インシデントレスポンスに求められる
脅威のモニタリングと標的型攻撃の可視化の必要性

アーバーネットワークス株式会社
シニアシステムズエンジニア
藤原　哲士

目次

1．アーバーネットワークスの紹介

アーバーネットワークスとは

本社所在地：米国マサチューセッツ州バーリントン

- 主要海外拠点：ロンドン、シンガポール、東京

沿革

- 2000年　米国マサチューセッツ州バーリントンで設立
- 2005年1月　1st ワールドワイド・インフラストラクチャ・セキュリティ レポート発表
- 2013年9月　Packetloopを買収

事業内容

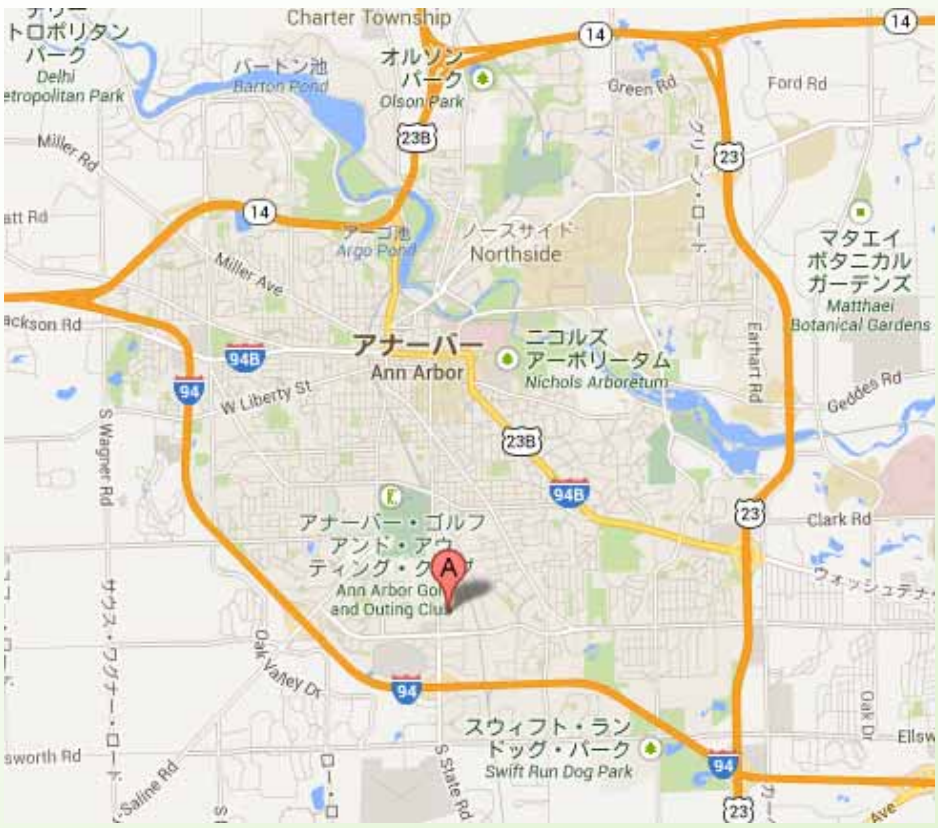
- キャリア・ネットワーク、データセンター、エンタープライズ向け、ネットワーク・セキュリティ/マネージメント・ソリューションの提供

主な製品 / ソリューション

- Arbor SP/TMS（サービス・プロバイダ向けDDoS対策ソリューション）
- Arbor APS（Availability Protection System: エンタープライズ向けDDoS対策ソリューション）
- Arbor Spectrum（エンタープライズ向け内部脅威検知、セキュリティインシデント分析ソリューション）
- Arbor Cloud （クラウド型DDoS対策ソリューション）

アーバーネットワークスとは

アーバーネットワークスとは

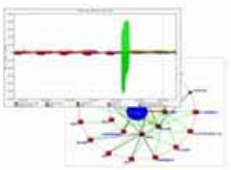


アーバーネットワークスとは

ARBOR NETWORKS

アーバーネットワークス　１７年間の軌跡

Arbor Networks設立
(ミシガン大学の
セキュティ研究より)



(ピアリング分析・
インフラの視認性)

Arbor SP TMS

DDoS Mitigation
市場に参入
(TMS 2700: 3Gbps)

Arbor SP TMS
10Gbps
DDoS Mitigation

INFONETICS RESEARCH

市場全体の61%の
シェアを持ちArborは
DDoS市場のリーダに
(インフォネティクス
リサーチ社より)

Arbor SP TMS
HD1000 100Gbps
DDoS Mitigation

2000 2002 2004 2005 2006 2008 2010 2012 2015 ソチ オリンピック 2016

2002
バンクーバー
オリンピック

2010
ロンドン
オリンピック

2015
リオ
オリンピック

Arbor SP

(Flowベース分析による
業界初のキャリア
クラスのDoS検知
ソリューション)

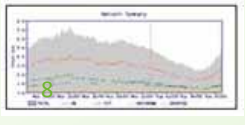
1st ワールドワイド・
インフラストラクチャ・
セキュリティ・レポート

ATLAS®
(世界初のグローバル
な脅威分析)

Arbor APS
インライン型DDoS
Mitigation

Spectrum
内部モニタリング、
脅威の可視化

Arbor SP TMS
TMS4000 40Gbps
DDoS Mitigation



8

アーバーネットワークスのビジョン

何が起こっているのかを可視化をすることが、脅威への適切な対応を可能にする

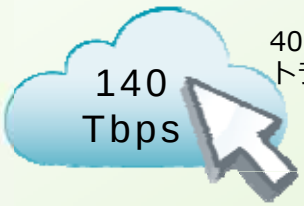
- 広大なインターネットのトラフィックの可視化
- 不正な通信を可視化し、ポリシーに準じてクリーニング
- 培った可視化技術を企業内のネットワークにも適用、リアルタイムでモニタリング
- 内部に潜む不正な通信を可視化

ARBOR NETWORKS

世界最大級のネットワーク監視システム

90% Tier1サービスプロバイダの90%がARBORのお客様

ARBORの製品は
107ヶ国に展開



40%のインターネット・
トラフィックをATLASで監視

40% by
139 ISPs

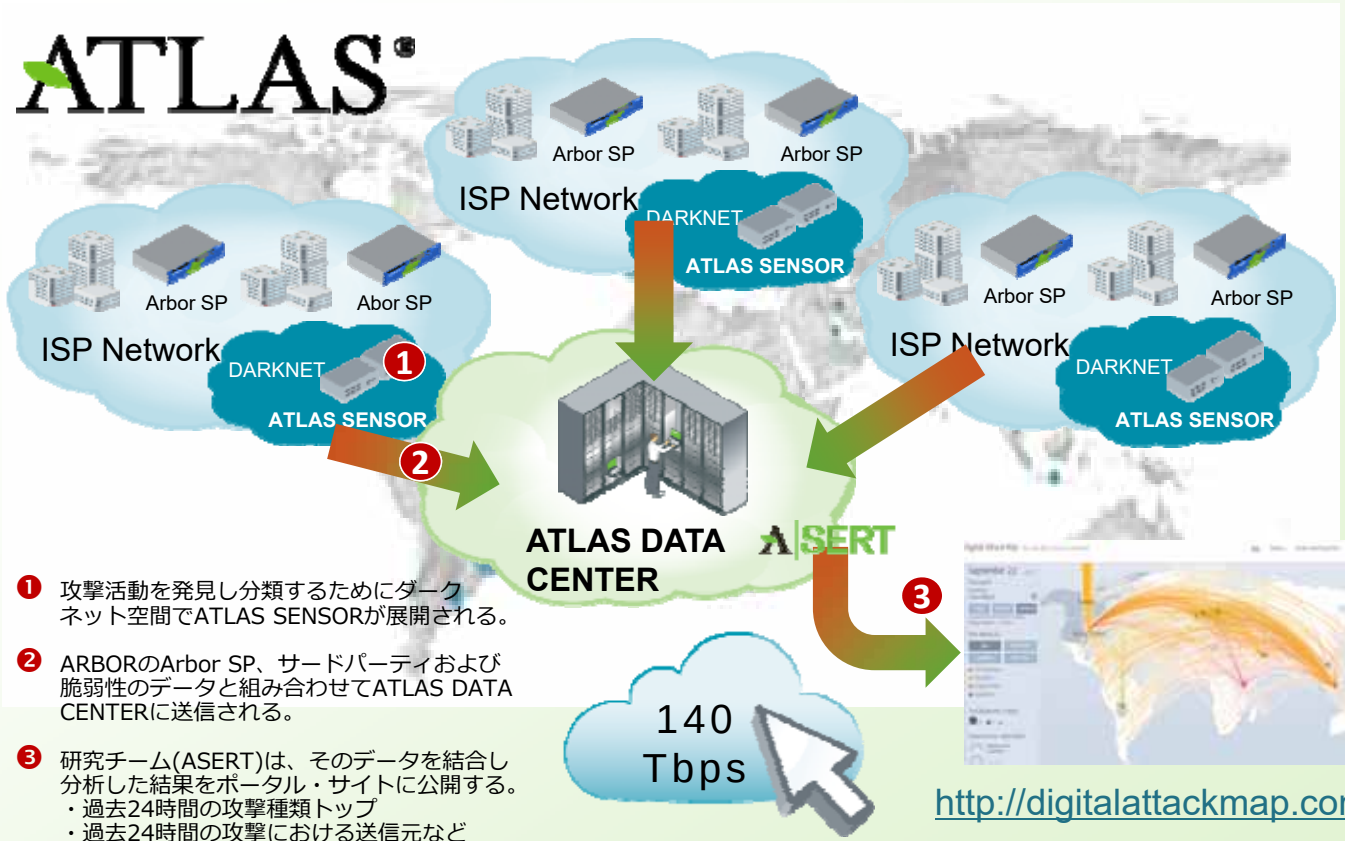
さらに下記のデータソースを保有
- IPv4 2.63億（総数約43億）
- Dark IPv4 176万
- ASN 44,570

ARBORの市場ポジションは
キャリア・エンタープライズ・
モバイルのDDoS市場において
61%のシェア
[Infonetics Research Dec 2011]

17 ARBORは革新的なセキュリティと
ネットワーク可視化技術を17年間に渡り提供

ARBOR NETWORKS

ATLAS (Active Threat Level Analysis System：脅威レベル解析システム)



❶ 攻撃活動を発見し分類するためにダークネット空間でATLAS SENSORが展開される。

❷ ARBORのArbor SP、サードパーティおよび脆弱性のデータと組み合わせてATLAS DATA CENTERに送信される。

❸ 研究チーム(ASERT)は、そのデータを結合し分析した結果をポータル・サイトに公開する。
・過去24時間の攻撃種類トップ
・過去24時間の攻撃における送信元など

http://digitalattackmap.com/

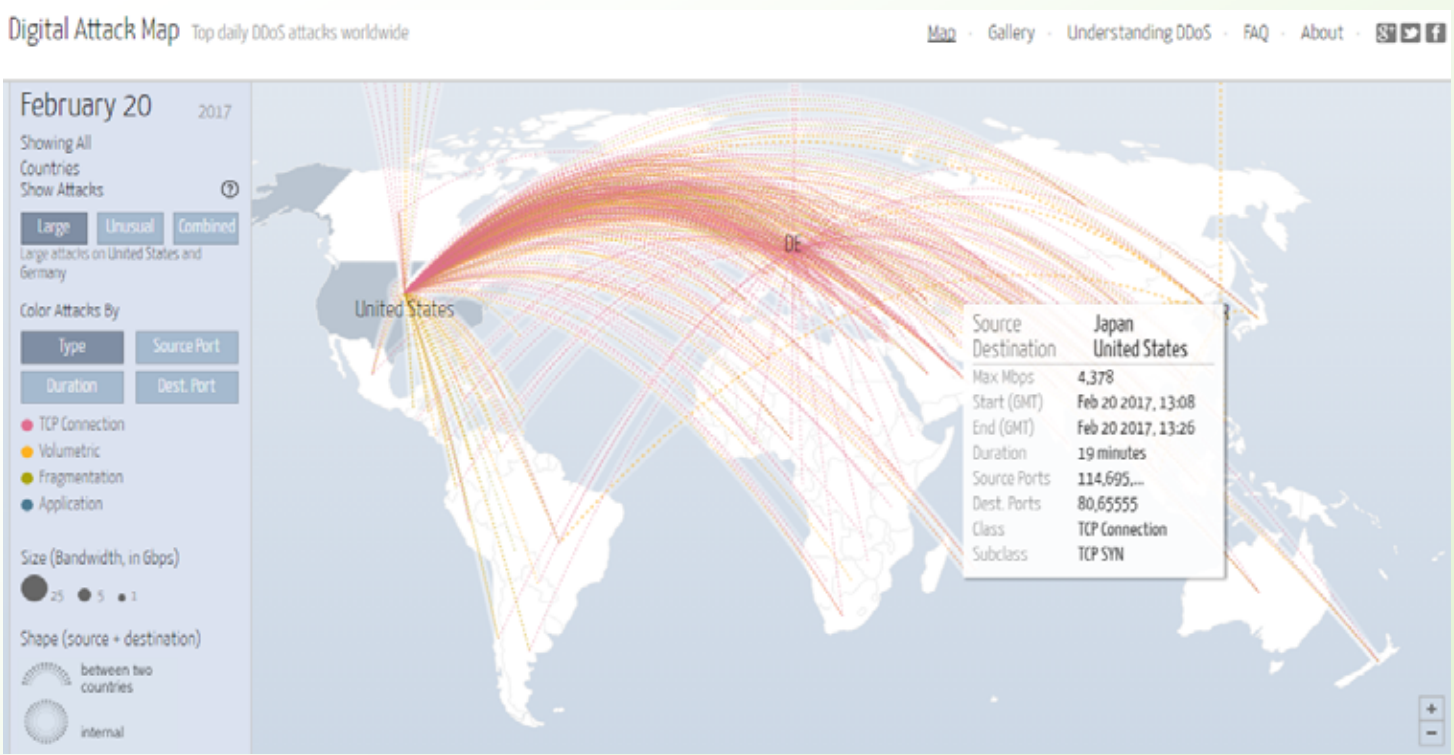
140 Tbps

ピーク時最大140Tbps のインターネット・トラフィックをATLASで収集

ARBOR NETWORKS

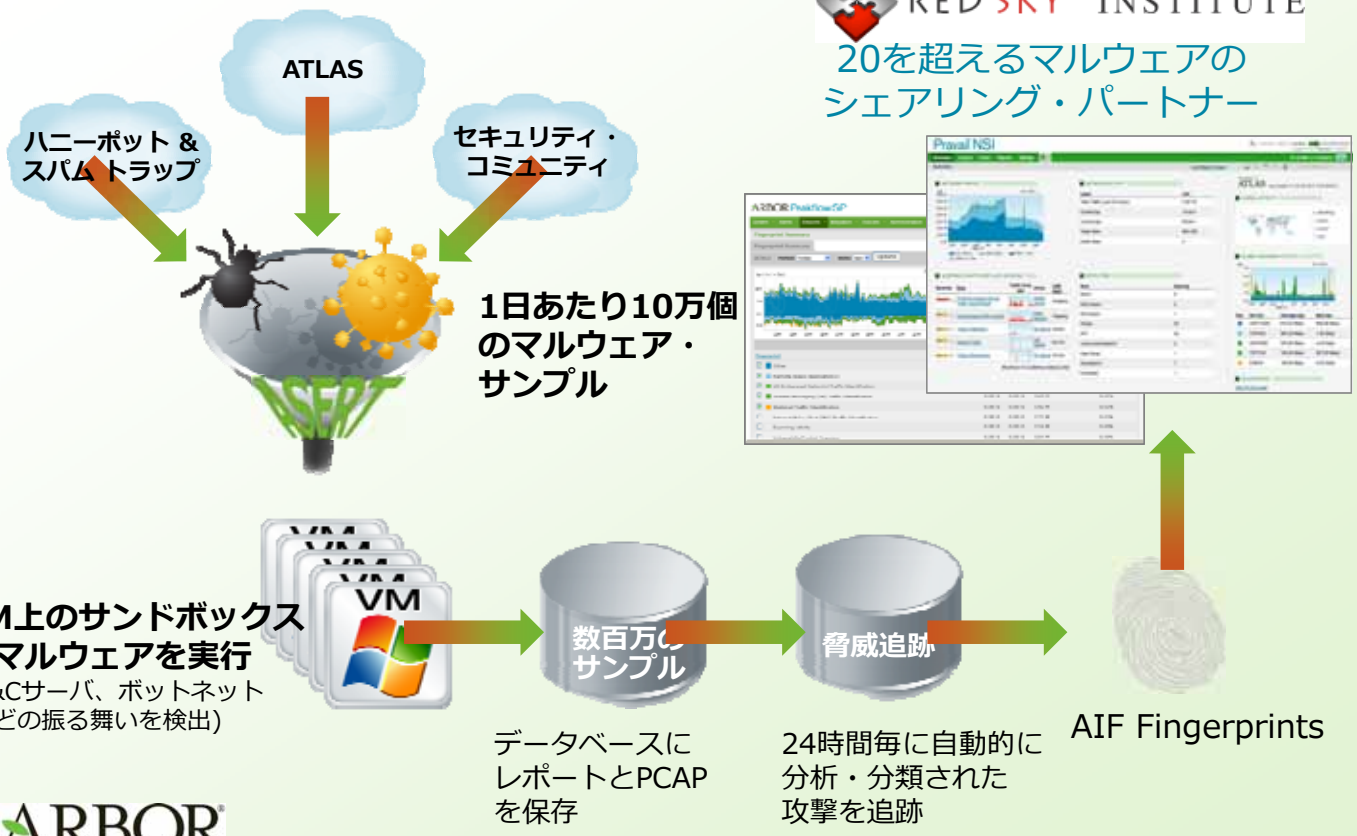
Digital Attack Map

http://www.digitalattackmap.com/



ARBOR NETWORKS

ASERT (Advanced Threat にフォーカスした解析チーム)

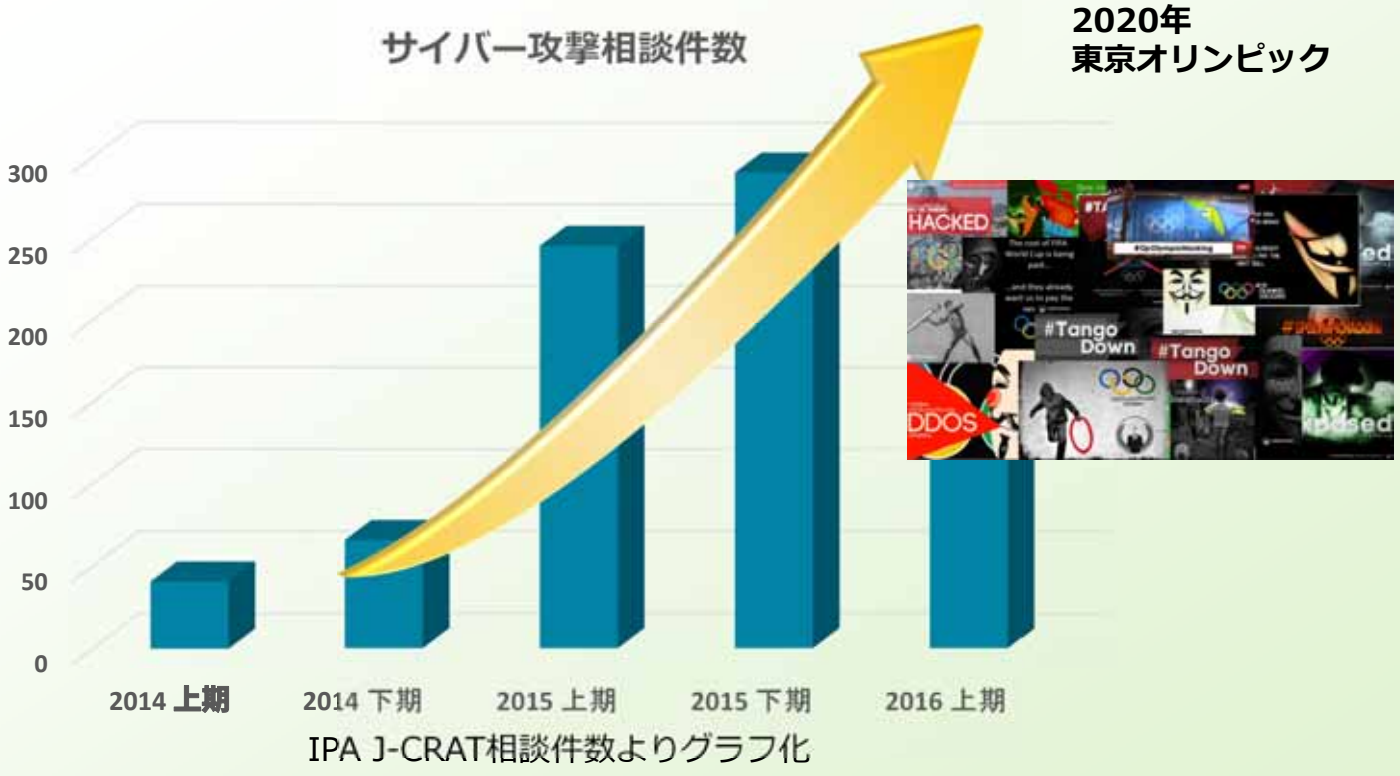


ARBOR NETWORKS

2．サイバー攻撃の増加と標的型攻撃の特徴・対策

ARBOR NETWORKS

増加するサイバー攻撃



2020年
東京オリンピック

IPA J-CRAT相談件数よりグラフ化

ARBOR NETWORKS

リオオリンピックに関連するDDoS攻撃

2015 | 2016 ARBOR

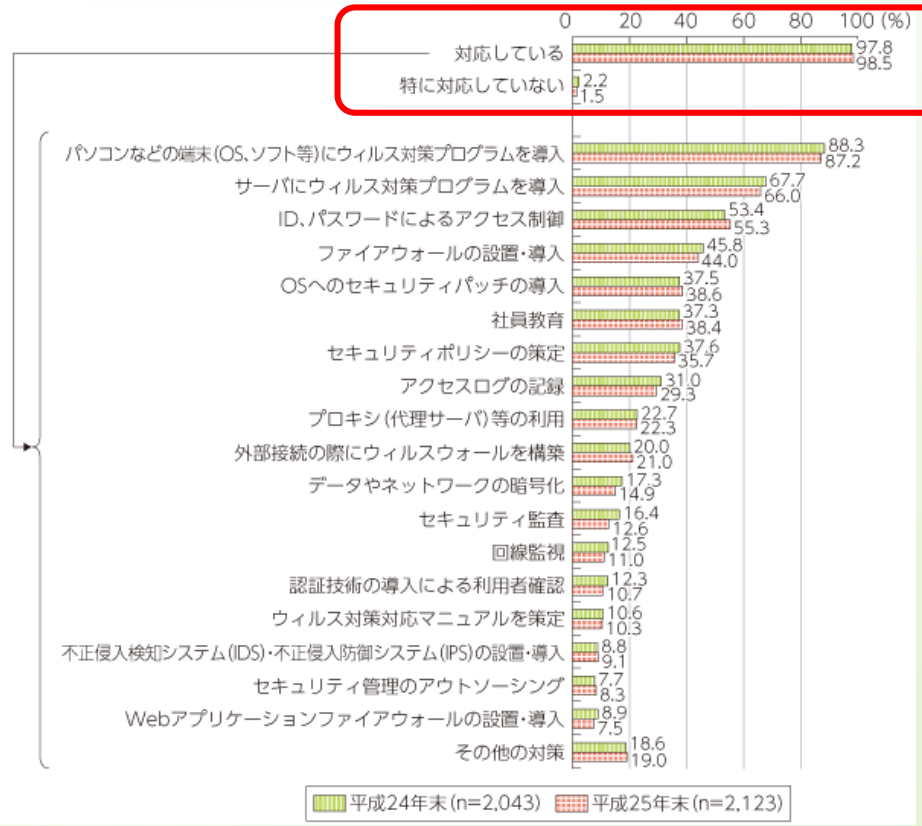
IoT ボットネットによる最初のDDoS攻撃活動

イベント期間中

アーバーネットワークスATLASよりデータ収集

ARBOR NETWORKS

企業のセキュリティ対策の実施状況



ARBOR NETWORKS

総務省H26年度情報通信白書
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/image/n5303080.png

サイバー攻撃への対策（例は一部）

入口対策
- FW
- IPS/IDS
- Sandbox

内部対策
- 認証サーバ
- Anti Virus
- ネットワーク機器

出口対策
- URLフィルタリング
- NG-FW
- Proxy Server

ログ監視、分析
- SIEM 、アクセスログ分析ツール

デジタル・フォレンジック
- コンピュータフォレンジック、ネットワークフォレンジック

ARBOR NETWORKS

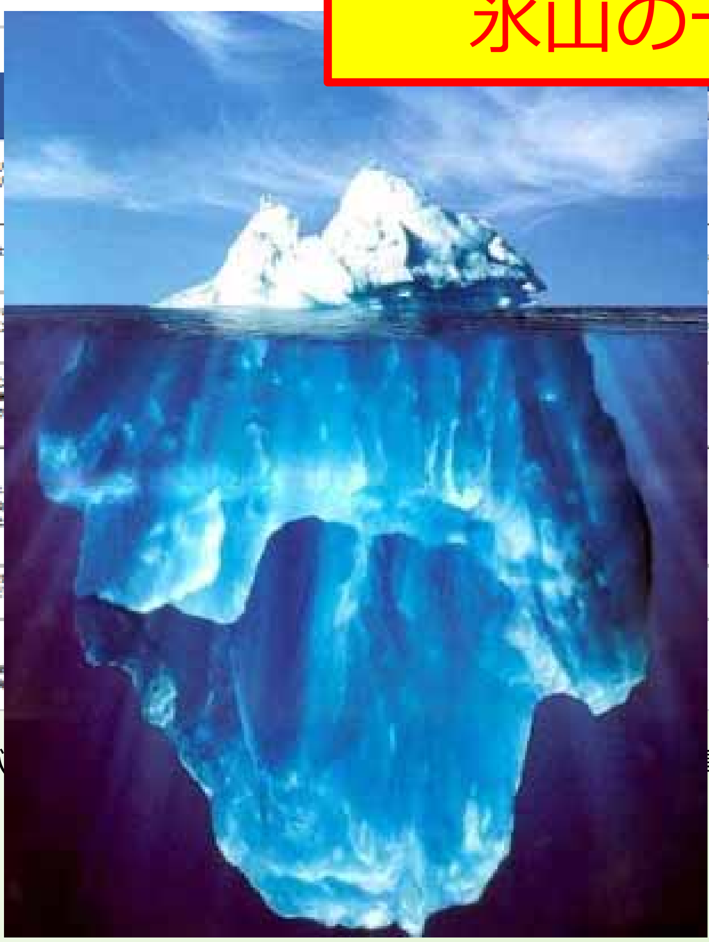
拡大する被害

公表日またはメディア掲載日	業種	詳細	タイトル	サイバー攻撃被害の具体的内容	国内/海外	個人情報（クレジットカード情報を含む）	（漏えい人数）	アカウント情報（ID・パスワード等）	その他の重要情報	改ざん	DoS/DDoS
2016/6/26	⑥公共機関・官庁	地方公務	少年による教育情報システム及び校内LANへの不正アクセスにより、教員及び生徒の個人情報が漏えい	[illegible]	国内	○	不明	○			
2016/6/14	⑤その他のサービス業	旅行業	グループ企業への標的型攻撃により、顧客の個人情報が社外に漏えい	[illegible]	国内	○	34万件				
2016/4/28	③製造業	映像・音声・文字情報制作業	所属アーティスト公式サイトへのコマンドインジェクション攻撃により、キャンペーン応募者の個人情報が漏えいした恐れ	[illegible]	国内	○	35万件			○	
2016/4/22	④情報通信業	民間放送業	FM放送局のWebサーバへのコマンドインジェクション攻撃により、メッセージ投稿者及びプレゼント応募者の個人情報64万件が漏えいした恐れ	[illegible]	国内	○	不明			○	
2016/4/21	④情報通信業	民間放送業	テレビ局のWebサーバへのコマンドインジェクション攻撃により、視聴者からの投稿43万件に含まれる個人情報が漏えいした恐れ	[illegible]	国内	○	不明				
2016/2/5	②医療、福祉	病院	ランサムウェア感染により電子カルテ等のデータが閲覧不可能となり、攻撃者にビットコインを支払ってデータの復号を依頼	[illegible]	海外						
2016/1/31	⑥公共機関・官庁	国家公務	DDoSとみられる攻撃により、複数の省庁のWebサーバにおいて閲覧障害が発生	2016年1月31日夜に複数の省庁（中央省庁5府以上）で閲覧障害が発生した。障害発生の原因は、外部から大量のデータ送信を受けたことによるものと考えられている。	国内						○

※IPA サイバーセキュリティ経営ガイドライン解説書　被害事例より抜粋

ARBOR NETWORKS

拡大する被害



氷山の一角

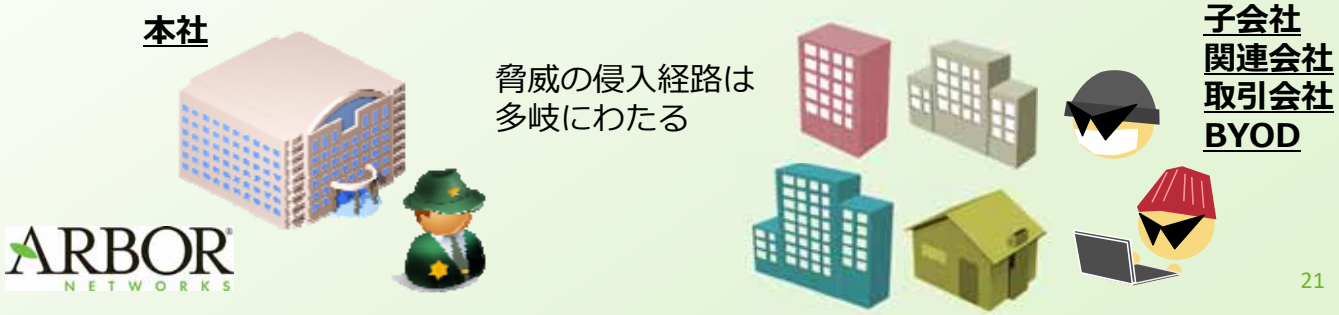
※IPA サイバ　事例より抜粋

ARBOR NETWORKS

拡大する被害

2016/6/14	⑨その他のサービス業	旅行業	グループ企業への標的型攻撃により、顧客の個人情報が社外に漏えい		
当該企業は2016年6月14日、不正アクセスによる個人情報流出の可能性について報道発表を行った。3月15日に同社のインターネット販売を受け持つ子会社の従業員が標的型攻撃電子メールを開封したことにより、子会社の端末がマルウェアに感染した。マルウェア感染後、社内で不審な通信が観測されているほか、社内サーバ内に攻撃者が作成したとみられるCSV形式のファイルが作成され、その後削除された形跡が発見されており、セキュリティ会社を交えた検討の結果、個人情報漏えいの可能性があるとの判断に至っている。漏えいした個人情報は自社分が678万名、このほかに提携先企業が扱う個人情報が34万件以上ある。個人情報の内容には、氏名・性別・生年月日・電子メールアドレス・住所・郵便番号・パスポート番号・パスポート取得日が含まれている。情報漏えいの可能性に関する公表が遅れた理由として、対象者の特定が不十分な				国内	34万件

※IPA サイバーセキュリティ経営ガイドライン解説書　被害事例より抜粋



ARBOR NETWORKS

標的型攻撃の特徴

数字で見る標的型攻撃

7+ Toolkits
2016年の標的型攻撃は平均7個以上のツールを用い、クリティカルな脆弱性を突いていました。

44%
44%の標的型攻撃は直接的にはマルウェアを含んでいませんでした。

25%
2015-2016年にかけて、25%の標的型攻撃はDDoSと同時に行われました。

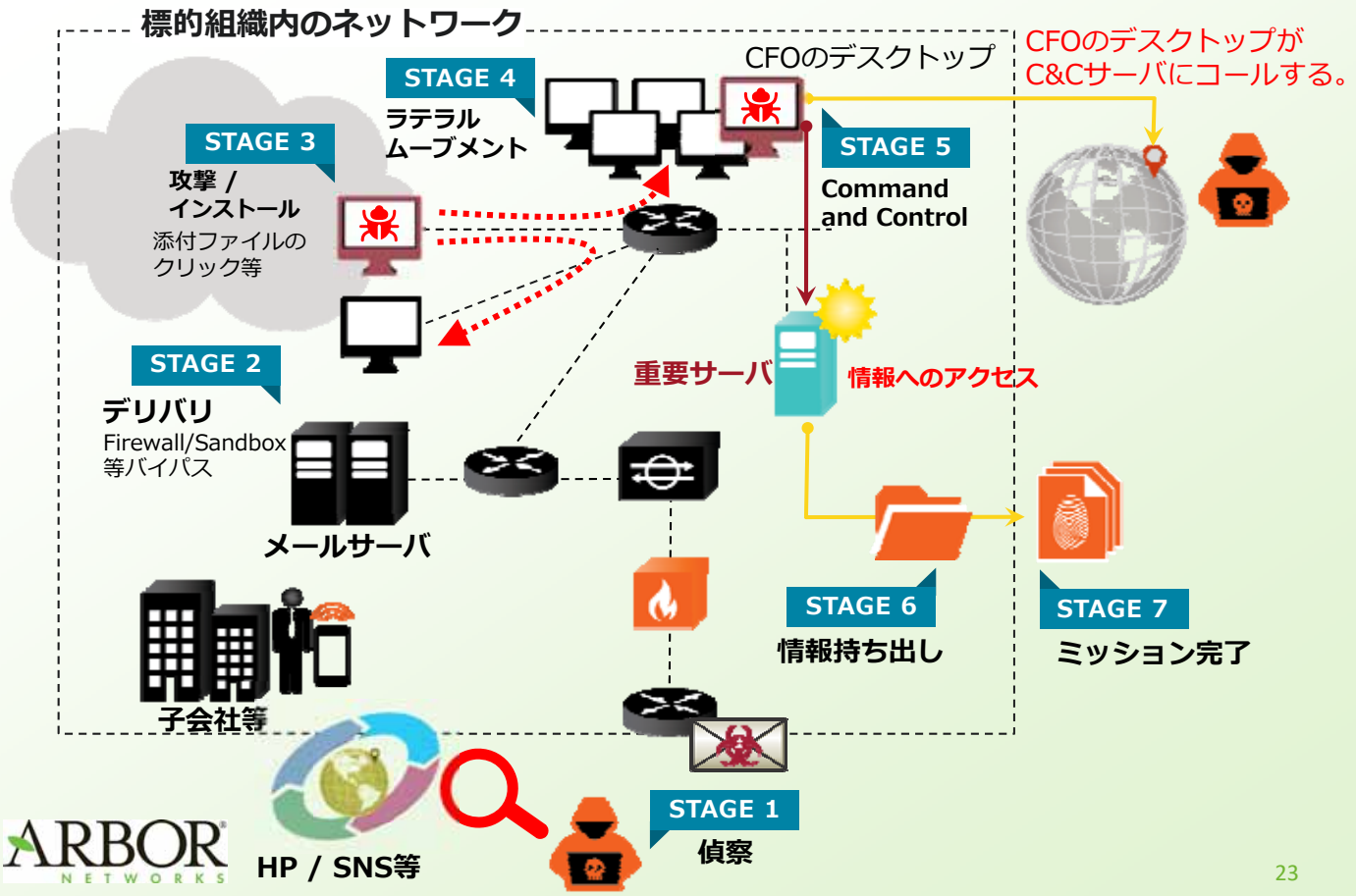
60%
60%の企業はクリティカルなセキュリティインシデントを調査するために、3日間以上要しています。

2016 140+ Days
マルウェアの平均的な潜伏期間は140日を超えています。

※Verizon DBIR, Neustar report, SANS 2016 survey data, IBM CyberSecurity 2016 Surveyより

ARBOR NETWORKS

標的型攻撃キャンペーン一例



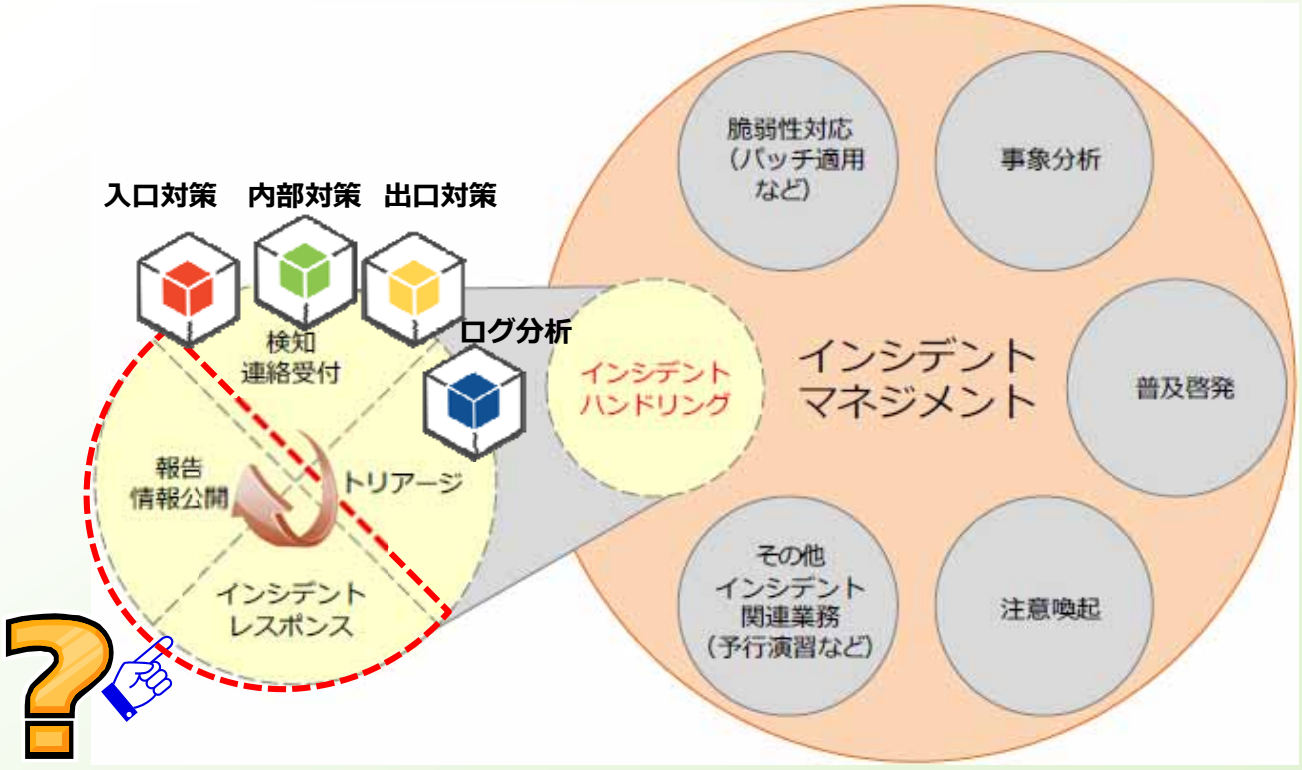
標的型攻撃への考えの変化

攻撃者は執拗な攻撃の中で、たった一度の成功で
100%の目的を達成することができる。

企業は常に勝ち続けなければならないが、
入口対策で100%検知、防御することは不可能。

侵入・感染は止められないが、被害を最小限に食い止めよう！

脅威（インシデント）に対するプロセス



※JPCERT　インシデント
ハンドリングマニュアルより抜粋

3．インシデントレスポンスに求められるもの

インシデントレスポンスとは

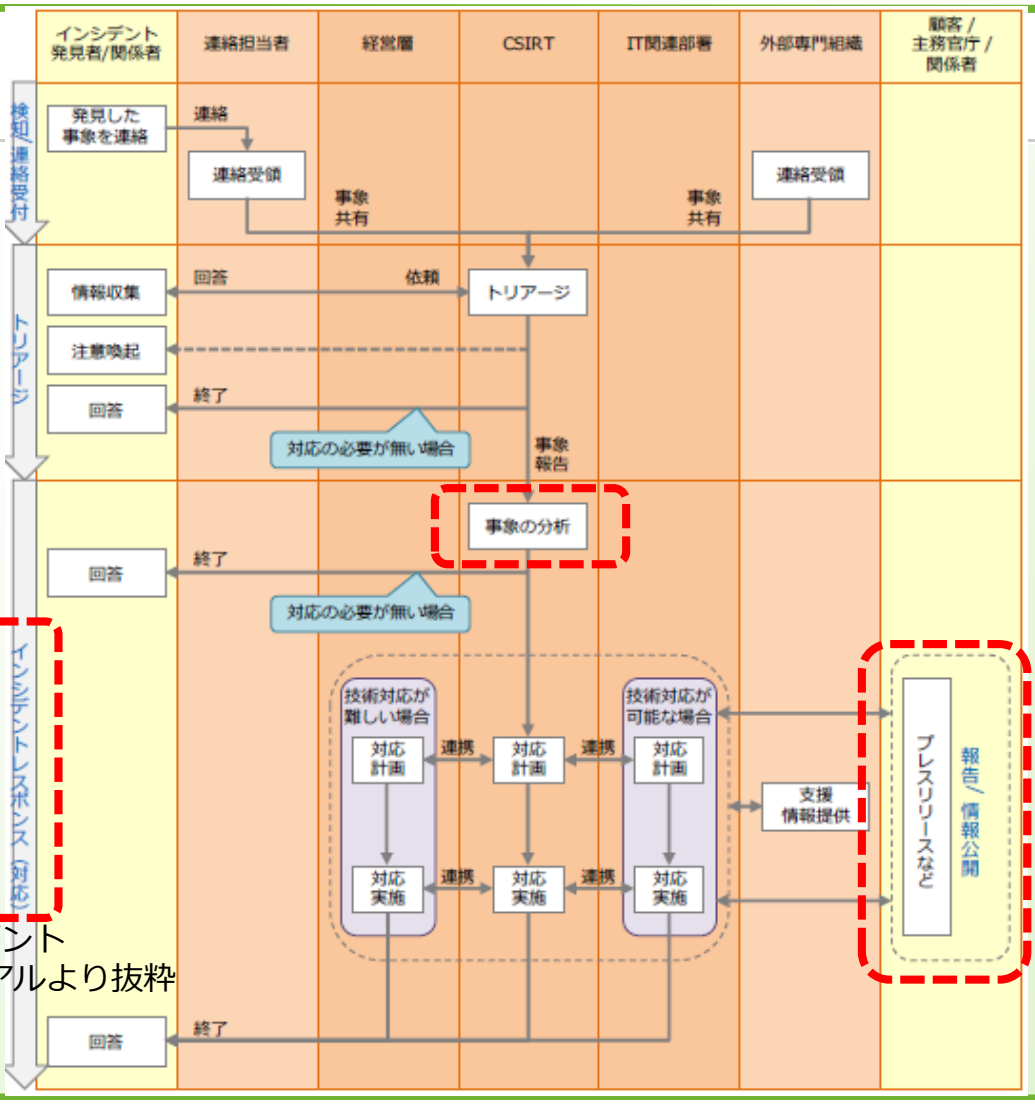
■ デジタル・フォレンジック研究会

コンピュータやネットワーク等の資源及び環境の不正使用、
サービス妨害行為、 データの破壊、意図しない情報の開示等、
並びにそれらへ至るための行為（事象）等への対応等

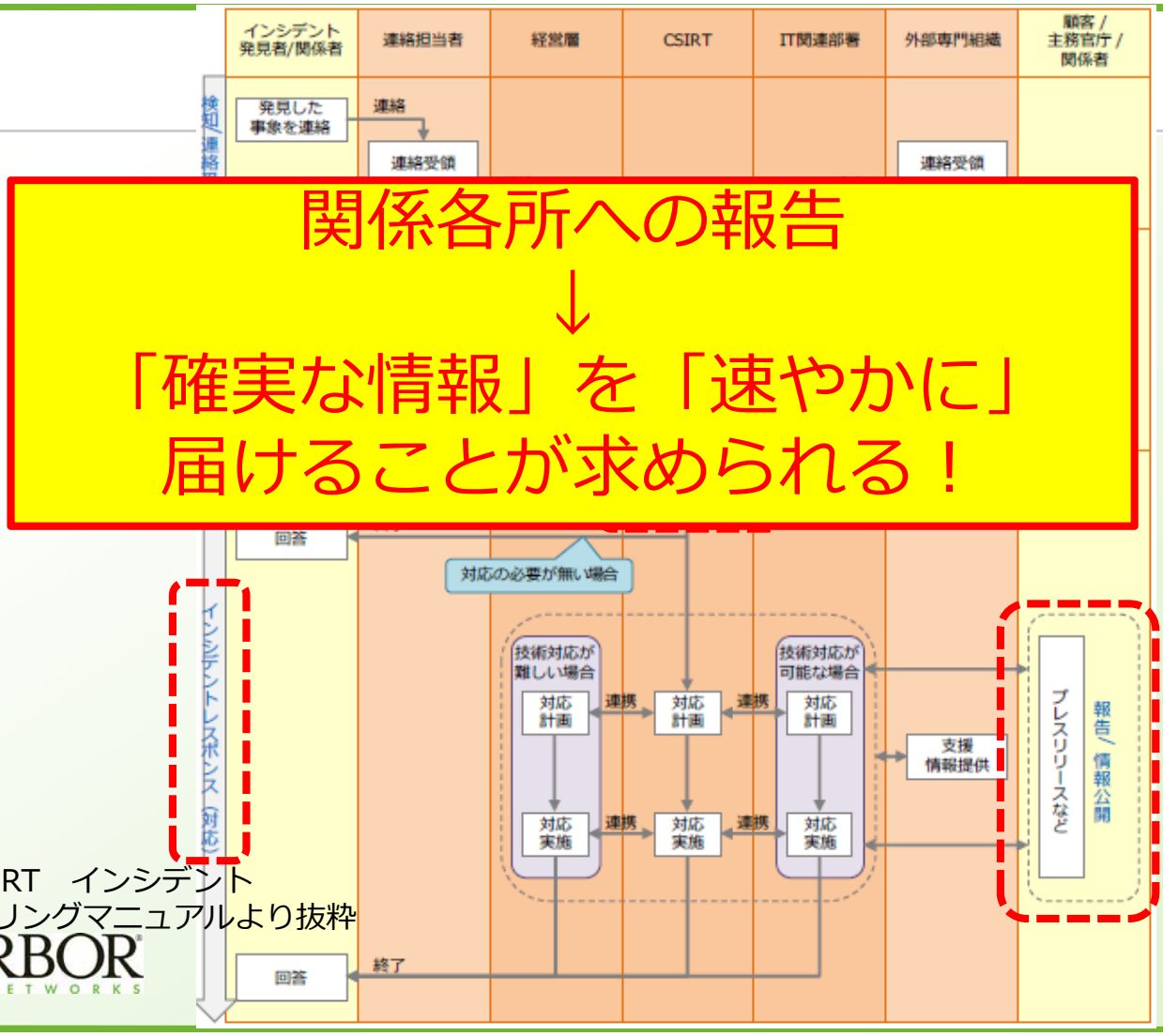
■ JPCERT

インシデントが発生した後の被害を最小限にするための
「事後」対応を、インシデント対応(レスポンス)

https://digitalforensic.jp/home/what-df/
https://www.jpcert.or.jp/ir/#response



※JPCERT　インシデント
ハンドリングマニュアルより抜粋



関係各所への報告
↓
「確実な情報」を「速やかに」
届けることが求められる！

※JPCERT　インシデント
ハンドリングマニュアルより抜粋

もし、、、

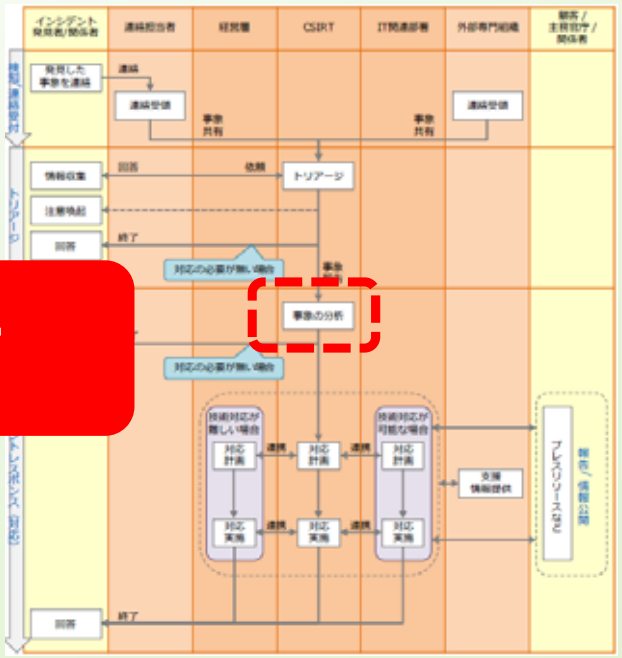
適切なインシデントレスポンスが
なされない場合には、、、

という結果になることもあります。

鍵となる「事象の分析」

インシデントレスポンスの初動対応

事象の分析



鍵となる「事象の分析」

事象の分析

具体的な手順や使用するべきツール、予め準備するリソース等が定義されているものはありません。

NIST National Institute of Standards and Technology U.S. Department of Commerce

行うべき指針は、NISTより勧告されています。

ARBOR NETWORKS

鍵となる「事象の分析」

NIST（米国標準技術研究所）「コンピュータインシデント対応ガイド」（日本語訳：IPA/NRI secure）によると、

インシデント対応チームは、各事件の分析と検証を行うために素早く作業し、各ステップを文書化する。事件が起きたとチームが確信した場合には、チームは迅速に初動分析を行い、影響のあるネットワーク、システム、アプリケーションなどの事件の範囲、事件の犯人や原因、どうやって事件が起きたか(どのツールや攻撃方法が使用されたか、どの脆弱性が悪用されたか)を特定する。初動分析を通じて、事件の封じ込めや、事件の影響のより詳しい分析など、以降の行動に優先度を付けるのに十分な情報を得ることができる。

と記載されています。

ARBOR NETWORKS

「事象の分析」のポイント

- 各ステップを記録、可視化
- 素早く影響範囲を特定
- 事象の根本原因の特定

ARBOR NETWORKS

例えば、、、

ある端末がマルウェアに感染していた！

- 外部から操作された形跡は？
- 影響範囲（他への感染等）は？
- 外部への情報流出の疑いは？
- 関連事象は？その時刻は？
- 疑いの通信のデータはあるか？

ARBOR NETWORKS

例えば、、、

URLフィルタリングシステムにおいて、ある端末がフィッシングサイトへアクセスした事を検知！

- 他に該当URLにアクセスした端末は？
- アクセスした端末の通信状況は？
- その後の端末の挙動は？

ARBOR NETWORKS

例えば、、、

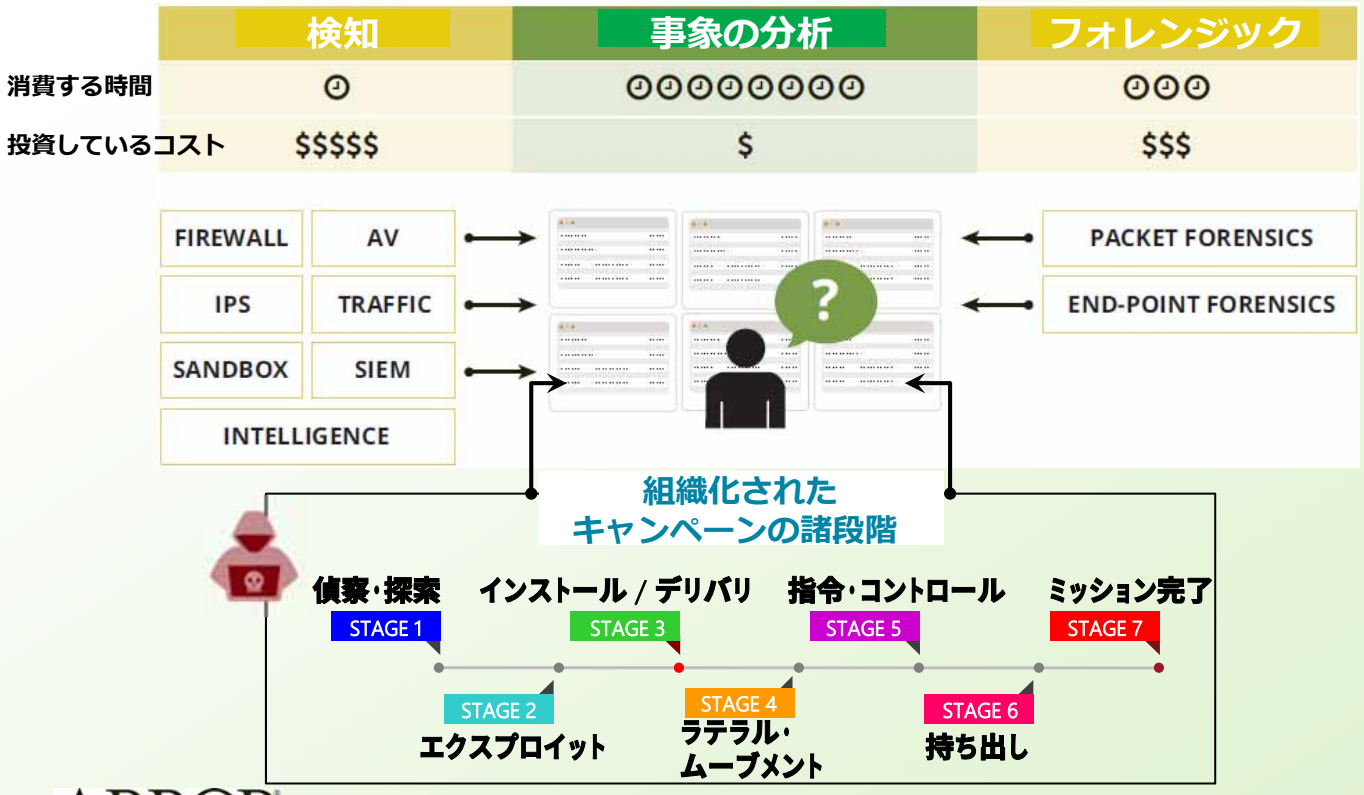
データ漏えいを社外から指摘された！

- 社内の機密情報サーバからデータを多くダウンロードした端末は？
- アクセスした端末の時間も確認したい

ARBOR NETWORKS

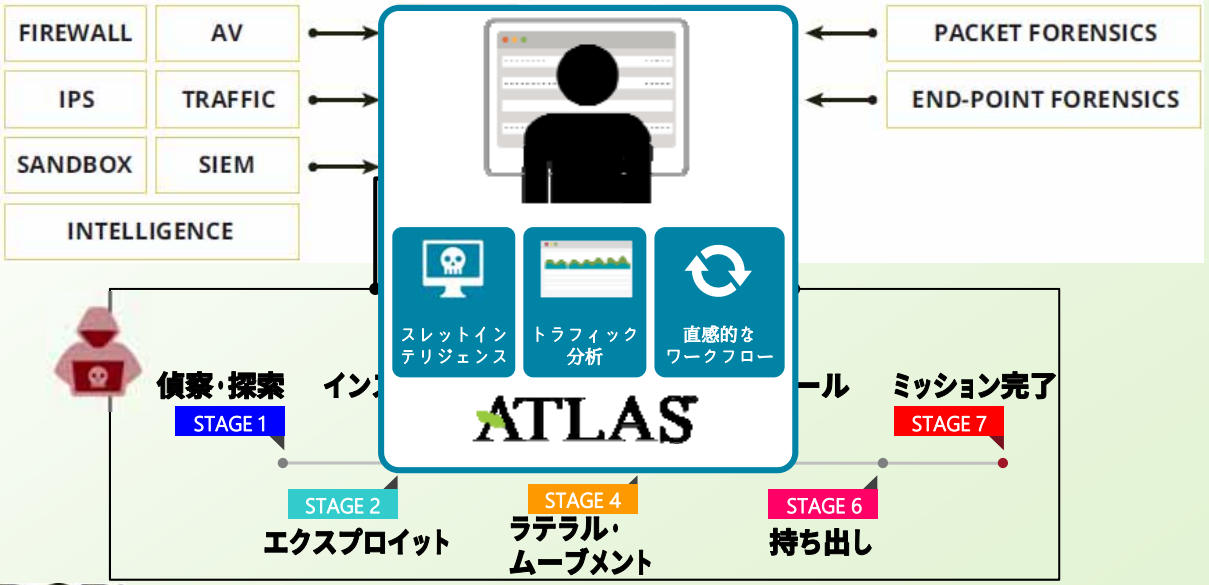
4. 「事象分析」へのアプローチ

従来の手法とインシデントレスポンスのギャップ



事象分析へのアプローチ

	検知	事象の分析	フォレンジック
消費する時間	◷	◷◷◷◷◷◷◷◷	◷◷◷
投資しているコスト	$$$$$	$	$$$



ARBOR NETWORKS

アーバーネットワークスのアプローチ

各ステップを記録、可視化

→ **セキュリティフォレンジック**

素早く影響範囲を特定

→ **内部ネットワークのモニタリング**

事象の根本原因の特定

→ **能動的探索、脅威のハンティング**

ARBOR NETWORKS

アーバーネットワークスのアプローチ（２）

セキュリティフォレンジック

内部ネットワークのモニタリング

能動的探索、脅威のハンティング

インシデントレスポンスの強化
with Arbor Spectrum

ARBOR NETWORKS

他のアプローチ

■SIEM
サードパーティのログを集約、異常分析や相関分析を実行。
あらかじめ定義されたテンプレートや、カスタマイズしたルールによってアラートを生成。
→脅威検知をより高度にするアプローチ。

■デジタル・フォレンジック
ファイルのハッシュ、イメージや操作ログの保存、またネットワークトラフィックの全てを保存して証拠として利活用。
→インシデントに対する証拠提示。

Arbor Spectrumとは異なる手法

ARBOR NETWORKS

Arbor Spectrumを用いた
オペレーションイメージ

注意点

次項より紹介している製品画面キャプチャに
表示されているIPアドレス、ホスト名等は
あくまでも例（細工したデータ）です。
それらが実際に不審なものであるという意味は
ございません。

アーバーネットワークスのアプローチ

各ステップを記録、可視化

セキュリティフォレンジック

素早く影響範囲を特定

内部ネットワークのモニタリング

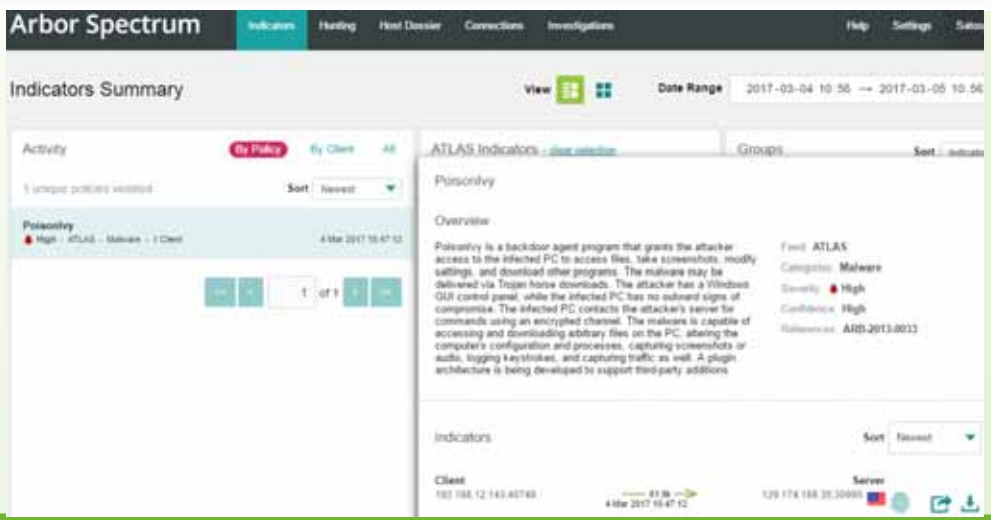
事象の根本原因の特定

能動的探索、脅威のハンティング

ARBOR NETWORKS

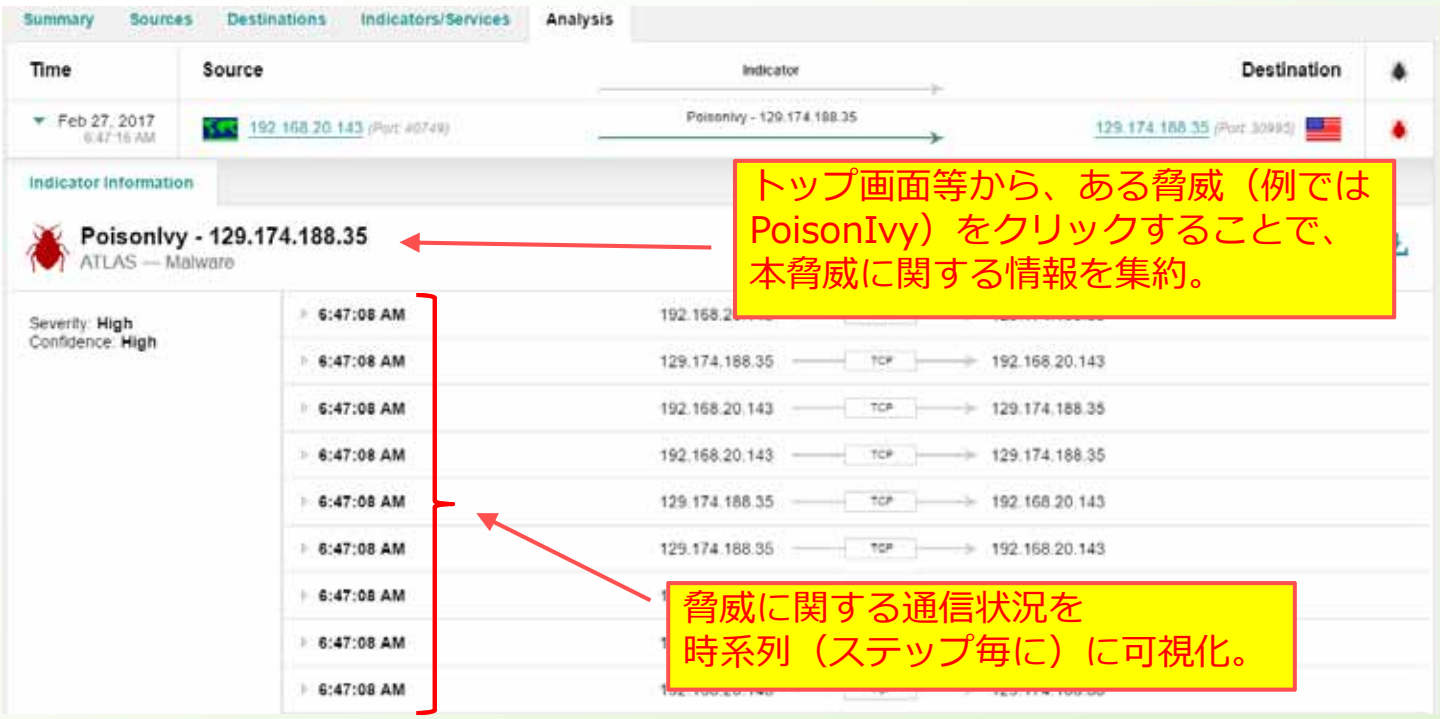
Arbor Spectrum “セキュリティフォレンジック”

【ケース１】
SpectrumにてPoisonIvyを検知。時系列とパケット内容を確認して分析チームにエスカレーションを行いたい。



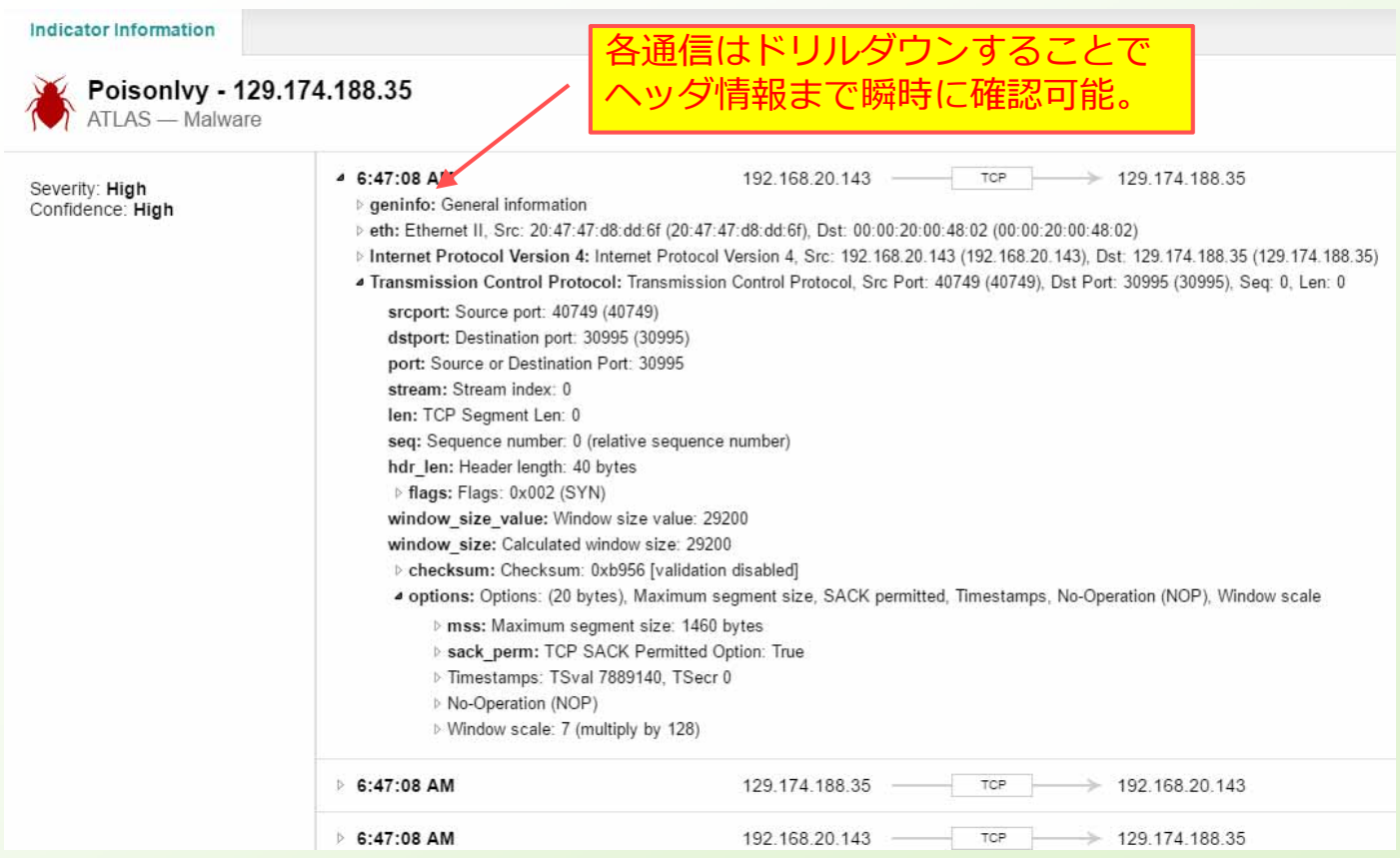
ARBOR NETWORKS

Arbor Spectrum “セキュリティフォレンジック”

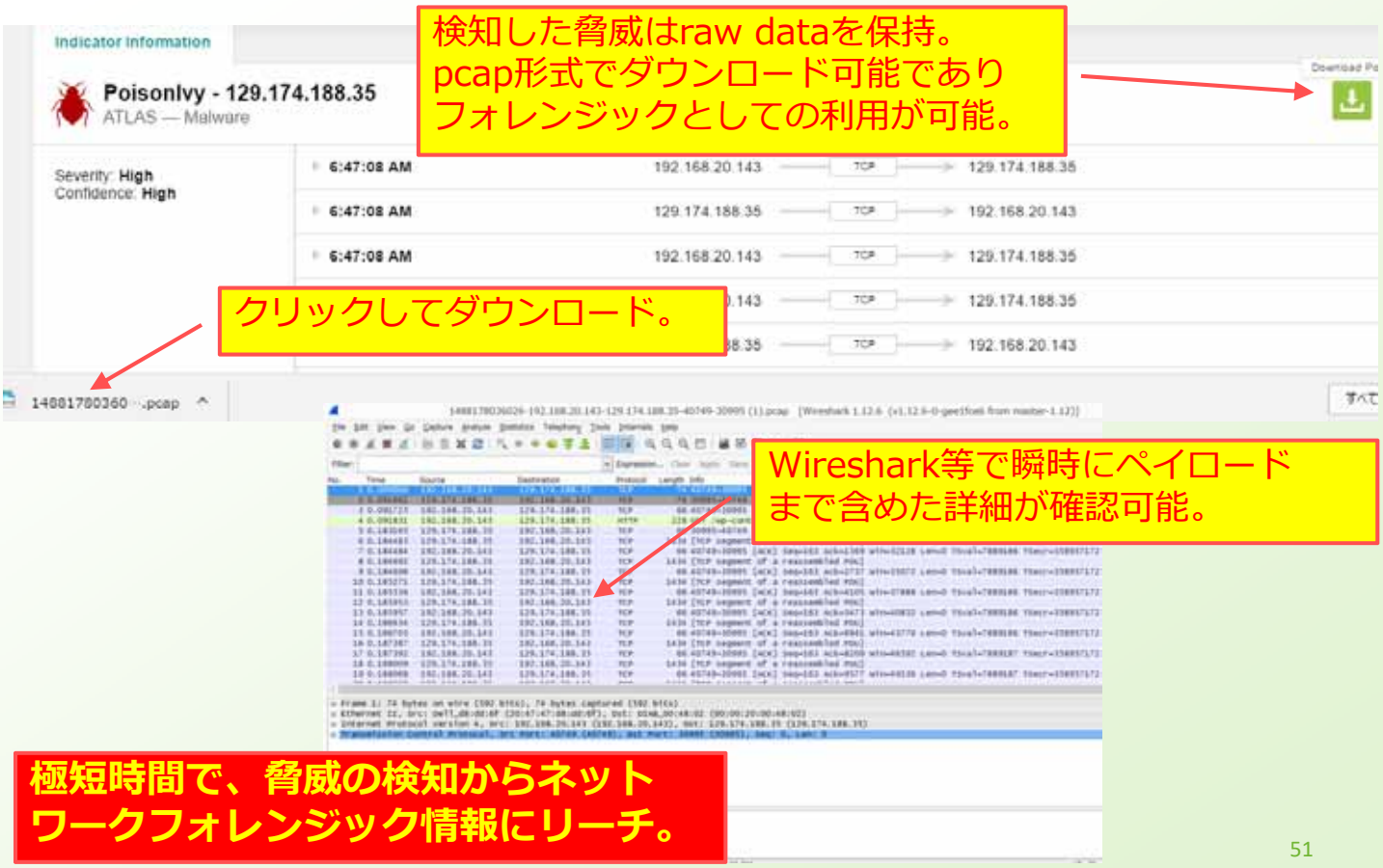


ARBOR NETWORKS

Arbor Spectrum “セキュリティフォレンジック”



Arbor Spectrum “セキュリティフォレンジック”



アーバーネットワークスのアプローチ

各ステップを記録、可視化

セキュリティフォレンジック

素早く影響範囲を特定

内部ネットワークのモニタリング

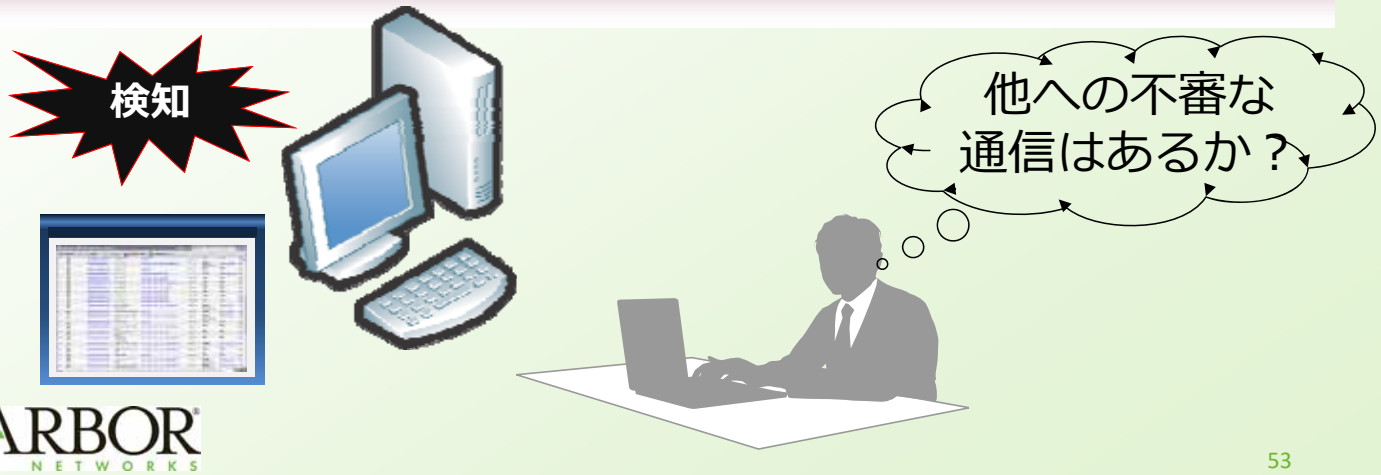
事象の根本原因の特定

能動的探索、脅威のハンティング

ARBOR NETWORKS

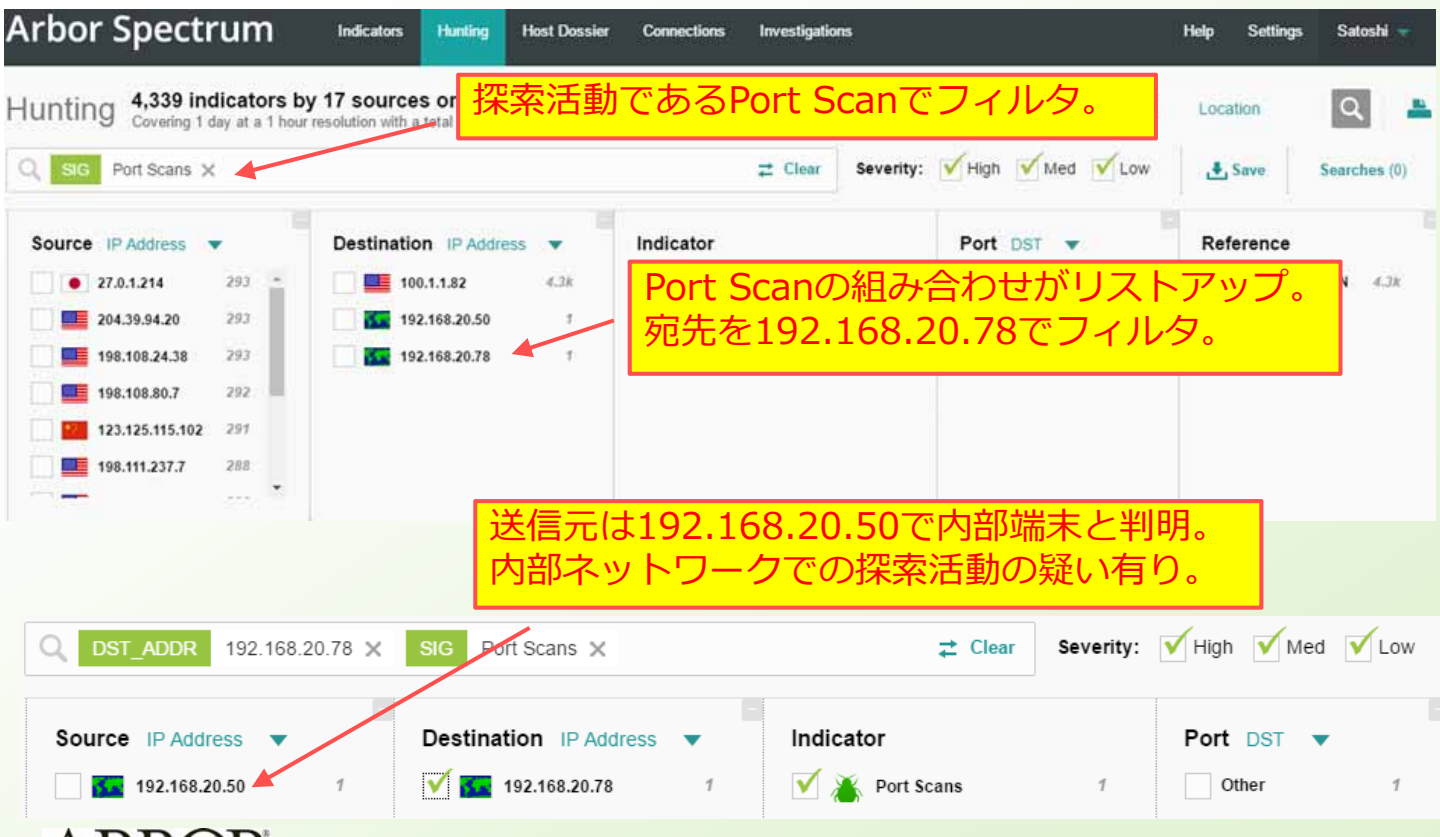
Arbor Spectrum “内部ネットワークモニタリング”

【ケース２】
Spectrum、または他の監視装置において、
ある端末のPortScanを検知。その端末の不審な
挙動を追う為に、通信量含めて確認したい。



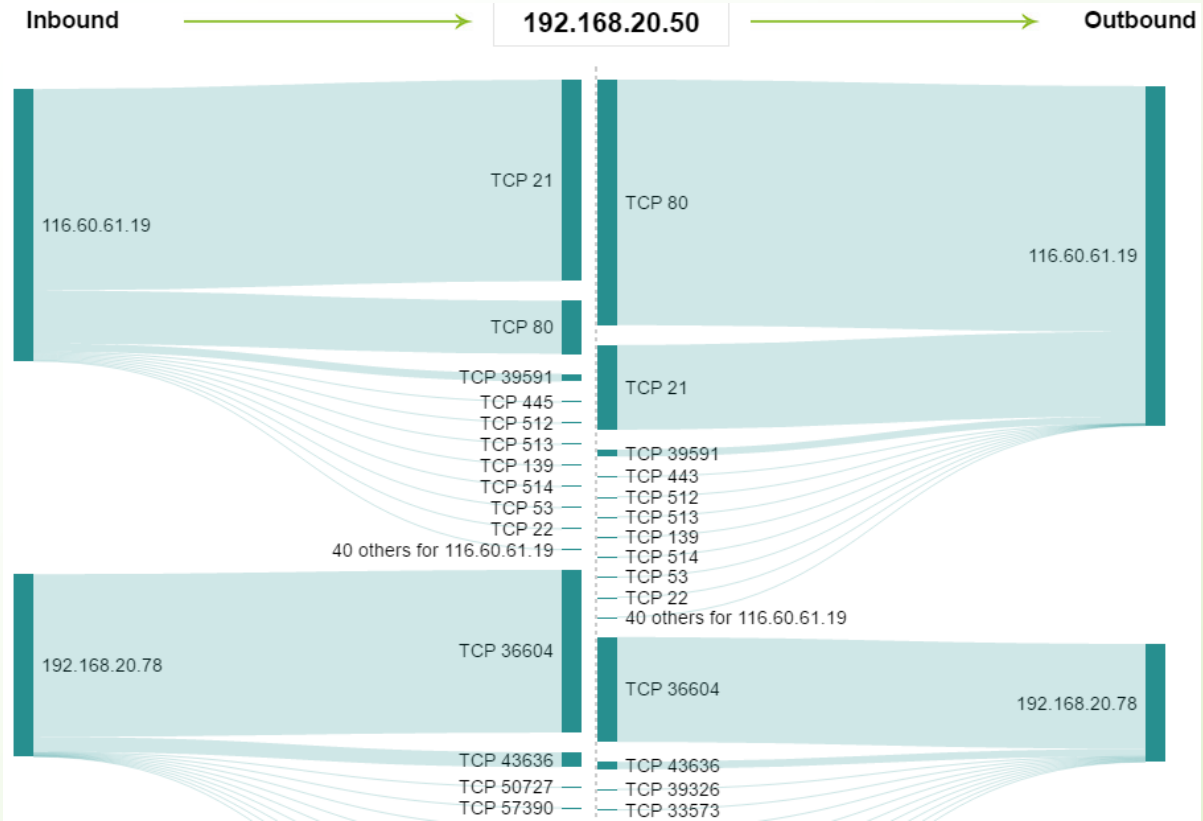
ARBOR NETWORKS

Arbor Spectrum “内部ネットワークモニタリング”

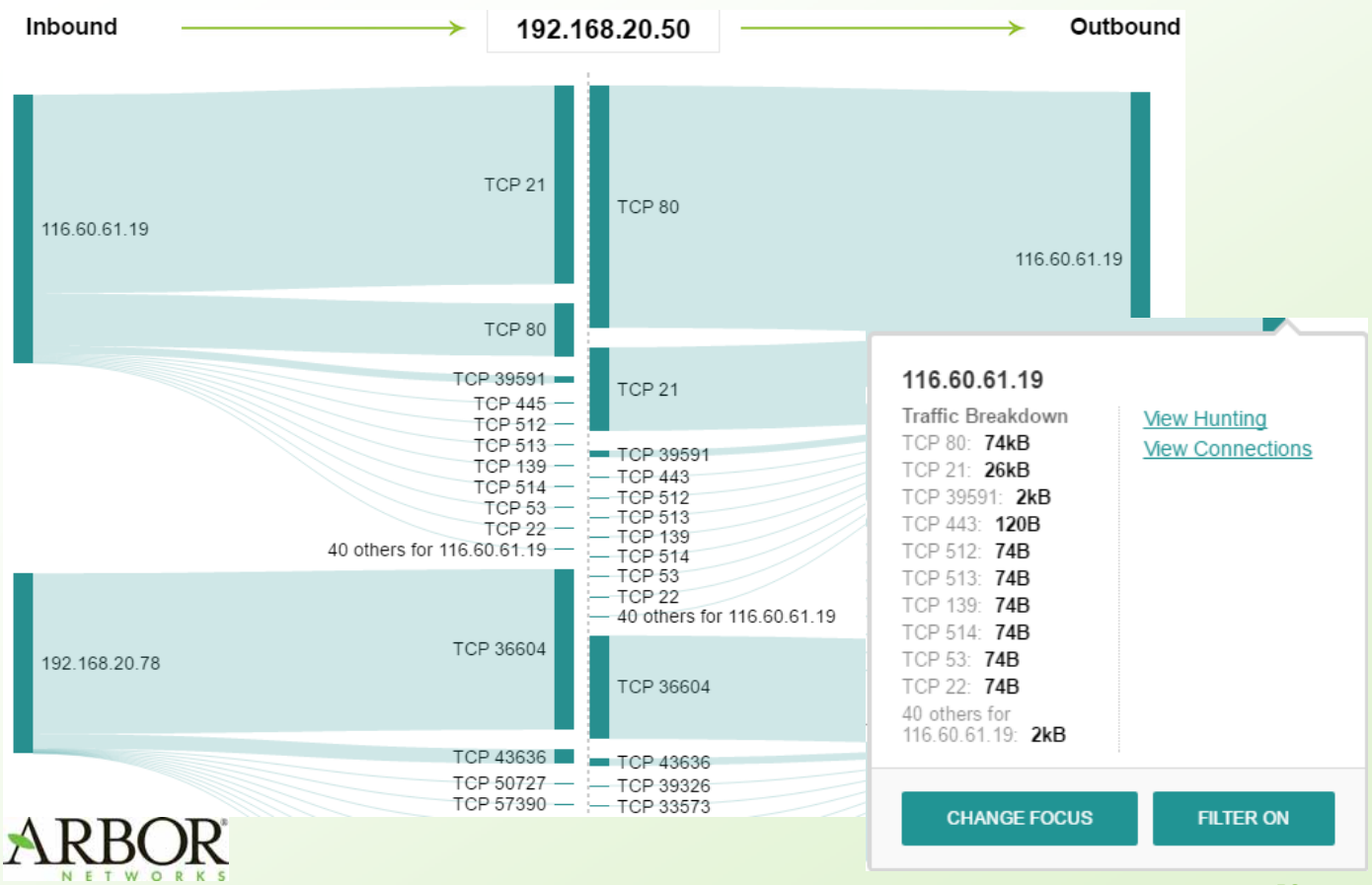


ARBOR NETWORKS

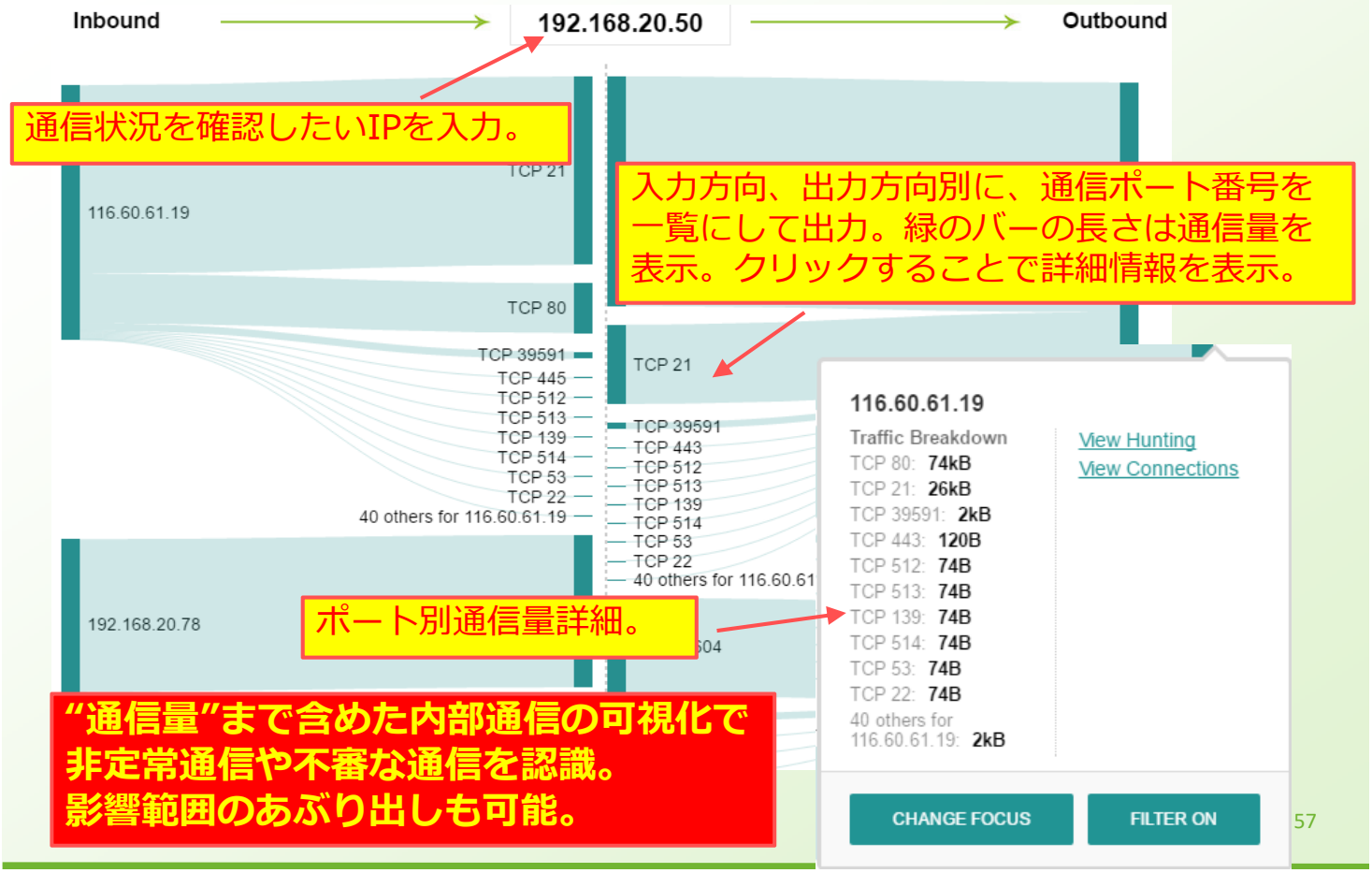
Arbor Spectrum “内部ネットワークモニタリング”



Arbor Spectrum “内部ネットワークモニタリング”



Arbor Spectrum “内部ネットワークモニタリング”



アーバーネットワークスのアプローチ

各ステップを記録、可視化

セキュリティフォレンジック

素早く影響範囲を特定

内部ネットワークのモニタリング

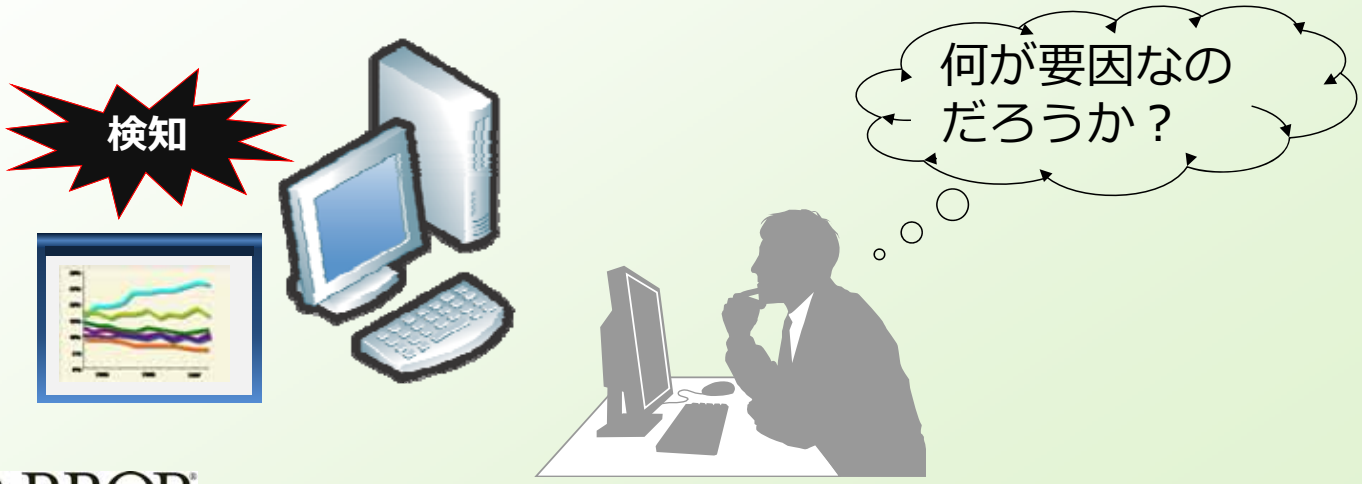
事象の根本原因の特定

能動的探索、脅威のハンティング

ARBOR NETWORKS

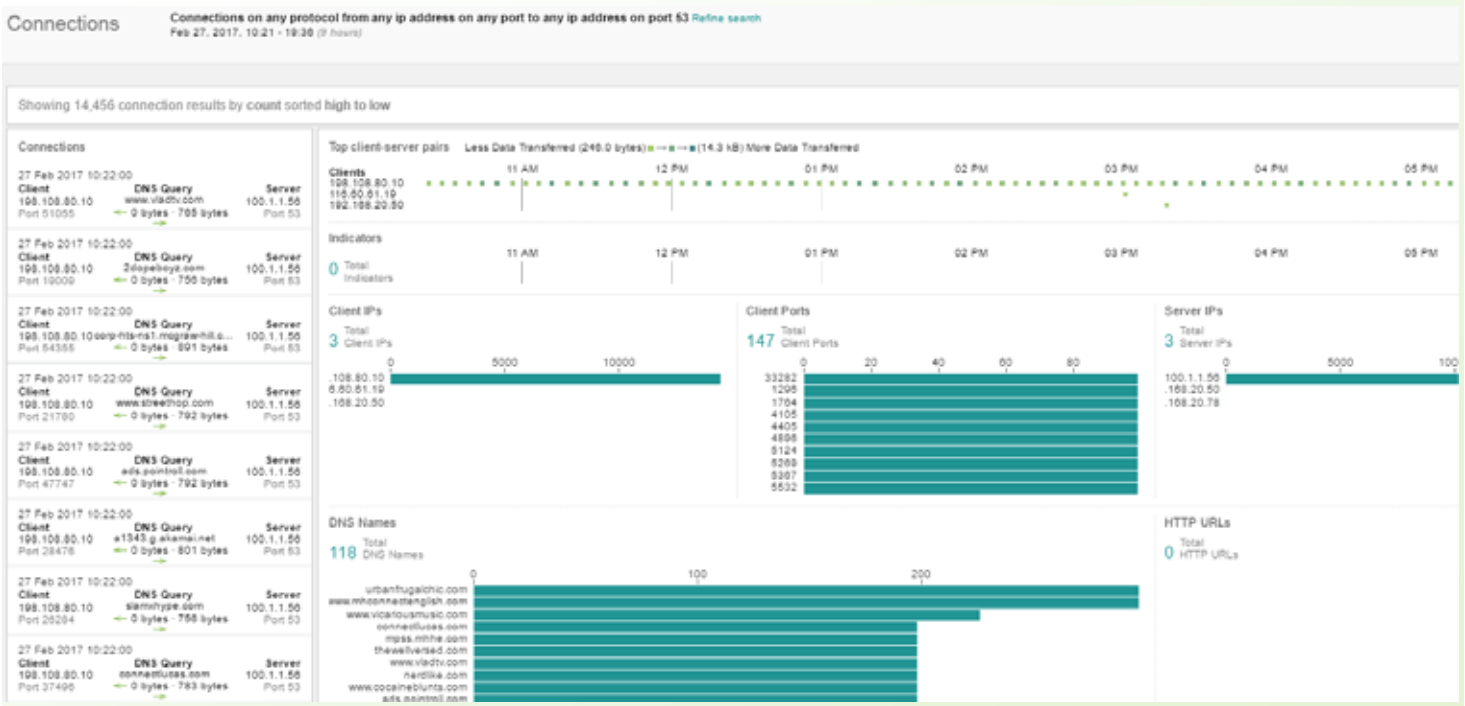
Arbor Spectrum “能動的探索、ハンティング”

【ケース３】
DNSサーバ、もしくはSIEMにてDNSサーバへのqpsの上昇を検知。要因を調査したい。



Arbor Spectrum “能動的探索、ハンティング”

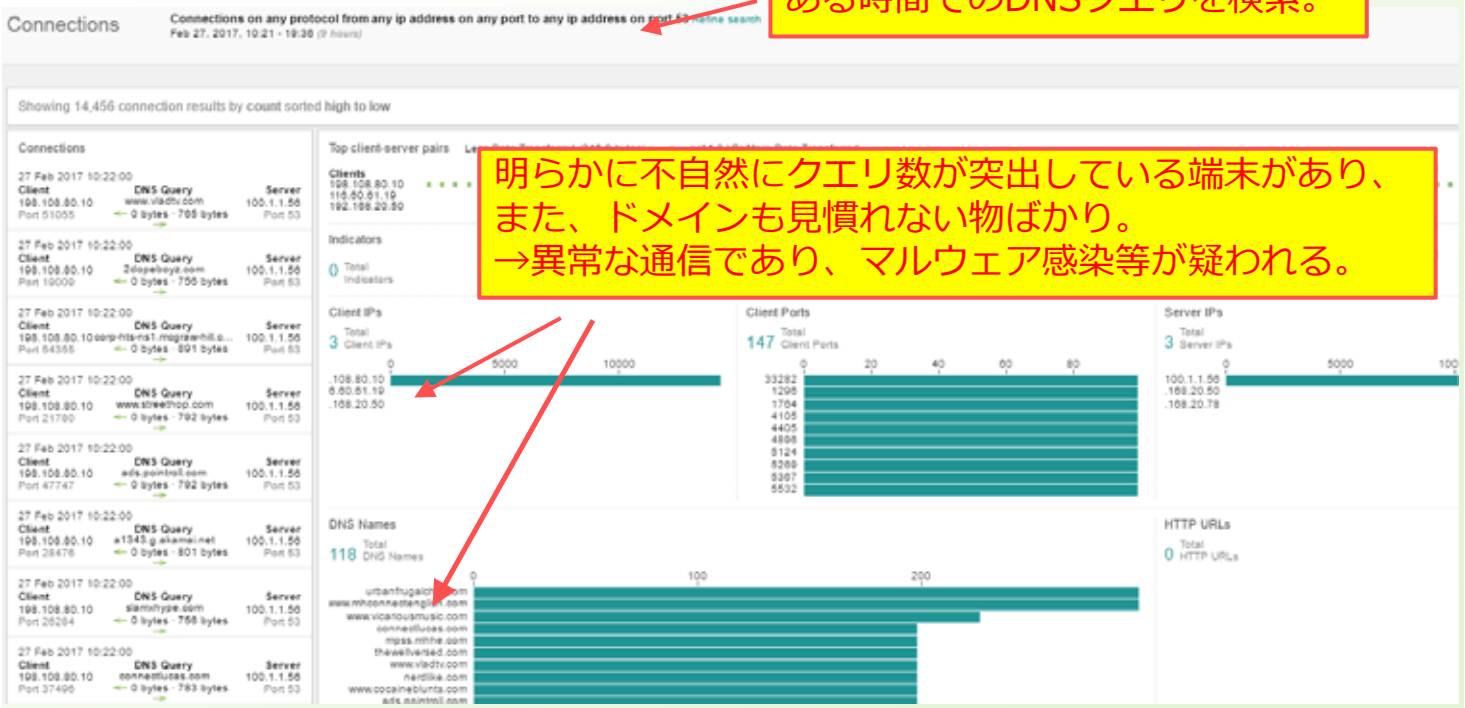
DNSのクエリから不審な端末をハンティング。



Arbor Spectrum “能動的探索、ハンティング”

DNSのクエリから不審な端末をハンティング。

ある時間でのDNSクエリを検索。

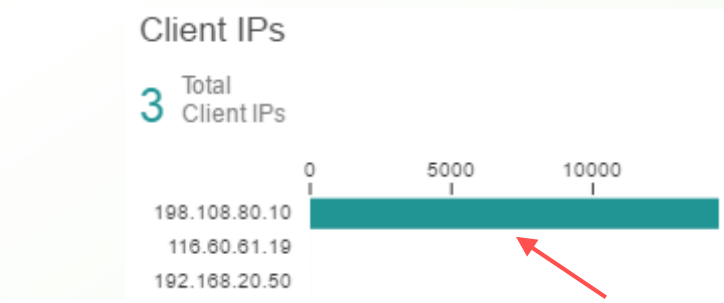


明らかに不自然にクエリ数が突出している端末があり、
また、ドメインも見慣れない物ばかり。
→異常な通信であり、マルウェア感染等が疑われる。

ARBOR NETWORKS

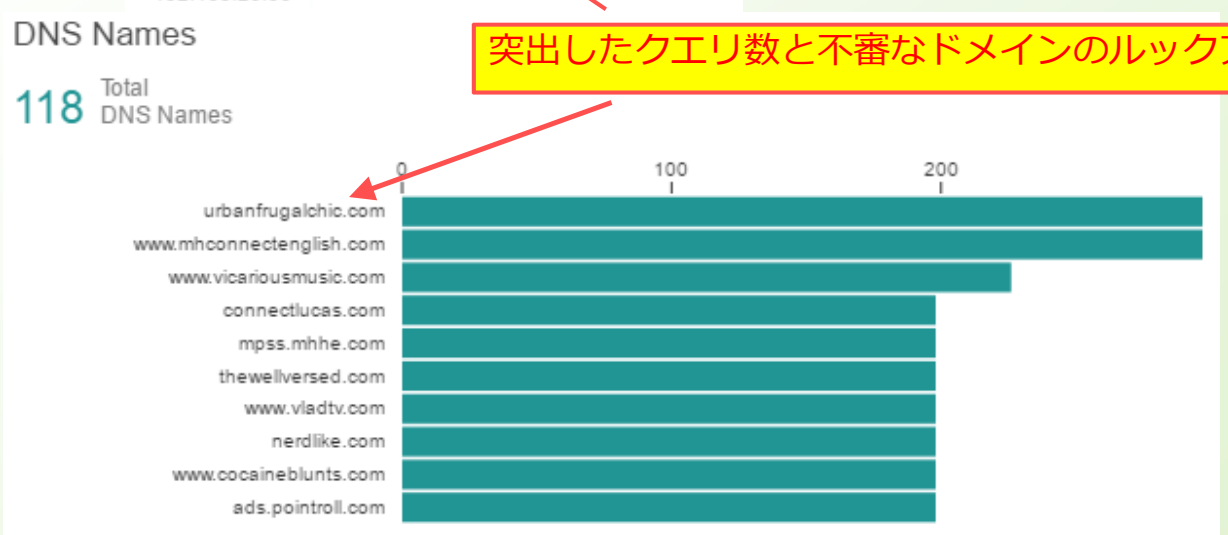
Arbor Spectrum “能動的探索、ハンティング”

DNSのクエリから不審な端末をハンティング。



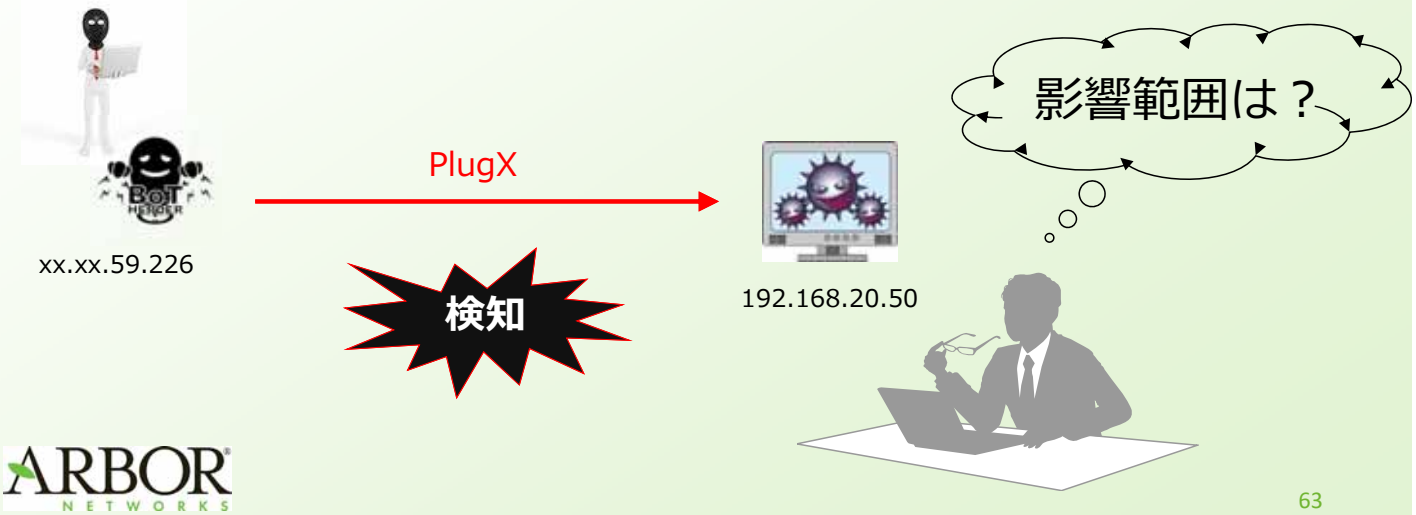
IP、ドメイン拡大

突出したクエリ数と不審なドメインのルックアップ



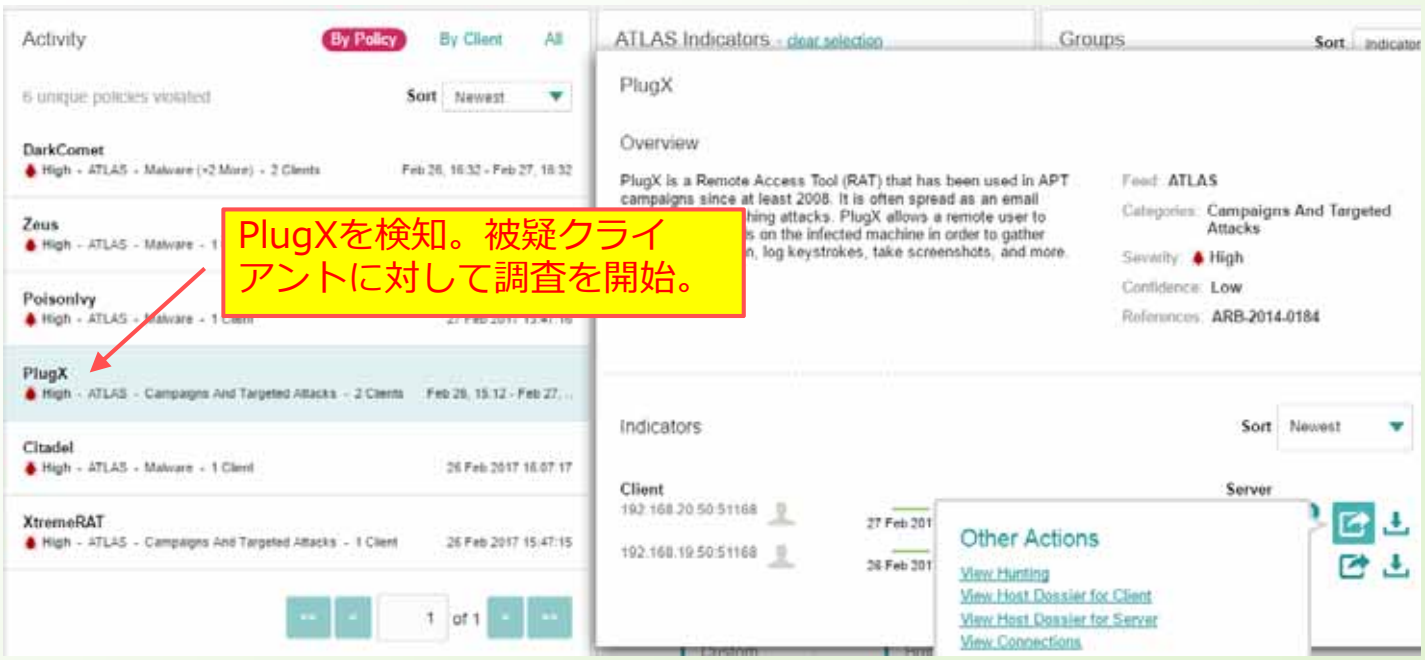
Arbor Spectrum “能動的探索、ハンティング”

【ケース４】
SpectrumでPlugXを検知。該当端末の感染だけなのかどうか、影響範囲を速やかに調査したい。

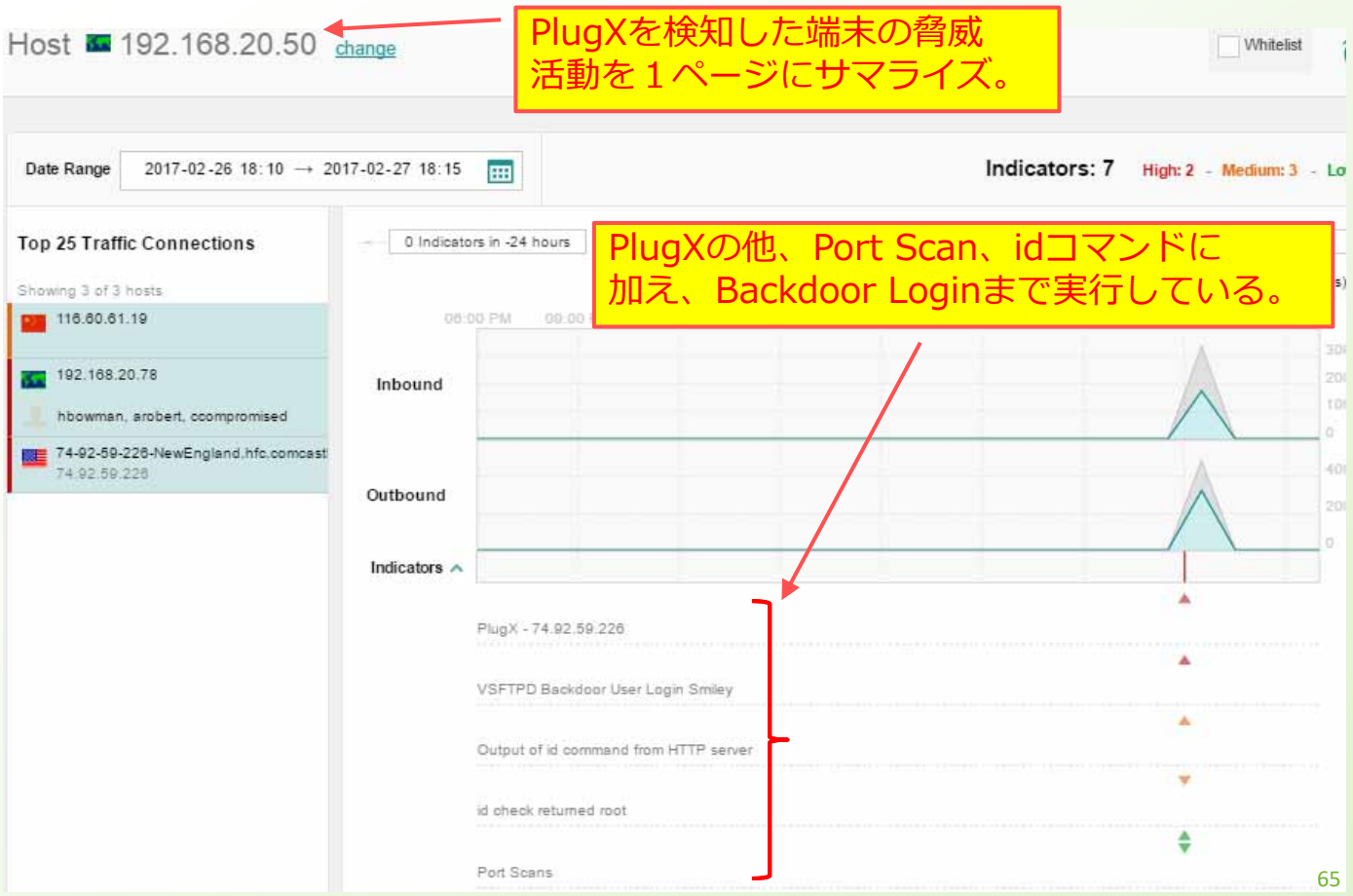


Arbor Spectrum “能動的探索、ハンティング”

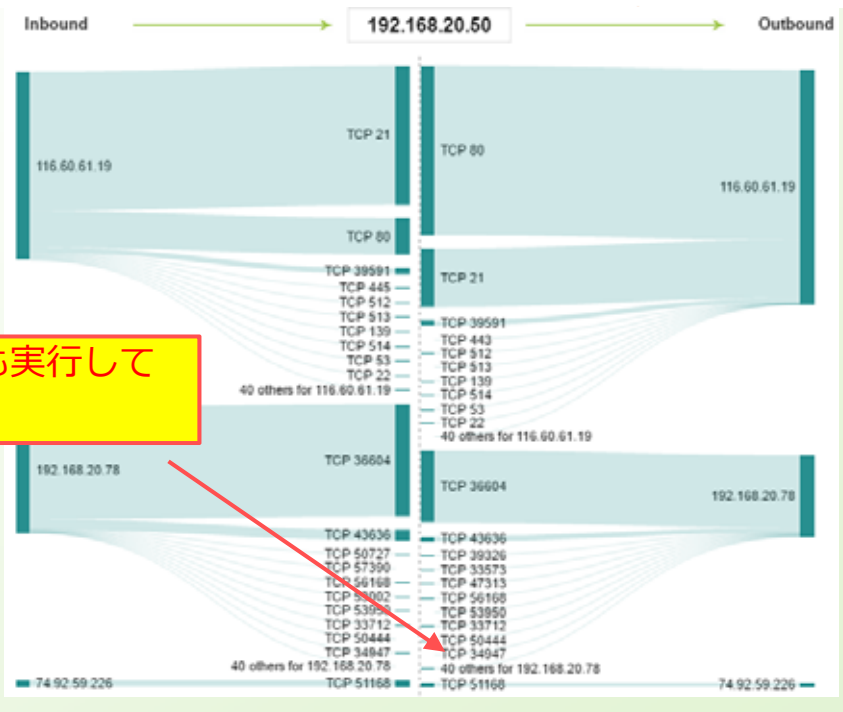
PlugXの検知から脅威活動の探索と全容の把握。



Arbor Spectrum “能動的探索、ハンティング”



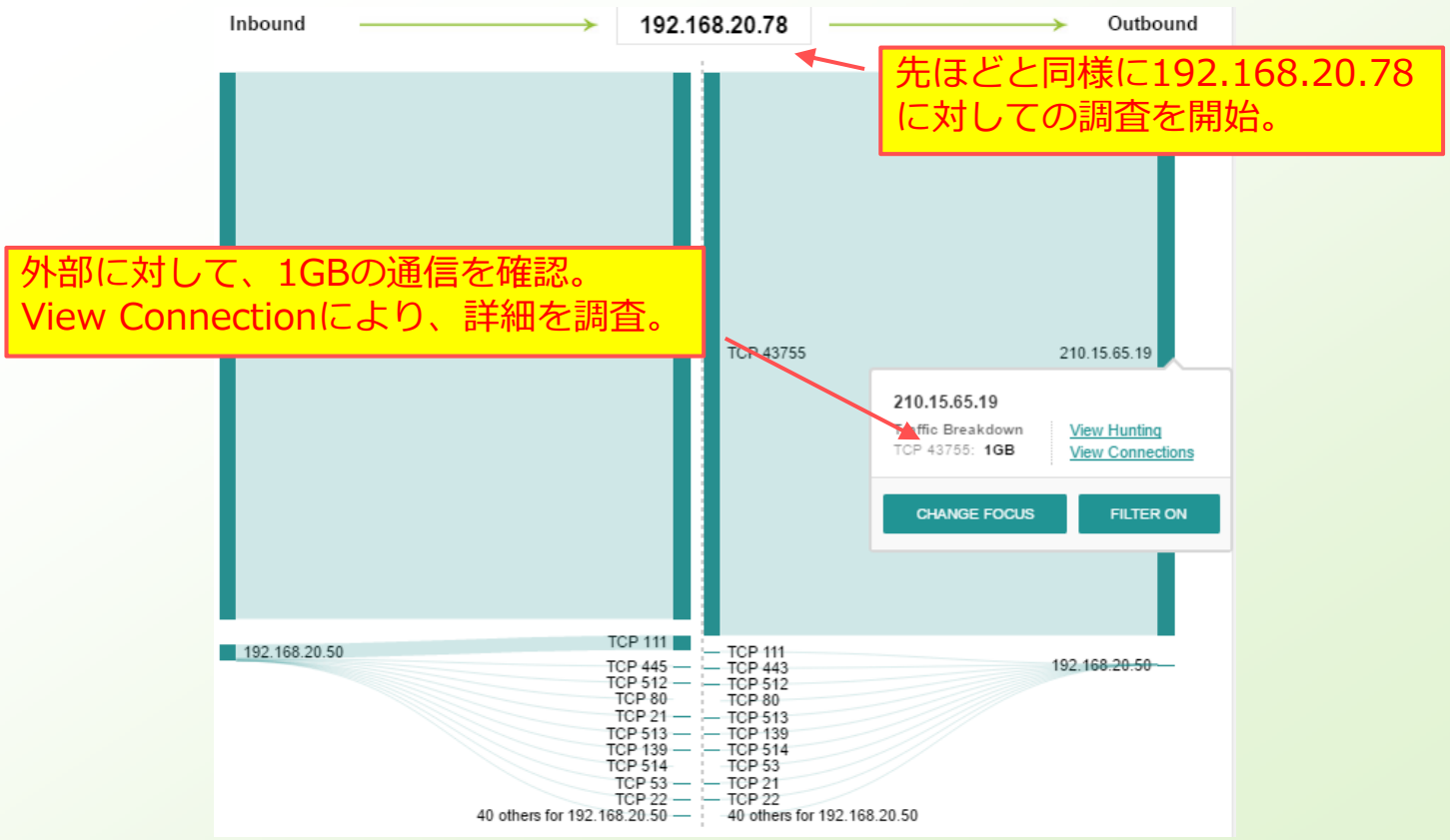
Arbor Spectrum “能動的探索、ハンティング”



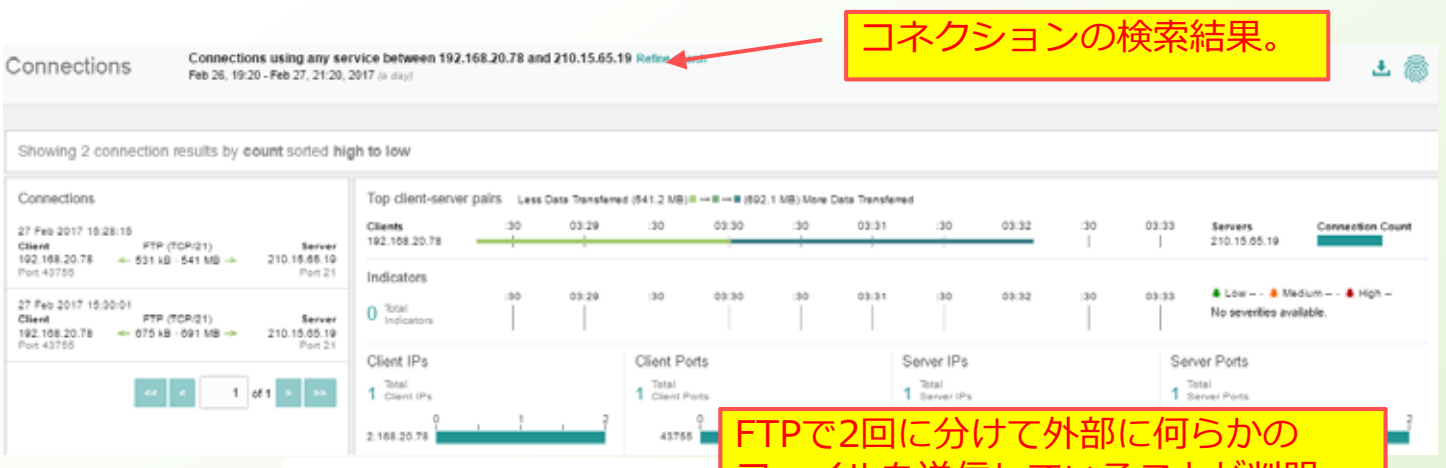
実際にPort Scanも実行して
いることがわかる。

ARBOR NETWORKS

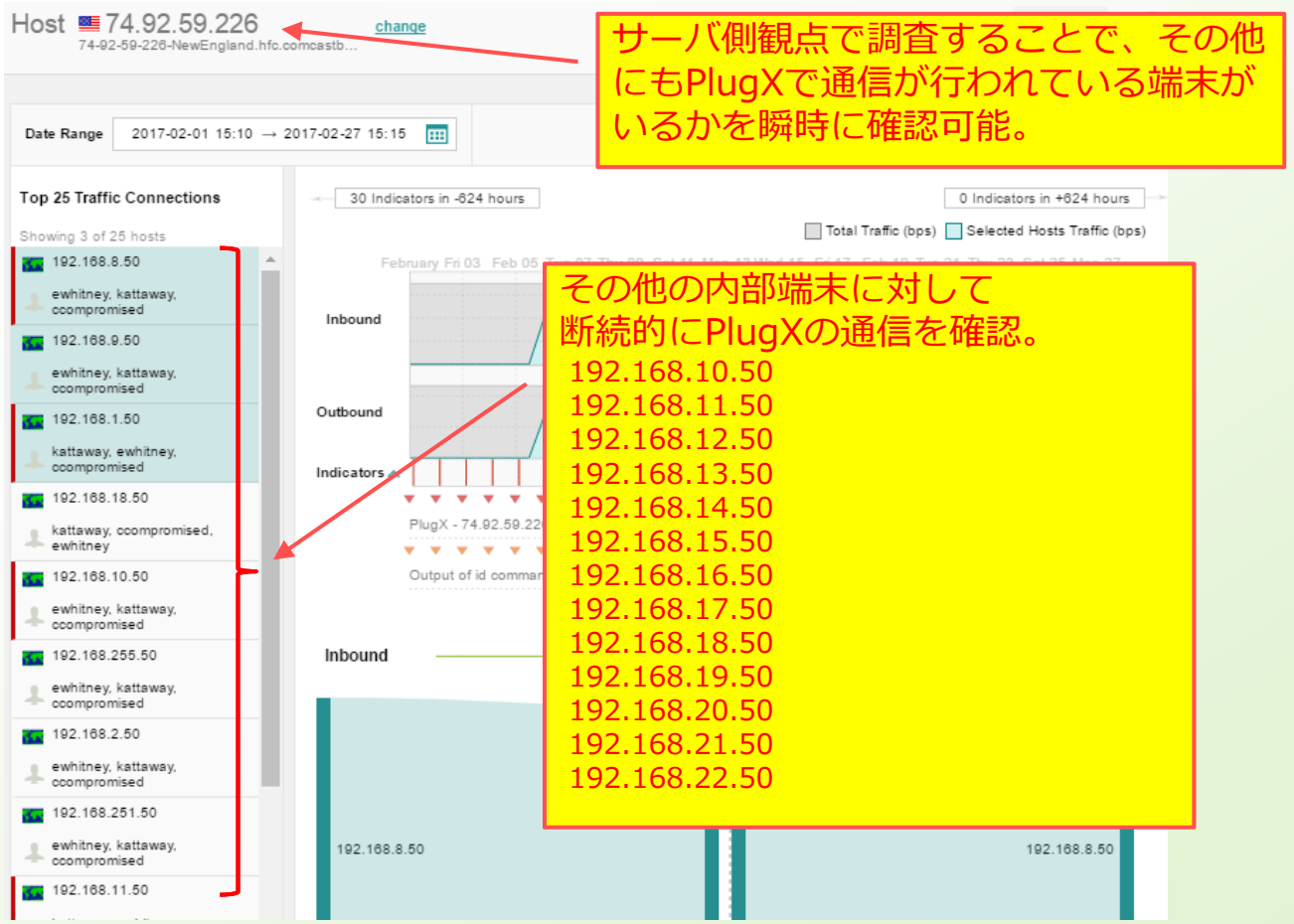
Arbor Spectrum “能動的探索、ハンティング”



Arbor Spectrum “能動的探索、ハンティング”



Arbor Spectrum “能動的探索、ハンティング”



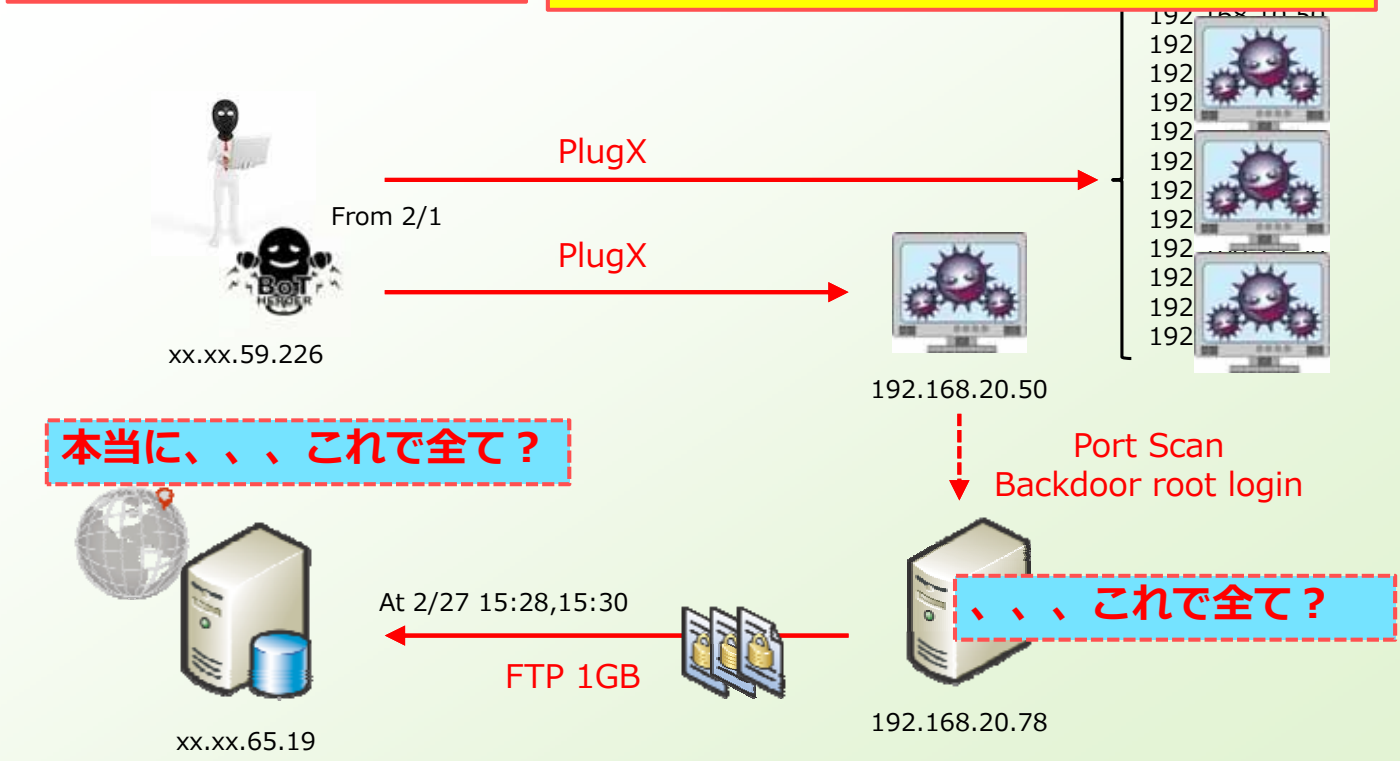
サーバ側観点で調査することで、その他にもPlugXで通信が行われている端末がいるかを瞬時に確認可能。

その他の内部端末に対して
断続的にPlugXの通信を確認。
192.168.10.50
192.168.11.50
192.168.12.50
192.168.13.50
192.168.14.50
192.168.15.50
192.168.16.50
192.168.17.50
192.168.18.50
192.168.19.50
192.168.20.50
192.168.21.50
192.168.22.50

Arbor Spectrum “能動的探索、ハンティング”

これが全体像！

攻撃キャンペーンの全容



求められるスピーディなインシデントレスポンス

適切なモニタリングと脅威の可視化

攻撃の全体像の正しい把握

漏えいした情報と感染原因の特定

関係各所への確実、かつ迅速な報告

ARBOR NETWORKS

まとめ

アーバーネットワークスのアプローチは、**ネットワークモニタリング観点からのインシデントレスポンスの改善**です。色々なトリガーから脅威活動の迅速な可視化を実現します。
可視化をすることで、より重点的に深堀するべき調査内容をあぶりだしていくことができます。

今あるセキュリティ財産をより有効に活用するためにも、現在のインシデントレスポンス能力を見直してみることが重要と考えます。

ARBOR NETWORKS

ARBOR NETWORKS

ご静聴ありがとうございました。

お問い合わせは
sfujiwara@arbor.net
japanall@arbor.net
までお願いします。