明治大学総合数理学部

2022 年度

広告配信手法検証のための独自アドサーバの試験実装とブラウザの評価

先端メディアサイエンス学科

田口 勇翔

目次

第 1 章

はじめに

GDPR や個人情報保護法の改正 [1] により, cookie を含む個人情報の保護は強化され, インターネット上の個人を識別する技術を規制する傾向にある. 例えば, Apple 社は Safari にトラッキング制限機能である ITP(Intelligent Tracking Prevention)[2] を搭載し, サードパーティ cookie をブロックしている. ブラウザで最もシェア率の高い Chrome は 2024 年にサードパーティ cookie を規制する予定である. サードパーティ cookie を用いたターゲティングの手法が規制されることで, ウェブ広告業界は大きな変化にさらされると考えられる.

多くのブラウザや広告の媒介サイトを含めたプラットフォーマでサードパーティ cookie が規制されることで, ITP 実装後に CNAME トラッキング [4] やブラウザフィンガープリント [5] が注目されたように, 新たな手法が導入される可能性がある, 例えば Google はサードパーティ cookie に替わる広告配信手法としてプライバシーサンドボックス [3] の構想を提案している. そのような未知の広告配信手法を検証する必要があり, また検証には実環境の調査のみならず, 広告配信側と広告閲覧側の両面から観察する必要がある.

そこで, 本研究は次の環境を実現することを目的とする.

- 未知な広告配信手法を検証できる環境
- ブラウザや拡張機能の cookie, トラッキング, 広告ブロック機能を検証できる環境

このため, 本手法では新しい手法を組み込むためのプレーンなアドサーバを開発した, また, 広告を閲覧したときのブラウザの挙動を調査した.

第 2 章

アドサーバの試験実装

2.1　概要

アドサーバのシステム構成図を図 A.2 に示す．システムの ER 図を図 2.2 に示す．開発には PHP, Javascript, MySQL を使用した．

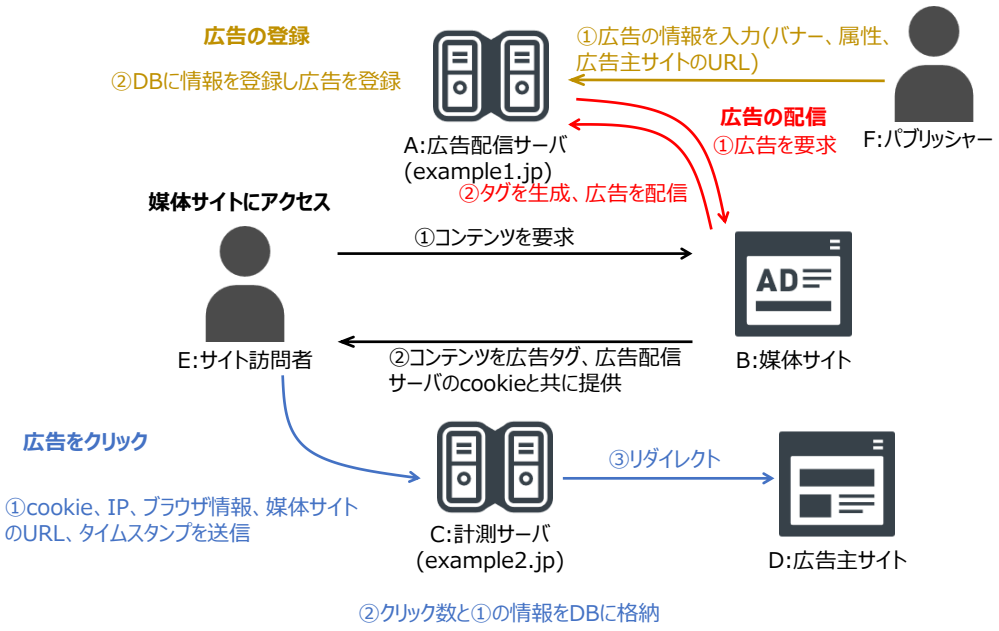

図 2.1　システム構成図

図 2.2　データベース構成の ER 図

2.2　機能

広告登録

パブリッシャ F はシステム A にログイン後, 広告を登録する．バナー, 広告の属性, 広告の目的のサイトの URL を登録する．入力された情報は A のデータベースに保存される．サイト訪問者 E が媒介サイト B を閲覧するたびに, 広告のインプレッション数, クリック数を記録する．

広告タグの生成

媒体サイト B は広告配信サーバ A に広告タグを要求する．タグは広告表示およびインプレッション計測のための iframe タグと, 透明で 1×1 サイズの gif に cookie が埋め込まれユーザを識別するための img タグである．

Listing 2.1　広告タグの例

```
1 <img src="https://example1.jp/tracking.php"></img>
2 <iframe src="https://example1.jp/AD_iframe.php" scrolling = "no" height = 500 width =
  500></iframe>
```

なお, 広告配信サーバ A のドメインは example1.jp であり, 媒介サイト B のドメインと異なる．

広告の表示

広告タグを埋め込まれた媒介サイト B にアクセスした訪問者 E は, コンテンツとともにバナー広告が配信される．img タグにより cookie が埋入される．iframe タグが読み込まれた時点で広告のインプレッション数がカウントされる．ユーザにどの広告を表示するかについて, cookie を用いたターゲティングが可能である．

Listing 2.2　img タグによる cookie 配信

```
setcookie("user",$value,[
        'SameSite'=>'None',
        'secure'=>'true',
        ]);
header("Content-type:image/gif");
echo base64_decode('R0lGODlhAQABAIAAAP///wAAACH5BAEAAAAALAAAAAABAAEAAAICRAEAOw==');
```

広告のクリック

訪問者 E が広告をクリックすると, 計測サーバ C に遷移する. 計測サーバ C はクリック数をカウントし, またユーザの cookie, IP, 媒体サイトの URL(どこのサイトから広告がクリックされたか), タイムスタンプをデータベースに保存し, 広告の目的のサイトにリダイレクトする.

第 3 章

各ブラウザでの動作

3.1　概要

開発したアドサーバにより, 広告が適切に配信されるか, また広告として扱われるかを検証するため, 広告を埋め込んだ媒介サイトに各ブラウザでアクセスした. 広告配信例を図 3.1 に示す. また, サードパーティ cookie の扱いについて調べた. 媒介サイト B に広告配信サーバ A の iframe, img タグを埋め込んでサードパーティ cookie として扱った. 調査したブラウザは Firefox, Chrome, Edge, Safari, brave であり. ブラウザの設定はデフォルトであり, 初回アクセス. 結果を表 3.1 に示す.
広告表示について, 広告が表示された場合を○, 広告が表示されなかった場合を×とした. cookie の埋入について, cookie が埋入された時○, cookie が拒否された時×とした.

図 3.1　広告配信例

表 3.1　各ブラウザでの動作

ブラウザ	広告表示	cookie
Firefox	○	×
Chrome	○	○
Edge	○	○
Safari	○	×
Brave	×	×

3.2　Firefox

Firefox はデフォルトの設定で広告は配信されたがサードパーティ cookie は即消去され, サーバで cookie の情報を読み取ることができなかった. ただし一度設定でサードパーティ cookie を許可してからサーバからサードパーティ cookie を配信すると. その後設定でサードパーティ cookie をブロックしても消去されずサーバで読み取ることができ, かつ有効期限もサーバで指定したものから変化がなかった.

3.3　Chrome, Edge

Chrome, Edge はデフォルトの設定で広告が配信され, またサードパーティ cookie が許可されており, サーバでユーザの cookie を読み取ることができた. ただしサーバで SameSite 属性で None を指定する必要がある. また Secure 属性が true でなくてはいけない. つまり広告配信サーバが SSL 環境 (https) でないといけない. これらを満たさないときアドサーバでサードパーティ cookie を配信することはできなかった.

3.4　Safari

Safari ではデフォルトの設定で広告は表示されたが, サードパーティ cookie は即消去され, サーバで cookie の情報を読み取ることができなかった.

3.5　Brave

Brave ではデフォルトの設定で広告がブロックされっ図 3.2 のように表示されなかった. サードパーティ cookie は配信された. ただし, firefox 同様一度設定でサードパーティ cookie を許可してからサーバからサードパーティ cookie を配信すると. その後設定でサードパーティ cookie をブロックしても消去されずサーバで読み取ることができた.

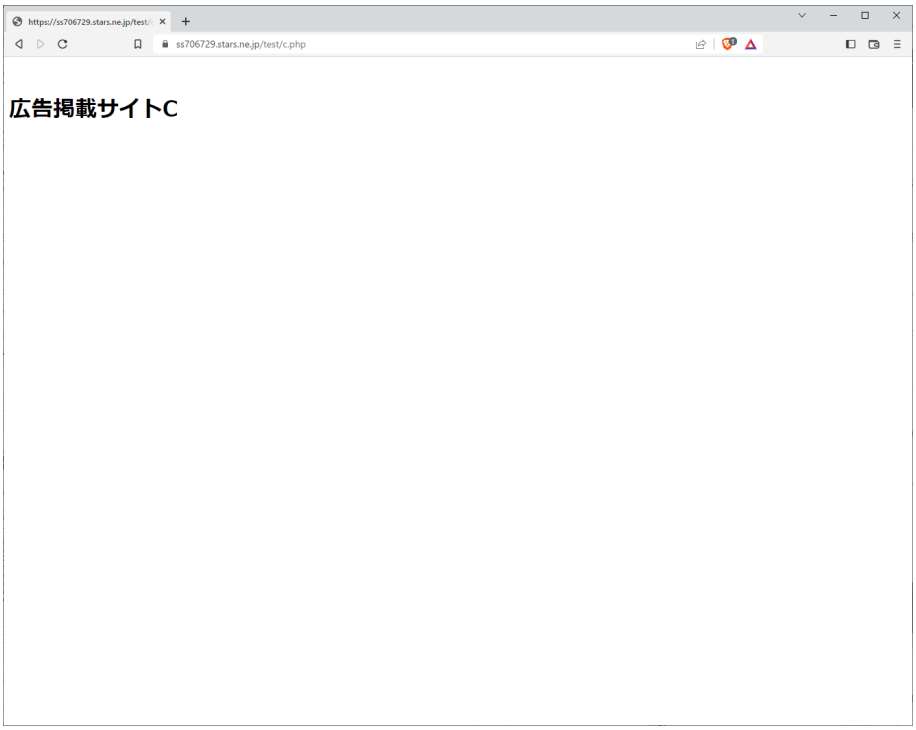

図 3.2　brave での画面

第 4 章

おわりに

本研究では, 未知の広告配信手法を検証するためのアドサーバを試験実装した. アドサーバはミニマムな構成であり拡張が容易になっているため新しい手法を取り入れやすい. どの広告を配信するかなどのアルゴリズムを組み込んだり, 広告配信を非同期処理にすること, UI を改善することでより実環境のアドサーバに近づけ, より本格的な検証に利用することを計画している.

参考文献

[1] 野村総合研究所, “日米欧におけるデジタル広告とプライバシーに関する規制の動向” (https://www.kantei.go.jp/jp/singi/digitalmarket/kyosokaigi_wg/dai2/siryou2.pdf, 2022 年 12 月参照).

[2] Apple, “Safari Privacy Overview” (https://www.apple.com/jp/safari/docs/Safari_White_Paper_Nov_2019.pdf, 2022 年 12 月参照).

[3] Google, “The Privacy Sandbox” (https://privacysandbox.com/intl/ja_jp/, 2022 年 12 月参照).

[4] YanaThe CNAME of the Game: Large-scale Analysis of DNS-based Tracking Evasion, arXiv:2102.09301.

[5] PIERRE, NATALIIA, BENOIT, GILDAS, Browser Fingerprinting: A survey, arXiv:1905.01051v2.

[6] Mozilla, “Firefox Now Available with Enhanced Tracking Protection by Default Plus Updates to Facebook Container, Firefox Monitor and Lockwise” (https://blog.mozilla.org/en/uncategorized/firefox-now-available-with-enhanced-tracking-protection-by-default/, 2022 年 12 月参照)

付録 A

インシデントの到着間隔を予測するウェブサイトの開発とモデルの評価

A.1　はじめに

2020 年における個人情報が漏洩した上場企業の数は 88 社, 事故件数は 103 件となり, 過去 9 年間で最多となった [1]. 2021 年 6 月 30 日に NTT グループに属する物流会社の NTT ロジスコにおいて, 同社が管理しているサーバ群に外部から不正アクセスがあり, 配送先情約 500 万件の情報の流出するセキュリティインシデントが発生した [2]. これらのセキュリティインシデントを防ぐため, 組織は現状のインシデントのリスクを把握して各種対策を講じる必要がある. そのため, 池上らはインシデントの履歴に基づき, インシデント生起の数理モデル [3] を作成している. しかし, リスクの算出にはパラメータの算出が必要であり, 誰もが利用できる状態になかった.

そこで, 本研究では, 池上による先行研究 [3] を元に, インシデント到着間隔を誰でも簡単に定量化できることを目的とする. そのために, R, PHP を用いて組織が次にインシデントを受ける日を予測し, 1 年以内のインシデント発生確率を求めるウェブサイトを新規に開発した. 本サイトを用いたモデルの評価を報告する.

A.2　データセットと先行研究

A.2.1　JNSA データセット

日本ネットワークセキュリティ協会 (JNSA) は, 組織の個人情報漏洩インシデントについて被害人数, 漏洩原因, 漏洩経路などの情報を収集している [5]. 本研究では, 2005 年から 2018 年までの本データセットに関して,「情報管理・保有責任者 (企業名)」の項目の表記ゆれを修正して使用した. 例えば, 組織名が○○銀行××支店や○○××店であれば○○銀行や○○に統一, 前株, 後株の誤入力を修正した.

A.2.2　CSR データセット

東洋経済新報社が毎年主要企業 1413 社に対して CSR(corporate social responsibility) に関する調査を行いデータセットを販売している [4]. [3] と同様に, 本研究ではデータセットからセキュリティに関する表 A.1 の 17 の項目を利用する.

表 A.1　情報セキュリティに関連する CSR17 項目

項目 ID	質問項目	略称
C122	内部告発者の権利保護に関する規定制定	告発保護
C139	内部統制委員会の設置	内統委員
C147	CIO(最高情報責任者) の有無	CIO
C150	CFO(最高財務責任者) の有無	CFO
C161	プライバシー・ポリシーの制定	PP
C153	情報システムに関するセキュリティポリシー	SP
C155	情報システムのセキュリティに関する内部調査	内部監査
C157	情報システムのセキュリティに関する外部調査	外部監査
C159	ISMS(情報セキュリティマネジメントシステム) 認証	ISMS
C120	内部告発窓口 (社内) の設置	内部窓口
C202	内部告発窓口 (社外) の設置	外部窓口
C207	業務部門から独立した内部監査部門の有無	独立監査
C227	リスクマネジメント・クライシスマネジメント体制の構築	RM・CM
C229	リスクマネジメント・クライシスマネジメントの基本方針の有無	RM・CMP
E082	環境監査の実施状況	環境監査
E087	観光マネジメントシステムの構築	環境 M
K136	労働安全衛生マネジメントシステムの構築の有無	労働 M

A.2.3　池上のインシデント発生間隔モデル

概要

池上らは, 過去に 4 回以上インシデントを起こした組織に対して最尤推定を用いた負の二項分布への当てはめによるインシデント発生間隔予測モデルと, そのパラメータである平均到着間隔 μ を予測するモデルを提案している. ある組織が過去に m 回インシデントを発生したとする. インシデント発生間隔を d_1, d_2, ... , d_{m-1} としたときに, d_1, d_2, ... , d_{m-2} を学習用データ, d_{m-1} を評価用データとし, 学習用データの最尤推定により負の二項分布のパラメータを次の様に推定し, 累積確率分布を求めた.

負の二項分布について, 1 日の発生確率が p のインシデントが発生するまでにかかる日数の確率変数を D とすると, d 日に発生する確率は

$$Pr(D = d) = \binom{d+r-1}{d} p^r (1-p)^d$$

で与えられる. 期待値である平均到着間隔 μ は

$$\mu = \frac{(1-p)r}{p} = \frac{d_1 + d_2 + \ldots + d_{m-2}}{m-2}$$

で表される.

組織がインシデントを X_1, X_2, ..., X_n 日後に発生させたときの負の二項分布の尤度関数は

$$L(p, r; x) = \prod_{i=1}^{n} \binom{n+r-1}{n} p^r (1-p)^{x_i}$$

で表され, その対数は

$$\log L(p, r; d) = \sum_{i=1}^{n} \log \binom{n+r-1}{n} p^r (1-p)^{x_i} + nr \log p$$
$$+ \log(1-p) \sum_{i=1}^{n} x_i$$

となる.

$\log L(p, r; d)$ が最大となる r, p を求める.

R の MASS パッケージの fitdistr では, 負の二項分布において, BFGS 法による対数尤度関数の最大化が行われる.

図 A.1 に, 岡山県が過去に起こしたインシデントを例に, 学習用データ, 評価用データの求め方について示す.

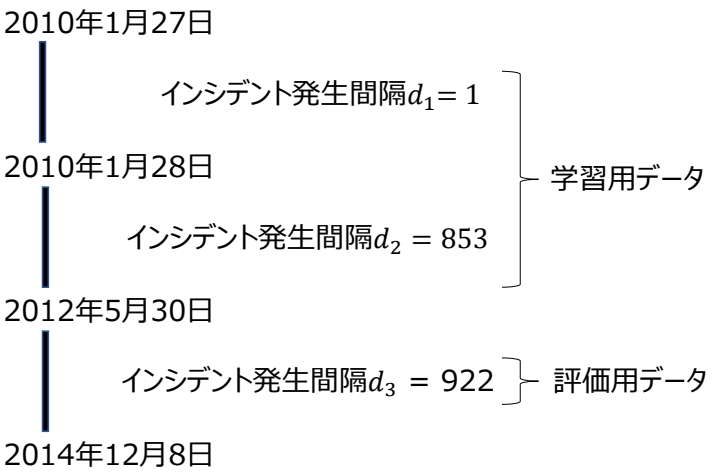

図 A.1　学習用, 評価用データ

平均到着間隔 μ についての一般化線形モデル

池上ら [3] は, インシデント発生間隔モデルのパラメータである平均到着間隔 μ についての一般化線形モデルを提案している.

$$\hat{\mu} = e^{\alpha+\beta_k k_j+\beta_g g_j+\beta_1 x_1+\ldots+\beta_{17} x_{17}}$$

k, g は業種, 従業員数であり, x_1, x_2, . . . , x_{17} はセキュリティに関する表 A.1 の 17 項目のマネジメントの有無である. 各係数を表 A.2 に示す.

表 A.2　一般化線形モデルの係数

		Estimate
α	(Intercept)	8.96
k	医薬品	-0.14
	運輸, 物流	-0.07
	機械	-0.04
	金融 (除く銀行)	-0.31
	銀行	-1.06
	建設, 資材	-0.37
	自動車, 輸送機	0.00
	商社, 卸売	-0.12
	小売	-0.30
	情報通信・サービスその他	-0.18
	食品	-0.02
	素材, 科学	-0.05
	鉄鋼, 非鉄	-0.03
	電気, 精密	-0.08
	電気, ガス	-2.24
	不動産	-0.46
g	LOG(従業員数)	-0.07
x_1	ISMS	0.04
x_2	CIO	-0.07
x_3	CFO	0.01
x_4	外部窓口	0.01
x_5	内部窓口	-0.07
x_6	告発保護	0.06
x_7	内統委員	-0.01
x_8	PP	0.00
x_9	SP	-0.01
x_{10}	内部監査	0.01
x_{11}	外部監査	-0.07
x_{12}	独立監査	0.02
x_{13}	RM_CM	0.03
x_{14}	RM_CMP	-0.08
x_{15}	環境監査	-0.03
x_{16}	環境 M	0.10
x_{17}	労働 M	0.00

.

A.3　インシデントリスク予測サイトの開発

A.3.1　概要

池上モデルを基に, 3 回以上インシデントが発生した組織が, 次のインシデントまでの日数 $\hat{x}$ と 1 年以内のインシデント発生確率 $\hat{p}$ を予測するウェブサイトを開発した.

池上モデルでは学習用データと評価用データに分けられていたためインシデントの発生回数が 4 回以上の組織を対象にしたが, 本サイトはすべてを学習用データとして用いる. よって, 過去のインシデント発生回数が 3 回以上の組織を対象にする.

過去のインシデント発生日を入力する部分は PHP, 計算とグラフの出力は R の MASS パッケージの fitdistr を用いた. 図 A.2 にシステム構成図を示す.

負の二項分布のパラメータで平均到着間隔の $\hat{\mu}$ を推定するモデルについても, 表 A.1 の CSR データセットのセキュリティに関する 17 の項目についてのモデルを用いて予測するサイトを実装した.

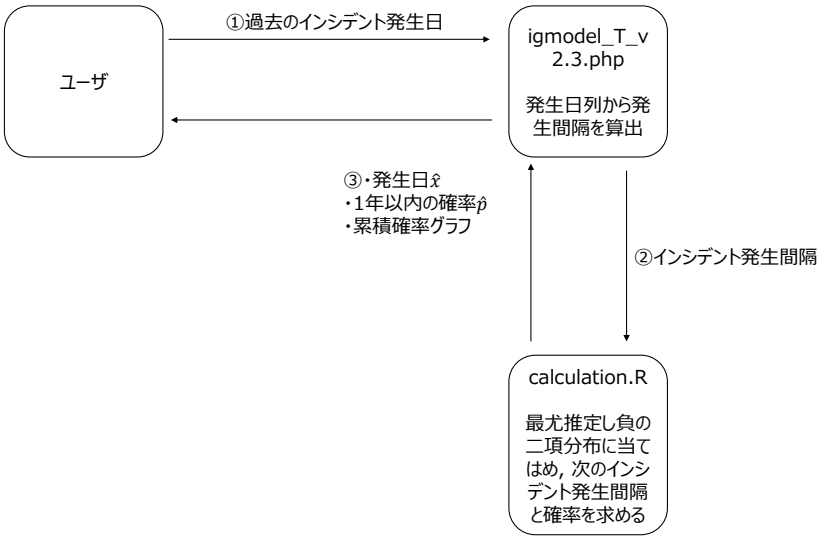

図 A.2　システム構成図

A.3.2　入力と出力

組織の過去のインシデント発生回数 m, インシデントの発生日 d_1, d_2, ... , d_m を入力する. 平均到着間隔 μ を推定するサイトの場合, 業種, 従業員数と, CIO の有無, プライバシーポリシーの制定など表 A.1 の CSR のセキュリティに関する 17 の項目について入力する. 平均到着間隔を予測するサイトの例を, 図 A.3 に示す, 1 年以内のインシデント発生確率 $\hat{p}$ と, 次のインシデントまでの日数 $\hat{d}$ の予測と, 累積確率分布のグラフを与えている.

1年以内のインシデント発生確率は59.88221%です

次にインシデントが発生するのは1020日後です(p=0.8)

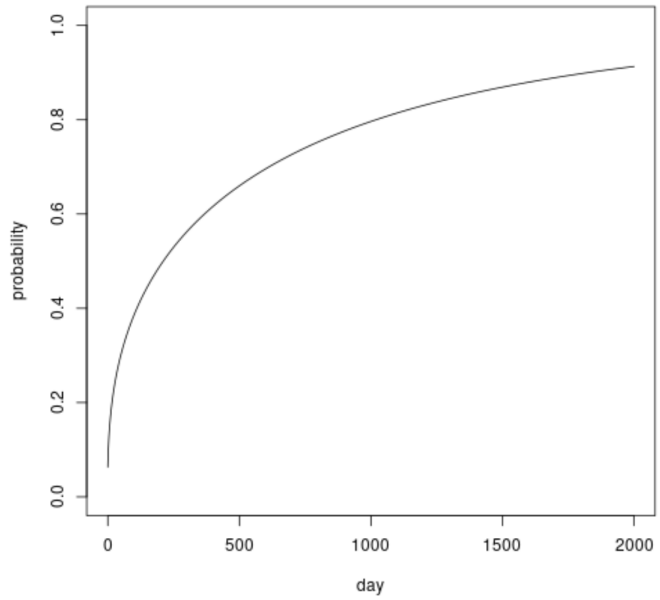

図 A.3　確率分布モデルでの出力結果

A.3.3　被験者実験

開発したサイトをユーザが正しく使えるか検証することを目的に, 20 代男性の学生 3 人の被験者に対してサイトを使って適切な出力結果が得られるか実験した. その結果 3 人中 3 人の被験者は正しく操作し結果を得ることができた.

A.4　モデルの評価

A.4.1　モデルの評価方法について

JNSA データセットに記載されているかつ, 過去にインシデント発生回数が四回以上発生した組織を評価にの対象にする. 対象の 440 組織の業種を表 A.3 に示す. 負の二項分布の累積確率が 0.8 になるときの $\hat{d}$ を「次のインシデントの発生日数」とした. 1 年以内のインシデント発生確率 $\Pr[\mathrm{X} = 365]$ を求める. 誤差は

$$g = |\hat{d} - d_{m-1}|$$

とする. さらにモデルの予測結果と評価用データを比較し, 二種類の精度を求める.

評価 (1) は, モデルによって予測された日数までインシデントが発生しなければ正解とする. すなわち,

$$\hat{d} \leq d_{m-1}$$

を満たす時正解とする.

評価 (2) は, 評価データとの値が近ければ正解とした. すなわち,

$$\hat{d}/2 \leq d_{m-1} \leq 3\hat{d}/2$$

を満たすとき正解とする.

表 A.3　対象組織の業種

業種	組織数
公務	170
金融, 保険	108
教育, 学習支援	38
情報通信	33
医療, 福祉	30
電気, ガス	25
卸売業, 小売	18
不動産, 物品賃貸	16
建築	9
サービス	8
運輸, 郵便	7
複合サービス	7
製造	5
生活関連, 娯楽	3
林業	1

.

A.4.2　評価結果

表 A.4 に予測日数の統計量を示す. 表 A.5 に結果を示す. 評価 (1) は, 正解数が 261 となり, $261/440 \fallingdotseq 59\%$ となった. 評価 (2) は, 正解数が 130 となり, $130/440 \fallingdotseq 30\%$ となった

A.4.3 考察

評価 (1) によって求められた精度は安全という面であれば有用であるが, 評価 (2) より, 実際のインシデント発生間隔を正確に当てることは精度が高くないと考える.

表 A.4　発生間隔予測の統計量

	平均	最小値	最大値	中央値	標準偏差
インシデント回数	9.8	4	196	5	14.7
正解値 d_{m-1}(day)	628.6	1	4345	399	705
予測値 $\hat{d}(day)$	667.2	36	2832	514	551.8
誤差 g(day)	615	4	4260	407.5	619.6

表 A.5

	正解率
評価 1	59%
評価 2	30%

A.5　おわりに

本研究では, インシデント被害間隔を誰でも簡単に定量化できるサイトの開発を行った. サイトはインシデント被害間隔の定量化および組織が次のインシデントまでの安全な日数を求めることに有用である. インシデント発生間隔を正確に当てるためには, モデルの精度をさらに上げる必要があり, モデルに合わせたサイトの修正が必要である.

参考文献

[1] 東京商工リサーチ, 「上場企業の個人情報漏えい・紛失事故」調査（2020 年）(https://www.tsr-net.co.jp/news/analysis/20210115_01.html, 2021 年 11 月参照).

[2] NTT ロジスコ, “不正アクセスによる個人情報流出の可能性に関する調査結果のご報告” (https://www.nttlogisco.com/info/2021/1806/, 2021 年 11 月参照).

[3] 池上, 菊池, 企業のサイバーインシデント予測〜あなたの会社は何年後にサイバーインシデントを受けるか？〜, Symposium on Cryptography and Information Security 2020(SCIS-2020), pp.20-29, 電子情報通信学会, 2020.

[4] 東洋経済データサービス, “CSR データ”(https://biz.toyokeizai.net/data/service/detail/id=321, 2021 年 5 月参照).

[5] 日本ネットワークセキュリティ協会, 2018 年 情報セキュリティインシデントに関する調査報告書【速報版】, 2019.

[6] 東京大学教養学部統計学教室, 統計学入門 (基礎統計学 I), pp.217-218, 東京大学出版社, 1991.

謝辞

本研究を行うにあたり，多くの方より御指導いただきました．特に，多大なる御指導を受け賜りました，明治大学総合数理学部先端メディアサイエンス学科，菊池浩明教授に深く感謝申し上げます．予備実験等に協力してくださった菊池研究室の皆様並びに先端メディアサイエンス学科の方々に深く感謝の意を表するとともに，謝辞とさせていただきます．