Computer Security Symposium 2019
21 - 24 October 2019

クラウドサービス悪用攻撃の大規模実態調査

福士 直翼[1,a)]　千葉 大紀[2]　秋山 満昭[2]　内田 真人[1]

概要：クラウドサービスはサイバー攻撃のためのインフラとして悪用される場合がある．クラウドサービス上に配置されたサーバにはクラウド事業者の所有する IP アドレスが割り当てられ，サーバの利用停止とともにその IP アドレスが解放され別のサーバに割り当てられる．そのため，クラウドサービスを悪用するサイバー攻撃が行われた場合，クラウド事業者には所有する IP アドレスがブラックリストに掲載されてレピュテーションが低下するリスク，ユーザには過去に悪用されてブラックリストに掲載された IP アドレスが自身に割り当てられるリスクが生じる．本研究では，クラウドサービスを悪用する攻撃の観測にはブラックリストの活用が有効であることに着眼した大規模調査を行う．45 種類のブラックリストを利用して代表的な 2 つのクラウドサービスを対象にした調査を 43 日間行った結果，一日あたり，約 1 万件のクラウド事業者の IP アドレスがブラックリストに掲載されることが明らかとなった．また，クラウドサービス悪用攻撃の種別や利用される IP アドレスのリージョンの傾向，クラウドサービス悪用攻撃へのクラウド事業者の対処に関する，これまでに知られていなかった実態も明らかとなった．

A Large-scale Analysis of Cloud Service Abuse Attack

Naoki Fukushi[1,a)]　Daiki Chiba[2]　Mitsuaki Akiyama[2]　Masato Uchida[1]

Abstract: Cloud services are abused as infrastructure for cyber-attacks. In a cloud service, an assigned IP address for a server is owned by the cloud service provider. When the server is shut down, the assigned IP address is released and then assigned to another server in the same cloud service. Thus, cyber-attacks abusing cloud services pose risks of degrading its reputation for the services and being falsely blacklisted for end-users. In this paper, we conduct a large-scale measurement study of cloud service abuse attacks using blacklisted IP addresses. Our analysis regarding two cloud services for 43 days using 45 types of blacklists revealed that about 10k IP addresses continue to be blacklisted daily. Moreover, our study showed some attack trends using cloud services such as attack types, regions, and anti-abuse actions.

1. はじめに

クラウドサービスとは，クラウド事業者が自らが所有するサーバ，ストレージ，アプリケーションといったコンピューティングリソースを，ユーザが必要なときに必要な分だけ提供するサービスのことである．その利便性の高さから，クラウドサービスの世界市場は急速に拡大を続けており，2019 年第 2 四半期には前年の 191 億ドルから 37.6%増加した 263 億ドル規模となったことが示されている [1]．一方で，クラウドサービスはサイバー攻撃の攻撃インフラとして悪用される場合もある．たとえば，インスタグラムのアカウントがクラウド上の大量のサーバを利用したブルートフォース攻撃により乗っ取られた事例 [2] や，クラウド上のサーバが C&C（Command & Control）サーバとして利用されていた事例 [3] が報告されている．本研究では，このようなクラウドサービスを悪用するサイバー攻撃を新たに「クラウドサービス悪用攻撃」と呼ぶ．

クラウドサービス悪用攻撃が行われると，クラウド事業者とユーザの双方にリスクが生じる．たとえば，クラウド事業者には，所有する IP アドレスが悪用されることによってブラックリストに掲載され，レピュテーションが低下してしまうというリスクが生じる．また，ユーザには，過去

[1] 早稲田大学
Waseda University
[2] NTT セキュアプラットフォーム研究所
NTT Secure Platform Laboratories
[a)] n.wing.fks.0319@akane.waseda.jp

に悪性活動に利用されてブラックリストに掲載されたIPアドレスが自らの利用するサーバに割り当てられ，様々な制約が生じるというリスクが生じる．これは，クラウドサービスではユーザに貸し出すサーバに割り当てるIPアドレスがユーザ間で共有されているためである．しかし，クラウドサービス悪用攻撃の実態は明らかにされていない．

そこで本研究では，クラウドサービス悪用攻撃の実態，及びそれに伴い生じるリスクを明らかにすることを目的とした大規模調査を行う．この調査を行う上では，幅広い攻撃種別のサイバー攻撃を行うクラウドサービス悪用攻撃を大規模に観測する手法が必要となる．本研究では，このような観測を実現するために，複数の異なる種類のブラックリストを組み合わせて活用することに着眼する．そして，代表的なクラウドサービスであるAWS EC2（Amazon Web Service Elastic Compute Cloud），及びMicrosoft Azureの2つを対象にしたクラウドサービス悪用攻撃の大規模実態調査を行う．45種類のブラックリストを用いた43日間にわたる調査の結果，延べ1,956,570件のIPアドレスが観測され，一日あたり，約1万件のクラウド事業者のIPアドレスがブラックリストに掲載され，そのうち約5%が入れ替わることが明らかとなった．また，クラウドサービス悪用攻撃の種別や利用されるIPアドレスのリージョンの傾向，クラウドサービス悪用攻撃へのクラウド事業者の対処などに関する，これまでに知られていなかった実態も明らかとなった．本研究の調査結果は，クラウド事業者，ユーザ，さらにはブラックリスト事業者のそれぞれがクラウドサービス悪用攻撃に効果的に対処するための足がかりとなる．

本研究の貢献は以下の通りである．

(1) クラウドサービス悪用攻撃について，はじめての大規模実態調査を行った
(2) 多量かつ多様なブラックリストを用いたクラウドサービス悪用攻撃の観測手法を提案した
(3) 調査結果にもとづいて，クラウド事業者，ユーザ，ブラックリスト事業者のそれぞれに対してクラウドサービス悪用攻撃への対策を提案した

2. クラウドサービスとブラックリスト

2.1 クラウドサービス

クラウドサービスを利用することで，ユーザはハードウェアの初期導入や保守・運用にかかるコストを削減することができる．一般にクラウド事業者は世界各国にデータセンタを所有しており，データセンタのある各地域のことをリージョンと呼ぶ．ユーザはクラウドサービスを利用する際に，コンピューティングリソースの配置されているリージョンを選択することができる．利用料金やサーバに割り当てられるIPアドレスの範囲は，選択したリージョンごとに異なる．また，サーバに割り当てられていたIPアドレスはサーバの利用停止とともに解放され，別のサーバに割り当てられる仕組みになっている．つまり，クラウドサービスのIPアドレスはユーザ間で共有されている．

クラウドサービスを提供する事業者は数多く存在するが，本研究ではAWS EC2とMicrosoft Azureの2つを対象にした調査を行う．これは，ユーザ数の多いサービスは多くの攻撃者も同様に利用することが考えられ，かつ，攻撃者によって悪用された場合の一般ユーザへの影響も大きくなるためである．実際，Canalys社により，2019年第2四半期において，クラウドサービス市場全体の収益の約50%を上記の2つのクラウドサービスが占めていることが示されている[1]．なお本研究では以降，AWS EC2，Microsoft Azureをそれぞれ EC2，Azureと表記する．

2.2 ブラックリスト

本研究で扱うブラックリストとは，悪性活動に関与したことが判明したIPアドレスをリスト化したもののことを示す．ブラックリストは，そこに掲載されているIPアドレスを送信元あるいは送信先とする通信を特定するために利用される．ブラックリストの作成方法には，大きく分けて2種類がある．一つは，ブラックリスト事業者が，悪性活動を行っているIPアドレスを自ら観測してリスト化する方法である．もう一つは，ブラックリスト事業者が，ユーザから報告された悪性活動を行っているIPアドレスをリスト化する方法である．

ブラックリストはある時点で作成されたものが使われ続けるのではなく，事業者によって定期的に更新される．ただし，更新される時間や間隔はブラックリストごとに異なる．また，一度掲載されたIPアドレスが，それ以降攻撃が観測されなかった場合でもそのまま掲載され続けられる期間もブラックリストごとに異なる．これは，ブラックリスト事業者のポリシーが異なるためである．一般にブラックリストには，公開ブラックリストと商用ブラックリストがある．本研究では公開ブラックリストのみを利用する．

また，ブラックリストの中には，掲載されているIPアドレスの登録解除を第三者が申請できるものがある．このような申請が可能な理由は大きく二つある．一つは，本来は悪性活動を行っていないユーザのIPアドレスが，誤ってブラックリストに掲載されてしまう場合があるからである．もう一つは，実際に悪性活動は行われていたIPアドレスが，その後の対処により，すでに悪性活動を行っていない場合があるからである．

3. 調査手法

本研究では，代表的なクラウドサービスであるEC2，及びAzureの2つを対象にしたクラウドサービス悪用攻撃の大規模実態調査を行う．この調査のためには，様々な種別の攻撃を行うクラウドサービス悪用攻撃を，大規模かつ継続的に観測することのできる環境が必要となる．しかし，

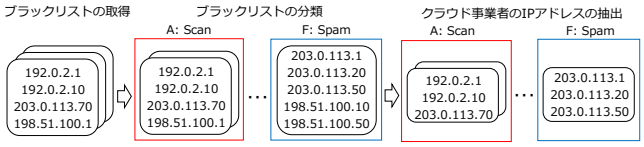


図 1　クラウドサービス悪用攻撃の観測手法の概要

そのような環境を用意することはきわめて困難である．たとえばクラウドサービス悪用攻撃の観測手法としてハニーポットやダークネットが考えられるが，どちらも観測範囲が限定され，かつ観測される攻撃の種別もブルートフォース攻撃やスキャンに限定されてしまうという問題がある．

本研究ではこの問題を解決するために，IP アドレスのブラックリストに着眼した．複数のブラックリストを統合することで，観測地点と観測できる攻撃の種別の両方を擬似的に増やすことができると考えたからである．さらにブラックリストは定期的に更新されるため，時系列調査が行いやすいという利点もある．従来のブラックリストに関する研究 [4], [5], [6] では，ブラックリストそのものの精度や特性に関する調査が主眼とされてきた．しかし本研究ではブラックリストを活用することに着眼しており，このことは本研究と従来のブラックリストに関する研究との大きな違いとなっている．本研究では，45 種類のブラックリストを用いて 43 日間にわたるクラウドサービス悪用攻撃の大規模実態調査を行う．

本調査手法の技術的な要点は以下の 2 点である．一つはブラックリストを観測する攻撃種別ごとに分類し，掲載される IP アドレスが利用された攻撃の種別を考慮した分析を行った点である．もう一つはブラックリストに掲載される IP アドレスの経時変化を分析し，クラウドサービス悪用攻撃の傾向をはじめて明らかにした点である．

3.1　クラウドサービス悪用攻撃の観測

本節では，ブラックリストを利用してクラウドサービス悪用攻撃を観測するための手法について説明する．本手法は入力とするブラックリストの取得，ブラックリストの攻撃種別ごとの分類，クラウド事業者の IP アドレスの抽出，の 3 つの手順で構成される．その概要を**図 1** に示す．以下では，各手順について順に説明する．

ブラックリストの取得：本研究では 2019 年 6 月 30 日から 2019 年 8 月 11 日までの 43 日間にわたって，22 種類の事業者から合計 45 種類のブラックリストを，日本時間の午前 10 時に毎日取得し続けた．ここで，ブラックリストの取得間隔を一日単位にした理由は，本研究で取得対象としたブラックリストの多くが一日単位で更新されるためである．本研究で取得したブラックリストについて，事業者名とその事業者から取得したブラックリストの個数を**表 1** にまとめる．表 1 より，複数種類のブラックリストを提供する事業者を確認することができる．

表 1　ブラックリストの事業者名と取得個数

#	事業者名	取得個数	#	事業者名	取得個数
1	Badips	11	12	DShield	1
2	Fail2ban	7	13	Feodo	1
3	Normshield	6	14	Haley	1
4	ProjectHoneyPot	3	15	LashBack	1
5	AlienVault	1	16	MyIP	1
6	Bambenek	1	17	NixSpam	1
7	Binary Defense	1	18	Nothink	1
8	BotScout	1	19	Sblam	1
9	CleanTalk	1	20	StopForumSpam	1
10	CyberCrime	1	21	Talos	1
11	Dangerrulez	1	22	VoIPBL	1

表 2　各ブラックリストの攻撃種別とその個数

攻撃種別	概要	個数
Scan	ポートスキャン，脆弱性スキャンを行うホスト	5
Brute-force	ブルートフォース攻撃を行うホスト	10
Malware	C&C サーバ，マルウェア配布サーバ	3
Exploit	脆弱性をリモートから悪用しようとするホスト	10
Botnet	ボットネットに属するホスト	7
Spam	スパムを送信するホスト	10
合計		45

ブラックリストの攻撃種別ごとの分類：次に，取得したブラックリストを攻撃種別ごとに分類する手順について説明する．本研究では取得した 45 種類のブラックリストをそれぞれ，ブラックリスト事業者による説明文にもとづいて，Scan，Brute-force，Malware，Exploit，Botnet，Spam という 6 種類の攻撃種別に分類する．上記の 6 種類の攻撃種別は，文献 [6] で定義されたものである．**表 2** に，各攻撃種別の概要と，そこに分類されるブラックリストの個数を示す．たとえば，説明文に「ハニーポットにおいて，ブルートフォース攻撃を行っていることが確認された IP アドレス」と記載されているブラックリストは Brute-force に，「スパムを送信していることが確認された IP アドレス」と記載されているブラックリストは Spam にそれぞれ分類される．これにより，各ブラックリストの掲載 IP アドレスがそれぞれどのような攻撃を行っていたのかまで考慮した分析が可能となる．

クラウド事業者の IP アドレスの抽出：最後に，ブラックリストに掲載されている IP アドレスから，クラウド事業者の IP アドレスを抽出する手順について説明する．本研究で調査対象としたクラウドサービスである EC2 及び Azure はそれぞれ，サービスの利用者に貸し出すサーバに割り当てる IP アドレスの範囲を公開している [7], [8]．そこで本研究では，各ブラックリストの掲載 IP アドレスと上記の IP アドレスの範囲を照合する．これにより，各ブラックリストに掲載されたクラウド事業者の IP アドレスを抽出できる．クラウド事業者の IP アドレスがブラックリストに掲載されることは，クラウドサービス悪用攻撃が行われ，それがブラックリスト事業者によって観測されたということを示す．つまり，ブラックリストに掲載されるクラウド事業者の IP アドレスを観測することで，クラウドサービス

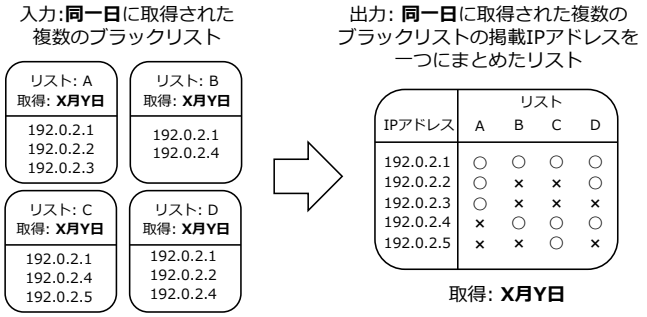


図 2　同一日に取得された複数のブラックリストの統合

悪用攻撃が行われたという事実を間接的に観測できる．なお本研究では，IPv4 アドレスのみを調査対象とした．この理由は，本研究で利用したブラックリストのほとんどが IPv6 アドレスを掲載していなかったためである．

3.2　クラウドサービス悪用攻撃の傾向の調査

本節では，ブラックリストを用いてクラウドサービス悪用攻撃の傾向を調査する手法について説明する．本研究では，日々取得した 45 種類のブラックリストを日毎に一つのリストに統合する．本研究では 43 日間ブラックリストを取得したため，このような統合リストも 43 個生成される．この方法を**図 2** を用いて説明する．図 2 では，ある同一日（X 月 Y 日とする）に取得された 4 種類の異なるブラックリスト A，B，C，D を統合する方法を示している．この統合リストを用いることで，統合に利用した各ブラックリストに掲載された IP アドレスの一覧と，各 IP アドレスが掲載されていたブラックリストを確認できる．統合リストに掲載された IP アドレスは，統合に利用した N 個（図 2 の例では $N = 4$ である）のブラックリストのうち，少なくとも 1 つのリストで掲載されていた IP アドレスである．この統合リストは，クラウドサービス悪用攻撃の日毎の傾向を明らかにする上で有用である．本研究では以下の 5 つの観点でクラウドサービス悪用攻撃の傾向を調査する．

- 一日あたりに悪用される IP アドレス数はどのくらいか（4.1 節）
- 悪用される IP アドレス数に経時変化は存在するか（4.1 節）
- クラウドサービス，及び攻撃種別の違いによって悪用される IP アドレス数に違いは存在するか（4.1 節，4.2 節）
- 異なる攻撃種別のブラックリストに同時に掲載されている IP アドレスは存在するか（4.3 節）
- 悪用される IP アドレスのリージョンに特徴は存在するか（4.4 節）
- 悪用される IP アドレスのブラックリストへの掲載継続確率はどのようになっているか（4.5 節）
- 悪用される IP アドレスの登録解除申請は観測できるか（4.6 節）

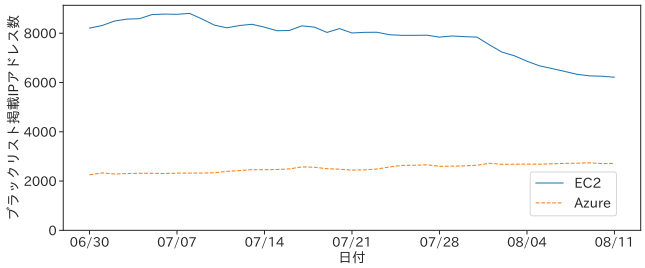
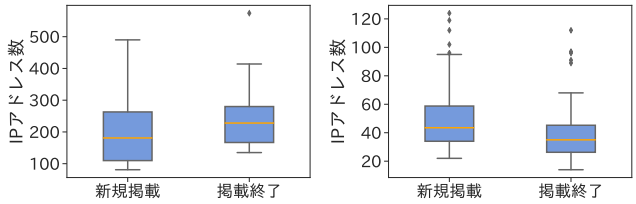
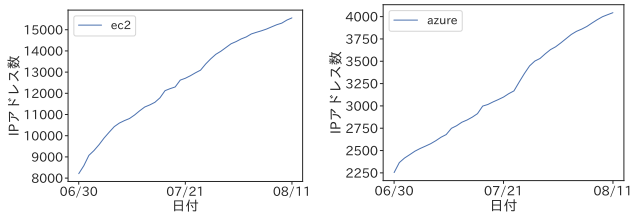


図 3　ブラックリスト全体での掲載 IP アドレス数の変化



(a) EC2　(b) Azure

図 4　日付ごとの新規掲載/掲載終了 IP アドレス数



(a) EC2　(b) Azure

図 5　観測されたユニークな IP アドレス数の経時変化

4.　調査結果

4.1　掲載 IP アドレス数とその経時変化

掲載 IP アドレス数の調査の結果，本研究で取得した 45 種類のブラックリスト全体で，EC2 の IP アドレスは一日あたり約 7,838 件，Azure の IP アドレスは一日あたり約 2,521 件掲載されていることが明らかになった．さらにこのうち，EC2 の IP アドレスは一日あたり約 436 件，Azure の IP アドレスは一日あたり約 94 件が入れ替わっていることも判明した．つまり，日々約 1 万件のクラウド事業者の IP アドレスが掲載され，そのうち約 5%は日々入れ替わっているという状況である．ここで，EC2 と Azure のそれぞれについて，横軸に日付，縦軸にその日付に取得されたブラックリスト全体での掲載 IP アドレス数を取ったグラフを**図 3** に示す．図 3 より，ブラックリスト掲載 IP アドレス数について，EC2 には減少傾向があり，一方で Azure にはゆるやかな増加傾向があることが確認できる．

この傾向をより詳細に確認するために，ブラックリスト全体で，日付ごとに新規掲載される IP アドレス数と掲載終了する IP アドレス数の調査を行う．調査はクラウドサービスごとに行った．調査結果を**図 4** に示す．図 4 では，合計で 42 日間の日付ごとに調査された複数の値を箱ひげ図

表 3 攻撃種別ごとの掲載 IP アドレス数とその割合

攻撃種別	個数	EC2 件数（割合）	Azure 件数（割合）
Scan	5	17（0.20%）	9（0.27%）
Brute-force	10	3,144（36%）	2,010（60%）
Malware	3	57（0.66%）	45（1.3%）
Exploit	10	665（7.7%）	404（12%）
Botnet	7	839（9.7%）	281（8.4%）
Spam	10	3,934（45%）	609（18%）
Total	45	8,656（100%）	3,361（100%）

で示している．ここで，ブラックリストの合計取得日数である 43 日間より 1 日分だけ少ない理由は，取得初日は前日の情報がないため新規掲載及び掲載終了 IP アドレスの数を調査することができないからである．図 4 より，EC2 では掲載終了 IP アドレスの方が多く，一方で Azure では新規掲載 IP アドレスの方が多くなる傾向があることが改めて確認できる．

さらに，ブラックリストの合計取得日数である 43 日間で，累計で観測されたユニークな IP アドレスの件数を調査する．調査の結果，このような IP アドレスの件数は EC2 で 15,528 件，Azure で 4,044 件であることがわかった．これらの件数がどのように経時変化していたのかを調査する．**図 5** に，縦軸に累計で観測されたユニークな IP アドレスの件数，横軸に日付を取ったグラフを示す．図 5 より，EC2 と Azure の双方で，累計で観測されたユニークな IP アドレスの件数は単調に増加していることが確認できる．また，一日あたりの累計で観測されたユニークな IP アドレスの増加数，すなわちグラフの傾きは，EC2 で約 171 件，Azure で 42 件である．これらの数は，図 4 に示した，一日あたりの新規掲載 IP アドレス数の中央値とほぼ等しい値になっている．つまり，新規に掲載される IP アドレスのほとんどが観測開始からはじめてブラックリストに掲載されたものであることが明らかになった．このことは，クラウド事業者の IP アドレスのうち，クラウドサービス悪用攻撃に利用されたことのあるものの割合が増え続けていることを示している．IP アドレスがユーザ間で共有されている現状において，ユーザに過去に悪用された IP アドレスが割り当てられるリスクもそれに伴って増加する．よって，上記の結果はクラウドサービス悪用攻撃への対策がより重要かつ必要なものとなっていることを示唆している．

4.2 攻撃種別ごとの調査

次に，各ブラックリストの攻撃種別に基づいた調査を行う．4.1 節における調査では，攻撃種別を考慮せずに 45 種類のブラックリストすべてを統合した．一方で本節では，攻撃種別ごとにブラックリストを統合し，一日あたりの平均掲載 IP アドレス数と，その数が各攻撃種別の総和に占める割合をそれぞれ調査する．調査結果を**表 3** に示す．なお，表 3 における各攻撃種別の総和が 4.1 節で明らかになったブラックリスト全体の掲載 IP アドレス数の日平均に一致していない．これは，複数の攻撃種別のブラックリストに同時に掲載されている IP アドレスが存在するためである．表 3 より，EC2 と Azure ではともに Brute-force と Spam に分類される IP アドレス数が多く，この 2 つの攻撃種別だけで全攻撃種別の合計数の 8 割近くを占めていることがわかる．このことは，クラウドサービス悪用攻撃には，ブルートフォース攻撃やスパムの送信が多いということを示唆している．また，EC2 では Spam に分類される IP アドレス数が Brute-force に分類される IP アドレス数の約 1.25 倍であるのに対し，Azure では Brute-force に分類される IP アドレス数が Spam に分類される IP アドレスの 3 倍以上になっていることがわかる．このことは，Azure は EC2 と比較して，ブルートフォース攻撃に悪用される傾向が強いことを示唆している．

表 4 攻撃種別の組み合わせの上位 5 種類

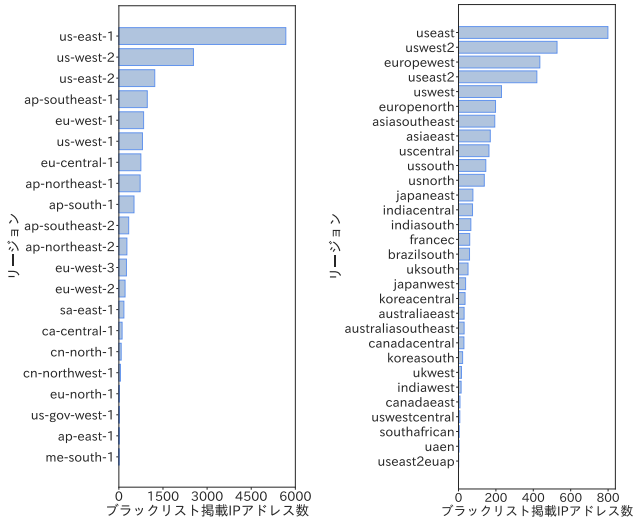
攻撃種別の組み合わせ	EC2 件数	Azure 件数
Exploit + Spam	87	54
Brute-force + Spam	59	45
Botnet + Spam	57	18
Brute-force + Exploit	15	10
Botnet + Brute-force	6	9

4.3 複数の攻撃種別のサイバー攻撃を同時に行うクラウドサービス悪用攻撃

4.2 節で言及したように，クラウド事業者の IP アドレスのなかには，複数の異なる攻撃種別のブラックリストに同時に掲載されるものが存在する．本節ではこのような複数の攻撃種別のサイバー攻撃を同時に行うクラウドサービス悪用攻撃について調査する．調査の結果，このような IP アドレスは一日あたりに EC2 で平均約 247 件（一日あたりの平均掲載件数に対して約 3.2%），Azure で平均約 163 件（一日あたりの平均掲載件数に対して約 6.5%）存在することがわかった．ここで，各 IP アドレスが行う攻撃種別の組み合わせについて，一日あたりの平均掲載 IP アドレス数が上位 5 件であったものをその数と共に**表 4** に示す．表 4 より，複数の攻撃種別のサイバー攻撃を同時に行うクラウドサービス悪用攻撃は EC2 と Azure に共通して，スパムの送信と同時に他の攻撃も行うものが多いという特徴があることがわかる．なお，攻撃種別の組み合わせの上位 5 件は，EC2 と Azure で一致していた．

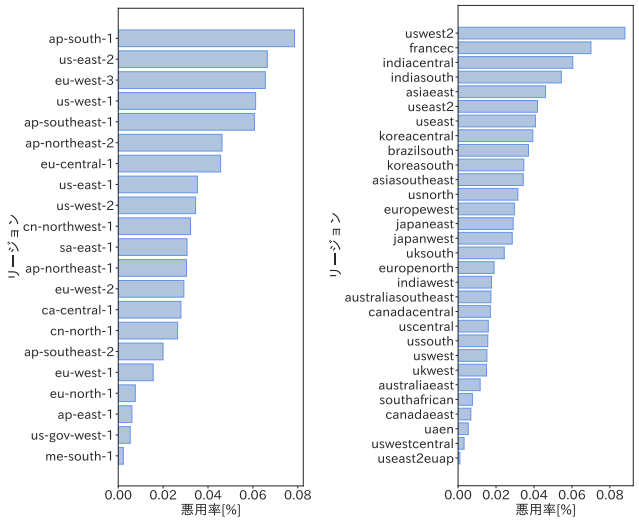
4.4 IP アドレスのリージョンの調査

本節では，クラウドサービスの IP アドレスのリージョンに着目した調査を行う．具体的には，観測期間中にブラックリストに掲載されたすべてのユニークな IP アドレスについて，そのリージョンの調査を行った．なお，調査対象の IP アドレスの数は，4.1 節で特定したように，EC2 で 15,528 件，Azure で 4,044 件である．調査結果として，各クラウドサービスごとに，縦軸にリージョン，横軸に掲載



(a) EC2　　(b) Azure

図 6　リージョンごとの掲載 IP アドレス数



(a) EC2　　(b) Azure

図 7　リージョンごとの悪用率

IP アドレス数を取った棒グラフを**図 6** に示す．図 6 より，EC2 と Azure ではともに，ブラックリスト掲載 IP アドレス数にはリージョンごとに偏りが存在することが確認できる．EC2 では，us-west1 をのぞき，us リージョンの利用料金は安く通信速度も速い [9]．そのため一般のユーザと同様に，攻撃者にも多く選択された可能性が高いと考える．同様に，Azure でも利用料金の安い us リージョンの掲載 IP アドレス数が多いが，利用料金が高めである europewest の掲載 IP アドレス数も上位となっており，単純に利用料金が安い順に使われているわけではないことも確認できる．なお，Azure のリージョンごとの利用料金は [10] を参照した．

上記の調査では，ブラックリストに掲載された IP アドレスの絶対数に着目した分析を行っている．そこで次に，これらの数が各リージョンの保有する全 IP アドレス数に占める割合について調査する．本研究では，この割合をリージョンごとの IP アドレスの「悪用率」と呼ぶ．調査結果

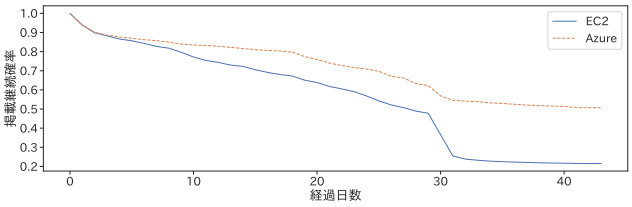


図 8　経過日数とブラックリストへの掲載継続確率の関係

を**図 7** に示す．図 7 より，ブラックリスト掲載 IP アドレス数と同様に，悪用率にもリージョンごとに偏りが存在することが確認できる．一方で，図 6 と図 7 を比較すると，ブラックリスト掲載 IP アドレス数が多かったリージョンの悪用率が必ずしも高くないことも確認できる．これを定量的に評価するために，リージョンのブラックリスト掲載 IP アドレスの順位と悪用率の順位の相関を算出することができるスピアマンの順位相関係数を用いる．算出したスピアマンの順位相関係数は，EC2 では約 0.42，Azure では約 0.13 となった．これは，ブラックリスト掲載 IP アドレス数と悪用率について，EC2 ではやや正の相関があり，Azure ではほとんど相関がないということを示している．

4.5　IP アドレスの掲載継続確率の分析

本節では，IP アドレスがブラックリストに掲載されてから N 日間後にも掲載され続けている確率を N 日間後の「掲載継続確率」として定義し，カプランマイヤー法を用いて分析する．本研究においては，観測期間が 43 日間で打ち切られている．カプランマイヤー法を用いることで，打ち切りがある場合の掲載継続確率を求めることができる．

カプランマイヤー法による分析結果として，縦軸に IP アドレスの掲載継続確率（累積補分布），横軸にブラックリストに掲載されてからの経過日数を取ったグラフを**図 8** に示す．図 8 より，Azure の IP アドレスの掲載継続確率は，EC2 と比較して全体的に高くなっていることがわかる．このことは，Azure ではクラウドサービス悪用攻撃がより長期化する，つまりクラウドサービス悪用攻撃にクラウド事業者が十分に対処していない傾向があることを示唆している．ここで，EC2 と Azure 間で，掲載から 30 日以上が経過した後の IP アドレスの掲載継続確率に約 30%の特に大きな違いが生じている理由について考察する．本研究で取得した 45 種類のブラックリストそれぞれにおけるクラウド事業者の IP アドレスの掲載数は，EC2 と Azure で大きな違いは存在していない．また，本研究で取得したブラックリストの多くは，掲載期間のポリシーは 30 日間である．つまり EC2 では，ブラックリストへの掲載を行った日以降は攻撃が観測されず，ポリシーによって 30 日間掲載された後に，すぐに掲載が終了したものが多いと考えることができる．一方で Azure では，経過日数が 30 日を過ぎても掲載継続確率は大きく減少していないため，継続的に悪

用されるものが多かったことがわかる．

EC2 と Azure でこのような掲載継続確率の違いが生じた理由の一つとして，AWS 不正使用対策チームの貢献があると考えられる．ユーザは AWS リソースが不正使用されていることに気がついた場合，AWS 不正対策チームに対して報告することができる．つまり，ユーザから行われた情報提供にもとづいて AWS 不正使用対策チームが対処を行っているため，クラウドサービス悪用攻撃の長期化を防ぐことができている可能性がある．図 4 においても，EC2 ではブラックリストに掲載されなくなる IP アドレスの数のほうが多く，一方で Azure では新しく掲載されるようになる IP アドレスの数のほうが多くなる傾向があることも上記の考察を補強するものとなっている．

4.6 クラウド事業者の IP アドレスへの登録解除申請

本節ではクラウド事業者の IP アドレスについて，登録解除申請の状況を調査する．この調査により，申請を行ったクラウド事業者またはユーザ，及び申請に対応したブラックリスト事業者の現状でのクラウドサービス悪用攻撃への対処状況をはかることができる．

たとえば掲載期間のポリシーが N 日間であると明記されているブラックリストにおいて，掲載された IP アドレスが N 日未満でブラックリストから削除された場合，それは第三者からの登録解除申請によるものであると考えられる．調査の結果，登録解除申請が行われていると考えられるクラウド事業者の IP アドレスを実際に確認することができた．具体的には，掲載期間のポリシーが 30 日間と明記されているあるブラックリストで，30 日未満で掲載が終了している IP アドレスが 215 件存在することが明らかになった．しかしこの件数はそのブラックリストに累計で掲載されたクラウド事業者の IP アドレスの約 3.7%であり，ほとんどの IP アドレスについては攻撃が継続して行われているか，登録解除申請が行われていないこともわかる．

5. 議論と制約事項

5.1 議論

4 章に示した調査結果をふまえて，本研究ではクラウドサービスのユーザ，クラウド事業者，そしてブラックリスト事業者に対して以下の提案を行う．

ユーザ：ユーザはクラウドサービスの利用の際には，割り当てられた IP アドレスをブラックリストと照合しておくことが望ましいと考える．割り当てられた IP アドレスが以前にクラウドサービス悪用攻撃に利用されたものであった場合，ブラックリストに当該 IP アドレスが掲載され続けており通信が遮断されるなど，サービスの利用に支障が生じるからである．たとえば IPVoid [11] という Web サービスでは，ブラウザ上で調べたい IP アドレスを入力するだけで，その場で合計 100 種類以上のブラックリストと照合した結果を得ることができる．もしもブラックリストへの掲載が認められた場合には，サーバを停止してから再起動することで，異なる IP アドレスの割り当てを受けるなどの対策を行うことができる．

クラウド事業者：クラウドサービス悪用攻撃が絶えず起こる状況下では，クラウドサービス悪用攻撃に利用された後に解放された IP アドレスをすぐに別のユーザに対して割り当ててしまうと，そのユーザのサービスの利用に様々な制限が生じる．そこでクラウド事業者は早期にクラウドサービス悪用攻撃を発見して対処することで，自社のサービスを利用したサイバー攻撃を最小限に抑えるとともに，ユーザに対して可用性の高いクラウドサービスを提供することが求められる．これを実現するために，クラウド事業者は本研究の調査手法を使用できる．つまり，複数の IP アドレスのブラックリストを横断的に観測し，自らの保有する IP アドレスの掲載が観測された場合には，当該 IP アドレスを利用するユーザに警告したり解約させるといった対処を取ることができる．

ブラックリスト事業者：ブラックリスト事業者は，ブラックリストを作成する際に誤検知をできるだけ減らす必要がある．4.5 節に示したように，EC2 の IP アドレスについて，ポリシーによって 30 日間掲載されていたが実際にはブラックリストに掲載された日以降に攻撃が観測されなかったと考えられる IP アドレスが多く存在する．クラウド事業者の IP アドレスはユーザ間で共有されるため，このような IP アドレスを長期間ブラックリストに掲載し続けることは望ましくない．ブラックリスト事業者は本研究の調査手法と同様に，クラウド事業者の IP アドレスを識別して異なる対処を行うことができる．たとえば，クラウド事業者の IP アドレスからの攻撃を特定した際には，ブラックリストに掲載するだけでなく，当該クラウド事業者へ通知することで，より迅速な対処が実現される可能性がある．

5.2 制約事項

本研究には大きく二つの制約事項が存在する．一つは，EC2 と Azure 以外のクラウドサービスについては調査していないことである．これは今後の課題としたい．もう一つは，本調査のクラウドサービス悪用攻撃の観測範囲が，ブラックリスト事業者の観測範囲に制限されていることである．インターネット上で発生しうる攻撃をすべてもれなく観測することは不可能であることから，この制限を完全に解決することは簡単ではないが，今後，調査対象のブラックリストとその期間を増やした調査を行うことで可能な限り網羅的な調査を行うこととしたい．

6. 関連研究

IP アドレスはインターネットにおける最も基本的かつ必須の識別子であるため，以前より多数の研究が行われて

きた．本稿では関連研究を攻撃に利用される悪性 IP アドレスに着目した研究と，IP アドレス自体の変化に着目した研究に大別して整理する．

悪性 IP アドレス：文献 [12] では，2004 年から 2005 年当時にスパムトラップで収集した大量のスパムメールの送信元 IP アドレスの特性を解析し，スパムメールの送信元が特定の IP アドレスレンジに偏っていることを観測している．また，文献 [4] は，スパムメール対策用の商用 IP ブラックリストが 3 割以上のスパムメール送信元 IP アドレスを特定できないこと，またそのようなスパムメール送信元 IP アドレスが 1 ヶ月以上ブラックリスト化されない事例を示している．文献 [5] は，悪性 IP アドレスが記載された複数のブラックリストを収集・調査することで，リスト間での重複は少なくリストごとにユニークな悪性 IP アドレスが多数存在することを明らかにしている．2019 年に文献 [6] は，公開と商用の IP ブラックリストを多数収集し，そのような IP ブラックリストに対する客観的な評価指標を提案し，その指標に基づき現状の IP ブラックリストはユーザや組織を守るという目的に対してはいまだに不十分であることを実証した．本研究は複数の悪性 IP アドレスまたは IP ブラックリストを起点としている点は上記の研究と共通するが，対象としている攻撃をスパムメールに限定せず現在の攻撃トレンドに追随している点，主な調査対象をクラウドサービス上の IP アドレスにして詳細に調査している点が大きく異なる．

IP アドレス変化：文献 [13] は，DNS レコードの参照先のリソース（例．ドメイン名や IP アドレス）がすでに利用されず無効化されているにも関わらず残存する DNS レコードを dangling DNS record (Dare) と定義し，そのセキュリティリスクをはじめて特定した研究である．特に Dare の参照先がクラウドサービス上の IP アドレスである場合，その IP アドレスが解放された後に第三者が取得可能であることを明らかにした．また，文献 [14] は，上記の文献 [13] と同様の問題を，Android アプリのアプリ内から参照されるドメイン名や IP アドレスに拡張して調査し，そのリスクを実証した研究である．文献 [15] は，サイバー攻撃の解析を IP アドレスを起点にして実施する際に，ISP から割り当てられる動的 IP アドレスやクラウドサービス上で割り当てられる IP アドレスの場合，同じ IP アドレスが常に同じユーザに割り当てられるわけではない問題があることに着目し，そのような変化しうる領域を PTR レコードの連続性から特定する手法を提案した．本研究は上記の研究で言及されているようなクラウド上の IP アドレスあるいは動的 IP アドレスの性質や所有者変更の実態を踏まえた上で，悪性 IP アドレスの変化を 45 種類のブラックリストを用いて解析し，継続的に掲載され続ける悪性 IP アドレスの特性やクラウドサービスならではの攻撃傾向をはじめて明らかにした．

7. おわりに

本研究では，多量かつ多様なブラックリストを用い，クラウドサービス悪用攻撃の実態についてはじめて大規模に調査した．本研究の調査結果は，クラウド事業者，ユーザ，さらにはブラックリスト事業者のそれぞれがクラウドサービス悪用攻撃に効果的に対処するための足がかりとなる．

謝辞　本研究の一部は，日本学術振興会における科研費（17K00135）の助成を受けている．ここに謝意を表す．

参考文献

[1] Canalys: Cloud infrastructure services spend up by US$7.2 billion in Q2 2019, driven by cloud migration, https://www.canalys.com/newsroom/cloud-market-share-Q2-2019.

[2] HOT FOR SECURITY: How any Instagram account could be hacked in less than 10 minutes, https://hotforsecurity.bitdefender.com/blog/how-any-instagram-account-could-be-hacked-in-less-than-10-minutes-21409.html.

[3] CYBERSGUARDS: Hackers abuse Microsoft Azure to use malware and evasion technology on C2 servers, https://cybersguards.com/hackers-abuse-microsoft-azure-to-use-malware-and-evasion-technology-on-c2-servers.

[4] Ramachandran, A., Feamster, N. and Vempala, S.: Filtering spam with behavioral blacklisting, *Proc. ACM CCS* (2007).

[5] Metcalf, L. and Spring, J. M.: Blacklist Ecosystem Analysis: Spanning Jan 2012 to Jun 2014, *Proc. ACM WISCS* (2015).

[6] Li, V. G. et al.: Reading the Tea leaves: A Comparative Analysis of Threat Intelligence, *Proc. USENIX Security* (2019).

[7] Amazon Web Services, Inc.: AWS IP Address Ranges, https://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html.

[8] Microsoft: [Deprecating] Microsoft Azure Datacenter IP Ranges, https://www.microsoft.com/en-hk/download/details.aspx?id=41653.

[9] Concurrency Labs: Save yourself a lot of pain (and money) by choosing your AWS Region wisely, https://www.concurrencylabs.com/blog/choose-your-aws-region-wisely/.

[10] azureprice.net: Average Price Per Azure Region, https://azureprice.net/Region.

[11] IPVoid: IPVoid, https://www.ipvoid.com/.

[12] Ramachandran, A. and Feamster, N.: Understanding the network-level behavior of spammers, *Proc. ACM SIGCOMM* (2006).

[13] Liu, D. et al.: All Your DNS Records Point to Us: Understanding the Security Threats of Dangling DNS Records, *Proc. ACM CCS* (2016).

[14] Pariwono, E. et al.: Don't throw me away: Threats Caused by the Abandoned Internet Resources Used by Android Apps, *Proc. ACM AsiaCCS* (2018).

[15] Nakamori, T. et al.: Detecting Dynamic IP Addresses and Cloud Blocks Using the Sequential Characteristics of PTR Records, *Journal of Information Processing* (2019).