令和2年4月24日

独立行政法人情報処理推進機構　御中

情報システム開発契約のセキュリティ仕様作成のためのガイドライン（案）に関する意見

名前	
所属企業／団体／その他	一般社団法人情報サービス産業協会
メールアドレス	

意見記入シート（セキュリティガイドライン）

No.	頁No	指摘箇所(章節項番/行等)	意見
1			脅威ベースでのガイドラインは、国内ではかつてない試みです。起草者のご努力に厚く感謝申し上げます。

意見記入シート（セキュリティ仕様策定プロセス）

No.	頁No	指摘箇所(章節項番/行等)	意見
1	6	1.4.5セキュリティ仕様に盛り込むべき事項	「セキュリティ仕様については、当該ソフトウェアの作成目的、当該ソフトウェアの使用環境、OS、言語等により一律に決めることは難しいが、セキュリティガイドライン以外に、最低限実施すべき設定等を設けた。」と記載されています。このうち、「最低限実施すべき設定等」との記述については、それを設定しなければ、ベンダーが何等かの法的責任を問われることを前提とするかのように読めるところ、参考５に示されたデフォルト緩和策は、ユーザーにおける教育の重要性に言及しているなど、ユーザーとベンダー間のセキュリティ仕様として盛り込む最低限の要求事項として適切ではない事項も含まれており、ここにいう「最低限実施すべき設定等」と乖離していると思われます。誰にとって最低限実施すべき設定等であるのかを明らかにして、参考５の内容も調整くださるようお願いします。

No.	頁No	指摘箇所(章節項番/行等)	意見
2	6	1.4.5セキュリティ仕様に盛り込むべき事項	「その納入の時点で政府が民間事業者に求めるセキュリティ水準を達成するものとすることが望ましい。」との記述については、「その納入の時点で国及びセキュリティを所掌する独立行政法人が民間事業者に求めるセキュリティ水準を達成するものとすることが望ましい。」とすることを提案します。ソフトウェアの利用時点ではなく、納入時点の技術水準におけるセキュリティを求めていることに賛同しますが、セキュリティ基準については、セキュリティを所掌する独立行政法人が民間事業者に求めるものも加えるべきと考えます。また、政府の求めるセキュリティについても単に「望ましい」というレベルから「すべきである・しなければならない」とするレベルまであり、ソフトウェアの作成目的（用途）に応じて異なるものの、「すべきである・しなければならない」とするレベルのものがデフォルト緩和策に掲げられるべきものと考えます。
3	18	図２　デフォルト緩和策の位置付け	デフォルト緩和策について、「重過失・予見性の課題対象」と記載されていますが、デフォルト緩和策を実装しないことが誰の「重過失」になるのか明らかではないと思われます。ユーザーがデフォルト緩和策のいずれかを実施しない選択をし、それに伴う一定のリスクを受容した場合、ユーザーのリスク受容の判断がセキュリティインシデントの発生時に故意又は重過失になり得るということであれば理解できるところですが、ベンダーの契約不適合責任について「重過失」になるとするとの前提で記載されているのであれば、修正が必要と思われます。また、実際に参考５で示されているものは、ベンダーにとっての重過失を構成する事項ではないと思われます。
4	18	第２パラグラフ	ここに記載されている通り、参考５は、ユーザー主体による運用管理および業務ルールによる対策として実施することが想定されるものです。他方、「システムによる自動化、制限機能、チェック機能等の実装または実施を促すような対策もある」ことにはありますが、そのような対策が最低限求められるものとは言い難いため、「必要に応じてシステム開発時のセキュリティ仕様として盛込むことも推奨」とするのではなく、真に最低限の対策として必須のものを具体的に明記することが望ましいと思われます。
5	18	第２パラグラフ	「また、この対策は、ガイドラインによるリスク低減の効果に大きく影響するため、ベンダーはユーザーに対して内容をレクチャーすることを推奨する。」とありますが、ここの述べる「推奨」がどのような法的義務（信義則上の説明義務など）につながるのかが曖昧であり、加えて、ユーザー自身がベンダーのレクチャーをあてにせずに自ら理解すべき事項が多いと思われることから、説明義務の対象となるものと単なるレコメンドに過ぎないものとを区別して示すことが必要と考えられます。

No.	頁No	指摘箇所(章節項番/行等)	意見
6	20	3.4(6)	内部設計に関するベンダーの行為として、「このセキュア開発セキュリティ要件概要もユーザーと共有し、また、詳細設計方針として合意して内部設計書として管理する。」とされ、【参考8：セキュアコーディングガイド】とともに示されていますが、この要件に沿ったコーディングを行っているかどうかを検証するテストツールの整備が急務と思われます。現状では、ベンダーがそのすべての委託先も含めて製造される大量のソースコードがこれに沿ってコーディングされているかどうかを確認する手立てには乏しいのではないかと考えられるからです。まずは、ベンダーの技術者がセキュアコーディングに関してどこまで習熟しているかを調査し、その普及を図る必要があるのではないでしょうか。今回の意見募集では、意見提出者が【参考8：セキュアコーディングガイド】の内容をどこまで吟味して意見を提出されるか定かでないものの、影響は多大なものとなるように思われます。
7	31	【参考5：デフォルト緩和策　端末編　＜一覧表＞】	先にNo.4で述べた通り、ユーザー自身がなすべき最低限の対策とソフトウェアの開発を求められたベンダーが最低限実施すべき事項とを区分して記載することが望まれます。
8	47	【参考8：セキュアコーディングガイド】	セキュアコーディングの重要性について注意喚起することは大切であり、またセキュアコーディングと一口に言っても何をどこまですればよいのかが定かではないところ、具体的な項目を参考資料として明示していただいたことは価値が高いものと考えます。もっとも、この「セキュリティ仕様策定プロセス」におけるセキュアコーディングの位置づけについては解説が必要と考えられます。むしろ、セキュリティガイドラインの参考資料として移動するか、あるいは独立の参考資料として提供すべきではないでしょうか。