情報セキュリティ対策

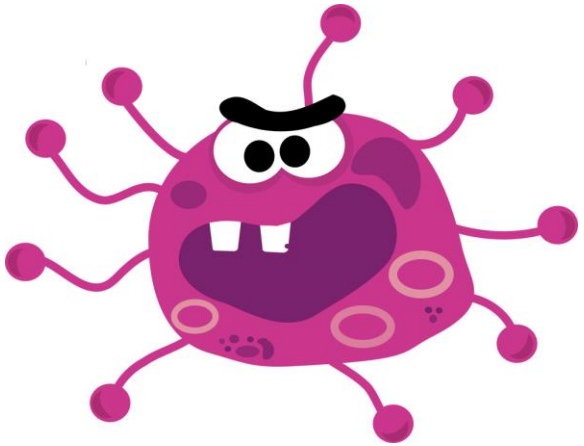
http://cobayasi.com/koza/security/6_taisaku.pdf

1. マルウェア対策
2. 不正アクセス対策

マルウェア対策

テキストP168-179

- マルウェアとは
- マルウェア対策



マルウェアとは

コンピュータウィルスを含む、悪意のあるソフトウェアの総称

- マルウェアの分類

呼び方	定　義
ウィルス（広義）	下の3種類のプログラム
ウィルス（狭義）	他のプログラムに寄生する
ワーム	他のプログラムに依存せず、独立して破壊活動し、自己増殖する
トロイの木馬	通常は、有用なプログラムとして動作するが、何かのきっかけで、破壊活動する

コンピュータウィルスとは

第3者のデータなどに対して、意図的に被害を及ぼすプログラム

- **コンピュータウィルスの3機能**

① 自己伝染機能
自分自身を、他のコンピュータにコピーして伝染させる

② 潜伏機能
特定の日時や処理回数に達するまで、症状を出さない

③ 発病機能
ファイルやデータ、プログラムを破壊したり、予期しない動作をする

コンピュータウィルスの感染経路

● 媒体感染
USBメモリなどの記憶媒体から感染する

- MBR(Master Boot Record)感染

ハードディスクのMBRやUSBメモリのブートセクタに潜伏し、システム起動時に感染する

● ネットワーク感染
インターネットなどのネットワークを媒体として感染する

- メール感染

メールに添付されている実行ファイル[.exe][.com]に潜伏し、このファイルを開くことで感染する

- ファイル共有感染
  ウィルスが実行したときに、アクセス可能なファイル（共有ファイル）に感染する

● マクロウィルス(マクロ型感染)
  ワープロソフト(ワードなど）や表計算ソフト（エクセル）などのマクロ機能で作られたファイルに感染して拡大する。
  比較的作成が容易で、なじみやすいソフトに感染しているんで、不注意になりがち。

その他のマルウェア

- スパイウェア

　パソコンやスマホの中の個人情報を収集して、クラッカーに送信するソフト。

　ゲームやユーティリティ（アプリケーションソフトの機能改善や操作改善するソフト）と一緒になっているので、ユーザが感染していることを知らないことが多い。

- ランサムウェア

　人質（例：コンピュータのロック、ファイルの暗号化）を取って身代金を要求するようなタイプ

- ポット

　乗っ取り（感染したコンピュータをリモート操作する）タイプ。
　乗っ取られたコンピュータを「ゾンビコンピュータ」と呼ぶ。

マルウェア対策

● ウィルス対策ソフト

ウィルス対策ソフトを導入する。

ウィルス対策ソフトは、パターンファイル（ウィルスの特徴を記述したデータベース）とコンピュータに入ってくるデータを、監視する。監視したデータに、ウィルスと同じパターンのデータがあると、ユーザに警告する。

● ウィルス対策ソフトの限界と対策

- パターンファイルにあるウィルスしか検出できない

新しいウィルスがパターンファイルに登録されるまでは危険。
パターンファイルを常に最新にする

- 圧縮データに弱い

ウィルスを圧縮すると、ファイルパターンでは検出できないので、解凍後に感染することがある

- ヒューリスティック法

　パターンファイルでは検出できないウィルスを検出するための方法で、実行ファイルの挙動を解析し、ライブラリファイルの書き換えなど、一般的なプログラムではあまり見られないような特異な挙動を探し出し、感染したウイルスによるもの推測する

- ビヘイビア法

　ウィルスであることが疑われるコード(プログラム)を実際に動作させ、その挙動によってウィルスどうかを判断する

- 検疫ネットワーク

　ウィルス検出専用のネットワーク。

　社内LANへ接続する前に、検疫ネットワークへ接続し、ウィルスが検出できなかった場合のみ、社内LANへの接続を許可する。

● ネットワークからの遮断

ウィルス感染の脅威を、完全に無効化するには、感染経路(ネットワークなど)を断ち切る。

システム設定する際には、「このコンピュータは、ネットワークに接続する必要があるのか」(ネットワーク接続の必要性)を考える。

● 感染後の対応

＜感染後の対応手順＞

- 初期対応

① 感染したシステムの停止
② ユーザへのアナウンス
③ ネットワークからの切断

- 復旧

④ ウィルスの影響範囲の特定
⑤ 復旧手順の確立と復旧作業

- 事後処理

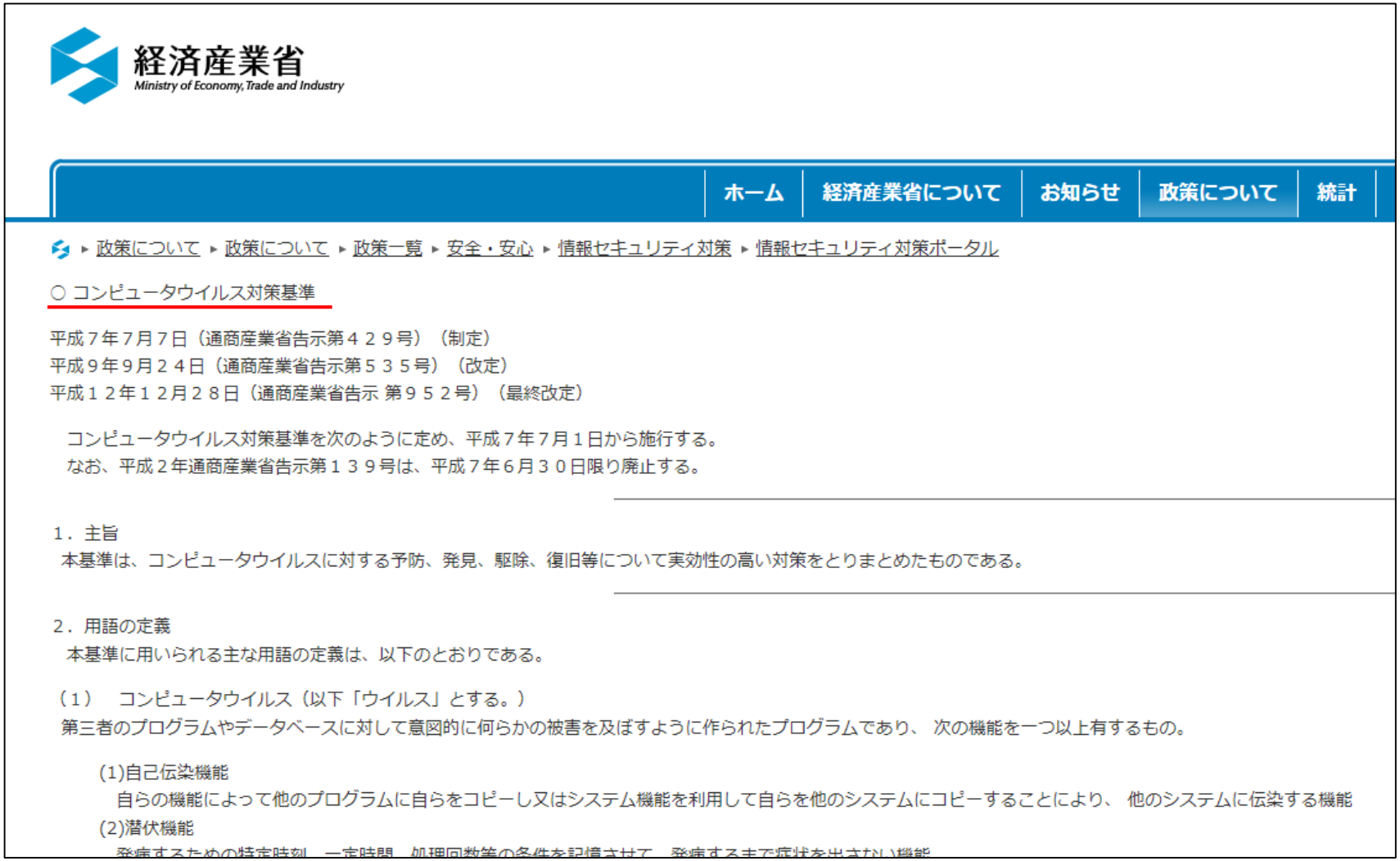
⑥ 原因の特定と対応策の策定
⑦ 関係機関への届出

- 初動対応
  - ✓ 感染したら、速やかに感染したシステムをネットワークから遮断する
  - ✓ ウィルス感染があったことを、他のユーザに通知する
  - ✓ 教育と対応マニュアルの整備
- 復旧
  - ✓ ウィルスの特定と復旧作業の着手
  - ✓ 普段からイメージファイル（OSやアプリケーションなどが入っているファイル）を作っておく
  - ✓ 復旧作業手順は記録に残す
- 事後処理
  - ✓ 再発防止策の策定と実施
  - ✓ 関係機関への通知

● ウィルス対策の基準

ウィルス対策は、経済産業省の「コンピュータウィルス対策基準」で定められている

http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm



経済産業省
Ministry of Economy, Trade and Industry

ホーム | 経済産業省について | お知らせ | 政策について | 統計

▸ 政策について ▸ 政策について ▸ 政策一覧 ▸ 安全・安心 ▸ 情報セキュリティ対策 ▸ 情報セキュリティ対策ポータル

○ コンピュータウイルス対策基準

平成７年７月７日（通商産業省告示第４２９号）（制定）
平成９年９月２４日（通商産業省告示第５３５号）（改定）
平成１２年１２月２８日（通商産業省告示 第９５２号）（最終改定）

コンピュータウイルス対策基準を次のように定め、平成７年７月１日から施行する。
なお、平成２年通商産業省告示第１３９号は、平成７年６月３０日限り廃止する。

１．主旨
本基準は、コンピュータウイルスに対する予防、発見、駆除、復旧等について実効性の高い対策をとりまとめたものである。

２．用語の定義
本基準に用いられる主な用語の定義は、以下のとおりである。

（１） コンピュータウイルス（以下「ウイルス」とする。）
第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、 次の機能を一つ以上有するもの。

(1)自己伝染機能
自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、 他のシステムに伝染する機能
(2)潜伏機能
発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能

① システムユーザ基準（18項目）
② システム管理者基準(31項目）
③ ソフトウェア供給者基準(21項目）
④ ネットワーク事業者基準(15項目）
⑤ システムサービス事業者基準(19項目）

4．システムユーザ基準

a．ソフトウェア管理

（1）ソフトウェアは、販売者又は配布責任者の連絡先及び更新情報が明確なものを入手すること。
（2）オリジナルプログラムは、ライトプロテクト措置、バックアップの確保等の安全な方法で保管すること。

b．運用管理

（1）外部より入手したファイル及び共用するファイル媒体は、ウイルス検査後に利用すること。
（2）ウイルス感染の被害が最小となるよう、システムの利用は、いったん初期状態にしてから行うこと。
（3）ウイルス感染を早期に発見するため、システムの動作の変化に注意すること。
（4）ウイルス感染を早期に発見するため、最新のワクチンの利用等により定期的にウイルス検査を行うこと。
（5）不正アクセスによるウイルス被害を防止するため、パスワードは容易に推測されないように設定し、その秘密を保つこと。
（6）不正アクセスによるウイルス被害を防止するため、パスワードは随時変更すること。
（7）不正アクセスによるウイルス被害を防止するため、システムのユーザＩＤを共用しないこと。
（8）不正アクセスによるウイルス被害を防止するため、アクセス履歴を確認すること。
（9）不正アクセスによるウイルス被害を防止するため、機密情報を格納しているファイルを厳重に管理すること。
（１０）システムを悪用されないため、入力待ちの状態で放置しないこと。
（１１）ウイルス感染を防止するため、出所不明のソフトウェアは利用しないこと。
（１２）ウイルスの被害に備えるため、ファイルのバックアップを定期的に行い、一定期間保管すること。

c．事後対応

（1）ウイルスに感染した場合は、感染したシステムの使用を中止し、システム管理者に連絡して、指示に従うこと。
（2）ウイルス被害の拡大を防止するため、システムの復旧は、システム管理者の指示に従うこと。
（3）ウイルス被害の拡大を防止するため、感染したプログラムを含むフロッピー ディスク等は破棄すること。

d．監査

（1）ウイルス対策の実効性を高めるため、ウイルス対策についてのシステム監査の報告を受け、必要な対策を講ずること。

【問題】
　データの破壊や改ざんなどの不正な機能をプログラムの一部に組み込んだものを送ってインストールし、実行したものはどれか

ア　DoS攻撃
イ　辞書攻撃
ウ　トロイの木馬
エ　バッファオーバフロー攻撃

キーワード:「データの破壊や改ざんなどの不正行為」
「プログラムの一部に組み込んだ」

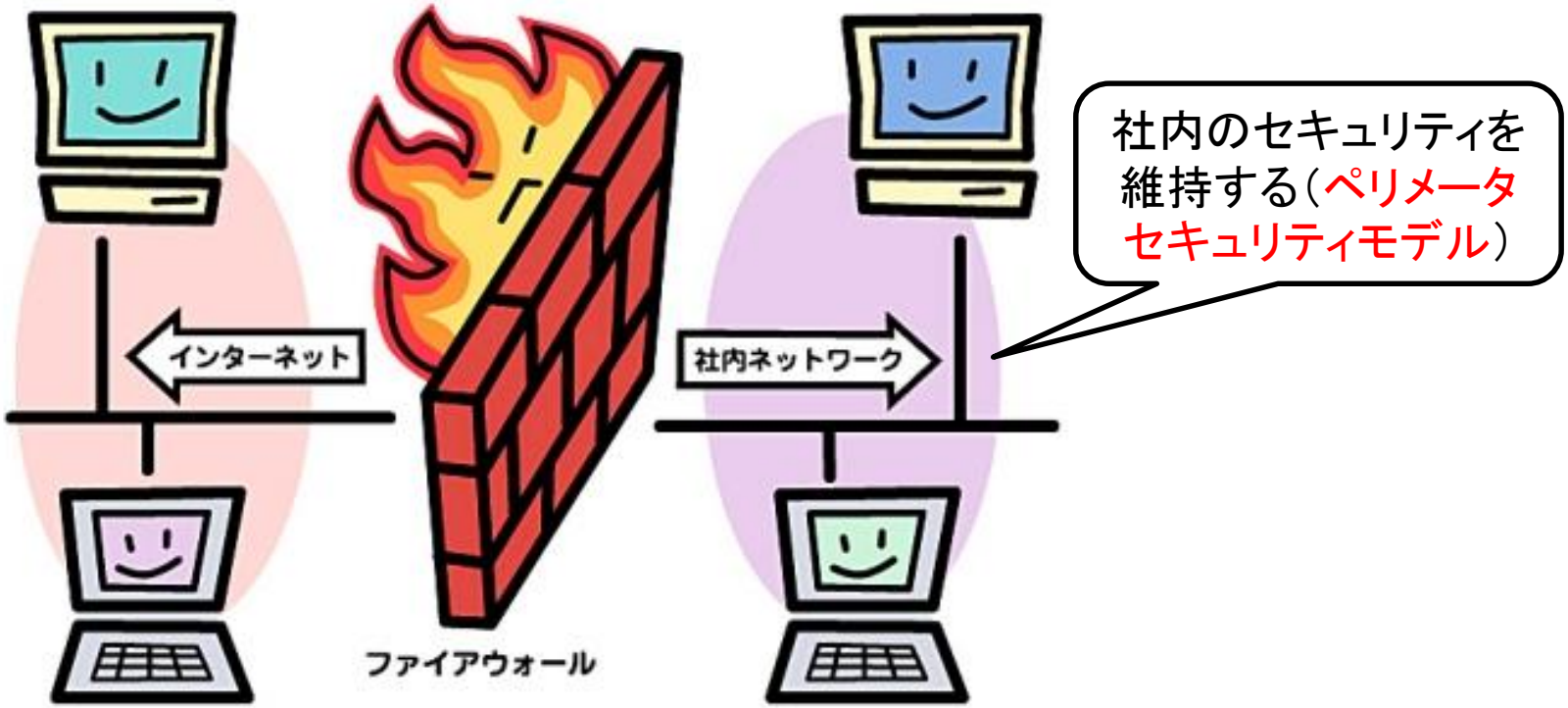
不正アクセス対策

テキストP180-200

- ファイアウォール
- DMZ
- その他のフィルタリング

ファイアウォール

「信頼できるネットワーク」（内部ネットワーク）と「信頼できないネットワーク」（外部ネットワーク）の二つのネットワーク間のアクセスを制御するために使われる。実際には、機器もしくはソフトウェアで実現する。



パケットフィルタリング型ファイアウォール

パケットのヘッダ情報（送信元・宛先IPアドレス、送信元・宛先ポート番号、プロトコルの種別など）によって、フィルタリングする

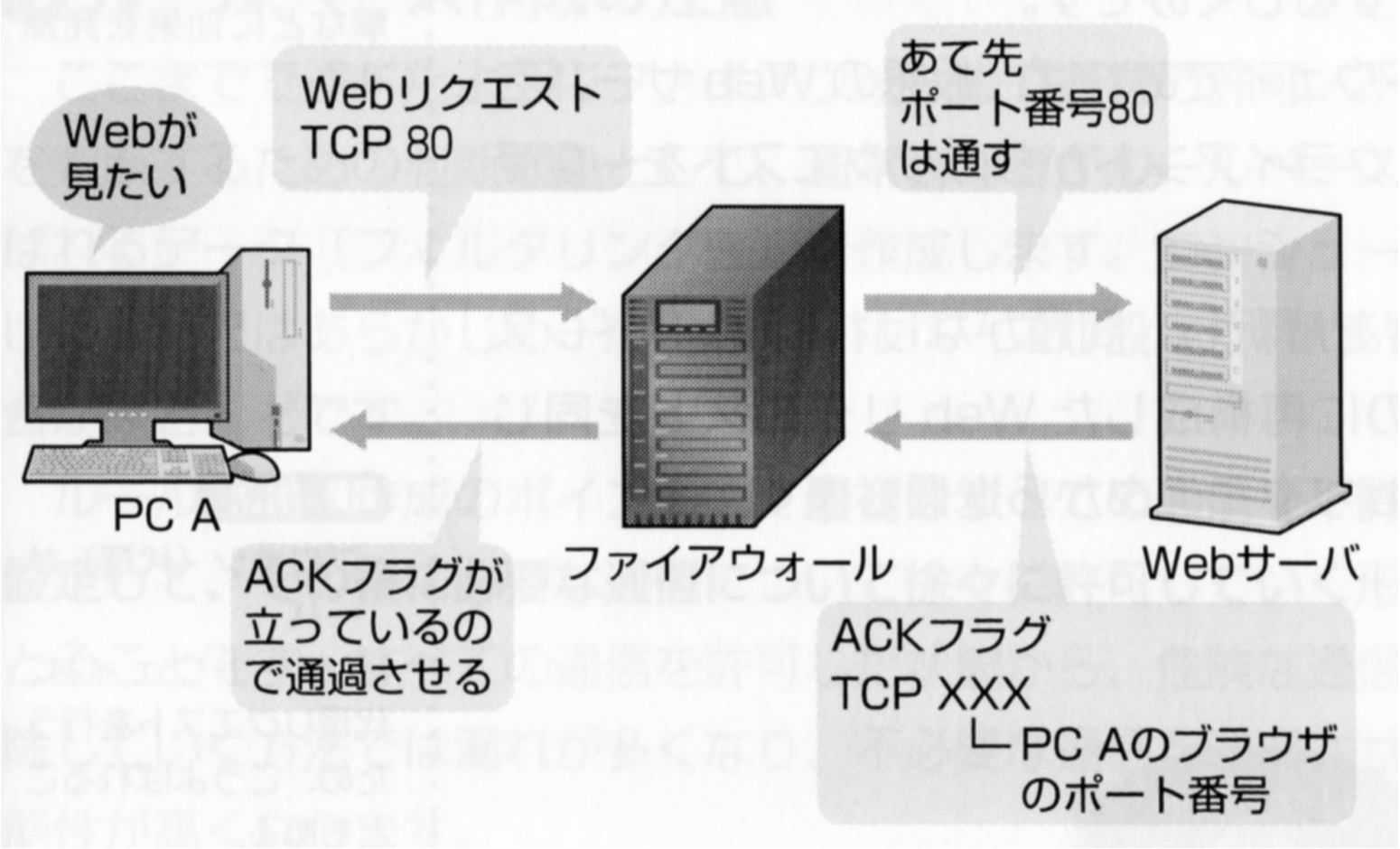
- IPアドレスを使ってフィルタリングする場合

順番（優先順位）	送信元	宛先	適否
1	192.168.0.1	すべて	○
2	すべて	10.0.0.1	○
3	すべて	すべて	×

- ポート名番号を使ってフィルタリングする場合

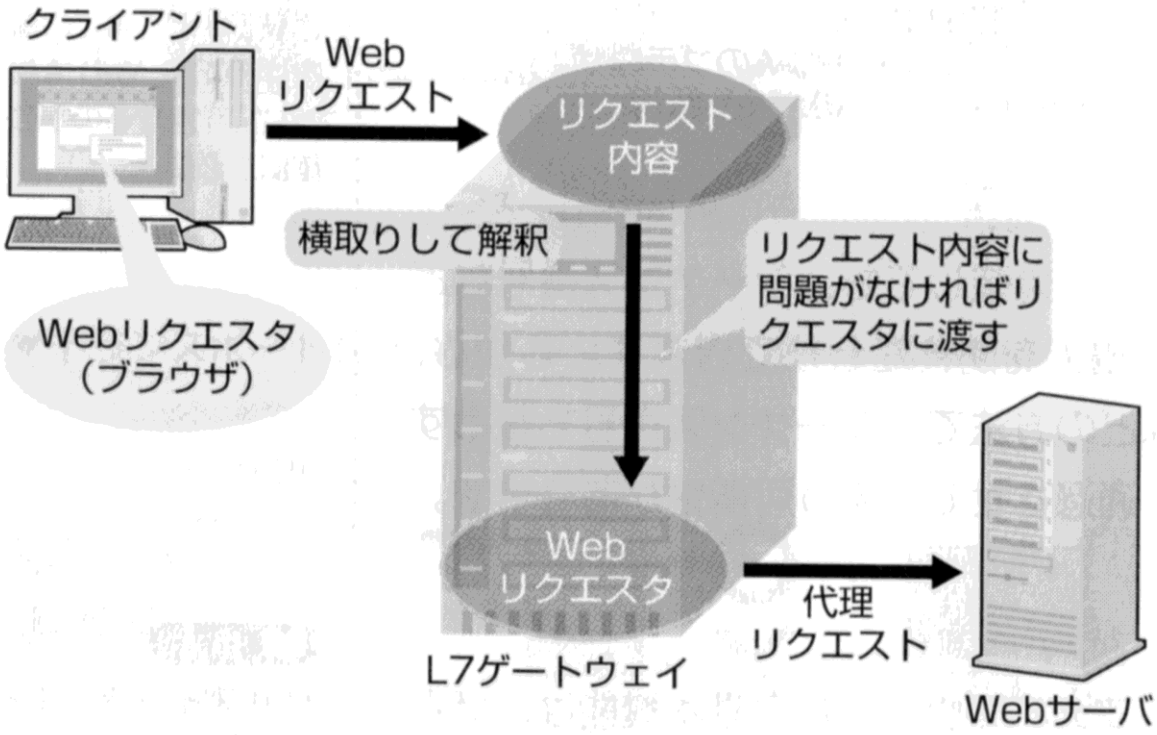
順番（優先順位）	送信元	宛先	適否
1	すべて	http(80)	○
2	すべて	smtp(25)	○
3	すべて	すべて	×

- リクエストの返信
  TCPヘッダのACKフラグを確認することで、フィルタリングする



アプリケーションゲートウェイ型ファイアウォール

アプリケーション層の内容を解釈して通信の可否を決めるファイアウォール



＜アプリケーションゲートウェイ型ファイアウォールのチェック機能＞

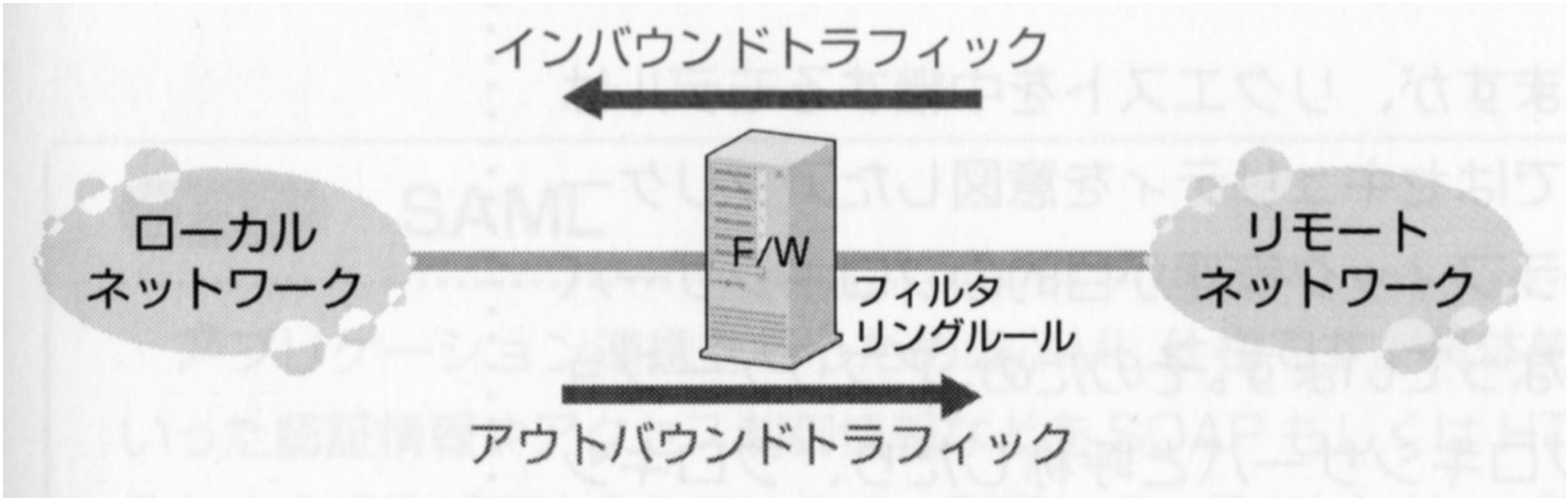
- ステートフルインスペクション
  前後のパケットや上下のプロトコルとの整合性をチェックする
- ディープパケットインスペクション
  ペーロード（送りたい情報）の内容をチェックする

ルールベースの作成上の注意

- ルールベースを作成するポイントは、
「はじめは、すべての通信を不許可にし、その後、必要な通信を少しずつ許可する」

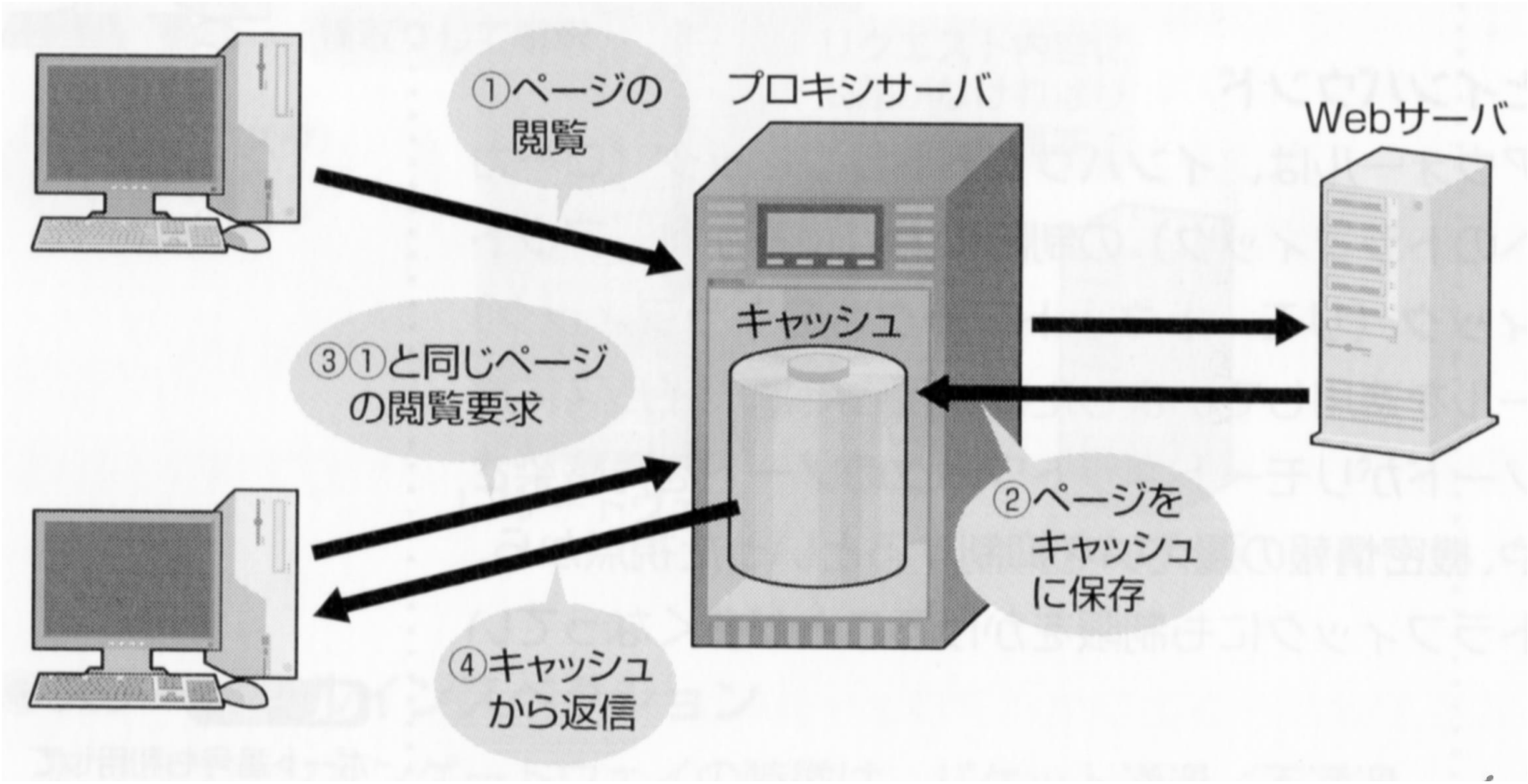
- アウトバウンドとインバウンド

どちらにもルールを適用

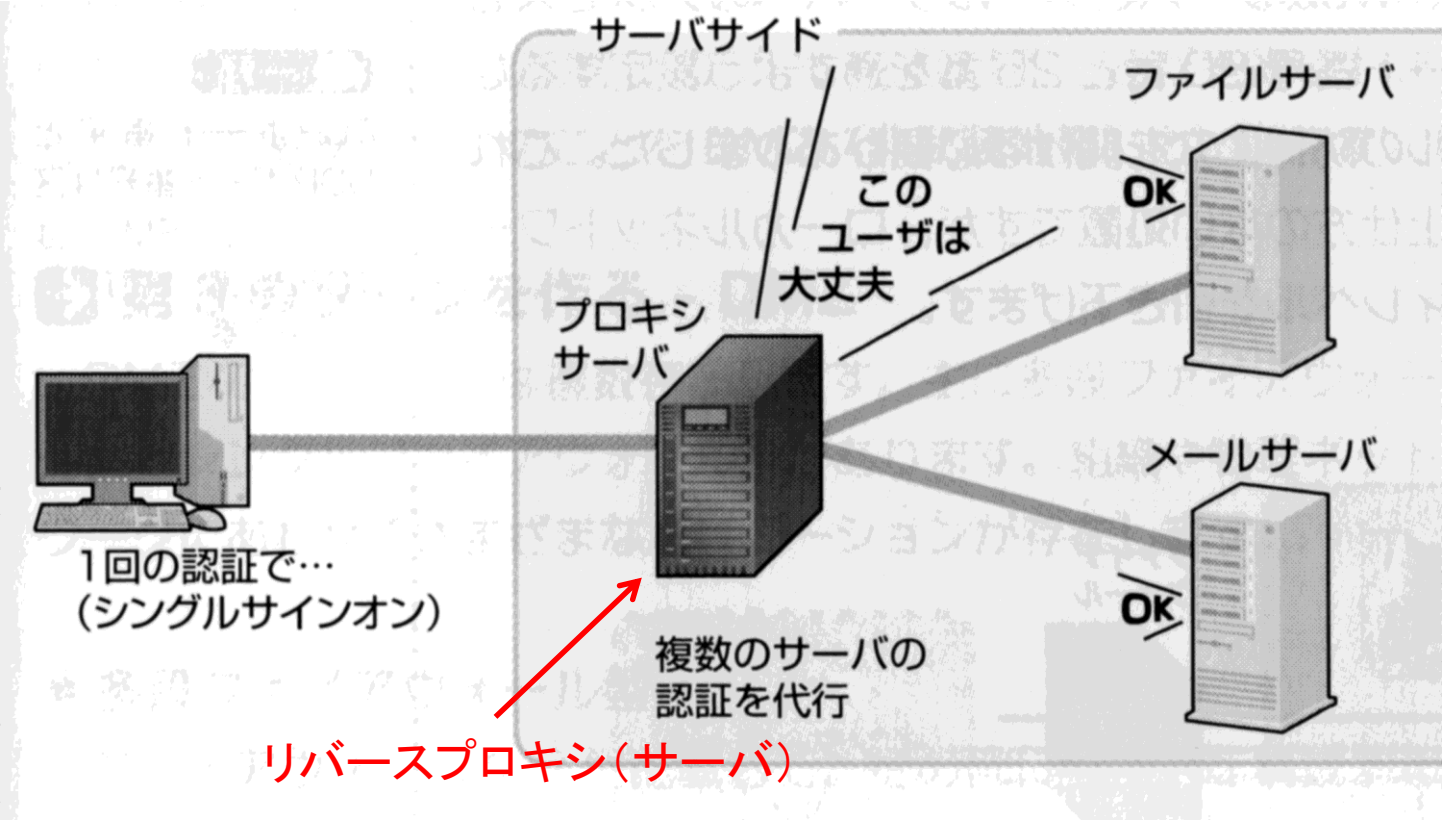


プロキシ(代理)サーバ

Webページの内容をキャッシュして、要求されている内容がキャッシュさえているものであれば、Webサーバからではなく、プロキシサーバから返信する



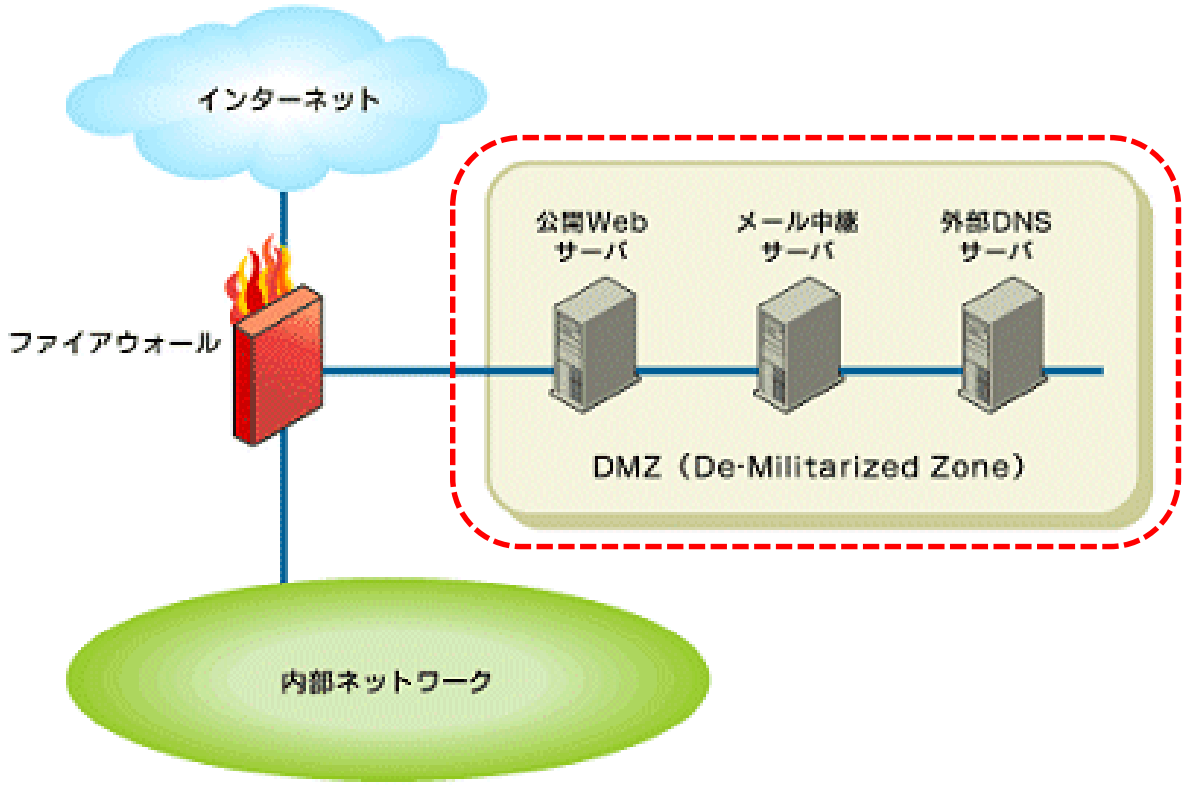
リバースプロキシとシングルサインオン



- シングルサインオン
  複数のサーバにアクセスするときに、1度の認証ですべてのサーバにアクセスできる(リバースプロキシで実現)

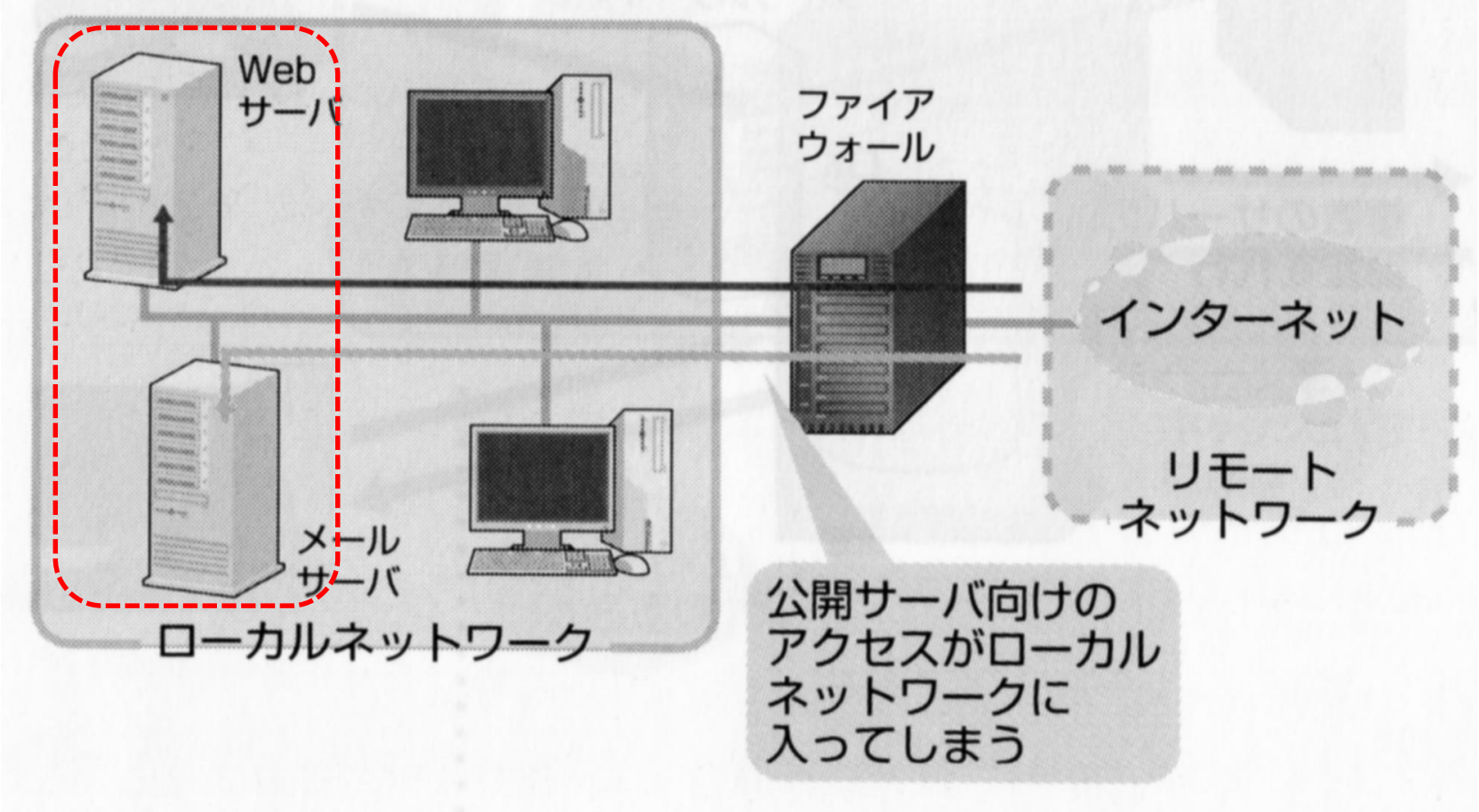
DMZ（DeMilitarized Zone）

ファイアウォールを設置すると、「信頼できないネットワーク」と、「信頼できるネットワーク」の中間に置かれる区域ができる。これを、非武装地帯(DMZ: DeMilitarized Zone)と呼び、ここに、Webサーバやメールサーバなどインターネットに公開しなければならないサーバを設置できる。



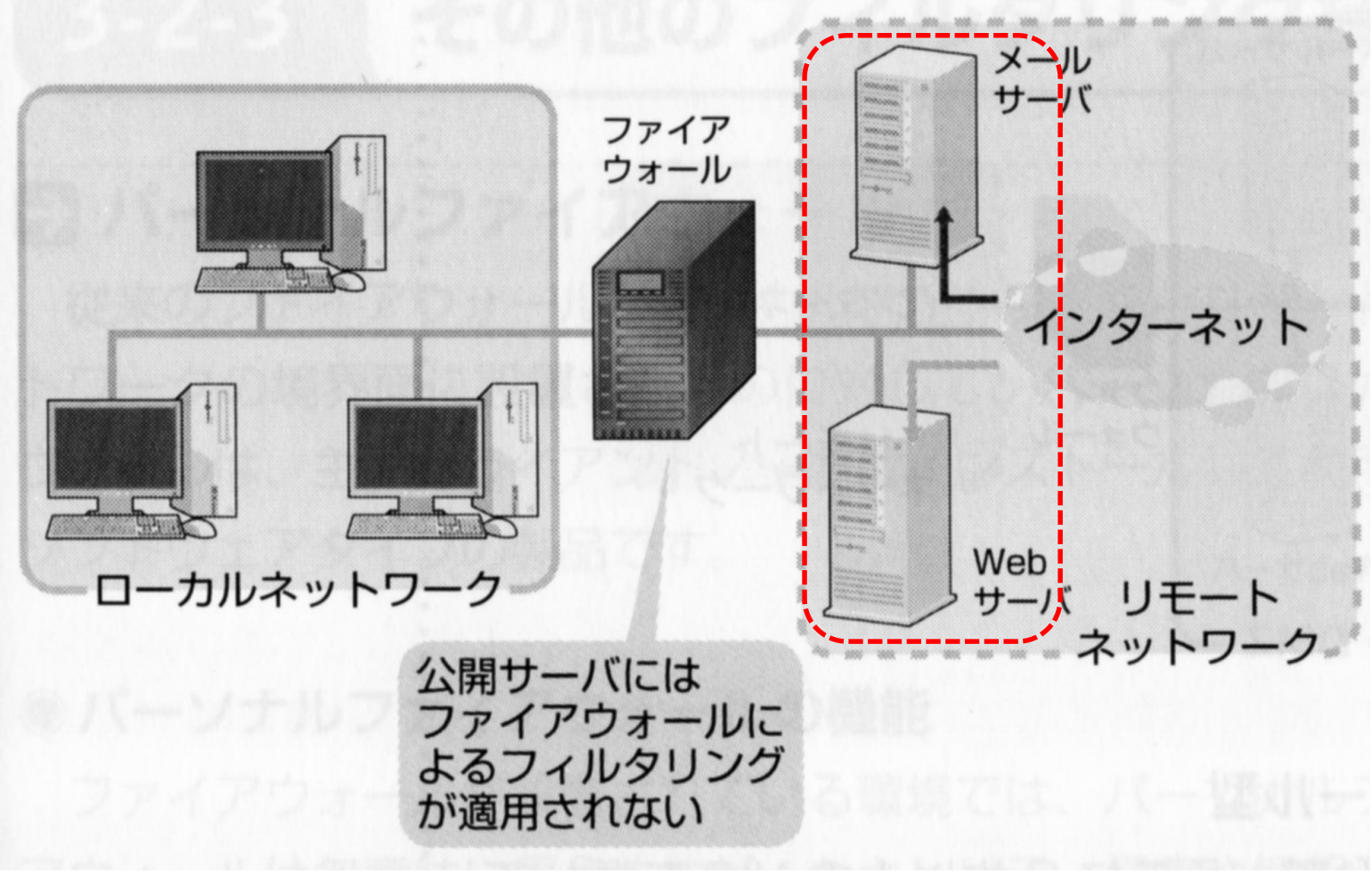
● 内部設置型

公開サーバをローカルネットワークに設置する



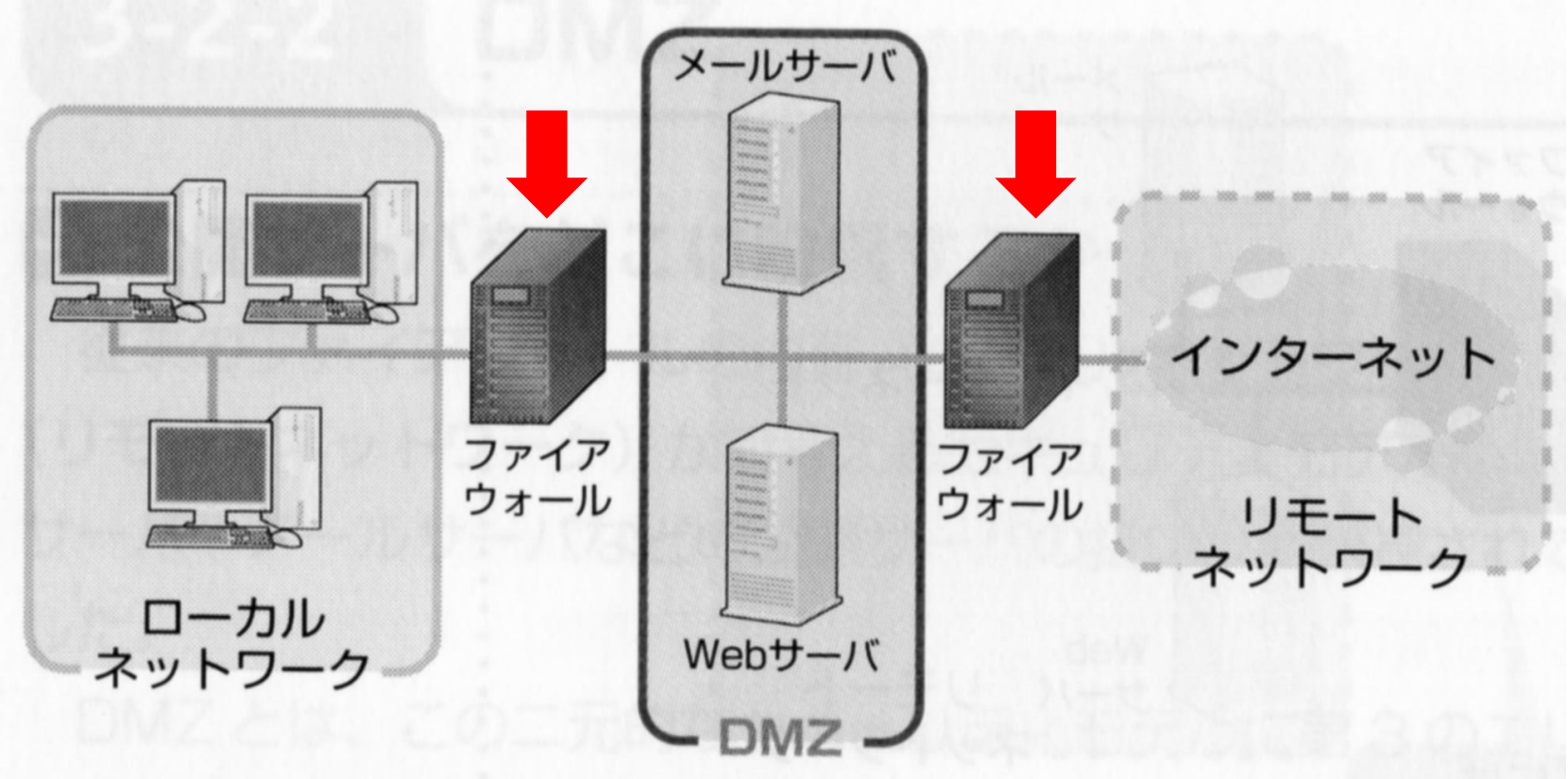
● 外部設置型

公開サーバをローカルネットワークに設置する



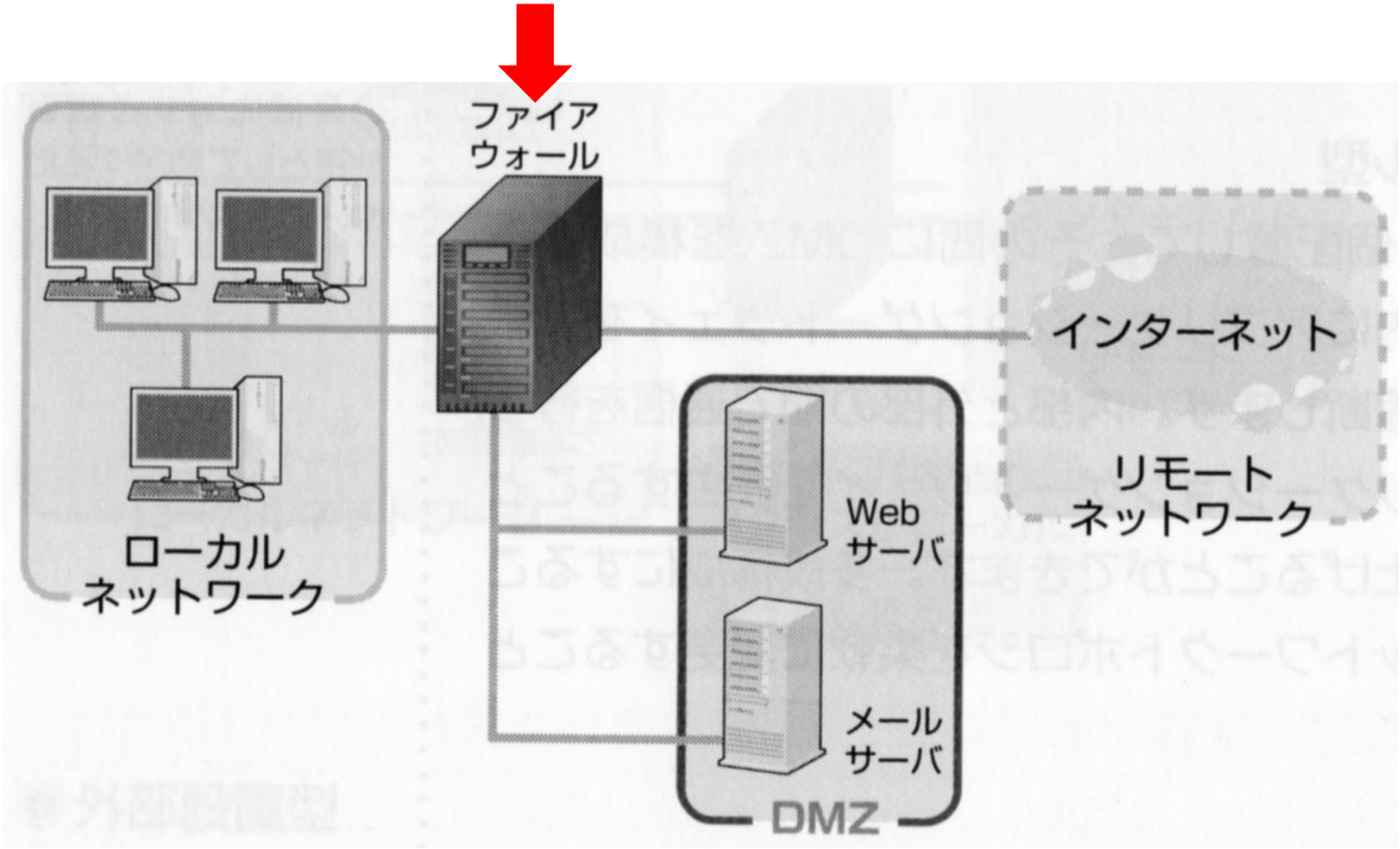
第3のゾーンを作る（DMZ）

- 多段ファイアウォール型
  2台のファイアウォールの間にDMZを設ける



● シングルファイアウォール型

1台のファイアウォールに3つのネットワークを接続し、その1つのDMZを設ける



その他のフィルタリング機能

● パーソナルファイアウォール
クライアントノードにインストールして利用するソフトウェア

- 内部犯による、情報漏えいやセキュリティ侵害
- ウィルスに感染したクラアントノードのパケット遮断

● コンテンツフィルタリング
やり取りされているデータの内容を確認したり、意味を理解したりして、通信の可否を決める

平成28年度 春期
基本情報処理技術者試験問題・解答（セキュリティ）

問38　スパイウェアに該当するものはどれか。

ア　Web サイトへの不正な入力を排除するために，Web サイトの入力フォームの入力データから，HTML タグ，JavaScript，SQL 文などを検出し，それらを他の文字列に置き換えるプログラム

イ　サーバへの侵入口となり得る脆弱なポートを探すために，攻撃者の PC からサーバの TCP ポートに順番にアクセスするプログラム

ウ　利用者の意図に反して PC にインストールされ，利用者の個人情報やアクセス履歴などの情報を収集するプログラム

エ　利用者のパスワードを調べるために，サーバにアクセスし，辞書に載っている単語を総当たりで試すプログラム