資料５－４

今後の情報通信環境の変化に対して必要となる情報セキュリティに関する取組

福智 道一
商用ネットワークセキュリティ推進室
ソフトバンクBB株式会社

SoftBank BB

SoftBankは生まれも育ちもインターネット

アジアNO.1のネット企業として…

SoftBankのセキュリティ対策は、めまぐるしく変化する状況に応じて、速やかに、重層的に、行うこととしています。

SoftBankの現況

【次世代網】(NTTさんでいう所の)「NGN」に相当するものを2002年より提供中

- QoSを用いてIP電話サービスを提供
- IPマルチキャストを用いてIP放送を実現

【セキュアネットワークへの取り組み】状況の変化に応じたセキュアなネットワーク設計

- 顧客宅内装置(独自設計によるモデム)のNAT化を早期から実施
- バックボーンネットワークには早期からプライベートアドレスを利用

【サービス事例】BB Communicator ～ 先進的サービスをオープンアーキテクチャで推進中

- インターネット上のVPNを利用したオーバーレイネットワーク技術によるメッセージングソリューション
- 厳密なユーザ認証と暗号化を実装

【v6】V6必須のアプリケーションの登場に備えIPv6網構築の準備中

SoftBank BB

インシデントは絶えること無し。

インシデントの原因となる脅威は人間の存在が根源。技術は変われども、新たな技術を人間が利用するところに、新たな脅威は生まれ、インシデントは絶えない。

「クローズド＝セキュア」神話

インシデントの根本的な原因の多くは人間そのものに由来し、人間が介在した時点で「クローズド」の概念は崩れる。

- 【例】セキュアな社内網を構築しても、社内PCの社外持ち出し→PCマルウエア感染→社内再持込→社内マルウエア感染
- ネットワークサービスは広く遍く国民に提供されることに価値がある。
  - NGNも広く遍く展開されインターネットに繋がる事だろう→インターネットに繋がる以上「クローズドだから安心」とはいえないだろう
- オープンアーキテクチャでは問題対処の局面でプレーヤーが連携することでセキュアな環境を維持しようと努力している

ISPは如何に脅威に対処しているか?

事例

- 迷惑メール
  → JEAGによる迷惑メール対策(OP25B～送信ドメイン認証…)
- Botnet
  → CCC(T-ISAC-J)による注意喚起
- DoS(大量アクセス系)
  → ＊NOGの場における発信者詐称パケットフィルタリング(Source Address Validation)の啓発と普及
- 経路ハイジャック
  → 経路奉行(T-ISAC-J)による経路情報監視

事業者横断の協調・連携によって脅威に対処

供給者の責任

·セキュリティ対策に関しては「消費者は何もできない」が供給者のあるべき認識。
·セキュリティ対策の責任は、通信事業者始め宅内機器メーカー・情報家電メーカー等、供給者側がそれぞれ持つべき。

- セキュリティパッチの提供はネットワークに接続する際の大前提
- ネット対応家庭用ゲーム機ではソフトウエア更新サービスを標準的に提供しているものもある

寡占が増幅するセキュリティリスク

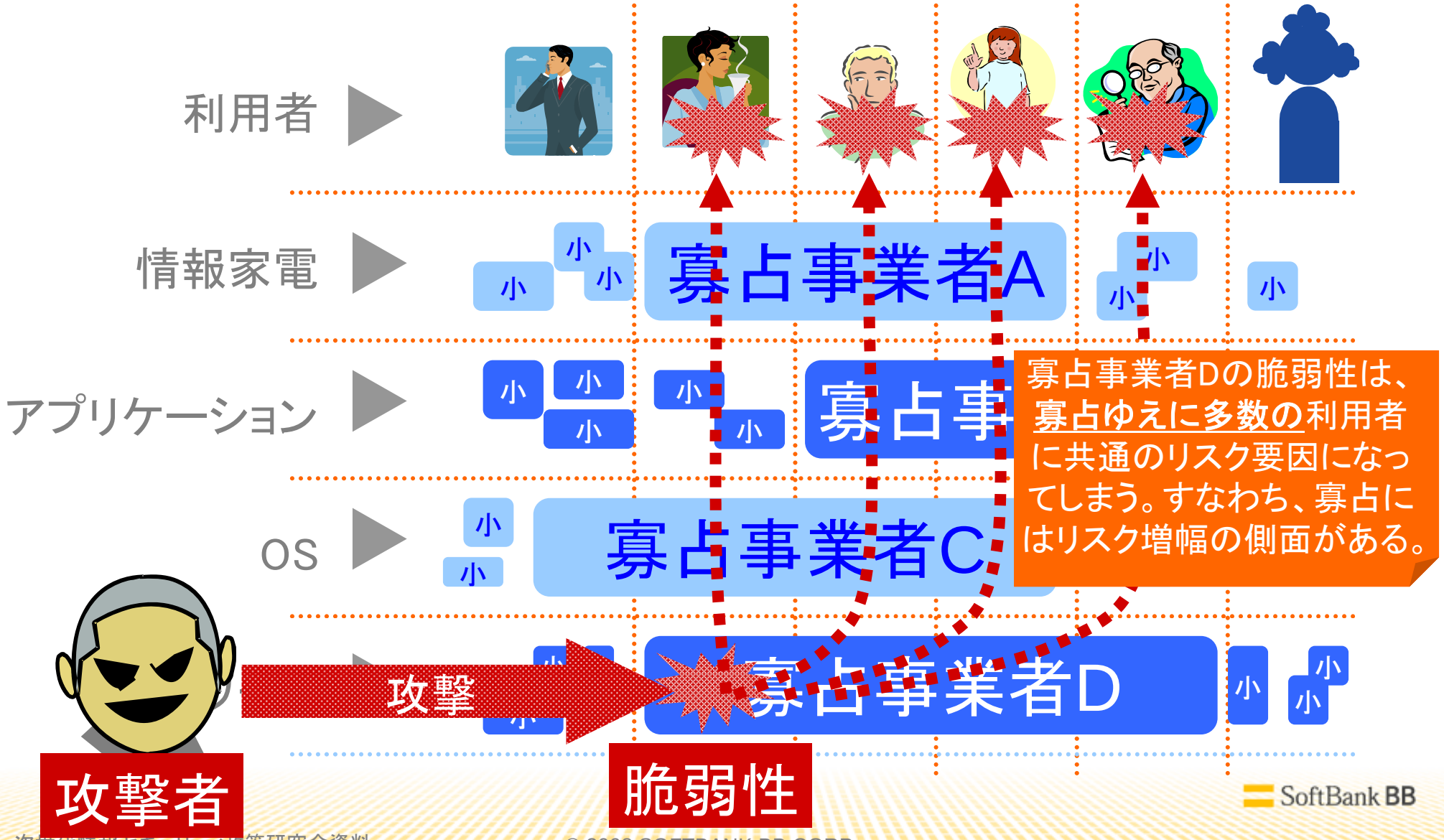
寡占状態においては寡占事業者のセキュリティ施策・レベル=セキュリティ標準となってしまう。その標準に脆弱性が存在した場合、業界全体のリスク要因となってしまう。

●アプリケーションサービス事業者がアクセス回線認証(NTTさんNGNの光アクセス等)に依存するような事業モデルになった場合、その認証方式の脆弱性はアプリケーションサービス事業者広く共通のリスク要因となる

●極めて広範 (PC、ネットワーク機器、家電、組み込み等)に利用されるOS (Windows、Linux、IOS等)の脆弱性は、容易に業界を跳び超えるリスク要因となる

●利用者の諸情報(ストレージ)を囲い込む形態の事業者の脆弱性は、利用者の視点では利用者のあらゆる情報に対するリスク要因となる

寡占が増幅するセキュリティリスク



SoftBankからの提言

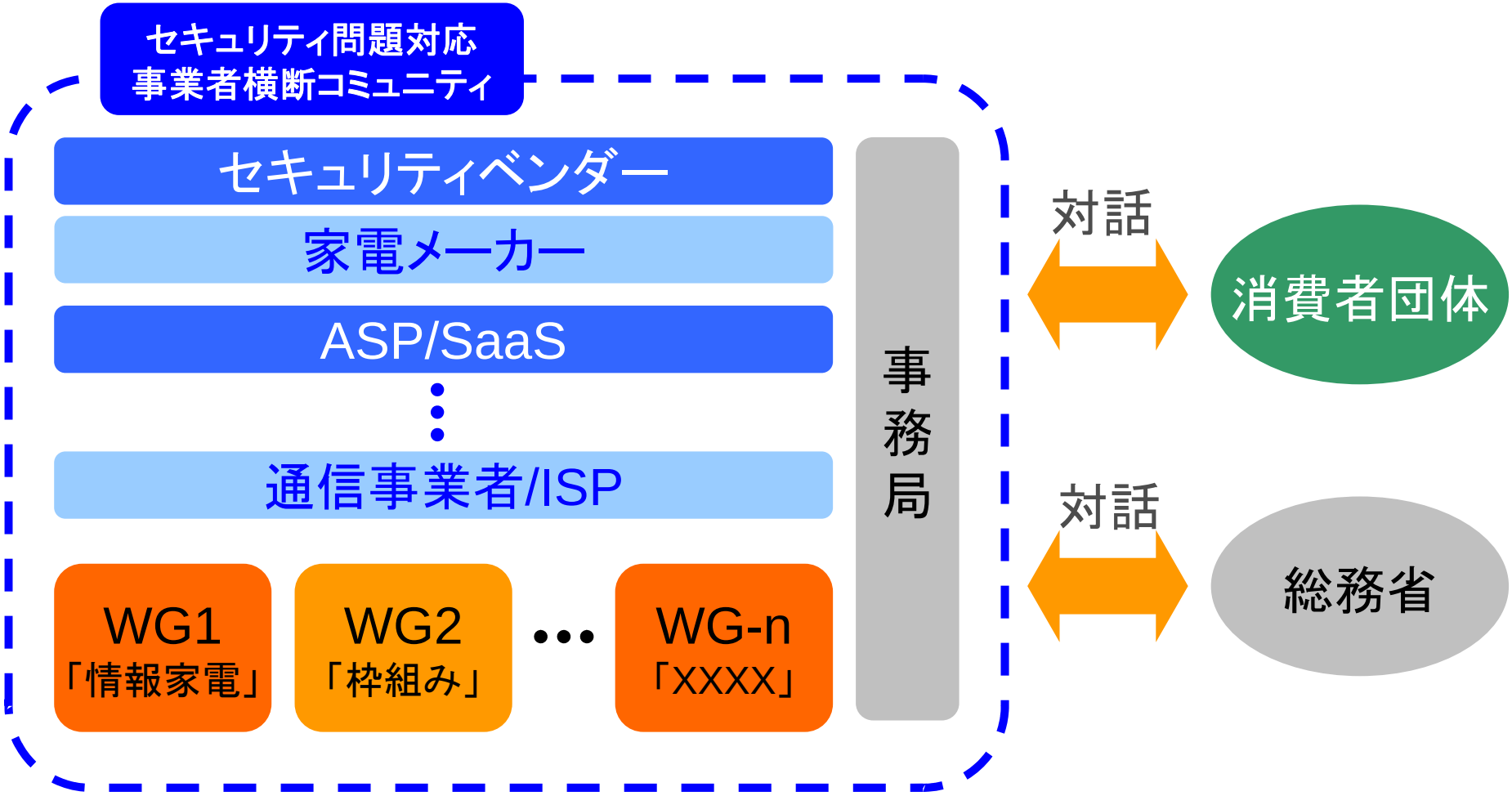
事業者連携コミュニティの育成・普及を

提言1

・脅威への対処はどこか一箇所で頑張ればOKということはありえず、ネットワークに繋がる全ての事業者/メーカーが、それぞれの所属業界を超えて連携する必要がある。
・産業界横断の事業者連携コミュニティの創出・普及が必要。
・総務省はじめ、政府からのコミュニティ育成支援策を期待する。

- 過去（v4時代）を振り返れば、コミュニティの力で新たな脅威に対応してきた。今後もコミュニティの重要性は変わらない。コミュニティの活性化で脅威へ対応する。
- ベストプラクティス→ BGPオペレータコミュニティは極めて発達している
  - 逆にコミュニティの存在しないところには早急の対処が必要
  - 情報家電はじめ、他業界もISP同様、業界内のコミュニケーションは早急に必要
    - ISP含め全ての業界を横断したコミュニケーションが必要
- ARIB,TELEC等のような制度的権限をもつことをターゲットとする
- コミュニティの要素として今後拡張・活用が期待できる団体
  - JPCERT/CC、T-ISAC-J、NCA、JEAG等

事業者横断コミュニティのイメージ



【案1】JPCERT/CC、T-ISAC-J、NCA、CEPTOAR、JEAG等の
既存団体・既存コミュニティを拡張・活用する
【案2】新たな機構を総務省主導で設立する

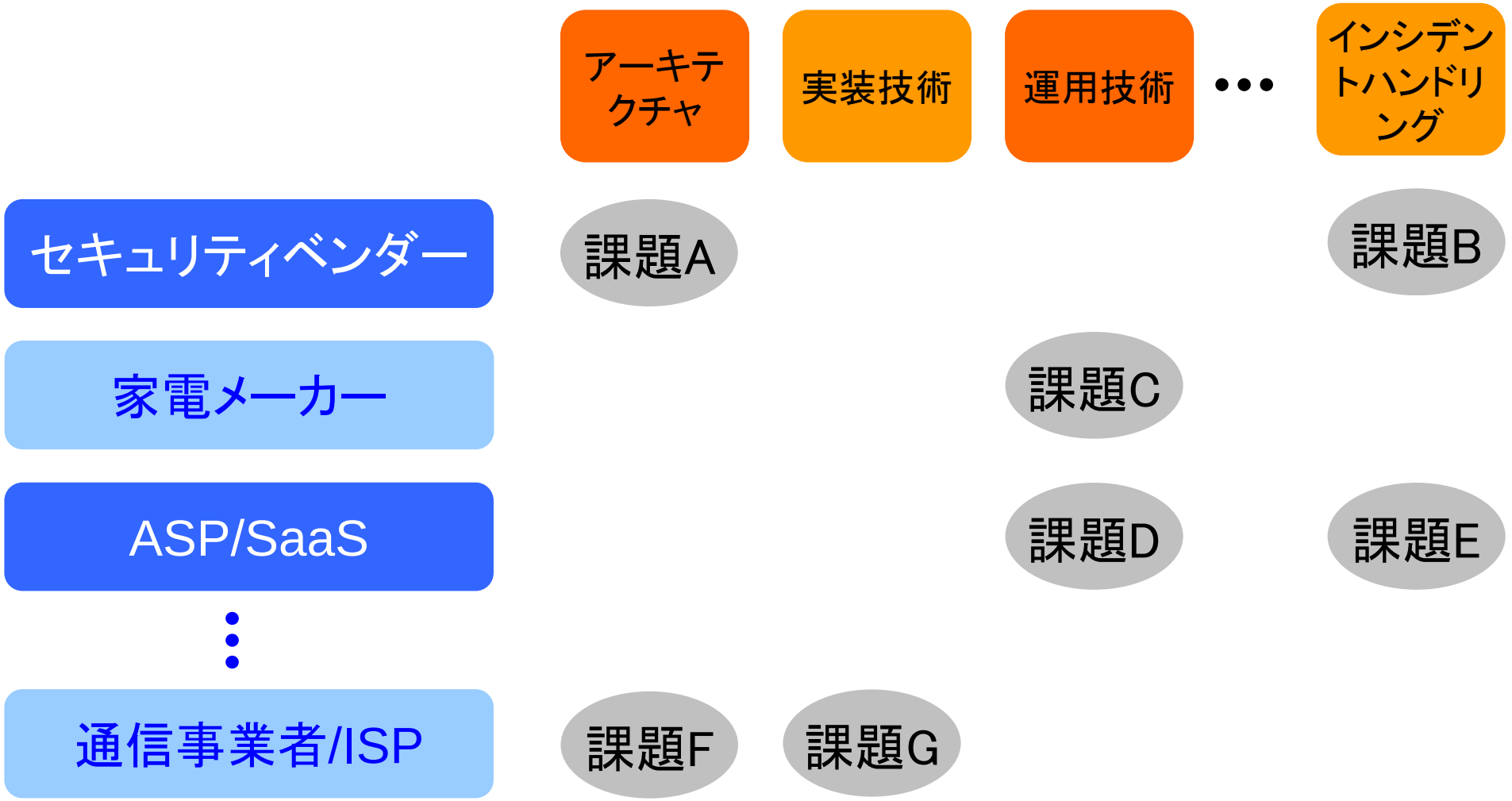
セキュリティ政策のフレームワークが必要

提言2

・セキュリティ政策の議論・立案・推進を効果的に行うには、問題・課題を認識するためのフレームワークが是非とも必要。
・このフレームワークは産業界横断の事業者連携コミュニティの経験・研究・議論を通じて作り上げるのが適当。

- 議論は業界横断コミュニティにて継続的に深化させていく必要がある

フレームワークのイメージ



注）上図中の区分名称はイメージです。今後のコミュニティの議論を通じて、これを定めていくことを期待しています。

競争を通じセキュリティ対策にも多様性を

提言3

·寡占化によるセキュリティレベル·施策の単一化の防止が必要。
·セキュリティの観点からも、事業者間のサービスや品質の競争は重要。

- 各事業者が自由競争を通じて切磋琢磨しあうことによって多様性を維持しつつ業界全体のセキュリティレベルを向上させるような市場環境作りを政府に期待する。
- 寡占状態における単一仕様環境においては、その仕様上の不備が重大な単一故障点(Single Point of Failure)になりうる。ICTにおいて、この傾向が顕著であることに注意が必要。

まとめ

- インシデントは人間が根本にあり絶えることが無い
- ISPは事業者横断の協調・連携で脅威に対処してきた
- セキュリティ対策の責任は、供給者側が持つべき
- 寡占はセキュリティリスクを増幅する

- 提言1: 事業者連携コミュニティの育成・普及を
- 提言2: コミュニティを通じてセキュリティ政策の枠組を
- 提言3:セキュリティの観点からも事業者間の競争は重要

SoftBankの理念

デジタル情報革命を通じて、
人々が知恵と知識を共有
することを推進し、人類と
社会に貢献する。