# めもおきば Tech Report

［めもおきば てっくれぽーと］
クラウドとセキュリティ、
TL 流速を支える
エンジニアの総合誌

December 2017 12

Hardening Day
Firming Day
Softening Day

## セキュリティ総合競技

# Hardening の衛り方

競技環境の
堅牢化を極めて
次回もセキュアな
回にしませんか

2017 年振り返り
2018 年予想

年末恒例の技術予想

# めもおきば TechReport 2017.12

## ― 目次 ―



Aki @ nekoruri

# Hardening 2017 Fes レポート

「衛る技術」を団体戦形式で競い合うセキュリティ・イベント「Hardening Project」の 11 回目、「Hardening 2017 Fes」に参加してきました。Hardening については、2015 年の「Hardening 10 ValueChain」を本誌 2015.12 でも取り上げていますので、合わせてご覧ください。

通常の Hardening は、実際の競技を行う「Hardening Day」と、振り返りプレゼンと攻撃チームからの解説、最終結果の表彰などを行う「Softening Day」の二日間で行われます。今回は「Fes」と銘打っている事もあり、全三日間の日程となり二日目に「Firming Day」が設けられました。募集段階では詳細は明かされず、「アンカンファレンス、ワークショップ、ラウンドテーブルなどの形」と公表されています。

会場もここ最近ずっと沖縄でしたが、今回は淡路島の淡路夢舞台国際会議場でした。いわゆる日本標準時（JST）の子午線が通る地域でもあります。

というわけで、我々「Team9 ¥>pin9」の闘いを、時系列で追っていきます。

## Day-0 競技前日

Hardening では、前日夜にはチームメンバーが集まって競技当日に向けた最終方針決定などを行うのが基本です。そもそも沖縄の場合には当日朝着が現実的に不可能であることから、ほぼ全員が参加します。

実はまずこの段階でつまずきまして、某 IPA の某研修プログラムの日程の都合によって、7 人中 4 人[1]が前日打ち合わせに参加できませんでした。正直ここでポプテピピックコラを貼りたい気持ちで一杯になりましたが、来られないものは仕方無いので来られる人だけで打ち合わせです。

前日打ち合わせのやり方もチーム毎におおきくことなりますが、私達は KDL さんに縁のある店で複数のチームが集まってお酒もそこそこに集まりました。途中でマーケットプレイスの方々も遊びに来たりしています。

より本気度の高いチームは、Airbnb で広めの家を借りてチームメンバー全員がそこに宿泊したりもしていたようです。正直その発想が無かったので、各々で高速バスの都合が良い三ノ宮などに宿を取りました。とにかく朝が早い（高速バスの場合は 7 時にはホテルを出ていないといけない）ので、高速バス乗り場から近いところが良いです。

ちなみに、接続用にポート数の多いラックマウントスイッチを持って行ったのですが、空港で見事に預け入れ荷物の重量制限に引っかかり、まさかの手持ち搭乗になりました。

---

[1] チームの人数は、今回は 6 人もしくは 7 人です。そして全 16 チーム 108 人。

## Day-1 Hardening Day

競技当日です。

チーム毎にあつまり参加費（メシ代）を支払って会場に入ります。会場にはネットワークケーブルが一本出てきている状態で用意されているので、持ち込んだスイッチ等で参加者の PC を接続していきます。私達のチームではありませんが、最近のノート PC はネットワークインターフェースを持っていないものが多く、持ち込んだ USB-NIC がうまく接続できないというチームもあったようです[2]。当初は 24 ポートのスイッチを使っていたのですが、今回のテーブル配置だと 8 ポートくらいの小さなスイッチを 2 箇所において近い方に接続する方が場所を取らず良かったようです。

まず競技内容の説明があり、それと並行してひっそりと 9 時間のカウントダウンもしれっと始まります。Hardening の場合は、このような競技説明にもヒントがあったりするため、接続確認を進めながらもきちんと耳を傾ける必要があります。

### 初動

さて、Hardening で重要とされる「初動」として、以下を迅速に進めます。

- 各サーバのログイン確認
- パスワード変更（一般ユーザ・管理者）
- 一般ユーザにログイン用 SSH 公開鍵を設定
- 各サーバの基本的なバックアップ
- マーケットプレイスの手配

パスワード変更や SSH 公開鍵の設定は、ある程度スクリプト化していたのですが、1 台混じっていた Ubuntu で上手く走らなかったりと若干の焦りもありつつも、ひとまずログインできるサーバについては実施しました。

バックアップについては、侵入を見越して対象と別のサーバ（踏み台 PC）への複製をしましたが、実は複製対象の確認が甘く、設定だけで Web コンテンツなどが取れていない状況でした。まさに「やるべきことをやりきることが重要」という Hardening の鉄則通り、バックアップ不備により、後のランサムウェアで痛い目に遭います。

その一方で、一般的な OpenSSH 環境でそのまま使える ProxyCommand 設定済み sshd_config をチーム内で共有して作業の迅速化を図ったりもしています。とにかくパスワードを打たないことが後々のキーロガー対策にもなるという予想から、基本的に全てこの段階から公開鍵認証でログインしてもらっています。後で

[2] それを見込んで、うちは念のため複数ベンダーの USB-NIC を持ち込んでいました。

他のチームのプレゼンを見て、このあたりのサーバ管理基本スキルについて事前訓練をやっておけば良かったなと感じます。

## 競技環境への誤解

これは思い返せばなんでこんな勘違いをしたのか判らないのですが、競技環境に接続したPCからはインターネットに出られないと思い込んでいました。そのため、事前に準備していたSlackやGoogle spreadsheetなどを活用できず、土壇場で用意した付箋紙ベースでのプロジェクト管理を強いられることになり、無駄に苦労することになりました。

いやこれほんとなんで勘違いしたのかいまだに謎です。

競技環境の対象サーバ群からはインターネットに出られませんが、接続しているPC自体はインターネットに出られたようです。

## 前任者による不正侵入

Hardeningで重要なことは「想像力」です。与えられた情報全てから、どんなストーリーで何が行われているのかを推測していく能力が求められます。それが一つ現れるのが退職者による不正侵入というインシデントです。

各サーバのプロセス状況の確認から、「ametani」というユーザがログインして色々悪さをしていることが判明しました。当然ながらametaniなんてユーザは知らないので、ひとまずアカウントへのログインをパスワード変更で停止しつつ、「親会社の社長」や「総務部門」に問い合わせます。

その結果、現役のリモート作業者ではなく退職者であることがわかり、そのままアカウント停止処分と相成りました。

## 外部業者によるコンテンツアップロード

この「ametani」氏インシデントと対称的なものが、外部業者からのコンテンツアップロードです。

あらかじめカバーストーリーとして、外部業者にイケてるデザインを発注しているのでそれが競技期間中に届く事が明示されていました。当然ながら、届いたデザインを組み込むことで売上＝スコアが上がるというわけです。そして競技環境にあるファイルサーバにあるテキストファイルをよく読むと、ウェブサーバの一般ユーザuser6でホームディレクトリにアップロードされる旨が書いてあります。

ここでおさらいですが、初動段階で一般ユーザのパスワードを一括で変更してしまっており、当然ながら外部業者がそのユーザでログインすることができなくなっています。「確認不足のまま現状を変更すると何かが起こる」というのはHardeningにおける王道パターンの一つで、見事にそれをぶち抜いた形です。

正しい対処としては、「別のリスクを許容しつつ、一般ユーザのパスワード自体は変更しない（そのかわり sudo 等を抑止）」もしくは「パスワードを変更して外部業者にその旨を連絡」の２パターンでしょうか。可能ならば後者が望ましいのは言うまでもないです。

ametani 氏の時は所属確認など注意深くできていたのに、かなり残念ポイント高いです。

## ウェブサーバのランサムウェア

見事にやられました。

本来ならばバックアップから書き戻せば良いはずが、コンテンツディレクトリのバックアップミスにより、痛恨の支払いが発生します。まさにこれは現実世界でも同じ事が言えます。取っているはずのバックアップ、ちゃんと必要なものを全て取れていますか？

またランサムウェア復旧サービス（いわゆる支払い）に泣き付くときもうっかりミスを重ね、10 万円の復旧サービス（今回は無関係）と、100 万円の復旧サービスの二つが用意されているのですが、100 万円の復旧サービスと明示されているにもかかわらず無駄に 10 万円の方を発注してしまいます。

会場には、攻撃側チーム Kuromame6 からのヒントを代弁する Google Home[3]が居たのですが、みごと Google Home から「10 万円なんかじゃ復旧できないよ」と煽られることになります。

復旧サービスに申し込むと、勝手に不正侵入して暗号化されたファイルを復号してくれるのも悔しい限りです。

## Windows マルウェア

定番として Windows 端末がマルウェアにやられます。というわけでエンドポイント製品、今回は Intel 製品を導入しました。見事に検知していただき、エンドポイント製品の重要性と威力を思い知りました。

複数サーバで連携してその経路などを追いかけてくれるのは流石ですね、かなり良いです。

## HTTPS 化

昨今の状況を顧み、カバーストーリーでも触れられていることから HTTPS 化が必須なので絶対やろうということに前日打ち合わせで決まっていたのですが、優先度判断が甘く最後の最後に回ってしまいました。おそらくこれによる売上低減が、中盤以降でスコアがまったく振るわなかった主要因の一つとみています。

HTTPS 化も、全て自前でやるという手法だけでなく、NEC InfoCage のような外部 Proxy 型の WAF であればそこに証明書を入れるだけで対応できたようです。正直マーケットプレイスに出ている製品の理解が

[3] これまでは Pepper でした。

まったく不足していたため、無駄に優先度を下げてしまったわけです。マーケットプレイスで購入を検討している製品は、どのような導入形態が取れるのか事前調査が勝利の鍵と思います。

## 壊れた Wordpress

コーポレートサイトでのリンク先が間違っているためアクセスが来ないという仕込みがあるのですが、この Wordpress の管理画面が壊れているため、まともにコンテンツが編集できないという問題がありました。

本当に Wordpress 自体が壊れているわけではなく、競技環境は本物のインターネットから隔離されているのですが、本物のインターネット上の Google CDN から取ってくる JS に依存するなど、このあたりを早めの時間帯で切り分けて対策できていれば良かったと思います。また、いっそ API での編集など別の手段を確保するという手もありかも知れません。

## 情報漏えい事故

Web コンテンツのディレクトリに、DB のバックアップなどがぽろっと置かれているという情報漏えい事故が仕込まれています。

Web コンテンツのチェック、初動での確認事項に入れたい項目の一つです。

また、今回は各チームが「子会社」という体になっていますが、その時点でスコアの高い一部チームに対して情報漏えいインシデントに対する「親会社からのお呼び出し」が掛かります。別の個室で行われる状況がメイン会場にも映し出され、まだ呼ばれていないチームは戦々恐々としていました。

## ルータへのログイン手段

競技ネットワークで 2 台用意されているルータ（これも競技対象の中）へは、踏み台として用意された PC から SSH でログインするように設定されていますが、ここもまたシナリオへの想像力が求められました。

基本的に user1 という一般ユーザを利用して作業をしていますが、ルータ 1 へは素直にファイルサーバ上の用意されている PuTTY とその秘密鍵を利用して user1 にログインができます。判りづらかったのがルータ 2 へのログインで、やはりファイルサーバ上に用意された別の秘密鍵を利用しますが、ログインできるのは user2 だったりします。こういう罠がたくさん用意された競技環境、とても楽しいです(白目)。

## 競技終盤

まあ終盤になってくるとだいぶ焦りが溜まってくるわけですが、細かい対応不足が重なってスコアが伸びず、よりさらなる焦りを呼びます。

仕掛かり作業をやりきろうと言うことで、HTTPS 化などに今更のように手を付けたのもこのあたりだったりします。当然ながら、そんなスピード感だと現実では Google chrome に怒られてしまうわけですね。

### 競技終了

9時間の競技を終え、レセプションホールでの立食パーティタイムです。

ここで運営側から競技時間の追加が告知され、「明日はまたゼロから」「引き継ぎをいかに詳細にするか」というキーワードが出ます。他チームとのスワップ辺りかなあと予想しつつ初日終了です。

## Day-2 Firming Day

問題の2日目「Firming Day」です。

競技時間の追加は、「人事異動」として「リーダー以外が隣のチームに異動」することが発表されます。つまり、リーダー一人だけを残して別のチームの人が自分たちの環境を見ることになります。まさに引き継ぎ力が重要という通りです。

延長競技時間は2時間、私達はリーダーを残して隣のチーム「Team10 天一」に移って引き継ぎを受けました。どうも引き継ぎ資料が不十分で、パスワードが分からないなんてチームもあったようです。隣のチームは、競技環境にsplunkを導入してログ分析をやっていたりと、色々各チームの特色が見えて価値の大きい2時間でした。

ちなみに、この日のランチがカレーでしたが、本当に美味しかったです。

## Day-3 Softening Day

Softening Dayでは、まず各チームがそれぞれの取り組みをプレゼンします。

特徴的だと思った取り組みをいくつか紹介します。

### 原価率などの戦略

仕入れ原価などを差し引いた売上額がスコアと言うことで、競技環境のECサイトに並んでいる商品の原価率などに売上戦略に注目したチームが複数有りました。特に高額商品の「アナゴ」をたくさん売ったチームはスコアが高かったようです。なかには、新しい商品としてネギを新規に売り出したチームもありましたが、惜しくも「お客さん」には刺さらなかった模様です。

その一方で、「32億円の誤発注」という伝説的なやらかしがあったチームもありましたが、それをきっかけにチームの雰囲気が良くなり笑いの絶えない職場になったりと、なにが幸いするか判りません。

### 社歌

メール担当者が、出すメールのフッタに社歌を入れていたチームがありました。

この社歌は、翌月に東京で行われた振り返り会にて無事披露されました。

### ツール

各チームいろいろ試行錯誤が見えましたが、タスク管理はTrello良さそうという感じです。

BacklogやGitHub issuesというチームもありました。

### 事前訓練

先ほど少し触れましたが、競技環境を模したサーバ群を用意して、基本的な作業や初動対応などを訓練したチームが複数有りました。

確かにHardeningの競技環境は「踏み台」の存在など癖のある部分も少なくなく、これは必ずやっておいた方が良さそうです。

### Kuromamoe6からの解説と表彰

各チームからのプレゼンの後、攻撃チームとしてKuromamoe6からの答え合わせの時間です。

そして、最終スコアの発表と表彰が行われます。私達Team9は辛うじて最下位ではない15位でしたが、得るものは多かったので実質優勝です。

### 動画公開

そして、ここまで全てYouTubeにて動画が公開されています。是非みましょう。

⇒ https://www.youtube.com/watch?v=me4rM9OVtNg

## Day-4

Day-3を夜までゆっくり楽しみたかったので後泊しています。

この日は、Hardeningの疲れを癒すべく有馬温泉に寄って帰りました。

## 今後に向けて

最近すっかりサーバーレス屋と化して、サーバの運用をあまりやっていない状況だったのですが、改めてサービス運用・サーバ運用の勘所を復習する良い機会になりました。

今後またHardeningに向けてやっておいた方がいいなーと思ったことをちらほら並べます。

- 事前訓練で競技環境の癖に慣れる
- バックアップなど、現実だったらやっていることをきっちり意志決定
- 前日打ち合わせは全員参加、場合によっては宿泊もAirbnbで一緒にする
- きっちりタスク管理、優先度判断
- 素人なりにでも良いから最低限の脆弱性診断
- splunk等によるログの一括管理
- コンテンツの全チェック
- ビジネスの利益率向上施策についての議論
- なんだかんだで世の中Wordpressなので WP力を付ける

これらは、Hardeningだけでなく、実世界でのサービス運用に通じるのは言うまでも無いです。

最後にあらためて、Hardening Projectという企画を動かしている全ての人達に感謝します。

# 2017年振り返りと2018年予想

今年個人的に心に残ったテーマと、来年盛り上がりそうなテーマをつらつら書きます。

## 「2017年予想」の振り返り

昨年「TechReport 2016.12」での2017年予想をふりかえってみます。

1. 「サーバーレスアーキテクチャ」の躍進
   黎明期から流行期にシフトしつつあり、間違いなく普及が進んでいます。
   具体的なテスト手法やCIなど開発に関する事例も増えてきています。「一つのシステムをDSLで定義し、そこに含まれる複数のFaaSを一括管理」という予想は、2016年末のAWS Step Functionsに続いてAzure Durable FunctionsやIBM Composerなど様々な形で登場しました。
   フルマネージドなコンポーネントについても、AzureのDocumentDBあらためCosmosDBや、AWSのAmazon Aurora Serverlessなど、データストアを中心にサービス側の拡充が進んでいます。
2. コグニティブとBot
   この分野では、抽選枠を取り合っているAmazon Echoや、半額セールで話題になったGoogle Homeなどのスマートスピーカー分野が一気に注目を浴びたことで、その背後にある技術領域として普及の芽が出ています。私自身もAmazon EchoとGoogle Home mini両方試していていますが、「ちょっとした便利」の積み重ねがなかなか良いです。
3. IoTとセキュリティ
   各クラウドベンダからIoT機器やIoTゲートウェイに対するデバイス管理SDKが登場したり、IoTデバイスに対してリーチャビリティとセットで識別/認証機能を提供するSORACOMがKDDIに買収されるなど、IoTとセキュリティにまつわる戦場は隣接領域を巻き込みながら拡がっています。
   なかでも「できる人が居たから」感もありますが、AWSがRTOSベースのディストリビューションまで踏み込んだのは面白い動きだと思います。
4. 新たなる「ラストワンマイル」競争
   SORACOMがKDDIに買収されたほかは、特に大きな動きはなかった分野でした。とはいいつつ、5Gフィールドトライアルなど、地道に研究開発が進んでいる分野です。SORACOMのSigfox対応や、LoRaWANによる「全国サービス」を展開しようとするセンスウェイなど、普及期に向けた動きは見えつつあります。
5. エッジコンピューティング
   AWS GreengrasやAzure IoT Edge SDKなど環境は揃ってきています。PoCレベルの事例は増えてきているため、来年持ち越しという感じでしょうか。
6. FinTech
   まさかここまで仮想通貨が盛り上がるというかバブルになるとは思っていなかったのが正直なとこ

ろです。その一方で、本丸である金融機関のAPI化は、規格化など地道に進んでいますがまだまだ道半ばといったところでしょうか。

7. ユーザーインターフェースの拡張
   淡々とVRがコンテンツを増やす一年でした。やはりエロは大事ですね。年末にはVR男優の特殊技能に関する記事が注目を集めました。
   ウェアラブル分野では、Apple Watch 3がついに単独でセルラー通信に対応したのが一番大きな動きです。この裏には組み込み型のeSIMなど様々な技術革新が存在しています。eSIMはいいぞ。
8. Dockerのコモディティ化
   世の中全てDockerどころか、そのオーケストレーションもKubernetesでまとまりつつあります。
9. セキュリティ教育
   私自身もSecHack365で関わっているNICT（情報通信研究機構）のナショナルサイバートレーニングセンターの発足など、国を挙げてのセキュリティ人材育成が進んでいます。
10. おまけ
    3月に無事本編完結した「本好きの下剋上」、なんと『このライトノベルがすごい！2018』単行本部門で1位でした。

## ボイスUI（VUI）の躍進

OSに紐付きであったApple SiriやWindowsのCortanaから時計の針が一つ進み、Amazon EchoやGoogle Home、LINE Clovaなどスマートスピーカーとしてのデバイスが登場しました。2016年ぐらいから拡充が進んでいたコグニティブ分野の成長との相乗効果もあり、ボイスUIが一気に花開きつつあります。

すでにプログラマブルになっていると言うこともあり、来年はその活用が進むと思いますが、その中でも「日常のちょっとした便利さの積み重ね」というのは潜在的な大きな魅力を秘めています。このようなデバイスで一番重要なことは「気づいたときには無いと困る状況」をいかに作り出すかですが、例えば料理中の音声メモなど、スマートスピーカーはそういった領域が得意に見えます。

ボイスチャットなどからスマートホームなどのボイスUIに「侵入」するという課題も明らかとなっていますが、これには「音声による識別」がまだまだ不十分という背景があります。風邪を引いて声が変わるなど、他の生体識別技術と比べても難しい技術分野ではありますが、重要な操作にはスマートフォンとの2FAを要求するなどのリスクベースの判断など、そういったセキュリティ上の考慮事項に関するガイドライン化が進むのでは無いかと考えています。

ボイスUIに引っ張られる形で、いわゆるIoT家電として少しずつ製品が増えているスマートライトなどに注目が当たっているのもなかなか面白いところです。この辺は、2018年から既存のIoT家電スタートアップの買収劇が大いに進んでいくものと見ています。

## PKI の抱える課題が顕在化

由緒正しい Verisign の流れを汲んでいた Symantec が、そのサーバ証明書事業を DigiCert に売却することになりました（2017 年 10 月に買収完了）。これはブラウザベンダーとしての Google と Symantec との争いが背景となっています。

Google は、以前より Certificate Transparency（CT）という枠組みを構築し全てのサーバ証明書に対して CT への対応を求めています。CT は証明書の誤発行や偽造を防ぐために、CA が証明書を発行するときに同時に CT にそれを登録する監査の仕組みで、RFC6962 としても標準化もされています。ブラウザは、HTTPS 等で通信するときに CT の監査ログを確認することで正しい証明書であることを確認します。この仕組みは、例えば Google Chrome であれば 2015 年 1 月より段階的に導入され、2016 年 6 月のリリースからは CT に登録されていない証明書で警告が表示されるようになっています。

ここには二つの課題があります。一つは、あの Verisign を買収した Symantec ですらも、Google の求める基準を達成することができていないということです。常時 TLS 化が進んだ結果、利用そのものが増えていることもその背景にあるかとは思います。

もう一つは、証明書という PKI の根幹に対して、ブラウザベンダーにすぎない Google の「力」が巨大になっているということです。DNS の信頼性が揺らぎ、証明書に通信の安全性を依存している現状において、証明書の偽造リスクは決して無視できず Google の圧力にも理はあります。その一方で、Symantec に対する「サーバ証明書の信頼を無効化」という強すぎるカードなど、PKI そのものに対する Google の支配力が高まっているのも事実です。綺麗な王様であるうちは良いのかも知れませんが、インターネットの信頼モデルの根幹を Google に握られつつある、という現状は知られるべきでしょう。

その一方で、Let's Encrypt やクラウドベンダによる無料証明書によって、とにかく DV（ドメイン認証）でよければ手軽に（たとえ悪意を持つものであっても）HTTPS による暗号化ができるようになった現状は、マルウェアの被害拡大なども経て 2018 年以後より議論が深まっていくことでしょう。

## Windows Subsystem for Linus

WSL は良いぞ。

Linux（Ubuntu）の amd64 バイナリがそのまま動く WSL は、まずは開発者向けリリースとして提供されている段階ですが、大きな可能性を持っています。実際に試した人はご存知だと思いますが、ターミナルが（昔に比べれば雲泥の差で頑張っているとはいえ）ショボい事を除けば、一般的なユーザアプリケーションはそのまま動くようになってきています。ターミナルも、代替のものが OSS でリリースされています。

Windows の世界観との繋ぎ込みはまだまだ道半ばですが、UNIX というか Linux っぽい作業環境のために Mac を使っているような人は一度試して見ると良いかも知れません[4]。とくにビルド環境としては Ubuntu/amd64 のバイナリを、クロスコンパイルではなく普通に作って動かす事ができます。是非はともかく、世の中大半の環境で Linux がポータブルなバイナリになりつつある現状ではかなり大きなメリットです。

2018 年にもおそらく 2 回の大きなアップデートが Windows に来ると思われますが、Linux 開発環境としての進歩が楽しみなところです。

## GPU コンピューティング

いままさに NVIDIA の EULA 変更による議論が真っ盛りですが、それはさておき、2017 年から 2018 年にかけて GPU がより一般化が一段階進むタイミングと見ています。特に根拠はありませんが、おそらく向こう 2 年くらい続くであろう機械学習のカジュアル化の波に乗って、GPU コンピューティングでモノが書ける人が増加し、それを活用した事例が出てくるような気がしています。

最終的にはクラウドベンダによりサービスに消化された機能を利用するようになっていくでしょうが、そうなってもやはり「中身を知っていることは強い」ので、そういった技術者の取り合いが過熱していくことでしょう。

また、末端でのデータ集約などのエッジコンピューティングの領域でも利用が広まり、AWS や Azure が提供しているエッジ側の FaaS と相まって、一つの技術領域として確立していくのではと予想しています。

## NGN の課題と IPv6 の普及？

現状の NGN における PPPoE 収容先の限界によって IPv6 IPoE 接続が急速に知られる[5]ようになるなんて理由で IPv6 の普及が進むなんてことになるとは正直思っていませんでした。

様々な歴史的経緯によってたまたま既存の IPv4 の通信が遅くなっているだけの話なのですが、既に PPPoE 収容方式の改善案などは見えてきているため、2018 年にはある程度改善されるのでは無いかと考えられます。

---

[4] もちろん、OS 自体との統合としてみるとまだまだ比較になりませんが。

[5] 一方で PPPoE を張り直して軽い収容先までリセマラする「NTE ガチャ」も行われている模様。

## 量子コンピュータ

IBM Q に続いて Azure などから使えるおもちゃが出てきたので、来年は「触ってみた」系の記事がたくさん出てくるものと思います。というか正直この本で扱う予定だったのですが落としました。

# あとがき

もう当日５時です！時間ないです！あとがき省略です！ごめんなさい！

」


めもおきば TechReport 2017.12

発行日　2017年12月29日　初版 コミックマーケット93

著者　Aki @nekoruri
aki@nekoruri.jp

発行　めもおきば
http://d.nekoruri.jp/

印刷　キンコーズ