Criminal IP ASM

ASMとDNSレコードから見る
外部攻撃対象領域管理

自社のデジタル登記簿謄本

Criminal IP

Criminal IP ASM

List

1. ASMの基礎

なぜIT資産の自動検出が必要なのか

2. DNSレコード

自社のIT資産を把握するための基本情報

3. 実際に確認された脅威

6つの公開リスク事例

4. セルフチェックリスト

14項目で確認する自社のセキュリティ対策状況

Criminal IP

01 ASMの基礎

なぜIT資産の自動検出が
必要なのか

ASMとは

Attack Surface Management – 攻撃対象領域管理

ASM (Attack Surface Management)とは、外部の攻撃者に狙われる可能性のある自社の「攻撃対象領域」を自動的に特定し、潜在的なセキュリティリスクを継続的に監視・管理するためのセキュリティプロセスです。

分かりやすく例えるなら、「自宅の塀にあるすべての隙間を24時間自動で見つけ出す監視カメラ」のようなものです。一度確認して終わるのではなく、日々新たに追加・変更されるIT資産を継続的に監視します。

セキュリティ担当者がExcelなどを用いて手作業で資産を管理する方法とは異なり、ASMは3つの主要なIT資産を自動的に検出し、それぞれの関連性を可視化します。

ASMによるIT資産検出の主な識別要素

IPアドレス	サーバーのIPアドレス	例: 59.7.xx4/24
ドメイン	自社名やブランド名に紐づくドメイン	例: example. co.jp
SSL/TSL 証明書	HTTPS通信の暗号化に使用されるTLS証明書	例: CN=example.co.jp

攻撃対象領域とは

攻撃者が自社のシステムへアクセスしたり、侵入を試みたりする可能性のある、外部に公開されたすべての接点を指します。ドメイン、IPアドレス、メールサーバー、TLS証明書、開放ポート、RDP・SSH・VPNなどのリモートアクセスサービス、Web管理画面、クラウド資産、既知の脆弱性などは、すべて攻撃対象領域に含まれます。

なぜ今、ASMが必要なのか

「Excelで管理しているIP資産が、すべてだと言い切れますか？」

多くの企業では、社内資料やExcelを使ってIT資産を管理しています。この方法は、把握済みのIPアドレスやドメイン、サーバー情報を整理するには有効ですが、変化し続ける外部公開資産をリアルタイムで反映するには限界があります。
特に、クラウド環境や一時的なテストサーバー、外部委託先が作成したサブドメイン、古いDNS設定などが混在する場合、実際の公開資産は社内の管理台帳より広範囲に存在する可能性があります。

公開DNS検索ツールを利用するだけでも、管理資料に記載されていないサブドメイン、IPアドレス、メールサーバー、ネームサーバー、TXTレコードなどが確認されることがあります。つまり、実際の攻撃対象領域は、自社が認識している範囲より広い可能性があります。

ASMの第一歩は、既存の資産台帳を整理することではなく、インターネットから見える自社資産を継続的に探索・特定することです。

社内で管理している資産一覧と、外部から観測される資産の範囲は、必ずしも一致するとは限りません。

自社が把握している資産

IT_assets_2026.xlsx

	A	B
1	www.example.co.jp	125.61.30.xx1
2	mail.company.co.jp	125.61.30.xx2
3	vpn.company.co.jp	125.61.30.xx3
4	....	

20件
(担当者がExcelで管理している資産)

攻撃者から見える資産

ASMで確認できる外部公開資産の例

```
www.example[.]co.jp
mail.company[.]co.jp
vpn.company[.]co.jp
oldshop.company[.]co.jp
dev2.company[.]co.jp
test-api.company[.]co.jp
backup-mail[.]company…
ec2-13-125-150-238……

and 492 more →
```

500+
(ASMで管理している自社資産)

ASN – 自社のインターネット上の領域

自律システム番号(Autonomous System Number)・IT資産を探索するための出発点

企業が保有するASNを確認することで、組織に割り当てられたIPアドレス帯やネットワーク範囲を把握できます。これは、外部公開資産を特定するための重要な手がかりです。企業には通常、複数の**IPアドレスをまとめた帯域(prefix)**　が割り当てられます。
例えば、/24のネットワークは合計256個のIPアドレスで構成され、ネットワークアドレスとブロードキャストアドレスを除く254個が利用可能です。

そのため、1つのASNに数百から数千以上のIPアドレスが含まれることもあります。企業規模が大きいほど、複数のASNや多数のIPアドレス帯を保有しているケースも少なくありません。
一方で、これらのIPアドレス帯がすべて社内の資産台帳に正確に反映されているとは限りません。

社内の管理資料に登録されていないIPアドレスや古いサーバー、テスト環境、外部委託先が構築したシステム、クラウドインスタンスなど、ASNの範囲内に存在する未把握の資産は、**シャドーIT**である可能性があります。

ASNとは

自律システム番号（ASN）とは、インターネット上で独自のルーティングポリシーを持つネットワークを識別するために割り当てられる固有の番号です。

シャドーITとは

シャドーITとは、IT部門やセキュリティ部門の正式な承認を受けず、管理体制の外で運用されているIT資産を指します。

ASNを起点としたIPアドレス帯の特定例

AS2xxx5	5 IPv4 prefixes
AS2xxx5	5 IPv4 prefixes
AS1xxx2	・・・
AS9xx3	・・・

```
59.x.xx4.0/24
59.x.xx5.0/24
61.4x.xx4.0/24
106.xxx.45.0/24
1xx.xx.201.0/24
```

数千件のIPアドレスが存在

例えば、企業が複数のASNを保有し、それぞれに複数の/24ネットワークが紐づいている場合、インターネット上で確認できるIP資産は数千件に及ぶことがあります。
一方、社内の資産台帳には、主要な運用サーバーや代表的なドメインしか記載されていないケースも少なくありません。

この差分、つまり**自社のネットワーク範囲内に存在しながら、社内で把握されていない資産**こそ、ASMで優先的に確認すべきリスク候補です。

02

DNSレコード

自社のIT資産を把握するための
基本情報

DNSレコードから読み解く外部IT資産の構造

ドメインに紐づく情報を記録した公開台帳

不動産を契約する際には、所有者や抵当権、差し押さえの有無を確認するために、登記簿謄本を確認します。
DNSレコードは、いわばIT資産の登記簿謄本です。どのサーバーがどのドメインに接続されているのか、メールをどこで受信しているのか、
どの事業者がドメインを管理しているのかといった情報が、公開情報として記録されています。
これらの情報は、インターネットに接続できる人であれば誰でも確認できます。

セキュリティ上重要な4種類のDNSレコード

DNSレコードにはさまざまな種類がありますが、セキュリティの観点で特に重要なのは、次の4種類です。
これらを分析することで、ドメインに紐づく主要な外部IT資産、メールセキュリティの設定、管理主体、サービス間の接続関係を把握できます。

A レコード

ドメイン → IPアドレス

ドメイン名を、Webサーバーなどの実際のIPアドレスに紐づけます。

例: example[.]co.jp → 125.61.30.xxx

MX レコード

受信メールサーバーを指定

自社ドメイン宛てのメールを、どのメールサーバーで受信するかを指定します。

*複数のメールサーバーがある場合は、優先順位も設定

NS レコード

ネームサーバーを指定

そのドメインのDNS情報を、どのサーバーが管理しているかを示します。

「ドメインの管理先」

TXT/SPF レコード

メール送信元の認証ポリシー

自社ドメインからのメール送信を許可するサーバーやIPアドレスを定義します。

*設定が不十分な場合、迷惑メール判定やドメイン詐称に悪用されるおそれがあります。

DNSレコード

PTRレコード ― Aレコードの逆引き

ドメインとIPアドレスの管理関係を確認する手がかり

Aレコードが「ドメイン名 → IPアドレス」を示すのに対し、
PTRレコード（Pointer Record）は「IPアドレス → ドメイン名」を示します。
この仕組みは、逆引きDNS（Reverse DNS）とも呼ばれます。

PTRレコードは、主に**メールセキュリティ**で利用されます。メール受信サーバーは、送信元IPアドレスのPTRレコードを参照し、送信元ドメインやメールサーバーの情報に不自然な点がないかを確認します。

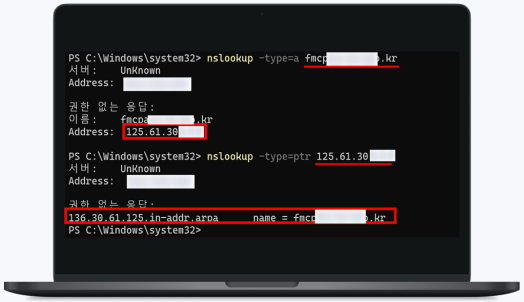
PTRレコードが未設定であったり、送信元情報と整合していなかったりする場合は、迷惑メールと判定される要因の一つとなります。

専用ホスティングと共有ホスティング

専用ホスティングでは、AレコードとPTRレコードが一致します。
一方、複数の企業が1つのサーバーIPアドレスを共有する共有ホスティングでは、AレコードとPTRレコードが異なります。
PTRレコードが異なる場合、**そのIPアドレスは自社所有の資産ではないことを意味**します。

つまり、ドメインは自社のものでも、サーバー自体は共有リソースです。

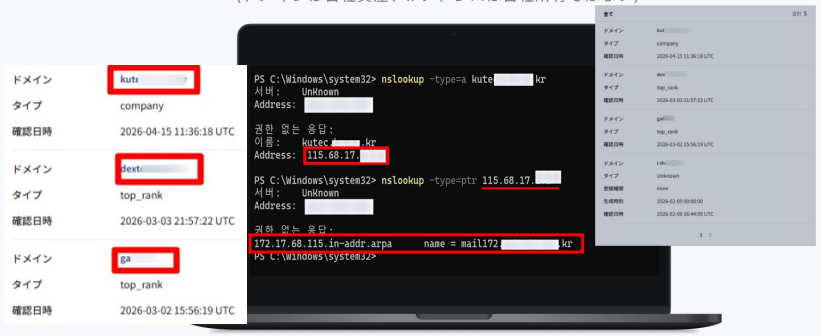
専用ホスティング：Aレコード = PTRレコード



IPアドレスとドメインが一致

共有ホスティング：Aレコード ≠ PTRレコード

（ドメインは自社資産、IPアドレスは自社所有ではない）



Criminal IPで確認した
115.68.17.xxxに紐づくドメイン

IPアドレスとドメインが不一致

1つのIPアドレスに複数のドメインが紐づいている

03

実際に確認された脅威

6つの公開リスク事例

実際に確認された脅威

1つのIPアドレスに紐づく500のサイト

同一IPアドレスを共有する複数のサイト — 共有ホスティングに潜む構造的リスク

事例 1

多くの中小企業では、コストを抑えるために共有ホスティング（Shared Hosting）を利用しています。
これは、1つのサーバーIPアドレスを複数の企業で共有する仕組みです。この場合、AレコードとPTRレコードは一致しません。

実際に確認された事例

`www.example[.]co.jp → 115.68.17.xx2`

IPアドレスを確認

www.example[.]co.jp 照会
→ 115.68.17.xx2

PTRレコードを確認

115.68.17.xx2を逆引きすると、
055-587.comなど別のドメインを確認

共有サーバーと判明

このIPアドレスは、example社の専用サーバーではなく、共有サーバーであることが判明

複数のドメインを確認

115.68.17.xx2を調査した結果、533件のドメインが同じIPアドレスに紐づいていることを確認

229のドメインが同一IPアドレスを共有

同一IPに紐づくドメイン

Reverse IP results for 115.68.17.xx2

There are 229 domains hosted on this sever.
The complete listing of these is below:

DOMAIN NAME
055-■■■■■.com
119■■■■■■.com
aceme■■■■.co.jp
acew■■■■.com

... and 531 more

なぜ危険なのか

自社のWebサイトを適切に管理していても、同じサーバーIPアドレスを共有する**229のサイトのうち、1つでも侵害されれば、サーバー全体が停止したり、同一サーバー上のデータが危険にさらされたりする可能性があります。**自社で十分な対策を講じていても、他社のセキュリティ不備によって影響を受ける構造です。

対策

ドメインは自社資産ですが、共有ホスティングのIPアドレスは自社資産ではありません。
両者を明確に区別して管理する必要があります。
重要な資産については、専用ホスティングへの移行を検討してください。

実際に確認された脅威

Cloudflare CDN

Cloudflare CDN の背後にあるオリジンIPを特定

事例 2: Cloudflare CDN

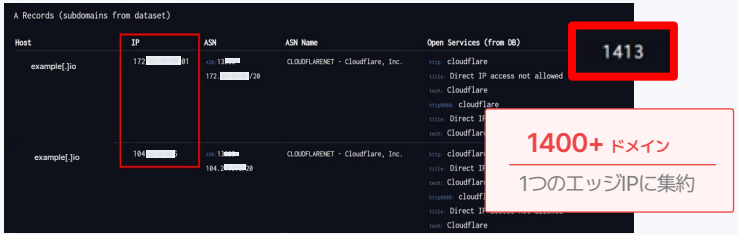
CDN（Content Delivery Network）は、世界各地に分散した
サーバーを利用し、Webサイトの表示速度や可用性を向上させる
仕組みです。

代表的なサービスとしてCloudflareがあり、CDNを導入すると、
ドメインのAレコードには実際のオリジンサーバー（Origin Server）
ではなく、CDNのエッジサーバーのIPアドレスが設定されます。

CDNエッジの特徴

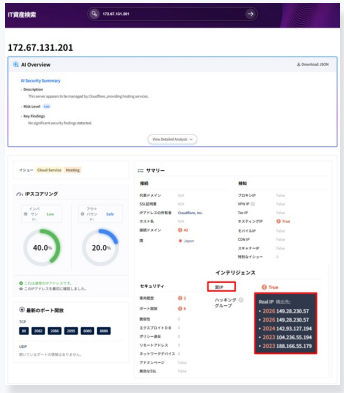
- オリジンIPアドレスを隠蔽
- IPアドレスへの直接アクセスを制限
- 1つのエッジIPを多数のサイトが共有
- 攻撃者に悪用されると追跡が困難

Cloudflare CDN適用時のAレコード例



CDNはDDoS対策に有効である一方、**追跡を困難にする仕組みとして、**
サイバー犯罪者に悪用されることもあります。オリジロンサーバーのIPアドレスを
保護できる反面、攻撃者も同じ仕組みを利用して、自身のインフラを隠すことができます。

Criminal IPによるオリジンIPアドレスの特定



AI SPERAは、「DNSサービスを利用する悪性サイトの隠されたIP（インターネット
プロトコル）アドレスを特定する方法および装置」に関する米国特許を取得しています。
この技術を活用したCriminal IPでは、CDNなどの背後に隠された
オリジンサーバーのIPアドレスを確認できます。

実際に確認された脅威

外部DNSに公開された内部IPアドレス

DNS Aレコード設定ミス — 社内ネットワークの露出

事例 3

よく見られるDNS設定ミスの一つに、外部DNSへ社内ネットワークのIPアドレス（10.x.x.x、192.168.x.xなど）が登録されているケースがあります。

主な原因は、次の2つです。

1. 内部DNSと外部DNSを分離せず、同一の設定で管理している
2. VPN経由でのみ利用する内部ドメインを、外部DNSにも登録している

対策

内部向けドメインは内部DNSにのみ登録し、VPN経由で利用するドメインは外部DNSから削除します。

また、**ASMを活用し、外部DNSに公開されているプライベートIPアドレスを定期的に検出**します。

実際に確認された事例

攻撃者は何を把握できるのか

「これらはVPN経由でアクセスする内部システムであり、内部IPアドレスには10.x.x.xの範囲が使用されている」

このように、侵入後に狙うべき内部IPアドレスを示す、ネットワーク構成図のような情報を与えてしまいます。

内部ネットワークのIPアドレス（プライベートIP）とは

社内ネットワーク内でのみ使用されるIPアドレスです。
10.0.0.0～10.255.255.255
172.16.0.0～172.31.255.255
192.168.0.0～192.168.255.255
これらがプライベートIPアドレスの範囲です。通常、インターネットから直接アクセスすることはできません。

실제로 확인된 위협

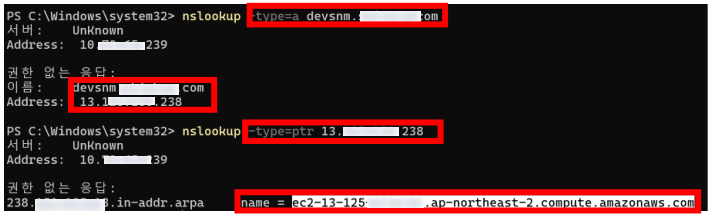
クラウドサーバーは隠してもPTRレコードから見える

AWS EC2のPTRレコード（逆引きDNS）から分かるクラウド資産

事例 4: AWS EC2 PTR

PTRレコードは、AWSのホスト名形式（ec2-リージョン）をそのまま返します。→ **ドメインだけでなく、クラウドインフラの構造自体も露出**

実際に確認された事例



1. 開発サーバーのドメインを照会すると、IPアドレスが判明
2. そのIPアドレスを逆引きすると、AWSのホスト名が返される
3. AWSホスト名から情報が露出

→ドメインだけでなく、クラウドインフラの構造自体も露出

`name = ec2-13-125-[redacted].ap-northeast-2.compute.amazonaws.com`

この一文から、攻撃者は以下を把握できます。

1. AWSを利用している
2. ソウルリージョン（ap-northeast-2）を使用している
3. 同じIPアドレス帯にある他のドメインも調査できる

攻撃者はAWSホスト名へ直接アクセスし、検知を回避することがあります。ASMを活用することで、こうした資産を把握できます。

クラウド資産もPTRレコードから追跡可能 — ASMがなければ、担当者も把握していないサーバーが外部に公開されます。

実際に確認された脅威

放置されたドメインは攻撃者のものになる

Shadow IT — サブドメイン乗っ取り（Subdomain Takeover）・NXDOMAINの脅威

事例 5: Shadow IT

この事例は、最も深刻な脅威の一つです。
サービスを終了したにもかかわらず、DNSレコードを削除しなかった場合に何が起こるのかを示しています。

①サブドメイン作成後に放置

`dev.company[.]co. jp → 10.x.x.x`

サーバーを構築・運用した後、サービスを終了したものの、DNSレコードを削除し忘れた状態

→ドメインは存在するが、接続先のIPアドレスがない（NXDOMAIN）

②攻撃者が発見し、IPアドレスを登録

サブドメインを発見した攻撃者が、
自身の管理するサーバーのIPアドレスを
そのドメインに登録

→正規のドメインが攻撃者に乗っ取られる

③フィッシング・マルウェア配布に悪用

メールセキュリティフィルターは、「これは〇〇社の公式ドメインなので信頼できる」と判断
→迷惑メールフィルターをすり抜け、フィッシングメールが受信トレイに到達

→正規ドメインを装ったフィッシング・迷惑メールの送信

サービス終了後にDNSレコードを削除しないと、そのドメインが攻撃に悪用される可能性があります。

実際に確認された脅威

放置されたドメインは攻撃者のものになる

Shadow IT — サブドメイン乗っ取り (Subdomain Takeover) ・ NXDOMAINの脅威

事例 5: Shadow IT

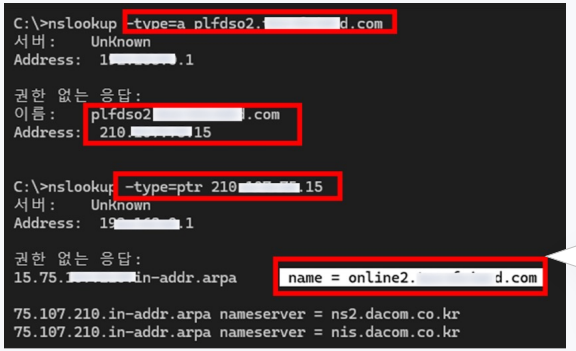
この事例は、最も深刻な脅威の一つです。

サービスを終了したにもかかわらず、DNSレコードを削除しなかった場合に何が起こるのかを示しています。

なぜExcel管理では検知できないのか

Excelの資産一覧には、基本的に**「現在運用中のサービス」**だけが記録されます。終了したサービスのDNSレコードは削除されないまま、インターネット上に残り続けることがあります。

実際に確認された事例



Aレコードと不一致
ステータス：NX（ドメイン不存在）

ASMは、NXDOMAINの状態をリアルタイムで検知し、担当者へ通知します。

メールセキュリティの第一関門、MXレコード

メール受信経路の優先順位設定ミスと外部サービス利用のリスク

事例 6: MXレコードの設定ミス

サイバー攻撃の約60%は、メールを起点に始まるといわれています。メールセキュリティの第一関門となるのが、MXレコードの優先順位設定です。MXレコードには優先度を示す数値が設定されており、**数値が小さいほど先に処理**されます。迷惑メールフィルターでメールを先に受信するには、迷惑メールフィルターのMX値をメールサーバーより小さく設定する必要があります。

MXレコードの確認結果

```
mdsit.co.kr  –  MX Records
20  mail[.]xxxx.co.jp    52.79.180.107    (メールサーバー：後で処理)
0   spam[.]xxxx.co.jp    43.200.56.216    ← 先に処理！
✓ 正しい設定：迷惑メールフィルター（0）がメールサーバー（20）より小さい値→ 迷惑メールを先にフィルタリング

cu.co.kr  –  MX Records
10  mail[.]xx.co.jp    61.85.84.27    IP: Not found ⚠ 危険！
5   spam[.]xx.co.jp    61.85.84.24    未使用・ホストが存在しない
⚠ 危険な設定：古いMXレコードを放置
→ 外部サービスが第三者に再取得されると、メール通信が攻撃者のインフラへ誘導される可能性があります。
```

セキュリティ上注意が必要なMXパターン

ステータス	リスク
古いメールホスト（Not Found）	高
Exchange OWAも外部公開	高
テスト用SMTPサーバー	高
サーバーは存在しSMTPポートも開放されているが、MXレコードなし	中〜高
SPFに含まれていないSMTPサーバー	中

ASMでは、MXレコードに登録されたメールサーバーを特定したうえで、外部公開の有無、SMTPバナー、TLS証明書、メールサーバー製品などの情報も確認できます。これにより、単に「メールサーバーが存在する」ことを把握するだけでなく、外部から観測できるメールインフラの構成や、潜在的な攻撃の手がかりまで確認できます。

04 セルフチェックリスト

14項目で確認する自社の
セキュリティ対策状況

セルフチェックリスト

自社のIT資産は、今安全ですか？

1つでも「いいえ」があれば、ASMが必要なサインです。

資産管理

- ☐ 自社のASN（自律システム番号）を把握している
- ☐ すべての外部IPアドレスとドメインの一覧を最新の状態に保っている
- ☐ サービス終了後、DNSレコードを速やかに削除している

ホスティング／クラウド

- ☐ 共有ホスティングの利用状況を把握している
- ☐ CloudflareなどのCDN背後にあるオリジンIPを管理している
- ☐ AWS EC2などのクラウド資産が資産一覧に含まれている

DNSレコード

- ☐ 外部DNSに内部IPアドレス（10.x.x.xなど）が登録されていない
- ☐ NXDOMAIN状態のまま放置されたサブドメインがない
- ☐ AレコードとPTRレコードの所有・管理主体を確認している

TLS証明書

- ☐ プライベート証明書（公的認証局以外）を使用している資産がない
- ☐ 有効期限が30日以内に迫った証明書がない
- ☐ CTログを監視し、類似ドメインに対する証明書発行を検知している

メールセキュリティ

- ☐ 迷惑メールフィルターのMX優先度が、メールサーバーより高く設定されている

ASM運用

- ☐ IT資産を自動的に探索するASMソリューションを運用している

1つでも「いいえ」があるなら、攻撃者は今この瞬間も、その隙を探しています。
ASMは、これらの情報を継続的に収集・分析し、外部公開資産やリスク候補を担当者が確認できる形で可視化します。

セルフチェックリスト

自社のデジタル登記簿謄本

今すぐ確認してください

IT資産の自動探索

Excelでは把握できない
シャドーITまで自動検出

IPアドレス・ドメイン・TLS証明書

リアルタイムの脅威検知

NXDOMAIN、内部IPアドレスの露出、
MXレコードの設定ミスなど、主要なDNS
リスクを迅速に検知

外部公開資産とDNS設定ミスを可視化

攻撃者視点での管理

公開DNS情報と外部観測データをもとに、
これまで把握できていなかった資産を優先的に確認

先回りしたセキュリティ管理体制を実現

不動産契約の前に登記簿謄本を確認するように、
企業のデジタル資産についても、DNSレコードと外部公開状況を定期的に点検する必要があります。

Criminal IP ASM

Criminal IP ASMの無料デモは、
お問い合わせフォームよりお申し込みいただけます。

Criminal IP

住所　東京都千代田区神田須田町2丁目19-23　Daiwa秋葉原ビル 2F
ウェブサイト　https://www.criminalip.io/ja
メール　support@aipsera.com

Criminal IP