個人情報などの重要データ流出を暗号化により防止

「D’Amo（ディ・アモ）」

システムプラザ株式会社

（https://www.systemplaza.co.jp）

データベース暗号化

近年、企業情報の流出などのトラブルが多発しています。これらトラブルからのリスクを回避する為に日本の企業は「外部からの攻撃への対策：外部脅威対策」へ投資を続けてきました。しかしながら近年高度化したサイバー攻撃を100%防ぐことはほぼ不可能であると言われております。また企業情報の流出は外部からの攻撃だけとは限りません。残念ながら最近の情報流出事件を鑑みると日本企業においても「企業関係者の不正：内部脅威」への対策も必要な状況といえます。
内部脅威に対しては、データベースに格納された機密性の高い情報を暗号化して「ファイルは盗まれても情報は盗まれない」状態にすることが有効な対策と言えます。
以下は、IPA（独立行政法人情報処理推進機構）が毎年発表する「情報セキュリティ10大脅威」の変化です。
内部不正による情報漏えいの脅威が順位を上げています。

順位	脅威
1 位	標的型攻撃による被害
2 位	ランサムウェア
3 位	ビジネスメール詐欺
4 位	脆弱性情報公開における悪用
5 位	セキュリティ人材不足
	・・・
8 位	内部不正による情報漏えい

2017 年

順位	脅威
1 位	標的型攻撃による被害
2 位	ビジネスメール詐欺
3 位	ランサムウェア
4 位	サプライチェーンの弱点
5 位	内部不正による情報漏えい
	・・・
	・・・

2018 年

順位	脅威
1 位	標的型攻撃による被害
2 位	内部不正による情報漏えい
3 位	ビジネスメール詐欺
4 位	サプライチェーンの弱点
5 位	ランサムウエア
	・・・
	・・・

2019 年

D'Amo（ディ・アモ）によるデータベース暗号化

主なデータベースセキュリティ対策は、「データベース暗号化」「アクセス制御」「ログ監査」の3つです。
データベース暗号化による機密性の高いデータの暗号化、職責に応じた権限の付与、ユーザのデータ操作ログを取得し不正アクセスを検知／通知する仕組みが必要となります。特にデータベース暗号化は、PCI-DSSや、HIPAA/Hitech、GDPRなど、コンプライアンスやデータプライバシーに関するほぼすべての規格や要件において、推奨のベストプラクティスとなっています。
D'Amoは、これらの機能を有した総合的なデータベースセキュリティソフトです。

■データベース暗号化
-データベース暗号化ではデータを変形し、無意味なビットに置き換えることにより、情報窃盗そのものの意義をなくし、情報漏えいの抑止力となります。
■ログ監査
-ユーザのデータ操作ログを取得し、不正アクセスを検知／通知します。
■アクセス制御
-セキュリティ管理者とデータベース管理者の操作権限分割するなど権限の一極集中を避け、職責に応じた権限を付与できます。

鍵管理

暗号化は、データを無意味な値に加工する技術です。より安全な暗号化は暗号化に加えそのカギの管理とアクセスコントロール迄実現することを意味します。鍵管理を徹底することで、大切な資産におけるよりセキュアな対策が実現できます。

低 ← 安全性 → 高

ソースに鍵を格納

外部者による情報漏洩リスク

ファイルに鍵を格納

サイバー攻撃などによる外部からの脅威

DBMSに鍵を格納

権限のない内部者による情報漏洩リスク

KMSに鍵を格納
(key management system)

暗号化鍵管理の専用ソリューション「D'Amo KMS」をハードウェアアプライアンスで別途提供しています

データベース暗号化にともなう課題

既存システム変更のハードル

既存環境への暗号化構築のためにアプリケーション開発を余儀なくされると、多くの開発者は恐れます。

データベース暗号化ソフト「D'Amo」はカラム単位で暗号化。暗号化のための追加コーディングが必要なく、既存システムに対し、修正等の影響を与えずに適用できます。暗号化や復号を意識することなく、暗号化データを扱うことができます。

透過型暗号化

- 既存システムに対し簡単導入
- アプリケーションに対し独立性

安全性の担保

データベースを安全に運用していくには、データベースへのアクセスを制御したりデータベースの稼働を監視するなどの機能が必須となります。鍵管理もしっかりなされていないと情報漏えいの恐れが発生します。

データベース管理者とセキュリティ管理者の完全分離を実現。データベース暗号化ソフト「D'Amo」はセキュリティ管理者のみ暗号化・復号の権限を付与することで、データベース管理者は復号の権限がなければ、暗号化されたデータの中身を参照することはできません。

職務分掌を実現

- 権限管理を実現

セキュリティ専門人材の不在

データベース暗号化に精通した開発担当者が不在あるいは会社を辞めたときの対応

セキュリティ専門人材は必要ありません。データベース暗号化ソフト「D'Amo」はOracleおよびMS SQL Server、「MyDiamo」ではOSSのMySQL, MariaDB, Postgreに対応。専門的知識を要さず数日で導入が完了します。また、「D'Amo」はDBのエディションを問いません。

DB Plug-In方式

- ADD-ONで暗号・復号のモジュールを導入

暗号化前後のパフォーマンス劣化が不安

データベース暗号化による著しいパフォーマンスの劣化対策は十分か。

機密性の求められるデータのみをカラム単位で暗号化できるため、適所暗号化を実現。データベース暗号化ソフト「D'Amo」は高パフォーマンスを維持します。

項目	Select	Update
暗号化前	4.27秒	4.13秒
暗号化後	4.49秒	4.45秒
劣化	5％	7%

汎用性と拡張性はあるか？

データベースセキュリティを考える際、データベース暗号化だけではなくアクセス制御や監査の機能が求められます。また、データベース暗号化の強化にはデータ単位での細かなセキュリティ設定が必要となります。

データベース暗号化ソフト「D'Amo」ならではの暗号化・復号の機能。さらに、アクセス制御およびログ監視、暗号化されたデータに対するアクセスの監査レポートなどの監査機能のトータルセキュリティを提供します。

トータルセキュリティ

- 暗号化 復号
- アクセス制御
- 監査

その他

米国国立標準技術研究所FIPS暗号化モジュール認証を取得しており、暗号化アルゴリズムは世界標準のAES/TDES/SEED/ARIAに対応しています。

PCI DSSへの対応

- グローバルスタンダードのクレジットカード情報保護セキュリティ対策

PCI-DSSの完璧な準拠

PCI-DSSは、カード会員情報の保護を目的として、国際ペイメントブランド5社が共同で策定したカード情報セキュリティの国際統一基準です。

カード会社はもちろん、カード情報を「保存、処理、伝送」する事業者であるカード加盟店や銀行、決済代行サービス企業などが、PCI-DSSに準拠する必要があります。データベース暗号化ソフト「D'Amo」は、PCI-DSSや個人情報保護法などで要求されるデータベースに対する機密データの暗号化・アクセス制御・ログ監査が可能です。

FPE	1902 7334 2139 4519
一般暗号化	8juYE62W%Uwjakes& dDFeruga2345WeFLK

「D'Amo」は、トークナイゼーションの特徴であるフォーマット維持を実現。平文の属性（長さ、タイプ）を維持しながらデータの暗号化・復号を実行（NISTのFPE標準運用モード採用）します。

OSSに対応する「MyDiamo」

メーカーでもあるペンタセキュリティシステムズ株式会社は、日本国内においてデータベース暗号化のためのソフトを2種類提供しています。
MyDiamoが優秀賞の候補に採択
商用DBMSであるOracleとMicrosoft SQL Serveに対応する「D'Amo」とは別に、世界初のオープンソースデータ暗号化ソリューションである「MyDiamo（マイ・ディアモ）」を用意。対応DBMSとしてはMySQL、MariaDB、PostgreSQLなどがあり、ECビジネスを展開する企業を中心にその利用が高まっています。

「D'Amo」と「MyDiamo」は、カラム単位の暗号化や権限付与、アクセスコントロール、ログ監査、PCI-DSS準拠等のコンセプトは同じですが、暗号化手法が異なります。「D'Amo」がDBに暗号化・復号のモジュールをアドオンするDB PLUG-IN方式なのに対し、「MyDiamo」は既存のDBMSエンジンとストレージエンジンの間にMyDiamo暗号化エンジンを搭載することだけで暗号化・復号を実行するIN-place方式（DBエンジン方式）となります。

TOPICS

MyDiamoが優秀賞の候補に採択

2019年12月2日、オープンソースデータベース暗号化ソリューション「MyDiamo」がSCメディア主催のSC Magazine Awards USの「最高のデータベース・セキュリティソリューション（Best Database Security Solution）」部門のファイナリストとして採択されました。

SC Magazine Awardsは約30年にわたってサイバーセキュリティ分野をリードする専門家および製品・サービスを選定し賞を授与するイベントであり、業界においてその権威と影響力が認められています。

セキュリティ産業分野の専門家たちの厳選な審査により受賞者が決められ、データベース部門以外にも、クラウドコンピューティング、フォレンジックソリューション、認証技術など、さまざまな分野における専門性が高く優秀な企業が授賞しています。

製品に関するお問い合わせ

製品・サービスについてのお問い合わせ及び「30日間無料体験」ご利用申し込みサイト

システムプラザ株式会社（https://www.systemplaza.co.jp）
TEL:03-6895-6804
E-mail :yarai_sales@systemplaza.co.jp
本製品に関する情報はインターネットでもご覧いただけます。
https://www.systemplaza.co.jp