参考資料

セキュリティチェックシート解説

<報告書>

目　次

図　表　目　次

1　はじめに

「セキュリティチェックシート解説」は、中堅・中小事業規模ユーザにおいてパッケージ取引・契約モデルに基づき、システム設計導入、更新時における契約活動を支援するためのものである。セキュリティについてユーザの仕様要求書（Request For Proposal、以下：RFP）の作成の支援、ならびに契約プロセスにおける重要事項説明書の理解促進を目的に作成を行なった。

具体的には、自社の IT システムの状況を把握し、自社の事業モデルにおいて必要とされるセキュリティ・可用性の要件定義について、補足資料にある「セキュリティ・可用性チェックシート」の活用を促進するものである。これにより、IT 専任担当者の配置が困難な企業ユーザにおいても適切な仕様要求が行なえることを目指している。

本解説を通じて上述のチェックシートの使用方法を理解し、より安全なシステム運用、事業計画の維持が中堅・中小事業規模の企業においても行なわれることを期待したい。

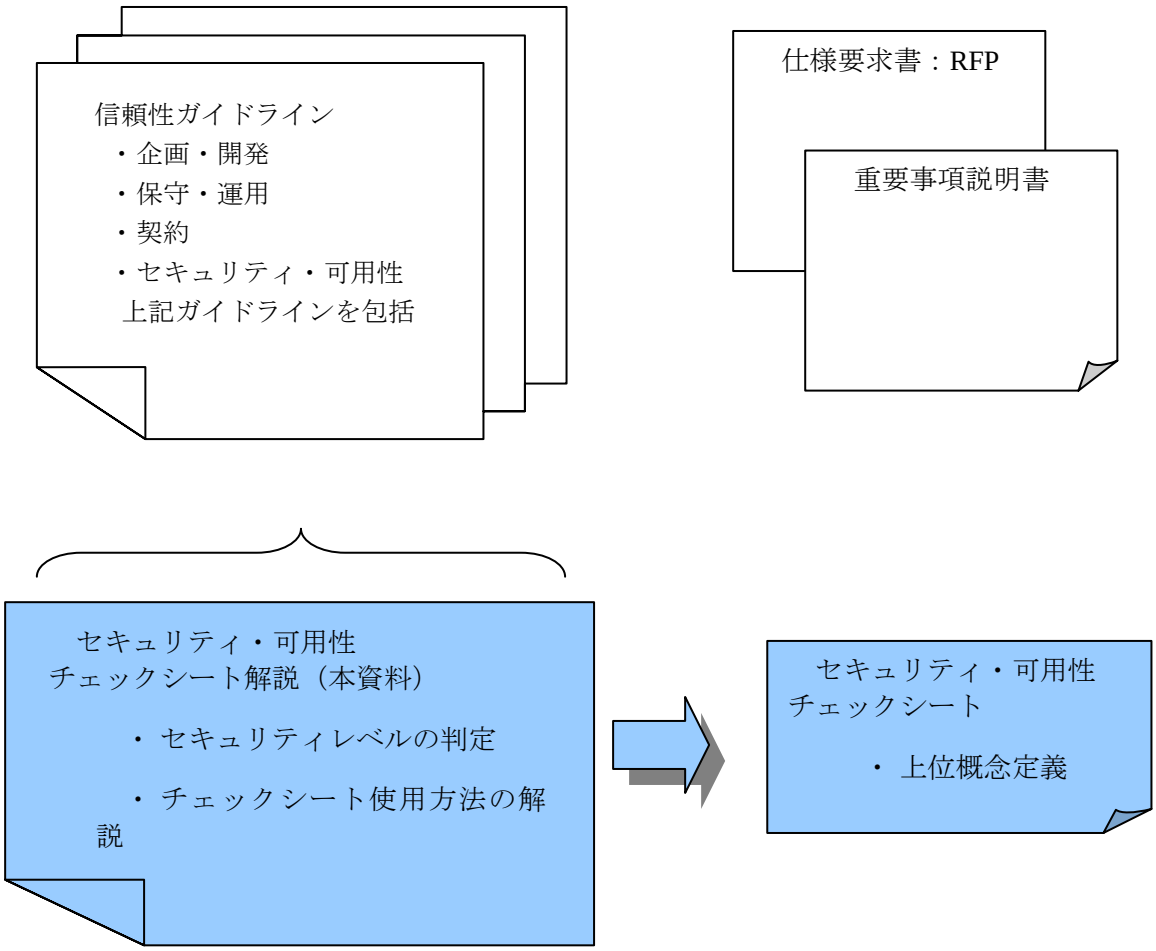


図 1　ガイドライン・チェックシート相関図

2　概要

2.1　　セキュリティチェックシート解説作成の背景

現在、IT は基幹システムのみならず、中堅、中小事業規模の企業においても事業継続において不可欠なツールとなってきている。反面、IT の進歩に従い、法令遵守の観点から取り扱う情報の保護ならびに防衛策の徹底、また、IT インフラを活用しての事業継続性の維持が事業規模に関わらず求められる。[1]

ただし、該当事業規模においては自社システムの導入・運用フェーズにおいて基幹システムと同等の開発を行うことは困難であり、概ね欧米を中心とする諸外国での実装モデルであり、汎用用途を目的に開発された「パッケージソフト」の導入を想定したシステムの構築を行うのが現状である。

本解説においては、このような認識から、平成 19 年 4 月に経済産業省商務情報政策局情報処理振興課より公表された「情報システムの信頼性向上のための取引慣行・契約に関する研究会　～情報システム・モデル取引・契約書～（受託開発（一部企画を含む)、保守運用）　＜第 1 版＞」（以降、「モデル契約書」）[2]　及び「追補版報告案」にベースに、中堅・中小事業規模の企業における IT セキュリティの確保のための指針に加え、事業継続性の観点より求められる要件定義、非導入リスクについて議論し取りまとめを行った。

2.2　　セキュリティチェックシート解説の目的

本解説の目的は、モデル契約書に基づき、これに準じた中堅・中小事業規模の企業を対象としたセキュリティチェックシート解説を提供することにある。本解説においては以下の点を留意されたい。

- 一般的なシステム導入時におけるセキュリティ対策、可用性設計の要素検討に加え、同一事業規模を対象とした指標・ガイドライン（例：経済産業省「企業における情報セキュリティガバナンスのあり方に関する研究会「情報セキュリティ対策ベンチマーク」、「事業継続計画（BCP)」など）を参照の上、検討を行なった。
- 「パッケージソフトウェア」、「中小事業規模ユーザ」における契約慣行に配慮する。
- 4 レベル（モデル例：大企業連結型、特定事業請負型、独立事業型など）を定義し、汎用パッケージにおけるシステム設計の簡素化を提案する。
- システム運用時における可用性についての定義付け、要求仕様について提言する。
- チェックシート解説に規定した項目を未実装とした場合の事業リスクについて定義を行い、情報システム取引契約時にシステム固有のリスクの可視化の促進を図る。

2.3　　基準とする標準規格

[1] 事業リスクについては「参考資料４．２ セキュリティ事故に従う被害額シミュレーション」を参照

[2] 公示内容は<http://www.meti.go.jp/press/20070116001/20070116001.html>を参照

現在、情報セキュリティ・事業継続計画については、国内外を問わず、多くの検討が行なわれている[3]が、ISO（International Organization for Standardization、国際標準化機構）と共通要件定義が進んでいる段階であり、日本においても今後国際規格に準じた対応を行っていくものと予想される。そのため、本解説作成においても以下の国際基準に基づいた要件定義の検討を行った。

(1) 情報セキュリティ

日本における情報セキュリティガイドラインについては英国規格 BS7799 をベースに JIS X：5080 としての規格化が進み、現在では JIS Q：27001 規格が基準となっている。そのため、セキュリティ要件項目の検討においては本規格に基づく検討を行った。

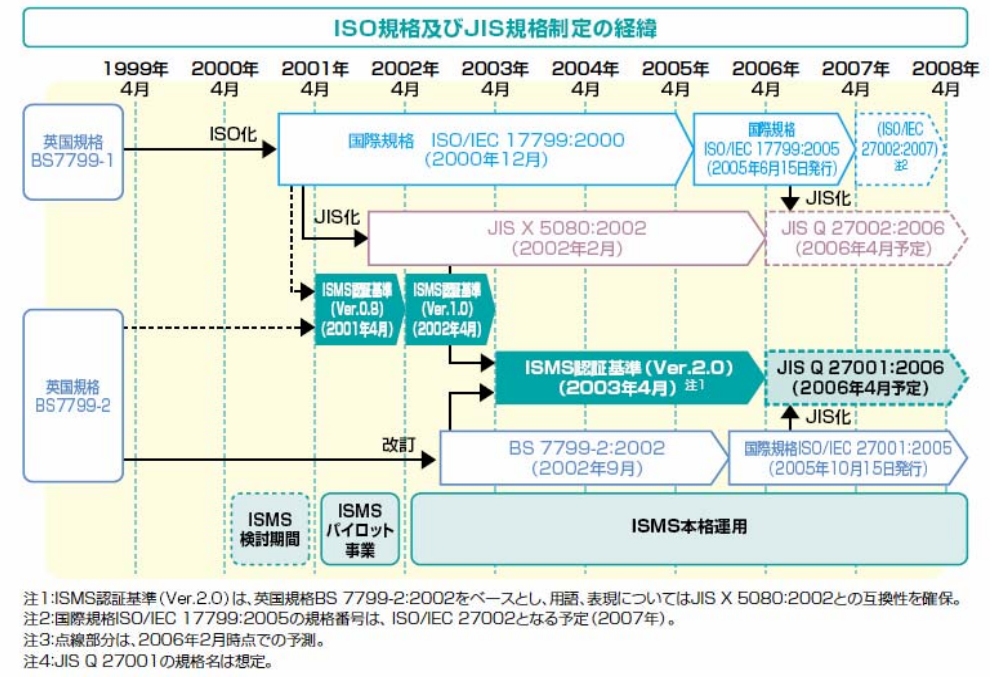


表 1　ISO 規格及び JIS 規格制定の経緯[4]

(2) 可用性

可用性についてはシステム運用の観点から ITIL（Information Technology Infrastructure Library）に基づき規定された IT サービスマネージメントの英国基準 BS15000 をベースに国際基準に発展した JIS Q：20000、また、事業モデルに応じて事業継続性の観点から制定された環境マネジメントシステム(EMS：Environmental Management Systems)の国際基準である JIS Q：14001 を参照したシステム実装が行われている。現在、事業継続計画（BCP：Business Continuity Planning）については事業計画管理（BCM：Business Continuity Management）としての国際基準化に向けた活動が活発化しており、英国規格協会（BSI：British Standards Institution）による PASS56、米国標準協会（ANSI：American National

[3]補足資料４．１　参考資料を参照

[4]出展：情報セキュリティマネジメントシステム 適合性評価制度の概要（ISO/IEC 27001:2005 対応版）（財）日本情報処理開発協会

Standard Institute）による NFPA-1600 の規定、日本においても経済産業省の企業における情報セキュリティガバナンスのあり方に関する研究会の報告書で示された「事業継続計画策定ガイドライン」、中央防災会議専門調査会（内閣府）「事業継続ガイドライン 第一版」などに基づいた提案活動を日本規格協会（JSA：Japan Standard Association）を通じて行われている[5]。ただし規格検討段階（規格提案国は 6 カ国：日本、英国、米国、カナダ、オーストラリア、イスラエル）であることを踏まえ、当検討委員会においては上述ガイドラインならびに ANSI 規定内容などを参照の上、今後の動向を見据えた検討を行った。

2.4 セキュリティチェックシート解説で使用される用語定義について

本解説において使用される用語については共通フレーム 2007 を準用した。ただし、セキュリティチェックシートなどの表記については中堅・中小事業規模のユーザにも理解しやすい内容とすることを目的に簡易表記を行なっている。

3 セキュリティチェックシート解説

モデル契約書において、セキュリティ・可用性に関する要件定義については広く議論がなされ、仕様要求書（RFP）作成における方針ならびにサンプルドキュメントの掲載が行なわれている。ただし、中堅・中小事業規模の企業においては専任のシステム管理者の配置が困難である場合も多く、システム導入についての明確なセキュリティ・可用性要件定義を行なうことが困難であるものと推測される。

本解説は、これら企業ユーザを対象に自社のシステム状況の把握、求められるシステム要件定義書作成における支援、ならびにベンダからの説明項目の標準化を目指し、策定を行なった。

3.1 セキュリティ・可用性レベル設定について

(1) 想定される事業モデル

RFP を作成するための知識、人的資源が十分に確保することが困難である中堅・中小事業規模の企業において、具体的な対策についての計画設計を行なうには今までベンダに依存する構造となっていた。今回、以下のようにセキュリティ・可用性対策の観点から事業モデルケースの考察ならびに求められるシステム要件のとりまとめを行なった。

ユーザには自社の事業モデルに基づき、まずはどのレベル達成が求められるのかを本表に基づき考察を進めることを希望する。

[5] 本議論の進捗については JSA の Web サイト<http://www.jsa.or.jp/stdz/mngment/mngment.asp>を参照

	想定される業務モデル	情報セキュリティ要件	可用性要件	SWベンダー要件
レベル４ （推奨）	行政機関、大企業向けの業務支援活動を中心に行う コンプライアンス対策などについて発注元と同等のものが求められる	・各クライアント対策に加え、ゲートウェイでのセキュリティ対策、コンテンツセキュリティの実装を行う ・管理する専任者を配置	・24×7システムの実装 ・システムダウンタイム 数時間/年間レベルの維持などを 専任管理者の下運用する	・J-SOX対応、P-mark対応などコンプライアンス対策への対応 ・日本国内での障害対応部門の設置 など
レベル３ （標準）	基本的に委託業務型であり、受注案件に応じて他企業・機関との情報の流通が行われる	・上記同様のセキュリティレベルを維持する。 ・専任管理者の配置が困難な場合には遠隔監視モデルの採用を検討する	・24×7システムの実装 ・システムダウンタイム 数時間/年間レベルの維持など遠隔モデルなどを活用し維持する	・J-SOX対応、P-mark対応などコンプライアンス対策への対応 ・日本国内での障害対応部門の設置 など
レベル２ （低）	独自事業展開により、他企業との情報の流通はほとんど無い	・クライアント対策など基本的な対応を行う ・導入に対しては企業単位にて管理ツールにて品質維持できる環境を構築	・データバックアップ方法の確立 ・システム障害発生時のリカバリー手段の確保	・管理ツールが実装可能など
レベル１ （非推奨）	情報閲覧などのみITを活用 事業継続性への影響が全くない	・基本ソフト標準の機能を活用する	・特に行わない	・対策未実装のリスク提示など

表 2　事業モデルにおけるセキュリティ・可用性レベル設定[6]

(2) セキュリティ・可用性　上位概念定義

上述の「2.1.1 想定される事業モデル」ではユーザが自社として実装すべきセキュリティ・可用性レベルについて定義を行なったが、中堅・中小事業規模の企業における実際のシステム運用においては具体的にパッケージソフトウェア製品ならびハードウェア機器を基本としたセキュリティ・可用性対策が求められる。本ワーキンググループの討議においては JIS Q：27001 規格に基づきセキュリティ・可用性対策についてレベルに応じた対策ならびに未実装の場合のリスクについての検討を進めた。ただし、中堅・中小事業規模の企業において、上記 JIS 規格に基づく仕様設計の検討を行なうことは容易なことではないため、上位概念についての検討を行い、取りまとめた。ユーザにはまずこのセキュリティ・可用性対策に関する上位概念定義を参照し、自社のシステムにおいて必要とされる要件定義を把握し、ベンダと対等に契約交渉を行なえるように配慮した。全体は、～情報システム・モデル取引・契約書～（パッケージ、SaaS/ASP 活用、保守、運用）＜追補版＞を参照されたい。

[6] 平成 19 年 4 月交付の信頼性ガイドラインとは異なり、レベル 4 を最高レベルとして定義を行った。これは、将来、より高度なセキュリティ強度が求められる場合に柔軟に対応するためのものである。

対策項目	リスクの詳細	参考情報			
		レベル1	レベル2	レベル3	レベル4
■認証 情報を参照している人が本人であることを証明する。	情報を参照している人が、本人であるかを管理していないと、他人に重要な情報を見られる可能性がある。	**■何も決められていない** 情報を誰が参照しているか特定できない状態。	**■個人を認識できる** パスワードを利用して、個人を認識できるようにする。	**■本人認証の強化** 特定のカードやログインの二重化などで、本人認証を強化する。	**■絶対的な本人認証** 生体認証等を組み合わせ、定期的なポリシー変更を実施する。
■アクセス権 情報よって、アクセスできる人を制限・管理する。	誰でも情報アクセスできるようになっていると、削除、改ざん、複製、持ち出しされたりする。	**■何も決められていない** 情報に誰でもアクセスできてしまう。	**■コンピュータ単位で設定できる** サーバ単位、フォルダ単位で、個人・グループがアクセスできように設定する。	**■認証情報に基づき資源単位でアクセス権が設定できる** ファイル単位で、個人・グループがアクセスできるように設定する。	**■資源単位でアクセスした内容の収集、分析ができる** アクセスされた情報（ログ）を収集・分析できる。
■暗号化 情報を暗号化して、紛失・盗難・盗聴の対策を施す。	情報機器（コンピュータやUSBメモリなど）が盗難又は紛失することにより、情報が漏えいするおそれがある。	**■何も対策されていない** 社外に持ち出すデータ、社内のコンピュータのデータに暗号化が実施されていない。	**■モバイルコンピュータやUSBメモリ単位で暗号化して持ち出す** 社外に持ち出すコンピュータ、USBメモリなどの中に入っているデータを暗号して持ちだす。	**■全てのコンピュータについて、データを暗号化する** 社内のコンピュータ、社外に持ち出すコンピュータ、業務で使用するUSBメモリ、外付けHDD、CD/DVDなど情報を書き込めるものに対して暗号化をする。	**■暗号されたものを復号する都度、認証をおこなう** 暗号化されたデータを復号するたびに認証を実施して、履歴を取得する。
■悪意あるプログラムの検出 悪意あるプログラムから情報資産を守る。	コンピュータに誤動作を起こさせる悪意あるプログラム（ウイルスやスパイウェア等）により、システムが利用できなくなる、データが消去される、情報が外部に漏えいしてしまう、などのおそれがある。	**■何も決められていない** ウイルス対策を実施していない。	**■ウイルス等を検出し侵入を停止・警告できる** コンピュータ上で悪意あるプログラムを検出して削除し、警告できる。	**■全システムに対するウイルス対策と集中管理** ネットワーク機器やコンピュータなど複数の対象に対して、悪意あるプログラムを検出、削除するための機能を導入し、被害状況の収集や定義ファイルの更新を集中的に管理できる。	**■不審な通信やコンピュータをシステムから隔離できる** 悪意あるプログラムが検出されたコンピュータをネットワークから遮断する。
■ネットワークの運用 ネットワークを流れるデータ量の管理をする。	ネットワーク障害や大量のデータ転送により、ネットワークが正常に利用できなくなるおそれがある。	**■何も決められていない** ネットワーク管理ツールもしくはサービスを導入していない。	**■管理ツールを導入する** 障害検知やネットワーク負荷を検知するツール、サービスを導入する。	**■冗長化する、使用状況を監視して記録できるようになる** ネットワーク機器を冗長化して大量データに備えたり、ネットワーク障害時にネットワークが利用できなくなるのを回避したりする。	**■トラフィックに応じた柔軟な制御ができる** ネットワークの使用状況に応じて、機器の設定を容易に変更できる。
■保守 OSやアプリケーション、ハードの保守を行なう。	保守がされていないと、不具合の発生や、セキュリティホールによって情報が漏えいするおそれがある。	**■何も決められていない** メンテナンス作業をやっていない。	**■障害発生時に対応する** 障害が発生した時点で、保守作業を実施する。	**■修正版発行時に対応する** 保守対象となる不具合修正版の発行時に、予備機でテストをおこない、適用する。	**■予防的に対応する** 定期的、計画的に、不具合修正版の取り込みを行う。
■機器運用監視 サーバ、ネットワーク機器の稼働監視を行う。	システムの状況を把握できないことにより、障害の対応が遅れて情報システムへのアクセスが長時間停止するおそれがある。	**■何も決められていない** サーバ、ネットワーク機器の稼働状況を監視していない。	**■運用状況を遠隔で、手動で把握できる** 遠隔で稼働状況を手動で確認する。	**■運用状況を自動で把握、記録ができる** 稼働状況を常時把握し、異常があれば通知する。	**■運用状況に異常があれば、自動的に設定された状態に切替わる** 異常を通知するとともに、代替手段に自動的に切替わる。

表 3　セキュリティ上位概念定義（抜粋）

(3) セキュリティ・可用性チェックシート（詳細項目版）

セキュリティ・可用性チェックシート（詳細項目版）は JIS Q：27001 規格を基準とし[7]、ユーザが実装すべきセキュリティ・可用性対策についてレベル別に定義を行なうものである。今回、対策を行なわなかった場合のリスク要素についても議論を進め、とりまとめを行っており、2008 年 4 月をめどに発表の予定である。

また、現段階では標準規格化に向けた準備段階である Web サイト、Web アプリケーションによるシステム導入時におけるセキュリティ・可用性についても議論を進め、定義付けの検討を行なっている。本チェックシートは上記した上位概念定義に基づくセキュリティ・可用性の仕様選定においての活用、重要事項説明書におけるリスク説明などの際にユーザ側のみならず、ベンダ側での活用を強く望むものである。

[7] 「参考文献（JIS Q 27002：2006 以外）」として、項目によっては他に参照したガイドラインの記載を行った。

	技術的セキュリティ対策 要素	分類	対策項目	リスクの詳細	レベル1	推奨レベル レベル2	レベル3	レベル4
1	情報を他人から守る(機密性保護)	認証	パスワードを利用する	パスワードが推測可能な容易な物になっていると、第三者がシステムに不正アクセスし、情報を漏えいしてしまうおそれがある。	・パスワードを利用しない。	・初期パスワードをすみやかに変更する。 ・定期的(六ヶ月毎)に、パスワードを変更する。 ・パスワードは、複雑なもの(八桁以上)を設定する。 ・パスワードは、管理者を含め誰にも教えない。 ・パスワードを書き留めたり、コンピュータ上のファイルに保管したり、メールで送信したりしない。やむを得ず紙片等にパスワードを記載する必要がある場合には、そのパスワードが容易に第三者に見られることがないように保管する。 ・自分のパスワードが他人に漏えいした可能性や疑いがある場合は、パスワードを変更する。	・定期的(三ヶ月毎)に、パスワードを変更する。 ・パスワードは、複雑なもの(八桁以上、パスワード世代管理、三種類以上の文字種の使用)を設定する。	・同一利用者が複数のアカウントをもつ場合は、それぞれ異なるパスワードを設定する。また、一つのパスワードから他方が推測しやすいパスワードを設定しない。 ・機密性が高い部署では、生体認証を使用する。
2			ネットワーク上の機器を識別する	不正な情報機器がネットワークに接続されると、情報が漏えいするおそれがある。	・未登録や不正なコンピュータの接続を検出できない。	・未登録や不正なコンピュータの社内ネットワークへの接続を、検出して警報をあげる。 ・接続コンピュータのログを取得する。	・未登録や不正なコンピュータの社内ネットワークへの接続を、検出し、警告して、接続を防止する。 ・接続コンピュータのログを取得する。	・未登録や不正なコンピュータの社内ネットワークへの接続を検出・警告し、接続を防止する。 ・正常な未登録のコンピュータを、自動的に登録する。
3			利用者が本人であることを証明し承認する	利用者の身分が証明できないと、権限がない利用者が情報を不正に取得して社外へ漏えいさせるおそれがある。	・一台のコンピュータを一つのアカウントで、複数の利用者が使用する。 ・認証ログは取得しない。	・Windowsのアカウント、パスワードを利用して、利用者を識別する。 ・一台のコンピュータを複数の利用者では使用させない。 ・認証ログを取得する。	・一台のコンピュータに対して、一人しか使用させない。 ・特定のカードやログインの二重化などで、本人認証を実施する。 ・認証ログを取得する。	・生体認証(静脈・指紋認証など)を利用して、利用者の本人認証を実施する。 ・二要素認証を実施し、認証強度を上げる。 ・認証ログを取得する。
4			業務ソフトウェアや機器認証で使うパスワードを管理する	パスワードの管理がされていないと、不正な活動や情報漏えいが確認できないおそれがある。	・パスワードを管理しない。	・認証機能を使用して、コンピュータを利用する。	・認証機能を使用して、コンピュータと業務ソフトウェアを利用する。	・生体認証を利用してパスワードを使わない。
5			業務ソフトウェアの起動時間を監視する	業務ソフトウェアが終了されずに放置されていると、情報が盗まれるおそれがある。	・業務ソフトウェアの未使用時間を監視しない。	・業務ソフトウェアの未使用時間を監視する。 ・一定時間以上利用されないセッションを監視する。	・業務ソフトウェアの未使用時間を監視し、警告する。	・業務ソフトウェアの未使用時間を監視し、警告して、遮断する。
6			情報へのアクセスを管理する	誰もが情報を閲覧できるようになっていると、情報の改ざんや漏えいのおそれがある。	・サーバ上の情報に誰でもアクセスできる。 ・情報を機密レベルに分類しない。 ・情報にアクセスした履歴を取得しない。	・サーバ上の情報にアクセス権をつけて、権限のない利用者は使用できないようにする。 ・情報にアクセスした履歴を取得しない。	・情報を重要度別((秘)(社外秘)(関係者外秘)など)に分類して、重要度別に利用者やグループ単位でアクセス権をつけて管理する。 ・情報にアクセスした履歴を取得する。 ・印刷物を減らすことにより、管理する対象を減らし、情報漏えいのリスクを減らす。 ・印刷物に対して、誰がいつ印刷したものか、わかるように「すかし」などを挿入する。	・アクセスの履歴を定期的に監査して、情報の持ち出しに問題があれば是正する。
7		暗号化	コンピュータや電子媒体を暗号化する	情報機器が盗難又は紛失されると、情報が漏えいするおそれがある。	・データを暗号化しない。	・社外に持ち出すコンピュータ、電子媒体(USBメモリ、外付けHDD、CD/DVDなど)の中のデータを暗号化する。	・社内のコンピュータ、社外に持ち出すコンピュータ、電子媒体(USBメモリ、外付けHDD、CD/DVDなど)に対して暗号化をする。	・社内のコンピュータ、社外に持ち出すコンピュータ、電子媒体(USBメモリ、外付けHDD、CD/DVDなど)に対して暗号化をする。 ・復号時には認証が毎回必要となる。
8			ネットワークを流れる情報を暗号化する	ネットワーク上のデータが盗聴されると、情報が漏えいするおそれがある。	・社外に送るデータは平文で送信する。 ・Webの通信は暗号化(SSL通信)しない。	・Webの通信を暗号化(SSL通信など)する。	・社外に出る情報を、事前に社内で暗号化して送信する。 ・Webの通信を暗号化(SSL通信など)する。	・コンピュータから発信する情報(メールの添付データなど)を、社内、社外にかかわらず、すべて事前に暗号化して送信する。 ・Webの通信を暗号化(SSL通信など)する。
9			暗号鍵の強度を上げる	暗号の複雑さが低いと、簡単に復号化されて情報が漏えいするおそれがある。	・暗号化しない。	・公に認知されているアルゴリズムで暗号化する。 ・鍵長が64ビット以上の暗号化を使用する(AES 64ビット以上など)。	・公に認知されているアルゴリズムで暗号化する。 ・鍵長が128ビット以上の暗号化を使用する(AES 128ビット以上など)。	―→ 前レベルと同様
10			暗号鍵を管理する	暗号鍵が外部に流出すると、暗号化したデータを復号されて、情報が漏えいするおそれがある。	・暗号化しない。	・暗号鍵を、平文(通常の文字列)のままソフトウェア上で管理する。	・暗号鍵を、暗号化してソフトウェア上で管理する。 ・サーバ上で、暗号鍵の保管場所を誰にでもわかるようにする。	・暗号鍵を暗号化して、独自のパスワード等で保護する。 ・暗号鍵の所在については、システム的に管理者以外は閲覧できなくする。

表 4　セキュリティチェックシート（詳細項目版：一部抜粋）

(4)　本チェックシート使用の際の留意事項

- 推奨レベル（網掛け部分）とは、中堅・中小事業規模のユーザにおいても実装することが望まれるセキュリティ対策について定義づけがなされている。
- 必要とされるレベル定義の判断については、網掛けがされている項目に特に留意し、これらの項目が満たされているかを中心に点検を行なう。
- 本チェックシートは業務要件定義でレベルを決定しユーザ、ベンダが仕様について合意する。パッケージ選定の際には、業務要件としてのセキュリティ要件を確認し、システム要件にあわせて具体的な仕様を決定する。
- セキュリティ要件は、技術的、システム的に解決するだけでなく、運用、保守、教育を含めた継続的な措置が重要であることをユーザ、ベンダともに合意する。

3.2　セキュリティ対策

今日では、情報システムがビジネスに密接に関係する比率は高くなっている。たとえば、10 年前に多くの企業で業務の遂行や連絡に、紙の文書、電話、郵便などの情報システムに直接依存しない方法を使用していた。今日では、電子メール、イントラネット、経理システムや Web サイトなどの情報システムを活用している。電子商取引に携わっている企業では、企業顧客間取引(B2C)、企業間取引(B2B)、企業従業員間取引(B2E)等の安定した運用がビジネスの成否に大きな影響を与えている。この様に、ビジネスが情報システムに依存する比率が高くなっており、情報システムの問題はビジネスへのリスクとなる。

環境内のサーバーに深刻な攻撃が行われた場合、組織全体に甚大な被害が及ぶ。例として、攻撃によって組織の Web サイトがダウンした場合、売上や顧客からの信頼を失い、組織の収益にも影響することも考えられる。また、個人情報を漏えいした場合、信頼を失い取引関係が消失し、漏えい後の顧客への対応に多くの費用を必要することが容易に予測できる。

このような問題は、大規模な組織のみでおこるものではなく、中堅・中小事業規模の企業を含め、どのような規模や環境でも起こり、セキュリティ問題をリスクとして真剣に考える必要がある。リスクは恐れるべき対象ではなく、管理すべき対象であり、情報システムの企画・開発・運用等の各段階において、不確実性を認識して最小化し、確認した各リスクに予防保全的に取り組むことによって管理できる。実際にセキュリティ問題が発生した場合、IT への依存度や問題の程度によっては、ビジネスの存続自体を不可能にし、この可能性はビジネスの規模が小さい程顕著となる。セキュリティ対策に投資することはネガティブにとらえられがちであるが、IT 依存度に比例したセキュリティ対策を導入することが、ビジネスの継続の基盤となる。

事業の内容や規模にあった適切なコストをかけたセキュリティ対策を行うことは、将来のビジネスを保護し不確定なリスクを排除する。セキュリティ問題が発生した場合でも、適切な対策を行っている事で顧客の理解を得られる場合も考えられる。また、適切なセキュリティ対策を行っていることが、取引の条件となる事が今後も増加すると考えられる。

本解説は、主として中小規模の事業者が、パッケージ製品、開発製品、Web サイトの構築を提供または導入する担当者双方が共通の認識で検討するべき事項を提供する。

推奨されるセキュリティ対策を ISO/IEC27001(JIS Q27001)による用語の定義「情報の機密性，完全性及び可用性を維持すること」に基づきセキュリティの重要な 3 要素である、「機密性保護 (個人情報、営業機密などの情報を守る)」「完全性保護 (改ざんやなりすましの様な不正な変更から情報を守る)」「可用性保護 (情報システムや情報が必要な時に利用できるように維持する)」を軸に対策と発生しうるリスクをコストに合わせて選択できるようにまとめを行った。

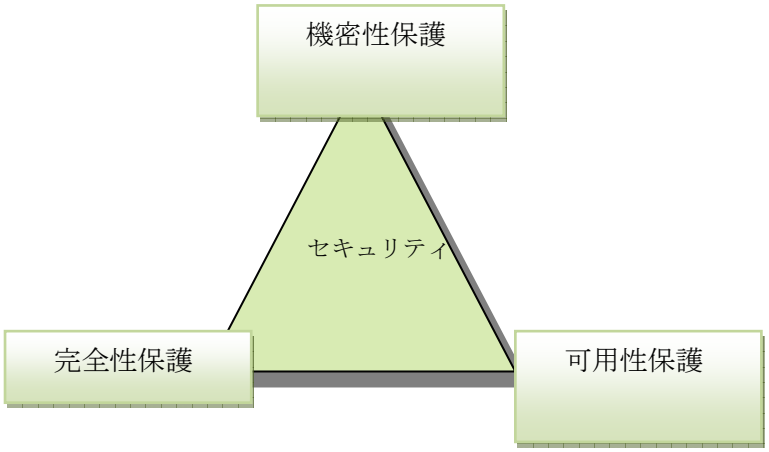


図 2　情報セキュリティに求められる 3 要素

3.3　　可用性対策

可用性とは国際標準化機構（ISO）が定める標準用語（Availability：アベイラビリィティ）に基づくものであり、その定義としては「認可された利用者が、必要なときに情報に

アクセスできることを確実にすること」[8]を示すものである。すでに小規模事業企業においても諸取引の電子化が進んでおり、業務の受託元企業との相互情報伝達の維持、自社のデジタル資産のバックアップが不可欠になってきている。システム導入期（企画・開発フェーズ）においては、システムの安定稼働についての議論がベンダ・ユーザ間で行なわれるが、反面、運用開始後の可用性（事業継続計画に基づく IT システムの安定稼動）については十分な対策が講じられていないのが現状である。そこで想定レベルに応じて、実運用時に起きるトラブル事例に基づいた対策案について議論を進めてきた。

コンピュータが機器である以上、連続使用による経年劣化、温度変化、結露などがもたらす障害発生は起こりえるものと想定し、それに対応するシステムの運用・保守体制が必要である。

(1) 起こりえるシステムトラブル・事業中断内容について
中小規模事業企業においても今日では会計システムに代表とする業務の IT 化が進んでおり、事業継続性の観点からコンピュータの障害・停止などに従うダウンタイムの原因と処置について取りまとめを行なった。

ダウンタイムの原因	例	処置	回避のための予防措置	
			導入（企画段階）	運用・保守
点検（計画保守）による停止、起動	ハードウェア 機器、OS、ソフトウェア	アップグレード、交換、清掃	クラスタリングによる冗長化	ログの監視
機器の障害	コンピュータ（メモリ、冷却ファン、システム ボード、電源装置、ドライブ、ドライブコントローラ、NIC）	交換、清掃	クラスタリングまたはフェイルオーバーによる冗長化 ホットプラグ、RAID構成、SNA構成	定期点検及び交換、清掃、設置環境の維持、必要に応じてファームウェアのアップグレード
	ルーター、ハブ	アップグレード、交換	クラスタリングまたはフェイルオーバーによる冗長化、ホットプラグ	定期点検、清掃、設置環境の維持、必要に応じてファームウェアのアップグレード
	ネットワーク ケーブル	交換	床上げ、無線化	ワイヤリングの見直し、定期点検及び交換
ソフトウェアの不具合	OSの応答停止、アプリケーションの応答停止、異常出力、ファイルの破損	アップグレード、再構築	クラスタリングによる冗長化、仕様の再検討、テスト体制の見直し	計画保守によるアップグレード、テスト及び再起動
悪意あるソフトウェア	外部攻撃、ウイルス、スパイウェアによるファイルの破損、書き換え	認証の強化、通信ポートの制限、OSのアップグレード、アンチウイルスによる駆除	複雑なパスワードの採用、認証システムの強化、必要な通信ポート以外の通信制限、アンチウイルスでの検索・駆除設定、バックアップ	定期的なアンチウイルスによるウイルスの検索及び駆除、定期的なパスワードの変更、パスワード履歴管理
操作員のミス	データの削除、書き換え、誤入力	UIの変更、権限の設定、操作の教育	管理権限と運用ルールの見直し、コード体系の設定、入力ルールの設定、バックアップ、操作員の現況把握と適切な教育	コード体系の見直し、GUIの見直し、ロールバックの設定
悪意のあるユーザー	データの持ち出し、外部漏洩、改ざん	アップグレード、再構築、暗号化、持ち出し制御	セキュリティポリシの策定、出力・複写の制御及び監視、ログ管理、バックアップ、従業員の現況把握と適切な教育	運用ルールの強化、定期的なログの分析、ロールバックの設定、セキュリティポリシの見直し、教育
災害による機器の損傷	火事、水濡れ、地震、台風、洪水、停電、高温障害	交換、再構築	データセンターでのハウジング、バックアップ	清掃、設置環境の維持

表 5　可用性の側面からみたトラブル事例および予防・処置対策

(2) 事業モデルに基づく可用性対策のレベル設定について
また、事業モデルに応じた可用性対策について検討を行なった。実際には事業形態に応じた考察が必要であるがモデルケースとして参照されたい。

[8] 総務省 国民のためのセキュリティサイト　用語辞典

	単独 スタンドアロン	LAN1 Internet共有・スタンドアロン	LAN2 ドメイン・2-Tier	LAN3 ドメイン・3-Tier	Saas Web, 3-Tier
管理者	オペレータが兼務	オペレータもしくは兼務の管理担当者	兼務の管理担当者もしくは管理者	管理者	←スタンドアロン以外
外部ネットワーク接続形態	なし	PPTPによるInternet接続	PPTPによるInternet接続	ルータによる固定IP接続	←スタンドアロン以外
内部ネットワーク接続形態	なし	ディスク共有、Workgroup	File-Server, Printer-Server	File-Server, Printer-Server, Apps-Server	←スタンドアロン以外
認証	ローカルパスワード	ローカルパスワード	ドメインパスワード	ドメインパスワード	←すべての形態
オペレーター以外のPC共有	あり	あり	なし	なし	←すべての形態
第三者とのデータのやりとり	リムーバブルメディア、DISK共有	リムーバブルメディア、DISK共有、電子メール	リムーバブルメディア、DISK共有、Server共有、電子メール		←すべての形態
プリンタ	ローカル	ローカル、共有			←すべての形態
主たるデータの場所	ローカル、内蔵、外付HDD	ローカル、内蔵、外付HDD	ローカル、内蔵、外付HDD、Server	DB-Server	Appsに依存、ローカル、Server、外部Server
主たるアプリの場所	ローカル、内蔵、外付HDD	PC、内蔵、外付HDD	PC、内蔵、外付HDD	PC、内蔵、外付HDD、Apps-Server	外部Server
主たるLANの用途	該当なし	電子メール、Web閲覧	電子メール、Web閲覧、基幹業務		
求められるセキュリティ・可用性レベル	レベル2	レベル2	レベル3	レベル4	レベル3 （社内システムはレベル2）

表 6　可用性対策におけるレベル別モデルケース

4　Web サイト、Web アプリケーションにおけるセキュリティ対策について

インターネットに接続された Web サイト（企業のポータルサイトや EC サイト等）は、そのシステム構築にパッケージソフトウェアを利用したとしても、技術者によるスクリプト・プログラム（Java、JSP、JavaScript、PHP、Perl….等）の開発作業割合が非常に多い。従って、Web サイトのセキュリティレベルも Web アプリケーションの開発者や開発ベンダの技術レベルに強く依存する。さらに、アンケート機能、E-Commerce 機能等の活用により、個人情報を含む重要な情報が格納されている。そのような特性にもかかわらず、インターネットに直接接続されているため、不正アクセス等の攻撃を受けやすい環境にあり、企業内ネットワークに構築されている各種のシステムと比較すると、より強固なレベルのセキュリティ対策が必要であるといえる。

そこで、本章では、インターネットに直接接続された Web サイトおよび Web アプリケーションのセキュリティ対策について解説する。

4.1　Web アプリケーションのセキュリティ対策の現状と課題

Web アプリケーションにおいて、脆弱性が存在した場合、以下のような被害が発生する可能性がある。

(1) 社内情報の漏洩・改ざん・破壊等
Web サイト（アンケートや会員登録機能）で管理している個人情報や社内の重要な情報が漏洩したり、Web を利用するシステムが破壊されたりする。また、課金情報など重要な情報の改ざん、漏洩の可能性がある。

(2) 会員や管理者への成りすまし
Web サイトの会員に成りすましてオンライン上での購入が行われたり、誹謗中傷

のメッセージを書き込まれたりする可能性がある。また、管理者権限で Web サイト内の情報を搾取・改ざんが行われる可能性もある。

(3) フィッシング詐欺や攻撃の踏み台などに悪用
Web サイトにフィッシング詐欺の勧誘記事を掲載されたり、攻撃者のサイトに誘導されたりする。また、Web サイトを踏み台（経由）して、他の Web サイトの攻撃に利用される可能性がある。

IPA/ISEC（独立行政法人 情報処理推進機構 セキュリティセンター）に届出のあった不正アクセスの被害・相談状況によると、OS の脆弱性に対する修正プログラムが長らく適用されていなかった、といった事例が見受けられる。また、古い脆弱性を攻撃対象としたアクセスも非常に多く、ボットに感染しているコンピュータが日本にもまだまだ多い、ということが推測されている。

これらの不正アクセスや攻撃の方法は、決して目新しいものではない。しかし、Web アプリケーションの開発者や運用を行う管理者の、脆弱性やセキュリティ対策に関する認識レベルには差がある。そのため、Web サイトを安全に運用するためには、開発者や管理者の能力に依存しないよう Web アプリケーションの開発ベンダの選定や、「予防保守」を含めた保守・運用の体制とルールの策定が重要である。

4.2 レベル設定について

(1) 想定される Web サイトモデル
Web サイトの役割、格納するデータの重要度によって、必要とされるセキュリティ対策は異なる。
本チェックシートでは、想定される Web サイトのモデルを以下の 4 段階に区別し、各 Web サイトに要求するセキュリティのレベルと、ソフトウェアベンダ要件について以下のように分類した。

	想定される Web サイトモデル	Web サイトの セキュリティレベル	ソフトウェアベンダ要件
レベル 4 （推奨）	EC サイト[9]等商取引を実行する Web サイト、企業の機密情報を取り扱う Web サイト	ハッキング[10]には非常に高度な知識が必要	実績の豊富なフレームワーク等を使用してセキュリティ対策を行っている。 専任の品質管理部門がセキュリティ監査を行っている
レベル 3 （標準）	個人情報、企業の重要情報を取り扱う Web サイト、Web サイトの管理者サイト	知識のある人がハッキング可能	セキュリティ開発ルールが定められ、ルールに従った開発・テストを実施している
レベル 2 （低）	インターネットに接続された Web サイト	知識の無い人が、ツールを入手すればハッキング可能	セキュリティを意識した開発が実施され、セキュリティに関するテストを実施している
レベル 1 （非推奨）	インターネットに未接続の Web サイト	知識の無い人も、方法が判ればツール無しでハッキング可能	セキュリティに関する対策を何も行っていない

表 7 事業モデルにおけるセキュリティ・可用性レベル設定（Web サイトモデル）

(2) 上位概念定義

[9] インターネット上で商品やサービスの販売を行っているサイト。
[10] 本来はシステムの解析などの意味。ここではクラッキング（他人のコンピュータへ不正に侵入する）の意味で、使用している。

本チェックシートの上位概念として、セキュリティ対策概要・脅威をまとめ、各項目について、その対策レベルを以下のとおり定義する。全体は、～情報システム・モデル取引・契約書～（パッケージ、SaaS/ASP 活用、保守、運用）＜追補版＞を参照されたい。

対策項目	リスクの詳細	参考情報			
		レベル1	レベル2	レベル3	レベル4
■認証 情報を参照している人が本人であることを証明する。	情報を参照している人が、本人であることを管理していないと、他人に重要な情報を見られる可能性がある。	**■何も決められていない** 情報を誰が参照しているか特定できない状態。	**■個人を認識できる** パスワードを利用して、個人を認識できるようにする。	**■本人認証の強化** 特定のカードやログインの二重化などで、本人認証を強化する。	**■絶対的な本人認証** 生体認証等を組み合わせ、定期的なポリシー変更を実施する。
■アクセス権 情報よって、アクセスできる人を制限・管理する。	誰でも情報アクセスできるようになっていると、削除、改ざん、複製、持ち出しされたりする。	**■何も決められていない** 情報に誰でもアクセスできてしまう。	**■利用者と管理者のアクセス権限の設定** 利用者がアクセスできる情報と、管理者だけがアクセスできる情報を区別し、管理する。ログを取得する。	**■グループ単位のアクセス権限の設定** 利用者が所属するグループごとにアクセスできる情報を区別し、管理する。ログを取得する。	**■アクセス権の集中管理機能を有する** 利用者・グループ毎のアクセス権限を管理する機能を使って、最新のアクセス権を維持することができる。ログを収集し、問題発生時に参照できる。
■暗号化 情報を暗号化して、紛失・盗聴・改ざんの対策をする。	通信経路やパスワードが暗号化されていない場合は、紛失・盗聴・改ざんや成りすましの可能性がある。	**■何も決められていない** 通信経路やシステムで保存するパスワードが暗号化されていない。	**■パスワードの暗号化を実装する** パスワードを暗号化し、容易に第三者にパスワードが漏えいしないようにする。	**■個人、決済等に関わる情報の暗号化を実装する** 個人情報、決済情報をすべて暗号化し、漏えい、改ざん、紛失しても悪用されないようにする。	**■全ての情報について高度な暗号化を実装する** あらゆる情報を暗号化し、第三者に悪用されないようにする。
■ページ間のデータ授受 Webのページをまたがってデータのやり取りをする際の対策をする。	ページ間のデータ授受が正しくなされない場合は、情報が漏えいしたり、成りすましされたりする可能性がある。	**■何も決められていない** ページ間のデータ授受について、何もルール化されていない。	**■データの取り扱いがルール化されている** データの有効期限や取り扱い方法が部分的にルール化されている。	**■データの取り扱いルールの強化** データの有効期限や取り扱い方法が規定されている。	**■ページ間でやり取りするデータの種類を規制する** 個人を特定できる情報、決済に関わる情報をページ間でやり取りをしないなどを規定する。
■悪意のあるコードの侵入阻止 悪意のあるコードがWebサーバに埋め込まれるのを阻止する。	悪意のあるコードがWebサーバ上で実行されると、フィッシング詐欺やユーザの成りすまし、パスワード漏えい等の可能性がある。	**■何も決められていない** 悪意のあるコードに対して、なにも対策がない。	**■悪意のあるコードの対策** 悪意のあるコードを排除する仕組みがある。必要最小限のアクセス権限設定をする。不要なファイルを公開しない。	**■悪意のあるコードの対策の強化** 悪意のあるコードを排除する仕組みがあり、対策方法、管理権限がシステム全体で規定されている。	**■Webアプリケーション以外の対策の併用** Webアプリケーション内の悪意のあるコード対策に併せて、WAF（Web Application Firewall）等を使用した対策を実施する。
■システム連携 他のシステムや他のアプリケーションとの連携を行う際に連携の仕組みを悪用されるのを阻止する。	連携の仕組みを悪用されると、フィッシング詐欺やユーザの成りすまし、パスワード漏えい等の可能性がある。	**■何も決められていない** 連携の仕組みを悪用されるのを阻止する対策がない。	**■システム連携悪用の対策** システム連携悪用を排除する仕組みがある。	**■システム連携悪用の対策の強化** システム連携悪用を排除する仕組みがあり、対策方法がシステム全体で規定されている。	**■Webアプリケーション以外の対策の併用** Webアプリケーション内のシステム連携悪用の対策に併せて、WAF等を使用した対策を実施する。
■Webサーバの設定 Webサーバの設定内容について、最適な設定がされているか。	Webサーバの設定が正しく設定されていない場合、サーバ攻撃に必要となるシステム情報が漏えいする。	**■何も決められていない** セキュリティ基準が決められていない。	**■セキュアな設定** Webサーバの設定が外部からの攻撃などを防ぐセキュリティを意識した設定になっている。	**■セキュアな設定の強化** Webサーバの設定がセキュリティを意識した設定になっており、設定内容が規定されている。	**■侵入検知** Webサーバの設定に対する侵入・攻撃の際に、検知し、管理者へ通知する
■内因的な情報漏えい 運用ミスなど内部側の原因で情報が漏えいする。	重要な情報が漏えいしたり、サーバ攻撃に必要となる情報が漏えいしたりする。	**■何も決められていない** Webサーバの運用について規定が何も設けられていない。	**■Webサーバの運用規約** 条件付でWebサーバの運用について規定が設定する。	**■Webサーバの運用規約を強化** 漏れなくWebサーバの運用について規定が設定されている。	**■情報表示の制限** 個人情報等の重要情報は、一覧表示を禁止する、一括してCSVファイル出力を禁止する、などを規定する。

表 8　Web サイト・アプリケーションにおけるセキュリティ・可用性 上位概念定義
（一部抜粋）

4.3　チェックシートの活用法について

(1)　チェックシート活用について
最初に、前項の表「3.2　(1)想定される Web サイトモデル」に従って、構築・運用の対象となる Web サイトが担う役割に従って基準となるレベルを設定する。ただし、あくまでも基準であり、チェックシートの全ての項目を基準レベルに設定する必要は無い。構築・運用計画として、常に上位のレベルを目標に設定したセキュリティ対策を組み入れ、PDCA サイクル[11] に基づく運用を実現することが重要である。

(2)　セキュリティ・可用性チェックシート（Web アプリケーション）
「3.2　(2)上位概念定義」の不明な点については、補足資料「セキュリティ・可用性チェックシート(詳細版）)」を確認すること。

(3)　チェックシートの活用ポイント
・　Web アプリケーションの脆弱性

[11]管理業務などを計画通りに実施する為の管理サイクル。PDCA は計画(Plan)、実施(Do)、評価（Check)、改善（Act）を表す。

チェックシートの「機密性保護」の「ユーザ認証」から「アプリケーションの欠陥」についてはWebアプリケーションの脆弱性について述べている。
これらの対策を怠ると「5.1　Web アプリケーションのセキュリティ対策の現状と課題」に示した問題が発生し社会的責任問題に発展し、ひいては会社存続の危機に陥る可能性があるので、対応レベルの相違はあっても、可能な限り対応する必要がある。

・　特に重要なチェック項目
Webアプリケーションの脆弱性について特に重要な項目について以下に述べる。

■SQL インジェクションとクロス・サイト・スクリプティング
IPA/ISEC（独立行政法人 情報処理推進機構 セキュリティセンター）によると、Web アプリケーションの脆弱性の内訳では、「SQL インジェクション 」と「クロス・サイト・スクリプティング 」の２つの脆弱性が全体の 60%以上を占める。[12]
このことから、「SQL インジェクション」を含む「他システム・アプリケーションとの連携」の「外部プログラムによる脆弱性」と「アプリケーション対策」の「第三者 Web サイトへの情報の送信」について優先的に対策を行う必要がある。これら最低限の対策すら出来ない開発業者への Web システムの発注は、他の Web 診断業者と連携を取るなど、慎重な対応が必要となる。

・　その他のチェック項目について
Web アプリケーションの脆弱性以外のチェック項目については、社内システムとほぼ同様のセキュリティ項目となるが、インターネットに直接接続されるという性質上、社内システムより１ランク上のセキュリティレベルを設定する必要がある。

・　WEF と電子証明書について
「WAF（web application firewall）の製品および対応業者の選定基準」、「電子署名の製品および対応業者の選定基準」については、次年度での本解説策定の課題とする。

5　【補足資料】

5.1　参考資料一覧

セキュリティ・可用性に関する参照ガイドライン一覧

•経済産業省：情報システムの信頼性向上に関する評価指標　（試行版：平成 19 年 4 月）
＜http://www.meti.go.jp/press/20070413003/20070413003.html ＞

• 経済産業省：情報セキュリティガバナンス研究会報告書　（平成 19 年３月）
<http://search.e-gov.go.jp/servlet/Public?CLASSNAME=Pcm1030&btnDownload=yes&hdnSeqno=0000025559 ＞

[12] http://www.ipa.go.jp/security/fy18/reports/contents/enterprise/html/614.html を参照

• 経済産業省：企業における情報セキュリティガバナンスのあり方に関する研究会（平成 17 年 3 月）
＜http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html ＞

• 経済産業省：個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（平成 16 年 10 月）

•IPA ：情報セキュリティ対策ベンチマーク
＜http://www.ipa.go.jp/security/benchmark/ ＞

•IPA ：セキュリティ要件の検討支援ツール
＜http://www.ipa.go.jp/security/fy18/development/localgov/lg_secstdy_top.html ＞

•「政府機関の情報セキュリティ対策のための統一基準」（2005 年 12 月版）
＜http://www.nisc.go.jp/active/general/kijun01.html ＞

• 総務省：次世代ＩＰインフラ研究会 第二次報告書
＜http://www.soumu.go.jp/s-news/2005/pdf/050707_2_2.pdf ＞

•IPA ：地方公共団体システム調達におけるセキュリティ要件の検討支援ツール
＜http://www.ipa.go.jp/security/fy18/development/localgov/lg_secstdy_top.html ＞

•IPA ：情報セキュリティ読本（2006 年 11 月 改訂版）
＜http://www.ipa.go.jp/security/awareness/management/management.html ＞

•IPA ：大企業・中堅企業の情報システムのセキュリティ対策～脅威と対策～

＜http://www.ipa.go.jp/security/fy18/reports/contents/enterprise/html/index.html＞

•IT セキュリティ評価及び認証制度（JISEC）
＜http://www.ipa.go.jp/security/jisec/index.html ＞

•JIPDEC 情報マネジメントシステム推進センター
＜http://www.isms.jipdec.jp/ ＞

•WASC ：Web Application Security Consortium
＜http://www.webappsec.org/ ＞

5.2 セキュリティ事故に従う被害額シミュレーション

(1) コンピュータウイルスによる被害額算出

独立行政法人 情報処理推進機構 セキュリティセンター（IPA/ISEC）の調査により、2003 年のコンピュータウイルスによる被害額の推計がおこなわれた。ウイルス被害額は、以下に挙げる金額の累積による、ウイルス被害算出モデルで算出されている。

表面化被害＝逸失利益＋システム復旧コスト
潜在化被害＝システム停止中の業務効率低下コスト＋復旧作業に関わる一般業務コスト
ウイルス被害額＝表面化被害＋潜在化被害

ウイルス被害額算出モデルに 115 事業所からのアンケート結果によるデータを基に算出された、事業所 1 社あたりの被害額は、約 28 万円となった。また、このサンプルに基づき推定された、2003 年 1 月～12 月の国内セキュリティインシデントの被害総額は、約 3,025 億円に達した。

なお、このウイルス被害額算出モデルには、各種補償や謝罪広告費、風評被害による利益源、等は含まれていないため、実質的なウイルス被害額はこれらを上回ることになる。

（出典：IPA/ISEC「国内・海外におけるコンピュータウイルス被害状況調査」）[13]

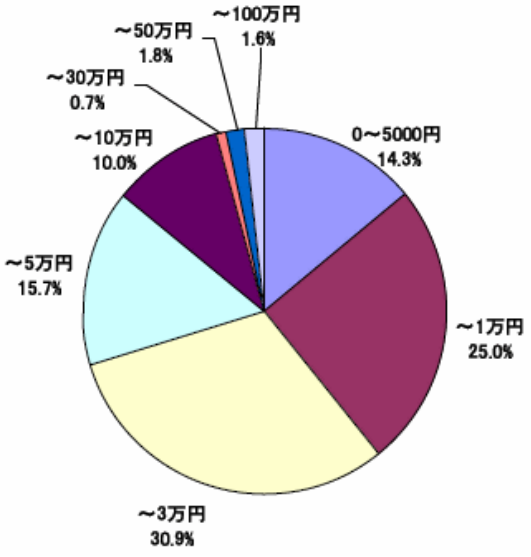
(2) 個人情報漏えいインシデントによる被害額算出

日本ネットワークセキュリティ協会（JNSA）の調査により、2006 年の個人情報漏えいインシデントに関する報告がおこなわれた。2006 年に発生した個人情報漏えいインシデント件数は 993 件で、個人情報が漏えいした合計人数は、約 2,224 万人に達する。この報告書では、「もし被害者全員が賠償請求したら」という仮定に基づく想定被害賠償額も算出されている。賠償額の計算には、以下の算出式が用いられている。

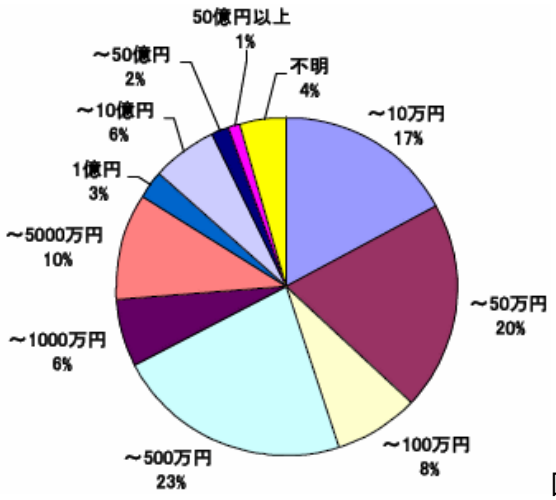
想定損害賠償額
＝漏えい個人情報価値×情報漏えい元組織の社会的責任度×事後対応評価

この算出式と、2006 年 1 年間に報道された個人情報漏えいインシデントに基づき計算された分布図が以下になる。

[13] http://www.ipa.go.jp/security/fy15/reports/virus-survey/index.html



図：一人当たりの想定損害賠償額



図：一件あたりの想定損害賠償総額

インシデント一件あたりの平均想定損害賠償額は 4 億 8,156 円であり、想定損害賠償総額は約 4,570 億円となった。
（出典：JNSA 「2006 年度 情報セキュリティインシデントに関する調査報告書[14]」）

[14] http://www.jnsa.org/result/2006/pol/insident/070720/

セキュリティガイドライン　ワーキンググループ委員名簿

【主査】
高田　和幸
トレンドマイクロ株式会社　コーポレートマーケティンググループ　シニアマネージャー

【委員】
脇坂　隆則
日立ソフトウェアエンジニアリング株式会社　ソリューション開発本部 セキュリティーソリューション部　部長

小野寺　匠
マイクロソフト株式会社　セキュリティレスポンスチーム　チームマネージャ

千葉　貴志
トレンドマイクロ株式会社　コーポレートマーケティンググループ　情報セキュリティマーケティング課マーケティングスペシャリスト

永来　真治
アップデートテクノロジー株式会社　取締役

中塚　勝
ソフトバンク・テクノロジー株式会社　情報セキュリティ推進室　マネージャー　情報セキュリティ教育責任者

奥天　陽司
マイクロソフト株式会社　チーフ　セキュリティ　アドバイザ、早稲田大学　非常勤講師

近藤　伸明
株式会社 神戸デジタル・ラボ　R&D システム部マネージャー

【事務局】
井上　星子　社団法人コンピュータソフトウェア協会　業務課　課長
鈴木　啓紹　社団法人コンピュータソフトウェア協会　業務課