


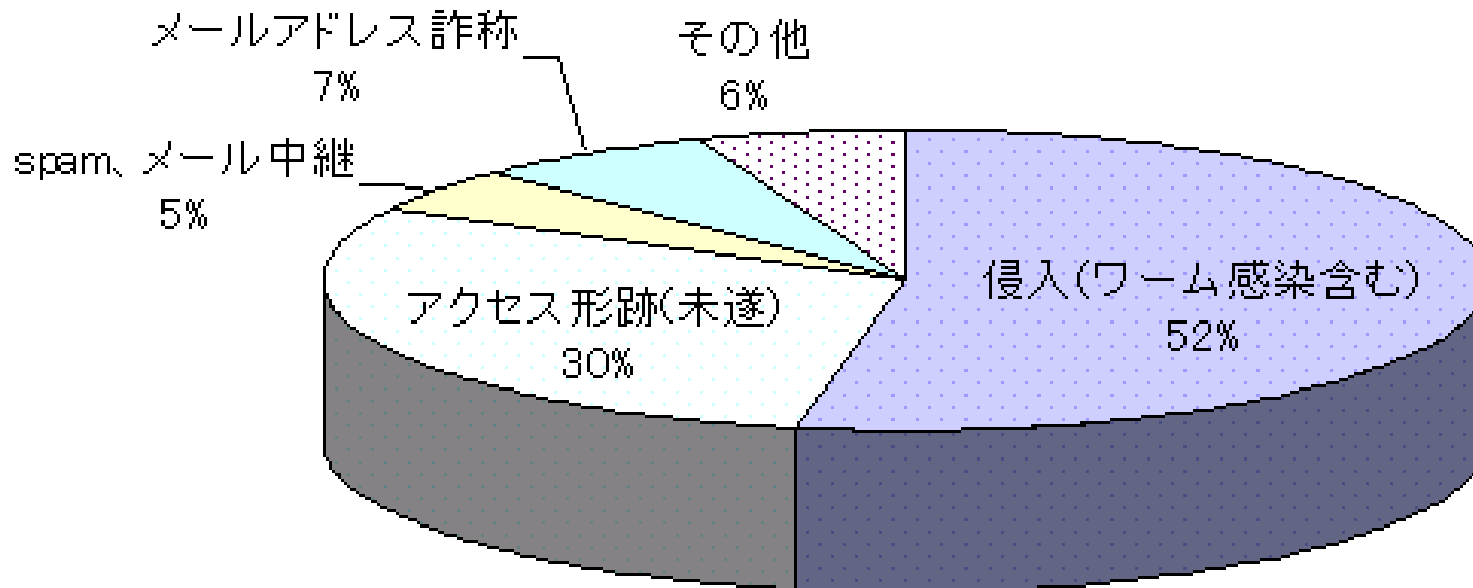
エンドユーザのパソコンにおける 不正アクセスの傾向と対策



情報処理振興事業協会 セキュリティセンター

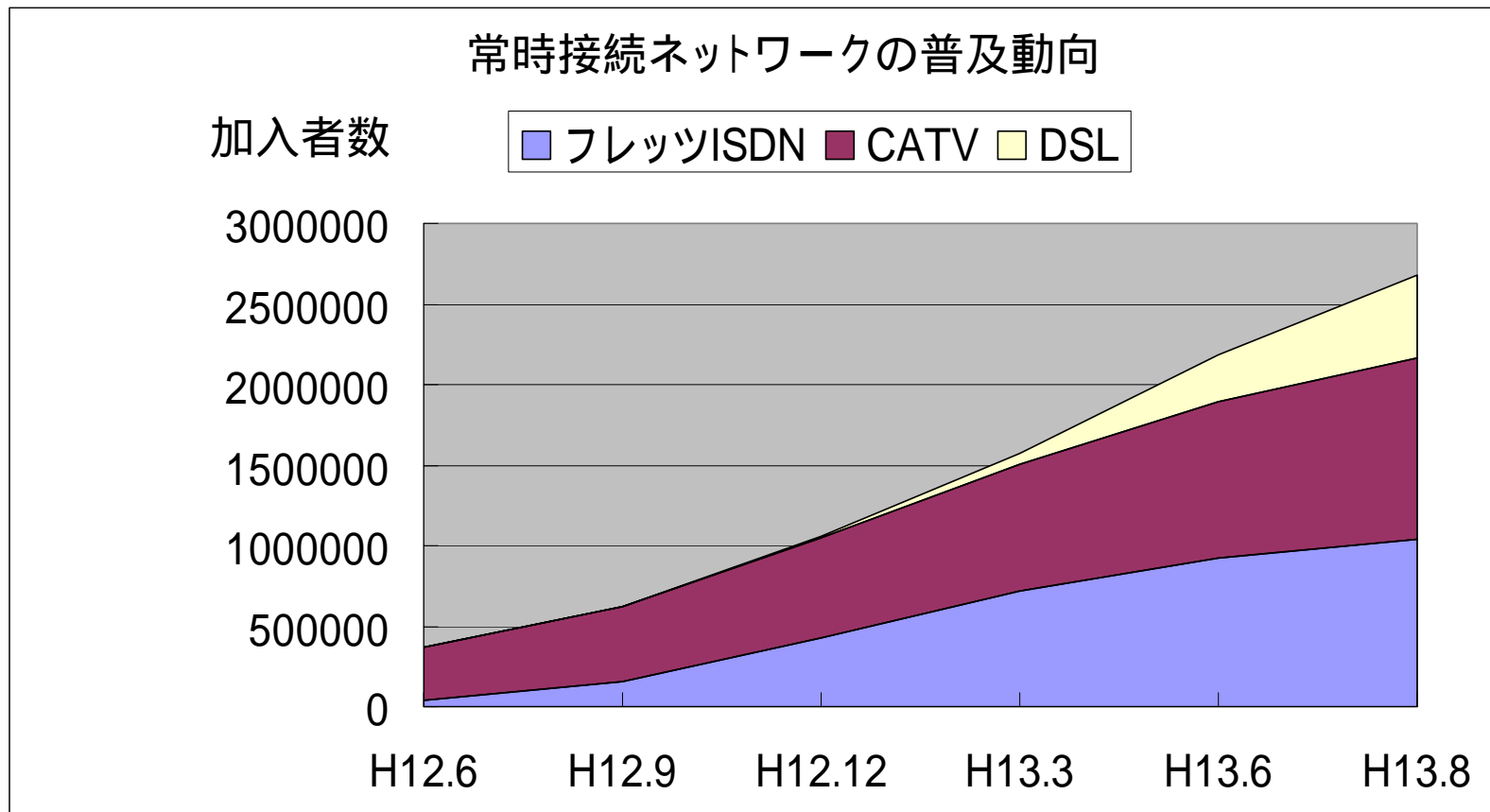
- 不正アクセスの傾向
 - IPAへの不正アクセス届出分類
 - 不正アクセス届出・相談内容
 - 届出・相談事例
 - 不正アクセスの手段
- 不正アクセス対策
 - ブラウザ
 - メール
 - 常時接続
 - その他の一般的な対策

IPAへの不正アクセス届出分類



届出期間:2001年 1月 - 9月

常時接続ネットワークの普及動向



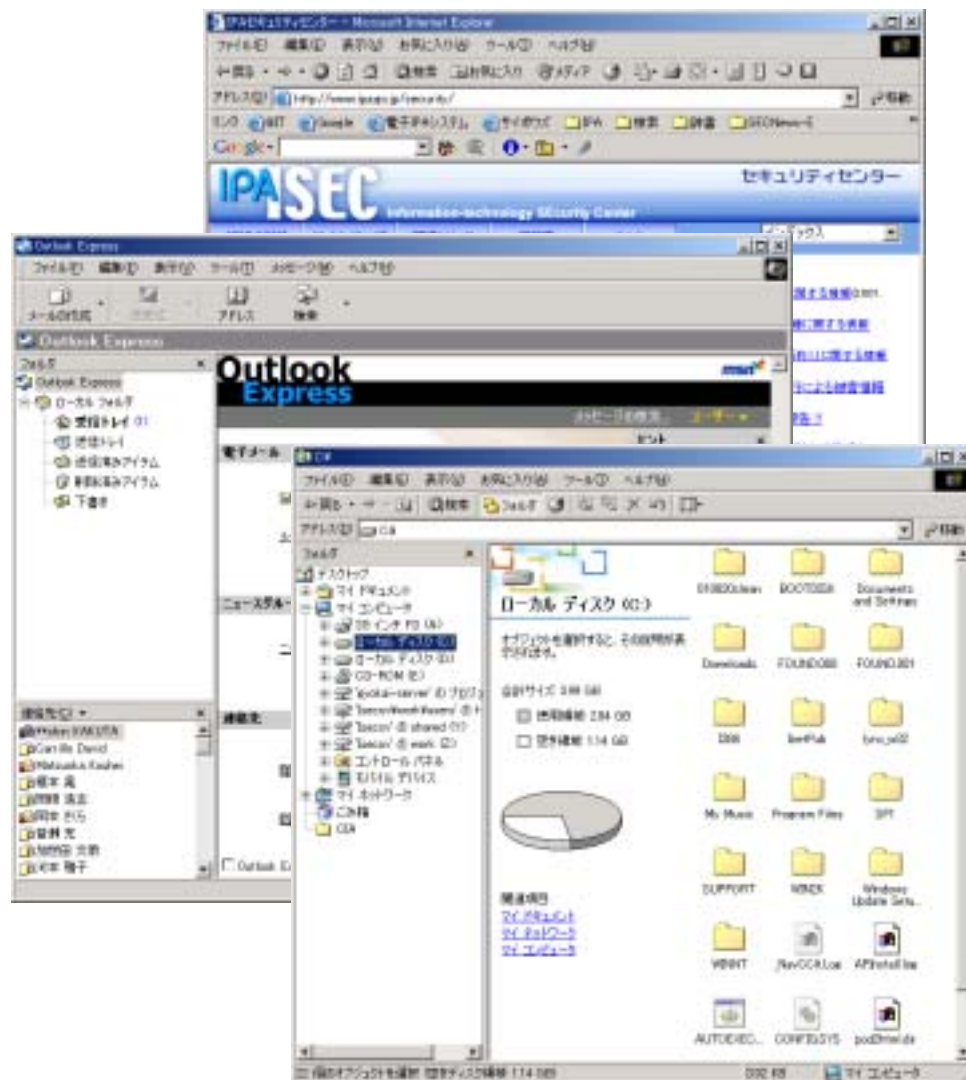
届出・相談内容のトップ4

- **ワームの感染や感染活動によるもの**
 - Nimda , CodeRed など
- **常時接続環境におけるポートスキャンやバックドアプログラム埋め込みのための攻撃**
 - BackOrifice , NetBus
- **ブラウザのセキュリティホールを利用した悪意のプログラム**
 - ダイヤルQ2、国際電話など
- **パスワードの盗用によるもの**
 - メール盗み見、プロバイダ使用料など

届出・相談事例(1) - ワーム

W32/Nimda

- ホームページやメール本文を見ただけで感染
- ネットワークを介してのファイル共有で感染
- 他のWebサーバーへの攻撃加担
- 感染ファイルをばら撒く



BackOrifice等

- メールの内容が第三者に読まれて(盗み見されて)いる
- 自分の日記の内容が掲示板に載っていた
- 自分のPCがリモートで操作されてしまう
- 夜中に勝手にPCの電源が立ち上がる



ダイヤルQ2等

- 利用した覚えの無いダイヤルQ2から情報料の請求が来た。
- かけたつもりが無い、多額の国際電話代金を電話会社から請求された。
- クレジット会社から海外のQ2相当サービス使用料請求が来た。



届出・相談事例(4) - なりすまし、 ソーシャルエンジニアリング

パスワードの盗用等

- プロバイダから接続していない期間の請求が来た。
- 退職した社員が旧ユーザIDを利用して、会社の重要書類を盗んだ。
- 自分になりすまされてオンラインショッピングで買い物をされた。
- プロバイダの管理者になりすまされ、パスワードを教えちゃい、勝手にパスワードを変更された。



不正アクセスの手段

不正アクセス

ワーム

クラッキングツール

なりすまし

ソーシャルエンジニアリング

ユーザの不注意

不正アクセス対策

不正アクセス対策

- ブラウザ
- メール
- 常時接続
- その他の一般的な対策

ブラウザのセキュリティ対策

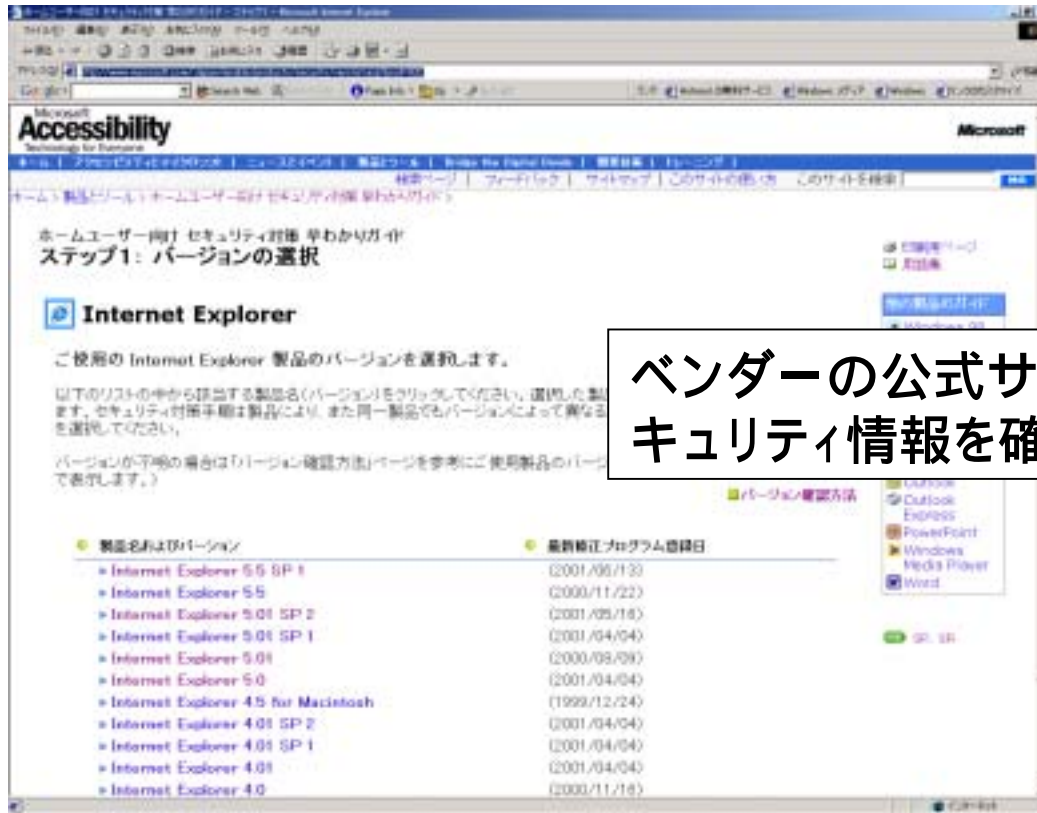
(脅威・被害要因・対策)

- プログラムの自動実行
 - ウイルス感染
 - ハードディスク破壊
 - PC内部の情報を自動的に送信
 - 悪意のプログラムインストール
- ダウンロード

被害要因 - ブラウザ

- セキュリティホール
- 設定の不備
- ユーザの不注意

セキュリティホールやセキュリティパッチの情報を確認



例) マイクロソフト社のホームユーザ向けセキュリティ対策早わかりガイド

<http://www.microsoft.com/Japan/enable/products/security/verslist.asp?prod=032>

■ セキュリティレベル設定



インターネット
ゾーンでは

セキュリティ
レベル = 高

インターネットエクスプローラ等
で「ツール」 「インターネットオ
プション」 「セキュリティ」

■ 信頼済みサイトの利用設定

信頼済みサイト

このゾーンに Web サイトを追加/削除するには、このゾーンのセキュリティの

次の Web サイトをゾーンに追加する(D):

Web サイト(W):

<http://www.ipa.go.jp/security>
<http://www.microsoft.com>

ベンダの公式サイトなどを登録

インターネットエクスプローラ等で
「ツール」「インターネットオプション」
「セキュリティ」
「信頼済みサイト」「サイト」

追加(A)

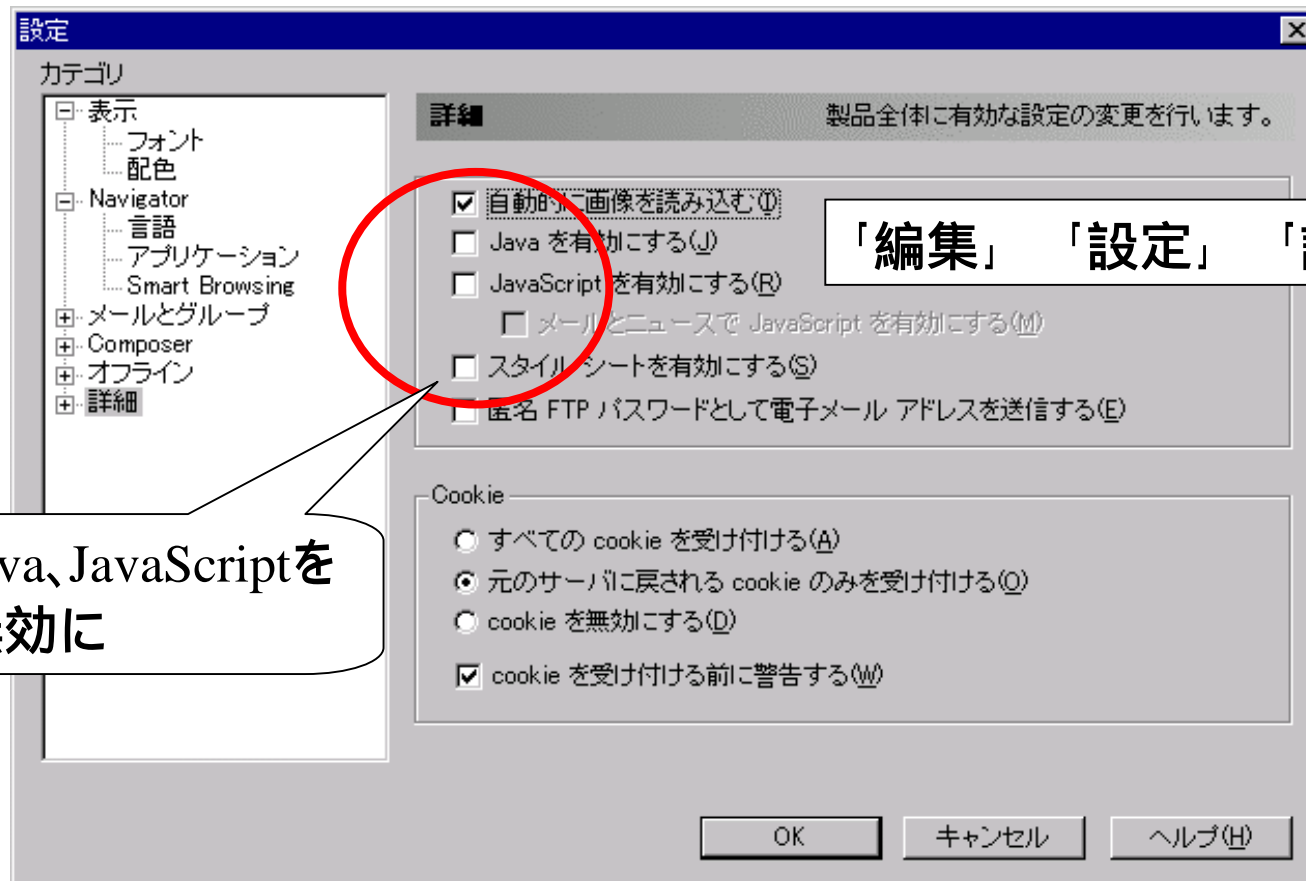
削除(R)

このゾーンのサイトにはすべてサーバーの確認 (https) を必要とする(S)

OK

キャンセル

■ Netscapeの設定例



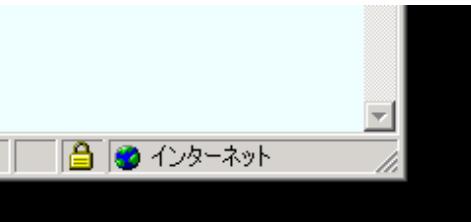
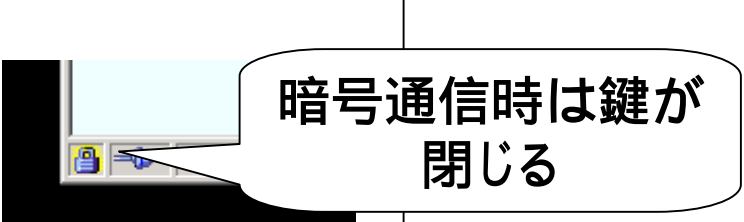


Java、JavaScriptを
無効に

「編集」 「設定」 「詳細」

- ワクチンソフトの導入
 - セキュリティパッチの未適用による被害の防止
 - 悪意のプログラムによる自動実行を検出
 - 設定ミスによる被害の防止
 - ユーザの不注意による被害の防止

- 安易にダウンロードはしない
- あやしいサイトには近づかない
- 重要な個人情報の入力時(カード番号、暗証番号等)は暗号化されているか確認する。

	Internet Explorer	Netscape
非暗号通信		
暗号通信 (SSL)		

メールのセキュリティ対策

(脅威・被害要因・対策)

- プログラムの自動実行
 - ウイルス感染
 - 悪意のプログラムインストール
- なりすましメール
- 内容の改ざん
- 盗み見
- 迷惑メール

- セキュリティホール
- 設定の不備
- ユーザの不注意

最新バージョン、セキュリティパッチの確認



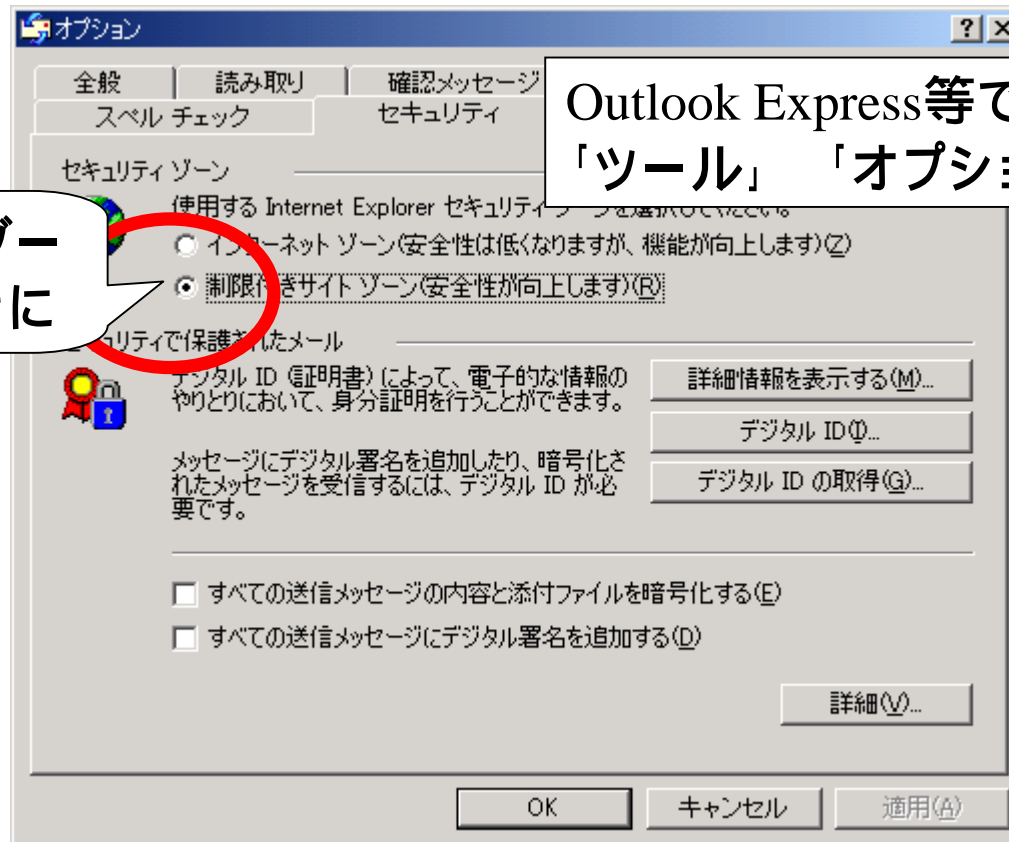
例) マイクロソフト社のホームユーザー向け セキュリティ対策 早わかりガイド

<http://www.microsoft.com/japan/enable/products/security/verslist.asp?prod=034>

セキュリティゾーンの設定例

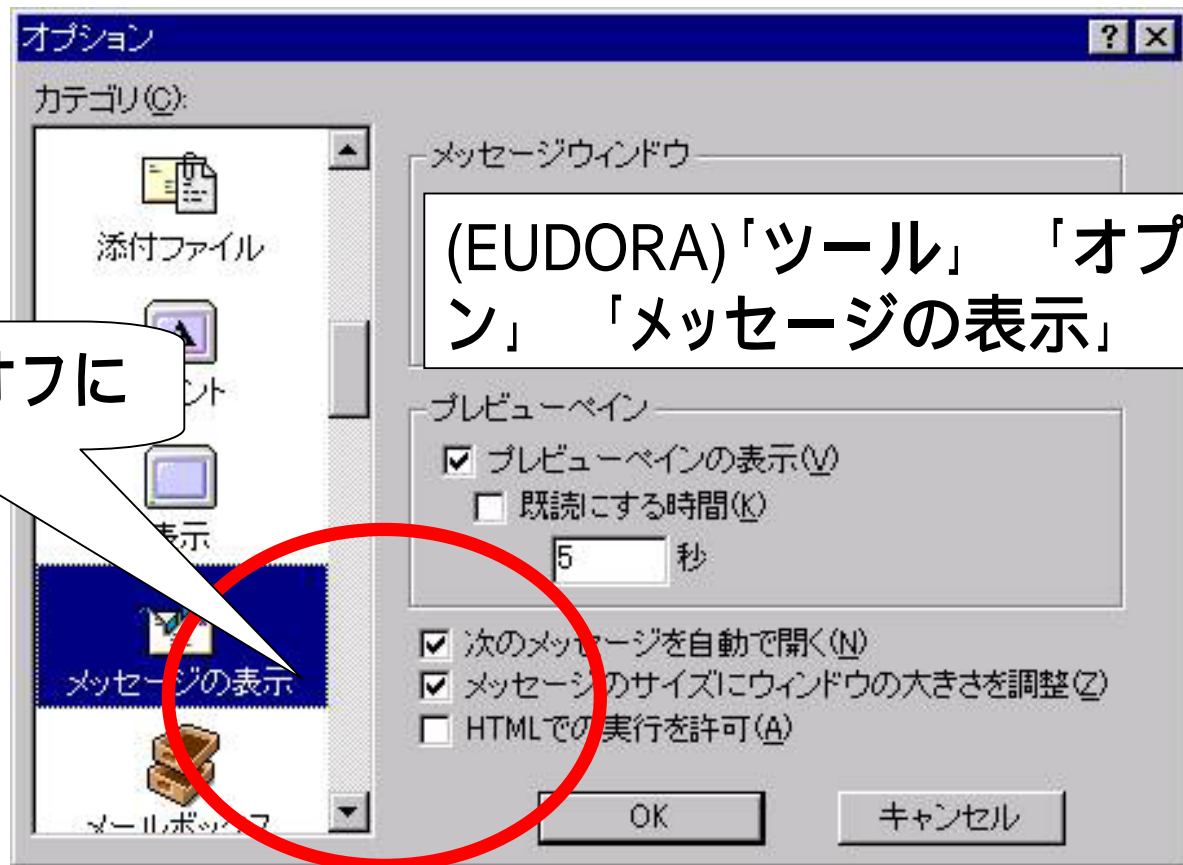
セキュリティゾーンを制限付きに

Outlook Express等で、「ツール」「オプション」「セキュリティ」



例) Outlook Expressのセキュリティゾーンの設定

■ プログラム実行排除の設定例



HTML実行をオフに

(EUDORA)「ツール」「オプション」「メッセージの表示」

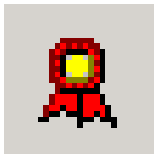
例) Eudoraのプログラム実行排除の設定

- ワクチンソフトの導入
 - メール読み込み時にウイルスの検出
 - 悪意のプログラムによる自動実行を検出
 - 設定ミスによる被害の防止
 - ユーザの不注意による被害の防止

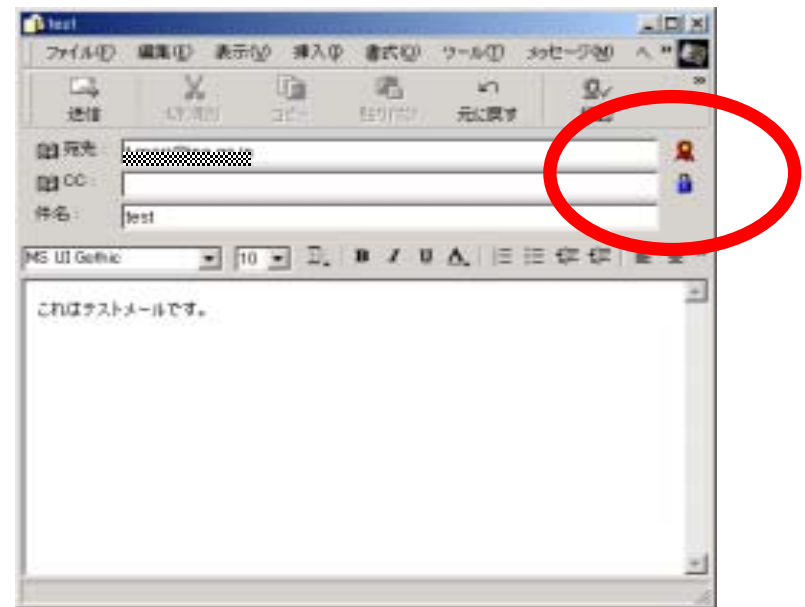
- メールの暗号化
 - 通信経路上での盗聴、改ざんを防止
- デジタル署名
 - メッセージの改ざん防止



暗号化メール



署名付きメール



暗号化 / 署名付きメール例

- 不審な添付ファイルなど
 - 送信元を確認し、ワクチンソフトでチェックする。
- 迷惑(勧誘)メールなど
 - 興味本位でブラウザで開かない
 - 不要ならばそのまま捨てる
 - メールの自動振り分け等の設定で捨てる
- スпамメール
 - 受信拒否の設定
 - プロバイダや管理者へ連絡しスプールの削除を依頼
- チェーンメール
 - 転送はせずそのまま捨てる

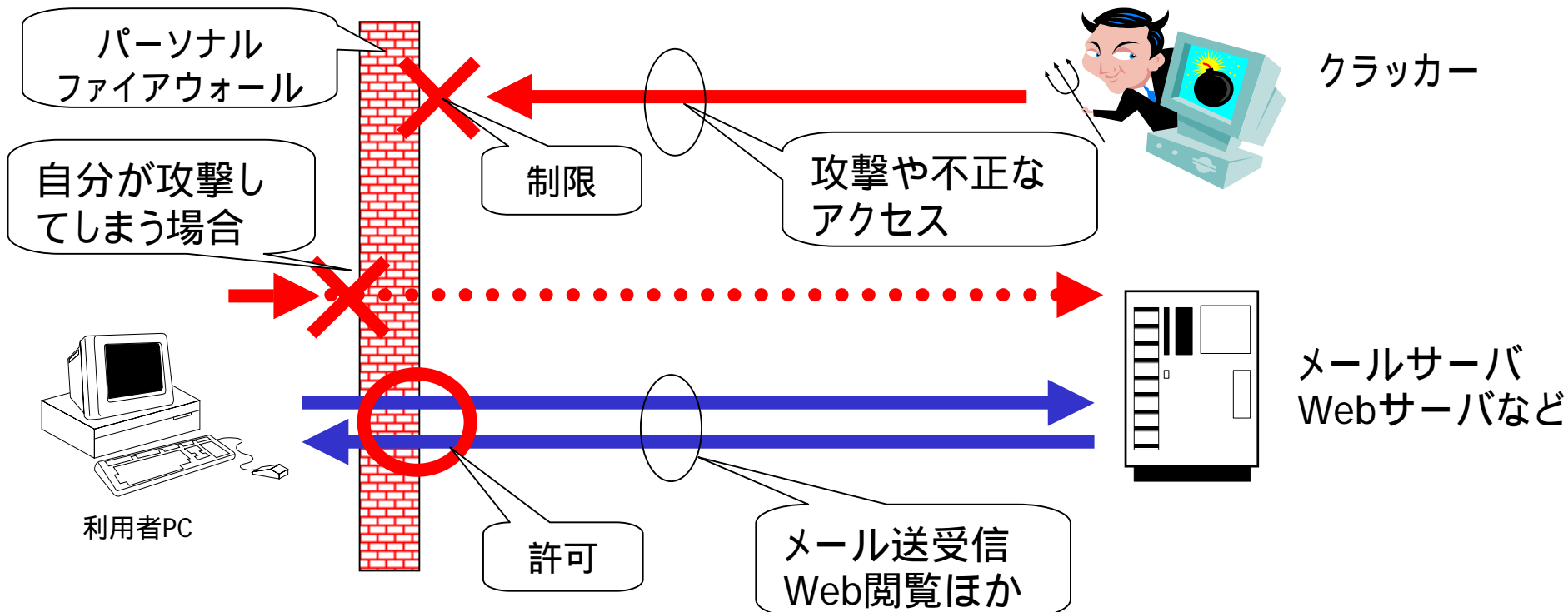
常時接続環境のセキュリティ対策

(脅威・被害要因・対策)

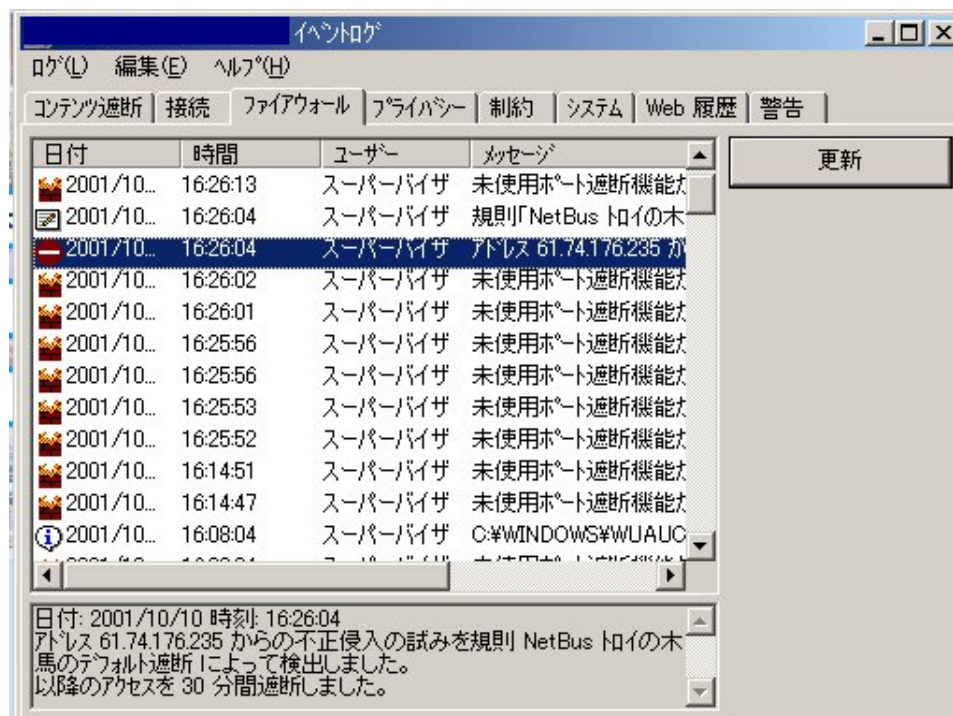
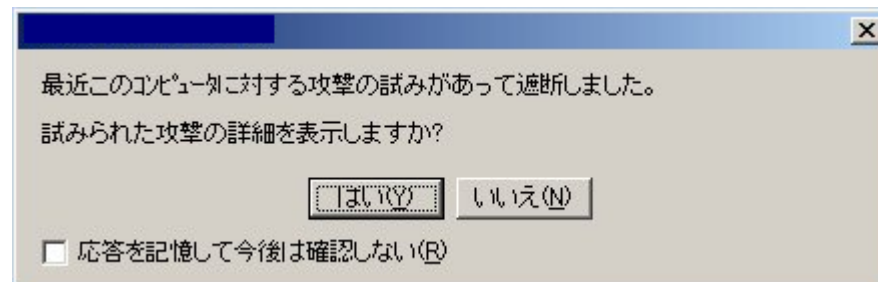
- 外部からの侵入
 - 悪意のプログラムの埋め込み
 - クラッキングツール
 - ファイル共有
 - 侵入行為そのもの
- ポートスキャン
- DoS攻撃
- 加害者となる危険性

- 常時(長時間)接続のため攻撃対象となりやすい
- 設定の不備

- パーソナルファイアウォール
 - 外部からのアクセスを制限
 - パケットフィルタリング機能

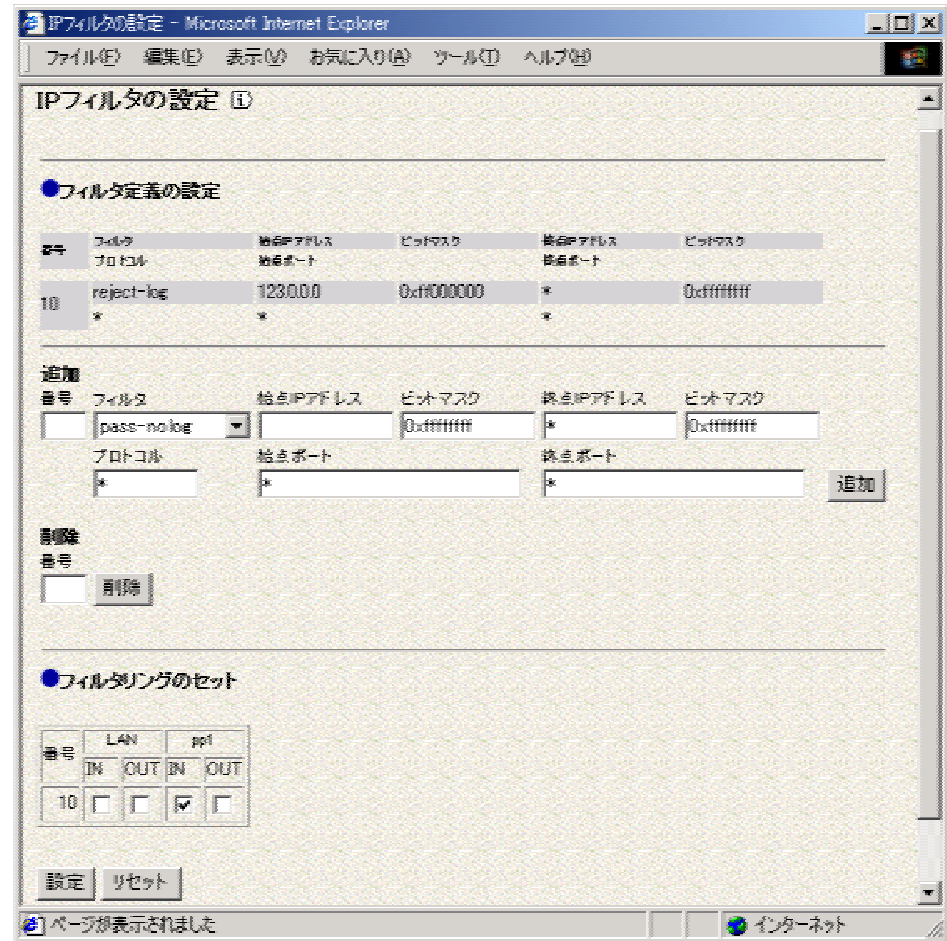


- 定期的なパターンファイルの更新
- ログの定期的なチェック
- 自分のマシンから他へマシンへのアクセスも注意



■ ホームルータ

- パケットフィルタリング機能



例) パケットフィルタの設定

ファイル共有の確認・設定解除

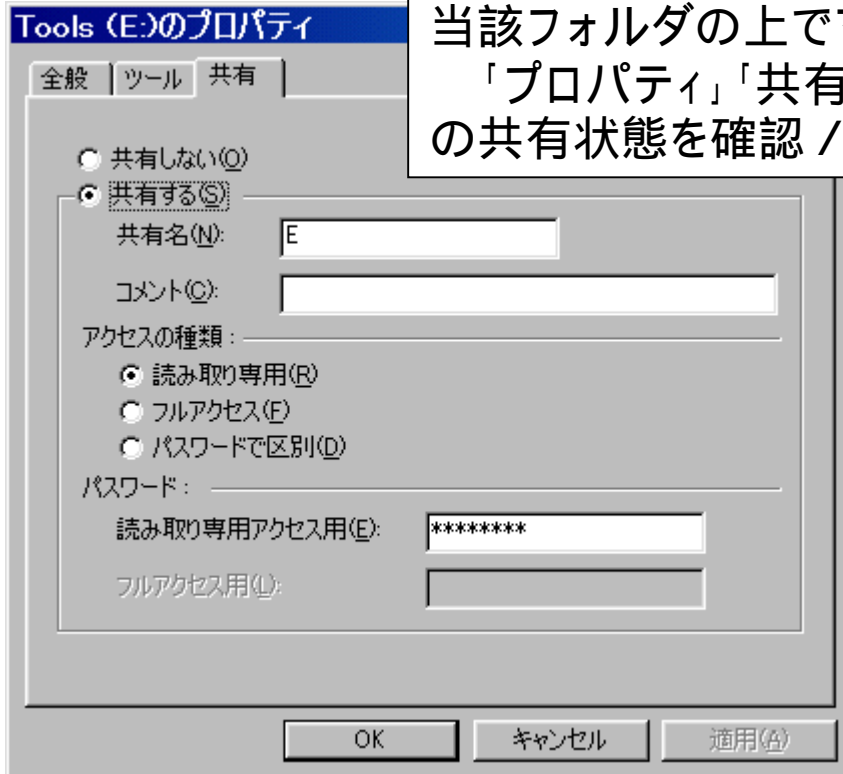
当該フォルダの上でマウス「右クリック」
「プロパティ」「共有」タブ選択で、実際の共有状態を確認 / 設定できる。



共有可能なディスク

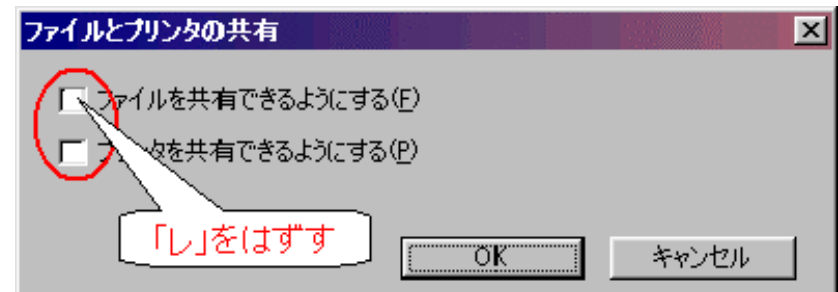


共有可能なフォルダ



例) フォルダのプロパティ

例) Windows9x, Me



「コントロールパネル」「ネットワーク」「ネットワークの設定」「ファイルとプリンタの共有」で「ファイルを共有できるようにする」マークをはずすことで**根本的に共有ができなくなる**

その他の一般的な対策

その他の一般的な対策

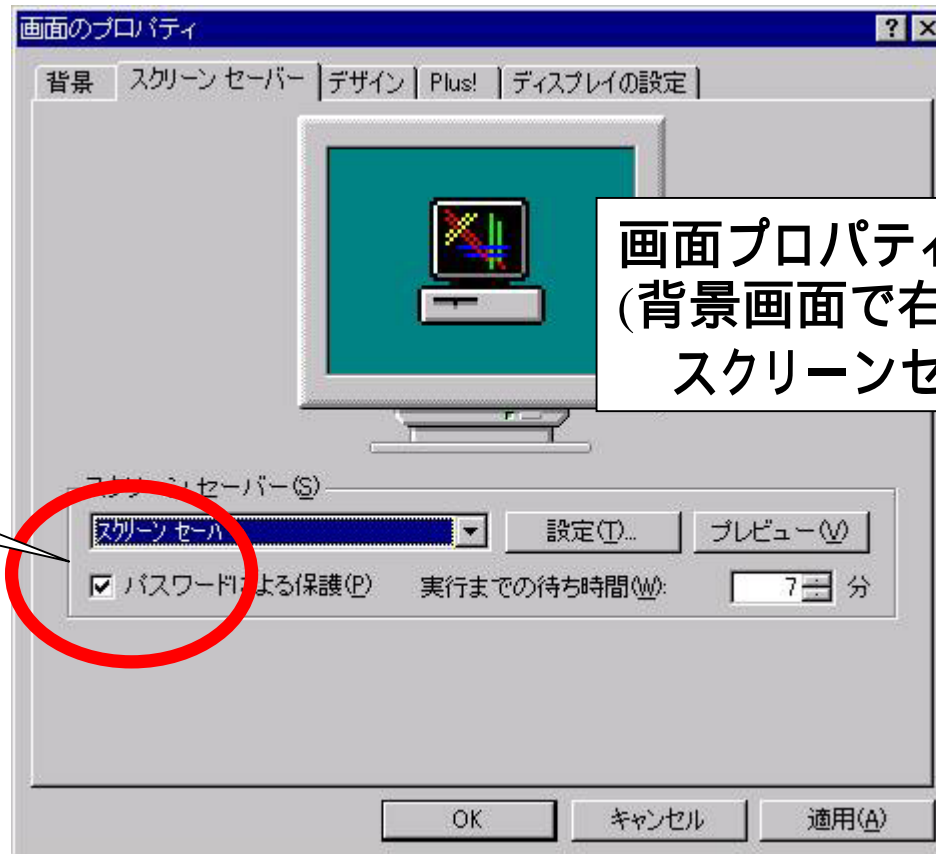
- 起動時(BIOS)のパスワードの設定
 - モバイルPCは必須



例) BIOSのパスワード入力画面

その他の一般的な対策

■ パスワードによる保護の利用



パスワードによる保護

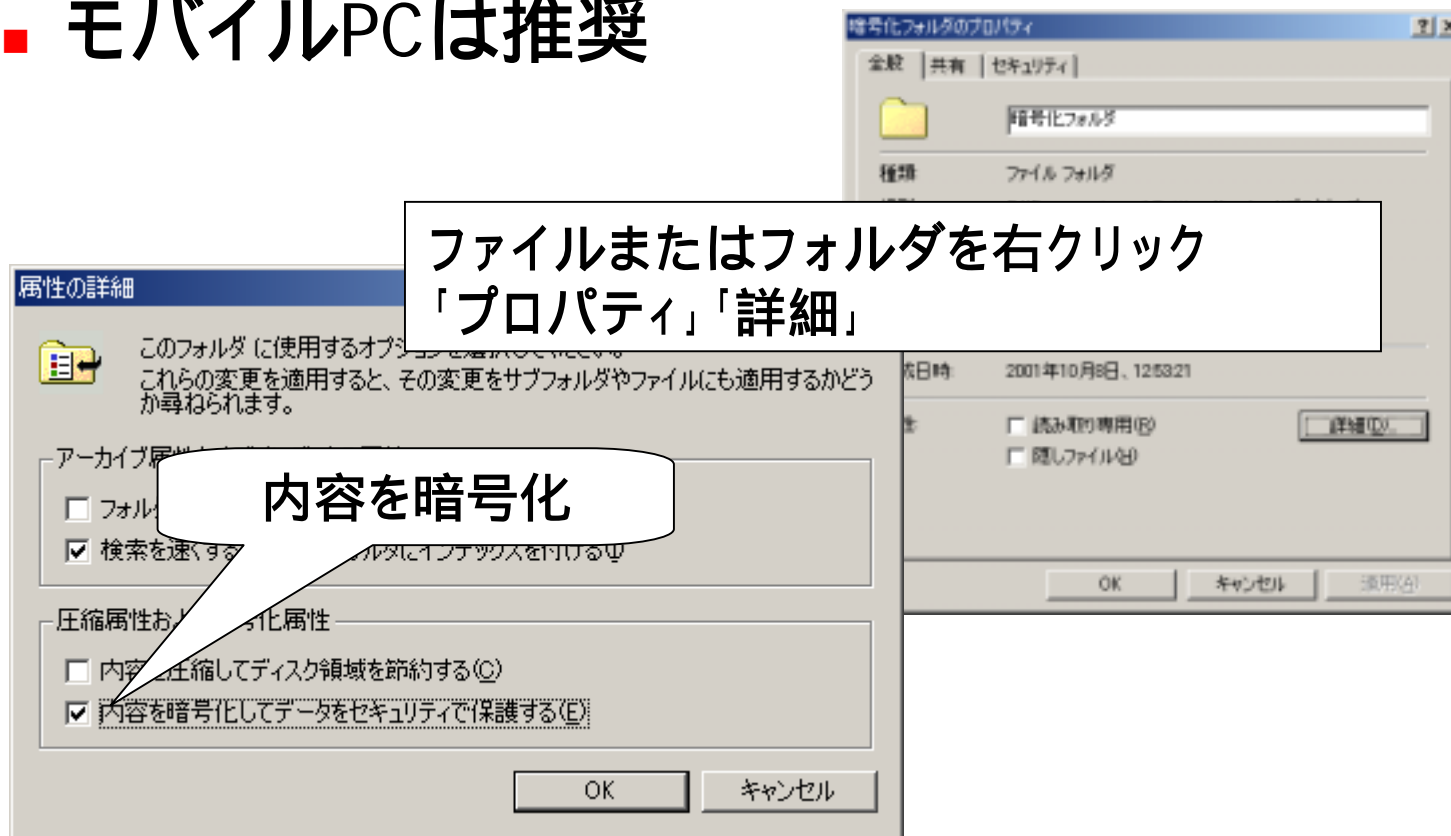
画面プロパティ
(背景画面で右クリックメニュー)
スクリーンセーバー

例) スクリーンセーバのパスワードによる保護機能の設定例

その他の一般的な対策

ファイルの暗号化ソフト(機能)の利用

- モバイルPCは推奨

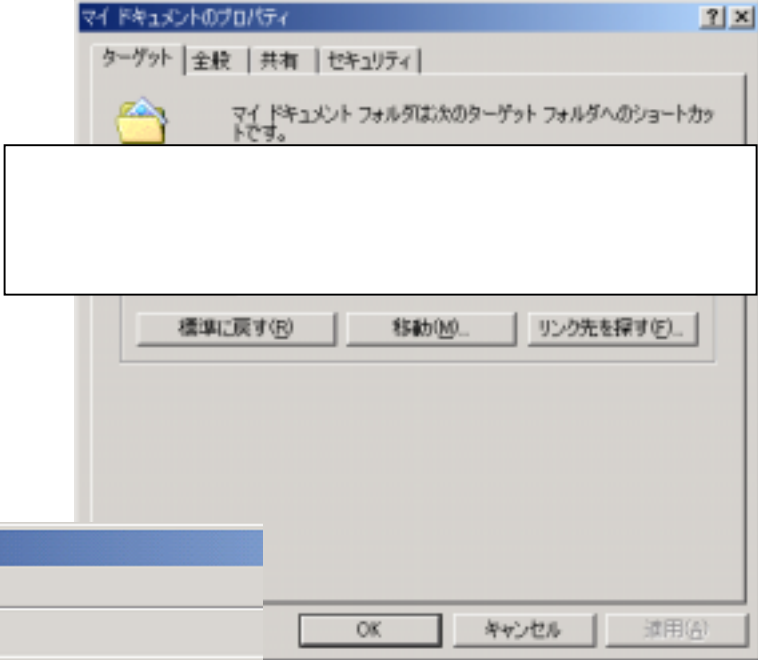


例) Windows2000のフォルダ暗号化

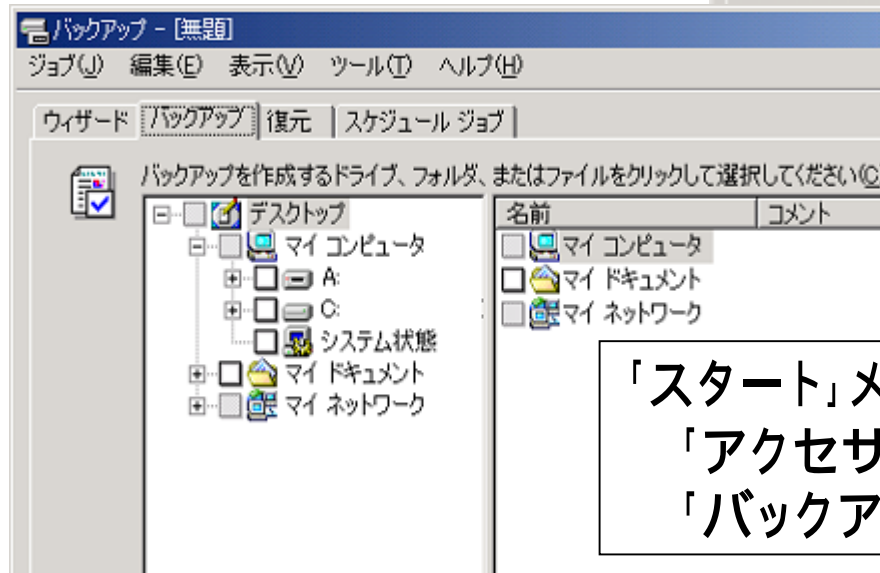
その他の一般的な対策

■ バックアップ

- システムドライブとデータドライブの分離
- バックアップソフト (機能) の利用



「マイドキュメント」を右クリック
「プロパティ」



「スタート」メニュー 「プログラム(P)」
「アクセサリ」 「システムツール」
「バックアップ」を選択

- パスワードの管理
 - 不適切なパスワード
 - 長さが不十分、辞書に載っている単語の利用、IDと同じ、自分・家族の情報、固有名詞、単純な数字や文字の並び、過去に使用したパスワードの再利用等
 - 適切なパスワード
 - 大文字・小文字・数字・記号の組み合わせ、長いパスワード、推測しづらく自分が忘れないパスワード
例えばパスフレーズによる設計
 - パスワード盗難対策
 - 定期的な変更、紙に書き留めない、マシンに保存しない人に教えない

その他の一般的な対策

- パスフレーズによるパスワードの設計
パスフレーズ

「H A R U H A A K E B O N O」

母音を抜き記号や数字を挿入

パスワード

「H R \$ H K % B N」

セキュリティ対策ポイント(まとめ)

- ブラウザ
 - セキュリティパッチの適用、設定、ワクチンソフトの利用、ダウンロードは注意
- メール
 - セキュリティパッチの適用、設定、ワクチンソフトの利用、メールの暗号化ほか
- 常時接続
 - パーソナルファイアウォール、ホームルータ
- その他の一般的な対策
 - パスワード管理、ファイルの暗号化、バックアップ

- エンドユーザにおいても**セキュリティ対策が必須**
 - 自分だけではなく他へ被害を及ぼす危険性もある
- **予防**と被害の拡散防止が肝心
 - 破壊された情報、漏洩した情報は元に戻らない
 - 事後の対応は非常に手間がかかる
- 被害拡散防止のためには
 - 面倒がらず各種確認等を**確実に実施**する
 - 『エンドユーザー向け不正アクセス対策チェックシート』参照
 - 必要と思われる対策情報は常に**手元に用意しておく**
- 特に個人でのインターネット接続においては**自己責任・自己防衛が基本**

情報処理振興事業協会 セキュリティセンター (IPA/ISEC)

〒113-6591

東京都文京区本駒込2-28-8

文京グリーンコートセンターオフィス16階

TEL 03(5978)7508 FAX 03(5978)7518

ウイルス/不正アクセス相談110番 TEL 03(5978)7509

電子メール virus@ipa.go.jp crack@ipa.go.jp

URL <http://www.ipa.go.jp/security/>