「2009年度重要インフラの共通脅威分析に関する調査」の結果について

2010年9月9日

内閣官房情報セキュリティセンター（NISC）

1. 共通脅威分析の背景

重要インフラ各分野のIT障害に係る波及を視点とした相互依存解析の3年間の成果を踏まえ、重要インフラ事業者に共通に存在する情報セキュリティの脅威を分析

相互依存解析から共通脅威分析へ

Phase1　第1次行動計画
相互依存性解析

Phase2　第2次行動計画
共通脅威分析

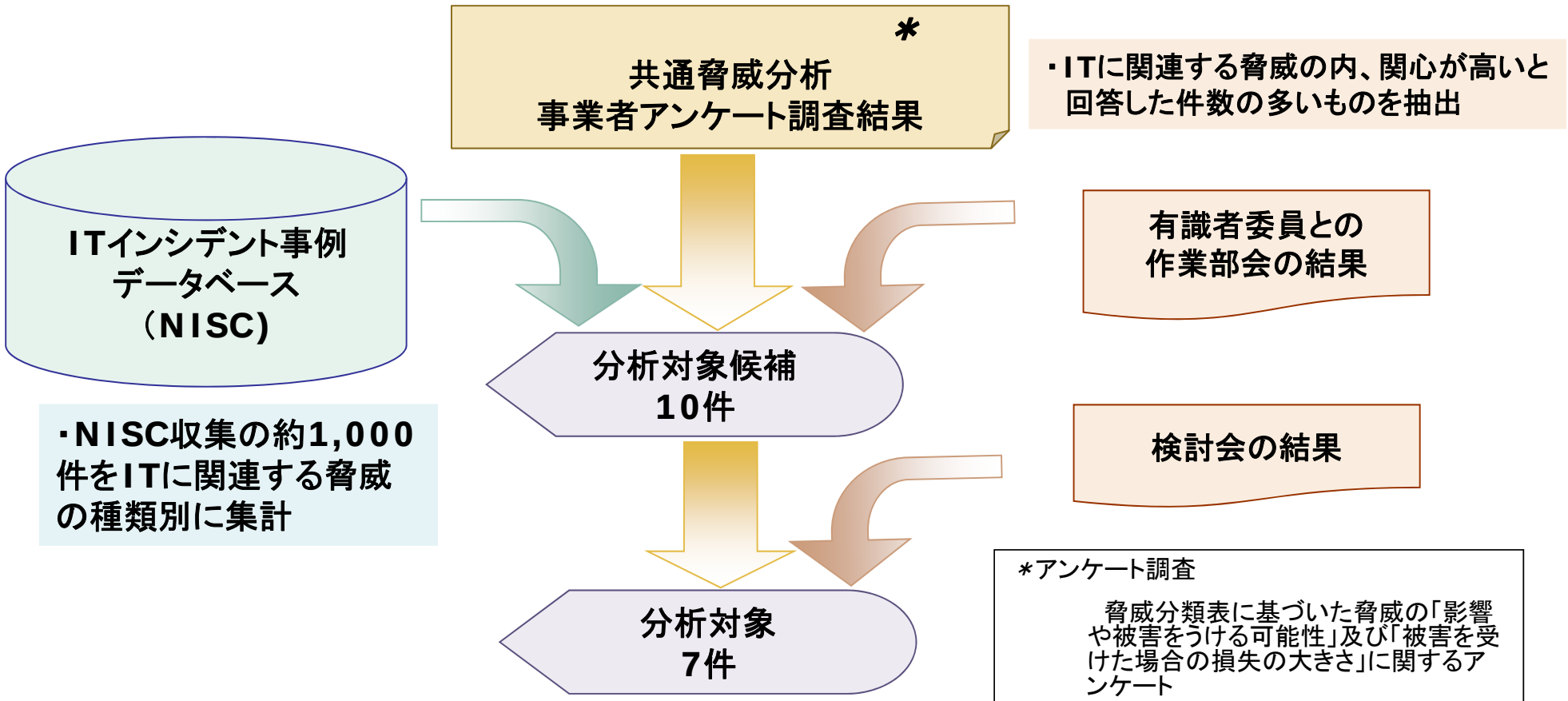
Step1	Step2	Step3	2009年	2010年～　2011年
2006年	2007年	2008年		
① 静的相互依存性解析 重要システムが他の重要システムにどのように依存しているか	① 静的相互依存性解析の総括 ② 動的相互依存性解析 IT障害時において時間経過とともに分野間の関係がどのように変化するか	① データ送受信に係る相互依存性解析 ② 研究動向・IT障害事例調査 ③ 共通脅威分析に係る検討 ある重要インフラ分野にIT障害が生じた場合に他のどの重要インフラ分野に影響が波及するか	①重要インフラ事業者等に共通に起こりうる脅威の分類 重要インフラ分野共通に起こりうる脅威は何か	①共通脅威分析 前年度成果等を踏まえ、対象をさらに絞り込んで分析を深化させる。

サービス提供に係る相互依存性解析

データ送受信に係る相互依存性解析

共通脅威分析

2. 共通脅威分析対象の決定手順



※共通脅威分析の検討に際しては、有識者、重要インフラ事業者等からなる検討会を設置し、適宜意見を聴取しながら実施。

3. 分析対象とした共通脅威の概要

IT関連脅威の分類			脅威によって発生する事象例
大	中	小　（分析対象）	
Ⅰ．意図的要因による脅威	１．分野システム運用上の脅威	・業務妨害目的のサイバー攻撃：業務妨害目的のサイバー攻撃による脅威	・同時大量送信（DoS攻撃）等によるシステムの機能不全 ・HP等の改ざんによる誤情報の流布
Ⅱ．非意図的要因による脅威	１．分野システム開発・保守上の脅威	・設計上の欠陥やプログラミング上のバグ：システムの設計上の欠陥やプログラミング上のバグによる脅威	・ソフトウェアの欠陥から起こる誤処理やシステムの機能不全 ・オフショア開発における低いシステム品質（ｺﾐｭﾆｹｰｼｮﾝｷﾞｬｯﾌﾟ等による）
		・システム設定上のミス（誤った運用、設定ミス、データの取り違い等）：システムの設定ミスによる脅威	・サーバ（ホスト）の運用ミスによる不正確な処理結果 ・データベースのセキュリティ上の設定ミスによる情報の漏えい ・パラメータ類の設定ミスによるシステムの機能不全
		・メンテナンス作業上の不備：システムバージョンアップ及びメンテナンス作業の不備による脅威	・不十分なテスト等によるシステム更新直後の機能不全
	２　分野システム運用上の脅威	・操作等のヒューマンエラー（不十分な訓練/マニュアルの不備/不十分なユーザインタフェース）：不十分な訓練、マニュアルの不備等が招く操作等のヒューマンエラーによる脅威	・メールの誤送信（アドレスのミス）等による情報漏えい ・誤ったデータ入力による市場の混乱 ・誤操作からのリカバリ不成功による業務の混乱
		運用ルールの不備・違反（特にコーポレートガバナンスを適用しない自宅等の環境下でのPC利用による脅威）	・自宅業務中における、私用PCのWinny暴露ウィルス感染による情報流出 ・USBメモリ等の紛失等、データの持ち出しによる情報流出
Ⅲ災害や疾病による脅威	１　分野システム範囲外の脅威	・パンデミック等によるシステムの操作・管理要員不足：新型インフルエンザ疾病によるシステム要員不足の脅威	・新型インフルエンザ等による要員の移動制限に伴うシステムの機能不全

4. 具体的題材による共通脅威分析の手順

5.　共通脅威に対する対策事例

IT関連脅威の分類			対策の例
大	中	小	
Ⅰ. 意図的要因による脅威	1. 分野システム運用上の脅威	・業務妨害目的のサイバー攻撃：業務妨害目的のサイバー攻撃による脅威	●外部との接続がないようにクローズなネットワークを構築している
Ⅱ. 非意図的要因による脅威	1. 分野システム開発・保守上の脅威	・設計上の欠陥やプログラミング上のバグ：システムの設計上の欠陥やプログラミング上のバグによる脅威	●ソフトウェア信頼性向上のためのガイドラインを自社で別途作成している ●アプリケーション開発に対してはコーディングルールまで規定している ●脆弱性診断を実施している ●外部機関によるコーディングチェックを実施し、バグの削除に努めている
		・システム設定上のミス（誤った運用、設定ミス、データの取り違い等）：システムの設定ミスによる脅威	●テスト等に費やすため工期を長めにスケジューリングしている ●設定ミスについては極力人手を介在させないよう工夫している
		・メンテナンス作業上の不備：システムバージョンアップ及びメンテナンス作業の不備による脅威	●運用保守業務は基盤を構築したベンダー1社に委託している ●バージョンアップについてはガイドラインを定めている ●何時でも元の状態に戻せるように工夫している ●ホットスタンバイシステム切り替えの定期的な実施訓練
	2. 分野システム運用上の脅威	・操作等のヒューマンエラー（不十分な訓練/マニュアルの不備/不十分なユーザインターフェイス）：不十分な訓練、マニュアルの不備等が招く操作等のヒューマンエラーによる脅威	●クロスチェック、複数人による作業、事前確認、具体的事例に基づく勉強会を開催している
		運用ルールの不備・違反（特にコーポレートガバナンスを適用しない自宅等の環境下でのPC利用による脅威）	●セキュリティ管理対策を徹底している ●監査指針、検査マニュアルの中で管理体制を見直している ●社内データの持ち出し自体が服務規程違反として罰せられる
Ⅲ. 災害や疾病による脅威	1. 分野システム範囲外の脅威	・パンデミック等によるシステムの操作・管理要因不足：新型インフルエンザ疾病によるシステム要因不足の脅威	●ITベンダの要因確保が困難な場合のために、自社社員がシステム運用、電源管理ができるように訓練を行っている ●パンデミック発生時のBCPを作成し、訓練を実施している ●宿泊施設の確保やその宿泊施設と職場間のシャトルバスの運行等を確保している
脅威全般			●起きたトラブルの徹底分析、原因の追究 ●悪い情報（失敗や落とし穴）の共有やIT業界全体、所管省庁の動向の情報収集 ●開発・運用含めてベンダー1社に委託している

6. 共通脅威分析の成果

◆重要インフラ事業者等に共通に起こりうる脅威は、①外部からの脅威、②システム自体が抱える脅威、③運用・管理体制における脅威、のほか、④システムを取り巻く環境における脅威、⑤社会・制度における脅威　の5つに分類できた。

システムの開発・運用面

システムごとにSIerが異なり、システム要素ごとに下請けや孫請けのベンダが受託しているため、システム全体を統一的に管理することが難しい

システムの構成要素

製品自体がマルチベンダ化しており、コストを抑えるためにオープン化されたコンポーネントから構成されており、メンテナンスが困難なレガシーコンポーネントも存在する

システムの大容量化・高速化・大規模化

大容量データを瞬時に処理しなければならず、外部接続とのIP化に対する対応が必要となってきている

共通脅威の概要

①外部からの脅威

サイバー攻撃は脅威となり得る

業務妨害目的のサイバー攻撃

②システム自体が抱える脅威

・コンポーネント間の関係が複雑化しており、システム更新による影響が把握しきれない
・COBOL等のレガシーコンポーネントのメンテナンスが困難になってきている

システム設定上のミス

設計上の欠陥やプログラミング上のバグ

③運用・管理体制における脅威

・外注先からの重要機密情報や顧客情報の漏えいは把握できない、特に海外へのアウトソーシングでは困難である
・非常時対応の際にITベンダーのリソースの取り合いになる可能性がある
・トラブル発生時、責任分解点が明瞭ではない

メンテナンス上の不備

操作等のヒューマンエラー

運用ルール上の不備・違反

パンデミック等によるシステムの操作・管理要員の不足

④システムを取り巻く技術環境における脅威

・オープン化、IPv6への移行、クラウドコンピューティング、IT業界の流れ等の技術変化への対応が脅威となり得る
・新たな技術の導入に伴うバグ、処理速度の低下等の影響は脅威となり得る
・重要システムを取り巻くファシリティ環境の実態が把握できていない

⑤社会・制度における脅威

・サービス要求の高度化、課金形態の複雑化等の社会的変化への対応が厳しい
・データセンター運用のための制度的な課題が整理されていない
・脆弱性の取り扱いに対する発注側と受注側の合意がなされてない