

版に対するご意見と、その対応

1. 全般に関して

0 1	ご意見	RFP の対象とするシステムの規模感（スケール）などがほしい。 業種や、システムサイズによりベースラインが異なるはず。 イメージしているシステムがもうすこし具体的にないか？ インシデント被害調査 WG で想定している、IT 依存度（0.2）などの説明が必要。
	対応	対象とするシステムを大枠で類型化し、対応レベルを分ける。
0 2	ご意見	E コマースサイトという表現からすると、かなりクリティカルな対策を要求されるのでは？ もともとのコンセプトが、ベースライン（最低線）という位置づけであるため、ここに記載されている内容は、必須要件と捉えるべき。 しかし、現実的には、必須要件としては厳しすぎるのではないか？
	対応	類型化したシステムによって、対応すべきレベルを 3 レベル（必須、推奨、任意）で定義する。

2. PFR パターン 1 に関して

0 1	ご意見	項目、説明、 について各々の位置づけがよくわからない。 説明があったほうがいいのでは。
	対応	各セクションの説明は、「×××のため、以下を考慮した対策を提案すること」とし、 項目は純粋な箇条書きにする。
0 2	ご意見	S1er から見ると、提案書を作りやすいパターンであるが、システムオーナーには、それなりの能力が要求される。
	対応	PFR を複数種類用意することで、レベルの異なる、システムオーナーの方にも使えるものをめざす。 また、このガイドライン作成に関する活動は、システムオーナーを含めた啓蒙を目的としているため、より一般に普及させることで、業界全体としての認識の向上をめざす。

0 3	ご意見	主語が不明確。「システム機能は」なのか「開発者は」なのか「運用者は」なのか明確でないため、機能要件なのか、運用要件なのかの区別がつかない。
	対応	現実的には、システム機能と運用でカバーすべき領域は時勢により流動的であるため、機能要件と運用要件を明確に区別することは困難と考える。よって、今回は明確にしない方向とする。
0 4	ご意見	今の項目分けだと、新たな手口への対応とか、追加的な提案などができない。
	対応	記載方法を工夫し、追加的な要件も盛り込めるようにする。
0 5	ご意見	外部からの攻撃への要件のみであり、内部的な視点が欠けている。
	対応	記載方法を工夫し、内部的な視点も盛り込めるようにする。

3 . P F R パターン 2 に関して

0 1	ご意見	項目 6 「不正アクセス対策」は、他の項目とレベル（粒度）が違いすぎる。
	対応	記載方法を工夫し、共通的な対策を記載する項目を設ける。
0 2	ご意見	項目 6 の中の、OS バグや、セキュリティホール.....には、具体的にパッチという表現を入れる。
	対応	指摘どおりに対応する。
0 3	ご意見	項目 9 の、「監視体制」など具体的な項目列挙はやめて、項目 8 までの対策についての運用設計を提案せよ！という記載がいいのでは。
	対応	指摘どおりに対応する。

3 . P F R パターン 3 に関して

0 1	ご意見	フリーフォーマットに近い提案が、SIer から提出されるはずであり、受け入れる側に、評価できるチェックリストが必要となる。 または、それなりの評価能力が要求される。
	対応	チェックリストは必要になると考えている。例として作成することは可能であるが、実際には、システムにより要件が異なるため、I S M S の管理策などを参考に作成いただくことになるものとする。