医療機関様におけるサイバーセキュリティー対策について

日本通信機器株式会社

背景

・医療機関に対するサイバー攻撃が増加しており、サイバー攻撃により診療が停止する事案が発生
　⇒2021年　徳島県つるぎ町立半田病院（一部診療停止）
　⇒2022年　大阪急性期・総合医療センター（診療停止期間　およそ2か月）

・サイバー攻撃により、医療に関する患者の個人情報が窃取されるなど甚大な被害となる可能性有

・2023年4月1日　医療法施行規則改正、**サイバーセキュリティ確保のための措置を講じる規則**の新設により、医療機関等へのサイバーセキュリティが義務化
（適切な対応は、「医療情報システムの安全管理に関するガイドライン」（以下「安全管理ガイドライン」）を参照）

・2023年5月31日　安全管理ガイドライン改定（第6版）、情報セキュリティに対する考え方を整理し、医療機関が優先的に取組むべき事項（**医療機関におけるサイバーセキュリティ対策チェックリスト**）提供
　⇒医療機関への立入検査を示唆

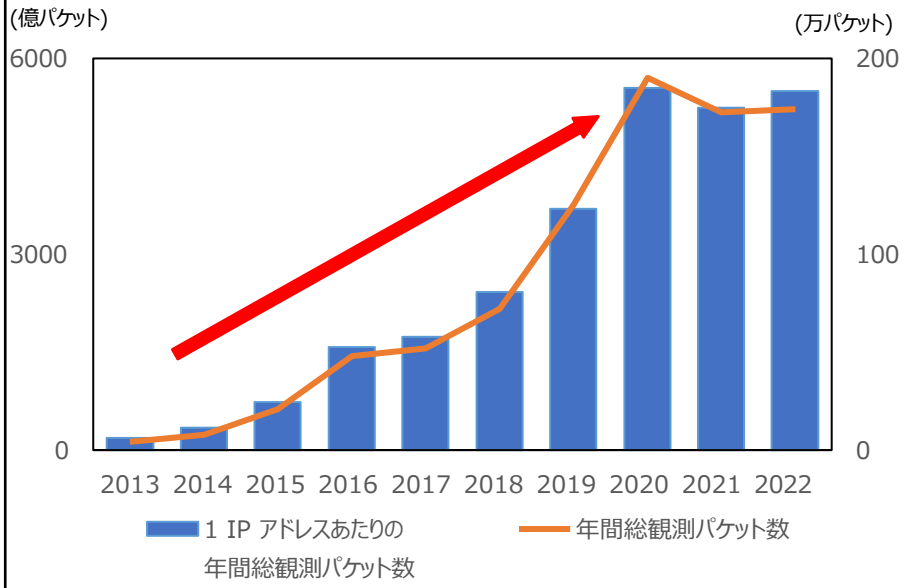
「サイバー攻撃＝事業継続リスク」であるという認識を持ち、
院内の情報（医療情報、個人情報等）を適切に管理するための**「安全ガイドライン」遵守**するため

セキュリティ診断で現状の確認をし、セキュリティ対策、ネットワーク機器最新化等の安心なネットワーク環境についてご提案します！

サイバー空間をめぐる脅威の情勢等

サイバー攻撃関連通信数の推移

⇒ とりまく脅威は増加の一途



出典元:NICT 国立研究開発法人情報通信研究機構の「観測レポート2022」の公表内容を元に整理

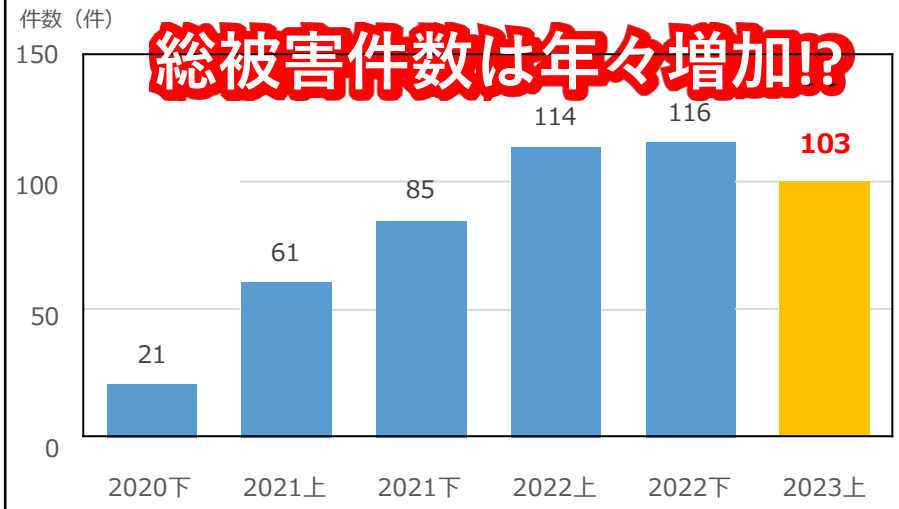
ランサムウェアとは

・「身代金」を意味する英語「ランサム（Ransom）」と「ソフトウェア（Software）」とを組み合わせた造語で金銭（身代金）を要求する不正プログラム

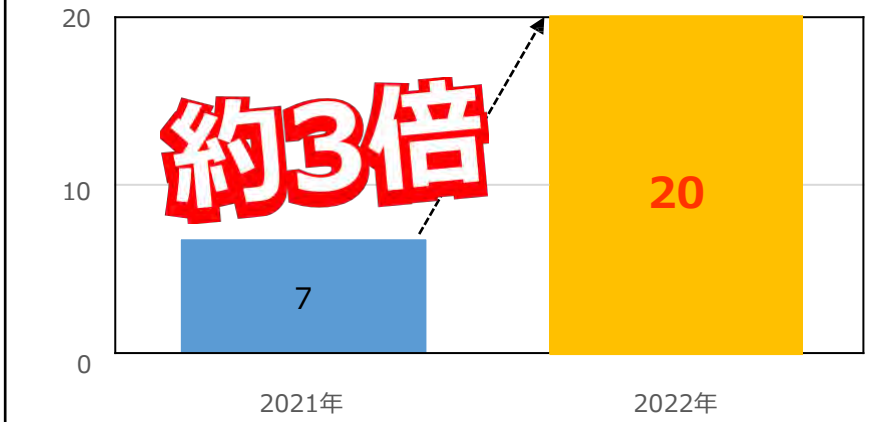
- PC等に保存されているファイルを暗号化され**使用不可に**
- 復旧と引き換えに**金銭を要求される**
- 情報を搾取しそれを**公開**、攻撃を受けている事を**公表**すると脅迫

企業・団体における ランサムウェア被害の報告件数推移

⇒「ランサムウェア」被害が急拡大



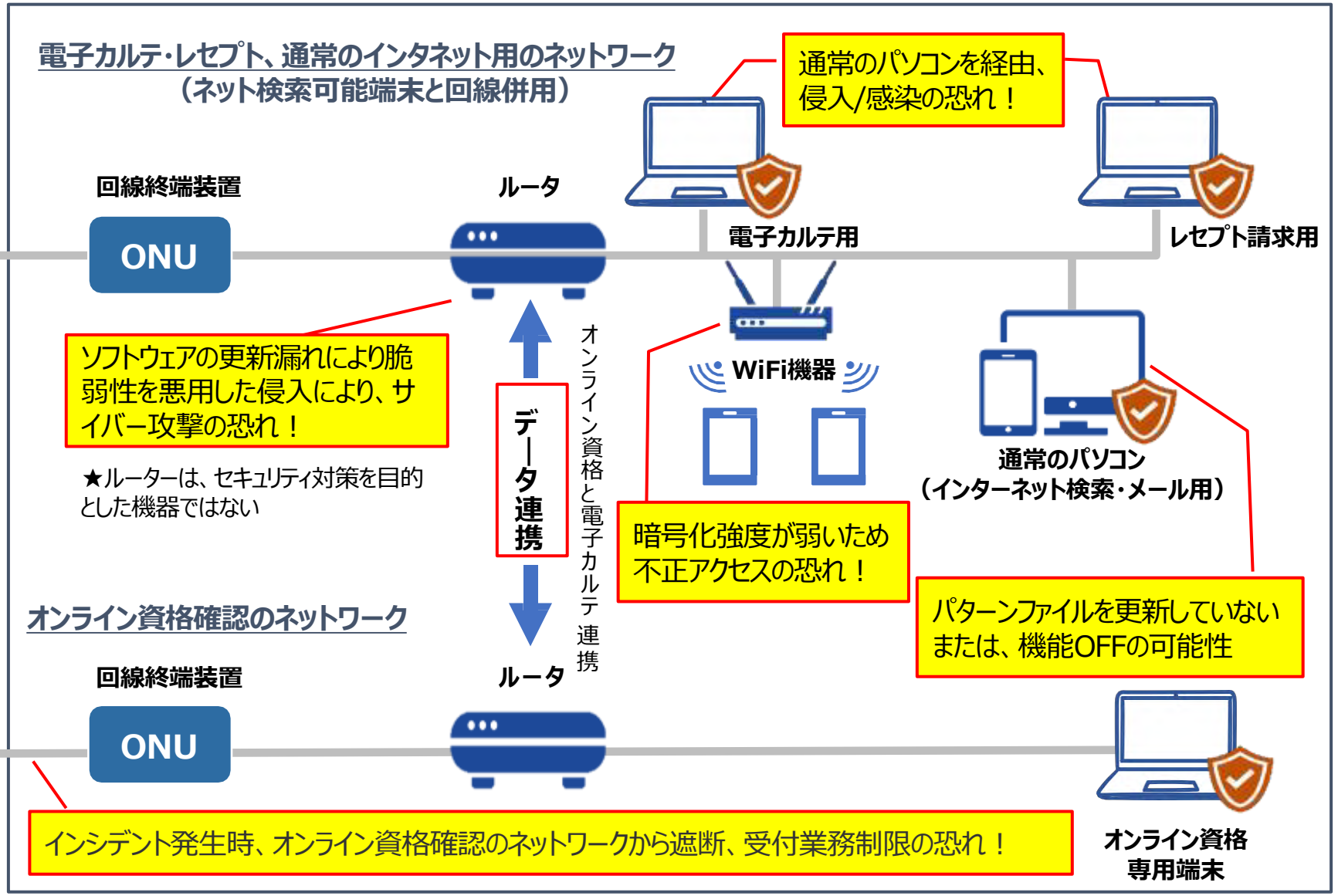
医療機関における ランサムウェア被害の報告件数推移



出典元:警察庁「サイバー空間をめぐる脅威の情勢等」（R3年、R4年）の公表内容を元に整理

院内ネットワークの一例

「閉域網は安全」という“閉域網神話”で対策は遅れていませんか？



安全ガイドライン　第6.0版の主な改定ポイント

出典元：厚生労働省「医療情報システムの安全管理に関するガイドライン第6.0版の主な改定ポイント（概要）」

医療情報システムの安全管理に関するガイドライン 第6.0版主な改定ポイント（概要）

次頁参照

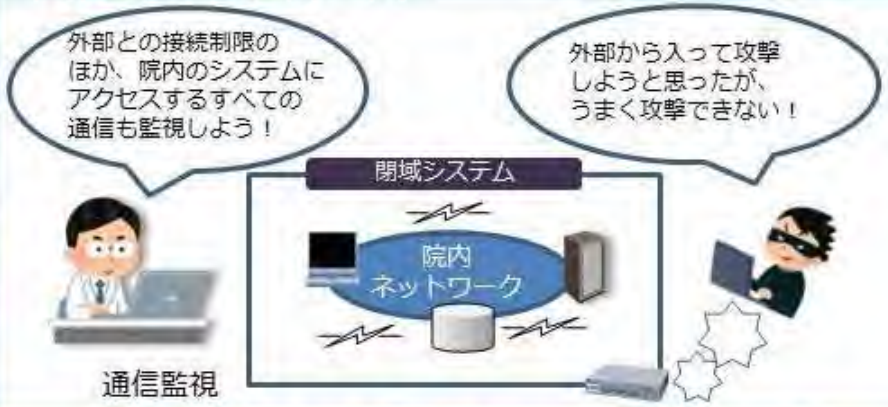
外部委託、外部サービスの利用に関する整理

クラウドサービスに医療情報システムの運用管理を、すべてを外部に任せる場合

クラウドサービスに医療情報システムの一部を運用管理を外部に任せる場合

ネットワーク境界防御型思考／ゼロトラストネットワーク型思考

ゼロトラストの思考を取り入れることで、個々の外部からの侵入にも適切な対応が可能となります。



災害、サイバー攻撃、システム障害等の非常時に対する対応や対策

非常時場面ごとのバックアップの考え方の違い（例）

本人確認を要する場面での運用（eKYCの活用）の検討

＜参考①＞境界防御型思考とゼロトラスト思考の比較

出典元：厚生労働省「医療情報システムの安全管理に関するガイドライン システム運用編」より引用

【用語の定義】
オープンな環境：管理者により管理されていない環境
オープンではない環境：管理者により管理されている環境

境界防御思考	ゼロトラスト思考
	
• オープンではない環境では、境界部分への侵入を防ぐため、監視を行う。 • オープンではない環境では、医療情報等、特に重要な情報の管理を行う。	• いずれの環境においても、情報資産へのアクセスは**不正なものが含まれることを前提（ゼロトラスト）**に、全てを検証。 • 検証は、情報資産に対するアクセスにおいて不正なトラフィックやアクセス等の異常行動などが起点。
✓ 境界防御では、サイバー攻撃への対応としては十分ではないため、境界防御を採用の場合、トラフィックの監視等、**多層防御の考え方を導入**することが求められる。	✓ ゼロトラスト思考の有効性は、認められているものの、実装するには現時点では費用や管理に対する**負担が大きく、小規模の医療機関等で導入は容易ではない。**

＜参考②＞医療機関におけるサイバーセキュリティ対策チェックリスト（令和５年６月）抜粋

出典元：厚生労働省「医療機関におけるサイバーセキュリティ対策チェックリスト（令和５年６月）及び「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル」より引用

○　令和５年度中

*以下項目は令和５年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*２（２）及び２（３）については、事業者と契約していない場合には、記入不要です。
*1回目の確認で「いいえ」の場合、令和５年度中の対応目標日を記入してください。

医療機関確認用

	チェック項目	確認結果（日付）			備考
		１回目	目標日	２回目	
１ 体制構築	（１）　医療情報システム安全管理責任者を設置している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
２ 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**				
	（１）　サーバ、端末PC、ネットワーク機器の台帳管理を行っている。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（２）　リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（３）　事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	サーバについて、以下を実施している。				
	（４）　利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（５）　退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（６）　アクセスログを管理している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	ネットワーク機器について、以下を実施している。				
	（７）　セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（８）　接続元制限を実施している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
３ インシデント発生に備えた対応	（１）　インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	

■実施すべき対策■
・スキャン用ソフトウェアの導入
・パターンファイルの更新
・セキュリティ・ホール（脆弱性）が報告されているソフトウェアへのセキュリティパッチの適用

■実施すべき対策■
・ネットワーク機器に接続出来るMACアドレス限定、不正アクセス対策等

セキュリティ診断のトリセツ

エビデンスの重要性

診断内容とその詳細について

診　断

エビデンス

提　案

＊ ルータのログ確認

＊ 不正アクセスの状況確認とその意図の分析

＊ アドウェア・マルウェアの有無

＊ メールアドレスの流出確認

＊ ホームページの改ざん確認

＊ 二重ルータ・通信速度などのネットワーク状況分析

＊ ID・パスワード流出確認

＊ Wi-Fiのセキュリティレベルや設定内容確認

＊ 機微情報の有無

＊ ウイルス対策ソフトの有効性の確認

Evidence example

```
Windows IP 構成


イーサネット アダプター イーサネット:

   接続固有の DNS サフィックス . . . . .:
   リンクローカル IPv6 アドレス. . . . .: fe80::40e9:4b48:6f84:f622%11
   IPv4 アドレス . . . . . . . . . . . .: 192.168.2.33
   サブネット マスク . . . . . . . . . .: 255.255.255.0
   デフォルト ゲートウェイ . . . . . . .: 192.168.2.1
```

①

②

```
Wireless LAN adapter Wi-Fi:

   接続固有の DNS サフィックス . . . . .:
   リンクローカル IPv6 アドレス. . . . .: fe80::2ce4:ca09:5d09:8579%2
   IPv4 アドレス . . . . . . . . . . . .: 192.168.34.163
   サブネット マスク . . . . . . . . . .: 255.255.255.0
   デフォルト ゲートウェイ . . . . . . .: 192.168.34.1

イーサネット アダプター Bluetooth ネットワーク接続:

   メディアの状態. . . . . . . . . . . .: メディアは接続されていません
   接続固有の DNS サフィックス . . . . .:

C:\Users\Hamasuna>tracert -d 8.8.8.8

8.8.8.8 へのルートをトレースしています。経由するホップ数は最大 30 です

  1     1 ms     1 ms     1 ms  192.168.34.1
  2     4 ms     2 ms     2 ms  118.23.14.243
  3     4 ms     4 ms     5 ms  118.23.14.149
  4    14 ms     9 ms     3 ms  118.23.175.181
  5    12 ms    23 ms    18 ms  122.1.245.197
  6    10 ms    10 ms    10 ms  122.1.245.206
  7    28 ms    11 ms    11 ms  122.1.245.10
  8    10 ms    10 ms    10 ms  142.250.168.41
  9    11 ms    11 ms    13 ms  142.251.254.143
 10    28 ms    11 ms    10 ms  172.253.75.97
 11     9 ms     9 ms     8 ms  8.8.8.8

トレースを完了しました。
```

③

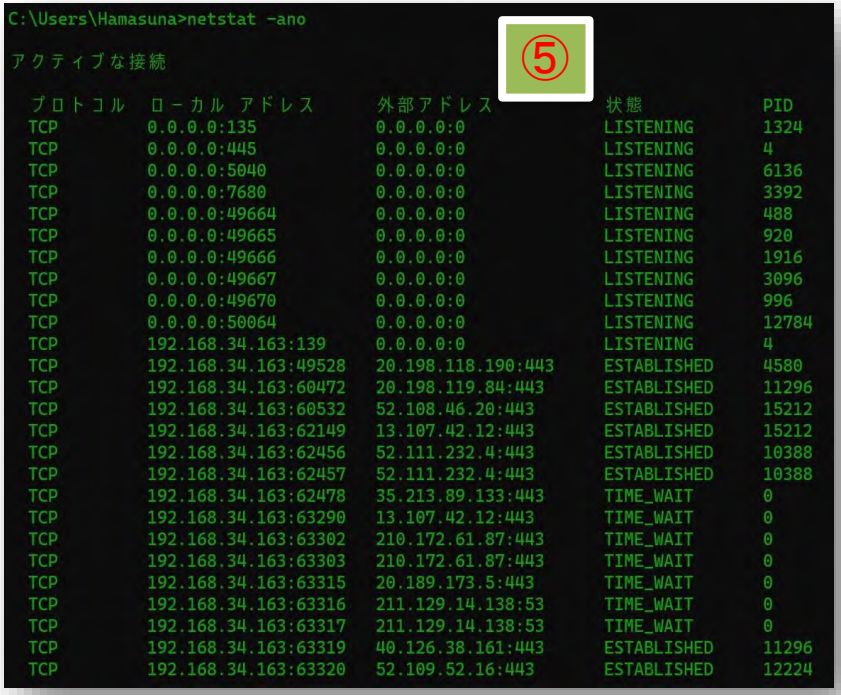
```
C:\Users\Hamasuna>netsh wlan show interfaces

システムに 1 インターフェイスがあります:

    名前                   : Wi-Fi
    説明                   : Intel(R) Wi-Fi 6 AX201 160MHz
    GUID                   : 0617ae2d-20bc-48aa-b31e-6bd574f12147
    物理アドレス           : 4c:77:cb:2a:a7:79
    インターフェイス 入力          : プライマリ
    状態                   : 接続されました
    SSID                   : Buffalo-A-5E40-WPA3
    BSSID                  : 00:e5:f1:25:5e:4a
    ネットワークの種類     : インフラストラクチャ
    無線の種類             : 802.11ax
    認証                   : WPA3-パーソナル
    暗号                   : CCMP
    接続モード         : 自動接続
    バンド                       : 5 GHz
    チャネル                   : 36
    受信速度 (Mbps)        : 1081
    送信速度 (Mbps)        : 1081
    シグナル               : 85%
    プロファイル           : Buffalo-A-5E40-WPA3
```

④

Evidence example

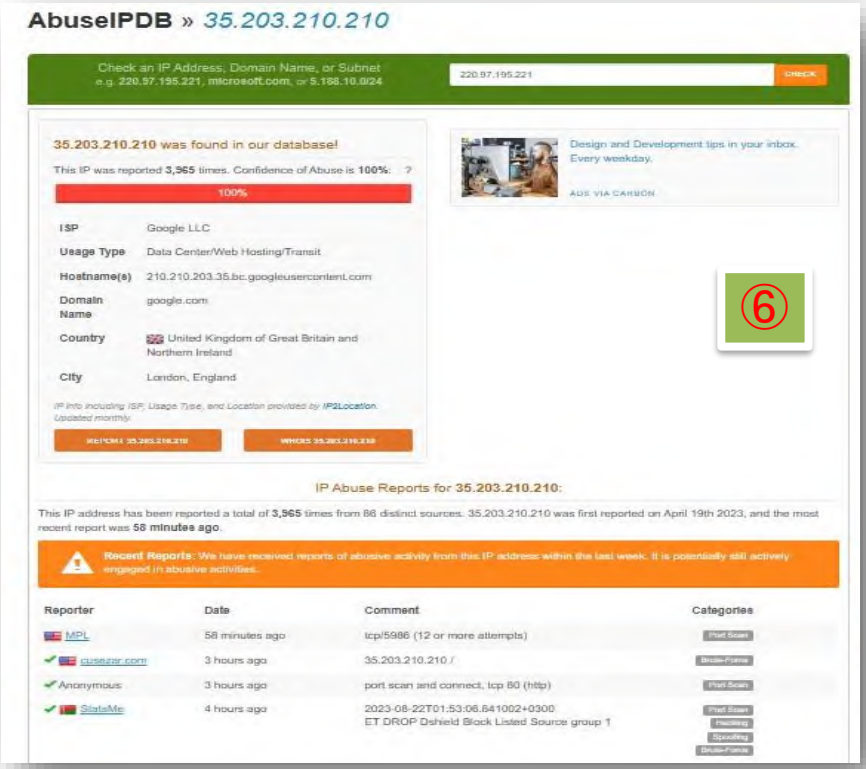


```
C:\Users\Hamasuna>netstat -ano

アクティブな接続

  プロトコル  ローカル アドレス          外部アドレス           状態           PID
  TCP         0.0.0.0:135            0.0.0.0:0              LISTENING       1324
  TCP         0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP         0.0.0.0:5040           0.0.0.0:0              LISTENING       6136
  TCP         0.0.0.0:7680           0.0.0.0:0              LISTENING       3392
  TCP         0.0.0.0:49664          0.0.0.0:0              LISTENING       488
  TCP         0.0.0.0:49665          0.0.0.0:0              LISTENING       920
  TCP         0.0.0.0:49666          0.0.0.0:0              LISTENING       1916
  TCP         0.0.0.0:49667          0.0.0.0:0              LISTENING       3096
  TCP         0.0.0.0:49670          0.0.0.0:0              LISTENING       996
  TCP         0.0.0.0:50064          0.0.0.0:0              LISTENING       12784
  TCP         192.168.34.163:139     0.0.0.0:0              LISTENING       4
  TCP         192.168.34.163:49528   20.198.118.190:443     ESTABLISHED     4580
  TCP         192.168.34.163:60472   20.198.119.84:443      ESTABLISHED     11296
  TCP         192.168.34.163:60532   52.108.46.20:443       ESTABLISHED     15212
  TCP         192.168.34.163:62149   13.107.42.12:443       ESTABLISHED     15212
  TCP         192.168.34.163:62456   52.111.232.4:443       ESTABLISHED     10388
  TCP         192.168.34.163:62457   52.111.232.4:443       ESTABLISHED     10388
  TCP         192.168.34.163:62478   35.213.89.133:443      TIME_WAIT       0
  TCP         192.168.34.163:63290   13.107.42.12:443       TIME_WAIT       0
  TCP         192.168.34.163:63302   210.172.61.87:443      TIME_WAIT       0
  TCP         192.168.34.163:63303   210.172.61.87:443      TIME_WAIT       0
  TCP         192.168.34.163:63315   20.189.173.5:443       TIME_WAIT       0
  TCP         192.168.34.163:63316   211.129.14.138:53      TIME_WAIT       0
  TCP         192.168.34.163:63317   211.129.14.138:53      TIME_WAIT       0
  TCP         192.168.34.163:63319   40.126.38.161:443      ESTABLISHED     11296
  TCP         192.168.34.163:63320   52.109.52.16:443       ESTABLISHED     12224
```

⑤



AbuseIPDB » 35.203.210.210

Check an IP Address, Domain Name, or Subnet
e.g. 220.97.195.221, microsoft.com, or 5.188.10.0/24

220.97.195.221 CHECK

35.203.210.210 was found in our database!

This IP was reported 3,965 times. Confidence of Abuse is 100%: ?

100%

ISP	Google LLC
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	210.210.203.35.bc.googleusercontent.com
Domain Name	google.com
Country	United Kingdom of Great Britain and Northern Ireland
City	London, England

IP Info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

REPORT 35.203.210.210 WHOIS 35.203.210.210

Design and Development tips in your inbox. Every weekday.

ADS VIA CARBON

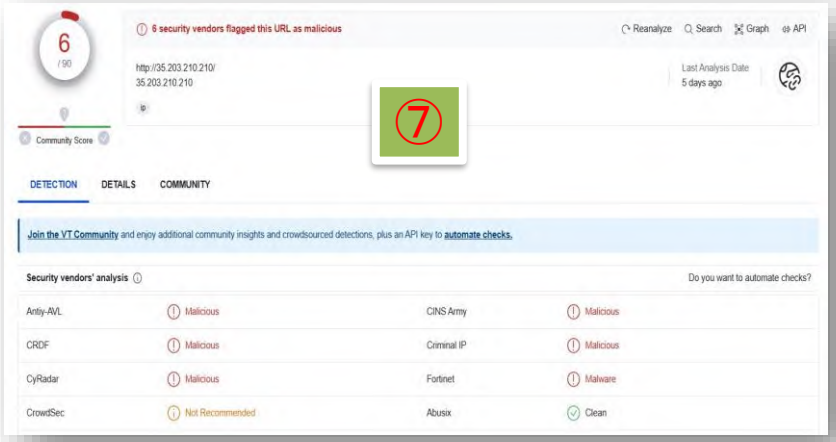
⑥

IP Abuse Reports for 35.203.210.210:

This IP address has been reported a total of 3,965 times from 86 distinct sources. 35.203.210.210 was first reported on April 19th 2023, and the most recent report was 58 minutes ago.

Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

Reporter	Date	Comment	Categories
MPL	58 minutes ago	tcp/5986 (12 or more attempts)	Port Scan
cusezar.com	3 hours ago	35.203.210.210 /	Brute-Force
Anonymous	3 hours ago	port scan and connect, tcp 80 (http)	Port Scan
StataMe	4 hours ago	2023-08-22T01:53:06.641002+0300 ET DROP Dshield Block Listed Source group 1	Port Scan, Hacking, Spoofing, Brute-Force



6 / 90

6 security vendors flagged this URL as malicious

Reanalyze Search Graph API

http://35.203.210.210/
35.203.210.210

Last Analysis Date
5 days ago

Community Score

DETECTION DETAILS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	Malicious	CINS Army	Malicious
CRDF	Malicious	Criminal IP	Malicious
CyRadar	Malicious	Fortinet	Malware
CrowdSec	Not Recommended	Abusix	Clean

⑦

IPアドレスから住所を検索できます。

172.16.254.1 search

IPアドレス、またはドメインを入力してください。

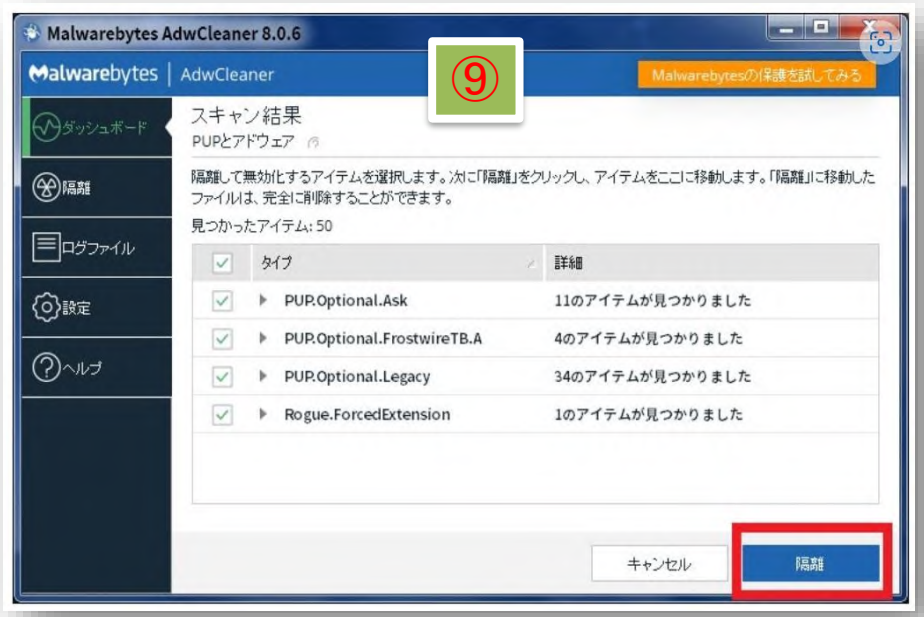
検索結果

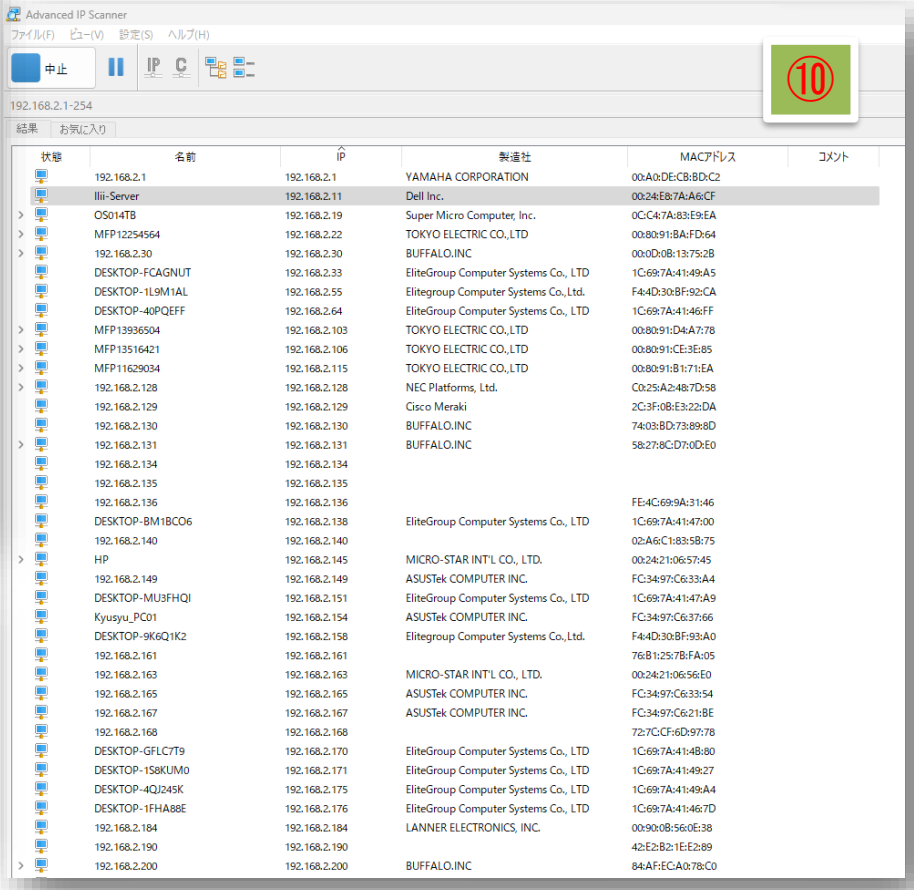
IPアドレス	45.146.164.196
ホスト名	45.146.164.196
プロバイダ	未入力
国	Russian Federation
郵便番号	101990
都道府県	Moskva
市区町村	Moscow
緯度	55.7522
経度	37.6156

調査結果の URL は共有することができます。

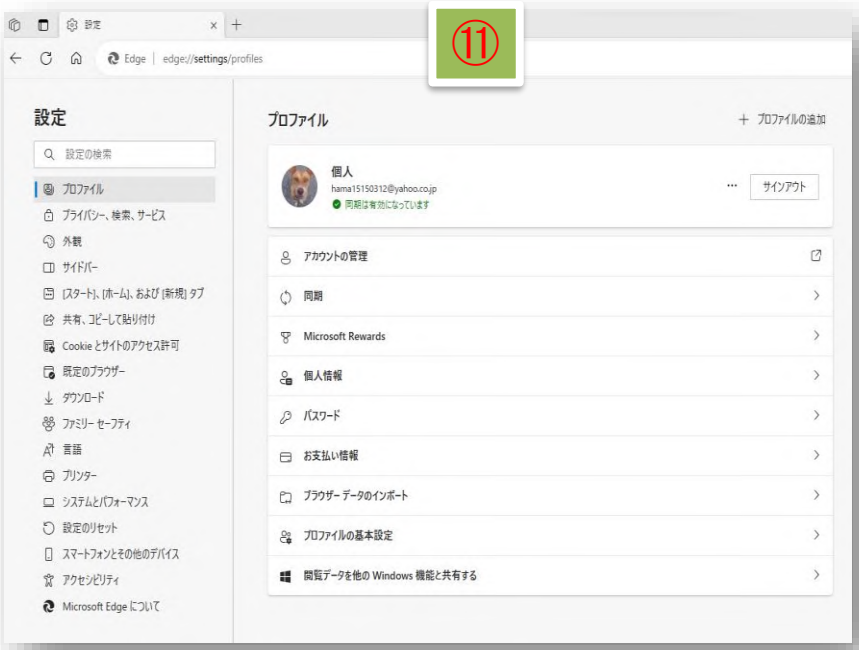
⑧

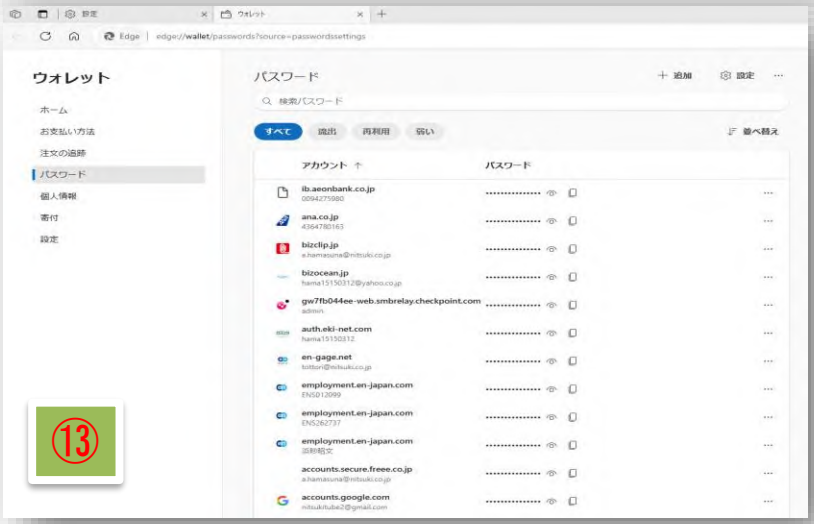
Evidence example





Evidence example





国内でも有名なウィルス対策ソフトメーカーの「ノートン」の幹部であったブライアン・ダイ氏が「ウイルス対策ソフトは死んだ。パターンファイル検知による検知率は45%で大半以上のウィルスは素通りしている」というコメントを紹介したのが2014年。

それから時間が流れ、マルウェアによる侵害被害を受ける企業が増える中で、いよいよウイルス対策ソフトの限界が現実のものになってきました。

抜粋：ウイルス対策ソフトは限界か？用意しておきたい有力な選択肢 | セキュリティ対策のラック (lac.co.jp

ウィルス対策ソフトは国内企業の9割もの企業は導入しているにも関わらず、

不正送金や不正アクセスによる被害は減るどころか増え続けているのが実情です。

更なる追加の対策を・・・

更なる安全対策に必要になるのが、

『ＵＴＭ』などのウィルス対策専用機器

Security Net Keeperのご案内

『ＵＴＭ』

と

『セキュリティ対策ソフト』

の違いは

ＵＴＭとセキュリティ対策ソフトとの違いは？

UTMとセキュリティ対策ソフトの役割は・・・

UTMとセキュリティ対策ソフト、どちらもウイルス感染や攻撃被害から **守る** システムである事に変わりはありませんが、**「守るもの」** が異なります。

■UTMが守るもの

社内ネットワークの「門番」として、

悪意ある何者かによる **社内ネットワークへの侵入・攻撃** から守ります。

■セキュリティ対策ソフトが守るもの

PCや各端末の「防犯」として、

悪意ある何者かによる **PCへの侵入や攻撃** から守ります。

■ＵＴＭとは・・・

「統合脅威管理」と呼ばれ、さまざまな視点から統合的なセキュリティ対策を実施すること、またそれを実現するためのセキュリティシステムのことをＵＴＭと呼びます。

ＳＮＫで出来ることは・・・

ウェブ対策

① Web不正プログラム対策

ゲートウェイセキュリティ本体でのエンジン検索と
クラウドデータを利用した検索を使い分け、
高い不正プログラム検出率を維持しながら
高スループットを実現！！

② URLフィルタリング

約80のカテゴリでURLをフィルタリングします。
ブラックリスト/ホワイトリストの設定も可能！！

③ Webレピュテーション

不正URLへのアクセスを防止します。
トレンドマイクロ社が保有する約16億URL情報でリアルタイムに判断！！

メール対策

④E-mailレピュテーション

スパムメール対策として使用します。
受信メールメッセージのIPアドレスを検証して、
スパムおよびフィッシングの送信元を特定し阻止！！

⑤ 機械学習型検索（添付ファイル）

メール攻撃で侵入する添付ファイルを、ＡＩ技術を利用して特徴を元に判断することで、
従来の検出技術では検出できなかった未知のマルウェアにも迅速に対処することが可能！！

⑥メールセキュリティ対策

E-mailレピュテーションとゲートウェイセキュリティ本体のエンジンを利用し、不正プログラム付メール、スパムメールをブロックします。
また、コンテンツフィルタリングにより、
不適切なメールを検知します。

コンテンツ対策

⑦アプリケーションコントロール

ＰＣで利用する1,000以上のアプリケーションを
サポートし、利用可否を制御できます。
一部アプリケーションでは機能単位の制御も可能！！

⑧コンテンツフィルタ（マイナンバー情報漏えい防止機能）

マイナンバーの情報漏洩に特化した機能。
「マイナンバーによるフィルタ」をONにするとメール本文に記載されたマイナンバーを検知することが可能！！

侵入対策

⑨ファイアウォール

攻撃をブロックし、適切なアプリケーショントラフィックのみを通過させます。
セキュリティ対策の基本！！

⑩侵入防止（IPS）

サーバやネットワークの外部との通信を監視し、
侵入の試みなど不正なアクセスを検知して攻撃を未然に防ぎます。
ファイアウォールで防げなかった脅威にも対応！！

お願い事項

診断内容とその詳細について

診　断

エビデンス

提　案

＊ ルータのログ確認

＊ 不正アクセスの状況確認とその意図の分析

＊ アドウェア・マルウェアの有無

＊ メールアドレスの流出確認

＊ ホームページの改ざん確認

＊ 二重ルータ・通信速度などのネットワーク状況分析

＊ ID・パスワード流出確認

＊ Wi-Fiのセキュリティレベルや設定内容確認

＊ 機微情報の有無

＊ ウイルス対策ソフトの有効性の確認

インターネット環境の安全チェック依頼シート

安全チェックをご要望の際は下記の事項をご記載の上、メールまたはＦＡＸでご返信下さい。

またメールにてご質問も承ります。

お客様名（法人名）	
代表者名	
住所	
電話番号	
希望日時	第一希望：　　月　　日　AM / PM　　第二希望：　　月　　日　AM / PM 第三希望：　　月　　日　AM / PM　　※ご希望に添えな場合もございます。ご了承下さい。

安全チェックのご依頼もしくはご質問のお問い合わせは・・・

ＦＡＸ：0952-36-9501　もしくは　メール：saga@nitsuki.co.jp　まで

佐賀市高木瀬西3丁目1番1号　ＮＴＴ高木瀬ビル1F　日本通信機器株式会社　佐賀営業所

ご清聴
ありがとうございました

日本通信機器株式会社