

「デジタルジャパン」の原案等の策定に関する意見

1. 個人/団体の別: 団体

2. 氏名/団体名: グローバルフレンドシップ株式会社

3. 連絡先: 非公開

4. ご意見:

(1) デジタルジャパンの目標についての設問に関しては、賛同します。

さて、本題となります(2)～これらの分野に限定されるものではありません。に対応し、コメントします。

1、概観

これまで、様々なIT基盤の話がありましたが、どれも米国又はイスラエルに根幹部分を握られている技術・暗号がベースとなっています。

アジアや日本には、「割符」という先人の英知でもある情報の運用管理手法があります。

暗号との比較で言えば、暗号が変換技術であり、逆変換ができれば、即、原本情報に戻ります。一方、割符は、原本情報をビットレベルでばらばらにして、複数の塊に振り分けます。つまり、一つの塊を偶然入手しても全体を復元できません。ちょうど、パズルの1ピースを道で拾ったようなもので、そこだけから全体を作ることはできません。このような技術が、内閣官房情報セキュリティセンター公表の資料でも具体的な利用シーンまで明記されるに至ってます。しかも、暗号したデータでも処理できます。つまり、過去のセキュリティー投資も無駄になりません。

このような基礎技術(秘密分散技術)を、新たな情報基盤構築の際に周辺技術と組み合わせれば、原理的にも非常に安全な情報基盤が構築され、様々な分野での利用・応用が可能です。原理的に安全な仕組みを自ら持つことは、国家としても大きな資産となりますし、将来は、輸出できる新たな産業に成長する可能性もあります。外交員のノートPCに実装すれば、安全な営業活動ができ、営業効率も向上し、無駄な移動回数も減るので、エコにもつながるでしょう。また、多数決のような仕組みで、原本復元も可能です。

例えば、取締役会で3人の取締役中2人しか揃っていないが、定刻を過ぎている場合、二人の分散データの開示で原本を復元できるような割り方も可能です。これを応用すると、原本のコピーを作らなくても、データのバックアップが可能になります。

参考になりましたら、幸いです。

以上