インターネットガバナンスにおけるセキュリティ分野の議論

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
Izumi[at]nic.ad.jp

JPNIC 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

IoTセキュリティ向上に向けた関係者と想定される役割

- **技術者だけでは対応できないことと技術者から問題提起をしていくことも重要**
  - 運用上懸念があり、標準化、ベンダーレベルで対応が必要な事項は声をあげる 等

関係者	できること	課題
運用者	運用上のセキュリティ対策	従来の対策では対応しきれない部分をどうするか、技術者のみでは解決できない問題をどうするか
標準化に関わる人々	安心安全な技術標準の策定	標準化の統一： 複数の標準化があり、IETF・他の標準化団体との連携が必要
ベンダー	一定の技術標準を満たす製品・ハグに対応したアップグレードの提供	多くが従来のインターネット機器のベンダーではなく、インターネットの一部であること、すなわち既存のインターネットの仕組みや標準化、運用の一部であるとの意識が希薄
政府	ベンダー・消費者の認識向上、対応促進策の検討・適用	機器が安価なため、アップグレードが困難・ベンダーが必要性を認識していない・対応したくない 機器は対応していても、セキュリティレベルや使い方、バグ更新等消費者の意識向上が必要な部分がある

インターネットガバナンスにおけるセキュリティに関する諸議論

レイヤー	分野	取り組み・着目されている議論
国家間	国への脅威、機密情報保護	・NATOの第4ドメインに指定 ・国連GGE(軍縮等も議論している委員会下の専門家グループ)での議論 ・Cyber norms
法整備	国際法 国内法	サイバー攻撃があった場合、攻撃が行われた国が責任をとるべきか
法執行機関	国を超えた犯罪対応 CSIRTや事業者等国内関係者との連携	・Budapest Convention等に基づいた国際協力 ・CSIRTの立ち上げ(欧州で法案) ・Backdoor Encryption(例：Apple vs　FBI)
官民連携	必要性は数年前から言われているが分野も多様で具体的にどうするのかがまだ見えづらい	・ハーグ会議 ・Collaborative Security：ISOC ・NTIAによるIoT Open Consultationの試み…等
技術コミュニティ	標準化、BPの文書化、能力育成等	・標準化における広範囲の監視対策(TLS) ・Cyber Green ・MANRS ・CSIRTに関するIGF BPF策定…等

運用者にも関わる議論例

- **サイバー犯罪等の対応における仲介事業者の責務**
  - 法執行機関等に提供する情報の明確化
  - ついでに他の情報を求められた場合どうするか
- **CGN導入に伴う犯罪者特定への影響**
  - IPアドレスのみではなくポート番号もないと特定できない
- **法執行機関によるWHOIS登録情報の正確性向上提案**
  - ICANNではgTLD WHOISのあり方を見直す議論が開始
  - IPアドレスに関するWHOIS情報の正確性向上についても法執行機関より提案予定

Q&A