PCIDSSセキュリティフォーラム 2013
～PCIDSSへの効率的な対策を探る～
2013年7月10日(水) 10:00～17:10(受付開始 9:30)
会　場　TKP大手町カンファレンスセンター
主　催　日本カード情報セキュリティ協議会ベンダー部会

仮想化環境におけるPCI DSS取得のカギは“早く”、“安く”、“手戻りなく”
～3拍子揃ったセキュリティ製品 Trend Micro Deep Securityのご紹介～

トレンドマイクロ株式会社
エンタープライズマーケティング部
福井　順一
2013年7月10日

目次

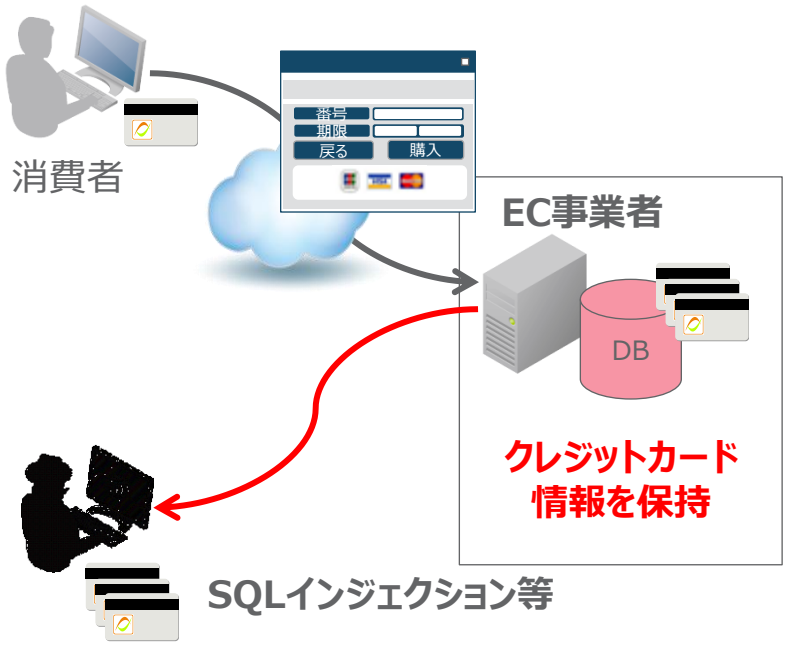
- 非保持でも漏れた、クレジットカード情報
- 事故の概要
- 今すぐ点検すべきこと
- PCIDSS要件に照らした考察
- ３拍子揃ったセキュリティソリューションのご紹介

非保持でも漏れた
クレジットカード情報

従来の事故との大きな違い

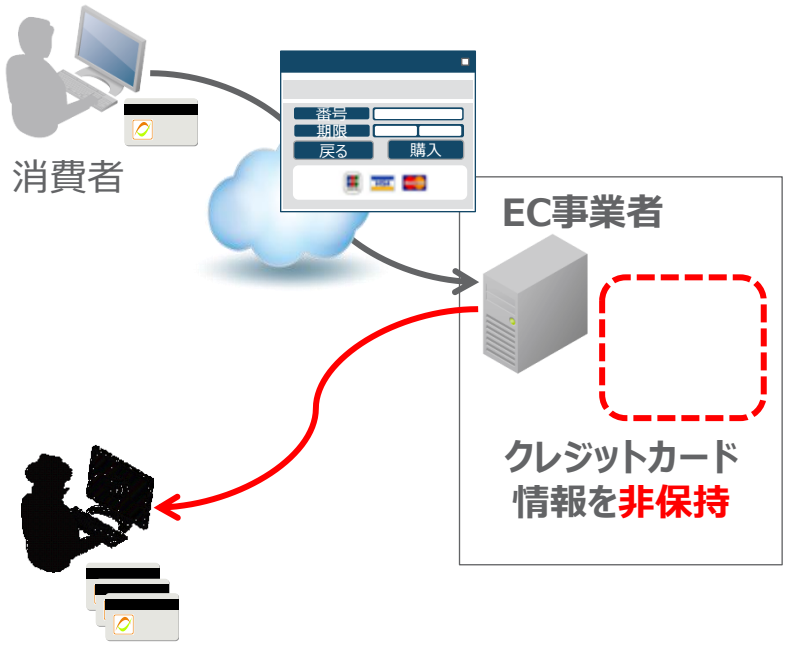
従来の事故

クレジットカード情報を**保持している場合**に、脆弱性を悪用され漏えいする事故が発生していた。



今回の事故

クレジットカード情報を**保持していない**のに、漏えいする事故が発生した。



クレジットカード情報を保持していない＝安全　という認識を改める

原因：既知の脆弱性の悪用

Apache Struts2の“既知の脆弱性”を悪用された

- Apache Struts2とは
  - オープンソースのJava Webアプリケーションのフレームワーク。
  - アプリケーションの開発を効率化することができる。
  - 2005年頃にはStruts1がJava Webフレームワークのデファクトスタンダードと呼ばれるほど普及。（※）
- 既知の脆弱性（主なもの）

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

※ http://ja.wikipedia.org/wiki/Apache_Struts

今すぐ点検すべきこと（隙間になりがちなミドルウェア）

分類	ソフトウェア（例）	点検項目
CMS（Content Management System）	・Joomla! ・Movable Type ・WordPress ・Orchard ・e107 ・MODX ・Moodle ・Plone ・Drupal　など	【共通】 □最新のバージョンを使用しているか（CMSのプラグインも含む） □不要な機能を無効にしているか □委託先との関係も含め、脆弱性管理のルールが定まっているか 【認証機能があるもの（※）】 □デフォルトのID/パスワードを変更しているか □推測されにくいパスワードを設定しているか □共有IDを使用していないか □アクセスできる人、端末、NWを必要最小限にしているか □アクセスログを取得しているか ※SSH,FTP,RDPなど、リモートログイン機能についても同様に確認
管理パネル・コンソール	・cPanel ・Parallels Plesk Panel ・phpMyAdmin ・Jboss　など	
フレームワーク	・Apache Struts ・Ruby on Rails　など	
ECプラットフォーム	・EC CUBE ・Zen Cart ・osCommerce　など	

PCIDSS要件に照らした考察

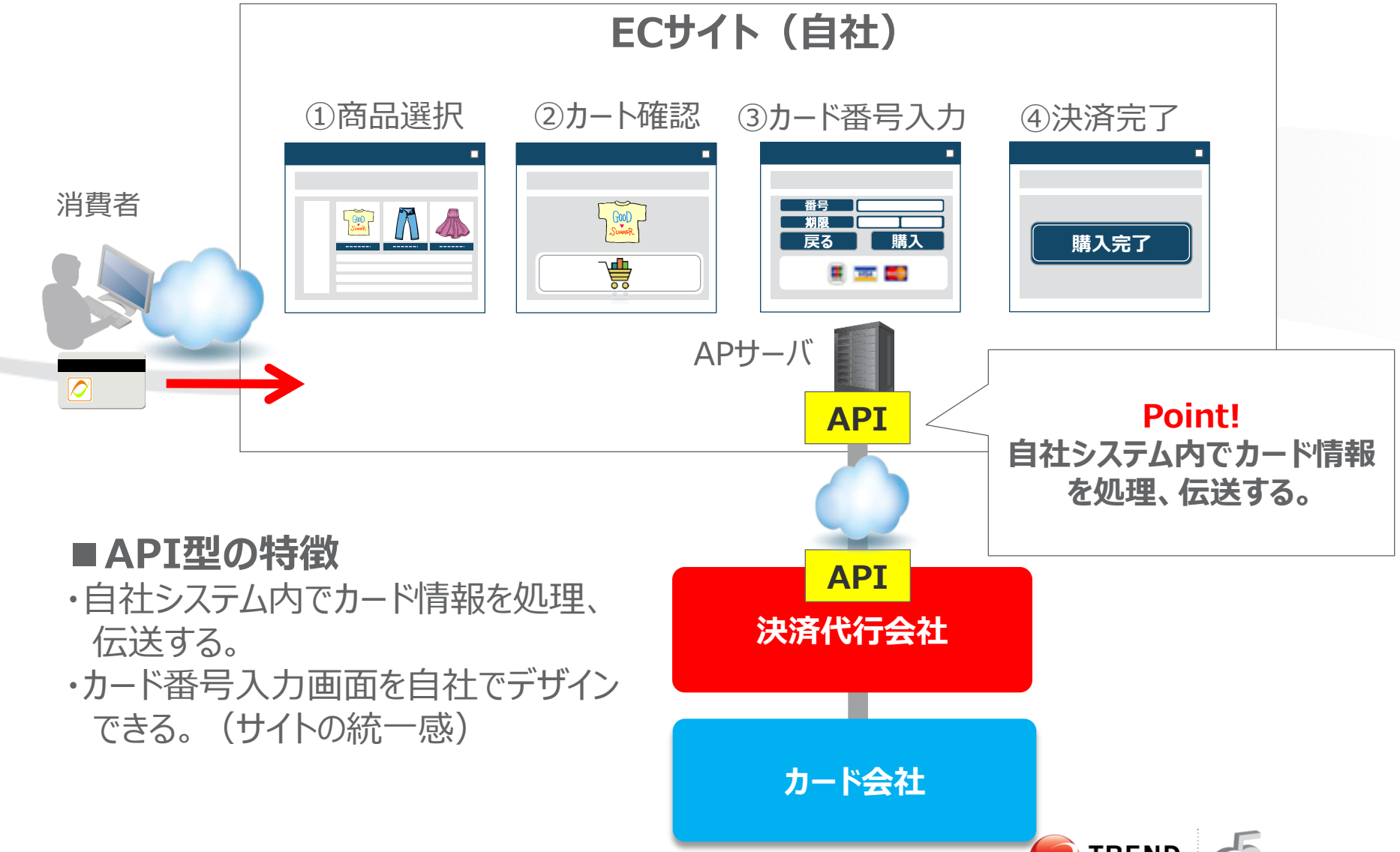
ECサイトの２つ（細かくは３つ）の決済形態

形態	カード情報の扱い（自社システム内）			特徴
	処理	伝送	保持	
①API型	する	する	する	・決済画面も含めて、自社で画面をデザインできる。 ・カード情報を保持しないケースが殆ど。但し、保持しなくても漏えいするリスクはある。
	する	する	しない	
②リンク型	しない	しない	しない	・決済画面は、決済代行会社の画面になる。 ・自社システムでカード情報は扱わないが、リダイレクト先を改ざんされた場合などは漏えいのリスクがある。

8割以上のECサイトが非保持を選択している（※）

※http://www.meti.go.jp/meti_lib/report/2011fy/E001269.pdf
→p77参照

①API型：処理の流れ



■API型の特徴

- 自社システム内でカード情報を処理、伝送する。
- カード番号入力画面を自社でデザインできる。（サイトの統一感）

②リンク型：処理の流れ

Point!
自社システム内でカード情報を扱わない
（処理、伝送、保管をしない）

■リンク型の特徴

・自社システム内でカード情報を扱わない。
・カード番号入力画面が決済代行会社の画面になる。

決済形態別のPCIDSS要件

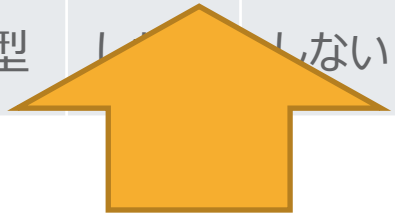
形態	カード情報の扱い（自社システム内）			コントロール数（※）	備考
	処理	伝送	保持		
①API型	する	する	する	300	PCIDSSフルセット
	する	する	しない	80	ウイルス対策、脆弱性スキャンなどが必要
②リンク型	しない	しない	しない	13	セキュリティ規程が求められる程度

非保持の場合のPCIDSS要件が存在するため、
該当するEC事業者には参考になる・・・が
これで十分なのか？

※ https://ja.pcisecuritystandards.org/minisite/en/saq-v2.0-documentation.php
- 約300のコントロール：SAQ D v2.0
- 80のコントロール：SAQ C v2.0
- 13のコントロール：SQQ A v2.0

当該サイトの決済形態

形態	カード情報の扱い（自社システム内）			コントロール数	備考
	処理	伝送	保持		
①API型	する	する	する	300	PCIDSSフルセット
	する	する	しない	80	ウイルス対策、脆弱性スキャンなどが必要
②リンク型	[illegible]	しない	しない	13	セキュリティ規程が求められる程度



当該サイトはこの形態

- カード情報は一切持っていない
- アプリケーションプログラムを改ざんされた

①API型の要件:カード情報保持(300項目)

	文書	実装		運用	
アプリ DB	開発基準 暗号鍵の管理手順	セキュアコーディング カード番号のマスク センシティブ認証データ非保持	カード情報暗号化(保管)	コードレビュー(随時) 随時のWebアプリ診断 or WAF	暗号鍵の更新(定期的)
サーバ PC NW	構成基準 NW構成図 構成定義書 FWのルールセット	ウイルス対策 変更監視 ステートフルFW DMZ・NAT IPスプーフィング IDS/IPS セキュアリモートログイン	WAF or 随時のWebアプリ診断 二因子認証(リモートアクセス時) 時刻同期 パーソナルFW 要塞化	脆弱性スキャン(四半期に1回以上) FWルールレビュー(半年に1回以上)	無線LAN検査(四半期に1回以上)
共通	セキュリティ規程 委託先管理手順 変更管理手順 アカウント管理手順 運用管理手順	アクセス制御 ログ取得 集中ログ管理 パスワードポリシー デフォルトID/Pass変更	パスワード暗号化(伝送、保管) カード情報暗号化(伝送)	パッチ適用(重要→1カ月以内) アカウント管理(随時) 変更管理(随時) ログレビュー(1日1回以上) ペネトレーションテスト(年1回以上)	リスク評価(年1回以上) 委託先評価(年1回以上) 事業継続訓練(年1回以上) 規程類見直し(年1回以上) セキュリティ教育(年1回以上)
物理	入退館規程	監視カメラ or 入退管理システム	クロスカットシュレッダー データ消去ソフト	入退室記録(随時) ゲストカード着用(随時)	バックアップ媒体確認(年1回以上)

②API型の要件：カード情報非保持（80項目）

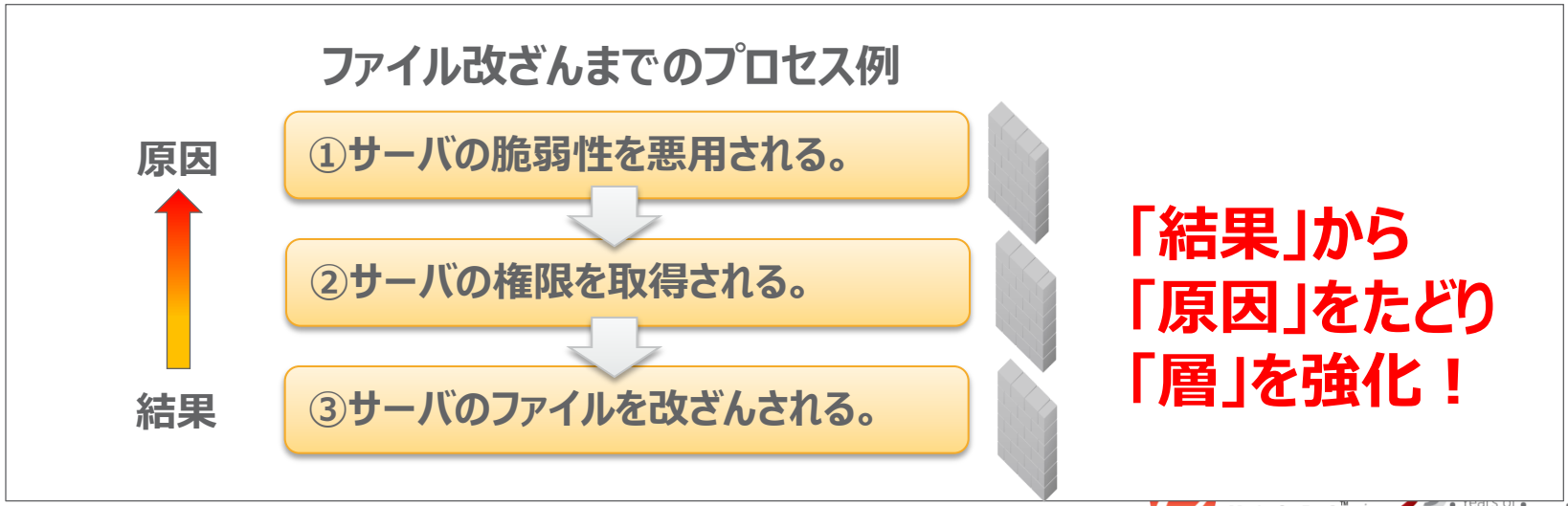
	文書	実装		運用	
アプリ DB	開発基準 暗号鍵の管理手順	セキュアコーディング カード番号のマスク センシティブ認証データ非保持	カード情報暗号化（保管）	コードレビュー（随時） 随時のWebアプリ診断 or WAF	暗号鍵の更新（定期的）
サーバ PC NW	構成基準 NW構成図 構成定義書 FWのルールセット	ウイルス対策 変更監視 ステートフルFW DMZ・NAT IPスプーフィング IDS/IPS セキュアリモートログイン	WAF or 随時のWebアプリ診断 二因子認証（リモートアクセス時） 時刻同期 パーソナルFW 要塞化	脆弱性スキャン（四半期に1回以上） FWルールレビュー（半年に1回以上）	無線LAN検査（四半期に1回以上）
共通	セキュリティ規程 委託先管理手順 変更管理手順 アカウント管理手順 運用管理手順	アクセス制御 ログ取得 集中ログ管理 パスワードポリシー デフォルトID/Pass変更	パスワード暗号化（伝送、保管） カード情報暗号化（伝送）	パッチ適用（重要→1カ月以内） アカウント管理（随時） 変更管理（随時） ログレビュー（1日1回以上） ペネトレーションテスト（年1回以上）	リスク評価（年1回以上） 委託先評価（年1回以上） 事業継続訓練（年1回以上） 規程類見直し（年1回以上） セキュリティ教育（年1回以上）
物理	入退館規程	監視カメラ or 入退管理システム	クロスカットシュレッダー データ消去ソフト	入退室記録（随時） ゲストカード着用（随時）	バックアップ媒体確認（年1回以上）

②リンク型の要件（13項目）

	文書	実装		運用	
アプリ DB	開発基準 暗号鍵の管理手順	セキュアコーディング カード番号のマスク センシティブ認証データ非保持	カード情報暗号化（保管）	コードレビュー（随時） 随時のWebアプリ診断 or WAF	暗号鍵の更新（定期的）
サーバ PC NW	構成基準 NW構成図 構成定義書 FWのルールセット	ウイルス対策 変更監視 ステートフルFW DMZ・NAT IPスプーフィング IDS/IPS セキュアリモートログイン	WAF or 随時のWebアプリ診断 二因子認証（リモートアクセス時） 時刻同期 パーソナルFW 要塞化	脆弱性スキャン（四半期に1回以上） FWルールレビュー（半年に1回以上）	無線LAN検査（四半期に1回以上）
共通	セキュリティ規程 委託先管理手順 変更管理手順 アカウント管理手順 運用管理手順	アクセス制御 ログ取得 集中ログ管理 パスワードポリシー デフォルトID/Pass変更	パスワード暗号化（伝送、保管） カード情報暗号化（伝送）	パッチ適用（重要→1カ月以内） アカウント管理（随時） 変更管理（随時） ログレビュー（1日1回以上） ペネトレーションテスト（年1回以上）	リスク評価（年1回以上） 委託先評価（年1回以上） 事業継続訓練（年1回以上） 規程類見直し（年1回以上） セキュリティ教育（年1回以上）
物理	入退館規程	監視カメラ or 入退管理システム	クロスカットシュレッダー データ消去ソフト	入退室記録（随時） ゲストカード着用（随時）	バックアップ媒体確認（年1回以上）

必要となる対策

- 「非保持でも漏えいする」、という認識を持つ
- ポリシーの見直し
  - 規格依存ではなく、リスクベースのアプローチをとる
  - 脆弱性管理のプロセスを見直す（ソフトの棚卸、作業範囲、SLAなど）
  - 内部からの脅威への対策も視野に入れる
- システム的な対策、運用の見直し
  - PCIDSS（300項目）のコントロール（多層防御）を参考にする
  - **その中でも重要となる「３つの層」を強化する**



「３つの層」の強化例
（弊社製品の場合）

PCI DSS準拠に必要なサーバ保護機能を1つのエージェントで実装した Trend Micro Deep Security

OSやアプリケーションの
脆弱性を保護

DoS攻撃など
不正な通信を防御

OSやミドルウェアのセキュリティイベントを
集中監視

IPS/IDS
Webアプリケーション保護

ファイアウォール

ウイルス対策

セキュリティログ監視

変更監視

SQLインジェクション等の攻撃から
らWebアプリを保護

リアルタイムに
ウイルスを検索

ファイルやレジストリ等の
変更を監視

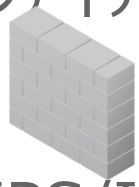
物理サーバ　仮想サーバ　クラウド上のサーバ　デスクトップの仮想化

TREND MICRO

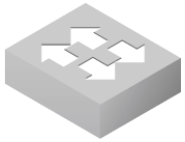
25 Years of inspiration

オールインワンタイプの
サーバセキュリティソフトウェア

- ファイアーウォール



- IPS/IDS



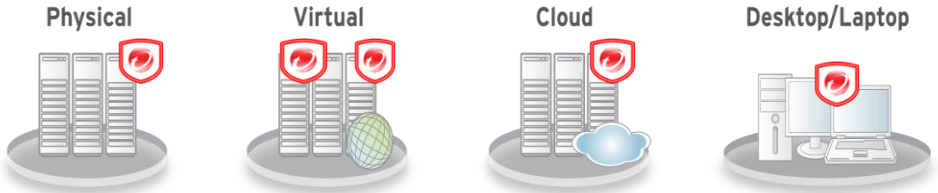
- Web Application Firewall

- 改ざん検知

- ウイルス対策

Trend Micro

Deep Security™



TREND MICRO 25 Years of inspiration

Deep Security で準拠支援できる PCI-DSS 準拠項目に対する具体的な運用方法例（1/2）

☑ (1.x)データを保護するためにファイアウォールの導入をし、最適な設定を維持すること

⇒ Deep Security が提供するファイアウォール機能を利用することで当該項目への準拠

☑ (2.x)システムまたはソフトウエアの出荷時の初期設定値（セキュリティに関する設定値）をそのまま利用しないこと

⇒ Deep Securityマネージャによるアカウント管理による準拠

☑ (5.x)アンチウィルスソフトウェアまたはプログラムを使用し、定期的に更新すること

⇒ ウイルス対策機能による不正プログラムの侵入検知

☑ (6.x)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

⇒ Deep Packet Inspection (IDS/IPS) の仮想パッチ機能による該当項目の準拠

Deep Security で準拠支援できる PCI-DSS 準拠項目に対する具体的な運用方法例（2/2）

☑ (10.6)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

⇒ **Deep Securityマネージャのログ分析機能による該当項目の準拠**

☑ (11.4)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

⇒ **Deep Packet Inspection (IDS/IPS)及びファイル・レジストリ変更監視機能による該当項目の準拠**

☑ (12.x)情報セキュリティに関するポリシーを整備すること

⇒ **Deep SecurityマネージャのSIEMとの連携機能による該当項目の準拠**

１つめの層の強化

- ファイル改ざんまでのプロセス例

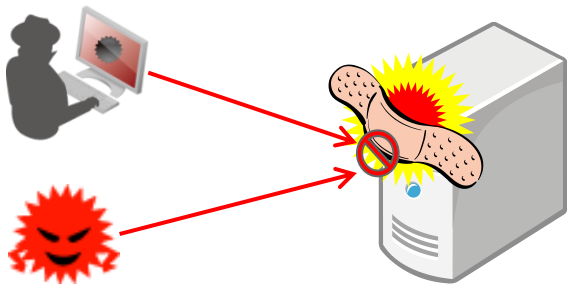
対策優先度
高
低

①サーバの脆弱性を攻撃される。
②サーバの権限を取得される。
③サーバのファイルを改ざんされる。

【課題】
・パッチの適用が適切に行えない。
【理由】
・適用前にシステムの検証が必須。
・適用時にはシステムを止める必要がある場合もある。

仮想パッチで運用を軽減

- 仮想パッチとは、仮想的に脆弱性を修正するプログラム
  - 自動、または手動で仮想パッチを適用
  - 脆弱性を悪用した攻撃を受けた場合は、仮想パッチが攻撃をブロック
  - 仮想パッチを適用するためにサーバを停止、再起動する必要がない



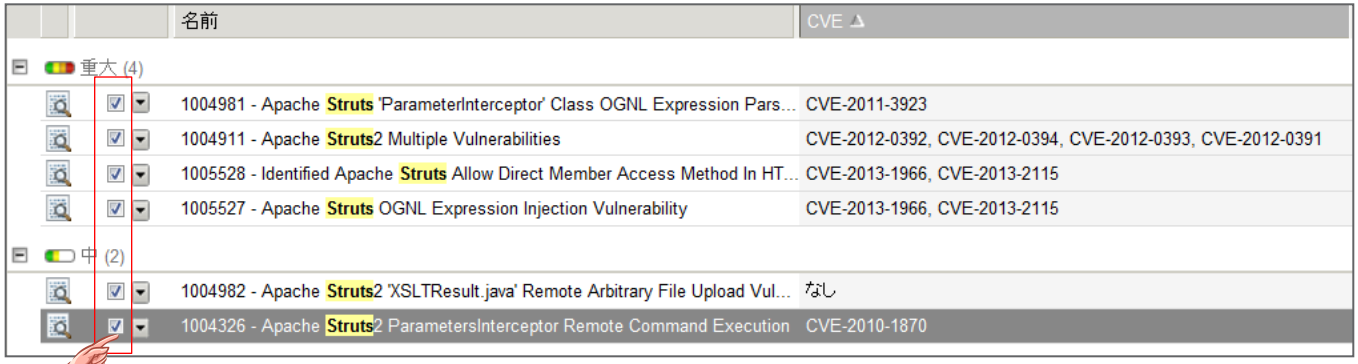
OSやアプリケーションの脆弱性を突いた攻撃をネットワークレベルでブロック
（本来のパッチ検証作業を十分に行ってからパッチの適用が可能となる）

（参考）仮想パッチの適用

例１）手動で仮想パッチを適用

①使用しているソフトの名称等で仮想パッチを検索

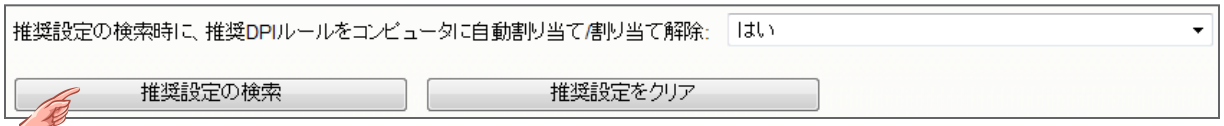
※以下は2013/6/28現在で対応しているStrutsの仮想パッチ



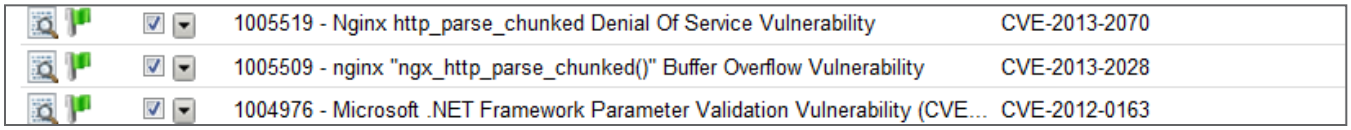
②チェックして仮想パッチを適用

例２）自動で仮想パッチを適用

①自動割り当ての設定を有効化



②推奨設定の検索を実行（サーバ上で適用を推奨するパッチを検索）



③自動的にパッチを適用（フラグは適用を推奨するパッチを意味する）

２つめの層の強化

- ファイル改ざんまでのプロセス例

対策優先度
高
低

①サーバの脆弱性を攻撃される。

②サーバの権限を取得される。

③サーバのファイルを改ざんされる。

【課題】
・不正なログイン試行に気づかない。

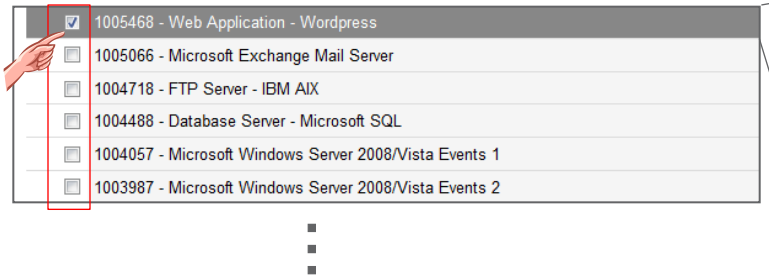
セキュリティログ監視で対応

- 攻撃の兆候があった場合はすぐに管理者へ通知する
  - OS/ミドルウェア/アプリのデフォルトID/パスワードの変更、パスワードポリシー強化、適切な権限設定を実施した上で、アクセスを監視
  - 疑わしいふるまい（認証試行、ポリシー違反、サーバエラーなど）を検知した場合は速やかに管理者へ通知

（参考）セキュリティログ監視の設定

例１）手動で監視ルールを適用

①監視対象を選択

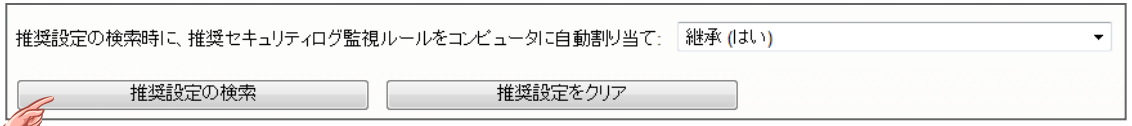


②監視ルールを定義（下記はWordPressの例）

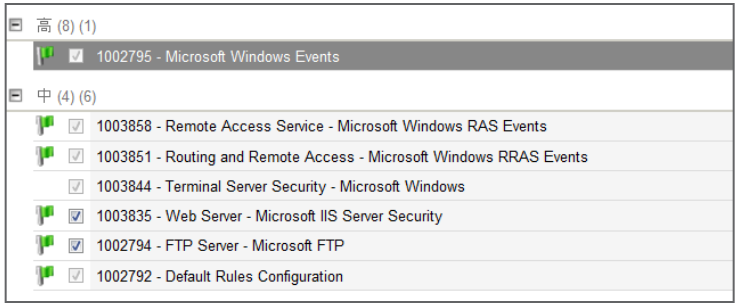
③重要度に応じて管理者へ通知
（メール、管理コンソール等）

例2）自動で監視ルールを適用

①自動割り当ての設定を有効化



②推奨設定の検索を実行（サーバ上で監視を推奨するルールを検索）



③自動的に監視ルールを適用
（フラグは推奨するルールを意味する）

３つめの層の強化

- ファイル改ざんまでのプロセス例

対策優先度
高
低

①サーバの脆弱性を攻撃される。

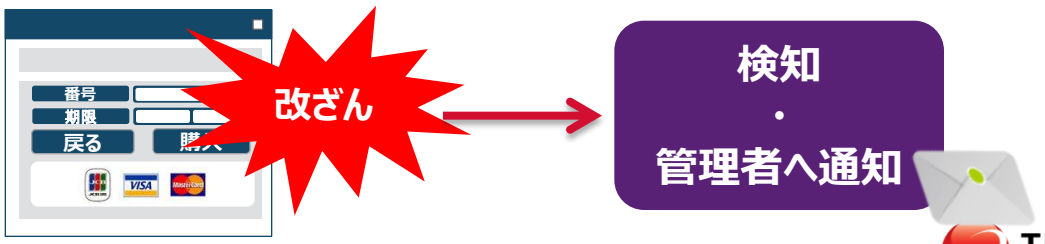
②サーバの権限を取得される。

③サーバのファイルを改ざんされる。

【課題】
・ファイルの改ざんに気づかない

変更監視で対応

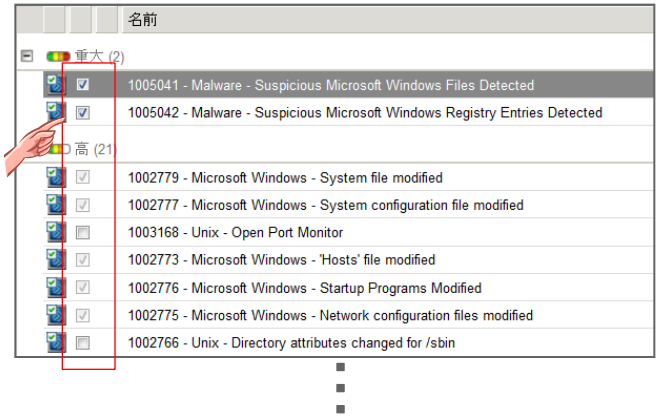
- 改ざんを検知した場合はすぐに管理者へ通知する
  - **Webコンテンツ/プログラム、構成及びパラメータファイル、アプリケーション実行可能ファイル、システム実行可能ファイル、レジストリの変更を監視**
  - 変更（バックドア設置、ファイル変更など）を検知した場合は管理者へ通知
  - 本番環境に対するシステム変更管理のプロセスを整備しておくことが望ましい



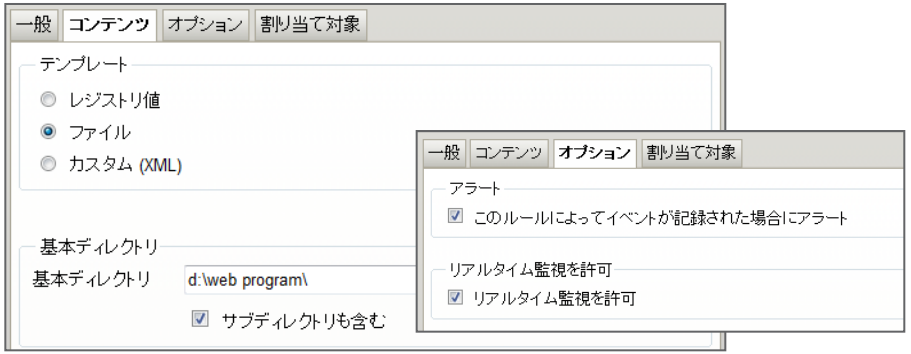
（参考）変更監視の設定

例１）手動で監視ルールを適用

①検知対象を選択



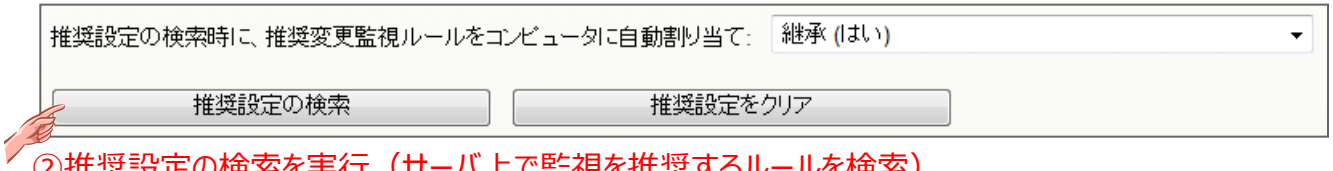
②Webコンテンツやプログラムは個別に監視ルールを作成



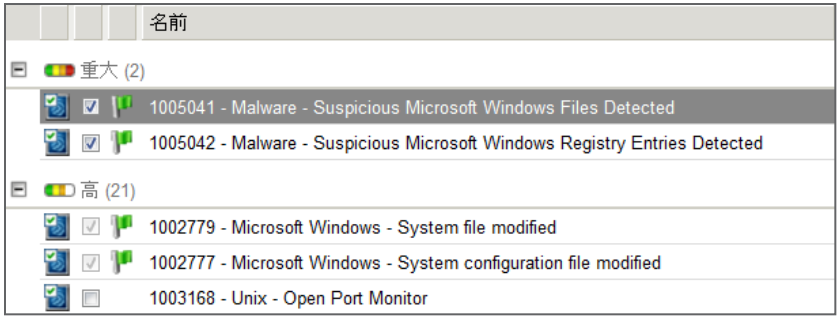
③重要度に応じて管理者へ通知
（メール、管理コンソール等）

例2）自動で監視ルールを適用

①自動割り当ての設定を有効化



②推奨設定の検索を実行（サーバ上で監視を推奨するルールを検索）



③自動的に監視ルールを適用
（フラグは推奨するルールを意味する）

テレコムクレジット株式会社様
PCI DSS準拠の為のセキュリティツール導入

TELECOM CREDIT
テレコムクレジット株式会社

- お客さまの要望：

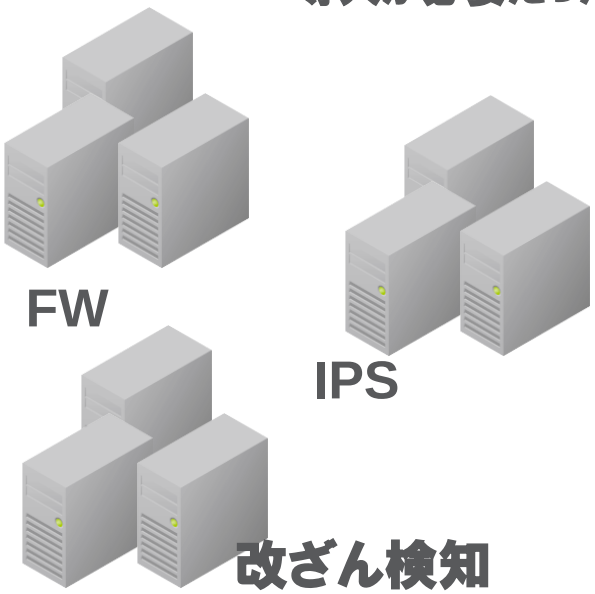
  PCI DSS準拠の為のセキュリティツールを検討

- 評価のポイント：仮想パッチ、推奨スキャン、統合管理

  5つの機能を1つの製品で実装しているため複数のセキュリティ製品を購入する必要が無く、コストが削減できた。

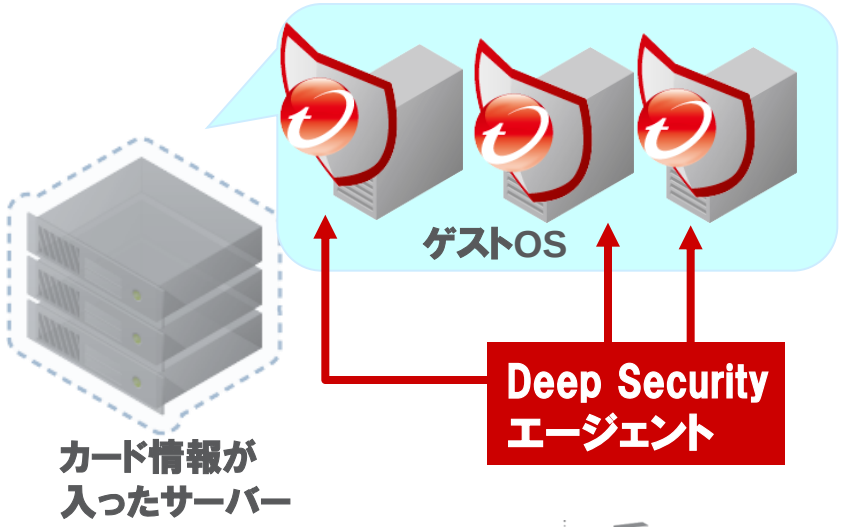
従来

複数のセキュイリティ製品の導入が必要だった



今後

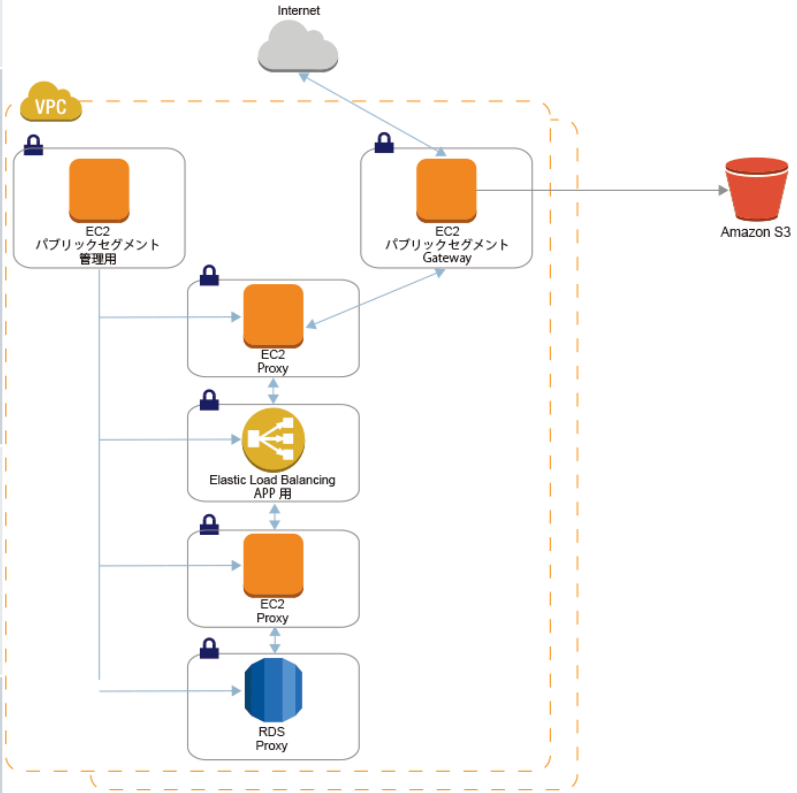
Deep SecurityでPCI DSS 7項目に準拠できた



TREND MICRO
25 Years of inspiration

コイニー株式会社

項目	内容
導入ソリューション	cloudpackオプションサービス「セキュリティ+　Deep Security」
業種	クレジットカード決済代行
採用理由	● PCI DSSに対応するためのネットワーク構築、CentOSをベースに、Trend Micro社のDeep Securityを採用。本番環境での設計～実装を、cloudpack社のサポートを得て行い、2012年11月～12月の約1ヶ月間で完了
導入によって得られたメリット	● PCI DSSに準拠するためのセキュリティ製品コストの低減 ● Cloudpack社からのサービス提供
導入時期	● 2012年12月（導入済み）



まとめ “早く”、“安く”、“手戻りなく”

- 早く
  - 増え続けるサイト改ざん、成りすます攻撃被害に素早く対応
- 安く
  - 購入するセキュリティ製品を極力少なく、管理コストも抑える
- 手戻りなく
  - =“前の状態に戻って、もう一度その作業をやり直すこと”
  - 何度も審査を受けない（一発合格！）

PCIDSS準拠支援ツール

Trend Micro Deep Security

を是非ご検討ください。

TREND MICRO™

25 Years of inspiration

ご清聴ありがとうございました。