

## オープンソース環境向けデータベース暗号化パッケージの提供開始

～Webアプリケーションのデータベースセキュリティをより強固にできる～

メディアスティック株式会社（代表取締役社長：宮内淑子、東京都渋谷区広尾、以下、メディアスティック）は、分割多重暗号化データベースシステム「データジグソー」を、オープンソース環境向けにパッケージ化した「データジグソー for LAMP」（以下、本パッケージ）を、5月25日より提供開始します。

2005年10月に発表した「データジグソー」は、個人情報漏洩対策として、株式会社サイバード様を始めとしてメディアスティックが構築したシステムに組み込み、各方面でご利用いただいております。

本パッケージは、オープンソース環境として広く利用されている、LAMP（ ）向けに特化し、データベースの暗号化と暗号鍵の管理とをパッケージ化することにより、データベースと連携したWebアプリケーション構築において、容易にかつ安価にセキュリティ強度を高めることができるのが特色です。

データベース内の一部を暗号化することができますので、個人情報に関わるデータのみを暗号化して秘匿性を高めるとともに、属性データ等については暗号化不要とし、検索スピードへの影響を最小限にすることも可能です。

また、各暗号鍵自体も別の暗号鍵で暗号化した上で、異なるデータベース内に保管するなど、暗号鍵の管理についても強固なセキュリティを施しています。

万一データベースへの不正アクセスが発生した場合でも、データベースが暗号化されていればデータを読み取ることができないため、最後の砦としてデータベースの暗号化は重要となります。

ところが重要性が認知されているにも関わらず、技術的なハードルの高さから、高額なデータベースソフトを使用する一部の大規模システムや、金融機関用システムなどでのみ暗号化が採用されているのが実態です。

またWebアプリケーションではコストを抑えるために、オープンソース環境を利用するケースが増えていますが、実装に必要なサポートや情報が不足しているケースも少なくありません。

メディアスティックはオープンソース環境向けに特化し、パッケージ化することにより、データベース暗号化を安価で導入しやすくしました。

本パッケージの機能は以下の通りです。

- 1 . Linux、Apache、MySQL、PHP の環境に対応しています。データベースとして PostgreSQL に対応しています。
- 2 . データベース内のデータを行 (RAW) 単位、列 (COLUMN) 単位、あるいは要素 (FIELD) 単位で、個別の暗号鍵により暗号化することができます。
- 3 . AES128 ビットを使用した専用の暗号化ライブラリにより、容易にデータを暗号化することができます。
- 4 . 暗号鍵管理システム構築のためのツールが用意されています。
- 5 . ライブラリ群は暗号化されているため、暗号化処理や暗号鍵管理も秘匿することができます。

メディアスティックは、QR コードを用いた電子商取引などをはじめとする多数の国内外特許を保有しており、分割多重暗号化データベースシステムや携帯電話を用いた個人認証システムなどのモバイル & セキュリティの先進ソリューションを提供しています。

本パッケージの価格は、CPU ライセンス 85 万円、年間保守料 20 万円、構築に関する初期コンサルテーション料は 20 万円です。

初年度は 100 セットの販売を目指しております。

LAMP : OS は Linux、Web サーバは Apache、データベースは MySQL、言語は PHP か Perl か Python を用いたオープンソフトウェアのシステム。

データジグソーはメディアスティック株式会社の登録商標です。

QR コードは (株) デンソーウェーブの商標登録です。

その他各会社の名称、各製品の名称等は、各社の登録商標です。

本件に対するお問い合わせ先

メディアスティック株式会社 <http://www.mediastick.co.jp/>

技術部：本郷

電話：03-5475-5015 / E-mail : [info@mediastick.co.jp](mailto:info@mediastick.co.jp)