


リスト型攻撃時代  
私たちはどう立ち向かうべきか  
～漏洩現場の小ネタを添えて～



ソフトバンク・テクノロジー株式会社  
辻 伸弘

それでは、はじまります

# おだいもく

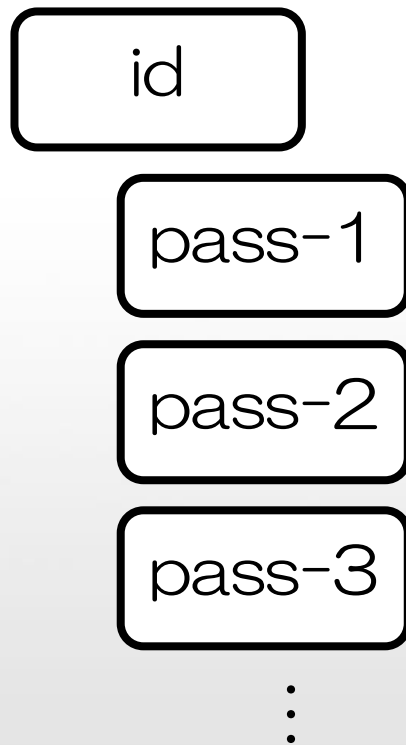
- 0x01. パスワードを取り巻く現状
- 0x02. リスト型攻撃の過去と今
- 0x03. ちょっと裏話
- 0x04. どう立ち向かうか
- 0x05. さいごに

0x01. パスワードを取り巻く現状

# 0x01. パスワードを取り巻く現状

## まずは、パスワードの突破手法整理

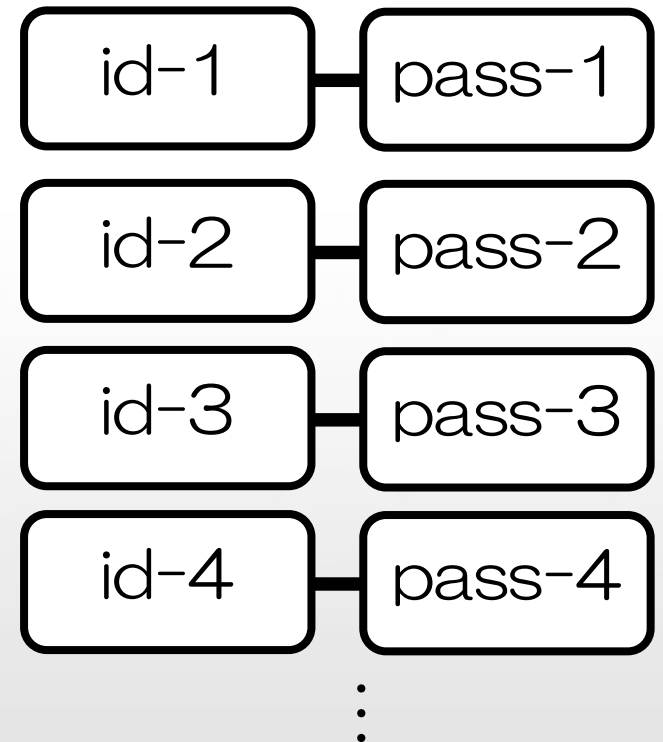
ブルートフォース、  
ディクショナリ



リバース  
ブルートフォース



リスト型



0x01. パスワードを取り巻く現状

2013年度に入ってから…

不正ログインが  
立て続けに発生

# 0x01. パスワードを取り巻く現状 なぜ多発しているのか

- 1人が扱うID, PASSの増加
- パスワードの鉄則（無理難題？）
  - 長く複雑なパスワード
  - 定期変更の亡霊？

0x01. パスワードを取り巻く現状

に加えて



# 0x01. パスワードを取り巻く現状



 iTunes

¥1000

```
file:///C:/Users/nobtsuji/AppData/Local/M...
ファイル(F) 編集(E) 書式(O)
451
452
453
454
OnFocus="this.blur();"
href="https://buy.itune
pple.jingle.app.finance
code=X5Z6ZFY46TVWYVXW&a
```

今すぐコードを使用する

# 0x01. パスワードを取り巻く現状



amazon.co.jp  
ギフト券

ギフト券番号:

U9Z8-34MGBV-MSS2

¥ 1,000

アカウントに登録する



0x01. パスワードを取り巻く現状

換金性が高い

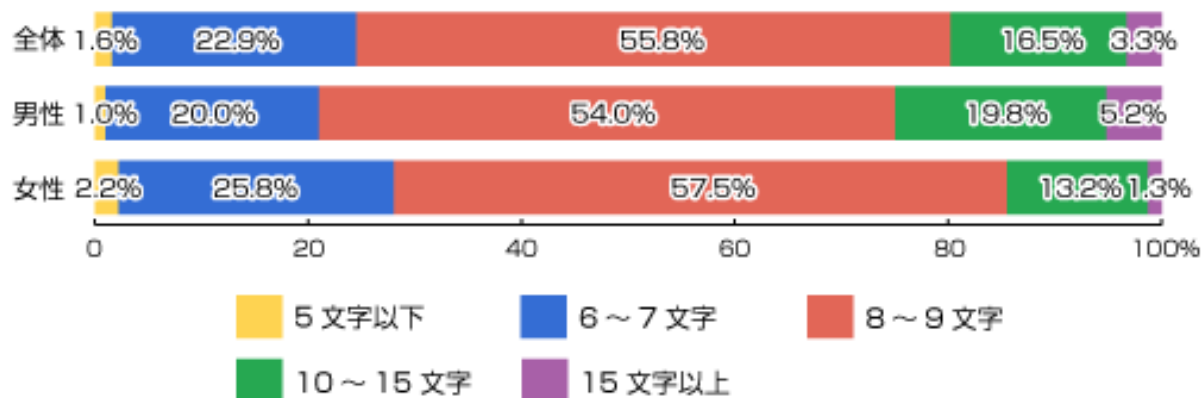
0x01. パスワードを取り巻く現状

一方ユーザの状況は？

# Ox01. パスワードを取り巻く現状 アンケート結果

■ Q3. あなたがログインが必要なウェブサイトで使うパスワードの平均的な文字数を教えてください。

※単一回答/10代から60代の全国男女(n=1200人)



リサーチバンク

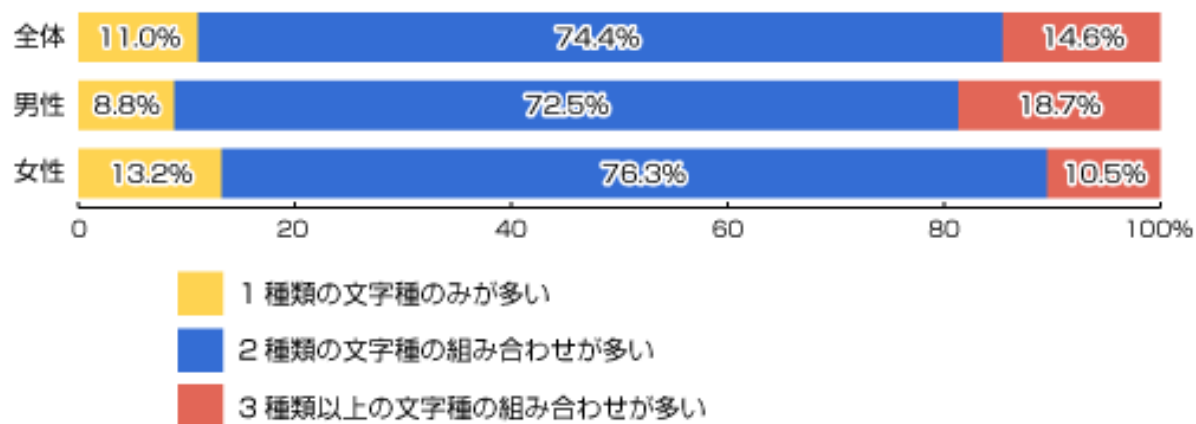
[http://research.lifemedia.jp/2014/04/140423\\_authentication.html](http://research.lifemedia.jp/2014/04/140423_authentication.html)

# Ox01. パスワードを取り巻く現状 アンケート結果

■ Q4. あなたがログインが必要なウェブサイトで使うパスワードは、異なる文字種を使っていますか？

※文字種とは、大文字・小文字・数字などのことです。

※単一回答/10代から60代の全国男女(n=1200人)



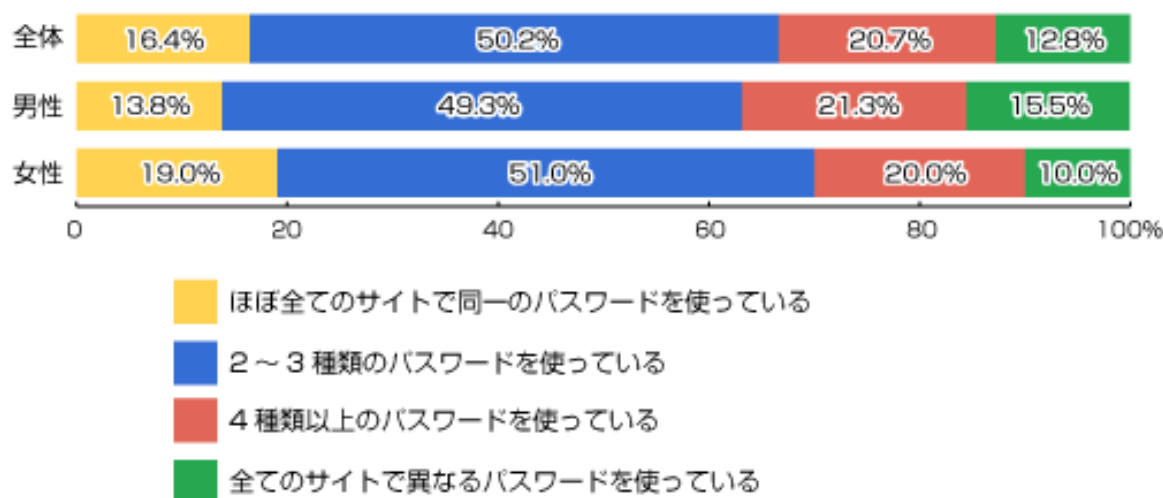
リサーチバンク

[http://research.lifemedia.jp/2014/04/140423\\_authentication.html](http://research.lifemedia.jp/2014/04/140423_authentication.html)

# Ox01. パスワードを取り巻く現状 アンケート結果

■ Q2. あなたがログインが必要なウェブサイトで使うパスワードの設定方法でもっとも当てはまるものを教えてください。

※単一回答/10代から60代の全国男女(n=1200人)



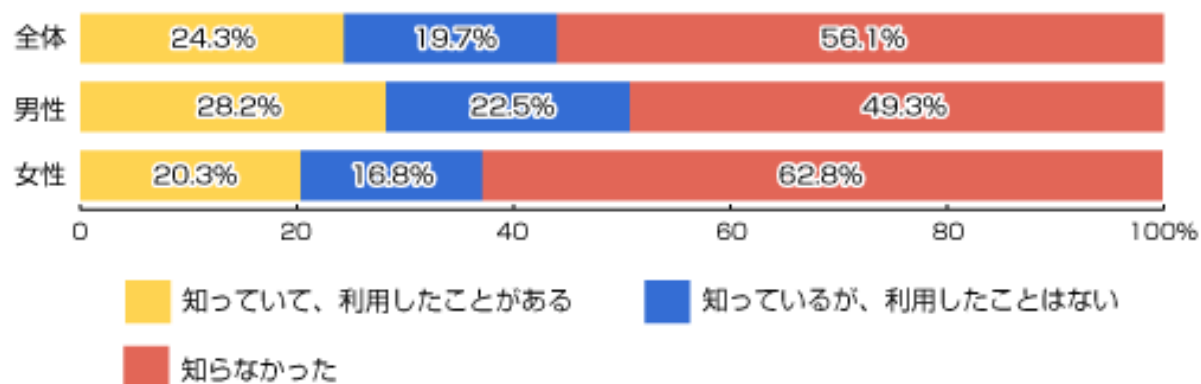
リサーチバンク

[http://research.lifemedia.jp/2014/04/140423\\_authentication.html](http://research.lifemedia.jp/2014/04/140423_authentication.html)

# Ox01. パスワードを取り巻く現状 アンケート結果

■ Q8. あなたは、2段階認証を知っていましたか？

※単一回答/10代から60代の全国男女(n=1200人)



リサーチバンク

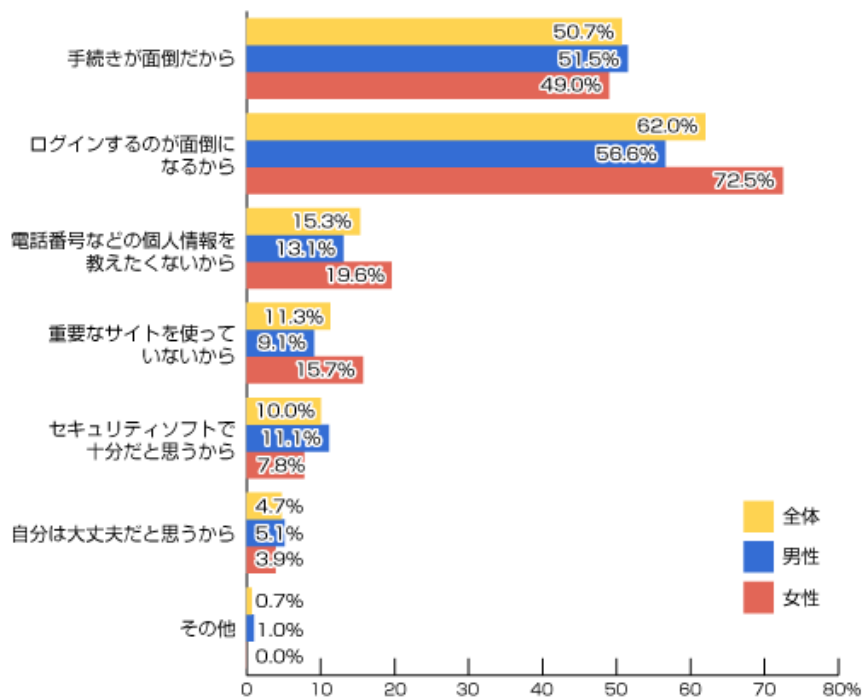
[http://research.lifemedia.jp/2014/04/140423\\_authentication.html](http://research.lifemedia.jp/2014/04/140423_authentication.html)



# Ox01. パスワードを取り巻く現状 アンケート結果

■ Q10. あなたはなぜ、リスクベース認証や2段階認証を今後使いたくないのですか？

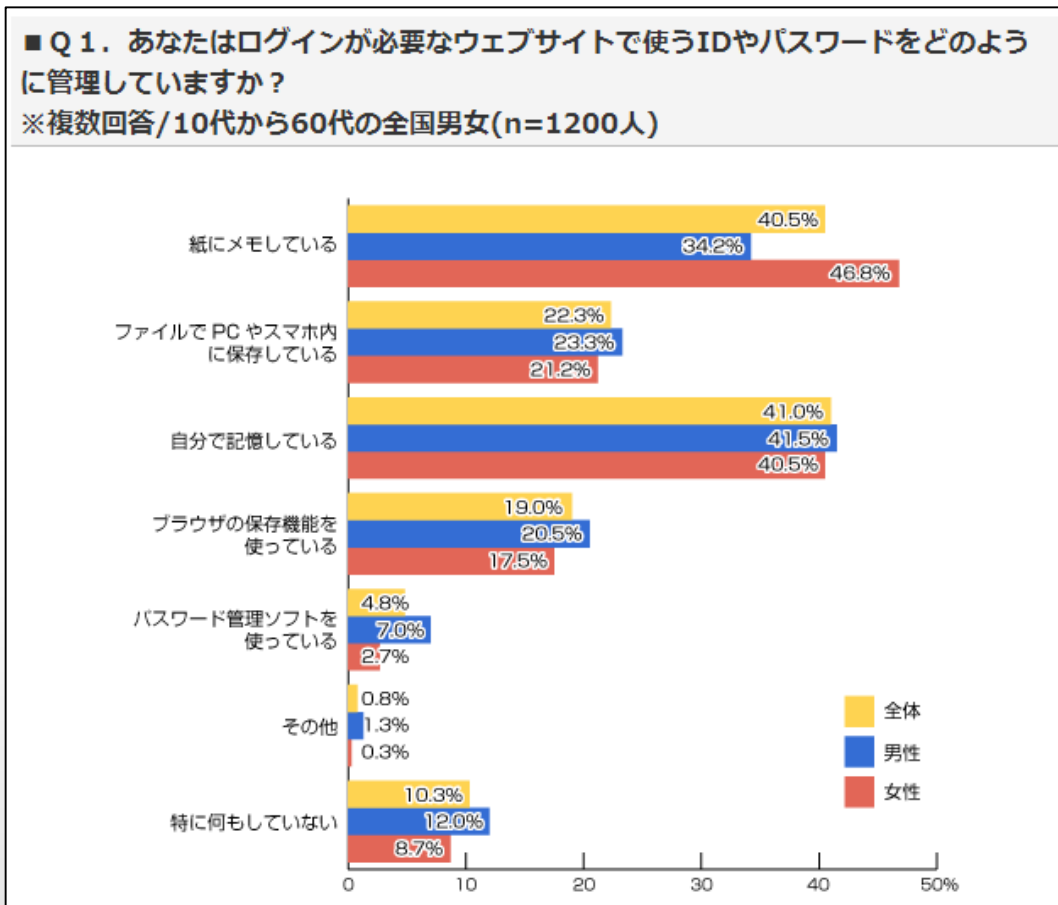
※複数回答/リスクベース認証や2段階認証を使いたくないと回答した人(n=150人)



リサーチバンク

[http://research.lifemedia.jp/2014/04/140423\\_authentication.html](http://research.lifemedia.jp/2014/04/140423_authentication.html)

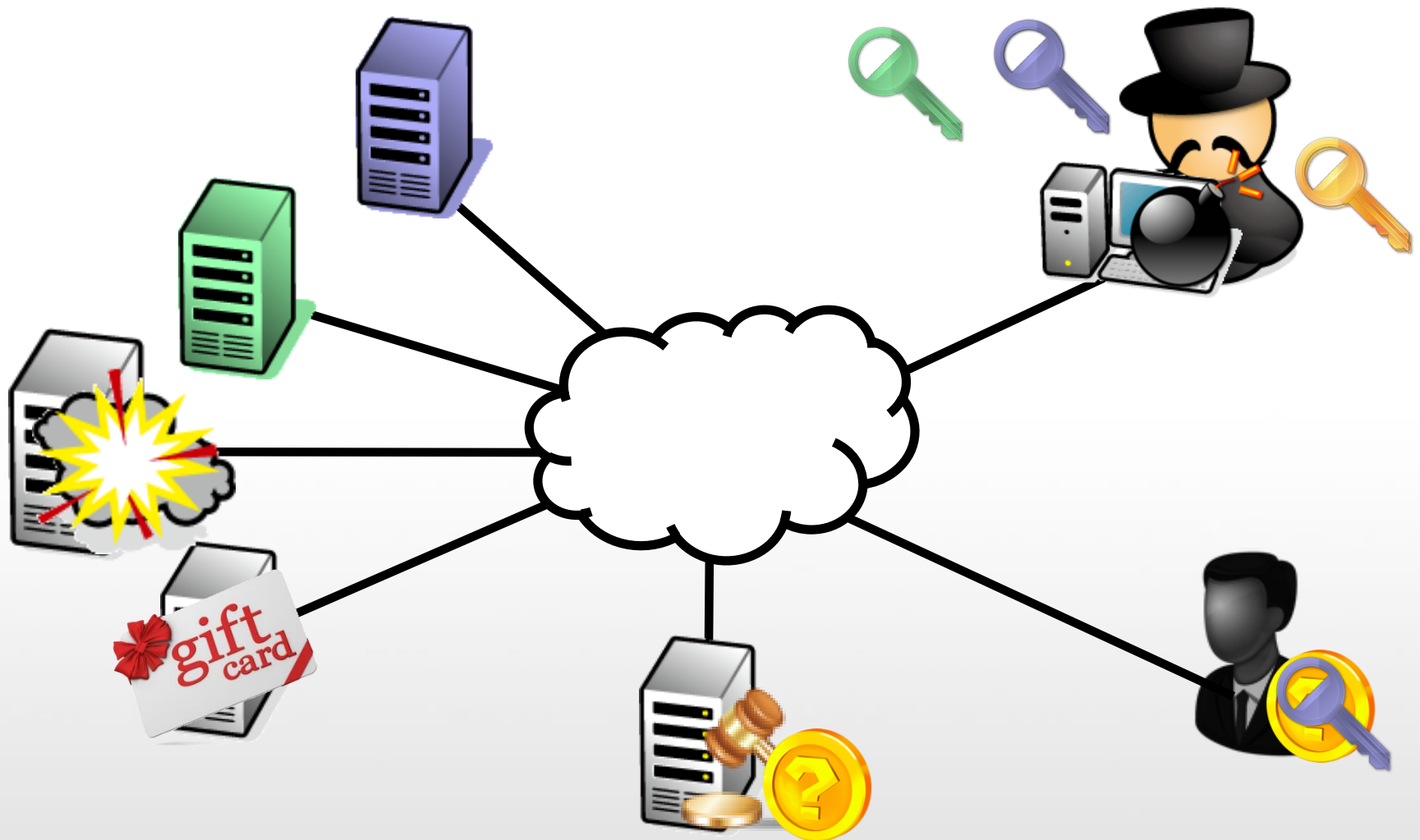
# OxO1. パスワードを取り巻く現状 アンケート結果



リサーチバンク

[http://research.lifemedia.jp/2014/04/140423\\_authentication.html](http://research.lifemedia.jp/2014/04/140423_authentication.html)

# 不正ログインの連鎖考察



モニタの前で犯行が完結

# 0x02. リスト型攻撃の過去と今

# 0x02. リスト型攻撃の過去と今

## 【過去】

- 少数のIPアドレスからアクセス
- 国外からのアクセスが多数
- 実質的被害が少ない

# 0x02. リスト型攻撃の過去と今

## 【現在】

- **複数**のIPアドレスからアクセス
- **国内**からのアクセスが増加
- **実質的被害、二次被害が増加**
- リストの洗練

# 0x02. リスト型攻撃の過去と今

## リストの洗練



# 0x02. リスト型攻撃の過去と今

## 実質的被害、二次被害が増加

PRESS RELEASE

### 「niconico」への不正ログインに関するご報告

株式会社ドワンゴ  
2014年6月13日



株式会社ドワンゴ（本社：東京都中央区、代表取締役社長：荒木隆司）及び株式会社ニワンゴ（本社：東京都中央区、代表取締役：杉本誠司）は、両社が運営する動画サービス「niconico」において、ご登録ユーザー以外の第三者による不正ログインを受ける「リスト型アカウントハッキング(※)」が発生したことをご報告いたします。

ご利用いただいているユーザーの皆様には、ご迷惑、ご心配をおかけしましたことを深くお詫び申し上げます。以下の通り、今回発生した被害の詳細をご説明いたします。

# 0x02. リスト型攻撃の過去と今

## 実質的被害、二次被害が増加

ニュース 日経コンピュータ

### ANAマイレージクラブへの不正ログインで112万マイルが詐取、住所なども閲覧可能に

2014/03/11  
浅川 直輝 = 日経コンピュータ (筆者執筆記事一覧)

[記事一覧へ >>](#)

 シェア ツイート ブックマーク

全日本空輸（ANA）は2014年3月10日、ANAマイレージクラブのWebサイトが不正ログインを受け、顧客のマイレージがiTunesギフトコードへ交換されていたことを明らかにした（特別なお知らせ）。

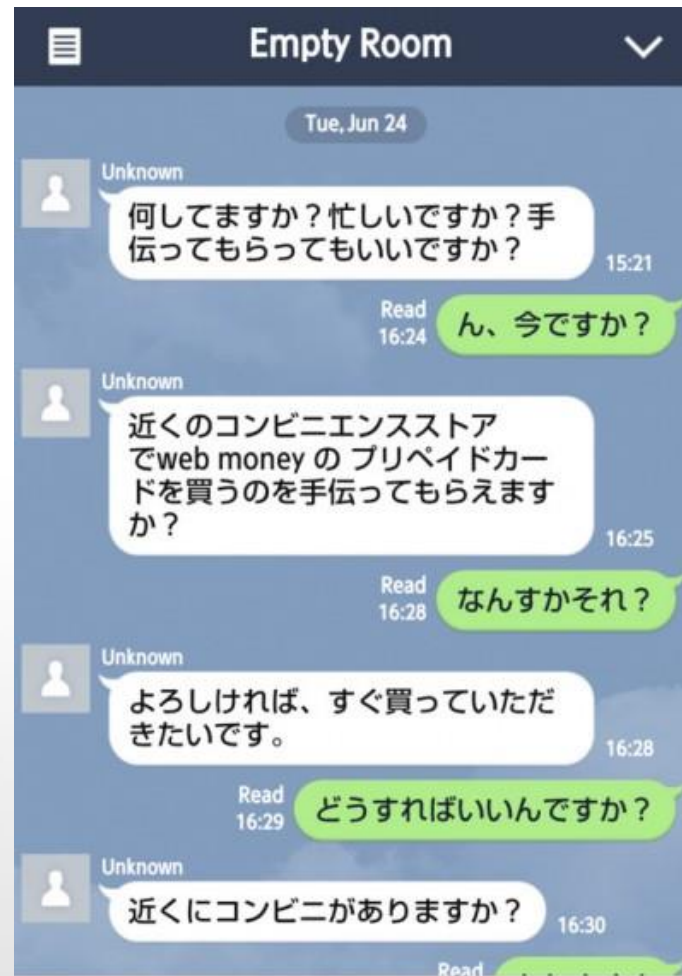


写真1●ANAマイレージクラブのログイン画面  
[画像のクリックで拡大表示]

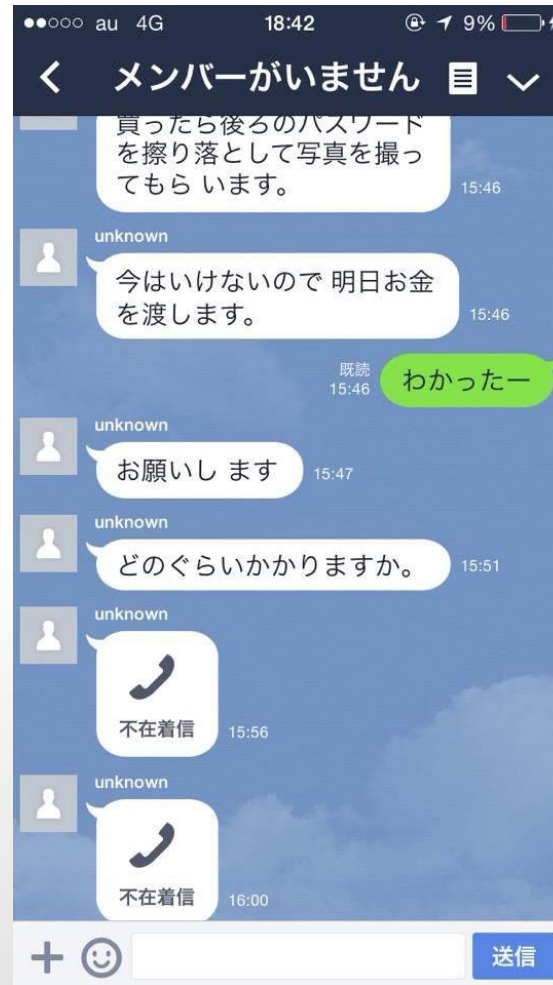
# 0x02. リスト型攻撃の過去と今

二次被害？

# 0x02. リスト型攻撃の過去と今



# 0x02. リスト型攻撃の過去と今



# 0x02. リスト型攻撃の過去と今

## 馬鹿にできない二次被害

日本経済新聞 11月19日 水曜日 English 中文

Web刊 速報 ビジネスリーダー マーケット マネー テクノロジー ライフ スポーツ

全て : 経済 : 企業 : 国際 : 政治 : 株・金融 : スポーツ : 社会 : ニュース18時 : その他ジャンル

速報 > 社会 > 記事

### LINE乗っ取り詐欺、都内の被害2800万円

2014/10/29 11:26

小 中 大 保存 印刷 リプリント Twitter Facebook 共有

無料通話チャット・アプリのLINE(東京・渋谷)の利用者アカウントが不正ログインで乗っ取られた問題で、警視庁サイバー犯罪対策課は29日、電子マネーを詐取された被害を東京都内で368件、約2800万円分確認したと発表した。金銭的な被害がなかったケースを含めると、計657件の相談や被害届があったという。

同課によると、大半は知人になりすましてメッセージを送り、コンビニなどで電子マネーを購入させる手口だった。同課は詐欺や不正アクセス禁止法違反の疑いで捜査している。

同課は7月22日に100件、650万円分の電子マネーの被害を確認したと発表しており、被害額は4倍以上に膨らんだが、被害は10月中旬から減少傾向にあるという。LINEが9月に導入した第2パスワード「PINコード」の設定義務付けや、電子マネー運営会社の対策の効果が出ているとみている。

# 0x02. リスト型攻撃の過去と今

## 馬鹿にできない二次被害

YOMIURI ONLINE

### IT&メディア

トップ ニュース セキュリティ 新製品 リポート コラム ITを語る イベント

文字サイズ 小 **中** 大

#### LINE「乗っ取りでは」被害防いだ店員の一言

2014年07月16日 09時08分  ツイート 0  おすすめ 0  8+1  17

無料通話アプリ「LINE(ライン)」のアカウントが乗っ取られ、電子マネーがだましとられる被害が全国で相次いでいる問題で、石川県警金沢中署は14日、金沢市のコンビニ店員が、客の男子大学生が被害に遭うのを未然に防いだと発表した。

発表によると、大学生は10日、同市の知人男性のアカウントから、「電子マネー買うの手伝って」とメッセージを受け取り、電子マネー2万円分をコンビニで購入しようとしたところ、男性店員から「最近よくある犯罪では」と声をかけられた。大学生が知人に電話で確認し、アカウントが乗っ取られてメッセージが送られていたことが判明した。

同署は不正アクセス禁止法違反容疑で捜査するとともに、詐欺未遂容疑も視野に調べている。

県警生活環境課によると、県内では6月中旬から7月11日までに、ラインのアカウントが乗っ取られた被害者は13人に上り、メッセージを受け取った8人が電子マネー計23万1000円分を購入した。

# 0x02. リスト型攻撃の過去と今

草の根って大事！



0x03. ちょっと裏話

0x04. どう立ち向かうか

# 0x04. どう立ち向かうか

攻撃者は  
どんどん巧妙に  
そして、私たちの身近に

# 0x04. どう立ち向かうか

攻撃者サイドは…

- モチベーションが高い
- 分業、組織化されている
- 洗練されてきている

0x04. どう立ち向かうか

こちら側は  
とにかく不利

# 0x04. どう立ち向かうか こちら側も…

- モチベーションを少しでも…
- サービス事業者、利用者の協力
- 草の根でも手口に追従

# Ox04. どう立ち向かうか

## 勘所

- 自衛部分は自分にしかできない
- 被害はどんどん身近なものに
- 専門家だけの情報発信は限界

## 0x04. さいごに

人は誰だってヒーローになれる。  
傷ついた少年の肩に上着を掛け  
世界は終わりじゃない  
と励ましてくれる男だ。



**thank you <3**