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･スクエアのご利用検討中の皆様から、そのセキュリティ対策について不安であるとのご意見が多数寄せられております。（2010 年 CRC と臨床試験のあり方を考える会議：ランチョンセミナーアンケート、2011 年統一書式導入後調査）

当然、カット・ドゥ・スクエアは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/plan/ctdos_security.html

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/plan/files/CtDoS2QA20100921_security.operation.pdf

2011 年 11 月に株式会社日立製作所によるカット・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確認いたしました。

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 1.1 版（2011 年 12 月 1 日）
社団法人日本医師会　治験促進センター