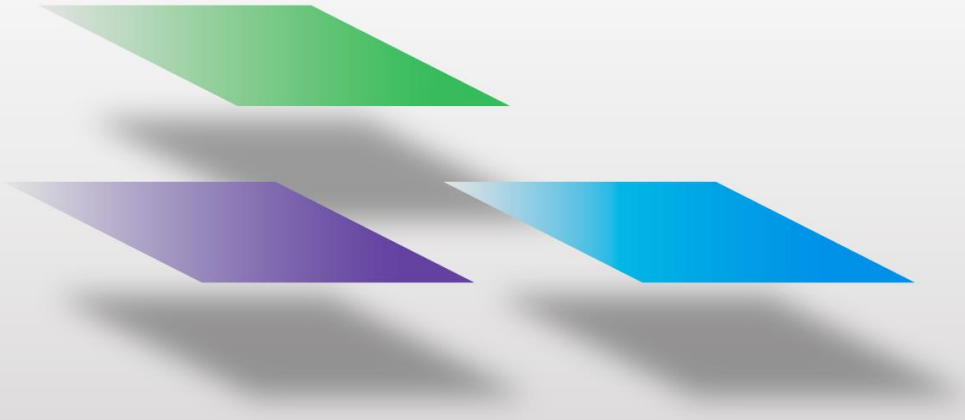
THE NEW VALUE FRONTIER

KYOCERA

【カード情報セキュリティの最新動向と「PCI DSS　Ver3.0」】

急増かつ巧妙化するサイバー攻撃から企業を守るには？

～セキュリティ専門家が分析する最新動向と対策～



2014年2月7日
京セラコミュニケーションシステム株式会社
プロダクトサービス事業本部　技術顧問
徳丸　浩

京セラ コミュニケーションシステム株式会社

KCCS Group

講演者紹介

KCCS Group

京セラコミュニケーションシステム株式会社
プロダクトサービス事業本部 技術顧問
徳丸　浩

経歴

1985年 京セラ株式会社入社
1995年 京セラコミュニケーションシステム株式会社(KCCS)に出向・転籍
2008年 KCCS退職、HASHコンサルティング株式会社設立

経験したこと

京セラ入社当時はCAD、計算幾何学、数値シミュレーションなどを担当
その後、企業向けパッケージソフトの企画・開発・事業化を担当
1999年から、携帯電話向けインフラ、プラットフォームの企画・開発を担当
Webアプリケーションのセキュリティ問題に直面、研究、社内展開、寄稿などを開始
2004年にKCCS社内ベンチャーとしてWebアプリケーションセキュリティ事業を立ち上げ

現在

- HASHコンサルティング株式会社　代表　http://www.hash-c.co.jp/
- 京セラコミュニケーションシステム株式会社 技術顧問　http://www.kccs.co.jp/security/
- 独立行政法人情報処理推進機構　非常勤研究員　http://www.ipa.go.jp/security/
- 技術士（情報工学部門）

最近の不正アクセス事例

KCCS Group

被害事例	
2014年　1月	某金融会社のシステムに不正アクセス。約4000万枚分のカード情報が漏えい
2014年　1月	某出版会社のサイトに不正アクセス。閲覧したユーザがウイルス感染
2013年　12月	某小売会社の通販サイトに不正アクセス。約3000件の顧客情報が漏えい
2013年　10月	某小売会社のサイトに不正アクセス。約15万件の個人情報が漏えい
2013年　8月	某掲示板サービス会社のサイトに不正アクセス。約3万7000件のカード情報など漏えい
2013年　8月	某ゲーム会社のサイトに不正アクセス。約4万件のアカウント情報漏えい
2013年　8月	某保険会社のサイトが改ざん、閲覧したユーザがウイルス感染 ※2013年4月から8月の間で約3600件のサイト改ざんの報告（ JPCERT / CC ）
2013年　7月	某通信サービス会社のサイトに不正アクセス。約169万件のアカウント情報漏えい
2013年　7月	某通信サービス会社のサイトに不正アクセス。約2万2000件のアカウント情報漏えい
2013年　6月	某ゲーム会社のサイトに不正アクセス。約2万4000件のアカウント情報漏えい 別のゲーム会社においても同様の事例。約3万6000件のアカウント情報漏えい
2013年　6月	某自動車会社のサイトが改ざん。閲覧したユーザがウイルス感染

不正アクセス急増の原因！？

新たな手口による「改ざん」事件が急増中！

ソフトウェアの脆弱性を悪用した「改ざん」による情報流出

基盤ソフトウェア（ミドルウェア）の脆弱性を悪用

急増している攻撃手口

KCCS Group

某ECサイトの例：フレームワークの脆弱性を悪用したカード情報漏えい

2013年3月6日にバックドアプログラムが設置され、第三者のサーバにクレジットカード情報が転送されるようにプログラムが改ざんされていたことが判明。

同社では3月14日に不正アクセスの痕跡を発見し、通販サイトを閉鎖。
漏えいした可能性のあるクレジットカード情報は2059件で、これまでに20件の不正利用の申告があり、不正侵入はミドルウェア（フレームワーク）「Apache Struts 2」の脆弱性を突いて行われた。

発表資料抜粋

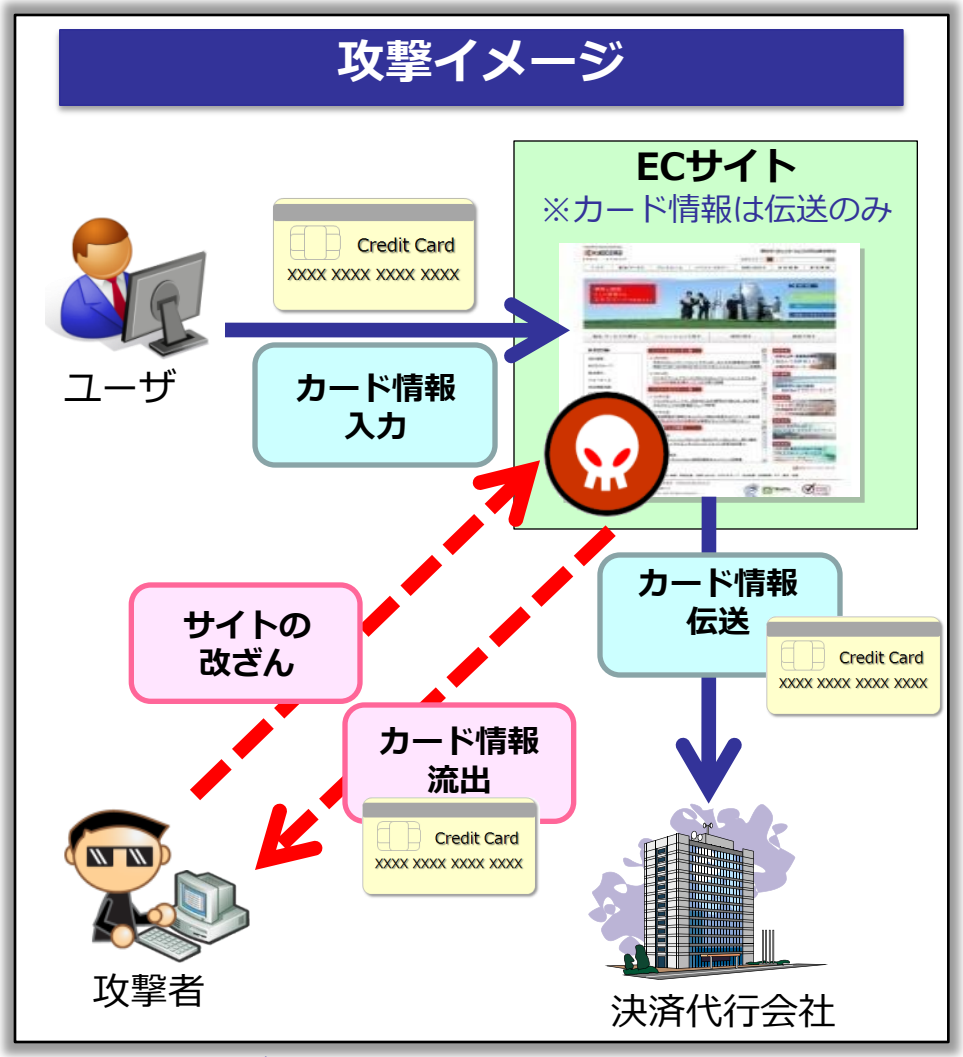
お客様のクレジットカード情報が第三者の外部データベースサーバに送信される内容の改ざんであり、**当社で保管していない**お客様のクレジットカード情報が外部流出する結果となりました。

自社に保管していない
カード情報を
盗む手口とは！？

急増している攻撃手口

KCCS Group

◎カード情報が保存されていないのに流出？



侵入経路（改ざん）には
Apacheフレームワークであるstruts 2の既知の脆弱性が悪用された。

脆弱性を攻撃し、攻撃者のサーバにクレジットカード情報が転送されるように**アプリケーションプログラムを改ざん。**

クレジットカード情報は、**正規の送信先（決済代行会社）と攻撃者双方に送信**されていた。

アプリケーションプログラムの改ざん後、発覚するまでの**9日間**クレジットカード情報が流出し続けた。

データベースへの直接攻撃ではなく、プログラムを改ざんしデータを外部に送信するという新しいタイプの攻撃手口

デモ

Apache Strutsに関する注意喚起

KCCS Group

JPCERT/CC Alert 2013-07-19
Apache Struts の脆弱性 (S2-016) に関する注意喚起

概要

Apache Software Foundation が提供している Apache Struts には脆弱性が存在します。

すでに、この脆弱性の実証コードが公開されており、JPCERT/CC にて実証コードを用いて検証した結果、Apache Struts アプリケーションを実行しているアプリケーションサーバの実行権限で任意の OS コマンドが実行されることを確認しました。

JPCERTコーディネーションセンターより引用 https://www.jpcert.or.jp/at/2013/at130033.html

7月16日にアップデートプログラムが公開され、翌日の17日に攻撃が急増！

**脆弱性情報の公開から攻撃対象となるまでの期間が短く、
アップデートプログラムの検証や適用が
間に合わないケースが増加！**

！ポイント！！

**最新情報の確認と脆弱性診断に加え、
狙われやすいアプリケーションは、
最新版にすることを推奨**

私が分析するポイント

KCCS Group

侵入経路（改ざん）には
Apacheフレームワークであるstruts 2の既知の脆弱性が悪用された。

脆弱性を攻撃し、攻撃者のサーバに
クレジットカード情報が転送されるように
アプリケーションプログラムを改ざん。

クレジットカード情報は、**正規の送信先（決済代行会社）と攻撃者双方に送信**されていた。

アプリケーションプログラムが改ざん後、
発覚するまでの**9日間**クレジットカード
情報が流出し続けた。

既知の脆弱性

公表日	CVE番号	概要	CVSS
2012/01/08	CVE-2012-0391	任意のJavaメソッド実行の脆弱性	9.3
2012/01/08	CVE-2012-0392	任意のコマンドを実行される脆弱性	9.3
2012/01/08	CVE-2012-0393	任意のファイルを作成または上書きされる脆弱性	6.4

！！ポイント①！！

**日々公開されるOSやミドルウェアの脆弱性を『把握』し対策をすることが重要です。
また、万が一の攻撃に備えて
WAFなどの活用も有効です。**

！！ポイント②！！

プログラムを改ざんし外部にデータ送信する攻撃は、迅速に『検知』することで被害を最小限に留めることが可能です。

新しい攻撃手口ではありますが、基本的な対応が有効です。

ポイント①におけるPCIDSS要件

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

『Webアプリケーション脆弱性スキャン』 および 『WAFの導入』

把握

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

KCCS Web脆弱性診断サービス

TRIPWIRE® PURECLOUD

防御

「Barracuda WAF」 Webアプリケーション脆弱性対策

BARRACUDA NETWORKS

ポイント②におけるPCIDSS要件

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
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

11.5： 重要なファイルの不正な変更を担当者に警告し、重要なファイルの比較を少なくとも週に1 回実行するようにメカニズムが構成されていることを確認する。

『変更管理ソリューションの導入』

検知

「Tripwre Enterprise」 改ざん検知・変更管理ソリューション

tripwire

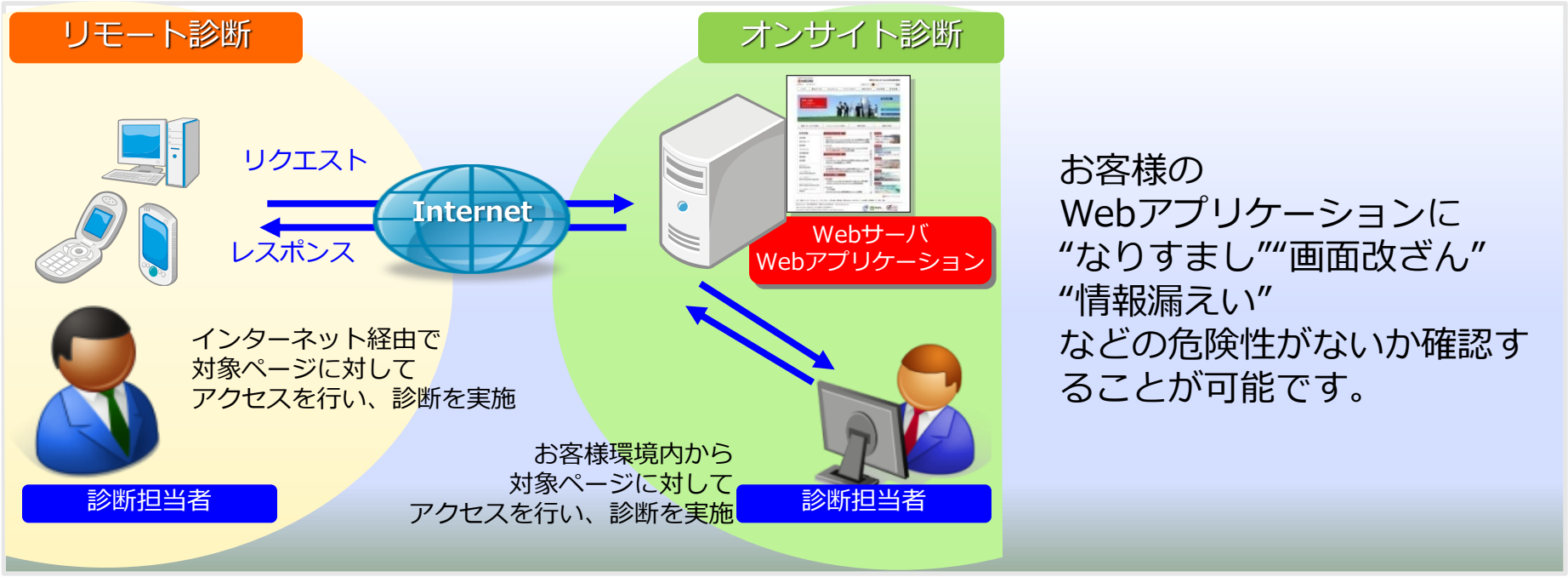
ポイント①『Webアプリケーション脆弱性スキャン』

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施。

KCCS Web脆弱性診断サービス



お客様の
Webアプリケーションに
“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！

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！

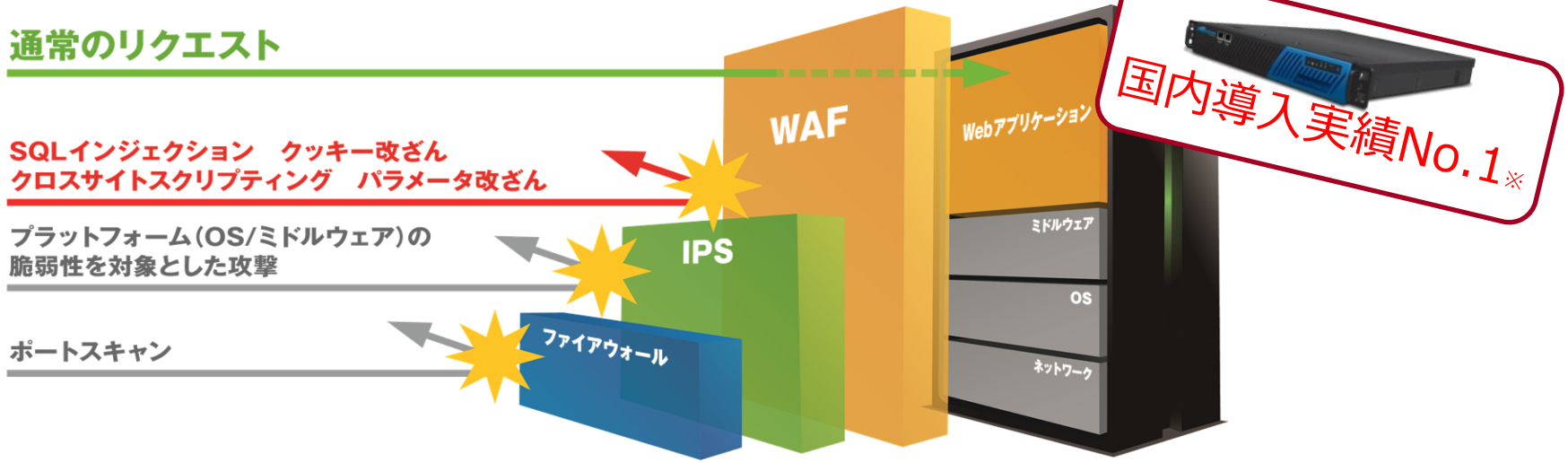
豊富な診断メニュー

初回診断と再診断など
お客様環境に応じたメニューを提供 ！

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



「Barracuda WAF」であれば、Webアプリケーション脆弱性対策の他にも・・・

L7 DDoS攻撃対策

通信量を常に監視し、
想定している通信量から判断

パスワードリスト攻撃対策

大量のパケットを検知した時だけ
2要素認証

IPレピュテーション

特定の国だけ
アクセス許可 or アクセス拒否
＋
怪しいネットワークからの通信拒否

※株式会社富士キメラ総研発行2012ネットワークセキュリティビジネス調査総覧

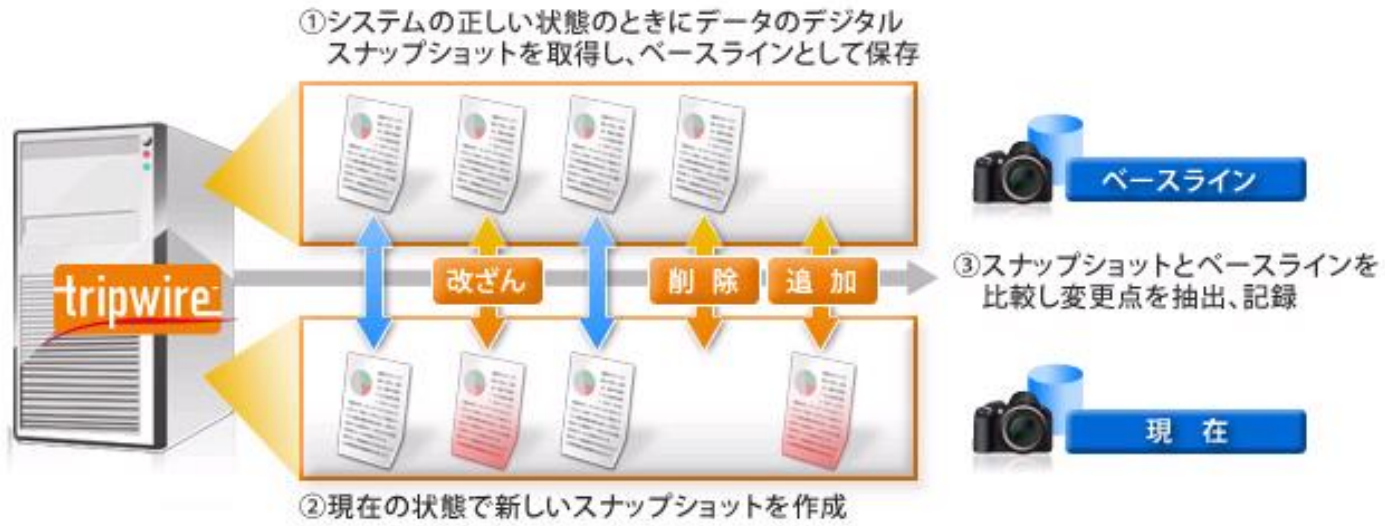
ポイント②『変更管理ソリューション』

KCCS Group

検知

「Tripwre Enterprise」 改ざん検知・変更管理ソリューション

tripwire



◎ツール導入のメリット

- 大量ファイルの目視確認は極めて困難である。また、更新日付やファイルサイズの確認では、見逃す可能性があるため、ツールでの対策が最適
- Webコンテンツ以外の設定ファイルやバイナリの改ざんチェックが可能
- リアルタイム・チェックによる迅速な対処
  →「実害」に至る前に検知し対処、「実害」自体も極小化が図れる

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 ・スマートフォン向けセキュリティサービス	**Web Application Firewall** ・Barracuda Web Application Firewall（WAF） Barracuda	**改ざん検知・変更管理** ・Tripwire Enterprise tripwire
	ﾌﾟ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** ・Tripwire IP360 ・Tripwire PureCloud ・SecureOWL tripwire　Secure OWL	**IDS / IPS** ・Trend Micro Deep Security（仮想パッチ機能） TREND MICRO ・WatchGuard ・TippingPoint WatchGuard　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 ・FFR tabaru　FFRI　tripwire
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

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 ・スマートフォン向けセキュリティサービス 要件11.3 要件11.4	**Web Application Firewall** ・Barracuda Web Application Firewall (WAF) 要件6 Barracuda	**改ざん検知・変更管理** ・Tripwire Enterprise 要件11.5 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** ・Tripwire IP360 ・Tripwire PureCloud ・SecureOWL 要件11.3 要件11.4 tripwire Secure OWL	**IDS / IPS** ・Trend Micro Deep Security（仮想パッチ機能） 要件11.4 ・WatchGuard ・TippingPoint TREND MICRO WatchGuard 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 ・FFR tabaru FFRI tripwire
サービス妨害攻撃		**DDoS対策製品** ・NSFOCUS　ADS NSFOCUS		

キャンペーンのお知らせ

KCCS Group

先着20社様限定　無償キャンペーン

セキュリティ対策として何から実施すれば良いのか分からないお客様、
PCI DSSを取得する前に現状のセキュリティリスクを簡単に把握したいお客様に

「リスクの可視化サービス」をご提供させていただきます。

- 脆弱性診断サービス
- ＧＡＰ分析
- ログ解析サービス

1）お申込み期間　：２０１４年2月7日　～　２０１４年3月２８日
2）実施時期　：２０１４年４月～
2）対象企業様　：本セミナーにご参加いただいたお客様に限り
3）価格　：無料
4）対象　：1IP、1サイト
5）お申込み方法　：下記の宛先まで、ご連絡ください。

宛先　：KCCSカスタマーサポートセンター
E-Mail　：kccs-support@kccs.co.jp
TEL　：0120-911-901（フリーコール）
050-2018-1827（携帯電話・PHS・IP電話など）

ご清聴、ありがとうございました。

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>

KCCSカスタマーサポートセンター

電　話：0120-911-901（フリーコール）
050-2018-1827（携帯電話・PHS・IP電話など）
メール：kccs-support@kccs.co.jp