Empowered by Innovation NEC

インターネット系情報通信のレジリエンス

2011年9月13日

NECビッグローブ株式会社
（Telecom-ISAC会長）
飯塚　久夫

目　次

- 東日本大震災におけるインターネットの利用状況
- 今後のインターネット系情報通信の災害対策
- 情報セキュリティに関する脅威と課題の変質

本年４月から総務省において開催されている
総務省「大規模災害等緊急事態における通信確保の在り方に関する検討会」
http://www.soumu.go.jp/main_sosiki/kenkyu/saigai/index.html
の公開資料を参照しています。

東日本大震災における情報通信の対応状況

○被災した通信インフラの復旧や被災地における被災者支援のためキャリア、ISP(プロバイダー)等は積極的な取組を実施

①通信インフラ復旧に係わる取組
- 移動基地局車の配備、衛星利用臨時基地局の設置
- 移動電源車の配備

②被災者等の通信手段確保に係わる取組
- 公衆電話無料化、携帯端末無償貸与
- 避難所等におけるインターネット接続環境の無償提供

③利用者料金の減免等
- 被災地のサービス基本料金等の減免、利用料金支払い期限延長

④情報収集(安否確認、震災情報等)の支援
- 災害用伝言ダイヤル、災害用Web伝言板の提供
- 震災関連情報をまとめた特集サイトの設置

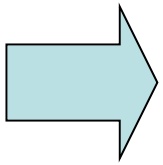
⑤情報発信のための支援
- アクセスの集中したウエブサイトへのミラーサイト提供
- 被災地域の自治体やNPO等へのクラウドサービスの無償提供

東日本大震災によるインターネット通信への影響

ISP(ビッグローブ)の被災状況

○建屋/設備
- サーバの装置故障が2件発生したがサービス影響なし
- 建物及び建物周辺に大きな損傷はなし
  （建物の外構のアスファルト部の亀裂、壁・天井の配管通関部の一部損傷など10箇所程度）

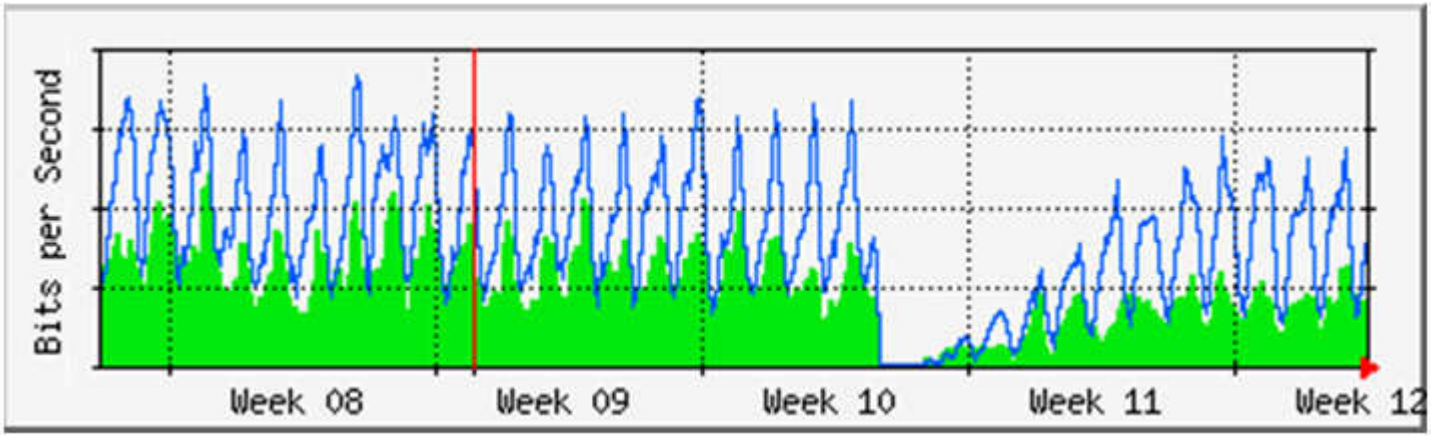
○回線
- バックボーンに利用している国内キャリア回線は影響なし
- 海外回線の一部で輻輳が発生した。
- キャリア内での故障により、以下の接続サービスで影響があった
  - フレッツ地域IP網 東北全断
  - イーアクセスADSLサービス 仙台収容一部ユーザ
  - WiMAX東北一部エリア
  - auひかり　東北一部エリア
  - BIGLOBEフォン(PN)050発－秋田エリア固定電話着の通話



被災地のユーザ収容回線以外大きなサービス影響なし

東日本大震災によるビッグローブ通信への影響①

宮城県のユーザが収容されているPOI（宮城県全域）における
地震発生前後2週間の2時間平均トラヒックの推移



3/11
地震

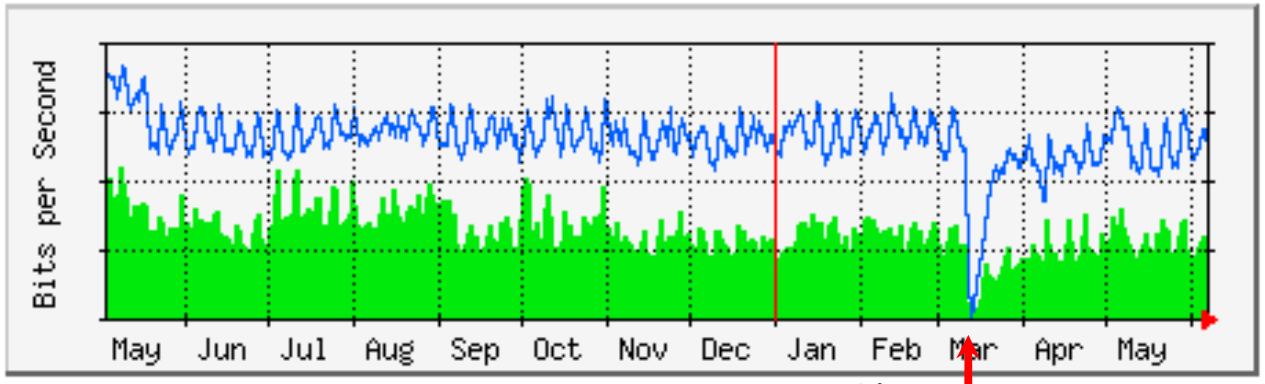
青の折れ線グラフ：ネットワーク→利用者
緑の領域グラフ：利用者→ネットワーク

震災地域では、２日間は完全に利用停止

東日本大震災によるビッグローブ通信への影響②

＜フレッツ地震発生前後一年間の一日平均トラヒック推移＞

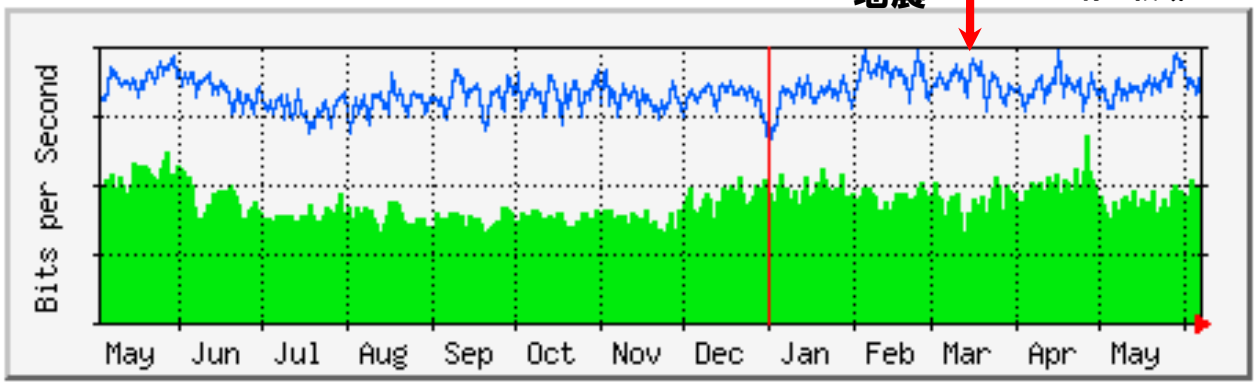
宮城



3/11
地震

青の折れ線グラフ：ネットワーク→利用者
緑の領域グラフ：利用者→ネットワーク

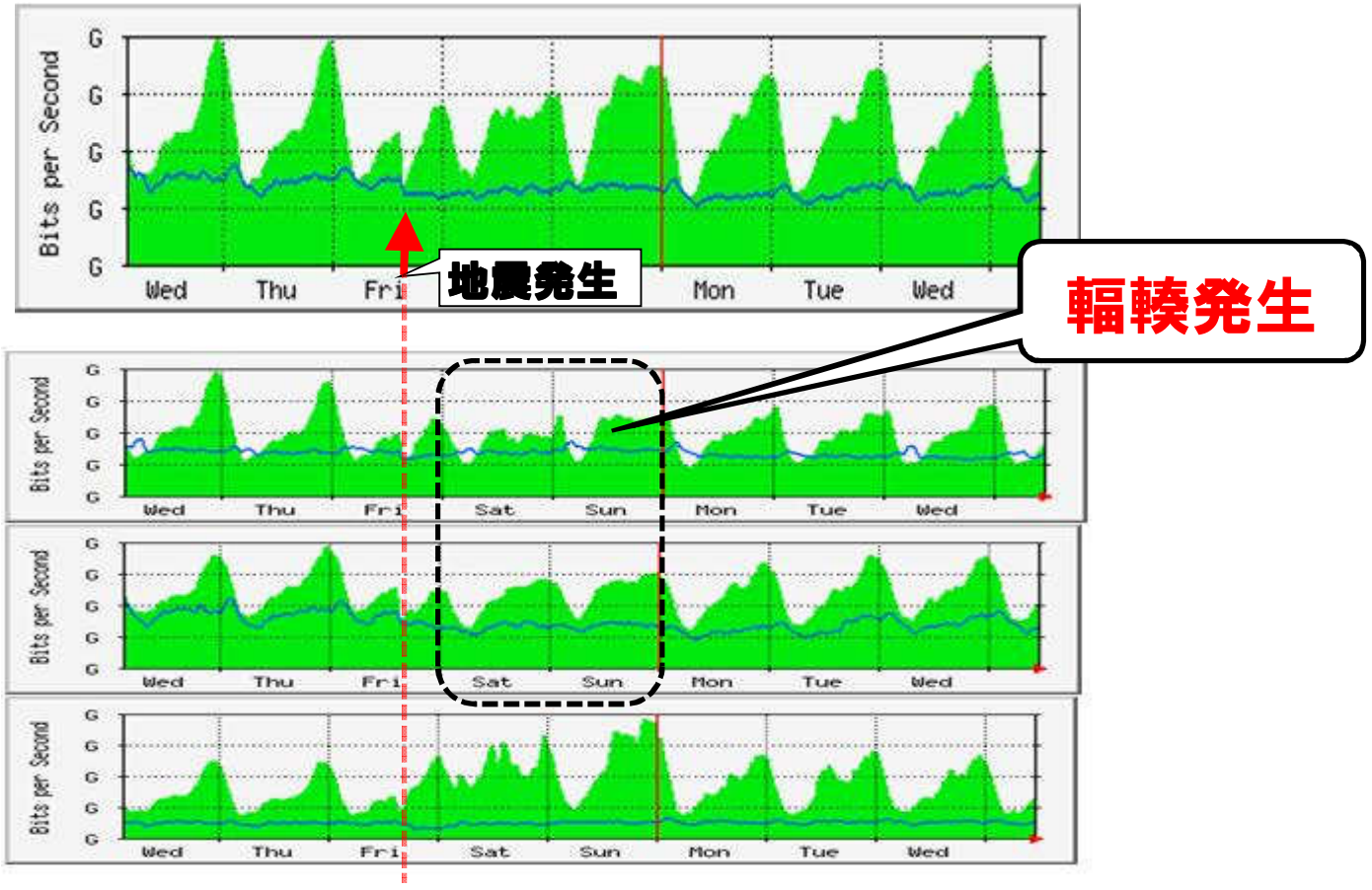
東京



震災地域以外では利用は平常どおり

東日本大震災によるビッグローブ通信への影響③

＜海外回線の震災直後輻輳状況＞



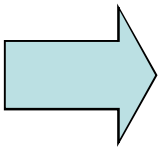
輻輳回避のため、ISPが一斉に空き業者Cにトラヒックを
まわすと輻輳が移転した可能性があった。

東日本大震災におけるインターネットの利用状況

○インターネットにアクセスできれば、メール、SNS、Twitterなどが使用でき、リアルタイムな安否確認や情報発信が行われた

○一部行政機関や電力会社等インフラ機関のHPにアクセスが集中し閲覧が困難になった事象があったものの、固定系・移動系とも比較的安定的に利用可能であった

○避難所検索や地図情報と組み合わせることにより付加価値のある情報提供が行われた。被災した自治体等の業務運営を支援するクラウドサービスが提供された



災害時におけるインターネットの有効性が示された。
今後も、災害に強いインターネットのネットワーク構築、
インターネットの効果的な活用を推進すべき。しかし．．．

大震災を踏まえた今後のインターネット系情報通信のあり方

①ISPのネットワーク構造見直し

・首都圏における大規模災害等に備えた災害に強いインターネットのネットワーク構築が必要
・緊急事態においても稼働することが可能なネットワークを作るためには費用回収構造の在り方の検討が必要

②災害発生時に備えた事業者間協力体制の構築

・災害発生時の通信疎通のための事業者間協力

③インターネットのより効果的な活用

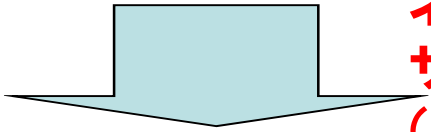
・インターネットの活用事例を収集・公表し広範に共有
・“マイナンバー”“自治体クラウド”の一層の推進

大震災の教訓は本質的なパラダイムシフトとして活かすべき！！

①ISPのネットワーク構造見直し

○現状の課題

・ISPの現状ネットワーク構造は東京集中型
・東京で同様な震災が起きた場合には壊滅的な影響が予想される
・集中ネットワーク構造となったのは、急速なトラヒック増に比して
収益が横ばいの構造だったことによるコスト削減の結果



ネットワーク設備をきちんと構築しその上で
サービス提供する事業者が報われるべき
（バランスのとれた競争、ユーザ理解、産業構造）

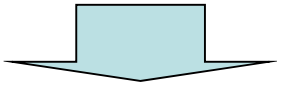
○今後の対応

・米国FCCの動向を踏まえ、ネット中立性についてあらためて議論すべき
→利用の公平性、コスト負担の公平性を担保する仕組みの確立
・キャリアとISPの役割分担、インフラ投資の在り方
→キャリア、ISPが一体となった信頼性の確保
・ユーザの理解を得るためのオープン性の確保
→トラヒック等の基礎情報の公開、ユーザから見てわかりやすい
インターネットのコスト構造の公開

②災害発生時に備えた事業者間協力体制の構築

○現状の課題

・東日本大震災においては海外回線が切断されたため、一部海外回線に輻輳が生じた
・現実には、各ISP同士の情報共有により輻輳の増大は回避された
・しかしながら、その際、各ISPが独自に入手した情報に基づき、各々が輻輳回避行動を取った場合、輻輳を起こしていない回線にトラヒックが集中し、かえって輻輳を増大させる可能性があった



○今後の対応

・災害発生時の通信疎通のための事業者間協力
　→情報共有や協力窓口の整備を行い、平時から関係者間で体制構築
・インターネットトラヒックのさらなる増大に向けた対応
　→より安定的なサービスを確保するため、サービスの需要に応じて、異なる通信サービス間での効率的かつ即時に通信リソースを融通するための研究開発

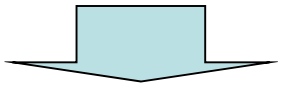
③インターネットのより効果的な活用

○現状の課題

・携帯電話のメールは輻輳状態になりやすい音声通話の代替としての期待が大きいが、今回の震災ではメール遅延が発生

・災害時にヘビートラヒック等が発生した場合、通信全体の疎通性を確保するためのトラヒック制御について検討すべき

・ほとんどの避難所等においてはインターネットを利用できる環境にはなかったため、クラウドサービスを活用した避難所運営の支援ツールなど十分利用することができなかった



○今後の対応

・携帯電話のメール遅延対策として、今回の震災での実態を踏まえて、メールサーバの増強・改善などその対応の在り方を早急に検討すべき

・通信全体の疎通性を確保するためのトラヒック制御については、帯域制御ガイドラインの見直しを早急に行うべき

・指定避難所等には平時からインターネットアクセス環境を整備すべき

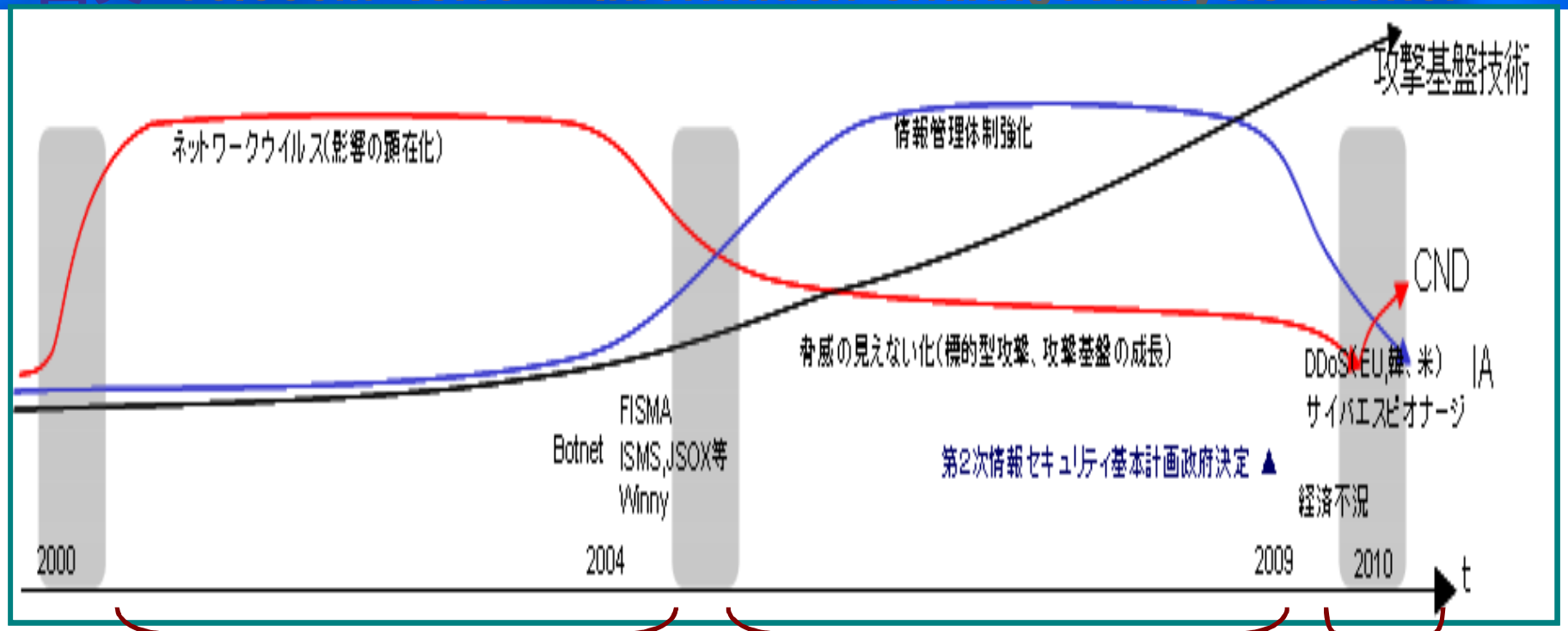
・行政機関等によるソーシャルメディアサービスの活用の在り方を検討すべき

・インターネットの活用事例を収集・公表し広範に共有すべき

・自治体クラウド等クラウドサービスの積極的活用

情報セキュリティに係る脅威と課題の変質

出典：Telecom-ISAC <Information Sharing&Analysis Center>



サイバー攻撃の大規模化
日本官公庁サーバへの攻撃
NIMDA、Code Red、SQL Slammer、
Blaster/Sobig F

組織内情報管理体制構築の普及
サイバー攻撃(脅威)の見えない化
大規模サイバー攻撃の潜在化

大規模サイバー脅威の再発
(再表面化)
韓国7.7大乱(2009)
エストニア、グルジアへのサイバー攻撃

情報管理体制強化動向のトリガー
個人情報保護法(2003)
ISO/IEC 27001(2005)
JSOX法(2006)

Botnet脅威の拡大

脅威変質に追従するためには、対処戦略の考え方に変化が求められる－“Resilience”思考！

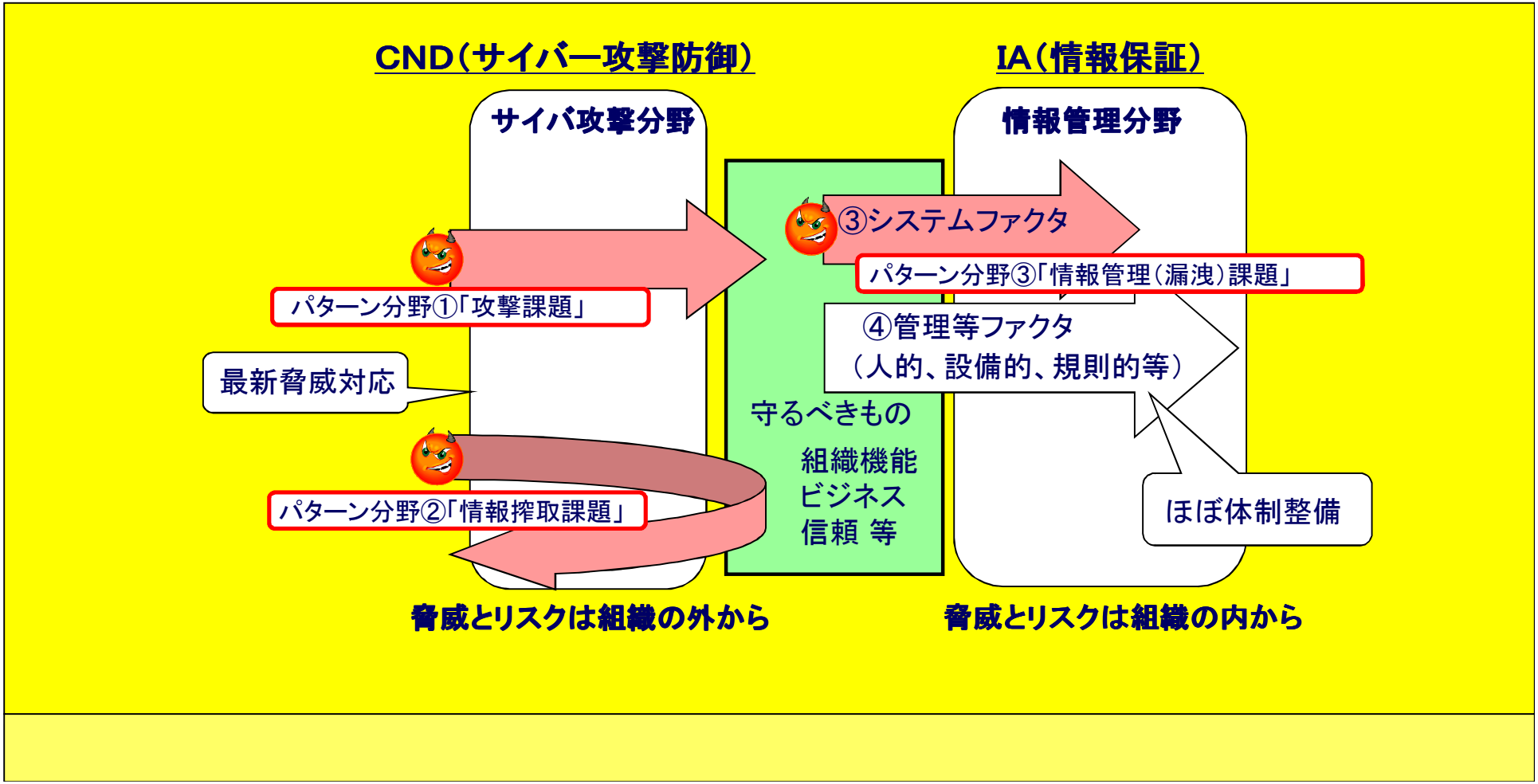
戦略変化のきざし：CNDとIA

日米政府動向： **情報セキュリティを CND (Cyber Network Defense) とIA (Information Assurance) に分けて考える**

米国の米国連邦政府のサイバーセキュリティ政策においても分けて考える動向

NISC（内閣官房情報セキュリティセンター）内でも情報セキュリティをCNDとIAとに分離した議論が進行中

【参考】ISO/IEC 27001:2005シリーズ、JIS Q 15001：2006では、一つの体系の中でまとめて（情報資産、サーバー防御、ネットワーク）見ていた。PCI DSS(2004年～)にて分離傾向が見られる



CNDに伴い整理すべき事項

問題意識：国民を守る情報セキュリティ戦略抜粋

「第2次情報セキュリティ基本計画」（平成21年2月2日）に基づき、官民の各主体によって取組が推進されてきた・・・他方で、「第2次情報セキュリティ基本計画」策定後、平成21年7月の米韓に対する大規模サイバー攻撃や大規模な個人情報漏えい事案の発生も後を絶たない・・・

- 日本におけるリアルの世界では、対抗手段・それを使う実施主体は（縦方向の）3つの階層で異なる
- たとえば、治安維持装備品（ピストル）は民間サービス業は使用できない
- 武器兵器（戦闘機、ミサイル）は民間サービス業も警察も使用できない
- CNDについてはどうか

ここのギャップは大きい！

重要事項	リアル世界における 主導主管庁	対抗手段	実行主体	行動原理	財務基盤資金調達先
国民の安全を守る	業界主管官庁	防災・防災設備	民間サービス業	平時活動分野 収益性に基づいた経済的競争領域として活動する分野	民間資金
	警察	治安維持装備品	警察庁	非競争領域分野	
国＿の安全を守る	首相官邸が危機管理省庁と連携して対応する	武器兵器	警備警察 自衛隊	武力攻撃事態（緊急対処事態）	税金

＜参考＞　米国の関心と日本の関心

サイバーセキュリティ・情報セキュリティに係る整理[7]

	政府（国防）	一般政府、重要施設（民間）	一般民間企業	個人
情報セキュリティ（広義）				
サイバーセキュリティ（悪意ある者によるオンラインを通じた行為からの保護）				
完全性 可用性	サイバー攻撃、サイバーテロ、クラッキング等			
機密性	サイバースパイ、不正アクセス、ハッキング等			
（非サイバーの）情報セキュリティ（非悪意的、又は、非オンラインにかかるリスク低減）				
完全性 可用性	（非オンライン）内部犯行によるシステム改竄等 （非悪意的）システム障害、バグ等			
機密性	（非オンライン）物理的情報流出、内部犯行による情報流出等 （非悪意的）情報流出ミス等			
cf.機密性の対象情報	国防機密情報	政府機密情報	企業機密情報	ID、個人情報

米国の関心

日本の関心

出典：「 米国連邦政府のサイバーセキュリティ政策を巡る動向」
http://www.jif.org/column/pdf2010/201003.pdf

Telecom-ISAC設立提唱時(2002. 7)のスローガン

“健全な競争は高邁なコラボレーションから”


BIGLOBE