

PISO™の FAQ

お客様から寄せられた PISO™に対するご質問及び、その回答を掲載しています。

一般的なご質問

- 個人情報保護法に対応するためには何が必要ですか？
- セキュリティ関連のソフトはたくさんあります。PISO™の位置づけ・特徴は？
- 他社製品との違いは何ですか？
- データベースのセキュリティを強化したい。どうすればよいですか？
- PISO™を導入すると何がわかりますか？
- PISO™で情報漏洩を防ぐことが出来ますか？
- 成りすまし（アクセス権限のあるユーザ）を監視することはできますか？
- インターネット・データ・センターを運営しています。PISO™を用いてどのような運用が可能ですか？
- PISO™を導入するためには何が必要ですか？
- なぜ、ログ蓄積・分析サーバ(ISM)を別途用意する必要があるのですか？監視対象のデータベースに保存することはできないのですか？
- PISO™でサポートしている OS は？
- PISO™でサポートしている Oracle のバージョンは？
- PISO™の価格体系
- Oracle のバージョンアップやパッチなどに対応できるのか？
- PISO™を導入する際に、稼働中のデータベースを止める必要がありますか？
- PISO™導入後の運用コストはかかりますか？

技術的な質問

- PISO™はどのような警告通知手段を実装していますか？
- PISO™はどのような情報を取得しているのですか？
- PISO™はアクセスログを取得する際にどのような Oracle の情報を参照しているのですか？

- 取得した SQL は全文が記録されるのでしょうか？
- SQL にビューやシノニムが使用されている場合でも、アクセスした元テーブル情報を記録することはできますか？
- どうやって取得したアクセスログを検索し犯行を特定するのですか？
- アクセスログの検索に時間はかかりませんか？
- どうやって、ユーザの異常行動を検知するのですか？
- データベースのメンテナンス時間帯は様々な操作をするので、PISO™から大量に警告が発生して運用に支障をきたす可能性があります。しかし、内部監査の観点からはアクセスログを取得しなければなりません。PISO™は、アクセスログを取得しながら、警告を一時的に停止させることはできますか？

蓄積サーバに関するご質問

- ISM サーバの二重化は出来ますか？
- 古くなったアクセスログはどのように削除されるのですか？また、削除されたアクセスログを復元・参照することは可能でしょうか？
- 不正アクセスを発見した場合の対応機能についてアクション機能はありますか？
- ISM サーバのスペックは？
- 1 日のデータ量はどのくらいになりますか？
- ISM サーバに蓄積するログの容量は？

アクセスログ取得に関するご質問と回答

- PISO を導入することで、監視対象のサーバに負荷がかかりませんか？
- AuditTrail とどう違うのですか？
- 一部 AuditTrail を使用しているようですが、なぜ使用しているのですか？
- PISO は全ての SQL 文が取れるのですか？
- SQL 情報取得のインターバルはどのように決めるのですか？
- ターゲット側にエージェント・プログラムを入れるのですか？
- なぜ、エージェントプログラムを入れても、データベースのパフォーマンスに影響がないのですか？

- ターゲット側のエージェント・プログラムが使用するメモリーリソースはどの程度でしょうか？
- ターゲット側のエージェント・プログラムが使用する CPU 使用率はどの程度でしょうか？
- 大量トランザクションによる負荷増や、ネットワーク遅延などの理由によりログの収集漏れは発生するのでしょうか？
- 取得行(Rows_Processed)等の SQL 統計情報は累計値を元に算出していますか？
- ネットワーク負荷は大丈夫ですか？
- 「DBMS_APPLICATION_INFO」を設定するメリットはありますか？
- Web3 階層構成 (Web→AP→DB) の場合、DBMS_APPLICATION_INFO はどこに設定すればいいのですか？
- DBMS_APPLICATION_INFO による情報追加によって、監視対象サーバの SQL 解析時間に影響を与えないでしょうか？

一般的なご質問と回答

Q. 個人情報保護法に対応するためには何が必要ですか？

A. 個人情報漏洩は外部と内部の両方から発生する可能性があるため、その両方に対応する必要があります。

外部漏洩対策としてはファイアーウォールや不正侵入検知システムなどが考えられ、これらの普及率はほぼ 100%に近いと言えるでしょう。

一方、個人情報漏洩事件の約 80%が内部漏洩が原因であるにもかかわらず、現状ではほとんど手付かずの状態です。

内部漏洩対策に重点を置いたセキュリティソリューションが PISO™です。

Q. セキュリティ関連のソフトはたくさんあります。PISO の位置づけ・特徴は？

A. 守るべき情報が格納されたデータベースの「最小限の対応で最大限の効果を発揮する」監査を実現します。

主な機能として、「監査ログ管理機能」「不正アクセス警告機能」「流出経路追跡調査機能（マイニングサーチ）」があります。

Q. 他社製品との違いは何ですか？

A. PISO™は監視対象データベースの中のメモリ領域から直接情報を取得しますので、データベースのパフォーマンスに影響を与えません。

Q. データベースのセキュリティを強化したい。どうすればよいですか？

A. データベース・セキュリティの概要は大別すると

1. ユーザー認証
2. ユーザー元管理
3. アクセスコントロール

4. 格納データの暗号化
5. 監査

となります。

セキュアなデータベースにするためには、守るべきシステムの特長、データの性質をわけて業務要件を考慮し、上記それぞれについて対応の有無を検討する必要があります。

実際は、100%セキュアな環境は構築不可能です。予防・防止だけでなく、万一情報漏洩が発生した場合、いかに迅速な対応ができるかに着目する必要があります。

Q. PISO™を導入すると何がわかりますか？

- A. PISO™は、監視対象データベースのパフォーマンスに影響を与えずに、「守るべき情報」に対するアクセスを監視します。

「守るべき情報」に対して実施された SQL 文（全文）を取得することにより、以下の内容を把握することができます。

Q. PISO™で情報漏洩を防ぐことが出来ますか？

- A. PISO™は不正／公正を問わず通常の振る舞いと違う SQL 文を警告に上げます。PISO™の警告は企業内のモラルの向上と維持を実現します。

実際に、PISO™の存在自体がもたらす犯罪の抑止効果や情報漏洩リスクの低減に成功したというお客様の声をたくさんいただいています。

Q. 成りすまし（アクセス権限のあるユーザ）を監視することは出来ますか？

- A. PISO™は、Oracle データベースサーバに依存しない方法で監視しているため、成りすまし等アクセス権限のあるユーザを監視することが可能です。

Q. インターネット・データ・センターを運営しています。PISO™を用いてどのような運用が可能ですか？

A. お客様へ定期的に蓄積した監査ログを提出するとともに、その内容から監査設定、内容の見直しを実施する運用はいかがでしょうか？ PISO™では「マイニングサーチ」、「監視設定」機能で簡単に実現できます。

Q. PISO™を導入するためには何が必要ですか？

A. PISO™を導入するためには、取得したログを蓄積・分析するための専用サーバ (ISM)をご用意いただく必要があります。

Q. なぜ、ログ蓄積・分析サーバ(ISM)を別途用意する必要があるのですか？監視対象のデータベースに保存することはできないのですか？

A. 必要があります。別途ログ蓄積・分析サーバを立てる理由（メリット）は次のようになります。

1. 監視対象データベースのパフォーマンスへの影響が減る

収集したログを監視対象サーバに保存する場合、データベースやファイル等保存方法を問わず、システムリソース（CPU やディスク I/O）を使用するため、パフォーマンスに影響します。

2. 収集したログデータの改ざんを防ぐ

外部サーバに、収集したログを格納することにより、監視対象データベースにアクセスできる人が、ログに直接アクセスできないようになります。結果として、収集したログの改ざんを防げるようになります。

3. ログの一元管理ができる

複数のデータベース管理の際に、ログ蓄積・分析サーバを使用することにより、最大 8 インスタンスを効率良く監視できます。

4. DB サーバのダウンする可能性を減らす

ログが監視対象サーバに保存されるため、ログの削除等の管理を怠ると、ディスクがいっぱいになり、DB サーバをダウンさせる可能性があります。そのようなリスク削減や管理の手間をなくします。

Q. PISO™でサポートしている OS は？

- A. マルチプラットフォーム対応です。AIX、HP-UX、Solaris、Windows2003、Windows2000、Red Hat Linux、Miracle Linux 近々Windows2008 へも対応する予定です。

Q. PISO でサポートしている Oracle のバージョンは？

- A. Oracle Database 8.0 以降をサポートしています。8.0 以前のバージョンについてはお問合せ下さい。また、RAC にも対応しています。

Q. PISO™の価格体系

- A. PISO™は、監視対象サーバ上で、アクセスログを取得する「Target 側モジュール」と、PISO™によって取得したログを蓄積・分析するサーバにインストールする「ISM」の2製品によって構成されております。

価格は PISO™の導入されるサーバ上に搭載されているプロセッサ（CPU）の総数により決定します。また、導入対象がクラスタ構成の場合、コールドスタンバイ運用に限り、そのマシン用のライセンスを購入する必要はありません。

Q. Oracle のバージョンアップやパッチなどに対応できるのか？

- A. 対応しております。ただし、PISO™は SGA 領域内のメモリのアドレスを参照していますので Oracle のバージョンアップによってアドレスが変更される可能性がありますので、バージョンアップの際は、別途ご相談ください。

Q. PISO™を導入する際に、稼働中のデータベースを止める必要がありますか？

- A. SQL 監視を導入する時には、稼働中のデータベースを止める必要は全くありません。データベースを止めることなく導入が可能です。

セッション監視を導入する時には、お客様の環境によっては、データベースの再起動が必要となります。

Q. PISO™導入後の運用コストはかかりますか？

A. PISO™導入後は、メンテナンスサポート費用（年間保守）のみかかります。

技術的な質問と回答

Q. PISO™はどのような警告通知手段を実装していますか？

A. PISO™のコンソール以外に、メール、SNMP TRAP、SYSLOG/EVENTLOG の通知手段を実装しています。また、パトランプを接続することにより音と光で警告を認知できます。更に、警告通知時に ISM および Target で設定したコマンドラインを実行することも出来ます。

Q. PISO™はどのような情報を取得しているのですか？

A. PISO™はデータベースへのアクセスに関わる全てのデータを取得、蓄積します。データベースから情報を抽出する最小単位は SQL です。SQL のアクセスログは情報流出時の監査証跡となります。

Q. PISO™はアクセスログを取得する際にどのような Oracle の情報を参照しているのですか？

A. PISO™は以下の 2 つの情報を参照しています。

- **SQL**

SQL 文は弊社の独自技術である「SQL Collector」を使用して取得します。SQL Collector は Oracle の機能に一切依存することなく低負荷で SQL を取得します。

- **セッション**

Oracle の AuditTrail を使用してアクセスログを取得しています。SQL Collector が取得した SQL だけではなく、ログオン失敗など AuditTrail が得意とする監査項目を利用することもできます。

Q. 取得した SQL は全文が記録されるのでしょうか？

A. 監視対象となったオブジェクトに関する SQL 全文をアクセスログとして蓄積しています（取得バイト数のデフォルトは約 20MB）。但し、同一 SQL が 2 回 以

上実行された場合は、2回目以降、キー情報で蓄積しています。これは容量上の問題を解決するためにできるかぎり蓄積量を低減します。

Q. SQL にビューやシノニムが使用されている場合でも、アクセスした元テーブル情報を記録することはできますか？

A. できます。万が一、犯人がビューやシノニムを作成し個人情報にアクセスがあっても、監視や警告を上げることが可能です。

Q. どうやって取得したアクセスログを検索し犯行を特定するのですか？

A. PISO™の「マイニングサーチ」機能を活用して、「期間(時間)」「オブジェクト(行動)」「ユーザ(人)」など様々な条件から絞り込んで、蓄積された全てのアクセスログの中から、疑わしいと思われる SQL 文を特定することができます。

Q. アクセスログの検索に時間はかかりませんか？

A. 検索結果のログ一覧を単純にリスト形式で表示するのではなく、グラフ化します。データの重要度(オブジェクト・セキュリティー・レベル)、アクセスされたデータ(オブジェクト)、アクセスしたユーザ名、時間などの条件により GUI 操作で簡単に絞り込んでいくことが可能です。

Q. どうやって、ユーザの異常行動を検知するのですか？

A. 製品を導入後、過去のアクセス行動を分析・監査し、学習機能により通常発生しない行動なのかを検知することが可能です。

Q. データベースのメンテナンス時間帯は様々な操作をするので、PISO™から大量に警告が発生して運用に支障をきたす可能性があります。しかし、内部監査の観点からはアクセスログを取得しなければなりません。PISO™は、アクセスログを取得しながら、警告を一時的に停止させることはできますか？

A. PISO™は指定した時間帯だけ警告を停止する機能（ブラックアウト機能）を実装しています。この機能を使うことでアクセスログを取得しながら、設定した監視項目の警告を一時的に停止させることができます。

蓄積サーバに関するご質問

Q. ISM サーバの二重化は出来ますか？

A. クラスタリング・ソフトウェアを導入することで二重化を実現することが可能です。その場合でも PISO™のライセンスは1台分で大丈夫です。

Q. 古くなったアクセスログはどのように削除されるのですか？また、削除されたアクセスログを復元・参照することは可能でしょうか？

A. PISO™では、お客様により任意に指定されたオンライン保持期間を過ぎたデータを自動的にバックアップ領域にバックアップし削除します。このバックアップデータをテープ装置などに保管しておくことでいつでも復元することができます。

復元・参照は WEB ブラウザから PISO™にアクセスし、GUI 上で簡単に行うことができます。

Q. 不正アクセスを発見した場合の対応機能についてアクション機能はありますか？

A. 警告が発生した際に Target 上で実行するコマンドラインを定義することが出来ます。

この機能を使用して、限定的なアクションを行うことは出来ます。

将来のバージョンで、より充実したアクション機能を提供する予定です。

Q. ISM サーバのスペックは？

- A.
- CPU クラス : Pentium4 3GHz 以上
 - CPU 数 : 2
 - メモリ : 2GB 以上
 - Disk 転送速度 : 20MB/sec 以上

Q. 1日のデータ量はどのくらいになりますか？

A. 左右される要因:

1. SQL文の長さ
2. トランザクション量
3. サンプルング・インターバル
4. SQL文の一定/不定

Q. ISM サーバに蓄積するログの容量は？

A. 5GB（通常の蓄積ログ用） + 15GB（バックアップ、リカバリ用） = 20GB/インスタンス/月

アクセスログ取得に関するご質問

Q. PISO™を導入することで、監視対象のサーバに負荷がかかりませんか？

A. PISO™のコンセプトは「監視対象サーバに極力負荷を掛けないで、より多くの情報を取得する」ということですので、弊社独自の技術である、SQL Collector を利用し負荷の低減を実現しております。

SQL 文の取得に関しては、

- CPU 負荷
現 CPU 稼働率 + 1~2%程度（監視データベース毎）
- DISK 容量
 1. データベースサーバ
PISO™モジュール 150MB + 一時データ領域 500MB（変更可）
 2. ISM サーバ
蓄積期間に依存します。（拡張可能な DISK 選定を推奨）

Q. AuditTrail とどう違うのですか？

A. 全ての SQL 文を負荷なく取るためには AuditTrail だけでは実現不可能です。

Q. 一部 AuditTrail を使用しているようですが、なぜ使用しているのですか？

A. ログイン、ログイン失敗、長時間ログイン、禁止時間帯ログイン、データベースへのアクション（DDL）などの不正なセッション情報を取得するためにのみ使用しています。AuditTrail を使用して SQL を取得するとシステムへ高い負荷を与えますので SQL の取得には使用していません。PISO™では最低限の負荷で情報取得できるセッション情報の取得のみに AuditTrail 機能の一部を利用しています。

Q. PISO™は全ての SQL 文が取れるのですか？

A. PISO™はデフォルトでは 200milli-second 単位で SGA スキャンを行います。そのときに見る SQL 情報は「現在実行中」と「直前に実行された」のもので、このときに取りこぼしが発生する可能性があるのはインターバル内で「直前に実行された SQL の『さらに直前』」の SQL 情報です。PISO™では 200milli-second すなわち 1 秒間に 5 回のサンプリングをデフォルトとしていますが、サンプリング回数を最大 100 回まで増やしても CPU 負荷は微少です。

Q. SQL 情報取得のインターバルはどのように決めるのですか？

A. 200milli-second すなわち 1 秒間に 5 回がデフォルトです。これは SQL 文の実行前に行われる Parsing（翻訳）にかかる時間がおおよそ 200milli-second（最増えますが、システムにかかる負荷はほとんど上がりません。

Q. ターゲット側にエージェント・プログラムを入れるのですか？

A. 監視対象データベースにエージェント・プログラムを導入する必要があります。しかし、弊社の独自技術である「SQL Collector」を使用することにより、パフォーマンスへ影響を与えることはありません。これがなければ Oracle の AuditTrail を補完するだけのソフトにしかならず、一番重要な SQL 文ベースでの追跡が出来なくなります。

Q. なぜ、エージェントプログラムを入れても、データベースのパフォーマンスに影響がないのですか？

A. PISO™は、データベースの中のメモリ領域（SGA 領域）から直接情報を取得しますので、データベースのパフォーマンスに影響を与えません。

Q. ターゲット側のエージェント・プログラムが使用するメモリーリソースはどの程度でしょうか？

A. デフォルトサイズは約 20MB です。取得された SQL 文は 5 秒ごとに蓄積サーバに http で転送されます。5 秒間蓄積しておく SQL 文の数と長さに比例してメモリ使用量は増加します。

Q. ターゲット側のエージェント・プログラムが使用する CPU 使用率はどの程度でしょうか？

A. 環境にある程度左右されますが、SQL 文の取得に関しては、現 CPU 稼働率 + 1~2%程度（監視データベース毎）です。

Q. 大量トランザクションによる負荷増や、ネットワーク遅延などの理由によりログの収集漏れは発生するのでしょうか？

A. 例えばネットワークやログ蓄積サーバのハード障害などでデータの転送が出来なくなった場合は、一定のサイズ(デフォルト 500MB)までファイル書き込みを行います。障害復旧後、通常どおりにログ蓄積サーバにログを転送することにより、ログの収集漏れ等の対応をしています。

Q. 取得行(Rows_Processed)等の SQL 統計情報は累計値を元に算出していますか？

A. いいえ、累計値を実行数等で割るような不正確な算出を行いません。PISO™では、あるセッションから実行された特定の SQL 文の統計を差分値から算出しているため正確な値を表示しています。

Q. ネットワーク負荷は大丈夫ですか？

A. 蓄積サーバの配置上、業務に直接影響することはありません。また、弊社の独自技術であるハッシュ管理を利用することにより、過去に実行された SQL テキストは、蓄積サーバに送らず、独自ハッシュ値のみ転送することにより、不必要なネットワーク負荷を避ける仕組みを採用しています。

Q. 「DBMS_APPLICATION_INFO」を設定するメリットはありますか？

A. メリットは、複数のアプリケーションが存在する環境で不正アクセスを行ったアプリケーションが特定できることです。アプリケーション改ざんなどの不測の事態により、アプリケーションから通常は発生しない事象を監視し、DBMS_APPLICATION_INFO から問題のアプリケーションが特定できます。

Q. Web3 階層構成 (Web→AP→DB) の場合、DBMS_APPLICATION_INFO はどこに設定すればいいのですか？

A. 通常、Web3 階層構成では、DBMS_APPLICATION_INFO をアプリケーションサーバで稼動するアプリケーションに設定しますが、 PL/SQL (ストアドプロシージャ) を基本としているアプリケーションの場合は、 PL/SQL (ストアドプロシージャ) に DBMS_APPLICATION_INFO を設定します。これによって、どのマシン (サーバ) から発行された SQL 文か認識できるので不正アクセスがあったアプリケーションを特定できます。

Q. DBMS_APPLICATION_INFO による情報追加によって、監視対象サーバの SQL 解析時間に影響を与えないでしょうか？

A. 影響はありません。DBMS_APPLICATION_INFO はセッション情報に区別されます。従って SQL の解析等には影響を及ぼしません。