事業継続に向けた
サイバー攻撃への対策の研究

アブストラクト

1. サイバー攻撃による脅威の増加

情報セキュリティを取り巻く環境は近年急速に変化している。要因としては、以下の通りである。

(1) インターネットの普及により世界中どこからでもアクセス可能となった。

(2) 機密文書の電子化推進により、情報流出・改ざんのリスクが増大した。

(3) 個人情報保護法や JSOX 法等で、情報セキュリティが経営課題と認識されるようになった。

これらの変化により以前のファイアウォールやアンチウイルスソフトで万全であった状況が、攻撃手口が巧妙となったことにより新しい技術を用いた対策を施す必要性が生じている。

さらに、侵入の手口が巧妙化・進化しており正規のサイトを見ただけでウイルスに感染するよう誘導されることもありユーザは感染に気付かない状況である。

セキュリティ対策に「100%の安全」はない。サイバー攻撃に対しては侵入を前提とした対策を講じる必要がある。

2015 年 5 月に発生した日本年金機構の情報流出事故でわかったように、ひとたび情報セキュリティインシデントが起こると、企業の事業継続を脅かすこととなるので各企業はサイバー攻撃においても災害時における事業継続計画（BCP）と同じレベルで対応手順をまとめる必要があると考えた。

2. サイバー攻撃による事業への脅威

ひとたび情報セキュリティインシデントが発生すると、企業の事業継続を脅かす問題に発展する。それは標的型攻撃による情報流出に限らず、DDoS 攻撃などによる従来からある攻撃であっても、ビジネスの中断や社内システム停止に追いやられる。

サイバー攻撃による事業への影響としては、以下の表 2-1 で示すものが考えられる。

表 2-1　サイバー攻撃による事業への影響

[企業]	[社員]
・機器等の破壊による直接的被害	・事故対応による膨大な作業
・多額な損害賠償や訴訟のリスク	・社員個人に対する懲罰
・マスコミ報道等による社会的信用の失墜	
・企業ブランドイメージが大きく低下し、顧客離れによる売上減や取引停止等の発生	

自然災害などの広域災害とは違い情報セキュリティインシデントは１社だけで損害が発生し、相対的にダメージが大きい。そのため情報セキュリティは重要な経営課題のひとつとなっている。

3. 研究成果

本分科会では、分科会メンバー各社のセキュリティ対策の実態について事業継続性の観点を調査した。実施した調査内容は以下の通りである。

表 3-1　実態調査した内容

A. 実態調査	B.事業継続性観点での調査
(1)サイバー攻撃の分析	(1)法律的な側面から必要とされている措置
(2)各社の守るべき情報資産の調査	(2)個人情報保護に関する監督省庁のガイドライン
(3)守らなければいけない業務の調査	(3)サイバー攻撃に対するインパクト分析
(4)各社のセキュリティ対策	(4)サイバー攻撃による情報漏えい発生時の対応フロー
(5)各社のセキュリティインシデント発生時の体制	(5)対応と復旧に関わるICT技術の洗い出し

分科会参加メンバー各社のセキュリティ対策状況を確認したところ、十分なセキュリティ対策は行われている状況であったが、侵入を前提とするサイバー攻撃の準備が行われている企業はほとんどなかった。

企業の事業継続を脅かすサイバー攻撃への対策として以下の課題があがった。

［課題］

・CSIRT で対応すべきことは明確になっているものの、実際に何をして良いかわからない

・サイバー攻撃は防ぎきれないことを前提とした対策を講じる必要がある

4. 情報セキュリティ非常時対応計画策定について（ガイドラインと支援ツールの作成）

地震とサイバー攻撃では、被害内容から対応まで全ての観点で想定が違いサイバー攻撃についての事業継続計画は、地震とは別枠としてまとめる必要がある。また、従来のセキュリティ対応（堅牢性、対応力）に加え、事業継続性の観点で、サイバー攻撃においても地震 BCP と同様に復元性を考慮した準備が必要である。この「復元性」を実現するための対応計画を効果的に策定できるように、情報システム部門向けの「情報セキュリティ非常時対応計画策定ガイドライン」と「情報セキュリティ非常時対応計画策定支援ツール」を作成した。

作成したガイドラインと支援ツールの内容は、以下の表 4-1 に示す通りである。

表 4-1　作成したガイドラインと支援ツールの内容

ガイドラインの内容	支援ツールの内容
(1)非常時体制役割分担	(1)情報セキュリティ非常時対応計画チェックリスト
(2)非常時対応への判定基準	(2)情報セキュリティインシデント対応ログ一覧
(3)非常時参集要員	(3)情報セキュリティインシデント発生時の対応ポイント
(4)非常時対応の全体フローと対応手順	(4)インシデント共有シート
(5)非常時装備品一覧	(5)情報セキュリティインシデント訓練シナリオ
(6)代替手段による運用計画	

また、作成したガイドラインと支援ツールの例は、以下の図 4-2 に示す通りである。

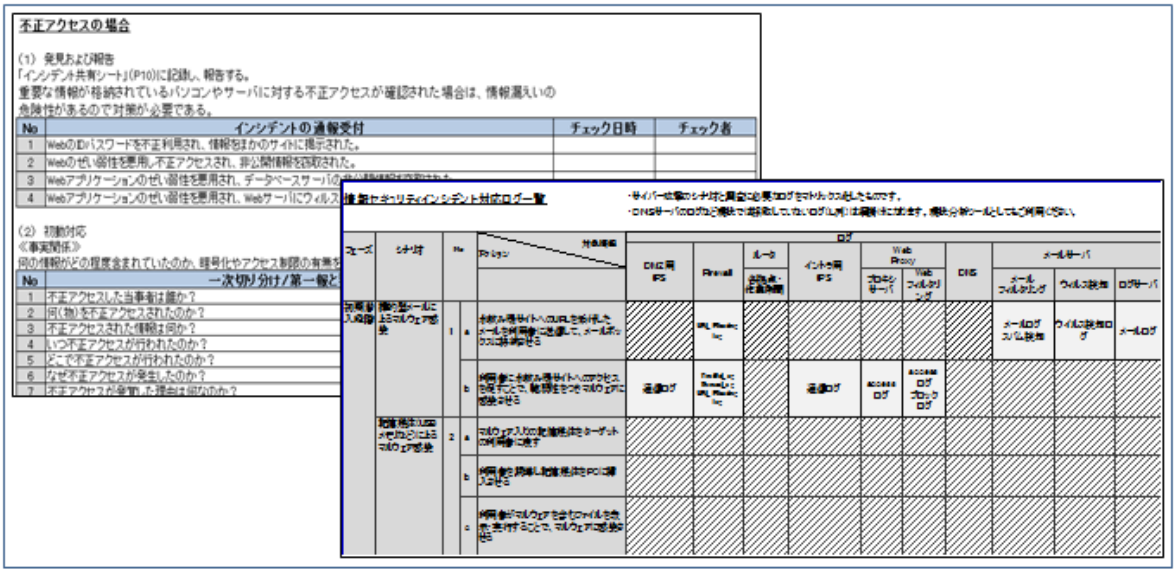

図 4-2　作成したガイドラインと支援ツールの例

5. サイバー攻撃に十分な準備を！

ひとたびサイバー攻撃による情報漏えいがおこると、事業継続が脅かされる。大規模災害と同じレベルでの BCP 対応手順や体制を整えることが重要である。

2020 年に東京五輪が開催されることから、サイバー攻撃がさらに増加傾向となることが予想され、早急な対応が求められている。本分科会で作成したガイドライン、支援ツールを利用して、各社でサイバー攻撃に対する BCP 対応手順や体制を準備することをお勧めしたい。