SANS Community Night (2020/06/09)

最近のサイバー攻撃動向

根岸 征史 (@MasafumiNegishi)

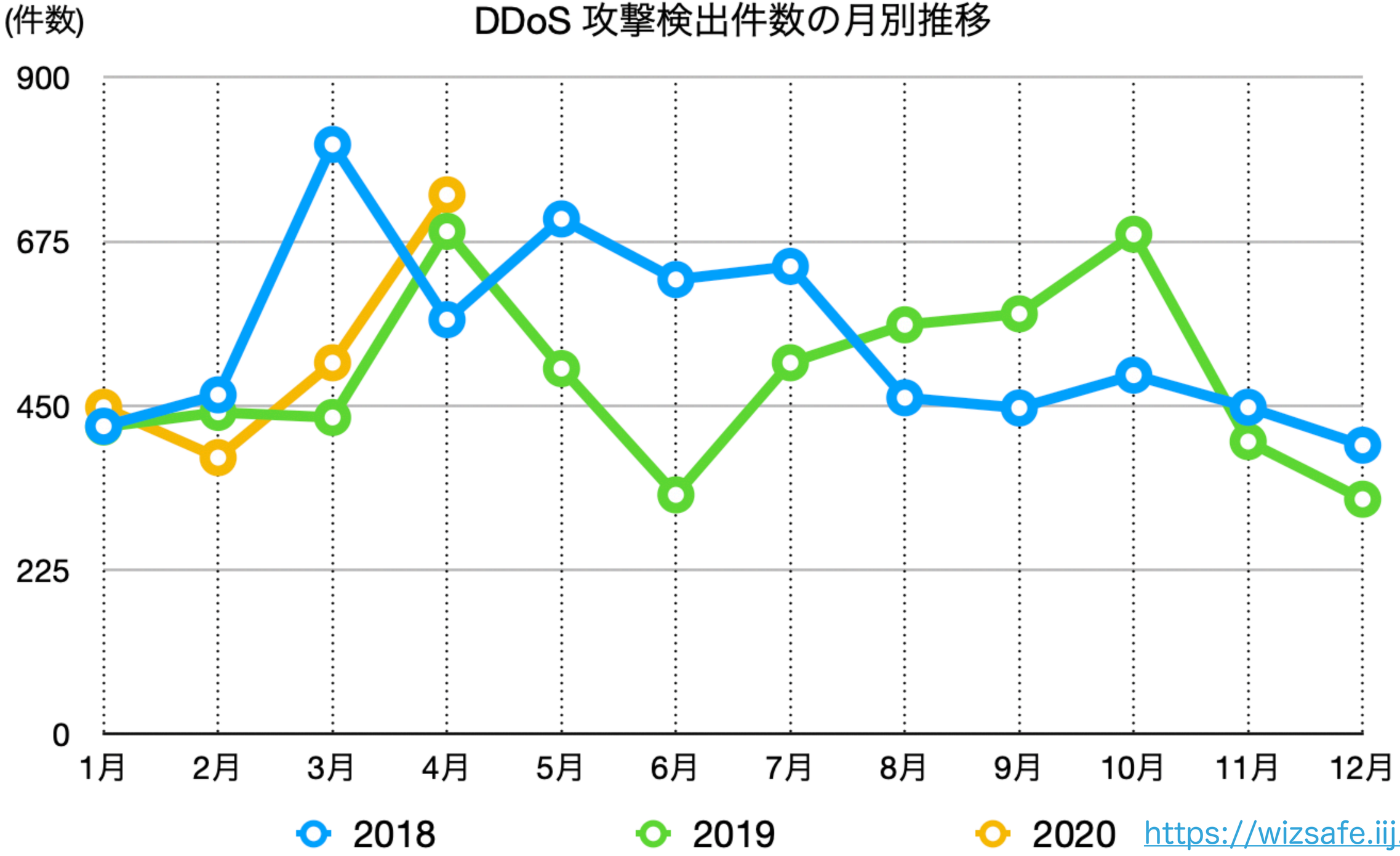
IIJグループの CSIRT 所属 (IIJ-SECT, 2001年結成)

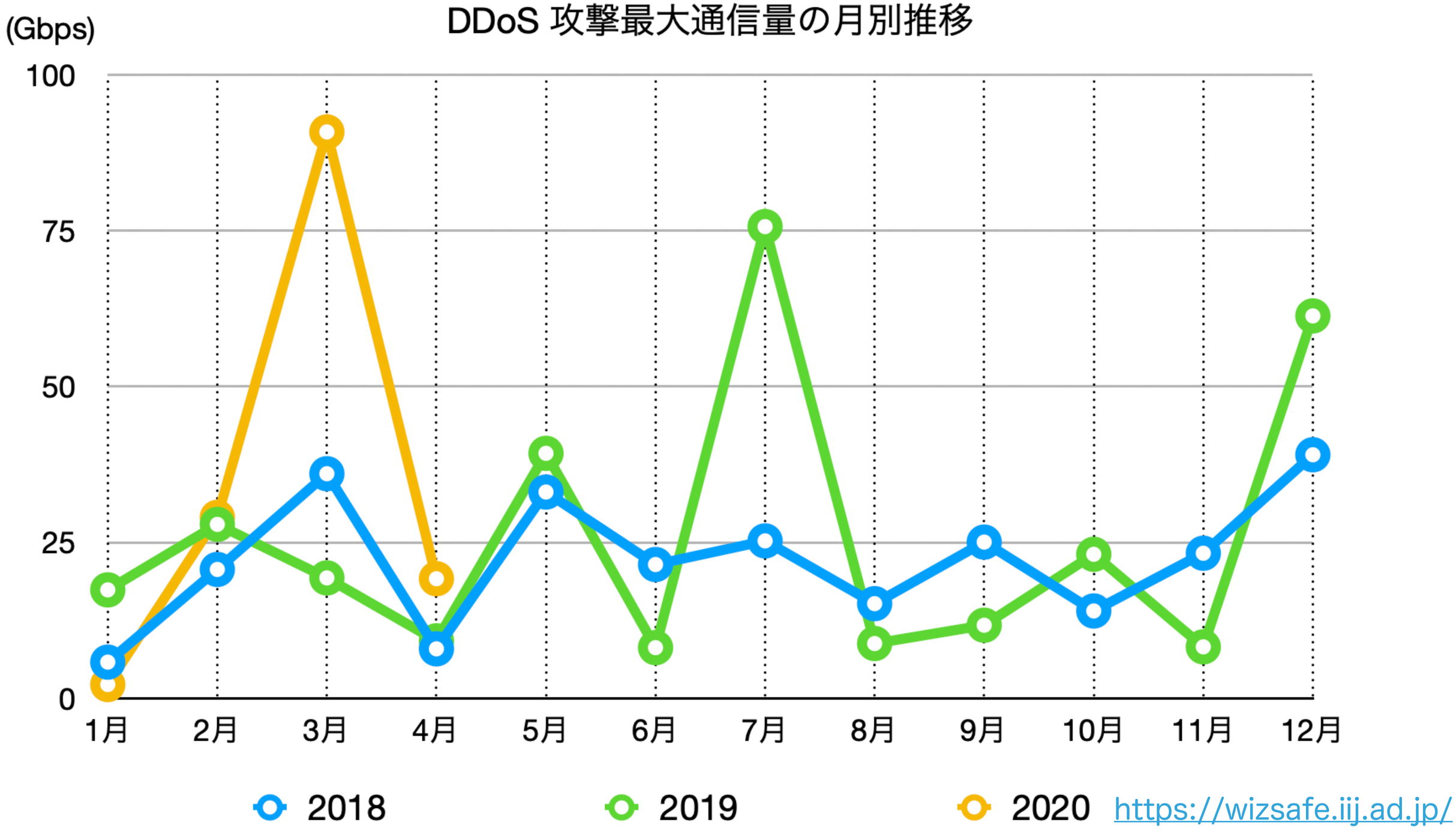
https://sect.iij.ad.jp/

SANS JAPAN 公式インストラクター (2007年〜)
OWASP Japan アドバイザリーボード (2012年〜)
WASForum Hardening Project 実行委員 (2012年〜)
CODE BLUE レビューボード (2015年〜)
ポッドキャスト「セキュリティのアレ」 (2017年〜)

本日のトピック

- DDoS 攻撃
  標的型ランサムウェア


DDoS 攻撃検出件数の月別推移
(件数)
900
675
450
225
0
1月
2月
3月
4月
5月
6月
7月
8月
9月
10月
11月
12月
2018
2019
2020
https://wizsafe.iij.ad.jp/


DDoS 攻撃最大通信量の月別推移
(Gbps)
100
75
50
25
0
1月
2月
3月
4月
5月
6月
7月
8月
9月
10月
11月
12月
2018
2019
2020
https://wizsafe.iij.ad.jp/

DDoS 攻撃の目的、動機

- ハクティビズム (政治的あるいは社会的な主義や主張)
  少数の確信犯による執拗な攻撃 (⇔ 多数の匿名参加者による攻撃)
  政治、外交、スポーツイベント
  日本および周辺諸国における活動
  - 歴史的特異日 (9/18 など)
  - 反捕鯨、小型クジラ漁反対 (#OpKillingBay 2013年〜)
  - 香港デモ (2019年 6月 Telegram, 2019年 8月 LIHKG)
  - 日韓関係 (2019年 10月)

- 金銭、怨恨、娯楽、ほか → カジュアルな攻撃の増加

Booter / Stresser (DDoS-as-a-Service, DDoS-for-Hire)

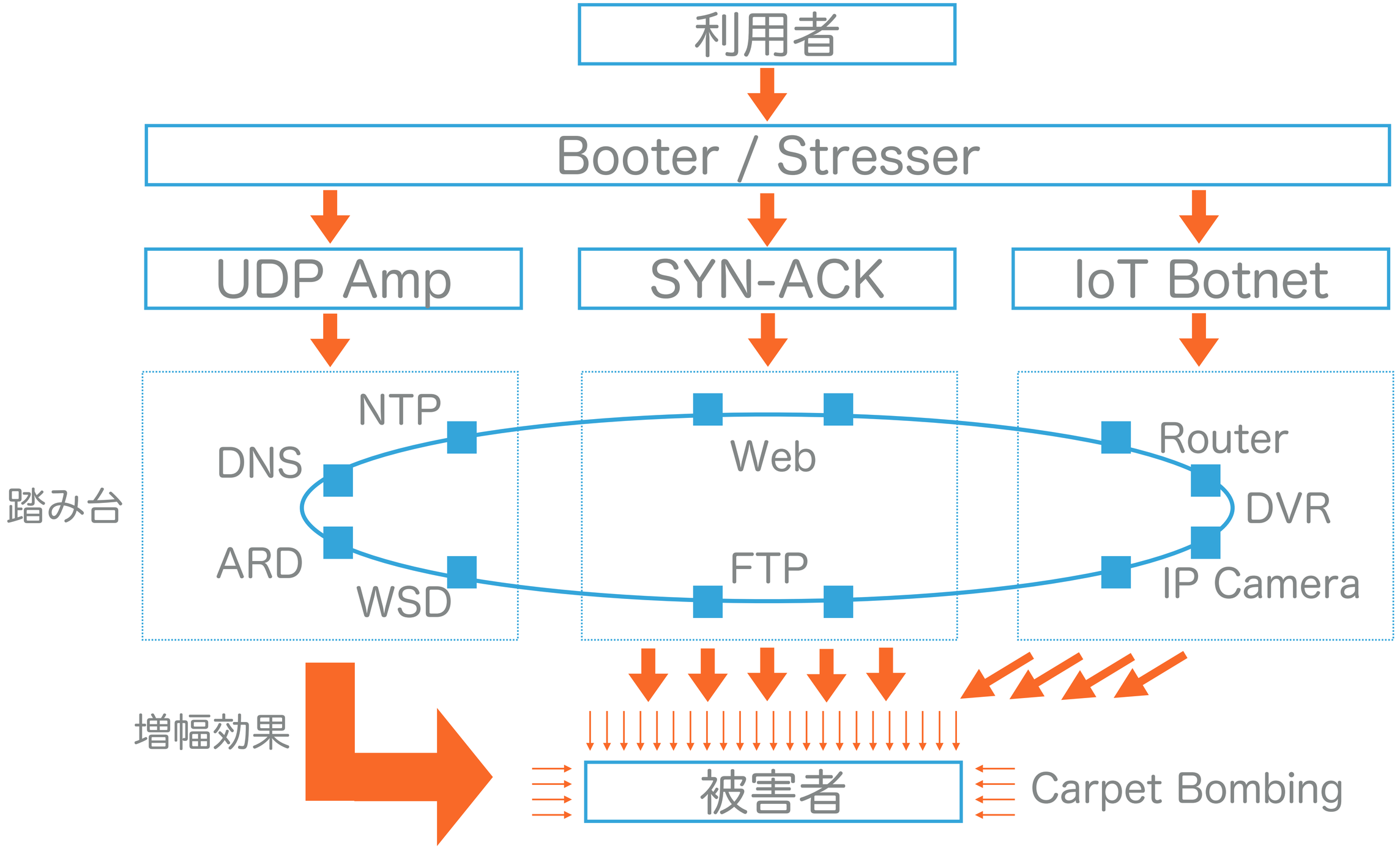
- 誰でも手軽に安く DDoS 攻撃が実施できるサービスの普及

DDoS 攻撃の主な攻撃手法

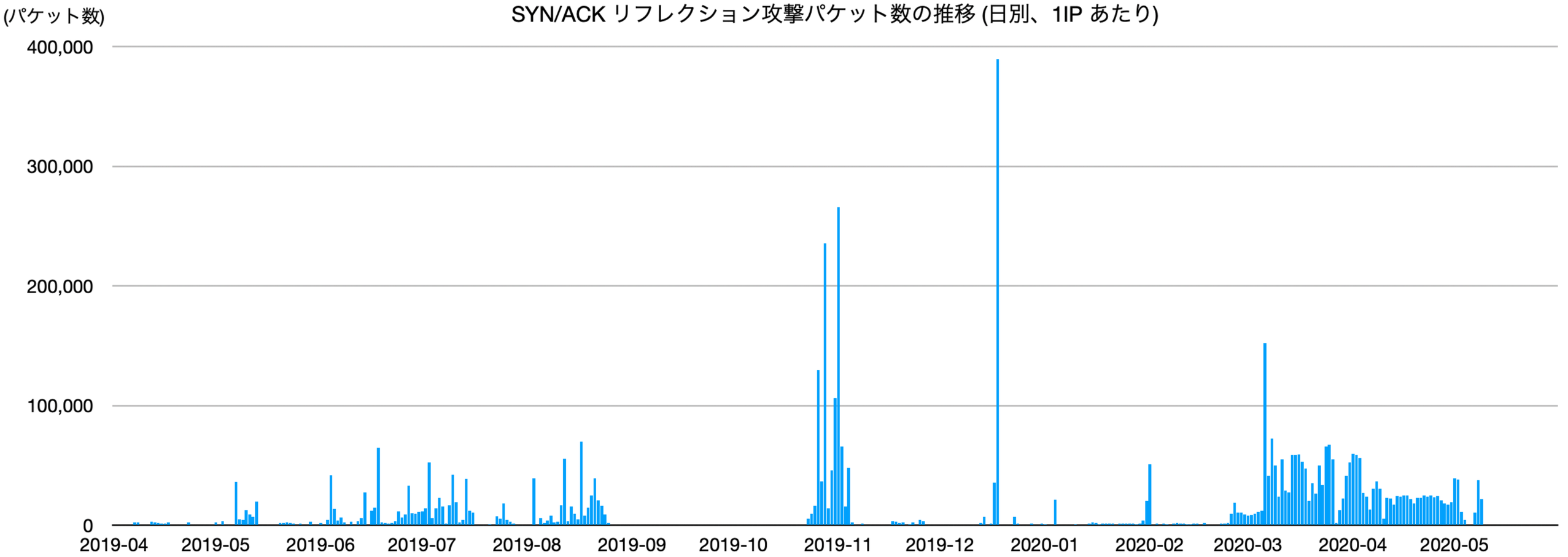
- UDP アンプ 攻撃
  DNS, NTP, CLDAP, SSDP
  Apple Remote Desktop (3283/udp), WS-Discovery (3702/udp)
- TCP SYN-ACK リフレクション攻撃
  2018年頃から急増, 2019年 8月 Servers.com への攻撃事例 (UDP + TCP)
- IoT ボットネットによる攻撃
  TCP / UDP / HTTP Flood
  多数の小規模ボットネット (数百 IP 程度) と一部の大規模ボットネット (数万 IP 程度)
  2019年 9月 Wikipedia, Twitch, Blizzard への攻撃事例 (moobot)

Carpet Bombing (絨毯爆撃)

- 単一の IP アドレスを狙うのではなく、サブネット (CIDR) 単位で攻撃する
- UDP アンプ攻撃や TCP SYN-ACK リフレクション攻撃との併用
- IP アドレス単位での攻撃検知を回避
- 2018年頃から急増


利用者
Booter / Stresser
UDP Amp
SYN-ACK
IoT Botnet
踏み台
NTP
DNS
ARD
WSD
Web
FTP
Router
DVR
IP Camera
増幅効果
被害者
Carpet Bombing

IIJ ハニーポットにおける攻撃観測



https://sect.iij.ad.jp/

クラス A (/8) 相当の広いレンジへの攻撃？

3月

4月

本日のトピック

- DDoS 攻撃
- 標的型ランサムウェア

標的型攻撃 + ランサムウェア + 情報流出

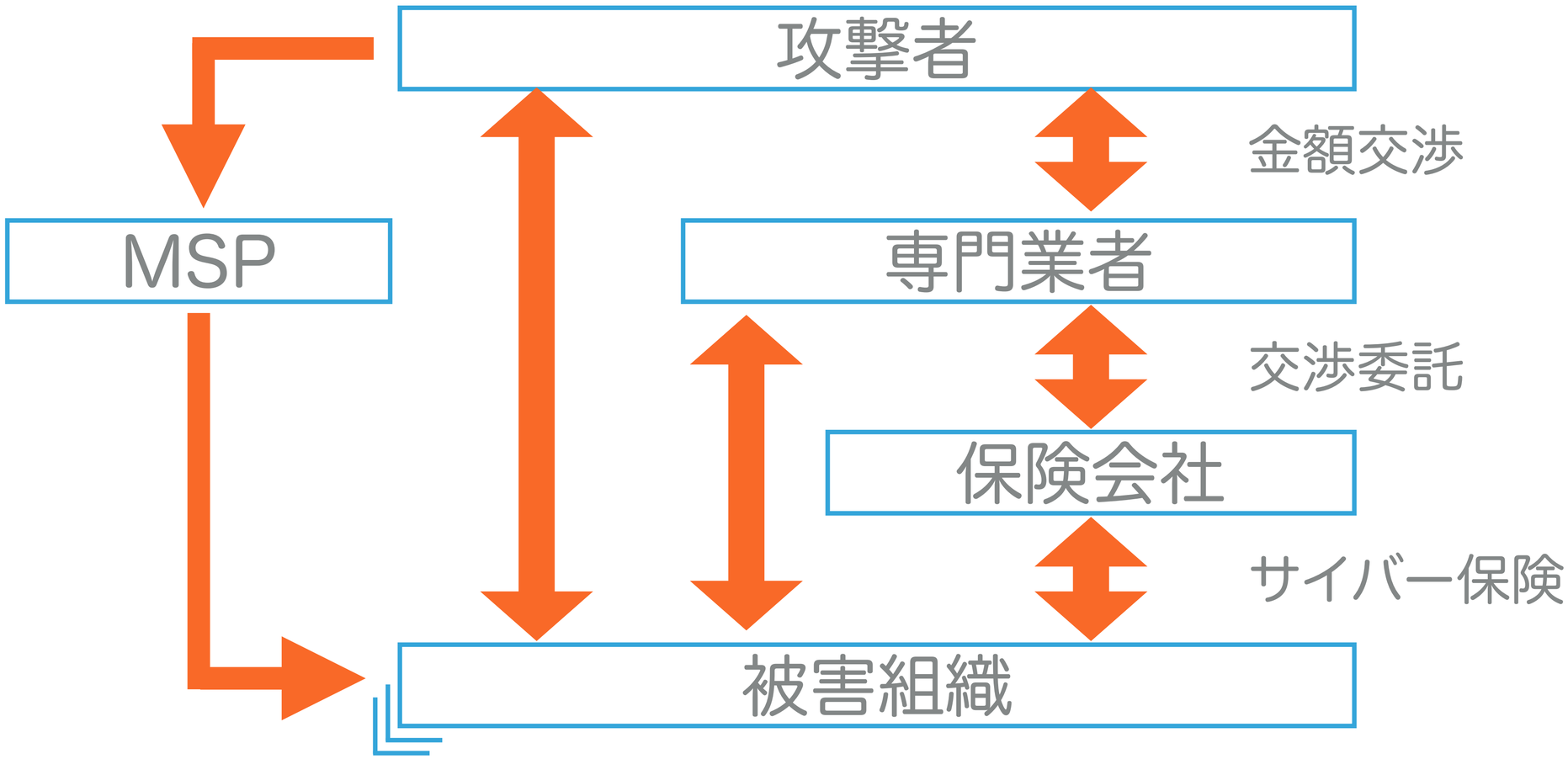
- 侵入からマルウェア感染に至る攻撃手法は標的型攻撃に近い
  → 組織内での横展開の活動もあり
- 長期間に渡る潜伏、調査活動 → 攻撃に慣れてくると短くなる傾向あり
- 最後にランサムウェアに一斉に感染させる
- 特定の業種、組織が狙われるケースが多い (病院、地方自治体など)
- 感染前に組織内の情報を窃取し、情報を流出させると脅迫するタイプの登場
  Clop, DoppelPaymer, Maze, REvil, など

標的型ランサムウェア攻撃

“Opportunistic” Ransomware		“Targeted” Ransomware
不特定多数の個人	攻撃対象	特定企業、業種の組織
スパムメール ドライブバイダウンロード	初期感染	スピアフィッシング RDP や VPN からの侵入
なし (あるいは自動)	感染拡大	手動による横展開 (潜伏調査期間あり)
低額 (端末単位)	身代金	高額 (組織単位、交渉の余地あり)
Locky, Cerber など	例	Ryuk, Maze など

時期	被害組織	ランサムウェア	身代金支払い	攻撃の特徴
2017年 6月	NAYANA	Erebus	あり	韓国のホスティングプロバイダー NAYANA で 6/10 に 153台の Linux サーバが Erebus ランサムウェアに感染。3,400〜5,000 の Web サイトに影響。2重のバックアップも含めてすべてのデータが暗号化されており、復旧が困難に。攻撃者は当初 1台あたり 10 BTCを要求。4日間にわたる交渉の結果、トータル 397.6 BTC (13億ウォン相当) で決着。
2018年 1月	Hancock Health	SamSam	あり	RDP から侵入し、バックアップデータを先に破壊。攻撃者は 4 BTC ($55K 相当) を要求。 1/11 感染、1/13 身代金支払い、1/14 復旧
2018年 3月	アトランタ市	SamSam	なし	攻撃者は 6 BTC ($51K 相当) を要求。市は緊急対応として $2.6M 相当のサービスを調達。 (復旧のために $17M 相当の支出が必要との試算)
2019年 3月	ジョージア州 ジャクソン郡	Ryuk	あり	攻撃者と交渉の末、$400K 相当の身代金を支払い。侵入経路は不明だが、攻撃者はシステム内に数週間潜伏していた可能性がある。
2019年 3月	Norsk Hydro	LockerGoga	なし	攻撃者は Active Directory を利用した可能性がある。多数の IT システムが影響を受け停止し、プラント操業は手動操作に切り替えて継続。復旧まで約 3ヶ月、約50〜55億円相当の被害金額を想定。
2019年 5月	ボルチモア市	RobbinHood	なし	攻撃者は 13 BTC ($76K 相当) を要求。復旧に1ヶ月以上。$18M 相当の被害金額を想定。
2019年 5月	フロリダ州 リビエラビーチ	Ryuk	あり	攻撃者は 65 BTC ($600K 相当) を要求。復旧のため、合計 400台の PCを $941K で購入。
2019年 6月	フロリダ州 レイクシティ	Ryuk	あり	攻撃者は 86 BTC を要求、交渉の結果 42 BTC ($460K 相当) を支払い。サイバー保険が適用された。
2019年 8月	テキサス州 22の地域	REvil	なし	攻撃者はトータル $2.5M を要求。MSP (TSM Consulting) 経由で感染した (ConnectWise Control が利用された)。
2019年12月	ニューオーリンズ市	Ryuk	なし	感染により少なくとも $7M の損害が発生、そのうち $3M は保険でカバーされた
2019年12月	Travelex	REvil	あり	1ヶ月以上サービス停止、285 BTC ($2.3M) の身代金を支払い
2019年12月	マーストリヒト大学	Clop	あり	DC 経由で 267台の Windows Server が感染、30 BTC ($220K) の身代金を支払い

特異なビジネス構造



対策の考え方

- 侵入経路はメールと RDP が大半を占める、MSP 経由にも注意
  → マルウェアやフィッシング対策など、基本をしっかりやる
  → 2019年から VPN などソフトウェアの脆弱性の悪用事例が増加

- バックアップ
  → 対応策は 2択 (1) バックアップから復旧 (2) 身代金を払って鍵を入手
  → 事後対応にあたってはどちらの選択肢も並行して検討する

- 事業継続の観点を忘れずに
  → 加えて、情報流出への対応も

(参考情報)

(1) DDoS 攻撃
wizSafe Security Signal 2020年4月 観測レポート https://wizsafe.iij.ad.jp/2020/05/985/
SOCレポート | Internet Infrastructure Review（IIR）Vol.46 https://www.iij.ad.jp/dev/report/iir/046/01.html
DDoS-as-a-Service: Investigating Booter Websites — University of Twente Research Information https://research.utwente.nl/en/publications/ddos-as-a-service-investigating-booter-websites
NETSCOUT Threat Intelligence Report | NETSCOUT https://www.netscout.com/blog/asert/netscout-threat-intelligence-report
UDP-Based Amplification Attacks | CISA https://www.us-cert.gov/ncas/alerts/TA14-017A
Anatomy of a SYN-ACK attack - Akamai Security Intelligence and Threat Research Blog https://blogs.akamai.com/sitr/2019/07/anatomy-of-a-syn-ack-attack.html
The Masked SYNger: Investigating a Traffic Phenomenon https://blog.rapid7.com/2020/05/28/the-masked-synger-investigating-a-traffic-phenomenon/

(2) 標的型ランサムウェア
日本国内で増加する標的型ランサムウェアインシデント https://www.secureworks.jp/resources/at-targeted-ransomware-spreading-in-japan
2019 年ランサムウェア最新動向 | トレンドマイクロ https://resources.trendmicro.com/jp-docdownload-form-m129-web-2019-ransomware.html
The state of ransomware 2020 https://news.sophos.com/en-us/2020/05/12/the-state-of-ransomware-2020/
Ransomware Payments Up 33% As Maze and Sodinokibi Proliferate in Q1 2020 https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report
Ransomware Attackers Aren't Sparing Anyone During Covid-19 https://blog.chainalysis.com/reports/ransomware-covid-19
List of ransomware that leaks victims' stolen files if not paid https://www.bleepingcomputer.com/news/security/list-of-ransomware-that-leaks-victims-stolen-files-if-not-paid/
Ransomware groups continue to target healthcare, critical services; here’s how to reduce risk - Microsoft Security https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
Research Report Examines Ransomware Negotiations and Response https://go.flashpoint-intel.com/forrester/forrester-guide-to-paying-ransomware
The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks — ProPublica https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks