# カット・ドゥ・スクエアのセキュリティに関する取組について

カット・ドゥ・スクエアは治験促進センターが定める情報システム構築の基準に加え、独立行政法人情報処理推進機構の「安全な Web サイトの作り方」にも則り構築しており、加えて物理的にも当センターが考え得るセキュリティ対策を施しております。しかし、その詳細について多くを明かすことは逆にセキュリティの低下を招くため非公開としておりますが、個別のご質問に関しましては皆様の不安を払拭すべく可能な限りご回答をいたしますので、下記の問い合わせ先までご確認事項をお纏めになりご連絡を下さい。

また、現時点で公開可能な情報につきましては当センターWeb サイト上にて公開をしておりますので併せてご参照くださいますようお願いいたします。

URL：http://www.jmacct.med.or.jp/cds/files/system/ctdos2_7.pdf

セキュリティと運用に関するお問い合わせ

URL：http://www.jmacct.med.or.jp/cds/files/system/ctdos2_7.5_qa.pdf

2011 年 11 月より株式会社日立製作所等によるカット・ドゥ・スクエアへの脆弱性診断を行いカット・ドゥ・スクエアではアプリケーション、データセンター、サーバー機器において脆弱性が無いことを定期的に確認しており今後も定期的に診断を行い、堅牢性を維持します。

**診断内容**

OWASP（The Open Web Application Security Project）の OWASP　Top10 に提示しているシステムセキュリティ上の問題が発生せずに管理できているかをこの診断により確認いたしました。この結果につきましては後日 Web サイト上にてお知らせを予定しております。

**＜参考＞OWASP　Top10 アプリケーションのセキュリティリスク-2010**

① インジェクション攻撃
② クロスサイトスクリプティング
③ 不完全な認証とセッション管理
④ 安全でないオブジェクトの直接参照
⑤ クロスサイトリクエルトフォージェリ
⑥ セキュリティの不適切な設定
⑦ 安全でない暗号化によるデータ保存
⑧ URL アクセス制御の不備
⑨ 不十分なトランスポート層の保護
⑩ 検証されていないダイレクトとフォーワード

（詳しくお知りになり方は、http://www.owasp.org/index.php/Top_10　）

お問い合わせ先

e-Mail：ctdos2@jmacct.med.or.jp

※セキュリティに関するお問い合わせは公開情報をご確認のうえ文書にてお願いいたします。

第 2.0 版（2013 年 10 月 30 日）

公益社団法人日本医師会　治験促進センター