

15コマ集中講義 ITブートキャンプ Part5

# サイバーセキュリティ



神山まると高専 技術教育統括ディレクター  
福野泰介 @taisukef

一日一創

# ITブートキャンプ カリキュラム

4/1	4/2	4/3	4/4	4/5	4/8
-	-	-	-	演習時間 Q&Aコーナー	開発時間
-	-	サイバーセキュリティ IchigoJamでネットワークと プロトコル	-	まるごとアイデアソン	開発時間
電子工作 IchigoJamはんだづけ	計測と制御 IchigoJam サーボ&センサー	マシン語とOS IchigoJam Armマシン語	ウェブアプリ開発 HTML+CSS+JavaScript	まるごとハッカソン	まるごとプレゼン *
プログラミング IchigoJamプログラミング	演習時間 * IchigoJamで自由工作	C言語 gccとIchigoJamをいじる	AIとVR * 自由に作ってみよう		

1限: 9:00-10:30, 2限: 10:45-12:15, 3限: 13:15-14:45, 4限: 15:00-16:30

\* レポート計3回

セキュリティ = 安全

**安全教室といえは？**





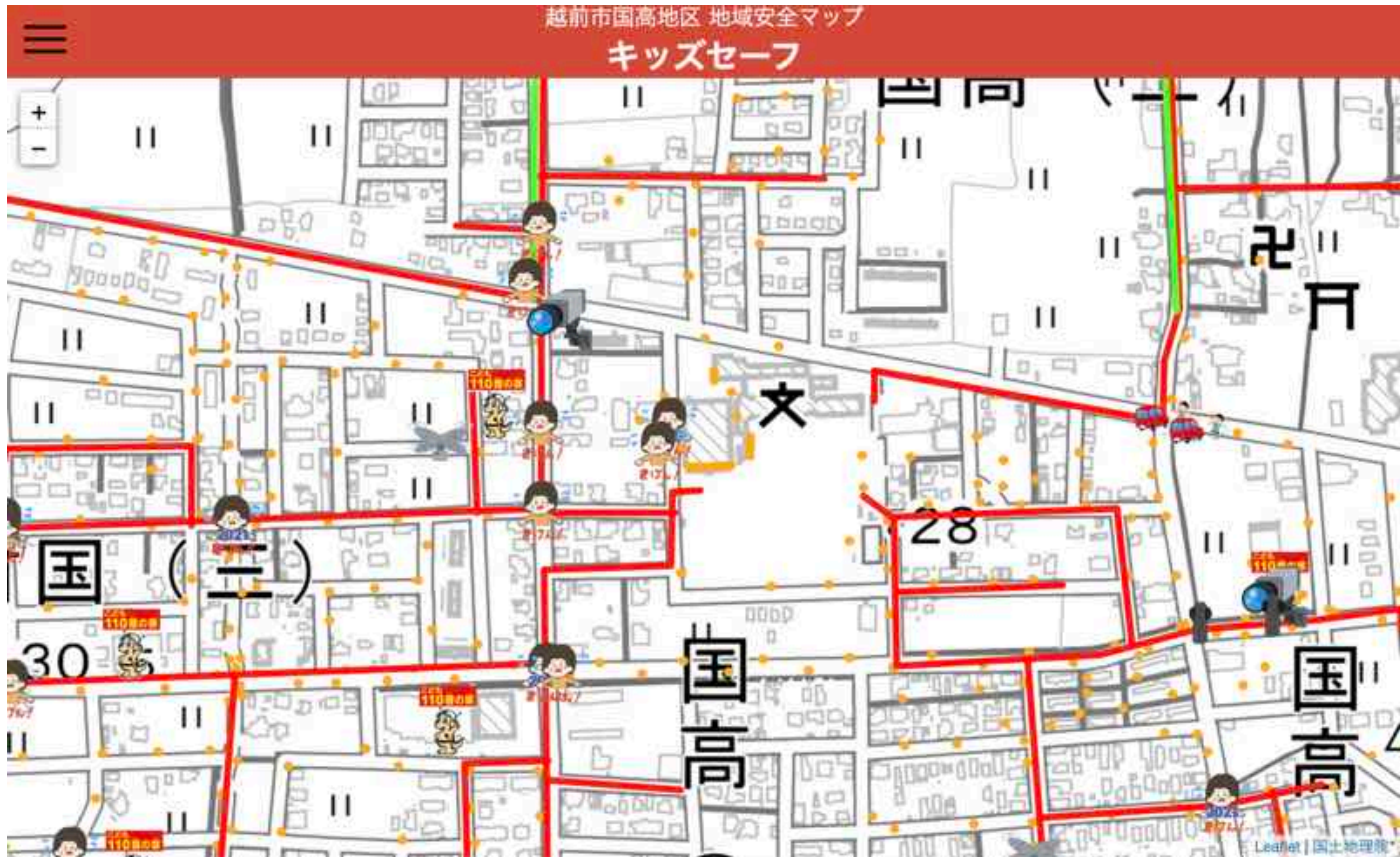
交通安全教室  
なぜ必要？





鯖江東小学校 1Fにて発見





越前市国高地区で運用している地域安全マップ「キッズセーフ」





1年で  
日本で30万件  
福井で1000件  
交通事故



**交通事故が危ないのはなぜ？**



# 交通事故が危ない理由

## 物理の基本法則

$$F=ma$$

(攻撃力 = 質量 x 速度の変化)



攻撃力 = 質量 x 速度の変化

手をゆっくり叩いてみよう

手をすばやく叩いてみよう



攻撃力 = 質量 x 速度の変化

やわらかいものを軽くたたく

硬いものを軽くたたく



攻撃力 = 質量 x 速度の変化

軽いものでたたく

重いものでたたく





どっちがやばそう？



危ないのでルールがある

法則の理解と危ないを避ける力  
大事！



**交通事故の他、危ないこと？**





鯖江東小学校 2F-3F 廊下にて発見



**学校の事故 年間100万件  
(交通事故の3倍)**

**家庭の事故死亡者数 15,000人  
(交通事故死者数の4倍)**



事故は怪我だけじゃない

事故＝思いがけず起きる悪いこと

悪口を言われる



なりすまし

(自分を名乗って嫌なことをする)



**事故の他、危ないこと？**

自然災害



窃盗（ぬすみ） 年38万件  
恐喝（おどし） 年1200件  
器物損壊（はかい） 年7万件  
詐欺（さぎ） 年1万7千件

※ただし、サイバー犯罪は含まず

	犯罪	サイバー犯罪
事故	悪口、なりすまし	ネット上で悪口、なりすまし
詐欺	口頭、電話、メール	メール、ウェブ
恐喝	口頭、電話、メール	ランサムウェア（アプリ）
窃盗	モノの盗難（著作権侵害）	データの盗難（著作権侵害）
器物損壊	自転車を壊される	データを壊される

サイバー犯罪も犯罪の一種



著作権=つくった人の権利

誰かが作ったデータは、  
その人の権利があるので、  
勝手に盗んだり、  
壊したりしたらダメ



# 例外 1

自分がつくるものの一部として  
引用する場合

## 例外 2

つくった本人がいいよと言った場合  
オープンデータもその一種



ここはどこだろう？



FIND/47 no.3925 雲の上の風力発電 © m\_someya クリエイティブ・コモンズ・ライセンス (表示 4.0 国際)

日本のステキ写真オープンデータ by FIND/47





コンピューターと  
なかよくなろう



IchigoJamを教える  
スライドも  
オープンデータ  
by IchigoJam

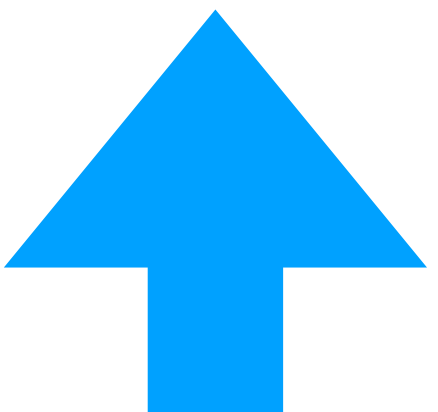
はじめてのプログラミング

with IchigoJam R



このプレゼンテーションは CC BY のオープンデータです  
出典記載のみで、編集・改変して自由に活用いただけます

<https://ichigojam.net/>





サイバーって何？

サイバー

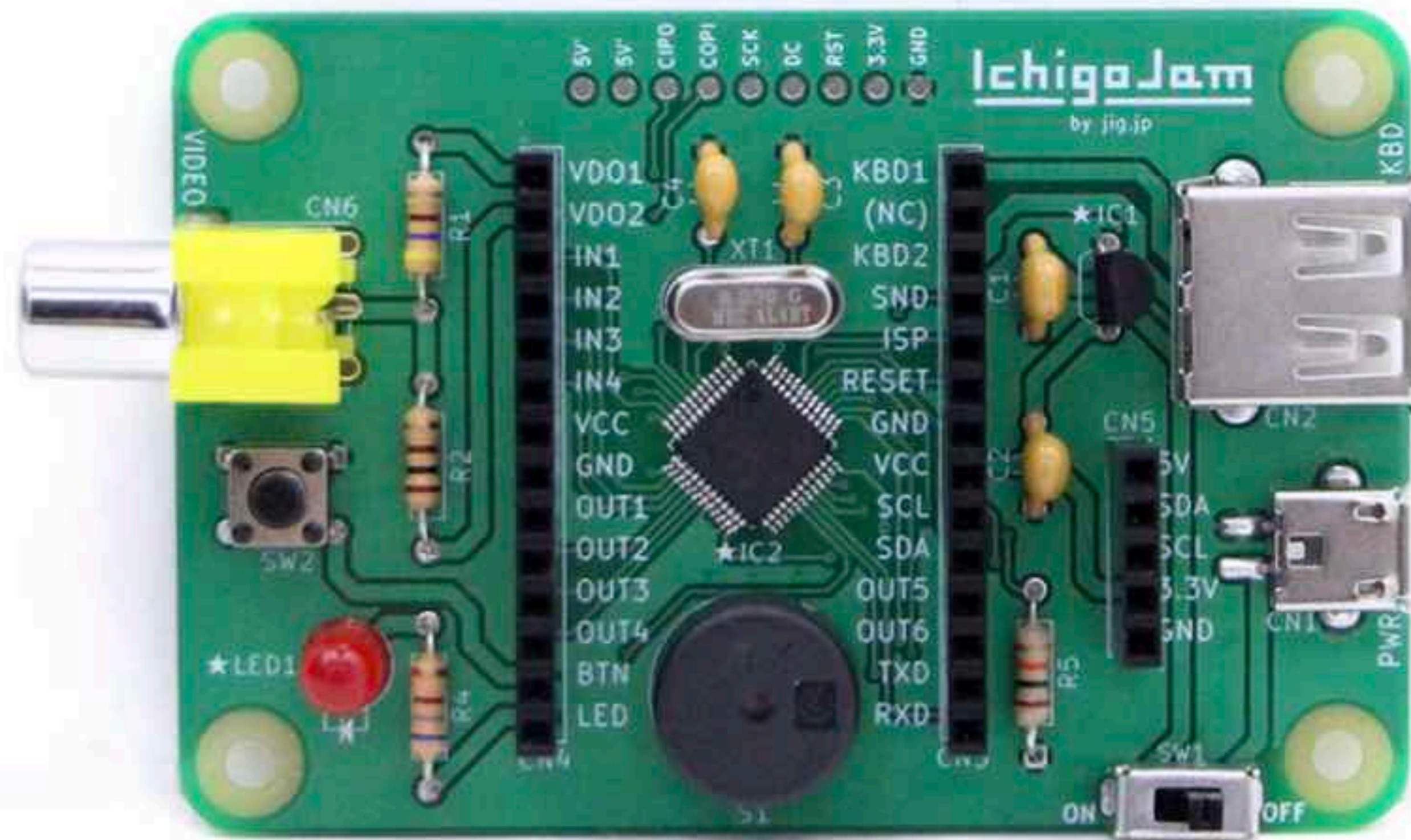
=

コンピュータや

ネットワークに関すること



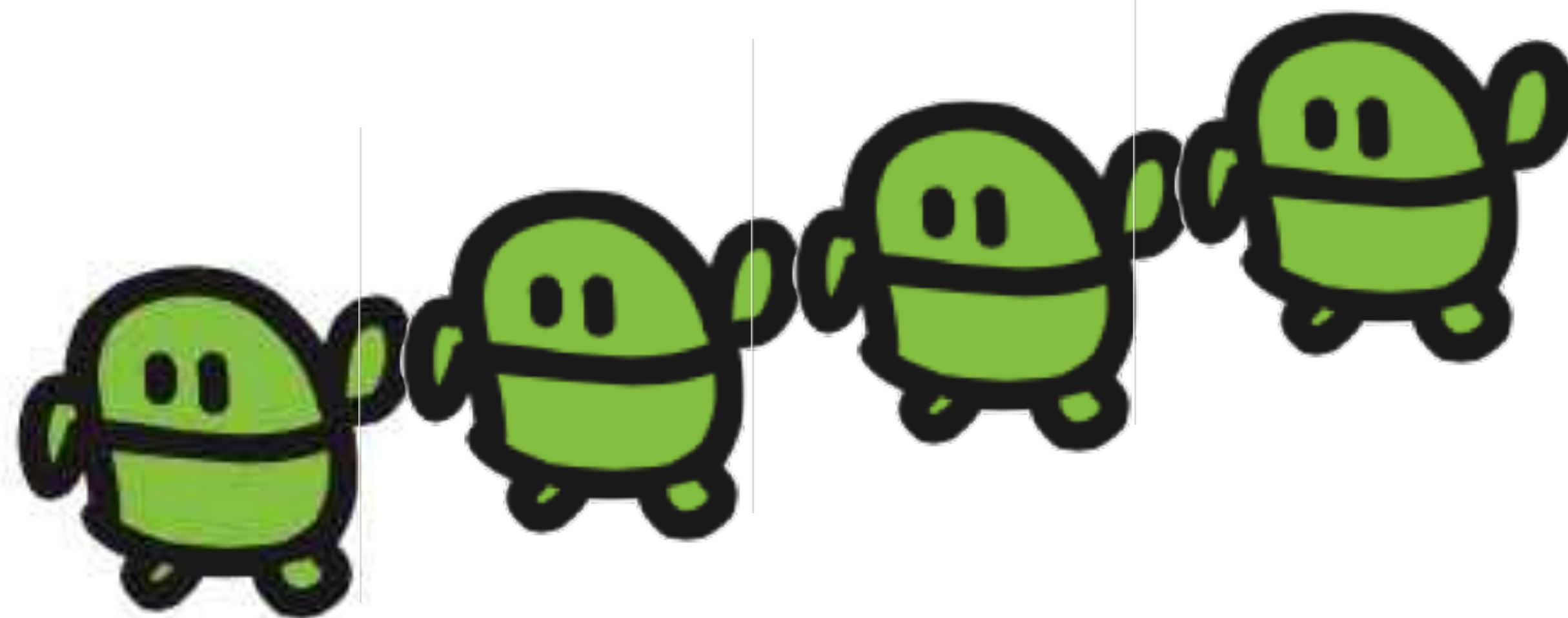
# コンピューター



ネットワーク



ネットワークとは  
コンピューターが  
つながったもの



インターネットは  
ネットワークが  
たくさんつながったもの

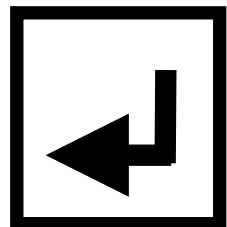
合計100おくらうい

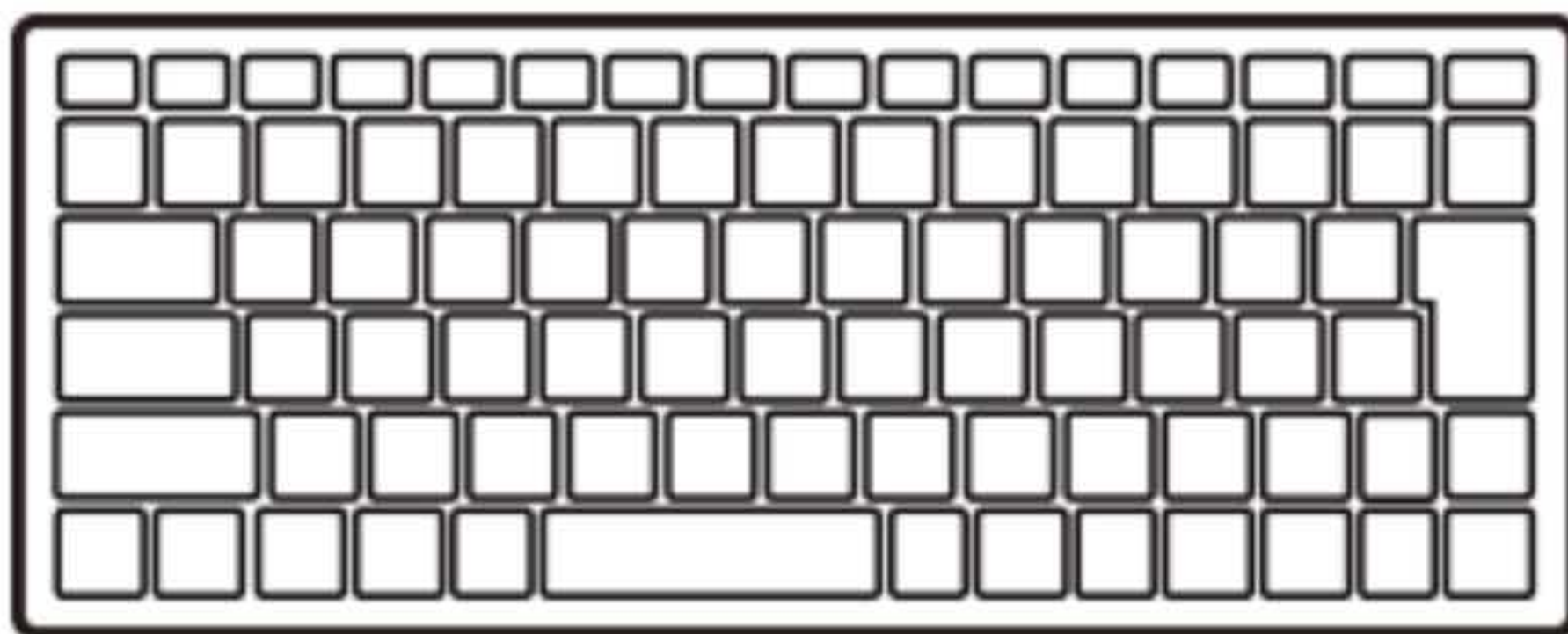
いちばんちいさな  
ネットをつくらう





さいしょから

NEW 



ほぞんしたのは  
きえないよ



2人でっうしんしよう  
Aさん、Bさんにわかります



それぞれちがういろの  
ジャンパー線を1本えらんでね





# プログラムをにゅりょく

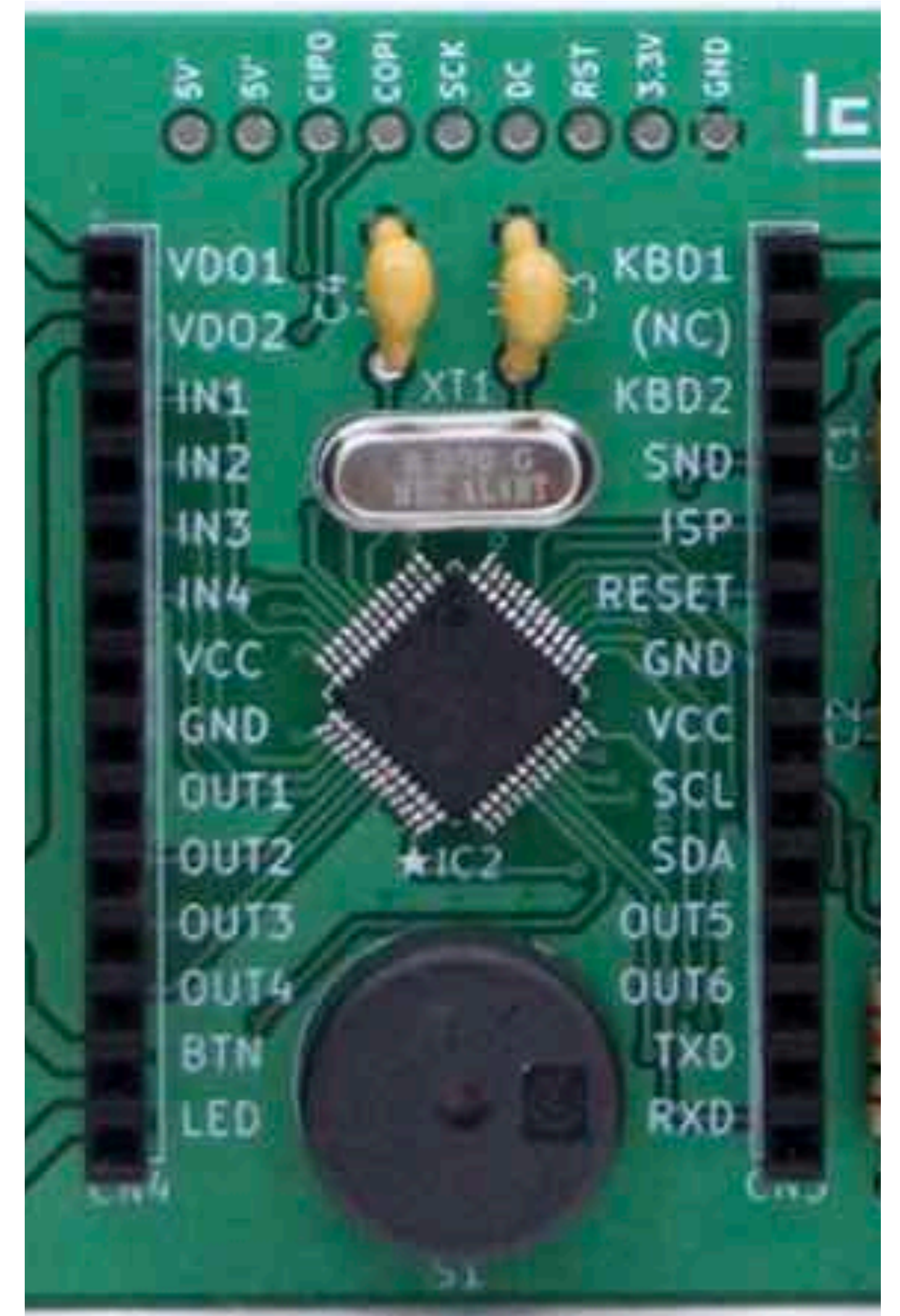
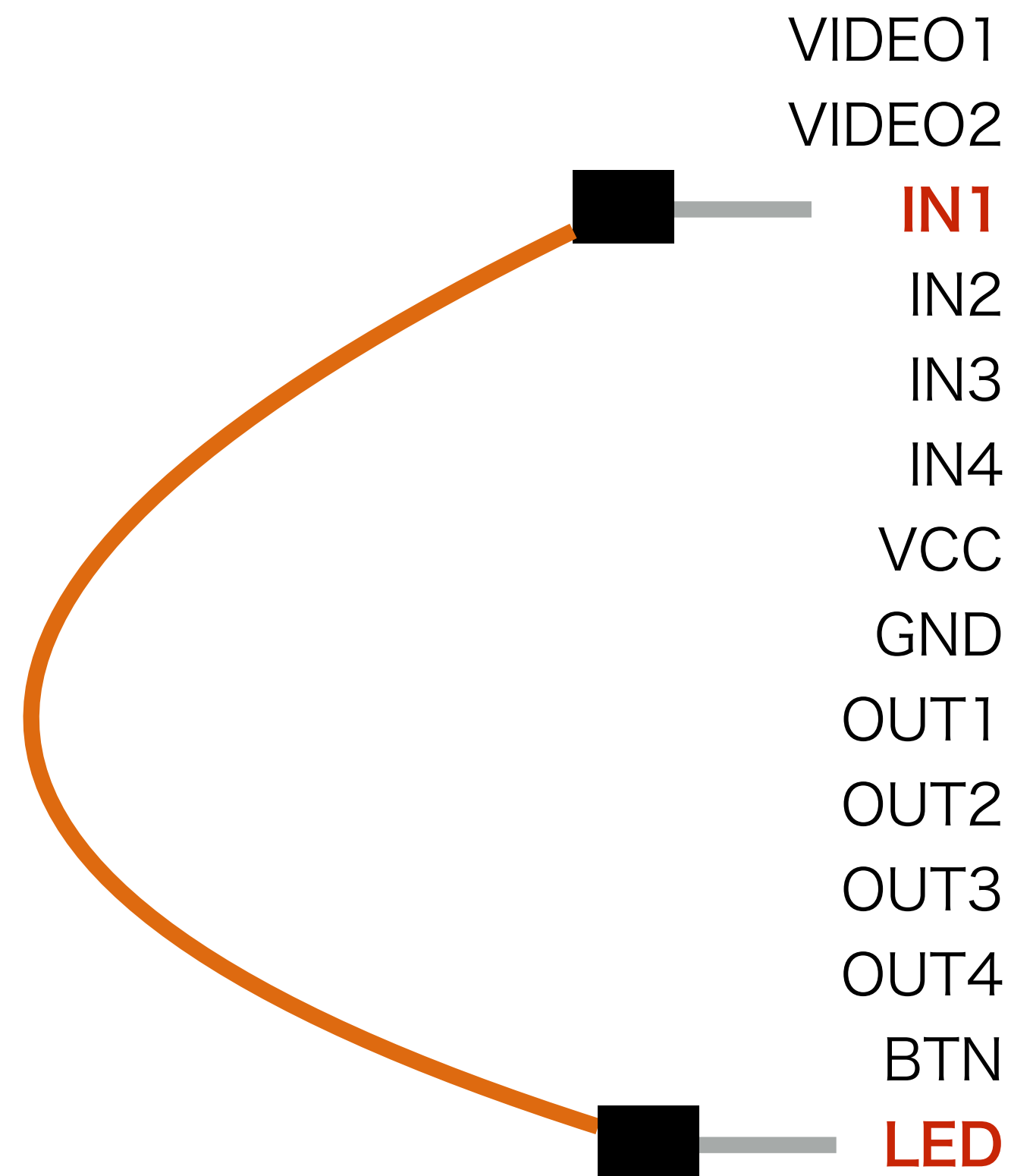
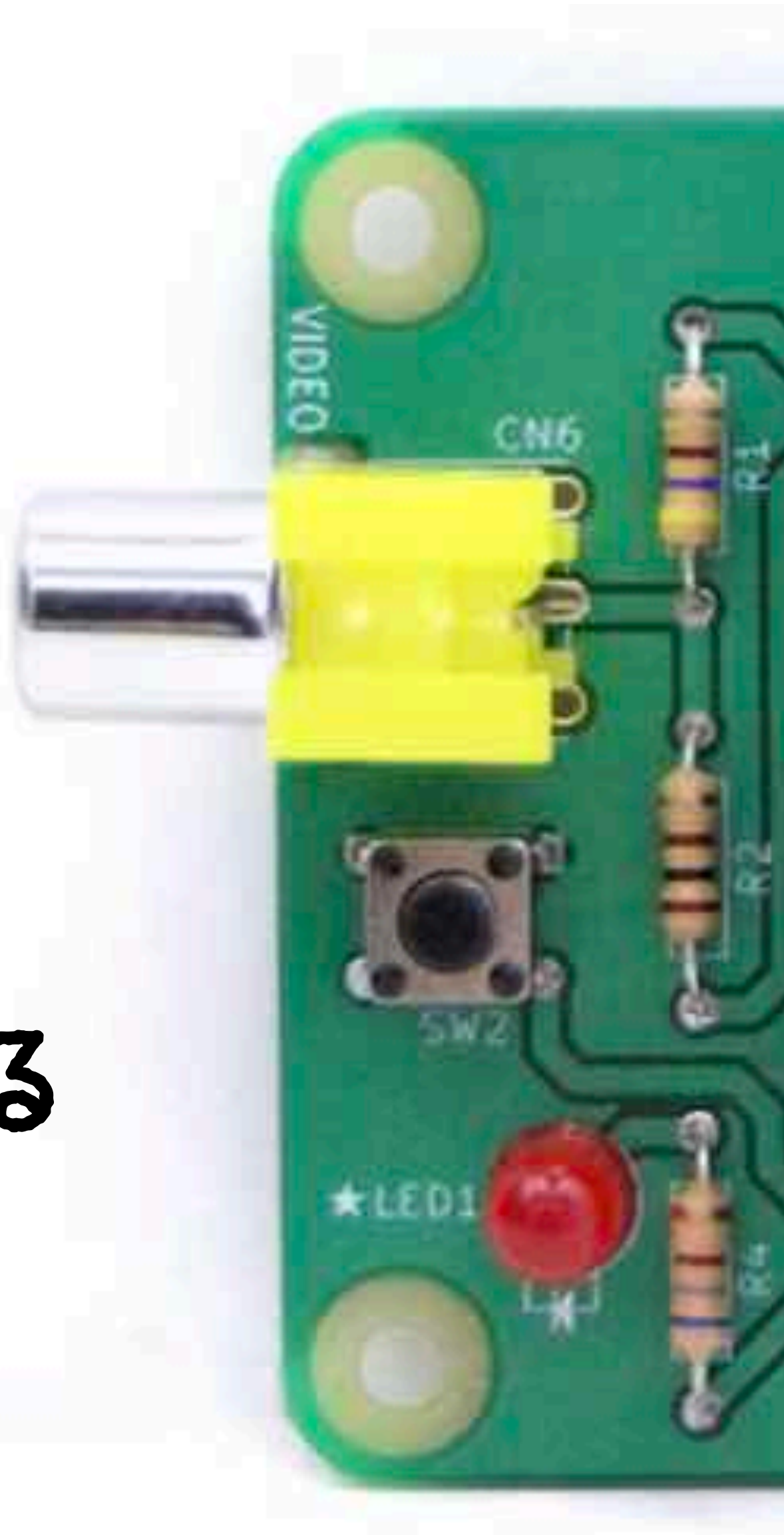
```
1 ?IN(1):LED BTN():WAIT5:CONT
```

```
SAVE 14
```

```
RUN
```

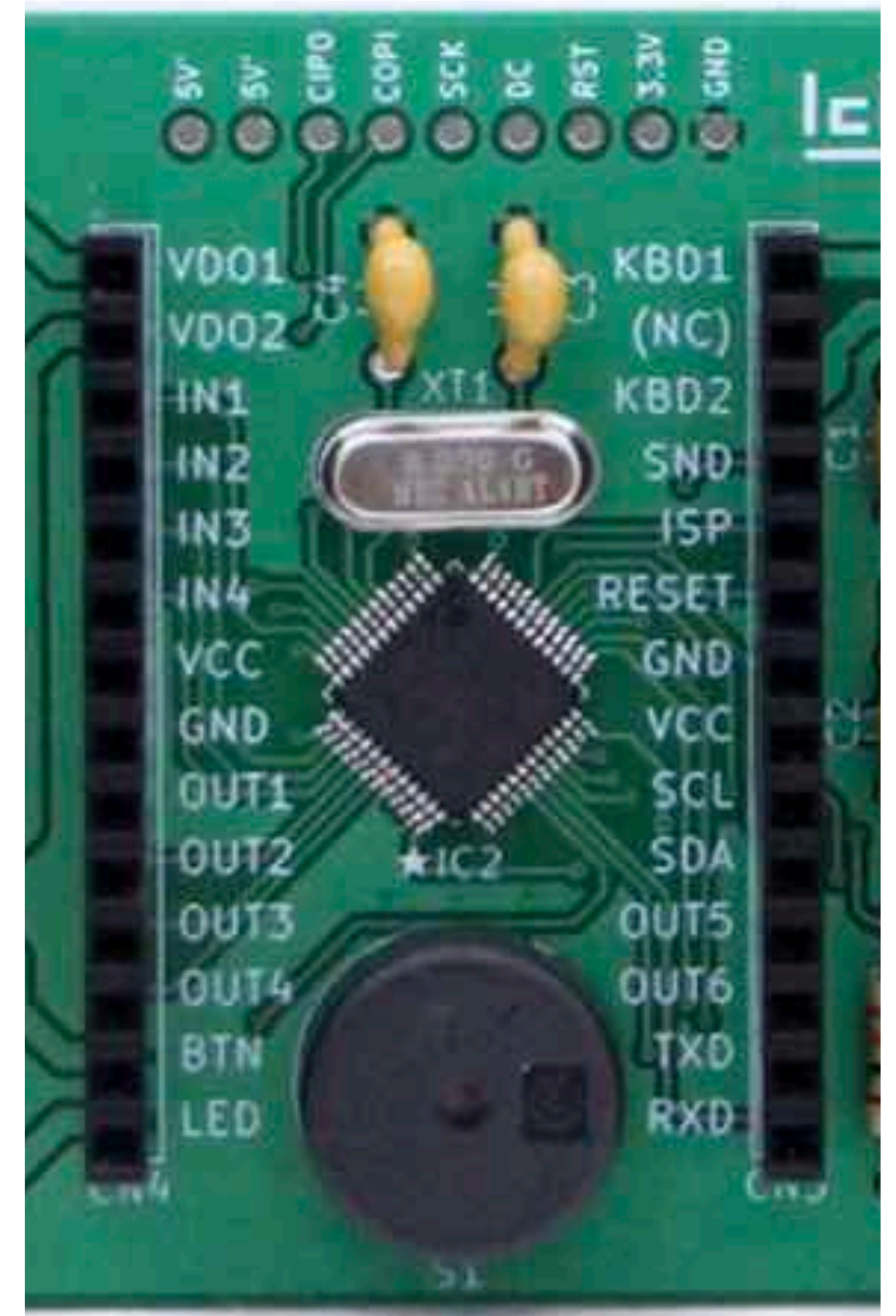
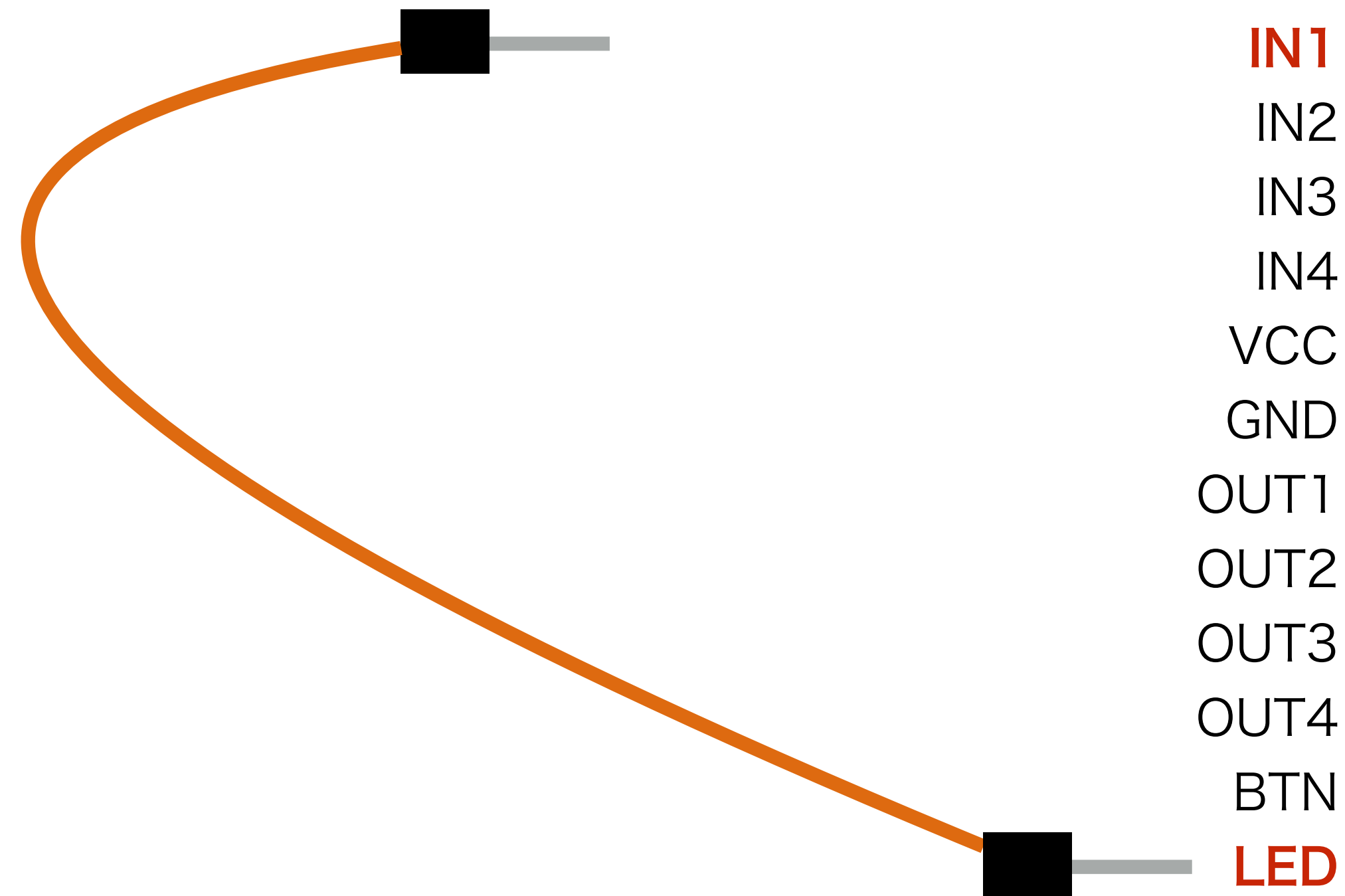
ジャンパーせんて"IN1からLEDにつなぐ"

ボタンを  
おしてみる





ジャンパーせん、IN1からぬく

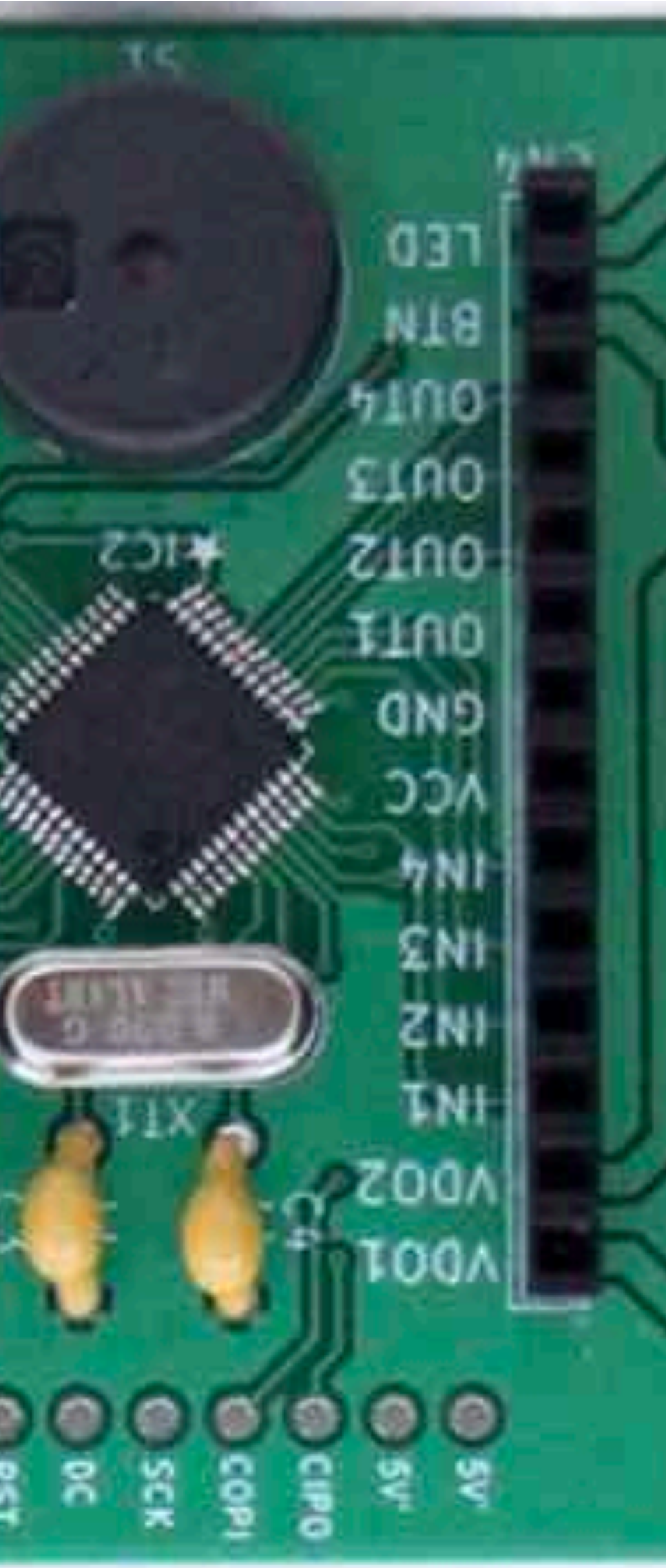




# おたがいのIN1へつながろう

Bさん

Aさん



AさんのLEDへ

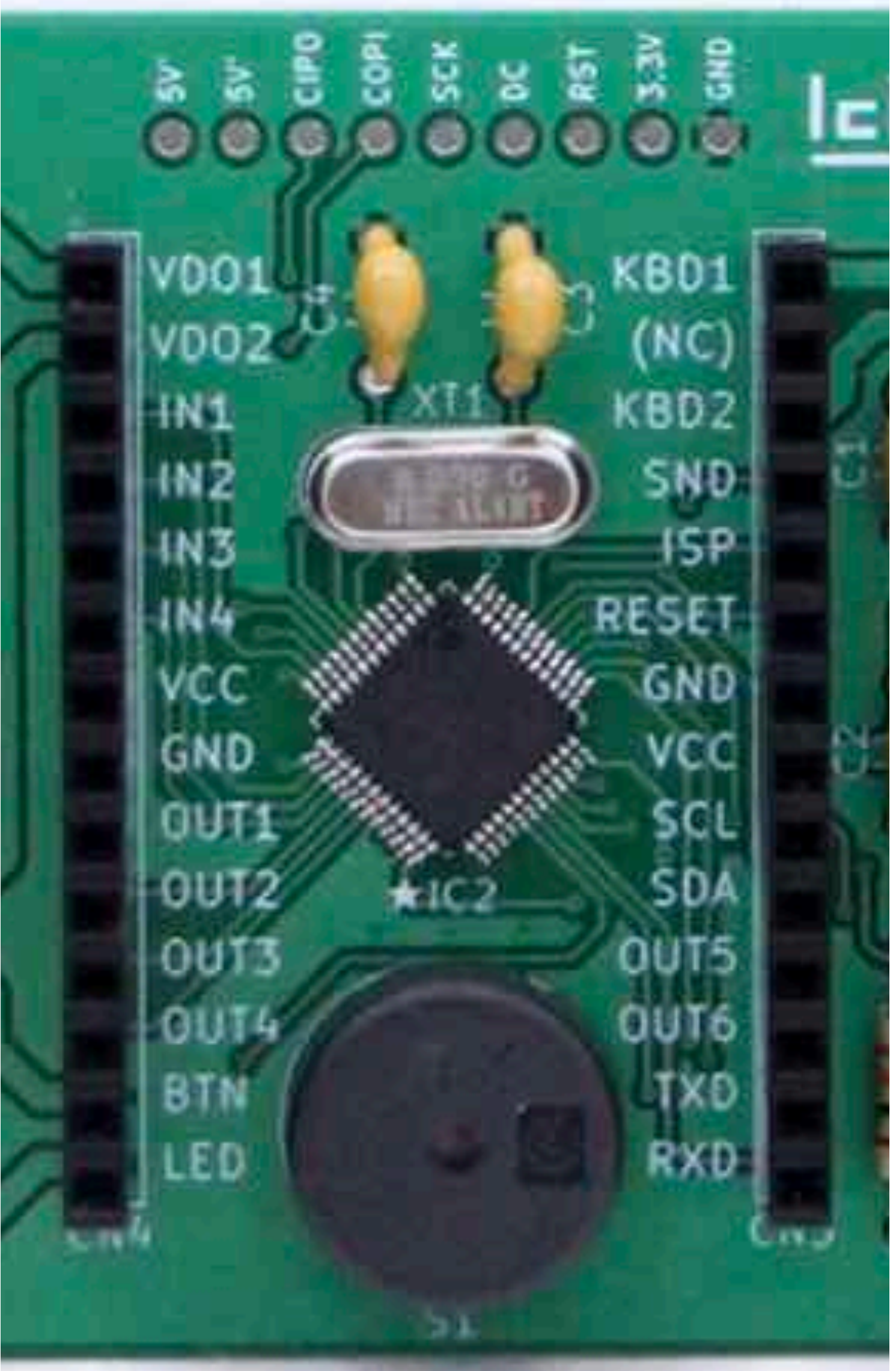


BさんのIN1から

VIDEO1  
VIDEO2  
**IN1**  
IN2  
IN3  
IN4  
VCC  
GND  
OUT1  
OUT2  
OUT3  
OUT4  
BTN  
**LED**

AさんのIN1から

BさんのLED



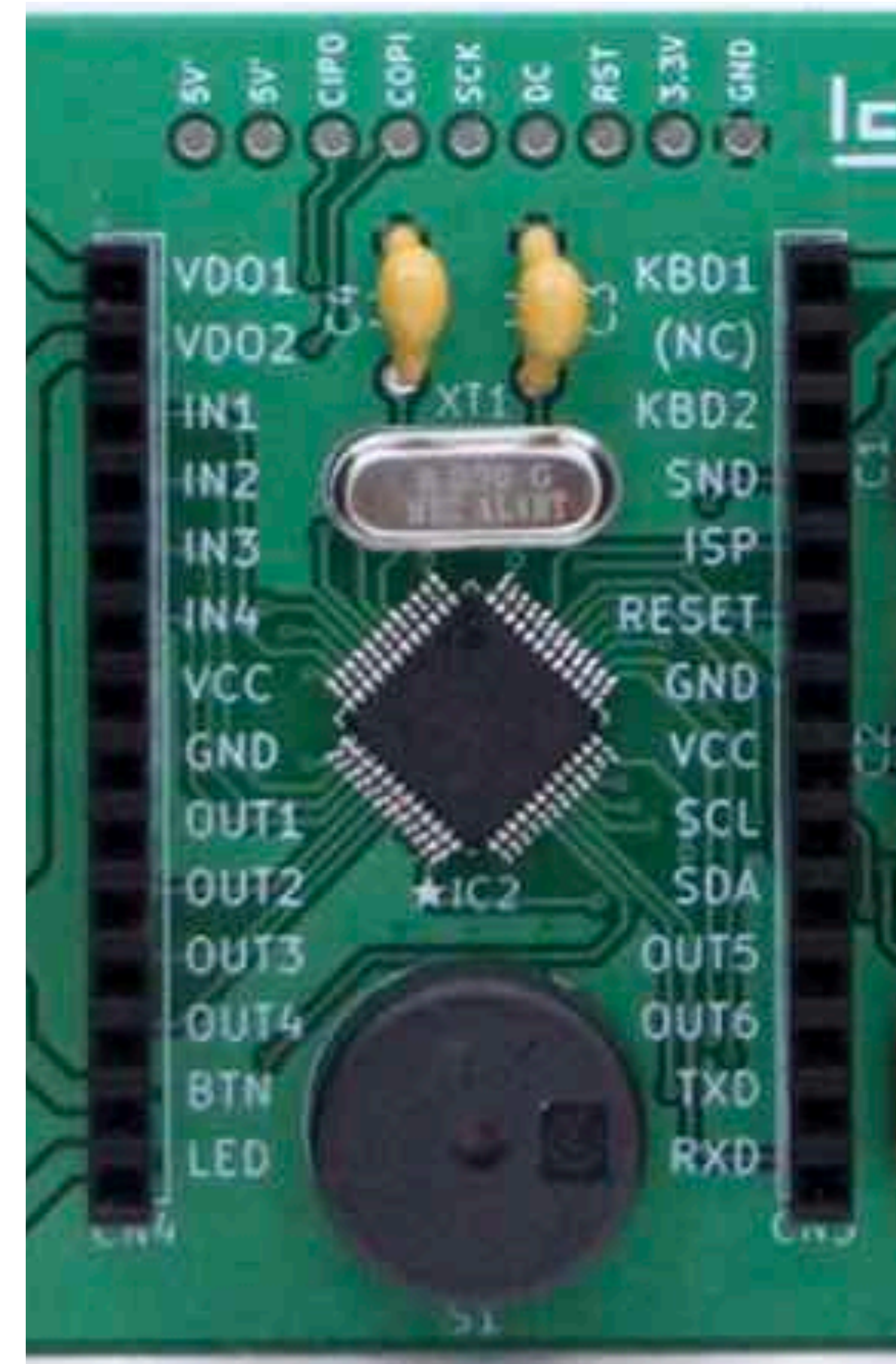
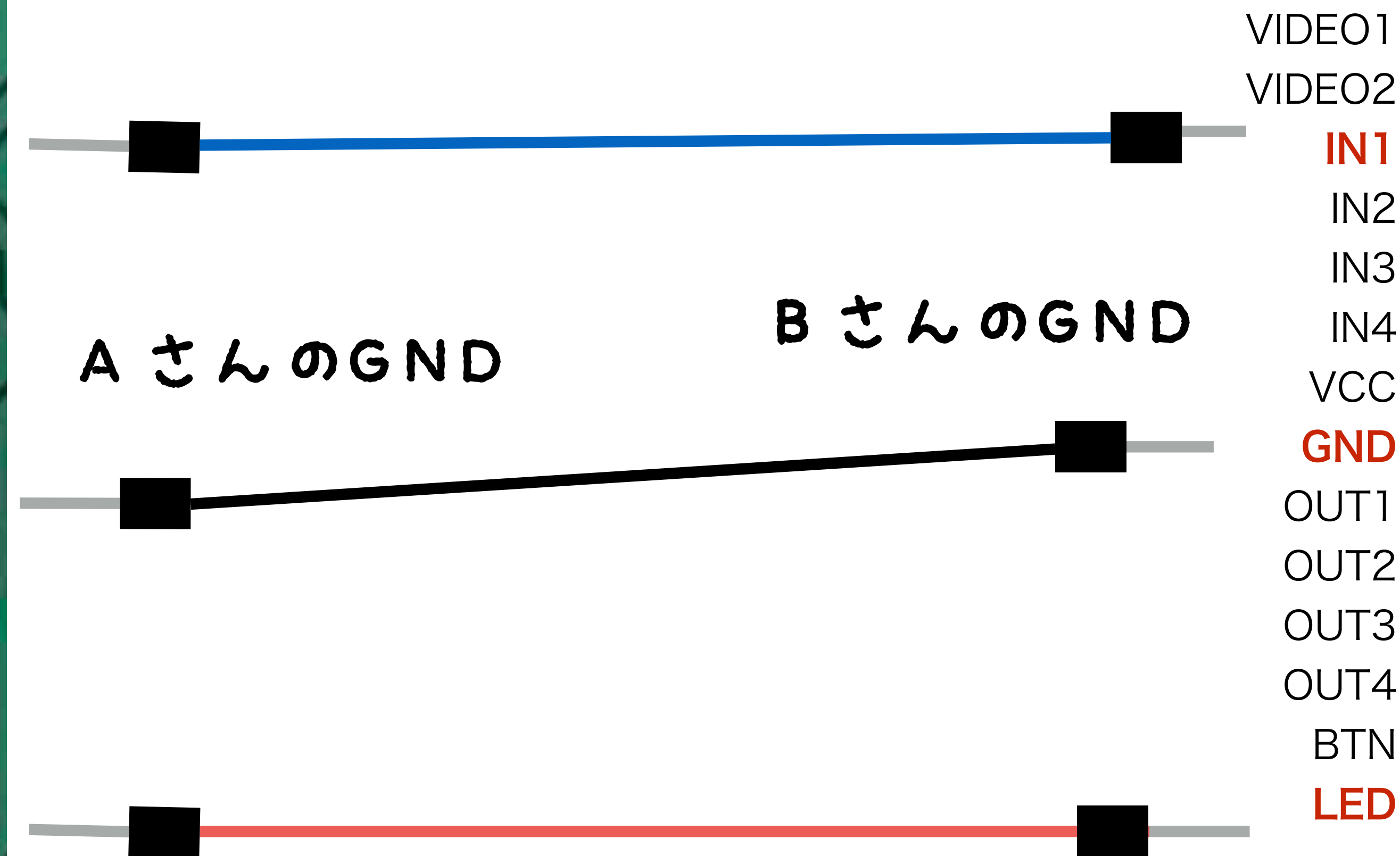
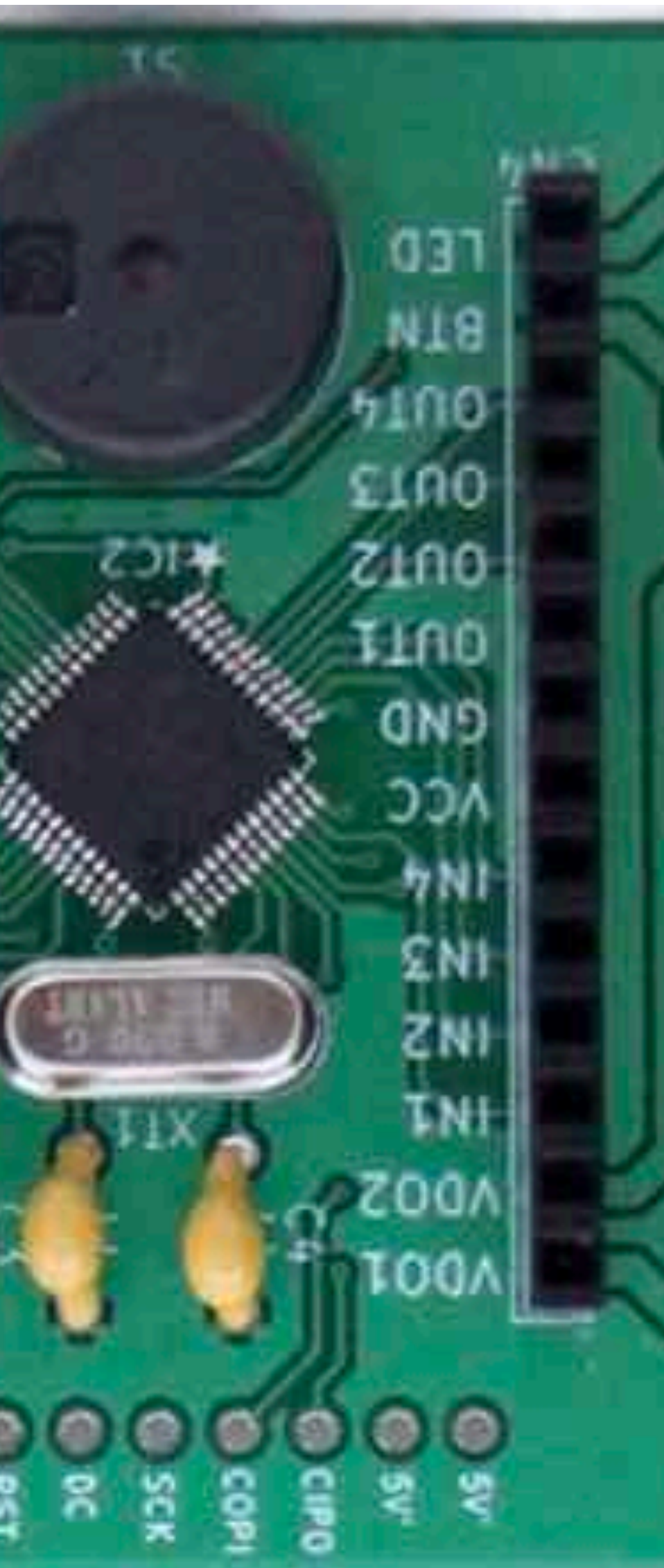


ジャンパー線を2人で1本だけついか

Bさん

GND どうしをつなごう

Aさん





ボタンをおすと、相手のがめんに・・・



```
1  ?IN(1):LED  BTN():CONT  
RUN
```



0 と 1 だけで"ったわる？



```
1  ? IN ( 1 ) : LED  BTN ( ) : CONT  
RUN
```

げんきかどうか  
かくにんしよう



おちあうば"しよを  
ったえよう





A さんにこっそり教えるよ

B さんはふせてね



こうてい



B さんにこっそり教えるよ

A さんはふせてね





はしのした



やくそく = プロトコル



# UART プロトコル

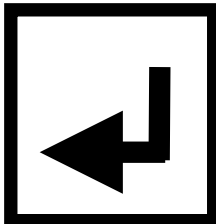
86 $\mu$ 秒で1文字(8bit)送信  
(1秒間に約1万文字)

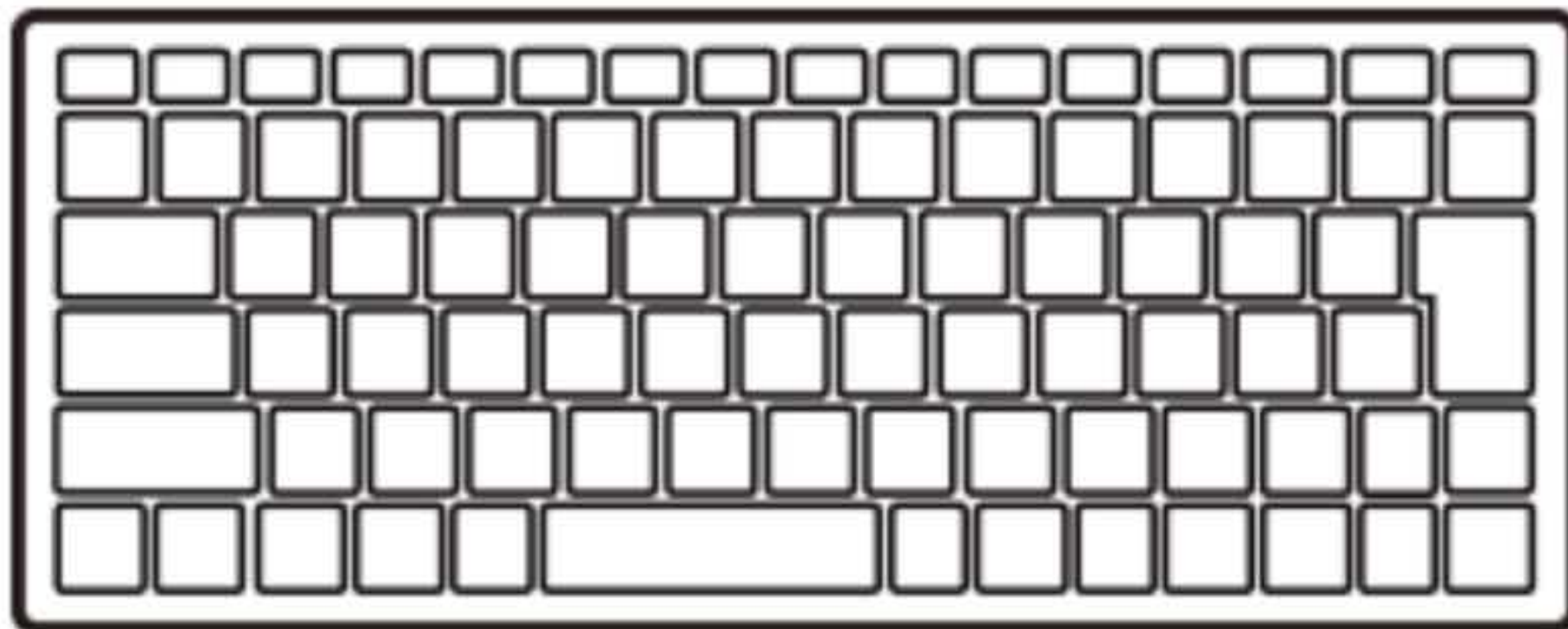


5G 10Gbps = 1秒間に1億文字  
1万倍速！



エラーをひょうじしない

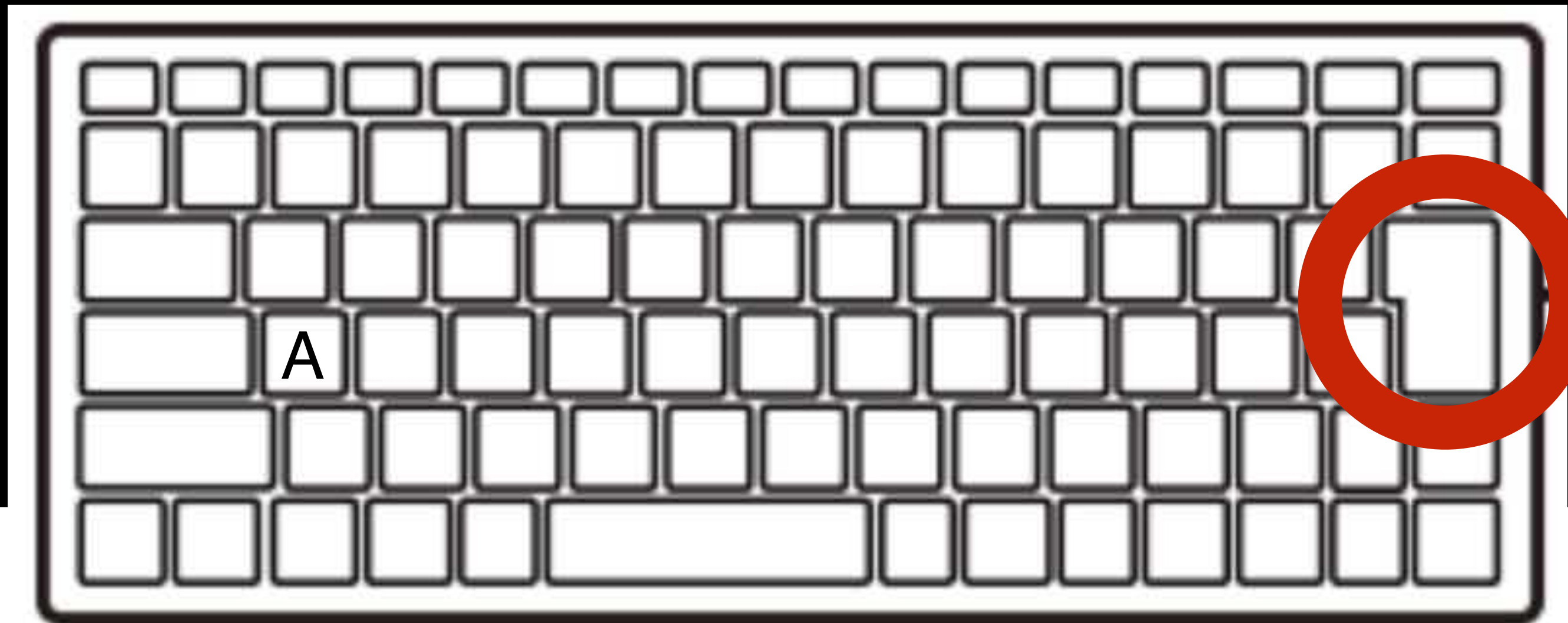
OK2 



どうなる？



IchigoJam BASIC  
OK  
AI



エンターキー

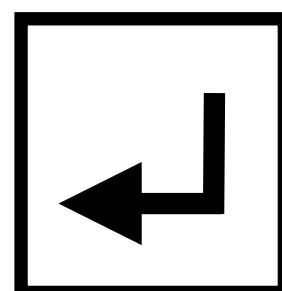
?



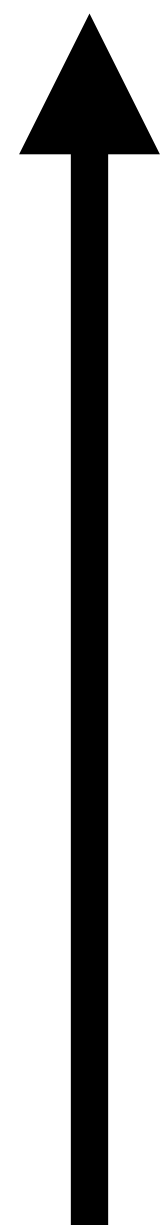
シラナイ

コトバハスルー

A

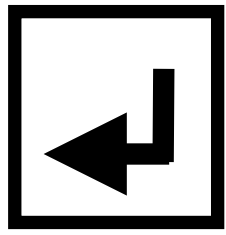


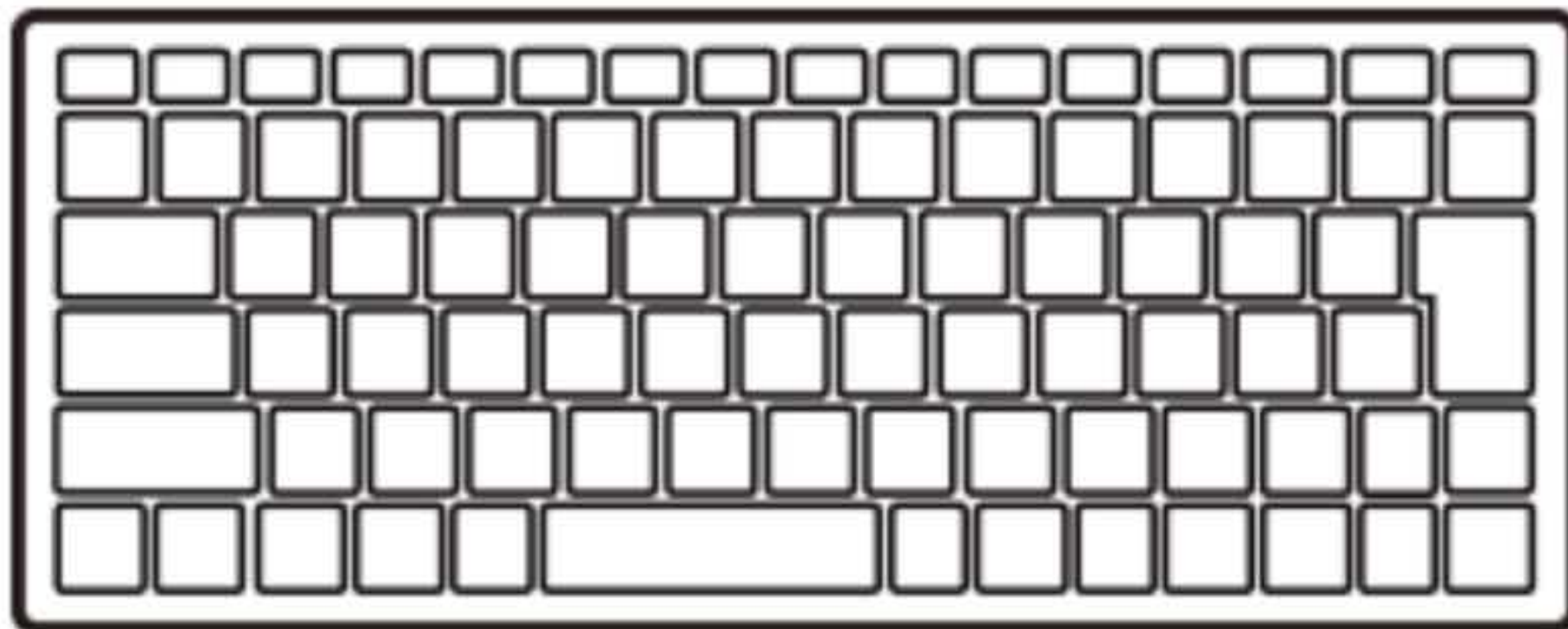
(エー、エンター)





エラーをひょうじする

OK 



OK!

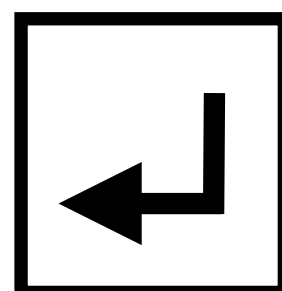


?



シラナイ  
コトバダナー

A

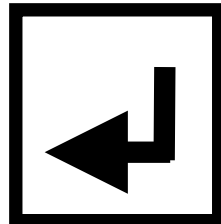


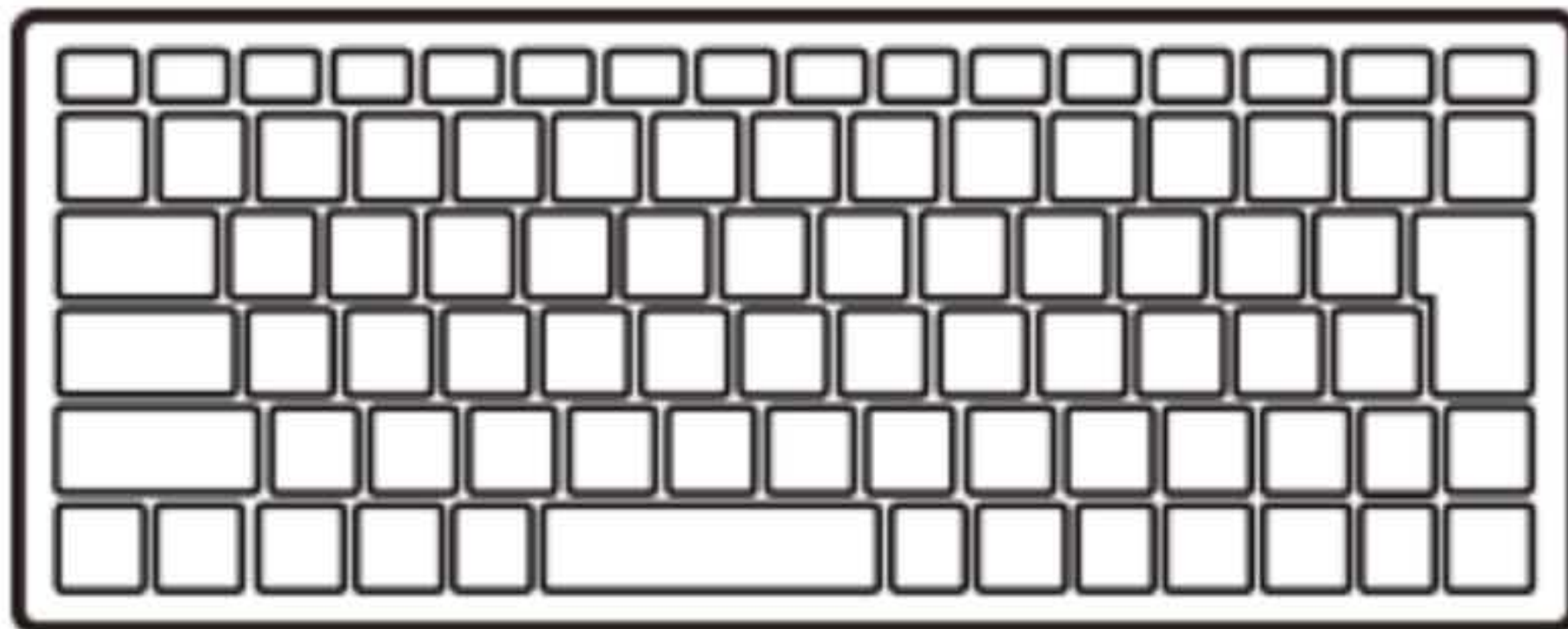
(エー、エンター)

Syntax error

(シンタックス エラー)

エラーをひょうじしない

OK2 



だまっとくよ！

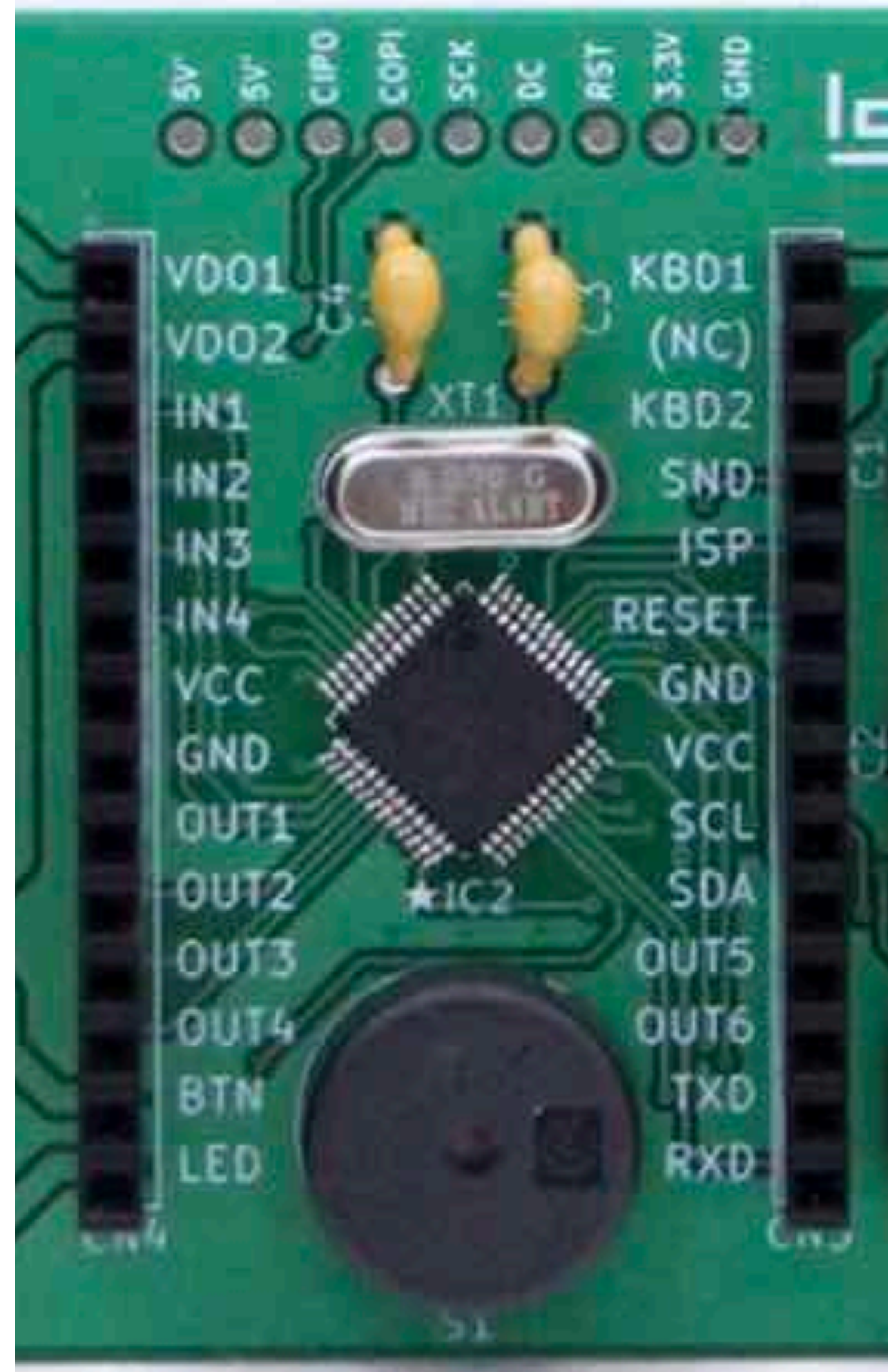




# ジャンパーせん、IN1からぬく



VIDEO1  
VIDEO2  
**IN1**  
IN2  
IN3  
IN4  
VCC  
GND  
OUT1  
OUT2  
OUT3  
OUT4  
BTN  
**LED**

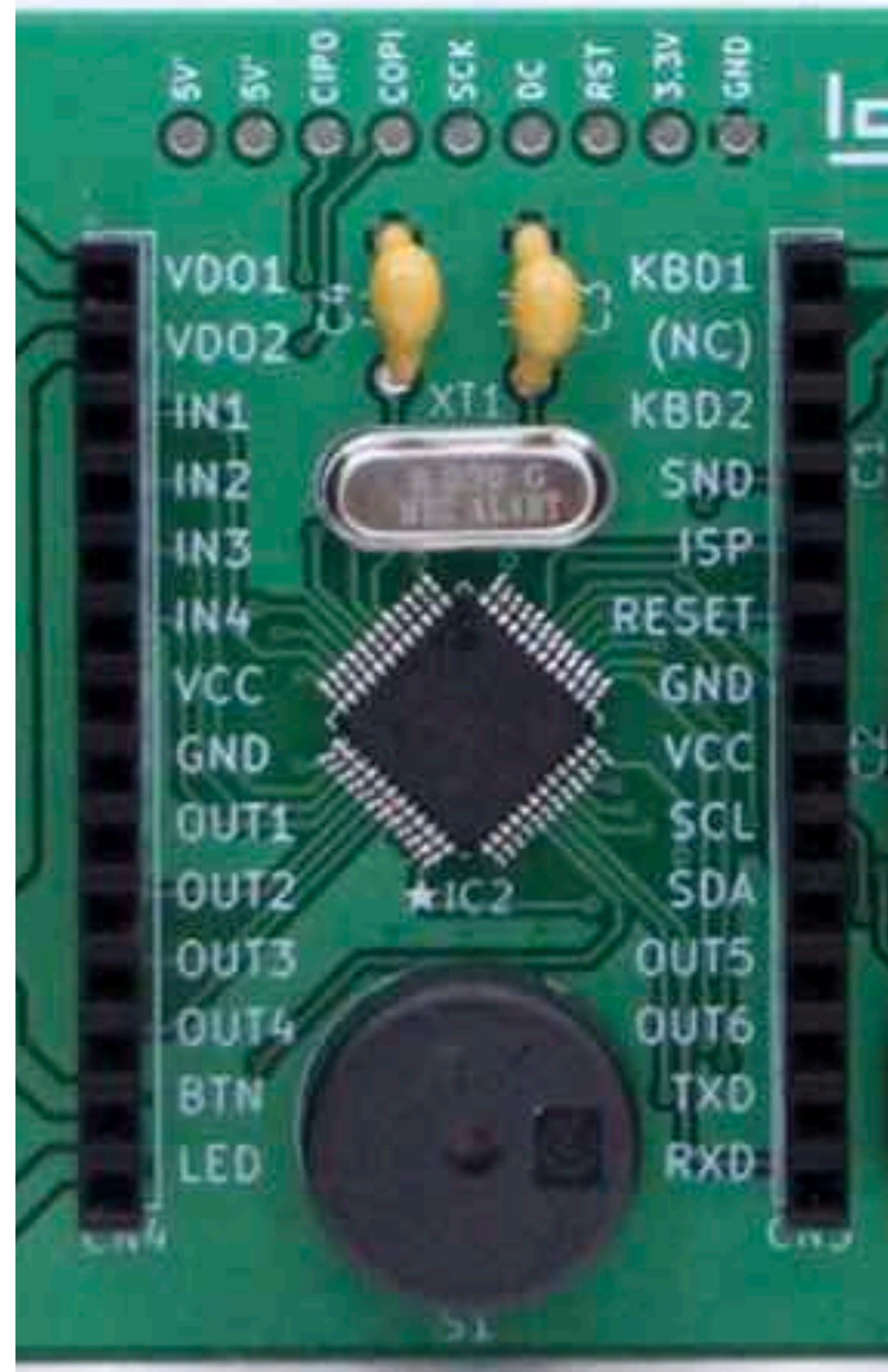


KBD1  
(NC)  
KBD2  
SOUND  
ISP  
RESET  
GND  
VCC  
SCL  
SDA  
OUT5  
OUT6  
TXD  
RXD



# ぬいたジャンパーせんをRXDにさしかえる

VIDEO1  
VIDEO2  
**IN1**  
IN2  
IN3  
IN4  
VCC  
GND  
OUT1  
OUT2  
OUT3  
OUT4  
BTN  
**LED**

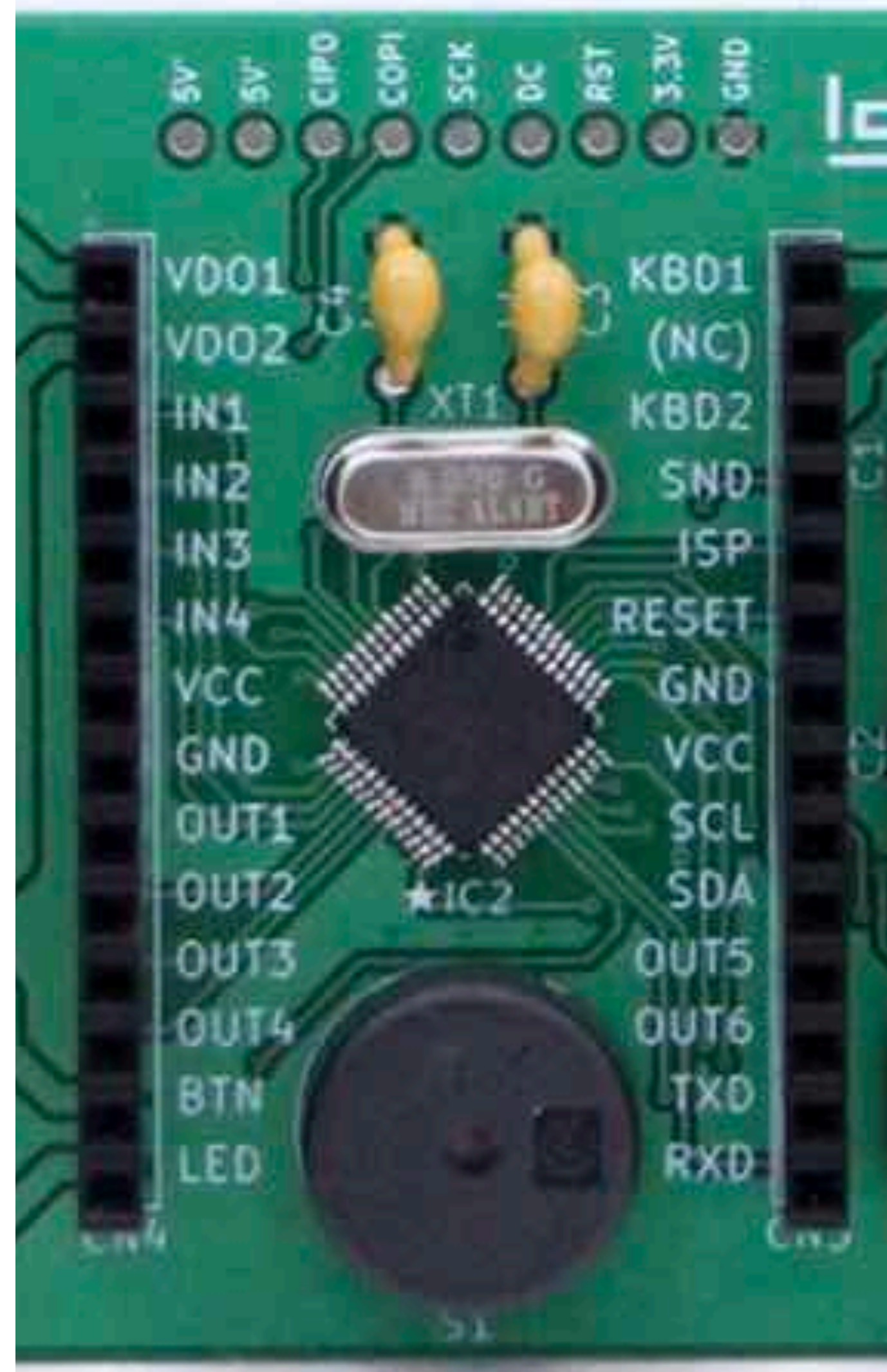


KBD1  
(NC)  
KBD2  
SOUND  
ISP  
RESET  
GND  
VCC  
SCL  
SDA  
OUT5  
OUT6  
TXD  
RXD



# ジャンパーせん、LEDからぬく

VIDEO1  
VIDEO2  
IN1  
IN2  
IN3  
IN4  
VCC  
GND  
OUT1  
OUT2  
OUT3  
OUT4  
BTN  
LED

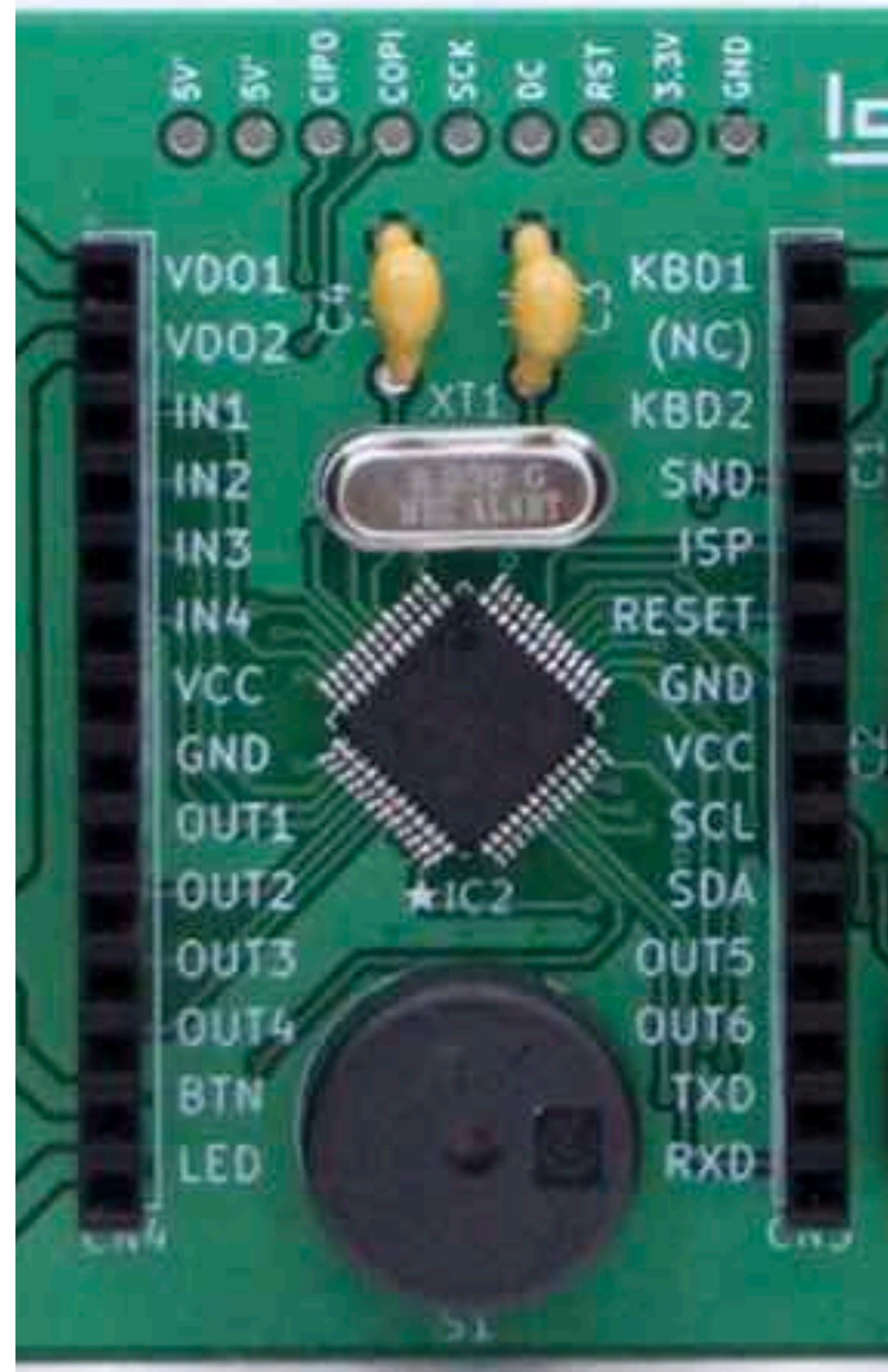


KBD1  
(NC)  
KBD2  
SOUND  
ISP  
RESET  
GND  
VCC  
SCL  
SDA  
OUT5  
OUT6  
TXD  
RXD



# ぬいたジャンパーせんをTXDにさしかえる

VIDEO1  
VIDEO2  
IN1  
IN2  
IN3  
IN4  
VCC  
GND  
OUT1  
OUT2  
OUT3  
OUT4  
BTN  
LED



KBD1  
(NC)  
KBD2  
SOUND  
ISP  
RESET  
GND  
VCC  
SCL  
SDA  
OUT5  
OUT6  
**TXD**  
RXD

A さん、おくってみよう

?" HI

B さん、 おくってみよう

? " LED1



A さん、おくってみよう

?" VIDEO4

Bさん、おくってみよう

?"LOAD@

B さん、 おくってみよう

? "LIST



A さん、おくってみよう

? " NEW : SAVE14

B さん、 おくってみよう

? " NEW : SAVE14

Bさん、まもってみよう

UART1, 0



A さん、おくってみよう

?"LED1

Bさん、まもりをかいじょ

UART1,1

A さん、おくってみよう

? "LED1



A さん、ま も っ て み よ う

UART1, 0

Bさん、おくってみよう

?"LED1

Aさん、まもりをかいじょ

UART1,1



B さん、 おくってみよう

? " LED1

# サイバーセキュリティ、守り方基本

受信、拒否

```
UART1, 0
```

受信、許可

```
UART1, 1
```

便利か怖いかは人間次第

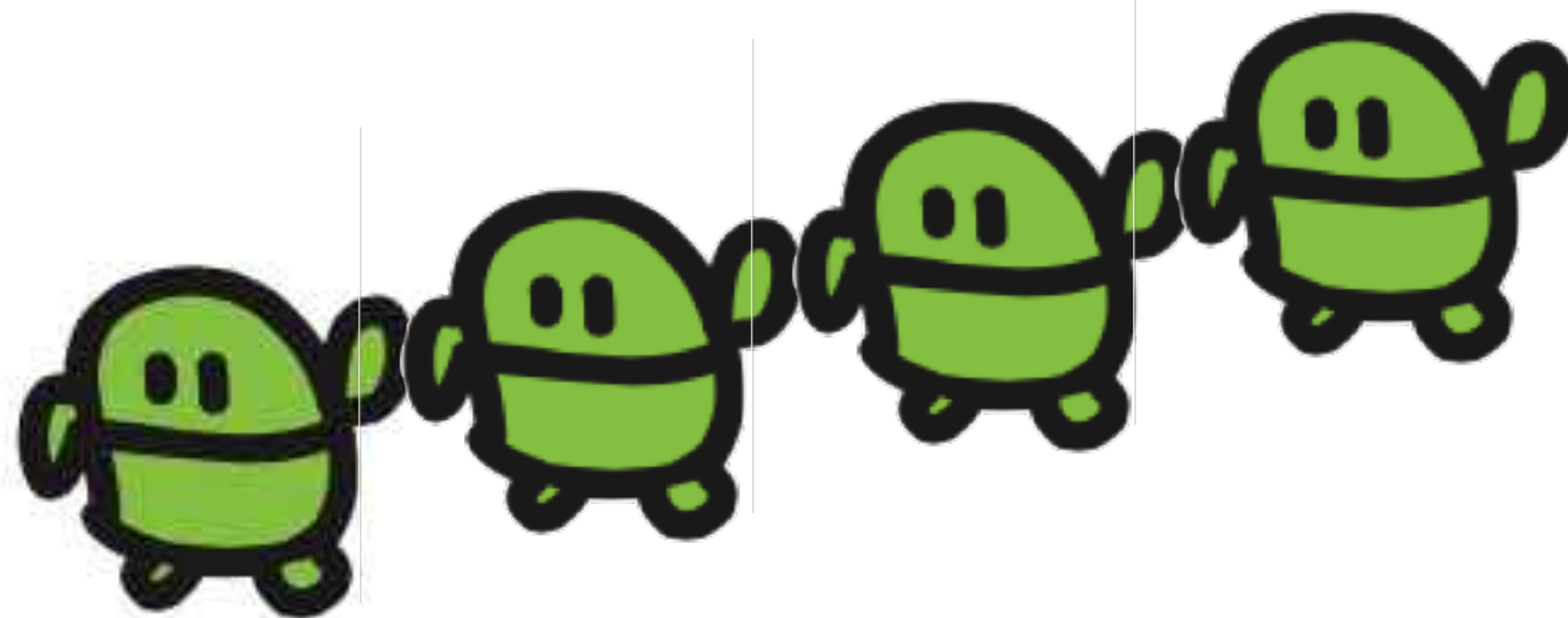


ソフトウェアが何ができるて  
どのようにつながっているか？

想像できること

インターネット

ネットワークとは  
コンピューターが  
つながったもの





インターネットは  
ネットワークが  
たくさんつながったもの

合計100おくらう

やってみよう！  
手紙のバケツリレー

## カメラでネット

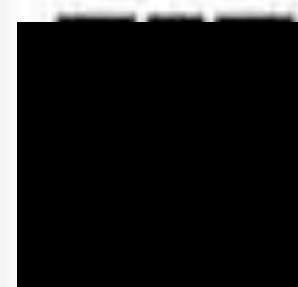
名前

宛先

本文

登録

共通鍵



QRコード読み込み

[src on GitHub](#) (with [Ango.js](#))



<https://code4fukui.github.io/cameradenet/>



暗号

カメラでネット

名前

ふくっち

宛先

だれか

本文

この文が読めるかな？

登録

1



名前	宛先	本文	
ふくっち	だれか	ゆほゝ	
ふくっち	だれか	ごは孝き読もれがに@	

ふたりできめた  
数をいれよう



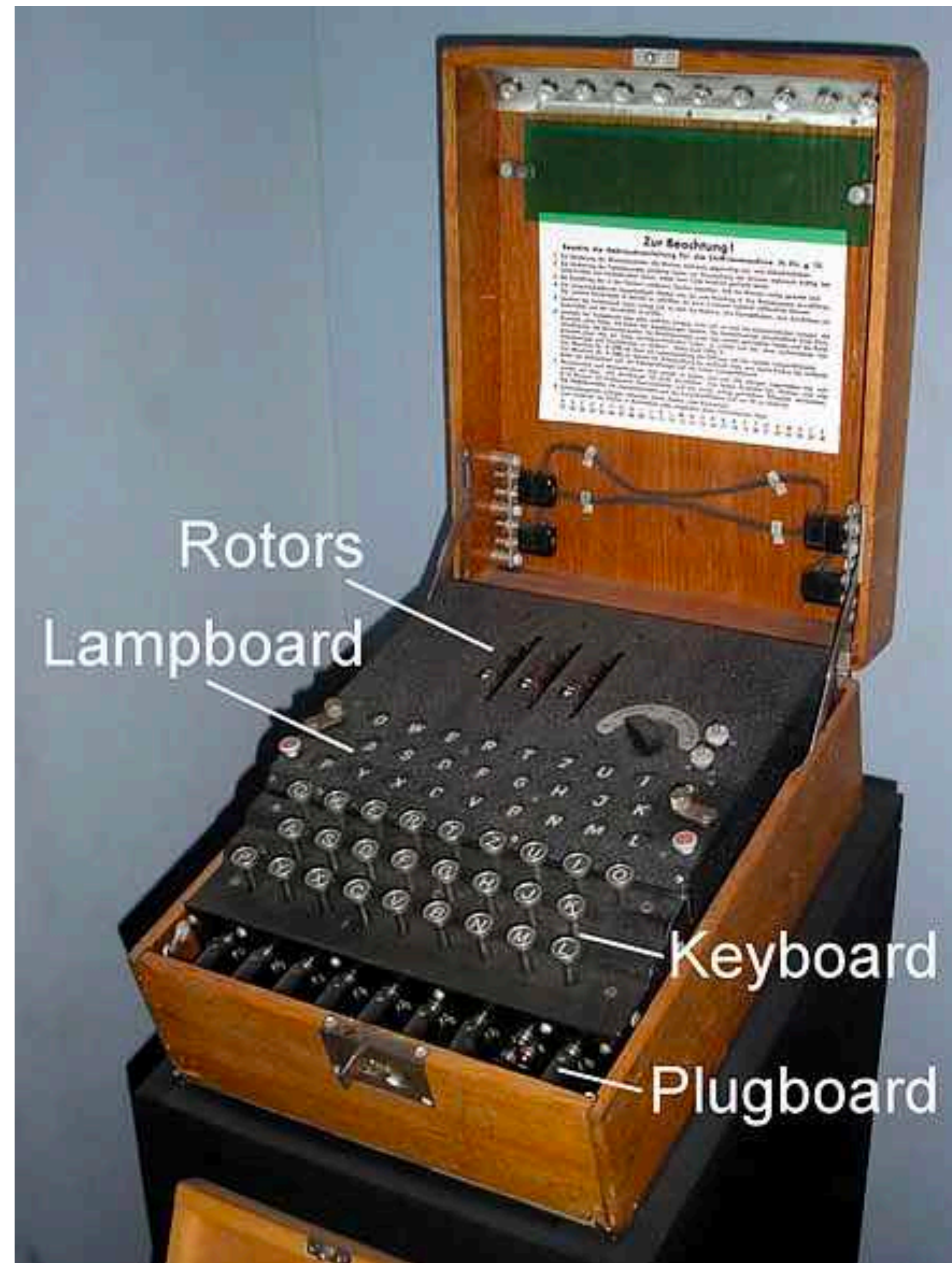
QRコード読み込み





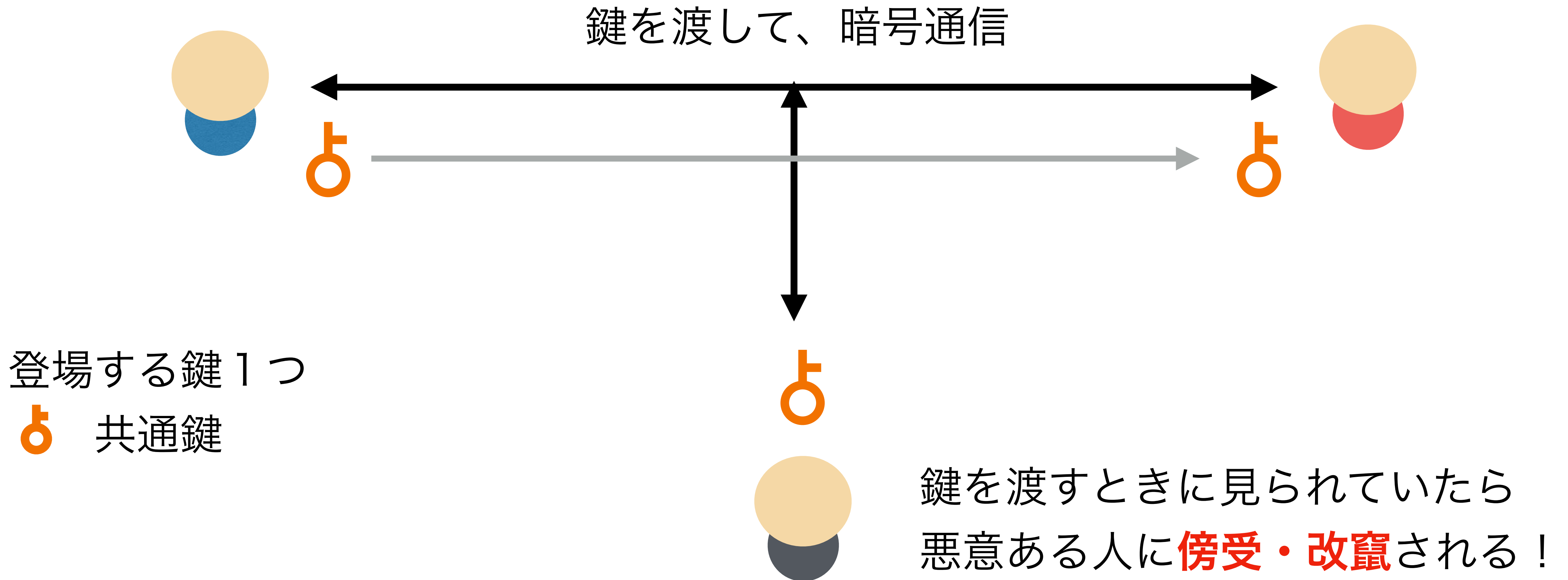
エニグマ (Enigma) とは、  
第二次世界大戦でナチス・ドイツが用  
いたローター式暗号機である。

名称はギリシア語「謎」に由来  
Wikipedia





# 共通鍵暗号



**安全に鍵を共有方法は？**

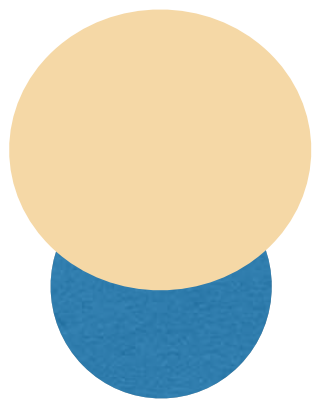
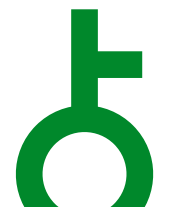
→ **大発明、公開鍵暗号**

鍵が2つ！



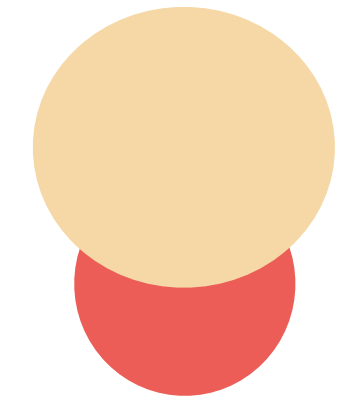
# 公開鍵暗号

Aさん公開鍵



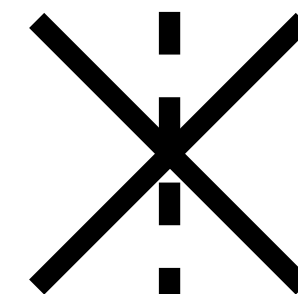
Aさん秘密鍵

Bさん公開鍵



Bさん秘密鍵

安心して通信したい

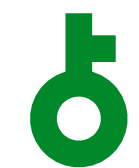


見られたくない

登場する鍵5つ



それぞれで生成される公開鍵



Aさんの公開鍵



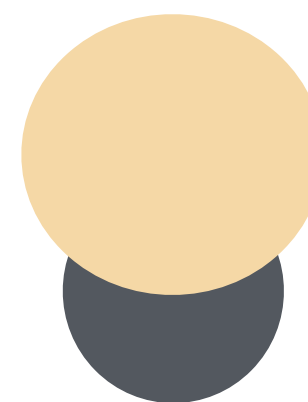
Aさんの秘密鍵



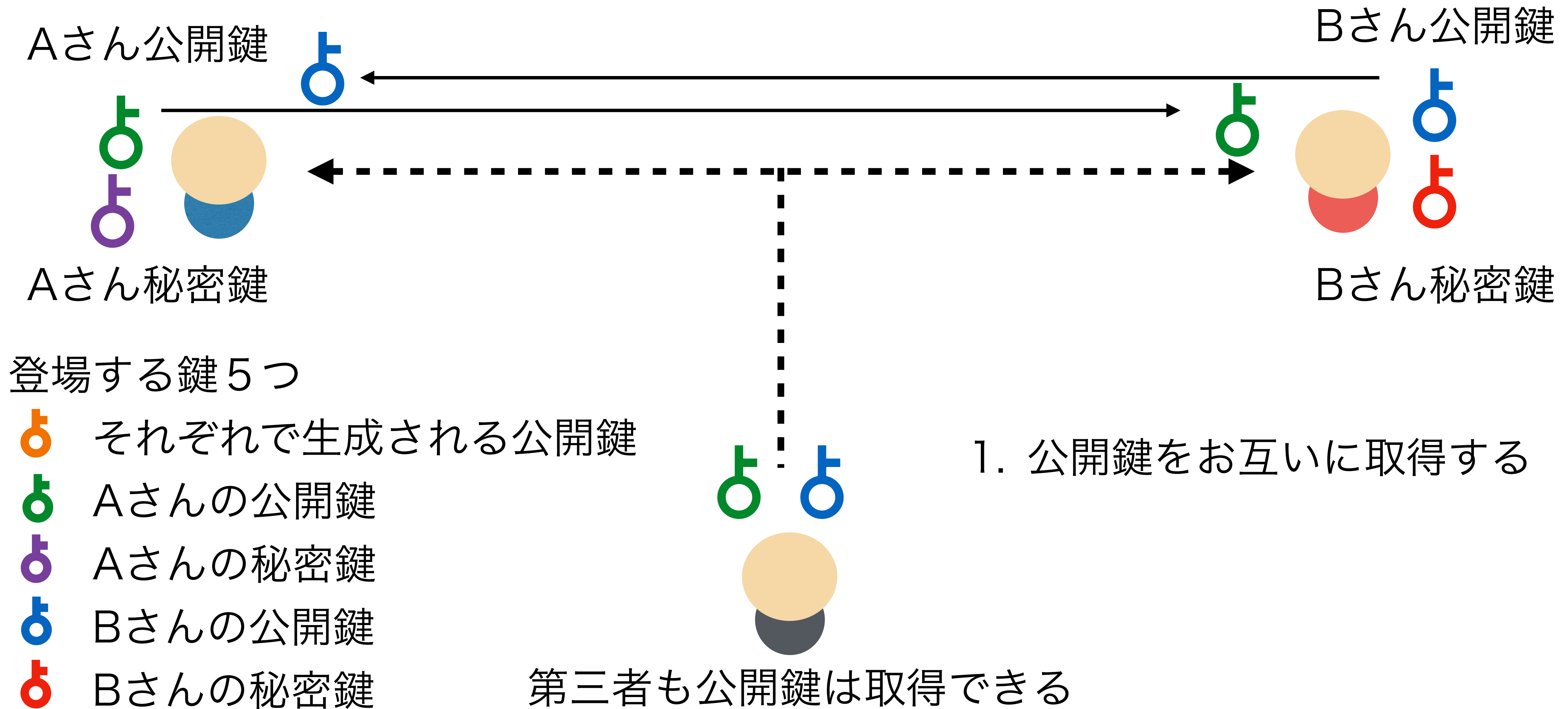
Bさんの公開鍵



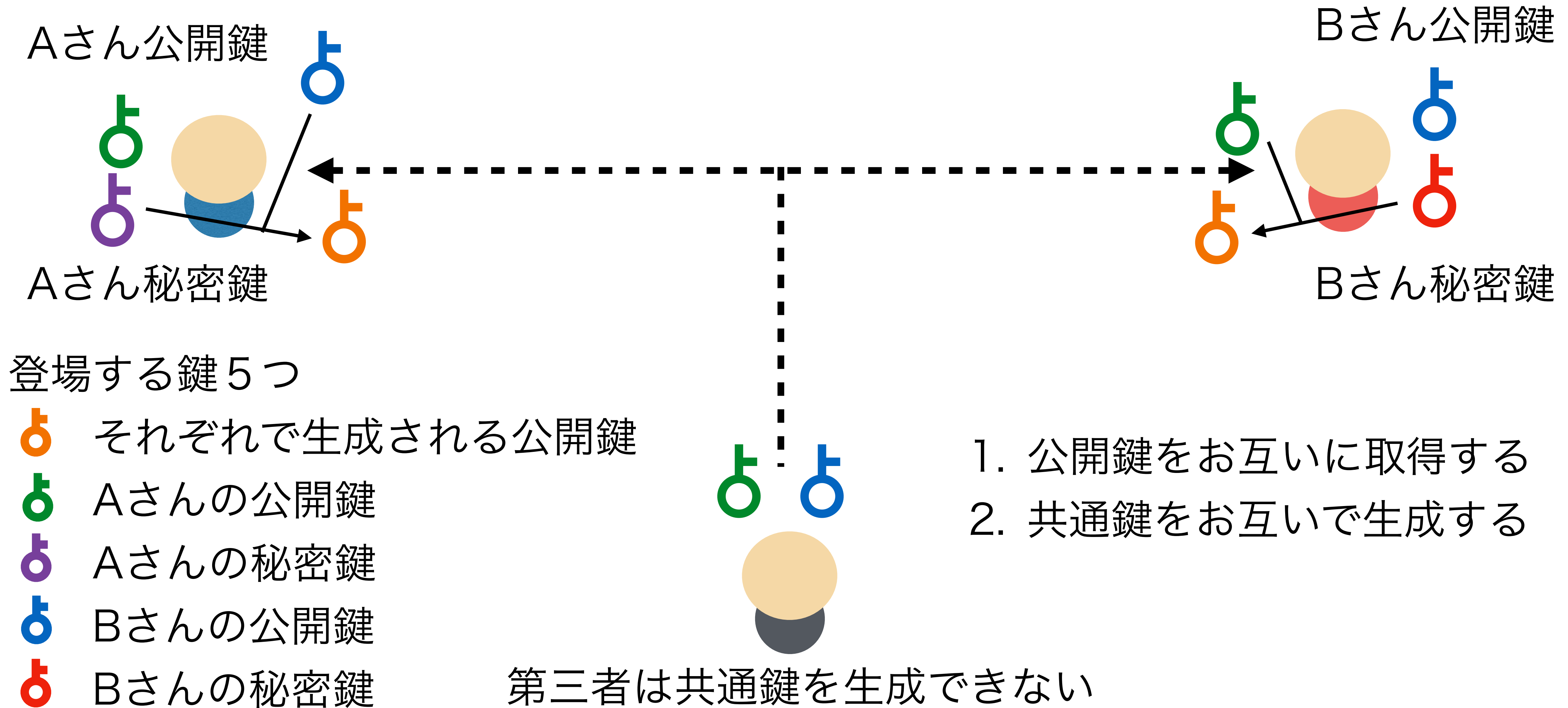
Bさんの秘密鍵



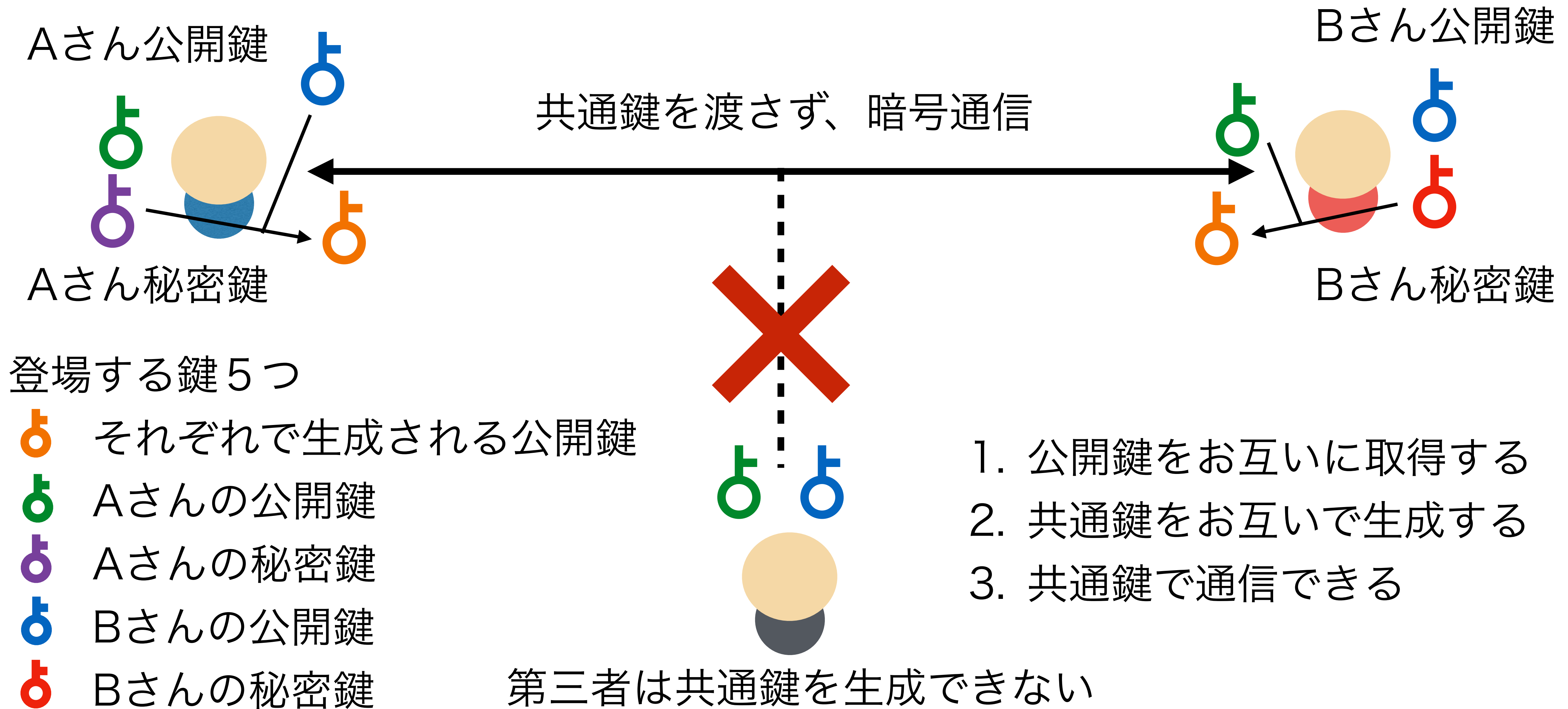
# 公開鍵暗号



# 公開鍵暗号



# 公開鍵暗号



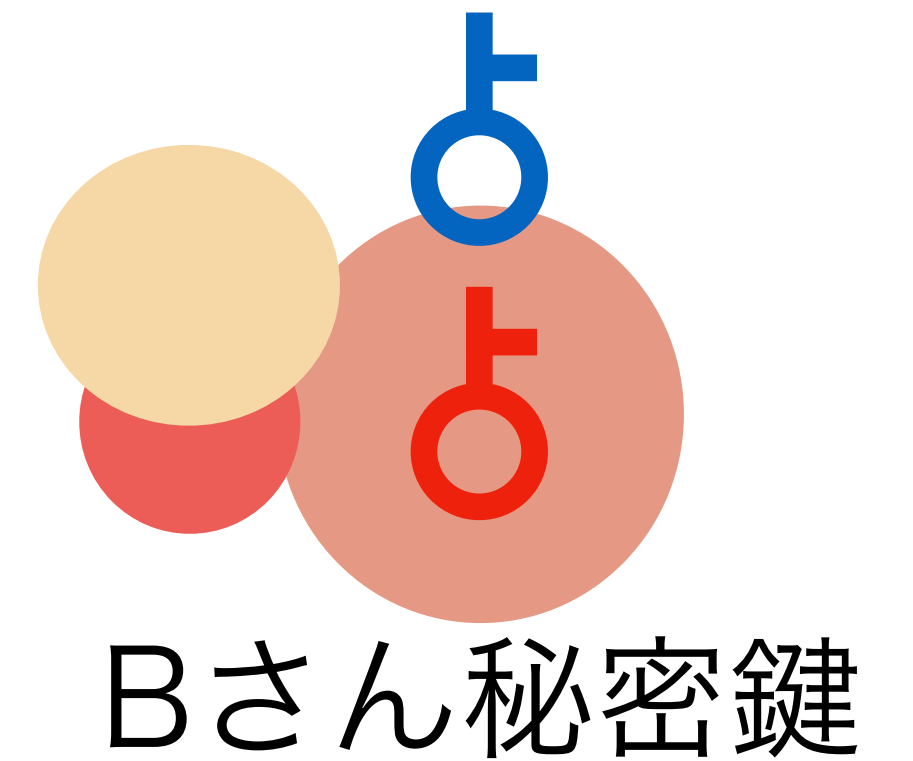


# 公開鍵暗号

Aさん公開鍵



Bさん公開鍵



秘密鍵は、その権限次第で  
実印以上に大事なデータ

# E2EE メッセージングヘルパー

既存の信用できない通信路を使った信用できる通信を実現する補助ツールです。

[Ed25519/X25519](#)でキーペアの生成と受け取った公開鍵から共通鍵の生成をし、共通鍵暗号 [AES-GCM](#) で暗号化復号化します。

本ページの読み込み後、サーバーとの通信はしません。[ソースファイル](#)でご確認ください。

1. キーペア（公開鍵と秘密鍵）をつくる

秘密鍵（誰にも見せてはいけない鍵）

公開鍵（相手に渡す鍵、公開してもOK!）

2. 相手の公開鍵（通信する相手から公開鍵をもらって書く、一人で試す場合→[新ウィンドウ](#)）

3. 通信用の共通鍵をつくる

共通鍵（ネットワークには流れていないけど、通信相手と同じ鍵）

メッセージ

暗号化→

←復号化

暗号

# やってみよう！

## E2EE

### End to End Encryption

## 「メッセージングヘルパー」 で検索

<https://code4sabae.github.io/e2ee/>

**公開鍵暗号の応用**

**→ 電子署名**



## 電子署名と検証の体験

1. **秘密鍵を生成する** ※秘密鍵は、10進法78桁の乱数です。自分だけの秘密にします。  
([Base32](#) 形式にしています)

秘密鍵 `WZ3H_YG2Q_3M9T_LE2D_1V84_736N_P95T_4YJC_MMCT_8JRT_F6L0_XZXN_84V0`

2. **公開鍵を生成する** ※公開鍵は、秘密鍵とペアになりますが、公開鍵から秘密鍵は推測不可能なので、誰に見せても大丈夫です

公開鍵 `ULQ5_AQCY_R4AV_4RP4_XQF6_UA30_6GAM_JWLR_19V8_JDVK_A5R0_FF1D_JRKH`

3. 電子署名したい文章を書く

文章 `あいう`

4. **電子署名を生成する** ※秘密鍵によって生成されるのであなたが書いた証明となります

電子署名 `TZA5_3KLT_2KGG_VLQA_DGZ8_NAT2_JXUD_MLMT_KXF0_2633_XZ24_GYWQ_CD3V_NZ30_LX3Z_KNN1_1YDE_RG4N_C2RL_8CD9_5MHK_ZEG4_FX6C_1M1N_7989_82H`

# やってみよう！



「電子署名と検証の体験」  
で、検索  
(Code for FUKUI)

<https://code4fukui.github.io/hanko/experience.html>



# デジタル庁で採用済み、公開鍵暗号技術によるトラスト（信頼）

＜ 戻る 接種証明書（日本国内用） ?

SMART®



氏名を表示する ▼

生年月日を表示する ▼

接種回数 **3** 回

最終接種日  
2022年03月20日

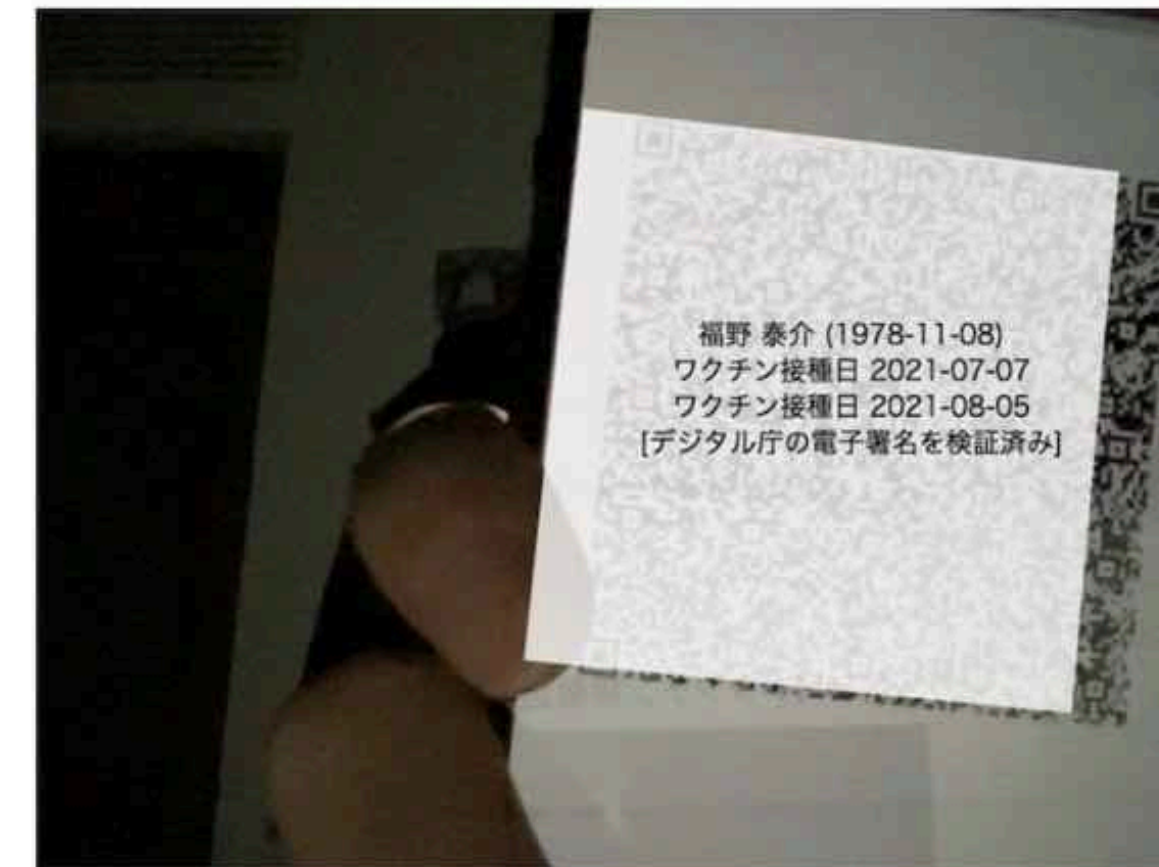
接種国  
日本

証明書ID  
182079-20220713-200005

発行日  
2022年07月13日

証明書発行者  
福井県鯖江市長  
日本国厚生労働大臣

高速ワクチン接種証明書チェッカー / vcchecker



福野 泰介 (1978-11-08)  
ワクチン接種日 2021-07-07  
ワクチン接種日 2021-08-05  
[デジタル庁の電子署名を検証済み]



普通のQRコードリーダーでは読めない→アプリ作成

生年月日、接種記録、公開鍵、電子署名が含まれる  
**デジタル庁の公開鍵**で検証可能

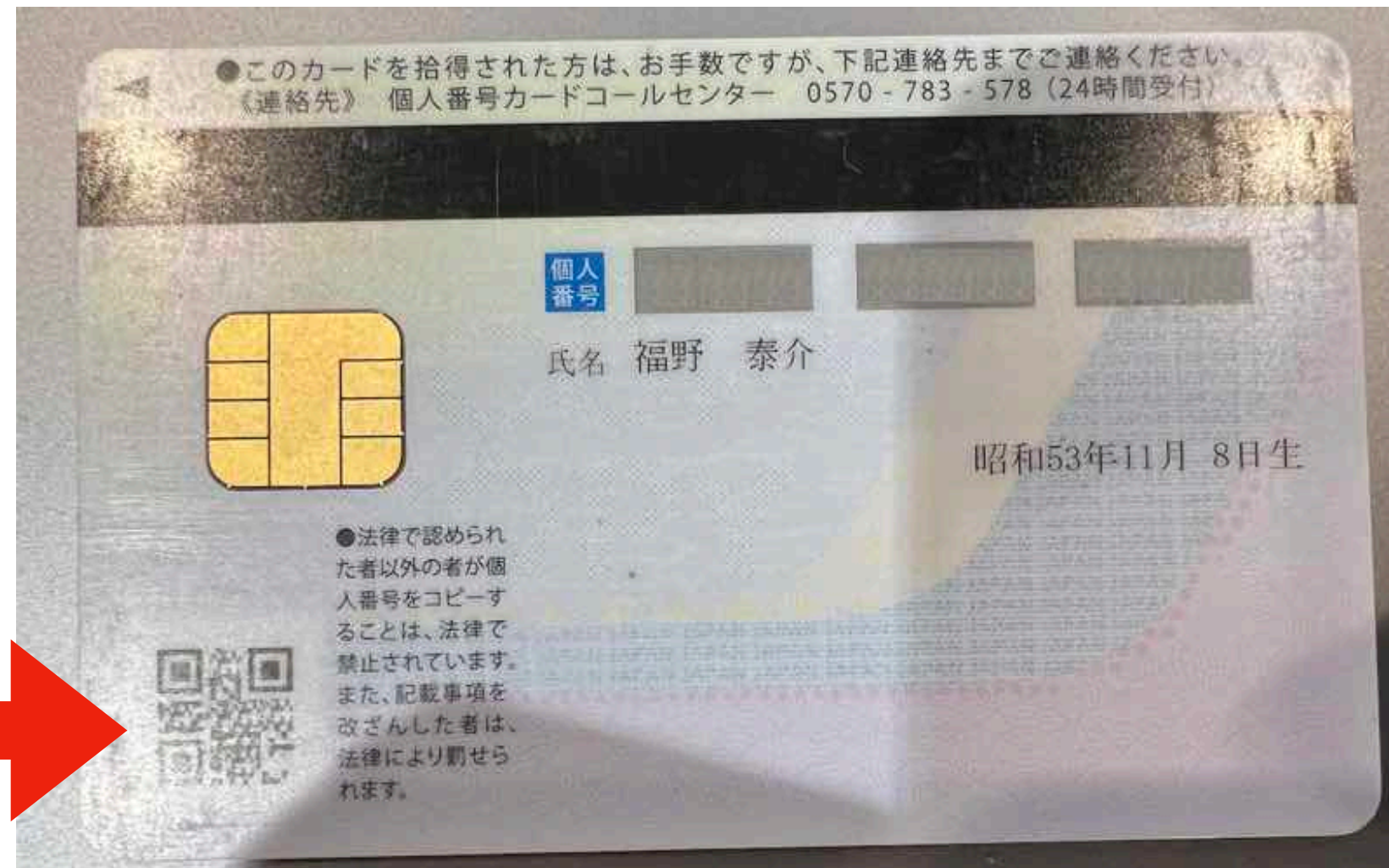
## 接種証明書のQRコードに含まれる電子署名で誰でも無料で検証可能



# マイナンバーカード

## 問題

- 秘密鍵を自分で作成できない
- マイナンバーが裏面に記載
- QRコードにもこそっと記載
- 電子証明書に関する説明がない



河野太郎  
9月26日 22:53

全ての国民の皆様には、マイナンバーカードの取得をお願いしています。

しかし、マイナンバーカードのセキュリティが不安だから取得したくないという声を伺いました。

そこで、マイナンバーカードのセキュリティについてご説明します。

マイナンバーカードには、ICチップが搭載されています。

このマイナンバーカードのICチップには、カードの券面に印刷されているあなたの情報（氏名、性別、生年月日、住所、顔写真、マイナンバー）のほか、あなたがあなたですよということを証明する電子的な鍵（公的個人認証の電子証明書）と、マイナンバーのもとになる番号（住民票コード）しか記録されていません。

あなたの年金や税などのプライバシー性の高い個人情報はマイナンバーカードには記録されません。

健康保険証として使用する場合も、あなたの特定健診結果や薬剤情報がICチップに入ることはありません。

ICチップの空き領域を使って、市町村等が独自のサービス（図書館カードでの利用等）を提供する場合でも、基本的に利用者番号以外は記録されません。

誰かがあなたのマイナンバーカードを拾って、情報を読み出そうとしても、あなたの設定したパスワードが必要となります。

パスワードを一定回数間違えると、自動的にロックがかかり、情報を読み出せないようになります。

また、不正な手段を使って情報を読み出そうとすると、ICチップが壊れ、やはり情報にアクセスすることができないようになっています。

ですからマイナンバーカードを取得することで、あなたの個人情報が流出してしまうようなリスクが高まることはありません。

万一、マイナンバーカードに暗証番号を貼り付けて財布に入れ、それを紛失してしまったような場合でも、利用を一時停止するために、24時間365日体制で、フリーダイヤル（0120-95-0178）を受け付けているので安心です。

では、なんでマイナンバーカードの取得をお願いしているのでしょうか。

マイナンバーカードには、大きく分けて三つの利用目的があります。

まず、1枚で本人確認とマイナンバーの確認ができる顔写真付きの公的身分証明書です。

行政機関や金融機関等で幅広く本人確認のための身分証として使うことができます。

また、就職、転職、出産一時金や育児手当、高額医療費の補助申請、年金受給、災害等、マイナンバーの提示が必要となる多くの場面で、マイナンバーカード一枚で本人確認とマイナンバーの確認ができます。

マイナンバーカードの表面にはマイナンバーは記載されていません。

[https://www.facebook.com/permalink.php?](https://www.facebook.com/permalink.php?story_fbid=pfbid02iBZQ5PfPV2ENH34u3ofrY8Bbe6EmGFdF5cCWoA1yYnXK3AfVUDLP9xuLJ3i1m5ptl&id=100044425659806)

[story\\_fbid=pfbid02iBZQ5PfPV2ENH34u3ofrY8Bbe6EmGFdF5cCWoA1yYnXK3AfVUDLP9xuLJ3i1m5ptl&id=100044425659806](https://www.facebook.com/permalink.php?story_fbid=pfbid02iBZQ5PfPV2ENH34u3ofrY8Bbe6EmGFdF5cCWoA1yYnXK3AfVUDLP9xuLJ3i1m5ptl&id=100044425659806)



**公開鍵暗号、スゴイ！**

インターネットは  
ネットワークが  
たくさんつながったもの

合計100おくらう



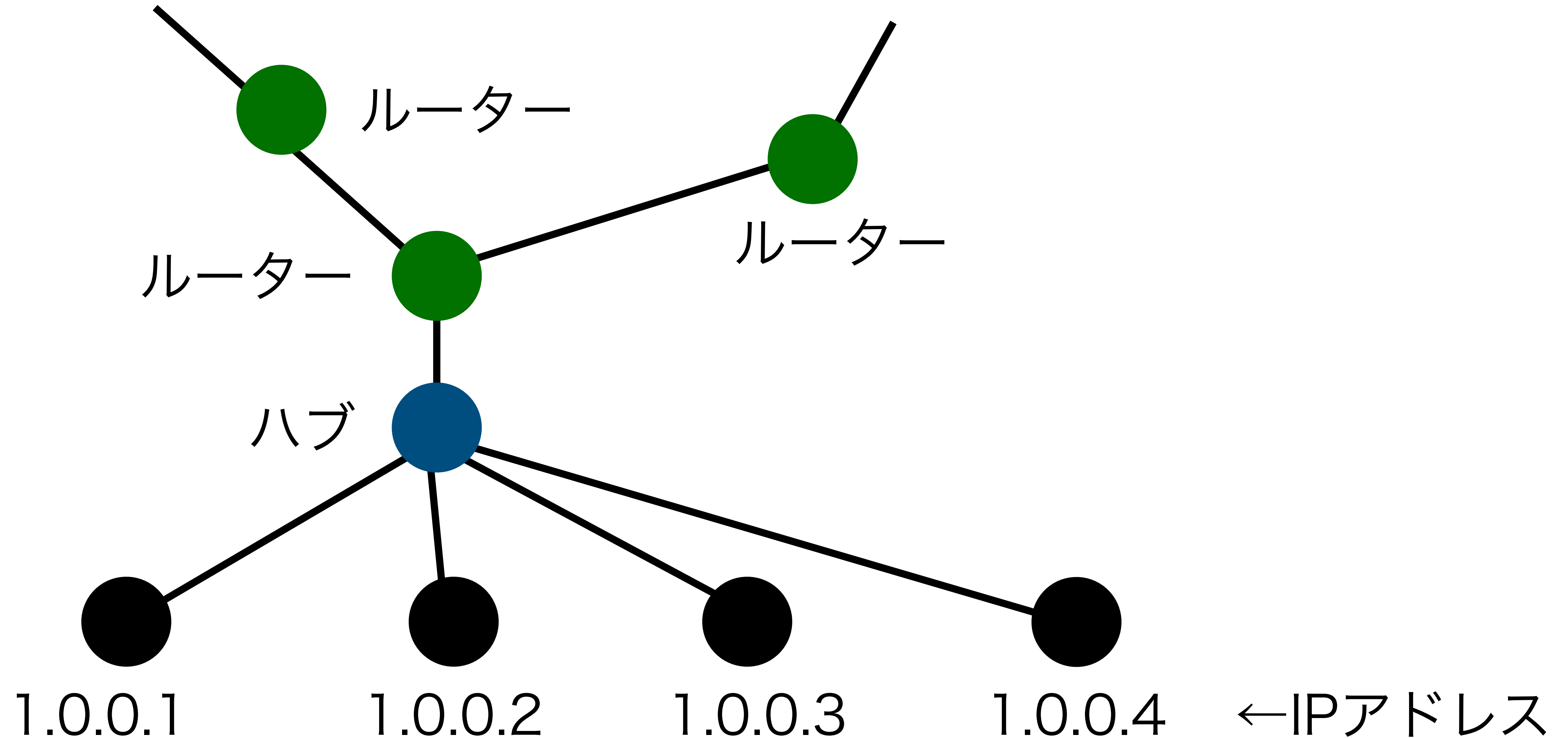
# IPv4

since 1978

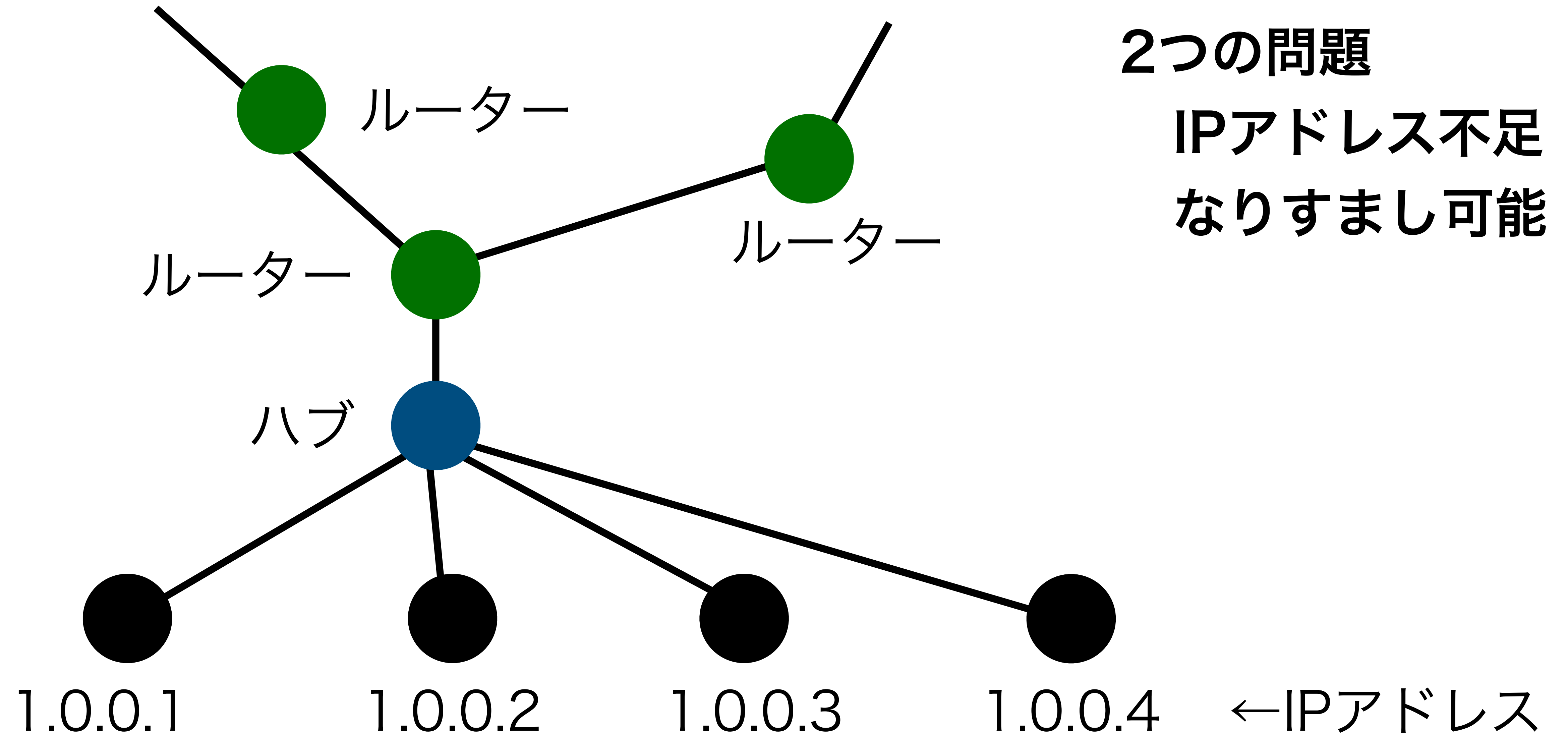
インターネット上の住所

IPアドレス

# IPv4のインターネット（32bit、4byte、最大43億アドレス）



# IPv4のインターネット（32bit、4byte、最大43億アドレス）





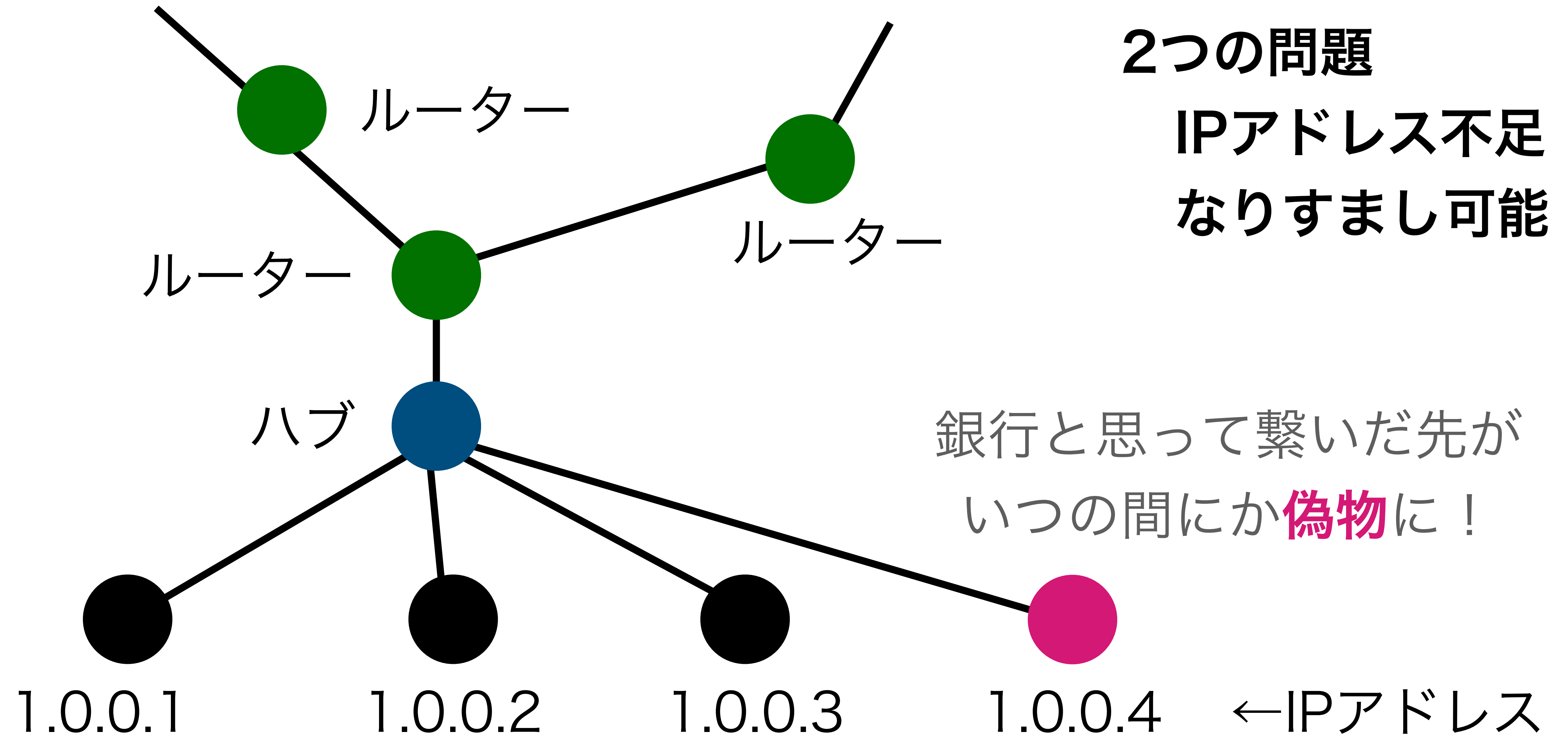
世界人口は何人？

# 世界人口は何人？

→ 80億人 > 43億IPアドレス

2022年79.5億人(+0.8億人/年)

# IPv4のインターネット（32bit、4byte、最大43億アドレス）



どう解決する？

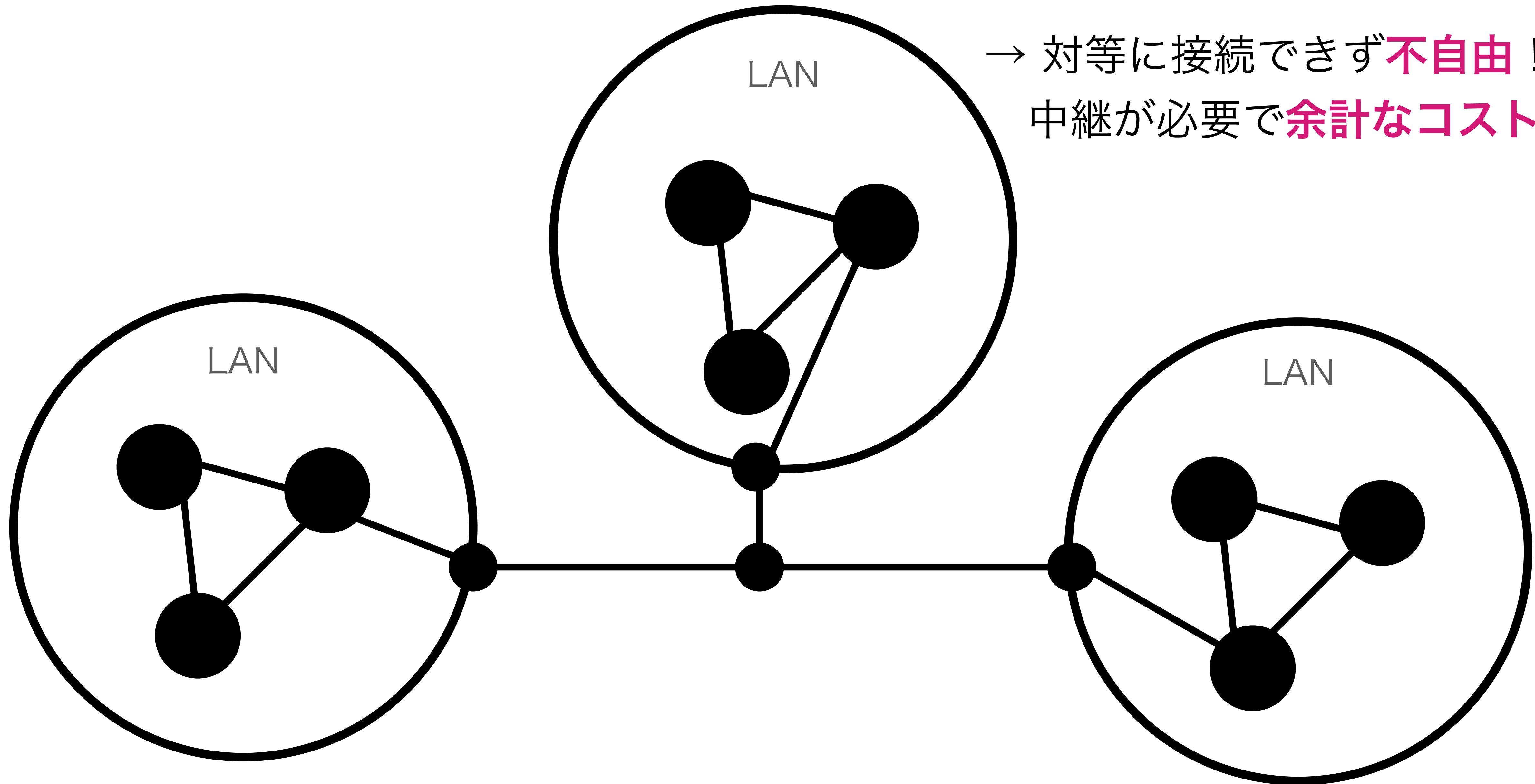


今までの解決方法

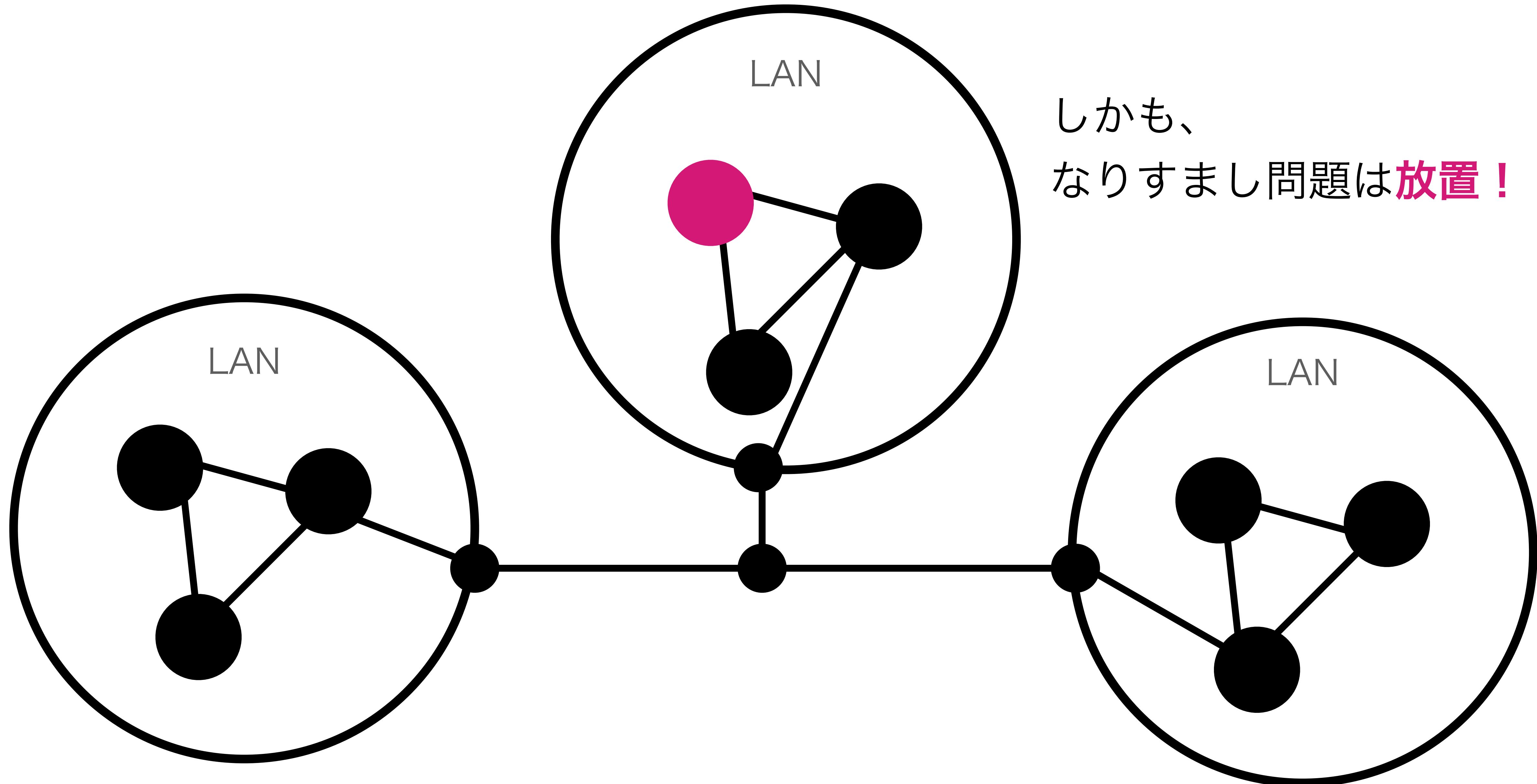
**今までの解決方法**

**→ 境界型セキュリティ**

境界型セキュリティ = LANに閉じて、LAN内は**信用しちゃう作戦**



境界型セキュリティ = LANに閉じて、LAN内は**信用しちゃう作戦**





IPv6?

# IPv6で数の問題だけ解決

	IPv4	IPv6
アドレス数	43億 (32bit = $43 \times 10^8$ )	340澗 (128bit = $340 \times 10^{36}$ )
なりすまし	可能	可能

「なりすまし」問題は未解決

# 信頼と運用に問題がある今のインターネット

1. すべての人々の人権と基本的自由を保護する。
2. 情報の自由な流れを促進するグローバルなインターネットを推進する。
3. すべての人々がデジタル経済から利益を得られるよう、包括的で安価な接続性を促進する。
4. プライバシーの保護を含め、グローバルなデジタルエコシステムへの信頼を促進する。
5. すべての人の利益のためにインターネットを稼働させ続けるガバナンスに対するマルチステークホルダーアプローチを保護し、強化する。  
  
(実現したい、未来のインターネット)

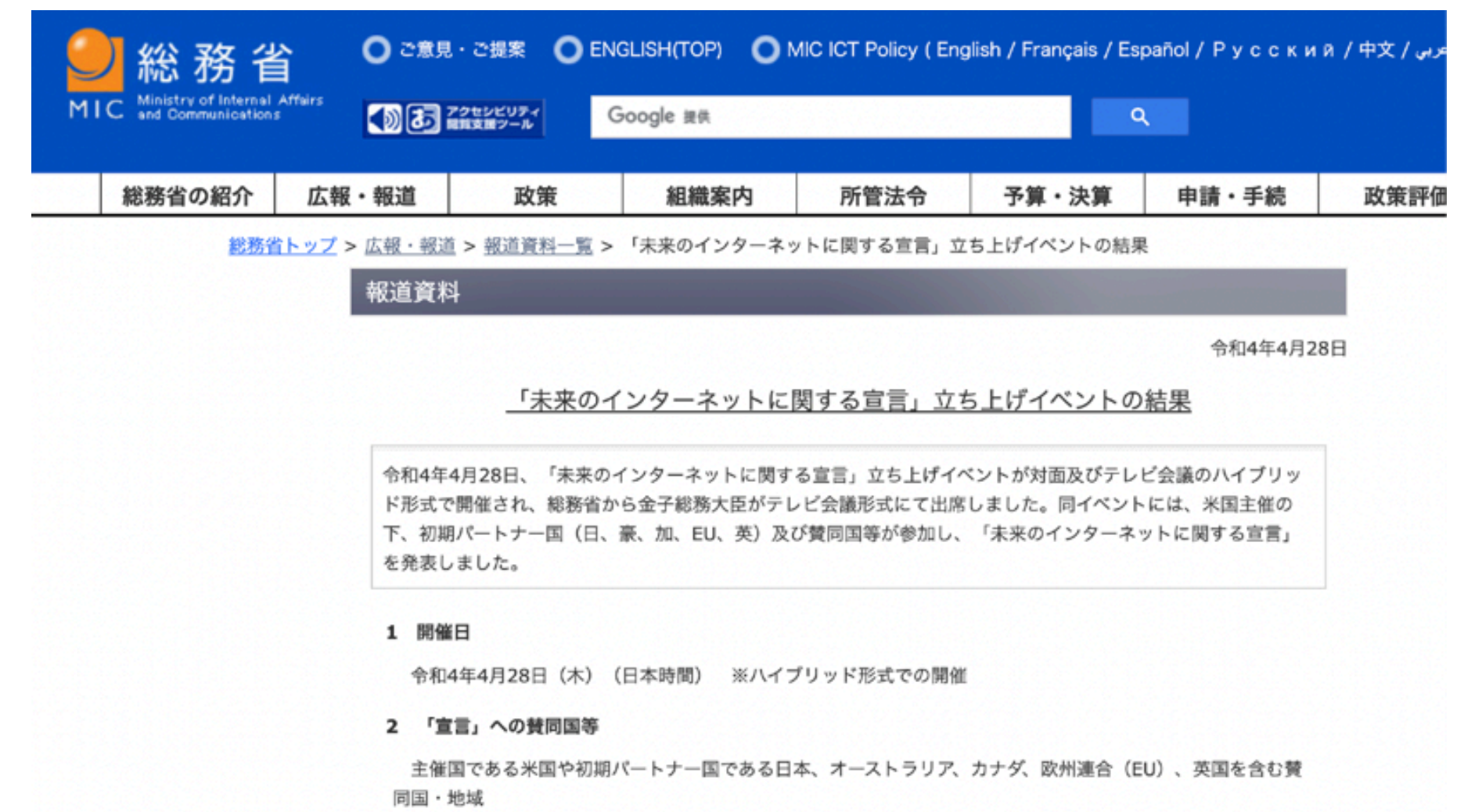
2022.4.28 アメリカ政府が発表

「A Declaration for the Future of the Internet」

日本を含む、61の国や地域が署名



<https://www.state.gov/declaration-for-the-future-of-the-internet>



[https://www.soumu.go.jp/menu\\_news/s-news/01tsushin06\\_02000235.html](https://www.soumu.go.jp/menu_news/s-news/01tsushin06_02000235.html)

(和訳、未来のインターネットに関する宣言)



# 日本ネットワークインフォメーションセンター(JPNIC)で 指摘される問題点

JPNICはインターネットの円滑な運営を支えるための組織です

 一般社団法人 日本ネットワークインフォメーションセンター  
Japan Network Information Center

WHOIS 検索 | サイト内検索 | WHOISとは? | JPNIC WHOIS Gateway

ホーム | ? Q&A | サイトマップ | アクセス | A A A | EN

JPNIC

IPアドレス・AS番号

JPNIC会員

[トップページ](#) > [ライブラリ](#) > [ニュースレター](#) > [バックナンバーオンライン版](#) > [No.54](#)

言語を選択 ▼

JPNICとは

IPアドレス

インターネットの基礎

ドメイン名

インターネットガバナンス

インターネットの技術

インターネットの歴史・統計

ライブラリ

トピックスとお知らせ一覧

Web更新履歴一覧

Q&A

イベントカレンダー

WHOIS

イベント・講演会資料

メールマガジン

ニュースレター

JPNIC公開文書ライブラリ

会議資料

インターネット白書

執筆記事

調査報告書

## ニュースレターNo.54/2013年7月発行

### IPv6セキュリティ ～問題点と対策～

今回のインターネット10分講座では、IPv6環境におけるセキュリティ問題について、代表的な問題点を挙げ、その対策や緩和策を解説します。

#### 1. はじめに

現在、IPv6に対応したネットワーク機器やサービスの普及が進みつつありますが、このIPv6環境におけるセキュリティ問題およびその対策・緩和策については広く理解されているとは言えません。本稿では、その理解の一助となるよう、IPv6環境のセキュリティについての誤解を取り上げた後、IPv6環境における代表的なセキュリティ問題であるFirst Hop SecurityおよびIPv6移行・共存技術に関わるトンネルの問題について、その対策や緩和策を解説します。

#### 2. IPv6セキュリティについての誤解

まず、IPv6に関するセキュリティ上の誤解について、取り上げておきます。

##### 2.1 IPv6環境でのIPsecについての誤解

よくある誤解として「IPv6環境ではIPsec(Security Architecture for Internet Protocol)が使われるためIPv4環境よりも安全である」という声をよく聞きます。これはある意味では正しいのですが、ある意味では間違っていると思われます。確かに、

<https://www.nic.ad.jp/ja/newsletter/No54/0800.html>



そこで登場



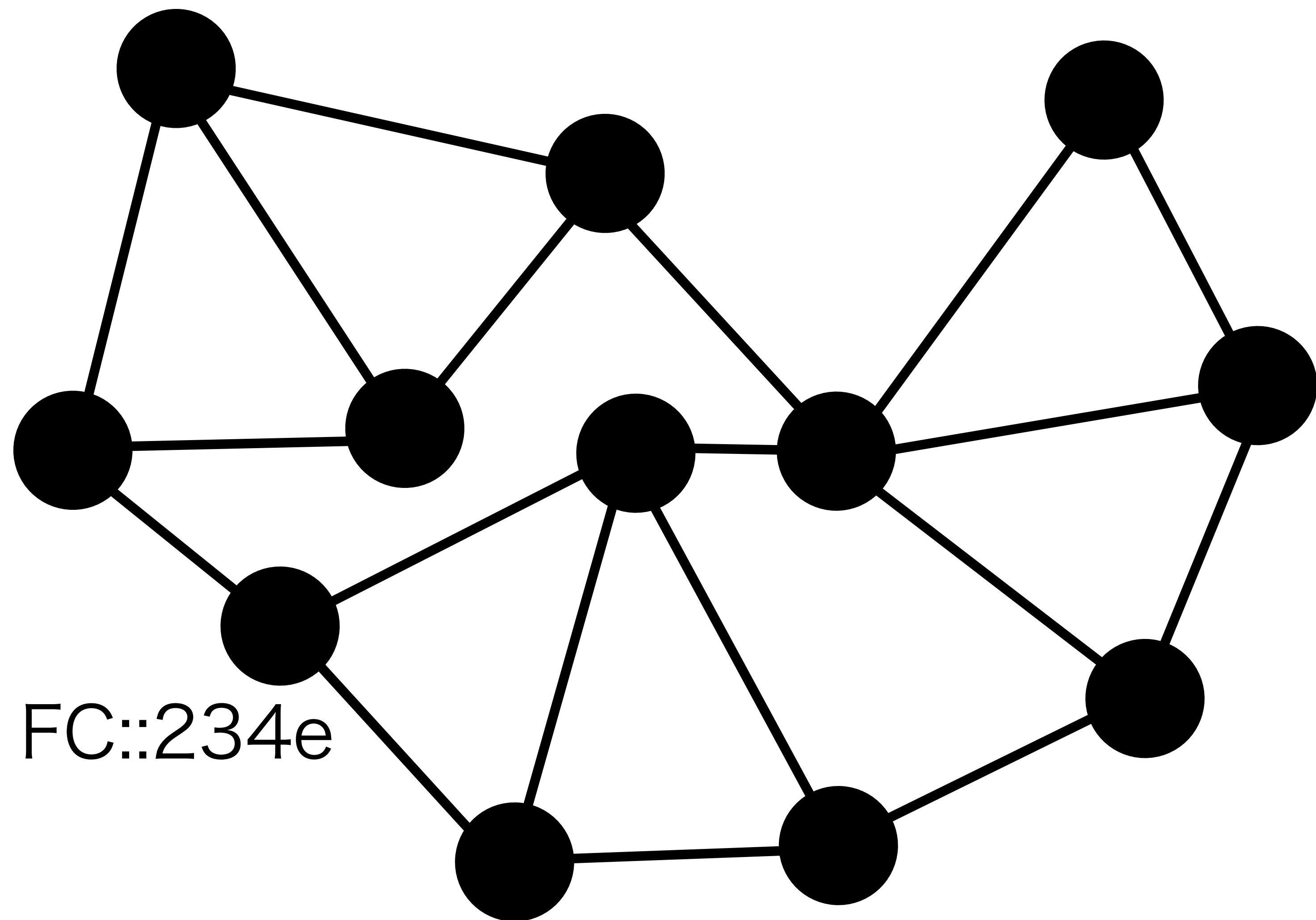
公開鍵暗号を活用したインターネット

# Internet3

EVER/IPで創る、安全安心安価な次世代インターネット

	Internet1 (IPv4)	Internet2 (IPv6)	Internet3 (EVER/IP)
十分なアドレス数	×	○	○
通信の暗号化	×	△	○
信頼できるIPアドレス	×	×	○
人で不要の運用	×	×	○

EVER/IPのインターネット（120bit、最大1兆x1兆x1兆アドレス）



FC::234e

fc\*\*.\*\*\*.\*\*

fc\*\*.\*\*\*.\*\*

fc\*\*.\*\*\*.\*\*

←IPアドレス

世界中の全端末が  
一意の信頼できる  
IPアドレスで  
直接つながる  
なりすましのない  
インターネット

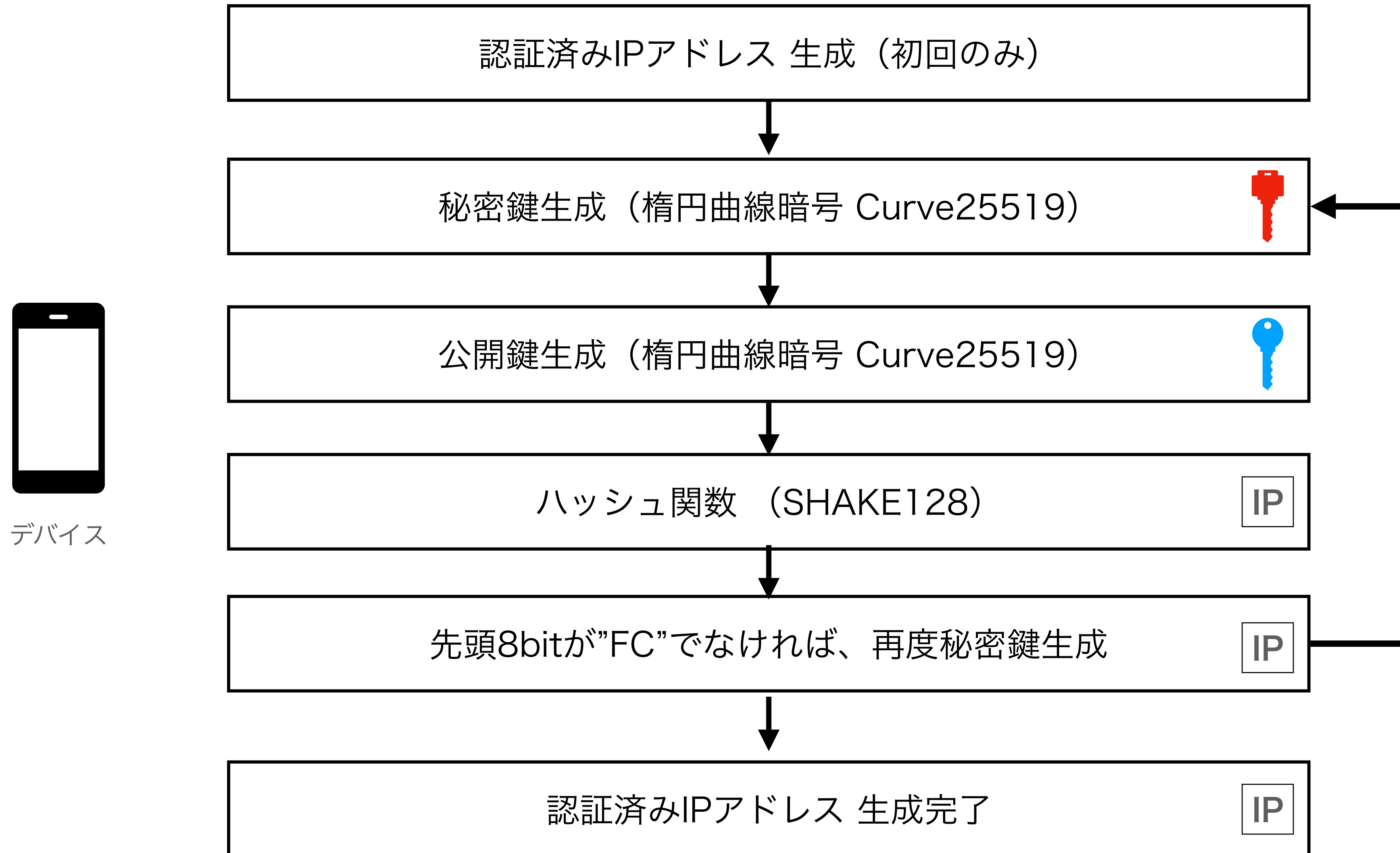


# アプリはいつも通りでOK！

OSI参照モデル	従来 Internet	Internet3
レイヤー7 アプリケーション層	アプリケーション	
レイヤー6 プレゼンテーション層	通信プロトコル  (HTTP / HTTPS)	
レイヤー5 セッション層		
レイヤー4 トラnsポート層	TCP / UDP	
レイヤー3 ネットワーク層	TCP/IP	必要な安全な通信 (EVER/IPが実現)
レイヤー2 データリンク層	MACアドレスなど	
レイヤー1 物理層	光ファイバー / WiFi など	

なぜなりすましができないか？

# IPアドレスが公開鍵で検証できるから







杉本知事

帝都久利寿

Internet3発明者  
帝都久利寿

福井県知事訪問  
&  
サイバーバレー  
宣言



安全の鍵は  
公開鍵暗号 と  $F=ma$



はやい

やすい

うまい

簡単、低コスト、高セキュリティ



第1位 HEXAGON

京都府立嵯峨野高等学校

スコア:181



<https://cybersakura.jp/>