「2013年度重要インフラの分野横断的演習に関する調査」の結果について

2014年3月11日
内閣官房情報セキュリティセンター(NISC)

「CIIREX 2013 」(シーレックス2013)
<Critical Infrastructure Incident Response EXercise 2013>

1　分野横断的演習の要点

・IT障害に適切に対応するには、連絡体制や対応手順などを含むBCP等の整備が必要です。
・BCP等の実効性の確保には**演習や訓練により、その検証と改善**を重ねることが不可欠です。

分野横断的演習とは

①官民の重要インフラ関係者が一堂に会する演習

重要インフラ事業者・セプター
（10分野・15セプター）

情報通信（通信、ケーブルテレビ、放送）、金融（生保、損保、銀行、証券）、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流

NISC

情報共有体制の検証

所管省庁
金融庁、総務省、厚労省、経産省、国交省

※2013年度は61組織・212名が参加

②官民／事業者間連携の検証が可能

・外部組織との情報共有体制等について検証が可能です。
・多く企業・団体が参加するため実践的な検証が可能です。

③他事業者との意見交換により新たな気づきが期待できる

・演習実施後には意見交換会を行い、相互の情報共有を図ります。
・他事業者の取組みや専門家（有識者）のアドバイスなど、自社の参考になる情報が得られます。

2013年度の分野横断的演習

テーマ
情報セキュリティインシデントの対応

検証課題

（1）情報セキュリティインシデントに関する情報共有体制
（2）情報セキュリティインシデントへの対応
（3）BCP等※の発動・解除方法

※BCP等：BCPそのものだけではなく、情報システムに関するIT-BCPや障害対応手順、システム操作マニュアル等の関係する文書を含む

得られた気づきの例
・社内の総務・企画部門との情報連携に課題を感じた。
・複数のシステムに障害が発生した際に、復旧の優先順位が課題となった。

⇒演習で得られた気づきや知見を「**情報セキュリティインシデント対応のためのチェックリスト**」としてまとめました。（本資料に添付）

2　演習の経緯－第2次行動計画における分野横断的演習の取組み

第1次行動計画（2006～2008年度）

【目標】 官民連携の充実

＜2006年度＞
官民連携の仕組みづくり

- **研究的演習**：演習実施概念、演習課題設定、演習手法の理解等を主眼として実施。
- **机上演習**：脅威として災害を設定し、会議形式の演習を実施。

＜2007年度＞
官民連携体制の機能向上

- **機能演習**：脅威としてDDoS攻撃を設定し、チーム毎に個室に分かれ、メールのみを利用した演習を実施。

＜2008年度＞
官民連携体制の実効性向上

- **機能演習**：参加者にIT障害の発生原因を知らせない等より現実に近い状況で、起こった現象に関する関係者間の情報共有により原因を特定し、サービスの維持・早期復旧や事業継続等を行っていく演習を実施。

分野横断的な演習手法に関する知見

第2次行動計画（2009～2013年度）

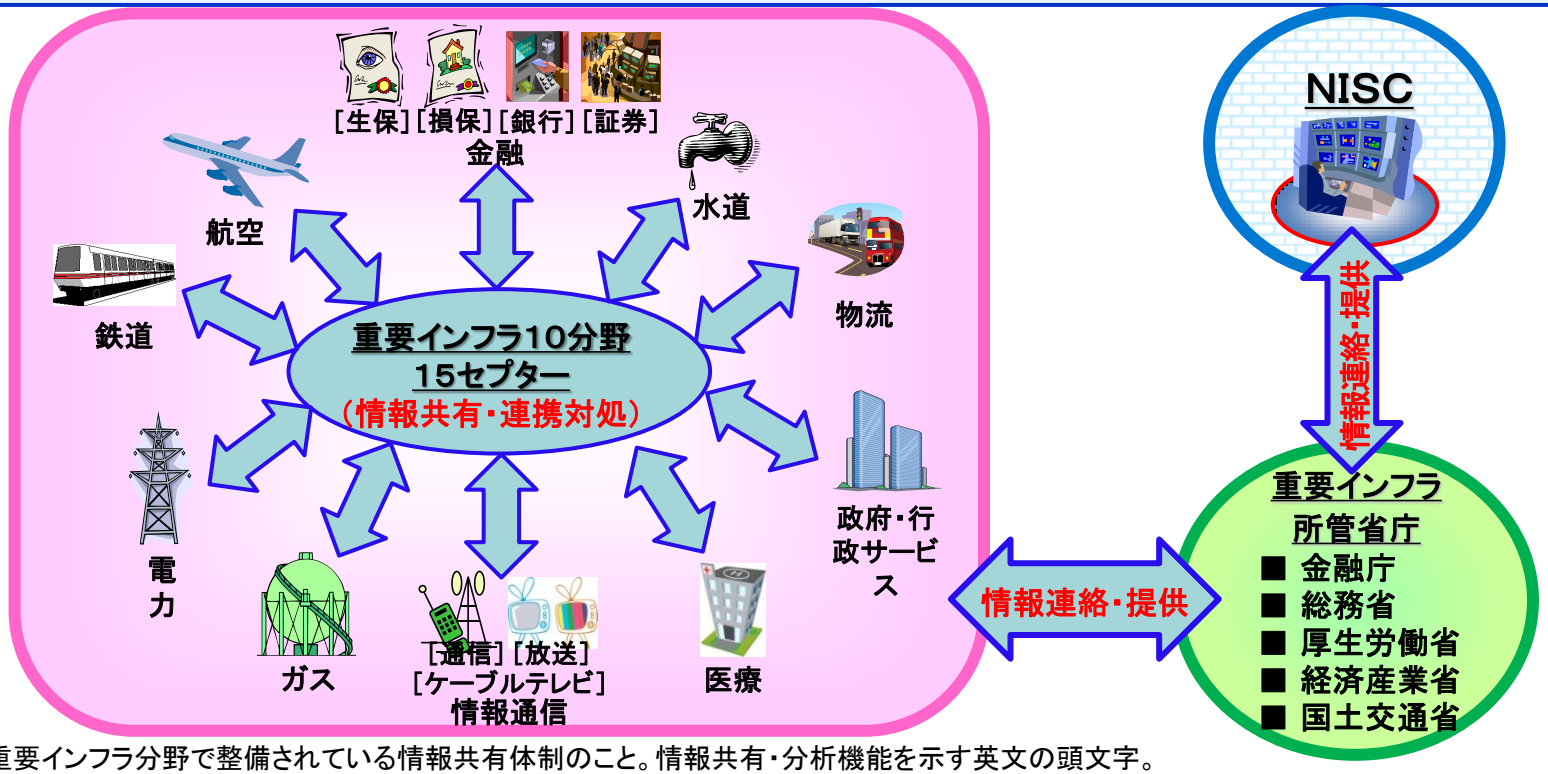
【目標】重要インフラ事業者におけるBCP等の実効性の確認・問題点抽出

①分野横断的な脅威に対する共通認識の醸成
②他分野の対応状況把握による自分野の対応力強化
③官民の情報共有をより効果的に運用するための方策

年度	2009年度	2010年度	2011年度	2012年度	2013年度
テーマ	広域停電	大規模通信障害	重要インフラ複合障害	重要インフラ複合障害＋便乗型ITインシデント	情報セキュリティインシデント
取組み	① シナリオ、実施方法、検証課題等を企画				
	② 早期復旧手順・事業継続計画等の検証、共有				
	③ 演習の実施方法等に関する知見の集約・蓄積				
		④ 自職場演習の導入			
			⑤ サブシナリオの導入		
			⑥ 重要インフラ分野、事業者間の連携推進		
				⑦ 第三者による助言の導入	⑦ 第三者による助言の充実

3　分野横断的演習の目的と参加機関、メリットについて

[目的]
　IT障害の要因となり得る事態に際し、重要インフラ各分野が的確に情報共有・連携し、IT障害の未然防止やIT障害に係る被害の最小化・早期復旧に関する検証を行なうことを目的とし、内閣官房情報セキュリティセンターの施策として、2006年度より継続実施（計8回）。
[参加機関]
　重要インフラ事業者等：　10分野（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流）
　セプター※1：　10分野の15セプター
　政府：　重要インフラ所管省庁（金融庁、総務省、厚労省、経産省、国交省）及び内閣官房情報セキュリティセンター（NISC）



※1　セプター：　各重要インフラ分野で整備されている情報共有体制のこと。情報共有・分析機能を示す英文の頭文字。

[分野横断的演習のメリット]
（1）分野横断的な脅威や各分野への波及（障害状況・対応など）の把握と、対応力の検証ができる
（2）官民間に加え、他分野、同業他社、関係機関等との情報共有や連携による対応力の向上を図ることができる
（3）他分野の対応方法や気づきを共有することで、新たな対応・改善方針を得ることができる

4　2013年度分野横断的演習実施概要

1. 日時：　2013年12月9日（月）　12:00　～　18:30
　　※　10:40～11:50　受付
　　※　10:45～11:45　ツール試用　（参加自由）

2. 場所：　株式会社三菱総合研究所（東京都千代田区永田町2－10－3）　4階会議室
　　一部事業者等における自職場

3. 参加者（プレイヤー、コントローラーを含む）：
　61組織212名が参加（内3組織10名が自職場参加）

（重要インフラ事業者等：**10**分野）
情報通信（通信、ケーブルテレビ、放送）、金融（銀行、生命保険、損害保険、証券）、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流
　※　証券事業者（1社）及び物流事業者（1社）が自職場演習

（セプター：**10**分野 **15**セプター）
　※　証券セプターが自職場演習、ガスセプターがサブシナリオ策定

（関係機関）　IPA、JPCERT／CC

（分野横断的演習検討会 有識者委員）
慶應義塾大学大学院　大林教授（座長）、名古屋工業大学大学院　渡辺教授（副座長）　他

（政府）
重要インフラ所管省庁、内閣官房情報セキュリティセンター

4. シナリオ概要
　複数の情報セキュリティインシデント予兆が検知される中、大規模な情報セキュリティインシデントが発生し、複数分野においてサービスへの影響が発生した。一部分野におけるサービスへの影響が他分野にも波及し、多くの重要インフラ事業者等において、インシデントの防止や被害最小化、あるいは事業継続のための、原因調査・復旧対応が求められた。

5　分野横断的演習の様子

事務局からの状況付与（各種障害状況、攻撃状況等）に従い、プレイヤーは、“メール”、“電話”、“掲示板（仮想HP）”等を用いて、他プレイヤーと情報共有しつつ発生した事象への対応を行う。
また演習後の意見交換会において、演習で得られた気づきを参加者間で共有する。

［演習当日のタイムスケジュール］

10:45　12:00　12:30　17:00　17:15　18:30

ツール試用	全体説明［約30分］	機能演習（個別部屋又は、自職場）［約4時間30分］	まとめ／休憩	意見交換会［約75分］

大部屋（集合）
個別部屋、自職場（分散）
演習（参加必須）

演習で使用する各種ツール（メール、掲示板等）の試使用、ホワイトボード書込み準備、通信確認などを事前に行う。

演習参加者全員が集合し、演習開会式の後、演習に関する留意事項等について説明。

演習参加者全員が集合し、演習における各事業者の対応内容の紹介や他分野事業者等への質問などの意見交換を行い、更なる気づきを得る。

［演習事務局、関係機関等］

・演習事務局は、各種障害状況、攻撃状況等を“メール”で付与する。
・関係機関は、“メール”又は、“掲示板（仮想HP）”でシナリオに則した関連情報の提供と共に、プレイヤー（事業者等）からの問合せ対応等もおこなう。

［事業者等、セプター］

［NISC、所管省庁］

［セプターカウンシル事務局］

演習参加組織毎に個室に分散し、演習事務局から与えられる状況付与（各種障害状況、攻撃状況等を“メール”で送信）や、関係機関から提供される情報（メールもしくは、掲示板［仮想HP］）に基づき、プレイヤーは、“メール”、“電話”、“掲示板（仮想HP）”、“ホワイトボード”等を用いて、他プレイヤーと情報共有しつつ発生した事象への対応を行う。

６　演習において得られた主な気づき（１）

■ 演習の事前説明会での講演や演習終了後の意見交換会等、分野横断的演習の取組み全体を通じて、各重要インフラ事業者等において、情報セキュリティインシデントの予兆検知時・障害発生時の情報共有・対処を効果的に行うための気づきを得ることができた。

演習において得られた主な気づき

●情報セキュリティインシデントに関する情報共有体制に関する気づき

・予兆をとらえるための情報収集先や収集内容の事前整理の必要性
・予兆を捉えた際やインシデント発生時における報告基準の明確化の必要性
・情報共有に関わる社内連携や対応フローの整備の必要性
・収集した情報の共有範囲の策定の必要性（予兆、インシデント）
・インシデント対処における情報収集の重要性
・インシデント発生時の情報収集先や収集内容の事前整理の必要性
・社内のインシデント対応状況集約に関する仕組み構築の有用性
・ネットワーク利用不可時の代替通信手段の確保
・インシデントに関する所管省庁への報告の判断基準の必要性
・外部への情報発信の有無、タイミングの判断基準の必要性
・HP利用不可時の代替情報開示手段の確保の必要性
・適時、適切に情報発信するための事前準備の有効性（フォーマットの作成等）
・メール利用不可時の分野内の情報共有手段確保の必要性
・他事業者や同業他社との情報共有方法に関する検討の重要性

7　演習において得られた主な気づき（2）

演習において得られた主な気づき

●情報セキュリティインシデントへの対応に関する気づき

・インシデントへの対応手順策定、体制整備の必要性
・被害想定の困難さや影響範囲が不明な中での対応の必要性
・想定される影響を踏まえた前広な対応の有効性
・既存の災害対応体制を活用したインシデント対応の有効性
・分野横断的・複合的な事象への対応検討の必要性
・イントラへの大規模インシデントを想定した対応検討の重要性
・制御システムへのインシデントを想定した対応検討の重要性

●BCP等の発動・解除方法に関する気づき

・情報セキュリティの観点を含めたBCP等策定の必要性
・BCP等を踏まえたシステム復旧順位の策定の必要性
・BCP等を踏まえたサービス継続と対応体制の検証の必要性

8 演習内容の総括

○検証課題の設定について	
・ほぼ全ての参加者が今年度の演習は有益だったと評価しており、検証課題の設定は概ね適切だったと言える。	
○検証課題ごとの評価	
情報セキュリティインシデントに関する情報共有体制	・予兆段階での社内外との情報共有についての検証ができ、不確実な予兆情報に基づく情報共有（判断基準や手順等）の改善に資する気づきが得られた。 ・インシデント発生時の情報共有についての検証ができ、共有すべき相手（政府、セプター、事業者等）や手段等、平時から点検しておくべき点に関する気づきが得られた。 ・他分野との情報共有のあり方について気づきが得られた。 ・情報開示は積極的になされ、複数の手段を用いての情報開示や顧客への影響に配慮した注意喚起等に関する気づきが得られた。
情報セキュリティインシデントへの対応	・インシデントの予防措置や対処についての検証ができ、複合的な障害における対応の優先順位付けや対応のルール・文書の改善に資する気づきが得られた。
BCP等の発動・解除方法	・情報セキュリティインシデントに対応するBCP等の内容や判断基準および対応内容についての検証ができ、これらの改善に資する気づきが得られた。

9 演習運営面の総括

○演習運営面の評価

・事前説明会を通じて参加者へ演習本番前に関係文書や体制の確認を促した結果、一部の参加者では、文書が最新の内容に更新されていない等の修正すべき点の発見につながった。一方で、シナリオの詳細が非開示だったため、文書や体制の事前確認を十分に行うことができなかったとの意見もあり、事前説明会を含めた演習実施方法の更なる検討が必要である。
・演習当日の意見交換会に加え、作業報告メモ、アンケート等の分析を踏まえた後日の意見交換会を開催することで、他事業者の取組みや気づきを共有できた。
・自職場から演習に参加した事業者では、実際の環境でより実践的に情報共有体制等の検証ができた。
・一部の分野では、セプターが事業者の検討を深める役割を果たし、より多くの気づきの創出を図る独自の取組みが行われた。
・第三者による助言は有益だとの意見が多かったが、演習参加者の増加に伴い助言の体制や実施方法のあり方について更なる検討が必要である。

○課題と今後の方向性

（1）参加者の特性や取組み等の多様性を踏まえた演習
・全分野共通の検証課題と、参加者の特性に応じて個別に設定する検証課題の整理
・個別に設定する検証課題に配慮した、シナリオ作成方法および演習実施方法の改善
・演習の自職場参加も活用し、より多くの参加者に対応できる演習実施形態を検討

（2）各参加者が効率的に演習の振り返りを行うための支援
・当日の時間配分を見直し振り返りの時間を確保
・効果的な振り返りを実現する仕組みづくり

（3）新規参加者の受け入れ拡大（重要インフラ防護施策の普及）
・新規参加事業者も取組みやすい難易度を下げた演習を一部取り入れることを検討
・新規参加がしやすい仕組みづくり（第三者助言の活用等）

情報セキュリティインシデント対応のための チェックリスト

２０１３年度分野横断的演習を通じて得られた知見をチェックリストにまとめました。
各チェック項目を確認・検討して頂くことにより、情報セキュリティインシデント発生時における情報システムの早期復旧及び各種サービスの継続能力の向上に寄与するものと考えておりますので、是非、ご活用ください。

セキュリティインシデント対応のためのチェックリスト①

1 情報セキュリティインシデントに関する情報共有体制

(1)情報セキュリティインシデント予兆時の社内外との情報共有

① 予兆に関わる情報収集方法

□ 予兆を捉える社内外の情報収集先や収集内容は整理されているか。

例）予兆に関して、セプター、JPCERT/CC、IPA、（所管省庁を通じた）NISC等の外部情報入手先からどのような情報が入手できるか確認。

例）予兆に関して、社内関係部門（CSIRT、情報システム部門、Web関係部門、現業部門等）からどのような情報が入手できるか確認。

② 対応判断の体制

□ 予兆を捉えた際、所管省庁等に報告するためのタイミングや基準が明確にされているか。

例）怪しいメールを受信した際、どのタイミングで標的型メールと判断し、どの基準（受信数、内容、マルウェアの攻撃力、影響等）で重大な事象と判断して所管省庁に報告するか確認。

□ 予兆に関する情報を共有するための、社内外の連携体制や対応フローが整備されているか。

例）予兆に関して、セプター、JPCERT/CC、IPA、（所管省庁を通じた）NISC等外部との連携体制や対応フローがあるか確認。

例）予兆に関して、CSIRT、情報システム部門、Web関係部門、現業部門等、自部門以外の社内部署が社外と直接情報共有する際に、自部門がどのように関わるか、中継するか確認。

③ 対応実施のための情報共有方法

□ 予兆に関する情報の共有範囲について定められているか。

例） 予兆に関して収集した情報を関係会社やグループ会社のどの範囲まで共有すべきか確認。

セキュリティインシデント対応のためのチェックリスト②

1 情報セキュリティインシデントに関する情報共有体制

(2)情報セキュリティインシデント発生時の社内外との情報共有

① インシデントの状況や影響把握のための情報収集方法

□ インシデント発生時の社内外の情報収集先や収集内容は整理されているか。

例)インシデント発生時、セプター、JPCERT/CC、IPA、(所管省庁を通じた)NISC等の外部情報入手先からどのような情報が入手できるか確認。

例)インシデント発生時、社内関係部門(CSIRT、情報システム部門、Web関係部門、現業部門等)からどのような情報が入手できるか確認。

② 対応判断の体制

□ インシデント発生時、所管省庁等に報告するためのタイミングや基準が明確にされているか。

例)インシデント発生時、サービスに影響がなくとも、どのタイミングで、どの基準(検知数、攻撃力、影響等)で重大な事象と判断して所管省庁に報告するか確認。

□ インシデント対応に関する、社内関係部門及び社外との連携体制や対応フローが整備されているか。

例)インシデント対応に関して、セプター、JPCERT/CC、IPA、(所管省庁を通じた)NISC等外部との連携体制や対応フローがあるか確認。

例)インシデント対応に関して、CSIRT、情報システム部門、Web関係部門、現業部門等、自部門以外の社内部署が社外と直接情報共有する際に、自部門がどのように関わるか、中継するか確認。

③ 対応実施のための情報共有方法

□ メールやWebサイト等、ネットワークが利用できない場合、社内外の代替連絡手段の確保や、複数の連絡手段の併用がなされているか。

例)ネットワークが利用できない場合の社内への連絡手段(FAX、館内放送等)が定められているか確認。

例)インターネットが利用できない場合の、顧客への連絡手段(電話、郵送等)が定められているか確認。

例)伝達内容に応じてメールの送受信を電話確認することが意識されているか確認。

セキュリティインシデント対応のためのチェックリスト③

1 情報セキュリティインシデントに関する情報共有体制

(3)所管省庁/マスコミ/顧客/他事業者等との情報共有

① 情報共有全般

□ インシデント発生時、外部機関との連携が迅速にとれる体制・手順が定められているか。

例)インシデント発生時、社内での検討・対応で多忙となる中で、外部への情報発信体制・手順が定められているか確認。

例)インシデント発生時、社内での検討・対応で多忙となる中で、所管省庁等への報告・連絡等が迅速にとれる体制・手順が定められているか確認。

□ 大規模なインシデントに関する情報について、他の重要インフラ事業者の情報を有効に活用できるか。

例)大規模なインシデントに関する情報について、JPCERT/CC・IPA等に加え、他の重要インフラ事業者がWebサイト等で開示する情報を入手する手順があるか確認。

例)大規模なインシデントに関する情報について、他の重要インフラ事業者の情報を入手するチャネルを持っているか確認。

□ 大規模なインシデントに関する情報について、分析された情報を有効に活用できるか。

例)大規模なインシデントに関する情報について、NISCやJPCERT/CC・IPA等から提供される統合・分析された情報を有効に活用できるか確認。

□ 担当者が不在の場合でも社内外の情報共有が円滑に進むための体制が組まれているか。

例)外部との情報共有窓口担当者について、不在時の代理担当者が定められているか確認。

例)提供された情報について、複数の担当者が共有できるか確認。

例)提供された情報について、休日・夜間でも共有できるか確認。

セキュリティインシデント対応のためのチェックリスト④

1 情報セキュリティインシデントに関する情報共有体制

(3)所管省庁/マスコミ/顧客/他事業者等との情報共有(続)

② マスコミ/顧客への情報開示体制

□ インシデント発生時、外部への情報開示やタイミングの判断等は定められているか。
例)インシデント発生時、外部へ情報開示するか否か、実施する場合のタイミングの判断等は定められているか確認。

□ 外部への情報開示手段が限定される場合、顧客や社会一般に情報開示を行う手段を準備しているか。
例)HP等、外部への情報開示手段が利用できない、利用が限定される場合、顧客や社会一般への情報開示手段(マスコミへの情報提供、電話、放送等)が定められているか確認。

□ 適時、適切に外部に情報発信するための準備等がなされているか。
例)外部に情報発信するためのフォーマットの準備がなされているか確認。
例)外部に情報発信するための内容確認体制が構築されているか確認。
例)インシデント発生時、外部への情報発信が想定される場合、事前に社内確認・調整等を行う体制が定められているか確認。

□ 行動主体と内容を明確にし、適切に情報開示ができるか。
例)顧客の財産や情報を守るために誰が何をすべきか、誰が何をしているのか等を明確にした情報発信を行う体制が定められているか確認。

③ 他事業者(他分野及び分野内)との連携や情報共有

□ 大規模なインシデントに関する情報について、他事業者や同業他社と情報を共有することができるか。
例)インシデントに関する情報について、情報共有が必要な他の事業者の窓口や情報共有手段が定められているか確認。
例)インシデントに関する情報について、同業他社と情報共有するための窓口や情報共有手段が定められているか確認。
例)インシデントに関する情報について、セプターと情報共有するための情報共有の基準や手順が定められているか確認。

セキュリティインシデント対応のためのチェックリスト⑤

2 情報セキュリティインシデントへの対応の検証

(1)予兆への対応

① リスク抑制対応

□ 予兆への社内の対応体制や対応ルールは定められているか。

例)標的型メールと判断した際の対応体制・ルール、対応手順が定められているか確認。

例)標的型メールに関する情報(メール件名、IPアドレス、ハッシュ値等)を入手した際の、対応体制・ルール、対応手順が定められているか確認。

(2)発生時の対応

① 発生時の対応全般

□ インシデント発生時、セキュリティ専門機関との協力が可能な体制が構築されているか。

例)インシデント発生時、JPCERT/CC・IPAの相談窓口が定められているか確認。

□ インシデント発生時、代替機器や対応人材が確保されているか。

例)大規模なマルウェア感染等のインシデント発生時、代替機器(パソコン等)が確保されているか確認。

例)大規模なマルウェア感染等のインシデント発生時、対応するための人材が確保されているか確認。

□ インシデント対応の人材が育成されているか。

例)インシデント対応が属人的にならず、対応可能な人材が育成される仕組みとなっているか確認。

② BCP等を踏まえた初動対応

□ インシデント対応手順の策定や、体制の整備がなされているか。

例)標的型メールによる情報流出、社内アカウント・PWの漏えい等、インシデント発生時の対応手順や、対応体制が整備されているか確認。

□ 被害想定の困難さや影響範囲が不明な中での対応できる体制が構築されているか。

例)HP改ざんや情報漏えい等、初期段階で被害や影響範囲の予測が難しい中、適切な被害想定と対策が検討できる体制が構築されているか確認。

例)徐々に判明するインシデントに関する情報を収集し、想定される被害や影響に応じた対策が検討できる体制が構築されているか確認。

セキュリティインシデント対応のためのチェックリスト⑥

2 情報セキュリティインシデントへの対応の検証

(2)発生時の対応(続)

② BCP等を踏まえた初動対応

□ インシデント発生時、その影響を想定して事前に準備する体制が構築されているか。

例)インシデント発生時、自社グループが抱える他事業への攻撃可能性も踏まえて、注意喚起や事前の対策が可能な体制が構築されているか確認。

例)インシデント発生時、システムで実施した対応が業務に与える影響を想定し、事前に準備する体制が構築されているか確認。

③ 技術的な判断および対処

□ 分野横断的・複合的な事象への対応が定められているか。

例)分野横断的・複合的な事象への対応を想定し、システムやサービスへの影響を踏まえ、必要な体制、ルール、手順等が定められているか確認。

□ イントラへの大規模なインシデントへの対応が定められているか。

例)イントラへの大規模なインシデントを想定し、システムやサービスへの影響を踏まえ、体制、ルール、手順等が定められているか確認。

□ 制御システムへのインシデントへの対応が定められているか。

例)制御システムへのインシデントを想定し、システムやサービスへの影響を踏まえ、体制、ルール、手順等が定められているか確認。

セキュリティインシデント対応のためのチェックリスト⑦

3 BCP等の発動・解除方法の検証

(1)発動・解除の条件および体制

□ BCPに情報セキュリティの観点が含められているか。
例)インシデント発生時のサービスへの影響を踏まえたBCPになっているか確認。

□ BCPを踏まえて、インシデント発生時のシステム復旧順位について定められているか。
例)インシデント発生時のサービスへの影響を想定し、BCPで定められるサービスの維持・復旧順位を踏まえ、システム復旧順位が定められているか確認。

□ BCPを踏まえて、インシデント発生時にサービスを継続するかの判断ができるか。また、対応体制が定められているか。
例)インシデント発生時のサービスへの影響を想定し、BCPで定められるサービスの継続判断ができるか確認。また、継続・復旧のための体制が定められているか確認。