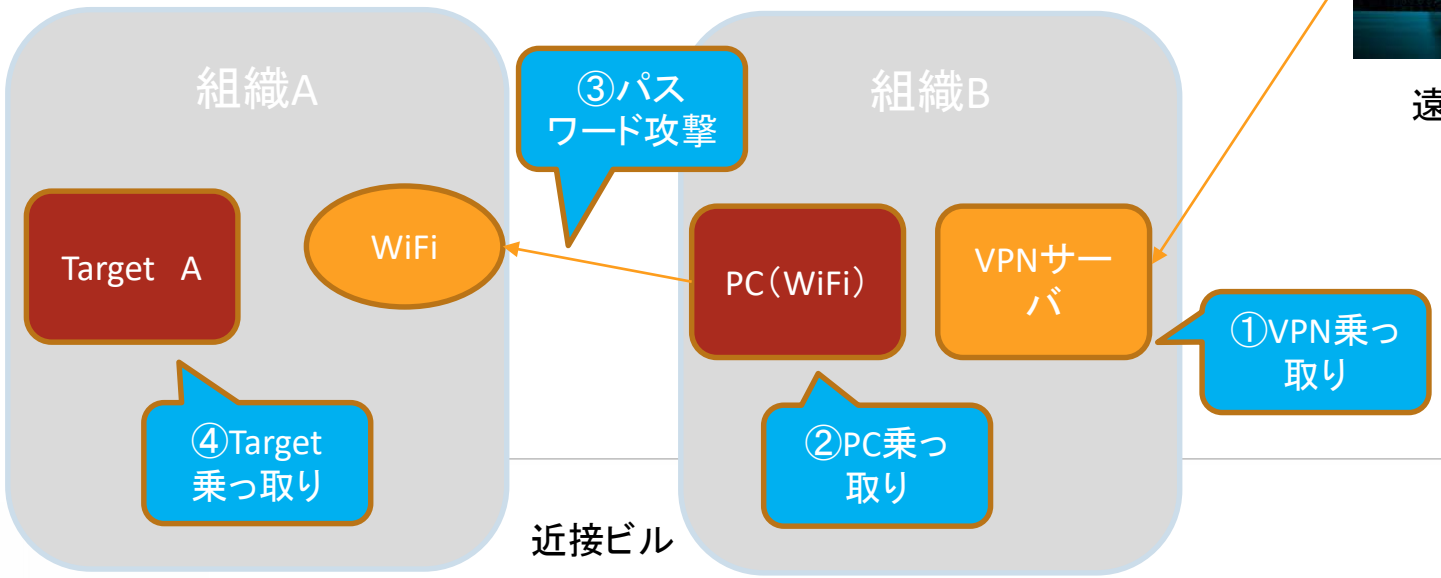
最近接攻撃について

- 最近接攻撃とは
  - Wi-Fi経由で社内システムに不正侵入するサイバー攻撃が実際に確認された。「Nearest Neighbor Attack（最近接攻撃）」と名付けられた
  - 2024/11にVolexity（US　セキュリティ会社）が公表
  - The Nearest Neighbor Attack: How A Russian APT Weaponized Nearby Wi-Fi Networks for Covert Access | Volexity
- 仕組み

遠隔地



最近接攻撃について

- 最近接攻撃とは
  - Wi-Fi経由で社内システムに不正侵入するサイバー攻撃が実際に確認された。「Nearest Neighbor Attack（最近接攻撃）」と名付けられた
  - 2024/11にVolexity（US セキュリティ会社）が公表
  - https://www.volexity.com/blog/2024/11/22/the-nearest-neighbor-attack-how-a-russian-apt-weaponized-nearby-wi-fi-networks-for-covert-access/
- 原因
  - ① VPNサーバ：MFAなしの設定で、パスワード攻撃で侵入可能
  - ② PC（wifi)：同上でMFAなしで、パスワード攻撃で侵入可能
  - ③ WiFiアクセス:WPA2-PSK（パスワードのみ）設定のため、パスワード攻撃で侵入可能
  - ④ Target A：PCに侵入し、WiFiで社内ネットワークで侵入成功
- 対策
  - VPNサーバ：MFA認証、証明書認証などに設定
  - WiFi:WPA2-PSK(personal)からWPA2-IEEE802.1x認証（enterprise)に変更
    - なお、WPA2-enterpriseを行うには、各PCに証明書をインストールし、Radiusサーバ+ADにより認証、手間とコストがかかります。

2．無線ＬＡＮの技術
セキュリティ（WEP/WPA/WPA2/WPA3）

Spectrum Technology

セキュリティ規格	WEP	WPA		WPA2		WPA3	
規格策定の団体	IEEE802.11	Wi-Fiアライアンス		IEEE802.11i		Wi-Fiアライアンス	
規格策定の時期	1997年	2002年10月		2004年6月		2018年6月	
暗号化方式	WEP	TKIP		CCMP		GCMP-256	
暗号化アルゴリズム	RC4	RC4		AES		AES/CNSA	
暗号鍵の長さ	40 or 104bit	104bit		128bit		128/192bit	
認証鍵の長さ	-	64bit		64bit			
IVの長さ	24bit	48bit		48bit			
整合性の検証	CRC32	MIC		CCM			
アンチ・リプレイ攻撃	なし	あり		あり			
認証方式		PSK	IEEE802.1x認証	PSK	IEEE802.1x認証	SAE	EAP
セキュリティ強度	×WEPは解読可能	○	◎	○:64文字	◎	○：128文字	◎
費用	ー	◎	△	◎	△：認証装置が必須	◎	△：認証装置が必須
運用				◎APの管理のみ	△端末、ID管理が必須	◎	△端末、ID管理が必須

問題外：危険

梅：価格と性能面で最低限

松1：TLS
松2：TTLS
竹：LEAP