NISC National Information Security Center

2008年度相互依存性解析について

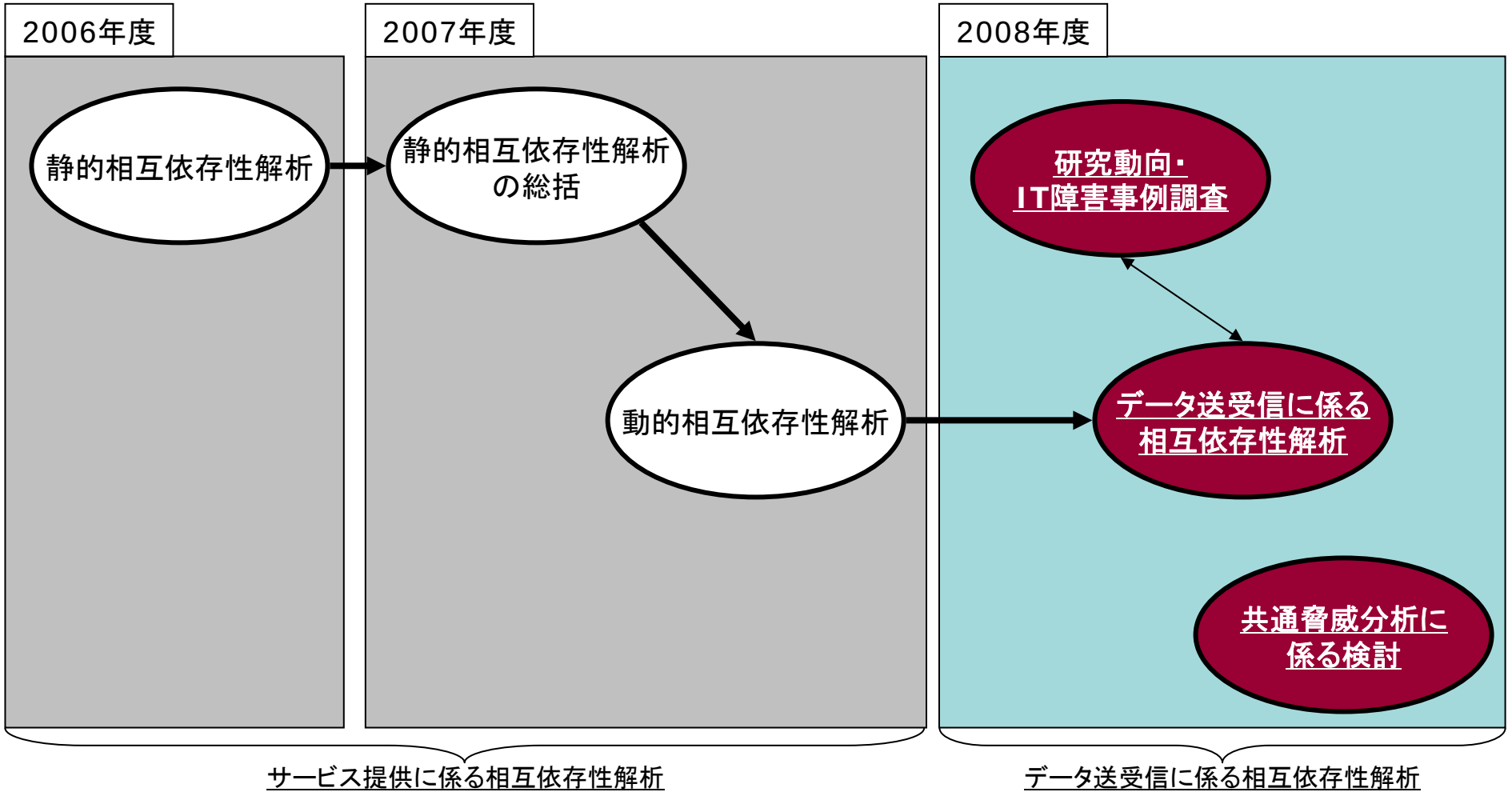
2009年5月8日

内閣官房情報セキュリティセンター（NISC）

資料6－2

相互依存性解析の実施項目

- 2006～7年度では、サービス提供に係る相互依存性の静的・動的解析に取り組んだ。その際、2008年度にデータ送受信に係る相互依存性解析が必要とされた。
- 2008年度は、データ送受信に係る相互依存性解析とともに、相互依存性に係る国内外の研究動向・IT障害事例調査に取り組んだ。また、第2次行動計画で実施することとなった共通脅威分析の準備も行った。



データ送受信に係る相互依存性解析の結果

- データ送受信に係る相互依存性解析の結果は以下のとおりである。

1. 金融、航空、物流各分野に着目して、各々の分野別送受信分析図を作成し、これらの重要インフラ分野と他の分野に対するデータ送受信関係を確認した（P3参照）。

2. データ送受信に係る相互依存性解析の視点として、国民等への影響も考慮する必要があることから、以下のように分析の対象を整理した。
   a. データ送受信に係る不適切な現象により、受信側の重要システムに機能不全が発生する場合や、国民等への影響が発生する場合を、データ送受信に係る相互依存性における波及として捉えた。
   b. データ送受信関係に係る相互依存性を、通信※・送受信システムの稼動状況により、以下のように大別した（P4参照）。
      ① 正常稼働時データつながり：通信※・送受信システムが正常に稼働している場合。
      ② 非正常稼動時データつながり：通信※・送受信システムが正常に稼働していない場合。

3. 波及の要因となるデータ送受信に係る不適切な現象を7種類（実際の分析では、更に14種類に細分）に類別した。

4. 作成した分野別送受信分析図からデータ送受信の例を選んで、不適切な現象が発生した場合の影響分析を試行し、以下の知見を得た。
   a. データ送受信に係る不適切な現象と、その影響の一般的特徴は、以下のように整理できる（P4参照）。
      ① 正常稼働時データつながり：波及の要因は論理世界の現象であり、影響範囲は局所的なことが多い。
      ② 非正常稼動時データつながり：波及の要因は物理世界の現象であり、影響範囲は広範なことが多い。
   b. データ送受信の個々のシチュエーションでは、発生しうる影響や、その影響を受ける主体が異なる場合がある。
   c. データ送受信に係る不適切な現象により、受信側に影響が発生するパターンの他に、受信側に影響が発生しない場合でも、国民等に影響が及ぶパターンがある。
   d. 波及が長時間に及んだ場合、短時間の場合とは異なる影響が発生する可能性がある。
   e. 個別打合せから得た知見として、種々の措置により、データ送受信に係る多くの不適切な現象が回避されている。

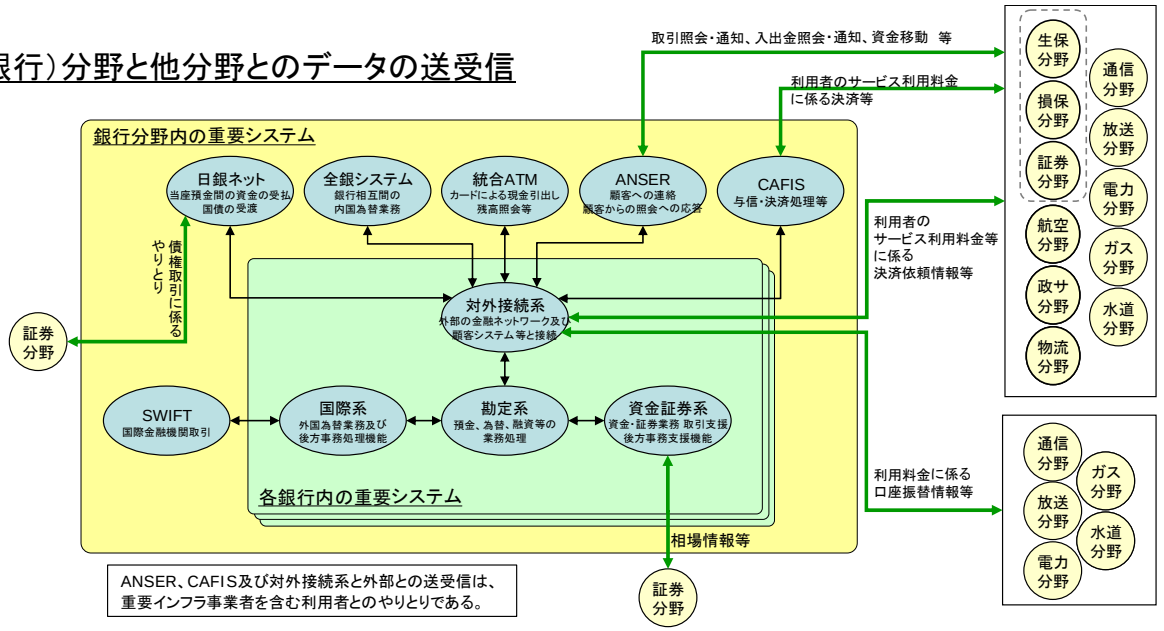
5. データ送受信に係る相互依存性解析の手法の一つとして、重要インフラ事業者等の関係者が、データ送受信に係る相互依存性における波及の影響を整理し、その対策を確認するための分析ワークシートを整備した（P5参照）。

※通信には、情報通信事業者が提供する回線の利用の他に、MTや紙媒体等の手交等によるデータのやりとりがある。

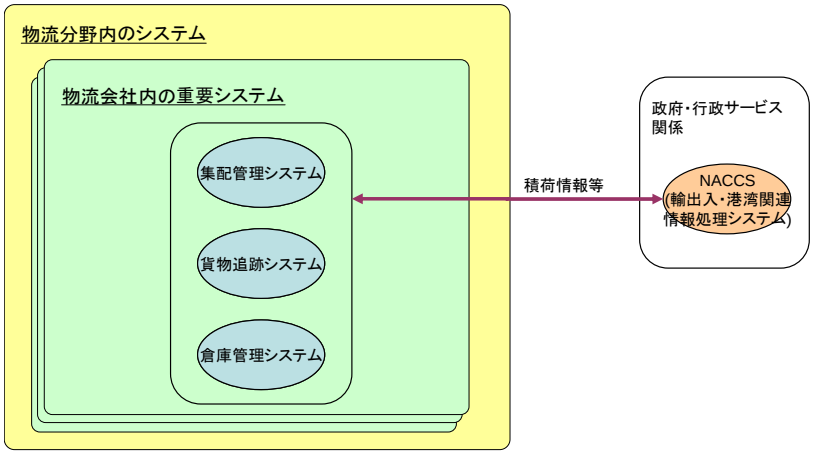
分野別送受信分析図の例

- 分野間のデータ送受信関係がある分野について、それぞれのデータ送受信の詳細を整理した分野別送受信分析図を作成した。

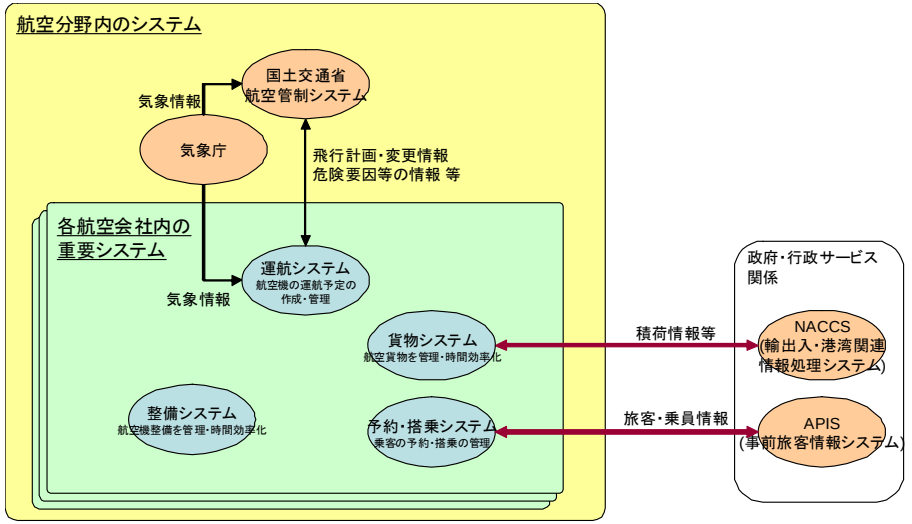
金融（銀行）分野と他分野とのデータの送受信



物流分野と他分野とのデータの送受信



航空分野と他分野とのデータの送受信



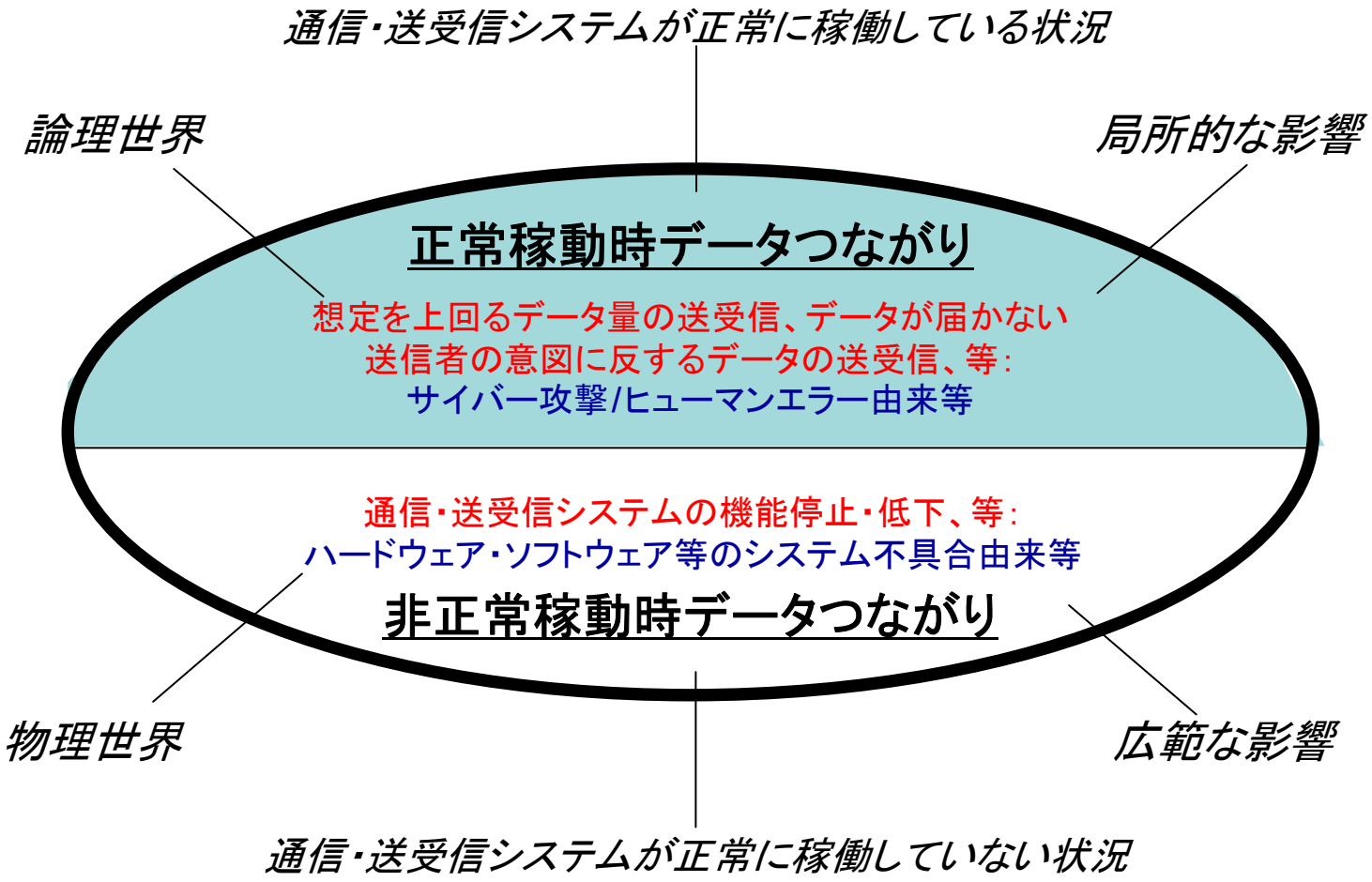
凡例：重要システム　他分野

→（通信事業者が提供する）専用線等によるデータのやりとり

→ インターネット経由（暗号化通信）、（通信事業者が提供する）専用線等を用いるデータ通信、MTや紙等の媒体によるやりとり

データ送受信に係る不適切な現象の特徴

- データ送受信に係る不適切な現象は、下図のように2つ（正常稼動時・非正常稼動時データつながり）に大別できた。
- 不適切な現象によって発生する影響は、上記の2つの分類ごとに、下図のように大略共通する特性を持つが、影響の形態や、その影響を受ける主体は状況によって異なる場合が多い。



分野相互依存分析のワークシートと手順

- データ送受信に係る波及の影響を定量的に把握し、対策を確認する手順を整理して実際に試行した。

下記ワークシートは仮想の「星」分野から仮想の「月」分野へのデータ送受信を想定した架空の分析イメージである。

補足）中間者攻撃等は右表の現象4に分類される。なお、各現象の典型的な原因は、国際標準(ISO、ITU-T)等で示される標準的なｾｷｭﾘﾃｨﾘｽｸ分析方法を一部参考とした。

①
ワークシート1枚を使用し、分野別送受信分析図から選定した分析対象の概要を、次のように記入
1)送受信分野名
2)送受信分野各ｼｽﾃﾑ名
3)ｻｰﾋﾞｽ名
4)送信データ名（ｼﾁｭｴｰｼｮﾝ）
5)通信手段

送信分野		通信手段	受信分野		分析ケース		データ送受信に係る不適切な現象		典型的な発生箇所と原因	受信側ｼｽﾃﾑ症状	サービスへの影響（◎：重大、○：ある程度、△：軽微、－：なし）			点	対策・受信側アクション		備考	特徴		
分野	ｼｽﾃﾑ		分野	ｼｽﾃﾑ	ｻｰﾋﾞｽ	ｼﾁｭｴｰｼｮﾝ					送信分野への影響	受信分野への影響	国民（ﾕｰｻﾞ）への影響		発生時	復旧時		範囲	特性	分類
「星」分野	ERPシステム	インターネット（TCP/IP）	「月」分野	統合受発注管理システム	物資受発注（受注内容に基く一斉発注）	生活物資直販を目的とする物資発注データの送信（定期）	1．ﾃﾞｰﾀが想定した時間に届かない	1.1データが想定した時間に間に合わない	送信側・業務上のヒューマンエラー等 ・サイバー攻撃等	・期日遅れ	数営業日の余裕を見た発注期日が決まっているため影響を未然に防止				・期日が遅れそうな場合、送信側に注意を喚起			局所	論理的	正常稼動時データつながり
								1.2データが想定した時間より早く到着	送信側・業務上のヒューマンエラー等	・2重発注発生（前回発注を再送信）	送信分野各企業からの発注は通常定期1回のため問合せにより影響を未然に防止				・送信側に問合せ		・人間系によるチェック。			
							2．想定を上回るﾃﾞｰﾀ量が発生	2.1正常データが大量に発生	送信側・非意図的処理の集中	・ビジー：当該機能停止	－ ・数営業日前が期日のため、特になし（一時的な場合）	○ ・発注データ受信サービス停止（一時的）	－ ・特になし（一時的な場合）	1.0	・発注データ送信予定者に障害を通知。	・状況によりサーバ増設	・長期の場合、物資の発注・送付への支障大			
								2.2仕様違反のデータが大量に発生	送信側・サイバー攻撃等	・エラー処理ビジー：当該機能停止	－ ・数営業日前が期日のため、特になし（一時的な場合）	○ ・発注データ受信サービス停止（一時的）	－ ・特になし（一時的な場合）	1.0	・発注データ送信予定者に障害を通知。	・ISPに対処依頼。	・長期の場合、物資の発注・送付への支障大			
							3．内容に問題のあるﾃﾞｰﾀを受信	3.1送信者に不利益なデータを受信	送信側・サイバー攻撃等（内部犯行）	・正常稼動（ｸﾚｰﾑがないと認識できない）	◎ ・直販計画に支障発生 ・物資不足の場合はﾕｰｻﾞからの信用低下。	－ ・特になし	◎ ・物資不足の場合、生活に影響。	4.5	・発生時対処不能	・DB復元作業発生	・異常に大量発注のあった場合は、人間系のﾁｪｯｸあり。			
								3.2送信者の意図しないデータを受信	送信側・業務上のヒューマンエラー等	・正常稼動	送信分野への発注確認情報送付により修正の機会有				・発注確認情報の自動送信（定常業務として）。	・修正された発注情報処理。	発注確認が見過ごされた場合は、3.1同様の影響有。			
							4．正常データに正常なサービスが施されない	4.1送信側の意図に反したｻｰﾋﾞｽを実施	受信側・サイバー攻撃等（改ざんされたｻｲﾄへのｱｸｾｽ等）	・発注ﾃﾞｰﾀ来ず	送信分野各企業からの発注は通常定期1回のため問合せにより影響を未然に防止				・発注期日遅れを送信側に注意喚起		・物資発注の情報漏えいの影響確認が必要。			
								4.2データが他所に着信して関知できない	通信路・サイバー攻撃等（送信先の粉飾等）	・発注ﾃﾞｰﾀ来ず	送信分野各企業からの発注は通常定期1回のため問合せにより影響を未然に防止				・発注期日遅れを送信側に注意喚起		・物資発注の情報漏えいの影響確認が必要。			
							5．通信システムの機能が停止・低下	5.1データが消失して届かない	通信路・通信/送信経路上の不具合・機能低下等	・正常稼動（ｸﾚｰﾑがないと認識できない）	△ ・応答なしｴﾗｰ発生により、発注ﾃﾞｰﾀを再送信（一時的な場合）	－ ・特になし（一時的な場合）	－ ・特になし（一時的な場合）	0.5	・発生時対処不能		・長期に及ぶ場合はシステムダウン相当の影響あり	広範	物理的	非正常稼動時データつながり
								5.2通信タイミングの遅延	通信路・通信/送信経路上の不具合・機能低下等	・ﾀｲﾑｱｳﾄｴﾗｰ	送信分野でのタイムアウトエラー対処のため発注データの再送が必要となるが、送信分野各企業からの発注は通常定期1回のため問合せにより影響を未然に防止（一時的な場合）						・長期に及ぶ場合はシステムダウン相当の影響あり			
							6．送信システムの機能が停止・低下	6.1送信側の機能停止	送信側・システムのハード/ソフト不具合等	・正常稼動	送信システムの二重化等により対処、最悪の場合も 数営業日の余裕を見た発注期日が決まっているため影響を未然に防止						・二重化の両方停止時は受信ｼｽﾃﾑ停止と同様の影響			
								6.2送信側の機能低下	送信側・システムのハード/ソフト不具合等	・正常稼動	送信システムの二重化等により対処、最悪の場合も 数営業日の余裕を見た発注期日が決まっているため影響を未然に防止						・二重化の両方機能低下時は受信ｼｽﾃﾑ停止と同様の影響			
							7．受信システムの機能が停止・低下	7.1受信側の機能停止	受信側・システムのハード/ソフト不具合等	・サービス停止	△ ・応答なしｴﾗｰ発生により、発注ﾃﾞｰﾀを再送信（一時的な場合）	◎ ・停止サーバに関する全ｻｰﾋﾞｽ停止（一時的な場合）	－ ・特になし（一時的な場合）	2.0	・送信予定者全員に障害を通知 ・ISPに対処依頼	・ITベンダに対処依頼 ・送信側に通知	・長期の場合、送受信・国民への影響発生			
								7.2受信側の機能低下	受信側・システムのハード/ソフト不具合等	・サービス機能低下	△ ・応答なしｴﾗｰ発生により、発注ﾃﾞｰﾀを再送信（一時的な場合）	○ ・発注データ受信サービス処理速度低下等（一時的な場合）	－ ・特になし（一時的な場合）	1.5	・送信予定者全員に障害を通知 ・ISPに対処依頼	・ITベンダに対処依頼 ・送信側に通知	・長期の場合、送受信・国民への影響発生			

注） ﾃﾞｰﾀつながりの特徴から洗い出した不適切な現象とその典型的発生箇所と原因。この“不適切な現象”発生時の影響を本表で検討する。

② “データ送受信に係る不適切な現象”毎に、最悪の“受信システム症状”と送受信分野・国民への“影響”を検討して記入（影響の大きさにより背景色を変え（◎はﾋﾟﾝｸ等）、時間経過で影響の変わるものは赤字とする）。

③ 送信、受信、国民の影響の和を入力(定量化の基準は、◎通常1.5点、国民の影響の場合は2倍の3点、等)。点数の高いものについては特に対策の確認に力を入れる。

④ 受信側アクション・備考を検討して記入（時間経過の影響は赤字で備考に記入）。

相互依存性の係る研究動向・IT障害事例調査の結果

- 相互依存性に係る国内外の研究動向・IT障害事例調査の結果は以下のとおりである。

1. 相互依存性に係る研究動向調査として、以下の対象を取り上げ、文献調査、対面調査、Eメールによる情報交換、学会参加による情報収集等を実施し、相互依存性解析の観点で取りまとめた。
   a. 国内外の調査研究プロジェクト(3件):
      ① 相互に連関したライフラインの復旧最適化に関する研究(首都直下地震防災・減災特別プロジェクトの一環)
      ② IRRIIS (Integrated Risk Reduction of Information-based Infrastructure Systems)
      ③ DIESIS (Design of an Interoperable European federated Simulation network for critical InfraStructures)
   b. 研究組織(1件):TNO(オランダ応用科学研究機構)
   c. 国際会議(1件):CRITIS(CRITICAL INFORMATION INFRASTRUCTURE SECURITY) 2008
   d. 専門書籍(1件):CRITICAL INFRASTRUCTURE –Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies–

2. 調査研究プロジェクト(3件)を、ITに係る相互依存性解析の観点で調査したところ、以下のように防災が中心課題であることが分かった(P7参照)。
   a. 調査研究プロジェクトでは、過去に大規模な影響を及ぼした災害等に着目し、その被害軽減を大きなテーマとしており、ITに係る相互依存性への関心は、現状ではそれほど高くない。
   b. 調査研究プロジェクトでは、過去の災害等の経験に基づき重要と考えられる重要インフラ分野に絞ったアプローチとなっている。

3. 相互依存性に係る研究動向調査により、今後の分析の参考となる以下の知見が得られた。
   a. 防災に係る相互依存性を分野間のマトリックスで図表化するなど、応用可能な分析手法
   b. 事案発生時における影響の波及予測を目指すシミュレータ開発とその普及等、意欲的な働きかけの実施
   c. 相互依存性における様々な視点の整理方法、他

4. 相互依存性に係るIT障害事例調査により、国内外で7件の事例を把握した。なお、IRRIISで着目しているテレコムイタリアの事例のようなIT障害は、日本国内では以下のような点で条件が異なっている(P8参照)。
   a. 冷却水等の水漏れ対策については、設置ガイドライン等の整備により、浸水による電源設備への影響は起こりにくい。
   b. 電力供給は通信分野に依存していないため、通信分野の障害は電力供給に影響しない。
   c. 通信、電源の二重化が進んでおり、通信回線、電力供給の途絶は起こりにくい。

調査対象プロジェクトの比較

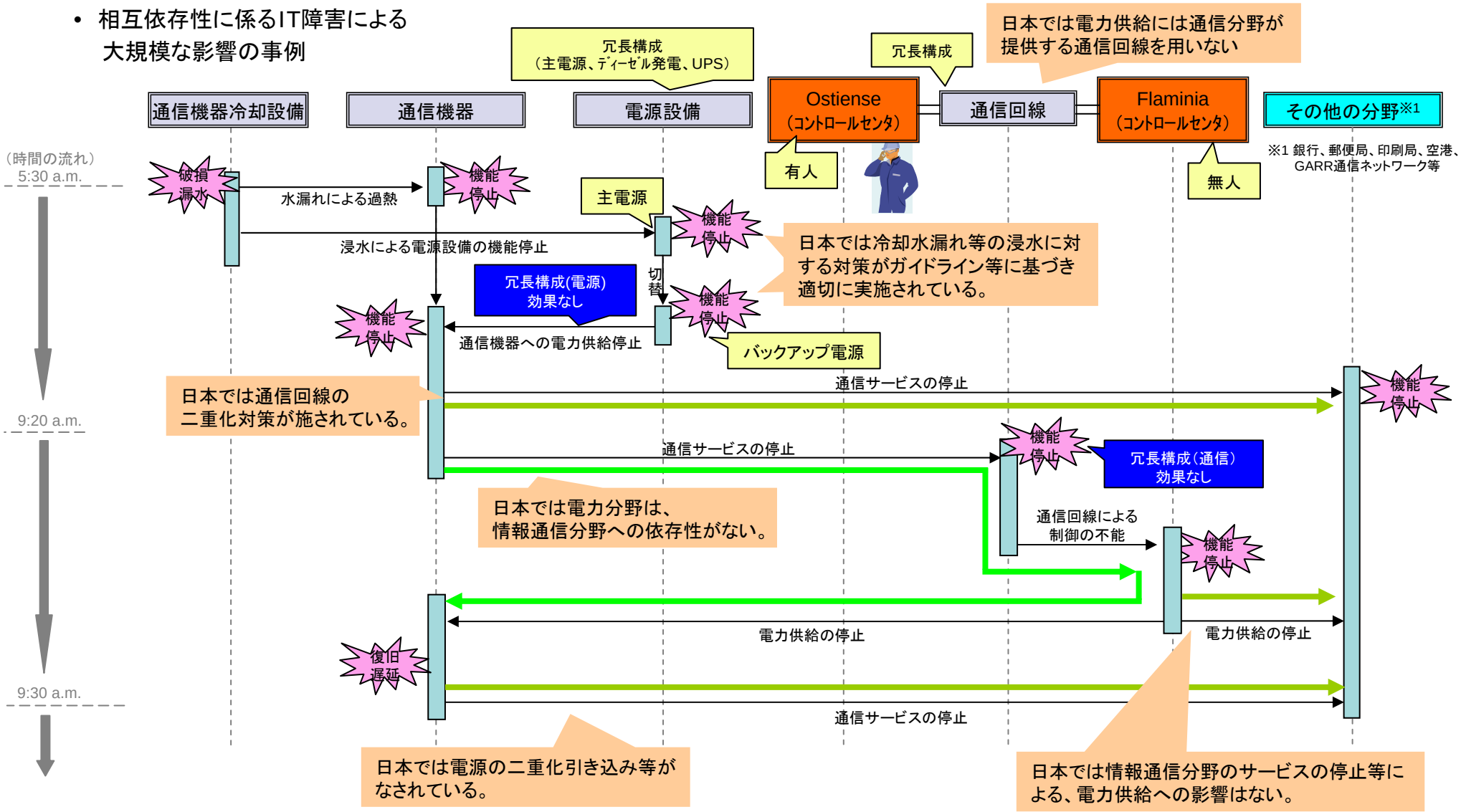
- 相互依存性解析に関連する調査対象プロジェクトの比較結果は以下のとおりである。

	比較項目	相互依存性解析関連プロジェクト			
		相互依存性解析 （重要ｲﾝﾌﾗの情報ｾｷｭﾘﾃｨ対策に係る行動計画の一環）	相互に連関したライフラインの復旧最適化に関する研究（首都直下地震防災・減災特別プロジェクトの一環）	IRRIIS （Integrated Risk Reduction of Information-based Infrastructure Systems）	DIESIS （Design of an Interoperable European federated Simulation network for critical InfraStructures）
構成	1. 実施主体等	NISC	京都大学防災研究所	Fraunhofer IAIS等16機関	Fraunhofer IAIS等5機関
	2. 期間	2006年4月～2009年3月	2007年6月～2011年3月	2006年2月～2009年7月	2008年2月～2010年1月
	3.地域	日本	日本	欧州	欧州
背景	4.きっかけとなる主な事案	中央省庁等に対するｻｲﾊﾞｰ攻撃	阪神・淡路大震災等	テレコムイタリアにおける障害等	欧州広域にわたる停電等
	5. 動機	増大する脅威への対応	再発時の被害軽減	再発時の被害軽減	再発時の被害軽減
目的	6. 活動目的	官民連携と重要インフラのセキュリティ対策強化	首都直下地震被害の大幅軽減と首都機能維持	欧州全体における重要インフラの信頼性・回復力の向上	欧州特有の重要インフラ防護に係る懸案事項の解決
	7. 対象分野	重要インフラ分野（10分野※1）	重要インフラ分野（13分野※2）	情報通信分野、電力分野	欧州の関連するステークホルダー全体（特にエネルギー、情報通信、水及び輸送分野）
	8. 展望	ITの社会への円滑な浸透	30年以内に発生する首都直下地震対策	停電や自然災害等による波及被害の未然防止、被害拡大の最小化	欧州全体のインフラに係るシミュレーション・解析を実施するためのセンター（EISAC）実現に向けた検討
活動	9. 活動内容	調査、報告	調査、報告	解析・モデルリング、ツール開発、実験　等	調査、ミドルウエア開発、報告　等
	10.注目する過去の事例	－	過去の都市災害	テレコムイタリアにおける障害等	欧州広域にわたる停電等※3
成果	11.期待される主な成果	重要ｲﾝﾌﾗの情報ｾｷｭﾘﾃｨ向上のための、以下に資する基礎資料 ①事業継続計画 ②復旧優先順位 ③重要インフラ連携	・災害時の被害波及構造の整理 ・被害波及モデルと解析法の開発	有効活用できる、以下のツールの開発 ①SimCIP（シミュレーション） ②MIT（コミュニケーション、アドオン等）	国・分野における横断的な相互依存性に係るモデリング及びシミュレーション環境を実現するためのミドルウエアに関する仕様
	12.成果の用途	重要インフラ事業者等における安全基準、BCP策定及び所管省庁における政策、検査への反映	災害対応従事者、地域住民・企業への還元による地域抵抗力及び回復力の向上	関連するステークホルダー等への成果の供与	関連するステークホルダー等への成果の供与
	13.成果の形態	報告書	報告書	報告書、ツール　等	報告書、設計仕様　等
スコープ	14.IT系	◎		○	○
	15.防災系		◎	◎	◎

※1　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　　※3　参考URL：http://www.iht.com/articles/ap/2006/11/05/europe/EU_GEN_Europe_Blackouts.php
※2　電力、ガス、上水道、下水道、情報通信、道路、鉄道、港湾、航空、運輸・物流・旅客、金融、医療、行政（警察、消防含む）

テレコムイタリアの事例

- 相互依存性に係るIT障害による大規模な影響の事例



［出典元］IRRIISホームページ（http://www.irriis.org/）より作成

凡例：テレコムイタリア（情報通信分野）　ACEA（電力分野）　相互依存性（interdependency）　相互依存性（dependency）

3年間の相互依存性解析の結果

- 2006～8年度の3年間にわたる相互依存性解析の結果は以下のとおりである。

1. 重要インフラ分野の相互依存性解析の共通理解のために波及等の視点を整理し、サービス提供に係る相互依存性解析及びデータ送受信に係る相互依存性解析を実施した。

2. サービス提供に係る相互依存性解析では、以下のような分野間の相互依存性があることが分かった。
   a. 「情報通信分野（通信）は他の7分野と」、「電力分野は他の10分野と」、「水道分野は他の8分野と」サービス提供に係る相互依存性がある。

   b. 波及が長時間に及んだ場合、短時間の場合とは異なる影響が発生する可能性がある。

3. データ送受信に係る相互依存性解析では、金融、航空、物流の各分野について作成した分野別送受信分析図からデータ送受信の例を選んで、不適切な現象が発生した場合の影響分析を試行し、以下のようなデータ送受信に係る相互依存性の特徴があることが分かった。なお、影響分析の試行に当たっては、データ送受信に係る相互依存性解析の手法の一つとして整備した分析ワークシートを使用した。
   a. データ送受信に係る不適切な現象と、その影響の一般的特徴は、以下のように整理できる。
      ① 正常稼働時データつながり：波及の要因は論理世界の現象であり、影響範囲は局所的なことが多い。
      ② 非正常稼動時データつながり：波及の要因は物理世界の現象であり、影響範囲は広範なことが多い。

   b. データ送受信の個々のシチュエーションでは、現象が同じでも発生しうる影響や、その影響を受ける主体が異なる場合がある。

   c. データ送受信に係る不適切な現象により、受信側に影響が発生するパターンの他に、受信側に影響が発生しない場合でも、国民等に影響が及ぶパターンがある。

   d. 波及が長時間に及んだ場合、短時間の場合とは異なる影響が発生する可能性がある。

   e. 個別打合せから得た知見として、種々の措置により、データ送受信に係る多くの不適切な現象が回避されている。

今後の課題：共通脅威分析への展開

- 相互依存性解析を含む、重要インフラ分野共通に起こりうる脅威の分析（共通脅威分析）への対象範囲の拡大が必要。