議事要旨

会合名称： 第６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）
セキュリティ検討 PT
開催日時： 2020 年 2 月 21 日（金）13:00～15:00
議事内容：

１．モデル契約第 50 条について

- （資料 6-3）に基づき、モデル契約書においてセキュリティ関連で追記したい条項案について説明が行われ、提案された。
- 上記の内容について議論が行われた。
  - ⇒ セキュリティ仕様作成のためにユーザがベンダに提供すべき「必要な情報」の内容を、もう少し詳細に書いた方が良いのではないか。
  - ⇒ ユーザの義務になるので、反発を受けない程度に慎重に記載する必要があると考える。
- ユーザがベンダに提供した「必要な情報」がいつの時点のものかを明記するようフォローした方が良いのではないか。
  - ⇒ 解説などで「セキュリティ仕様書に書き込むことが求められる事項」として示すのはどうか。
- 「必要な情報」のところで、ユーザはわかっている範囲で手持ちの情報は全て出した、と言えれば良いと思うので、そこの表現を工夫してほしい。
  - ⇒ ユーザが手持ちの情報を全て出したら免責される、ということにはならないのではないか。
  - ⇒ ベンダが求める必要な情報を適時提供する、という書き方にすれば良いのではないか。
  - ⇒ この点はより議論を深めたい論点である。
- 納品後にベンダが知り得た納品物のセキュリティ上のリスクについて、たとえ納品後であってもユーザに対して一定の情報提供義務があるのではないかとの考えに基づいて起草した部分（「納入物の納品後〇日間～通知するものとする」）について、〇日間経過後の情報提供は保守契約で担保されると想定しているのか。
  - ⇒ 保守契約を意識しているが、保守契約に限定しないほうが良いと考える。
  - ⇒ ユーザに保守契約等を結ばない場合のリスクを教示してほしい。

２．セキュリティ仕様策定プロセスについて

- （資料 6-4-1、6-9）に基づき、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について説明が行われ、共有された。
- 上記の内容について議論が行われた。
  - ⇒ 「2.4 外部設計作成（支援）プロセス」の部分がこのプロジェクトの最大の肝だと思っているが、方式設計と実装化設計が両方含まれているのなら、わかりやすくした方が良いのではないか。
  - ⇒ これは共通フレーム 2013 に準拠している。ソフトウェア方式設計の対応部分を追記する。

- （資料 6-4-2）に基づき、ユーザが仕様を確定する義務、ベンダの助言責任、インシデント発生の責任について説明が行われ、論点が提起された。
- 上記の内容について議論が行われた。
  - ⇒ インシデント発生時にはユーザとベンダが協力して解決にあたるなど、インシデント発生後の責任についても記述してほしい。
- 同じ件で、法的な責任と倫理的な責任を区別して議論し、法的な責任はその所在を明らかにするよう書かないと、誤解を持たれる場合がある。
  - ⇒ 法的な責任の部分を書くことは可能か。
  - ⇒ ユーザとベンダが協力しながらセキュリティを維持しなければならない。インシデント発生時にベンダの道義責任はあるかも知れないが、現実的にはコストが発生する。そういう背景を踏まえた上で書けないか。
- 事例になるが、大規模開発を行っている中でベンダに対して、セキュリティも含めてすべてガイドライン化したところ、ベンダの質が低下した。

３．最低限のセキュリティ仕様について

- （資料 6-5）に基づき、最低限実施すべきセキュリティ関連の設定や運用案について説明が行われ、提案された。
- 上記の内容についてより良くするための意見が示され、反映することとなった。

４．セキュリティガイドライン作成の進捗状況について

- （資料 6-6-1、6-6-2、6-6-3）に基づき、セキュリティガイドライン（Ver.0.92）作成の進捗状況について報告された。

５．セキュアコーディングガイドについて

- （資料 6-7-1、6-7-2）に基づき、Java Framework、Spring Framework を用いたセキュアコーディングガイドについて説明が行われ、紹介された。

６．今後のスケジュールについて

- （資料 6-8-1）に基づき、今後のスケジュールについて説明が行われ、確認された。
- （資料 6-8-2）に基づき、セキュリティ関連取引プロセスモデルと対策ガイドラインの意見募集のイメージについて説明が行われ、共有された。
- 上記の内容について議論が行われた。
  - ⇒ 取引プロセスモデルのところでガイドライン本体の使い方をしっかり書くが、重複しないか。ガイドライン自体に説明をつけなければならないか。ガイドラインはそれだけにしたい。
  - ⇒ このガイドラインは適用範囲が限られているが、取引プロセスモデルは一般のガイドラインに汎用的に適用できるようすべき。
  - ⇒ 今書いている取引プロセスモデルは、今回作成しているガイドラインを想定した書きぶりになっている。

⇒ ガイドラインを特定すると、一般的なプロセスにならない。

⇒ モデル契約で一般論的な書きぶりにするのは問題ないが、取引プロセスモデルでは他のガイドラインは考えていない。

⇒ スコープを明記して意見募集しないと、読者は混乱する。

⇒ 構成は色々あると思う。意見募集の説明の始めで作成中のガイドラインの位置付けをきっちり書けば良い。今の構成にこだわらなくても良いのではないか。柔軟な形でやってみてはどうか。

⇒ 意見募集の説明の案を書いてほしい。それで議論した方が早い。

7．その他

- 今回初めて最低限のセキュリティ仕様を提示したが、中小企業向けの議論も必要であるため、中小企業の取引の実態に詳しい方からも本 PT にご意見を頂きたくメンバーを追加したい、との意見が主査から述べられた。

以上