tripwire
CONFIDENCE: SECURED

情報セキュリティ新時代に向けての備えと取組みの考察

～ Tripwire の考える最先端のサイバーセキュリティ対策と実例 ～

トリップワイヤ・ジャパン株式会社

トリップワイヤ・ジャパン　会社概要

本社：米国オレゴン州ポートランド　1997年設立
トリップワイヤ・ジャパン株式会社　2000年設立
（100%出資の子会社）

導入実績：世界約90カ国 7,000社
- Fortune 500社の 43%が顧客

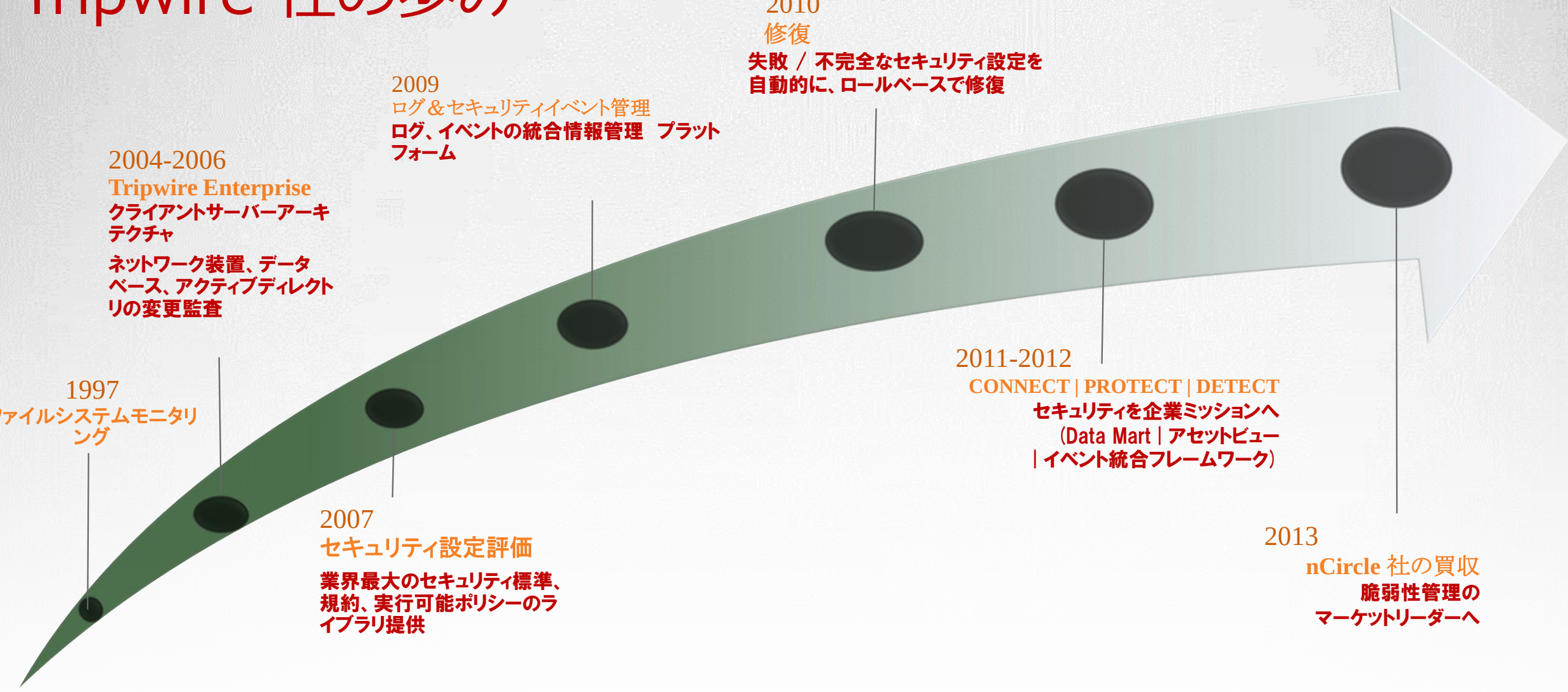
導入実績：日本 1,000社（官公庁・一般企業・etc）
- IPAウェブサイトでWeb改ざん検知製品として紹介

✓変更検知に特化して15年
✓変更検知のパイオニアであり、デファクトスタンダード
→　No.1 のマーケットシェア
→　実績による安定性と信頼

SC MAGAZINE AWARDS 2012 Honored in the U.S. WINNER Best Policy Management Solution

SC MAGAZINE AWARDS 2011 Honored in the U.S. WINNER Best Enterprise Security Solution

Tripwire 社の歩み



1997
ファイルシステムモニタリング

2004-2006
Tripwire Enterprise
クライアントサーバーアーキテクチャ
ネットワーク装置、データベース、アクティブディレクトリの変更監査

2007
セキュリティ設定評価
業界最大のセキュリティ標準、規約、実行可能ポリシーのライブラリ提供

2009
ログ＆セキュリティイベント管理
ログ、イベントの統合情報管理　プラットフォーム

2010
修復
失敗 / 不完全なセキュリティ設定を自動的に、ロールベースで修復

2011-2012
CONNECT | PROTECT | DETECT
セキュリティを企業ミッションへ
（Data Mart | アセットビュー | イベント統合フレームワーク）

2013
nCircle 社の買収
脆弱性管理のマーケットリーダーへ

セキュリティを企業ミッションへ

原文: CSTB --- *“Connect Security to The Business”*

CISO,
情報システム統括責任者
“知識、経験” レベル

CONNECT

セキュリティの可視化、定量化、アクションアイテム化

- 経営会議へのレポーティング
- リスクのスコアリング
- セキュリティの可視化

セキュリティ部門長,
セキュリティアーキテクト
“情報” レベル

PROTECT

組織を動かす原動力となるシステムを様々な脅威から保護

- 継続的モニタリング
- システムの要塞化
- 除外対象／例外処理マネジメント
- 構成検査の自動化
- 遵守ポリシーの適用＆カスタマイズ
- ワークフロー＆修復プロセス確立

セキュリティアナリスト
“データ” レベル

DETECT

企業の日々のビジネスを阻害する行為の先行指標を検知

- 広範なデバイス、OS、ミドルウェアのサポート
- システム統合・連携
- ファイル＆システムの整合性監視
- ログ収集分析
- 自動修復
- 変更検知ルール／ベースライン

企業ミッションとしての取組みを阻害する要因

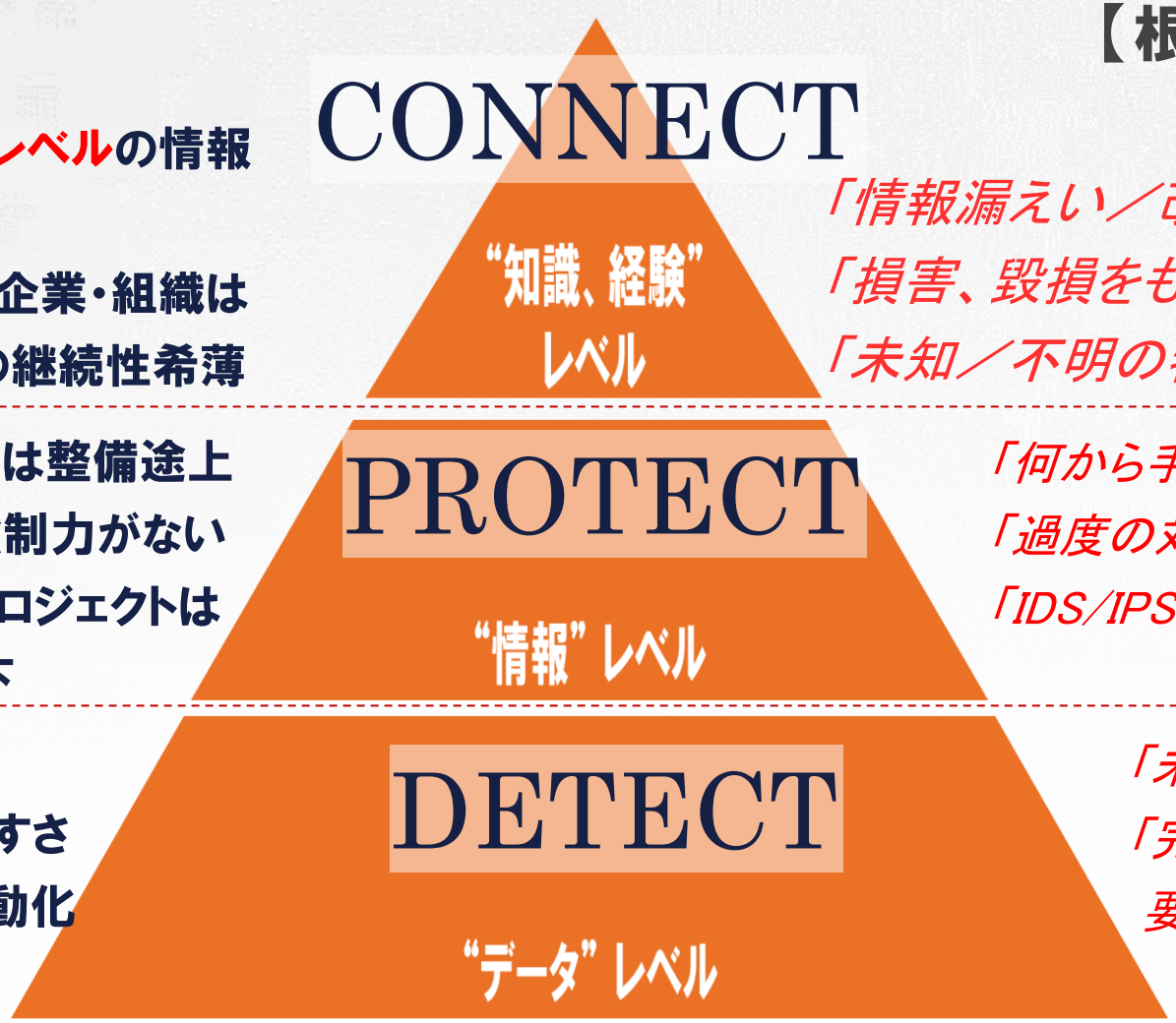
【現状】

- 企業／組織の KPI に**リスクレベル**の情報セキュリティ指標がない
- CISO アサイン, CSIRT 設立企業・組織は未だ少数に留まり、取組みの継続性希薄

- 情報セキュリティ関連法規制は整備途上
- 公的機関のガイドラインに強制力がない
- 情報セキュリティ単独要件プロジェクトは全 IT プロジェクトの 1% 以下

【重視される要件】

- データの見やすさ、分かりやすさ
- オペレーションの簡素化・自動化
- インシデント対応の即時性



【根底にあるもの】

「情報漏えい／改ざんで人が死ぬことはない」
「損害、毀損をもたらしても 100% 責任はない」
「未知／不明の物への多大な投資理由がない」

「何から手を付けていいか分からない」
「過度の対策で利便性／業務効率が低下」
「IDS/IPS 導入、外部診断で対策は十分」

「未知の脅威への追従が困難」
「完全性よりも運用の効率性が強く要求される」

企業ミッションを部門レベルで共有し「強い組織」作り

日本のお家芸:「安全衛生目標管理」のやり方を活かす

キーワードは “JK” と “KY”

PCI DSS 改訂の要旨 (v2.0 → v3.0)

BSI グループジャパン株式会社様のホームページ (http://www.bsigroup.jp) より

- **認証範囲（スコーピング）の明確化**
- **新要件（メモリ上のカード番号、POS端末の保護等）**
- **実務に配慮した要件の柔軟化　他**

Ver. 2.0

要件	内容
6.6	「Webアプリケーションファイアウォール」をインストールする
11.5	ファイル整合性監視ツールを導入すること
12.3.4	デバイスへの所有者、連絡先情報、目的を記載したラベルの添付

Ver. 3.0

要件	内容
6.6	「自動化された技術的ソリューション」をインストールする
11.5	変更検知メカニズムを導入すること（例：ファイル整合性監視ツール）
12.3.4	所有者、連絡先情報、目的を正確かつ容易に判別できる方法（例．ラベルの添付、コード情報の添付と装置台帳の組合せ）

解決手段を一意に明確化せず
- **今後の技術革新への対応**
- **継続的な改善促進**

PCI DSS 要件	テスト手順	ガイドライン
1.3.1 DMZ を実装し、誰でもアクセス可能な承認済みのサービス、プロトコル、ポートを提供するシステムコンポーネントにのみ着信トラフィックを制限する。	1.3.1 ファイアウォール、及びルータの構成ファイルを調査し、DMZ が実装され、誰でもアクセス可能な承認済みのサービス、プロトコル、ポートを提供するシステムコンポーネントにのみ着信トラフィックが制限されていることを確認する。	DMZは、インターネット（またはその他の信頼できないネットワーク）と組織が公開する必要がある内部サービス（Webサーバなど）との間の接続を管理するネットワークの一部です。内部ネットワークと通信する必要があるトラフィックをそうで フィックから分離して隔離する、防御 （以下略）

実践手順をより具体化

評価指標の提示

Tripwire ソリューションによる PCI DSS 要件カバレッジ

要件10, 11 だけでなく整合性監視／ポリシー可視化により PCI DSS の要件を広くカバー

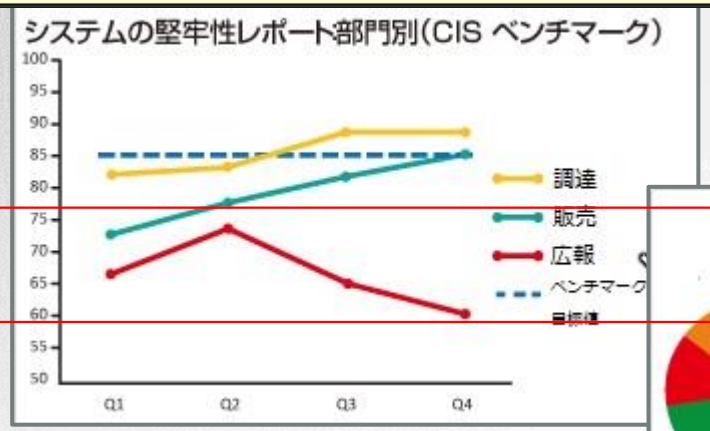
安全なネットワークの構築と維持	
要件1	カード会員データを保護するために、ファイアウォールをインストールして構成を維持する
要件2	システムパスワードおよび他のセキュリティパラメータにベンダ提供のデフォルト値を使用しない
カード会員データの保護	
要件3	保存されるカード会員データを保護する
要件4	オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する
脆弱性管理プログラムの整備	
要件5	アンチウィルスソフトウェアまたはプログラムを使用し、定期的に更新する
要件6	安全性の高いシステムとアプリケーションを開発し、保守する
強固なアクセス制御手法の導入	
要件7	カード会員データへのアクセスを、業務上必要な範囲内に制限する
要件8	コンピュータにアクセスできる各ユーザに一意のIDを割り当てる
要件9	カード会員データへの物理アクセスを制限する
ネットワークの定期的な監視およびテスト	
要件10	ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する
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
情報セキュリティ・ポリシーの整備	
要件12	すべての担当者の情報セキュリティポリシーを整備する

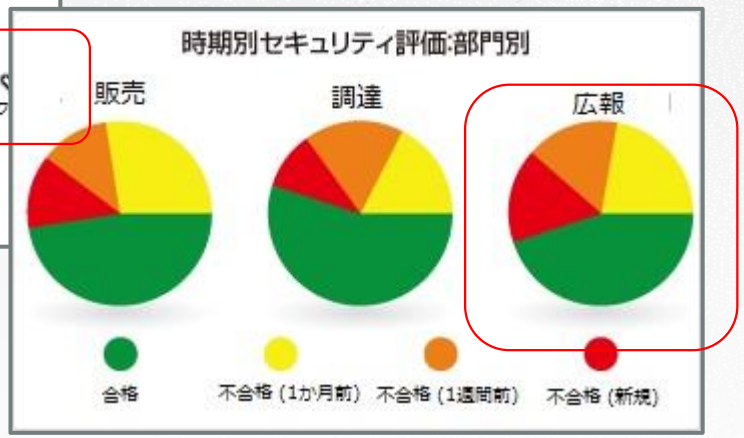
2014年7月
v3.0 対応ルール／
ポリシーテンプレート
をいち早く公開

「PCI データセキュリティ基準 v2.0　2010年10月」より抜粋

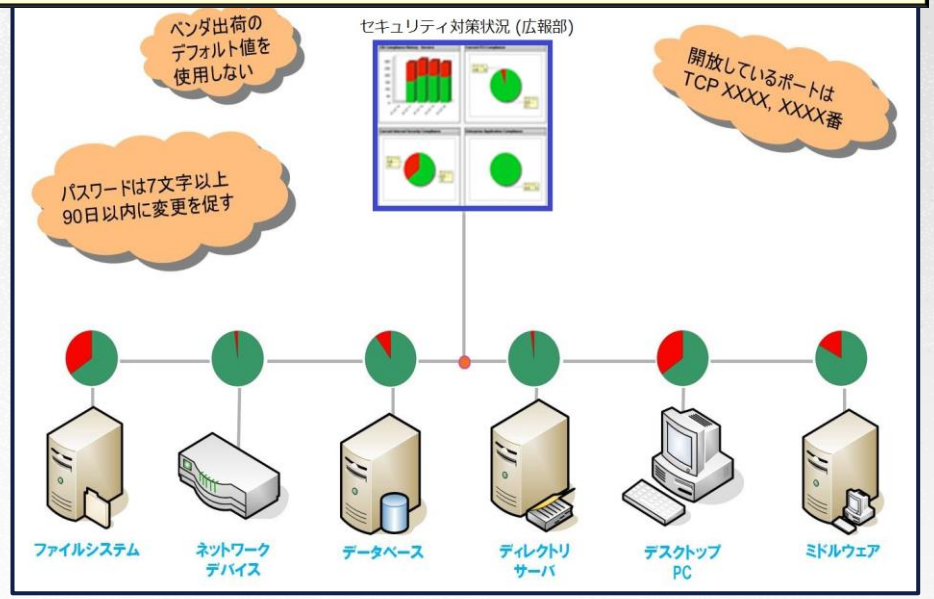
目標共有のためのセキュリティ・インテリジェンス構築

組織全体のコンプライアンス順守状況を定期的にスコアリングして定量化





問題のある部門、ポイントを特定し、改善へのガイダンスを提示＋改善状況を追跡



セキュリティ・コンプライアンス　データハブ

企業・組織内の IT 資産ネットワーク（オンプレミス＆クラウド）

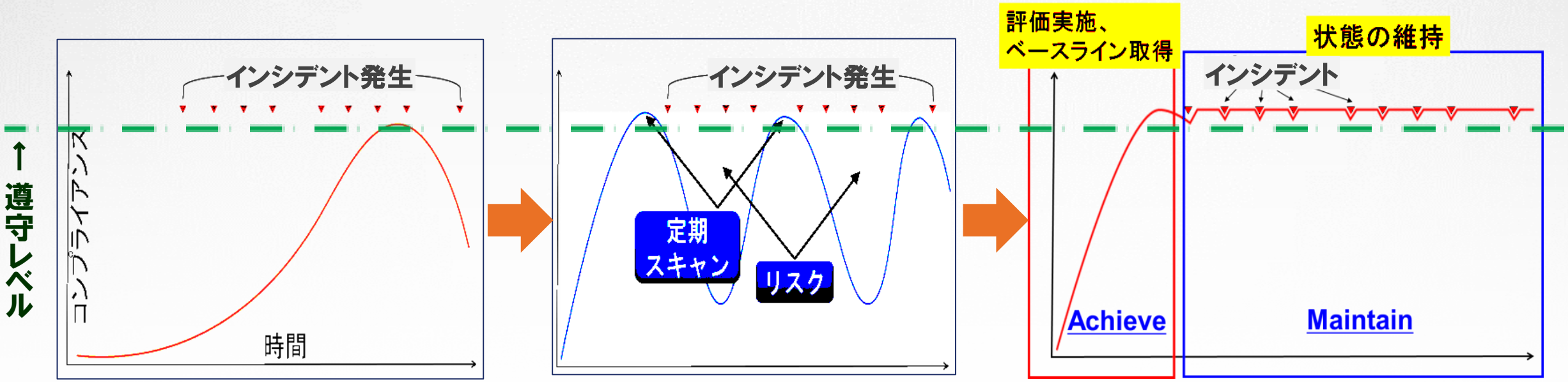
日々の改善活動のレベルを継続的に維持するツール導入＆レベル向上

- 単発的な 100 点満点を目指さず、達成可能な改善目標を適宜設定してツールによる自動化／効率化を実施
- 起ってしまったインシデントへの事後対応迅速化 (イベント駆動型 / 発見的統制)
  → インシデントの起らない仕組みの設計・インシデントの要因特定 (リスク駆動型 / 予防的統制) へ

Lv.1. マニュアル作業
(PCI 認定取得等)

Lv.2. ツール導入
(外部委託型／イベント駆動型)

Lv.3. ツール導入
(内製継続型／リスク駆動型)



リスク因子として「脆弱性」に特化する理由

【昨今の状況】

- 昨今のサイバー攻撃事例の 95% 以上が、脆弱性を突いたもので占められている
- 対外常駐サーバー／機密データソースへの直接的な攻撃に加え、内部からの回り込み・伝搬も常態化
- その中でも、Adobe, Java 他のクライアントソフトの脆弱性をついた攻撃が常套手段化
  - 脆弱性診断を実施し、その結果に基づきセキュリティホールを塞ぐことで被害を未然に防止
  - 定期的な脆弱性診断の実施状況を開示し、企業自身や、製品／サービスの信頼性を向上

【意識／実際とのギャップ】

- 検出される脆弱性の量と出処が多すぎて、即対応に踏み切れない／優先度付ができない
- そもそも脆弱性の出処となる IT 資産全体の所在／管理状況を把握できていない
- 結果として、既知の脆弱性はますます対応しにくく／狙われやすくなる
  - 2012年の統計では**99.8%が既知の脆弱性を悪用**
  - Adobe Readerの更新は、**45%のユーザしか対応していない状況**

→ 脆弱性診断 (定期的な実施→改善策提示→終り) から
脆弱性管理 (発見→分析→対応→評価) へ

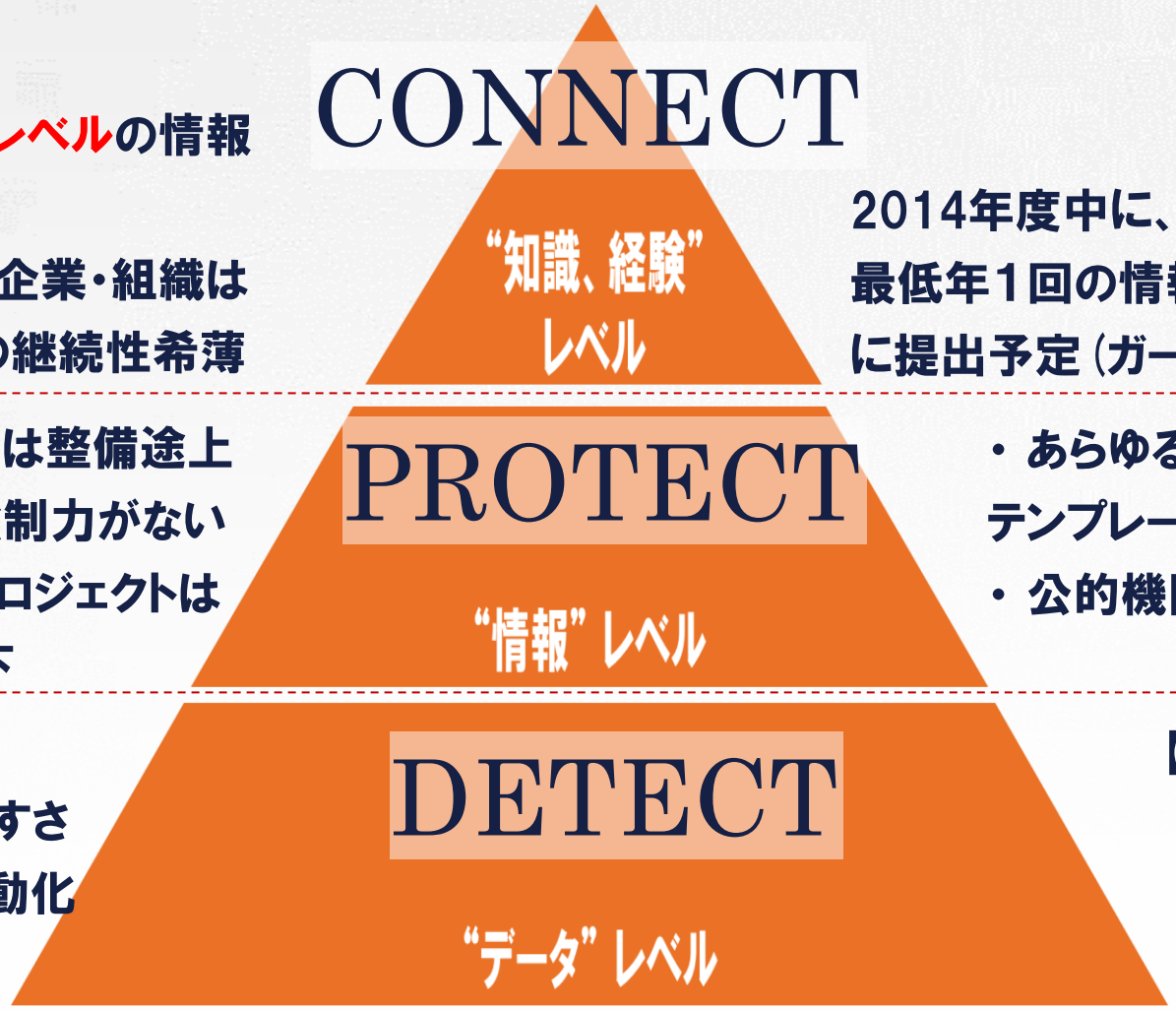
日本 vs 諸外国の取組状況差異

【日本】

- 企業／組織の KPI にリスクレベルの情報セキュリティ指標がない
- CISO アサイン, CSIRT 設立企業・組織は未だ少数に留まり、取組みの継続性希薄

- 情報セキュリティ関連法規制は整備途上
- 公的機関のガイドラインに強制力がない
- 情報セキュリティ単独要件プロジェクトは全 IT プロジェクトの 1% 以下

【重視される要件】
- データの見やすさ、分かりやすさ
- オペレーションの簡素化・自動化
- インシデント対応の即時性



【諸外国】

2014年度中に、グローバル企業／組織の 80% が、最低年１回の情報セキュリティ・リスクレポートを経営陣に提出予定（ガートナー ‘12）

- あらゆる業界で、法規制→ガイドライン→IT テンプレート実装までの流れを一貫工程で整備
- 公的機関が実装仕様まで関与（SCAP 等）

【重視される要件】
- データの永続性、網羅性、多面性
- オペレーションの完全性、共有化
- インシデントの予防性、初動性

SCAP (Security Content Automation Protocol)

情報セキュリティ遵守目標と、IT による実装要件の橋渡し

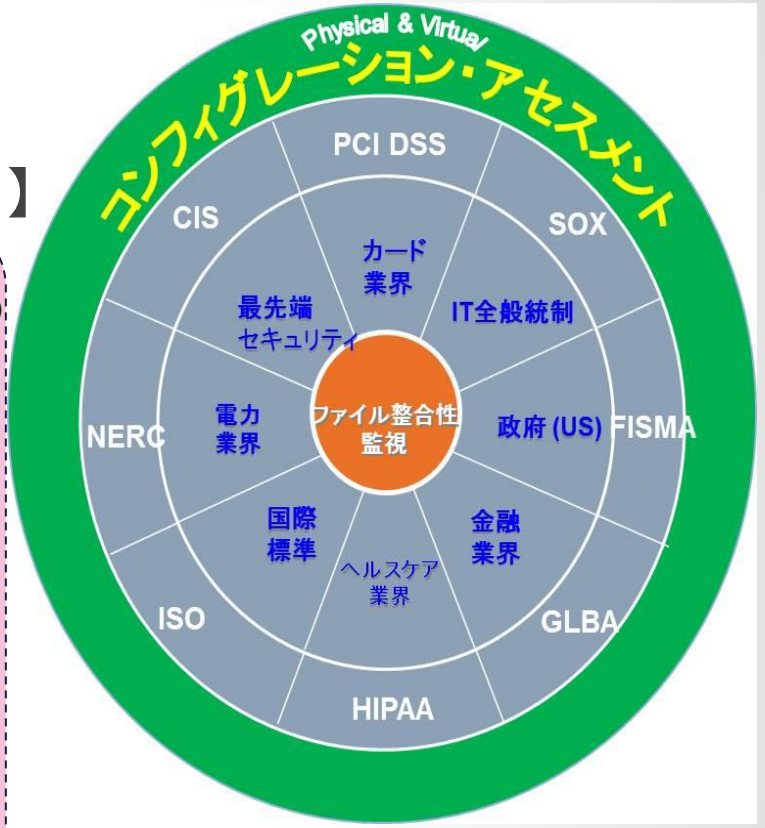
【SCAP の構成要素】

1. 脆弱性を識別するためのCVE
（Common Vulnerabilities and Exposures：共通脆弱性識別子）
2. セキュリティ設定を識別するためのCCE
（Common Configuration Enumeration：共通セキュリティ設定一覧）
3. 製品を識別するためのCPE
（Common Platform Enumeration：共通プラットフォーム一覧）
4. 脆弱性の深刻度を評価するためのCVSS
（Common Vulnerability Scoring System：共通脆弱性評価システム）
5. チェックリストを記述するためのXCCDF
（eXtensible Configuration Checklist Description Format：セキュリティ設定チェックリスト記述形式）
6. 脆弱性やセキュリティ設定をチェックするためのOVAL
（Open Vulnerability and Assessment Language：セキュリティ検査言語）

【Tripwire での活用】

法規制／プロトコルの実装

共通仕様による 3rd パーティ連携



情報処理推進機構 (IPA) ホームページ: 「セキュリティ設定共通化手順SCAP概説」より

Tripwire のソリューションラインナップ

セキュリティの企業ミッション化を強力に支援

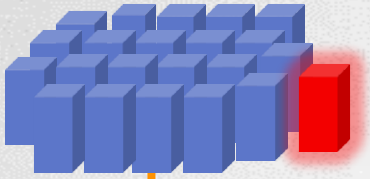
- **システム設定とモニタリング**
  - 業界随一ののエージェント／エージェントレス対応ソリューション
- **脆弱性管理**
  - 業界随一のエンタープライズグレード脆弱性管理ソリューション
  - 企業ネットワーク、クラウド、仮想環境導入と、様々なユーザー環境に対応
- **セキュリティ情報管理**

  セキュアで信頼性の高いログ／イベントの収集、分析、管理
- **レポーティング＆可視化**

  IT 資産管理とリスク分析／特定にフォーカス
- **テンプレート＆ポリシー**

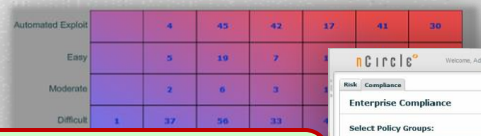
  SCAP に忠実に沿った検証作業の実施

Tripwire IP360 の利用イメージ ～ オンプロミス型ソリューションによる継続的改善 ～

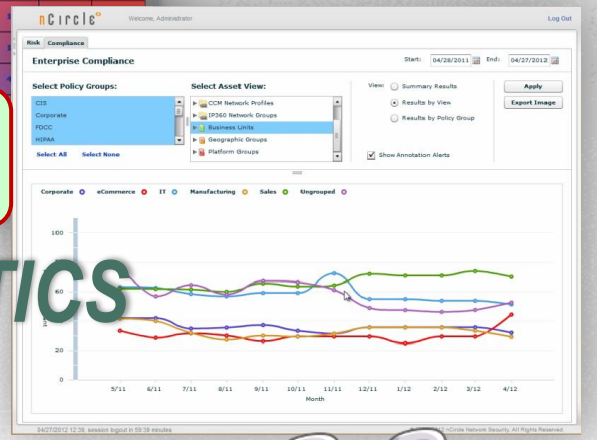


どのような IT 資産が
存在しているか？

DISCOVERY



セキュリティコンプライアンス
遵守状況は？



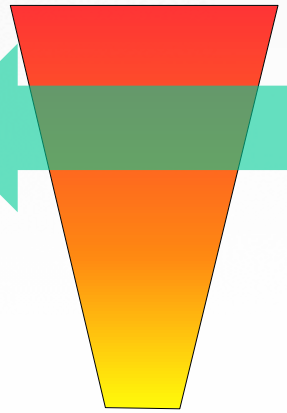
ANALYTICS

TRIPWIRE®
IP360
Vulnerability Management

未知の脅威への追従
IT 資産の最適運用

すぐに改善すべき上位10個
の問題は？

責任の所在は？
改善状況は？



PRIORITIZATION

Vulnerability		alue
MS01-023: Microsoft IIS .printer ISAPI Available		
MS01-026: Microsoft IIS CGI Filename Decode Error	28826	10,000
MS01-033: Micros[illegible] Buffer Over	28519	10,000
Multiple Vendor System V Derived login Buffer Overflow Vulnerability	26862	7,000
MS03-007: Microsoft Windows ntdll.dll Buffer Overflow Vulnerability - WebDAV	21980	5,000
MS98-003: Microsoft Windows NT IIS ASP Alternate Data Streams Vulnerability	6304	5,000
MS02-028: Microsoft IIS HTR Chunked Encoding Transfer Heap Overflow Vulnerabili	6302	4,000
MS99-013: Microsoft Windows NT IIS showcode.asp File Access Vulnerability	5807	4,000
MS99-019: Microsoft Windows NT IIS 4 Malformed HTR Request Buffer Overflow Vu	5758	3,700

Tripwire Enterprise 運用の流れ ～ オペレーションの完全性、共有化を重視 ～

ケース2: 情報セキュリティ対策
目標管理の実例

TRIPWIRE® IP360

TRIPWIRE® ENTERPRISE

TRIPWIRE® PURECLOUD

営業窓口

ソリューションや製品に関するお問い合わせは弊社までお願いいたします。

トリップワイヤ・ジャパン(株)
営業本部
sales@tripwire.co.jp

〒112-0014
東京都文京区関口1-24-8　東宝江戸川橋ビル8F
TEL：(03) 5206-8610　　FAX: (03) 5206-8613

評価版の取得

一部の製品については、評価版をご用意しております。
下記URLからお申し込みください。

https://www.tripwire.co.jp/downloads/