IPTPC認定技術者資格制度
技術者教育プログラム

IPTPC
IP Telephony Promotion Center

テキストサンプル

セキュリティデザイナ研修

教育テキスト

- 第4.0版 -

IP電話普及推進センタ

注意事項

- 本テキストの内容については断りなく変更を行うことがあります
- 本テキストの誤りに関連して生じた偶発的、あるいは派生的な損害については、その責任を負いかねます
- 本テキストはセキュリティデザイナ研修の評価用にセキュリティデザイナ研修テキスト4.0版を基に作成したものです。他の目的での複製、再利用、再使用を禁じます。

第１章

セキュリティ基礎

（4.0版）

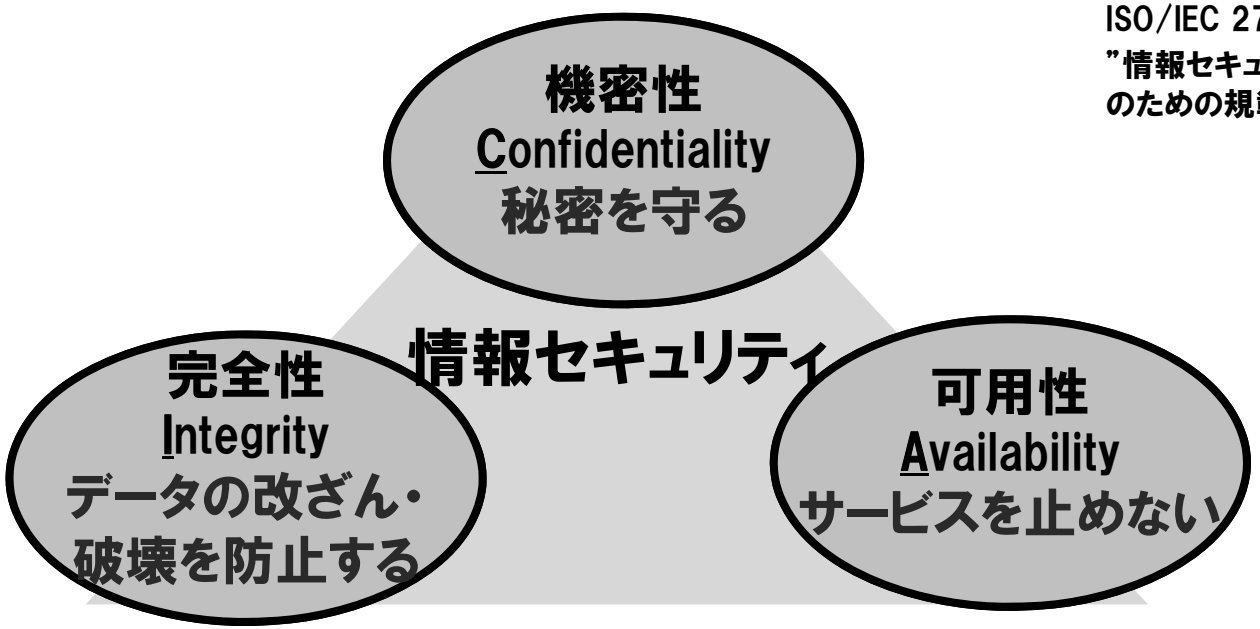
1. 現在の企業ITインフラでのセキュリティの必要性
2. 情報セキュリティとは
3. 保護すべき情報資産
4. 本テキストの構成

IPTPC
IP Telephony Promotion Center

1-2-1 情報セキュリティの三要素 機密性・完全性・可用性

「情報セキュリティとは機密性・完全性・可用性を維持すること」

ISO/IEC 27002（JIS Q 27002）
”情報セキュリティマネジメントの実践のための規範” の定義



「情報セキュリティ」の目的は、ISO/IEC27002（JIS Q 27002）では、『「機密性」「完全性」「可用性」の3要素を維持すること』とされている。

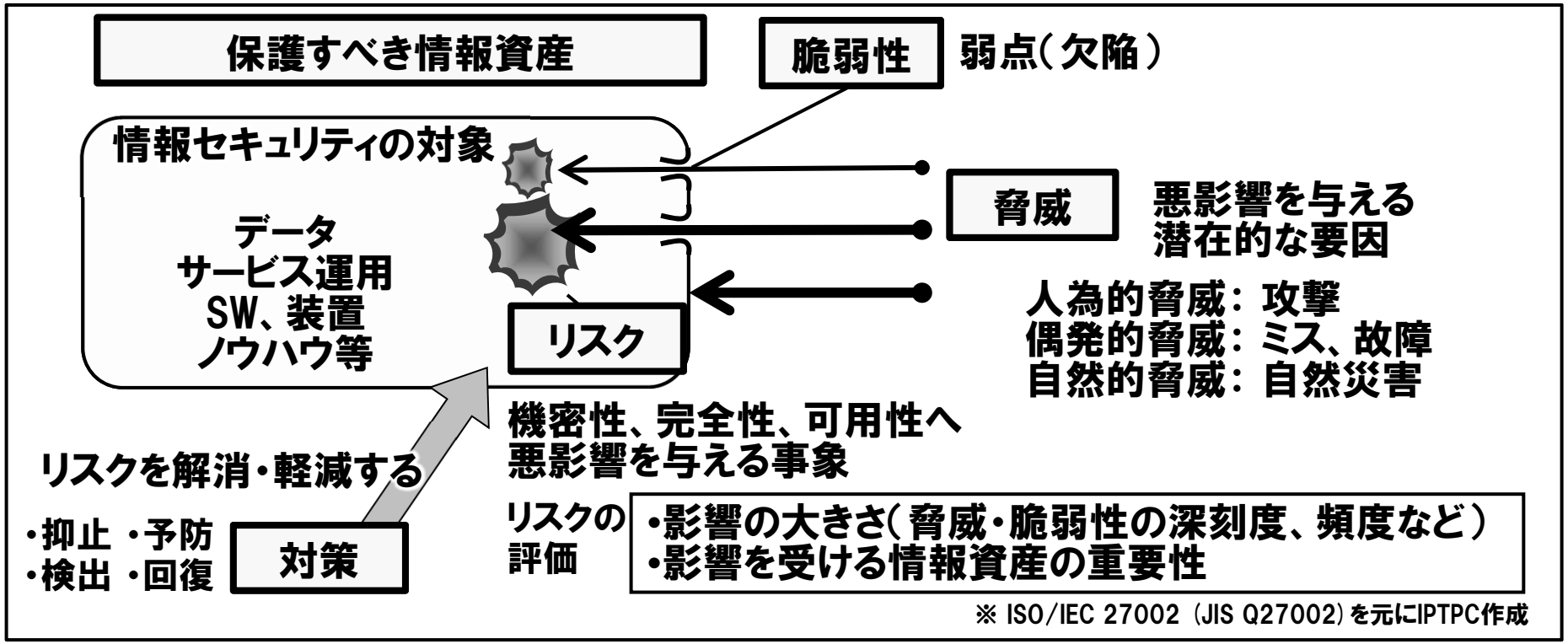
- 機密性：権限を持つ者のみが情報にアクセスできること（秘密を守る）
- 完全性：情報の改ざん・破壊がされていないこと
- 可用性：権限を持つ者は常に情報にアクセスできること（サービスを止めない）

セキュリティ活動は、これら3要素を脅かすリスクを把握して、それに対する対策を立案・運用して安定した状態を維持することが目的となる。

システムの 機密性・完全性・可用性 を維持することが
セキュリティ活動の目標となる

IPTPC
IP Telephony Promotion Center

1-2-2. セキュリティマネジメント



セキュリティを維持運用するための対象である「保護すべき情報資産」へのリスク分析を行い、それに基づきセキュリティ設計運用を行う。「保護すべき情報資産」はハードウエアだけでなく、ソフトウエア、サービス、顧客データといった情報も含まれる。これらに対し影響を及ぼす潜在的な要因である「脅威」を分析する。「脅威」には攻撃など意図的な要素だけでなく偶発的なミス、自然災害、故障なども含まれる。

情報資産に弱点(「脆弱性」)があると「脅威」が現実化し、機密性・完全性・可用性に悪影響を与える「リスク」となる。「リスク」の大きさは脅威・脆弱性の深刻度・頻度だけでなく、影響を受ける情報資産の重要性によっても変わり、リスク毎に「対策」を立案する。

保護すべき情報資産を定め、それぞれに想定される脅威と脆弱性・資産の重要性からリスクを評価して対策を検討・実施する。

第2章

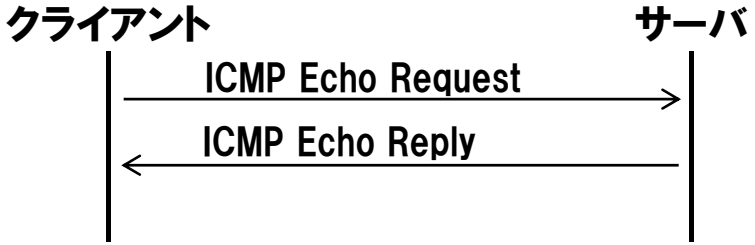
サーバインフラへの脅威と対策

（4.0版）

1. サーバインフラへの脅威
2. サーバの脆弱性
3. サーバへの脅威と対策
4. SIPプロトコル・音声系サーバへの脅威と対策
5. 暗号技術
6. WEBセキュリティ

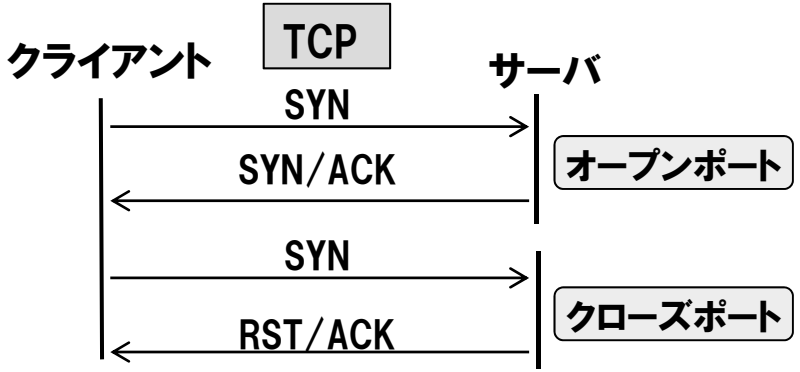
2-3-2　脅威：攻撃対象サーバの調査

Ping

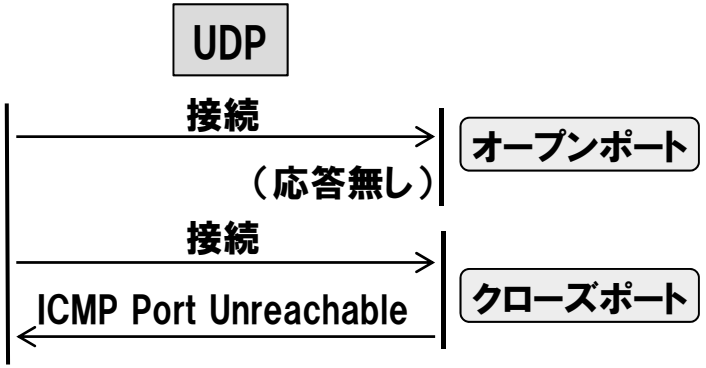


クライアントからサーバへのping 要求は、ICMPのEcho Request としてサーバに届く。
サーバはICMPの送信元に Echo Reply で応答する。
クライアントからのPingに応答させない場合は、サーバのOS設定やファイアウォールでEcho Requestを無視するように設定する

ポートスキャン



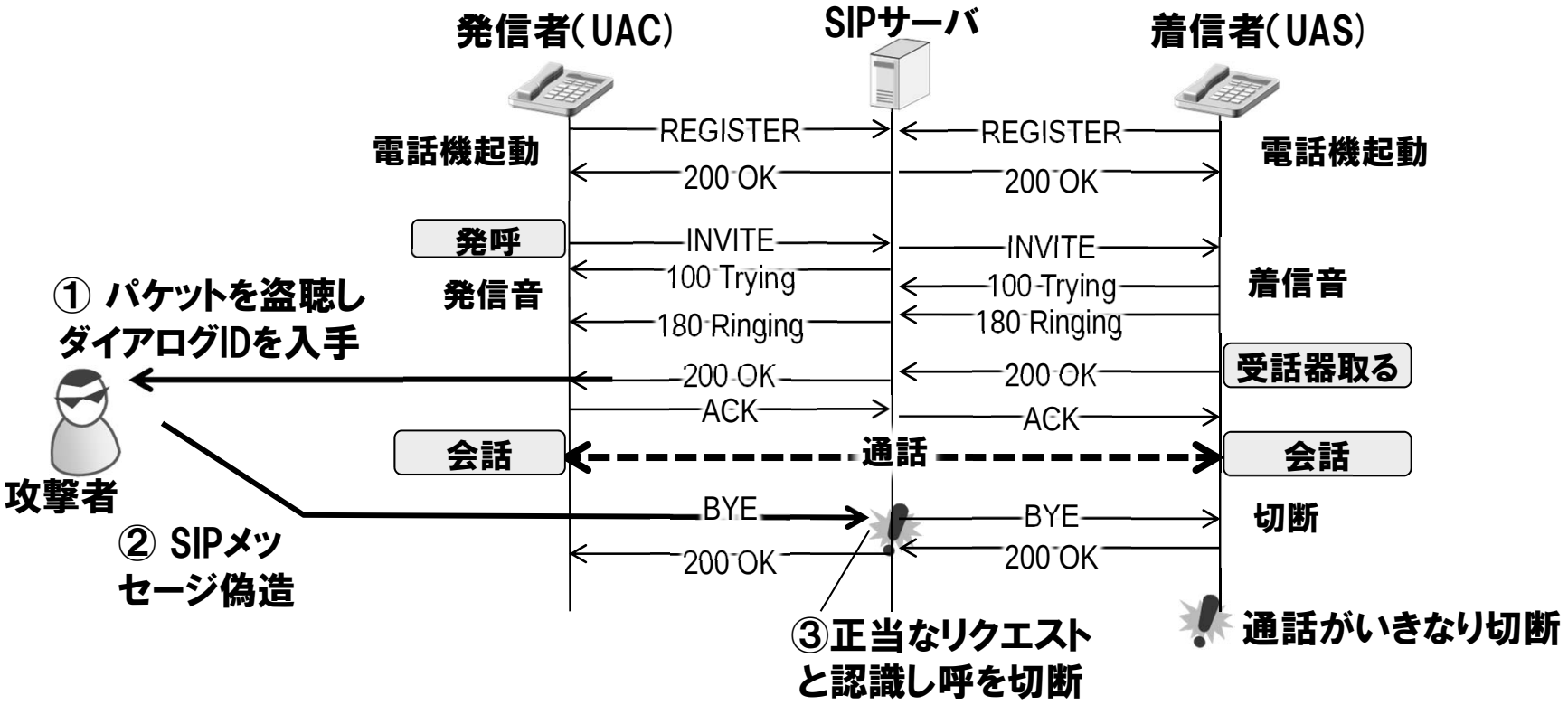
TCPポートへの接続への応答は、ポートが開いている(サービスが動作している)場合、“SYN/ACK” で応答する。
ポートが閉じている(サービスが停止している)場合 “RST/ACK”で応答する。



UDPポートへの接続への応答は、ポートが開いている場合、サーバ側からの応答はない。
閉じている場合、ICMP Port Unreachable が戻る。 サーバのOS設定、ファイアウォール設定で応答を戻さない設定にすると、UDPポートスキャンのリスクを低減することができる。

2-4-3　SIPメッセージのなりすまし（1/2）

SIPシーケンス（BYEリクエスト偽造の例）



攻撃者がダイアログIDを入手し、SIPメッセージを偽造する攻撃として、「TearDown攻撃」と呼ばれる、第三者からの呼の強制切断の例をしめす。

① 攻撃者は攻撃対象のSIPメッセージをパケットキャプチャ等で入手してダイアログIDを入手
② 対象のダイアログのダイアログID(“Call-ID”、“ローカルタグ”、“リモートタグ”)の値を入れ込んだ偽のBYEリクエストを作成しSIPサーバに送信する
③ SIPサーバは正当なリクエストと認識して呼を切断してしまう

IPTPC
IP Telephony Promotion Center

2-4-13 IP電話システムの不正使用・悪用

IP電話の不正使用

SIPサーバ、PBXの設定ミスなどにより攻撃者が利用者に成りすまし不正に国際回線に発呼を行う。業界団体の注意喚起によれば次のような原因で発生

- 攻撃者がインターネット経由で不正にSIPサーバにアクセスして利用者になりすまし
- 利用者が外出先から外線発信できる機能を悪用
- IP電話接続用ID/パスワードを入手して悪用

国際回線に架電することで接続先から報酬を受けるなどの犯罪手法があるといわれており、以前から事例が多い。

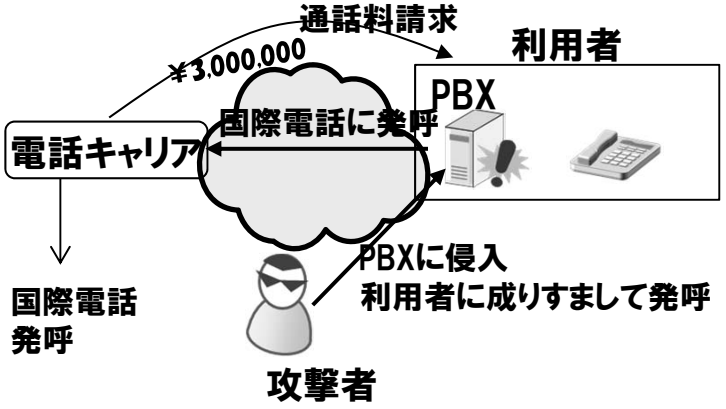
2015年には国内のIP電話サービスの不正利用が頻発し高額の国際電話費用が請求されることで社会問題化し総務省から業界団体に対策が要請された。

利用者等に対し、ホームページへの掲載などにより、接続・利用環境の確認※1、セキュリティ対策の強化※2などを要請する

※1 PBX等の通信機器の設定状況を確認し、不要に外部からの接続ができる設定になっていないかを確認し、不要な場合は削除する。
また、国際電話を利用しない場合には端末側で発信制限を行う。 等

※2 外部からの接続を許可する場合、「外部から接続する際のパスワード」や「各種設定や管理用のパスワード」について、第三者が推測しやすいパスワードや簡易なパスワードは設定しない。
また、使用するソフトウエアについて、最新のバージョンにアップデートする。通信機器にアクセスログを記録・保存する機能がある場合には、この機能を用いて不審なアクセスの有無をチェックする。 等

“第三者によるIP電話等の不正利用への対策について(要請)” (抜粋)



外部から接続でき、かつセキュリティ設定の弱いPBXに攻撃者が侵入し、 利用者に成りすまして国際電話を架電する。 利用者には電話会社から高額な請求が来る。


総務省
MIC Ministry of Internal Affairs and Communications

総務省トップ > お知らせ > 第三者によるIP電話等の不正利用に関する注意喚起

お知らせ

平成27年6月12日

第三者によるIP電話等の不正利用に関する注意喚起

IP電話をはじめとする電話サービスが第三者に不正利用され、利用者に高額な国際電話料金の請求がなされる問題が発生しています。こうした問題は、利用者がIP電話等の電話サービスを利用する際にインターネットに接続している通信機器(PBX(注)、IP電話対応のルータ等)におけるソフトウェアやハードウェアの設定の問題や、セキュリティ上の脆弱性を突いた「なりすまし」や「乗っ取り」による不正利用が原因であることが確認されています。
このため、IP電話等の電話サービスを利用する場合には、第三者による不正利用が行われないよう、ネットワークに接続している通信機器の設定状況を確認し、以下のようなセキュリティ対策を講じるよう お願いいたします。

1. PBX等の通信機器や使用しているソフトウェアの設定状況を確認し、不要に外部からの接続ができる設定になっていないかを確認するとともに、不要な接続環境は削除する。
2. 外部からの接続を許可している場合、「外部から接続する際のパスワード」や「各種設定や管理用のパスワード」について、第三者が推測しやすいパスワードや簡易なパスワードは設定しない。
3. 必要に応じて、通信機器やサービスを提供している事業者、保守ベンダー等に対して次の点を相談する。
(1)使用するソフトウェアについて、最新のバージョンにアップデートする等のセキュリティ対策を行う。
(2)通信機器やソフトウェアにアクセスログを記録、保存する機能がある場合には、アクセスログを記録、保存するようにし、不審なアクセスの有無をチェックする。
(3)電気通信事業者によっては、海外向けの電話番号への発信を規制するサービスを提供している場合があるので、国際通話を利用しない場合は、国際通話発信規制サービスの申込みを行う。
(4)電気通信事業者によっては、IP電話等が不正利用された場合に通話の宛先となることが多い国/地域を公表していることがあるので、機器やソフトウェアの設定により、これらの国/地域への発信を制限する。

総務省による注意喚起 (2015年6月)
http://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000191.html

第３章

ネットワークインフラへの脅威と対策

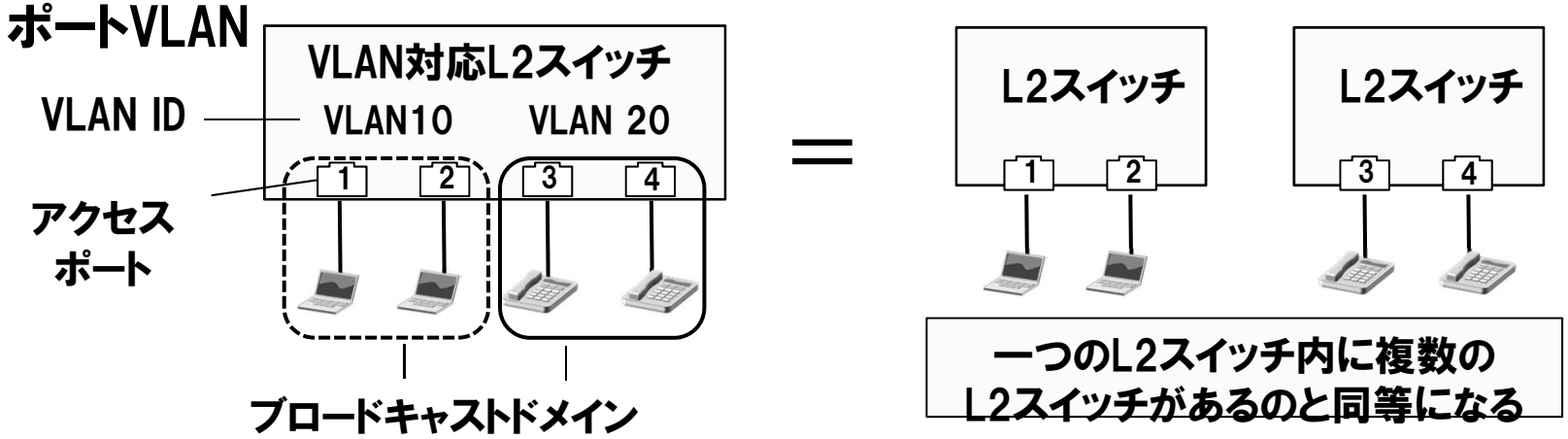
（4.0版）

1. IPネットワークインフラへの脅威
2. VLANによるネットワーク分割
3. フィルタリング
4. 外部ネットワークからの脅威と対策
5. ファイアウォール
6. NAT越えの課題と解決方法

3-2-2. VLANによるネットワーク分割（1/4）

VLAN（Virtual LAN）

- 論理的にLAN（ブロードキャストドメイン）を分割する機能
- VLANを利用することで、1台のスイッチを仮想的に複数のL2スイッチとして、LANケーブルを仮想的に複数の独立したLANケーブルとして扱えるため、収容効率が向上
- スイッチの設定でVLAN設定が行えるので、物理的なネットワーク構成を変更することなく論理的な構成を変更することが可能
- スイッチのポートとVLANが1:1に紐づく「ポートVLAN」、複数のVLANが紐づく「タグVLAN」がある



- VLAN対応のL2スイッチでは、ポートをグループ化してそれぞれのグループを独立したLANとして扱うことができ、ブロードキャストドメインを分割できる
- VLANは「VLAN ID」と呼ばれる識別子で管理され同じVLAN ID に属す通信は同じLANに接続されているのと同じ挙動となる。
- VLAN ID は1～4094 の範囲で利用できる（VLAN ID 0と4095は特別用途として利用される）
- 上図のように、ポートとVLAN ID を1:1に紐づける方式を「ポートVLAN」と呼ぶ。またポートVLANで利用するポートを「アクセスポート」と呼ぶ

3-6-1. NAT越え問題(NATとは)

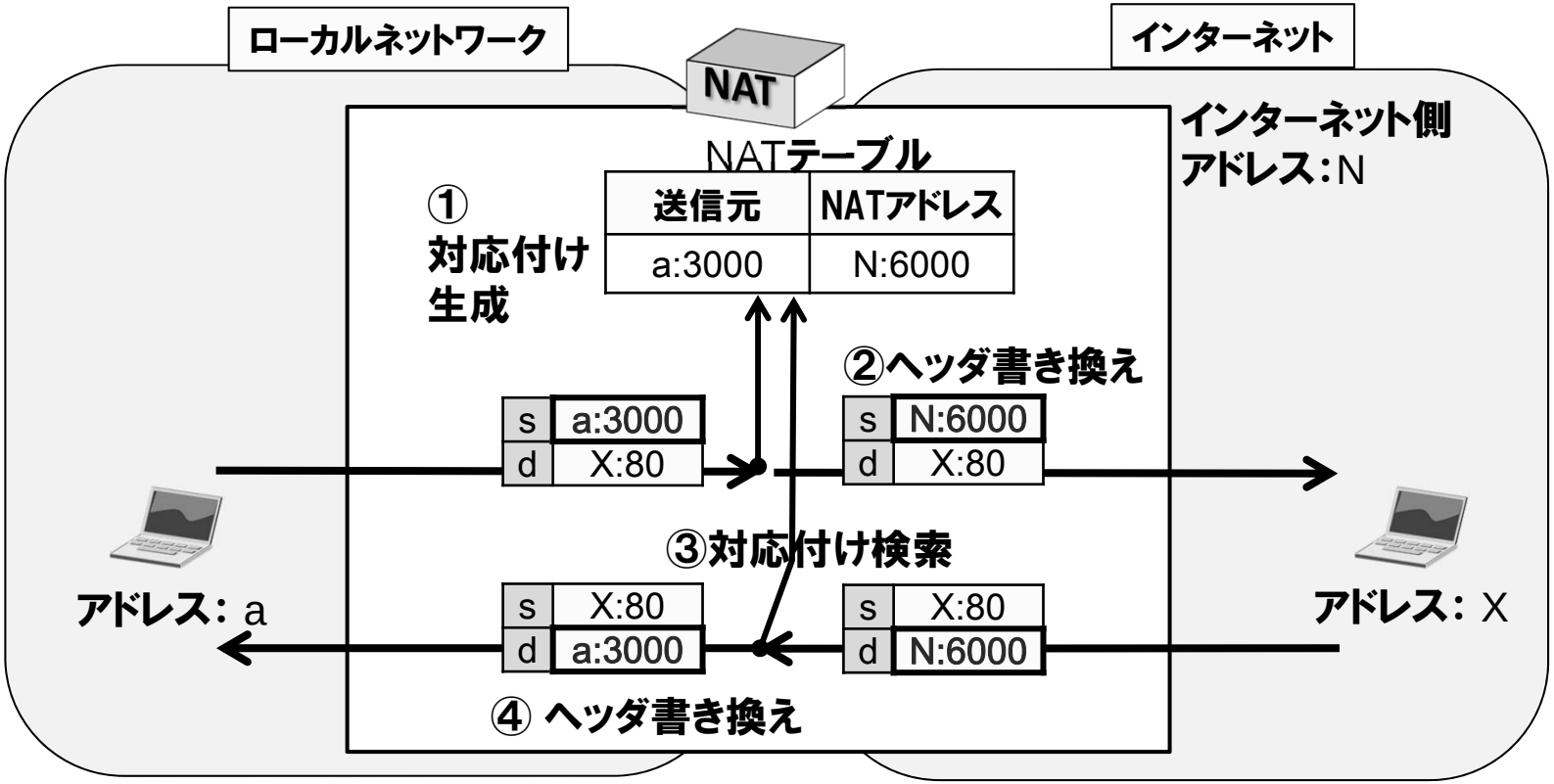
NAT (Network Address Translator)

直接通信ができないネットワーク間で通信を可能にするためのアドレス変換装置。ファイアウォールにも実装されている
送信元とNATのアドレス情報(IPアドレスとポート番号)の対応付けを行い(①)、IPヘッダの書き換えを行う(②)
インターネット側のデバイスがNAT宛てに返信すると、NATテーブルで対応付けを検索し(③)ヘッダを書き換えて転送する(④)

本テキストでの記法

s	a:3000
d	X:80

「s」:送信元
IPアドレス: a ポート番号: 3000
「d」:送信先
IPアドレス: X ポート番号:80
太枠: ヘッダの書き換え対象



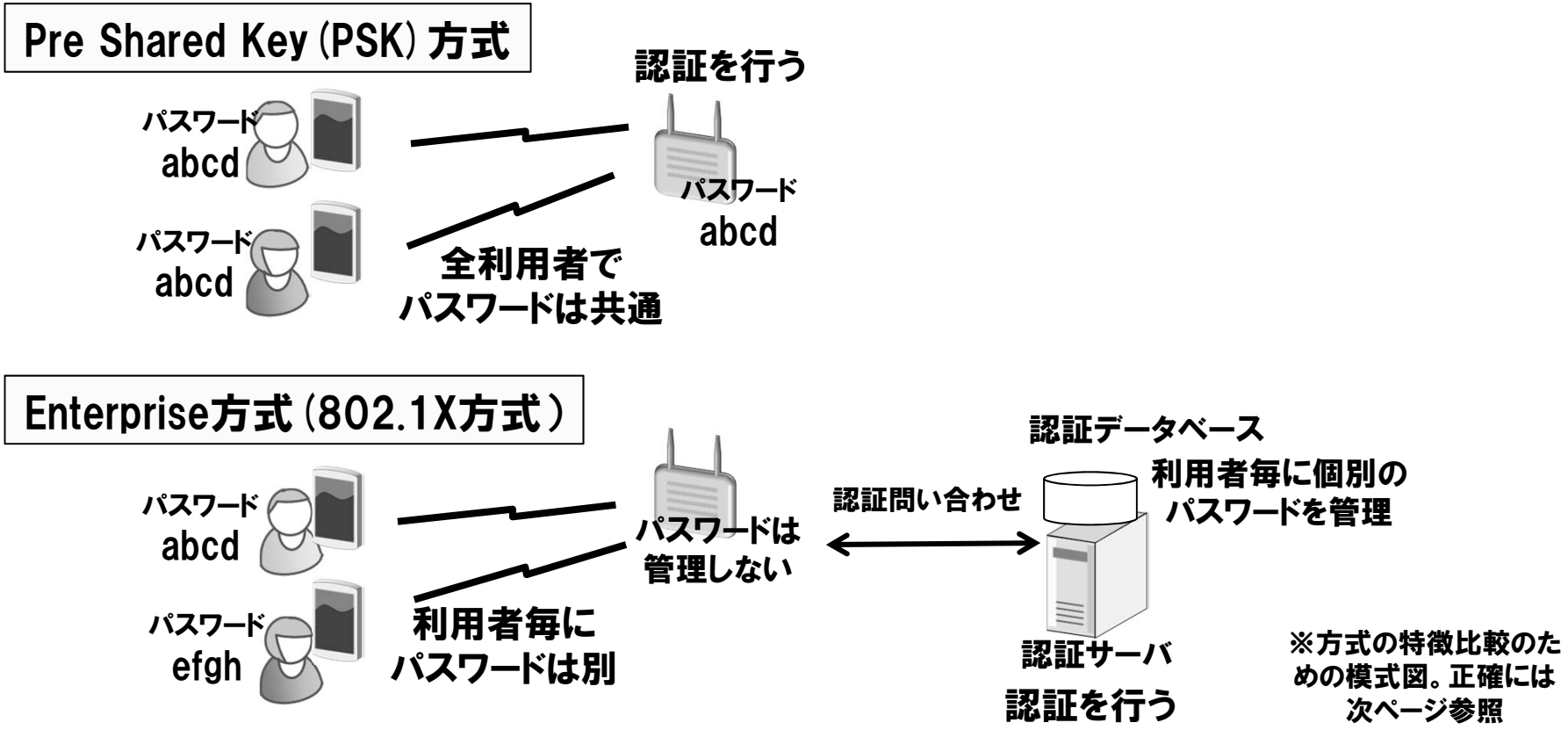
第4章

クライアント・ユーザアクセスインフラの脅威と対策

(4.0版)

1. クライアント・ユーザアクセスインフラの脅威
2. 無線LANの脅威と対策
3. 有線LANの脅威と対策
4. リモートアクセスの脅威と対策
5. クライアントデバイスの脅威と対策

4-2-9　認証(PreShared Key方式とEnterprise方式の比較)



PreSharedKey(PSK) 方式: 認証はAPで行う。APに設定したパスワードと同じパスワードで各ユーザが接続する。パスワードが漏洩した場合、全員のパスワードを更新する必要がある
Enterprise方式: 認証は「認証サーバ」で行う。利用者毎に個別にパスワードを設定する。認証には IEEE802.1X という方式を用いる。

企業用途では一般的にはEnterprise 方式を用いる

IPTPC
IP Telephony Promotion Center

4-2-11　認証：EAP 各方式

EAPは認証サーバ、サプリカントの認証方式の違いなどで複数の方式が存在する。
Windowsの標準サプリカントのサポート状況と、導入の手間から、EAP-PEAPの使用事例が多い

セキュリティレベル　高 ⟷ 低
導入コスト・手間　高 ⟷ 低

認証サーバの認証	証明書	証明書	独自方式	なし
サプリカントの認証	証明書	IDパスワード等	IDパスワード等	IDパスワード等
方式	EAP-TLS	EAP-PEAP EAP-TTLS EAP-GTC	EAP-LEAP EAP-FAST	EAP-MD5

標準サプリカントのEAP各方式サポート状況

	Windows 8 Windows10	iOS 8.1	Android 5.0 (*)
EAP-TLS	○	○	○
EAP-PEAP	○	○	○
EAP-TTLS	○	○	○
EAP-GTC	×	○	×
EAP-LEAP	×	○	×
EAP-FAST	×	○	×
EAP-MD5	×	×	×

(*) 機種により差異あり

第５章

セキュリティ設計概論

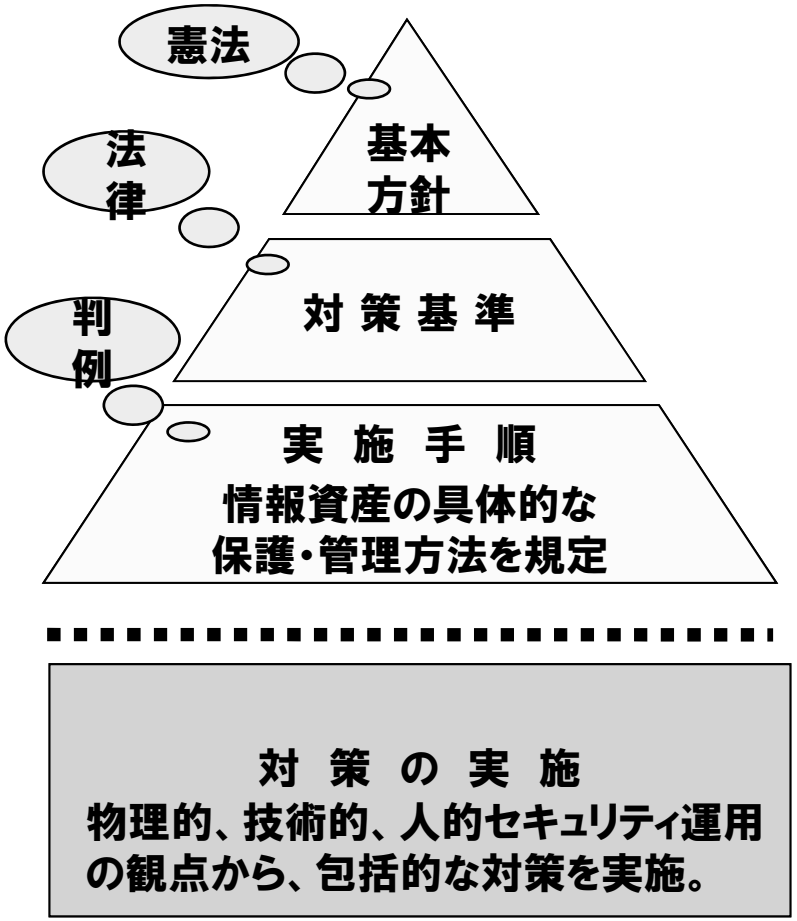
（4.0版）

１．セキュリティ設計の手順
２．VoIPシステムのセキュリティ設計
３．セキュリティの評価

5-1-2. ポリシー策定(1/4) - ポリシーとは -

参考

セキュリティポリシーは、組織や情報システムが持つどのような情報資産をどのように保護するかの方針を定めたものである。通常、各システムのポリシーの策定時には組織レベルのポリシーがあり、それに準じて策定する。



・基本方針
情報資産の保護に関する組織の基本的な考え方を示す。

・対策基準
情報資産を保護するために遵守すべき行為、判断等に係る共通の基準を示す。

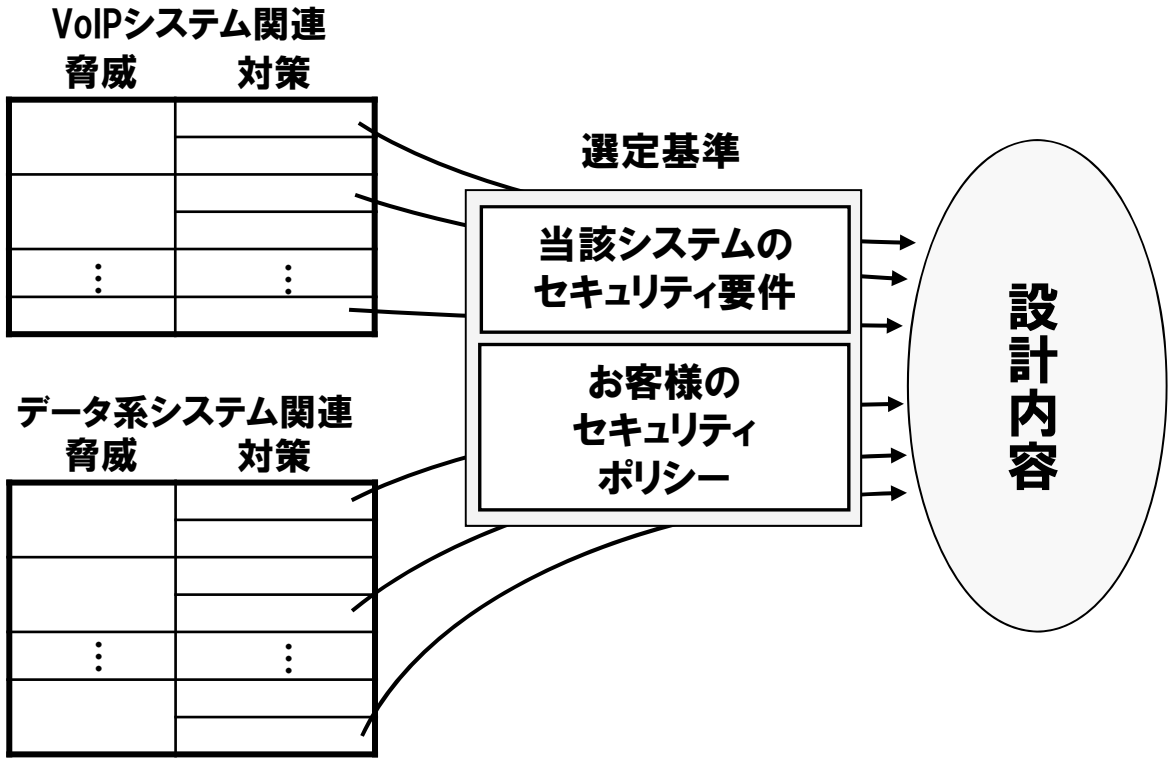
・実施手順
対策基準に定められたことをどのように実現するか、どのような情報資産をどのように保護するか、具体的な方法を明文化したもの(マニュアル、手続き)。

※ どこまでをポリシーに含めるかは場合による。
ファイアウォール機器などの設定ファイルのことをセキュリティポリシーと呼ぶ場合もある。

5-2-1. VoIPシステムにおけるセキュリティ設計(1/2)

VoIPシステムにおけるセキュリティ設計では、お客様それぞれのシステムに対する脅威を洗い出し、前節で述べたような対策の中から適切な対策を選定する。対策の選定においては、当該システムにおけるセキュリティ要件や、お客様のセキュリティポリシーに従って選定する。

また、VoIPシステムのセキュリティ設計は、データ系システムのセキュリティ設計と併せて行う必要がある。



第6章

セキュリティ運用

（4.0版）

１．セキュリティの運用とは
２．セキュリティ維持管理のための運用
３．VoIPシステムにおけるセキュリティ運用ポイント

IPTPC
IP Telephony Promotion Center

6-1-1. セキュリティの運用の意味

■セキュリティの運用の二つの意味

「セキュリティの運用」には、以下の二つの意味がある。

・組織として、セキュリティを維持管理、改善するための枠組みを運用する

・上記の仕組みの中で、実際にリスク対応の対策を実施し、運用する

組織としてのセキュリティ維持管理の枠組みのことを、ISMS(情報セキュリティマネジメントシステム)と呼ぶ。

■ISMSのプロセスモデル

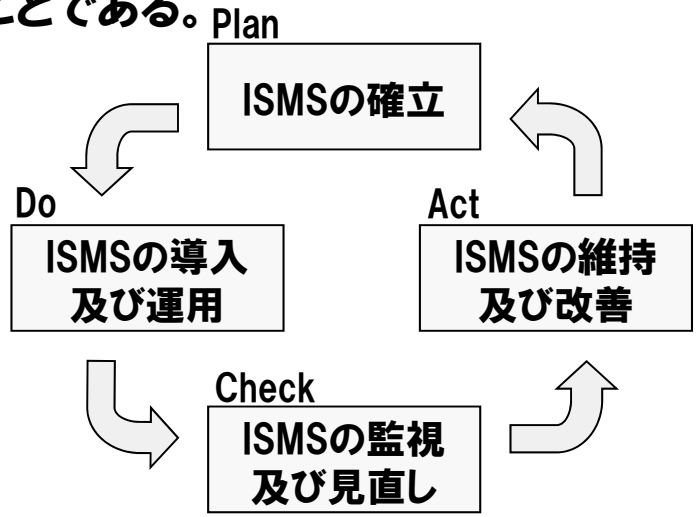
ISMSの運用とは、以下のPDCAサイクルを回すことである。

・Plan-計画:ISMSの確立
　ポリシー、規程、対策立案

・Do-実施:ISMSの導入及び運用
　対策実施、運用

・Check-点検:ISMSの監視及び見直し
　実施状況の評価

・Act-処置:ISMSの維持及び改善
　是正処置、予防処置



構築、維持、及び改善サイクル

出展:ISMS認証基準(Ver. 2.0)
(財)日本情報処理開発協会

※ ISMSの標準規格:国際標準「ISO/IEC 27001:2005」、
国内ガイドライン「JIS Q 27001、27002」

※ ISMS適合性評価制度:(財)日本情報処理開発協会が実施、企業のISMSがISO/IEC 27000に準拠していることを認証

IPTPC
IP Telephony Promotion Center

6-3-1. 運用の実施項目

VoIPシステムの運用は、セキュリティポリシーの策定の段階で作成した実施手順に従って、システムを正常に利用できる状態に保つために必要な活動である。
これらはVoIPシステムに限らず、全てのネットワークの運用に共通する。

■NWの監視と構成見直し
トラフィック量が増加し、システム設計時の条件に合わなくなると予想される場合、機器の増設、帯域の増加などを計画する必要がある。

■機器の最新アップデート
セキュリティの問題や不具合の修正など、機器ベンダが提供する最新アップデートを入手し※、アップデートの必要性を判断した上で必要なアップデートを実施する必要がある。

■異常の検出と原因の排除
異常の検出はVoIP機器、ネットワーク機器の監視による検出が主になるが、利用者からの申告も重要な手掛かりとなる(電話が繋がらない、通話中の音が悪いなど)。
原因にはウイルスの影響だけでなく機器の故障、使用方法の誤りなどなど様々なものが考えられるが、原因を突き止めて解決する必要がある。

■バックアップ
ウイルスによるシステム破壊や機器のハードウエア故障など、機器の交換や再インストールによる復旧に備えて、装置やシステムの構成を変更した際には構成ファイルなどのバックアップを取る必要がある。

※ 機器のアップデートは、製品ベンダからの情報に従うのが基本である。例えば機器のOSの製造元からパッチが出たような場合でも、製品ベンダが確認を取った後に適用する。

巻末資料

（4.0版）

IPTPC
IP Telephony Promotion Center

巻末2. セキュリティ対策(暗号)の用語

■ 暗号アルゴリズム (Cipher Algorithm)

- オリジナルのデータを第3者から覗き見されるあるいは改ざんされるのを防ぐ目的で、データを平文から暗号文に変換するアルゴリズムを適用した処理。平文(Clear-text、クリアテキスト)とは暗号化されていないデータであり、プレーンテキストとも言う。暗号化されたデータは暗号文と言う。
- 対称暗号アルゴリズムと非対称暗号アルゴリズムある。暗号化と復号化に公開鍵(パブリック鍵)と秘密鍵(プライベート鍵)を使用する方法が異なる。

■ セキュリティ・プロトコル

- 暗号化鍵のやりとりを含めた、平文→暗号化アルゴリズム→暗号文の組合せのこと。暗号化プロトコルともいう。

■ AES (Advantage Encryption Standard)

- 米国商務省のNIST が、解読される可能性が高まったDES (Data Encryption Standard) 及び3DES ("triple" DES)に代わって公募した新しい標準暗号化プロトコルである。「Rijndael」が選ばれた。
- DESは64ビットをブロック単位として64ビットの鍵長を用いているが、AESは128、192、256ビットの鍵長を用いている
- AESは高速での暗号化・復号化が可能であり、汎用性においても優れているため、ハードウエアやソフトウエアに対しても実装が可能となっている。

■ 電子証明書 (Certificate, Digital Certificate)

- 認証局(CA:Certificate Authority) が発行する証明書で、公開鍵が特定のユーザまたは端末、サーバ等とそのアプリケーションのものであることを保証するものである。

■ デジタル署名 (Digital Signature)

- 受信したメッセージが、送信者本人から送られてきたものであることを証明できる電子的な署名。
- 送信者は送信メッセージをダイジェスト化し、送信者本人の秘密鍵で暗号化してデジタル署名とする。受信者がそのメッセージ認証をするために、受信したデジタル署名を送信者の公開鍵で復号する。

IPTPC
IP Telephony Promotion Center

セキュリティ関連の法規制

情報セキュリティに関する法令

著作権法

1985年　法改正により「コンピュータプログラムの著作権」追加
1986年　法改正により「データベースの著作権」追加
1987年　法改正により「ホームページの著作権」追加

刑法

1987年　法改正により「コンピュータ犯罪防止法」追加

- 161条の2　文書偽造の罪（電磁的記録不正作出及び供用）
- 163条　支払用カード電磁的記録に関する罪
- 234条の2　信用および業務に対する罪（電子計算機損壊等業務妨害）
- 246条の2　詐欺罪（電子計算機使用詐欺）
- 258,259条　毀棄（きき）および隠匿の罪（公用文書等毀棄、私用文書等毀棄）

不正競争防止法

1991年　法改正により「トレードシークレット（営業秘密）に対するスパイ行為やハッキングによる侵害」追加

不正アクセス禁止法（不正アクセス行為の禁止等に関する法律）

2000年　施行、 不正アクセス行為（セキュリティホールを突く行為も含む）の禁止、不正アクセスを助長する行為の禁止、および不正アクセスを受けた管理者への援助処置を含む

電子署名法（電子署名及び認証業務に関する法律）

2001年　施行

- 第二章　電磁的記録の真正な成立の推定
- 第三章　特定認証業務の認定等