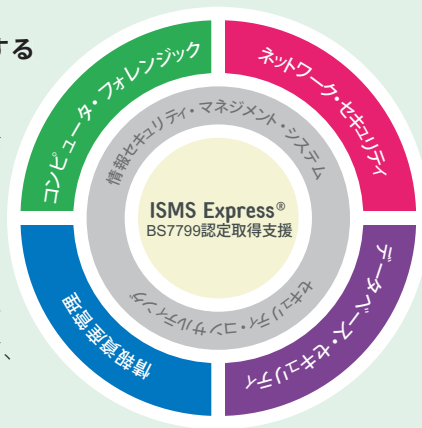


Whistle-blower® for DB -データベース監視ソリューション-

認証されたユーザのセキュリティ違反行為を検知・防御し、通信記録を証拠化する 内部情報漏えい対策ソリューション

近年、「個人情報保護法」「不正競争防止法」などの国の法整備が進む中、多くの情報漏えい事故が表面化しており、個人情報の保護や漏えいに対する関心は今までにないほど高まっています。情報セキュリティに関して管理・ITインフラの両面から対策をとることは、信頼される企業の条件になりつつあります。

日本SGIは、重要な情報資産が格納されるデータベースやそれらの情報が流れるネットワークといった、ITインフラへの不正アクセスや情報漏えいの対策ソリューションとして、セキュリティ違反行為の検知と警告を行う「Whistle-Blower®シリーズ」を提供します。



個人情報漏えい・個人情報保護法対策 - データベース監視ソリューション Whistle-blower® for DB

特長

■ ユーザアクセスの脆弱性、設定や権限の変更を定期的に監視

データベースの持つディクショナリ、オーディット・ログなどを定期的に監視することで、「普段とは異なる」ユーザの行動には警告を通知

■ データベースの脆弱性を評価

データベース全体を参照し、セキュリティ・パッチの適応状況やユーザのデフォルトパスワードなど、「ベスト・プラクティス」に基いて脆弱性を評価し、レポート化

■ アクセスログを監査証拠として保管

データベースにいつ、誰が、どこからアクセスしたかを監査証拠として保管

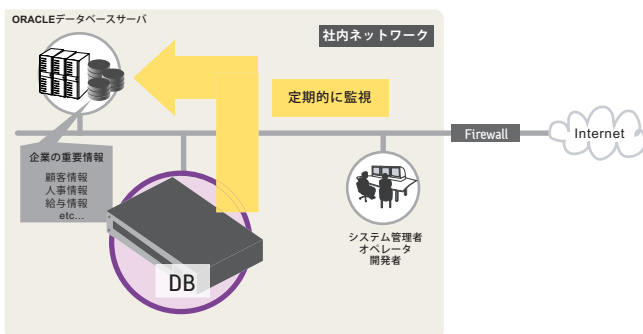
■ 混在データベースを一括監視

Oracle、DB2、SQL Server、Sybase、HiRDBの異種データベースを同時に複数監視

Whistle-blower® for DBはネットワークから定期的にデータベースのログや設定を監視することにより、不正行為やオペレータのミスなどの「普段とは異なる」ユーザのデータベース・アクセスを検知し、セキュリティ管理者にアラームやメールで警告を通知します。また、データベースへのアクセスログを監査証拠として保存することも可能です。

Whistle-blower for DBではネットワーク上の監視サーバから定期的にデータベースのログや設定を監視するため、基本的にデータベース・サーバへの特別な設定は必要とせず、サーバに負荷をかけることもありません。また、1台の監視サーバでOracle、DB2、Microsoft SQL Serverなど、混在したデータベースを同時に監視することができます。Whistle-blower for DBは不正アクセスの監視と警告を自動化するだけでなく、内部犯行の抑止効果としても有効です。

Whistle-blower for DBの導入に際しては、ネットワークやデータベースの利用状況などの環境調査から、セキュリティ・ポリシーの策定支援、運用コンサルティングまで、お客様のニーズに合わせ、経験豊富な日本SGIのセキュリティ・コンサルタントが担当いたします。



分析	導入	運用
<ul style="list-style-type: none"> データベースの分析 	<ul style="list-style-type: none"> Whistle-blower for DBの実装 データベース・セキュリティポリシーの構築 	<ul style="list-style-type: none"> 教育 評価
<ul style="list-style-type: none"> データベース・ポリシー定義 	<ul style="list-style-type: none"> Whistle-blowerの導入資料 データベース運用基準書 	<ul style="list-style-type: none"> 教育資料

主な仕様


監視対象データベース	ORACLE、DB2、SQL Server、Sybase、HiRDB
監視方法	データベースのオーディット・ログ、ディクショナリの定期的な監視
監視項目	セキュリティ・ポリシーによる普段と違う行動の監視 <ul style="list-style-type: none"> ■ ユーザ行動（時間、端末、読取り量など） ■ ユーザ権限、DB設定 ■ トランザクションの変更 ■ データ内容
警告方法	ビューワによるアラート、メール、SNMP通知
その他の機能	データベースの脆弱性評価
証跡化	アラートやオーディット・ログを証跡化
追加時の変更点	データベース・サーバで次の設定をする場合があります。 <ul style="list-style-type: none"> データベースのオーディットを有効 監視用のデータベースユーザの作成
ハードウェア環境	<ul style="list-style-type: none"> CPU Xeon 3GHz ネットワークのポート1つ 電源（二重化を推奨） 監視用のPC端末（Microsoft Internet Explorer 6.0 以上）

 日本SGI セキュリティ・コンサルティングに関するお問い合わせ：security@sgi.co.jp

©2004 SGI Japan, Ltd. All rights reserved. 本紙に掲載されている商標、画像についてはその所有者に所有権が属しています。掲載されている仕様は、予告なしに変更される場合があります。SGI、SGIのロゴマーク、Whistle-blower、およびSGIのキューブは日本SGI株式会社の登録商標です。(11/2004)

日本SGI株式会社

〒150-6031 東京都渋谷区恵比寿4-20-3 恵比寿ガーデンプレイスタワー31階

 TEL：0120-161-086 FAX：0120-161-087 <http://www.sgi.co.jp>

本社 TEL：03-5488-1811（大代表） FAX：03-5420-7201
 西日本支社 TEL：06-6343-6700（代表） FAX：06-6343-6713
 中部支社 TEL：0565-35-2561（代表） FAX：0565-35-2189
 つくば・東北事業所 TEL：029-858-1551（代表） FAX：029-858-1071
 東北営業所 TEL：022-221-2301（代表） FAX：022-221-2304
 テクニカルサポートセンター
 横浜ラーニングセンター TEL：045-682-3700（代表） FAX：045-682-0850