ネットトラブルにあわないための置き薬

第4回

山西潤一：　yamanisi@yamalab2025.com

富山大学名誉教授、富山県青少年安心・安全ネット利用促進連絡会座長

佐藤宏隆：satou.hirotaka@flownexus.jp

有限会社詩季代表取締役、ITコンサルタント

セキュリティプレゼンター

不審な連絡にあったときの置き薬　困った時

1. 金融機関やショッピングサイトを騙る

- 銀行から身に覚えのない取引結果が届いた
- クレジットカード会社からサービス停止の案内が来た
- 宅配便の連絡が来たが、送り主などに覚えがない

不審な連絡にあったときの置き薬　困った時

2．儲かる、あたるなど甘い言葉で誘われる

- 顧客満足度調査がきた。答えるとボーナスがあたるらしい
- 仮想通貨ってものを買うと、儲かるらしい

3．ハッキングしたなどと危機感を煽られる

- 私のIDとパスワードがハッキングされた！？
- 突然「ウィルスに感染している」と表示が。

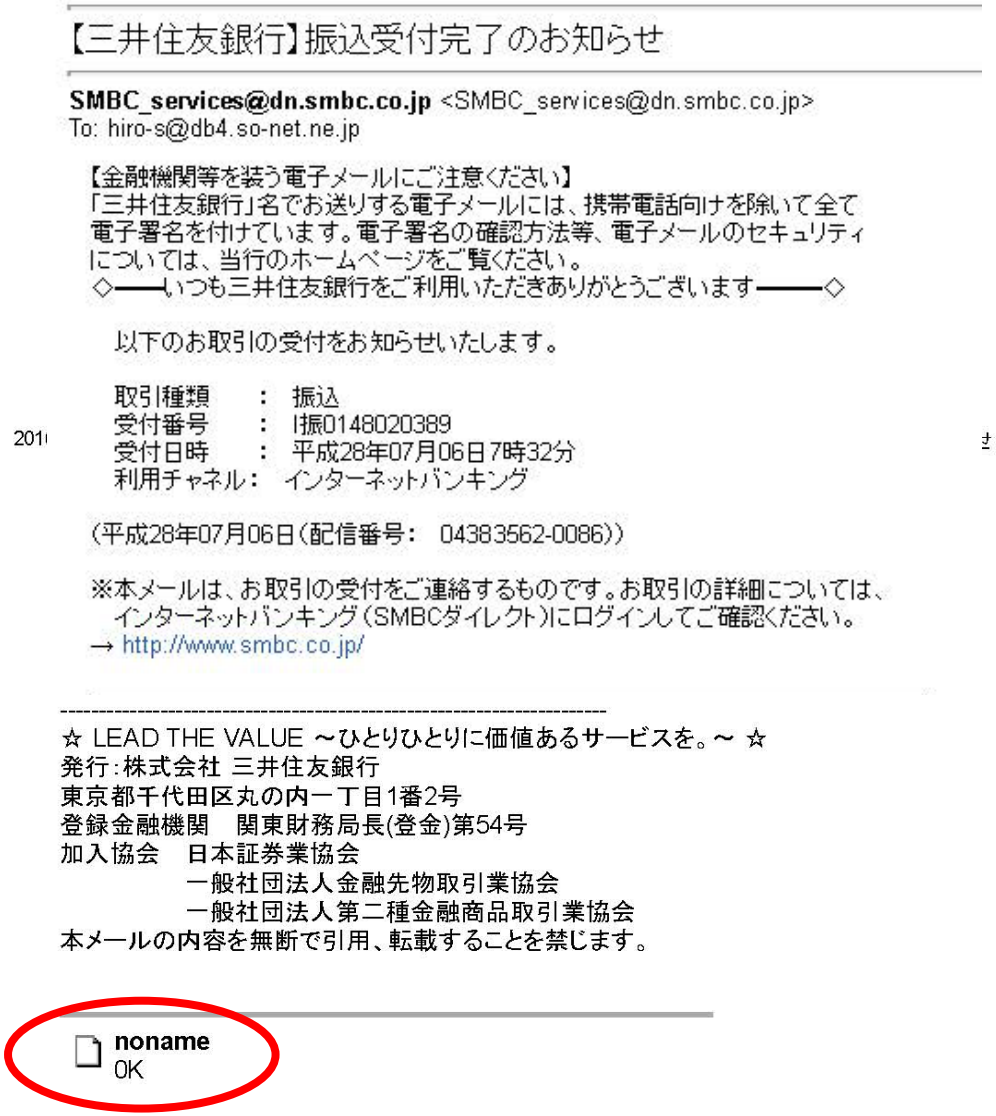
契約していない銀行から取引結果が届いた

トラブル事例：偽取引メール

・実際には取引は行われていない
・本文は本物をそのまま
・添付されている「ファイル」＝ウィルス

被害にあった場合は

・パソコンをネットから切断
・再度パソコンを使う場合は初期化



【三井住友銀行】振込受付完了のお知らせ

SMBC_services@dn.smbc.co.jp <SMBC_services@dn.smbc.co.jp>
To: hiro-s@db4.so-net.ne.jp

【金融機関等を装う電子メールにご注意ください】
「三井住友銀行」名でお送りする電子メールには、携帯電話向けを除いて全て電子署名を付けています。電子署名の確認方法等、電子メールのセキュリティについては、当行のホームページをご覧ください。
◇――いつも三井住友銀行をご利用いただきありがとうございます――◇

以下のお取引の受付をお知らせいたします。

取引種類　：　振込
受付番号　：　I振0148020389
受付日時　：　平成28年07月06日7時32分
利用チャネル：　インターネットバンキング

（平成28年07月06日（配信番号：　04383562-0086））

※本メールは、お取引の受付をご連絡するものです。お取引の詳細については、インターネットバンキング（SMBCダイレクト）にログインしてご確認ください。
→ http://www.smbc.co.jp/

☆ LEAD THE VALUE ～ひとりひとりに価値あるサービスを。～ ☆
発行：株式会社 三井住友銀行
東京都千代田区丸の内一丁目1番2号
登録金融機関　関東財務局長(登金)第54号
加入協会　日本証券業協会
一般社団法人金融先物取引業協会
一般社団法人第二種金融商品取引業協会
本メールの内容を無断で引用、転載することを禁じます。

noname
OK

クレジットカード会社からサービス停止のお知らせが来た

トラブル事例：通常連絡を装った詐欺メール

・クレジットカード会社等からメンテナンス等の案内がくる
・確認用のボタンが用意されており、アクセスすると個人情報を要求

突然、SMSに荷物の不在連絡がきた

トラブル事例：宅配業者を装った詐欺SMS

・佐川急便など宅配業者から不在の連絡がくる
・連絡に書かれているアドレスにアクセスすると被害にあう
　１）不正なスマホアプリのインストール
　２）ID、パスワードの漏洩

パソコンやAndroidスマホでアクセスした場合

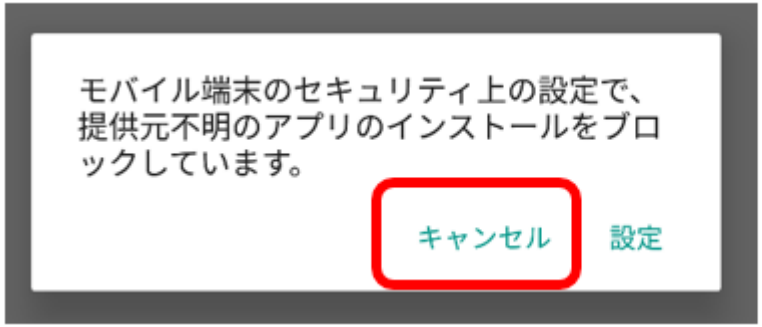
偽佐川アプリをインストールさせようとする
⇒スマホからデータを盗む

iPhoneやiPadでアクセスした場合

Andoridスマホで気をつけるべきこと

1. 提供元不明のアプリをインストールしない

・Androidスマホは公式（GooglePlay）以外からもアプリを入れられる
　⇒不正なアプリは**この仕組みを悪用**する
・標準では、公式以外からアプリを入れようとすると警告がでる
　⇒キャンセルをタップすることで不正なアプリが入ることを防ぐ



・設定を変更させようとする場合は要注意
　⇒公式に載せられない（審査を通らない）アプリ

顧客満足度調査がきた。答えると10000円があたるらしい

トラブル事例：満足度調査を騙ったメール

・調査に答えると10000円があたると言われる
・実際には現金はもらえず、個人情報が漏洩する

お客様から収集される情報は、Amazon.co.jp でのお買い物をお客様に合ったよりよいものにし、Amazon.com, Inc. および／またはその関連会社（以下総称して「Amazon」といいます）が提供する店舗、プラットフォーム、情報検索等のサービスをお客様にご利用いただくために役立てられます。

■ 通常、どのくらいの頻度で当サービスをを利用していますか？
- ○ いつも利用している
- ○ 大抵利用している
- ○ たびたび利用している
- ○ たまに利用している
- ○ 一度も利用したことない

■ 他社の提供する同様のサービスと比べた場合、当サービスの質はどの程度優れていると感じますか？
- ○ 極めて優れている
- ○ 結構優れている
- ○ 多少優れている
- ○ どちらでもない　同じぐらい
- ○ 多少劣っている
- ○ 結構劣っている
- ○ 極めて劣っている

■ 当サービスを他の方にご紹介いただける可能性はどのくらいありますか？
- ○ 確実にある
- ○ 可能性が高い
- ○ 可能性がある
- ○ 可能性が低い
- ○ 全く可能性はない

■ 当社の提供する別のサービスにどの程度ご興味がありますか？
- ○ 可極めて興味がある
- ○ 結構興味がある

- 結構興味がある
- ある程度興味がある
- 多少興味がある
- 全く興味がない

あなたの報酬：

に送る：

カード番号

月（00）

年（0000）

セキュリティコード

仮想通貨ってものを買うと、儲かるらしい

トラブル事例：LINE等で投資を勧誘される

・仮想通貨（暗号資産）などを対象にしたもうけ話
・勧誘方法がLINEやFacebookなどSNSを使ったものに

朝日新聞　H30.6.3　朝日新聞

仮想通貨 もうけ話のワナ

LINEで勧誘 消えた100万円

仮想通貨をめぐる投資トラブルが後を絶たない。違法性が疑われるケースもあり、訴訟や捜査の動きも出てきた。金融庁などの関係機関も、監視を強めている。（岡野翔）

「出資は最低1BTC（ビットコイン）から。100倍まで上げるので参加しませんか」

神戸市の40代男性は昨夏、メッセージアプリ「LINE」で仮想通貨情報を配信する自称「投資家」から、もうけ話を持ちかけられた。

募ったビットコインを原資にして、知名度が低く取引量が少ない仮想通貨銘柄を大量に買い付け、価格をつり上げた段階で一挙に売り抜ける仕手戦を試み、売却益を出資者に分配する――。そんな計画だった。

投資家は業界情報に詳しいと評判で、SNS上で「師」と仰がれていた。男性は面識がなかったが信頼できると感じ、指定のアドレスに2BTC（当時約100万円相当）を送った。

ところが1カ月後、投資家は「想定外の事態が起きてマイナスになった」と計画の失敗をLINEで釈明。その後、連絡が途絶えた。男性は「自己責任だが、元本は返してほしい」と警察に被害を相談した。

金融庁によると、こうした投資家の行為は改正資金決済法に抵触する可能性があるという。同法では、仮想通貨の売買や交換、それらの媒介や代理の業務には国への登録が必要とされ、実質的に認められているのは交換業者16社と登録申請中の「みなし業者」だけだ。

「市場に革命を起こす」「最後のチャンス」――。昨年、代表格のビットコインが高騰したのを引き合いに、ネットやSNSでは様々な銘柄の仮想通貨に絡んだもうけ話が紹介され、投機心をあおる情報や広告も拡散している。金融庁の担当者は「不特定者に対し継続的に事業を行っている実態があると判断された無登録業者は、違反対象になり得る。捜査当局に連絡することもある」と話す。

リーダーのLINEメッセージ。配当ポイントをビットコインに交換するサービスの利用停止を告げ、その後、連絡が取れなくなった（個人情報の部分にモザイクをかけています）

「年利数百%」■客紹介で配当増

相次ぐ投資被害 訴訟へ

「甘かった。投資前の生活に戻りたいです」

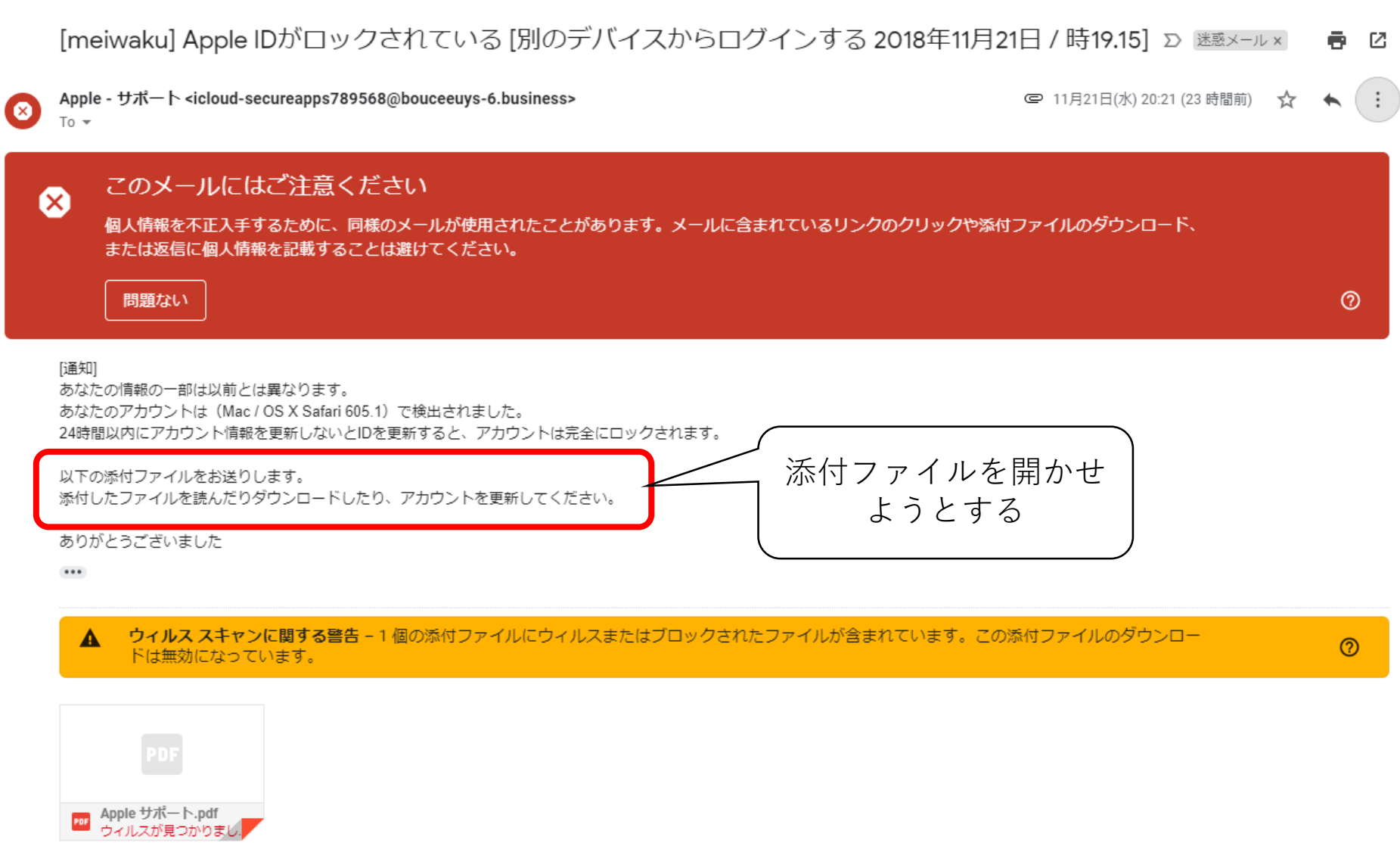
東京都の30代の会社員男性は昨年、「HYIP」（高収益投資プログラム）と呼ばれる投資案件に約700万円分のビットコインを投じ、約600万円の損失を出した。増資のために借りたカードローン400万円の返済に苦しむ。

HYIPは主に、外国の運営法人が「日利数%」「年利数百%」の超高利回りをうたい、ネットを介して客から募ったビットコインなどを原資にブックメーカー（賭け）や為替取引に投資し、得られた収益を客に配当する仕組みだ。ただ、資金繰りが悪化して破綻する事例もある。

日本では一昨年から昨春にかけて、運営側に新規客を紹介すると配当が増える

私のIDとパスワードがロックされた？

トラブル事例：IDロックを騙った詐欺



アカウントがハッキングされた？

hiro-s@db4.so-net.ne.jp
To hiro-s

11月17日(土) 22:21 (5 日前)

このメールにはご注意ください

個人情報を不正入手するために、同様のメールが使用されたことがあります。メールに含まれているリンクのクリックや添付ファイルのダウンロード、または返信に個人情報を記載することは避けてください。

問題ない

親愛なるドメインユーザーdb4.so-net.ne.jp！

私はスパイウェアソフトウェア開発者です。
2018年の夏にアカウントがハッキングされました。

私の証拠はここにあります： あなたのアカウントからこのメールをお送りしました。

ハッキングは、オンラインで行ったハードウェアの脆弱性を使用して行われました（Ciscoルータ、脆弱性CVE-2018-0296）。

私はルーターのセキュリティシステムを回り、そこに悪用をインストールしました。
あなたがオンラインになったとき、悪意のあるコード（ルートキット）があなたのデバイスにダウンロードされました。
これはドライバソフトウェアです。私は絶えず更新していますので、あなたのアンチウィルスは常に黙っています。

それ以来、私はあなたに従っています（私はあなたのデバイスにVNCプロトコルで接続できます）。
つまり、あなたがしているすべてのことを絶対に見ることができ、自分のファイルやデータを自分自身に見てダウンロードすることができます。
私はまた、あなたのデバイス上のカメラにアクセスして、定期的にあなたと写真やビデオを撮ります。

現時点では、私は固体の汚れを収穫しています...あなたに...
私はすべてのあなたの電子メールとチャットをメッセンジャーから救った。訪問したサイトの全履歴も保存しました。

私は、パスワードを変更することは役に立たないことに注意します。私のマルウェアは毎回あなたのアカウントのパスワードを更新します。

あなたが大好きなもの（アダルトサイト）を知っています。
ああ、そうです。私は皆から隠れているあなたの秘密の人生を知っています。
ああ、私の神、あなたのようなもの...私はこれを見た...ああ、あなたは汚いいたずらな人... :)

大人のコンテンツであなたの最も情熱的な楽しみの写真やビデオを撮り、カメラの映像とリアルタイムで同期させました。
それは非常に高品質になったと信じて！

IDだけではなく、
パスワードを明記しているケースもあり

だから、ビジネスに！
私は一つのことを確信しています。 あなたはしたくないこの汚れを見せてあなたの連絡先に.

だから私を送る私のビットコインウォレットに504ドル Bitcoin: 1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC
転送時にウォレット番号をコピーして貼り付けるだけです。
あなたがそれをする方法を知らない場合 - Googleに尋ねる。

消して欲しければ仮想通貨で
支払うよう指示

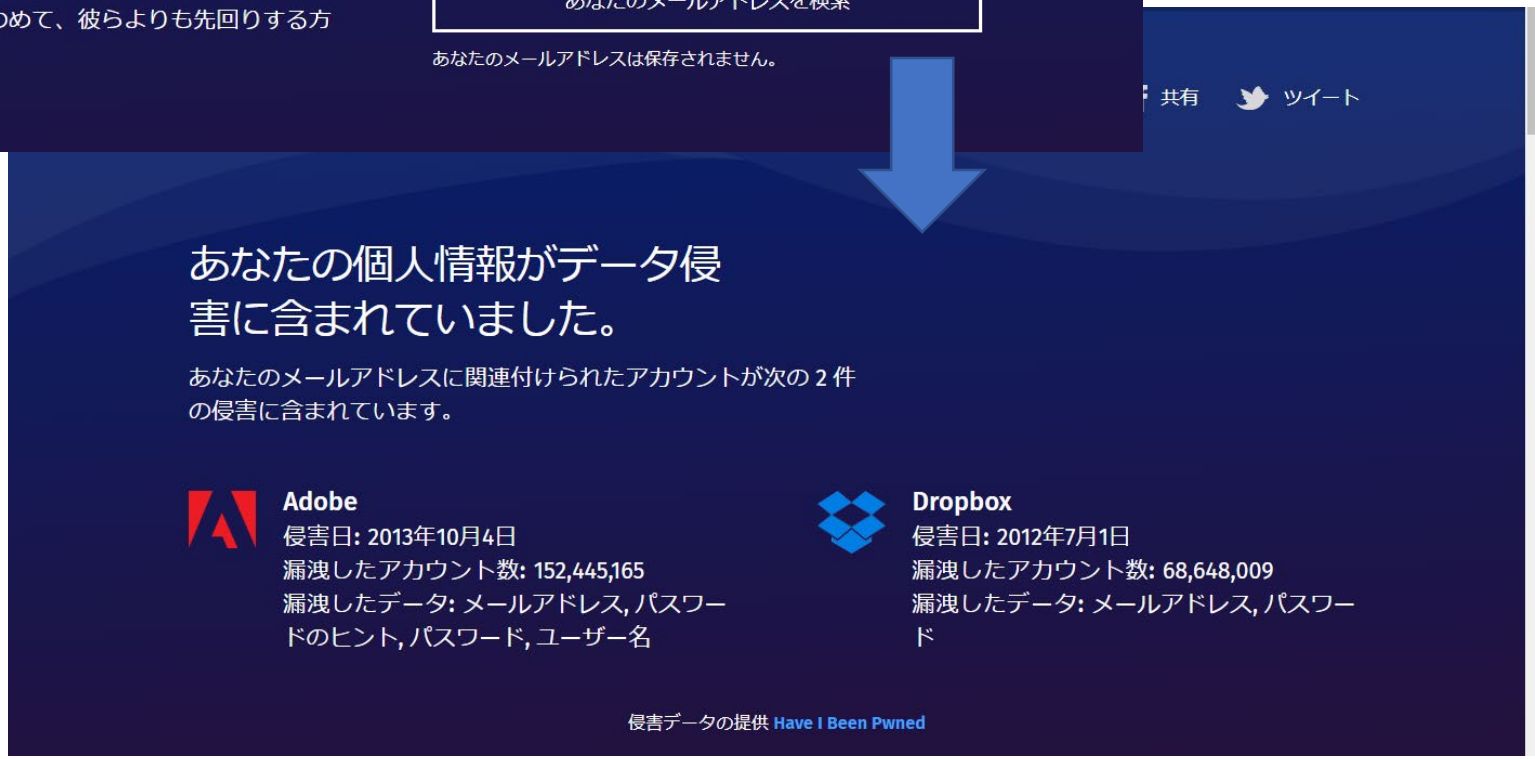
私のシステムは翻訳を自動的に認識します。
指定された金額を受け取るとすぐに、私のサーバーからすべてのデータ
心配しないで、私は本当にあなたの立場に落ちた多くの人々と "働いている"ので、私は本当にすべてを削除します。
ルータの脆弱性についてプロバイダに通知するだけで、他のハッカーがそれを使用しないようにする必要があります。

この手紙を開いて以来、あなたは50時間あります。
指定された時間が経過すると、資金が受け取られない場合は、デバイスのディスクがフォーマットされ、
私のサーバーから自動的にあなたの連絡先すべてに電子メールとSMSが送信されます。

私は賢明なままで、ナンセンス（私のサーバー上のすべてのファイル）に従事しないことをお勧めします。

がんばろう！

あなたのIDとパスワードは流出している？



「偽メール」にだまされないためには

1. 自分が使っているサービスか

・使っていないサービスの場合は要注意。問い合わせしない
・使っているサービスの場合も、宛先等が正しいか

2. 送り主のメールアドレスが正しいか

・@sagawa-ihg.comのように、本物とよく似ているが違うアドレス
・意味の無い文字が羅列されているようなアドレス

3. 添付ファイルやID・パスワードの入力には注意

・メール本文など不審な場合、添付ファイルは開かない
・関係の無いIDやパスワードが求められる場合は入力しない
　例）「佐川」急便なのに「Apple」 IDを要求される　など

4．迷惑メール対策を有効にする

・ウィルス対策ソフトのインストール、有効化
・契約しているプロバイダの迷惑メール対策機能を使う