安心・安全で自由なネット社会を目指して(概要)

2003年3月18日
(社)日本経済団体連合会
電子商取引の推進に関するワーキング・グループ

はじめに

(1)活力と魅力溢れる経済社会を実現するためには、企業や個人によるITの利活用を推進することが必要。
(2)特に、個人によるITの利用を促すためには、企業、政府による個人情報の適切な取扱いが不可欠。
(3)企業、個人、政府など各主体は、取引や手続の重要性に応じて適切な情報セキュリティ水準を確保することが責務。
(4)安心・安全なネット社会を脅かす犯罪行為を効果的に抑止するため、必要最小限の法整備が必要。

(1)自立、自助、自己責任の原則に基づく取組みにより「安心・安全」と「自由」を確保。
(2)政府ついては、他の主体に増して厳格な対策が必要。

Ⅰ．個人情報の適切な取扱い

1．個人情報保護法制の整備

(1)個人情報保護法制は、電子商取引や電子政府などITの利活用を促進するための基盤であり、わが国の国際競争力上も速やかに整備することが必要。
(2)個人情報保護法制は、(イ)企業の自己規律に基づく自主的な取組みを基本とし、政府の関与は必要最小限にとどめること。
(ロ)個人情報の保護と利用による便益とのバランスを確保するとともに、事業活動の実態を踏まえること。

2．何をなすべきか

企業
・個人情報保護措置(プライバシーポリシー、コンプライアンスプログラムの策定等)の自主的な実施
・経営トップによる上記措置の定着と継続的な改善

個人
・個人情報の不用意な提供の自制
・企業のプライバシーポリシーの閲覧、オプトアウトなどの活用
・ADRの積極的な活用

政府
・個人情報保護法制の整備
・プライバシーポリシー、コンプライアンスプログラムの策定等(地方公共団体にも要請)
・個人情報保護に資する技術の積極的な採用
・個人情報保護の重要性の周知、啓蒙

Ⅱ．情報セキュリティの確保 ＝民間部門の情報セキュリティ対策＋政府など重要インフラの保護＋サイバー犯罪への対応(Ⅲへ)

1．「セキュリティ文化」の確立

(1) ネット社会においては、「安全」は与えられるものではなく、ネットワーク参加者全員が分担して作り上げていくもの。
(2) 昨年改定されたOECD情報セキュリティガイドラインに盛り込まれた「a culture of security(セキュリティ文化)」の確立が必要。

「注」「セキュリティ文化」とは、「情報システム及びネットワークを開発する際にセキュリティに注目し、また、情報システム及びネットワークを利用し、情報をやりとりするに当たり、新しい思考及び行動の様式を取り入れること」。

2．何をなすべきか

企業(重要な経営課題として、トップが関与)
①情報セキュリティポリシーの策定、PDCAサイクルの継続
②情報セキュリティ担当役員の任命または情報セキュリティ対策委員会の設置
③人間系まで含めた包括的な対策の実施
④安全性の高いIT関連製品・サービスの調達
⑤内部で相互運用可能なセキュリティ関連技術・サービスの実装
⑥情報セキュリティ監査、ISMS適合性評価制度の活用
⑦企業間の情報交換・共有
⑧情報セキュリティに関する知識の蓄積

個人(二次感染源や「踏み台」とならないための対策)
①不正コピーソフトの使用厳禁
②アンチウィルスソフトの最新化
③ファイアーウォールソフトの導入・定期更新
④差出人不明のメールに対する注意
⑤OS、アプリケーションの定期更新

政府(「電子政府＝ネット社会の最重要インフラ」に相応しい対策)
・民間部門の範となる最高水準の情報セキュリティの確保(外部の専門家の活用を含む)
・「地方自治」に委ねることなく、国・地方均一のセキュリティ水準の確保(地方公共団体については、セキュリティ水準の高い複数のシステムの共用利用・共同運用)

10の具体策
①国・地方共通の情報セキュリティポリシーの策定、PDCAサイクル(外部監査を含む)の継続、人間系も含めた包括的な対策の実施
②電子政府における利用暗号の信頼性向上
③安全性の高いITハードウェア、ソフトウェアの調達
④セキュリティ製品・サービスの省庁横断的な調達・運用・保守
⑤電子認証システムの相互運用性の確保
⑥通信サービス停止時の代替措置の技術的有用性、費用対効果の検討
⑦省庁間、国・地方公共団体間、地方公共団体間での情報交換・共有
⑧自らの情報システムに最高水準の情報セキュリティ技術を適用するための研究開発の実施、開発成果の普及
⑨情報セキュリティの重要性に関する国民意識の向上
⑩国民に対するセキュリティ教育の義務教育段階からの実施

Ⅲ．サイバー犯罪への対応

(1) 国際的な連携と制度の調和
サイバー犯罪条約の国内法制化に際して、
・既存の法律との整合性確保、重複排除
・民間企業に過度の負担を課さないような配慮
(サービスプロバイダーの責任の限定、営業秘密の適切な取扱い、個人のプライバシー保護への適切な配慮)
・国内法制化案の早期公表、パブリックコメントの実施　　等

(2)情報資産の刑事的保護
・情報の窃盗等は刑事罰の対象でないと考えられてきたが、事業活動上の重要性に鑑み、情報資産を不正取得、不正使用行為等から刑事的に保護することについて、検討が必要。

Ⅳ．個のエンパワーメント

(1)ネット上における紛争を未然に防止するためには、「自立した賢い個人」の存在が不可欠。
・情報に係るモラル、セキュリティに関する教育の義務教育段階からの実施
・第三者による企業の信頼度の評価(国内外で通用する各種マーク制度)による判断・選択の容易化
(2)簡易で迅速な紛争解決のためには、裁判の迅速化とアクセスの改善に加え、ADR制度の確立が必要。
・人材の質量の拡充、資金・広報面の支援

Ⅴ．政府への提言(上記Ⅰ～Ⅳの記載事項のうち、政府への提言事項を再掲)

・加えて、情報セキュリティの確保に関し、統一的な推進体制の強化を要請。