サイバー攻撃対応演習
（防災訓練型）
～Telecom-ISAC Japan 主催～

Telecom-ISAC Japan
サイバー攻撃演習ワーキンググループ
三浦　雄大

第一章　演習実施の意義

どうして、防災訓練形式になったのか

- いざとなった時に
  - 天災への対応とおなじく、サイバー攻撃も災害と同じ目線でみて、対応力を養う
  - 訓練でも経験により、いざという時に余裕がうまれる。

継続は力なり

- 限りあるリソースの中で最大限の効果を出すためには
  - 稼働の軽減
    - 皆様も毎年行われる防災訓練のように、決まったフレームワークで再利用がある程度可能なシステム構築。
  - 定期的に開催することにより、運用者レベルの交流（人的交流）
  - 想像力の強化
    - 演習を経験することにより、インシデント発生時に障害/攻撃の切り分けが多少スピーディーに行える
  - 経験を通して、沈着冷静な判断を行える。

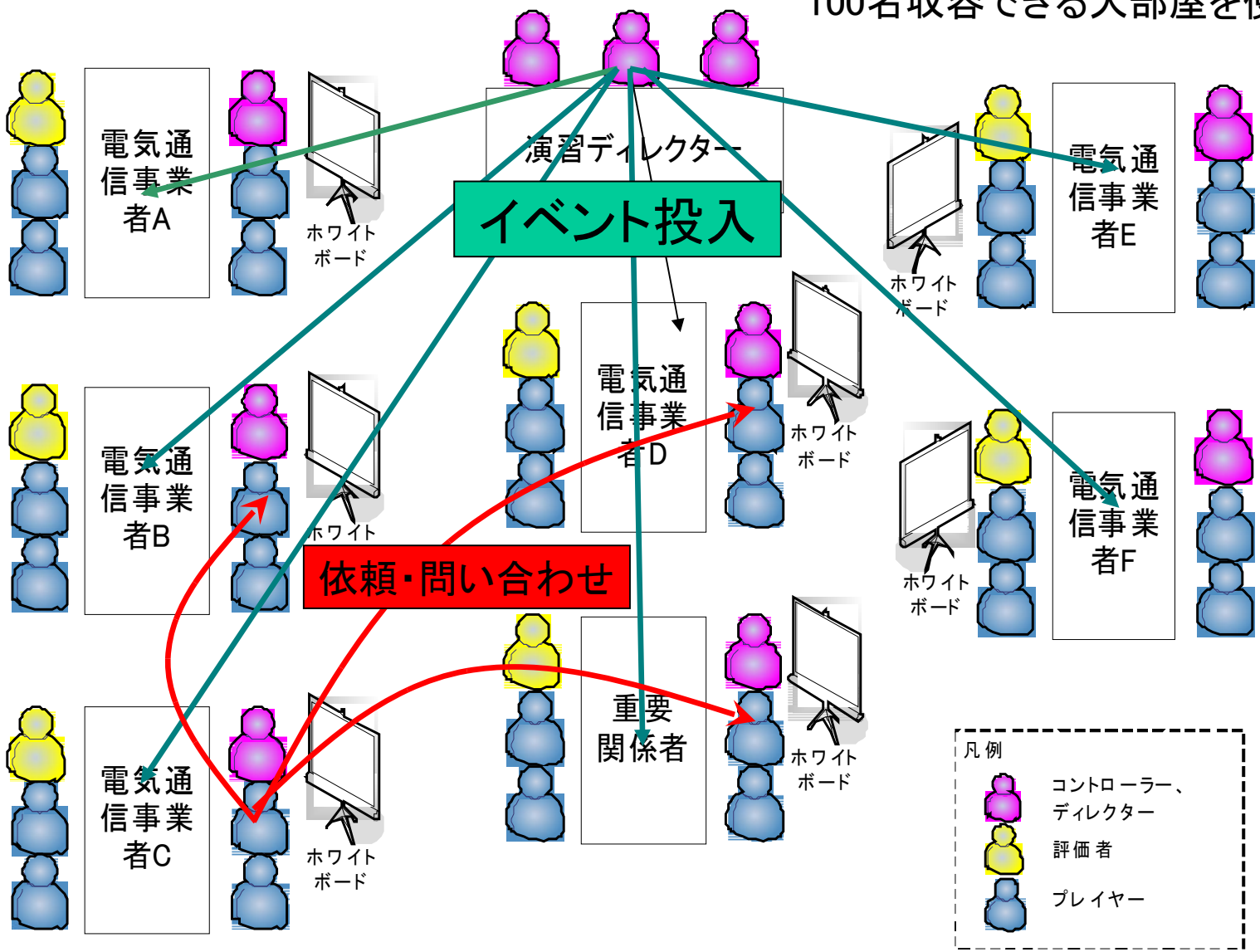
第二章　実際の演習の様子

2009年度サイバー攻撃対応演習

昨年12月11日（金）
朝9時から夕方5時すぎまで
、
大田区産業プラザにて開催

参加者
・重要インフラ ・ネット証券会社、ロジスティックス会社　合計3社
・電気通信事業者 ・国内主要ISP、アクセス網事業者　合計8社
・政府関係者、テレコムアイザック　等
総勢100名強が参加

サイバー攻撃対応演習の進め方



演習の進め方

①大会場に集合。進め方を説明

②ディレクターがイベントを投入

③参加者島毎に対応を検討・他島問合せ

演習のメインです。プレイヤーの訓練を実施し、各社で課題を抽出します

④島毎にコメント発表、全体講評

連携等の各社共通的課題や自社における改善点等を中心に発表します

演習で実施された攻撃

・DDoS（サービス不能攻撃）
一般のインターネットユーザを受け入れているサイト等は攻撃自体とめる方法がない。攻撃を止めるとサービスの提供も止まってしまう。

・BGP経路ハイジャック
よく発生するのは、ミスオペ。
検知する方法はいろいろ工夫（経路奉行など）
現在では、完全に止める方法はない。

・DNSサーバ関連の攻撃
DNSプログラムの脆弱性は適宜発見され、その脆弱性を利用した攻撃が発生する可能性がある。
DNSが止まってしまうとインターネットへの影響が甚大である。

・その他
悪性サイトへのアクセスなど

参加者の声分析

プレイヤー
・演習参加当初のモチベーション水準によらず、演習に参加した人はその効果を実感し、来年度も参加したいという意見がほとんど
～対応訓練（ドリル）としての意義を感じてもらっている

課題抽出
・何年か参加している企業であっても、演習により新たな課題が抽出されている。
～対応環境や攻撃の変化により、業務運用のチェックが定期的に必要であることがわかる。