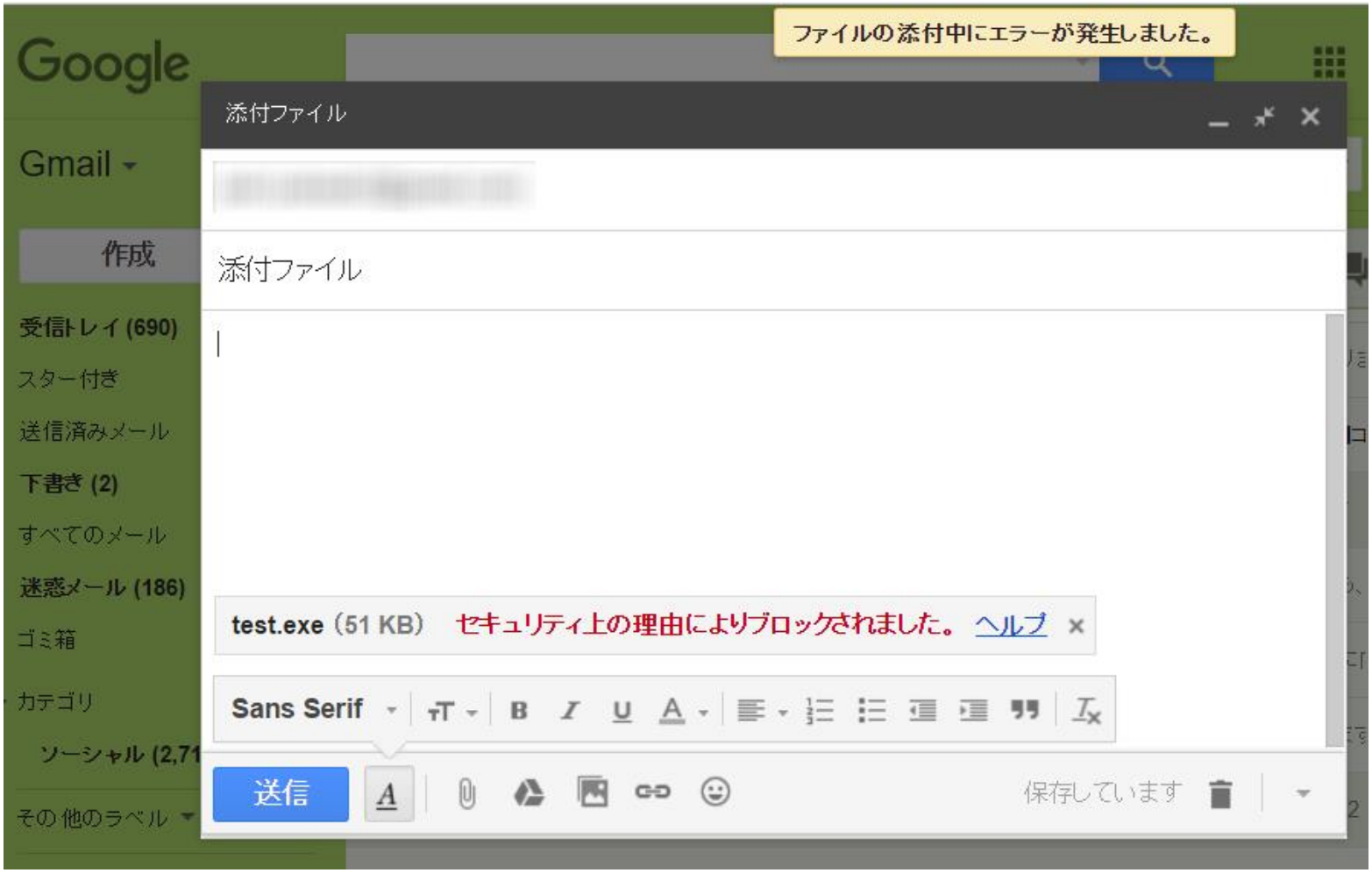

より使いやすくて安全なインターネット分離
コンテナ型仮想ブラウザ利用の提案

会社概要

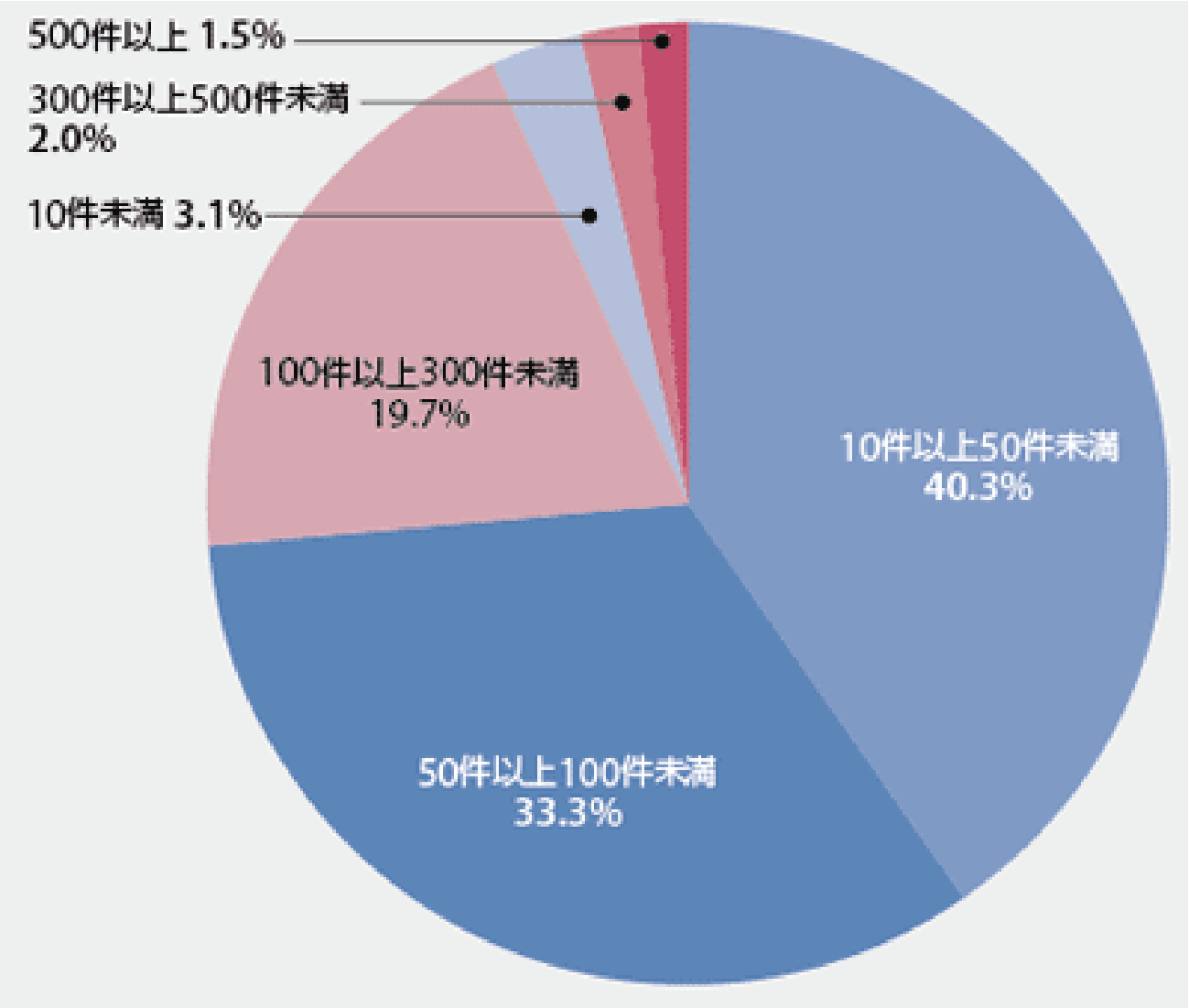
社名	株式会社ムービット
設立	1995年12月8日
所在地	東京都北区王子1－28－6
主な製品	Powered BLUE シリーズ アプライアンスサーバー（Linux） ソフトウエア開発

Gmail、JavaScriptファイルの添付を禁止へ（2月13日から）

Googleが、セキュリティ上の理由からGmailへの添付を禁じているファイルに、JavaScriptコード（.js）を追加する。2月13日から.jsファイルを添付しようとすると、警告が表示されるようになる。



メールの受信件数



出典　インプレスビジネスヘッドライン

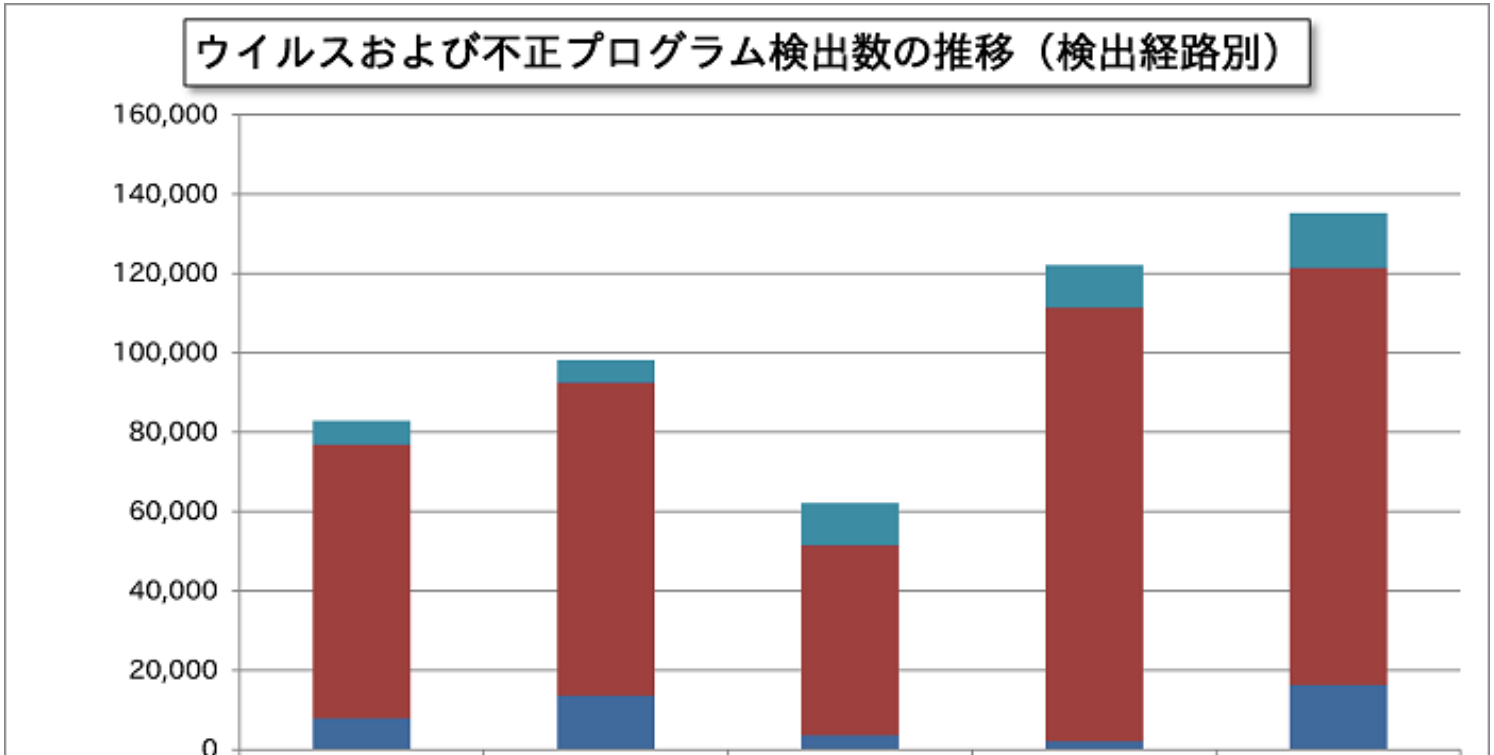
ウイルス感染の経路

１） メール　添付経由

２） Web閲覧　経由

３） USBなどのデバイス　経由

ウイルス感染の経路



	2015/ 1～3	2015/ 4～6	2015/ 7～9	2015/ 10～12	2016/ 1～3
不明・その他	5,963	5,603	10,646	10,658	13,839
ネットワーク	109	154	112	105	79
外部記憶媒体	0	4	0	1	1
ﾀﾞｳﾝﾛｰﾄﾞﾌｧｲﾙ	68,933	78,806	47,763	109,241	105,006
メール	7,855	13,599	3,661	2,094	16,293
合計	82,860	98,166	62,182	122,099	135,218

「ダウンロードファイル」の割合が最も多く全体の約77.7%を占め、次いで「メール」が、全体の約12.1%でした

出典　IPA / 2016

標的型メール

組織	特定の人をターゲットにしたメール
内容	業務に即した「本物らしい」内容
サンドボック回避	遅延発症やサンドボック内では、発症しない場合

標的型メール　例　JTB

・タイトル：航空券控え　添付のご連絡
・送信元：●●航空 aaaaaa@●●●.co.jp

・本文：

お世話になっております。
eチケットを送付しますのでご確認下さい。

●●航空　担当者名
・添付ファイル：E-TKT控え.pdf

送信元はJTBの取引先の航空関連会社
メールアドレスのドメイン（メールアドレスの@以下の部分）も
取引先の正式なもの。

佐川急便を名乗るウイルスメール （私宛に送付）

注文番号：941991-20170213-2130359265

只今ご注文殺到につきましてお客様へはお待たせして誠に申し訳ございませんでした。

本日、お客様のご注文商品を下記要領で発送いたしましたのでお知らせいたします。

[お届け運送会社]　佐川急便
[出荷日]　2017/02/13
[お届け予定日]　指定無し
[お問合せ番号]　035494428716

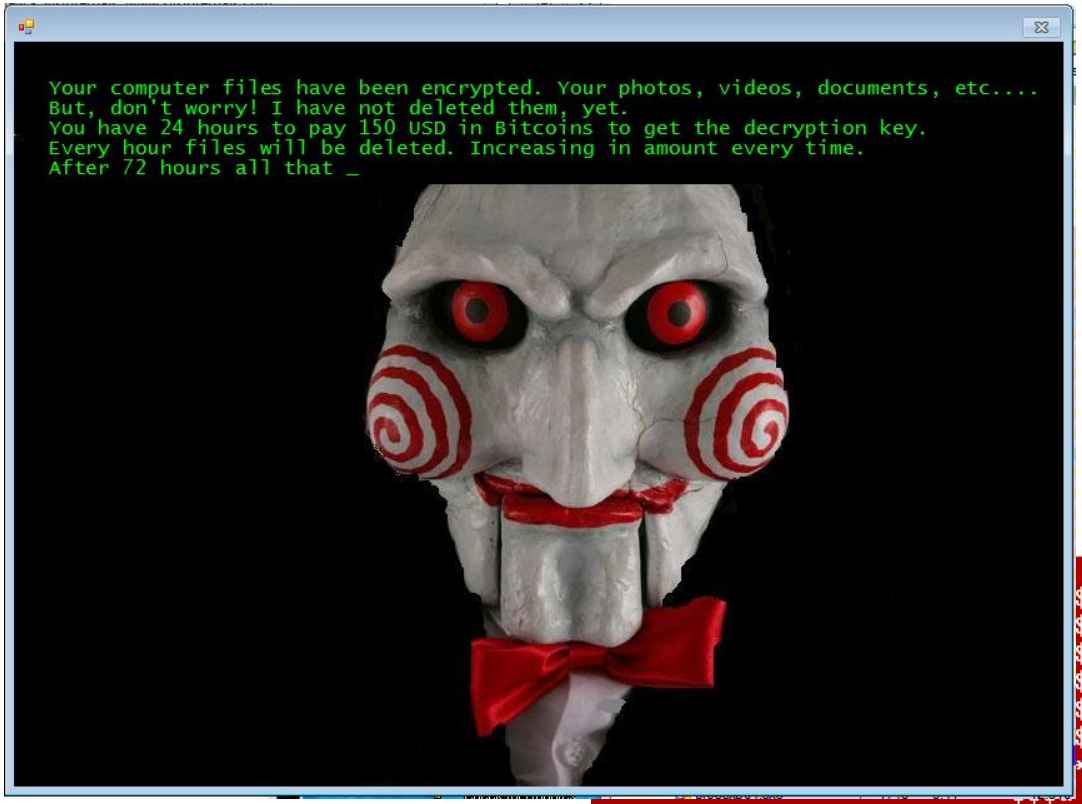
※反映は夕方以降となる場合がございます。予めご了承くださいませ。

★佐川急便利用時は委託倉庫先の**KIロジスティクスが発送元**になることがありま すので予めご了承くださいませ。

ランサムウエア

・ファイルを暗号化
・ファイルを削除
・ファイルを元に戻してほしいなら「お金を払え」

ランサムウエア

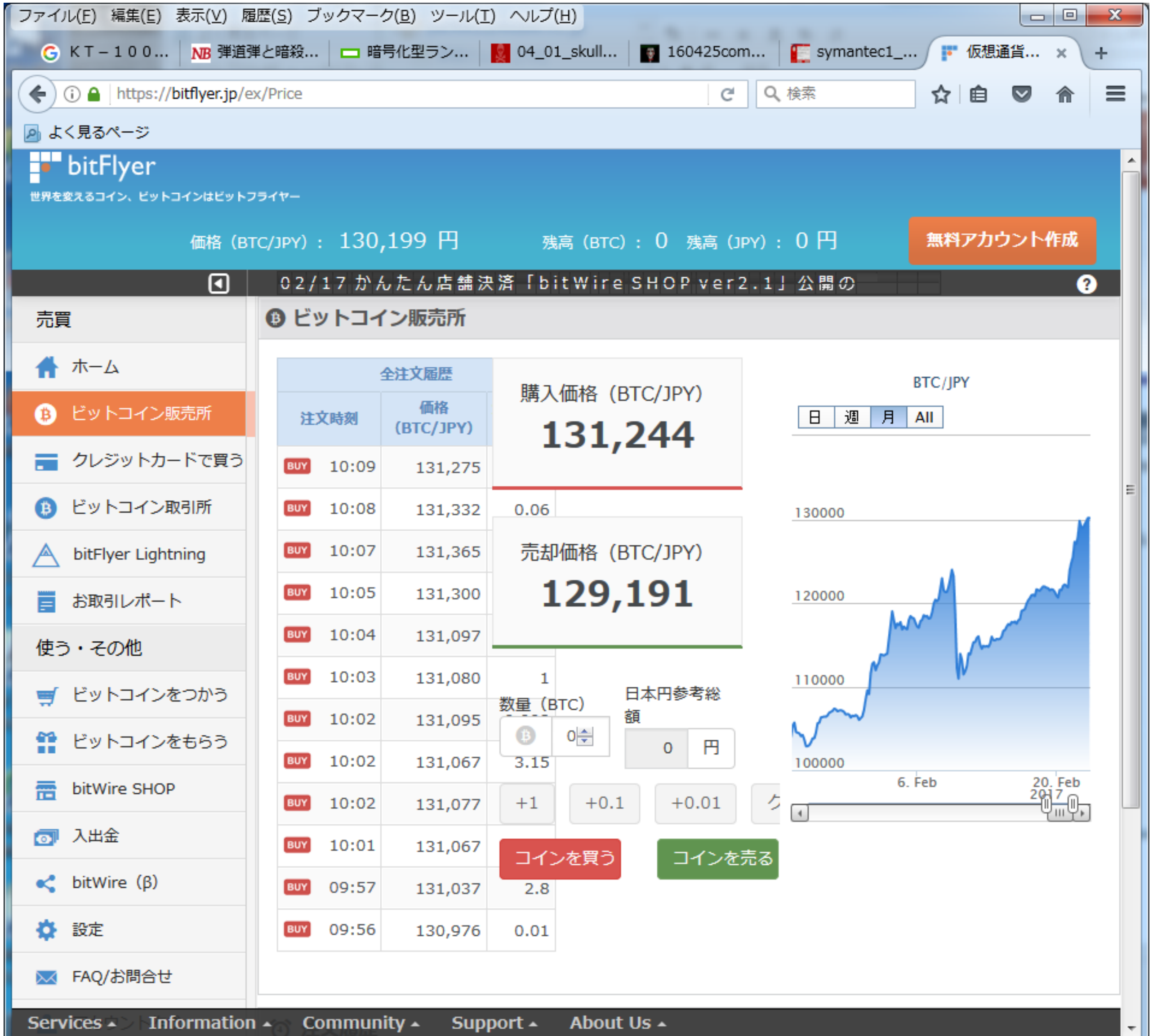

Your computer files have been encrypted. Your photos, videos, documents, etc....
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that _


PRESS ANY KEY!

支払いはビットコイン

出典　パルアルトネットワークス

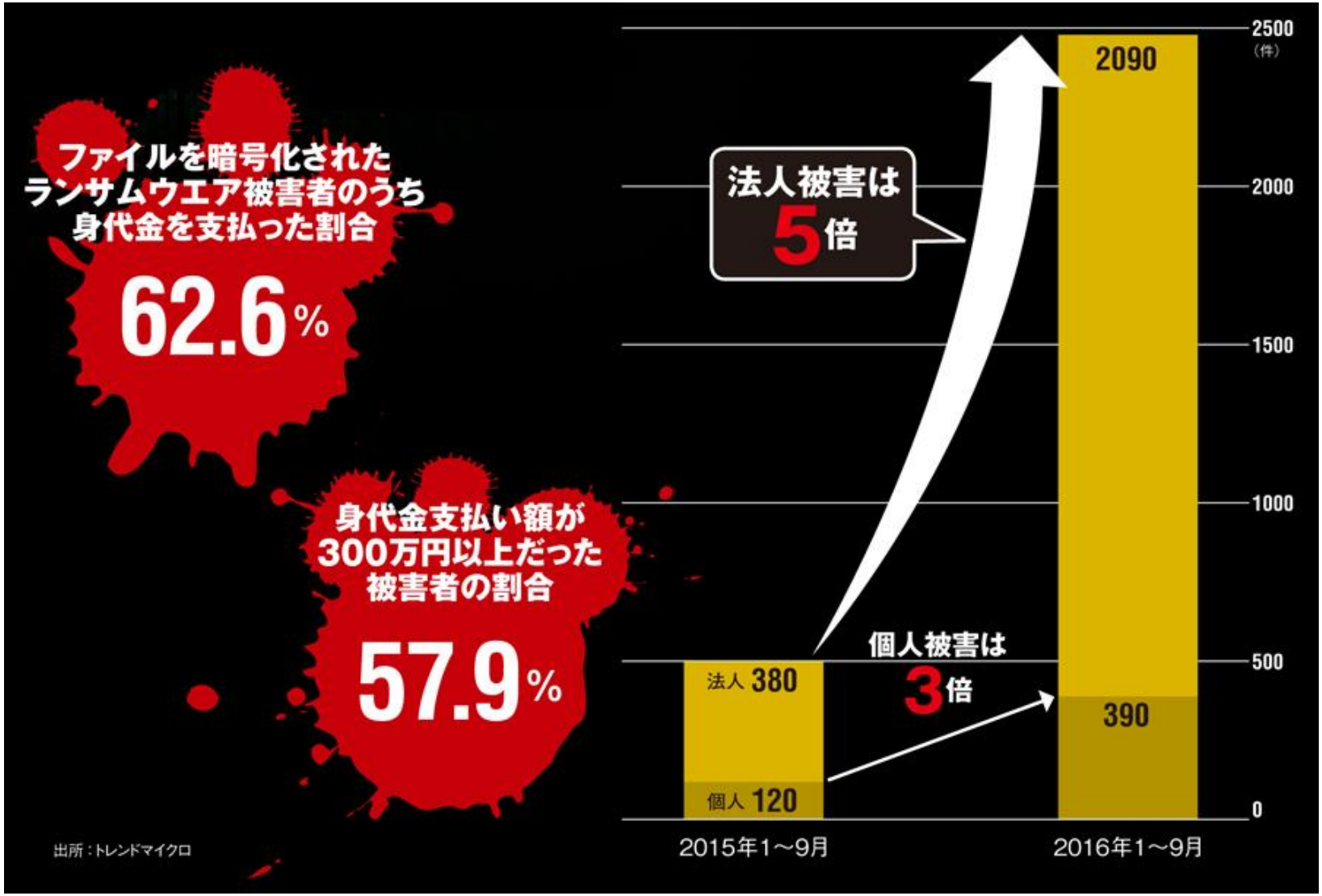
購入



ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)
https://bitflyer.jp/ex/Price
よく見るページ
bitFlyer
世界を変えるコイン、ビットコインはビットフライヤー
価格（BTC/JPY）： 130,199 円
残高（BTC）： 0 残高（JPY）： 0 円
無料アカウント作成
02/17 かんたん店舗決済「bitWire SHOP ver2.1」公開の
売買
ホーム
ビットコイン販売所
クレジットカードで買う
ビットコイン取引所
bitFlyer Lightning
お取引レポート
使う・その他
ビットコインをつかう
ビットコインをもらう
bitWire SHOP
入出金
bitWire（β）
設定
FAQ/お問合せ
ビットコイン販売所
全注文履歴
注文時刻
価格（BTC/JPY）
BUY 10:09 131,275
BUY 10:08 131,332 0.06
BUY 10:07 131,365
BUY 10:05 131,300
BUY 10:04 131,097
BUY 10:03 131,080 1
BUY 10:02 131,095
BUY 10:02 131,067 3.15
BUY 10:02 131,077
BUY 10:01 131,067
BUY 09:57 131,037 2.8
BUY 09:56 130,976 0.01
購入価格（BTC/JPY）
131,244
売却価格（BTC/JPY）
129,191
数量（BTC）
日本円参考総額
0 円
+1 +0.1 +0.01
コインを買う
コインを売る
BTC/JPY
日 週 月 All
130000
120000
110000
100000
6. Feb
20. Feb
2017
Services Information Community Support About Us

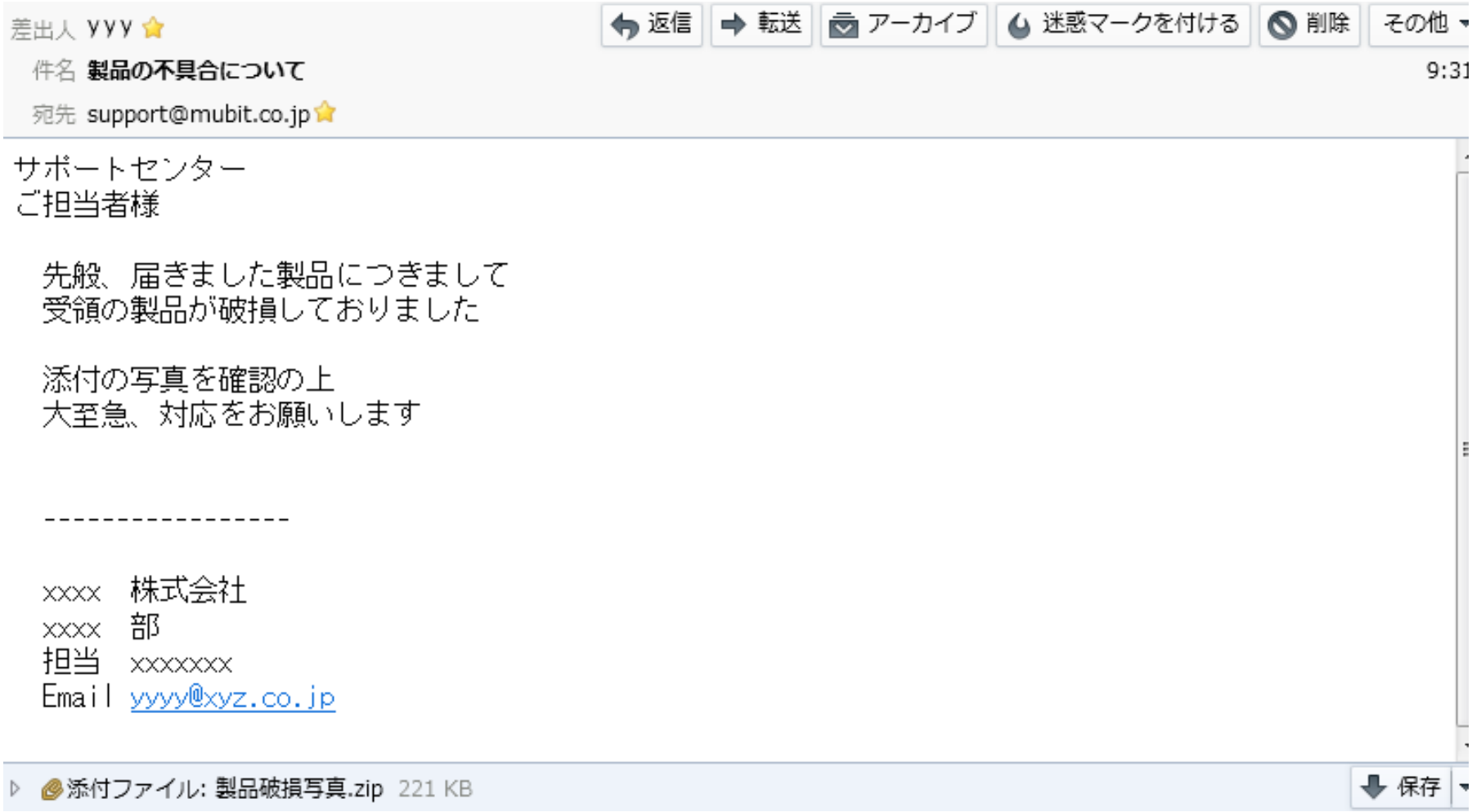
ットワークス

ランサムウエア被害件数



出典　トレンドマイクロ

開封する必要のあるメール


差出人 yyy
返信 転送 アーカイブ 迷惑マークを付ける 削除 その他
件名 製品の不具合について
9:31
宛先 support@mubit.co.jp

サポートセンター
ご担当者様

先般、届きました製品につきまして
受領の製品が破損しておりました

添付の写真を確認の上
大至急、対応をお願いします

---

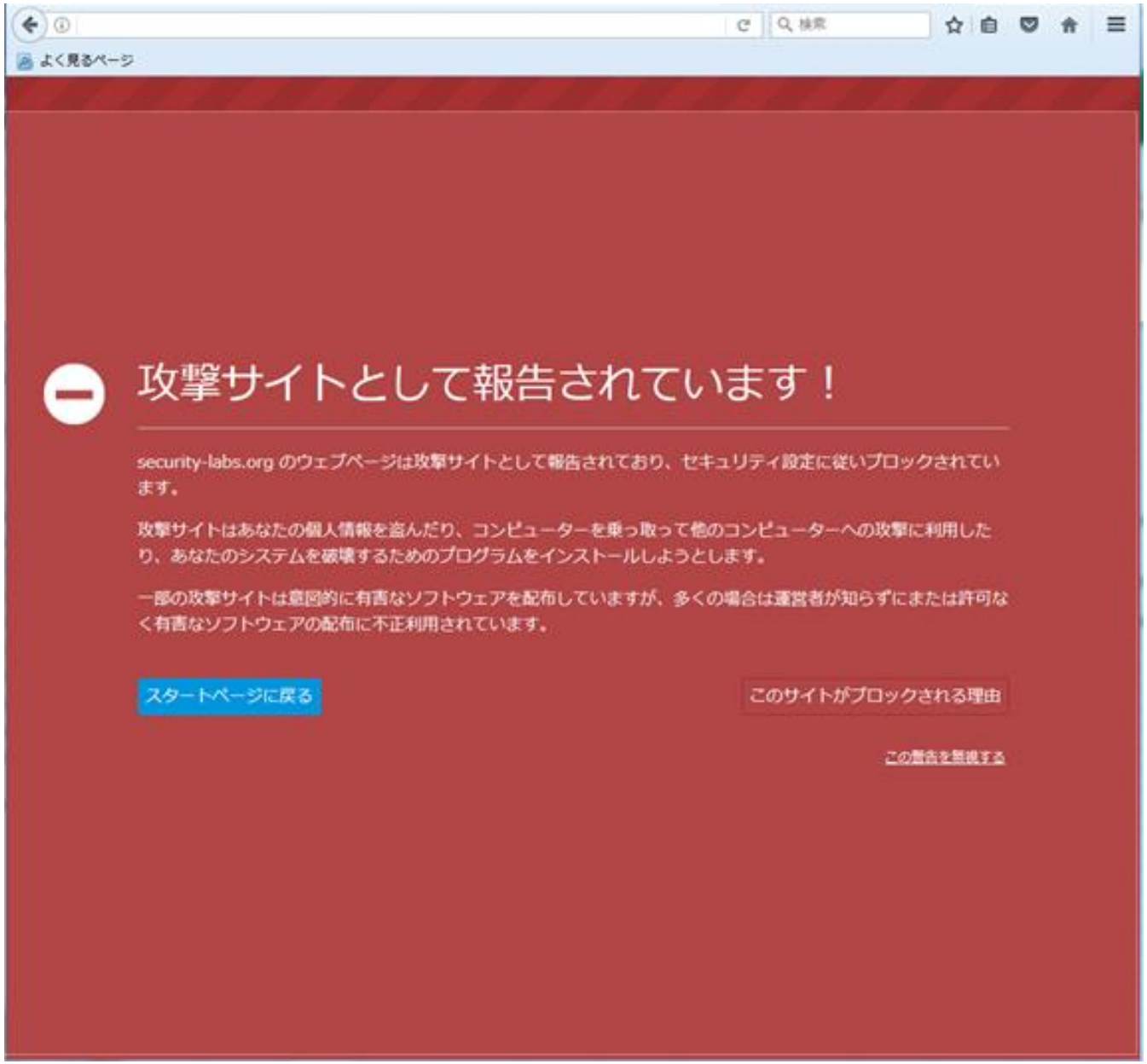
xxxx　株式会社
xxxx　部
担当　xxxxxxx
Email yyyy@xyz.co.jp

添付ファイル: 製品破損写真.zip 221 KB
保存

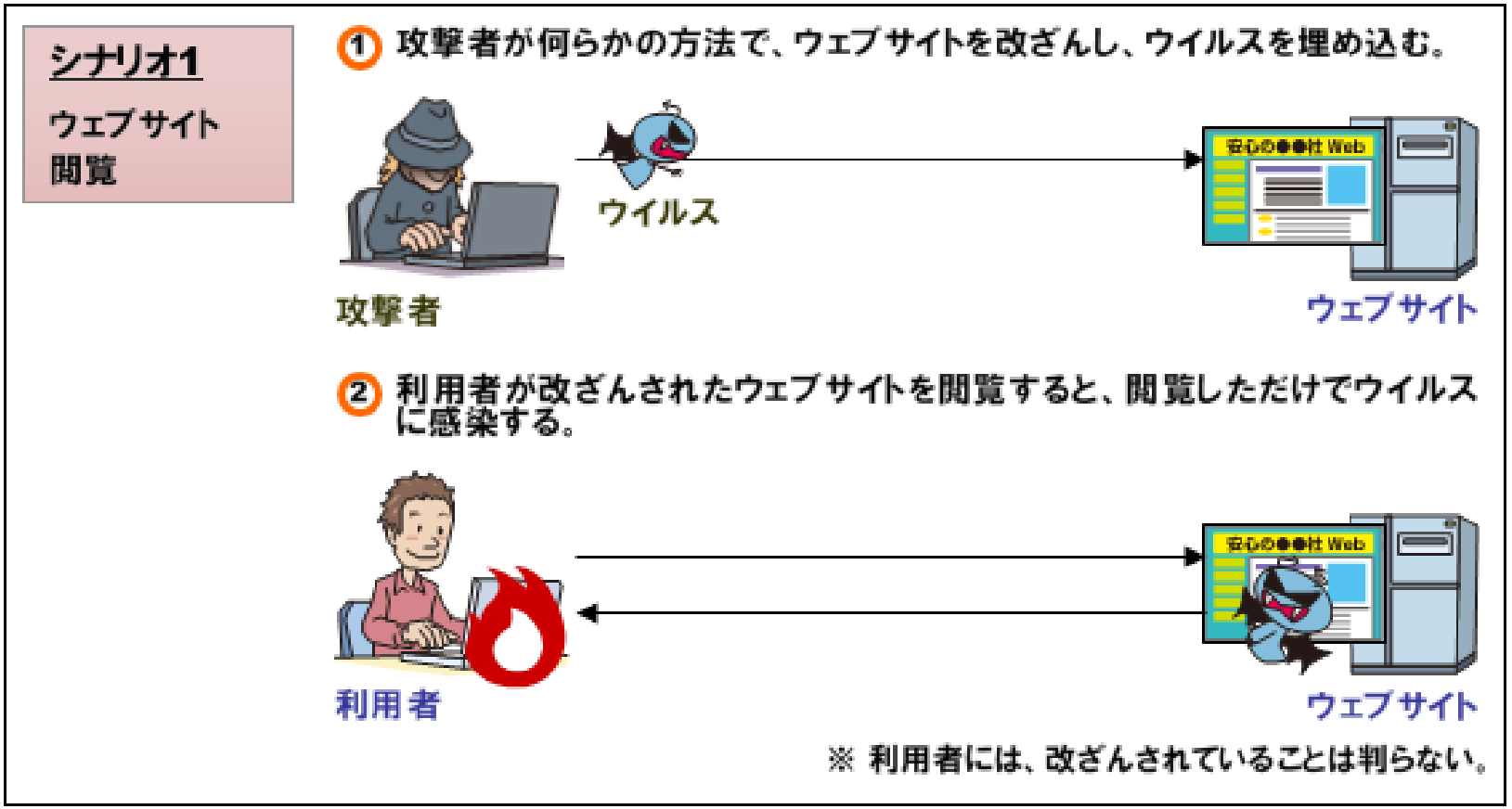
警告サイト


ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)
ウイルスバスター クラウドか...
よく見るページ
ウイルスバスター クラウドからのお知らせ
このWebサイトは、安全ではない可能性があります。
http://www.reconstructer.org/code/OfficeMalScanner.zip
このWebサイトは、安全ではない可能性があります。
この画面を閉じてください。
判定内容をご確認のうえでアクセスを希望されますか? ※アクセス先の安全性について判断できない場合は、アクセスをお控えください。
TREND MICRO
Copyright © 2015 Trend Micro Incorporated. All rights reserved.
OfficeMalScanner
すべて強調表示(A)
大文字/小文字を区別(C)
完全一致(W)
5 件中 1 件目

攻撃サイト


よく見るページ
攻撃サイトとして報告されています！
security-labs.org のウェブページは攻撃サイトとして報告されており、セキュリティ設定に従いブロックされています。
攻撃サイトはあなたの個人情報を盗んだり、コンピューターを乗っ取って他のコンピューターへの攻撃に利用したり、あなたのシステムを破壊するためのプログラムをインストールしようとします。
一部の攻撃サイトは意図的に有害なソフトウェアを配布していますが、多くの場合は運営者が知らずにまたは許可なく有害なソフトウェアの配布に不正利用されています。
スタートページに戻る
このサイトがブロックされる理由
この警告を無視する

Web アクセス&ダウンロードタイプ



「ダウンロードファイル」の割合が最も多く全体の約77.7%を占め、次いで「メール」が、全体の約12.1%でした

出典　IPA / 2016

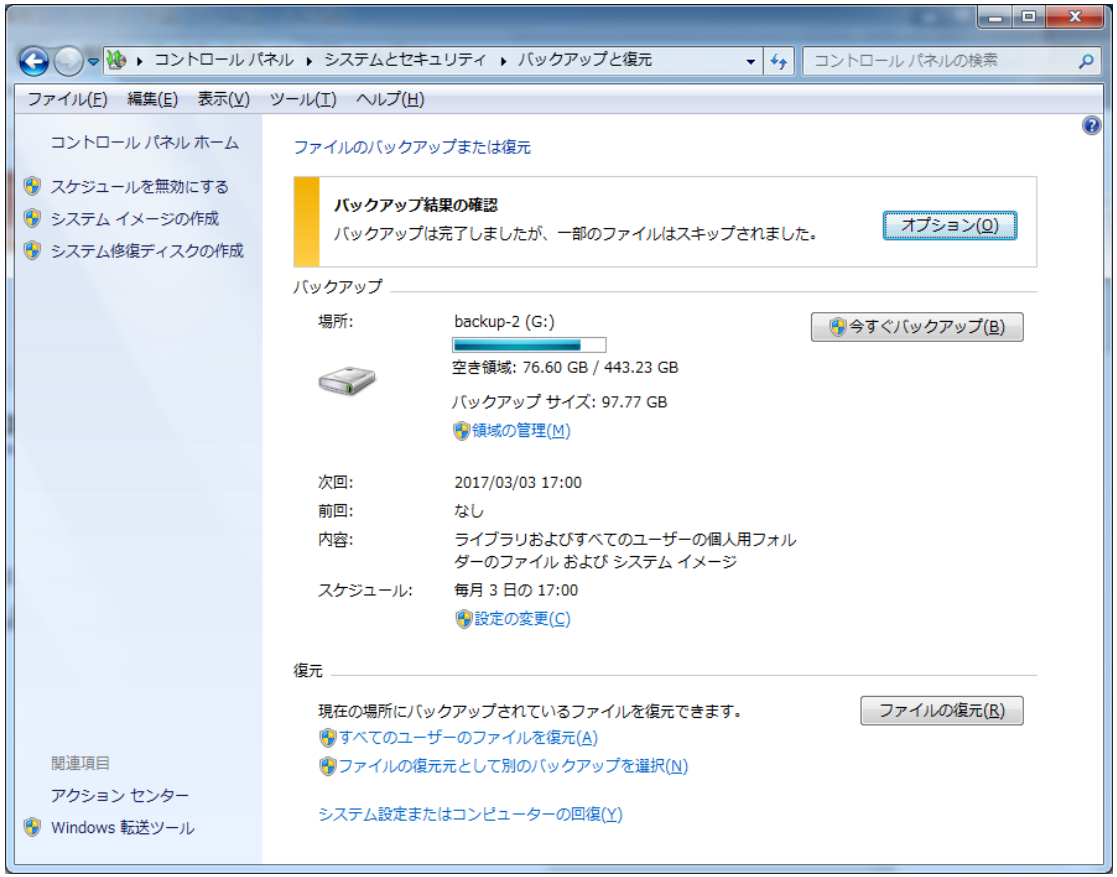
「怪しいファイルやURLのチェック」

「ランサムウエアの感染した場合」 の対処法

1） バックアップしてあるデータから戻す

「ランサムウエアの感染した場合」 の対処法

1）バックアップしてあるデータから戻す
　　遅延発症の場合もあるので、数世代のバックアップがベター

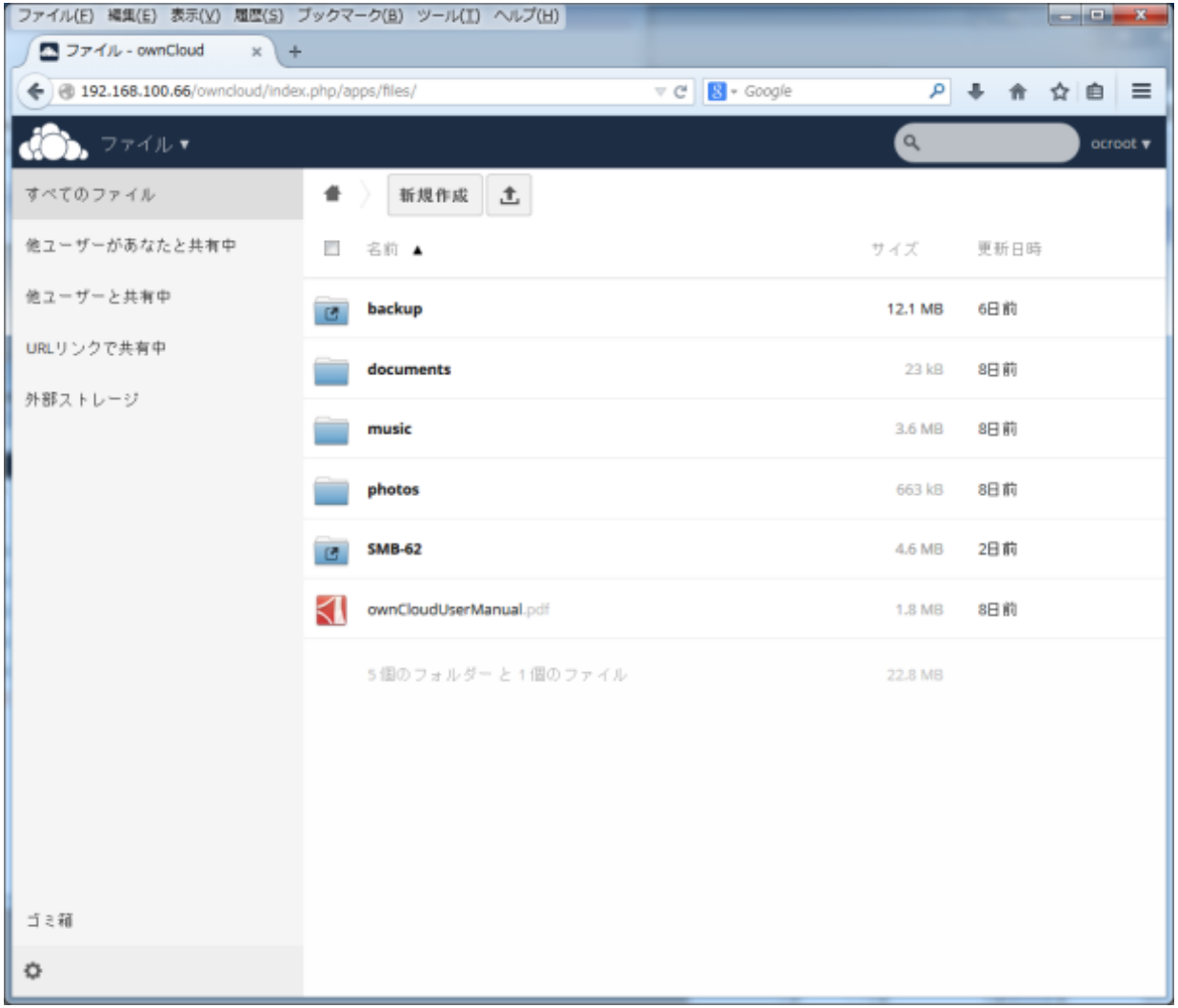


「バックアップ先」

1）USB-HDD

「バックアップ先　ownCloud」

「外部ストレージ連携　ownCloud」



Amazon S3 / DropBox / SMB / CIFS / WebDAV

「ランサムウエアの感染した場合」 の対処法

。

「ランサムウエアの感染した場合」 の対処法

3) 身代金の支払い

値引き交渉が可能な場合もあるらしい

「感染前」の対処法

・インターネット分離

「年金機構の流出」

・2015年５月

日本年金機構に対し外部から「標的型攻撃メール」が送付

年金管理システムに保管の125万人分の個人情報が漏洩

「総務省のガイドライン」

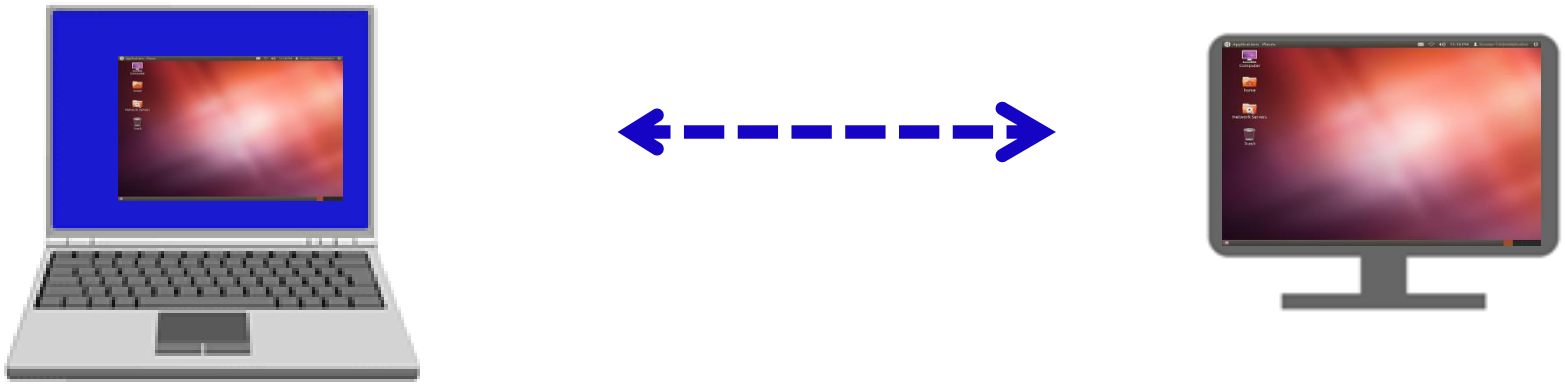
1) 無害化

LGWANへ持ち込むメールやファイルの無害化

2) ネットワークの分離

インターネット側のメール閲覧やWeb閲覧の通信経路を分離

仮想ブラウザによるネットワークの分離

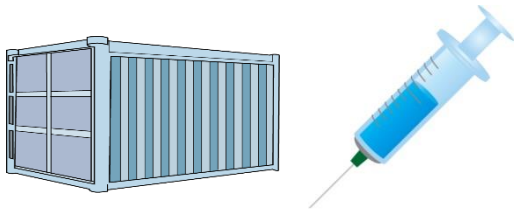


- **Linux の リモートデスクトップ を 利用**
- **仮想ブラウザで 画像のみ を自分の端末へ転送**

1コンテナ　/　1サーバー　/　1ユーザー

- コンピュータのワンルームマンション
- 隣のコンテナとは分離

コンテナは　使い捨て



- 新品
  毎回ユーザー毎に、新品サーバーを用意

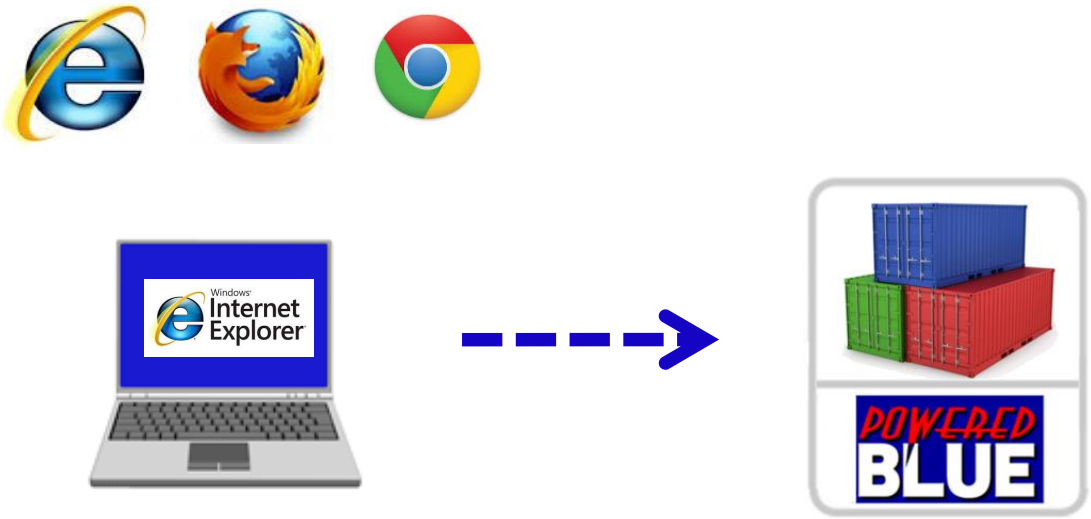
- サービスの終了
  コンテナは廃棄

Powered　BLUE　仮想ブラウザ

- 仮想アプライアンス（Linux）

利用手順-１

ブラウザで コンテナへアクセス

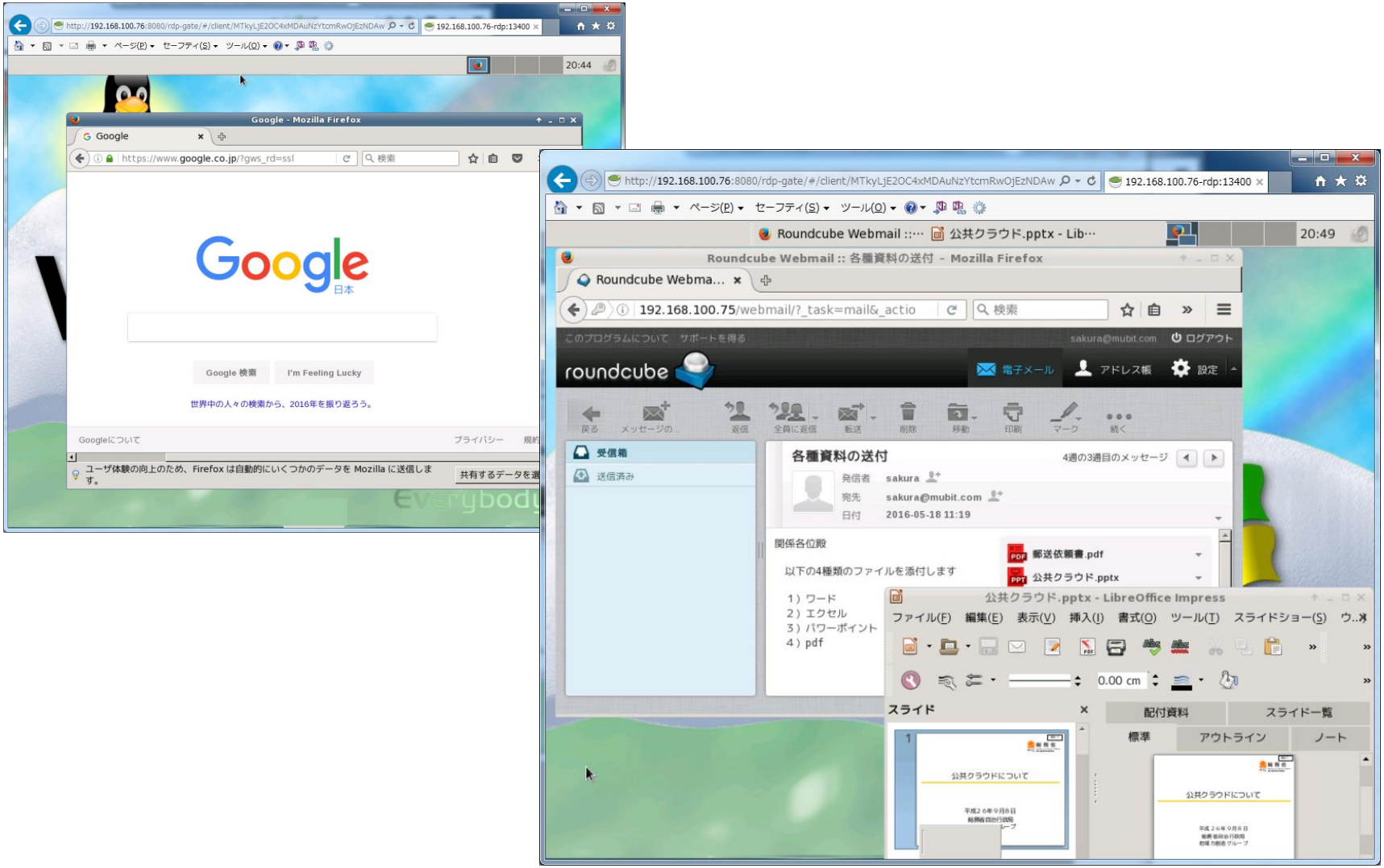


自分専用のコンテナが利用できる

コンテナ内の仮想ブラウザで作業

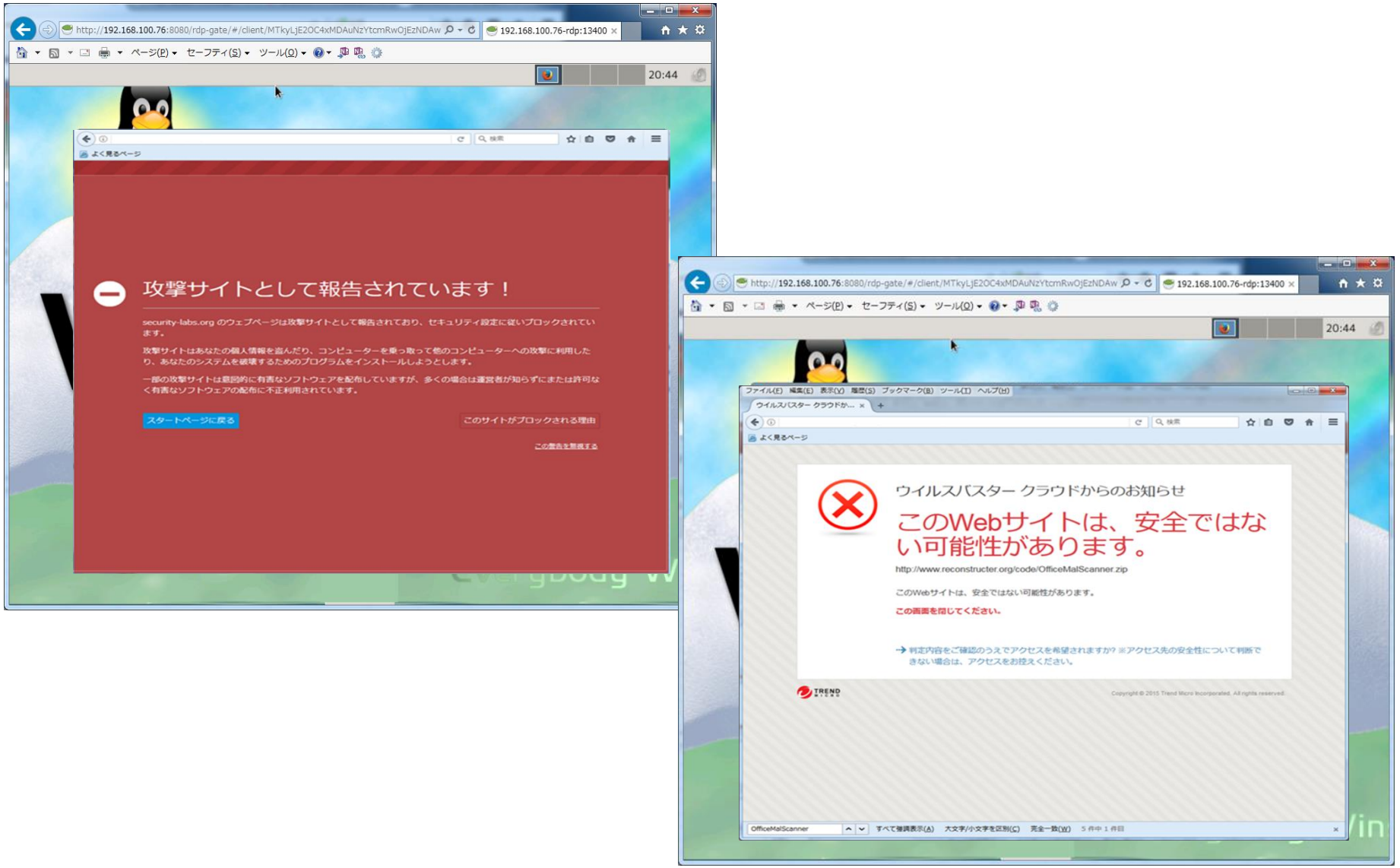
ネットサーフィン
Webメール閲覧

仮想ブラウザでのインターネット・アクセス



- ネットサーフィン　/　Web Mail 閲覧　/MS Office文書

仮想ブラウザでのインターネット・アクセス



- やばいサイトにもアクセスできます

ウイルス感染のファイルを取り込んだ場合

→ ローカルの　端末　には　影響なし

利用手順-6　フィニッシュ

■ 仮想ブラウザでの作業終了

→　　コンテナの廃棄

Powered BLUE 仮想ブラウザの特徴

- ユーザー端末側でのインストール不要
  → ブラウザでアクセスするだけ

- セキュアブラウザ
  → ユーザーの操作端末側にデータを残しません

- メールやファイルの操作
  → Web Mail による閲覧・編集・送受信
  → MS Office 編集・消毒（サニタイズ）も可能

オフィス関連のファイル

- word / excel / ppt

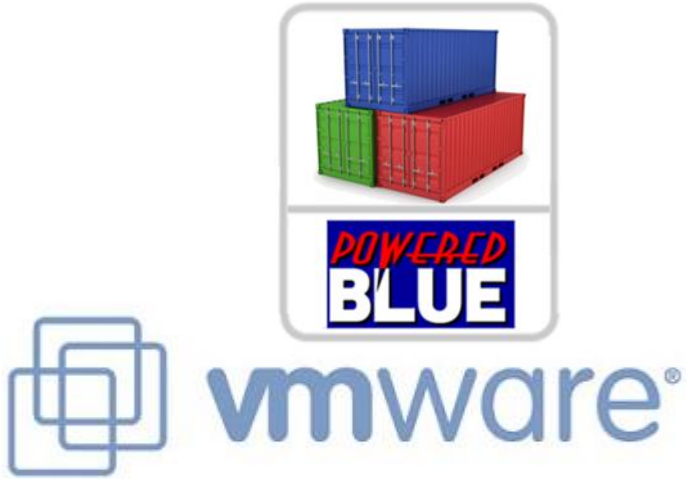
（リブレオフィス）

- pdf

- 圧縮解凍
  zip

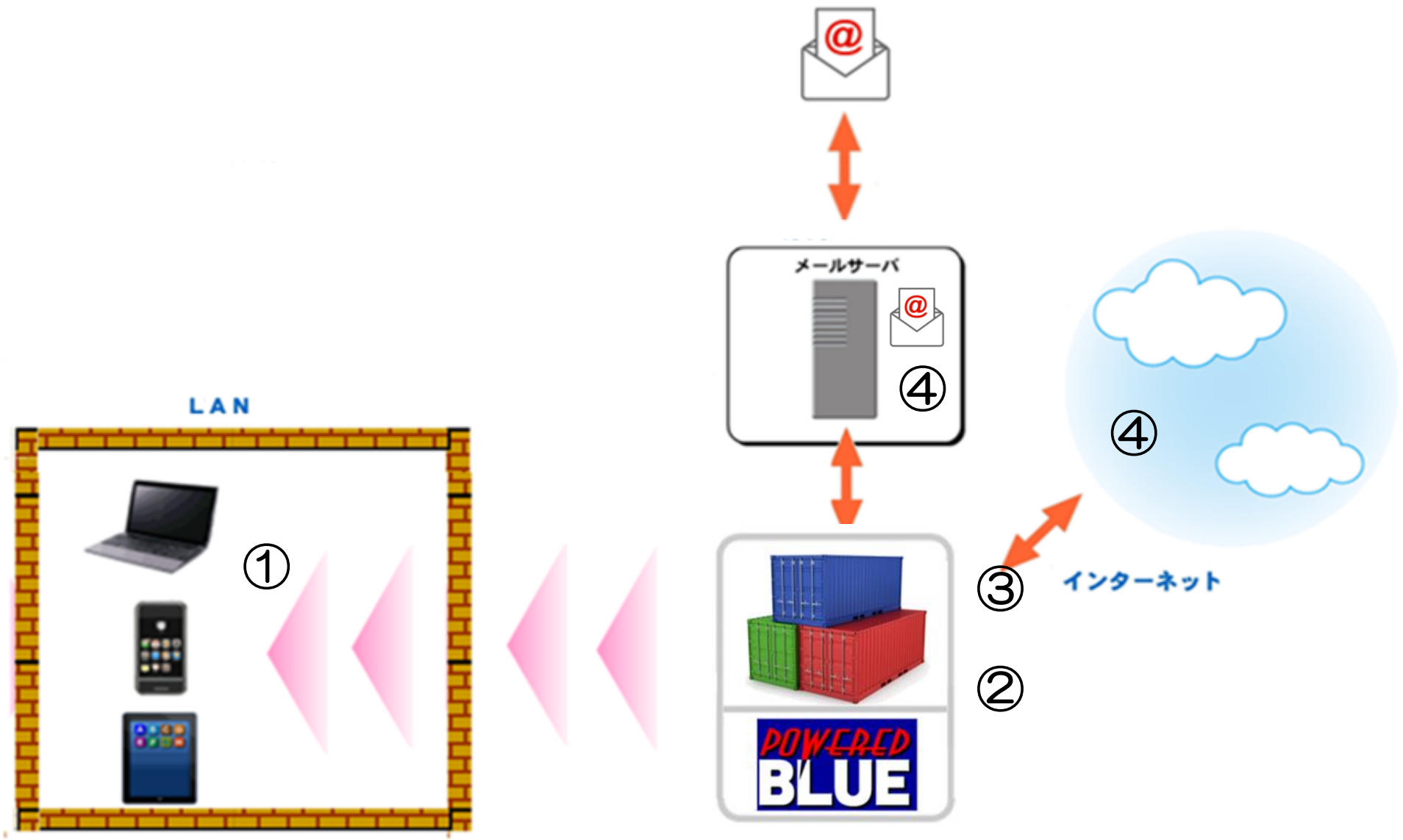
動作環境

- **VMware基盤**

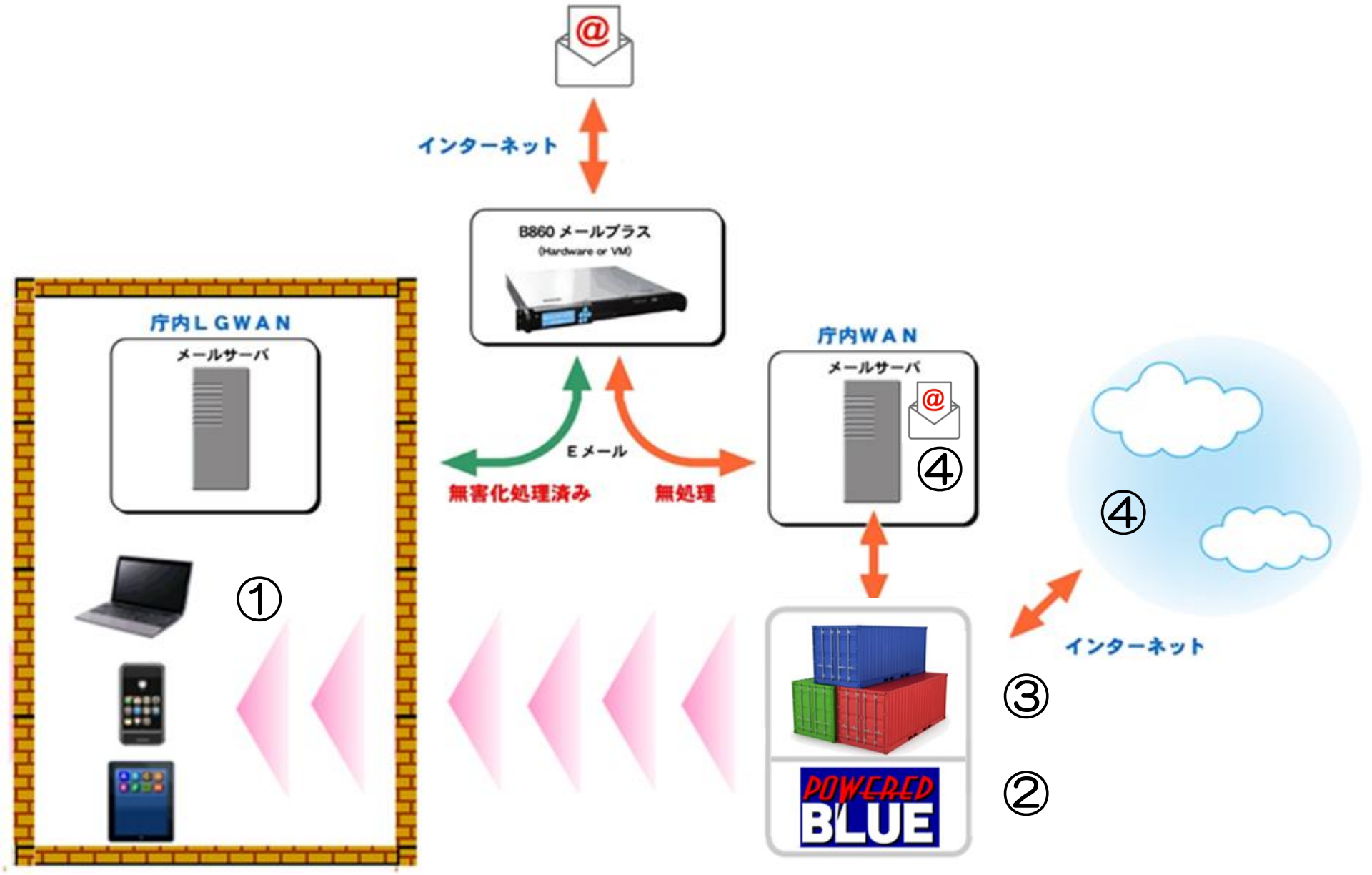


- **VMware ESXi 無償版でも動作**

インタネット分離　構成例　一般企業



インタネット分離　構成例　LGWAN



Powered BLUE 仮想ブラウザ　の　おさらい

- **専用ソフト不要**
  → ブラウザ のみ

- **仮想アプライアンス**
  → インポート するだけ

- **低価格**
  → Windowsの CAL 不要