「ICT フォーラム 2014in 東京」開催報告書

日時：2014 年 9 月 26 日（金）13:30～17:35
場所：コンベンションルーム AP 渋谷（A+B）

主催：一般社団法人日本インターネットプロバイダー協会（JAIPA）
一般財団法人日本データ通信協会 テレコム・アイザック推進会議（Telecom-ISAC Japan）
協賛：日本マイクロソフト株式会社
後援：総務省
参加者：93 名
プログラム：
13:00～受付開始

13:30～13:35　開会挨拶
　一般社団法人日本インターネットプロバイダー協会　監事　秋山 卓司
13:35～14:30　基調講演「サイバーセキュリティ政策の現状と通信の秘密について」
　情報セキュリティ大学院大学教授
　情報セキュリティ政策会議構成員　林 紘一郎氏
14:30～15:10　Telecom-ISAC Japan セッション
「スポーツイベントとサイバー攻撃の妖しい関係」
　一般財団法人日本データ通信協会 テレコム・アイザック推進会議
　ステアリング・コミッテイ運営委員
　株式会社インターネットイニシアティブ
　サービス本部 セキュリティ情報統括室　室長　齋藤 衛氏
15:10～15:20　休憩
15:20～16:00　総務省講演「総務省のサイバーセキュリティ政策と通信の秘密について」
　総務省 情報流通行政局 情報セキュリティ対策室　室長　赤阪 晋介氏
16:00～16:40　JAIPA セッション
「大量通信ガイドラインの執筆を終えて、主な変更点と今後の展望」
　一般社団法人日本インターネットプロバイダー協会　会長補佐
　ニフティ株式会社 経営推進室 経営戦略推進部　担当部長　木村 孝氏
16:40～17:30　特別講演「通信の秘密とサイバーセキュリティ対策」
　一般財団法人日本データ通信協会 テレコム・アイザック推進会議
　会長　飯塚 久夫氏
17:30～17:35　閉会挨拶
　一般財団法人日本データ通信協会 テレコム・アイザック推進会議
　企画調整部　部長　佐藤 晴樹

概要：

基調講演として情報セキュリティ大学院大学　教授 林 紘一郎氏には、「サイバーセキュリティ政策の現状と通信の秘密について」としてサイバーセキュリティを取り巻く課題と政府の取り組みについて理解を促しつつ、通信の秘密に関する学識者としてのお考え、実務者が見過ごしがちな視点や論点について、お話しいただきました。

次に Telecom-ISAC Japan セッションについては、Telecom-ISAC Japan 運営委員 / IIJ 齋藤衛氏に「スポーツイベントとサイバー攻撃の妖しい関係」として、林先生の講演内容を踏まえつつ、現実のインターネットの世界に焦点をあてます。特に、2020 五輪に沸き立つ日本、しかし国際的なスポーツイベントの裏側では、相手国の関連サイトへの DDoS 攻撃が常態化している。最近ではアノニマスによる攻撃に加え、ネットゲームや SNS でのトラブルが大規模な攻撃に発展した事例もある。リフレクション攻撃など最新のサイバー攻撃の実態と通信の秘密の関係について、サイバー攻撃対策の専門家の知見をご披露いただきました。次は、総務省講演です。総務省 情報流通行政局 情報セキュリティ対策室　室長 赤阪 晋介氏による「総務省のサイバーセキュリティ政策と通信の秘密について」を林先生の政策・法律面からのご意見や、齋藤さんの実務面での課題を踏まえ、総務省が通信の秘密の具体的な一歩をどう踏み出したのか、消費者行政課の担当分野も包含して、実務者にわかりやすい論点をご紹介いただきました。次は、JAIPA セッションです。JAIPA 会長補佐/Nifty 木村孝氏による「大量通信ガイドラインの執筆を終えて、主な変更点と今後の展望」として、ガイドラインの解説に近い実務的な説明をしていただきました。

最後に特別講演として、一般財団法人日本データ通信協会 テレコム・アイザック推進会議　会長　飯塚久夫氏による「通信の秘密とサイバーセキュリティ対策」です。サイバーセキュリティ攻撃など様々な問題に対して、参加者を始めとする通信事業者や ICT 関係者を鼓舞し、日本が一丸となって取り組んでいくメッセージをいただきました。

半日開催でしたが、それぞれの立ち位置や方向性をお話しいただくには、最適な講師の方々で、参加者にも分かり易くご説明いただきました。沖縄 ICT フォーラム in 久米島でのセッションが生み出した、踏み込んだ講演になったかと思います。引き続き様々なところで、このようなミニセッションを行えたらと思っております。

ICTフォーラム2014 in 東京

日時：2014年9月26日（金）13:30～　　場所：AP渋谷
参加者数：93名　　回答者数：56名（60%）

時間配分は適切でしたか？	長い	3	5.4%
	ちょうど良い	45	80.4%
	足りない	1	1.8%

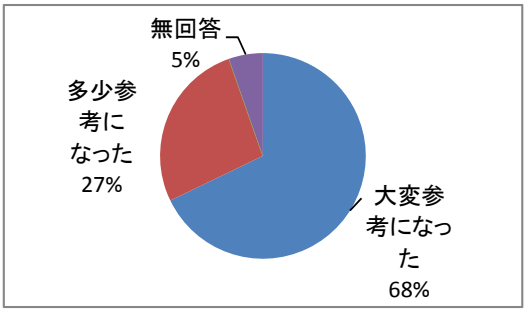
今回のセミナーの参加目的をお聞かせください。また、どのプログラムに興味がありましたか。

- IoT時代の情報セキュリティの動向調査。サイバーセキュリティ政策の現状と通信の秘密について、と、スポーツイベントとサイバー攻撃の妖しい関係
- ISPとしてセキュリティ対策を考えるきっかけにする為
- ISPの運用業務の中で、ますます増加するサイバー攻撃とそれに伴い注目される情報セキュリティについて、現在の動向を知りたかった。
- Telecom-ISAC Japan Session
- お客様対応時の通信の秘密に関する考え方の把握
- 官民連携プロジェクト等の情報収集
- 業界、政策の動向を掴むため
- 講演内容に興味があり
- 最近の「通信の秘密」取扱動向が知りたい
- 最近のサイバーセキュリティの課題や政策についての情報
- 最新のセキュリティ対策動向
- サイバー・セキュリティの知見を深めるため
- サイバー攻撃ガイドと大量通信ガイドに関わらせていただきましたため
- サイバー攻撃に関する情報収集
- サイバーセキュリティ政策の現状と通信の秘密について
- サイバーセキュリティ動向と政策に関しての情報収集
- サイバーセキュリティと通信事業者としての法的関係を知るため
- サイバーセキュリティに関する情報収集
- 情報収集のため
- 情報通信と通信の秘密の再認識
- スポーツイベントとサイバー攻撃の－
- セキュリティ最新動向
- セキュリティ政策動向の理解、通秘に関する理解
- セキュリティ対策
- セキュリティ対策の最新状況の把握
- セキュリティ対策の知見を得るため
- セミナー内容に興味あったコト、上司の指示
- 全部
- 総務省のサイバーセキュリティ政策と通信の秘密について、と、通信の秘密とサイバーセキュリティ政策
- 総務省のサイバーセキュリティ政策と通信の秘密について
- 大変参考になりました。
- 通信の秘密に関する現状の把握
- 通信の秘密に関する理解のため
- 通信の秘密について、最新動向を知るため
- 通信の秘密により阻害されているセキュリティビジネスの将来性検討の参考のため
- 通信の秘密の在り方に関心があり参加した。参考になった。
- 通信の秘密の過去～現在～未来の解釈・取組を理解したかったため
- 通信の秘密始め諸規制について知見を深める。
- 通秘とセキュリティ問題
- 通秘の新たな考えの理解
- 通秘の新たな考えの理解問題を正しく理解するため。非常によかった
- 目的：ガイドライン上、総務省でのDoS攻撃対する策の見会について

それぞれの講演はいかがでしたか？

a. サイバーセキュリティ政策の現状と通信の秘密について

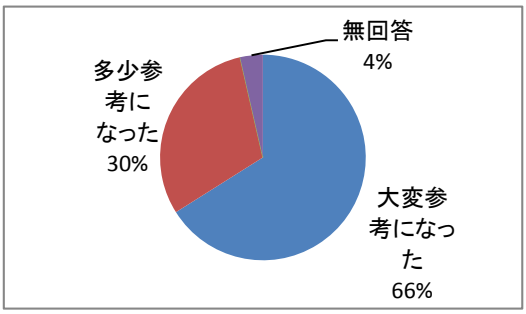
大変参考になった	38	67.9%
多少参考になった	15	26.8%
参考にならなかった	0	0.0%
無回答	3	5.4%



- セキュリティ政策の現状が理解できた
- 通信が電話であった時代と現在とを比べ、時代に合った政策法律改正の必要性をわかりやすく話していただいた。
- 通信の秘密・他人の秘密の分析を通じ、本当にあるべき通信の秘密を定義し、使えるようにしてほしい
- 通信の秘密が海外では重視されていないことは気になった
- テクノロジーと新たなサービスの進化に規制はもはや追い付けません。通信の秘密は、発信者と受信者が責務を負うモデル（内容の暗号化）も検討してはいかがでしょう
- 電気通信事業者以外についての法適用について、米国での通信の秘密について。とても参考になりました。
- 電気通信に係る日本の歴史について大変勉強になった
- 短いです。もっともっと詳しく聞きたかったので、又お願いします。

b. スポーツイベントとサイバー攻撃の妖しい関係

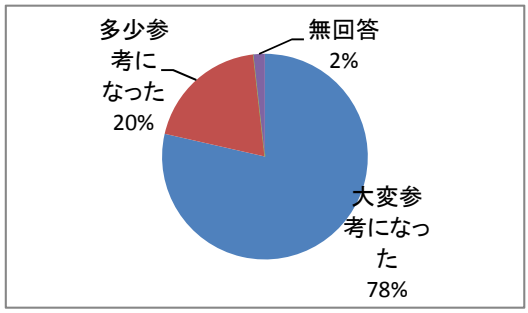
大変参考になった	37	66.1%
多少参考になった	17	30.4%
参考にならなかった	0	0.0%
無回答	2	3.6%



- いつも通り
- 資料があればよかった
- 対策の必要性を感じた
- IOTへの危機感を強めました
- ガイドラインの中ではあるが、DNSampへの対処が「正当業務行為」として扱われることに大きな驚きを感じた。
- 資料欲しい（差しさわりのない範囲で）
- 身近な話題が多く、また話も聞きやすく勉強になりました。
- 笑いありでありつつも将来について考える上で参考になった

c. 総務省のサイバーセキュリティ政策と通信の秘密について

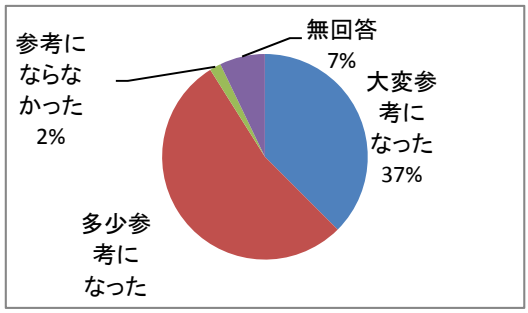
大変参考になった	44	78.6%
多少参考になった	11	19.6%
参考にならなかった	0	0.0%
無回答	1	1.8%



- 国として政策の方向性が分った
- 国の斬新な取り組みについてよく理解できた
- よくまとまってました
- M2Mなど次世代のセキュリティ対策について参考となった。わかりやすかった。
- 資料の文字、絵が小さく、見難い所だけ、残念です
- 政府主導・連携のプロジェクトの活動内容とその結果がフィールドバックされて、進歩してきたことを理解できた。

d. 大量通信ガイドラインの執筆を終えて、主な変更点と今後の展開

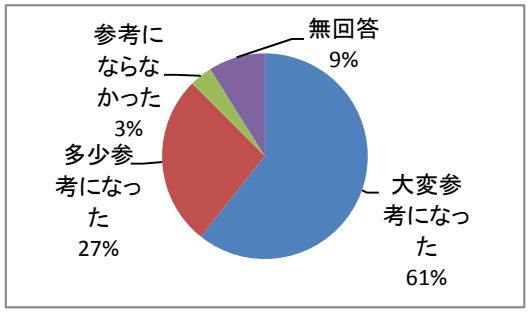
大変参考になった	21	37.5%
多少参考になった	30	53.6%
参考にならなかった	1	1.8%
無回答	4	7.1%



- ガイドラインをHPから手得し参考としたい
- それなりに知っていたので
- Fairuseではないが、各論でなく総論で解禁できないか
- ISPオペレーションの立場から、ガイドラインの（法的）有効性が気になる。ぜひ明確な根拠となるよう、進めていただきたい。
- ガイドの位置づけをきちんと説明されて良かったです
- ガイドラインに込められた関係者一同の想いを理解できた

e. 通信の秘密とサイバーセキュリティ対策

大変参考になった	34	60.7%
多少参考になった	15	26.8%
参考にならなかった	2	3.6%
無回答	5	8.9%



- いつも安定
- 元気が出ました
- 内容に異和感を覚えます
- 非常に勉強になった
- 思いの強いお話で、異和感ありました。言いすぎ？むちゃくちゃ
- 私見的な面もあるが参考となった
- 通信業務の枠を超えた視点がついた
- 日本人の観念という点から見た世界の中での得意性が興味深かった

今回のセミナーの全般的な感想をお聞かせください。

・「フェアであるとは？」について、学ばせていただけた。
・SIMフリーなどの通信の多様化に関するいろいろ（市場、制度など…）
・沖縄よりテーマがフォーカスされたのが良い
・面白かったです
・思っていたよりも、講演者のメッセージがそれぞれ強く伝わってくる内容で想定外に良かった
・官学民の連携が始まるだけでなく、国民一人一人のICTへの積極的関心が必要だと感じました。
・興味深く話が聞けました
・現在のセキュリティ対応状況がよく理解できた
・参加できてとてもよかったと思える有意義なセミナーでした
・素晴らしかったです。
・全体として、ひとつのテーマにつながっており、良く整理されたセミナーでした。
・大変参考になりました
・大変参考になりました。ありがとうございました。
・大変充実した内容でした
・通信の秘密というテーマに沿って様々な角度から情報・意見をいただけ参考になった。
・通信の秘密等に関らず法整備や取り組みを各講演の中で様々な角度から語られていたのがよかった
・非常になごやかな空気がよかったです
・非常に幅広いテーマを取り扱って頂き、深い知見を得られました。
・普段なかなか聴けない話を聴くよい機会だった

今後、とりあげてほしいテーマ・開催してほしいセミナーがあれば、お聞かせください。

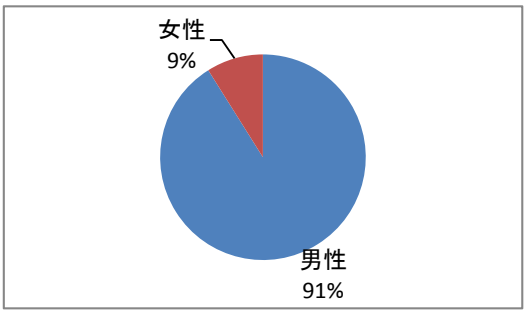
・IoT，M2Mの普及に向けたセキュリティ対策の（国際）連携
・サイバー攻撃からの防衛につき各方面で実施している対策を把握したい。
・サイバー攻撃関連
・サイバー攻撃への対処について、まだその合法性が裁判の場に出てはいないとのことだったが、具体的なケースを元に実際どうなのか、有識者や総務省などの関係者の考えを取り込んだケーススタディを聞きたい
・担当者レベルでのセキュリティに関する情報交換
・通秘の具体的な解釈論
・林先生の話をもっと長くとって欲しいです

その他、ご意見・ご感想があれば、お聞かせください。

・プログラム概要に、開始時間しか書かれておらず、終了時刻がわからず困りました
・おもしろかったです。また参加したいです。
・継続的に今回のようなフォーラムを開催していただければ幸いです。
・山下さんの進行はお上手で安心して見てられますね

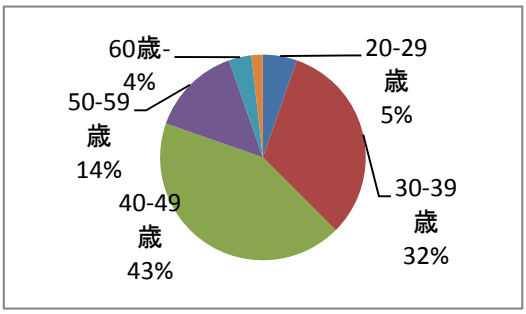
性別

男性	51	91.1%
女性	5	8.9%



年齢

20-29歳	3	5.4%
30-39歳	18	32.1%
40-49歳	24	42.9%
50-59歳	8	14.3%
60歳-	2	3.6%
無回答	1	1.8%



職種　（※複数回答あり）

NW設計/構築/運用/保守	11	19.6%
サーバ設計/構築/運用/保守	4	7.1%
アプリケーション設計/構築/運用/保守	2	3.6%
カスタマーサポート	4	7.1%
セキュリティ技術者	7	12.5%
セキュリティマネジメント	10	17.9%
研究開発	2	3.6%
営業	5	8.9%
企画	9	16.1%
管理	2	3.6%
法務	3	5.4%
コンサルタント	2	3.6%
その他	4	7.1%

（※お茶くみ、標準化、通信など）