チューニングレスを実現するネットワーク型IPSとは？

IPSの運用課題を解決するトレンドマイクロの TippingPoint

2018年2月
トレンドマイクロ株式会社
プロダクトマーケティング本部
シニアプロダクトマーケティングマネージャ
福井 順一

2017年、相次ぐ発見されるWebシステムの脆弱性

Apache Struts 2の脆弱性「CVE-2017-5638」、遠隔で任意コード実行が可能に

投稿日: 2017年3月13日
脅威カテゴリ: 不正プログラム，サイバー攻撃，脆弱性，TrendLabs Report
執筆: Vulnerability Research Engineer - Suraj Sahu

WordPress の深刻な脆弱性によって全世界でサイト改ざん被害が発生

2 月にはオープンソースのコンテンツ管理システムである WordPress で脆弱性が発覚しました。WordPress 4.7.0 以降のバージョンで標準機能となった REST API に深刻な脆弱性（4 月 2 日に「CVE-2017-1001000」として採番）[25]が発覚し、ほぼ同日にその脆弱性の「POC」が公開されたことによって、全世界で多数の Web サイトが改ざんされました。

出典:2017年第 1 四半期セキュリティラウンドアップから引用
https://www.trendmicro.com/ja_jp/security-intelligence/research-reports/sr/sr-2017q1.html

ITシステムの脆弱性対策が急務

脆弱性を悪用して改竄、破壊、窃取をする攻撃

脆弱性を悪用して内部拡散するマルウェアの出現

セキュリティ・パッチが適用されていない状態で運用されてる システムが存在していませんか？

- RHEL4, 5のサポートが終了予定だが、アップグレードする計画はない
- WindowsXP/2003などサポート終了後も継続運用している
- Windows Server 2008は延長サポート期間終了は2020年1月14日

システム運用におけるセキュリティ対策の実情

セキュリティ管理者はリスク対策の観点から「修正パッチは適用すべき」

しかし、**サーバー管理者**の実情は・・・・・課題が多い

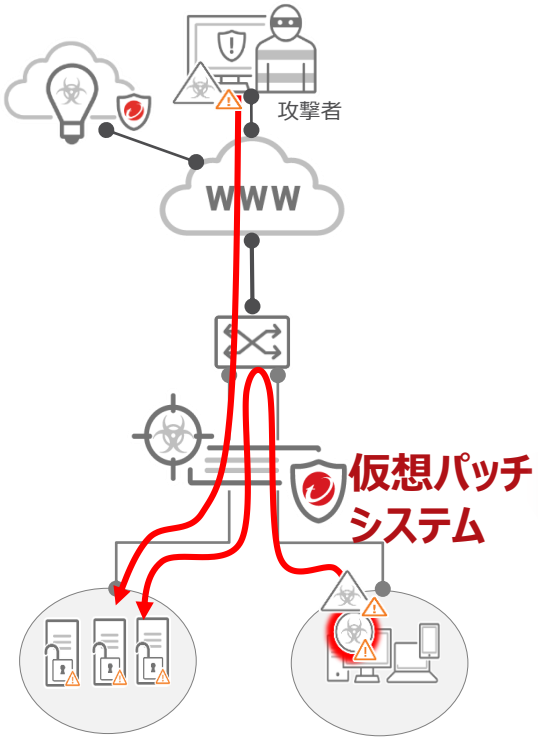
修正パッチ適用のための
計画停止が業務運用上困難

ベンダーサポートが終了したため
修正パッチがリリースされない

安定稼働しているため
敢えて保守していない

- **準備のための時間、コスト、人材が足りない**
  - 最新の構成情報が共有されていない事による負担
    - 自社のどのシステムが該当しているか判らないので都度各担当者に確認する
    - 適用作業後の業務影響が判らないのでシステム構成を調べる
  - 技術者不足による負担
    - 不具合がどの程度業務に影響を与えるか判断が難しい
    - 一度に対応できないほどのサーバー数
  - 調整ごとによる負担
    - 業務との計画停止スケジュール調整
    - 限られた変更期間
- **問題の出ていないシステムをあえて変更するのはリスクがある**
- **その割に効果が見えにくい**
  - 不具合修正しておいてよかったという事をあまり感じることはない

仮想パッチによる対策



仮想パッチとは、ソフトウェアの脆弱性を突いた攻撃を遮断し、“あたかもパッチが当たっているかの様な状態”にすること。

インライン運用による脆弱性対策の自動化に必要な要件

- 誤検知が発生しにくいこと
- 最新の対策に適時自動更新されること
- 業務通信を遅延させないこと
- 高信頼性・高可用性であること

Trend Micro TippingPointのご紹介

TippingPoint は

企業内サーバやクライアント端末に残る
既知の脆弱性やゼロデイ脆弱性を
サイバー攻撃などの脅威から守る
ネットワークセキュリティアプライアンスです

- 脆弱性をベースにしたセキュリティフィルタにより高いパフォーマンスと低い誤検知率を実現
- 脆弱性発見・調査・分析を行う自社研究機関に加え、第三者機関からの情報も活用することによりゼロデイ脆弱性に対する迅速な対応が可能
- ASICの処理を独自カスタマイズで行うことにより高速のインスペクションスループットを実現

TippingPoint仮想パッチシステムの特徴

1. “チューニングレス”を想定した製品デザイン
2. 世界トップレベルの脆弱性リサーチ力
3. H/W型なのに柔軟な導入が可能

TippingPoint仮想パッチシステムの特徴

1. “チューニングレス”を想定した製品デザイン
2. 世界トップレベルの脆弱性リサーチ力
3. H/W型なのに柔軟な導入が可能

従来のNW型IPS/IDSの課題①

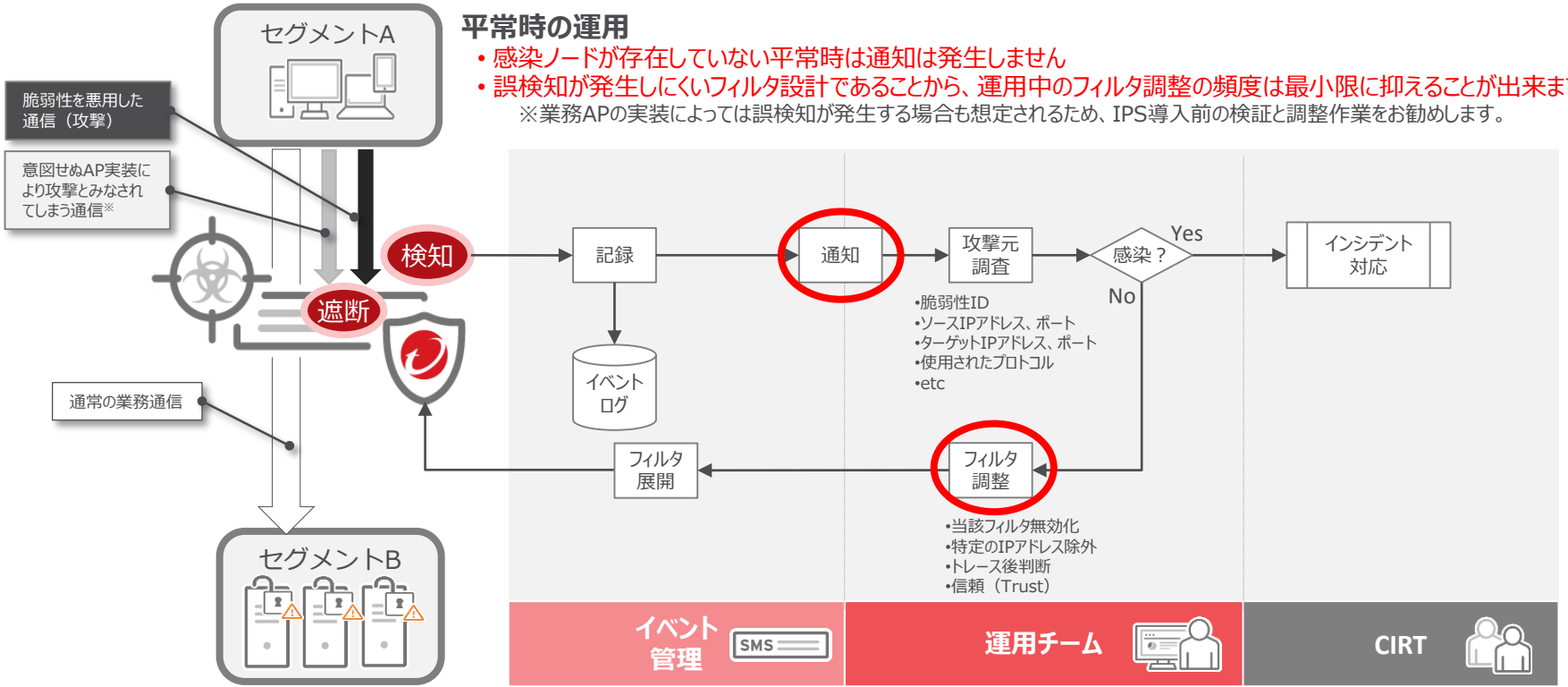
- **導入に時間がかかる**
  - チューニングが必須で難しい (多くの場合、最初に出てくるシグネチャは検知モードであることが多い)

“チューニングレス”を想定した製品デザイン

推奨ルールでの運用を前提とした製品設計になっています。

導入	**質問：フィルタ構成を最適化しないと使えないのでは・・** 回答：DVLabs（脆弱性解析チーム）が事前に分析・精査を行った上で、利用目的に合わせたチューニングルール群（推奨フィルタ）を提供しています。 そのため導入後に時間を掛けたチューニング、ラーニング等の作業は必要ありません。
運用	**質問：セキュリティ運用には専門家が必要なのでは・・・** 回答：攻撃を自動的にブロックする事を目的に作られた精度の高いフィルタになっています。フィルタ・チューニング、攻撃内容の分析等の専門性の高い運用を無理に行う必要はありません。

仮想パッチシステムの運用



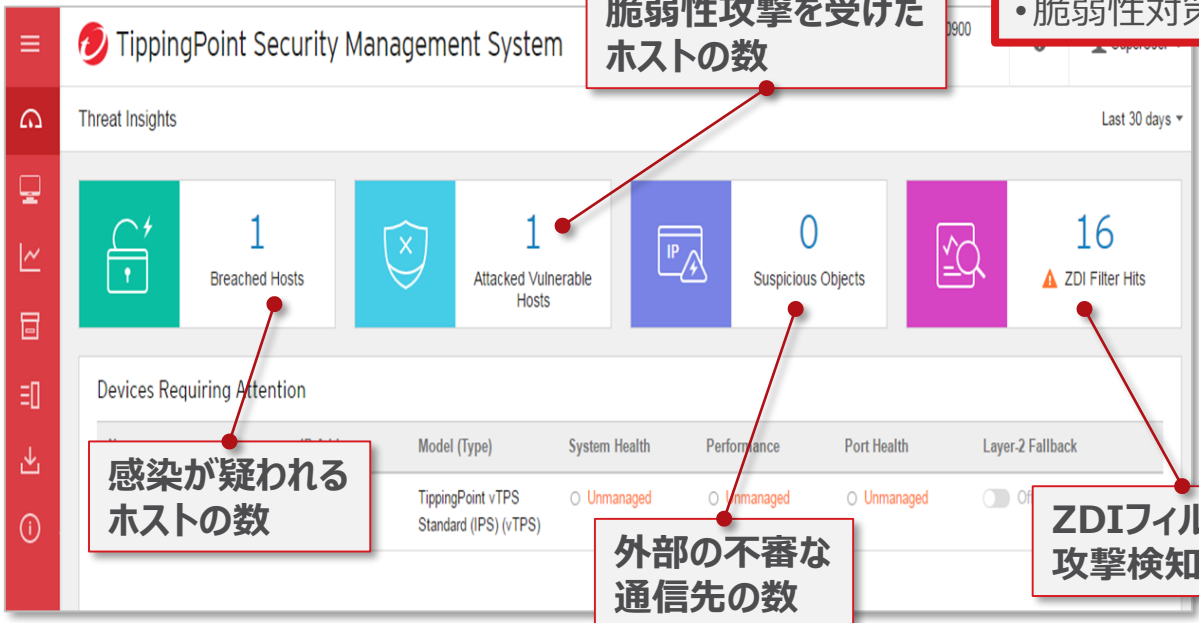
平常時の運用

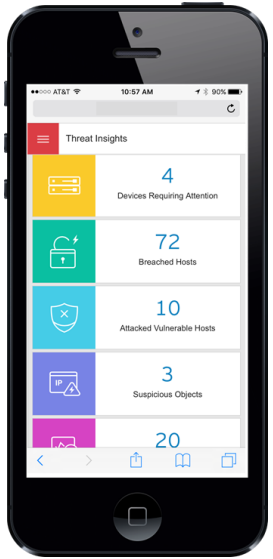
- 感染ノードが存在していない平常時は通知は発生しません
- 誤検知が発生しにくいフィルタ設計であることから、運用中のフィルタ調整の頻度は最小限に抑えることが出来ます。
  ※業務APの実装によっては誤検知が発生する場合も想定されるため、IPS導入前の検証と調整作業をお勧めします。

見やすいダッシュボード(Threat Insight)

社内IT環境の安全性をシンプルにKPIで可視化

SMSダッシュボードによる可視化
- 社内ネットワークの安全性とリスク
- 脆弱性対策の効果





従来のNW型IPS/IDSの課題②

- **誤検知、過検知が多く運用が大変**
  - 誤検知（False negative）を無くそうとすると過検知（False positive）の可能性が多くなる
  - ログが多すぎて結局見切れない

TippingPoint仮想パッチシステムの特徴

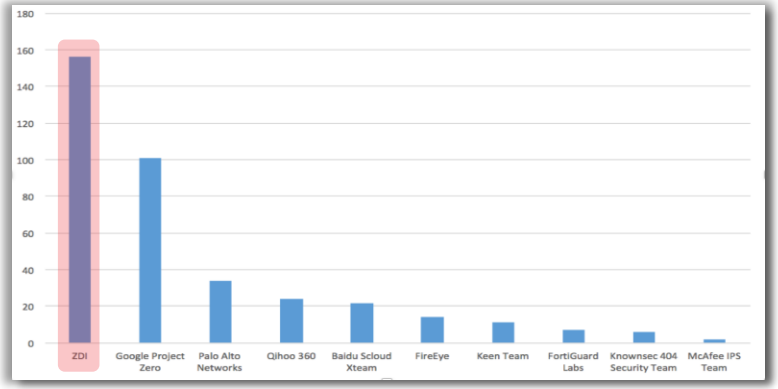
1. “チューニングレス”を想定した製品デザイン
2. 世界トップレベルの脆弱性リサーチ力
3. H/W型なのに柔軟な導入が可能

世界トップレベルの脆弱性リサーチ力

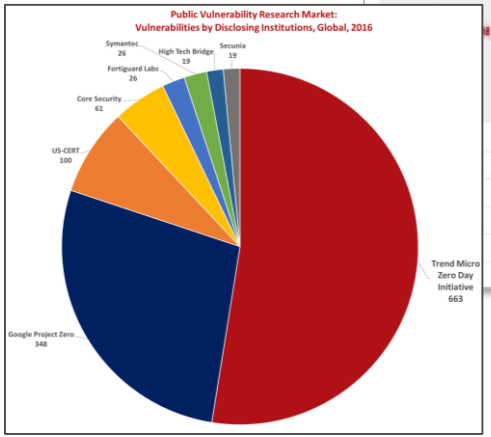
2016年における世界で報告された脆弱性の内、
約52.2%がZero Day Initiative(TPの脆弱性リサーチ機関)の報告によるものでした。※

- 脆弱性リサーチを2005年8月から11年以上の実績
- 世界80ヶ国3,000名以上のセキュリティリサーチャーと連携
- 業界をリードするゼロデイ脆弱性発見/報告数
- 5,000件超の脆弱性報告を受け、2,000件以上をベンダーに報告
- Pwn2Own などの脆弱性発見コンテストも国際的に主催

※第三者機関　Frost & Sullivan の調査レポートによる

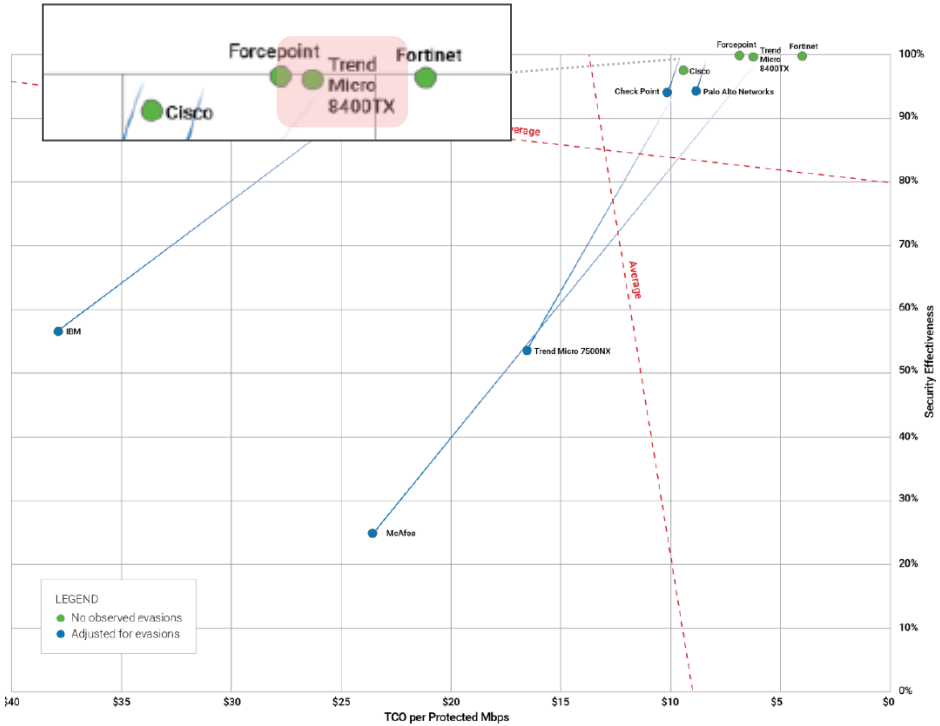


Microsoft社の公開情報からの統計データ（2015年）から集計
https://technet.microsoft.com/ja-jp/library/security/mt674627.aspx



Frost & Sullivan. Analysis of the Global Public Vulnerability Research Market, 2016. July 2017.

NSS Labsによる評価結果



Product	Security Effectiveness		Value in US$ (TCO per Protected Mbps)		Overall Rating
Check Point 15600	94.1%	Above average	$10	Above average	Recommended
Cisco FirePOWER 8350	97.4%	Above average	$9	Above average	Recommended
Forcepoint NGFW 3301	99.9%	Above average	$7	Above average	Recommended
Fortinet FortiGate 600D	99.7%	Above average	$4	Above average	Recommended
IBM XGS 5200	56.7%	Below average	$38	Below average	Caution
McAfee NS9100	25.0%	Below average	$24	Below average	Caution
Palo Alto Networks PA-5250	94.3%	Above average	$9	Above average	Recommended
Trend Micro 7500NX	53.6%	Below average	$17	Below average	Caution
Trend Micro 8400TX	99.6%	Above average	$6	Above average	Recommended

Figure 2 – NSS Labs' 2017 Recommendations for Next Generation Intrusion Prevention Systems (NGIPS)

参考:NSS Labsが2017年に発表したNGIPSの各社評価結果と推奨製品一覧

これまで提供されてきたフィルターの実績

TippingPoint仮想パッチシステムの特徴

1. “チューニングレス”を想定した製品デザイン
2. 世界トップレベルの脆弱性リサーチ力
3. H/W型なのに柔軟な導入が可能

従来のNW型IPS/IDSの課題③

- **最大のネットワーク帯域を考慮した設計にする必要**
  - 保護対象のホスト数は少ないのにネットワークの帯域は広い
  - どれくらいのネットワーク量か分からない

TippingPointはラインナップ２つだけ

Threat Protection System	
Tシリーズ	**TXシリーズ** NEW
物理/仮想アプライアンス	物理アプライアンス
 440T 2200T	 8200TX 8400TX
• 最新シリーズ（Nシリーズの後継） • 小中規模環境向けエントリーモデル • NWインタフェース：固定（ZPHA内蔵） • 検査スループット可変 • SSLインスペクション機能（2200Tのみ） • サンドボックス型製品と連携	• 最新シリーズ（NXシリーズの後継） • 大規模環境向けハイエンドモデル • NWインタフェース：モジュール式* • 検査スループット可変 • SSLインスペクション機能 • サンドボックス型製品と連携 • スタック構成で120Gbpsまで拡張可能
440T, 2200T, vTPS	8200TX, 8400TX

* I/Oモジュール，トランシーバ等が別途必要になります

- Tシリーズ
  - 小中規模環境向けエントリーモデル
- TXシリーズ
  - 大規模環境向けハイエンドモデル

スループットに応じてライセンスを変えられます！

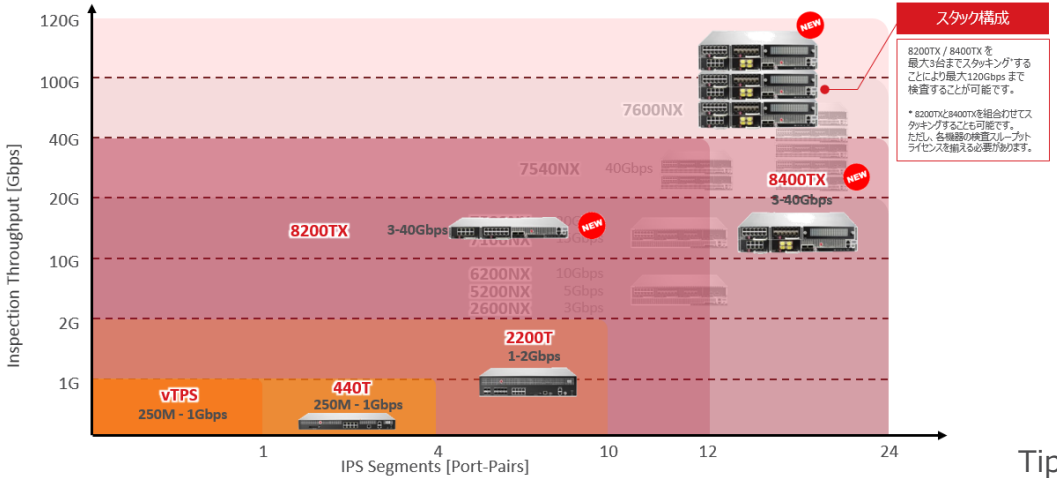
モデル	検査スループット／ThreatDVスループット（bps）											SSL検査
	250M	500M	1G	2G	3G	5G	10G	15G	20G	30G	40G	
440T	✓	✓	✓									
2200T			✓	✓								✓
8200TX					✓	✓	✓	✓	✓	✓	✓	✓
8400TX					✓	✓	✓	✓	✓	✓	✓	✓

高速処理を可能にするシステム基盤

インライン設置を前提とした低遅延なシステム設計

独自カスタマイズの FPGA による高スループット

- トラフィック処理をFPGA で行う専用設計のハードウェアで高いスループットを実現
- HDD レスで障害にも強く、パフォーマンスや信頼性を下げない
- 広帯域ネットワークにも対応



HDDを搭載せず、FPGA処理により耐障害性と高速・低遅延を実現！

第三者機関テストで他社の3倍以上の能力！

	TP	A社	B社
レイテンシ（遅延時間）		(UDP)	
128 bytes	29 µs	94 µs	40 µs
256 bytes	32 µs	94 µs	65 µs
512 bytes	33 µs	97 µs	119 µs
1024 bytes	36 µs	101 µs	120 µs
1514 bytes	39 µs	102 µs	120 µs

※ NSS Labs 2012 Latency Test

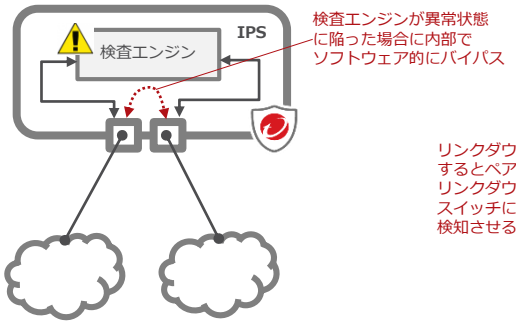
TippingPoint(TP): **40** マイクロ秒以下

高可用性を実現するシステム基盤

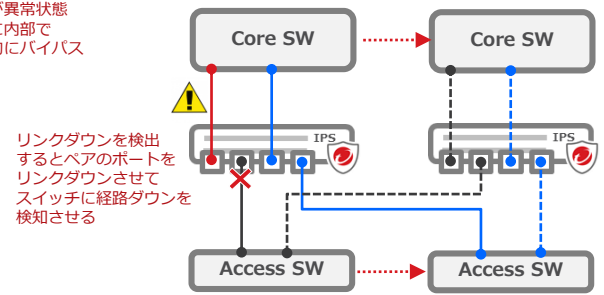
異常時でも通信継続を可能にするための機能

イベント	高可用性機能	発動時の動作
IPS障害による停止 IPS再起動 TOSアップデート時	L2 fallback	自動的に検査エンジンをバイパスし、通信を継続させる
リンクダウン時	Link Down Synchronization	Core, Access SWにリンクダウンを検知させ経路切替えを行わせ通信を継続させる
電源供給停止時	Bypass Module	TippingPointを通過する通信すべてを物理的にバイパスし、通信を継続させる

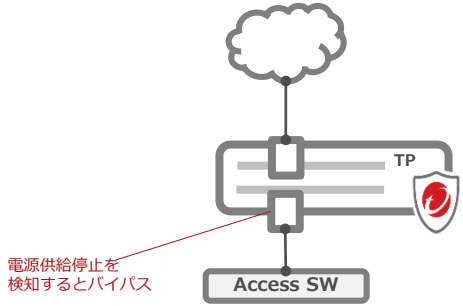
L2 fallback



Link Down Synchronization



Bypass Module



高信頼性を実現するシステム基盤

長期間使用できる高信頼性システム

直近サポート終了（EOS）
となったシリーズは
販売開始からEOSまで10年の実績

Product End-of-Life Dates

Milestone	Definition	Milestone Date
End-of-Life, End-of-Sales Announcement	The date on which HP TippingPoint announces the end of sale and end of life of a product.	May 1, 2015
End-of-Sale	The last date to order product through TippingPoint point of sale. The product is removed from the price list after this date.	July 31, 2015
End of 1-year Renewals	The last date to order 1-year maintenance renewals.	July 31, 2019
End of Support	The last date that support calls will be accepted for the affected product. RMA's will no longer be provided or supported on the product.	July 31, 2020

2010年頃にリリースしたSシリーズについては、EOSが2020年と、約10年近くも販売開始からサポートした実績があります。
※現在販売のモデルも同様の期間サポートするという保証するものではございません。

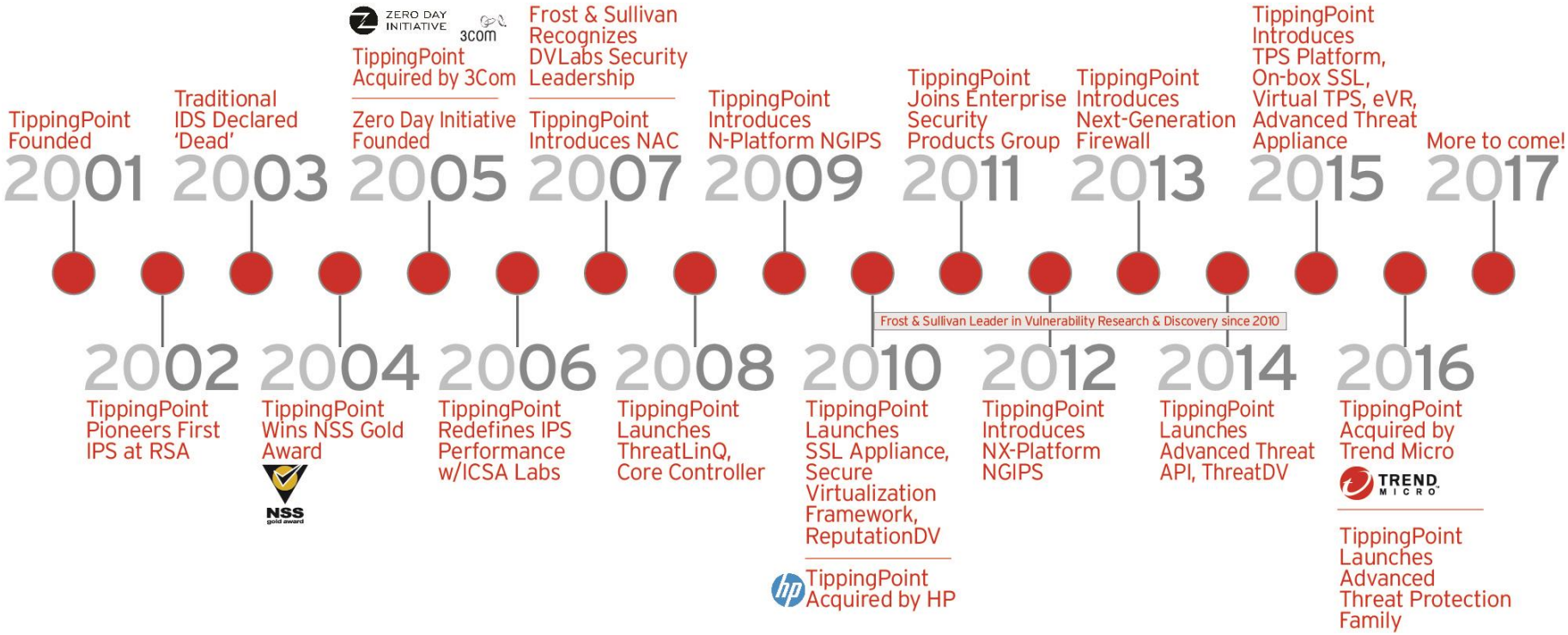
他社類似製品は**平均5年**に対し、
倍以上のMTBF結果(10年以上)

安定化試験（リーチインチャンバー）装置をHW製造元・開発元に設置。高温、多湿など様々な環境下において、HW部品などの故障率について厳格な試験を実施しリリースしています。結果として、故障平均時間(MTBF)についても**13～15年**という時間を実現しています。

S1020F/S1050F/440T	S3010F/S3020F/2200T
AC	AC
4/2 Amp	12/6 Amp
90 - 264 V	90 - 264 V
85%	85%
47-63 Hz	47-63 Hz
142W	493W
484 BTU/hr	1341 BTU/hr
1.73	3.46
4.40	8.80
16.78	16.77
42.62	42.60
17.72	18.70
45.00	47.50
15.28	22.66
6.93	10.28
7.36	9.10
18.70	23.10
21.93	21.26
55.70	54.00
24.49	30.12
62.20	76.50
25.35	35.32
11.50	16.02
131,238 hrs (15.0 years)	113,194 hrs (12.9 years)

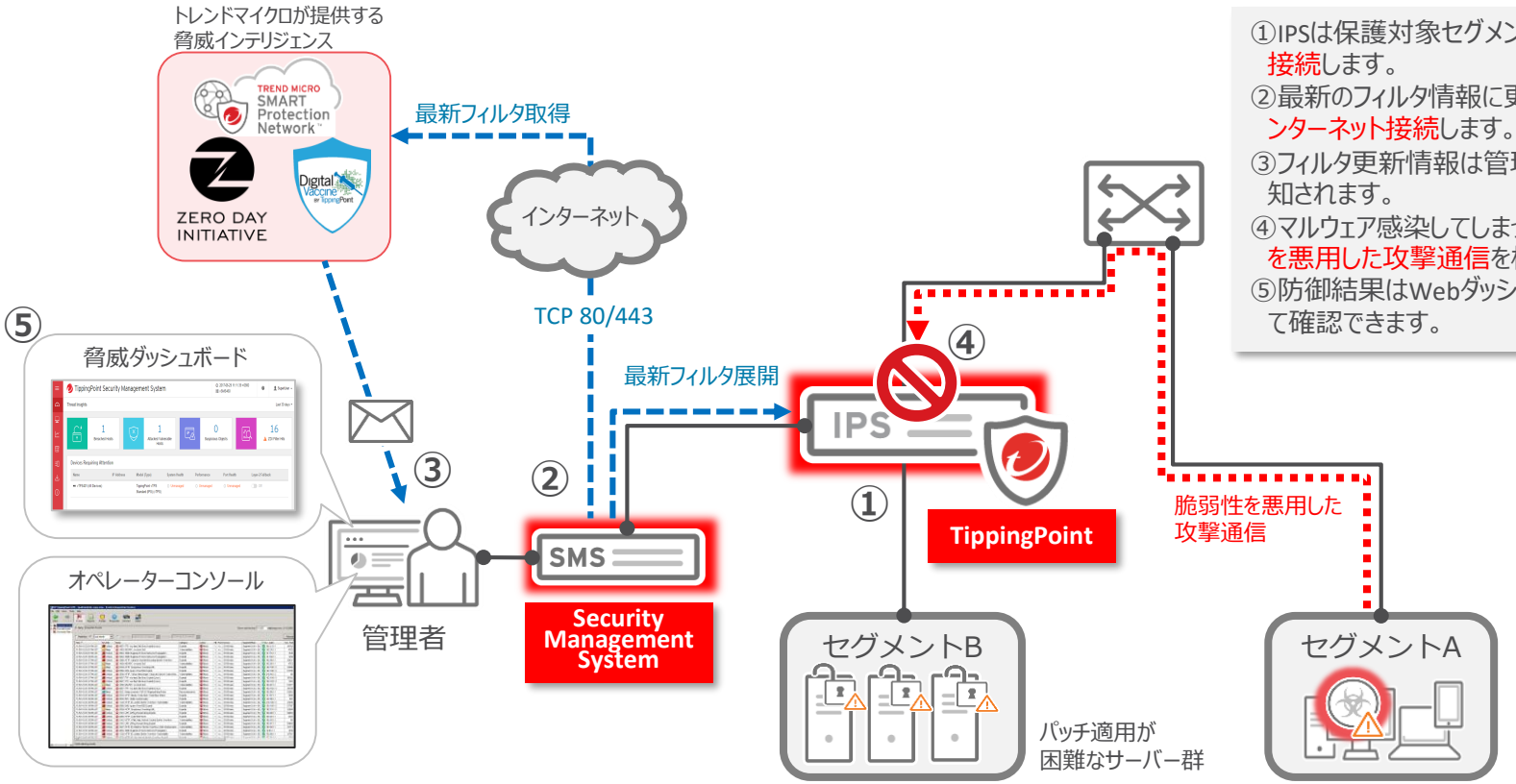
他社IDS/IPSのMTBF（平均故障率）**平均5年**に対し、**倍以上の結果**に

TippingPointの歴史



製品ラインナップとライセンス

仮想パッチシステム構成イメージ



①IPSは保護対象セグメントの上位でインライン接続します。
②最新のフィルタ情報に更新するためにSMSをインターネット接続します。
③フィルタ更新情報は管理者宛ににメールで通知されます。
④マルウェア感染してしまった端末からの脆弱性を悪用した攻撃通信を検知し、ブロックします。
⑤防御結果はWebダッシュボードで数値化されて確認できます。

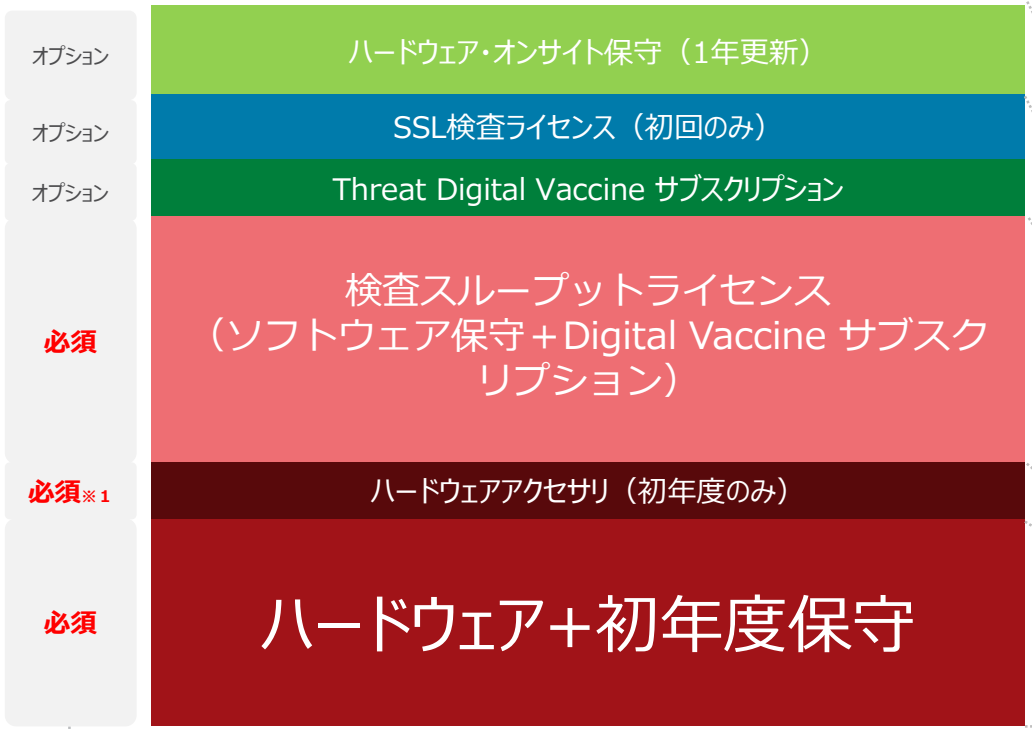
TippingPoint 製品ラインナップ

Threat Protection System		SMS
Tシリーズ	**TXシリーズ** NEW	
物理/仮想アプライアンス	物理アプライアンス	物理/仮想アプライアンス
 440T 2200T	 8200TX 8400TX	 SMS H3 SMS H3 XL
• 最新シリーズ（Nシリーズの後継） • 小中規模環境向けエントリーモデル • NWインタフェース：固定（ZPHA内蔵） • 検査スループット可変 • SSLインスペクション機能（2200Tのみ） • サンドボックス型製品と連携	• 最新シリーズ（NXシリーズの後継） • 大規模環境向けハイエンドモデル • NWインタフェース：モジュール式* • 検査スループット可変 • SSLインスペクション機能 • サンドボックス型製品と連携 • スタック構成で120Gbpsまで拡張可能	• TP専用 統合管理サーバ • Javaクライアントによる詳細設定・監視・機器管理・レポート作成 • Webポータル（SMS Threat Insight）による閲覧機能 • DDIとの連携
440T, 2200T, vTPS	8200TX, 8400TX	SMS H3, SMS H3 XL, vSMS

* I/Oモジュール，トランシーバ等が別途必要になります

ライセンスの考え方

初年度



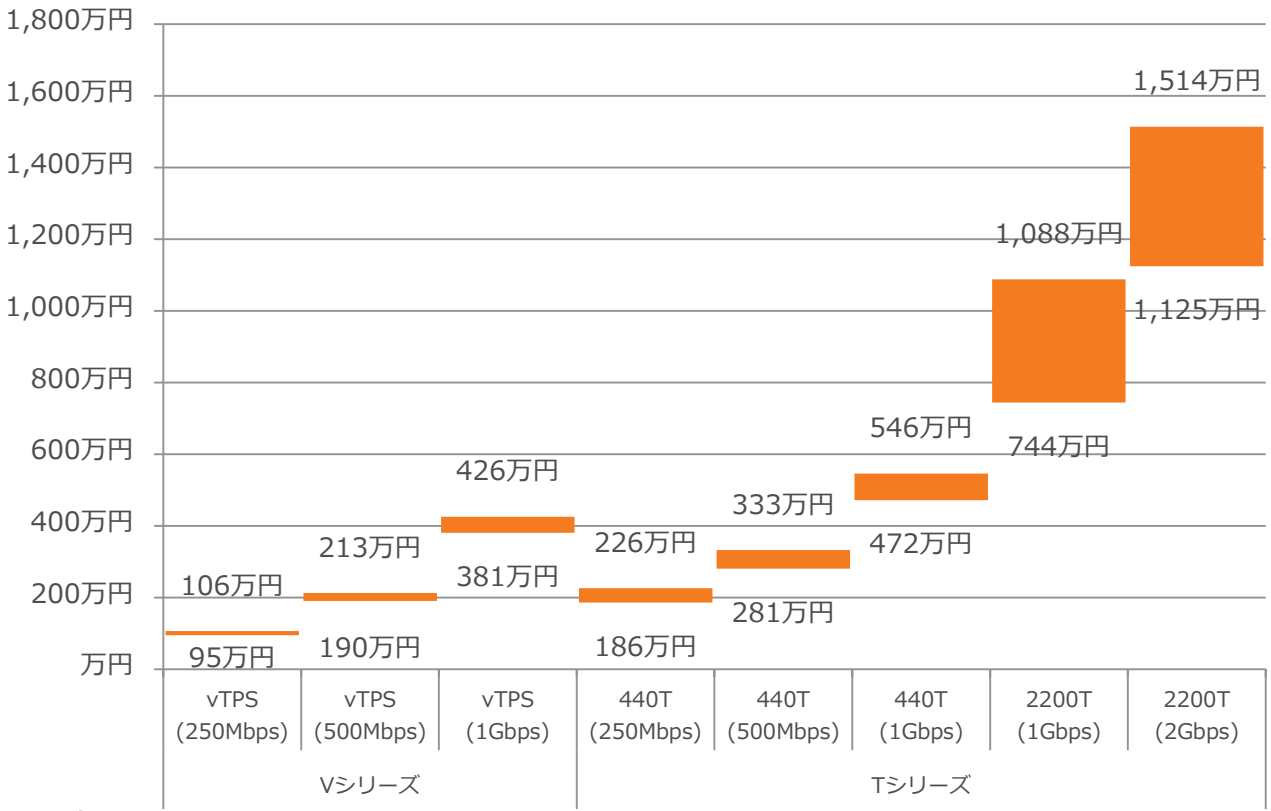
次年度以降

機種-検査スループット対応一覧

モデル	検査スループット／ThreatDVスループット（bps）											SSL検査
	250M	500M	1G	2G	3G	5G	10G	15G	20G	30G	40G	
vTPS	✓	✓	✓									✓*
440T	✓	✓	✓									
2200T			✓	✓								✓
8200TX					✓	✓	✓	✓	✓	✓	✓	✓
8400TX					✓	✓	✓	✓	✓	✓	✓	✓

* vTPS “Performance image” のみ対応

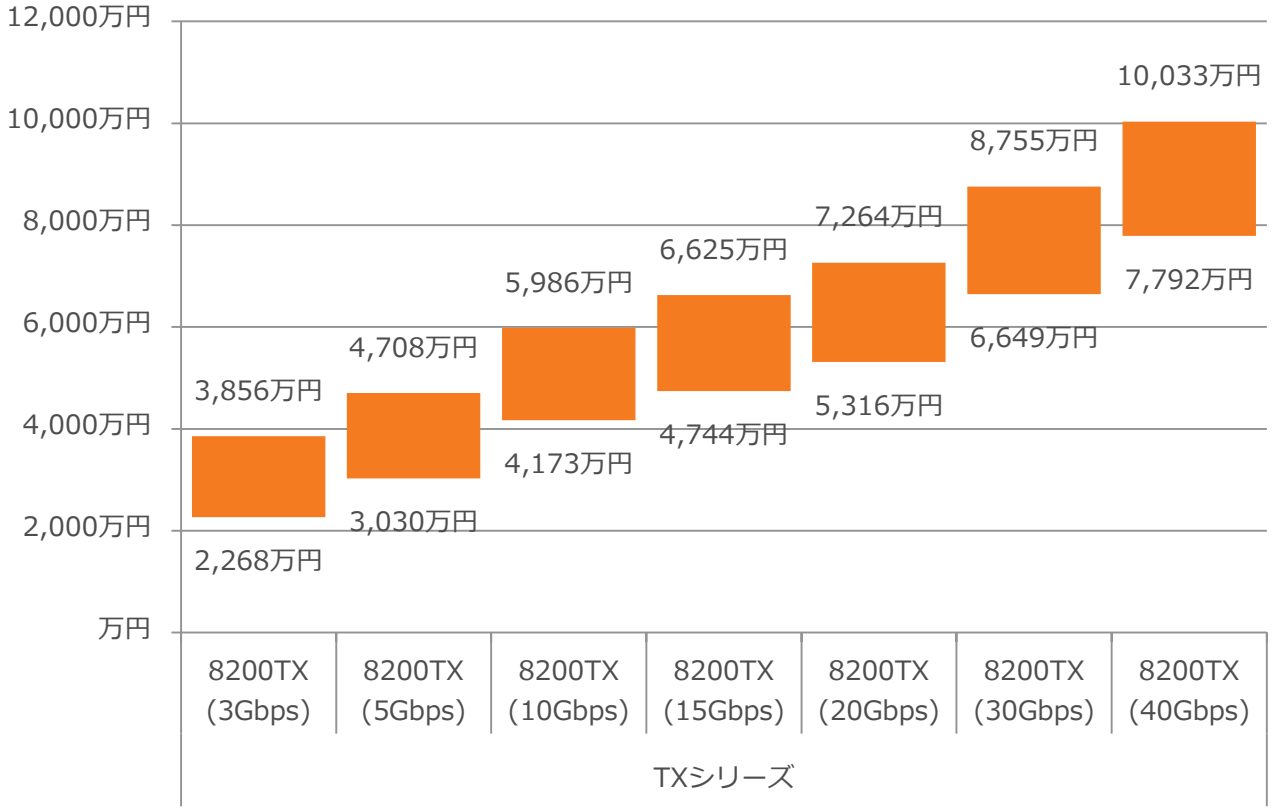
T/vTPSシリーズ 価格帯イメージ



*1 最低価格時の製品構成
HW+Support （vTPSを除く）
+ Inspection Lic.+Support+DV

*2 最高価格時の製品構成
HW+Support （vTPSを除く）
+Inspection Lic.+Support+DV
+Threat DV
+SSL Inspection （440Tを除く）
+HW On-site support(4Hr)

8200TXシリーズ 価格帯イメージ



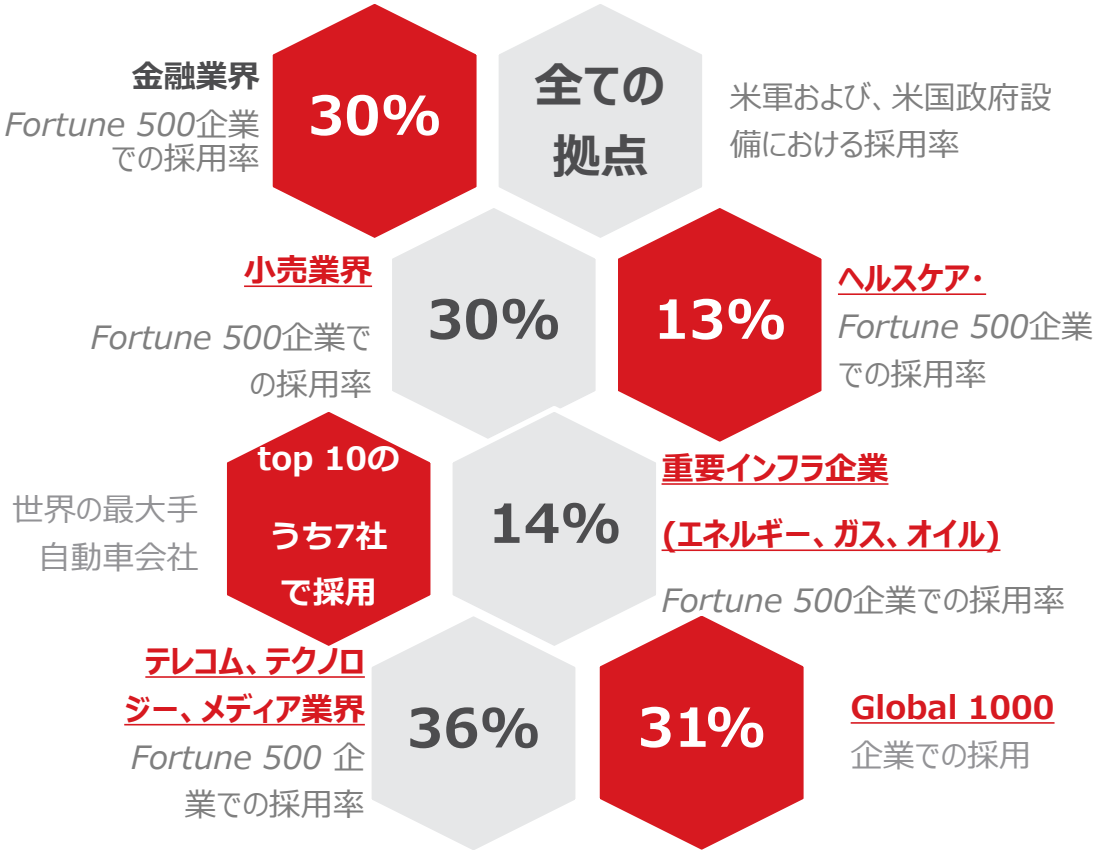
*1 最低価格時の製品構成
HW+Support
+ Inspection Lic.+Support+DV
+IO Module: 6-segment Gig-T x 1

*2 最高価格時の製品構成
HW+Support
+Inspection Lic.+Support+DV
+Threat DV
+SSL Inspection
+HW On-site support(4Hr)
+IO Module: 2-segment 10G Fiber LR Bypass x 2
+Transceiver: 10G SFP+ LC LR Transceiver x 8

導入事例のご紹介

全世界でご利用いただいています

具体的な導入例



まとめ

1. 増え続ける脆弱性に対し、目を背けることはできない
2. “仮想パッチ”の導入により計画的な脆弱性対策計画を行う
3. 対策ソリューションの検討ポイントは、“導入・運用・サポート”

Trend Micro TippingPointは
チューニングレス”、“高い検知率”、“柔軟な導入”
が可能な次世代型IPS製品です。