CBT およびテストのセキュリティについて

○ 劉　東岳 (学研ホールディングス／学研教育総合研究所)

〈はじめに〉

International Test Commission (ITC、国際テスト委員会)が公開している 6 つのガイドラインのうち、本発表では次の 2 つのガイドラインの概要を示す。

- ITC Guidelines on Computer-based and Internet Delivered Testing
  (CBT ガイドライン)
- The ITC Guidelines on the Security of Tests, Examinations, and Other Assessments
  (Test Security ガイドライン)

〈CBT ガイドライン〉

本ガイドラインのリリースは 2005 年だが、これに先立ち ITC は 2001 年に「テスト利用のガイドライン」をリリースしている。本ガイドラインは「テスト利用のガイドライン」を補完する位置づけで作成され、CBT/IBT に特化した内容となっている。なお、2013 年には「テスト利用のガイドライン」の改訂版がリリースされている。

概要

本ガイドラインの内容は、大きな枠組みとして次の 4 つのセクションで構成されている。

- 技術 (Technology)
- 品質 (Quality)
- 制御　(Control)
- セキュリティ (Security)

それぞれのセクションは、さらに複数のトピックで構成されている。たとえば技術のセクションには、次の 5 つのトピックが含まれている。

- ハードウェアとソフトウェアの要件
- システムのロバスト設計
- 人的要因
- 特別な配慮を必要とする受検者への対応
- サポート・ドキュメント

それぞれのトピックでは、テストに関わる次の 3 つの立場からの視点を軸にして、具体的なガイドラインの内容が整理されている。

- テスト開発者 (Developer)
- テスト発行者 (Publisher)
- テスト利用者 (User)

また、本ガイドラインを実際に適用する場面では、テストが実施される状況やテスト結果の利用目的などを包括する概念である Testing Scenario を意識する必要がある。たとえば、ハイステークなテストとローステークなテストに対して同レベルの制御やセキュリティのガイドラインを適用することの非効率性は、比較的容易に想像がつくだろう。

本ガイドラインでは、この議論を整理するために次の 4 つの監督モードを示している。

- Open
- Controlled
- Supervised (Proctored)
- Managed

これらの監督モードは、それぞれに適切な利用状況が存在し、いずれかのモードが常に望ましいということではない。Testing Scenario と監督モードを考

慮して、現場ごとにガイドラインの適用を検討する必要がある。

モード	説明 (ガイドラインの定義を、発表者の解釈により発展させたもの)
Open	**人による監督は行われていない** 個人情報の事前登録は要求されず、受検時にIDやパスワード等の入力も求められないため、匿名で繰り返し受検することが可能。
Controlled	**人による監督は行われていない** 個人情報の事前登録が要求され、受検時にIDやパスワード等の入力が求められるが、実質的な意味での本人確認は不可能。
Supervised (Proctored)	**人による監督が行われている** 遠隔地の監督員が受検者の本人確認を行った後に、試験開始を許可する。監督員は受検の様子をモニターし、テストの適切な終了が確認可能。
Managed	**人による監督が行われている** 受検環境が標準化されたテスト会場に受検者が来場してテストを受ける。受検の際には厳密な本人確認が要求され、テスト中は監督員の見回りなどにより、カンニング等の不正受検を防止する対策がとられている。

〈Test Security ガイドラインの概要〉

本ガイドラインのリリースは 2014 年で、ITC によるガイドラインの中では、比較的新しいものだ。ICT の発展が著しい昨今、いわゆるカンニング行為を助けるデバイスの小型化、操作性の向上、また情報共有の即時性が高まる傾向が続いている。その意味では、もっと早く本ガイドラインがリリースされても良かったのかもしれない。CBT/IBT の普及が進む中、セキュリティの意識は今後ますます必要になる。

概要

本ガイドラインの内容は、大きな枠組みとして次の 3 つのセクションで構成されている。

- セキュリティ計画の策定
- セキュリティ対策の実践
- セキュリティ事故への対応

策定のセクションでは、不正受検の行為と項目窃盗の行為を分類・整理し、開発・実施運用側の果たすべき役割と、受検者側に求める責任と周知徹底の方法について、13 のガイドラインを設けている。

実践のセクションでは、テストの設計から、受検者の登録、テストの実施運用、採点、情報管理に至る全ての過程においてセキュリティを確保する具体的な方法について、25 のガイドラインが示されている。

そして、「どんなに強固なセキュリティ施策が実践されようと、不正は必ず可能で必ず発生する」という前提に従い、対応のセクションでは、セキュリティ違反が発生した場合の対応策について、10 のガイドラインを示している。

なお、テストのセキュリティに関連する特殊な用語および一般的な用語の特殊な使い方については、ガイドラインの最後に Terms And Definitions のセクションを設けている。

〈参考文献〉

International Test Commission (ITC) (2005). *ITC Guidelines on Computer-Based and Internet Delivered Testing.*

International Test Commission (ITC) (2014). *The ITC Guidelines on the Security of Tests, Examinations, and Other Assessments.*

Both downloaded on Aug. 3, 2015 from www.intestcom.org.

劉 東岳 (LIU, Dongyue Louis) DL.Liu@mmf.gakken.co.jp