情報セキュリティ対策の経済合理性評価

武田 圭史[†1]

概要：情報セキュリティ対策の採否を判断する際においてその費用対効果など有効性の評価が求められることがあるが，その評価に関する方法論は未だに確立されておらず経験もしくは伝聞等の情報に基づき主観的に行われることが多い．本稿ではセキュリティ対策の意思決定において適用可能な情報セキュリティ対策の経済合理性評価のフレームワークを提案する．

キーワード：リスク管理, セキュリティ設計, セキュリティ評価, 経済合理性, 意思決定

Evaluation of Economic Rationality on Information Security Measures

Keiji Takeda[†1]

Abstract: It has been expected to examine cost effectiveness at the time of decision making of introduction of security counter measures. However, methodology for such evaluation has not been established and often it is conducted subjectively based on one's experience or hearsay information. In this research framework for evaluation of economic rationality on information security measures would be proposed.

Keywords: Risk Management, Security Design, Security Evaluation, Economic Rationality, Decision Making

1. はじめに

企業など様々な組織における情報セキュリティに関する脅威の及ぼす影響が具体化するについてその対策のための組織的な取り組みが行われるようになり，その費用対効果や採用すべき対策に関する意思決定について経済的な観点からの評価が求められている．

情報セキュリティの経済性の評価に関してはこれまでも様々なアプローチが提案されているが，情報セキュリティに関する意思決定の現場においてそういったアプローチが十分に活用されているとは言い難い．

本稿では情報セキュリティ対策の経済性評価に関して従来の手法を踏まえた上で，今後そう言った評価手法を情報セキュリティにおける施策に関する意思決定の根拠として使用することを可能とすることを目指し，その試験的なフレームワークを提案し今後の議論の基礎とする．またより具体的な議論を進めるため，提案するフレームワークを適用したケーススタディとしてパスワードを一定期間内に変更するセキュリティ施策の経済合理性評価への適用を試みる．

情報セキュリティに関する施策は単純に経済合理性のみよって決定されるものではなく道義的責任を含む広義のコンプライアンス等様々要求事項によって意思決定されるべきものであるが，同時に経済合理性に欠く施策は経営者や利用者の理解を得られずその実現性や継続性の面から困難な状況が考えられる．

2. 情報セキュリティ対策の経済性分析

情報セキュリティ対策の意識決定における経済性の分析についてはこれまでにも様々なアプローチから提案が行われてきた．特に情報セキュリティに関する研究としては情報セキュリティの経済的側面を中心とする学際的な課題について議論する国際的なワークショップ The Workshop on the Economics of Information Security (WEIS)が 2002 年より継続して開催されている．また日本国内においても情報セキュリティに関連する学会においてしばしば経済学的なアプローチに関する研究発表が行なわれているほか，情報処理推進機構がセキュリティエコノミクスなど学際的なアプローチから情報セキュリティに関する調査研究を行う情報セキュリティ分析ラボラトリーが 2008 年に設立されている．

2002 年に発表された Gordon らによる論文[1]は企業等組織における情報セキュリティ投資に関する経済的な評価の視点の必要性を提示し以後議論の基礎となった．Gordon らはセキュリティ対策を講じることによって軽減されるセキュリティ被害の期待値の大きさを比較することによって最適なセキュリティ投資を決定するモデルを示した．

芝口ら[2]は情報セキュリティ対策によって追加的に発生する仕事量及び対策の徹底度という指標を用いて利便性

†1 慶應義塾大学
Keio University

低下コストと仕事量に注目したセキュリティ対策選定量を提案している．また呉ら[3]はプロジェクト環境におけるセキュリティ対策の組み合わせをプロジェクトの特性に応じて選定するための評価する方法を提案している．

こういった様々な視点から情報セキュリティに経済的な評価を試みる論文や研究の発表が行われているもののそういった評価方法が実際のセキュリティ対策の導入に適用されるケースはそれほど多くはない．その理由として考えられるのはこれらの経済的な評価モデルにおいてリスクの経済的価値（被害）の評価を行うために様々なリスク事象毎の発生確率とその事象が発生した場合に発生すると想定される被害の大きさの積で表現される期待値が用いられる場合が多い．ここに用いられる被害の大きさについては企業等の活動においてはある程度の精度の見積もりを立てることが可能である．少なくとも最低限どの程度の損失が発生し復旧のための費用が必要となるかを見積もることが可能である．しかしもう一つの変数となる事象の発生確率の見積もりについては適切な根拠をもって示すことは容易ではない．その理由は個々の情報システムが置かれている環境や利用形態はそれぞれ異なり，過去の発生事象から特定のシステムにおける情報セキュリティ事象の発生確率を定量的に示すことの妥当性が薄いためである．また外部の攻撃者によってもたらされる情報セキュリティの脅威事象に関しては単独または少数の攻撃者によって引き起こされるものも多くその場合そういった特定個人の意思に大きく左右され確率的な事象として現れにくいという面もある．

こういった点から情報セキュリティの脅威の見積もりにおいて特に発生確率に関しては，専門家の経験に基づく主観的な憶測に頼らざるを得ない面が限界となる．

情報セキュリティに関する対策の意思決定において経済的な評価モデルが意味がないわけではなく，まずある前提において複数の対策の投資対効果に関する相対的な比較を行うためのツールとして使用することができる．また仮定された事象の発生確率を前提とした上である対策の費用対効果を評価するためのツールとして使用することが可能である．

以降本稿では従来の提案を参考としつつ情報セキュリティ対策の経済合理性評価を行うための一般的なモデル化を行い，広く適否が議論をされているパスワードを一定期間以内に変更するというセキュリティ対策の評価を行いその妥当性について検証を行う．

3. 情報セキュリティ対策の経済合理性評価フレームワーク

情報セキュリティ対策の経済合理性を評価するフレームワークを検討する上で，本稿では組織におけるセキュリティ対策の組み合わせや総合的な評価を行うのではなく，特定の個々のセキュリティ施策の採否に関する検討を行う際に参考とすることのできる経済的な評価の枠組みを提示することを目的とする．ここではモデルを単純化するためにある回避すべきリスク事象 R_i が単位期間 T の間に発生する確率を P_i, 事象 R_i によってもたらされる損害を D_i と表現することとする．ここで損害の大きさは金銭的な価値をもって表現される．そこには攻撃によって発生する直接的な金銭被害だけでなく事業停止による機会損失, ブランド毀損, 復旧作業その他精神的な被害等を換算したものを含む．またこれらの評価を行う視点をあらかじめ定義しておく必要がある。つまりそれはサービスやシステムを利用者に提供する立場からの評価であるのか，またそれを利用する利用者の視点によるものなのかという観点の違いである．こう言った観点の違いは場合によって利害が対立することもあるため注意が必要である．

評価対象となる対策を講じない場合において単位期間 T の間にリスク R_i に起因して見積もられる被害の期待値 EL_i は以下のように表現される．

$$EL_i = P_i \times D_i$$

ある施策 A を採用することによって Ri の発生確率を pA, 発生時の被害規模を diA だけ減少させることができると見積もると施策 A を採用することによってもたらされる被害の期待値の残存リスクの期待値とリスク変化量 Δ EliA は以下のように示される．

$$EL_{iA} = (P_i - p_{iA}) \times (D_{iA} - d_{iA})$$

$$\Delta EL_{iA} = P_i \times \lambda_i - (P_i - p_{iA}) \times (D_{iA} - d_{iA})$$

このようなリスク期待値の変化は複数の対策を組み合わせて使用する場合その組み合わせによって変化すると考えられるが本稿においてはまず単一の対策を対象にその評価の試算を行う．

ある施策の効果について経済合理性の観点から評価を実施するためには，その施策に必要なコストを考慮する必要があるここでは施策 A を採用することによって生じるコストを C_A とする．このコストには施策の導入にかかる費用だけではなく，その利用や運用にかかる負担やそれに伴う損失なども含める．この前提において施策 A の採否を検討するにあたっては施策 A の実施にかかるコスト C_A 及び施策を実施した場合の残存リスクの期待値の和及び施策を実施しない場合のリスク期待値を評価することでその経済合理性を判断することができると考えられる．

具体的には

$C_A + EL_{iA} = CA \quad + (P_i - p_{iA}) \times (D_{iA} - d_{iA})$

及び

$EL_i = P_i \times D_i$

を比較する．

$C_A + EL_{iA} < EL_i$

が成立する場合において施策Aについて一定の経済合理性があるということが言える．

さらにその経済合理性の大きさを相対的に評価するにはコストに対する被害額の変化量

$$\frac{\Delta EL_{iA}}{C_A} = \frac{P_i \times D_i - (P_i - p_{iA}) \times (D_{iA} - d_{iA})}{C_A}$$

を指標として用いることができる．
複数の施策の組み合わせについて各施策毎に同様の計算を行った結果の合計により評価を実施する．

4. ケーススタディ

4.1 パスワードを一定期間内に変更する施策

本稿で提案する情報セキュリティ対策の経済合理性評価フレームワークを用いて現在情報セキュリティ管理の分野において議論となっている「パスワードを一定期間内に変更する施策」の経済合理性の評価を取り上げる．パスワードを一定の期間以内に変更する施策は一般に「パスワードの定期的な変更」の推奨または強制と表現されることが多いが，「定期的」という表現は「物事が一定の期間を置いて行われるさま。[4]」という意味があるとされ必ず一定の期間を置いて変更が行われなければならない「周期的」という言葉に近い意味があるが実際にはそのような運用が行われているわけではなく一定の期間以内に変更をするという意味で用いられることが多い．そこで本稿ではその意味を明確なものとし誤解を避けるために「パスワードの定期的に変更する」ではなく「パスワードを一定期間内に変更する」という表現を用いる．

「パスワードを一定期間内に変更する」セキュリティ上の施策に関してはどういったリスクを想定してその対策を実施するのかという点について様々な誤解が生じておりそのためその効果の評価についてもどういったリスク変化を評価の対象とするかを正しく選定する必要がある．「パスワードを一定期間内に変更する」施策についてはパスワードが何らかの理由によって漏洩した場合に次の変更時期以降攻撃者が不正にそのパスワードを不正に使用される漏洩リスクによる被害を防ぐことが可能であるが，連続したパスワードの試行によってパスワードが特定され不正に利用される推測リスクを防止する対策であるとの誤解が広まっておりその評価のみを持ってセキュリティ上の効果がないとの誤解を招く論説が広まっている[5][6]．　対象としてインターネット等から利用されるオンラインサービスを想定した場合，連続したパスワード試行の失敗は検出が容易であり一定時間当該アカウントに対するパスワード試行の回数を制限したりさらに失敗が連続する場合には当該アカウントへの認証を停止するなどの処置が行われるのが一般的である．そのためここで想定される連続試行による推測リスクについてはオンラインサービスのパスワード試行制限の施策により対応すべきものであり「パスワードを一定期間内に変更する施策」の効果を期待すべきものではないと考えられる．また仮にそのような効果を期待する者がいたとしても確率論の観点からその効果はパスワードを推定に必要な時間を最も良い条件で高々最大で２倍にする程度の効果しかなくその目的を考えればほぼ無視できる程度の効果しかないと言える．

一方パスワードを一定期間内に変更をさせることによって利用者は弱いパスワードをつけるようになるとの指摘も行われている[7]．これはパスワードの定期変更を行った場合の影響と言えるが本質的には「推測しにくいパスワードを選択する」施策によって対応すべきリスク事象である．「パスワードを一定期間内に変更する」と「推測しにくいパスワードを選択する」を組み合わせる場合の経済合理性の評価は別途実施する必要があるが，ここではまず前提として利用者は「推測しにくいパスワードを選択する」施策が徹底されている，もしくはシステムの制約により攻撃に用いられる可能性のない十分推測しにくいパスワードのみが選択されるという状況に限定した評価を行う．

4.2 経済合理性評価フレームワークの適用

本稿では以下の条件を仮定して経済合理性の評価を試みる．

対象サービス：インターネット上で無料で利用可能なポータルサービス。電子メール、SNS、ブログ等の機能を備える。
利用者：非 IT 業界就労の一般利用者 30 代，平均的な情報リテラシー，男性
脅威環境：2015 年 7 月から 2016 年 6 月を想定
パスワードの変更が必要な最長期間：９０日
評価の観点：一般利用者

ここではまず前提として「パスワードを一定期間内に変更する施策」を実施しない場合のリスクを評価する．この

ケースにおいてリスクとして想定する状況はパスワードが漏洩しそれが悪用されるという事態である．パスワードの漏洩はサービス事業者のシステムが侵入され漏洩しその事実に気づいていないケース，利用者の端末がマルウェア等に感染しパスワードが盗まれるケース，利用者自身がフィッシングサイト等に対してパスワードを入力してしまうケース，パスワードの使い回しを行っており他のサイトからそのパスワードが漏洩するケース，などが考えられる．ここでは１年間のうちそれぞれの事象の発生し悪用される確率について以下のように表現する．

P_1: サービス事業者からのパスワードの漏洩
P_2: 利用者端末からのパスワードの漏洩
P_3: 利用者自身からのパスワードの漏洩（フィッシング等）
P_4: 同じパスワードを利用している他サイトからの漏洩

T＝365　(day)

この場合上記３つの想定される漏洩経路から漏洩したパスワードによる被害の期待値の総和は以下のように表現される．

$$\sum_{i=0}^{4} EL_i = \sum_{i=0}^{4} (P_i \times D_i)$$

ここで各漏洩経路毎に想定される漏洩の確率を推定する必要がある．この推定には本来客観的に取得されたデータを使用するべきであるが，一般に特定の利用者その環境や使用するサービスなどは個々に異なるためそれらを想定して漏洩確率を事前に示すためのデータを取得することは不可能である．そのため現状において可能な漏洩確率を推定するには類似した利用者や環境におけるインシデントの事例から推定するほかない．しかし異なる利用者や環境をカバーするだけの十分なデータは存在しないためこの前提条件で実施可能な推定方法としては以下のようなものが考えられる．

１　専門家の主観的に推定値を指定する
２　候補となる複数の推定値を提示し評価者が選択する

これらの複合的なアプローチとして専門家による推定値を複数示した上で評価者が選択する推定値を集計し推定値を補正する．本稿では今後の推定の基礎として著者による見積を推定の候補値とすることを試みる．以下それぞれの漏洩経路別に推定値に対する考え方を示す．

P_1: サービス事業者からのパスワードの漏洩

主要なインターネットポータル等からの大規模な個人情報漏洩事故は毎年数万件から数十万件規模のものが十数件発生している．これらの多くはパスワードを含まないケースが多いがハッシュされたパスワードやパスワードそのものがふくまれているケースが存在する．そう言った点を考慮して１年のうちにサービス事業者からのパスワード漏洩が漏洩され不正アクセスに利用される確率の候補を 2%, 4%, 8%とする．

P_2: 利用者端末からのパスワードの漏洩

利用者の端末が不正なプログラムに感染しそこから当該サービスのパスワードが漏洩し悪用される確率．これは利用者が利用する端末の環境にもよるが，近年ではウイルス対策ソフトの導入の普及などによって一般的なウイルス感染自体の件数が減少している．一方で攻撃者のコミュニティにいて対象サービスを明示したパスワードリストも流通しており，それらのアカウント情報の一部はマルウェアによって収集されている可能性もある．また利用者に近い人物が不正な意図を持って不正プログラムをインストールしパスワードの窃取を試みるといったケースも考えらえる．これらを考慮し本漏洩経路による不正アクセス被害の年間発生確率の候補としては 1%, 2%, 5%とする．

P_3: 利用者自身からのパスワードの漏洩（フィッシング等）

利用者自身からのパスワードの漏洩経路としてはフィッシングによるものが多いと考えられる．現状において中程度の一般的な利用者が一般的なフィッシングにかかる可能性は高くはなく，またフィッシングサイトにパスワードを入力してしまったとしても大規模な攻撃であれば報道等により事後的に気付く可能性も高いと考えられるため本漏洩経路によって漏洩したパスワードが不正なアクセスに利用される確率の候補を 0%, 1%とする．

P_4: 同じパスワードを利用している他サイトからの漏洩

前述の通り様々なサービスで利用されているパスワードのリストが不正な市場で流通しておりこれらを用いた不正アクセスインシデントが継続して確認されている．実際に主要なサービスで利用な可能パスワード等が確認されていることから利用者が多くのサイトで同じパスワードの使い回しを行っている場合には本漏洩経路による不正アクセスの被害に遭遇する可能性が他の漏洩経路にも増して多いものと考えられる．各種調査結果では一般の利用者の 80%から 90%がパスワードの使い回しを行っていると言われている．

パスワードの使い回しをしていない場合は本経路からの漏洩による被害は発生しないことが予想されるため確率は 0%t となる．本漏洩経路からの被害発生確率の候補としては 0%, 5%, 10%とする．

以上をまとめると各漏洩経路毎に想定される被害発生の確率の選択肢は以下の通りとなる．

P_1: サービス提供者からの漏洩　2%, 4%, 8%
P_2: 利用者端末からの漏洩　1%, 3%, 5%
P_3: 利用者自身からの漏洩　0%, 1%, 2%
P_4: 他サイトからの漏洩　0%, 5%, 10%

次に漏洩したパスワードが悪用され不正アクセスの被害が発生した場合の Di について考える．不正アクセスの被害の規模についてはそのアカウントの利用者やその目的によって大きく異なる．例えばストーカーやドメスティックバイオレンスなど本人に対して具体的な脅威が存在する場合などにおいては人命に関わるような事態も発生しうる．

他にも経営上の秘密に関する事項やスキャンダルに関連する内容など第三者に漏洩することによって大きな被害をもたらす情報を扱う可能性がある場合も大きな損害をもたらすと見積もることができる．しかし一般にはそう言った用途にインターネット上のポータルサービスのアカウントを使用するということは考えにくく，多くの場合は個人的な利用でありそれほど重要な情報を含まないケースが大半であると考えられる．不正アクセス等情報セキュリティによって発生する被害の見積もりは個別の直接的に生ずる被害の金銭的な価値，復旧に要する被害等を個別に見積もる方法もあるが，上記のような私的なサービスの利用によって生ずる損害をこのような方法で評価することは必ずしも適切とは言えない．そこで本稿では利用者自身が発生が想定される被害についての主観的な評価を用いるものとする．具体的には対象となるアカウントにおいて不正アクセスによる被害が発生したと想定される状況において（その被害の発生を認識していない状況も含め）その被害がなかったことにするためにどれだけの金額を支払うことを認めるか，その金額を持って不正アクセスによる主観的な被害額として評価するものとする．この主観的な被害額の評価については個別の利用者の金銭感覚等も反映されるため大きく変動することが考えられる．ここでは漏洩経路による被害額評価の差はないものと仮定した上で被害評価額Ｄの候補の例として５万円，５０万円，５００万円の３つ挙げる．

D: [50000, 500000, 5000000]　(円)

最後に「パスワードを一定期間内に変更する」行為によって生ずる利用者の負担をコストとして評価する．これは変更を必要とする一定期間をどのように設定するかに依存するが，先に想定として示している９０日の期間とする．またこのコストには変更したパスワード管理する手間，変更したパスワードを忘れた場合の再発行の手間などもこのコストの算定に含めるものとする．このコスト評価額の算定は被害額の算定と同様に「パスワードを一定期間内に変更する」を１年間行った場合に要求を免除するためにはどの程度の金額を支払うことを認めるかを主観的に評価するものとし，ここでは例として１回の変更につき５００円，１０００円，２０００円を選択肢として設定する．この場合最長９０日の期間を設定した場合少なくとも４回のパスワード変更を行うことになるそれらを含めパスワードを管理する負担や年間のコストの選択肢として以下の金額を仮定する．

C_A: [3000, 5000, 10000]　(円)

また最長９０以内にパスワードを変更することの効果として被害発生確率の差分 p の見積もりとして

p_A 1%, 2%, 5%を設定する．

以上の前提と各パラメータを設定した上でいくつかのシナリオについての経済合理性の評価の試算を行う．

(1) **一般的なシナリオ**

一般的なポータルサービスの利用を想定し特に秘匿性が求められる情報などが扱われていないケースを想定する．このケースでの試算パラメータとしては以下の通り各確率選択肢の中間の選択肢の値を用いる．

$P_1 = 4\%$
$P_2 = 3\%$
$P_3 = 1\%$
$P_4 = 5\%$

被害発生時の被害評価額Ｄについては一般的なシナリオであるため大きな損害と評価される可能性は低く最も低い評価額である 50000 円とする．
この場合「パスワードを一定期間内に変更する」を行わない場合の被害の１年間での期待値は以下の通りとなる．

$$EL = (P_1+P_2+P_3+P_4)\times D$$
$$= (4\%+3\%+1\%+5\%)\times 50000$$
$$= 6500$$

次に「パスワードを一定期間内に変更する」を行う場合について考える．パスワード変更のコスト評価については中間の選択肢を用いる．

$C_A = 5000$　(円)

「パスワードを一定期間内に変更する」ことによる被害発

生確率の差分 p を中間の選択肢である 2%とする．

この場合

$C_A+EL_A = C_A+ (P_1+P_2+P_3+P_4-p)\times D$

$= 5000 + (4\%+3\%+1\%+5\%-2\%)\times 50000$

$= 5000 + 5500$

$=10500$

「パスワードを一定期間内に変更する」を実施しなかった場合の被害の期待値 EL と実施した場合のコスト及び被害の期待値の和 C_A+EL_A を比較すると C_A+EL_A が 4000 円分多いこととなり対策を行うことによって全体の支出が多いこととなる．またそれによって得られる被害の期待値の変化量も 6500-5500 の 1000 円分に留まり「パスワードを一定期間内に変更する」労力やコストに対してあまり大きな効果は期待できないと判断することができる．

(2) 機微な情報を取り扱っているシナリオ

次に対象となるポータルサービスの電子メールの機能を利用してプライベートであるが第三者には知られたくない重要な情報をやり取りしているケースを想定する．

この場合取り扱う情報の性質を考慮しより慎重な仮定を置くことを想定して試算パラメータとしては最もリスクを高く見積もる選択肢を用いるものとする．

$P_1 = 8\%$

$P_2 = 5\%$

$P_3 = 2\%$

$P_4 = 10\%$

被害発生時の被害評価額 D については機微なシナリオであるため最も高い評価額である 5000000 円を想定する．

$D = 5000000$　　（円）

この場合「パスワードを一定期間内に変更する」を行わない場合の被害の１年間での期待値は以下の通りとなる．

$EL = (P_1+P_2+P_3+P_4)\times D$

$= (8\%+5\%+2\%+10\%)\times 5000000$

$= 1375000$

「パスワードを一定期間内に変更する」を行う場合のコストについては大きい方の選択肢を用いる．

$C_A = 10000$　(円)

「パスワードを一定期間内に変更する」ことによる被害発生確率の差分 p を効果が大きいとされる選択肢である 5%とする．

この場合

$C_A+EL_A = C_A+ (P_1+P_2+P_3+P_4-p)\times D$

$= 10000 + (8\%+5\%+2\%+10\%-5\%)\times 5000000$

$= 10000 + 1000000$

$= 1010000$

「パスワードを一定期間内に変更する」を実施しなかった場合の被害の期待値 EL と実施した場合のコスト及び被害の期待値の和 C_A+EL_A を比較すると対策を行わないあ場合の被害の期待値 EL の方が 365000 円大きく，このようなケースでは「パスワードを一定期間内に変更する」対策を行うことによる経済性において優れることがわかる．

5. おわりに

本稿では情報セキュリティ対策の採否を判断する際において費用対効果などの有効性の評価を行う際に用いることを想定した経済合理性評価フレームワークを提案し，そのモデルケースとして「パスワードを一定期間内に変更する」施策の経済合理性に関する評価を試行した．個別に異なる情報システムの利用環境におけるリスクの評価となるため客観的データの取得に制約があり現段階では評価者の主観に基づく評価値を用いているためその客観性や評価結果の正当性については議論の余地が大きい．今後は何らかの統計データや複数人による評価値の投票などより精度の高い評価を実現するための根拠データの取得等についても検討を行う必要がある

参考文献

[1] Gordon L. and Loeb M.. The Economics of Information Security Investment. ACM Transactions on Information and System Security (TISSEC). 2002, vol. 5 Issue 4, p. 438-457.

[2] 芝口誠仁, 稲場太郎, 中山佑輝, 岡田謙一. 仕事量を考慮したセキュリティ対策選定手法. 情報処理学会論文誌, 2010, vol. 51, no. 2, p. 648-657.

[3] 呉洋, 小崎真寛, 岡田謙一. プロジェクトの特性を考慮した最適なセキュリティ対策選定手法. 情報処理学会論文誌, 2013, vol. 54, no. 1, p. 309-317.

[4]“デジタル大辞泉”. http://dictionary.goo.ne.jp/jn/149728/meaning/m0u/, (参照 2016-08-12).

[5]“パスワードの定期変更"はもはや無意味! セキュリティの現実を直視すべし―NTT データ先端技術、辻氏”. http://news.mynavi.jp/articles/2013/07/31/itsummit/, (参照 2016-08-12).

[6]“パスワードの定期的変更について徳丸さんに聞いてみた(1)(2)”. http://blog.tokumaru.org/2013/08/1.html (参照 2016-08-12).

[7] Cranor L., “Time to rethink mandatory password changes”. https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes (参照 2016-08-12).