			Oracle					
			Oracle	IPLocks	PISO	Audit Master	Chakra	SecureSphere
4.2 検知、追跡系のDBセキュリティ対策								
4.2.1 ログの管理								
4.2.1.1 ログの取得								
(1)ログイン情報取得								
● ログイン時のログを取得する		必須						
	ログイン成功および失敗時のログ取得		○ 監査系機能によりログ取得 標準監査 トリガー（ログイン成功のみ） リスナーログ (ログインの成否は不明)	◎	◎	◎	◎ ログイン失敗時はアラート情報として記録	◎
(2)DBMS一般情報へのアクセス情報の取得								
● 重要な一般情報へのアクセス(参照/更新)をログとして取得する。		必須						
	テーブルへのアクセスログ取得		○ 監査系機能によりログ取得 DBA監査、標準監査 ファイングレイン監査 トリガー（Insert,Update,Delete） REDOログ/アーカイブログ (update、insert、delete)	◎	◎	◎	◎	◎
	SQLで実際に扱われたデータ (例：参照データ)のログ取得		×	×	×	×	△ 参照データの先頭64KB	◎
	DBMS構成ファイルへのアクセスログ取得		× OSレベルでファイルアクセスログを収集					
	DBMS移行およびバックアップコマンドに対するログ取得 ○：想定しているバックアップコマンドすべてログ取得可能 △：一部のコマンドはログ取得可能 ×：まったくログ取得不可能		○ DBA監査 標準監査 ファイングレイン監査	◎	◎	◎	◎	◎
			想定しているバックアップコマンド：エクスポート･ユーティリティ(exp)、Data Pump Export(expdp)					
(3)DBMS管理情報へのアクセス情報の取得								
● 重要な管理情報へのアクセス(参照/更新)をログとして取得する		必須						
	リポジトリテーブルへのアクセスログ取得		○ DBA監査 標準監査 ファイングレイン監査 トリガー（Insert,Update,Delete） REDOログ/アーカイブログ (update、insert、delete)	◎	◎	◎	◎	◎
	DBMS設定ファイルへのアクセスログ取得		× OSレベルでファイルアクセスログを収集 # Oracleの場合、設定パラメータの変更は、起動時または変更時にアラート･ログに出力される。					
(4)DBオブジェクトの変更情報の取得								
● DBオブジェクト(DBアカウント、テーブル、ビューなど)の作成、変更ログを取得する		必須						
	DDL文に対するログ取得		○ DBA監査 標準監査 トリガー REDOログ/アーカイブログ	◎	◎	◎	◎	◎
	DBの権限変更に対するログ取得		○ DBA監査 標準監査 トリガー REDOログ/アーカイブログ	◎	◎	◎	◎	◎
4.2.1.2 ログの保全								
(1)ログの保管								
● ログを外部記憶媒体に保管すること ※"外部"とは、ログの主たる管理場所（DBMSであればDBシステム、サードパーティ製品であれば導入システム)以外を指す		必須	○ Data Pumpを利用してログをファイルに出力し、外部に保管	◎	◎ リアルタイムで保存可能	◎ リアルタイムで保存可能	×	◎
● ログを保存した外部記憶媒体は安全な場所に保管する		必須						
	外部記憶媒体を施錠出来るところに保管		×					
	台帳による持ち出し管理		×					
(2)ログの改ざん防止								
● ログの改ざん対策を講じる		必須						
	監査ログへのアクセス制御設定 ※OSに頼らず製品でアクセス制御できるか否か		○ 監査ログにアクセスできる権限を付与するユーザーを限定する ※Oracle Database Vault(Option)を導入した場合は、特権ユーザを含めたアクセス制御が可能	◎	◎	◎	◎	◎
	監査ログに電子証明書を付けて管理する		×（運用により対応）					
	書換え不能なストレージを使用する		△ 監査ログをファイルに出力し、ストレージのWORM機能を使用					
4.2.2 不正アクセス検知								
4.2.2.1 監視の仕組み作り								
● 検知した不正アクセスを通知する仕組みを設ける		必須						
	メールによる不正の通知		○ ファイングレイン監査（要スクリプト作成） トリガー	◎	◎	◎	◎	◎
	SNMPによる通知		×	◎	◎	◎	△ アラート時のプログラム実行	◎
	検知した接続の切断、あるいは遮断		○ ファイングレイン監査 （要スクリプト作成） トリガー	△	△	△	△	◎
			検知した接続が既に終了しており、不正検知”後”の切断、あるいは遮断が失敗に終わるケース有り					
4.2.2.2 アクセス時間のチェック								
(1)DBMS管理情報へのアクセス検知								
● ログを監視し、申請されていない時間帯のアクセスを検知する		必須	○ ファイングレイン監査 （要スクリプト作成） トリガー	◎	◎	◎	◎	◎
● 申請された内容と、作業結果に相違のないことをログと申請内容を確認する		必須	×(運用により対応)					
(2)一般情報へのアクセス検知								
● 一般(AP)ユーザアカウントごとに、DBMSにアクセスし得る正規の時間帯、曜日がいつであるのかの定義を行う		必須	× DBセキュリティポリシーなどを基に規定					
● セッション情報の監査ログを監視し、正規のアクセス時間帯でないアクセスを検知する		必須	○ ファイングレイン監査 （要スクリプト作成） トリガー	◎	◎	◎	◎	◎ ※許可されない時間帯にアクセスがあった場合に、これを自動遮断することも可能

			Oracle					
			Oracle	IPLocks	PISO	Audit Master	Chakra	SecureSphere
4.2.2.3 アクセス不可の接続元（IPアドレスなど）のチェック								
(1)アクセス不可の接続元の検知								
● DBMSへアクセス可能な接続元を定義する		必須	× DBセキュリティポリシーなどを基に規定					
● 許可されていない接続元からのアクセスを検知する		必須	○ ファイングレイン監査 （要スクリプト作成） トリガー	◎	◎	◎	◎	◎
(2)管理者アカウントによるアクセス								
● DBMS管理者が使用する接続元/OSユーザ/アカウントの組合せを定義する		必須	× DBセキュリティポリシーなどを基に規定					
● 上記の組合せ以外のアクセスを検知する		必須	○ ファイングレイン監査 （要スクリプト作成） トリガー	◎	◎	◎	◎	◎ ※Webアプリケーション経由のアクセスの場合、Webアプリケーションへのログインユーザ名との組み合わせもチェック可能
(3)一般アカウントの不正なアクセス								
● 一般アカウントによるアクセスのパター（接続元/OSユーザ/アカウントなど）を定義する		必須	× DBセキュリティポリシーなどを基に規定					
● 上記パターン以外のアクセスを検知する		必須	○ ファイングレイン監査 （要スクリプト作成） トリガー	◎	◎	◎	◎	◎ ※Webアプリケーション経由のアクセスの場合、Webアプリケーションへのログインユーザ名との組み合わせもチェック可能
4.2.2.4 その他の不正アクセスのチェック								
● ログインの失敗の回数が、ある期間想定以上に多くないかログを監視し、パスワードの辞書攻撃を検知する ※ 辞書攻撃＝1秒間に3回以上連続ログイン失敗と		推奨	×	○ 要スクリプト作成	×	○ 要スクリプト作成	×	◎
● 取得したログを監視し、SQL文の発行を検知する		推奨	○ ファイングレイン監査 （要スクリプト作成） トリガー	◎	◎	◎	◎	◎
● 取得したログを監視し、DBオブジェクトの作成、変更を検知する		推奨	○ トリガー	◎	◎	◎	◎	◎
4.2.3 ログの分析								
4.2.3.1 ログ分析の仕組み作り								
● ログを分析する仕組みを設ける		必須	○ 監査ログをSQL文で分析	◎	◎ ※ForensicOptionで詳細な分析が可能 弊社で標準で用意している分析テンプレートを記述 ･実行アクション別分析 ･オブジェクト別SQL分析 ･ログオン数分析 ･ログオン経路分析 ･SQL実行開始日時分析 ･SQL実行経路別分析 -マシン別 -DBユーザー別 -端末別 -プログラム別 -オブジェクトセキュリティレベル別	◎	◎	◎
4.2.3.2 定期的なログの分析								
(1)定期的なセッション情報の分析								
● セッション情報を分析する		必須						
	ログイン失敗回数が多いセッションの傾向分析		○ 監査ログを手動（SQL文）で分析	◎ DB-SOX監査レポート （テンプレート提供）	◎	◎	◎	◎
	長時間に渡りログインしているセッションの傾向分析		○ 監査ログを手動（SQL文）で分析	◎	◎	◎	△ 要スプレッドシートによる手動分析	△ 要スプレッドシートによる手動分析
	大量のリソースを消費するセッションの傾向分析		○ 監査ログを手動（SQL文）で分析 CPU時間、I／O使用量等	◎ CPU時間、I/O使用量等	◎ 取得件数、SQL文の実行時間およびSQLの実行回数	◎ 論理･物理I/O、CPU時間	◎	△ 要スプレッドシートによる手動分析 SQL実行時間、レスポンスタイム
(2)定期的なDBアクセス情報の分析								
● SQL文を分析する		必須						
	長時間に渡り実行されているSQLの傾向分析		×	×	◎	◎	◎	◎
	大量のリソースを消費するSQLの傾向分析		×	×	◎ 取得件数、SQL文の実行時間およびSQLの実行回数を分析可能	○ SQL追跡オプションにて物理読込数、論理読込数、検索件数	◎ 入出力パケット数、入出力バイト数	◎
	エラーで終了しているSQLの傾向分析		○ 監査ログを手動（SQL文）で分析	◎ DB-SOX監査レポート （テンプレート提供）	△ コマンドタイプのみ確認可能	◎	◎ SQL文のエラーコードを指定して検索可能	◎
	全件検索の傾向分析 ※ 全件検索＝where句のないselect文とする		○ 監査ログを手動（SQL文）で分析	○ カスタムレポート（要テンプレート作成）	◎	◎ SQL文をフィルタ	◎	◎

		Oracle					
製品	バージョン	10g Release 2	IPLocks Version 6.3	PISO Version 3.2	Ver 1.8.10	Ver3.0	Ver6.0
	エディション	Enterprise Edition					
	オプション		DB-SOX監査オプション	Forensic Option	SQL追跡オプション		DSG
対象DBMS	バージョン	同上	10g Release 2	10g Release 2	10g Release 2	10g Release 2	10g Release 2
	エディション	同上					

＜補足＞表中の記号は、下記の基準(実現度、簡易性)に基づいて定義されています
◎：既存の機能で実現可能
○：何かしらの作りこみをすることで実現可能
△：部分的に実現可能
×：実現不可能、あるいは運用面で対応する事項

	Oracle					
	Oracle	IPLocks	PISO	Audit Master	Chakra	SecureSphere

別表：ログ取得方式

ログ取得方式		Oracleが標準監査、DBA監査機能を用いてログ取得	標準構成でメモリにダイレクトアクセス(SQL文でのアクセスは皆無) - オプションにて標準監査機能を併用可能	Oracleの標準監査、FGA、DBA監査で取得したログをAMサーバにコピー（SQL追跡オプションにてメモリ上に存在しているSQLを検索して取得可能）	ネットワーク上の通信パケットを取得	ネットワーク上の通信パケット、及びエージェントによる IPC、Named Pipe、TCP のループバックの監視結果から取得
例外（ログが取得できないケース）		なし	sampling間隔内に開始・終了するSQL	SQL追跡オプションではsampling間隔内に開始・終了するSQL（標準構成では全て取得可能）	通信が暗号化されている場合 ローカルアクセス	レイヤー4より上で独自の暗号化機能が使われている場合 （SSLでの暗号化は取得は可能

別表：取得できるログの種類

いつ（When）	ログイン、ログアウト	時間(タイムゾーン付き)	DBログイン時刻、DBログオフ時刻	DBログイン時刻、DBログオフ時刻	DBログイン時刻、DBログオフ時刻	DBログイン時刻、DBログオフ時刻	アクセス時間
	SQL実行		SQL開始時刻	SQL開始時刻、SQL終了時刻	SQL開始時刻、SQL終了時刻	SQL開始時刻、SQL終了時刻	
誰が（Who）	DBユーザ名、 ログオン名（SQL Server）	DBユーザ名	DBユーザ名	DBユーザ名	DBユーザ名	DBユーザ名	DBユーザ名
	OSユーザ名	OSユーザ名	OSユーザ名	OSユーザ名	OSユーザ名	OSユーザ名	OSユーザ名
	アプリケーションユーザ名	クライアント識別子 （CLIENT_IDENTIFIER）	クライアント識別子 （CLIENT_IDENTIFIER）		クライアント識別子 （CLIENT_IDENTIFIER）		アプリケーションユーザ名
	その他						
どこから（Where）	マシン名、IPアドレス	マシン名	マシン名、IPアドレス	マシン名、IPアドレス	マシン名、IPアドレス	マシン名、IPアドレス	マシン名、IPアドレス
	端末プログラム名 （アプリケーション名）			端末プログラム名	端末プログラム名	端末プログラム名	端末プログラム名
	その他	ターミナル番号	ターミナル番号				Web経由の場合：アクセスURL、クライアントのIPアドレス、Webセッション ID
何に対して（what）	オブジェクトレベル	スキーマ名、オブジェクト名	スキーマ名、オブジェクト名	スキーマ名、オブジェクト名	スキーマ名、オブジェクト名	オブジェクト名	スキーマ名、オブジェクト名
	行列レベル				列名	列名	列名
	その他						データベース名
何をした（how）	SQL文、SQLタイプ、 コマンド名（非SQL）	SQL文、コマンド名	SQL文、SQLタイプ	SQL文、SQLタイプ	SQL文、SQLタイプ	SQL文	SQL文
	操作結果（成功可否）、エラーコード	エラーコード	エラーコード		エラーコード	エラーコード	エラーコード
	バインド変数にセットされた値		バインド値				バインド値
	処理行数、該当SQL実行回数			処理行数、実行回数	処理行数、実行回数	処理行数	
	レスポンスデータ					レスポンスデータ（先頭64KB）	レスポンスデータ（すべて）
	その他	SCN			推定実行時間、物理読込数	推定実行時間	ストアドプロシージャの内容
その他	セッションID（SPID）、プロセスID	セッションID、プロセスID	セッションID、プロセスID	セッションID、プロセスID	セッションID、エントリーID	セッションID	
	その他			クライアント情報		入出力パケット数、入出力バイト数	

			SQL Server					
			SQL Server	IPLocks	PISO	Chakra	SSDB監査	SecureSphere
4.2 検知、追跡系のDBセキュリティ対策								
4.2.1 ログの管理								
4.2.1.1 ログの取得								
(1)ログイン情報取得								
● ログイン時のログを取得する		必須						
	ログイン成功および失敗時のログ取得		○ 監査系機能によりログ取得 プロファイラ Audit Login/Audit Login Failed	◎	◎	○ ログイン失敗時はアラート情報として記録	○	◎
(2)DBMS一般情報へのアクセス情報の取得								
● 重要な一般情報へのアクセス(参照/更新)をログとして取得する。		必須						
	テーブルへのアクセスログ取得		○ 監査系機能によりログ取得 プロファイラ(SQL文全体) TSQL	◎	◎	◎	◎	◎
	SQLで実際に扱われたデータ (例：参照データ)のログ取得		×	×	×	△ 参照データの先頭64KB	×	◎
	DBMS構成ファイルへのアクセスログ取得		× OSレベルでファイルアクセスログを収集					
	DBMS移行およびバックアップコマンドに対するログ取得 ○：想定しているバックアップコマンドすべてログ取得可能 △：一部のコマンドはログ取得可能 ×：まったくログ取得不可能		○ SQL Server Management Studio (SQL Server ログ) プロファイラ (Audit Backup/Restore Event)	◎	◎	△ BACKUP(T-SQL)とManagement Studioのバックアップ操作はログを取得 VDIはログ取得不可能	◎	◎
			想定しているバックアップコマンド：BACKUP (T-SQL), Microsoft SQL Server Management Studio (バックアップ) , VDI (VDI:Virtual Backup Device Interface)					
(3)DBMS管理情報へのアクセス情報の取得								
● 重要な管理情報へのアクセス(参照/更新)をログとして取得する		必須						
	リポジトリテーブルへのアクセスログ取得		○ 監査系機能によりログ取得 プロファイラ audit schema object access	◎	◎	◎	◎	◎
	DBMS設定ファイルへのアクセスログ取得		× OSレベルでファイルアクセスログを収集 # Oracleの場合、設定パラメータの変更は、起動時または変更時にアラート･ログに出力される。					
(4)DBオブジェクトの変更情報の取得								
● DBオブジェクト(DBアカウント、テーブル、ビューなど)の作成、変更ログを取得する		必須						
	DDL文に対するログ取得		○ 監査系機能によりログ取得 プロファイラ Object : Altered/Created/Deleted	◎	×	◎	◎	◎
	DBの権限変更に対するログ取得		○ 監査系機能によりログ取得 プロファイラ Audit Schema Object GDR Event	◎	×	◎	◎	◎
4.2.1.2 ログの保全								
(1)ログの保管								
● ログを外部記憶媒体に保管すること ※"外部"とは、ログの主たる管理場所 (DBMSであればDBシステム、サードパーティ製品であれば導入システム)以外を指す		必須	○ プロファイラ ネットワークディスク、およびリモートデータベース (監査対象以外のデータベース)を指定可能	◎	◎ リアルタイムで保存可能	×	◎	◎
● ログを保存した外部記憶媒体は安全な場所に保管する		必須						
	外部記憶媒体を施錠出来るところに保管		×					
	台帳による持ち出し管理		×					
(2)ログの改ざん防止								
● ログの改ざん対策を講じる		必須						
	監査ログへのアクセス制御設定 ※OSに頼らず製品でアクセス制御できるか否か		○ securityadmin または sysadmin 固定サーバーロールをもつユーザーのみが参照可能 SQL Server Management Studio または、SQL文により管理	◎	◎	◎	× ファイルとして保持しているため、OSのアクセス権限に依存	◎
	監査ログに電子証明書を付けて管理する		× (運用により対応)					
	書換え不能なストレージを使用する		△ 監査ログをファイルに出力し、ストレージのWORM機能を使用					
4.2.2 不正アクセス検知								
4.2.2.1 監視の仕組み作り								
● 検知した不正アクセスを通知する仕組みを設ける		必須						
	メールによる不正の通知		○ 要通知サービス設定	◎	◎	◎	◎	◎
	SNMPによる通知		×	◎	◎	△ アラート時のプログラム実行	×	◎
	検知した接続の切断、あるいは遮断		○ 要スクリプト作成	△	△	△	×	◎
			検知した接続が既に終了しており、不正検知”後”の切断、あるいは遮断が失敗に終わるケース有り					
4.2.2.2 アクセス時間のチェック								
(1)DBMS管理情報へのアクセス検知								
● ログを監視し、申請されていない時間帯のアクセスを検知する		必須	○ 要通知サービス設定	◎	◎	◎	◎	◎
● 申請された内容と、作業結果に相違のないことをログと申請内容を確認する		必須	×(運用により対応)					
(2)一般情報へのアクセス検知								
● 一般(AP)ユーザアカウントごとに、DBMSにアクセスし得る正規の時間帯、曜日がいつであるのかの定義を行う		必須	× DBセキュリティポリシーなどを基に規定					
● セッション情報の監査ログを監視し、正規のアクセス時間帯でないアクセスを検知する		必須	○ 要通知サービス設定	◎	◎	◎	◎	◎ ※許可されない時間帯にアクセスがあった場合に、これを自動遮断することも可能

			SQL Server					
			SQL Server	IPLocks	PISO	Chakra	SSDB監査	SecureSphere
4.2.2.3 アクセス不可の接続元（IPアドレスなど）のチェック								
(1)アクセス不可の接続元の検知								
	● DBMSへアクセス可能な接続元を定義する	必須	× DBセキュリティポリシーなどを基に規定					
	● 許可されていない接続元からのアクセスを検知する	必須	○ 要通知サービス設定	◎	◎	◎	△ コンピュータ名で検知可能	◎
(2)管理者アカウントによるアクセス								
	● DBMS管理者が使用する接続元/OSユーザ/アカウントの組合せを定義する	必須	× DBセキュリティポリシーなどを基に規定					
	● 上記の組合せ以外のアクセスを検知する	必須	○ 要通知サービス設定	◎	◎	◎	◎	◎ ※Webアプリケーション経由のアクセスの場合、Webアプリケーションへのログインユーザ名との組み合わせもチェック可能
(3)一般アカウントの不正なアクセス								
	● 一般アカウントによるアクセスのパター（接続元/OSユーザ/アカウントなど）を定義する	必須	× DBセキュリティポリシーなどを基に規定					
	● 上記パターン以外のアクセスを検知する	必須	○ 要通知サービス設定	◎	◎	◎	◎	◎ ※Webアプリケーション経由のアクセスの場合、Webアプリケーションへのログインユーザ名との組み合わせもチェック可能
4.2.2.4 その他の不正アクセスのチェック								
	● ログインの失敗の回数が、ある期間想定以上に多くないかログを監視し、パスワードの辞書攻撃を検知する ※ 辞書攻撃＝1秒間に3回以上連続ログイン失敗と	推奨	○ 要通知サービス設定	◎ DB-SOX監査レポート（テンプレート提供）	×	×	×	◎
	● 取得したログを監視し、SQL文の発行を検知する	推奨	○ 要通知サービス設定	◎	◎	◎	×	◎
	● 取得したログを監視し、DBオブジェクトの作成、変更を検知する	推奨	○ 要通知サービス設定	◎	×	◎	◎	◎
4.2.3 ログの分析								
4.2.3.1 ログ分析の仕組み作り								
	● ログを分析する仕組みを設ける	必須	○ 監査ログを手動（SQL文）で分析	◎	◎ ※ForensicOptionで詳細な分析が可能 弊社で標準で用意している分析テンプレートを記述 ･実行アクション別分析 ･オブジェクト別SQL分析 ･ログオン数分析 ･ログオン経路分析 ･SQL実行開始日時分析 ･SQL実行経路別分析 -マシン別 -DBユーザー別 -端末別 -プログラム別 -オブジェクトセキュリティレベル別	◎	◎	◎
4.2.3.2 定期的なログの分析								
(1)定期的なセッション情報の分析								
	● セッション情報を分析する	必須						
	ログイン失敗回数が多いセッションの傾向分析		○ 監査ログを手動（SQL文）で分析	◎ DB-SOX監査レポート（テンプレート提供）	◎	◎	△ 要スプレッドシートによる手動分析	◎
	長時間に渡りログインしているセッションの傾向分析		○ 監査ログを手動（SQL文）で分析	◎	◎	△ 要スプレッドシートによる手動分析	△ 要スプレッドシートによる手動分析	△ 要スプレッドシートによる手動分析
	大量のリソースを消費するセッションの傾向分析		◎ CPU時間、ディスクI/O、実行時間、メモリ使用量、キャッシュ情報	×	◎ 取得件数、SQL文の実行時間およびSQLの実行回数	◎	×	△ 要スプレッドシートによる手動分析 SQL実行時間、レスポンスタイム
(2)定期的なDBアクセス情報の分析								
	● SQL文を分析する	必須						
	長時間に渡り実行されているSQLの傾向分析		○ 監査ログを手動（SQL文）で分析	×	◎	◎	△ 要スプレッドシートによる手動分析	◎
	大量のリソースを消費するSQLの傾向分析		◎ CPU時間、ディスクI/O、実行時間、メモリ使用量、キャッシュ情報	◎	◎ 取得件数、SQL文の実行時間およびSQLの実行回数を分析可能	◎ 入出力パケット数、入出力バイト数	×	◎
	エラーで終了しているSQLの傾向分析		○ 監査ログを手動（SQL文）で分析	×	△ コマンドタイプのみ確認可能	◎ SQL文のエラーコードを指定して検索可能	△ 要スプレッドシートによる手動分析	◎
	全件検索の傾向分析 ※ 全件検索＝where句のないselect文とする		○ 監査ログを手動（SQL文）で分析	○ カスタムレポート（要テンプレート作成）	◎	◎	△ 要スプレッドシートによる手動分析	◎

製品	バージョン	2005	IPLocks Version 6.3	Version 3.2 (for SQLServer)	Ver3.0	Ver1.3	Ver6.0
	エディション	Enterprise Edition					
	オプション		DB-SOX監査オプション	Forensic Option			DSG
対象DBMS	バージョン	2005	2005	2005	2005	2005	2005
	エディション						

	SQL Server					
	SQL Server	IPLocks	PISO	Chakra	SSDB監査	SecureSphere

別表：ログ取得方式

ログ取得方式		SQLServerのトレースファイルを作成･取得	SQLServer標準のprofiler機能を利用	ネットワーク上の通信パケットを取得	トレースファイルをファイル単位で生成･取得	ネットワーク上の通信パケット、及びエージェントによる IPC、Named Pipe、TCP のループバックの監視結果から取得
例外（ログが取得できないケース）		SQLServer側で、トレースファイルを生成できない場合	SQLServer標準のprofiler機能にてログを取りこぼす場合(高負荷時)	通信が暗号化されている場合 ローカルアクセス	ネットワーク切断の場合、生成は継続するが、取得は保留	レイヤー4より上で独自の暗号化機能が使われている場合 （SSLでの暗号化は取得は可能）

別表：取得できるログの種類

いつ（When）	ログイン、ログアウト		DBログイン時刻、DBログオフ時刻	DBログイン時刻、DBログオフ時刻	DBログイン時刻、DBログオフ時刻	アクセス時間	アクセス時間
	SQL実行	SQL開始時刻、SQL終了時刻	SQL開始時刻	SQL開始時刻、SQL終了時刻	SQL開始時刻、SQL終了時刻		
誰が（Who）	DBユーザ名、 ログオン名（SQL Server）	Windoアカウント名/ドメイン、ログオン名	Windoアカウント名/ドメイン、ログオン名	Windoアカウント名/ドメイン、ログオン名	Windoアカウント名/ドメイン、ログオン名	Windoアカウント名/ドメイン、ログオン名	Windoアカウント名/ドメイン、ログオン名
	OSユーザ名						
	アプリケーションユーザ名						
	その他						
どこから（Where）	マシン名、IPアドレス	マシン名	マシン名	マシン名、IPアドレス	マシン名、IPアドレス	マシン名	マシン名、IPアドレス
	端末プログラム名 （アプリケーション名）	アプリケーション名	アプリケーション名	端末プログラム名	端末プログラム名		端末プログラム名
	その他					ドメイン名	Web経由の場合：アクセスURL、クライアントのIPアドレス、Webセッション ID
何に対して（what）	オブジェクトレベル	オブジェクト名	オブジェクト名	スキーマ名、オブジェクト名	オブジェクト名	オブジェクト名	スキーマ名、テーブル名
	行列レベル				列名		列名
	その他	セッション、トランザクション他					データベース名
何をした（how）	SQL文、SQLタイプ、 コマンド名（非SQL）	SQL文	SQL文	SQL文、SQLタイプ	SQL文	SQL文	SQL文
	操作結果（成功可否）、エラーコード	操作結果、エラーコード	エラーコード				エラーコード
	バインド変数にセットされた値						バインド値
	処理行数、該当SQL実行回数			処理行数	処理行数		
	レスポンスデータ				レスポンスデータ（先頭64KB）		
	その他				推定実行時間		ストアドプロシージャの内容
その他	セッションID（SPID）、プロセスID	SPID、プロセスID	SPID、プロセスID	SPID、プロセスID			
	その他	データベースID			入出力パケット数、入出力バイト数		