「サイバーセキュリティ 2014(案)」に対する意見

一般社団法人新経済連盟

下記のとおり、９項目意見を提出いたしますので、よろしくお取り計らいください。

(９・10 頁「公開ウェブサーバに対する脆弱性検査の実施」関係)

１．検査対象：検査対象を全府省庁のすべての公開ウェブサーバとすべき。もしくは、別途、検査対象外になる公開ウェブサーバにおける脆弱性を確認する手段を確立すべき。

検査内容：サーバ脆弱性と Web アプリケーション脆弱性の両面での対応をすべき。

対処時間：脆弱性への対処時間は短くするべき。ＯＳ等の脆弱性に関しては、ホストベースの仮想パッチ技術などを用い、脆弱性への即時対応が必要。

（理由）

・原案では、対象が「希望」府省庁の「主要」な公開ウェブサーバとされており、事実上、各府省庁の判断に検査対象がゆだねられており、希望がなければ検査が実施されないことになってしまう。この結果、検査対象外の公開ウェブサーバが残り脆弱性が解消されないおそれがある。

・公開ウェブサーバの場合、外部にさらされた状態にあるため、サーバ脆弱性だけでなく Web アプリケーション脆弱性の対応も必要である。

・脆弱性検査だけでなくその結果を踏まえた対応の早期実施を行わないと意味がない。

(22 頁　「上場企業における事業等のリスクとしての開示の検討」)

２．制度設計の際は事業運営に与える負担や影響を十分に留意し、導入の際に極力混乱がないよう留意いただきたい。また、リスクの公開に際しては、情報セキュリティ対策が確立している企業に対してメリットがあるような仕組みにすべきである。

(理由)

・事業運営に与える負担や影響が増える一方で、実質的なセキュリティ対策につながらないことになっては本末転倒であるため、負担・影響、公開のインセンティブ等について十分留意する必要がある。

(23 頁　「企業の運営するウェブサイトの安全性向上」関係)

３．検出ツールは民間の知見と創意工夫を活用することにも留意いただきたい。また、昨今の web 改ざん事案の多発に言及すると共に、啓発活動についても明記いただきたい。

（理由）

・検出ツールについては、既存のセキュリティ企業において多用なソフトが提供されている。

・web 改ざんについては、ここ数年、我が国において、改ざんされた正規の web サイトを経由したマルウェア感染が広がっているが、必ずしも企業で十分に問題視されていない現状がある。

（26 頁　「ソフトウェア教育との連携」関係）

4．ソフトウェア教育の更なる推進（総合的学習の時間等の活用、官民連携、プログラミング等とあわせた情報関係科目としての導入の検討等）に言及いただきたい。

（理由）

・新経済連盟ではかねてよりプログラミング教育の導入を提言しているが、情報セキュリティの推進のみならず、我が国の経済発展に大きく資すると考えるため。また、プログラミングは論理思考を鍛えることにもつながるため、プログラミングは重要と考える。

（27 頁　「各種メディア等を通じた普及・啓発の推進」関係）

5．スマートフォンにおけるウイルス対策ソフトの利用を促す啓発と、ネットにおけるリテラシーを授業で教えることについて言及すべきである。

（理由）

・スマートフォンは、パソコンと比較して、まだウイルス対策ソフトを導入しなくても良いという意識の人が比較的多い。

・諸外国では、WEB での公共マナーを教えており、ネットでの人とのつきあい方のようなものを授業で行うことは重要である。少なくともパソコンもスマホもウィルス対策ソフトを入れる教育を小学校レベルから徹底し、マスコミを通じてそれらを啓発すべき。

（28 頁　「情報漏えい対策への取組」関係）

6．a）について、「IPA を通じて当該機能を有するツールの利用を促進する」というコンテキストの文章になるよう改正いただきたい。

（理由）

・まずは対策の必要性の訴求が必須である現状がある。

・また、対策手法についてはセキュリティベンダーを含む民間の知見や創意工夫を活

用することがより高い効果を期待できる。

（36 頁「ログの保存の在り方の検討」関係）

7．具体的な導入についてはきわめて慎重な議論が求められるべきである。

（理由）

・事業者に過度の負担を課す可能性があるとともに、自由な情報流通への妨げとなるおそれがあるので、多角的かつ慎重な議論が必要である。

（39 頁「国家レベルのサイバー攻撃への対応の強化」関係）

8．サイバー空間関連事業者など関係機関の役割の整理・明確化を行うにあたっては、自由な情報流通の確保との関連で十分なバランスをとることが前提である旨明確に記述するべきである。

（理由）

・サイバー攻撃対策との名目で国民の自由な情報流通やアクセスへの不当な介入や制限、民間事業者や個人に対する萎縮効果を引き起こすような政策が実施されてはいけない。

（61 頁　「官民の情報共有のさらなる推進」関係）

9．セキュリティ事業者のみならず、事業者の過度な負担とならない範囲で必要に応じてユーザー企業とも連携を行い、我が国全体として安全なサイバー空間を実現できるようにしていただきたい。

（理由）

・過去の取り組みでは官民連携とは基本的に関連企業との連携であるが、大多数を占めるユーザー企業のセキュリティを底上げすることが我が国のセキュリティレベルを上げるために重要である。

以　上