IIJ
Internet Initiative Japan

Ongoing Innovation

資料7－3

ISPから見た国際事案とその協調対処について

2008年05月01日
株式会社インターネットイニシアティブ
セキュリティ情報統括部
齋藤 衛

Agenda

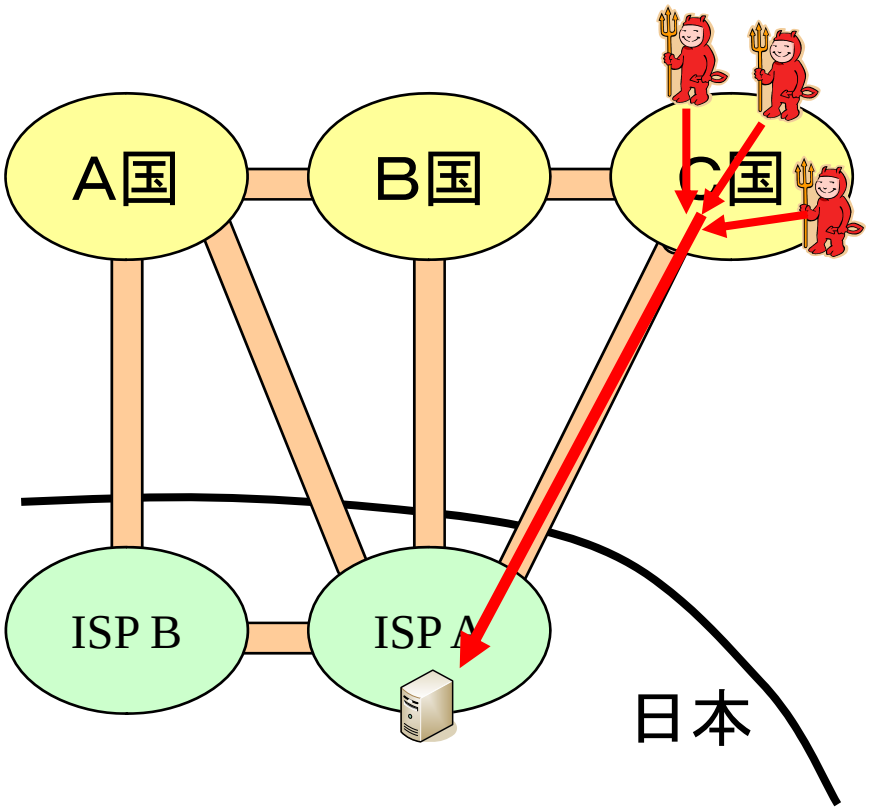
- 国際事案の例
- 国際事案の複雑化
- 国際協調の場
- 国際政策への提言

国際事案の例

- 単純な国際間DDoS
- Phishing

国際事案の例 (1) 単純な国際間DDoS

事例
■特定の国から、日本に存在する複数のWebサーバに対するDDoS攻撃が発生した。

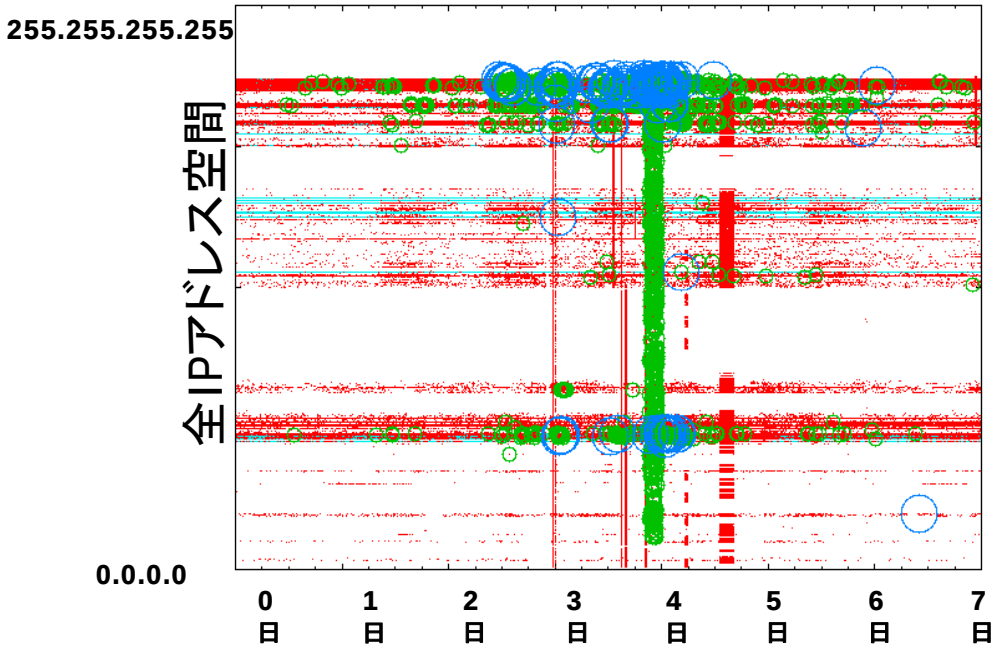


- 現象
  - 攻撃の技術的な内容は、不要なIPパケットで回線を埋めるような攻撃から syn flood まで多様であった。
  - 攻撃先 Web サーバおよび接続回線は陥落した。
  - IPアドレスの詐称(IP spoofing)の利用。
- 被害者とISP A での対策
  - さまざまな点でのフィルタなど。
- 問題
  - 被害者とISP Aの契約回線容量を超えた時点で被害者での対応は不可能に。
  - IPアドレスの詐称により被害者側では行為者を特定不可能に。

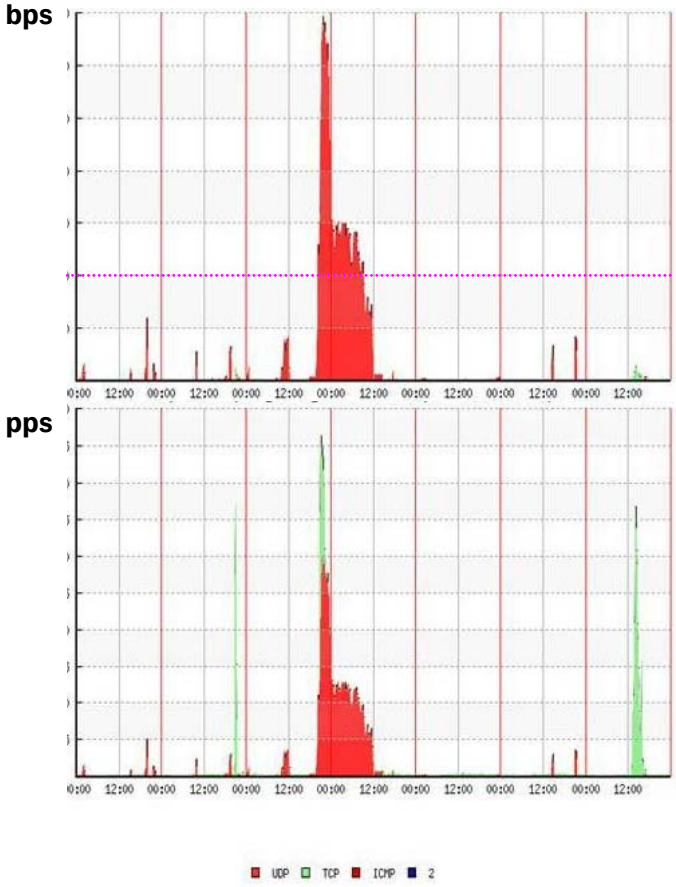
国際事案の例 (1)単純な国際間DDoS(2)
SYN Flood とSource Address Spoofing およびUDP Flood の実態

- Syn flood と
  Source Address Spoofingの分布状況

凡例：赤100以下、緑100以上1000以下、青1000以上のsyn/sec

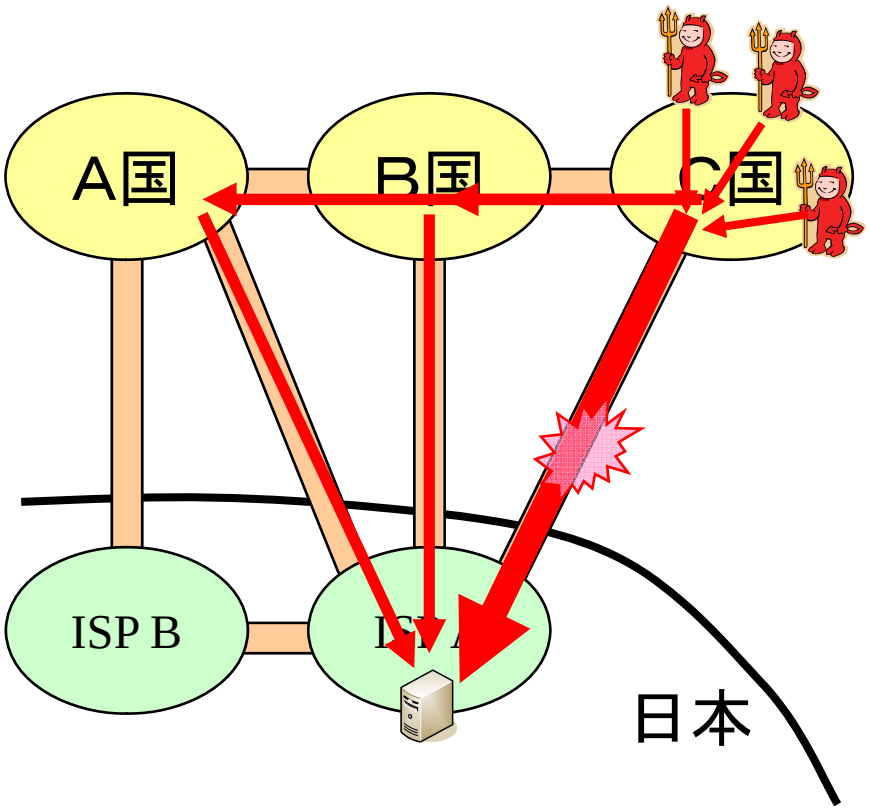


- UDP Flood + Syn Floodの実態



国際事案の例 (1) 単純な国際間DDoS(3)

事例
■特定の国から、日本に存在する複数のWebサーバに対するDDoS攻撃が発生した。

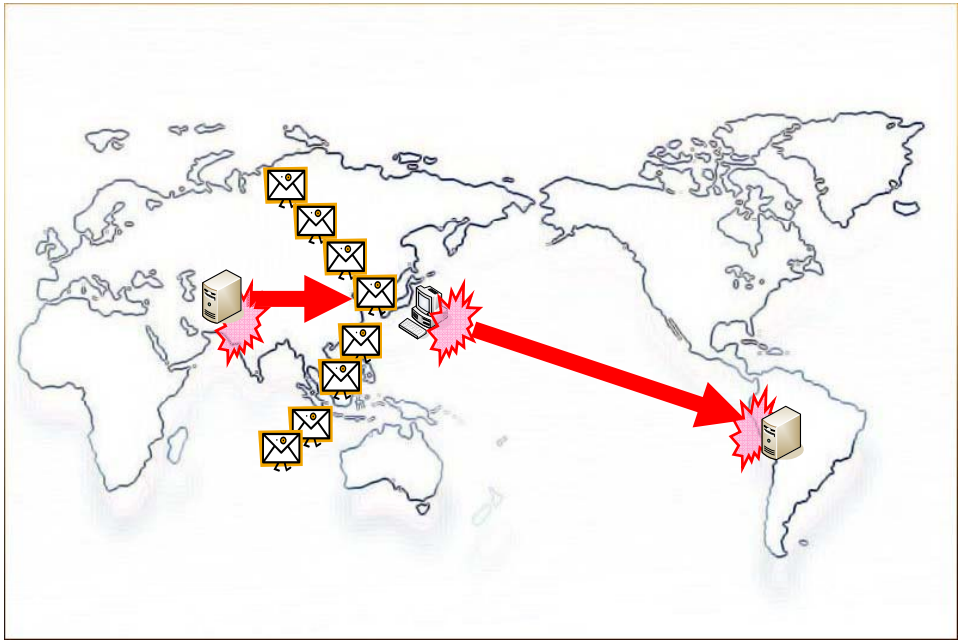


- **現象**
  - 攻撃の技術的な内容は、不要なIPパケットで回線を埋めるような攻撃から syn flood まで多様であった。
  - 攻撃先 Web サーバおよび接続回線は陥落。
  - IPアドレスの詐称(IP spoofing)
  - **攻撃元となった国のISPと攻撃先を収容するISPの peering 回線が影響を受けた。**
  - **攻撃側の経路操作で攻撃トラフィックが移動。**
- **被害者とISP A での対策**
  - さまざまな点でのフィルタ
  - **Peering先への対応依頼。**
- **問題**
  - 被害者とISP Aの契約回線容量を超えた時点で被害者での対応は不可能に
  - IPアドレスの詐称により攻撃を受けているサーバでは行為者を特定不能に
  - **相手国の peering ISP は存在するが、適切な対話ができない。**
  - **相手国に操作点が無い。**
  - **ISPとしてどこまで対応してよいのか不明だった。(正当業務行為の範囲が不明。後の「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン 」で、ある程度の範囲を規定。)**

国際事案の例 (2) Phishing

事例

■日本の国内銀行のphishingが発生した。



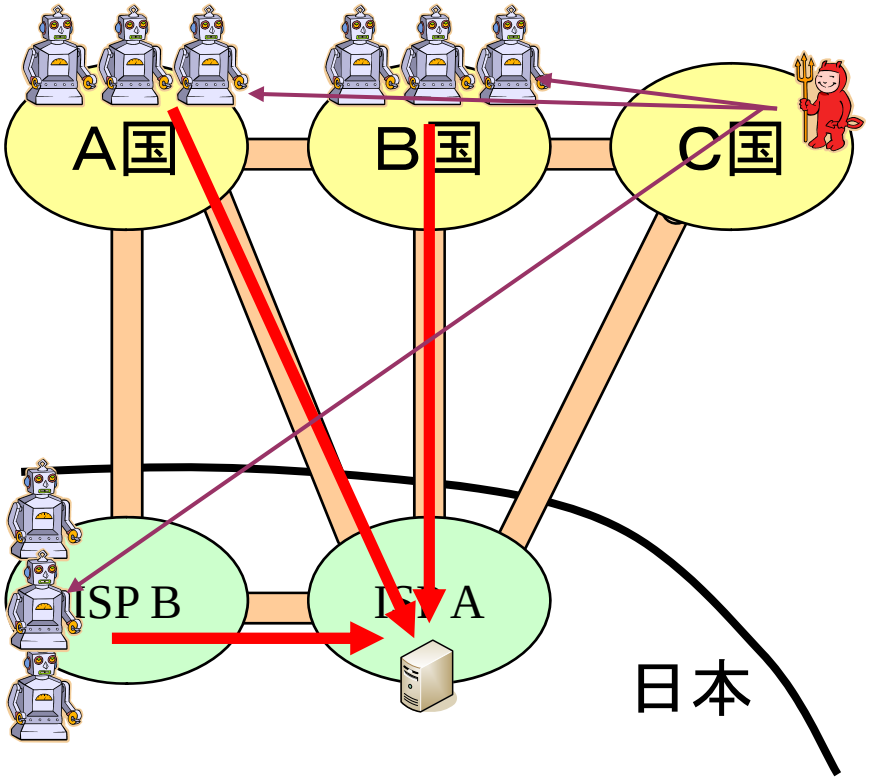
- **現象**
  - 東欧から日本の利用者向けにスパムメールが配信された。
  - 内容は日本語で記述されており、銀行の窓口Webへのログインを促し、アカウント情報を搾取するもの。
  - Web サーバは南米など数カ国に設置されていた。
- **対策**
  - 関連組織(FISC,JPCERT/CC,警察など)が対策に動いた(らしい)。
  - Telecom ISAC Japan でも対策を検討した。
  - 日本側からFIRSTや nanog などの国際組織で takedown の要請が行われた。
- **問題**
  - 言語の壁。HomePage にはロシア語やスペイン語での記載しかなく、セキュリティ対応窓口やabuse 対応窓口を見つけることすらできなかった。
  - 時差の壁。日本での昼間にはほとんど活動しておらず、対応が遅れてしまった。
  - 被害者からの申告がなかった。
  - Web サーバの停止に、まる3日必要とした。
  - 最終的に誰がリーチしたのか不明。

国際事案の複雑化

- 攻撃にOpen Proxyや Botnetを利用されることで、事態はより複雑化する。

国際事案の複雑化(1)

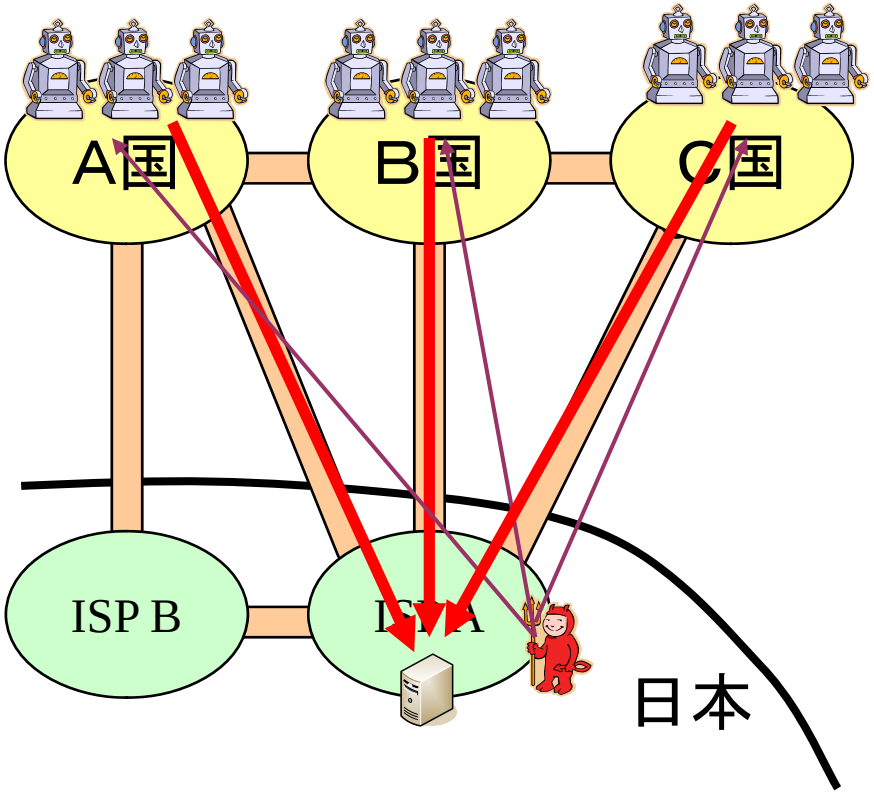
事例
■日本国内を狙ったDDoS事案。



- 国内の OpenProxy を踏み台にしたり、botnet を利用した事案など。
- 日本国内に閉じた通信で攻撃を成立させる事案もある。
- 攻撃の行為者と攻撃の通信が分断され、行為者が不明となる。

国際事案の複雑化(2)

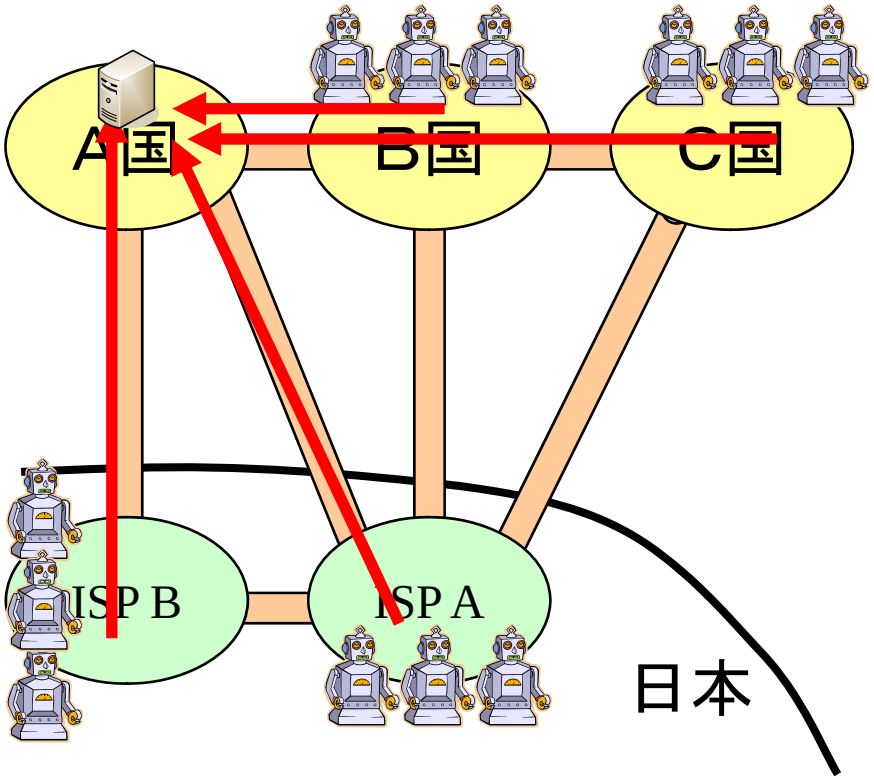
事例
■国内事案の国際化。



- 国内の事案も国際事案に発展する場合がある。
- SPAMメール配信やDDoS事案など。
- メールの内容やDDoS発生の背景情報からのみ、国内の行為であると判断できる場合。

国際事案の複雑化(3)

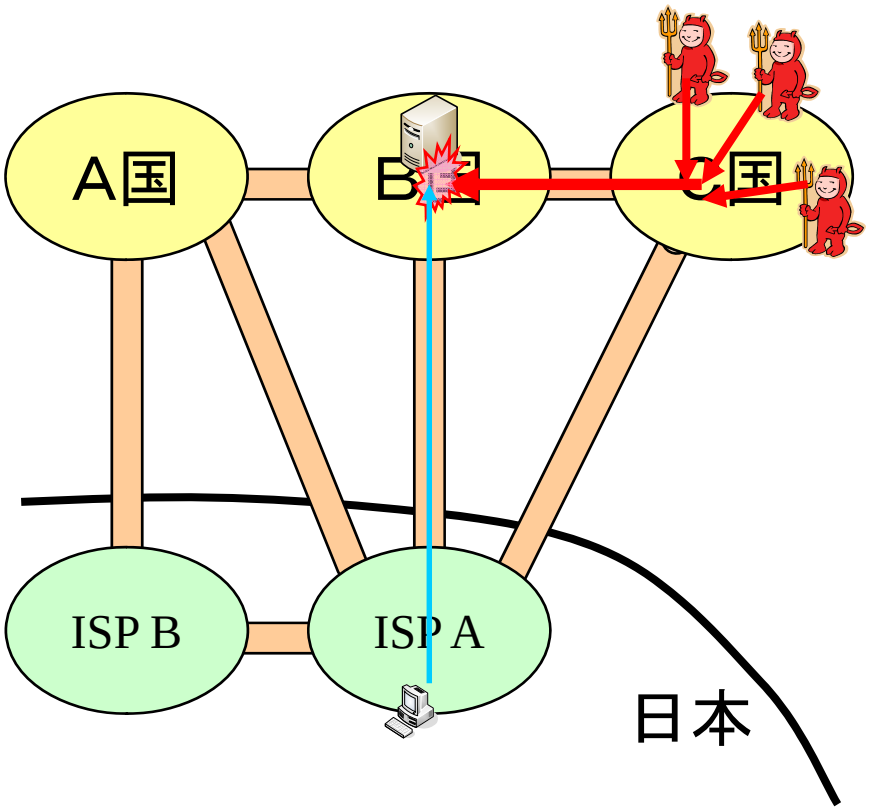
事例
■日本の介在しない事案への関与。



- 直接日本が関係しないと判断できる、外国と外国の間の事案においても、日本国内のbotに感染したPCからの攻撃が観測される。
- ニュースなどの情報や、被害者(国)からの申告があってはじめてわかる場合。

国際事案の複雑化(4)日本の通信環境を経ない日本への攻撃

事例
■国内の資源と考えられているサーバなどが、国外に存在する場合。



- サーバなどが海外にある場合。
- サービスの一部が海外の資源に依存する場合。
- (世界規模の企業など)IT部門が日本国内に無い場合。
- この場合、日本のISPでは攻撃の発生すら観測できず、ニュースや利用者からの申告ではじめてわかる。

これまでのまとめ

- インターネットでは、喧嘩も、嫌がらせも、金銭目的の犯罪も、戦争も同じネットワークで運んでいる。
- 攻撃に使われた通信の主体と、行為者は別の場合があり、攻撃の通信だけでは国際問題と国内問題の切り分けは難しい。

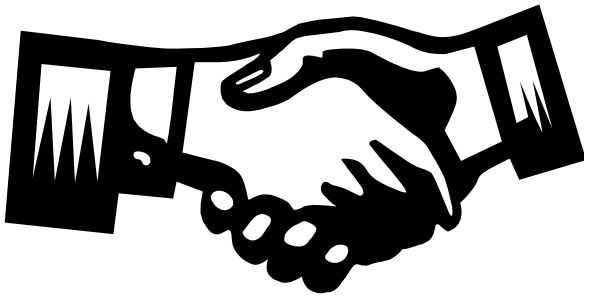
- 国際事案対処上の問題
  - 文化の違い
  - 技能やネットワーク環境の違い
  - 時差
  - 言語
  - 通信事業に関連する法的、制度的環境の違い
  - 通信事業者と利用者の関係の違い
  - 対応の品質
  - 日本国内の問題

国際協調の場

国際協調の場（1）ISPとしての国際協調の場

- Peering対向ISP
  - 契約に基づくインシデントハンドリング
- Network Operators Group(s): *nog (Nanog, Janog, CNnog, Sanog,…)
  - ネットワークオペレータコミュニティ
- NIC系活動(ARIN, RIPE , APNIC, LACNIC, AfriNIC)
  - IPアドレス割り当てに関する関係
- 特定目的の活動団体(MAAWG,APWGなど)
  - SPAMメール対策、Phishing対策など特定の問題への解決

- Nsp-security
  - http://puck.nether.net/mailman/listinfo/nsp-security
  - 参加資格：ルータやサーバなど対策実施が可能な操作点を持つ人。
  - 参考：Nsp-leo-security
    - https://www.nspsec.org/mailman/listinfo/nsp-leo-security
    - Nsp-securityとLEOの情報交換の場。



- 問題
  - 公平な場かどうか。相手の技量の問題
  - 秘密の共有の問題
    - 誰がいるのかわからないコミュニティ
  - 目的の違い
  - 権限や法制度の違い

国際協調の場 (2) CSIRTとしての国際協調の場

- FIRST
- Forum of Incident Response and Security Teams
- 1990年に異業種セキュリティ対応チーム間で結成された組織で、世界中の193組織が加盟している(南極大陸を除くすべての大陸)。
- 日本からは現時点で13組織が加盟。
- CSIRTチームの団体だが、チームのホスト組織は政府、民間、学術系と様々。
- 活動
  - 年に一度のConferenceを、年に数回の技術交換会議を開催している。
    - 事案情報、脆弱性情報流通や、PhishingやDDoSなどのインシデントに対する国際協調の場。
    - 事例紹介や技術検討の議論CSIRT設立補助。
  - MLでの議論

- 信頼できる相手であること
  - 責任範囲、連絡方法などを定義、公開できるチーム
  - 加盟にはスポンサー2組織の紹介と審査が必要
  - Pgpを利用した暗号通信基盤
  - Conferenceなどで顔を合わせて信用
  - チーム単位の守秘義務(ホスト組織ではなく、参加チーム内のみの情報流通)
- お願いベースの対応
  - 相手の立場(法制度や文化の違い)を理解し、無理強いをしない
  - 対応の品質(対応時間や内容)を指定することはできない
- それでも効果的に動いている(Best Current Practice)
- National PoC (Point of Contact):対応責任をもった国単位の窓口

より良い国際協調のために

- 国際事案対処上の問題
  - 文化の違い
  - 技能やネットワーク環境の違い
  - 時差
  - 言語
  - 通信事業に関連する法的、制度的環境の違い
  - 通信事業者と利用者の関係の違い
  - 対応の品質
  - 日本国内の問題

- より良い協調のためには
  - まずは日本の状況を整理し
  - その上で国際間で責任のある関係を結ぶ必要があるのではないか

国際政策への提言

国際政策への提言

- 国際事案に対応するために、まずは国内をしっかりしよう
  - 事案対応における通信事業者の役割を明確に
  - 国内被害者と対策組織がコンタクトできる仕組みを
  - 国内対策組織の間の連携、協調促進を
- 日本国民が利用するサービスの国内誘致を促進
  - 諸外国との通信事情の悪化を想定し、国民生活に必要なサービスは国内に誘致する仕組みを
- 国際協力の場の醸成
  - 国際の場への積極的参加を促す仕組みを
  - 対策技術、研究開発、演習などの国際展開を
  - 日本のNational PoC を