資料３１－１

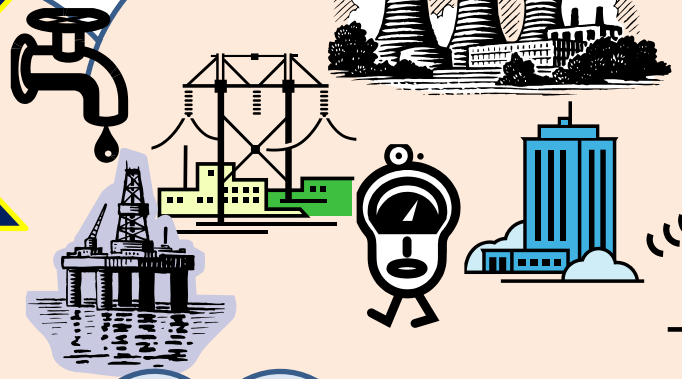
Some key agenda toward IoT

Hiroshi ESAKI, Ph.D.,
Professor, The University of Tokyo
Board of Trustee, ISOC
Executive Director, IPv6 Promotion Council, Japan
Director, Task Force on IPv4 Address Exhaustion, Japan
Director, WIDE Project

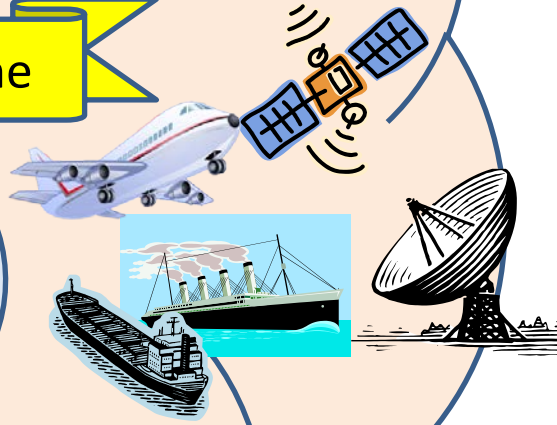
IP for Everyone

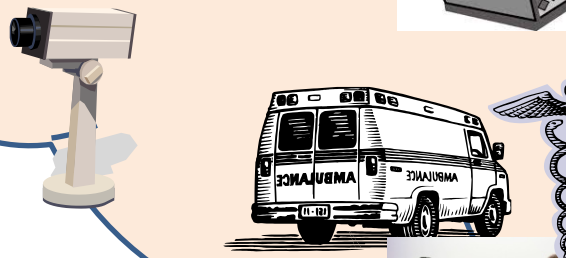
IoT (Internet of Things)

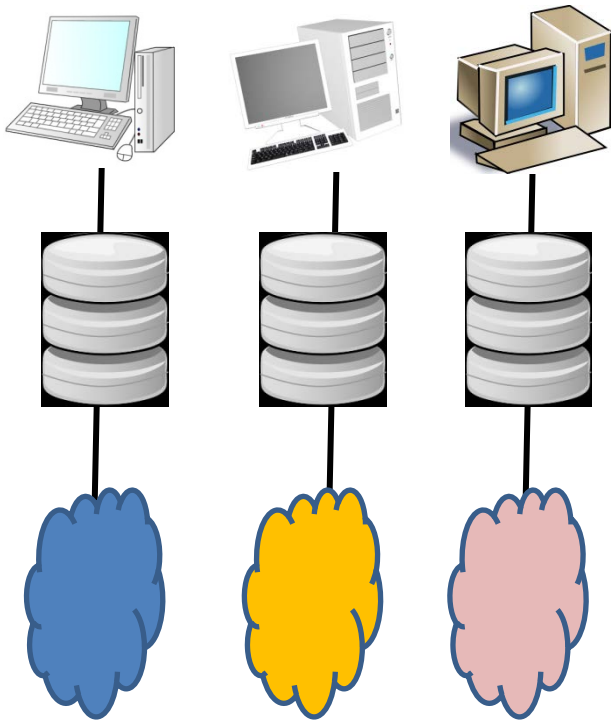
IP for Everything



IP for Everyone







Vertical Lock-on
with isolated Silos

Horizontal Cooperation
with the unique common
platform

Discussion in 2007

What is our goal ; toward the "Eco-System"

- Back-Ground
  1. There are many systems/networks with IP
  2. Still, there are many non-IP systems/networks
  3. Networks and Systems are tend to be **Fragmented**…
- Objective and Goal
  a. **Avoiding the fragmentation** of IP systems/networks
  b. Encourage the **collaboration among sub-systems**
  c. Explore the "Eco-System", that deliver the cheapest system deployment , **while delivering innovations**.

Security & Privacy by Design

◆NIST SGIP CoS mandates Cyber Security

- ✓ Many legacy protocols, e.g., BACnet can not be listed in Catalogue of Standards

◆IAB Announcement on Nov.13, 2014

- ✓ Encryption by Default https://www.iab.org/documents/correspondence-reports-documents/2014-2/iab-statement-on-internet-confidentiality

◆Collaborative Security by ISOC

- ✓ http://www.internetsociety.org/sites/default/files/CollaborativeSecurity-v1-0.pdf

◆Security by Design in Japan

総合科学技術・イノベーション会議
Council for Science, Technology and Innovation

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

CSSC 技術研究組合 制御システムセキュリティセンター
Control System Security Center

CCDS 一般社団法人 重要生活機器連携セキュリティ協議会
Connected Consumer Device Security Council

科学技術イノベーション総合戦略 2015

- P.6

  「システム化」が進むとともに、より大量なデータをリアルタイムで取得し、高度かつ大規模なデータ処理等を行うことが求められる。このため、将来を見据え、IoT（Internet of Things）、ビッグデータ解析、数理科学、計算科学技術、AI（Artificial Intelligence）、サイバーセキュリティ等の先導的な基盤技術の強化が必須である。

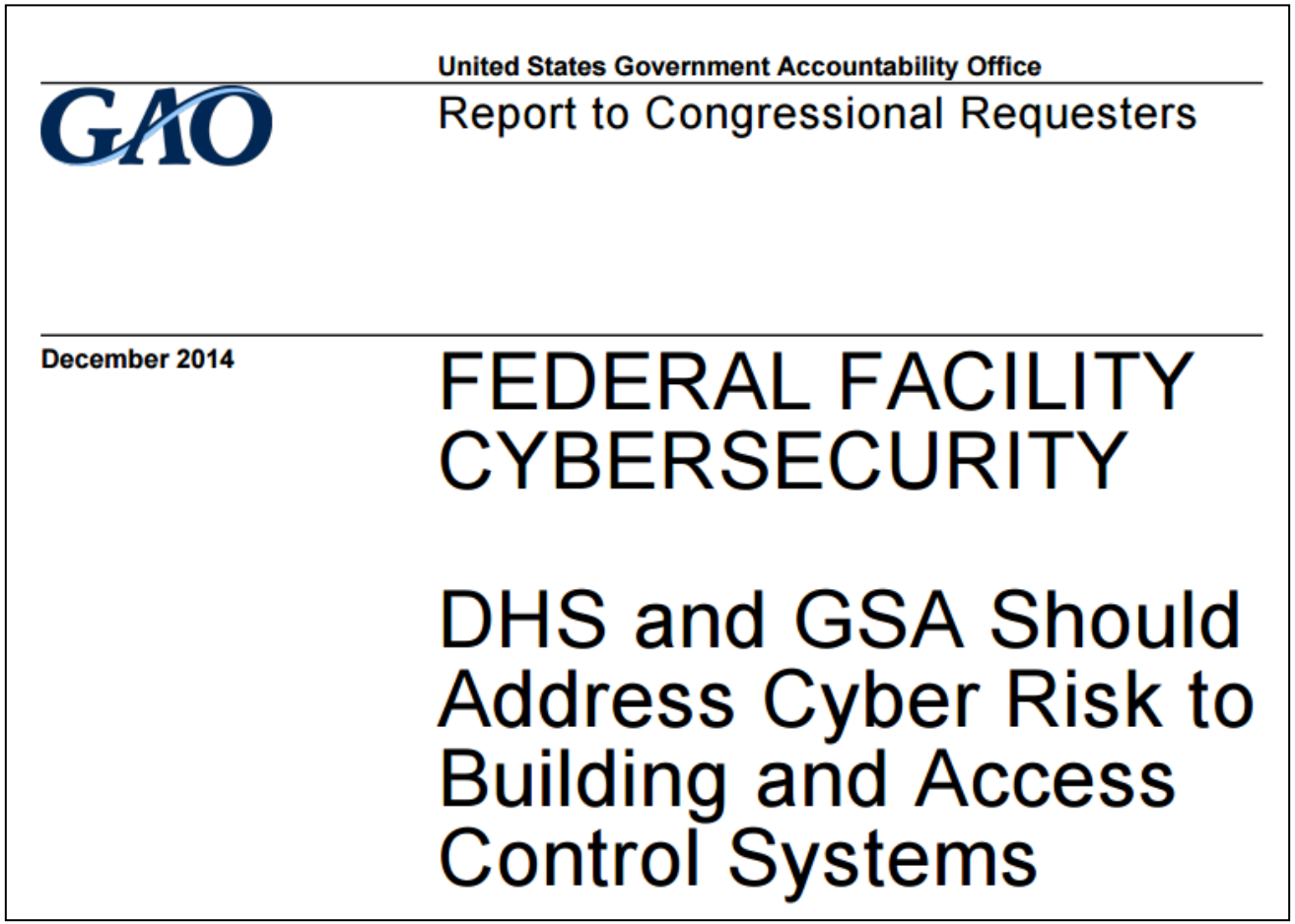
- P.33

  このうち情報セキュリティについては、電力を含む重要インフラ各分野で安定的・持続的なサービス提供を困難にするサイバー攻撃の脅威が日々高まっていることから、その対策に必要となる技術開発とともに、重要インフラの情報セキュリティ対策に係る第 3 次行動計画を踏まえ、国際標準に基づくセキュリティ認証の推進や、各重要インフラ企業への認証機器導入を図る。これにより、総合的なセキュリティが確保された安全・安心なIoTシステムを構築し、重要インフラを支えるネットワーク基盤を強固なものとする。なお、情報セキュリティの推進に当たっては、内閣サイバーセキュリティセンター（NISC）との密な連携により、サイバーセキュリティ戦略や情報セキュリティー研究開発戦略も踏まえた上で具現化を図る。

  （＊）重要インフラの情報セキュリティ対策に係る第３次行動計画では、「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」及び「石油」を重要インフラ分野として定義している

Report by GAO, December 2014

(United States Government Accountability Office)



United States Government Accountability Office

GAO

Report to Congressional Requesters

December 2014

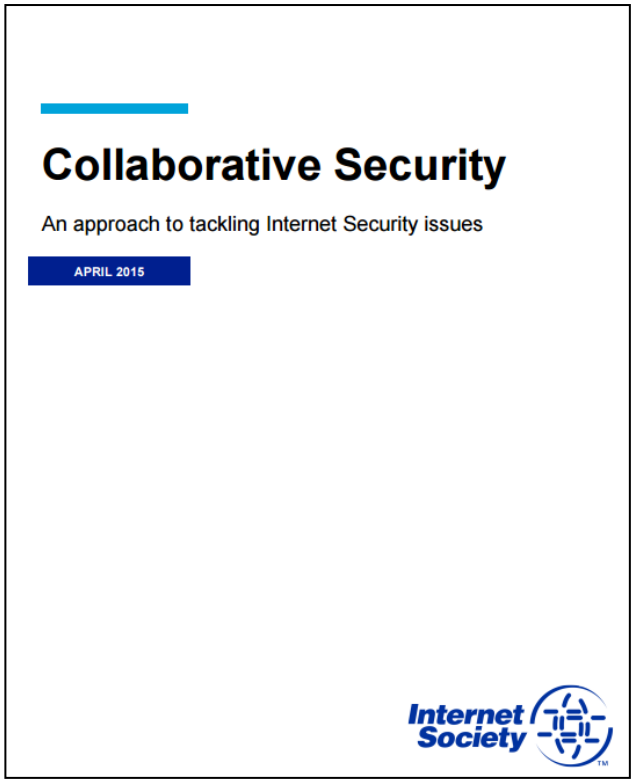
FEDERAL FACILITY CYBERSECURITY

DHS and GSA Should Address Cyber Risk to Building and Access Control Systems

http://www.gao.gov/assets/670/667512.pdf

ISOC (Internet Society) Collaborative Security

1. **Fostering confidence and protecting opportunities**:
   - ✓ Internet as a driver for economic and social innovation.
2. **Collective Responsibility**:
   - ✓ Internet participants share responsibility.
3. **Fundamental Properties and Values**:
   - ✓ compatible with fundamental human rights.
   - ✓ preserve the fundamental properties of the Internet.
4. **Evolution and Consensus**:
   - ✓ Agile evolutionary steps with stakeholders.
5. **Think Globally, act Locally**:
   - ✓ Voluntary bottom-up self-organization.



セキュリティに対する考え方
(基本となる10の考え方)(案)

Internet Governance Conference Japan
IGCJ
日本インターネットガバナンス会議
http://igcj.jp/

1. **インターネットはグローバルなインフラである**
2. 強制する(enforce)・制限する (restrict)のではなく、活動の**活力向上を応援(encourage)**する
3. **「過保護」は、かえって危険度を増大させる。つながることを前提に考えなくてはいけない**。
4. 「やらされる」ではなく、**「やりたくなる」を目指す**
5. 経験と知見の**「共有」**を行う
6. インシデントの経験者を、「被害者」として**「保護・支援」する**
7. 「原理主義」ではなく**「実践主義」**で進める
8. 「匿名性」の堅持
9. 「実施権」は個人にある、ただし第三者への委任は可能
10. セキュリティ施策の実施を、**品質向上のための投資**と 捉える