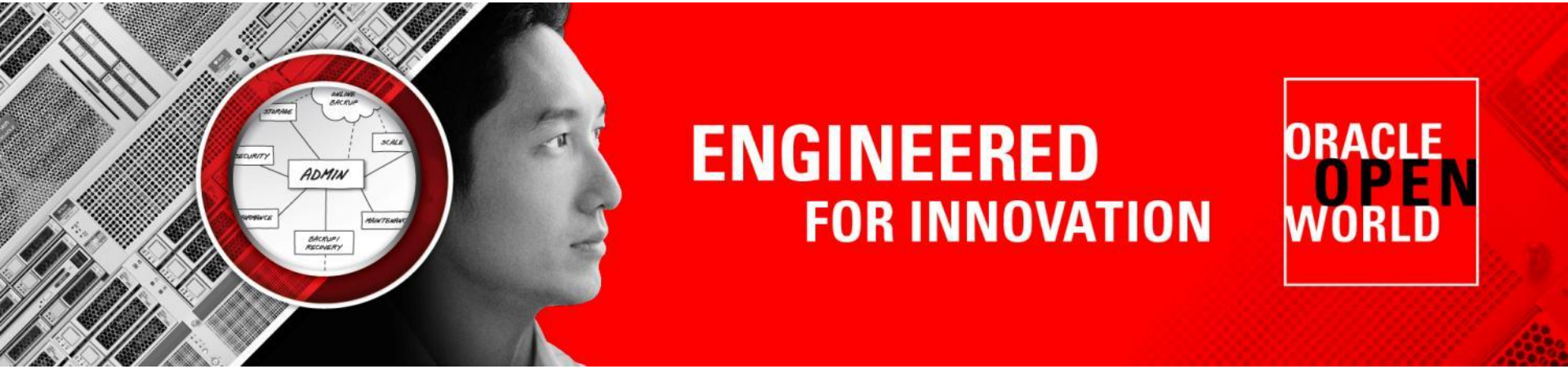


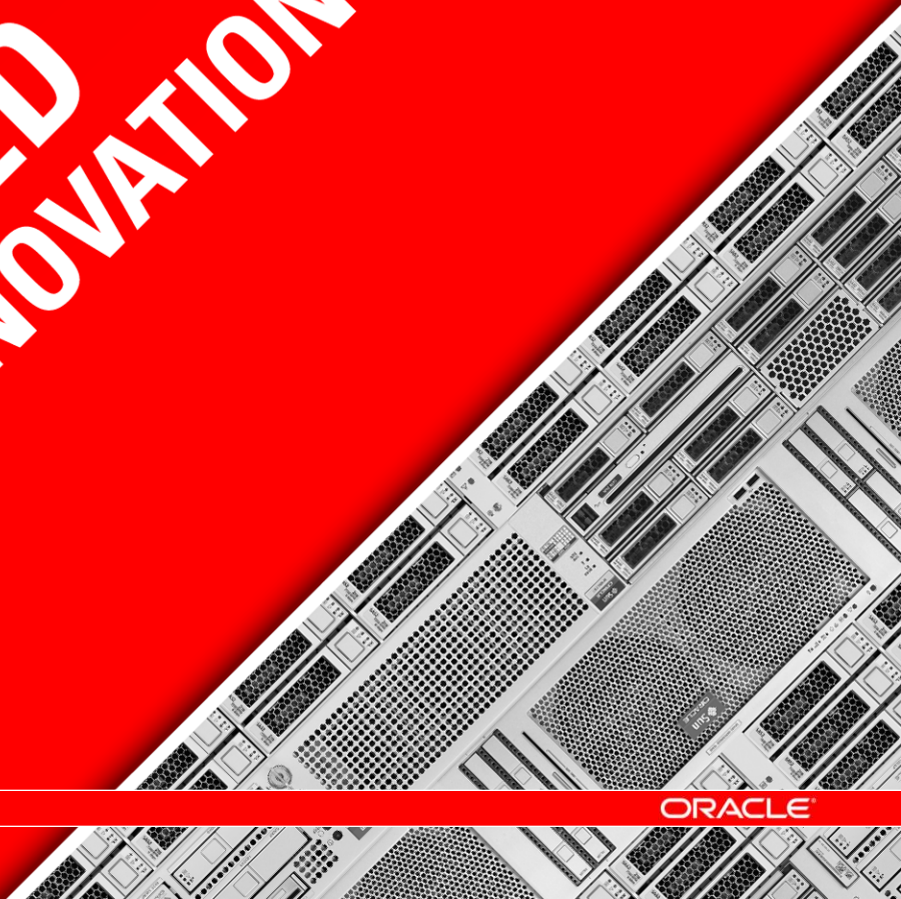
ORACLE®

Oracle Database Firewall 導入ベストプラクティス

製品事業統括 製品戦略統括本部 戦略製品ソリューション本部
シニアエンジニア,CISSP 西村克也

ORACLE OPEN WORLD

ENGINEERED FOR INNOVATION



ORACLE

ORACLE DEVELOP

Russia

17–18 April 2012

India

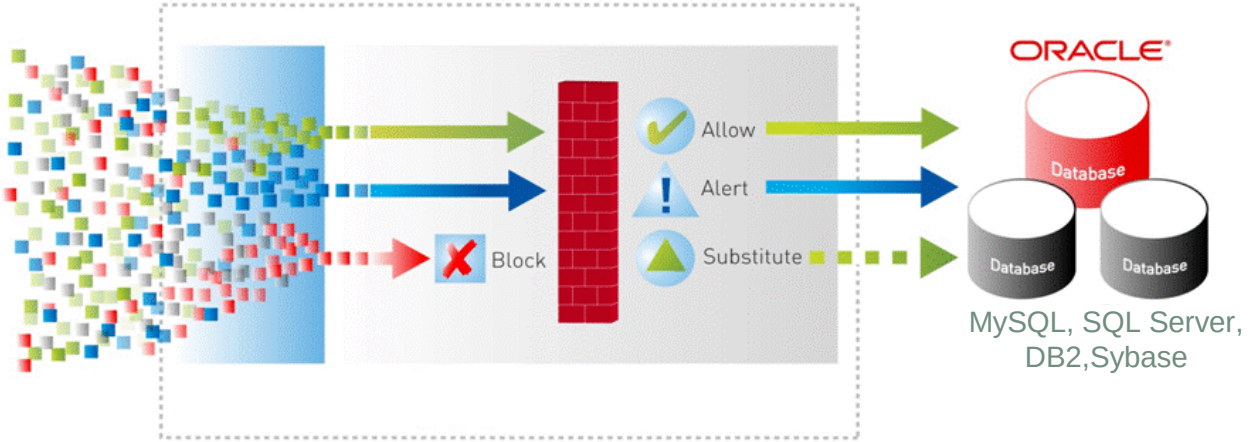
3–4 May 2012

San Francisco

September 30–October 4, 2012

以下の事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。以下の事項は、マテリアルやコード、機能を提供することをコミットメント（確約）するものではないため、購買決定を行う際の判断材料になさらないで下さい。オラクル製品に関して記載されている機能の開発、リリースおよび時期については、弊社の裁量により決定されます。

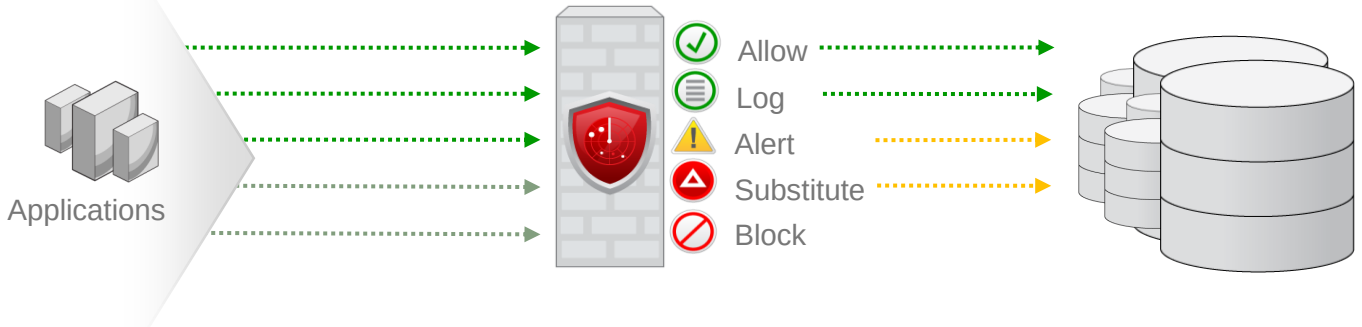
Oracle Database Firewall



- アプリケーションとデータベースの中間に位置し、ネットワークトラフィックからSQL文を収集・解析する
  - **ブロッキング**： SQLを解析し、危険と判断されるものはブロックや警告を行うことで内部不正・外部攻撃からデータベースを保護する
  - **モニタリング**： 収集したSQLをログとして記録・管理・レポーティング

Oracle Database Firewall

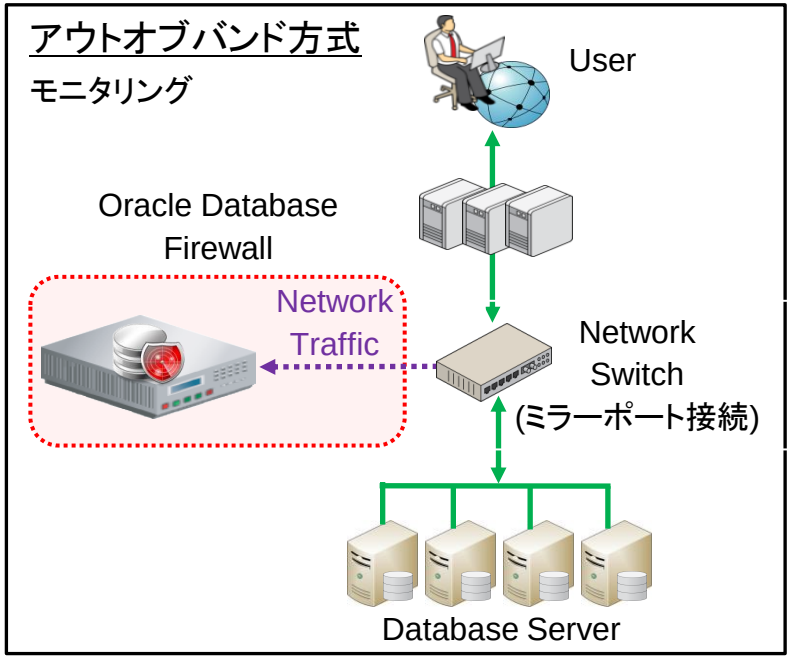
防御のファースト・ライン

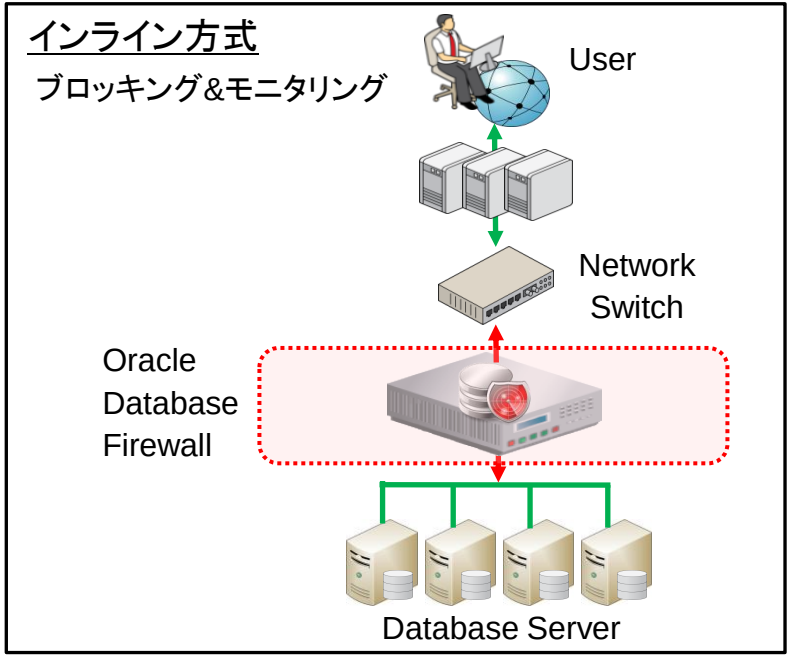


- ✓ **透過的**
  既存のアプリケーション、データベースの変更不要な独立した構成
- ✓ **正確な検知**
  SQL文を正確に理解し検知するSQL文法解析エンジンを搭載
- ✓ **漏れのない監視**
  データベースへのローカル接続等、DBFWを経由しないSQLさえも監視

透過的な2種類の配置

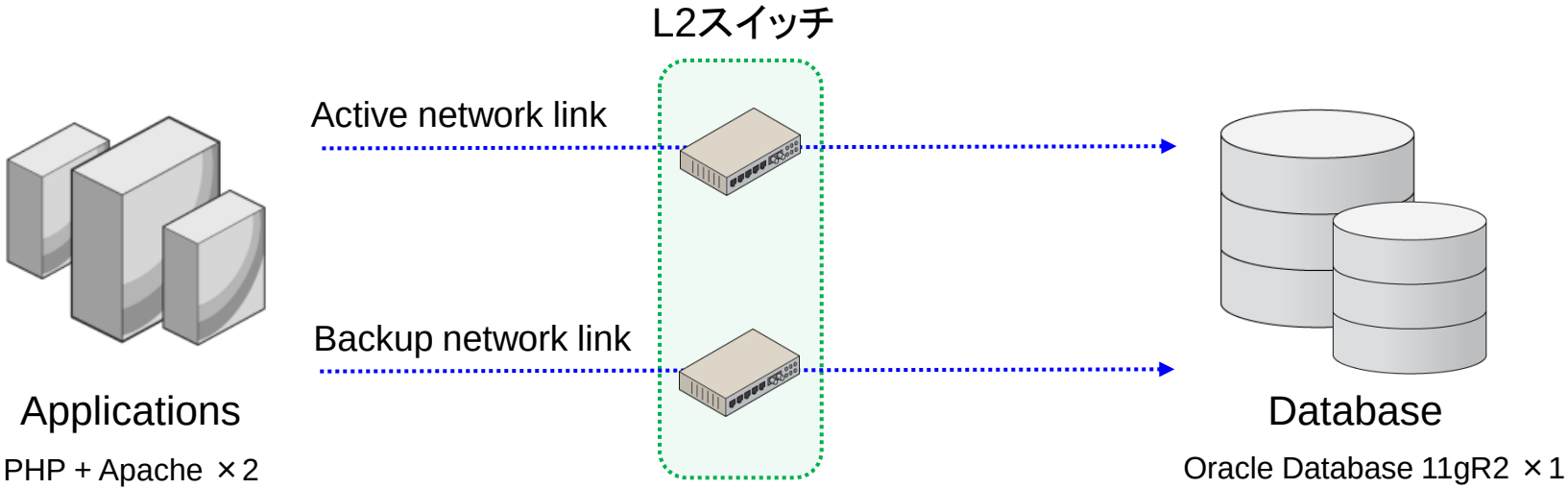
- モリタリングは、ネットワークスイッチと並列に配置
- ブロッキングは、アプリケーションとデータベース間に直列に配置



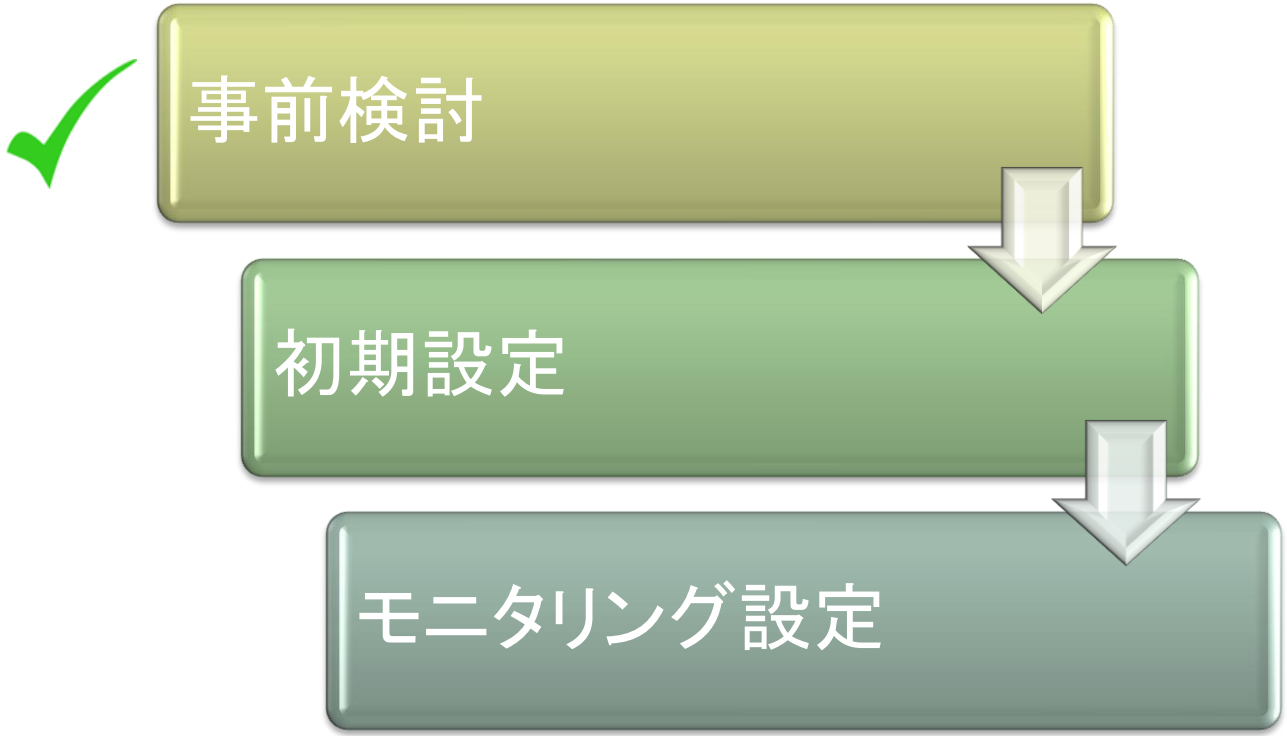


おらくる社　ネットワーク構成

- まずは、データベースへのアクセスをモニタリングする仕組みを導入する
- 次に、外部からの不正アクセス、内部からの不要なアクセスのブロッキングへ移行



Oracle Database Firewallの導入 ～モニタリング編

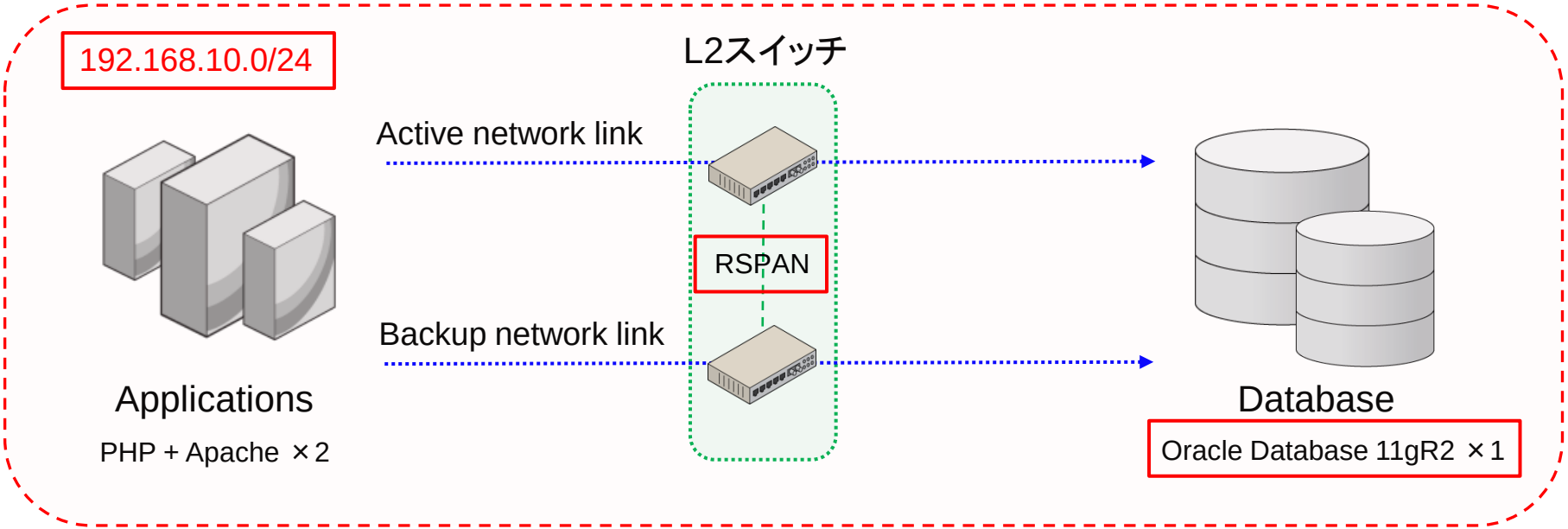


事前検討

	作業項目	作業項目詳細
事前検討	用途	アウトオブバンド(モニタリング)、インライン(モニタリング、ブロッキング)
	ネットワーク構成の確認	アプリケーション～データベースの経路、冗長化有無、ネットワーク・セグメント数
	スイッチの確認	モニタリングの場合は、ポートミラーリング機能の有無、RSPAN等の機能があるか等
	監視対象DBの確認	監視対象可能DB (Oracle 8i～11gR2、SQL Server 2000,2005,2008, MySQL 5.0,5.1,5.5 DB2 on LUW v9.x. Sybase ASE 12.5.4 - 15.0.x)
	DBFW構成の決定	用途に応じた配置場所、DBFWとDBFW Management Serverの台数を決定
	H/Wモデルの選定	CPU、メモリ要件は、監視するDBの数、トランザクション数から判断 ディスク要件は、モニタリングログの検索、保持期間から判断

おらくる社　ネットワーク構成

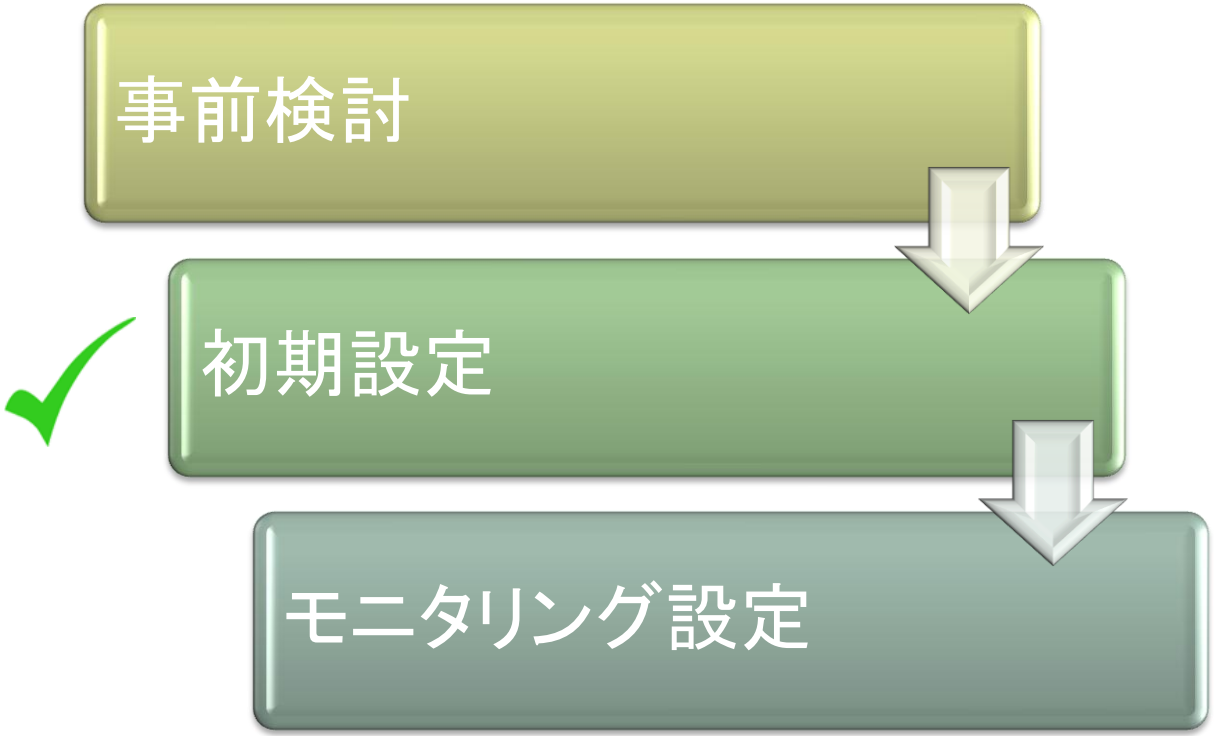
モニタリング (アウトオブバンド構成)



Oracle Database Firewall用　ハードウェア

- Sun Fire X4170 M2
  - Intel Xeon X5675 6-core 3.06 GHz processor x 2
  - 24GB Memory (4GB DIMM x6)
  - 600GB 10Krpm Disk x2
  - Sun x4 Quad-port Gigabit Ethernet Adapter UTP x1 S/W
  - N/W Port: 8
  - ※ DBFW Management Server用はスペックを若干変更

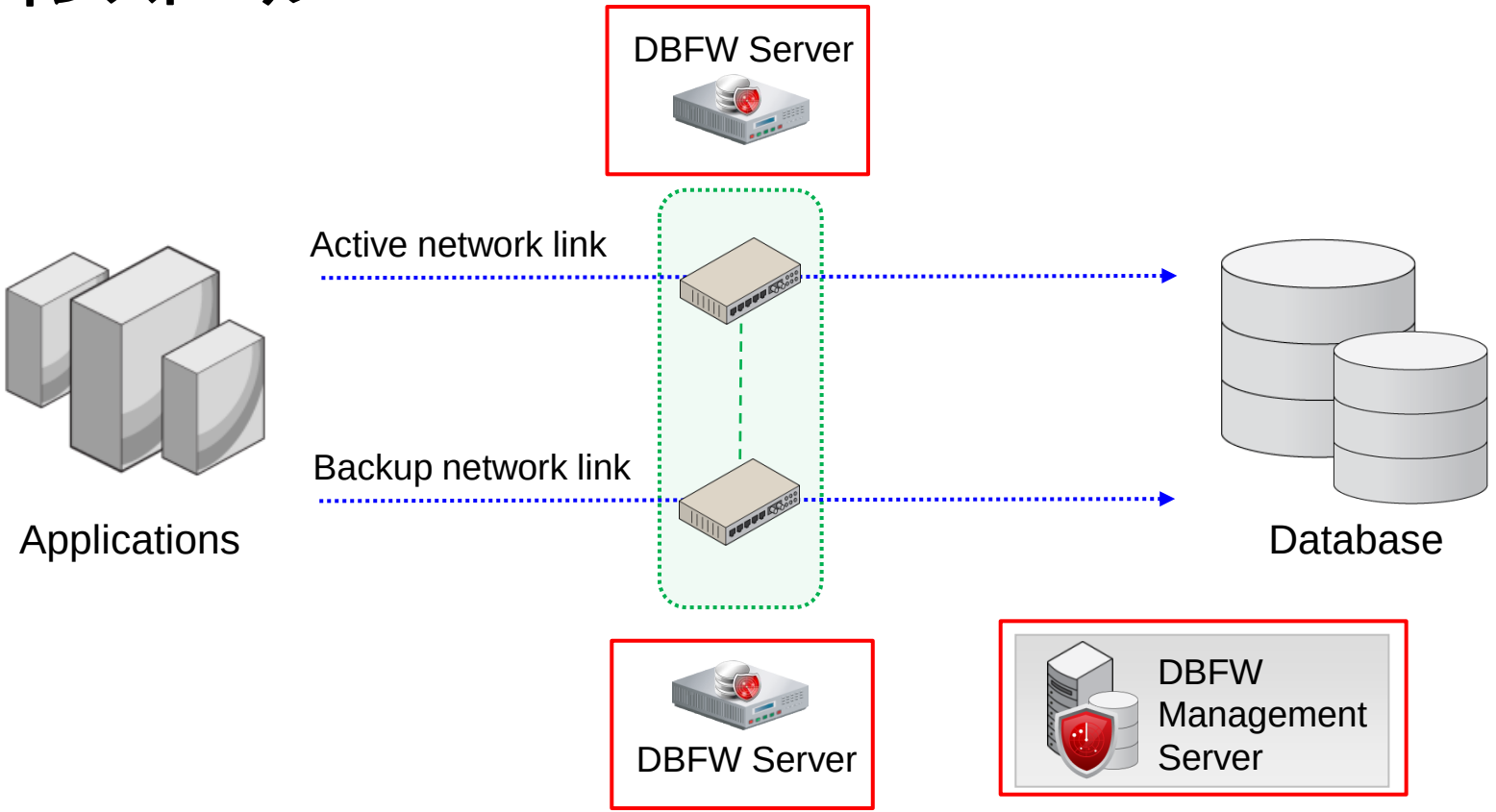
Oracle Database Firewallの導入 ～モニタリング編



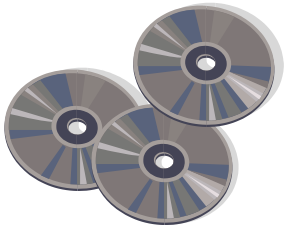
初期設定

	作業項目	作業項目詳細
事前設定	スイッチの設定	ポートミラーリングの設定、RSPANの設定
初期設定	インストール	DBFW Server、DBFW Management Server
	ネットワークへの接続	スイッチのミラーポートに接続
	導通確認	ミラーポートからパケットが受信できているか確認 （PING、TNSPING等）
	Mg Serverとの連携	DBFW ServerをDBFW Mg Serverの監視対象に追加
	モニタリングの設定	Enforcement Pointsの作成 モード: DAM ポリシー:logall.dna、または、logall-nomask.dna
	受信ログの確認	トラフィックログ検索で該当するSQLが表示されることを確認

インストール



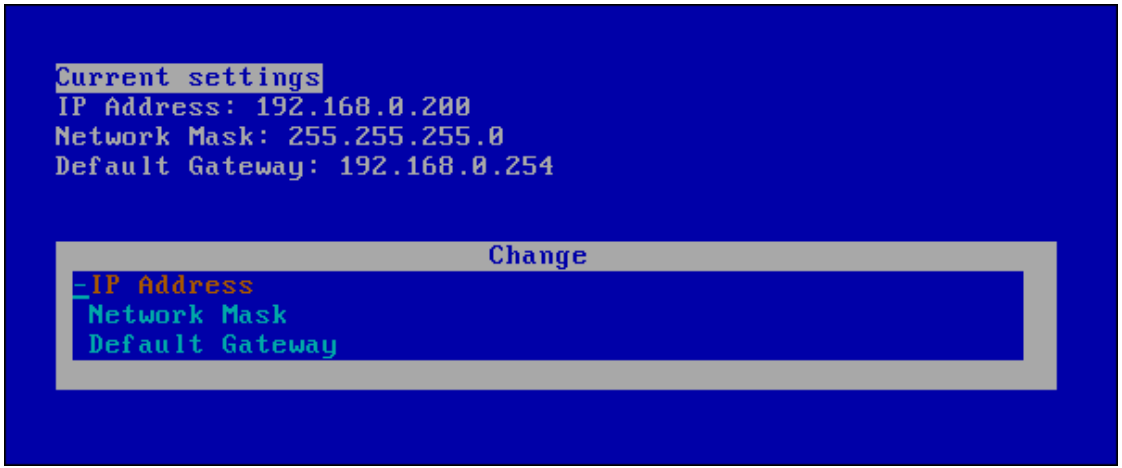
インストール



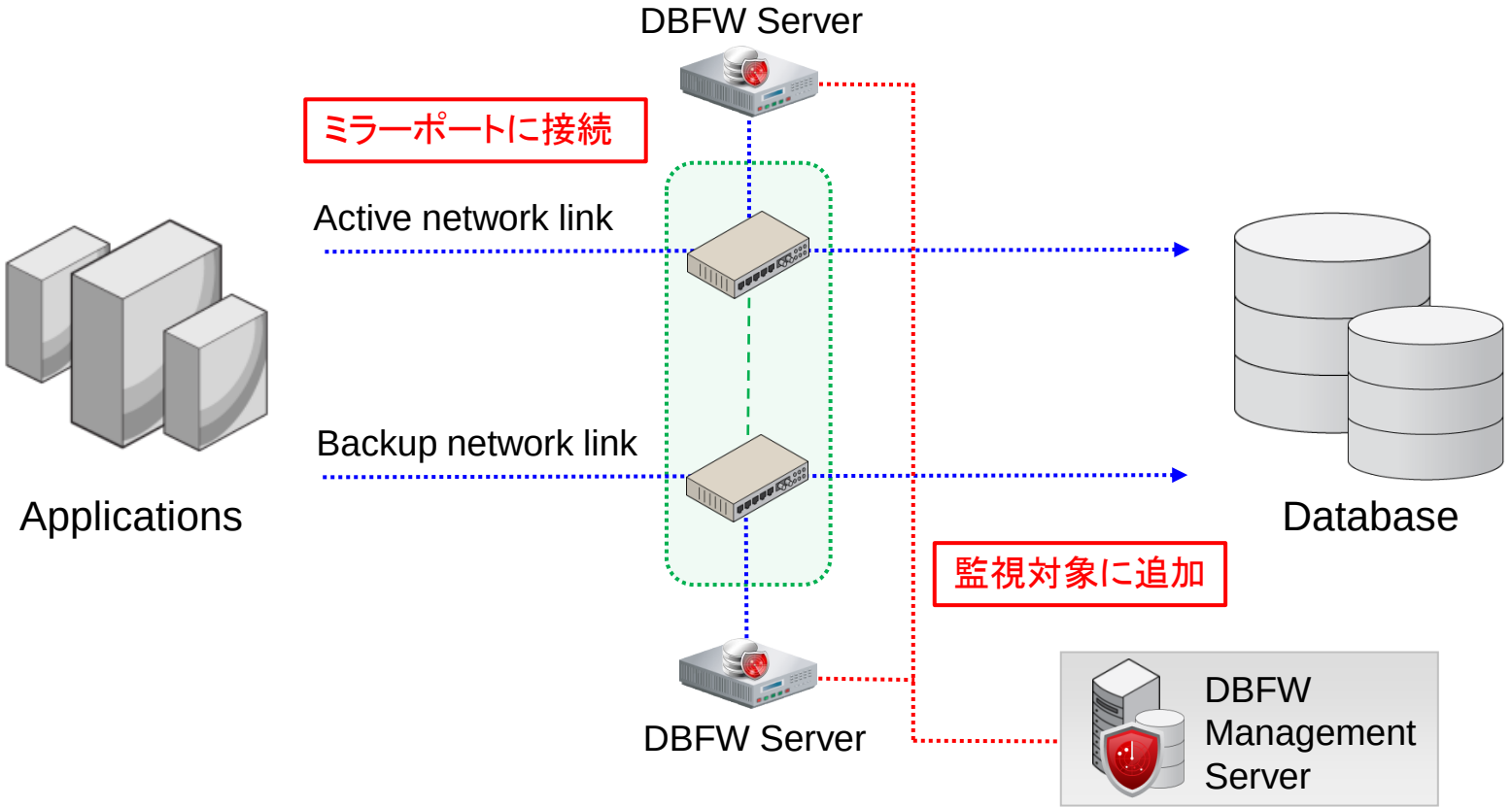
必要メディア

- Oracle Linux Release 5 Update 5 for X86(32bit)
- Oracle Database Firewall 5.1 Disc 1,2,3
- Oracle Database Firewall 5.1 Utilities

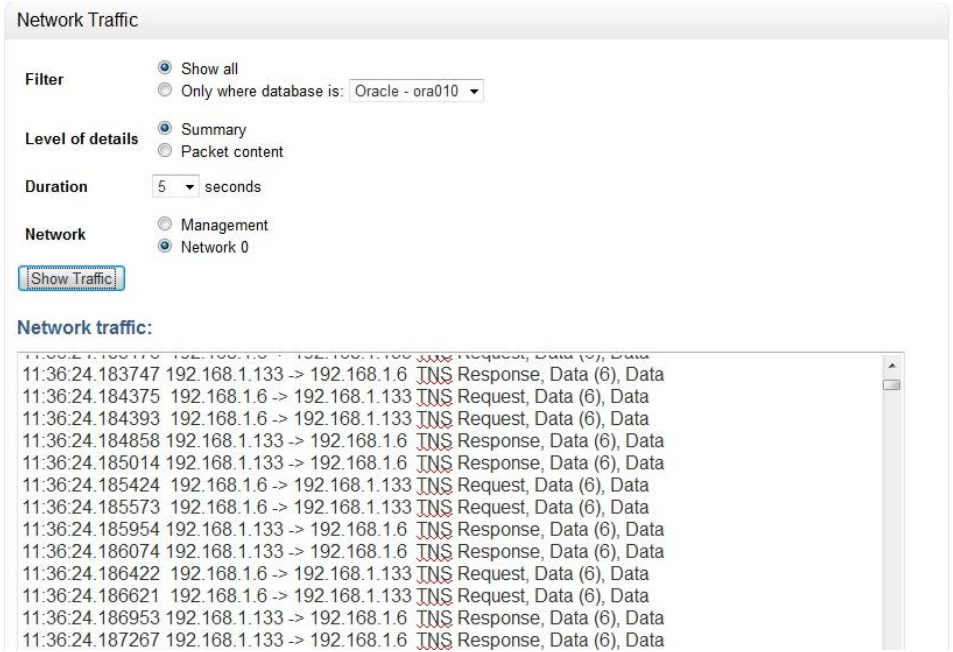
インストール終了後画面

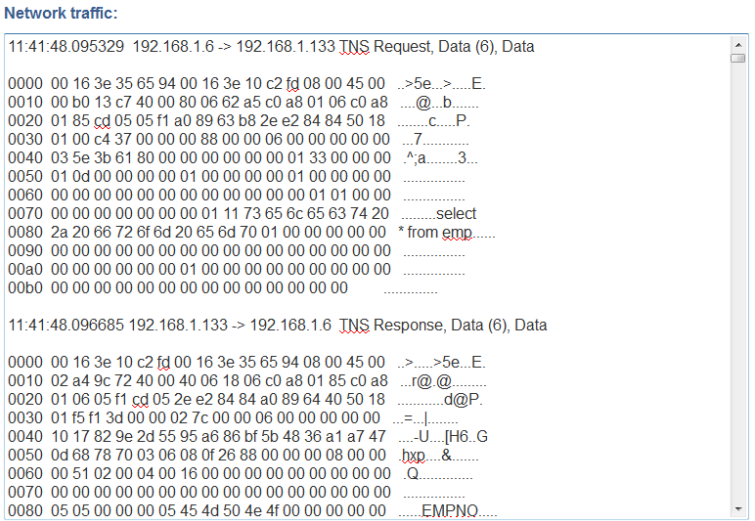


ネットワークへ接続

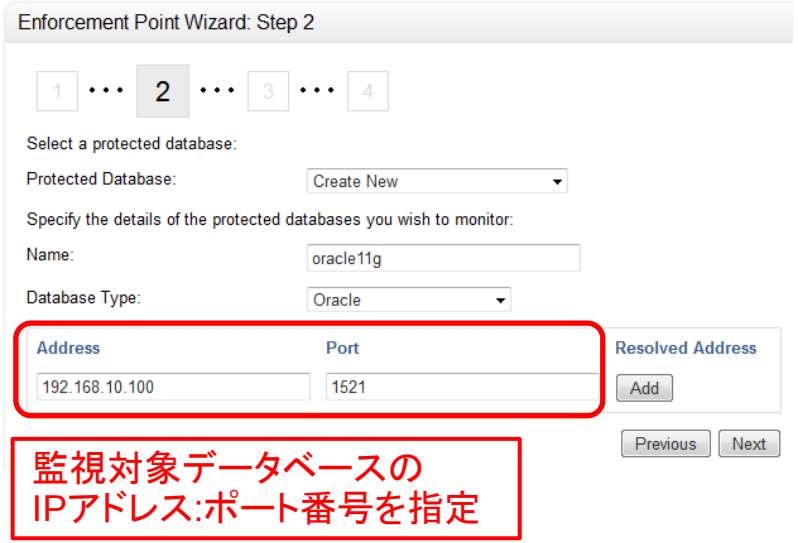


導通確認



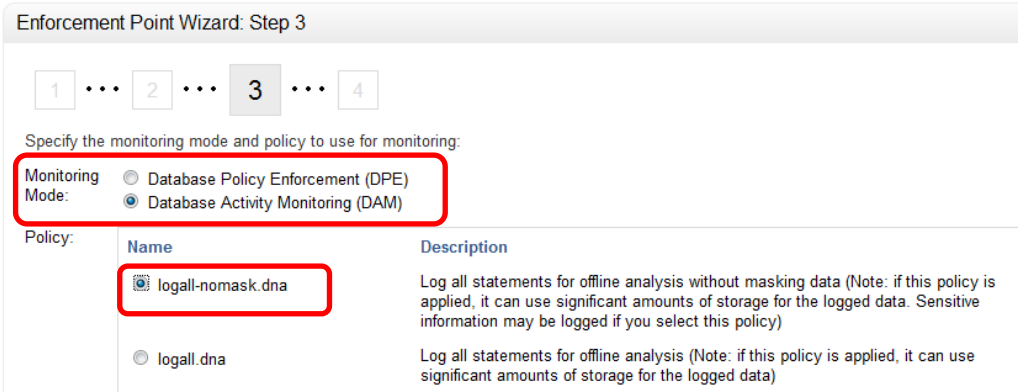


モニタリングの設定



監視対象データベースの
IPアドレス:ポート番号を指定

モード: DAM (Database Activity Monitoring)
ポリシー: logall-nomask.dna (列や値をマスクしない)



受信ログの確認

Search Results

Report Filter (no filter active)

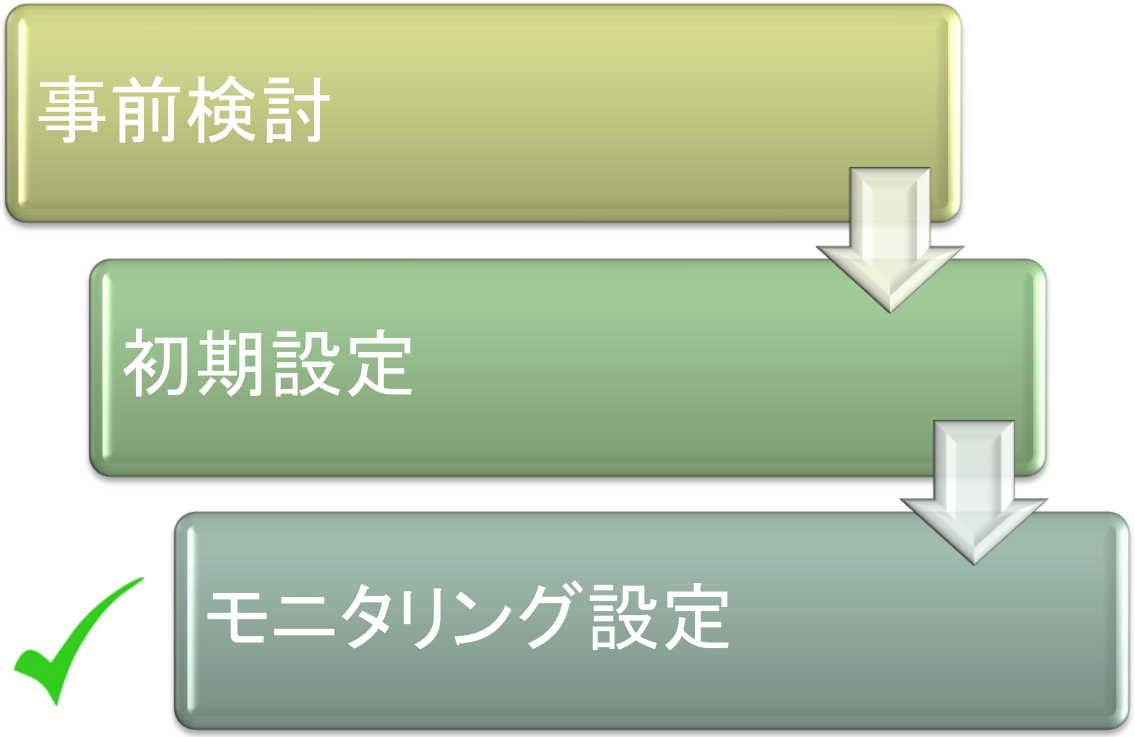
< 1 ... 5 ... 9 10 11 12 13 14 ... 16 >

Time	Type	Origin	Description	DB Client	DB User	Action Code	Thr Sev
2012-03-09 13:59:35.302	statement		select * from DBFW_TEST_EN where COLUM...	192.168.1.6:49442	SCOTT	pass	
2012-03-09 13:59:35.305	statement		select * from DBFW_TEST_EN where COLUM...	192.168.1.6:49442	SCOTT	pass	
2012-03-09 13:59:35.307	statement		select * from DBFW_TEST_EN where COLUM...	192.168.1.6:49442	SCOTT	pass	
2012-03-09 13:59:35.310	statement		select * from DBFW_TEST_EN where COLUM...	192.168.1.6:49442	SCOTT	pass	
2012-03-09 13:59:35.312	statement		select * from DBFW_TEST_EN where COLUM...	192.168.1.6:49442	SCOTT	pass	
2012-03-09 13:59:35.314	statement		select * from DBFW_TEST_EN where COLUM...	192.168.1.6:49442	SCOTT	pass	
2012-03-09 13:59:35.316	statement		select * from DBFW_TEST_EN where COLUM...	192.168.1.6:49442	SCOTT	pass	
2012-03-09 13:59:35.318	statement		select * from DBFW_TEST_EN where COLUM...	192.168.1.6:49442	SCOTT	pass	
2012-03-09 13:59:35.322	statement		select * from テスト表51 where カラム1 = :1	192.168.1.6:49442	SCOTT	pass	
2012-03-09 13:59:35.324	statement		select * from テスト表51 where カラム1 = :1 o...	192.168.1.6:49442	SCOTT	pass	
2012-03-09 13:59:35.326	statement		select * from テスト表51 where カラム1 = :1 o...	192.168.1.6:49442	SCOTT	pass	
2012-03-09 13:59:35.328	statement		select * from テスト表51 where カラム1 = :1 o...	192.168.1.6:49442	SCOTT	pass	
2012-03-09 13:59:35.331	statement		select * from テスト表51 where カラム1 = :1 o...	192.168.1.6:49442	SCOTT	pass	
2012-03-09 13:59:35.333	statement		select * from テスト表51 where カラム1 = :1 o...	192.168.1.6:49442	SCOTT	pass	

2012-03-09 13:59:35.302 statement select * from DBFW_TEST_EN where COLUM... 192.168.1.6:49442

Name	Origin	Value
Transaction Status		
Request Text		select * from DBFW_TEST_EN where COLUMN1 = :1 or COLUMN2 = :2 or COLUMN3 = :3
Response Status		statement success
Response Code		0
Record Type		statement
Performance		
Request Time		2012-03-09 13:59:35.302
Response Time		2012-03-09 13:59:35.303
Transaction Time		0.001
Context		
Traffic Source		network
DB User Name		SCOTT
DB User Name Origin		network
DB User Name (raw)		SCOTT
DB Client Program Name		JDBC Thin Client
DB Client Program Name Origin		network
DB Client IP Address		192.168.1.6
DB Client Port		49442
DB Server IP Address		192.168.1.133
DB Server Port		1521
Service Name		unknown_service
Service Name Origin		generated
Database Type		Oracle
OS User Name		Administrator
OS User Name Origin		network

Oracle Database Firewallの導入 ～モニタリング編

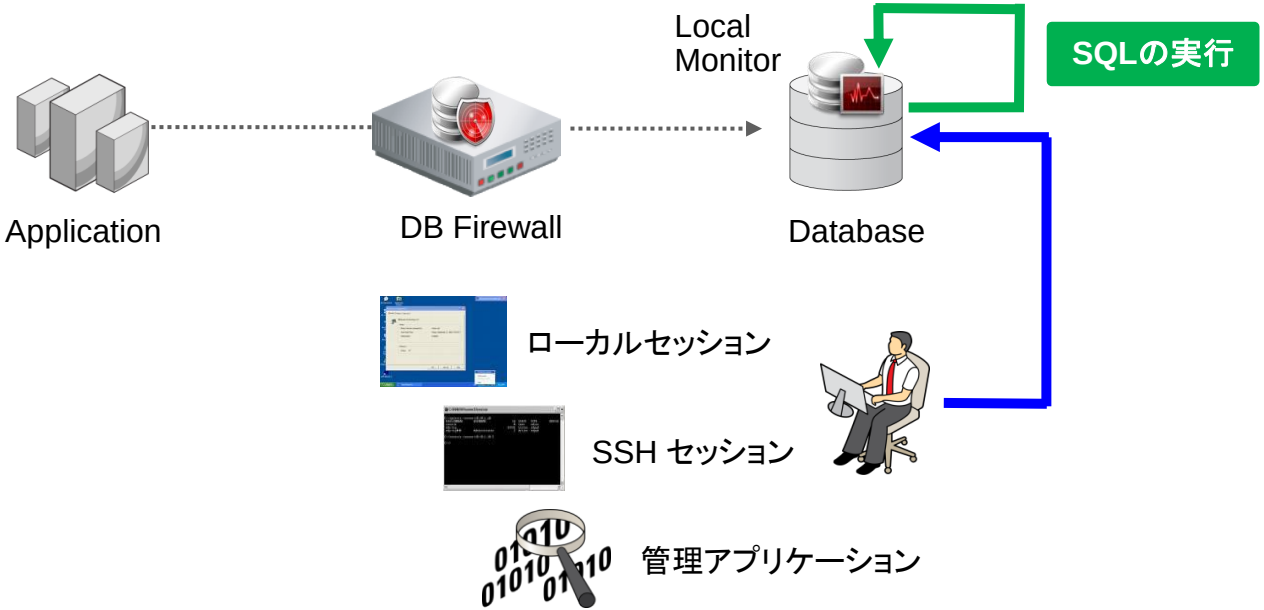


モニタリング設定

	作業項目	作業項目詳細
モニタリング	ローカルモニター	対象となるDBでローカルモニター用のスクリプト実行
	デフォルトレポート (期間指定)	特に作業なし
	デフォルトレポート (特定条件指定)	検索条件の作成 (トランザクション時間や特定の表・列へのアクセス、特定のコマンド等)
	カスタムレポート	Word を使用したレポート定義の作成 (Oracle BI Publisher Desktopアドインを使用)
	スケジュール配信	定期的なレポート配信
リアルタイム アラート	ログ取得期間	ポリシー：logall-nomaskで一定期間ログを収集
	ポリシーの作成	Passする(アラートをしない)SQLを選択、それ以外はWarn(警告)

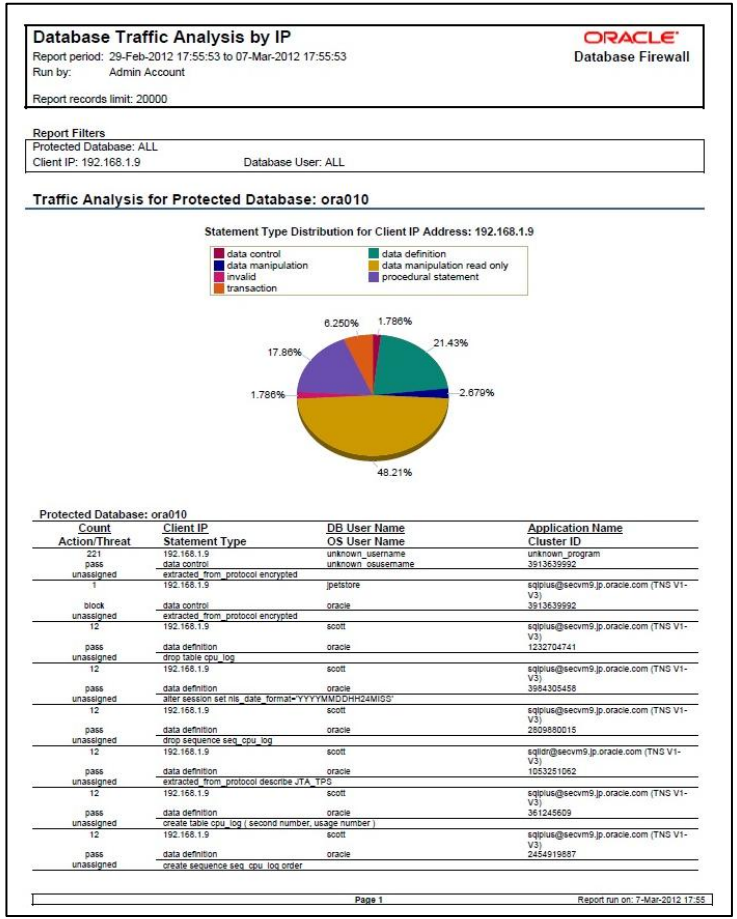
ローカルモニター

- ネットワークを経由しないデータベースへのアクセスログを取得
- トリガーの仕組みを使用し、漏れなくログイン、ログオフ、DDLのログを取得
- 直接SGAを参照し、ローカルで実行されたDMLのログも取得



デフォルト・レポート

- データベースへの管理アクセス
- データベースへのアクセス
- スループット・サマリー
- ある期間に接続していたDBユーザ・リスト
- 最後にログインしたDBユーザ・リスト
- アクセスしたクライアントアプリケーション・リスト
- ある期間に接続していたOSユーザ・リスト
- セッション・サマリー (IPアドレス)
- セッションごとのSQL実行件数サマリー
- ログイン失敗
- 失敗したSQL
- 実行したDDL
- 実行DML (SELECTのみ)
- 実行DML (SELECT以外)



Database Traffic Analysis by IP

ORACLE Database Firewall

Report period: 29-Feb-2012 17:55:53 to 07-Mar-2012 17:55:53
Run by: Admin Account

Report records limit: 20000

Report Filters

Protected Database: ALL
Client IP: 192.168.1.9 Database User: ALL

Traffic Analysis for Protected Database: ora010

Statement Type Distribution for Client IP Address: 192.168.1.9

data control, data definition, data manipulation, data manipulation read only, invalid, procedural statement, transaction

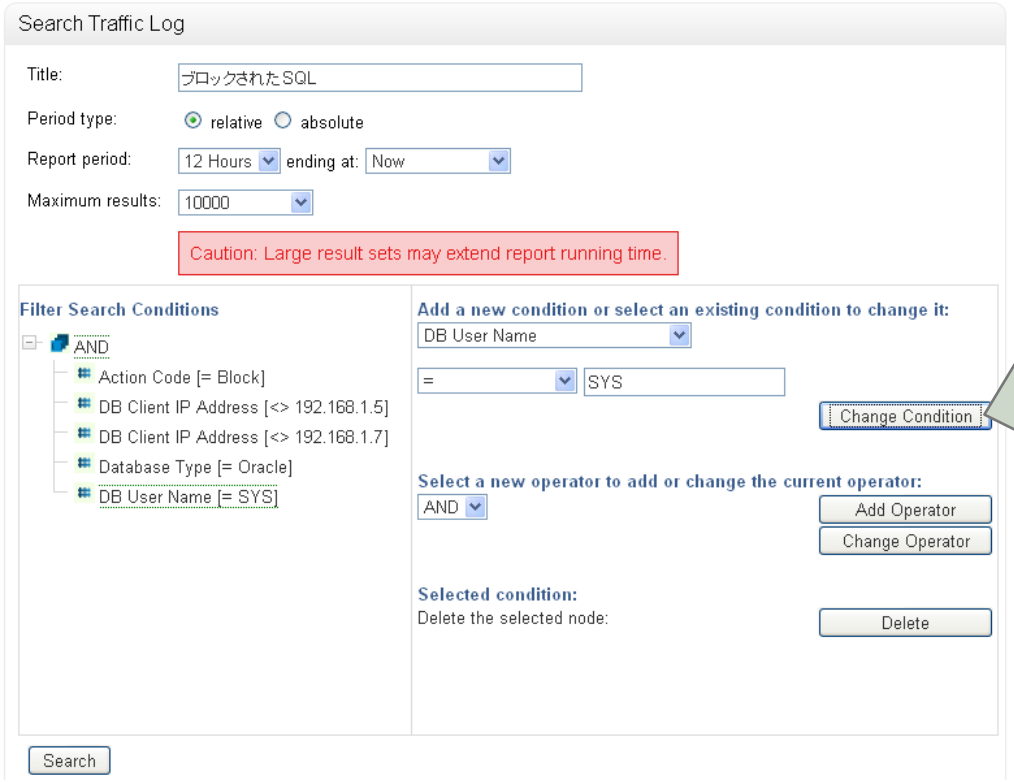
6.250%, 1.786%, 21.43%, 17.86%, 1.786%, 2.679%, 48.21%

Protected Database: ora010

Count / Action/Threat	Client IP / Statement Type	DB User Name / OS User Name	Application Name / Cluster ID
221	192.168.1.9	unknown_username	unknown_program
pass	data control	unknown_osusername	3913639992
unassigned	extracted_from_protocol encrypted		
1	192.168.1.9	jpetstore	sqlplus@secvm9.jp.oracle.com (TNS V1-V3)
block	data control	oracle	3913639992
unassigned	extracted_from_protocol encrypted		
12	192.168.1.9	scott	sqlplus@secvm9.jp.oracle.com (TNS V1-V3)
pass	data definition	oracle	1232704741
unassigned	drop table cpu_log		
12	192.168.1.9	scott	sqlplus@secvm9.jp.oracle.com (TNS V1-V3)
pass	data definition	oracle	3984305458
unassigned	alter session set nls_date_format='YYYYMMDDHH24MISS'		
12	192.168.1.9	scott	sqlplus@secvm9.jp.oracle.com (TNS V1-V3)
pass	data definition	oracle	2809880015
unassigned	drop sequence seq_cpu_log		
12	192.168.1.9	scott	sqlldr@secvm9.jp.oracle.com (TNS V1-V3)
pass	data definition	oracle	1053251062
unassigned	extracted_from_protocol describe JTA_TPS		
12	192.168.1.9	scott	sqlplus@secvm9.jp.oracle.com (TNS V1-V3)
pass	data definition	oracle	361245609
unassigned	create table cpu_log (second number, usage number)		
12	192.168.1.9	scott	sqlplus@secvm9.jp.oracle.com (TNS V1-V3)
pass	data definition	oracle	2454919887
unassigned	create sequence seq_cpu_log order		

Page 1 Report run on: 7-Mar-2012 17:55

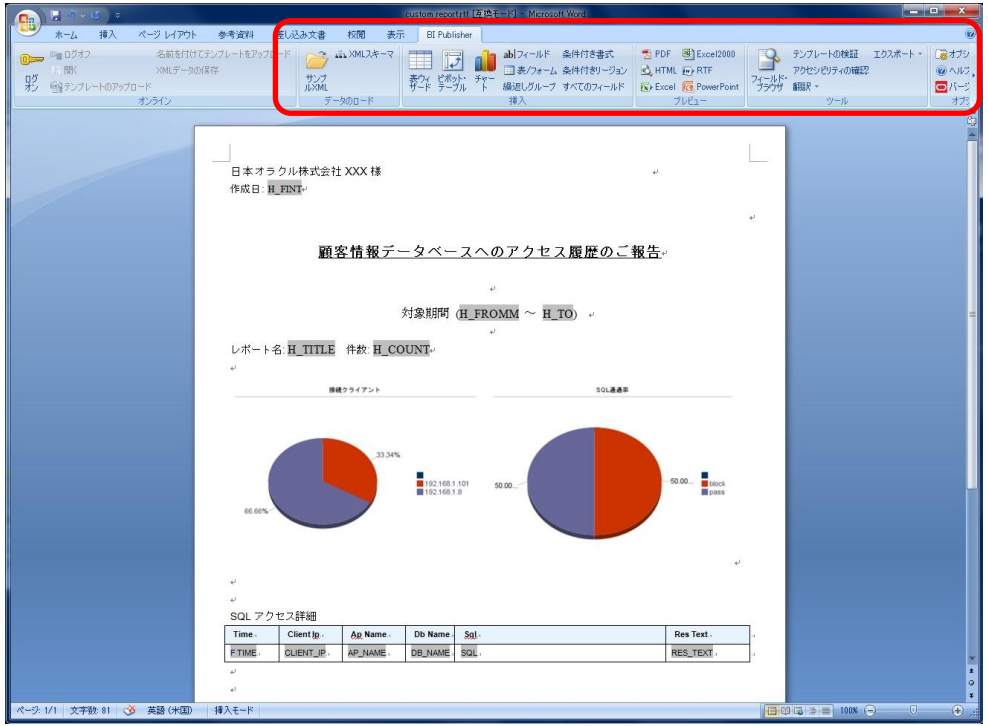
条件指定検索

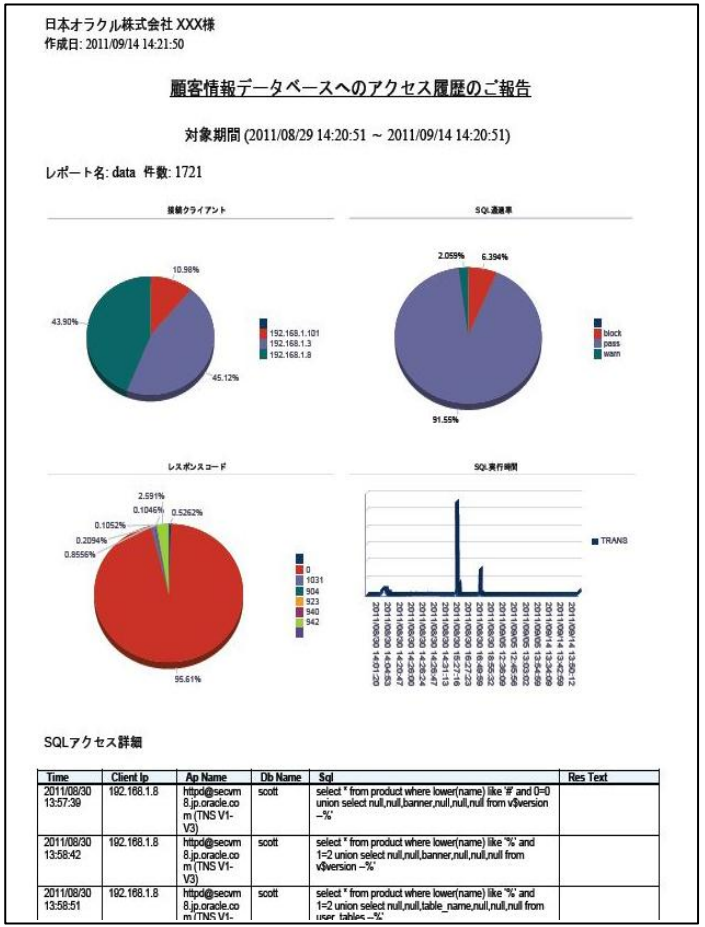


検索条件
- 日付/時間
- アクション結果
- クライアント情報
  - -IPアドレス
  - -OS/DBユーザ名
  - -アプリケーション名
- DBユーザ情報
- SQL
- レスポンスコード
- トランザクション時間など

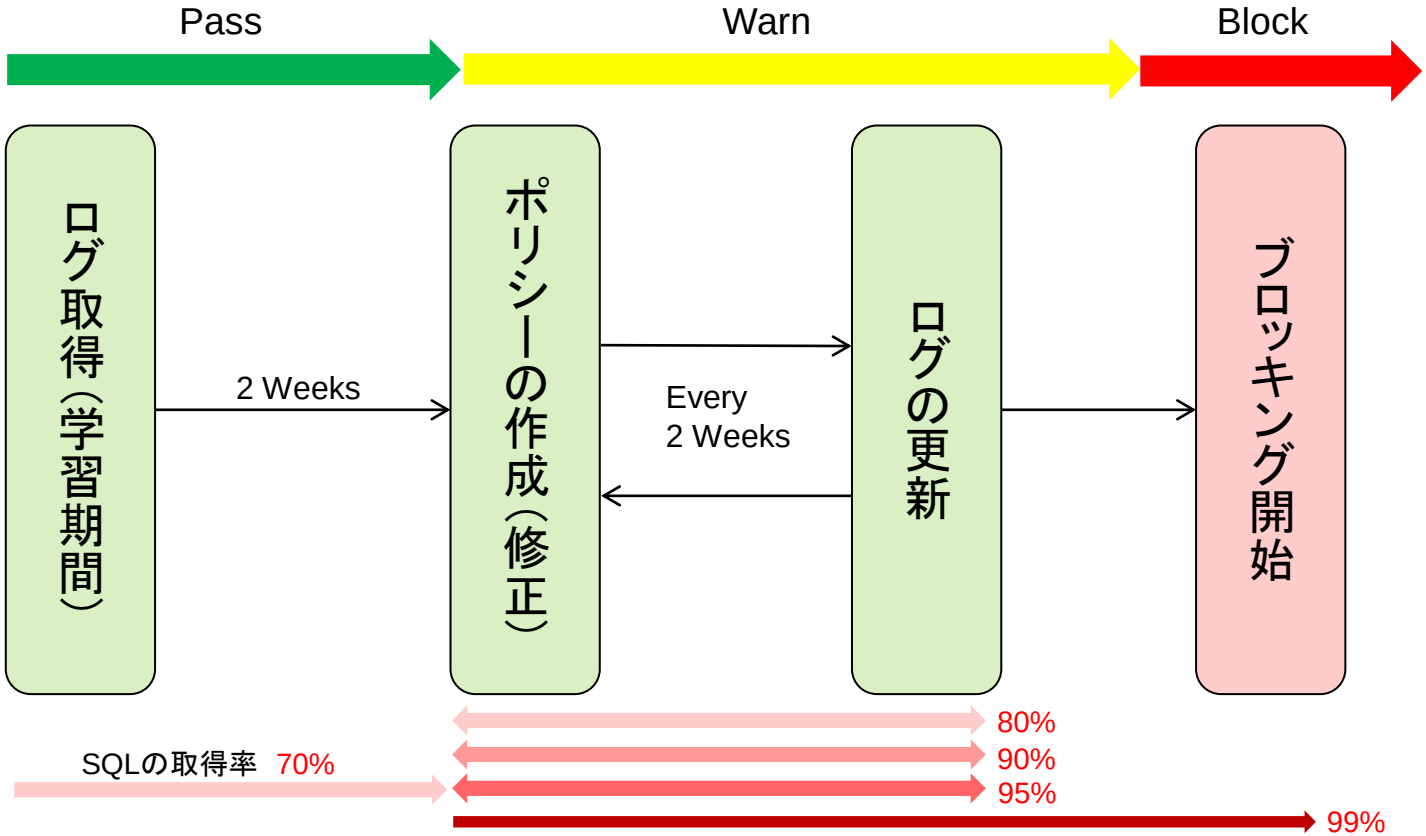
カスタム・レポート

Wordでテンプレート作成 ⇒ DBFWへアップロード





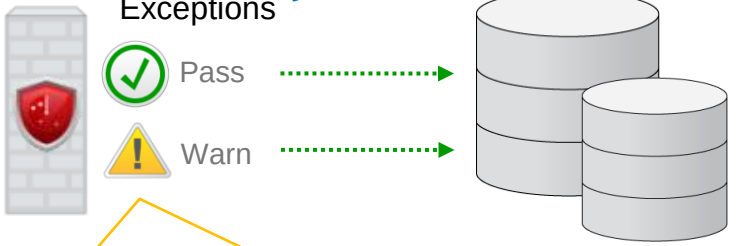
アクセス・ポリシーの作成プロセス例



セッションベースのブラックリスト・ポリシー

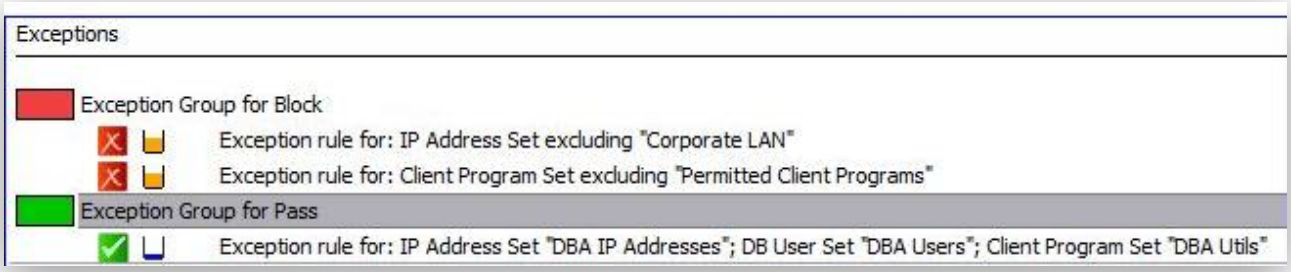
対象とできる セッション情報
IPアドレス
クライアントプログラム名
DBユーザ名
OSユーザ名
時間

SQL
Traffic



192.168.1.10からSYSTEMユーザの場合のみ
ポリシー適用しない

192.168.1.100～245のアクセスはWarn
SQL*PLUSからの直接アクセスをWarn



SQLベースのホワイトリスト・ポリシー

定義ポリシー

PassさせるSQL

それ以外はWarn

SQL Traffic

Pass

Warn

予め許可しておいたSQL以外のアクセスがあった場合は、
ホワイトリスト(デフォルト警告)でリアルタイムアラート

許可するSQL文

Action	Loggin	Statement	Count	IpAddress	Tables	Columns	Users
Pass	Never	select * from product where lower(name) like '%database%'	333	192.168.1.8	PRODUCT	*, NAME	scott
Pass	Never	select * from logon where id='' or 0=0 --' and password=''	8	192.168.1.8	LOGON	*, ID	scott
Pass	Never	select * from logon where id='#' and password='#'	13	192.168.1.8	LOGON	*, ID, PASSWO	scott
Unassigned	Unassigned	select * from product where lower(name) like '########'	1	192.168.1.8	PRODUCT, SCO	*, ADDRESS, CA	scott
Unassigned	Unassigned	select * from product where lower(name) like '########'	1	192.168.1.8	PRODUCT, SYS.	*, COLUMN_NA	scott
Unassigned	Unassigned	select * from product where lower(name) like '########'	1	192.168.1.8	PRODUCT, SYS.	*, COLUMN_NA	scott
Unassigned	Unassigned	select * from product where lower(name) like '########'	1	192.168.1.8	DUAL, PRODUC	*, NAME	scott
Unassigned	Unassigned	select * from product where lower(name) like '########'		192.168.1.8	PRODUCT, SYS.	*, NAME, USERI	scott

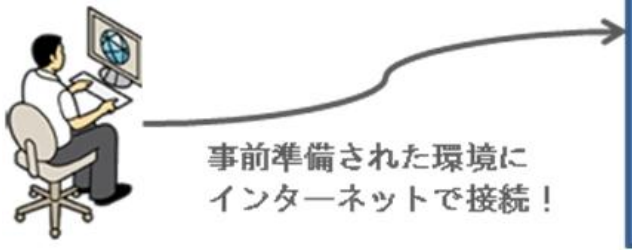
それ以外は定義しない

Oracle Database Firewall 製品無償評価サービス

- **インストールや初期設定などの面倒な作業をすることなく、インターネット経由で簡単に製品環境にアクセスし、製品の機能をお試し頂けます**

体験できるシナリオ

・不正SQL文をモニタリング、アクセス防止
・Database アクセスリソースごとのアクセス制御
・SQL文の内容別にDatabaseアクセス制御
・ストアド・プロシージャやユーザの変更や追加を全て監査
・Oracle Database Firewall のレポート機能



- http://www.oracle.co.jp/campaign/security/productssolutions/solution01/_database_firewall.html

ご質問・ご相談はOpenWorld終了後もお受けしております

あなたにいちばん近いオラクル

Oracle Direct

0120-155-096

（平日9:00-12:00 / 13:00-18:00）

http://www.oracle.com/jp/direct/index.html

各種無償支援サービスもございます。

Hardware and Software

ORACLE

Engineered to Work Together


ORACLE®