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？～

2020. 01. 31.

SCIS2020

池上和輝　菊池浩明

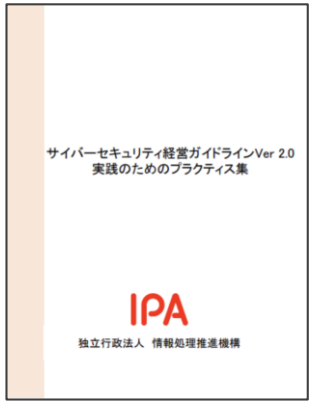
明治大学大学院　先端数理科学研究科 先端メディアサイエンス専攻

はじめに


県庁HDD 転売18個
税滞納など流出 9個未回収
神奈川県発表

■内部犯行、不正アクセスによる情報漏洩増加
- 2019年12月6日、神奈川県庁のHDD18個が流出
- (2018年 443件)

■経済産業省が「サイバーセキュリティ経営ガイドライン」作成
- 大、中小企業にセキュリティ対策を推進
  - リスクの特定と対策の実装
  - インシデントに備えた対策等の必要性



■組織に適切なマネジメント投資、リスク認識が求められる

研究目的

- 組織毎のインシデント発生リスク、インシデント発生間隔に与えるマネジメント効果を定量的に示す

関連研究比較

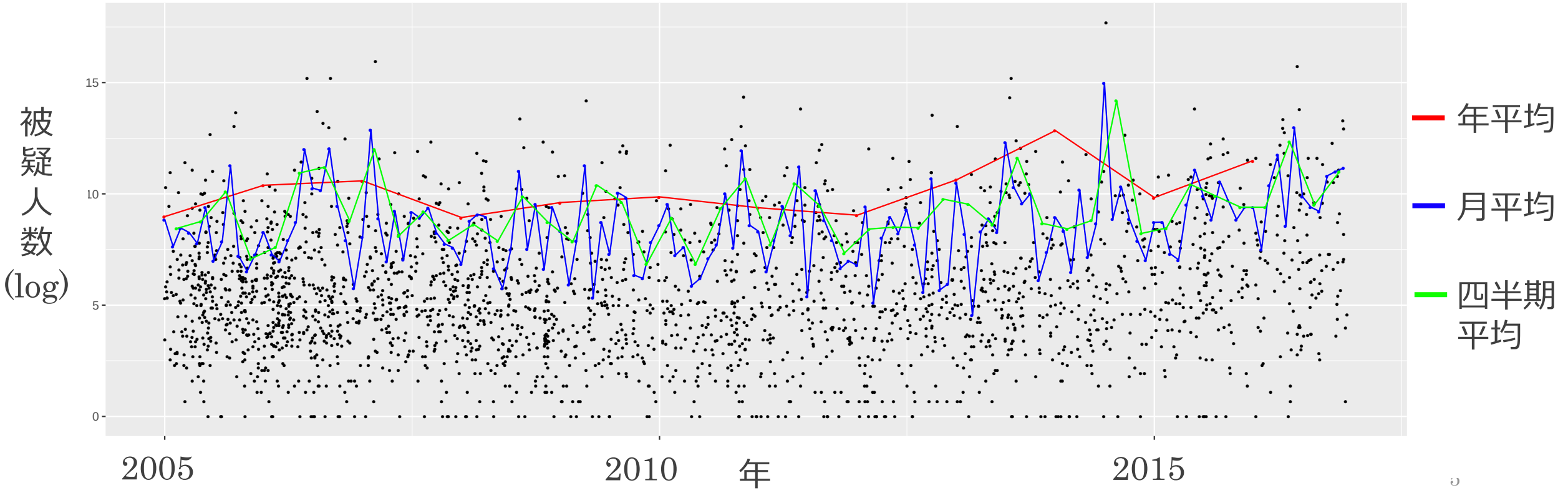
	本研究	山田[1]	Edword[2]
目的	**組織毎のリスク評価**	**マネジメント効果の定量化**	**インシデント傾向の調査**
手法	負の二項分布	ロジスティック回帰	ベイズ一般化線モデル
インシデントデータ	JNSA(2005-2018)	JNSA(2012-2016) Security Next	CSR(2005-2015)
分析対象	**日本の391組織**	**日本の17業種の企業 企業規模別**	**全米の全企業**

組織ごとのリスク評価できていなかった

[1] 山田道洋，池上和輝，菊池浩明，乾考治，経営マネジメント状況による情報漏洩インシデント削減効果の評価(2)，Computer Security Symposium 2018, pp.376-384, 2018.
[2] B.~Edwards, S.~Hofmeyr, and S.~Forrest, Hype and heavy tails: A closer look at data breaches, Journal of Cybersecurity, 2(1):3--14, 2016.

問題点

- 業種や企業規模が同じ集合を分析しており、
  特定の組織のリスクを定量化できていない



Research Question

A) ある組織が一年以内にインシデントを起こす確率は？

B) ある組織が次にインシデントを起こすまでの日数は？

C) あるマネジメントがインシデント発生間隔に与える影響は？

Research Question

A) ある組織が一年以内にインシデントを起こす確率は？
- 神奈川県は82%
- 平均で11%

B) ある組織が次にインシデントを起こすまでの日数は？
- 神奈川県は234日後
- 平均で426日後

C) あるマネジメントがインシデント発生間隔に与える影響は？
- ISMS認証取得により発生間隔が1.04倍になる
- 外部監査の設置により発生間隔が0.9倍になる

研究アプローチ

■データセット取得

A インシデント データセット
- JNSA

×

B マネジメント状況 データセット
- 東洋経済CSR

■リスク評価, マネジメント評価
- インシデント発生間隔を確率分布によるモデル化
- 発生間隔を一般化線形モデルでモデル化

インシデントデータ

- JNSAインシデントデータセット(2005-2018)
  - 日本ネットワークセキュリティ協会（JNSA）の セキュリティ被害調査ワーキンググループ
  - 新聞やインターネットなどで報道されたインシデントの記事，組織からリリースされた文書の情報

- 13年間でインシデントを4件以上起こした391組織3,789インシデント使用

東洋経済CSRデータ

- 株式会社東洋経済新報社は，上場,主要未上場企業1400社に800項目の調査票を送付
- 2017年調査、1574社、19マネジメント使用

雇用編		CSR全般		環境	
Q1	従業員数、年齢、勤続年、給与	Q1	CSR全般を統括する部署	Q1	環境対策を統括する部署
Q2	離職者	Q2	CSR担当役員	Q2	環境担当役員
Q3	従業員の世代分布	Q3	CSR活動の基本的方針姿勢	Q3	環境報告書
Q4	30歳賃金	Q4	IR、消費者対応等の各専任部署	Q4	環境会計
Q5	残業時間、手当て	Q5	社会貢献活動支出、政治献金等	Q5	環境会計の主要なコスト
Q6	役職登用状況	Q6	各種制度	Q6	環境監査
Q7	多様な人材の能力活用	Q7	NPO、NGOとの連携	Q7	環境マネジメントシステム
Q8	障害者雇用	Q8	ESGの情報開示、ファンド等組入	Q8	ISO14001認証取得事業割合
Q9	有給休暇	Q9	CSR関連行動基準への参加状況等	Q9	CO2排出量の削減中期計画
Q10	労働安全衛生の取り組み	Q10	CSR調達	Q10	環境対策
Q11	入社3年後在籍状況	Q11	内部告発	Q11-13	グリーン購入
Q12-13	社内制度	Q12	対応マニュアル	Q14	環境ラベリングの取り組み
Q14	産休、育休、介護休業等	Q13	ISO9000S	Q15	環境リスクマネジメント
Q15	両立支援	Q14	内部統制	Q16	環境関連法令の有無
Q16-17	採用	Q15	リスクマネジメント	Q17	表彰事例
Q18	人権・労働問題	Q16	企業倫理方針と倫理行動規定・規範マニュアル	Q18	気候変動や生物多様性など環境への影響

分析手法1：リスクの定量化

Research Question

A) ある組織が一年以内にインシデントを起こす確率は？

B) ある組織が次にインシデントを起こすまでの日数は？

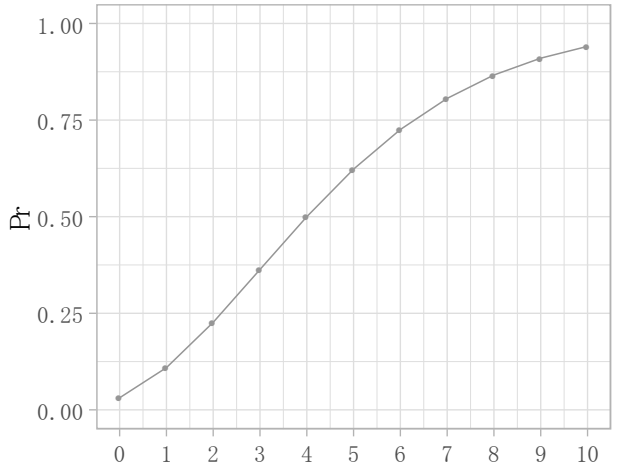
C) あるマネジメントがインシデント発生間隔に与える影響は？

分析手法1-1：確率分布へ当てはめ

- インシデント発生間隔を確率分布でモデル化
  - 発生間隔データから各確率分布（**正規分布**，**ポアソン分布**，**負の二項分布**）のパラメータを最尤推定
  - 累積確率分布を求める

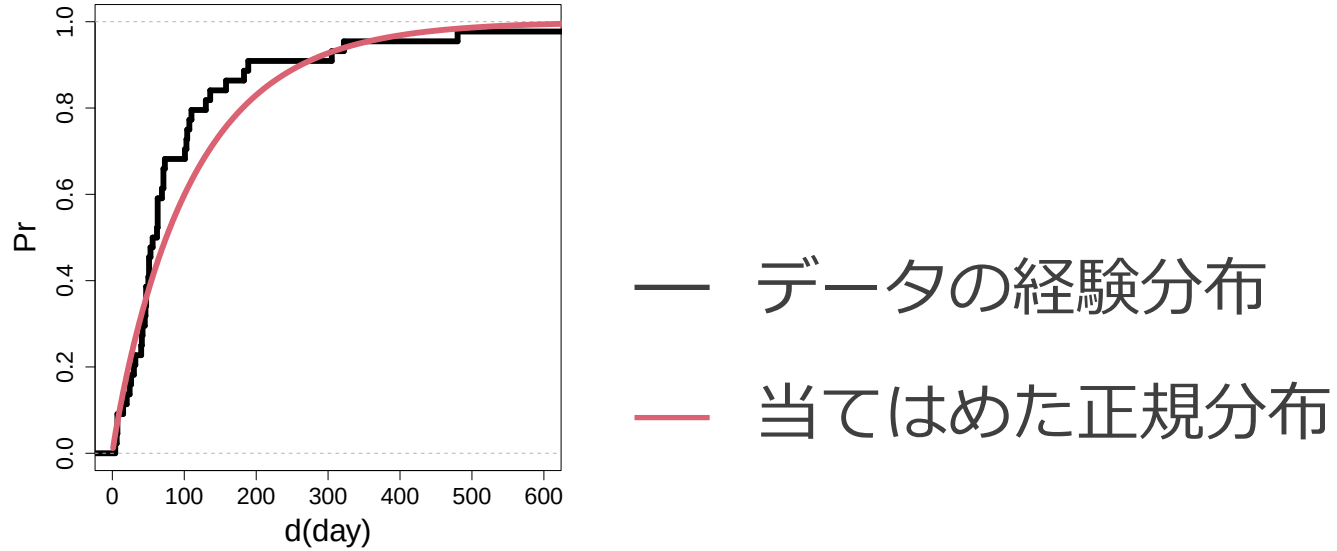
例）神奈川県

累積確率分布



分析手法1-2 ：KS検定(Kolmogorov-Smirnov)

- 目的：異なる確率分布が同一かどうか検定するもの
- 帰無仮説(例：正規分布)
  - H_0「標本の分布が、正規分布に従う」
- 対立仮説
  - H_1「標本の分布が、正規分布に従わない」

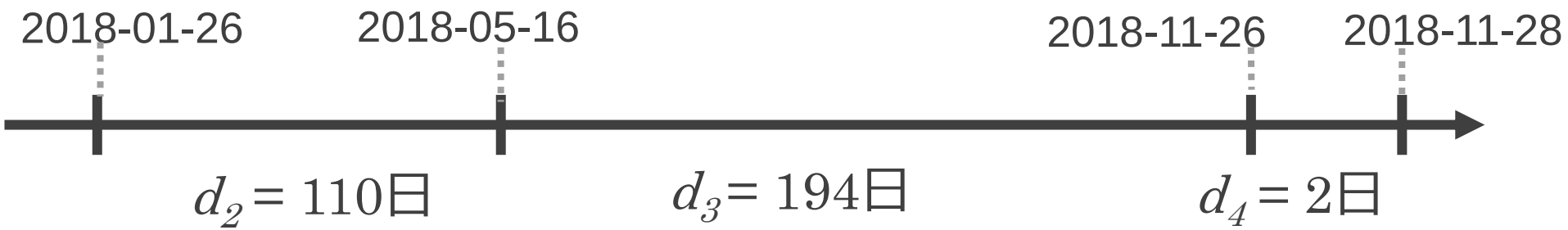


— データの経験分布

— 当てはめた正規分布

モデル作成手順

1. JNSAデータセットから到着間隔d_i取得
   - インシデントは最低でも4件以上必要



1. 確率分布のパラメータを最尤推定により求める

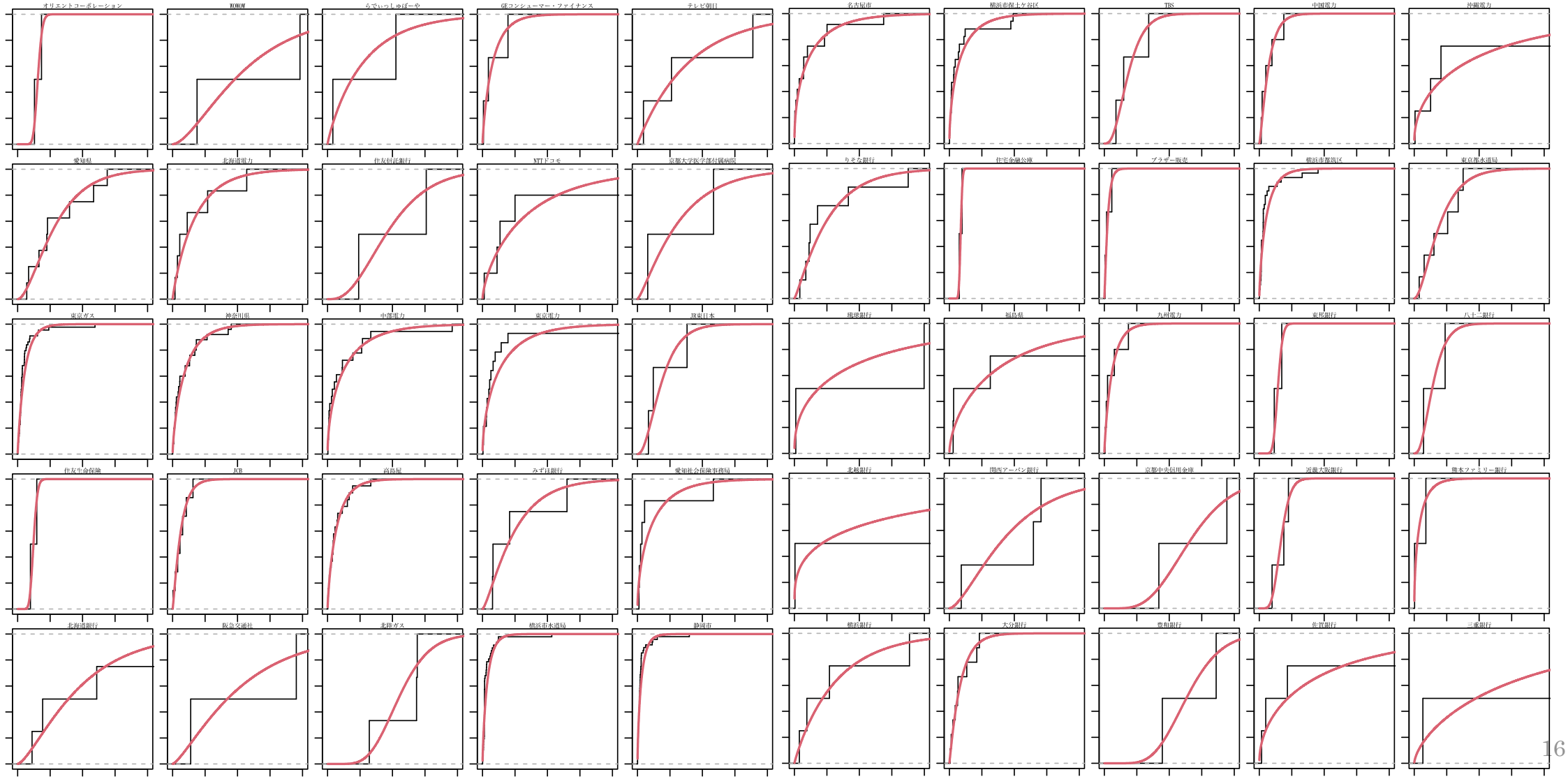
2. KS検定によりモデルの確からしさを確認

確率分布候補

- 対象とするデータの特徴(インシデント到着間隔)
  - 0以上、離散値

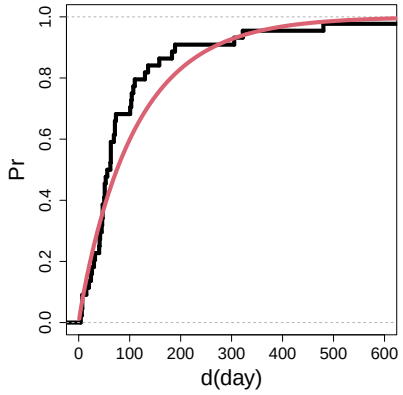
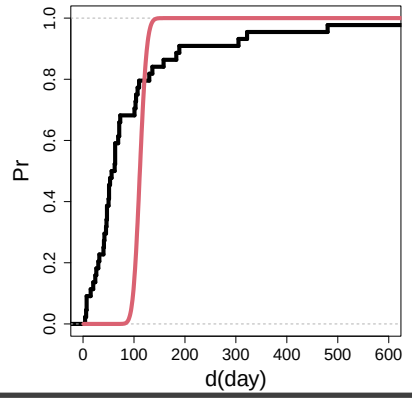
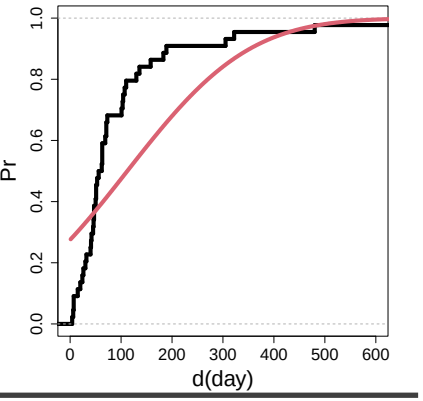
	負の二項分布	ポアソン分布	正規分布
確率変数	離散値	離散値	連続値
値の範囲	$[0, +\infty]$	$[0, +\infty]$	$[-\infty, +\infty]$
平均と分散の関係	平均<分散	平均=分散	無関係
確率密度関数	$\binom{x+r-1}{x} p^r (1-p)^x$	$\frac{\lambda^x e^{-\lambda}}{x!}$	$\frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)$
パラメータ	成功回数：r, 成功確率： p	平均：λ	平均：μ, 分散：σ

391組織への当てはめ結果（一部）



分析結果：確率分布への当てはめ・KS検定

- 391組織を各確率分布に当てはめ
  - **例)東京ガス**

	負の二項分布	ポアソン分布	正規分布
当てはめ			
検定結果	P-value=0.09	P-value=0.00	P-value=0.00

- 5%水準で帰無仮説を否定された組織数の割合

負の二項分布	ポアソン分布	正規分布
0.02(9/391)	0.39(155/391)	0.08(31/391)

研究アプローチ

■データセット取得

A インシデント データセット
- JNSA

×

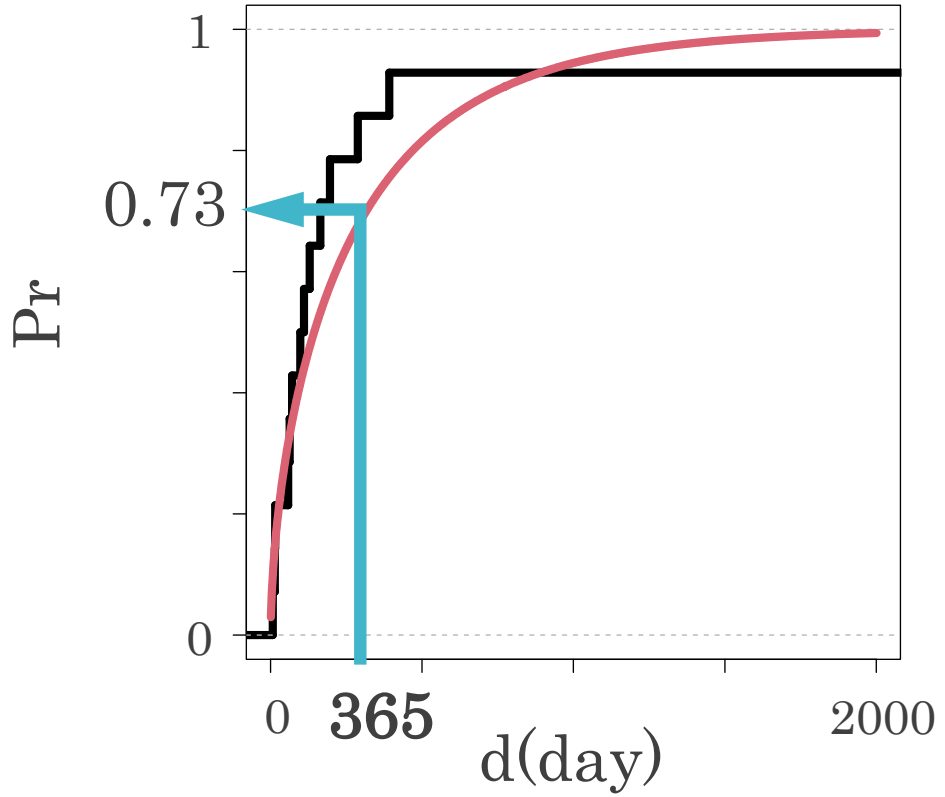
B マネジメント状況 データセット
- 東洋経済CSR

■リスク評価, マネジメント評価
- インシデント発生間隔を確率分布によるモデル化
- 発生間隔を一般化線形モデルでモデル化

RQ： 1年以内のインシデント発生確率

A) ある組織が1年内にインシデントを起こす確率は？

- **1年以内**のインシデント発生確率$\Pr[D \leq 365]$
  - 例）東京電力
  - **1年以内**の発生確率73%
  - パラメータ：$\mu = 284,\ r = 0.56$



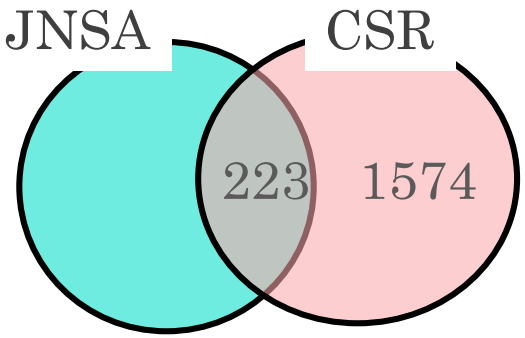
1年以内のインシデント発生確率の平均

■全組織の平均算出方法

組織数	発生確率
391	各Pr[$D \leq 365$]
1955	0

インシデント無の組織数を近似

$1955 = 391 * 6\ (1351/223)$



■一年後のインシデント発生確率統計量(n=2,346)

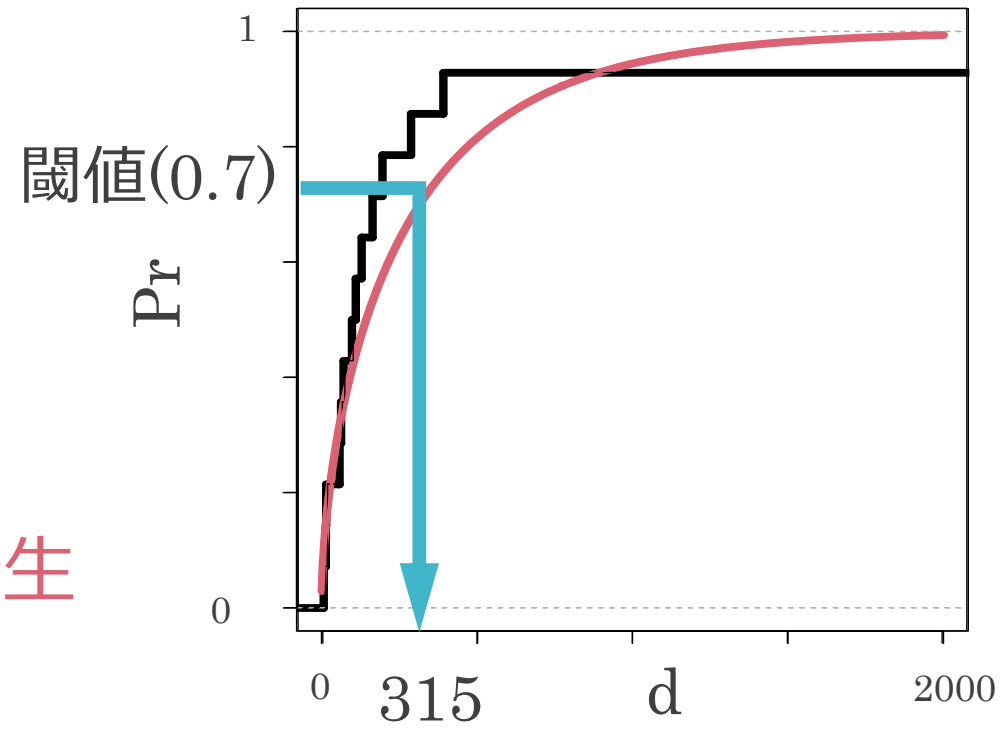
平均	最大	最小	分散
0.11	1	0	0.08

RQ：インシデント発生間隔の予測

B) 次にインシデントが発生するのは何日後か？

- $\Pr[D \leq 365] = 0.7$を閾値としてインシデント発生の予測
- 予測インシデント到着間隔$\hat{d}$
- $\hat{d} = 315$

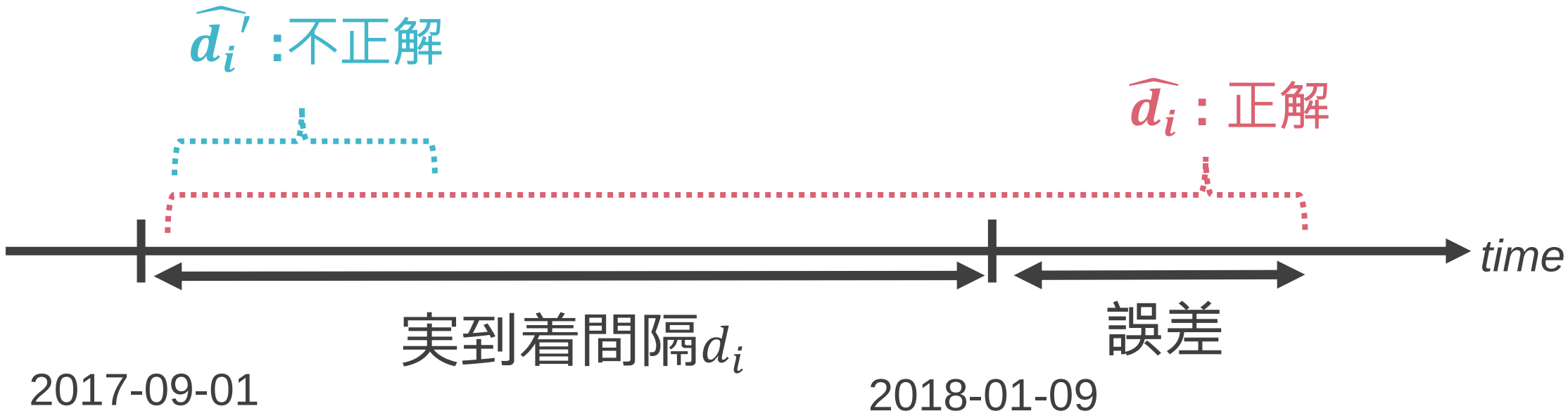
例）東京電力



315日以内に次のインシデント発生

予測の判定方法

- 予測の判定



各組織の予測結果

B) 次にインシデントが発生するのは何日後か？(n=391)

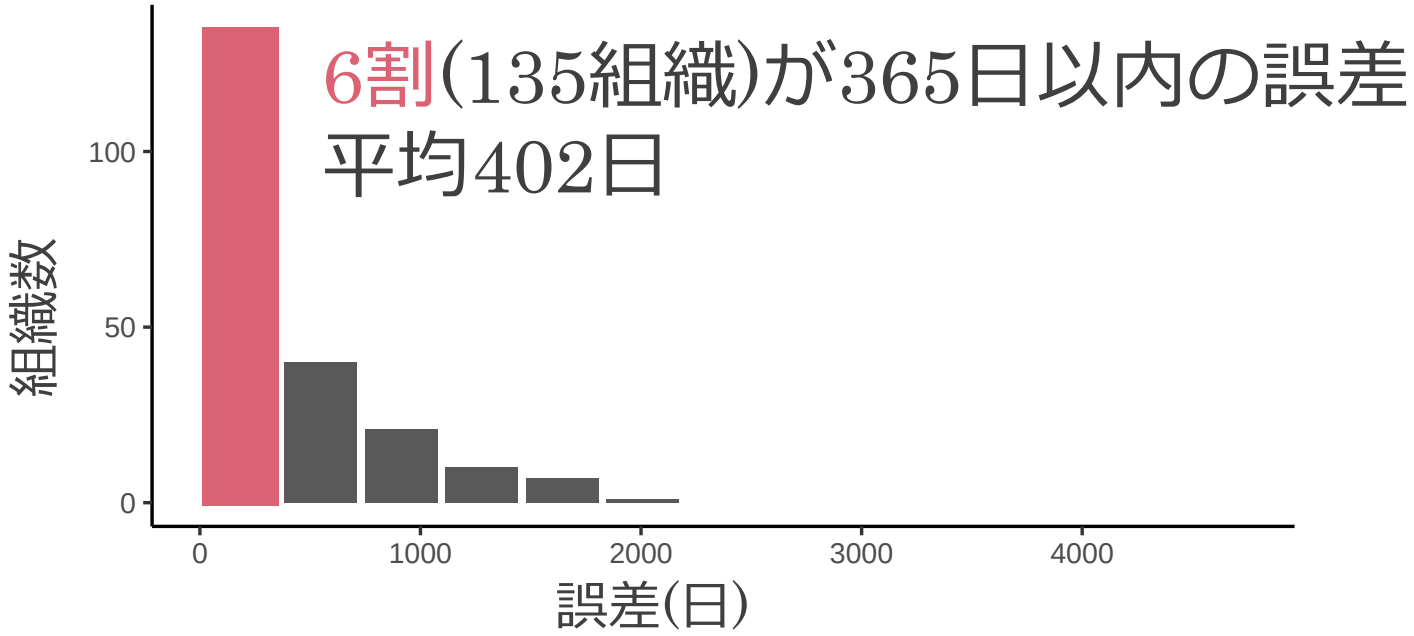
組織名	実到着間隔(日)	予測(日)	判定
神奈川県	2	234	正解
東京ガス	150	133	不正解
NTT西日本	72	138	正解
ゆうちょ銀行	45	96	正解
平均	643	496	

予測精度・誤差

- 予測結果・誤差(n=391)

正解率	予測到着間隔(日)
0.55(214/391)	426

- 正解した予測の**誤差分布**



分析手法2

A) ある組織が一年後にインシデントを起こす確率は？

B) ある組織が次にインシデントを起こすまでの日数は？

C) マネジメントがインシデント発生間隔に与える影響は？

分析手法2：一般化線形モデル

- 組織iがマネジメントmを実施した時のインシデント到着間隔μ_i
  - $\mu_i = e^{\alpha+\beta_1 x_1+\beta_2 x_2+\beta_3 x_3+\cdots+\beta_{x_{19}} x_{19}}$
    - x_1：業種，x_2：企業規模，x_m：マネジメントmを実施しているか

- マネジメントx_lによる効果
  - 発生間隔比 $= \dfrac{\mu_l^+}{\mu_l^-} = \dfrac{e^{\alpha+\beta_1 x_1+\beta_2 x_2+\beta_3 x_3+\cdots+\beta_l x_l}}{e^{\alpha+\beta_1 x_1+\beta_2 x_2+\beta_3 x_3+\cdots+\beta_{l-1} x_{l-1}}}$

$$= e^{\beta_l}$$

分析結果2：発生間隔に与えるマネジメント効果

C)マネジメント効果は？

ISMSにより発生間隔1.04倍
外部監査により発生間隔0.93倍

17中9マネジメントに
発生間隔を伸ばす効果がある

	Estimate	発生間隔比	Pr(>|t|)	
ISMS	0.04	1.04	0.18	
CIO	−0.07	0.93	0.01	**
CFO	0.01	1.01	0.64	
外部窓口	0.01	1.01	0.70	
内部窓口	−0.07	0.93	0.14	
告発保護	0.06	1.06	0.24	
内統委員	−0.01	0.99	0.65	
PP	0.00	1.00	0.98	
SP	−0.01	0.99	0.79	
内部監査	0.01	1.01	0.75	
外部監査	−0.07	0.93	0.00	**
独立監査	0.02	1.02	0.61	
RM_CM	0.03	1.03	0.42	
RM_CMP	−0.08	0.92	0.03	*
環境監査	−0.03	0.97	0.33	
環境M	0.10	1.10	0.01	**
労働M	0.00	1.00	0.98	

分析結果2：業種による影響

銀行は発生間隔が0.35倍
電気・ガス業界は0.11倍

	Estimate	発生間隔比	Pr(>|t|)	
(Intercept)	8.96		< 2e-16	***
医薬品	−0.14	0.87	0.26	
運輸・物流	−0.07	0.93	0.55	
機械	−0.04	0.96	0.72	
金融(除く銀行)	−0.31	0.73	0.01	*
銀行	−1.06	0.35	0.00	***
建設・資材	−0.37	0.69	0.00	**
自動車・輸送機	0.00	1.00	0.98	
商社・卸売	−0.12	0.89	0.31	
小売	−0.30	0.74	0.01	*
情報通信・サービスその他	−0.18	0.83	0.12	
食品	−0.02	0.98	0.87	
素材・化学	−0.05	0.95	0.66	
鉄鋼・非鉄	−0.03	0.97	0.84	
電機・精密	−0.08	0.92	0.49	
電気・ガス	−2.24	0.11	0.00	***
不動産	−0.46	0.63	0.00	***
LOG(従業員数)	−0.07	0.94	< 2e-16	***

まとめ・今後の課題

- 391組織のインシデント発生間隔を確率分布に当てはめた
  - 負の二項分布の当てはまりが最も良かった

- ３つのRQを明らかにした
  - A) ある組織が一年以内にインシデントを起こす確率は？
    - 神奈川県は82%,、東京電力は73%
  - B) ある組織が次にインシデントを起こすまでの日数は？
    - 神奈川県は234日、東京電力は315日
  - C) マネジメントによる効果は？
    - ISMS認証取得により到着間隔が1.04倍になる

- 今後は、モデルの精度改善とインシデントの漏洩原因、被害規模を考慮にいれたモデルに発展させたい

質疑応答用

サイバーセキュリティ経営ガイドライン

- 目的
  - 経営者指揮のもとで、サイバーセキュリティ対策を推進するため
  - 2018.11.16にVer2公開
- 対象
  - ITを活用する、大企及び中小企業
  - 経営者、情報セキュリティ対策の責任者
- 内容
  - 経営者が認識すべき3原則
  - 経営者が、CISO等にだすべき指示である重要10項目
    - リスク管理構築、インシデントに備えた体制構築、他

経済産業省HP https://www.meti.go.jp/policy/netsecurity/mng_guide.html
ガイドVer2 https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf

負の二項分布

- **パラメータ**　成功確率p，成功回数r
- **確率変数**　r回成功するまでの失敗回数
- **確率密度関数**　$f(x) = P(X = x) = \binom{x+r-1}{x} p^r (1-p)^x$
- **実数値に拡張**　$f(x) = P(X = x) = \frac{\Gamma(x+r)}{\Gamma(x+1)\Gamma(r)} p^r (1-p)^x$

※ガンマ関数　$\Gamma(x+1) = x!$

- 成功回数rが正の実数値を取るため物理的な意味は与えられないが、確率密度関数により、対象の分布を正式に定義できる

Wikipedia https://en.wikipedia.org/wiki/Negative_binomial_distribution

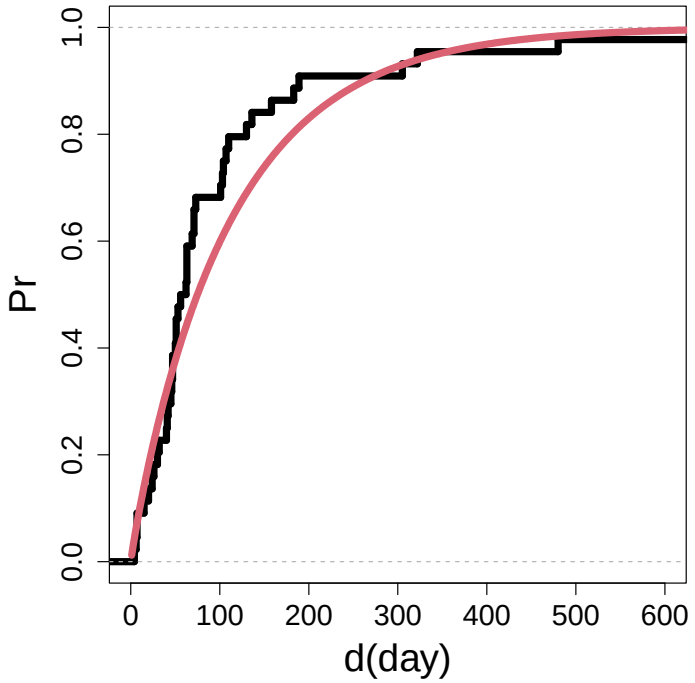
予測結果・誤差

	正解率	予測到着間隔
全体(n=391)	**0.55**(214/391)	426

正解したインシデント到着間隔の**誤差分布**

1年以内	1-2年	2-3年	3-4年	4-5年	6年以上
0.63 (135/214)	0.18 (40/214)	0.09 (21/214)	0.04 (10/214)	0.03 (7/214)	0.004 (1/214)

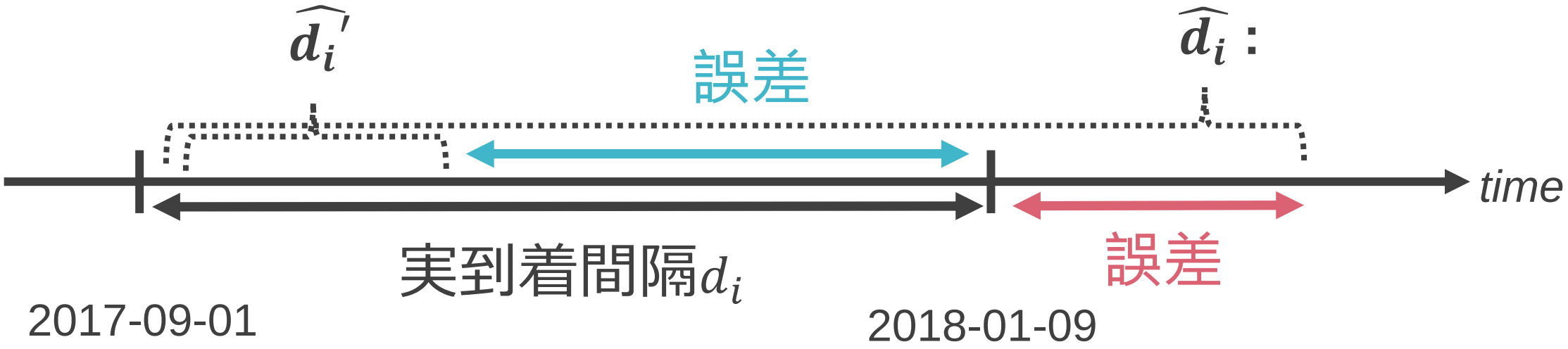
経験分布関数



経験分布関数 F_m は

$$F_m(D) = \begin{cases} 0 & D < d_1 \\ \dfrac{i}{m} & d_{(i)} \le D < d_{(i+1)}, \quad i = 1, \ldots, m-1 \\ 1 & D \ge d_{(m)} \end{cases}$$

誤差のよる予測判定



	183日	365日	730日
正解率	0.34(135/391)	0.52(204/391)	0.73(287/391)

マネジメント効果の考察

先行研究

- 山田[1]
  - 目的：インシデントとマネジメント方策の関係を明らかにすること
  - 結論：ISMSによりインシデント発生確率20%削減

- Edword[2]
  - 目的：全米のインシデント発生傾向を明らかにすること
  - 結論：10年間でインシデント発生に頻度・被害規模が変化していない

[1] 山田道洋，池上和輝，菊池浩明，乾考治，経営マネジメント状況による情報漏洩インシデント削減効果の評価(2)，Computer Security Symposium 2018, pp.376-384, 2018.
[2] B.~Edwards, S.~Hofmeyr, and S.~Forrest, Hype and heavy tails: A closer look at data breaches, Journal of Cybersecurity, 2(1):3--14, 2016.

セキュリティマネジメント例

- ISMS(情報セキュリティマネジメントシステム)
  - 自身のリスク評価によるセキュリティレベルの決定、プラン作り、企業資源の配分によってシステムを運営すること
- 情報セキュリティシステムに関する外部監査
- CIO(情報最高責任者)など

https://isms.jp/isms/

インシデント事例

- 神奈川県が利用したHDD廃棄依頼
  ブロードリンクの社員がヤフオクに18個が転売
- ヤフオク購入者の調べで発覚
- 神奈川県の行政文章等が流出の可能性
- 神奈川県（総務局　ＩＣＴ推進部）
  ブロードリンクは**ISMS認証を取得済み**

県庁HDD転売18個

税滞納など流出 9個未回収

神奈川県発表

窃盗容疑で社

- どのマネジメントに効果があるのか不明確
- インシデント発生リスクも不明確