THE NEW VALUE FRONTIER

KYOCERA

PCIDSSセキュリティフォーラム 2013

KCCSの
PCI DSS 準拠支援ソリューション

コストを抑えたPCIDSSソリューション
脆弱性診断＋WAF

2013年7月10日

京セラコミュニケーションシステム株式会社
セキュリティ事業部　佐藤　宏昭

京セラ コミュニケーションシステム株式会社

KCCS Group

会社概要

KCCS Group

京セラコミュニケーションシステム株式会社（略称　KCCS）

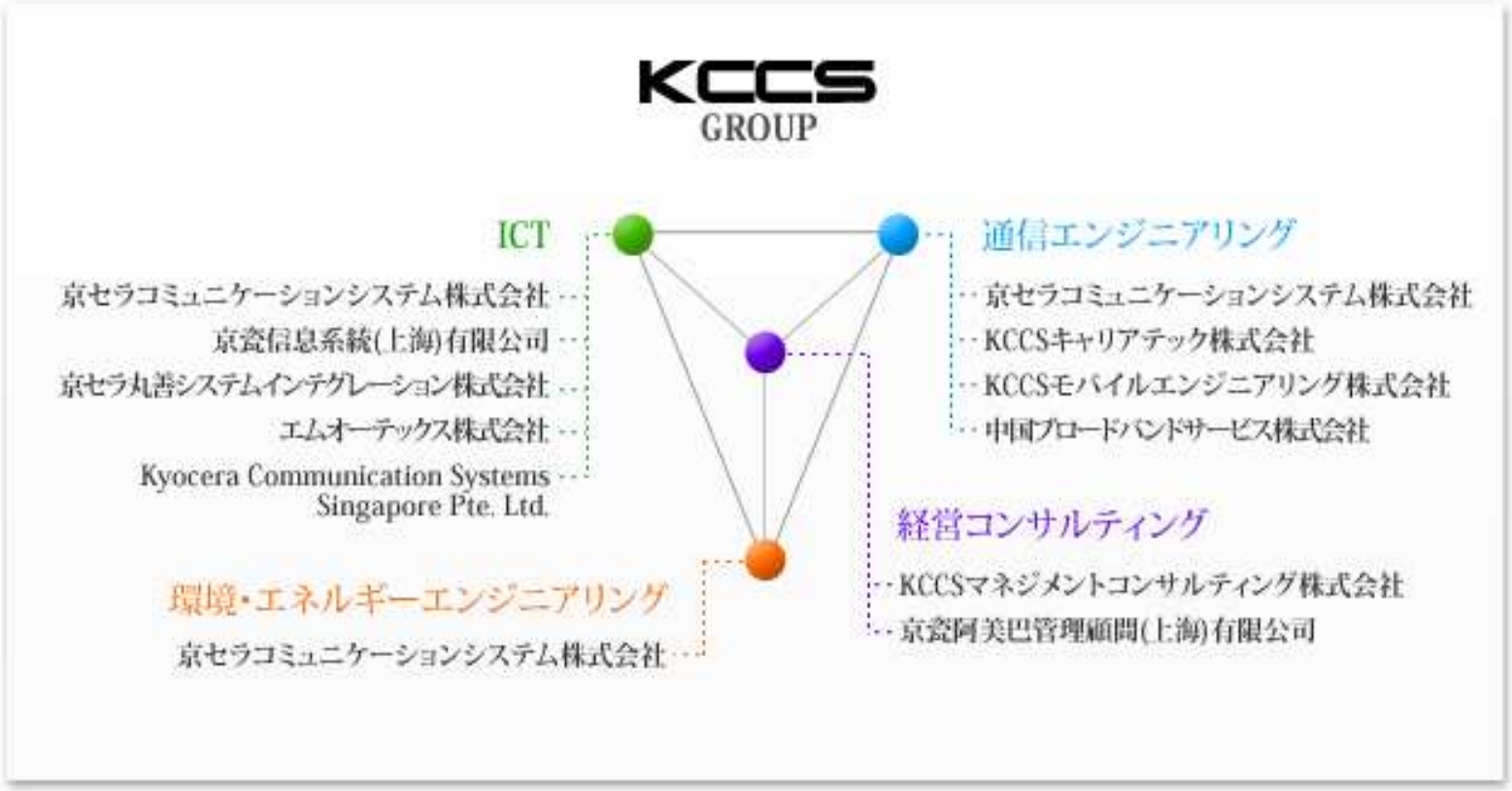
THE NEW VALUE FRONTIER
KYOCERA

資本金	29億8,594万6,900円
出資比率	京セラ㈱76.3％、 KDDI㈱23.7％
代表者	佐々木　節夫
従業員数（連結）	2,789名（2013年3月末現在）
売上高（連結）	1,109億4,278万円 （2013年3月期連結実績）

沿革

1986.11　京セラ（株）APS事業部を社内ベンチャーとして設立
1991.12　情報システム部門を統合し経営情報システム事業部と改称
1995.10　経営情報システム事業部が分離独立し、会社設立
2001.01　上海にシステム開発会社「京瓷信息系統（上海）有限公司」設立
2012.06　京瓷阿美巴管理顧問（上海）有限公司を設立
2012.08　中国ブロードバンドサービス（株）に資本参加
2012.11　エムオーテックス（株）を子会社化
2013.04　Kyocera Communication Systems Singapore Pte. Ltdを設立

会社概要（KCCSの事業展開とグループ会社）KCCS Group



KCCS　KYOCERA / MARUZEN 京セラ丸善システムインテグレーション株式会社　KCMC　KCSS　MOTEX

KCME　CBBs　KCCT　KAMC　KCSG

KCCSセキュリティソリューション（沿革）

KCCS Group

1999.10　KDDIと共同でインターネットデータセンターを設立

1999.10　Tripwire, Inc.とKCCSが提携（日本国内への販売を開始）

2002.11　nCircle Network Security, Inc.とKCCSが提携（日本国内への販売開始）

2004.11　脆弱性診断サービスを販売開始（2013.03までに3500サイト以上の診断実績）

KCCS Web脆弱性診断サービス

2007.11　SaaS型脆弱性管理ポータル：SecureOWLを販売開始

2009.08　PCIDSSに対応した診断サービス：PCIスキャンサービス販売開始

（2009.08　業界唯一「Web健康診断」を地方自治情報センター及び業界有識者と共に策定）

2011.10　バラクーダネットワークスジャパン株式会社と一次店契約を締結

2011.11　トレンドマイクロ社「Trend Micro Deep Security」を提供開始

2012.08　グローバル対応のクラウド型脆弱性診断「nCircle PureCloud」販売開始

（2012.10　Webアプリケーションセキュリティに絞った脆弱性対策の要求仕様モデルを、地方自治情報センターと業界有識者と共に策定）

2012.11　エムオーテックス株式会社を子会社化

キャリアグレードのセキュリティノウハウ

豊富なアセスメント＆製品導入実績

基準策定など業界全体の底上げ活動

KCCSのセキュリティソリューション

KCCS Group

公開サーバを狙った不正アクセス対策ソリューション

		把握	防御	検知
脆弱性を突いた攻撃	WEBアプリの脆弱性を突いた攻撃	**Web脆弱性診断** ・Webアプリケーション脆弱性診断サービス ・PureCloud (nCircle)	**Web Application Firewall** ・Barracuda Web Application Firewall(WAF) (BARRACUDA NETWORKS)	**改ざん検知・変更管理** ・Tripwire Enterprise (tripwire)
	プラットフォームの脆弱性を突いた攻撃	**ネットワーク脆弱性管理** ・nCircle IP360 ・nCircle PureCloud ・SecureOWL (nCircle)	**IDS / IPS** ・Trend Micro Deep Security（仮想パッチ機能） (TREND MICRO) ・WatchGuard (WatchGuard) ・TippingPoint (TippingPoint)	
Web感染型マルウェア		**アンチウイルス** ・Trend Micro Deep Security(アンチウイルス機能) (TREND MICRO)		**マルウェア検知** ・Tripwire Enterprise (tripwire) ・Origma+ (FFR)
サービス妨害攻撃		**DDoS対策製品** ・NSFOCUS ADS (NSFOCUS)		

KCCSのセキュリティソリューション

KCCS Group

内部ネットワークを狙った不正アクセス対策

特定ターゲットへの攻撃脆弱性の悪用	カスタムマルウェアの感染	システム認証情報の窃取	システム深部への侵入	機密情報の抜き取り
				
脆弱性管理 •nCircle IP360 •nCircle PureCloud nCircle	**ふるまい型マルウェア検知** •FFR Yarai •標的型攻撃マルウェア検査サービス FFR	**外部との通信検知** •TrendMicro Deep Discovery TREND MICRO	**脆弱性管理** •nCircle IP360 •nCircle PureCloud nCircle **重要サーバ** •TrendMicro Deep Security TREND MICRO	**外部との通信検知** •TrendMicro Deep Discovery TREND MICRO

本日のポイント

KCCS Group

目的	要件
安全なネットワークの構築・維持	要件1： カード会員データを保護するためにファイアウォールを導入し、最適な設定を維持すること
	要件2： システムパスワードと他のセキュリティ・パラメータにベンダー提供のデフォルトを使用しないこと
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
	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
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・ソフトウェアを利用し、定期的に更新すること
	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
強固なアクセス制御手法の導入	要件7： カード会員データへのアクセスを業務上の必要範囲内に制限すること
	要件8： コンピュータにアクセスする利用者毎に個別のIDを割り当てること
	要件9： カード会員データへの物理的アクセスを制御すること
定期的なネットワークの監視およびテスト	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
	要件11： セキュリティ・システムおよびプロセスを定期的にテストすること
情報セキュリティ・ポリシーの整備	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

要件11：
セキュリティシステムおよびプロセスを定期的にテストすること

11.2： 4半期に一回/構成変更時の『外部/内部脆弱性スキャン』

把握

「nCircle PureCloud」クラウド型Web／ネットワーク脆弱性診断サービス

nCircle

本日のポイント

KCCS Group

目的	要件
安全なネットワークの構築・維持	要件1： カード会員データを保護するためにファイアウォールを導入し、最適な設定を維持すること
	要件2： システムパスワードと他のセキュリティ・パラメータにベンダー提供のデフォルトを使用しないこと
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
	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
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・ソフトウェアを利用し、定期的に更新すること
	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
強固なアクセス制御	要件7： カード会員データへのアクセスを業務上の必要範囲内に制限すること

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

6.6： 年一回/構成変更時の
『ウェブアプリケーション脆弱性スキャン』及び『WAFの導入』

把握
「KCCS Web脆弱性診断サービス」「nCircle PureCloud」

KCCS Web脆弱性診断サービス nCircle

防御
「Barracuda WAF」Webアプリケーション脆弱性対策

BARRACUDA NETWORKS

Q:

脆弱性診断は
高い？手間がかかる？

脆弱性診断について

KCCS Group

診断対象

Webアプリケーション
（独自に開発されたもの）

Webアプリケーション脆弱性診断

各サイト個別に開発したアプリケーションが対象

正確な診断を行うためには、人手によるきめ細かな診断が必要

診断コストが高い

診断後の対策にも改修費用も必要

コスト

ミドルウェア※
（Tomcat, Apache、IIS等）

OS※
（Windows、Linux、UNIX等）

ネットワーク（プラットフォーム）脆弱性診断

多種多様なOSやミドルウェアが対象

脆弱性は日々報告されるためツールによる自動診断が主流

できれば内製化したい

コストは最小限に留めたい

手間

※ ミドルウェア及びOSを併せて以後、ソフトウェアと表記

要件11.2『 外部 脆弱性スキャン』

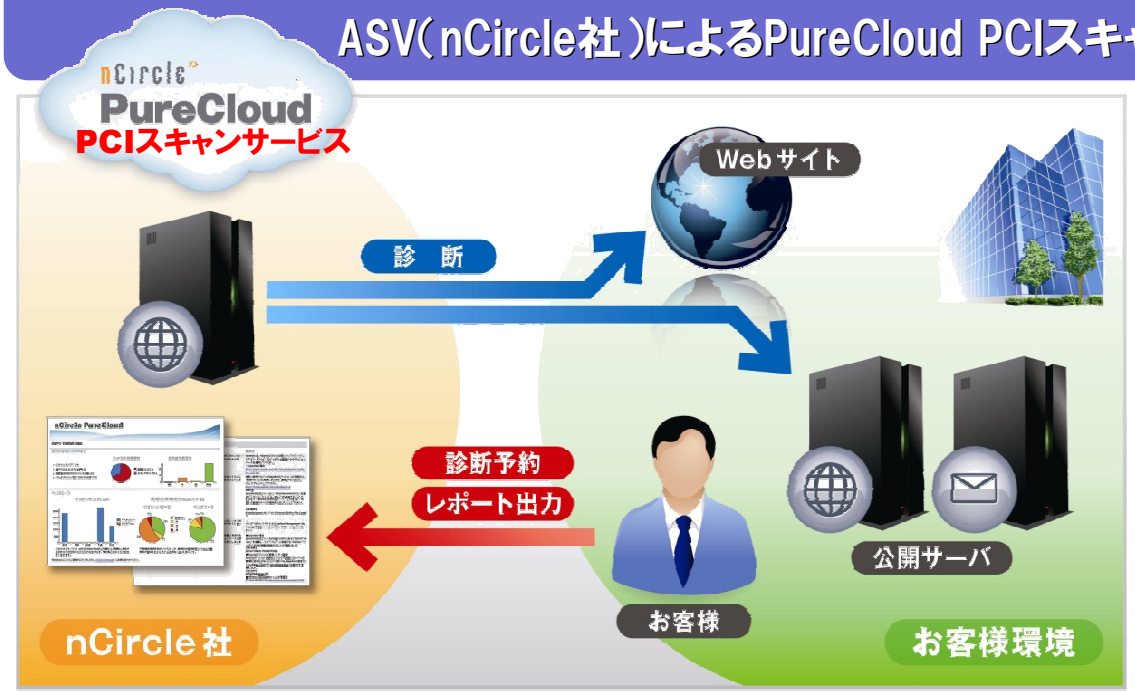
KCCS Group

把握

「nCircle PureCloud」クラウド型Web／ネットワーク脆弱性診断サービス

専用設備を必要とせず、日々発見される脆弱性を把握するための脆弱性診断サービス

『外部スキャン』には、
ASV(nCircle社)によるPureCloud PCIスキャンサービスがご利用いただけます。



Webアプリケーション脆弱性診断

- SQLインジェクション
- クロスサイトスクリプティングなど

ネットワーク脆弱性診断

- セキュリティパッチの適用状況
- アプリケーションのバージョン
- サービス(ポート)の稼働状況など

※ローカル環境に対しては、独自モジュールをPCにインストールするだけで診断可能です。

専用設備不要『外部スキャン』
PureCloudのPCIDSS対応専用診断サービス
ASV(nCircle社)による診断！

低コスト
税込 126,000円(3IP:年4回)
からご利用いただけます！

KCCSによるサポート
QAはもちろん、ご担当者へ四半期
毎に診断実施時期をご連絡！

要件11.2『 内部 脆弱性スキャン』

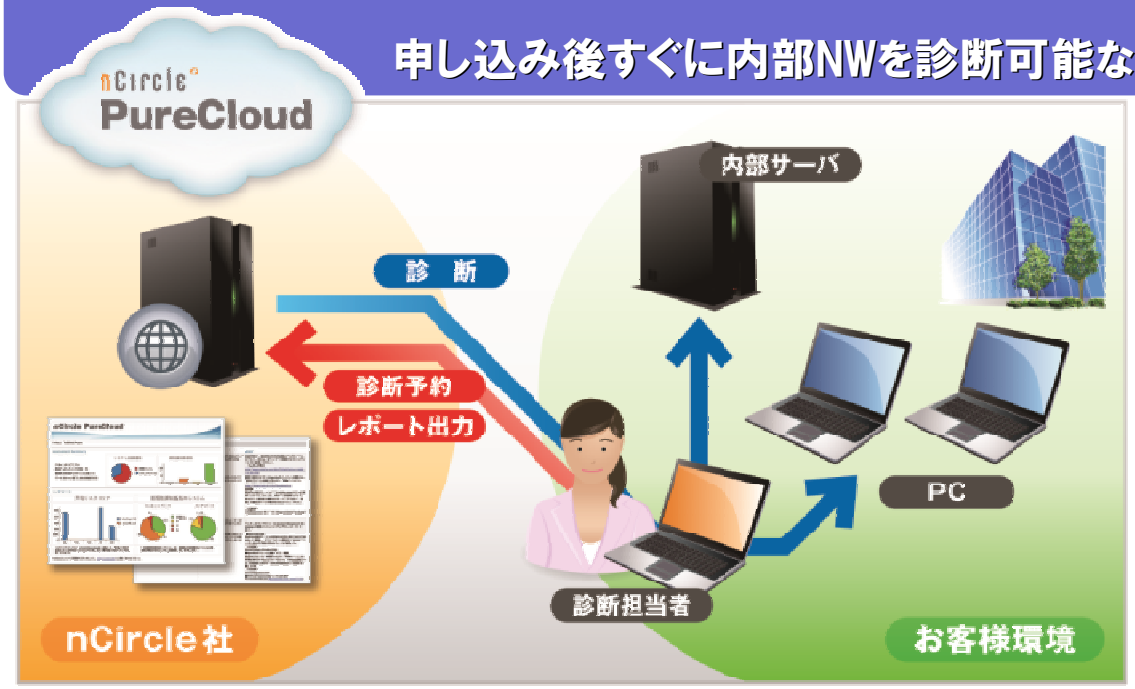
KCCS Group

把握

「nCircle PureCloud」クラウド型Web／ネットワーク脆弱性診断サービス

専用設備を必要とせず、日々発見される脆弱性を把握するための脆弱性診断サービス

『内部スキャン』には、
申し込み後すぐに内部NWを診断可能なPureCloud がご利用いただけます。



ネットワーク脆弱性診断

- セキュリティパッチの適用状況
- アプリケーションのバージョン
- サービス（ポート）の稼働状況など

※ローカル環境に対しては、独自モジュールをPCにインストールするだけで診断可能です。

専用設備不要『内部スキャン』
PCに簡単な設定をするだけで
イントラネットに診断可能！

低コスト
年間8,000円（税別）／IPで
10IPからご利用いただけます！

日本語GUIで操作が簡単
診断実行までのウィザードも提供
社内での内製化も容易！

要件6.6『Webアプリケーション脆弱性スキャン』

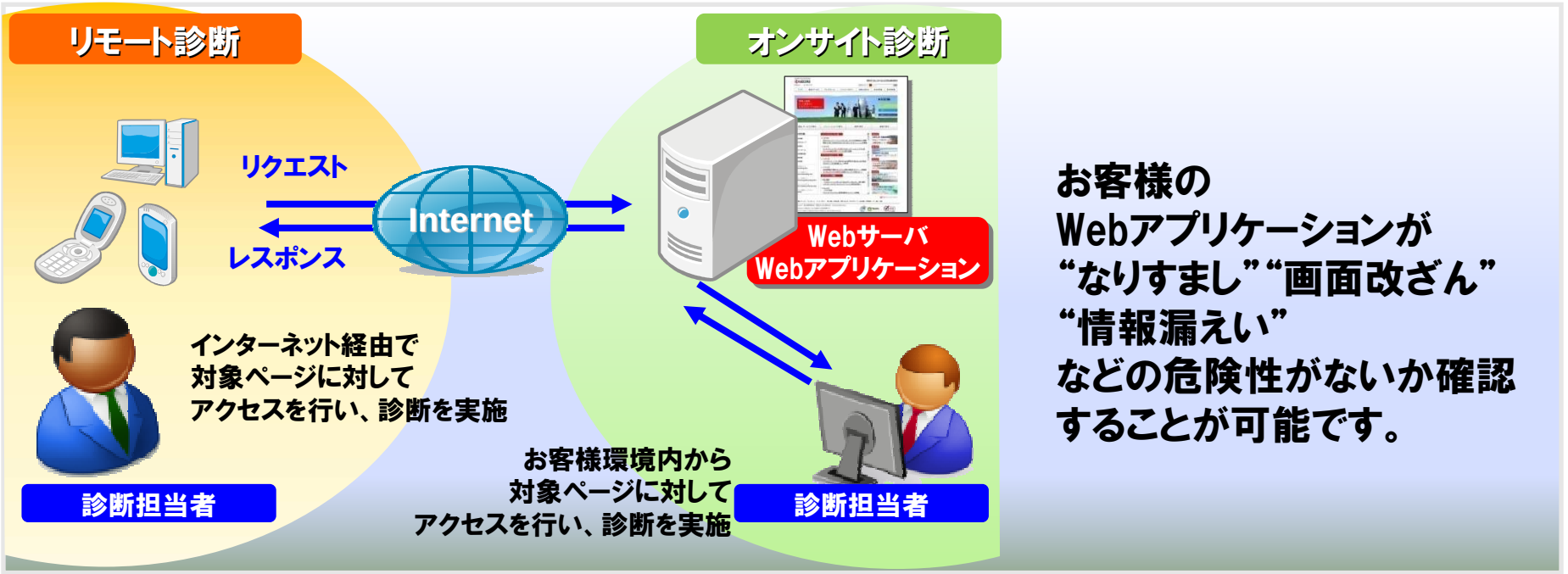
KCCS Group

把握

「 KCCS　Web脆弱性診断サービス」

セキュリティ・スペシャリストによる、きめ細かく信頼性の高い診断を実

KCCS
Web脆弱性
診断サービス



お客様の
Webアプリケーションが
“なりすまし”“画面改ざん”
“情報漏えい”
などの危険性がないか確認
することが可能です。

高精度な診断の提供

セキュリティスペシャリストによる
高精度なマニュアル診断！

提供多様なニーズに対応

PCサイトはもちろん、携帯やスマート
フォンアプリの診断も可能！

豊富な診断メニュー

初回診断と再診断等
お客様環境に応じたメニューを提
供 ！

Q:

ウェブアプリケーション
の脆弱性は
システムの改修が必須？

脆弱性診断について

KCCS Group

診断対象

Webアプリケーション
（独自に開発されたもの）

Webアプリケーション脆弱性診断

各サイト個別に開発したアプリケーションが対象

正確な診断を行うためには、人手によるきめ細かな診断が必要

診断コストが高い

診断後の対策にも改修費用も必要

コスト

ミドルウェア※
（Tomcat, Apache、IIS等）

OS※
（Windows、Linux、UNIX等）

ネットワーク（プラットフォーム）脆弱性診断

多種多様なOSやミドルウェアが対象

脆弱性は日々報告されるためツールによる自動診断が主流

できれば内製化したい

コストは最小限に留めたい

手間

※ ミドルウェア及びOSを併せて以後、ソフトウェアと表記

発見された脆弱性は改修すべき？

KCCS Group

ウェブアプリケーション診断で脆弱性が検出！

Webアプリケーションへの攻撃手法は、
日々変化し、**高度化**している

セキュアプログラミングによる対応

開発者のスキルに大きく依存する
既存アプリケーションの修正は困難
膨大な時間と費用がかかる
日々進化する攻撃手法へ対応できない

Web Application Firewallの導入

簡単導入、簡単設定
優れたコストパフォーマンス

ハッカーは、対策が施されるまで待ってくれない

発見された脆弱性は(どこまで)改修すべき？

KCCS Group

- 1000行のプログラムの中に、15個の脆弱性があると報告（米国国防総省）
- セキュリティの問題を1つ発見するのに、75分かかり、それを修正するのに、6時間かかる
- ビジネスアプリケーションは、150,000～250,000行のコードからなる(Software Magazine)

コードを修正する場合:

問題発見:15*150k*1.25hrs/40 = 84週

問題修正:15*250k*6hrs/40 = 562週

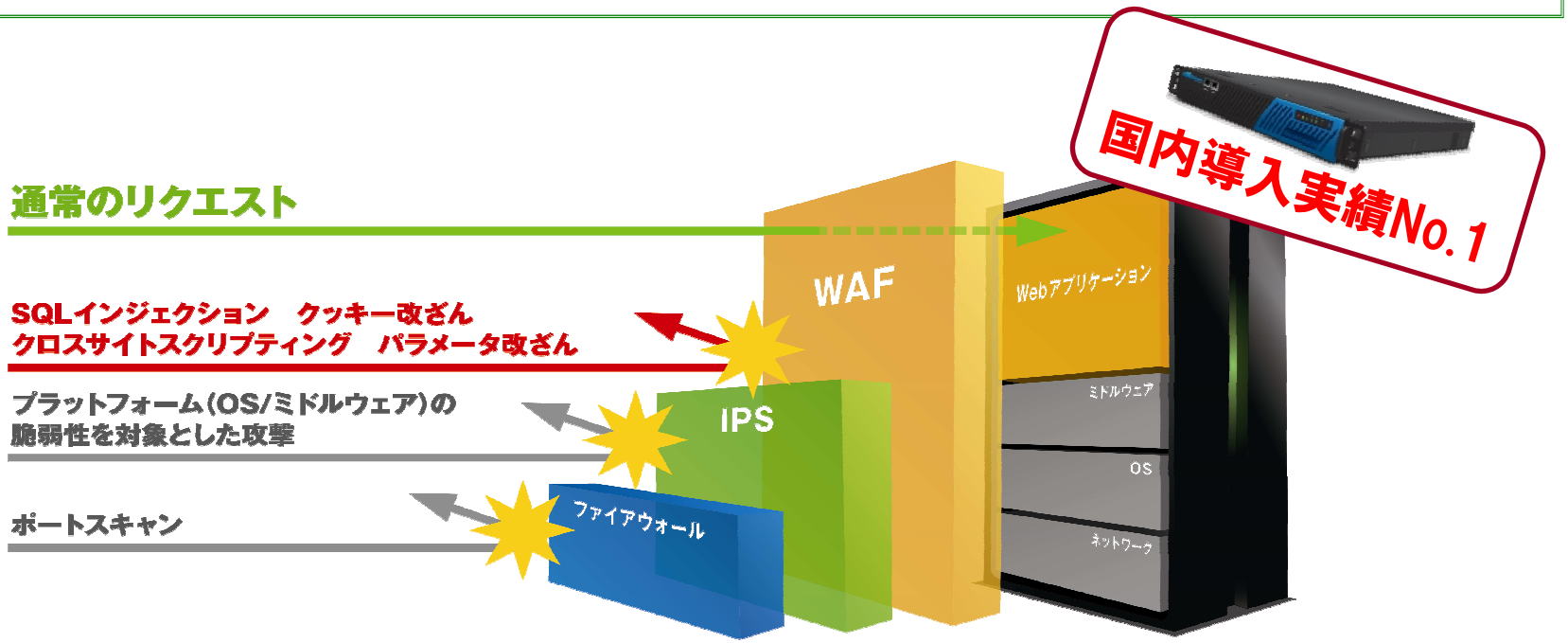
完璧な機能を求めるのか？
セキュリティの強化を優先するのか

Webアプリケーション脆弱性対策「Barracuda WAF」KCCS Group

防御

「Barracuda WAF」Webアプリケーション脆弱性対策

従来のFWやIDS／IPSでは守りきれない、Webサーバに対する脅威を徹底ブロック



精度の高い ブラックリスト

検知漏れや過剰検知の少ない精度の高いブラックリスト

低価格・低ランニングコスト

130万円台(初年度保守含む)から
設定工数や運用工数を大幅削減

日本語GUIで操作が簡単

直感的な操作で
導入後の運用も簡単

Webアプリケーション脆弱性対策「Barracuda WAF」KCCS Group

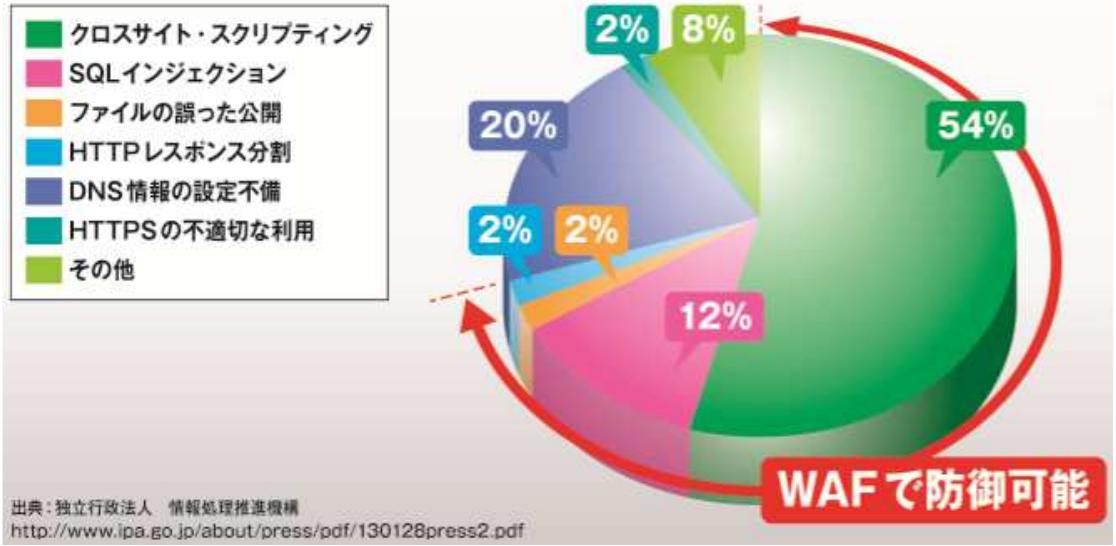
防御

「Barracuda WAF」×　KCCS WEB脆弱性診断サービス

KCCS
Web脆弱性
診断サービス

情報漏えい被害の原因となる脆弱性の多くは

「SQLインジェクション」や「クロスサイトスクリプティング」



脆弱性関連情報に関する届出情報（2012/10-12月）

KCCSの
Web脆弱性診断サービスなら

WAFにおける
脆弱性防御可否をご案内

脆弱性名	WAF	WAF備考
SQLインジェクション	◎	シグネチャで防御可能
パス・トラバーサル	◎	シグネチャで防御可能
クロスサイト・スクリプティング	◎	シグネチャで防御可能
不適切なHTMLコメント	○	個別のチューニングにより防御は可能 ※一律非表示は難しい

万が一攻撃された時の「防御」

約70%の攻撃はWAFによる一括防御、
その他の攻撃には、KCCSのWEB脆弱性診断（マニュアル）による検査と対策で
堅牢なWebサイトの構築！

まとめ

KCCS Group

脆弱性診断によるリスクの「把握」

日々発見される環境(OS/ﾐﾄﾞﾙｳｪｱ)の脆弱性は、ツールによる定期診断を！

把握

「nCircle PureCloud」クラウド型Web／ネットワーク脆弱性診断サービス

nCircle

低コストのツール選定　SaaS型ASV診断　診断の内製化

万が一攻撃された時の「防御」

WAF＋KCCS Web脆弱性診断による堅牢なWebサイトの構築

把握

「 KCCS　Web脆弱性診断サービス」

KCCS Web脆弱性診断サービス

信頼性の高いWeb診断 ＋ 診断結果を元にしたWAF導入　改修/再診断コスト低減

防御

「Barracuda WAF」Webアプリケーション脆弱性対策

BARRACUDA NETWORKS

ご清聴、誠に有り難うございました。

本日ご案内した商品については、以下URLでもご案内しております。
http://www.kccs.co.jp/pcidss/

THE NEW VALUE FRONTIER

KYOCERA

京セラ コミュニケーションシステム株式会社

＜お問い合わせ先＞
京セラコミュニケーションシステム株式会社
KCCSカスタマーサポートセンター
〒108-8605 東京都港区三田3-11-34（センチュリー三田ビル5F）
電　話：0120-911-901（フリーコール）
　　050-3161-3924（携帯電話・PHS・IP電話など）
メール：kccs-support@kccs.co.jp

※製品の仕様などは予告なく変更させていただく場合があります。
※記載の製品ならびにサービス名および会社名などは、それぞれ各社の商標または登録商標です。
※KCCSは京セラコミュニケーションシステム㈱の略称です。