tripwire™
TAKE CONTROL.

ファイル整合性監視は なぜ重要なのか
要件 11.5

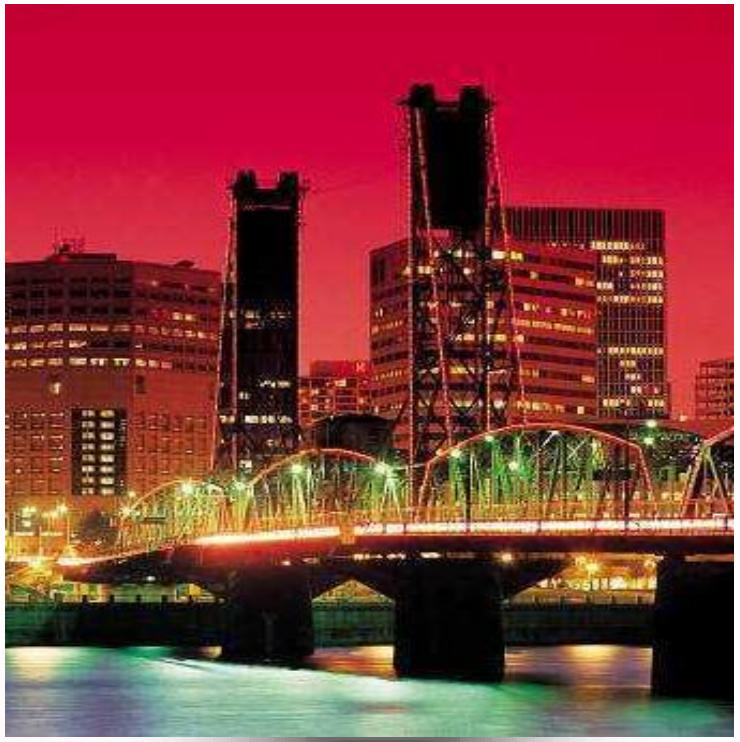
トリップワイヤ・ジャパン株式会社

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）
代表取締役社長：杉山富治郎

導入実績：世界87カ国 6,500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改ざん検知推奨製品として紹介



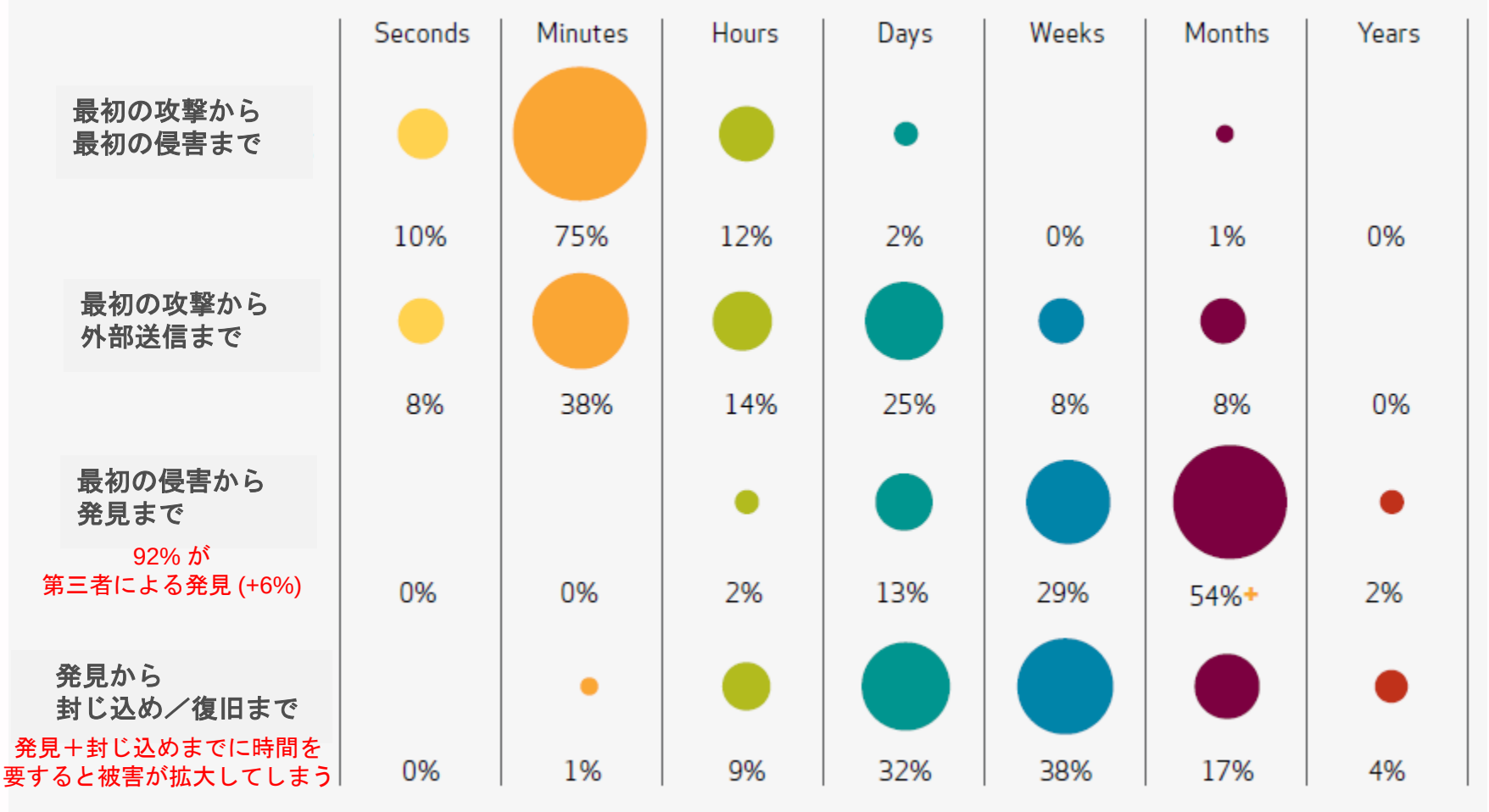
✓ 変更検知に特化して15年
✓ 変更検知のパイオニアであり、デファクトスタンダード
→ No.1 のマーケットシェア
→ 実績による安定性と信頼

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

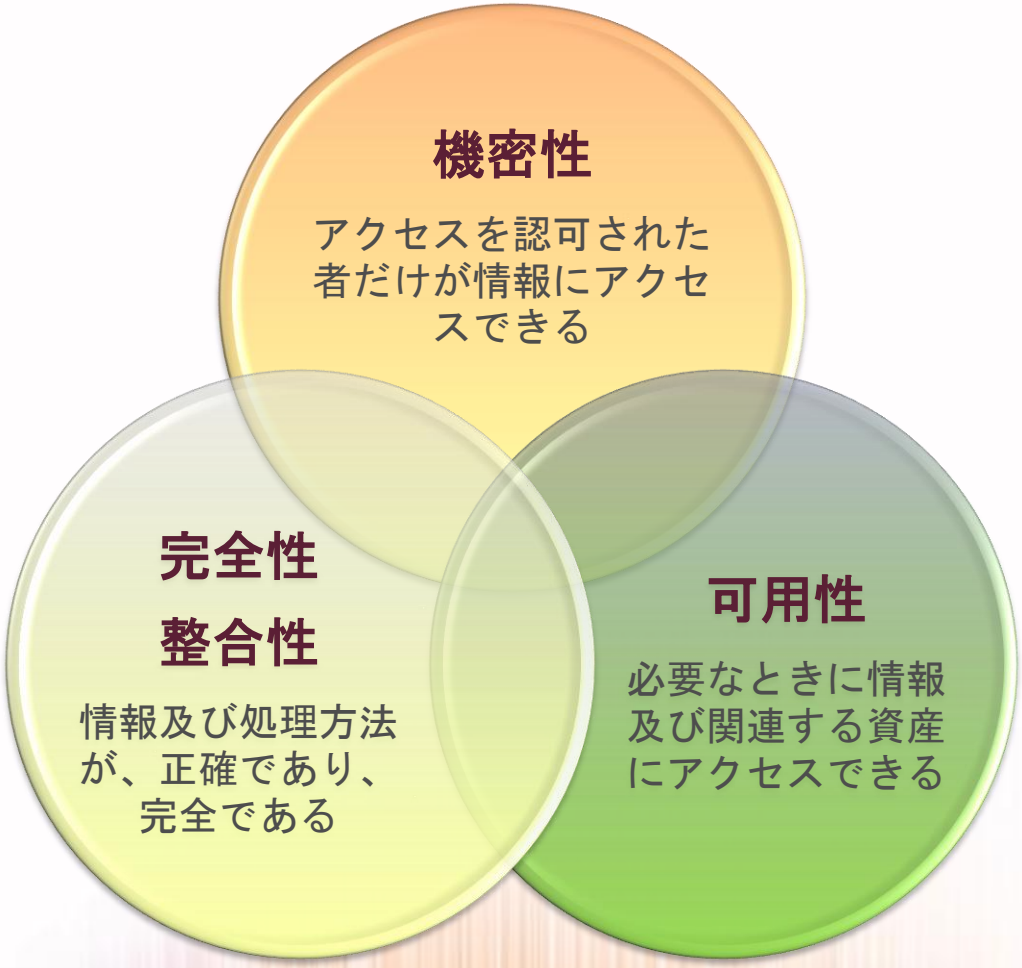
検知対策：早期発見の重要性

- セキュリティ強化には、**防御／検知**のバランスの取れた対策が必要



(引用) ベライゾンビジネス　"2012 DATA BREACH INVESTIGATIONS REPORT

整合性とは？



「先進企業から学ぶ事業リスクマネジメント　実践テキスト」より

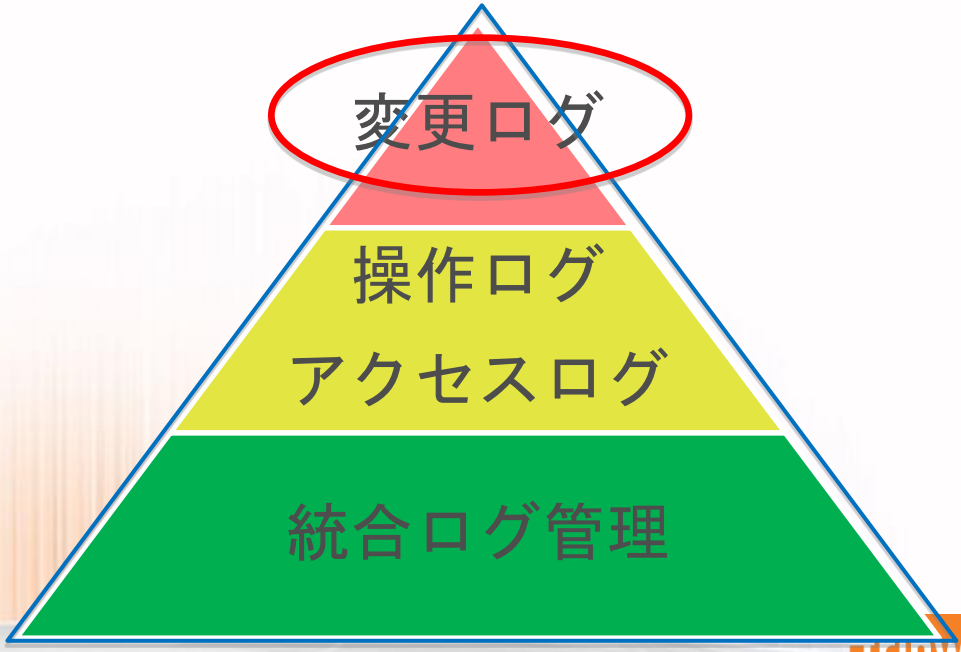
整合性監視(変更検知)は発見対策の最前線です

クリティカルな
セキュリティ侵害

- 情報漏洩対策
  - サイバー犯罪のほとんどが、システムへの変更を行う　(OS設定ファイル、ライブラリ、レジストリへの変更)
- Web改ざん対策
  - 企業の顔とも言うべきWeb改ざんへの迅速な対応

- 設定したアクセス制御が知らない間に変わっている
- 脆弱性を利用して、マルウェアを置かれた

システムの変更にフォーカス



セキュリティ属性の何が侵害されているのか

表13. セキュリティ属性と、各セキュリティ属性が侵害されたデータ漏洩/侵害事例の割合

侵害された属性	定義	漏洩/侵害（%）
機密性	アクセス、閲覧、開示が制限されている状態	100%
所有	独占的（または意図的）に所有・管理すること（また所有を証明できる能力）	0%
整合性	欠落がなく、また当初の状態から変わっていないこと	90%
信憑性	正当であり、必要な条件に合致し、本物であること	5%
可用性	存在し、準備ができており、したがって必要なときに使用できること	1%
有用性	実用的であり、使用目的に適合していること	0%

(引用) ベライゾンビジネス「2011年度 データ漏洩 / 侵害　調査報告書」

整合性監視はセキュリティの基礎対策です

Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers

整合性監視が定義されているセキュリティ基準

- SOX - Sarbanes-Oxley Act (Section 404)[3]
- NERC SIP - Nerc Standard SIP (System Security R15-R19)[4]
- Department of Defense Information Assurance (IA) Implementation (DODI 8500.2)[5]
- FISMA - Federal Information Security Management Act (NIST SP800-53 Rev3)[6]
- HIPAA - Health Insurance Portability and Accountability Act of 1996 (NIST Publication 800-66)[7]

ウィキペディアより

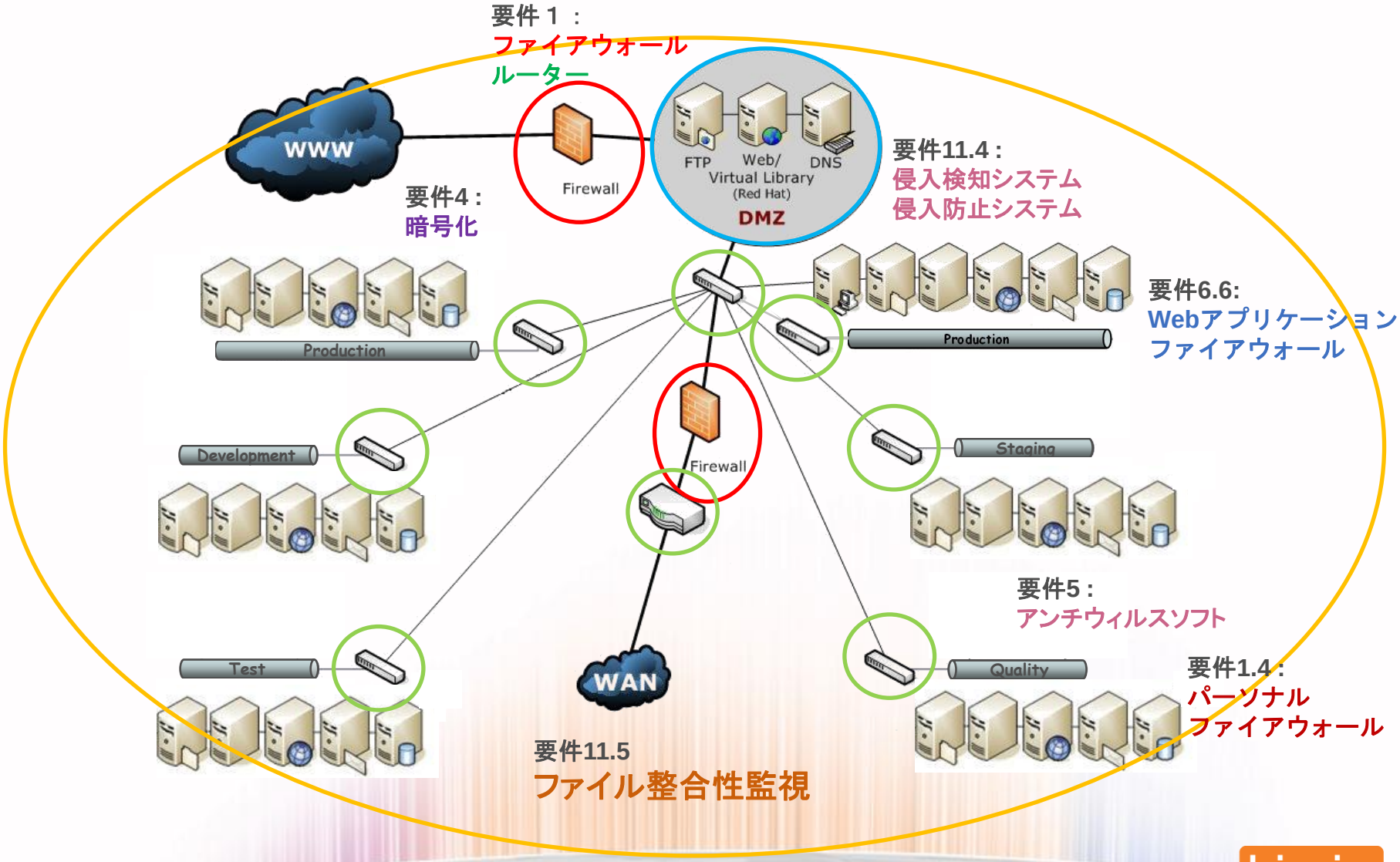
PCI DSS 2.0 ファイル整合性監視

要件10.5.5
ログに対してファイル整合性監視または変更検出ソフトウェアを使用して、既存のログデータを変更すると警告が生成されるようにする。
（ただし、新しいデータを追加する場合は警告を発生させない）

要件12.9.5
侵入検知、侵入防止、およびファイル整合性監視システムからの警告を含める。

要件11.5
ファイル整合性監視ツールを導入して重要なシステムファイル、構成ファイルまたはコンテンツ・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一度実行するようにソフトウェアを構成する。

PCI DSS 2.0 が要請しているセキュリティ・システム



どんな整合性監視が求められているか

- 何を監視すれば良いのかを示してくれる
- 素早く導入できる
- 怪しい変更 = 整合性違反を迅速、的確に検知する
- コストを掛けない自動運転
- 監査レポートの作成
- 監視対象システムに負荷を掛けない
- 整合性監視ソフト自体は改ざんされない

tripwire ENTERPRISE

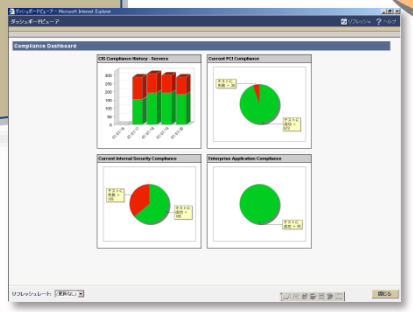
PCI DSS 2.0 : 達成度を可視化します

ベンダ出荷の
デフォルト値を
使用しない

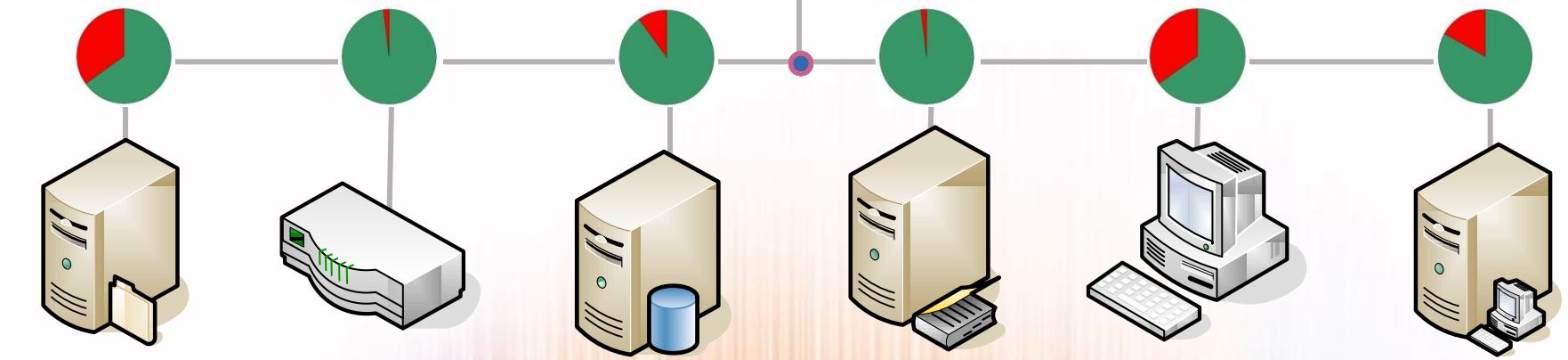
開放しているポートは
TCP XXXX, XXXX番

パスワードは7文字以上
90日以内に変更を促す

PCI DSS 2.0
ポリシー



緑が
ポリシー遵守です



ファイルシステム

ネットワーク
デバイス

データベース

ディレクトリ
サーバ

デスクトップ
PC

ミドルウェア

PCI DSS 2.0 : Tripwire Enterprise ができること

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

「PCI データセキュリティ基準 v2.0　2010年10月」より抜粋

ありがとうございました

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

Tripwire Enterprise の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/

30日間、すべての機能を
ご評価いただけます