ネットワークとセキュリティ

「情報II」第5章

Contents

クラス：　　番号：　　氏名：

TCP/IP

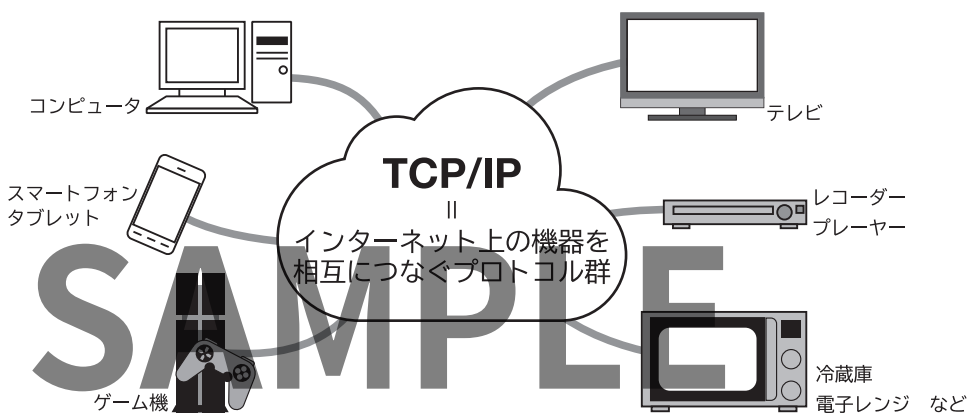
インターネットでは、TCP/IPと呼ばれるプロトコル群が標準的に使われています。主にTCPはデータをパケットに分割する取り決めを、IPは送信するパケットのあて先となるIPアドレスを定めています。ここではTCP/IPの詳しい役割について学びます。

（教科書Ⅰ：p.172 – p.175 , 教科書Ⅱ：p.108 – p.109）

■ TCP/IP

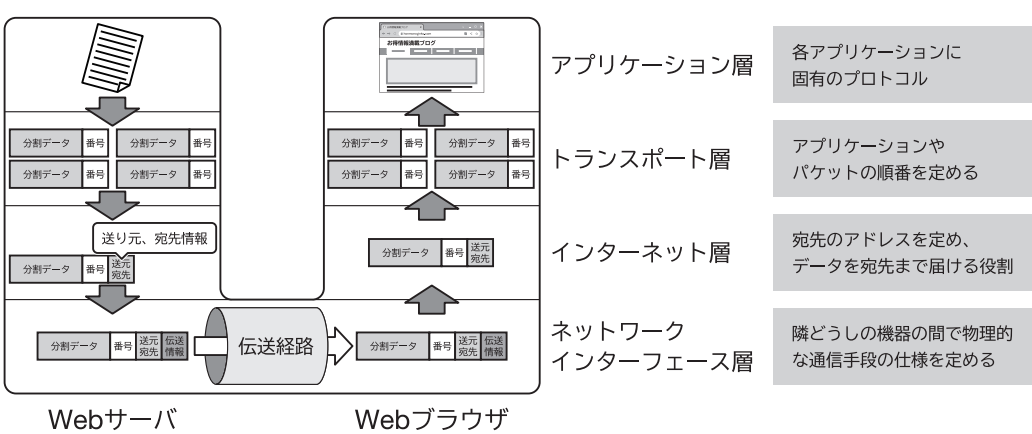
TCP/IPとは

TCP/IP＝〔1　　〕と〔2　　〕を中心としたインターネット標準のプロトコル群



TCP/IPの4階層モデル

TCP/IPは、次の4つの階層から構成される



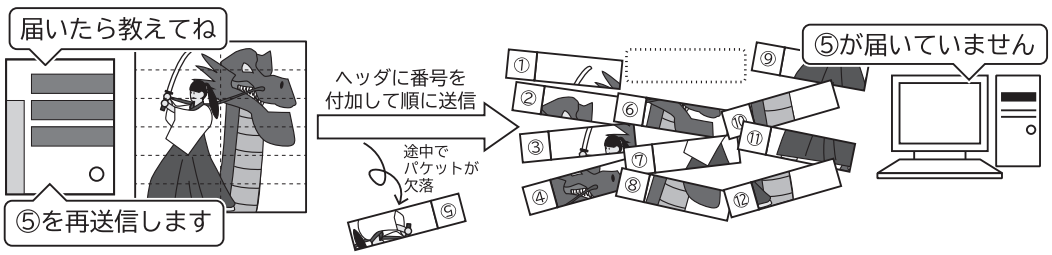
TCPは〔3　　〕のプロトコル

IPは〔4　　〕のプロトコル

TCPとUDP

TCP（Transmission Control Protocol）

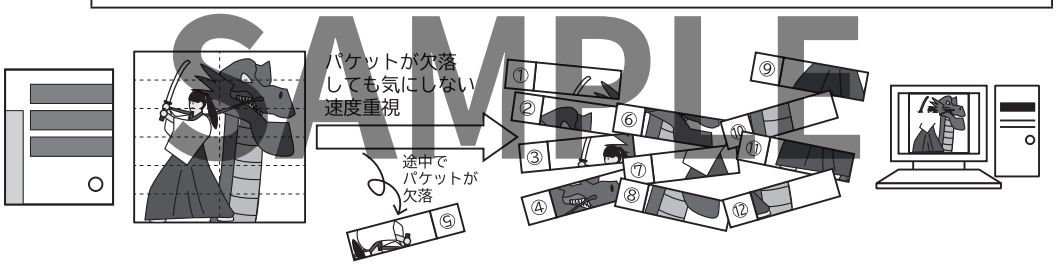
TCP＝ 通信途中で欠落したパケットがあれば〔5　　〕する



通信の〔6　　〕を役割としている

UDP（User Datagram Protocol）

UDP＝ データの欠落を〔7　　〕→ 欠落したパケットは〔8　　〕



〔9　　〕を重視し、〔9　　〕の高い通信を役割としている

問題1

次の各通信は、TCPを用いる方が適切か、UDPを用いる方が適切かを答えてください。

(1)文字中心のSNSのデータを受信する　〔10　　〕

(2)動画のストリーミング再生　〔11　　〕

(3)音声通話　〔12　　〕

(4)動画データのダウンロード　〔13　　〕

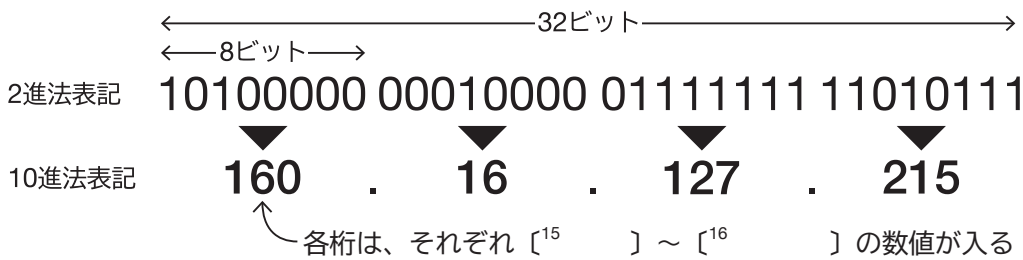
■ IP

IP（Internet Protocol）

IP＝ パケットを正しい送り先に届けるために、〔[14]　　〕を定める

IPアドレス

〔[14]　　〕＝ ネットワーク上の機器に割り当てられた住所に相当する番号



問題2

IPアドレスとして通用するものには○、通用しないものには×を書いてください。

（1）10.73.87.3.1	[17]	（2）192.168.2.251	[18]	（3）192.168.78.263	[19]
（4）10.98.–25.126	[20]	（5）19.58.3	[21]	（6）10.240.0.3	[22]

IPv6

上記のIPアドレス（[23]　　）は〔[24]　　〕でアドレスを表現

→IPアドレスの総数は約〔[25]　　〕通り

→世界的規模でみると地球上の人口よりも少なく、〔[26]　　〕している

→〔[27]　　〕で表現する〔[28]　　〕が登場

IPv4アドレス  32ビット

IPv6アドレス  128ビット

IPv6は、約〔[29]　　〕通りのアドレスが実現

→地球上のありとあらゆるモノにIPアドレスを割り当てることが可能に！

→これにより〔[30]　　〕([31]　　）が進展

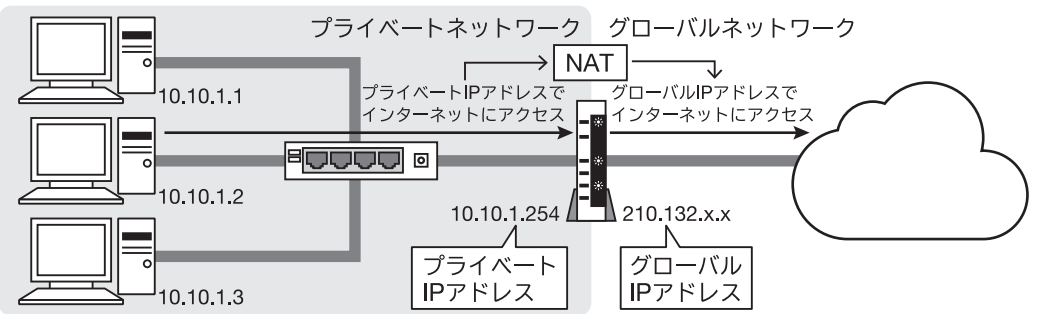
※IPv6と比較したときの従来型のIPアドレスをIPv4アドレスという

NAT（Network Address Translation）

LAN内のネットワーク　＝〔[32]　　〕

インターネット　　＝〔[33]　　〕

〔32〕と〔33〕でIPアドレスを**相互に変換**する技術



LAN内では〔[34]　　〕を使用

インターネットでは〔[35]　　〕を使用

ルータは〔34〕と〔35〕の両方のアドレスを持つ → NATは、〔34〕と〔35〕を変換

プライベートIPアドレスの範囲

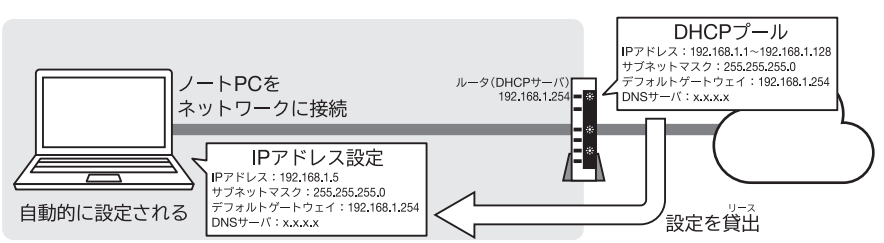
プライベートIPアドレスは、次の範囲内で設定することが定められている

→LAN内で自由に設定することができる　※LAN内での重複は許されない

クラスA	10 . 0 . 0 . 0	～	10 . 255 . 255 . 255
クラスB	172 . 16 . 0 . 0	～	172 . 31 . 255 . 255
クラスC	192 . 168 . 0 . 0	～	192 . 168 . 255 . 255

DHCP（動的ホスト構成プロトコル）

端末をネットワークに接続した際、自動的にIPアドレス等を設定する機能



※ルータにDHCPサーバの機能が付いていることが多い

ネットワークアドレス

同じ〔[36]　　〕を持つ機器同士は同じ組織内の機器として扱う

→ネットワークアドレスは、IPアドレスと〔[37]　　〕を比較して求める

→〔37〕が1となっているビットはそのままに、0のビットは0にする

	(192)	(168)	(100)	(91)
IPアドレス（192.168.100.91）	11000000	10101000	01100100	01011011
サブネットマスク（255.255.0.0）	(255) 11111111	(255) 11111111	(0) 00000000	(0) 00000000
ネットワークアドレス	11000000 (192)	10101000 (168)	00000000 (0)	00000000 (0)

IPアドレス	192	.	168	.	100	.	91
サブネットマスク	255	.	255	.	0	.	0
ネットワークアドレス	[38]	.	[39]	.	[40]	.	[41]	

問題3

次のそれぞれの場合、ネットワークアドレスを求めてください。

(1)IPアドレス　　：192.168.1.5
　サブネットマスク　：255.255.0.0

[42]

(2)IPアドレス　　：192.168.1.5
　サブネットマスク　：255.255.255.0

[43]

(3)IPアドレス　　：10.20.20.1
　サブネットマスク　：255.255.0.0

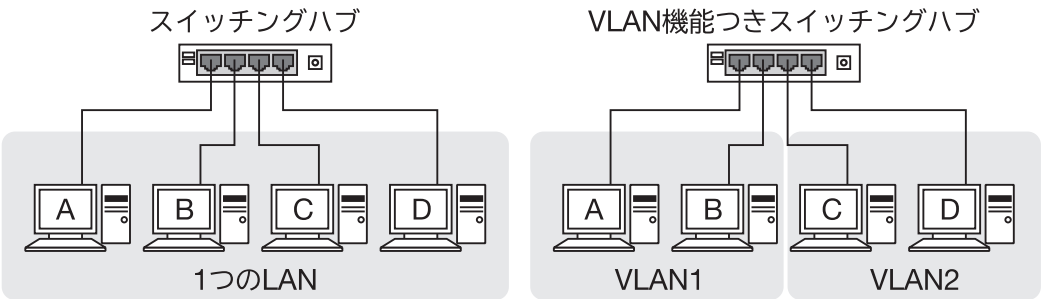
[44]

(4)IPアドレス　　：10.20.0.1
　サブネットマスク　：255.255.255.0

[45]

VLAN（仮想LAN）

1つのLANを物理的な接続形態を変えることなく仮想的に分割して複数のLANに分割



※従来のLANの構成は変えることなく、組織を分割することができる

振り返り

次の各観点が達成されていれば□を塗りつぶしましょう。

□TCPおよびUDPの役割について理解できた

□IPアドレスがどのようなものであるかについて理解できた

□IPアドレスが枯渇しており、NATやIPv6といった対応がされていることを知った

□ネットワークアドレスの求め方を理解できた

今日の授業を受けて思ったこと、感じたこと、新たに学んだことなどを書いてください。

情報セキュリティの確保

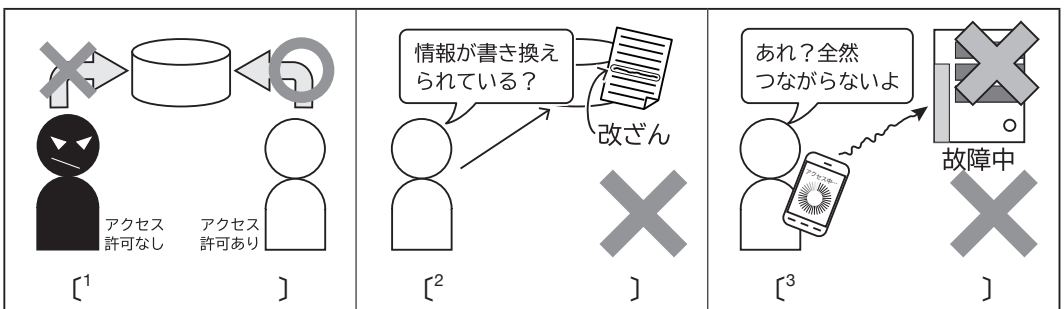
たとえどんなに便利な情報システムであったとしても、情報漏えいやサービス停止の脅威にさらされていると、利用者は安心してそのシステムを使うことはできません。利用者が安心して情報システムを利用できるようにするための対策について学びます。

（教科書Ⅰ：p.34 – p.37 , p.178 – p.181 , 教科書Ⅱ：p.106 – p.109）

■ 情報セキュリティの確保

情報セキュリティとは

情報セキュリティとは、一般に以下の3つの事柄が保たれている状態



〔1 〕	〔2 〕	〔3 〕
許可された者だけが、その情報にアクセスできる状態	情報が改ざんされておらず、完全な状態が保たれている	必要なときに情報を利用できること

情報セキュリティとは、単に秘密が守られるということだけではない

問題1

次の各説明のうち、機密性の説明にはC、完全性の説明にはI、可用性の説明にはAを書いてください。

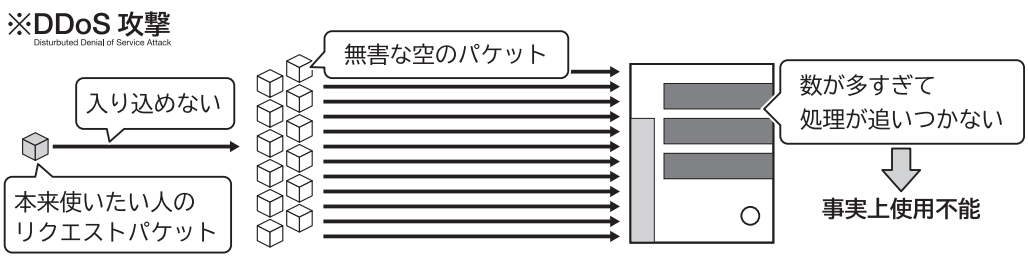
①社員が誤ってデータベースのデータを書き換えてしまった。〔4 〕

②通信内容が盗み見られた。〔5 〕

③サーバのハードディスクが壊れ、読み出し不能になった。〔6 〕

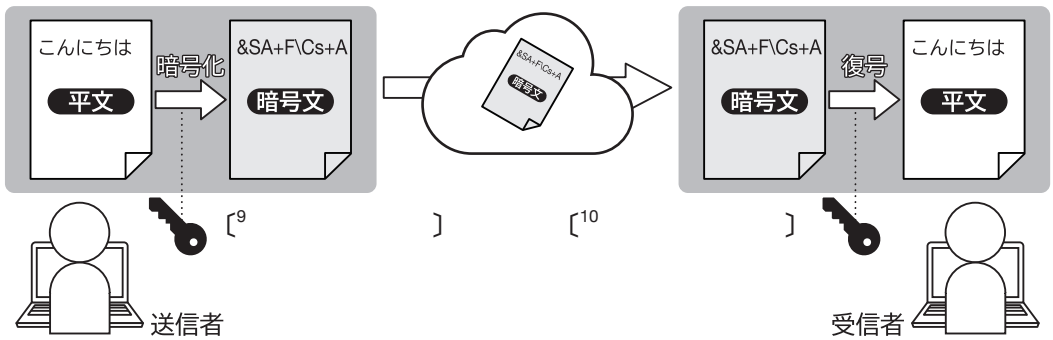
④携帯電話を紛失し、携帯電話の中の個人情報が漏洩する危険が高まった。〔7 〕

⑤サーバに多量にアクセスを集中させる攻撃を受け（DDoS攻撃という）、サーバが使用できない状態になってしまった。〔8 〕

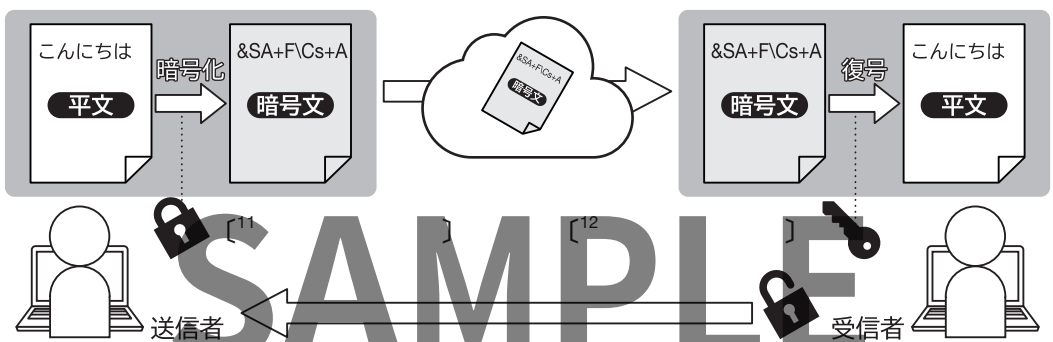


暗号化による情報流出の防止

共通鍵暗号方式



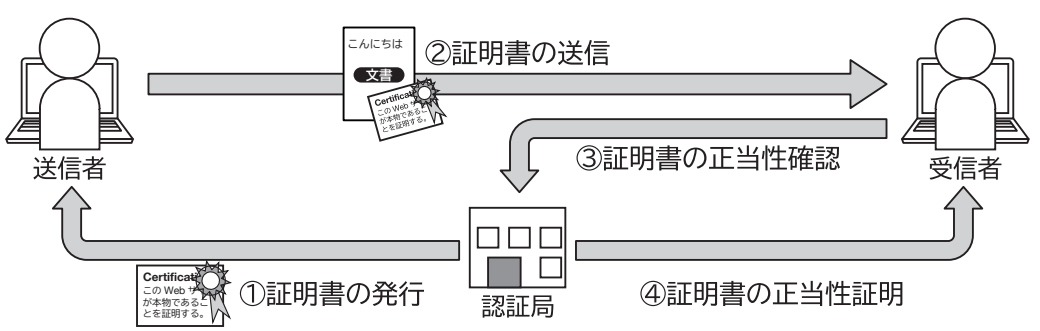
公開鍵暗号方式



※〔11〕〔12〕ともに受信者が生成したもの

認証局（CA）

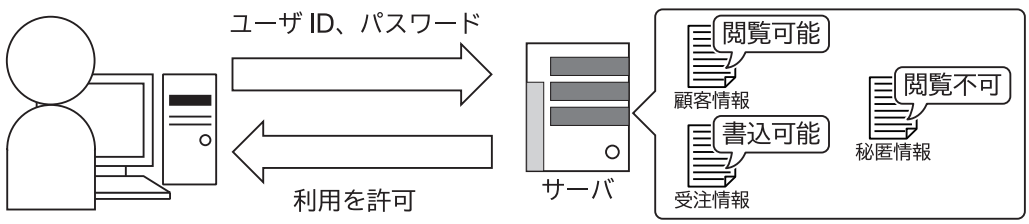
認証局＝ 公開鍵が正当なものであることを保証する証明書を発行する機関



アクセス制御とアクセス権

アクセス制御＝ 利用者に与えられた、データなどを利用する権限を管理すること

個人認証により個人を確認し、〔[13]　　〕（**権限**ともいう）を与える



問題2

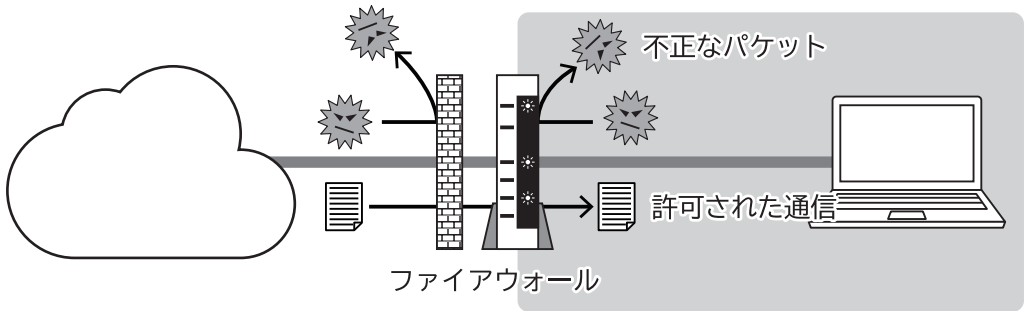
ネットワーク上のある情報について、次の表のようなアクセス制御が設定されています。次の各場合で、読取、書込が可能であれば○を、不可であれば×を書いてください。設定が「許可」である場合のみその動作が許可され、「許可」と「拒否」の両方が設定される場合は「拒否」設定が優先されるものとします。

	読取		書込	
	許可	拒否	許可	拒否
総務部	○			
事業部	○		○	
営業部				○
部長	○		○	
契約社員				○
アルバイト		○		○

		読取	書込
①	総務部員	[14]	[15]
②	事業部員	[16]	[17]
③	総務部長	[18]	[19]
④	営業部長	[20]	[21]
⑤	事業部アルバイト	[22]	[23]
⑥	事業部契約社員	[24]	[25]

ファイアウォール

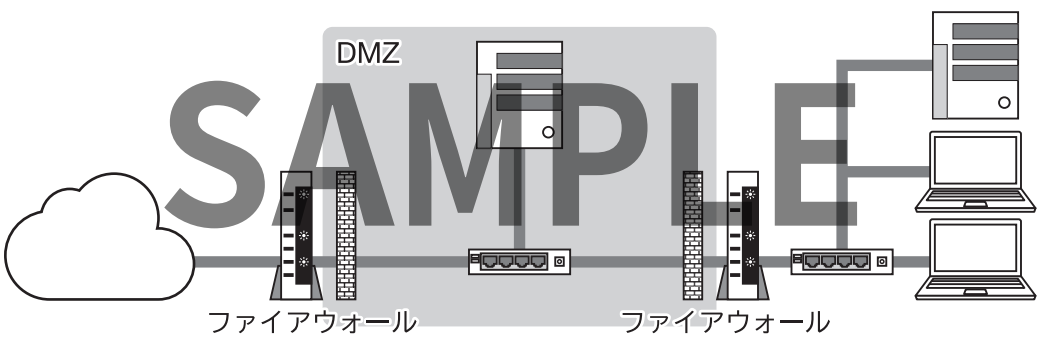
ファイアウォール＝ 不正なパケットを〔[26]　　〕し〔[27]　　〕する



DMZ（非武装地帯）

DeMilitarized Zone

DMZ＝ インターネットと組織内ネットワークの間につくられる緩衝領域

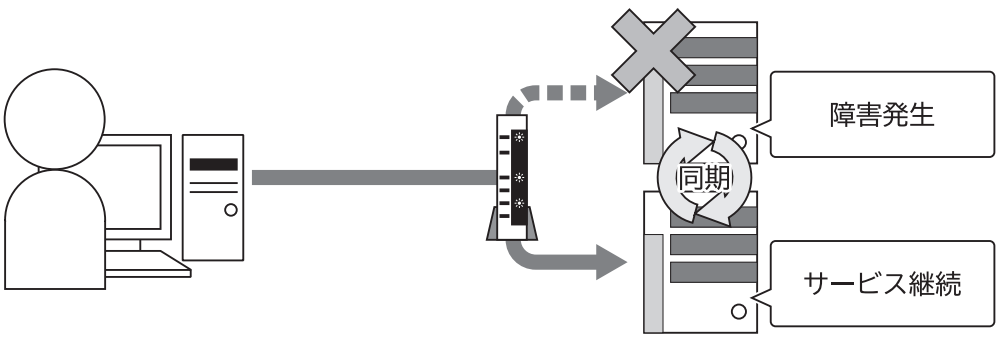


※Webサーバやメールサーバなど、外部から頻繁にやりとりのあるサーバはDMZに置く
→組織内ネットワークへの進入を防ぎつつ、外部とのやり取りを確保する

システムを止めない工夫

冗長化

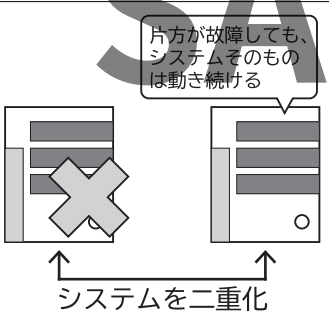
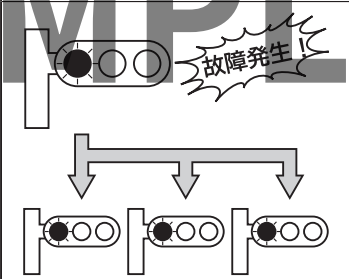
冗長化＝ 同じ機能や役割のものを2台以上用意し、システムの停止を防ぐ考え方



※障害が発生すると、予備のサーバに切り替え

フォールトトレランス

フォールトトレランス＝ システムに障害が発生しても全体の機能を維持する能力

28	29	30
		
障害が発生した際、機能縮小しても動作し続ける能力	正常な動作ができないとき、安全側に作動するように設計	誤った使い方をしても誤動作が起こりにくいように設計

問題3

次の各説明がフォールトトレランスのうちのどの説明になっているか、下の選択肢から選び、記号で答えてください。

(1)交差点の信号機のうち1機が故障した際、すべての信号機を赤にする。

31

(2)同じ機能をするサーバを複数台用意しておき、1台が故障してもシステムはそのまま動かし続けることができる。

32

(3)データを削除する際、うっかり誤って削除しないよう「本当に削除しますか？」と確認メッセージを出す。

33

(4)停電が発生した際に、予備電源から少しの間機器を動作させ、その間にデータの保存を行うなどし、安全にシステムを停止する。

34

(5)一部のサーバが故障したが､他のサーバが自動的にその役割を引き継いだことにより、営業活動には影響は出なかった。

35

ア フェイルソフト　**イ** フェイルセーフ　**ウ** フールプルーフ

振り返り

次の各観点が達成されていれば□を塗りつぶしましょう。

□情報セキュリティの基本的な考え方（機密性、完全性、可用性）を理解した
□共通鍵暗号方式、公開鍵暗号方式の違いを理解した
□アクセス制御の設定を読み取ることができるようになった
□ファイアウォールの役割を知ることができた
□フォールトトレランスのそれぞれの違いを理解した

今日の授業を受けて思ったこと、感じたこと、新たに学んだことなどを書いてください。

章末問題

[問題1]

次の端末と同一ネットワーク上の端末をすべて選んでください。

IPアドレス：192.168.152.16　サブネットマスク：255.255.0.0

（1）IPアドレス　　：192.168.1.3
　　サブネットマスク：255.255.255.0

（2）IPアドレス　　：192.168.152.254
　　サブネットマスク：255.255.0.0

（3）IPアドレス　　：192.168.152.154
　　サブネットマスク：255.255.255.0

（4）IPアドレス　　：192.168.243.36
　　サブネットマスク：255.255.0.0

[問題2]

次の各説明が、機密性、完全性、可用性のどの脅威となっていますか。

（1）DDoS攻撃によって、Webサイトがダウンした。

（2）キーボードの打ち間違いによって、不正確なデータが入力された。

（3）マルウェアの感染により、個人情報が漏えいした。

[問題3]

ある会社には、総務部、開発部、営業部があり、それぞれにデータベースを持っています。各部の社員には、自分の所属する部のデータベースの読み書きを許可しています。

また、開発部のデータベースは、総務部の社員に読み出しを許可しており、営業部のデータベースは、総務部、開発部の社員に読み出しを許可しています。

次の表の（1）～（3）はそれぞれ何部ですか。

データベース	（1）	（2）	（3）
データベースA	読み書き可能	読み出し可能	読み出し可能
データベースB	アクセス不可	読み書き可能	アクセス不可
データベースC	アクセス不可	読み出し可能	読み書き可能

（1）		（2）		（3）	

コラム～ VPN

■ VPN（Virtual Private Network）

VPN（Virtual Private Network：仮想プライベートネットワーク）

VPN＝ 物理的に離れた場所どうしで組織内ネットワークを構築するしくみ

※遠く離れた場所からLANのように同一ネットワークのような接続が可能になる

VPNの成り立ち

VPNは、**認証**、**暗号化**、**トンネリング**の3つの技術から成り立っている

→認証、暗号化はすでに学習した通りのもの

トンネリング

インターネット上に仮想的なトンネル（閉域網）をつくることで安全に拠点間通信

※トンネルには、インターネット網に構築するタイプと専用の回線を設けるタイプがある

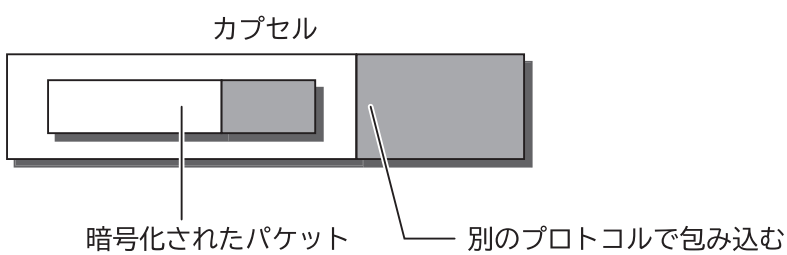
→インターネット網に構築するタイプの方が安価で導入が可能

→専用回線を設けるタイプはセキュリティがより強固になる

カプセル化

万が一トンネルの中を盗み見られた場合に備え、トンネルに流すパケットは**カプセル化**

→パケットを暗号化した上で、更に別のプロトコルで包み込む



SAMPLE

2025年度近「情報Ⅱ」ワークブック見本
CQ出版社