2016年4月

サイバー攻撃に対する重要インフラ分野横断的演習の成果と企業における活用

データ処理にかかわる機器、利用技術、およびネットワークの拡大と進展に伴い、企業等組織体における情報システムと保有するデータの効果的な活用は組織活動のキーファクターになりつつあり、データ等の情報資産をいかに護るのかがまさしく重要になってきている。情報漏えい、データ破壊、情報システムの誤作動や機能障害等をもたらすサイバー攻撃に対する防御と、事態発生時の速やかな対応が求められている。

国内の社会インフラを担う企業等組織体の情報システムが、このようなサイバー攻撃にさらされて障害が生じ、それがまた連鎖的に発生した場合、国民の社会生活、経済活動は深刻な影響を受けるのは言うまでもない。その対応策として、国と企業等組織体が互いにこれらの侵害に対して連携する仕組みを定めている。これは、コンピュータウイルス、DDos攻撃等の不正アクセス等情報セキュリティ侵害を主とした攻撃に関する発生情報・対応情報を、重要インフラにかかわる企業等組織体と、内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity、以下「NISC」という）および各業態の主管官庁の間で緊密に連携、連絡、報告するものである。その仕組みを理解し、確認するための演習をNISCが中心となり、この10年間、継続的に実施している。

筆者は、その演習を支援する委員として参加しており、その経験を踏まえ、本稿ではNISCと重要インフラ事業者がこれまで実施してきた分野横断的演習の内容とその成果、および一般企業等での演習の活用に関して概括する。

なお、本文中の意見に関する部分は筆者の私見であることを、あらかじめお断りしておく。

1. 重要インフラ分野横断的演習について

（1） 目的とこれまでの状況

エネルギー、経済、金融、流通、交通、通信等といった、ライフラインを制御するそれぞれの情報システムに、外部よりさまざまな攻撃がなされ機能障害に陥ると、社会生活、経済活動に大きな影響が生じることは容易に想定される。事態の発生防止、発生時の早期発見と拡大防止、原因追及と被害の復旧、またその後の再発防止策の策定は、近年、情報セキュリティ対策の基本として、各企業で取り組まれていることと思う。

一方、政府の対策としては、NISCにおいて重要インフラ分野横断的演習を2006年度から毎年実施している。2015年度で10回目となるこの演習は、現在では、2014年度に始まった「重要インフラの情報セキュリティに係る第3次行動計画（2015年5月改訂）」[1]が目指す方向性、「分野内外の事業者等やサイバー空間関連事業者との依存関係が強くなる中、重要インフラ全体の防護には、全体の対策水準の底上げや関係主体間の連携の維持・強化が重要」[2]に基づいて実施されている。

分野横断的演習では、当初、複数の事業者に対して影響のある広域停電、通信の途絶等の事態に対して、その状況把握、情報収集、情報連携に関する演習が実施されてきた。近年は情報セキュリティにかかわるインシデントの対応が主なテーマとなり、毎年、演習日時点の情報セキュリティ環境をもとに、仮定の情報セキュリティインシデントが参加者に付与され、自社の対策、規定等に基づく対応と情報連携（伝達、報告、収集、整理等）についての演習が実施されている。事案を想定し、対応を行うことは、「訓練」とも思えるが、これが「演習」と位置付けられているのは、想定した事態への対応を学習することが目的ではなく、その対応が現時点で正当で実効性があるかを確認し、不具合を明らかにする意味合いがあるためである。

なお、対象となる重要インフラ分野は、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、化学、クレジットおよび石油の13分野である。

（2） 2015年度の演習

2015年度の演習は、数ヵ月間の準備を経て、昨年12月7日に開催された。集合会場は東京、大阪に設けられ、この集合会場以外に自社の職場で演習に参加できる方式も用意された。前回までの参加者は、100名～300名程度であったが、昨今の情報セキュリティにかかわるインシデントの発生、および対策の必要性の認識の高まりを背景に、302組織1,168名の参加（うち36組織、315名が自職場での参加）と大幅な増加となった。

演習は、2部構成からなり、第1部は各事業分野においてサービスへの影響が少ないIT障害（標的型攻撃）が発生したことを想定し、分野間・官民間での連携を図ることによる情報共有体制の実効性を検証、第2部ではサービスへ影響が生じるIT障害（DDos攻撃、OS脆弱性、制御システム障害のいずれかの事象）が発生して事業継続が脅かされる事態を想定し、事業継続計画の発動手順やその内容を確認する等、事態への対処を検証した。

大規模な演習であったが、多くの参加者が自社の規定、対応手順書、事業継続計画等に準拠した行動（連絡、検討、システム対応、復旧等）を模擬的に実施し、その正当性の確認、不整合・不具合項目の明確化を行った。演習の最後には東京、大阪間をテレビ電話で接続し、全員による演習の振り返りの意見交換も行われた。また、その翌月には、事後意見交換会として参加者と他の企業等の担当者がグループを組み、情報セキュリティにかかわる状況等について話し合う場も設けられた。参加者によるアンケート調査では、情報連携の仕組みや自社のセキュリティ対策に関して確認と課題抽出ができたとして、多くの回答者から有効な演習であったと評価された。

---

1 「重要インフラの情報セキュリティに係る第3次行動計画（改訂版）」（平成26年5月19日NISC情報セキュリティ政策会議決定。平成27年5月25日NISCサイバーセキュリティ戦略本部改訂）
http://www.nisc.go.jp/active/infra/pdf/infra_rt3_r1.pdf

2 「重要インフラ13分野が一堂に会してIT障害対応のための演習を実施【2015年度分野横断的演習】（報道関係資料）」（NISC 2015年11月30日）
http://www.nisc.go.jp/active/infra/pdf/bunya_enshu2015.pdf

2. 重要インフラ分野横断的演習で何が得られたか、何を学ぶのか

過去10回に渡る重要インフラ分野横断的演習は、関係者に2つの成果をもたらしてきた。

第1の成果としては、それぞれの演習で付与された事態発生時の情報連携の重要性の認識と、その連携方法、連携先の確認が官・民双方で行えたことである。平時は文書で整理されている連携方法、連携先について、実際にその手順で情報連絡を行うことで、不具合を発見し修正することができた。

参加した事業者側では、自社における情報セキュリティ対策と事態発生時の対応計画（IT-BCPとして整理している事業者も多い）を見直す範囲がわかり、視点の整理ができたといえる。毎年、異なるIT障害、情報セキュリティ侵害の事象の演習が実施されてきたが、これまでのすべての事象に適合する対応計画を準備している事業体は多くはなく、演習がそれを確認する良い機会ともなっている。特に以前に定めた対応計画は、その後の規定類の改訂、組織や情報システム自体の変更等の観点からは見直しが行われていないことがある。これらの事業体にとって、分野横断的演習への参加で得られた知見は大いに参考になるものと考えられる。

第2の成果としては、年度を単位として実施される演習に参加することで、情報セキュリティにかかわる各関係組織、関係者とのつながりができることである。演習日は、毎年12月のある1日が充てられるが、そのための準備、全体検討会、それぞれの企業に対するヒアリングやレビュー等、多くの参加機会があり、社外の関係者との意見交換、情報交換が行われる。その結果、関係者間の面識ができ、その後のコンタクトや情報交換にもつながることとなる。情報セキュリティ対策では、広い領域での最新の状況把握、あるいは相談先等、幅広い範囲の知識、多くの関係者との面識が必要である。この演習により、同業者も含め広く他社・他者とのパイプができることは、自社のなかだけでは得られない大きな成果であるといえる。

3. 各組織における情報セキュリティインシデント対応演習の実施のすすめ

分野横断的演習は、前述の13業種の重要インフラ組織を対象にしたものであり、また主たる目的が官民間を中心とした連携の確認である。しかしこの演習に参加していない一般企業・組織体においても、自組織の情報システムの健全な稼働は経営の最重要事項であり、またコンピュータウイルス、標的型メール等によって情報セキュリティが脅威にさらされている状況は同様である。各企業・組織体では、情報システムの障害対策や情報セキュリティ侵害への対応策は備えていても、その内容を十分に検証できていない場合もある。策定当初は適切な内容であったものが、その後の情報システムの変化、社内外の規定・基準の改訂、そして組織変更等、関係要素が変化するなかで陳腐化していることも考えられる。また策定後、確認済みの対策・手順等の内容を関係者が忘れていないとも限らない。

予測がつかない情報セキュリティ侵害に対し、発生した場合に、策定済みの対策を実効性あるものとするためには、対策のレビューとそれに基づく演習が重要であり、NISCの重要インフラの分野横断的演習で実施している事項は、大いに参考となる。それらを活用して、関係会社を含め自社での情報セキュリティ侵害への対応演習を実施することは有効といえる。

演習には、あらかじめ、侵害発生の確率が高く、かつ事態発生時の対応によって被害が甚大となるケースをシナリオとして用意し、演習全体を整理するコントローラがそのシナリオを順次提示し、関係者が対応を行う形式で実施する。その際、関係者が一堂に会して実施する場合と、自席についたまま社内ネットワークを使用して実施する方式、あるいはそれを併せたやり方等がある。自社ビジネスにかかわる子会社、委託先業者等の関係会社を巻き込んで実施することも効果的である。さらに重要なことは、経営トップやCIOなどが参加することである。情報セキュリティ対策の内容、体制、今後の展開への理解等から、全社的立場で取り組む確認にもなる。またこのような演習は、毎年定期的に実施することが重要である。ちょうど、今は4月。年度計画の詳細を検討する際に、情報セキュリティ侵害の演習を計画に加えられてはいかがであろうか？

KPMGコンサルティング株式会社
顧問　喜入 博

KPMGコンサルティング株式会社

東京本社
〒100-0004
東京都千代田区大手町1丁目9番5号
大手町フィナンシャルシティ ノースタワー
TEL ： 03-3548-5305
FAX ： 03-3548-5306

大阪事務所
〒541-0048
大阪市中央区瓦町3丁目6番5号　銀泉備後町ビル
TEL ： 06-7731-2200

名古屋事務所
〒450-6426
名古屋市中村区名駅三丁目28番12号　大名古屋ビルヂング
TEL ： 052-571-5485

kpmg.com/jp/kc