

JPOPF-ST

インターネット番号資源 ホットトピックス

たにざきふみのり/JPOPF-ST

2019/11/27

この発表では…

- インターネットに関する話題のうち、主に番号資源とポリシーに関わるものやその周辺を話題として取り上げます。
- ポイントは…
 - (できるだけ)旬な話題
 - 一回お休みしたので、1年分です…
 - ちょっと違った切り口
 - 私見がたくさん
 - 短くお話しします

インターネット関連団体 人事情報(?)

松崎さん@IJJ



皆さんの協力とAPNICコミュニティのサポートを受けて、APNIC ECに当選しました。期待に応えられるように頑張ります！



午後4:10 · 2019年2月28日 · [Twitter for Android](#)

https://twitter.com/maz_zzz/status/1101016718644662272

前村さん@JPNIC

各位

2019年3月28日

一般社団法人日本ネットワークインフォメーションセンター(JPNIC)

前村昌紀がICANN理事会第10議席に再選

「2018～2019年 ICANN理事会第10議席選挙¹」において、JPNICインターネット推進部部長である前村昌紀が再選されました。2018年12月12日付アナウンス²の通り、JPNICは、ICANNアドレス支持組織(ASO)³による同議席の改選にあたり、ASOのアドレス評議会(AC)に対して前村を推薦しておりました。選挙の結果、2019年3月27日にASO ACは、同議席に前村を選出すると発表しました。

ICANN ASOによる選任アナウンス

<https://asao.icann.org/https://asao.icann.org/asao-ac-selects-akinori-maemura-to-serve-in-seat-10-of-the-icann-board-of-directors/>



これを受け前村は、2019年11月2日から7日までカナダ・モントリオールで開催される第66回ICANN会議の直後から、2022年の年次総会までの3年間、2期目となる同議席の理事を務めることになります。

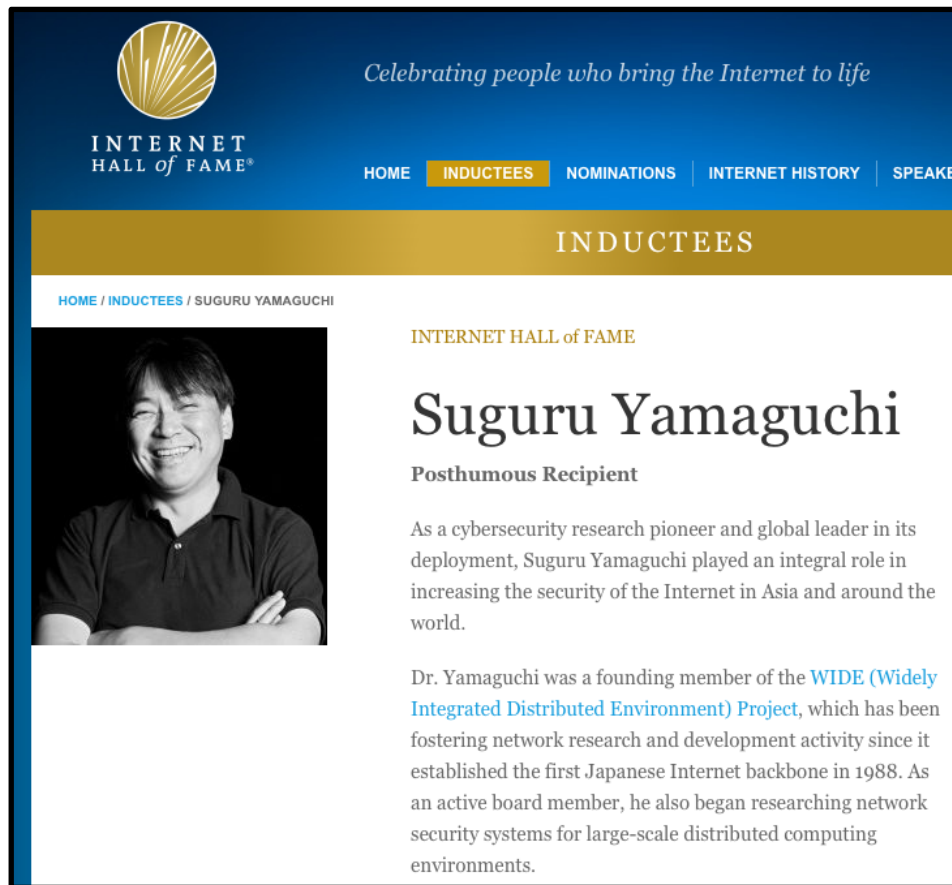
前村からのコメント

国内外問わずたくさんの皆さまに、ご声援、ご支援をいただいた結果、おかげさまで再選を果たすことができました。

2016年11月以来ICANN理事会に参画し、当初は手探りだった理事としての業務も、徐々に成果を積み上げることができるようになってきました。再選に向けた選挙にあたっては、旧知の友人との競合となりましたが、今一度私の能力と実績を見つ

<https://www.nic.ad.jp/ja/topics/2019/20190328-01.html>

山口英氏が「インターネットの殿堂」入り



The screenshot shows the Internet Hall of Fame website. The header is dark blue with a gold sunburst logo and the text "INTERNET HALL of FAME®". Below the header is a gold bar with the word "INDUCTEES". The main content area is white and features a black and white portrait of Suguru Yamaguchi. To the right of the portrait, the text reads "INTERNET HALL of FAME", "Suguru Yamaguchi", and "Posthumous Recipient". Below this, a paragraph describes him as a cybersecurity research pioneer. Further down, another paragraph mentions his role as a founding member of the WIDE (Widely Integrated Distributed Environment) Project.

Celebrating people who bring the Internet to life

INTERNET HALL of FAME®

HOME INDUCTEES NOMINATIONS INTERNET HISTORY SPEAKERS

INDUCTEES

HOME / INDUCTEES / SUGURU YAMAGUCHI

INTERNET HALL of FAME

Suguru Yamaguchi

Posthumous Recipient

As a cybersecurity research pioneer and global leader in its deployment, Suguru Yamaguchi played an integral role in increasing the security of the Internet in Asia and around the world.

Dr. Yamaguchi was a founding member of the [WIDE \(Widely Integrated Distributed Environment\) Project](#), which has been fostering network research and development activity since it established the first Japanese Internet backbone in 1988. As an active board member, he also began researching network security systems for large-scale distributed computing environments.

<https://www.internethalloffame.org/inductees/suguru-yamaguchi>

- The Internet Hall of Fame
 - インターネットの発展や進化に多大なる貢献をした個人を称えるバーチャルミュージアム
- 過去の日本の受賞者
 - 2012年：高橋徹氏
 - 2013年：石田晴久氏、村井純氏
 - 2014年：平原正樹氏
 - 2017年：後藤滋樹氏

紛争とサイバー攻撃 -1-

北大西洋条約機構(North Atlantic Treaty Organization)は、北大西洋条約に基づき、アメリカ合衆国を中心とした北アメリカ(=アメリカとカナダ)およびヨーロッパ諸国によって結成された軍事同盟である。(Wikipediaより)

Cyber defence

Last updated: 06 Sep. 2019 13:49

English | French | Russian | Ukrainian



Cyber threats to the security of the Alliance are frequent, complex, destructive and coercive. The Alliance must adapt to the evolving cyber threat landscape. It needs strong and resilient cyber defences to fulfil its collective defence, crisis management and communication. The Alliance needs to be prepared to defend its networks against the growing sophistication of the cyber threats it faces.

Highlights

- Cyber defence is part of NATO's core task of collective defence.
- NATO has affirmed that international law applies in cyberspace.
- NATO's main focus in cyber defence is to protect its own networks (including operations and missions) and enhance resilience across the Alliance.

In July 2016, Allies reaffirmed NATO's defensive mandate and recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea.

- Allies also made a Cyber Defence Pledge in July 2016 to enhance their cyber defence capabilities and ensure they can defend their

(超訳)サイバースペースは空中、陸上、海上と同様に、効果的に防衛しなければならない作戦領域である。

紛争とサイバー攻撃 -2-

 Israel Defense Forces
@IDF

CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work.


HamasCyberHQ.exe has been removed.

ツイートを翻訳



午前0:55 · 2019年5月6日 · Twitter Web Client

- ・ **イスラエル国防軍**はハマスからのサイバー攻撃に対して、サイバー防衛作戦を行い、この作戦が成功したのち、**ハマスのサイバー攻撃の拠点**を物理的に爆撃した。
- ・ サイバー攻撃に対して物理手段を用いたのは世界で初めて？

**海上自衛隊幹部学校**
JMSDF Command and Staff College

交通案内 | [リンク](#) | [サイトマップ](#) | English

HOME	ごあいさつ	幹部学校の紹介	教育課程	セミナー	留学制度
------	-------	---------	------	------	------

[HOME](#) / [戦略研究会](#) / [コラム](#) / コラム139

戦略研究会

- > 役員等紹介
- > トピックス
- > **コラム**
- > 「海幹部戦略研究」

サイバー攻撃にミサイルで応酬
—イスラエルのハマスのサイバー工作員攻撃を受けて—

(コラム139 2019/06/18)

イスラエル国防軍(The Israel Defense Forces :IDF)は、2019年5月4日土曜日、イスラエル保安局(Shin Bet)と第8200情報部隊の統合作戦によりハマスのサイバー工作員(cyber operatives)を爆撃したと発表した¹。IDFは、「サイバー防衛作戦の成功に続いて、未遂に終わったハマスのサイバー攻撃を阻止した。我々はハマスのサイバー工作員が活動するビルを標的とした」と

<https://www.mod.go.jp/msdf/navcol/SSG/topics-column/col-139.html>

<https://twitter.com/IDF/status/1125066395010699264>

紛争とサイバー攻撃 -3-

Trump approved cyber-strikes against Iranian computer database used to plan attacks on oil tankers



President Trump speaks to the media outside the White House. (Jim Lo Scalzo/EPA-EFE/REX/Shutterstock)

By **Ellen Nakashima**

https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html



TECHNOLOGY NEWS

私見)アメリカのサイバー攻撃に関する報道を見るに、今まであまり表面化しなかった紛争としてのサイバー攻撃が、**徐々に報道(表面化)される**ようになってきたように感じる。

Exclusive: U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack: officials

Idrees Ali, Phil Stewart

4 MIN READ



WASHINGTON (Reuters) - The United States carried out a secret cyber operation against Iran in the wake of the Sept. 14 attacks on Saudi Arabia's oil facilities, which Was

<https://uk.reuters.com/article/us-usa-iran-military-cyber-exclusive/exclusive-u-s-carried-out-secret-cyber-strike-on-iran-in-wake-of-saudi-oil-attack-officials-idUKKBN1WV0EK>

The RIPE NCC has run out of IPv4 Addresses

- RIPE NCCは2019/11/25に最後の/22の割り振りを行なった
- これにより**RIPE NCCのIPv4アドレス在庫は完全に枯渇した**
- 今後は**返却されたアドレスから新規事業者が/24を1回だけ割り振りを受けられる**
 - ただし『Waiting List』です！
- JPOPM36の『APNIC47・RIRレポート』でこのポリシーに関する議論を紹介しています
 - http://www.jpoppf.net/JPOPM36Program?action=AttachFile&do=view&target=7_RIPE78.pdf



RIPE NCC

RIPE NETWORK COORDINATION CENTRE

The RIPE NCC has run out of IPv4 Addresses

Today, at 15:35 (UTC+1) on 25 November 2019, we made our final /22 IPv4 allocation from the last remaining addresses in our available pool. We have now run out of IPv4 addresses.

Our announcement will not come as a surprise for network operators - IPv4 run-out has long been anticipated and planned for by the RIPE community. In fact, it is due to the community's responsible stewardship of these resources that we have been able to provide many thousands of new networks in our service region with /22 allocations after we reached our last /8 in 2012.

Recovered IPv4 Addresses and the Waiting List

Even though we have run out, we will continue to recover IPv4 addresses in the future. These will come from organisations that have gone out of business or are closed, or from networks that return addresses they no longer need. These addresses will be allocated to our members (LIRs) according to their position on a new waiting list that is now active.

<https://www.ripe.net/publications/news/about-ripe-ncc-and-ripe/the-ripe-ncc-has-run-out-of-ipv4-addresses>

IPv4アドレス売買詐欺事件 -1-

ARIN Wins Important Legal Case and Precedent Against Fraud

- Fraudulently obtained IP addresses uncovered and revoked -

Centreville, VA - May 13, 2019 - The [American Registry for Internet Numbers, Ltd. \(ARIN\)](https://www.arin.net/vault/about_us/media/releases/20190513.html) defeated an elaborate multi-year scheme to defraud the Internet community of approximately 735,000 IPv4 addresses, has successfully required the return of all the addresses, and stopped the defrauding party from continuing their scheme. The emergent IPv4 address transfer market and increasing demand have resulted in more attempts to fraudulently obtain IPv4 addresses from ARIN, the nonprofit member-based organization responsible for distributing Internet number resources in the US, Canada, and parts of the Caribbean.

https://www.arin.net/vault/about_us/media/releases/20190513.html



- サウスカロライナ州連邦検事局の連邦検察官は**ARIN**に対する詐欺で、**Amir Golestan**と**Micfo**を起訴したと発表
- Amir GolestanとMicfoは11のシェルフコーポレーションを利用し、ARINから約**757,760個のIPv4アドレス**を不正に取得した疑い
 - /13 + /15 + /16 + /17 + /20 = 757,752個

IPv4アドレス売買詐欺事件 -2-

詐欺に使用されたシェルフコーポレーション

	Company	Fabricated Individual
a.	Contina	John Lieberman
b.	Virtuzo	Jeff Farber / Mark Schmidt
c.	Oppobox	Kevin Chang
d.	Telentia	Yong Wook-Kwon
e.	Univera Network / HostAware	Steve Cunningham
f.	Roya Hosting	Brian Sherman
g.	Host Bang	Ahmad Al Bandi
h.	Hyper VPN	Sebatian Buszewski
i.	Fiber Galaxy	Pooya Torabi
j.	Cloudiac	Paul Lampert

8. In 2017 and 2018 GOLESTAN sold, and attempted to sell, IP addresses he had fraudulently obtained the rights to. Using a third party broker, GOLESTAN sold 65,536 IPv4 addresses for \$13.00 each, for a total of \$851,896.00. GOLESTAN also organized a second transaction for another 65,536 IP addresses, for another approximately \$1,000,000.00. During this same time period, GOLESTAN had a contract to sell 327,680 IP addresses at \$19.00 per address, for a total of \$6,225,910.00, with half of these addresses consisting of Channel Partner addresses obtained fraudulently. However, ARIN became aware of GOLESTAN's fraud at that time and was able to prevent the transaction from going through.

- 2017年から2018年にかけてGolestanはブローカーを利用しIPv4アドレスを販売
- 65536個を\$851,896で販売(1address=\$13)
- 65536個を\$1,000,000で販売(1address=\$15.26)
- 327,680個を\$6,225,910で販売(1address=\$19)
 - この取引はARINにより阻止された。

<https://www.courtlistener.com/docket/15619660/united-states-v-golestan/>

IPv4アドレス売買詐欺事件 -3-

不正に取得されたIPv4アドレスブロックの一部？)

2. IP Number Resources:

IP Block	Entity	Number of IP addresses
104.166.96.0/19	OppoBox	8,192
104.247.96.0/19	OppoBox	8,192
104.250.224.0/19	OppoBox	8,192
172.98.0.0/18	Telentia	16,384
174.136.192.0/18	Telentia	16,384
45.41.0.0/18	OppoBox	16,384
45.41.192.0/18	OppoBox	16,384
45.59.128.0/18	OppoBox	16,384
104.167.192.0/18	OppoBox	16,384
104.224.0.0/18	OppoBox	16,384
104.249.128.0/18	OppoBox	16,384
155.254.192.0/18	OppoBox	16,384
172.110.128.0/18	OppoBox	16,384
172.111.0.0/18	OppoBox	16,384
169.197.128.0/18	Border Technology	16,384
172.81.0.0/18	Border Technology	16,384

<https://www.courtlistener.com/docket/15619660/united-states-v-golestan/>

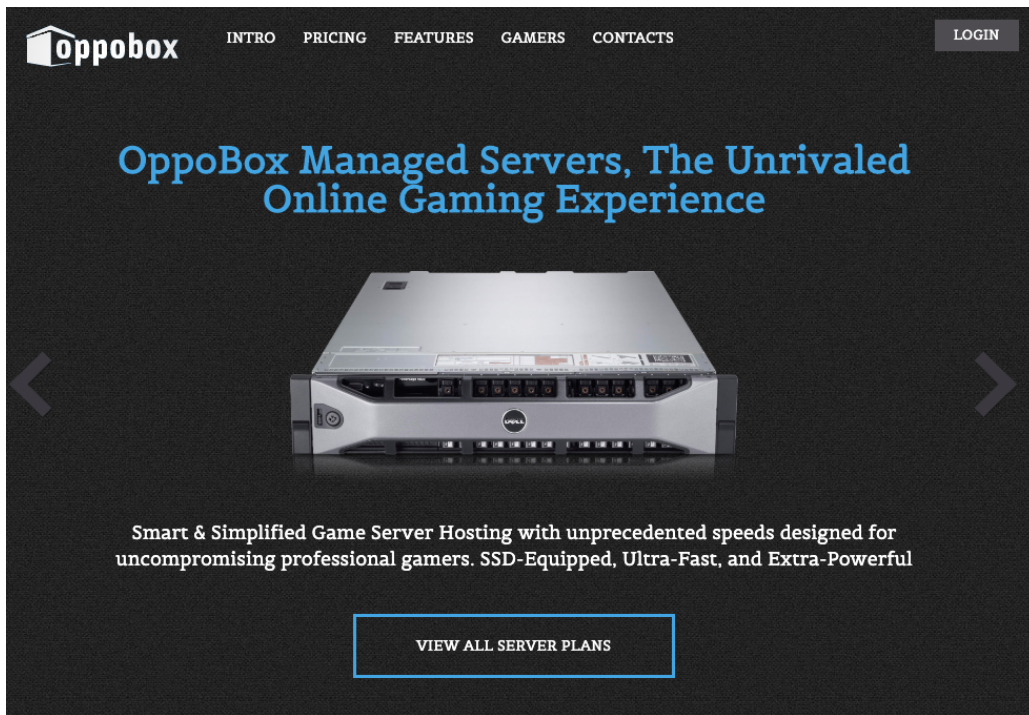
一部のアドレスがSPAMメールに使われたとの報道あり

<https://krebsonsecurity.com/2019/05/a-tough-week-for-ip-address-scammers/>

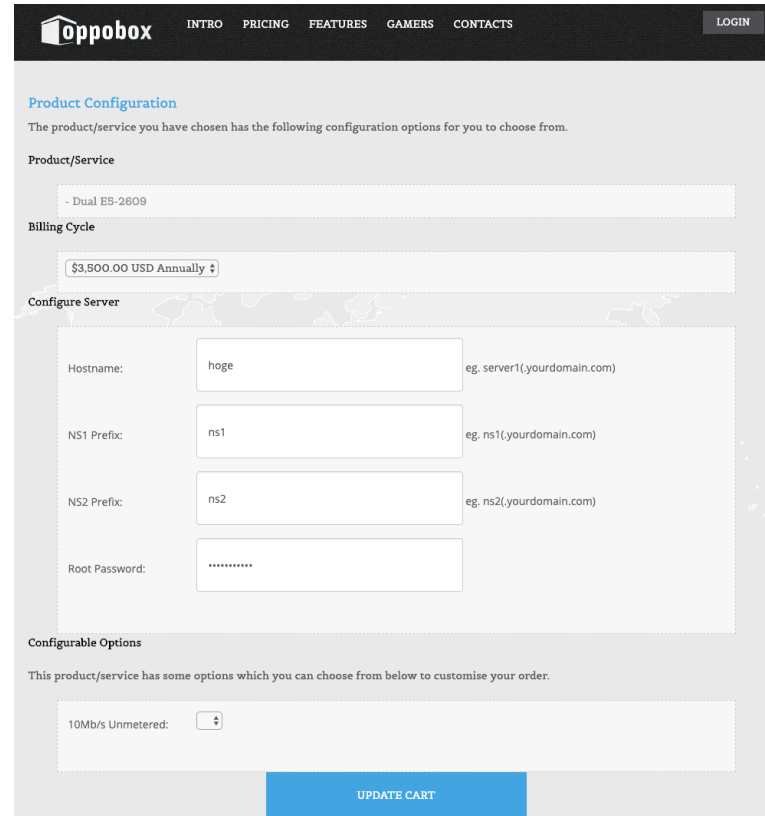
107.181.64.0/20	Contina	4,096
167.160.96.0/19	Contina	8,192
209.161.96.0/20	Telentia	4,096
104.128.16.0/20	Telentia	4,096
104.143.192.0/19	Telentia	8,192
104.222.192.0/19	Telentia	8,192
104.247.0.0/19	Telentia	8,192
107.190.160.0/20	OppoBox	4,096
107.182.112.0/20	OppoBox	4,096
104.207.64.0/19	OppoBox	8,192
155.254.96.0/19	OppoBox	8,192
167.88.96.0/20	Virtuzo	4,096
104.128.128.0/20	Virtuzo	4,096
104.156.192.0/19	Virtuzo	8,192
104.222.128.0/19	Virtuzo	8,192
104.143.16.0/20	Roya	4,096
104.237.80.0/20	Univera Network	4,096
45.62.32.0/19	Univera Network	8,192
45.61.32.0/20	Border Technology	4,096
173.44.0.0/19	Border Technology	8,192
172.97.80.0/20	Fiber Galaxy	4,096
206.223.224.0/19	Fiber Galaxy	8,192
172.102.128.0/20	Queen Systems	4,096
209.209.224.0/19	Queen Systems	8,192
172.110.208.0/20	Fairway Network	4,096
207.189.0.0/19	Fairway Network	8,192

IPv4アドレス売買詐欺事件 -4-

- oppobox(シェルフコーポレーション)にアクセスしてみた。



The landing page for Oppobox Managed Servers features a dark background with a central image of a server unit. The text 'Oppobox Managed Servers, The Unrivaled Online Gaming Experience' is prominently displayed in a light blue font. Below the server image, a tagline reads: 'Smart & Simplified Game Server Hosting with unprecedented speeds designed for uncompromising professional gamers. SSD-Equipped, Ultra-Fast, and Extra-Powerful'. At the bottom, a blue button labeled 'VIEW ALL SERVER PLANS' is visible. The navigation bar at the top includes links for INTRO, PRICING, FEATURES, GAMERS, and CONTACTS, along with a LOGIN button.

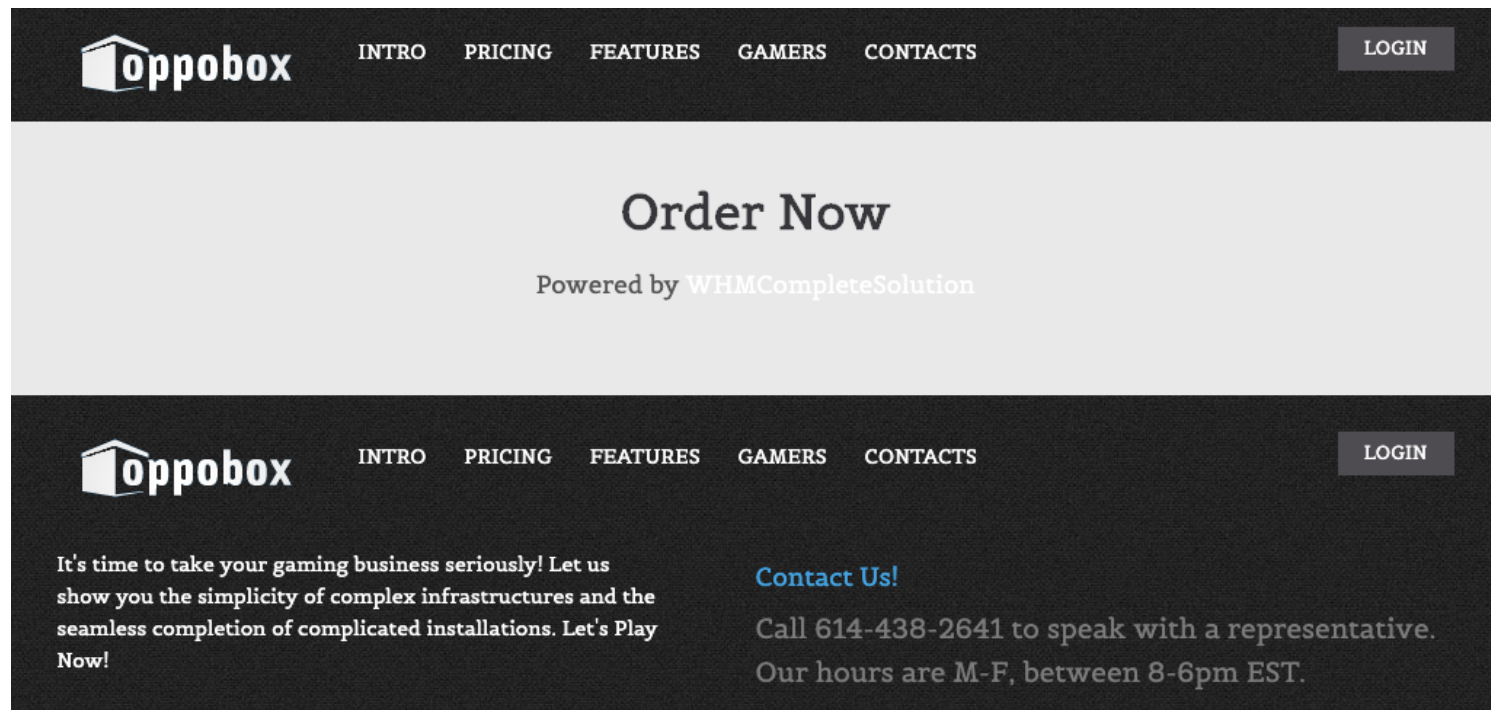


The Product Configuration page shows the options available for a selected product/service. The configuration options are as follows:

- Product/Service:** - Dual ES-2609
- Billing Cycle:** \$3,500.00 USD Annually
- Configure Server:**
 - Hostname:** hoge (eg. server1(yourdomain.com))
 - NS1 Prefix:** ns1 (eg. ns1(yourdomain.com))
 - NS2 Prefix:** ns2 (eg. ns2(yourdomain.com))
 - Root Password:** (masked with asterisks)
- Configurable Options:**
 - 10Mb/s Unmetered:** (dropdown menu)

An 'UPDATE CART' button is located at the bottom right of the configuration section.

IPv4アドレス売買詐欺事件 -5-



- オーダーされた？！

IPv4アドレス売買詐欺事件 -6-

• ARINの対応

What to Do If You Suspect Fraud

<https://teamarin.net/2019/05/13/taking-a-hard-line-on-fraud/>

ARIN works to protect the registration rights of its IP address holders and to prevent the fraudulent transfer of IP address space. Our staff actively investigates suspected cases of fraud. If you have reason to believe a certain block of Internet number resources may have been inappropriately obtained from ARIN or improperly transferred, please [submit a fraud report to us](#), and we will investigate it.

Submit a Fraud Report

Submit this form to report suspicion of fraudulently obtained Internet number resources from ARIN, or unauthorized modifications to existing ARIN records.

This form is NOT for reporting illegal or fraudulent Internet activity like network abuse, phishing, spam, identity theft, hacking, scams, or any other activity unrelated to the scope of ARIN's mission. Visit our Network Abuse page for more information on these activities.

You do not need to be logged in to submit a fraud report.

Contact Information and Attribution

Please provide complete contact information for internal ARIN staff purposes. If ARIN staff are unable to reach you, your fraud report may be considered invalid.

* denotes required field

*First Name:

<https://account.arin.net/public/fraud>

(超訳)

ARINはIPアドレス所有者の登録権を保護し、IPアドレススペースの不正な転送を防止します。スタッフは詐欺の疑いがあるケースを積極的に調査します。**IPアドレスがARINから不適切に取得、もしくは譲渡されたと思われる場合は報告してください。調査します。**

IPv4アドレス売買詐欺事件 -7-

- IPv4アドレス売買における**大規模な詐欺が現実になり、訴訟**になった。
- 詐欺側はとても巧妙に罠をしかけている。
- ARINはIPアドレス譲渡に関する不正行為に対して、毅然とした態度を取っている(ように見える)。
- **APNICでは？**

APNIC remains vigilant against fraud, but if you know of any resources that may have been obtained or used in breach of APNIC policies, please report it via the APNIC Helpdesk.

超訳) APNICは詐欺に対して警戒を続けています。APNICポリシーに違反して取得もしくは使用されているリソースを知っていたら、**APNICヘルプデスクに連絡**してください。



The screenshot shows the APNIC website header with navigation links: Get IP, Manage IP, Training, Events, Research, and Com. The main content area features a blue header with a magnifying glass icon over a warning triangle. The article title is "Taking a hard line on fraud" by Stephen Ryan on 22 May 2019, categorized under Community. Tags include ARIN, Fraud, Guest Post, and IPv4. The article text mentions ARIN's recent legal case against fraudulent acquisition of IPv4 addresses in the USA. A red arrow points from the Japanese text on the left to the APNIC Helpdesk link in the article. The URL at the bottom is https://blog.apnic.net/2019/05/22/taking-a-hard-line-on-fraud/.

APNIC

Get IP ▾ Manage IP ▾ Training ▾ Events ▾ Research ▾ Com ▾

Taking a hard line on fraud

By [Stephen Ryan](#) on 22 May 2019

Category: [Community](#)

Tags: [ARIN](#), [Fraud](#), [Guest Post](#), [IPv4](#)

[Like 0](#) [Share](#) [Twitter](#) [Facebook](#) [LinkedIn](#)

[← Blog home](#)

ARIN [recently announced](#) it had won a legal case against fraudulent acquisition of IPv4 addresses in the USA. The case is receiving significant attention in the media, and ARIN's Legal Counsel explains some of the background behind the case in the following post.

APNIC remains vigilant against fraud, but if you know of any resources that may have been obtained or used in breach of APNIC policies, please report it via the [APNIC Helpdesk](#).

<https://blog.apnic.net/2019/05/22/taking-a-hard-line-on-fraud/>