文書番号：MOE10-業仕様-3014

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

「ネットワーク設計書」

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及び対象範囲

本設計書では、要件定義に定められる、システムの実現する機能範囲と、システムが満たさなければならない制約に基づいて設計を行う。

本設計書の各章では、利用拠点、運用、セキュリティ、性能、アーキテクチャのそれぞれの観点から、「ユースケース図及び業務フロー」、「運用条件書・運用設計書」、「セキュリティ設計書」、「性能要件設計書」、「システムアーキテクチャ設計書」の５つの設計書で規定する要件に基づいて、ネットワークの検討を行う。

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いるが、本設計書では、最も大量のデータを扱い条件的にも厳しい ASP 運用のネットワークについて主に記述する。

大企業自社運用及び中小企業自社運用については、利用者数、利用拠点数及び本システムを利用する際に必要となるインターネットの通信帯域について試算する。

なお、大企業自社運用及び中小企業自社運用に関するネットワーク構築及び接続性については、本設計書を参考として、各企業の責任において行うものとする。

２．利用拠点

本システムは、発注者システム、受注者システム、出荷拠点システム、入荷拠点システムとして稼動する。それぞれのシステムは、大企業または中小企業が１つのシステムを自社の拠点で運用する場合、４つのシステムを同じ拠点内で運用する場合（ASP 運用）を想定している。

システム区分（発注者システム、受注者システム、出荷拠点システム、入荷拠点システム）単位での利用者数及び利用拠点数を以下に試算する。

2.1 利用者数

「ユースケース図及び業務フロー」で規定される利用者、及び、「性能要件設計書」で規定された拠点数から本システム全体の利用者数を試算する。

「ユースケース図及び業務フロー」のアクター一覧から、それぞれのシステムの利用者は表２．１のとおりとなる。

表２．１　システムの利用区分と利用者

システム区分	システム利用者
発注者システム	発注担当者、支払担当者、発注商品管理者、発注者システム運用担当者、発注在庫管理担当者、販売管理担当者
入荷拠点システム	入荷担当者、入荷商品管理者
出荷拠点システム	出荷担当者、出荷商品管理者
受注者システム	受注担当者、請求担当者、受注商品管理者、 受注者システム運用担当者
その他	スケジューラ

また、「性能要件設計書」より、本システムの前提となる企業数（拠点数）は以下のとおり。

表２．２　利用形態、システム区分毎の企業数（拠点数）

	発注者	入荷拠点	出荷拠点	受注者
大企業自社運用	100	100	2,000	20
中小企業自社運用	100	100	700	70
ASP	400	400	10,000	10,000

表２．１及び表２．２より、すべての企業（拠点）において各システムの利用者が兼任をしないと仮定した場合は、以下のような利用者数になる。

表２．３　利用形態、システム区分毎の利用者数（最大値）

	発注者	入荷拠点	出荷拠点	受注者
大企業自社運用	600	200	4,000	80
中小企業自社運用	600	200	1,400	280
ASP	2,400	800	20,000	40,000
利用者合計	3,600	1,200	25,400	40,360

なお、１拠点または１企業当たりの取引データが少ない場合は、担当を兼任することが多くなると思われるので、実際は、表２．３の利用者合計の１／３～１／２程度の利用者になると想定される。

2.2 全体構成

拠点間の相互接続の全体構成イメージを以下に示す。

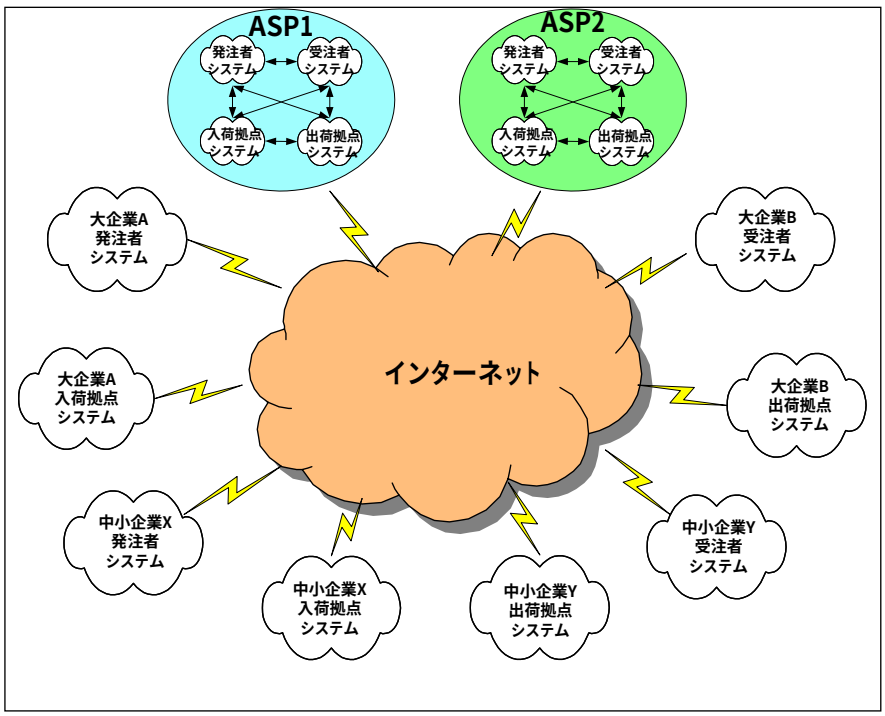

図２．１　拠点間の相互接続の全体構成

図２．１の各拠点の接続先は下表のとおりとなる。

表２．４　各拠点の接続先

受信側 / 送信側	ASP1	ASP2	大企業 A		大企業 B		中小企業 X		中小企業 Y	
			発注者	入荷拠点	受注者	出荷拠点	発注者	入荷拠点	受注者	出荷拠点
ASP1	-	○	○	○	○	○	○	○	○	○
ASP2	○	-	○	○	○	○	○	○	○	○
大企業 A 発注者	○	○	-	○	○	○	×	×	○	○
大企業 A 入荷拠点	○	○	○	-	○	○	×	×	○	○
大企業 B 受注者	○	○	○	○	-	○	○	○	×	×
大企業 B 出荷拠点	○	○	○	○	○	-	○	○	×	×
中小企業 X 発注者	○	○	×	×	○	○	-	○	○	○
中小企業 X 入荷拠点	○	○	×	×	○	○	○	-	○	○
中小企業 Y 受注者	○	○	○	○	×	×	○	○	-	○
中小企業 Y 出荷拠点	○	○	○	○	×	×	○	○	○	-

２.３ ネットワーク拠点

「性能要件設計書」で記述されているシステム区分毎の参加企業数（表２．２)、及び、１企業当たりの性能要件から、データ交換対象となるシステムの最大拠点数を試算する。

本システムの拠点間（システム間）のデータ（ファイル）転送について図示すると図２．２のようになる。

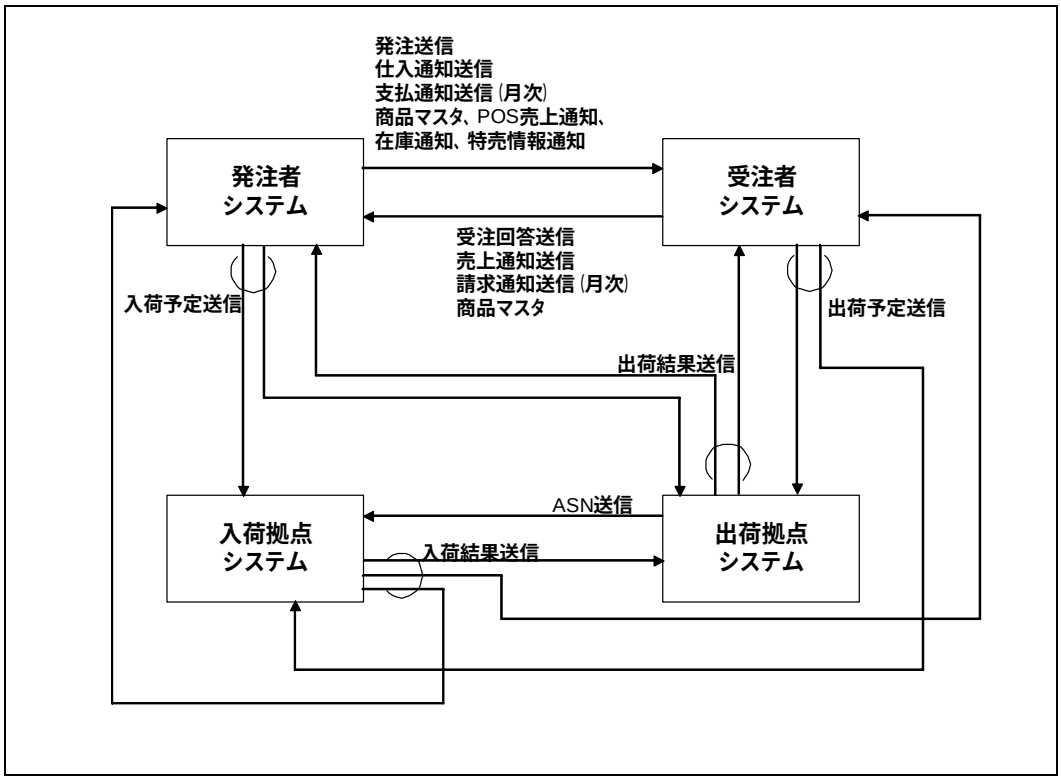

図２．２　データ転送関連図

ASP は１０拠点で稼動する（各 ASP は、発注者、入荷拠点、出荷拠点、受注者の４つのシステムは、表１．２の ASP の企業数の１／１０がそれぞれ利用する）と想定し、各利用形態のデータ交換対象となるシステムの最大値（拠点数）を以下に試算する。

ASP 運用の拠点では、４つのシステムが共存しているため、システム間のデータ転送が ASP 内のみで完結する場合がある。この場合はデータ交換の対象拠点数としてカウントしない。

また、大企業自社運用の場合、１つの発注者システムに対して、１つの入荷拠点システムが存在し、１つの受注者システムに対して、１００の出荷拠点システムが存在する。

中小企業自社運用の場合は、１つの発注者システムに対して、１つの入荷拠点システムが存在し、１つの受注者システムに対して、１０の出荷拠点システムが存在する。

2.3.1 大企業自社運用発注者システムの接続拠点

大企業自社運用の発注者システムに関する接続拠点関連図を図２．３に示す。

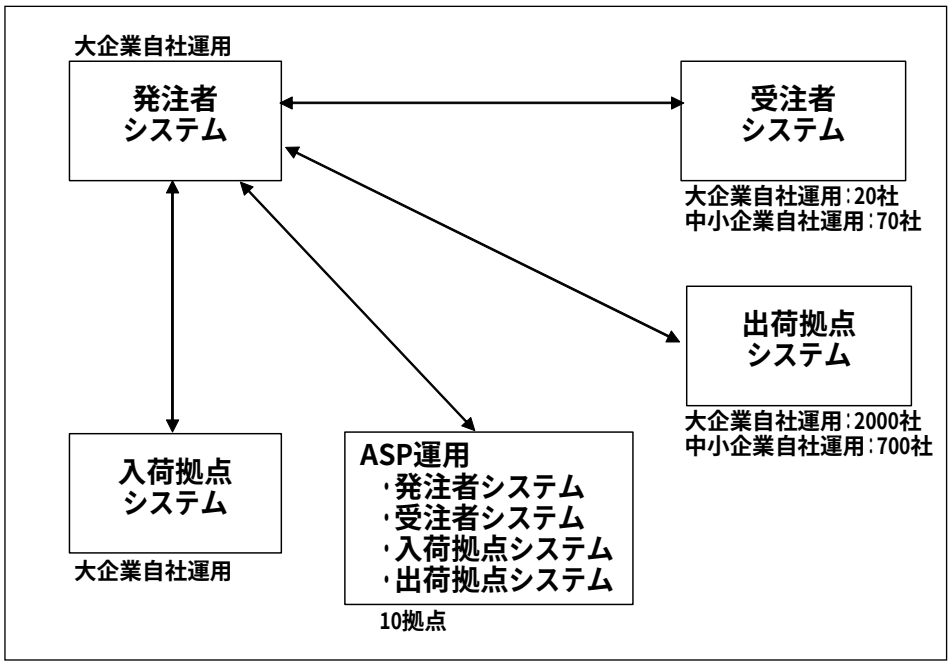

図２．３　発注者システム（大企業自社運用）接続拠点関連図

大企業自社運用の発注者システムがデータ交換対象となる出荷拠点システムは、「大企業自社運用出荷拠点数（2000）＋中小企業自社運用出荷拠点数（700）＋ASP 運用拠点数（10）」で計算できる。

同様にデータ交換対象となる受注者システムは、「大企業自社運用受注者システム数（20）＋中小企業自社運用受注者システム数（70）＋ASP 運用拠点数（10）」で計算できる。

2.3.2 中小企業自社運用発注者システムの接続拠点

中小企業自社運用の発注者システムに関する接続拠点関連図を図２．４に示す。

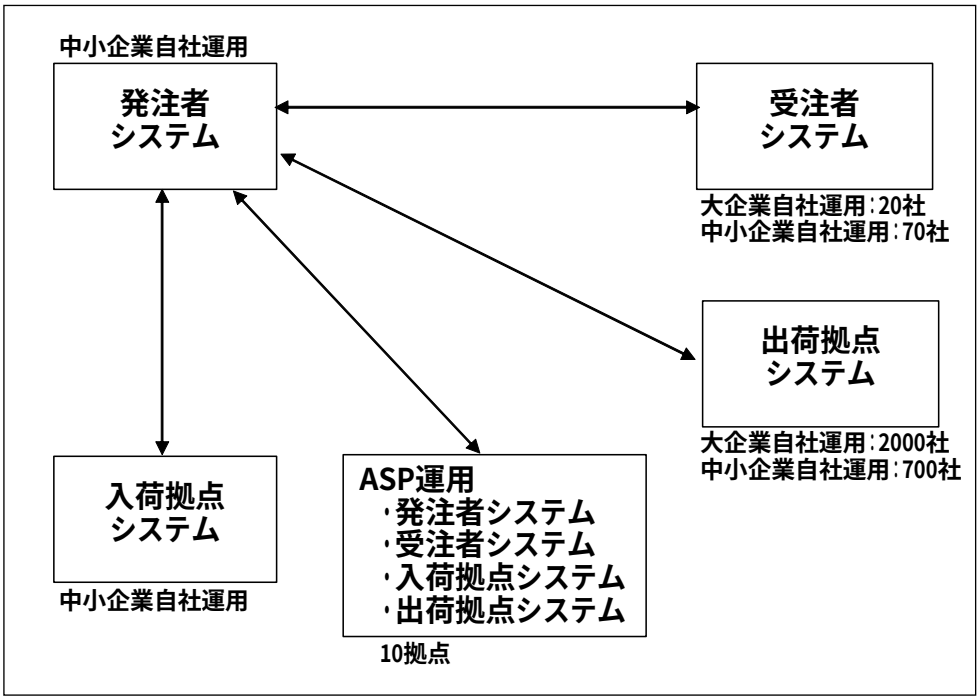

図２．４　発注者システム（中小企業自社運用）接続拠点関連図

中小企業自社運用の発注者システムがデータ交換対象となる出荷拠点システムは、「大企業自社運用出荷拠点数（2000）＋中小企業自社運用出荷拠点数（700）＋ASP 運用拠点数（10）」で計算できる。

同様にデータ交換対象となる受注者システムは、「大企業自社運用受注者システム数（20）＋中小企業自社運用受注者システム数（70）＋ASP 運用拠点数（10）」で計算できる。

2.3.3 ASP 運用拠点内発注者システムの接続拠点

ASP 運用の発注者システムに関する接続拠点関連図を図２．５に示す。

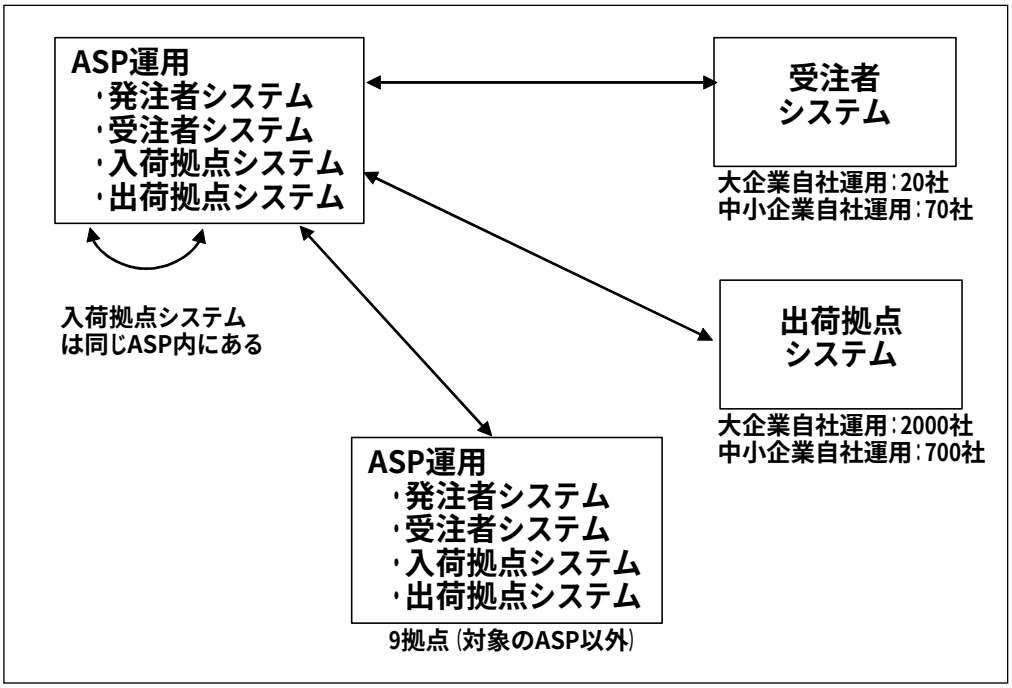

図２．５　発注者システム（ASP 運用）接続拠点関連図

ASP 運用の拠点内発注者システムがデータ交換対象となる出荷拠点システムは、「大企業自社運用出荷拠点数（2000）＋中小企業自社運用出荷拠点数（700）＋ASP 運用拠点数（対象の ASP 以外）(9)」で計算できる。

同様にデータ交換対象となる受注者システムは、「大企業自社運用受注者システム数（20）＋中小企業自社運用受注者システム数（70）＋ASP 運用拠点数（対象の ASP 以外）(9)」で計算できる。

2.3.4 接続拠点数の試算

前項までの内容を、システム区分ごとに、各利用形態と接続拠点数にまとめると表2．5～表2．8のとおりとなる。

表2．5　システム区分：発注者システム

利用形態	入荷拠点システム	出荷拠点システム	受注者システム
大企業自社運用	1	2,710	100
中小企業自社運用	1	2,710	100
ASP	(データ転送なし:ASP内のみ)	2,709	99

表2．6　システム区分：受注者システム

利用形態	発注者システム	入荷拠点システム	出荷拠点システム
大企業自社運用	210	210	100
中小企業自社運用	210	210	10
ASP	209	209	(データ転送なし:ASP 内のみ)

表2．7　システム区分：入荷拠点システム

利用形態	発注者システム	出荷拠点システム	受注者システム
大企業自社運用	1	2,710	100
中小企業自社運用	1	2,710	100
ASP	(データ転送なし:ASP 内のみ)	2,709	99

表２．８　システム区分：出荷拠点システム

利用形態	発注者 システム	入荷拠点 システム	受注者 システム
大企業自社運用	210	210	1
中小企業自社運用	210	210	1
ASP	209	209	(データ転送なし:ASP 内のみ)

表２．５～表２．８より、最大接続拠点数は、システムの利用形態及びシステム区分ごとに接続拠点数が大きく異なる。実際に接続する拠点数に応じてネットワーク機器等を選定する必要がある。

３．性能検討

３.１ ハードウェア構成

「システムアーキテクチャ設計書」より、本システムハードウェア構成イメージを図３．１に、各ハードウェア構成要素とその機能の概要を表３．１に示す。

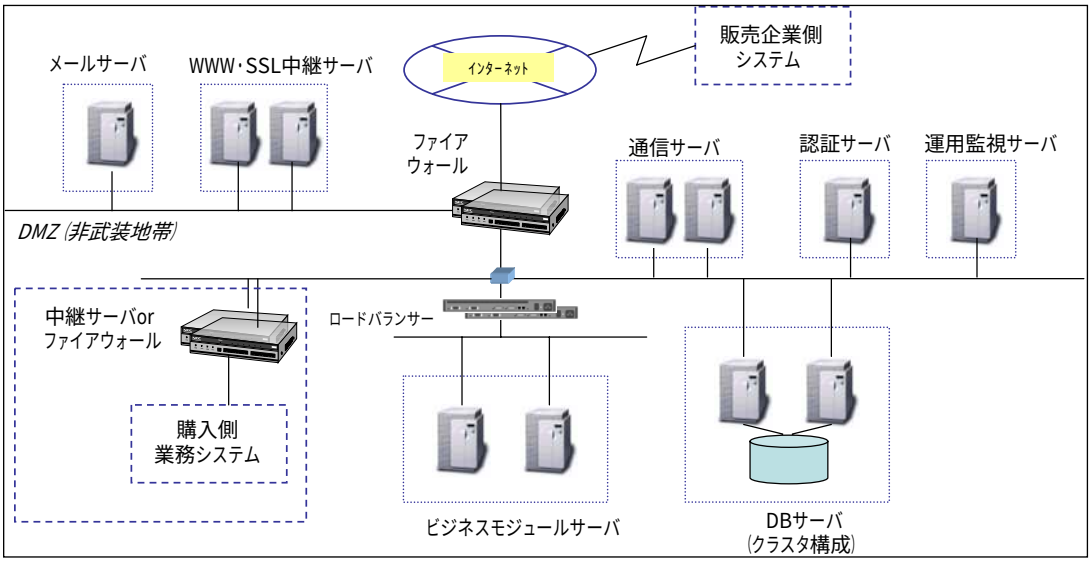

図３．１　ハードウェア構成

表３．１　ハードウェア構成要素と機能

サーバ名	機能
ビジネスモジュールサーバ（BM サーバ）	ビジネスプロセス情報に基づき、既存の業務システムや通信サーバと連携して、企業間取引を実現する。
DB サーバ	ビジネスモジュールで利用されるデータを格納するサーバ。
ファイアウォール	第三者による内部システムへの不正アクセスからシステムを守る。
メールサーバ	メールの送受信を行うサーバ。システムからの通知等に利用する。
WWW･SSL 中継サーバ	Web クライアントからの業務の入り口となるサーバ。
通信サーバ	通信サーバの機能を配置するサーバ。ebXML の通信を解釈･生成するためのミドルウェアで、XML 処理･通信処理を担当する。
認証サーバ	本システムを利用する上でのユーザの正当性を確認し、各種利用権限を管理するサーバ。
運用監視サーバ	システムのサービス状況の監視や、バックアップ等日々のシステム運用を制御するサーバ。

3.2 データフロー

3.2.1 データ転送（送信側）

拠点間でデータ転送を行う場合のデータ送信側のデータフローは以下のとおりとなる。

① 通信サーバは認証サーバにあて先（送信先）の参照を行う。

② 通信サーバと SSL アクセラレータを介して、https セッション開始する。

③ https リクエスト＋電子証明書を送付する。

④ あて先（送信先）は、電子証明書を確認して問題ないことを返答する。

⑤ SSL トンネルを作成する。

⑥ 互いの通信条件を確認する。

⑦ 通信サーバは、あて先（送信先）に転送するデータを検索・抽出する。

⑧ 通信サーバはあて先（送信先）にデータを転送する

上記データフローを図示すると以下のとおりとなる。なお、ハードウェア構成については、図３．１の機器を一部省略して図示している。

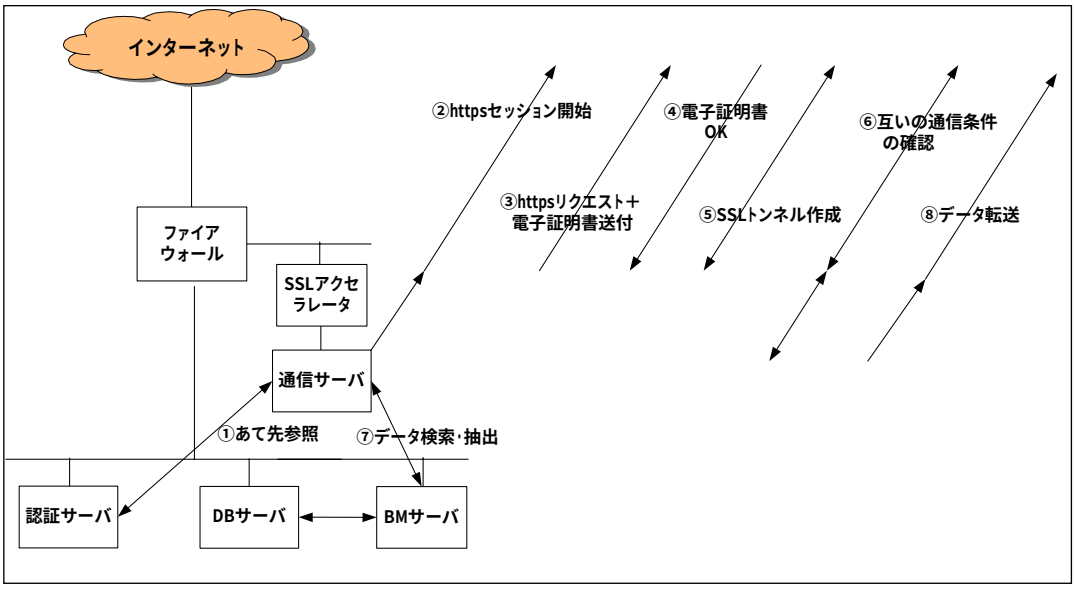

図３．２　送信側データ転送データフロー

3.2.2 データ転送（受信側）

拠点間でデータ転送を行う場合のデータ受信側のデータフローは以下のとおりとなる。

① SSL アクセラレータは、送信元の https リクエスト＋送信元電子証明書を受信する。

② SSL アクセラレータは、認証サーバに送信元の電子証明書の有効性を確認する。

③ SSL アクセラレータは、送信元の電子証明書が有効であることを返答する。

④ SSL トンネルを作成する。

⑤ 互いの通信条件を確認する。

⑥ 通信サーバは、送信元からのデータを受信する。

⑦ 通信サーバは、受信したデータを登録する。

上記データフローを図示すると以下のとおりとなる。なお、ハードウェア構成については、図３．１の機器を一部省略して図示している。

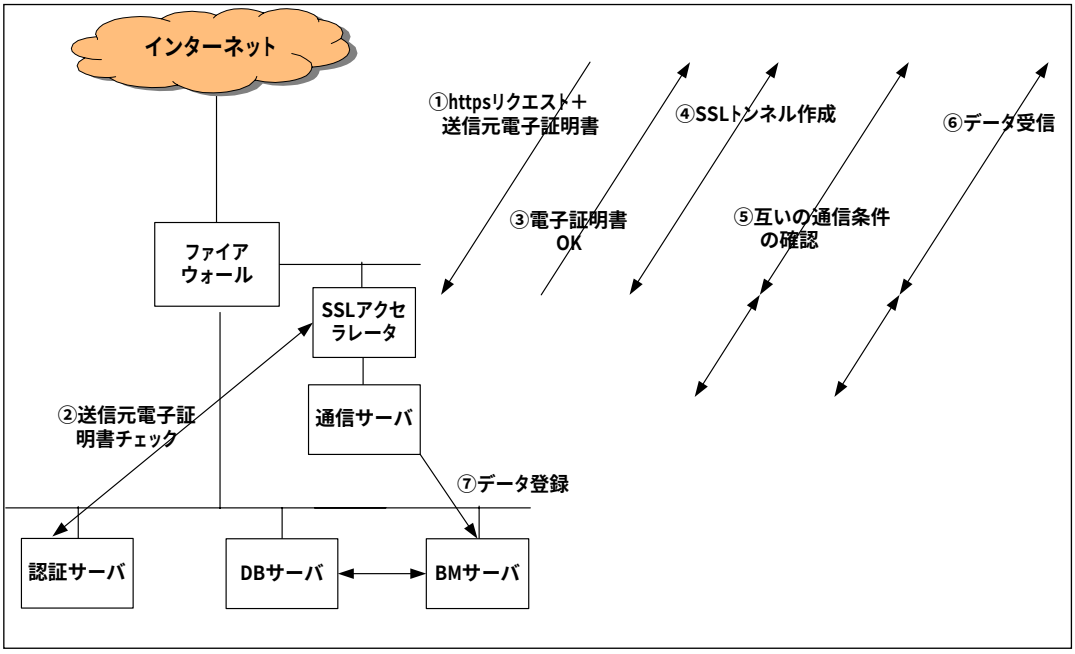

図３．３　受信側データ転送データフロー

3.2.3 Web アクセス（ASP 運用）

ＡＳＰ運用において、Web アクセスの場合のデータフローは以下のとおりとなる。

① SSL アクセラレータは、クライアント PC からの https リクエストを受信する。

② PC が電子証明書を利用する場合は、認証サーバに PC のクライアント電子証明書の有効性を確認する。

③ SSL トンネルを作成する。

④ WWW サーバはクライアント PC の http リクエストを受け付ける。

⑤ WWW サーバはアクセス条件を確認する。

⑥ WWW サーバは、PC クライアントとデータ通信を開始する。

上記データフローを図示すると以下のとおりとなる。なお、ハードウェア構成については、図３．１の機器を一部省略して図示している。

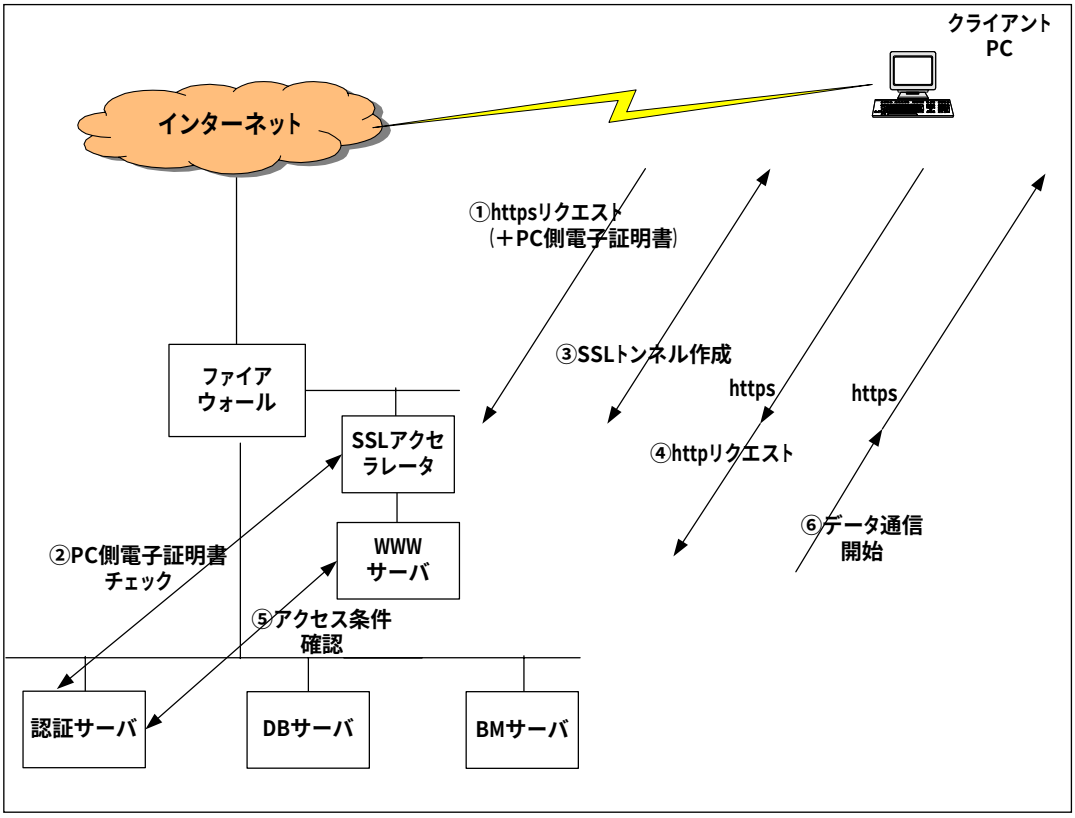

図３．４　Web アクセス（ASP 運用）データフロー

3.3 通信帯域の試算の前提

（1） データ量

「性能要件設計書」で規定している発注、受注、出荷、入荷の各データ量を表３．２に示す。このデータ量からデータ転送及び Web アクセスに必要となるインターネットの通信帯域等を試算する。

なお、内部ネットワークは十分な帯域が確保されており、コリジョンは無視できる程度であるものとする。アプリケーションの処理時間や機器類の応答時間等は考慮せず、ネットワーク上を流れるデータ伝送を対象とした試算を行う。

表３．２　発注、受注、出荷、入荷のデータ量

利用形態	項目	発注数	受注数	出荷数	入荷数
大企業 自社運用	総データ量	10,000,000	7,200,000	7,200,000	10,000,000
	企業数（拠点数）	100	20	2,000	100
	1 企業あたりのデータ量	100,000	360,000	3,600	100,000
中小企業 自社運用	総データ量	1,600,000	5,400,000	5,400,000	1,600,000
	企業数（拠点数）	100	700	700	100
	1 企業あたりのデータ量	16,000	7,714	7,714	16,000
ASP 運用	総データ量	6,400,000	5,400,000	5,400,000	6,400,000
	企業数（拠点数）	400	10,000	10,000	400
	1 企業あたりのデータ量	16,000	540	540	16,000

※データ量の単位：伝票明細件数／日　1 件あたりのデータ量：500 バイト

表３．２は、1 企業あたりのデータ量である。ASP 運用の場合は複数の企業が利用することになる。ここでは、ASP 運用でサービスを提供する組織は 10 組織（10 拠点）、各 ASP は発注者システム及び入荷拠点システム×40 社（同じ企業が２つのシステムを利用）、出荷拠点システム及び受注者システム×1,000 社（同じ企業が２つのシステムを利用）の合計：1,040 社の企業が利用することを前提とする。

また、各システムにおける処理（発注送信、受注回答受信など）は同時に実行されないようスケジューリングされているものとする。ASP 運用の場合は、発注者、受注者、入荷拠点、出荷拠点のそれぞれのシステムが稼動する

ため、例えば、発注者システムが「発注送信」をしているときに、同じ ASP 内の受注者システムは「発注受信」することになる。

なお、送受信 1 回あたりの許容処理時間は、「性能要件設計書」で規定する時間とする。

（2） 新規接続セッション数と通信帯域の算出

新規接続セッション数及び通信帯域は、データ転送、Web アクセスそれぞれについて算出する。なお、大企業自社運用及び中小企業自社運用の場合は、内部のネットワークから本システムに接続することを想定しているので、Web アクセスについては、ASP 運用のみを対象として試算する。

接続セッションやデータ転送及び Web アクセスは、一日のうちの特定の時間帯に集中する。算出に当たり接続やデータが集中する時間帯と接続数及びデータ量を定義する。新規接続セッション数及び通信帯域は、この時間帯の平均値とする。

算出手順は以下のとおり。

- メッセージ発生率（件／秒、または、画面／秒）を計算する
- メッセージ発生率にメッセージ（データまたは画面）のサイズを乗ずる

① メッセージ発生率（単位時間当たりのメッセージ発生件数）

1） データ転送の場合

1 日当たりのデータ量×最大データ集中度／許容処理時間

（各値は性能要件設計書を参照）

2） Web アクセス（ASP 運用　受注システム）の場合

1 ユーザあたりのダウンロード画面数×同時アクセス企業数／全企業のアクセス時間

Web アクセスの場合、ダウンロード画面数は、

1 ユーザあたりのアクセス頻度×アクセス時間

とする。それぞれの値を表３．３のように定義すると 1 ユーザあたりのダウンロード画面数は、20 画面となる。

表３．３　アクセス頻度とアクセス時間

１ユーザあたりのアクセス頻度	30 秒に 1 回
アクセス時間	10 分

また、同時アクセス企業数、全企業のアクセス時間を表３．４に定義する。

表３．４　同時アクセス企業数と全企業のアクセス時間

同時アクセス企業数	1000 社(受注者システムを利用する企業数)
全企業のアクセス時間	30 分間

② メッセージサイズ（データまたは画面のサイズ）

データ転送、Web アクセスの 1 件あたりのサイズを表３．５に定義する。なお、この値は、TCP/IP ヘッダ情報等の伝送オーバーヘッドを含んだサイズとする。

表３．５　メッセージサイズ

データ転送	500 バイト
Web アクセス	50,000 バイト

3.4 大企業自社運用の場合の必要帯域等の試算

3.4.1 新規接続セッション数

「1．3．4接続拠点数の試算」より、データ転送における新規の接続セッション数の最大値（受信側）は、以下のようになる。

・発注者システムが出荷拠点システムから受信する「出荷結果受信」

2,710 セッション

・入荷拠点システムが出荷拠点システムから受信する「ASN 受信」

2,710 セッション

いずれも 10 分間に接続するセッション数であり、1 秒間の新規接続セッション数（10 分間の平均）は以下のとおりとなる。

2,710／（10×60）　4.5（セッション／秒）

3.4.2 データ転送に必要な通信帯域

（1） 発注者システム

本システムを発注者システムとして利用する場合、データ転送に関して最も負荷が高くなるパターンを下表に示す。

表3．6　発注者システムの試算条件

処理名称	発注送信、受注回答受信、入荷予定送信、出荷結果受信
1日あたりのデータ量	100,000（配信明細件数／日）
配信明細1件あたりのサイズ	500 バイト
送受信1回あたり最大データ集中度	85%
送受信1回あたり許容処理時間	10 分

データ通信量（10 分間の平均）を計算すると以下となる。

表３．７　発注者システムの試算結果

配信件数（件／分）	8,500　（件／分）
配信件数（件／秒）（メッセージ発生率）	142　（件／秒）
配信データ	70,833　（バイト／秒）
必要通信帯域	566,667　（bps）

本システムが大企業自社運用の発注者システムで稼動する場合、本システムが必要とするインターネットの通信帯域（平均）は約 0.57Mbps と試算される。

（２）　受注者システム

本システムを受注者システムとして利用する場合、最も負荷が高くなるパターンを下表に示す。

表３．８　受注者システムの試算条件

処理名称	発注受信、受注回答送信、出荷予定送信、出荷結果受信、入荷結果受信
１日あたりのデータ量	360,000（配信明細件数／日）
配信明細１件あたりのサイズ	500 バイト
送受信１回あたり最大データ集中度	85%
送受信１回あたり許容処理時間	20 分

データ通信量（20 分間の平均）を計算すると以下となる。

表３．９　受注者システムの試算結果

配信件数（件／分）	15,300　（件／分）
配信件数（件／秒）（メッセージ発生率）	255　（件／秒）
配信データ	127,500　（バイト／秒）
必要通信帯域	1,020,000　（bps）

本システムが大企業自社運用の受注者システムとして稼動する場合、本システムが必要とするインターネットの通信帯域（平均）は約 1.0Mbps と試算される。

（3） 出荷拠点システム

本システムを出荷拠点システムとして利用する場合、最も負荷が高くなるパターンを下表に示す。

表３．１０　出荷拠点システムの試算条件

処理名称	出荷予定受信、入荷予定受信、ASN 送信、入荷結果受信、出荷結果送信
１日あたりのデータ量	3,600（配信明細件数／日）
配信明細１件あたりのサイズ	500 バイト
送受信１回あたり最大データ集中度	85%
送受信１回あたり許容処理時間	10 分

データ通信量（10 分間の平均）を計算すると以下となる。

表３．１１　出荷拠点システムの試算結果

配信件数（件／分）	306　（件／分）
配信件数（件／秒）（メッセージ発生率）	5　（件／秒）
配信データ	2,550　（バイト／秒）
必要通信帯域	20,400　（bps）

本システムが大企業自社運用の出荷拠点システムとして稼動する場合、本システムが必要とするインターネットの通信帯域（平均）は約 0.02Mbps と試算される。

（4） 入荷拠点システム

本システム入荷拠点システムとして利用する場合、最も負荷が高くなるパターンを下表に示す。

表３．１２　入荷拠点システムの試算条件

処理名称	出荷予定受信、入荷予定受信、ASN 受信、入荷結果送信
１日あたりのデータ量	100,000（配信明細件数／日）
配信明細１件あたりのサイズ	500 バイト
送受信１回あたり最大データ集中度	85%
送受信１回あたり許容処理時間	10 分

データ通信量（10 分間の平均）を計算すると、以下となる。

表３．１３　入荷拠点システムの試算結果

配信件数（件／分）	8,500　（件／分）
配信件数（件／秒）（メッセージ発生率）	142　（件／秒）
配信データ	70,833　（バイト／秒）
必要通信帯域	566,667　（bps）

本システムが大企業自社運用の入荷拠点システムとして稼動する場合、本システムが必要とするインターネットの通信帯域（平均）は約 0.57Mbps と試算される。

なお、各システムを同じ拠点内に設置する場合、上記システム毎の試算結果の通信帯域を合わせた帯域を確保する必要がある。

3.5 中小企業自社運用の場合の必要帯域等の試算

3.5.1 新規接続セッション数

「1．3．4接続拠点数の試算」より、データ転送における新規の接続セッション数の最大値（受信側）は、以下のようになる。

・発注者システムが出荷拠点システムから受信する「出荷結果受信」

2,710 セッション

・入荷拠点システムが出荷拠点システムから受信する「ASN 受信」

2,710 セッション

いずれも 10 分間に接続するセッション数であり、1 秒間の新規接続セッション数（10 分間の平均）は以下のとおりとなる。

2,710／（10×60）　4.5（セッション／秒）

3.5.2 データ転送に必要な通信帯域

（1） 発注者システム

本システムを発注者システムとして利用する場合、データ転送に関して最も負荷が高くなるパターンを下表に示す。

表3．14　発注者システムの試算条件

処理名称	発注送信、受注回答受信、入荷予定送信、出荷結果受信
1日あたりのデータ量	16,000（配信明細件数／日）
配信明細1件あたりのサイズ	500 バイト
送受信1回あたり最大データ集中度	85%
送受信1回あたり許容処理時間	10 分

データ通信量（10 分間の平均）を計算すると以下となる。

表３．１５　発注者システムの試算結果

配信件数（件／分）	1,360　（件／分）
配信件数（件／秒）（メッセージ発生率）	23　（件／秒）
配信データ	11,333　（バイト／秒）
必要通信帯域	90,667　（bps）

本システムが中小企業自社運用の発注者システムで稼動する場合、本システムが必要とするインターネットの通信帯域（平均）は約 0.09Mbps と試算される。

（２）　受注者システム

本システム受注者システムとして利用する場合、最も負荷が高くなるパターンを下表に示す。

表３．１６　受注者システムの試算条件

処理名称	発注受信、受注回答送信、出荷予定送信、出荷結果受信、入荷結果受信
１日あたりのデータ量	7,714（配信明細件数／日）
配信明細１件あたりのサイズ	500 バイト
送受信１回あたり最大データ集中度	85%
送受信１回あたり許容処理時間	20 分

データ通信量（20 分間の平均）を計算すると、以下となる。

表３．１７　受注者システムの試算結果

配信件数（件／分）	328　（件／分）
配信件数（件／秒）（メッセージ発生率）	5　（件／秒）
配信データ	2,732　（バイト／秒）
必要通信帯域	21,856　（bps）

本システムが中小企業自社運用の受注者システムとして稼動する場合、本システムが必要とするインターネットの通信帯域（平均）は約 0.02Mbps と試算される。

（3） 出荷拠点システム

本システム出荷拠点システムとして利用する場合、最も負荷が高くなるパターンを下表に示す。

表３．１８　出荷拠点システムの試算条件

処理名称	出荷予定受信、入荷予定受信、ASN 送信、入荷結果受信、出荷結果送信
１日あたりのデータ量	7,714（配信明細件数／日）
配信明細１件あたりのサイズ	500 バイト
送受信１回あたり最大データ集中度	85%
送受信１回あたり許容処理時間	10 分

データ通信量（10 分間の平均）を計算すると以下となる。

表３．１９　出荷拠点システムの試算結果

配信件数（件／分）	656　（件／分）
配信件数（件／秒）（メッセージ発生率）	11　（件／秒）
配信データ	5,464　（バイト／秒）
必要通信帯域	43,713　（bps）

本システムが中小企業自社運用の出荷拠点システムとして稼動する場合、本システムが必要とするインターネットの通信帯域（平均）は約 0.04Mbps と試算される。

（4） 入荷拠点システム

本システム入荷拠点システムとして利用する場合、最も負荷が高くなるパターンを下表に示す。

表３．２０　入荷拠点システムの試算条件

処理名称	出荷予定受信、入荷予定受信、ASN 受信、入荷結果送信
１日あたりのデータ量	16,000（配信明細件数／日）
配信明細１件あたりのサイズ	500 バイト
送受信１回あたり最大データ集中度	85%
送受信１回あたり許容処理時間	10 分

データ通信量（10 分間の平均）を計算すると以下となる。

表３．２１　入荷拠点システムの試算結果

配信件数（件／分）	1,360	（件／分）
配信件数（件／秒）（メッセージ発生率）	23	（件／秒）
配信データ	11,333	（バイト／秒）
必要通信帯域	90,667	（bps）

本システムが中小企業自社運用の入荷拠点システムとして稼動する場合、本システムが必要とするインターネットの通信帯域（平均）は約 0.09Mbps と試算される。

なお、各システムを同じネットワーク内に設置する場合、上記システム毎の試算結果の通信帯域を合わせた帯域を確保する必要がある。

3.6 ASP 運用の場合の必要帯域等の試算

3.6.1 新規接続セッション数

「1．3．4接続拠点数の試算」より、データ転送における新規の接続セッション数の最大値（受信側）は、以下のようになる。

・発注者システムが出荷拠点システムから受信する「出荷結果受信」

2,709 セッション

・入荷拠点システムが出荷拠点システムから受信する「ASN 受信」

2,709 セッション

いずれも 10 分間に接続するセッション数であり、順次接続するとすれば、1 秒間の新規接続セッション数（10 分間の平均）は以下のとおりとなる。

2,709／（10×60）　4.5（セッション／秒）

また、Web アクセスにおける新規の接続セッション数は以下の条件で試算する。

表3．22　Web アクセスの接続セッションの試算条件

Web アクセスの頻度（1 社当たり）	30 秒に 1 回程度
1ユーザあたりのアクセス時間	10 分
1ユーザあたりのダウンロード画面	20 画面
全ユーザのアクセス時間帯	30 分間
同時アクセス企業数	1000 社(受注者システムを利用する企業数)

アクセス時間の 10 分間はセッションが維持されているものと仮定する。全ユーザのアクセス時間帯が 30 分間であり、各ユーザのアクセス時間が 10 分であるから、最初の 20 分間に 1000 社の新規アクセスが発生することになる。

従って、Web アクセスの場合の 1 秒間の新規接続セッション数（20 分間の平均）は以下のとおりとなる。

1000／（20×60）　0.8（セッション／秒）

3.6.2 データ転送に必要な通信帯域

ASP 運用の場合、発注者、受注者、入荷拠点、出荷拠点の４システムが稼動することを前提とする。すなわち、発注者システムが「発注送信」をしているときに、同じ ASP 内の受注者システムは「発注受信」することになる。

このように各システムで送受信が重なり、かつ、最も負荷が高くなるパターンは、入荷拠点システムが他の３システム（発注者、受注者、出荷拠点）に対して送信する「入荷結果」であり、この処理を通信帯域の算出対象とする。なお、ASP 内で稼動する発注者システムと入荷拠点システムは同じ企業が利用する前提であれば、内部での送受信となるので対象外とする。

また、「入荷結果」を受信する受注者システム及び出荷拠点システムも ASP 内に存在するものは対象外とする必要がある。「性能要件設計書」の受注者のシェアの割合から、内部での送受信となる割合は 3%となる（ASP 運用のシェアは全体の 30%であり、ASP は 10 拠点を前提としているのでシェア 3%が ASP 内の受注者となる）。なお、大企業自社運用と中小企業自社運用はすべて外部のシステムとなる。

「入荷結果」の内部／外部の送受信割合を図示すると以下のようになる。

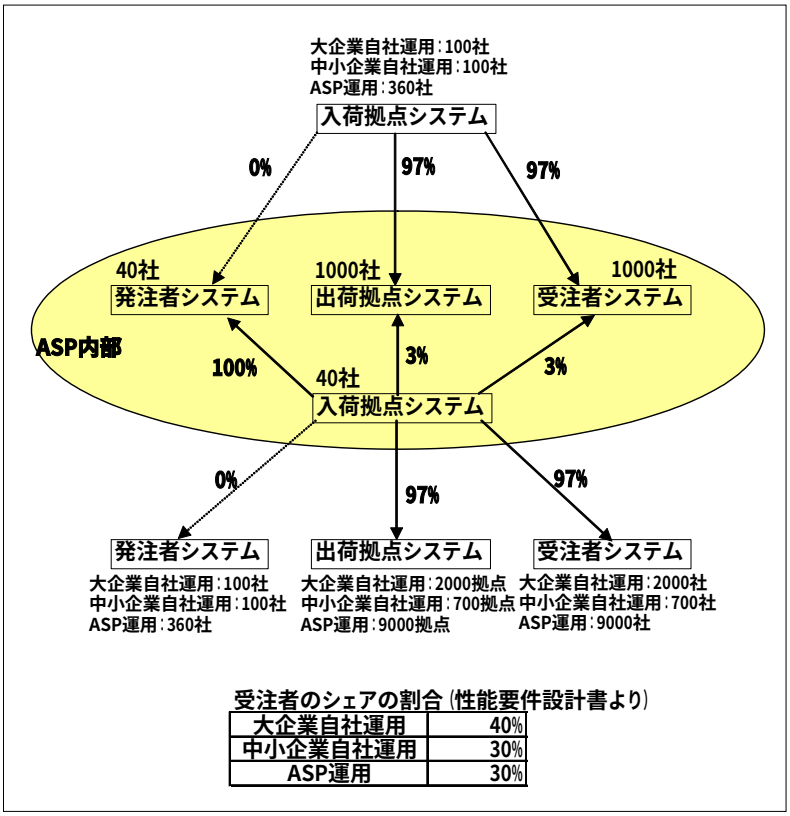

図３．５　「入荷結果」の送受信割合

入荷拠点システムが他の３つのシステムに対して送信する「入荷結果」はそれぞれの次のようなデータ量となる。

表３．２３　発注者システムの試算条件

処理名称	入荷結果受信
１日あたりのデータ量	16,000×40 社（配信明細件数／日）
配信明細１件あたりのサイズ	500 バイト
送受信１回あたり最大データ集中度	85%
送受信１回あたり許容処理時間	10 分
外部からの受信比率	0%

表３．２４　受注者システムの試算条件

処理名称	入荷結果受信
１日あたりのデータ量	540×1,000 社（配信明細件数／日）
配信明細１件あたりのサイズ	500 バイト
送受信１回あたり最大データ集中度	85%
送受信１回あたり許容処理時間	10 分
外部からの受信比率	97%

表３．２５　出荷拠点システムの試算条件

処理名称	入荷結果受信
１日あたりのデータ量	540×1,000 社（配信明細件数／日）
配信明細１件あたりのサイズ	500 バイト
送受信１回あたり最大データ集中度	85%
送受信１回あたり許容処理時間	10 分
外部からの受信比率	97%

表３．２６　入荷拠点システムの試算条件

処理名称	入荷結果送信
１日あたりのデータ量	16,000×40 社（配信明細件数／日）
配信明細１件あたりのサイズ	500 バイト
送受信１回あたり最大データ集中度	85%
送受信１回あたり許容処理時間	10 分
外部への送信比率	発注者システム：0% 受注者システム及び出荷拠点システム：97%

ASP 運用の場合は、入荷結果送受信（表３．２３～表３．２６の送受信）が同時に実行されたときに最も負荷がかかる。ASP 運用の場合の必要通信帯域は、各システムの通信帯域（10 分間の平均）の試算結果を合計したものとなる。

表３．２７　受注者システムの試算結果

配信件数（件／分）	44,523　（件／分）
配信件数（件／秒）（メッセージ発生率）	742　（件／秒）
１件あたりのデータ	500　（バイト）
配信データ	371,025　（バイト／秒）
必要通信帯域	2,968,200　（bps）

表３．２８　出荷拠点システムの試算結果

配信件数（件／分）	44,523　（件／分）
配信件数（件／秒）（メッセージ発生率）	742　（件／秒）
１件あたりのデータ	500　（バイト）
配信データ	371,025　（バイト／秒）
必要通信帯域	2,968,200　（bps）

表３．２９　入荷拠点システムの試算結果

配信件数（件／分）	52,768	（件／分）
配信件数（件／秒）（メッセージ発生率）	879	（件／秒）
１件あたりのデータ	500	（バイト）
配信データ	439,733	（バイト／秒）
必要通信帯域		
発注者システムへの送信	0	（bps）
受注者システムへの送信	3,517,867	（bps）
出荷拠点システムへの送信	3,517,867	（bps）

なお、発注者システムに対しては内部からの配信のみとなるため必要通信帯域は 0（bps）となる。

入荷拠点システムが他の３つのシステム（発注者、受注者、出荷拠点の各システム）に対して送信する「入荷結果」の送受信が規定の時間内に終了するために必要な通信帯域は、表３．２７～表３．２９の試算結果の必要通信帯域（平均）の合計、すなわち、約 13.0（Mbps）と試算される。

3.6.3 Web アクセスに必要な通信帯域

次に Web アクセスのために必要な通信帯域を試算する。１企業あたりの前提条件を表３．３０、Web アクセスの通信帯域の試算結果（30 分間の平均）を表３．３１に示す。

表３．３０　Web アクセスの試算条件

Web アクセスの頻度（1 企業当たり）	30 秒に 1 回程度
１企業あたりのアクセス時間	10 分
１企業あたりのダウンロード画面	20 画面
全企業のアクセス時間帯	30 分間
同時アクセス企業数	1000 社(受注者システムを利用する企業数)
アクセスの発生率（30 分間の平均）	11.1 回／秒
Web アクセスの１回あたりのダウンロードデータ（1 画面のデータサイズ）	50KB

表３．３１　Web アクセスの試算結果

配信画面数（画面／秒）（メッセージ発生率）	11.1　（画面／秒）
１画面あたりのデータ	50,000　（バイト）
配信データ	555555.6　（バイト／秒）
必要通信帯域	4,444,444　（bps）

システム間（サーバ間）のデータ転送の最大値と Web アクセスの最大値が重なった場合は、データ転送に必要な帯域に、Web アクセスの試算結果を合わせた通信帯域が必要となる。

3.7 ネットワーク機器の性能検討

本システムのネットワーク機器のうち、SSL アクセラレータ、ロードバランサ、L3 スイッチ、ルータ、ファイアウォールの性能について以下に記述する。

（1） SSL アクセラレータ

SSL アクセラレータは、将来の接続数及びデータ量の増加を考慮して、性能に余裕のあるものを選定する。選定条件を以下に示す。

- SSL 同時接続数：データ転送先のサーバ数、または、Web アクセスユーザ数の最大値より大きい同時接続数を提供する機種であること
- SSL 性能（セッション／秒）：メッセージ発生率の最大値よりも大きい性能を有する機種であること
- サーバ認証、クライアント認証に対応した機種であること
- 提示された証明書の有効性を検査し、送信元の信頼性を確認できること
- CRL（Certificate Revocation List：認証書失効リスト）を調べ、クライアントまたはサーバが提示した証明書が失効していないことを確認できること
- 電子証明書登録数は接続する拠点のサーバの数より大きいこと
- 認証サーバと連携できる機能を有すること
- SSL バージョンは、SSL ｖ2 及びｖ3 に対応していること

（2） ロードバランサ

各システム区分とも負荷が高くなる WWWサーバ、Web 業務サーバ、BM サーバ、通信サーバにはロードバランサによる負荷分散を導入する。ロードバランサの選定条件を以下に示す。

- メッセージ発生率の最大値よりも大きいロードバランス性能を有する機種であること
- 負荷分散先のサーバとのセッション維持機能を有すること

（3） L3 スイッチ及びルータ

・ スイッチング容量及びパケット転送速度は、十分な処理能力を持った機種であること

（4） ファイアウォール

・ 接続サーバ数と Web アクセスユーザ数を合わせた程度の同時接続が可能であること
・ 性能試算で算出した通信帯域より大きい処理能力を有すること
・ 冗長化できる機能を有すること
・ 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

４．アーキテクチャ設計

４.１ ネットワーク構成検討

４.１.１ 全体構成

大企業自社運用及び中小企業自社運用の場合は、内部のネットワークから本システムを利用することを想定している。ASP 運用の場合は、利用者はインターネット経由で接続して本システムを利用する。

また、本システムは、あらかじめ登録されているデータ交換先（発注者システム、受注者システム、入荷拠点システム、出荷拠点システム）のシステムと接続してメッセージの送受信を行う。

拠点（各システム）間接続の全体構成イメージを図４．１に示す。

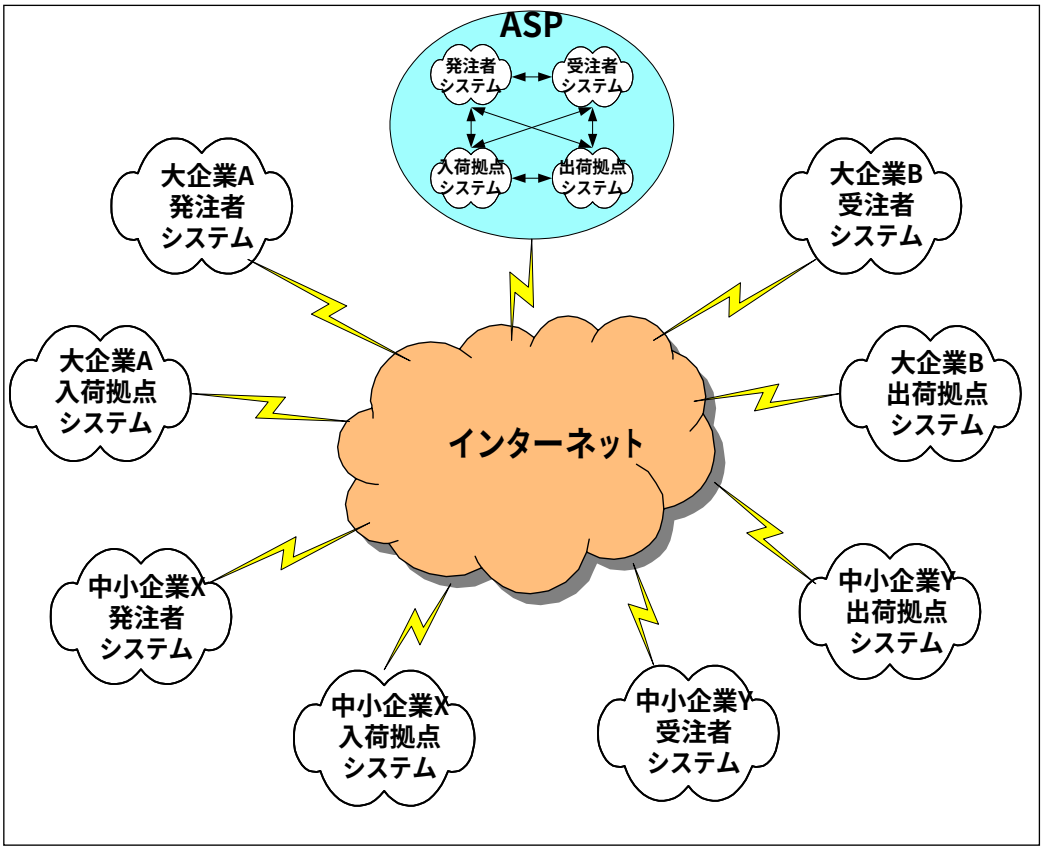

図４．１　全体構成イメージ

4.1.2 物理構成図（ASP 運用）

「運用条件書・運用設計書」のハードウェアの信頼性・拡張性要件で規定されている構成を反映し、かつ、ルータ・リンク・ネットワーク経路を二重化する。ネットワーク物理構成例を図４．２に示す。

WWWサーバ、Web 業務サーバ、通信サーバ、BM サーバは負荷の状況に応じてシステムの拡張が容易な構成とする。

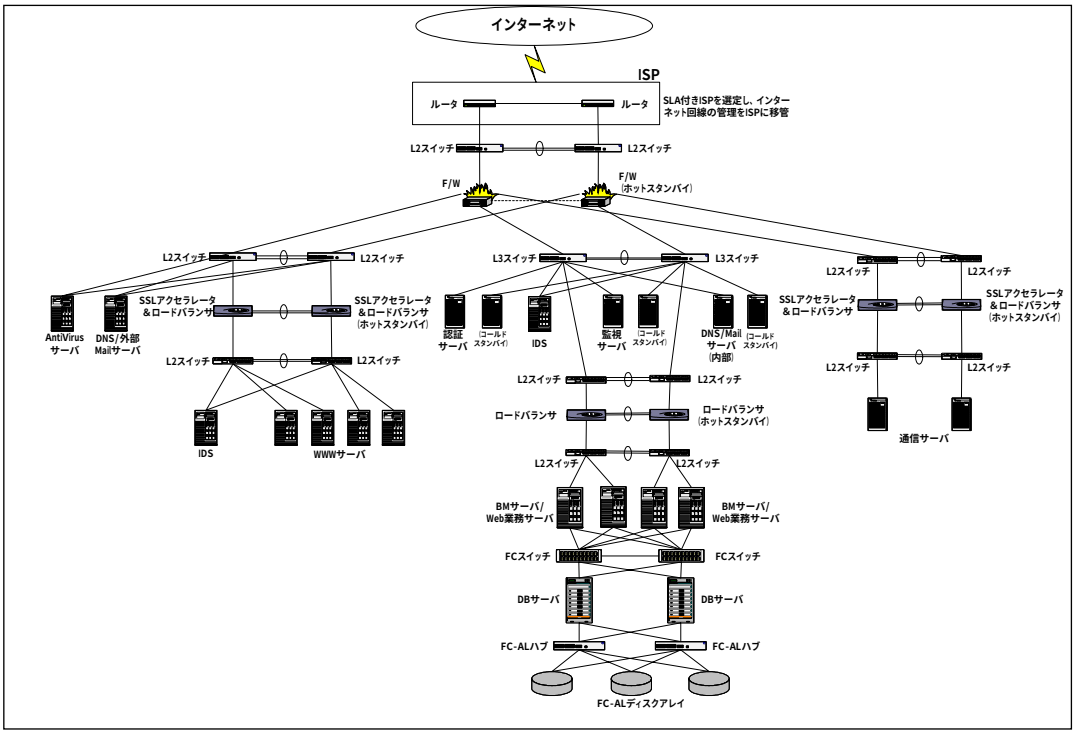

図４．２　物理構成図（ASP 運用）

4.1.3 物理構成図（大企業自社運用）

大企業自社運用の場合のネットワーク物理構成イメージを図４．３に示す。

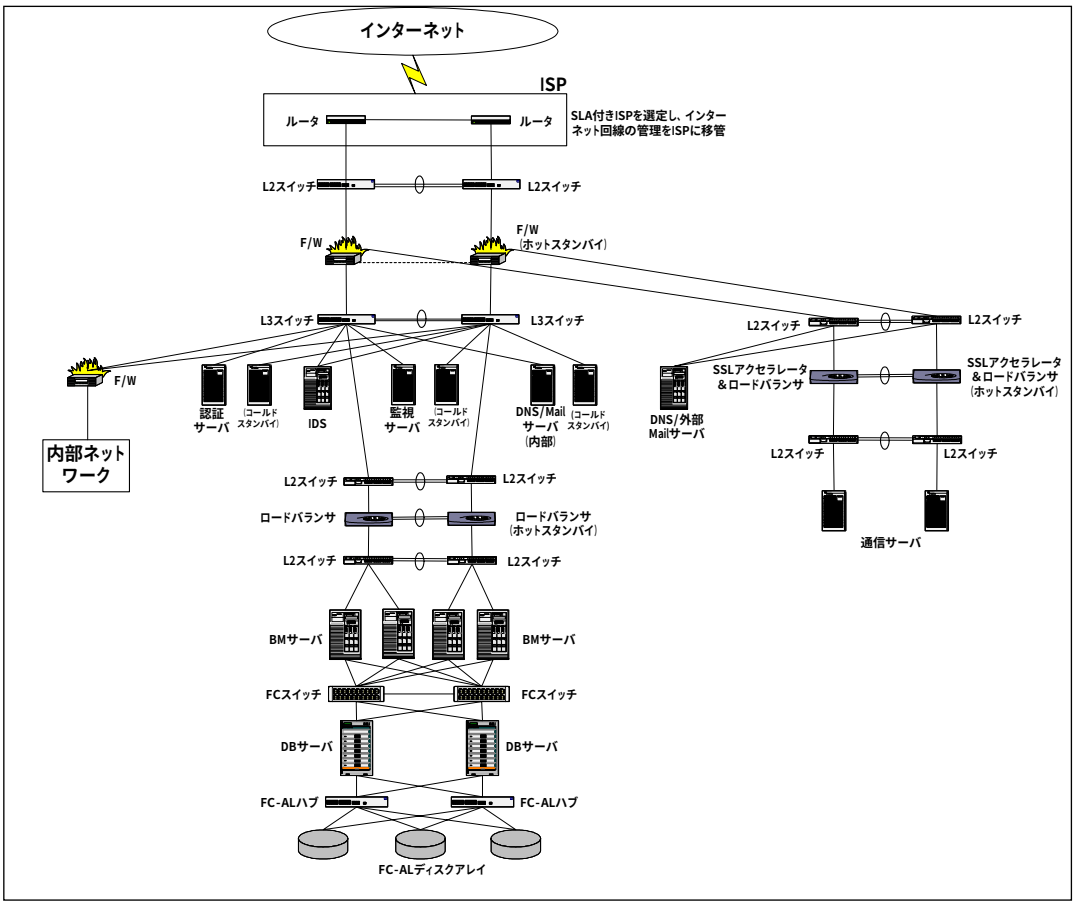

図４．３　物理構成図（大企業自社運用）

４.１.４ 物理構成図（中小企業自社運用）

中小企業自社運用の場合のネットワーク物理構成イメージを図４．４に示す。

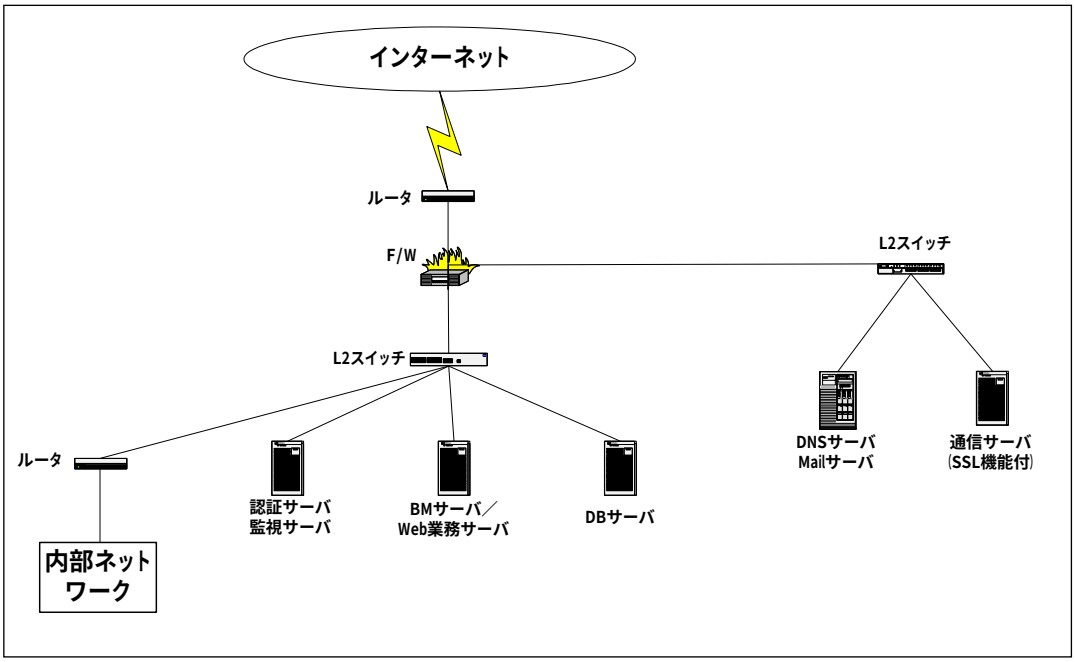

図４．４　物理構成図（中小企業自社運用）

4.2 使用するネットワーク機能

4.2.1 ルータの二重化

ルータを二重化するために、VRRP（Virtual Router Redundancy Protocol）または、HSRP（Hot Standby Routing Protocol）のいずれかを利用する。

（1） VRRP

VRRP に対応した複数のルータを 1 つのグループに所属させ、通常はそのうち 1 つのルータが通信を行なうが、そのルータが障害を起こした時に同グループに属するルータが自動的に通信を受け継ぐ。同一グループで通信を行なうルータは 1 台に限られるが、1 つのルータが複数のグループに所属することもできるため、設定によって負荷分散を同時に実現することも可能。

（2） HSRP

各ルータに一つずつ IP アドレスを振った上で、多重化されているルータ全体にさらに 1 つ IP アドレスを割り当て、通信する際は全体用の IP アドレスに要求を送信する。通常の通信に使用されるルータは 1 つで、使用中のルータが停止すると自動的に別のルータ 1 台が停止したルータに代わって通信を行なう。切り替えに必要な時間は数秒程度。

なお、VRRP と HSRP は相互運用性がないので注意が必要である。

4.2.2 リンクの二重化

FEC（Fast Ether Channel）や GEC（Giga Ether Channel）は、スイッチ間で Ethernet リンクを複数本束ね、論理的に 1 本の回線として処理する技術である。

仮に 1 本のケーブルが切れても、ネットワークトポロジの変化無しに数秒以内に残りの回線で処理されるようになる。

4.2.3 ネットワーク経路の二重化

STP（Spanning Tree Protocol）は、レイヤ 2 レベルで経路を二重化するのに使用する。通常の STP は、障害時の切り替えに数十秒の時間がかかるが、

より短時間で切り替えが可能な RSTP（高速スパニングツリー：Rapid STP）や MSTP（多重スパニングツリー：Multiple STP）の利用も検討する。

4.2.4 ルーティングプロトコル

本システムを ASP 運用する場合は、ダイナミック・ルーティングの OSPF（Open Shortest Path First）、EIGRP（Enhanced Interior Gateway Routing Protocol)などのルーティングプロトコルの利用を検討する。

ダイナミック・ルーティングは、経路情報がルーティングプロトコルにより動的に学習されるため、管理に要する手間を省くことができる。また、ネットワークの更新をダイナミックに反映できるため、利用不能となった経路あてのトラフィックを速やかに破棄したり、適切な迂回経路を選択させたりすることができる。

4.2.5 負荷分散機能

負荷分散機能は、1 台のサーバが過負荷になるのを防止するため、トラフィックを同一のアプリケーションが稼動しているサーバのグループにダイナミックに振り分けて、そのサーバのグループをあたかも 1 台のサーバであるかのようにネットワークに対して見せる機能である。

本システムでは、「運用条件書・運用設計書」にも記載されているように、WWWサーバ、Web 業務サーバ、BM（ビジネスモジュール）サーバ及び通信サーバは、負荷分散することで信頼性・拡張性を向上させる。

4.2.6 SSL アクセラレータ

HTTP の暗号化処理はサーバの CPU を消費するため、専用機（SSL アクセラレータ）を導入し、暗号化処理の高速化を図る。

本システムでは、Web 業務サーバ及び通信サーバの処理能力の低下防止と HTTPS の高速化を実現するために、SSL アクセラレータを導入する。

4.2.7 サーバ接続の二重化

サーバに接続されたスイッチが二重化されている場合で、サーバを二重化しない場合は、各スイッチからサーバに配線してサーバ接続の二重化（ネットワークインターフェースの二重化）を検討する。

4.3 ISP 接続の二重化

ISP 接続を二重化し、信頼性・拡張性を確保する。また、ISP 接続に必要なネットワーク機器の予備機も準備しておく。

なお、インターネット回線の品質向上のため、SLA（Service Level Agreement）付き ISP を選定するか、異なる複数の ISP 業者を利用することを検討する。

ISP 接続図例を以下に示す。

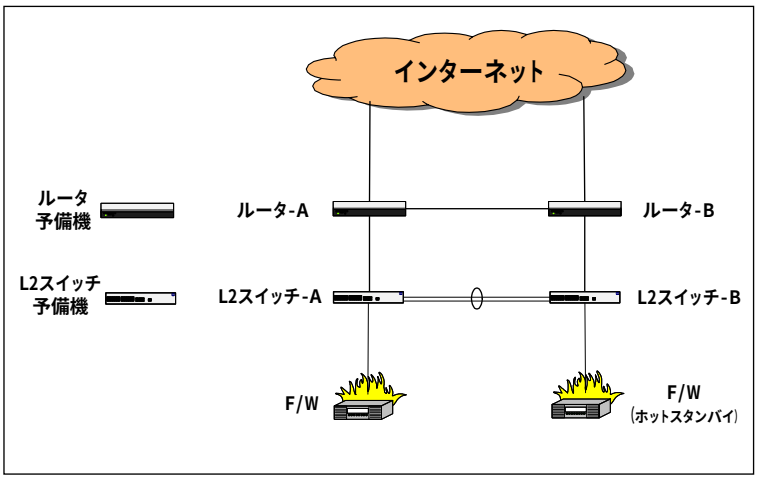

図４．５　ISP 接続イメージ

4.4 論理設計

4.4.1 IP アドレス設計

本システムでは、ルータ～ファイアウォール間、及び、DMZ に配置したサーバネットワーク機器にはグローバル IP アドレスを使用する。

ファイアウォールより内側はローカル IP アドレスを使用する。

4.4.2 ルーティング設計

本システムにおいて、STP、負荷分散機能、VRRP／HSRP を使用する箇所を下図に示す。

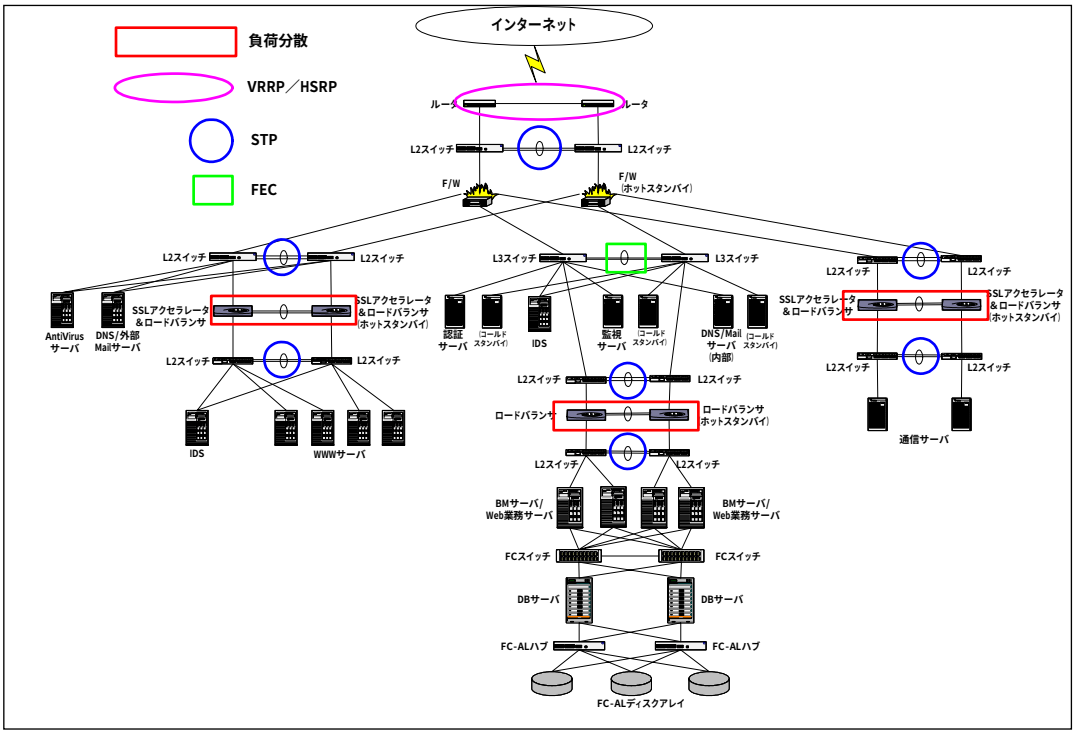

図４．６　STP 等の使用箇所

4.5 物理設計

4.5.1 LAN 配線設計

ASP 運用の場合に使用するケーブル及び速度は以下を基準とする。

表４．１　使用ケーブル及び速度（ASP 運用）

規格	適用部位	使用ケーブル	速度
Fiber Chanel、または、1000BASE-SX	BM サーバ～FC-AL ディスクアレイ間	FC ケーブル、または、マルチモード光ファイバー	1000Mbps
100BASE-TX、または、1000BASE-T	上記以外	CAT5E（エンハンスドカテゴリー５）	100Mbps、または、1000Mbps

4.5.2 機器設計

ネットワーク機器は基本的に二重化する。また、全てのネットワーク機器について、予備の機器を準備する。

ネットワーク機器はそれぞれ２台配置することで、機器構成を二重化し、かつ、経路を二重化する。

4.6 データフロー

4.6.1 正常時のデータフロー

ASP 運用における正常時のデータフローを以下に示す。

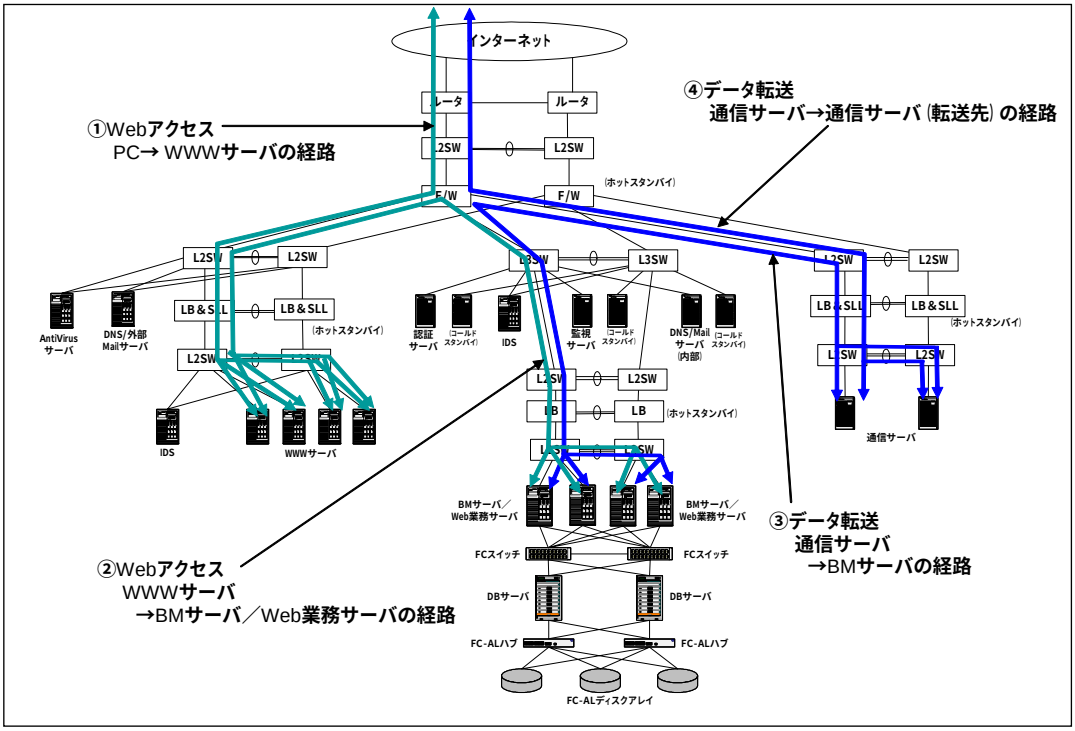

図４．７　正常時のデータフロー

４.６.２ 異常時のデータフロー

（１） ファイアウォールが故障した場合

ファイアウォールが故障した場合のデータフローを以下に示す。

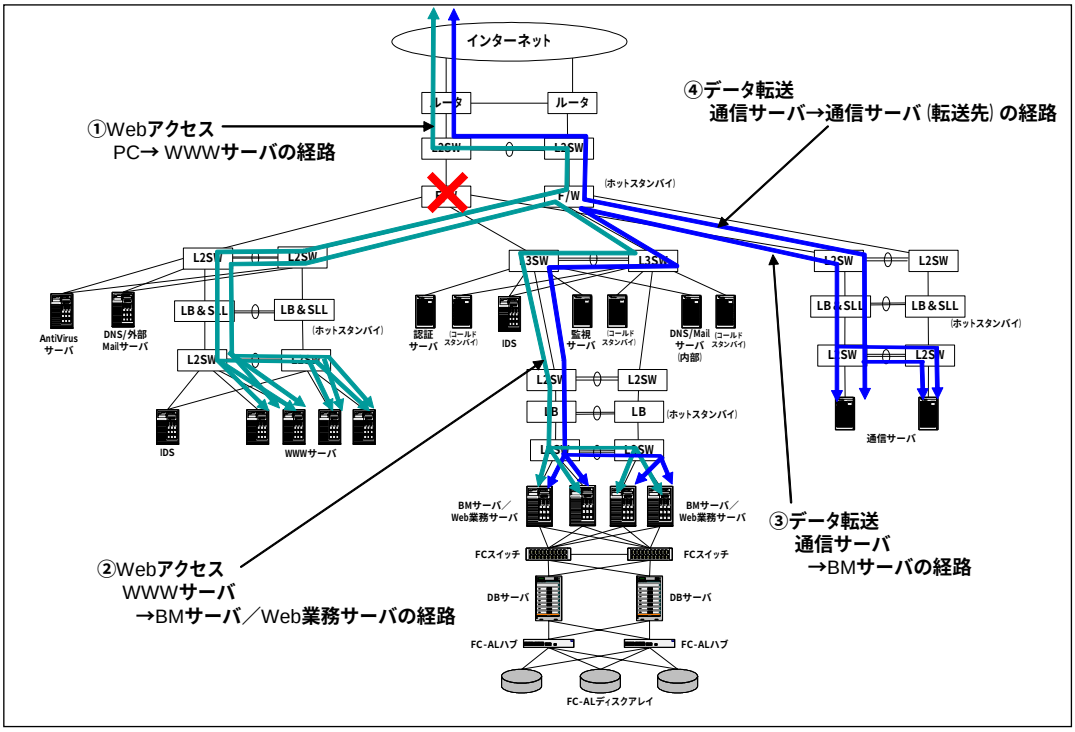

図４．８　ファイアウォールが故障した場合のデータフロー

（２） WWW サーバ側のロードバランサ＆SSL アクセラレータが故障した場合

WWW サーバ側のロードバランサ＆SSL アクセラレータが故障した場合のデータフローを以下に示す。

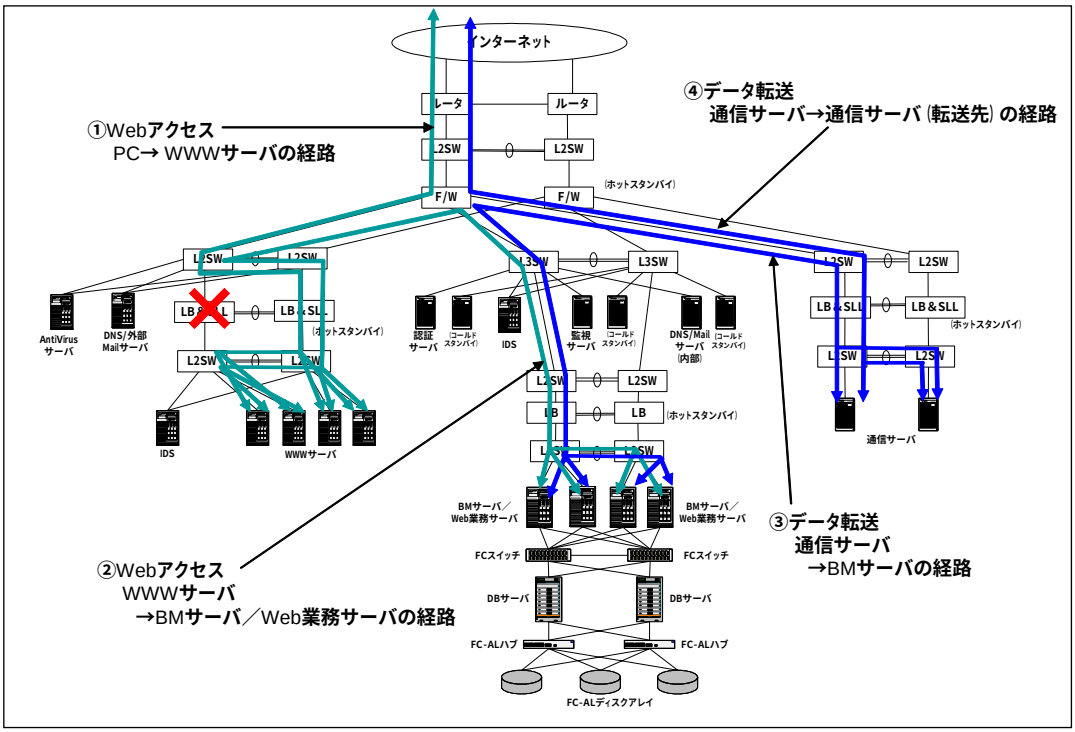

図４．９　ロードバランサ＆SSL アクセラレータ（WWW サーバ側）が故障した場合のデータフロー

（３） 内部の L3 スイッチが故障した場合

内部の L3 スイッチが故障した場合のデータフローを以下に示す。

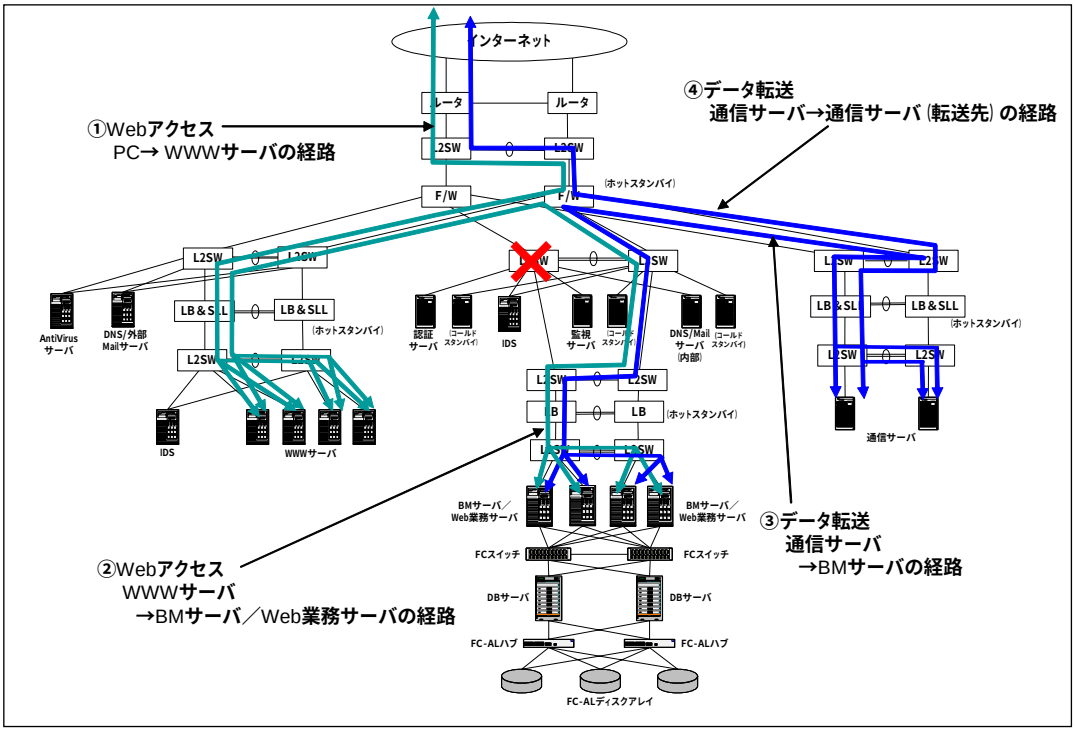

図４．１０　内部の L3 スイッチが故障した場合のデータフロー

（４） 通信サーバ側のロードバランサ＆SSL アクセラレータが故障した場合

通信サーバ側のロードバランサ＆SSL アクセラレータが故障した場合のデータフローを以下に示す。

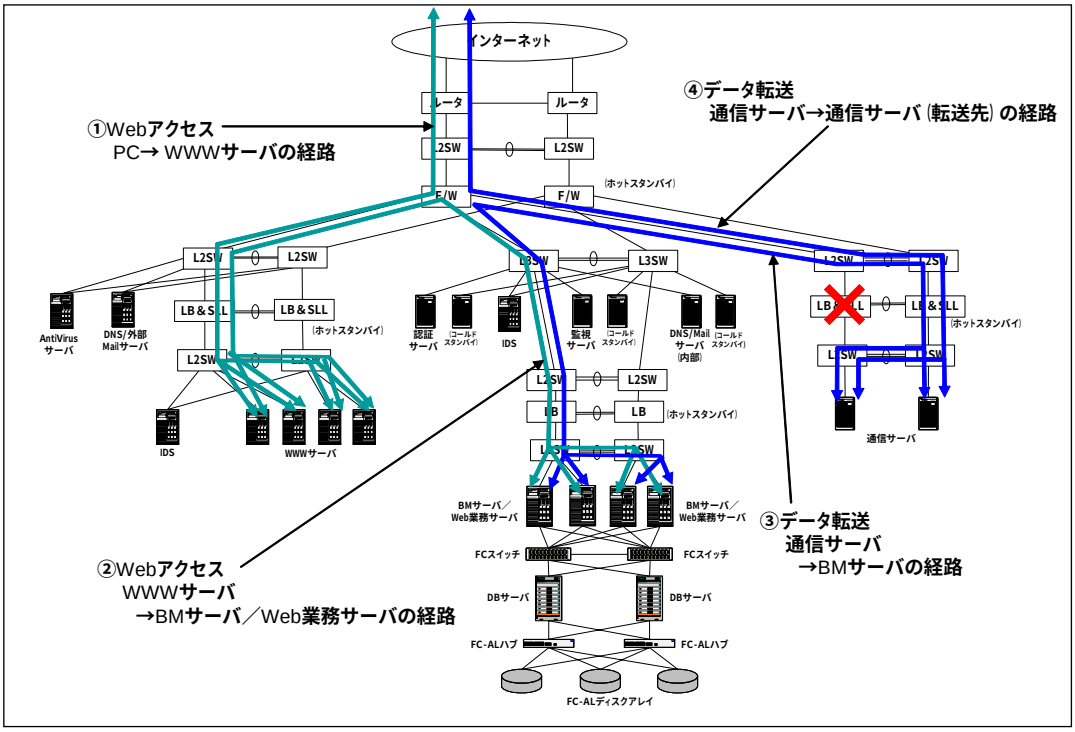

図４．１１　ロードバランサ＆SSL アクセラレータ（通信サーバ側）が故障した場合のデータフロー

５．運用条件

５.１ システムの運用条件

システムの運用条件については、「運用条件書・運用設計書」で記述されているが、ネットワークの運用条件と関連する事項は以下のとおり。

（１） 運用時間

ASP サイトのサービス時間は 24 時間 365 日を基本とする。ただし、システムメンテナンスや臨時メンテナンスについては計画停止することを許容する。

（２） 許容停止時間

ASP サイトの許容停止時間は２時間以内とする。ただし、データセンタに接続されている外部ネットワークの障害は、サイトの許容停止時間に含めないものとする。

（３） 運用体制

運用監視機能と連動し、障害を迅速に検知可能な体制を 24 時間確保するとともに、障害通知から一次切分～エスカレーション、復旧まで、業務停止時間を最小限にとどめるための体制を取るものとする。

5.2 ネットワーク監視

5.2.1 ネットワークの監視方法

監視対象であるサーバ及びネットワーク機器に対して、Ping 送信と SNMP により状態を監視する。Ping 送信の応答が規定回数以上ない場合には、障害と判断して運用管理者に通知する。

5.2.2 ネットワーク監視項目

ネットワークの監視項目は以下のとおりとする。

- Ping による死活監視（サーバ、ネットワーク機器）
- IDS（Intrusion Detection System）による不正アクセス監視
- ファイアウォールのアクセスログ監視
- ポート接続監視
- トラフィック監視
- ネットワーク機器の CPU・メモリ使用率の監視

5.2.3 ネットワーク監視の構成

ネットワーク監視の構成イメージ（一部の機器は省略）を以下に示す。なお、監視用に別途セグメントを設け監視サーバを配置することを推奨とする。

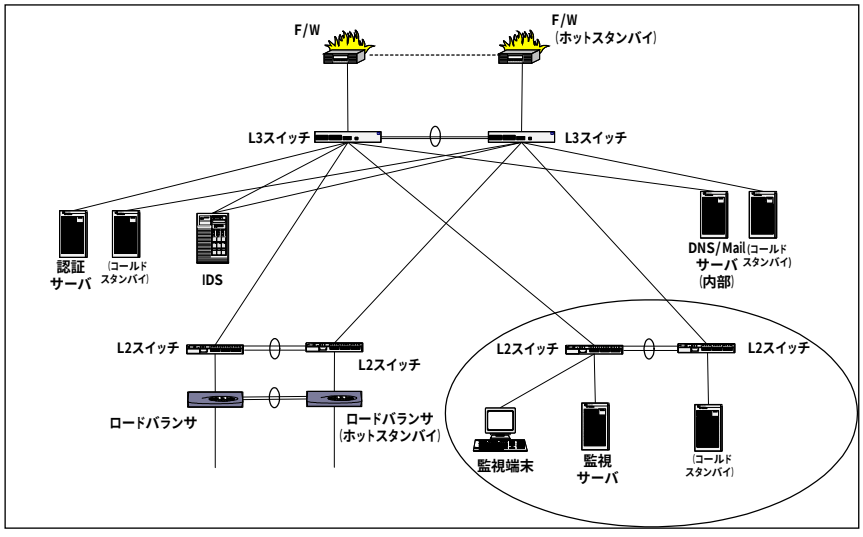

図５．１　ネットワーク監視の構成例

5.3 DNS

ネットワーク内は、プライマリ及びセカンダリ DNS サーバを利用して名前を解決する。

5.4 ネットワーク運用管理

ネットワーク障害が発生した場合の業務停止時間を最小限にするには、24時間の運用・監視体制とネットワークの運用上の管理業務（運用管理、障害管理、構成管理、性能管理、セキュリティ管理）が必要となる。

表５．１　ネットワーク運用上の管理業務

管理項目	業務の内容
運用管理	ネットワークを効率良く、円滑かつ安全・確実に利用できるようにネットワーク稼動状況等を監視・管理する。
障害管理	ネットワークに対し発生する障害を迅速に検出して対応する。障害記録など管理する。
構成管理	ネットワークを構成する資源（ネットワーク機器類)、構成情報、接続関係、設定情報などを管理する。
性能管理	ネットワークによるサービスの提供レベルを落とさないように、性能の監視を行うとともに性能に関する情報を収集･管理する。
セキュリティ管理	セキュリティリスクからネットワークを保護する。

以下に、各管理業務の具体的な内容について記述する。

（1） 運用管理

運用管理業務は、通常時運用、障害時運用、保守に分かれる。通常運用時に何らかの障害が発生して、通常時運用が困難な場合には障害時運用を適用する。

以下に、本システムでの各運用業務を示す。

表５．２　運用状態と作業内容

状態	作業内容
通常時運用	稼動状況監視、ネットワーク監視、ウイルス監視、IDS 監視、ログ監視（ファイアウォール等のアクセスログ）
障害時運用	情報収集、一次切り分け／一次対応、障害連絡、エスカレーション、障害報告／記録
保守	パスワード変更、証明書登録・削除・更新、パッチ適用、ソフトウェアバージョンアップ、設定情報変更、メンテナンス計画立案

通常時運用の各監視については、24 時間 365 日体制で行うものとする。何らかの異常（障害や不正アクセス等）が検知された場合の処置方法を記した手順書を整備しておく。同様に、保守時のパスワード変更や証明書登録・削除・更新手順などについても手順書を整備しておく。

また、証明書の有効開始・終了時刻、CRL の有効期限及びログの生成時刻等の不整合が、セキュリティ上重大な問題を引き起こす場合があるので、NTP を利用して各機器の時刻を統一する。なお、NTP の調時元については、十分信頼のおけるタイムソースとする。

（２）　障害管理

ネットワークの障害には、完全に通信ができない、一部の通信だけできない、通常よりもレスポンスが遅いなど様々なパターンが考えられるが、先ずどのような状態を障害と判断するのかの基準を明確にする必要がある。想定される障害ごとに障害の確認方法、一次対応、エスカレーションの手順、予防方法、回避方法、調査すべきログなどを記した手順書を整備しておく。

（３）　構成管理

ネットワークを構成する各機器の設定情報及び接続情報を管理する。常に最新の状態に保つことが重要である。

ネットワークを構成する要素としては、ハブ、スイッチ、ルータなどがある。

（4） 性能管理

性能管理は、ネットワークの性能を一定のレベルに維持することを目的とする。ネットワーク性能を測るための項目としては、帯域幅、トラフィック量、各機器の CPU やハードディスクの使用率などが挙げられる。それぞれの項目ごとに、あらかじめ上限値（または下限値)、測定方法、測定間隔などを決めて監視する。上限値（または下限値）を超えた場合は、メール等で運用管理者に通知するようにする。また、基準値を超えた場合の対処方法について手順書を準備しておく。

本システムの場合、接続数が多くなれば、性能を一定のレベルに維持することが困難になることが予想される。システム拡張のタイミングについて計画を立てておく必要がある。

（5） セキュリティ管理

セキュリティ管理は、ウイルスや不正アクセスなどの脅威からネットワーク内の情報資産を保護することを目的とする。本システムを利用する企業またはＡＳＰ業者毎に、保護対象の資産およびその資産に対する脅威（リスク）を抽出し、脅威ごとの対策方針を明確にする。

以下にセキュリティ管理として明確にすべき項目を示す。

- ファイアフォールの設置とアクセスログの取得
- ネットワーク機器へのアクセス制御（アクセス可能な機器を限定する）
- トラフィックのモニタリング
- ネットワーク機器やサーバ間のルーティング
- IDS の設置とログの取得
- 外部ネットワークとのアクセス

６．セキュリティ設計

６.１ ネットワークに対する脅威および対策

「セキュリティ設計書」では、本システムに対する脅威全般について記述している。ここでは、ネットワークに関連する脅威である、サービス妨害、盗聴、改ざん、なりすましのそれぞれの対策について検討する。

（１） サービス妨害

サービス妨害攻撃（DoS attack： Denial of Service attack)は、コンピュータ資源やネットワーク資源が、本来のサービスを提供できない状態に陥れる攻撃である（独立行政法人情報処理推進機構　セキュリティセンターのネットワークセキュリティ関連用語集より)。

一般に DoS 攻撃の検知及び対策には十分なものは存在しないので、複数の対策を準備する。

① ファイアウォールによる DoS 対策

ファイアウォールの設定により、DoS 対策を行う。ファイアウォールの機能として、既知の DoS 攻撃（SYN Flood、Ping Of Death、IP Spoofing、LAND Attack、Smurf Attack 等）の対策を備えたものを選定する。

② IDS による DoS 対策

DoS 攻撃を検出できる IDS を選定する。なお、DoS 攻撃の検出方法として、登録されているシグネチャ（DoS 攻撃などの不正アクセスのパケットが持つパターン）とのマッチングを行っているものを選定した場合は、常に最新のシグネチャを登録しておく必要があるので、シグネチャの更新頻度高いものを選定する。

既知の DoS 攻撃に対しては、ファイアウォール、IDS でそれぞれ DoS 対策を実装するものとする。また、DoS 攻撃の標的となるセキュリティホールが発見された場合は、原則として速やかにパッチを適用するものとする。

（2） 盗聴

インターネットはオープンなネットワークであり、ネットワークに流れる情報（データ）は、第三者に盗み見られる可能性がある。本システムの場合、発注データ等の業務データ、電子メールが該当する。

盗聴の危険性に対して、本システムではサーバ間のデータ交換では相互認証で接続相手先を特定し、通信路（インターネット上）を SSL で暗号化することで対応する。利用者が Web 経由でアクセスする場合も同様に通信路を SSL で暗号化する。

また、電子メールでは、発注データ等の業務に関わるデータを送信しないようにする。

（3） 改ざん

電子データはデジタル情報であるため、比較的容易に内容を書き換えることができる。このため、悪意を持ったユーザによって情報を不正に改ざんされる可能性がある。本システムでは、発注データ等が途中で改ざんされて相手に届くといったことが考えられる。

通信経路上の改ざん対策として、SSL による暗号化を導入する。データベースの改ざん対策としては、データベースへ直接アクセスできるホストを限定すること、データベースへのアクセスの際に必要となる認証情報を厳重に管理すること、ネットワークへのアクセスを適切にコントロールすることで対応する。

また、その他の改ざん対策として、データそのものの暗号化や取引データへの署名等も挙げられる。これらは本システムの必須要件ではないが、推奨項目として検討すべき対策である。

（4） なりすまし

ネットワーク上では、第三者が当事者になりすまして不正な行為を行う可能性がある。例えば、正規ユーザの認証情報（パスワードなど）を不正に取得し、その認証情報を利用するなどが考えられる。

なりすましの危険性への対策は、認証及び適切なアクセスコントロールにより対応するが、利用者側が認証情報を厳密に管理することが前提となる。

6.2 ライフサイクルによるセキュリティ対策

ネットワークのセキュリティ対策はシステム全体のセキュリティ対策と整合を取る必要がある。個々の対策を有機的に結合し、効果的なものとするには、下表に示す一連のライフサイクル（設計、構築、運用、評価）により継続的にセキュリティ対策を強化していく必要がある。

表6．1　セキュリティライフサイクル

項目	内容
設計	セキュリティポリシー設計／改訂 システム設計／見直し
構築	システム構築 管理策構築
運用	ポリシーの運用管理システム構築 システムマネージメント（防御、検出、対応）
評価	セキュリティ監査 リスク監査 セキュリティ分析