

米国における CUI (Controlled Unclassified Information) の概念

— 「情報の適切な管理」 を考えるための予備的考察 —

氏名 林 紘一郎 Koichiro Hayashi

Keywords : CUI、情報の秘匿と共有、Executive Order 13556、32 CFR 2000、NIST 800-171

1. 目的

サイバー・インシデント対策の本質は、ICT 依存を深めた社会システムを健全に維持管理することにある。それは「情報」の秘匿性 (Confidentiality)・完全性 (Integrity)・可用性 (Availability) を保つことで達成可能との見方もあるが、その代表格である「秘匿性」を維持するための手続きが確立されている訳ではない。特に「時と場所と態様」によって評価が変化する「情報」を、どのように「事前に格付け」(classify)して管理するかは、各国にとって悩みの種である。本稿では、安全保障に敏感で厳格な情報管理を行なっているとされる米国で、CUI (Controlled Unclassified Information) という概念が生まれた背景と、その運用の実態と実効性を検討することを通じて、「情報の適切な管理」を考えるための予備的考察としたい。

2. 方法

米国で 9.11 テロの教訓を踏まえて発出された大統領令 (Executive Order) 13556 は、それまで連邦政府の各機関で、SBU (Sensitive But Unclassified) とか FOUO (For Official Use Only) という名称でアクセスや配布が制限されてきた情報 (100 種類以上あった) を、CUI (Controlled Unclassified Information) という形で統一的に扱う方針を定めたものである。それを受けて国立公文書記録管理局 (National Archives and Records Administration) が政府部門における実施方針を策定し (2015 年 12 月 32 CFR 2000)、国立標準技術研究所 (National Institute of Standard and Technology) が非政府部門への展開指針を定めている (2015 年 6 月 NIST 800-171)。これら进行分析することで、以下の諸点を解明することとした。① なぜ CUI が必要なのか、② 連邦機関横通しの手続きはどこまで可能か、③ 従来のシステムからの移行はスムーズに進むのか、④ 移行費用や格付け担当者の育成はどうするのか、⑤ 情報の秘匿と共有のバランスはどうするのか、⑥ 情報公開法 (FOIA) との関連はどうか。

3. 結果

各種の資料を比較して概要を把握することができ、予備的考察としては一定の成果を上げた。上記 ② に関しては、CUI/Basic (各省共通) と CUI/Specialized (各省独自) の区分を設けて対応するなどの工夫が見られるが、③ と ④ は現在進行形であり、今後の展開を注視して行かねばならない。① ⑤ ⑥ は、この制度の本質に関わり結論部分でもあるので、次項でまとめる。

4. 結論

EO 13556 は、9.11 の教訓として「テロ情報は入っていたが、関係者に共有されていなかった」という反省から、従来の Need-to-Know の原則よりも Need-to-Share の必要性が叫ばれる中で発出された。情報の価値は「誰もが知っていれば意味がない」が、「誰一人も知らなければ意味がない」という両極端の中間にあるため、微妙なバランス論とならざるを得ない。CUI がその先駆的試みであることに変わりなく、多くの教訓が得られたので、本格的考察に移りたい。

【主要参考文献】

林紘一郎 [2017] 『情報法のリーガル・マインド』勁草書房