

平成 24 年 3 月 21 日  
重要インフラ専門委員会

最近の環境変化への対応についての  
重要インフラ第 2 次行動計画への反映について（報告）

1 概要

重要インフラの情報セキュリティ対策については、平成 21 年（2009 年）2 月、第 2 次情報セキュリティ基本計画の策定と同時に「重要インフラの情報セキュリティ対策に係る第 2 次行動計画」（以下、「第 2 次行動計画」という。）が策定されており、策定当初には、3 年で見直すこととされていた。

一方、基本計画については、平成 22 年 5 月に「国民を守る情報セキュリティ戦略」（以下、「戦略」という。）が策定されたが、重要インフラの情報セキュリティ対策については、環境変化に対応するような特段の問題はなかったことから、戦略においても第 2 次行動計画に基づいて実施することとなった。

しかしながら、戦略策定後、①東日本大震災発生時における複数の IT システムの同時的な障害発生及びその際の事業継続計画（BCP：Business Continuity Plan）の実施、②政府関係機関や重要インフラ事業者を含む我が国の主要企業の IT システム（制御システムを含む）に対するサイバー攻撃等、いくつかの環境変化が生じていることから、現在までの第 2 次行動計画の施策の実施状況を点検し、早急に取組を強化・補強すべき点について第 2 次行動計画に反映を行うこととする。また、第 2 次行動計画の期間を戦略の実施期間に合わせて平成 25 年度まで延長することとする。

## 2 検討の経緯

平成24年2月9日に第27回重要インフラ専門委員会を開催し、第2次行動計画にもとづき取り組むこととされている情報セキュリティ対策についての施策の推進状況を点検するとともに、第2次行動計画強化・補強すべき点について議論を行い、以下の項目のとおり整理することとした。

- (1) 情報セキュリティ政策会議において、早急に第2次行動計画に反映する（すなわち、今年度に対応する）ことが必要な部分として例示した次の3項目について、具体的にどのような強化・補強を行うことが必要か。

(政策会議において強化・補強が必要であると例示した項目)

① B C P等の充実

東日本大震災における教訓を踏まえた、安全基準等の策定に当たっての指針（特にB C P）の一層の充実

② 環境変化を踏まえた安全基準の改善

標的型攻撃など最近の環境変化を踏まえて、制御システム等についての安全基準の検証を行い、必要に応じて第2次行動計画、指針等を改定

③ 情報共有体制の強化

平素からの情報収集・情報共有体制の充実

- (2) 上述(1)①～③に掲げる項目に関して、①ほど早急な対応は必要としないが、行動計画強化・補強することが必要な点として何があるのか。

- (3) (1)、(2)以外の事項について中長期的に検討が求められる点として何があるのか。

専門委員から出された意見をもとに、平成24年3月21日に第28回専門委員会を開催し、第2次行動計画改訂案をとりまとめた。また、その実施に際して注意すべき事項（例：『重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針』（以下、「指針」という。）等への反映）についてもとりまとめた。

なお、中長期的な検討が求められるとされた事項については、引き続き検討を行い、次期行動計画策定時にその結果を反映することとする。

### 3 検討の結果

前述2における(1)～(3)についての専門委員会における意見及びその対応(案)は以下のとおりである。

(1) 情報セキュリティ政策会議において、早急に行動計画に反映する(すなわち、今年度に対応する)ことが必要な部分として例示した次の3項目について、具体的にどのような強化・補強を行うことが必要か。

#### ① 事業継続計画(BCP)等の充実

東日本大震災における教訓を踏まえた、安全基準等の策定に当たっての指針(特にBCP)の一層の充実

(意見)

東日本大震災発生時にITシステムにおいて発生した障害とその対応を鑑み、特にITシステムに関するBCPを作成あるいは見直し、複合的に障害が発生した場合においても、事業継続計画を適切に実行できることが求められる。その際、中央防災会議における検討動向等と整合性をとって進めることが望ましい。

(対応(案))

行動計画 II 1.(1) 指針の継続的改善 において、BCPに関する記述を修正・追加(第4章を参照)。

なお、「指針」及び「指針 対策編」の見直しの際には、現在実施中の「東日本大震災における重要インフラに係る対応状況等の調査」の結果、分野横断的演習における気づき等を踏まえ、通信途絶時の対策等IT-BCPに関する項目を追記することとする。

#### ② 環境変化を踏まえた安全基準の改善

標的型攻撃など最近の環境変化を踏まえて、制御システム等についての安全基準の検証を行い、必要に応じて行動計画、指針等を改定

(意見)

情報システム自体の変化に対応して整合性を確保しつつ、可用性などの安全基準を見直していくことが望ましい。

(対応(案))

行動計画 II 1.(2) 安全基準等の継続的改善 において、対策が求められる例として「標的型攻撃」、「制御システムへの攻撃」を追加(第4章を参照)。

安全基準等の浸透状況を調査する際、攻撃の動向、情報システムの変化等、環境変化への対応状況を精査し、必要に応じて「指針」または「対策編」に必要な項目を追加するとともに、国際標準に準拠した評価認証機関の活用またはセキュリティ検証施設の活用等制御システムのセキュリティ評価・検証を容易にするための方策を追加することとする。

### ③ 情報共有体制の強化

平素からの情報収集・情報共有体制の充実

(意見)

情報共有に関して、全てを共有することが難しい。米国でも情報共有の重要性は理解されているが、重要インフラ業界との間の情報共有の仕組みを機能させるのに大変な苦勞をしているようだ。このため、情報共有を具体的に進めるための施策を行動計画にも盛り込むことが望ましい。

(対応(案))

行動計画 II 2.(4)セプターカウンシル において、重要インフラ事業者等と政府機関等の密接な意見交換や事業者にも役立つ情報の共有等、取組みを具体的に追加(第4章を参照)。

セプターカウンシルにおいては、システムの運用状況の客観的判断材料等事業者間で共有可能な情報の追加等を具体的に検討

(2) 上述(1)①~③に掲げる項目に関して、①ほど早急な対応は必要としないが、行動計画上強化・補強することが必要な点として何があるのか。

(意見)

民間同士あるいは官民における情報共有を進めるため、企業秘密を確保しつつ、必要な者との間で共有を行うために求められる要件の緩和条件やその仕組みについての検討を進めることが求められる。

(対応(案))

現行の情報共有の枠組みによる情報共有を進めるとともに、現行を超える情報共有の在り方については、その必要性を含めて中長期的な課題として検討することとする。

- (3) (1)、(2) 以外の事項について中長期的に検討が求められる点として何があるのか。

(意見)

企業はシステム監査について内部で体制を整備することが必要であり、人員の確保、育成及び活用について十分な配慮を行うとともに、システム調達から廃棄までの全体のライフサイクルの中で、システムやデータについての情報セキュリティについて考えてほしい。

ネットワークを含めたシステムの高度化・複雑化が進展し、各階層（レイヤ）の運用者が異なる等により、セキュリティ対策が講じられない部分が生じることが想定される。このような部分における課題と対応に必要な対策を検討すべき。

現在の情報セキュリティ対策は、重要インフラにおけるIT障害が国民生活や社会経済活動に重大な影響を及ぼさないよう重要インフラを防護するとともに、重要インフラ事業者等のサービスの維持及びIT障害発生時の迅速な復旧等の確保を図る観点から講じられているが、防護対策を意図的に破られた場合にどのような対応を行う必要があるかについては更なる検討の余地がある。

(対応（案）)

人材の育成については、別途人材育成・普及啓発専門委員会において議論されている内容を踏まえて、重要インフラを対象とした方策について中長期的な課題として検討することとする。

ライフサイクルを踏まえたセキュリティの確保については、ライフサイクル全体を考えた際に現行のセキュリティ対策に追加することが望ましい事項について中長期的な課題として検討することとする。

システムの高度化・複雑化に伴い求められる、特に階層と階層の間でのセキュリティ対策については、技術面での環境変化への対応に関して中長期的な課題として検討することとする。

防護のための対策が破られた場合に求められる情報セキュリティ対策については、システム運用面で求められる対策に関して中長期的な課題として検討することとする。

## 4 行動計画 改訂（案）

3（1）における改訂（案）及び行動計画期間の延長を盛り込んだ改訂（案）は次のとおりである。（下線が追加・修正を行った部分、取り消し線は削除を行った部分。）

### I 総論

#### 5. 行動計画の改訂

第2次行動計画策定後、平成22年5月に「国民を守る情報セキュリティ戦略」（以下、「戦略」という。）が策定されたが、重要インフラの情報セキュリティ対策については、環境変化に対応するような特段の問題はなかったことから、戦略においても第2次行動計画に基づいて実施することとなった。

しかしながら、戦略策定後、①東日本大震災発生時における複数のITシステムの同時的な障害発生及びその際の事業継続計画（BCP：Business Continuity Plan）の実施、②政府関係機関や重要インフラ事業者を含む我が国の主要企業のITシステム（制御システムを含む）に対するサイバー攻撃等、いくつかの環境変化が生じていることから、第2次行動計画の施策の実施状況を点検し、早急に取組を強化・補強すべき点について第2次行動計画に反映を行った。また、行動計画の期間を延長し、次回の見直しを平成25年度に行うこととした。

### II 計画期間内に取り組む情報セキュリティ対策

#### 1. 安全基準等の整備及び浸透

##### （1）指針の継続的改善

社会動向の変化等に対応し、また新たな知見を適時反映していくために、指針の分析・検証を1年毎、及び必要に応じて実施し、その結果を公表することとする。なお、指針の改定に関する検討は原則として3年に1度実施するものとする。ただし、必要に応じて追加的に検討を実施し、必要があると認められた場合には指針の改定を行うこととする。

なお、指針の改定に関する検討にあたっては、東日本大震災において重要インフラ分野に生じた複合的な障害における教訓を踏まえ、事業継続計画において情報セキュリティ上のリスクを十分想定する必要性が生じている状況~~重要インフラ事業者等において事業継続計画の策定が進みつつある状況~~や、事業継続計画に関する国際規格化の進展状況等を踏まえ

つつ、分野横断的な観点からも実効的であるかを検証できるように指針の内容を充実させるものとする。

各重要インフラ事業者等の自主的な取組みに資する項目を充実させるために、指針に記載される事項を「要検討事項」と「参考事項」に分類し、対策項目の具体化の例示を行う事により、引き続き記載事項の充実を図ることとする。

「要検討事項」とは対策の底上げの観点から全分野共通で特段の理由のない限り対策することが望まれる事項であり、安全基準等に規定する必要性を各分野が検討すべき事項とする。また「参考事項」とは進んだ対策として盛り込む事が望ましい事項とし、各分野が任意で参考とする事項とする。

要検討事項及び参考事項は、現行指針の項目に加え、行動計画に基づく各重要インフラ分野及び重要インフラ事業者等の取組みから得られる知見・教訓等を候補として必要に応じて充実させていくこととする。

## (2) 安全基準等の継続的改善

各分野においては、対策の経験から得られた知見を安全基準等に反映するため、安全基準等の継続的な改善に取り組むこととする。なお、安全基準等の検証に際しては、指針や毎年実施される指針の分析・検証の結果を踏まえた検討を行うこととするが、その際標的型攻撃、制御システムへの攻撃への対策等最近の環境変化に対応しているか否かの分析・検証も行い、必要に応じて安全基準等の改訂を行うこととする。

情報セキュリティ対策に関する知見の共有を促進するために、従来検証対象となっている安全基準等の他に、情報セキュリティ対策に関する基準又は参考文書類を、可能な範囲で共用できるよう改めて広く安全基準等として整理することとする。

安全基準等に基づく対策状況については、関係性を有する主体間で互いに把握しておくことができることが重要である。そのため、情報セキュリティ監査又はそれに対する相当するものの実施や、情報セキュリティ報告書又はそれに相当するものの作成等の自主的な取組みを一層推奨し、分野や重要インフラ事業者等における情報セキュリティ対策の対外的な説明に努める。

## 2. 情報共有体制の強化

### (4) セプターカウンスル

セプターカウンスルは、各セプターにより構成される共助・互恵の活動の取組みの場として創設を目指すを促進するために創設されたものであり、相互理解及びベストプラクティス等の具体的な事例共有等の分野横断的な情報共有が行われることが望まれる。

また、政府機関等とは独立した活動が可能な位置付けにあることから、情報共有の改善等のための検討に関し自ら積極的な活動に取り組むことが期待される。特に重要インフラ事業者等と政府機関等の協力関係を今後一層深めていくためには、両者間の状況認識等の共有を進めていくことが重要であることから、重要インフラ事業者等と政府機関等との意見交換を行うなどの平時から重要インフラ事業者等と政府機関等の意見交換を密接に行うことが望まれる。また、事業者間においても相互に役立つ情報の共有を進めるなどの取組みがなされることが望まれる。なお、この取組みを進めるに当たって、セプターカウンスルの事務局を努める内閣官房においては、2(1)カ②に示す環境整備を行うことが重要である。

## IV 評価・検証と見直し

### 1 行動計画の推進体制

#### (6) 行動計画の見直し

第2次行動計画については、対策の成果、施策の成果、補完調査、評価の内容等（以下「評価等」という。）を踏まえ、また、脅威、IT障害、ITを利用したサービス等に関する社会情勢等の変化等をふまえ、3年毎または必要に応じ、見直しを行う。~~第2次行動計画期間中においては、少なくとも策定から2年後から12ヶ月かけて見直すこととする~~再度の見直しについては、平成25年度に行うものとする。

特に見直しの要点となるのは、目標とそれに基づく基本的な方向性、重要インフラ事業者等の対象範囲、関係主体とすべき主体の対象範囲、対策や施策の追加や廃止、想定すべき脅威の例示、対象とすべき重要インフラサービスの範囲、サービスレベル、検証レベル、評価指標の設定等である。またこれに併せて、各用語の定義や行動計画の対象範囲についても、必要に応じて見直しを行うものとする。

第2次行動計画の見直しに際しては、各分野の特性や取組状況に配慮しつつ、事業者の取組みが自主性に基づくものであることを踏まえた検



討を行うことが必要である。また、第2次行動計画が想定し得なかった事象が発生した場合はこれに対応できるようにすることが重要である。

行動計画の見直しは重要インフラ専門委員会において行うこととし、委員会の合意を経て、情報セキュリティ政策会議で新たな行動計画を決定するものとする。