豊富な経験と実績

金融、通信、製造、流通、運輸、建設、公共など様々な業種/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
暗号通信対応	MS SQL Server(セッション情報), SSH
DBMS 側の負荷	なし
ロギング	すべてのデータベースアクセス
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（アラートの条件に指定不可）*1	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
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

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、実行ブロック（ゲートウェイモード）、セッション破棄
アラート時の実行ブロック（ゲートウェイモード）	全 DBMS
アラート時のセッション破棄	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	データベースアクセスは、通常のソフト
ハイブリッドモード時のみの機能	SQL インジェクション検知・防御
ゲートウェイモード時・ハイブリッド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・アラート時の実行ブロック

*1　一部データは DBMS の種類によっては取得できない

動作環境

対応 DBMS	Oracle 7.3.4, 8.0, 8i, 9i, 9iR2, 10g, 10gR2, 11g, 11gR2, 12c　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　Teradata 12, 13 SAP Sybase ASE/IQ 12.x, 15　Symfoware 7, 8, 9, 10(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(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（ログの検索が多い場合は 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 3/4/5/6 (64bit)　/　CentOS 5.5 – 5.9, 6.1 – 6.4 (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/Vista/7 (32bit/64bit), Windows Server 2008 R2, 2012, 2012 R2 (64bit) .NET Framework 4.0, Oracle　クライアント
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/Vista/7 (32bit/64bit), Windows Server 2008 R2, 2012, 2012 R2 (64bit)

chk150413

NST New System Technology
株式会社ニューシステムテクノロジー
〒105-0022 東京都港区海岸 1-2-20 汐留ビルディング 3 階
TEL：03-6721-8883　FAX：03-6721-2020
Email：info@kknst.com　http://www.kknst.com

パートナー／代理店
まごころをこめて KOUBU SYSTEM
株式会社 甲武システム
〈本　社〉
〒113-0024 東京都文京区西片1-17-11 大和ビルディング302号
tel.03-3813-2596　fax.03-3813-2597
E-mail:info@koubu.co.jp　http://www.koubu.co.jp

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

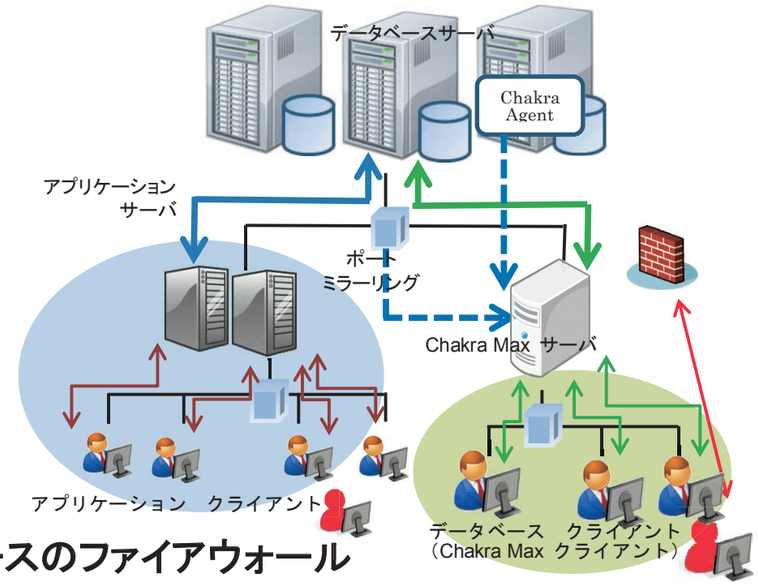
NST New System Technology

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や漏えいが許されない個人情報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。これらのデータベースアクセスは、通常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し、そのセッションを破棄することもできます。

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、事前にその SQL 文の実行をブロックするか、セッションを破棄することができます。

データベース操作のワークフローやマスキング

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。また、非常に重要なデータについては特定ユーザ以外にはデータを取得させたくないことも多々あります。

Chakra 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。重要データについては、Chakra Max で指定された条件にあう SELECT 文について結果をマスキングしてユーザに渡すことも可能です。

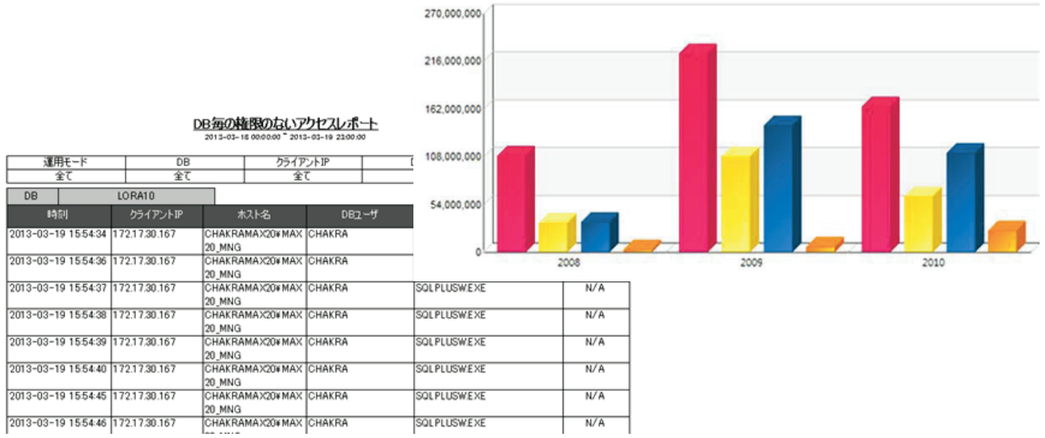
データベースアクセスをすべて記録

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観点からも求められています。

Chakra 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。

データ変更の監査証跡として、変更前と変更後のデータを記録する必要がある場合も、Chakra Max で対応できます。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。



DB毎の権限のないアクセスレポート

2013-03-16 00:00:00 ～ 2013-03-19 23:00:00

運用モード	DB	クライアントIP
全て	全て	全て

DB: LORA10

時刻	クライアントIP	ホスト名	DBユーザ		
2013-03-19 15:54:34	172.17.30.167	CHAKRAMAX20¥MAX20_MNG	CHAKRA		
2013-03-19 15:54:36	172.17.30.167	CHAKRAMAX20¥MAX20_MNG	CHAKRA		
2013-03-19 15:54:37	172.17.30.167	CHAKRAMAX20¥MAX20_MNG	CHAKRA	SQLPLUSW.EXE	N/A
2013-03-19 15:54:38	172.17.30.167	CHAKRAMAX20¥MAX20_MNG	CHAKRA	SQLPLUSW.EXE	N/A
2013-03-19 15:54:39	172.17.30.167	CHAKRAMAX20¥MAX20_MNG	CHAKRA	SQLPLUSW.EXE	N/A
2013-03-19 15:54:40	172.17.30.167	CHAKRAMAX20¥MAX20_MNG	CHAKRA	SQLPLUSW.EXE	N/A
2013-03-19 15:54:45	172.17.30.167	CHAKRAMAX20¥MAX20_MNG	CHAKRA	SQLPLUSW.EXE	N/A
2013-03-19 15:54:46	172.17.30.167	CHAKRAMAX20¥MAX	CHAKRA	SQLPLUSW.EXE	N/A

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、その違反内容によっては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。

Chakra Max は、アラート発生時に、メールや SNMP トラップで管理者に通知し、任意のプログラムを実行し、さらに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 文の実行を事前にブロックできます。

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、エージェントでも低負荷

Chakra 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。エージェントを使用する場合では、NIC から対象のパケットだけを Chakra Max サーバへ転送し、データベースシステムに与える負荷は高くありません。

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 Chakra 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の監査記録を取得することも必要もありません。

重要なシステムは、定型のアクセスをスニフィングモードで監視し、開発者などの非定型のアクセス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。