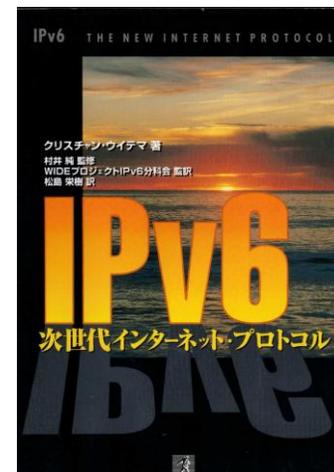


見落とされがちなネットワーク監視 ～ IPv6見えていますか？

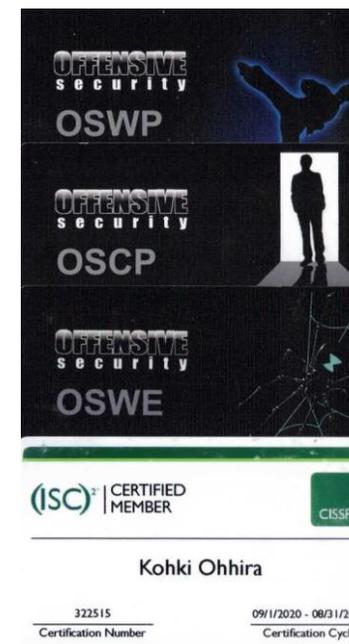
デジタル庁 大平浩貴 / 東京科学大学 北口善明

自己紹介（大平）

- 現在デジ庁に所属
 - 今回の発表は個人によるものであり、所属組織とは無関係です。
- IAjapan IPv6ディプロイメント委員
 - IPv6の存在を初めて知ったのはこちらの本から
- スキル：セキュリティ屋（Red Team）
 - サイバー攻撃技術を専門
 - レッドチーム立ち上げ
 - レッドチームスキルの習得や活用
 - OSWE/ OSCP/ OSWP/ CISSP



初めて読んだ
v6本



お願い

- 悪用すれば犯罪になる
 - 学習はみんなの安全を守るために行う（侵入を目的としない）
 - 確認は自身の閉鎖ネットワークの中で、会社では経営者の許可を得て行う
 - 許可を得ていない他ネットワークに対しては決して行わない

今日、焦点をあてること



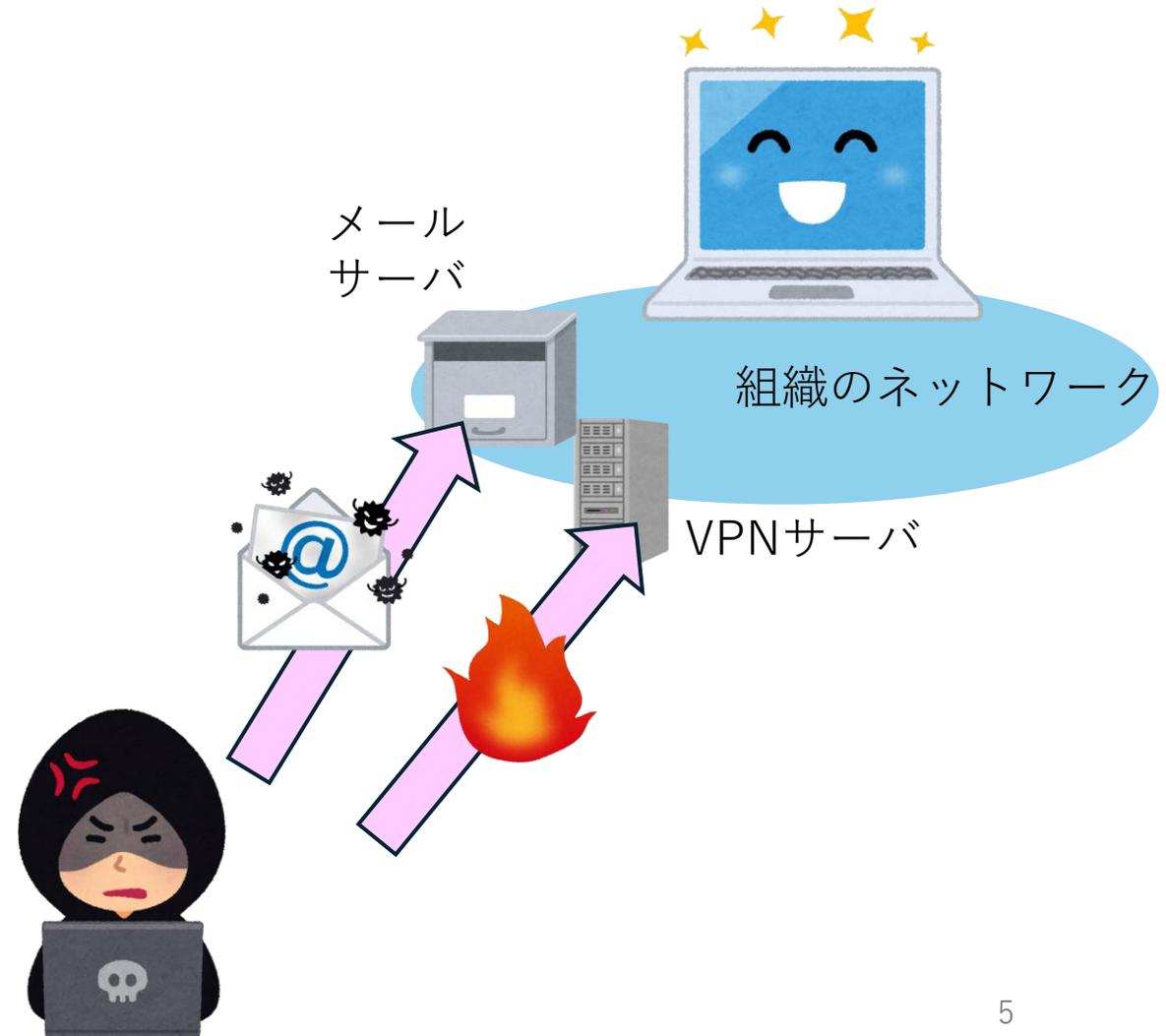
IPv6を監視するために
IPv6を理解しよう



サイバー攻撃を監視するために
サイバー攻撃を理解しよう

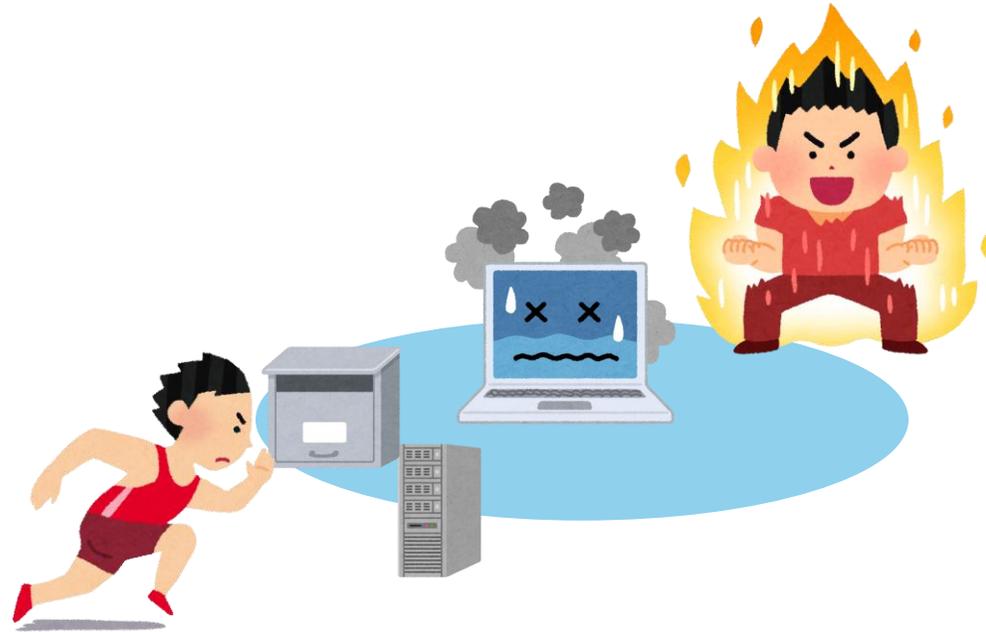
前提

- 企業等の組織ネットワーク
 - 境界防御のモデルで説明してまいります



サイバー攻撃の情報を
自習するテクニック

今日、焦点をあてる侵入



- 今回焦点をあてるサイバー侵入
1. 外部から内部に侵入して
 2. イン트라ネット内で感染拡大

2つの方法を紹介

- IPAによる今年の10大脅威を使って学習する
- MITRE ATT&CKを使って学習する

外部から組織内に侵入する活動を 2025年の10大脅威からピックアップ

順位	組織向け脅威	初選出年	10大脅威での取扱
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

イントラネット内で感染拡大する脅威を 2025年の10大脅威からピックアップ

順位	組織向け脅威	初選出年	10大脅威での取扱
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

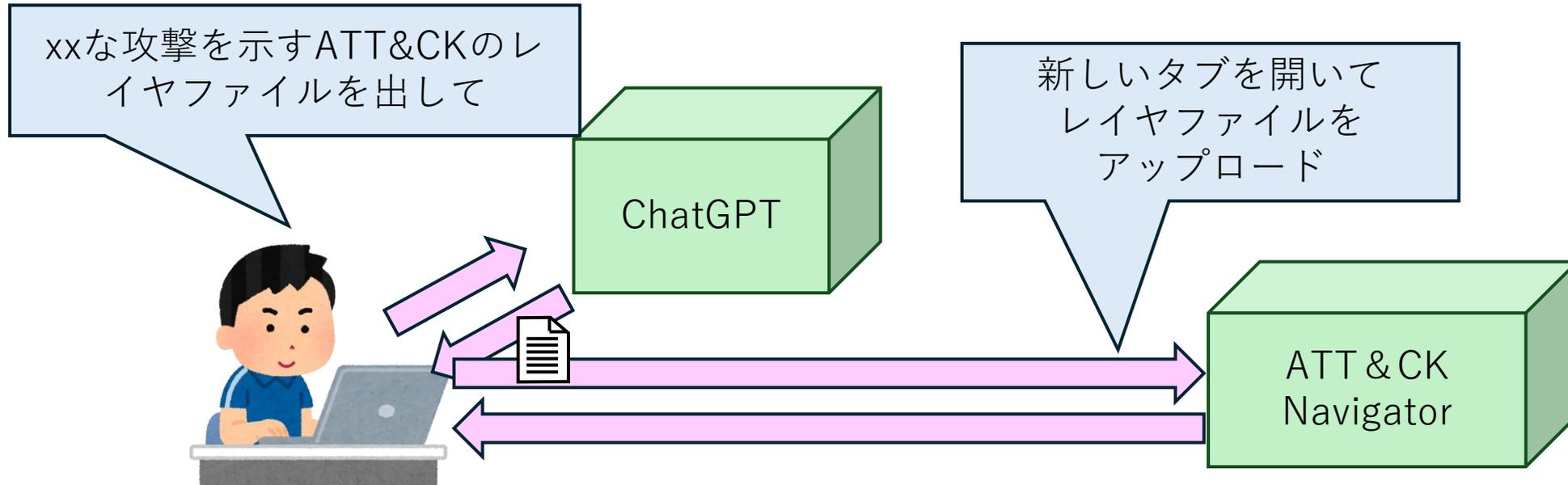
2つの方法を紹介

- IPAによる今年の10大脅威を使って学習する
- MITRE ATT&CKを使って学習する

MITRE ATT&CK ってなあに？

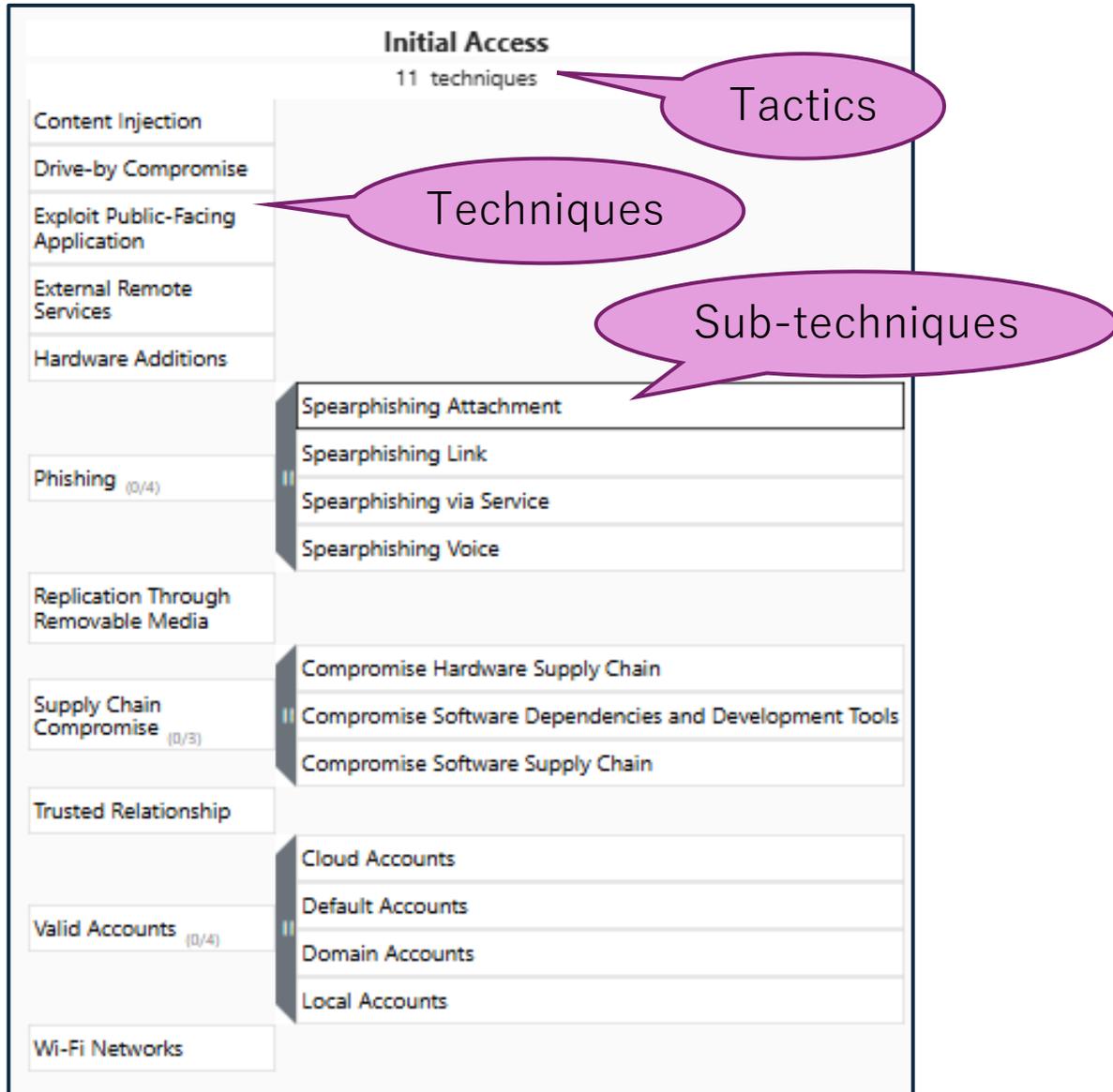
- MITREとは
 - 米国政府から資金提供されている非営利団体
 - 国家・自治体・重要プロジェクト（航空・宇宙・教育等）の安全を扱う
 - 脆弱性を識別するCVEを管理する
- MITRE がサイバー攻撃を体系化 & 解説したのがATT&CK

ATT & CKを用いた学習の流れ



1. LLMなどで「xxな攻撃を示すATT&CKのレイヤファイルを出して」と依頼
2. それをATT & CK Navigatorの「新しいタブ+アップロード」から送信する
3. ATT & CK Navigator の特定の攻撃が着色されて一目でわかる

Attack Navigator と各項目について



- ATT&CK Navigator
 - <https://mitre-attack.github.io/attack-navigator/>
- 階層構造
 - 第1層：Tactics（戦術）
 - 第2層：Techniques（技術）
 - 第3層：Sub-techniques（部分の技術）
- (Sub-) Techniquesを
[右クリック]→[View technique]
 - 攻撃の解説

ATT&CK Navigator にレイヤファイルを投入



- レイヤファイルを投入すると、特定の攻撃を着色できる
- 今回のレイヤファイルは2つ
 - 外部から侵入する攻撃
 - 内部で感染拡大する攻撃
- 新しいタブを生成して
- そのレイヤファイルを、[Upload from local]から流し込む

外部から初期侵入する脅威をピックアップ

- 右図のように初期侵入にかかわるものをスコア付きで記載
 - 濃い緑(Score 90)～橙色 (Score 40)
- もっと制限すればもっと実用的に
 - 例1：VPNルータの脆弱性を用いた初期侵入
 - 例2：メールを用いた初期侵入

TA0001 Initial Access 11 techniques	
T1659 Content Injection	
T1189 Drive-by Compromise	
T1190 Exploit Public- Facing Application	
T1133 External Remote Services	
T1200 Hardware Additions	
	T1566.001 Spearphishing Attachment
	T1566.002 Spearphishing Link
T1566 Phishing (4/4)	T1566.003 Spearphishing via Service
	T1566.004 Spearphishing Voice
T1091 Replication Through Removable Media	
	T1195.003 Compromise Hardware Supply Chain
T1195 Supply Chain Compromise (0/3)	T1195.001 Compromise Software Dependencies and Development Tools
	T1195.002 Compromise Software Supply Chain
T1199 Trusted Relationship	
	T1078.004 Cloud Accounts
	T1078.001 Default Accounts
T1078 Valid Accounts (4/4)	T1078.002 Domain Accounts
	T1078.003 Local Accounts

イントラ内で感染拡大する脅威をピックアップ

- Lateral Movement に関するアクセスは [TA0008 Lateral Movement] に含まれる
- それ以外にも関連するものもある

OS Credential
の奪取

TA0006 Credential Access 17 techniques	TA0007 Discover 34 techniques	TA0008 Lateral Movement 9 techniques
T1555 Credentials from Password Stores (0/6)	T1217 Browser Information Discovery	T1570 Lateral Tool Transfer
T1212 Exploitation for Credential Access	T1580 Cloud Infrastructure Discovery	T1563 Remote Service Session Hijacking (2/2)
T1187 Forced Authentication	T1538 Cloud Service Dashboard	T1563.002 RDP Hijacking
T1606 Forge Web Credentials (0/2)	T1526 Cloud Service Discovery	T1563.001 SSH Hijacking
T1056 Input Capture (0/4)	T1619 Cloud Storage Object Discovery	T1021.007 Cloud Services
T1556 Modify Authentication Process (0/9)	T1613 Container and Resource Discovery	T1021.008 Direct Cloud VM Connections
T1111 Multi-Factor Authentication Interception	T1622 Debugger Evasion	T1021.003 Distributed Component Object Model
T1621 Multi-Factor Authentication Request Generation	T1652 Device Driver Discovery	T1021.001 Remote Desktop Protocol
T1040 Network Sniffing	T1482 Domain Trust Discovery	T1021.002 SMB/Windows Admin Shares
T1003 OS Credential Dumping (0/8)	T1083 File and Directory Discovery	T1021.004 SSH
	T1615 Group Policy Discovery	T1021.005 VNC
	T1680 Local Storage Discovery	T1021.006 Windows Remote Management
	T1654	T1091 Replication Through Removable Media
		T1072 Software Deployment Tools

外部から侵入と 内部で感染拡大の 基本



外部から内部に侵入される基本スタイル

うちにはFirewallがあるから
外部から内部にアクセスできないよ

- 攻撃者が使用する**C2**と**RAT**がFirewallを超えてしまう

名称	接続	役割
C2 (Command & Control)	サーバー (レスポнда)	主にインターネット上にあり、RATに対して指示を送る
RAT (Remote Administration Tools)	クライアント (イニシエータ)	侵入先コンピュータ上で動き、C2と通信して命令を受け、攻撃行動をとる 遠隔操作ウィルス とも呼ばれる

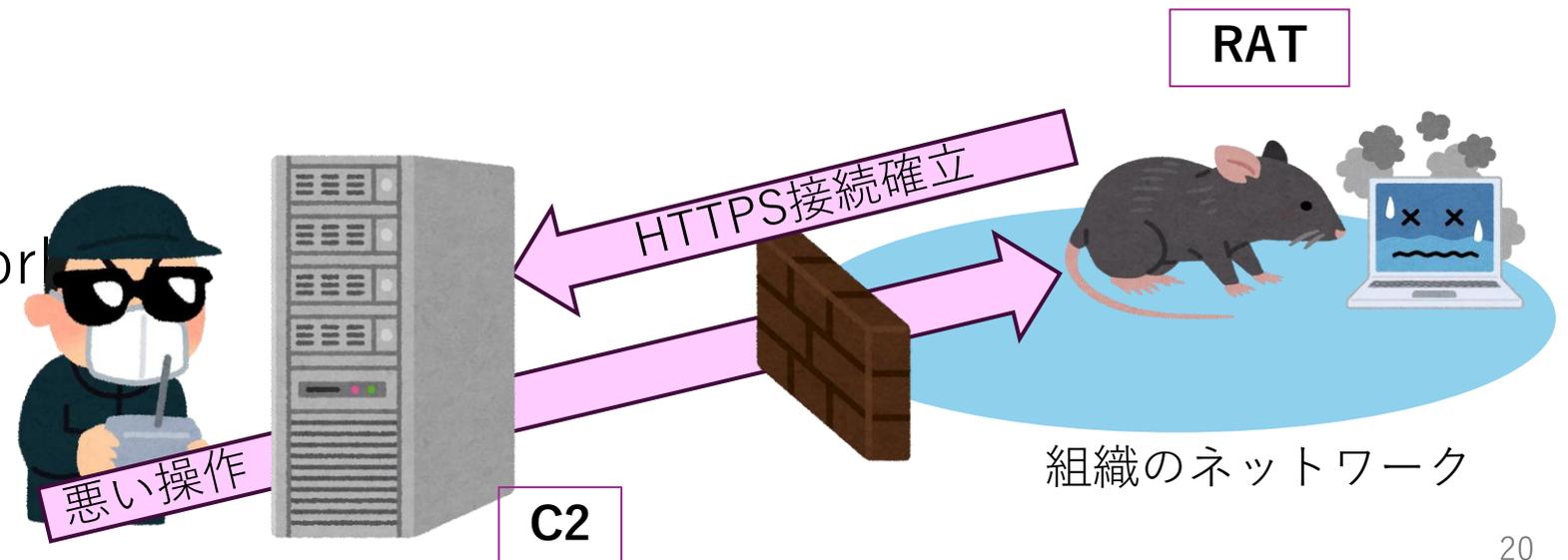
外部から構内網に侵入される流れ

- 侵入と遠隔制御の例

1. RATをメールの添付ファイルとして送り付ける
2. 被害者が添付ファイルを実行してしまう
3. RATからC2にアクセスする (httpsアクセス・DNSアクセスなど)
4. C2は折り返しでRATに対して動作指示を送る。

- RAT/C2の例

- Cobalt Strike
- Metasploit Framework



組織網内部で感染拡大ってどういうこと？

- 組織内には貴重な情報がある
 - サーバアクセスのBookmark
 - 最近使ったファイル
 - リモートへのシンボリックリンク
 - VPNのクレデンシャル
 - ADのクレデンシャル
 - 業務統合パッケージのクレデンシャル
 - 内作Webアプリのクレデンシャル
- 感染範囲を広げる
 - 昇格
 - ラテラルムーブメント
 - ピボットティング
- 攻撃者にとっての利益を得ていく
- 対策としては、EPP、EDR、SIEM、脅威ハンティングなどを用いる

北口先生へハンドオーバー

21分

3、侵入の実例

検証1

LAN内ホストの発見法



[LAN内ホスト発見]IPv6スキヤンの難しさと克服

- IPv4のLAN検索
 - 例：192.168.222.0/24、1～254まで254回試行すればよい。
- IPv6のLAN検索
 - 例：/64のネットワークで、::～::ffff:ffff:ffff:ffffまで、 $\approx 1.8 \times 10^{19}$ 1アドレスを1秒で確認すると、5800億年かかる
- テクニック：RFC7707を読もう
 - 背景知識：アドレスの振られ方：4.1節（4.1.1～4.1.5）
 - 基本検索法：4.2節～4.6節
 - 応用検索法（さらに思考を広げた検索法）：5.1節～5.11節
 - 全部のまとめ：6章

[近隣ホスト発見] pingで見よう

- pingをLANのオールノードマルチキャストに送る

ping ff02::1% I/F名

```
kali@kali: ~  
セッション 操作 編集 表示 ヘルプ  
kali@kali:~$ ping ff02::1%eth0  
PING ff02::1%eth0 (ff02::1%eth0) 56 data bytes  
64 bytes from fe80::693c:ea68:55aa:97fe%eth0: icmp_seq=1 ttl=64 time=0.136 ms  
64 bytes from fe80::a09a:8eff:fe85:e666%eth0: icmp_seq=1 ttl=64 time=0.383 ms  
64 bytes from fe80::f31e:959e:3ea0:cd34%eth0: icmp_seq=1 ttl=64 time=0.665 ms  
64 bytes from fe80::693c:ea68:55aa:97fe%eth0: icmp_seq=2 ttl=64 time=0.090 ms  
64 bytes from fe80::a09a:8eff:fe85:e666%eth0: icmp_seq=2 ttl=64 time=0.484 ms  
64 bytes from fe80::f31e:959e:3ea0:cd34%eth0: icmp_seq=2 ttl=64 time=0.786 ms  
64 bytes from fe80::693c:ea68:55aa:97fe%eth0: icmp_seq=3 ttl=64 time=0.091 ms  
64 bytes from fe80::a09a:8eff:fe85:e666%eth0: icmp_seq=3 ttl=64 time=0.498 ms  
64 bytes from fe80::f31e:959e:3ea0:cd34%eth0: icmp_seq=3 ttl=64 time=0.839 ms  
^C  
— ff02::1%eth0 ping statistics —  
3 packets transmitted, 3 received, +6 duplicates, 0% packet loss, time 2031ms  
rtt min/avg/max/mdev = 0.090/0.441/0.839/0.273 ms  
kali@kali:~$ █
```

さらに検索

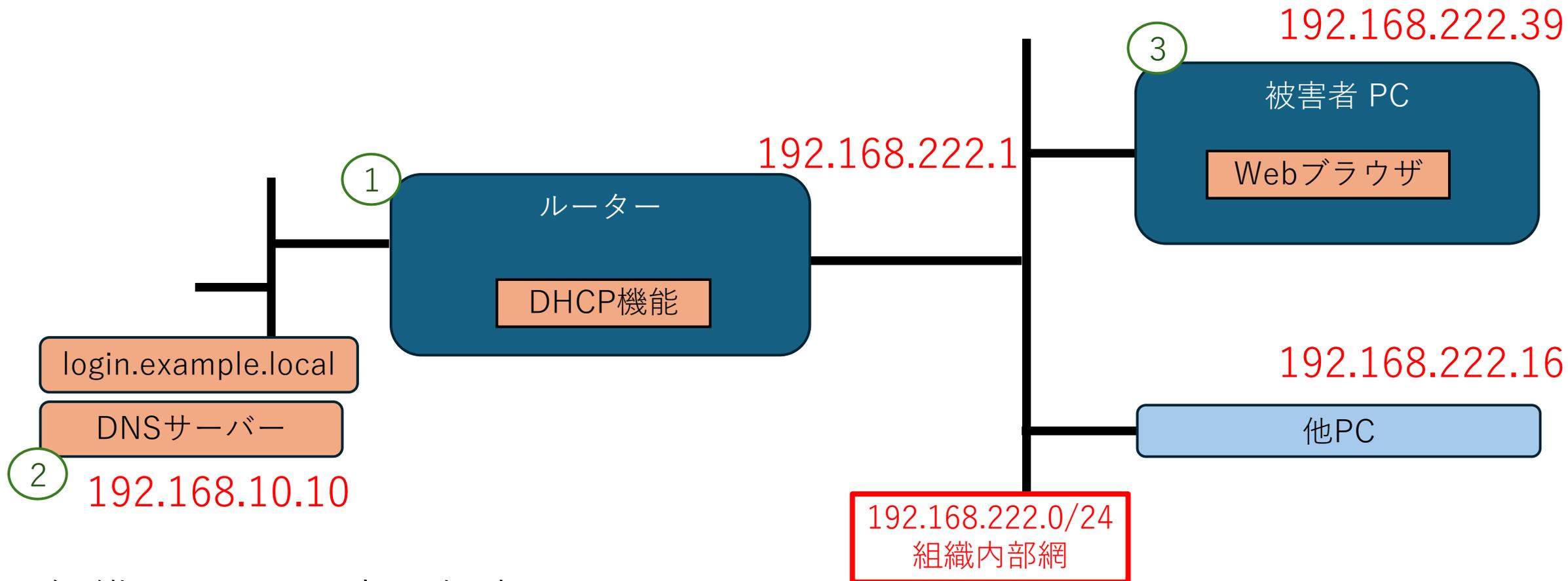
- ホストを発見したら、すぐに ip n (neighbor の略であり、arp やndpのテーブルを参照) する
- 新しいprefixでRAを配布する
 - IPv6のアドレス設定されるが、その際に DADが走行してIPv6アドレスが判明する
- その他の発見法
 - ペリフェラルなどのサービス発見プロトコル
 - mDNS、ssdp、WSD、SLP を使うなど
 - nmap
 - IPv4の単純なポートスキャンだけでなく、アプリバージョンやscriptを用いた高度検索もできる

検証 2

社内Webサービスの乗っ取り (偽サーバの設置)

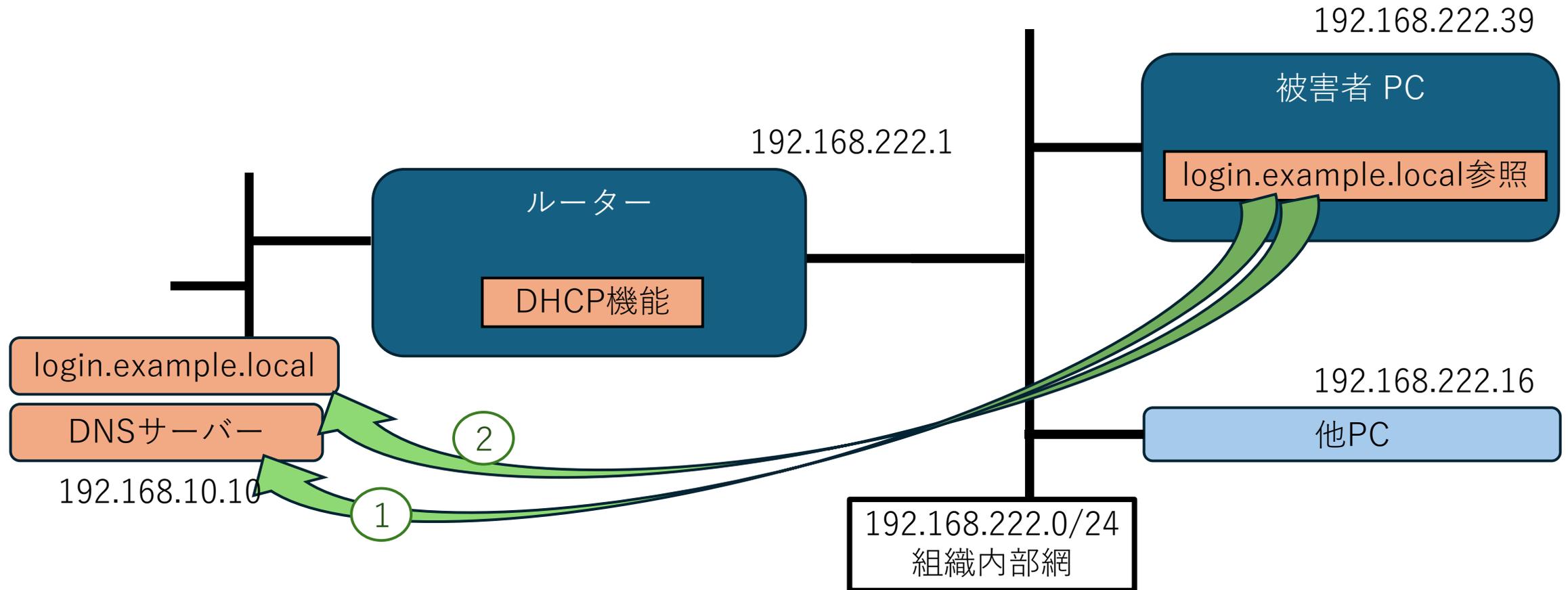


[乗っ取りデモ] IPv4のみを扱うネットワーク



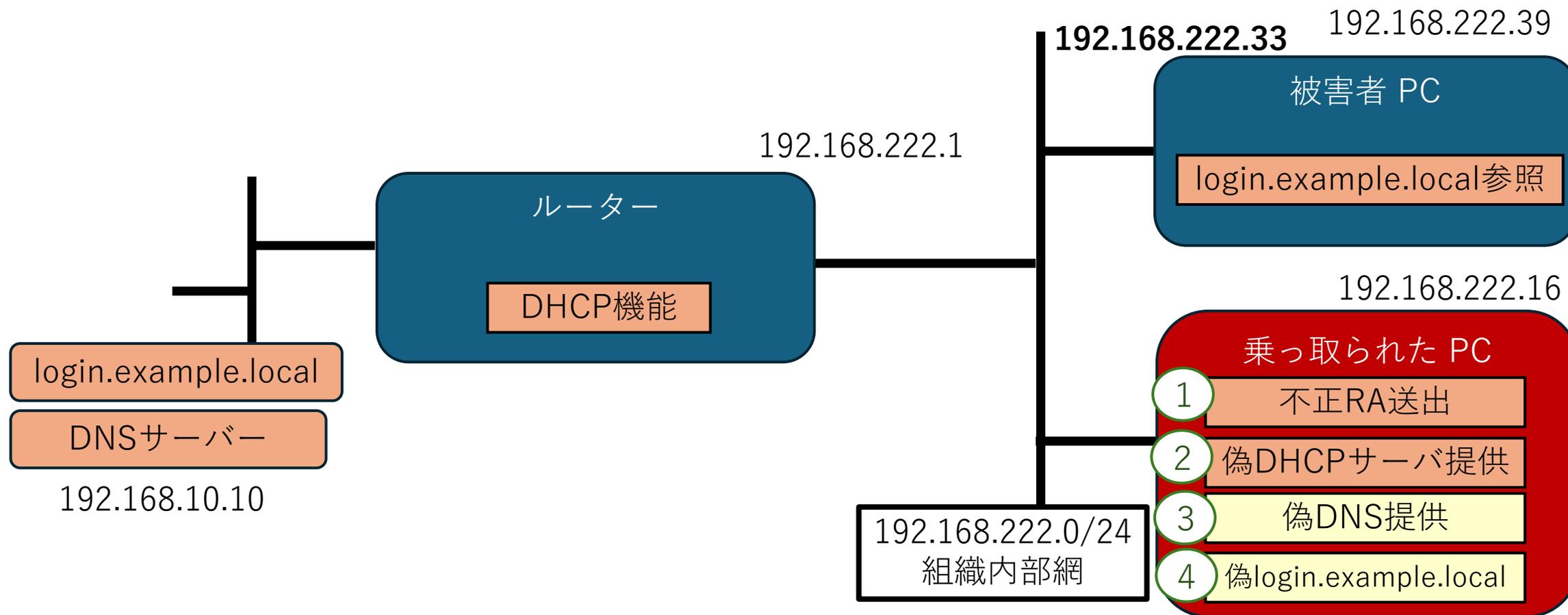
- 組織のintranet内を想定
 - ルーター
 - 社内サーバ (Web・DNS)
 - 被害者となるユーザーのPC

[乗っ取りデモ] IPv4のみを扱うネットワーク



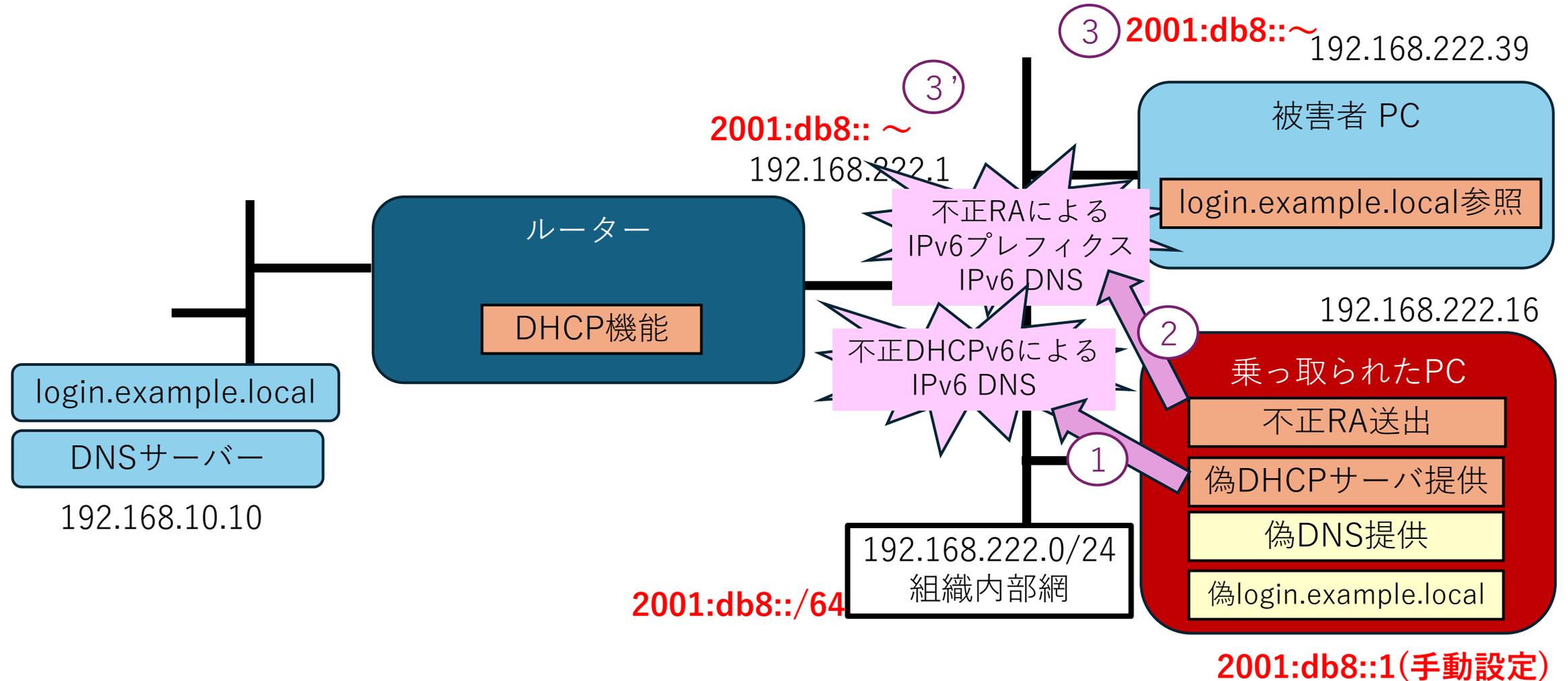
- ユーザーはlogin.example.localを参照

[乗っ取りデモ] IPv4のみを扱うネットワーク



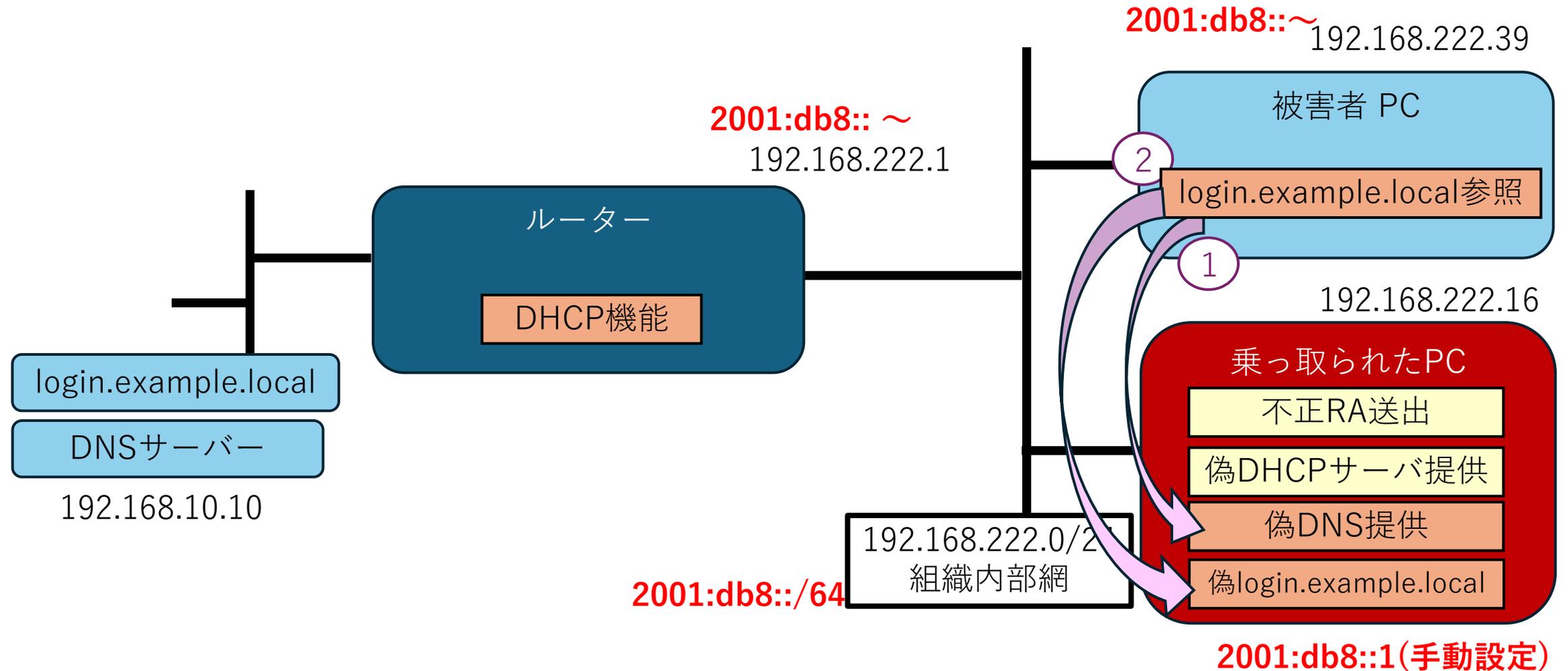
- 近傍のPCが乗っ取られて、1~4の不正サービスを開始

[乗っ取りデモ] 攻撃者がその情報を流し込む様子



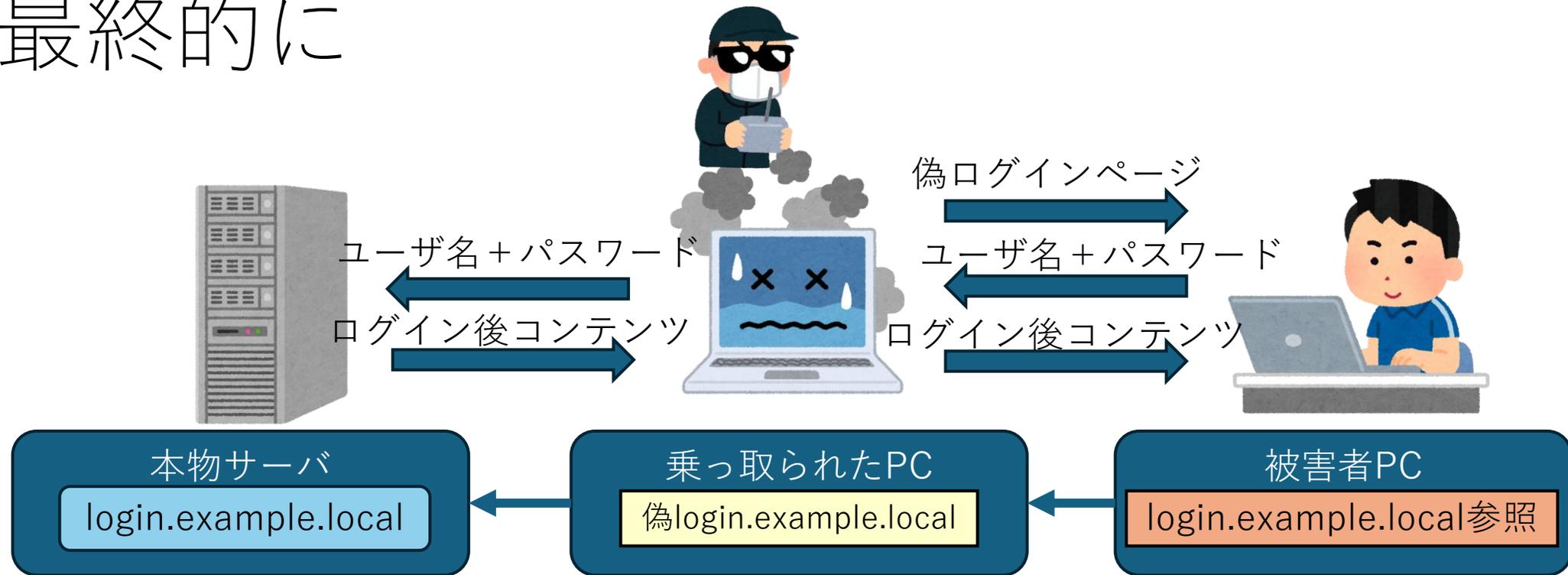
- 乗っ取られたPCによってLAN内に不正なIPv6設定が行われる

[乗っ取りデモ] うそのサーバーに誘導された様子



- 社内Webサーバのlogin.example.local (192.168.10.10) を見ようとしても、偽物 (2001:db8::1) を見てしまう

最終的に



- MITMいけるぜ
 - クレデンシャル窃取
- The Internet上のはTLS (https) を使っているが、内部Webサーバーでは平文 (http) のケースが案外多い

[乗っ取りデモ] DNS設定の変化

イーサネット アダプター イーサネット 3:

```
接続固有の DNS サフィックス . . . . .: example.local
説明 . . . . .: vmxnet3 イーサネット アダプ
物理アドレス . . . . .: 00-0C-29-B5-F2-A5
DHCP 有効 . . . . .: はい
自動構成有効 . . . . .: はい
リンクローカル IPv6 アドレス . . . . .: fe80::d24c:6423:272a:c911%1
IPv4 アドレス . . . . .: 192.168.222.39(優先)
サブネット マスク . . . . .: 255.255.255.0
リース取得 . . . . .: 2025年11月7日 18:59:41
リースの有効期限 . . . . .: 2025年11月8日 16:15:19
デフォルト ゲートウェイ . . . . .: 192.168.222.1
DHCP サーバー . . . . .: 192.168.222.1
DHCPv6 IAID . . . . .: 419433513
DHCPv6 クライアント DUID . . . . .: 00-01-00-01-30-72-B7-C3-20-7B-00-00-00-00
DNS サーバー . . . . .: 192.168.10.10
NetBIOS over TCP/IP . . . . .: 有効
```

PS C:\Users\tester> |

```
自動構成有効 . . . . .: はい
IPv6 アドレス . . . . .: 2001:db8::3(優先)
リース取得 . . . . .: 2025年11月8日 11:46:42
リースの有効期限 . . . . .: 2025年11月8日 11:47:19
IPv6 アドレス . . . . .: 2001:db8::b16c:cad0:223f:a7ce
リンクローカル IPv6 アドレス . . . . .: fe80::d24c:6423:272a:c911%12
IPv4 アドレス . . . . .: 192.168.222.39(優先)
サブネット マスク . . . . .: 255.255.255.0
リース取得 . . . . .: 2025年11月7日 18:59:41
リースの有効期限 . . . . .: 2025年11月8日 11:54:30
デフォルト ゲートウェイ . . . . .: fe80::d6cc:3ec:1afe:8aaa%12
192.168.222.1
DHCP サーバー . . . . .: 192.168.222.1
DHCPv6 IAID . . . . .: 419433513
DHCPv6 クライアント DUID . . . . .: 00-01-00-01-30-72-B7-C3-20-7B-00-00-00-00
DNS サーバー . . . . .: 2001:db8::1
192.168.10.10
2001:db8::1
NetBIOS over TCP/IP . . . . .: 有効
```

接続固有の DNS サフィックス検索の一覧:

www.example.com
example.com

```
PS C:\Users\tester> nslookup login.example.local
サーバー: UnKnown
Address: 2001:db8::1

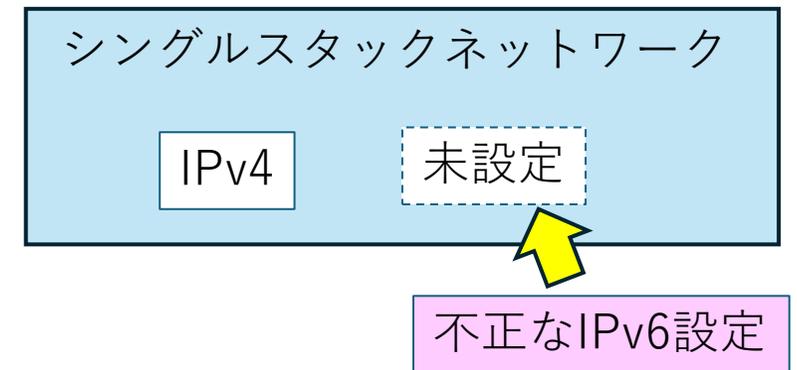
名前: login.example.local
Address: 2001:db8::1
```

PS C:\Users\tester> |

4、对策

今回の問題を許した原因は？

- 原因
 - ネットワーク設計
 - IPv4のことしか考えていなかった
 - 各端末
 - IPv6に対応していた
 - 悪者がIPv6を配布した
 - みんな騙された
- では対策は？



問題と対策案

問題	対策案
IPv6が勝手に配布されてしまった	不正にIPv6を配布できないようにする
使用中のIPv4よりも未使用のIPv6を優先してしまった	IPv6を無効にする IPv4の優先順位を上げる

使っていないIPv6機能を無効にする

- メリット
 - 今回のIPv6起因問題は確実に解決
- デメリット
 - Microsoft社はIPv6停止を非推奨
 - <https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/configure-ipv6-in-windows#summary>
 - 過去、Windows 1809 で不具合が出た例も
 - MS社が否定している行為をエンタープライズで許容できる？
 - モバイル端末や他OSにもIPv6を使わないことを強制できる？



IPv4の優先度を上げる



- IPv4を優先する
 - netsh interface ipv6 show **prefixpolicies** で見られる (Windows)
- メリット
 - 不正なIPv6よりも正しいIPv4を優先する
 - 将来IPv6を使うようになって通信できないことはない
- デメリット
 - 通常のデュアルスタックの挙動と異なる
 - 問題を生じうる
 - モバイル端末や他OSでもIPv6の優先度を下げる管理ができる？

問題と対策案

問題	対策案
IPv6が勝手に配布されてしまった	不正なIPv6配布をできないようにする
使用中のIPv4よりも未使用のIPv6を優先してしまった	IPv6を無効にする IPv4の優先順位を上げる

歴史的な、不正RAや不正DHCPv6の抑制

- PKIベースの証明書認証を用いた根治療法
- SEND
 - SEcure Neighbor Discovery RFC3971
- seDHCPv6
 - Secure DHCPv6 (2017年2月Updateのid21が最終)
 - <https://datatracker.ietf.org/doc/draft-ietf-dhc-sedhcpv6/>
- 一般化はしていない
 - LANでの証明書取り扱いが手間がかかって難しい

現在ある不正なIPv6配布対策

• RA-Guard、DHCPv6-Shield

- L2スイッチの機能
- 前もって下記を設定
 - RAを流すルータが**接続された**ポート
 - RAを流すルータが**いないはずの**ポート
 - DHCPv6サーバが**接続された**ポート
 - DHCPv6サーバが**いないはずの**ポート

このポートの先には
ルーターがいるよ

他のポートの先には
ルーターがないよ



- **いないはずのポートからDHCPv6応答やRAが来たらブロック！**

RA-Guard は rfc6105, 7113, 6104にて記述
DHCPv6-Guardは rfc7610にて記述

NDPの観測

- NDPプロトコルの監視
 - Palo Alto Networks社の商品例
 - [Enable NDP Monitoring](#)
 - <https://docs.paloaltonetworks.com/ngfw/networking/configure-interfaces/layer-3-interfaces/enable-ndp-monitoring>
 - RA-Guard のロギング機能を用いる
 - tcpdump でRS/RAを取得する（下記）

```
sudo tcpdump -i eth0 'icmp6 and (icmp6[0] == 135 or icmp6[0] == 136)' -n |  
logger -t "RA_CAPTURE" -p local0.info
```

Chat GPTより

検知、脅威ハンティングとして

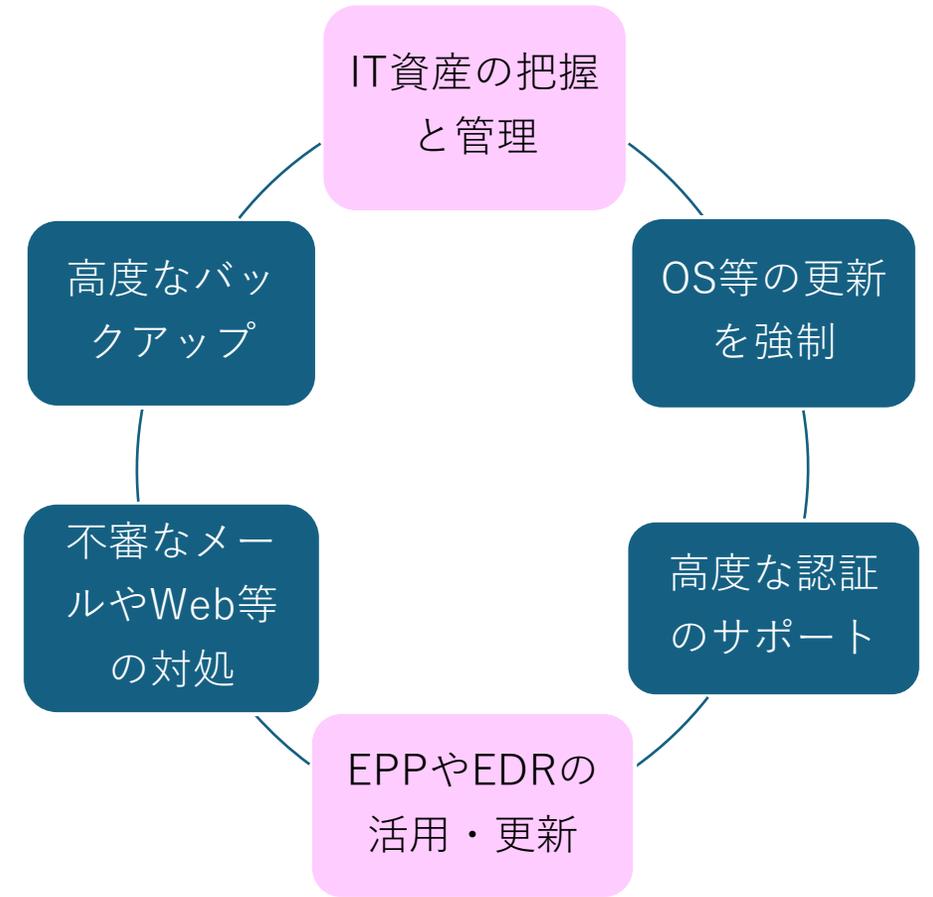
- 侵入検知の情報源
- アノマリーな様相の検知
 - 聞いたことのないプレフィックス
 - 聞いたことのないルーター
 - 聞いたことのないMACアドレスによるRouter Advertisement
 - 適切な量を逸脱するICMP Echoなど、各種パケット
- 従来 of 主な観測値（例：認証失敗の多発など）に組み合わせると有用

観測の一例で、到達性がアヤシイ時

- DoS攻撃にも留意しましょう
 - 戦争・紛争開始の合図かも
 - DoSが国内で同時多発した際の対応シナリオを用意するなど
- どうやって見る？
 - <https://downdetector.jp/>
 - <https://health.aws.amazon.com/>
 - <https://azure.status.microsoft.com/ja-jp/status>
 - <https://status.cloud.google.com/>

サイバーハイジーンと連携すること

- LAN内監視をサイバーハイジーンの体制に組み込む
 - 資産の発見・管理
 - エンドの防御とRS/RA、NDP、リダイレクトの監視など



まとめ

- 正常な通信が何かを知ろう
- 攻撃者が何をするか知ろう
- 目的
 - 監視によって攻撃を早期発見する
 - どうやって侵入されたかが後からわかる
- 自分の組織のために
 - 防御と攻撃の両方を知った方々は、教導隊（アグレッサー）となるように

ありがとうございました