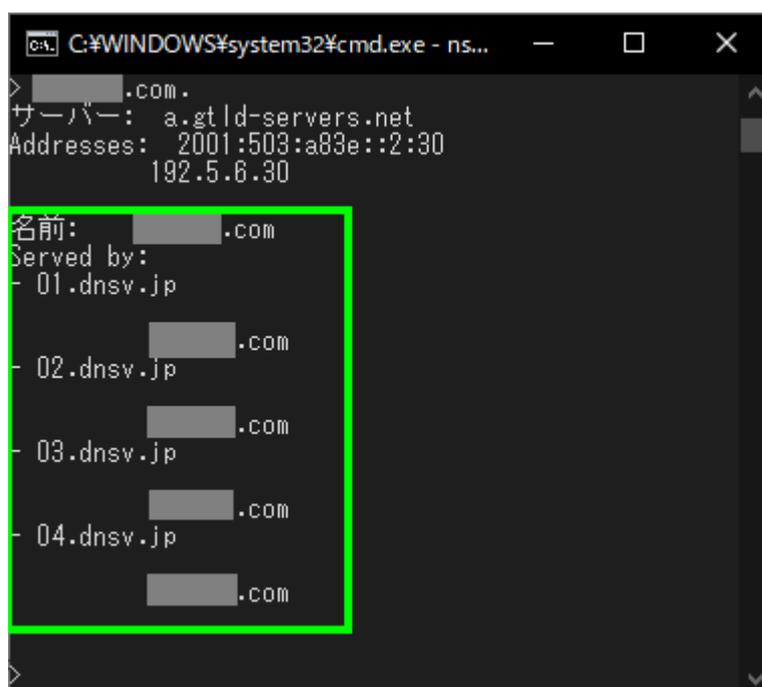
DNS 権威サーバーがダウンすると大変な事態になることは、試験開始後の受験中でも、同様である。本システムでは、試験受験中にも随時通信が行なわれる。通信が途切れると、ページ送りができなくなり、問題文の表示や、回答内容の送付ができなくなってしまう。

このような観点から、DNS 権威サーバーの正常動作は、試験実施の生命線であるといえる。本システムの DNS サーバーのような、極めて重要な DNS 権威サーバーは、必ず、以下の 2 つの条件を満たして設置しなければならない。

- (a) 複数の DNS 権威サーバーからインターネットまでの接続経路は、全体をみて、異なる 2 以上の運営主体のネットワーク（異なる AS 番号）に分散的に収容され、設置されていること。すなわち、特定の運営主体（AS）に不具合が発生した場合でも、すべての DNS サーバーとの通信経路が全断するというおそれがないこと。
- (b) 複数の DNS 権威サーバーの運営をレンタルサービスや DNS ホスティングサービスを活用して社外に委託する場合は、全体をみて、少なくとも 2 つの異なるレンタル基盤またはホスティング基盤を用いて運用すること。すなわち、特定のサービス主体のシステムまたは経

常に不具合が発生した場合でも、すべての DNS 権威サーバーが同時に停止するというおそれがないこと。

ところが、本システムのドメイン「〇〇〇.com」は、4 個の権威 DNS サーバーに分散配置されているものの、いずれも、「dnsv.jp」というホスト名の DNS レンタルサービス (これは、GMO インターネット社の「お名前.com」という製品ブランドのレンタル DNS 権威サーバーサービスであると思われる) 上で動作している。これらのレンタル DNS 権威サーバーは、いずれも AS55907 (GMO-DNS GMO Internet,Inc) という AS 番号を用いてインターネットに接続されている。したがって、AS55907 で不具合が発生した場合に全断が発生する可能性があり、条件 (a) を満たさない。また、単一の DNS レンタルサービスのソフトウェア基盤に依存しているため、当該ソフトウェア基盤に不具合が生じた場合に全断が発生する可能性があり、条件 (b) を満たさない。よって、本システムの試験サーバー「〇〇〇.com」を司る DNS 権威サーバーは、レンタル DNS の不具合により、すべて同時に突然ダウンする可能性があり、この際に試験を受験できない受験者が多数発生することが予想される。



```
C:\WINDOWS\system32\cmd.exe - ns...
> [redacted].com.
サーバー: a.gtld-servers.net
Addresses: 2001:503:a83e::2:30
           192.5.8.30
名前: [redacted].com
Served by:
- 01.dnsv.jp
- 02.dnsv.jp [redacted].com
- 03.dnsv.jp [redacted].com
- 04.dnsv.jp [redacted].com
- [redacted].com
```

実際に、この GMO インターネット社の「お名前.com」ブランドのレンタル DNS サーバーサービスは、2009 年に、約 13 時間もダウンしたことがあり、この際には、ホストされている合計 3.3 万個のドメイン名に影響があった<sup>①</sup>。

なお、本記事の著者は、GMO インターネット社の「お名前.com」という DNS レンタルサーバーサービスが、特別に何らかの問題があるということを主張している訳ではない。他社の DNS レンタルサーバーサービスでも、リスクは全く同じである。要点は、(1) 同レンタルサーバーサービスであろうと、他社の DNS レンタルサーバーサービスであろうと、どのようなサービスも、たとえば DNS サーバーが複数台あったとしても、単一の会社が運営している以上は、ソフトウェア負荷上昇やネットワーク帯域圧迫等で、一斉にダウンすることもあり得る、(2) 多数のドメイン (顧客) が 1 社の DNS 権威サーバーを共有していると、いずれかのドメインを指した大量の名前解決トラフィックが寄せられると、レンタルを受けているすべてのドメイン (顧客) がダウンするので、DNS レンタルサーバーには、自ら DNS サーバーを立てる場合と比較して、可用性のリスクがかなり大きい、という点である。

このように、現在、本システムの試験サーバー「〇〇〇.com」に係る障害点のリスクは、DNS 権威サーバーを支える GMO インターネット社の「お名前.com」ブランドのレンタル DNS サーバーサービスと、前述の GCP ネットワーク設備との 2 個存在し、これら 2 個の障害点が直列的に連結してしまっていることにある。すなわち、Google 社の GCP ネットワーク設備も、GMO インターネット社の当該レンタル DNS サービスも、いつでも停止してしまう可能性があるが、いずれか一方でも停止してしまうと、受験者の PC が本システムを用いた試験サーバーに対するアクセスができなくなり、試験が停止してしまうということを意味する。

このことから、本システムのインターネット接続経路に係る冗長化の度合いは、物理的な試験会場に対するアクセス手段の冗長化の度合いと比較しても、かなり低

---

<sup>①</sup> <https://internet.watch.impress.co.jp/docs/news/332542.html>

いものであると言わざるを得ない状態にある。将来の改善が、強く望まれる。

なお、最近、海外クラウド事業者等が DNS レンタルサービスを「クラウド型 DNS」等の名称でイメージ付けして販売をしているが、これも、その実体は、レンタル DNS サービスである。ただし、DNS サーバーが物理的に全世界の地域に分散している点が特徴である。ところが、単一の海外クラウド事業者によって、複数の地域で DNS サーバーが運用されていると謳われているとしても、単一の DNS レンタルサービスのソフトウェア基盤に依存しているため、当該ソフトウェア基盤に不具合が生じた場合に全断が発生する。したがって、海外クラウド事業者等のクラウド型 DNS サービス 1 社のみには依存してはならない。必ず 2 社以上に跨がって分散配置しなければならない。

本文書によるこれらの指摘は、決して、レンタル DNS 権威サーバーを利用することを否定するものではない。レンタル DNS 権威サーバーを利用するのは良いが、決して、あるドメインのすべての DNS サーバーを、そのレンタル業者に依存させてはならないということを主張しているのである。複数の DNS サーバーのうち一部をレンタル業者 A にホスティングさせ、残りをレンタル業者 B にミラーリングさせるという方法であれば、レンタル DNS サーバーに頼っても、ドメインの IP アドレス解決について、十分な可用性を確保できるので、安心である。

## (7) どのように権威 DNS サーバーの冗長化を実現すべきか

実際に、上記の条件を満たすように権威 DNS サーバーを分散配置することは、比較的簡単かつ低コストに実現できる。これらは、基本的なインターネット知識とサーバー管理スキルのみで、実現することができる。クラウドを活用するのであれば、複数のクラウド事業者 (同一のクラウド事業者の複数アベイビリティゾーンでは不十分であることに注意する。ソフトウェア等の不具合により、すべてのアベイビリティゾーンが全部同時に 1 時間以上停止する事象が、実際に発生しているためである。) に跨がってサーバーと IP アドレスを契約し、それぞれで DNS サーバーを運用すればよい。これは、極めて低コストに実現できる。オンプレミスのサーバー設備があれば、2 つ以上の異なる設備で DNS サーバーを運用すればよい。

なお、権威 DNS サーバーを複数運用する場合は、さらに、DNS サーバーのソフトウェアの種類も異なるものにしたほうが良い。DNS サーバーのソフトウェアには (特に「BIND」という DNS サーバーソフトウェアには)、しばしば脆弱性が発見され、インターネット上から任意の悪意のある者がいつでもその DNS サーバーの動作を停止または麻痺させることができる状態に陥るためである。複数の種類の DNS サーバーソフトウェアを分散利用していれば、そのような脆弱性があつた場合にも、全部の DNS サーバーが同時に停止することを免れることができる。

## (8) 権威 DNS サーバーの問題は、不具合が発生してから切り替えるのは遅すぎる

権威 DNS サーバーの冗長化は、不具合が発生するよりも遥か以前に、予め実施しておかなければならない。あるドメインに対して登録してある複数台の権威 DNS サーバーが、冗長化不足で、いずれもアクセスできなくなってしまった場合、その事象が発生してから権威 DNS サーバーのアドレス登録を書き換えるのでは、もはや遅すぎる。

その理由は、その対象ドメインの 1 つ上位のドメインの DNS サーバー (例えば、本システムにおけるドメイン「〇〇〇.com」の 1 つ上位のドメインは「.com」である) の TTL (Time To Live: 情報の有効期限、すなわちキャッシュされることが許容される最大時間を示す) の値が、統一的に、48 時間等の極めて長い値に設定されていることに由来する。これは、「.com」の DNS サーバーへのアクセス数をできるだけ減らすことによる運営コストを削減するため、「.com」の DNS サーバーの運営者によって、そのように長い時間が TTL として設定されているのである。

「.com」の DNS サーバーは、アクセスをしようとしてきた DNS クライアントに対して、ドメイン「〇〇〇.com」の DNS サーバーの一覧の IP アドレスを返却する。これは 48 時間インターネット上の各所の DNS サーバー上で保持 (キャッシュ) される。その後、権威 DNS サーバーに障害が発生したとき、急いで権威 DNS サーバーを切り替えるならば、権威 DNS サーバーの変更登録する

必要がある。ところが、その変更登録の効果がインターネット上で生じるのに、ユーザーの利用する DNS サーバーにおけるキャッシュが消え去るまでに、最大 48 時間程度 (したがって、平均 24 時間程度) かかるのである。これでは、試験開始前日、当日または試験日において DNS 権威サーバーに不具合が発生しても、その時点から対応することでは遅すぎることを意味する。よって、権威 DNS サーバーは、予め、確実に複数ネットワークおよび DNS サーバー運営基盤に対して冗長化しておく必要があるのである。

### (9) 「.com」ドメインやルート DNS サーバーの可用性リスクについての一応の考察

仮に本システムにおけるドメイン「〇〇〇.com」の DNS 権威サーバーの可用性を万全な状態にしたとしても、その 1 つ上位のドメインである「.com」の DNS 権威サーバーの可用性が万全な状態でなければ、全く無意味である。本システムはドメイン「〇〇〇.com」に完全に依存している以上、上位ドメインの「.com」の可用性を慎重に検討する必要がある。

「.com」ドメインは、本文書執筆時において、合計 10 台の DNS 権威サーバーによって稼働している。これらの DNS 権威サーバーの IP アドレスは、AS396576, AS396741, AS397199, AS397210 の 4 個の AS 番号 (独立ネットワーク) 上にまたがって動作している。したがって、異なる AS 上で動作するという要件を、一見満たしているように見える。

一方で、これら 4 個の AS および DNS サーバーは、すべて、実は米国の私企業である「VeriSign Inc.」という株式会社が運営している。その点で、インターネット・システム上は一見分散がなされているが、運営主体は全く分散がなされておらず、可用性には、限界がある。

ただし、これらの重要な DNS 権威サーバーは、「エニーキャスト」と呼ばれる特殊な冗長化手法で、全世界に分散配置されており、全部の通信経路が止まる可能性はかなり低い。

また、「.com」ドメインは、本記事執筆時点で、全世界で 1.6 億個のサブドメイ

ンをホストしており<sup>①</sup>、世界中の様々な 1.6 億個ものシステムが依存している。

「.com」ドメインの権威 DNS サーバーの稼働に不具合が生じたならば、インターネット全体の動作に不具合が発生したのと同じ結果になる。その発生確率はかなり低く、発生頻度は、従来型の集合型紙試験において会場が火災になるような確率よりも同等程度か、さらに低いと考えられる。したがって、「.com」ドメインがダウンした場合に、サブドメイン「〇〇〇.com」がダウンして、本システムが利用できなくなったとしても、本システムを用いた試験運営主体が社会的に非難される可能性はかなり低そうであり、事実上心配する必要は無いという考え方も可能である。

ところが、「.com」ドメインは、「.」というルートドメインのサブドメインであるので、さらに、「.」というルートドメインに依存していることになる。ルートドメインは、ルート DNS サーバーと呼ばれる、世界中に論理的に 13 台しかない DNS 権威サーバーに依存している。13 台の論理的なサーバーは、実際には、前述と同じ「エニーキャスト」と呼ばれる頑強な仕組みで、全世界に分散されて配置されている。これらは、合計 12 の互いに独立した組織によって運営されている（その組織のうち 1 つは、日本における WIDE プロジェクトである<sup>②</sup>）。よって、単一障害点の問題は発生しない。

そこで、誰でも疑問に思うことは、これらの 13 台の「.」というルートドメイン DNS 権威サーバーの IP アドレスは、一体どのようにして世界中で共有されているのであろうか、というものであろう。ルートドメインよりもさらに一層上位のドメインが存在するとすれば、無限後退（あることを成立させている根拠を求めて、その根拠の根拠の根拠というように、限りなくさかのぼっていくこと。）の問題が発生する。実際には、そのような、さらに一層上位のドメインなどは、存在しない。実は、これらの 13 台の IP アドレスは、ユーザーのルータに内蔵されている DNS サーバーや、ユーザーが利用する世界中の DNS サーバーの中に、固定的に埋め込まれているのである。

---

<sup>①</sup> <https://www.nic.ad.jp/ja/stat/dom/gtld.html>

<sup>②</sup> <https://m.root-servers.org/>

これは、かなり原始的な手法であるが、大昔からそうなっていて、それなりに安定している (ただし、ごく稀に 13 台のうち 1 台の IP アドレスを変更しなければならないような事象が発生し、大騒ぎになる<sup>①</sup>)。そして、合計 12 の互いに独立した組織が、13 台の DNS サーバーの IP アドレスを、前述した BGP の仕組みを用いて、インターネットに対して広報しているのである。かなりの安定性が見込まれる。むしろ、この程度の大きな努力をしなければ、インターネット上における真の通信の可用性は、維持できないのである。

これらのことから、本システムの運営者に課せられた DNS の可用性を確保する責任としては、本システムにおけるドメイン「〇〇〇.com」の DNS 権威サーバーの可用性を確保するだけで足りるものと考えられる。それよりも上位の「.com」や「.」というドメインの可用性に対するリスクは存在するものの、本システムの運営者が心配する程度ではない。これらの上位ドメインがダウンする可能性は、従来型の物理的な集合試験の会場がダウンする可能性よりも低いためである。

### 3 本システムにおける試験サーバー動作の可用性の検討

#### (1) 概説

在宅型 CBT 試験システムにおいては、試験サーバーそのものの可用性は、サーバーのインターネット接続経路の可用性以上に重要である。いくら通信経路の可用性を実現していても、サーバーそのものがダウンしてしまったら、いかなるサービスも継続できないためである。

そして、サーバーというものは、いつでも、突然故障する可能性がある。在宅型 CBT 試験システムを用いた試験は、受験者の人生に影響が生じるような重要な社会的行事である。そこで、試験サーバーは、故障に備えて、予備サーバーを用意しておき、メイン (現用) のサーバーが故障した場合に、直ちに予備を稼働できる状態を整えておく必要がある。

もちろん、予備サーバーも現用サーバーと全く同時に故障する可能性はあるが、

---

<sup>①</sup> <https://h.root-servers.org/renumber.html>

その確率はかなり低いので、試験実施主体としては、対策できる対策は一応施していたということで、受験者に対する責任を果たしたことになるであろう。在宅型 CBT 試験においてメインサーバーと予備サーバーのいずれも同時に利用できない事象が発生する確率が、従来の集合型紙試験において天変地異や火災等によって試験会場が全く利用できない事象が発生する確率以下であれば、いざ不具合が発生しても、在宅型 CBT 試験システムを利用することに決めた試験実施主体が社会的に強く非難されることはないと考えられるのである。

## (2) 試験サーバーをどのように冗長化すべきか

そこで、試験サーバーをどのように冗長化するかが重要となる。

これは、オンプレミスまたはプライベートクラウドでサーバーを用意する場合と、パブリッククラウドでサーバーを用意する場合とで異なる。

### (a) オンプレミスまたはプライベートクラウドでサーバーを用意する場合

試験サーバーの冗長化のためには、それが物理的なサーバーを占有する場合であっても、仮想的なサーバー (VM) を用いる場合であっても、物理的な筐体として、異なるものを用意する必要がある。また、サーバーを設置するデータセンタの電源 (UPS 等) がダウンする可能性もあるので、電源は 2 系統用意する必要がある。データセンタそのものの火災もあり得るが、これは、従来型の集合試験会場が火災になる可能性と同等かより低いと考えられるので、電源系統がある程度信頼できるのであれば、データセンタの冗長化までの対策は不要かも知れない。

そして、インターネットまでの接続経路は、すべてのサーバーを合わせて見て、最低 2 本必要である。インターネットまでの接続経路部分は、異なるネットワーク運営主体 (AS 番号) によって収容されている必要がある。ある単一のネットワーク運営主体で障害が発生した場合も、ネットワーク運営主体との契約上認められる極めて低い金額の違約金 (損害賠償のみ) が認められ、それ以上の損害賠償は認められない契約になっていることが多い。いざというときには、ネットワーク運営

主体は、契約で免責されてしまう。このことから、障害が発生した場合は、その大半の損害は、サーバー設置者の側でいわば泣き寝入りを迫られる結果になるのである。よって、試験サーバー設置者は、異なる 2 つの独立主体から、インターネットに向けたネットワークを引く必要があるということになる。

## (b) パブリッククラウドでサーバーを用意する場合

前述の (a) の手法はそれなりに大変である。パブリッククラウドでサーバーを用意したほうが良いという場合も多い。この場合、冗長化された複数のサーバーは、異なるパブリッククラウド運営基盤に委ねられる必要がある。

たとえば、合計 2 台のサーバーのうち 1 台を、クラウド事業者 A (例: AWS) に委ねたとする。もう 1 台を決して同じクラウド事業者 A に委ねてはならない。たとえ異なるアベイリティゾーン、異なるリージョンへの分散設置を行なっても、これは、十分な冗長化にならない。なぜならば、単一クラウド事業者内のクラウド運用基盤システム (VM や仮想ネットワーク、ストレージ等のクラウド構成部品を運営管理するシステム) は、ソフトウェアで構成されており、そのソフトウェアに予期せぬ不具合があった場合、異なるアベイリティゾーン、異なるリージョンで同時に障害が発生する可能性があるためである。

たとえば、最近の例では、2023 年 1 月 25 日に米国の「Microsoft Corporation」という株式会社の運用する「Azure」というクラウドサービスにおいて、米国、ヨーロッパ、中東、アフリカ、アジア等の全リージョンで全部同時にネットワーク機能の障害が発生した<sup>①②</sup> (中国のみ、運営ソフトウェアが異なっていたようなので、影響を免れたようである。)。このことから、2 台以上のサーバーをクラウド上に設置する場合、少なくとも 2 以上のクラウド事業者にまたがって設置しなければならないことが分かる。

異なるクラウド事業者間に分散すれば、なぜ同時の障害発生を免れることができ

---

① <https://www.itmedia.co.jp/news/articles/2301/25/news175.html>

② <https://news.yahoo.co.jp/articles/939fd8813dea4b2fba443d9d265e7088f79cc7b2>

るのだろうか。それは、異なるクラウド事業者であれば、クラウド運用基盤システムのソフトウェアが異なることに由来する。ソフトウェアというものは、同じものを異なる場所で利用していれば、何らかの事象や、そのソフトウェアのアップデートが引き金になり、異なる場所で同時に障害が発生するものである。単一のソフトウェアや単一の運用手法に頼った複数のシステムは、一見独立しているように見えても、極めて脆い。強靱なシステムを実現する唯一の方法は、多様性の確保である。異なるクラウド事業者を跨がって利用すれば、多様性が確保されたことになる。多様性が確保されている互いに独立したシステム間で、同時に障害が発生する可能性は、極めて低い。また、異なるクラウド事業者を利用してサーバーを分散配置すれば、思いがけない利点もある。必然的に、インターネットに対する出入り口も異なることになり、前述のような通信経路における可用性低下の問題を自動的に避けることができるという点である。

このように、少なくとも 2 以上のパブリッククラウド事業者を跨がってサーバーを冗長化する手法を、「マルチクラウド」と呼ぶ。冗長化においてマルチクラウドを利用すれば、パブリッククラウドであっても、慎重に設計をしたオンプレミス環境またはプライベート環境と同等かそれ以上の可用性を実現することが可能である。

### (3) 本システムの試験サーバーは単一クラウドに完全に依存しており冗長化がなされていない

ところが、本システムの試験サーバーは、単一クラウド (GCP: Google Cloud Platform) に完全に依存しており、複数クラウド事業者間における冗長化がなされていないように見える。このことは、前述した本システムの試験サーバー用ドメイン「〇〇〇.com」のレコードの TTL の値からも判別可能である。

GCP は、米国の「Google LLC」という単一の有限責任会社が運営するパブリッククラウドサービスである。仮に GCP の内部で異なるアベイビリティゾーンや異なるリージョンにサーバーを分散配置していても、これらはすべて「Google LLC」社に起因する障害の影響を受ける。

前述のとおり、「Microsoft Corporation」社によって発生した「Azure」の障害は、中国をのぞくすべてのリージョンで同時に発生したが、この障害は少なくとも2023年1月25日の午後5時ごろから午後6時45分頃（日本時間）まで、1時間以上にわたって発生している。このことから、単一のパブリッククラウド事業者が引き起こす全世界的障害は、1時間以上にわたって持続することが分かる。これは、重要な試験においては致命的な問題となる。

#### (4) どのように改善をすれば良いか

したがって、本システムの試験サーバーは、重要な試験を実施することができる程度の可用性を実現するために、少なくとも2以上の異なるパブリッククラウドに冗長配置される必要がある。

このようなマルチクラウド構成を実現する場合、2倍のコストがかかるのではないかという点が懸念となる。ところが、実際にはコストはそれほど大きくならない。

なぜならば、実際の試験をホストするサーバー群については、一方の現用として利用する側のクラウドを常時稼働状態にしておき、もう一方の予備として利用する側のクラウドでは、VMのインスタンスを作成せずに、いつでもVMを立ち上げられる状態に維持しておくことが可能であるためである。そうすれば、予備の側のクラウドでは、VMの時間に応じた課金が発生しない。

ただし、試験データ等は、現用のクラウド上のシステムから、予備のクラウド上のシステムに、常時ミラーリング（コピーによる同期）を行なっておく必要がある。したがって、最小限のVMは予備の側のクラウドでも稼働させておく必要がある点に注意する必要がある。

その上で、現用のクラウドで障害が発生した場合は、すぐさま予備のクラウドを立ち上げるようにしておけば、いざ必要になった場合でも、5分くらいあれば予備のクラウドで全システムが立ち上がるであろう。あとは、本システムの試験サーバー用ドメイン「〇〇〇.com」のレコードを書き換えて、IPアドレスの設定を予備のクラウドの側の試験サーバーに向けるようにすれば、回復完了である（すでに述

べたとおり、DNS 権威サーバーのレコードの TTL の値は、1 分とか 5 分といった短いものにしておく必要がある。)

## 第 2 節 機密性に対するリスク（在宅型・集合型の両方）

### 1 試験システムにおける機密性とは

CBT 試験システムにおいて、機密性は極めて重要である。機密性の最重要箇所は、いうまでもなく、試験開始前の試験問題のデータである。

試験運営主体としては、試験問題のデータが試験開始前に不正に読み取られる可能性を、合理的に可能な範囲の努力を払って、防止しなければならない。

### 2 システム運業者の関係者による不正のリスク

#### (1) 概説

CBT 試験システムは、多くの場合、専門業者（試験代行業者）によって開発・提供される。試験運営主体が試験実施の主人であるが、実際の試験システムの稼働のシステム面でみると、いわば試験運営主体の履行補助者としての立場である試験代行業者の関係者が、絶大な権力を有してしまう瞬間が、従来の紙を用いた集合型試験と比較して、かなり多い。

第 1 章で述べたように、従来の紙を用いた集合型試験においては、試験実施主体は、試験問題の作成・印刷・製本及び試験会場への配送の各家庭における様々な機密的プロセスを、自らの手で組み立て、自らの目で目視確認し、自らの頭脳で様々なリスクを排除することが可能であった。試験会場における試験実施の段階に於いて、はじめて、試験代行業者の現場レベルの援助も借りて試験問題を全受験者に対して一斉配布することになるが、この直前の状態に至るまで、試験問題は厳重に封印された状態の封筒に格納されており、試験代行業者の経営者や被用者達であっても、試験問題の内容の一部又は全部を目視して、これを、内通している特定の受験者（問題の流出を囑託した者等）に伝達することは、物理的に困難であった。

ところが、CBT 試験システムでは、システムに試験実施主体が試験問題をいったん登録した後は、試験実施主体の知らない所で、試験代行業者の経営者達または一部のシステムに関係する被用者達は、その試験問題を読み出すことができしてしまう。この際に、「アクセスログ等が残るであろうから、不正な問題読み出しのリスクはない。」と安心することはできない。アクセスログは、まさにこれらのシステムの内部挙動として作成されるものであるから、システムそのものを自由自在に支配・制御することができる CBT 試験システムの提供業者の経営者やシステム関係の被用者たちは、アクセスログ保存を無効化したり、ログの一部を消去したりすることも可能であるためである。このようなシステムのレイヤにおける不正が原理的になされ得る限り、いかなる監査システムも無力である。

従来の紙を用いた試験において、同等の不正を行なうことができたのは、試験実施主体の役員や相当の権力を有するごく一部の職員達であったが、今や、CBT 試験システムでは、そのような権限の濫用のリスクが、試験代行業者の役員や被用者にまで広がってしまったのである。

## (2) システム運業者の関係者による不正を防止するほとんど唯一の手法は、試験直前に問題文をすることである

したがって、重要な試験（資格試験等）を実施する場合において、CBT 試験システムを使用する場合、試験実施主体としては、試験問題の登録を、試験開始直前まで先延ばしする必要が生じることになる。

この方法は、前述したような紙方式における問題文の配布直前に、初めて、封印を解いた問題文を試験会場で試験代行業者に手渡すプロセスとよく似ている。

この方法で、試験代行業者によって問題文流出の不正を行なうことができる無防備な時間を、数分程度に短縮することができる。

## (3) 本システムは直前の問題文登録ができず、かなり前に問題文を登録しなければならない

ところが、本システムの説明書によると、本システムでは試験実施主体は問題文

を試験開始直前に登録することができない。本システムの説明書によると、事前に登録をした上で、本システムの運営業者に依頼して、事前登録した問題文を、「本番環境への適用」と呼ばれる内部的プロセスを経て、試験サーバーに送り込む必要がある、ということになっている<sup>①</sup>。

これは、あたかも、従来の紙試験において、試験問題の印刷と封入のプロセスすらも、目の届かないところで、すべて試験代行業者に任せてしまうのとほとんど同じ状態を招来することになってしまう。この仕組みにより、本システムの運営業者は、かなり前から試験問題を読み取ることができてしまうのである。これは、機密性に対する重大な懸念となり得る。

現状では、本システムにおいては、試験実施主体自らの視点においても、すべての受験者の視点においても、事前登録を必要とする問題文が、試験の直前まで不正に流出しているのではないかという疑惑を取り去ることができない。受験者の立場を想定しても、また、試験実施主体の経営者の立場を想定しても、従来型紙試験と比較して、これでは機密性の面でかなりの不安があることになる。試験実施主体の経営者は、試験問題の流出の可能性を最大限予防・排除する措置を講じている旨の説明責任を、当該試験の公平性・公正性を信頼して自らの人生を決定する可能性がある試験を受験することを決意した全ての受験者に対して、果たさなければならない立場にある。また、試験の公共性に鑑みると、そのような説明責任は、社会に対しても同様に存在する。これらの説明可能性を、従来型の紙試験と同等程度に維持しなければならない。さらに、万一の問題流出があった場合に、試験実施主体の責任が社会的非難の対象となるかどうかは、試験実施主体が頭脳を最大限に駆使して合理的に不正発生の可能性を排除しようとして努めていたか否かで左右される。ところが、現行の本システムの現在の事前問題文登録を強いる仕様により、残念ながら、このような不正発生の可能性を排除できない。

本記事を執筆するにあたり、評価者は、もちろん、個人的には、本システムの運営業者を大いに信頼している。決して、本システムの運営業者の信用に問題がある

---

<sup>①</sup> 本システムの「主催者ビルド管理画面マニュアル\_ver1.1」より

という訳ではない。そうではなく、本システムを用いることを決定した試験実施主体の視点において、前記のような不正排除を行なうべくして行なっていたという説明責任を果たすことができる水準を維持できる状態に至っていないという点が、問題である。これは、大いに改善を要する事柄である。

#### (4) それでは、ひとまずどのように改善すれば良いか

上記の問題の原因は、本システムの仕様において、試験実施主体による事前の問題登録を必要とし、その後本システムの運営業者による「本番環境への適用」と呼ばれる前処理プロセスを必要とする点に存在する。これが、試験実施主体がかなり前に試験問題を前もって業者に対して全面的に開示しなければならない（すなわち、無防備な時間が発生する）ということの原因となっている。

改善方法は簡単である。試験実施主体は、いつでも本番の問題文が登録でき、本番システムにこれが反映できるような仕組みにすれば良い。そうすれば、試験実施主体は、機密性が最も高い試験の問題文を、試験開始直前に登録することになり、試験代行業者の内部者によって問題文が持ち出される可能性がある無防備な時間を、最短化することができるのである。

この方法は、在宅型 CBT 試験システムであれば利用できる。しかし、試験会場が全国に分散しているタイプの集合型 CBT 試験システムの場合、試験実施主体が問題文を試験開始数分前に業者に渡しても、システムが高度にネットワーク化されていないと、その問題文を配信することができない。

#### (5) 試験直前までの問題文暗号化手法

それでは、どうすれば良いのだろうか。直前の問題文の注入とは別の有効な方法は、問題文を予めシステムに登録しておくものの、その登録データは試験実施主体によって予め暗号化されている状態とし、その復号化キーは試験実施直前に別の方法で投入または配布するというような暗号化技術を用いた機能を実装する方法である。

この手法では、問題文を前日とか 1 週間前とかに事前に余裕をもって登録しておくことができるので、試験開始日の運営ミスが発生するリスクを大幅に削減することができる。復号化キーをどのように配布するかが問題になるが、これは、試験開始直前 (数分前など) に何らかの方法で明らかにして、これを試験システムに対して投入するか、または、別の手段によって受験者全員に対して一斉に配信する (インターネットを利用する方法もある。試験実施者自らが運営する冗長化された Web サイトに復号化キー文字列を掲載しておき、その文字列が、特定の時刻になったら表示できる状態にするというものである。) 等の方法で、ほとんど確実に実現することができる。

このような試験直前までの問題文暗号化手法は、試験開始前においてもシステム上で試験問題の表示結果をプレビューすること必要な場合がある。ただし、問題文暗号化手法を用いる場合、プレビュー機能における復号化は、必ず、試験実施主体のローカル端末上の演算で、これを行なう必要がある。復号化キーは、いかなる時点においても、試験開始前は、システム運営業者の手元に送付されてはならないのである。なぜならば、システム運営業者はその復号化キーを用いて、事前投入された問題文を復号化してしまえるためである。よって、このような機能を実装するとしたら、復号化機能は JavaScript を用いてローカルの Web ブラウザ上で動作するような仕組みにしなければならない。そして、復号キーや復号後の問題文データが、いかなる時点においても、試験サーバーに流れ出ないことを、試験実施主体が自ら確認できる手段が提供されなければならない。とはいっても、それらの実装は、それほど難しいことではないであろう。

### 3 パブリッククラウド運営業者の関係者による不正のリスク

第 1 章第 2 節 3 で述べたように、パブリッククラウド運営業者の経営者やシステム上の権限を有する被用者たちは、当該パブリッククラウド基盤上で動作しているすべての仮想サーバーについて、完全な支配権を有する。これらパブリッククラウドの管理者たちは、仮想サーバーが有するメモリの内容や、仮想ハードディスク等のストレージのデータの内容を、自由自在に読み書きすることが可能である。

したがって、試験実施における機密性の保護（問題文流出の防止）を確実にするためには、パブリッククラウド運営者の関係者による不正のリスクを考慮しなければならない。

このリスクの緩和は、前節におけるシステム運営者の関係者による不正のリスクへの対策と同様の手法で実現できるので、容易に実現できる。

すなわち、問題文の試験開始直前の登録手法または試験直前までの問題文暗号化手法が本システムにおいて実現できるようになったならば、パブリッククラウド運営者も、試験開始よりも随分前の時点で、問題文を不正に事前に読み出すことはできなくなる。

## 第 3 節 完全性に対するリスク（在宅型・集合型の両方）

### 1 試験システムにおける完全性とは

試験システムにおいて要求される完全性のうち、最も重要なことは、受験者が試験終了時に試験サーバーに対して送付する答案データが、試験終了後には、決して何者によっても改変されないことを、システムの的に保証することである。

なぜならば、仮に不正な内通者によって試験終了後にも答案データの書き換えが可能になれば、不正受験者は容易に満点を取ることができてしまうためである。

### 2 システム運営者の関係者による不正のリスク

#### (1) 概説

完全性に対する最大のリスクは、前述の機密性のリスクに関する解説でも述べたように、システム運営者の経営者またはシステム上の権限を有する被用者たちによる事後的な不正な答案データの書き換えが、技術的に可能な点にある。そして、この問題の本質は、試験サーバーを試験代行業者が完全な支配下で運営してしまっており、試験実施主体は内部的不正行為を見抜くことができないという点にある。

答案データの書き換えは、試験が終了してから一定の時間的間隔を経た後に行な

われることが多いと考えられる。したがって、試験終了時に受験者が送付した答案データの内容を確定し、それ以降にデータが改ざんされることを防止する仕組みの完備が必要である。

従来の集合型紙試験においても、マークシート用紙や答案用紙の内容を、後から試験運営代行業者の経営者または被用者達が、受験者からの嘱託を受けて書き換えるリスクは存在する。このリスクは、回収したマークシート用紙や答案用紙を代行業者が物理的に占有している時間に比例して増大する。そこで、試験実施主体は、試験終了後、できるだけ早く、マークシート用紙や答案用紙の引渡しを受け、それ以降は自らこれを自身の設備で保管することが重要であった。

これと同じように考えれば、CBT 試験においても、試験終了と同時に答案データが試験サーバーに送付されたときは、できるだけ時間的間隔を経ずに（理想的には瞬時に）、試験実施主体がその答案データを確保することができる仕組みが必要である。

ただし、仮に何らかの業務フロー上の事由により、試験終了後一定期間は試験実施代行業者の手中にのみ答案データが存在することが必要なケースも存在するかも知れない。この場合は、その間にデータが改ざんされていないことを確実に検証することができる仕組みが必須となる。

データが改ざんされることを防止する仕組みとして、試験システムにおける内部的な各種のセキュリティの仕組みは、全く役に立たない。なぜならば、システム運営業者の経営者またはシステム上の権限を有する被用者たちは、試験システムそのものの挙動を自由自在に変化させてしまうことができるためである。

監査もほとんど役に立たない。監査は、試験システムそのものに備わった各種のセキュリティ機構（ログ保存等）の完全性を前提として行なわれるが、権限がある内部者たちは、これらのセキュリティ機構に予め穴を空けたり、保存されたログ等を一部消去したりすることが物理的に可能であるためである。

よって、データが改ざんされる仕組みは、外部的な（すなわち、システム運営業者以外の第三者または試験実施主体本人によって確実に提供される）何らかの改ざん防止機構によって実現されなければならない。

## (2) 試験サーバーにおける答案データ受け取り直後に直ちに試験実施者に答案データまたはそのハッシュ値を送信する方法

試験終了の瞬間に試験サーバーが受験者から受け取っている答案データが改ざんされることを防止するためには、いくつかの有効な方法がある。

第一の手法は、最も簡単な方法である。試験サーバーが受験者から答案データを受け取ったら、直ちに、試験実施者に対して、その答案データそのものを送付する手法である。送付の手法はさまざまなものがあるが、瞬時に送付する必要があるので、電子的でなければならない。試験実施主体としては、試験代行業者に対して、インターネットを経由した何らかの通信チャネルを用いた送付を行なうことを義務付ければ良い。たとえば、試験実施主体の側で完全な支配権を有する HTTPS サーバーやメールサーバー等への答案データの送付等の方法が考えられる。この通信チャネルにおける機密性、完全性、可用性のセキュリティ対策は、別途具備する必要がある。

送付は、答案データそのものでなくともよい。十分な強度を有するハッシュ関数を用いたデジタル署名結果でもよい。最も簡単な実装としては、答案データを CSV 形式等に変換したテキストデータを SHA-2 等でハッシュし、そのハッシュ値 (数十文字程度の短い文字列である) を、試験実施主体に対して、直ちにメールで送付する等でも、改ざん防止の手法としては、かなり有効である。なぜならば、そのハッシュ値の送付は、少なくともその時刻において、答案データはそのハッシュ値を有していた (そして、その他のハッシュ値を有していることはなかった) という旨が、試験代行業者によって宣明されることを意味するためである。その後、試験代行業者が特定の受験者の答案データの書き換えを行なうと、ハッシュ値が変わるので、試験実施主体は、試験代行業者に対して、改ざんがあったとみなし、責任追及することができる。このような責任関係における統制を行なっておけば、試験代行業者の内部者に対して、不正な答案データの事後的書き換えを諦めさせることができる。よって、不正の発生を予防できる。

### (3) 試験サーバーにおける答案データ受け取り直後に直ちに外部の信頼できるタイムスタンプ署名を施す方法

第二の有効な方法は、試験サーバーにおける答案データ受け取り直後に直ちに外部の信頼できるタイムスタンプ署名を施しておき、試験実施主体が、時間的間隔を経た後に試験システムにログインして答案データをダウンロードした上で、そのタイムスタンプ署名を検証することができる状態を保証させる方法である。

この場合、タイムスタンプ署名を行なう主体（認証局）は、第三の独立した信頼できる認証局である必要がある。試験代行業者のタイムスタンプサーバーではいけない。自分で設置したタイムスタンプ署名サーバーの時計は、極めて容易に変更できるためである。

このタイムスタンプ署名は、われわれの物理社会において運用されている、「確定日付」の仕組みと同様である。確定日付というものは、書類を公証人役場に持っていくと、日付が記載された公証人の印鑑の押印を受けることができるという公的サービスである（ただし、確定日付は日付しかスタンプされないので、試験答案データのような、確定時刻までが重要であるケース（試験終了後に間髪を入れずにタイムスタンプが押されたことを保証しなければならないケース）では、有効性に乏しい。）。

タイムスタンプ署名による改ざん防止の手法は、それなりに有効であるが、厳密に考えると、実はこれには大きな落とし穴がある。タイムスタンプ署名は、あるデジタル文書がその日時に確かに存在していたことを証明するものであるが、そのデジタル文書の一部を書き換えた他のデジタル文書がその日時に不存在であったことを証明することはできない。すなわち、署名対象文書の唯一性が証明できないのである。

したがって、たとえば、試験問題が 3 問で、回答選択肢が 1 か 2 のマークシート方式であった場合、存在し得る答案は「111」, 「112」, 「121」, 「122」, 「211」, 「212」, 「221」, 「222」の合計 8 通り存在する。この 8 通りの答案について、不正を働く者は、タイムスタンプ署名をそれぞれ得ることができてしまう。そして、後で正答が分かった場合に、正答となった答案データとタイムスタ

ンプ署名とを試験実施主体に提出し、それ以外の答案データは隠滅するという不正が可能になる。

このようなタイムスタンプ署名に関する抜け穴は、問題数が増えたり、回答選択肢がより多かったり、自由記述入力欄が存在する試験問題であっても、やはり存在する。正解の自信がない問題の答案（甲乙のいずれかが正しそうだが、どちらが正しいか分からない状態の答案）において、あり得る可能性がある答案データすべてを作り出し、すべてについて、それぞれ独立したデータとしてタイムスタンプ署名を施しておけば、後から正答が分かったときに、最も得点が高くなる答案データとそれに対応するタイムスタンプ署名だけを取り出して、そのみが最初から存在しましたというような顔をし、試験実施主体にそれを引き渡すという不正が可能になる。よって、タイムスタンプ署名を過信することはできず、試験実施主体としては、この抜け穴の可能性を常に意識しなければならない。

#### (4) 即時送信手法とタイムスタンプ署名手法との複合手法

答案データの完全性を実現するための前記の第一の手法（即時に試験実施主体に送信）と、第二の手法（タイムスタンプ署名の取得）とは、いずれもそれなりに有効であるが、完全ではない。

第一の手法の欠点としては、試験実施主体が送信を受ける際に受領するサーバーやメールアドレス等との間の通信チャンネルに不具合があった場合、試験実施主体がリアルタイムに受け取れない可能性が存在する。後から再送してもらえば良いが、その時点で、すでに答案データが改ざんされている疑いを拭うことはできなくなってしまっている。

第二の手法の欠点は、先に述べた通り、内通不正受験者のいくつかのパターンの答案を作り出し、すべてタイムスタンプ署名を施した上で、最も得点が高いもの1つを提出できるという可能性である。

いずれの欠点もカバーする第三の手法を考えてみたが、著者としては、なかなか思い付かなかった。そこで、今のところの最善策としては、試験実施主体が第一の手法と第二の手法の両方を実施することを試験代行業者に契約上義務付けること

が一応の対策であると考えられる。なぜならば、これら 2 つのセキュリティメカニズムを具備させたならば、試験代行業者の側における不正内通者は、自らこれらを両方いかくぐって不正行為を行なおうというリスクがかなり高くなり、発覚の危険が増し、よって、不正行為が抑制されるためである。また、試験実施主体の側の受験者に対する公平・公正性の維持の責任について考えても、現在の技術的水準で行ない得る対策はすべて行なっていたと説明することができるようになり、それを超えた予期せぬ不正がなされても、そのことについては非難を一応免れることができると考えられるためである。

#### (5) 本システムも答案データ改ざん防止機能を具備するべきである

ところが、本システムには、本システムの運営業者そのものの関係者（役員、システム上の権限を有する被用者等）による答案データの不正改ざん防止の仕組みが見あたらなかった。上記の第一の手法も、第二の手法も、またその他に有効であると思われる手法も存在しないようである。

すなわち、試験実施主体の視点から見ると、本システムでは、試験終了後、答案データは、一定の期間、完全な無防備な状態に置かれてしまう。これから、本システムが、従来型紙試験と同等程度の重要な試験を担うことができるような状態を実現するためには、本システムの運営業者そのものが不正受験者と内通して実施し得る改ざんを防止するための完全性保証の仕組みを、確実に具備するべきである。

もちろん、現行システムにおいても、試験終了後、試験運営主体が、できるだけ時間的間隔を空けずに管理画面にログインをして答案データをすべてダウンロードすれば良いのではないかという反論も考えられる。しかしながら、その反論は、有効ではない。なぜならば、システム管理権限がある者は、試験終了後に、試験運営主体が、できるだけ時間的間隔を空けずに管理画面にログインをして答案データをダウンロードしようとした際、内通不正者は、管理画面へのログインやダウンロード等の際に、一時的に自然なシステムエラーを発生させる等して、ある程度の時間を経て再試行すべき旨を案内することが、容易にできてしまうためである。そのようなシステム上の一時的不具合は、各種のシステムにおいて日常茶飯事であるの

で、試験実施主体は、その案内を信用して、しばらく待って再試行するであろう。再びログインすると、今度は答案データがダウンロードできる状態になっているのである。この状態で、その時点ですでに答案データが改ざんされている可能性があるという訳である。これでは、試験実施主体としては、すでに、完全性が維持されていることをすべての受験者（公的試験であれば、社会全体）に対して保証できない状態に陥ってしまっていることになる。

よって、現行システムの流れは、答案データ改ざん防止の面では不十分であり、前記のような第一の手法や第二の手法、その他の有効な手法により、客観的な改ざんの一応の防止措置を実現する必要があるということができるのである。

# 第4章 考察とまとめ

## 第1節 試験における不正行為の防止の重要性

試験は、極めて重要な社会的行事である。公平・公正性の実現のために、不正行為の防止が特に重要である。

不正行為は、試験の開始前（試験問題の漏えい等）、試験中（不正情報摂取、替え玉受験等）、試験終了後（答案データの改ざん等）の3つの段階で行なわれ得る。これらの不正行為は、受験者本人、または受験者と内通している試験実施代行業者の関係者等によって行なわれ得る。

したがって、試験実施主体としては、数々の不正行為防止手法対策を、自ら講じる必要がある。仮に試験代行業者と契約して一部の試験業務を代行させる場合でも、受験者との契約上、受験者に対して公平・公正な試験を実施する責任を負っているのは試験実施主体そのものであるから、試験実施主体自身が、試験代行業者の実施する試験システムについて、積極的にその仕組み、原理、手続き、内部的実装等を調べて、よく点検する必要がある。

試験実施主体は、その名のとおり、試験の主人である。したがって、主人としての行動が求められる。使用人（履行補助者）に過ぎない試験代行業者に、このような最も重要な点を任せきりにすれば、代行業者は、必ずや、さまざまな点で安楽さやコスト削減を狙い、本質的問題を解決せずに試験実施主体に対してこれを覆い隠すことにより、問題が存在しても存在しないように見せかけてしまう（これは、プリンシパル=エージェント問題である）。

これでは、試験実施主体は、主体としての責任を果たしたことにはならない。そこで、試験実施主体の側としては、試験システムの動作原理や付随する技術について、一定の水準の知見を維持した上で、各種の現実的な不正行為のリスクをできるだけ多く列挙し、これら不正行為に対する防止手段を、試験代行業者と一体となり、または試験代行業者よりもさらに一歩進んで考案・検討し、これを試験代行業者に対して、確実に実施させなければならない。

## 第 2 節 不正防止機能の必要性と本システムに対する考察

### 1 CBT 試験における集合型紙試験と同等程度の不正防止機能の必要性

これまでの集合型の紙を用いた試験の実施者は、長い紙試験の歴史と蓄積された豊富な試験実施ノウハウを有してきた。また、試験会場が物理的な集合会場で実施されてきたことから、試験中の物理的視認性が高く、試験会場における受験者同士の相互監視関係の自然的形成も相まって、物理的に不正が困難であり、さらには、試験問題用紙も答案用紙も物質的に手に取って確認・確保することができる状態で室内に存在したから、各種の不正行為を防止するための手法は、比較的容易に講じることができた。

ところが、これらの試験実施主体は、今や、コンピュータやインターネットを用いた各種の CBT 試験 (集合型であっても、在宅型であっても) に置換されようとしている。CBT 試験を用いることにより、試験実施主体として、大幅なコスト削減が可能である。また、受験者の側としても、特に在宅型 CBT 試験が利用できれば、朝早くから遠方の試験会場へ赴く必要もなくなり、試験そのものに集中することができる等、得ることができる利益は大きい。

このような利点が強調される CBT 試験を用いるとしても、それにより、従来型の紙試験と比較して、不正が容易になってしまえば、本末転倒な結果となる。試験実施主体の責任としては、すべての不正を防ぐことができないとしても、少なくとも、従来型の紙試験と比較して同等程度の不正防止措置を講じているといえる状態を維持することが必要となる。すなわち、従来型試験と比較して、CBT 試験における不正行為が、不正実施者の視点からみて、(a) 簡単に、(b) 低コストで、または (c) 発覚しづらく実施できる状態にあってはならないということである。

## 2 CBT 試験システム（在宅型・集合型の両方）の試験問題の機密性と答案データの完全性に関する関係者による不正防止の必要性

### (1) 概説

CBT 試験においては、試験の重要なプロセスである、問題用紙の機密管理、試験直前の配布、試験中の不正行為の防止、試験後の内通者を通じた答案用紙の改ざん等の各種過程が、高度・複雑なコンピュータシステムの中に埋没してしまう。そして、そのコンピュータシステムは、試験実施主体の手を離れ、試験実施主体からほとんど検証できないブラックボックスである、試験実施代行業者（CBT システムの開発・運業者）に完全に支配された状態で稼働するケースが多くなる。試験実施代行業者の経営者やシステムに関する権限を有する被用者たちは、自らが完全に支配・管理するシステムについて、その挙動を自由自在に変更することが可能な立場にある。この権限が秘かに濫用されれば、試験問題の事前の読み出し、試験中の特定の内通受験者に対する便宜の供与、試験後の内通受験者の答案データの書き換え等を行なうことができる。これに対する監査は、役に立たない。当該システムに内蔵された監査記録手段を用いて実施される以上、システムそのものを書き換えることができる権限がある者の行為について、実効性のある監査の仕組みは、原理的に存在し得ないためである。

したがって、受験者の人生に影響を与える程度の重要な試験を実施する試験実施主体としては、試験実施代行業者の提供する CBT システムを利用する場合には、問題文の投入を試験直前に行なうか、予め暗号化しておいた試験問題を事前に投入しておき、試験開始直前に復号化キーを配布するというような措置を講じる必要がある。そして、試験終了後には、間髪を入れず、直ちに答案データの引渡しを求めるか、または改ざん防止のためのタイムスタンプ付きデジタル署名等のセキュリティ技術を導入するかを試験実施代行業者に要求する必要がある。これらの不正防止のための工夫が措置されれば、従来型の集合型の紙ベースの試験と完全に同等とまではいかなくとも、おおむね近い水準の試験問題の機密性と答案データの完全性を確保することができる。これにより、試験実施主体が受験者および社会に対して求められている責任を果たすことができる状態が実現できる。

そうすれば、試験実施主体としては、考えられるリスクの高い不正を列挙した上で、考えられる合理的・現実的な技術的対策手段を施していたと言えれば、万一それをかいくぐる不正が行なわれてたとしても、受験者たちからの非難または社会的非難は、かなり緩和することができる。

## (2) 本システムの評価結果

ところが、本文書で評価対象とした CBT 試験システム製品（「本システム」）においては、前に詳しく述べたとおり、試験問題の機密性を紙試験と同等程度に確保する仕組みが、現状、必ずしも十分とはいえない状態にあった。

本システムでは、仕様上、試験実施主体は、試験開始よりもある程度前の時点で、試験問題をシステムに投入した上で、業者に対して手動による「本番環境への適用」プロセスを実行するよう依頼する必要がある。

したがって、業者は、試験開始よりもかなり前の時点で、試験問題を入手することができてしまう。

また、本システムにおいては、答案データの完全性についても、前に詳しく述べたとおり、紙試験と同等程度に確保する仕組みが、現状、必ずしも十分とはいえない状態にあった。試験終了時に試験サーバーが答案データを受け取った時点での答案データの改ざん防止措置が存在しないのである。

これでは、試験実施主体の視点からみて、従来の紙ベースの集合試験と比較して、機密性・完全性の両方の点で十分な不正防止措置が実現できない。

そのため、本システムにおいて、今後、社会的に重要な各種試験が公平・公正に実施できるようにするため、将来、この点で何らかの対策が追加的に講じられることを強く期待したい。

### 3 在宅型 CBT 試験システムにおける試験中の受験者による不正情報採取や替え玉受験等の不正防止の必要性

#### (1) 概説

CBT 試験のうち、特に在宅型 CBT 試験システムにおいては、試験中の受験者による不正情報採取や替え玉受験等に対する不正防止措置が具備されていることが必要となる。たとえば、受験者の PC に接続された Web カメラ等による受験中の受験者の目線や行動等の監視である。これらの在宅型試験における不正防止措置は、在宅型である以上、集合型試験における会場での不正防止措置（試験監督者の配置と視覚的な会場の注視）よりも、不正が、より困難に、高コストに、そして、不正行為が発覚しやすい状態が維持されるようなシステムでなければならない。

このような在宅型受験者の監視システムは、Web カメラの監視映像を試験サーバーに送付し、試験サーバー側で、AI を用いて、または人間による目視で不正被疑点を検出し、これを最終的には試験実施主体自らが確認して、不正行為の有無を判断するという手法によって実現される。

#### (2) 本システムの評価結果

ところが、本文書で評価対象とした CBT 試験システム製品（「本システム」）の不正防止機能を検証した結果、以下のようないくつかの方法で、監視カメラによる不正行為監視をすり抜けることが、実際に可能であった。

- (1) 監視カメラの映像送信のうち一部を、その通信について、自作した SSL 中間者攻撃プロキシを用いて妨害することで、その間の不正行為の様子の映像は一切試験サーバーに送付されず、かつ、試験サーバー側でもその映像の欠落の様子を含めて何らアラートが表示されず、試験実施主体は、映像が欠落していることに気付くことが困難な状態であった。また、AI による記録映像分析結果として、「正常受験」という判定が自動的になされ、不正実施が見逃される結果となった。他方で、試験画面の表示や答案データの提出等の試験そのものに関する通信は正常になされ、試験は正常に完了

してしまった。

- (2) (1) と同様の監視カメラの映像送信の通信は、SSL 中間者攻撃よりもさらに簡単な方法で妨害できた。通信経路 (受験者の自宅のインターネット回線やルータ、WiFi 等) を意図的に混雑させることで、おおむね 65% 程度のパケットロスが生じる状態に維持すれば、試験そのものの実施のための HTTPS の通信は成功させ、監視カメラ映像の送付は失敗させるという状態を作り出すことが容易にできた。
- (3) 西暦 2000 年台に発売された安価・低画質な 10 万画素 CMOS カメラを引っ張り出してきて、受験者 PC 側の Web カメラとして用いることにより、その解像度の低さと、ピントのぼけとをうまく利用することができ、不正目線を AI に検出されない程度に画質を低くして、かつ、映像の不鮮明さが異常受験であると AI に判定されない程度の一定の画質を維持することにより、目線を大きく画面外に出して不正情報撮取を行なうことに容易に成功した。
- (4) 受験者 PC における試験システム画面のアプリ (Web ブラウザ) とは別のプログラムを実行し、当該別のプログラムで CPU 負荷率を極端に引き上げることで、試験システムアプリから試験サーバーに対する Web カメラ映像のコマ落ちを激しくさせ、この間に不正行為を行なう様子が撮影・捕捉・AI 検出されない状態を作り出すことに容易に成功した。
- (5) 受験者 PC から試験システムに対して送付されるカメラ映像送付データを、SSL 中間者攻撃プログラムを用いて、事前保存したものに置き換えることにより、試験中の不正行為を一切撮影されない状態を作り出し、かつ、試験サーバー側には試験時間一杯 (50 分間など) の映像データが蓄積され、これを AI が判定しても、人間が判定しても、不正行為がなされていない

ることが全くわからない状態を作り出すことに容易に成功した。

- (6) 2枚のモニタをうまく重ね合わせて、奥側のモニタで不正に情報摂取（Web 百科事典や過去問の閲覧等）を行なう際の目線の動きを自然にし、AI による不正目線検出から逃れ、正常受験結果判定を得ることに容易に成功した。

上記のような各種不正手法は、不正受験者が自宅の PC やネットワーク環境において行なうことができる手法である。したがって、不正発覚のリスクはとても低い。また、これらのいくつかの手法では、SSL 中間者攻撃のプロキシ型プログラムと呼ばれるものを利用している。このプログラムは、今回、評価者が本システムを欺く目的のためだけに作成した特注プログラムである。しかし、開発には合計で 2、3 時間しかかからなかったため、開発コストはせいぜい数万円程度である。また、これは、任意の受験者の PC 上で動作させることが可能である。インターネットにこのようなプログラムがオープンソースとして出回れば、不正受験者は知識がなくてもこれを (a) 簡単に、(b) 無料で、(c) 発覚のリスクがほとんどなく利用することができる。

よって、不正受験者は、上記の手法により、本システムを用いた在宅型 CBT 試験において、不正に満点を取ることができることになる。

### (3) 対策方法

そこで、試験実施主体の視点として、上記のような不正受験に対する対策を考えてみたところ、上記のような各種不正行為に対する対策については、いくつかの技術的手法を組み合わせれば、かなりの範囲の不正防止が可能になると考えられるのである。例えば、以下のような不正防止手法が実装し得る。詳しくは、本文書における第 2 章のそれぞれの検証結果のところ述べておおりである。

- (1) ワンタイムパスワード等を表示したスマートフォン等を受験中の試験者

の左右または背後に設置するなどして、映像の差し替えを困難にする手法。ただし、受験者の側で追加設備が必要になる。

- (2) 試験中に画面指示に基づきワンタイムパスワード等を読み上げさせる方法。ただし、集中阻害がされ、紙ベースの試験と比較して、受験者にとって不利益な結果となる。
- (3) 試験中に画面に色鮮やかな大きな塗りつぶしを次々に表示し、受験者の顔面にその色がそのタイミングで変化することをカメラで確認する方法。ただし、(2)と同様に大きな集中阻害につながる。
- (4) スマートフォン等で第二の監視カメラの設置を受験者に要求し、これは受験中の様子を背後から撮影させる方法。ただし、受験者の側で追加設備が必要になる。

ただし、仮に上記のような将来の対策方法を実施したとしても、受験者の PC を代行して操作する替え玉受験等がなされた場合は、それを見抜くことは困難な場合がある。考えられる替え玉受験の手法は、第 2 章第 3 節 5(2)で詳しく述べた。

本システムにおいて、今後、社会的に重要な各種試験が公平・公正に実施できるようにするため、将来、不正防止の観点においても、何らかの対策が追加的に講じられることを強く期待したい。しかし、そのためには、技術的進歩が必要である。

その技術的進歩は、本システムの開発業者のみが考えることではなく、後述するように、真に良い試験を実施したいと切望する試験実施主体において、これから、その職員たちの技術力や創造力が発揮されることにより、具体的に考案され、自然発生的に実現され得るものであると考える。

## 4 インターネットやクラウドサービスを用いる場合の CBT 試験システムの可用性の実現の必要性

### (1) 概説

試験は、受験者の人生を左右するものである。受験者に責任がない原因によって、試験の開始時に試験にアクセスができなかったり、試験実施中に試験が中断されたりすることがないように、試験実施者は、採用する試験システムの可用性の維持について、最大限の努力を払わなければならない。試験システムが試験代行業者によって運営されるものであれば、当該業者に対して、可用性を実現する手段を講じることを要求し、技術的に可用性が真に実現できていることを検証しなければならない。

CBT システムは、サーバー / クライアント方式のコンピュータシステムを利用するので、試験サーバーの冗長化が重要となる。加えて、在宅型の CBT システムは、インターネットを利用するので、インターネット通信経路の冗長性が重要になる。インターネット接続経路に付随して、ドメインにおけるホスト名を IP アドレスに変換するための DNS 権威サーバーと呼ばれる機能も冗長化する必要がある。

そして、確実な冗長性の実現にあたって、外注のサーバー提供事業者、ネットワーク回線提供事業者および DNS 権威サーバー提供事業者（近年では、パブリッククラウド事業者がこれらを合わせて提供していることが多い）を活用する場合は、単一の事業者のシステムは同時にダウンし復旧に 1 時間以上を要することがしばしば発生していることから、必ず、異なる 2 以上のパブリッククラウド事業者等に跨がって冗長化を図る必要が生じる。

### (2) 本システムの評価結果

ところが、本文書で評価対象とした CBT 試験システム製品（「本システム」）においては、試験サーバーの冗長性、インターネットとの接続のためのネットワークシステムの冗長性、および DNS 権威サーバーの冗長性のいずれの点でも、冗長化が不十分であった。

- (1) 本システムの試験サーバーについては、単一のパブリッククラウドブランド (GCP: Google Cloud Platform) を提供する単一事業者 (米国の「Google LLC」という有限責任会社) への依存がみられた。大手海外系パブリッククラウド事業者においては、全アベイビリティゾーン、全リージョンにおけるソフトウェアや基盤システムが同一であることにより、これらのソフトウェア等の不具合により、全アベイビリティゾーン、全リージョンを巻き込んだダウンがいつでも発生し得るし、実際に、復旧に数時間を要することもある。よって、異なるソフトウェアや基盤システムによって互いにリスクが隔離された、異なる 2 以上のパブリッククラウドにまたがって冗長化することは容易であるが、本システムは、これを実施していなかった。重要な試験において障害が発生した際に復旧までに数時間または数日間を要したとすれば、試験実施主体は、簡単に実施できる冗長化の対策が不十分であったとして、強い社会的非難を免れない結果となる。
- (2) 本システムの試験サーバーがインターネットに接続される際の経路においても、(1) のサーバーそのものの GCP への依存関係から、必然的に、GCP のみに依存する状態となっていた。これによって発生する問題は、(1) と同様である。
- (3) 本システムの DNS 権威サーバーは合計 4 台存在するが、GMO インターネット社の「お名前.com」ブランドのレンタル DNS サーバーサービスであると思われる DNS サーバーによってホスティングされており、すべて、同一の AS (インターネット上の独立自律ネットワーク) に収容されてインターネットに接続されていた。この AS で障害が発生したり、DNS サーバー運営基盤でハードウェアまたはソフトウェアの不具合が発生したりすると、本試験サーバーの IP アドレスが不明となり、受験者は、試験サービスのサーバーにアクセスできなくなる (実際に、同 DNS サービ

スは、過去に復旧まで 1 日程度を要する障害を起こしている。)。一度試験が開始した後も、ページめくりや答案送付の都度、試験サービスのサーバーとの通信が発生し、必要に応じて DNS が参照されるので、試験開始前と試験中のいずれの状態でも、DNS 権威サーバーがダウンしないように、冗長化を施す必要がある。DNS 権威サーバーの冗長化は、2 以上の複数のパブリッククラウドを用いれば、容易に、かつ低コストで実現できる。

(1), (2), (3) のいずれも、マルチクラウドと呼ばれる方式で、複数のパブリッククラウド事業者にまたがる形での冗長化を図ることが、容易に可能である。

本システムにおいて、今後、社会的に重要な各種試験が確実に実施できるようにするため、将来、可用性の観点においても、何らかの対策が追加的に講じられることを強く期待したい。

### 第 3 節 まとめ

試験実施主体は、受験者に対して、機密性・完全性・可用性が保たれ、かつ、公平・公正性が保証された試験の確実な実施に関する責任・権限・能力を有している。

従来の集合型の紙試験においては、試験実施主体は、さまざまな工夫を凝らして、組織的にノウハウを蓄積し、これらの責任を果たしてきた。従来の集合型紙試験には、長い歴史がある。例えば、記録によると、中国では西暦 598 年 (隋時代) に、「科挙」と呼ばれる集合型紙試験が開始されたが、これは、1,300 年間以上にわたり続いている。その間、各種の不正行為の試みが発見され、都度対策されてきている。このように、各試験実施主体たちは、長年をかけて、紙試験における不正行為のパターンを見出し、その予防に努めてきた。その結果、現代の集合型の紙試験は、かなり高い水準で、不正行為を防止することができている。従来の紙試験は、物理空間上の試験であり、また、人間の試験監督等の被用者を中心とした試験運営であった。そこで、試験実施主体は、物理法則や物理的な動作原理と、心理法則および

人間の行動についてある熟知した上で、不正防止を実現してきた。試験実施主体は、この点で、常に公平・公正で確実な試験の実施を担える権威・責任・能力を有していた。その力強い権威・責任・能力によって、具体的な不正防止対策が立案され、その具体的対策は、その基礎となる精神とともに、被用者や試験代行業者たちの隅々まで浸透していた。これにより、試験実施主体が主、被用者や試験代行業者たちが従の関係が構成され、主従の緊張関係において試験の精神が正しく浸透し、よって、高い品質の試験が組織的に実現できてきたのである。まさに、従来の集合型紙試験における不正防止のための各種の措置・工夫は、芸術的価値すら有している程度に、人類の知見の限界まで高められた、輝かしい知見と能力の塊であったのである。

これと比較すると、CBT 試験システムを用いた試験は、歴史が浅い。特に、在宅型 CBT 試験は、サイバー空間上で実施され、人間の試験監督等の被用者に代わりコンピュータシステムが不正を検知・防止する役割を担っている。そうすると、在宅型 CBT 試験システムを用いた試験を行なう場合、試験実施主体は、当然、サイバー空間 (コンピュータ、ネットワーク、システム、ソフトウェア) の法則や動作原理およびそれらの動作についてある程度熟知した上で、不正防止のために、リスク予測や具体的立案を行なわなければならない。そして、試験実施主体が主となって立案された各種の具体的対策は、その基礎となる精神とともに、利用しようとする試験代行業者の実装する在宅型 CBT 試験システムの隅々まで浸透しなければならない。紙試験においては、試験実施主体は、名目上も、実質上も、不正防止と公平性の担保がなされた試験の実施のために必要な力強い権威・責任・能力を有していた。在宅型 CBT 試験システムにおいても、試験実施主体は、これらの権威・責任・能力を名実共に研磨していき、ついには、前記のような芸術的知見限界水準にまで高められた集合型紙試験における不正防止にかかるそれらと同等程度のものに高めることができるのである。

そのためには、試験実施主体においては、これらの権威・責任・能力を単に名目上のものに形骸化させてはならない。すなわち、不正防止と公平性担保を、CBT 試験システムを開発・運用する試験代行業者等といった外注先に、すなわち、試験実

施主体外の第三者に、盲目的に委ねてしまってはならない。そのような盲目的依存と、担保のない信頼は、必ず、受託側業者の安楽さとコスト削減を求めた不十分な対策結果を発生させる。そこで、試験実施主体は、利用しようとする CBT 試験システムを隅々までよく光で照らして、現実的に可能な不正をあれこれと試し、システムがそれらの不正を見抜くことができなかつたならば、開発者に対して、これを速やかに是正するための技術的措置を講じてもらうことを目指して、議論しなければならない。このような、これからの創意工夫に満ちた CBT 試験の水準の引き上げプロセスを果たして、初めて、試験実施主体は、不正防止と公平性の担保がなされた試験の実施のための権威・責任・能力を名実共に確保している状態を維持することができるようになる。試験におけるそのような状態の維持は、まさに試験実施主体が社会的に存続を許されていることの条件である。したがって、CBT 試験システムを利用しようとする場合、CBT 試験システムに対する奥深い評価は、試験実施主体にとって、重要な経営問題であるといえる。

本文書は、試験実施主体が、前記の目的のために、利用しようと検討する CBT 試験システムについて、奥深く本質的な評価を加えるために参考になる情報を提供するために記述された。本文書の指摘したさまざまな不正の可能性やその実証実験結果、秘密性・完全性・可用性に対するリスク等は、本文書の評価対象とした本システムに関して、わずかな試験の結果でも、次々に見出されたものであるが、これは、本システムの市場における特段の優劣を意味するものではない。仮に試験実施主体またはそのための評価者が他の CBT 試験システムにおいて評価したならば、必ず、類似のような問題が、同じ程度に、見出されるであろう。CBT 試験システムは発展途上にあることから、このような点で、従来の紙試験と比較して色々と不十分な点も否めないのである。しかし、CBT 試験システム、特に在宅型試験システムは、試験実施主体のコストを引き下げ、受験者に利便を与える、素晴らしいシステムであるから、さまざまな問題を克服しつつ、今後ますますさまざまな試験において普及することが望ましい。

われわれ人類が、そのような未来を目指すために、今まさに CBT 試験システムを利用しようとする試験実施主体に対して、社会的に期待している役割は何である

うか。それは、優れた試験実施主体が、さまざまな CBT 試験システムを積極的に比較検討し、これらをかなり奥深くまで評価した上で、CBT 試験システムを通じて現実的に行なわれる可能性のある不正行為や完全性・機密性・可用性に対する脅威を、本文書に挙げられているような簡単に見つかるようなものをその入口として、これら以外にもさまざまに内奥を見て発見し、それらの本質を分析した上で、現在の世界における技術水準を考慮した上で、それぞれの新しい不正を防止するための新しい方法を、できれば、各 CBT 試験システム開発業者達と一体となって議論して考案していくことで、人類社会における試験という重要な社会的行事における不正対策技術や完全性・機密性・可用性の向上技術を、どんどんと進歩させていくという、輝かしい役割である。

このような、人類における試験という領域における最先端を歩む際の、高いレベルの技術進歩は、各 CBT 試験システム開発業者 1 社ずつが、単体で孤立して行なうことでは、実現困難である。各社は、自社のシステムの実装についてはよく見えていても、他社の競合システムの実装については、詳しく知る手段がない。ゆえに、すべてのベンダの CBT 試験システムを見渡して比較検討し、それぞれのシステムの創意工夫を知った上で初めて考案することができる新たな技術上の工夫を考案することができる立場にいるのは、試験実施主体自らしか存在しない。このような試験実施主体自らの、CBT 試験システムの水準を大変に進化させようとする着実な努力が、これから、徐々に行なわれたならば、CBT 試験システム業界全体の水準はどんどんと引き上げられ、現行のシステムのように、紙ベースの試験と比較してさまざまな点に容易に見つかる穴があるというような、初歩的な状態からは、早期に脱却することができる。

そして、このように、CBT 試験システムに対して深い分析と評価を加えることにより、試験実施主体に生じる、何よりも大きなメリットは、その努力過程が、各試験実施主体の経営者や内部職員において、CBT 試験システムを成り立たせる技術の動作原理と、その周囲に密接に関連するコンピュータ、ネットワーク、ソフトウェア、OS といった基礎的デジタル技術に関する必要不可欠で基本的な、デジタル時代における必須的知識を、自然に楽しみながら自律的に学ぶ機会が自動的に生

じることにつながるという点にある。

このような自律的技術習得の流れが、各試験実施主体の経営者や内部職員でいったん発生したならば、それは組織的な資本となり、試験実施の業務はもちろん、組織の経営課題を次々に解決していくことにも直接的につながり、自組織が社会からさらなる承認と支持と評価の高まりを得る状態の自然な形成にも役立ち、さらには、本来業務に付随し、または派生した様々な社会活動において、組織的に獲得したデジタル能力を活用して、創意工夫に富んだ様々な事業が展開できるようになり、組織の存続可能性と、そこに集まっている職員達の人生におけるさまざまな価値の実現を目指した創造性が、やがて、世界に対して、無限大の広がりをみせ始めるのである。

#### 【本サンプル記事について】

執筆者: 登 大遊

対象システムの検証に要した日数: 2.5 日間 (第 2 章で解説した試験システムを欺くための SSL 中間者攻撃等の必要な自作プログラムの開発を含む)

記事の執筆: 5 日間