

後期高齢者医療 広域連合電算処理システム

信頼性設計書

目次

1 概要	1
2 冗長化	3
2.1 サーバの冗長化	3
2.2 ネットワーク機器の冗長化	7
2.3 ネットワーク経路の冗長化	11
2.4 ディスクの冗長化	13
2.5 電源の冗長化	16
2.6 プロセッサの冗長化	17
2.7 ストレージの冗長化	18
3 ストレージ	21
3.1 ストレージの適用	21
4 負荷分散	23
4.1 負荷分散の適用	23
5 停電対策	25
5.1 無停電電源装置の導入	25
6 稼働時間	27
6.1 サーバダウン許容時間	27

1 概要

本書は「後期高齢者医療広域連合電算処理システム(以下、「標準システム」という)」の信頼性設計について記載する。

信頼性設計書は、システムが提供するサービスや機能をユーザが継続して利用できることを目的とし、以下の 4 点について記載している。

- ・サーバ、ネットワーク機器などの冗長化
- ・ストレージの導入
- ・サーバの負荷分散処理
- ・停電に備えた無停電電源装置の導入

本書で説明する内容の一覧を表 1-1 に示す。

表 1-1 本書での説明内容一覧

No.	項目	説明内容
1	冗長化	サーバ、ネットワーク機器、ネットワーク経路、ディスク、電源、プロセッサおよびストレージの冗長化について記載する。
2	ストレージ	ストレージを適用するサーバについて記載する。
3	負荷分散	Web サーバおよび AP サーバの負荷分散について記載する。
4	停電対策	停電対策として、無停電電源装置の導入について記載する。
5	稼働時間	各サーバのダウン許容時間について記載する。

本書では、標準システムを構成する機器を表 1-2 に定義する。

表 1-2 機器の定義

No.	区分	機器名
1	サーバ機器	Web サーバ
2		AP サーバ
3		DB サーバ
4		帳票サーバ
5		AD サーバ
6		運用管理サーバ
7		バックアップサーバ
8		(検証用)Web サーバ
9		(検証用)AP サーバ
10		(検証用)DB サーバ
11		(検証用)帳票サーバ
12	ネットワーク機器	ファイアウォール
13		L3 スイッチ
14		L2 スイッチ
15		負荷分散装置
16	ストレージ機器	ハードディスク
17		ディスクアレイコントローラ
18		HBA (Host Bus Adapter)
19		キャッシュメモリ
20		FC(Fibre Channel) スイッチ
21		FC(Fibre Channel) ケーブル

※標準システムにおいて、市区町村側機器の信頼性設計については対象外とする。各広域連合で必要と判断された場合は検討のうえ、設計を行う。

第 2 章以降では、表 1-1 のそれぞれの項目についての詳細を説明する。

2 冗長化

本章では、次の項目の冗長化について記載する。

- ・サーバ
- ・ネットワーク機器
- ・ネットワーク経路
- ・ディスク
- ・電源
- ・プロセッサ
- ・ストレージ

2.1 サーバの冗長化

(1) 目的

サーバの冗長化は、サーバの機能やサービスを継続して提供することを目的とする。

(2) 概要

同じ機能を持つサーバを複数台設置してサーバの冗長化を行う。これにより、1 つのサーバに障害が発生した場合、縮退しサーバの機能を継続して提供する。

(3) 対象範囲

サーバの冗長化の対象範囲について表 2-1 に示す。

表 2-1 サーバの冗長化の対象範囲

No.	サーバ	実施の有無
1	Web サーバ	○
2	AP サーバ	○
3	DB サーバ	○
4	帳票サーバ	○
5	AD サーバ	○
6	運用管理サーバ	△
7	バックアップサーバ	△
8	(検証用)Web サーバ	△
9	(検証用)AP サーバ	△
10	(検証用)DB サーバ	△
11	(検証用)帳票サーバ	△

凡例 ○：必須

△：任意

(4) 方式

(a) Web サーバの冗長化方式

標準システムでは、負荷分散装置を前提とし Web サーバは Active-Active 構成とする。詳細は「4. 負荷分散」を参照のこと。

(b) AP サーバの冗長化方式

標準システムでは、負荷分散装置を前提とし AP サーバは Active-Active 構成とする。詳細は「4. 負荷分散」を参照のこと。

(c) DB サーバの冗長化方式

標準システムでは、Oracle RAC 構成を前提とし、DB サーバは Active-Active 構成とする。通常時には 2 台の DB サーバ#1、#2 がそれぞれ処理 A、処理 B を並列で実行する。DB サーバ#1 に障害が発生した場合、DB サーバ#2 だけで処理を行い、DB サーバ#1 の復旧後は再び並列で処理を行う。ただし、DB サーバ#1 で実行中の処理 A は DB サーバ#2 には引き継がれないため、処理 A は再実行する必要がある。

DB サーバの冗長化方式について図 2-1 に示す。

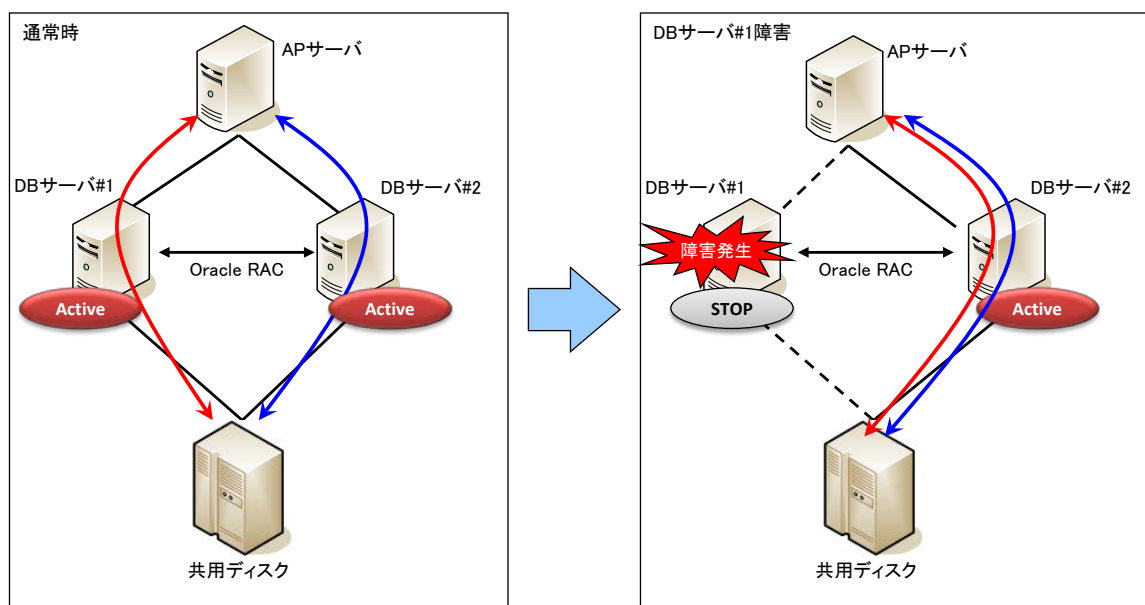


図 2-1 DB サーバの冗長化方式

(d) 帳票サーバの冗長化方式

標準システムでは、Windows 標準機能の WSFC (Windows Server Failover Clustering) を前提とし、Active-Standby 構成とする。通常時は帳票サーバ#1 で処理を行い、帳票サーバ#1 に障害が発生した場合、帳票サーバ#2 に切り替えて処理を行う。WSFC は、Active Directory ドメインサービスが必要となる。

帳票サーバの冗長化方式について図 2-2 に示す。

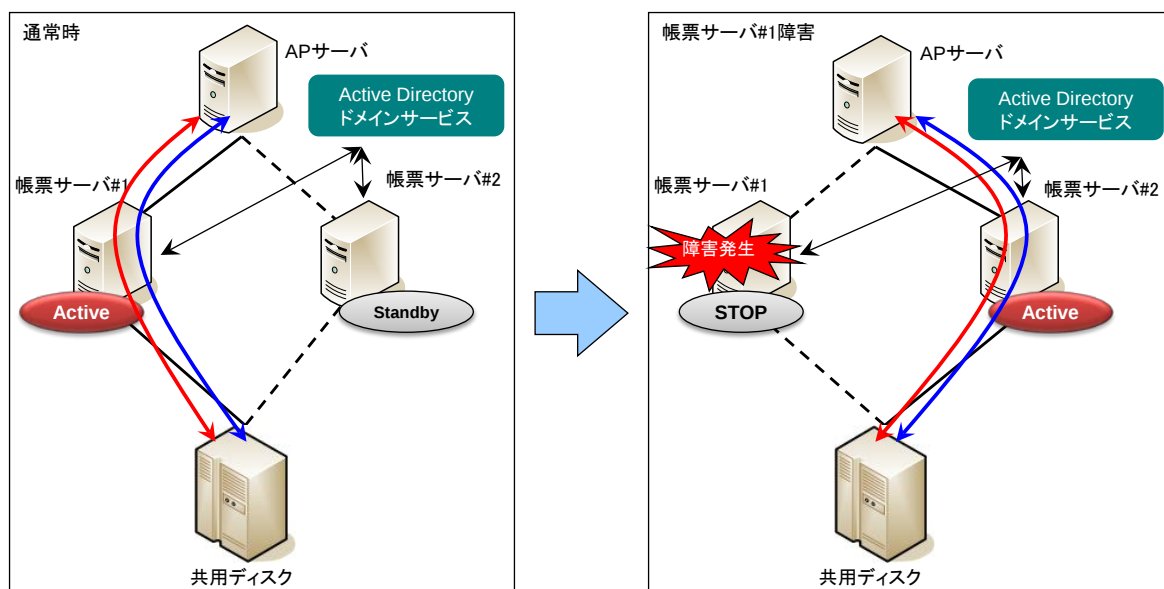


図 2-2 帳票サーバの冗長化方式

(e) AD サーバの冗長化方式

標準システムでは、Active Directory の機能による Active-Active 構成とする。通常時には 2 台の AD サーバ#1、#2 で認証を行う。AD サーバ#1 に障害が発生した場合、AD サーバ#2 だけで認証を行う。AD サーバ#1 の復旧後は、再び並列で認証を行う。Active Directory による AD サーバの冗長化方式について図 2-3 に示す。

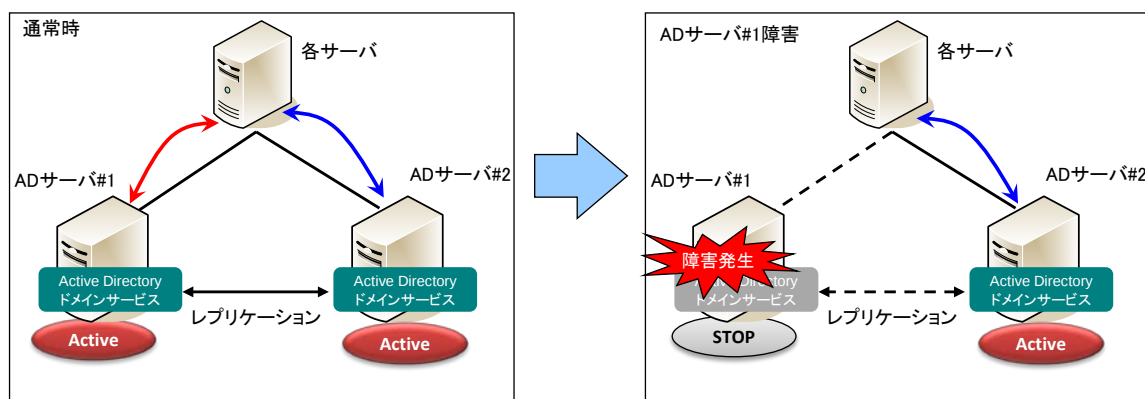


図 2-3 AD サーバの冗長化方式

2.2 ネットワーク機器の冗長化

(1) 目的

ネットワーク機器の冗長化は、ネットワーク機器を多重化することによって、一方の機器に障害が発生した場合でもネットワークサービスを継続して提供することを目的とする。

(2) 概要

広域連合内のネットワーク機器について二重化を行う。

(3) 対象範囲

ネットワーク機器の冗長化の対象範囲について表 2-2 に示す。

表 2-2 ネットワーク機器の冗長化の対象範囲

No.	ネットワーク機器	実施の有無
1	ファイアウォール	○
2	L3 スイッチ	○
3	L2 スイッチ	○
4	負荷分散装置	○

凡例 ○：必須

ネットワーク機器の冗長化の対象範囲について図 2-4 に示す。太線内が冗長化の対象範囲である。

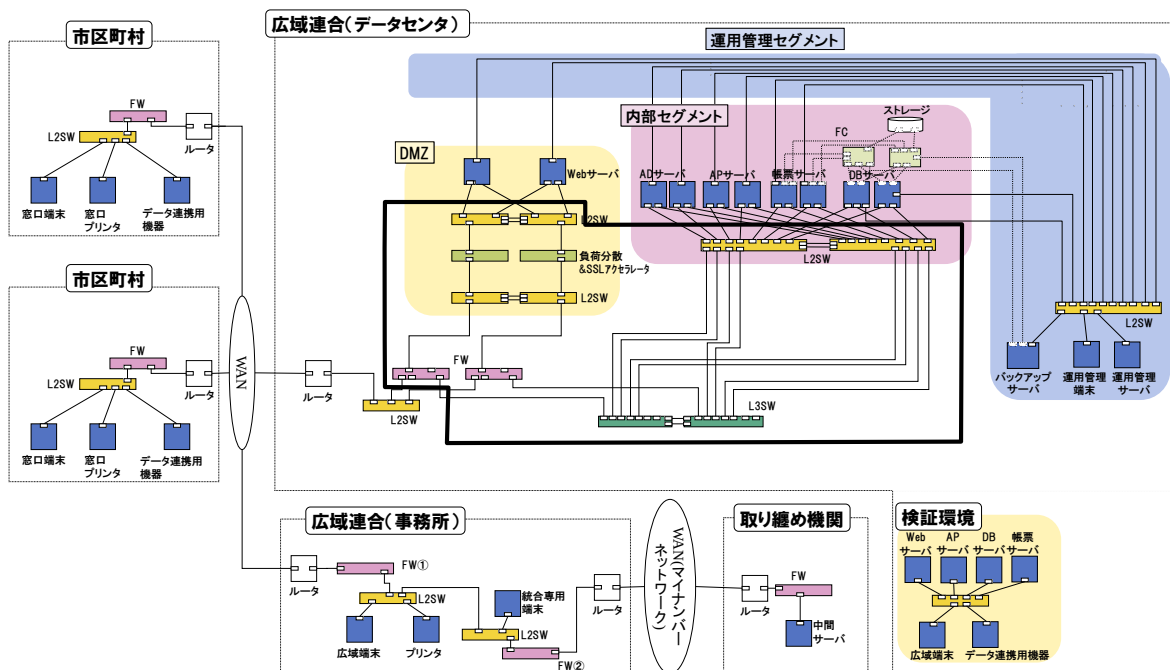


図 2-4 ネットワーク機器の冗長化の対象範囲

(4) 方式

広域連合内のネットワーク機器の二重化を行い、一方の機器に障害が発生した場合でも、通信サービスを継続して提供する。

(a) ファイアウォール

ファイアウォールは、Active-Standby 構成とし、通常時にはファイアウォール#1 がファイアウォール機能を提供する。ファイアウォール#1 の障害時にはファイアウォール#2 が Active となり、ファイアウォール機能を提供する。ファイアウォールの冗長化方式について図 2-5 に示す。

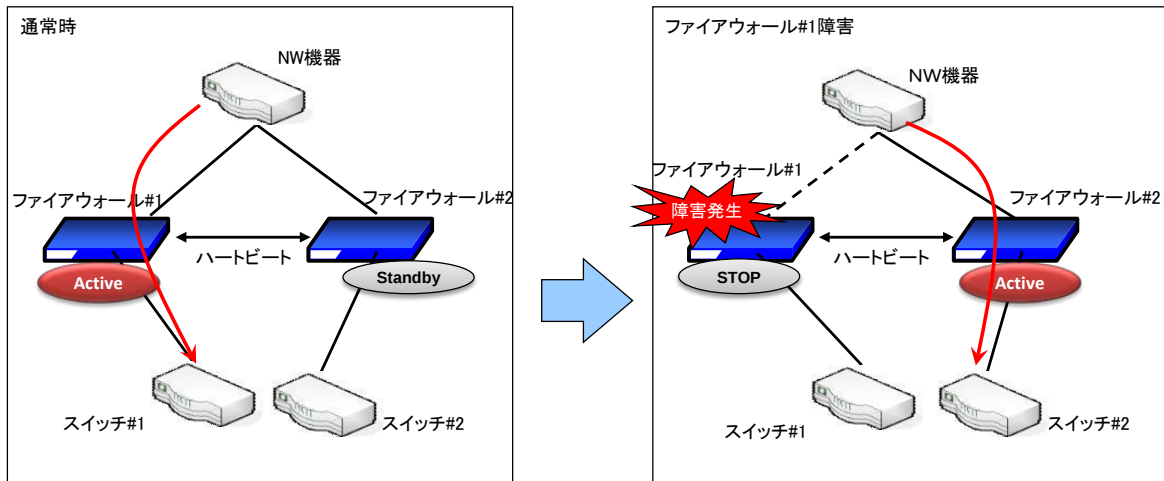
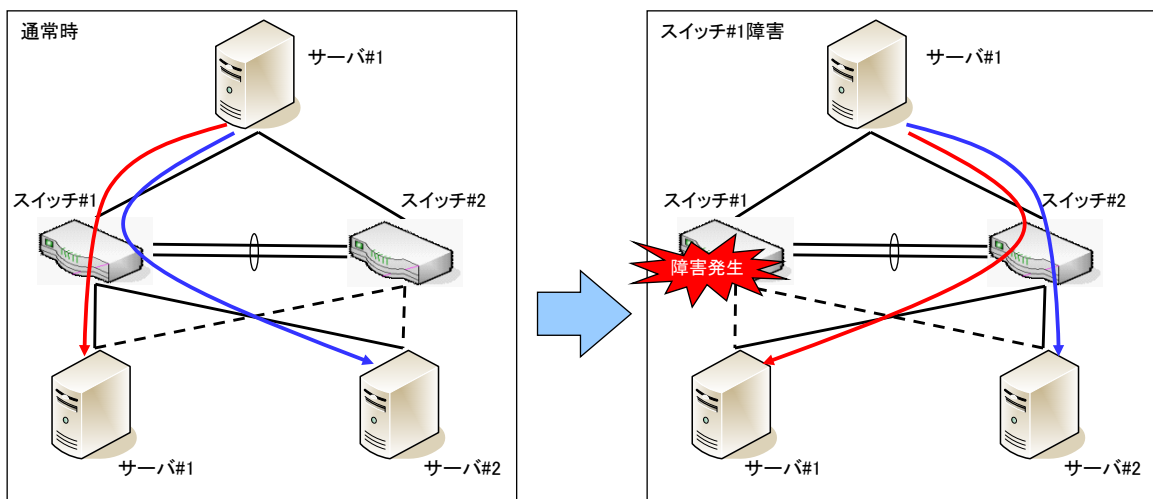


図 2-5 ファイアウォールの冗長化方式

(b) L2 スイッチおよび L3 スイッチ

L2 スイッチ、L3 スイッチ(以下「スイッチ」という)は、二重化構成とし、通常時には適切な経路を選択して通信を行う。一方のスイッチに障害が発生した場合には、もう一方のスイッチのみで継続して通信サービスを提供する。スイッチの冗長化方式について図 2-6 に示す。



凡例 0 : リンクアグリゲーション

図 2-6 スwitchの冗長化方式

(c) 負荷分散装置の冗長化

負荷分散装置は、Active-Standby 構成とし、通常時には負荷分散装置#1 が端末からのリクエスト受付を行う。負荷分散装置#1 の障害時には負荷分散装置#2 が Active となり、端末からのリクエスト受付を行う。

負荷分散装置の冗長化方式について図 2-7 に示す。

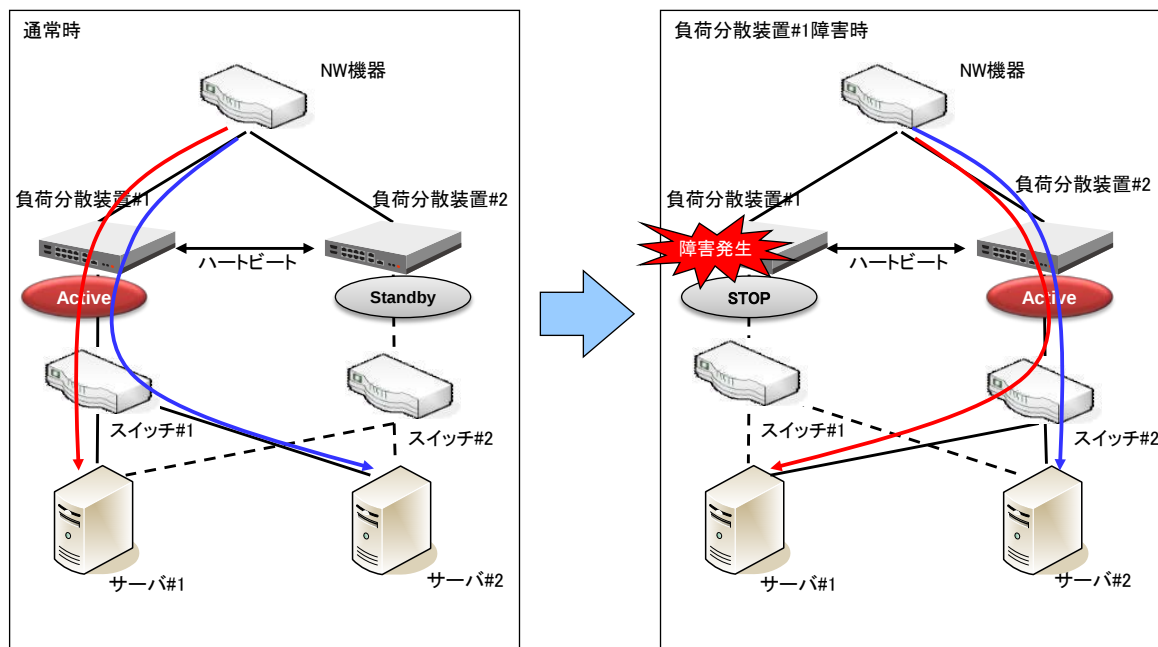


図 2-7 負荷分散装置の冗長化方式

2.3 ネットワーク経路の冗長化

(1) 目的

ネットワーク経路の冗長化は、各ネットワーク機器とサーバ間のネットワーク経路を冗長化することによって、一方の機器に障害が発生した場合でも、通信サービスを継続して提供することを目的とする。

(2) 概要

広域連合内のネットワーク機器およびサーバ機器について、ネットワーク経路の二重化を行う。

(3) 対象範囲

ネットワーク経路の冗長化の対象範囲について表 2-3 に示す。

表 2-3 ネットワーク経路の冗長化の対象範囲

No.	機器名	実施の有無
1	Web サーバ	○
2	AP サーバ	○
3	DB サーバ	○
4	帳票サーバ	○
5	AD サーバ	○
6	運用管理サーバ	△
7	バックアップサーバ	○
8	(検証用)Web サーバ	△
9	(検証用)AP サーバ	△
10	(検証用)DB サーバ	△
11	(検証用)帳票サーバ	△
12	ファイアウォール	○
13	L3 スイッチ	○
14	L2 スイッチ	○
15	負荷分散装置	○

凡例 ○：必須

△：任意

(4) 方式

(a) サーバ

サーバのネットワーク経路を冗長化するには、NIC(Network Interface Card)を2枚取り付け、チーミング設定を行う。一方の LAN に障害が発生した場合に、もう一方の LAN に通信を切り替える。これにより継続して通信サービスの提供が可能である。また、それぞれの NIC とスイッチ間の接続を異なるスイッチにすることで高信頼化を図る。NIC の冗長化方式について図 2-8 に示す。

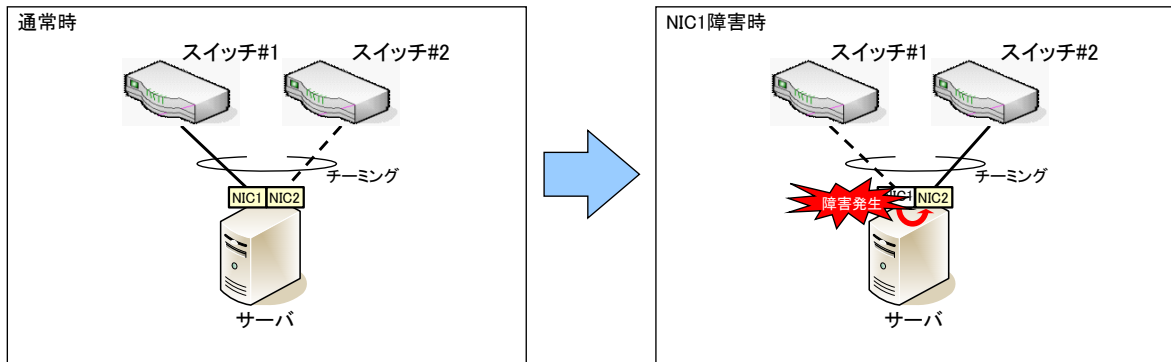


図 2-8 NIC の冗長化方式

(b) ネットワーク機器

ネットワーク機器の経路の冗長化するには、各ネットワーク機器間を複数経路とする。一方の機器またはポートに障害が発生した場合に、ネットワーク経路を変更する。これにより継続して通信サービスの提供が可能である。ネットワーク機器接続の冗長化方式について図 2-9 に示す。

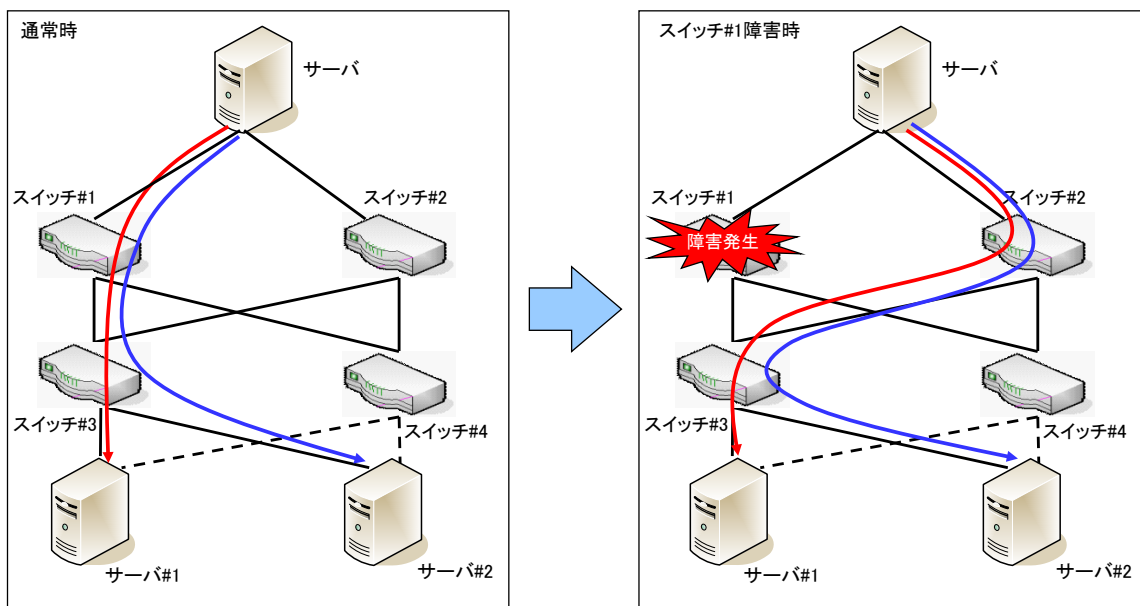


図 2-9 ネットワーク機器接続の冗長化方式

2.4 ディスクの冗長化

(1) 目的

ディスクの冗長化では、各サーバの内蔵ディスクおよびストレージディスクに障害が発生した場合に、RAID 構成およびスペアディスクを用いることで継続してデータを提供することを目的とする。

(2) 概要

RAID1、RAID1+0、RAID5 およびスペアディスクを導入することにより、ディスクの冗長化を行う。

(3) 対象範囲

ディスクの冗長化の対象範囲について表 2-4 に示す。

表 2-4 ディスクの冗長化の対象範囲

No.	サーバ	実施の有無	
		内蔵ディスク	ストレージ ディスク
1	Web サーバ	○	△
2	AP サーバ	○	△
3	DB サーバ	○	○
4	帳票サーバ	○	○
5	AD サーバ	○	△
6	運用管理サーバ	○	△
7	バックアップサーバ	○	○
8	(検証用)Web サーバ	△	△
9	(検証用)AP サーバ	△	△
10	(検証用)DB サーバ	△	△
11	(検証用)帳票サーバ	△	△

凡例 ○：必須

△：任意

(4) 方式

各広域連合で RAID を用いたディスク構成を検討し、ディスク単体の故障によるデータ破壊の防止およびデータの信頼性を高めた設計とする。

主な RAID 構成のメリットおよびデメリットについて表 2-5 に示す。

表 2-5 主な RAID 構成のメリット、デメリット

No.	RAID 構成	概要	メリット	デメリット
1	RAID1	複数のディスクに同じデータを書き込む方式。	・ディスクの信頼性に優れる。 ・最低 2 本のディスクから構成可能なため、導入コストが低い。	・2 倍の領域が必要なため、容量の利用効率が悪い。
2	RAID1+0	複数のディスクに同じデータを書込み、さらにデータをブロック単位に分割して並列に書き込む方式。	・ディスクの信頼性とデータの書込み、読み性能に優れる。	・2 倍の領域が必要なため、容量の利用効率が悪い。 ・最低 4 台のディスクが必要なため、導入コストが RAID1/RAID5 と比較して高い。
3	RAID5	複数のディスクにデータとパリティデータ（冗長コード）を同時に分散して書き込む方式。	・ディスクの信頼性とデータの読み性能に優れ、容量の利用効率が良い。	・データの書き込み時に、パリティ計算のオーバーヘッドが発生する。 ・最低 3 台のディスクが必要なため、導入コストが RAID1 と比較して高い。
4	RAID6	RAID5 の方式に加え、パリティデータを 2 重に生成し、異なるディスクに書き込むことで信頼性を高めた方式。	・RAID5 のメリットに加え、構成するディスクのうち 2 台に障害が発生しても稼働を継続できる。	・データの書き込み時に、パリティデータを 2 重に生成するため RAID5 より書き込みパフォーマンスが低下する。 ・最低 4 台のディスクが必要なため、導入コストが RAID1/RAID5 と比較して高い。

標準システムの内蔵ディスクおよびストレージディスクの RAID 構成例について表 2-6 に示す。

表 2-6 標準システムの RAID 構成例

No.	ディスク	サーバ	標準システム RAID 構成	構成理由
1	内蔵 ディスク	Web サーバ	RAID1	ディスク容量が小さいため、導入コストを優先。
2		AP サーバ		
3		DB サーバ		
4		帳票サーバ		
5		AD サーバ		
6		運用管理サーバ		
7		バックアップサーバ	RAID5 スペアディスク ※	ディスク容量が大きいいため、容量の利用効率を優先。
8	ストレージ ディスク	DB サーバ (データベース領域)	RAID1+0 スペアディスク ※	業務データが格納されるため、性能を優先。
9		帳票サーバ (帳票データ格納領域)		
10		バックアップサーバ (バックアップ領域)	RAID5 スペアディスク ※	バックアップデータが格納されており、業務性能に影響がないため、容量の利用効率を優先。

※ スペアのディスクを用意する。これは、1 本のディスクに障害が発生した場合、残りのディスクのデータから障害ディスクのデータを生成し、RAID 構成を継続するためのディスクである。

2.5 電源の冗長化

(1) 目的

電源の冗長化は、一方の電源に障害が発生した場合に、もう一方の電源で継続して電力を供給することを目的とする。

(2) 概要

広域連合内のサーバについて電源の二重化を行う。

(3) 対象範囲

電源の冗長化の対象範囲について表 2-7 に示す。

表 2-7 電源の冗長化の対象範囲

No.	サーバ	実施の有無
1	Web サーバ	○
2	AP サーバ	○
3	DB サーバ	○
4	帳票サーバ	○
5	AD サーバ	○
6	運用管理サーバ	○
7	バックアップサーバ	○
8	(検証用)Web サーバ	△
9	(検証用)AP サーバ	△
10	(検証用)DB サーバ	△
11	(検証用)帳票サーバ	△

凡例 ○：必須

△：任意

(4) 方式

標準システムでは、広域連合内のサーバについて電源の二重化を行う。電源ユニットは、一方の電源に障害が発生した場合でも、もう一方で電源供給を可能とする。

2.6 プロセッサの冗長化

(1) 目的

プロセッサの冗長化は、CPU を多重化することによって、一方の CPU に障害が発生した場合に、もう一方の CPU で処理を行うことができる。

(2) 概要

各サーバの CPU を二重化することにより信頼性を高める。

(3) 対象範囲

プロセッサの冗長化の対象範囲について表 2-8 示す。

表 2-8 プロセッサの冗長化の対象範囲

No.	サーバ	実施の有無
1	Web サーバ	○
2	AP サーバ	○
3	DB サーバ	○
4	帳票サーバ	○
5	AD サーバ	○
6	運用管理サーバ	○
7	バックアップサーバ	○
8	(検証用)Web サーバ	△
9	(検証用)AP サーバ	△
10	(検証用)DB サーバ	△
11	(検証用)帳票サーバ	△

凡例 ○：必須

△：任意

(4) 方式

本システムでは、各サーバについて CPU の二重化を行い、一方の CPU に障害が発生した場合でも、もう一方の CPU でサーバの動作を可能とする。

2.7 ストレージの冗長化

(1) 目的

ストレージは、ディスク、ディスクアレイコントローラ、HBA(Host Bus Adapter)、キャッシュメモリおよびFC(Fibre Channel)から構成される。それぞれの機器を冗長化することにより信頼性の向上を図る。

(2) 概要

ストレージの構成要素を冗長化する。

(3) 対象範囲

ストレージの冗長化の対象範囲について表 2-9 に示す。

表 2-9 ストレージの冗長化の対象範囲

No.	対象	構成要素	実施の有無
1	ストレージ	ディスク	○
2		ディスクアレイコントローラ	○
3		HBA	○
4		キャッシュメモリ	○
5		FC スイッチ	○
6		FC ケーブル	○

凡例 ○：必須

ストレージの構成図について図 2-10 に示す。

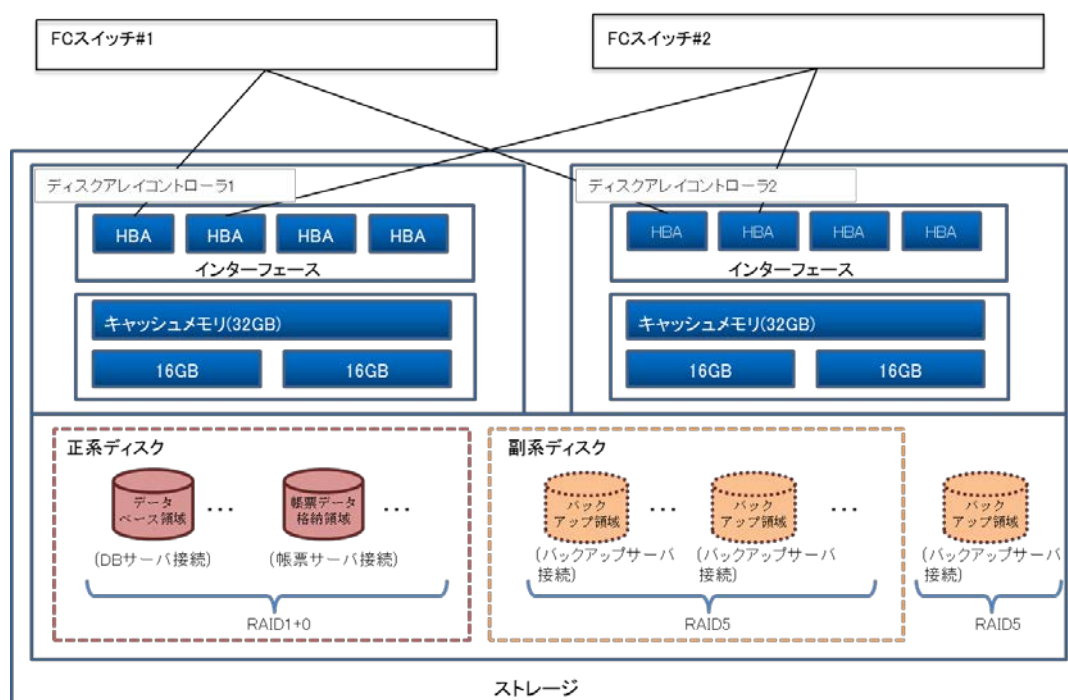


図 2-10 ストレージの構成図

(4) 方式

(a) ディスクの冗長化

各広域連合で RAID を用いたディスク構成を検討する。詳細については、「2.4 ディスクの冗長化」を参照のこと。

(b) ディスクアレイコントローラの冗長化

ディスクアレイコントローラとは、図 2-10 のディスクアレイコントローラ 1（基本コントローラ）およびディスクアレイコントローラ 2（二重化コントローラ）のことを示す。サーバから送られた情報を RAID に読み書きする際の I/O 制御などを行う。

ディスクアレイコントローラを二重化することによって、一方のコントローラに障害が発生した場合でもサーバからディスクへのアクセスが可能である。

(c) HBA の冗長化

HBA は、サーバをストレージに接続するために必要なアダプタであり、FC は、サーバをストレージに接続するケーブルである。FC および HBA を二重化することによって、一方の FC に障害が発生した場合でも通信の継続が可能である。

(d) キャッシュメモリの冗長化

キャッシュメモリは、サーバから送られてきたデータをディスクに格納するまでの間一時的に保存する。キャッシュメモリを二重化することにより、一方のメモリに障害が発生した場合でも、ディスクへのデータ書込みが可能である。

(e) FC スイッチの冗長化

サーバとストレージを結ぶ FC スイッチを二重化することで、一方の FC ケーブルまたは FC スイッチに障害が発生した場合に、サーバとストレージ間の通信を継続して提供する。FC スイッチの冗長化方式について図 2-11 に示す。

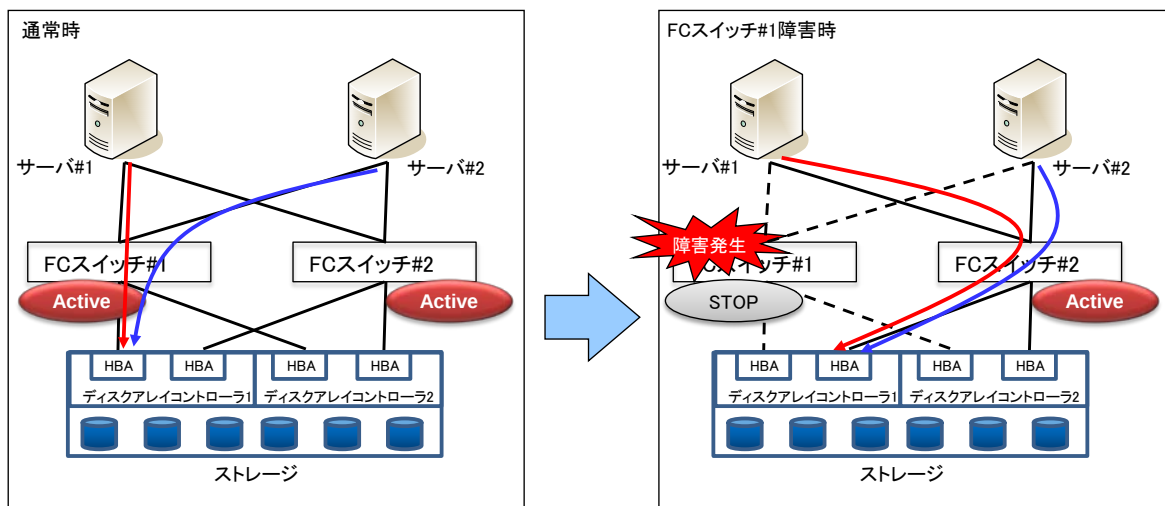


図 2-11 FC スイッチの冗長化方式

(f) FC ケーブルの冗長化

サーバと FC スイッチを結ぶ FC ケーブルを二重化することで、一方の FC ケーブルに障害が発生した場合に、サーバと FC スイッチ間の通信を継続して提供する。FC 経路の冗長化方式について図 2-12 に示す。

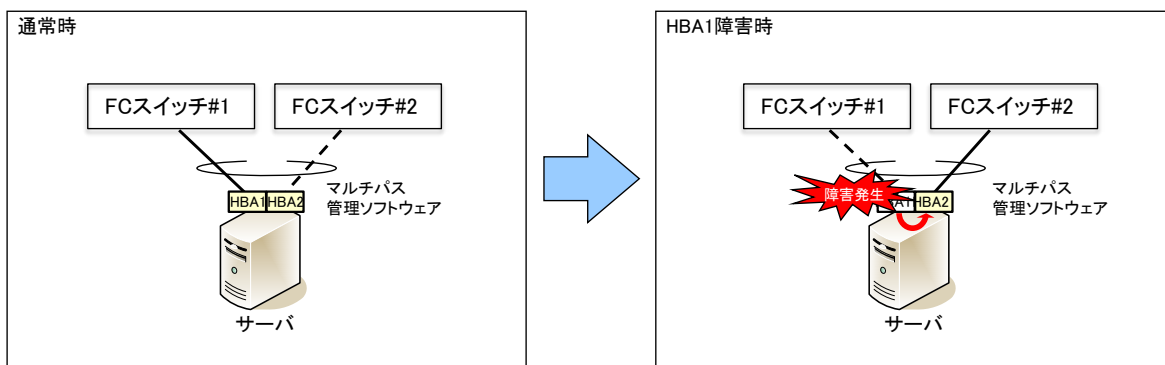


図 2-12 FC ケーブルの冗長化方式

3 ストレージ

本章では、ストレージを適用するサーバについて記載する。

3.1 ストレージの適用

(1) 目的

高信頼性のストレージをサーバのローカルディスクに割り当てることで、ディスクの信頼性の向上と、ディスクアクセスの高速化を図る。

(2) 概要

サーバのローカルディスクに高信頼性のストレージを割り当てる。

(3) 対象範囲

ストレージの適用の対象範囲について表 3-1 に示す。

表 3-1 ストレージの適用の対象範囲

No.	サーバ	実施の有無
1	Web サーバ	△
2	AP サーバ	△
3	DB サーバ	○
4	帳票サーバ	○
5	AD サーバ	△
6	運用管理サーバ	△
7	バックアップサーバ	○
8	(検証用)Web サーバ	△
9	(検証用)AP サーバ	△
10	(検証用)DB サーバ	△
11	(検証用)帳票サーバ	△

凡例 ○：必須

△：任意

サーバとストレージ間の接続について図 3-1 に示す。

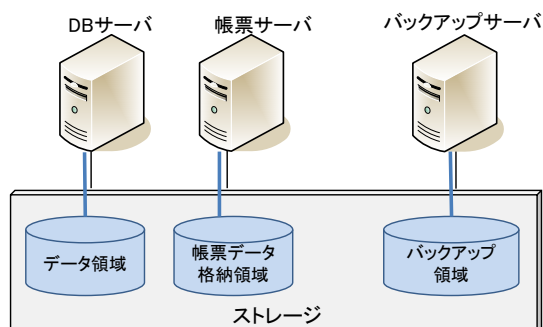


図 3-1 サーバとストレージ間の接続

(4) 方式

対象サーバからストレージに接続する。標準システムで規定するストレージに接続するサーバについて表 3-2 に示す。

表 3-2 標準システムで規定するストレージに接続するサーバ

No.	対象	使用用途
1	DB サーバ	データベース領域割り当てに使用。
2	帳票サーバ	帳票データ格納領域割り当てに使用。
3	バックアップサーバ	バックアップ領域割り当てに使用。
4	(検証用)DB サーバ	データベース領域割り当てに使用。
5	(検証用)帳票サーバ	帳票データ格納領域割り当てに使用。

4 負荷分散

本章では、Web サーバ、AP サーバの負荷分散方式について記載する。

4.1 負荷分散の適用

(1) 目的

同じ機能を持つ複数台のサーバに処理を分散して実行することで、一方のサーバへの負担を軽減することを目的とする。また、一方のサーバが故障した場合でも、縮退運転を行いサーバ機能の継続が可能である。

(2) 概要

負荷分散装置を用いて負荷分散を行う。

(3) 対象範囲

負荷分散を行うサーバの対象範囲について表 4-1 に示す。

表 4-1 負荷分散を行うサーバの対象範囲

No.	サーバ	実施の有無
1	Web サーバ	○
2	AP サーバ	○
3	DB サーバ	×
4	帳票サーバ	×
5	AD サーバ	×
6	運用管理サーバ	×
7	バックアップサーバ	×
8	(検証用)Web サーバ	△
9	(検証用)AP サーバ	△
10	(検証用)DB サーバ	×
11	(検証用)帳票サーバ	×

凡例 ○：必須

△：任意

×：不要

(4) 方式

(a) Web サーバの負荷分散方式

Web サーバについては、負荷分散装置を用いて負荷分散を行う。Web サーバの負荷分散方式について図 4-1 に示す。

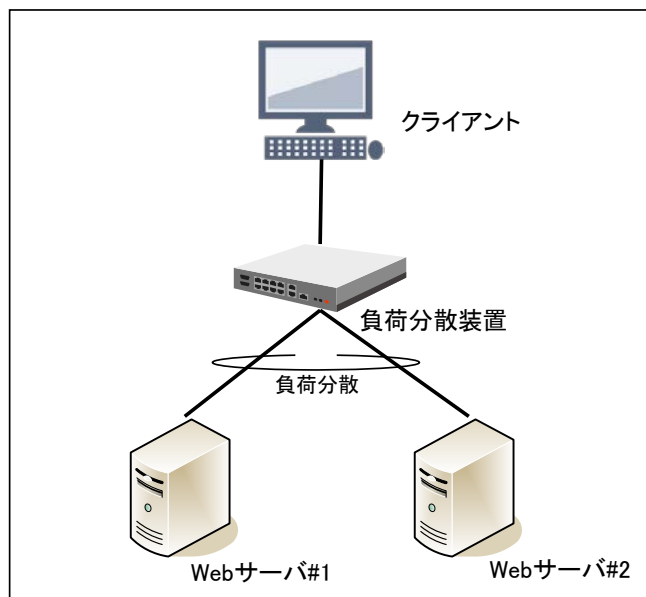


図 4-1 Web サーバの負荷分散方式

(b) AP サーバの負荷分散方式

AP サーバについては、負荷分散装置を用いて負荷分散を行う。AP サーバの負荷分散方式について図 4-2 に示す。

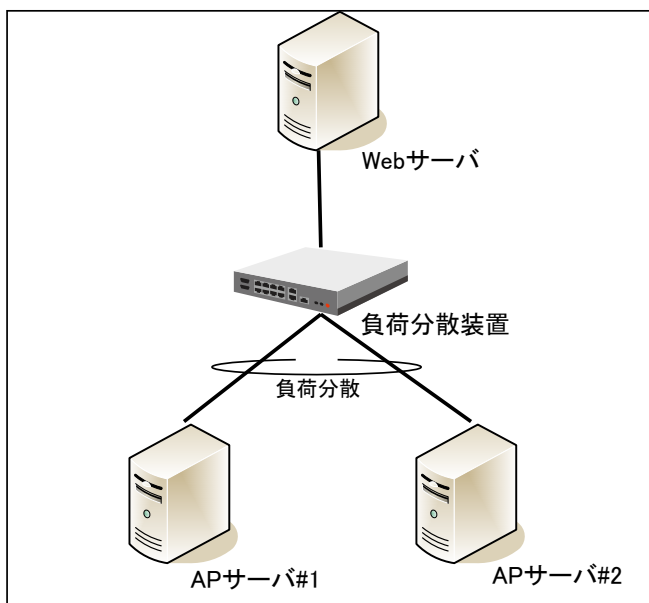


図 4-2 AP サーバの負荷分散方式

5 停電対策

本章では、停電対策として、無停電電源装置の導入について記載する。

5.1 無停電電源装置の導入

(1) 目的

無停電電源装置の導入は、停電時に安全にシステムを停止させることを目的とする。

(2) 概要

各サーバに無停電電源装置を設置し、停電時に電力を供給する。無停電電源装置を用いることで、停電時にも安全にシステムを停止させることができる。

(3) 対象範囲

無停電電源装置の対象範囲について表 5-1 に示す。

表 5-1 無停電電源装置の対象範囲

No.	サーバ	実施の有無
1	Web サーバ	○
2	AP サーバ	○
3	DB サーバ	○
4	帳票サーバ	○
5	AD サーバ	○
6	運用管理サーバ	○
7	バックアップサーバ	○
8	(検証用)Web サーバ	△
9	(検証用)AP サーバ	△
10	(検証用)DB サーバ	△
11	(検証用)帳票サーバ	△

凡例 ○：必須

△：任意

(4) 方式

無停電電源装置は、バッテリーを内蔵し、停電時でも一定時間システムに電力を供給する装置である。無停電電源装置から電源遮断の信号を受信したサーバは、即時停止処理に入る。実行中の処理はキャンセルされるため、電源復旧後にサーバを再起動し、処理を再実行する必要がある。無停電電源装置の概要について図 5-1 に示す。

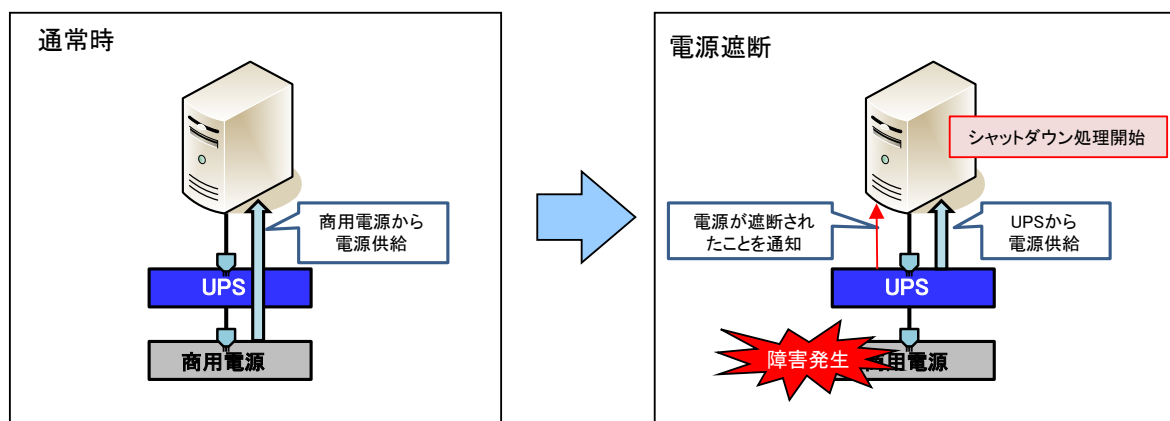


図 5-1 無停電装置の概要

6 稼働時間

本章では、各サーバのダウン許容時間について記載する。

6.1 サーバダウン許容時間

(1) 目的

サーバ障害が発生した場合の対処方法を規定することを目的とする。

(2) 概要

障害の原因によって対処方法が異なるため、適切なサーバダウン許容時間を設定する。

(3) 方式

サーバダウン許容時間の設定例について表 6-1 に示す。

表 6-1 サーバダウン許容時間の設定例

No.	現象	事象	対処	許容時間
1	ソフトウェア障害	パフォーマンス低下/ハングアップなどの一時的なソフトウェア障害。	該当ソフトウェアのプロセスを再起動し、必要であればサーバ再起動を行う。	発生検知から 1 時間以内。
		OS 破損などの致命的なソフトウェア障害。	サーバ再起動を行い、動作確認を行う。 ※再起動不可能な場合は、バックアップからのリストアを行う。	発生検知から 12 時間以内。
2	ハードウェア障害	CPU、メモリなど冗長化されている箇所のハードウェア障害。	保守ベンダに連絡し、点検/部品交換を行う。	発生検知から 6 時間以内。
		筐体などシステムの運用に影響がある致命的なハードウェア障害。	保守ベンダに連絡し、点検/部品交換を行い、必要であればバックアップからのリストアを行う。	発生検知から 24 時間以内。

【このページは白紙】