tripwire
CONFIDENCE: SECURED

「PCIDSS準拠に対する網羅性と選択肢をご提供」
～トリップワイヤのソリューションを導入事例と共にご紹介

トリップワイヤ・ジャパン株式会社
マーケティング部

2015/7/28

Agenda

- 会社紹介：トリップワイヤについて
- Tripwire Enterpriseを最大限活用
  トリップワイヤ　PCI DSSソリューション
- トリップワイヤの脆弱性管理ソリューション
- オンプレミスだけではない、クラウドサービスを利用してのPCI DSS対応
- トリップワイヤソリューション活用によるユーザ事例のご紹介

会社紹介：トリップワイヤについて

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96カ国 9,000社
- Fortune 500社の 50%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
- **PCI　認定スキャンベンダー**として
  日本カード情報セキュリティ協議会で紹介

✓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 のマーケットシエア
→　実績による安定性と信頼

Tripwire 社の歩み

イノベーションとリーダーシップ

1992

多くの侵入検知テクニックの先駆けとして、初期ソフトウェアが作成される

1997

Tripwire社創業

商用製品として Tripwire for Servers をリリース

2005

Tripwire Enterprise 初出荷

2010

ActiveWorx社を買収し、ログ・インテリジェンスを製品ポートフォリオに追加

2011

Thoma Bravoによる買収で、更なる成長と収益性を向上

2013

nCircle社を買収し、完全なセキュリティ/脆弱性管理ソリューションポートフォリオを提供

2014

IDCがTripwireをポリシー/コンプライアンス市場でNo.2のベンダーと発表

2015

Belden社　セキュアな産業用IoTを目指しTripwireを買収

Fortune 500社の半分がTripwire製品を使用

このページは当日の講演で説明します

もしかすると

改ざん検知、
要件11.5のためだけに
利用していませんか？

Tripwire Enterprise の検知する改ざん内容

要件11.5　変更検出メカニズム（ファイル整合性監視ツールなど）を導入

- OS, ネットワーク設定の改ざん
- ログの改ざん
- アクセス権限の改ざん
- データ（コンテンツ）の改ざん

正常な成長は、変更として検知しない

設定ファイル

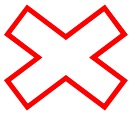
設定ファイル

変更

バイナリファイル

追加

レジストリ



削除

「チェックボックス」を埋めることに集中・・・

そのために各要件ごとにポイントソリューションやポイント対応実施

- PCI DSSの監査の合格に向けて
  チェックボックスを埋めることにエネルギーをそそぐ

- 終わったあとは日常業務に戻る

この間に・・・

- 四半期に一度のチェックを迎える
- 次の監査を迎える

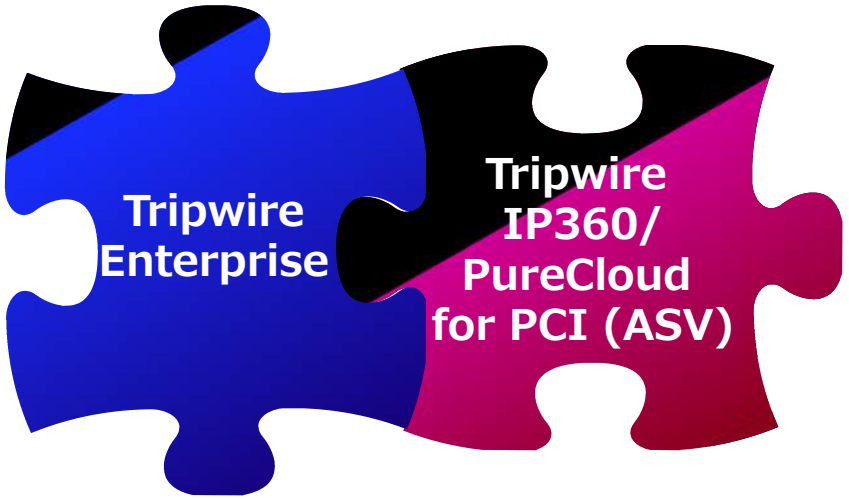
Tripwire Enterpriseを最大限活用

トリップワイヤ　PCI DSSソリューション

トリップワイヤがPCI DSS対応に選ばれるのは

単なるPCI対応だけではなく、継続と最新版対応をサポート

- PCI 対応範囲
- 製品の経験と幅
- 常に動向を把握
- 迅速な侵害検知
- サイバー犯罪制御 – すぐに使える侵害検知のルールを提供
- 修復に対するガイダンス
- 産業に対するポリシー適用の広さ
- 75%もの“ノイズ”削減
- 優先付けされた脆弱性アセスメント



トリップワイヤは二つの役割を行う

- PCI 3.1コンプライアンスの達成と継続
- 多くのその他コンプライアンスやセキュリティ強化要求に応える（SOX, HIPAA, NIST, ISO, DISAなど）

Tripwire Enterprise の機能と監視対象

改ざん検知だけではない、広範に渡る **ポリシー管理** も実現

Tripwire Enterprise コンソール

変更監査

下記のあらゆる監視対象での変更を検知し、指定した条件に沿って変更の要因、承認可否等を評価

ポリシーの可視化

企業や組織が守るべき内部的／対外的標準(ポリシー)に沿ってセキュリティ設定の正しさを評価

ファイルシステム (FS)			ND	DB	DS	HV
サーバ Windows UNIX, Linux	デスクトップ XP Vista	アプリケーション Web App 業務App	ネットワーク装置 ルーター ファイアウォール スイッチ	データベース Oracle SQL Server	ディレクトリサービス LDAP Active Directory	ハイパーバイザ VMware ESX

レポート&通知

調整／すり合せ

修復

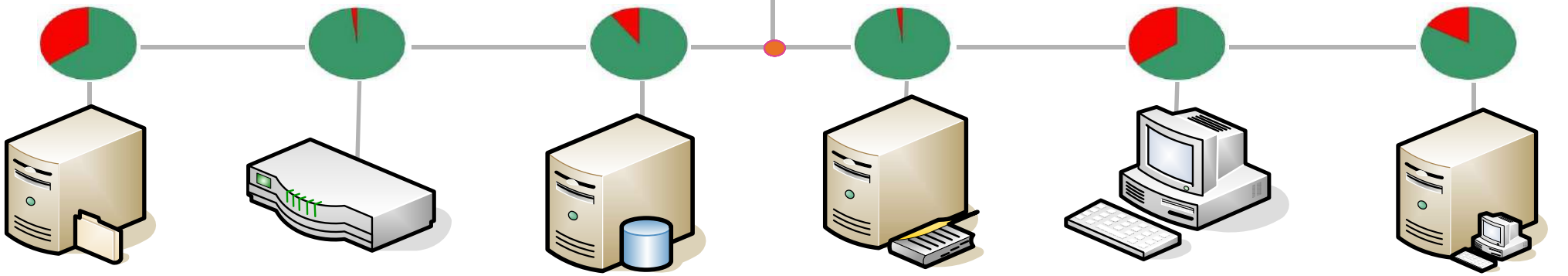
ポリシー適用によるセキュリティ対策状況の可視化

ベンダ出荷の
デフォルト値を
使用しない

**セキュリティ
ポリシー**

開放しているポートは
TCP XXXX, XXXX番

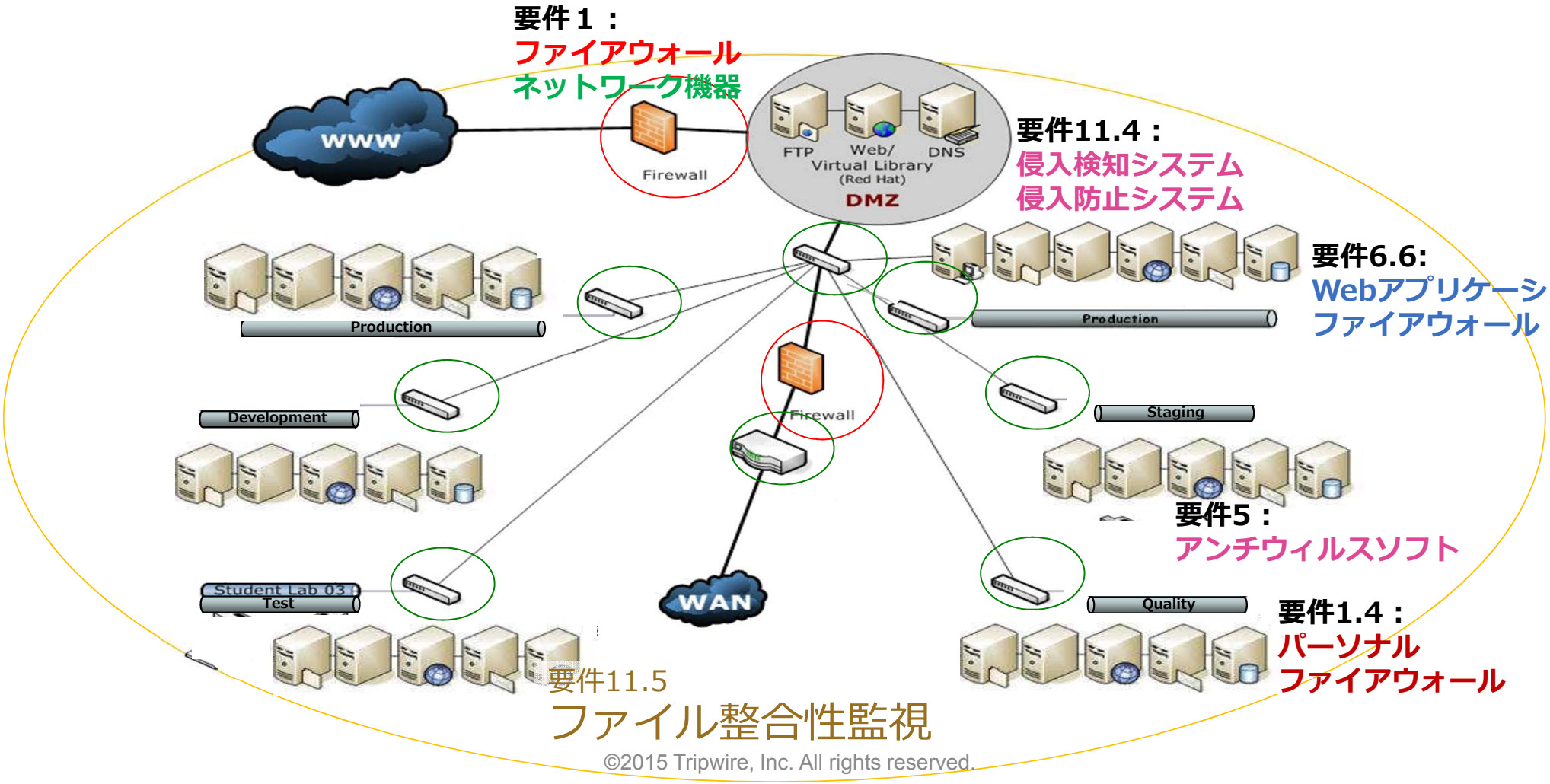
パスワードは7文字以上
90日以内に変更を促す



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

Tripwire Enterprise による統合的監視イメージ

PCI DSSの要件に対応するとともに組織全体の情報セキュリティ・コンプライアンスを確立する



Tripwire Enterprise の優位性

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維持	
要件5	すべてのシステムをマルウェアから保護し、ウィルス対策ソフトウェアまたはプログラムを定期的に更新する
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
強力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	システムコンポーネントへのアクセスを確認・許可する
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・ポリシーの維持	
要件12	すべての担当者の情報セキュリティに対応するポリシーを維持する

「PCI データセキュリティ基準 バージョン3.0 2013 年11月」より抜粋

脆弱性管理をTripwire Enterpriseと組み合わせる

TRIPWIRE® ENTERPRISE

- ただしい変更
- 不正な変更
- ファイル整合性監視
- エージェント型 “内から外”に視覚化

TRIPWIRE® IP360

- デバイスとアプリケーションのディスカバリ
- 脆弱性アセスメント
- Webアプリの脆弱性
- エージェントレス“外から内”を視覚化

手動では手間のかかる情報の連携

TRIPWIRE® ENTERPRISE

手作業もしくは Tripwire Enteprise での自動化によるサイバー脅威の検知と修復、リスクのある重要システムの要塞化

一昔前の サイバー脅威対策に基づいて、**手作業**で Tripwire Enterprise のモニタリングを構築

脆弱性診断サービスや他の脆弱性管理製品

環境をスキャンし、資産や脆弱性を限定的に抽出

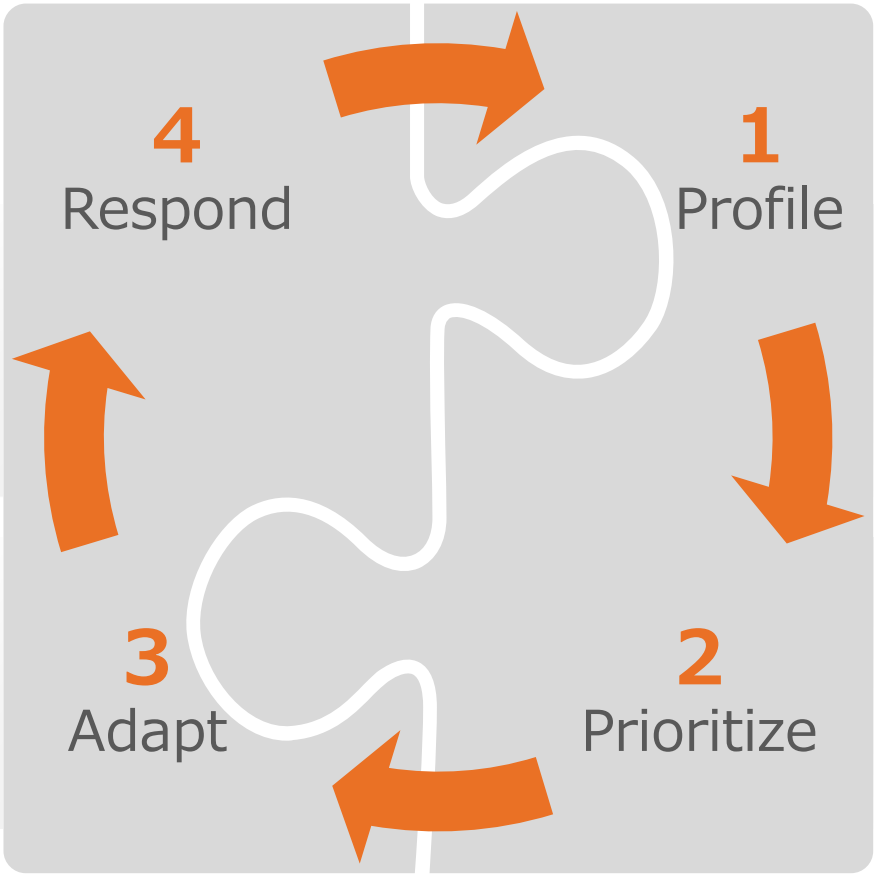
PDF レポート作成、対応の優先度付け、およびチーム内作業の割当ては全て手作業ベース

連携することで脅威とのギャップを低減

TRIPWIRE® ENTERPRISE

手作業もしくは Tripwire Enteprise での自動化によるサイバー脅威の検知と修復、リスクのある重要システムの要塞化

日々変化するサイバー脅威に迅速に追従する Tripwire Enterprise モニタリング



TRIPWIRE® IP360

Tripwire IP360 により脆弱性やアプリケーションの所在を分かりやすくプロファイリングしデータ化

Tripwire IP360 のスコアリングやリスクマトリクス分析により脆弱性リスクを定量化／優先度付け

Tripwire IP360 とTripwire Enterpriseをあわせる利点

PCI DSSに求められる改ざん検知、脆弱性スキャニングを
クリアするだけではない、真のセキュリティコンとコールを実現

このページは当日の講演で説明します

特別な対応ではなく日常業務に組み込む

だから継続可能

- PCI DSSを企業の全体的なセキュリティ戦略の一環として通常業務内で遂行する
- セキュリティコントロールが常に実行される

トリップワイヤの脆弱性管理ソリューション

脆弱性を『診断』でなく『管理』として提供

PCI DSSの6.1、6.2、11.2を始めとする要件をサポート

PCI DSS 要件
6.1 セキュリティ脆弱性情報の信頼できる社外提供元を使ってセキュリティの脆弱性を特定し、新たに発見されたセキュリティの脆弱性にリスクのランク（「高」、「中」、「低」など）を割り当てるプロセスを確立する。 ***注:*** *リスクのランク分けは、業界のベストプラクティスと考えられる影響の程度に基づいている必要があります。たとえば、脆弱性をランク分けする基準は、CVSS ベーススコア、ベンダによる分類、影響を受けるシステムの種類などを含む場合があります。*

6.2 すべてのシステムコンポーネントとソフトウェアに、ベンダ提供のセキュリティパッチがインストールされ、既知の脆弱性から保護されている。重要なセキュリティパッチは、リリース後 1 カ月以内にインストールする。 ***注:*** 要件 6.1 で定義されているリスクのランク分けプロセスに従って、重要なセキュリティパッチを識別する必要があります。

PCI DSS 要件
11.2 内部と外部ネットワークの脆弱性スキャンを少なくとも四半期に一度およびネットワークでの大幅な変更（新しいシステムコンポーネントのインストール、ネットワークトポロジの変更、ファイアウォール規則の変更、製品アップグレードなど）後に実行する。 ***注:*** *四半期ごとのスキャンプロセスの複数のスキャンレポートをまとめて、すべてのシステムがスキャンされ、すべての脆弱性に対処されたことを示すことができる。未修正の脆弱性が対処中であることを確認するために、追加の文書が要求される場合がある。* *初期の PCI DSS 準拠では、評価者が 1）最新のスキャン結果が合格スキャンであったこと、2）事業体で四半期に一度のスキャンを要求するポリシーと手順が文書化されていること、および 3）スキャン結果で判明した脆弱性が再スキャンにおいて示されているとおりに修正されたことを確認した場合、初回の PCI DSS 準拠のために、四半期に一度のスキャンに 4 回合格することは要求されない。初回 PCI DSS レビュー以降は毎年、四半期ごとのスキャンに 4 回合格しなければならない。*

【ご参考】日本国内　情報セキュリティ10大脅威 2015　（IPA）

2014年において社会的影響がおおきかったセキュリティ上の脅威について順位付け

このページは当日の講演で説明します

【ご参考】攻撃は脆弱性を放っておかない

このページは当日の講演で説明します

なぜ脆弱性『管理』が必要か？

【昨今の状況】

- 対外常駐
- クラウド
- その中で

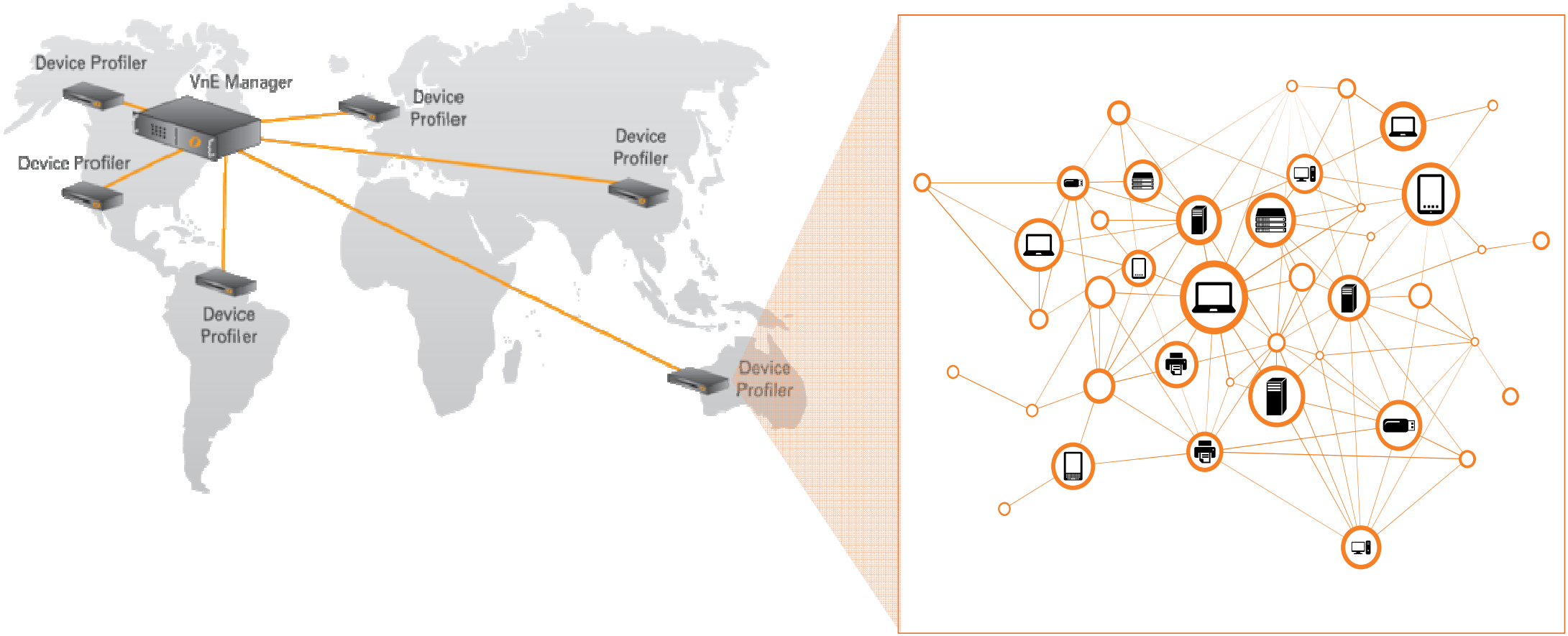
脆弱性診断
(定期的な実施→改善策提示→終り) から

脆弱性管理 (発見→分析→対応→評価) へ

- 脆弱性
- 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

脆弱性管理　－　Tripwire IP360

全ネットワークデバイスの情報収集と脆弱性アセスメントを自動化



脆弱性管理製品　Tripwire IP360

脅威とのギャップを埋めるために一番にすべきことに注力

自社のネットワークには何が存在するか？

セキュリティの自動化

最重要アクションに注力するためにプロセスを自動化

どこが最も脆弱か？

ビジネスコンテキスト

変化し続ける自社のビジネス環境に特有のコンテキストに関わるセキュリティリスクを管理

エンタープライズインテグレーション

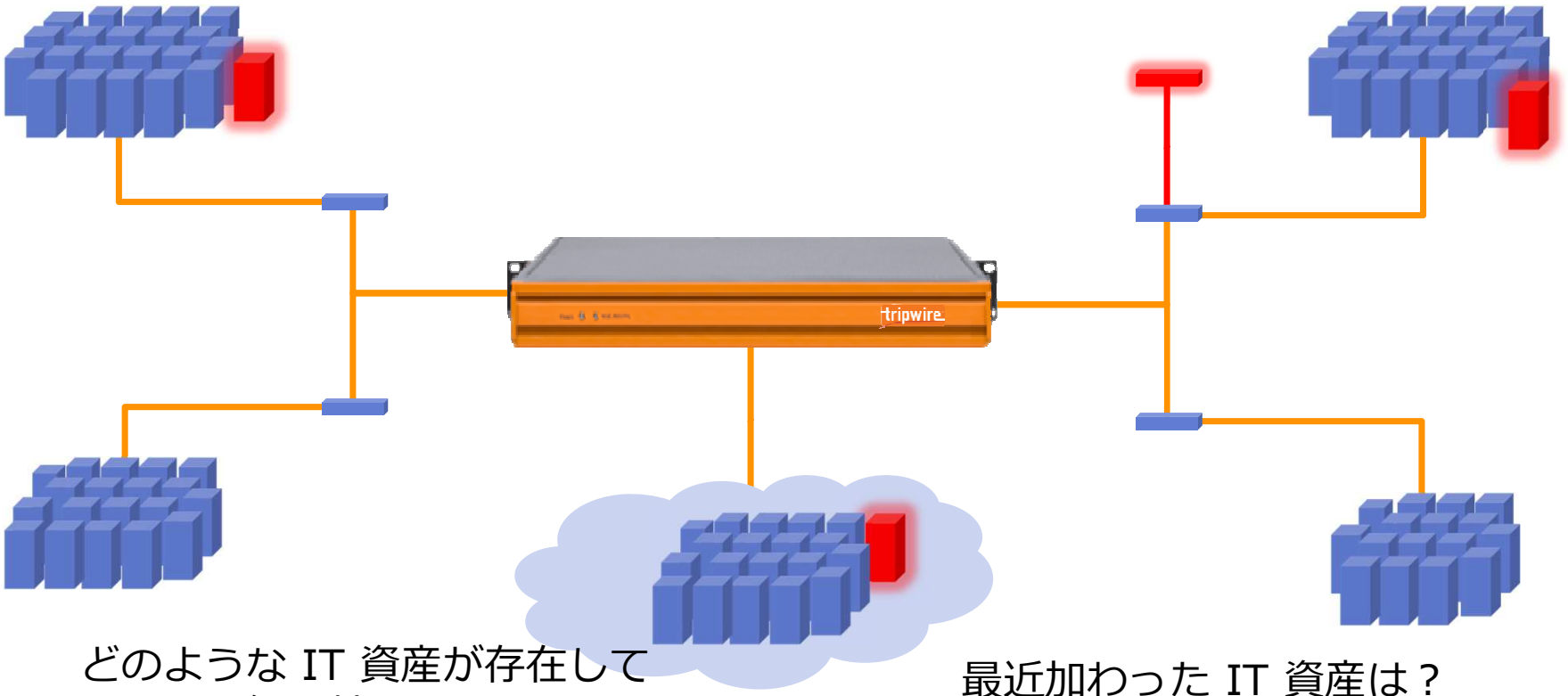
脅威への対応を向上させるため、脆弱性とイベントを関連付け

データ収集

WEB APPLICATIONS　ENTERPRISE APPLICATIONS　MIDDLEWARE　DATABASES　OPERATING SYSTEMS　INFRASTRUCTURE　APPLICATIONS

動的なホストトラッキング

ディスカバリは課金なし、脆弱性スキャン対象IPにのみ課金



どのような IT 資産が存在しているか？(網羅性)

最近加わった IT 資産は？
既存環境への影響は？(継続性、関係性)

他の追従を許さない脆弱性診断情報の量と緻密さ

- 100,000 以上の脆弱性検出
  （2015年4月現在）
- 2,400+ の OS
- 15,000+ のアプリケーション
- アプリケーションの情報
  - サービス、アプリケーション、バージョン、IP
- ターゲットに正確にマッチする脆弱性スキャンの調整

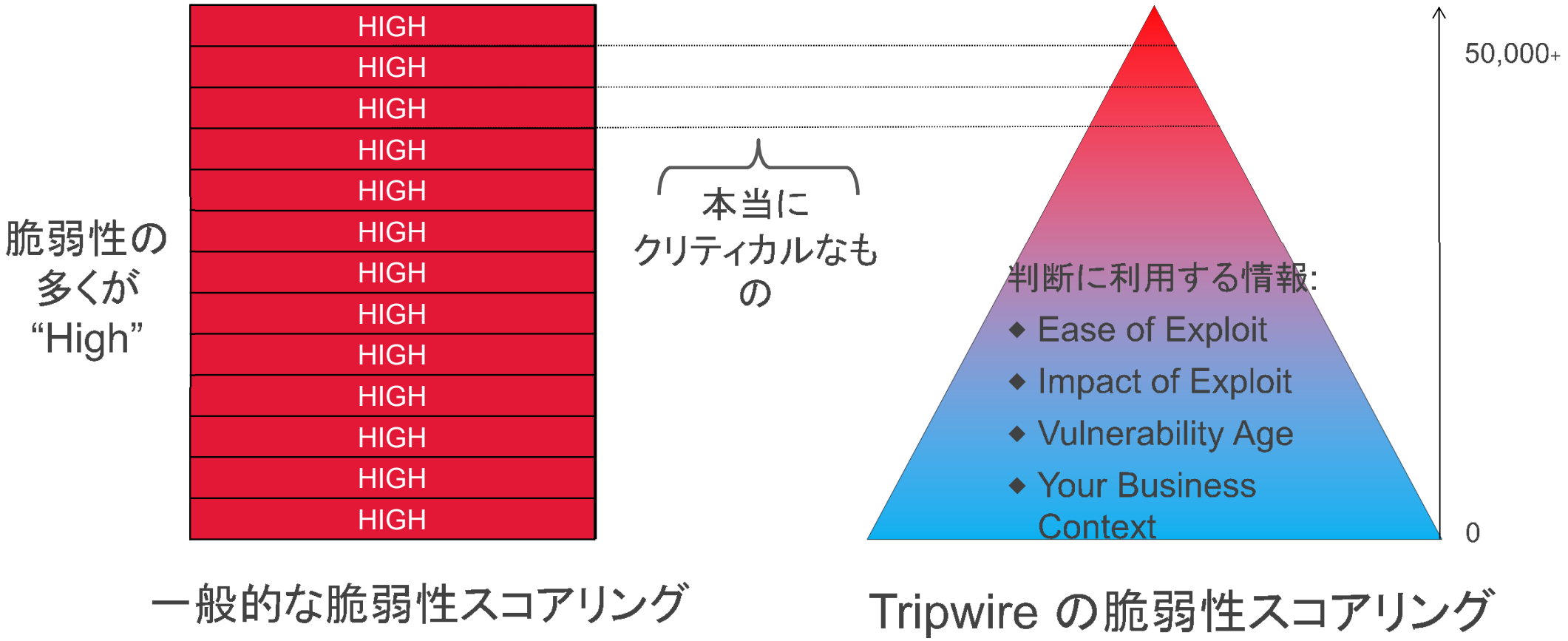
検出ミス、ネットワークへの影響を最小化

Summary | Hosts | Unmatched Hosts | Vulnerabilities | Applications | Audits

Service	Application	Hosts
Direct SMB Hosting Service	Windows Direct SMB Hosting Service	3
Direct SMB Hosting Service	Windows XP Direct SMB Hosting Service	9
DNS TCP	Bind 9 tcp DNS	4
DNS TCP	Microsoft tcp DNS	3
Finger	SCO UnixWare Finger	1
Finger	Sun Finger	5
FTP	Microsoft IIS FTP	3
FTP	Microsoft IIS FTP Service 4.x	1
FTP	Nokia IPSO FTP	2
FTP	Oracle Database 10g XML DB FTP (10.1.0.3)	1
HTTP	Apache 1.3.20 HTTP	1
HTTP	Apache 1.3.22 HTTP	2
HTTP	Apache 1.3.x HTTP	1
HTTP	Microsoft IIS HTTP 6.0	1
HTTP	NetScreen HTTP	3
HTTP	Oracle 10g XML DB HTTP (10.1.0.3)	1
HTTP	Oracle Management Agent HTTP	1
HTTP	PHP 4.x	2
IMAP	Microsoft Exchange IMAP	1
LDAP	ldap v2	1
LDAP	ldap v3	1
Microsoft RPC over TCP	Microsoft Windows RPC-DCOM	1
LPR Printing	Microsoft Windows 2000 LPD	1
LPR Printing	SunOS LPD	3

Page 1 of 3 Total Records: 287 Per Page: 100 Jump to Page: 1

Tripwire IP360のユニークなリスク優先度付け

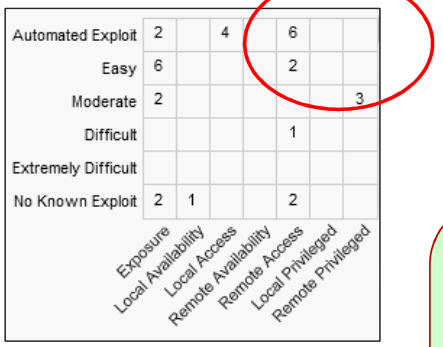


一般的な脆弱性スコアリング

Tripwire の脆弱性スコアリング

Tripwire IP360のユニークな脆弱性分析手法

- ▶厳選のためのリスクの数値化
- ▶ビジネス的価値付与
- ▶悪用のインパクト・可能性付与



Vulnerability	Score	Asset Value
MS01-023: Microsoft IIS .printer ISAPI Available	28952	12,000
MS01-026: Microsoft IIS CGI	28826	10,000
MS01-033: Microsoft Index	28519	10,000
Multiple Vendor System V	26862	10,000
MS03-007: Microsoft Windo	21980	10,000
Samba 'call_trans2open' Re	21731	10,000
MS03-026: Microsoft Windo	20504	10,000
Sun Solaris SAdmin Client	19704	10,000
MS04-011: Microsoft Windo	16715	8,000
MS04-011: Microsoft Windo	16715	8,000
MS04-035: Microsoft SMTP	13603	8,000
MS04-045: Microsoft Windo	12738	7,500
MS05-011: Microsoft Windows	1118	7,500
	9524	7,000
	9246	7,000
	6422	7,000
	6342	5,000
	6304	5,000
	6302	4,000
	5807	4,000
	5758	3,700

100 万～の脆弱性

最も重要な数十の脆弱性

【ビジネス的資産価値の適用基準例】

- 機密性の高い情報を取り扱っているか？
- 外部ネットワークにさらされているか？
- 高サービスレベルを維持するシステムか？
- 監査情報を保持しているか？

タイムリーに脆弱性情報を提供するVERT

ワールドクラスの脆弱性リサーチチーム

Tripwire VERT (Vulnerabilities and Exposures Research Team)

タイムリー

脆弱性インテリジェンスを、ワールドクラスのセキュリティ/脆弱性研究者からなる専門チームが提供

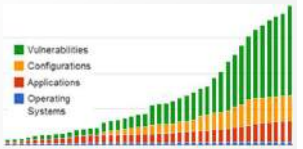
必要とされる情報

企業が気にするエンタープライズ製品の脆弱性をカバー

ORACLE Microsoft Novell cisco hp vmware McAfee IBM NetApp

継続

Tripwire IP360は脆弱性のカバー範囲を継続して広げている



迅速

クリティカルなマイクロソフト セキュリティ情報に対しては24時間のSLAで対応

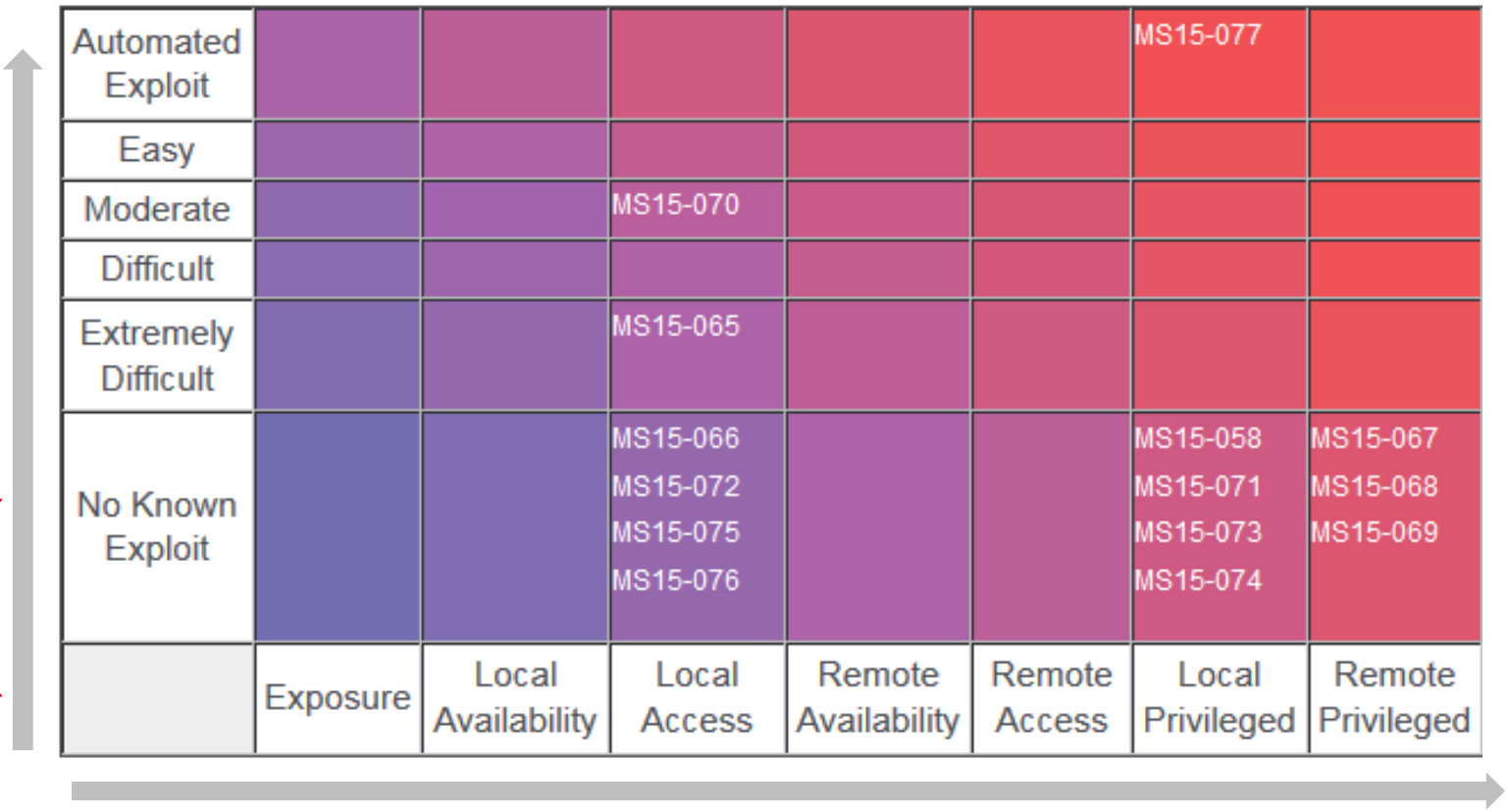
【ご参考】VERTによる“July 2015 Patch Tuesday Analysis”

2015年７月に出たマイクロソフト社のパッチ情報を可視化して紹介

- http://www.tripwire.com/vert/vert-alert/vert-alert-july-2015/

悪用可能性と
権限範囲によって
マッピング

Webでぜひ
ご確認
ください



トリップワイヤ　脆弱性管理ソリューション

要件5，6　そして要件11.2を中心に

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維持	
要件5	すべてのシステムをマルウェアから保護し、ウィルス対策ソフトウェアまたはプログラムを定期的に更新する
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
強力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	システムコンポーネントへのアクセスを確認・許可する
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・ポリシーの維持	
要件12	すべての担当者の情報セキュリティに対応するポリシーを維持する

「PCI データセキュリティ基準
バージョン3.0

2013 年11月」
より抜粋

オンプレミスだけではない、
クラウドサービスを利用してのPCI DSS対応

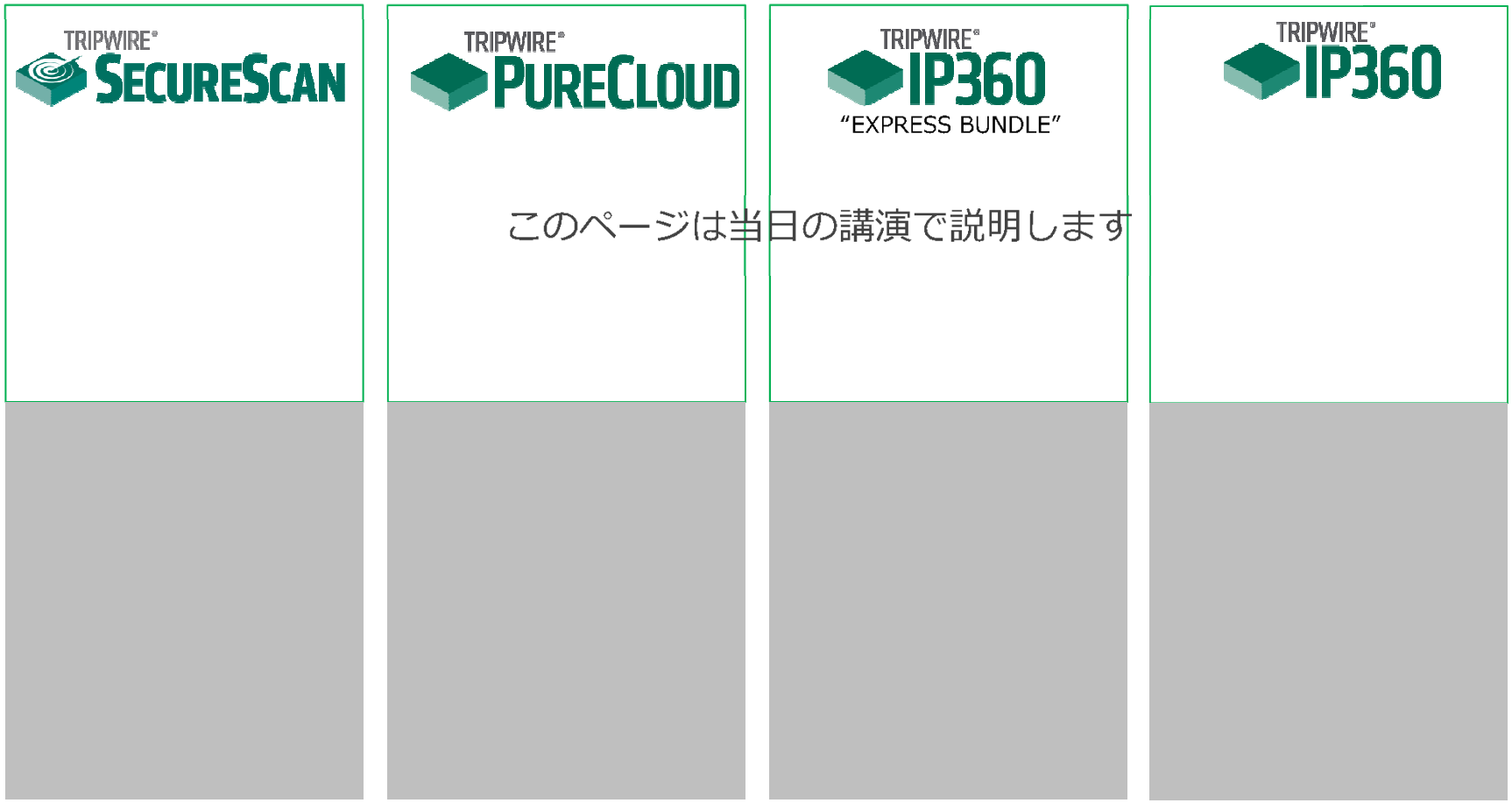
Tripwire Enterpriseをサービスで提供

トリップワイヤ　パートナー様によるサービス展開

このページは当日の講演で説明します

トリップワイヤの脆弱性管理ソリューション

クラウドサービスも含めたラインナップ



トリップワイヤソリューション活用による
ユーザ事例のご紹介

国内ユーザ事例：

このページは当日の講演で説明します

海外ユーザ事例：

このページは当日の講演で説明します

海外ユーザ事例：

このページは当日の講演で説明します

おわりに

このページは当日の講演で説明します

tripwire
CONFIDENCE: SECURED

ありがとうございました

〒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

お問い合わせ先：　https://www.tripwire.co.jp/contact/