参考資料2

NISC National Information Security Center

重要インフラにおける「指針・対策編」改定案に対するご意見について

2013年1月31日

内閣官房 情報セキュリティセンター（NISC）

指針・対策編の改定案に対するご意見について

○第29回重要インフラ専門委員会（H24.9.27）で提示した指針・対策編の改定案に対する意見照会において、専門委員、所管省庁から以下のご意見をいただき、事務局としては以下の通り対応したいと考えている。

意見照会結果	事務局案
（1）インシデント対応人材の育成策	
＜意見＞ ・標的型攻撃は検知が難しく、初期段階ではシステム障害なのか攻撃なのか判別が困難であり、システム運用者の検知力を上げるべきである。システム運用者、とりわけインシデント対応人材の教育・育成が必要である。システム運用の現場で適切に初動がとれるようにすることが重要である。	○標的型攻撃に対しては、被害を最小限に抑える観点より、検知力・初動対応力の向上が重要であることから、「ア　組織・体制及び資源の対策」に盛り込むこととしたい。 ＜文案＞：対策編 ア　組織・体制及び資源の対策 （イ）情報セキュリティ人材の育成等【参考事項】 ・インシデント発生時に対応ができる人材の計画的な育成
（2）WAF	
＜意見＞ ・WAF（ウェブアプリケーションファイアウォール）の導入は費用負担が大きいと思われ、小規模な情報システムや機密性の低い情報を扱う情報システムの場合、導入は非現実的な場合もあるのではないか。 ・WAFだけで完璧に防御できるわけではなく、多層防御が重要。対策例としては記載すべき。	○対策編に記載の個別対策については、「各重要インフラ分野においては、自らの特性を踏まえ、対策項目の追加・選択・修正等を適宜行」うものであるので、現行案通りとしたい。

指針（本編・対策編）改定案に対するご意見について

意見照会結果	事務局案

（3）共用IDの禁止

＜意見＞
・共用IDを全て禁止すると、さまざまな形態の情報システムがあることから運用上厳しい場合もあるのではないか。

○対策編に記載の個別対策については、「各重要インフラ分野においては、自らの特性を踏まえ、対策項目の追加・選択・修正等を適宜行」うものであり、共用IDのリスク（だれが操作したのか判別できない）を考えれば、対策としては重要なものであると認識するので、追加する方向としたい。（現行案通り）
但し、表現を以下に変更したい。

＜文案＞：対策編
ウ　情報セキュリティ要件の明確化に基づく対策
ア） 情報セキュリティ確保のために求められる機能 【要検討事項】
○主体認証
・利用者IDの管理（個人単位のID付与、不要IDの削除等）

（4）ウェブサーバからの攻撃の端緒となる情報の送信を防ぐ対策

＜意見＞
・「ウェブサーバからの攻撃の端緒となる情報の送信を防ぐ対策」は具体的にはどのような対策なのか。（読者にとって少し意味が分かりにくいと思う。）

○ わかりやすいように、以下の文言に変更したい。

＜文案＞：対策編
エ　情報システムについての対策
（ウ） アプリケーションソフトウェア 【要検討事項】
○導入時
・攻撃に利用されるウェブサーバ情報の送信を防ぐ対策

指針（本編・対策編）改定案に対するご意見について

意見照会結果	事務局案

（5）ネットワーク構成等に関する情報の秘匿

＜意見＞
・情報システムの運用では組織間で相互にBCP(Best Current Practice)を情報交換して、より良い構成へと見直していく運用が望ましいと考える。(攻撃者に対する)秘匿を実現しつつ、適切な情報共有が行えるような指針が望ましい。

○「情報共有」については、進んでいる分野もあればそうでない分野もある。また、事業者だけでできる対策ではないので、対策編には記載しない方向で考えたい。

（6）首都直下地震等に備えた対策

＜意見＞
・重要業務の継続に必要となるデータについては、特に首都直下地震等に備えた対策が不可欠であり、同時被災をしない遠隔地でデータを保管するなど、重要度に応じた対策の徹底を行うことが必要である。
・データの重要度によっては、災害発生時に早期に復旧させるべきデータもあり、この場合は、遠隔地へ媒体保管をするようなバックアップではなく、オンラインによるバックアップが望まれる。

○ご指摘通り、以下の文言を追加したい。

＜文案＞：指針
ア　IT障害の観点から見た事業継続性確保のための対策
（ア）　事業継続性確保のための個別対策の実施　【要検討事項】
・・・その際、東日本大震災に見られた広域災害・複合障害や新型インフルエンザ等、社会全体で対応が望まれる脅威についても考慮されるべきである。
あわせて、事業継続に必要なデータが東京に一極集中している状況を踏まえ、首都直下地震についても考慮されるべきである。

＜文案＞：対策編
ア　IT障害の観点から見た事業継続性確保のための対策
（ア）　事業継続性確保のための個別対策の実施　【要検討事項】
○拡大防止・早期復旧のための措置
・情報の格付けに応じたデータバックアップ（オンライン、媒体保管等 ）、遠隔地への保管
（「・データバックアップ、遠隔地への保管」は削除）

指針（本編・対策編）改定案に対するご意見について

意見照会結果	事務局案

（7）通信回線の冗長化

＜意見＞
・今回の震災は、広域かつ大規模な災害であり、その教訓を受けて追加した対策をとるのは、すべてのシステムではなく、業務継続に不可欠な重要なシステムにのみ適用されることを明示したほうがよいのではないか。すべてのシステムに適用されるわけではないと思う。
・「同時被災しないような通信回線の冗長化」などとしないと、同じルートで多重化するだけでは、東日本大震災の教訓を反映していないのではないか。

○「同時被災しないような」ということを具体的に示すことは不可能であるので、現行案（「通信回線の冗長化」）通りとしたい。
但し、以下の文言を追加したい。

＜文案＞：対策編
ア　IT障害の観点から見た事業継続性確保のための対策
（ア）　事業継続性確保のための個別対策の実施　【要検討事項】
○未然防止措置
・通信回線の冗長化（業務継続に必要なシステム等）

（8）代替手段に必要なシステムの準備

＜意見＞
・「・・・代替手段に必要なシステム（在宅勤務管理システム等）の準備」の記載では、在宅勤務システムを準備していれば大丈夫とのミスリードとなりかねない。

○ 具体例を削除し、以下の文言としたい。

＜文案＞：対策編
ア　IT障害の観点から見た事業継続性確保のための対策
（ア）　事業継続性確保のための個別対策の実施　【要検討事項】
○拡大防止・早期復旧のための措置
・バックアップシステムの整備、代替手段及び代替手段に必要なシステムの準備

指針（本編・対策編）改定案に対するご意見について

意見照会結果	事務局案

（9）サプライチェーンにおける情報セキュリティを考慮した機器の調達

＜意見＞
・マイクロソフトの調査では、工場からの出荷時やサプライチェーンでの輸送時などに、PCにマルウェアが混入した可能性が指摘されている。今後は、納品時のシステムおよびシステムの構成要素のセキュリティ検査が重要となると考えられる。上記の脅威に対する対策という点をもう少し分かりやすい表現で記載しても良いと思う。
・具体的な対策は難しいが、留意することを例として記載してはどうか。

○サプライチェーンにおける情報セキュリティの脅威に対する対策が、今後重要となると考えられることから、「エ　情報システムについての対策」に盛り込むこととしたい。

＜文案＞：対策編
エ　情報システムについての対策
（イ）　電子計算機 【要検討事項】
○設置時
・サプライチェーンにおける情報セキュリティを考慮した機器の調達（信頼のできるベンダーから調達する等）

（10）IPv6移行に関する対策

＜意見＞
・IPv4アドレスの在庫は、すでに枯渇している状況にある。今後は「『IPv6移行』に関する継続的な情報収集の実施 」よりももう少し進んで、実装あるいはその検討を促す時期になると考えている。

○「『IPv6移行』に関する継続的な情報収集の実施」に、「実装検討」も盛り込むこととしたい。

＜文案＞：対策編
オ　ITに係る環境変化に伴う脅威のための対策【要検討事項】
・『IPv6移行』に関する継続的な情報収集と実装検討の実施

指針（本編・対策編）改定案に対するご意見について

意見照会結果	事務局案
（11）その他	
＜意見＞ ①セキュリティ対策では、リスクの評価がなかなか難しく定性的な説明にとどまり、投資判断に困っている企業が多いのではないか。 リスク評価と施策の優先順位の決定方法論などの記載が必要ではないか。 ②現在、実務で策定運用しているガイドラインと内容の構成が大きく異なり、業務要件とシステム要件が混在して列挙されており、チェックシートとして使いにくいと思われる。 一般的な情報セキュリティガイドラインの内容構成と異なっているのは、何か理由があるのか。 ③クラウドのサービス品質、セキュリティのレベル、運用体制等は、それぞれの業者に任せた状態であり、また業者から必ずしもこれらの条件を明確に提示されていない状況である。クラウドに移行すれば、経費が安くなる、運用が楽になるということでシステム環境を移行して、事故があって初めてずさんさが分かることもある。クラウド環境を提供する業者に対する安全基準を示す必要があると考える。	①リスク評価の仕方は業種や企業規模によって異なる思われ、分野共通的な事項を記載している指針に、リスク評価の方法を記載するのは適当ではないと考える。 ②各分野の安全基準は指針をもとに作成されており、章立ては似通ったものになっていると思われる。特に、指針の章立てが特別であるとは考えていない。 ③クラウド環境を提供する事業者は、現在重要インフラ事業者には含まれていないので、指針の内容を直接適用することは適当ではないが、重要インフラ事業者がクラウド環境を提供する事業者に外部委託する場合の情報セキュリティ確保のための対策については、今後追加等を検討していく余地があると認識している。

指針（本編・対策編）改定案に対するご意見について

意見照会結果	事務局案
（11）その他（続き） ＜意見＞ ④せっかくの「安全基準等」策定にあたっての指針及び対策編について、各セプターを通じて、重要インフラ事業者に義務づけに近い形で、周知することが必要ではないか。重要インフラ事業者として、義務づけをするなど強制力が必要と考える。	**④指針は、各重要インフラ分野の「安全基準等を策定するにあたっての指針」であるため、指針の内容を事業者へ直接強制することは適当ではないと考える。**