IGF2015 セキュリティ関連の議論

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
インターネット推進部・IP事業部
奥谷泉

Copyright © 2016 Japan Network Information Center

IGF 2015
セキュリティ関連のセッション

Type: **Cybersecurity And Trust** [Clear Filter]

Tuesday, November 10

09:00	WS 13 Keeping Your Credentials Secure Online: A Roundtable
11:00	WS 118 How communities restore trust in the digital environment

Wednesday, November 11

10:00	WS 131 Commonwealth approach on National Cybersecurity Strategies
12:00	WS 141 Law enforcement in a world where encryption is ubiquitous
14:00	WS 111 Understanding Effective Cyber Security Capacity Building
	WS 160 Managing security risks for sustainable development
	WS 6 Child Online Protection through Multistakeholder Engagement
16:00	WS 195 Hancel: a mobile tool for safety of journalists
	WS 28 Multistakeholder Solutions for Youth-Produced Sexual Content

Thursday, November 12

14:00	WS 190 Evolving Cyber Assurance across Societies & Supply Chains
16:30	WS 17 Cybersecurity Awareness though Multistakeholder outreach

Friday, November 13

11:00	WS 186 A multistakeholder and humanrights approach to cybersecurity

- Best Practice Forum
- Critical Internet Resources
- Cybersecurity and Trust
- Dynamic Coalition
- Emerging Issues
- Enhancing Multistakeholder Cooperation
- Inclusiveness and Diversity
- Internet and Human Rights
- Internet Economy
- Main Session
- Open Forum
- Openness
- Other
- Pre-Event

合計12セッション＋メインセッション

https://www.intgovforum.org/cms/igf-2015-schedule

Copyright © 2016 Japan Network Information Center

IGFにおけるセキュリティ関連の議論傾向

- **ここ数年着目されてきたテーマ**
  - 特にスノーデン事件以降、国防とプライバシー
  - サイバー犯罪への対応、より一歩踏み込んだ連携
  - 昨年のBest Practices Forum(最適事例紹介)のテーマも5つ中、2つはセキュリティ関連
- **IGF2015ではメインセッションが開催され、2014と同じBest Practices Forumのテーマ継続**
  - Establishing and supporting Computer Security Incident Response Teams (CSIRTs) for Internet security
  - Regulation and Mitigation of unsolicited Communications
- **パリのテロ事件を受け、今後サイバース空間と国防が着目される可能性**

Copyright © 2016 Japan Network Information Center

セキュリティに関わる主な議論

- **国防とプライバシー、広範囲の監視**
  - IETFではプロトコルレベルで対策
- **法執行機関からの要請とプライバシー**
  - Backdoor Decryptionを認めるか等
- **サイバー犯罪対策への整備**
  - 実社会での違法行為はオンラインでも違法
- **国境のないインターネット上で、国をまたがる犯罪に対する国際連携・国際条約**
- **国の中での各種関係者の連携整備・強化**
- **サイバー犯罪と迷惑メールの影響の区分け**
- **迷惑メールの経済的コスト**

Copyright © 2016 Japan Network Information Center

メインセッションでの議論

- **Enhancing Cybersecurity and Building Digital Trust：** http://igf2015.intgovforum.org/event/4bog/enhancing-cybersecurity-and-building-digital-trust
- **各種関係者による連携強化の必要性**
  - Collaborative Security (ISOC)
  - 米国：Cyber Security Framework(官民間の連携、民間に対する任意の枠組み)
  - サイバーセキュリティの問題はもはや技術コミュニティのみの問題から離れている、一方、政府のみで対応するべきものでもない
  - 技術的な対応、国際協定、信頼できる技術標準の設定、データ保護対策に分けた検討
- **IoT等人を介さない通信におけるセキュリティ**
- **サイバーセキュリティと人権のバランス**

Copyright © 2015 Japan Network Information Center

暗号化がユビキタスな環境での法執行

- **WS 141 Law enforcement in a world where encryption is ubiquitous**
  - 法執行機関の関係者、暗号化技術の推奨を進めているIETF関係者が着目
  - https://www.intgovforum.org/cms/igf-2015-schedule
- **プライバシー保護のために、広範囲への監視対策として暗号化強化・一般化された場合の法執行のあり方**
  - 広範囲の監視ができていた今までが特殊な環境 ？
  - 他の手段の有無、人命に関わる場合どうするか？
  - 裏で複合化を認めるべきか？結局セキュリティホールにつながり、犯罪推奨につながらないか？

Copyright © 2016 Japan Network Information Center

インターネットセキュリティのためのCSIRTの設立と支援

- **2014からBest Practices Forum(BPF) が開始、2015年も継続**
  - 2014：CSIRTの役割の誤解がCSIRTコミュニティ以外から多いことへの対応に重点
  - セルビアでのCSIRT新設につながった
  - OECD、CSIRTコミュニティ、FIRSTなどでのインプットを受け2015年もBPFを継続
- **2015年の継続課題**
  - CSIRTの定義を実情の役割は一致しているか
  - CSIRTによる活動を効果的にするための影響の拡張
  - CSIRT間の信頼、情報交換
  - 法執行機関との連携

Copyright © 2016 Japan Network Information Center

IGF BPF：CSIRT　概要

- スイスSWITCH、韓国KrCERT/CC等の事例紹介

- CSIRTとプライバシー、CSIRTと公共政策、CSIRTと法執行機関、文化の違い、責任ある情報開示などのテーマをカバー

- 14のCSIRTに関わる推奨

http://www.intgovforum.org/cms/best-practice-forums/2-establishing-and-supporting-csirts

Copyright © 2016 Japan Network Information Center

IGF BPFによる推奨：CSIRT

- **Recommendation 1:**
  - There is a need for policymakers to discuss the role of CSIRTs with the CSIRT community to avoid misconceptions around the role of CSIRTs.
- **Recommendation 2:**
  - CSIRTs are recommended to be actively involved in relevant policy discussion at both the national and international level. In order to engage with other stakeholders it is important to be where they are. The provided examples show that it brings influence and understanding.
- **Recommendation 3:**
  - Every government has the right to create the CSIRT it needs. It is recommended though that governments make an informed decision, taking into consideration the potential consequences of their choice.
- **Recommendation 4:**
  - Where CSIRTs are concerned privacy and security have to stand together in order for a CSIRT to be truly successful.
- **Recommendation 5:**
  - Data protection is a term that is better understood in a general sense than privacy. Hence it is advised to use this term in a CSIRT context more as it is far more concrete.
- **Recommendation 6:**
  - Data protection has to be at the core of the work of a CSIRT.

JPNIC

Copyright © 2016 Japan Network Information Center

IGF BPFによる推奨：CSIRT(続)

- **Recommendation 7:**
  - It is recommended to involve Data Protection Commissioners more in the work of CSIRTs.
- **Recommendation 8:**
  - To ensure transparency and accountability where data protection is concerned, it is advised to make a study whether a standard protocol can assist attaining transparency, as well as more conscious decisions about limits to data sharing, anonymization of data where possible and the handling of data by CSIRTs.
- **Recommendation 9:**
  - CSIRTs should minimize data collection and processing, while also focusing on their constituency and anonymizing relevant information.
- **Recommendation 10:**
  - A well-run CSIRT is an essential part in the protection of data and security within a society.
- **Recommendation 11:**
  - Further study is recommended into the expanding role of CSIRTs. This could e.g. include whether there are sensible limits to tasks given and what role a CSIRT can play in enhancing cooperation in the security chain between other stakeholders, e.g. manufacturers of ICT products and providers of ICT services and does the current definition of a CSIRT match the reality of work asked and tasked.

Copyright © 2016 Japan Network Information Center

IGF BPFによる推奨：CSIRT(続)

- **Recommendation 12:**
  - Further study is recommended into the ways CSIRTs and law enforcement can enhance their cooperation in meaningful ways, each from within its respective mission.
- **Recommendation 13:**
  - Further study is recommended into responsible disclosure and how to create conditions that ethical hackers can contribute to a safer Internet experience for all.
- **Recommendation 14:**
  - CSIRTs have a role in handling effects of cybercrimes and providing technical support for investigations, but cybercrime is overall crime and as such should be dealt by law enforcement entities, like the police. Containing too much of this work within a CSIRT, or making a CSIRT part of a law enforcement agency is likely to have significant impact on its ability to work with the private sector.

Copyright © 2016 Japan Network Information Center

求められていない通信の規制と回避

- THE REGULATION AND MITIGATION OF UNSOLICITED COMMUNICATIONS
- 2014年：技術標準、最適事例、迷惑メール対策に関する各国の規制を紹介
- 2015年：スパムに限定しない求められない通信の問題を対象とし、統計、対策に向けた各種関係者による連携の事例、アクセスと途上国における問題との関連性を紹介
- 9点の推奨

http://www.intgovforum.org/cms/best-practice-forums/regulation-and-mitigation-of-unsolicited-communications

Copyright © 2016 Japan Network Information Center

IGF BPFによる推奨：求められていない通信への規制と回避

- **Recommendation 1:**
  - That newly connected economies consider multistakeholder anti-botnet efforts (botnet mitigation centers) as they have a role in reducing the number of infections on end users' devices.
- **Recommendation 2:**
  - That effort be taken by law enforcement to categorise crimes undertaken using the Internet.
- **Recommendation 3:**
  - That governments and law enforcement take proactive steps to encourage the reporting of cybercrime by all users: citizens and industry.
- **Recommendation 4:**
  - That further attention ought to be given to surveying the needs of African nations (and other developing nations), not only in dealing with the problem of spam, but the broader issues of cybersecurity and cyber safety.
- **Recommendation 5:**
  - That there is a need for basic cybersecurity training, including in relation to the mitigation of unsolicited communications, in the African region and perhaps other regions of the globe. Active participation from other regions is recommended. An example could be to organise workshops at the African Internet Summit.

Copyright © 2016 Japan Network Information Center

IGF BPFによる推奨：求められていない通信への規制と回避(続)

- **Recommendation 6:**
  - That there is a need for education of citizens, including children, on matters relating to cybersecurity in economies coming newly online.
- **Recommendation 7:**
  - That industries affected by spam, phishing, etcetera must continue to evolve in order to protect their own reputations and to ensure that their own customers do not become victims; including the provision of funding for education programs.
- **Recommendation 8:**
  - That further consideration ought to be given to producing simple lists of low or no cost initiatives that can assist newly-connected economies to protect their infrastructure.
- **Recommendation 9:**
  - That consideration ought to be given by newly connected economies to a wide variety of multi-stakeholder arrangements, including public-private and private-private initiatives in combating unsolicited communications.

Copyright © 2016 Japan Network Information Center

まとめ

- セキュリティに関する議論は今後もインターネットガバナンスの場で着目される可能性大
- 特に既存の関係者間の連携をどう強化していくか、国防や法執行機関による対応とプライバシーのバランスは継続課題
- 2016年もBest Practices Forumのテーマとしてセキュリティに関するものが選ばれた場合、日本の知見・経験の共有、不適切な内容が反映されないかの確認をより能動的にするべきか。その場合、どう対応できるのか。

Copyright © 2016 Japan Network Information Center