



最新のWebアプリケーション攻撃の動向と データセキュリティ対策

2013年10月22日

株式会社Imperva Japan, Technical Director
桜井 勇亮

© 2013 Imperva, Inc. All rights reserved.

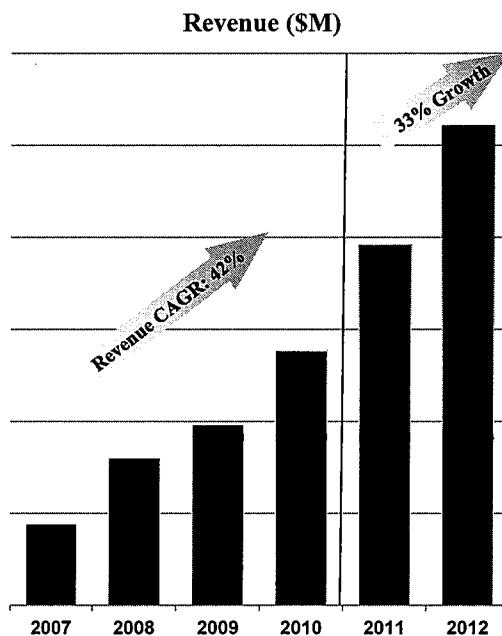
本日のアジェンダ

- 弊社紹介
- 2013年 Webセキュリティ事件簿
 - 深刻なWeb関連の脆弱性情報公開 – Apache Struts2
 - アカウントリスト型攻撃
- Imperva SecureSphereの製品紹介
 - Web Application Firewall
 - Database Firewall / File Firewall

Impervaのご紹介

お客様のビジネスの原動力となるデータを保護すること

- 事業 データ・セキュリティ製品の開発・販売
- 設立 2002年(2011年11月 NYSE上場)
- 本社 米国カリフォルニア州Redwood City
- CEO & President Shlomo Kramer(シュロモ・クレイマー)
- CTO Amichai Shulman(アミカイ・シュルマン)
- 従業員数 550名+



実績:

- 60カ国以上の展開
2,600社、数千を超えるサイトを保護
- 世界的な金融データ・サービス会社
 - 世界的な電気通信会社
 - 世界的なコンピュータ・ハードウェア会社
 - 200を超える政府機関や部署
 - Forbes グローバル2000に選出された企業279社

3 | © 2013 Imperva, Inc. All rights reserved.

© IMPERVA®

2,600社を超えるお客様のデータを守る

銀行 & 金融

Bank of America

Deutsche Bank



GE Money
UNITED STATES

WELLS FARGO

WESTERN UNION

VISA

政府機関 & 軍事機関



Homeland
Security



小売

ESTEE LAUDER

BEST BUY
BORDERS.

OfficeMax*

GameStop

SAFEWAY

Pier1 imports*

テクノロジ

DELL

EDS

EMC²

GoDaddy.com

hp

MOTOROLA

at&t

cingular

DIRECTV

COX

verizon
wireless

Vonage



Hertz

ESPN

LG

KAI SER PERMANENTE

AirTran
AIRWAYS

ExxonMobil

LexisNexis*

2013年セキュリティ事件簿①

アプリケーションの脆弱性を悪用した攻撃

Apache Struts2の脆弱性

© 2013 Imperva, Inc. All rights reserved.



Apache Struts2の脆弱性

- CVE-2013-2251, CVE-2013-2248 (Apache Advisory 2013/7/16公開)
 - 外部から任意のコマンド実行を許可する脆弱性
 - 任意のURLのリダイレクトを許可する脆弱性
- 攻撃(Exploit)ツールも公開され、実際の攻撃が多く観測されている
- 大手企業も被害に

CVE-2013-2251
Struts2のexploit
デモ画面

metasploitのデモ



自社のWebサイトに脆弱性があつたら。。。。

- アプリケーションを即座に修正する... But
 - ミドルウェアやCMS等、自社開発のアプリケーションでなければパッチが公開されるまで修正できない
- リリースされた公式パッチを当てる... But
 - サービス停止を伴う可能性が
 - テスト期間が必要
- ネットワーク経路で攻撃を検出・ブロックする 既向かせません
すがない、
 - 即時対処が可能な仮想的なパッチ
 - Network IPSやWeb Application Firewallによって防御

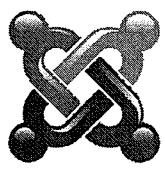
7

© 2013 Imperva, Inc. All rights reserved.

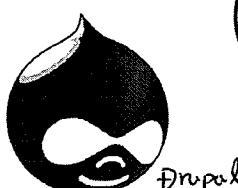


最近はCMSも標的になりやすいので要注意

- CMS = Contents Management System
- WordPress, Joomla, Drupal, MovableType等
- 多くの企業サイト、商用サイト、Hosting Serviceで採用
- 機能を拡張する豊富なプラグイン・エクステンション
 - 80%の脆弱性は3rd Party製のコードに存在¹⁾
- Application(機能)の構成が同じなので、攻撃を受けやすい



Joomla



Drupal



WordPress



Movable Type

1) Source: https://www.bsi.bund.de/DE/Publikationen/Studien/CMS/Studie_CMS.html
BSI is Germany's federal office for information security

8

© 2013 Imperva, Inc. All rights reserved.

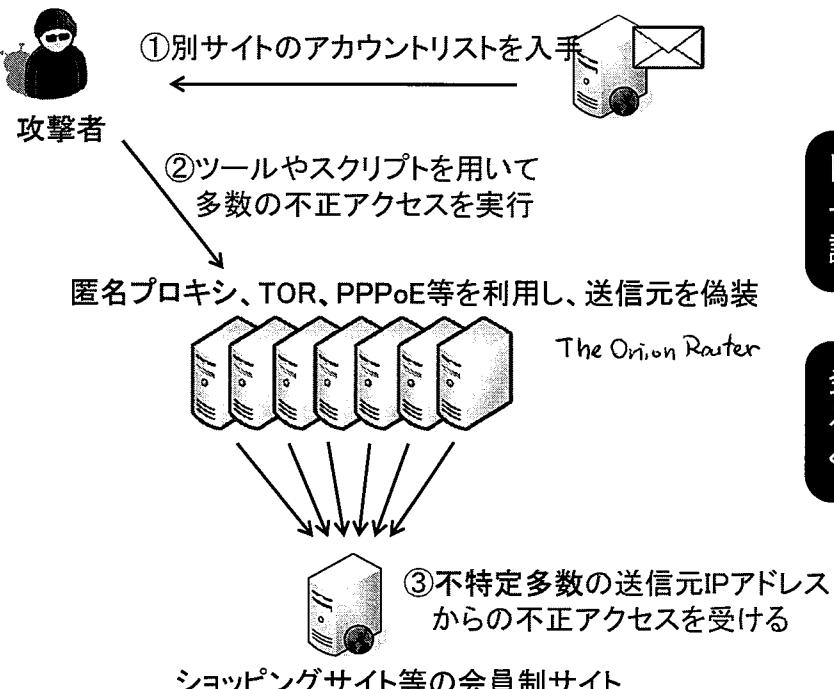


2013年セキュリティ事件簿② ログインブルートフォース攻撃 アカウントリスト型攻撃

© 2013 Imperva, Inc. All rights reserved.

© IMPERVA®

アカウントリスト型攻撃の仕組み



アカウントリスト型攻撃の特徴

- 従来型のブルートフォース攻撃と比較し成功率が高い
- 一般の利用者と攻撃者のアクセスが区別出来ない
- Torなどの匿名サービスを利用し、発信元を頻繁に変更する
- 攻撃の防御には「相関ルール」と「レビューション」の活用が効果的

既存のブルートフォース(総当たり)攻撃との差異

	①総当たり型	②辞書型	③アカウントリスト型
ログイン試行例	ID=test, PW=a ID=test, PW=b ID=test, PW=c ... ID=test, PW=z ID=test, PW=ab	ID=test, PW=test ID=test, PW=123456 ID=test, PW=abcefg ... ID=admin, PW=test ID=admin, PW=123456 ...	ID=suzuki, PW=taro ID=yamada, PW=hanako ID=sato, PW=abc123# ... ID=naka, PW=987IPA ID=mickey, PW=donald ...
IDあたりの試行回数	非常に多い	多い (数百～数千)	非常に少ない (1～数個)

SecureSphere WAFによるアカウントリスト型攻撃対策①

Webカスタムポリシーによって攻撃を防御する

ポリシーの設定: 認証結果は [成功] 詳細な説明

アクション: ブロック 重大度: 中

フォロー アクション: Long IP Block 有効:

アラート名: Custom Violation

一致条件

HTTP Request

Operation:	Match All
Part:	+ Name
URI:	Includes /login-auth.php
Parameter:	username Matches Regular Express ^*

件数

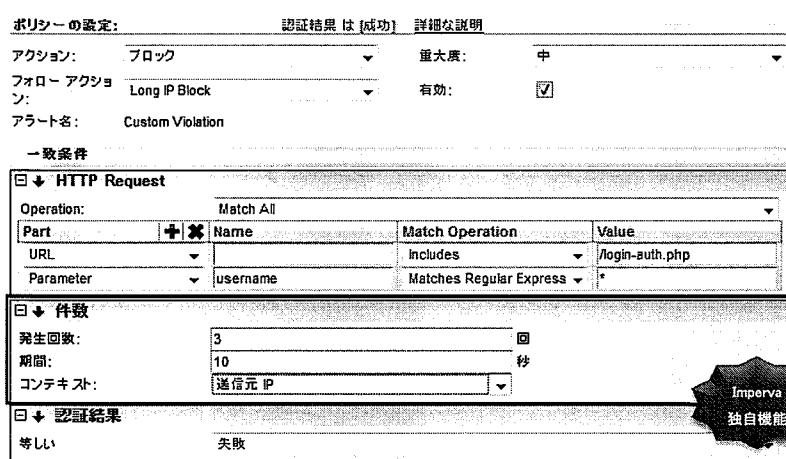
発生回数: 3 回

期間: 10 秒

コンテキスト: 送信元 IP

認証結果

等しい 失敗



■ 攻撃検知条件

- ・ ログイン認証の失敗を判定
- ・ ログインアクションURLの指定
- ・ ユーザ名入力パラメータの指定
- ・ 上の条件にマッチするアクセスのカウントアップ
- ・ 10秒間に3回同じ送信元IPから上の条件にマッチするアクセスを検知

- ・ 攻撃検知した送信元IPアドレスを一定時間ブロック

SecureSphere WAFによるアカウントリスト型攻撃対策②

THREATRADAR



- インターネット上の悪意あるIPや匿名プロキシサーバのIPを捕捉、ThreatRadarサーバが危険なIPアドレス情報をWAFへ自動送信することで、様々な脅威を迅速にブロック！

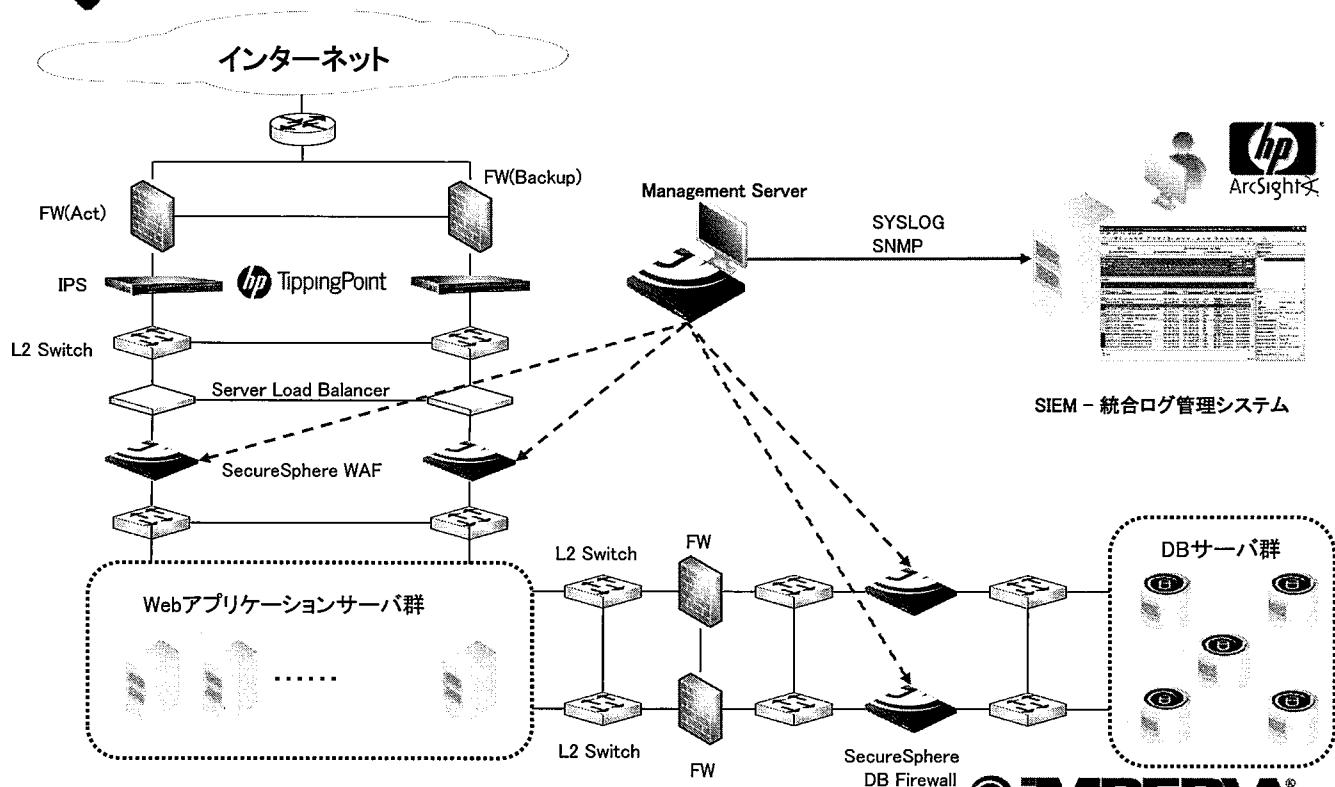


13

© 2013 Imperva, Inc. All rights reserved.

© IMPERVA®

IPS/WAF/SIEMによる統合ネットワークセキュリティソリューション



14

© 2013 Imperva, Inc. All rights reserved.

© IMPERVA®

アプリケーション攻撃からデータを守る

～ SecureSphere Web Application Firewall のご紹介～



Web Apps

82% of Web applications have vulnerabilities¹

75% of all Internet attacks target applications²

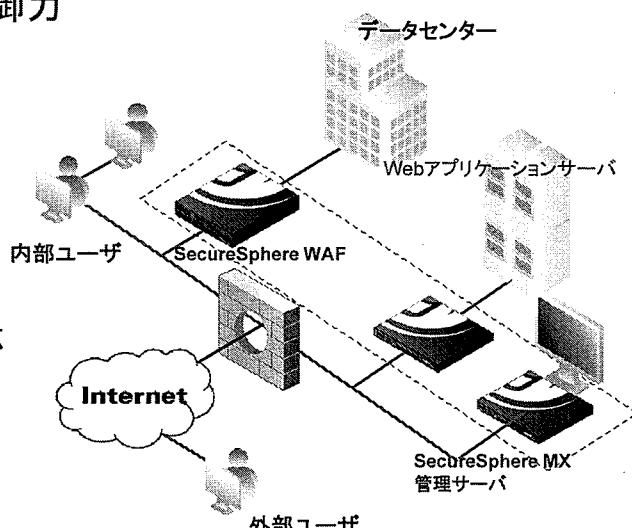
¹ White Hat - statistic for initial examination; ² Gartner Research

© 2013 Imperva, Inc. All rights reserved.



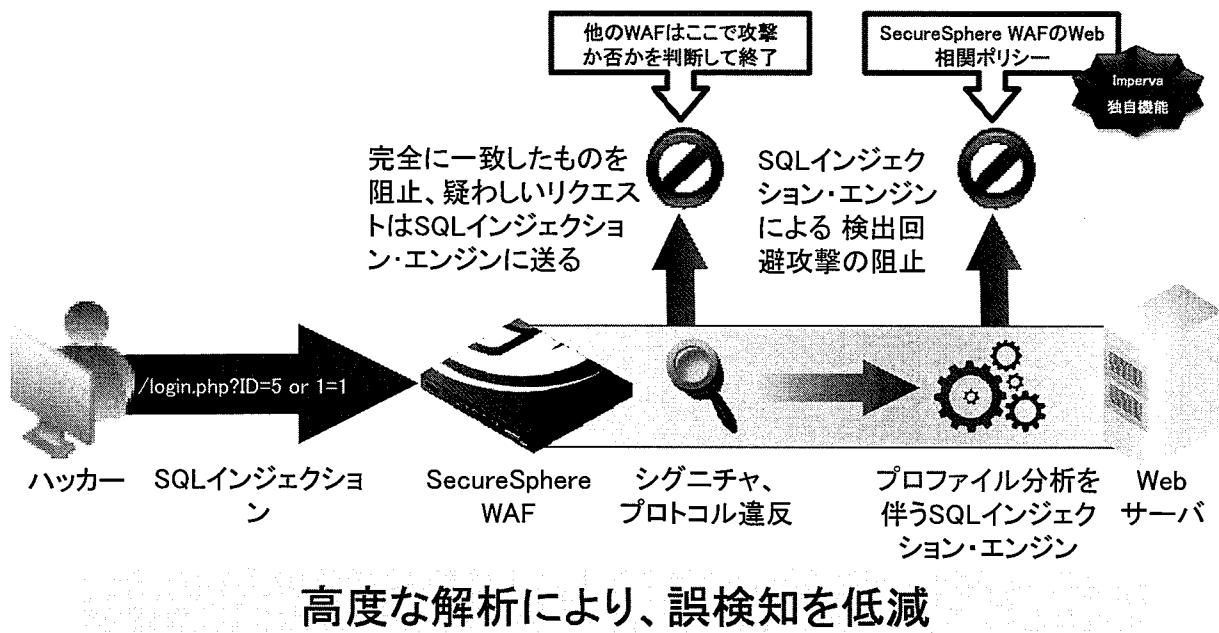
SecureSphere WAFの特長

- 専業ベンダーならではの高い攻撃防御力
 - ・ 独自の相関攻撃検証エンジン
 - ・ ADCシグニチャ更新サービス
 - ・ レピュテーション防御
- 導入・運用のしやすさ
 - ・ 透過モードなど様々な導入形態に対応
 - ・ アプリケーション・NWの変更不要
 - ・ ホワイトリスト自動学習
- 豊富な導入実績
 - ・ WAF国内シェア1位



独自の検出アルゴリズムによる高い攻撃防御率

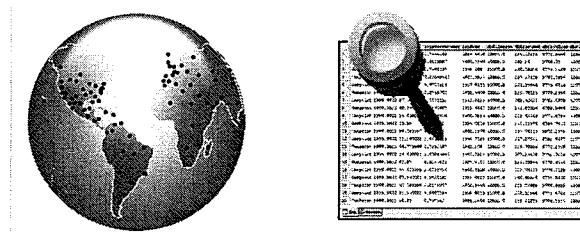
- 2段階のパケット解析によりSQLインジェクション、XSSで正確に阻止！



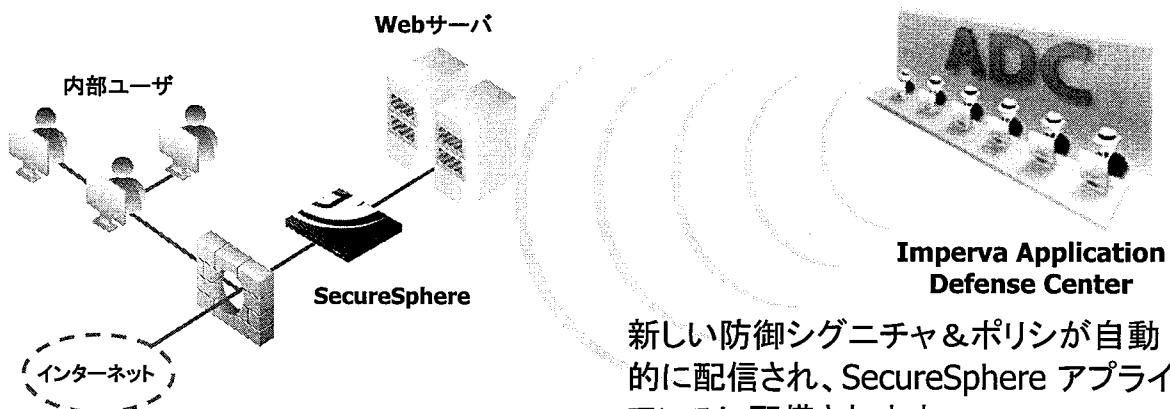
高度な解析により、誤検知を低減

SecureSphereテクノロジー： シグニチャー更新サービス – Imperva ADC

セキュリティ専門化
チームが最新の脅
威を調査・情報収集



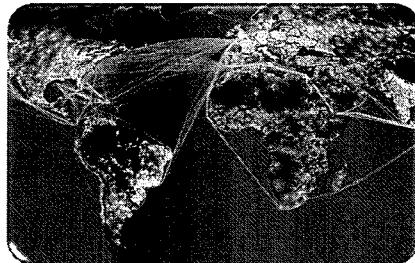
ADC が実トラヒックの解析
やペネトレーションテストを
実施し、脆弱性を調査



新しい防御シグニチャ&ポリシが自動
的に配信され、SecureSphere アプライ
アンスに配備されます

SecureSphereテクノロジー: ThreatRadar: レピュテーション防御

THREATRADAR



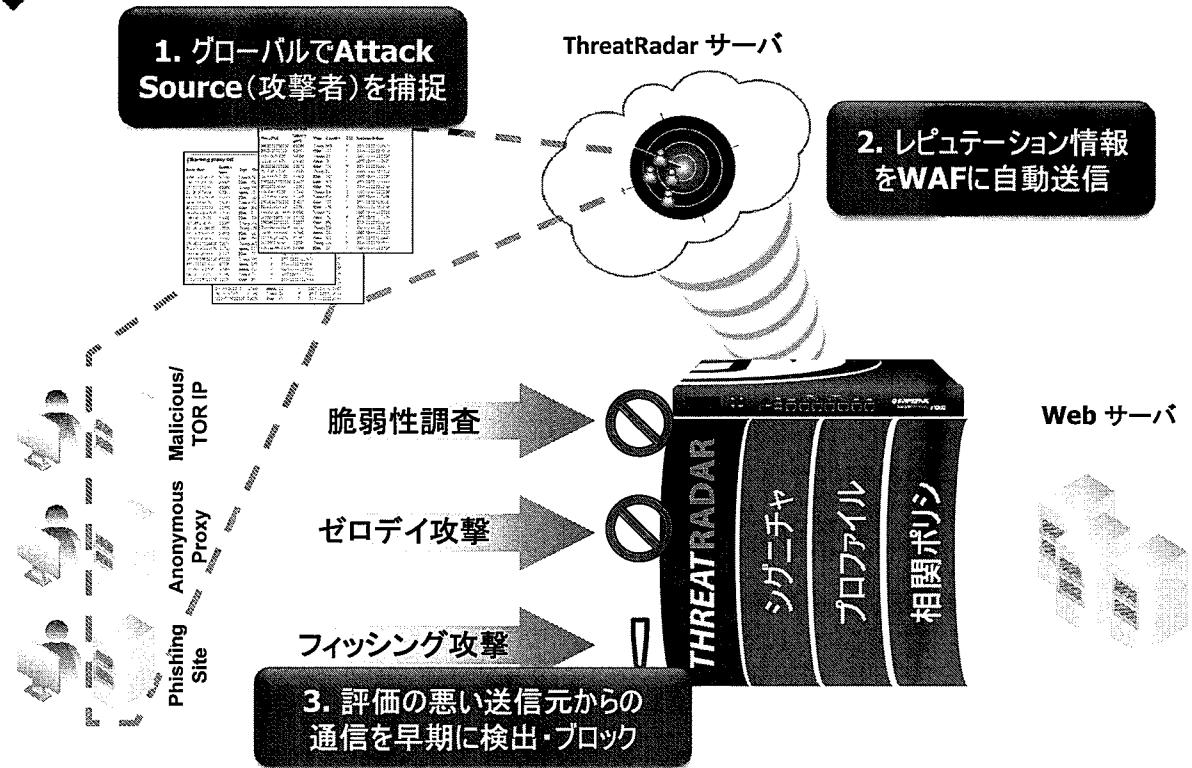
- 大規模かつ自動化された攻撃の防御
- 常に最新の状態に更新される防御メカニズム
- ボットサイトからの攻撃、匿名プロキシを経由した発信元隠蔽攻撃などからの防御

19

© 2013 Imperva, Inc. All rights reserved.

© IMPERVA®

レピュテーション防御 - ThreatRadar



20

© 2013 Imperva, Inc. All rights reserved.

© IMPERVA®

アプリケーションに応じた柔軟な相関ポリシーの作成

ポリシー名: DOS攻撃

一致条件 通用先 詳細 保存

ポリシーの設定: URL プレフィックス は [/veda1/login.asp]
Occurrence definition is: Occurred more than 5 times within 10 seconds in the context of a single 送信元 IP 詳細な説明

アクション: ブロック 重大度: 中
フォロー アクション: 有効:
アラート名: カスタム違反

一致条件

特定の URL

操作: 1つ以上
値: [/veda1/login.asp]

件数
発生回数: 5
期間: 10
コンテキスト: 送信元 IP

一定時間内のアクセス回数

ログイン済みセッション
等しい いいえ

ログイン済みセッションでない

使用可能な一致条件

- Accept Languages (ヘッダー)
- Data Set Attribute Lookup
- Lookup Data Set Search
- Referrer Hostname (ヘッダー)
- Request Content Type (ヘッダー)
- User-Agent (ヘッダー)
- Web ページレスポンス サイズ
- Web ページ応答時間
- シグニチャ
- セッション
- センシティブ ティクショナリの検索

- Available Match Criteria
- Accept Languages (Headers)
 - Authenticated Session
 - Authentication Result
 - Authenticated User URL
 - Cookie
 - Enrichment Data
 - File Types
 - Generic Dictionary Search
 - Headers
 - Host Names
 - Lookup Data Set Search
 - Methods
 - Occurrence
 - Parameters
 - Profiled Referer Host
 - Protocols
 - Proxy IP Addresses
 - Referrer Hostname (Headers)
 - Referrer URL (Headers)
 - Request Content Type (Headers)
 - Request Cookie Names
 - Request Cookies
 - Request Headers
 - Response Code
 - Response Headers
 - Sensitive Dictionary Search
 - Session
 - Signatures
 - Source IP Addresses
 - Time of Day
 - URL Prefix
 - User
 - User-Agent (Headers)
 - Violations
 - Web Page Response Size
 - Web Page Response Time

20+の一致条件を組み合わせて定義

21 | © 2013 Imperva, Inc. All rights reserved.



SecureSphereテクノロジー: 多層防御アーキテクチャ

プロトコル違反

HTTPプロトコル違反

攻撃シグニチャ

既知の攻撃を特定

- 6,500+ のシグニチャ(定期更新)

アプリケーションプロファイル

アプリケーション利用のアノマリを検知

データ漏洩防御

機密データの外部流出を防止

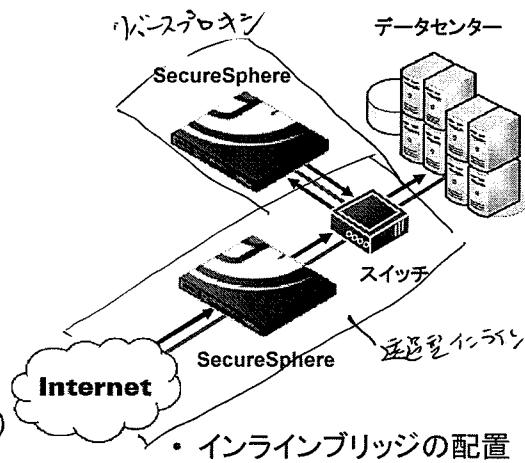
ThreatRadar

攻撃前に発信元を評価

環境に応じて設置タイプを選択できます

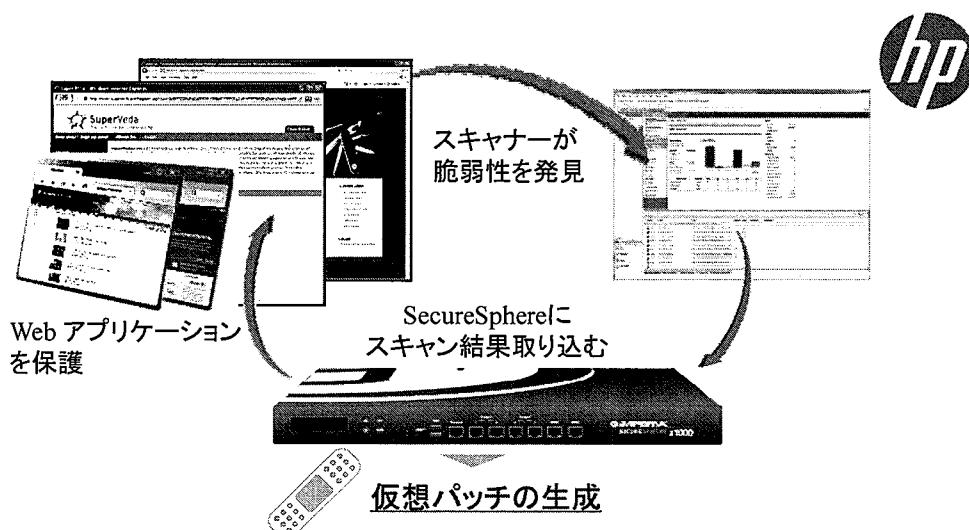
Imperva
独自機能

- 透過型インラインブリッジ
 - 既存環境に最適
 - 高スループットと低遅延
 - フェイルオーバンインターフェース
- リバースプロキシ
 - コンテンツ修正
 - URL書き換え、クッキー署名
 - SSL終端
- ノン-インライン配置(Snifferモード)
 - 評価・監視用
 - ゼロネットワーク遅延



Web脆弱性スキャナーとWAFの連携

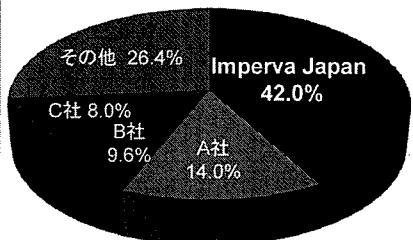
- スキャン結果を基にしたSecureSphereのポリシーを適用
- 緊急修正および検証サイクルを削減



日本国内WAF市場 3年連続1位

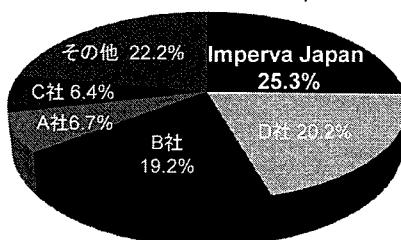
2010年、2011年、2012年 3年連続市場シェア *Imperva Japan 1位*

株富士キメラ総研



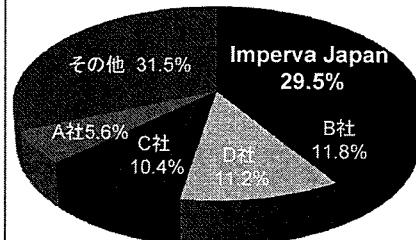
「2013 ネットワークセキュリティビジネス
調査総覧:Webアプリケーション
ファイアウォール 2012年度(実績)」

ミック経済研究所



「情報セキュリティソリューション市場の
現状と将来展望 2013:2012年度」

株アイ・ティ・アール



「ITR Market View:セキュリティ市場
2013:WAF市場2012年度」

25 | © 2013 Imperva, Inc. All rights reserved.

※全て出荷金額ベース

IMPERVA®

データ侵害の脅威は「外部」だけでなく、 実は「内部」にも存在します

- 個人情報漏洩件数トップ10の内8件が内部漏洩
- 個人情報漏洩事故の原因の8割以上が内部漏洩

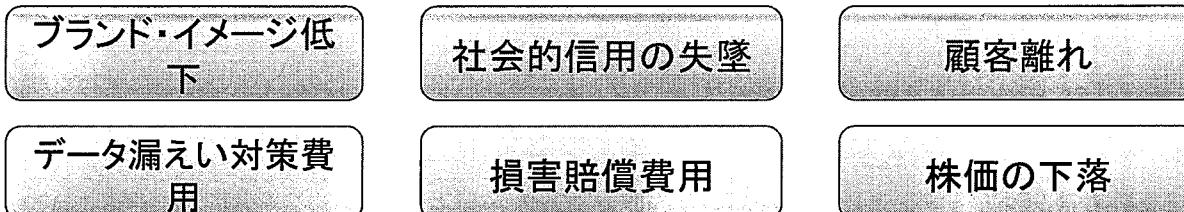
(日本ネットワークセキュリティ協会 2011年情報セキュリティインシデントに関する調査報告書 ~個人情報漏えい編~より)

内部情報漏えい被害の現状

□ 近年の主な内部情報漏えい被害

発生時期	被害内容
2013年2月	スカパーJSATのサーバやPC等17台がウイルスへ感染、取引先情報や技術情報が流出した可能性
2012年11月	ジブラルタ生命保険を退職した社員や代理店の保険販売員計19人の不正行為により顧客情報が流出
2012年7月	NTTドコモの携帯電話顧客情報(約3万件)が派遣社員の不正行為により流出
2011年11月	総務省の職員用PC23台がウイルス感染、外部へ情報が流出
2010年10月	ルーク19が運営するオンライン・サービスの会員個人情報(約47万件)が派遣社員の不正行為により流出
2009年1月	三菱UFJ証券会社の顧客情報(約5万件)と企業情報(約122万件)が正社員の不正行為により流出(持ち出された顧客情報は約148万件)

□ 内部情報漏えい被害により、企業が受ける損失



27 | © 2013 Imperva, Inc. All rights reserved.

© IMPERVA®

Data Breach .. データ侵害

内部情報漏えい被害の現状

□ 内部情報漏えい被害の傾向

□ 内部情報漏えいの犯行者

- 元社員
- 元派遣やパートナー企業の元社員
- 遠隔操作系の不正プログラムに感染した社員のPC

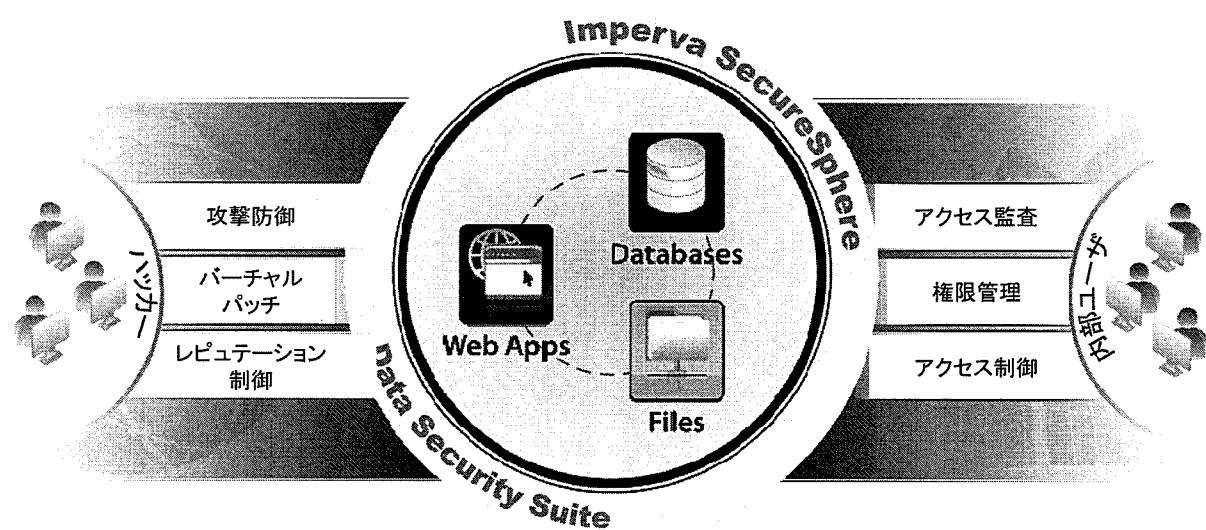
□ 2次被害の確率(2次被害の例:漏えいした個人情報等を悪用した詐欺)*

- | | |
|-------------------------|-------|
| □ 元社員等による情報漏えいの場合 | 52.4% |
| □ 不正プログラムによる情報漏えいの場合 | 50.0% |
| □ Winny/Shareへの情報漏えいの場合 | 5.0% |
| □ 紛失・盗難による情報漏えいの場合 | 4.1% |

元社員等による内部情報漏えいは情報セキュリティ以外に企業の内情や全社員のモラル等を疑わせてしまうため、外部からの不正アクセスよりも、社会や顧客へ与えるインパクトは非常に大きい！

* 出展:独立行政法人 情報処理推進機構 情報漏えいインシデント対応方策に関する調査報告書

外部・内部の脅威からデータを保護する



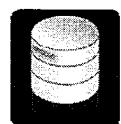
29

© 2013 Imperva, Inc. All rights reserved.

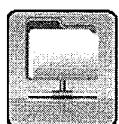
© IMPERVA®

データベース・ファイルセキュリティ

～アクセスモニタリング・監査・権限管理～



Databases



Files

The average organizational cost of a data breach increased to \$7.2 million and cost companies an average of \$214 per compromised record.

(Ponemon Institute, 2010 Annual Study Cost of a Data Breach)

© 2013 Imperva, Inc. All rights reserved.

© IMPERVA®

データベース・ファイルセキュリティのライフサイクル

診断・分類



- ✓ データベース自身に脆弱性がないか？
- ✓ ユーザ権限の設定が適切か？
- ✓ 保護すべき重要な情報がどこに格納されているか？

記録・監査



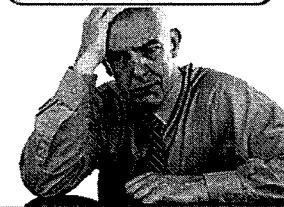
- ✓ アクセス全件記録
- ✓ 特権ユーザ監視
- ✓ アクセス傾向把握
- ✓ 異常操作の検出

コントロール



- ✓ ユーザID制御
- ✓ テーブル・フォルダ毎のフィルタリング
- ✓ 特権操作の制御
- ✓ 時間帯による制御

分析・報告



- ✓ ステータス管理
- ✓ 相関分析レポート
- ✓ 即時アラート
- ✓ ポリシ管理

← 最近のトレンド

データセキュリティにおけるアクセス監査とセキュリティ

データへのアクセス

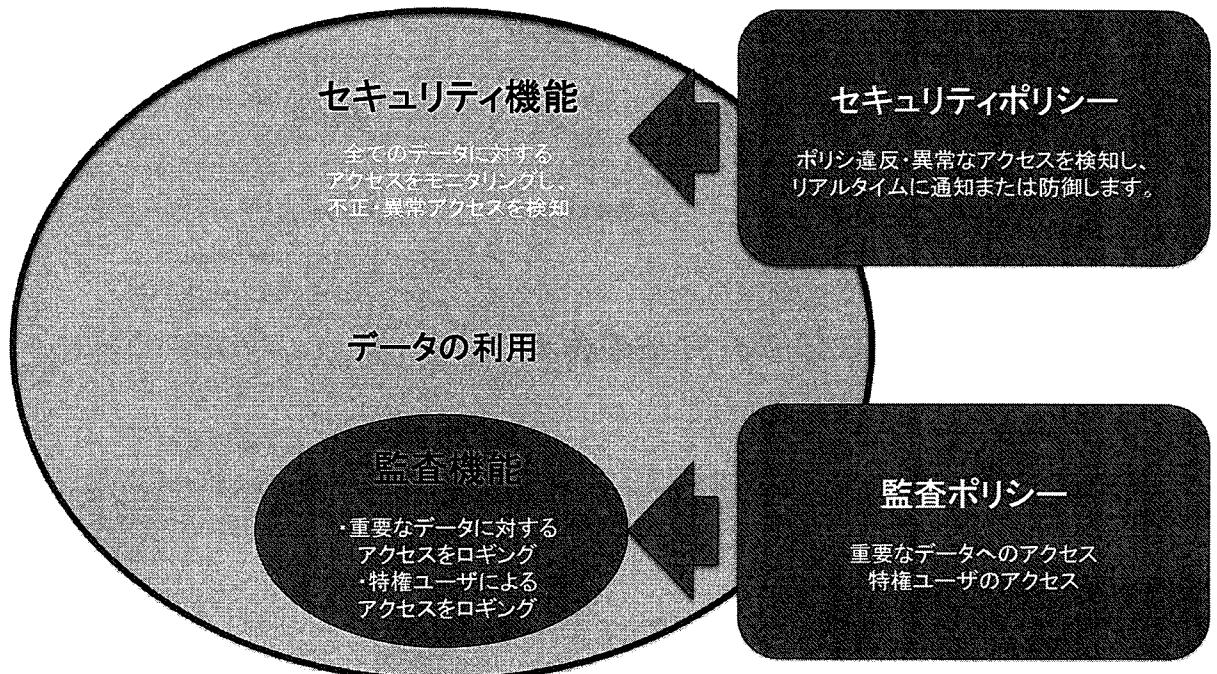
セキュリティ機能

データに対するアクセスをモニタリングし、不正・異常アクセスを検知

監査機能

データに対するアクセスや特権ユーザによるアクセスをロギング

監査とセキュリティの概念

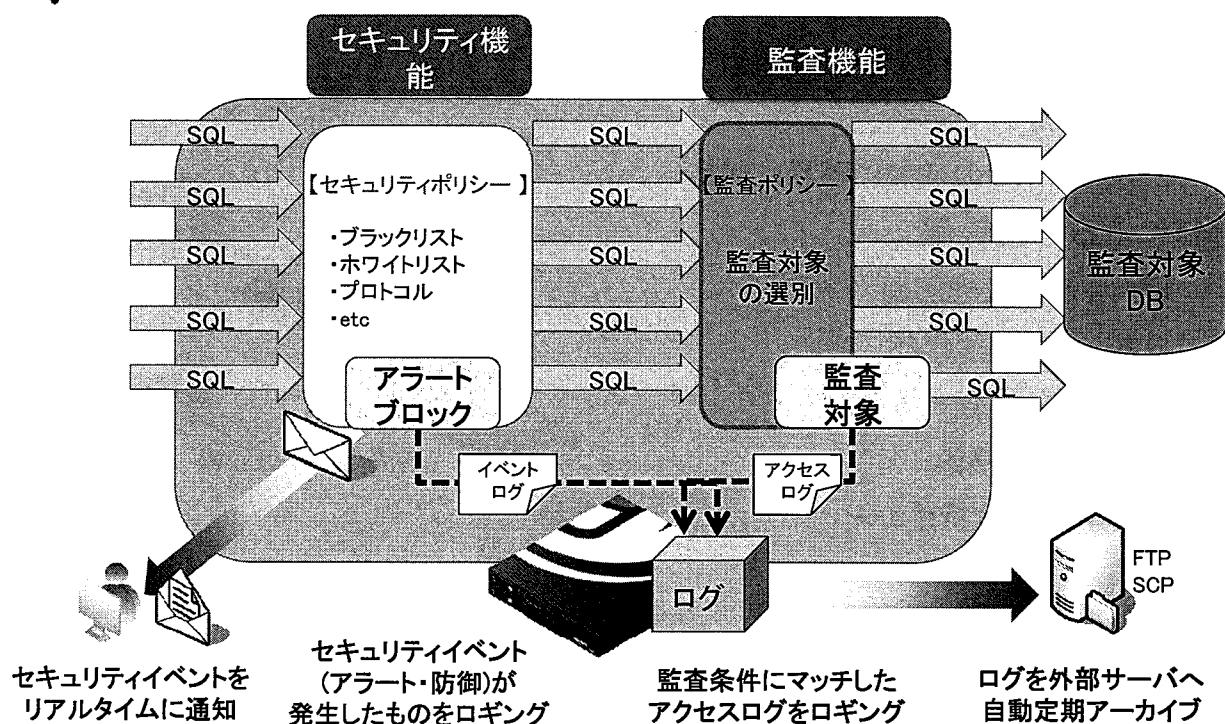


33 | © 2013 Imperva, Inc. All rights reserved.

他社製品では監査対象データに限定した
モニタリング(セキュリティ機能)しか行えないものが存在する

Imperva®

データベースアクセスにおけるセキュリティ・監査の仕組み



Database監査とフォレンジック

アクセスサマリ(項目ごとの発生件数)の表示

SecureSphere 特長

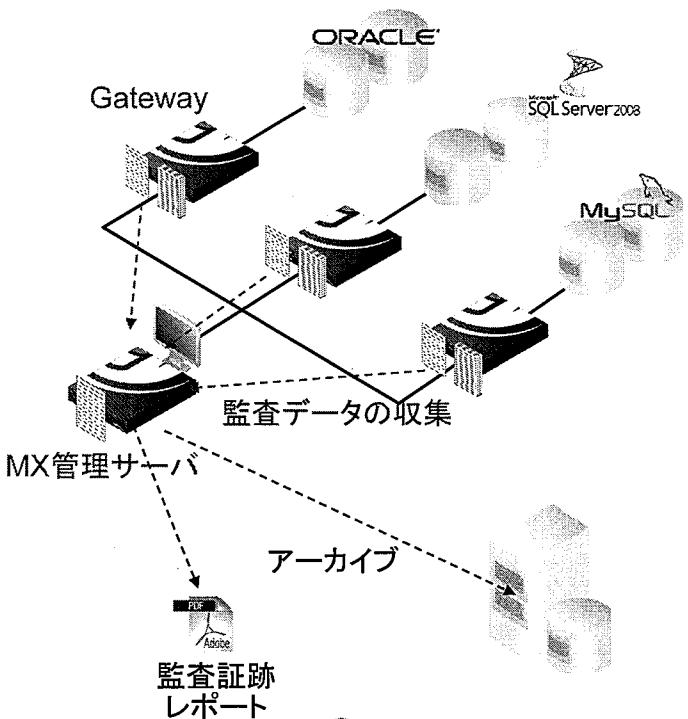
- ① 全件記録(20万TPS)
 - ② 特権ID等の多角的な分析
 - ③ 全レスポンスの記録
 - ④ ローカルトラヒックに対応

35 | © 2013 Imperva, Inc. All rights reserved.

 IMPERVA®

分散監査アーキテクチャ

- 各Gatewayが個々にデータ記録
 - ハイパフォーマンス
 - トラヒック/DBの増加に容易に対応
 - MXによる一元管理
 - 統一された管理画面
 - レポートの一括作成
 - リアルタイム監査・分析
 - インデックス検索
 - 多彩な監査分析ビュー



いかなる環境にも
スケーラブルに対応

取得したログを様々な角度から分析

SecureSphere - DB Audit Data - Mozilla Firefox

SecureSphere - DB Audit Data

IMPERVA SECURESPHERE Discovery & Classification | Setup | Profile | Risk Management | Policies | Audit | Reports | Monitor | Threat Radar | Main | Admin | Preferences | Tasks | Log out | Help

DB Audit Data | File Audit Data | Audit Management Statistics | Archive Management

Administrator Save As

Scope: **L1** [L1] [L2] [L3] [L4] [L5] [L6] Audit Rate - Application_Users (RPT)

Policy: Default Audit Rule (42,248 Events)

Time Frame: 03/14/2011, 09:00 - 06/14/2011, 09:59 (92 Days, 8 hrs) **Update**

Reported Period: 1. Warning

Filter: **Empty** Select Field Select Value

Application Users - Number of Databases
Additional Filter: Application User is not empty

Hits by Application Users (Broken by Database)
Additional Filter: Application User is not empty

Hits Sum

Database	Hits Sum
Veda2010_DB	146
ysakurai_2	40
lact	15

Additional Filter: Application User is not empty | Showing records 1-3 out of 3 available |

Application User	Service	# Users	# Databases	Hits Sum
lact	Veda2010_DB	1	1	146
ysakurai_2	Veda2010_DB	1	2	40
lact	Veda2010_DB	1	2	15

一日でできるかな

Main > Audit > DB Audit Data

User admin | Version: 8.5.0.2 Enterprise Edition | © 2011 Imperva Inc.

37

© 2013 Imperva, Inc. All rights reserved.

©IMPERVA®

特権操作を細かく制限

- ・作業に必要な最小の権限を許可する
 - ・管理用特権コマンド
 - ・アクセス時間帯

The screenshot shows the IMPERA SECURESPHERE web application. The top navigation bar includes links for Main, Admin, Preferences, and Help. Below the main header, there's a sub-navigation bar with tabs for Discovery & Classification, Setup, Profile, Risk Management, Policies, Audit, Reports, and Monitoring.

The main content area displays a list of users under the 'Users' tab. The list includes columns for User Name, Group, # Queries, and # Query Groups. A 'Details' button is available for each user entry. On the left, a sidebar titled 'Filter' lists 'Users & Groups' and 'Sensitive'. The right side of the screen shows a detailed configuration panel for 'operator' roles, including sections for 'Details: operator', 'Restrictions', 'Privileged Operations', and 'Learning Preferences'. It also features a 'Black list table groups' section and a 'Time Restrictions' grid for specific days of the week.

平日9時～17時のみアクセス可

リアルタイムモニタリング・ブロック

- プロファイル違反
- カスタムポリシー

Policy name: データベース大量データ抽出

Hatch Criteria	Apply To	Advanced
Action: Block	Severity: High	
Followed Action: Report	Enabled: <input checked="" type="checkbox"/>	
Alert Name: Custom Violation		
Match Criteria		
<input checked="" type="checkbox"/> Database User Names <input checked="" type="checkbox"/> Match Events with Unknown User (Hashed or Connected) Operations: Exclude all Selected: System		
<input checked="" type="checkbox"/> Names: Admin Test administrator User Defined:		
<input checked="" type="checkbox"/> Destination Tables Operations: At least one Selected: user_list		
<input checked="" type="checkbox"/> Tables: Search Stats Users User Defined:		
<input checked="" type="checkbox"/> Query Response Size Operations: Greater than Value: 1000 レコードの抽出数を制限		

Alert 15496: Unauthorized Source Application sqlplus@superviseda-app (tns v1-v3) by a

Actions: None
Policy: SQL_Profile Policy

Event 1592526504162882499: Unauthorized Source Application !| o+|

Save

Profile Policy

Unauthorized Source Application sqlplus@superviseda-app (tns v1-v3) by admin 12.168.1.210 admin, Source Application: sqlplus@superviseda-app (tns v1-v3)

Gateway GW85-1

Service Application Oracle Default Oracle Application

Source of Activity User DB Application OS User OS Host

Remote sqlplus@superviseda-app admin (tns v1-v3) root superviseda-app

Response Size 0 Records 通常とは異なる
クライアントからの接続

tables

39 | © 2013 Imperva, Inc. All rights reserved.



アクセス監査証跡レポート PCI DSS等のコンプライアンス要件への対応

- クレジットカード情報や個人情報など重要な情報を格納するテーブルへのアクセスを全て記録し、必要な監査証跡を保存します。

10.3.3 日付と時刻

10.3.1 ユーザ識別

10.3.2 イベント識別

10.3.5 イベント発生元

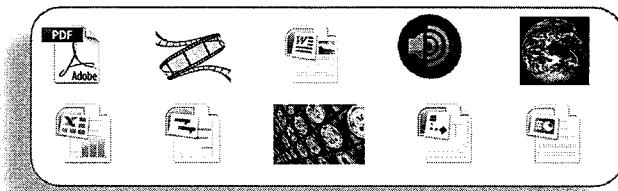
10.3.6 影響を受けるデータ

Date/Time	Server Group	Server IP	Source IP	Web Client IP	App User	DB User	DB/Schema	Raw Query	Source URL
10/02/2007 07:21:41	VEDA-DB	192.168.0.14	192.168.0.13	192.168.0.83	bugsb	veda_app	(veda_db,N/A)(veda_db,N/A)	SELECT * FROM Orders WHERE Orders.OrderID = 65	/superviseda/orderdetails.asp
10/03/2007 12:46:25	VEDA-DB	192.168.0.14	192.168.0.13	192.168.0.83	bugsb	veda_app	(veda_db,N/A)(veda_db,N/A)	SELECT * FROM Orders WHERE Orders.OrderID = 67	/superviseda/orderdetails.asp
10/03/2007 12:46:33	VEDA-DB	192.168.0.14	192.168.0.13	192.168.0.83	bugsb	veda_app	(veda_db,N/A)(veda_db,N/A)	SELECT * FROM Orders WHERE Orders.OrderID = 61	/superviseda/orderdetails.asp
10/03/2007 12:46:29	VEDA-DB	192.168.0.14	192.168.0.13	192.168.0.83	bugsb	veda_app	(veda_db,N/A)(veda_db,N/A)	SELECT * FROM Orders WHERE Orders.OrderID = 104	/superviseda/orderdetails.asp
10/03/2007 12:46:31	VEDA-DB	192.168.0.14	192.168.0.13	192.168.0.83	bugsb	veda_app	(veda_db,N/A)(veda_db,N/A)	SELECT * FROM Orders WHERE Orders.OrderID = 77	/superviseda/orderdetails.asp
10/03/2007 12:46:27	VEDA-DB	192.168.0.14	192.168.0.13	192.168.0.83	bugsb	veda_app	(veda_db,N/A)(veda_db,N/A)	SELECT * FROM Orders WHERE Orders.OrderID = 77	/superviseda/orderdetails.asp



非構造化データ(ファイル)の保護

非構造化データ
Office文書・PDF・動画など



ファイルサーバ・NASには、ビジネス文書やソースコードなどの知的財産、経理事務用のスプレッドシートなどが保管、共有されています

- 分析 重要データへのアクセス権限を分析
- 特定 過剰に付与されている権限を特定
- 監視 ビジネスピリシーに違反するアクセスを監視またはブロック

ファイルアクセス監査ログ

IMPERVA SPHERE™ Discovery & Classification, Search & Find, Real-time access, Policy, Events, Indexing, ThreatRecov										
File Access Audit Log - User: shingen Date: June 14, 2011 8:30:00 AM										
Search: shingen, 2011年度 営業計画.xlsx, Read, Permissions Change, Modify, Delete, Read, Read, Modify, Read, Read, Modify										
誰が			どのファイル			どこのフォルダ			いつ	
User Name	User Department	Operation	File	Folder	Classification	Hits Sum	Destination IP	Time Group - 30 Minutes		
shingen	人事部	Read	店舗リスト.xlsx	WW2K3SV\営業資料	営業部	3	192.168.1.203	June 14, 2011 8:30:00 AM		
leyasu	技術部	Read	2011年度 営業計画.xlsx	WW2K3SV\共有	営業部	2	192.168.1.203	June 14, 2011 8:30:00 AM		
shingen	人事部	Permissions Change	店舗リスト.xlsx	WW2K3SV\営業資料	営業部	2	192.168.1.203	June 14, 2011 8:30:00 AM		
leyasu	技術部	Modify	店舗リスト.xlsx	WW2K3SV\営業資料	営業部	1	192.168.1.203	June 14, 2011 8:30:00 AM		
leyasu	技術部	Modify	2011年度 営業計画.xlsx	WW2K3SV\営業資料	営業部	1	192.168.1.203	June 14, 2011 8:30:00 AM		
kenshin	技術部	Read	店舗リスト.xlsx	WW2K3SV\営業資料	営業部	1	192.168.1.203	June 14, 2011 8:30:00 AM		
shingen	人事部	Modify	店舗リスト.xlsx	WW2K3SV\営業資料	営業部	1	192.168.1.203	June 14, 2011 8:30:00 AM		
leyasu	技術部	Delete	2011年度 営業計画.xlsx	WW2K3SV\営業資料	営業部	1	192.168.1.203	June 14, 2011 8:30:00 AM		
leyasu	技術部	Read	2011年度 営業計画.xlsx	WW2K3SV\営業資料	営業部	1	192.168.1.203	June 14, 2011 8:30:00 AM		
leyasu	技術部	Read	店舗リスト.xlsx	WW2K3SV\営業資料	営業部	1	192.168.1.203	June 14, 2011 8:30:00 AM		
leyasu	技術部	Modify	2011年度 営業計画.xlsx	WW2K3SV\共有	営業部	1	192.168.1.203	June 14, 2011 8:30:00 AM		

全てのファイルアクセスの可視化

- ・フォルダー及びファイル
- ・新規作成・読み込み・書き込み・修正・削除・権限変更

インストール不要

- ・ファイルシステムのパフォーマンスに影響を与えません
- ・アプリケーション・サーバ・クライアントの設定変更不要

アクセス監査ログの解析 – フォレンジック

File Access Breakdown By Data Type

経理部門のファイルデータを対象

最もアクセスの多いユーザは?

なぜ研究開発部の職員が財務データにアクセス?

User Name	Server Group	User Department	Hits Sum
uyau	2k3sv	経理部	10
yoshihiro	2k3sv	経理部	7
hideyoshi	2k3sv	研究開発部	6
nobunaga	2k3sv	経理部	5
Yoshimoto	2k3sv	経理部	4
Yashiro	2k3sv	経理部	3

Event Date and Time Event ID User Name Operation File Folder

Event Date and Time	Event ID	User Name	Operation	File	Folder
June 16, 2011 10:40:54 AM	8372121093724440550	hideyoshi	Read	平成22年度下半期収支報告書.docx	\WW2K3SV\経理部
June 16, 2011 10:41:05 AM	8372121093724440581	hideyoshi	Read	平成22年度下半期収支報告書.docx	\WW2K3SV\経理部
June 16, 2011 10:41:06 AM	8372121093724440582	hideyoshi	Modify	平成22年度下半期収支報告書.docx	\WW2K3SV\経理部
June 16, 2011 10:41:10 AM	8372121093724440600	hideyoshi	Read	平成23年度収支報告書.docx	\WW2K3SV\経理部
June 16, 2011 10:41:10 AM	8372121093724440601	hideyoshi	Modify	平成23年度収支報告書.docx	\WW2K3SV\経理部

43 | © 2013 Imperva, Inc. All rights reserved.

© IMPERVA®

監査証跡レポート

◎IMPERVA® SECURE SPHERE™

Event Date and Time	User Name	Operation	Folder	File
May 21, 2011 9:33:33 PM	kenshin	Read	\WW2K3SV\営業資料	顧客情報.txt
May 21, 2011 9:33:36 PM	kenshin	Modify		
May 21, 2011 9:33:36 PM	kenshin	Read		
May 21, 2011 9:41:50 PM	kenshin	Read		
May 21, 2011 9:41:53 PM	kenshin	Modify		
May 21, 2011 9:42:19 PM	kenshin	Create		
May 21, 2011 9:42:19 PM	kenshin	Modify		

豊富なレポートテンプレート

- マネジメント向けのグラフ付きレポート
- 担当者向けの詳細レポート

Departments with Access to Largest Number of Files

柔軟にカスタマイズ可能

- PDF or CSV
- スケジュール(月次・週次など)

レポート: 未承認の経理データアクセス

一般的な詳細	データ範囲	表形式	データ分析ビュー	スケジューリング	結果	許可
--------	-------	-----	----------	----------	----	----

SecureSphere共通プラットフォーム

X シリーズ・M シリーズ アプライアンス 仮想アプライアンス

© 2013 Imperva, Inc. All rights reserved.



アプライアンスマルチ一覧 – X series

外観					
モデル名	X1010	X2010	X2500 (FTL)	X4500 (FTL)	X6500 (FTL)
選択可能なライセンス	WAF	WAF	WAF/DB/File	WAF/DB/File	WAF/DB
スループット(WAF,DB)	100 Mbps	500 Mbps	500 Mbps	1 Gbps	2 Gbps
スループット(File)	利用不可	利用不可	2 Gbps	4 Gbps	利用不可
フォームファクタ	1U	1U	2U	2U	2U
監視セグメント数	2 (bridge)	2 (bridge)	2 (bridge) 4に増設可	2 (bridge) 4に増設可	4 (bridge)
10Gbps	なし	なし	オプション	オプション	オプション
HDD	1 TB	1 TB	2 x 500GB Hot Swap	2 x 1TB Hot Swap	2 x 1TB Hot-swap
RAM	8 GB	8 GB	4 GB	8 GB	8 GB
SSL Accelerator	追加可能	追加可能	追加可能 ²	追加可能 ²	標準搭載
HBA/LOM/HSM ¹	なし	なし	追加可能 ²	追加可能 ²	追加可能 ²

1) ハードウェア拡張オプション

HBA = Host bus adaptor(ファイバチャネルアダプタ)

LOM = Light on management(リモート制御用プロセッサ)

HSM = Hardware Security Module(暗号鍵管理プロセッサ)

2) HSM と SSL Accelerator は同時使用はできません

専用管理サーバアプライアンス - M series

外観



FTLモデルはHDD(RAID1)、PSU
(電源)、冷却ファンが2重化された、
耐障害性モデルです

モデル名	M110	M150 (FTL)
------	------	------------

フォームファクタ	1U	2U
----------	----	----

RAM	8 GB	4 GB
-----	------	------

管理ポート数	2 (Copper)	2 (Copper)
--------	------------	------------

HDD容量	500 GB	2 x 300GB
-------	--------	-----------

HBA/LOM オプション	なし	追加可能
------------------	----	------

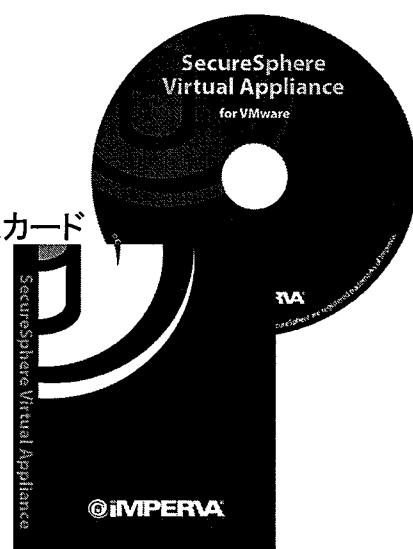
仮想アプライアンス – V series

Host PC要件

- hypervisor: VMWare ESX/ESXi 3.5以上
- プロセッサ: Dual Core Server Intel VTx or AMD-V
- HDD容量: 250GB
- NIC: hypervisorがサポートするネットワークインターフェースカード

仮想アプライアンス・Guest要件

Model	V1000	V2500	V4500	VM150
スループット	100 Mbps	500 Mbps	1 Gbps	-
CPU Core	1	2	4	2
Memory	2 GB	4 GB	8 GB	4 GB
Hard Disk	80 GB	80 GB	80 GB	80 GB

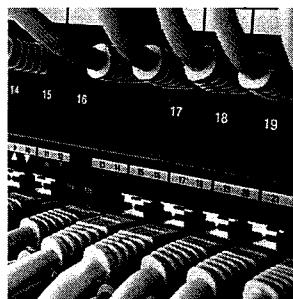


進化するエンタプライズ・セキュリティ

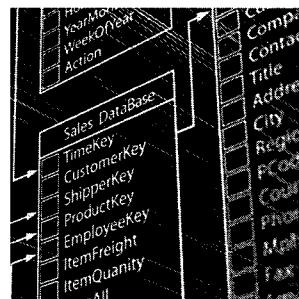
Impervaは、エンタプライズ・セキュリティの新たな中核を提案



第一の中核：
エンドポイント・セキュリティ



第二の中核：
ネットワーク・セキュリティ



第三の中核：
データ・セキュリティ

デバイスを狙った
脅威を阻止

ネットワークへの
アクセスを試みる脅威を
阻止

価値あるデータ資産の
保全を確保し、保護

© IMPERVA®

ご静聴ありがとうございました

株式会社Imperva Japan

お問い合わせ先
Email: Info_jp@imperva.com
Web: www.imperva.com

