もっと遠くに、もっと近くに。
Geolocation Technology

Internet Week 2019
D1-3 セキュリティとIPアドレスの深イイ話

知っておきたいIPアドレス分析テクニック

2019/11/26

株式会社Geolocation Technology
風間　勇人

IP Geolocation(GeoIP)をご存じでしょうか。

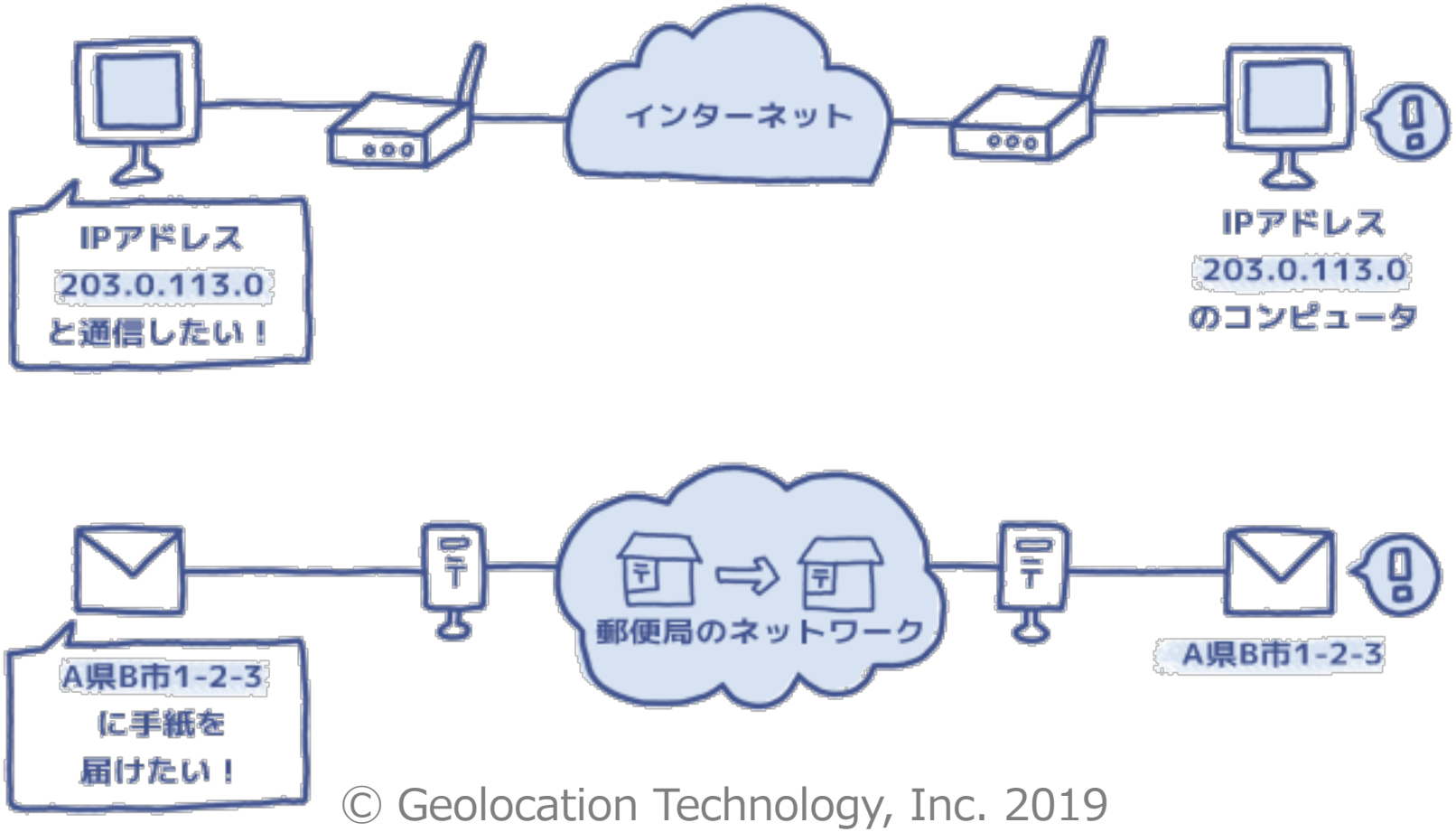
IPアドレスから、アクセスユーザーの位置情報やインターネット接続環境、匿名ネットワーク情報などを取得し、
不正検出からコンプライアンス、 さらにはマーケティングなど、幅広い用途に利用可能なデータセットです。

しかしながら、 このデータセットを有効に活用するにはコツがあります。

本プログラムでは、
IPv4アドレス共有や地理情報共有に関わる業界団体の動きに触れつつ、
IP Geolocationデータを使った調査・分析時に気をつけるべきことや
利用例をご紹介いたします。

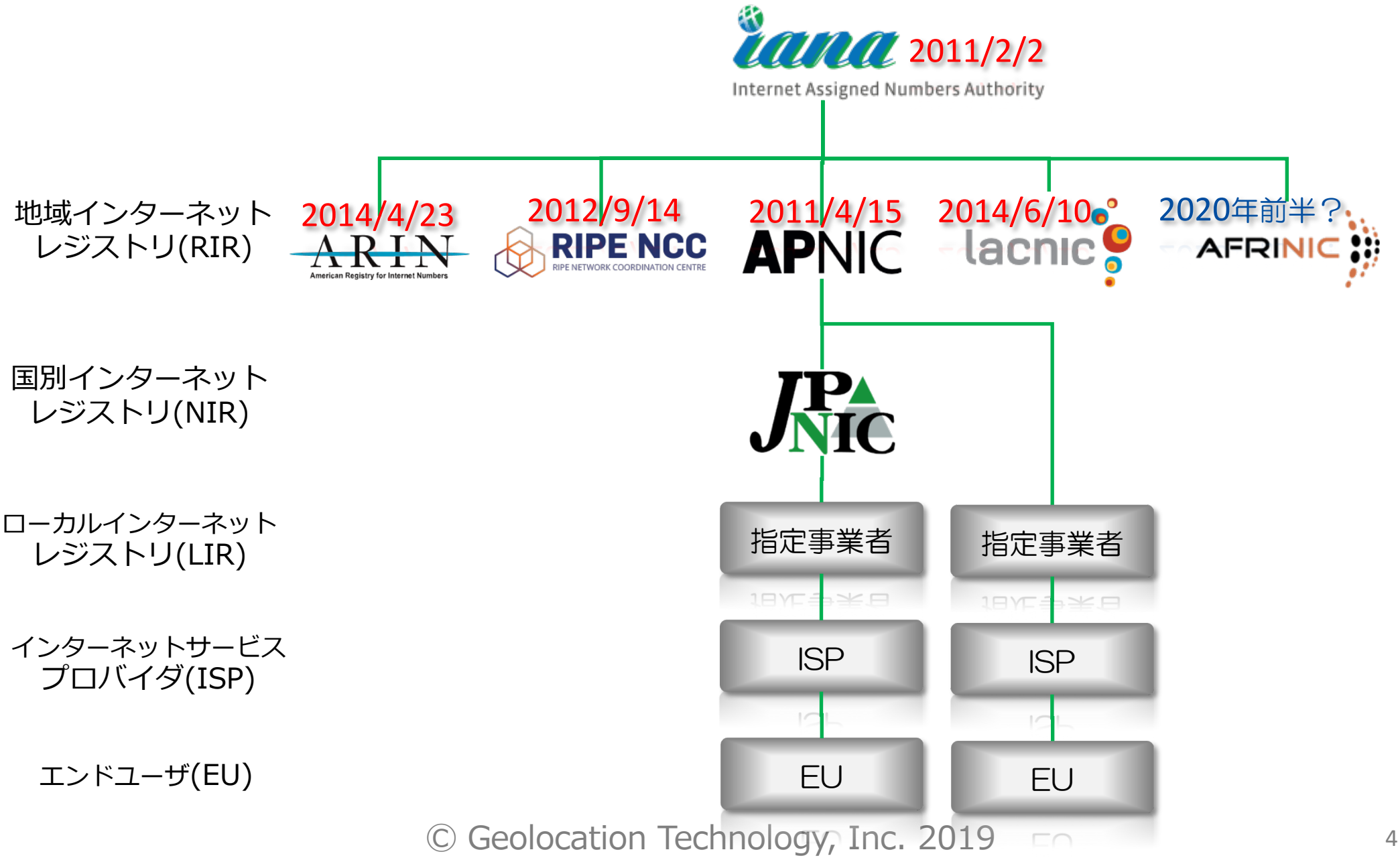
IPアドレスとは？

IPアドレスとは、ネットワーク上の機器ひとつひとつに割り振られた識別用の番号です。手紙を出すときに住所を書くように、ネットワーク上の機器（他のコンピュータや、Webサーバなど）と通信する時は、宛先となるIPアドレスが必要になります。このように、IPアドレスはしばしば「ネットワーク上の住所」に例えられます。



IPアドレス管理の構造とIPv4アドレスの枯渇時期

もっと遠くに、もっと近くに。
Geolocation Technology



もっと遠くに、もっと近くに。
Geolocation Technology

JPNIC IPv4アドレス移転履歴

・JPNIC IPv4アドレス移転履歴 サマリ※2019/11/24現在

移転件数：395件

内訳

JPNIC→JPNIC移転	296件
Inter-RIR移転	77件

19.49%

※2017/6　12.84%

移転IPv4アドレス数：10,088,960IP

内訳

JPNIC→JPNIC移転	7,916,544IP
Inter-RIR移転	2,172,416IP

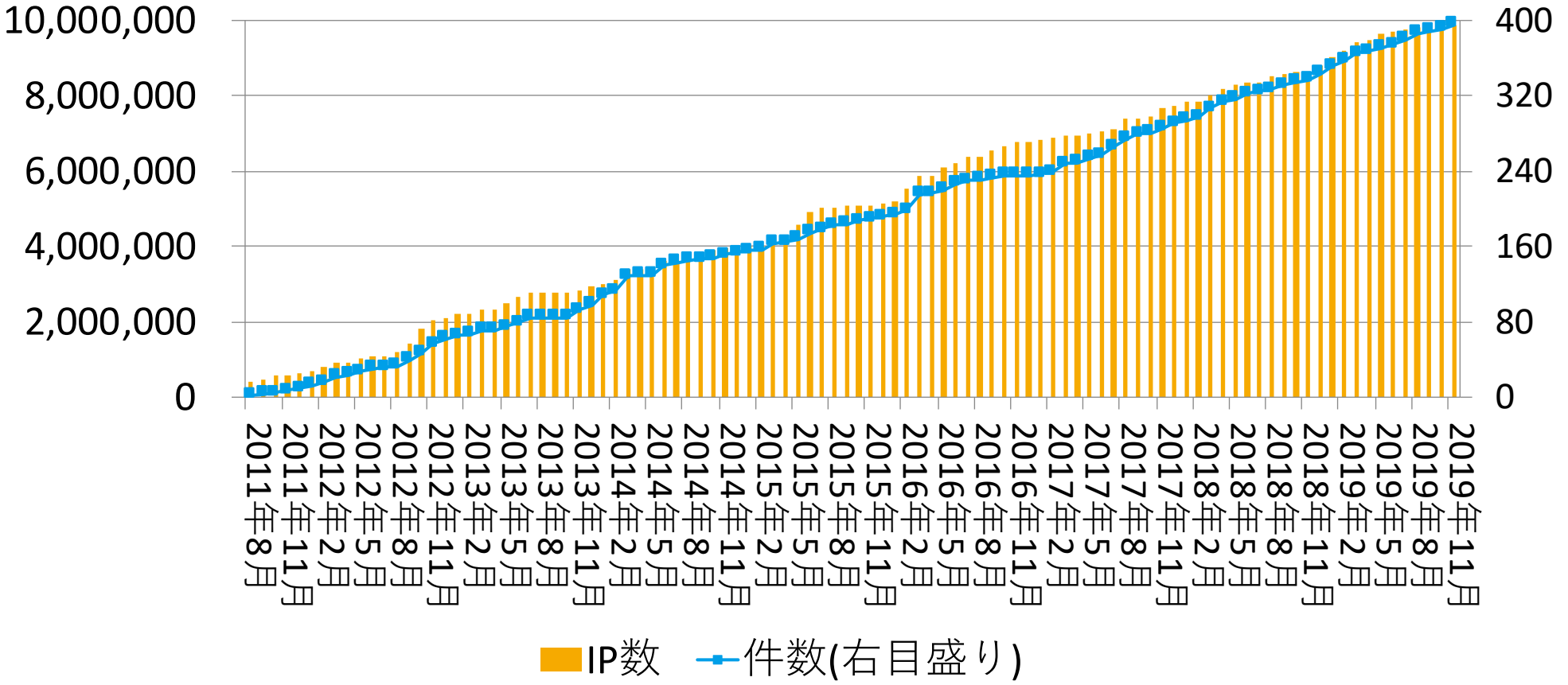
21.53%

※2017/6　23.84%

もっと遠くに、もっと近くに。
Geolocation Technology

JPNIC IPv4アドレス移転履歴の推移

・JPNIC 移転履歴の推移(累積)

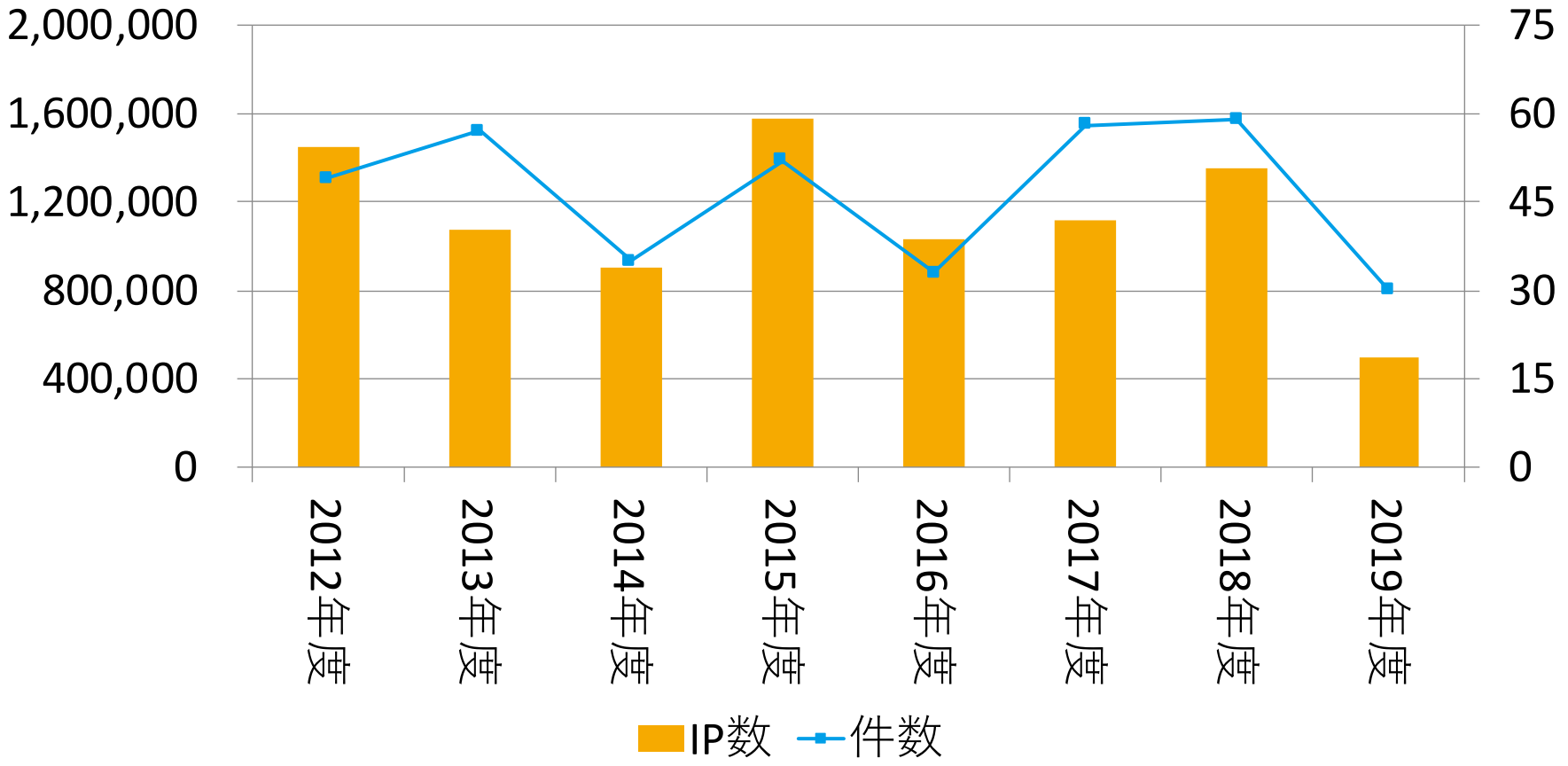


※算出根拠：https://www.nic.ad.jp/ja/ip/transfer/ipv4-log.html

もっと遠くに、もっと近くに。
Geolocation Technology

JPNIC IPv4アドレス移転履歴の推移

・JPNIC 移転履歴推移(年度) ※2019/11/24現在

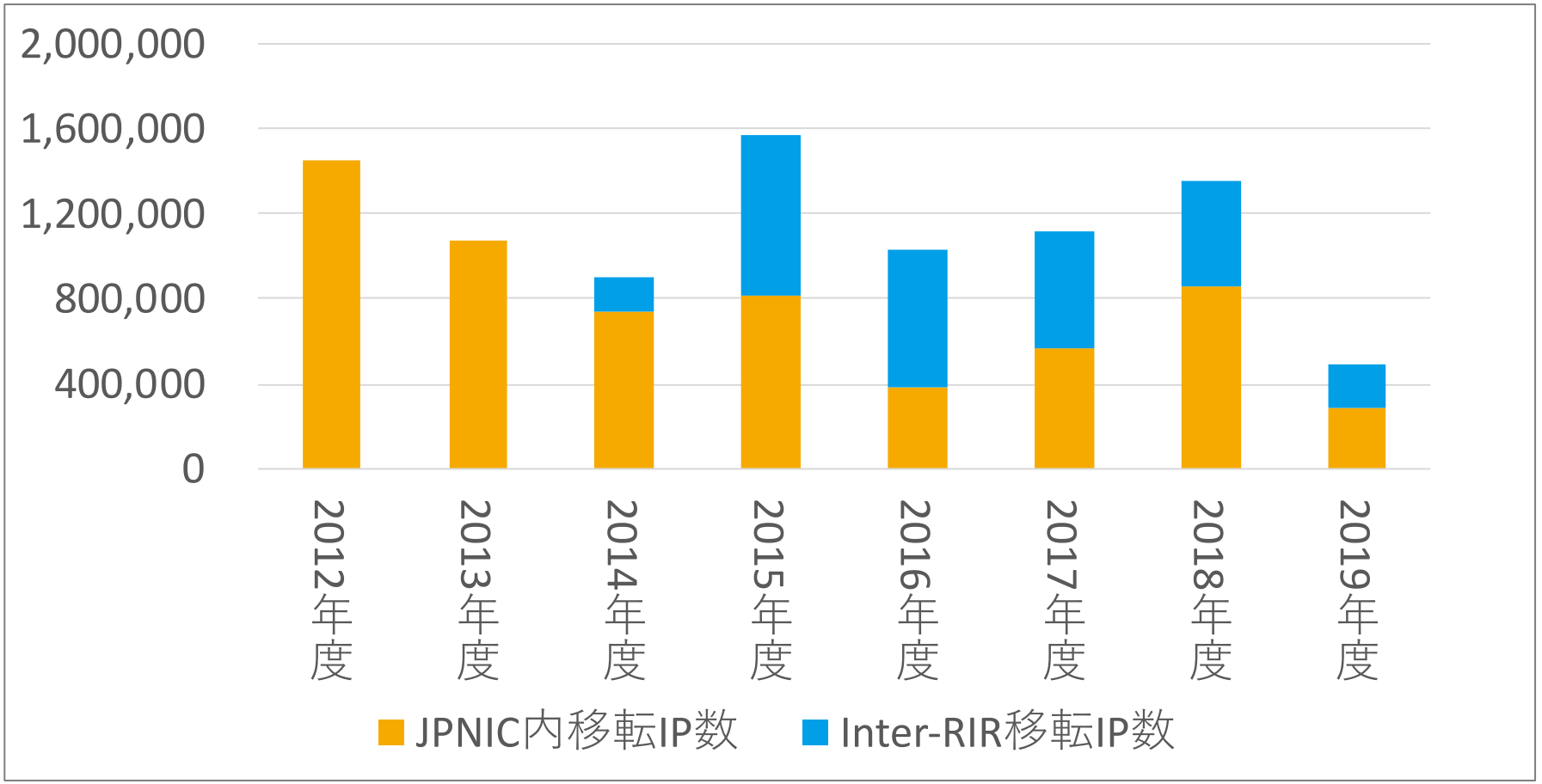


※算出根拠：https://www.nic.ad.jp/ja/ip/transfer/ipv4-log.html

もっと遠くに、もっと近くに。
Geolocation Technology

JPNIC IPv4アドレス移転履歴の推移

・JPNIC 移転履歴推移(国内/国際移転比較)_IPアドレス数ベース

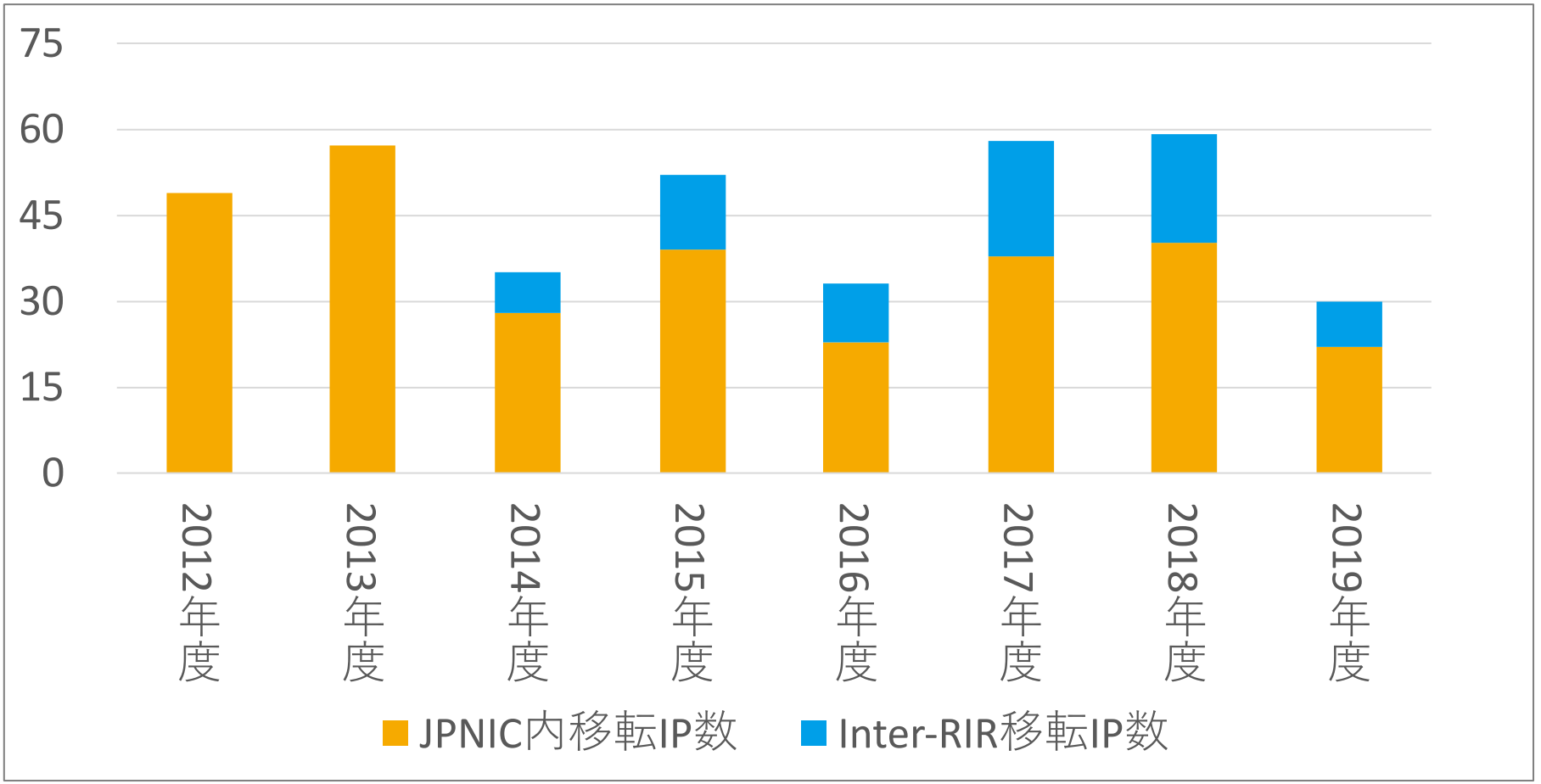


※算出根拠：https://www.nic.ad.jp/ja/ip/transfer/ipv4-log.html

もっと遠くに、もっと近くに。
Geolocation Technology

JPNIC IPv4アドレス移転履歴の推移

・JPNIC 移転履歴推移(国内/国際移転比較)_移転件数ベース



※算出根拠：https://www.nic.ad.jp/ja/ip/transfer/ipv4-log.html

もっと遠くに、もっと近くに。
Geolocation Technology

IPv4アドレスの相場

単価は、引き続きゆるやかに「上昇中」

国内移転相場：2,200円～2,500円(税別)

国際移転相場：20ドル～24ドル

IPv4アドレスが国や地域を越えて移転するようになった。

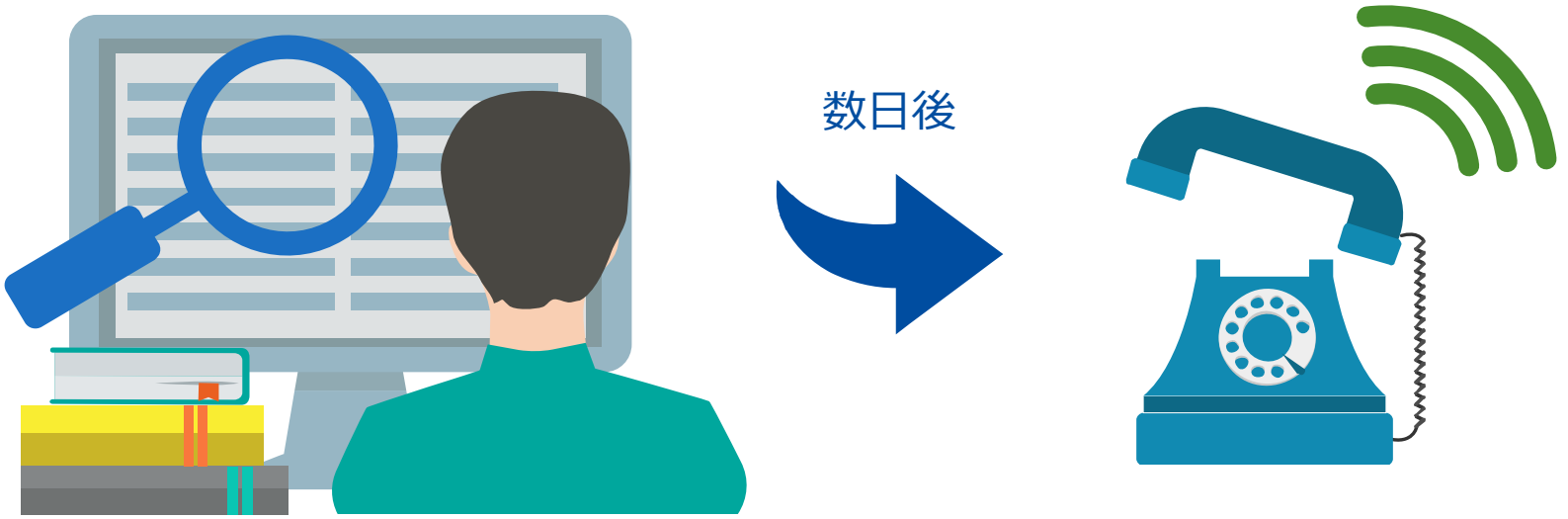
海外のIP Geolocationデータを使っているWebサイトで見られないトラブルが発生？

突然ですが、
こんな経験はありませんか？

天気予報サイトを訪問

地元の予報が自動で表示

ほかにも、
こんな経験はありませんか？



企業のWebサイトを訪問

営業電話がかかる

この仕組みを実現しているのが…

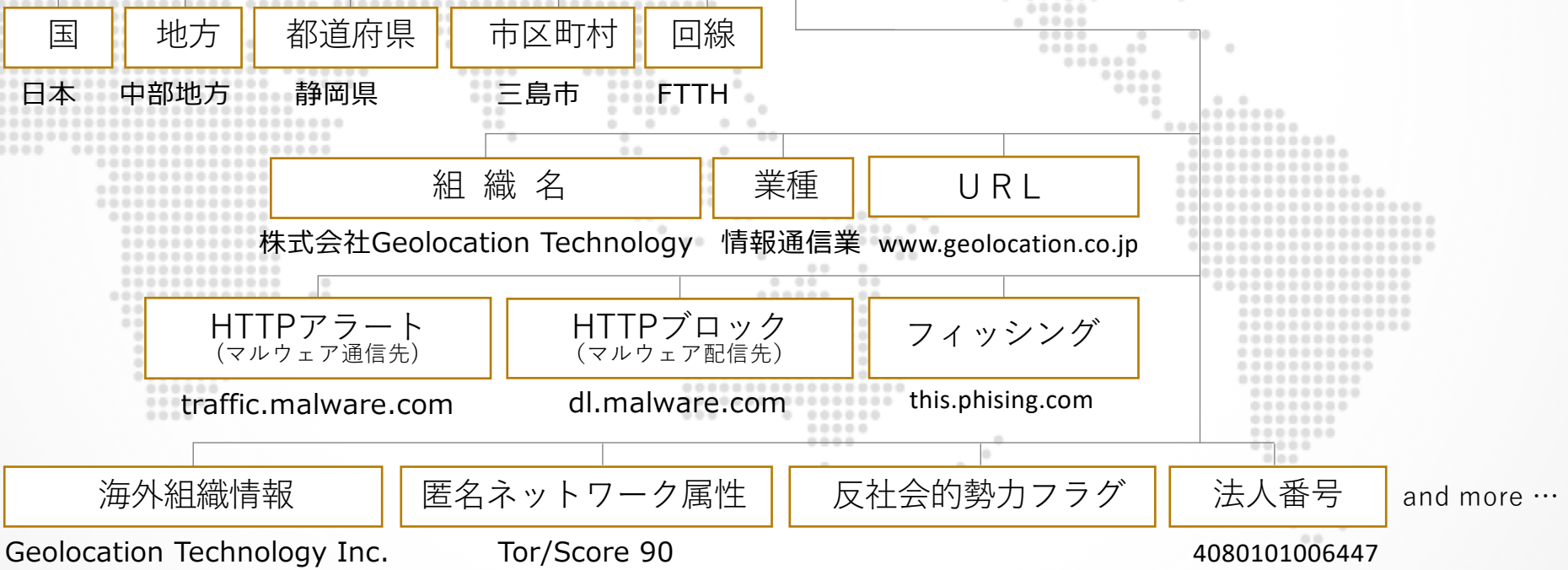
IP Geolocation

(GeoIP)

もっと遠くに、もっと近くに。
Geolocation Technology

IPアドレスから導く情報は
多様なアプローチでセキュリティを強化します

210.251.250.30



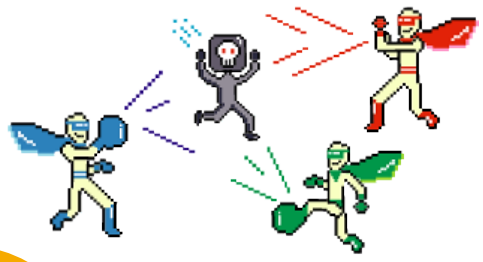
IP Geolocationテクノロジーと カバー領域

もっと遠くに、もっと近くに。
Geolocation Technology

マーケティング
MARKETING
IPアドレスと組み合わせた情報で最適化

位置情報や企業情報を活用したWebサイトは、情報を最適化します。リードジェネレーションからリードナーチャリングまで。デジタル広告やデータ分析の分野でも活躍しています。

不正検出
FRAUD DETECTION
オンラインでの不正を検出する技術



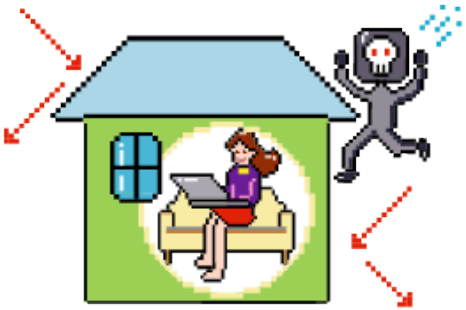
ネット上の不正やなりすましなどの詐欺行為を検出します。位置情報の特定や接続環境を認識することで、オンラインバンキングをはじめとした様々なサービスで不正アクセスからアカウントを守っています。

IP Geolocation

コンプライアンス
COMPLIANCE
コンテンツ配信の権利を守る

デジタル配信される映像や音楽。世界中のインターネットアクセスにおいて、位置情報を特定することでコンテンツの配信権利は守られています。ブランド保護はロイヤリティや長期的な信頼につながります。

セキュリティ
SECURITY
セキュリティインシデント対応を支援



データの保全や解析、サイバー攻撃における侵入経路調査や被害状況の究明、ウィルス発信元調査やサイバー犯罪の初期捜査にIPアドレス情報が役立てられています。

日本のIP Geolocation登場の背景

インターネットプロバイダー企業で営業担当訪問していく中で、
県庁や地元のラジオ局から「県民の割合を教えてほしい」
「地域でバナーを切り替えたい」という要望をいただいたこと。

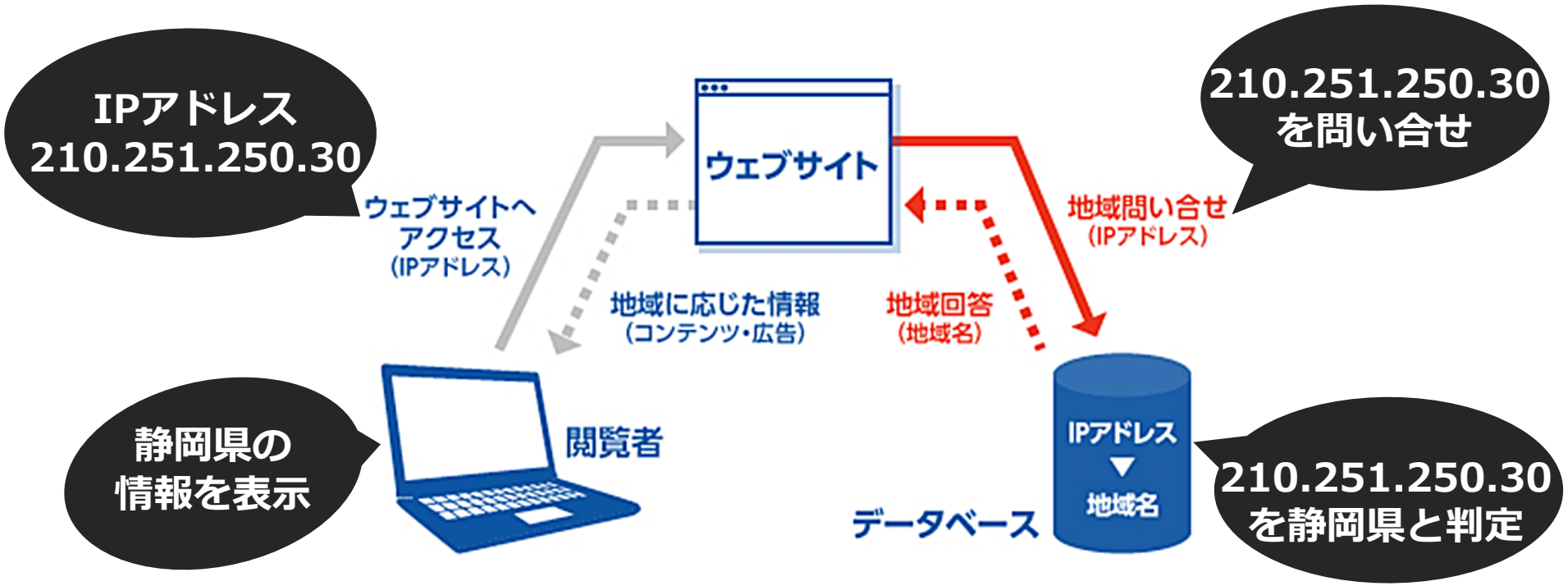
IPv4アドレスにおける IP Geolocationの利用例

IP Geolocationの利用例

MARKETING

✓ ①Webコンテンツでの利用

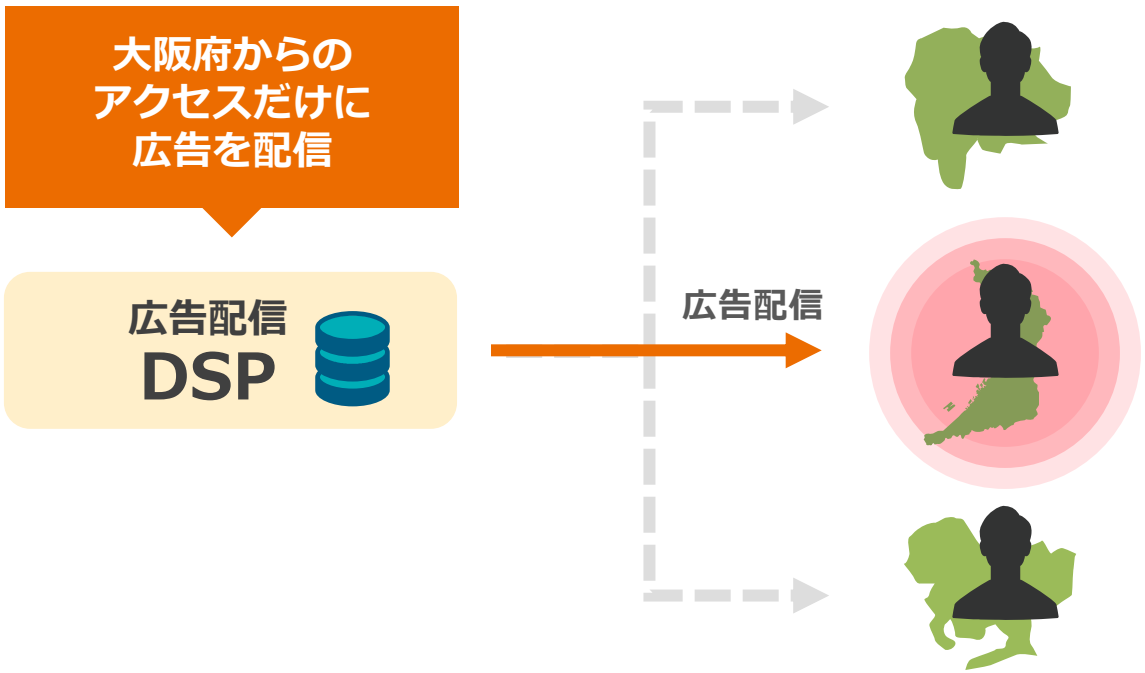
地域ごとにコンテンツを切り替えて最適な情報を発信



MARKETING

✓ ②-1 インターネット広告での利用

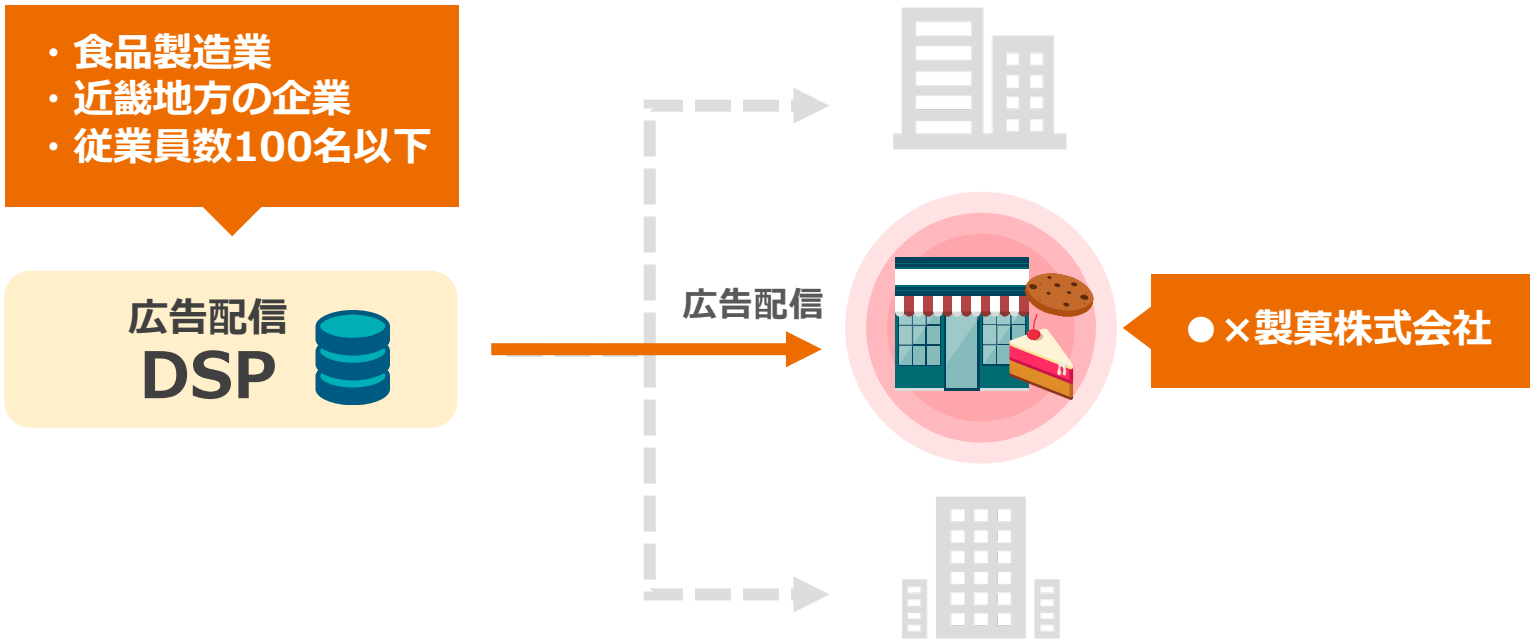
狙いたい地域を指定して広告配信



MARKETING

✓②-2 インターネット広告での利用

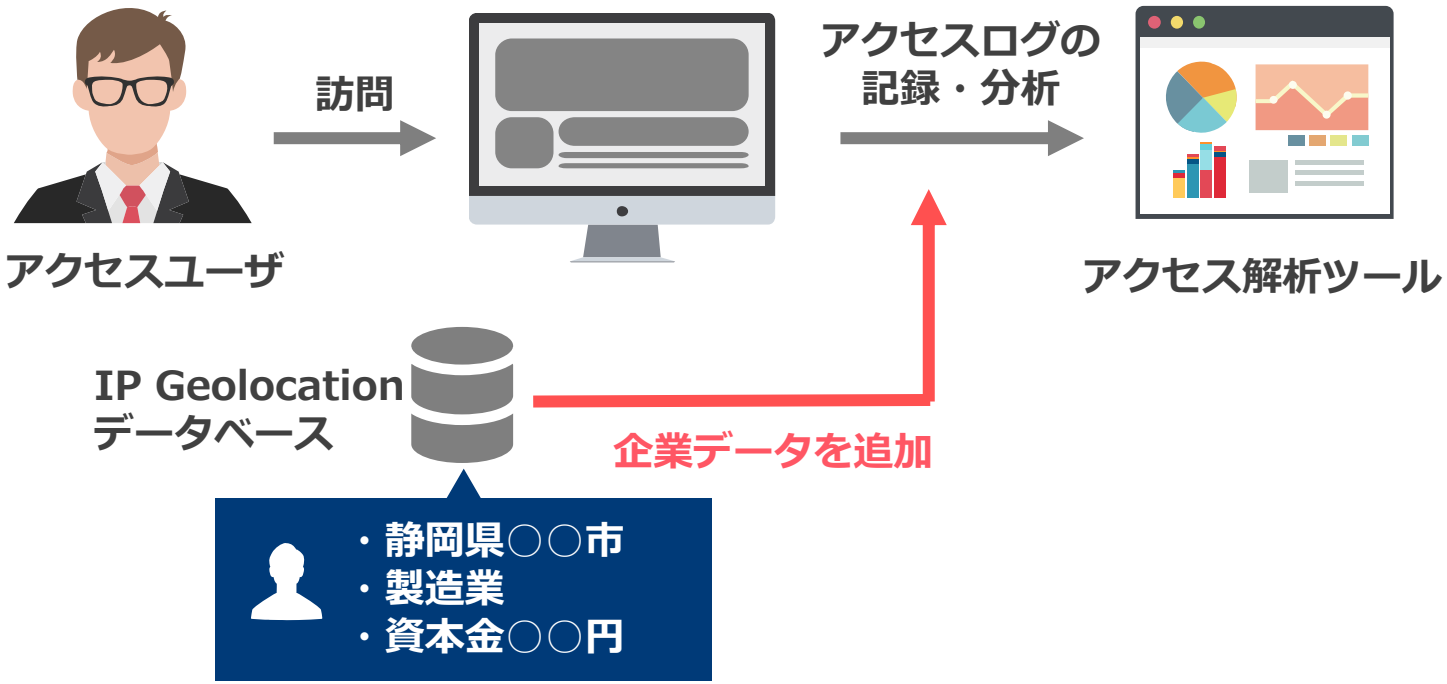
狙いたい企業属性を指定して広告配信



MARKETING

✓ ③アクセス解析での利用

アクセスログを解析ツールに送る際に企業データを付与

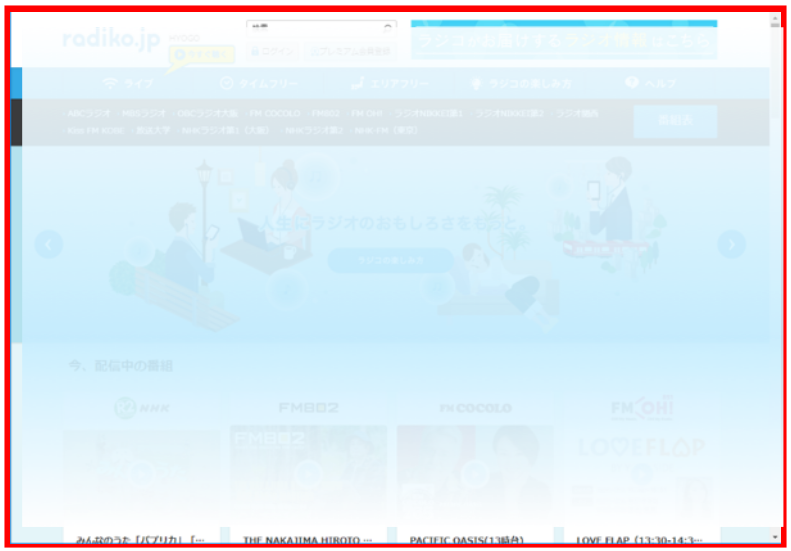


もっと遠くに、もっと近くに。
Geolocation Technology

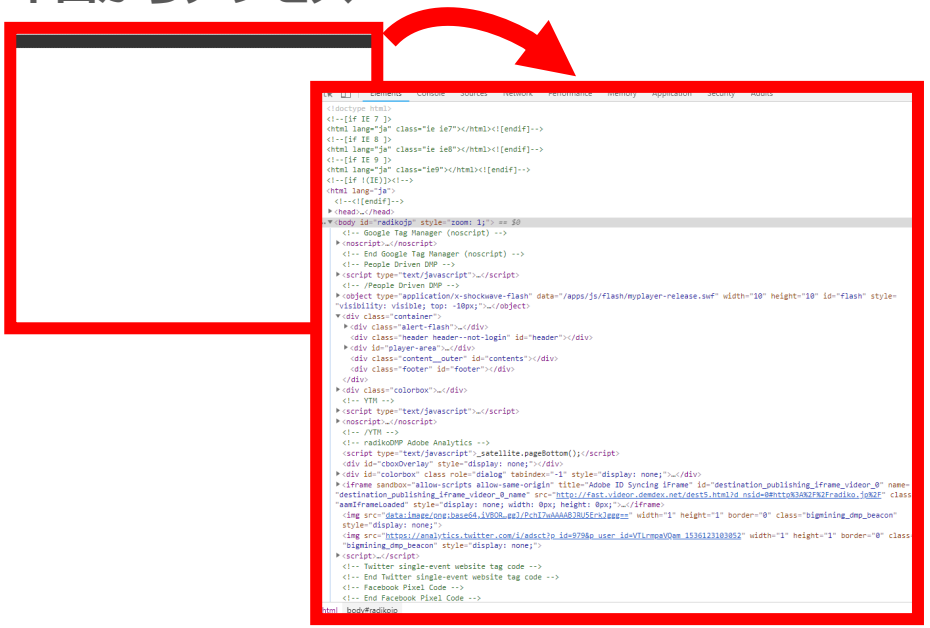
COMPLIANCE

- ✓ コンテンツビジネスの配信制御での利用
  - ・国際的なスポーツイベントの配信制御（国内限定/国別配信）
  - ・動画コンテンツの配信制御（国別配信/国内限定/都道府県別配信制御）
  - ・サイマルラジオの配信制御（国内限定/都道府県別配信制御）

大阪からアクセス



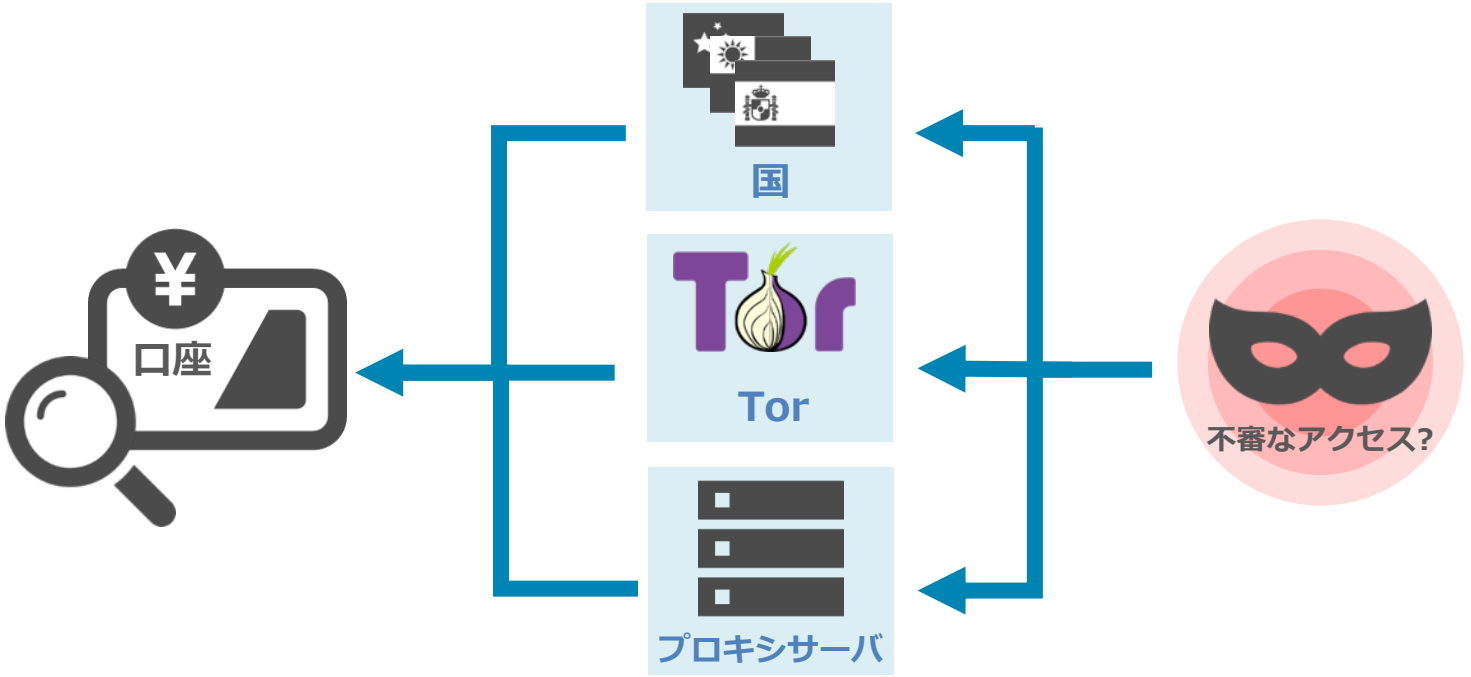
中国からアクセス



FRAUD DETECTION

ハイリスク取引の検出

ハイリスクの国や、Torやプロキシサーバ等など不審なアクセスの可能性が高い取引を検出。

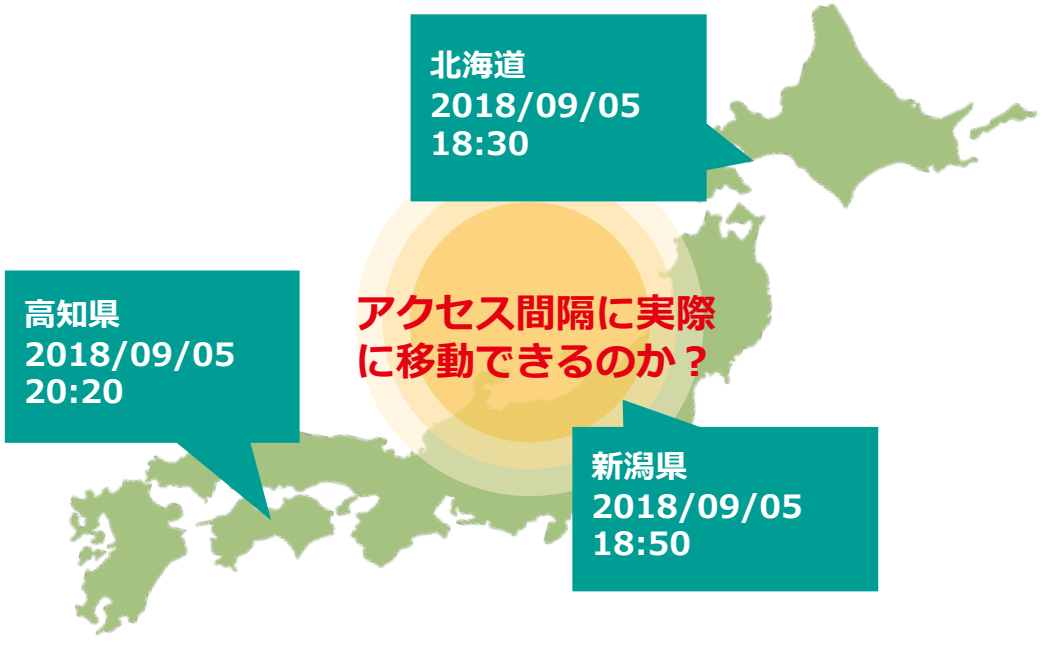


もっと遠くに、もっと近くに。
Geolocation Technology

FRAUD DETECTION

なりすましの検出①

複数のIPから同一の口座にアクセスがある場合、現実にありうる範囲なのか疑う。



取引履歴

IPの場所	取引日時
北海道	2018/09/05 18:30
新潟県	2018/09/05 18:50
高知県	2018/09/05 20:20

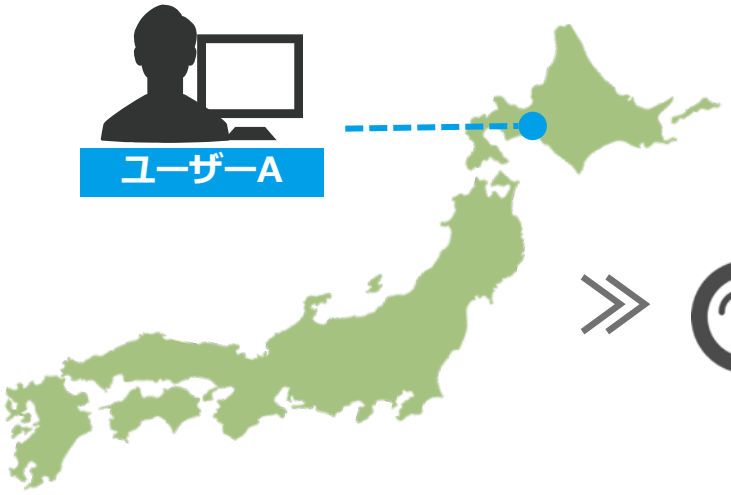
計算上の移動時間とアクセス時間を比較して検出する

もっと遠くに、もっと近くに。
Geolocation Technology

FRAUD DETECTION

なりすましの検出②

ユーザーのトランザクションパターンをためこみ、ユーザーの傾向をつかむ。これと外れた挙動を示したとき（自宅または勤務先都道府県以外からのアクセスがあるときなど）、本当にユーザー本人かどうかを疑う。



ユーザーA

IPの場所	取引日時	金額
北海道	14/12/14	80,000
北海道	15/03/22	70,000
北海道	15/09/10	10,000
北海道	16/02/04	50,000
北海道	16/08/18	90,000
北海道	17/05/30	10,000
東京	17/09/01	500,000
大阪	17/09/02	300,000

本人からのアクセス?

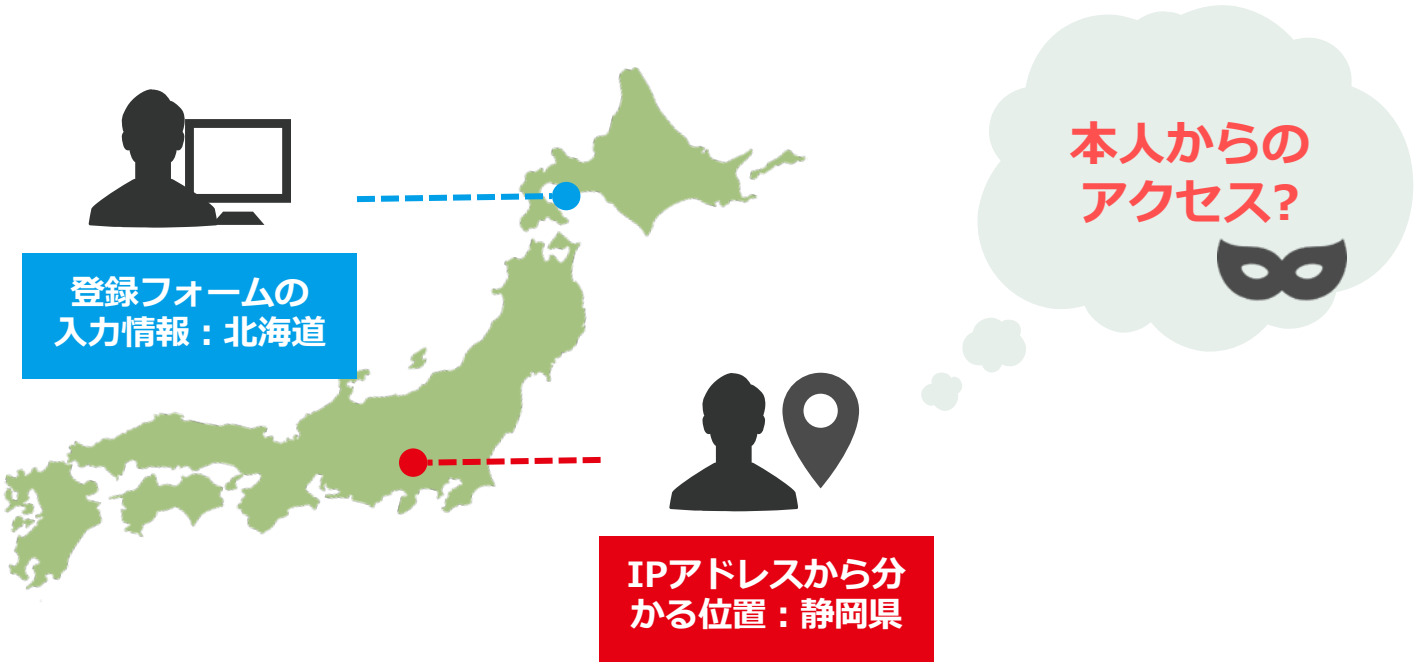
場所・時間帯・金額・日にち・取引内容などをチェック

もっと遠くに、もっと近くに。
Geolocation Technology

FRAUD DETECTION

虚偽登録の検出

「ユーザがアカウント作成時に入力した住所」と「IPアドレスからわかる地域」を比較し、地理的な不一致を検出。



FRAUD DETECTION

セッションハイジェックの検出

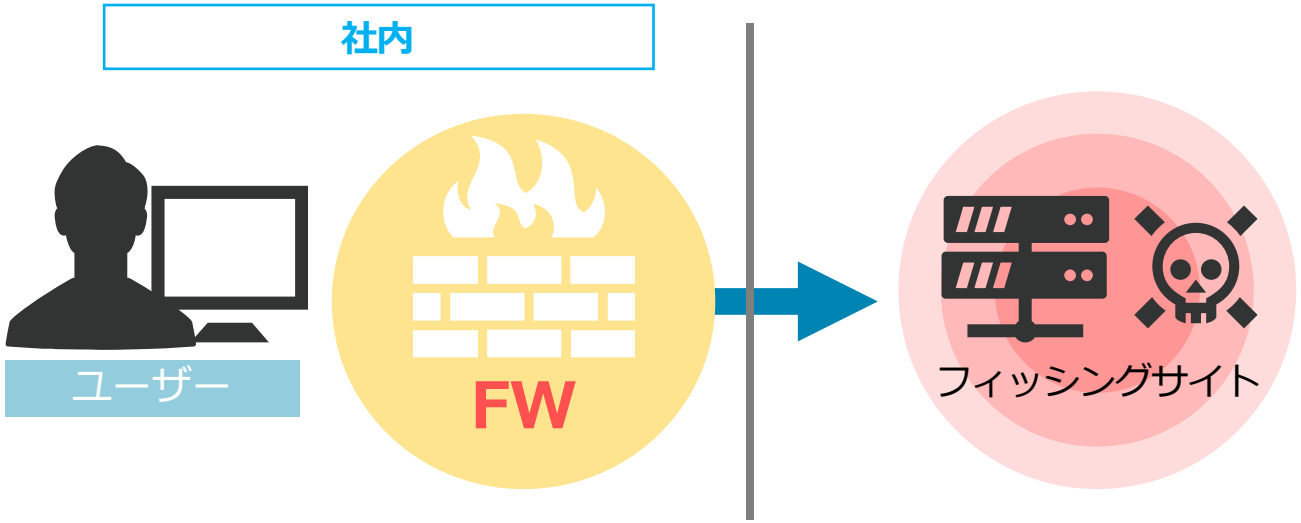
認証後のユーザアカウントに紐づくIPアドレスの遷移を分析することで、トランザクションへの不正侵入を発見します。

アカウント名	日時	セッション内容	IPアドレス	IPの地域
abc1234567	2017/9/1 18:00:55	アカウントログイン試行	10.1.11.1	静岡県
abc1234567	2017/9/1 18:01:30	ログイン認証	10.1.11.1	静岡県
abc1234567	2017/9/1 18:02:08	ログイン	10.1.11.1	静岡県
abc1234567	2017/9/1 18:10:23	取引選択	192.168.0.1	CN
abc1234567	2017/9/1 18:11:10	自動レビュー	192.168.0.1	CN

SECURITY

不審な通信の検出①

マルウェア等の通信先として使われていたIPアドレスへのログを検出。
フィッシングサイトとして使われていたIPアドレスへのログを検出。

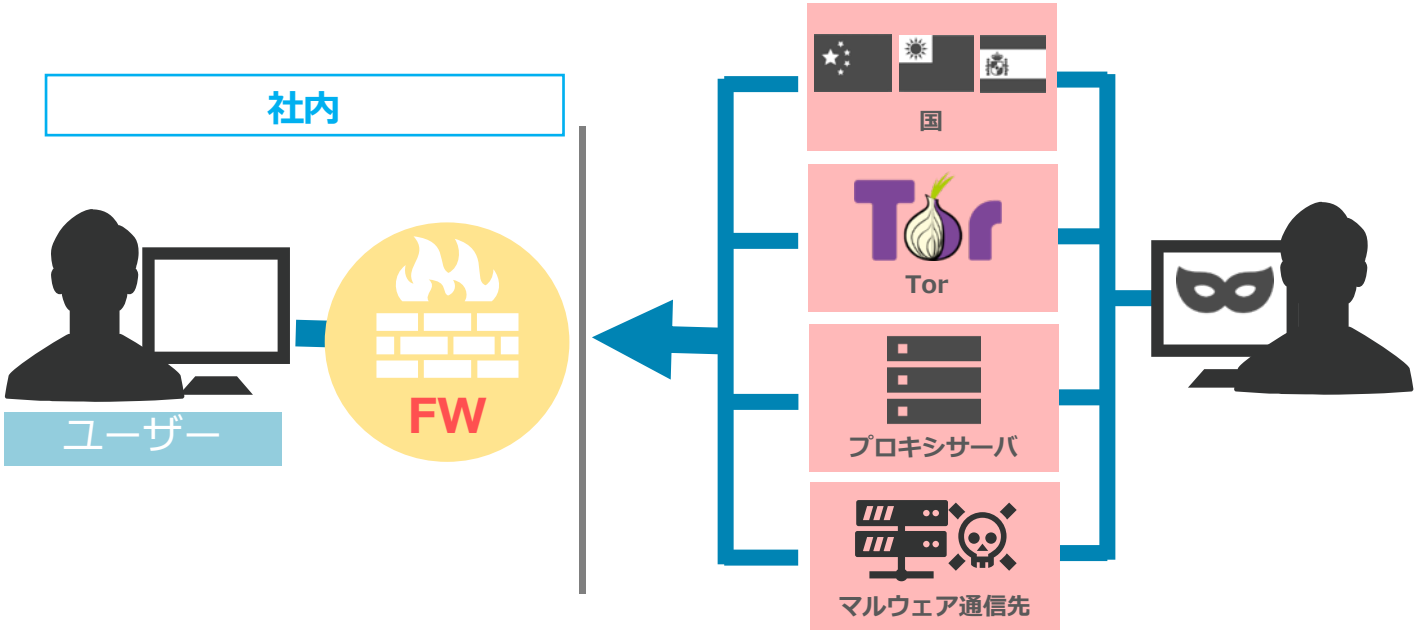


もっと遠くに、もっと近くに。
Geolocation Technology

SECURITY

不審な通信の検出②

自社ネットワークに対する通信ログを分析し、社員のいない国やマルウェア通信先、Proxy・Tor・等の匿名ネットワークからのアクセスなど、攻撃の疑われる不審なログを検出します。

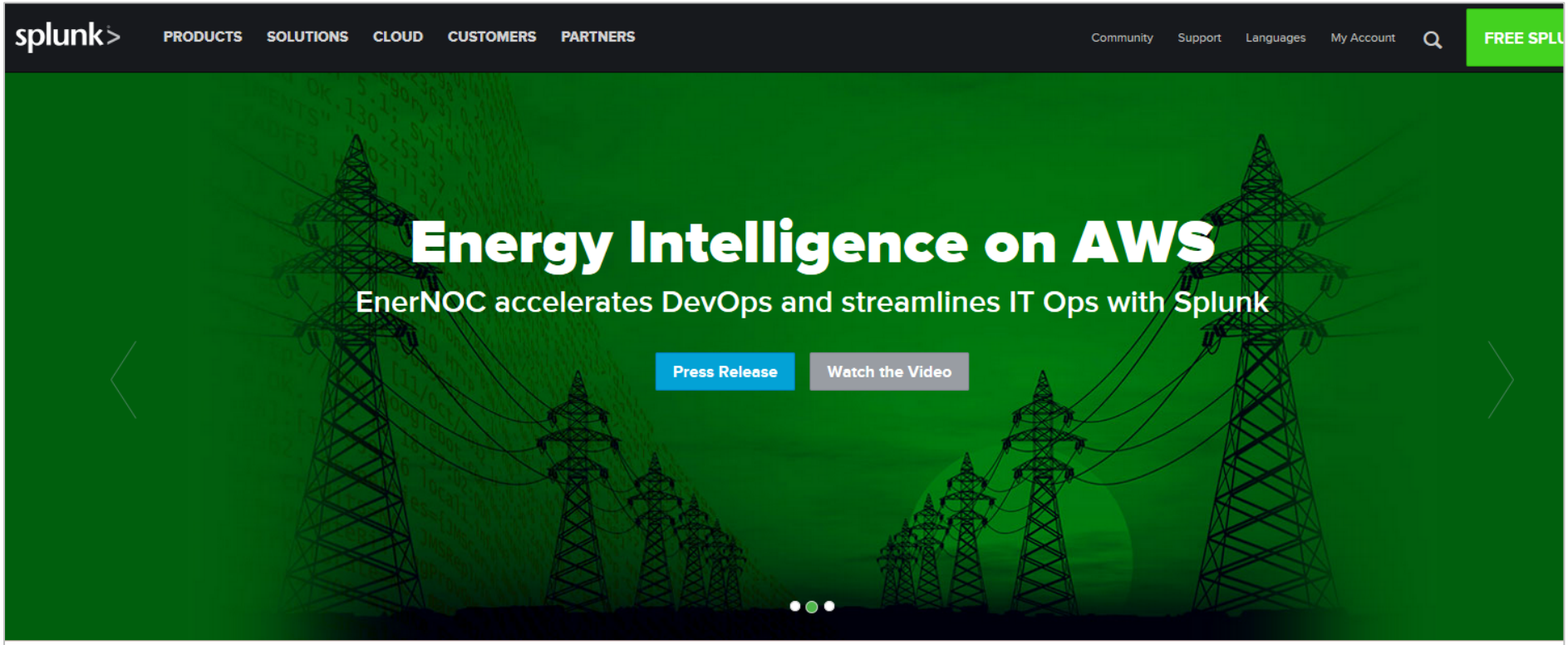


Splunkとどこどこjpを使った分析例

参考URL… https://www.docodoco.jp/block/splunk.html

Splunkとは

米Splunk社の提供するマシンデータ分析プラットフォーム。ITシステムから生成される多様なマシンデータを収集・可視化し、セキュリティやITインフラの管理、データ分析など、幅広い分野の課題解決に利用されています。



http://www.splunk.com/

IPアドレスから地域・組織・回線など多様な情報を提供するAPIサービス。

ご利用料金

初期費用　¥100,000(税抜)
月額費用　¥10,000～(税抜)/月

犯罪捜査やセキュリティ技術など高い精度が必要とされる場面での活用のために、全世界のIPアドレスデータを搭載しているだけでなく、継続した調査によってデータの品質を向上させる取り組みを日々行っています。

どこどこJP のデータセット

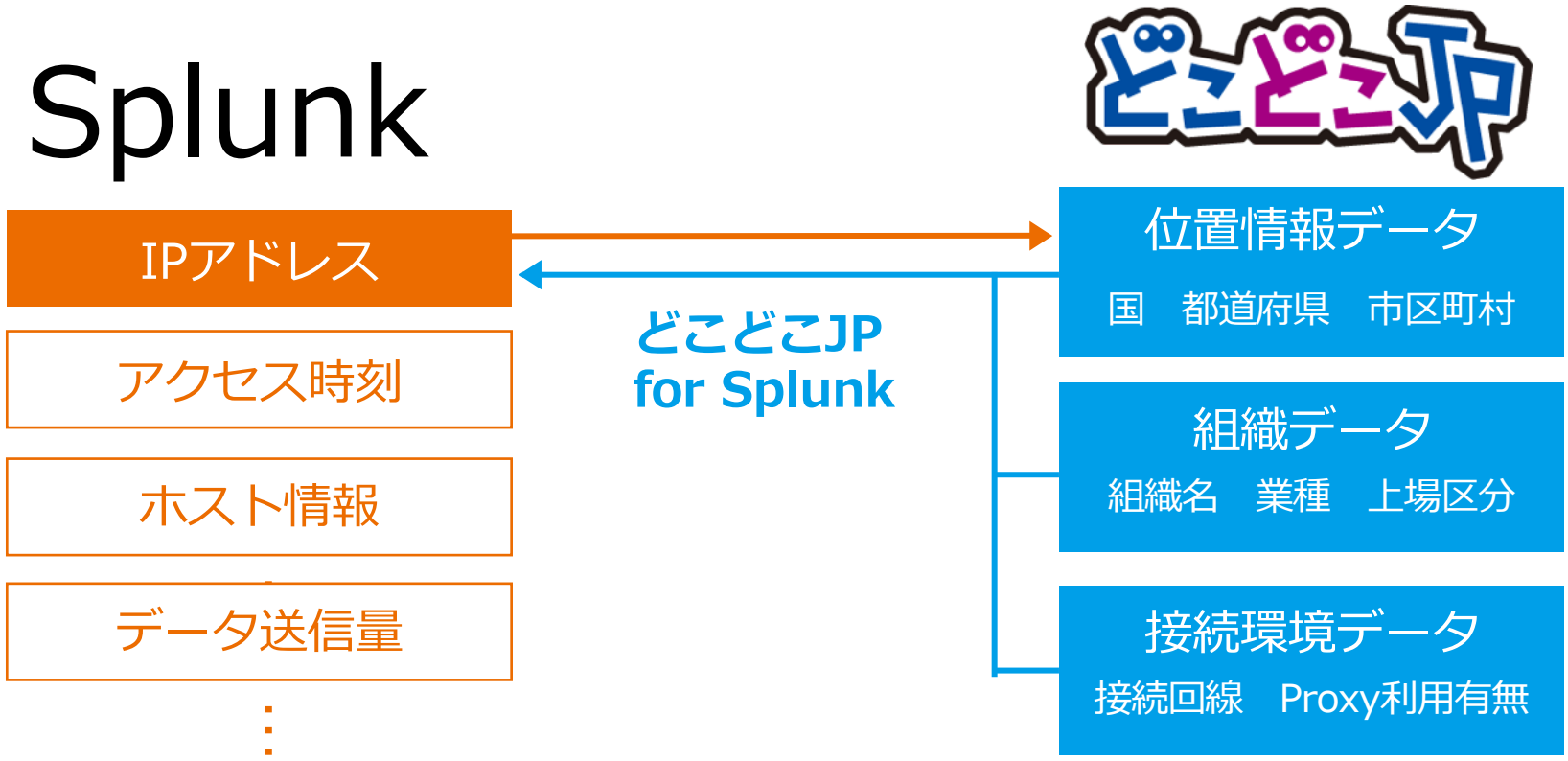
もっと遠くに、もっと近くに。
Geolocation Technology

位置情報データ　組織データ　環境データ　匿名ネットワーク属性データ*　AS番号関連データ**　国勢調査データ**　気象データ*　*…有償オプション
刑法犯データ**　事業所数データ**　ドメイン検索機能*　平均年収データ**　タグトラッキングデータ*　IP Threatデータ*　**…無償オプション

大陸 コード	国 コード	国名（日本語表記）	国名（英語表記）	地方 コード	第一行政区画コード	第一行政区画日本語表記
第一行政区画英語表記	第一行政区画緯度	第一行政区画経度	第一行政区画CF値	第二行政区画コード	第二行政区画日本語表記	第二行政区画英語表記
第二行政区画緯度	第二行政区画経度	第二行政区画CF値	組織名 日本語表記	BCフラグ	企業コード	組織名 英語表記
本支店フラグ	自営業フラグ	組織 都道府県コード	組織 市区町村コード	組織 緯度	組織 経度	組織 郵便番号
組織住所 日本語表記	組織住所 英語表記	組織 電話番号	組織 FAX番号	市外局番	組織 URL	組織　ドメイン名
組織 ドメイン種別	上場区分	証券コード	設立年月日	資本金コード	従業員数コード	売上高コード
代表者氏名	業種コード大分類	業種コード中分類	業種コード小分類	業種コード細分類	法人番号関連データ更新日	法人番号
商号または名称 （法人番号に基づく）	本社所在地 （法人番号に基づく）	IPアドレス	ドメイン名（IPに基づく）	回線種別コード	回線種別 日本語表記	回線種別 英語表記
IPアドレスを 暗号化した文字列	タイムゾーン	回線種別CF値	Proxyフラグ	匿名ネットワーク サービス属性	匿名ネットワーク属性 サービスの危険度	匿名ネットワーク属性 付属情報
AS番号	AS番号保有組織	人口	人口増減率	人口密度	世帯数	世帯増減率
今日の天気（今夜の天気）	気象予報情報更新日時	予報最高気温（℃）	今日の最高気温（℃）	明日の天気	明後日の天気	今日の天気テロップ番号
明日の天気テロップ番号	明後日の天気テロップ番号	明日の最低気温コード	今日の降水確率（%）	明日の最高気温（℃）	明日の最低気温（℃）	予報最高気温コード
今日の最高気温コード	明日の最高気温コード	明日の降水確率（%）	今日の風向き （今夜の風向き）	明日の風向き	気象現況情報更新日時	現況の天気
現況の天気コード番号	現況の気温（℃）	現況の気温コード	現況の湿度（%）	現況の降水（mm/h）	今日の紫外線強さ予報	認知件数
認知件数順位	認知件数増減率	認知件数の全体に占める割合	検挙件数	検挙件数順位	検挙件数増減率	検挙件数の全体に占める割合
検挙率	業種中分類別事業所割合	業種中分類別事業所数	フリーメール判定	フリーメール名	フリーメール運営組織名	ドメイン検索ISPメール判定
全体平均年収	全体国内平均との差	男性平均年収	男性国内平均との差	女性平均年収	女性国内平均との差	
カテゴリID	サービスID	HTTPアラートフィード （マルウェア通信先）	HTTPブロックフィード （マルウェア通信先）	フィッシングフィード		

どこどこJPとSplunkの連携で実現すること

Splunkに格納されたIPアドレスデータに対し、位置情報データ、企業データ、接続環境データなどを付与することで、IPアドレス情報を詳細に可視化することが可能。
インターネットを通じてサービスを提供する企業に対し、Webトランザクションの分析・運用業務の効率化とセキュリティ向上に役立つデータを可視化します。

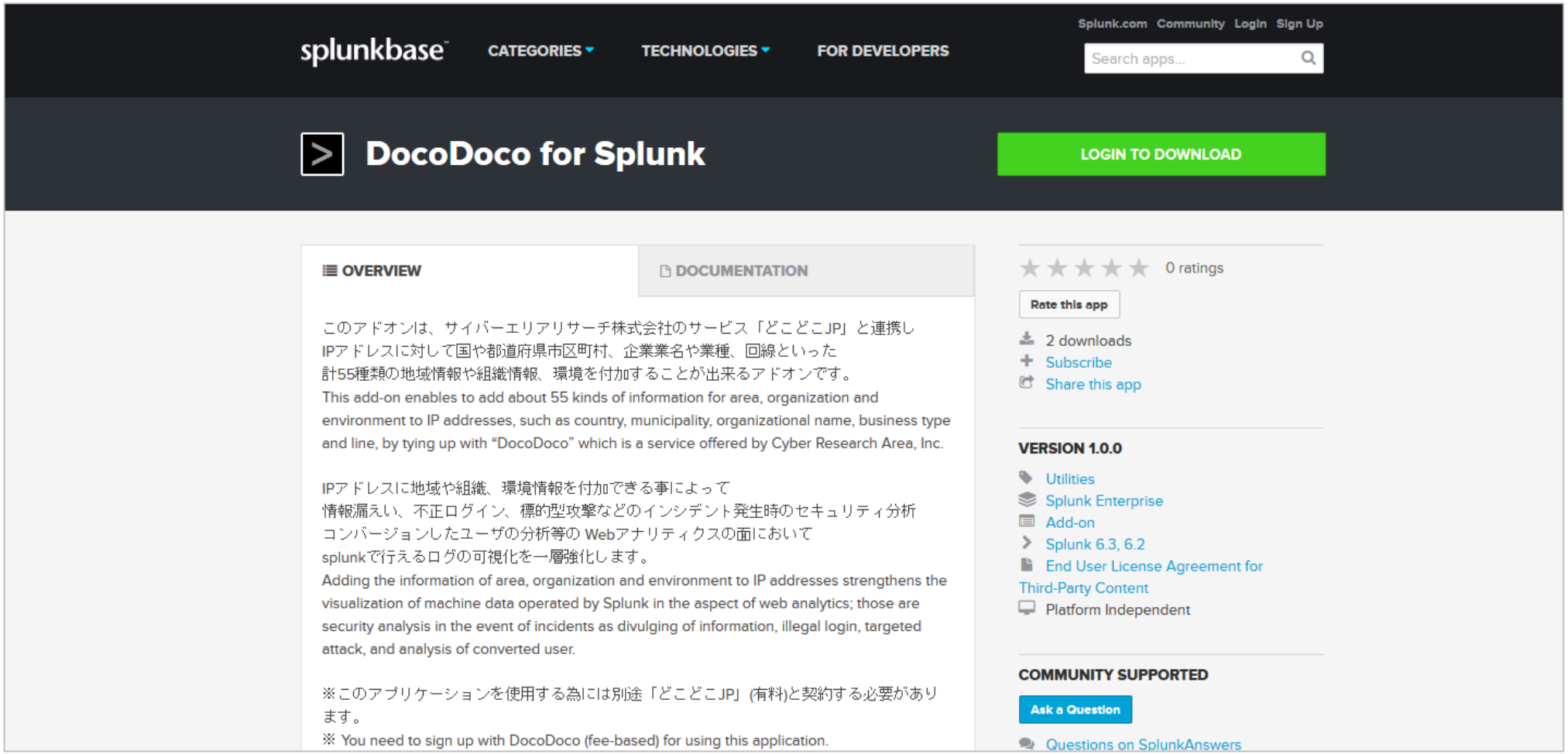


※上記の項目は取得可能なデータの一例です。

分析前準備：①連携アプリケーションの取得

もっと遠くに、もっと近くに。
Geolocation Technology

アプリケーションを、Splunkbase上のどこどこJP for Splunkページ（https://splunkbase.splunk.com/app/3078/）よりダウンロード。



https://splunkbase.splunk.com/app/3078

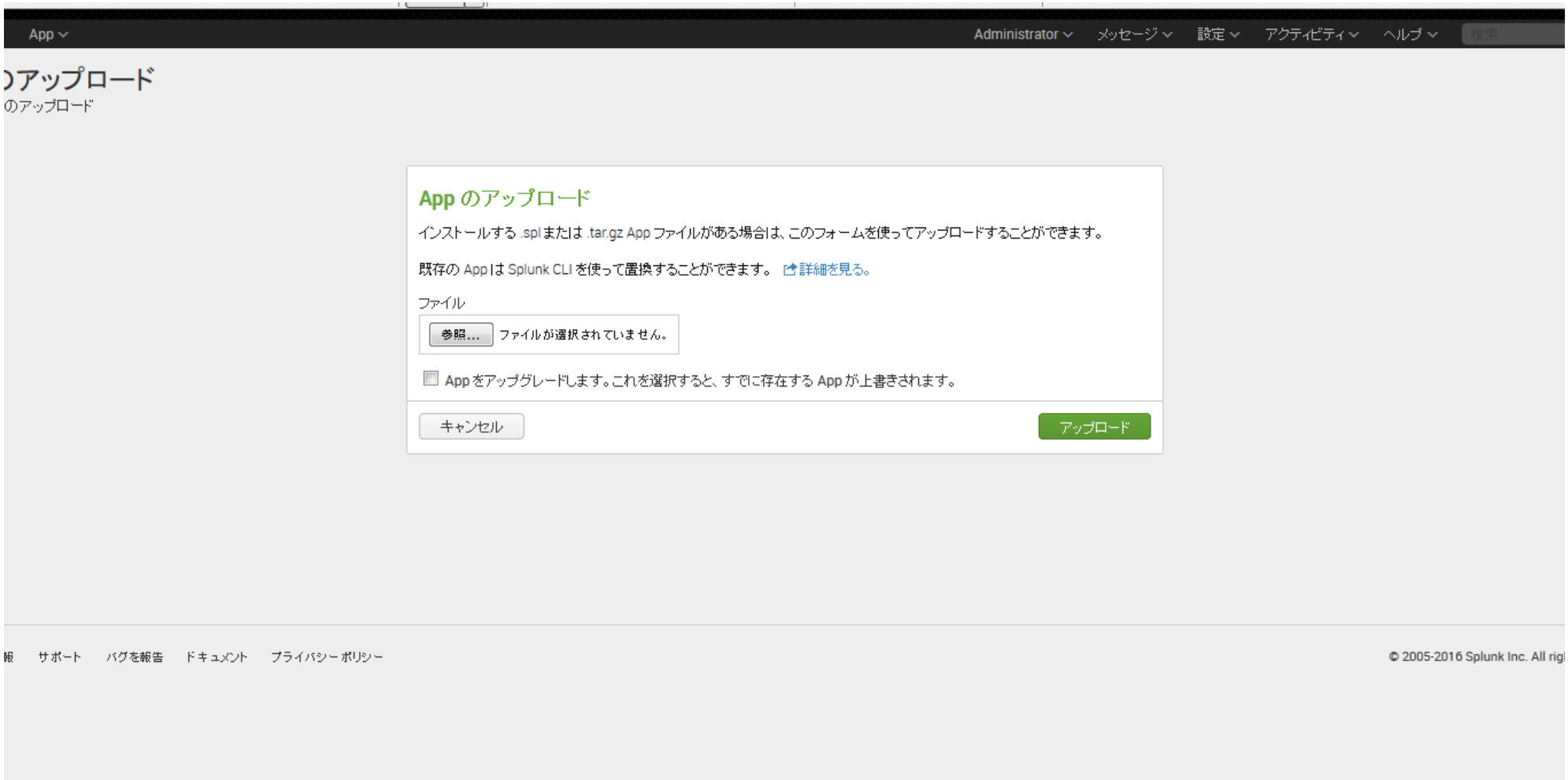
分析前準備：②どこどこJPのAPIキー取得

どこどこJPのご利用登録画面（https://admin.docodoco.jp/signup/）より、新規ご利用登録してAPIキーを取得。
http://www.docodoco.jp/block/howto.html
※APIキー2が表示されない場合は、サポート窓口に連絡。

分析前準備：③アプリケーションのアップロード

もっと遠くに、もっと近くに。
Geolocation Technology

①でダウンロードした「どこどこJP for Splunk」のファイルを、「Appのアップロード」よりアップロード。



分析前準備：④APIキーの設定

Appのインストールが完了したら、
「$SPLUNK_HOME$¥etc¥apps¥docodoco/bin/config.ini」ファイル中の
「key1」「key2」に、②で取得したAPIキー1、APIキー2を書き込む。
「count」は、どこどこJPの並列リクエスト数を設定。自社の環境に合わせて
変更してください。

```
[docodoco]
key1 =
key2 =

[process]
count = 10
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
```

利用例①アクセス数の多いIPアドレスの情報を表示

もっと遠くに、もっと近くに。 Geolocation Technology

データ中に重複の多いIPアドレスを抽出し、データを付与。ログデータから、アクセス数が不自然に多いなど、攻撃的なアクセスが疑われるIPアドレスを発見し、より詳細な情報を得ることができます。

例：アクセス数上位100位までのIPアドレスを抽出し、IPアドレスから判定できる情報を表示

```
top limit=100 clientip | lookup docodoco ipaddr as clientip
```

clientip	count	percent	BCFlag	CityAName	CityCF	CityCode	CityJName	CityLatitude	CityLongitude	ContinentCode	CountryAName	CountryCode	CountryJName	DomainName	Do
210.251.250.30	3597	0.261061	b	kumamoto-shi chuo-ku	55	43101	熊本市中央区	32.80308	130.70790	3	Japan	JP	日本	arearesearch.co.jp	.co
59.84.175.173	2002	0.145300		shizuoka-shi	30	22100	静岡市	34.97520	138.38333	3	Japan	JP	日本	arearesearch.co.jp	.co
68.180.229.229	1888	0.137026	b	sunnyvale	20	US-CA77000		38.89715	-77.03620	1	United States	US	アメリカ合衆国		
17.138.55.240	1761	0.127809	b	washington	0	US-DC50000	ワシントンd.c.	38.89715	-77.03620	1	United States	US	アメリカ合衆国		
17.138.55.109	1570	0.113946	b	washington	0	US-DC50000	ワシントンd.c.	38.89715	-77.03620	1	United States	US	アメリカ合衆国		
210.160.194.73	1516	0.110027		yokohama-shi	14	14100	横浜市	35.44318	139.63734	3	Japan	JP	日本		
202.246.252.97	1349	0.097907	b	sendai-shi	14	04100	仙台市	38.26794	140.86953	3	Japan	JP	日本	hitachi.co.jp	.co
59.106.108.116	1067	0.077440	b	shibuya-ku	29	13113	渋谷区	35.66404	139.69787	3	Japan	JP	日本	hatena.ne.jp	.ne
202.246.252.102	984	0.071416	b	chiba-shi	14	12100	千葉市	35.60771	140.10644	3	Japan	JP	日本	hitachi.co.jp	.co

利用例②アクセス元地域のプロット

もっと遠くに、もっと近くに。
Geolocation Technology

抽出したIPアドレスの位置情報をマップ上にプロット。円の大きさで、
IPアドレス数のボリュームを表します。

例：アクセス数上位100位までのIPアドレスに対し、市区町村単位の位置情報を判定

```
top limit=100 clientip | lookup docodoco ipaddr as clientip | geostats latfield=CityLatitude longfield=CityLongitude count
```

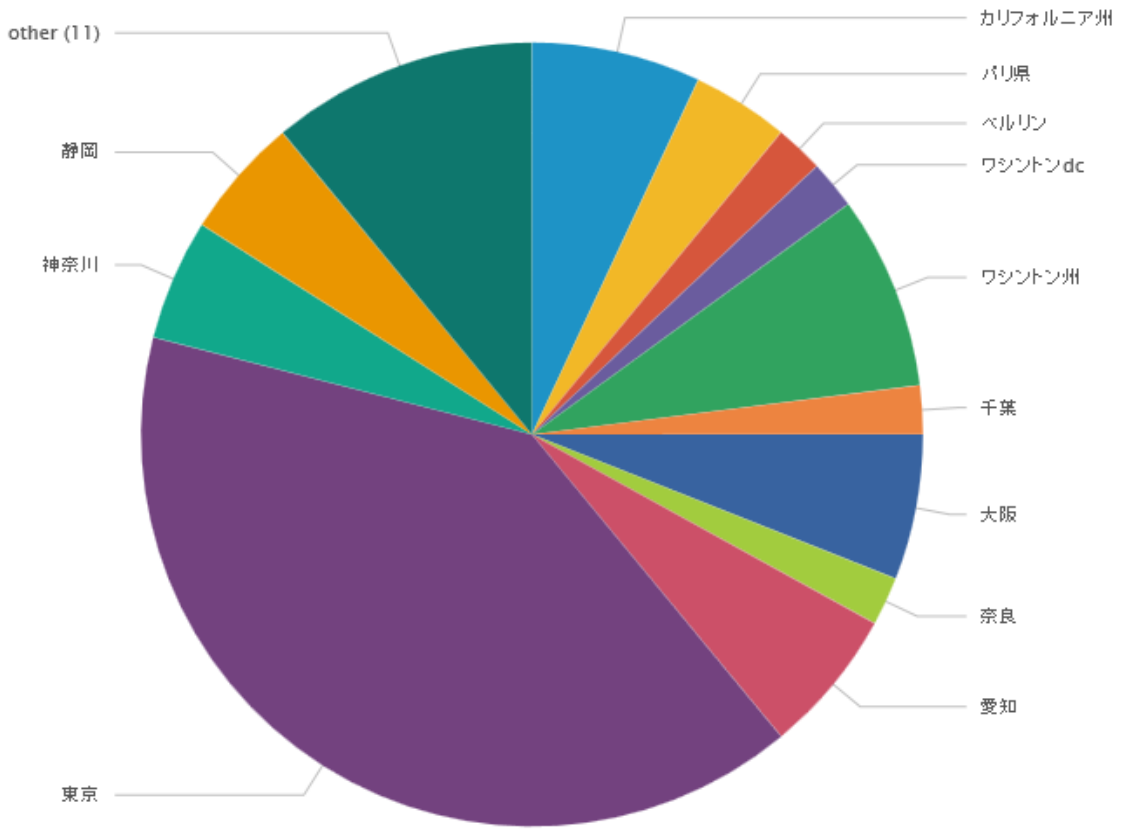
利用例③アクセス元地域の構成割合を可視化

もっと遠くに、もっと近くに。
Geolocation Technology

抽出したIPアドレスの位置情報をもとに、都道府県ごとの構成割合を算出

例：アクセス数上位100位までのIPアドレスに対し、都道府県単位の位置情報を判定

```
top limit=100 clientip  | lookup docodoco ipaddr as clientip |stats count by PrefJName
```



利用例④攻撃的なアクセスのIPアドレスを分析

もっと遠くに、もっと近くに。
Geolocation Technology

攻撃的なアクセスや不正なアクセスの可能性があるIPアドレスを抽出し、IPアドレスから判定した情報を付与。
アクセス元の国・地域や、公開プロキシサーバを利用したアクセスかどうかなど、分析・対策立案に有用な情報が得られます。

サーバログ

⚠	**集中的なアクセス**	IPアドレス **203.0.113.30**
⚠	**不正が疑われるアクセス**	IPアドレス **198.51.100.250**

＋

国・地域

アクセス元の国や地域を特定し、アクセス制限等の対策に生かすことができます。

ドメイン名

アクセス元が利用しているISPの情報を得ることができます。

プロキシサーバ利用有無

プロキシサーバを経由したアクセスか否かを判定することができます。

利用例⑤VPNへの接続ログを分析

もっと遠くに、もっと近くに。
Geolocation Technology

VPNの接続ログに含まれるIPアドレスに対し情報を付与。
位置情報、接続環境などの情報から、想定される利用用途と異なる不審なアクセスを発見することができます。

VPNサーバ

アクセス時刻	ログイン情報	IPアドレス
2016/02/01 10：00	**ID・パスワード ログイン成功**	**203.0.113.30**

＋

国・地域

国外からのアクセスなど、不審なアクセスを検知することができます。

ドメイン名

アクセス元が利用しているISPの情報を得ることができます。

プロキシサーバ利用有無

プロキシサーバを経由したアクセスか否かを判定することができます。

利用例⑥なりすまし・不正利用の発見

もっと遠くに、もっと近くに。
Geolocation Technology

ネットバンキング等のアクセスログに含まれるIPアドレスに対し情報を付与。
IPアドレスから取得できる情報を分析することにより、不正利用が疑われるアカウントを発見できます。

例1 なりすましログインが疑われるアクセス

普段と大きく異なる環境からのアクセスや、不自然なアクセス元位置の変化は、本来のユーザと異なる第三者によるなりすましの可能性が考えられます。

ログイン時刻	口座番号	IPアドレス	位置情報	回線種別
2016/02/01 10:00	A123-456-789	203.0.113.250	東京都	FTTH
2016/02/03 12:00	A123-456-789	203.0.113.250	東京都	FTTH
2016/02/03 12:15	A123-456-789	198.51.100.5	北海道	CATV

例2 複数アカウントの利用が疑われるアクセス

同一人物による複数口座の開設を認めていないサービスでは、複数口座へ同一IPアドレスから複数の口座へアクセスがある場合、不正利用の可能性が考えられます。

ログイン時刻	口座番号	IPアドレス	位置情報	回線種別
2016/02/01 10:00	A123-456-789	203.0.113.250	東京都	FTTH
2016/02/01 11:00	Z111-222-333	203.0.113.250	東京都	FTTH
2016/02/01 12:00	M009-008-007	203.0.113.250	東京都	FTTH

利用例⑦製品ページにアクセスした企業の情報を表示

もっと遠くにも近くに。Geolocation Technology セキュリティ以外にも

製品ページ（サンプルでは/product/index.html）にアクセスした企業ユーザを抽出し、企業情報を付与。Webサイトに訪問し、情報収集をしている見込み顧客の発見・分析に役立つ情報が得られます。
競合企業のアクセスがある場合には、どのような情報を閲覧しているかなど、競合の動向分析にもお役立ていただけます。

例：製品ページにアクセスしたユーザのIPアドレスに対し、企業名・本社所在地などの企業情報を判定

```
uri="/product/index.html" | stats count by clientip | lookup docodoco ipaddr as clientip output OrgName OrgPrefCode OrgCityCode OrgZipCode OrgAddress OrgTel OrgFax StockTickerNumber OrgDate OrgPresident OrgIndustrialCategoryL OrgUrl OrgDomainName DomainType BCFlag | search BCFlag=b | sort -count
```

OrgCityCode	OrgDate	OrgDomainName	OrgFax	OrgIndustrialCategoryL	OrgName	OrgPrefCode	OrgPresident	OrgTel	OrgUrl	OrgZipCode
13103	194110	[redacted]	[redacted]	I	[redacted]株式会社	13	[redacted]	03-3455-8811	http://[redacted]	108-0073
27127	198612	[redacted]	[redacted]	E	株式会社[redacted]	27	[redacted]	06-6346-2800	http://www.[redacted]	530-0001
13101	19660105	[redacted]		G	株式会社[redacted]研究所	13	[redacted]	03-5533-2111	http://[redacted]	100-0005
13102	194511	[redacted]		G	株式会社[redacted]	13	[redacted]	03-6800-1111	http://www.[redacted]	104-0061
13101	19200201	[redacted]		E	株式会社[redacted]	13	[redacted]	03-3258-1111	http://www.[redacted]	100-8280
13103	199108	[redacted]	[redacted]	L,O	株式会社[redacted]	13	[redacted]	03-6253-8000	http://www.[redacted]	105-0021
13101		[redacted]	[redacted]	K,L	株式会社[redacted]	13		03-5282-8000	http://www.[redacted]	101-0052

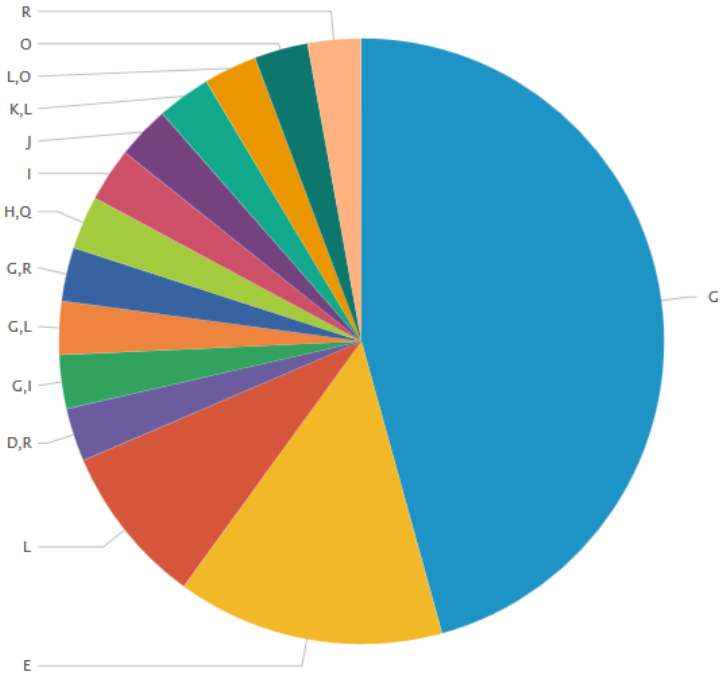
利用例⑧アクセスした企業の業種構成割合を可視化

もっと遠くにも近くに。Geolocation Technology セキュリティ以外にも

製品ページ（サンプルでは/product/index.html）にアクセスした企業ユーザを抽出し、業種大分類ごとの構成割合を算出。
Webサイトを閲覧している企業の傾向を把握することにより、ターゲットとする業種をWebサイトに呼び込めているかを判断し、Webコンテンツの改善・拡充につなげることができます。

例：製品ページにアクセスした企業ユーザのIPアドレスに対し、業種大分類を判定

```
uri="/product/index.html" | stats count by clientip | lookup docodoco ipaddr as clientip output OrgIndustrialCategoryL BCFlag | search BCFlag=b | stats count by  OrgIndustrialCategoryL | sort -count
```



業種大分類　コード対応表

業種大分類コード	業種	業種大分類コード	業種
A	農業，林業	K	不動産業，物品賃貸業
B	漁業	L	学術研究，専門・技術サービス業
C	鉱業，採石業，砂利採取業	M	宿泊業，飲食サービス業
D	建設業	N	生活関連サービス業，娯楽業
E	製造業	O	教育，学習支援業
F	電気・ガス・熱供給・水道業	P	医療，福祉
G	情報通信業	Q	複合サービス事業
H	運輸業，郵便業	R	サービス業（他に分類されないもの）
I	卸売業，小売業	S	公務（他に分類されるものを除く）
J	金融業，保険業	T	分類不能の産業

利用例⑨コンバージョンしたユーザの分析

もっと遠くにも近くに。Geolocation Technology セキュリティ以外にも

コンバージョンページ（サンプルでは /inquiry/thanks.html ）にアクセスしたユーザのIPアドレスを抽出し、情報を付与します。
フォーム等で詳細な企業情報の入力を求めなくても、コンバージョンした企業を把握することができます。

例：コンバージョンページにアクセスしたIPアドレスに対し、位置情報と企業名を判定

```
uri="/inquiry/thanks.html" | stats count by clientip | lookup docodoco ipaddr as clientip output CountryJName PrefJName CityJName OrgName
```

clientip	count	CityJName	CountryJName	OrgName	PrefJName
1.72.2.183	1	新宿区	日本		東京
101.226.166.245	1	黄浦区	中華人民共和国		上海市
101.226.167.218	1	黄浦区	中華人民共和国		上海市
101.226.168.248	1	黄浦区	中華人民共和国		上海市
104.236.243.138	1		アメリカ合衆国	Digital Ocean, Inc.	アラバマ州
107.158.113.34	2		アメリカ合衆国	Eonix Corporation	アイオワ州
107.178.195.129	1		アメリカ合衆国		ヴァージニア州
114.191.84.219	1	岡山市	日本		岡山
118.238.210.154	1	新宿区	日本		東京
118.243.24.8	1	大阪市	日本		大阪
122.133.186.116	1	横浜市	日本		神奈川
122.21.142.112	1	福岡市	日本		福岡
124.41.77.163	3	朝来市	日本	株式会社インターネットレボリューション	兵庫
124.99.147.196	1	静岡市	日本		静岡
126.87.102.37	1	静岡市	日本		静岡

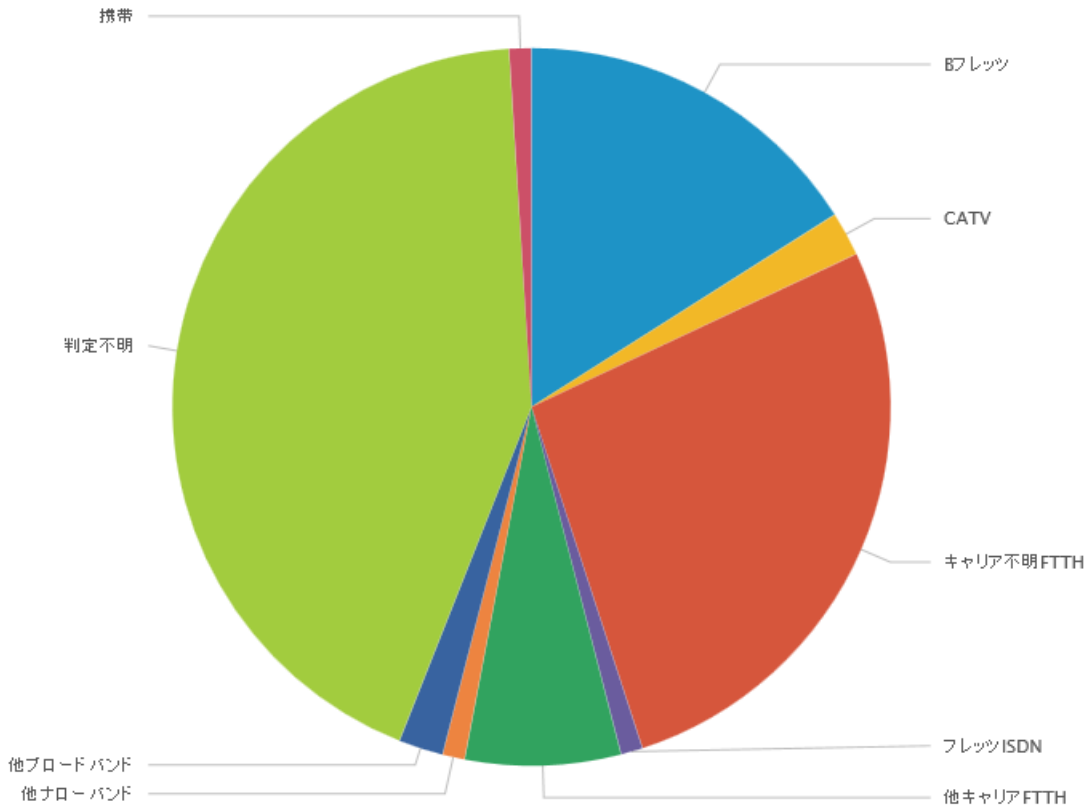
利用例⑩ユーザの利用回線種別を可視化

もっと遠くにも近くにも。Geolocation Technology セキュリティ以外にも

抽出したIPアドレスに対し、ユーザが接続に利用している回線種別の構成割合を算出します。

例：アクセス数上位100位までのIPアドレスに対し、回線種別を判定

```
top limit=100 clientip  | lookup docodoco ipaddr as clientip output LineJName | stats by LineJName | sort -count
```



IP Geolocationデータを使った調査・分析時に気をつけるべきこと

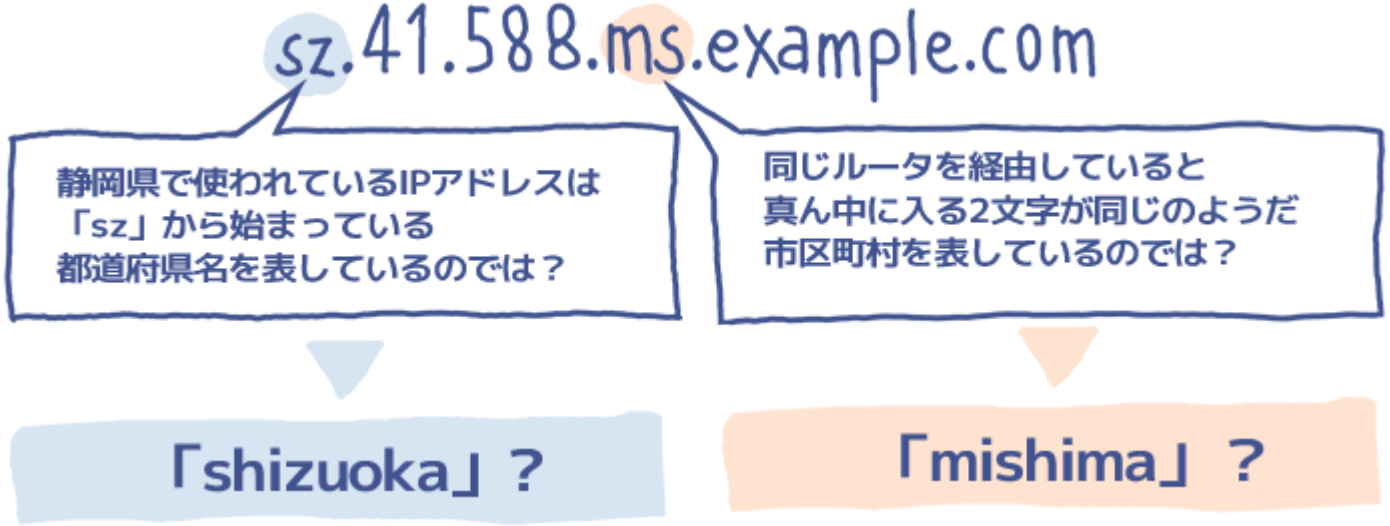
参考URL… https://www.geolocation.co.jp/learn/

①IP Geolocation DBの基本的な作り方を知る

もっと遠くに、もっと近くに。
Geolocation Technology

ホスト名から調査

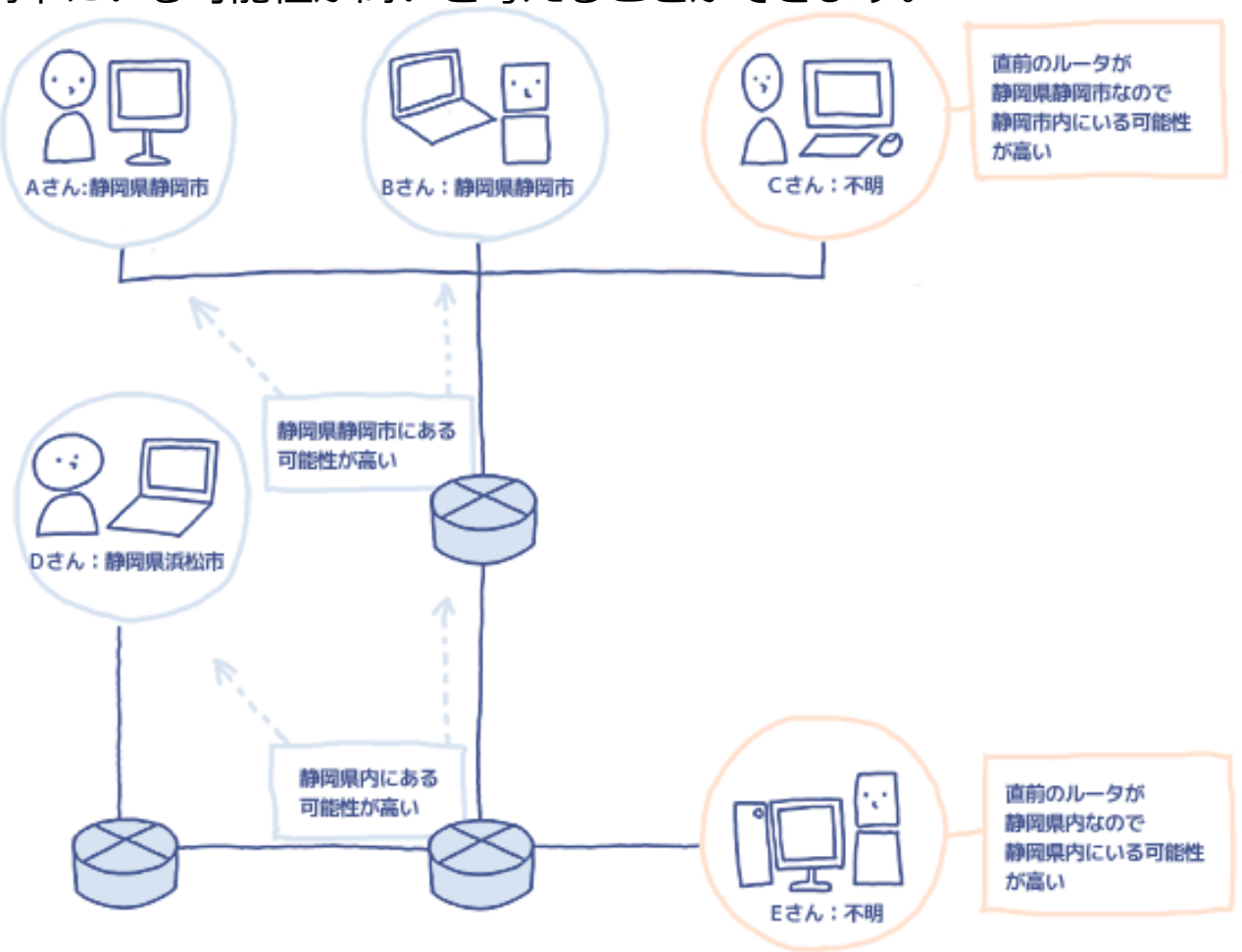
家庭用にインターネット環境を提供するISPが、どのようにIPアドレスを管理しているかを調査した結果、ISPによっては、ホスト名に地域名や地域コードなどの情報を含め、管理しやすくしている場合があります。これがIPアドレスと位置情報を紐づける手掛かりの一つとなっています。



とはいえ、ホスト名を見ただけでは、どの部分が手掛かりになるのかさえ分かりません。
そこで「おなじ文字列を含むホスト名が近い地域に集中している。市の名前とも符合するようだ」「この数字が県内で共通しているので、この数字が都道府県を表しているのかもしれない」など、ホスト名の中からキーワードとなる部分を推測し、仮説を立てます。
その上で、異なる分析手法を組み合わせ、仮説が正しいかどうかを検証します。 IPアドレス情報の調査には、ISPに対する深い知識が求められます。

ネットワーク機器の繋がりを分析する

ネットワーク機器の繋がりから推定する事ができます。例えば、トレースコマンドの結果より、
Cさんの直前ルータが静岡県静岡市と判定出来ているAさんBさんと同じだとわかった場合、
Cさんは静岡県静岡市にいる可能性が高いと考えることができます。



①IP Geolocation DBの基本的な作り方を知る

外部フィードバック情報を活用する

IPアドレスの情報は一度調べれば終わりではありません。IPアドレスは日々流動的に変化しているため、IPアドレスの位置情報もいつまでも調査したときと同じでいてくれるとは限らないのです。
そのため、IP Geolocationデータベースの品質を保つためには、継続した調査とデータ更新が必要不可欠となっています。
重要な情報源の１つに「サービスご利用者様（エンドユーザ）からのフィードバック」があります。
ホスト名からの調査やネットワーク機器の分析の際、判断するための材料として活用できます。

②IPアドレスの「行動範囲」に気をつける

もっと遠くに、もっと近くに。
Geolocation Technology

日本のネットワークは複雑です。
IPアドレスと位置情報の関係を考えるに際し、IPアドレスがどの範囲で使われるのかを意識することが重要です。

・市区町村内：固定IPアドレスサービス利用者、サービス提供範囲が市区町村内のCATV利用者。
・都道府県内：フレッツ利用者、
・日本国内　：４G、CGN利用者（アドレス共有）

当社では、CF(Confidence Factor)値という「確かさ」を示す弊社独自の指標で表しています。

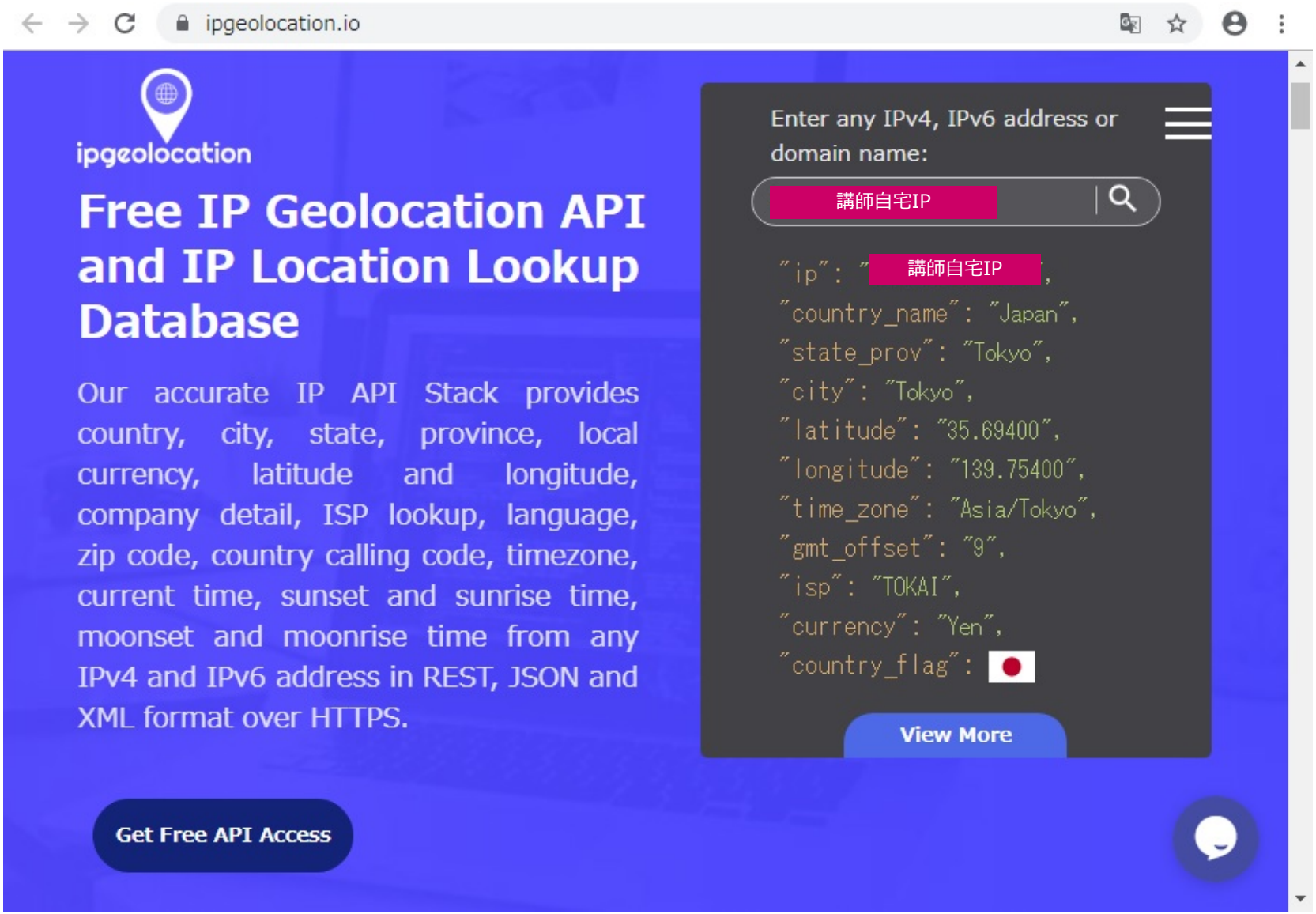
③国外のIP Geolocation DB問題

非公開

投影ONLY

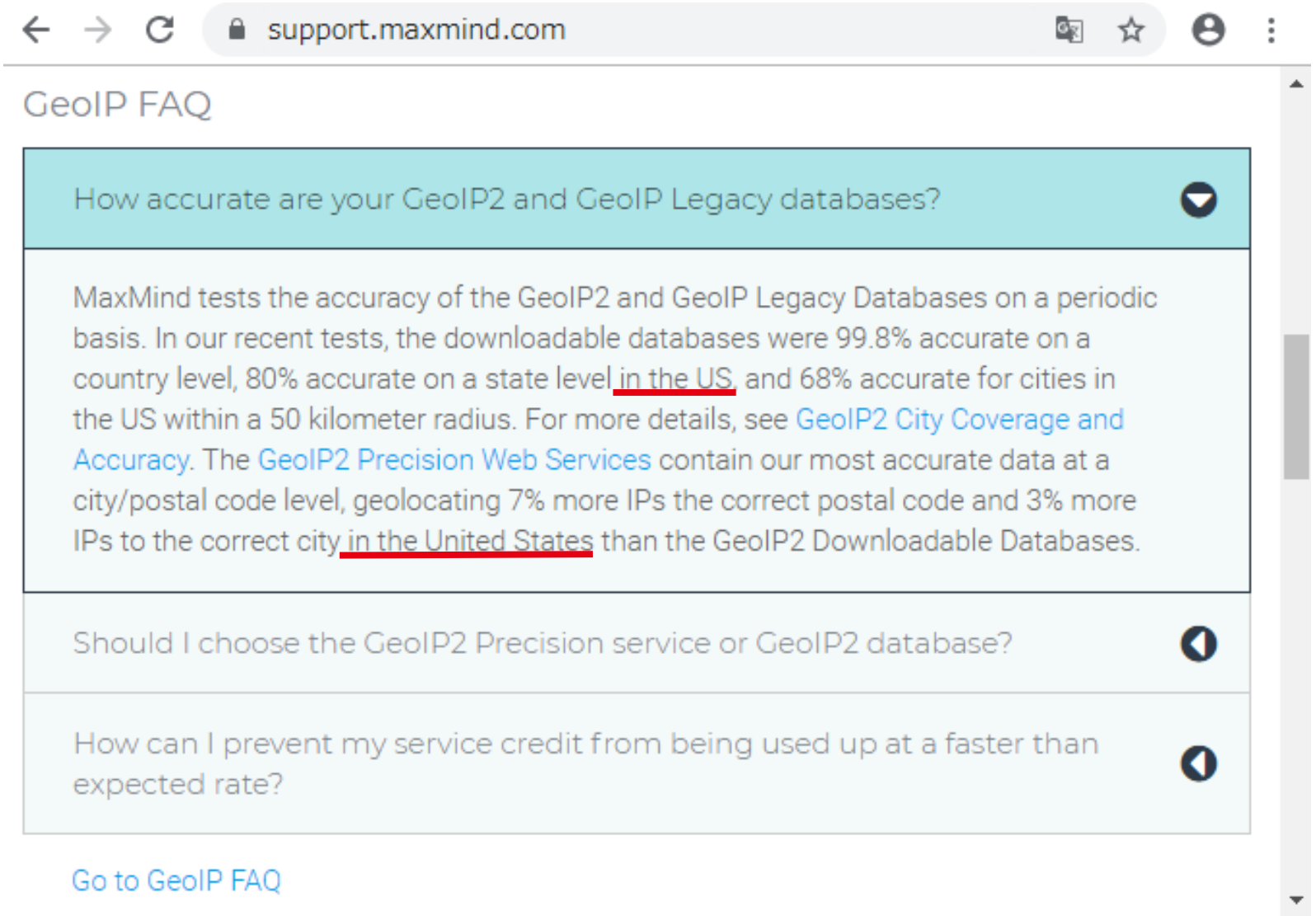
③国外のIP Geolocation DB問題

例：「静岡県駿東郡清水町」なのに国外のデータでは「Tokyo」となっている。



③国外のIP Geolocation DB問題

「確かさ」の基準がUSとなっている国外のIP Geolocation DB事業者。



IPv6の IP Geolocation DBに関する取り組み

もっと遠くに、もっと近くに。
Geolocation Technology

2019年4月に、NGN IPoE協議会が「IPv6国内地理情報共有ワーキンググループ」を発足。※参考URL：https://ipoe-c.jp/　assets　/pdf/20190424.pdf

NGN IPoE協議会

プレスリリース

2019 年 4 月 24 日
NGN IPoE 協議会

「IPv6 地理情報共有ワーキンググループ」の発足について

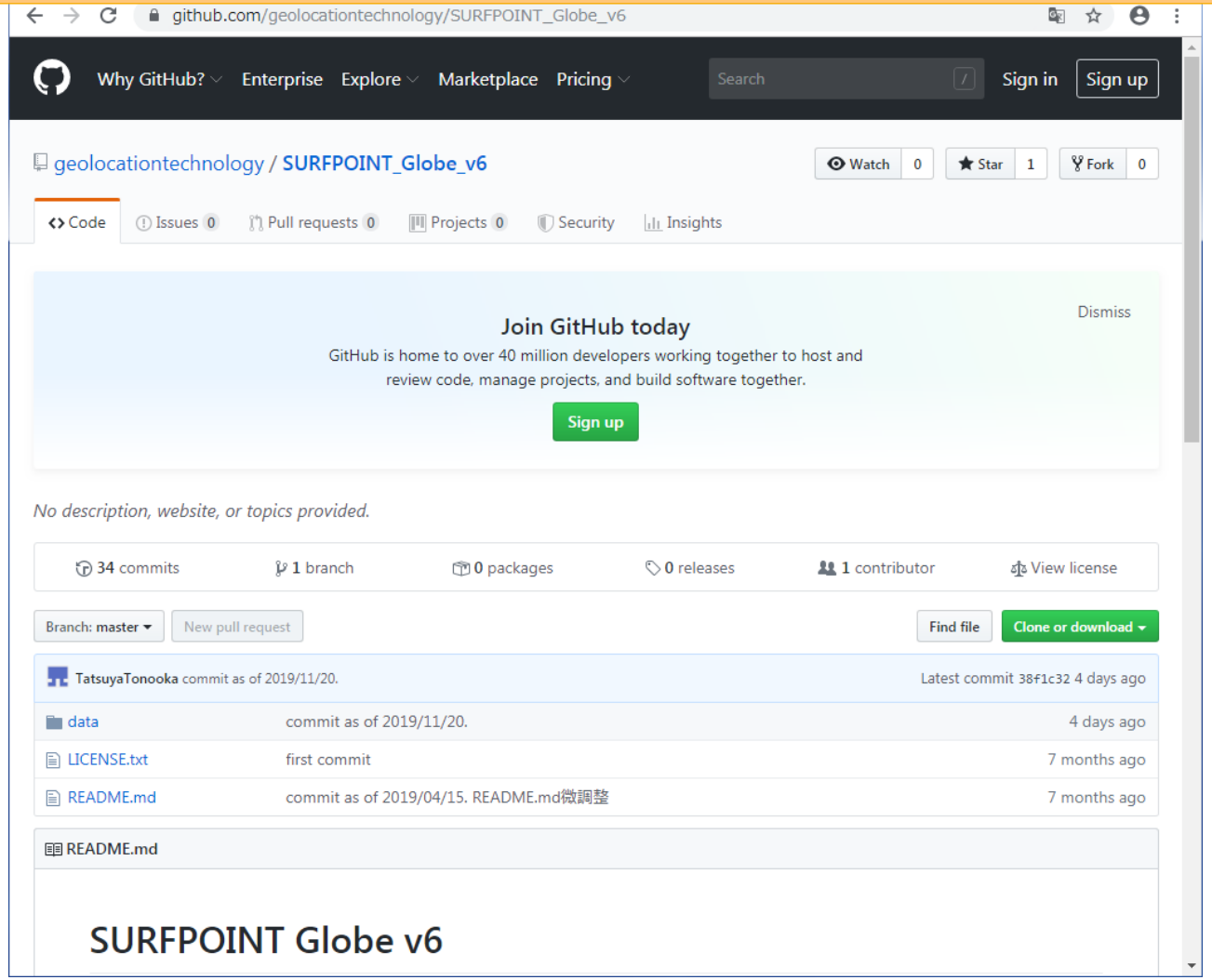
－IPv6 アドレスの更なる普及推進のため、都道府県単位での地理情報を
コンテンツ事業者と試験的に共有し、データ共有方式の検討や実証実験を実施－

NGN IPoE 協議会(会長：石田慶樹、以下 IPoE-C)は、2019 年 4 月、IPoE-C 内において IPv6 地理情報共有ワーキンググループ（以下 GeoIPv6 WG）を発足いたしました。
IPv6 普及・高度化推進協議会の調査によると、2018 年 12 月現在、東日本電信電話株式会社・西日本電信電話株式会社が提供する NGN 上での IPv6 の普及率は 57.8%となり、順調に普及が進んでいることが報告されています。またスマートフォンを利用したインターネット接続サービスにおいても主要キャリアでの IPv6 の導入が開始されており、今後ますます IPv6 の普及促進が見込まれています。
一方で国内コンテンツ事業者においては IPv6 の普及が同様に進んでいるとは必ずしもいえない状況にあります。この理由の一つとして、IPv4 で得られているアドレスに紐づく種々の情報が IPv6 では得られないからということがあります。その中でも地理情報が取得できないということが一つの大きな障壁となっています。

GeoIPv6 WG はこの課題に対処するために、IPv6 アクセス網の地理情報を国内コンテンツ事業者と共有し、IPv6 によるコンテンツ配信促進の一助とします。具体的には、フェ

IPv6の IP Geolocation DBに関する取り組み

2019年4月に、Geolocation TechnologyがIPv6版の国別データを
GitHubに公開。※参考URL：https://github.com/geolocationtechnology/SURFPOINT_Globe_v6



金融庁発表の
疑わしい取引の参考事例から

参考URL…　https://www.fsa.go.jp/str/jirei/

疑わしい取引の参考事例

もっと遠くに、もっと近くに。
Geolocation Technology

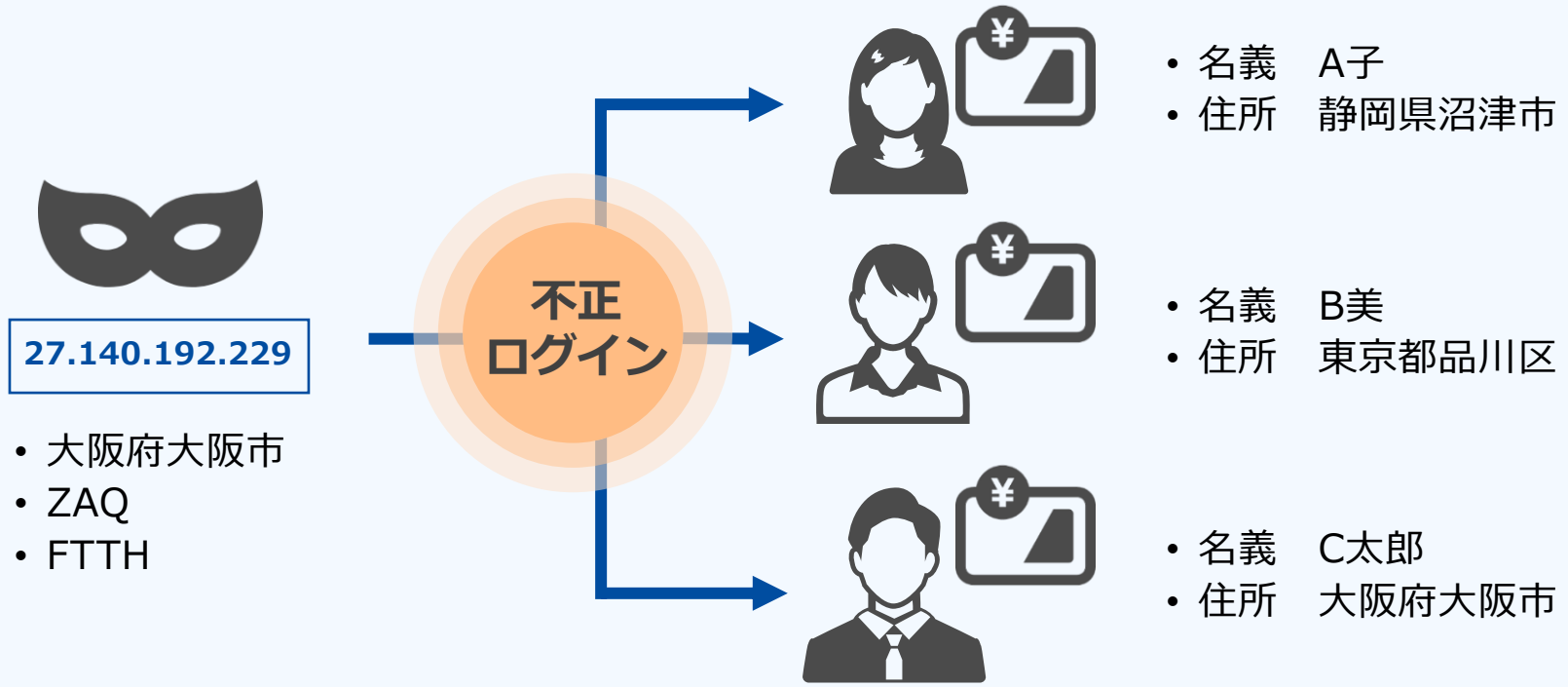
真の口座保有者を隠匿している可能性に着目した事例

- 名義・住所共に異なる顧客による取引にもかかわらず、同一のIPアドレスからアクセスされている取引。
- 国内居住の顧客であるにもかかわらず、ログイン時のIPアドレスが国外であることや、ブラウザ言語が[illegible]とに合理性が認められない取引。
- IPアドレスの追跡を困難にした取引。
- 取引時確認で取得した住所と操作している電子計算機のIPアドレス等とが異なる口座開設取引。

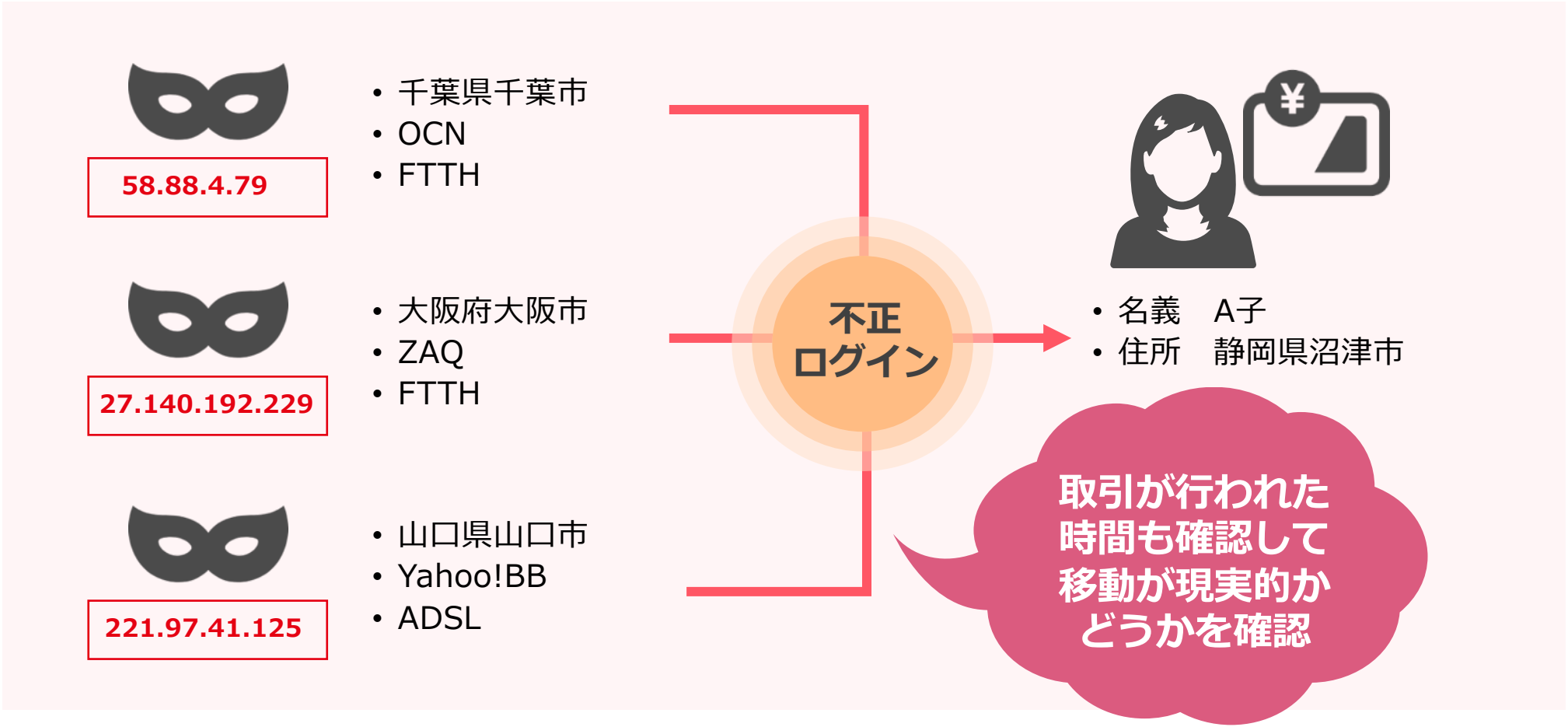
特に詳しく解説します！

名義・住所共に異なる顧客による取引にもかかわらず
同一のIPアドレスからアクセスされている取引

同一のIPアドレスから多数の口座へのログインが見られた場合、
疑わしい取引として注意する必要があります。

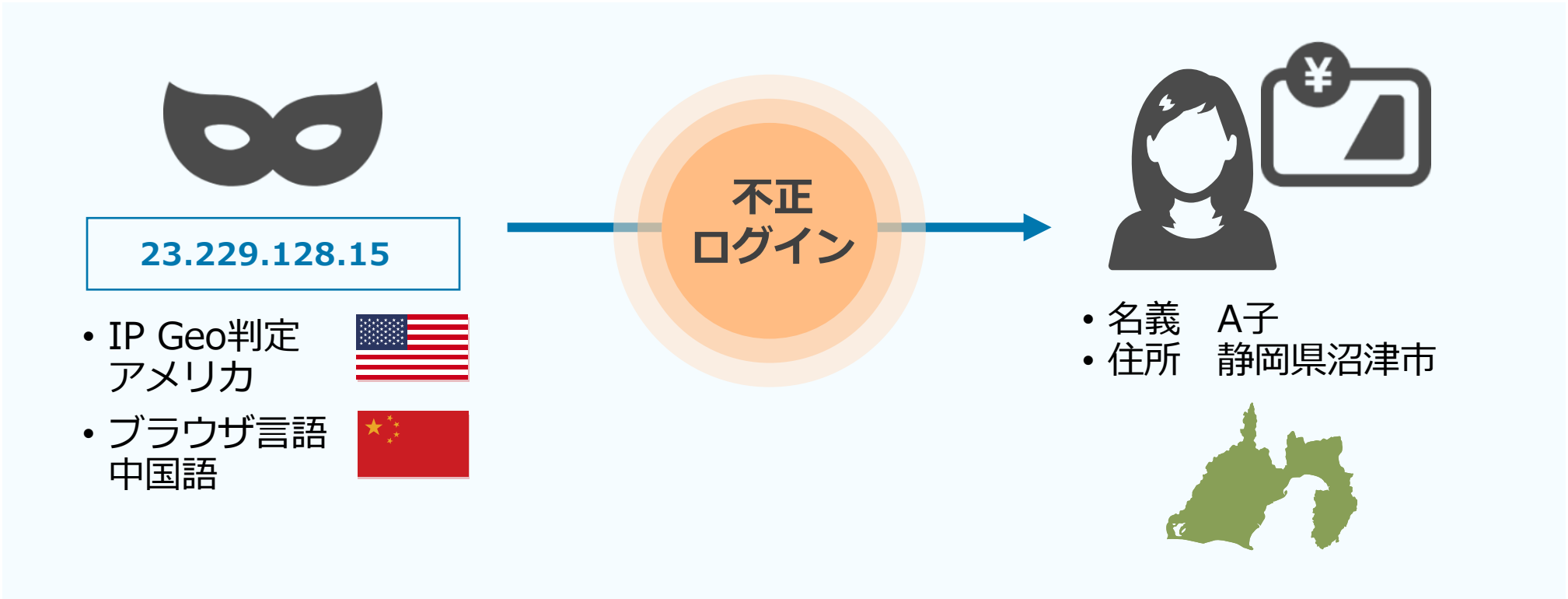


逆に、一つの口座に複数属性のIPアドレスからのログインが見られる場合も、
疑わしい取引として注意する必要があります。



国内居住の顧客であるにもかかわらず、
ログイン時のIPアドレスが国外であることや、
ブラウザ言語が外国語であることに
合理性が認められない取引

国内住居の顧客名義にもかかわらず、ログイン時のIPアドレスが
海外のIPアドレスや、ブラウザ言語が外国語の場合も、
疑わしい取引として注意する必要があります。



IPアドレスの「位置情報」について

IPアドレスの位置情報は、「IP Geolocation」を使って確認します。
IP Geolocationで確認できるIPアドレスの位置情報は以下の通りです。

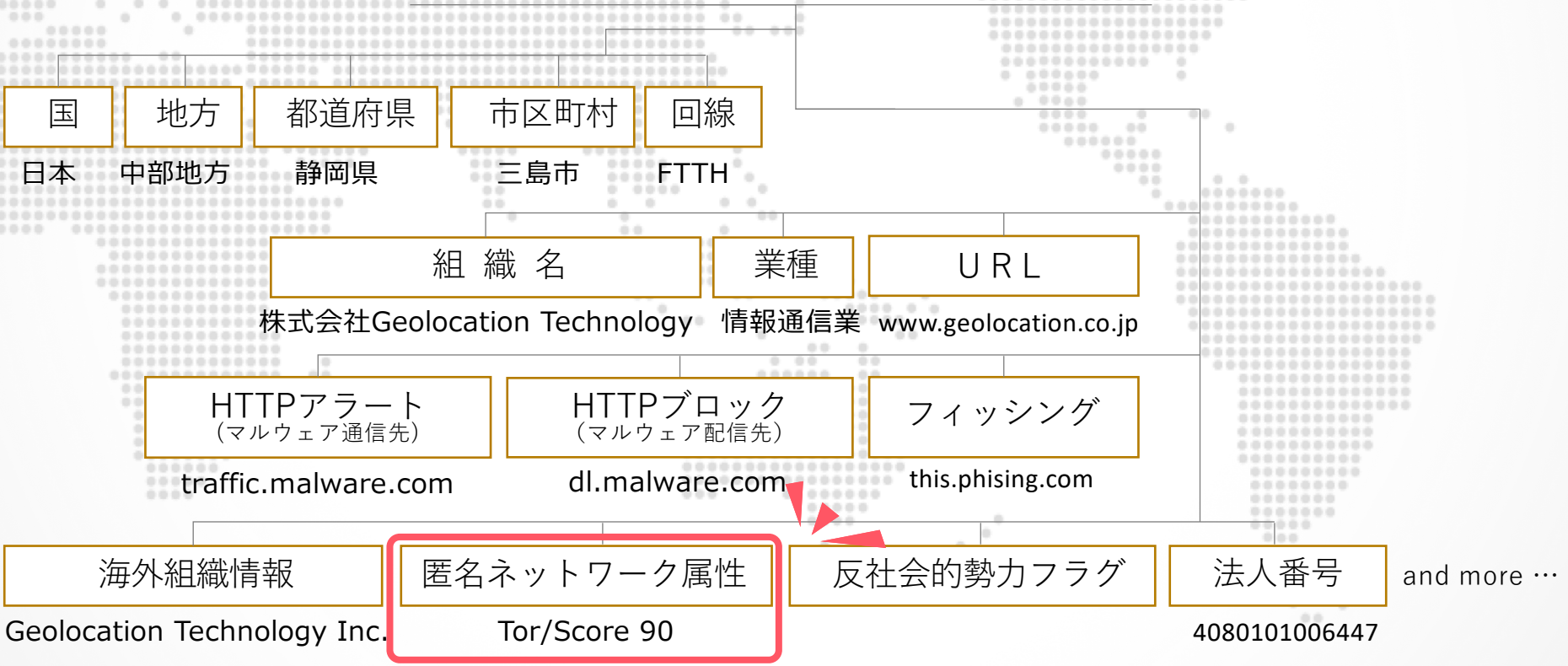
大陸 コード	国 コード	国名 （日本語表記）	国名 （英語表記）	地方 コード	第一行政区画 コード	第一行政区画 日本語表記
第一行政区画 英語表記	第一行政区画 緯度	第一行政区画 経度	第一行政区画 CF値	第二行政区画 コード	第二行政区画 日本語表記	第二行政区画 英語表記
第二行政区画 緯度	第二行政区画 経度	第二行政区画 CF値				

IP Geolocationとは？

もっと遠くに、もっと近くに。
Geolocation Technology

IPアドレスから導く情報は
多様なアプローチでセキュリティを強化します

210.251.250.30



IPアドレスの追跡を困難にした取引

IPアドレスの追跡を困難にする技術とツール

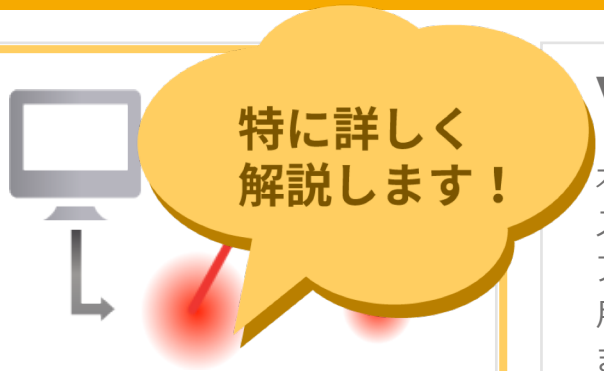
もっと遠くに、もっと近くに。
Geolocation Technology

匿名ネットワーク属性とは、通信元を秘匿化する技術やツールを使い、通信元をカムフラージュしたIPアドレスを判別するデータです。通信元を隠匿したアクセスは、違法・不法目的で使われる場合があり、オンライン取引におけるリスクと考えられます。

IP Geolocationで判別できる匿名ネットワークの種類

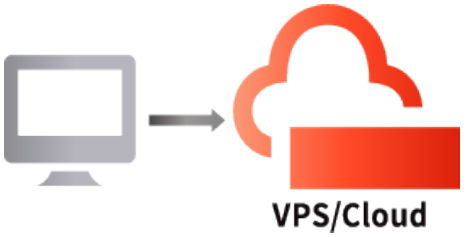
Tor（トーア）

「オニオンルーティング」と呼ばれる接続技術を使い、複数の機器を経由することによって接続経路を秘匿しています。



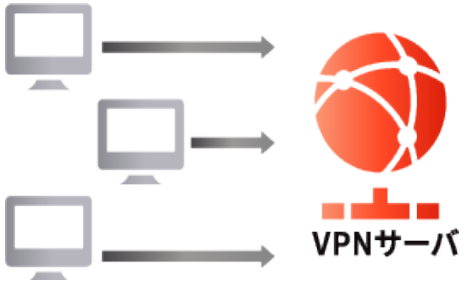
VPS/クラウド

本来はサーバーサービス等に使われますが、アクセス元の秘匿に利用される可能性もあります。



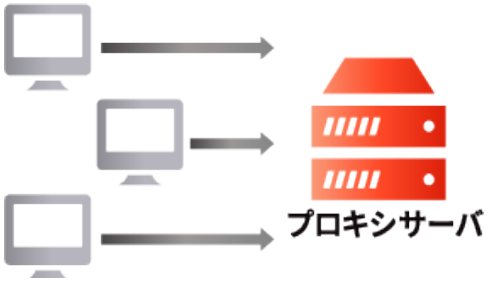
公開VPNサービス

一般に公開されているVPNサーバを経由してアクセスすることで、通信内容の暗号化とアクセス元の秘匿を行います。



プロキシサーバ

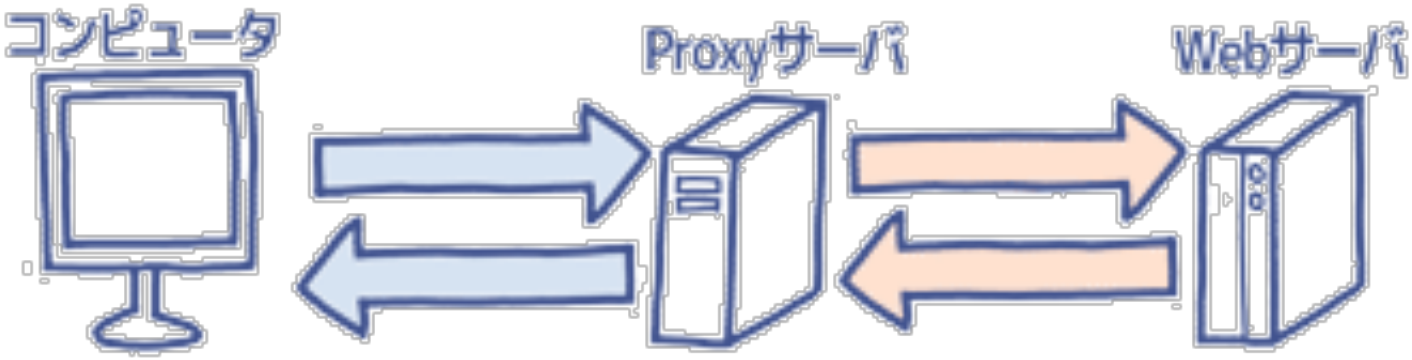
インターネット上に公開されている、接続を中継するためのサーバです。プロキシフラグに相当します。



プロキシサーバ(Proxy Server)とは

「Proxy」とは「代理」と言う意味を持ち、「プロキシサーバ」とは、その名の通り他のコンピュータの「代理」として他のサーバと通信するサーバの事を指します。
肩代わりする通信の種類により、HTTPプロキシ、FTPプロキシなどさまざまな種類がありますが、ここではHTTPプロキシのことを指します。

プロキシサーバを利用すると、ユーザのコンピュータはプロキシサーバにアクセスし、プロキシサーバが目的のWebサーバにアクセスします。
ちょうど、ユーザとWebサーバの間にプロキシサーバが入って中継しているような形になります。



IP Geolocation:静岡
210.251.250.30

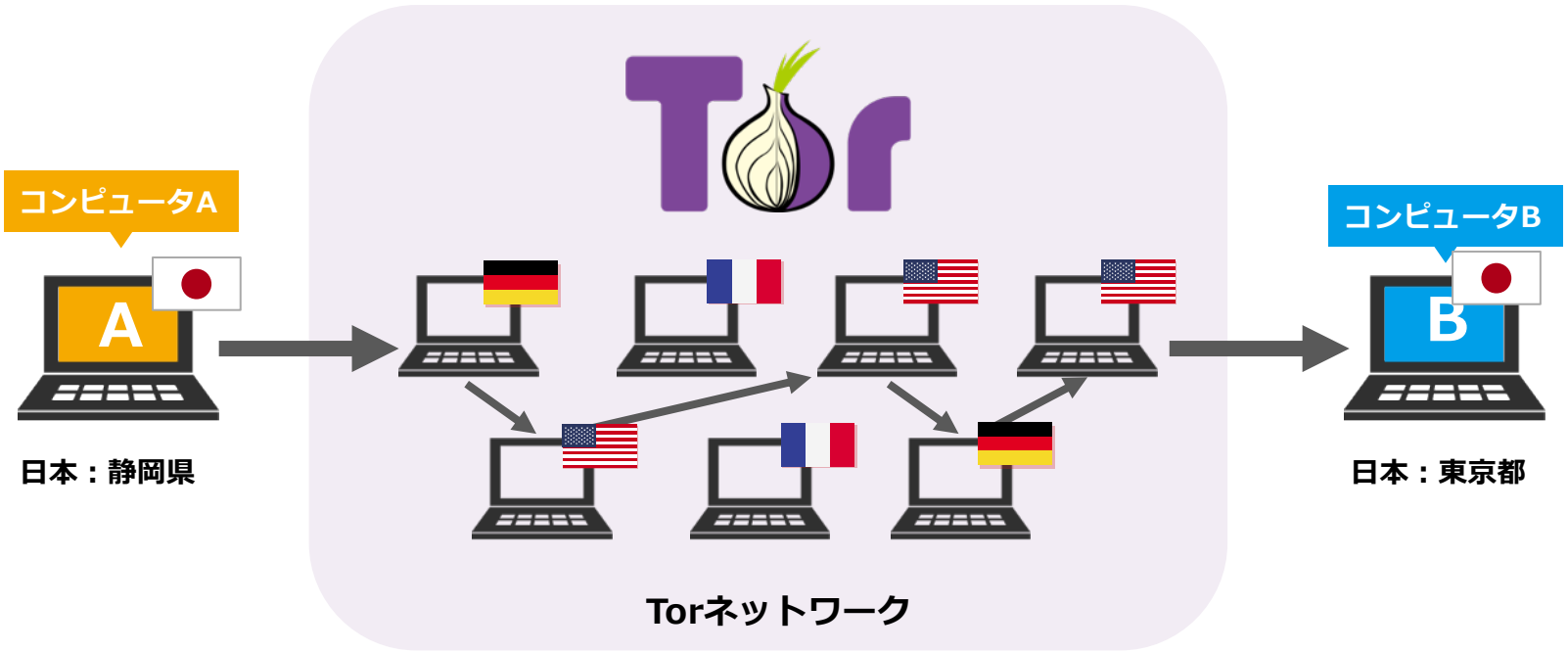
IP Geolocation:アメリカ
24.157.32.8

証券会社サイト

Torとは

Tor(The Onion Router)の概要

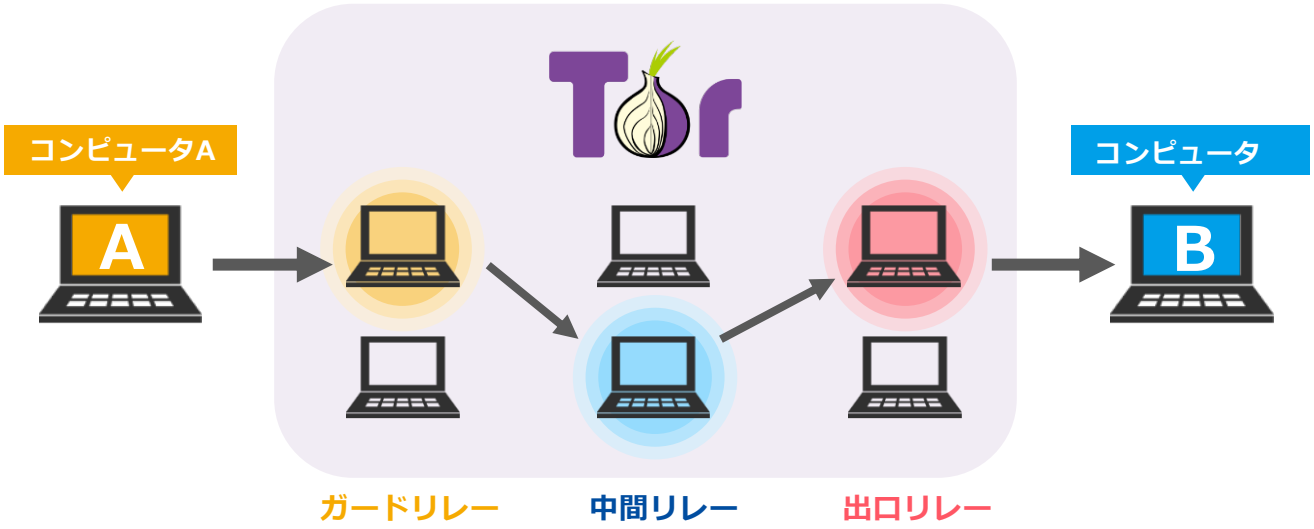
- 複数のノードを経由(リレー)する仮想回線接続（オニオンルーティング：タマネギの皮のように暗号化が積み重ねられることに由来）を用いて、通信元の接続経路を匿名化する技術
- 複数ノードを経由するため、本来の通信元にたどり着くことが困難



Torの仕組み

複数のノードで情報をリレーすることで、匿名性を高めている。

ガードリレー	Torネットワークの入り口のノード
中間リレー	ガードリレーから出口リレーへ中継するリレーするノード
出口リレー	Torネットワークの終端のノード。 出口リレーが最終的な目的地(PC等)にデータを配信する。



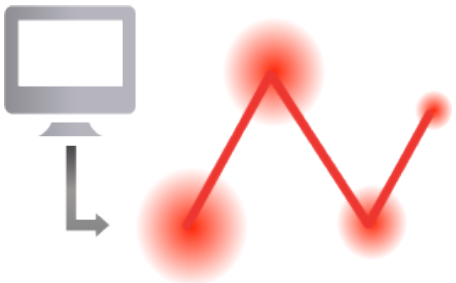
IP Geolocationの匿名ネットワーク属性

もっと遠くに、もっと近くに。
Geolocation Technology

IP Geolocationで判別できる匿名ネットワークの種類

Tor（トーア）

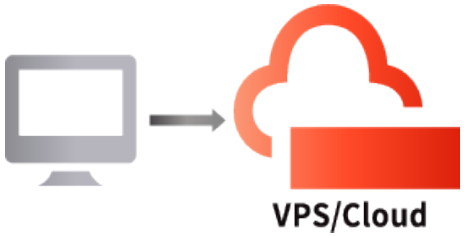
「オニオンルーティング」と呼ばれる接続技術を使い、複数の機器を経由することによって接続経路を秘匿しています。



16,988 IP

VPS/クラウド

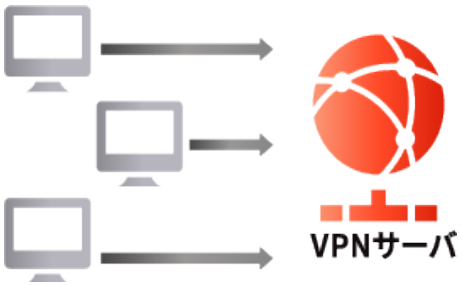
本来はサーバーサービス等に使われますが、アクセス元の秘匿に利用される可能性もあります。



85,634,164 IP

公開VPNサービス

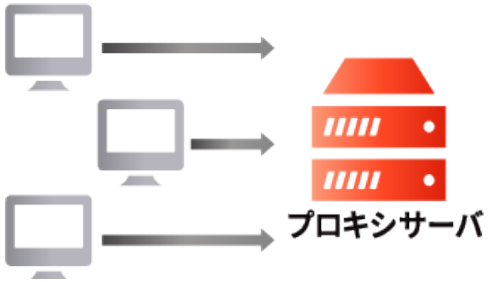
一般に公開されているVPNサーバを経由してアクセスすることで、通信内容の暗号化とアクセス元の秘匿を行います。



12,509 IP

プロキシサーバ

インターネット上に公開されている、接続を中継するためのサーバです。プロキシフラグに相当します。



11,131 IP

※2019年4月時点

当社データのサマリー(インターネット全体)

もっと遠くに、もっと近くに。
Geolocation Technology

Tor判定のIPアドレス数：約17,000
日々の調査による増減：300～400(約2%)

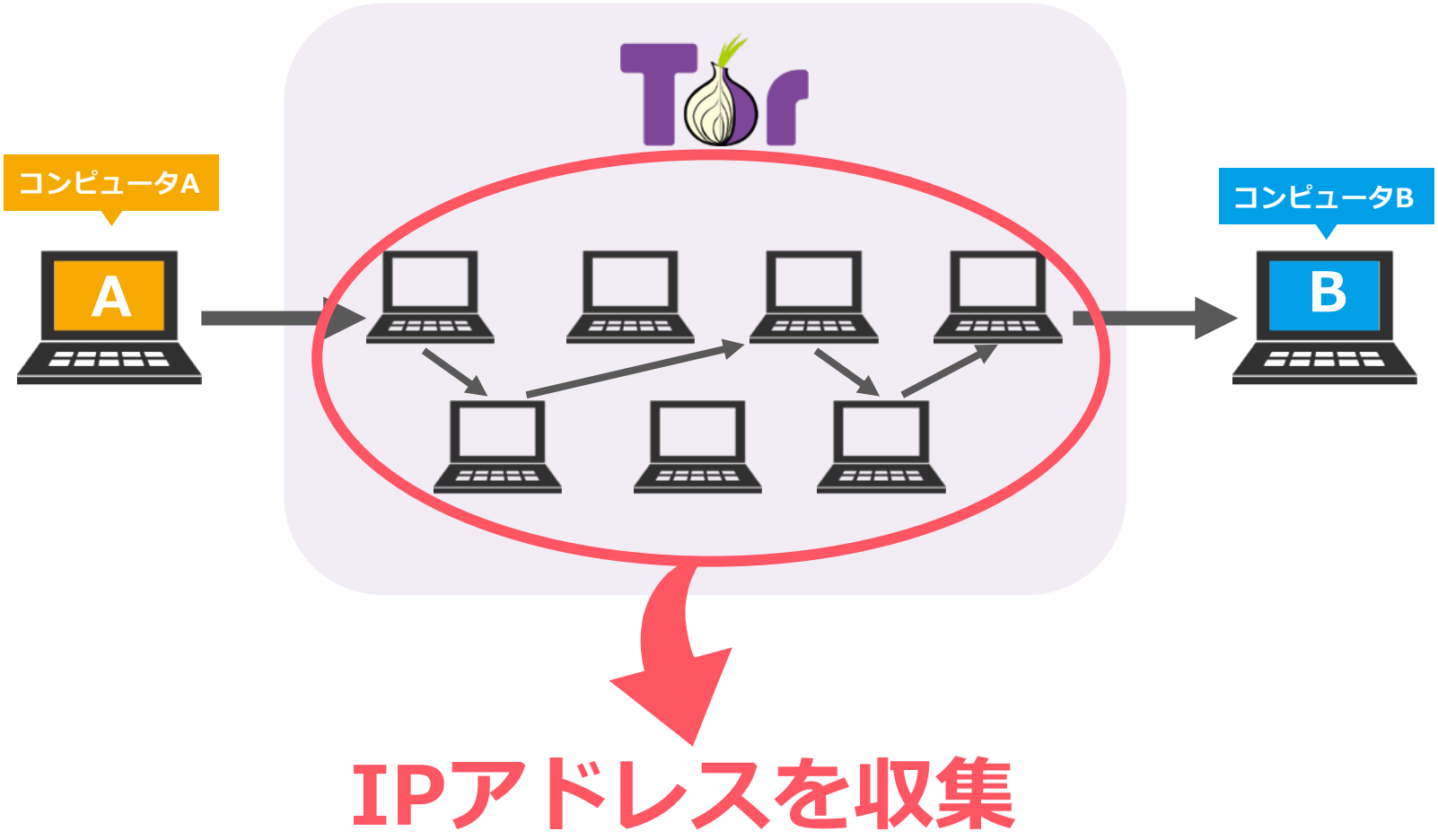
No	Tor判定IPアドレス保有企業名	左記国名	IPアドレス数
1	Deutsche Telekom AG	ドイツ	2247
2	Dynamic DSL Pool, Versatel Deutschland	ドイツ	1018
3	不明		511
4	1&1 Telecom GmbH	ドイツ	382
5	Telefonica Germany GmbH & Co. OHG	ドイツ	356
6	Telefonica Deutschland GmbH	ドイツ	345
7	ARCOR AG	ドイツ	212
8	Digital Ocean, Inc.	米国	201
9	Dedicated Servers and cloud assignment, abuse reports		187
10	ISP Ltd.	ドイツ	187

当社データのサマリー(日本国内)

もっと遠くに、もっと近くに。
Geolocation Technology

No	Tor判定IPアドレス保有企業名	IPアドレス数
1	wide Network of Softbank Corp.	27
2	NTT COMMUNICATIONS CORPORATION , NTTPC Communications, Inc	27
3	OCN	18
4	Vultr Holdings, LLC	18
5	SAKURA Internet Inc.	11
6	Japan Network Information Center(JPNIC)	9
7	Jupiter Telecommunications Co., Ltd.	7
8	So-net Service	6
9	TYO_VULTR_CUST	6
10	Asia Pacific Network Information Centre(APNIC)	5

TorノードのIPアドレスを収集



IPアドレスを収集方法(公開情報から収集)

非公開

Tor Projectが公開している出口ノードのIPアドレス
https://check.torproject.org/exit-addresses

Tor Projectが公開しているノード情報に掲載されているIPアドレス
https://torstatus.rueckgr.at/

上記のサイトの情報を毎日収集し、データ化している

投影ONLY

IPアドレスを収集方法(Torノードから収集)

非公開

投影ONLY

精度を上げる取り組み内容

非公開

□ Torノードの情報連携

ラック様提供情報
Tor　6,225 IP
Tor通信を利用するマルウェア通信先の中で9001番ポート宛ての通信先

1,575 IP

弊社データベース
Tor　16,988 IP
Tor内の中間ノードにて[tcp 443]でフィルターしたIP

弊社 VPS/Cloud
85,634,164 IP

引き続き、データ強化に取り組んでいきます！

投影ONLY

取引時確認で取得した住所と操作している電子計算機のIPアドレス等とが異なる口座開設取引

例) 口座開設時の取引時確認のケース

犯罪収益移転防止法について

もっと遠くに、もっと近くに。
Geolocation Technology

犯罪収益移転防止法において疑わしい取引の届け出を定めており、同法律に関するQ&Aでは「なりすまし」調査においてIPアドレスで調査・判断する事をあげている。

55.既存口座の「なりすまし」調査について

１．全顧客を対象とした定期的な調査
＜定期的な名寄せによる不審口座の抽出＞
半期に一回以上（日次、週次、月次で行う方法を含む。）の周期で全顧客を対象に名寄せ調査を行い、次のような口座を「なりすまし」の可能性がある口座として抽出する。
① 設置型電話番号が同一の口座
② Ｅメールアドレスが同一の口座
③ 携帯電話番号が同一の口座
・ このような口座のうち、住所や姓が異なったり、ＩＰアドレスが同一である口座については「なりすまし」の可能性が高いため、特に慎重な確認が必要であると考えられる。

引用：犯罪による収益の移転防止に関する法律及び同政省令に関するＱ＆Ａ【改訂２.２版】

IPアドレス情報が活用された事例

もっと遠くに、もっと近くに。
Geolocation Technology

インターネットによる商取引を取り入れている金融機関では、すでに信用調査・疑わしい取引の調査にIPアドレスが用いられています。身元調査・不正口座開設の防止に役立てられている事例と、不正取引の検知にIPアドレス情報が使用された例をご紹介します。

インターネット新規口座開設時のマネー・ロンダリングチェック

インターネットを通じた口座開設申込み時に、不正口座開設が疑われるものを抽出して厳しいチェックを行う金融機関の事例です。同一のIPアドレスから都道府県が異なる複数口座の申込みがある場合に、それらを抽出し、チェックの対象にすることで、マネー・ロンダリング等の不正行為を防止しています。

「金融検査結果事例集」金融庁検査局(2015)より

オンライン証券会社を使った借名取引・株価操作の検知

IPアドレスが借名取引の検知に役立った事例もあります。
2012年、親族や知人名義の3つの取引口座・2社の証券会社を利用した不正な株価操作事件が発覚しました。
この事件では、証券会社が同一IPアドレスによる複数口座へのログインを検知したことから借名取引を疑い、同一人物による恣意的な取引による株価の操作が発覚しました。

「株式会社ミマキエンジニアリング株式に係る相場操縦に対する課徴金納付命令の決定」金融庁(2013)より

主要な活用シーン

もっと遠くに、もっと近くに。
Geolocation Technology

1 位置情報・環境情報の不一致からなりすましリスクを判定

ユーザの普段のアクセス環境や直近のアクセス環境をもとに位置情報・環境情報の不自然な変化を検知する「リスクベース認証」の根幹は、IP Geolocation技術が支えています。ID・PASSによる認証が突破されたとしても、水際でユーザの被害を食い止めます。

2 ハイリスクなアクセス元を検知・遮断

「Torなどの匿名化サービスを経由したアクセス」「特定のハイリスク国からのアクセス」など、悪意あるユーザの可能性が高いと考えられるアクセスをIPアドレスから判定。これらのアクセスに対し、認証の強化やアクセス遮断といった対策を取ることができます。

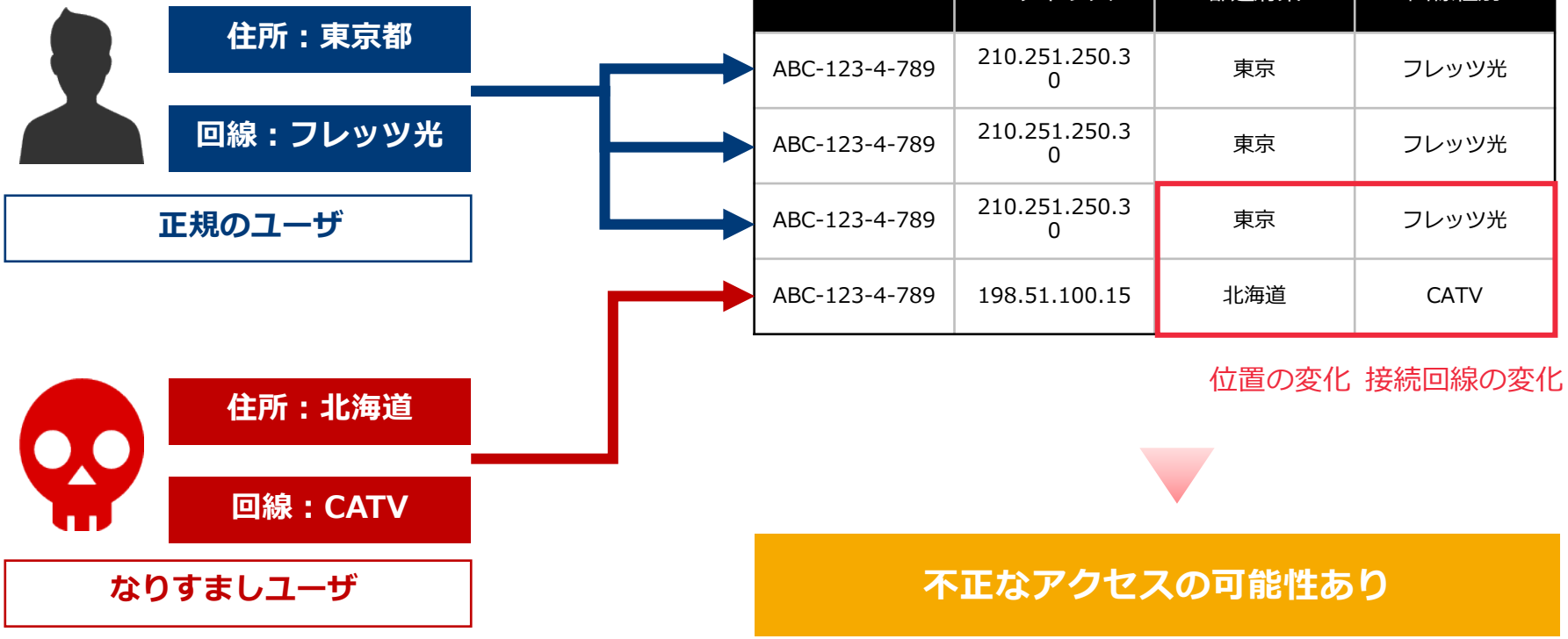
3 フリーメールでのアカウント登録を制御

フリーメール（無料で取得できるメールアドレス）は、身元詐称しやすく、使い捨てしやすい点から、詐欺行為などに使われるリスクが高いと考えられます。フリーメールによる登録時には身元確認のプロセスを追加するなど、悪意あるユーザがサービスを利用することを事前に防ぐ施策を実施できます。

位置情報・環境情報からなりすましリスクを判定

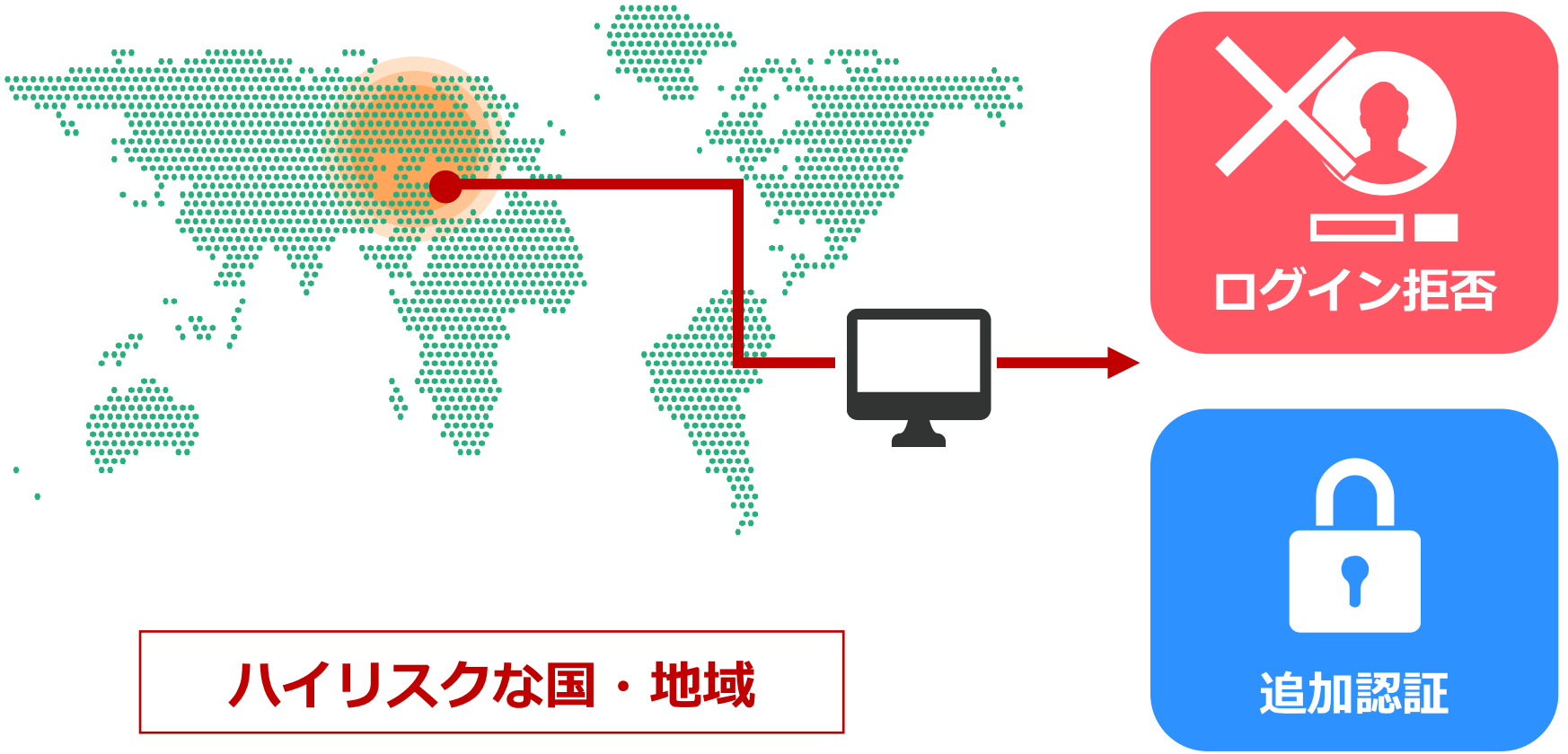
もっと遠くに、もっと近くに。 Geolocation Technology

オンラインバンキング等で導入の進む「リスクベース認証」には、IPアドレスから判定された情報が利用されています。
位置情報の大きな変動や、普段と異なるISPからのアクセスがあった場合に「なりすまし・不正ログイン」の可能性を疑い
追加の認証を求めるというソリューションです。



ハイリスクな国・地域のログイン拒否

特定の国や地域を「ハイリスクな国・地域」と位置付け、ログインを拒否したり、追加認証を求めたりすることもできます。

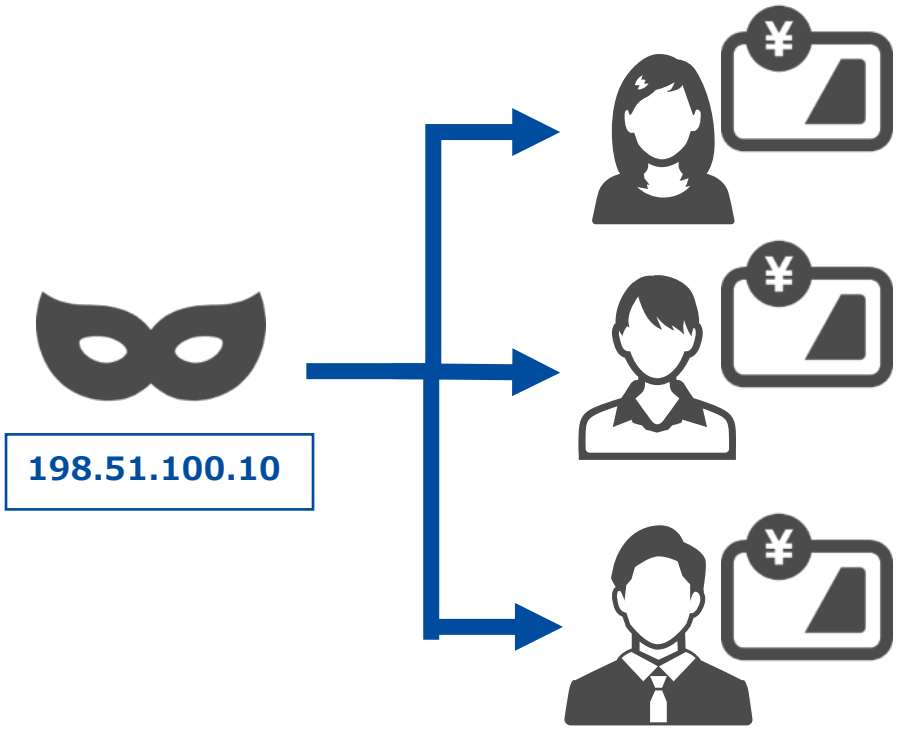


同一または複数のIPからの口座不正利用を検知

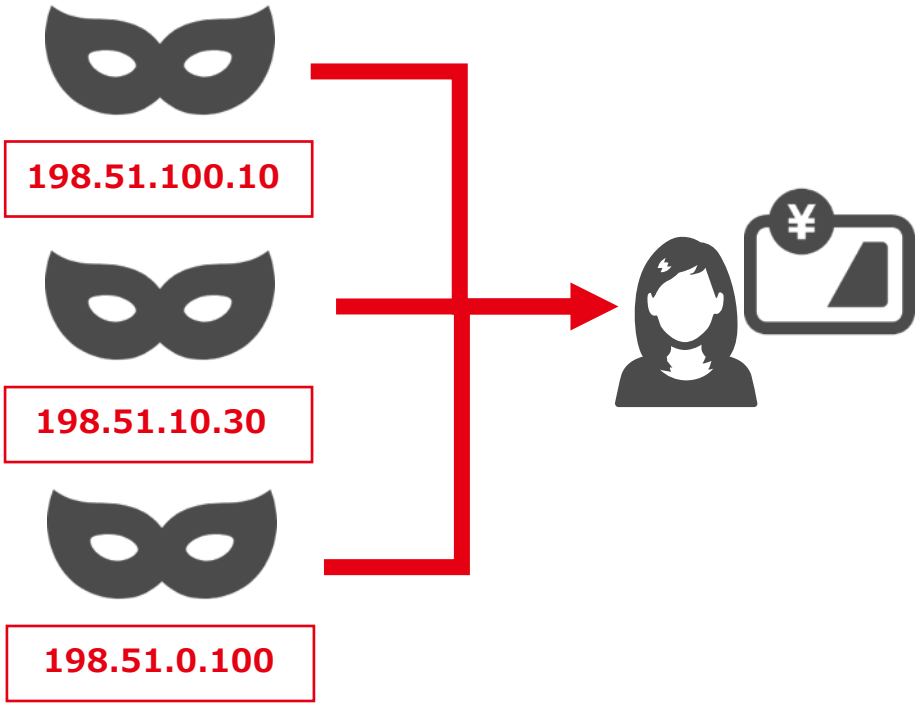
もっと遠くに、もっと近くに。
Geolocation Technology

同一のIPアドレスから多数の口座へのログインが見られた場合、複数口座の開設を許可していない場合は、不正利用を疑う必要があります。
逆に、一つの口座に複数属性のIPアドレスからのログインが見られる場合も、口座の不正な利用が疑われます。

同一のIP→複数口座へのログイン



複数属性のIP→同一口座へのログイン



匿名ネットワーク属性とは

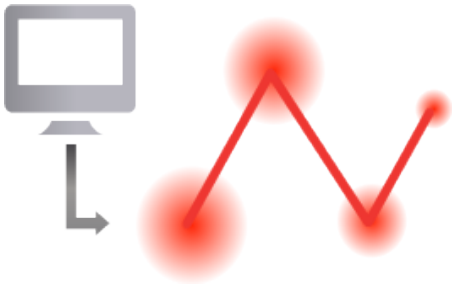
もっと遠くに、もっと近くに。
Geolocation Technology

匿名ネットワーク属性とは、通信元を秘匿化する技術やツールを使い、通信元をカムフラージュしたIPアドレスを判別するデータです。通信元を隠匿したアクセスは、違法・不法目的で使われる場合があり、オンライン取引におけるリスクと考えられます。

どこどこJPで判別できる匿名ネットワークの種類

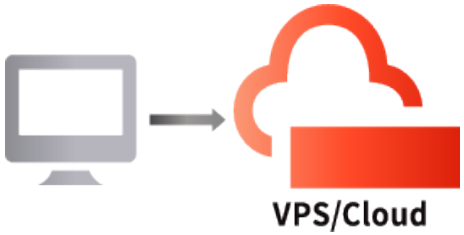
Tor（トーア）

「オニオンルーティング」と呼ばれる接続技術を使い、複数の機器を経由することによって接続経路を秘匿しています。



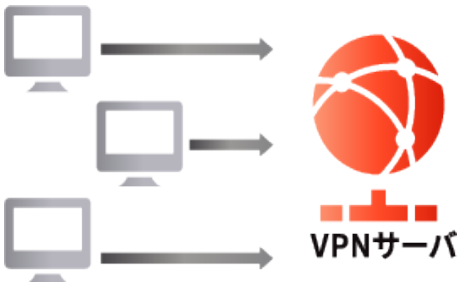
VPS/クラウド

本来はサーバーサービス等に使われますが、アクセス元の秘匿に利用される可能性もあります。



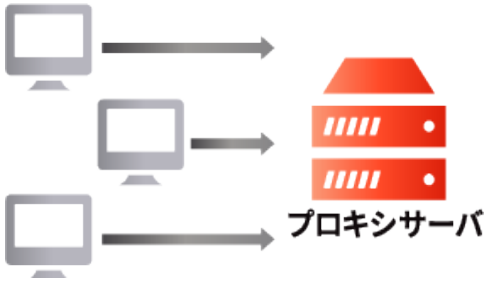
公開VPNサービス

一般に公開されているVPNサーバを経由してアクセスすることで、通信内容の暗号化とアクセス元の秘匿を行います。



プロキシサーバ

インターネット上に公開されている、接続を中継するためのサーバです。プロキシフラグに相当します。



匿名ネットワーク属性による不正アクセスの検知

もっと遠くに、もっと近くに。 Geolocation Technology

違法・不法な目的で利用されるリスクが高い匿名ネットワーク経由のアクセスに対し、適切な防御策を用意することが、被害を未然に防止することにつながります。ユーザのIPアドレスが匿名ネットワーク経由のものかどうかを判別し、「身元を隠匿したアクセスに対してログイン時に認証要素を追加する」「匿名ネットワーク経由によるエラーはリクエストを遮断する」といった対応を行うことでセキュリティを強化することが可能です。

パターン ①

IPアドレス	タイムスタンプ	匿名ネットワーク属性	危険性
198.51.100.15	2016-05-12 T12:00:15	–	✓
210.251.250.30	2016-05-12 T12:30:01	Tor	⚠
210.251.250.30	2016-05-12 T12:30:01	Tor	⚠
210.251.250.30	2016-05-12 T12:30:02	Tor	⚠

同一のIPアドレス　　ほぼ同時刻のアクセス

不正なアクセスの可能性あり

パターン ②

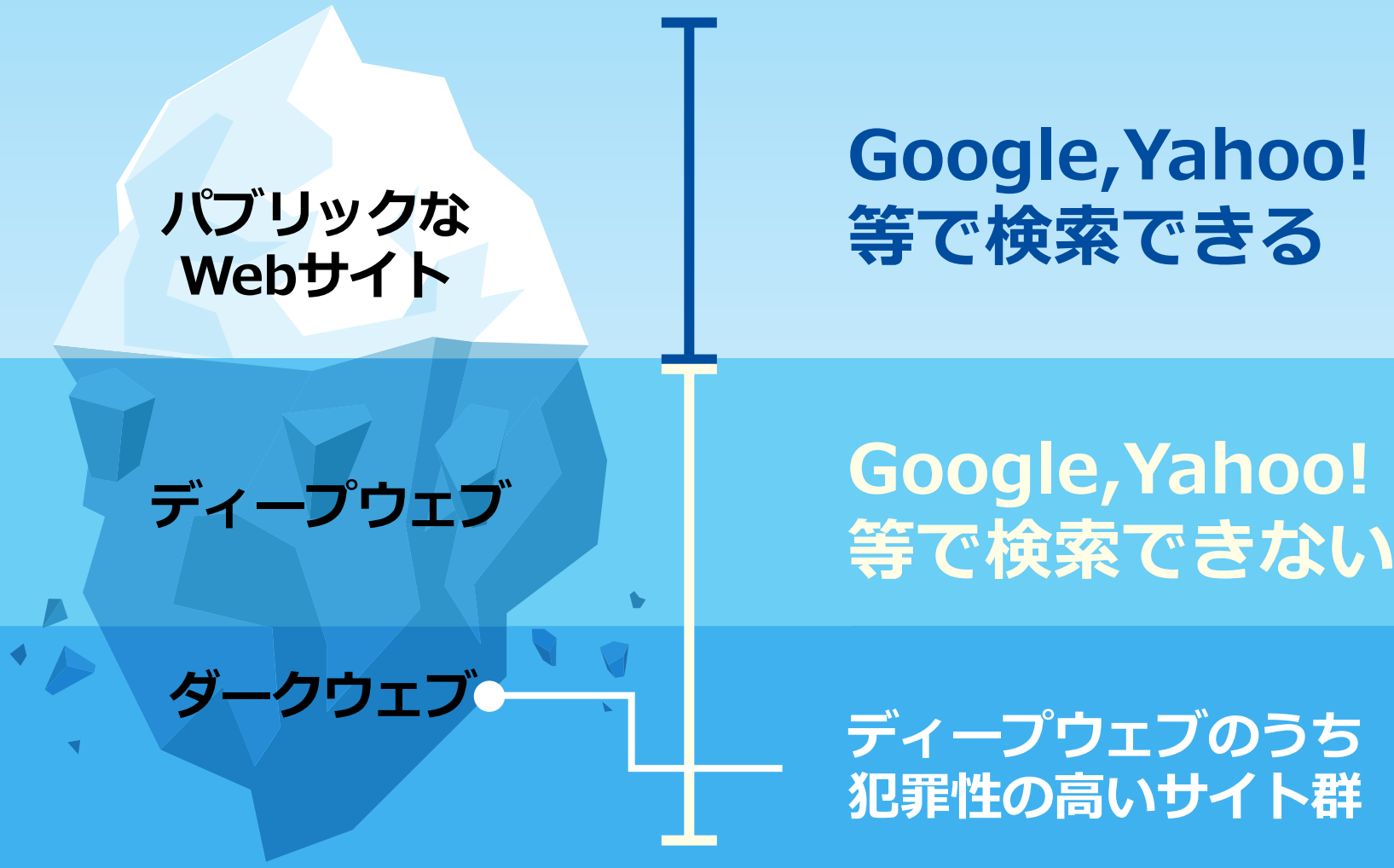
IPアドレス	ステータスコード	匿名ネットワーク属性	危険性
210.251.250.30	200	–	✓
203.0.113.10	404	パブリックプロキシ	⚠
203.0.113.11	404	パブリックプロキシ	⚠
203.0.113.12	404	パブリックプロキシ	⚠

連続したIPアドレス　　多数のエラー

不正なアクセスの可能性あり

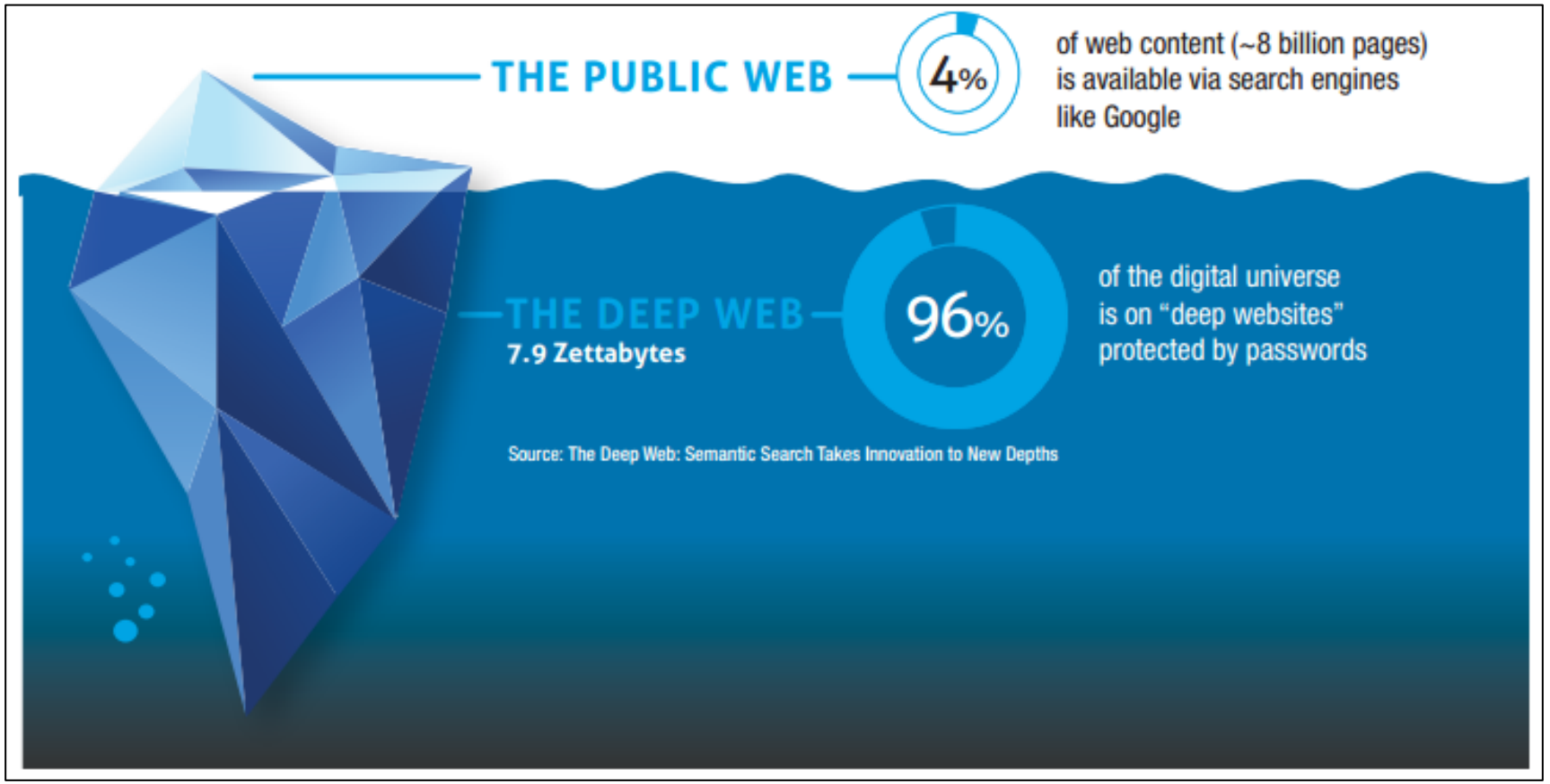
ダークウェブとは

見えるサイトと見えないサイト



【参考】ディープウェブの規模

全ウェブサイトの96%がディープウェブというデータがある



https://www.jurnalweb.com/konten-yang-ada-di-deep-web-dunia-gelap-di-internet/

ディープウェブとは

もっと遠くに、もっと近くに。
Geolocation Technology

動的Webページ

HTTPリクエスト上で
動的に生成されるページ

ブロックされたサイト

検索エンジンのクローラーの
巡回等を禁止したサイト

**リンクされていない
サイト**

他のページからリンク
されていないサイト

プライベートサイト

登録やログイン、パスワード
認証が必要なサイト

**非HTMLサイト・スクリプト化されたサイト
コンテキストされたサイト**

Jacaスクリプト、Flashを介してアクセス、
もしくはIPアドレス等でアクセス制限されたサイト

アクセス制限されたネットワーク

公共のインターンネットインフラから
アクセスできないサイト

→ **ダークウェブ**

トレンドマイクロ社「Deep Webとサイバー犯罪」より

ダークウェブを閲覧するには

Torブラウザのダウンロード

非公開

投影ONLY

ダークウェブの閲覧

非公開

投影ONLY

ダークウェブ関連のニュース 1

非公開

■2018年12月　PayPayの不正利用にダークウェブが利用される

ダークウェブにてPayPayで認証済みの
クレジットカード番号の売買が
されている書き込みがありメディアに取
り上げられた。

PayPayのカード認証が何度でも試すこ
とができてしまい、買い
認証済みカードの売買
あった。

投影ONLY

■2018年流行語大賞に「仮想通貨 / ダークウェブ」がノミネート

■Torプロジェクトへの寄付金が過去最高額に達した

ダークウェブ関連のニュース 2

非公開

■2019年2月　16のサービスから流出した6億1700万人分の
アカウント情報が売買されていた

16サイトのユーザーのアカウントデータが
TorネットワークにあるDream Marketに売りに出されていた。
全データで220万円で購入できる状態であった。

■2019年2月　22億件を超えるアカウントデータが
22億件がダークウェブ上で無料ダウンロードできる状態になっていた

過去の様々なアカウント流出事件で漏れてしまったアカウントが
ひとつにまとめられ無料で一括ダウンロードできる状態になっていた。
これらのデータは古いものが多数であるが、
いまだアカウントとして利用できるものもあり注意が必要。

投影ONLY

ダークウェブ関連のニュース 3

非公開

■2019年5月

世界最大級の闇サイト「ウォールストリート・マーケット」摘発

ドイツと米国の捜査当局は、世界最大級の闇サイト「ウォールストリート・マーケット」を運営したなどとして両国の５人を逮捕し、サイトを閉鎖したと発表。同サイトは匿名化ソフトを使ってのみ接続できるネット空間「ダークウェブ」上で世界２位の規模の違法売買サイトだった。

投影ONLY

まとめ

IP Geolocationはインターネット上の様々なビジネスシーンで利用されています。

IPアドレス分析の際、IPアドレスの行動範囲を意識しましょう。

ETL処理・セキュリティなどで利用する際、信頼出来るデータセットを使いましょう

もっと遠くに、もっと近くに。
Geolocation Technology

講演内容は以上です。ご清聴ありがとうございました。

社名	株式会社Geolocation Technology （旧社名：サイバーエリアリサーチ株式会社）
英文名	Geolocation Technology, Inc.
設立日	2000年2月21日
事業内容	IP Geolocation事業　AdTech事業 IPアドレス移転事業
本社	〒411-0036　静岡県三島市一番町18-22 アーサーファーストビル4階
東京営業所	〒150-0001　東京都渋谷区神宮前6-28-9 東武ビル6階
那覇コンタクトセンター	〒900-0032　沖縄県那覇市松山2丁目1-12 合人社那覇松山ビル303
参加団体 その他	（社）日本インターネットプロバイダー協会、 NPO法人ふじのくに情報ネットワーク機構 JPNIC IPアドレス管理指定事業者、 総務省 登録電気通信事業者

SHIMIZU S-PULSE

Geolocation Technologyは清水エスパルスの
オフィシャルマーケティングパートナーです。

たいせつにします プライバシー
10823227

NSF
NSF-ISR
Registered to ISO 9001 and ISO 27001

ANAB ACCREDITED
ISO/IEC 17021
MANAGEMENT SYSTEMS CERTIFICATION BODY