Chakra Max™

進化したリアルタイムデータベースセキュリティソリューション

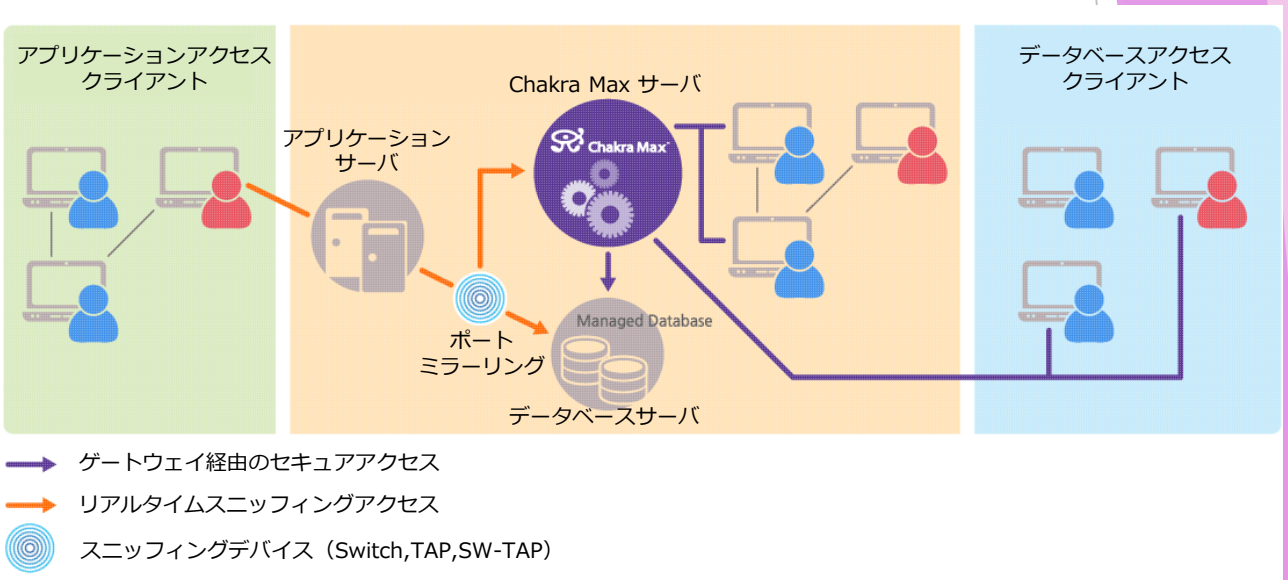
NST
New System Technology

データベースセキュリティの進化

企業においてもっとも重要なデータが格納されるデータベース。そのセキュリティは万全でしょうか。内部漏洩やSQLインジェクションによる攻撃など、データベースに対するリスクは高まる一方です。

Chakra Maxは、定評のあるChakraから一段進歩したデータベースセキュリティソリューションです。

Chakra Maxでは、データベースシステムにまったく影響を与えずにすべてのアクセスをリアルタイムで監視するスニフィングモードと、データベースアクセスをすべてChakra Max経由にすることでそのアクセスを厳密にコントロールできるゲートウェイモードがあり、それぞれの特色を生かしたデータベース監視を行うことができます。アプリケーションサーバなどからの定型アクセスは、スニフィングモードで監視を行い、開発者などの非定型のデータベースアクセスは、ゲートウェイモードで厳密に監視するハイブリッドモードで運用することもできます。

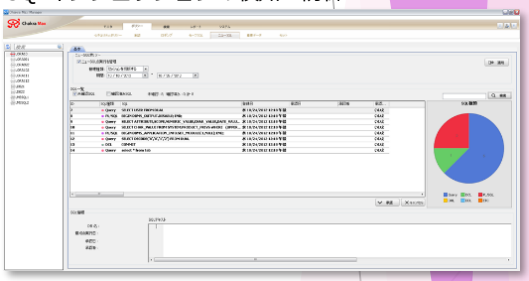


データベースのファイアウォール

SQLインジェクション攻撃の検知と防御

アプリケーションサーバやWEBサーバからデータベースアクセスを行っている場合、SQLインジェクション攻撃を受けることがあります。これらからのデータベースアクセスは、定型アクセスであるため、問題のないSQLをすべてリストにするホワイトリスト方式により、SQLインジェクション攻撃を検知・防御できます。
Chakra Maxでは、一定期間に実行されたSQL文をホワイトリストとして記録し、それら以外のSQL文の実行があったときに検知・防御することができます。

SQLインジェクションの検知・防御



ブラックリストによる検知と防御

開発者や運用オペレータなどのデータベースアクセスについては、実行を許可するSQL文をホワイトリスト方式で列挙しておくことは現実的ではありません。こういったアクセスはブラックリスト方式で監視し、漏洩や攻撃を検知・防御します。
Chakra Maxでは、ウィザード方式でブラックリストを定義できます。ブラックリストの定義にはSQL文だけでなく、テーブル名や取得行数、アカウント名、クライアント端末やIPアドレス、アプリケーション名などさまざまな条件を指定することができます。ブラックリストに指定した条件に合致するデータベースアクセスではアラートが発生し、それらを検知・防御することができます。

ブラックリストの定義

データベース操作のワークフロー

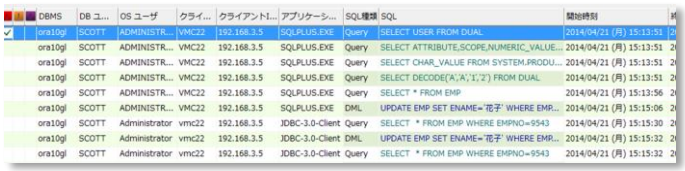
非常に重要なデータベースへのアクセスについては、SQL文の実行の都度、上司や監督官などの承認を必要とする場合があります。
Charka Maxは、指定された条件にあうSQL文の実行については、承認ルートにそって上司や監督官などの事前の承認を得た場合のみ、そのSQL文の実行を可能にするワークフロー機能があります。承認ルートの設定は柔軟で、事後承認・代理承認といった設定も可能です。

データベースアクセスをすべて記録

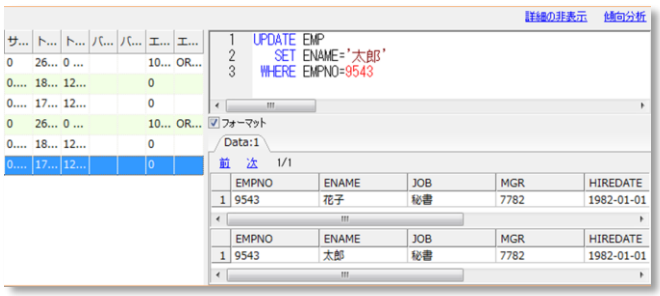
すべてのデータベースアクセスを記録

データベースへのアクセスログを監査証跡として保管することが、コンプライアンス対策からも説明責任を果たす上からも求められています。
Charka Maxは、ネットワーク上を流れているデータベースアクセスのパケットを取得し、解析し、記録しています。何時、誰が、何処から、何をしたのか、何件取得したのかを、リアルタイムに監視し、設定されているホワイトリスト、ブラックリストと照合してアラートを発生させます。SQLによるアクセスだけでなく、SSH、TELNET、FTPといったリモートアクセスも解析し、記録し、アラートを発生させます。
アラート発生時には、アクセスを遮断し、データベースを防御することもできます。
また、Charka Maxは、指定されたテーブル/カラムに対する更新SQLが実行されると、ポップアップ画面を表示して変更前と変更後のデータを確認させた後、それらを記録します。

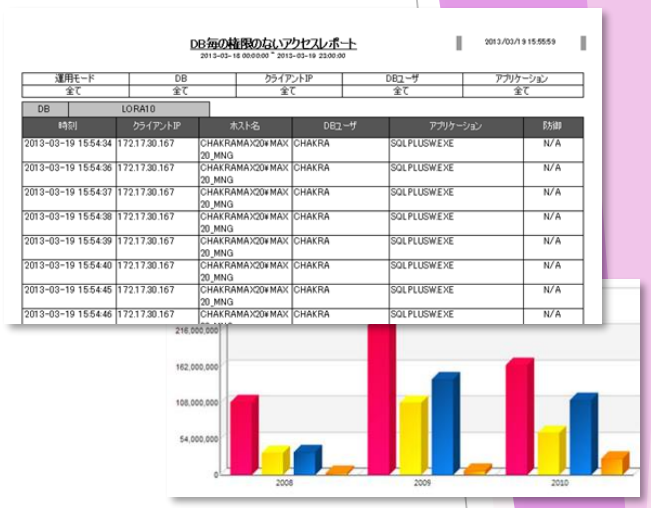
データベースアクセスのパケットをすべて解析



変更前・変更後のデータを記録



柔軟で効率的なレポート作成機能



不正なアクセスをリアルタイムに遮断

アラート発生時にセッションを切断

重大なセキュリティ違反を検知した場合、そのデータベースアクセスを直ちに遮断しなければならないことがあります。
Charka Maxは、アラート発生時に、メールで管理者に通知、SNMPトラップで管理者に通知、任意のプログラム実行、アラート発生元のセッションの切断を行うことができます。ゲートウェイモードでは、アラート発生時には、アラート発生元のSQL文の実行そのものを遮断します。

データベースシステムに影響を与えません

スニフィングモードでは影響はゼロ

Charka Maxは、ネットワーク上を流れているデータベースアクセスのパケットを取得し、解析し、記録しています。スニフィングモードでは、ネットワークスイッチのポートミラーリングなどでパケットを取得するため、データベースシステムに全く影響を与えません。監視対象サーバ内のローカルアクセスや仮想環境などネットワークスイッチからパケットを取得することが難しい場合は、監視対象サーバ内にエージェントを導入しますが、この場合でも負荷は大きくありません。

ゲートウェイモードでも影響は最小

ゲートウェイモードでは、データベースアクセスのパケットをCharka Maxサーバ経由にさせることでパケットを取得します。データベースシステムにエージェントを導入することもデータベースシステムで監査記録を取得する必要もありません。
重要なシステムは、スニフィングモードで監視し、開発者など非定型のアクセスを行うユーザのみをゲートウェイモードで監視することで、影響を最小限に抑えることができます。

豊富な経験と実績

金融、通信、製造、流通、運輸、建設など様々な業種/業態の数多くの大企業での豊富な導入実績を持つChakra。その後継製品であるChakra Maxは、Chakraの技術を継承し発展させた製品です。Chakra Maxもすでに多くの企業に導入されています。

主な仕様

データ収集方法	ネットワーク上のパケットまたは監視対象内のエージェント
暗号通信対応	SSH（ゲートウェイ） MS SQL Server(セッション情報)
DBMS側の負荷	なし(ネットワークからデータ収集時)
ロギング	すべてのデータベースアクセス（Windows, Linuxサーバのローカルアクセスを含む※1）
SQLインジェクション	ホワイトリストとの比較により未知のSQL文の検知と防御
収集するデータ（アラートの条件に指定可能）※1	時刻、全SQL文、ユーザ名、IPアドレス、アプリケーション名、端末名、応答時間、出力行数、パケット数、エラーコード、エラーメッセージ、リモートアクセスのコマンド
収集するデータ※1（アラートの条件に指定不可）	出力データ(64KB)、バインド変数、リモートアクセスの出力、変更前後のデータ

※1 一部のデータはDBMSの種類によっては取得できません

アラート時のアクション	メール送信、SNMPトラップ送信、任意のプログラム起動、実行拒否（ゲートウェイ）、セッション破棄
アラート時の実行拒否対応（ゲートウェイ）	全DBMS
アラート時のセッション破棄対応（スニフィング）	全DBMS 全リモートアクセス （resetパケットの送出）
データベース操作のワークフロー	DBMSアクセスは、任意のソフト
スニフィングモード時のみの機能	SQLインジェクション検知と防御・アラート時のセッション切断
ゲートウェイモード時のみの機能	SSHの監視・データベース操作のワークフロー・変更前後のデータの記録・重要データのマスキング・アラート時の実行拒否
レポート	PDFやExcel出力、カスタマイズ可能、スケジュールでメール送信

動作環境

対応DBMS	Oracle 7.3.4, 8.0, 8i, 9i, 9iR2, 10g,10gR2, 11g, 11gR2,12c,12cR2　MySQL 4, 5 IBM DB2 for Linux/Windows/Unix 6, 7, 8, 9, 9.5,10.1,10.5　PostgreSQL 7, 8, 8.4, 9 MS SQL Server 6.5, 7.0, 2000, 2005, 2008, 2012,2014,2016　Teradata 12,13,15 SAP Sybase ASE/IQ 12.x, 15　Symfoware 7, 8, 9, 10,12（スニフィングモード）
対応リモートアクセス	SSH（ゲートウェイモード）, TELNET, FTP, R-Login, R-command Remote Desktop/RDP（セッション情報のみ）
Chakra Max サーバ（推奨動作環境）	X64 (64bit) の 4コア、3GHz 相当以上のCPU 16GB以上のメモリ（検索ログ件数が多い場合は32GB） ディスクサイズは取得するログのサイズに依存（1TB以上）/スニフィング専用のNIC Red Hat Enterprise Linux 5.5-5.9,6.1-6.7（64bit）/CentOS 5.5-5.9,6.1-6.7（64bit） Windows Server 2008 R2,2012,2012 R2（64bit）
Chakra Max マネージャ（推奨動作環境）	1GB以上のメモリ、100GB以上のディスクサイズ、画面の解像度が1280x1024以上 Windows 2003/ 7 /8/10 (32bit, 64bit), Windows Server 2008 R2,2012,2012 R2（64bit） .NET Framework 4.0, Oracle クライアント(任意)
Chakra Max クライアント（推奨動作環境）	1GB以上のメモリ、100GB以上のディスクサイズ Windows 2003/ 7 /8/10 (32bit, 64bit),Windows Server 2008 R2,2012,2012 R2（64bit）

製品アライアンス

アライアンスパートナー

chk180307

株式会社ニューシステムテクノロジー
〒103-0027 東京都中央区日本橋2-1-3
アーバンネット日本橋二丁目ビル10階
TEL：03-4405-3143　FAX：03-6700-1868
Email：info@kknst.com　https://ssl.kknst.com

販売パートナー