

PCIDSSセキュリティフォーラム2014

サイバー攻撃、その被害実態を 解明する手段とは？

～サイバー攻撃の証跡を解明する
ネットワークフォレンジックご紹介～

2014年7月29日

トーテックアメニティ株式会社

テクニカルサービス事業部セキュリティシステム部

トーテックアメニティ会社概要

金沢営業所

高岡営業所

岐阜事業所

本社
(名古屋)



大阪事業所



福岡事業所

東北オフィス

トヨタ事業所

東濃・各務原・春日井・刈谷SC

東京本社



【設立】昭和46年5月20日
【資本金】1億8,062万円
【売上高】182億2,992万円(連結)

*2014年3月期

【社員数】1,835名(連結)

*2014年6月末現在

【事業内容】

1. システムインテグレーション(SI)事業
2. ソフトウェア開発請負、
機械・電気・電子設計派遣事業

トーテックアメニティ事業構成

情報化戦略

有機的に結合

テクノロジーアウトソーシング
(Technology Outsourcing)事業

エンジニアリング

ICTアライアンス

テクニカルサービス

開発請負・技術者派遣

ソリューションアウトソーシング
(Solution Outsourcing)事業

公共医療システム

産業システム

ネットワークソリューション

システムインテグレーション(SI)

有機的に結合

技術戦略

新規事業への取り組み



To the future
Totec Amenity Recruiting 2015



特集

次のステージへ

Next Business style

次代の社会に貢献する新しい価値を生み出しています。



スマートコミュニティ

あらゆる技術と企業が融合し、システムとなる次世代社会の実現

3つの目的事業モデルであるスマートコミュニティの概念である「クラウドコンピューティング」、「IaaSプラットフォーム」、「無線通信」、「ネットワーク」、「IoT/クラウド/AI」の活用によるネットワーク構築です。また、スマートコミュニティの活用により、電力・ガス・水道の効率的な供給を実現します。

◆関連ページはこちら
[トーテックアメニティサイト](#) | [製品・サービス情報](#) | [スマートコミュニティ](#)



福祉・介護システム

自治体・介護事業者・ユーザをつなぐ情報インフラを整備

●福祉・介護システム
 ●介護事業者情報連携システム「けあプロ・new」
 ●情報プラットフォーム「ケア倶楽部」
 ●適正化支援パッケージ「トリトンモニター」

◆関連ページはこちら
[トーテックアメニティ](#) | [福祉・介護システム紹介](#)

セキュリティソリューション

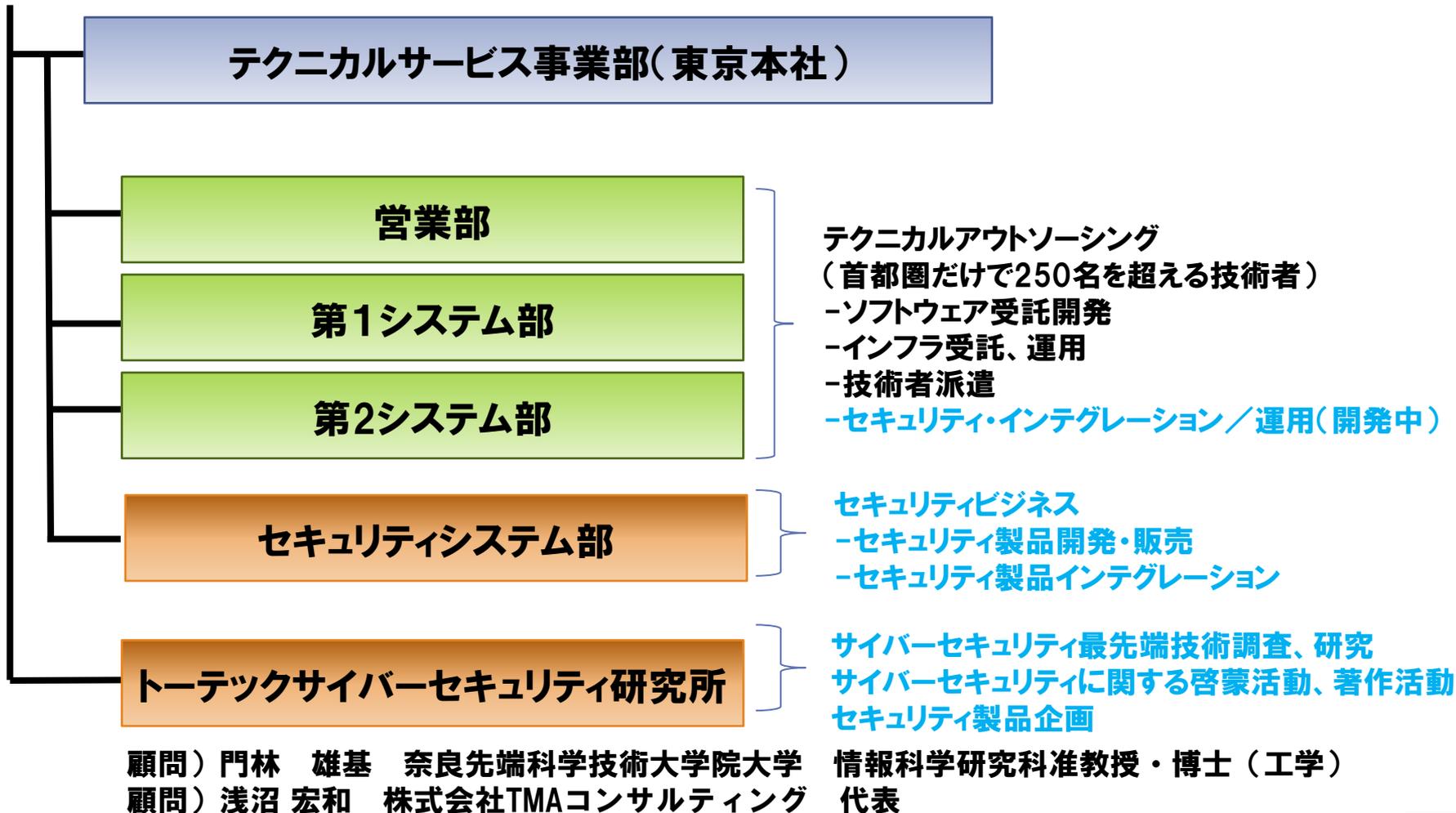
セキュリティ強化を次のステージへ



- NetRAPTOR
 企業とインターネットの出入り口を流れるすべての通信データを記録・保存・解析。内部監査対策や、情報流出事故に備えるための高性能ネットワークフォレンジックサーバ。
 ◆関連ページはこちら [NetRAPTORサイト](#)
- EASY FILE EXPRESS
 ビジネス専用のセキュアな大容量ファイル・データ送信サービス。SSL暗号化・操作ログ管理で高セキュリティを実現。一度に最大10GMまで送信可能であり、高速通信バージョンも開発。
 ◆関連ページはこちら [EASY FILE EXPRESSサイト](#)
- MagiPass
 ワンタイムパスワード生成システム&トークン型認証ソリューション。USBポートへトークンを差し込むだけで、ワンタイムパスワードを生成。
 ◆関連ページはこちら [MagiPassサイト](#)
- トーテックサイバーセキュリティ研究所
 お客様を守り、自社を守り、ひいては社会を守るために。サイバー社会を通してより良い社会を共に創っていくことがミッション。
 ◆関連ページはこちら
[トーテックアメニティサイト](#) > [製品・サービス情報](#) > [トーテックサイバーセキュリティ研究所](#)



テクニカルサービス事業部



サイバーセキュリティ啓蒙活動の取組み

サイバーセキュリティ

サイバーセキュリティと経営戦略 研究会 [編]

CYBERSECURITY

サイバーセキュリティは、現代社会を機能不全から守る必須要件となった！
国家の安全保障のみならず、市民生活と経済活動のあらゆる場面に
関わる現代社会人にとって、その本質を見極めることは急務である。

本書は、サイバーセキュリティの技術的な視点にとどまらず、
「サイバー攻撃の実態」「セキュリティ概念」「政府の政策」
「国際的動向」「経営におけるサイバーリスク管理」「法の現状」の観点から
多面的に解説し、豊富な知見を提示する。

**サイバーリスクに立ち向かい、
新たな価値を創造する！**

本書は世に出るべくして出た良書であり、“痺
い処に手が届く”内容が随所に発見できる。執
筆者らの研究成果が遺憾無く発表されており、
実務に携わる技術者に幅広い素養を身につけ
させるばかりでは無く、IT関連の社会学での講
義材料にも活用できる価値が高い書である。

(中略)

ITの観点から見たコーポレートガバナンス論や
内部統制論についても啓蒙される事が多い。今
後も情報セキュリティ論も進化を余儀なくされる
中で、本書により様々な課題解決の研究に着
手して組織運営や経営戦略へITツールを積極
的に導入する事例が増えていくと思う。

アマゾン書籍レビューより抜粋
石津 龍虎 アマゾンTOP1000レビューワ

NTT出版・新刊『サイバーセキュリティ』2014年3月13日(木) 発売

～サイバーセキュリティと経営戦略研究会[編]

※サイバーセキュリティと経営戦略 研究会

事務局 トーテックアメニティサイバーセキュリティ研究所

著者: 守屋英一氏(日本アイ・ビー・エム株式会社)

藤原礼征氏(トーテックサイバーセキュリティ研究所 所長)

武智洋氏(株式会社ラック、日本セキュリティオペレーション事業者協会代表)

門林雄基氏(奈良先端科学技術大学院大学 情報科学研究科 准教授)

浅沼宏和氏(株式会社TMAコンサルティング代表取締役)

杉浦 宣彦氏(中央大学大学院 戦略経営研究科 教授)



トーテックサイバーセキュリティ研究所
所長 藤原 礼征 著
2012年3月 中経出版社

サイバーセキュリティ脅威対策製品

- 弊社企画・開発によるサイバーセキュリティ脅威対策製品

NetRAPTOR

インターネット通信の全記録と見える化によるサイバー攻撃の早期発見と追跡
中央省庁、大企業を中心に導入

MagiPass

モバイル・在宅環境から社内システムへのアクセスでのなりすましを防ぐ、安全で強固な二要素認証を実現
企業向けでは、SSL VPNの強化策として、また特に金融系では不正アクセス・不正送金防止対策として注目

EASY FILE EXPRESS

社外と社内との安全・安心なデータのやり取りを実現する大容量のファイル送受信ソリューション
全国で50を超える自治体での導入実績、10000人を超える利用実績。ビジネス向け製品として自治体、大企業を中心に利用者増加中

セキュリティ対策製品インテグレーション

- セキュリティ対策は極めて幅広く多岐に渡る
 - 利用する製品・サービスも多くなる
- 
- お客様の状況に合わせた製品・サービス選定
 - セキュリティ導入・運用のインテグレーションサービスご提供

入口対策

代表的な対策

次世代ファイアウォール
マルウェア検知システム
(sandbox)
IPS/IDS
認証強化(二要素認証)
Web Application Firewall
Proxy ... etc

内部対策

代表的な対策

アンチウィルス
未知のマルウェア対策
エンドポイント管理/MDM
DB/ ファイル監視
ログ管理
SIEM ... etc

出口対策

代表的な対策

ネットワークフォレンジック
Data Loss Prevention
ボットネットアクセス監視
次世代ファイアウォール
メールセキュリティ
ファイル送信システム...etc

セキュリティ対策導入インテグレーション

直近のサイバー攻撃と被害の状況

- 8～9割の企業から標的型ウイルスが見つかる(ファイア・アイ)
- 「ブラックPOS」が日本でも検出された
 - 昨年末、ターゲットのPOSシステムからクレジットカード情報を1億1千万件を盗んだウイルス
- ネットバンキングからの不正送金を狙う攻撃による昨年度の被害総額は14億円超
- 日本で検出される不正送金ウイルス数はこの1年で世界6位から2位になった(トレンドマイクロ)
- GOMプレーヤーでアップデート用サーバーが悪用された

- 政府が7月10日に決定したサイバーセキュリティに関する年次報告によると、日本の政府機関を標的にした平成25年度のサイバー攻撃は約508万件に上り、約108万件だった前年度に比べ5倍に急増
- 政府の情報セキュリティセンター(NISC)に報告された25年度のサイバー攻撃は133件と、こちらも前年度の2倍

日本へのサイバー攻撃が急増している

企業経済圏に
おけるセキュリ
ティ課題

大企業
秘密情報

3. 踏み台から攻撃

信頼

信頼関係

信頼関係

踏み台

取引先

委託業者

セキュリティの弱点

2. 弱点の攻撃

(社外なので) セキュリティ強化
策などのコントロールができない
セキュリティ対策が弱い可能性

1. 公開情報の調査



セキュリティ・インシデントの成立要因

様々な脆弱性の存在

- ソフトウェアにおける脆弱性
- 人における脆弱性

特にソフトウェアの脆弱性に関する課題について

- 一見、正常に動作しているように見える
 - 攻撃手法を熟知したセキュリティの専門家が、疑似攻撃を行うテスト(脆弱性検査)を行わなければ発見が困難
- 機能を実現するだけで精一杯
 - 開発につかえるコスト(金銭的、時間的)が限られている
 - 安全なソフトウェアの開発には、よりレベルの高い開発者の関与が必要になる
 - 要求側の安全性よりコスト重視の姿勢

JPCERT/CC による注意喚起(2014年度)

		2014		
		公開日	注意喚起内容	テキスト (PGP署名付き)
2014-04-09	Adobe Flash Player の脆弱性 (APSB14-09) に関する注意喚起 (公開)			
2014-04-09	2014年3月 Microsoft Word の未修正の脆弱性に関する注意喚起 (更新)	2014-07-16	2014年7月 Oracle Java SE のクリティカルパッチアップデートに関する注意喚起 (公開)	4.19KB
2014-04-08	OpenSSL の脆弱性に関する注意喚起 (公開)	2014-07-09	Adobe Flash Player の脆弱性 (APSB14-17) に関する注意喚起 (公開)	4.03KB
2014-03-25	2014年3月 Microsoft Word の未修正の脆弱性に関する注意喚起 (公開)	2014-07-09	2014年7月 Microsoft セキュリティ情報(緊急 2件含) に関する注意喚起 (公開)	3.16KB
2014-03-12	2014年3月 Microsoft セキュリティ情報(緊急 2件含) に関する注意喚起 (公開)	2014-06-12	ISC BIND 9 サービス運用妨害の脆弱性 (CVE-2014-3859) に関する注意喚起 (公開)	3.44KB
2014-03-12	2014年2月 Microsoft Internet Explorer の未修正の脆弱性に関する注意喚起 (更新)	2014-06-11	Adobe Flash Player の脆弱性 (APSB14-16) に関する注意喚起 (公開)	3.84KB
2014-03-07	Apache Commons FileUpload および Apache Tomcat の脆弱性に関する注意喚起 (更新)	2014-06-11	2014年6月 Microsoft セキュリティ情報(緊急 2件含) に関する注意喚起 (公開)	3.17KB
2014-02-28	Apache Commons FileUpload および Apache Tomcat の脆弱性に関する注意喚起 (更新)	2014-05-15	旧バージョンの Movable Type の利用に関する注意喚起 (公開)	5.82KB
2014-02-21	Adobe Flash Player の脆弱性 (APSB14-07) に関する注意喚起 (公開)	2014-05-14	Adobe Reader および Acrobat の脆弱性 (APSB14-15) に関する注意喚起 (公開)	2.92KB
2014-02-20	Apache Commons FileUpload および Apache Tomcat の脆弱性に関する注意喚起 (更新)	2014-05-14	Adobe Flash Player の脆弱性 (APSB14-14) に関する注意喚起 (公開)	3.70KB
2014-02-20	2014年2月 Microsoft Internet Explorer の未修正の脆弱性に関する注意喚起 (公開)	2014-05-14	2014年5月 Microsoft セキュリティ情報(緊急 3件含) に関する注意喚起 (公開)	3.51KB
2014-02-12	2014年2月 Microsoft セキュリティ情報(緊急 4件含) に関する注意喚起 (公開)	2014-05-02	マイクロソフト セキュリティ情報(MS14-021)に関する注意喚起 (公開)	4.19KB
2014-02-10	Apache Commons FileUpload および Apache Tomcat の脆弱性に関する注意喚起 (公開)	2014-05-02	2014年4月 Microsoft Internet Explorer の未修正の脆弱性に関する注意喚起 (更新)	7.70KB
2014-02-05	Adobe Flash Player の脆弱性 (APSB14-04) に関する注意喚起 (公開)	2014-04-30	Adobe Flash Player の脆弱性 (APSB14-13) に関する注意喚起 (公開)	3.87KB
2014-01-15	2014年1月 Microsoft セキュリティ情報に関する注意喚起 (公開)	2014-04-28	2014年4月 Microsoft Internet Explorer の未修正の脆弱性に関する注意喚起 (公開)	
2014-01-15	Adobe Flash Player の脆弱性 (APSB14-02) に関する注意喚起 (公開)	2014-04-16	2014年4月 Oracle Java SE のクリティカルパッチアップデートに関する注意喚起 (公開)	4.19KB
2014-01-15	Adobe Reader 及び Acrobat の脆弱性 (APSB14-01) に関する注意喚起 (公開)	2014-04-15	DNS キャッシュポイズニング 攻撃に関する注意喚起 (公開)	4.66KB
2014-01-15	2014年1月 Oracle Java SE のクリティカルパッチアップデートに関する注意喚起 (公開)	2014-04-11	OpenSSL の脆弱性に関する注意喚起 (更新)	5.08KB
2014-01-15	ntpd の monlist 機能を使った DDoS 攻撃に関する注意喚起 (公開)	2014-04-09	2014年4月 Microsoft セキュリティ情報(緊急 2件含) に関する注意喚起 (公開)	3.71KB
		4.13KB		
		4.63KB		

事故前提社会であることを認識する

- **特定企業を狙った標的型攻撃**
 - 巧妙で執拗なソーシャルエンジニアリング手法
 - 容易な犯罪ツールの入手(技術はお金で買える)
 - さまざま手法を駆使、事前の発見が極めて困難
- **明確な目的(経済的利益)を持った犯罪行為**
 - 外部)国家を含む犯罪組織
 - 内部)不正行為
- **守る側では情報が不足**
 - 詳細な手法や仕組みの把握が遅れる
 - 日々進化、変化する攻撃手法
 - 守るべき箇所や課題が多すぎる
- **従来のセキュリティ対策技術では不十分**
 - モバイル環境、クラウド環境の普及などで防御する対象が急増
 - セキュリティ対策製品毎に防御可能な範囲が狭い
 - 先回りの防御が難しい
 - 人間系の脆弱性は防御が困難

セキュリティ・インシデントが発生する前提で、備えを怠らないことが重要

しかし、実際は・・・
実際に何が起こったのか説明できない
何がどれだけ漏洩したのか、明確に示せない

善管注意義務を怠った場合、
経営者責任として被害の範囲によっては社会問題化

新たなセキュリティ概念の形成

セキュリティ事件・事故
を100%防止することは**不可能**
セキュリティ事件・事故への
対応

- 原因の究明
- 被害の回復
- 責任の訴追

CIA+T

- 機密性
(Confidentiality)
- 完全性 (Integrity)
- 可用性 (Availability)
- **可遡及性**
(Traceability)

現実世界のアナロジー



ログ管理



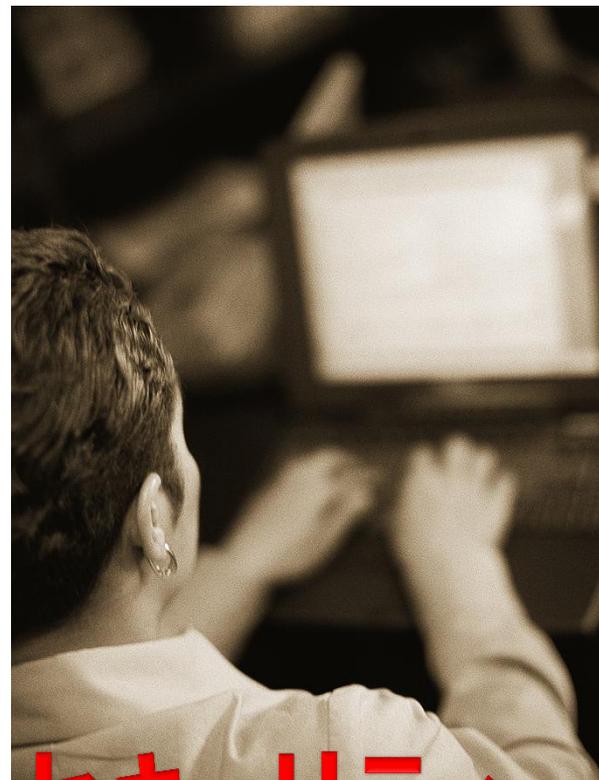
```
127.0.0.1 - - [20/Jun/2003:20:45:14 +0900] "GET / HTTP/1.1" 200 1835
127.0.0.1 - - [20/Jun/2003:20:45:14 +0900] "GET /apache_pb.gif HTTP/1.1" 200 2326
127.0.0.1 - - [20/Jun/2003:20:45:20 +0900] "GET /manual/index.html HTTP/1.1" 200 9904
127.0.0.1 - - [20/Jun/2003:20:45:14 +0900] "GET / HTTP/1.1"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

アクセスログ

オペレーション



ガードマン



セキュリティ オペレーション

**被害があった際
通過履歴(ログ)
+ 明確な証跡で
原因究明**

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



エックス線
手荷物検査

```
13
14 <script type="text/javascript" src="common/js/jquery.js"></script>
15 <script type="text/javascript" src="common/js/scroll.js"></script>
16 <script type="text/javascript" src="common/js/jquery.page-scroller.js"></script>
17 <script type="text/javascript" language="javascript" src="common/js/heightLine.
18 <!-- JASNET, INC. Web Analysis & Live Chat START -->
19 <script type="text/javascript">
20 //
21 function xlogAScript(){
22     HTTP_MSN_MEMBER_NAME="";/*member name*/
23     var
24     prt=(document.location.protocol=="https:")?"https://":"http://";
25     var hst=prt+"conf.log-marketing.jp";
26     var rnd="r"+(new Date().getTime()*Math.random()*9);
27     this.ch=function(){
28
29     if(document.getElementsByTagName("head")[0]){this.dls();}else[window.setTimeout(x
30     ]
31     this.dls=function(){
32         var h=document.getElementsByTagName("head")[0];
33         var
34         s=document.createElement("script");s.type="text/jav"+"ascript";try[s.async=true;]
35
36     if(h)[s.src=hst+"/UserConfig/t/Conf_totec062130.js?s="+rnd;h.appendChild(s);]
37
38     this.init= function(){
39         document.write('&lt;img src="'+hst+'/sr.gif?d'+rnd+' " style="width:
40     ]
41     }
42     if(typeof xlogAnalysis=="undefined"){ var xlogAnalysis=new
43     xlogAScript();xlogAnalysis.init();}
44     //]]&gt;
45 &lt;/script&gt;
46 &lt;noscript&gt;&lt;img src="
47 http://suite.log-marketing.jp/HTTP_MSN/Messenger/NoScript.php?key=totec062130
48 " border="0" style="display:none;width:0; height:0;" /&gt;
49 &lt;/noscript&gt;
50 &lt;!-- JASNET, INC. Web Analysis &amp; Live Chat END --&gt;
51 &lt;/head&gt;
52
53 &lt;body id="topPage"&gt;
54 &lt;div id="header"&gt;
55 &lt;div class="header01"&gt;
56 &lt;div class="logo"&gt; &lt;a href="http://www.netstor.jp/"&gt;&lt;img src="img/hl.gif" alt="
57 &lt;/a&gt;
58 &lt;/div&gt;</pre></div><div data-bbox="580 685 910 881" data-label="Text"><p>フォレンジック<br/>調査</p></div><div data-bbox="388 926 607 979" data-label="Page-Footer"><p>©All Rights Reserved TOTEC<br/>Amenity,Ltd. 2014</p></div><div data-bbox="750 922 890 983" data-label="Page-Footer"><img alt="TOTEC AMENITY LIMITED logo"/></div><div data-bbox="918 940 947 965" data-label="Page-Footer"><p>20</p></div>
```

NetRAPTOR

Unified Network Forensic Appliance

個人情報・機密情報の漏えい抑止や内部統制強化を実現する
高機能ネットワークフォレンジックサーバー「NetRAPTOR」

社内の通信データをすべて捕捉・検知
セキュリティ強化を次なるステージへ



NetRAPTORとは

インターネット出入り口の監視カメラ
パケットレコーダー

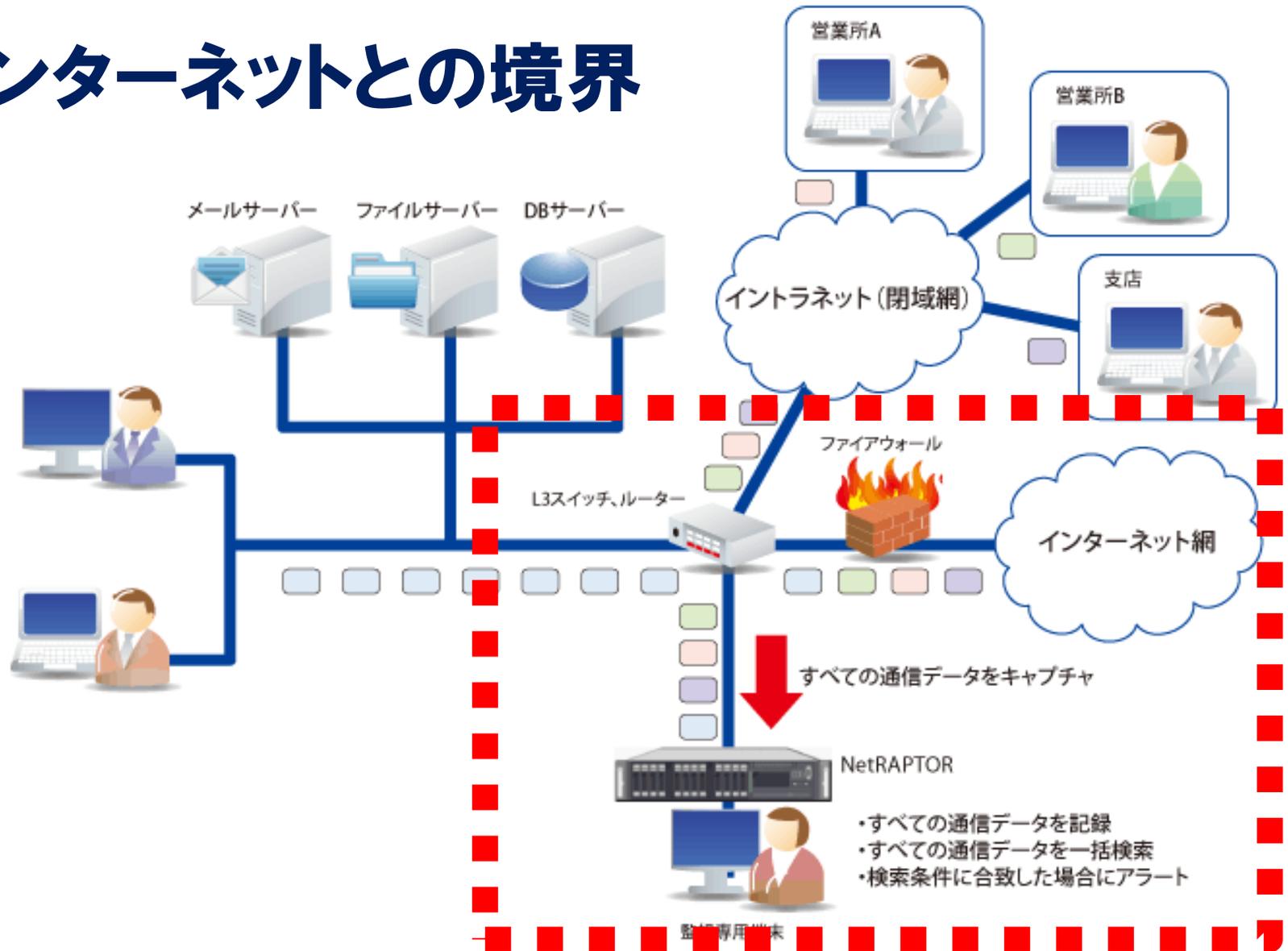


どこへ通信しているか
どんな内容の通信か
何が外部へ出て行っているか
・・・を把握し、分析する！

Webアクセス



インターネットとの境界



アプライアンス製品

- ・アプライアンス(IAサーバ)で提供されるインターネット通信の記録・見える化ネットワーク／端末環境に影響なし
- ・簡単に使えるセキュリティソリューション
→短期構築が可能



NetRAPTOR の機能

PCIDSS対応支援

記録する

保存する

NetRAPTOR

見つける

再現する



警告する

NetRAPTOR 記録する

取りこぼさない
Full キャプチャー

PCIDSS対応支援

通信パケットの
全記録

保存する

NetRAPTOR

見つける

再現する

警告する



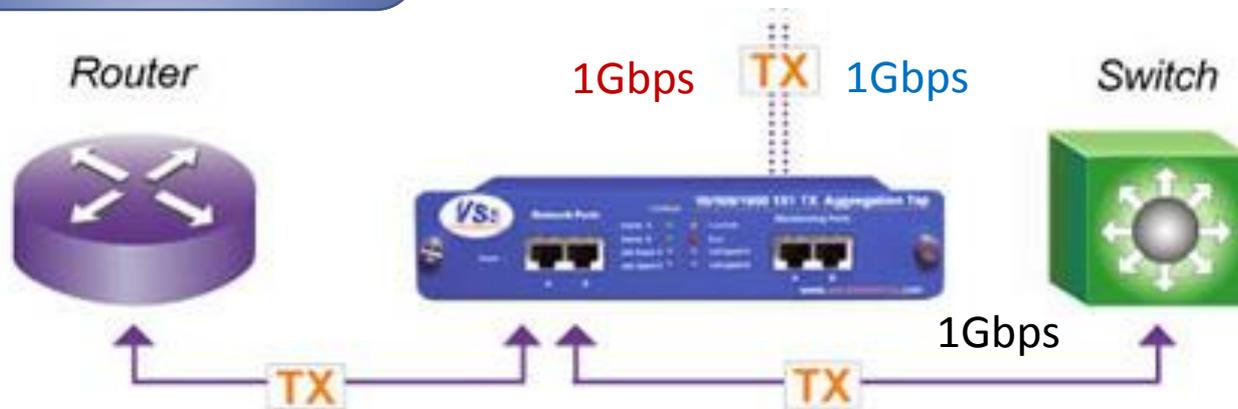
ロスゼロの PACKET キャプチャ

- ギガビット全二重(1Gbps x 2)で PACKET 取得

ベンダー標準NIC採用
独自の制御により
パケットロスゼロを実現



リアルタイム解析+
HDD保存の高速化



※10G対応製品もQ3に発表予定

NetRAPTOR 保存する

取りこぼさない
Full キャプチャー

PCIDSS対応支援

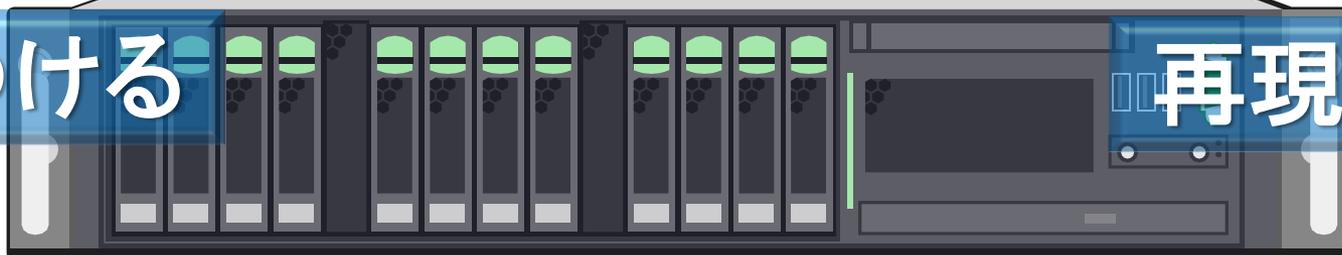
大容量ストレージ
に自動保存

通信パケットの
全記録

NetRAPTOR

長期間の
証拠保全

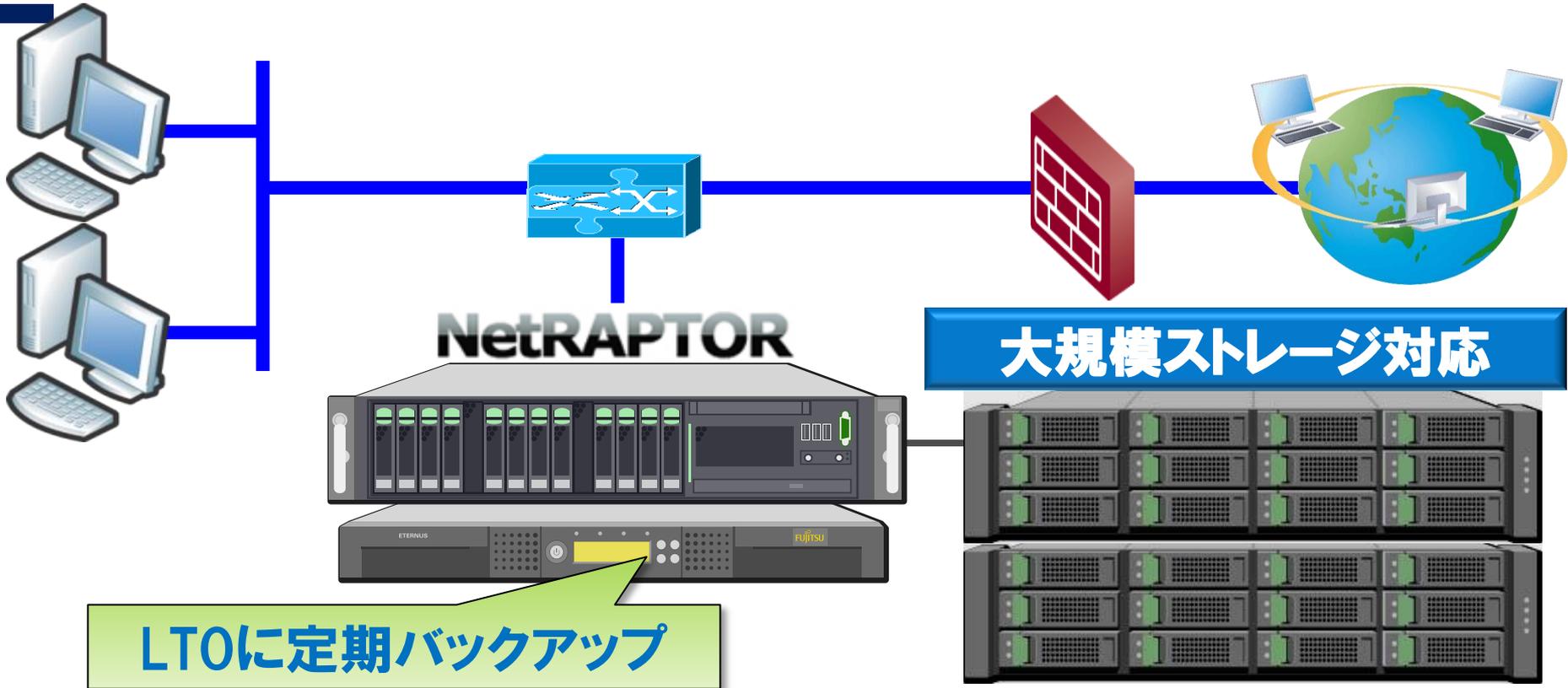
見つける



再現する

警告する

長期間の証拠保全が可能



運用例) 3ヶ月から1年間は即時、検索と再現・抽出可能
それ以上はテープ等で保存 (リストアして再現)

NetRAPTOR 見つける

取りこぼさない
Full キャプチャー

PCIDSS対応支援

大容量ストレージ
に自動保存

通信パケットの
全記録

NetRAPTOR

長期間の
証拠保全

高速で簡単な
全文検索

キーワード入力に
よる簡単検索！



再現する

警告する

高速で簡単な全文検索

NeTRAPTORは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

簡易検索条件 2007/02/06 ~ 2007/02/06

プロトコル	全て
データ内	
ヘッダー情報	
サーバIPアドレス (例: xxx.xxx.xxx.xxx)	
クライアントIPアドレス (例: xxx.xxx.xxx.xxx)	
クライアントMACアドレス (例: xx:xx:xx:xx:xx:xx)	
ホスト名/IPアドレス	
URL	
HTTP	全て
	全て
メール(SMTP, POP)	<input type="checkbox"/> あり
TO, CC, BCC	
コンテンツタイプ (例: plain, html, msword, zipなど)	

あり ※ファイルが添付されているものを検索対象とする場合にチェックしてください

高速
全文検索
エンジン

日付範囲

キーワード
IPアドレス
MACアドレス...etc

メール宛先
件名...etc

リアルタイムに検索

NetRAPTOR 再現する

取りこぼさない
Full キャプチャー

PCIDSS対応支援

大容量ストレージ
に自動保存

通信パケットの
全記録

NetRAPTOR

長期間の
証拠保全

高速で簡単な
全文検索

通信内容の
見える化

キーワード入力に
よる簡単検索！

メールやWebを
そのまま再現

警告する

通信内容の見える化

49320857639870477700703284210374

6647650846400159720037201927

984756862537475998

749506068948394767

938476211039485969

295746280

984756862537475998

749506068948394767

938476211039485969

295746280082611463

パケットデータ

HTMLソース

ブラウザで確認

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

見たまま、送ったままと再現

通信内容そのままを再現、電子メールや添付ファイル、
掲示板への書き込みなどが手に取るようになります

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@enico.jp
宛先: 山田 太郎<raptor@enico.jp>
cc: Ken Anno<kanno@enico.jp>

メールのヘッダ情報

調査結果です。
また連絡します。
-----kadoo@enico.jp Thanks a lot★

メールデータ検索結果

メール本文

会社概要.txt

セッション情報

簡易表示 | 詳細表示 | ソース

ホスト名: www.enico.jp
URL: /netraptor/network_forensic.html
メソッド: GET
ステータス: 200

アクセス情報

Webデータ検索結果

通信内容:
2007_08_10/http/192.168.3.158/11/11_12_42_011/1.html

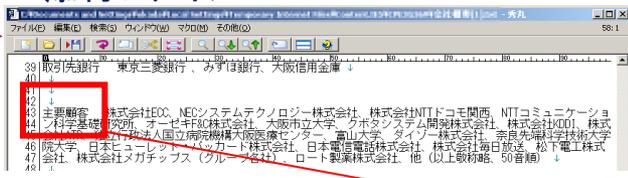
Click!

NetRAPTOR
Unifide Network Forensic Appliance



Click!

添付ファイル



NetRAPTOR
Unifide Network Forensic Appliance

圧力的な実用性能。
過剰な検出のネットワーク探知率100%、
高速全文検索エンジン標準搭載！

電子データに対する情報セキュリティの重要性が高まっています。個人情報や機密情報の漏洩といった問題は、従来のセキュリティ対策だけでは完全に防ぐことができません。

※はめ込み画像です

それぞれ「データ内:主要顧客」「データ内:個人情報」で検索した結果

※css、Ajaxなどの再現性は不完全な場合があります

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せん。

The screenshot displays an email client interface with a list of emails on the left and a detailed view of an email on the right. The email being viewed is from 'okada@eni.co.jp' to 'raptorde mo@eni.co.jp' with the subject '顧客情報401.zip'. The attachment is a zip file named '顧客情報401.zip' with a MIME type of 'application/x-zip-compressed'. A yellow callout box highlights the file type icons: XLS, DOC, JPG, TXT, PDF, ZIP, and Web.

件名(メール)	FROM	TO,CC,BCC	内容種別	受信日時
Merry Christmas★	okada@eni.co.jp	raptorde mo@eni.co.jp, anno@eni.co.jp	text/plain; charset=ISO-2022-JP	2010/09/02 10:44:58.583
顧客情報401.zip			application/x-zip-compressed; name=顧客情報401.zip	
ご覧下さい	okada@eni.co.jp	raptorde mo@eni.co.jp		10:44:55.972
ごちそうさまでした	okada@eni.co.jp	raptorde mo@eni.co.jp	text/plain; charset=ISO-2022-JP	2010/09/02 10:44:55.972

NetRAPTOR 警告する

取りこぼさない
Full キャプチャー

PCIDSS対応支援

大容量ストレージ
に自動保存

通信パケットの
全記録

NetRAPTOR

長期間の
証拠保全

高速で簡単な
全文検索

キーワード入力に
よる簡単検索！

問題行動の
監視と警告

リアルタイムに
メールで通知

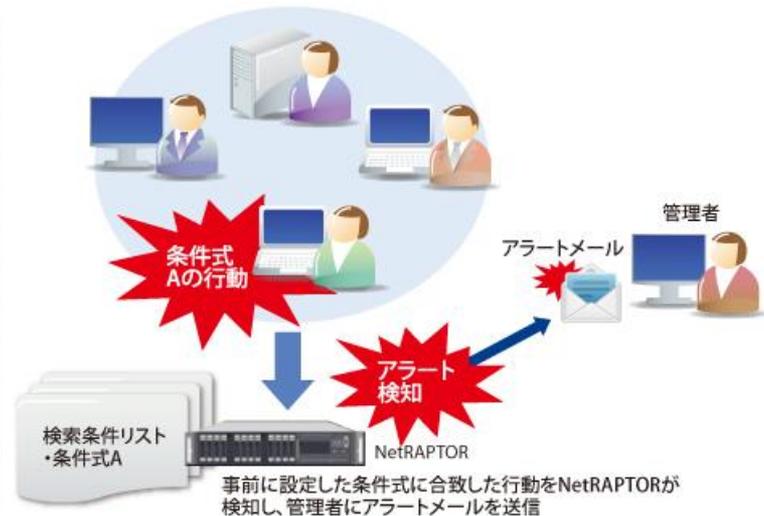
通信内容の
見える化

メールやWebを
そのまま再現

問題行動の監視と警告

アラート条件	登録者	名前	コメント	対象アナライザ
警告	初期管理者	1-1 Yahooメール(添付ファイル付)		全アナライザ
注意	初期管理者	1-2 2chへのアクセス	2006/5/1より実施	全アナライザ
なし	初期管理者	1-3 HTTPS通信		全アナライザ
注意	初期管理者	2chへの投稿	保留	全アナライザ
警告	初期管理者	FTP通信		全アナライザ
なし	初期管理者	Googleへのアクセス		全アナライザ
警告	初期管理者	webへのpost		全アナライザ
警告	初期管理者	yahoo MSN	YAHOO MSN WEBメール	全アナライザ
なし	初期管理者	yahoo text		全アナライザ
なし	初期管理者	yahoo access	yahoo access	全アナライザ

名前	1-1 Yahooメール(添付ファイル付)
検索条件	protocol:http AND host:mail.yahoo.co.jp AND status:200 AND att...
コメント	
アラート条件	警告
対象アナライザ	全アナライザ
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**

条件アラート例

- 特定のWebサイトに集中的にアクセスしている
- 夜間や土日にメールを定期的送信している

条件式記述例

日本以外のサイトにファイルアップロードを行った
(protocol:http) AND NOT (host:".jp") AND (method:POST) AND (attach:true)

**業務・職務内容に合わせ、
端末IP単位で細かく監視！
弊社だけの機能！**

リアルタイム解析

インターネット通信データの取得【フルキャプチャ】

通信データを解析、通信内容を【組立て直し・再構成】

再現データを全文検索エンジン用【インデックス化】

指定キーワードや条件設定で【アラート通知】

メール／Web／添付ファイルの【検索】 【再現】

リアルタイム処理

検索イメージ(1)

”大容量データ”というキーワードでファイル送信したWebアクセスを検索、該当するアクセスを発見

The screenshot shows the NetRAPTOR web interface. The search criteria are: 2010/09/02 to 2013/11/28, Protocol: WEB(HTTPのみ), Data: 大容量データ. The search results table shows three entries for HTTP requests to jp.f9.mail.yahoo.co.jp with content type application/vnd.ms-excel.

クライアントIPアドレス	クライアントMAC	プロトコル	クライアント	ホスト(WEB) 件名(メール)	URL(WEB)	メソッド	ステータス	クエリー	コンテンツタイプ	添付	日時	
		http	192.168.3.146	jp.f9.mail.yahoo.co.jp	/ym/Attachments	POST	200	○	application/vnd.ms-excel	○	2010/09/02 10:44:54.853	詳細
		http	192.168.3.146	jp.f9.mail.yahoo.co.jp	/ym/Attachments	POST	200	○	application/vnd.ms-excel	○	2010/09/02 10:44:54.203	詳細
		http	192.168.3.146	jp.f9.mail.yahoo.co.jp	/ym/Attachments	POST	200	○	application/vnd.ms-excel	○	2010/09/02 10:44:53.148	詳細

検索結果イメージ(1)

検索結果の内容(postしたhtmlと送信したExcelファイル)を再現

The screenshot shows the NetRAPTOR interface with search results and a file upload dialog. The search results table is as follows:

検索結果	送信したExcelファイル	postしたhtml
大容量データ送信	410,000	
1 @Tovas	http://www.attovas.com/	手軽なファイル送信ASP http://www.pic-up.net/mvpageASP/
2 宅ファイル便	http://www.filesend.to/	宅ふあいる便 大容量ファイル受け渡しサービス http://www.filesend.to/
3 株式会社ドライブデータ:大容量データ送信ソリューション	http://www.news2u.net/NRR20055786.html	大容量データ送信サイトの投票ランキング cat.ip.siterank.org/ip/cat/1100100300/
4 メモ「大容量データ送	1470.net/mm/relate	So-net blogdrop cafe:大容量データ送信 blog.so-net.ne.jp/drop_cafe/2005-01-29-2
5 アゲルね.jp		

The file upload dialog shows the following details:

- 添付済みファイル: **キーワード調査.xls** (2171k) [削除]
- 添付ファイルを選択してください (追加)
- ファイル 2: 参照...
- ファイル 3: 参照...
- ファイル 4: 参照...
- ファイル 5: 参照...
- ボタン: ファイルを添付

Red arrows in the original image point from the search results to the file upload dialog, indicating the flow of information.

検索イメージ(2)

NGFWによってポリシー違反に相当するサーバへのアクセスを検知、サーバのIPアドレスが判明

判明したIPアドレスの通信を検索

ファイル送信のある通信を特定

The screenshot shows the NetRAPTOR search interface. The search criteria are set to 'WEB(HTTPのみ)' and the date range is from 2010/09/02 to 2013/11/28. The server IP address is 65.52.103.234. The search results table is as follows:

URL	プロトコル	クライアント	ホスト(WEB) 件名(メール)	URL(WEB)	メソッド	ステータス	クエリー	コンテンツタイプ	添付	日時	
HTTP	http	192.168.0.2	windows.microsoft.com	/WoIAuthenticationHandler.ashx	POST	200		application/octet-stream	<input type="radio"/>	2013/11/28 17:39:40.814	詳細
	http	192.168.0.2	windows.microsoft.com	/en-us/skydrive/download	GET	200	○	text/html; charset=utf-8	<input type="radio"/>	2013/11/28 17:39:40.814	詳細
	http	192.168.0.2	windows.microsoft.com	/WoIAuthenticationHandler.ashx	POST	200		application/octet-stream	<input type="radio"/>	2013/11/28 17:36:32.118	詳細
	http	192.168.0.2	windows.microsoft.com	/WoIAuthenticationHandler.ashx	POST	200		application/octet-stream	<input type="radio"/>	2013/11/28 17:35:50.141	詳細
	http	192.168.0.2	windows.microsoft.com	/ja-jp/skydrive/download	GET	200		text/html; charset=utf-8	<input type="radio"/>	2013/11/28 17:35:50.141	詳細
	http	192.168.0.2	windows.microsoft.com	/scripts/4.2/wol/ClientBI/Settings.Wol.js	GET	200	○	text/javascript	<input type="radio"/>	2013/11/28 17:35:50.140	詳細
	http	192.168.0.2	windows.microsoft.com	/scripts/4.2/wol/wol.com	GET	200		text/javascript	<input type="radio"/>	2013/11/28 17:35:50.140	詳細

検索結果イメージ(2)

判明した通信(html)を再現

送信されたファイルを特定し、内容を確認



NetRAPTOR

セッション情報

簡易表示 | 詳細表示 | ソース

ホスト名 : windows.microsoft.com
URL : /ja-jp/skydrive/download
メソッド : GET
ステータス : 200

通信内容:
2013_11_28/http/192.168.0.2/17_36/37_107_1/2.html

http ホスト名 : windows.microsoft.com
URL : /WolAuthenticationHandler.ashx
http メソッド : POST
http ステータス : 200
http アップロード
file
2013_11_28/http/192.168.0.2/17_36/37_107_1/request-c15495ca-bd77-496d-9bd8-edf3bd2ec3ff.bin

通信内容:
2013_11_28/http/192.168.0.2/17_36/37_107_1/3.bin

```
{"authenticationEnabled":true,"silentAuthDisabled":false,"displayName":"大輔 佐藤","firstName":"大輔","authenticated":true,"isWLDogfoodUser":false}
```

検索イメージ(3)

NetRAPTOR

データ: Live

検索 | レポート | 統計 | 閲覧ログ | ダンプデータ | 設定 | ユーザ管理 | パスワード変更 | ログアウト

レポート(指定した期間のアラートの発生状況を確認することができます)

レポート対象

日付: 2010/09/02 ~ 2013/11/28

日別集計 | 項目別集計

日付	全件	注意	警告
2013/11/27	3523	123	7
12/02	147	123	23

レポート(条件式リストによる警告通知一覧)の確認

該当日時の警告の一覧を確認

アラート内容 表示項目切り替え: 簡易表示

名前	プロトコル	クライアント	ホスト(WEB) 件名(メール)	URL(WEB)	メソッド FROM	ステータス TO,CC,BCC	クエリー	コンテンツタイプ	送信日時	詳細
2ちゃんねるへの投稿	http	192.168.0.2	qb5.2ch.net	/test/bbs.cgi	POST	200	○	text/html; charset=shift_jis	2013/11/27 18:36:36.341	詳細
2ちゃんねるへの投稿	http	192.168.0.2	qb5.2ch.net	/test/bbs.cgi	POST	200	○	text/html; charset=shift_jis	2013/11/27 18:33:08.361	詳細
2ちゃんねるへの投稿	http	192.168.0.2	qb5.2ch.net	/test/bbs.cgi	POST	200	○	text/html; charset=shift_jis	2013/11/27 18:32:32.826	詳細
2ちゃんねるへの投稿	http	192.168.0.2	qb5.2ch.net	/test/bbs.cgi	POST	200	○	text/html; charset=shift_jis	2013/11/27 18:31:49.175	詳細
2ちゃんねるへの投稿	http	192.168.0.2	qb5.2ch.net	/test/bbs.cgi	POST	200	○	text/html; charset=shift_jis	2013/11/27 18:31:49.175	詳細
社外秘の情報を含	pop	192.168.0.3	企画連							
		192.168.0.3	企画連							

警告の具体的な条件式

検索条件登録

名前	検索条件
2chへの投稿	protocol:http AND host:2chx AND method:POST
コメント	保留
アラート条件	注意
対象アナライザ	全アナライザ
メール送信先	初期管理者

検索結果イメージ(3)

警告対象のWebアクセスを確認

NetRAPTOR セッション情報

簡易表示 | 詳細表示 | ソース

サーバ

アドレス	ポート	MAC アドレス
207.29.225.225	80	00:1b:8b:bc:ec:7f

クライアント

アドレス	ポート	MAC アドレス
192.168.0.2	2692	00:24:21:86:b5:19

リクエスト内容

名前: 書きこみ & クッキー確認

E-mail: 名前:

内容: E-mail:

ステータス: 200

メソッド: POST

URL: /test/bbs.cgi

ホスト名: qb5.2ch.net

リクエスト内容

name	value
cookie	READJS="off"; NAME
cache-control	no-cache
content-type	application/x-www-fo

レスポンス内容

name	value
content-type	text/html; ch
connection	close
set-cookie	PON=p8226=
content-length	1164
server	Apache/2.2.10 (Unix) PHP/5.2.5 mod_ssl/2.2.10 OpenSSL/0.9.8e
content-encoding	gzip
date	Wed, 27 Nov 2013 09:27:57 GMT
vary	Accept-En

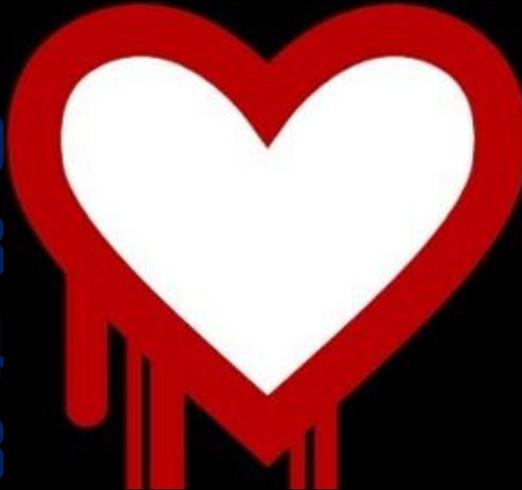
通信内容:
2013_11_27/http://192.168.0.2/18_31/42_469_1/1.html

投稿確認

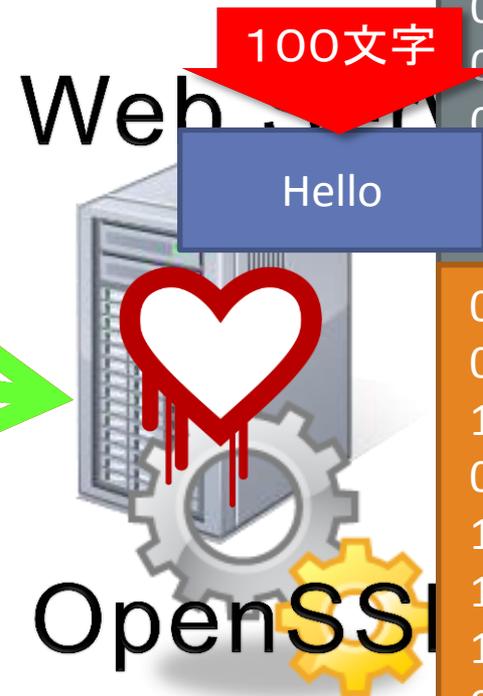
- 投稿者は、投稿に関して発生する責任が全て投稿者に帰すことを承諾します。
- 投稿者は、話題と無関係な広告の投稿に関して、相応の費用を支払うことを承諾します。
- 投稿者は、投稿された内容及びこれに含まれる知的財産権、(著作権法第21条ないし第28条に規定される権利も含む)その他の権利につき(第三者に対して再許諾する権利を含みます。)、掲示板運営者に対し、無償で譲渡することを承諾します。ただし、投稿が別に定める削除ガイドラインに該当する場合、投稿に関する知的財産権その他の権利、義務は一定期間投稿者に留保されます。
- 掲示板運営者は、投稿者に対して日本国内外において無償で非独占的に複製、公衆送信、頒布及び翻訳する権利を投稿者に許諾します。また、投稿者は掲示板運営者が指定する第三者に対して、一切の権利(第三者に対して再許諾する権利を含みます)を許諾しないことを承諾します。
- 投稿者は、掲示板運営者あるいはその指定する者に対して、著作者人格権を一切行使しないことを承諾します。

OpenSSL Heart Bleed Bug

0937879423984923572572904932852
9489238928528023402358**PASSWORD**2
52752374821)5710321084
95804239859)4835439085
17863715658)2857493071
67855481604)1981856437
01003922388)9786666666
60061**PRIVATEKEY**01647658237748399
3100610540366167403574890068235

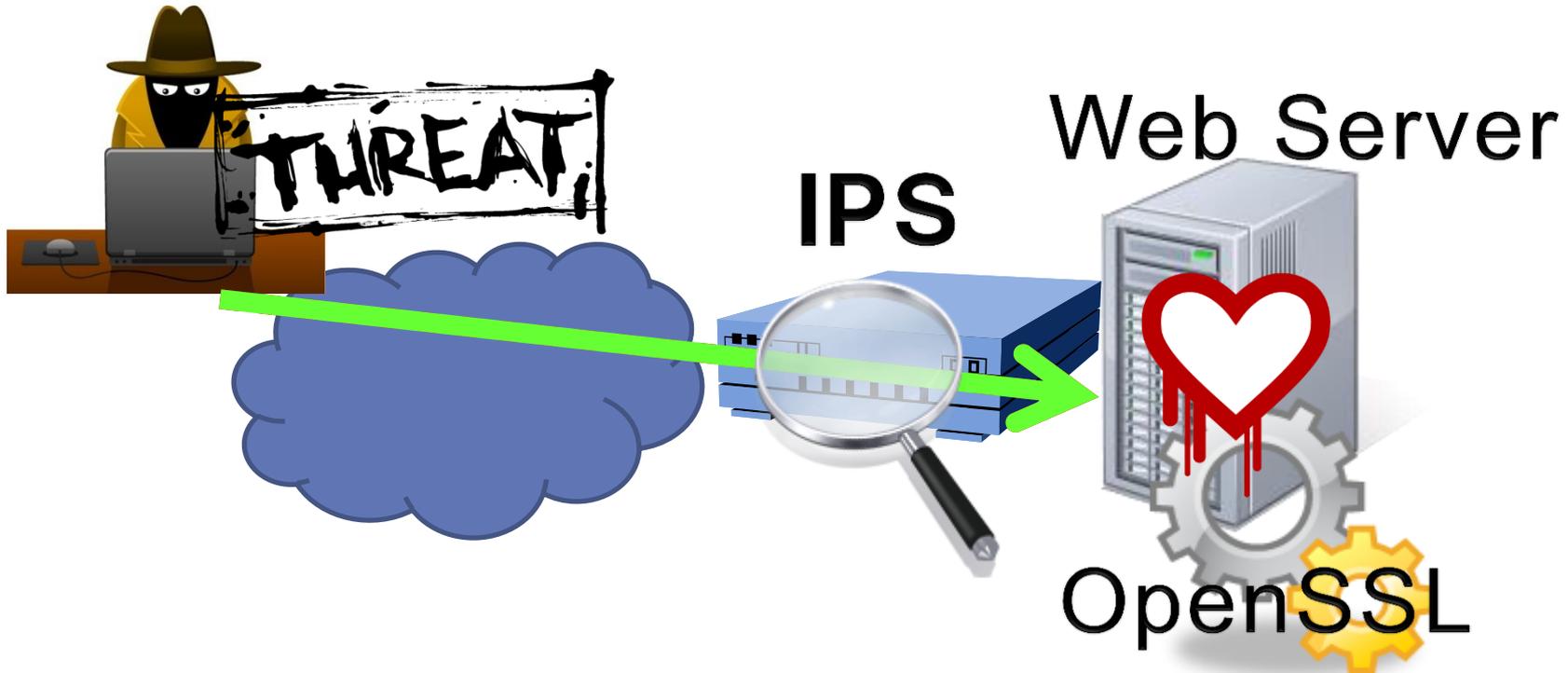


Heartbleed bug

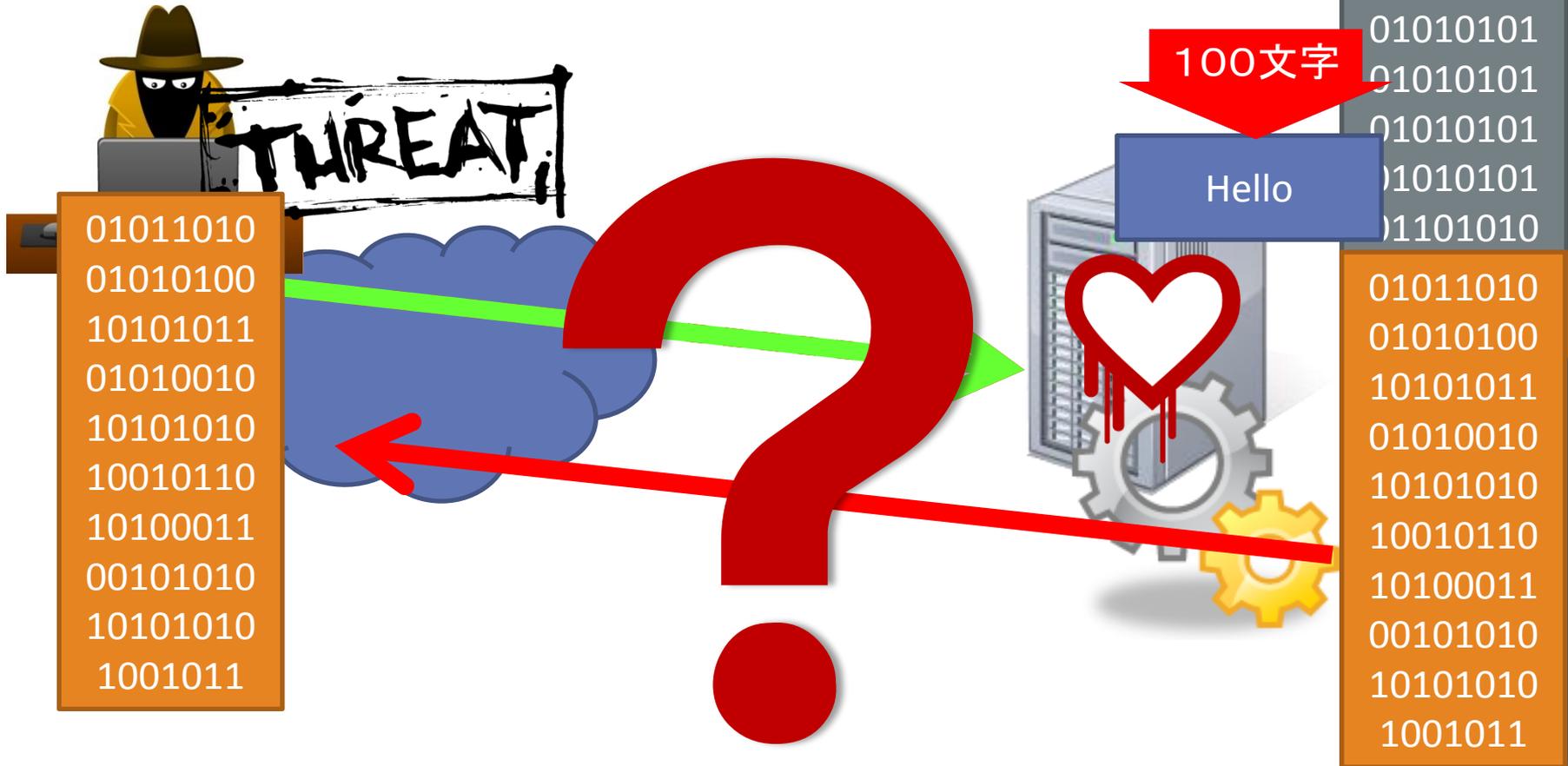


メモリ
01010100
10101001
01010101
01010101
01010101
01010101
01010101
01010101
01010101
01101010
01011010
01010100
10101011
01010010
10101010
10010110
10100011
00101010
10101010
1001011

IPS で検知可能



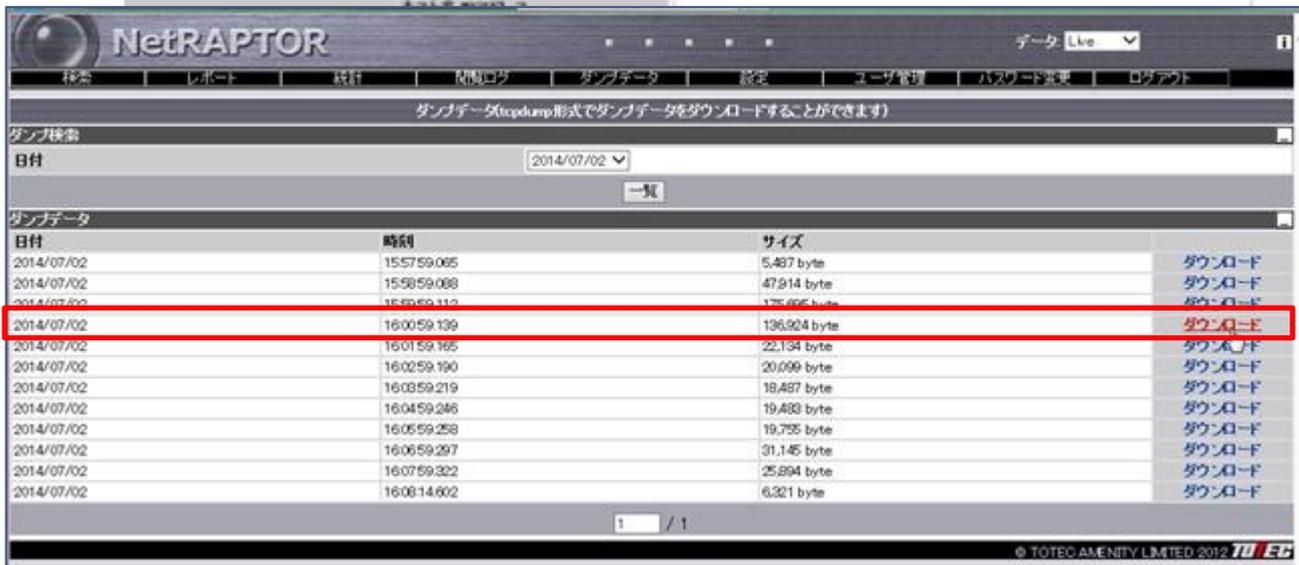
盗まれたメモリの情報は？



盗まれたメモリの情報は？



Heartbleed bug を検証する



Wiresharkを使ってパケットを再現

The screenshot displays the Wireshark interface with a capture file named '2014_07_02_16_00_59_139.dump'. The main packet list pane shows a series of network packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. A filter 'tcp.port==443' is applied. The packet details pane for the selected packet (No. 161) shows the following structure:

- Ethernet II, Src: Realtek... (00:e0:4c:ab:09:4a), Dst: ...
- Internet Protocol Version 4, Src: 192.168.68.211 (192.168.68.211), Dst: 192.168.68.113
- User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
- TCP, Seq=0, Win=146, Len=0, Flags=ACK, Window=146
- Application/javascript

The packet bytes pane shows the raw data in hexadecimal and ASCII format. A context menu is open over the packet details pane, listing various actions such as 'Mark Packet (toggle)', 'Ignore Packet (toggle)', 'Set Time Reference (toggle)', 'Time Shift...', 'Packet Comment...', 'Manually Resolve Address', 'Apply as Filter', 'Prepare a Filter', 'Conversation Filter', 'Colorize Conversation', 'SCTP', 'Follow TCP Stream', 'Follow UDP Stream', 'Follow SSL Stream', 'Copy', 'Protocol Preferences', and 'Decode As...'. The status bar at the bottom indicates 'File: D:\Works\Solutions\heartblee... Packets: 369 · Displayed: 369 (100.0%) · Load time: ...'.

Basic認証のパスワード漏洩をキャプチャー

Follow TCP Stream

Stream Content

```
..*.H..  
.....0.....c[...D;*..p.B].....='.....6tR.b...2z.e.....  
..v'(C...y.'...{...}]K.v.....c.g.G.b...~'Li..  
+..x?.V.7...RSV..X.<.#.I...v...T.O.....PON0...U...../..U.#..  
..l..e...&00...U.#..0.../..U.#..  
..l..e...&00...U...0...0  
..*.H..  
| " f &KB8al 02 } d = C > x
```

//snip

```
.....#.....t: 192.168.68.213  
If-Modified-Since: Wed, 02 Jul 2014 06:34:13 GMT  
If-None-Match: "1f9f8-f-4fd30149fd55d"  
Connection: Keep-Alive  
Authorization: Basic YWRtaW5pc3RyYXRvcjpwYXNzd2QwMTIz  
...e.@%....ug`)..=..+..r+?.
```

Trying SSL 3.0...Connecting...Sending Client Hello...Waiting for Server Hello... .. received message: type = 22, ver = 0300, length = 86 ... received message: type = 22, ver = 0300, length = 845 ... received message: type = 22, ver = 0300, length = 397 ... received message: type = 22, ver = 0300, length = 4Sending heartbeat request... .. received message: type = 24, ver = 0300, length = 16384Received heartbeat response: 0000: 02 40 00 D8 03 00 53 43 5B 90 9D 9B 72 0B BC 0C .@....SC[...r...

```
00d0: 10 00 11 00 23 00 00 0F 00 01  
01 74 3A 20 31 .....#.....t: 1  
00e0: 39 32 2E 3T 36 38 2E 36 38 2E 32  
31 33 0D 0A 48 92.168.68.213..C  
00f0: 6F 6E 6E 65 63 74 69 6F 6E 3A 20  
4B 65 65 70 2D ..connection: Keep-  
0100: 41 6C 69 76 65 0D 0A 41 75 74 68  
6F 72 69 7A 6E ..Alive..Authoriza  
0110: 74 69 6F 6E 3A 20 42 61 73 69 63  
20 59 57 52 74 ..tion: Basic YWRt  
0120: 61 57 35 70 63 33 52 79 59 58 52  
76 63 6A 70 77 ..aW5pc3RyYXRvcjpw  
0130: 59 58 4E 7A 64 32 51 77 4D 54 49  
7A 0D 0A 0D 0A ..YXNzd2QwMTIz....
```

YWRtaW5pc3RyYXRvcjpwYXNzd2QwMTIz

↓ BASE64をdecode

administrator:passwd0123

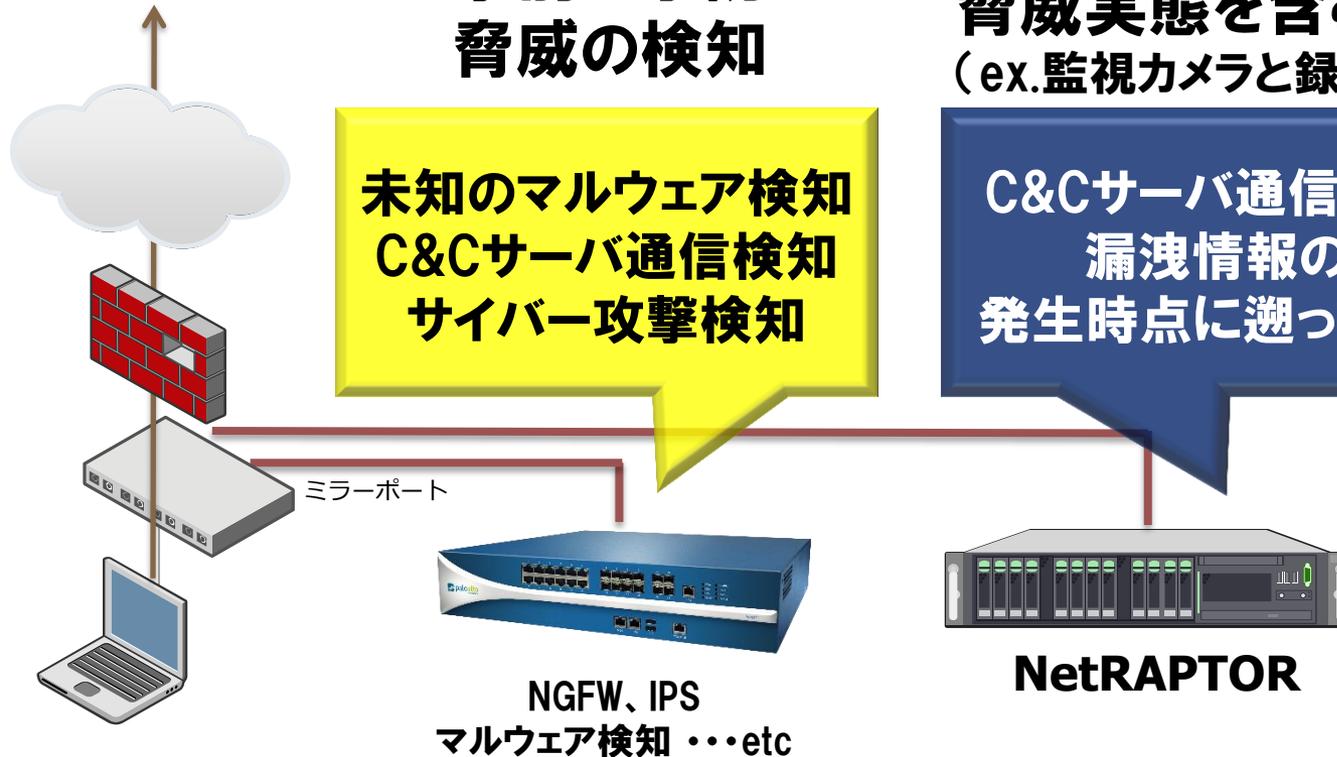
検知だけではわからない脅威情報を記録

事前の予防 脅威の検知

未知のマルウェア検知
C&Cサーバ通信検知
サイバー攻撃検知

事案発生時の調査 脅威実態を含む全記録 (ex.監視カメラと録画)

C&Cサーバ通信内容記録、
漏洩情報の記録、
発生時点に遡って実態調査



アクセスログがあればパケットはいらない？

- 例えばサーバログは有効な情報・・・だが
 - ファイルに記載されていた内容は分からない
 - ファイルは書き換えられている可能性もある
 - 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

ログ収集：パケット収集：監視

ログ収集

膨大なログ情報を可視化したり要約することで根本原因を追究する
フォレンジックの観点では非オリジナルデータ

パケット収集

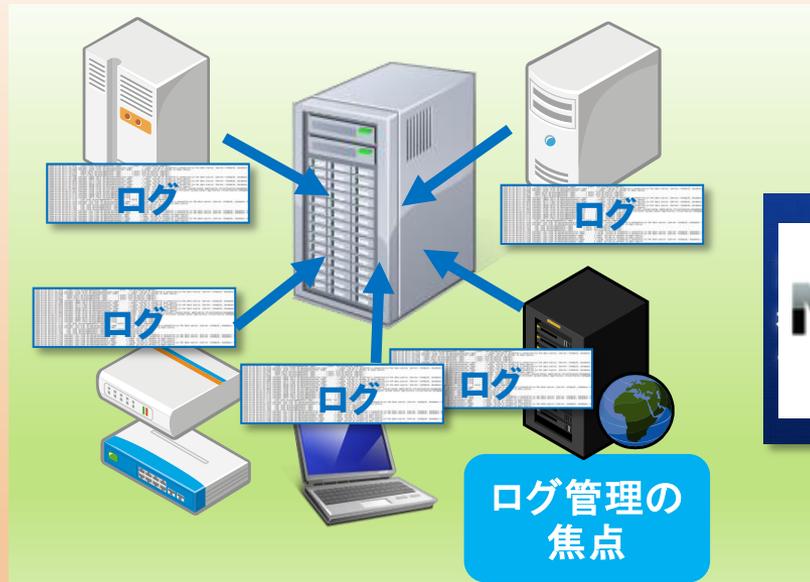
オリジナル性を持ったデータを元のままの形で保存する
加工された形ではないため、オリジナルデータとしての証拠性

ネットワーク監視

セキュリティに特化した監視・通知を行う
検知・通知だけでもっとも有効な手段だが、証拠を保存しない

ログ監査製品とネットワークフォレンジック

サイバー空間と組織の融合／サイバーセキュリティ対策



組織内の監査／SOX対応

ネットワークフォレンジックス
サイバー攻撃によるインシデント解析

NetRAPTOR
Unified Network Forensic Appliance



メールアーカイブ
メール監査／標的型攻撃メール証跡

ログ管理とネットワークフォレンジック

NetRAPTOR

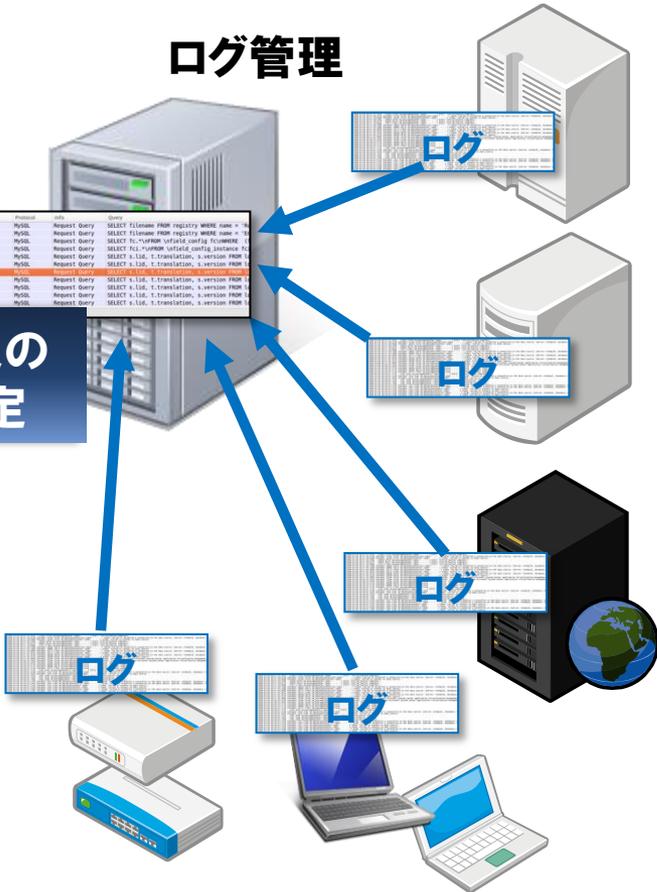
特定のログから実際の
アクセス記録を取り出す



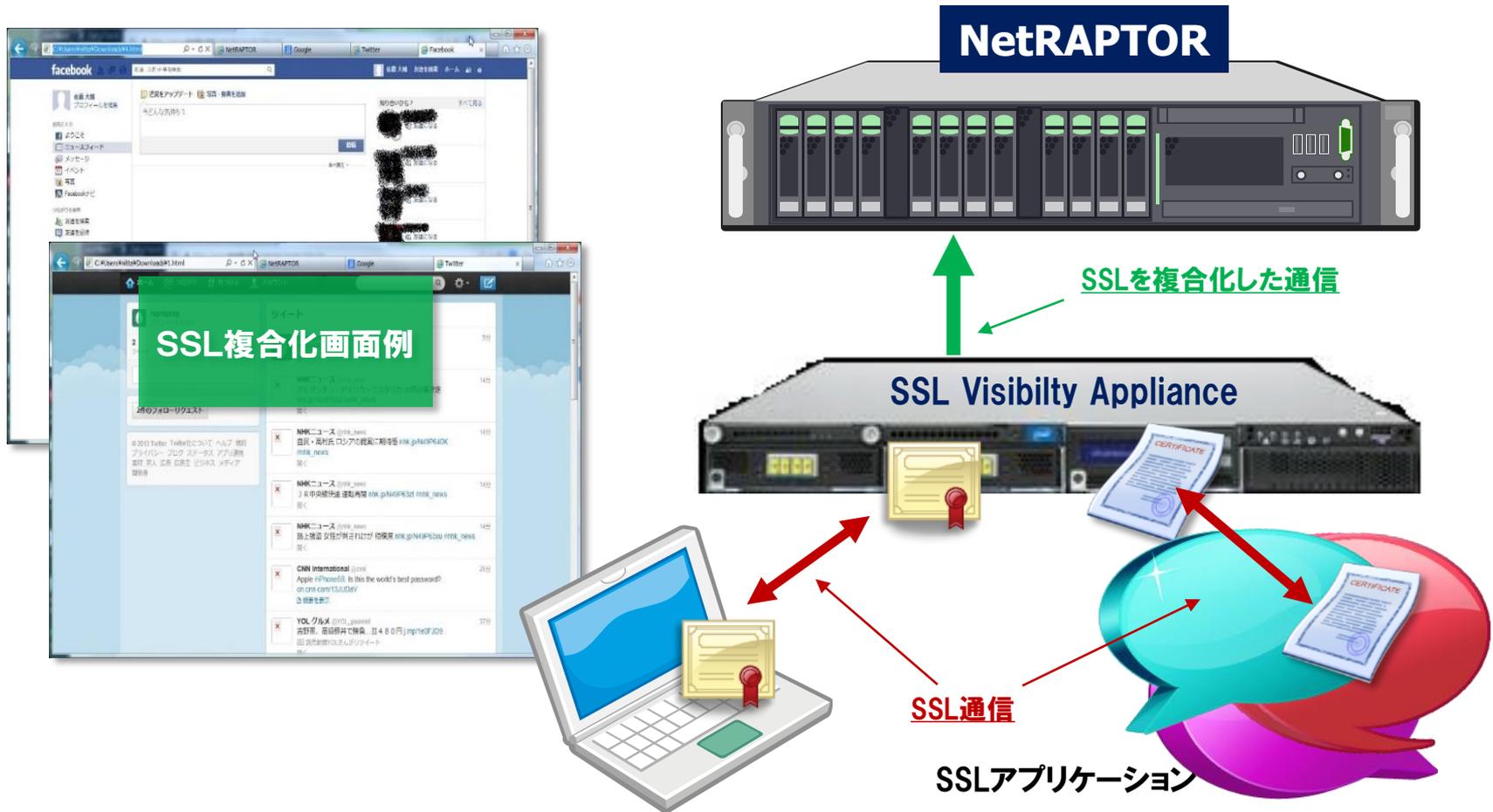
種別	レポート	実行	監視ログ	タスクデータ	設定	ユーザ管理	パスワード変更	ログアラート
検索結果の件数 表示欄 日時 表示項目切り替え 検索条件								
IPアドレス	クライアント	ホスト名(ED)	URL(ED)	メソッド	ポート	ステータス	エラー	コメント
http	192.168.0.146	q65.schu.net	/test/abc.caf	POST	200			text/html
http	192.168.0.146	q65.schu.net	/operate/	GET	200			text/html
http	192.168.0.146	q65.schu.net	/operate/	POST	200			text/html
http	192.168.0.146	q65.schu.net	/operate/	GET	200			text/html
http	192.168.0.146	q65.schu.net	/test/abc.caf	POST	200			text/html
http	192.168.0.146	q65.schu.net	/operate/	GET	200			text/html
http	192.168.0.146	my.vector.co.jp	/fs/usb/4/abc.css	GET	200			text/css
http	192.168.0.146	my.vector.co.jp	/fs/usb/html	GET	200			text/html
http	192.168.0.146	vector.co.jp	/advertisement/images/90006296/0/515a2a5c_vector.js.swf	GET	200			text/html
http	192.168.0.146	vector.co.jp	/download/file/vb-95/personal/1680275.html	GET	200			text/html
http	192.168.0.146	vector.co.jp	/ssi-bin/rgb-overture	GET	200			text/html
http	192.168.0.146	vector.co.jp	/advertisement/images/90006296/0/522e3c7c_288000_bates.swf	GET	200			text/html
http	192.168.0.146	vector.co.jp	/fs/usb/vb95/personal/ee096017.html	GET	200			text/html
http	192.168.0.146	vector.co.jp	/fs/usb/vb95/personal/ee096017.html	GET	200			text/html
http	192.168.0.146	vector.co.jp	/ssi-bin/rgb-overture	GET	200			text/html
http	192.168.0.146	vector.co.jp	/ssi-bin/rgb-overture	GET	200			text/html
http	192.168.0.146	vector.co.jp	/fs/usb/vb95/personal/ee096017.html	GET	200			text/html

調査対象の
ログを特定

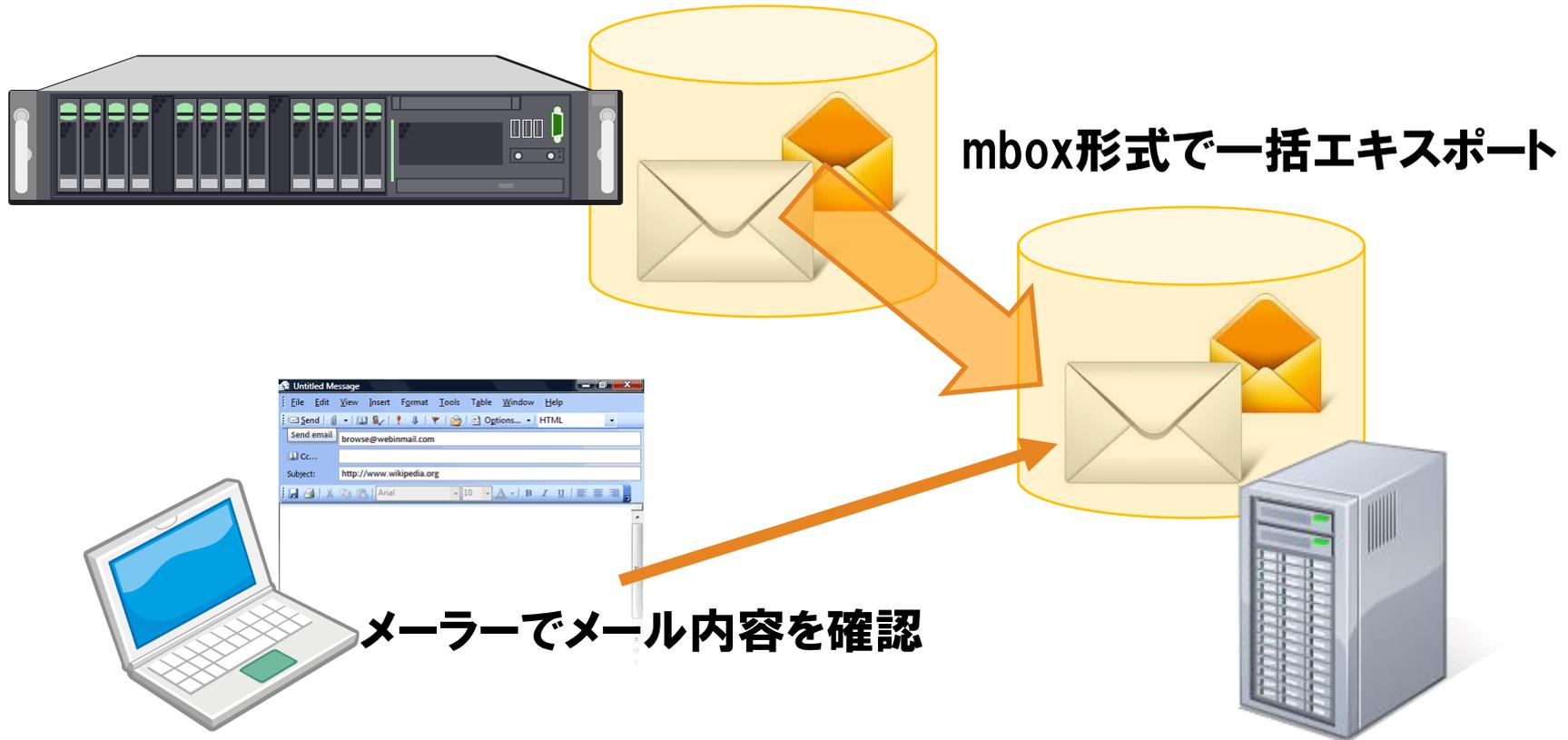
ログ管理



SSL通信の解析・再現



mbox形式一括エクスポート



導入事例

・事例)某省庁 様

導入背景

WebサイトでNetRAPTORを見つけ、商品指定入札

選定ポイント

キャプチャ性能と検索性能で選定。既設ネットワークへの影響なしが決め手

運用と評価

海外のニュースサイトを閲覧し、時系列を持って記録

その他

通信パケット解析用データ取得にも利用

★その他バンダイビジュアル様他、約40社・団体で導入

導入事例

・ 事例) タカラスタンダード株式会社 様

導入背景

利便性を維持しながらセキュリティ強化を目指した新たなIT基盤を模索

選定ポイント

抑止効果の高い監視インフラの構築へ！負荷をかけない迅速な導入が魅力

運用と評価

70GBの検索がわずか5秒！業務負荷を軽減しながら抑止力を最大限発揮

今後の展望

業務効率化に繋がる攻めのネットワークフォレンジック活用に期待

・ 事例) JAあいち 様

導入背景

経営層含めて管理の課題や情報漏洩のリスクについて、危機感を感じていた

選定ポイント

「メール監視」「添付ファイルを含む全文保存」「保存情報の高速検索」

運用と評価

導入直後の4月に23件あったフリーメール使用が、11月ではわずか1件

その他利用方法

誤って消したメールデータの復元に「メールアーカイブ」機能を使っている

価格情報

	NetRAPTOR 300 M type	NetRAPTOR 300 U type	NetRAPTOR 500 M type	NetRAPTOR 500 U type
対応機能	メール解析・検索専用	メール/Web/ftp 解析・検索	メール解析・検索専用	メール/Web/ftp 解析・検索
想定利用者数	100人～500人程度		500人～2,000人程度	
想定パケット量/日	～20GB(1ヶ月 400GB程度)		～50GB(1ヶ月 2.5TB程度)	
CPU数	Xeonクアッドコア 1 CPU		Xeonクアッドコア 2 CPU	
メモリ構成	8GBから16GB		24GBから48GB	
ディスク構成	システム領域 (RAID-1) データ領域 1TB～4TB RAID-5 (3D+1P)		システム領域 (RAID-1) データ領域 4.5TB～7.2TB RAID-5 (3D+1P+Hotspare)	
テープバックアップ	LTO(オプション)			
外部ストレージ	N/A		NAS(カスタム・オプション)	
市場想定価格(税別)	180万円～	260万円～	480万円～	580万円～

必要機能別、パケット量別に最適な処理能力で機種選定します。



MagiPass

Magi Pass

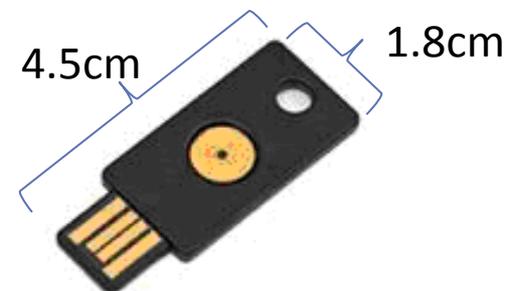
二要素認証による不正アクセス防止

MagiPassとは

- ワンタイムパスワード認証ソリューション
- PIN (Personal Identification Number、個人を認証するパスワード) とトークンデバイスという物理的・機械的な要素を組合わせて強固で安全な認証を提供
- トークンデバイスにYubiKey(Yubico社)を採用
- VMware ESXi version 5 環境で動作するVirtual Applianceとして提供



© VMware, Inc.



二要素(二因子)認証

- 知っているもの + 持っているもの
- 知っているもの
 - (記憶している)パスワード、PIN
- 持っているもの
 - デバイス、証明書など



二要素(二因子)認証の例

ユーザアカウント

User ID

Password

PIN

OTP

Personal
Identification
Number

One
Time
Password

トークンデバイスを使ったOTP

OneTimePasswod

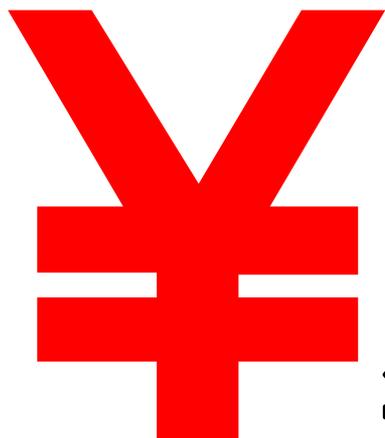
893248

従来のトークンの課題

時刻同期式：手入力

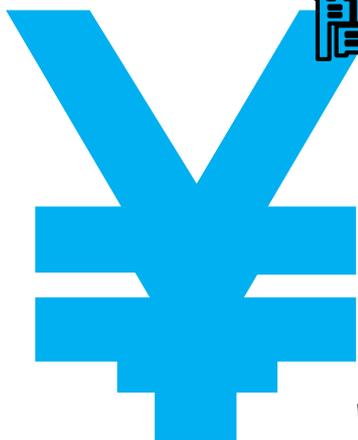


従来のトークンの課題



**高い入力
の負荷
電池交換
が必要
運用コスト
増
高額な管理
ソフトウェア
生成アルゴリズム
漏えいの危険性**

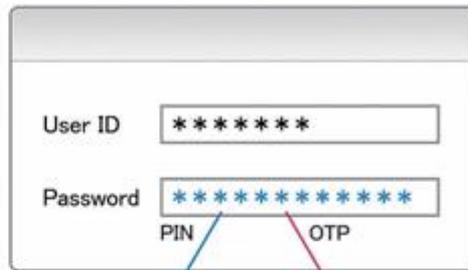
MagiPassのメリット



簡単に使える(運用が変わらない)
電池交換は不要
運用コストも低額
安価な管理ソフトウェア
なりすまし、漏えいの危険性なし

MagiPassによる認証操作(イメージ)

通常のIDとパスワードを入力



固定パスワード ワンタイムパスワード



トークン・デバイス
YubiKey



トークン・デバイスをPCのUSBポートに挿入する
トークン・デバイスを押下して、ワンタイムパスワードを入力する
※ワンタイムパスワードは自動入力される



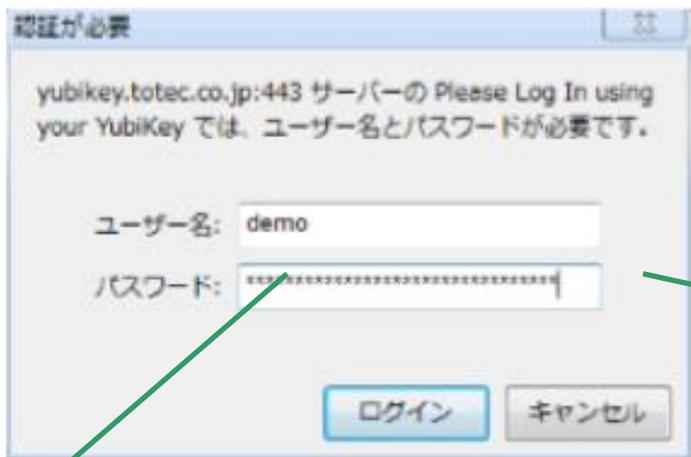
1) パソコンのUSB ポートにトークン・デバイスを挿入する

2) インターネット・バンキングのログイン画面にアクセスする

3) ID とパスワードを手入力する (要素1)

4) 続けてパスワードの入力領域でトークン・デバイスを指で触り、トークン・デバイスから自動的にワンタイムパスワード(要素2)を入力する

5) ログイン処理の実行を行い、ログイン成功



Touch!



パスワード発行例

totec01b|hfefetivgekkvrrv ivgfhrjvehlggckikfe
totec01b|hfefcihi ehcuucjfkjhjibrdvrtgdrkfbr|
totec01b|hfegjhcgjkhfrkbkkugkujrgvenjvvrngfv

PIN

+

ワンタイムパスワード

認証の流れ

- (1) ログインリクエスト
- (2) 認証リクエスト
- (3) 認証結果応答
- (4) 接続確立



※ADサーバーとの連携は
MagiPass拡張版にて提供予定

利用環境(オペレーティングシステム)

OSを選ばない

MagiPassのハードウェアトークンはUSBキーボードとして認識されるため、WindowsやMac、Linuxなどの各種OSをはじめ、iPadなどで用いられるiOSやAndroidなどのタブレット端末やシンクライアント環境など、USB接続をサポートしている様々な環境で利用可能



NFC対応もリリース済み



他のワンタイムパスワード製品と比較

液晶表示デバイス



イメージ認証

7080	3904
7459	4658
0885	4374
8309	4700

ソフトウェア
トークン



電池交換が必須
コスト負担！作業(費用)負担！
手入力する ⇒ 74894354
利用者に負担！
パスワード強度が弱い(6桁)



4.5cm

1.8cm

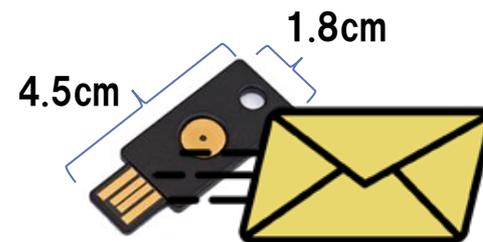


Magi Pass

電池交換不要
コストが安い！作業(費用)も不要！
タッチするだけ！
44桁のワンタイムパスワードを自動入力
パスワード強度が強い
⇒ blhfefetivgekkvrrrvivgfhrrjvehlggckikfe



- **配布が簡単**
 - 例えば普通郵便（※1）でも送れる形状
 - 小さい、軽い、壊れない
- **登録が簡単**
 - ユーザを選択
 - デバイスにタッチ
 - 割り当て(登録)完了
- **使い方が簡単**
 - PCに挿入してタッチするだけ
 - 入力不要



ユーザの編集

ユーザ名: user01@example.jp
パスワード:
メモ:
管理者: はい

ユーザに割り当てられたYubiKey-IDの一覧

YubiKey ID	作成日時	変更日時	状態	操作
YubiKey IDは割り当てられていません。				
新しいYubiKeyを入力: <input type="text" value="dpcobsooc kdrdklshfbcnkibgnono tyjhiksklthf"/>				<input type="button" value="割り当て"/>



(※1) 実際に配布されるときは、セキュリティ上安全な方法で配布いただくことを強くお勧めします。

MagiPass価格情報

MagiPassシリーズ製品価格表

2014年1月現在

MagiPassソフトウェアライセンス

製品名	型番	製品標準価格	保守標準価格 (初年度必須)	アカウント	1アカウント単価
MagiPass BL-50	MP-BL50	¥500,000	¥100,000	50	¥10,000
MagiPass BL-100	MP-BL100	¥1,000,000	¥200,000	100	¥10,000
MagiPass BL-500	MP-BL500	¥2,000,000	¥400,000	500	¥4,000
MagiPass BL-1000	MP-BL1000	¥3,000,000	¥600,000	1,000	¥3,000

YubiKey認証トークン

製品名	型番	製品標準価格	保守参考価格 (任意契約)	アカウント	1アカウント単価
YubiKey	YK-10	¥60,000	¥4,200	10	¥6,000
YubiKey	YK-100	¥500,000	¥35,000	100	¥5,000
YubiKey	YK-500	¥2,000,000	¥140,000	500	¥4,000
YubiKey	YK-1000	¥3,000,000	¥210,000	1,000	¥3,000
YubiKey	YK-10000	¥20,000,000	¥1,400,000	10,000	¥2,000

MagiPassライセンス (アカウント無制限)

製品名	型番	製品標準価格	保守標準価格 (初年度必須)	アカウント	備考
MagiPass BX-20	MP-BX20	¥24,000,000	¥4,800,000	無制限	同時稼働は 1,000認証程度

セキュリティ対策製品インテグレーション

- セキュリティ対策は極めて幅広く多岐に渡る
 - 利用する製品・サービスも多くなる
- 
- お客様の状況に合わせた製品・サービス選定
 - セキュリティ導入・運用のインテグレーションサービスご提供

入口対策

代表的な対策

次世代ファイアウォール
マルウェア検知システム

(sandbox)

IPS/IDS

認証強化(二要素認証)

Web Application Firewall

Proxy ... etc

内部対策

代表的な対策

アンチウィルス

未知のマルウェア対策

エンドポイント管理/MDM

DB/ ファイル監視

ログ管理

SIEM ... etc

出口対策

代表的な対策

ネットワークフォレンジック

Data Loss Prevention

ボットネットアクセス監視

次世代ファイアウォール

メールセキュリティ

ファイル送信システム...etc

セキュリティ対策導入インテグレーション

弊社サイバーセキュリティセミナーご案内

【日時】2014年7月31日(木)14:00～16:00(13:30受付開始)

【テーマ】終わらない脆弱性との戦い — 企業と顧客を守るサイバーセキュリティ

【セッション】

サイバーセキュリティ国際標準 — 脆弱性の管理と対応

～ITU-Tで進められるサイバーセキュリティ国際標準と、その活用方法について～

講師：門林 雄基 氏(奈良先端科学技術大学院大学情報科学研究科 准教授)

検証 — OpenSSL Heartbleed Bugと可遡及性

～OpenSSL Heartbleed Bugを検証し、ネットワークフォレンジックスによる被害特定の重要性について検討～

講師：藤原 礼征(トーテックサイバーセキュリティ研究所 所長)

【会場】大崎・ゲートシティホール「ルームB」

(東京都品川区大崎1-11-1 ゲートシティ大崎B1F)

詳しくはこちら⇒http://www.totec.jp/seminar/2014/month_07.html#date0731

