k-匿名性を維持しつつ他組織との比較可能なサイバーリスク可視化システムの試作

小林晴貴[1] 齊藤泰一[2] 佐々木良一[3]

概要：近年，あらゆる組織がディジタル化を進め，多様なITシステムを導入するようになった．一方，その普及に伴ってセキュリティインシデント(事件事故)が頻発しており，このようなサイバーリスクへの対策を効率良く実施することが課題になっている．解決策として，情報部門が経営者とのリスクコミュニケーションを行い，意思決定支援を行うことが挙げられるが，セキュリティ専門家ではない経営者に対してこれを実施することは容易ではない．このような経営者にとっては，同業他組織の状況を知り，そこに合わせる，もしくは近づける，あるいはそれを凌駕するというアプローチが効果的だと考える．しかし，組織間の情報共有は様々な懸念が存在し積極的な取り組みは進んでいない．そこで，本稿では自組織のサイバーリスクを可視化するとともに，*k*-匿名性を維持できる範囲でその結果を他組織と比較できるシステムを検討し，オープンソースのWebアプリであるLimeSurveyを用いて試作した．本試作により，自組織の匿名性を維持しつつ同業他組織との状況を比較できることを確認できたので報告する．

Trial Development of a Cyber Risk Visualization System with Function of *k*-Anonymity and compatibility to Other Institutes

HARUKI KOBAYASHI[1] TAIICHI SAITO[1] RYOICHI SASAKI[2]

1. はじめに

近年，あらゆる組織がディジタル化を進め，様々なITシステムを導入することで，業務効率の向上やグローバル化を目指している．一方で，サイバーセキュリティインシデント(事件・事故)が頻発しており，多くの組織にとって予算が限られた中でサイバーセキュリティ対策をどこまで実施すべきか決定することが課題になっている[1].

米国などでは国立標準技術局(NIST)の Cybersecurity-Framework[2]における評価指標を用いて，経営者によって実施すべきレベル(文献[2]では Tir と呼んでいる)を明確にした上で，各部門の管理者が現状のレベルを設定の上，その差を最も効率よく縮められるものから対策を実施するというアプローチが取られている．

経済産業省のサイバーセキュリティ経営ガイドライン[3]では，情報部門と経営層がリスクコミュニケーションを積極的に行うことで経営層の意思決定を支援し，効果的な対策を実施するよう求めている．しかし，サイバーセキュリティの専門家ではない経営者が専門的な情報に基づいて意思決定することは容易でない[4]．むしろ他組織，特に同業他組織の状況を知り，それと差のない形，あるいはそれを凌駕するというアプローチが経営者の理解を得て，そして意思決定を支援する手法として効果的であると考える．

一方で，他組織のサイバーセキュリティへの対策状況は知りたいが，自組織の状況は知られたくないというのが実情である[5]. JPCERT/CCによれば他組織との情報共有を積極的に行うことが対策として効果的であると述べている[6]が，日本においては

・共有データに含まれるパーソナルデータの取り扱い

・同業他組織との情報共有が独占禁止法とされる可能性

・提供情報により違法行為が指摘される危険

などといった懸念から共有が期待通りに進まないと考えられる．

そこで，1 つの組織におけるリスク評価の実施状況は他組織から保護しつつ，その概要，例えば同業他組織のリスク評価指標の平均値や，同業で類似規模の他組織のリスク評価指標の平均値を後述する *k*-匿名性を維持できる範囲で可視化しようとするものである．

このシステムは図 1 に示すように，①(独)情報処理推進機構(IPA)のような組織のリスク評価サービス提供組織と，②リスク評価サービスを利用する各種の組織からなる．①の組織では，本システムを用いてリスク評価項目ごとにそのレベル候補を表示する．②の各組織では，自組織の各評価指標の現状のレベルを選択して送り返す．各組織がそれを入力すれば，自組織の状態だけでなく，*k*-匿名性を維持した同業他組織などの平均値の状態がわかる．これらの結果を用い，情報部門と経営層によるリスクコミュニケーシ

1 東京電機大学大学院 工学研究科 情報通信工学専攻
2 東京電機大学 工学部情報通信工学科
3 東京電機大学 総合研究所

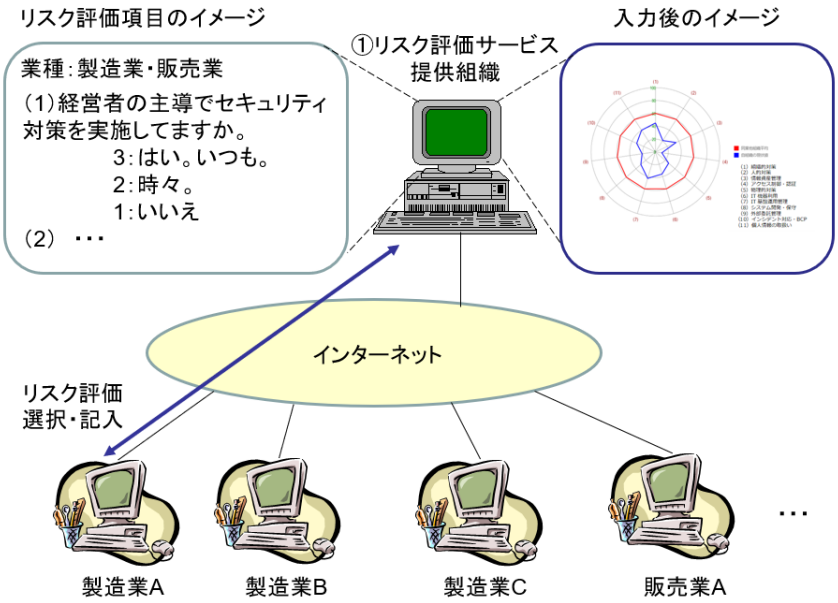


図 1　提案システムの概要

ョンを行いつつ自組織の今後とるべき対策を明確化することができる．

本稿では，そのシステムの構成や機能などを述べるとともに，試作システムの評価結果と今後の開発方針について報告する．

2. サイバーリスク可視化に関する既存手法

まず，サイバーリスクとはサイバー攻撃など，サイバー空間で発生する脅威[7]のことである．サイバー攻撃を防ぎ，その被害の影響を抑えるためには，経営者がこのリスクを十分に認識しサイバーセキュリティ対策を主導することが必要とされているが，サイバー攻撃の脅威や影響の大きさを十分に認識していないことがある．確かに，サイバーリスクの認識や評価は複雑であるが，図示することがそれらの問題の解決に役立つとされている[8]．

そこで，情報部門の担当者に自組織のプロフィールやセキュリティ対策への取組状況を回答してもらい，サイバーリスクをレーダーチャートなどで可視化することでリスク認識を支援する手法がある．

IPA では，組織における情報セキュリティ対策の整備や運用状況の自己評価を支援する情報セキュリティ対策ベンチマークを提供している[9]．これは WEB 上にて無償で提供されており，情報セキュリティ対策への取り組みに関する 25 問と企業プロフィールに関する 15 問に回答すると診断結果と推奨される取り組みが表示される．このベンチマークでは ISMS 認証基準(JIS Q 27001)[10]を評価基準に用いており，133 項目の情報セキュリティ対策を 25 項目まで絞り込むことで簡易化し，簡便な自己評価を実現している．しかし，簡易化したことで正確な評価が行えているのか，それぞれの業種や組織規模に最適な情報セキュリティ対策を行えるのかについて，情報セキュリティ対策ベンチマークでは分かりづらいと指摘されている[11]．また，状況によっては ISMS 認証基準だけでなく，個別の基準によって自己診断を行う場合も想定できる．したがって，評価に用いる設問項目の拡張や変更が簡易的で，かつ同業種や同じ規模の組織間と比較可能で匿名性が確保されたサイバーリスク可視化システムが必要であると考えられる．

また，サイバーリスクだけでなくセキュリティ要件を可視化する手法も提案されている[12]．セキュリティ要件とは，セキュリティシステム開発時に満たすべき条件や要件間の依存性の定義[13]を指し，セキュリティ評価基準であるコモンライテリア(ISO/IEC15408)[14]やアシュアランスケース(ISO/IEC15026)[15]を用いて開発者によるセキュリティ要件の可視化や検証，妥当性の確認を容易にし，その製品やシステムの利用者の認識の齟齬を防ぐシステムを提案している．

セキュリティ対策状況の可視化手法としては，二次元マップ上に可視化することも提案されている[16]．これは対策実施の有無とそれぞれの対策レベルの 2 つの指標を対策箇所と脅威を軸にした二次元マップ上に可視化することで評価を行う手法である．ただし，要求される対策レベルは対象の組織や業務によって変化するが，この手法ではそれらへの対応は実現できていない．

経営層にも有効なサイバーリスク可視化システムとしては，CVSS(Common Vulnerability Scoring System)[17]という情報システムの脆弱性評価手法を用いて，技術的側面からシステム内の脅威をリスク評価し，対処にかかる投資効果を算定する技術が提案されている[4]．これは，経営者に

とって馴染みのあり事業継続性への影響などを定量化するBIA(Business Impact Analysis)[18]からセキュリティ投資対効果算定モデルに基づき，投資対効果を算定するものである．しかし，投資対効果を算定する上で情報流出に伴う損害賠償額などのパラメータを要するが，これは各組織や業界に依存するものであり，妥当性を高めるためステークホルダー間などで調整する必要がある．

以上のように，様々なサイバーリスク可視化手法が提案されているが，他組織や業界ごとの比較を行う手法については十分な研究が行われていないのが現状である．

3. 他組織と比較可能なサイバーリスク可視化システムのモデルと要件

3.1 モデル

本稿で試作するシステムはIPAのような組織のリスク評価サービス提供組織によって運営されるサービスの1つとして追加するものとする．

今回のモデルは，図2に示すように端末を用いて回答するサービス利用組織と回答データを集計するサービス提供組織のサーバ(集計サーバ)から成る．

ここで，このサービスを利用する組織の競合他組織が参加することを考えると，共有した回答データからどの組織が回答したかを特定できないようにする必要がある．一方で，リスク評価サービス提供組織に対してもどの組織がどのような回答を行ったかは秘匿したい．

また，前述の通り，設問内容や回答形式を変える可能性があることから、変更容易性を持つシステムにすべきであると考える．そのため，サービス提供組織の希望によってアンケートの設問が容易に変更できるほか，回答形式についても多段階のリッカート尺度や「はい / いいえ」から選ぶ2件法などを選択できるものとする．

3.2 要件

3.1で述べたモデルにおいてシステムを考えた場合に満たすべき要件を以下に示す．

(1)回答者にとって回答することが煩雑ではない

・Webブラウザ上で実施できるようにし，ソフトウェアの導入を伴わないこと．

(2)設問設定者にとって設問を作りやすく，修正しやすい

・Webブラウザを用いてGUIで編集できることとし，プログラミング知識を不要とすること．

(3)サービス利用組織へのデータの秘匿性

・共有された回答データから他組織がどのような回答を行ったか特定できないこと．

(4)回答者による不正回答の防止

・1組織が2回以上回答する多重回答を行えないこと．また，回答する権利がない者が回答を行えないこと．

(5)集計サーバにあるデータの秘匿性

・秘密計算[19]などの技術により，外部からの攻撃や内部犯に対してデータの秘匿性が確保されること．

本稿では，(1)，(2)，(3)を満たすシステムの試作結果を報告する． なお，リスク評価サービス提供組織に対しての秘匿性について今回は対象外とし，今後の課題とした．

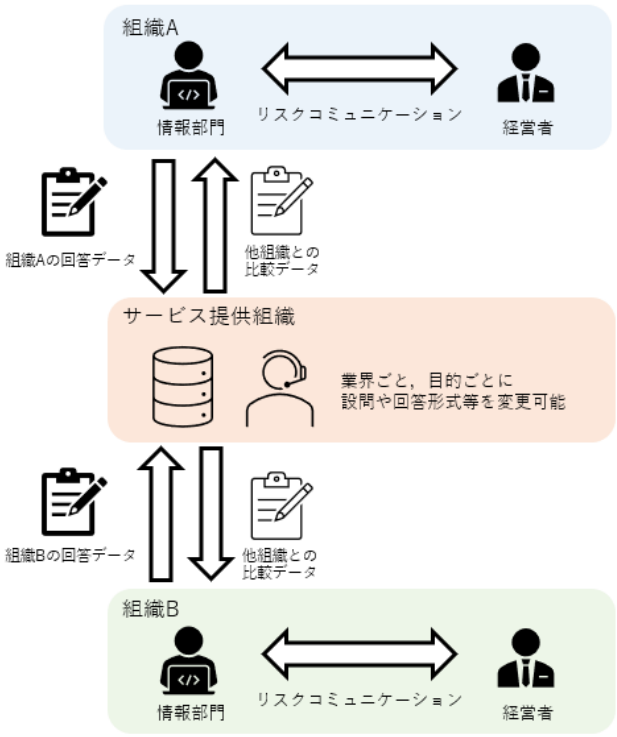


図 2 システム概要

4. *k*-匿名化技術

4.1 *k*-匿名性の一般的方法

本研究では，*k*-匿名化処理を用いて他組織の回答結果の特定を防ぐことで，組織間の情報共有を可能にする．*k*-匿名性とは，回答者が匿名化されたデータから再識別されるリスクを計測する指標の1つである[20][21]. この指標では，元データは以下の属性で構成されると整理されている[22].

・識別子：
単独で回答者を識別できる属性(例：組織名，連絡先)

・準識別子：
組み合わせることで回答者を識別できる属性(例：業種，従業員数，財務状況)

・センシティブ属性：
第三者に知られたくない属性(例：セキュリティ投資費用)

・その他の属性：
上記以外の属性

k-匿名処理では，準識別子について，同じ値を持つ回答者が少なくとも *k* (*k* > 1)存在するようにデータを処理する．*k*-匿名性のリスクについてはこれまで多数検討されており[23][24][25]，また，*k*-匿名性を保証する指標として *Pk*-匿名性[26]が提案されているが，今回は *k*-匿名性のみを指標とする．

4.2 *k*-匿名性の本システムへの適用方法

今回の試作において，組織名のような識別子は直接収集しないものとし，組織プロフィールである「業種」「従業員数」「売上高」「資本金」「国内拠点数」「海外拠点数」などの準識別子を収集する．これらのデータは一般化階層を用いた処理を施すことで *k*-匿名化処理を行うこととする．一般化とはデータの一部を削除する，もしくはより広い値域を示す値に置き換える操作のことである．

本試作では各組織プロフィールに対して一般化階層を設定し，データの書き換えを行う．従業員数における一般化階層の例を表 1 に示す．元データは設定した一般化階層に基づいて書き換えていき，各区分で *k*-匿名性を求める．*k*-匿名性が定めた値になるまで，この書き換え処理を続ける．なお，この条件が満たされなかった場合は，サービス利用組織に情報提供しない．なお，今回の試作では *k*-匿名性の値はサービス提供組織が定めるものとする．

表 2 はセキュリティ投資額をセンシティブ属性，その他を準識別子とし，入力された回答結果を 3-匿名化(*k* = 3 で *k*-匿名化)した例である．

5. システムの試作

5.1 システムの構成

試作したシステムには LimeSurvey[27]を使用した．LimeSurvey とは，LimeSurvey GmbH が GNU ライセンスの下で配布するオープンソースのアンケートアプリケーションで，開発には PHP 言語[28]が用いられている．

LimeSurvey はサーバにインストールする WEB アプリケーションで，図 3, 4 のように WEB インターフェースで容易にアンケート項目の作成や修正，回答が可能である．また，回答形式も 2 件法や，スライダーによる入力，数値入力，自由入力など様々選択できる．したがって，それぞれの状況に応じてサイバーリスク分析の基準や精度を変更することができる．

さらに，プラグイン機能を有しており，容易にカスタマイズできる特徴を持つ．また，開発者コミュニティも整備されている[29]．

表 1　一般化階層の例

区分	従業員数				
区分 1	100 名以下				・・・
区分 2	1 - 50 名		51 - 100 名		・・・
元データ	1 名	・・・	51 名	・・・	・・・

表 2　匿名化前のテーブル

No.	業種	従業員数	資本金	セキュリティ投資
1	卸売業	55	8000 万	10 万
2	製造業	378	3 億	100 万
3	製造業	607	4 億	2 万
4	製造業	403	2 億	5 千
5	卸売業	76	1 億	15 万
6	卸売業	37	1000 万	7 千
7	:	:	:	:

表 3　*k*-匿名化後のテーブル(*k* = 3)

No.	業種	従業員数	資本金	セキュリティ投資
1	卸売業	100 名以下	1000 万以上	10 万
2	製造業	200 名以下	1 億以上	100 万
3	製造業	200 名以下	1 億以上	10 万
4	製造業	200 名以下	1 億以上	38 万
5	卸売業	100 名以下	1 億以上	15 万
6	卸売業	100 名以下	1000 万以上	7 千
7	:	:	:	:

図 3 アンケート項目編集画面

5.2 *k*-匿名性の実装

4.2 で述べた *k*-匿名性の適用方法の実装には，LimeSurvey のプラグイン仕様に則り PHP 言語を用いた．この実装により，一般化階層を用いた匿名化はサービス提供組織のサーバで行われ，サービス利用組織にデータが提供される．匿名化に関する設定項目は管理者画面から変更可能とし，変更容易性を持たせた．

5.3 システム概要

本システムは，主に回答フェーズと匿名化フェーズ，集計フェーズ，公開フェーズの 4 つから成る．
各フェーズの流れを図 5 に示し，概要は次に述べる．

（1） 回答フェーズ

(ア) 企業規模別，業種別による比較を行うため，事業内容や従業員数，売上高，資本金，拠点数，業種などの組織プロフィールのデータを収集する．

(イ) サイバーセキュリティ対策を評価するため，サイバーセキュリティ対策の取り組みに関するデータを収集する．

（2） 集計フェーズ

サービス利用組織の回答データを集計サーバに送信する．

（3） 匿名化フェーズ

回答データに *k*-匿名性を満たす匿名化を施す．

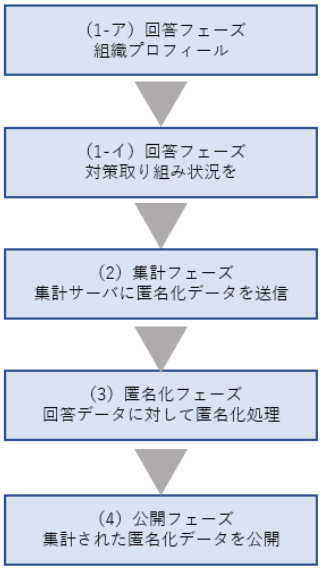
（4） 公開フェーズ

集計された匿名化データをサービス利用組織に公開する．

例として中小企業の情報セキュリティ対策ガイドライン[30]に基づいた場合の回答フェーズ画面を図 5 に，サイバーリスクの可視化結果を図 6 に示す．ここでいう平均値はそれぞれの分野ごとの設問における平均値を指し，望まれる水準というのは，サービス利用組織でかつ同業種における平均値を示したものである．

以上のような試作システムにより，自組織の匿名性を維持しつつ同業他組織との状況を比較できることを確認した．

図 4 回答ページ例



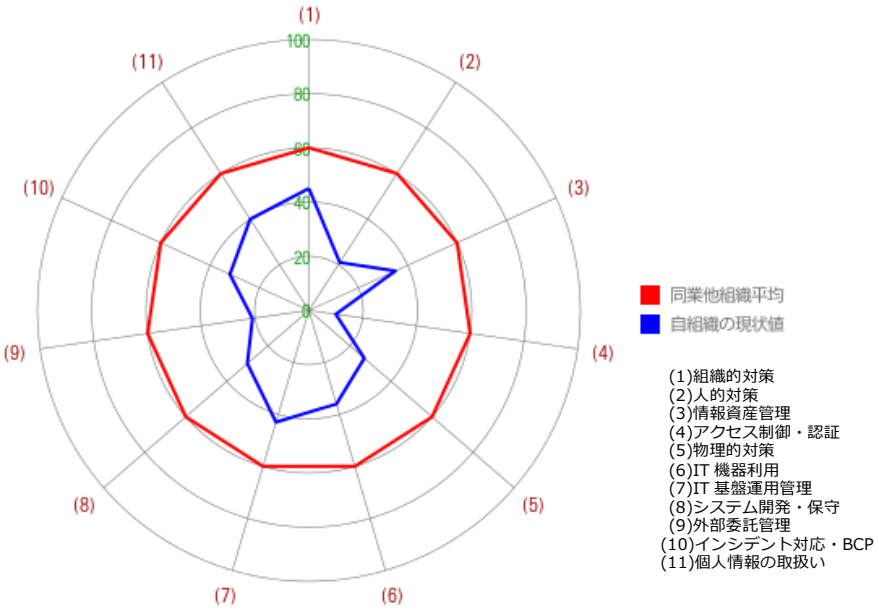


図 6　サイバーリスク可視化結果

6. おわりに

本稿では，LimeSurvey を用いて *k*-匿名性を維持しつつ他組織と比較可能なサイバーリスク可視化システムの試作について報告した．このシステムによって組織におけるサイバーリスクを可視化するとともに，他組織の状況とを比較し，自組織が優先的に取り組むべき対策を容易に選定できるようになると考えられる．このシステムでは GUI で設問等をカスタマイズできるため，各組織やセキュリティ評価基準によって容易に設問や回答形式を変更できることから，例えば PCIDSS(クレジットカード業界におけるセキュリティ基準)[31]などへの対応など多様な活用が期待できる．

今後の取り組みとして，その他のシステム要件を満たすための検討と試作を続ける．特に集計サーバにおける回答データの秘匿性については，準同型暗号などを用いて暗号化したまま処理するなど秘密計算技術の活用による効果的な手法について検討を進めたい．さらに，サービス利用組織にとって回答が快適に行えるか，サービス提供組織にとって回答項目の編集は容易かについて実験･評価を実施し，改善を行いたい．

今後の課題として，匿名化処理を施すことによって生じるデータの歪曲度が与える影響についても検討が挙げられる．そのため，その他の匿名化手法についても適用し，評価を実施したい．

参考文献

[1] (独)情報処理推進機構，「2018 年度 SECURITY ACTION 宣言事業者における情報セキュリティ対策の実態調査」報告書，https://www.ipa.go.jp/security/fy30/reports/sme/index.html，(参照 2020-5-10)

[2] National Institute of Standards and Technology (NIST)，CYBERSECURITY FRAMEWORK，https://www.nist.gov/cyberframework(参照 2020-5-10)

[3] 経済産業省，サイバーセキュリティ経営ガイドライン，https://www.meti.go.jp/policy/netsecurity/mng_guide.html，(参照 2020-5-10)

[4] 杉本暁彦，磯部義明，仲小路博史．"セキュリティ運用のための経営層向けビジネスリスク評価技術の開発." 情報処理学会論文誌 58.12 (2017): 1926-1934.

[5] 林紘一郎．"サイバーセキュリティ事故情報共有のあり方." 情報通信学会誌 34(3)，pp.97-100 (2016).

[6] JPCERT/CC，経営リスクと情報セキュリティ -CSIRT：緊急対応体制が必要な理由，https://www.jpcert.or.jp/csirt_material/files/csirt_for_management_layer_20151126.pdf，(参照 2020-5-10)

[7] Refsdal, A., Solhaug, B., Stølen, K. (2015). Cyber-risk management. In Cyber-Risk Management (pp. 33-47). Springer, Cham.

[8] Hall, P., Heath, C., Coles-Kemp, L.: Critical visualization: a case for rethinking how we visualize risk and security. Journal of cybersecurity 1(1), 93–108 (2015)

[9] (独)情報処理推進機構，情報セキュリティ対策ベンチマークの概要 http://www.ipa.go.jp/security/benchmark/benchmark-gaiyou.html，(参照 2020-5-10)

[10] ISO/IEC：Information technology - Security techniques - Information security management systems- Requirements，International Standard ISO/IEC27001.

[11] 村田真理．"中小企業の情報セキュリティ対策の投資に対する費用対効果について." 研究報告電子化知的財産・社会基盤 (EIP) 2010.8 (2010).

[12] 金子朋子，髙橋雄志，勅使河原可海，田中英彦．(2016)．CC-Case を用いた IoT セキュリティ要件の可視化．研究報告コンシューマ・デバイス & システム (CDS)，2016(5)，1-8.

[13] 府川真理子，松浦佐江子．"ゴール指向を用いたセキュリティ要件の定義手法の提案." 研究報告組込みシステム (EMB) 20

09.10 (2009): 1-8.
[14] ISO/IEC 15408-1:2009 Information technology Security techniques Evaluation criteria for IT security.
[15] ISO/IEC 15026-2:2011 Systems and Software engineering.
[16] 武曽徹, 飯田茂. "情報セキュリティ対策状況の評価手法の提案." 研究報告コンピュータセキュリティ (CSEC) 2009.4 (2009): 1-5.
[17] FIRST.org, Inc., Common Vulnerability Scoring System SIG, https://www.first.org/cvss/, (参照 2020-5-10)
[18] Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., Lynes, D. (2010). Contingency Planning Guide for Federal Information System. NIST Special Publication, 800-34.
[19] Yao, Andrew Chi-Chih. "How to generate and exchange secrets." 27th Annual Symposium on Foundations of Computer Science (sfcs 1986). IEEE, 1986.
[20] L. Sweeney. “Guaranteeing anonymity when sharing medical data, the Datafly system.” Journal of the American Medical Informatics Association, pp.1‐5, (1997)
[21] 小栗秀暢, 松井くにお, 黒政敦史. "匿名加工・再識別コンテストにおける有用性と安全性指標の社会実装に向けた検討." コンピュータセキュリティシンポジウム 2016 論文集 2016.2 (2016): 797-804.
[22] 竹之内隆夫. "*k*-匿名化技術と実用化に向けた取り組み (特集 プライバシーを守った IT サービスの提供技術)." 情報処理 54.11 (2013): 1125-1129.
[23] 渡邉奈津美, 土井洋, 趙晋輝. "*k*-匿名化手法の効率向上に関する一提案." 第 75 回全国大会講演論文集 2013.1 (2013): 519-520.
[24] 山岡裕司, 伊藤孝一. "*k*-匿名性による特定可能性分析に基づいたデータプライバシーのリスク分析." 研究報告コンピュータセキュリティ (CSEC) 2016.31 (2016): 1-8.
[25] 小栗秀暢, 曽根原登. "実サービスのデータを用いた *k*-匿名状態の推移調査と, 合理的な匿名状態評価指標の検討." 研究報告コンピュータセキュリティ (CSEC) 2014.4 (2014): 1-8.
[26] 五十嵐大, 千田浩司, 高橋克巳. "*k*-匿名性の確率的指標への拡張とその適用例." コンピュータセキュリティシンポジウム 2009 (CSS2009) 論文集 2009 (2011): 1-6.
[27] LimeSurvey.org, LimeSurvey.org-The Leading Open, http://www.LimeSurvey.org/, (参照 2020-5-10)
[28] PHP, https://www.php.net/, (参照 2020-5-10)
[29] LimeSurvey.org, Development Conference, https://manual.limesurvey.org/Development_overview, (参照 2020-5-10)
[30] (独)情報処理推進機構, 中小企業の情報セキュリティ対策ガイドライン, https://www.ipa.go.jp/security/keihatsu/sme/guideline/, (参照 2020-5-10)
[31] PCI Security Standards Council. “Organizational Structure”, http://www.pcisecuritystandards.org, (参照 2020-5-10)