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

【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

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

東北オフィス

東京本社

福岡事業所

トヨタ事業所

東濃・各務原・春日井・刈谷SC

トーテックアメニティ事業構成

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）

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

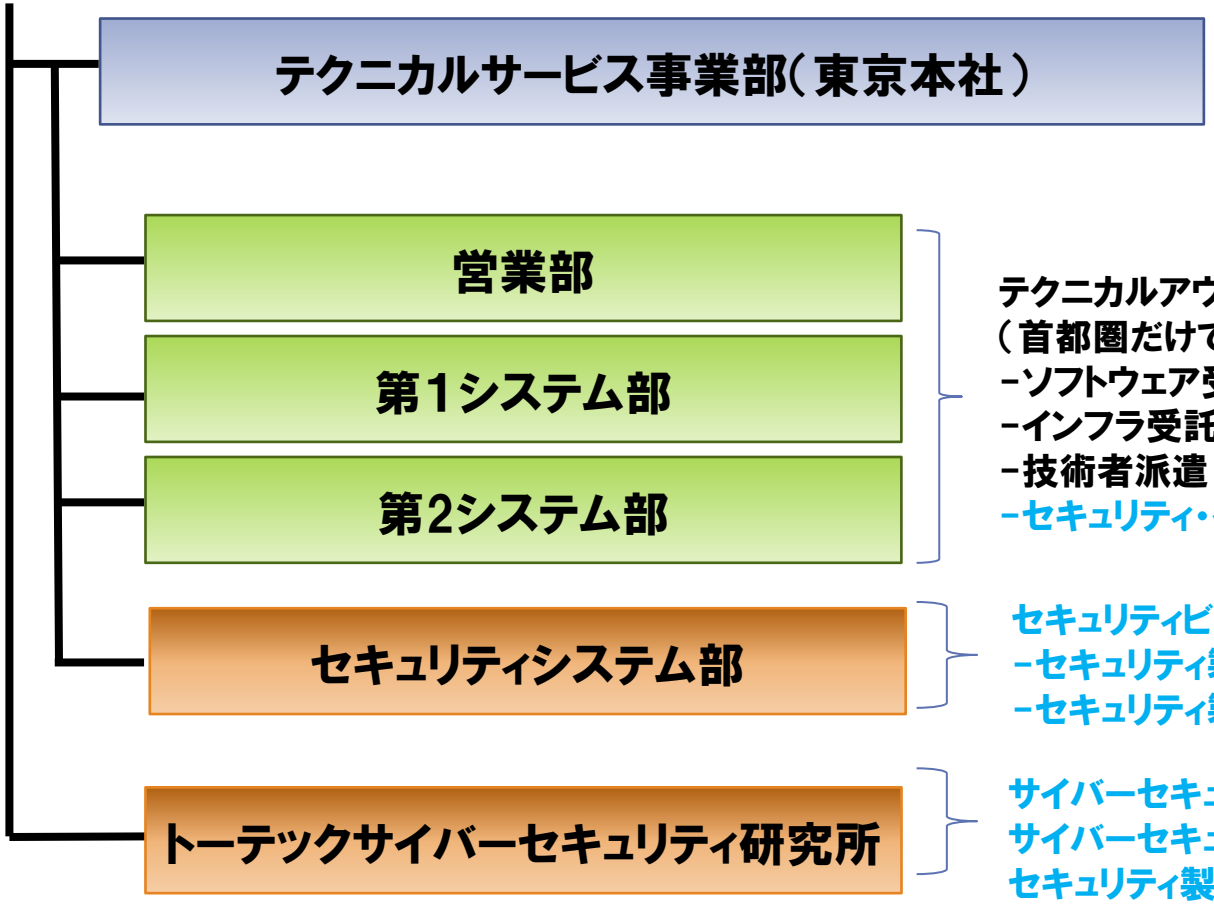
開発請負・技術者派遣

有機的に結合

技術戦略

新規事業への取り組み

テクニカルサービス事業部



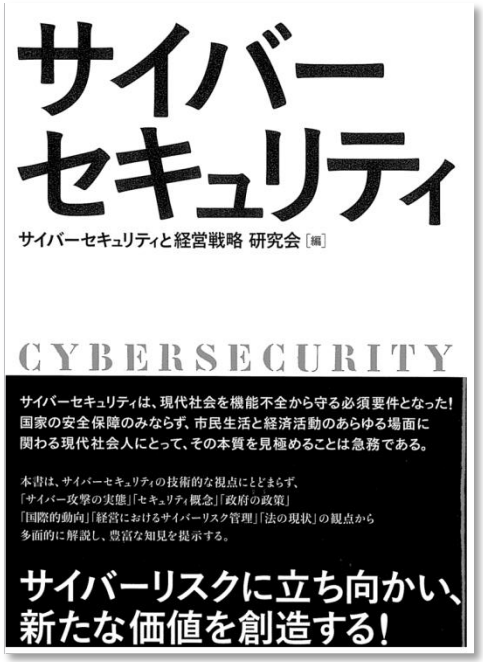
テクニカルアウトソーシング
（首都圏だけで250名を超える技術者）
-ソフトウェア受託開発
-インフラ受託、運用
-技術者派遣
-セキュリティ・インテグレーション／運用（開発中）

セキュリティビジネス
-セキュリティ製品開発・販売
-セキュリティ製品インテグレーション

サイバーセキュリティ最先端技術調査、研究
サイバーセキュリティに関する啓蒙活動、著作活動
セキュリティ製品企画

顧問）門林　雄基　奈良先端科学技術大学院大学　情報科学研究科准教授・博士（工学）
顧問）浅沼 宏和　株式会社TMAコンサルティング　代表

サイバーセキュリティ啓蒙活動の取組み



本書は世に出るべくして出た良書であり、"痒い処に手が届く"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の観点から観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レビュワー

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	内部対策	出口対策
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	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	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ー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

信頼関係

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)

2014-04-09	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)	
2014-04-08	OpenSSL の脆弱性に関する注意喚起(公開)	
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)	
2014-03-12	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)	
2014-03-12	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)	
2014-03-07	Apache Commons FileUpload および Apache Tomcat の脆弱性に関する注意喚起(更新)	
2014-02-28	Apache Commons FileUpload および Apache Tomcat の脆弱性に関する注意喚起(更新)	
2014-02-21	Adobe Flash Player の脆弱性(APSB14-07)に関する注意喚起(公開)	
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)	
2014-02-20	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)	
2014-02-12	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)	
2014-02-10	Apache Commons FileUpload および Apache Tomcat の脆弱性に関する注意喚起(公開)	
2014-02-05	Adobe Flash Player の脆弱性(APSB14-04)に関する注意喚起(公開)	
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)	
2014-01-15	Adobe Flash Player の脆弱性(APSB14-02)に関する注意喚起(公開)	
2014-01-15	Adobe Reader 及び Acrobat の脆弱性(APSB14-01)に関する注意喚起(公開)	
2014-01-15	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)	4.13KB
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)	4.63KB

2014

公開日	注意喚起内容	テキスト (PGP署名付き)
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
2014-07-09	Adobe Flash Player の脆弱性(APSB14-17)に関する注意喚起(公開)	4.03KB
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
2014-06-12	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
2014-06-11	Adobe Flash Player の脆弱性(APSB14-16)に関する注意喚起(公開)	3.84KB
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
2014-05-15	旧バージョンの Movable Type の利用に関する注意喚起(公開)	5.82KB
2014-05-14	Adobe Reader および Acrobat の脆弱性(APSB14-15)に関する注意喚起(公開)	2.92KB
2014-05-14	Adobe Flash Player の脆弱性(APSB14-14)に関する注意喚起(公開)	3.70KB
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
2014-05-02	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
2014-05-02	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
2014-04-30	Adobe Flash Player の脆弱性(APSB14-13)に関する注意喚起(公開)	3.87KB
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)	
2014-04-16	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
2014-04-15	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
2014-04-11	OpenSSL の脆弱性に関する注意喚起(更新)	5.08KB
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

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)

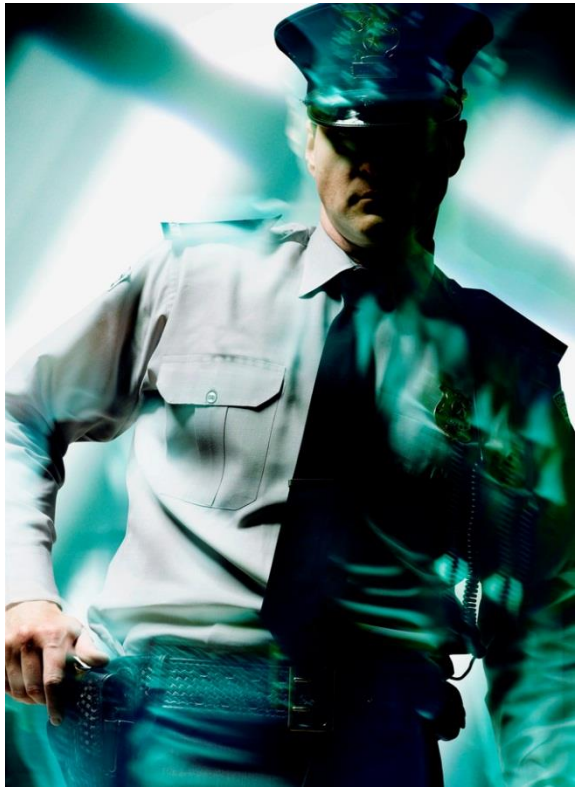
現実世界のアナロジー

ログ管理

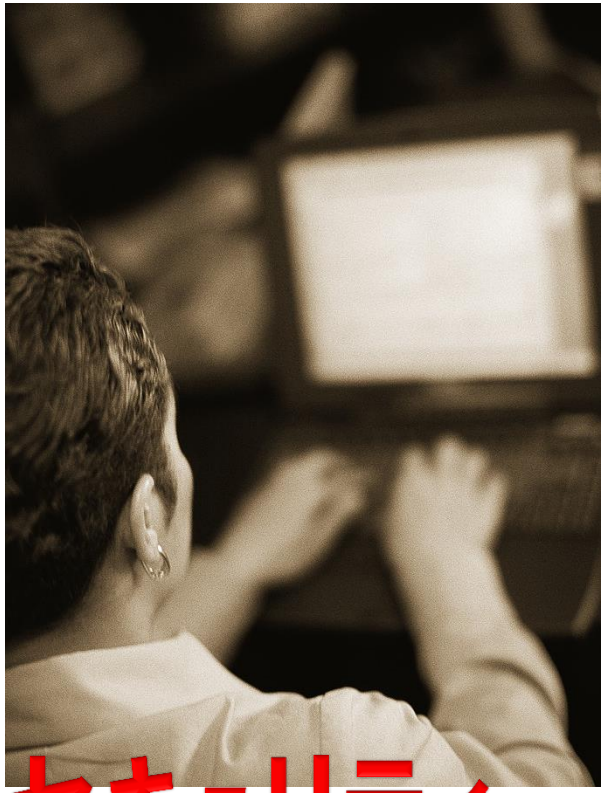

```
127.0.0.1 - - [20/Jun/2003:20:45:14 +0900] "GET / HTTP/1.1" 200 1835
127.0.0.1 - - [20/Jun/2003:20:45:14 +0900] "GET /apache_pb.gif HTTP/1.1" 200 2326
127.0.0.1 - - [20/Jun/2003:20:45:20 +0900] "GET /manual/index.html HTTP/1.1" 200 9904
127.0.0.1 - - [20/Jun/2003:20:45:14 +0900] "GET / HTTP/1.1"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

```
<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="topPage">
<div id="header">
<div class="header01">
<div class="logo"><a href="http://www.netmonitor.jp/"><img src="img/h1_bf.gif" alt=
<h1>
```

フォレンジック
調査

TOTEC AMENITY LIMITED

NetRAPTOR

Unified Network Forensic Appliance

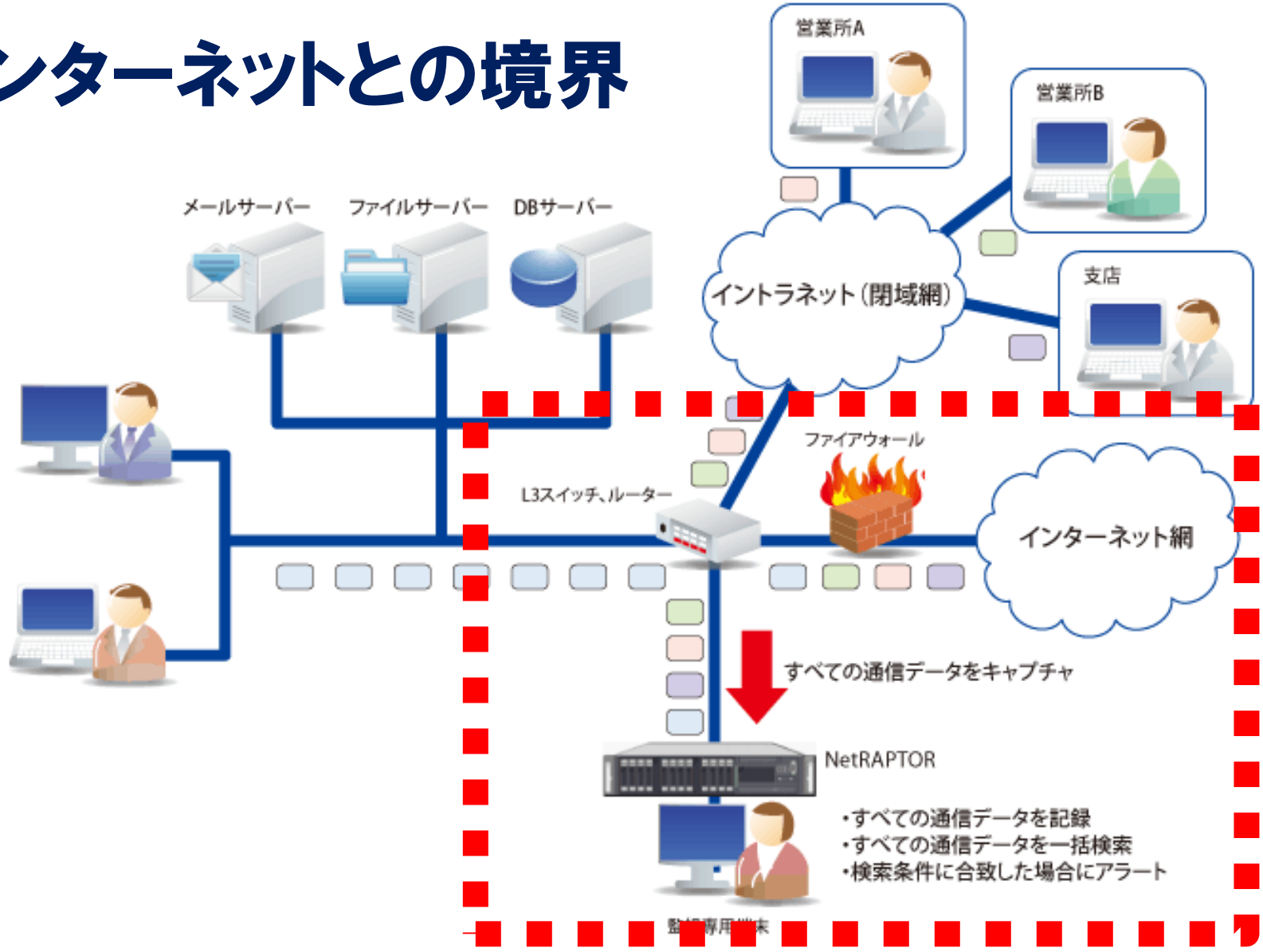
NetRAPTORとは

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！

TOTEC AMENITY LIMITED

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

TOTEC AMENITY LIMITED

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

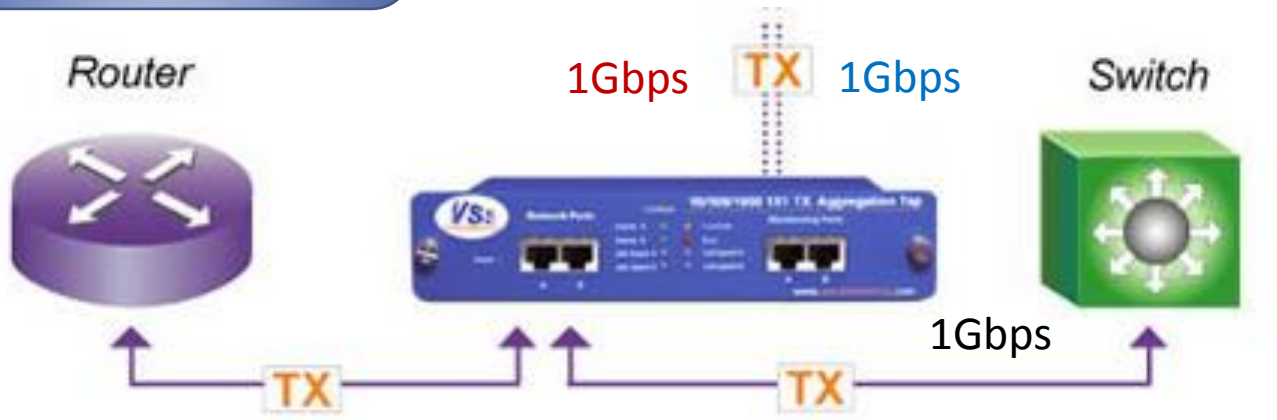
TOTEC AMENITY LIMITED

ロスゼロのパケットキャプチャー

- ギガビット全二重(1Gbps x 2)でパケット取得

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

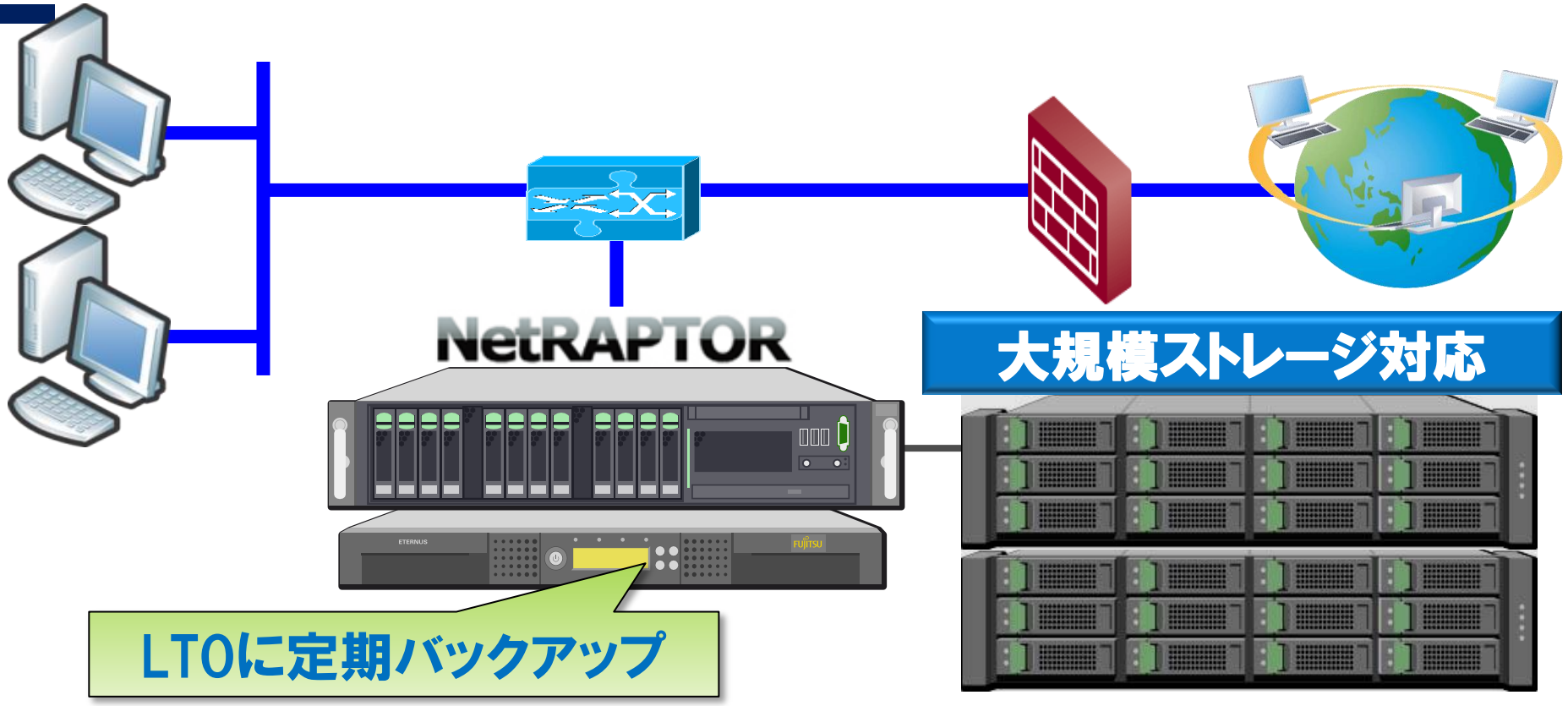
見つける

再現する

警告する

TOTEC AMENITY LIMITED

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

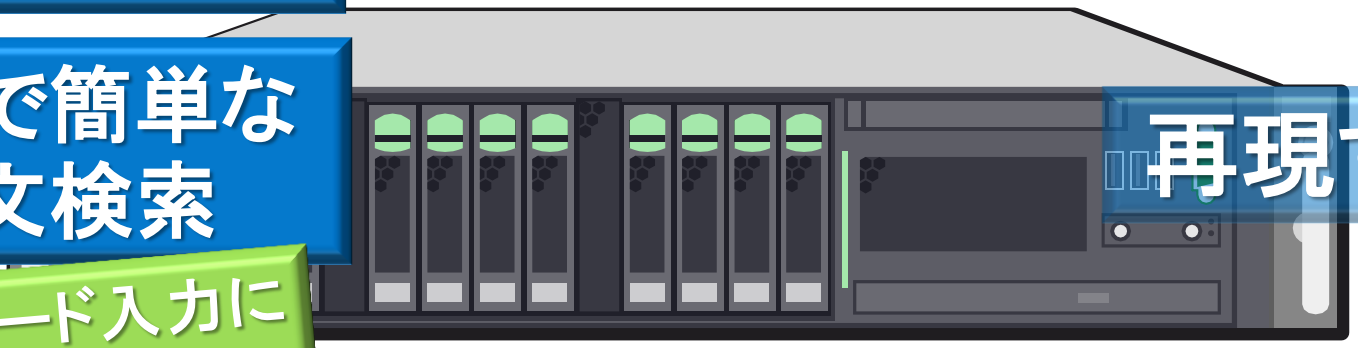
PCIDSS対応支援

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

再現する

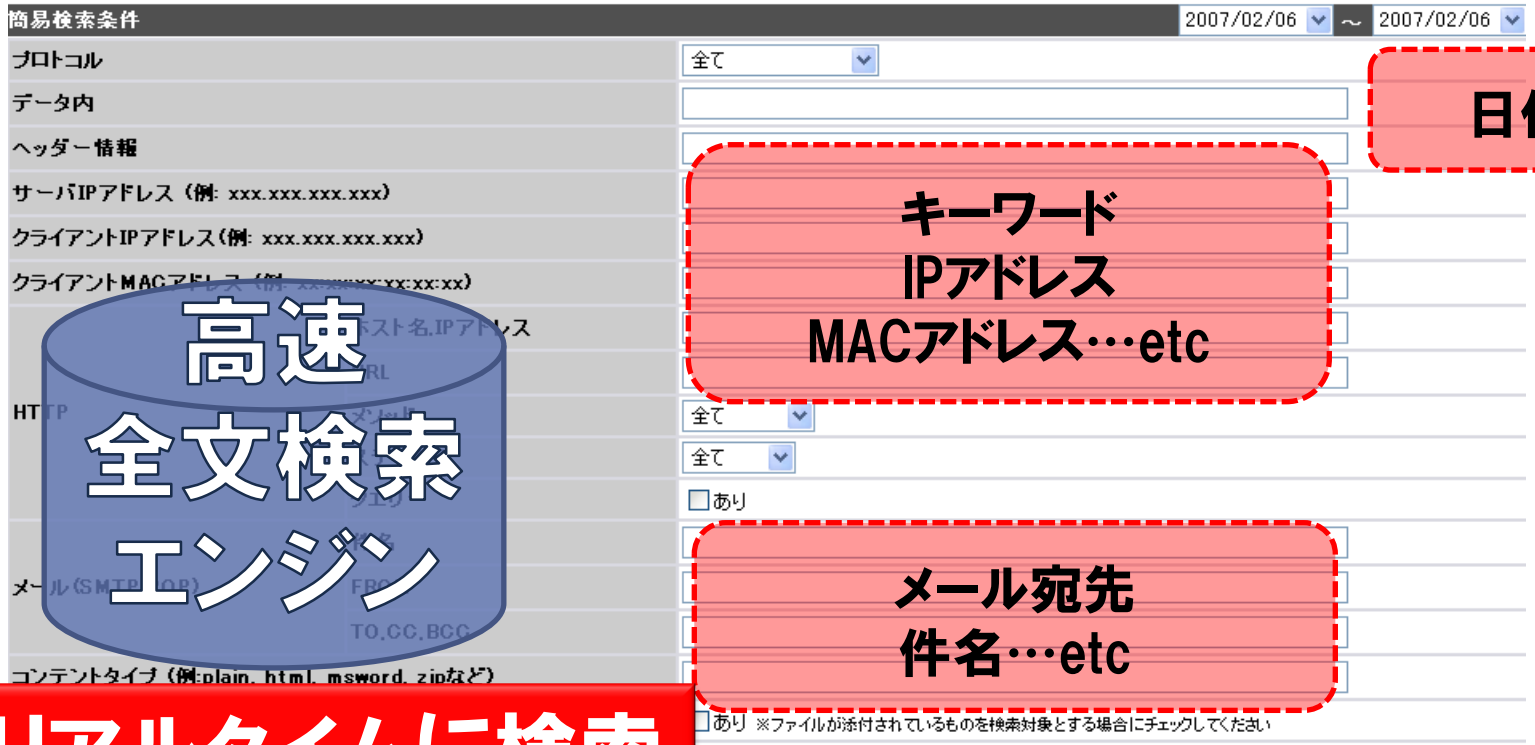
キーワード入力に
よる簡単検索！

警告する

TOTEC AMENITY LIMITED

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



TOTEC AMENITY LIMITED

NetRAPTOR　再現する

PCIDSS対応支援

取りこぼさない
Full キャプチャー

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

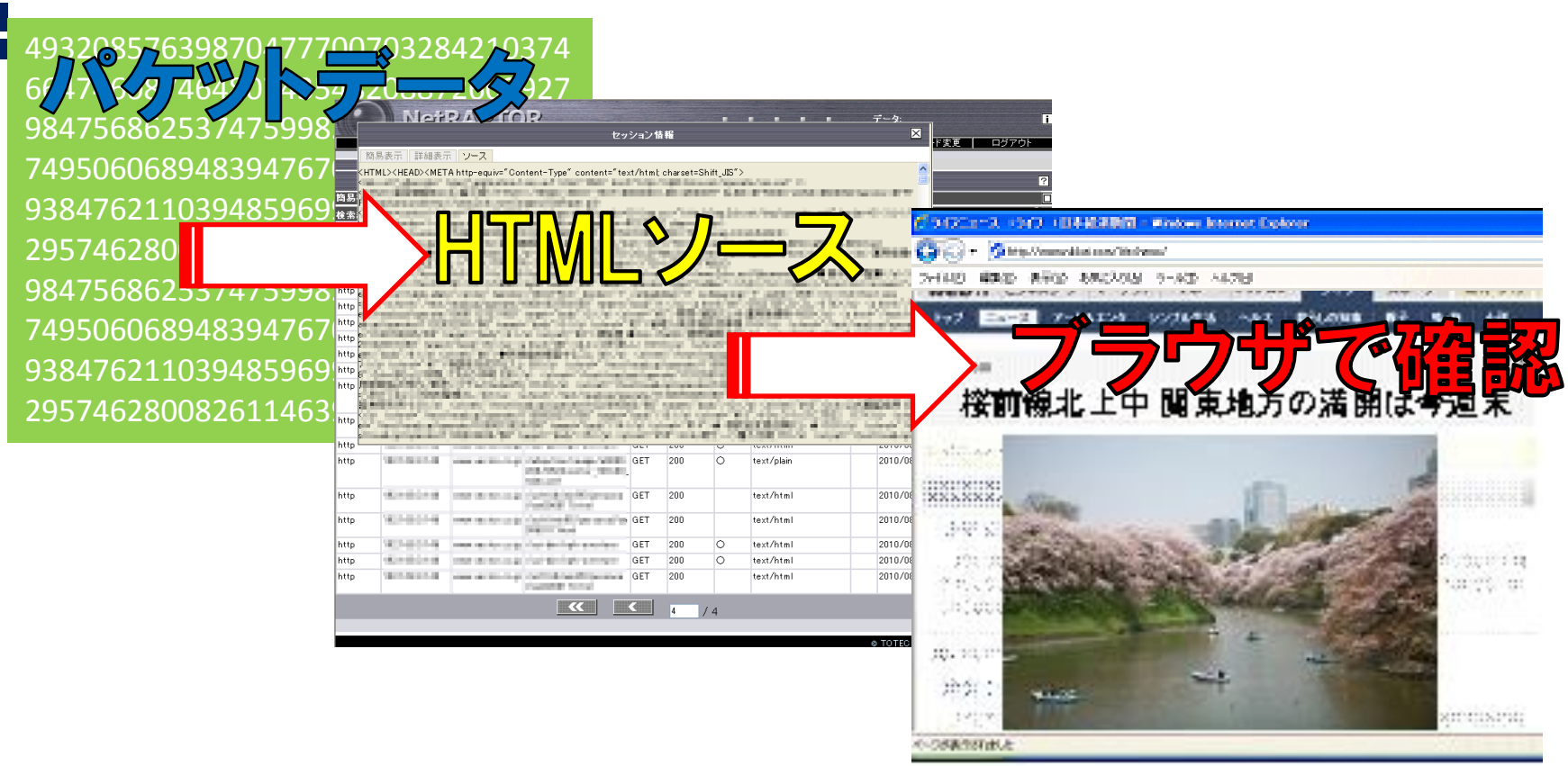
キーワード入力に
よる簡単検索！

メールやWebを
そのまま再現

警告する

TOTEC AMENITY LIMITED

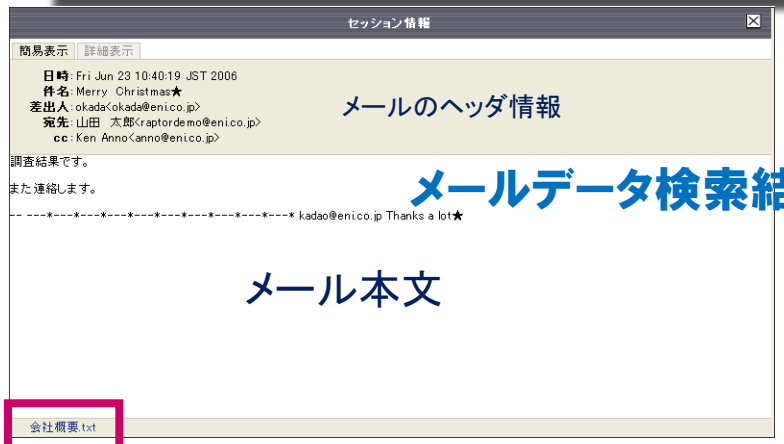
通信内容の見える化



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、送ったままを再現

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



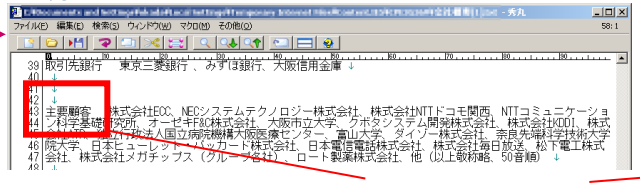
メールのヘッダ情報

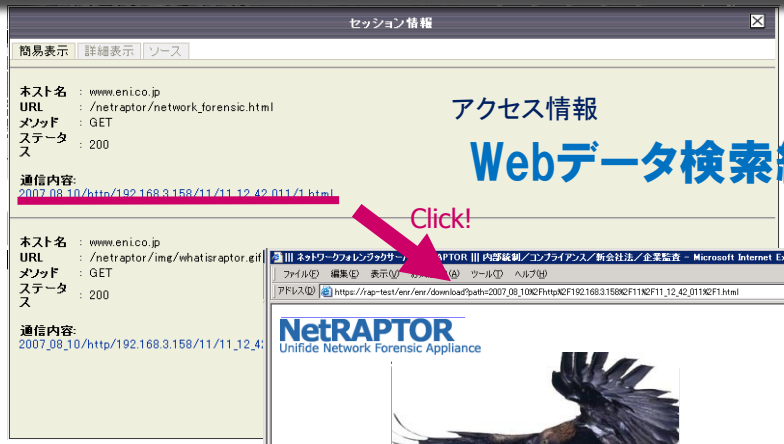
メールデータ検索結果

メール本文

Click!

添付ファイル





アクセス情報

Webデータ検索結果

Click!

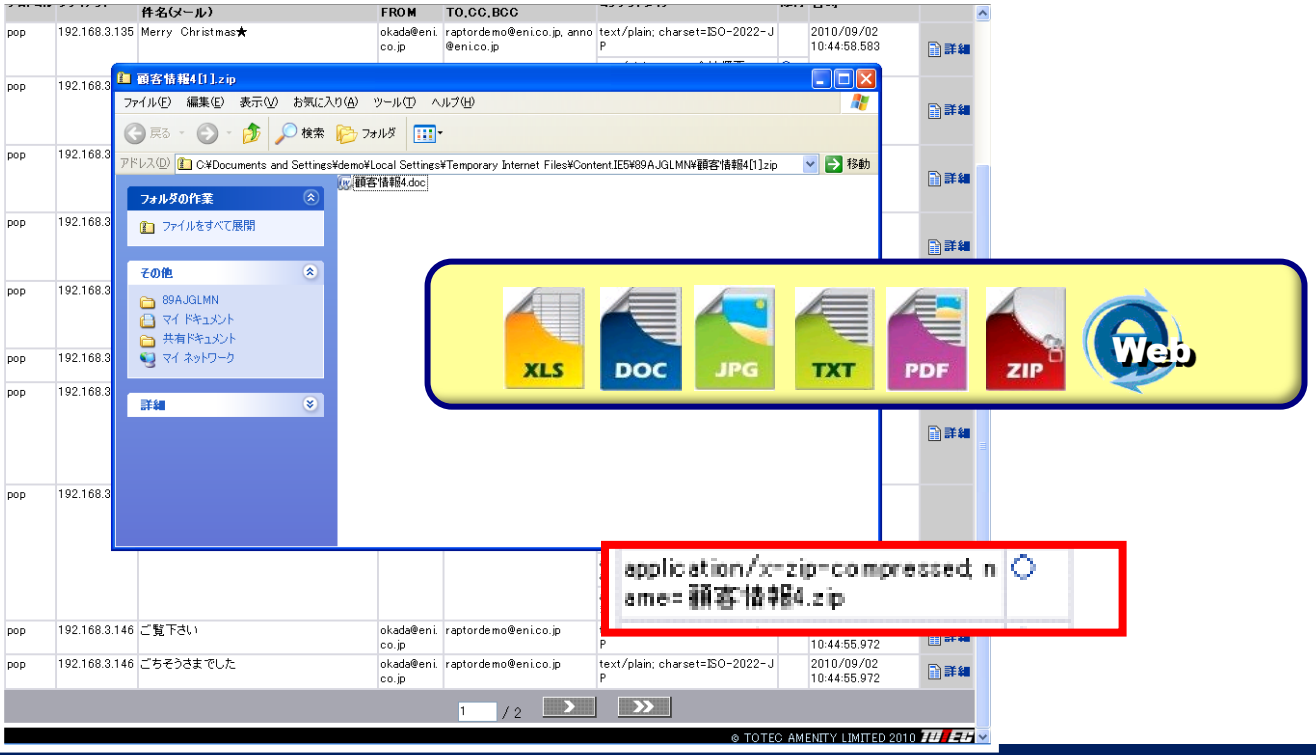
※はめ込み画像です

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す。



NetRAPTOR　警告する

PCIDSS対応支援

取りこぼさない
Full キャプチャー

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！

問題行動の
監視と警告

メールやWebを
そのまま再現

リアルタイムに
メールで通知

TOTEC AMENITY LIMITED

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 acess	全アナライザ

1 / 3

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 atta
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に送信している

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

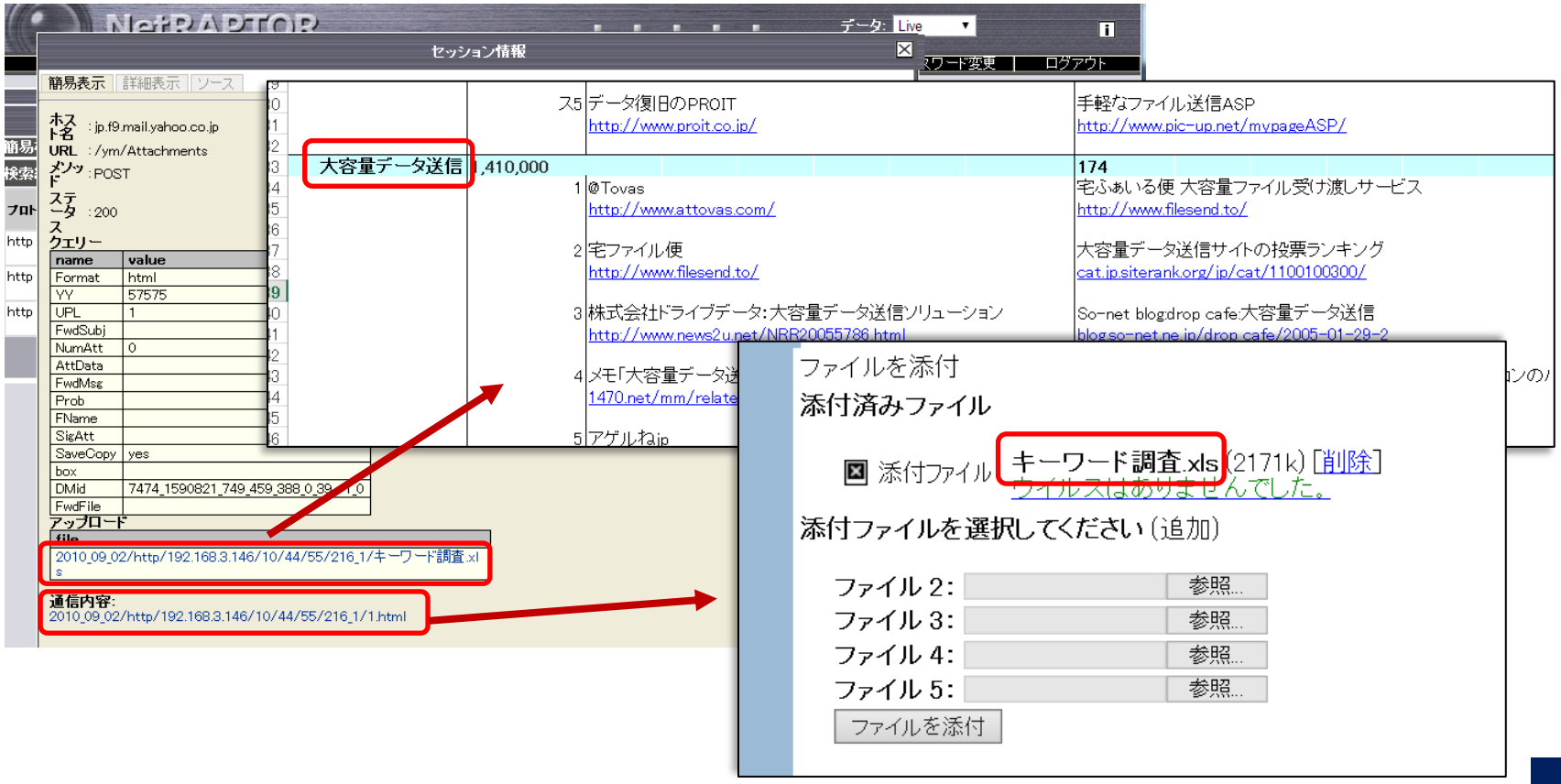
TOTEC AMENITY LIMITED

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

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

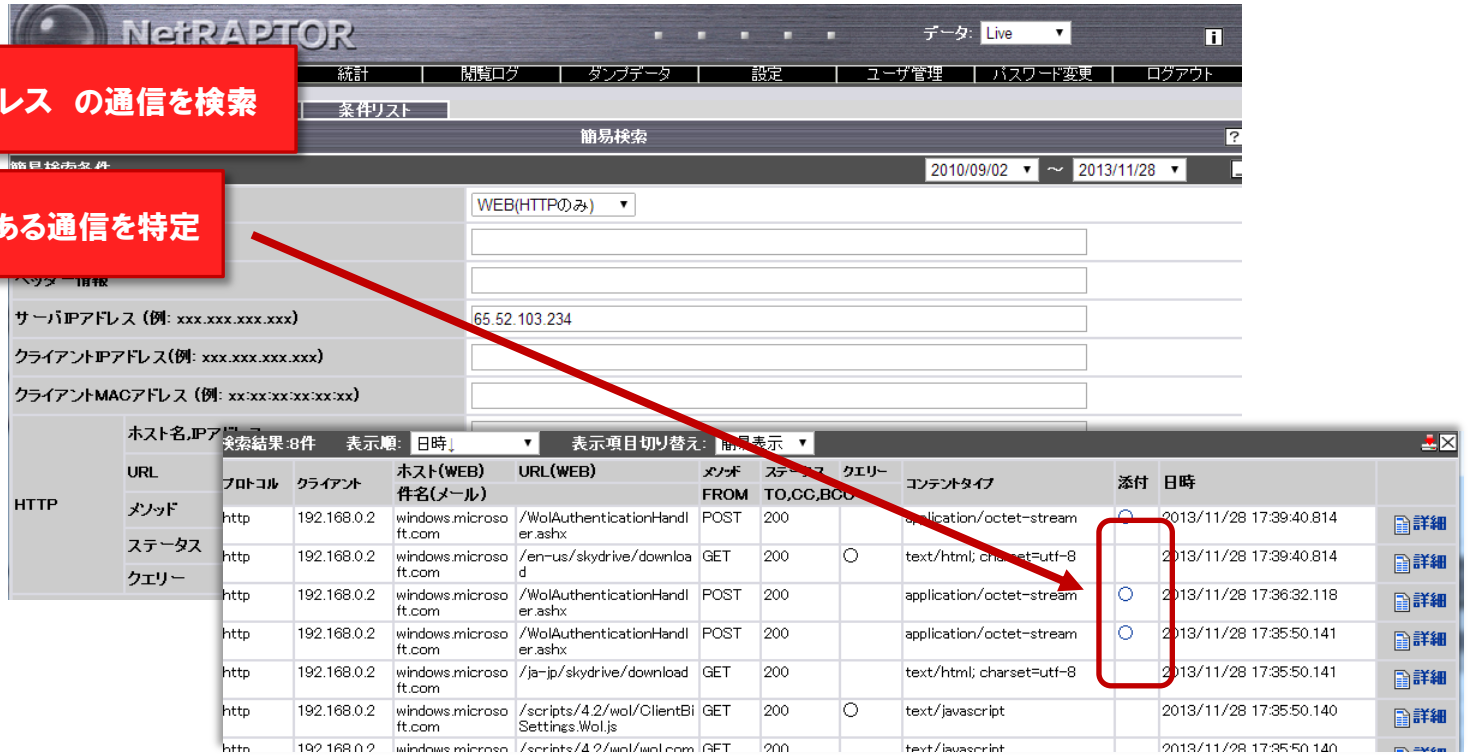


検索イメージ(２)

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、サーバーのIPアドレスが判明

判明したIPアドレス　の通信を検索

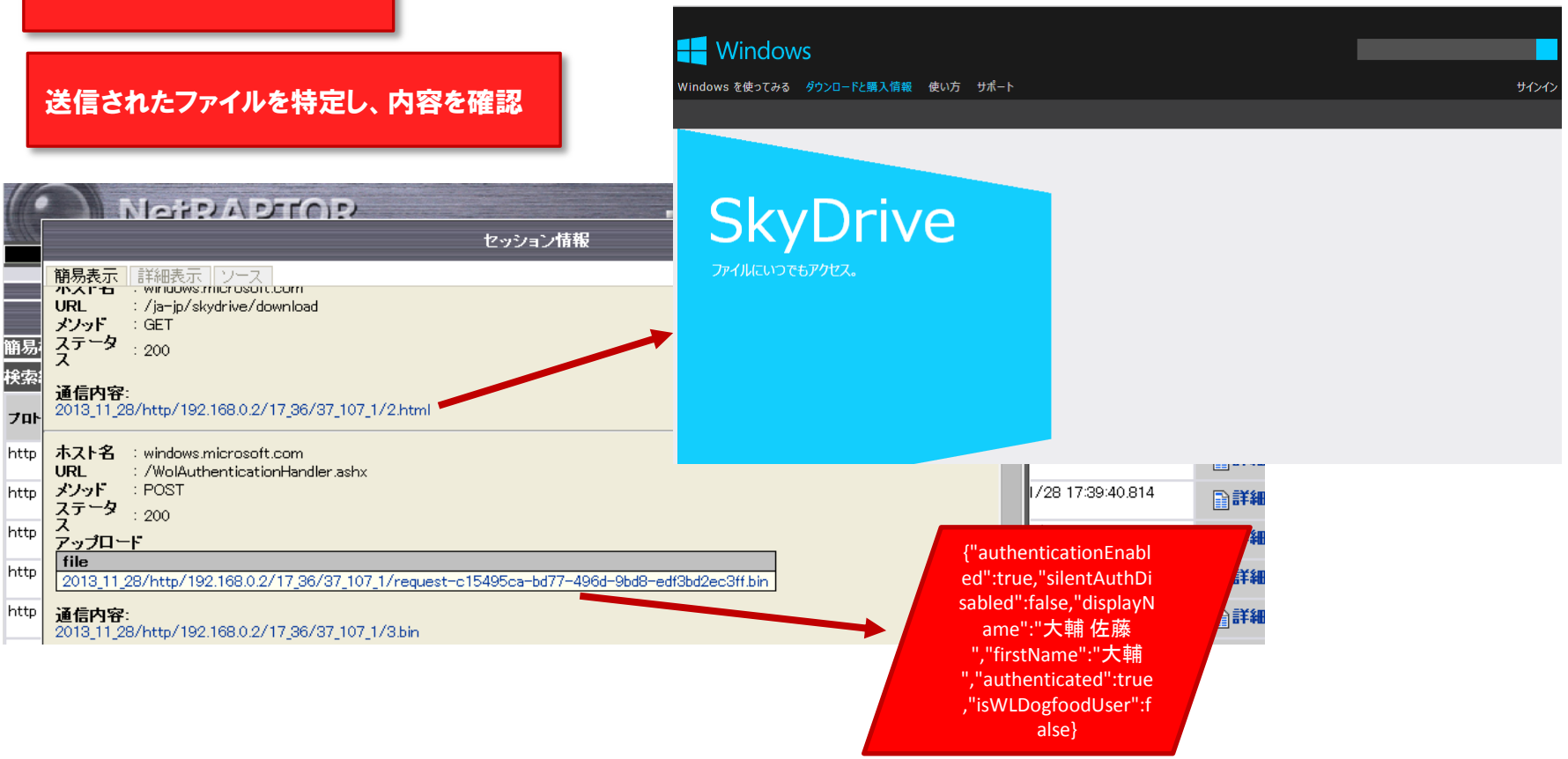
ファイル送信のある通信を特定



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



検索イメージ(３)

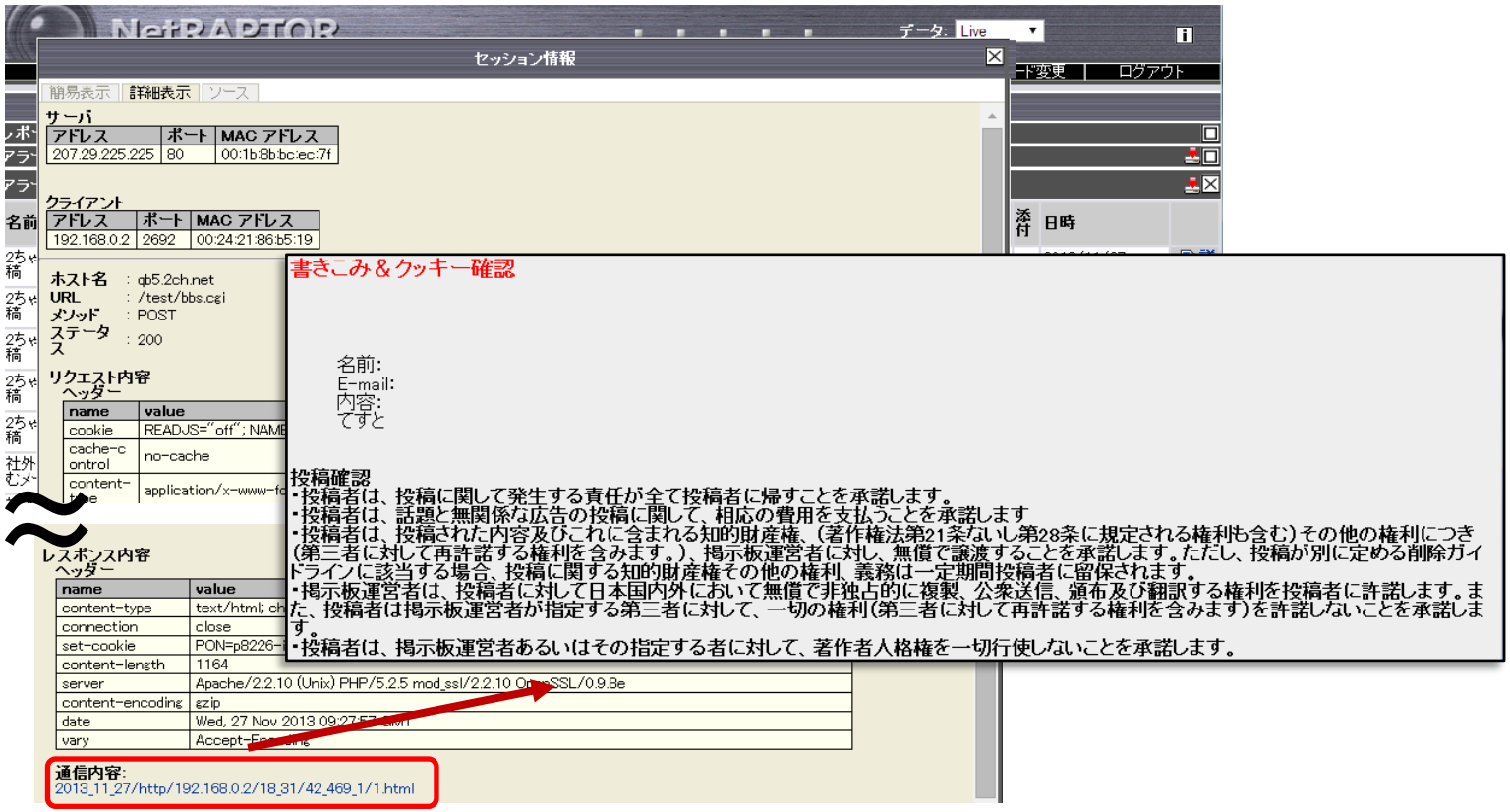
レポート(条件式リストによる警告通知一覧)の確認

該当日時の警告の一覧を確認

警告の具体的な条件式

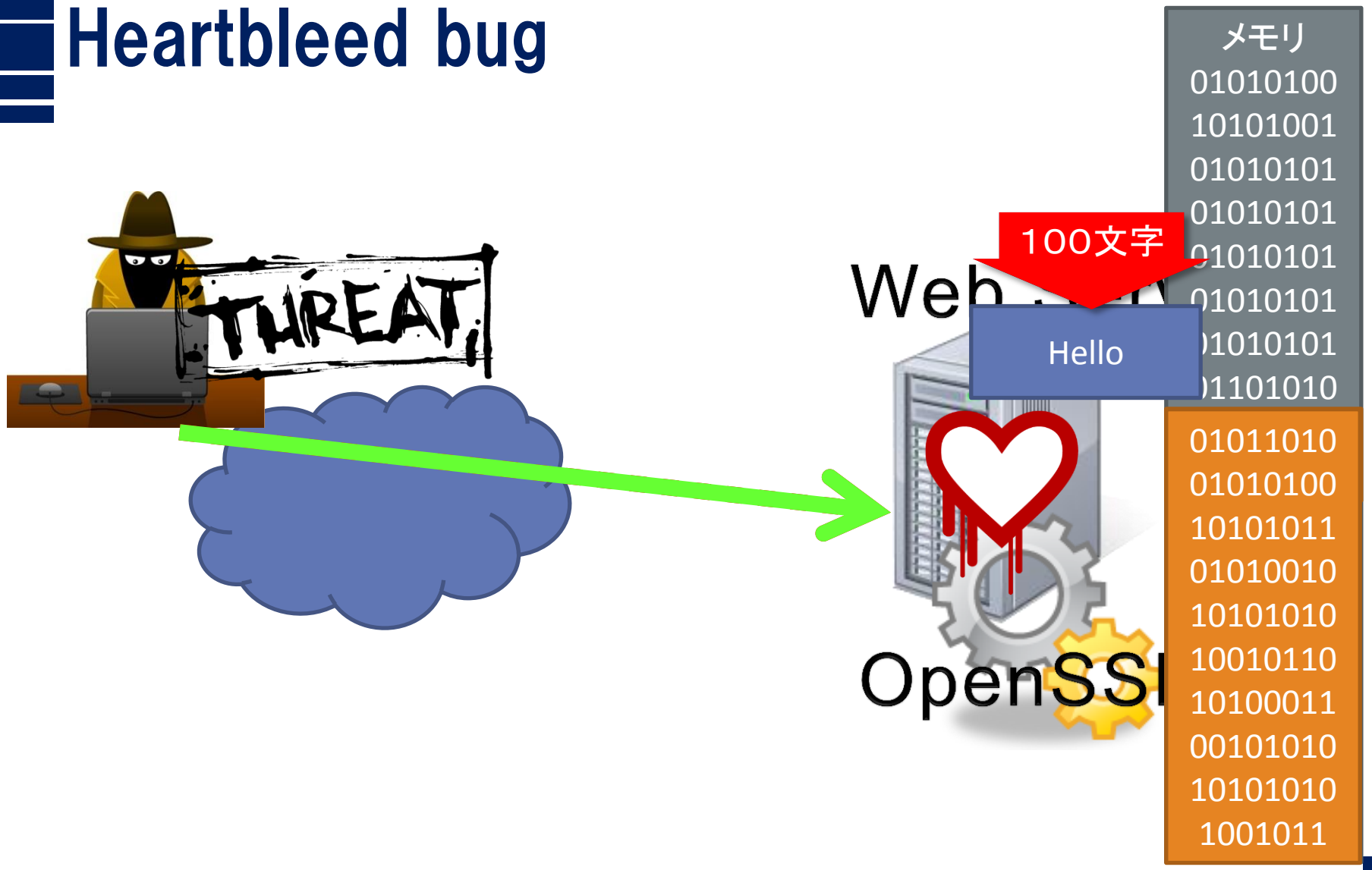
検索結果イメージ(３)

警告対象のWebアクセスを確認

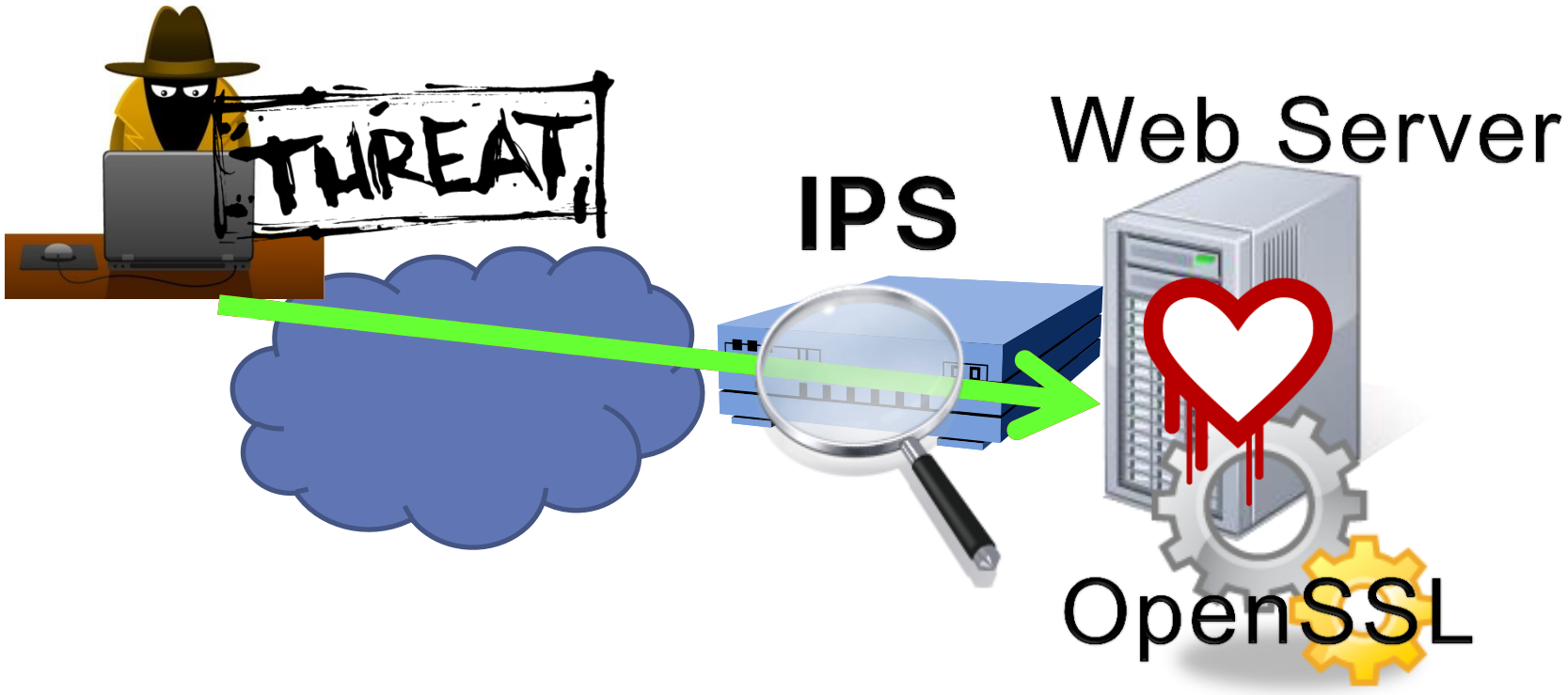


OpenSSL Heart Bleed Bug

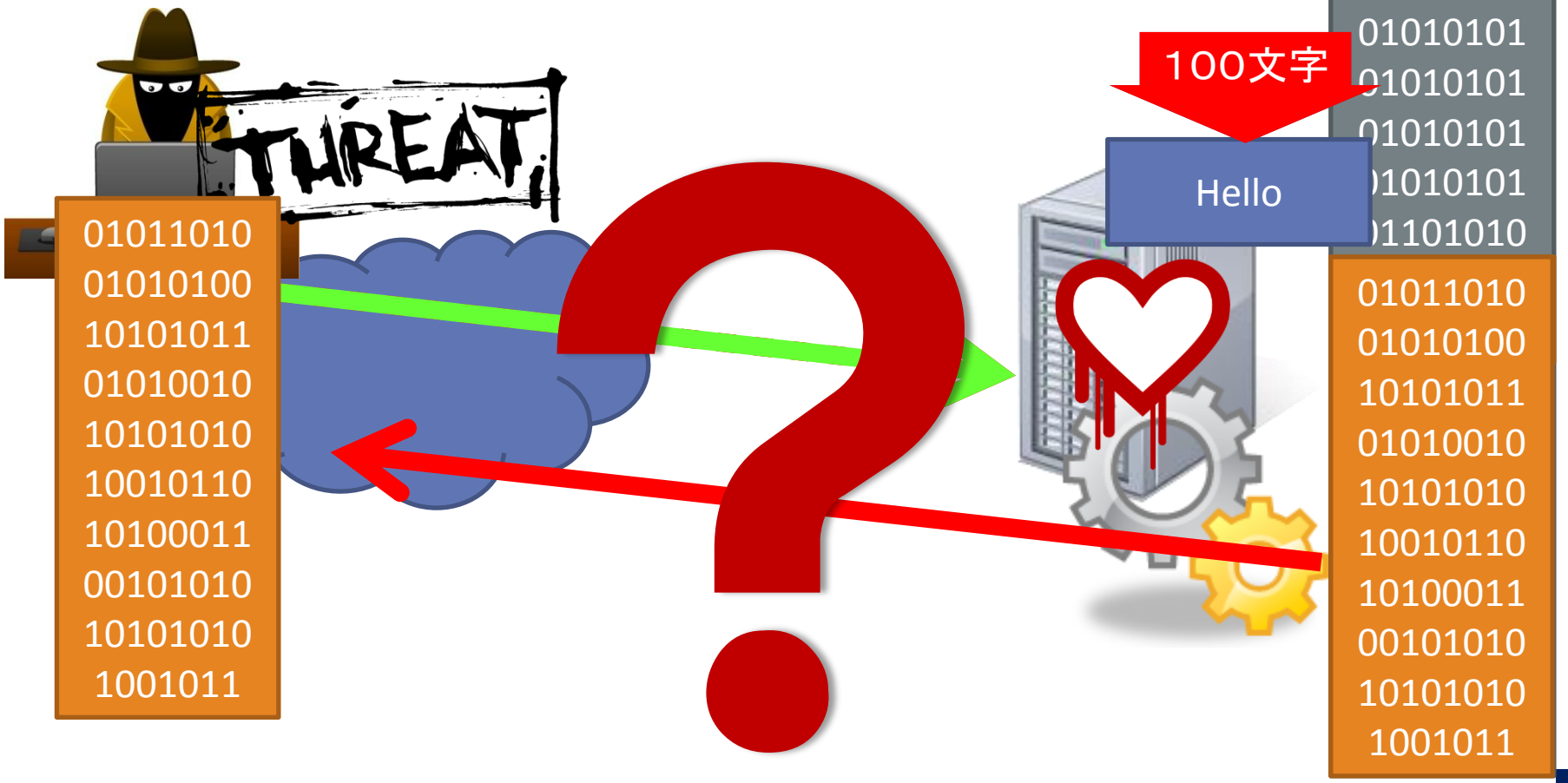
Heartbleed bug



IPS で検知可能

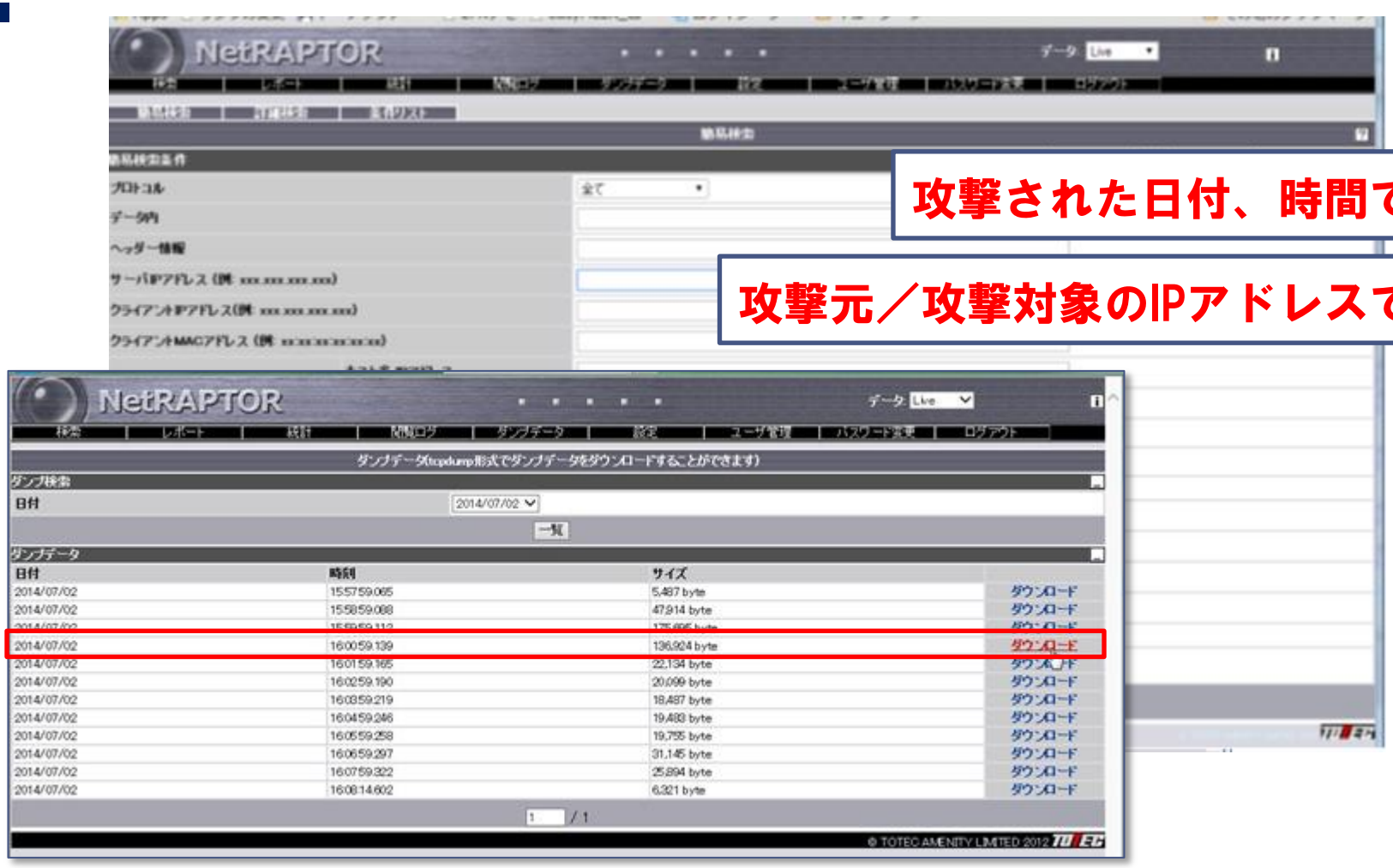


盗まれたメモリの情報は？

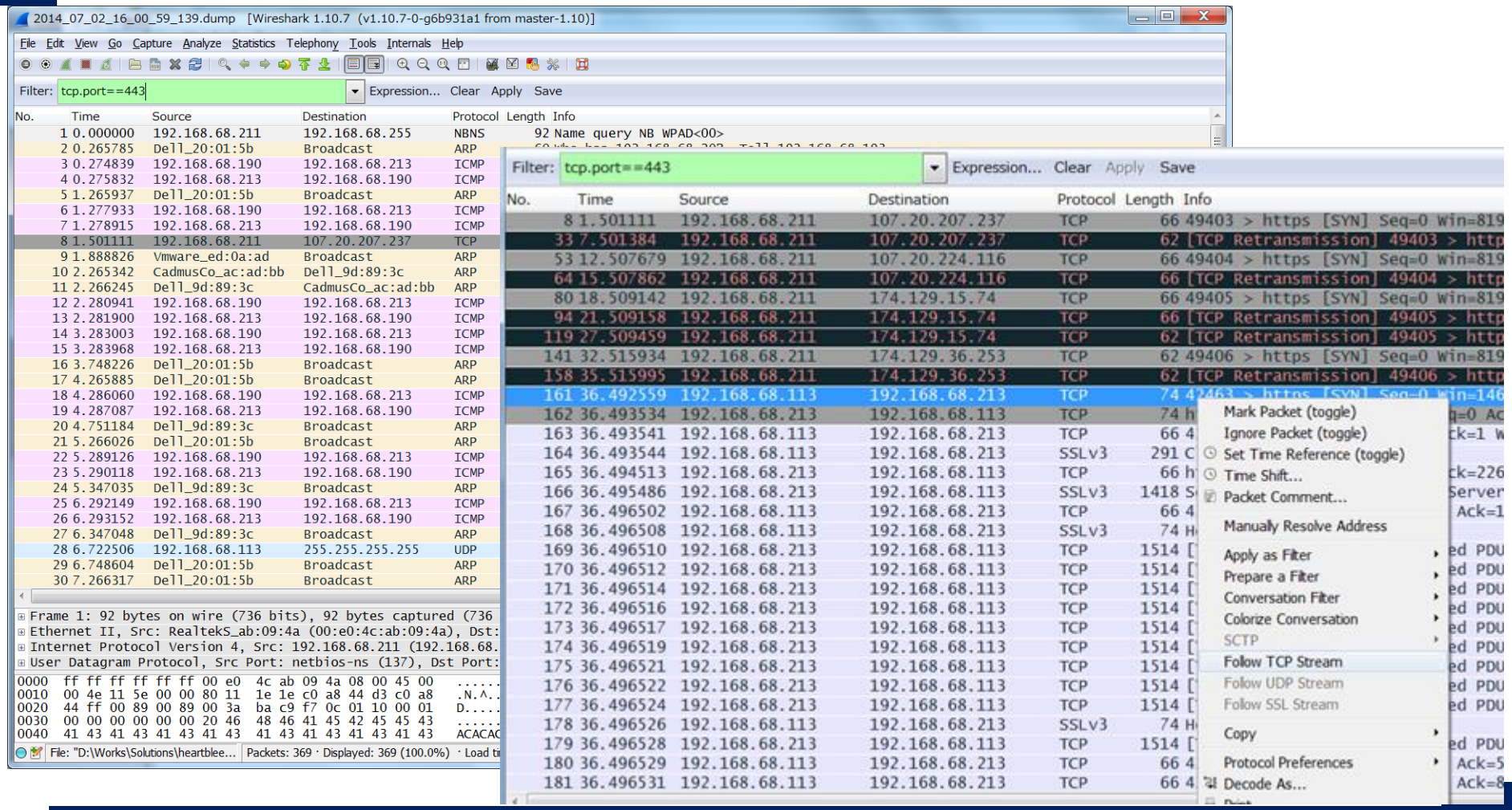


盗まれたメモリの情報は？

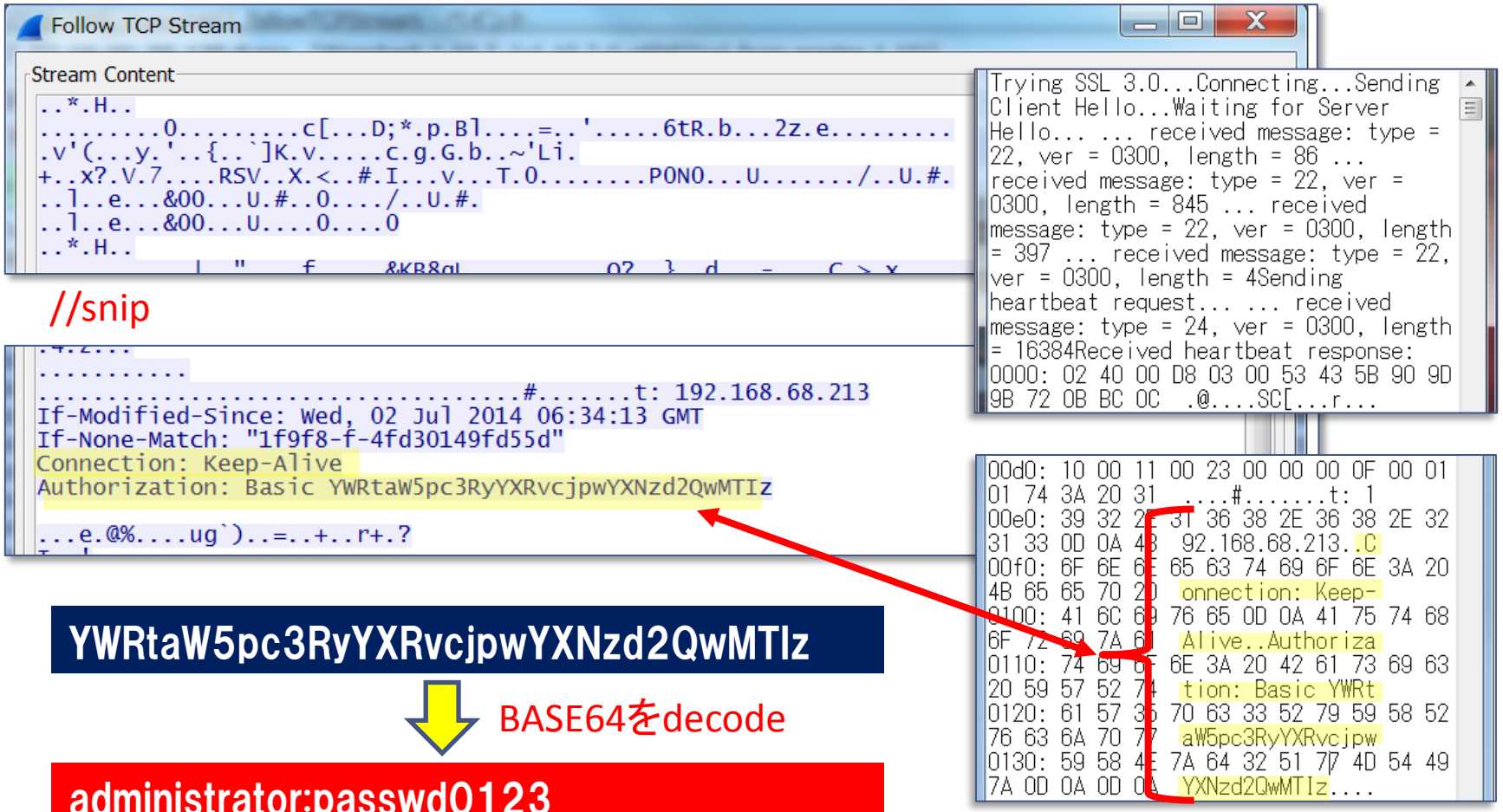
Heartbleed bug を検証する



Wiresharkを使ってパケットを再現



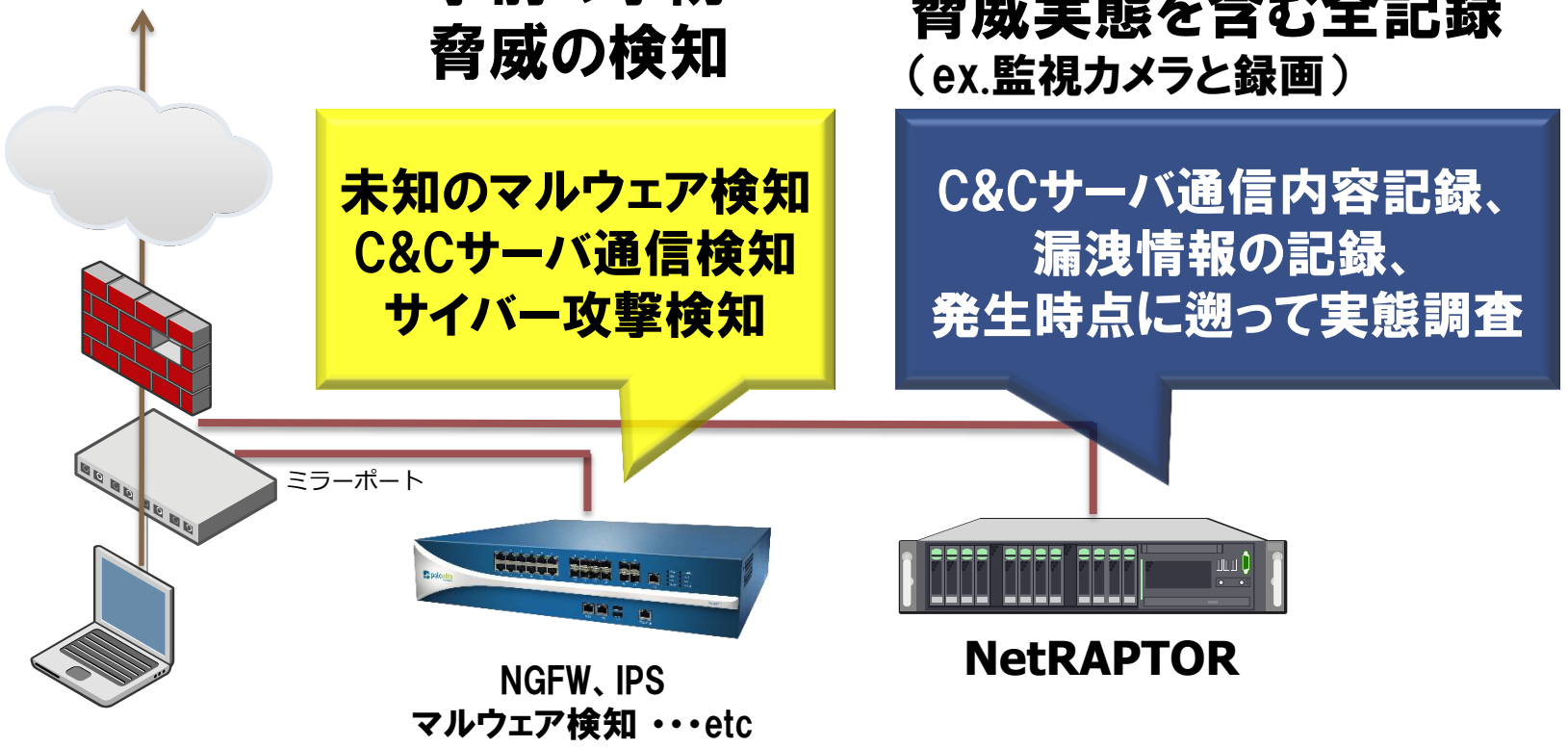
Basic認証のパスワード漏洩をキャプチャー



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

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）



TOTEC AMENITY LIMITED

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

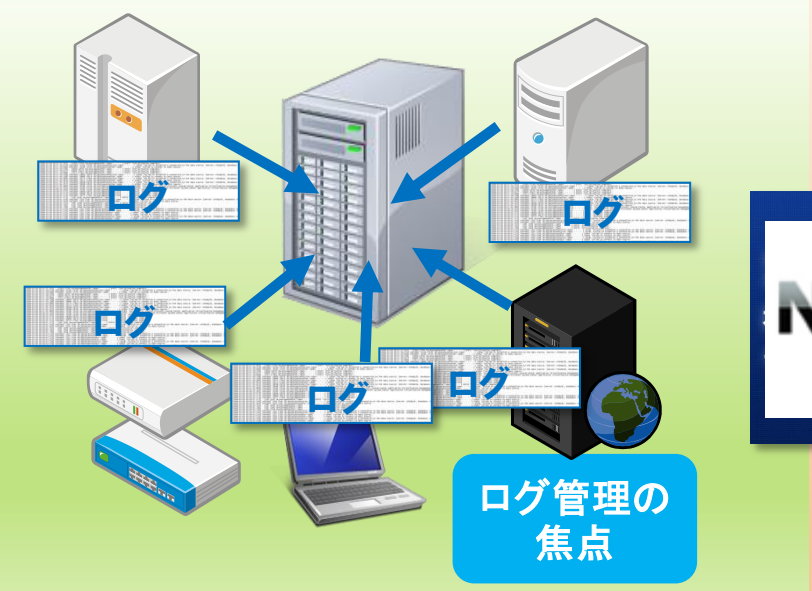
ログ収集
膨大なログ情報を可視化したり要約することで根本原因を追究する
フォレンジックの観点では非オリジナルデータ

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・通知だけなら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

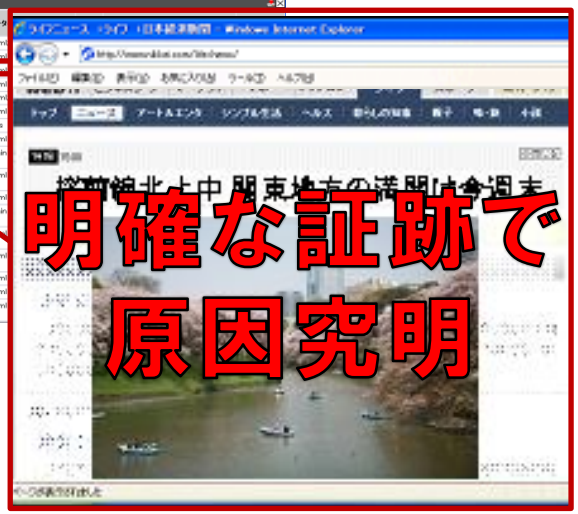
TOTEC AMENITY LIMITED

ログ管理とネットワークフォレンジック

NetRAPTOR

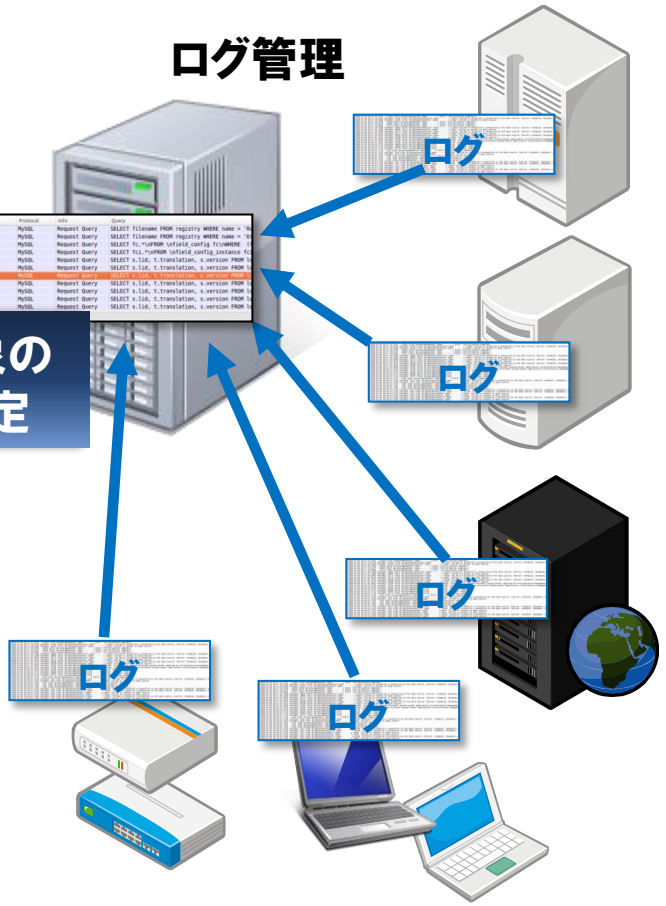
特定のログから実際のアクセス記録を取り出す

調査対象のログを特定

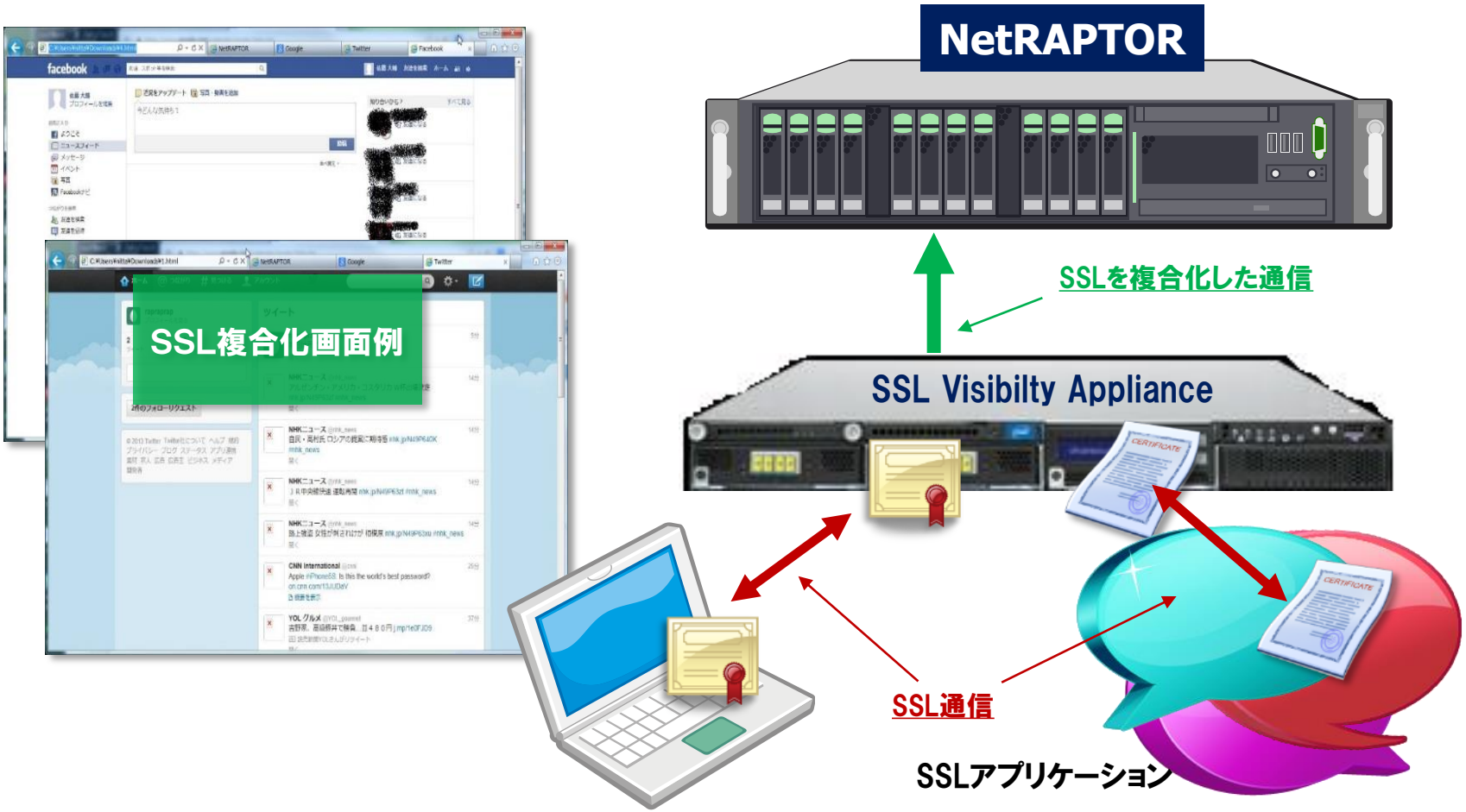


明確な証跡で原因究明

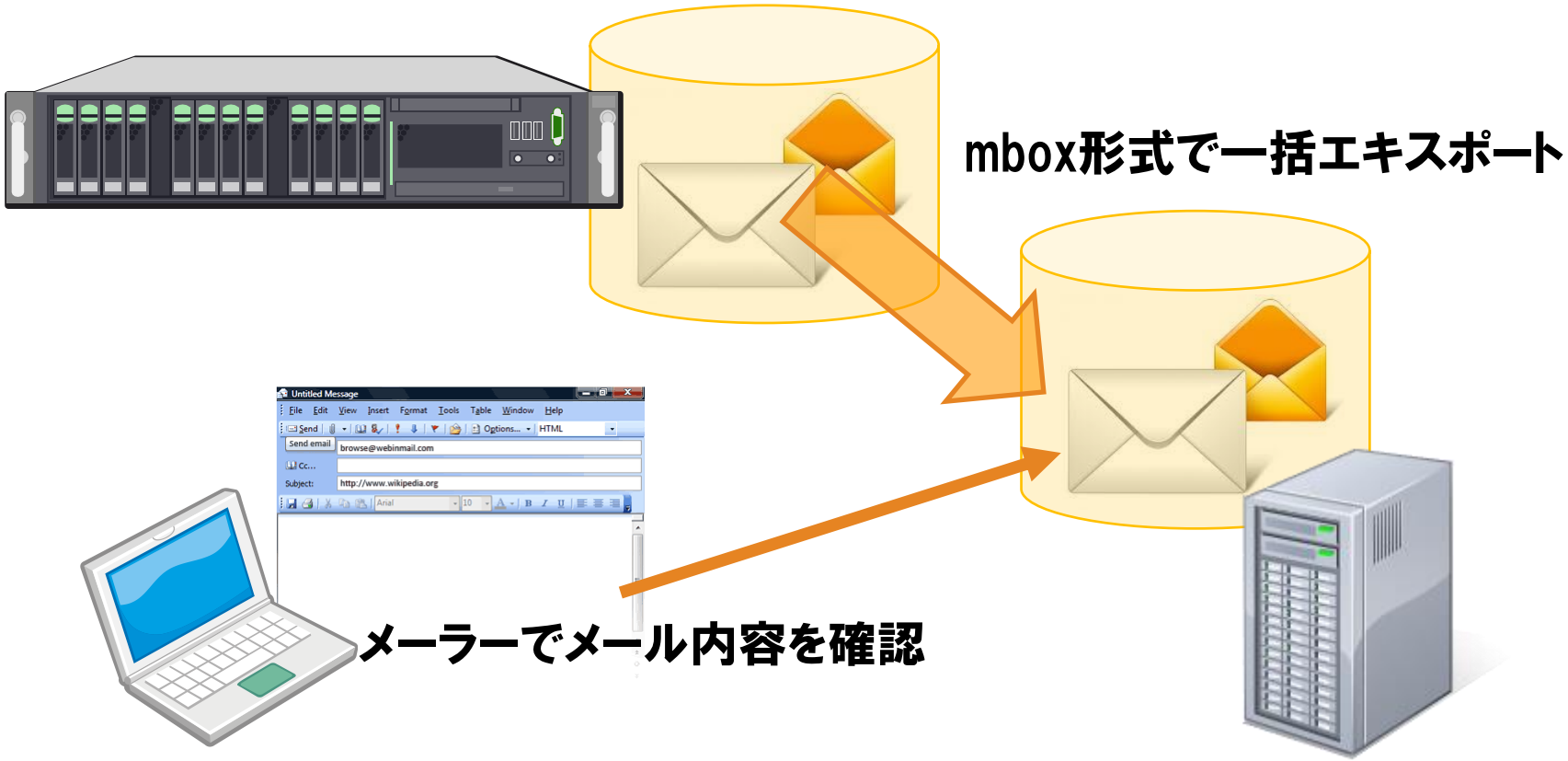
ログ管理



SSL通信の解析・再現



mbox形式一括エキスポート



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

MagiPass

二要素認証による不正アクセス防止

TOTEC AMENITY LIMITED

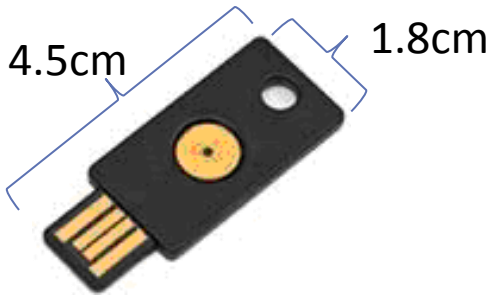
MagiPassとは

- 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

MagiPass

Virtual Appliance

© VMware, Inc.



TOTEC AMENITY LIMITED

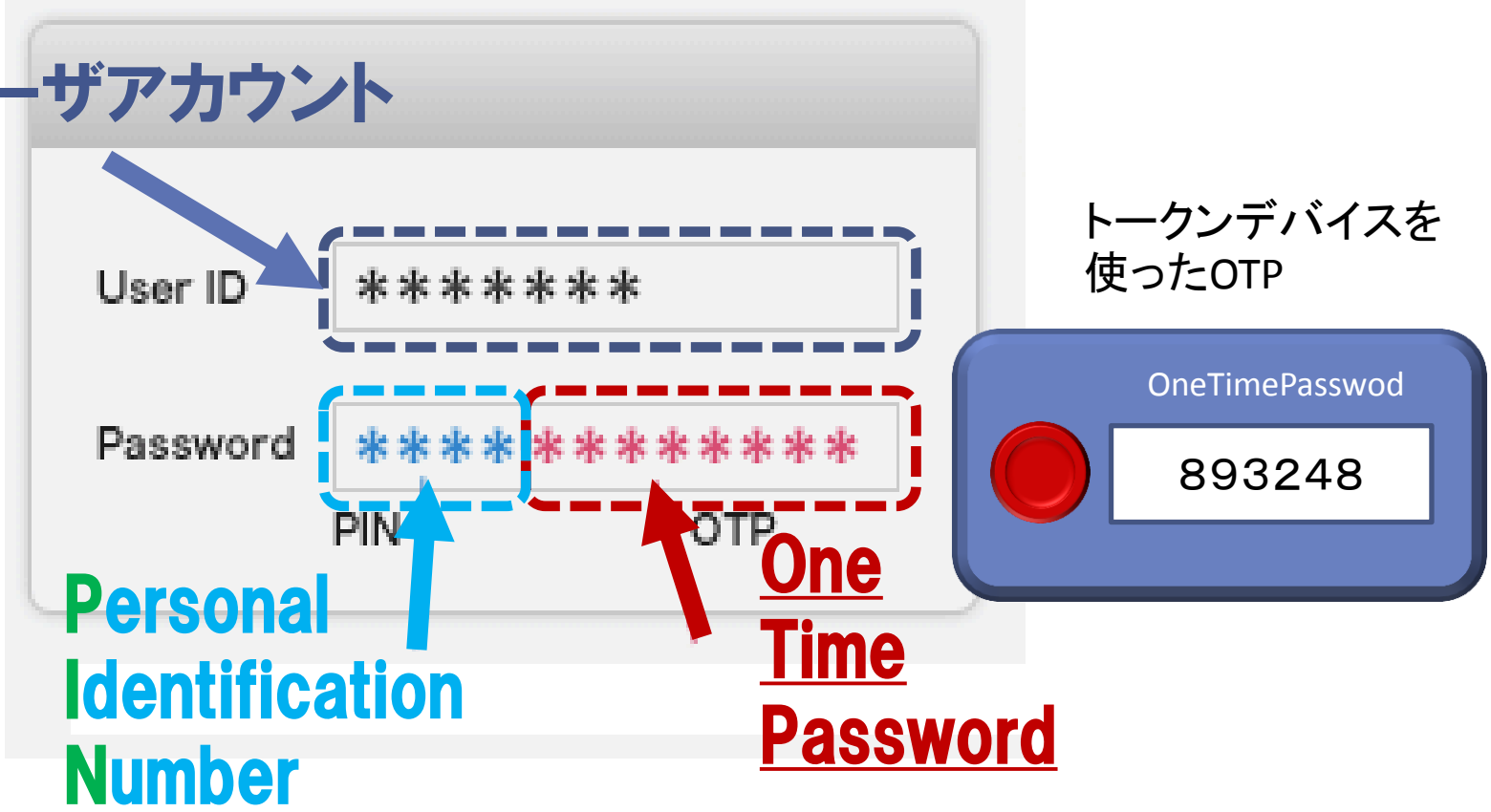
二要素(二因子)認証

- 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



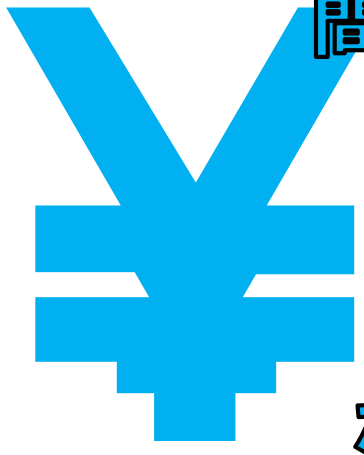
従来のトークンの課題

時刻同期式：手入力

従来のトークンの課題

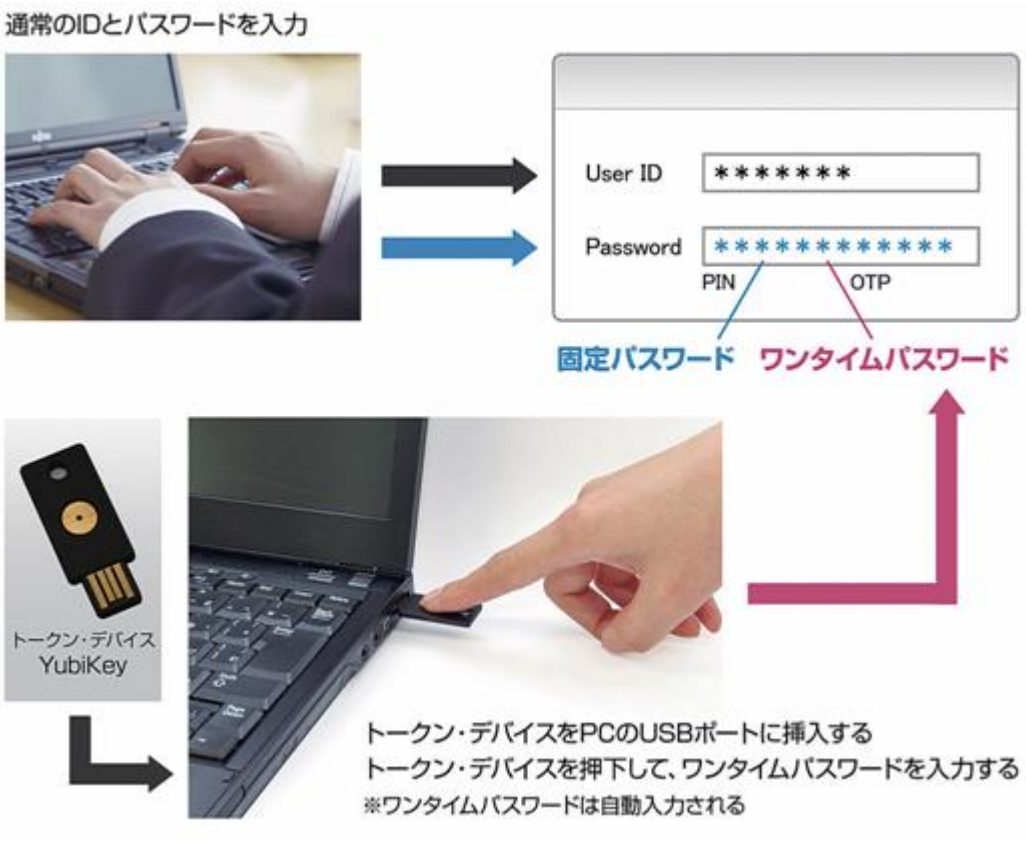
高い入力の負荷
電池交換が必要
運用コスト増
高額な管理ソフトウェア
生成アルゴリズム漏えいの危険性

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)



1) パソコンのUSB ポートにトークン・デバイスを挿入する

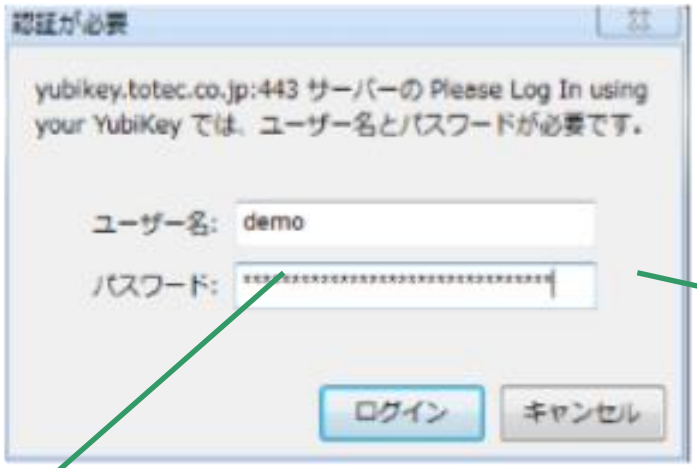
2) インターネット・バンキングのログイン画面にアクセスする

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

MagiPass ユニークな入力方式



Touch!

パスワード発行例

totec01blhfefetivgekkvrrvivgfhrjvehlggckikfe
totec01blhfefcihiehcuuucjfkhjibrdvrtgdrkfbrl
totec01blhfegjhcgjkhfrkbkkugkujrgvenjvvrngfv

PIN ＋ ワンタイムパスワード

TOTEC AMENITY LIMITED

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

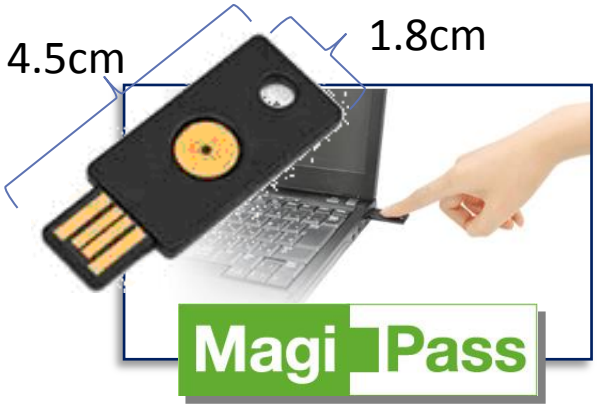
電池交換が必須

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)



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

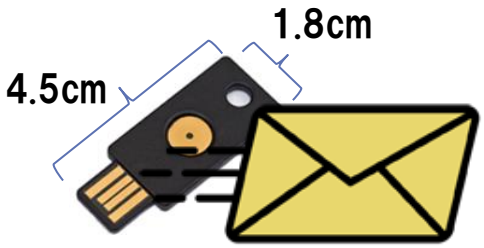
パスワード強度が強い

⇒ blhfefetivgekkvrrvivgfhrjvehlggckikfe

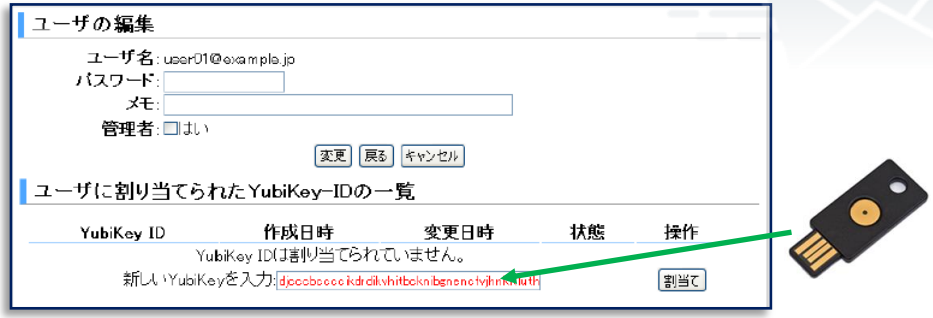
TOTEC AMENITY LIMITED

MagiPass 特長のまとめ

- 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
  - 入力は不要

（※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薦めします。

TOTEC AMENITY LIMITED

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	同時稼動は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	内部対策	出口対策
代表的な対策	代表的な対策	代表的な対策
次世代ファイアウォール	アンチウィルス	ネットワークフォレンジック
マルウェア検知システム（sandbox）	未知のマルウェア対策	Data Loss Prevention
IPS/IDS	エンドポイント管理/MDM	ボットネットアクセス監視
認証強化(二要素認証)	DB/ ファイル監視	次世代ファイアウォール
Web Application Firewall	ログ管理	メールセキュリティィ
Proxy ・・・ etc	SIEM ・・・ etc	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