



AWS
Black Belt
Online Seminar

【AWS Black Belt Online Seminar】

AWS IoTにおけるデバイス管理

アマゾン ウェブ サービス ジャパン株式会社
ソリューションアーキテクト 小梁川 貴史
2018/03/27

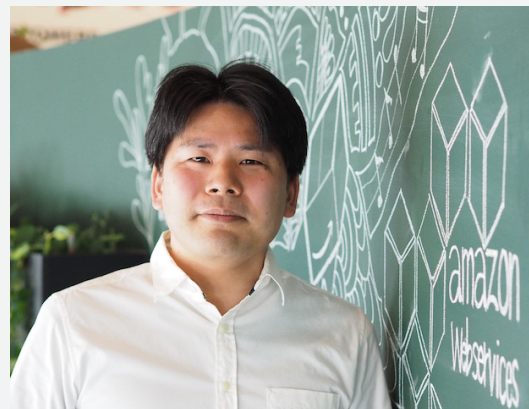
自己紹介

名前

小梁川 貴史 (こやながわ たかし)

所属

技術統括本部 IoT/AI ソリューションビルダー
ソリューション アーキテクト



前職

電機メーカー自社サービスの開発・運用
元AWSユーザ

好きなAWSサービス

AWS IoT , AWS Lambda(python), Amazon Kinesis

AWS Black Belt Online Seminar とは

AWSJのTechメンバがAWSに関する様々な事を紹介するオンラインセミナーです

【火曜 12:00~13:00】

主にAWSのソリューションや業界カットでの使いどころなどを紹介
(例 : IoT,金融業界向け etc.)

【水曜 18:00~19:00】

主にAWSサービスの紹介やアップデートの解説
(例 : EC2, RDS, Lambda etc.)

※開催曜日と時間帯は変更となる場合がございます。最新の情報は下記をご確認下さい。
オンラインセミナーのスケジュール&申し込みサイト

<https://aws.amazon.com/jp/about-aws/events/webinars/>

内容についての注意点

- 本資料では2018年03月27日時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(<http://aws.amazon.com>)にてご確認ください
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます
- 価格は税抜表記となっております。日本居住者のお客様が東京リージョンを使用する場合、別途消費税をご請求させていただきます

AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at <http://aws.amazon.com/agreement/>. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

はじめに

IoTの特性として、小さなPoC=数点のデバイスからstartし、大量のデバイスを管理することがワークロード上に発生することがある。また、接続情報やセキュリティ情報を埋め込んだ“機器”を配置/管理することが発生します
また機器が配置される場所は、ITの現場とは遠い生産現場やお客様の手元にあるものということもあります

本セッションにおいて、AWSにおけるIoTデバイスのセキュア/効率的な管理方法などについて説明します

アジェンダ

- デバイスのセキュリティの考え方
- 大量デバイスの管理
- まとめ

デバイスのセキュリティの考え方

AWS IoTとその他AWSサービスでの管理/セキュリティの違い

- IAM/Roleを使ってデバイスを管理？
セキュリティクレデンシャルベースでの認証
上限数の問題。PoCは良くても大量デバイスの管理で厳しい
- Cognitoを使う？
Gateway/Edgeサーバ/sensorなど、画面の問題や定期的な認証など事実上不可能。(B2Cの製品については対応可能な事もある)
- AWS IoT Thingとして扱う(=証明書、Policy)

AWS IoT の制限

モノの制限

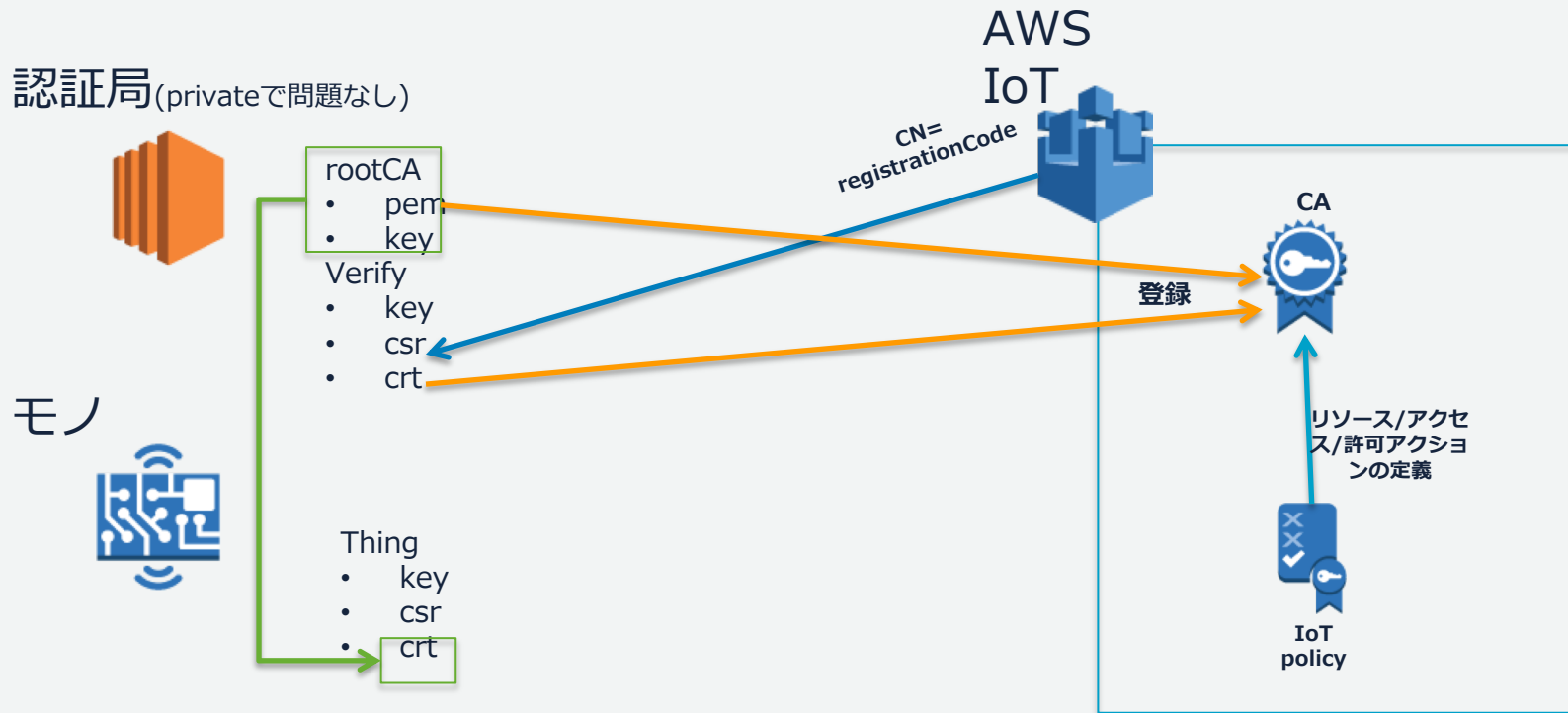
リソース	制限
モノ名のサイズ	UTF-8 エンコード文字で 128 バイト。この制限は Thing Registry および Thing Shadows サービスの両方に適用されます。
モノのタイプがあるモノのモノ属性の最大数	50
モノのタイプがないモノのモノ属性の最大数	3
モノを関連付けることのできるモノのタイプの数	1
AWS アカウントのモノのタイプの最大数	無制限

AWS IoTの証明書

- AWS IoT機能での証明書作成
- 自前認証局(持ち込みCA)からの証明書作成

https://docs.aws.amazon.com/ja_jp/iot/latest/developerguide/device-certs-your-own.html#create-device-cert

持ち込みCAセキュリティチェーン概念図



Just in time registration

認証局で作成したデバイス証明書を元に、初回通信時に、AWS IoTが証明書を有効化/Policyの関連付けが出来る機能。

※証明書の有効化、Policyの関連付けが完了するまでは通信がrejectされる点に注意

Just in timeの証明発行処理：概要

CERT-ID単位でのtopicになる
ので、種別などでpolicyを分
けたい場合はCAを複数使う
ことで対応可能

未認可な証明証のアクセスは暗黙的に
\$aws/events/certificates/registered/<CERT-ID>
のtopicにイベント通知される



publish (or subscribe)
Thing.crt+CAroot.pem
Thing.key
Root.pem(Verisign)



IoT
rule



証明書/AWS IoT policyのactivate処理

```
{  
  "certificateId": "",  
  "caCertificateId": "",  
  "timestamp": "",  
  "certificateStatus": "PENDING_ACTIVATION",  
  "awsAccountId": "",  
  "certificateRegistrationTimestamp": ""  
}
```

証明書のactivate/
policy処理が完了するまでは
errorとなることをに注意

Just in time registration のサンプルコード

```
8 var AWS = require('aws-sdk');
9
10 exports.handler = function(event, context, callback) {
11
12     //Replace it with the AWS region the lambda will be running in
13     var region = "us-east-1";
14
15     var accountId = event.awsAccountId.toString().trim();
16
17     var iot = new AWS.Iot({'region': region, apiVersion: '2015-05-28'});
18     var certificateId = event.certificateId.toString().trim();
19
20     //Replace it with your desired topic prefix
21     var topicName = `foo/bar/${certificateId}`;
22
23     var certificateARN = `arn:aws:iot:${region}:${accountId}:cert/${certificateId}`;
24     var policyName = `Policy_${certificateId}`;
25
26     //Policy that allows connect, publish, subscribe and receive
```

Policy template

```
27 var policy = {
28     "Version": "2012-10-17",
29     "Statement": [
30         {
31             "Effect": "Allow",
32             "Action": [
33                 "iot:Connect"
34             ],
35             "Resource": `arn:aws:iot:${region}:${accountId}:client/${certificateId}`
36         },
37         {
38             "Effect": "Allow",
39             "Action": [
40                 "iot:Publish",
41                 "iot:Receive"
42             ],
43             "Resource": `arn:aws:iot:${region}:${accountId}:topic/${topicName}`
44         },
45         {
46             "Effect": "Allow",
47             "Action": [
48                 "iot:Subscribe",
49             ],
50             "Resource": `arn:aws:iot:${region}:${accountId}:topicfilter/${topicName}/#`
51         }
52     ]
53 };
```

Create Policy

```
55 /*
56 Step 1) Create a policy
57 */
58 iot.createPolicy({
59     policyDocument: JSON.stringify(policy),
60     policyName: policyName
61 }, (err, data) => {
62     //Ignore if the policy already exists
63     if (err && (err.code || err.code !== 'ResourceAlreadyExistsException')) {
64         console.log(err);
65         callback(err, data);
66         return;
67     }
68     console.log(data);
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
```

attach Policy

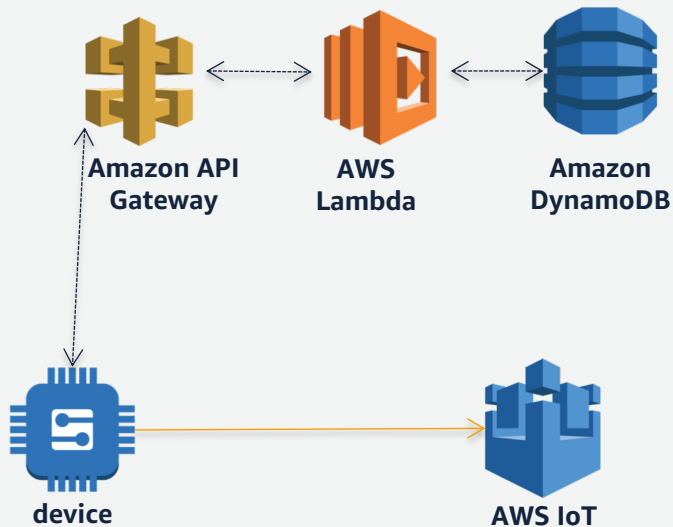
```
73 iot.attachPrincipalPolicy({
74     policyName: policyName,
75     principal: certificateARN
76 }, (err, data) => {
77     //Ignore if the policy is already attached
78     if (err && (err.code || err.code !== 'ResourceAlreadyExistsException')) {
79         console.log(err);
80         callback(err, data);
81         return;
82     }
83     console.log(data);
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
```

証明書activate

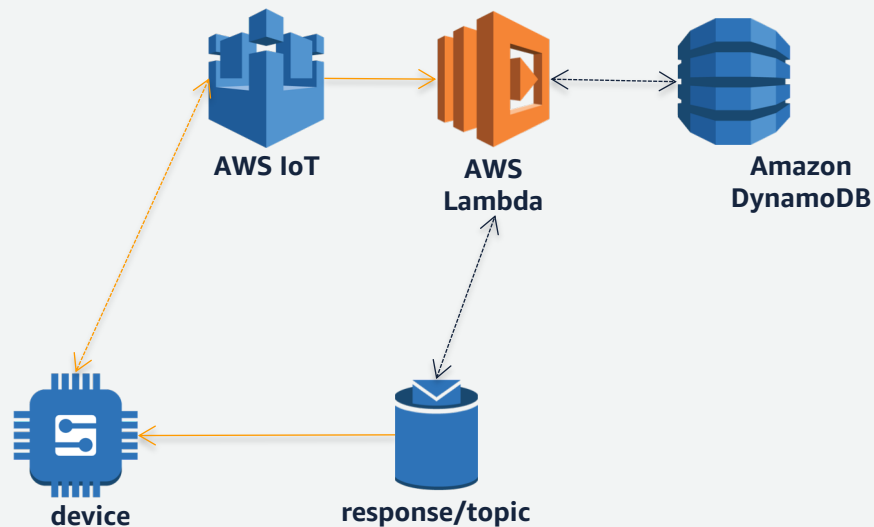
```
88 iot.updateCertificate({
89     certificateId: certificateId,
90     newStatus: 'ACTIVE'
91 }, (err, data) => {
92     if (err) {
93         console.log(err, err.stack);
94         callback(err, data);
95     }
96     else {
97         console.log(data);
98         callback(null, Success, created, attached policy and activated the certificate - certificateId);
99     }
100 });
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
```

Bootstrapping:

個別証明書の発行が難しい場合のアーキテクチャ
HTTP / MQTTで初回起動時に個別証明書を発行



初回ユーザ登録など合わせてHTTP request
で証明書を生成して返却する



プリンする証明書のpolicyは初期化用の
mqtt topicのみが実行できるようにする

証明発行のパターンのまとめ

1. AWS IoTによる証明書発行

- AWS IoTの権限、APIが発行できる環境が必要、事前に証明書、関連policy紐付けを完了させる

2. 持ち込みCAによる証明書発行

- 発行の流れは1)と同じ、自分たちで証明書を生成出来るので証明書の期限がコントロール出来る点が1と比較したメリット

3. Just in time registration

- デバイス証明書をoff line/AWSの操作権限なしで作成できる。事前にpolicy、証明書のアクティベートなどをしなくてもよく、自前認証局でdevice証明書を発行だけすれば良い

4. Bootstrapping

- 生産現場とCloudでどうしても連携が難しい場合の手段

使い分けの例

1) AWS IoTの発行証明書、2) 自前認証局で証明書発行するケース

- 生産ラインですでにserial-IDを入れるなど機器毎の個別処理を持っている、secure ラインがあるケースで検討されることが多い
- 証明書の発行はクラウドの操作権限がある人

3) Just in time registrationを利用するケース

- 生産に関わる機器をinternetに繋げない、外部システムとの連携が難しい場合で、イントラ内のマシンに認証局を建てられるケースで検討される
- AWS IoTへCAの登録が完了していれば、工場内で証明書を生産可能

4) Bootstrappingを利用するケース

- クラウド側とデバイス生産で連携が難しく、クラウド側のみでクラウドのセキュリティの検討が必要なケースで検討されることが多い

**証明書がより便利になり、
証明書を元に他のAWSサービスへの一時権限の取得が可能に**

テナラリトークン取得パターン

対象シーン

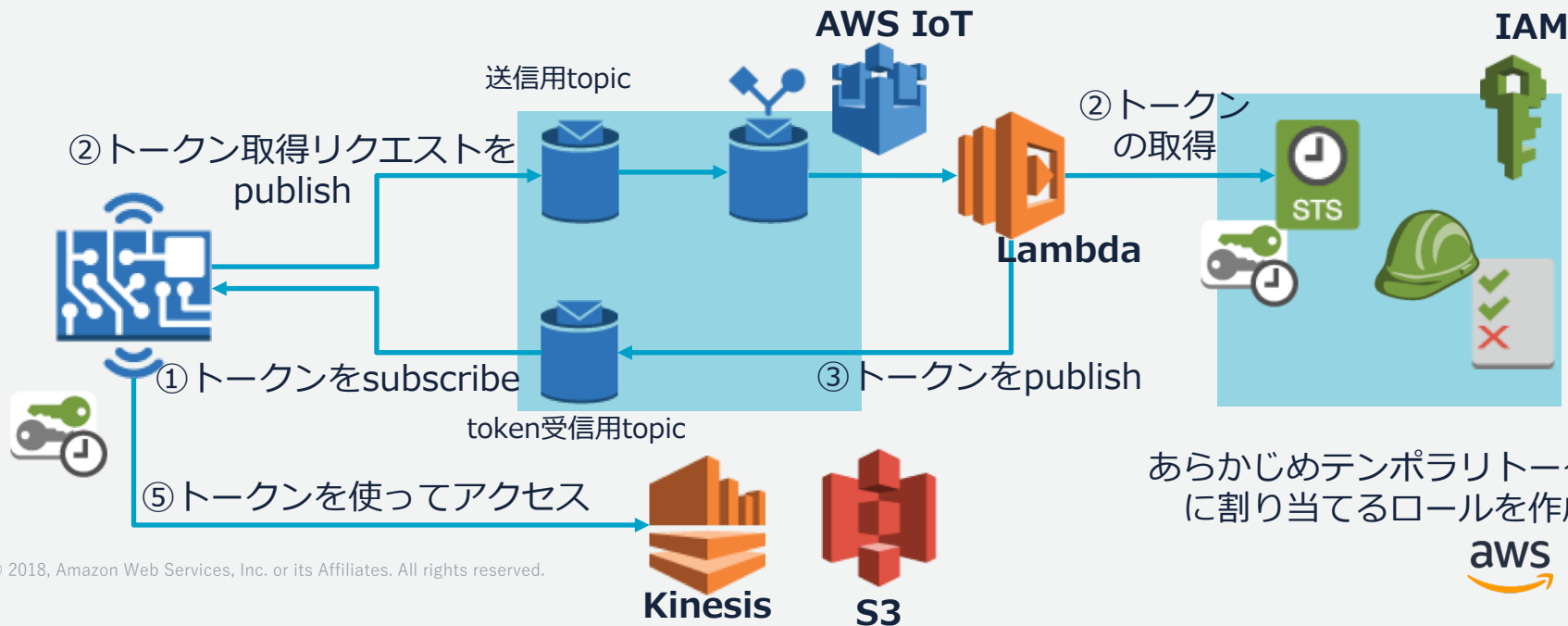
- AWS IoTの証明書を利用したセキュアな接続を利用してデバイスへAWSリソースに対してアクセス権を付与

条件

- 事前に利用するIAMが必要

注意点

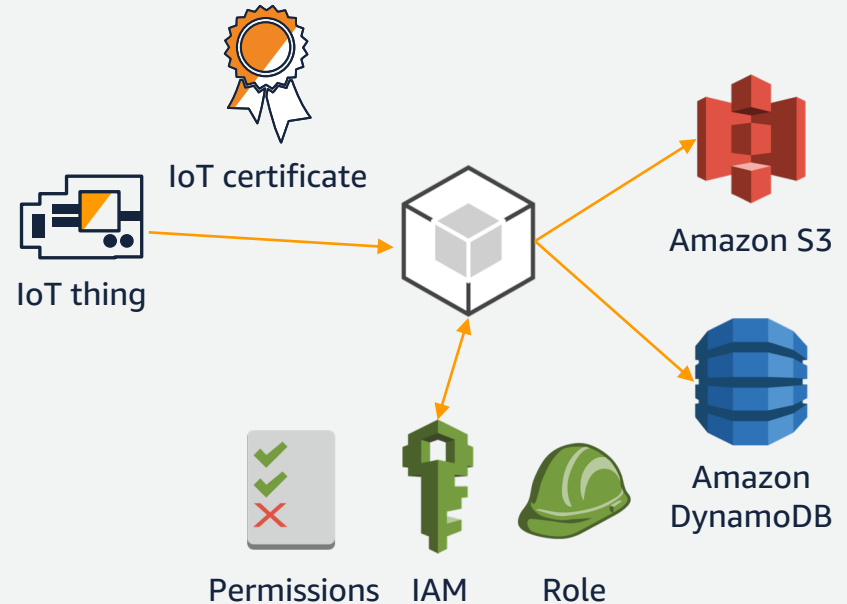
- 特になし



あらかじめテナラリトークンに割り当てるロールを作成

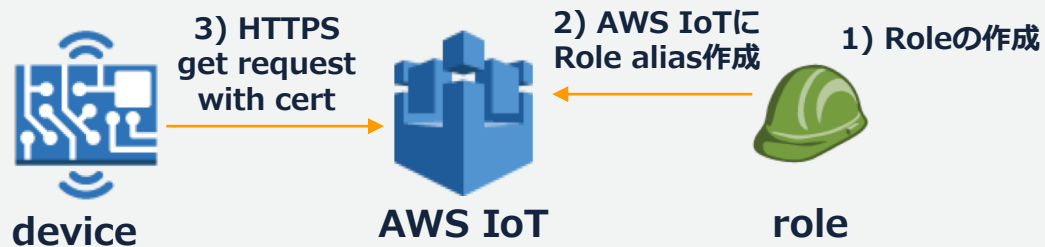
AWS SDK X.509 support

Control via IoT/MQTT
Data via HTTPS
e.g.,
Streaming video (CCTV)
Telemetry upload (Sensors)



x.509を利用したtoken取得

テンポラリトークン取得パターンと同等



e.g) wgetでtempolayな認証情報の取得

wget

--private-key= private.pem.key

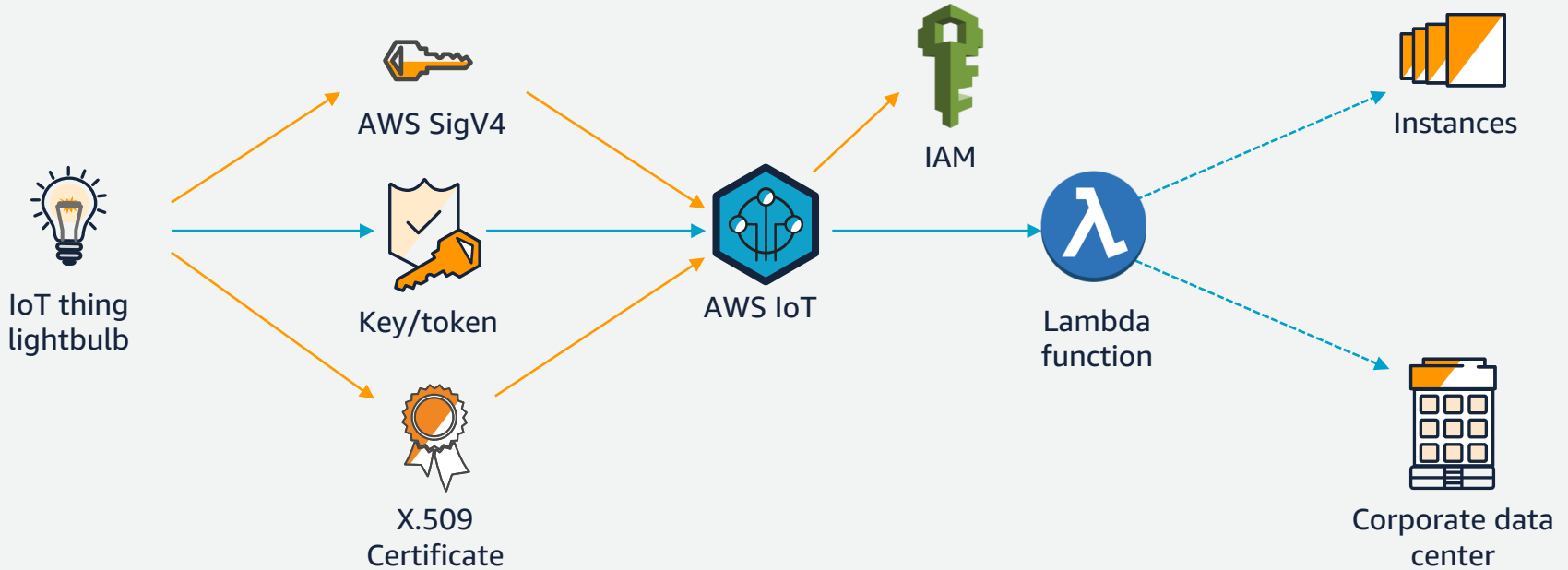
--certificate= certificate.pem.crt

--ca-directory= [AmazonRootCA1.pem](#)

https://<your_info>.credentials.iot.us-west-2.amazonaws.com:443/role-aliases/<2で登録したalias>/credentials

※)Credentialの有効期間は 2)の[CreateRoleAlias API](#)で指定可能(900-3600秒)

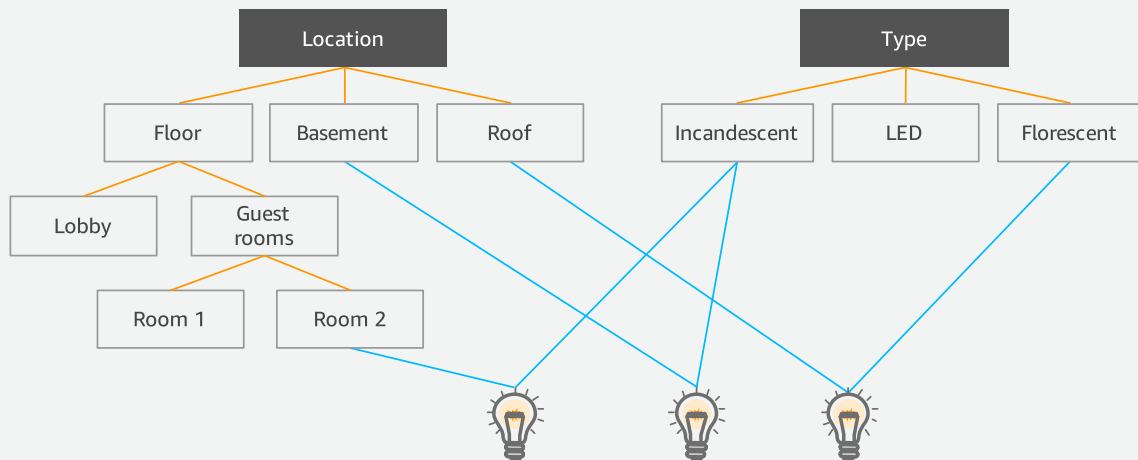
Custom authorizers



<https://aws.amazon.com/jp/blogs/security/how-to-use-your-own-identity-and-access-management-systems-to-control-access-to-aws-iot-resources/>

大量デバイスの管理

Thing Group

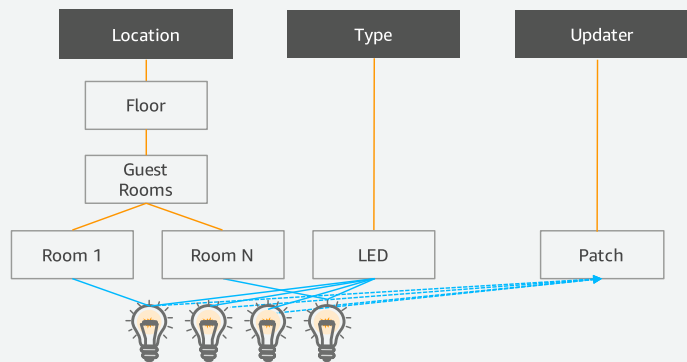


ThingをGroupとして、論理表現できる。また、Group単位でのPolicy設定が可能
- 個々のThing単位でPolicyを設定しなくても良い

例)

ビル => フロア => 部屋 などの階層設計など自由に設定可能

Groupの制約



- Group名の変更は出来ない
- Groupの階層設計(Hierarchy)の変更はできない
- 1Thing - 10Groupが上限
- 1つの階層の中で1つのグループにのみ所属出来る
 - 左記の例だと、Location : roo1, roo2に所属できない
- 1Group の下に100個の子グループ
- 階層は7階層まで
- グループにPolicyを設定できる。

今までご紹介していたデバイス管理デザインパターン

インテリジェントシャドウパターン(マルチshadowを利用している場合)

対象シーン

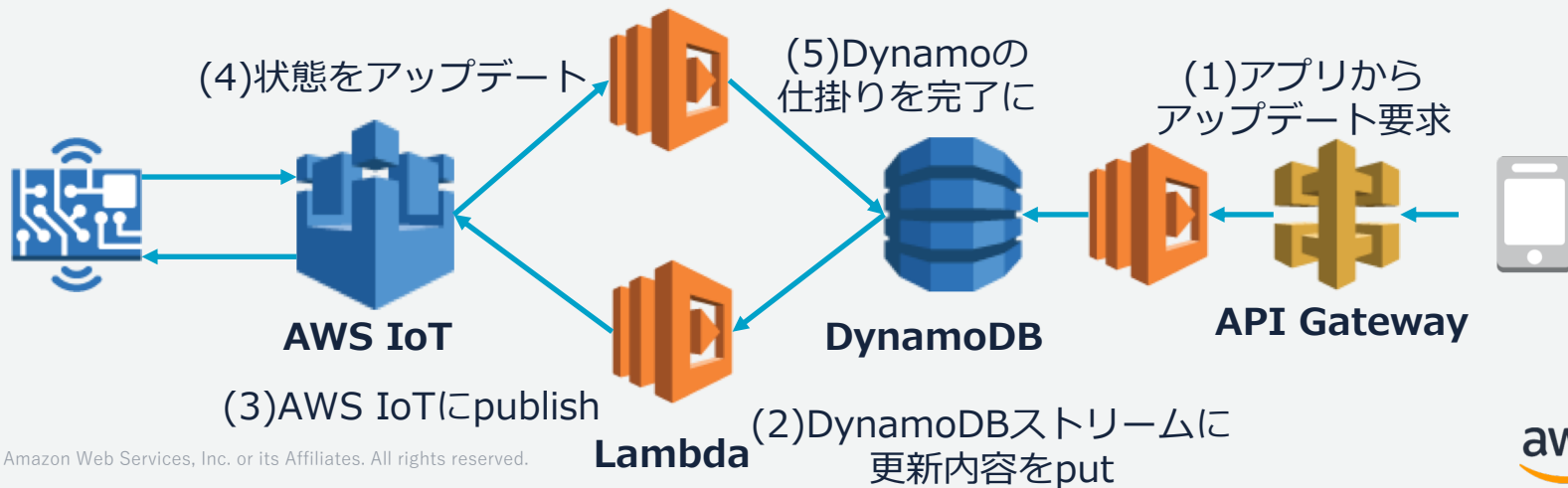
- Web/スマホアプリなどからデバイスをコントロールしたい

条件

- マルチshadowを利用している

注意点

- シャドウを利用することが必須(シャドウは8Kbの制約)



本デザインパターンでの残課題

1. shadow updateによる通知

- 大量通知が必要でも1つ1つのデバイスのshadowをupdateする必要がある。
 - 30万台：30万回のDynamoDB write, Lambda実行、shadow update API
 - 例えば、スロットル回避でsleep(1)とすると、30万秒 = 約3.5日くらいかかる
 - 効率的な配信のためのAPI発行プログラムの検討など

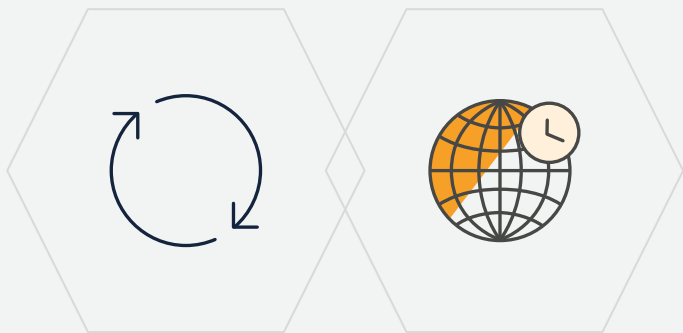
2. AWS IoTではなく、DynamoDBの状態が絶対

- Shadowの状態を正として動くほうが論理不整合起きにくい

AWS IoT Device Management

Jobs: アップデート機能

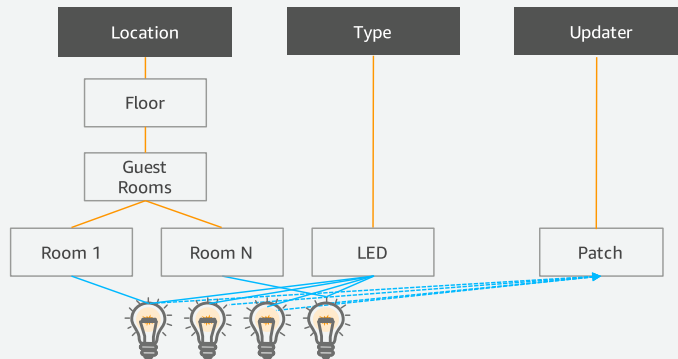
異なるスケジュールモデル



Continuous

Snapshot

柔軟な配信



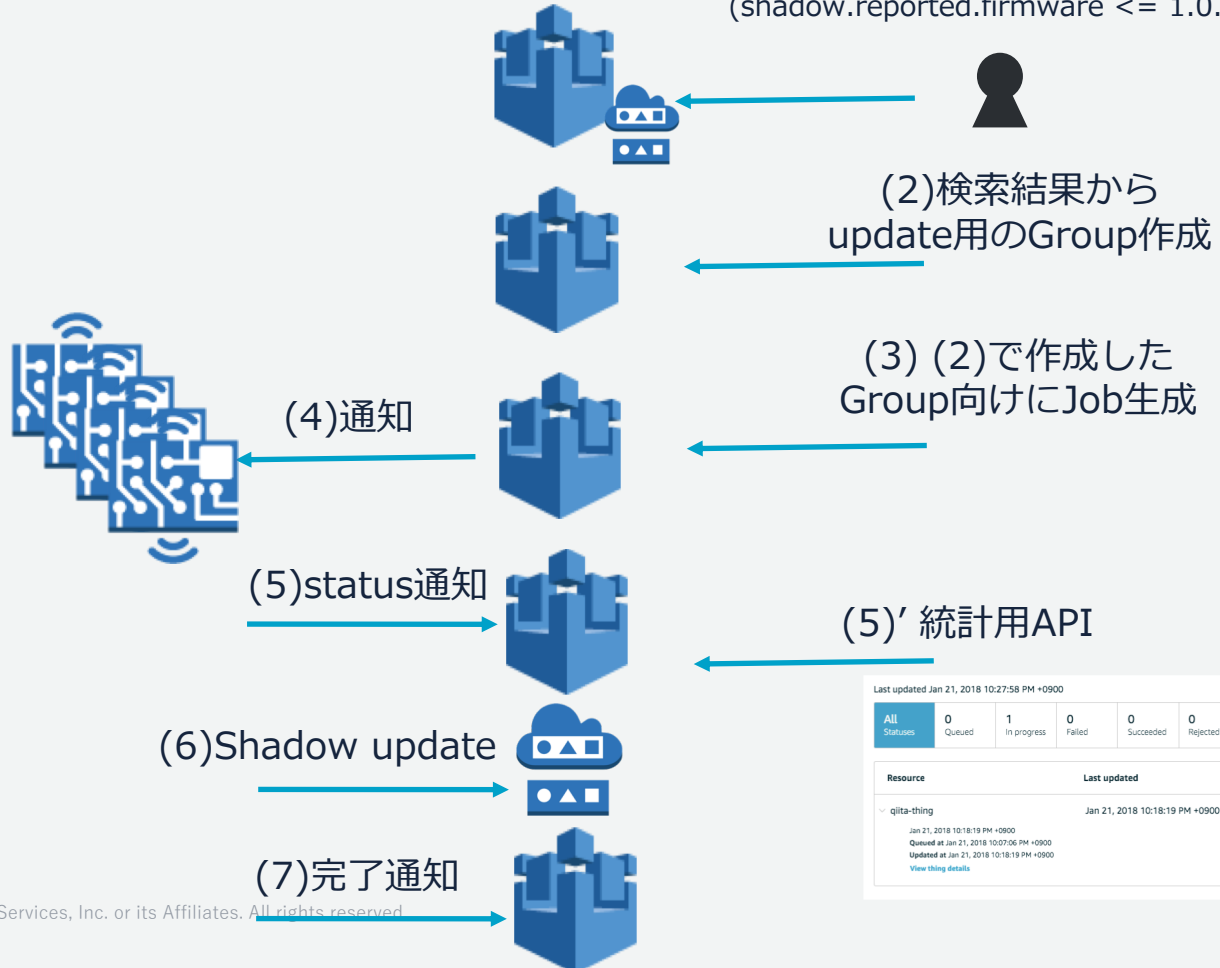
ステータス確認



Status

AWS IoTで完結可能

(1) indexを使って
対象を検索
(shadow.reported.firmware <= 1.0.0)



Last updated Jan 21, 2018 10:27:58 PM +0900 [Refresh](#)

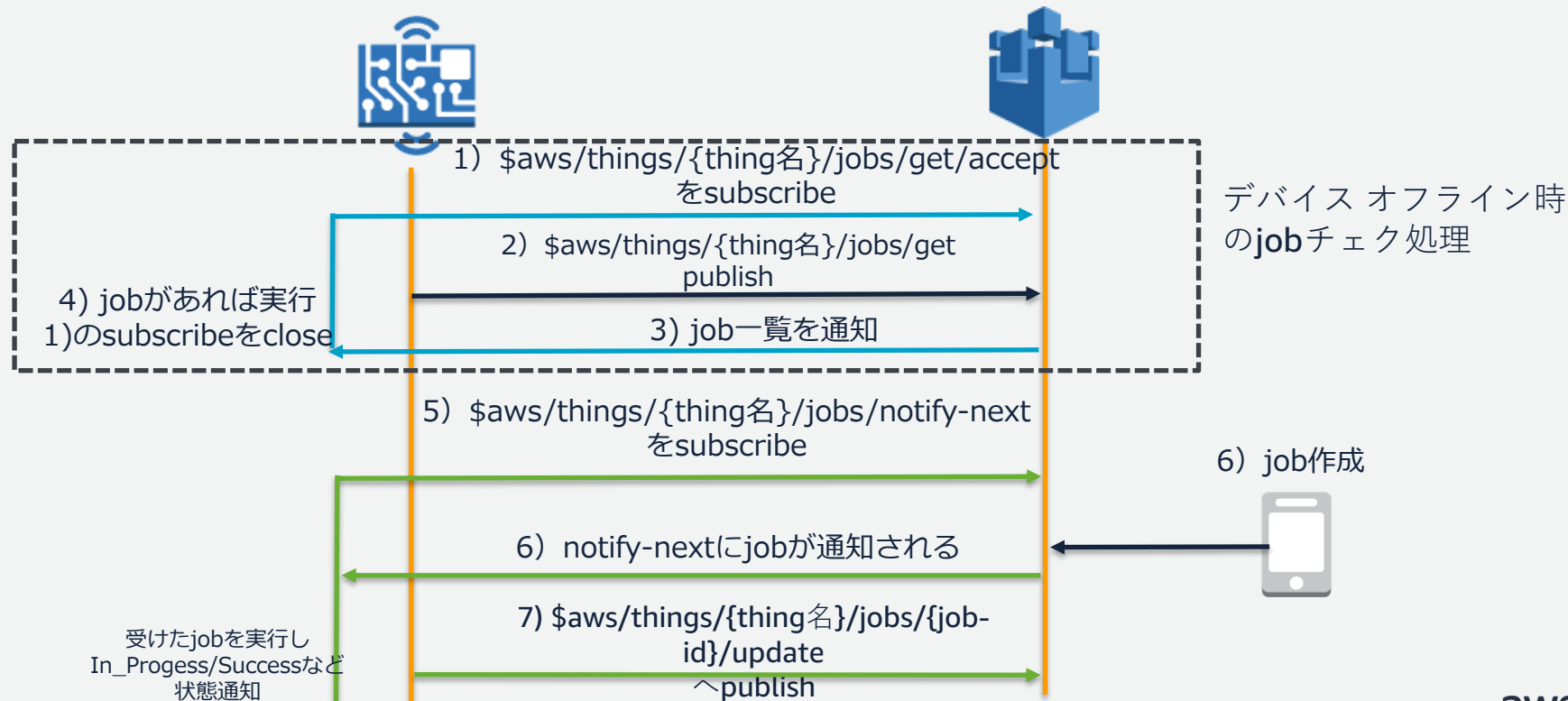
All Statuses	0	1	0	0	0	0	0
	Queued	In progress	Failed	Succeeded	Rejected	Canceled	Removed

Resource	Last updated	Status
▼ qita-thing	Jan 21, 2018 10:18:19 PM +0900	In progress
	Jan 21, 2018 10:18:19 PM +0900	
	Queued at Jan 21, 2018 10:07:06 PM +0900	
	Updated at Jan 21, 2018 10:18:19 PM +0900	
	View thing details	



Jobを受けるDeviceのtask

(SDKがリリースされれば抽象化される：現在device-sdk-js/embedded Cのみ対応)



Jobs: アップデート機能

Jobモデル



Continuous

Snapshot

- **Snapshot:**
Jobを作成したタイミングに存在するthingが対象で一度作るとJob通知の対象は変更されない
- **Continuous:**
Jobを作成した後も**配信対象となるGroupにthingが追加される**と通知が行われる。

作成された**Jobは90日間有効**。90日経過するとlistからも除外されるため、恒久的にJob履歴を残す場合は別途APIで結果を取得し、保管を検討

job開始時刻指定の機能はないので、Job作成をscriptなどで準備しjob作成を時刻指定する必要がある

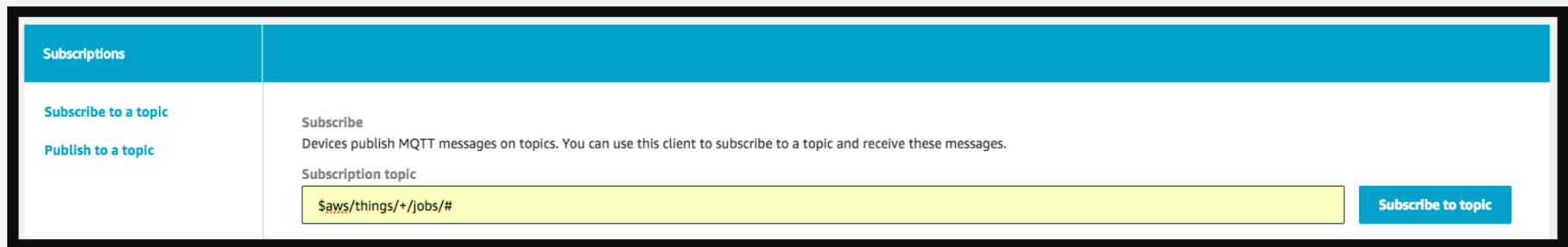
Jobの簡単なテスト方法(1/3)

Jobの通知の確認方法

AWSのマネージメントコンソールから、AWS IoTを選択し左側メニューの "Test" を選択

Jobで利用されるtopicが `$aws/things/{thingname}/jobs/{job-id}` であるので、ワイルドカードを利用し、画面のSubscription topicへ

"\$aws/things/+/jobs/#"を入力し、subscribe to topicを押下して、受信状態(この画面を開いた状態)のままにしておく。



Subscriptions	
Subscribe to a topic	Subscribe Devices publish MQTT messages on topics. You can use this client to subscribe to a topic and receive these messages.
Publish to a topic	Subscription topic <input type="text" value="\$aws/things/+/jobs/#"/> Subscribe to topic

Jobの簡単なテスト方法(2/3)

Jobの作成

1)と別のブラウザタブからAWS IoTコンソール=>管理=>ジョブ=>作成
=>カスタムジョブの作成

CREATE_JOB

Create a job

STEP 2/2

Job ID

ジョブ名を入力

Description

Select devices to update

Browse and select the devices you want to include in this job.

No devices or thing groups selected

Thing / Thing Groupの選択

Add a job file

Upload a job file that defines what your job should do.

File not selected

Taskで通知するdocumentを選択

事前に、Jobで通知する内容をJSONファイルを作成しS3へ配置する必要がある

Pre-sign resource URLs

For an extra layer of security, you can pre-sign URLs that refer to resources in your job file, like a binary for a firmware update. [Learn more.](#)

Please select a job file to continue.

Job type

ジョブの種類を選択

A job can run on the devices and/or groups selected, or remain open, and apply to devices later added to a group. [Learn more.](#)

Your job will complete after deploying to the selected devices/groups (snapshot)

Your job will continue deploying to any devices added to the selected groups (continuous)

Job executions rollout configuration

Specify how quickly devices will be notified of a pending job execution.

Maximum per minute (1-1000)

1000

毎分何台ごとに通知するかを入力

Back Create

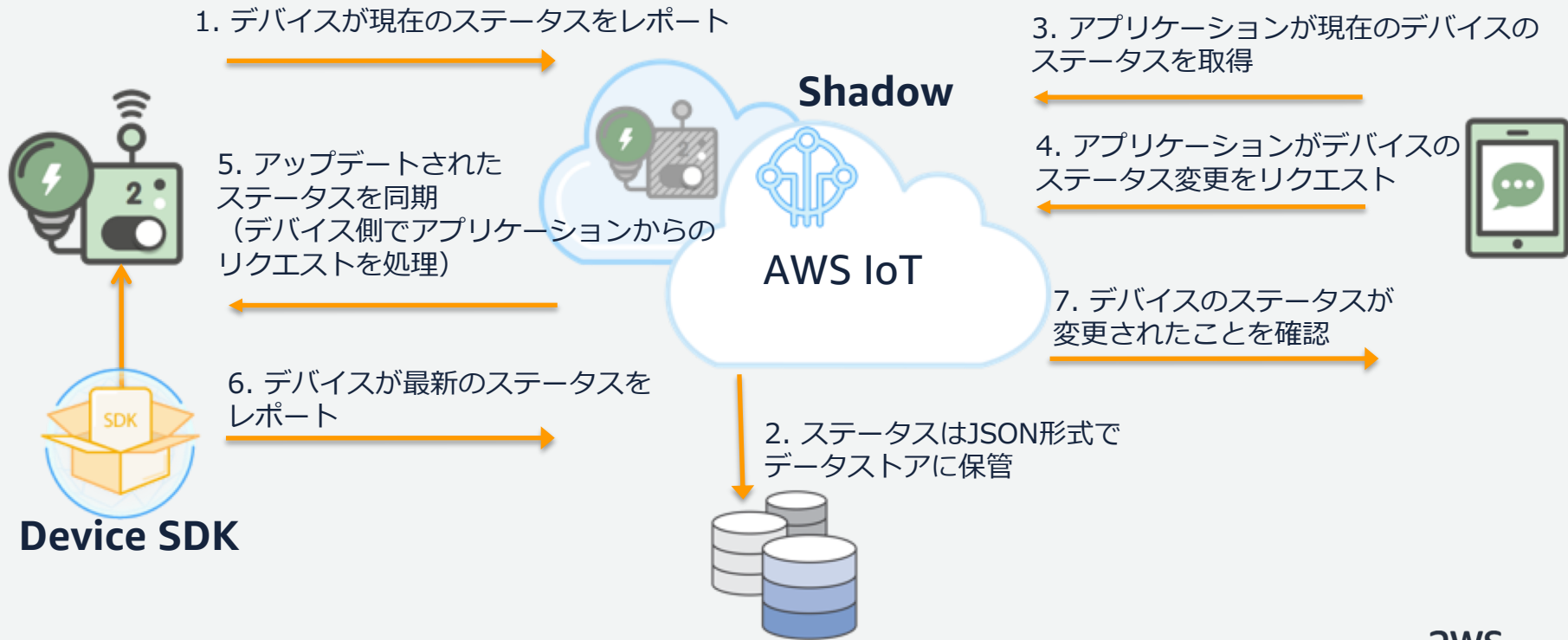
ShadowとJobの使い分け？

AWS IoT Shadow

結果整合性として、強い管理機能がある。
Shadowを一度使うと、機器の制御のコントロールプレーンとしてShadowを中心に考える必要がある

以降でshadowのフローを説明

デバイス シャドウの動作フロー



デバイス シャドウ



Thing

1つまたは複数の現状ステータスをシャドウに通知
シャドウから要求されるステータスを取得



Shadow

シャドウは、delta, desired 及びreported
ステータスをメタデータとバージョンをつけて管理

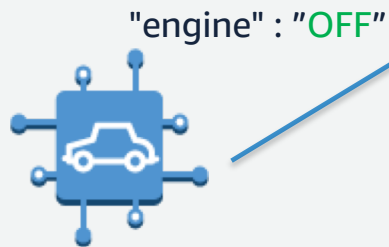


Mobile App

デバイスに対して変更したいステータスをセット
最新の通知されたステータスを取得
シャドウの削除

```
{
  "state" : {
    "desired" : {
      "engine" : "ON"
    },
    "reported" : {
      "engine" : "OFF"
    },
    "delta" : {
      "engine" : "ON"
    }
  },
  "version" : 10
}
```

デバイスは現在のステータスをアップデート

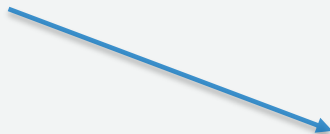


```
{  
  "state" : {  
    "desired" : {  
      "engine" : "ON"  
    },  
    "reported" : {  
      "engine" : "OFF"  
    }  
  },  
  "version" : 10  
}
```

アプリケーションからエンジンON



"engine" : "ON"



```
{  
  "state" : {  
    "desired" : {  
      "engine" : "ON"  
    },  
    "reported" : {  
      "engine" : "OFF"  
    }  
  },  
  "version" : 10  
}
```

deltaが通知される



"engine" : "ON"

```
{  
  "state" : {  
    "desired" : {  
      "engine" : "ON"  
    },  
    "reported" : {  
      "engine" : "OFF"  
    },  
    "delta" : {  
      "engine" : "ON"  
    }  
  },  
  "version" : 10  
}
```

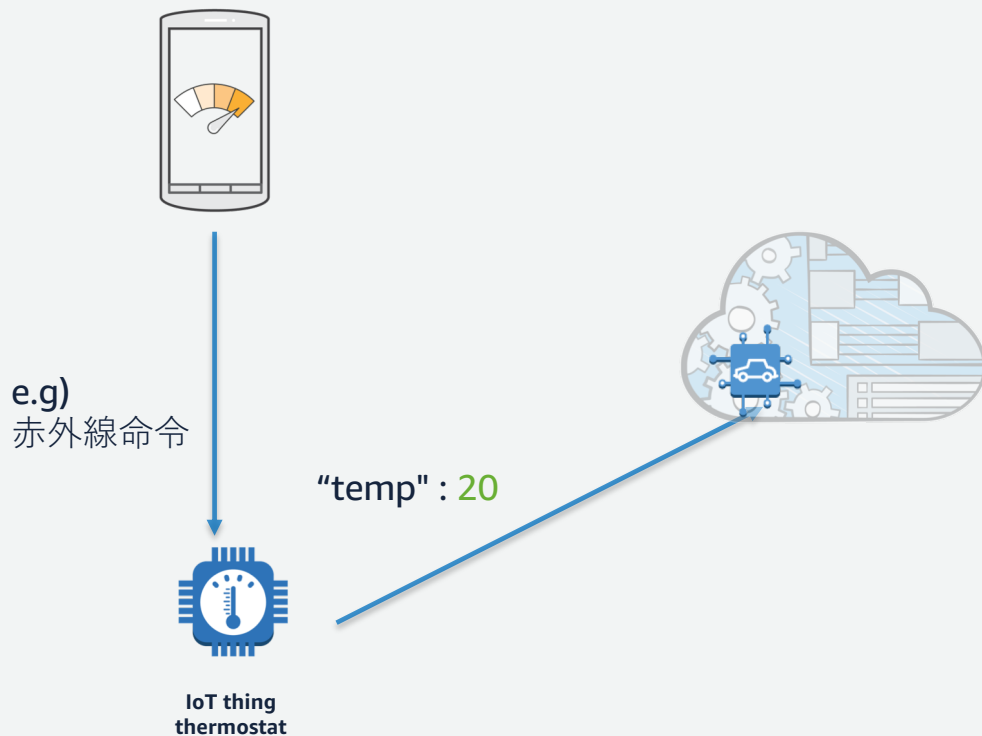
最新のステータスにアップデート(deltaは消える)



"engine" : "ON"

```
{  
  "state" : {  
    "desired" : {  
      "engine" : "ON"  
    },  
    "reported" : {  
      "engine" : "ON"  
    },  
    "delta" : {  
      "engine" : "ON"  
    }  
  },  
  "version" : 10  
}
```

User操作によりreportだけ変更すると？

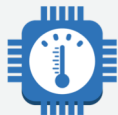


```
{  
  "state" : {  
    "desired" : {  
      "temp" : 25  
    },  
    "reported" : {  
      "temp" : 20  
    },  
  },  
  "version" : 10  
}
```

User操作によりreportだけ変更すると？



"temp" : 25



IoT thing
thermostat

```
{  
  "state" : {  
    "desired" : {  
      "temp" : 25  
    },  
    "reported" : {  
      "temp" : 20  
    },  
    "delta" : {  
      "temp" : 25  
    },  
  },  
  "version" : 10  
}
```

Shadowの使い所

管理者のみがコントロール出来る値/configの一部を管理するようなユースケースや特定機器に対しての設定変更が行いやすい。

例) debug level 、 データ送信頻度など

Shadow のdesiredを同値でupdateすると、deltaは発生しないが、
\$aws/things/*thingName*/shadow/update/documents
にpublishは発生する。ユースケースに応じてshadow関連のtopicは理解しておくこと

シャドウのMQTT Topic

デバイスSDK (C-SDK, JS-SDK)で
シャドウのMQTTトピックを利用

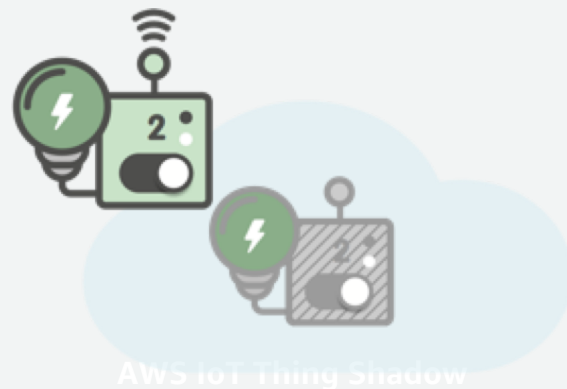
Sensor	Reported	Desired	Delta
LED1	RED	YELLOW	LED1 = Yellow TEMP = 60F
ACCEL	X=1,Y=5,Z=4	X=1,Y=5,Z=4	
TEMP	83F	60F	

UPDATE: `$aws/things/{thingName}/shadow/update`

DELTA: `$aws/things/{thingName}/shadow/update/delta`

GET: `$aws/things/{thingName}/shadow/get`

DELETE: `$aws/things/{thingName}/shadow/delete`



https://docs.aws.amazon.com/ja_jp/iot/latest/developerguide/device-shadow-mqtt.html

Jobの使い所

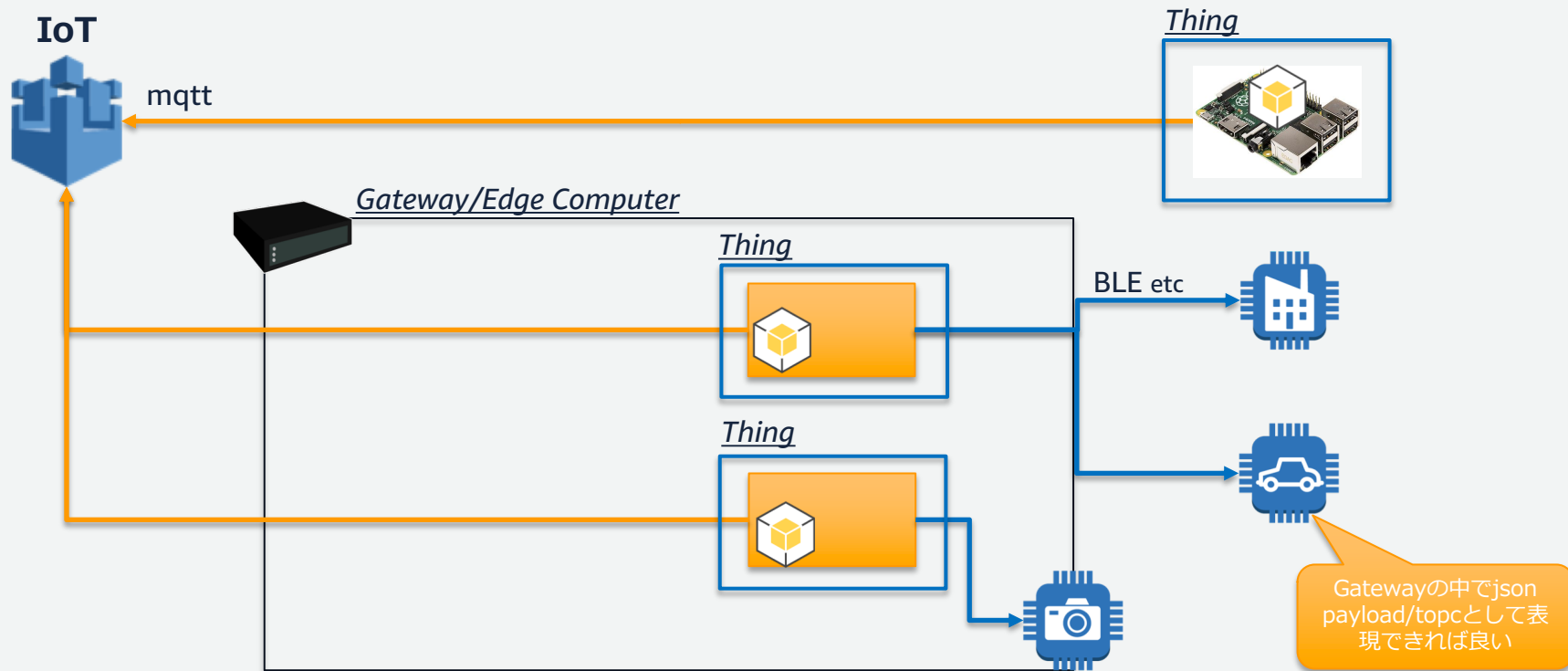
Stateをもたない通知や実行命令などを大量のデバイスに行いたい場合に利用をしやすい。(統計機能もある)

firmware version,コンテンツ配信などは前述の通り、shadowと組み合わせる事で、Index機能でshadow検索 =>update Group作成が可能となり、組み合わせで便利に使える機能となる

まとめ

Thing? AWS IoTの場合

AWS IoTと通信するものが証明書を持てば良い



大量デバイスに関わる制約事項の理解も重要

AWS IoT limitより引用:

- アカウントを 1 秒あたり最大 300 MQTT CONNECT リクエストに制限します。
- アカウント別に 1 秒あたり 9,000 publish
インバウンド発行リクエスト - 最大 1 秒あたり 3,000、
アウトバウンド発行リクエスト数 - 最大 1 秒あたり 6000
- 1 秒あたり最大 500 のサブスクリプションにアカウントが制限されます。

上限融和可能だが、**デバイス単位でタイミングがばらつく**ような設計を推奨

https://docs.aws.amazon.com/ja_jp/general/latest/gr/aws_service_limits.html#limits_iot

まとめ

証明書など個別機器に対してのセキュリティなどを後回しにしがちだが、**プロジェクト最初からデバイスの管理** (セキュリティやfirm管理など)について決めておくことを推奨

出荷済みの機器や対象のthingに対してクラウドからコントロールできる仕組みを予め検討し、手段を用意しておくことも重要となる

オンラインセミナー資料の配置場所

AWS クラウドサービス活用資料集

- <http://aws.amazon.com/jp/aws-jp-introduction/>



AWS Solutions Architect ブログ

- 最新の情報、セミナー中のQ&A等が掲載されています
- <http://aws.typepad.com/sajp/>

公式Twitter/Facebook AWSの最新情報をお届けします



@awscloud_jp



検索

もしくは
<http://on.fb.me/1vR8yWm>

最新技術情報、イベント情報、お役立ち情報、
お得なキャンペーン情報などを日々更新しています！

AWSの導入、お問い合わせのご相談

AWSクラウド導入に関するご質問、お見積り、資料請求をご希望のお客様は以下のリンクよりお気軽にご相談ください

<https://aws.amazon.com/jp/contact-us/aws-sales/>

お問い合わせ	<h2>日本担当チームへのお問い合わせ</h2>
日本担当チームへのお問い合わせ >	AWS クラウド導入に関するご質問、お見積り、資料請求をご希望のお客様は、以下のフォームよりお気軽にご相談ください。平日営業時間内に日本オフィス担当者よりご連絡させていただきます。
関連リンク フォーラム	<p>※ご請求金額またはアカウントに関する質問はこちらからお問い合わせください。 ※Amazon.com または Kindle のサポートに問い合わせはこちらからお問い合わせください。</p>
	<p>アスタリスク(*)は必須情報となります。</p> <p>姓*</p> <input type="text"/> 名* <input type="text"/>

※「AWS お問い合わせ」で検索してください

AWS Well Architected 個別技術相談会お知らせ

- Well Architectedフレームワークに基づく数十個の質問項目を元に、お客様がAWS上で構築するシステムに潜むリスクやその回避方法をお伝えする個別相談会です。

<https://pages.awscloud.com/well-architected-consulting-2017Q4-jp.html>

- 参加無料
- 毎週火曜・木曜開催



【1, 2, 3 月開催】AWS Well Architected 個別技術相談会

AWS 上で構築するシステムのリスクの把握・回避方法をご希望のお客様

この度 AWS をご活用頂いているお客様を対象に「AWS Well Architected 個別技術相談会」を開催致します。

Well Architected 個別技術相談会では、リスクの把握・回避を目的として、セキュリティ・信頼性・パフォーマンス・コスト・運用の5つの観点で、お客様の AWS 活用状況や構成についてお伺いします。AWS のベストプラクティスに基づき作成された Well Architected フレームワークを元に、今までお客様がお気づきでなかったリスクやAWS活用の改善点を見つけることができます。例えば、自動車においては納車前点検、車検を定期的に行うのと同様に、本相談会はお客様の AWS 上のシステムをよりよく活用頂くことを目的にしております。

Well Architected 個別技術相談会にご参加頂くには、本ページにてお申込み後、弊社担当者からお送りするヒアリングシートにご記入・担当者にご送付頂く必要があります。その内容を元に、当日の相談会では AWS のソリューションアーキテクトと共に技術的なディスカッションをさせていただきます。また、遠方のお客様、アマゾン東京オフィスへのご来社が時間等の関係で難しいお客様は、Web のプレゼンテーションツールや、お電話を活用したリモートでのご相談も承ります。

その他にも個別にご相談内容があれば、こちらもご相談を承りますので、是非お気軽にご参加ください。

034	毎週火曜、木曜開催
-----	-----------



下記のおフォームよりお申込みください。

* 姓:

* 名:

* Eメールアドレス:

