

## 議事要旨

会合名称： 第10回 モデル取引契約見直し検討部会 民法改正対応モデル契約見直し検討WG (WG1)

開催日時： 2020年2月17日(月) 16:00~18:00

議事内容：

### 1. セキュリティに関する論点について (SPT: セキュリティ検討PT)

#### (1) 関連資料の説明

- ・ SPT 主査より(資料 10-6)に基づき、SPT で作成中のセキュリティガイドラインが有効に活用されるための、セキュリティ仕様策定プロセス案について説明が行われ、共有された。
- ・ SPT 主査より(資料 10-8)に基づき、セキュリティガイドラインのデフォルト緩和策に関する緩和案と、そのイメージについて説明が行われ、共有された。
- ・ 委員より(資料 10-9、10-10)に基づき、SPT で作成中のセキュリティガイドライン(ver. 0.91)について説明が行われ、共有された。
- ・ 委員より(資料 10-3)に基づき、セキュリティ関連条項についての、JEITA コメント事項について説明が行われた。
- ・ 専門委員、委員より(資料 10-5-1、10-5-2)に基づき、セキュリティ関連条項についての、JEITA コメントを反映した条項案について説明が行われ、提案された。
- ・ METI より(資料 10-7)に基づき、セキュリティ関連条項についての、修正案について説明が行われた。

#### (2) 討議

上記(1)の関連資料の説明その他について各委員から意見等が挙げられ、議論が行われた。セキュリティ関連条項については引き続き議論することとなり、モデルプロセスとガイドラインについては今回の版を元に、適宜修正の上、パブリックコメントの募集を行うこととなった。主な議論は以下。

- セキュリティの定義が情報の滅失・毀損の対策のみが範囲になっていて、ソフトウェアそのものやソースへの対策が範囲外に読めてしまうので、定義の見直しが必要ではないか。
- セキュリティ仕様を定めてから、その後発見されるセキュリティについての情報提供を双方に促すことが望ましいと思っている。ベンダからユーザへの説明義務はあると思うが、どこまで説明しなければいけないかは、ユーザとの関係性、ユーザの持つ知見、作ろうとするシステムの性質等によって変わってくる。
- 日々発生する脅威に対して、誰がどういう責任でウォッチするのか。ベンダとしては、セキュリティ要件確定後は、セキュリティ情報を追っているセクションが個別のプロジェクトにブレイクダウンしてまで、「セキュリティの脅威がこうなっている」と落とし込めている会社はないと思う。脆弱性があることを知った場合と言っても、知った以上は伝えなければいけないのか等、WGとしては、ある程度の基準のようなものを示さなければいけないのではないかと。

以上