モバイルワーキンググループ 2017 年 2 月以前の活動報告

- 2017 年 2 月

1.国内活動

1-1. 京都女子大学との連携活動

・2017 年 2 月 4 日（土）、京都女子大学 現代社会学部 現代社会学科 丸野研究室の「情報系女子×myThings ハンズオンイベント」の運営に協力

（京都女子大学および立命館大学の女子学生 16 名が参加）

・京都女子大学内に IoT コミュニティとして立ち上がる「Universal Robot Club」の活動に協力する予定

⇒関西圏の大学・研究機関との連携ネットワークづくりのユースケースに

2. グローバル活動

2-1. CSA Mobile Working Group

2-1-1. CSA Mobile WG: Online Meeting（2 月）（終了）

日時：2017 年 2 月 10 日（金）2:00am-3:00pm（JST）

会場：WebEx Online

司会：Hillary Baron

概要：

Update Top Threats to Mobile

- *ACTION ITEM*: provide a list of the risks to mobile that you see in the industry

Co-chair voting

- *ACTION ITEM*: contact me if you are interested by Feb 17th
- Voting will begin after RSA via survey monkey (look for the link in your inbox and Basecamp)

Mobile Guidance

- *ACTION ITEM*: continue to make comments on the sections that need to be updated. Just a quick comment with what needs to be changed and why

Other items in queue

- Update mobile controls within CCM
- Update questions in CAIQ
- BYOD and EMM paper(s)

次回ミーティング：2017 年 3 月 10 日午前 2 時〜3 時

2-2.　CSA Internet of Things (IoT) WG

　　2-2-1.　Internet of Things (IoT) WG: Bi-Weekly Call　2 月）　（終了）

日時：2017 年 2 月 10 日（金）　3:00am-4:00pm（JST）

会場：WebEx Online

司会：Brian Russell, Chair of the CSA Working Group on Internet of Things

概要：

GUEST SPEAKER

"Securing Drones: Lessons from the Front Lines of the Industry"

Jared Ablon, CISO at AirMap

https://www.airmap.com/

As Chief Information Security Officer, Jared Ablon is responsible for securing the leading network for real-time information exchange related to unmanned aircraft systems. His purview also includes the development of future-thinking protocols for authenticating UAS and their operators, filing secure flight plan trajectories, and detecting and defending against intrusions from bad actors. Previously Ablon worked at MITRE Corporation, where he led efforts to ensure security of next generation GPS navigation systems and other communications technologies for multiple U.S. Air Force programs. He began his career at the U.S. Department of Defense leading large teams of security experts and developing cutting-edge cryptanalysis, network exploitation and vulnerability analysis security technologies.

2-2-2.　CSA IoT WG@RSA Conference 2017（終了）

日時：2017 年 2 月 13 日（月）

会場：Marriott Marquis, San Francisco, CA

司会：Brian Russell, Chair of the CSA Working Group on Internet of Things

概要：

As you might have already guessed, IoT was an incredibly hot topic at RSA 2017. The IoT topics discussed can be broken into key themes:

1. IoT in the commercial sector has been around for a long time, which isn't new - what is new are the new challenges created as IoT devices get more attention. One example is the blurred lines between OT and IT networks. Many of the IoT device challenges we're seeing today are linked to the proper configuration of these devices and the protection of the data these devices are collecting and reporting on.

2. Home/Consumer IoT devices are more susceptible; a major topic at RSA 2017. There's a lot of on-going development with many companies manufacturing devices as fast and as cost effectively as possible, while also delivering them with incredibly poor security and update functionality in place. This, combined with the tendency for many consumers to focus less on the security of what they're configuring and more on just getting the device working as quickly as possible, opens us up to these recurring scenarios of compromised consumer IoT devices.

3. IoT market infancy was a focus of many discussions. Everyone seems to be keeping an eye on things, but few prospects seem to have a handle on what their IoT strategy or plans are at this time.

4. IoT ecosystem is bigger than just IoT devices, and it's critical that IoT security focuses on the entire IoT ecosystem. The ecosystem is not only made up of the IoT devices, the software that runs on them and the information that they store or pass along, but also covers any other devices that are used to manage, configure, or communicate with them. As the IT and OT worlds continue to collide, there's an even greater requirement to understand what endpoint and infrastructure devices populate the enterprise network and how those devices are behaving in real-time.

5. Partnerships: Partnerships are going to play a critical role in IoT security. There are many players in the space due to how diverse the ecosystem is, and all seem to focus on specific parts of the overall solution. This allows us to play very nicely based on our "see all, know all, enhance all" philosophy.

During the RSA 2017 Conference, there was also some interesting discussion around the legality of wireless discovery, which plays into IoT, as many IoT devices are wireless. This is still a bit of a grey area in many cases, depending on the technology in question of course.

Finally, there was certainly some buzz around AI throughout the conference, however, within the technical talks it was more

> about caution and understanding of 'Machine Learning'
> implementations and their limitations. One speaker at the
> conference spoke about AI in this regard: "[AI] will move
> the needle, but likely not as much as people think, or want
> you to think, it will".

- 2017 年 1 月

1．国内活動

1-1. CSA Japan Congress 2016（終了）

日時：2016 年 11 月 22 日（火）03:40pm - 03:55pm

公演予定者：WG リーダー　笹原英司

講演概要：「モバイル・ファースト」「クラウド・ファースト」の波
が企業システムに広がる中、アプリケーション開発から運用まで一元
的に管理する「DevOps」を活用したセキュリティのエコシステム作
りの取組みと課題を紹介します。

2．グローバル活動

2-1. CSA Mobile Working Group

2-1-1. CSA Mobile WG: Online Meeting (11 月)（終了）

日時：2016 年 11 月 18 日（金）　2:00am-3:00pm（JST）

会場：GoToMeeting

司会：John Yeoh

概要：

・Discuss with those individuals who joined what they would like to get out of the group and their background

・Review charter, group goals, and potential deliverables

・Action Item:

-Review NISTIR 8144 Assessing select the top 10 or 15 threats from the document

(http://csrc.nist.gov/publications/drafts/nistir-8144/nistir8144_draft.pdf)

-Next meeting we will discuss everyone's selections and create a survey that will go out after the 1st of the year with the goal of creating a white paper on the top 10 mobile threats

・次回ミーティング（12/16）予定

2-2.　CSA Internet of Things (IoT) WG

　　2-2-1.　「Establishing a Safe and Secure Municipal Drone Program」

　　　　・スマートシティ等、サービスにおける無人飛行機（ドローン）利用時の IoT セキュリティに関するホワイトペーパー

　　　　・公開ピアレビュー期間終了（11 月 6 日）

　　　　・2016 年 12 月最終版公開予定

　　2-2-2.　「Observations and Recommendations on Connected Vehicle Security」

　　　　・次世代自動車のセキュリティに関するホワイトペーパー

・公開ピアレビュー期間終了（11 月 14 日）

・2016 年 12 月最終版公開

2-2-3. 「Examining the Use of Block Chain technology for a Secure Internet of Things」

・ブロックチェーン技術の IoT セキュリティへの適用可能性に関するホワイトペーパー

・現在、WG 内でピアレビュー中。

2-2-4. Internet of Things (IoT) WG: Bi-Weekly Call　11 月）（終了）

日時：2016 年 11 月 18 日（金）　3:00am-4:00pm（JST）

会場：WebEx Online

司会：Brian Russell, Chair of the CSA Working Group on Internet of Things

概要：(1) Draft first set of IoT Security Controls - John and Victor will post first draft to Basecamp for review and present on one of the upcoming calls by December 15

　-Based on our IoT documents and the CCM

　-Reference the need for IoT regulation

　http://www.computerworld.com/article/3141803/security/us-lawmakers-balk-at-call-for-iot-security-regulations.html

　(2) Final review for Connected Vehicles - Last feedback allowed through Sunday November 20

　　-Observations and Recommendations on Connected Vehicle Security

(3) Review latest draft for Blockchain - John and Sabri to provide project plan on next call by December 1
- Blockchain and the IoT

(4) Our collaboration with Securing Smart Cities, "Establishing Safe and Secure Municipal Drone System" has completed Open Peer Review and the incorporation of final feedback. Release date will be in December but still TBD.

(5) Discussed Charter and initiatives updates for 2017 - TBD

- 2016 年 11 月

1. 国内活動

2017 年 1 月は、特に活動実績なし

2. グローバル活動

2-1. CSA Mobile Working Group

2-1-1. CSA Mobile WG: Online Meeting（1 月）（終了）

日時：2017 年 1 月 13 日（金）2:00am-3:00pm（JST）

会場：WebEx Online

司会：Hillary Baron

概要：

・Co-chair Needed!: Anyone interested in learning more about the position or would like to be considered for the position email Hillary Baron.

・Top Threats to Mobile: Send me your top 10 - 15 threats selected from the NISTIR 8144 - Mobile Threat Catalogue by Feb 6th.

・Mobile Guidance Update: Security Guidance for Critical Areas of Mobile Computing v1 is in need of updating. Provide your comments and feedback on the content that needs updating, deleting, or modifying for v2 of the document. Please focus on the content NOT grammar, syntax, etc.

次回ミーティング：2017 年 2 月 10 日午前 2 時～3 時

2-2. CSA Internet of Things (IoT) WG

2-2-1. Internet of Things (IoT) WG: Bi-Weekly Call 1 月）（終了）

日時：2017 年 1 月 26 日（金） 3:00am-4:00pm（JST）

会場：WebEx Online

司会：Brian Russell, Chair of the CSA Working Group on Internet of Things

概要：

Discussed the status of our ongoing efforts.

- "Establish a Safe and Secure Drone Program" Guidance document is now posted on the CSA website. Official release is 2/2/2017.

（アウトプットの利活用で、CSA ジャパンの健康医療情報管理 WG が協力する）

- "Observations and Recommendations on Connected Vehicle Security" document has gone through peer review and is in final technical edits.

- "Blockchain and the IoT" document is ready for peer review. （ピアレビューで、CSA ジャパンのブロックチェーン WG が協力する）

Discussed potential CY2017 Work Efforts.

-IoT / Cloud Controls Matrix (CCM) Integration.   John Yeoh is working out the format for this and has identified a handful of IoT -specific controls for inclusion.   We will put out a call for additional volunteers once we have the format defined. Guarav P has volunteered to support this.

-Securing Cloud Connected IoT Systems.   This will be a large effort for the year and is focused on the cloud components that support IoT systems as well as the gateways and interfaces to the cloud.   This guidance will have several companion guides that are industry-specific.

-Europe-specific guidance documentation for secure IoT.   John mentioned that there is a desire to identify Europe-specific IoT security controls.   There may be opportunities to work across Europe (by bringing together various stakeholders) to support this.   One of the CSA chapters in Europe can help to lead this effort, reporting back to the CSA IoT WG.

-CSA IoT Certification Program. No real progress made yet, but this is still being researched to determine viability. Focus for CSA would be certifying the cloud providers that support IoT products.

-Attack Tree. John mentioned that it would be good to create an Attack Tree for the IoT. We decided that this should be a standalone work item. It is applicable across all guidance documents that we product. Need volunteers to help build this tree

Discussed options for Industry-specific IoT security guidance:

-Industrial IoT

-Manufacturing

-Health Care

-Transportation

-Smart Cities

-Fintech

-Aviation

-Energy (Oil/Gas)

*It was mentioned that we need to reach out to CSPs and other IoT organizations to gather real use cases for our new research.

(Industry-specific の観点から、CSA ジャパンの健康医療情

報管理、ビッグデータ／ICS、ブロックチェーン各 WG が協力する

We put out a call for speaker volunteers.   We will maintain a list of interested speakers (by region?) to provide speaking opportunities about the WG and IoT security as those opportunities arise.

Brian mentioned that there is material available to build up presentations

for anyone that might be speaking somewhere and wants to mention our WG.

To access our gitlab site go to:

https://gitlab.com/brianr/CloudSA_IoT_.

Feel free to use content (with attribution to the CSA IoT WG).

次回ミーティング：2017 年 2 月 10 日午前 3 時〜4 時

- 2016 年 10 月

1. 国内活動

1-1.　　SBR2016　-　Security Groups Roundtable, 2016.9.23（終了）

　　　パネル・ディスカッション

　　　日時：2016 年 9 月 23 日（金）　03:40pm - 04:30pm

　　　会場：御茶ノ水　ソラシティ・カンファレンスセンター

　　　パネリスト：岡田　良太郎（OWASP Japan）、吉田雄哉（マイクロソフト）、仲田翔一（OWASP Japan）、笹原英司（CSA ジャパン・モバイルユーザーWG）、

表題：DevSecOps x サービス x セキュリティ

概要：セキュリティは脅威と闘っているだけではなく、IT 環境とも闘っています。日本においては、2000 年頃から IT セキュリティが意識されるようになりましたが、2016 年の現在においては、当時とは異なる IT 環境が構築されており、現在の IT 環境への従来のセキュリティの適用ではなく、現在の IT 環境に適したセキュリティのあり方が必要とされています。当セッションでは、DevOps をキーワードに、「箱を買う」のではなく、「サービスを活用する」ようになった現在の IT 環境を俯瞰し、競争力と安全性の高い IT 環境を実現するための構築・運用モデルを示します。

詳細：　http://wasforum.jp/2016/09/sgr2016-sched/

1-2.　CSA Japan Congress 2016（予定）

日時：2016 年 11 月 22 日（火）03:40pm - 03:55pm

公演予定者：WG リーダー　笹原英司

講演概要：「モバイル・ファースト」「クラウド・ファースト」の波が企業システムに広がる中、アプリケーション開発から運用まで一元的に管理する「DevOps」を活用したセキュリティのエコシステム作りの取組みと課題を紹介します。

2.　グローバル活動

2-1.　CSA Mobile Working Group

2016 年 9 月は、特に活動実績なし

2-2.　CSA Internet of Things (IoT) WG

　　2-2-1.　Internet of Things (IoT) WG: Bi-Weekly Call　9 月）（終了）

　　日時：2016 年 9 月 9 日（金）　2:00am-3:00pm（JST）

　　会場：WebEx Online

　　司会：Brian Russell, Chair of the CSA Working Group on Internet
of Things

　　概要：　・（仮）Designing and Developing Secure IoT Products

　　　　　　2016 年 10 月 7 日公開予定

　　　　　　・New GitLab Repo for our IoT Working Group

　　　　　https://gitlab.com/brianr/CloudSA_IoT_WG/

- 2016 年 9 月

1.　国内活動

1-1.　　SBR2016　‐ Security Groups Roundtable, 2016.9.23（終了）

　　パネル・ディスカッション

　　日時：2016 年 9 月 23 日（金）　03:40pm‐04:30pm

　　会場：御茶ノ水　ソラシティ・カンファレンスセンター

　　パネリスト：岡田　良太郎（OWASP Japan）、吉田雄哉（マイクロソ
フト）、仲田翔一（OWASP Japan）、笹原英司（CSA ジャパン・モバ
イルユーザーWG）、

　　表題：DevSecOps　x サービス x セキュリティ

　　概要：セキュリティは脅威と闘っているだけではなく、IT 環境とも闘
っています。日本においては、2000 年頃から IT セキュリティが意識
されるようになりましたが、2016 年の現在においては、当時とは異
なる IT 環境が構築されており、現在の IT 環境への従来のセキュリテ
ィの適用ではなく、現在の IT 環境に適したセキュリティのあり方が

必要とされています。当セッションでは、DevOps をキーワードに、「箱を買う」のではなく、「サービスを活用する」ようになった現在の IT 環境を俯瞰し、競争力と安全性の高い IT 環境を実現するための構築・運用モデルを示します。

詳細： http://wasforum.jp/2016/09/sgr2016-sched/

1-2. CSA Japan Congress 2016（予定）

日時：2016 年 11 月 22 日（火）03:40pm - 03:55pm

公演予定者：WG リーダー　笹原英司

講演概要：「モバイル・ファースト」「クラウド・ファースト」の波が企業システムに広がる中、アプリケーション開発から運用まで一元的に管理する「DevOps」を活用したセキュリティのエコシステム作りの取組みと課題を紹介します。

2. グローバル活動

2-1. CSA Mobile Working Group

2016 年 9 月は、特に活動実績なし

2-2. CSA Internet of Things (IoT) WG

2-2-1. Internet of Things (IoT) WG: Bi-Weekly Call　9 月）（終了）

日時：2016 年 9 月 9 日（金） 2:00am-3:00pm（JST）

会場：WebEx Online

司会：Brian Russell, Chair of the CSA Working Group on Internet of Things

概要： ・（仮）Designing and Developing Secure IoT Products

2016 年 10 月 7 日公開予定

・New GitLab Repo for our IoT Working Group

https://gitlab.com/brianr/CloudSA_IoT_WG/

- 2016 年 8 月

1. Mobile Application Security Testing Initiative

ホワイトペーパー「Mobile Application Security Testing」

リリース日：2016 年 7 月 28 日

リーダー：

・Eric Wang, co-chair of the CSA Mobile Application Testing Initiative and

Chief Advisor at Gapertise（台湾）

・Douglas Lee, co-Chair of the CSA Mobile Application Testing Initiative and

Head, Solutions Architecture, Strategic ISV Partners at Amazon Web Services

概要：The report details the issues of mobile app vetting from a life-

cycle perspective, mobile app development management, mobile app coding, and audit management security issues. The group then plans to create an assessment and certification scheme white paper based on NIST special publication 800163: "Vetting the Security of Mobile Applications" and also set up a vetting plan for a mature model and mobile apps security. Also planned is the establishment of a vetting plan for mobile apps and guidance to allocate resources to resolve potential security problems or certification-period incidents.

参考 URL：https://cloudsecurityalliance.org/media/news/research-brief-cloud-security-alliance-mobile-working-group-releases-mobile-application-testing-initiative-report/

- 2016 年 7 月

1. Mobile Working Group Meeting（終了）

日時：2016 年 7 月 1 日（金） 1:00am-2:00am（JST）

会場：Online（Fuze）

司会：John Yeoh, Senior Research Analyst, CSA

概要：

- Review charter

- Discuss deliverables

- 2016 年 6 月

1. CSA Internet of Things (IoT) WG: Bi-Weekly Call

日時：2016 年 5 月 6 日（金） 2:00am-3:00pm（JST）

会場：Online

司会：Brian Russell, Chair of the CSA Working Group on Internet of Things

概要：

- Welcome

- CSA Updates

- Building the Connected Hospital - Securely

- Establishing a Safe & Secure Municipal Drone Program

- Observations & Recommendations for Connected Vehicle Security

- OAB

1. CSA Internet of Things (IoT) WG: Bi-Weekly Call

日時：2016 年 5 月 6 日（金） 2:00am-3:00pm（JST）

会場：Online

司会：Brian Russell, Chair of the CSA Working Group on Internet of Things

概要：

- Welcome

- CSA Updates

- Building the Connected Hospital - Securely

- Establishing a Safe & Secure Municipal Drone Program

- Observations & Recommendations for Connected Vehicle Security

- OAB

GUEST SPEAKER

Mike Schwartz is the Founder of Gluu, a software development company that specializes in identity and access management. Gluu has been working with several companies to design centralized security for next-generation IOT products, including the Toshiba Cloud TV, which has been launched in Japan. He participates in several working groups at the Kantara Initiaitive, an identity-focused standards organization, including the User Managed Access (UMA) working group and he co-chairs the OTTO working group, a new standard designed to enable multi-party federations using both SAML, PKI and OAuth2.

日時：2016 年 5 月 20 日（金） 2:00am-3:00pm（JST）

会場：Online

司会：Brian Russell, Chair of the CSA Working Group on Internet of Things

概要：

(1) Establishing a Safe and Secure Municipal Drone Program

(2) Observations and Recommendations on Connected Vehicle Security

(3) Designing and Developing Secure IoT Products

(4) IoT Standards

- 2016 年 5 月

1. CSA Internet of Things (IoT) WG: Bi-Weekly Call（終了）

日時：2016 年 5 月 6 日（金） 2:00am-3:00pm（JST）

会場：Online

司会：Brian Russell, Chair of the CSA Working Group on Internet of Things

概要：

1. Welcome

2. CSA Updates

3. Building the Connected Hospital - Securely

4. Establishing a Safe & Secure Municipal Drone Program

-Introduction & Overview

-Small Unmanned Aerial System (sUAS) Municipal Use Cases

-Securing Command & Control Channels

-Securing Video and Sensor Transmissions.

-Securing Cloud Integrations

-Privacy Considerations

-Safety Controls and no fly zones

-Mis-use identification

5. Observations & Recommendations for Connected Vehicle Security

-Focus on System-Wide Security

Platform and Supplier Security

Third-Party Attack Risks

   -Misbehavior Detection Mechanisms are Critical

-Establish Standards and Best Practices for Software Updates

-Establish Standards and Best Practices for Local Authentication to Infrastructure

Equipment

   -Evaluate Impacts of Future Technology

> Cloud
>
> 　　5G Communications
>
> GUEST SPEAKER
>
> 　Mike Schwartz is the Founder of Gluu, a software development company that specializes in identity and access management. Gluu has been working with several companies to design centralized security for next-generation IOT products, including the Toshiba Cloud TV, which has been launched in Japan. He participates in several working groups at the Kantara Initiaitive, an identity-focused standards organization, including the User Managed Access (UMA) working group and he co-chairs the OTTO working group, a new standard designed to enable multi-party federations using both SAML, PKI and OAuth2.

- 2016 年 3 月

1. CSA Internet of Things (IoT) WG: Bi-Weekly Call（終了）

日時：2016 年 3 月 25 日（金）　2:00am-3:00pm（JST）

会場：Online

司会：Brian Russell, Chair of the CSA Working Group on Internet of Things

概要：

　(1) Welcome New Members

　(2) Overview of IoT Initiatives

　　　-Open Peer Review for Securing the Development of IoT Devices document

（参照 URL）https://cloudsecurityalliance.org/document/securing-the-development-of-iot-devices/

（3）Connected Vehicles - Security briefing from the Federal Highway Administration（FHWA）

2．CSA Mobile Working Group Monthly Call（予定）

日時：2016 年 4 月 5 日　（金）　1:00am-2:00pm（JST）

会場：Online

概要：TBD

- 2016 年 2 月

1．CSA Internet of Things (IoT) WG: Bi-Weekly Call

日時：2016 年 2 月 26 日（金）　3:00am-4:00pm（JST）

会場：Online

司会：Brian Russell, Chair of the CSA Working Group on Internet of Things

概要：

（1）　Introduction brief on Connected Vehicles

　・IEEE 1609.2 Defines Certificate Format for use with V2V/I/X

　・SCMS Certificate Types（PoC）

・Pseudonym Certificates

・Special privacy controls

（2）　Brief on Risks to Connected Vehicles with Federal Highway

Administration

（3）　CSA Document describing our thoughts on Risks/mitigations for a

safe & secure connected vehicle environment.

2. CSA Mobile Working Group Meeting at RSA（予定）

日時：2016 年 3 月 2 日

　　　10:00am-10:30am: Mobile Application Security Testing (MAST)

working group

　　　 1:15pm- 1:45pm: Internet of Things Working Group

会場：Practising Law Institute (PLI) Center San Francisco

685 Market St., San Francisco, California, United States

（参照 URL）

https://www.eventbank.com/event/496/

- 2016 年 1 月

1. CSA Mobile Application Security Testing (MAST) Initiative について

2015 年 12 月 2 日プレスリリースを CSA-APAC より発表

"Cloud Security Alliance Releases Mobile Application Security Testing

Initiative"

https://cloudsecurityalliance.org/media/news/cloud-security-alliance-releases-mobile-application-security-testing-initiative/

White Paper Ready for Peer Review

https://s3-ap-southeast-1.amazonaws.com/csaapac/MAST/Peer+Review/MobileApplicationSecurityTestingInitiativeWhitePaper.pdf

2. CSA Internet of Things (IoT) WG: Bi-Weekly Call

日時：2015 年 12 月 18 日（金） 3:00am-4:00pm（JST）

会場：Online

司会：Brian Russell, Chair of the CSA Working Group on Internet of Things

概要：

1) CSA Updates

-CSA Summit at RSA 2016 on February 29th

-Full day of CSA speakers to kick-off RSA 2016 week

-CSA Working Groups at RSA on March 1st, 2016

-IoT Working Group to be represented

2) 2015 Recap

(a) Publishings

-Security Guidance for Early Adopters of IoT (4/15)

-Identity and Access Management for IoT 10/15

-Cyber Security Guidelines for Smart City Technology Adoption 11/15

https://cloudsecurityalliance.org/media/news/securing-smart-cities-issues-guidelines-for-smart-city-technology-adoption/

(b) Industry Collaborations

-FCC Technological Advisory Council

（関連資料は、下記 URL よりダウンロード可能）

https://www.fcc.gov/general/technological-advisory-council

-Securing Smart Cities

http://securingsmartcities.org/

3) 2016

(a) Initiatives

-Secure Design and Development of IoT Devices (2/16)

-Cloud Security for the IoT (changed from Cloud Security for Smart Cities) (Q1)

-Guidance for IoT Adopters v2 (Q2)

(b) Industry Initiatives

-Auto

-Retail

-Healthcare

-Financial (ブロックチェーン)

(c) Industry Collaborations

-FCC Technological Advisory Council

-Securing Smart Cities

-Alliance for Internet of Things Innovation

-Federal Highway Administration

-European Commission（DG Connect、ENISA）

(d) Further Engagement

-Call for papers/presenters on behalf of working group

-Awareness/participation in more IoT conferences

-Educational sessions from IoT technology providers

- 2015 年 12 月

1. **CSA Mobile Application Security Testing (MAST) Initiative について**

2015 年 12 月 2 日プレスリリースを CSA-APAC より発表

"Cloud Security Alliance Releases Mobile Application Security Testing Initiative"

https://cloudsecurityalliance.org/media/news/cloud-security-alliance-releases-mobile-application-security-testing-initiative/

White Paper Ready for Peer Review

https://s3-ap-southeast-1.amazonaws.com/csaapac/MAST/Peer+Review/MobileApplicationSecurityTestingInitiativeWhitePaper.pdf

2. **CSA Internet of Things (IoT) WG: Bi-Weekly Call**

日時：2015 年 12 月 18 日（金） 3:00am-4:00pm（JST）

会場：Online

司会：Brian Russell, Chair of the CSA Working Group on Internet of Things

概要：

1) CSA Updates

-CSA Summit at RSA 2016 on February 29th

-Full day of CSA speakers to kick-off RSA 2016 week

-CSA Working Groups at RSA on March 1st, 2016

-IoT Working Group to be represented

2) 2015 Recap

(a) Publishings

-Security Guidance for Early Adopters of IoT (4/15)

-Identity and Access Management for IoT 10/15

-Cyber Security Guidelines for Smart City Technology Adoption 11/15

https://cloudsecurityalliance.org/media/news/securing-smart-cities-issues-guidelines-for-smart-city-technology-adoption/

(b) Industry Collaborations

-FCC Technological Advisory Council

（関連資料は、下記 URL よりダウンロード可能）

https://www.fcc.gov/general/technological-advisory-council

-Securing Smart Cities

http://securingsmartcities.org/

3) 2016

(a) Initiatives

-Secure Design and Development of IoT Devices (2/16)

-Cloud Security for the IoT (changed from Cloud Security for Smart Cities) (Q1)

-Guidance for IoT Adopters v2 (Q2)

(b) Industry Initiatives

-Auto

-Retail

-Healthcare

-Financial (ブロックチェーン)

(c) Industry Collaborations

-FCC Technological Advisory Council

-Securing Smart Cities

-Alliance for Internet of Things Innovation

-Federal Highway Administration

-European Commission (DG Connect、ENISA)

(d) Further Engagement

-Call for papers/presenters on behalf of working group

-Awareness/participation in more IoT conferences

-Educational sessions from IoT technology providers

- 2015 年 11 月

1. <u>CSA Mobile Application Security Testing (MAST) Initiative について</u>

10 月 26 日ミーティングの補足資料

・White Paper の Peer Review が当初の予定（2015 年 10 月）よりも遅れて

いる。

2. <u>CSA Internet of Things (IoT) WG: Bi-Weekly Call</u>

日時：2015 年 11 月 20 日（金）　2:00am-3:00pm（JST）

会場：Online

司会：Brian Russell, Chair of the CSA Working Group on Internet of

Things

概要：

1)　CSA Updates (John Yeoh /Frank)
2)　Latest IoT Security News
3)　Research Updates, Plan and Volunteer Sign-up
　　-Published "Cyber Security Guidelines for Smart City Technology
　　Adoption"
　　-Finalizing inputs to Federal Communications Commission (FCC) TAG
　　IoT WG

Report to be provided to FCC in December

（参考）FCC IoT WG 資料

https://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting92415/TACpresentations9-15.pdf

-Continued IoTWG work on "Secure Development of IoT Devices"

     Thanks to Priya Kuber (lead) and all who are helping shape this document!

-Created collaboration document on blockchain technology's application to IoT Security

4) BlockChain Discussion

5) Secure IoT Development Document – Review & Discussion

6) Special Briefing: Insurance & the IoT

   by Dr. Shyam Sundaram（NTT データでの勤務経験あり）

Abstract: IoT is changing the paradigm in which consumers are interacting in the overall ecosystem and with the insurers. These realities will challenge the way insurers will conduct business (risk determination) based on a customer's characteristics and behaviours. This will also bring into play an increased context on the privacy and data related concerns. Insurance products that cover commercial insurance will also be impacted by these technology capabilities; this also needs to be considered from an insurance product evolution perspective as well. This talk will cover some of these aspects at a broad level.

- 2015 年 10 月

---

1. CSA Mobile Application Security Testing (MAST) Initiative Call

日時：2015 年 10 月 26 日（月）　4:00am-5:00pm（JST）

会場：Online

司会：Lynne Yang, APAC Assistant Research Analyst, CSA

概要：

(1) Introduction
-"Taiwan to launch mobile phone security certification"
http://en.ctimes.com.tw/DispNews.asp?O=HJY8ED04SAKSAA00N5
- "National Cybersecurity Center of Excellence to launch 3 new projects to provide mobile device security, attribute based access control and derived personal identity (PIV) credentials for mobile devices"
http://www.nist.gov/itl/nccoe_model_systems_controlling_access_it_assets.cfm
(2) Roadmap
- MAST Whitepaper
- Certification Scheme
- Vetting Scheme
- Resources
(3) Project updates
-Audience
　Guidance for app developers

Auditor

User

-Security Frameworks

ISO 27034

NIST's 800-163

CSA's Mobile Security Guidance

-98 mobile security vulnerabilities

(4) Next steps

-End of Content Development Phase

-CSA Working Group Peer Review

-Mobile Application Security Testing Initiative

-Mobile Working Group

-CSA Open Peer Review

(5) Questions

2. <u>CSA Internet of Things (IoT) WG: Bi-Weekly Call</u>

日時：2015 年 10 月 23 日（金）　1:00am-2:00pm（JST）

会場：Online

司会：Brian Russell, Chair of the CSA Working Group on Internet of

Things

概要：

1) CSA Updates

2) Discuss some of the latest news

<Blockchain Discussion>

-News shared by Heath

-IBM and Samsung looking at blockchain tech for IoT – ADEPT

(Autonomous Decentralized P2P Telemetry)

"uses elements of bitcoin's underlying design to build a distributed

network of devices – a decentralized Internet of Things."

-Three protocols:

   -BitTorrent (file sharing)

   -Ethereum (smart contracts)

   -TeleHash (p2p messaging)

http://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-

internet-things/

3) Work on our Secure Development of IoT Devices document

4) Pending time- Work on our Smart Cities document

- 2015 年 9 月

1. CSA Internet of Things (IoT) WG: In-person WG meeting in Las Vegas

日時：2015 年 9 月 28 日（金）　8:00am-5:00pm（現地時間）

会場：Las Vegas, USA

司会：Brian Russell, Chair of the CSA Working Group on Internet of

Things

概要：

1. IoTWG Introduction

2. Security Recommendations for Early IoT Adopters

3. IoTWG Collaborations

4. IoTWG Research Roadmap

5. New Research Discussion

　　-IoT IAM Summary Guidance

　　-Hardware Security Analysis

　　-Cloud security for Smart Cities

　　-Version 2 IoT Guidance

6. How to contribute

- 2015 年 8 月

1.　CSA Mobile WG　定例会議

日時：2015 年 8 月 14 日（金）　午前 1 時〜1 時 30 分

会場：オンライン（Fuze）

司会：John Yeoh, Senior Research Analyst, CSA

概要：

1) IoT Working Group Spin Off

　-- How to stay involved in IoT efforts

2) Mobile and Security Guidance in Cloud v4.0

3) Mobile Guidance v2.0

　-- Components

4) MAST Initiative

2. CSA Internet of Things (IoT) WG 定例会議

日時：2015 年 8 月 14 日（金）　午前 2 時〜3 時

会場：オンライン（join.me）

司会：Brian Russell, Chair of the CSA Working Group on Internet of

Things

概要：

1) Recap from 7/30/2015 Discussion
2) IoT Security News of the week: Discussion & Analysis
3) IoT in Health Care Discussion
4) IoT in the Cloud Discussion
5) Working Group Research Efforts

　-Security Guidance for the IoT v2

　-Industry-specific Guidance

　-Summary Guidance Sheets

　-IAM for IoT　（パブリックコメント募集中）

　-Hardware Security Analysis

　-Automotive Cyber Security Research (proposed)

- 2015 年 7 月

1.

1. CSA Mobile Application Security Testing (MAST) initiative

・2015 年 7 月は、Proposed Project Charter のピアレビュー作業を実施

・現時点で、日本より 3 名が MAST のボランティア活動に参画中

・Deliverables/Activities 計画

　<Q3 2015>

　　-Deliverables: Charter

　　-Deliverables: Project Plan

　　-Activities: Project Execution

　<Q4 2015>

　　-Activities: Project Execution

　　-Deliverables: Mobile Application Vetting Whitepaper

　<Q2 2016>

　-Deliverable:　Proposed Application Vetting Scheme

　（参考文献）

-　「NIST Special Publication 800-163: Vetting the Security of Mobile

Applications」（2015 年 1 月）

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf

2. CSA Internet of Things (IoT) WG　定例会議

日時：2015 年 7 月 31 日（金）　午前 2 時～3 時

会場：オンライン（join.me）

司会：Brian Russell, Chair of the CSA Working Group on Internet of Things

概要：

1) Discussion- latest news on IoT Security

2) Opportunity to collaborate with the FCC IoT efforts

3) Quick discussion on plans for collaboration with IOActive

4) Smart City guidance document discussion - potential for CSA Asia to lead?

5) Last call prior to peer review - IoT IAM Summary Guidance

6) Call for WG review - IoT Device Security Checklist

7) Discussion - Hardware Security Analysis of IoT Devices (Priya)

8) Other items

2015 年 8 月に、「Identity and Access Management for the Internet of Things - Summary Guidance」のパブリックコメントを募集する予定

- 2015 年 6 月

1. CSA Mobile Working Group Monthly Meeting

日時：2015 年 6 月 19 日（金）午前 1 時〜2 時

会場：オンライン（join.me）

司会：John Yeoh、CSA Research

概要：

(1) MAST Initiative

The Mobile Application Security Testing (MAST) initiative will develop a white paper outlining challenges and guidelines to mobile application vetting.

- Outline for review

- Review reference documents on application vetting and management: NIST 800-163, ISO 27034

- Call for volunteers: identifying SMEs and key stakeholders in mobile application development

Discussion

- What are the next steps?

Idenifying SMEs to key stakeholders to particpate and contribute

Review the current outline and reference docs

(2) Other Mobile Working Group Initiatives

- Reviewing components of Mobile Security Guidance v1.0

- Identifying initiatives for v2.0

- Execute project plan and call for volunteers

(3) Internet of Things (IoT)

IoT initiative is now the IoT Working Group

- Calls follow Mobile Working Group at 10am (Pacific Time)

- Next call is July 16th, 10am Pacific

2. CSA Internet of Things (IoT) Initiative Bi-Weekly Meeting

日時：2015 年 6 月 19 日（金）　午前 2 時〜3 時

会場：オンライン（join.me）

司会：Brian Russell, Chair of the CSA Working Group on Internet of Things

概要：

(1) Industry-specific security use case guidance

　・SMART Cities

　　-India

　・SMART Retail

　・SMART Health

　　-Telemedicine

(2) Practical Guidance

　・IdM for IoT (Arlene Mordeno)

　・Auditing the IoT (Arron Guzman)

　・Authentification Options for the IoT (Girish Bhat)

(3) Focused Research Reports

　・Hardware Security Options for IoT (Priya Kuber)

・RFID of Rogue IoT device (Drew Van Duren)

- 2015 年 5 月

1. <u>CSA Mobile Working Group Monthly Meeting</u>

日時：2015 年 5 月 22 日（金）午前 1 時〜1 時 30 分

会場：オンライン（join.me）

司会：John Yeoh、CSA Research

概要：

(1) RSA Recap

4 月 20 日の CSA Summit 2015、21 日の IoT Initiative、22 日の Mobile

Application Security Testing (MAST) Initiative に関する状況報告

(2) Mobile Application Security Testing (MAST) Initiative

Kick-off meeting → ボランティア募集　に向けて準備中

(3) Mobile Guidance v2.0 and CSA Security Guidance v4.0

当初は、CSA ガイダンス v4.0 と同期しながら Mobile ガイダンス v2.0

を進める方針だったが、モバイル独自のトピックがいろいろと出てきて

いるので、別個に策定作業を進める。

2. <u>CSA Internet of Things (IoT) Initiative Bi-Weekly Meeting</u>

日時：2015 年 5 月 22 日（金）　午前 2 時～3 時

会場：オンライン（join.me）

司会：Brian Russell, Chair of the CSA Working Group on Internet of Things

概要：

(1) RSA In-Person WG Meeting Summary

　　4 月 21 日サンフランシスコで開催したオフラインミーティングの状況報告

(2) Proposed Roadmap for IoT WG

　　　「New Security Guidance for Early Adopters of the IoT」の次の成果物

(3) Discussion on IoT and the Cloud

　　Secure IoT Reference Architecture のモデルとしてどんなものがあるか

(4) Discussion on IoT Hardware Security

(5) Guest Speaker - Joe Gaska from Xively on IoT

　　Xively は、IoT 向けクラウドストレージのサービスプロバイダー

　　（参考 URL）　https://xively.com/

(6) 次回オンラインミーティング

・6 月 5 日（金）午前 2 時より開催予定

・IoT 向け PKI/IAM テクノロジー企業 GlobalSign の LaChance 氏が、特別

ゲストとしてプレゼンテーションを行う予定。

- 2015 年 4 月

1. CSA Legal Information Center Seminar

日時：2015 年 4 月 20 日（月）午後 4 時 20 分〜5 時 15 分

会場：PLI Center, 685 Market Street, San Francisco, CA 94103

概要：パネルディスカッション

「Be Prepared for Big Data and Internet of Things」

前半：「Technical Overview of Big Data and the Internet of Things」

[パネラー①] Dr. PA. Subrahmanyam, Co-Chair of the CSA Working

Group on Big Data

[パネラー②] Brian Russell, Chair of the CSA Working Group on Internet

of Things

・Mobile WG が傘下のサブグループとして立ち上げた「IoT Initiative」の

リーダーとして「New Security Guidance for Early Adopters of the IoT」

策定に貢献。

・Council on Cybersecurity の 20 Critical Controls Editorial Panel とし

て、Unmanned Aerial Vehicles (UAVs)、Connected Cars などの制御セキ

ュリティにも精通している。

後半：「FTC position on Big Data and Internet of Things」

[パネラー③] Laura Berger, Attorney, Division of Privacy and Identity

Protection, FTC

・FTC の場合、ビッグデータに関わりの深いデータ・ブローカーの判例が過

去にたくさんあり、それらを参考にしながら法規制の方向性を検討してい

る。また、消費者保護の観点から、アドネットワークの問題に関心を持って

いる。

・EU 諸国のビッグデータ／IoT に関わりの深いプライバシー保護指令改正

の状況に関しては、CSA-EMEA の Daniele Catteddu 氏が補足説明（最終

的には EU 全加盟国の承認が必要で、確定するのは早くても 2018 年頃。そ

れまでの間は、現行の CCM や STAR を有効活用する方策を考えた方が現実

的ではないかとのこと）。

2. CSA Internet of Things (IoT) Working Group Meeting

日時：2015 年 4 月 21 日（火）　午前 10 時 15 分〜11 時 30 分

会場：PLI Center, 685 Market Street, San Francisco, CA 94103

演者：Brian Russell, Chair of the CSA Working Group on Internet of Things

概要：

(1) Welcome, Thanks and Definitions

(2) IoT Challenges

(3) IoT Threat Discussion

(4) Recommended IoT Security Controls

(5) WG Roadmap for 2015

(6) Q&A

・Mobile/IoT WG の会合に初参加というメンバーが多かったので、IoT イニシアティブの今までの活動状況、4 月 20 日に発表した成果物「New Security Guidance for Early Adopters of the IoT」等の説明が中心だった。

・Mobile WG は、進行中の Mobile Security Guidance 2.0 の策定作業に加えて、IoT、アプリケーション・セキュリティ・テスティング等、新規分野のインキュベーターとしての役割も積極的に担う方針である。

・IoT WG としては、エンタープライズ市場に重点を置きながら、4 半期に 1 本リサーチレポートを発行する方針である。

（2015 年の IoT WG ロードマップ）

3. Mobile Application Security Testing Kick-off Meeting

日時：2015 年 4 月 22 日（水）午前 9 時～10 時

会場：EMC Offices: 250 Montgomery Street (4th Floor) Russian Hill

Conference Room

演者：Constant Lee, Gapertise Mobile Vetting Service

　　　（CSA Executive Member, Taiwan）

概要：（Proposed Charter）

Mobile Applications are becoming an integral part of not just modern enterprises but also of human existence and a huge part of this shift is due to the emergence of cloud computing. Cloud computing has allowed for the instantaneous utilization of applications which imparts tremendous agility to the enterprise. Accompanying such convenience are risk management challenges due to a lack of transparency, leading to security concerns that include applications.

The project will aim to create a safer cloud eco-system for mobile applications by creating systematic approaches to application testing and vetting that helps integrate and introduce quality control and compliance to mobile application development and management.

The project hopes that more research into mobile application security vetting and testing will help reduce the risk and security threats that organizations and individuals expose themselves to by using mobile applications.

（Project Responsibilities）

Specific fields of action of the initiative could include:

・To develop a whitepaper for vetting and certification scheme based off the NIST Special Publication 800-163: Vetting the Security of Mobile Applications;

・To develop a certification scheme for mobile application security with a maturity model;

・To develop a vetting scheme (i.e. approval-rejection basis) for mobile applications;

・To develop resources for addressing potential security issues or an incident during certification period.

（Scope）

・The app security testing and vetting process uses both static and dynamic analysis to analyse the application. The testing and vetting process covers permissions, exposed communications, potentially dangerous functionality, application collusion, obfuscation, excessive power consumption and traditional software vulnerabilities. The testing covers the internal communications such as debug flag and activities and external communication such as GPS, NFC access as well as checking the links that is written in the source code.

・In addition to security testing and vetting, the project will also develop processes and procedures for security incidence response.

- 2015 年 3 月

Mobile Working Group Monthly Call
-2015 年 2 月 27 日（日本時間）に、全体 Monthly Call を開催

-アジェンダ

(1) Mobile Guidance v2.0 content
（参考）IoT に関連する定義の変更

Section 1 Mobile Definition
1.0 Mobile Computing Definition　　（Inclusion of new mobile devices）
1.1 What Is Mobile Computing?　　（Add IoT to definition）
1.2 What Comprises Mobile Computing?　（Add IoT, reference separate IoT document, Inclusion of laptops）
1.3 The Characteristics of Mobile Computing　（Add IoT）
(2) Guest Speaker:
Majid Bemanian - Director of Marketing at Imagination Technologies. Majid is a High-tech industry veteran with broad hands-on experience in engineering, marketing and business management in the area of Cloud Computing and Embedded Systems (IoT). Before Imagination, Majid held various senior positions at Applied Micro, LSI, Raytheon Semi, Encore Video, Ascom-Timeplex and several early stage startups.
（参考）Imagination Technologies

http://www.imgtec.com/jp/
2. IoT Security Guidance for Early Adopters
-2015 年 2 月 27 日（日本時間）に、IoT サブグループの Call を開催

-アジェンダ

Finalize "IoT Security Guidance for Early Adopters" paper
（参考）ドキュメントの主要項目（例）

[1] Analyze privacy impacts to stakeholders and adopt a Privacy-by-design approach to IoT development and deployment
[2] Apply a Secure Systems Engineering approach to architecting and deploying a new IoT System.
[3] Implement layered security protections to defend IoT assets
[4] Define Life Cycle Security Controls for IoT devices
[5] Define and implement an authentication/authorization framework for the Organization's IoT Deployments
[6] Define a logging and audit framework for the Organization's IoT ecosystem
[7] Develop safeguards to assure the availability of IoT-based systems and data

[8] Information Sharing

- 2015 年 2 月

1. Mobile Working Group Monthly Call

-2015 年 1 月 31 日（日本時間）に、全体 Monthly Call を開催

-アジェンダ

(1)2015 Roadmap

(2)CSA Mobile Guidance v2.0

IoT の項目を追加する（Taxonomy パートの策定作業から動いている）

(3)Security Guidance for Critical Areas of Focus in Cloud Computing v4.0

新たに Mobile Domain を追加する

(4)IoT Security Guidance for Early Adopters　　*詳細は 2. 参照

(5)ゲストスピーカーによるレクチャー

Lasse Andresen, CTO and co-founder at ForgeRock,

http://www.forgerock.com/en-us/

*トヨタ自動車が主要ユーザーの 1 社

*ノルウェーのスタートアップ企業支援も手掛けている

2. IoT Security Guidance for Early Adopters

-2015 年 1 月 31 日（日本時間）に、IoT サブグループの Call を開催

-アジェンダ

(1)FTC IoT Report

FTC Report on Internet of Things Urges Companies to Adopt Best Practices to

Address Consumer

Privacy and Security Risks (January 27, 2015)

http://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-

urges-companies-

adopt-best-practices

> FTC Internet of Things - Privacy and Security in a Connected World (NOV 19, 2013)
>
> http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world
>
> (2)IoT Security Guidance for Early Adopters
>
> 4 月の RSA カンファレンスでの公開を目標に作業進行中。　現在は、IoT Taxonomy のレビューが中心。
>
> Privacy and the IoT に関して、EU の動向を反映させる　＋APAC の取組の情報があれば
>
> 日本から 2 名（二木さん、笹原）Contributors に入っている

- 2015 年 1 月

  - 2014 年 12 月 5 日午前 3 時～(日本時間)　IoT サブグループの月例電話会議がありました。

  - 電話会議では、このようなことが話し合われました。

Logging/Audit Discussion:

- General Discussion on logging. Could have a built-in API that calls back for state information. Make sure you understand what data you need to capture.

- Working in mobile/wireless sector, it takes 1000x as much energy to transmit a bit over radio. Not feasible for low power devices to generate logging data (drains battery).

- There is a logical extension of a "thing" to the cloud. Exists in both a physical form and virtual form.

- Think about what actually provides the data? A single sensor or a consolidation of sensors. Perhaps a good architecture involves multiple layers – endpoints logging to a consolidator.

- We need to define profiles of IoT devices; will drive recommended architectures
    - Where you log depends heavily on the profiles
    - Need a taxonomy for the types of "things"

- Types of data for collection
    - Info the thing is detecting (e.g., water temp)
    - Info about myself (internal state, on/off, last transmission time)

- Individually this info is disposable, but if lots of sensors go quiet then there is an issue

- Data Analytics: Would sensors in infrastructure feed data to traditional SIEMs

- o Traditional SIEMS don't work for raw feeds from sensors; too much volume.
- o Understand sensor data, aggregate information, send event to SIEM.

Action: Two Scenarios for logging/audit

- What does the logging architecture look like in these industry-based scenarios?
- What are the minimum data elements to log at the endpoint?
- Are there aggregation points?
- What types of security relevant information would be passed from the aggregation points to the SIEMs

<u>Manufacturing</u>: Jarrod Stenberg & Aaron Guzman

<u>Health Care:</u> Brian Russell & Geoff Web

<u>**Privacy and the IoT**</u>

1) Do you see that identifying privacy concerns within an IoT-based system is any different than a traditional enterprise computing system? Why/Why not?

2) What questions would you ask while performing a privacy assessment for an IoT-based system?

3) What resources can you point the group to related to privacy regulations and/or best-practices?