取引件数の時間分布の相関を用いたBitcoin取引所のユーザのタイムゾーン推定

草野蘭之介＊　山崎孝順＊　井垣秀星＊　松本寛輝*＊　菊池浩明＊

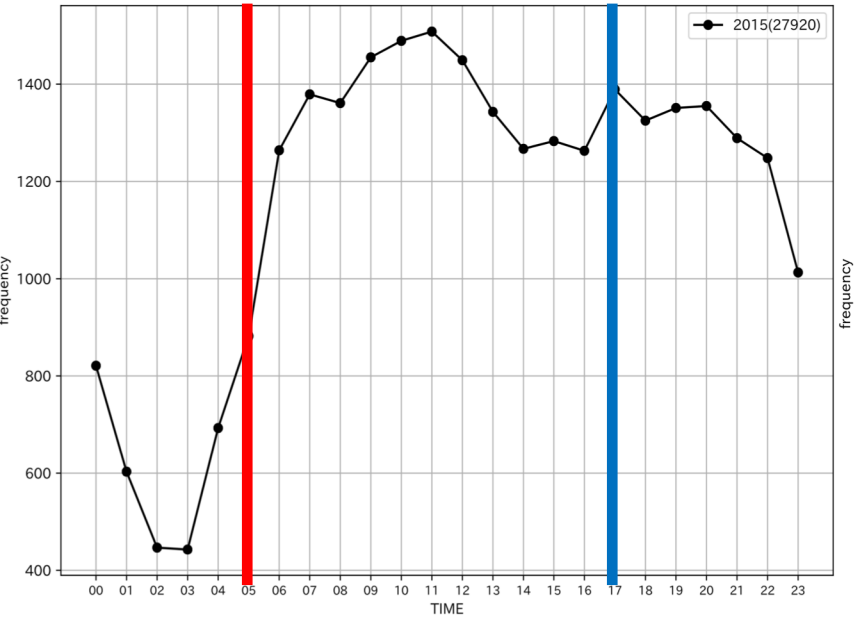
明治大学総合数理学部＊　明治大学大学院先端数理科学研究科*＊

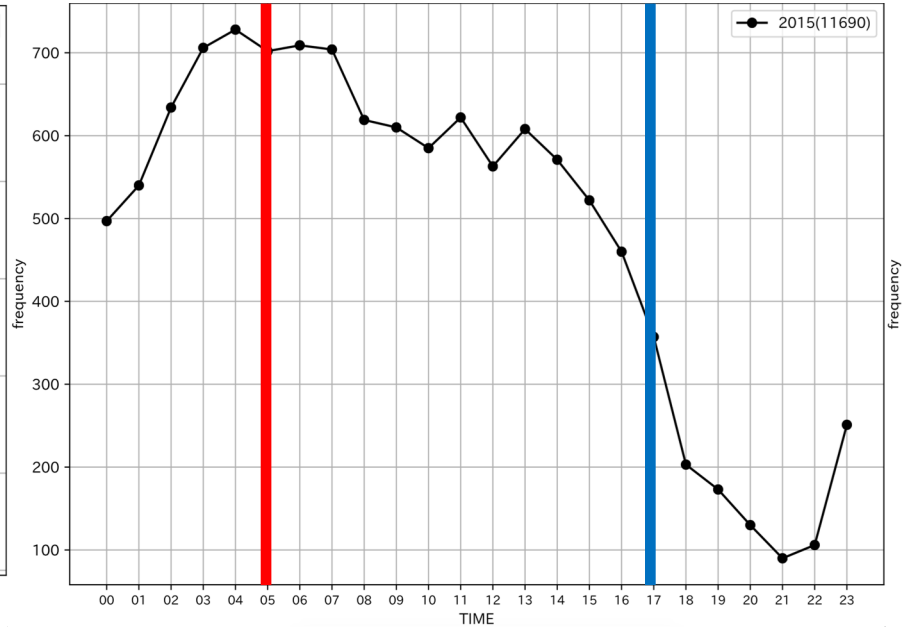
どの分布がタイの取引所でしょう？？

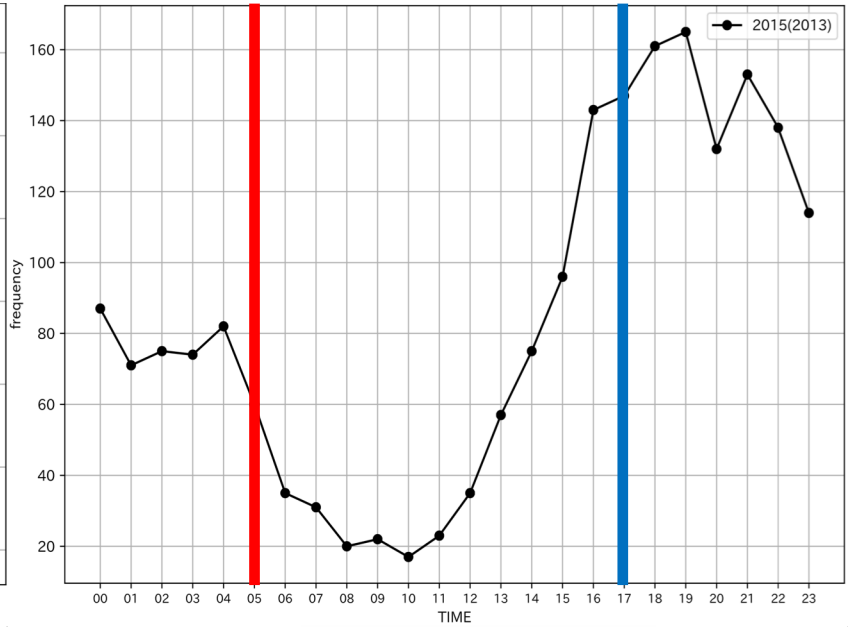
UTC+1

UTC+7

UTC -5







TST12

TST 0

Bitcoin.de

BX.in.th

CoinCafe

研究目的

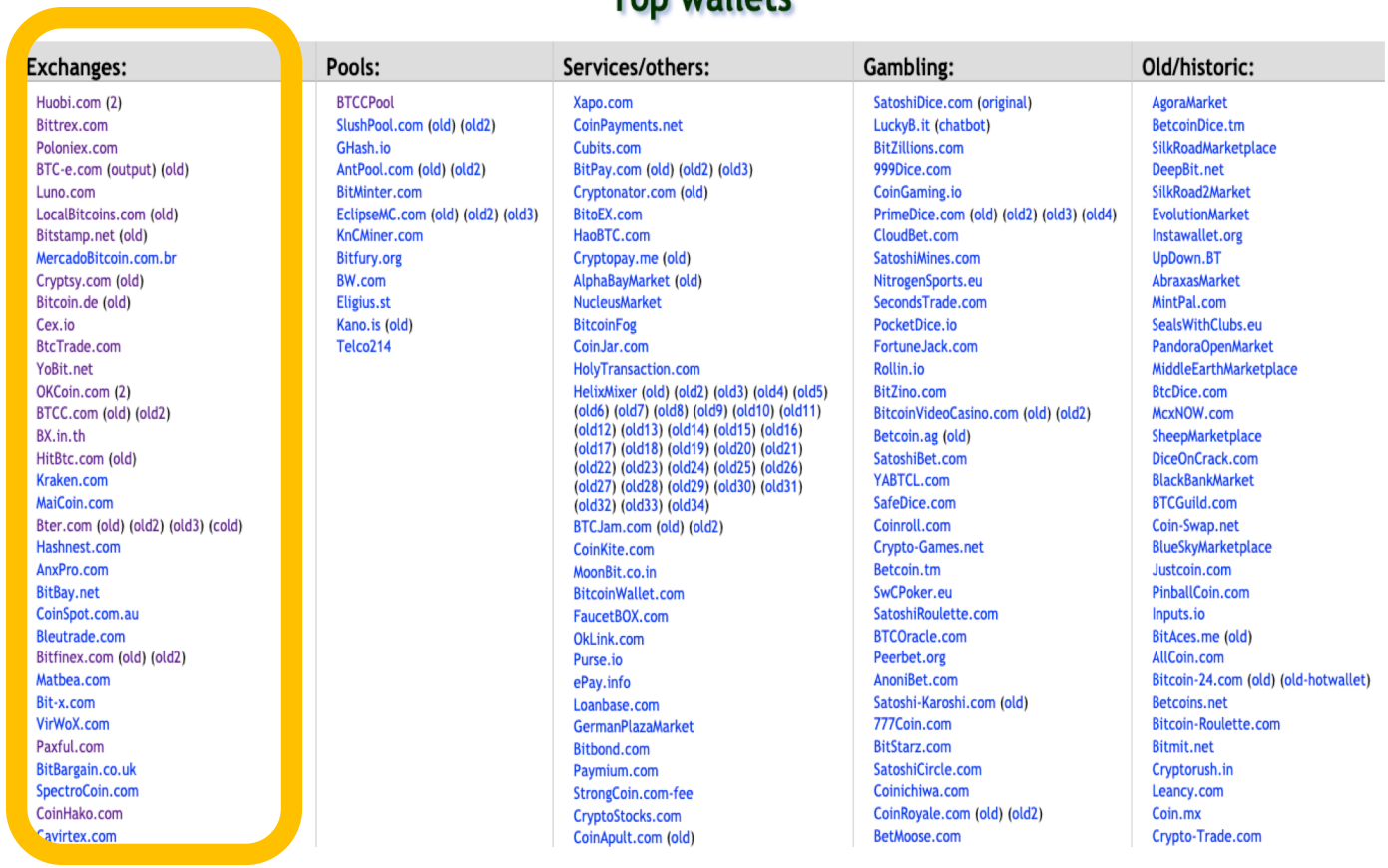
・暗号資産取引所(exchange)ユーザのタイムゾーンを明らかにする

～調査対象～

世界32カ国

８０取引所

抽出



Top wallets

Exchanges:	Pools:	Services/others:	Gambling:	Old/historic:
Huobi.com (2)	BTCCPool	Xapo.com	SatoshiDice.com (original)	AgoraMarket
Bittrex.com	SlushPool.com (old) (old2)	CoinPayments.net	LuckyB.it (chatbot)	BetcoinDice.tm
Poloniex.com	GHash.io	Cubits.com	BitZillions.com	SilkRoadMarketplace
BTC-e.com (output) (old)	AntPool.com (old) (old2)	BitPay.com (old) (old2) (old3)	999Dice.com	DeepBit.net
Luno.com	BitMinter.com	Cryptonator.com (old)	CoinGaming.io	SilkRoad2Market
LocalBitcoins.com (old)	EclipseMC.com (old) (old2) (old3)	BitoEX.com	PrimeDice.com (old) (old2) (old3) (old4)	EvolutionMarket
Bitstamp.net (old)	KnCMiner.com	HaoBTC.com	CloudBet.com	Instawallet.org
MercadoBitcoin.com.br	Bitfury.org	Cryptopay.me (old)	SatoshiMines.com	UpDown.BT
Cryptsy.com (old)	BW.com	AlphaBayMarket (old)	NitrogenSports.eu	AbraxasMarket
Bitcoin.de (old)	Eligius.st	NucleusMarket	SecondsTrade.com	MintPal.com
Cex.io	Kano.is (old)	BitcoinFog	PocketDice.io	SealsWithClubs.eu
BtcTrade.com	Telco214	CoinJar.com	FortuneJack.com	PandoraOpenMarket
YoBit.net		HolyTransaction.com	Rollin.io	MiddleEarthMarketplace
OKCoin.com (2)		HelixMixer (old) (old2) (old3) (old4) (old5) (old6) (old7) (old8) (old9) (old10) (old11) (old12) (old13) (old14) (old15) (old16) (old17) (old18) (old19) (old20) (old21) (old22) (old23) (old24) (old25) (old26) (old27) (old28) (old29) (old30) (old31) (old32) (old33) (old34)	BitZino.com	BtcDice.com
BTCC.com (old) (old2)			BitcoinVideoCasino.com (old) (old2)	McxNOW.com
BX.in.th			Betcoin.ag (old)	SheepMarketplace
HitBtc.com (old)			SatoshiBet.com	DiceOnCrack.com
Kraken.com			YABTCL.com	BlackBankMarket
MaiCoin.com			SafeDice.com	BTCGuild.com
Bter.com (old) (old2) (old3) (cold)			Coinroll.com	Coin-Swap.net
Hashnest.com			Crypto-Games.net	BlueSkyMarketplace
AnxPro.com			Betcoin.tm	Justcoin.com
BitBay.net			SwCPoker.eu	PinballCoin.com
CoinSpot.com.au			SatoshiRoulette.com	Inputs.io
Bleutrade.com			BTCOracle.com	BitAces.me (old)
Bitfinex.com (old) (old2)			Peerbet.org	AllCoin.com
Matbea.com			AnoniBet.com	Bitcoin-24.com (old) (old-hotwallet)
Bit-x.com			Satoshi-Karoshi.com (old)	Betcoins.net
VirWoX.com			777Coin.com	Bitcoin-Roulette.com
Paxful.com			BitStarz.com	Bitmit.net
BitBargain.co.uk			SatoshiCircle.com	Cryptorush.in
SpectroCoin.com			Coinichiwa.com	Leancy.com
CoinHako.com			CoinRoyale.com (old) (old2)	Coin.mx
Cavirtex.com		CoinApult.com (old)	BetMoose.com	Crypto-Trade.com

walletexplore.cpm[3]

研究背景

＊取引例＊

アドレスからタイムゾーンの推定は困難である

先行研究

- Toward De-Anonymizing Bitcoin by Mapping Users Location [1]

- 平均取引時間分布の相関を用いたBitcoinユーザのタイムゾーン属性の推定 [2]

[1] J. Dupont, A. C. Squicciarini,
”Toward De-Anonymizing Bitcoin by Mapping Users Location”, In Proceedings of Conderence on Data and Application Security and Privacy(CODASPY’ 15), pp.139-141, ACM, 2015.

[2]井垣秀星, 永田倖大, 菊池浩明,
”平均取引時間分布の相関を用いたBitcoinユーザのタイムゾーン属性の推定”, 情報処理学会第 81 回全国大会, pp.3 481-3 482, 2019.

研究アプローチ

我々は，取引の時間に着目し

仮説：「ある国の取引所のユーザは

その国のタイムゾーンでの日中に取引を行う」

を立てた．

取得データ

取引データ（walletexplorer[3]）

Txid	6f57e323ef80248000637cde04c87ff1714f6eca89d41b84a26dfba0914daa07
Included in block	614656 (pos 1188)
Time	2020-01-26 17:40:38
Sender	BTC-e.com
Fee	0.00001591 BTC (0.83 satoshis/byte)
Size	1912 bytes

inputs: 12 (0.02378858 BTC) unique addresses: 12,

0. 3NouHN7q6YuBXdcvFKJCB8n2Eyyx2ZXe4w 0.00001063
1. 1QGpaFvJ9DhqsALUVLqmMsbLLbPdqRdFZW 0.00103569
2. 1CjZ2S8sAG8Jv24cH5AMBacmvw2YVNoBU8 0.01361266
3. 38jwm1csPs9BKtVM3yXXTa5CiNtuWQwgkZ 0.00001836
4. 3BnWRhsLX6fzqXukq8HGF1XExkF65cJsWC 0.00002323
5. 1FhHZGiyPDTqSx1aZHQB6mVf9X7VnCZjSP 0.00005888 BTC prev. tx
6. 12LXGakSsMDcLqoJVKAAGsiQmxLAVMFAHu 0.00896146 BTC prev. tx

tions: 12 **outputs: 1** (0.02377267 BTC)

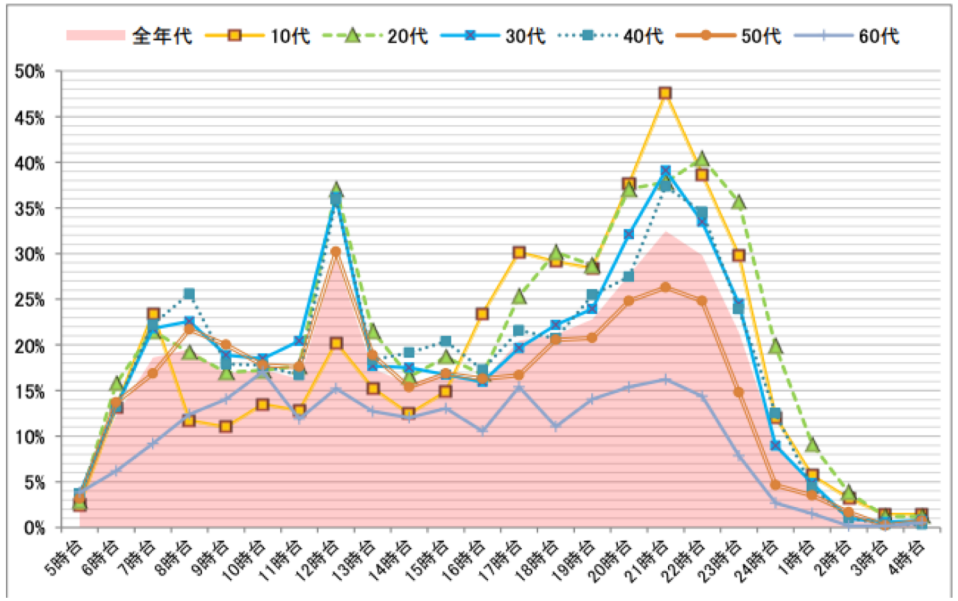
0. 38EpBrnQJwPvyBwAL5WK8bp6sPQ3PB4KLu [013baec425] 0.02377267 BTC

参照データ

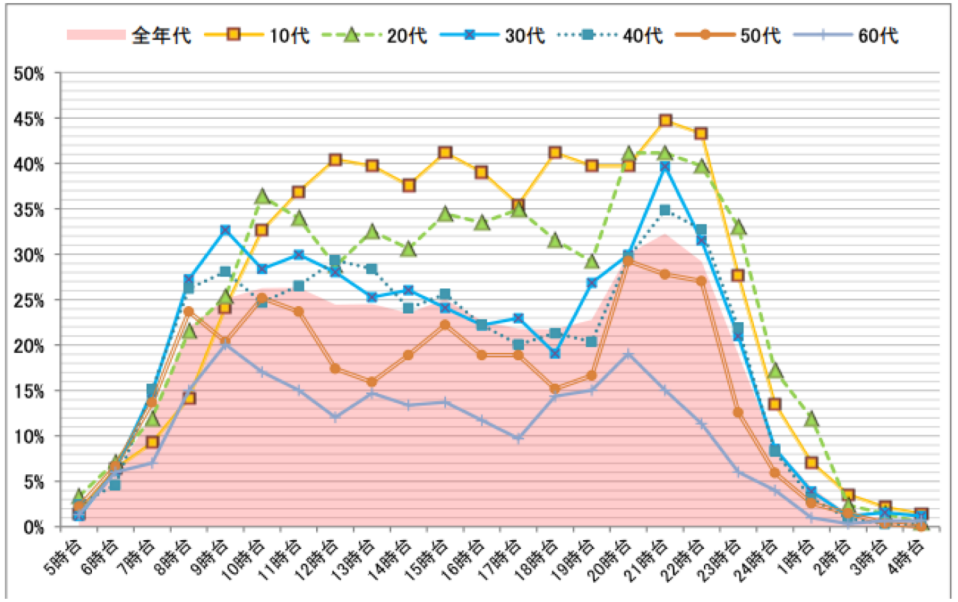
インターネット利用時間帯データ [4]

図 1-1-2-4 平成 30 年度「インターネット利用」の時間帯別行為者率（全年代・年代別）

平日

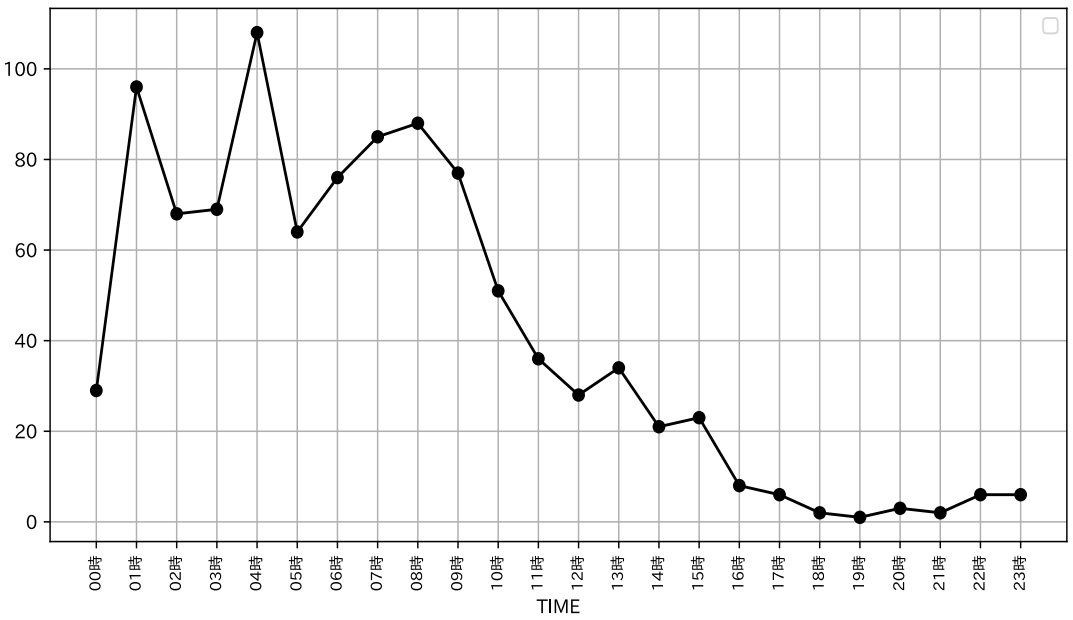


休日



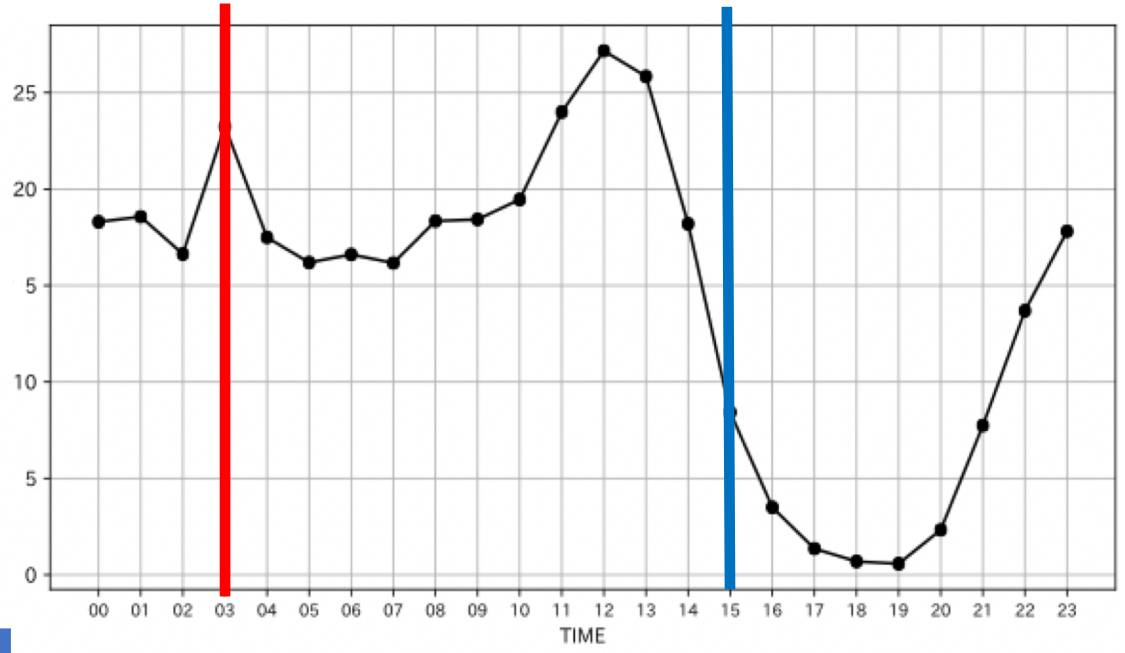
[4]総務省HP

推定方法（相関係数）



ユーザAの取引時間分布

JST 12　　JST 0



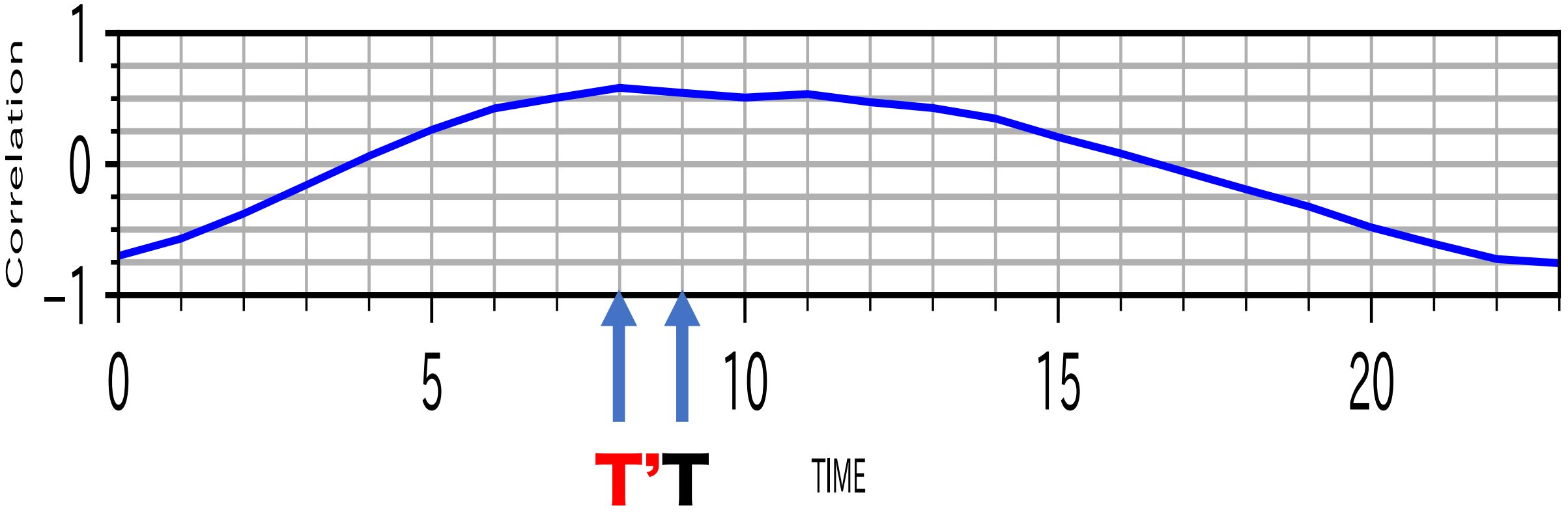
インターネット利用時間分布

ピアソンの
相関係数に
基づいて推定

ユーザAのタイムゾーンは UTC ？

推定方法例

CoinCheckとインターネットデータの相関分布



T：正解(UTC+9)　T'：推定値(UTC+8)➡相関係数最大値

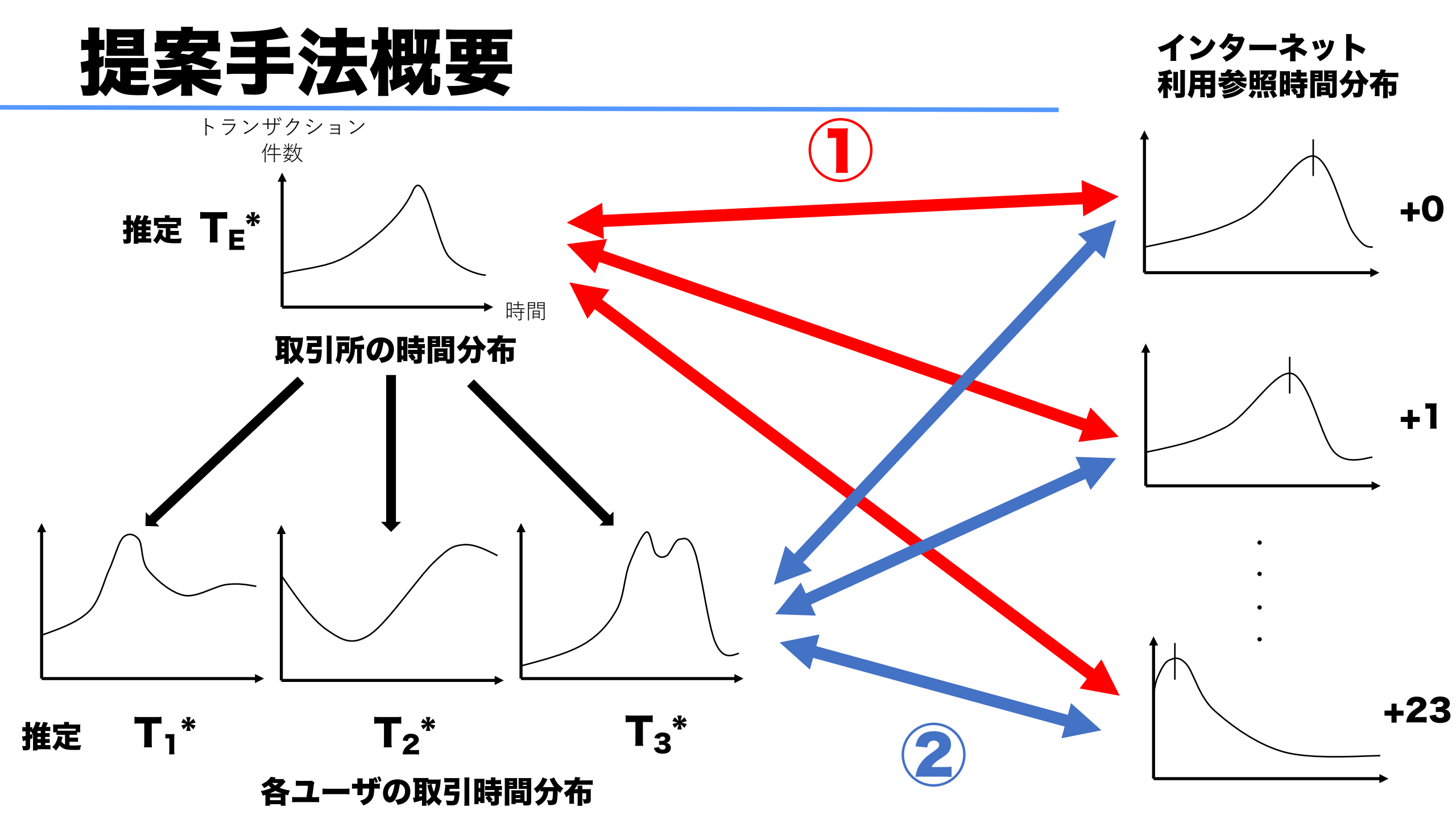
提案手法

① 各取引所の取引データとインターネット利用時間のデータの相関から取引所のタイムゾーンを推定

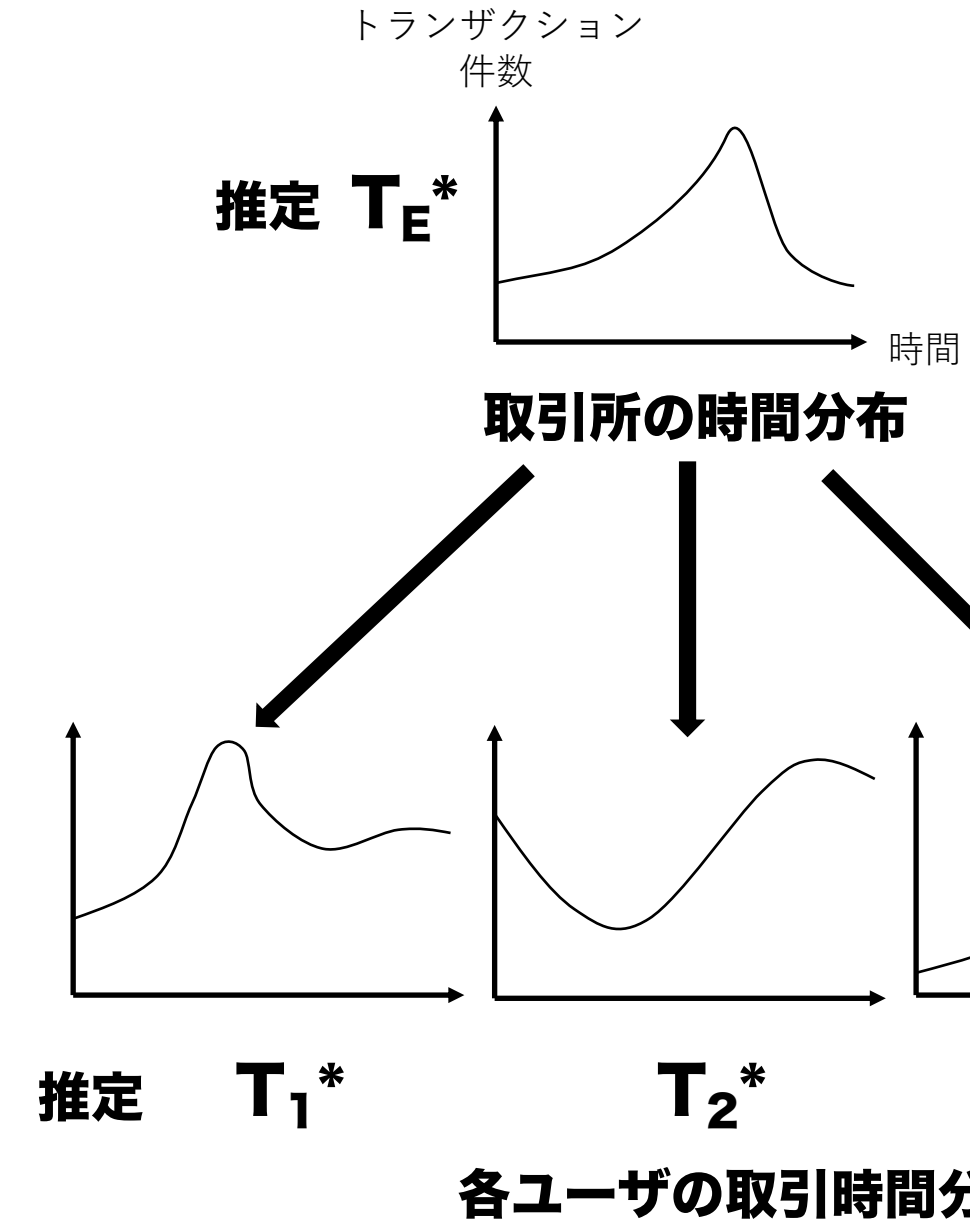
② 各取引所に属する全アドレスの取引データとインターネット利用時間データの相関から利用者のタイムゾーンを推定

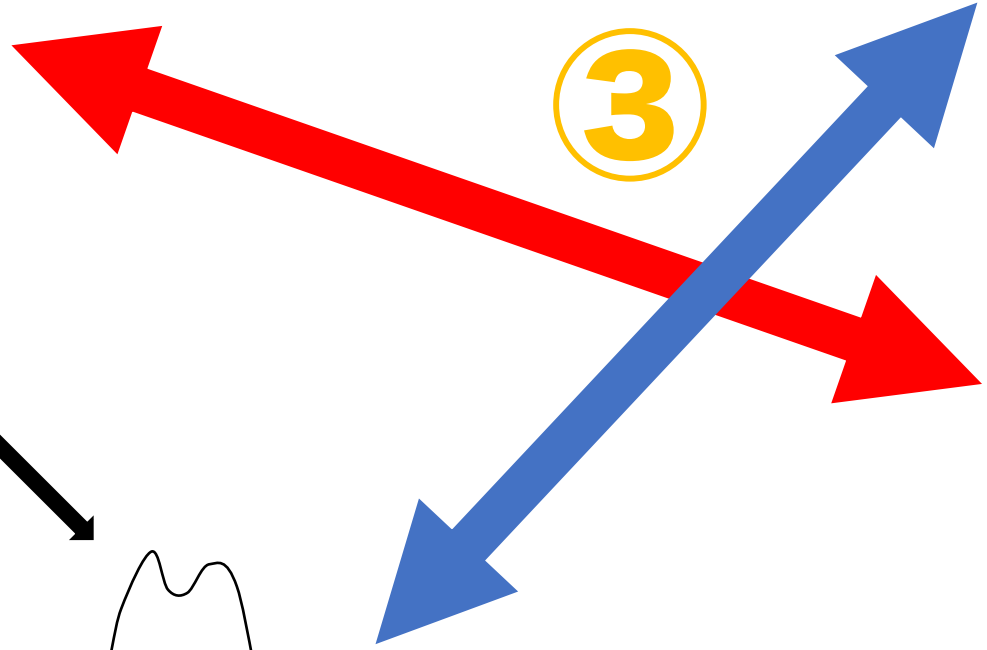
③ ①と②で求めたUTCの比較

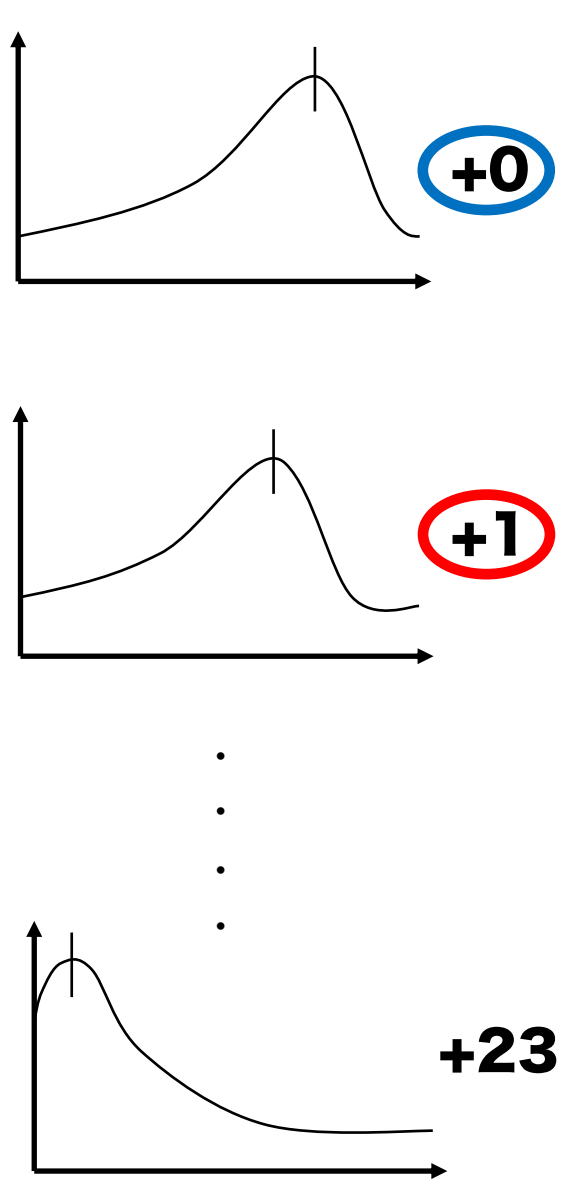
提案手法概要


トランザクション
件数
推定 T_E^*
時間
取引所の時間分布
推定 T_1^*
T_2^*
T_3^*
各ユーザの取引時間分布
①
②
インターネット
利用参照時間分布
+0
+1
+23

提案手法概要


トランザクション
件数
推定 T_E^*
時間
取引所の時間分布
推定 T_1^*
T_2^*
T_3^*
各ユーザの取引時間分布

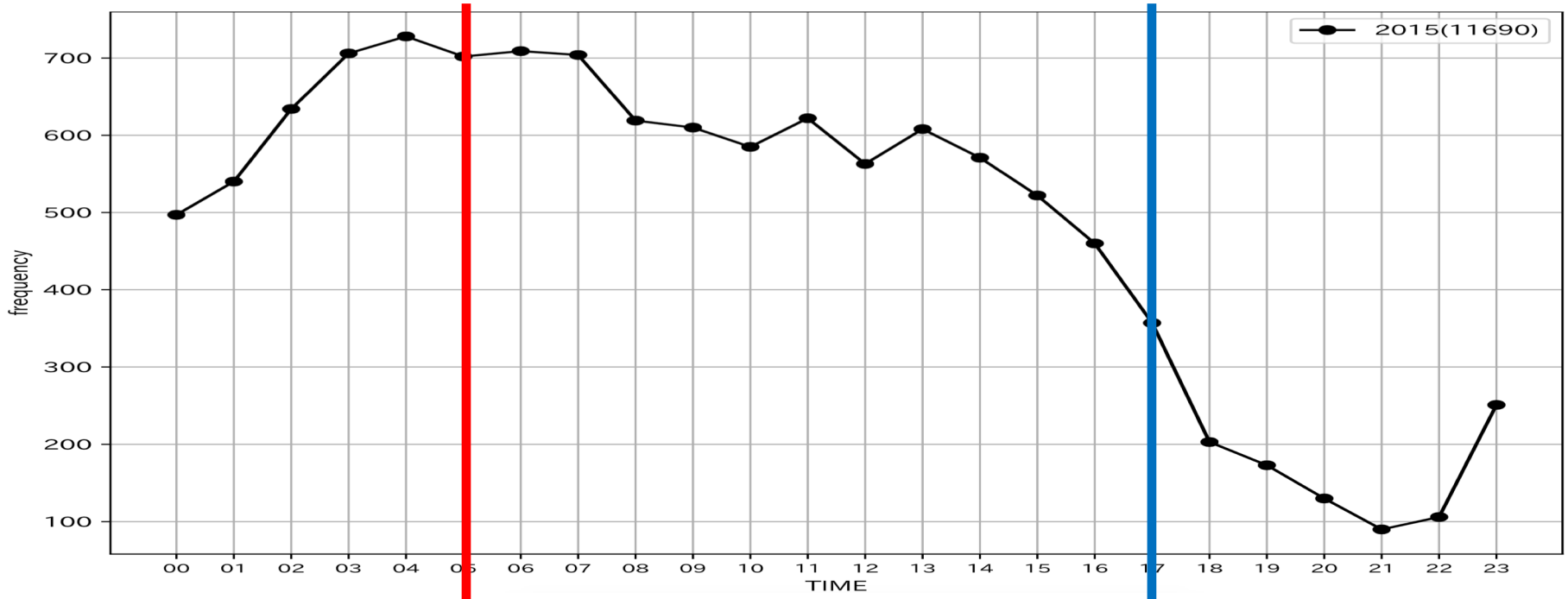

3


インターネット
利用参照時間分布
+0
+1
+23

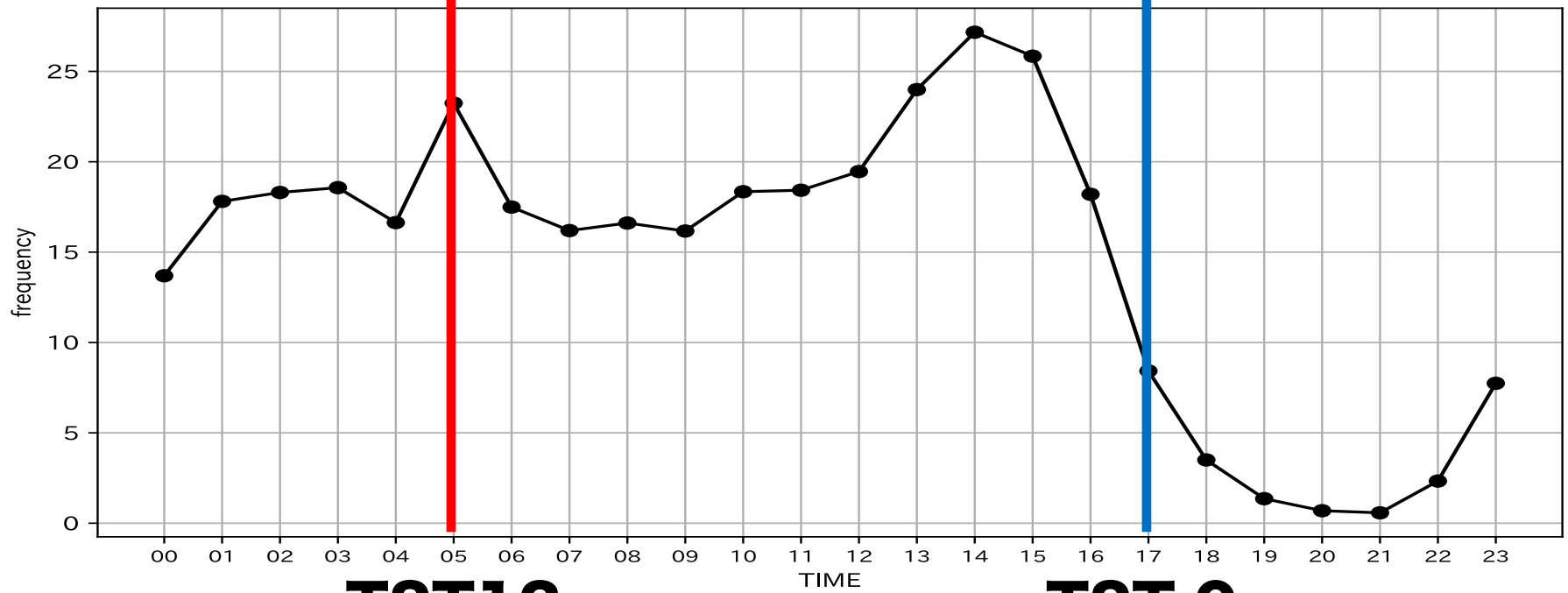
タイムゾーン推定結果 (一部)

国	取引所名	UTC(正解)	UTC(推定値)	誤差	総取引所数	総アドレス数
香港	oneCoin	+8	+7	-1	1922	876
香港	AnxPro	+8	-7	-15	326265	122166
シンガポール	CoinHako	+8	+10	+2	136698	20588
タイ	BX.in.th	+7	+7	0	323191	48571
ドイツ	Coinomat	+2	+1	-1	14688	5481
デンマーク	Ccedk	+1	0	-1	2645	1040
イギリス	Coinmate	0	0	0	43402	5297
イギリス	Exmo	0	+1	+1	90813	8430
ブラジル	FoxBit	-3	-4	-1	91641	3670
ケイマン諸島	BlockTrades	-5	-5	0	52426	27748
アメリカ	EmpoEx	-7	+1	+8	2688	741

取引時間分布



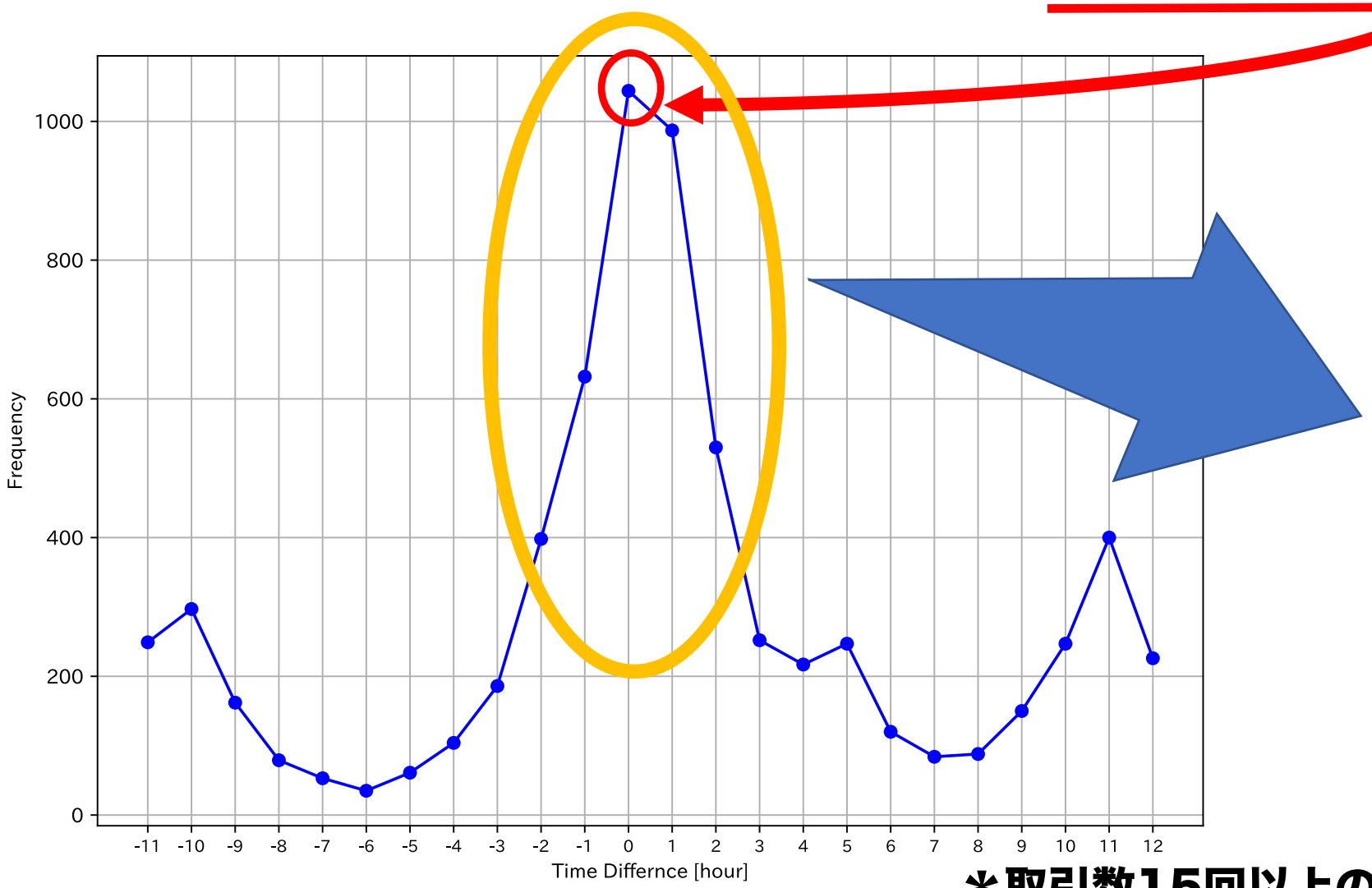
インターネット利用時間
(UTC+7)



TST12 **TST 0**

取引所BX.in.thのアドレス推定時間分布

国：タイ　推定値：UTC+7　正解：UTC+7



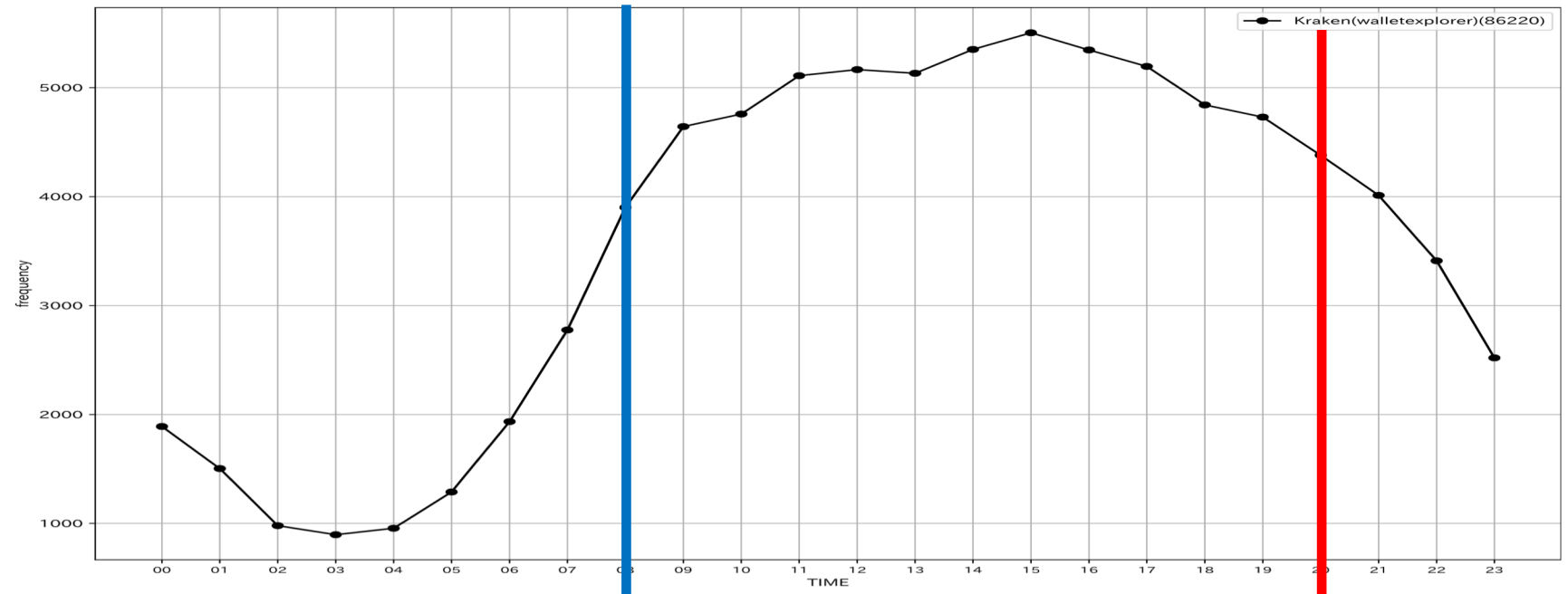
誤差0（UTC+7）：1044個

誤差-1（UTC+6）：632個

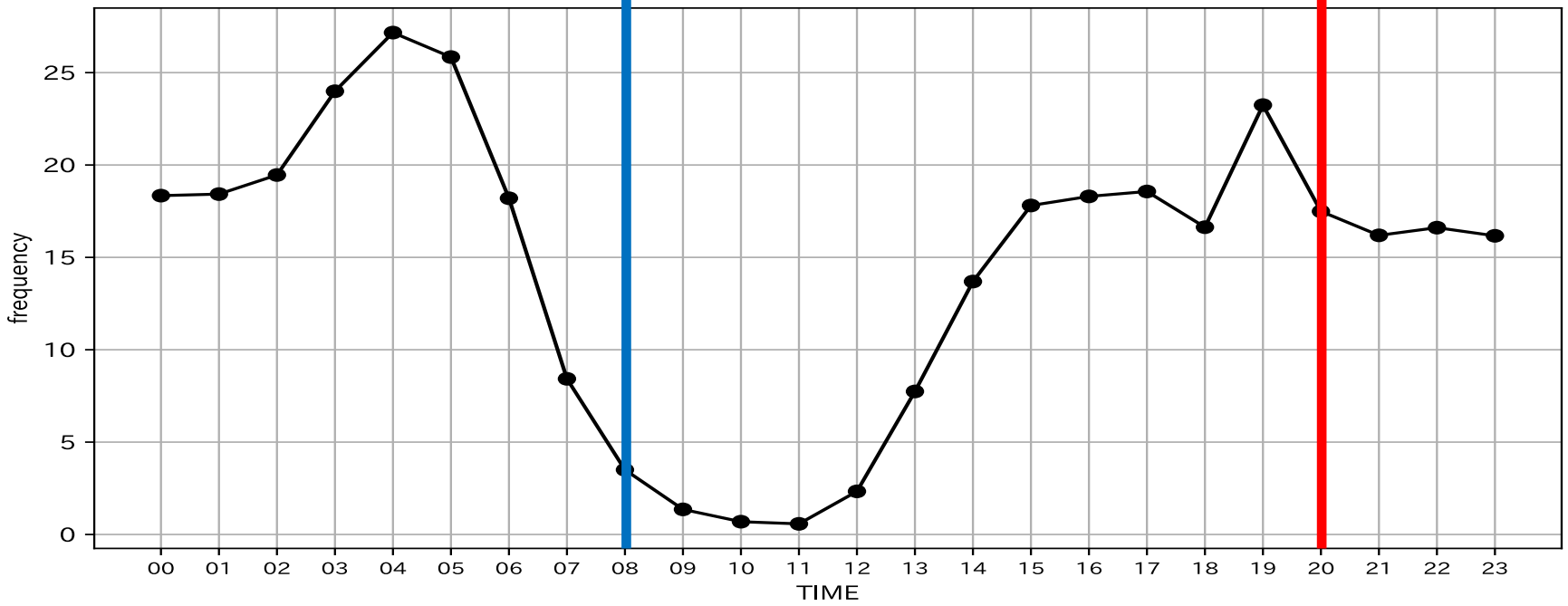
誤差+1（UTC+8）：987個

＊取引数15回以上のアドレスが対象である（6848個）

取引時間分布



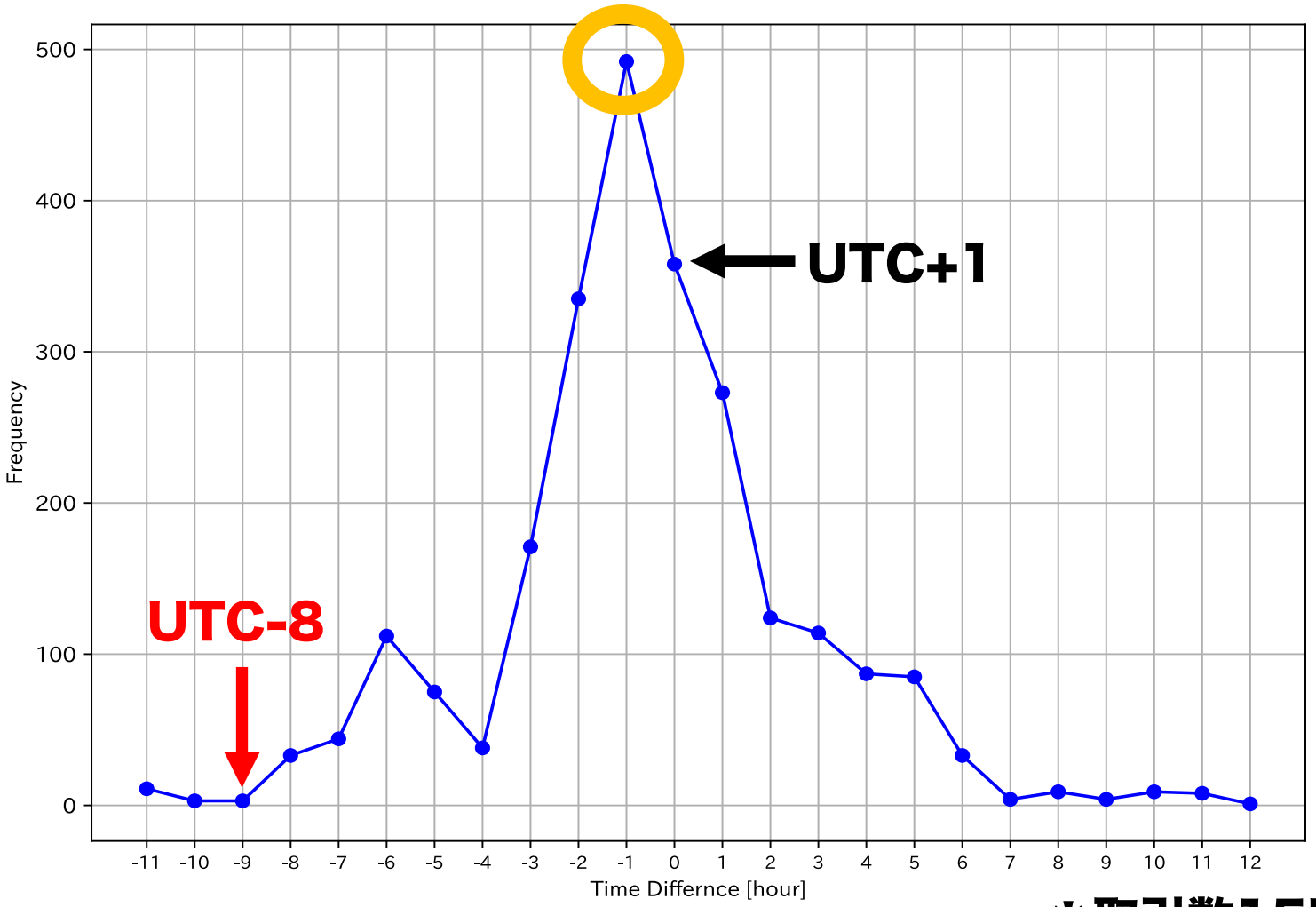
インターネット利用時間 (UTC-8)



PST0 PST12

取引所Krakenのアドレス推定時間分布

国：アメリカ　推定値：UTC+1　正解：UTC-8



誤差+0（**UTC+1**）：358個

誤差-1（UTC+0）：492個

誤差-9（UTC-8）：3個

＊取引数15回以上のアドレスが対象である（2426個）

精度

推定値と正解の差	取引所数
0	19
1	36
2	10
3	4
4以上	11

80取引所中65箇所

まとめ

ユーザは日中に取引をすることが多いという仮説のもとで，
ユーザと取引所のタイムゾーンを推定した．

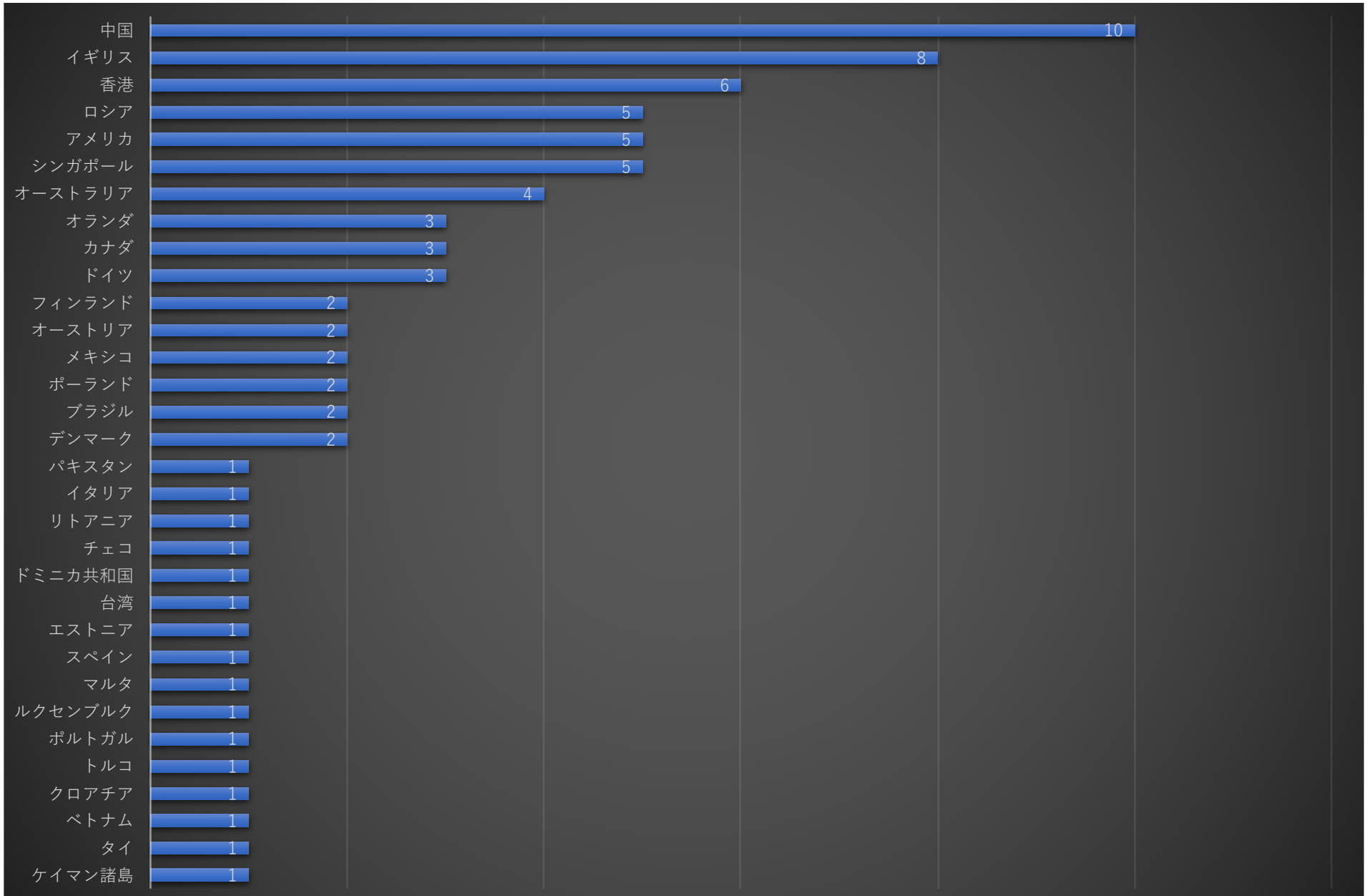
- 誤差範囲2以内の割合が約81％という結果より，
  ユーザは取引所が属する国で生活する可能性が高い．

- 他の取引所は約19％で，グローバル化が進んでいる
  国が多く，多国籍の人たちが使用していると考えられる．

ご清聴ありがとうございました

質問用スライド

取引所80箇所の内わけ



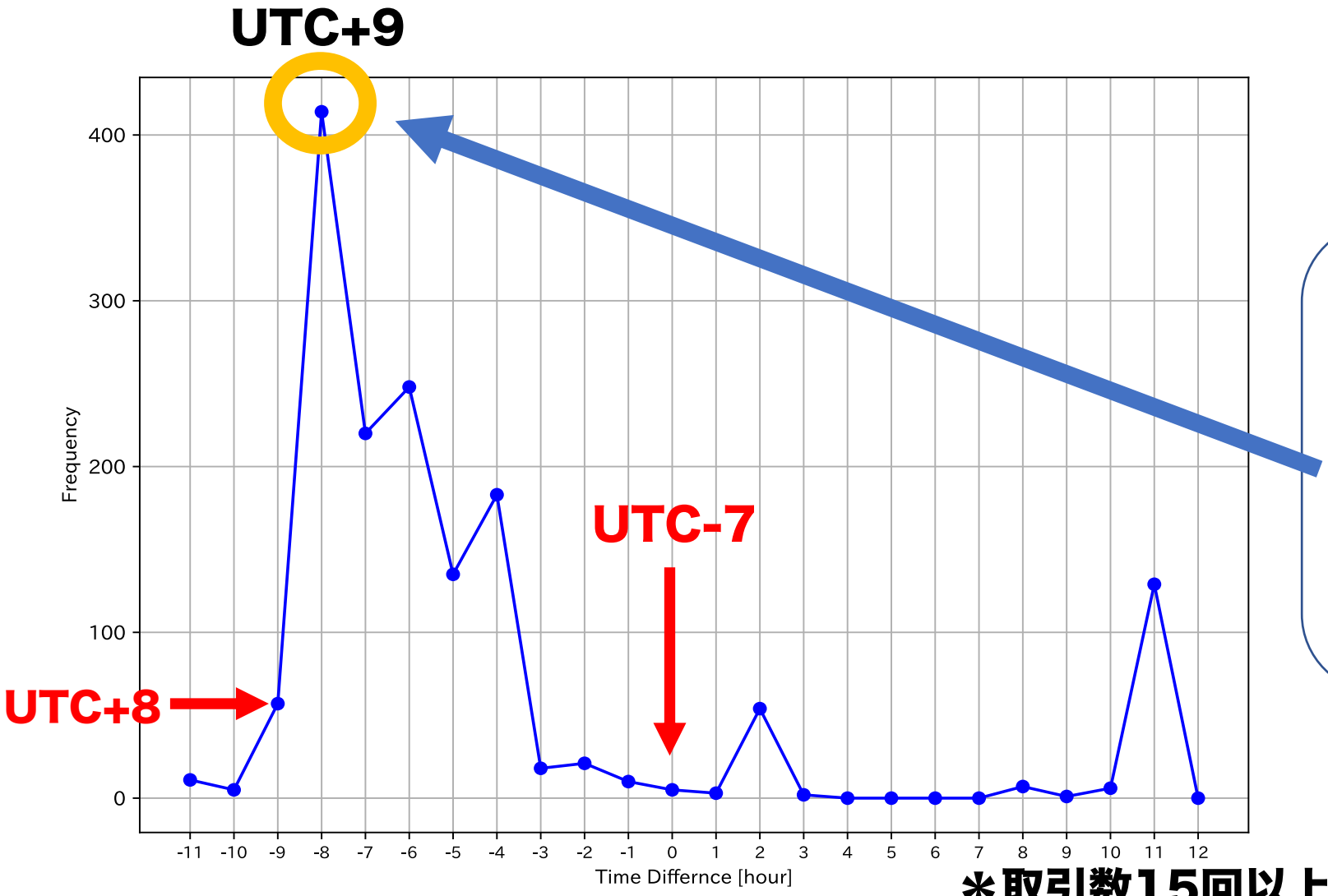
失敗した国一覧

国	取引所	正解	推定値
香港	Gatecoin	+8	+3
香港	Bitfinex	+8	-4
香港	AnxPro	+8	-7
中国	Hashnest	+8	+4
中国	Banx.io	+8	+1
シンガポール	FYBSG	+8	+5
シンガポール	CoinArch	+8	-6
ロシア	CoinChimp	+3	-5
ポーランド	Bitcurex	+1	+5
フィンランド	LocalBitcoins	+1	-2
イギリス	Indacoin	0	+3
ドミニカ共和国	OrderBook	-4	0
カナダ	Coins-e	-5	-2
アメリカ	EmpoEx	-7	+1
アメリカ	Kraken	-7	+1

取引所AnxProのアドレス推定時間分布

国：香港　正解：UTC+8　推定値：UTC-7

アメリカ？カナダ？



誤差0（UTC-7）：５個

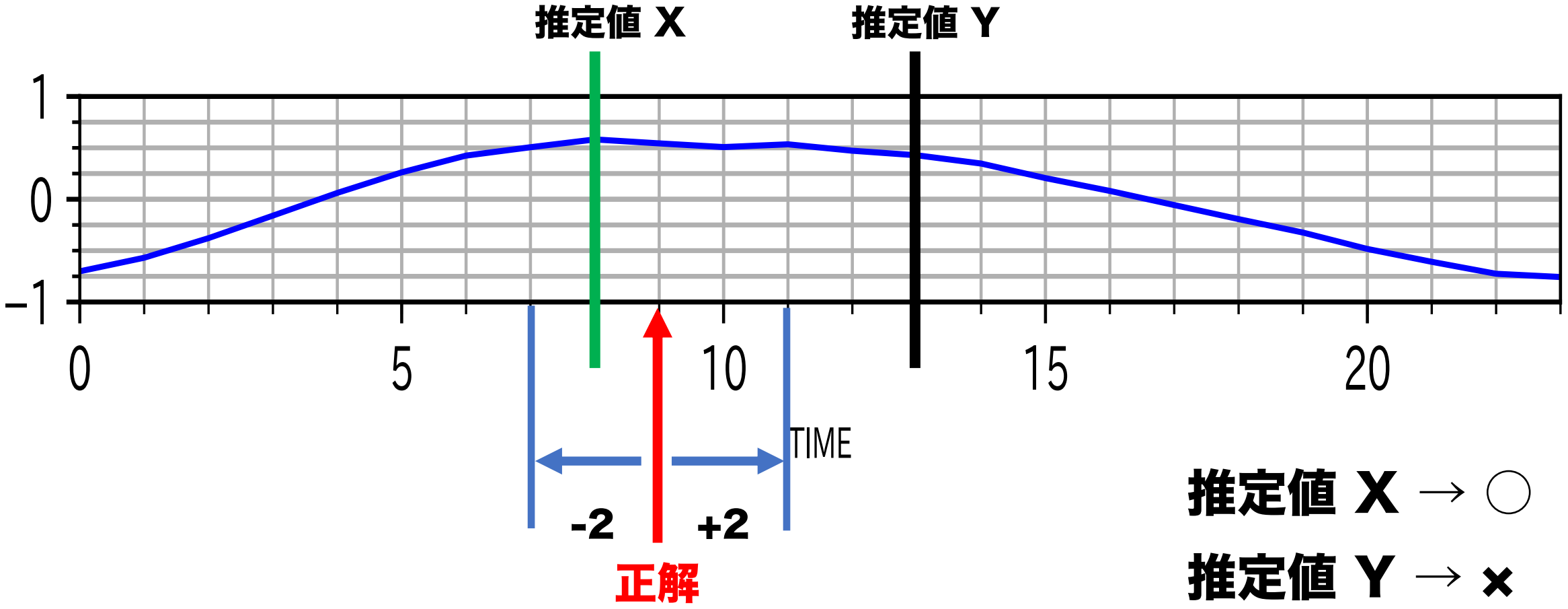
誤差-8（UTC+9）：414個

誤差-9（UTC+8）：57個

＊取引数15回以上のアドレスが対象である（1546個）

評価手法

・推定値と正解との差が２時間以内のものを推定できたとする

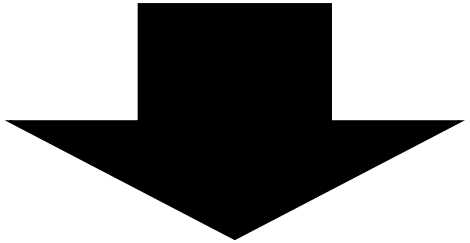


推定値 X → ○

推定値 Y → ×

なぜ利用時間を24時間分？

インターネットを利用する時間帯は世界中どこでも同じ



UTCを-11～12の24時間分ずらせば
世界中の国々に対応させることができる