Vol.2022-CSEC-99 No.17
Vol.2022-SPT-49 No.17
Vol.2022-EIP-98 No.17
2022/12/23

USB メモリ紛失から考える組織・人間の脆弱性

内田 勝也 [1]

概要：自治体の委託先企業の再々委託先社員は，鞄に入れた USB メモリを鞄ごと紛失した． 前夜，作業終了後，委託先企業の社員３名と，飲食をし，酩酊して，帰宅途中で，鞄を紛失した． 翌朝，鞄を探したが見つからず，警察に届出をし，更に，委託先企業にも報告した． 幸い，USB メモリの入った鞄は無事に見つかり，USB メモリはパスワードが設定されており，アクセスされた様子もなかった．

契約主体は、自治体と大手システム業者で，システム業者は長期間にわたり，自治体と委託を行っており，いわゆる，『ベンダーロック』状態を非難され，鞄の所有者は，システム業者の再々委託先社員だが，20 年程，この自治体の業務を経験していた．

自治体システムの業務委託先は，大手システムベンダーで，長期間にわたり，業務を受託しており，本件が発覚後，いわゆる，『ベンダー・ロックイン』との非難や鞄の所有者は，委託業者の再々委託先社員であることが判明した． ただ，この再々委託先社員は，20 年程，自治体でのシステム業務を経験しており，業務経験は豊富であると思われる．

再々委託先社員と一緒に飲食した３名は，委託先企業（大手システムベンダー）の社員２名と再委託先社員１名で，鞄の所有者である再々委託先社員が USB メモリの保持を知って飲食した可能性があると思われる．

今回の事案では，自治体，委託先業者／社員，鞄所有者である再々委託先社員が関係しており，非技術的セキュリティ（ノンテクニカルスキル）で，それぞれ課題を抱えており，その考察を行った．

キーワード：USB メモリ、人的セキュリティ対策，セキュリティ心理学，Human element

The review of vulnerabilities of Organization and Human due from the loss of USB memory stick

KATSUYA UCHIDA[1]

Abstract:

Keywords: USB Memory, Human element, Security psychology,

1. はじめに

1.1 事故の概要

関西地区の**自治体**で，住民税非課税世帯等に対する臨時給付金支給事務のシステム業務を受託していた**受託業者**の**協力会社社員**が自治体の情報センターで情報をダウンロードし，コピーした USB メモリを持参した鞄にいれ，受託業者のコールセンターに移動し，そこで，データ移管作業を実施した． データ移管作業完了後、受託業者社員３名と飲食し、帰宅時に USB メモリを入れた鞄を紛失した．

協力会社社員は，路上で寝ていることに気づき，更に，鞄がないことも気づいたが，帰宅した．

翌朝，協力会社社員は，鞄を探したが，発見できず，警察に遺失物届を提出し，午後，受託業者に鞄の紛失を報告した．受託業者は，鞄の中身，USB メモリの内容を確認し，住民情報が含まれていることを確認し，当該自治体に報告

1 九州大学 リカレント講座 非常勤講師
Part-time Lecturer，recurrent education，Kyushu University

Vol.2022-CSEC-99 No.17
Vol.2022-SPT-49 No.17
Vol.2022-EIP-98 No.17
2022/12/23

した.

翌日，紛失した鞄は発見できず，自治体の記者会見，及び，自治体と受託業者共同の記者会見が行われた

記者会見翌日，USB メモリは警察と協力会社社員とで発見したと自治体から報告があった.

当該 USB メモリは、パスワードが付され、内容は『暗号化』されており，現時点で外部への漏洩は、確認されていない

本稿は執筆時点までの当事者やマスコミ報道を基に分析したもので，公開される資料等とは異なる可能性があります.

1.2 保存されていた個人情報の内容

6 月 23 日午前 11 時現在，判明している内容であり，**マイナンバーは含まれていない**.

① 全市民の住民基本台帳の情報（460,517 人分）： 統一コード、氏名、郵便番号、住所、生年月日、性別、住民となった年月日など

② 住民税に係る税情報（360,573 件）： 統一コード、住民税の均等割額

③ 非課税世帯等臨時特別給付金の対象世帯情報 （R3 年度分 74,767 世帯、R4 年度分 7,949 世帯）

④ 世帯主の統一コード、申請書番号、申請受付日、申請書不達理由、振込済処理日時など

⑤ 生活保護受給世帯と児童手当受給世帯の口座情報（生保 16,765 件、児手 69,261 件）

⑥ 統一コード、金融機関コード、支店コード、口座区分、口座番号、口座名義

（注意）統一コードは、庁内システムで使用する番号で、マイナンバー（個人番号）ではない

2. 事件・事故分析の考察

2.1 はじめに

IT システムの高度化が進展し，AI 等の技術が高度化しているが，事件・事故などでも組織や人間が行う行為を分析，考察することが重要になる．そこで，組織や人間関係の分析を，**『組織・人間関係分析』**と定義する.

また，事件・事故では，発生時刻やその前後の直接的，間接的時刻を含め，それぞれの時刻や時刻間で発生した内容の考察を考える**『時系列分析』**を行うことも重要であり，，「組織・人間関係分析」と一緒に考察する.

勿論，組織・人間関係が明確に表面化していない場合や複雑な場合，更に，時刻が明確でない場合もあるため，過去の経験や推測で考察することもある.

2.2 組織・人間関係分析

今回の事案では自治体の業務委託処理であり，委託先業者社員と協力会社社員（再々委託先社員）**注)** が関係しており，当然ながら，自治体職員や紛失鞄の発見に努めた警察官が関係しているが，自治体職員，協力会社社員，及び委託先社員などと考えられる.

注) 当初，再委託先の社員と思われていたが，事故後，孫請け企業（再々委託先）の社員であることが判明している.

(ア) **自治体**側では，事故発覚前には，特定の職員（職位）が明確でないため，自治体社員とする

(イ) 委託先企業では，①社員 2 名（役職等は不明）②協力会社社員（USB メモリ保存の鞄を紛失した社員）

(ウ) その他： 警察官：直接的には関係ないと思われるが，紛失した鞄を協力会社社員と一緒に探した

2.3 時系列分析

今回の事案について，受託業者が，詳細な経過を時刻毎に掲載しているので，それを中心に記載するが， 6 月 24 日に USB メモリの入った鞄の発見があり，それを追加した.

今回の事案では，週次定例会（6 月 16 日開催）【業務は 21 日（火）に実行】から 6 月 23 日（木曜日）までの短期間であり，その経緯は以下のようになる[1].

6/16 (木) 10:30～11:30 毎週開催されている週次定例会議（木曜日）にて 21 日に給付金コールセンター（吹田市）のデータ更新作業を実施することを報告し、承認いただいた

6/21 (火) 17:00 市政情報センターから協力会社社員（以降、当該本人）1 名にて USB にデータ格納し、給付金コールセンターへ移動

18:00 コールセンター現地にて弊社社員 2 名、協力会社社員 1 名と合流、計 4 名。

18:00～19:30 給付金コールセンターにてデータ更新作業実施。

19:30～22:30 作業終了後、4 名で飲食。

22:30 解散後、飲食店を出たときは、当該本人の鞄所持を確認。

6/22 (水) 03:00 当該本人は路上で寝ていることに気づいたが、この時点で鞄が無いことに気づく。その後、徒歩で一旦、帰宅。

09:00 当該本人から弊社に 1 日休みの連絡あり。この時点で鞄紛失の報告なし。再度、当該本人が現地に捜索に行くが見つからず。吹田警察に紛失届提出。

14:00 当該本人から弊社へ鞄を紛失した旨、連絡あり。

14:30 弊社から当該本人に連絡し、鞄の中身を確認、USB メモリが含まれており、住民情報等のデータが含まれていることが判明。

14:30～15:45 作業担当者から状況および事実確認を実施。

15:45 尼崎市様へ今回の事象を報告。（行政法務部、情報政策課）

16:00 住民情報等の件数調査実施。尼崎市様へ件数を報告。（行政法務部、情報政策課）

6/22 (水) 21:00 尼崎市様（行政法務部）からのヒアリングにて上記経緯ならびに正確な件

Vol.2022-CSEC-99 No.17
Vol.2022-SPT-49 No.17
Vol.2022-EIP-98 No.17
2022/12/23

数を報告。
6/23 (木) 09:00～11:30 弊社社員にて鞄捜索を実施するが発見には至らず。
6/23(木) 11:00～ 尼崎市様による記者会見。
6/23(木) 12:00～ 尼崎市様からのご要請を受け、弊社参画のもと共同記者会見。
6/23(木)13:30～ 尼崎市長による定例会見ならびに記者からの質疑応答。
6/24(金) USB メモリが協力会社社員と警官により発見されたとの報告があった

2.4 調査報告書及びその検証

調査報告書は，自治体での情報管理業務手続強化や再発防止の取組を推進するにあたり，３名の調査委員に以下の３点を諮問したが，その内容が公開された[2].

1 当該事案への対処について
2 原因の検証について
3 再発防止策に関する事項について

報告書は約 40 ページあり，USB メモリ内部のアクセス有無の記録等，技術的な考察も行われているが，ここでは業務対応についてのみ考察した.

① 自治体サーバー室への管理カードが貸与されており，市政情報センターへの入退館許可だけでなく、サーバー室への入退室も登録された登録情報との照合により許可されたカードを使用する場合に限りサーバ室への入退室が可能

2.5 時系列分析及び調査報告書で見えてきたもの

非技術的セキュリティ（Human element）の観点からの考察を列挙する

① **管理カード利用**： サーバー室への入退館用だが，複数人で利用していた． 利用者各人に貸与すれば，入退室ログの確認も可能になり，未承認の利用者を防ぐことができる[i]. 今回は，管理カード利用での問題はないが.

② **情報機器の持込み**： 一部の自治体で，コンピュータ画面を撮影し，外部に持ち出した例も過去にあった. 今回の事案で，自治体職員，委託先社員のサーバー室への持ち込みを制限したが，もっと情報漏洩に敏感になる必要がある.

③ **セキュリティポリシー**：自治体は，職員や自治体内で作業を行う委託先社員へのセキュリティポリシーの遵守が不徹底. 例： (i) 二者間での機密情報の送受信でのファイルの暗号化やパスワード設定が不十分，(ii) スマホや情報端末管理など

④ **USB メモリ管理**： 自治体外への運搬規則（鍵付きケースに保管し，運搬車両で運ぶ）を委託業者は遵守していない. ただ，通信回線の高速化を考えれば，USB メモリのような可搬媒体での搬送でなく，オンラインで行うべきであろう

⑤ **データの消去**： 可搬媒体の利用がなくなれば，原則データ消去は限定される. サーバーやパソコンのハードディスクは原則，物理破壊を行う[ii].

⑥ **再委託，再々委託**： 一般論で言えば，国内外を問わず再委託，再々委託はかなりあると聞く. 一部の企業では名刺の作成や関連会社の所属社員として自社の業務を遂行させているケースもある. なお，一部マスコミでは，今回の再々委託先社員は，約 20 年，当該自治体の業務をやってきたとの報道もあり，隠す必要があったのだろうか？

⑦ **業務終了後の飲酒**： 委託先社員等 3 名と業務終了後飲食をし，そこで酩酊し，USB メモリの入った鞄を紛失した.

⑧ **監査**： 誰が監査（セキュリティ監査？）をやるのだろうか？ 業務監査やセキュリティ監査を行った個人的経験から言えば，今回のケースでは，自治体が監査を行うのであろう． 委託先企業の執務室が自治体職員のオフィスと離れていれば，関係者の来室を自治体に報告しない可能性が高い.

3. 非技術的スキルの確立

3.1 はじめに

今回は，再々委託の社員が酔って，USB メモリの紛失であるが，その裏に自治体職員や委託先社員等がおり，それらを組織／チームと考え『**組織事故**』とあらわす. 国内では，ヒューマンエラーを個人の問題ととらえることが多いが，今回も組織として対応できていれば，事故は防げたと考えられ，このような課題を筆者は『**セキュリティ心理学**』[3]と定義している． これは，組織事故やヒューマンエラーは，通常，『**悪意**』の想定がなく，サイバーセキュリティを考える場合，狭い範囲の議論になる恐れがある.

今回の USB メモリ紛失事案は，『**ノンテクニカルスキル**』等を考えるのが適切であろう.

3.2 ノンテクニカルスキル

(ア) **ノンテクニカルスキル（非専門技術）**は，**①コミュニケーション能力，②チームワーク、③リーダーシップ、④状況認識、⑤意思決定**など IT やサイバーセキュリティでの技術的分野でなく，これらのノンテクニカルスキルを利用してチーム全体で問題解決を目指すものと考えられる. 特に，④や⑤では，瞬時に対応できるスキルが必要になることもあり，作業終了後の飲酒（禁止の指摘）や USB メモリの搬送等は事前／直前に指摘する必要があった.

i ID カードではないが，開発環境で，同一のユーザ ID／PW を複数の開発者が利用し，約 56 万件の情報漏洩が発覚したが，犯人を特定できなかった

ii サーバー等，リース物件では，ハードディスクを物理破壊できないが，ハードディスク内を完全消去するソフトウェアを使うべき. リース物件では，ハードディスクの所有者はリース会社であっても，データの所有者（データオーナー）は自治体等である.

Vol.2022-CSEC-99 No.17
Vol.2022-SPT-49 No.17
Vol.2022-EIP-98 No.17
2022/12/23

(イ) 1976 年、NASA（アメリカ航空宇宙局）は，技術・経験豊富なベテランクルー36 組を集め，シミュレータによる膨大な実験を行った。 その結果、適切な状況認識を行いチームワークが取れていれば無事に乗り越えられる負荷・トラブルから生還出来たのは，たった 1 組であった。この結果、安全運航に利用可能な資源、即ち、人間や情報などの有効活用を目指し、CRM（Cockpit Resource Management）を公表した。CRM は、

①積極的コミュニケーション，②機長のリーダーシップ，③適切な権威勾配，④正確な意思決定

が人的航空事故減少に重要とした．当初コックピット内からであったが，チームでの改善を目指し，客室乗務員、地上運航管理者、整備士等も含め、Crew Resource Management: CRM」とした[4].

(ウ) 医療安全では，**チームステップス**：Team STEPPS (Team Strategies and Tools to Enhance Performance and Patient Safety) [5]があり，良好なチームワークを確立し、医療行為全般のパフォーマンス（医療行為の経過から結果までの全過程の行い方）と患者の安全性を高めるために作成されたチーム戦略

(エ) 権威者と他のスタッフ等の落差を『**権威勾配**』と言い，権威者は自分が過ちを犯すことはないと考え，周りの助言をすべて無視することがある．このため，誰も何も言わなくなるが，権威者も過ちを犯すことがあり，エラーや事故につながる． 権威者に対しても，他者に対しても，怯えたりせず，自然体で対応できることを，『**心理的安全性**[iii]』と呼んでいる．

4. 脆弱性への対応を考える

4.1 情報機器，可搬媒体の取り扱い

今回の事案は，鞄にいれた USB メモリの紛失で，**表 1** で示したように，人的な脆弱性（誤送信，紛失，盗難等）は，技術的インシデントより遥かに多い．実際，情報機器・可搬媒体の紛失等は，飲酒時だけの問題ではない．基本は，可搬媒体の利用をやめるべきだが，直ちに対応できないこともあり，以下のようなことを教育・訓練すべきであろう．

【電車内に情報機器や鞄を忘れる人の特徴】

① 普段，何も持たない
② 電車では，荷物を網棚にあげ，座っても荷物を膝上に置かない
③ 情報機器／可搬媒体を持っているのに，帰りに飲酒する
④ 荷物が 2 つ以上あり， 1 つにまとめて持てない

今回の事案では，③に相当するが，普段，鞄など持たない ① に相当する可能性もある．

【可搬媒体への対応】

① 自治体での対応は，総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」[8]にあり，(i) 端末には利用許可された媒体のみ接続可能とする，(ii) データは暗号化しパスワードを設定する，(iii) 利用媒体は、全て管理し利用履歴を残せる，(iv) データの受け渡しには、必ず情報セキュリティ管理者の承認と承認記録を残す
② 可搬媒体は単独で持ち出さず，紛失防止用のストラップや超小型の GPS 等を利用し，紛失等を防ぎ，紛失時の発見を容易にする
③ 前述したが，最大の防止策は，可搬媒体を利用しないこと．今回でも，直接，サーバ室に保存してあるデータを給付金コールセンターにオンラインで送付できれば防止可能であった．

順位	%	2021 年 日本（n=1,616）
1	25.2	電子メール，FAX，郵便物の誤送信・誤配送
2	14.9	標的型メール攻撃
3	14.5	情報機器，外部記憶媒体の紛失・置忘れ，棄損
4	11.9	マルウェア感染
5	11.4	社員証，業務書類等物品の紛失，置忘れ，棄損
6	10.6	システム設定ミス，誤操作
7	9.0	情報機器 電子記憶媒体 紙媒体等の盗難・紛失
8	6.1	DoS／DDoS 攻撃
9	5.3	ランサムウェアによる金銭等の要求
10	4.0	退職者，転職者による在宅時に利用していた情報の使用

影： サイバー攻撃

表 1 セキュリティ事件／事故 [6]

5. セキュリティ管理／教育・訓練を考える

5.1 はじめに

今回の事案は，鞄にいれた USB メモリを泥酔して紛失したもので，自治体の住民のデータが含まれていたことが直接的原因である．

(1) 権威勾配（逆権威勾配），心理的安全性

ノンテクニカルスキルでも，短時間の教育・訓練で身につくものではなく，無意識に対応ができるようになっていれば，事故を防げた可能性もある．

(ア) 週次定例会議（6/16 木）開催で，21 日のデータ移管作業概要は，自治体，受託業者 双方からなかった

(イ) コールセンター作業後，委託先社員 2 名，再委託先社員 1 名，本人の 4 名で，飲食店で会食（飲酒）した．

定例会議では，データ移管は，短期間の作業であるが，住民情報の取り扱いであり，非常に重要な事柄だが，比較的短時間で終わる作業との認識が，双方ともあり，また，暗黙の了解があったのではないかと考えている．

また，USB メモリを鞄の中とはいえ，持ち帰りながら，

iii **心理的安全性（Psychological safety）**とは，組織内で自分の考えや気持ちを誰に対しても言える状況をいう[11].

Vol.2022-CSEC-99 No.17
Vol.2022-SPT-49 No.17
Vol.2022-EIP-98 No.17
2022/12/23

飲酒すべきでないことを委託先社員は指摘すべき．また，再々委託先社員にもその認識が感じられない．

推測であるが，再々委託先社員と委託先社員（２名）は，年齢，経験等も逆転している可能性もあり，委託先社員 2 名共，住民情報が入った USB メモリを持って，飲食する，即ち，嫌なこと（飲酒しないこと）を言う教育・訓練が不十分であり，一種の**権威勾配（逆権威勾配）**があり，心理的安全性が確保できず，結果として，委託先社員と再々委託先社員の間で，自由に意見を述べる「心理的安全性」が確保できなかった可能性があると考えている．

(ii) 再々委託先社員について

今回の再々委託先社員は，USB メモリの紛失発覚後，委託企業から，再委託でなく，再々委託であることが明らかにされたが，約 20 年自治体のシステムに携わっており，新任の自治体職員に対しても，システム関連知識を職員に教えていたとあるとの報道もある[9]．

この再々委託先社員は，20 年間，大きな事故も起こさず業務推進を行ってきたのであれば，自治体業務に対しての知識・経験は，新任の自治体職員や委託先社員より高いものがあると考えている．

なお，再委託先，再々委託先がどのような契約形態であったかが不明であるが，この再々委託先社員は，6/16 開催の週次定例会議（木）終了後，委託先社員（データ移行作業主任）に，「来週よろしく」と言われ，翌 21 日、自治体のサーバー室（市情報センター3 階）の給付金サーバーに保存されている個人データを USB メモリにコピーしてコールセンターまで持って行くことを依頼された．作業の重要性はあるが，作業自体は難しいものではないと思われる．

再々委託社員は，業務遂行レベルが劣っていることもないと思われるが，ノンテクニカルスキル，特に状況認識等が十分でなかった感じを受ける： ノンテクニカルスキルやセキュリティポリシー等を十分理解していない，あるいは，教育・訓練を受講していない可能性を感じる．

(iii) ベンダー・ロックインについて

今回もベンダー・ロックインが報じられているが，**ベンダー・ロックインは，原因ではなく，結果である**．ベンダー・ロックインは，一種の『**丸投げ**』であるが，それを正常に戻すことは可能であろう．

特に，自治体等では IT やセキュリティの専門家が少ない／いないのが現状で，CIO や CISO は，多くの場合，『あて職』になっている．

興味がないものは，目の前にあっても，見えない，聞こえないことは，心理学では，多々例があるが，有名な『**見えないゴリラ**』は，その一例である[iv][7]．

知らないことは罪ではないが，
興味がないことは大罪である

知らないことを聞くことを躊躇する人が多いが，知らないことを知らないと言い，それを聞くことができるようになることは，**心理的安全性**に繋がる．

(iii) 自治体 vs 委託先企業

6 月 16 日に，「週次定例会議」が開催されたが，自治体センターから，委託先コールセンターへデータ移動については，話題にならなかったと調査報告書にはある．委託先社員が，何故，言わなかったのかもあるが，自治体職員が確認しなかったことも理解できない．21 日にデータ更新を行うことが分かっており，総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」の内容を理解していれば，データ移送も含め，その処理手順の確認を行うべきであった． ガイドラインの内容をすべて記憶していなくても，手順の確認（説明をさせること）によって，必要な事柄を思いだすことができた可能性はある．

(iv) 指紋認証システム導入の脆弱性

指紋認証システムの導入により，自治体サーバー室への入室を制限するため，システムの導入を行ったが，これは自治体職員が立会し，委託先社員が勝手にデータを持ち出すことを改善するためとしている[10]．

指紋認証システムでは，当然ながら，指紋登録をしていない委託先社員は，自治体職員に声掛けをし，サーバー室に入ることになる．自治体職員がサーバー室にいなければ，職員が在籍する所に声掛けをする．長時間の作業の場合，トイレに行くこともあるが，職員は対応できるようにしなければならない．認証システムに未登録で，職員の立会がなければ，室外にでる場合，ストッパーでドアを開けて対応する，入室は「**友連れ**」を行うのが，個人的経験であった．セキュリティ技術の導入が効果的かの検証が大切になる．

6. おわりに

本稿の締め切り直前（11 月 28 日）に，市長の諮問委員会からの調査報告書[12]が公開された．原稿の投稿を断念しようと考えたが，『多分，技術的観点からの調査報告が中心になるのでは？』との指摘があり，本稿では，『**組織・人間の脆弱性**』を中心に，書きあげた．

ただ，調査報告書を詳細に読んでいない部分もあり，齟齬がある可能性もあることをお断りする．

かつて，2012 年に発生した「**ストーカー殺人事件**」を基に，自治体で「**セキュリティ心理学**」の教育・訓練を行い，査読論文を書き上げた**[13]**．

今回の事案についても，更に，検討を重ね，教育・訓練，論文に繋げていきたい．

---

iv **非注意性盲目**と言われ，『**見えないゴリラ**』が有名で，ビデオ内で、白シャツの選手へバスケットボールがパスされるので，パス回数を数えるもの（黒シャツの選手のパスは無視する）．
https://youtu.be/vJG698U2Mvo

Vol.2022-CSEC-99 No.17
Vol.2022-SPT-49 No.17
Vol.2022-EIP-98 No.17
2022/12/23

謝 辞

（公社）日本心理学会 セキュリティ心理学研究会メンバー及び研究会参加者の方々，九州大学 リカレント講座（小出洋先生，元 IT 副大臣 福田峰之先生，藤岡福資郎先生，及び セキュリティ心理学講座３期生）から貴重な意見を頂きました.

参考文献

[1] 住民税非課税世帯等に対する臨時特別給付における個人情報を含むＵＳＢメモリの紛失について，2022.06.24，https://www.biprogy.com/pdf/topics/info_20220624_1.pdf
[2] 尼崎市 USB メモリ―紛失事案調査委員会，尼崎市 USB メモリ―紛失事案に関する調査報告書，2022.11.28，https://www.city.amagasaki.hyogo.jp/_res/projects/default_project/_page_/001/030/947/1128houkokusyo.pdf
[3] 内田勝也，セキュリティ心理学入門，学術研究出版，2020
[4] 村上 耕一／斎藤 貞雄、機長のマネジメント―コックピットの安全哲学「クルー・リソース・マネジメント」、1997、 産能大出版部
[5] 慈恵医大附属病院、医療安全文化の醸成に向けて、https://www.hosp.jikei.ac.jp/diagnosis/administration/security/security_02.html
[6] NRI Secure，NRI Secure Insight 2021，https://www.nri-secure.co.jp/download/insight2021-report
[7] C. チャブリス／D. シモンズ，錯覚の科学，20011，文芸春秋
[8] 総務省，地方公共団体における情報セキュリティポリシーに関するガイドライン(令和 4 年 3 月版)，2022.3
[9] 読売新聞，ＵＳＢメモリー紛失業者、「他社では困難」と３０年以上の「ベンダー・ロックイン」，2022.07.04
[10] 読売新聞，全市民の個人情報入りＵＳＢの一時紛失受け、市のサーバー室に指紋認証…委託先も切り替えへ，2022.09.17
[11] エイミー・C・エドモンドソン（Amy C. Edmondson），恐れのない組織――「心理的安全性」が学習・イノベーション・成長をもたらす，英治出版，2021
[12] 尼崎市 USB メモリ―紛失事案調査委員会，尼崎市 USB メモリ―紛失事案に関する調査報告書，2022.11.28
[13] 内田勝也，誘導質問術からみた個人情報漏えいの考察，情報処理学会，論文誌，2015