意見書

2012 年 7 月 23 日

佐藤　慶浩

情報セキュリティ対策とは、一般的に、情報の機密性・完全性・可用性[1]の３つの機能を確保することであるとされており、これらの機能はそれぞれ重要な要件となります。しかし、これらの中で、機密性が偏重されてしまい、完全性と可用性が比較的疎かになることがあります。これを防ぐための形式上の方法として、情報セキュリティ対策とだけ記載するのではなく、これら３つの機能を区別して明記することが考えられます。

情報連携基盤技術ＷＧの資料においては、「情報提供ネットワークシステム等の機能の概要（案）」の表中の「セキュリティ管理機能」の「機能概要」には、概ね機密性の観点での項目が例示列記され、その後の「等」により完全性と可用性の観点を暗黙に含む表記になっています。これは概要であり、詳細記載時には完全性と可用性の観点の項目が記載されることになるはずですが、このような全体機能概要の段階から、機密性・完全性・可用性を区別して記載することで、より確実に完全性・可用性の要件を明確にすることができます。

このとき、情報セキュリティ対策には、業務レベルと情報システムレベルの階層があり、業務レベルでインパクト・アセスメント（影響評価）をした後に、情報システムレベルでリスク・マネジメント等をするという関係が重要になります。このことは可用性の確保を意図する事業継続において言及されています[2]。

また、可用性の確保のために用いるバックアップデータの機密性の確保には、秘密分散技術の利活用が有用となります。これを単純なデータの分割と区別して理解しておく必要がありますが、両者の用語の定義が明確ではない点に注意が必要です。インパクト・アセスメントにより明らかになるとおり、全データが長期に保存されるバックアップデータの機密性の確保は至上の要件となります。これを保護する対策として、単独のデータだけから暗号鍵の総当たり攻撃等による不正な復号が可能となる対策では不十分とすれば、秘密分散技術の利用が解決策のひとつになります。

---

[1] 機密性・完全性・可用性とは、「政府機関の情報セキュリティ対策のための統一基準」で以下のように定義しています。
「機密性」とは、情報に関して、アクセスを認められた者だけがこれにアクセスできる状態を確保することをいう。
「完全性」とは、情報が破壊、改ざん又は消去されていない状態を確保することをいう。
「可用性」とは、情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保することをいう。

[2] 経済産業省「IT サービス継続ガイドライン 改訂版」平成 24 年、
http://www.meti.go.jp/policy/netsecurity/docs/secgov/2011_IoformationSecurityServiceManagementGuidelineKaiteiban.pdf

【参考】秘密分散の説明

仮に「２０１２」と「０７２３」という２つの数字を含むデータのバックアップの機密性を確保する例を使って、暗号化やデータ分割と秘密分散の違いを以下に説明します。

暗号化：
「２０１２」と「０７２３」を暗号鍵を使った暗号技術で暗号化して、その暗号化データを保管した場合には、暗号化データに対して、考えられるすべての暗号鍵値を試みることで、不正な復号ができてしまう可能性があります。一般的には、すべての値を試みるために必要な計算量が膨大になることで、現実的には不正な復号ができない「暗号強度」で保護することになります。

単純なデータ分割：
単純には「２０１２」を「２０」と「１２」に、「０７２３」を「０７」と「２３」に分割して、異なる２か所、以下の例では保管場所ＡとＢで保管します。

	保管場所Ａ	保管場所Ｂ
「２０１２」　→	「２０」	「１２」
「０７２３」　→	「０７」	「２３」

保管場所Ａにある「２０」から「２０１２」を情報の加工や計算などで導き出すことはできません。保管場所Ｂにある「１２」を入手しない限りは、保管者自身も「２０１２」を復元することはできません。
しかし、単純なデータ分割の場合だと、ＡとＢのそれぞれの保管場所では、元のデータの半分の情報量（４文字のうちの２文字）が単独でわかってしまいます。

秘密分散：
たとえば、「２０１２」を「１０００＋１０１２」という足し算の要素に分けます。

	保管場所Ａ	保管場所Ｂ
「２０１２」　→	「１０００」	「１０１２」
「０７２３」　→	「０５０９」	「０２１４」

データ分割のときと同様に、それぞれの保管場所にあるデータから元のデータを単独で推測したり復元することはできません。また、ＡとＢのそれぞれの保管場所では、上述の単純なデータ分割に比べると、元のデータの情報量を持っていないのが特長です。
しかし、この例のような単純な足し算の場合には、保管場所Ａの「１０００」というバックアップデータにより、元のデータは、それ以上の値であることがわかるため、情報量がゼロではありません。
これを、足し算の代わりに、コンピュータが用いる排他的論理和という計算処理などを用いることで、情報量をゼロにすることができます。（ただし、実際には、用いる乱数生成の再現を防ぐなどの追加技術を併用することになります。）
このように断片データに元の情報量がゼロになるような処理を秘密分散と定義することができますが、現状では様々な呼び方（秘密分割や割符など）をされています。

【参考】秘密分散の説明（つづき）

秘密分散の注意点：

秘密分散は、断片データに元の情報量がないことで高い機密性を確保できますが、これは２箇所に保管していても、その一方のデータが消失すると、本人でもデータを復元できないことを意味します。
保管場所でのデータ消失に備えるために冗長化する場合には、２分散の場合で４箇所以上に保管する必要があります。

秘密分散の応用：

仮に保管場所Ａの断片データが流出した可能性がわかった場合には、保管場所Ｂの断片データを消去することで、流出した保管場所Ａの断片データを無効化することができます。

断片データの複数箇所での同時流出時の機密性を確保するためには、分散数を増やすことができます。（以下の例は、単純な足し算の例にしています。）

	保管場所Ａ	保管場所Ｂ	保管場所Ｃ
「２０１２」　→	「５０１」	「７０２」	「８０９」
「０７２３」　→	「２９３」	「１１０」	「３２０」

ただし、この場合には、冗長化するには、６箇所以上の保管場所が必要になります。