

Oracle DBA & Developer Days 2011

日本オラクル、今年最大の技術トレーニングイベント

2011年11月9日(水)～11月11日(金) シェラトン都ホテル東京



ORACLE®

データベース不正アクセス検知の特効薬！！ Oracle Database Firewall

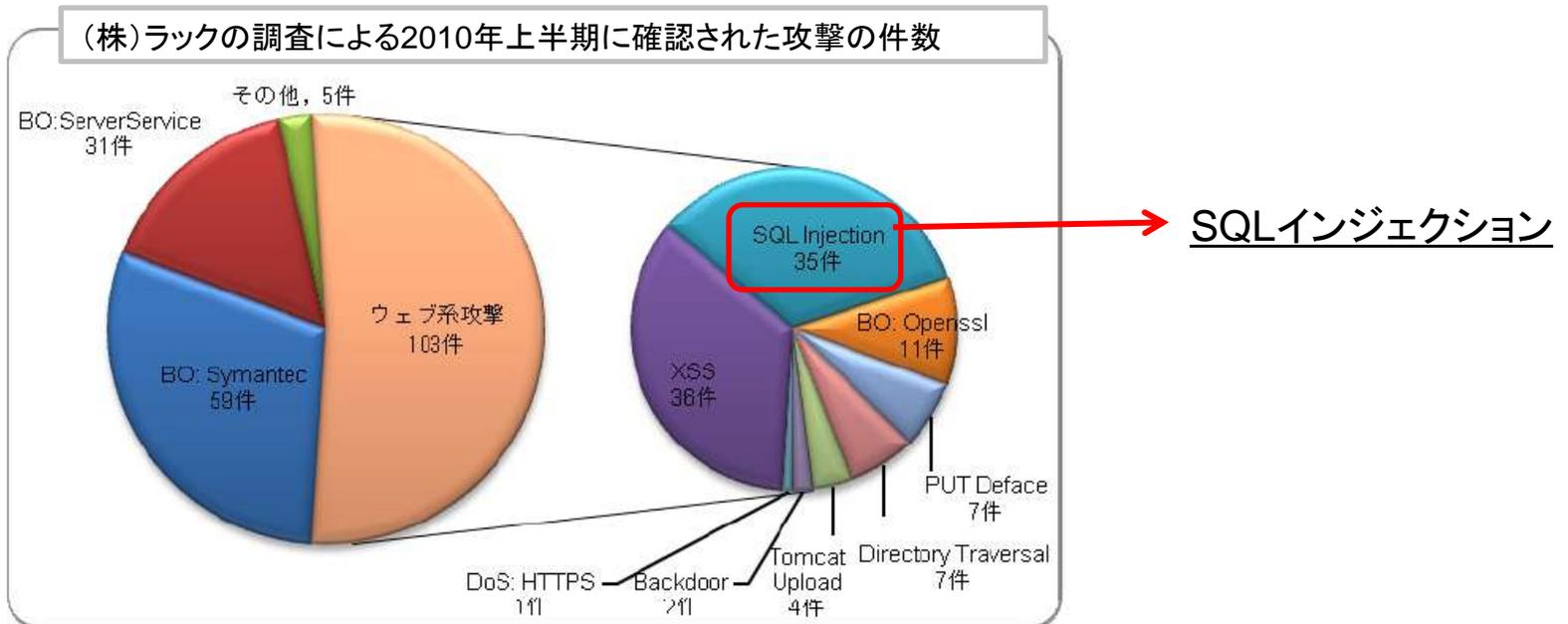
日本オラクル株式会社 製品戦略統括本部 - 戦略製品ソリューション本部
シニアエンジニア, CISSP 西村克也

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とJavaは、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。文中の社名、商品名等は各社の商標または登録商標である場合があります。

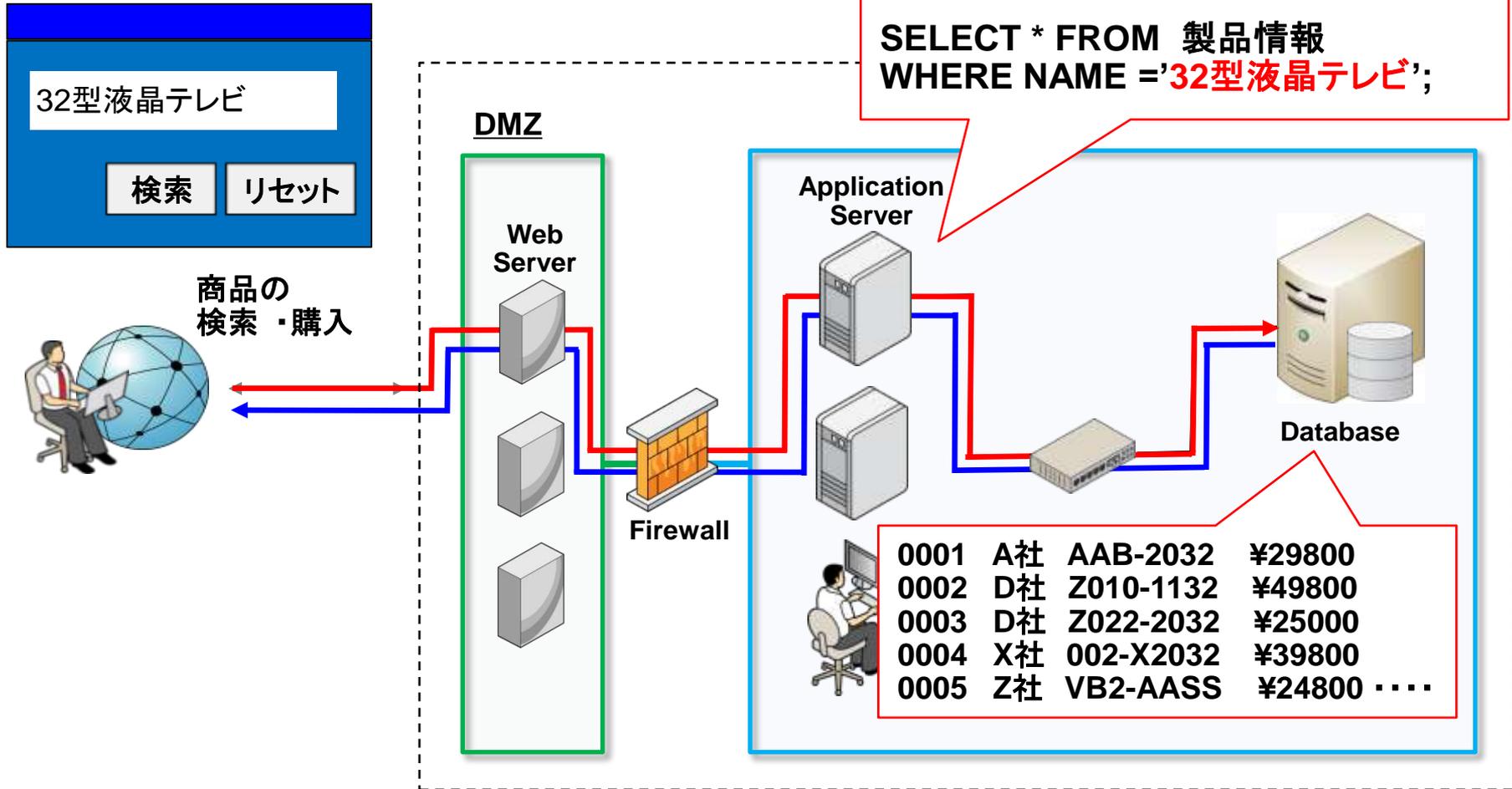
インターネットからの攻撃動向

- SQLインジェクションは引き続き最も多い攻撃の1つ
 - クレジットカード情報などの盗難事故は継続している
 - 情報を盗むだけではなく、他の攻撃の足がかりとして使われることも多い
例：ウイルスの頒布や、受動的攻撃)



例) SQLインジェクション攻撃

～アプリケーションからデータベースへの正常な問い合わせ



例) SQLインジェクション攻撃

~アプリケーションの脆弱性を利用し不正なSQLコマンドを注入

```
SELECT 列1,列2,列3 FROM 製品情報 WHERE  
NAME =" UNION SELECT 列1,列2,列3 from 顧客情報 --
```

```
' UNION SELECT  
列1,列2,列3 from  
顧客情報 --
```

検索

リセット

商品の
検索・購入



顧客情報の
漏えい

脆弱な
アプリケーション

Web
Server

Application
Server

Database

Firewall

```
001 山田太郎 taro.yamada@oracle.com  
002 佐藤花子 hanako.sato@oracle.com  
003 清水次郎 Jiro.shimizu@oracle.com  
004 東三郎 saburo.higashi@oracle.com  
005 鈴木史郎 shiro.suzuki@oracle.com .....
```

遅れがちなSQL インジェクション対策

- 脆弱性を発見したとしても、修正に1ヶ月以上の時間を要している
 - すでに開発ベンダーがない、仕様が分からない等の技術的な問題
 - 膨大に増えていくWEBサイトをすべてチェックできない等の運用的な問題
 - WEBサイトの長期停止による機会損失や膨らんでいく改修費用等のコスト的な問題

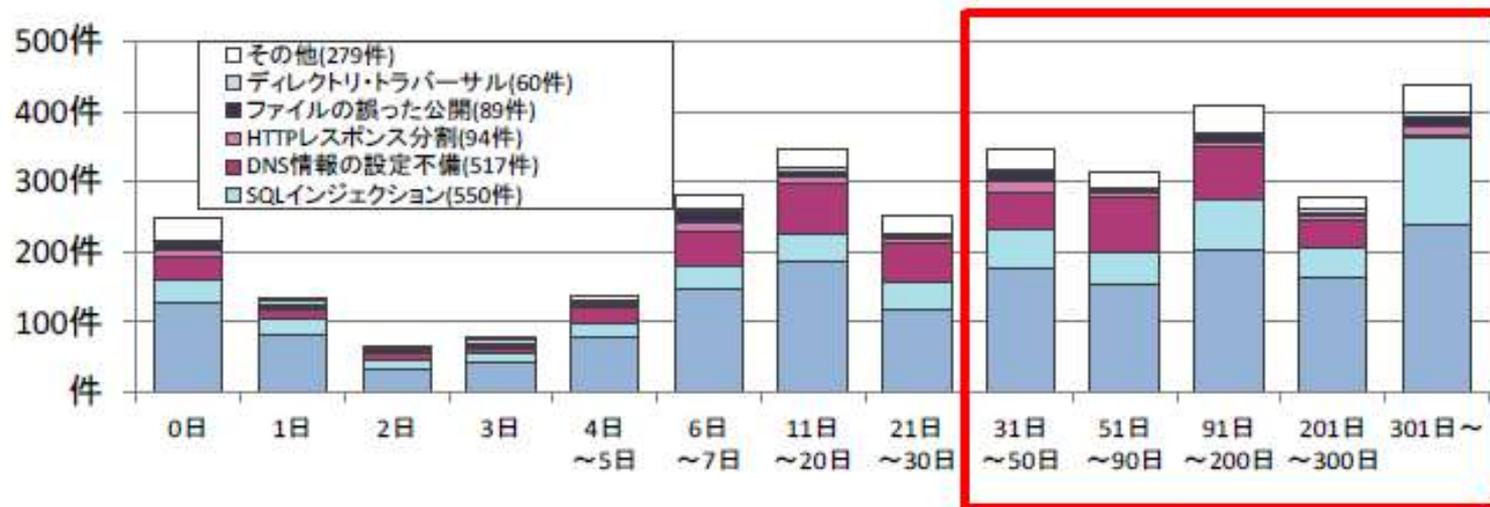


図 1-3 ウェブサイトの修正に要した日数 (2010 年第 4 四半期時点)

引用: IPA Web Application Firewall (WAF)読本 改訂第2版

データベース監査の現実

- 外部や内部からの不正アクセスの早期検知という点では、ログを取ることが非常に重要だが・

データベースの監査ログの機能を知らない

データベースに与えるパフォーマンスへの影響を懸念

何のログを取得すべきか、監査条件の絞り込めない

ログを保存する領域が膨大になる

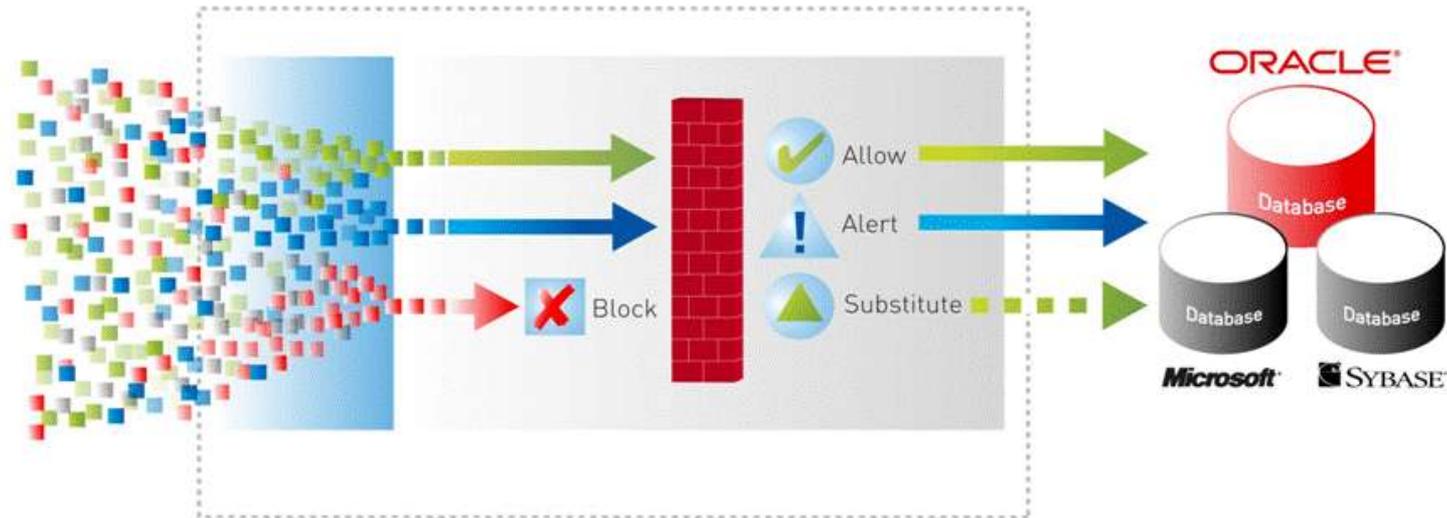
ログをモニタリングしていない

Oracle Database Firewall

不正アクセス防御 & データベース監査



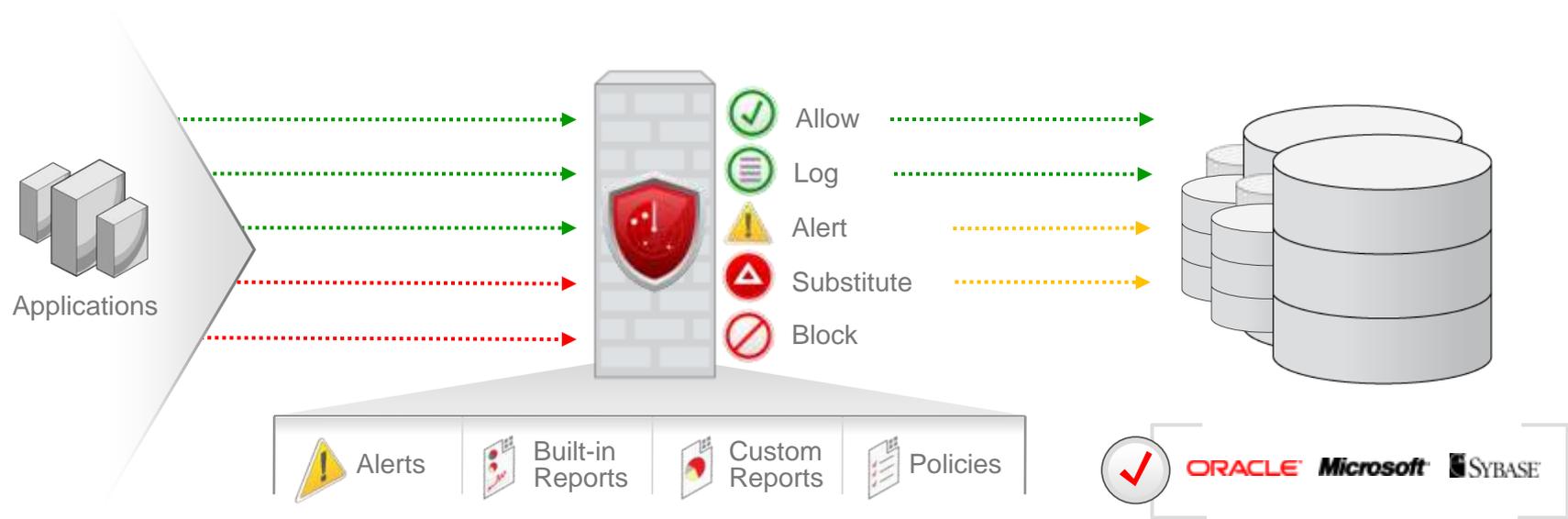
Oracle Database Firewall



- アプリケーションとデータベースの間に位置し、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・レポート

Oracle Database Firewall

防衛のファースト・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

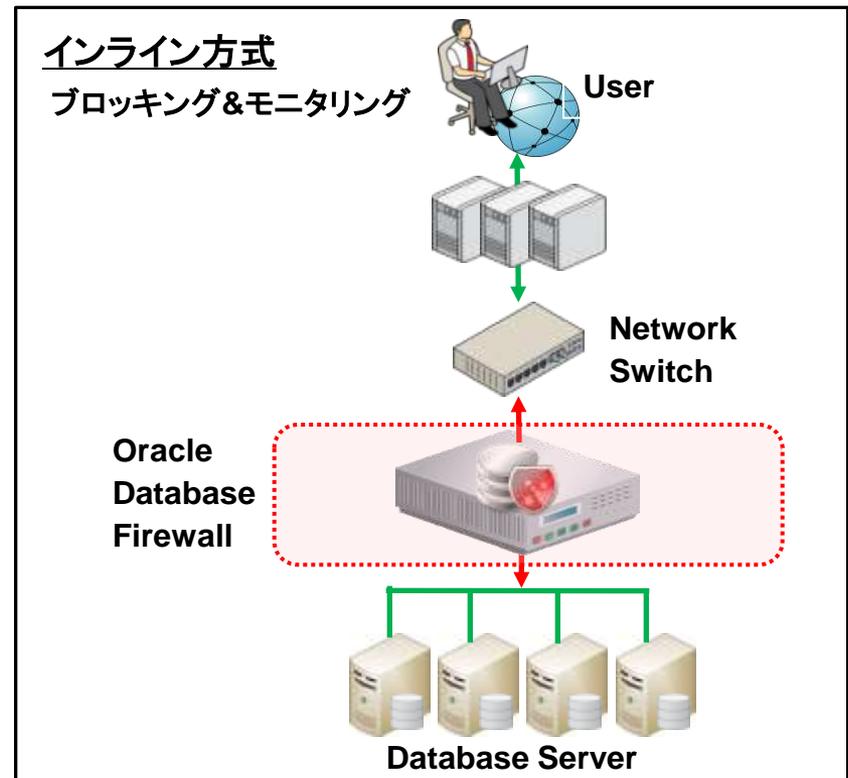
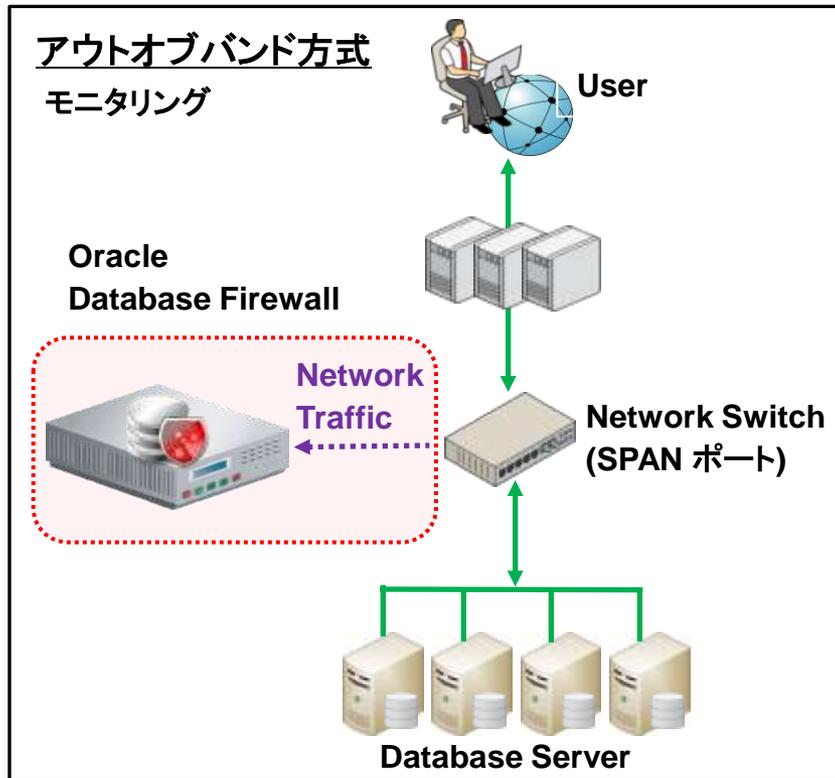
SQL文を正確に理解し検知するSQL文法解析エンジンを搭載

✓ 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

用途に合わせた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
 - ミラーリングポートからネットワークトラフィックを受信してログを生成
- 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
 - ネットワークトラフィックを受信し、Block、Passのポリシーを適用し、ログを生成



正確な検知の重要性

- フォールスポジティブ (False positives)
 - 誤検出
 - 正しいSQLを不正なSQLとして検出してしまうこと
- フォールスネガティブ (False negatives)
 - 検出漏れ
 - 不正なSQLを検出せず見逃してしまうこと
- 例えば、
- 1秒あたり3000SQL = 1日あたり260万SQL
- 0.001%をフォールスポジティブ = 1ヶ月あたり7800件のアラート発生
- 0.0001%のフォールスネガティブ = 1ヶ月あたり 26件の不正アクセスの可能性

正確に検知ができなければ、
不正なアクセスを見逃し、さらに運用が追いつかない

パターンマッチングの限界

- パターンマッチング
 - 正規表現などによって特定の文字列を見つける

TRUEとなる条件

- 1=1
- 10=10
- 20000=(1000+19000)
- 'cat'='cat'
- 'dog'='dog'
- LEFT('catastrophe', 3)='cat'
- SQRT(49) = (8-1)/1
- 'cat' <> 'mouse'
- SIN(45) = COS(45)
- CAST(123) as STR <> 123
- '567'<>567<>789
- " = "

様々なUNIONの記述

```
uni/* */on
u/* */nion
char(117,110,105,111,110)
u n i o n
```

検出する文字列を漏れなくすべて網羅することは不可能
フォールスポジティブとフォールスネガティブの増加

Oracle Database Firewallの検知方法

～SQLの文法を理解した正確な検知

- SQLは約400のキーワードや厳格な文法のルール(ISO/IEC 9075)が定義されており、それらの文法構造を理解し判断する

```
UPDATE tbl_users SET comments = 'The user has asked for another
account no [and] wishes to be billed for services [between] 1/2/2009
and 2/2/2009, [and] wants to know [where] the invoice should be sent
to. She will [select] the new service level agreement to run [from]
3/7/2009 next month' WHERE id = 'A15431029';
```

KEY WORDS

SCHEMA

DATA

OPERATORS

- SQLは分析され、クラスタにグループ化される
 - SQLポリシーの管理対象は、クラスタ単位で行われる
 - DATAの値が異なっても、同じクラスタとして文法構造が同一であれば、漏れなくポリシーが適用される

```
Cluster 1 : SELECT * FROM certs WHERE cert-type = '18'
```

```
Cluster 1 : SELECT * FROM certs WHERE cert-type = '3999'
```

```
Cluster 2: SELECT * FROM certs WHERE cert-type = 'PHE8131' and location = 1
```

Oracle Database Firewall

ホワイトリスト方式



- ユーザーやアプリケーションからのアクセスに対して、許可するSQLを定義
- 時間、日、曜日、ネットワーク、アプリケーション等の要素を組み合わせ、アクセス許可の定義をすることが可能
- 許可するSQLのリスト生成は、アプリケーションから簡単に収集
- 定義されたSQLのリストにないトランザクションは、即座に拒否

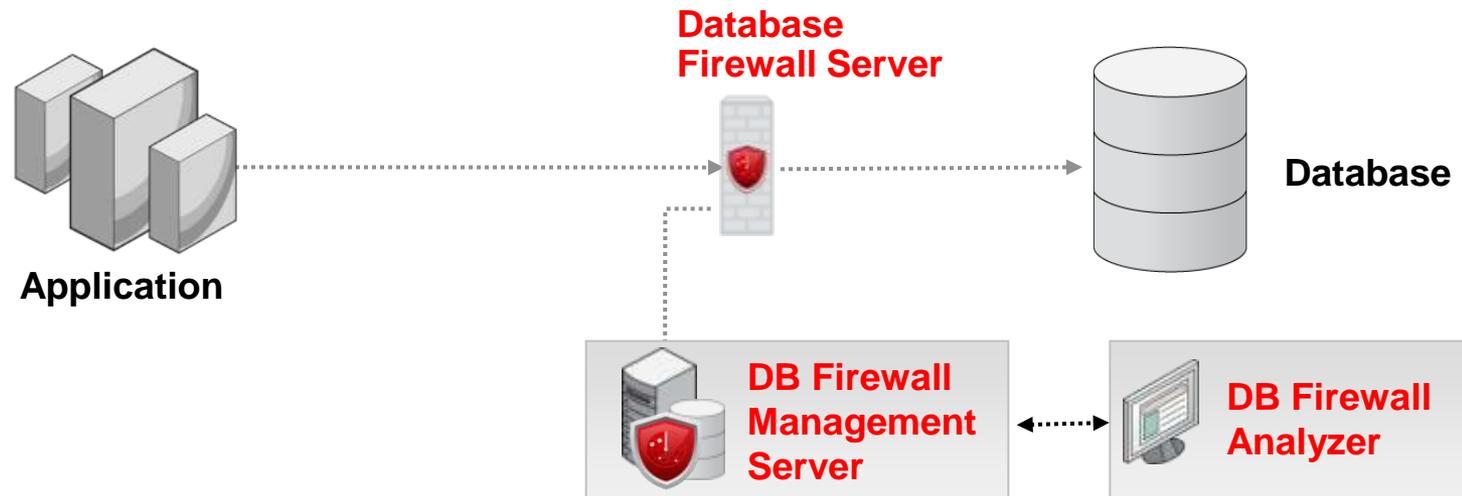
Oracle Database Firewall

ブラックリスト方式



- ユーザーやアプリケーションからのアクセスに対して、拒否するSQLを定義
- 時間、日、曜日、ネットワーク、アプリケーション等の要素を組み合わせて、アクセス拒否の定義をすることが可能
- 拒否するSQLは、テキストファイルから一括してローディング
- 定義されたSQLのリストを含むトランザクションは、即座に拒否

Oracle Database Firewall コンポーネントの役割



• Oracle Database Firewall Server

- ネットワークトラフィック内のSQLをキャプチャし、ブロッキング・モニタリングを行う
- AP～DB間に配置するインライン方式、ミラーリングポートを利用したアウトオブバンド方式の2種類
- スタンドアロン構成の場合は、Management Serverのすべての機能を担う

• Oracle Database Firewall Management Server

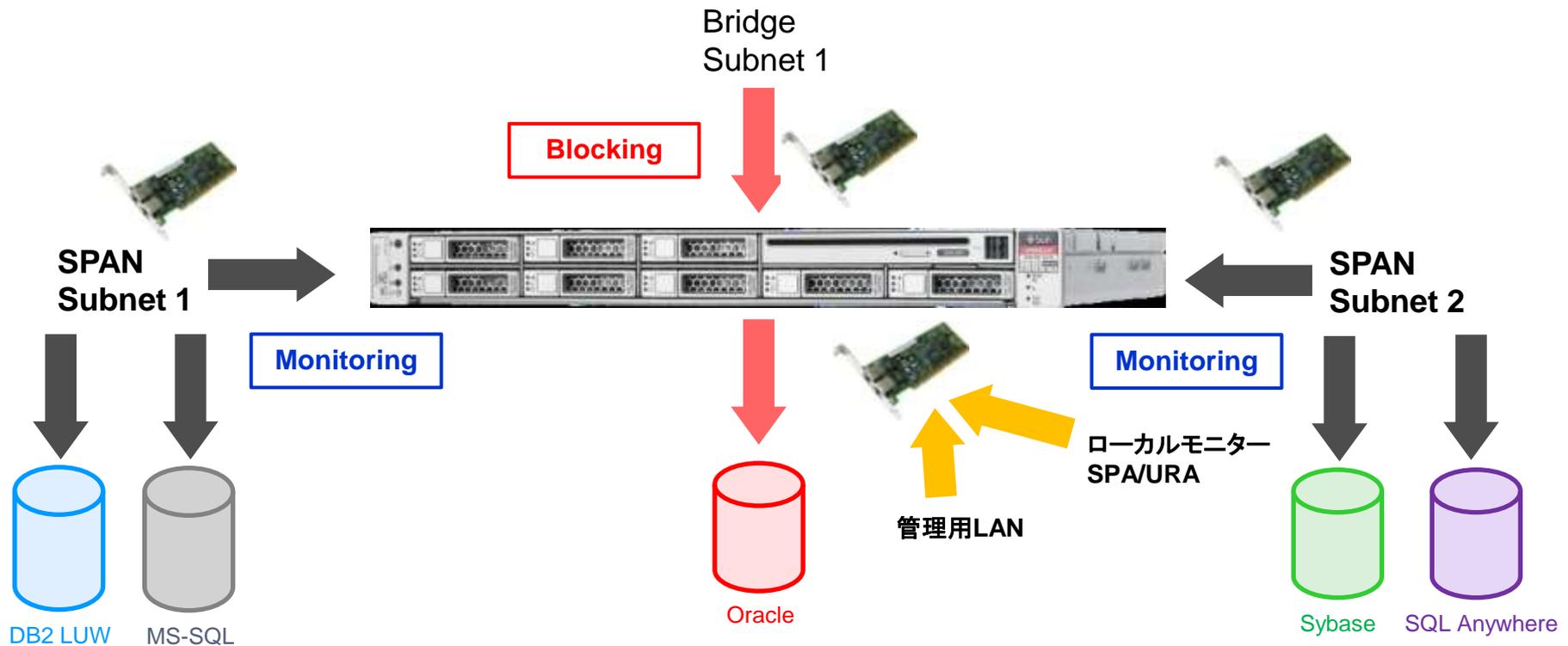
- DBFWのモニタリング・ログのリポジトリサーバ
- すべてのDBFWの管理・監視を一元的に管理し、ログの分析、レポートを行う

• Oracle Database Firewall Analyzer

- ポリシー作成を行うクライアントアプリケーション

1台でネットワーク全体を防御・検知

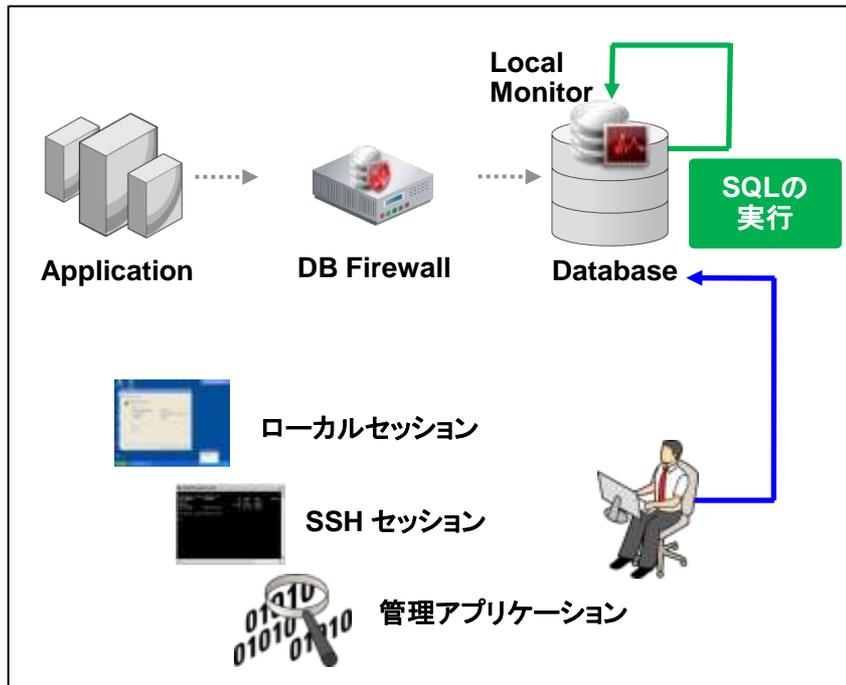
- 最大8ポートを使用してモニタリング、ブロッキングの組み合わせ可能
- 1つのOracle Database Firewallで複数の異なるネットワーク・セグメントに対応
- Oracle Database 8i~11gの全エディション、SQL Server、DB2、Sybase等にも対応



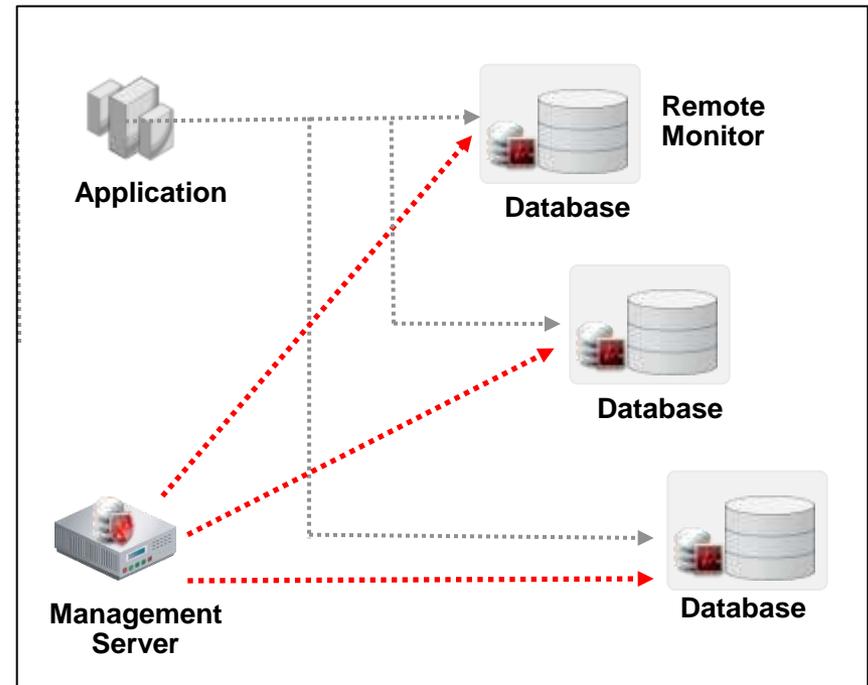
すべてのデータベースアクセスを記録

- DB Firewallを経由しないデータベースへのアクセスも漏れなくモニタリング
 - ネットワークを経由せずに、直接データベースサーバにログインしたアクセス
 - 小規模に点在する個々のデータベースのアクセス

ローカルモニター



リモートモニター



モニタリングログの検索機能

Search Traffic Log

Title:

Period type: relative absolute

Report period: 12 Hours ending at: Now

Maximum results: 10000

Caution: Large result sets may extend report running time.

Filter Search Conditions

- AND
 - Action Code [= Block]
 - DB Client IP Address [<> 192.168.1.5]
 - DB Client IP Address [<> 192.168.1.7]
 - Database Type [= Oracle]
 - DB User Name [= SYS]

Add a new condition or select an existing condition to change it:

DB User Name

= SYS

Change Condition

Select a new operator to add or change

AND

Selected condition:
Delete the selected node:

Search Results

Report Filter (no filter active)

Time	Type	Origin	Description	DB Client	DB User	Action Code	Threat Severity
2011-04-07 15:33:48.000	statement		SELECT OBJOID, CLSOID, DECODE(BITAN...	0.0.0.0	SYS	pass	unassigned
2011-04-07 15:34:49.000	statement		SELECT OBJOID, CLSOID, DECODE(BITAN...	0.0.0.0	SYS	pass	unassigned
2011-04-07 15:57:05.000	statement		SELECT OBJOID, CLSOID, DECODE(BITAN...	0.0.0.0	SYS	pass	unassigned
2011-04-07 15:57:50.000	statement		SELECT OBJOID, CLSOID, DECODE(BITAN...	0.0.0.0	SYS	pass	unassigned
2011-04-07 15:58:50.000	statement		select u.name, o.name, decode(...	0.0.0.0	SYS	block	unassigned
2011-04-07 16:01:58.000	statement		insert into wrh\$_latch (snap_id, dbi...	0.0.0.0	SYS	block	unassigned
2011-04-07 16:19:52.000	statement		SELECT OBJOID, CLSOID, DECODE(BITAN...	0.0.0.0	SYS	pass	unassigned
2011-04-07 16:20:16.143	statement		select * from employees	10.159.223.201:4029	unknown_username	pass	unassigned
2011-04-07 16:20:17.468	statement		select * from employees	10.159.223.201:4029	unknown_username	pass	unassigned

検索条件

- ・アクション結果 (Pass/Block/Warn)
- ・DBサーバ情報
- ・クライアント情報
- ・ユーザ情報
- ・SQL
- ・レスポンスコード
- ・トランザクション時間

などの組み合わせ

用途に応じたログの検索例①

- 正常に実行されなかったSQLを一括して検索

Response Codeが0以外のSQLは？

2011-07-13 11:21:53.715	session		CONNECTED,FAILED LOGIN	192.168.1.3:50051
Name	Origin	Value		
Transaction Status				
SQL Request		CONNECTED,FAILED LOGIN		
Response Status		login fail		
Response Code		1017		
Response Text		ORA-01017: ユーザー名/パスワードが無効です。ログオンは拒否されました。		

ORA-XXXXのエラーコードのSQLを抽出

2011-07-13 11:23:17.499	statement		select * from dba_users	192.168.1.3:50052
Name	Origin	Value		
Transaction Status				
SQL Request		select * from dba_users		
Response Status		statement fail		
Response Code		942		
Response Text		ORA-00942: 表またはビューが存在しません。		

2011-07-13 11:22:16.477	statement		grant dba to hr	192.168.1.3:50052
Name	Origin	Value		
Transaction Status				
SQL Request		grant dba to hr		
Response Status		statement fail		
Response Code		1031		
Response Text		ORA-01031: 権限が不足しています。		

用途に応じたログの検索例②

- トランザクションの実行時間を定期的に監視し、極端に遅いSQLを特定する

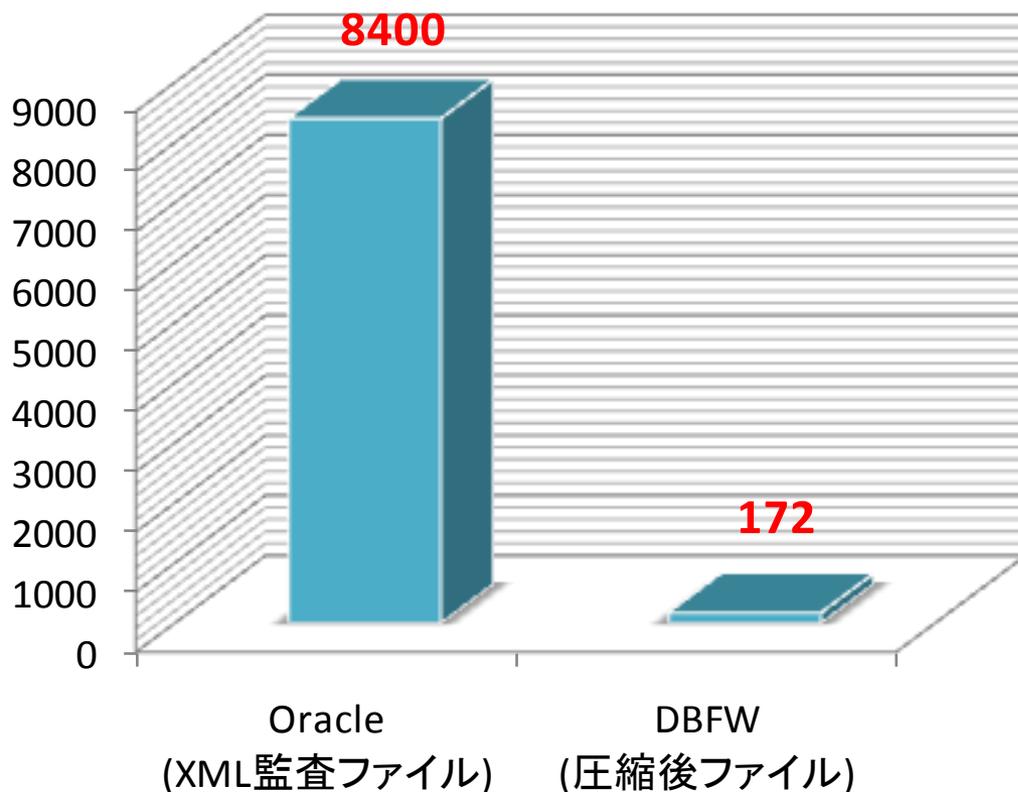
Transaction Timeが30秒を超えるSQLは?

Time	Type	Origin	Description	DB Client	DB User	Action Code
2011-06-22 20:59:56.136	statement		<code>select * from base_tbl where col1=5999</code>	192.168.1.3:44301	scott	pass
Name	Origin	Value				
Transaction Status						
SQL Request		<code>select * from base_tbl where col1=5999999</code>				
Response Status		statement success				
Response Code		0				
Record Type		statement				
Performance						
Request Time		2011-06-22 20:59:56.136				
Response Time		2011-06-22 21:00:53.119				
Transaction Time		56.983				

性能劣化を引き起こすSQLを特定

モニタリング・ログの圧縮

1200万 監査レコード(MB)



OracleのXML監査ログを
1200万件生成した場合
総サイズは約8.4GB

DBFWの圧縮ファイルの場合
172MB

ログの保全量を50分の1に
することができる

※ログのサイズはSQLの種類
や長さに依存する

海外事例: 某投資銀行(大規模DB監査システム)

ビジネス要件:

- 従来のマニュアル監査を廃止
- 監査要件を満たすPDFとExcelレポートを生成
- 1日 1.7億発生するトランザクションを24時間×365日漏れなく取得すること

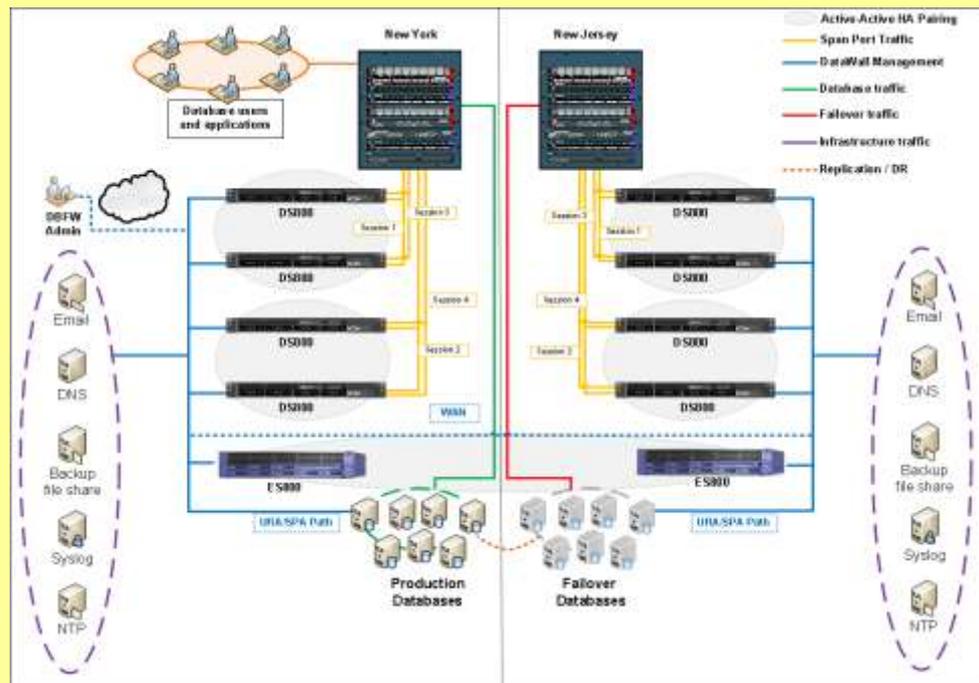
Oracle Database Firewall によるソリューション:

- 600を超えるデータベースをすべてモニタリング
- データセンターのフェイルオーバー時であっても、Database Firewallの高可用性機能によりサポート
- Database Firewall Management Serverにレポートリング機能を集約して管理

導入における効果:

- Delivery of 20+ audit reports per day to database security team.
- 1日あたり20種類の監査レポートがセキュリティ部門に自動的に配信
- 100%のモニタリングを実現

600を超えるデータベースを24時間365日 完全なモニタリングを実現



Oracle Database Firewallを選択した理由は
「ハイパフォーマンスと正確なモニタリングを
両方実現することができるから」

Oracle Database Security ソリューション

不正アクセス防御 & データベース監査

特権ユーザ管理

Oracle Database Firewall

Oracle Database Vault

SQLインジェクション

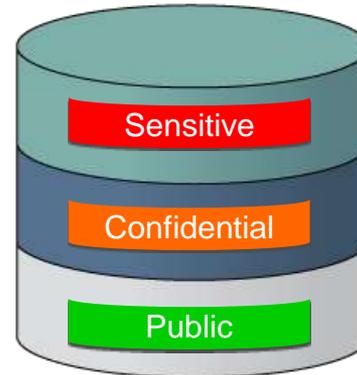


サーバへの侵入



不正SQLの検知と遮断

- Allow
- Log
- Alert
- Substitute
- Block



権限のない不正な操作の防止

管理者権限のコントロール



データの暗号化 & マスキング

データベース暗号化



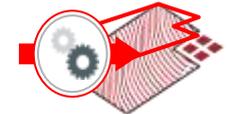
ネットワーク暗号化



外部出力データの暗号化



テストデータのマスキング



Oracle Advanced Security

Oracle Data Masking

ORACLE

OTNセミナーオンデマンド

コンテンツに対する
ご意見・ご感想を是非お寄せください。

OTNオンデマンド 感想



http://blogs.oracle.com/oracle4engineer/entry/otn_ondemand_questionnaire

上記に簡単なアンケート入力フォームをご用意しております。

セミナー講師/資料作成者にフィードバックし、
コンテンツのより一層の改善に役立てさせていただきます。

是非ご協力をよろしくお願いいたします。

OTNセミナーオンデマンド

日本オラクルのエンジニアが作成したセミナー資料・動画ダウンロードサイト

掲載コンテンツカテゴリ(一部抜粋)

Database 基礎

Database 現場テクニック

Database スペシャリストが語る

Java

WebLogic Server/アプリケーション・グリッド

EPM/BI 技術情報

サーバー

ストレージ



超入門! Oracle データベースって何
再生時間: 60分

100以上のコンテンツをログイン不要でダウンロードし放題

データベースからハードウェアまで充実のラインナップ

毎月、旬なトピックの新作コンテンツが続々登場

例えばこんな使い方

- 製品概要を効率的につかむ
- 基礎を体系的に学ぶ/学ばせる
- 時間や場所を選ばず(オンデマンド)に受講
- スマートフォンで通勤中にも受講可能



毎月チェック!



[コンテンツ一覧](http://www.oracle.com/technetwork/jp/ondemand/index.html) はこちら

<http://www.oracle.com/technetwork/jp/ondemand/index.html>

[新作&おすすめコンテンツ情報](http://oracletech.jp/seminar/recommended/000073.html) はこちら

<http://oracletech.jp/seminar/recommended/000073.html>

OTNオンデマンド



オラクルエンジニア通信

オラクル製品に関わるエンジニアの方のための技術情報サイト

オラクルエンジニア通信 - 技術資料、マニュアル、セミナー

Oracleエンジニアのための技術情報サイト by Oracle Japan

新着情報を知りたい

技術資料を探したい

セミナーを受けたい

About

Oracleエンジニアの方がスキルアップしていただくために、厳選した情報をお届けしています

技術資料	<p>インストールガイド・設定チュートリアルetc. 欲しい資料への最短ルート</p>	アクセスランキング	<p>他のエンジニアは何を見ているのか？人気資料のランキングは毎月更新</p>
特集テーマ Pick UP	<p>性能管理やチューニングなど月間テーマを掘り下げて詳細にご説明</p>	技術コラム	<p>SQLスクリプト、索引メンテナンスetc. 当たり前運用/機能が見違える!?</p>

<http://blogs.oracle.com/oracle4engineer/>

オラクルエンジニア通信



The screenshot shows the top section of the oracletech.jp website. On the left is the 'oracletech.jp' logo with the tagline '好奇心が、エンジニア人生を豊かにする。'. On the right is the 'ORACLE' logo, a search bar, and social media icons for Twitter, Facebook, LinkedIn, YouTube, and RSS. Below these is a red navigation bar with five buttons: '製品/技術情報', 'スキルアップ', 'セミナー', 'キャンペーン', and 'ちょっと一息'.

製品/技術
情報



Oracle Databaseっていくら？オプション機能も見積れる簡単ツールが大活躍

セミナー



基礎から最新技術までお勧めセミナーで自分にあった学習方法が見つかる

スキルアップ



ORACLE MASTER ! 試験頻出分野の模擬問題と解説を好評連載中

Viva!
Developer



全国で活躍しているエンジニアにスポットライト。きらりと輝くスキルと視点を盗もう

<http://oracletech.jp/>

oracletech



あなたにいちばん近いオラクル



Oracle Direct

まずはお問合せください

Oracle Direct



システムの検討・構築から運用まで、ITプロジェクト全般の相談窓口としてご支援いたします。
システム構成やライセンス/購入方法などお気軽にお問い合わせ下さい。

Web問い合わせフォーム

専用お問い合わせフォームにてご相談内容を承ります。
http://www.oracle.co.jp/inq_pl/INQUIRY/quest?rid=28

※フォームの入力にはログインが必要となります。
※こちらから詳細確認のお電話を差し上げる場合がありますので
ご登録の連絡先が最新のものになっているかご確認下さい。

フリーダイヤル

0120-155-096

※月曜～金曜
9:00～12:00、13:00～18:00
(祝日および年末年始除く)

ORACLE

Hardware and Software **Engineered to Work Together**

ORACLE®