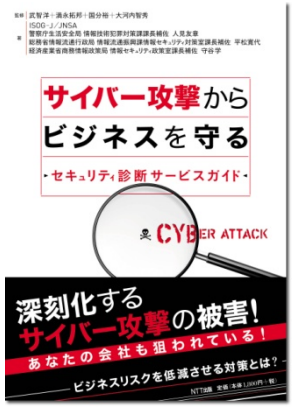
東京大学 情報学環

# *Big Data Analysis for Cyber Security*

Takuho Mitsunaga,
The University of Tokyo

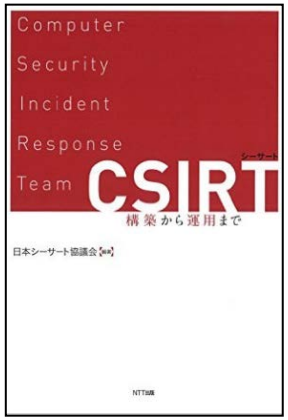
# プロフィール

- 名前：満永　拓邦(みつなが　たくほう)
- 所属：東京大学情報学環 セキュア情報化社会寄付講座(SiSOC)
  特任准教授
  JPCERTコーディネーションセンター
  早期警戒グループ 技術アドバイザー
- 業務：・セキュリティに関する情報の収集・分析・発信
  ・外部の組織や企業の経営層やシステム管理部門との連携
  ・セミナーや大学などでの講演活動
  ・セキュリティ関連調査のレポート執筆




「サイバー攻撃からビジネスを守る」
監修/共著

「情報セキュリティ白書　2013」
分担執筆




「CSIRT:構築から運用まで」
共著

# 東京大学情報学環
# セキュア情報化社会研究寄付講座とは

- 産官学連携により、安心安全なインターネット環境構築に資する研究を実施する
  - 産官学の協力の下に広く人材を糾合し、実際に生じている社会的かつ国際的な課題に対し、自然科学的なアプローチのみならず社会科学的なアプローチも取り入れ調査研究を行い、その検討結果を広く情報発信
  - セキュリティをはじめとするサイバー空間に関する課題について巨視的長期的視座から学際的研究・人材育成・政策提言を推進

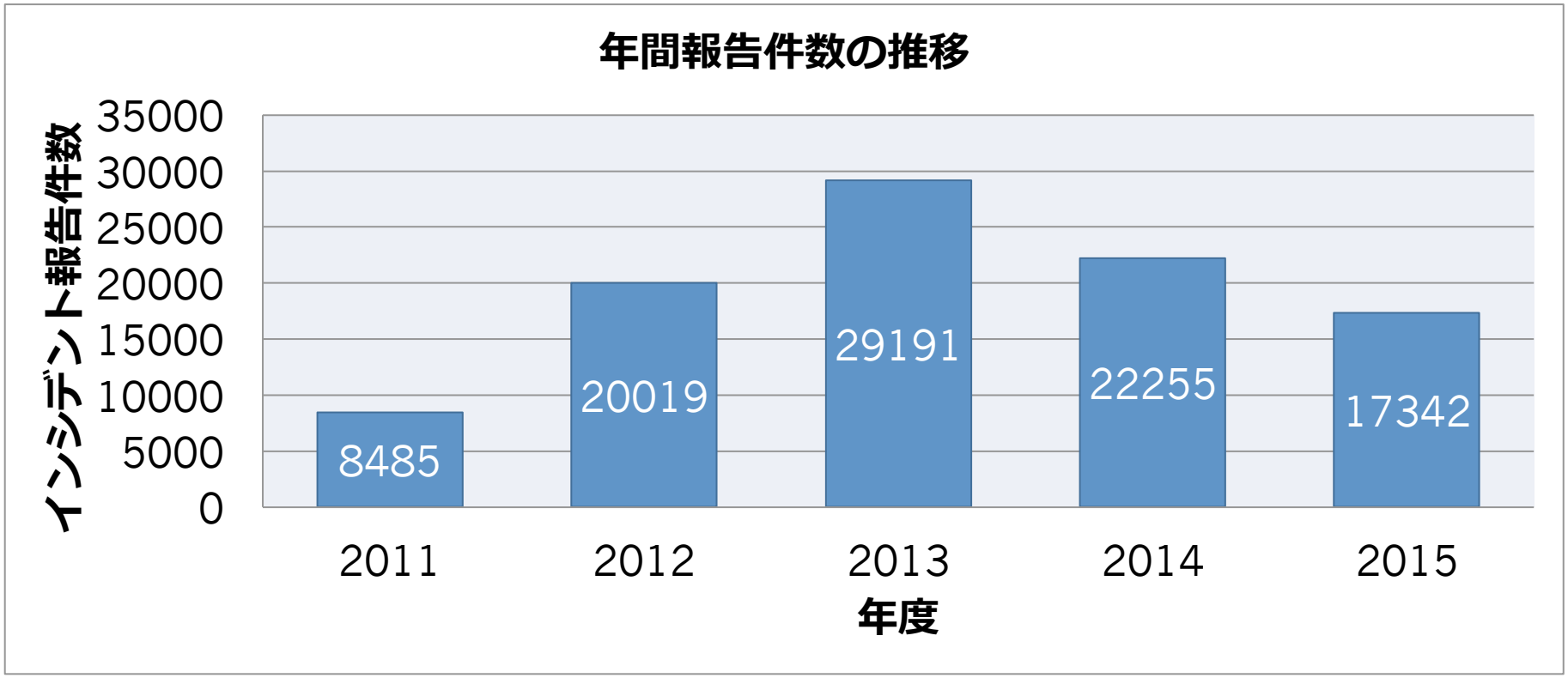
# アジェンダ

1. サイバーセキュリティ動向
2. Big Data/Machine Learning × Security
3. 研究紹介
4. まとめ

# サイバーセキュリティ動向

# インシデント発生状況(1)

- 情報技術の進歩とともに、攻撃手法や傾向は変化し続け、一定数のインシデント(セキュリティ事故)が発生し続けている



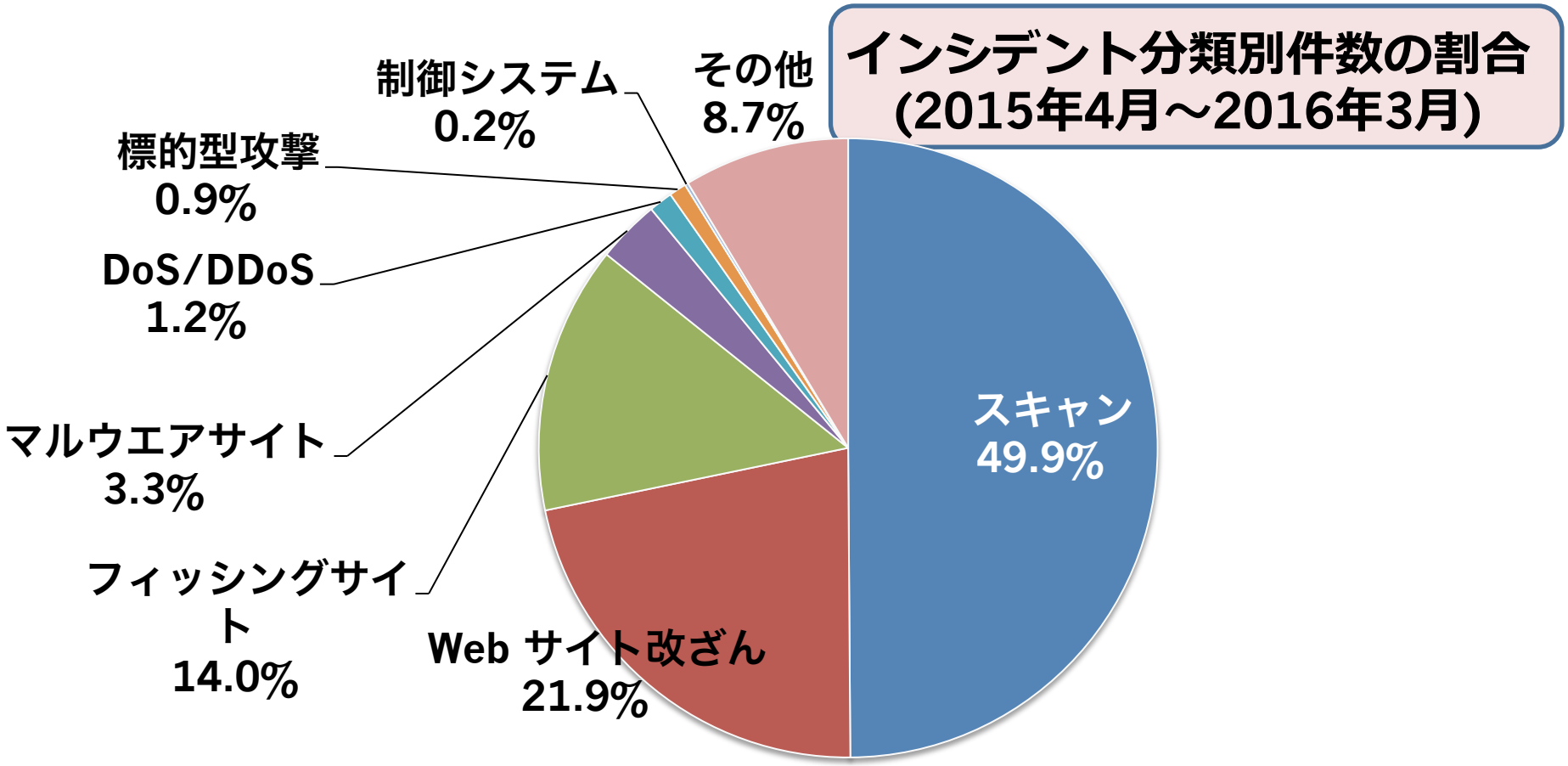

JPCERT CC®

一般社団法人JPCERTコーディネーションセンター
(JPCERT/CC (ジェーピーサート・コーディネーションセンター))

・経済産業省からの委託事業として、コンピュータセキュリティインシデントへの対応支援、国内外にセンサをおいたインターネット定点観測、ソフトウエアや情報システム・制御システム機器等の脆弱性への対応などを通じ、セキュリティ向上を推進
・インシデント対応をはじめとする、国際連携が必要なオペレーションや情報連携に関する、我が国の窓口となる　CSIRT

# インシデントの発生状況 (2)

- 様々な種類のインシデント事故が発生している



# インシデント発生の背景

**ITの社会インフラ化**

- 企業活動のIT化
- 電子商取引の発展
- 制御系システムへの利用

**インターネットの世界的な普及**

- ボーダレスの通信
- 物理的な追跡困難性

**攻撃用インフラの整備**

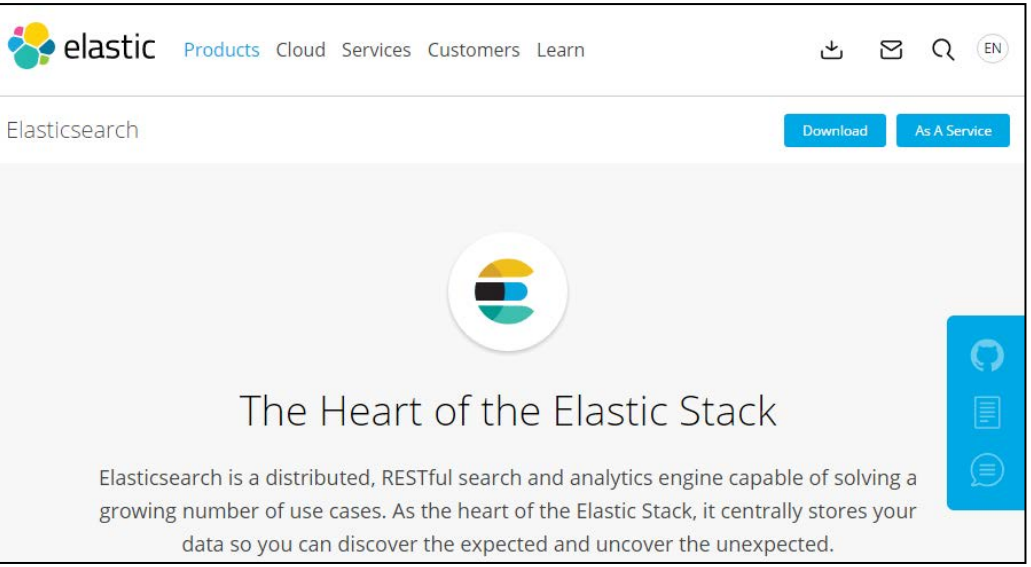
- 攻撃ツールの進歩
- 分業化された攻撃集団

**サイバー攻撃は増加が予想される為、各組織での対応体制が必要**

# Big Data/Machine Learning × Security

# 機械学習の利用例

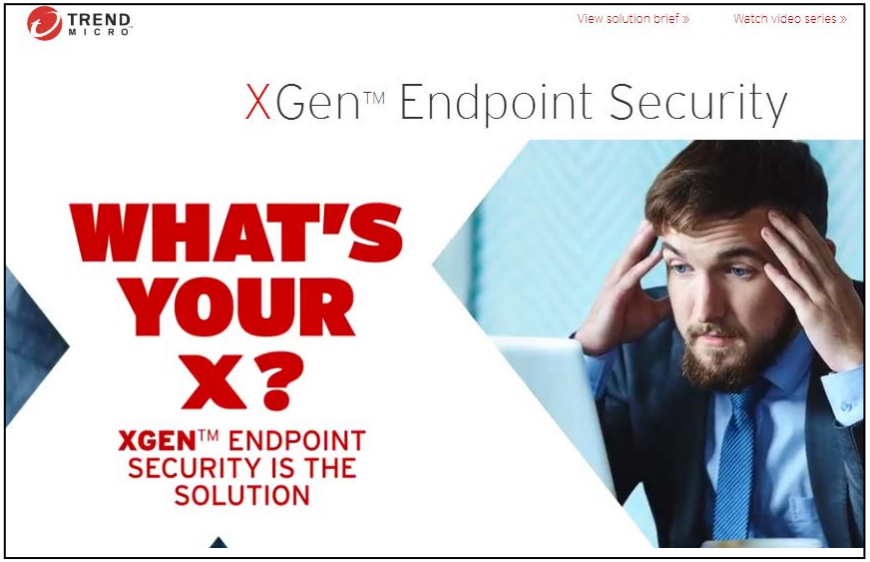
- Monitoring and Attack Detection
  - 大量の通信データ等に対し、分析、可視化を行うことで異常通信などを検知
    **ex. Elasticsearch, Kibana**



https://www.elastic.co/ https://www.elastic.co/jp/blog/kibana-4

# 機械学習の利用例

- Antivirus Protection
  - 機械学習やビックデータに基づく、新たなタイプのウイルス対策などが開発されている
  - 既存のシグネチャマッチングと比較して、新種のマルウエアの検知能力が向上すると言われる

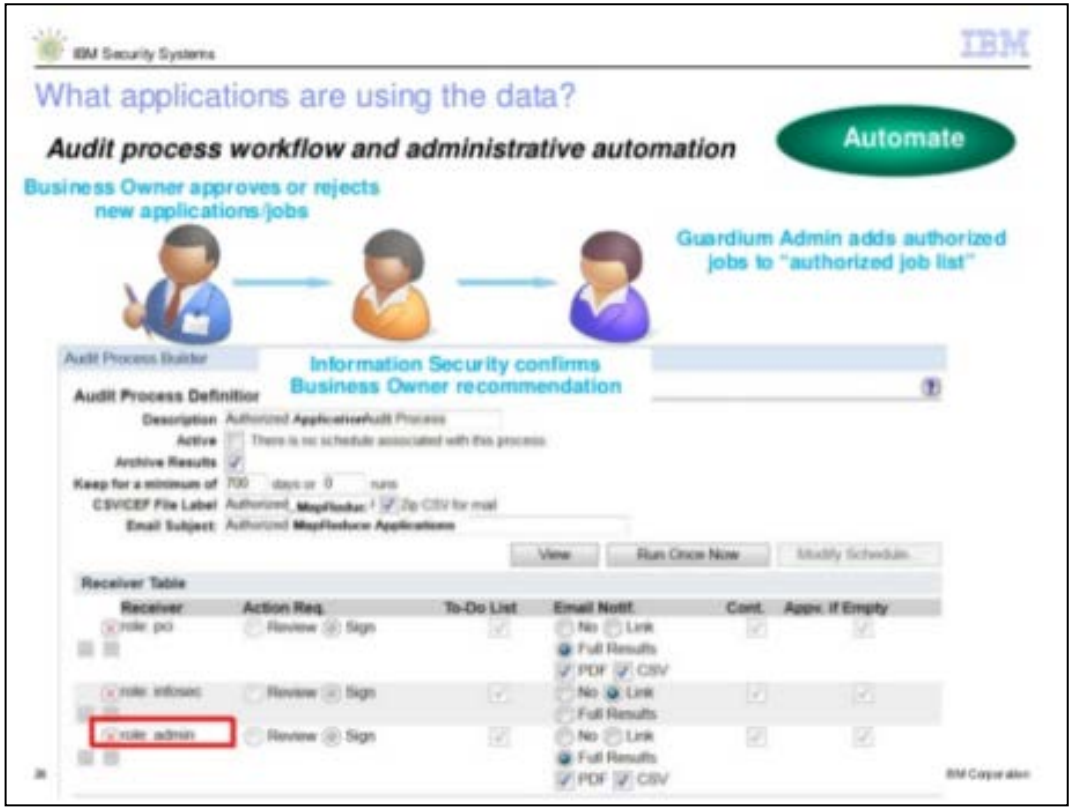



http://www.trendmicro.com/us/business/xgen/index.html

https://www.cylance.com/

# 機械学習の利用例

- Big Data for Security Audit
  - ビックデータ処理に基づき、監査プロセスでの異常を検知する




http://www.slideshare.net/NicolasJMorales/ibm-hadoop-securityaudit

# 研究の紹介

# モチベーション

- ビックデータやAIとセキュリティは相性が良く、新しい技術も登場している。ただし、ユーザにとって容易でない内容のため、活用するための学習コストが必要となる場合も多い

- アンケート等では""を期待する声も多いが、ビックデータを利用するためには、十分に訓練された人間が必要になるケースもある（人間の手を減らすために、人間に対する教育が必要？）

- Which of challenges does your organization face?

1. Lack of Adequate staffing in security operation（39%）
2. Too many false positive responses(35%)
3. Incident detection depends upon too many manual processes(29%)

[1] EMC, "The Big Data Security Analytics Era is Here", 2013

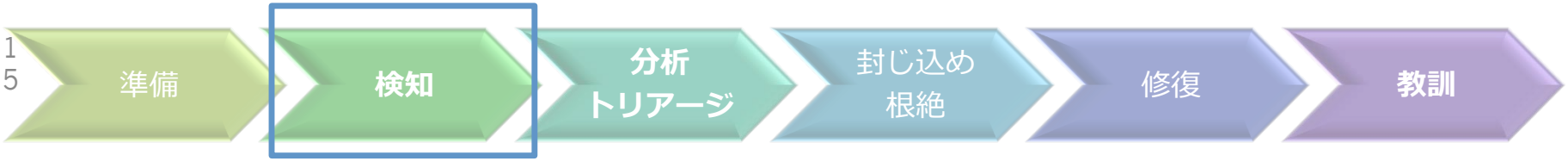
# インシデント対応プロセス

アメリカ国立標準技術研究所 NIST SP800-61 に基づくインシデント対応において、以下のフェーズでBig Dataや機械学習の分析を活用する

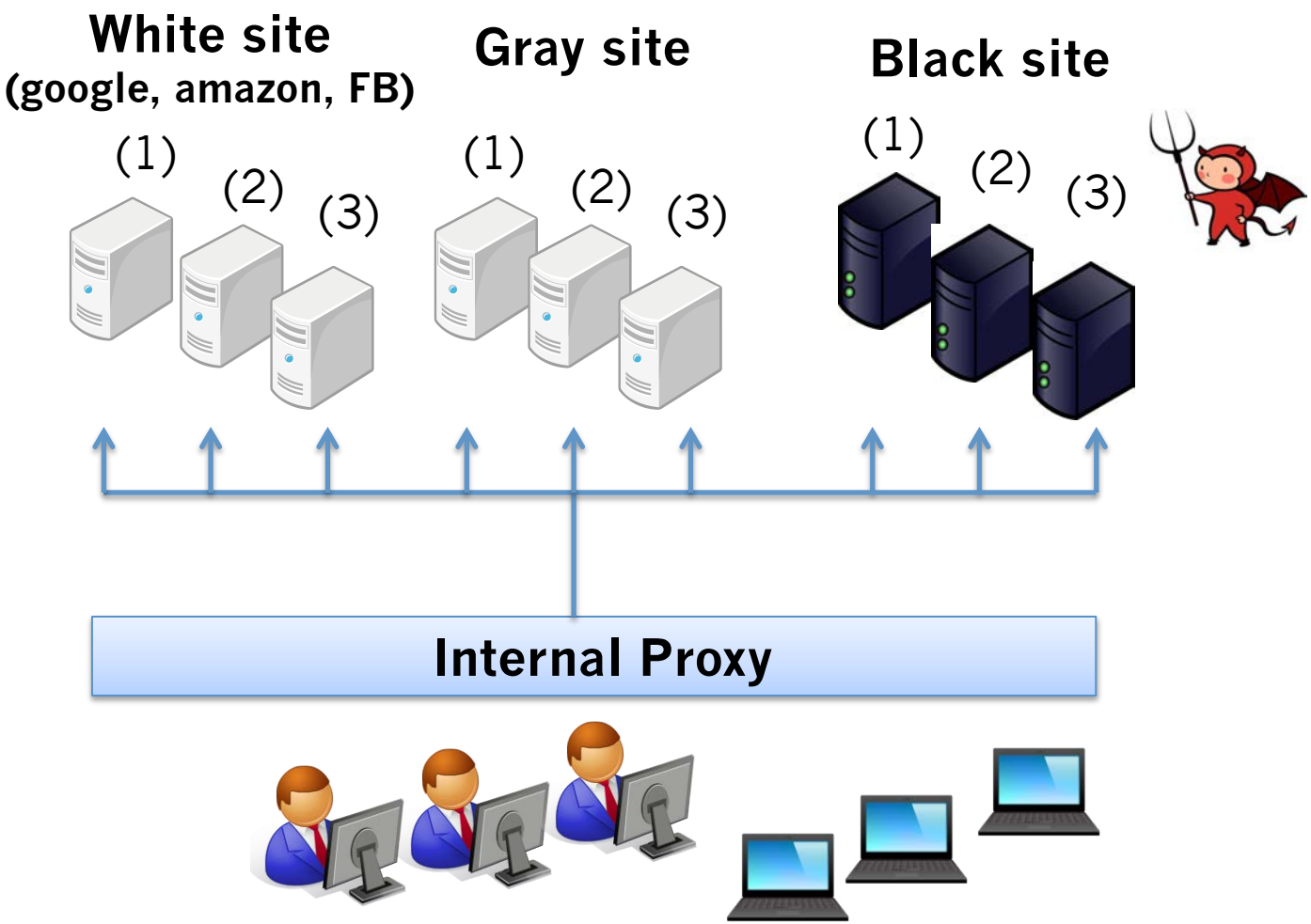
1．検知フェーズ
- ネットワーク機器等のログに対する機会学習

2．分析・トリアージフェーズ
- マルウエア感染時の脅威度判定

3．封じ込め・根絶フェーズ
- 脅威度による自動封じ込め



検知フェーズでは、Proxy で取得する複数の通信に対して、White, Gray, Black に分類することを試みる



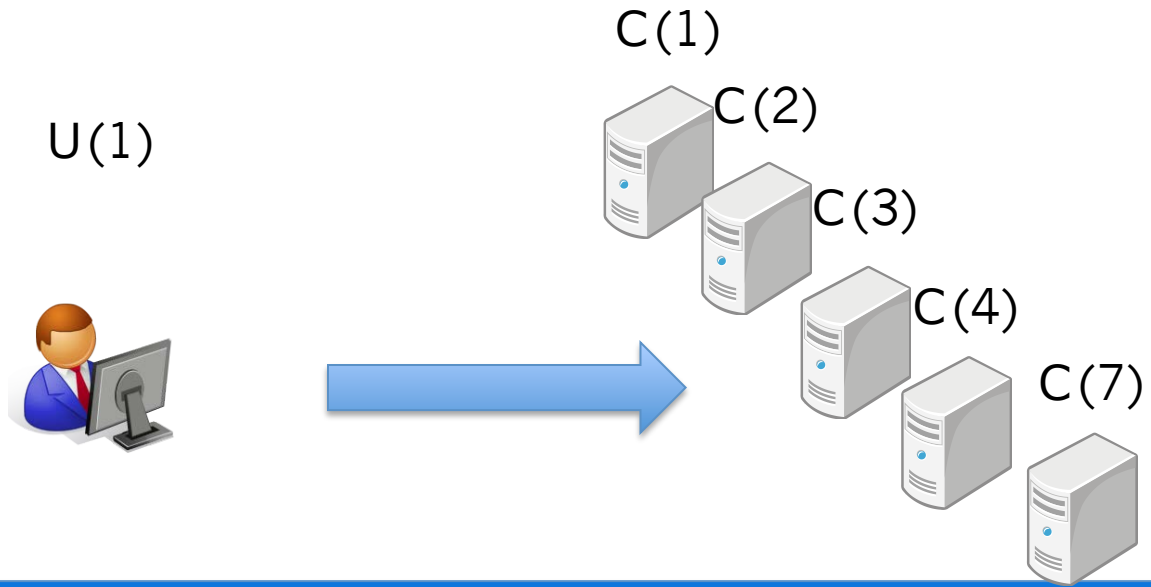
# 分析

- 前提
  - malicious に通信している端末は、１００％マルウエアに感染している
  - マルウエアに感染している端末は、malicious 以外のsafe や gray にも通信する
  - malicious に通信していない場合でも、マルウエアに感染している可能性がある

- 定義
  - ユーザの端末をU(1), U(2),...,U(m)と表現する
  - 通信先全体を、C(1),C(2),...,C(n)とし、Safe, Gray, Malicious を
    W, G, B とする
- 分析
  - ユーザ端末と通信先の関連性を見ることで、Gray の中に Malicious が存在するかを調べる

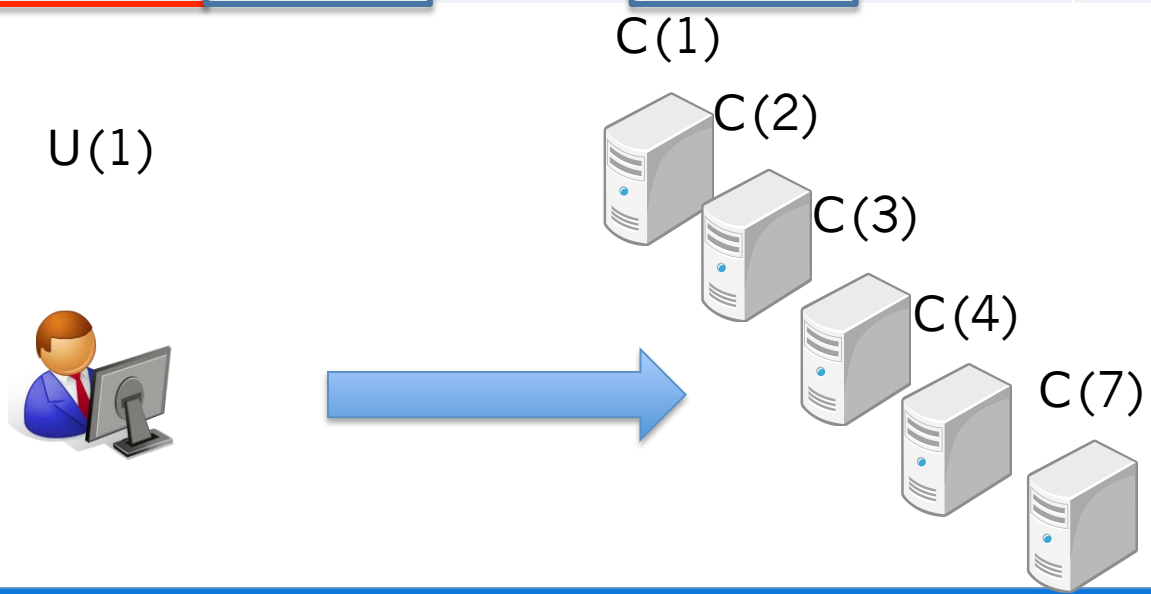
# 通信状況の把握

| ユーザ/通信先 | C(1) | C(2) | C(3) | C(4) | C(5) | C(6) | C(7) |
|---|---|---|---|---|---|---|---|
| U(1) | ○ | ○ | ○ | ○ | | | ○ |
| U(2) | | | ○ | ○ | ○ | ○ | |
| U(3) | ○ | | | | ○ | ○ | |
| U(4) | | ○ | ○ | ○ | | | ○ |
| U(5) | | ○ | | ○ | ○ | | ○ |
| U(6) | | | | | | ○ | ○ |



# 悪意ある通信の類似性探索

| ユーザ/通信先 | C(1) | C(2) | C(3) | C(4) | C(5) | C(6) | C(7) |
|---|---|---|---|---|---|---|---|
| U(1) | ○ | ○ | ○ | ○ | | | ○ |
| U(2) | | | ○ | ○ | ○ | ○ | |
| U(3) | ○ | | | ○ | ○ | ○ | |
| U(4) | | ○ | ○ | ○ | | | ○ |
| U(5) | | ○ | | ○ | ○ | | ○ |
| U(6) | | | | | | ○ | ○ |



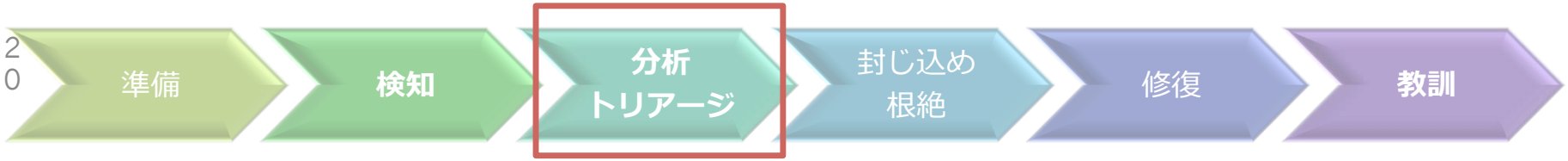
# インシデント対応プロセス

NIST SP800-61 に基づくインシデント対応において、以下のフェーズでBig Dataや機械学習の分析を活用する

1．検知フェーズ
- ネットワーク機器等のログに対する機会学習

2．分析・トリアージフェーズ
- マルウエア感染時の脅威度判定

3．封じ込め・根絶フェーズ
- 脅威度による自動封じ込め



# 攻撃者の分類

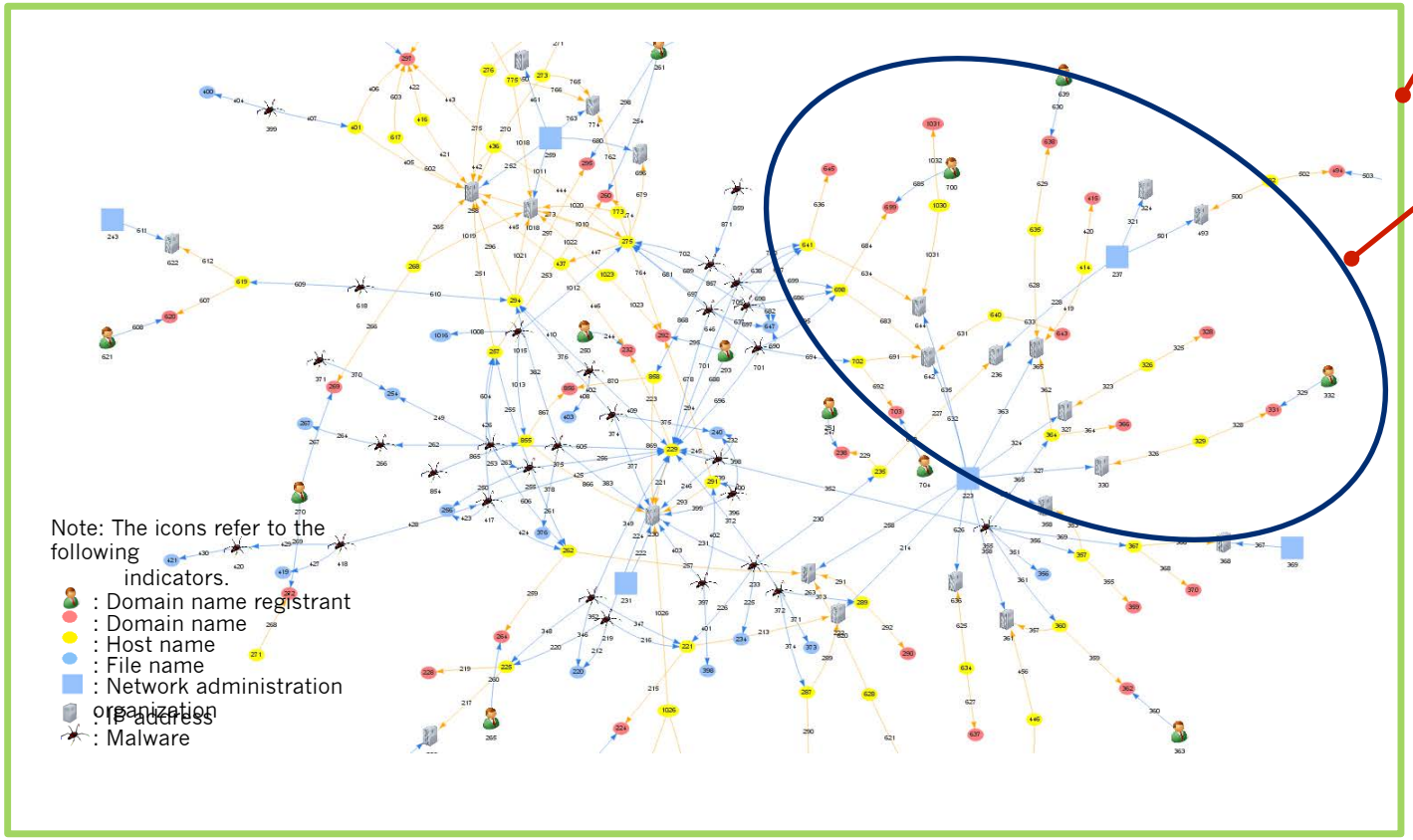
- 攻撃の目的をもとに攻撃者を分類すると、それぞれの攻撃手法や技術力が異なることが推察できる

| | **愉快犯/ハクティビスト** | **金銭目的の攻撃者** | **標的型攻撃の実行者** |
|---|---|---|---|
| 攻撃の目的 | · 政治的な主張<br>· 技術力のアピール | · 金銭の獲得(不正送金) | · 標的とする組織内の重要情報窃取やシステム破壊 |
| 主な攻撃手法 | · Web サイトに対するDoS<br>· 政治的な主張を目的とする Web サイトの改ざん<br>· SNS アカウント乗っ取り | ·マルウエアが添付されたメールの送付<br>·Web サイト改ざんによるマルウエアの配布 | ·マルウエアが添付されたメールの送付<br>· Web サイト改ざんによるマルウエアの配布<br>(ただし攻撃対象のみに限定) |
| 技術力 | 低 | | 高 |

JPCERT/CC 早期警戒グループにて独自に分類

# 高度サイバー攻撃のインフラ分析事例

Emvidi と呼ばれる攻撃に関して、共有情報や複数のオンサイト調査などを通じて得た攻撃関連情報（マルウエア、C2サーバなど）を可視化

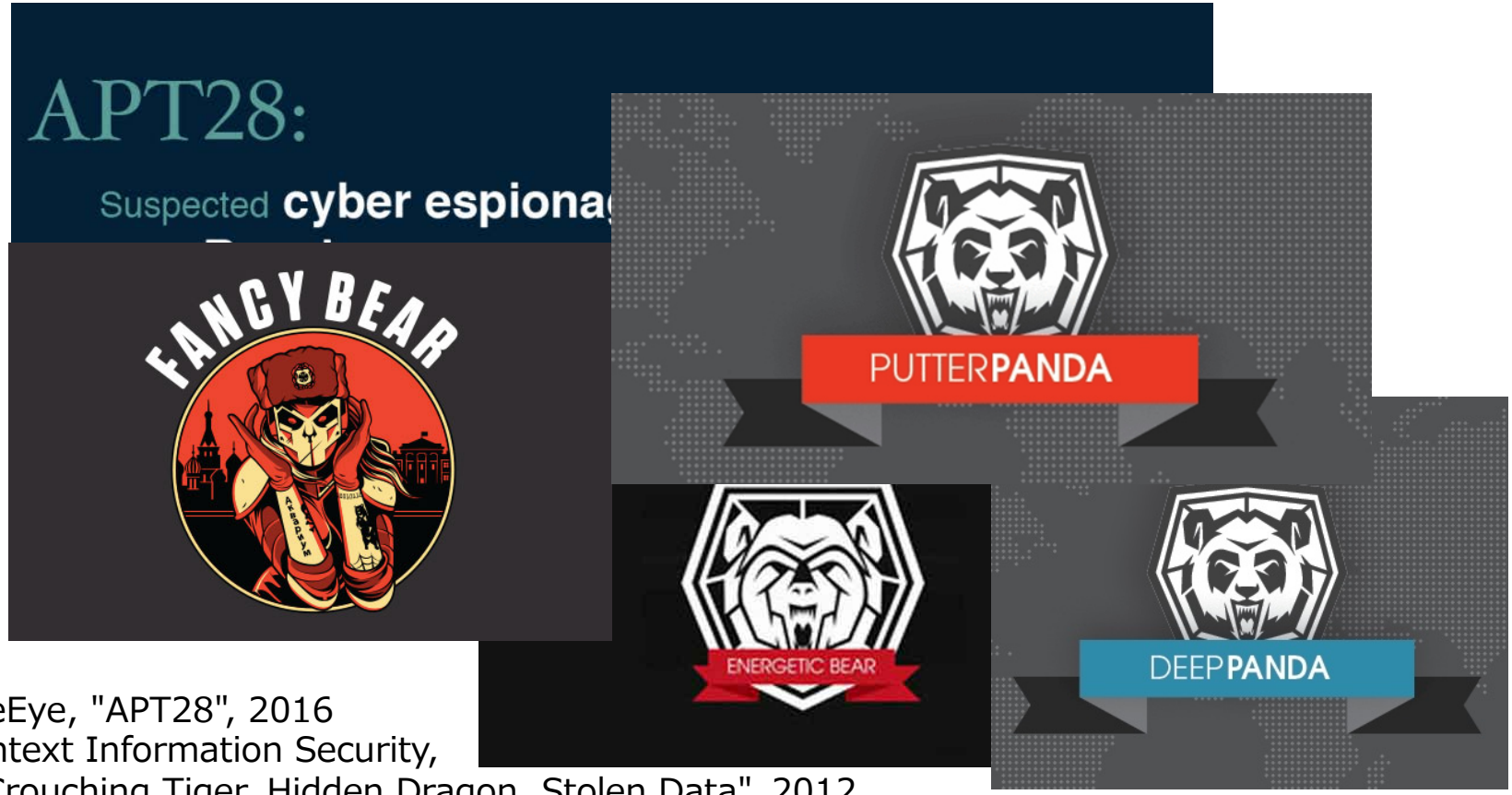



ある時点で判明した全貌

ひとつの調査で判明した攻撃（イメージ）

# その他の事例

- Security vendors published a report about a campaign or groups regarding targeted attacks




FireEye, "APT28", 2016
Context Information Security,
"Crouching Tiger, Hidden Dragon, Stolen Data", 2012
CrowdStrike, "Putter Panda", 2014
CrowdStrike, "DEEP PANDA", 2014
Kaspersky, "Energetic Bear – Crouching Yeti", 2014

# 分類のためのデータ

- file Name, path, registry, communication etc.

**DEEP PANDA**

## File System Artifacts

The following file system artifacts are indicative of a compromised host:

**Dropper/DLL**
C:\Documents and Se
C:\Documents and Se
C:\Documents and Se
MD5: 47619fca20895a

**Post Explotiation Too**
MD5: 2dce7fc3f52a69

**Backdoor**
MD5: de7500fc1065a0

**Kernel Driver:**
MD5: dae6b9b3b8e39
"%sysdir%\Drivers\{6A

**Malware #1**

```
alert tcp any any <> any any (msg: "BackDoor Beacon Attempt"; content:"|78 7c
71 4c 4a 49 49 49 4A 4C 46|"; classtype:backdoor; sid:123456; rev:27122011;)

alert tcp any any <> any any (msg: "BackDoor Beacon Attempt"; content:"Goo-
gle"; http_uri; c

alert ip 1.9.5.38
type:backdoor; si
```

**Malware #2**

```
alert tcp any any
74 80 82 21 b5 64
0000 00 00|"; cla

alert ip 202.86.1
type:backdoor; si
```

**1. C&C backend**

The C&C Backend is written in PHP, consisting of 3 files:

- **"log.php"** is a Web-Shell, used for file level operations.
- **"testlog.php"** is not a PHP-script but it contains the C&C Server logfile of Backdoor-connections. Please see **"source.php"** below for further information.
- **"source.php"**

The Backdoors interact with *"source.php"*, which is the control script. These are its functions on execution:

# 分類

- 既存のデータを用いて、検知された攻撃の脅威度を推定

脅威度低　　脅威度高

| | 愉快犯/ハクティビスト | 金銭目的の攻撃者 | 標的型攻撃の実行者 |
|---|---|---|---|
| 攻撃の目的 | - 政治的な主張<br>- 技術力のアピール | - 金銭の獲得(不正送金) | - 標的とする組織内の重要情報窃取やシステム破壊 |
| 主な攻撃手法 | - Web サイトに対するDoS<br>- 政治的な主張を目的とする Web サイトの改ざん<br>- SNS アカウント乗っ取り | -マルウエアが添付されたメールの送付<br>-Web サイト改ざんによるマルウエアの配布 | -マルウエアが添付されたメールの送付<br>- Web サイト改ざんによるマルウエアの配布<br>(ただし攻撃対象のみに限定) |

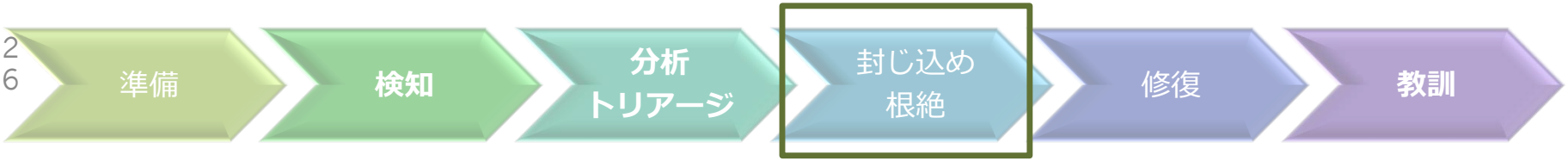
# インシデント対応プロセス

NIST SP800-61 に基づくインシデント対応において、以下のフェーズでBig Dataや機械学習の分析を活用する

1．検知フェーズ
- ネットワーク機器等のログに対する機会学習

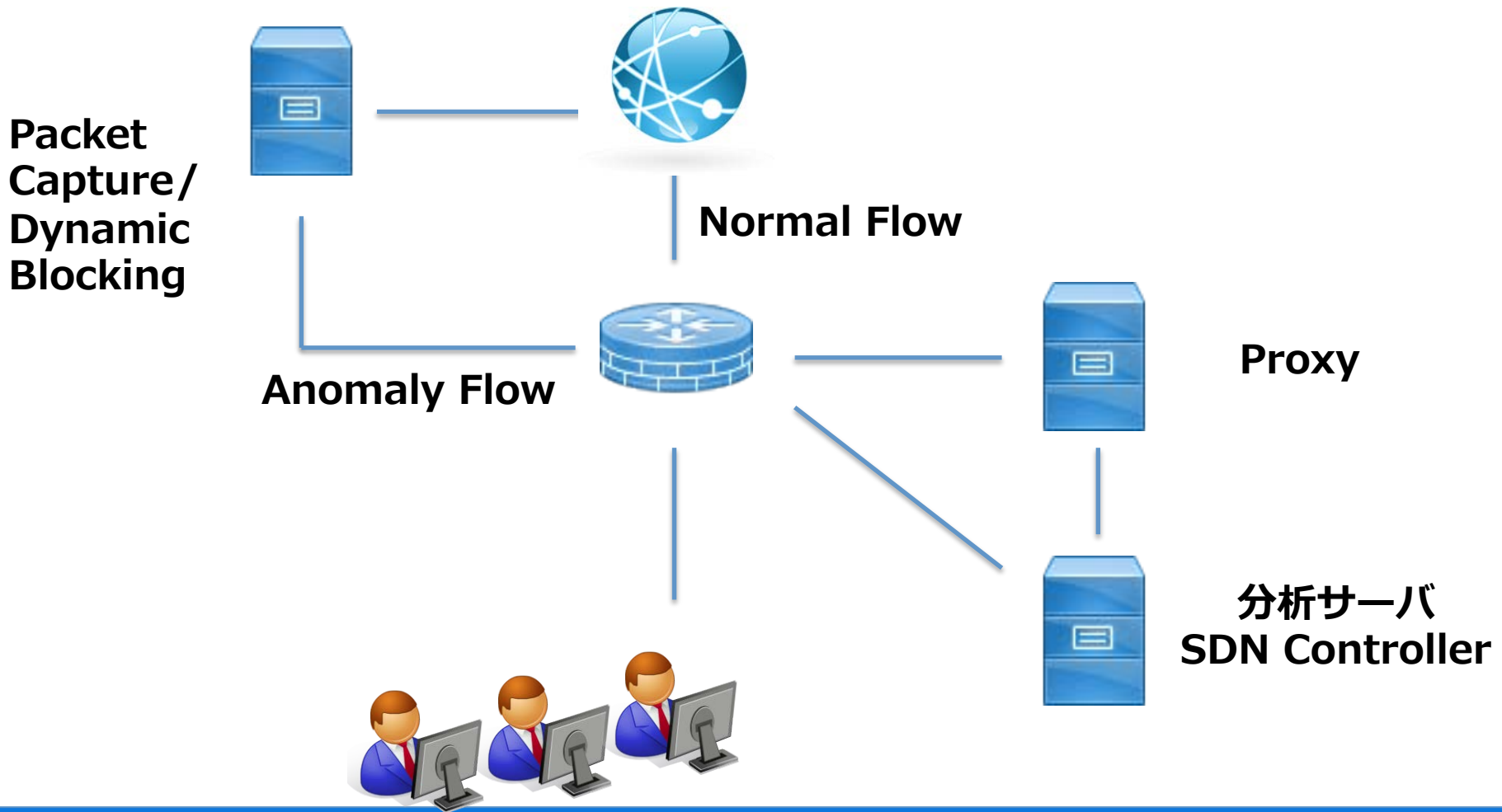
2．分析・トリアージフェーズ
- マルウエア感染時の脅威度判定

3．封じ込め・根絶フェーズ
- 脅威度による自動封じ込め



# SDNを用いた自動対応

- SDNを活用することにより、脅威度に応じて、自動的に通信を区分けする



# まとめ

# まとめ

- ビックデータ関連や機械学習の技術がセキュリティに使われる事例が増加しており、製品化も進んでいる
- しかしながら、ユーザや企業の理解が進んでいない分野であるため、難しい内容ではなくシンプルかつ効果的なアプローチが必要だと考える
- 今回の発表では、我々の研究成果を組み合わせてアプローチを紹介した
  - 組織内の通信ログからマルウエア感染の疑いがある端末を見つけ出し
  - それらの脅威レベルを過去のデータから自動で判定して
  - 脅威度が高い場合は自動で通信を遮断する