既存PLM内のファイルを暗号化して利用

■DataClasys導入事例■

業種	機密区分	顧客のリスクと要望
機械製造メーカ	機密図面	PLMにて管理されている設計ファイルは国内外の拠点およびOEM先へも提供し製造を行なっている。 現状の仕組では社内やOEM先から図面ファイルの漏洩リスクがある。 設計業務で様々なCADアプリケーションに対応できる暗号化・DRM製品を採用し、設計ファイルの安全性を確保したい。

対策の骨子	社内、出張者、OEM先、海外子会社も含めて設計ファイルの外部流出、漏洩を防止することを最終目標にDataClasysを導入した。 設計ファイルは、PLMで管理されておりDataClasysを導入、暗号化したまま管理することとした。国内に3ヵ所、海外OEM先等2か所、出張者（海外出張も含む）にDataClasysを導入し、暗号化した設計ファイルを操作するようにした。
具体策	社内ではAutoCAD（LT含む）、手書き図面等をTIFF形式に変換後自動的にPLMに取込んでいる。（PDF形式含む）今回、PLMに取込む前にこれらの設計ファイルを暗号化し暗号化したままPLMで管理することとした。 設計ファイルは本社PLMサーバで一元管理、既存ファイルに関しては今後随時暗号化の予定。今後、他のCADアプリケーションも暗号化対応の予定。
効果	現状セキュリティの確保は、運用等で工夫する必要もあったが、製品のバージョンアップにも迅速な対応ができスムーズな運用が可能になった。 従来は相手側に渡った暗号化されていない設計ファイルが外部に送信されていたが、暗号化することにより権限のある人しか操作できないので、セキュリティレベルが大きく向上した。