NECOMA

フィッシングサイト対策のすべて

東京大学
情報基盤センター
助教　宮本大輔

フィッシング詐欺とは？

PayPal

Account Status Update.
Log in to your paypal as soon as possible

Hello

Recently, there's been activity in your PayPal account that seems unusual compared to your normal account activities. Please log in to PayPal to confirm your identity and update card information.

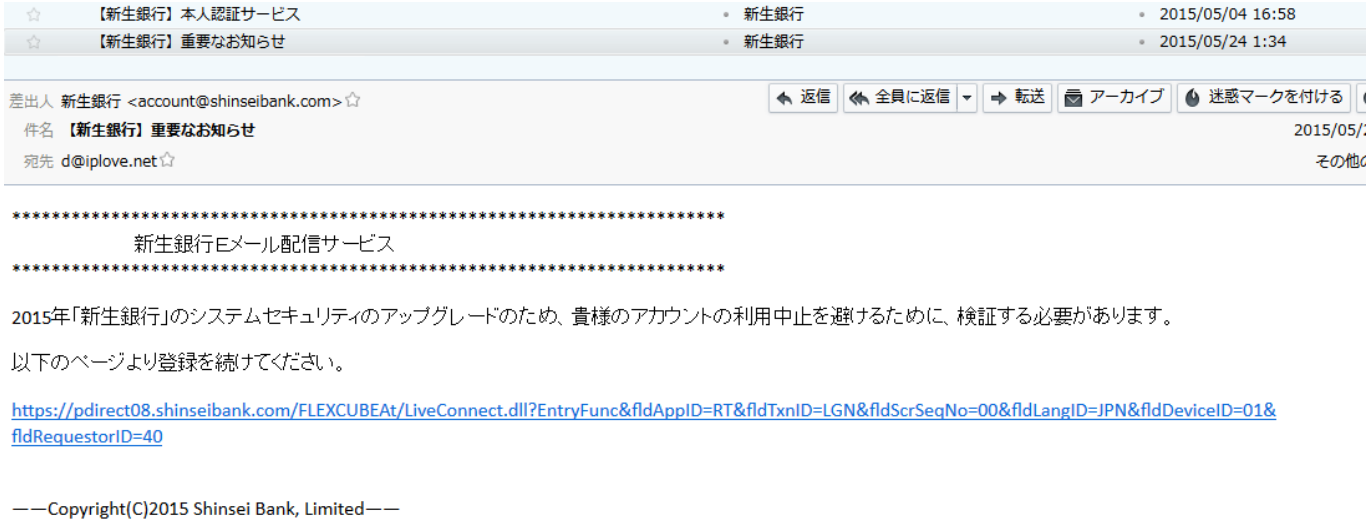
We're concerned that someone is using your PayPal account without your knowledge. Recent activity from your account seems to have occurred from a suspicious location or under circumstances that may be different than usual.

What do I need to do?

- **Click here**
- **Log in to your PayPal account as soon as possible. We may ask you to confirm information you provided when you created your account to make sure you're the account holder. We'll then ask you to change your password and security questions.**

Yours sincerely,
PayPal

日本語の壁は機能するか



【新生銀行】本人認証サービス • 新生銀行 • 2015/05/04 16:58
【新生銀行】重要なお知らせ • 新生銀行 • 2015/05/24 1:34

差出人 新生銀行 <account@shinseibank.com>
返信 全員に返信 転送 アーカイブ 迷惑マークを付ける
件名 【新生銀行】重要なお知らせ 2015/05/
宛先 d@iplove.net その他

****
新生銀行Eメール配信サービス
****

2015年「新生銀行」のシステムセキュリティのアップグレードのため、貴様のアカウントの利用中止を避けるために、検証する必要があります。

以下のページより登録を続けてください。

https://pdirect08.shinseibank.com/FLEXCUBEAt/LiveConnect.dll?EntryFunc&fldAppID=RT&fldTxnID=LGN&fldScrSeqNo=00&fldLangID=JPN&fldDeviceID=01&fldRequestorID=40

——Copyright(C)2015 Shinsei Bank, Limited——

フィッシングの被害額

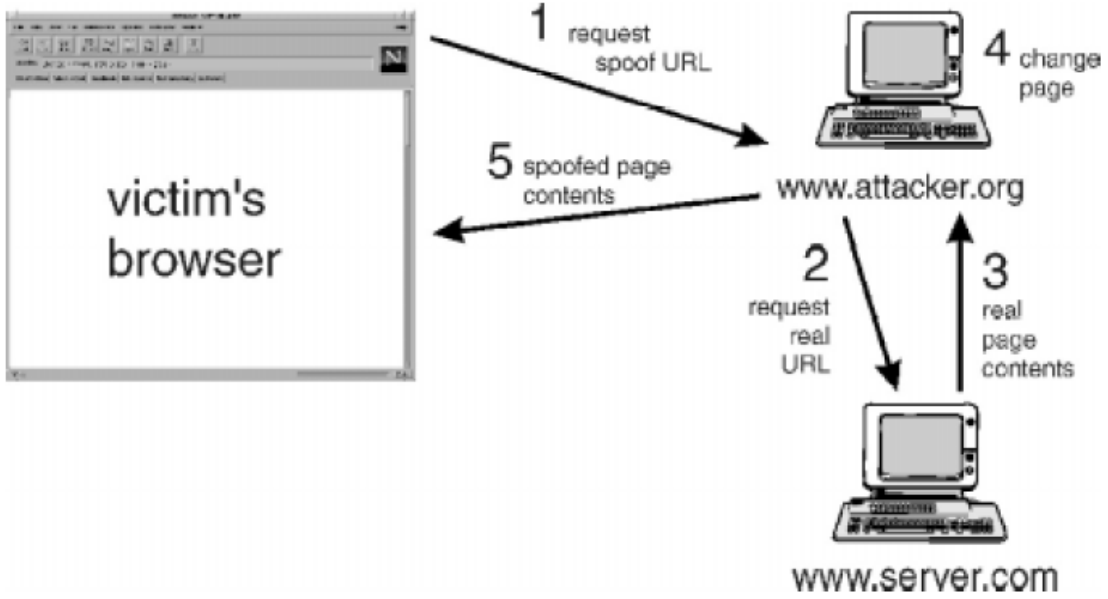
- フィッシングによる被害報告
  - 被害総額（概算）
    - 2005年の被害額は $929mil
      Gartner Survey Shows Frequent Data Security Lapses and Increased Cyber Attacks Damage Consumer Trust in Online Commerce (Gartner)
    - 2008年の被害額は $3.6bil
      Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks.（Gartner)
    - 2013年で $5.9bil
      THE CURRENT STATE OF CYBERCRIME 2014(RSA)
    - 2014年12月で $453mil
      2014 CYBERCRIMR ROUNDUP (RSA)
  - オンライン犯罪でいえば・・

期間	件数	被害額（実被害額）
H26	1,876件	約29億1000万円（約24億3600万円）
H25	1,315件	約14億 600万円（約13億3000万円）
H24	64件	約 4800万円（約 4800万円）

※ 被害額 ・・・犯人が送金処理を行ったすべての額
※ 実被害額・・・「被害額」から金融機関が不正送金を阻止した額を差し引いた実質的な被害額

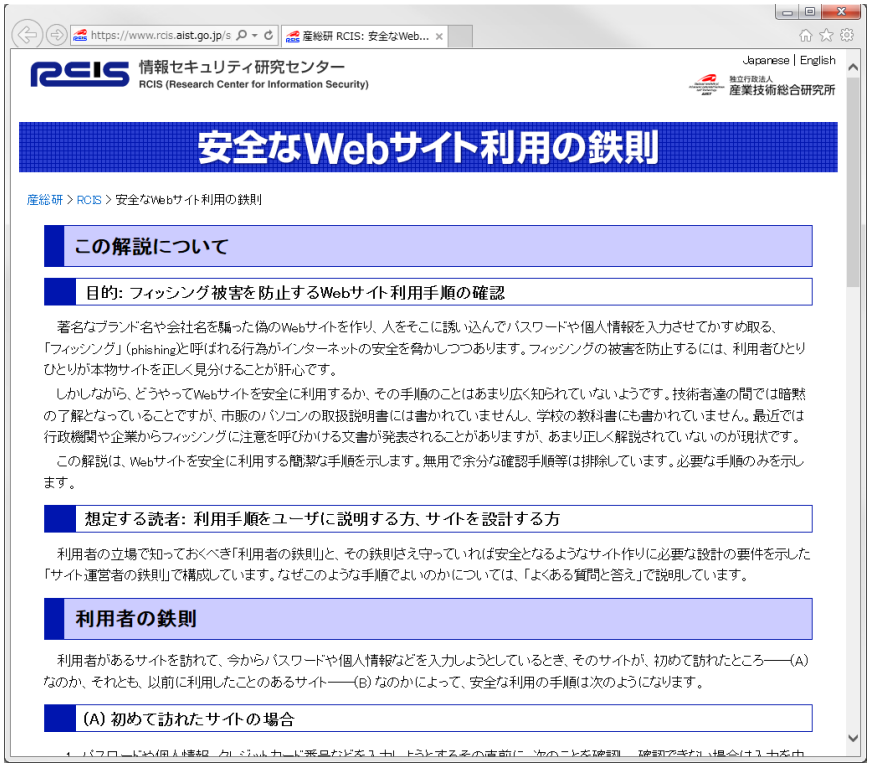
1997年頃に言われていたこと

E.W. Felten et al. “Web Spoofing: An Internet Con Game”, 1997



- 短期的な解決方法
  - JavaScriptの無効にする
  - ロケーションバー（アドレスバー）の表示を常に見えるようにし、注意して閲覧する
- 長期的な解決方法
  - ブラウザは常にアドレスバーが表示されるようなものにしていきましょう
  - セキュアな接続の表示を確認できるようにしましょう

2007年頃に言われていたこと



産総研, “安全なWebサイト利用の鉄則”, 2007
高木浩光, “正しいフィッシング対策について”, 2007

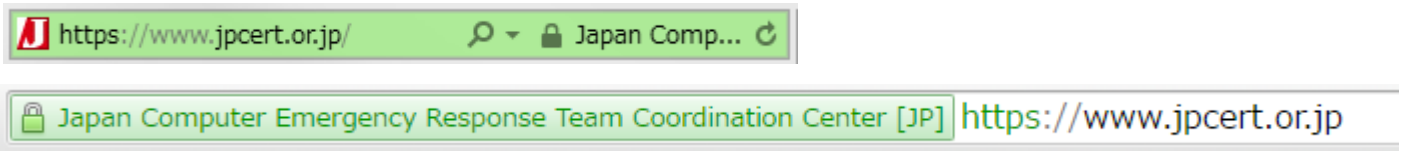
- 初めて訪れたサイトの場合
  - サイト運営者のことを知っている場合
    - その運営者のドメイン名を既に知っている場合
      - アドレスバーのドメイン名を確認する
    - その運営者のドメイン名をまだ知らない場合
      - SSLのサーバ証明書の内容を確認する
  - サイト運営者のことをまだ知らない場合
    - （信用できる運営者か見極める）
- 再度訪れたサイトの場合
  - アドレスバーのドメイン名を確認する

そして今

- アドレスバーの確認ことの意味は重要
  - URL の確認だけでなく、証明書の確認の意味も込められるようになった

ステータスバーの証明書情報がアドレスバーで見られるようになった

EV-SSL証明書によりアドレスバーが緑色で表示されるようになった



問題はなにか

- 「アドレスバーを確認する」という鉄則は約20年前に確立されている
- その一方で、フィッシングによる被害は増加し続けている
- 果たして20年間、何を対策してきたのか？

NECOMA

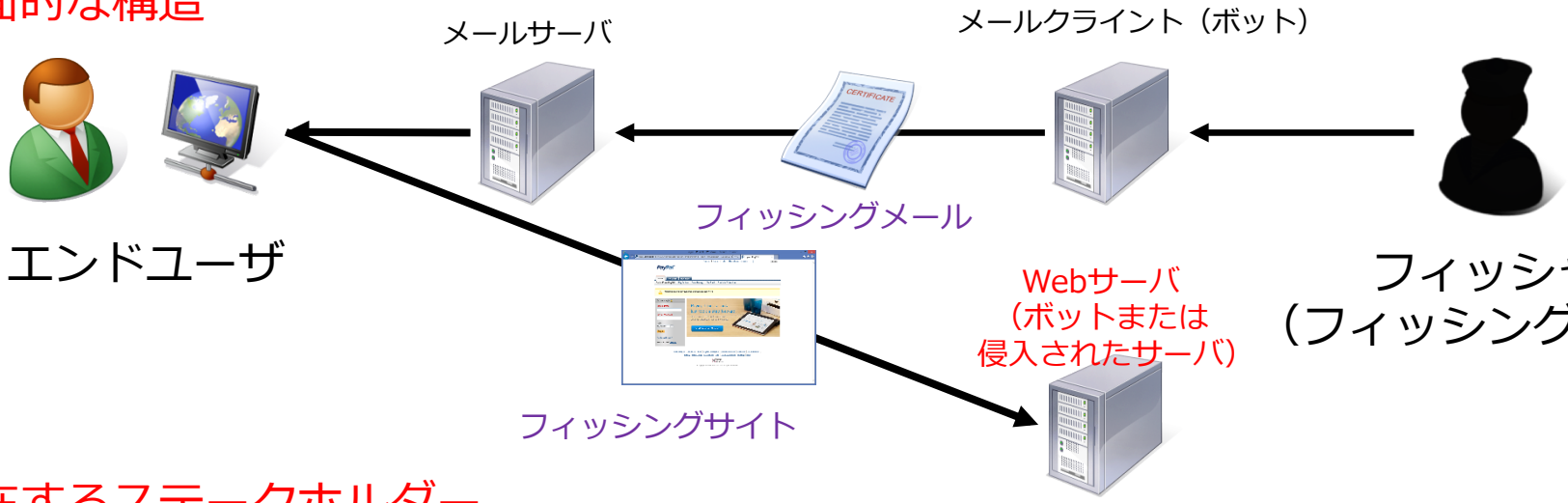
本日のテーマ：
フィッシングサイト対策のすべて

- フィッシング対策技術のこれまでの10年
- フィッシング対策技術のこれから
- フィッシングメールとサイトの対策

NECOMA

フィッシングサイト問題の構図

表面的な構造



内在するステークホルダー

ブラウザベンダー

フィッシング対策ソフトウェアのベンダー

PhishWall®

フィッシングサイト閉鎖事業者

SECURED BY RSA

FraudWatch International

対策のコーディネータ

APWG

フィッシング対策協議会
Council of Anti-Phishing Japan

警察・法的機関

その他のステークホルダー

・フィッシングサイトが設置されたSP

・エンドユーザのISP

・フィッシングサイトに真似られるウェブサイト事業者
etc…

「エンドユーザを守る視点」の原理

意思決定のサポートを行う

意思決定に役立つ情報を提示

教育による解決

注意喚起による解決

検知による解決

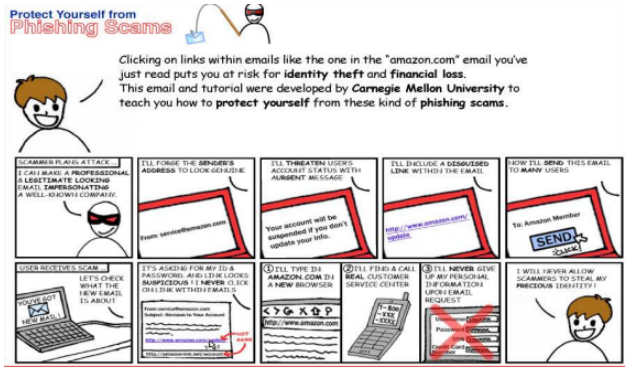
教育によるフィッシング対策 (1)

- 「アドレスバーを確認しましょう」
  - 何を確認するのか、どう確認するのかを教材を使って教える

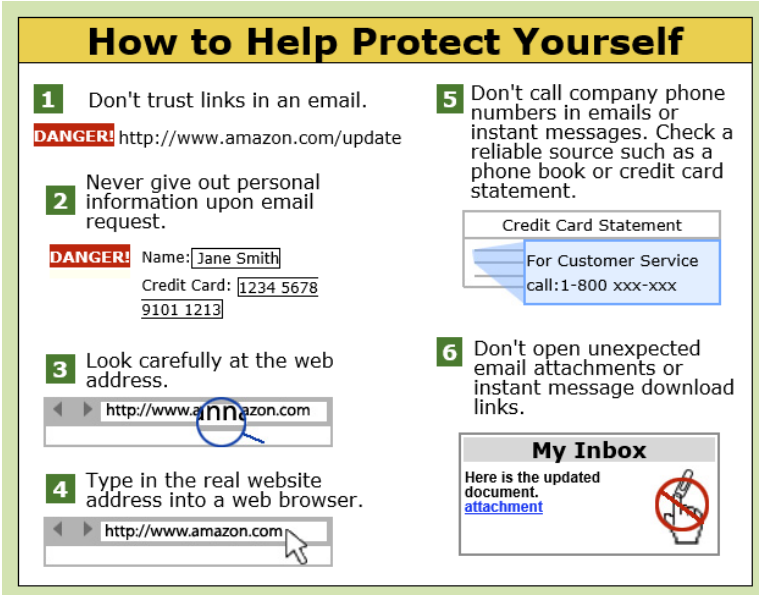
- テーマ：どのような教材が、どのようなユーザに効果的か？

教育によるフィッシング対策 (2)

- 手法：コミカライズ、ゲーミフィケーション



- 対象：騙されやすそうなエンドユーザ



- フィッシングサイトの跡地に教材を設置する

P. Kumaraguru, “Protecting people from phishing: the design and evaluation of an embedded training email system”, 2007
S. Sheng “Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish”, 2007

教育によるフィッシング対策 (3)

- Stay Smart Online (オーストラリア)
  - 政府主導のサイバーセキュリティ教育
  - 子供向け対策
    - エデュテインメント

- Klick Dengan Bijak (マレーシア)
  - 25万人に延べ1700時間の講義
  - 子供向け対策
    - Cool & Fun
    - モラル、マナー、エチケット
    - ロールプレイモデル

- Stop Think Connect (USA)

教育によるフィッシング対策 (4)

- 小中学校向けのサイバーセキュリティ教育
  - 演習 = フィッシング判定クイズ（ゲーム化）
  - 座学 = 物語形式（ロールモデル）
  - 演習 = クイズ（達成度テスト）

千葉県	2/27	**サイバーセキュリティ授業** 小学6年生の児童に対し，フィッシング攻撃の概要及び対策について授業を行い，サイバー犯罪に巻き込まれないような基礎知識の習得とリテラシーの向上を狙う.	鎌ケ谷市立道野辺小学校	鎌ケ谷市立道野辺小学校，株式会社インク，東京大学(NECOMA Project)	—

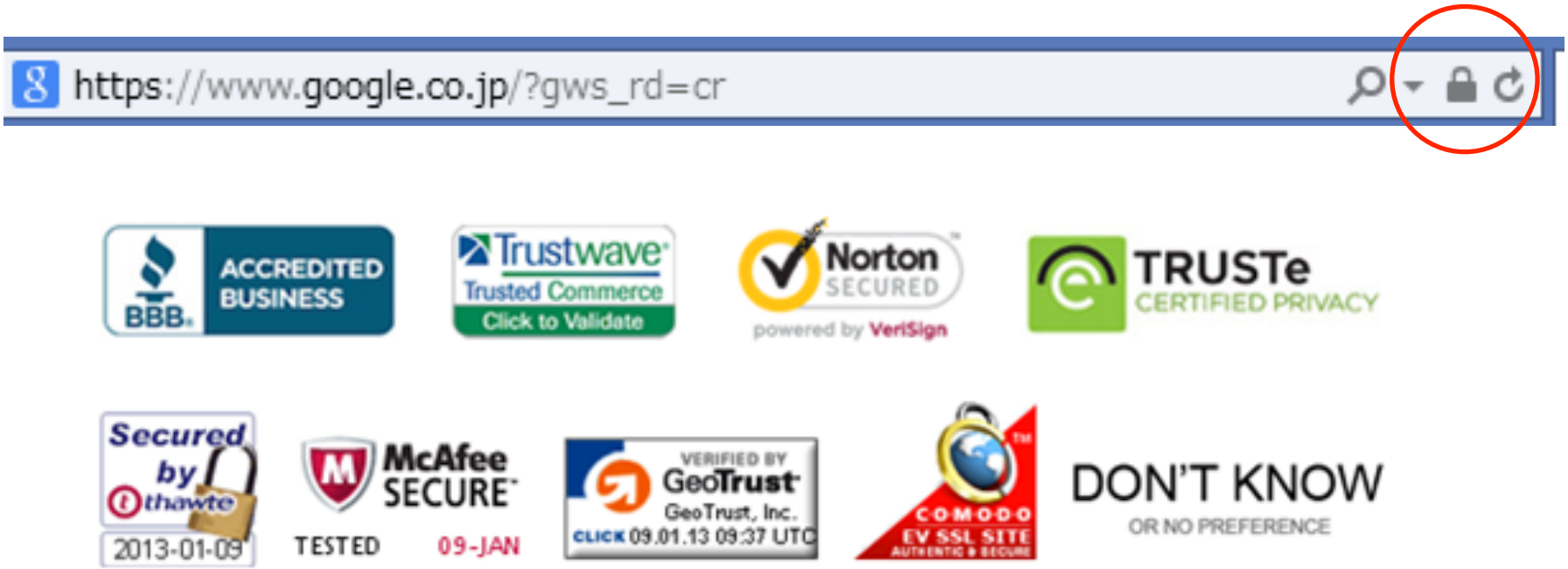
http://www.nisc.go.jp/security-site/month/event/chiba.html

教育によるフィッシング対策（5）

- 今後、教育が必要となるであろう対象
  - 高校生(15-18)、高齢者（60-)
- まだ研究されていない教材の様式
  - アニメーション化
    - 防火教育、交通安全教育アニメ

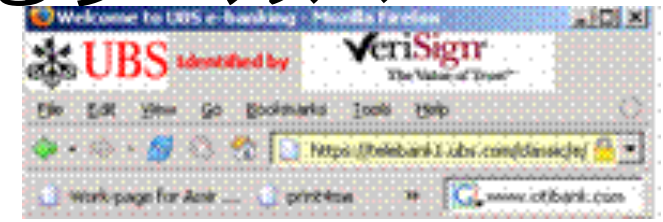
注意喚起・インタフェースによるフィッシング対策 (1)

- 見るべきところは証明書ですが・・



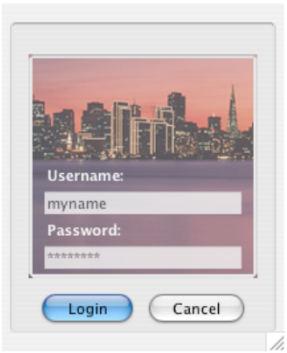
注意喚起・インタフェースによるフィッシング対策 (2)

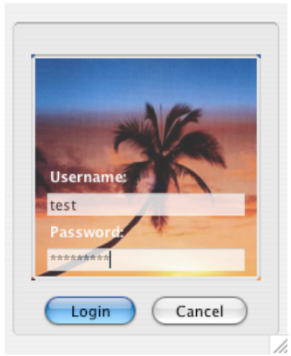
- アドレスバーの情報を強調するツールバー
  - SSL の情報を表示
  - ドメイン情報を表示
  - 特定のウェブサイトであることを表示（例：Account Guard)
- 「本物」との見分けやすさ

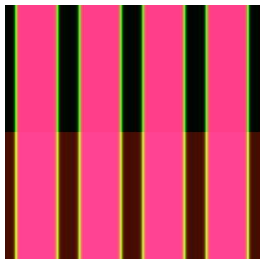


E. Herzberg, “Trustbar”, 2004

Netcraft Toolbar



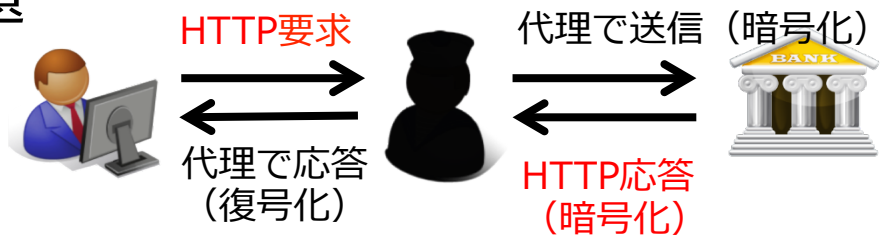




R. Dhamija. “Battle Against Phishing”, 2005

注意喚起・インタフェースによるフィッシング対策 (3)

- HTTP Mutual Authentication
  - Man-In-The-Middle問題



  - MITMに耐えられるには

  - IETF (httpauth WG)で議論されている
    - Mutual Authentication Protocol for HTTP
    - クライアントの実装は 2015年3月
    - サーバの実装は 2015年4月

注意喚起・インタフェースによるフィッシング対策 (4)

- Extended Validation SSL 証明書
  - 実社会のエンティティとの結びつきの強化

- DNSSECとの連携
  - DANE/TLSA Verification (RFC6698)

背景
・認証局の危殆化(compromise)
例：DigiNotar事件（2011）

・DNSSECの運用(2010)

注意喚起・インタフェースによるフィッシング対策 (5)

Google Chrome 36

Title: The site's security certificate is not trusted!

You attempted to reach example.com, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, especially if you have never seen this warning before for this site.

Google Chrome 37

Title: Your connection is not private

Attackers might be trying to steal your information from example.com (for example, passwords, messages, or credit cards).

1. 専門用語を避ける
2. 簡潔性を重視
   （正確性とのトレードオフ）
3. 具体的なリスクを描写

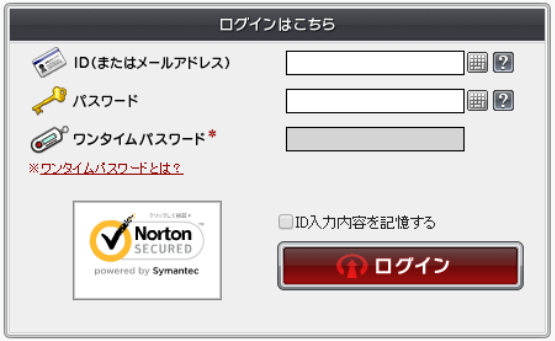
A.P. Felt "Improving SSL Warnings: Comprehension and Adherence", 2015

注意喚起・インタフェースによるフィッシング対策 (6)

- 多要素認証
  - 持ち物認証
  - パスワード以外の記憶型認証
    - ジェスチャ認証

- 利用の促進が課題
  - オンラインゲームの場合「セキュリティトークン」を使うと、ゲーム内で特典がもらえるという対応

スクウェアエニックス社の場合



NECOMA

注意喚起・インタフェースによるフィッシング対策 (7)

- サイバー社会における信頼の担保
  - サーバの証明書とサイトの証明書
- パスワードに変わるものと Usability, Deploy-ability, Security

J. Bonneau "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes", 2012

- 様々なエンドユーザ
  - 赤＝危険、緑＝安全で本当にいいのか
  - 視覚障がい者はどうすれば分かるのか

検知によるフィッシング対策 (1)

- 検知技術は大きく3通り
  - ブラックリスト型のURLフィルタリング
    - ユーザがアクセスするURLを、フィッシングサイトのURLデータベースと照合
    - 検知精度は60% - 70% (2007)から 40%へ (2009)
  - ホワイトリスト型のURLフィルタリング
    - 正規サイトのURLデータベースと照合
  - ヒューリスティクスによる検知
    - フィッシングサイトらしさを計算し、閾値と比較
    - Uselessという評価 (2007) からの70%へ (2009)

Y. Zhang et al, “Phinding Phish: Evaluating Anti-Phishing Tools”, 2007
S. Sheng et al, “An Empirical Analysis of Phishing Blacklists”, 2009

URLの分析

- あやしいURLの特徴
  - ドメイン名の代わりにIPアドレスを用いる
  - 正規サイトと視覚的に似ている
    - paypal.comに対するpaypai.com, paypak.com, paypay.com …
  - 記号が多い
    - http://www.paypal.com.brah.brah.brah.brah.....
    - http://paypal.com@/webcmd.run.org/

DNS 登録情報の分析

- レジストラに登録されてからの期間が短い
- TTL が短い
- ホスティング先の地理情報がおかしい
  - 正規サイトのコンテンツと視覚的に似ている

IP アドレスの分析

- レピュテーション
  - WebサーバのIPアドレス
  - Webサーバの存在するAS番号

コンテンツの分析

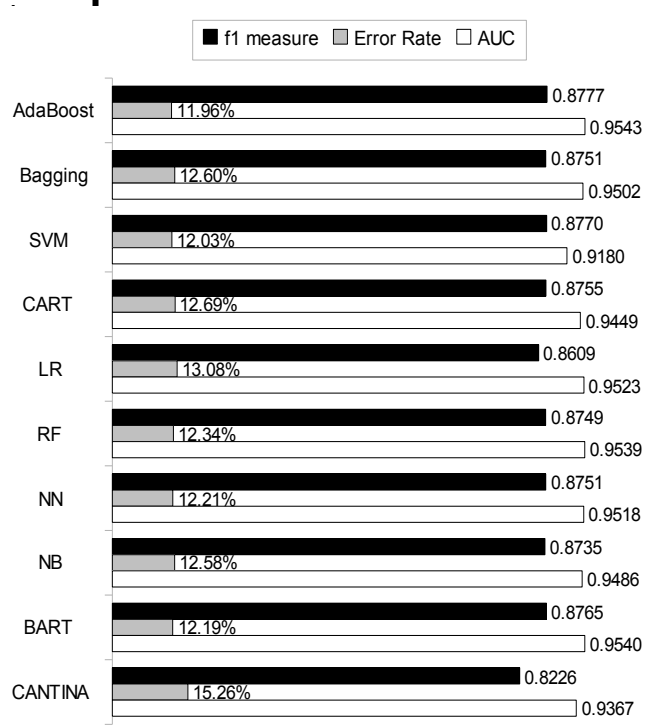
- 人気が低い
  - 自然言語解析によりキーワードを抽出
  - Googleで検索する
  - 正規サイトは上位にくるが、フィッシングサイトは上位に来ない
- アーカイブされていない
- コンテンツの類似性

検知によるフィッシング対策 (2)

- 二値分類問題への置き換え

	H_1	H_2	H_3	H_4	H_5	H_6		H_T	Actual Conditions
Site #1	1	0	1	1	1	1		1	phishing
Site #2	1	0	0	0	0	1		0	phishing
Site #3	0	1	0	1	1	1		0	phisl
Site #m	0	1	0	0	0	0		0	legiti

- パターン認識の問題
  - 機械学習による判別



検知によるフィッシング対策 (3)

- 個人に特化したフィッシングサイトの検知
  - 個人向けURLホワイトリスト
- 各ユーザに合わせた調整
  - ユーザ固有の弱点
  - ユーザの心理状態
  - ユーザの行動のリスク

検知によるフィッシング対策 (4)

ユーザの意思決定を分析に加える

弱判定器

ユーザの真贋判定における意思決定（フィッシングか否か）は、少なくとも二値を返す判定器と捉えられる

結合方法

Boosting には、弱点を補強するように重み付けを行う理論的特徴がある

$$D_{t+1} = \frac{D_t(i)}{Z_t} \times \begin{cases} e^{-\alpha_t} \ if \ h_t(x_i) = y_i \\ e^{\alpha_t} \ if \ h_t(x_i) \neq y_i \end{cases}$$

機械学習を用いて各個人ごとに調整する

- ユーザ固有の弱点の補強
- Personalization:求められるユーザ各個人向けの調整

Personalization

任意のエンドユーザにとって
間違えやすいウェブサイトを
正しく判定できる判定器が
高い重みを獲得する

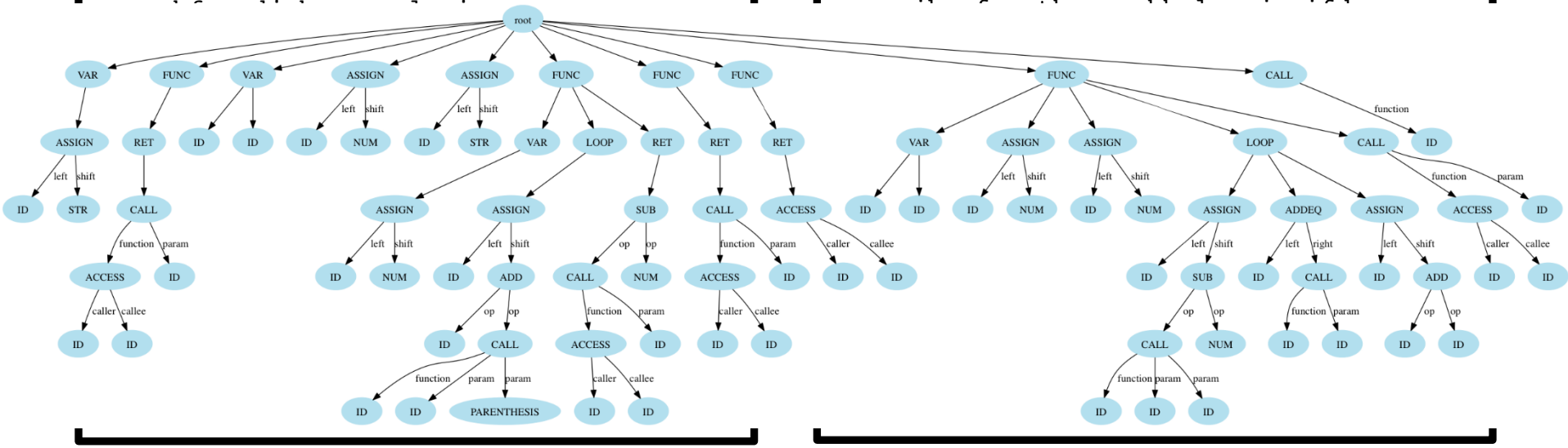
D. Miyamoto et al, “HumanBoost: Utilization of Users' Past Trust Decision for Identifying Fraudulent Websites”, 2009
H. Pareek et al, “Human Boosting”, 2013

検知によるフィッシング対策 (5)

- 難読化の類型化

```
var ftspzxjwygbc =
"07300785076907840775078207860702077807670780077307870767077307710731077607670788076707850769078407750782078.....
(snip)
function mljbkqwugvy() {
```

```
var ihuaplwebvcjo =
"013901940178019301840191019501110187017601890182019601760182018001400185017601970176019401780193018401910195.....
(snip)
function okuaqebt() {
```



検知によるフィッシング対策 (6)

- フィッシング検知とマルウェア検知
  - 自然言語解析の壁
  - 日本語の壁
- 解析時間に対する要求
  - ウェブの8秒ルール

NECOMA

フィッシングサイト対策の10年

Principle: Supporting Users' Decision-Making

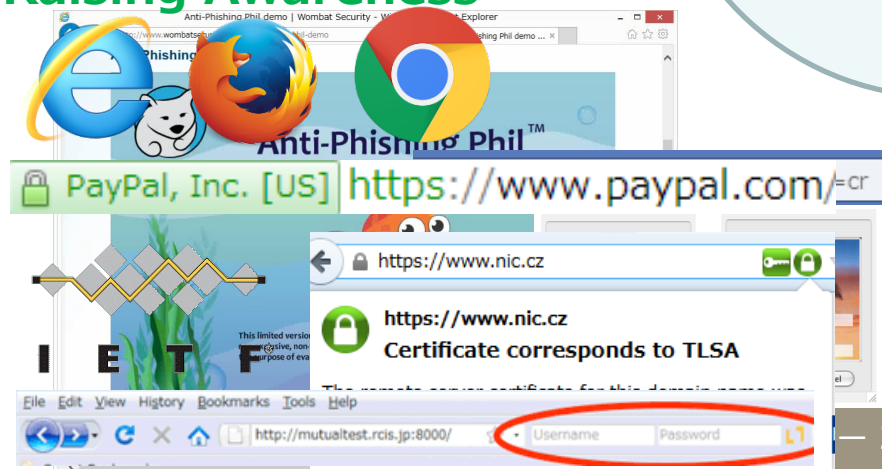
Education
- Educational materials

Raising Awareness
- User Interface for Trust

Detection
- Warning suspicious websites

Education

Raising Awareness

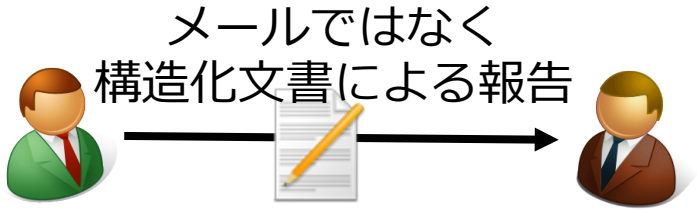


L: 1 (phishing)

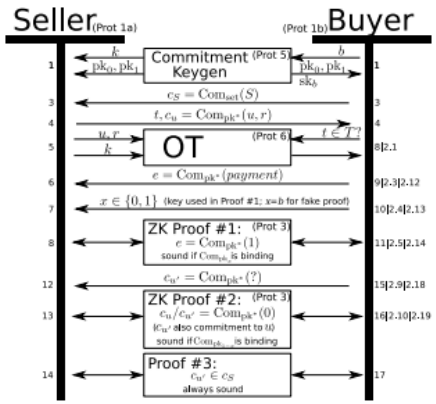
Detection

フィッシングサイト情報の共有

- コーディネータ間との情報共有
  - IODEF 及び IODEF の拡張によるフィッシング報告
    - APWG のフィッシング報告ツールに採用
    - RFC5070/RFC5901
    - IETF MILE WGで標準化が続く
  - STIX/TAXI による脅威情報共有



- フィッシングサイト閉鎖事業者の情報共有
  - このサイトを知っているかどうかに
    ゼロ知識証明を利用



T. Moore “The Phish Market Protocol: Securly Sharing Attack Data Between Competitors”, 2009

NECOMA

フィッシングメールの対策 (1)

- 似て非なるスパムとフィッシングメール

Buy Viagra for Lowest Cost on Net - Order Viagra Online 100mg, 50mg for Cheapest Price on Net and get Free Pills, we accept Visa cards Safe & Secure Processing since the year 1999 http://...../

The security questions and answers of PayPal account were changed on 21 Sep. 2013.

If you did not authorize this change, please contact us immediately using the phone number found on the following page:

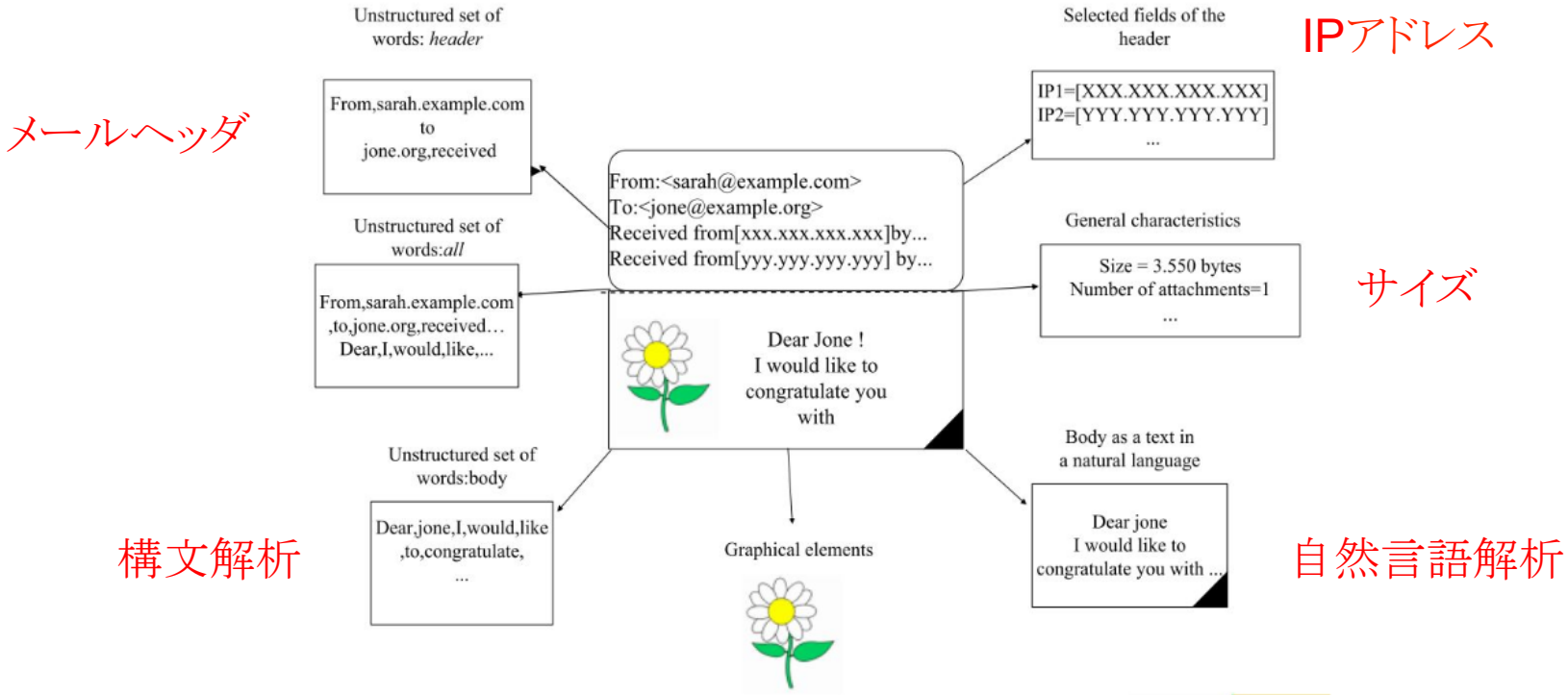
https://www.paypal.com/uk/login/

Thank you for using PayPal!
The PayPal Team.

Please do not reply to this email. This mailbox is not monitored any you will not receive a response. For assistance, lo in to your PayPal account and click the Help link located in the top right corner of any PayPal page.

フィッシングメールの対策 (2)

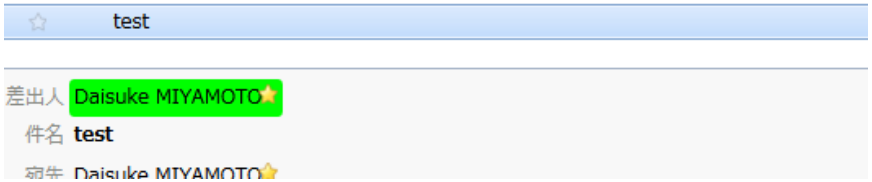
- メールに含まれるURLの解析
- メールヘッダの解析



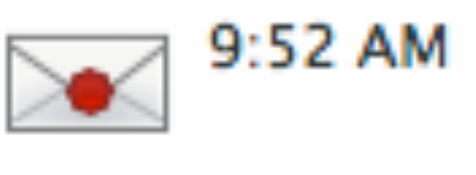
A. Almomani et al, "A Survey of Phishing Email Filtering Techniques", 2013

フィッシングメールの対策 (3)

- DNS 情報を使った信頼性向上
  - DKIM / Verifier
  - SPF



- アカウントの証明書

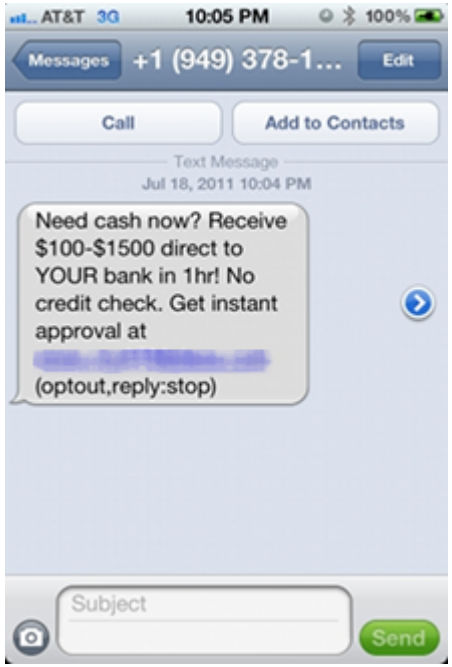


- ウェブメーラーの機能追加

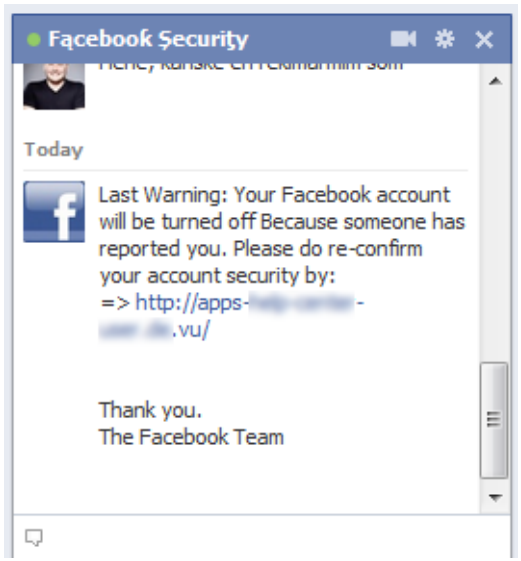
メールによらないフィッシング

- SMS / IM

SMS



IM



- Voice Phishing
  - 別名
    - Vishing
    - Voice over Phishing
    - 電話詐欺（韓国）
    - 振り込め詐欺（日本）
  - ウェブサイトも不要

NECOMA

マルウェア対策とフィッシング

- マルウェアに感染したPCのフィッシング対策は困難
  - Man-In-The-Browser
    - マルウェアがブラウザの通信を監視
    - 銀行にログインすると通信（セッション）を
      乗っ取り、ユーザの送金手続きの宛先を任意の振込先に改ざん
  - Pharming
    - Hostsファイルを書き換える
    - 「一度だけ動作して消える」パターンもある
- 感染が前提条件の場合の対策
  - 複数のデバイスを使った確認
  - トランザクション署名

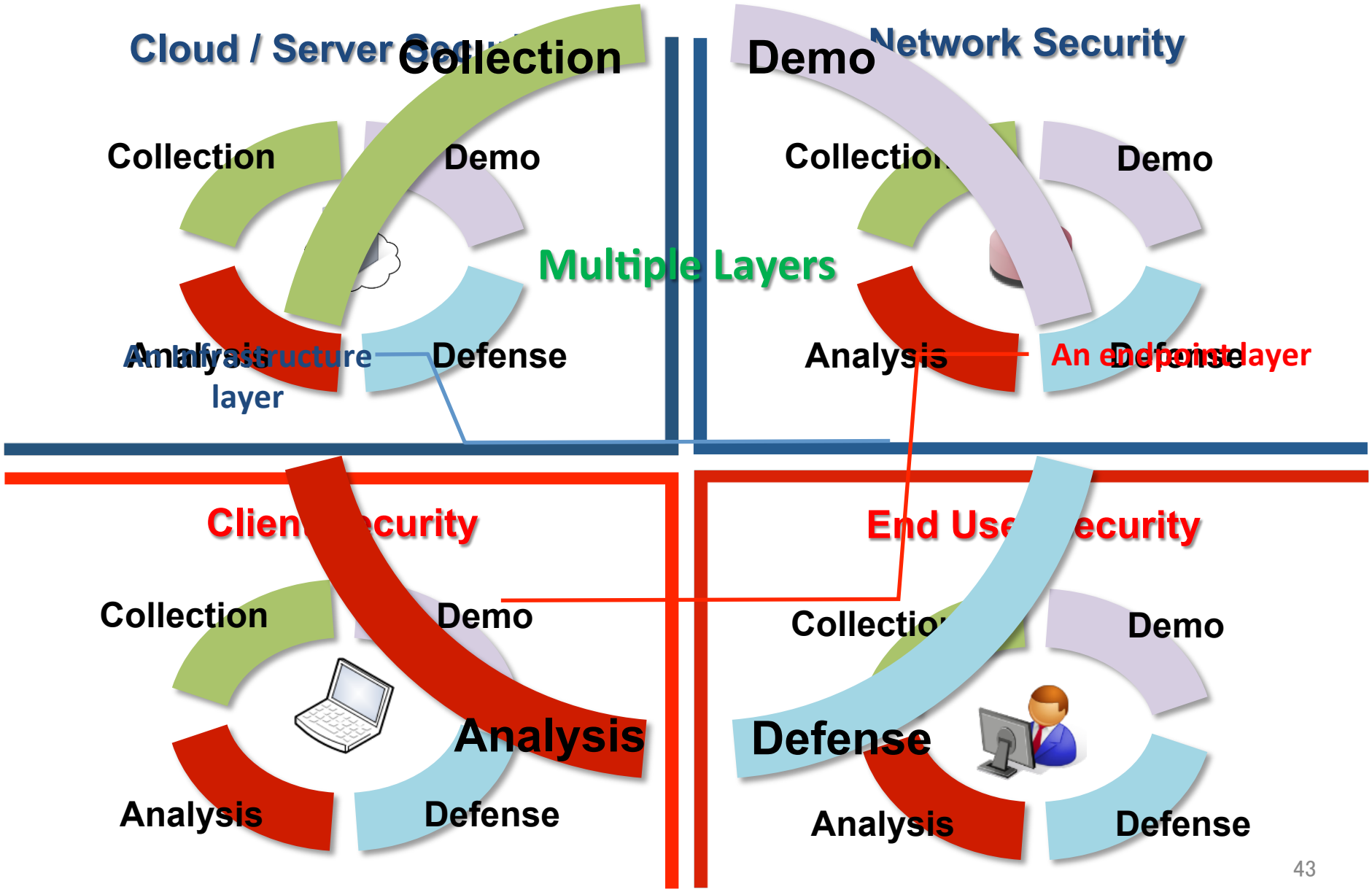
NECOMA

フィッシング対策研究の最先端 (NECOMAの場合)

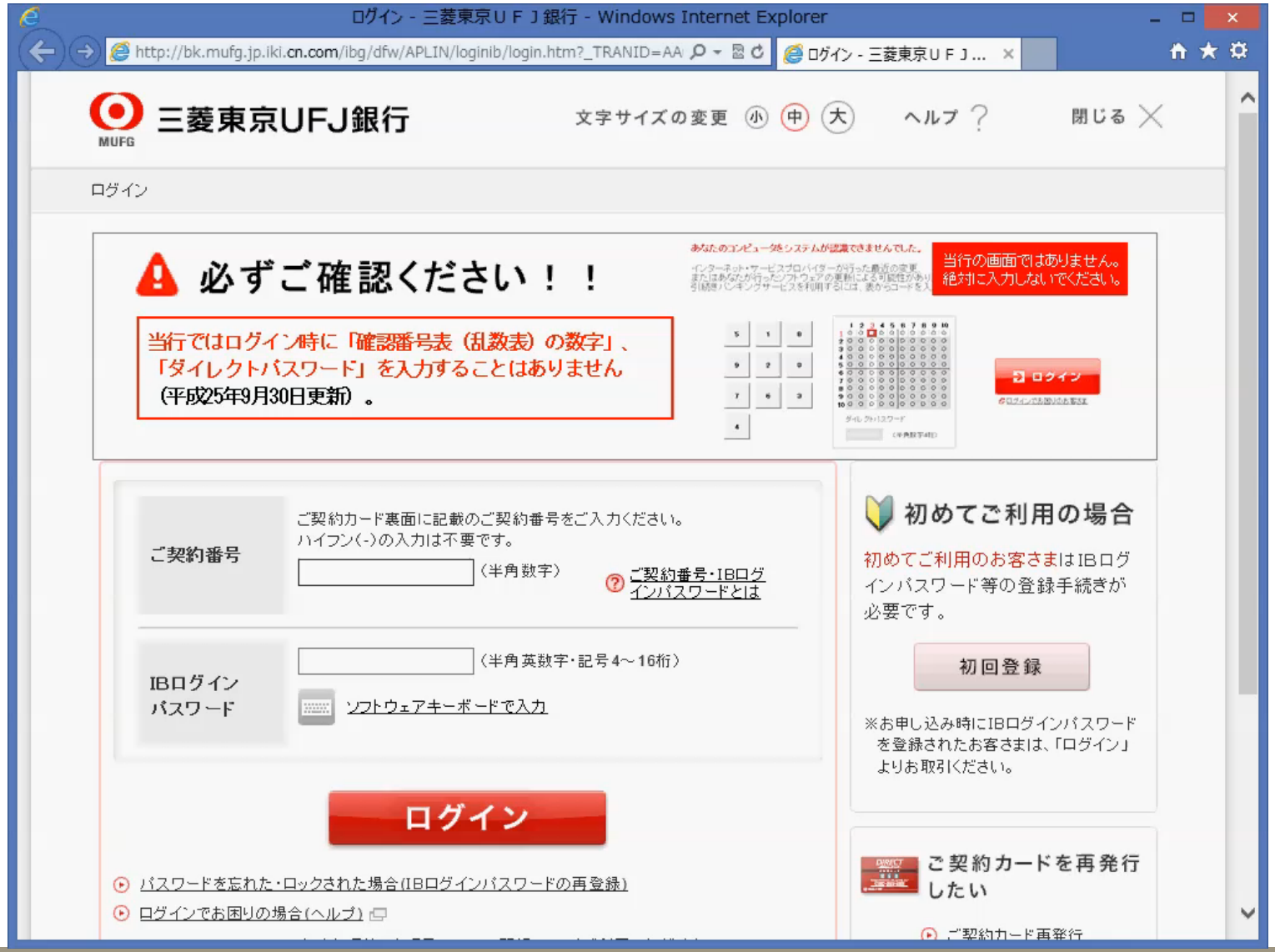
NECOMAとは？

- NECOMAプロジェクト (Nippon-European Cyberdefense-Oriented Multilayer threat Analysis)では、欧州委員会 FP7 プログラム (Seventh Framework Programme) と総務省 戦略的国際連携型研究開発推進事業の日欧 ICT 協調課題である「サイバー脅威に対する回復性強化のためのサイバーセキュリティ」に取り組んでいます（平成25年度～27年度）

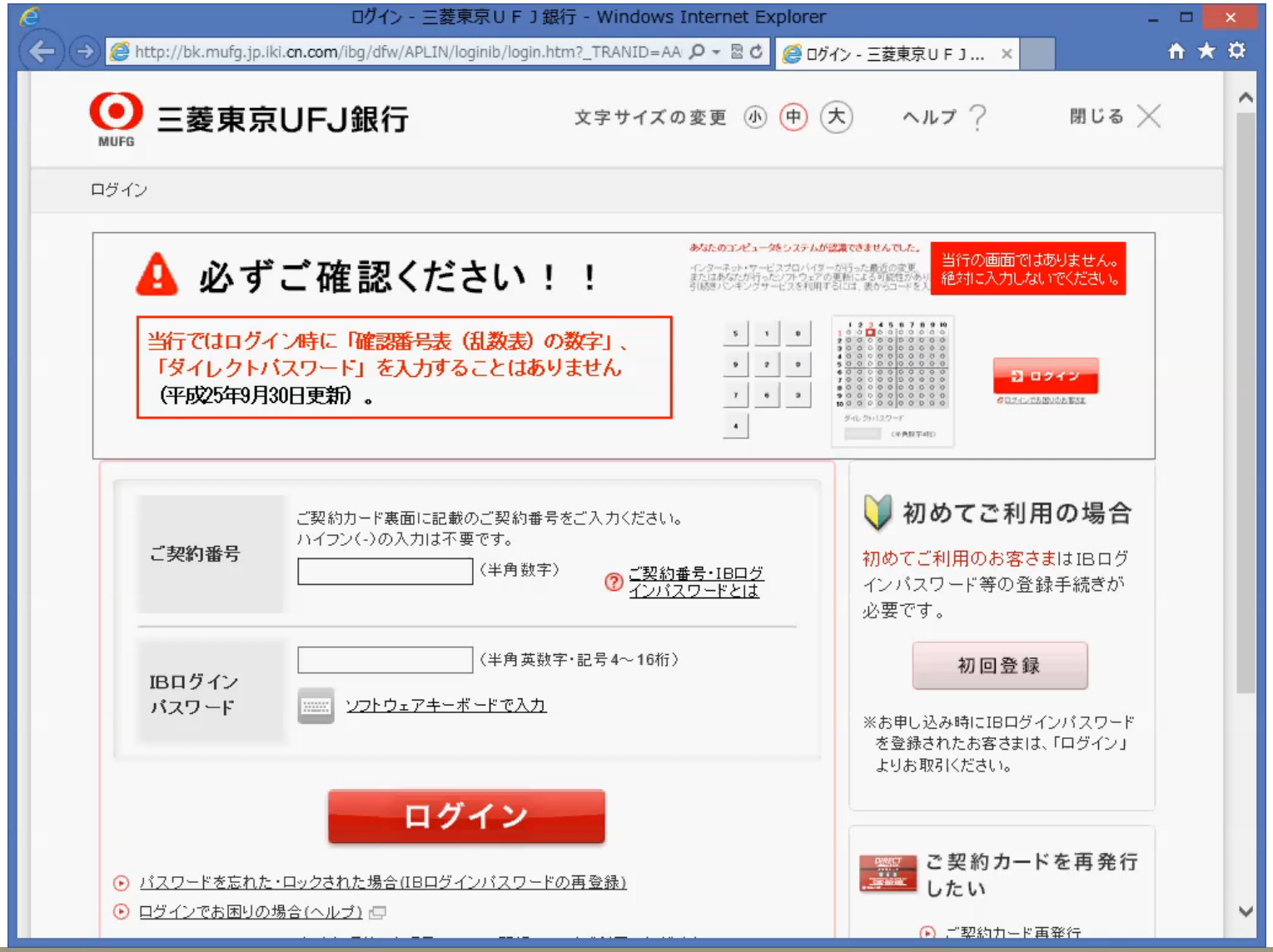
NECOMA


Collection
Demo
Collection
Demo
Analysis
Defense
Multiple Layers
Demo
Collection
Demo
Analysis
Defense
An endpoint layer
Collection
Demo
Analysis
Defense
Collection
Demo
Analysis
Defense

熟練者の視線解析（偽サイト）

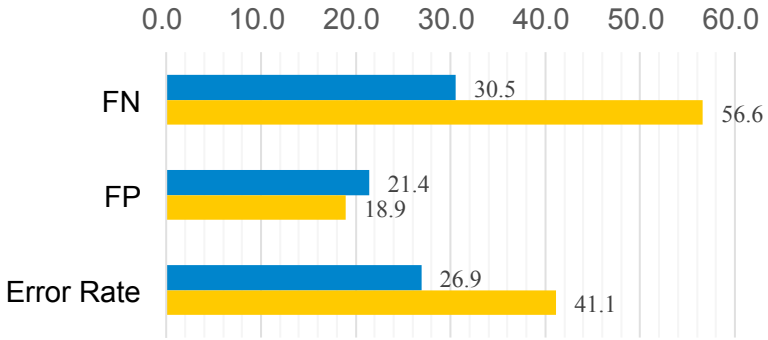


初心者の視線解析（偽サイト）



初心者と熟練者の違い

- 視線の特徴
  - 熟練者
    - アドレスバーに表示されるURL や SSL 情報から分析する
    - 認識にかかる時間が短い
  - 初心者
    - コンテンツに注力する
    - アドレスバーを見ない
- アドレスバーを見る/見ない効果
  - アドレスバーを見た場合
  - アドレスバーを見ない場合
- これまで何度も言われていますが
  - アドレスバーを確認するべき



セキュリティの習慣 (1)

- セキュリティ習慣
  - 情報を入力する前にアドレスバーを見ましょう

- 教育への効果
  - URLやセキュリティの知識は、アドレスバーを見ない限り働かない

- 注意喚起への効果
  - URLやセキュリティの知識は、アドレスバーに表示されるため、アドレスバーを見ることが役立てられる

- 検知の結果
  - 素人かどうかを判別しやすくなる

- 利便性の欠如はそれほど高くないと思われる

セキュリティの習慣 (2)

- 習慣は、無意識下においても動作する

PayPal

Account Status Update.
Log in to your paypal as soon as possible

Hello

Recently, there's been activity in your PayPal account that seems unusual compared to your normal account activities. Please log in to PayPal to confirm your identity and update card information.

We're concerned that someone is using your PayPal account without your knowledge. Recent activity from your account seems to have occurred from a suspicious location or under circumstances that may be different than usual.

What do I need to do?

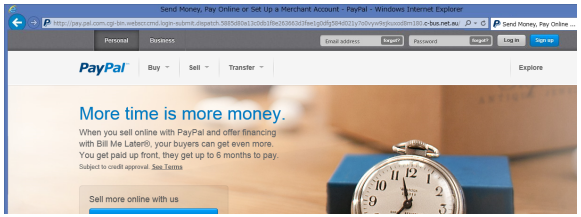
- **Click here**
- **Log in to your PayPal account as soon as possible. We may ask you to confirm information you provided when you created your account to make sure you're the account holder. We'll then ask you to change your password and security questions.**

Yours sincerely,
PayPal

アカウントの凍結

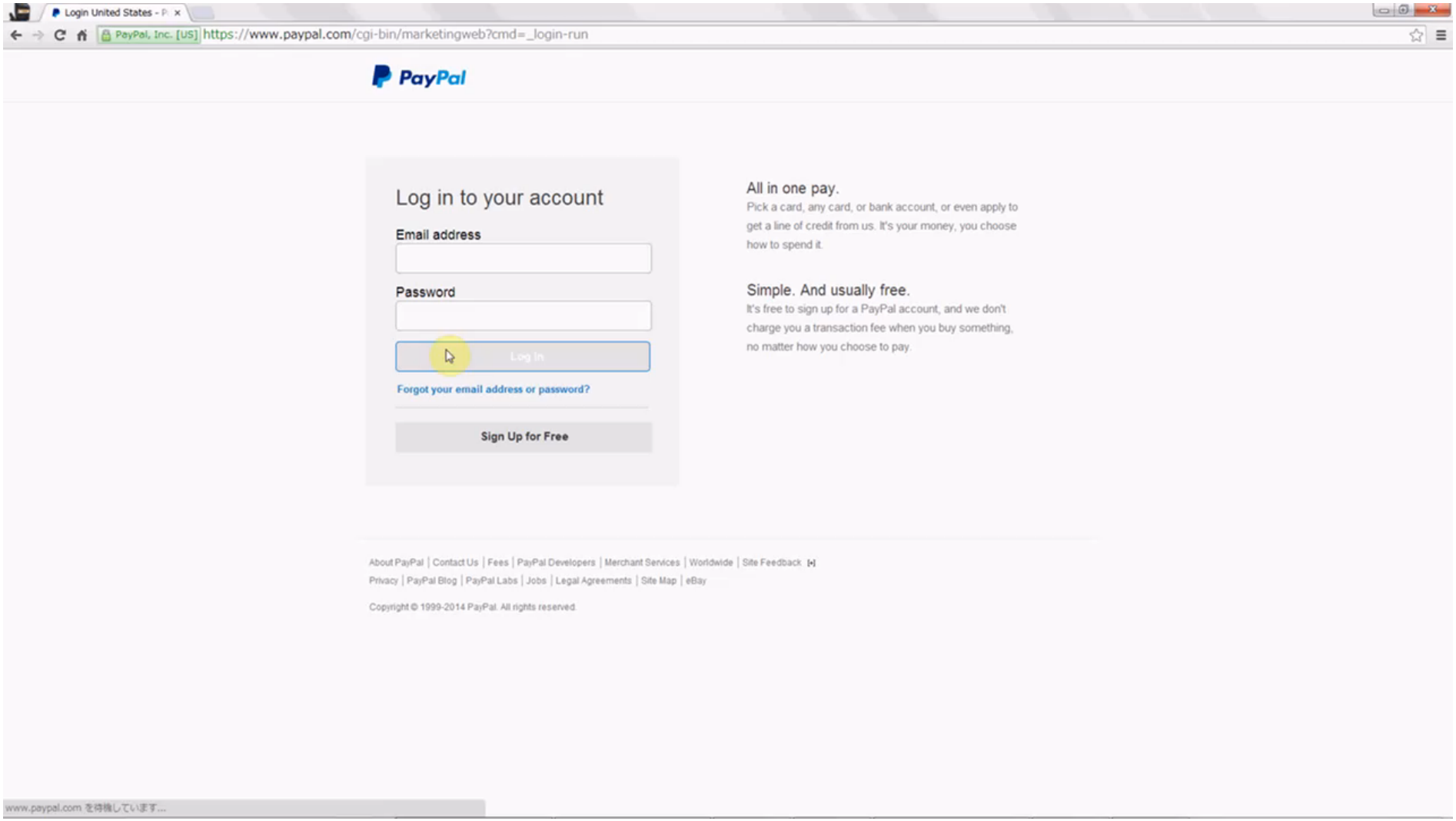
目的は「凍結」された
アカウントの確認であって
セキュリティではない

ログインして確認したい



無意識化でも動作する習慣を身につけさせるには？

アドレスバーを確認する習慣を身につけさせる研究



D. Miyamoto “EyeBit”, 2014

そしてパラダイムシフトへ

- 既存の研究

意思決定のサポート

情報

意思決定に役立つ情報を提示

Education **Attention** **Detection**

- 未来の技術へ

意思決定プロセスのチェック

認知心理学における活動分析技術

Cognitive task analysis	
Blinking, EOG (electrooculography) [Veltman 1998, Wilson 2003]	Gaze tracking [Marshall 2003, Zhai 1999]
Pupil dilation [Marshall 2002]	Facial warmth [Veltman & Vos, 2005]
Voice stress [Rothkrantz 2004]	Respiratory [Veltman 1998, Wientjes 1992]
Blood pressure [Veltman 1996, Miyake 2000]	EEG (electroencephalogram) [Wilson 2001, Prinzel 1999]
Skin conductivity [Haag 2004]	EMG (electromyography) [Lundberg 1994, Karthikeyan 2012]
Gesture recognition [Ehlert 2003]	Facial expression [Kuilenburg 2005, Jeniffer 2007]

視線分析とフィッシング対策 (1)

- そもそも、何を見たかを調査するのは重要
- 認知心理学から裏付けると・・
  - 目線の動きと精神状態異常
    [Crawford 2005, Noris 2007]
    - サッケーディック
    - 凝視
  - 目線が動いている中に意思決定しない
    [Irwin 2007]
  - サッケーディック反応から高負荷を推測可能
    [Tokuda 2011]

視線分析とフィッシング対策 (2)

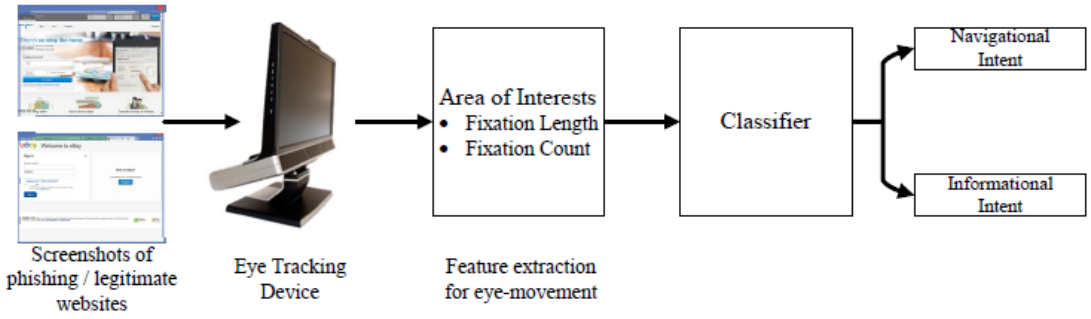
- サッケーディック反応を取得するには
  - サンプリングレート の問題
- 個人毎のキャリブレーションが必要
  - 赤外線を照射し、瞳の反応を取得
  - 非装着の場合
    - キャリブレーションが頻繁に必要な場合がある
  - 装着式の場合
    - キャリブレーションの問題はそうでもないが、サンプリングレート300Hzを満たすことが難しい

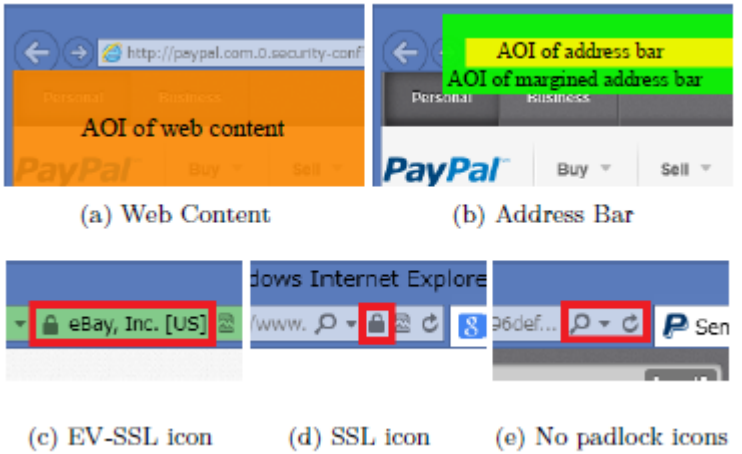
視線分析とフィッシング対策 (3)

視線分析とフィッシング対策 (4)

- 視線の意図
  - Informational Intention: 意図に基づいて閲覧
  - Navigational Intention: 特に意図なく閲覧

- フィッシングサイト認識との相関





(a) Web Content (b) Address Bar

(c) EV-SSL icon (d) SSL icon (e) No padlock icons

NECOMA

ユーザの心理とセキュリティ

- 「人」に対する理解が必要
  - ネットワークセキュリティ
    - ネットワークの知識が必須
  - エンドユーザを守るセキュリティ
    - エンドユーザの知識が必須？
- 日本国内ではセキュリティ心理学とトラスト研究会
  - 安心・安全という言葉の難しさ

フィッシングと多層解析

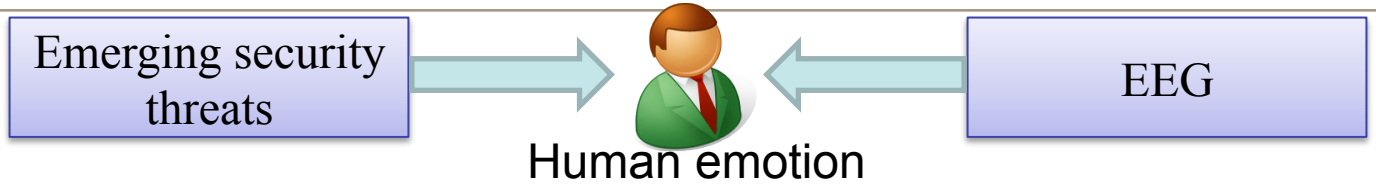
- SSL 解析との連携
  - SSL handshake の特徴との分析
- ボットネット解析との連携
  - IPアドレス/FQDN と悪用の形跡
- ちなみに NECOMA では・・
  - 全部のデータを Presto (Hadoop) 上に乗せて
  - 複数のデータを sql ライクに検索

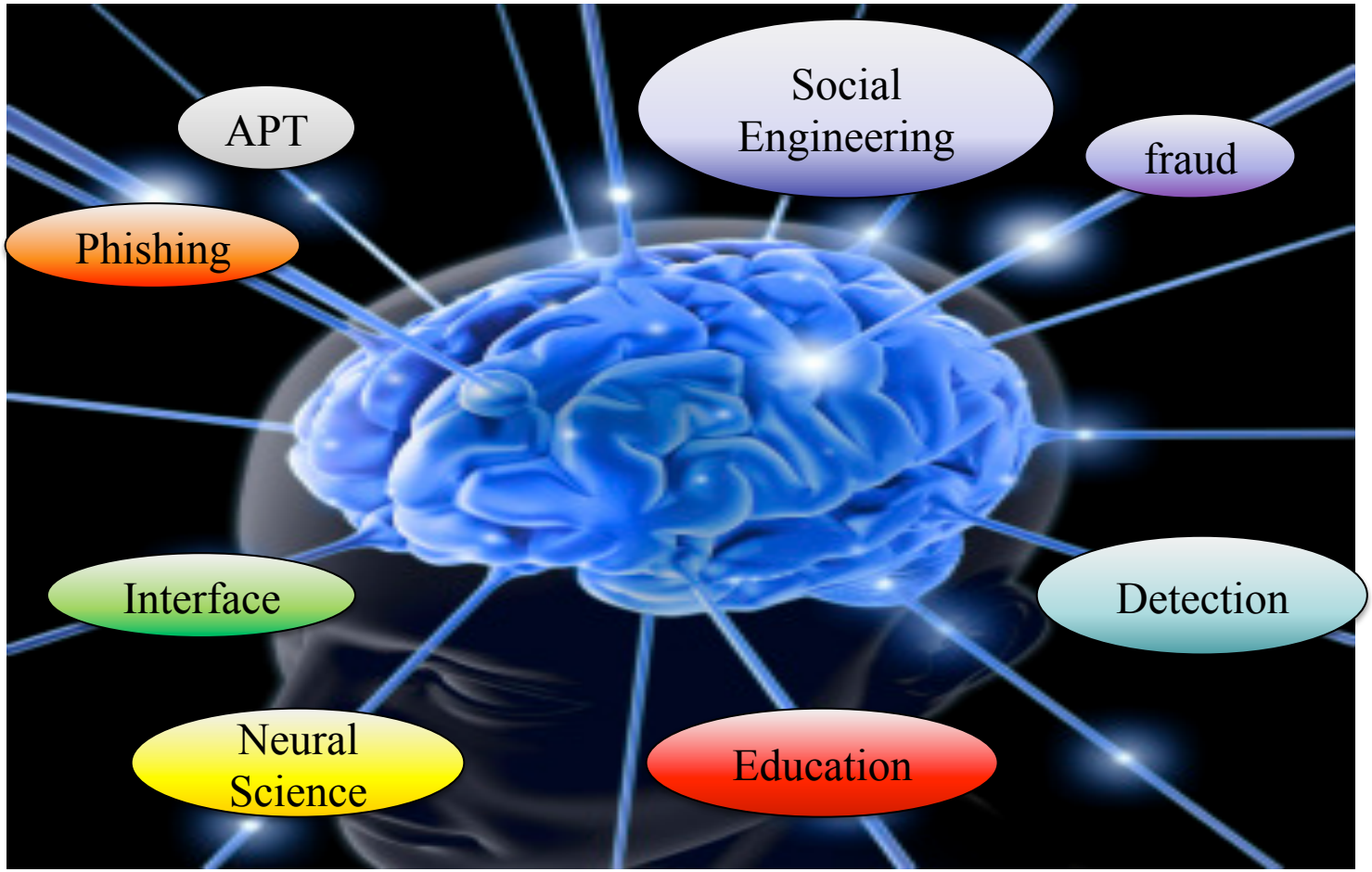
NECOMA

フィッシング対策研究の最先端の更にその先に見えてきた幻影

Daisuke MIYAMOTO, UTokyo, IIJ-labセミナー 2015年5月27日

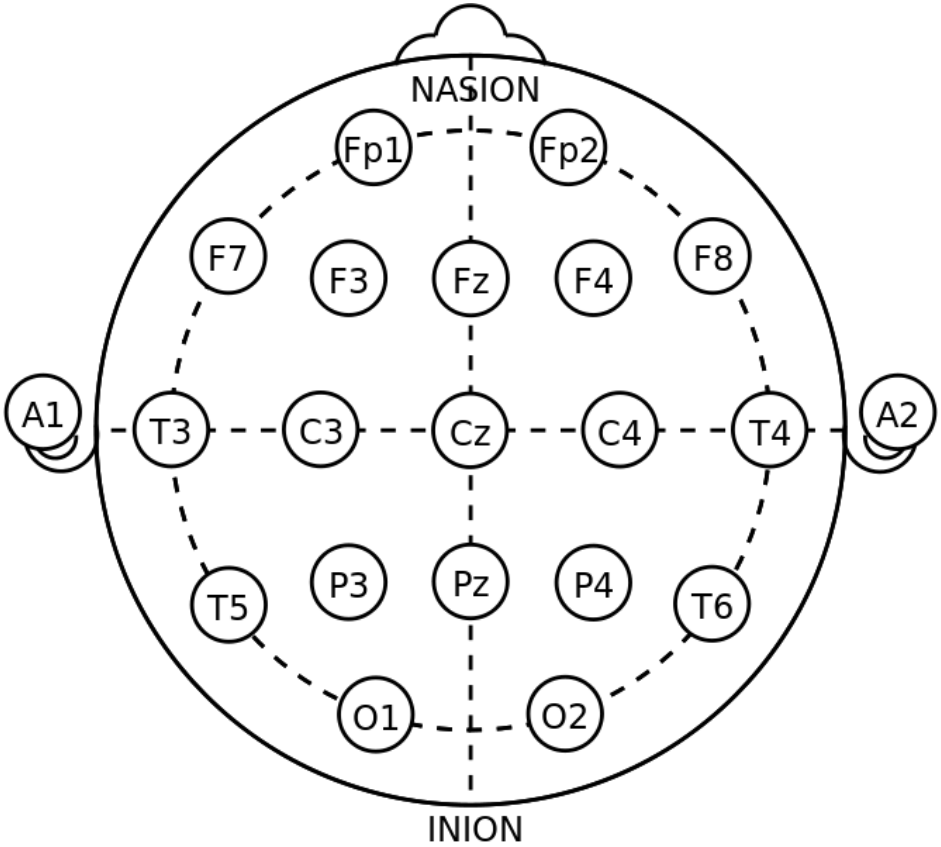
Neuro Cybersecurity の時代へ (1)





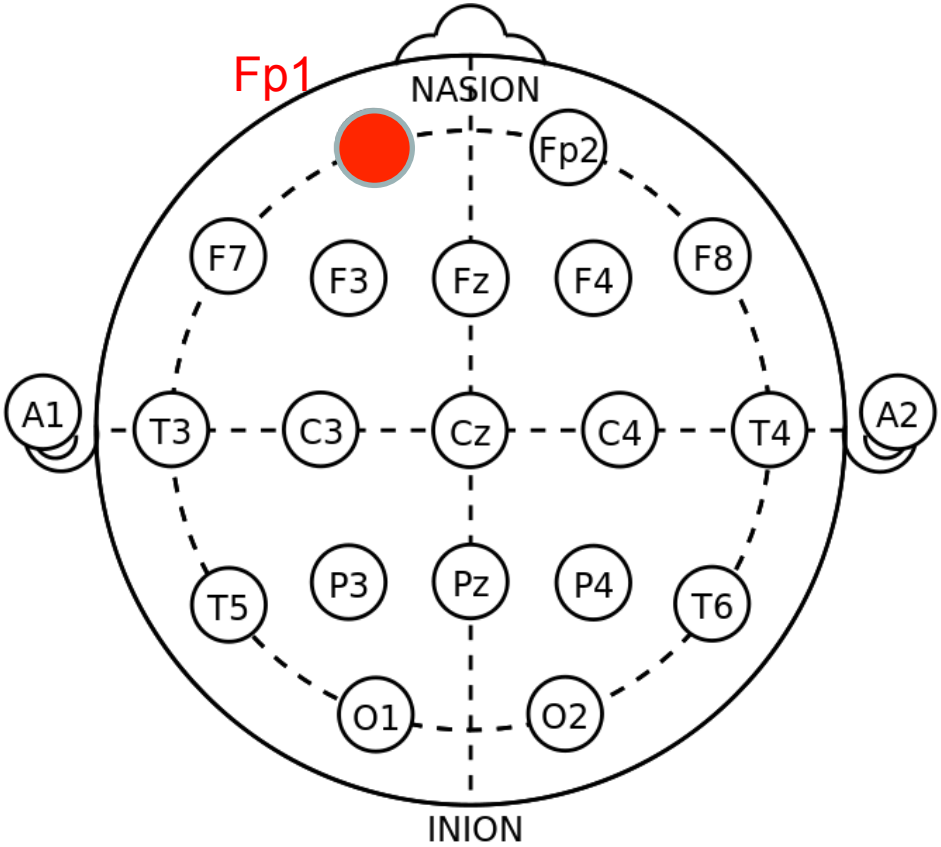
Neuro Cybersecurity の時代へ (2)

- EEG and 10-20 system



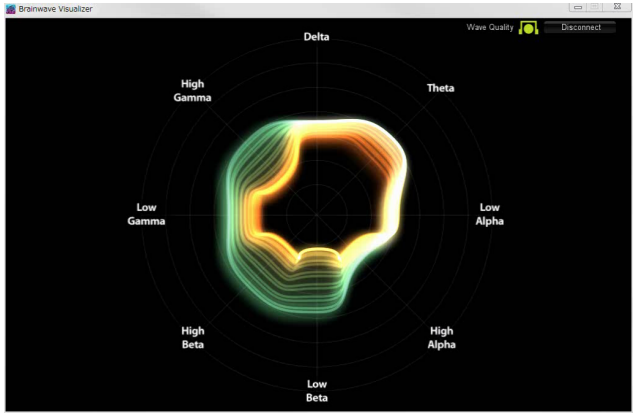
Neuro Cybersecurity の時代へ (3)

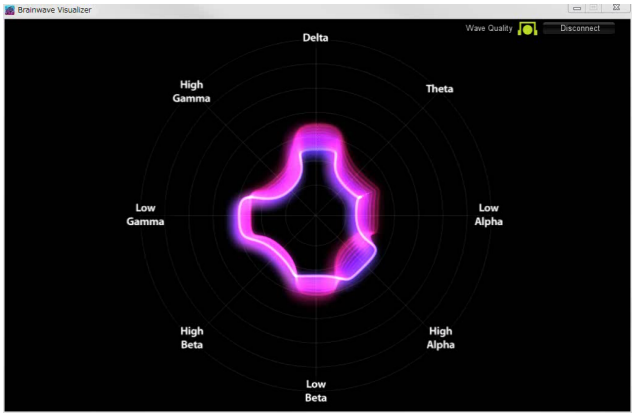
- Less than $100
  - One point (FP1)



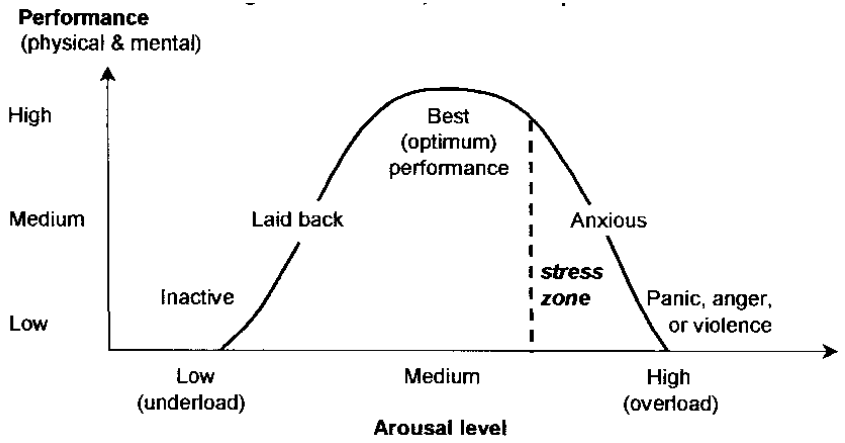
Neuro Cybersecurity の時代へ (4)

- 認知活動の計測と意思決定予測





- ストレス予測

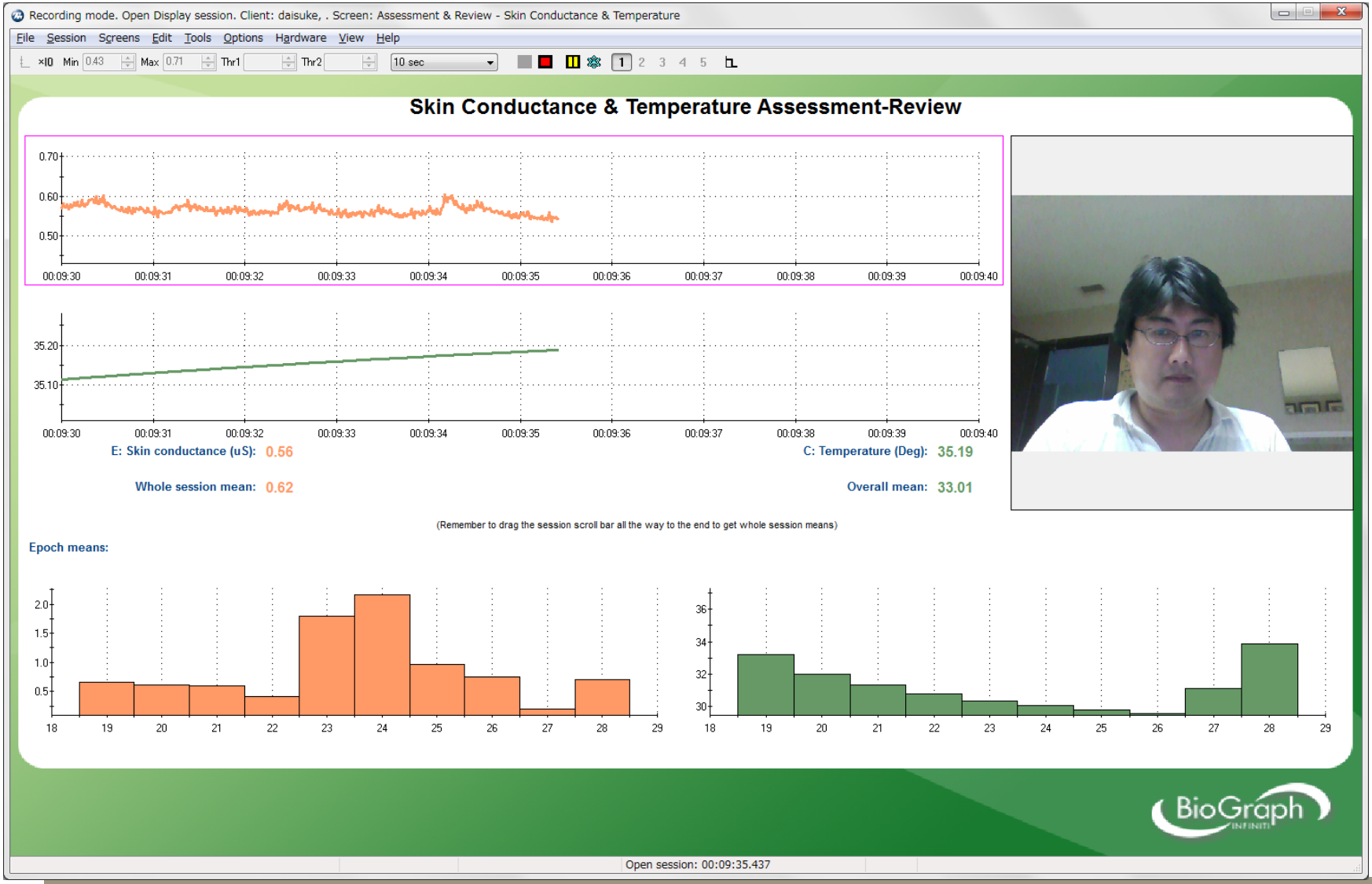


Neuro Cybersecurity の時代へ (5)

- 高度な情報処理活動の観測

- 問題点
  - 利用している想定環境がPCの前であるため、電磁波の影響を受けやすい
  - 汗、皮脂による影響を受けやすい
  - 皮膚電位、まばたきなどによって生じるノイズ除去

皮膚電位・温度とフィッシング対策 (1)



皮膚電位・温度とフィッシング対策 (2)

- 緊張による皮膚電位の変化
- 体温の増加（特に顔の体温）[Ora 2010]
- 筋電位との関係

プライバシーへの配慮 (1)

- 観測可能な生体情報
  - 情報の取り扱いについての異なる規定
    - 医療分野、脳神経科学
    - 情報技術
  - “個人特定可能” の意味の違い
    - 匿名性
    - 技術的進化

プライバシーへの配慮 (2)

1. 社会的受容
   - インフォームドコンセント
     - システムの利用者がベネフィットとリスクを両方とも理解していること
   - 認知タスク分析によるメリット
     - セキュリティの向上
   - システムを用いるリスク
     - 意志決定パターンをシステムが知ること
   - ガイドラインの公表
     - 目的、ゴール、データ使用方法など

プライバシーへの配慮 (3)

2. データの機密性
   - 集積したデータの暗号化
   - データ転送における機密性

3. ユーザへの安全性
   - システムの誤作動時における安全性
   - ネットワーク障害時における安全性

プライバシーへの配慮 (4)

- 資料
  - Guidelines considered in Japan
    - Brain Machine Interface (BMI)
    - Brain Computer Interface (BCI)
    - Heart to Heart Science (HHS)
  - Society for Neuroscience (SfN)
    - http://www.sfn.org/member-center/professional-conduct/sfn-ethics-policy
  - National Institute of Health (NIH)
    - http://videocast.nih.gov/pdf/ohrp_appendix_belmont_report_vol_2.pdf

人間の認知の限界 (1)


5554:AVD_for_Nexus_One
15:08
hiroba.dqx.jp.osxk.co.vu/a
SQUARE ENIX ACCOUNT

人間の認知の限界 (2)

- スクリーンが小さいと判別困難な文字がある

www.japánnetbänk.co.jp

アクサン記号 “á”

ウムラウト “ä”

www.japánnetbänk.co.jp

キリル語の “a”

人間の認知の限界 (3)

フォント	アルファベットの “a”	キリル文字の “a”
Arial	www.japannetbank.co.jp	www.japannetbank.co.jp
Times New Roman	www.japannetbank.co.jp	www.japannetbank.co.jp
Century	www.japannetbank.co.jp	www.japannetbank.co.jp
メイリオ	www.japannetbank.co.jp	www.j a pannetbank.co.jp
ＭＳ明朝	www. japannetbank. co. jp	www. j a pannetbank. co. jp
ＭＳゴシック	www. japannetbank. co. jp	www. j a pannetbank. co. jp

NECOMA

フィッシングサイト対策のすべて

Daisuke MIYAMOTO, UTokyo, IIJ-labセミナー 2015年5月27日

フィッシングサイト対策のすべて

- 「アドレスバーを確認する」がすべて
  - エンドユーザの意思決定をサポートするために教育、注意喚起・インタフェース、検知による解決が試みられてきた
  - 研究発表されたアイデアの多くは利用可能になっている
- 先端研究では
  - 「アドレスバーを確認する」習慣付け
  - 「ただしく判断しているか」を生体情報から分析する