Webサイトの最新防御法：WAFを低コストで導入・運用

WAFを利用した脆弱性診断＆対策サービス（WSS）のご紹介

三和コムテック株式会社

PRESENTATION

三和コムテック（SCT)って、どんな会社か？

三和コムテック株式会社

〒106-0032
東京都港区六本木3-4-3　三和ビル
Tel　03-3583-2386　　Fax　03-3583-2387
URL　http://www.sct.co.jp

設立：　　１９９１年
業務内容：　Webシステムインフラの構築
　　Webアプリケーション開発
　　PCI DSS準拠の普及促進（JCDSC活動）

技術提携先：日本IBM
　　McAfee, Inc. (米国)
　　Penta Security Systems Inc.(韓国)
　　Tango/04 (スペイン)
　　Razlee（イスラエル）

参加団体：　日本カード情報セキュリティ協議会（JCDSC）運営委員
　　情報システム学会
　　日本ガイドシェア（JGS）IP部会メンバー

PCI DSS準拠対策の前に

PCI DSS準拠に関係なく、WAFは必要です！

漏えいや改ざんがいっぱい起きてます。

たとえば、２０１３年前半だけでも、こんなにいっぱいですよ。例えば、こんな具合です…

2013/1

UCCに不正アクセス、会員情報が改ざん - 外部流出は否定

桜島フェリーのサイトが改ざん - 閲覧でウイルス感染のおそれ

宮崎県の農業向け気象情報サイトが改ざん - 閲覧でマルウェア感染のおそれ

須坂市公式サイトが改ざん - ウイルス感染は発生せず

農業環境技術研究所のサイトが改ざん被害 - 情報流出は確認されず

鳥取県立博物館のサイトが改ざん - 個人情報漏洩は発生せず

栃木県の雨量水位観測システムにサイバー攻撃 - データ改ざんが発生

2013/2

不正アクセスでTwitterのユーザー情報約25万人分が外部漏洩の可能性

振袖レンタルサイトが改ざん、閲覧でウイルス感染のおそれ

2013/3

2013/3

Evernoteのアカウント情報が流出 - パスワードリセットを実施

サイト改ざんで閲覧者にウイルス感染のおそれ - 日本郵政グループ会社

JINSのオンラインショップに不正アクセス - カード情報流出の可能性

サイトが改ざん被害、閲覧でウイルス感染のおそれ - 日本エアロゾル学会

環境省の運営サイトが改ざん被害 - 不正サイトへ誘導

素粒子原子核研究所・理論センターのウェブサイトが改ざん被害

企業サイトや通販サイトなど関連21サイトが改ざん - マイクロマガジン

情報処理学会HCI研究会のウェブサイトが改ざん被害

2013/4

「gooID」に対してブルートフォース攻撃 - 約3万件に不正ログイン

「Yahoo！JAPAN」サーバに不正プログラム-ファイル抽出途中で強制停止、情報流出は否定

特定IPより「フレッツ光メンバーズクラブ」に大量アクセス- 一部アカウントをロック

いしかわ動物園のサイトが改ざん被害 - 閲覧でウイルス感染のおそれ

「gooID」への攻撃、使い回しアカウント狙った可能性 - 全アカウントをロック対象に

JR東の会員向けサイトでも不正ログイン - 他社被害を受け調査したところ判明

国内のDNSキャッシュサーバがDDoS攻撃の踏み台に - JPCERTが適切な設定呼びかけ

「にんしんSOS」サイトに不正アクセス、改ざんや情報漏洩は否定 - 大阪府

アノニマスによる攻撃で朝鮮新報の登録者情報が流出

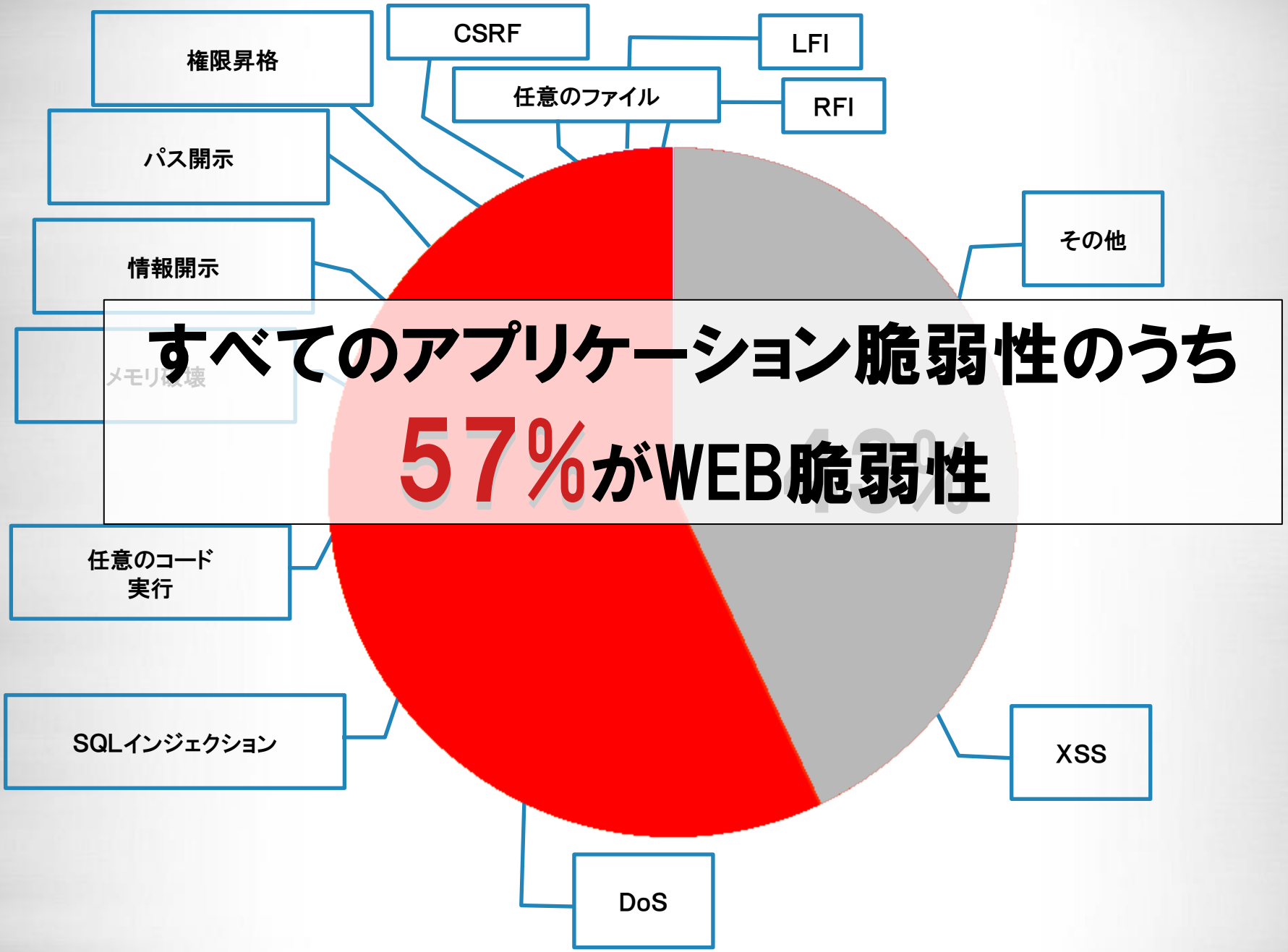
スマホ向け認証決済サービス「mopita」で不正ログインが発生 - 不正課金は確認されず

これって、今よく耳にする標的型攻撃、ですか？

いいえ、おそらく大部分は標的型攻撃ではない、と思います。

それでも、ハッキングされてしまうのですか？

はい、残念ながら。なかでも、WEBアプリケーションの脆弱性をよくつかれますね。



すべてのアプリケーション脆弱性のうち
57%がWEB脆弱性

“Application Security Trends Report” March 11, 2012 Cenzic, Inc.

Webアプリケーションファイアウォールの必要性

国際Webアプリケーションセキュリティ研究団体であるOWASPから発表された
2010年度の主なWeb脆弱性の項目及び各セキュリティ製品の対応能力の分析。

OWASP Top 10 2010	Firewall	IDS / IPS	WAF
A1: Injection	X	△	O
A2: Cross Site Scripting (XSS)	X	△	O
A3: Broken Authentication and Session Management	X	△	O
A4: Insecure Direct Object References	X	X	O
A5: Cross Site Request Forgery (CSRF)	X	X	O
A6: Security Misconfiguration	X	X	O
A7: Failure to Restrict URL Access	X	X	O
A8: Insecure Cryptographic Storage	X	X	O
A9: Insufficient Transport Layer Protection	X	O	O
A10: Unvalidated Redirects and Forwards	X	X	O

Webアプリケーションファイアウォール(WAF)だけがWeb脆弱性に完璧に対応。

なぜ、WEBアプリは脆弱なのでしょうか？

簡単に直せないからです！

Webアプリケーションの脆弱性対策と問題点

Webアプリケーション脆弱性への解決方法は、下記の２通り。

①Webアプリケーションのプログラムを修正する。

②WAF(Web Application FireWall)を導入する。

【Webアプリケーション修正の問題点】

- 開発環境がなく、本番をそのまま修正する場合が多い
- 修正した場合の現行WEBサービスへの不具合発生のリスクが計り知れない

脆弱性を直せない／放置！！

それなら、WAFを入れれば良いのでは？
何か問題点が……。

はい、あるんです！

どんな問題点ですか？

高い！

運用できない！！　から

意味がない！！！

あるSierの営業マンの話では---、

もうWAFの話は、

聞くのも嫌だ！

なぜですか？

数年前に金融系に当時著名なWAFを販売したが、その後、運用負荷（＝コスト）の高さから、放置状態となり、顧客との関係悪化！

SANWA COMTEC K.K.

それなら、WAFはみんなダメじゃないですか？

いいえ、そんなことはありません。

それは、

WAPPLES(WAF）と脆弱性診断を利用したWAFの運用サービス、

ＷＳＳです！

ＷＳＳ（web security suite）

従来のWAF利用における、全ての問題を解決したサービスだからです！

どういうこと？ もう少し教えてよ、どこが良いの

つまり、

・WAPPLESの優れたWAF機能 /運用性

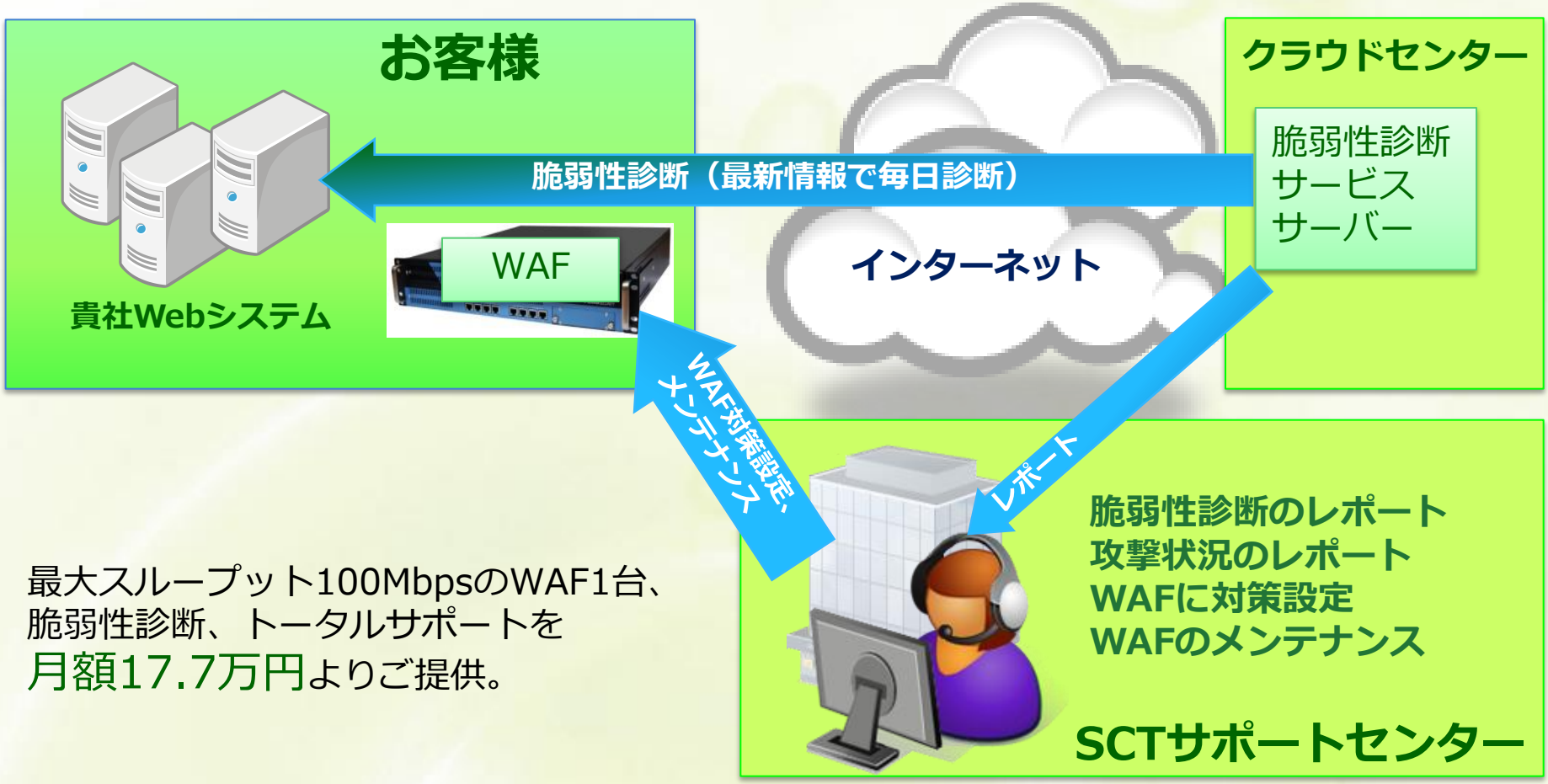
・脆弱性診断　を組み合わせて、

=> WAF**本来の機能及び適切な運用**を

低コストでサービスで提供できるのです。

SCT Web Security Suite概要

Webシステムの脆弱性を発見する診断サービスと、脆弱性に対処して貴社システムを守るWAF、そしてWAFのメンテナンスサポートをセットにしてご提供します。



最大スループット100MbpsのWAF1台、
脆弱性診断、トータルサポートを
月額17.7万円よりご提供。

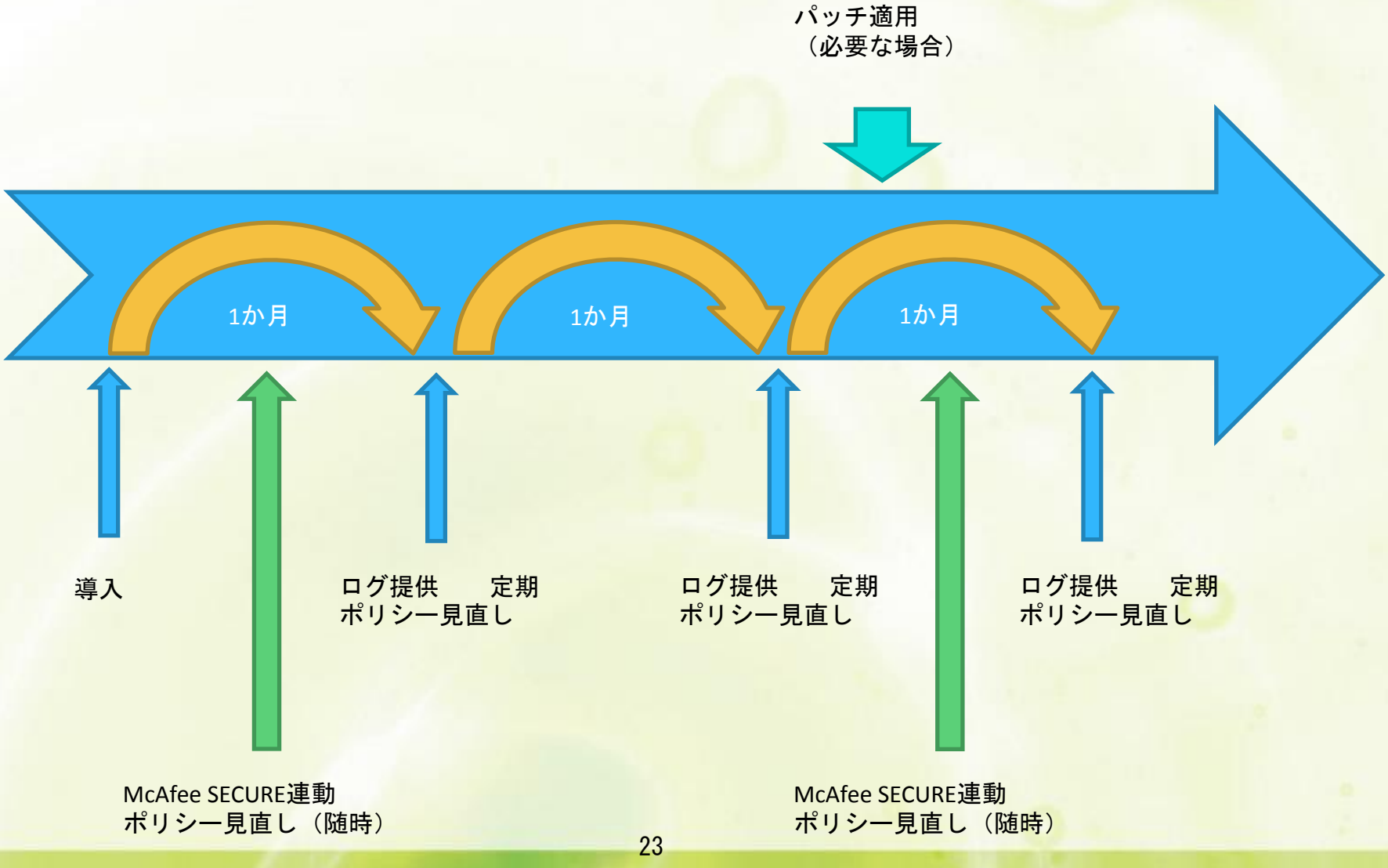
診断と対策、対応をセットで月額サービスとしてご提供。

WSSサービス詳細へ

WAF導入運用 + デイリー脆弱性診断（ASV）をパッケージにした WAFソリューション

WEB SECURITY SUITE（WSS）とは

WSSサービスの流れ（時系列）



（1）導入時作業

- 事前調査・導入プラン作成

- 導入・セットアップ（訪問）

検知のみ・遮断なしのポリシーに設定します

＜約2週間～1か月後＞

- ログ取得・ログ解析・ポリシー設定

遮断ありのポリシーに設定します

- ログの確認

（2）検知ポリシー確認（月次）

- **ログ取得・レポート送付**
  - WAFにて取得した検知ログを月次でレポート致します。

- **検知ポリシーの見直し（適宜）**
  - ログレポートより、不正アクセスの可能性があれば、お客様と確認の上、保護できるよう検知ポリシーを見直します。

（３）パッチ適用

- WAPPLESのパッチ適用は、パッチの内容・必要性・重要度等を考慮し、必要な場合に適用します。

- 導入準備・環境確認

- バックアップ

- パッチ適用

- ログの確認

（４）McAfee SECURE連動（随時）

PCI DSS / ASVとしても定評のあるMcAfee Inc. の McAfee SECURE のデイリー診断をWAFの保護対象サイトへ診断します！

- **McAfee SECUREによる診断で、一定レベルのWebアプリケーションの脆弱性が検出された場合に、適宜検知ポリシーの見直しを行い、当該脆弱性をついた不正アクセスから防御します。**
- **ログの確認**
- **McAfee SECUREによる再検査実施・結果の確認**
  - 検知ポリシー見直しによる保護設定の有効性を確認します。

なぜ、WAFにて保護しているサイトに脆弱性診断をかけるのか？

WAFの保護設定が不正アクセスに対する効果があるか、設定不備がないか、を確認するのに重要だからです。

価格体系は、どうなっていますか？

アプライアンス或いはソフトウェアWAFを販売或いは月額レンタルし、弊社のWAF運用サービスを課金する形になります。

価格体系は、どうなっていますか？

アプライアンス或いはソフトウェアWAFを販売或いは月額レンタルし、弊社のWAF運用サービスを課金する形になります。

具体的には？

保護対象サイトへのトラフィック量、サイト数、保護レベルにもよりますが、月額15万円くらいから利用可能です。

アプライアンス型の月額レンタルの場合

WSSサービスメニュー

サービス名称	SWSS50	SWSS100	SWSS500
ご提供形式	HW+サービススィート	HW+サービススィート	HW+サービススィート
最大スループット	100 Mbps	300 Mbps	500 Mbps
HTTP TPS	2,000	9,000	15,000
Form Factor	1U	1U	1U
WAF保護対象サーバー数	2 Servers	無制限	無制限
初期費用	148,000	198,000	248,000
月額サービスご提供価格	177,000	210,000	300,000

上記のスペックのWAFに加えて

- 3IPのWebサイトに対して毎日の脆弱性診断サービス
- WAFのメンテナンス
- 定期的にWAFの対策設定実施

ちなみに、もっと安いものは、ないの？

ソフトウェア型WAFの利用の場合なら、更に安くなります。

そろそろ時間がないので、まとめに入ります。

- **WAFによる脆弱性対策とその有効性を毎日の脆弱性診断で確認**
- **対策も診断も、お客様の手間（殆ど）いらず**
  - 診断は自動
  - 対策運用は弊社にて対応
- **WAF検知レポートにて月次で状況変化を確認**
- **高価で運用負担も大きいWAFを、安価な月額サービスで利用可能。**
- **PCIDSS準拠サービス/ツールの利用による確かな品質**
  - **McAfee SECURE:　要件11.2 (PCI DSS ASV)**
  - **WAF (WAPPLES):　要件　6.6　機能適合証明取得**

他にも是非ご紹介したい、

PCI DSS対策ソリューション

SCTはPCI DSSの12の要件の視点からソリューションをご提案します

ファイアウォール

インフラ/DB/アプリの監視・管理：Visual Message Center

SSL証明書発行

Webサイトの脆弱性テスト：McAfee Secure/AppScan

アンチウィルス

運用負荷の小さいWAF：WAPPLES

Webセキュリティコンサルティングサービス

Ⅰ．安全なネットワークの構築・維持

要件1．ファイアーウォールを導入し最適な設定を維持すること
- 「信用しない」ネットワークからのアクセスを拒否しないといけない
- FTPには対策を施さないといけない
- DMZを設置しなければならない

要件2．システムまたはソフトウェアの出荷時の初期設定値をそのまま使用しないこと
- 不要なアカウントは削除しないといけない
- システムセキュリティパラメータは悪用を防ぐように設定されていなければいけない

Ⅱ．カード会員データの保護

要件3．保存されたカード会員データを安全に保護すること
- 保存するデータは最小限にしなければならない
- 認証データは削除しなければならない
- カード番号は判読不能にしなければならない
- 暗号鍵を管理しなければならない

要件4．公衆ネットワーク上でカード会員データを送信する場合、暗号化すること
- 伝送データをSSLなどで暗号化しなければならない

Ⅲ．脆弱性を管理するプログラムの整備

要件5．アンチウィルスソフトウエアを利用し、定期的に更新すること
- アンチウィルスの監査ログを取得しなければならない

要件6．安全性の高いシステムとアプリケーションを開発し、保守すること
- 産業のベストプラクティスに基づく開発を行うこと
- 変更管理基準に従ったソフトウエア設定変更を行うこと
- コーディングの脆弱性をつぶさなければならない
- WAFを設置しなければならない

Ⅳ．強固なアクセス制御手法の導入

要件7．カード会員へのアクセスを業務上の必要範囲に制限すること
- アクセス権は業務上の必要範囲に制限しなければならない

要件8．コンピュータにアクセスする利用者毎に個別IDを割り当てること
- 利用者ごとに個別のIDを付与しなければならない

Ⅴ．ネットワークの定期的な監視およびテスト

要件9．カード会員データへの物理アクセスを制限すること
- 物理アクセスを制限しなければならない
- 媒体管理をしなければならない
- マシンルームへの入退出を監視しないといけない

要件10．ネットワーク資源およびカード会員データに対するすべてのアクセスを追跡し、監視すること
- 関連するログをすべて監視しなければならない
- 時計を合わせなければならない
- アクセスログを3ヶ月間保管しなければならない

Ⅵ．情報セキュリティ・ポリシーの整備

要件11．セキュリティシステムおよび管理手順を定期的にテストすること
- 四半期に一回以上、脆弱性スキャンをしなければならない
- すべてのネットワークトラフィックを監視しなければならない

要件12．情報セキュリティに関するポリシーを整備すること
- ポリシーを整備しなければならない
- リスク評価のプロセスを含まなければならない
- リスクを評価しなければならない
- インシデント対応計画を導入しなければならない
- サプライチェーンを考慮しなければならない

➢SCT社はPCI DSSに準拠するためのコンサルティングサービスや特別なソリューション製品・サービスをご提供します。

一押し対策ソリューション

脆弱性診断ツール	・WEBアプリケーション診断
脆弱性診断サービス	・PCI DSS準拠各種診断
DBアクセス保護監視	・Guardium（ガーディアム）

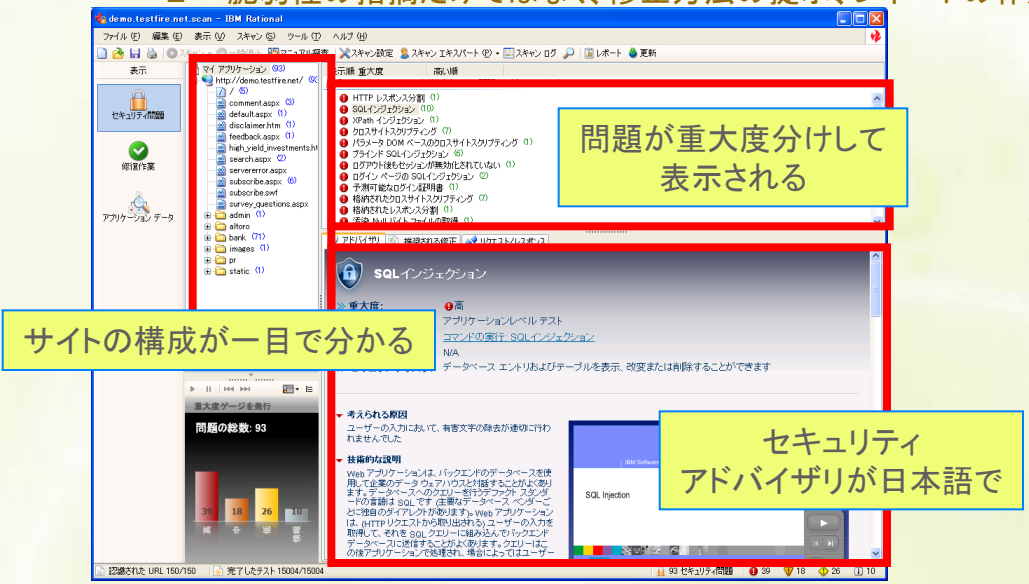
WEBアプリケーションの脆弱性診断
– 公開前診断による脆弱性リスクの早期対策を実現

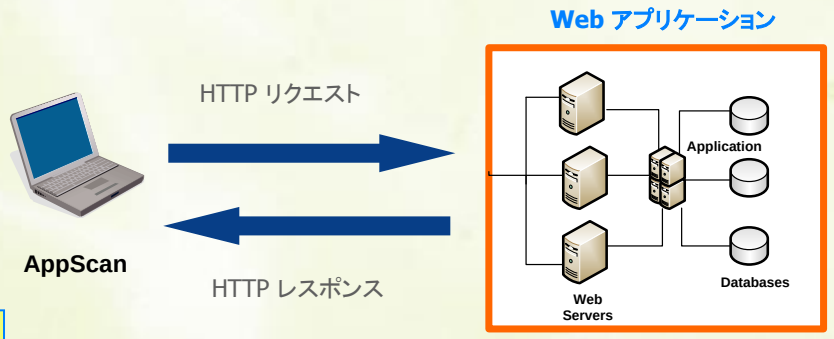
WEBアプリケーション脆弱性診断ツール

「AppScan」

世界標準の脆弱性診断ツール
AppScan Standard Edition の概要

- **市場シェア No.1(*) の Webアプリケーション セキュリティ テスト ツール**
  - 使いやすいインターフェースで、Webアプリケーションの脆弱性と、インフラ(Webサーバー等)の設定ミスや既知の問題を検知
  - Web アプリケーションをブラックボックスとして検査するため、OSや利用言語によらず検査可能
  - テストを自動化し、手作業に比べて圧倒的な網羅性を確保し、テスト時間とコストの削減が可能
  - 脆弱性の指摘だけではなく、修正方法の提示、レポートの作成

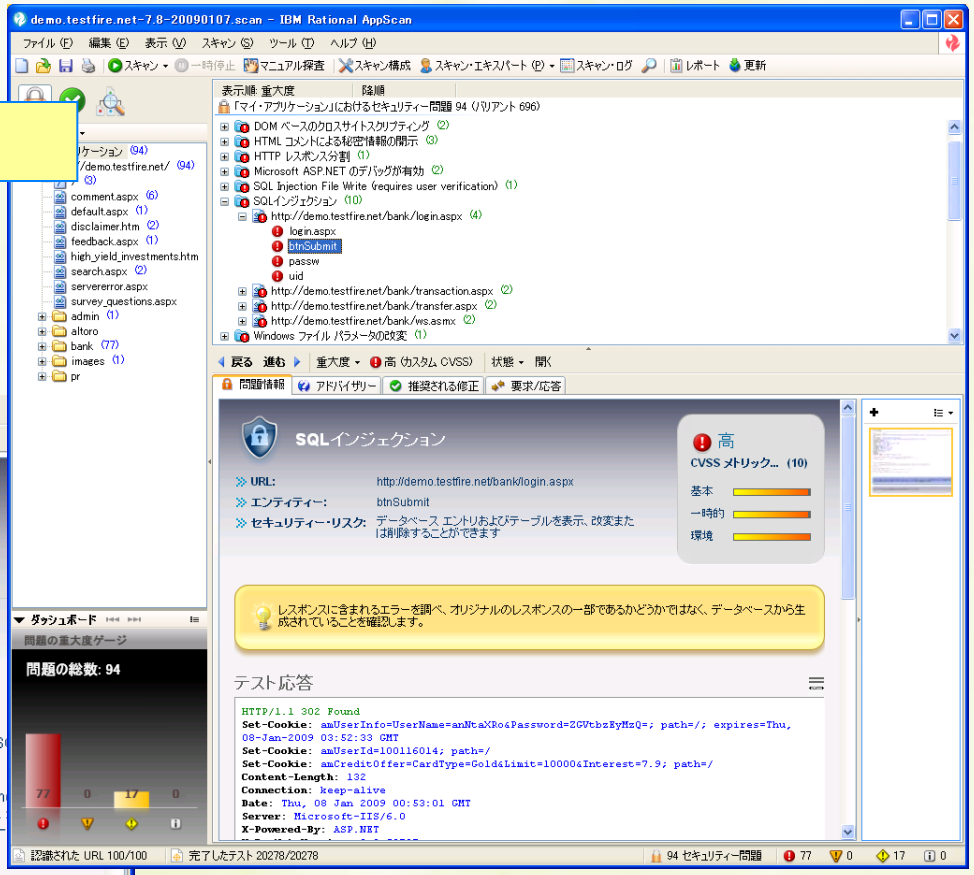


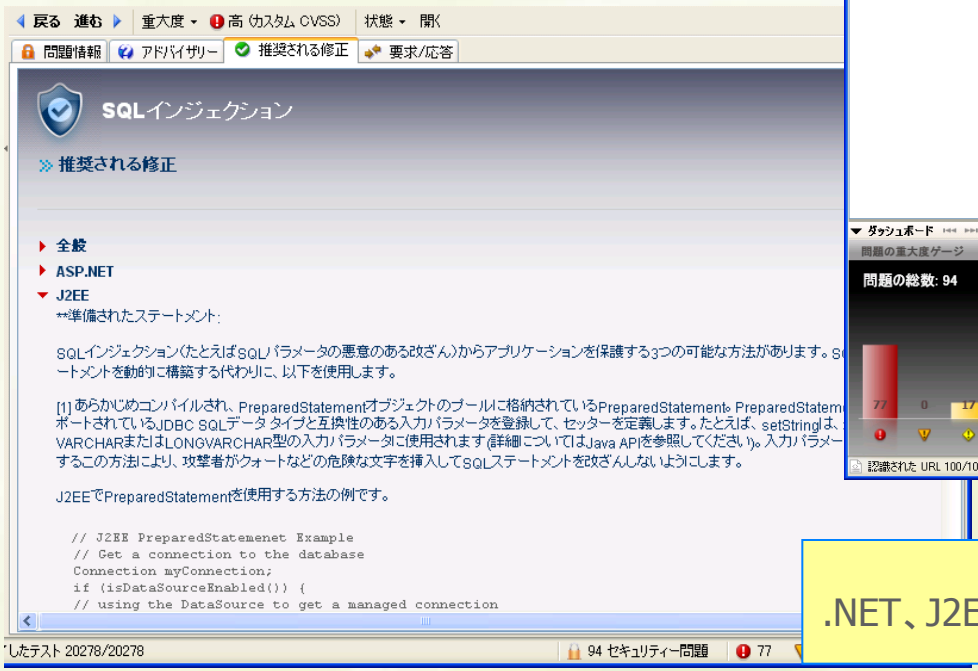


Source: Worldwide Security and Vulnerability Management Software 2006-2010 Forecast and Analysis: Managing Security Knowledge and Control, IDC #204693, December 2006; Gartner Dataquest, "Market Share: Application Development and Project and Portfolio Management, Worldwide, 2005, Table 2-1," Laurie F. Wurster and Fabrizio Biscotti, 18 May, 2006; Gartner Dataquest, "Market Share: Application Development and Project and Portfolio Management Software, Worldwide, 2006."

AppScan SE - 分かり易い情報表示

問題の詳細な解説と影響を提示

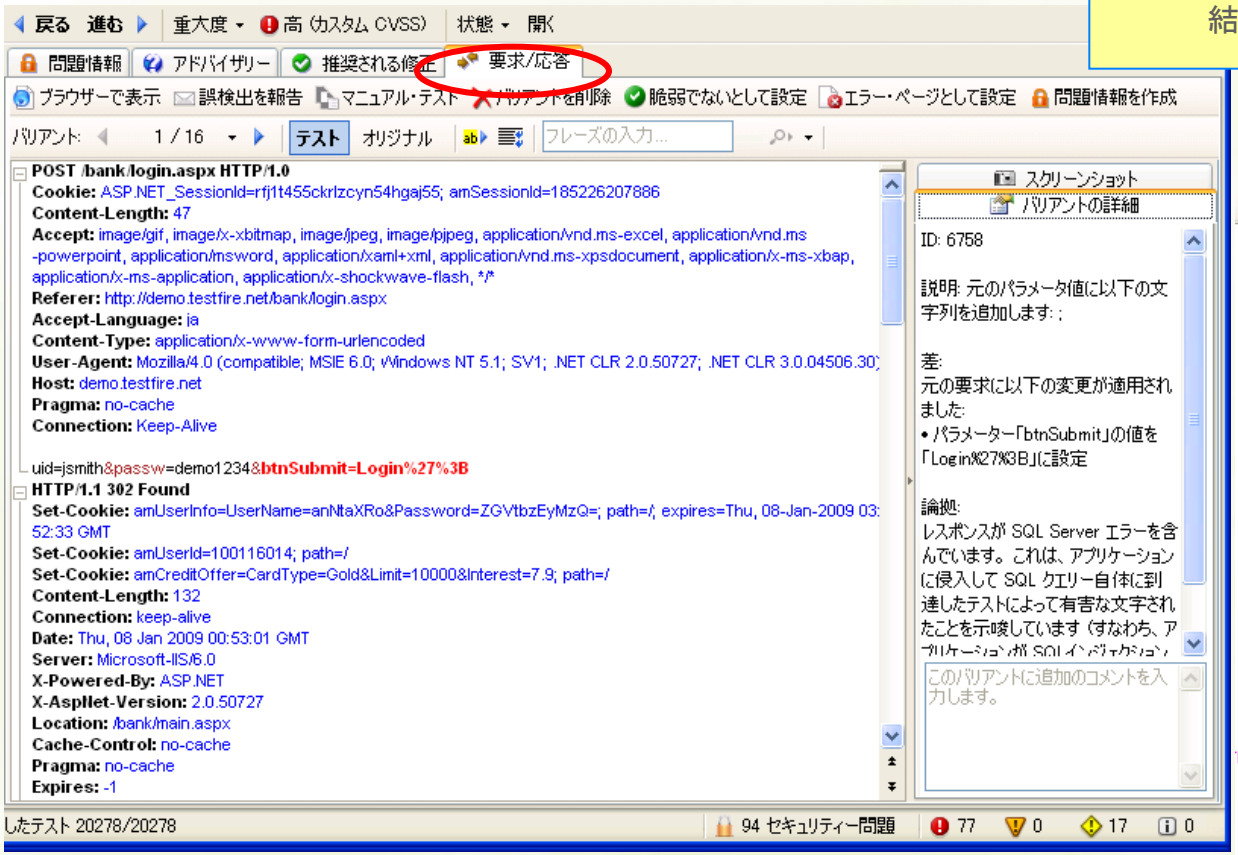




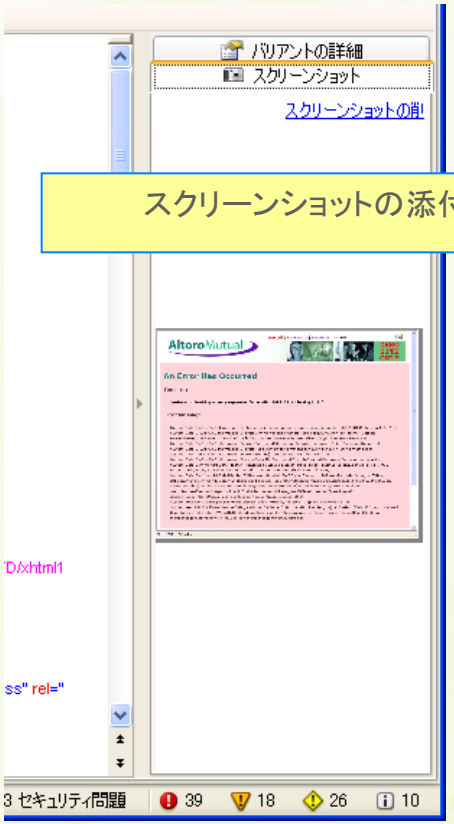
修正方法の提示
.NET、J2EE、PHP に特化した修正方法も提示

AppScan SE - 詳細なテスト情報の表示

結果をブラウザでも表示可能



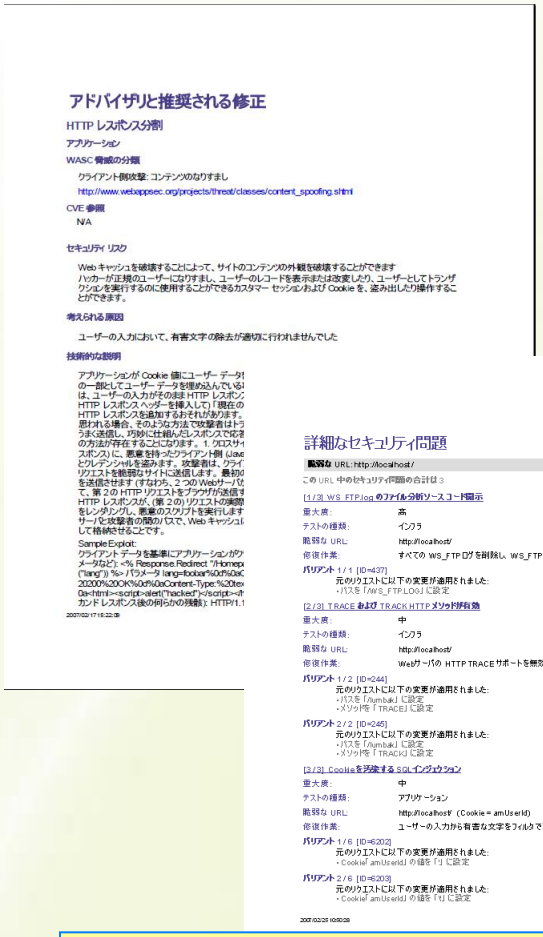
スクリーンショットの添付

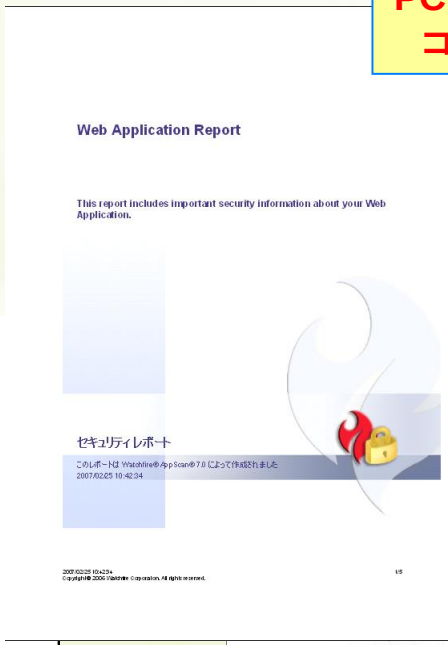


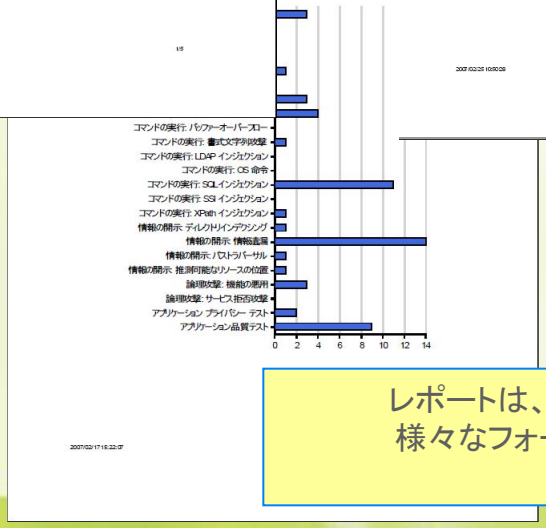
リクエスト/レスポンスの詳細を確認可能
変更点と問題点が強調表示される

AppScan SE - 詳細なレポート

PCI-DSS、OWASP Top 10 などの コンプライアンス レポートも豊富





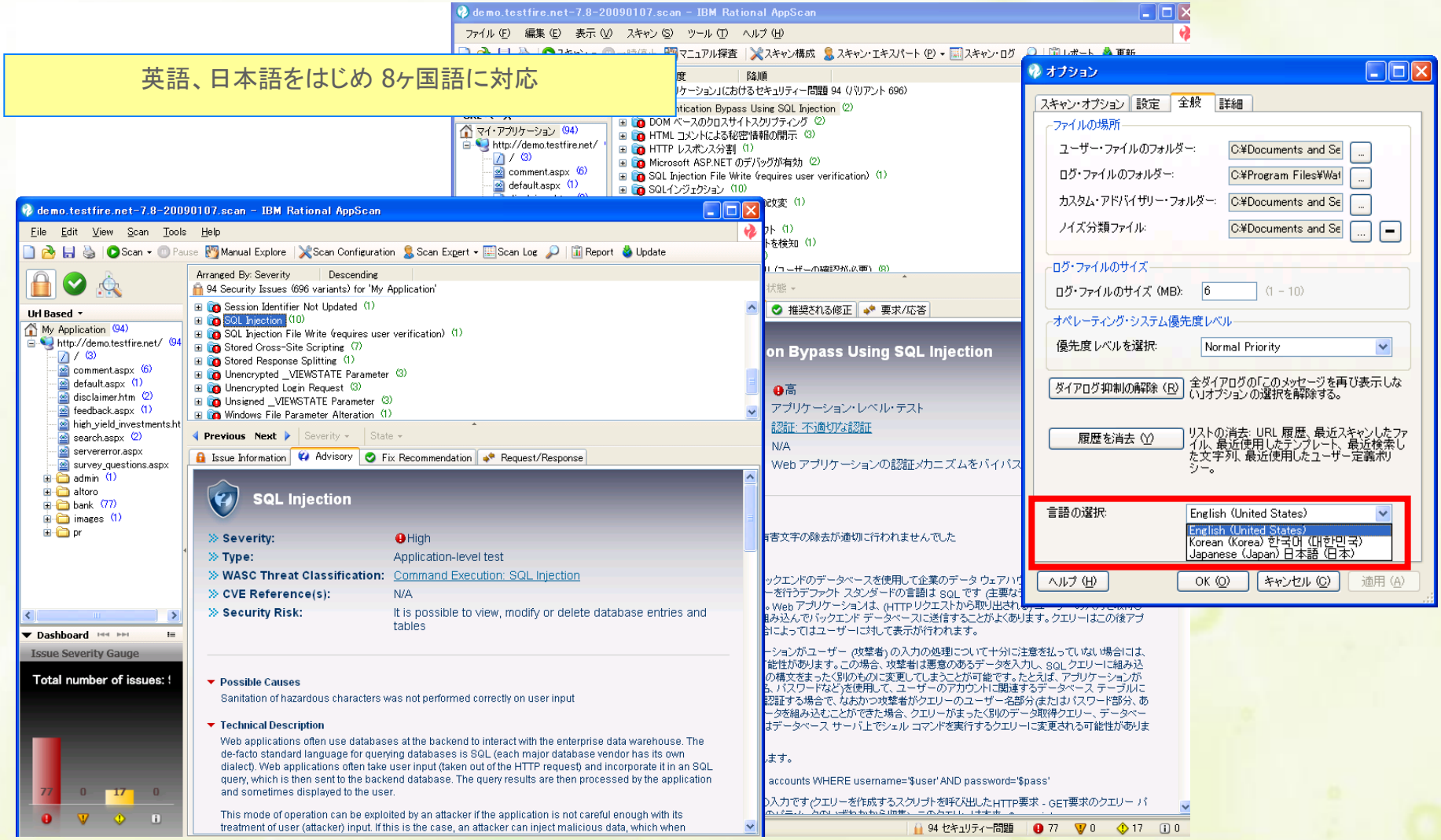


レポートに載せる内容は選択可能

レポートは、pdf、html、txt など
様々なフォーマットで保存可能

AppScan SE - 国際化

英語、日本語をはじめ 8ヶ国語に対応



ASV診断だけではない、PCI DSS準拠診断

PCI DSS対策診断サービス

なぜ、弊社サービスなのか？

せっかく良い診断ツールがあっても、

社内にリソースがない！

オンデマンドで気軽に！

なんて、声にお応えします！

PCI DSS準拠診断の概要

テストの種類	要件	目的	実施頻度	実施主体			弊社における該当サービス
				社内	ASV	第三者	
脆弱性スキャニング・テスト	11.2.1 11.2.3	内部ネットワークにおけるOSや各種サービス等に対する脆弱性の有無を調査する。	最低4半期ごと ネットワークの大きな変更時	○	○	○	ネットワーク診断(オンサイトによる脆弱性診断)
	11.2.2 11.2.3	外部ネットワークにおけるOSや各種サービス等に対する脆弱性の有無を調査する。	最低4半期ごと ネットワークの大きな変更時	△ (大きな変更時)	○	△ (大きな変更時)	ネットワーク診断(インターネット経由による脆弱性診断)
ペネトレーション・テスト	11.3.1	外部及び内部のネットワーク層における脆弱性の検出に加え、検出した脆弱性を利用して攻撃者の視点から実際に侵入が可能か検証する。	最低年1回 ネットワークの大きな変更時	○※	○	○	ネットワーク診断(ペネトレーション)
	11.3.2 6.5	外部及び内部のアプリケーション層における脆弱性の検出に加え、検出した脆弱性を利用して攻撃者の視点から実際に侵入が可能か検証する。	最低年1回 アプリケーションの大きな変更時	○※	○	○	Webアプリケーション診断
無線アクセスポイントのテスト	11.1	無線装置(無線アクセスポイント)の設置場所の調査及びセキュリティ設定が適切に実施されているかを調査する。	最低4半期ごと	○	○	○	無線LAN調査
IDS/IPSの稼働調査	11.4	IDS/IPSが不正な攻撃に対して適切に警告が発生するか調査する。	最低年1回 システムの大きな変更時	○	○	○	ネットワーク診断 (IDS/IPSの調査)
セキュリティ運用管理に関するテスト	12.1	セキュリティ基準(PCI DSSの各要件及びセキュリティポリシー)に基づき、対象範囲のシステムの運用状況を確認する。	最低年1回	○	○	○	情報セキュリティ監査 (ヒアリングや現地視察等)

※社内ネットワークからインターネット経由での診断は現実的には難しいと想定されます。

最後はDatabase監視

GUARDIUM（ガーディアム）

セキュリティ-対策 - アプローチの変化 -

	既存のアプローチ	高度なアプローチ
コントロールの範囲	全ての情報資産	もっとも重要な資産の保護に注力
コントロールの焦点	**防御的コントロール（Anti-Virus, Firewall）**	**発見的コントロール（偏差、データ、常時監視）**
視点	ネットワークの境界線	データ中心
ログ収集の目的	コンプライアンス用のレポート	脅威の発見の為
インシデント管理	部分的な対応：マルウェアの駆除と感染PCの復旧	全体像の把握：発見と攻撃パターンの分析
脅威情報	マルウェアの情報収集	昨今の攻撃者の“ターゲット”、手口、組織の重要な資産を深く理解する
成功の定義	攻撃者がネットワークに侵入して来ない事	ネットワークに侵入はされるかもしれないが、迅速に発見し、影響を最小化する

参考情報：Security for Business Innovation Council Report by RSA, The Security Division of EMC

SANWA COMTEC K.K.

コンプライアンス　監査　セキュリティ　J-SOX　PCI-DSS

Guardium
マルチ・データベースのセキュリティ・監査ソリューション

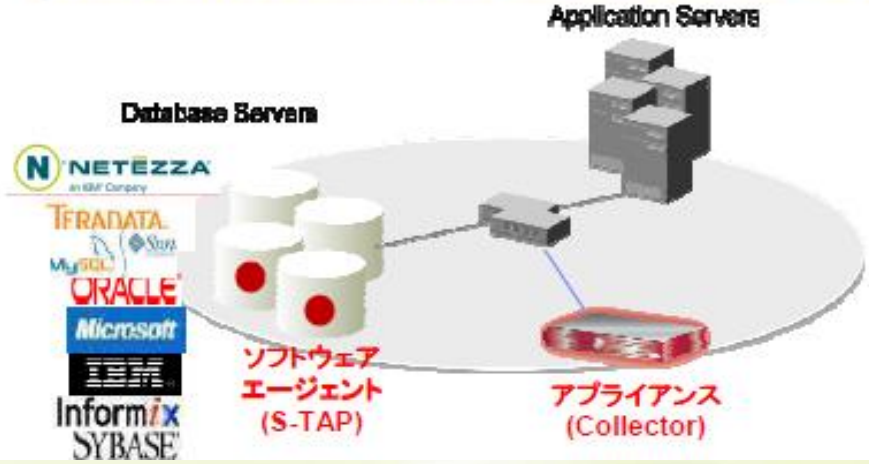
Guardium

【こんな事で悩んでいませんか？】

1. データベースセキュリティが不十分なため、情報漏洩という大きなビジネス・リスクを抱えている
2. J-SOXやPCI-DSS対応の監査ログを取りたくても、DB標準の機能では負荷が高く、業務への影響が大きい
3. 様々なDBやOS毎にDB監査の仕組みを用意するのでは運用が困難。監査対応のコストが膨大

【当製品導入のメリット】

1. 既存環境、データベースに負荷なしに全てのDBアクセスをリアルタイム監視、記録
2. いつ、誰が、どこから、どんなアクセスをしたかの詳細なDBアクセス・ログを収集可能
3. 様々なDBやOS、ERPパッケージのアクセスログを一元管理、統合的なレポートの出力が可能



製品価格: 600万円～（税抜き）

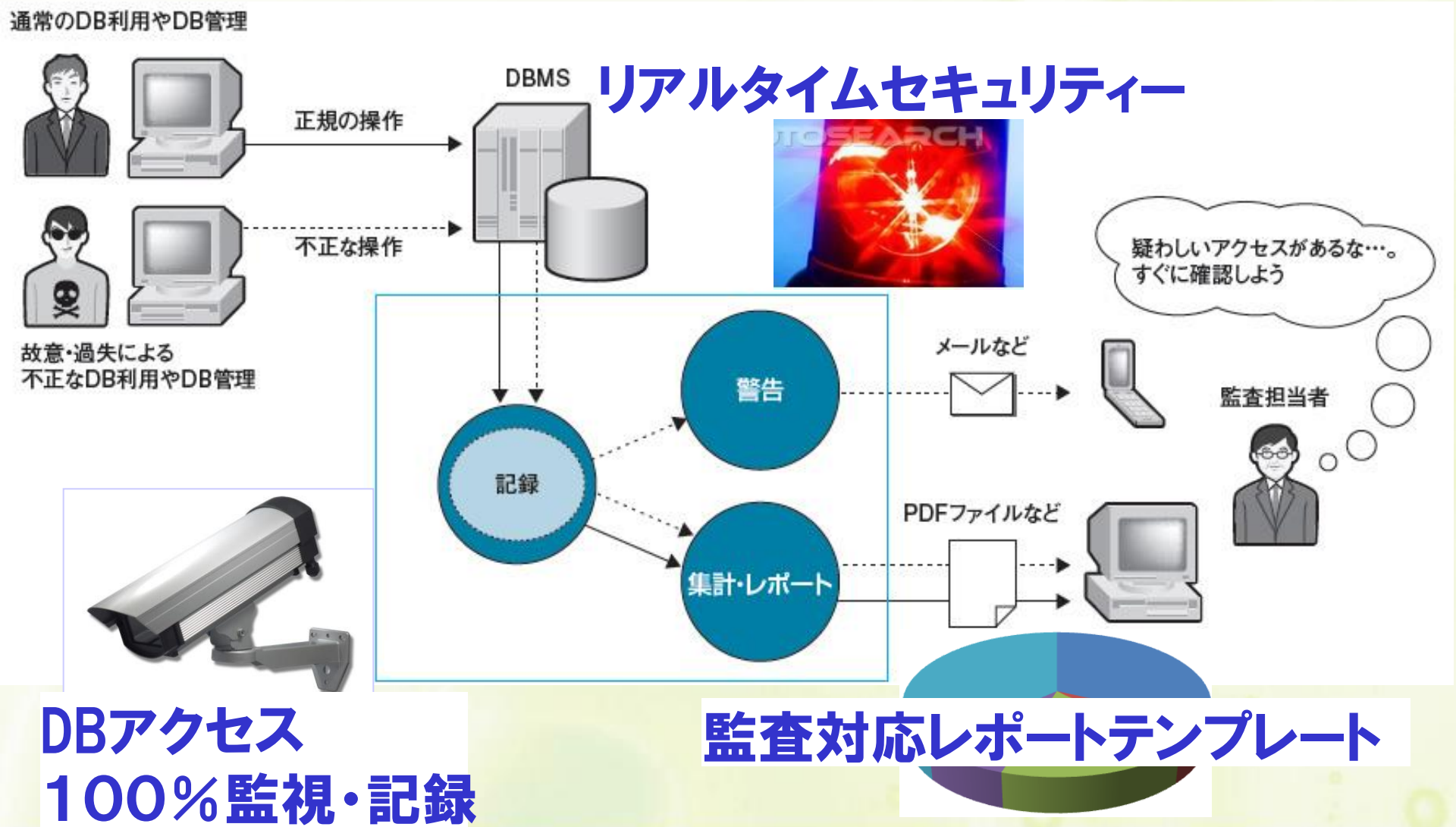
（内訳）
- S/Wライセンス
- H/W 1台
- 初年度年間保守料

導入費用: 150万円～（税抜き）

（内訳）
- ポリシー設定
- S/Wインストール、H/Wセットアップ
- ユーザートレーニング

Guardium 3 大機能

DB層に必要な 記録、警告、集計・レポート



DBアクセス
100%監視・記録

監査対応レポートテンプレート

ちょっと、脱線しましたが最後のまとめです。

- **WSSは、面倒かつコストの見えなかったWAFの導入と運用を、サービス提供、かつリーズナブルな費用で定額対応。**

- **PCIDSS準拠サービス/ツールの利用による確かな品質**
  - **McAfee SECURE:　要件11.2 (PCI DSS ASV)**
  - **WAF (WAPPLES):　要件　6.6　機能適合証明取得**

- **WSS以外にも、WEBアプリケーションを初め、各種診断（ASV、ソース、ペネトレーション）やDBアクセス監視ソリューションを提供**

ご清聴ありがとう

ございました！

三和コムテック株式会社

〒135-0047 東京都港区六本木3-4-3 三和ビル
TEL. 03-3583-2518
FAX. 03-3583-2387
sales@sct.co.jp