Vol.2017-SPT-22 No.12
2017/3/13

セキュリティインディケータの改善による なりすましメール対策の提案と評価

伊藤 俊一郎[1,a)]　小林 和真[1]　門林 雄基[1]

概要：なりすましメールを手段としたサイバー攻撃の脅威が拡大している．既存対策では，メール送信者の認証結果をメール受信者に通知する，セキュリティインディケータが表示される．しかし，その有効性は充分に議論されていない．本研究では，画像を用いたセキュリティインディケータを提案するとともに，Web アンケートを利用したユーザ調査により，提案手法と既存対策のセキュリティインディケータを評価する．アンケート結果の分析により，提案手法は視認性等の面で優れ，またメール確認時にストレスを感じているユーザには，認知的負荷の少ないセキュリティインディケータが効果的であることがわかった．

キーワード：なりすましメール，セキュリティインディケータ，セキュア UI

Improving Security Indicator toward Mitigation of Spear-Phishing E-mail Threats

Ito Shun'ichiro[1,a)]　Kobayashi Kazumasa[1]　Kadobayashi Youki[1]

Abstract: The threat of cyber attack using spear-phishing e-mail is expanding. In the existing countermeasures, a security indicator that notifies the e-mail recipient of the authentication result of the e-mail sender is displayed on the e-mail. However, its effectiveness has not been fully discussed. In this work, we propose a security indicator using images and evaluate the security indicator of proposed method and existing method by using a Web questionnaire. The analysis of the questionnaire showed that the proposed method is superior in terms of visibility, a user who feels stressful when checking the e-mails tend to prefer security indicators with less cognitive load.

Keywords: Spear-phishing e-mail, Security indicator, Secure UI

1. はじめに

電子メールは人の通信手段として広く普及している．しかし，情報セキュリティ上の脅威が高いサイバー攻撃の手段として，メールが悪用されている [1]．メールをマルウェアの配送手段として利用するとき，特定の人物や組織になりすましてメールを送る，なりすましメールを使用することがある．日本においては，企業等を騙るなりすましメールが後を絶たず，なりすましメールの脅威は拡大している [2]．

なりすましメール対策としては，送信ドメイン認証や電子署名を利用したメール送信者の認証手法がある．メール送信者の身元の正当性を検証することで，メール送信者がなりすまされていないことを証明する．これらの既存対策においては，文字やアイコン等を利用することで，メール受信者に認証結果の情報を通知する．メール受信者は認証結果の情報を利用して，受信メールが正規メール，もしくはなりすましメールであるのかを識別する．このように，なりすましメールの脅威を軽減するためには，人とシステム間の情報伝達を担うユーザインタフェースでの対策も必要となる．しかし，既存対策のユーザインタフェースについて調査を行った結果，対策としての有効性が充分には検

[1] 奈良先端科学技術大学院大学
NAIST, Takayama-cho, Ikoma, Nara 630–0192, Japan
[a)] ito.shunichiro.in0@is.naist.jp

ⓒ 2017 Information Processing Society of Japan

図 1 送信ドメイン認証結果

図 2 DKIM Verifier による認証結果の表示

討されていないことがわかった．

本研究では，既存対策におけるメール送信者の認証結果をユーザに通知する機能（以下，「セキュリティインディケータ」という．）の問題点について分析するとともに，なりすましメール対策として効果的なセキュリティインディケータのあり方について検討し，新たなセキュリティインディケータを提案する．また，Web アンケートを用いたユーザ調査を行うことにより，提案手法および既存対策のセキュリティインディケータの有効性を評価する．

2. 関連研究

本章では，なりすましメール対策において用いられている，既存のセキュリティインディケータとその問題点について述べる．

2.1 送信ドメイン認証

送信ドメイン認証では，Sender Policy Framework（SPF）[3] や Domain Keys Identified Mail（DKIM）[4] が主な認証手法としてある．受信メールのドメイン情報から，メール送信元ドメインにメール送信者の身元の正当性を問い合わせる手法である．身元の正当性を保証する範囲は，以下に示すメールアドレスの下線部になる．

foo@example.com

送信ドメイン認証では，図 1 の下線部に示すように，メールヘッダに認証結果が表示される．しかし，すべてのユーザがメールヘッダを確認しているわけではなく，確認するにしても労力がかかる．

送信ドメイン認証の結果を可視化する方策として，Thunderbird ではアドオンが開発されている．DKIM Verifier[5] では，DKIM の認証結果に応じて，メール送信者欄の文字色や背景色が設定できるようになっている．図 2 は，送信ドメイン認証の結果に異常がないときに，メール送信者の背景色を緑色で表示した例である．認証結果に異常がある場合，初期設定では赤色で表示される．また，ThunderSec[6] では，SPF や DKIM 等の認証結果を通知バーにより表示している．図 3 は，受信メールの認証に成功したことを，黒色の通知バーと説明文で示している．異常がある場合には，赤色の通知バーと警告文が表示される．

図 3 ThunderSec による認証結果の表示

図 4 S/MIME による認証結果の表示

2.2 電子署名

電子署名の一つである S/MIME[7] は，公開鍵暗号方式を利用したメール送信者の認証機能を提供する．メール送信者は自らの秘密鍵を用いた電子署名を送信メールに付加する．メール受信者は，メール送信者の公開鍵を用いてメールに含まれる電子署名を検証し，メール送信者の身元の正当性を確認することができる．身元の正当性を保証する範囲は，以下に示すメールアドレスの下線部になる．

foo@example.com

S/MIME では，図 4 に示すように，署名マークを用いて認証結果を示している．図 4 は，メーラーとして Thunderbird を使用している環境で表示される署名マークである．メールの形をしたアイコンに赤丸を表示することで，受信メールに付加されている電子署名の検証に成功したことを示している．検証に失敗した場合には，赤丸にバツ印が付く．また，電子署名が付いていない受信メールでは，署名マークが表示されない．そのため，認証の有無は署名マークの有無で判別することになる．

2.3 既存のセキュリティインディケータの問題点

関連研究を調査した結果，なりすましメール対策における，既存のセキュリティインディケータの有効性が充分議論されていないことがわかった．セキュリティインディケータの有効性は，使用するメールユーザにより評価される必要があるが，調査した範囲では示されていない．一方で，フィッシングサイト対策としてのセキュリティインディケータについては，ユーザ調査による評価を行った研究が多く公表されている．3 章において，フィッシングサイトを識別するためのセキュリティインディケータについて調査し，提案手法の参考とする．

3. 効果的なセキュリティインディケータの検討

本章では，なりすましメール対策として効果的なセキュリティインディケータについて検討する．

3.1 フィッシングサイト判別のためのセキュリティインディケータ

フィッシングサイト判別のためのセキュリティインディケータに関する研究では，Felt らの研究 [8] がある．Web

サイトを閲覧するためのブラウザは複数存在するが，アクセス先の Web サイト（正規もしくはフィッシングサイトの可能性がある Web サイト）で，表示されるセキュリティインディケータが異なる．ユーザ調査による評価として，同じ意味を持つセキュリティインディケータでも，ユーザが捉える意味が異なることを示している．Wu らの研究 [9] では，セキュリティインディケータの表示方法や表示位置によって，フィッシングサイトの被害率が変化していることを示している．また，画像を用いたセキュリティインディケータによる，フィッシングサイト判別の効果を調査した研究もある [10]．画像の大きさや点滅等の設定によって，フィッシングサイト判別率に変化があることを示している．

画像を用いたセキュリティインディケータの実例としては，インターネットバンキングがある．フィッシングサイトへのユーザ名やパスワードの入力を防止するために，ログイン画面にセキュリティイメージと呼ばれる画像を表示する [11]．ユーザがセキュリティイメージを事前に設定することで，正規サイトのログイン画面では設定したセキュリティイメージが表示され，フィッシングサイトのログイン画面では表示されないため，ユーザがフィッシングサイトを判別できる．

3.2 セキュリティインディケータの要件

なりすましメールは人を欺くことで，マルウェア感染を引き起こす．攻撃者は人を欺くために，興味のあるメール内容，時間的圧力，権威がある人（上司等）のなりすましなどを利用して，人の脆弱性を突いてくる．巧妙ななりすましメールを受信したユーザは，平常時であれば気付く異常な情報を認識することができずに，エラーを引き起こす可能性が大きくなる．エラーとは，マルウェアが含まれた添付ファイルを実行する行為などである．このとき，セキュリティインディケータにより，受信メールの危険性を的確にメール受信者に伝えることができれば，人のエラーを局限できる．

認知科学には，行為の 7 段階モデル [12] と呼ばれる，ユーザが物理的世界に働きかけて何らかの目的を果たそうとするときに要求される処理の段階を表したモデルがある．このモデルは人の行為を理解して，ユーザインタフェースデザインの指針を決定する際に使用することがある．なりすましメールを識別する行為をこのモデルに当てはめ，ユーザのエラーを局限するために重要なセキュリティインディケータの要素を分析した．セキュリティインディケータとして重要な要素は以下の 3 つである．

(1) 存在の認識
(2) 正確な意味の伝達
(3) 認知的負荷の軽減

存在の認識とは，メール受信者にセキュリティインディケータの存在を知覚させることである．受信メールがなりすましメールであった場合には，危険を示すセキュリティインディケータが表示されることになる．しかし，メール受信者がその存在を知覚できなかった場合，受信メールの危険性を認識することができない．結果，正規メールとして扱うことにより，マルウェア感染を引き起こすことになる．よって，セキュリティインディケータを設定するにあたり，存在の認識を考慮する必要がある．

正確な意味の伝達は，セキュリティインディケータが示す意味をユーザに確実に伝えることである．セキュリティインディケータがメール受信者に知覚されたとしても，その示す意味を誤って解釈すれば意味がない．例えば，なりすましメールであることを示すセキュリティインディケータを知覚したとしても，正規メールであると誤って解釈すれば，なりすましメールの被害に遭うことになる．そのため，セキュリティインディケータが持つ意味を正確にメール受信者に伝えることは重要な要素である．

認知的負荷の軽減とは，セキュリティインディケータの意味を解釈する際に，負荷を軽減することである．正確な意味の伝達で述べたように，メール受信者に正確な情報を伝えることが重要である．しかし，情報量が多すぎる，認識するのに時間がかかるなど，ユーザに認知的負荷をかけるのは，優れたユーザインタフェースとは言えない．セキュリティインディケータを解釈する際に，認知的負荷が増えてしまうと，メールを読むというタスクの時間が増すとともに，メール利用時の不快感も増える．よって，認知的負荷を軽減したセキュリティインディケータが必要となる．

4. 画像を用いたセキュリティインディケータの提案と評価

本章では，3 章で調査した結果をもとに提案するセキュリティインディケータの概要と，その有効性の評価について述べる．4.1 節において，提案するセキュリティインディケータのデザインを，表示位置，表示内容，表示方法の観点から決定する．4.2 節では，セキュリティインディケータについて，Web アンケートを用いて評価した結果を示す．

4.1 画像を用いたセキュリティインディケータのデザイン

4.1.1 表示位置

メール確認画面において，メール受信者がセキュリティインディケータを知覚できる箇所としては，図 5 に示す 4 つが考えられる．なりすましメールの特性上，メール送信者のなりすましに関する情報を強調することが自然な対応付けとなる．よって，図 5 の (1) が，メール送信者の認証結果を表示するのに最適な箇所である．

4.1.2 表示内容

セキュリティインディケータが受信者に伝えるべき情報を検討する．送信ドメイン認証や電子署名の既存対策で

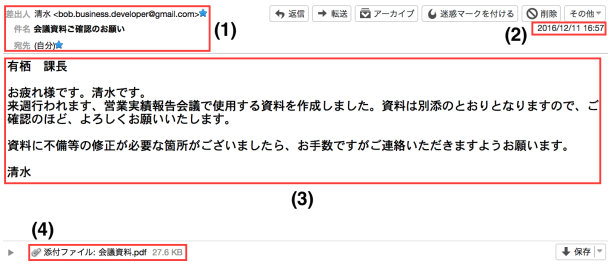

図 5 セキュリティインディケータの表示位置

は，ユーザに伝えるべき情報という観点で問題がある．その問題とは，認証が行われていないメールに対するセキュリティインディケータが存在しないことである．調査した既存対策では，以下の二つの情報しか示されていないものがある．

(1) メール送信者の認証が成功
(2) メール送信者の認証が失敗

メール送信者の認証手法をメーラーに導入していないユーザは，セキュリティインディケータが表示されていないメールを普段扱っていることになる．このようなユーザが対策を導入したとき，認証されていないメールと従来の通常のメールを誤認識する可能性が大きい．本来，メール送信者の認証が行われていないメールに対しては，注意を払うべきである．しかし，認証が行われていないメールであることを示すセキュリティインディケータが表示されない場合，メール受信者が知覚する認証の有無に関する情報が曖昧になる．よって，メール送信者の認証が行われていないメールについても，セキュリティインディケータを表示する必要がある．

以上を踏まえて，提案手法のセキュリティインディケータとして，メール受信者に提示する内容は以下の 3 種類とする．

(1) メール送信者の認証が成功
(2) メール送信者の認証が失敗
(3) メール送信者の認証が行われていない

4.1.3 表示方法

ユーザに受信メールの情報を知らせる方法としては，パッシブインディケータとアクティブインディケータの二つが考えられる [13]．パッシブインディケータは，ユーザのタスクを遮らずに警告を行うインディケータである．アクティブインディケータは，ユーザのタスクを遮ることで，警告を強制的に知覚させる．本研究においては，既存対策で多く使用されているパッシブインディケータの有効性と比較評価するために，提案手法においてもパッシブインディケータを用いる．具体的なインディケータとしては，画像を使用する．理由として，人は文字の認識よりも画像の認識を得意としており，かつフィッシングサイトの判別には，セキュリティイメージという画像を用いたセキュリティインディケータがあるが，メール送信者の認証には画像を用いたセキュリティインディケータはない．評価においては，提案手法と既存対策の有効性を比較することで，画像を用いたセキュリティインディケータの有効性をより明確に示せる．

図 6 提案する 3 種類のセキュリティインディケータ

図 7 提案するセキュリティインディケータの表示例

4.1.1 項〜4.1.3 項の検討結果をもとに提案する，画像を用いたセキュリティインディケータを図 6 に示す．各画像の意味は左から，メール送信者の認証が成功したことを示す画像，メール送信者の認証が失敗したことを示す画像，メール送信者の認証が行われていないことを示す画像である．また，メール画面におけるセキュリティインディケータの表示例は，図 7 のとおりである．

セキュリティインディケータの画像を設定するにあたり，アフォーダンスを考慮した画像を検討した．アフォーダンスとは心理学において，モノの属性とそれをどのように使うことができるかを決定する主体の能力との間の関係と定義されている [14]．人という主体が画像というモノを見たときに，その画像が持つ意味を正しく認識できるように，アフォーダンスを考慮した画像を用いた．具体的には，緑十字は安全を意味する画像として，黄色時にドクロマークは危険を意味する画像として，疑問符は不明を意味する画像として設定した．また，メール受信者が各セキュリティインディケータを見間違えないようにするため，形や色を明確に区別した．

4.2 セキュリティインディケータの評価

提案手法およびなりすましメール対策において使用される既存対策のセキュリティインディケータの評価を行う．評価では，Web アンケートを用いたユーザ調査を行った．Web アンケートの概要は以下のとおりである．

ⓒ 2017 Information Processing Society of Japan

- 調査対象者
  パソコン上で業務等に関するメールを扱うユーザ
- 調査期間
  2016 年 12 月 16 日〜12 月 19 日
- 回答者
  - WIDE プロジェクト研究会参加者
  - 本学インターネット工学研究室所属の学生
- 有効回答数
  31 件
- 調査対象のセキュリティインディケータ
  - 画像（提案手法）
  - 差出人背景色の強調（図 2）
  - 通知バー（図 3）
  - 署名マーク（図 4）
- 評価項目
  - セキュリティインディケータの視認性
  - セキュリティインディケータの正確な意味の伝達
  - メールを確認する環境におけるストレスの多寡
- 実験方法
  安全（メール送信者の認証に成功）もしくは危険（メール送信者の認証に失敗）を示すセキュリティインディケータが表示されたメール画面を提示し，評価項目に関する質問を行った．なお，セキュリティインディケータの持つ意味等は事前に通知していない．

評価項目の一つでもある，メールを確認する環境におけるストレスの多寡は，ユーザ特性として調査した．なりすましメールは人のエラーを誘引することで，マルウェア感染を引き起こす．セキュリティインディケータはエラーを引き起こさないように設定されるが，エラーの発生率にはストレスの影響があると言われている．そのため，Web アンケートの回答者を，「ストレスが多いユーザ群」と「ストレスが少ないユーザ群」に分類し，ストレスの多寡による効果的なセキュリティインディケータへの影響を調査した．

セキュリティインディケータの有効性は，評価項目に関する質問により，以下の 3 つの観点から評価した．また，各評価に最も該当するセキュリティインディケータを合わせて記述する．

(1) 効果的なセキュリティインディケータ
視認性が良く，セキュリティインディケータが持つ意味を正確に認識できたユーザ数を調査
- 安全: 提案手法
- 危険: 提案手法，通知バー

(2) 意味を誤認識されたセキュリティインディケータ
セキュリティインディケータが持つ意味を反対に捉えたユーザ数を調査
- 安全: 署名マーク
- 危険: 通知バー

(3) 意味が不明なセキュリティインディケータ
セキュリティインディケータが持つ意味に対して，「わからない」と回答したユーザ数を調査
- 安全: 署名マーク
- 危険: 差出人背景色の強調

5. 考察

4.2 節の Web アンケートの評価結果をもとに，調査したセキュリティインディケータの特徴を分析するとともに，なりすましメール対策として効果的なセキュリティインディケータについて考察する．

提案手法では，視認性や正確な意味の伝達という点で，既存対策よりも有効性が高いということがわかった．しかし，安全を示す画像の意味を「わからない」と回答したユーザが比較的多かったため，画像の再考が必要である．差出人背景色の強調を行うセキュリティインディケータは，意味を「わからない」と回答したユーザが多かった．これは，メールの認証結果を判断する材料が色のみであるため，意味を識別できないユーザが多かったと考える．しかし，誤認識が少なかったことから，緑色が安全性を示し，赤色が危険性を示すという，色の使い分けは適切であったと言える．通知バーのセキュリティインディケータは，視認性等の面で比較的優れているという結果が得られた．しかし，安全を示す黒い通知バーについては，赤い通知バーに比べて視認性が低いという結果が得られた．通知バーや説明文の色を改めて検討することで，視認性等が改善できると推測する．また，危険を示す通知バーは誤認識も多かったため，説明文が必ずしもユーザに読まれているとは言えない現状であることがわかった．署名マークのセキュリティインディケータは，全体的に有効性が低いという結果が得られた．原因は，安全と危険を示す各セキュリティインディケータの明確な区別が行われていないこと，そしてメールの差出人情報等から離れた位置にインディケータが表示されているためであると推測する．よって，Thunderbird で使用される S/MIME の認証結果の表示方法は，改善すべきである．

ストレスの多寡による，効果的なセキュリティインディケータへの影響が一部見られた．ストレスの多いユーザ群には，提案手法のように認知的負荷の少ないセキュリティインディケータが効果的であることがわかった．反対に，通知バーのように認知的負荷の大きいセキュリティインディケータでは，意味の誤認識が多いという結果が得られた．この結果より，ストレスの少ないユーザ群に比べて，警告文を読んでいないことが判明した．よって，ストレスの多いユーザ群には，認知的負荷の少ないセキュリティインディケータを設定することで，より効果的になりすましメールの判別が行えるものと考える．

次に，メール送信者の認証手法に適したセキュリティイ

ⓒ 2017 Information Processing Society of Japan

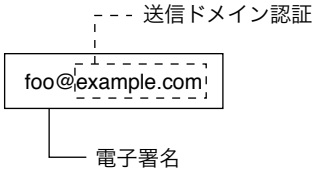

図 8 メール送信者の認証手法によるメールアドレスの認証範囲

ンディケータについて述べる．2 章で示したように，メール送信者の認証手法ごとに，メールアドレスの認証する範囲が異なる．図 8 にその違いを示す．

図 8 からわかるように，認証手法が保証する範囲に応じたセキュリティインディケータが必要となる．電子署名のように，メールアドレス全体に対する認証結果を表示する場合は，提案手法の画像，署名マークおよび差出人背景色の強調は適切である．しかし，送信ドメイン認証のように，ドメインを認証している場合は，すべてのメールアドレスを認証しているかのようなセキュリティインディケータの表示は避けるべきである．例えば，DKIM Verifier ではメールアドレスすべての背景色を強調しているが，認証範囲と強調範囲が矛盾する．また，画像等のセキュリティインディケータを使用する場合は，メールアドレスのドメインを認証していることを示す説明が別に必要となる．画像等のセキュリティインディケータの表示のみでは，メールアドレスの認証範囲が不明確なためである．同様に，通知バーを表示するセキュリティインディケータは，説明文によってメールアドレスの認証範囲を示すべきである．以上のように，メール送信者の認証結果を示す場合は，各認証手法の特徴に応じたセキュリティインディケータを使用する必要がある．

6. まとめと今後の課題

本研究では，メール送信者の認証結果を表示するセキュリティインディケータに着目し，既存対策の問題点について分析するとともに，画像を用いたセキュリティインディケータを提案した．ユーザ調査により評価した結果，提案手法は，視認性や正確な意味の伝達という点で，既存対策に比べ優れていることを示した．一方で，S/MIME で使用される署名マークは，有効性が低いという結果が得られたため，別の表示方法を検討すべきであると考える．また，ストレスの多いユーザ群には，認知的負荷の少ないセキュリティインディケータが効果的であることがわかった．このことから，ユーザに適したセキュリティインディケータを使用することが，より効果的なセキュリティインディケータの運用方法と言える．また，メール送信者の認証手法を分析した結果から，メールアドレスにおいて，メール送信者のなりすましを識別できる範囲が異なることがわかった．よって，セキュリティインディケータを使用する際には，メール送信者の認証手法の特性に合わせた表示方法が必要である．

今後の課題として，長期的な使用を考えた場合のセキュリティインディケータの不快度や，馴化の影響を確認する必要がある．また，本研究において行ったアンケートとは異なる状況として，事前にセキュリティインディケータの意味を通知した場合の有効性も調査する必要がある．

謝辞 快く被験者実験に応じて下さいました，WIDE プロジェクト研究会参加者の皆様に感謝いたします．

参考文献

[1] 情報処理推進機構セキュリティセンター. 情報セキュリティ 10 大脅威 2016 個人と組織で異なる脅威、立場ごとに適切な対応を. https://www.ipa.go.jp/files/000051691.pdf. (2016 年 8 月 9 日閲覧).
[2] フィッシング対策協議会. フィッシングに関するニュース. https://www.antiphishing.jp/news/. (2017 年 1 月 31 日閲覧).
[3] D. Scott Kitterman. Sender policy framework (spf) for authorizing use of domains in email. Technical report, RFC 7208, 2014.
[4] Murray Kucherawy, Dave Crocker, and Tony Hansen. Domainkeys identified mail (dkim) signatures. Technical report, RFC 6376, 2011.
[5] Mozilla Foundation. DKIM Verifier. https://addons.mozilla.org/ja/thunderbird/addon/dkim-verifier/. (2017 年 1 月 10 日閲覧).
[6] Mozilla Foundation. ThunderSec. https://addons.mozilla.org/ja/thunderbird/addon/thundersec/. (2017 年 1 月 10 日閲覧).
[7] Sean Turner and Blake C. Ramsdell. Secure/multipurpose internet mail extensions (s/mime) version 3.2 message specification. Technical report, RFC 5751, 2011.
[8] Adrienne Porter Felt, Robert W Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo. Rethinking connection security indicators. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 2016.
[9] Min Wu, Robert C Miller, and Simson L Garfinkel. Do security toolbars actually prevent phishing attacks? In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pp. 601–610. ACM, 2006.
[10] Joel Lee, Lujo Bauer, and Michelle L Mazurek. The effectiveness of security images in internet banking. *IEEE Internet Computing*, Vol. 19, No. 1, pp. 54–62, 2015.
[11] The PNC Financial Services Group. An Added Layer of Security. https://www.pnc.com/en/security-privacy/added-layer-security.html. (2017 年 1 月 10 日閲覧).
[12] 加藤隆. 認知インタフェース. オーム社, 2002.
[13] Jason Hong. The state of phishing attacks. *Communications of the ACM*, Vol. 55, No. 1, pp. 74–81, 2012.
[14] DA ノーマン, 岡本明, 安村通晃, 伊賀聡一郎, 野島久雄. 誰のためのデザイン: 認知科学者のデザイン原論. 新曜社, 2015.

ⓒ 2017 Information Processing Society of Japan