



Chakra MaxTM

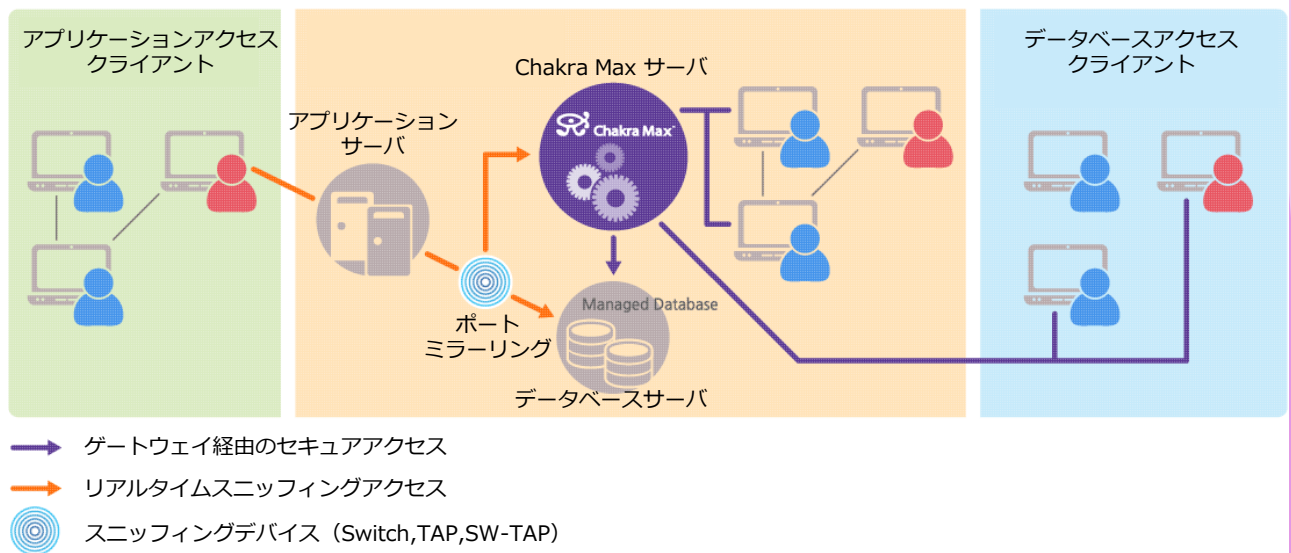
進化したリアルタイムデータベースセキュリティソリューション

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リングモードと、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、それぞれの特徴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、スニフリ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。

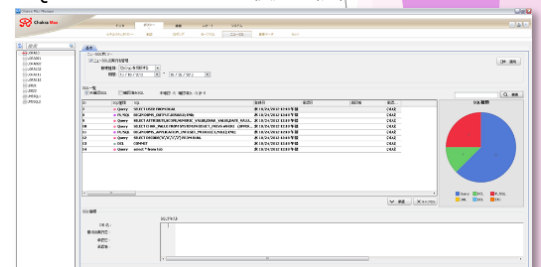
Chakra Maxでは、一定期間に実行されたSQL文をホワイトリストとして記録し、それら以外のSQL文の実行があったときに検知・防御することができます。

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。

SQLインジェクションの検知・防御



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。

Chakra Maxは、指定された条件にあふ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。

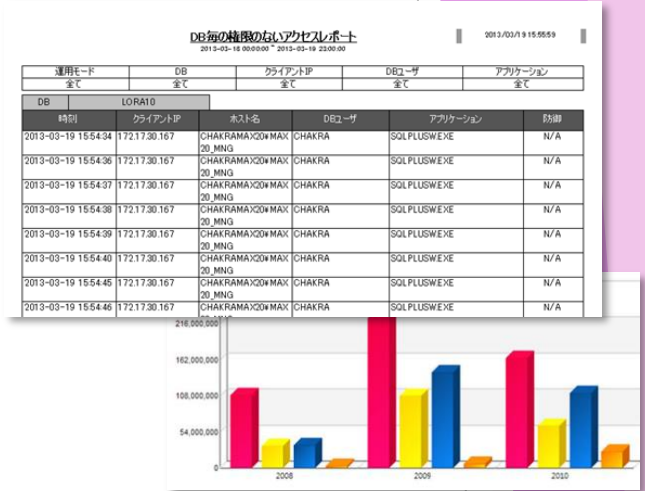
Charka Maxは、ネットワーク上を流れているデータベースアクセスの packets を取得し、解析し、記録しています。何時、誰が、何処から、何をしたのか、何件取得したのかを、リアルタイムに監視し、設定されているホワイトリスト、ブラックリストと照合してアラートを発生させます。SQLによるアクセスだけでなく、SSH、TELNET、FTPといったリモートアクセスも解析し、記録し、アラートを発生させます。アラート発生時には、アクセスを遮断し、データベースを防御することもできます。

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 packets をすべて解析

DBMS	DB ユーザ	OS ユーザ	クライアントIP	アプリケーション	SQL文種別	SQL	開始時刻	
ora10g	SCOTT	ADMINISTR...	192.168.3.5	SQLPLUS.EXE	Query	SELECT USER FROM DUAL	2014/04/21 (月) 15:13:51	
ora10g	SCOTT	ADMINISTR...	192.168.3.5	SQLPLUS.EXE	Query	SELECT ATTRIBUTE_SCOPE, NUMERIC_VALUE...	2014/04/21 (月) 15:13:51	
ora10g	SCOTT	ADMINISTR...	192.168.3.5	SQLPLUS.EXE	Query	SELECT CHAR_VALUE FROM SYSTEM.PRODU...	2014/04/21 (月) 15:13:51	
ora10g	SCOTT	ADMINISTR...	192.168.3.5	SQLPLUS.EXE	Query	SELECT DECODE(A,'A','Z') FROM DUAL	2014/04/21 (月) 15:13:51	
ora10g	SCOTT	ADMINISTR...	192.168.3.5	SQLPLUS.EXE	DML	UPDATE EMP SET ENAME='花子' WHERE EMP...	2014/04/21 (月) 15:15:06	
ora10g	Administrator	vmc22	192.168.3.5	JDBC-3.0-Client	Query	SELECT * FROM EMP WHERE EMPNO=9543	2014/04/21 (月) 15:15:30	
ora10g	SCOTT	Administrator	vmc22	192.168.3.5	JDBC-3.0-Client	DML	UPDATE EMP SET ENAME='花子' WHERE EMP...	2014/04/21 (月) 15:15:32
ora10g	SCOTT	Administrator	vmc22	192.168.3.5	JDBC-3.0-Client	Query	SELECT * FROM EMP WHERE EMPNO=9543	2014/04/21 (月) 15:15:32

柔軟で効率的なレポート作成機能



変更前・変更後のデータを記録

```
1 UPDATE EMP
2 SET ENAME='太郎'
3 WHERE EMPNO=9543
```

EMPNO	ENAME	JOB	MGR	HIREDATE
1	花子	秘書	7782	1982-01-01

EMPNO	ENAME	JOB	MGR	HIREDATE
1	太郎	秘書	7782	1982-01-01

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

スニフリ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 packets を取得し、解析し、記録しています。スニフリングモードでは、ネットワークスイッチのポートミラーリングなどで packets 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 packets 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 packets を Charka Max サーバ経由にさせることで packets 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、スニフリ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	スイッチでのパケットミラーまたは監視対象内のエージェント
暗号通信対応	SSH (ゲートウェイモード時) MS SQL Server(セッション情報)
DBMS側の負荷	なし(スイッチからデータ収集時)
ロギング	すべてのデータベースアクセス※1 (Windows, Linuxサーバのローカルアクセスを含む)
SQLインジェクション	自動収集したホ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※1 (アラートの条件に指定可能)	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)、バインド変数値、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、アクセス方法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 (ゲートウェイモード時)、セッション破棄
アラート時の実行拒否対応 (ゲートウェイモード時)	全DBMS
アラート時のセッション破棄対応	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	申請・承認は専用のソフトウェアデータベースアクセスは任意
スニフingモード時のみの機能	SQLインジェクション検知と防御
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、重要データのマスクing、アラート時の実行拒否
レポート	PDF・ExcelやCSV出力、スケジュールでメール送信

動作環境

対応DBMS	Oracle 8.0-11gR2, 12c, 12cR2, 18c, 19c MySQL 4, 5, 8 MariaDB 5-10 IBM DB2 for Linux/Windows/Unix 6-9, 9.5, 10, 11 PostgreSQL 7, 8, 9, 10, 11 MS SQL Server 6.5-2008, 2012, 2014, 2016 Teradata 12, 13, 15 SAP HANA v1,v2 SAP Sybase ASE/IQ 12.x, 15, 16 Symfoware 7, 8, 9, 10, 12(スニフing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ing専用のNIC Red Hat Enterprise Linux / CentOS 5.5-5.9, 6.1-6.7, 7.0-7.5, 8.0-8.1 (64bit) Windows Server 2008R2, 2012, 2012R2, 2016(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 7/8/10(32bit,64bit), Windows Server 2008R2, 2012, 2012R2, 2016(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) (ゲートウェイモード時のみ)	1GB以上のメモリ、100GB以上のディスクサイズ Windows 7/8/10(32bit, 64bit), Windows Server 2008R2, 2012, 2012R2(64bit)

製品アライアンス



アライアンスパートナー



販売パートナー



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

本誌掲載の会社名、製品名およびロゴは各社の登録商標または商標です。