ネットワークフォレンジックスによる PCIDSS要件10への対応強化

～ログに残らないサイバー攻撃の危険性と、ネットワークフォレンジックスによる対応強化策について～

トーテックサイバーセキュリティ研究所

所長　藤原礼征

TOTEC AMENITY LIMITED

PCIDSSにおけるログの重要性

PCIDSS 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監視する

- ログ記録メカニズムおよびユーザの行動を追跡する機能は、**データへの侵害を防ぐ、検出する、またはその影響を最小限に抑える**うえで不可欠です。
- すべての環境でログが存在することにより、何か不具合が発生した場合に**徹底的な追跡、警告、および分析**が可能になります。
- **侵害の原因の特定**は、システムアクティビティログなしでは非常に困難です。

アクセスログがあれば十分か？

- ログは有効な情報・・・だが
  - ファイルの内容など、侵害された詳細までは分からない
  - ログから対象のファイルを特定しても、ファイルが書き換えられたり、消去される可能性がある
  - メモリ上のデータの漏えいなどはわからない
  - ログが残らない操作が存在する
  - プロトコル上で、ログが記録されない通信がある
  - サーバログが消去される可能性もある
  - サーバが破壊される可能性もある

CVE-2014-0160: OpenSSL Heart Bleed Bug 2014/4/8

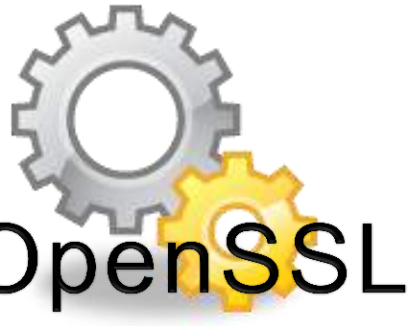
OpenSSL の heartbeat 拡張に情報漏えいの脆弱性

- OpenSSL のコードを実行しているプロセスのメモリ内容が漏えいする可能性
  - 通信内容のみならず、サーバの秘密鍵も危険
  - 警察庁の定点観測システムにて、攻撃を多数観測
  - 三菱UFJニコスで、894件の顧客情報漏えいの可能性
- 過去最大級の影響範囲と深刻性
  - OpenSSLを使用するapache等のwebサーバ、SMTP/POP/IMAPサーバ、MySQL/postgresql等のDBサーバ
  - CVSS Baseスコア10点満点中9.4点。ネットワーク越しに、単純な方法で、認証の必要なしに、情報が漏洩もしくは損なわれる

webサーバ

5文字

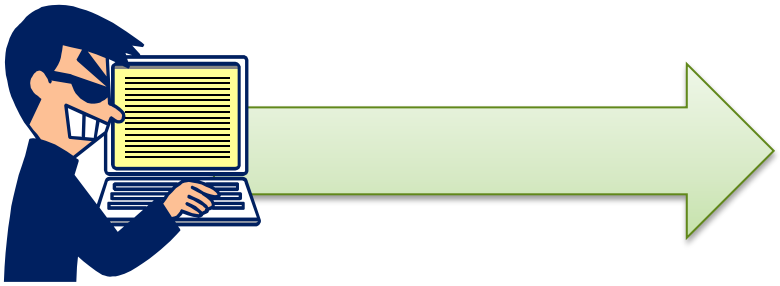
Hello



メモリ

01010100
10101001
01010101
01010101
01010101
01010101
01010101
01101010

10101010
10101001
01010101
01001011
01010001
10010101
01010101
01001011



webサーバ

メモリ
01010100
10101001
01010101
01010101
01010101
01010101
01010101
01101010

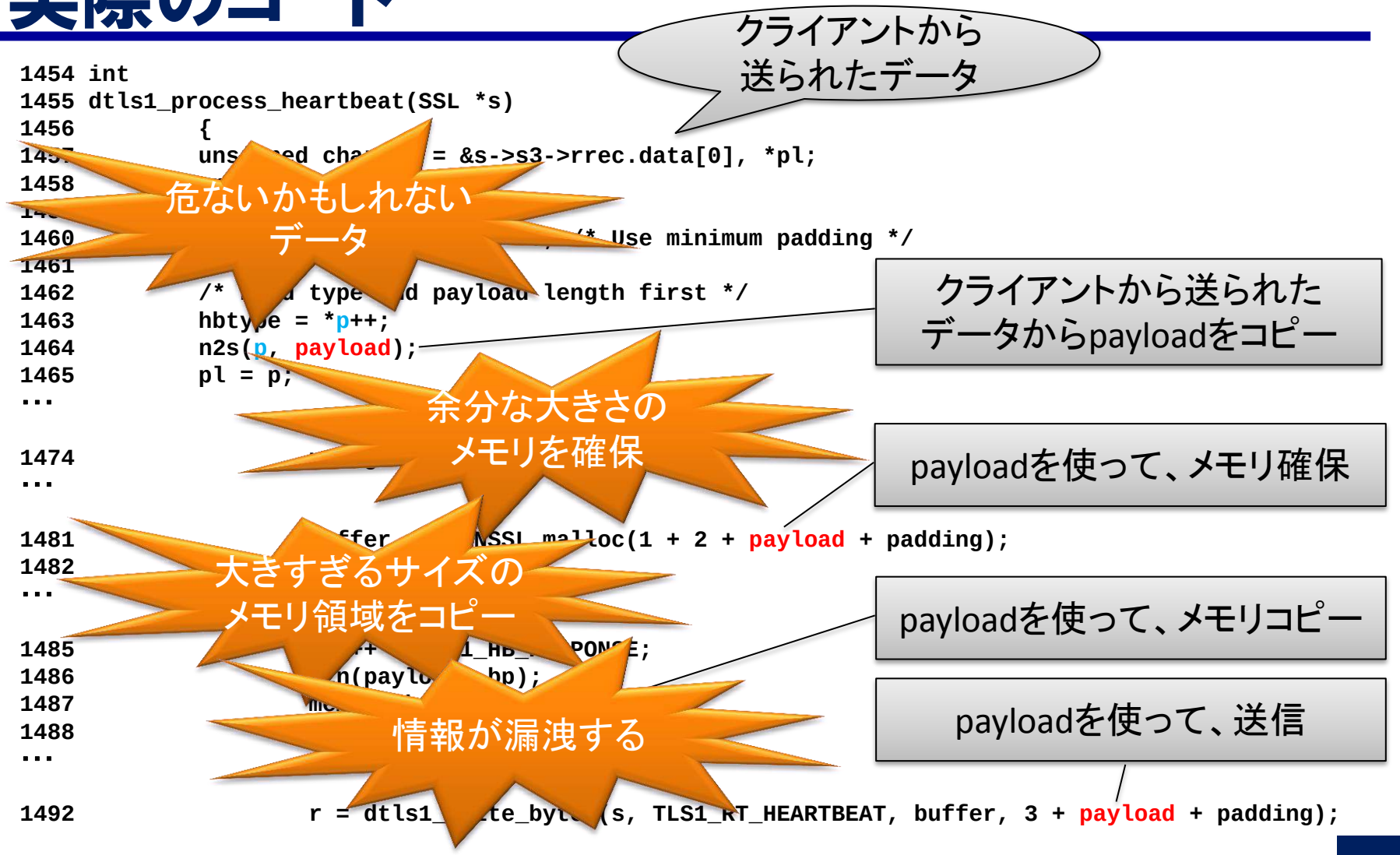
100文字

Hello

O SL

01011010
01010100
10101010
10101001
01010101
01001011
01010001
10010101
01010101
01001011

実際のコード




```
1454 int
1455 dtls1_process_heartbeat(SSL *s)
1456         {
1457         unsigned char *p = &s->s3->rrec.data[0], *pl;
1458
1460                                  /* Use minimum padding */
1461
1462         /* Read type and payload length first */
1463         hbtype = *p++;
1464         n2s(p, payload);
1465         pl = p;
...
1474
...
1481                 buffer = OPENSSL_malloc(1 + 2 + payload + padding);
1482
...
1485                 *bp++ = TLS1_HB_RESPONSE;
1486                 memcpy(bp, pl, payload);
1487                 bp += payload;
1488
...
1492                 r = dtls1_write_bytes(s, TLS1_RT_HEARTBEAT, buffer, 3 + payload + padding);
```

分析結果

Heartbeat Request

```
0000    18 03 00 00 03 01 40 00    あるべきデータがない    ......@.
```

18　Heartbeat

03 00　SSLv3

00 03　長さ

01　Request

40 00　ペイロード長 16384byte

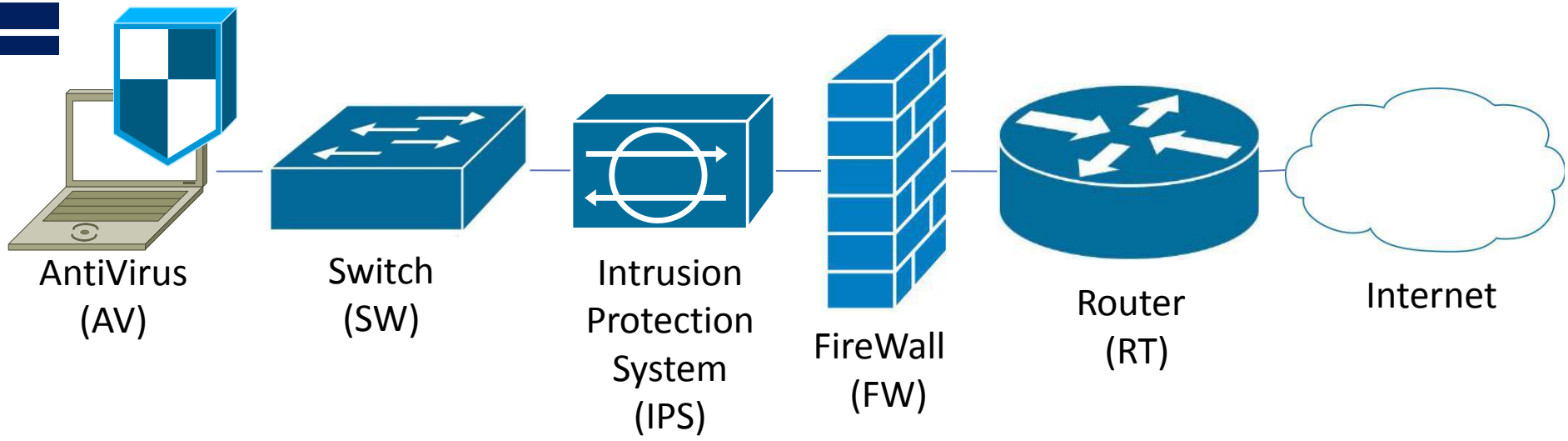
Heartbeat Response

```
0000    18 03 00 40 00 02 40 00 d8 03 00 53 43 5b 90 9d   ...@..@....SC[..
...     01    Request
00e0    40 00 74 3a 20 31 39 32 2e 31 36 38 2e 36 38 2e 32   .t: 192.168.68.2
00f0    31 33 0d 0a 49 66 2d 4d 6f 64 69 66 69 65 64 2d   13..If-Modified-
0100    53 69 6e 63 65 3a 20 57 65 64 2c 20 30 32 20 4a   Since: Wed, 02 J
0110    75 6c 20 32 30 31 34 20 30 36 3a 33 34 3a 31 33   ul 2014 06:34:13
0120    20 47 4d 54 0d 0a 49 66 2d 4e 6f 6e 65 2d 4d 61    GMT..If-None-Ma
0130    74 63 68 3a 20 22 31 66 39 66 38 2d 66 2d 34 66   tch: "1f9f8-f-4f
0140    64 33 30 31 34 39 66 64 35 35 64 22 0d 0a 43 6f   d30149fd55d"..Co
0150    6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41   nnection: Keep-A
0160    6c 69 76 65 0d 0a 41 75 74 68 6f 72 69 7a 61 74   live..Authorizat
0170    69 6f 6e 3a 20 42 61 73 69 63 20 59 57 52 74 61   ion: Basic YWRta
0180    57 35 70 63 33 52 79 59 58 52 76 63 6a 70 77 59   W5pc3RyYXRvcjpwY
0190    58 4e 7a 64 32 51 77 4d 54 49 7a 0d 0a 0d 0a 01   XNzd2QwMTIz.....
...
```

漏洩したデータ

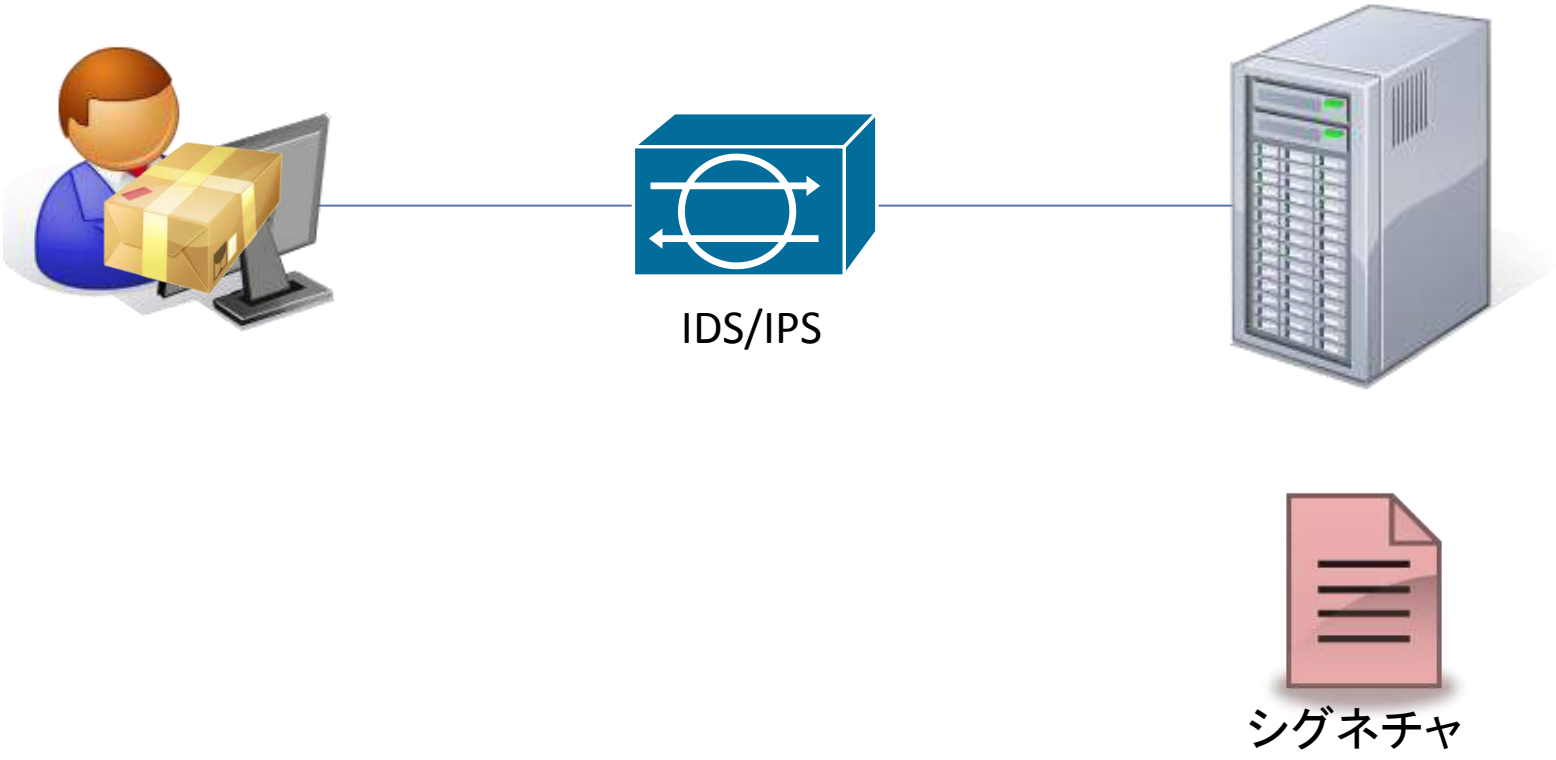
administrator:passwd0123　BASE64でデコード

従来のネットワークセキュリティの問題

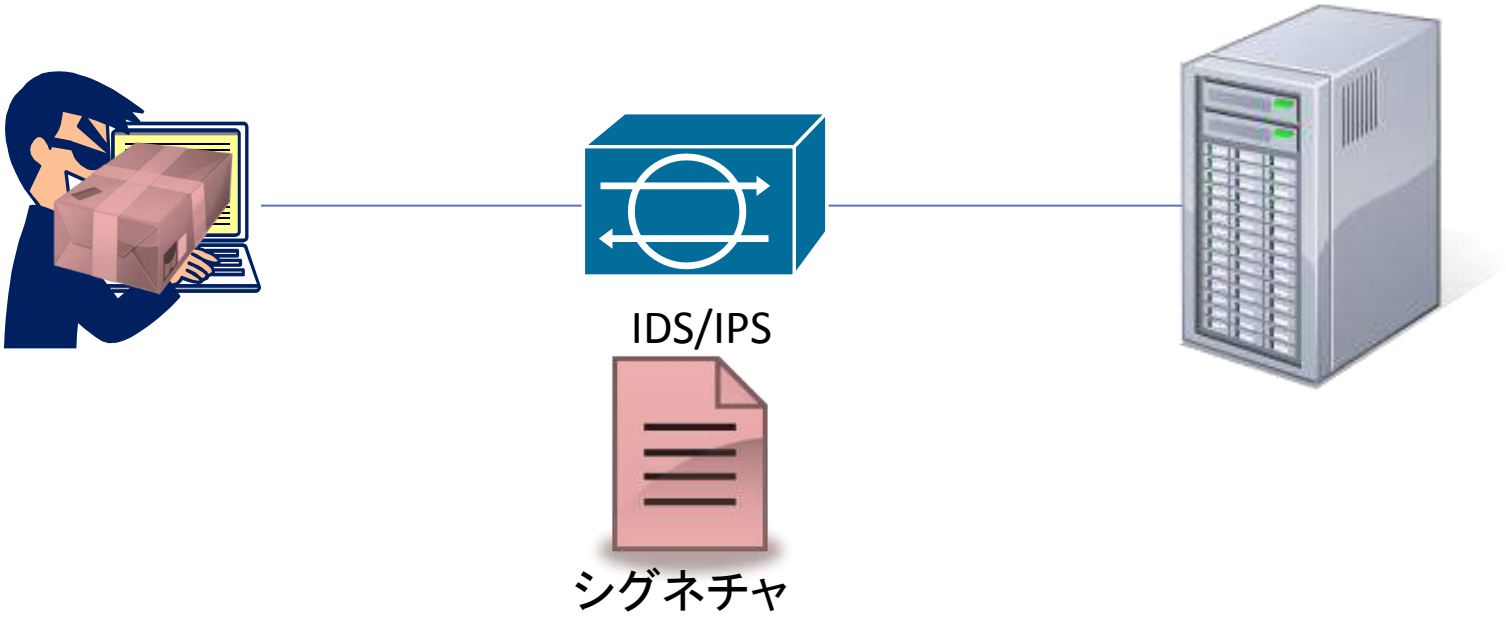


- FWは、IPアドレスとポートによるアクセス制御ルールに基づき、遮断
  - 通信の中身はチェックしない為、攻撃性のある通信を検知して遮断できない
- AVでは、不正プログラムを検知して、クライアントを防御
  - ブラックリスト(シグネチャ)で検知するため、未知のマルウェアは検知できない
  - 一度、感染するとすべての権限が乗っ取られるため、周囲へ被害が拡散する
- IPSでは、通信パケットの中身をチェックして、攻撃性を検知し、遮断
  - ブラックリスト(シグネチャ)で検知するため、未知の不正通信は検知できない
  - 外部への情報漏えいなど、通常の通信と見分けがつかないものは、遮断できない

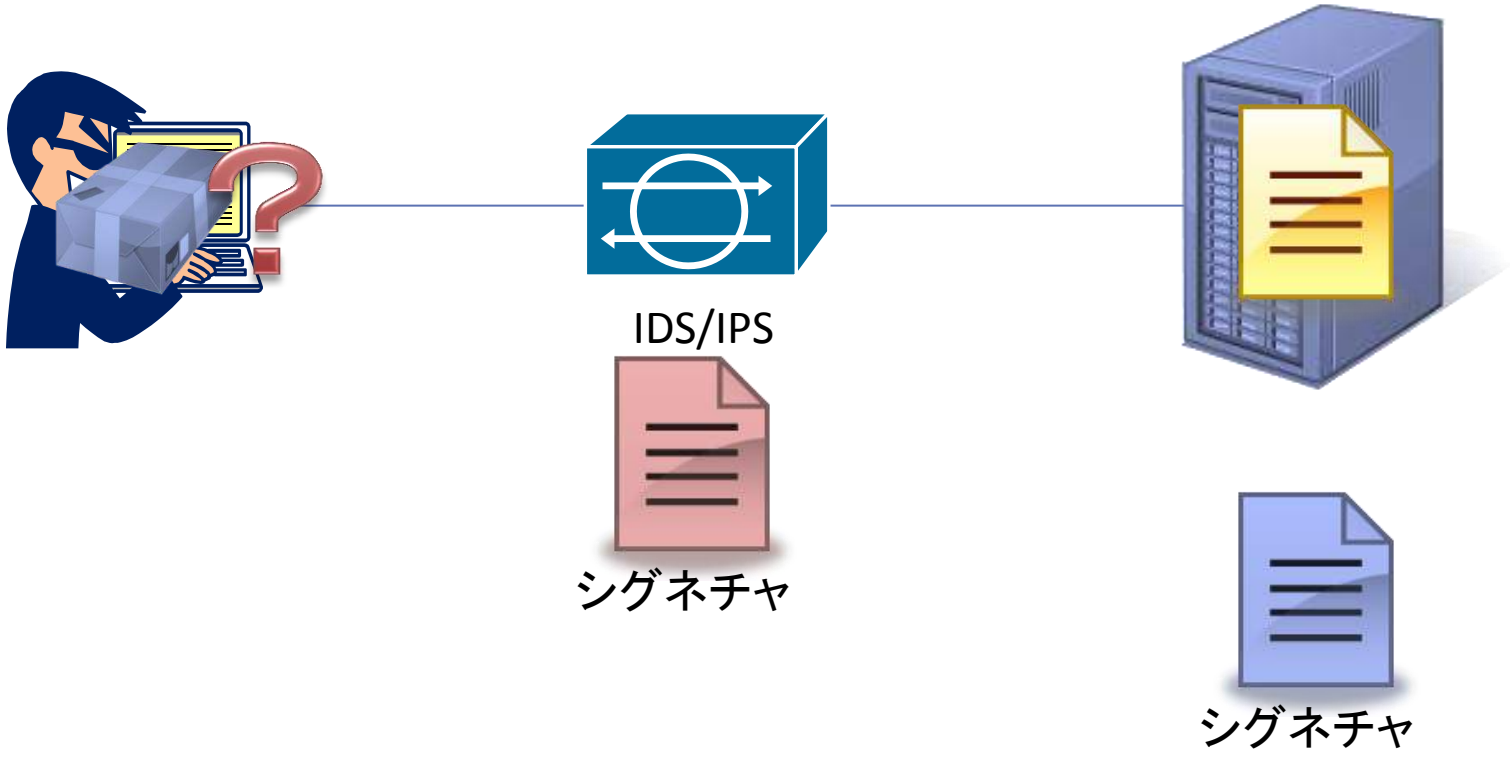
シグネチャによる攻撃検知



シグネチャによる攻撃検知



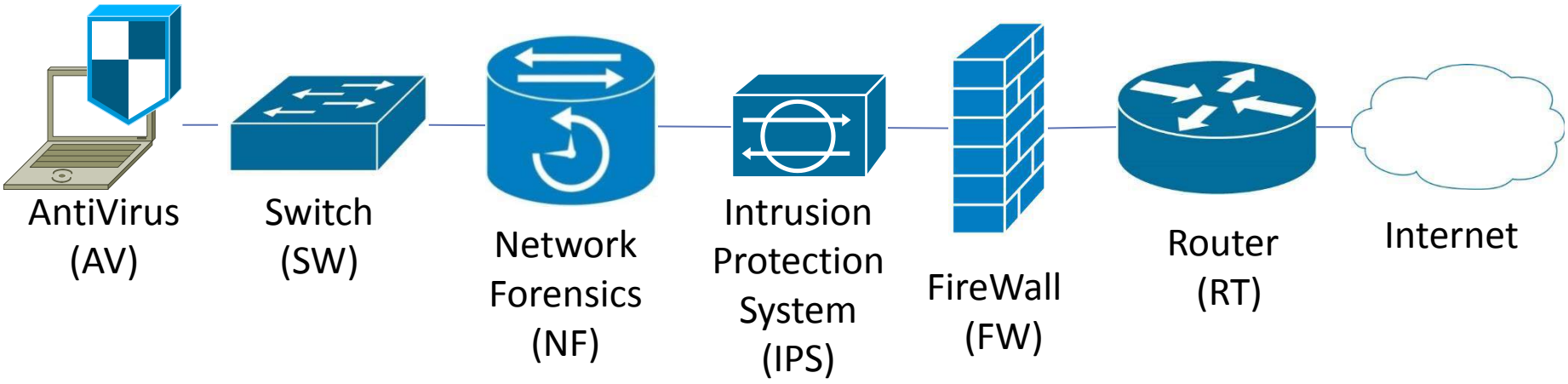
シグネチャによる攻撃検知



従来のネットワークセキュリティの課題

- 外部から行われる既知の攻撃を「防御」することを目的
  - シグネチャのない未知の攻撃は検知できない
  - 外部への情報漏えいを検知するのが難しい
  - 攻撃の影響範囲を特定するのが難しい
  - 攻撃に関連する事象の証拠保全が難しい

Network Forensics



インシデント発生を前提にしたセキュリティ対策が重要

- 情報漏洩やサイバー攻撃が頻発している現状において、事故の未然防止だけではなく、**事故発生後の迅速な対応能力**が求められている

顧客情報流出により企業ブランドや業績が低下する事件が頻発するなか、証拠保全/被害範囲特定に有効なネットワークフォレンジックスが注目される

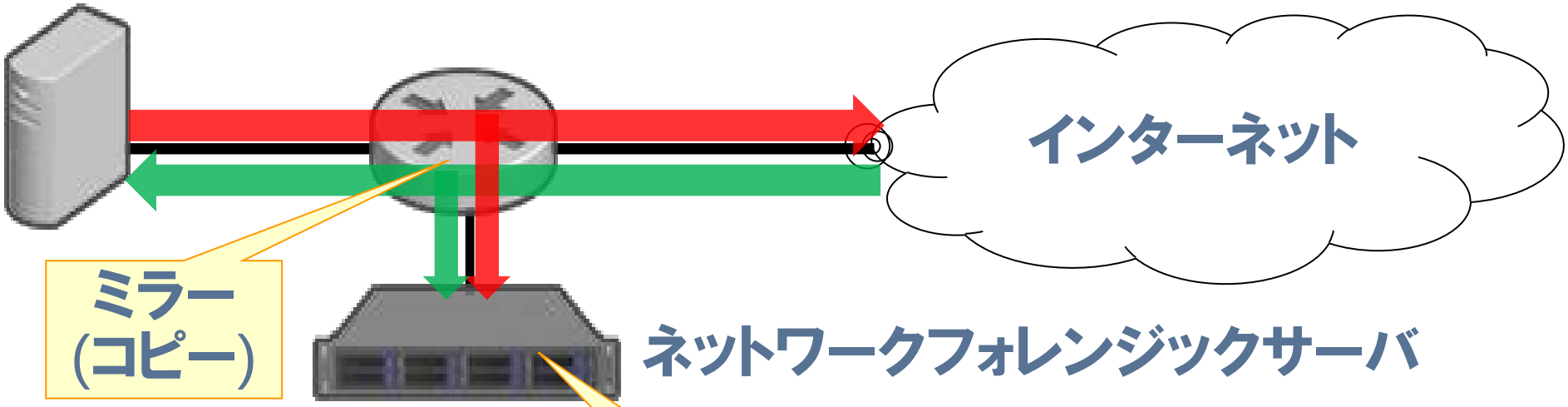
TUTEC AMENITY LIMITED

Forensicsとは？

- Forensicsとは？
  - Forensic（形容詞）では、「法廷の～」「法医学の～」
  - Forensics（名詞）では、「鑑識課」「科学捜査」
  - 犯罪立証のための物的証拠を採取し、証拠保全を行うこと
- Digital Forensicsとは？
  - コンピュータやネットワークに関する事象の、調査・分析と証拠保全
  - 大きく、Computer Forensicsと、Network Forensicsに分けられる
- Computer Forensics
  - コンピュータのハードディスクやメモリに記録された情報の分析
  - 証拠隠滅のために消去されたファイルの復元などを行う
  - 事件・事故の後に、事後的に調査分析が行われる

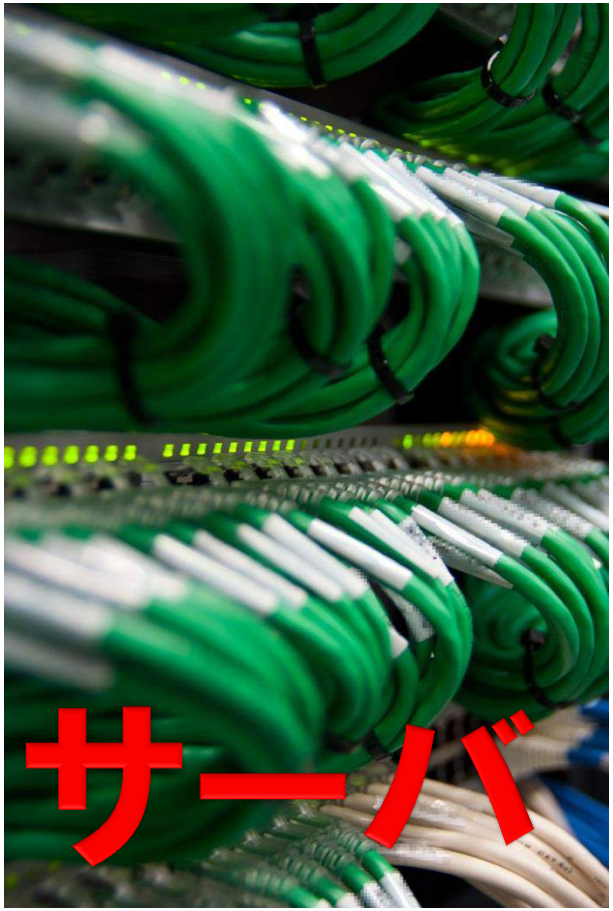
NetworkForensicsとは？

→ネットワーク上の通信をすべて記録し、証拠保全することで攻撃経路、被害範囲を特定するセキュリティ対策



犯罪の証拠保全→事故発生時に迅速に対応

現実世界のアナロジー



TUTEC
AMENITY LIMITED

ログ管理


```
127.0.0.1 - - [20/Jun/2003:20:45:14 +0900] "GET / HTTP/1.1" 200 1835
127.0.0.1 - - [20/Jun/2003:20:45:14 +0900] "GET /apache_pb.gif HTTP/1.1" 200 2326
127.0.0.1 - - [20/Jun/2003:20:45:20 +0900] "GET /manual/index.html HTTP/1.1" 200 9904
127.0.0.1 - - [20/Jun/2003:20:45:14 +0900] "GET / HTTP/1.1" 200 1835
127.0.0.1 - - [20/Jun/2003:20:45:14 +0900] "GET /apache_pb.gif HTTP/1.1" 200 2326
127.0.0.1 - - [20/Jun/2003:20:45:29 +0900] "GET /cgi-bin/tup.pl HTTP/1.1" 200 241
127.0.0.1 - - [20/Jun/2003:20:45:39 +0900] "POST /cgi-bin/tup.pl HTTP/1.1" 200 392
127.0.0.1 - - [20/Jun/2003:20:45:39 +0900] "POST /cgi-bin/tup.pl HTTP/1.1" 200 392
127.0.0.1 - - [20/Jun/2003:20:45:14 +0900] "GET / HTTP/1.1" 200 1835
127.0.0.1 - - [20/Jun/2003:20:45:14 +0900] "GET /apache_pb.gif HTTP/1.1" 200 2326
127.0.0.1 - - [20/Jun/2003:20:45:20 +0900] "GET /manual/index.html HTTP/1.1" 200 9904
127.0.0.1 - - [20/Jun/2003:20:45:14 +0900] "GET / HTTP/1.1" 200 1835
127.0.0.1 - - [20/Jun/2003:20:45:14 +0900] "GET /apache_pb.gif HTTP/1.1" 200 2326
127.0.0.1 - - [20/Jun/2003:20:45:29 +0900] "GET /cgi-bin/tup.pl HTTP/1.1" 200 241
127.0.0.1 - - [20/Jun/2003:20:45:39 +0900] "POST /cgi-bin/tup.pl HTTP/1.1" 200 392
127.0.0.1 - - [20/Jun/2003:20:45:39 +0900] "POST /cgi-bin/tup.pl HTTP/1.1" 200 392
127.0.0.1 - - [20/Jun/2003:20:45:14 +0900] "GET / HTTP/1.1" 200 1835
127.0.0.1 - - [20/Jun/2003:20:45:14 +0900] "GET /apache_pb.gif HTTP/1.1" 200 2326
127.0.0.1 - - [20/Jun/2003:20:45:20 +0900] "GET /manual/index.html HTTP/1.1" 200 9904
127.0.0.1 - - [20/Jun/2003:20:45:14 +0900] "GET / HTTP/1.1" 200 1835
127.0.0.1 - - [20/Jun/2003:20:45:14 +0900] "GET /apache_pb.gif HTTP/1.1" 200 2326
127.0.0.1 - - [20/Jun/2003:20:45:29 +0900] "GET /cgi-bin/tup.pl HTTP/1.1" 200 241
127.0.0.1 - - [20/Jun/2003:20:45:39 +0900] "POST /cgi-bin/tup.pl HTTP/1.1" 200 392
- [20 n/2003:20: 39 +0900] " bin/tup.pl HTTP/1.1" 392
```

アクセスログ

TOTEC AMENITY LIMITED

サイバー世界の監視カメラ

監視カメラ　通信パケットキャプチャ

脅威を可視化する

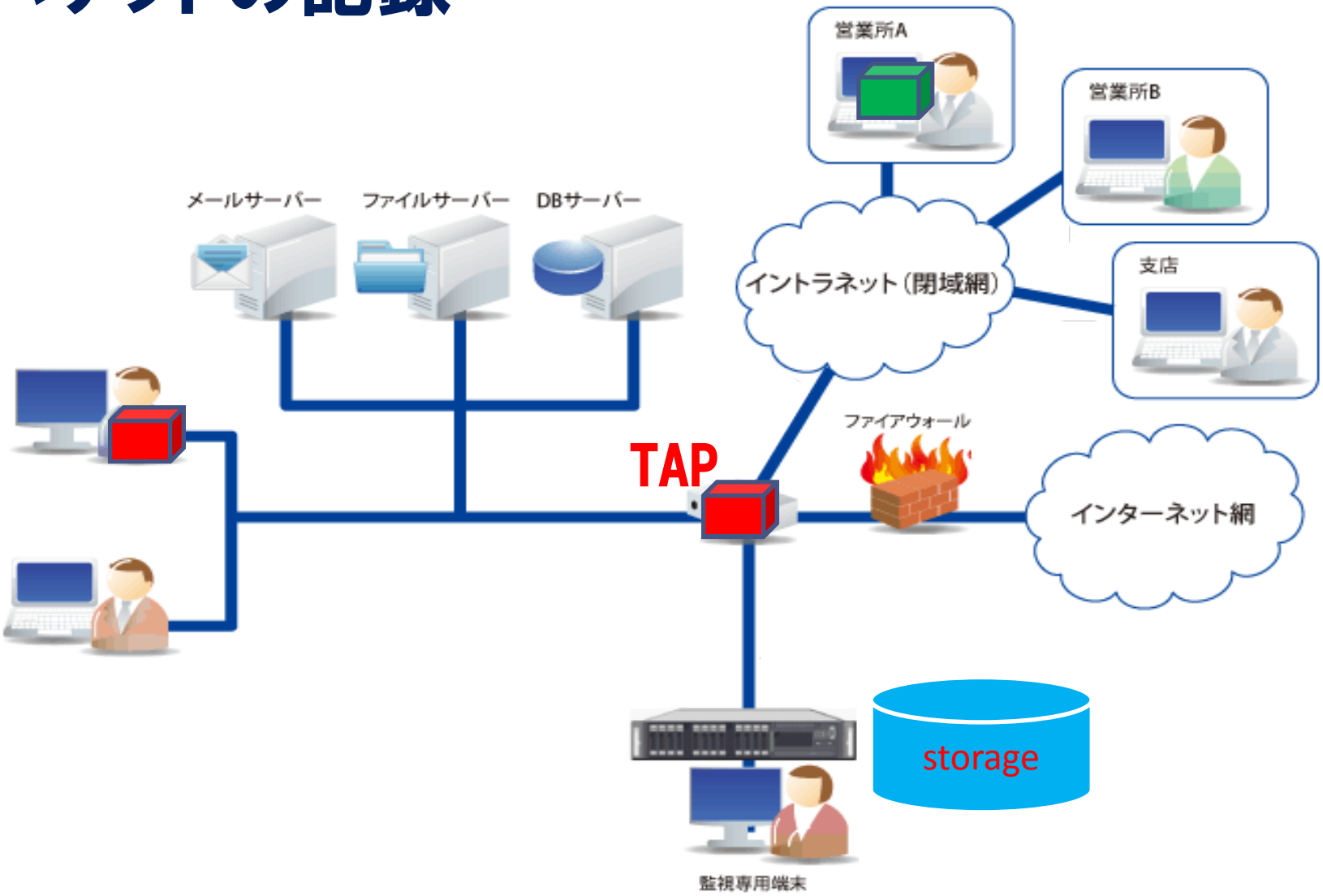
```
<script type="text/javascript" src="common/js/jquery.js"></script>
<script type="text/javascript" src="common/js/scroll.js"></script>
<script type="text/javascript" src="common/js/jquery.page-scroller.js"></script
<script type="text/javascript" language="javascript" src="common/js/heightLine.
<!-- JASNET, INC. Web Analysis & Live Chat START -->
<script type="text/javascript">
//<![CDATA[
function xlogAScript(){
        HTTP_MSN_MEMBER_NAME="";/*member name*/
        var
prtc=(document.location.protocol=="https:")?"https://":"http://";
        var hst=prtc+"conf.log-marketing.jp";
        var rnd="r"+(new Date().getTime()*Math.random()*9);
        this.ch=function(){

if(document.getElementsByTagName("head")[0])[this.dls();]else[window.setTimeout(x
        }
        this.dls=function(){
                var h=document.getElementsByTagName("head")[0];
                var
s=document.createElement("script");s.type="text/jav"+"ascript";try[s.async=true;]c

if(h)[s.src=hst+"/UsrConfig/t/Conf_totec062130.js?s="+rnd;h.appendChild(s);]
        }
        this.init= function(){
                document.write('<img src="'+hst+'/sr.gif?d='+rnd+'" style="width:
        }
}
if(typeof xlogAnalysis=="undefined"){   var xlogAnalysis=new
xlogAScript();xlogAnalysis.init();}
//]]>
</script>
<noscript><img src="
http://suite.log-marketing.jp/HTTP_MSN/Messenger/Noscript.php?key=totec062130
" border="0" style="display:none;width:0;height:0;" />
</noscript>
<!-- JASNET, INC. Web Analysis & Live Chat END -->
</head>

<body id="to ge">
<div i "hea ">
<
<div ass="  o"><  ef="http:/ w.netraptor  "><img src="im /1.gif" alt=
<
```

エックス線　フォレンジック

手荷物検査　調査

TOTEC AMENITY LIMITED

パケットの記録


営業所A
営業所B
支店
メールサーバー
ファイルサーバー
DBサーバー
イントラネット（閉域網）
ファイアウォール
TAP
インターネット網
storage
監視専用端末

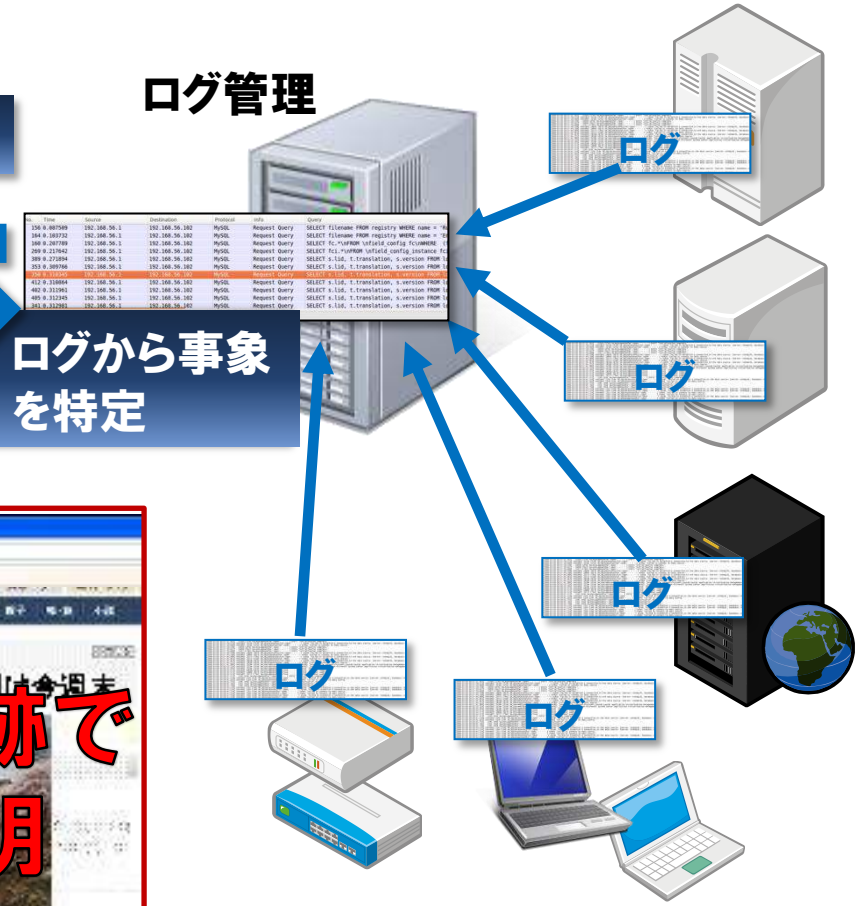
ログ管理とネットワークフォレンジック

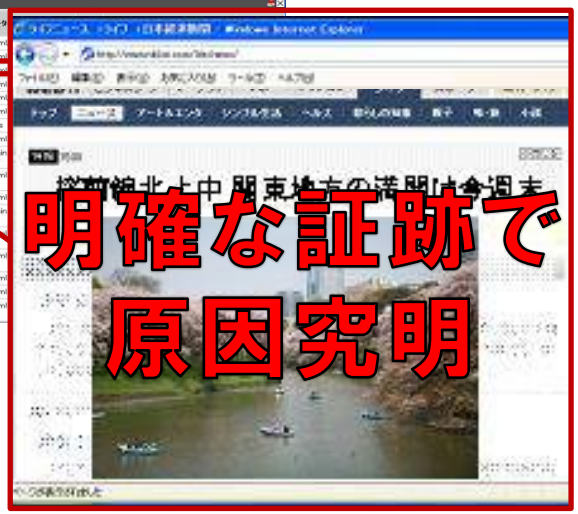
ネットワーク
フォレンジックス

実際の通信内容を復元

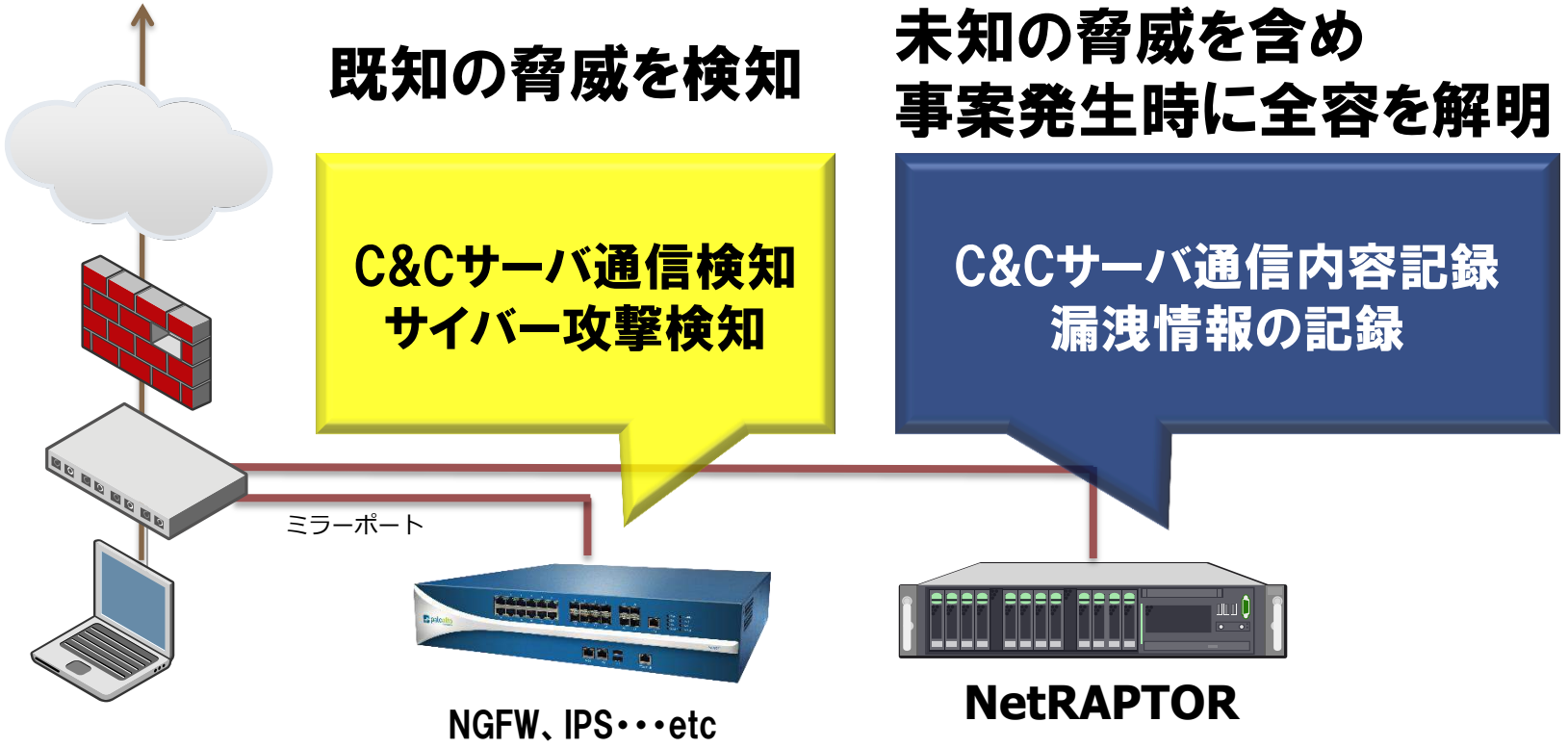
ログから事象を特定

ログ管理





検知だけではわからない事象の全容を記録

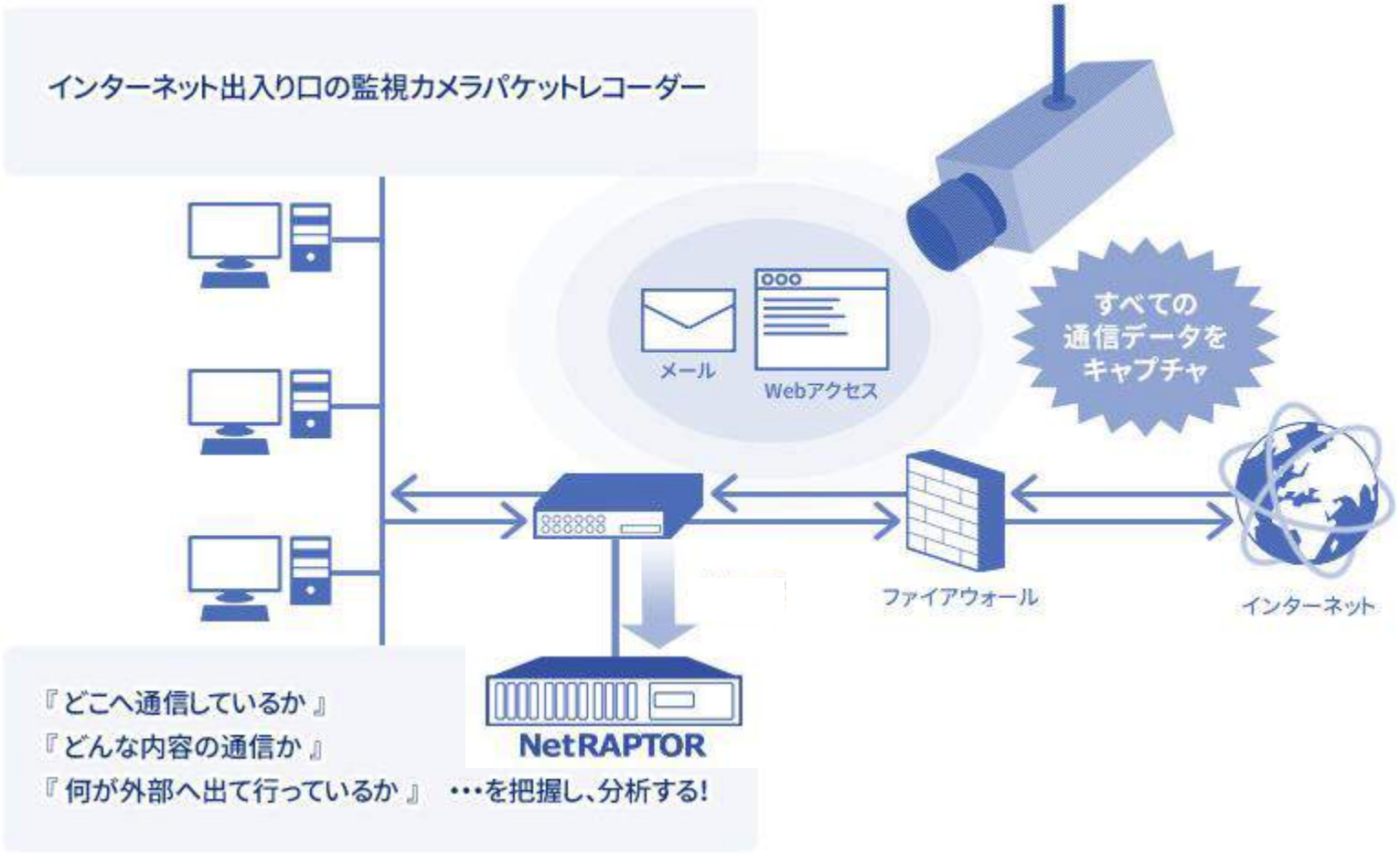


NetRAPTOR

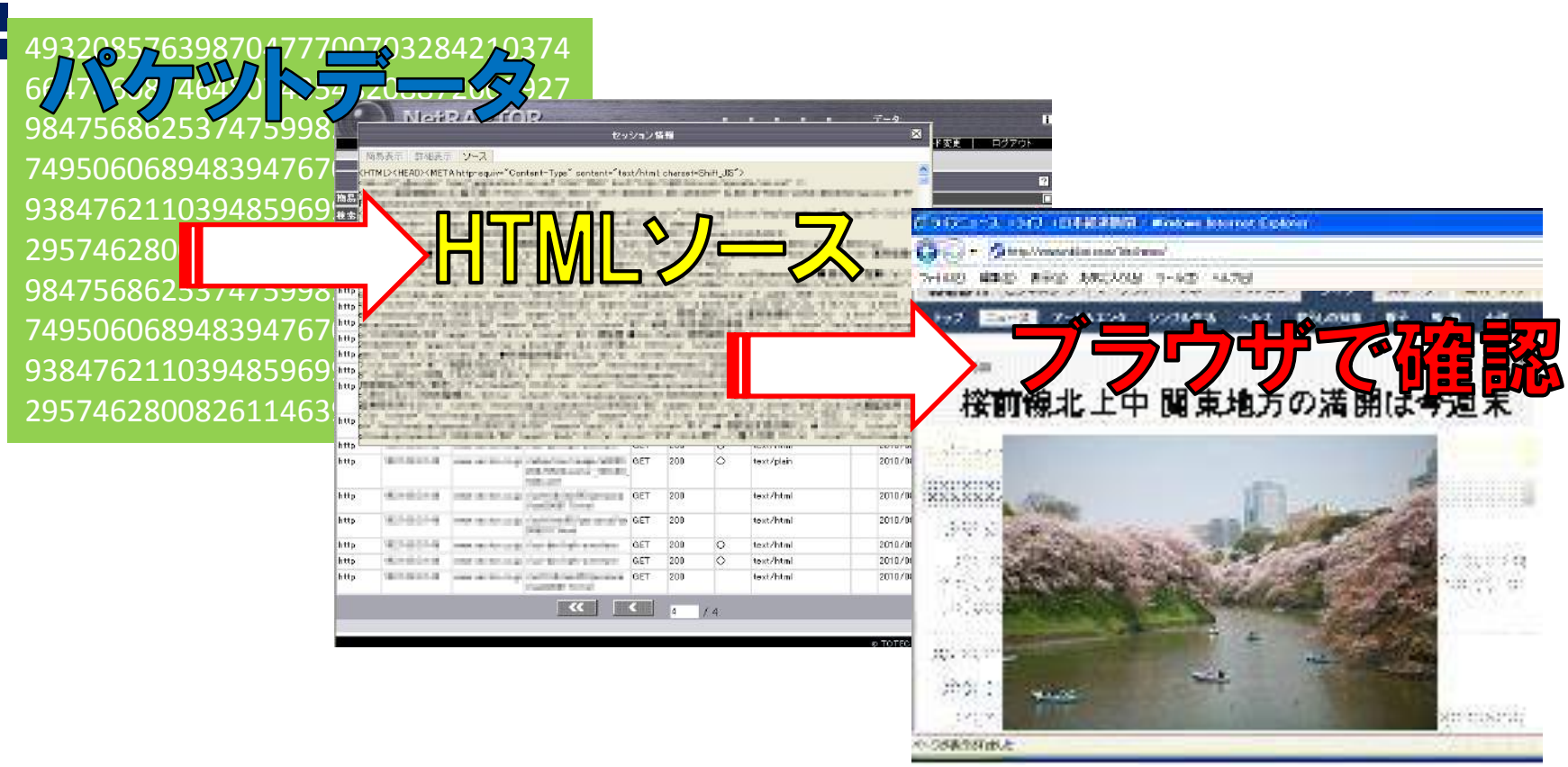
Unified Network Forensic Appliance

TUTEC
AMENITY LIMITED

NetRAPTORとは

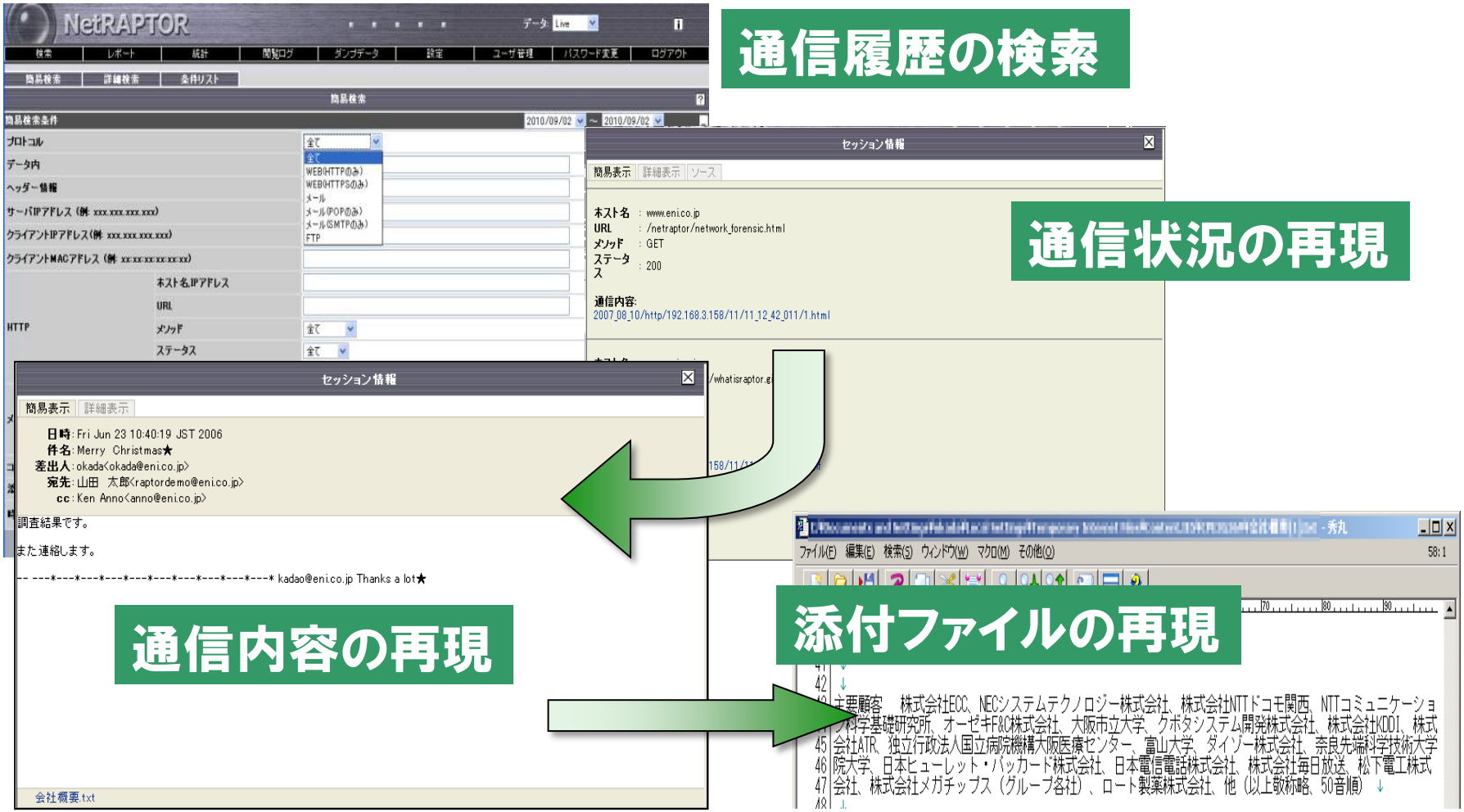


プロトコル解析とデータの復元



TCP/IPパケットをそのままでは理解できないので、プロトコル、セッション毎に通信を組み立てることで、誰にでも見える形に再現する

通信内容の見える化

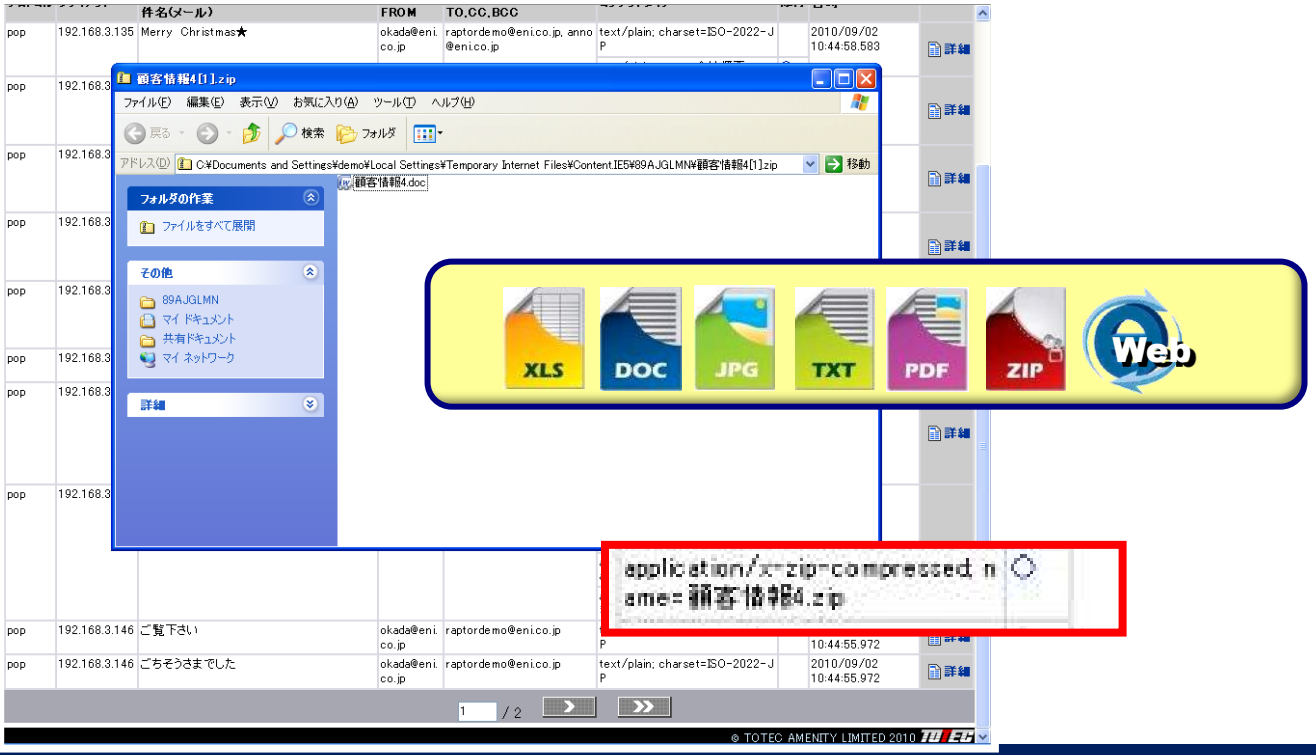

NetRAPTOR
通信履歴の検索
通信状況の再現
セッション情報
簡易表示
詳細表示
日時: Fri Jun 23 10:40:19 JST 2006
件名: Merry Christmas★
差出人: okada<okada@eni.co.jp>
宛先: 山田 太郎<raptordemo@eni.co.jp>
cc: Ken Anno<anno@eni.co.jp>
調査結果です。
また連絡します。
-- ---*---*---*---*---*---*---*---*---* kadao@eni.co.jp Thanks a lot★
会社概要.txt
通信内容の再現
添付ファイルの再現

高速で簡単な全文検索

NeTRAPTORが採用している独自の高速全文検索エンジンで高速検索を行い、情報を様々な角度から検索・分析することが可能

添付ファイルの再現と検索

再現し、かつ、その中を検索できるファイルは、MS Office系のドキュメントや、pdf 、そしてzipファイルなどが対象になります
※CADデータや画像など再現はします。



問題行動の監視と警告

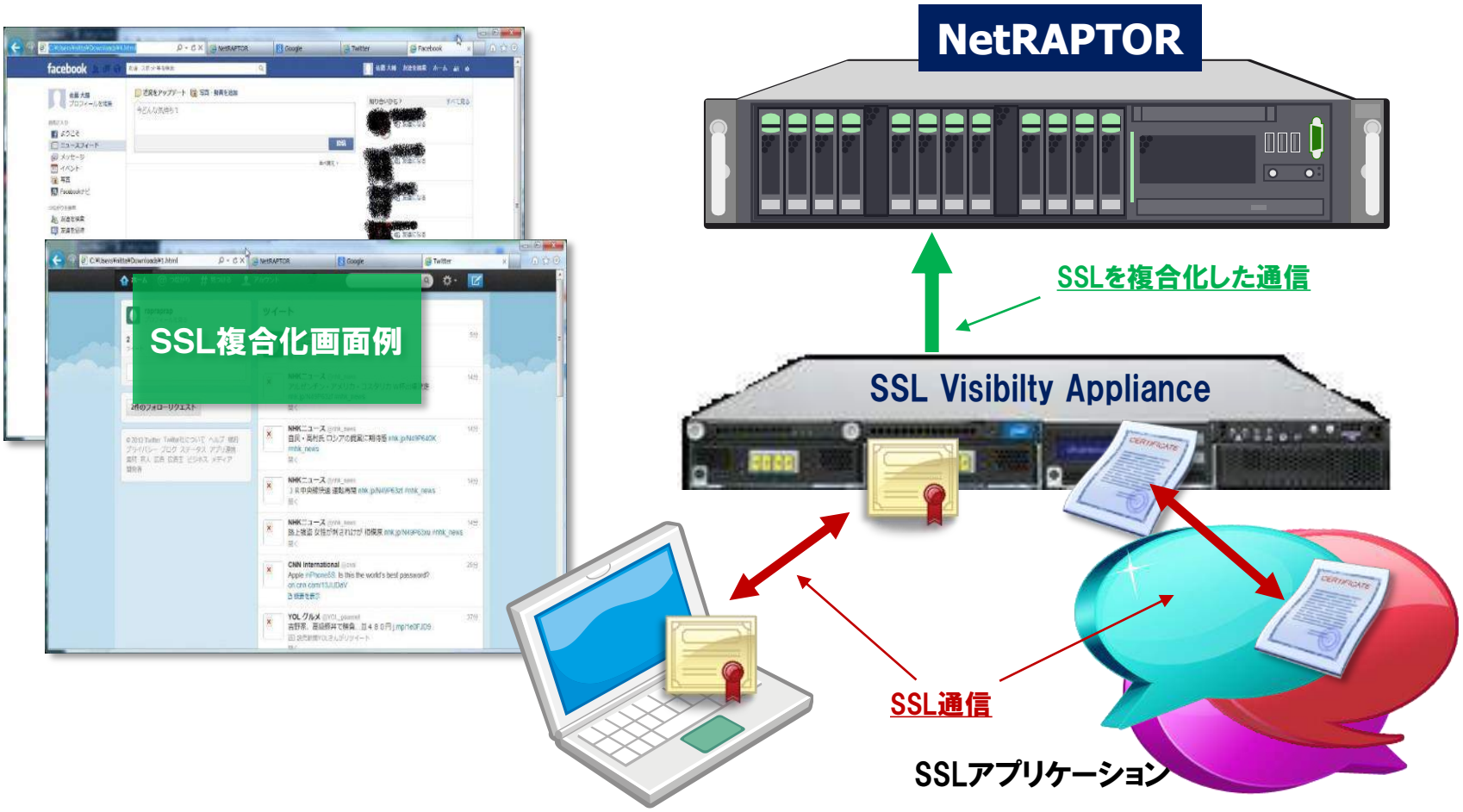
条件式例）添付ファイルつきのWebメール送信

アラート条件	登録者	名前
警告	初期管理者	1-1 Yahooメール(添付ファイル付)
注意	初期管理者	1-2 2chへのアクセス
なし	初期管理者	1-3 HTTPS通信
注意	初期管理者	2chへの投稿
警告	初期管理者	FTP通信
なし	初期管理者	Googleへのアクセス
警告	初期管理者	webへのpost
警告	初期管理者	yahoo MSN
なし	初期管理者	yahoo text
なし	初期管理者	yahoo access

検索条件登録	
名前	1-1 Yahoo
検索条件	protocol:ht
コメント	
アラート条件	警告
対象アナライザ	全アナライ
メール送信先	初期管理者

該当事象が発生すると
リアルタイムで警告メールを発信

SSL通信の解析・再現


NetRAPTOR
SSLを複合化した通信
SSL Visibilty Appliance
SSL複合化画面例
SSL通信
SSLアプリケーション

執拗な巧妙で標的型メール攻撃

- 成功するまで、何度でも、執拗に試みられる標的型メール攻撃
  - 攻撃側も失敗から学び、さらに精巧な侵入を試みるようになる
- 標的型メール攻撃は、ますます巧妙化
  - 新聞等の取材申し込み、人事部へのエントリーシート、行政機関への陳情書
  - ファイルを開いて確認せざるを得ない

人に頼り切った標的型メール攻撃対策の問題

- 教育/訓練により、標的型メール攻撃を見抜いて、防御できることを前提にできるか？
  - 全員が正しく対処できることを期待することは難しい
  - 対策を進めることで、攻撃者がさらに進化
- 訓練の成果を開封率で見ても意味がない
  - 攻撃は、一か所でも成功すればよい。**防御は、すべて守りきらなければならない**
  - 役職者が一人、開封するだけで、甚大な被害が起こる
- **セキュリティシステムの強化で、標的型メール攻撃を検知する仕組みが必要**

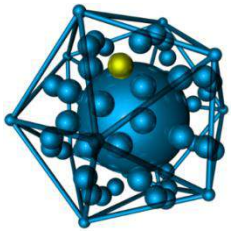
サンドボックス型マルウェア検知エンジンとネットワークフォレンジックスの連携

トーテックアメニティ株式会社
http://www.totec.co.jp

高機能ネットワークフォレンジックサーバ
NetRAPTOR

標的型攻撃の自動検知

株式会社ＦＦＲＩ
http://www.ffri.jp



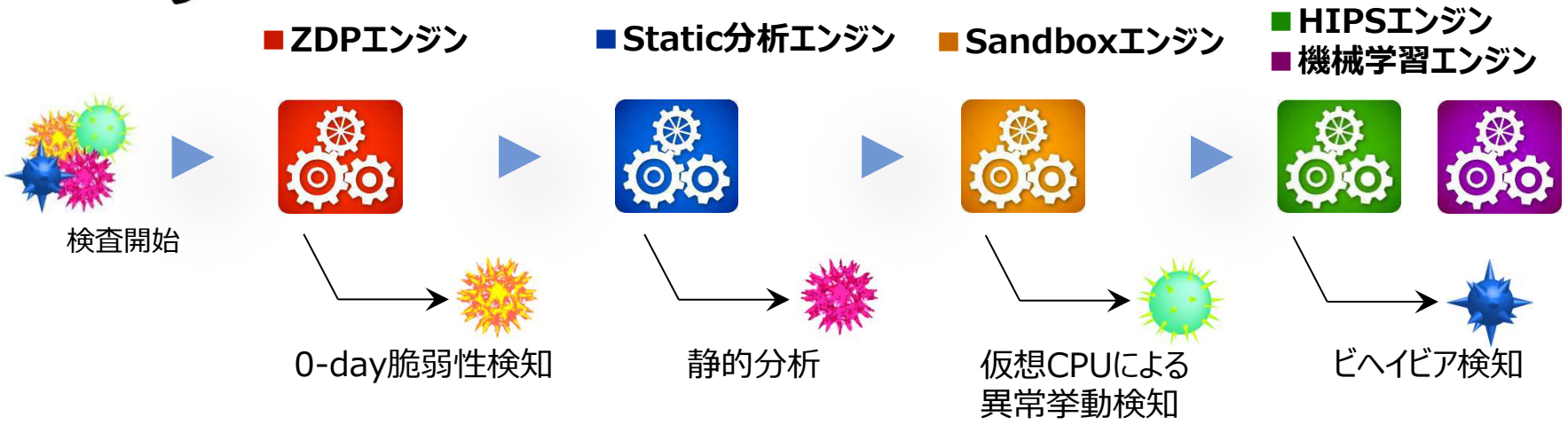
マルウェア自動解析システム Yarai Analyzer

サンドボックス型マルウェア検知とは

- サンドボックスとは？
  - 保護領域内でプログラムを動作させることで、外部への影響を隔離するセキュリティモデル
  - 「子供を砂場（サンドボックス）の外で遊ばせない」という言葉が語源
  - プログラムが暴走したり、悪質なウイルスであっても、「箱」の外に影響を与えない
- サンドボックス型マルウェア検知
  - 仮想マシンでサンドボックスを作り、プログラムをサンドボックス内で挙動解析し、マルウェアを検知
  - シグネチャの存在しないマルウェアも検知可能

FFR yarai のエンジンでパターンファイルに依存せず振る舞い検知

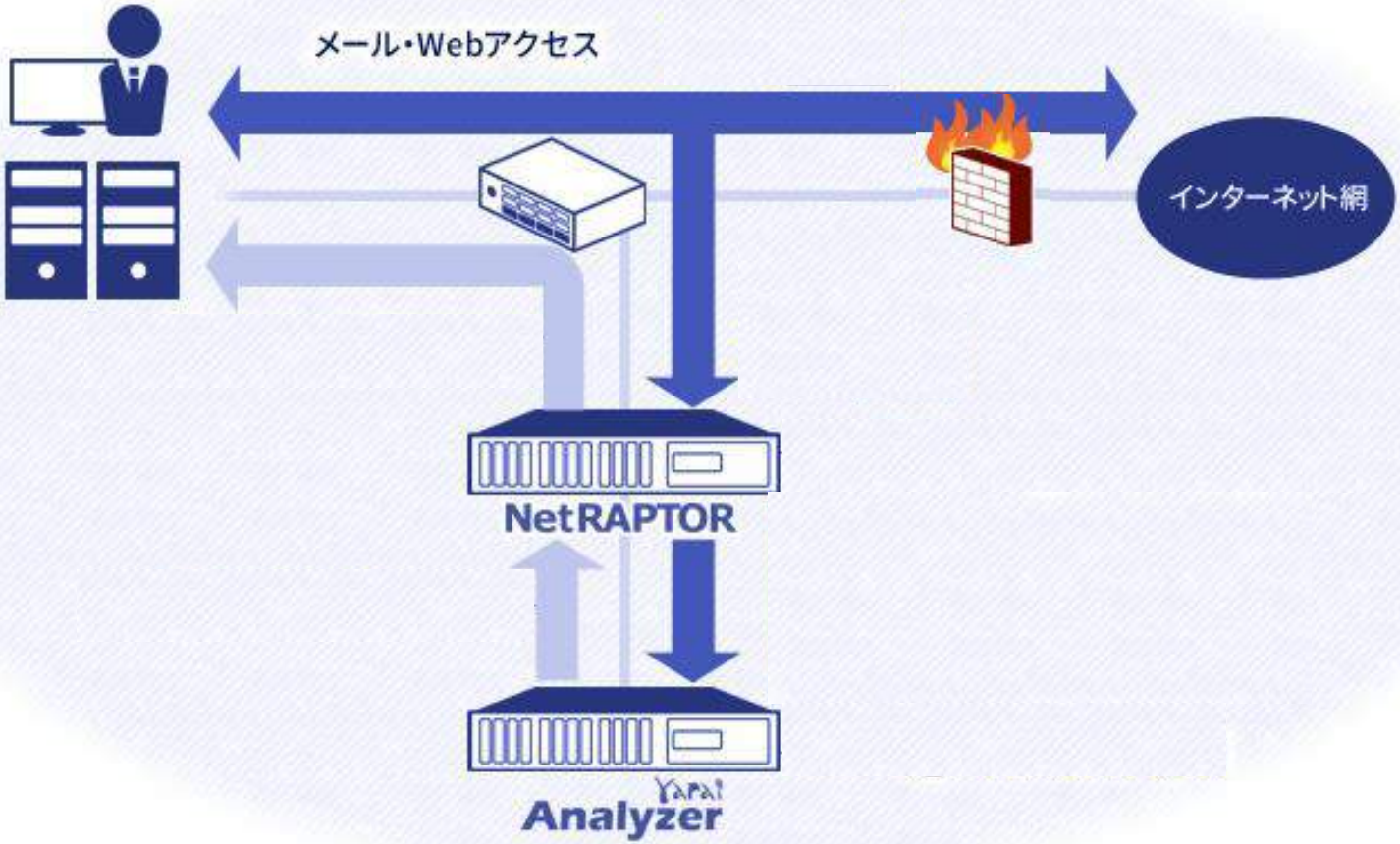
Yaraiが搭載する5つの振る舞い検知エンジン



パターンファイルに依存することなく、
0-day攻撃をはじめとした未知の攻撃を検出可能

- **近年のマルウェアは、解析されることを前提に様々な細工が施されている**
- **これらマルウェアを多数解析し、解析を妨害するロジックを解析、解明**
- **妨害ロジックもマルウェアの特徴として認識、判定**

NetRAPTORとFFR yarai analyzerによる純国産「サンドボックス型マルウェア検知システム」を共同検証



NetRAPTOR & FFR yarai analyzerのポイント

- パケットキャプチャによる通信データの証拠化
- Web/Mailのプロトコル解析による通信の見える化
- 高速な全文検索エンジンによるフォレンジック調査
- 混在する日本語文字コードへの対応
- アラート条件による情報漏えいの監視
- SSL通信の解析機能
- “完全振舞い検知”による未知攻撃の検出
- 関連する通信の記録による侵入経路の調査
- 純国産サイバーセキュリティソリューションの安心感

本日は、御清聴いただき、
誠にありがとうございました

TOTEC
AMENITY LIMITED