文書番号：MOE10-業仕様-3003

平成１５年度
流通サプライチェーン全体最適化情報基盤整備事業
（業務連携支援システム基本設計）

基本設計書

「セキュリティ設計書」

平成 16 年 3 月

日本電気株式会社

改版履歴

日付	版数	改版内容
2004 年 03 月 31 日	初版	新規

基本設計書作成責任者
日本電気株式会社　：曽根田　雄一

検　印

目 次

1．本設計書の位置づけと対象範囲 1-1

2．システム環境のセキュリティ 2-1

2.1 セキュリティ対策方針の検討 2-1

2.1.1 対象システム 2-1

2.1.2 システムのセキュリティ環境 2-1

2.1.3 セキュリティ対策方針 2-6

2.2 ネットワーク接続環境 2-10

2.2.1 ネットワーク接続構成 2-10

2.2.2 ネットワークセキュリティの要件 2-10

2.2.3 各運用形態における必須要件 2-13

2.3 サーバ運用環境 2-15

2.3.1 施設・設備の要件 2-15

2.3.2 可用性要件 2-17

2.3.3 施設の運用管理の要件 2-17

2.3.4 各方式における必須要件 2-17

2.4 認証方法 2-19

2.4.1 認証方式の比較 2-19

2.4.2 アクセス制御の方法 2-20

2.4.3 利用者認証の要件 2-21

2.4.4 アクセス制御の要件 2-22

2.4.5 システム間認証の要件 2-22

2.4.6 検討事項 2-23

2.4.7 各方式における必須要件 2-24

2.5 取引情報の安全性・信頼性検討 2-25

2.5.1 対象となる情報 2-25

2.5.2 取引情報の安全性・信頼性に関する要件 2-25

2.5.3 暗号化通信が必要な経路及び暗号化通信の方法 2-26

2.5.4 データの暗号化 2-26

2.5.5 各方式における必須要件 2-27

3．運用におけるセキュリティ 3-1

3.1 運用規定の要件 3-1

3.2 本システムで準備すべき運用規定及び記述すべき内容 3-3

3.2.1 情報資産の分類及び管理 3-3

３.２.２ 人的セキュリティ ３-４
３.２.３ 物理的及び環境的セキュリティ ３-５
３.２.４ 通信及び運用管理 ３-７
３.２.５ アクセス制御 ３-９
３.２.６ システムの開発及びメンテナンス ３-１２
３.２.７ 事業継続管理 ３-１４

４. 監査 ４-１
４.１ 監査の概要 ４-１
４.２ 監査基準 ４-２
４.３ 監査項目 ４-３

１．本設計書の位置づけと対象範囲

本設計書では、システムの基本的なセキュリティ方針を作成し、どのような脅威から何を守るか、そのためにはどのような体制及び設備を持つのかを明確にする。

本設計書の各章では、システム環境のセキュリティ、運用におけるセキュリティ、監査についてそれぞれ記述する。システム環境のセキュリティではネットワーク接続環境のセキュリティ、サーバ環境のセキュリティ、認証方法、取引情報の安全性・信頼性の各項目について記述する。

本システムは、３つの運用形態（大企業自社運用、中小企業自社運用、ASP 運用）での利用を想定しており、本設計書では、主に ASP 運用のセキュリティについて記述する。大企業自社運用及び中小企業自社運用に関するセキュリティについては、本設計書を参考として各企業の責任においてセキュリティ対策を行うものとする。

２．システム環境のセキュリティ

まず、検討の対象となるシステムを明確にし、セキュリティ環境（前提条件、保護対象資産及び想定される脅威）及びセキュリティ対策方針について検討する。

なお、セキュリティ環境及びセキュリティ対策方針の各検討項目は、ISO/IEC15408 に基づくセキュリティ設計仕様書（Security Target）で規定する項目を参照して列挙した。

2.1 セキュリティ対策方針の検討

2.1.1 対象システム

本システムは、以下の３つの形態での利用を想定している。

- 大企業自社運用（主に大手企業が自社システムと本システムを接続して利用する）
- 中小企業自社運用（主に中小企業が本システムを自社システムとして利用）
- ASP 運用（主に中小企業が ASP 業者の提供する本システムを利用する）

セキュリティ要件の対象は、ファイアウォール、ビジネスモジュールサーバなどの各種サーバ及びネットワーク機器を対象とする。また、インターネットを経由したビジネスモジュール間の通信経路も検討対象とする。

なお、利用者が本システムを利用する際に接続する独自の業務システム及びクライアント PC については、IPA（独立行政法人情報処理推進機構）の不正アクセス対策のページ（http://www.ipa.go.jp/security/fusei/ciadr.html）等で公開されている各種情報を参照し、個々の責任でセキュリティ対策が施されていることを前提とする。

2.1.2 システムのセキュリティ環境

（1） 前提条件

システムセキュリティ要件を検討する上での前提条件を以下に記述する。

① システムの利用環境

- 取引主体は、製造業、卸売業、小売業である。
- 大手企業は、本システムを自ら所有し、自社のシステムと直接接続して利用する。
- 中小企業は、本システムを自社システムとして利用する。または、ASP 業者などが提供する本システムをインターネット経由で利用する。
- システムは、販売側・購入側の２つの機能を持ち、通常は片方の機能で稼動する。
- ASP 業者を考慮し、販売側・購入側の双方の機能搭載も可とする。

② 物理環境

- 各種サーバ及びネットワーク機器は、物理的に不正侵入できないように制御された場所に設置される。
- 施設内外の回線は十分に信頼性があるものとする（回線の信頼性については、「運用条件書・運用設計書」に記載）。
- 各種サーバ、ネットワーク機器等は十分に信頼性があるものを使用する（「運用条件書・運用設計書」に記載）。

③ ネットワークへの接続条件

- 本システムでは、インターネットとの境界にファイアウォールを設置する。
- 本システムを自社システムとして利用し社内 LAN と接続する場合、本システムと社内 LAN はファイアフォール等で分離するものとし、社内 LAN からも認証された利用者のみアクセス可能とする。

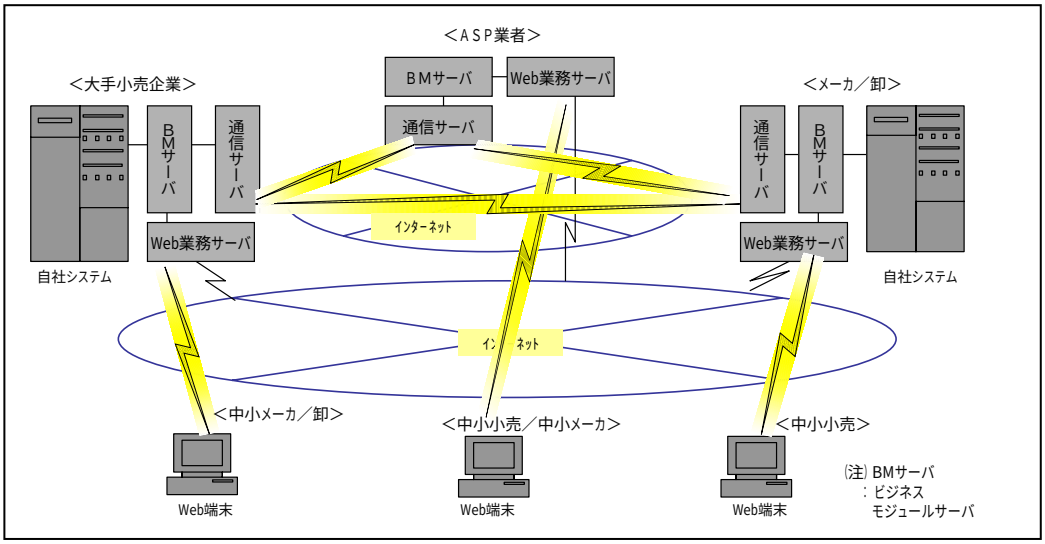

図２．１　ネットワーク接続の概要

④ 人的条件

・ システムの利用者は製造業、卸売業、小売業の関係者であり、不特定多数の利用者を対象としない。

（２） 保護対象資産及び想定される脅威

本システムにおける保護対象となる情報資産を表２．１に規定する。

表 ２．１　保護対象資産

No.	資　　産	概　　要
1	業務データ	ビジネスプロセス情報 （商品マスタ情報／発注データ／入荷予定データ／検品受領データ／請求データ／支払案内データ／POS 売上データ／在庫情報） 取引履歴

No.	資　　産	概　　要
2	業務ログ	システムの利用履歴 ・利用者履歴（利用者 ID、利用時間等、有効／無効ログイン等） ・アクセス履歴（利用者 ID、利用機能、利用情報、データ追加／更新／削除等） ・エラーログ（利用者 ID、利用機能、エラー内容等）
3	バックアップデータ	業務データのバックアップ媒体
4	パスワード	業務アプリケーションのパスワード ＯＳ／ネットワーク機器のパスワード アプリケーション（データベース、ファイアウォール等）のパスワード
5	設定情報	システムを構成するハードウェア及びソフトウェアの設定情報
6	監査ログ	監査用に記録するログ（業務ログ以外のＯＳやアプリケーションが記録するログのうち、監査対象とするログ）
7	電子証明書・私有鍵	実在が確認され、信頼できる運営がされているサイト向けに発行されるサーバ証明書及び暗号通信や電子署名に利用する私有鍵。 ※クライアント認証を実装する場合は、個人向けに発行されるクライアント証明書も対象となる。
8	設計書、マニュアル	電子ファイル及び紙に印刷したもの
9	帳票	業務で使用する帳票の電子ファイル及び紙に印刷したもの

本書では、システムにおいて保護対象となる上記情報資産に対する人為的な脅威を対象として検討する。

以下に、表２．１で規定した保護対象資産に対して想定される人為的な脅威とその概要を示す。

表２．２　想定される脅威と概要

No.	想定脅威	概　　要	対策
1	サービス妨害	第三者がシステムで稼動するサービスに対して妨害を行い、サービスの利用を困難にする。	アクセス制御 不正侵入対策
2	盗聴	第三者が回線上（インターネット回線）を流れる情報を盗聴する。または、データベースの保存されたデータを盗聴する。	通信路の暗号化 データの暗号化
3	改ざん	第三者が回線上（インターネット回線）を流れる情報またはサーバ（データベース）上にある情報に直接アクセスし、業務データ等を改ざんする。	識別・認証・認可 アクセス制御
4	なりすまし	正当な利用者になりすましてシステムを利用し、業務データ等を参照、改ざん、破壊する。	識別・認証・認可 アクセス制御
5	ウイルス、不正プログラム	送受信データ等によりウイルスに感染、または、不正プログラムが実行される。	ウイルス対策
6	不正利用	利用者が許可されていない操作を行い、業務データ等を参照、改ざん、破壊する。	アクセス制御 不正侵入対策
7	事実否認	正当な利用者が発注等の事実を否認することで、取引の無効を主張する。	電子署名 監査（監査ログ） 業務ログ

本システムで最も重要な情報は、業務データである。本書では、業務データに直接関与する改ざん、なりすまし、事実否認の各脅威を重視して対策を行う。

2.1.3 セキュリティ対策方針

前節での検討内容を踏まえ、本システムのセキュリティ対策方針を以下に規定する。

（1） 識別・認証・認可

本システムでは、利用者がシステムを使用する前には識別・認証・認可される。

また、管理主体の異なるシステム同士を接続する場合は、システム同士が相互に認証する。

識別・認証・認可されない利用者、及び、相互認証されないシステムは本システムを利用することはできない。

（2） アクセス制御

① 利用者権限

権限のある利用者のみが、本システム及びそのリソースにアクセスできる。権限には参照、追加・更新、無効、実行の 4 種類を準備し、利用者権限付与担当者が各利用者に権限を付与する。

② ファイアウォール

本システムでは、インターネットの出入り口にファイアウォールを設置し、使用するポート以外へのアクセスは全て遮断する。

（3） 不正侵入対策

不正侵入については、本システムでは、以下の２つの対策を講じる。

① 不正侵入監視サーバの導入

ネットワーク監視タイプの不正侵入監視サーバを設置し、ネットワークへの攻撃を監視する。

② クロスサイト・スクリプティング脆弱性対策

クロスサイト・スクリプティング脆弱性は、Web ページとして動的に HTML や XML 等のマークアップ言語のソースを生成する仕組みを設けている場合に問題となるセキュリティホールである。利用するアプリケーションとして、クロスサイト・スクリプティング脆弱性対策のなされているものを選定する。

（4） 通信路の暗号化

本システムでは、インターネットを経由する通信路を暗号化する。なお、電子メールを利用し、メッセージを暗号化せずに送受信する場合は、業務データ等の重要な情報はメッセージに含ませないものとする。

（5） データの暗号化

本システムの利用形態のうち、特に ASP 運用については、契約や取引関連データの暗号化についても検討する必要がある。データ暗号化の導入により、取引の関係者のみ暗号化されたデータを復号化して参照可能となる。

（6） 電子署名

電子的な契約においては、契約相手の確認、契約情報改ざんの有無の確認等が必要になる。従来より日本では、押印による契約書の取り交わしが行われてきた。これらを電子的に成立させるための基盤となるのが、2001 年 4 月 1 日に施行された電子署名法（電子署名及び認証業務に関する法律）である。電子署名法では、所定の条件のもと、電子署名の施された電磁的記録は、押印された文書同様、真正に成立したものとしてみなされる。電子署名の概要については以下のとおり。

電子署名法では、電子署名とは、電子計算機によって施される電磁的記録であって、その結果がその記録を行った者を特定し、かつ、それが改変されていないことを確認できるものであるものをいう。これを実現するための基盤として、最も広く利用されているものが、公開鍵基盤（PKI: Public Key Infrastructure）である。公開鍵基盤では、電子署名は、公開鍵暗号系を利用し、記録を行った者が秘密裏に所有する情報（私有鍵）を用いて計算される。電子署名から、私有鍵を計算することは莫大な計算量が必要であるため、現実的な時間では困難である。電子署名は、私有鍵と一対になった情報（公開鍵）と共に定められた演算を施すことにより、それが改変されていないこと

を確認できる。記録を行う者が私有鍵を保有していることを示す情報として電子証明書が利用される。電子証明書には、公開鍵及び記録を行う者を特定する情報が記載されている。

本システムにおいて、電子的な取引（発注、請求など）の真正性を主張するためには取引データに対して電子署名を施すことが有効である。署名されたデータはデータベースに保存され、署名の有効性の検証や改ざんを検出できる仕組みが提供される必要がある。

本システムでは、重要な取引データに対しては、電子署名を施すことを推奨する。

（7） 暗号アルゴリズム

本システムで利用する公開鍵暗号アルゴリズムは、以下の理由から、1024 ビット RSA 方式を標準とする。

- 電子署名に利用する暗号アルゴリズムは、「電子署名及び認証業務に関する法律施行規則」の第二条で電子署名の安全性を確保するために利用すべき方式として規定されているが、最も実績があるものは、RSA 公開暗号鍵方式（1024 ビット）である。
- 暗号化に用いる公開鍵暗号アルゴリズムで、最も普及している。
- 通信路暗号化アルゴリズムの公開鍵暗号アルゴリズムとして、最も普及している。

（8） 電子証明書

本システムで利用する電子証明書は、最も実績のある、X.509 形式（RFC3280 にて規定）とする。

（9） ウイルス対策

本システムでは、システムで利用するメールのウイルスチェックを行う。また、ウイルス定義ファイルは最新のものに更新するものとする。

（１０） 環境・設備

本システムを ASP 運用で利用する場合は、物理的に不正侵入できないように制御され、かつ、停電・漏水等の対策も十分に施された区画に設置される。

システムの設置された区画への入退室はＩＣカード等で権限がコントロールされる。また、施設内の機器間の回線の信頼性は十分でなければならない。

（１１） 運用管理

業務上必要な各種情報は、その重要度に応じて適切に保護されなければならない。流通サプライチェーンという本システムを利用したサービスの安定的な供給を目的とするために、これらの本システムの運用上発生し得るリスクを防止するための対策として、情報セキュリティの３要素である機密性、完全性及び可用性を考慮した運用規定を定める。

（１２） 監査

本システムは、セキュリティ維持のために必要な項目を監査記録として保管する。

（１３） 業務ログ

本システムは、取引の正当性の裏づけとなる業務ログを記録・保管する。

2.2 ネットワーク接続環境

2.2.1 ネットワーク接続構成

本システムのネットワークの接続構成例を図２．２に示す。

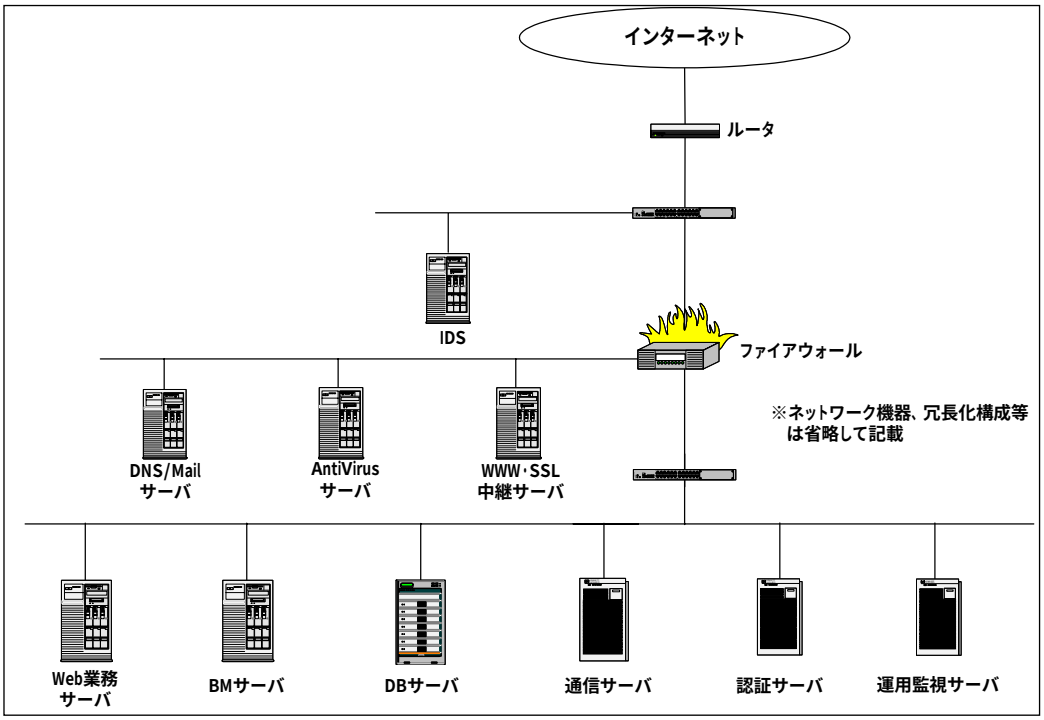

図２．２　ネットワーク構成例

2.2.2 ネットワークセキュリティの要件

ネットワークを介して第三者の不正行為からシステムを守るためのネットワークセキュリティの各対策の要件を以下に記述する。

（1） 共通

① 全般

・ 各種サーバの OS に対し、不要なサービスを停止する等のセキュリティ設定を施す。

② パスワード

各種サーバのＯＳ及びネットワーク機器の管理者用のパスワードは、原則として下記要件を満たすものを使用する。

・ ８文字以上の大・小文字の英字、数字、及び、特殊文字から構成される（１０文字以上を推奨するが、現行のネットワーク機器のスペックを考慮し、８文字以上とした）。
・ 辞書攻撃を避けるため、辞書にあるような文字列を利用することは避け、推測困難なものを使用する。

また、不要なユーザを削除し、必要なユーザのパスワードは上記要件を満たすものを使用する。また、パスワードは定期的に更新する。

③ 脆弱性の排除

各種サーバのＯＳやアプリケーション、ネットワーク機器のファームウェアについて、本システムのサービスに関わるセキュリティ上の問題が修正されたパッチがリリースされた場合、検討の上、原則として速やかに適用する。

（２） ファイアウォール

ファイアウォールは、第三者の内部ネットワークへの侵入を防ぐための仕組みであり、本システムの入り口となる。ファイアウォールの要件を以下に示す。

・ 使用するポート以外へインターネット側及び内部ネットワーク側からのアクセスは全て遮断すること。
・ 使用するポートへのアクセスであっても、不正なアクセスの場合も考えられるため、ファイアウォールを通過するパケットのデータを読み取り、内容を判断して動的にポートを開閉する機能（ステートフルインスペクション）を備えること。

（３） ウイルス対策

ウイルス対策の要件を以下に示す。

・ 多くのウイルスは Windows をターゲットとしており、いわゆるオープン系の OS をターゲットとしたウイルスは非常に少ない。リスクを低減するために、各種サーバのＯＳはオープン系のものを推奨する。

・ 電子メールについてウイルスをチェックする。
・ 最新のウイルスを検出するにはウイルスを定義しているパターンファイルを速やかに更新する必要がある。パターンファイルは、自動更新できることとする。

ウイルス対策については、本システムの一部としてウイルス対策サーバを導入する場合と、利用施設のサービスを利用する場合が考えられる。本設計書では、これらのいずれを選択しても良いものとする。

また、本設計書の範囲外であるが、クライアント側のウイルス対策は、必須項目とする。

（4） 不正侵入対策

不正侵入監視は、ネットワーク監視タイプとサーバ監視タイプの 2 種類があり、その概要は以下のとおりである。

① ネットワーク監視

一般に、個別のマシンを準備して、監視したいセグメントに配置する。ネットワーク監視タイプは、ネットワークパケットを監視して、ネットワークへの攻撃を示すイベントを探す。ネットワーク監視タイプは、配置されているセグメント上のすべてのトラフィックを監視し、不正アクセスの可能性がある場合は警告通知する。

② サーバ監視

サーバに直接導入し、ログファイル、保護されたコンピュータ間のネットワークトラフィックを監視する。監視中に、不正、または、注意を要する行動を示す兆候を発見した場合は、警告通知する。サーバ監視タイプは、不審なトラフィックがオペレーティング システムに到達するのを阻止することができる。

本システムでは、監視対象がそのマシンのみに限定されるサーバ監視タイプは採用せず、ネットワークセグメント上の複数のマシンへの攻撃を監視することができるネットワーク監視タイプを導入する。

不正侵入監視についても、本システムの一部としてサーバを導入する場合と、利用施設のサービスを利用する場合が考えられるが、本設計書では、これらのいずれを選択しても良いものとする。

また、クロスサイト・スクリプティング脆弱性対策として、Web 業務サーバや、BM サーバ、通信サーバにて利用するアプリケーションソフトウェアについては、クロスサイト・スクリプティング脆弱性対策が講じられているものを使用する。

2.2.3 各運用形態における必須要件

大企業自社運用、中小企業自社運用、ASP 運用のそれぞれに対し、以下を考慮し、ネットワーク接続環境の必須要件を決定する。

- ASP 運用では、サービス利用者の重要なデータを取扱うことに対し、責任を負う必要がある。データ漏洩に対し細心の注意を払うと共に、システムダウンが本システム全体に与える影響の重大さを考慮し、十分なセキュリティ対策を講じなければならない。
- 大企業自社運用では、自社のシステムダウンが本システム全体に与える影響の重大さを考慮したセキュリティ対策を講じなければならない。
- 中小企業自社運用では、自社のシステムダウンが本システム全体に与える影響度はそれほど大きくなく、自社システムにかけることのできるコストが少ないことを考慮し、必要なセキュリティ対策を講じなければならない。

表２．３に、各運用形態におけるネットワーク接続環境の必須要件を示す。

表２．３　ネットワーク接続環境の要件

項目			大企業	中小企業	ASP
全般					
	ＯＳのセキュリティ設定		○	○	○
	パスワード対策		○	○	○
	脆弱性の排除（パッチの適用）		○	○	○
ファイアウォール					
	使用するポート以外へのアクセス禁止		○	○	○
	ステートフルインスペクションの採用		△	△	○
ウイルス対策					
	ウイルス対策ゲートウェイの導入		○	△	○
		電子メールのチェック	○	△	○
		ウイルス定義ファイルの自動更新	○	△	○
	クライアントでのウイルス対策		○	○	○
不正侵入対策					
	ネットワーク監視		○	△	○
	クロスサイト・スクリプティング脆弱性対策		○	○	○

※表内説明　○：必須、△：任意、－：対象外

2.3 サーバ運用環境

システムを運用するサーバの安全性を維持するために、サーバが設置される施設、設備面における環境、冗長化構成、入退出のあり方など運用環境について検討する。

2.3.1 施設・設備の要件

施設、設備の要件について以下に記述する。各項目は、「ISMS 認証基準」（ISMS：Information Security Management System）の「物理的及び環境的セキュリティ」を参照し、施設、設備に関する項目を抽出している。

（1） 空調設備

- ハウジングスペースの空調機を二重化
- 漏水のおそれのある場所には漏水検知器等を設置
- 耐火性に優れた配管、ダクト類の使用
- 外気取入口及び排気口は、雨が侵入しない構造

（2） 防火対策

- 建築基準法に規定する耐火性能
- 自動火災報知設備及び消火器の設置
- 24 時間有人対応
- 防火区分されたフロア設計
- 建物、内装等には、不燃材料の使用

（3） 防犯対策

- 機械警備システムの導入
- 24 時間有人対応
- 入退出記録
- 監視カメラ録画画像の保管
- 金属探知機

（4） 電気設備

- 変電所より 2 系統の別ルートで受電（自動切り替え式）
- 自家発電機の設置
- CVCF（Constant-Voltage Constant-Frequency）の並列構成
- 法定年次点検時も無停電対応

（5） 通信設備

- 複数ルート化
- MDF（Main Distributing Frame）入退出は中央設備監視室により常時監視
- ネットワーク回線の冗長化構成

（6） 建物、その他

- 建築基準法に規定する耐震構造
- 24 時間 365 日体制
- 緊急時の迅速な対応

なお、各要件と「ISMS 認証基準」の「物理的及び環境的セキュリティ」の管理策との対応を以下に示す。

表2．4　要件と管理策との対応

管理策		要件
セキュリティが保たれた領域		―
	物理的セキュリティ境界	⑥建物、その他
	物理的入退出管理策	③防犯対策
	オフィス、部屋及び施設のセキュリティ	③防犯対策 ⑥建物、その他
装置のセキュリティ		―
	装置の設置及び保護	①空調設備 ②防火対策
	電源	④電気設備
	ケーブルの配線のセキュリティ	⑤通信設備

2.3.2 可用性要件

本システムでは可用性の向上を実現するために、重要性の高いサーバについては冗長化構成とする。冗長化構成の形態としては、クラスタ構成とパラレル構成などがある。

各サーバの冗長化構成については、「運用条件書・運用設計書」に記載。

2.3.3 施設の運用管理の要件

施設への入退出は、入退出記録をとり、IC カード等でコントロールされている。

詳細は、「3．運用におけるセキュリティ」を参照のこと。

2.3.4 各方式における必須要件

大企業自社運用、中小企業自社運用、ASP 運用のそれぞれにおける施設・設備等の要件を以下に示す。

表2．5　施設・設備等の要件

項目			大企業	中小企業	ASP
施設・設備要件					
	空調設備：	空調機の二重化	△	△	○
		漏水検知器等を設置	○	△	○
		耐火性の配管、ダクト類	○	△	○
		外気取入口及び排気口雨防止	○	△	○
	防火対策：	建築基準法に規定する耐火性能	○	○	○
		自動火災報知設備及び消火器	○	○	○
		24 時間有人対応	△	△	○
		防火区分されたフロア設計	△	△	○
		建物、内装の不燃材料使用	○	△	○
	防犯対策：	機械警備システムの導入	○	△	○
		24 時間有人対応	△	△	○
		入退出記録	○	○	○
		監視カメラ録画画像の保管	○	△	○
		金属探知機	△	△	△

項目			大企業	中小企業	ASP
	電気設備：	変電所より 2 系統で受電	△	△	△
		自家発電機の設置	△	△	○
		UPS の設置	○	○	―
		CVCF の並列構成	△	△	○
		法定年次点検時も無停電対応	△	△	○
	通信設備：	複数ルート化	△	△	○
		MDF 入退出は常時監視	△	△	○
		ネットワーク回線の冗長化構成	○	△	○
	建物、その他：	耐震構造	○	△	○
		24 時間 365 日体制	△	△	○
		緊急時の迅速な対応	○	○	○
可用性要件：「運用条件書・運用設計書」参照					
施設の運用管理の要件					
	入退出記録		○	○	○
	IC カード等による入退出制御		○	△	○

※表内説明　○：必須、△：任意、－：対象外

2.4 認証方法

本節では、システム利用者の確認をするための認証方法について電子証明書の活用など認証の最適化について検討する。また、システムや情報へのアクセス制御の方法について検討する。

2.4.1 認証方式の比較

本システムでは、システムを使用する前に、利用者を認証する。また、管理主体の異なるシステム同士を接続する場合は、システム同士が相互に認証する。認証されない利用者、及び、相互認証されないシステムは本システムを利用することはできない。認証には各種方式があるが、ここではID／パスワード、バイオメトリックス、電子証明書の利用について、それぞれのメリット／デメリットを以下に示す。

表2．6　ユーザ認証方式の比較

方式		説　　明	メリット／デメリット
ID/パスワード		文字列情報の保有確認による認証方式。最も多く使われている認証方法のひとつ。セキュリティを維持するには、パスワードの定期的な更新が必要。	一般に第三者に漏洩しやすいと言われているため、安全性は低い。運用は容易でコストは最も低い。
電子証明書の利用	私有鍵の保存先：ハードディスク	電子証明書に記載された情報と一対になった秘密情報（私有鍵）の保有確認による認証方式。 セキュリティ維持のため、ハードディスクに保存された私有鍵はパスワードで保護されている必要がある。	私有鍵の複製は可能であるが、不正使用するためには、私有鍵の入手及びパスワードの特定が必要となるため、安全性は比較的高い。
	私有鍵の保存先：ICカード	電子証明書に記載された情報と一対になった秘密情報（私有鍵）の保有確認による認証方式。 IC カードに保存された私有鍵を利用するには、一般に PIN: Personal Identification Number が必要。	私有鍵の複製は困難であるため、不正使用するためには、一般に IC カードの入手及びパスワードの特定が必要となるため、安全性は高い。クライアント側に IC カードリーダが必要となる。

方式		説　明	メリット／デメリット
電子証明書の利用	私有鍵の保存先：サーバ	電子証明書に記載された情報と一対になった秘密情報（私有鍵）の保有確認による認証方式。 利用時のみ、サーバに保存された私有鍵をクライアント側へダウンロードする方式。私有鍵はパスワードにて暗号化されている。利用後は、私有鍵は自動的に消去される。私有鍵を利用するにはパスワードが必要となる。	私有鍵は、利用時のみサーバよりダウンロードし、利用後は自動的に消去されるため、複製は困難である。私有鍵は暗号化され、サーバにて厳重に管理されているため、安全性は高い。また、クライアントでの利便性は高い。
	私有鍵の保存先：専用装置(HSM)	電子証明書に記載された情報と一対になった秘密情報（私有鍵）の保有確認による認証方式。 私有鍵は専用の装置内に保管され、利用するにはパスワードが必要となる。一般に、サーバの私有鍵を保管するために利用する。	私有鍵を不正に利用するには、専用装置ごと入手が必要となる。安全性は非常に高い。
バイオメトリックス		利用者の身体的または行動的な特徴を利用。	紛失の恐れはないが、認識率の問題で本人を認識できない場合がある。一般に、クライアント側に専用のデバイスを準備する必要がある。

本システムでは利用者の認証には、ID／パスワード、または、電子証明書の利用を検討する。また、管理主体の異なるシステム同士を接続する場合は、電子証明書を利用したシステム同士の相互認証を必須とし、私有鍵の保管にはHSM（Hardware Security Module）を利用することを推奨する。

2.4.2 アクセス制御の方法

本システムのアクセス制御について、利用者、または、利用者グループ毎にアクセス権を設定する。また、特定のサーバについては、アクセスできるサーバを限定する。さらに、入力、参照、変更、削除等の権限を設定し、必要な情報のみアクセスできるようにする。

（1） ネットワークアクセス制御

利用施設内の業務システムを保護するために、ファイアウォールに一定のルールを設定し、許可された通信のみアクセス可能とする。

（2） 機器レベルアクセス制御

各サーバでは、OS レベルで、管理者用及び必要な権限を持ったユーザに対してパスワードを設定し、アクセスを制限する。

ネットワーク機器については、管理者用パスワードを設定し、アクセスを制限する。

（3） アプリケーションレベルアクセス制御

本システムにおけるアプリケーションレベルのアクセス管理は一元化して、権限に応じたアクセス制御を行う。

2.4.3 利用者認証の要件

システムの利用者を確認するための認証として、利用者は、ID／パスワードによる認証、若しくは、電子証明書を利用したクライアント認証のどちらかを利用可能なものとする。利用者認証の要件として、以下を挙げる。

（1） ＩＤ／パスワードによる認証

- 利用者に推測困難なパスワードを設定させること。
- システムはパスワード変更が可能な機能を提供すること。
- 認証時はパスワードが保護されない状態で伝送することがないように、ＳＳＬ通信にて通信路を暗号化すること。
- 離席時に正当な利用者になりすまし、不正に PC を利用されることを防止するため、セッション情報を管理し、一定時間アクセスしなかった場合、強制的にログアウトする。
- ログオン履歴を管理するとともに、ログオン時に前回ログオンの情報を利用者に提供することで、利用者自身以外のログオンの有無を利用者自身でチェックできる仕組みを検討する。

（2） 電子証明書を利用したクライアント認証

- 電子証明書に紐付けられた私有鍵の保存先は、PC のハードディスク、ＩＣカードまたはサーバを可能とする。
- セッション情報を管理し、一定時間アクセスしなかった場合、強制的にログアウトさせ、再度認証を行なわせる。
- 私有鍵の保存先がサーバである場合は、私有鍵の利用が終わった後は、クライアント端末上から私有鍵を消去する。
- 電子証明書の有効期間内にその証明書を利用して自動的に再発行の手続きを実行し、証明書を自動的に更新する仕組みの提供を検討する。

2.4.4 アクセス制御の要件

利用者個人またはグループに対し、以下のアクセス権限を設定できるものとする。

- 参照：業務データを参照できる権限
- 追加／更新：業務データを追加・更新できる権限
- 無効：業務データを無効にできる権限（データの削除は不可とする）
- 実行：機能単位での実行権限

また、アクセス制御の要件は、以下とする。

- 予め設定した利用者以外はシステムを利用できないこと。
- 権限のない利用者は、参照、追加・変更、無効、実行ができないこと。
- 権限の与えられた者のみが、利用者を登録し、利用者権限を付与することができること。
- システム管理者は管理情報以外の情報（業務データなど）の参照はできないこと。

2.4.5 システム間認証の要件

本システムでは、管理主体の異なるシステム同士を接続する場合は、電子証明書を利用したシステム同士の相互認証を必須とする。以下にシステム間認証の要件を示す。

・ 私有鍵の保管には HSM（Hardware Security Module）を利用することを推奨するが、サーバ内に保管する場合は、暗号化して管理するものとする。HSM の PIN（Personal Identification Number）や、暗号化に利用したパスワードは、権限者のみが利用できるよう、厳重に管理する。

・ 認証時、相互認証に利用する電子証明書の有効性（有効期限、失効情報）を確認すること。

・ その他細かな接続条件は、システム間にて事前に合意したものを利用するものとする。

2.4.6 検討事項

（1） 認証サーバ

本システムにおいて、利用者認証、システム間認証を一元管理する方法として、認証サーバの導入を検討する。

（2） 認証局

電子証明書を発行する認証局については、全国中小企業団体中央会が運営しているものが存在する。本設計書では、電子証明書を発行する認証局について限定することは避けるが、電子証明書は、既存のサービスであって、十分に信頼のおける認証局から発行されているものを利用可能であることとする。

2.4.7 各方式における必須要件

大企業自社運用、中小企業自社運用、ASP 運用のそれぞれにおける認証方法の要件を以下に示す。

表２．７　認証方法の要件

項目		大企業	中小企業	ASP
利用者認証				
	ＩＤ／パスワード認証	○	○	○
	電子証明書を利用したクライアント認証	△	△	△
利用者アクセス制御				
	アクセス制御機能の提供	○	○	○
	アクセス管理の一元化	△	△	○
システム間認証				
	相互認証	○	○	○
	HSM による私有鍵の保管	△	△	△

※表内説明　○：必須、△：任意、－：対象外

2.5 取引情報の安全性・信頼性検討

取引情報の安全性・信頼性を確保するために、取引相手の確認ならびに情報の改ざん検知が可能となる電子署名等の導入等について、システムにおける最適な方法を検討する。また、通信の機密性を保持するためにSSLなどの暗号化通信の方法について検討する。

なお、利用者が使用するクライアントＰＣについて、各クライアントＰＣで本システムの重要なデータの閲覧などが可能であり、そのセキュリティについては、ウイルス対策、パスワード管理、離席時のログオフなどを個々で十分に注意する必要がある。

2.5.1 対象となる情報

取引情報の安全性及び信頼性を検討する上で、対象となる情報は次のように分類できる。

（1） データ交換

商品データ／売上データなど

（2） 受発注情報

発注データ／受注回答データなど

（3） 物流情報

入荷予定データ／入荷結果データ／出荷予定データ／出荷結果データ／仕入れデータなど

（4） 決済情報

支払いデータ／支払い確定データ／請求データ／請求確定データなど

2.5.2 取引情報の安全性・信頼性に関する要件

取引情報の安全性及び信頼性について、以下に要件を規定する。

- 取引情報に電子署名できる機能を提供すること。
- 電子署名された取引情報データを検証し、改ざんの検知や、正当性を確認できる機能を提供すること。

・ 電子署名に使用される電子証明書は、既存のサービスであって、十分に信頼のおける認証局から発行されているものを利用可能であること。
・ 取引が成立した旨を通知する機能を提供すること。
・ 取引に関して論争が発生した場合に備え、取引内容に関するログを残し、参照できる機能を提供すること。

なお、電子署名方式については、W3C にて議論されている XML 署名とする。その他詳細な条件は、取引相手と事前に合意するものとする。

2.5.3 暗号化通信が必要な経路及び暗号化通信の方法

インターネットを経由する取引データは、サーバ間及びクライアント／サーバ間のいずれの場合もすべて暗号化して通信する。

暗号化通信の方法については、ID／パスワードで認証する場合は、SSL サーバ認証を組み合わせ、通信経路を暗号化する。

また、管理主体の異なるシステム同士を接続する場合は、システム同士が SSL 相互認証を行い、通信経路を暗号化する。

また、ファイアウォールの内側のサーバ間通信及びクライアント／サーバ間通信は、十分に保護されているため、暗号化通信を行わなくてもよいものとする。

2.5.4 データの暗号化

ＡＳＰ運用の場合は多くの企業の機密情報がデータベース内で管理されることになるため、データそのものの暗号化の検討が必要である。また、特定の企業は、セキュリティ確保のため、データの暗号化を要求する場合がある。

データ暗号方式については、特定のフィールド単位で暗号化が可能な、W3C にて議論されている XML 暗号とする。その他詳細な条件は、取引相手と事前に合意するものとする。

2.5.5 各方式における必須要件

大企業自社運用、中小企業自社運用、ASP 運用のそれぞれにおける取引情報の安全性・信頼性を確保するための必須要件を以下に示す。

表２．８　取引情報の安全性・信頼性を確保するための要件

項目		大企業	中小企業	ASP
取引情報の安全性・信頼性				
	XML 署名のサポート	○	△	○
	通知機能	○	○	○
	取引情報ログ生成／参照機能	○	○	○
暗号化通信		○	○	○
データ暗号化				
	XML 暗号のサポート	△	△	△

※表内説明　○：必須、△：任意、－：対象外

３．運用におけるセキュリティ

３.１ 運用規定の要件

業務上必要な各種情報は、その重要度に応じて適切に保護されなければならない。これらが適切に保護されていないことにより、情報の漏洩、不正確な情報、必要なときに必要な情報が使えない等、業務に支障をきたす場合がある。流通サプライチェーンという本システムを利用したサービスの安定的な供給を目的とするためには、これらの本システムの運用上発生し得るリスクを防止するための対策として、情報セキュリティの３要素である機密性、完全性及び可用性を考慮した運用規定を定め、実行することが重要である。

表 ３．１ 情報セキュリティの３要素

機密性	許可されたものだけが情報にアクセスできることを確実にすること
完全性	情報及び処理方法が、正確であること及び完全であることを保護すること
可用性	許可された者が、必要なときに情報及び関連する資産にアクセスできることを確実にすること

本章におけるセキュリティ要件は、財団法人日本情報処理開発協会が運用する「情報セキュリティマネジメントシステム(ISMS=Information Security Management System) 適合性評価制度」、及び経済産業省が定める「情報セキュリティ管理基準」を参照し、流通サプライチェーンにおいて必要となる運用要件を記述している。

本システムの利用形態は「大企業自社運用」、「中小企業自社運用」及び「ASP サービス利用」の３パターンを前提としているが、本章では第三者として企業や組織の重要な情報を取り扱う ASP 業者の実施するデータセンターサービスを対象としてセキュリティ要件を定めるものとする。ただし、自社でシステムを構築し運用する企業や、ASP サービスを利用する中小企業等の Web クライアントが本章の対象外となるわけではなく、各社の利用形態や取引する情報等の重要性を勘案したうえで、必要と思われるセキュリティ要件は定めるべきであり、本章を推奨条件として提示するものとする。

なお、各組織や企業等においてはすでに自社のセキュリティポリシが存在することが想定される。その存在により本章のセキュリティ要件と各社のセキュリティポリシとの整合性が確保されないことや矛盾が生じることは避けなければならない。従って、本章のセキュリティ要件には全社的なマネジメ

ントに関する要求は含めず、かつ、すでにセキュリティポリシを保有する各社に対しても適用可能となるように、本システムを利用しサービスを提供する主体に対する個別要件に汎用性をもたせた形で提示するものとする。

3.2 本システムで準備すべき運用規定及び記述すべき内容

3.2.1 情報資産の分類及び管理

取引先に関する情報や商品の受発注に関する情報等、組織の情報資産は適切に保護されなければならない。情報資産の管理不足は、自組織や取引先等の安全又は利益に損害を与えるおそれを招く要因のひとつであり、それらのリスクを軽減し情報資産を適切に保護するためには、適切な管理策を講じなければならない。

情報資産の管理策として、以下（1）、（2）の項目を挙げることができる。

（1） 情報資産に対する責任に関する規定

- 情報資産を管理する台帳を作成し、重要な情報資産をすべて登録すること。

（2） 情報の分類に関する規定

- 運用上の必要性や問題が生じた場合の影響度に応じた情報資産の分類基準を設けること。
- 情報資産を分類基準に従って分類し、管理者、保管場所、保管期間、廃棄方法等に関する取り扱い手順を定めること。

情報分類の例として、以下を挙げる。

表 3．2 情報分類産の例

情報資産	情報資産の区分	重要度
本システム上の磁気媒体 （電子的な取引記録等）	物理的資産	機密
業務マニュアル	情報資産	社外秘
公開文書	情報資産	一般

- 「機密」とは、特定の関係者のみに開示・提供可能な情報であり、その漏洩によってビジネスへの影響が深刻かつ重大なものをいう。
- 「社外秘」とは、組織内での開示・提供が可能なものであり、内容が漏洩した場合のビジネスへの影響は少ないものをいう。
- 「一般」とは、第三者に対して開示・提供可能なものをいう。

3.2.2 人的セキュリティ

人的セキュリティは、情報処理施設や設備に関する物理的セキュリティ及びネットワークに関する論理的なセキュリティを支えるための基となるものである。現実問題として、内部の人による不正操作やシステムの誤用によるセキュリティ事件、事故は後を絶たない。

運用要員による不正行為や、本システムの誤用等の人的セキュリティ不足によるリスクを軽減するための管理策として、以下（1）から（3）の項目を挙げることができる。

（1） 職務定義に関する規定

- 本システムを運用、管理する組織における役割及び責任を明確にすること。
- 運用要員として雇用する際、被雇用者に対してセキュリティに関する役割及び責任を明示すること。
- 運用要員の採用条件の一部として、被雇用者から機密保持に関する誓約書等への署名を得ること。

（2） 利用者の教育・訓練に関する規定

- 運用要員に対し、本システムを運用する上でのセキュリティ基準及び関連する手順に関する教育・訓練を定期的に実施すること。

（3） セキュリティ事故及び誤動作への対処に関する規定

- セキュリティ事件、事故及び誤動作は、適切な連絡経路を通して、できるだけ速やかに報告すること。
- 情報システムの利用者に対し、セキュリティ事件や事故に準ずる事象を発見した場合の報告を周知徹底すること。
- ソフトウェア等、情報システムが誤動作した場合の報告手順を定めること。
- 事件、事故や誤動作の種類や規模、事業への影響度の大きさ、復旧のための関連費用等を明確にすること。
- 組織の方針及び手順に違反した要員に対する、正式な懲戒手続を備えること。

3.2.3 物理的及び環境的セキュリティ

本システムを設置するデータセンター設備は、サービスを安定的に供給する上で、認可されていないアクセスや自然災害等による環境上の妨害から保護されなければならない。物理的及び環境的な脅威から保護するための管理策として、以下（1）から（3）の項目を挙げることができる。

（1） セキュリティ区画に関する規定

- 本システム及び本システムを設置する施設は、他の区画とは明確に分離し、セキュリティが保たれた領域に設置され、業務の重要度に応じた適切な保護策がなされること。
- セキュリティ区画は、認可されないものがアクセスできないように設備の重要度に応じた入退室管理策等のアクセスコントロールがなされること。
- セキュリティ区画は、火災、洪水、地震、その他の自然又は人為的災害による損害の可能性を考慮すること。
- セキュリティ区画において作業を行うために必要な手順や管理策を整備すること。

（2） 装置のセキュリティに関する規定

- 本システムの設置場所における環境上の脅威（窃盗、火災、水、ほこり等）を軽減するための措置を講ずること。
- 本システムを許可されないアクセスから保護すること。
- 本システムを、停電、その他電源異常から保護すること。
- データ伝送や情報サービスに使用する電源及び通信ケーブルの配線に対し、傍受や損傷等を防止するための措置を講ずること。
- 本システムを使用する際、装置の製造業者が提供する取扱説明書や手順書に従って保守を正しく実施し、装置の可用性及び完全性を確実に維持すること。
- 本システムを組織の敷地外で使用する際、管理者が承認する等の適切に保護するための手順を定めること。
- 本システムを処分あるいは再利用する際、システムに格納された情報を事前に消去すること。

（3） 一般管理策に関する規定

- 離席時は、机上その他の場所への重要な情報の放置を禁止すること。

・ 離席時には、パスワードの施されたスクリーンセーバの使用やログオフを徹底し、他人による本システムへのアクセスを防止するための措置を講ずること。
・ 組織が所有する情報資産を承認なしに組織外へ持ち出さないこと。

3.2.4 通信及び運用管理

セキュリティ事件、事故の発生を最小限にするために、本システムの正確、かつ、セキュリティを保った運用を確実に維持するために、あらゆる管理・運用の責任及び手順を確立しなければならない。

セキュリティ事件、事故を防止するために運用上の管理策として、以下（1）から（6）を挙げることができる。

（1） 運用手順及び責任に関する規定

- 本システムを利用する上で必要な操作手順は、文書化し維持していくこと。
- 手順に変更が発生する場合は、管理者の承認を得ること。
- システム又はセキュリティ障害発生を軽減するため、業務上使用する施設や設備の変更について管理すること。
- システム障害や不正行為の発覚等に対して、遅滞なく効果的な対処が行えるよう、事件・事故管理の責任及び手順を明確にすること。
- システムの故障や不正操作等の運用上の問題を回避するために、本番環境及びテスト環境の役割を明確に定め、かつ施設の分離を行うこと。

（2） システム計画の策定及び受け入れに関する規定

- 本システムの処理能力及び記憶容量を十分に確保するため、容量や処理能力を監視し、将来に必要な容量や処理能力を予測すること。
- 情報システムの新規導入や変更する際の受け入れ基準を明確にすること。

（3） 不正ソフトウェアからの保護に関する規定

- コンピュータウィルスやネットワークワーム等の悪意のあるソフトウェアの侵入を防止し、検出するための対策を講じること。

（4） 情報システム管理に関する規定

- 重要な情報及びソフトウェアのバックアップを定期的に取得すること。
- 本システムの操作担当者による処理の履歴を記録すること。

（５） 媒体の取り扱い管理に関する規定

- 情報の誤用や不必要な開示等を防止するため、テープ、ディスク、カセット等の移動可能な電子的記憶媒体や書類等の適切な管理手続きを定めること。
- 不要になった媒体を処分する場合の、情報漏えいを防止するための措置を講ずること。

（６） 組織間における情報及びソフトウェアの交換に関する規定

- 取引先や協業相手等と情報を交換する場合は、必要に応じて情報交換の実施に関する正式な契約を締結すること。
- 移送を必要とする媒体を、許可されないアクセス、誤用及び改ざんから保護すること。
- 電子取引を行うに際して、詐欺行為、契約紛争、情報の許可されないアクセス及び改ざんを防止するための措置を講ずること。

3.2.5 アクセス制御

業務上の各種情報に対する機密性、完全性及び可用性を維持するためにアクセス制御の方針を明確に定め、実行する必要がある。例えば、契約先との間で製品の受発注に使用される本システムが誰にでも使用可能であり、操作に関する制限もなされていなかった場合、情報の改ざんや機密情報の漏洩等の脅威にさらされ、さらには自組織や取引先の安全又は利益等に損害が発生するリスクを抱えてしまっているということは明白である。

各種情報へのアクセスを制御するための管理策として、以下（1）から（7）の項目を挙げることができる。

（1） アクセス制御に関する業務上の要求事項に関する規定

- 情報へのアクセスは、業務上必要な範囲のみに制限されること。

（2） 利用者のアクセス管理に関する規定

- 複数の登録された利用者を持つ情報システムにおける、利用者の登録及び抹消手順を定めること。
- 特権（管理者権限等）の割り当て及び使用を制限し管理すること。
- 情報システムにおける利用者に対するパスワードの割り当ては、確立された管理手続に従い実施されること。
- 情報システムにおける利用者のアクセス権を定期的に見直すこと。

（3） 利用者の責任に関する規定

- パスワードを設定及び使用する際、情報セキュリティ上の問題を考慮すること。
- 装置を常時監視することが不可能な場合、当該装置を適切に保護するための措置を講ずること。

（4） ネットワークのアクセス制御に関する規定

- 明確に許可されたサービス以外のサービスへのアクセスを防止するための措置を講ずること。
- 本システムの利用者がコンピュータの各サービスにアクセスする場合のネットワークの経路を制御すること。

・ 本システムに対する遠隔地からのアクセスを許可する場合、ユーザ認証を行うこと。
・ 遠隔地のコンピュータに対するアクセスを許可する場合、接続の認証を行うこと。
・ 診断用の通信ポートへの許可されないアクセスを防止するための措置を講ずること。
・ 本システムに対する許可されないアクセスを防止するため、ネットワークを適切に分離すること。
・ 共有ネットワークへのアクセスを許可する場合、アクセス制御の方針を明確にし、可能な限り経路を制御すること。
・ ネットワークに関する外部のサービスを受ける場合、そのサービスに施されたセキュリティに関する情報を入手し、これを文書化すること。

（5） オペレーティングシステムのアクセス制御に関する規定

・ 接続が許可された特定の場所や携帯装置に対する認証を行うため、端末を自動的に識別する機能を備えること。
・ 情報サービスへのログオンプロセスを明確にすること。
・ 本システムの利用者は、個人専用のユーザ ID を有すること。
・ パスワードの管理システムは、情報システムユーザに有効なパスワードを設定させるための対話式の機能を備え、パスワードの内容や文字数、文字の種類、変更の頻度等を制限すること。
・ システム設定プログラムの使用を制限し管理すること。
・ 情報へのアクセスに際して、脅迫の対象となり得るユーザを保護するため、脅迫に対して警報を発信する機能を備えること。
・ 取扱いに慎重を要する情報システムに接続された端末が活動停止状態にある場合、その端末をシャットダウンすること。
・ リスクの高いアプリケーションシステムへの接続時間は、制限されること。

（6） アプリケーションシステムのアクセス制御に関する規定

・ アプリケーションシステムへのアクセスは、限られた権限者のみに制限されること。
・ 取扱いに慎重を要するシステムは、隔離した環境に設置されること。

（7） システムアクセス及びシステム使用の監視に関する規定

- 例外事項やその他のセキュリティ関連イベント等の監査ログを記録し、定められた期間において保存すること。
- 情報処理施設及び設備の使用を監視するための手順を定めること。
- 情報処理施設及び設備の監視活動の結果を定期的に検証すること。
- すべての重要なコンピュータにおいて時刻設定を同期化すること。

3.2.6 システムの開発及びメンテナンス

本システムに関する新たなる設計、変更及びその実施は、セキュリティ上極めて影響の大きなものである。システム開発に際してセキュリティ上の要求事項を分析し、関係者が認識し合意を得た上で本システムへの組み込みを確実にすべきである。

新たな設計や変更等におけるデータの消失や誤用等のリスクを軽減するための管理策として、以下（1）から（5）の項目を挙げることができる。

（1） システムのセキュリティ要求事項に関する規定

- 情報システムを新規導入あるいは変更する際、事業の要求事項に基づいたセキュリティ要件を明確にすること。

（2） アプリケーションシステムのセキュリティに関する規定

- アプリケーションシステムに入力されるデータが妥当なものであることを確認するための機能を整備すること。
- アプリケーションシステムで処理されたデータに対する改ざんを検出する機能を備えること。
- メッセージの完全性を保護する必要がある場合、メッセージが改ざんされていないことを確認する機能を備えること。
- アプリケーションシステムから出力されるデータが妥当なものであることを確認するための機能や手順を整備すること。

（3） 暗号による管理策に関する規定

情報を保護するために暗号技術を用いる場合は、以下の事項を考慮すること。

- 情報を保護するために暗号を用いる場合、リスクを考慮し、暗号使用ポリシ（私有鍵の管理方法、暗号アルゴリズム、鍵の長さ等）を定めること。
- 電子情報の真正性及び完全性を保護するため、電子署名を適用すること
- 取引に関わる紛争を解決するため、取引情報による取引事実の否認を防止するための措置を講ずること。
- 情報を保護するために暗号を用いる場合、関連する対策基準類や手順等に準拠し、適切に鍵管理を行うこと。

（4） システムファイルのセキュリティに関する規定

- 本システムを損なうリスクを最小限に抑えるため、稼動中の本システムへのアプリケーションソフトウェアの導入は適切に管理されること。
- コンピュータプログラムが破壊される危険性を軽減するために、プログラムソースライブラリへのアクセスを厳格に管理すること。

（5） 開発及びサポートプロセスにおけるセキュリティに関する規定

- 本システムの変更管理の手順を定め、変更を厳格に管理すること。
- ソフトウェアの購入、使用及び変更を厳格に管理すること。
- ソフトウェア開発をアウトソーシングする場合、リスクを考慮し、それに基づいた正式な契約を締結すること。

3.2.7 事業継続管理

事業活動の中断に対処するとともに、重大な障害又は災害の影響から業務手続を保護するための手続を定めることは、本システムを使用したサービスの可用性を維持する上で重要な要素である。業務を保護する手続には、予防管理策及び復旧管理策が含まれる。

業務を保護するための管理策として、以下の事項が挙げられる。

事業継続管理に関する規定

- 業務手続の中断を引き起こし得る事象を特定し、リスク分析に基づく戦略計画を立てること。
- 重要な業務に障害又は故障が発生した際に事業の運営を維持し、許容時間内に復旧させるための、必要な計画を立案すること。
- 事業継続計画を定期的に試験し見直すこと。

４．監査

４.１ 監査の概要

本設計書の本章でいう監査とは、主として情報セキュリティを確保するために行う監査またはチェック機能を指す。会計監査とは異なる意味で使用している。

本システムを監査する場合、２つの視点から監査のあり方を考えることができる。ひとつは、本システムの運用を中心とした見方（組織横断）であり、もうひとつはシステムを運用する単位ごと観点（組織単位）である。

前者は本システムを使用するもの全てを対象として、本システム全体に求められる規則などへの準拠性をチェックするものである。後者は、本システムを使用し、運用する会社・団体または個人（以下、「団体等」）ごとに監査を実施するという考え方であり、団体等は、既に存在する内部チェック機能の一環として、監査を実施することが可能である。

前者の場合、監査対象が広範囲にわたることや監査を受ける主体者の費用負担などの課題が存在する。後者の場合、団体等による監査のレベルに相違やシステム全体として機能していることが監査としてまとめられにくいという課題が存在する。

これらの課題を検討し、監査を有効かつ公正に実施するためには、監査コストの問題を含めて、本システムの運用を詳細に定めるフェーズで決定すべきであり、本設計書ではこれ以上詳細を検討することは避ける。

4.2 監査基準

（1） 本システムの監査基準

本システムの情報セキュリティを監査する場合、監査を実施するものが留意すべき基準（監査の基準）として、以下のものが存在する。

・ 平成１５年４月１日に運用を開始した情報セキュリティ監査制度の情報セキュリティ監査基準

（http://www.meti.go.jp/policy/netsecurity/audit.htm）

ただしこの基準は、情報セキュリティ監査制度の監査を実施するものが満たすべき基準であり、本システムを監査するものは参考にすべきであるが、これにとらわれる必要はない。

（2） 本システムの管理基準

本システムを監査する際に、ベースとして考えるべき基準（管理の基準）として、以下のものが存在する。

・ 平成１５年４月１日に運用を開始した情報セキュリティ監査制度の情報セキュリティ管理基準

（http://www.meti.go.jp/policy/netsecurity/audit.htm）

・ 昭和６０年1月（平成８年１月３０日（改正））に開始したシステム監査基準

（http://www.meti.go.jp/policy/netsecurity/systemauditG.htm）

ただし、前者の管理基準は、団体等における情報をセキュリティ管理の観点から網羅しているリスト（管理策）を含んでいるものであり、本システムを中心とした業務に特化した項目を含んでいるものではない。

また、本システムの使用する上で、管理策の一部は適用されないものが存在する可能性があるため、本システムの監査では、ベースである管理基準を追加および削除するなどの修正を行い、本システムに必要な管理を定め、それに対応する監査を実施することが望ましい。後者は対象である情報システムの企画、開発、運用及び保守業務並びに共通業務に関する項目を定めているが、業務に特化した項目を含んでいないために本システムの監査にあたり、項目などの検討が必要となる。

以下、本システムの運用の上で必要と考えられる監査項目を検討する。

4.3 監査項目

監査項目を検討する場合、次の観点からの議論が必要である。

- 業務に関わる環境（準拠すべき法令、監督官庁からの指導要領、業界団体のガイドラインなど）
- 国際標準または国内の基準（標準的な管理の基準）
- 業務を実施する企業または団体などの方針

このうち、2 番目に関しては、前節で記述しており、ここではこれ以上の詳細を記載しないが、ASP 事業者に関しては、本システムの信頼性を維持し、ASP 事業者からサービスを受けるユーザに一定レベルの情報セキュリティを確保していることを示すため、実施することを推奨する。3 番目に関しては、個別の団体等の問題であるため、ここでは検討の対象外とする。

業務に関わる環境（遵守すべき法令、監督官庁からの指導要領、業界団体のガイドラインなど）に関して、監査に関係すると思われる項目を検討する。なお、遵法性の検討、つまり法的な問題が存在しないことを詳細に検討することは、本設計書の範囲外であるため、最小限の検討に留める。

（1） 電子商取引の観点

一般に電子データにて取引を行う場合、取引の成立の定義、取引の証拠（ログ）の保管、障害時のデータロスなどによる損害の責任などを明確にする必要がある。

現行において参考となるのは、電子契約法である。電子契約法（電子消費者契約及び電子承諾通知に関する民法の特例に関する法律、平成 13 年 12 月 25 日施行）は、電子商取引などにおける消費者の操作ミスの救済、契約の成立時期の転換などを定めたものであるが、この法における契約成立の時期は BtoC だけでなく、BtoB においても遵守すべきであると考えられる（p3「電子消費者契約及び電子承諾通知に関する民法の特例に関する法律　逐条解説」経済産業省、平成 13 年 12 月）。

つまり電子契約において契約成立の解釈に関して、到達主義の原則が本システムの運用においても成り立つと推定される。データの授受だけでなく、商行為を実施する場合には、データの送受信の記録、データの可読性確認、取引内容の確認（確認画面などにより誤操作の防止）などを履歴として残し、取引成立時期の推定に必要なログが後日確認できるようにすることが重要であると推測される。

（２） 取引の当事者特定の観点

電子取引において、注文をしたものが本人であること、また権限を有するものであることを特定できる仕組みを持つことは非常に重要である。これらを電子データの中で表したものが電子署名であり、参照する法律としては電子署名法（電子署名及び認証業務に関する法律、平成 12 年 5 月 31 日施行）が存在する。

ただし、本システムの運用にあたってこの法律で定義されている認定認証事業者として、証明書発行に関する業務を行うか否かは、諸要素を勘案して決定するべきであり、別途議論するのが望ましい。電子署名をベースとしない本人特定に関しても、通常合理的に期待する安全性よりもセキュリティレベルが相当程度低い場合には、本人特定の効力が減じられる可能性があるため、ID・パスワードによる本人特定の運用に関しても、相応の注意を払い、適切な管理を実施していることを後日確認できるようにすることが重要である（電子商取引等に関する準則、平成 15 年 6 月 13 日、経済産業省）。

今後、証明書をベースとした認証方法が信頼性を確保するために主流となると推測されるが、電子署名により本人であることを特定する時、その署名をした鍵（公開鍵方式における私有鍵を指す）を本人のみが所有していること、その鍵を使用するものは署名する権限を有するものであることなどに合理的な根拠がなければならない。

署名に使用する鍵の一意性やその鍵が本人であることを証明することに関して、合理的な範囲で適正に運用していることを示し、また証明書発行の関するログや記録を保護しておくことが必要であると想定される。

（３） 電子帳簿の保管の観点

本システムを自社の会計システムや戦略システムなどと連動させる場合のみならず、電子取引（EDI：Electronic Data Interchange）を行う場合、電子帳簿保存法（電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律（平成１０年法律第２５号）平成 10 年 7 月 1 日施行）の要件に注意を払う必要がある。

団体等がこの法律の適用を申請しない場合においても、団体等が所得税法及び法人税法で原始記録の保存が義務付けられている場合、電子取引の原始記録を保存する義務が生じる。

例えば、取引に関して受領し、または交付する注文書、契約書、領収書等に通常記載される事項を対象として、取引記録を保存する義務がある。ただし、その取引情報のやり取りの過程と全て残す必要はなく、最終的な確定情報のみを保存すればよいこととされている。

なお、団体等が電子帳簿保存法への適用申請を行う場合には、電子取引のみならず、同法の電子帳簿としての要件に合致したシステムを構築し、維持する義務が生じるが、本システムとは別のシステムであり、詳細は省略する。ただ、同法は「自己が一貫して電子計算機で処理」するシステムの真実性を要求しているため、本システムと他のシステムを含めて真実性の要求を満たすか否か検討することが重要となる可能性がある。

以下、発生する業務ごとに監査として必要となると思われる項目をまとめる。

①－④に関しては、業務に関して使用する側で注意を払う項目、⑤に関しては ASP 事業者を中心に情報セキュリティの観点から注意を払う項目を挙げている。詳細設計のフェーズにおいて、コストを考慮し、以下の項目から取捨選択し、必要な事項を実装すべきである。

① データ交換

商品マスタ情報には、メーカー・卸間、卸・小売間ともに、販売条件や関係依存情報など商業上重要なデータが含まれる。そのため、データ交換時に団体等において、以下の情報を記録しておく。

- 送信側：送信時間（受領確認が必要な場合には確認時間）、送付者、データ情報（データ名、サイズ、作成日時）
- 受信側：受信時間、受領者（受領確認が必要な場合には確認時間）、データ情報（データ名、サイズ、作成日時）

② 受発注

受発注確定は取引が確定することであり、その情報は記録として残すことが必要である。なお受注側が FAX などデータ以外の場合、受注回答が必要な場合などにおいても、取引確定時のデータを保存しておく必要がある。

- 受注側：受注データ（条件を含む）、担当者名（双方）、受注確定日時、発注者確認記録（電子署名などの認証の記録など）
- 発注側：発注データ（条件を含む）、担当者名（双方）、発注確定日時

③ 物流

物流の形態は各種考えられるが、物の動きをトレース可能であり、最初の発注データと結び付けられるような記録を確保しておくことが必要である。

なお、出荷および入荷確定後、会計上の処理が必要となるため、結果確認も必要である。

- 発送側：出荷データ（注文番号、商品名、数量、輸送業者名、予定納入日など）、発送担当者、発送日時、入荷結果の報告、事前検品データ（ASNの場合のみ）
- 受取側：入荷データ（注文番号、商品名、数量、輸送業者名など）、入荷担当者、入荷確認日時、検品データ（ASN以外の場合）、入荷結果の報告データ

④ 決済

入荷結果の報告（受領確認）に含める場合や別途送付する場合も存在するが、金の流れを記録として残すことが必要となる。

- 発注側：受領データ（注文番号、商品名、数量など）受領報告日時、受領報告者、支払請求受取日時、支払日時
- 受注側：受領データ（注文番号、商品名、数量など）受領報告受付日時、受領報告受取者、支払請求発行者、支払確認日時

なお、ASP事業者に対する監査項目は、前節の本システムの管理基準を参考にしてASP事業者が定めるが、この標準に準じて記録すべき項目を次に記述する。

⑤ ASP事業者として推奨すべき記録

- 情報資産の分類と管理：情報資産管理記録
- 職責：職務権限と要員アサインメントの記録、教育記録
- 設備：セキュリティ区画設計、入退室記録、設備使用記録、設備点検記録、保守関連記録、消防法準拠の記録、その他標準（旧安全対策基準など）への準拠記録
- 運用記録：作業記録、システム稼動記録、システム変更記録、バックアップ取得記録、媒体管理記録
- 性能記録：NW性能監視記録、機器性能記録、
- 通信記録：FWログ、不正侵入（不成功を含め）記録、メール送受信ログ、リモートアクセス記録

- アクセス制御記録：アクセスログ、OS 監査ログ、アカウント管理記録、パスワード管理記録
- 障害、問題の記録：障害管理記録、セキュリティ事故管理記録
- 事業継続：事業継続に関するテスト記録
- 認証記録：Web サーバへのアクセスログ