

OpenSSL 脆弱性（CVE-2014-0224）の弊社開発製品への影響について

クオリティ株式会社

<http://www.quality.co.jp/>

OpenSSL 脆弱性（CVE-2014-224）の影響について、弊社製品の状況は以下の通りです。

製品名	バージョン	影響の有無
QND Advance	サポート対象の全バージョン	なし
QND Standard	サポート対象の全バージョン	なし
LicenseGuard	サポート対象の全バージョン	なし
QND ClientLog	サポート対象の全バージョン	なし
ISM CloudOne	サポート対象の全バージョン	あり(※1)
QGG	サポート対象の全バージョン	なし
Quality Gaaiho PDF Server	サポート対象の全バージョン	なし
Quality Gaaiho PDF Suite	サポート対象の全バージョン	なし
KeyServer	サポート対象の全バージョン	なし
DKS Plus	サポート対象の全バージョン	なし
QQR	サポート対象の全バージョン	なし
eX WP	サポート対象の全バージョン	なし
eX Report	サポート対象の全バージョン	なし
eX PDS	サポート対象の全バージョン	なし
eX IPD	サポート対象の全バージョン	なし
eX IFM	サポート対象の全バージョン	なし

※1 ISM CloudOne ご利用環境の対応方法について(2014 年 6 月 10 日現在)

・アプリケーションサーバーが「RHEL 5.x」環境の場合

[openssl-0.9.8e-27.el5_10.3]を適用してください。

ISM CloudOne システム上の影響はありませんが、サーバー運用上、セキュリティ脆弱性の対象となる可能性がありますので、修正パッチの適用をお願いいたします。

なお、修正パッチの適用に伴う ISM CloudOne システムへの影響はありません。

・アプリケーションサーバーが「RHEL 6.x」環境の場合

[openssl-1.0.1e-16.el6_5.14]を適用してください。

ISM CloudOne システムに対して影響が確認されておりますので、修正パッチの適用をお願いいたします。

なお、修正パッチの適用に伴う ISM CloudOne システムへの影響はありません。

※yum コマンドを利用した適用手順例：

Linux サーバー上で以下のコマンド実行します。

```
yum -y update openssl
```