



**NTT**

Security Holdings

# イスラエルとハマスの軍事衝突における ハッカーグループの活動と日本への波及

NTTセキュリティ・ジャパン

OSINTモニタリングチーム

2023年10月27日

最終更新日：2023年10月30日

# イスラエルとハマスの軍事衝突における ハッカーグループの活動

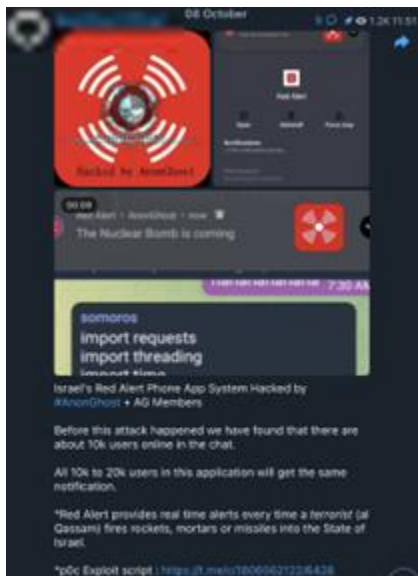
# ハマスの急襲とサイバー戦

- 10月7日、パレスチナのガザ地区を実効支配するハマスは突如、イスラエルに対して大規模な攻勢を開始した。数千発のミサイルと共に陸海空からの電撃的な奇襲を行い、不意を突かれたイスラエルは境界を突破された。この攻勢により自領域内で大きな損害を被ったイスラエルがパレスチナに対し空爆を行う等、軍事衝突が続いている。
- ハマスの攻勢開始から間もなく、世界中のイスラエル、パレスチナそれぞれを支持するハッカーグループが双方を攻撃するサイバー戦がはじまった。

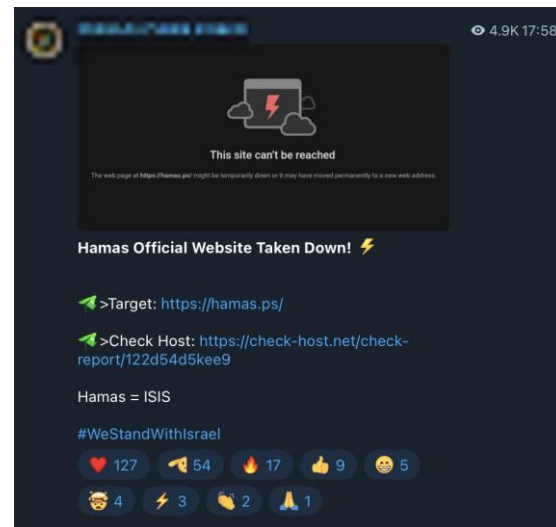


イスラエルの空爆を受けるガザ地区のマンション

- ハッカーグループとして、双方合わせて100以上のグループが参加しており、DDoSは元よりデータベースの窃取・漏洩、改ざん、システム破壊等、多岐に渡る攻撃を繰り返している。
- パレスチナを支持するグループはイスラム教国を中心に多数の支持を集めている。
- イスラエルを支持するグループはイスラエル、インドなど一部の国に限られている。

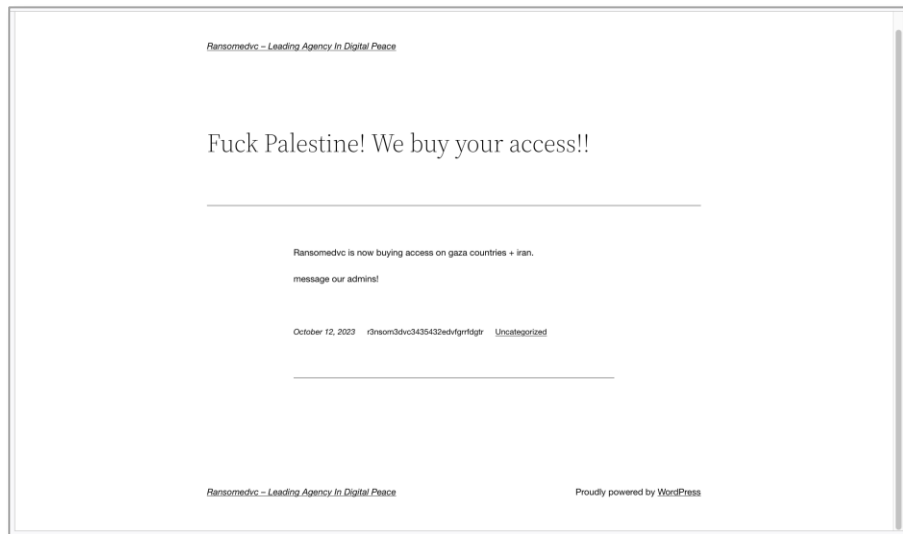


イスラエルのロケットアラートシステムをハッキングしたと主張する親パレスチナのハッカーグループの投稿



10月8日にハマスの公式サイトをダウンさせたと主張するインド系親イスラエルのハッカーグループの投稿

- 一部のランサムウェアグループの参加も見られる。ランサムウェアグループ“Ransomed.vc”はパレスチナを非難すると共に ガザとイランへのアクセス情報を買取ると、暴露サイトにて宣言している。
- 同グループはSNSで、130万件を超える看護記録と160万件を超える医療システムデータと主張するファイルを投稿した。



暴露サイトでアクセス情報を買取ると宣言



SNSにてパレスチナの看護記録と主張するデータをアップロード

# 日本への波及

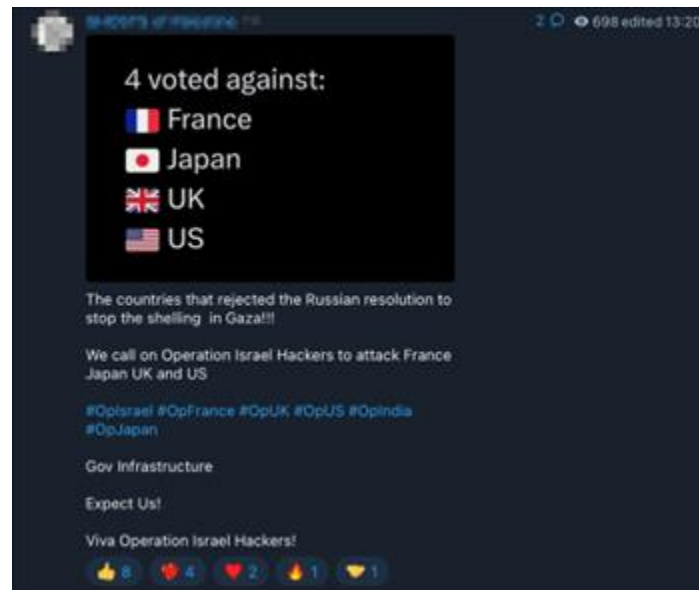
# 国連安保理での停戦案の否決と反対国への反発

- 国連の安全保障理事会（国連安保理）では、ロシアが提出した停戦案に対して、ハマスを非難する文言がないとしてアメリカ、イギリス、フランスと共に日本が反対し、16日に否決された。
- これに対して、18日、親パレスチナのハッカーグループはSNSにて、反対した4か国への攻撃を呼びかけた。



国連安保理でのロシア案否決のニュース

<https://www3.nhk.or.jp/news/html/20231017/k10014227411000.html>



親パレスチナのハッカーグループによる反対した4か国に対する攻撃の呼びかけ

- 続いて、20日に親パレスチナのハッカーグループはターゲットリストとして、DDoS攻撃の対象とする日本の政府関連のWebサイト一覧（ドメインやIP等を含む）を公開した。

```
www.mofa.go.jp IP address 104.73.46.52 Akamai
ns1.mofa.go.jp. <=> 111.108.45.58 [JP] MOFA01
Réseau = 111.108.45.32 - 111.108.45.63
ns2.mofa.go.jp. <=> 106.184.125.90 [JP] MOFA02
Réseau = 106.184.125.64 - 106.184.125.95
ns3.mofa.go.jp. => 95.131.158.22

www.kantei.go.jp 202.214.216.10
ns8.kantei.go.jp. => 202.214.216.7 202.214.194.138
ns7.kantei.go.jp. => 202.214.194.135
202.214.216.10
KANTEI-29
Réseau = 202.214.194.128 - 202.214.194.255
KANTEI-29
Réseau = 202.214.216.0 - 202.214.216.127
2001:240:1e00:1021::10
2001:240:1e00:f21::138

www.sangiin.go.jp IP address 210.128.112.21 210.128.112.21
gnwedns31v2.sangiin.go.jp. => 113.43.242.109
gnwedns31v3.sangiin.go.jp. => 202.221.224.29
dns-a.lij.ad.jp. => 210.138.20.82
HOC-NW
Réseau = 210.128.112.0 - 210.128.112.255
TK0115020122
Réseau = 113.43.242.96 - 113.43.242.111
H31-GLAN Réseau = 202.221.224.16 - 202.221.224.31

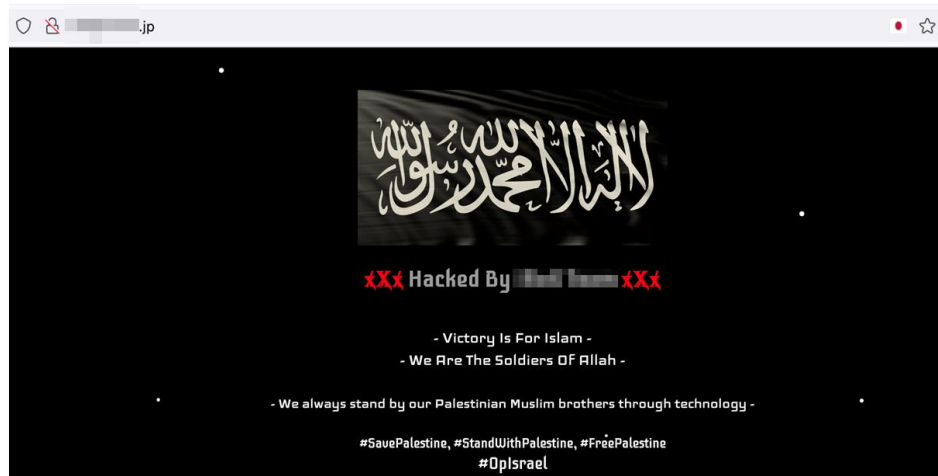
www.shugiin.go.jp IP address 210.136.96.6 210.136.96.6
ns2.sphere.ad.jp. <=> 202.239.113.26 SHUGIIN-NET
Réseau = 210.136.96.0 - 210.136.97.255
ns.shugiin.go.jp. => 210.136.96.35
```

ターゲットリストの投稿（一部）

ターゲットリスト記載の政府機関等
日本銀行
外務省
首相官邸
参議院
衆議院
総務省
財務省
政府機関がホスティングされているネットワークの事業者（IIJ）



- 10月25日、別の親パレスチナのグループにより、日本の事業者のサイトが改ざんされた。
- 改ざんされたページでは、アッラーの戦士としてパレスチナに協力する旨のアピール文が書かれている。
- 同グループはSNSで、日本のサイトをハッキングした旨の犯行声明を発表している。



改ざんされた日本の事業者のサイト



SNSに投稿された犯行声明

# 改ざんを行ったハッカーグループについて

- 改ざんを行ったグループは9月22日から活動を開始した新興のハッカーグループで、当初はインドをターゲットとし、情報窃取及び暴露を示唆する投稿を繰り返していた。
- パレスチナでの衝突後の10月14日にイスラエルとイスラエルを支援する国々に対して、サイバー戦を宣言し、攻撃を繰り返している。
- 投稿は主に英語で、稀にアラビア語を利用することがある。なお、グループの創設者はバングラデシュ出身とみられている。



窃取したと主張する  
インドの学位証明書の画像



イスラエルと  
イスラエルを支援する国々に対し  
サイバー戦を宣言

2023年10月27日 第1版発行

2023年10月30日 第2版発行（P8のターゲットリスト公開日を、18日から20日に修正）



**NTT**

Security Holdings