セキュアなネットワーク構築について

～企業における社内LAN構築から
公開サービスの提供までのリスクと対策～

平成16年度　OISA技術研究会
「セキュリティ部会」

部会員紹介

松茂良　潔	（部会長）	株式会社富士通ソフトウェアラボラトリ
		株式会社オーイーシー
大塚　哲教	（副部会長）	中津コンピュータカレッジ
藤本 伸一		株式会社エイビス
上田　雄三		新日鉄ソリューションズ株式会社
奥山　洋平		有限会社オール人材活用センター
岡崎　慎司		日立SC株式会社
平井　　亮		株式会社オーイーシー
黒川　梨沙		システムエイジ株式会社
臼杵　敏雄	（技術委員）	三井造船システム技研株式会社
三宮　由裕	（技術委員）	

目次

はじめに

◆ 情報漏洩の事例

2004年3月

大手通販会社から数十万人分の顧客情報流出の可能性

システム開発会社から漏洩した可能性大。販売活動自粛等で損失は数十億にのぼる勢い

2002年5月

大手エステの5万人分の詳細情報が閲覧可能状態に

大規模なクレーム対応窓口を編成して対処
10人が計1，150万円の損害賠償を求める訴訟中

2002年2月

某コンピュータメーカによる防衛庁機密データ流出

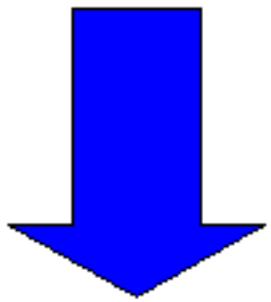
外注技術者が資料を家に持ち帰り漏洩
横浜地裁で、実刑判決(2003.4)

はじめに

◆ 何故情報が漏洩するか？

必要なだけのセキュリティレベルが確保されていない

関係者の教育が不完全である



セキュアなネットワークを

構築するところから考えてみる

概要

企業におけるLAN構築について、社内LANの構築・インターネットへの接続・公開サービスの提供という流れの中で想定されるリスク（情報漏洩など）と、その原因、具体的な対策の提案を行う。

1．社内LAN構築におけるリスク・原因・対策

1－1. 社内LAN構築におけるリスク

- リスク一覧
  - A） なりすましによる社内LANへの侵入。
  - B） 情報の損失・漏洩・改ざんが行われる。
  - C） LANが破壊される。

A） なりすましによる社内LANへの侵入

◆ 想定される被害

1. 社内LANへの不正アクセス。
2. 社内機密情報への不正アクセス。

◆ 原因

1. 外部の人間から出力装置が見える。
2. 外部の人間が利用出来る範囲に端末がある。
3. 推測しやすいパスワードの使用。
4. パスワードの保持期間が長い。

B） 情報の損失・漏洩・改ざんが行われる

◆ 想定される被害

1. 信頼の喪失。

◆ 原因

1. 外部の人間が利用出来る範囲にHUBがある。
2. 通信機器の空ポートを塞いでいない。
3. ESSIDがデフォルトである。
4. 暗号化していない。
5. 接続許可端末を設定していない。
6. サーバへのアクセスが制限されていない。
7. プリンタへの印刷権限がされていない。
8. 記録媒体の保管が不適切。
9. 端末が固定されていない。
10. 廃棄したパソコンのHDDの取り扱いが不十分。
11. パケット盗聴の対策がとられていない。

C） LANが破壊される

◆ 想定される被害

1. 社内機密情報の漏洩。
2. 社内LANへの不正アクセス。
3. 業務の停止。

◆ 原因

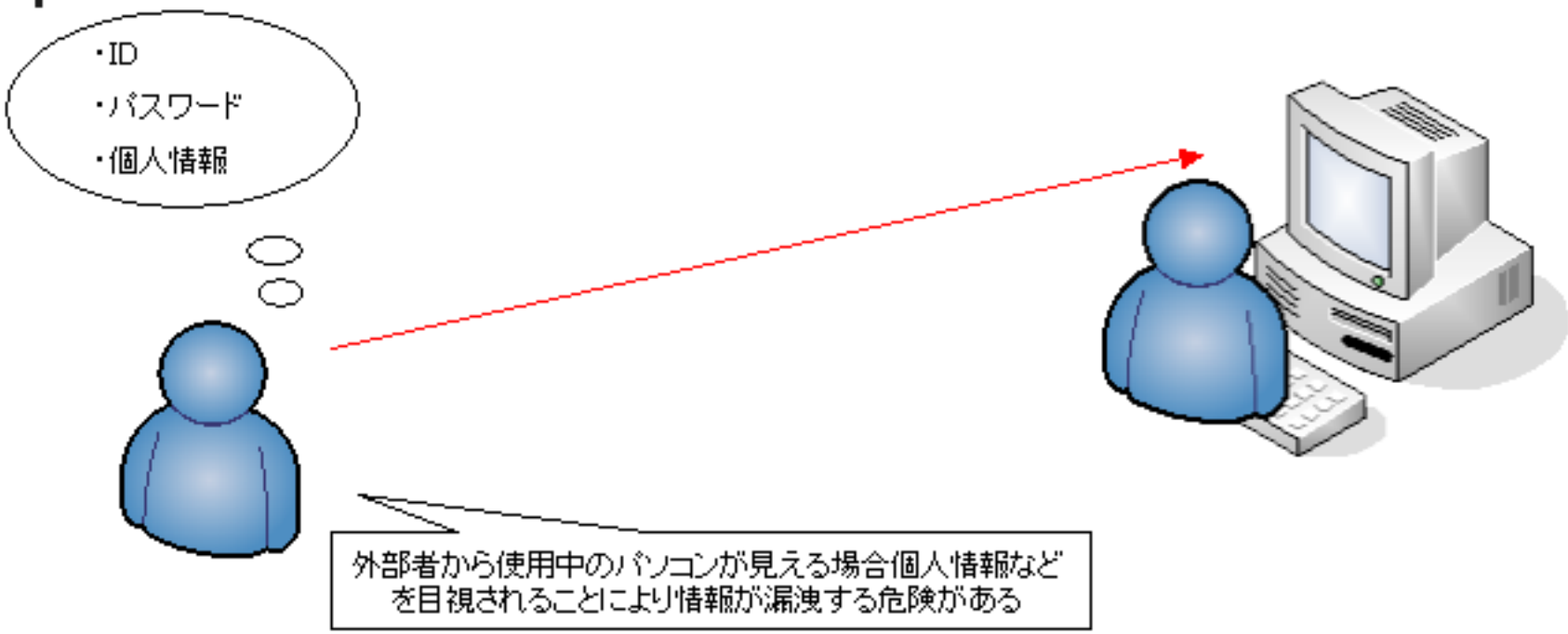
1. 外部の人間が利用出来る範囲にHUBがある。
2. 通信機器の空ポートを塞いでいない。
3. ESSIDがデフォルトである。
4. 暗号化していない。
5. 接続許可端末を設定していない。

１－２. 社内LAN構築におけるリスクの原因と対策

◆ 原因一覧

A) 外部の人間から出力装置が見える。
B) 外部の人間が利用出来る範囲に端末及びHUBがある
C) 無線LANの管理体制に不備がある
D) パケット盗聴の対策がとられていない。
E) サーバへのアクセスが制限されていない。
F) プリンタへの印刷権限がされていない。
G) コンピュータ または 記録媒体の保管が不適切。
H) 廃棄したパソコンのHDDの取り扱いが不十分。
I) パスワードの管理体制の不備。

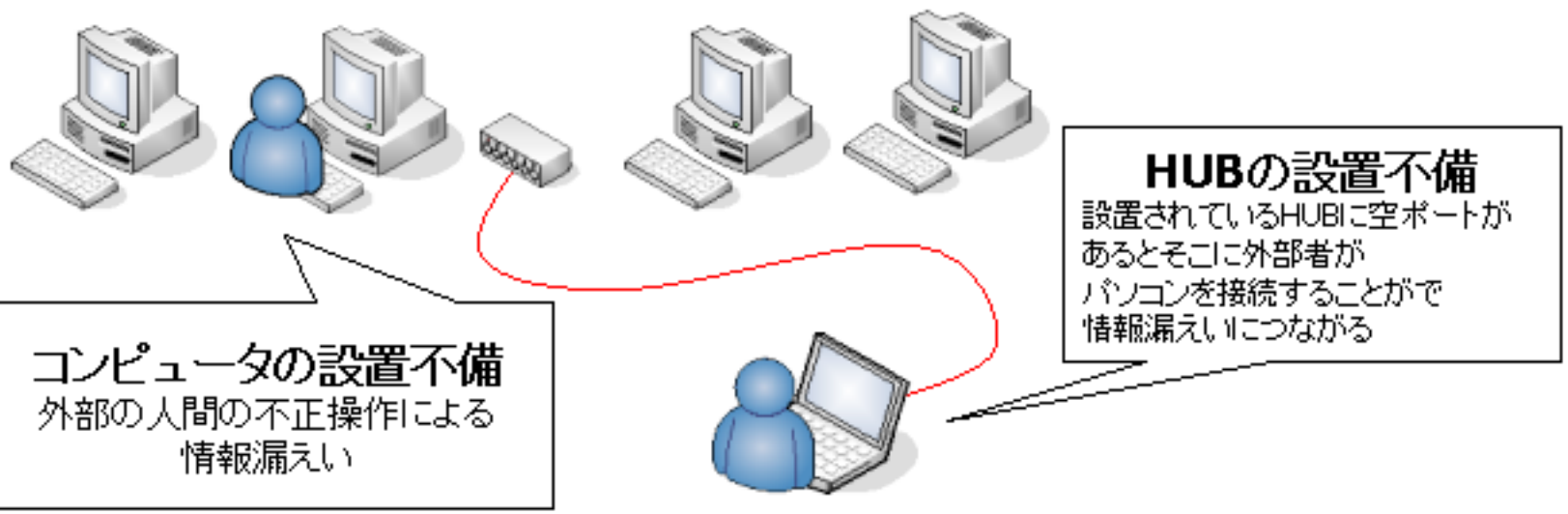
A）外部の人間から出力装置が見える



◆導入時の対策

- 外部の人間が直接画面を見ることができないようなレイアウトにする
- 閉鎖された空間におく場合は、外部の人間が入れないようにIDカードなどの認証システム、監視カメラを設置する

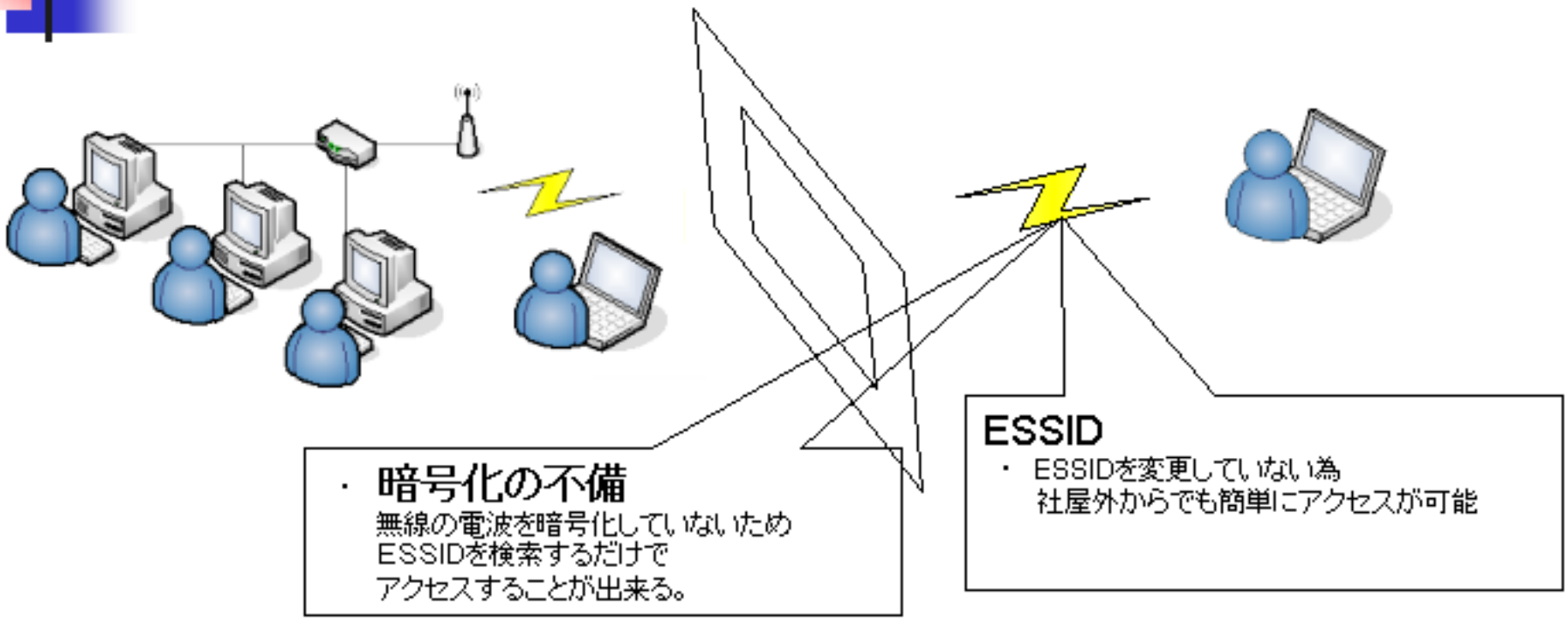
B）外部の人間が利用出来る範囲に端末及びHUBがある



◆導入時の対策

- 外部の人間外出入りする共有スペースにHUBを設置しない。
- MACアドレスで接続可能な端末の制限を行う。
- 床下やサーバラック内などにHUBを設定する。
- 外部の人間外出入りする共有スペースにHUBを設置しない。
- MACアドレスで接続可能な端末の制限を行う。
- 床下やサーバラック内などにHUBを設定する。

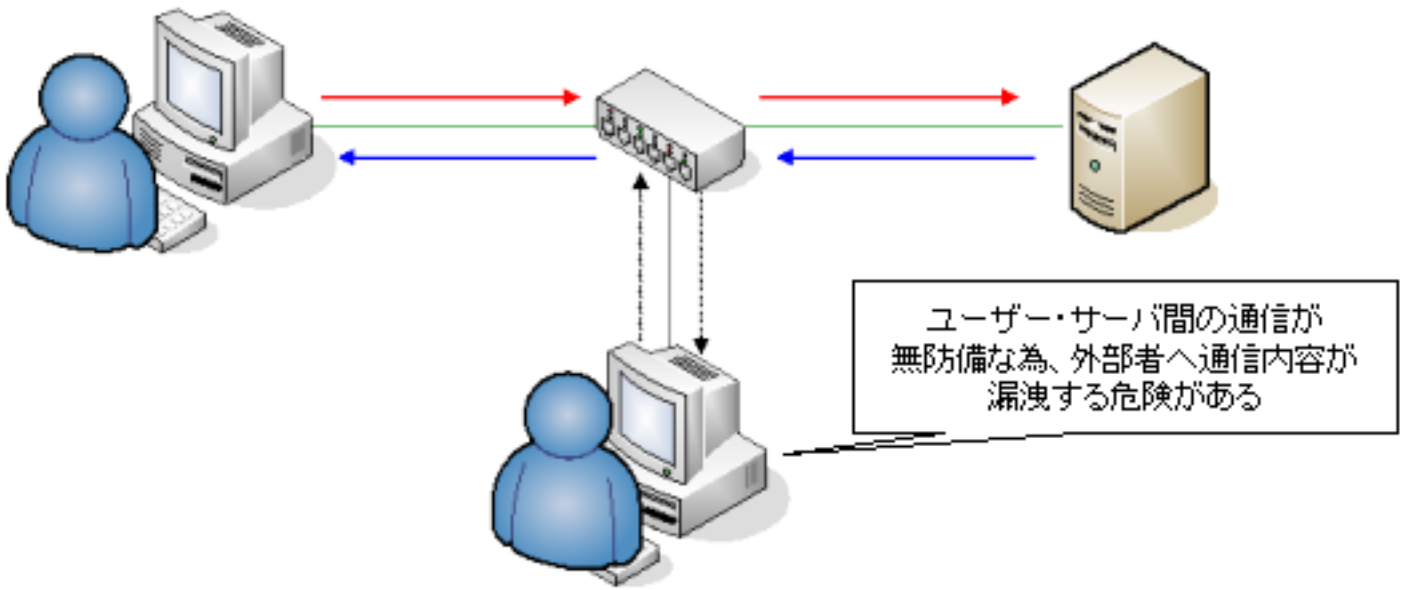
C）無線LANの管理体制に不備がある



◆導入時の対策

- ESSIDを非通知設定に変更する。
- デフォルトで設定されているESSIDを削除する
- 推測されにくいESSIDを設定する。
- WEPを使用してデータの暗号化を行う。
- よりセキュリティ強度の高いWPAを使用する

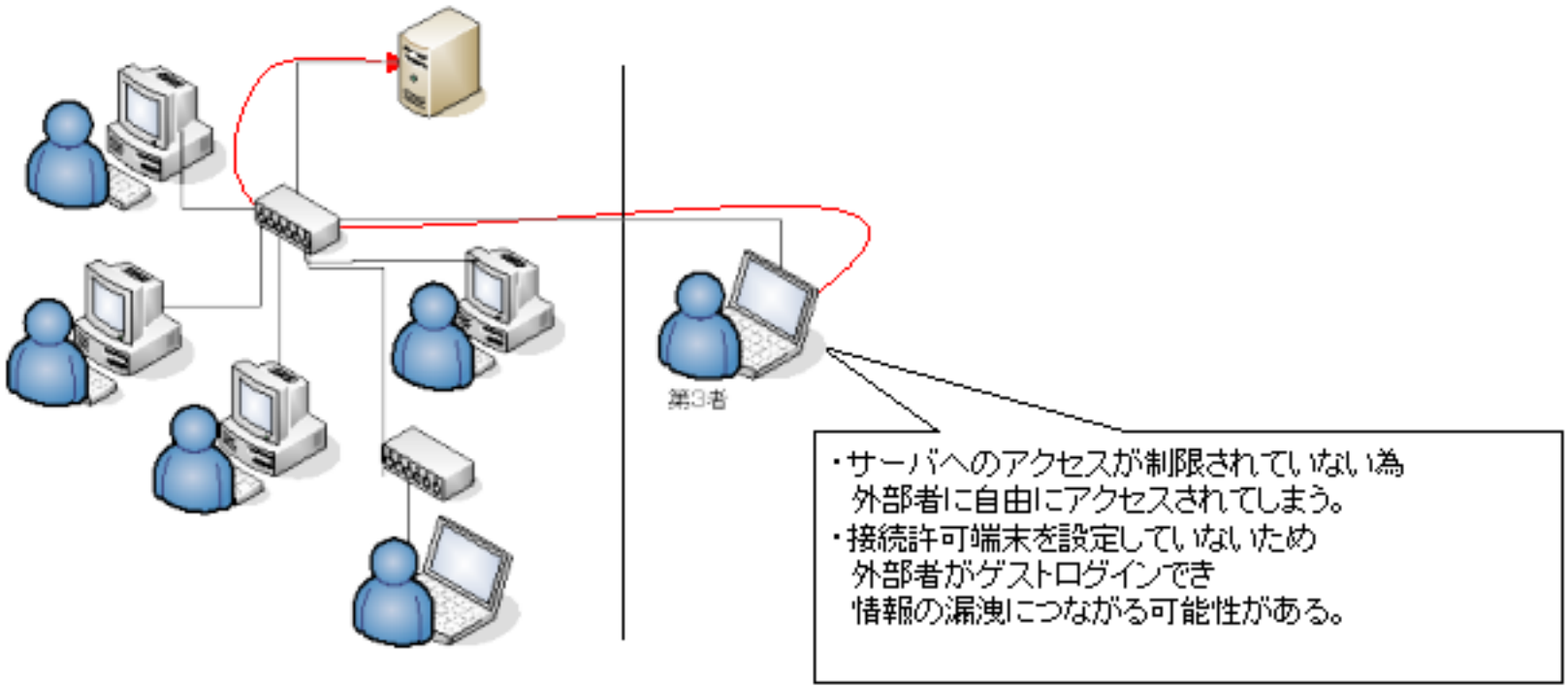
D）パケット盗聴の対策がとられていない



◆導入時の対策

- SSLなどを利用して通信データを暗号化する。
- スイッチングHUBなどを利用して不要な場所にデータを流さないようにする。

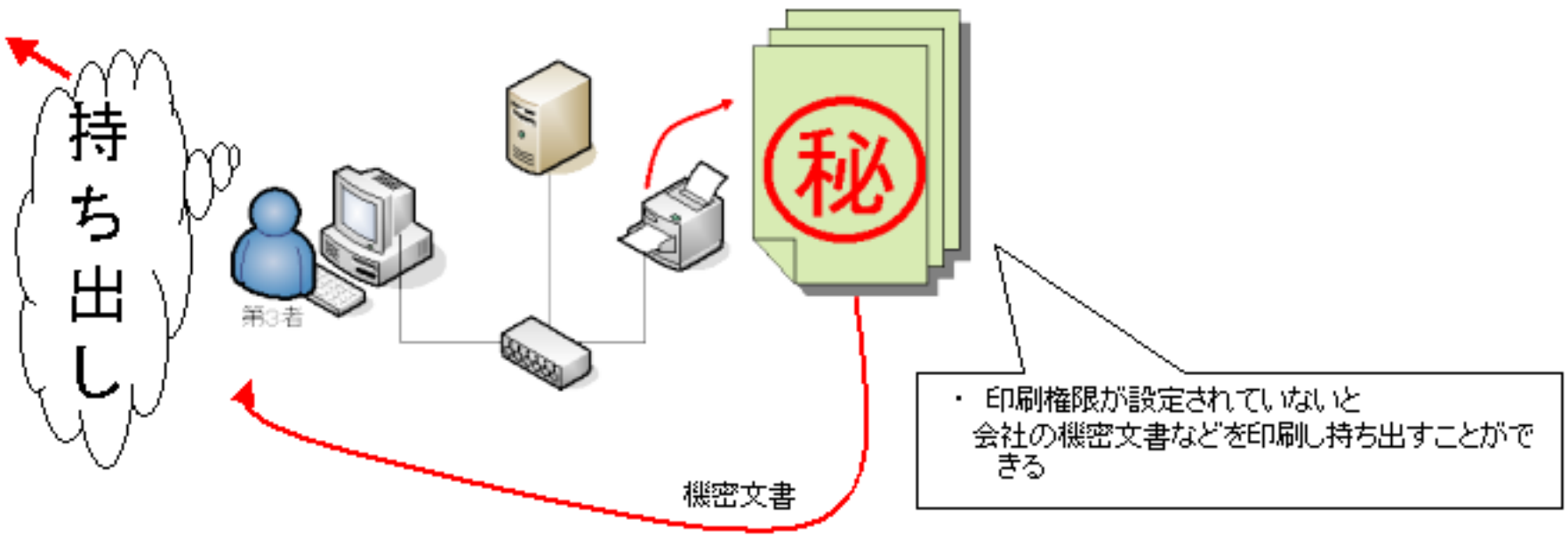
E）サーバへのアクセスが制限されていない



◆導入時の対策

- 管理者権限を持つユーザーは最小限にとどめる。
- データの使用目的に合わせて適切なアクセスコントロール設定を行う。
- 接続可能なクライアントを制限する。
- MACアドレスによる接続可能名端末の制限を行う。

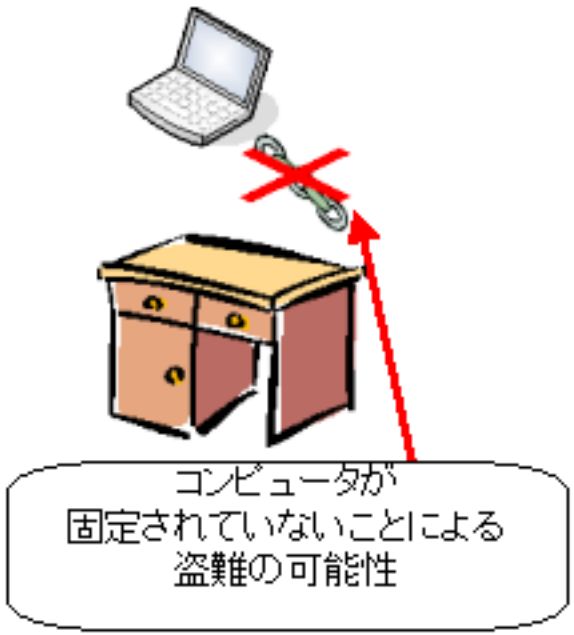
F)プリンタへの印刷権限がされていない



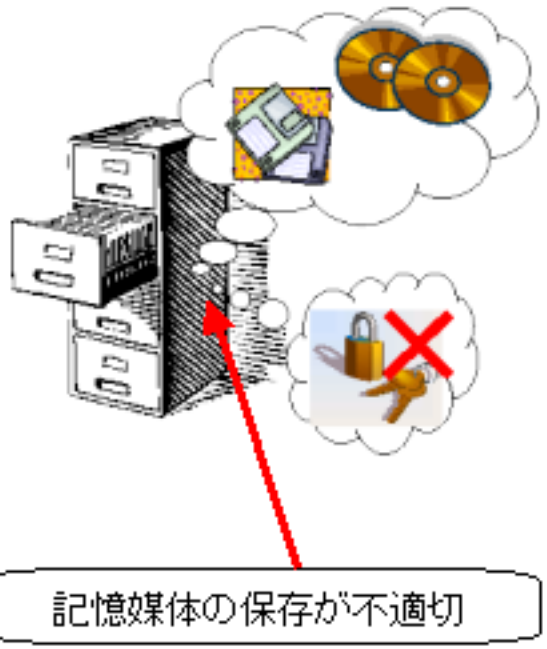
◆導入時の対策

- 全体でプリンタを共有している場合は、IDカードなどで個人を特定してプリンタの印刷制限を行う。
- 端末ごとにプリンタを共有している場合は、端末の印刷設定を管理する。

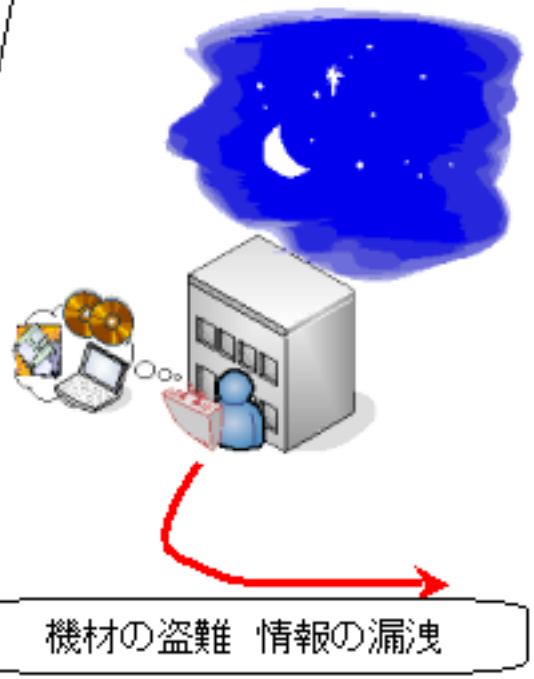
G)コンピュータ または 記録媒体の保管が不適切



コンピュータが
固定されていないことによる
盗難の可能性



記憶媒体の保存が不適切



機材の盗難　情報の漏洩

◆導入時の対策

- 施錠できる保管場所で記録媒体の管理を行う。
- 記録されているデータを暗号化しておく。
- 盗難防止ワイヤーなどを利用して端末を固定する。

H）廃棄したパソコンのHDDの取り扱いが不十分

廃棄パソコン

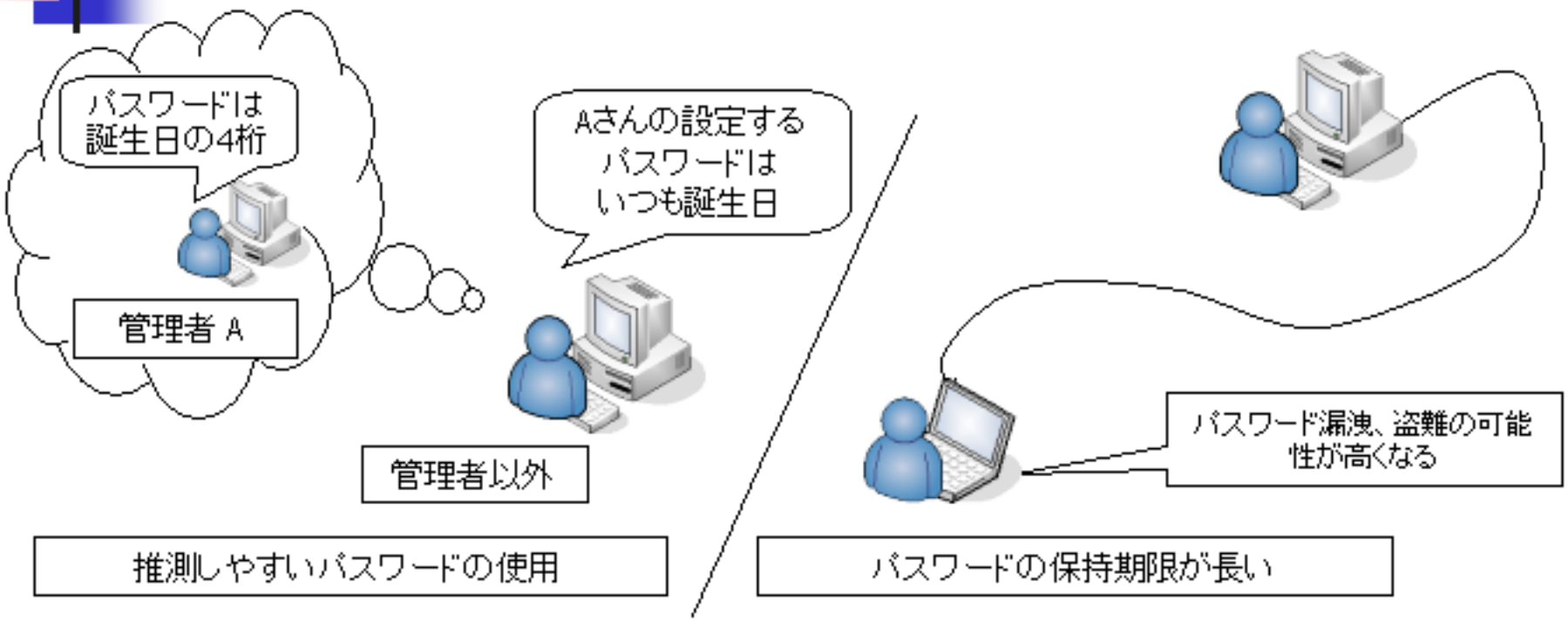
重要データ取り出し

流出

◆導入時の対策

- 削除ツールなどを利用してHDDの初期化を行う。
- 記録されているデータを暗号化しておく。

I) パスワードの管理体制の不備



◆導入時の対策

- 定期的にシステムのパスワード変更を強制させる。
- 世代管理を行い、以前入力したパスワードを設定できないようにする。
- ポリシーを作成し、英数特殊文字を含む8文字以上のパスワード設定を強制する。
- 初期パスワードを変更させる。

2. 外部との接続におけるリスク・原因・対策

2－1．外部との接続におけるリスク

◆ リスク一覧

A） インターネット経由での漏洩

B） インターネット経由でのウイルス感染と二次被害

C） インターネット経由での不正侵入による
情報の漏洩、損失、改ざん

D） 外部からの攻撃

E） 通信が盗聴される

F） 通信経路からの不正侵入

A） インターネット経由での漏洩

◆ 想定される被害

1. 外部への個人情報の漏洩
2. 個人情報の悪用

◆ 原因

1. インターネットへの接続制限がされていない
2. 不必要な通信を許可している
3. ユーザのセキュリティ知識の不足

B） インターネット経由でのウイルス感染と二次被害

◆ 想定される被害

1. 社内情報の漏洩、改ざん、破壊
2. 社外へのウィルスの散布
3. バックドアの設置による不正アクセス

◆ 原因

1. ウィルス対策ソフトが未導入、未更新
2. ルータ、ファイアウォールの設定が不適切
3. OS、ブラウザのパッチが古い

C） インターネット経由での不正侵入による情報の漏洩、損失、改ざん

- 想定される被害
  1. 社内機密情報（顧客情報、社員情報等）の漏洩、損失、改ざん
  2. 企業イメージの低下
  3. 信頼の喪失
- 原因
  1. ルータ、ファイアウォールの設定が不適切
  2. OS、ブラウザのパッチが古い
  3. 外部からの不正アクセスの対策が不十分

D） 外部からの攻撃

◆ 想定される被害

1. ポートスキャンによる不正侵入
2. Dos攻撃によるサーバのダウン
3. 踏み台として利用される

◆ 原因

1. ルータ、ファイアウォールの設定が不適切
2. OS、ブラウザのパッチが古い
3. 外部からの不正アクセスの対策が不十分

E） 通信が盗聴される

◆ 想定される被害

1. 社内機密情報の漏洩
2. 漏洩情報の悪用

◆ 原因

1. データ通信が暗号化されていない
2. データ通信の暗号化強度の不足
3. 同一暗号鍵を長期間利用している
4. 重要文章を暗号化せずに送信している

F） 通信経路からの不正進入

◆ 想定される被害

1. 社内機密情報（顧客情報、社員情報等）の漏洩、損失、改ざん
2. 企業イメージの低下
3. 信頼の喪失

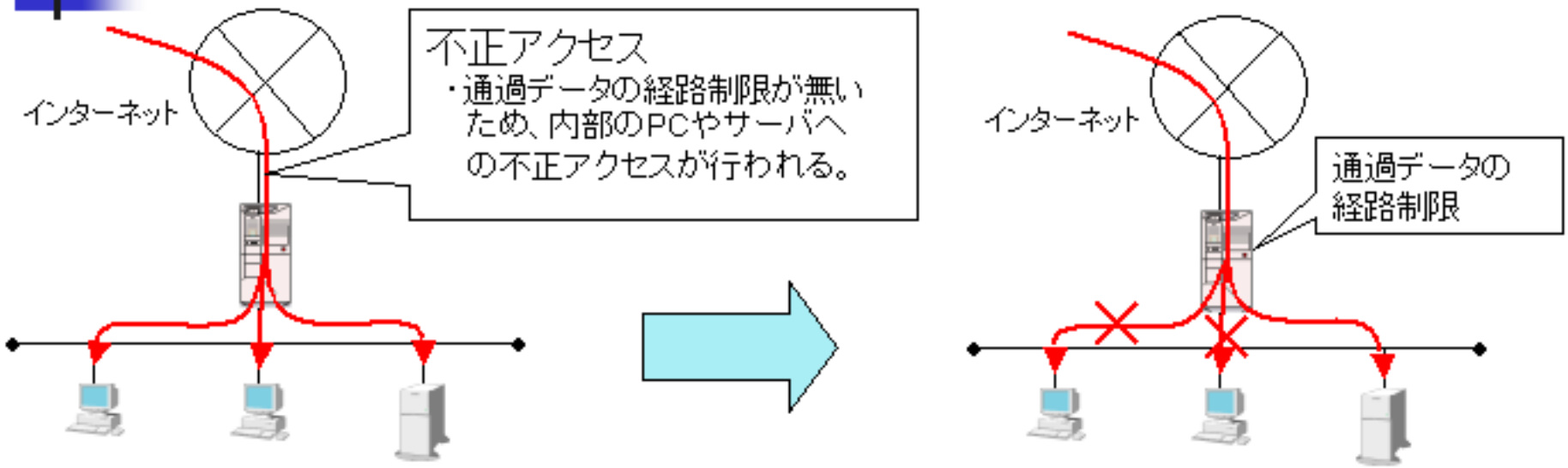
◆ 原因

1. ネットワークが分断されていない
2. 発信、着信制御を行っていない
3. 接続用グローバルIPアドレスを固定していない
4. サーバへのアクセスが制御されていない
5. 通信機器のファームウェアが古い

2－2. 外部との接続におけるリスクの原因と対策

- 原因一覧
  - A) ルータ、ファイアウォールの設定が不適切
  - B) インターネットへの接続が未制限
  - C) OS、ブラウザのパッチが古い
  - D) ウイルス対策ソフトが未導入、未更新
  - E) 不必要な通信が許可されている
  - F) 外部からの不正アクセスの対策が不十分
  - G) ユーザのセキュリティ知識の不足
  - H) ネットワークが分断されていない
  - I) 発信、着信制御を行っていない
  - J) 接続用グローバルIPアドレスを固定していない
  - K) データ通信が暗号化されていない
  - L) データ通信の暗号強度の不足
  - M) 同一暗号鍵を長期間利用している
  - N) 重要文章を暗号化せずに送信している
  - O) サーバへのアクセスが制限されていない
  - P) 通信機器のファームウェアが古い

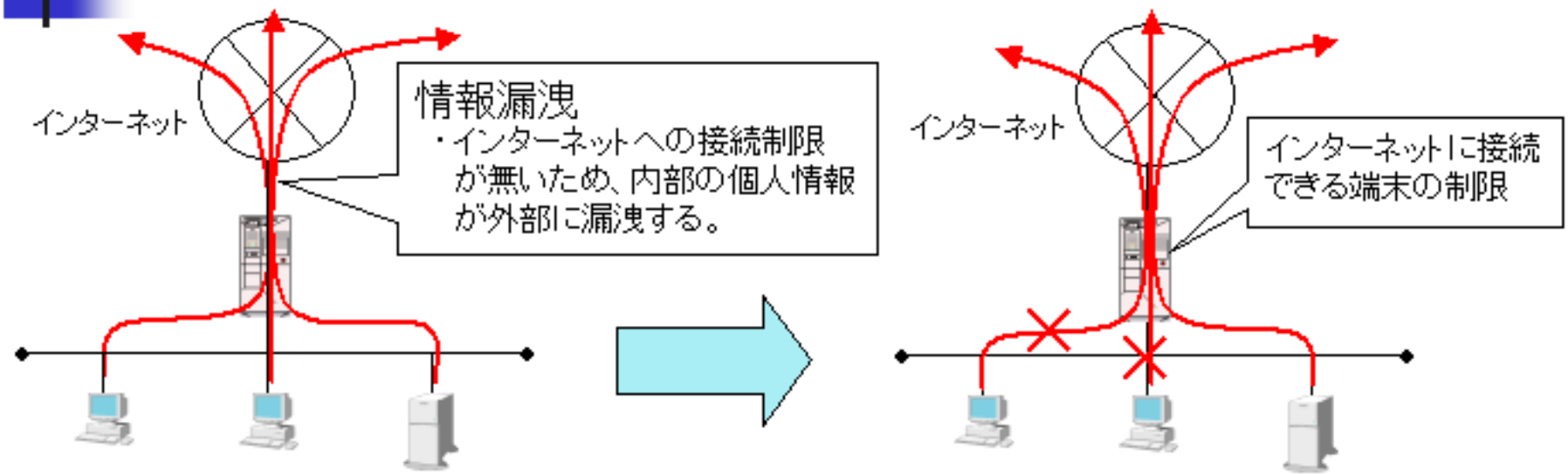
A) ルータ、ファイアウォールの設定が不適切



◆導入時の対策

- 通過するデータの経路を適切に設定する。
- パケットフィルタリングの設定を行い、通過するデータを制限する

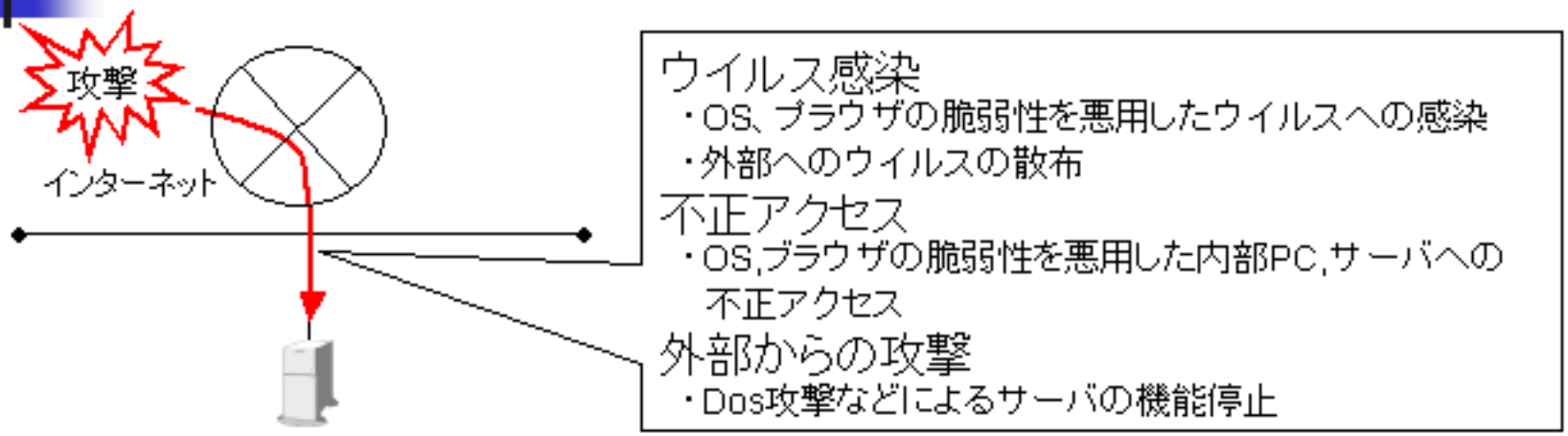
B) インターネットへの接続が未制限



◆導入時の対策

- インターネットに接続できる端末を制限する。
- 送信されるデータの接続先を制限する。
- 使用できる機能を制限する。(端末:セキュリティ設定、サーバ:フィルタリングツール)

C) OS、ブラウザのパッチが古い



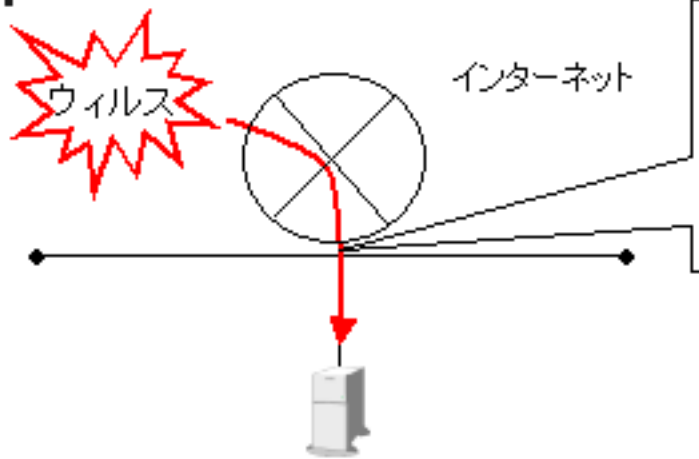
◆導入時の対策

- 端末:最新のセキュリティパッチを適用する。自動更新機能を有効にする。
- サーバ:コールドスタンバイ機能を備えておき、予備のサーバにパッチを適用して問題が無いことを確認した後に本番サーバにパッチを適用する。

◆運用時の対策

- 定期的に最新のセキュリティパッチが適用されているか確認する。
- 緊急のパッチが提供された場合、速やかに適用する。

D) ウイルス対策ソフトが未導入、未更新



ウイルス感染
・インターネット経由でのメール、ファイルダウンロードによるウィルス感染
・外部へのウイルスの散布
・バックドア設置による内部のPC,サーバへの不正アクセス

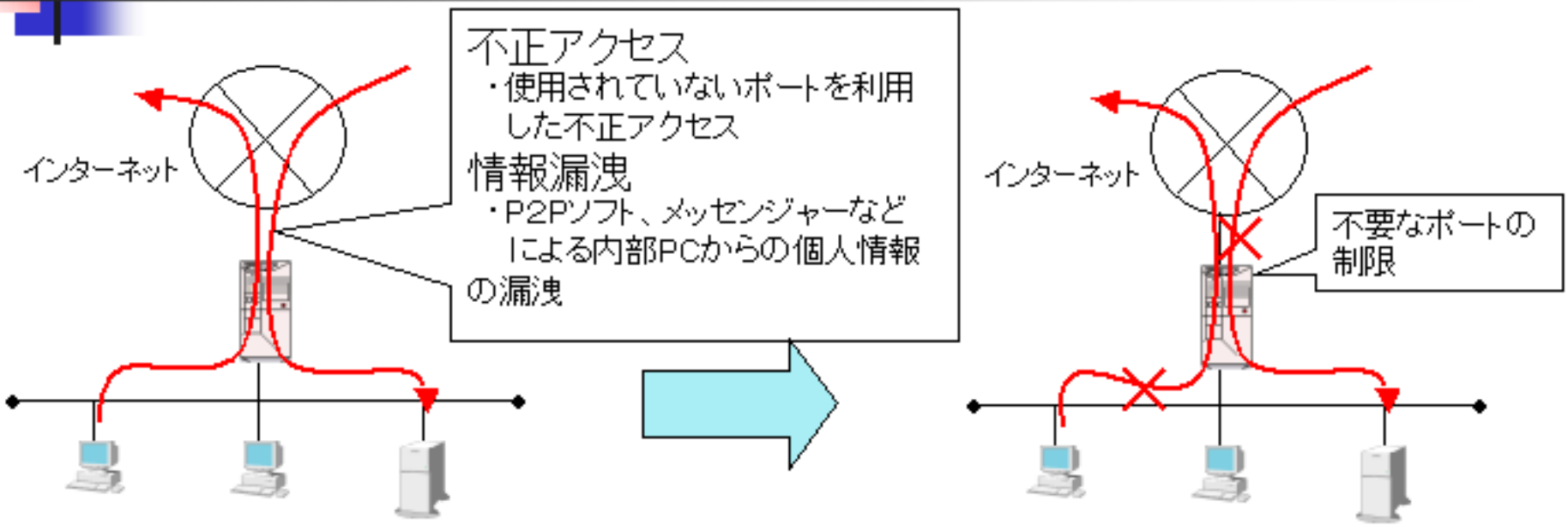
◆導入時の対策

- ウイルス対策ソフトを導入する。
- ウイルス定義ファイルの自動更新機能を有効にする。

◆運用時の対策

- 定期的にファイルのウイルスチェックを行うようにする。

E) 不必要な通信が許可されている



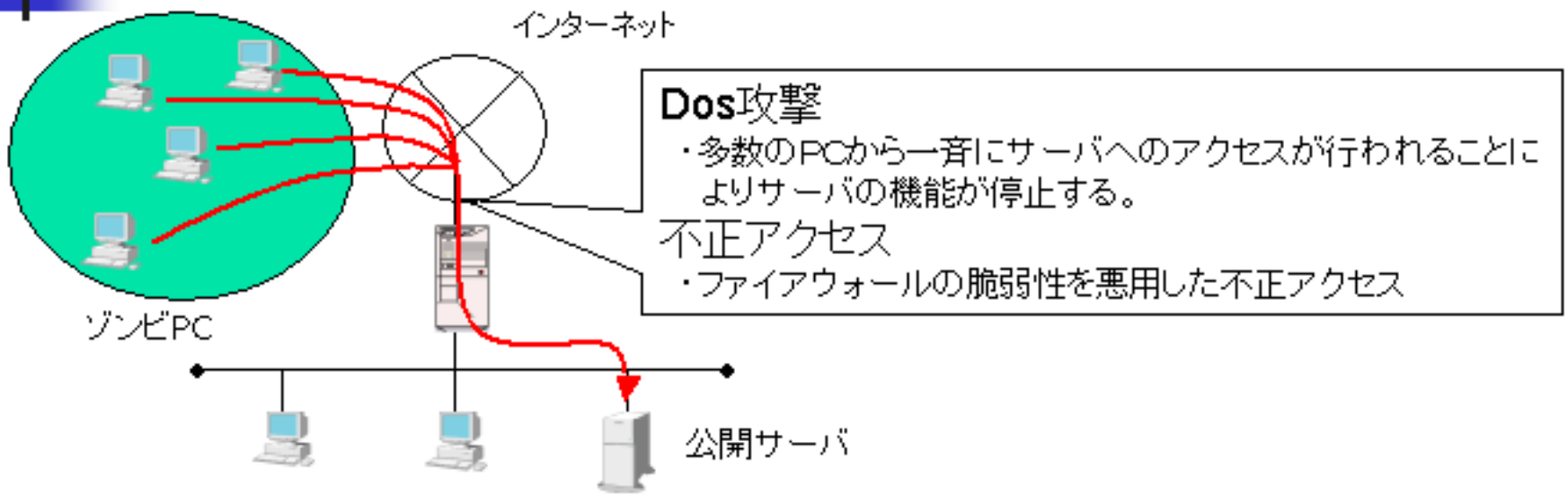
◆導入時の対策

- 不要なポートを塞ぐ。

◆運用時の対策

- 定期的に開いているポートの確認を行う。

F) 外部からの不正アクセスの対策が不十分



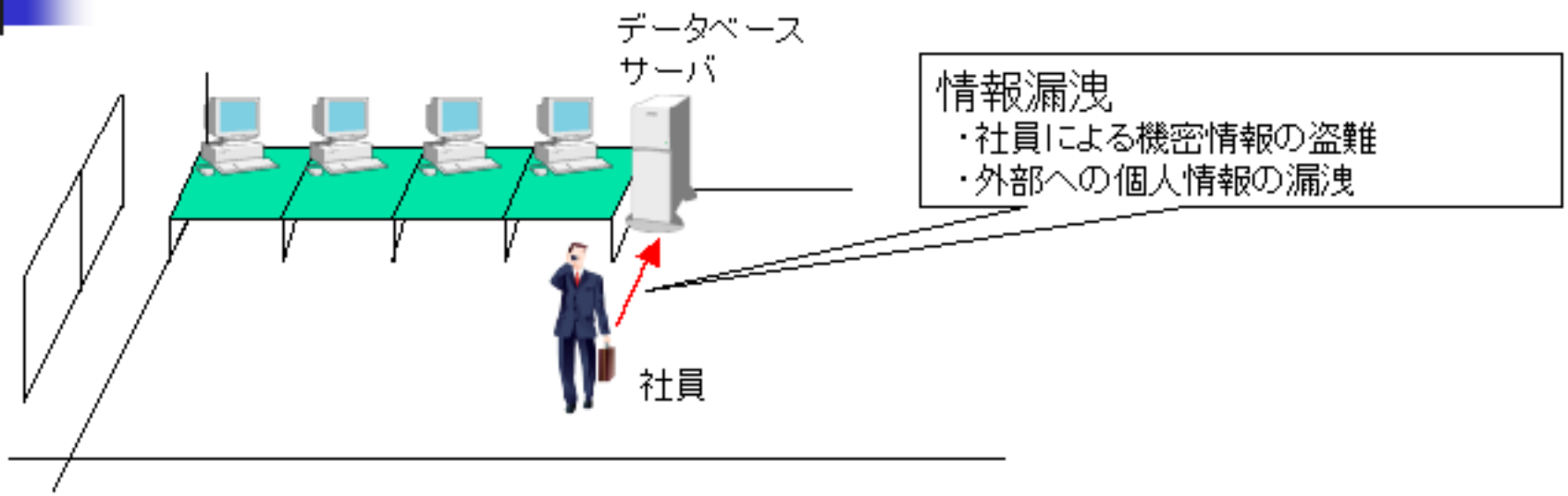
◆導入時の対策

- 不正侵入検知システム(IDS)を導入する。
- 負荷分散装置を導入する。
- ファイアウォールの脆弱性の対策を行う。

◆運用時の対策

- 定期的にログの監視を行う。

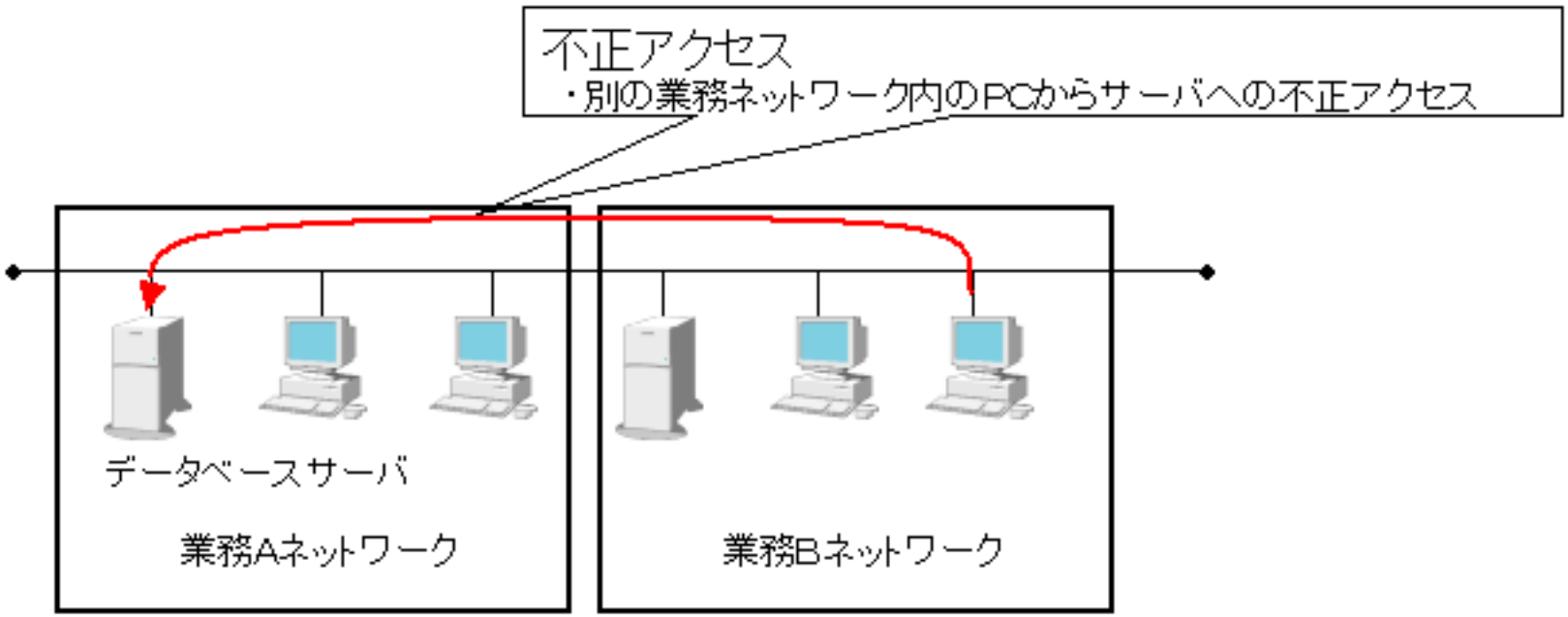
G) ユーザのセキュリティ知識の不足



◆運用時の対策

- 社員へのセキュリティ教育を定期的に行う。

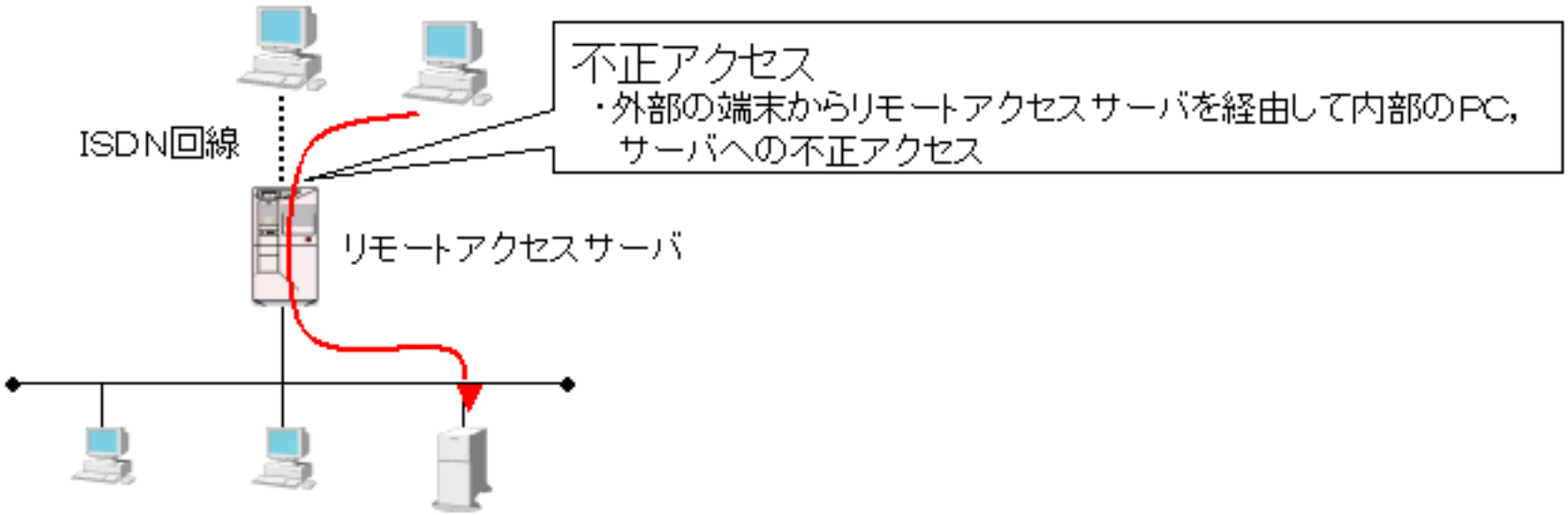
H) ネットワークが分断されていない



◆導入時の対策

- 業務毎にLANを構築して物理的にLANを分割する。
- サブネットマスクを設定して論理的にネットワークを分割する。

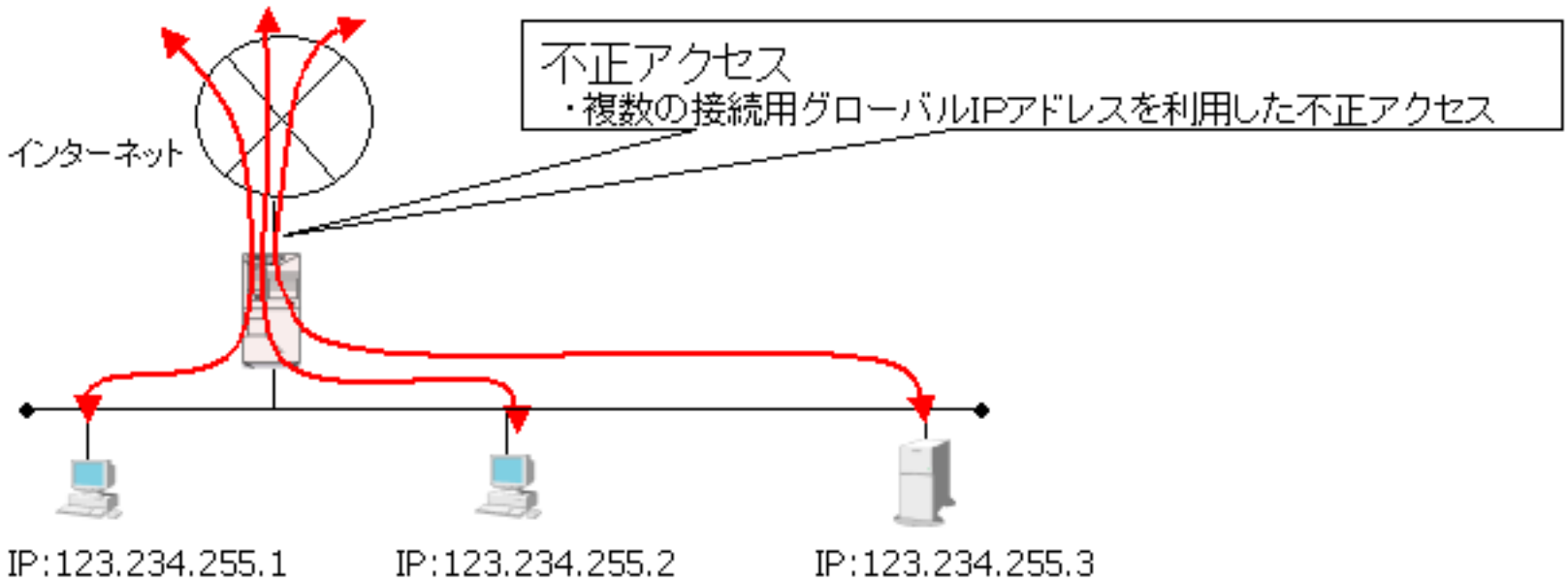
I) 発信、着信制御を行っていない



◆導入時の対策

- 接続する電話番号を登録して発信、着信制限を行う。
- コールバックの設定を行う。

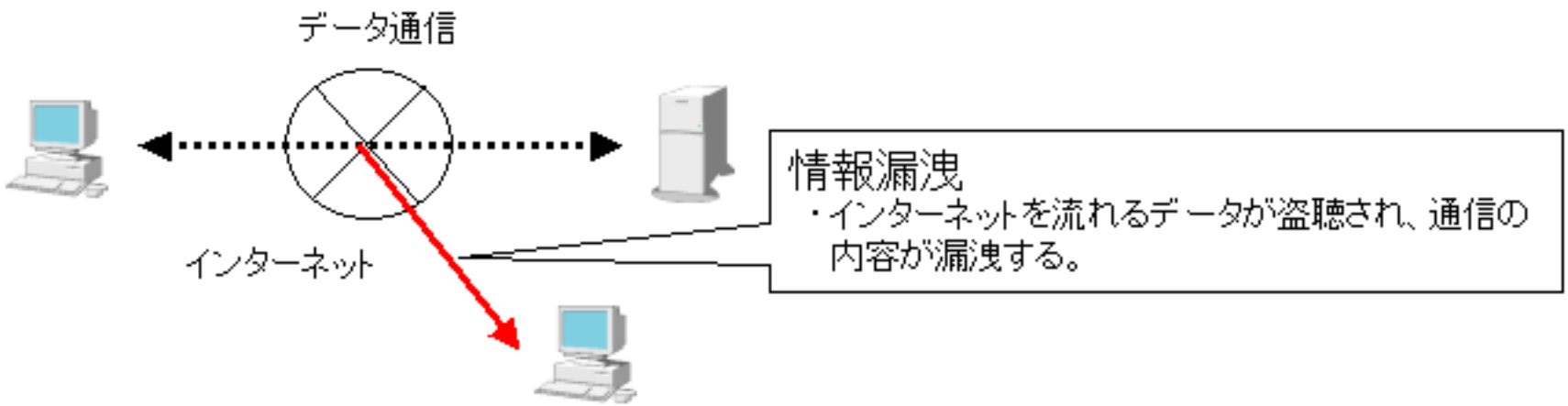
J) 接続用グローバルIPアドレスを固定していない



◆導入時の対策

- 接続用グローバルIPアドレスは必要最小限にする。

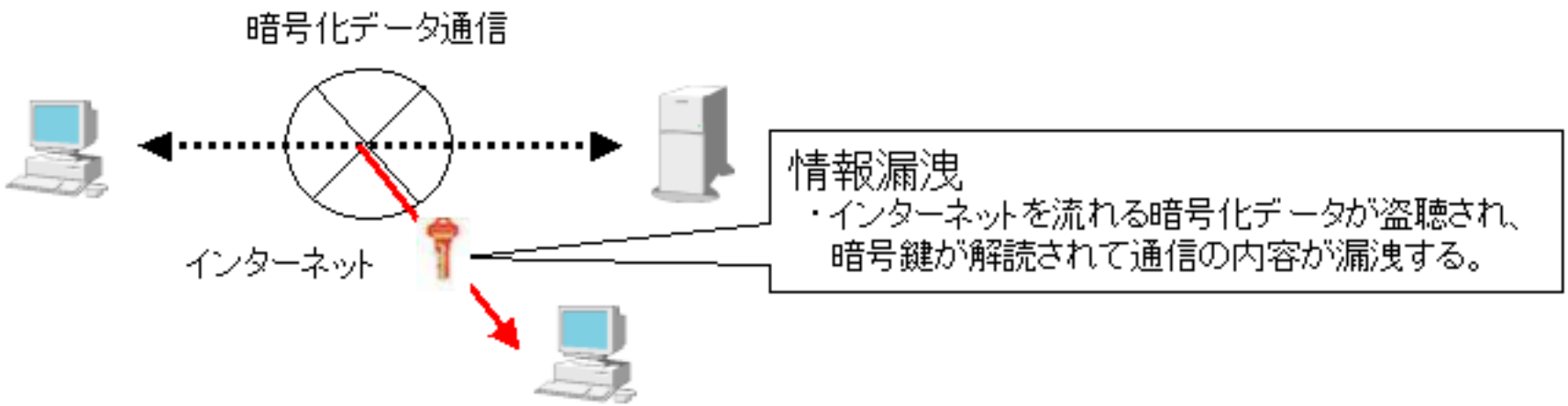
K) データ通信が暗号化されていない



◆運用時の対策

- IPSec,SSL等を利用して通信の暗号化設定を行う。

L）データ通信の暗号強度の不足

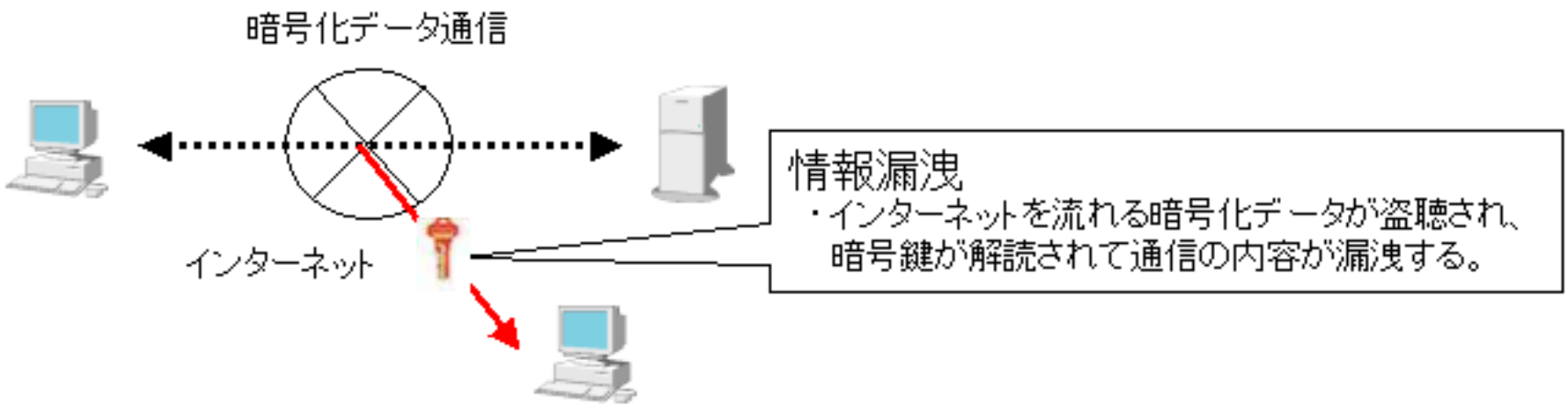


◆運用時の対策

- 適切な暗号強度を選択する。

  （外国との通信の場合、相手国の暗号強度にあわせる）

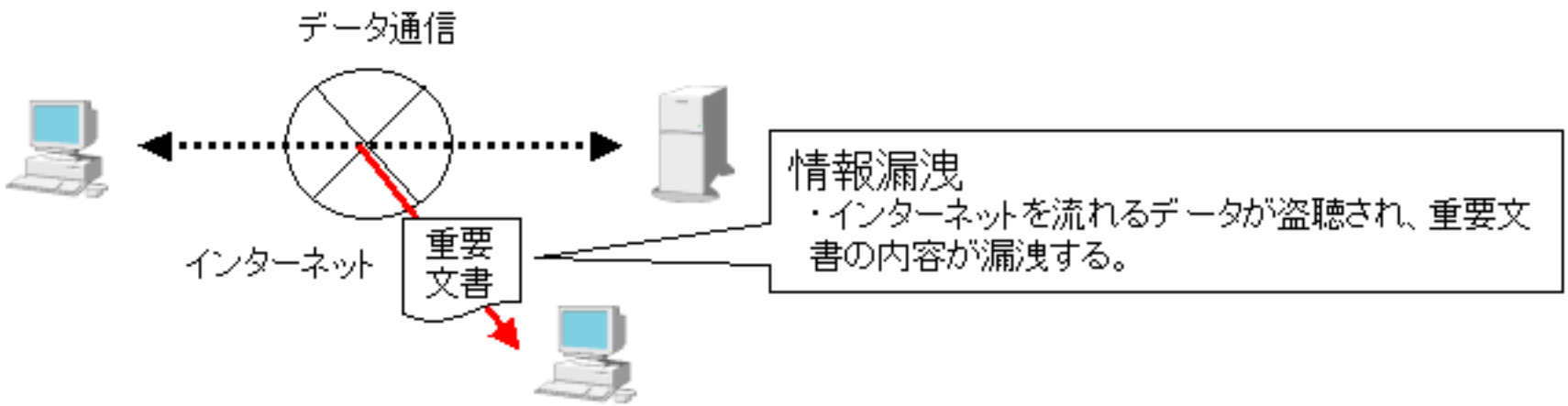
M) 同一暗号鍵を長期間利用している



◆運用時の対策

- 定期的に暗号化鍵を変更する。
- USBキー等を利用した認証方法を用いる。

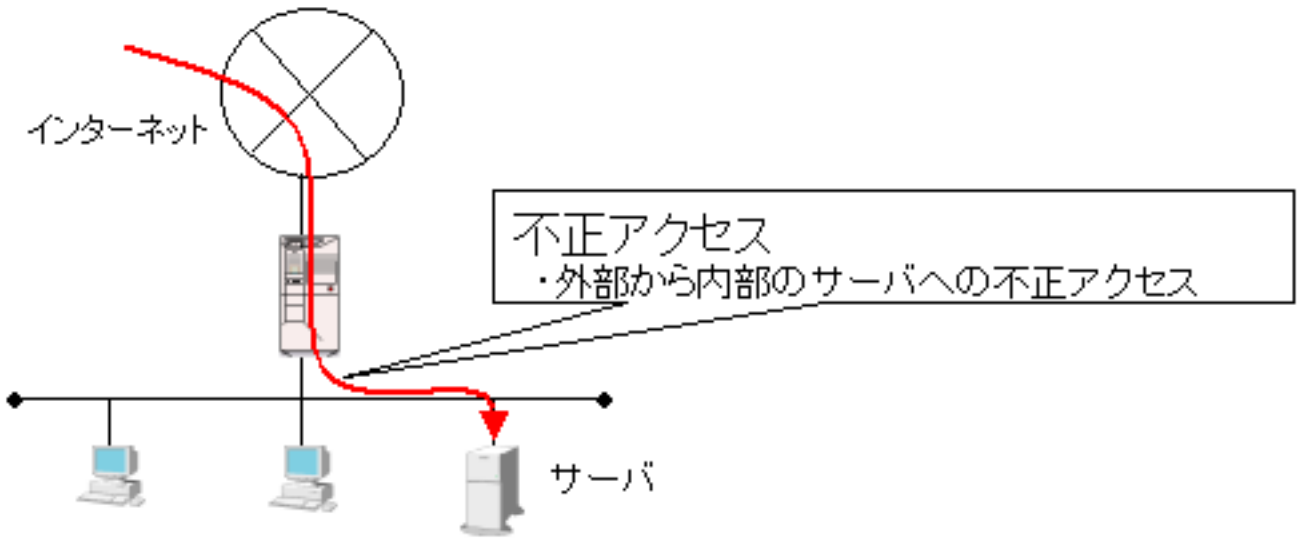
N) 重要文章を暗号化せずに送信している



◆運用時の対策

- 重要文書データを暗号化する。
- IPSec,SSL等を利用して通信の暗号化設定を行う。

0）サーバへのアクセスが制限されていない



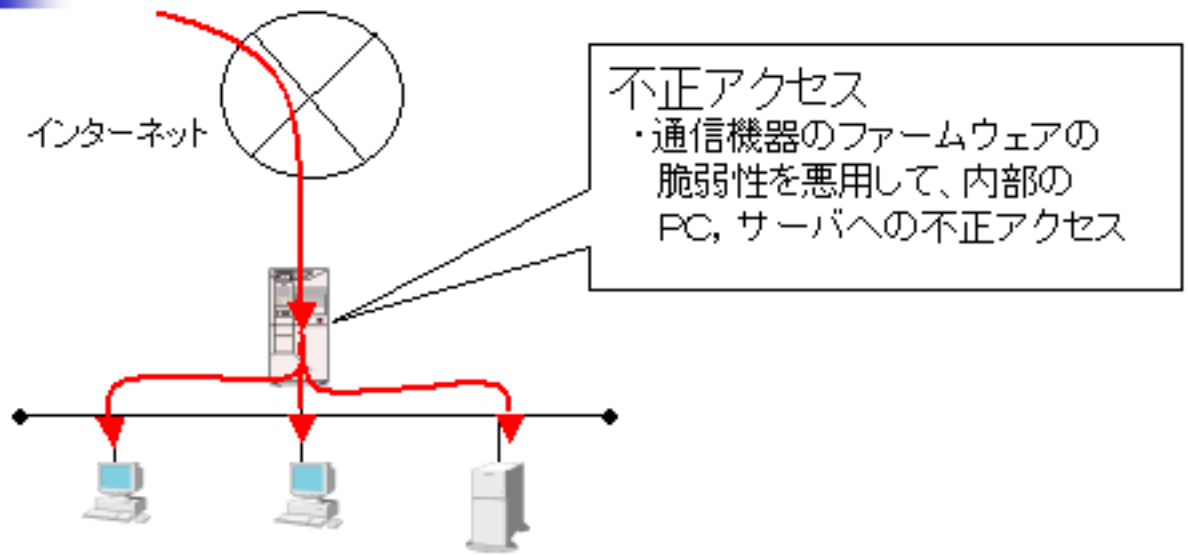
◆導入時の対策

- 外部からのサーバへの接続を遮断する。

◆運用時の対策

- メンテナンス等で外部からサーバに接続する必要がある場合、サーバとの通信を暗号化する。

P) 通信機器のファームウェアが古い



◆導入時の対策

- 通信機器のファームウェアを最新版にアップデートする。

◆運用時の対策

- 通信機器のファームウェアのアップデートを定期的に行う。

3. サーバ公開におけるリスク・原因・対策

3－1. サーバ公開におけるリスク

◆ リスク一覧

A） 公開サーバを踏み台にされる。

B） 提供するサービスが利用不能にされる。

C） 社内ネットワーク内部へ侵入される。

D） リソースを不正利用される。

E） サービスを不正利用される。

F） 顧客情報の漏洩。

G） 権限の無い者がサーバへ直接アクセス。

A） 公開サーバを踏み台にされる

◆ 想定される被害

1. 公開サーバ経由での不正アクセス。
2. 公開サーバ経由でのSPAM送信。
3. 公開サーバ経由でのウィルス被害。
4. 信頼の喪失。

◆ 原因

1. 不必要なサービスが起動している。
2. 不必要なポートが開いている。
3. セキュリティホールの対策が行われていない。
4. ユーザ管理が不適切である。
5. フォルダ等へのアクセス権設定が不適切。

B） 提供するサービスが利用不能にされる

◆ 想定される被害

1. WEBの改ざん。
2. ビジネスチャンスの喪失。
3. 信頼の喪失。

◆ 原因

1. 不必要なサービスが起動している。
2. 不必要なポートが開いている。
3. セキュリティホールの対策が行われていない。

C） 社内ネットワーク内部へ侵入される

◆ 想定される被害

1. 社内機密情報の漏洩。

◆ 原因

1. 不必要なサービスが起動している。
2. 不必要なポートが開いている。
3. セキュリティホールの対策が行われていない。
4. ユーザ管理が不適切である。
5. 公開サーバを不適切なネットワーク上に設置している。

D） リソースを不正利用される

◆ 想定される被害

1. 公開サーバへの過負荷。
2. 公開サーバが提供するサービスの不良。

◆ 原因

1. 不必要なサービスが起動している。
2. 不必要なポートが開いている。
3. セキュリティホールの対策が行われていない。
4. ユーザ管理が不適切である。
5. フォルダ等へのアクセス権設定が不適切。
6. 外部からアクセスする際に共通のユーザで行っている。

E） サービスを不正利用される

◆ 想定される被害

1. 正規ユーザのアカウントが不正に利用される。
2. 不正なアカウントが作成される。

◆ 原因

1. ユーザ管理が不適切である。
2. 認証に暗号化通信を利用していない。

F） 顧客情報の漏洩

◆ 想定される被害

1. 信頼の喪失。
2. ビジネスチャンスの喪失。

◆ 原因

1. Webアプリケーションの虚弱性。
2. フォルダ等へのアクセス権設定が不適切。
3. Webサーバ上に機密情報を置いている。
4. ユーザ管理が不適切である。

G） 権限の無い者が公開サーバへ直接アクセス

◆ 想定される被害

1. 情報の漏洩。
2. 公開サーバ内のユーザ設定を変更される。
3. セキュリティ設定を変更される。

◆ 原因

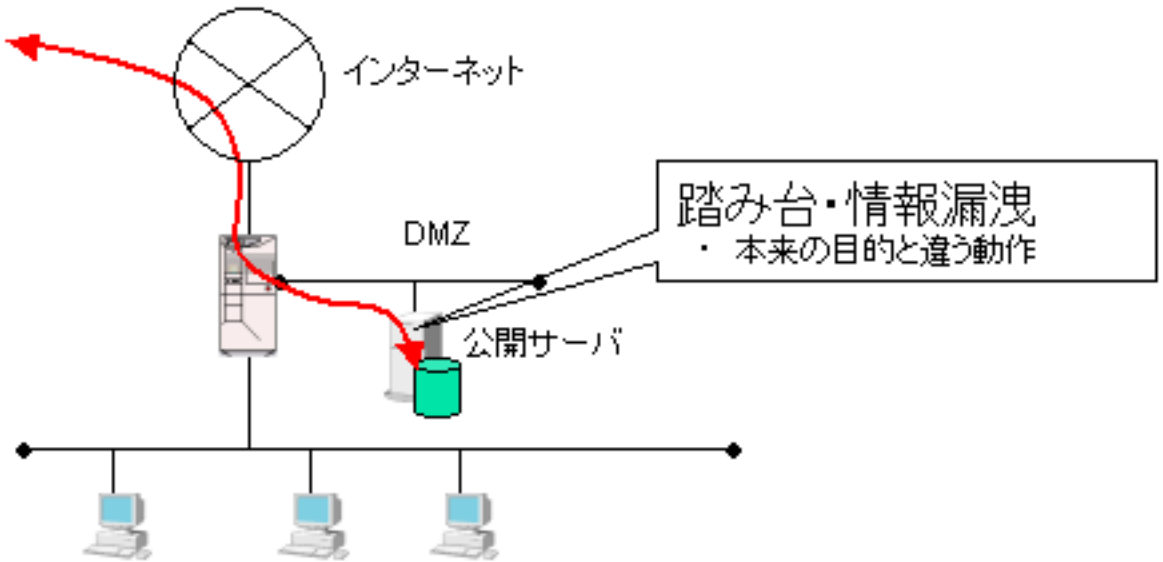
1. 外部の人間が直接アクセスできる所に設置されている。
2. 外部からのアクセスに共通のユーザで行っている。

3－2. サーバ公開におけるリスクの原因と対策

◆ 原因一覧

A) 不必要なサービスが起動している。
B) 不必要なポートが開いている。
C) ユーザの管理が不適切である。
D) ネットワーク上の設置場所が不適切である。
E) 外部の人間が直接アクセスできる所に設置されている。
F) 外部からのアクセスに共通のユーザで行っている。
G) Webサーバ上に機密情報を置いている。
H) 認証に暗号化通信を利用していない。
I) セキュリティホールへの対策が行われていない。
J) フォルダ等へのアクセス権設定が不適切。
K) Webアプリケーションの虚弱性。

A) 不必要なサービスが起動している



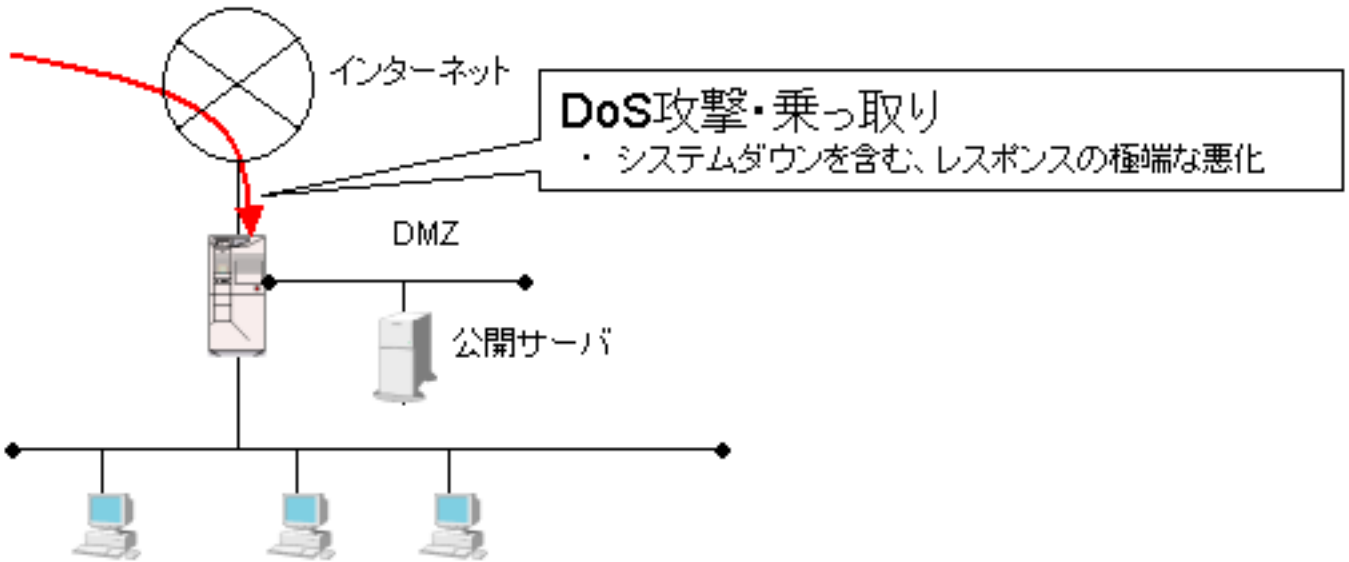
◆導入時の対策

- 不要なサービスを停止する。

◆運用時の対策

- 不要なサービスが起動していないか定期的に確認する。

B) 不必要なポートが開いている



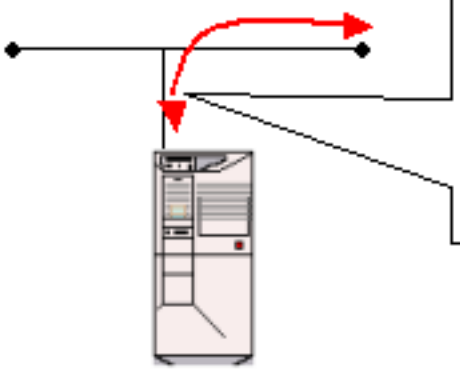
◆導入時の対策

- 不要なポートを塞ぐ。

◆運用時の対策

- 不要なポートが開いていないか定期的に確認する。

C) ユーザの管理が不適切である



不正アクセス
- デフォルトID(特にパスワードが設定されていないものや、初期のパスワードのままのもの)を使用したアクセス
- ウィルス/ワーム等で作成されたバックドアを使用してのアクセス
- 内部関係者により悪意を持って作成されたIDを使用してのアクセス
- 退職者により、退職前に使用していたIDを使用してのアクセス
- 部署変更後、アクセスする必要が無くなった情報へのアクセス
- アクセス制限の登録/削除/変更ミスにより、アクセスする必要が無い情報へのアクセス

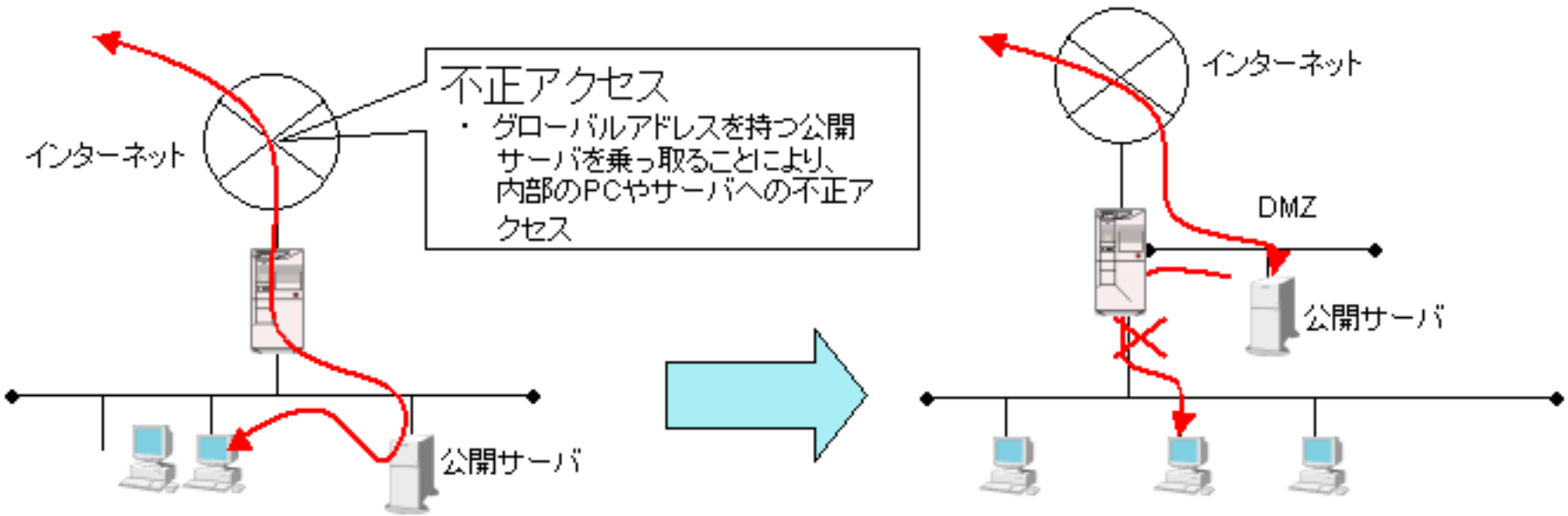
◆導入時の対策

- デフォルトで設定されているユーザを削除する。なお、デフォルトのID内で、削除できないIDの場合は、十分な強度を持つパスワードを設定する。

◆運用時の対策

- 退職等で不要となったユーザIDは速やかに削除する。
- 配置変更等が発生した場合、ユーザIDのアクセス権限の見直しを速やかに行う。
- 定期的に作業記録(システムログ等)を確認し、不正なユーザの追加・変更・削除が行われていないか監視する。
- 定期的に登録ユーザを確認し、不要なユーザIDが存在しないか確認する。

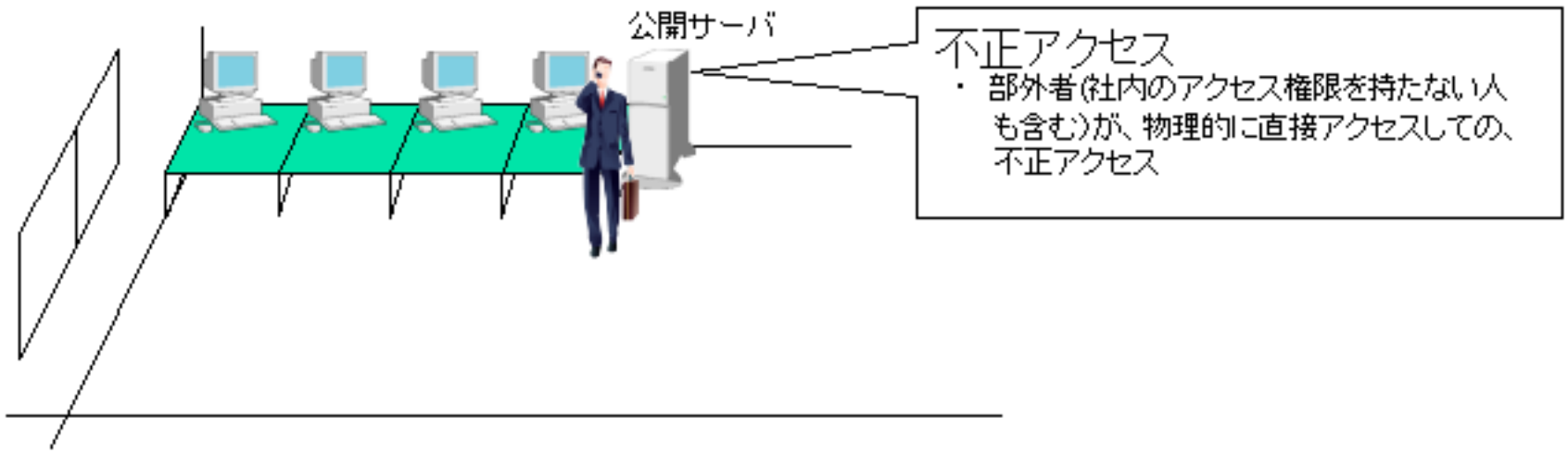
D) ネットワーク上の設置場所が不適切である



◆導入時の対策

- ファイアウォールを導入し、DMZに外部公開サーバを設置する。
- ファイアウォールで、外部からのアクセスは、DMZ上のみにアクセスを許可する。
- ファイアウォールで、公開サーバから内部セグメントへのアクセスは禁止する。
- アクセスの負荷と費用が許せば、DMZ上にリバースプロキシサーバを設置し、公開サーバも内部ネットワークに設置する。

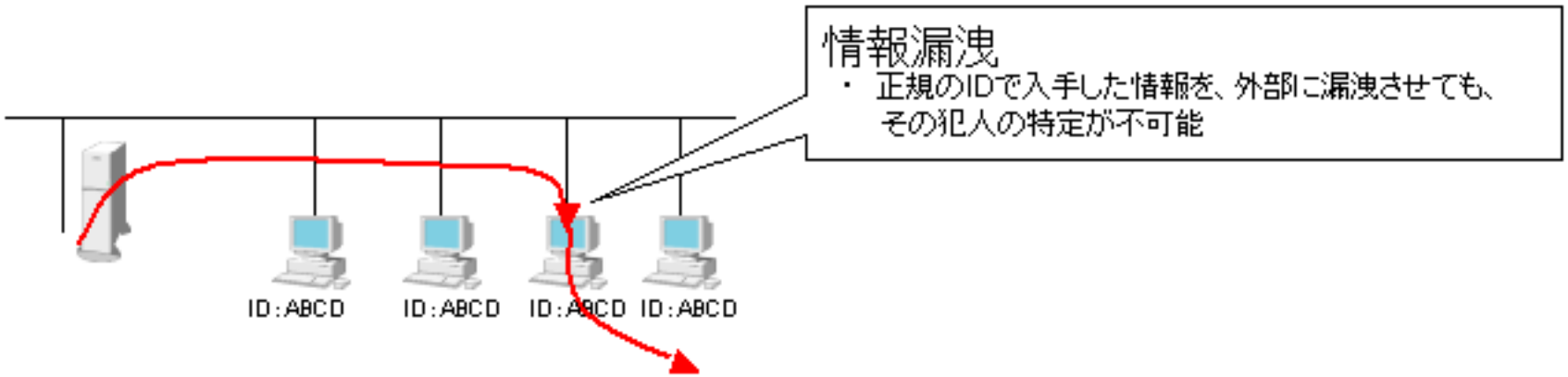
E) 外部の人間が直接アクセスできるところに設置されている



◆導入時の対策

- マシン室など、施錠でき、必要最低限の人のみが出入りできる場所に設置する。
- 電源や地震・回線などによる不足の事態の回避が自前では難しく、考慮する必要がある場合、外部のiDCにサーバを設置する。

F) 外部からのアクセスに共通のユーザで行っている



◆導入時の対策

- 個人毎に別々のユーザIDを割り当て、アクセスした個人を特定できるようにする。
- 個々に割り当てたIDの二重ログオンを禁止する。
- サーバで、何時・どのIDから・どの様なアクセスがあったか、アクセスログを採取する。

◆運用時の対策

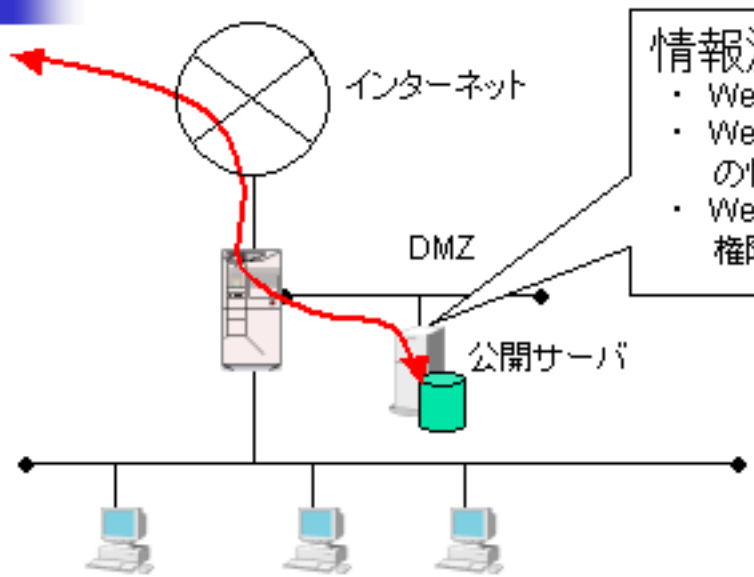
- 相当な期間、アクセスログを保存する。
- 定期的にアクセスログを監査する。

  ・勤務時間外(夜間・休日等)のアクセスがないか。

  ・アクセス失敗を繰り返しているIDはないか。

  ・不当に長い時間または、多くの回数ログインしたIDはないか。

G) Webサーバ上に機密情報を置いている



情報漏洩
- Webアプリケーションのバグによる予想外の情報表示
- Webアプリケーションの脆弱性突いた攻撃により、カレントのドライブ内の情報の表示
- Webサーバの脆弱性を突いた攻撃により、サーバへの不当なアクセス権限の取得

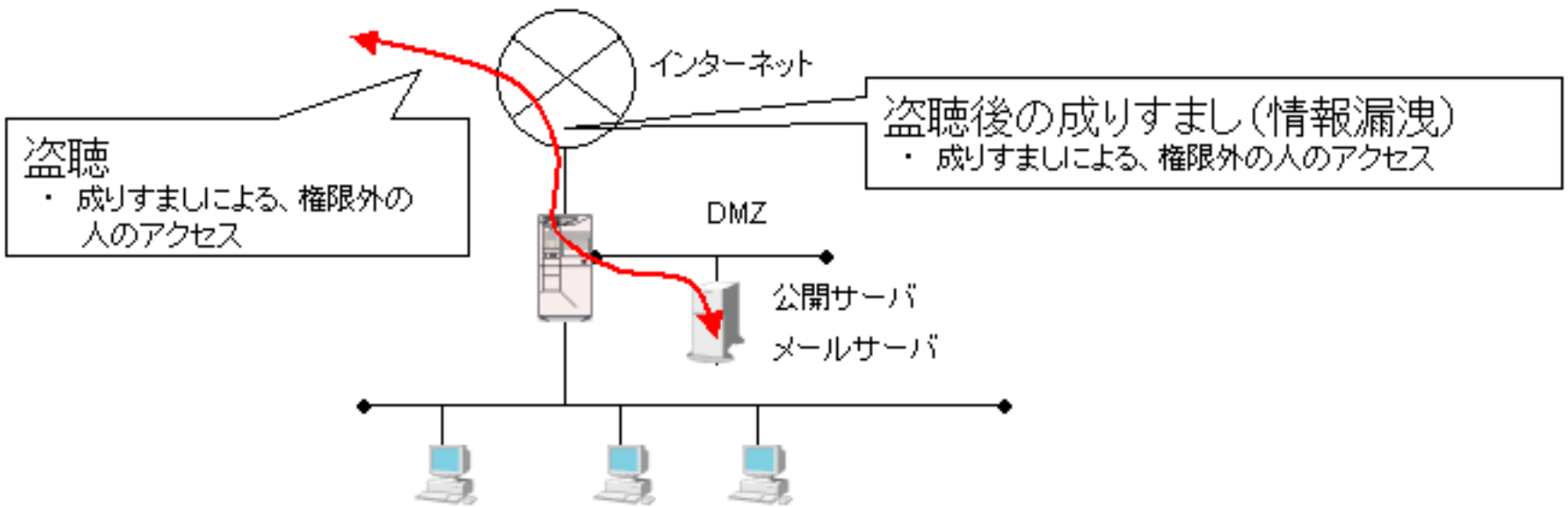
◆導入時の対策

- Webアプリケーション作成に際し、情報は、Webサーバ内に置かなくて済むように設計する。
- Webアプリケーション作成に際し、脆弱性を排除するためのコーディング規約を儲け、遵守させる。

◆運用時の対策

- Webサーバ上に機密情報およびアプリケーションのソースを置かないように管理ルールを作成して徹底させる。
- 特別な事情により、機密情報を置かざるを得ない場合は、パーミッションを設定して外部から閲覧できないようにする。

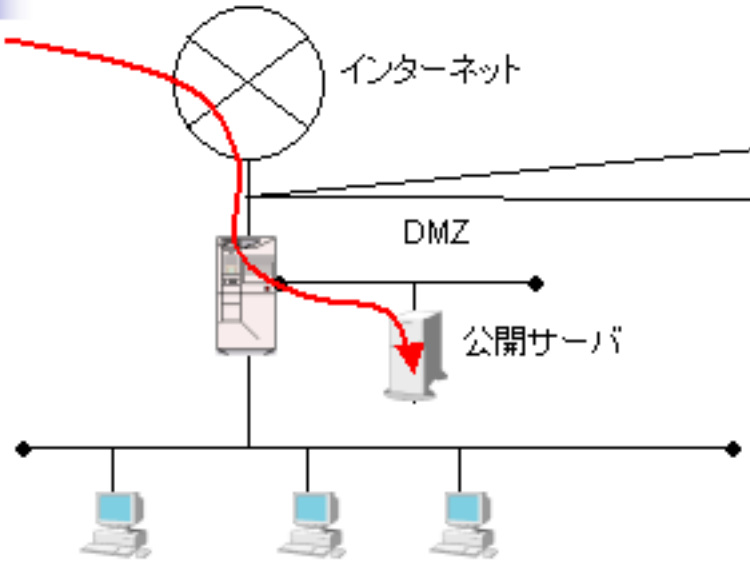
H) 認証に暗号化通信を利用していない



◆導入時の対策

- SSL等を利用してサーバの個人認証時にデータを暗号化する。
- APOP等を利用してメールサーバの認証時にデータを暗号化する。

I) セキュリティホールへの対策が行われていない



サーバの脆弱性を突いた攻撃
- 業務停止
- システム改竄
- 不正アクセスによる情報漏洩

(注)対策を行うに当たり、パッチ適用のために
業務が停止するという新たなリスクが発生する。

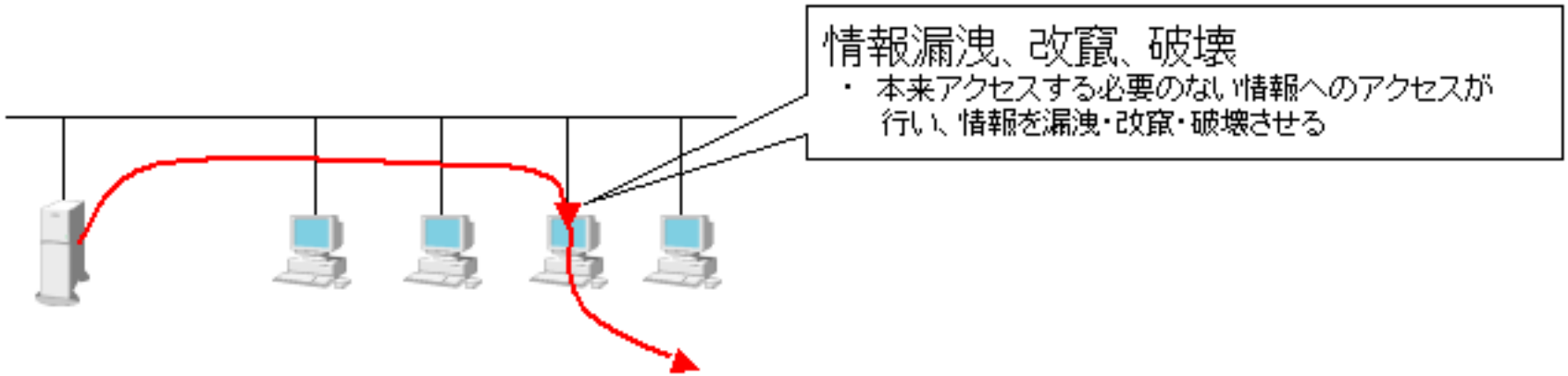
◆導入時の対策

- 定期的にセキュリティパッチの適用日を決めておく。
- コールドスタンバイ機能に備えておき、予備のサーバにパッチを適用して問題が無いことを確認した後に本番サーバにパッチを適用する。

◆運用時の対策

- 定期的にパッチを適用する。
- 緊急のパッチが適用された場合、すぐに適用する。

J) フォルダ等へのアクセス権設定が不適切



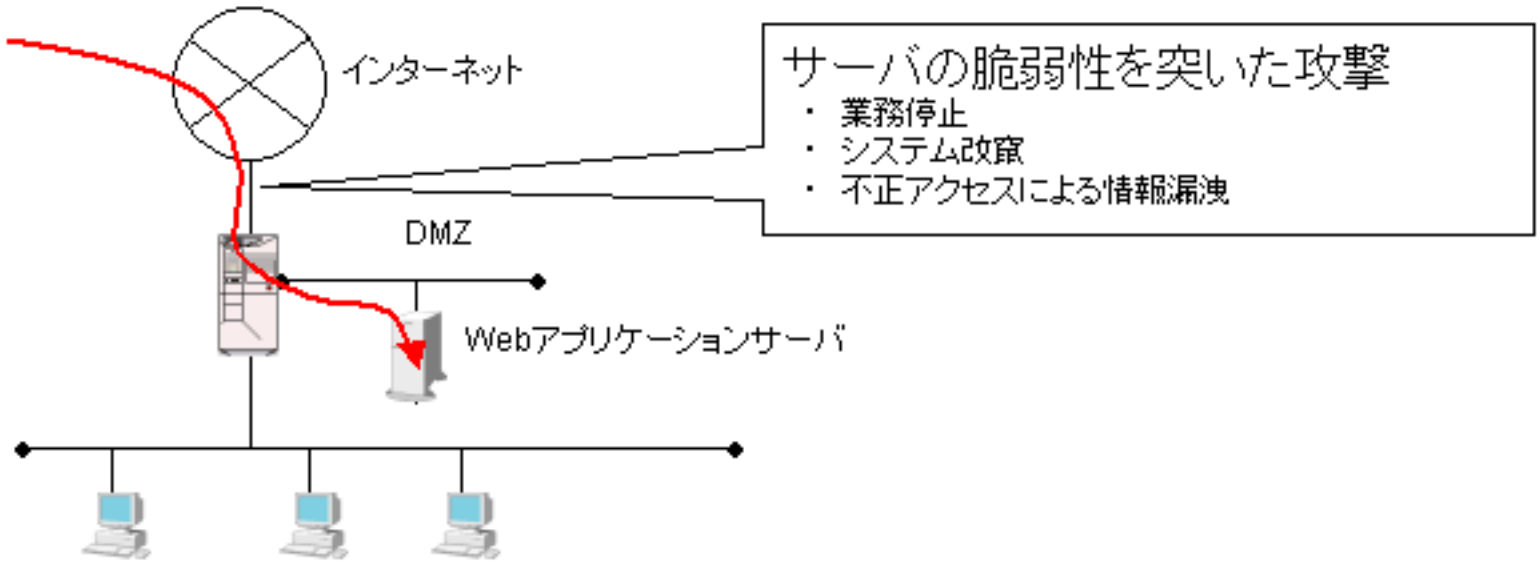
◆導入時の対策

- アクセス権の設定はすべて拒否にしておいて、最低限必要なものだけを許可する。

◆運用時の対策

- 定期的にアクセス権限設定内容の見直しを行う。

K) Webアプリケーションの虚弱性



◆導入時の対策

- クロスサイトスクリプティング、バッファオーバーフローなどの脆弱性を補うためのコーディング規約を作成する
- コーディング規約に沿った作成を行う。

◆運用時の対策

- 新たな脆弱性が発見された場合、コーディング規約の見直しを行う。
- コーディング規約の見直しを行った際、現システムへの影響を検査し、修正する。

最後に

完全なセキュリティを確保する事は不可能である。

保有するリスクを知り、

対策が必要かどうかを判断し、

必要な対策を選択する。

ネットワークを構築するにあたり、必要な対策を取るための参考としていただければ幸いです。

＜参考＞　セキュリティ対策ツール

参考

◆ 情報漏洩対策の各種ツールのご照会

情報漏洩を防止するためのツールを、6つのカテゴリに分けて
ご照会いたします。

(注)本資料で掲載した製品は、Webサイトで掲示されている情報より 一部を抜粋して掲載させていただきました。
また、そのカテゴリの区分に関しても著者の独自の判断の基づいています。
なお、掲載しているURLに関して、特にリンクの許可を受けていないため、ハイパーリンクでの掲載とはしておりません。

1） 情報漏洩防止のための統合ツール

抑止(ログの取得等)や防止(コピー禁止等)を統合的に管理するツールです

2） Webコンテンツ漏洩防止ツール

Web上コンテンツからの情報漏洩(不正な印刷等)を防ぎます

3） メールフィルタリングツール

スパムメールやウィルス感染メールの受信、添付メールの送信を制御します

4） Webフィルタリングツール

私的なWebアクセス(私的サイト閲覧・掲示板・Webメール)等を制御するツールです

5） 個人認証ツール

USBキーやICカード等で個人認証を行います

6） 暗号化ツール

機器の盗難や置忘れ等での情報漏洩を防ぎます

参考

- 情報漏洩防止のための統合ツール
  - A） セキュリティプラットフォーム
    http://www.canon-elec.co.jp/products/software/sep/
  - B） CWAT
    http://www.iwi.co.jp/japanese/cwat/
  - C） LanScope
    http://www.motex.co.jp/
  - D） 秘文
    http://www.hitachi-sk.co.jp/Products/Security/
  - E） Systemwalker
    http://systemwalker.fujitsu.com/jp/
  - F） Document Security
    http://www.alsi.co.jp/pro/DocumentSecurity/index.htm

など

参考

- Webコンテンツ漏洩防止ツール
  - A） Webコンテンツプロテクター
    http://www.ntt-me.co.jp/probix/
  - B） デジカプセル
    http://www.mitsubishielectric.co.jp/digicpsl/web/index_b.html

など

参考

◆ メールフィルタリングツール

E） InterScan

http://www.trendmicro.com/jp/products/smb/isvw-smb/evaluate/overview.htm

A） GUARDIAN WALL

http://www.necsoft.com/soft/guardian/wall/index.html

B） Eメールフィルター

http://www.filtering.jp/email/index.html

C） AntiLeak

http://www.ant.co.jp

D） マトリックス　スキャン

http://www.imatrix.co.jp/

F） WISE　Audit

http://www.air.co.jp/products/wise_audit/wa.html

など

参考

◆ Webフィルタリングツール

A） WEBSENSE

http://www.websense.co.jp/products/

B） InterSafe

http://www.alsi.co.jp/security/s_01_01.html

C） WEB GUARDIAN

http://www.canon-sol.co.jp/guardian/product/wg

D） SurfControl Web Filter

http://www.filtering.jp/scwf/index.html

E） i-フィルター

http://www.daj.co.jp/bs/b_ifbe/index.htm

F） NGSecureWeb

http://canon-sol.jp/product/ng/

など

参考

◆ 個人認証ツール

A） iKey

http://www.giken.co.jp/products/ikey/index.html

B） eToken

http://www.aladdin.co.jp/etoken/index.html

C） LOCK STAR

http://www.logicaltech.co.jp/index1.html

D） HOT TOPICS

http://www.secugen.co.jp/news/news_031113.html

F） SmartOn

http://www.tni.co.jp/solutions/security/smarton.html

E） マネージドPKI

http://www.verisign.co.jp/mpki/solution/smail/

など

参考

◆ 暗号化ツール

A） SafeBoot

http://www.macnica.net/cbi/

B） DataClasys

http://www.vertexlink.co.jp/dataclasys/

C） VoiceK

http://voicek.jp/

D） MyDearDrive

http://www.cpiinc.co.jp/

E） モバイル割符

http://www.hitachi.co.jp/media/New/cnews/month/2004/07/0714.html

など