



# あなたの企業のセキュリティ対策は 万全ですか？。

---



株式会社 Geolocation Technology フェロー  
静岡県警サイバー犯罪 テクニカルアドバイザー



但野 正行

# 講師紹介

- 但野正行 (ただの まさゆき)
  - 株式会社Geolocation Technology 技術開発部 フェロー
  - 静岡県警 サイバー犯罪テクニカルアドバイザー(2020～2024年)
  - 情報処理安全確保支援士 登録番号018105
    - 2021～2023年にて、関東管区警察学校にて、全国のサイバー犯罪課所属の警察官に対して教養を実施。
    - 学生時代は、パターン認識とAIの研究(今で言う第2次ブーム)に取り組んでいました。卒業後、i-modeが始まった頃から、インターネットやWebアプリケーション開発に従事していました。また、それらを行いながら、IT系専門学校、大学・社会人向けITエンジニア育成についても関わってきました。その頃から必然的にWebとセキュリティについても関わるようになり、現在に至ります。
    - 特に最近では、県警のサイバー犯罪対策のテクニカルアドバイザーとして、捜査機関向けのIT技術向上のためのサポートや、民間企業向けのサイバーセキュリティ対策のためのコンサルティングやアドバイス、啓蒙活動を行っています。
  - [masayuki@geolocation.co.jp](mailto:masayuki@geolocation.co.jp)

# 株式会社Geolocation Technology



<https://www.geolocation.co.jp/>

■本社三島オフィス  
〒411-0036 静岡県三島市一番町18-22 アーサーファーストビル4F  
Tel: 055-991-5544 Fax: 055-991-5540

■大阪営業所 (シティプロモーション研究所)  
〒550-0006 大阪市西区江之子島2丁目1番34号  
大阪府立江之子島文化芸術創造センター2F Room-9

■福岡営業所  
〒812-0011 福岡県福岡市博多区博多駅前3-6-12 オヌキ博多駅前ビル621

■那覇コンタクトセンター  
〒900-0016 沖縄県那覇市前島3丁目25番2号 泊ポートビル2F 2-C/ルーム

■設立日: 2000年2月21日

■上場取引所: 福岡証券取引所Q-Board (証券コード 4018)



## 取引先



Internet Initiative Japan



# アジェンダ

## ① インターネット上の様々な脅威

- 昨今のサイバー犯罪事情
- 正しく怖がるには、仕組みを理解する

## ② OSINT情報からわかること

- 自分たちのことはどこまで知られているのか。
- 正しく怖がるには、情報を把握しよう

## ③ 対策とは

- 対策方法は意外と簡単
- それでも、事件は起きる

# 本日お伝えしたいこと

---

- 概念的な話はしません。
- なるべく難しい単語は出しません。
- 対応済みのかたは、再確認。
- 不安と思っている方には、何が問題なのかを認識。
- ここに取り上げたことは明日からできることばかり。

# インターネット上の脅威

# IPAの10大脅威

## ・ 会社や組織における脅威とは

順位	組織	昨年 順位
1	ランサムウェアによる被害	1
2	サプライチェーンの弱点を悪用した攻撃	2
3	内部不正による情報漏えい等の被害	4
4	標的型攻撃による機密情報の窃取	3
5	修正プログラムの公開前を狙う攻撃 (ゼロデイ攻撃)	6
6	不注意による情報漏えい等の被害	9
7	脆弱性対策情報の公開に伴う悪用増加	7
8	ビジネスメール詐欺による被害	7
9	テレワーク等のニューノーマルな働き方を 狙った攻撃	5
10	犯罪のビジネス化 (アンダーグラウンドサービス)	10

<https://www.ipa.go.jp/security/10threats/10threats2024.html>

# 標的型とランサムウェア

- **結局のところ、標的型攻撃かランサムウェア攻撃**
  - ランサムウェア攻撃は、お金を得ることが目的のために、犯行後は犯行声明を出すことで、表面化する。
  - 標的型はひっそりと機密情報を窃取することが目的なので、犯行は行われたことがわからないようにする。したがって、知らないうちにこの攻撃を受けているということが考えられる。
  - 攻撃の目的は異なるが、そのための手法には共通点が多い。
  - 10大脅威のその他のものは、その攻撃の手法が挙げられていて、これらを利用して、この2つの攻撃は行われている。



# ランサムウェアの動向

- **RaaS(Ransomware-as-a-Service)**

- 専用ポータルやハッキングフォーラムを介して、他の犯罪グループにランサムウェアを貸し出すグループによるサービス。

- **アフィリエイト**

- RaaSで提供されるツールを利用する犯罪グループで、身代金として得た金額の中から、手数料をRaaSへ支払う。

- **「二重脅迫」型**

- 従来のランサムウェアは、データを暗号化して、復号のための身代金を要求するだけだったが、第二弾の脅迫として、コンピュータ内に保存されているデータを公開(ダークウェブなど)すると脅迫し、金銭を要求する。

- **IAB(イニシャルアクセスブローカー)**

- サイバー攻撃の対象となる組織へのアクセス権を販売する、ダークウェブ上で活動するサイバー犯罪者集団。


# ランサムウェアの動向

## • Lockbitのリークサイト

<p><b>isosteo.fr</b> 3D 11h 19m 08s</p> <p><b>PUBLISHED</b></p> <p>Institut Supérieur d'Ostéopathie Lyon, ISOstéo Lyon a participé activement à la création du 1er enseignement de l'ostéopathie en formation initiale post-bac. Le Diplôme d'Ostéopathie</p> <p>Updated: 18 Feb, 2023, 09:35 UTC 3061</p>	<p><b>primorossi.com.br</b></p> <p><b>PUBLISHED</b></p> <p>Invista em seu sonho de forma planejada. Adquirá seu consórcio de forma prática e segura. Confie em quem tem mais de 50 anos de tradição. Saiba mais!</p> <p>Updated: 18 Feb, 2023, 09:12 UTC 3065</p>	<p><b>innophaseinc.com</b></p> <p><b>PUBLISHED</b></p> <p>InnoPhase is a fabless semiconductor company that develops innovative and efficient RF architectures using CMOS technology. Building on our previous experience with WLAN IoT</p> <p>Updated: 20 Feb, 2023, 21:52 UTC 3399</p>
<p><b>hotdesk.me</b></p> <p><b>PUBLISHED</b></p> <p>Hotdesk.me and their customers such as Barrington James (barringtonjames.com), Sarnac Partners (sarnacpartners.com), Hardman &amp; Watson (hardmanandwatson.co.uk).</p> <p>Updated: 20 Feb, 2023, 21:54 UTC 3441</p>	<p><b>alliedtools.com</b> 11D 01h 07m 50s</p> <p><b>PUBLISHED</b></p> <p>Allied International was founded in 1962 as an import distributor of hardware products. Over the years, with our unwavering commitment to innovation, quality, value and service, we have</p> <p>Updated: 17 Feb, 2023, 15:04 UTC 3297</p>	<p><b>fikes.com</b></p> <p><b>PUBLISHED</b></p> <p>https://www.fikes.com/ COMMERCIAL CLEANING &amp; FACILITY MAINTENANCE SERVICES There are many moving parts to make sure a business runs successfully, and</p> <p>Updated: 17 Feb, 2023, 13:36 UTC 3330</p>
<p><b>cordfinancial.com</b></p> <p><b>PUBLISHED</b></p> <p>Our Story – ATM Services Nationwide Provider of Innovative Solutions: ATM Services &amp; Products In 2001, CORD Financial Services was founded by The FIKES Companies. With a small</p> <p>Updated: 17 Feb, 2023, 13:33 UTC 3271</p>	<p><b>sandycove.org</b> 7D 15h 39m 45s</p> <p><b>PUBLISHED</b></p> <p>Sandy Cove's mission is to help you connect with God and each other in order to be transformed into the image of Christ, through His Word</p> <p>Updated: 16 Feb, 2023, 21:36 UTC 2703</p>	<p><b>royalpage.ca</b> 2D 17h 28m 02s</p> <p><b>PUBLISHED</b></p> <p>Since 1913, Royal LePage has been helping Canadians buy and sell their homes and supporting communities Quebec City branch</p> <p>Updated: 16 Feb, 2023, 19:24 UTC 3362</p>

# ARE PUBLISHED

Deadline: 04 Aug, 2023 04:30:49 UTC



**berg-life.com**

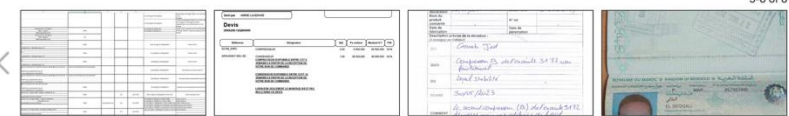
It is the leader in the manufacture of aerosol drugs in Tunisia, it is the only laboratory in Africa and the Middle East which masters the new technology of HFA propellants which respect the environment in pharmaceutical applications.


**ALL AVAILABLE DATA PUBLISHED !**

UPLOADED: 18 JUL, 2023 12:30 UTC

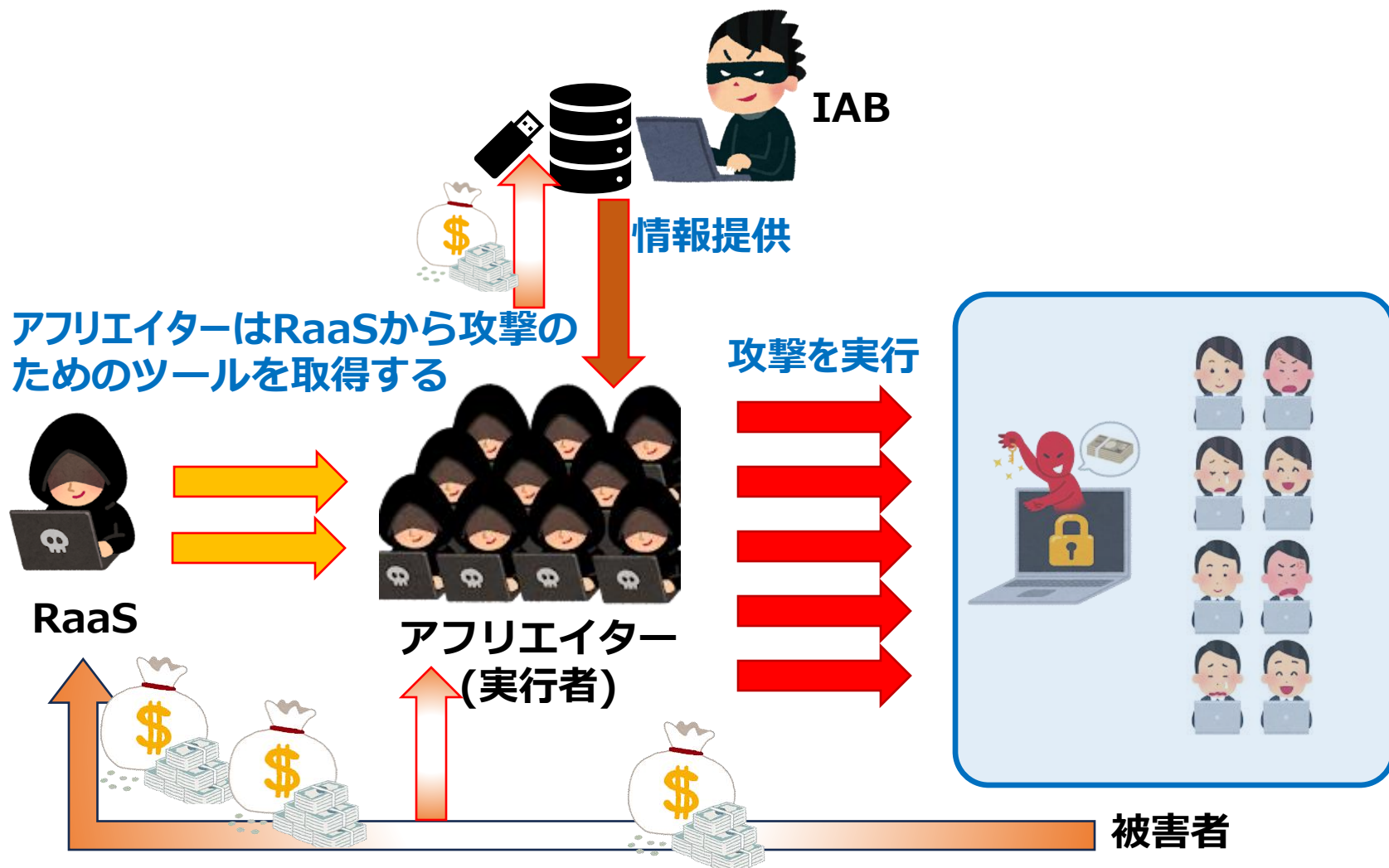
UPDATED: 18 JUL, 2023 12:33 UTC

5-8 of 8



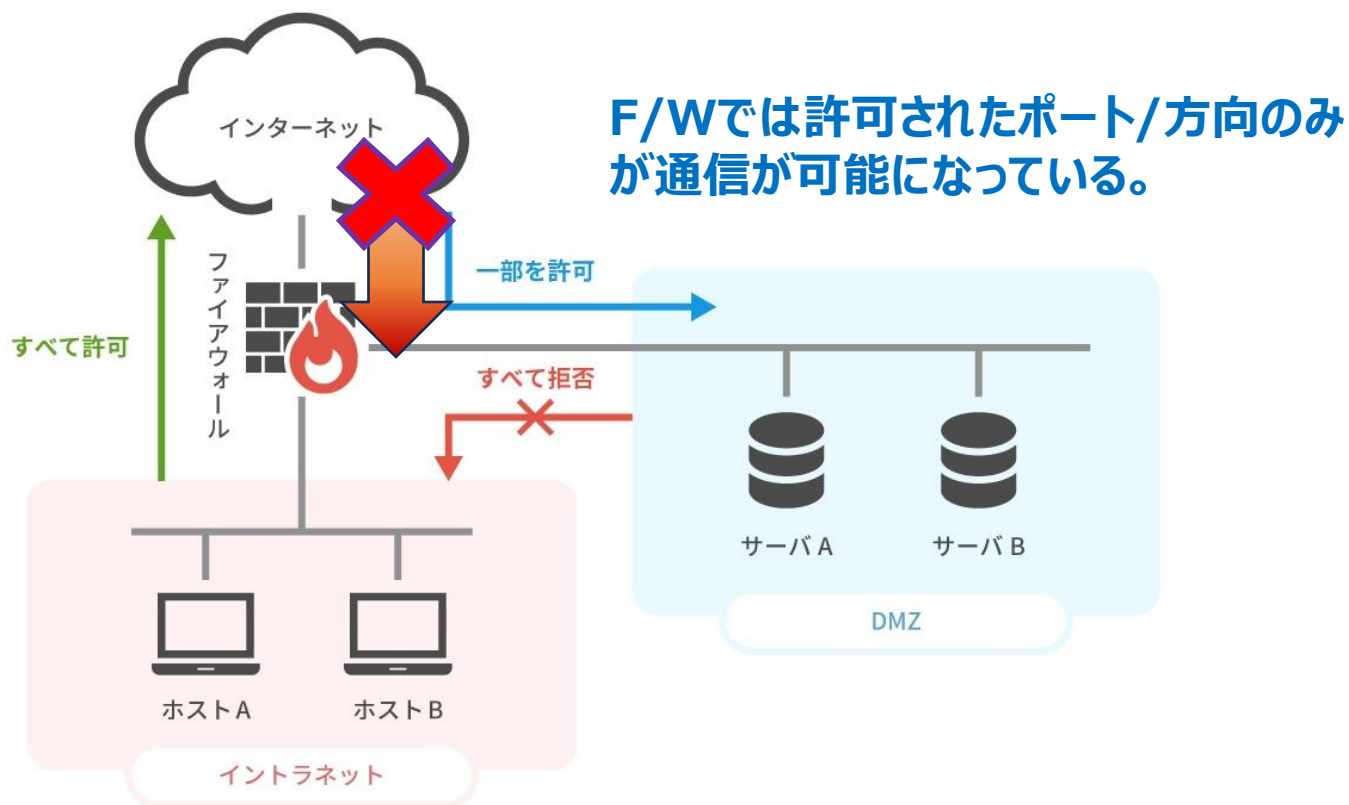


# 犯罪のビジネス化



# 攻撃者はどこからやってくるのか

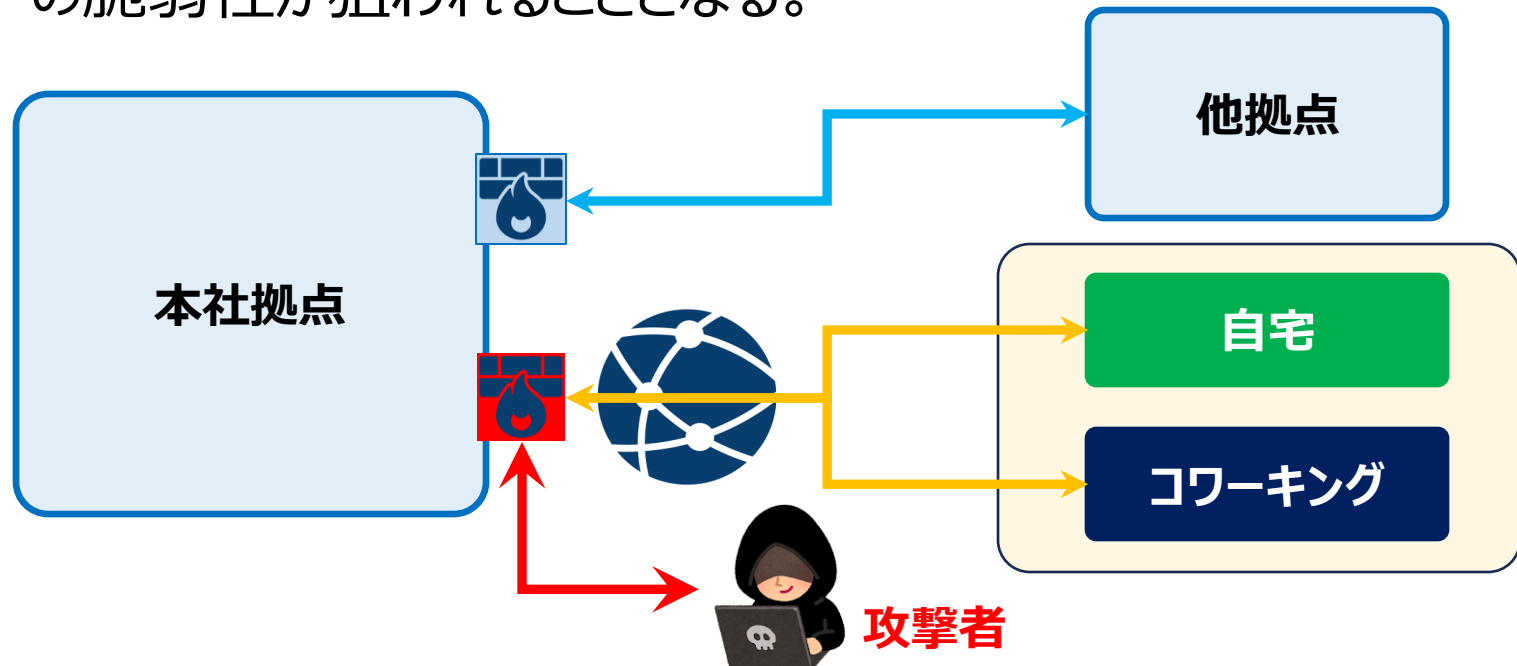
- 簡単には組織の中には入ってくることは難しい
  - 組織のネットワークは、F/W(ファイアーウォール)等で外部からの侵入は困難になっている(はず)。



# 外部からの侵入口

## • コロナ禍以降、組織のネットワーク構成の変更

- テレワークの導入などで、VPNやRDPの利用が広まった(ニューノーマルな働き方)。
- そのことから、インターネットとの接続点が増えることになり、その脆弱性が狙われることとなる。



# サイバー攻撃のターゲット

- **昨今のサイバー攻撃の原因としてネットワーク機器の脆弱性が狙われていることが非常に多い**
  - 2019~2020年 三菱電機（ルータなど）
  - 2020年11月 カプコン（VPN）
  - 2021年10月 徳島県半田病院（VPN）
  - 2022年10月 大阪大阪急性期総合医療センター（VPN）
  - 2023年7月 名古屋港コンテナターミナル（VPN？）
  - 2023年~2024年 JAXA（VPN）

# 内部者への侵入

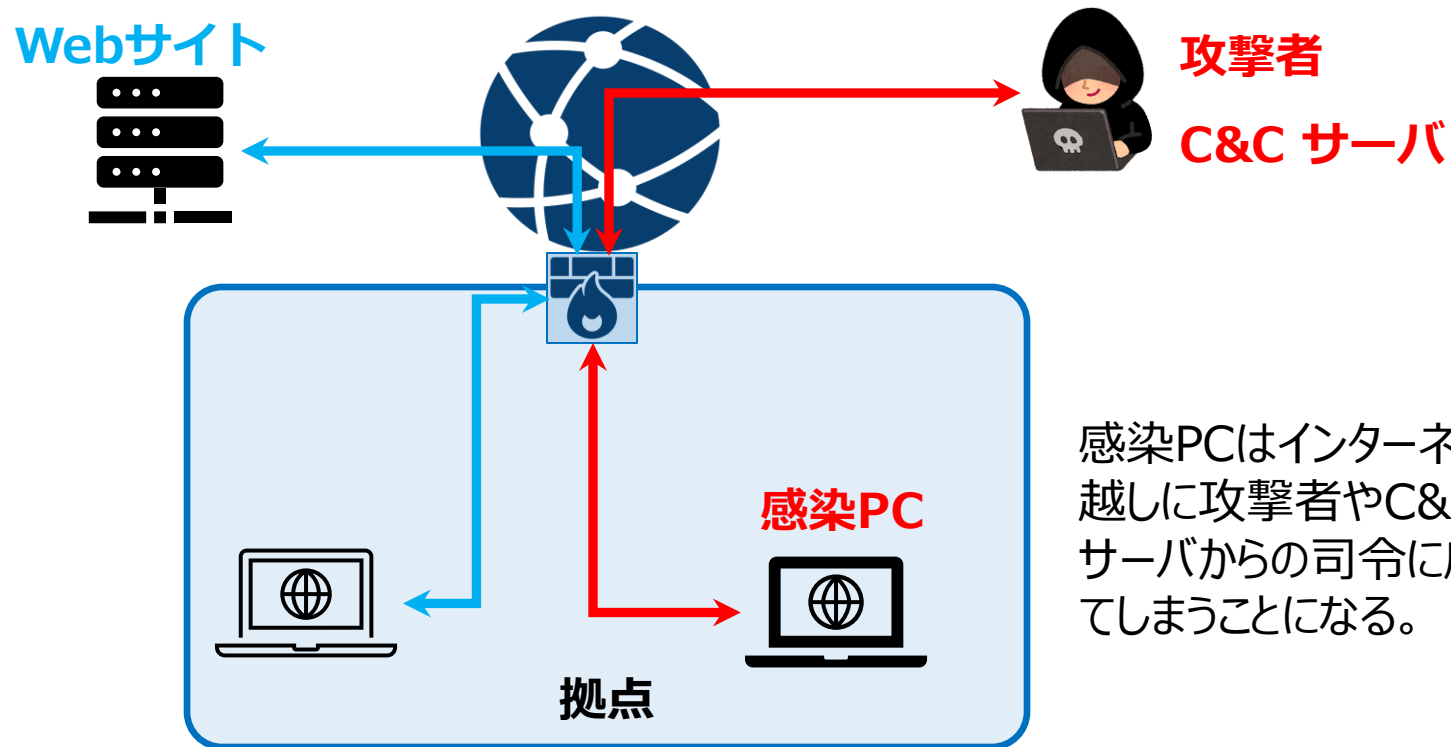
## • いかにも内部者を騙すのか

- F/W等のアクセス制限は、内部からのアクセスからの戻って来る通信は許可していることが多い。
- 外部からの侵入が難しいときには、内部にいる人を騙して(環境を乗っ取り)、外部へアクセスさせるように試みる。
- そのためには、以下のような手段を試みる。
  - サプライチェーンを利用して、脆弱な組織からのアクセス。
  - フィッシング、ビジネス詐欺メール。
  - ゼロデイを利用した、利用者の環境の乗っ取り。

# 内部からの通信は通過する

## • F/Wのパケットフィルタリング

- パケットフィルタリングの中でもステートフルパケットインスペクションを利用していることが多い。



感染PCはインターネット越しに攻撃者やC&Cサーバからの命令に応じてしまうことになる。



# OSINT情報から わかること

# OSINT情報とは

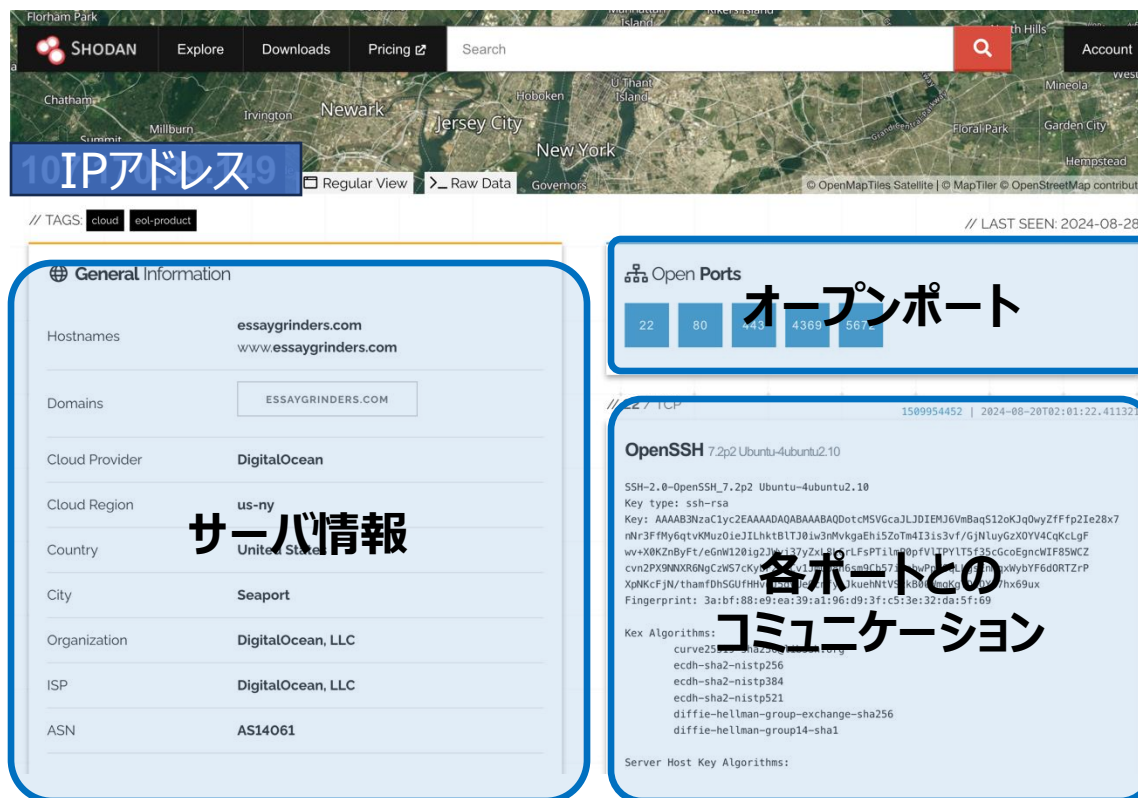
- **Open Source Intelligence(オシント)**
  - 公開されていて誰もが利用可能なオープンな情報を情報源に、機密情報を収集する技術や活動、組織を指す。
  - 近年、このOSINTを使ってサイバー脅威を調査し、セキュリティ強化に役立てることが注目されている。
  - 一方、攻撃者にとっても有用な情報源となっている。

# 自組織の情報はどこまでわかるか？

- **インターネットに直接接続している機器の情報は常に収集されている。**
  - グローバルIPアドレスを保有し、アクセス元IP制限などが施されていなく、外部から接続することが可能な機器は情報が収集されている。
  - 収集されている情報としては、下記のようなものがある。
    - オープンになっているポート番号
    - 製品、アプリケーション情報（バージョンなど）
    - CVE脆弱性情報

## • shodan.io

- インターネットに接続している機器を、IPアドレスでの検索することで、その機器の情報を調べることができる。



The screenshot shows the Shodan search results for IP address 10.10.10.9. The page is divided into several sections:

- General Information:** Hostnames (essaygrinders.com), Domains (ESSAYGRINDERS.COM), Cloud Provider (DigitalOcean), Cloud Region (us-ny), Country (United States), City (Seaport), Organization (DigitalOcean, LLC), ISP (DigitalOcean, LLC), and ASN (AS14061).
- Open Ports:** A bar chart showing open ports at 22, 80, 443, 4369, and 6672.
- OpenSSH:** Details for OpenSSH 7.2p2 Ubuntu-4ubuntu2.10, including key type (ssh-rsa), key fingerprint, and supported Kex Algorithms (curve25519-sha256, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group14-sha1).

## 脆弱性情報

### サーバの脆弱性

#### Vulnerabilities

All ports ▾ Latest ▾

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

#### 2023


**CVE-2023-46118** falseRabbitMQ is a multi-protocol messaging and streaming broker. HTTP API did not enforce an HTTP request body limit, making it vulnerable for denial of service (DoS) attacks with very large messages. An authenticated user with sufficient credentials can publish a very large messages over the HTTP API and cause target node to be terminated by an "out-of-memory killer"-like mechanism. This vulnerability has been patched in versions 3.11.24 and 3.12.7.

**CVE-2023-44487** falseThe HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

#### 2022

**CVE-2022-31008** falseRabbitMQ is a multi-protocol messaging and streaming broker. In affected versions the shovel and federation plugins perform URI obfuscation in their worker (link) state. The encryption key used to encrypt the URI was seeded with a predictable secret. This means that in case of certain exceptions related to Shovel and Federation plugins, reasonably easily deobfuscatable data could appear in the node log. Patched versions correctly use a cluster-wide secret for that purpose. This issue has been addressed and

### アプリケーションの脆弱性

// 80 / TCP 

-1604956909 | 2024-08-23T06:58:02.678252

#### nginx 1.10.3

#### 502 Bad Gateway

HTTP/1.1 502 Bad Gateway  
Server: nginx/1.10.3 (Ubuntu)  
Date: Fri, 23 Aug 2024 06:58:02 GMT  
Content-Type: text/html  
Content-Length: 584  
Connection: keep-alive

**CVE-2019-9513** **CVE-2019-9511** **CVE-2018-16844** **CVE-2018-16843** **CVE-2017-20005**

7 more

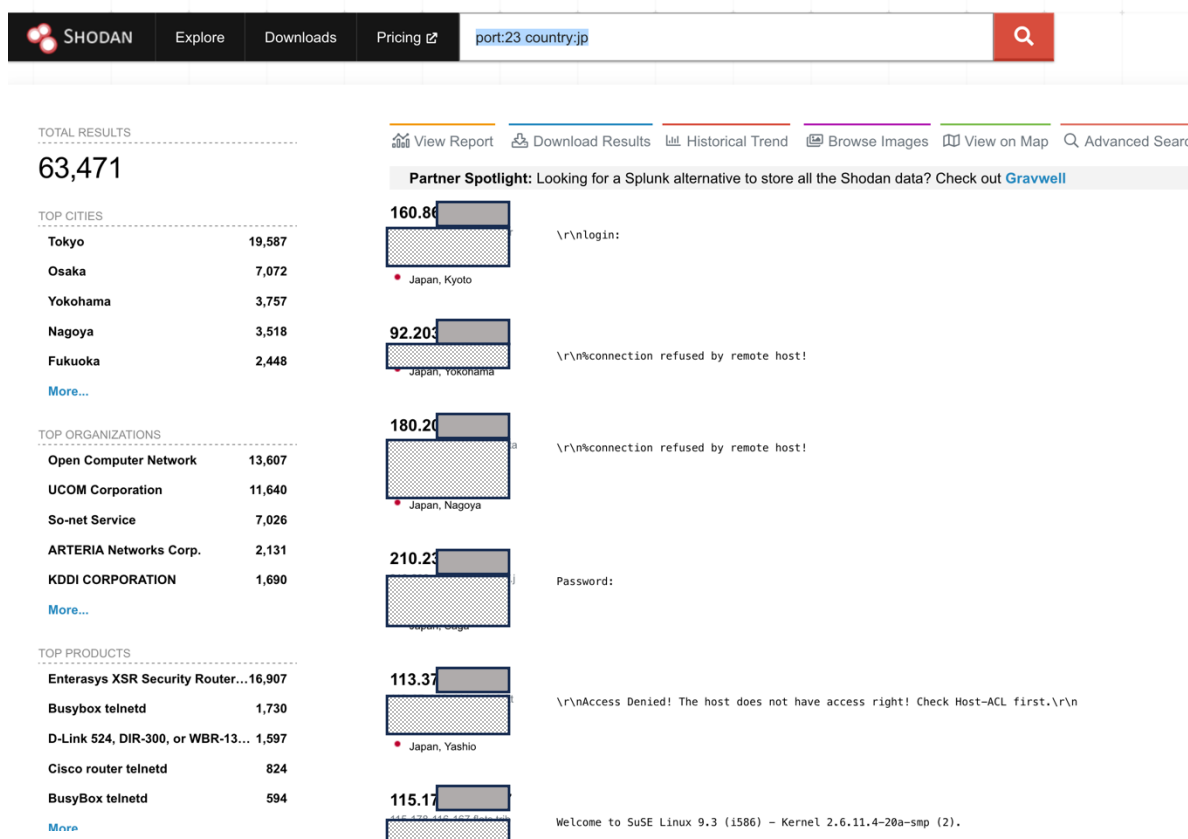
# Shodanので各種検索

- IPアドレスだけではなく、以下のような条件での検索も可能。(ただし、契約条件による)
  - 国や都市名
  - ポート番号
  - ページタイトル
  - 製品情報やOSのバージョン
  - 脆弱性(CVE番号)
  - これらの条件を and や or で組み合わせることが可能

# Shodan検索例

- 日本国内で、telnetを公開している。

## 「port:23 country:jp」



# Shodan検索例

- 日本国内で、RDPを公開している。

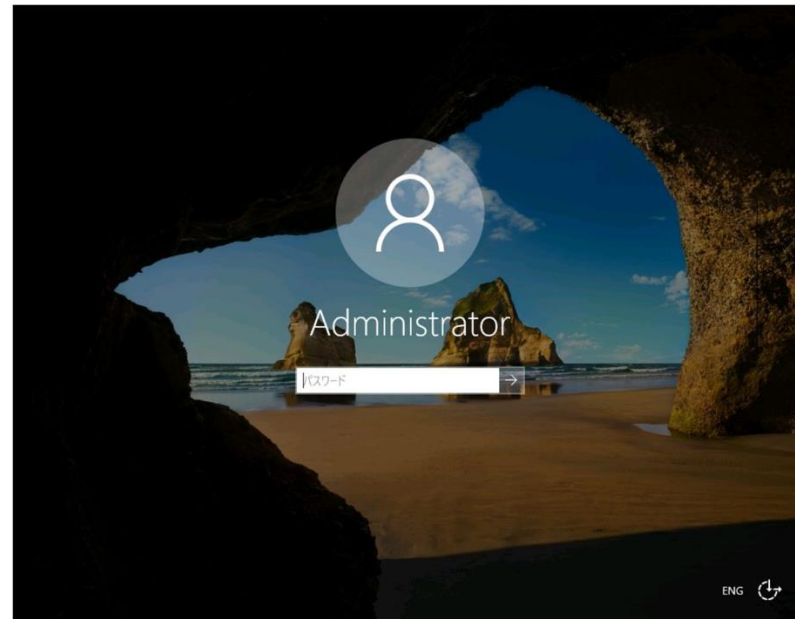
「port:3389 country:jp」



**SSL Certificate**  
 Issued By:  
 j-Common Name: 118-2...  
 Issued To:  
 j-Common Name: 118-2...  
 Supported SSL Versions:  
 TLSv1, TLSv1.1, TLSv1.2

Remote Desktop Protocol  
 \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\xf\x08\x00\x02\x00\x00\x00  
 Remote Desktop Protocol NTLM Info:  
 OS: Windows 10 (version 1809)/Windows Server 2019 (version 1809)  
 OS Build: 10.0.17763  
 Target Name: 118-2...  
 NetBIOS Domain Name: 118-2...  
 NetBIO...

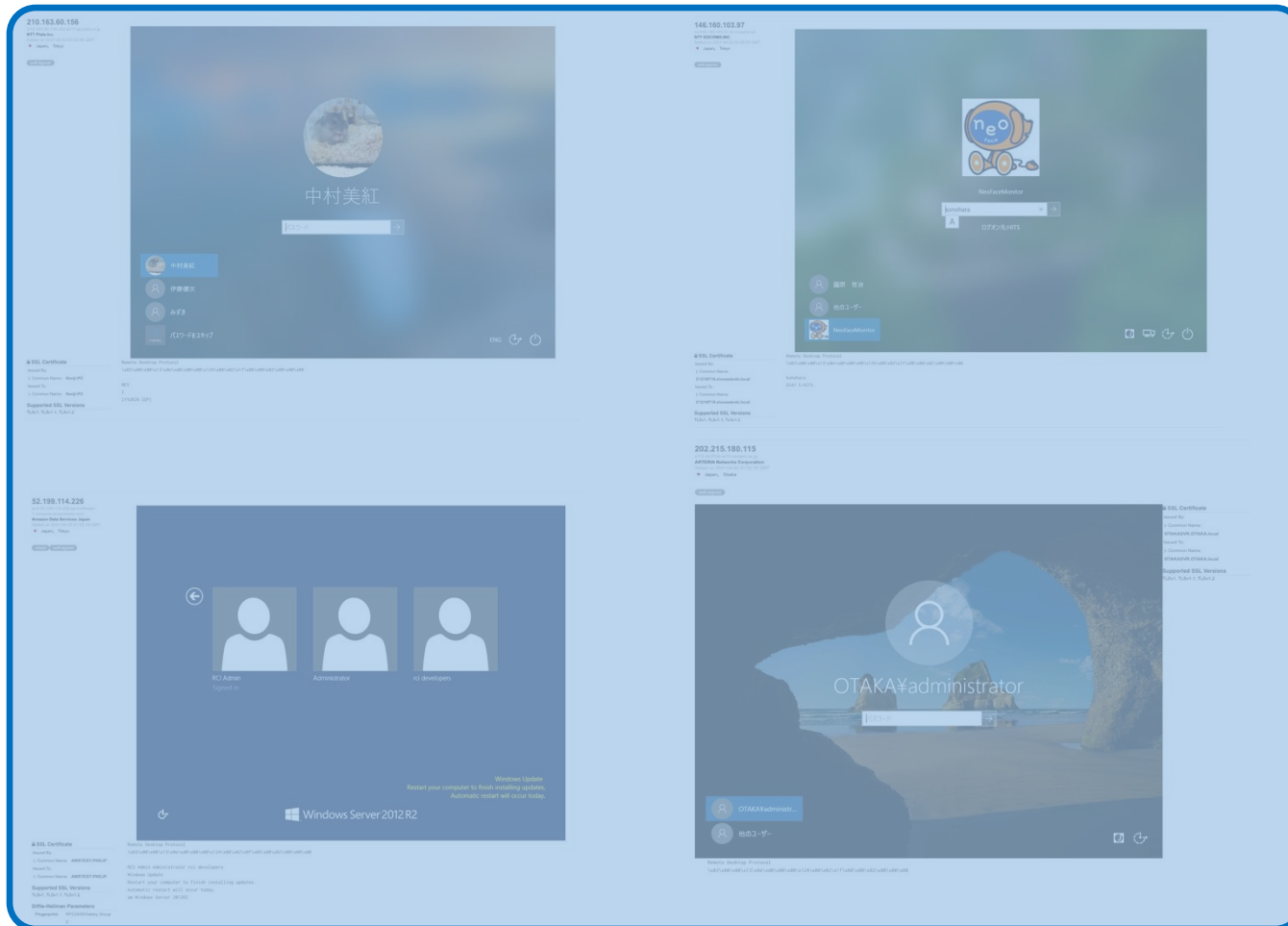
2024-08-29T01:49:07.845276





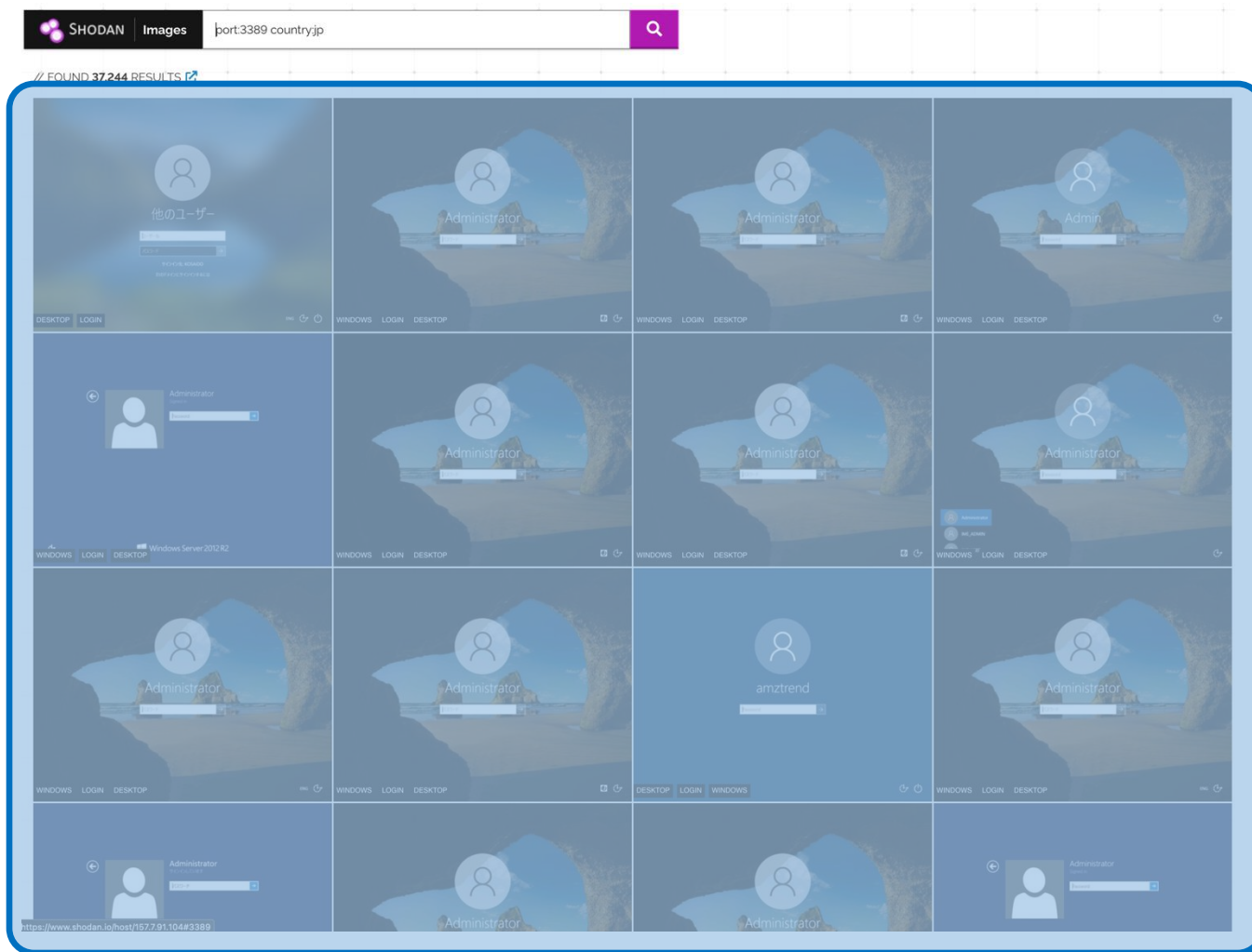
# Shodan検索例

## • RDPでの検索例



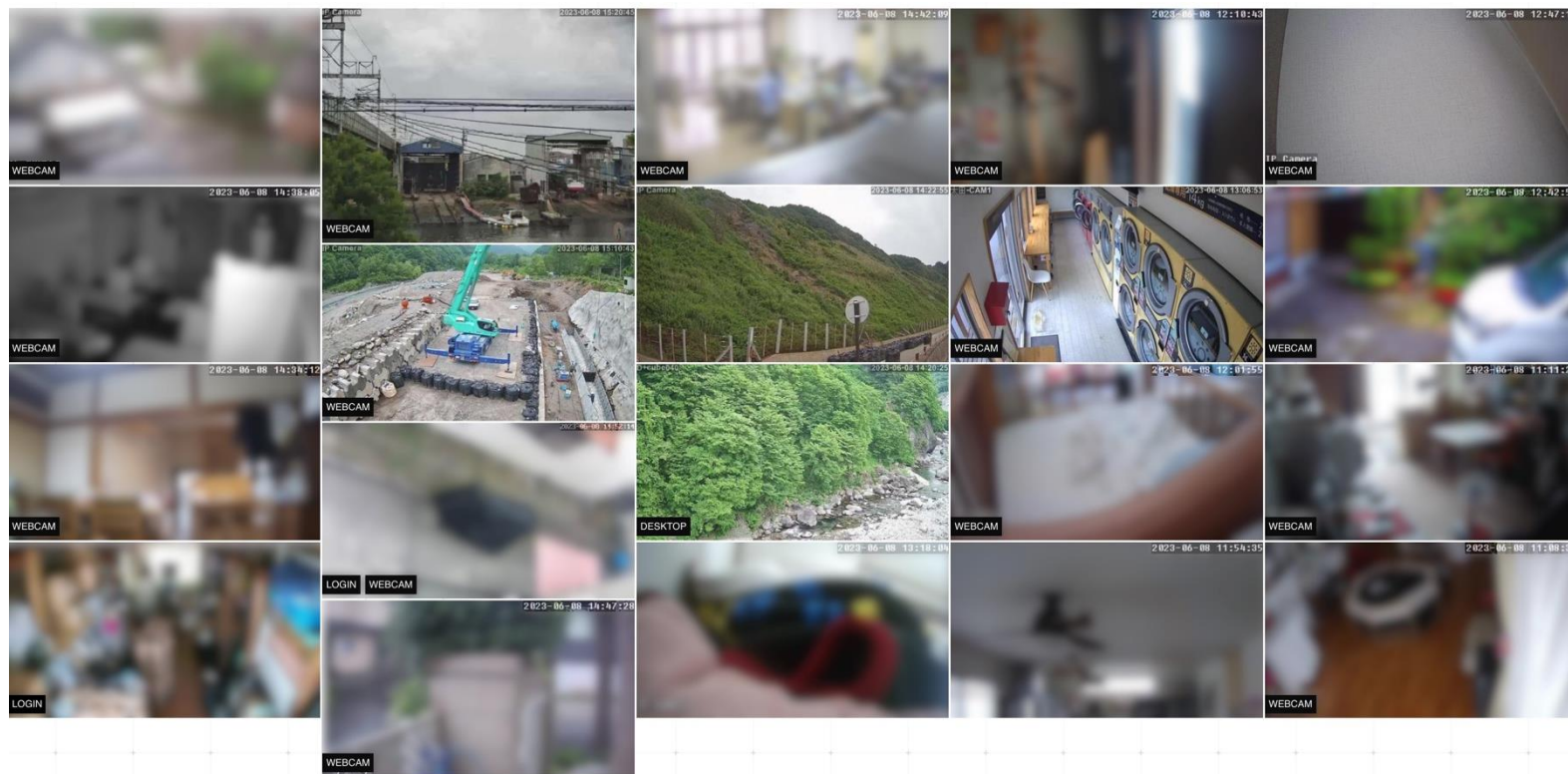
# Shodan検索例

- 画像検索でRDPを検索する



# Shodan検索例

- 画像検索でWebカメラの製品名での検索



# Shodanと同様なサイト

- **CriminalIP**

- shodan同様に各種検索ができ、日本語での表示が可能。
- いくつかの料金プランがあり、それにより利用できる機能が異なる。
- <https://www.criminalip.io/jp>

- **censys**

- 無料で利用できるサービス。
- <https://search.censys.io/>

# dnsdumpster

## ドメイン内のサーバ検索

- nslookupやdigでは、ドメイン内のすべてのAレコードを取得できないが、ドメイン名を入力すると各種DNSレコードやサブドメイン一覧、関連情報を列挙する。部署単位でサブドメインを設定したりして、管理されていないサーバなどを調べることができる。
- <https://dnsdumpster.com/>

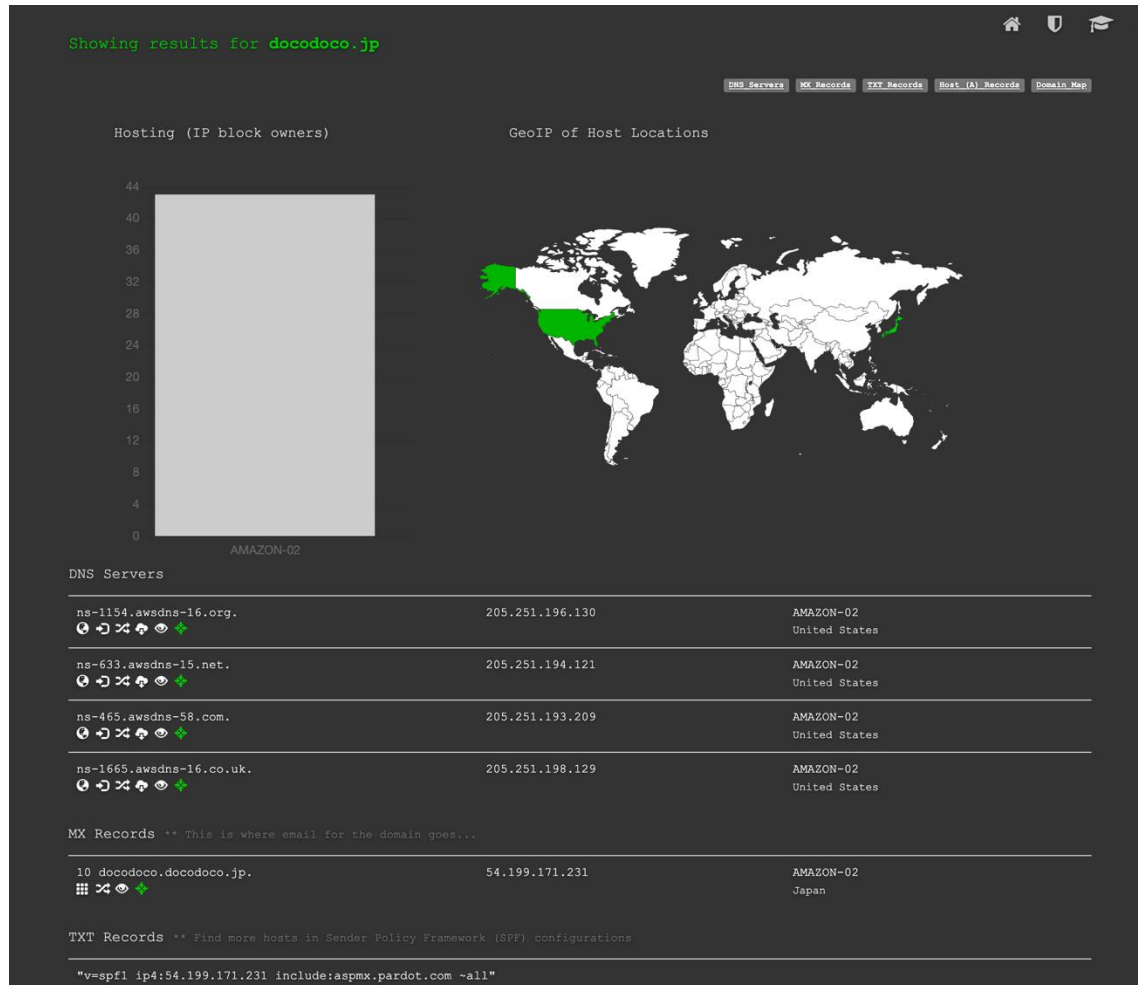
- 例 : docodoco.jp

```
% dig ANY docodoco.jp
;; ANSWER SECTION:
docodoco.jp.          36392      IN         NS        ns-633.awsdns-15.net.
docodoco.jp.          36392      IN         NS        ns-1154.awsdns-16.org.
docodoco.jp.          36392      IN         NS        ns-465.awsdns-58.com.
docodoco.jp.          36392      IN         NS        ns-1665.awsdns-16.co.uk.

;; ADDITIONAL SECTION:
ns-465.awsdns-58.com. 1379 IN       AAAA      2600:9000:5301:d100::1
ns-633.awsdns-15.net. 2889 IN       AAAA      2600:9000:5302:7900::1
ns-1154.awsdns-16.org. 228  IN       AAAA      2600:9000:5304:8200::1
ns-1665.awsdns-16.co.uk. 172324  IN       AAAA      2600:9000:5306:8100::1
ns-465.awsdns-58.com. 1379 IN         A         205.251.193.209
ns-633.awsdns-15.net. 2889 IN         A         205.251.194.121
ns-1154.awsdns-16.org. 228  IN         A         205.251.196.130
ns-1665.awsdns-16.co.uk. 172324  IN         A         205.251.198.129
```

# dnsdumpster

- DNSサーバ情報とTXTレコード



# dnsdumpster

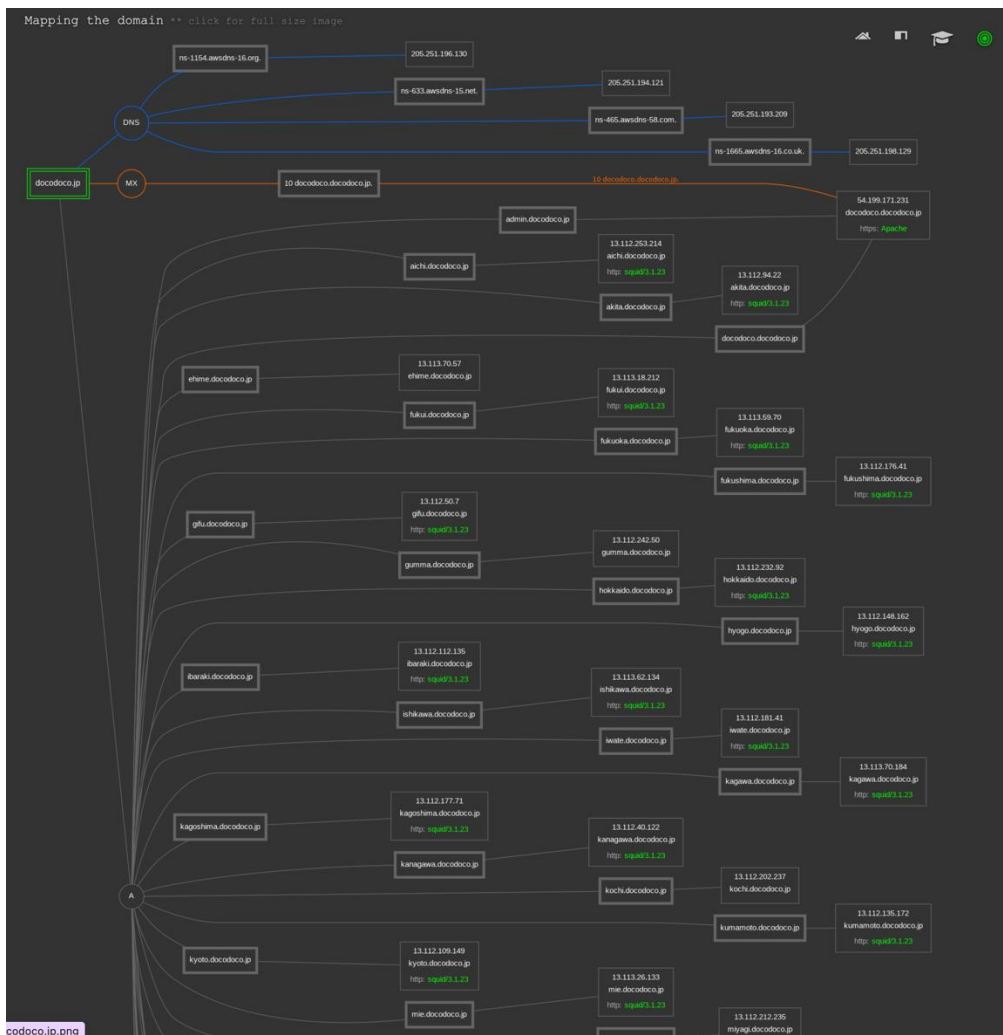
## • サーバ情報(Aレコード)

Host Records (A) \*\* this data may not be current as it uses a static database (updated monthly)

admin.docodoco.jp	54.199.171.231	AMAZON-02 Japan
aichi.docodoco.jp	13.112.253.214	AMAZON-02 Japan
akita.docodoco.jp	13.112.94.22	AMAZON-02 Japan
docodoco.docodoco.jp	54.199.171.231	AMAZON-02 Japan
ehime.docodoco.jp	13.113.70.57	AMAZON-02 Japan
fukui.docodoco.jp	13.113.18.212	AMAZON-02 Japan
fukuoka.docodoco.jp	13.113.59.70	AMAZON-02 Japan
fukushima.docodoco.jp	13.112.176.41	AMAZON-02 Japan
gifu.docodoco.jp	13.112.50.7	AMAZON-02 Japan
gumma.docodoco.jp	13.112.242.50	AMAZON-02 Japan
hokkaido.docodoco.jp	13.112.232.92	AMAZON-02 Japan
hyogo.docodoco.jp	13.112.148.162	AMAZON-02 Japan
ibaraki.docodoco.jp	13.112.112.135	AMAZON-02 Japan
ishikawa.docodoco.jp	13.113.62.134	AMAZON-02 Japan
iwate.docodoco.jp	13.112.181.41	AMAZON-02 Japan
kagawa.docodoco.jp	13.113.70.184	AMAZON-02 Japan
kagoshima.docodoco.jp	13.112.177.71	AMAZON-02 Japan

# dnsdumpster

- 各種データの関連性の表示





## ● 証明書情報の検索

- ウェブサイトの証明書を  
確認したいとき、過去の  
ものまで遡って調べること  
ができてしまうサイト。実  
際に稼働していなくても、  
発行されている証明書  
について内容を確認する  
ことができる。
- ドメイン名のみを入れる  
ことで、サブドメインの証  
明書も確認が可能。

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	13181138631	2024-05-26	2024-05-26	2025-06-25	report.docodoco.jp	report.docodoco.jp	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	13031738372	2024-05-13	2024-05-13	2025-06-12	report-stg.docodoco.jp	report-stg.docodoco.jp	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	12516574905	2024-03-28	2024-03-28	2025-04-26	dsp.docodoco.jp	dsp.docodoco.jp	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	12508389277	2024-03-28	2024-03-28	2025-04-26	dsp.docodoco.jp	dsp.docodoco.jp	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	12339263194	2024-03-10	2024-03-10	2025-04-11	*.docodoco.jp	*.docodoco.jp	C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA OV SSL CA 2018
	12131502698	2024-02-20	2024-02-20	2025-03-21	v6.docodoco.jp	v6.docodoco.jp	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	12050031446	2024-02-12	2024-02-12	2025-03-13	api.docodoco.jp	api.docodoco.jp	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	12049997306	2024-02-12	2024-02-12	2025-03-13	www.docodoco.jp	www.docodoco.jp	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	12013572211	2024-02-08	2024-02-08	2025-03-09	knowledge.docodoco.jp	knowledge.docodoco.jp	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	12013205337	2024-02-08	2024-02-08	2025-03-09	knowledge.docodoco.jp	knowledge.docodoco.jp	C=US, O=Amazon, CN=Amazon RSA 2048 M02
	1249677635	2023-06-26	2023-06-26	2024-07-24	report.docodoco.jp	report.docodoco.jp	C=US, O=Amazon, CN=Amazon RSA 2048 M01
	9640763560	2023-06-13	2023-06-13	2024-07-11	report-stg.docodoco.jp	report-stg.docodoco.jp	C=US, O=Amazon, CN=Amazon RSA 2048 M01
	8944183454	2023-03-21	2023-03-21	2024-04-19	v6.docodoco.jp	v6.docodoco.jp	C=US, O=Amazon, CN=Amazon RSA 2048 M01
	8873159009	2023-03-13	2023-03-13	2024-04-11	api.docodoco.jp	api.docodoco.jp	C=US, O=Amazon, CN=Amazon RSA 2048 M01
	887291767	2023-03-13	2023-03-13	2024-04-11	www.docodoco.jp	www.docodoco.jp	C=US, O=Amazon, CN=Amazon RSA 2048 M01
	8872764417	2023-03-07	2023-03-07	2024-04-07	*.docodoco.jp	*.docodoco.jp	C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA OV SSL CA 2018
	862228494	2023-02-10	2023-02-10	2023-05-19	v6.docodoco.jp	v6.docodoco.jp	C=US, O=Amazon, CN=Amazon RSA 2048 M01
	6729290316	2022-05-14	2022-04-19	2023-05-19	v6.docodoco.jp	v6.docodoco.jp	C=US, O=Amazon, OU=Server CA 18, CN=Amazon
	6570482542	2022-04-19	2022-04-19	2023-05-19	v6.docodoco.jp	v6.docodoco.jp	C=US, O=Amazon, OU=Server CA 18, CN=Amazon
	6180508680	2022-02-15	2022-02-15	2023-03-19	*.docodoco.jp	*.docodoco.jp	C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA OV SSL CA 2018
	4012275843	2021-01-31	2021-01-31	2021-05-01	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=R3
	4012270311	2021-01-31	2021-01-31	2021-05-01	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=R3
	4012275325	2021-01-31	2021-01-31	2021-05-01	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=R3
	4012275186	2021-01-31	2021-01-31	2021-05-01	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=R3
	3984401133	2021-01-26	2021-01-26	2022-02-27	*.docodoco.jp	*.docodoco.jp	C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA OV SSL CA 2018
	3728644674	2020-12-02	2020-12-02	2021-03-02	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=R3
	3728640061	2020-12-02	2020-12-02	2021-03-02	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=R3
	3462950449	2020-10-03	2020-10-03	2021-01-01	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	3462921026	2020-10-03	2020-10-03	2021-01-01	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	3186550211	2020-08-03	2020-08-03	2020-11-01	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	3186551404	2020-08-03	2020-08-03	2020-11-01	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2937598512	2020-06-04	2020-06-04	2020-09-02	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2905551350	2020-06-04	2020-06-04	2020-09-02	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2667191844	2020-04-04	2020-04-04	2020-07-03	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2667191844	2020-04-04	2020-04-04	2020-07-03	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2432844077	2020-02-04	2020-02-04	2020-05-04	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2415035864	2020-02-04	2020-02-04	2020-05-04	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2379323018	2020-01-26	2020-08-25	2010-08-26	www.docodoco.jp	www.docodoco.jp	C=BE, OU=Domain Validation CA, O=GlobalSign nv-sa, CN=GlobalSign Domain Validation CA
	2379320537	2020-01-26	2020-06-17	2010-07-21	api.docodoco.jp	api.docodoco.jp	C=BE, OU=Domain Validation CA, O=GlobalSign nv-sa, CN=GlobalSign Domain Validation CA
	2359725885	2020-01-22	2020-01-05	2021-02-23	*.docodoco.jp	*.docodoco.jp	C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA OV SSL CA 2018
	2289054220	2020-01-05	2020-01-05	2021-02-23	*.docodoco.jp	*.docodoco.jp	C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA OV SSL CA 2018
	2211403387	2019-12-06	2019-12-06	2020-03-05	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2181468046	2019-12-06	2019-12-06	2020-03-05	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2231846135	2019-12-06	2019-12-06	2020-03-05	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2200195171	2019-12-06	2019-12-06	2020-03-05	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1972518444	2019-10-07	2019-10-07	2020-01-05	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1970546240	2019-10-07	2019-10-07	2020-01-05	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1748348305	2019-08-04	2019-08-04	2019-11-02	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1739329879	2019-08-04	2019-08-04	2019-11-02	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1553204446	2019-06-05	2019-06-05	2019-09-03	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1540662329	2019-06-05	2019-06-05	2019-09-03	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1362139201	2019-04-06	2019-04-06	2019-07-05	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1355598480	2019-04-06	2019-04-06	2019-07-05	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1176057527	2019-02-05	2019-02-05	2019-05-06	www3.docodoco.jp	www3.docodoco.jp	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

# 自組織の構成を再確認

- **シャドーITがないかの確認**
  - dnscumprsterやcrt.shなどを利用して、把握していない機器やサーバがないかを確認する。
- **各種機器が外部からどう見えているかを確認**
  - 自組織内で、インターネットに直接接続している機器(グローバルIPアドレスが設定されている)をshodanで検索し、不要なポートが空いていないか、脆弱性が残っていないかを確認する。
- **運用として回していく**
  - これらのことを一度確認して終わりではなく、定期的に確認することが必要。

# 対策とは

# 対策は難しくない

- **自組織の構成を整理する（資産管理、構成管理）**
  - ネットワーク構成図は論理構成図だけではなく、物理構成図も。
  - 各機器の利用OSやその中で稼働しているミドルウェアのバージョンを正確に把握する。
- **セキュリティアップデート**
  - 各機器のセキュリティアップデートについては、迅速に対応する。
  - 特に個人利用PC以外の機器については、先延ばしになってしまっていることが多いが、そこそそが外部からの侵入の足がかりになっている。

# 対策は難しくくない

## • ID管理

- VPNなどの機器へのログイン、RDPでのPCへのログインには、IDとパスワードを使用している場合が多いと思われるが、そこで使用しているIDやパスワードを適切に管理すること。
- パスワードは適切な複雑度を満たしていれば、定期的な変更は必要ではない。
- 適切に設定したIDやパスワードでも、それらが外部へ流出してしまえば、IABに利用されてしまうので、そのようにならないように管理する。
- また、インターネット越しにログインする必要がある環境においては、可能ならば、アクセス元IPアドレスの制限、MFAへの対応、証明書の利用など、IDやパスワードのみに依存しない仕組みを導入する。

# 対策は難しくない

## • アクセス元の確認（ログの確認）

- 普段からネットワーク機器などへのログイン状態を確認する仕組みを構築する。
- ログインが成功したものだけではなく、失敗しているログを確認することで、不正にアクセスしようとしているアクセス元(IPアドレス)が確認できる。
- アクセスに失敗しているIPアドレスには、通常の利用目的とは異なり、位置情報を隠蔽する目的に利用されているアドレスが使われている場合があるので、特にそのような場合には、ブロックするなどの対応を適切に行う必要がある。

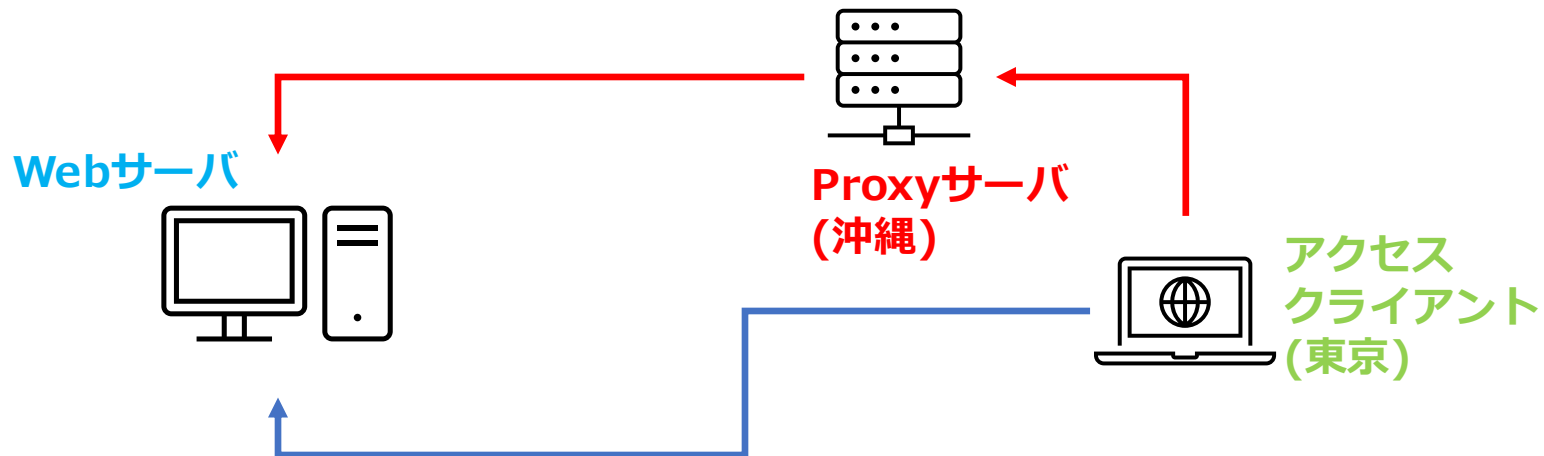
## • 匿名化技術

- 通信元(IPアドレス)を秘匿化する技術やツールを使い、通信元を特定しづらくすることであり、このようなアクセスは、違法・不法目的で使われ、オンライン取引におけるリスクと考えられる。
- このような方法には下記にあげる4種類がある。
  - ① Proxy
  - ② VPN
  - ③ VPS/Cloud
  - ④ Tor
- 匿名ネットワーク(匿名化技術を利用したネットワーク)からのアクセスであるかを監視する必要がある。

# 匿名化技術①

## • Proxy(プロキシ)

- プロキシサーバとは、インターネット接続を直接させない内部ネットワークのクライアントPCの代理として、インターネット接続を行うサーバのこと。
- アクセス先のWebサーバでは、クライアントPCのIPアドレスは隠蔽され、プロキシサーバのIPアドレスが送信元として見えることで、位置情報もプロキシサーバの情報になる。
- 下記の図では、Proxyサーバ経由では、沖縄からのアクセスに見える。

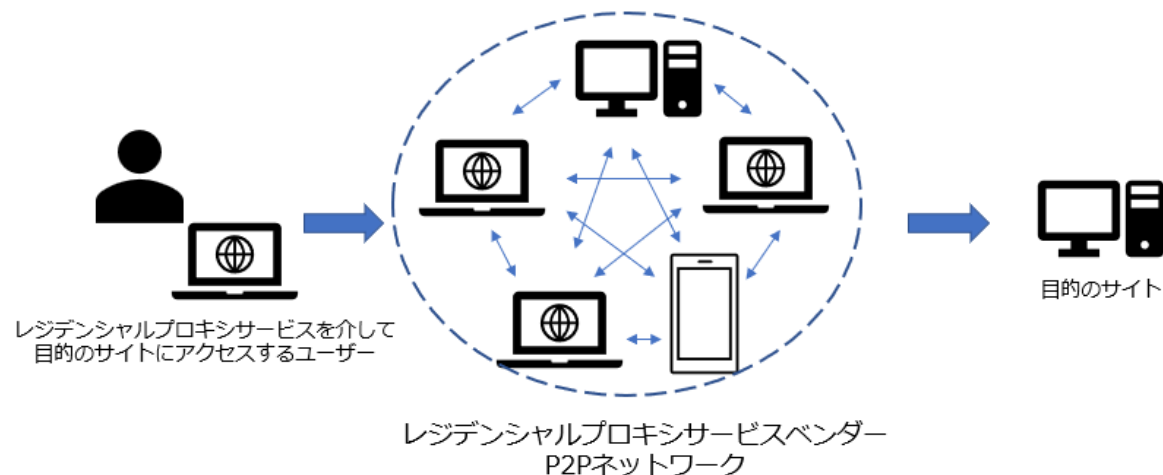




# 匿名化技術①

## • レジデンシャル・プロキシ

- このサービスを介してWebにアクセスした場合、本来のIPが隠れてしまい、実在するIPからのアクセスと判断されてしまうため、不正利用をブロックすることが困難になる。
- サービスベンダーによって方法は異なるが、下記のように、特にP2Pを利用しているベンダーがあることから本来のアクセス元の特定がより困難となる。
  - サービスベンダーが個別にISPと契約し、IPを付与したサーバーを用意する。
  - P2Pを使用して稼働中デバイスを経由する。



# 匿名化技術②

## • VPN(Virtual Private Network)

- 公開VPNサービス
  - 無料で利用できるサービスがあり、それを経由したアクセスは、Proxyと同様に位置情報を匿名化することができる。
- 匿名VPNサービス
  - 公開VPNに対して匿名VPNは、ログを取らずに匿名性を謳っている。
  - 匿名VPNサービスの例

サービス名	特徴
<b>ExpressVPN</b> <a href="https://www.expressvpn.com/jp">https://www.expressvpn.com/jp</a>	<ul style="list-style-type: none"> <li>• 最速で、高レベルのセキュリティ機能を提供。</li> <li>• 月約13ドルで、世界105カ国にサーバを設置。</li> </ul>
<b>NordVPN</b> <a href="https://nordvpn.com/ja/">https://nordvpn.com/ja/</a>	<ul style="list-style-type: none"> <li>• 世界60カ国で、5,500台以上のサーバを運用している。</li> <li>• 月500円から（最初の2年の割引価格）</li> </ul>
<b>MullvadVPN</b> <a href="https://millenvpn.jp/">https://millenvpn.jp/</a>	<ul style="list-style-type: none"> <li>• 日本の企業が提供しているサービス。</li> <li>• 月額400円からで、10デバイスで利用可能。</li> </ul>
<b>CyberGhost</b> <a href="https://www.cyberghostvpn.com/ja/">https://www.cyberghostvpn.com/ja/</a>	<ul style="list-style-type: none"> <li>• 長期プランの場合、月額320円から。</li> <li>• 6,800台を超えるサーバ。</li> </ul>

# 匿名化技術③

## • VPS/Cloud

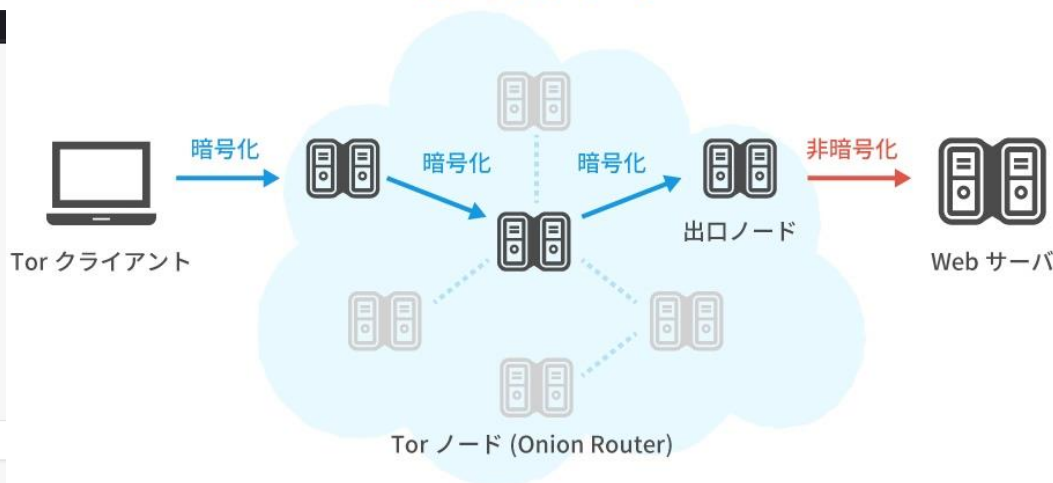
- VPS/Cloudとは、クラウドサービスやレンタルサーバ事業者に割り当てられているIPアドレスになる。
- このようなサービスのコンピュータは、Webサイトなどの外部向けのサービスを行うために利用するものであり、一般のユーザが通常の利用にて、これらのサーバ類を経由してアクセスすることは考えにくい。
- 一方、上記サーバにおいて、データ収集のために各種サイトをアクセスしていることもあるため、一概に怪しいアクセスとは判定できない。

# 匿名化技術④

## • Tor(The Onion Router)

- 複数のノードを経由する仮想回線接続(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のこと。
- 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。
- ドメインが「.onion」になるので、専用のブラウザ(Torブラウザ)が必要になるが、それを利用すれば、容易に閲覧できる。

Tor ネットワーク



# 匿名化技術④

## • Torネットワーク内の世界

- いわゆるダークウェブと呼ばれていて、闇サイトとして稼働している場合も多く、代表的なのは、以下のようなものがある。
  - 偽造カードやパスポートの販売
  - 大麻や麻薬の取引
  - ランサムウェアグループ(RaaS)の犯罪声明サイト
- ProxyやVPNより匿名性が高いため、その目的で利用することが多くある。
- ただし、Torネットワークから通常のインターネットへの接続点としてのIPアドレスは公開情報であるので、監視することは可能である。

# アクセス元の確認の重要性

## • 匿名ネットワーク利用状況

- Proxy(公開Proxy,レジデンシャルプロキシ)、Tor(出口ノード,Torネットワーク中間ノード)、VPNサービス事業者、VPS/クラウドサービス事業者の調査検証を実施。
- IP数：2024年7月での判定数
- SURFPOINT™ 搭載IPv4アドレス総数：約37億

	IP数	保有率(%)
Proxy	28,374	<b>0.00076</b>
Tor	15,293	<b>0.00041</b>
VPN	60,653	<b>0.00163</b>
VPS/Cloud	175,099,256	<b>4.71975</b>

# アクセス元の確認の重要性

## • 匿名ネットワーク利用状況

- 下記データは、2024年6月~7月の1ヶ月平均数
  - アクセス率(%) : IP数/利用されたIP総数(約5.5億)
  - 使用率 : アクセス率/保有率

- **VPS以外は、IPアドレスの保有率より遥かに多く、使用率が高いことがわかる**

	アクセス率(%)	使用率
Proxy	0.0467	<b>61.0</b>
Tor	0.0040	<b>9.7</b>
VPN	0.0063	<b>3.8</b>
VPS/Cloud	2.1732	<b>0.46</b>

## • 脆弱性情報を常に確認する

- CVE(Common Vulnerabilities and Exposures)番号
  - 情報セキュリティの脆弱性などをリスト化した辞書で、問題となる脆弱性を一意に識別するためCVE-ID(CVE識別番号)を付与している。CVE-IDは、「CVE-〈西暦年号〉-〈連番〉」の体系となっている。
  - 日本国内では、JVN(Japan Vulnerability Notes)という脆弱性データベースがあり、JPCERT/CCとIPA(情報処理推進機構)が共同で運営しており、JVNで公表する脆弱性に対して、CVEの割り当ての申請を行っている。
  - <https://cve.mitre.org/>
- JVN pedia
  - <https://jvndb.jvn.jp/>
- その他の情報
  - <https://www.jpccert.or.jp/vh/top.html>
  - <https://www.ipa.go.jp/security/vuln/scap/cve.html>



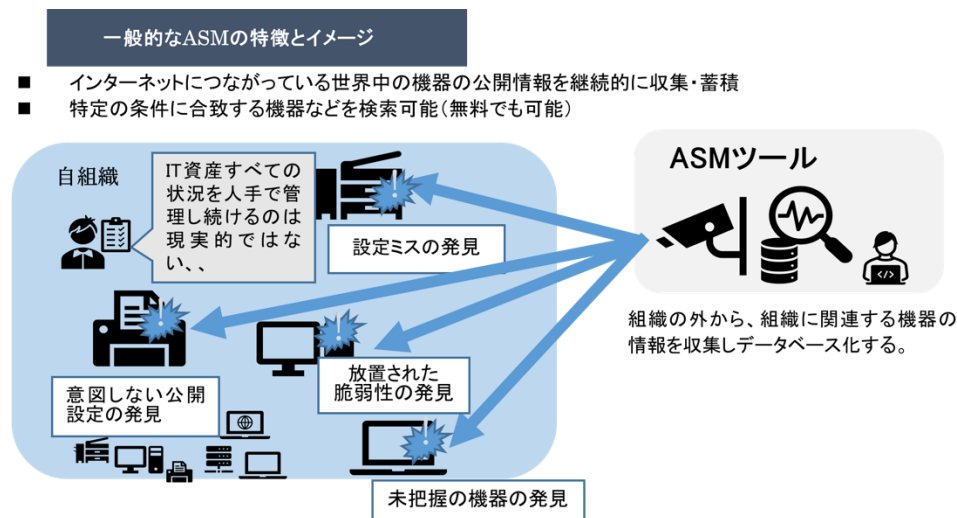
# 情報収集と対策

- **脆弱性情報を常に確認するのは大変、…。**
  - X(Twitter)のアカウントをフォローする。
    - IPA(JVNiPedia) : @JVNiPedia
    - JVNレポート : @jvnjp
    - JPCERTコーディネーションセンター : @jpcert
  - jpcertによるRSS配信
    - <https://www.jpcert.or.jp/rss/>
  - これらの情報と自組織の機器の情報を照らし合わせ、機器に該当する脆弱性があったときには対策する。
    - と言われても、常にこれを調べているのは大変、…。

# アタックサーフェスマネジメント

## • ASM(Attack Surface Manegement)

- ASMは、組織の外部(インターネット)からアクセス可能なIT資産を発見し、それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセスのこと。
- ASMの継続的な実施により、組織管理者の未把握の機器や意図しない設定ミスを攻撃者視点から発見でき、脆弱性管理活動において、リスク低減の効果が期待される。
- ASMを提供するサービス(ツール)が出てきているので、これで自動化することが可能。



<https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html>

# アクティブサイバーデフェンス

- サイバー空間では、圧倒的に攻撃側が有利
  - 1箇所でも、欠点(穴)があれば、そこから侵入してきてしまう。
- アクティブサイバーディフェンスとは
  - 能動的サイバー防衛とも呼ばれ、脅威情報の活用により攻撃被害が出る前にリアルタイムな検知、阻止を目指すアプローチのこと。
  - 政府においても、2024年6月に有識者会議が開かれ、国としては、平時から通信を監視し、基幹インフラへの攻撃などの兆候を探り、兆候段階で相手のシステムに入り無害化する仕組みを指す。
  - 今後としては、官民での情報共有を目指しているので、通信状態を把握していく必要がある。

## • 組織内の教育

- ネットワーク、機器の脆弱性対策を施すことで、外部からの侵入を防ぐことには対応は可能。
- あとは、内部者への侵入の経路をどのように防ぐのかという課題になる。
  - ソフトウェアや機器の設定や監視で防御
    - サプライチェーンを利用して、脆弱な組織からのアクセス。
    - ウィルス対策ソフトから、EDR、XDEへ
  - 人の努力
    - フィッシング、ビジネス詐欺メール。
    - ゼロデイを利用した、利用者の環境の乗っ取り。

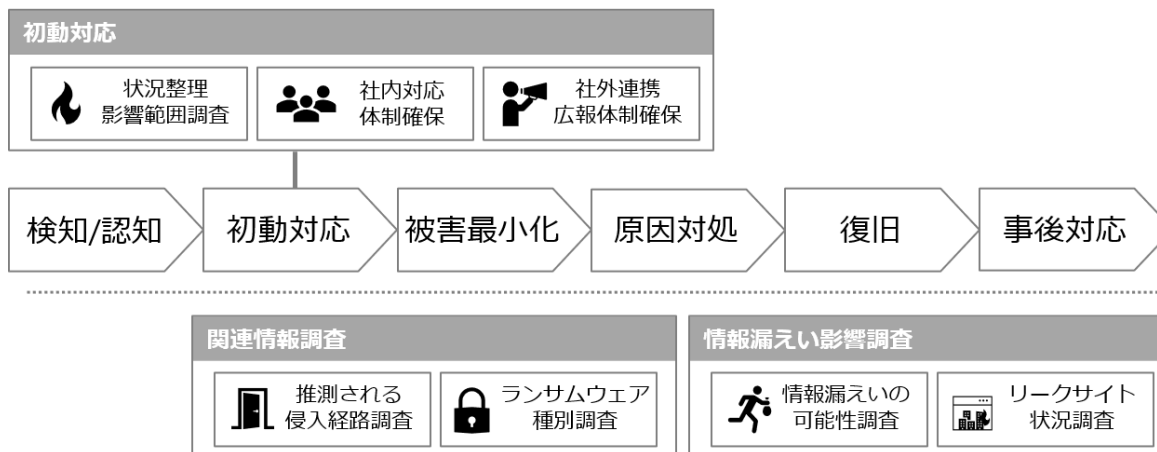
# それでも事件は起きる

## • 事前に手順を確認する

- 発生が予想されるインシデントごとに事前に対応の手順を確認し、実際に予行演習をする。
- 利用ユーザ、システム管理者、経営者と役割を設定し、組織全体として対応する手順を決めておく。

(例)侵入型ランサムウェア攻撃を受けたら読むFAQ

<https://www.jpccert.or.jp/magazine/security/ransom-faq.html>



# それでも事件は起きる

## • 万が一へ準備

- インシデントが発生したときには、予想以上の費用がかかる。
  - 特定非営利活動法人日本ネットワークセキュリティ協会(JNSA)が2021年8月18日に「インシデント損害額調査レポート」として発表した。
  - <https://scan.netsecurity.ne.jp/article/2021/08/20/46161.html>
- 調査に時間がかかる。
  - インシデントが発生してから、調査を実施してくれる会社を探して契約してとなると、実際の調査までに時間がかかってしまう。
  - あらかじめ対応可能な会社との契約が済んでいると、速やかに調査が進められる。
- 費用と時間への対策
  - サイバー保険の加入という方法もある。

# ニューノーマル時代の対策

## • オンプレミスからクラウドへ

- VPNやRDPを利用して、社内インフラ(オンプレミス)へアクセスする前提になっていると、そのエンドポイントを攻撃者に狙われるので、社内インフラをクラウド環境やサービスへ移行する。
- 共有ファイルサーバなどをクラウドストレージへ。
  - 自分たちでバックアップを取る必要がなくなる。
  - ランサムウェアの直接的な被害を受けにくい。
- 社内で利用しているアプリケーションもSaaSへの移行へ。
  - VPNやRDPを利用せずに、アプリケーションを利用できる。
- VDI(仮想デスクトップ)を導入することで、情報漏洩の防止にもつながる。
  - どこからでも、自分の環境をいつでも利用可能になる。
  - 外部インターフェイスを制限することが可能になる。

# ニューノーマル時代の対策

## ・クラウド移行での留意点

### ・ 移行のための費用

- ・ サービスの利用の費用以外に、初期の移行のための工数を検討する。
- ・ いわゆるサブスクでの利用になるので、オンプレミスの時よりは、見た目の費用は増加する。一方運用するために目に見えないコストとのバランスをあわせて検討する。

### ・ クラウド利用のためのスキル

- ・ オンプレミスでの運用と、クラウドでの運用ではセキュリティポリシーや運用基準が変わるので、そこを理解できるメンバが必要になる。

### ・ 多要素認証の導入

- ・ クラウドサービスには、多要素認証(2段階認証)を必須となっているものが増えてきているが、その際には認証に利用するスマートフォンは、MDMを利用して管理する。