

不正プログラム対策ガイドライン

Ver. 2.0

不正プログラム調査WG

渡部 章

2006年3月31日

- はじめに
- ステップ1 理解と認識
- ステップ2 対策の実施と維持
- ステップ3 調査と現状把握
- まとめ
- WGメンバー紹介

はじめに

- 近年、トロイの木馬、スパイウェア、ボットなどの不正アクセスを目的とした不正プログラムが増加している。また、ウイルス、ワームも同様に不正アクセスを目的としたものも少なくない。
そのような状況を鑑み、不正プログラムを分類化し、タイプ別、侵入経路別に、その対策ソリューションを分かりやすく取りまとめた。
- 本ガイドラインの目的は
 - ユーザ企業の視点でセキュリティソリューション購入のガイドとなる。
 - セキュリティソリューションの販売者がユーザ企業への説明用に使用できる。
- ここに上げた不正プログラムとは、ユーザマシンでユーザが意図しないで侵入し、ユーザの意図しない不正を働くプログラムを対象としている。
- 対策には技術的対策とセキュリティポリシー運用などの組織的対策に限ることとし、施設管理等の物理的対策および法的対策は除いた。
 - 本ガイドライン中の「社内」は、学校、自治体など各組織の呼び方に置き換えてお読みください。



ステップ1

理解と認識

被害状況



- 国内初、スパイウェア作成者逮捕 ネット銀不正送金で (2006/1/27)
 - <http://www.itmedia.co.jp/news/articles/0601/26/news041.html>
- 2005年のキーロガー攻撃、65%増加 (2005/11/17)
 - <http://www.itmedia.co.jp/news/articles/0511/16/news051.html>
- 画像クリックで不当請求、ワンクリック詐欺へ注意呼びかけ (2005/8/16)
 - <http://www.itmedia.co.jp/news/articles/0508/16/news040.html>
- ネット銀行の不正対策相次ぐ (2005/8/2)
 - <http://www.itmedia.co.jp/news/articles/0508/02/news059.html>
- 「防ぎようがなかった...」、ネット銀不正引き出しの被害者語る (2005/7/23)
 - <http://www.itmedia.co.jp/news/articles/0507/22/news089.html>
- スパイウェアによる不正送金被害が拡大 (2005/7/6)
 - <http://www.itmedia.co.jp/news/articles/0507/06/news024.html>
- 他人事ではない？ 「ワンクリックウェア」の実態 (2006/3/31)
 - <http://www.itmedia.co.jp/enterprise/articles/0603/31/news079.html>
- Winny 流出事件頻発 (2005/6 ~ 2006/3)

出展: ITmedia

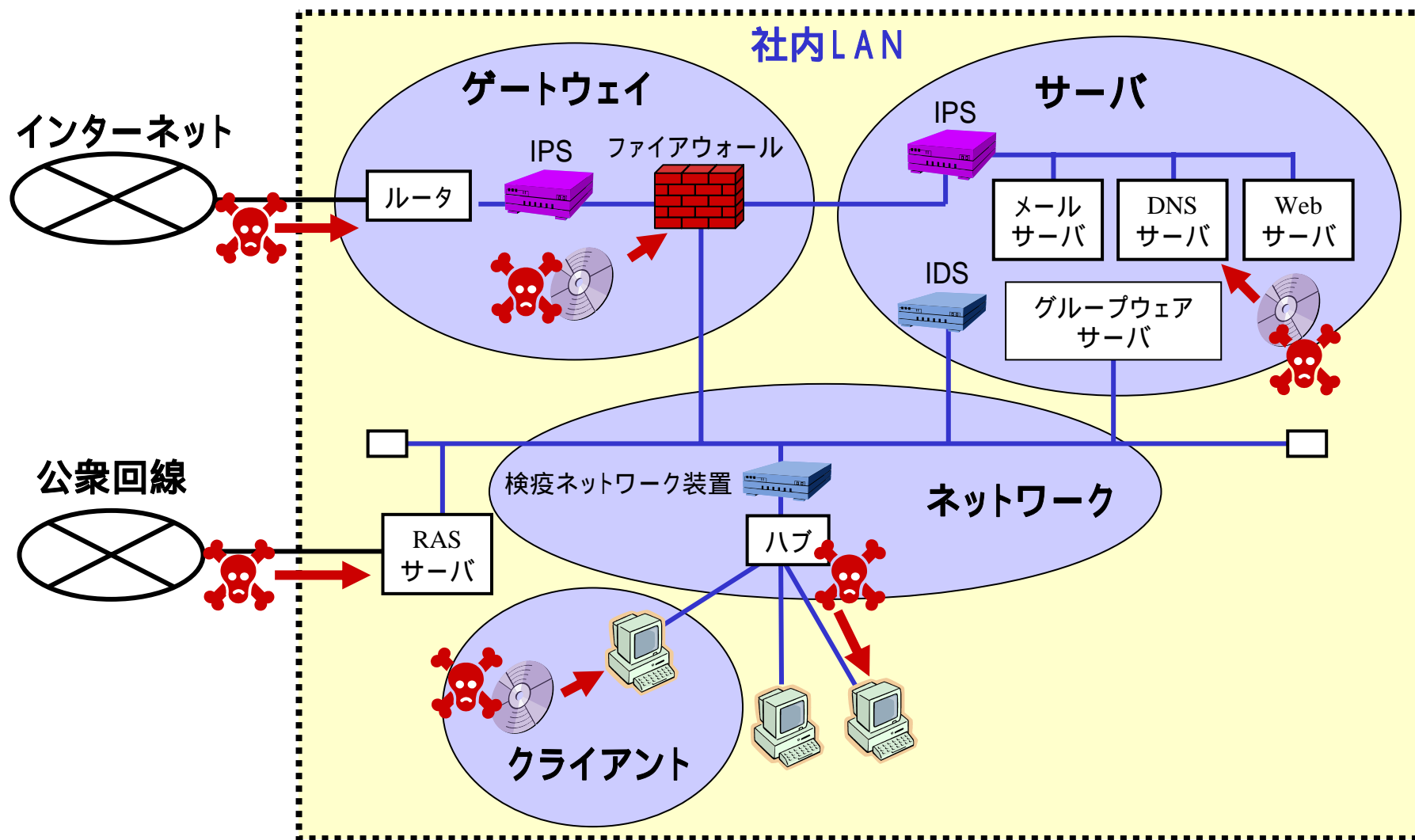
不正プログラムの解説

- 前提

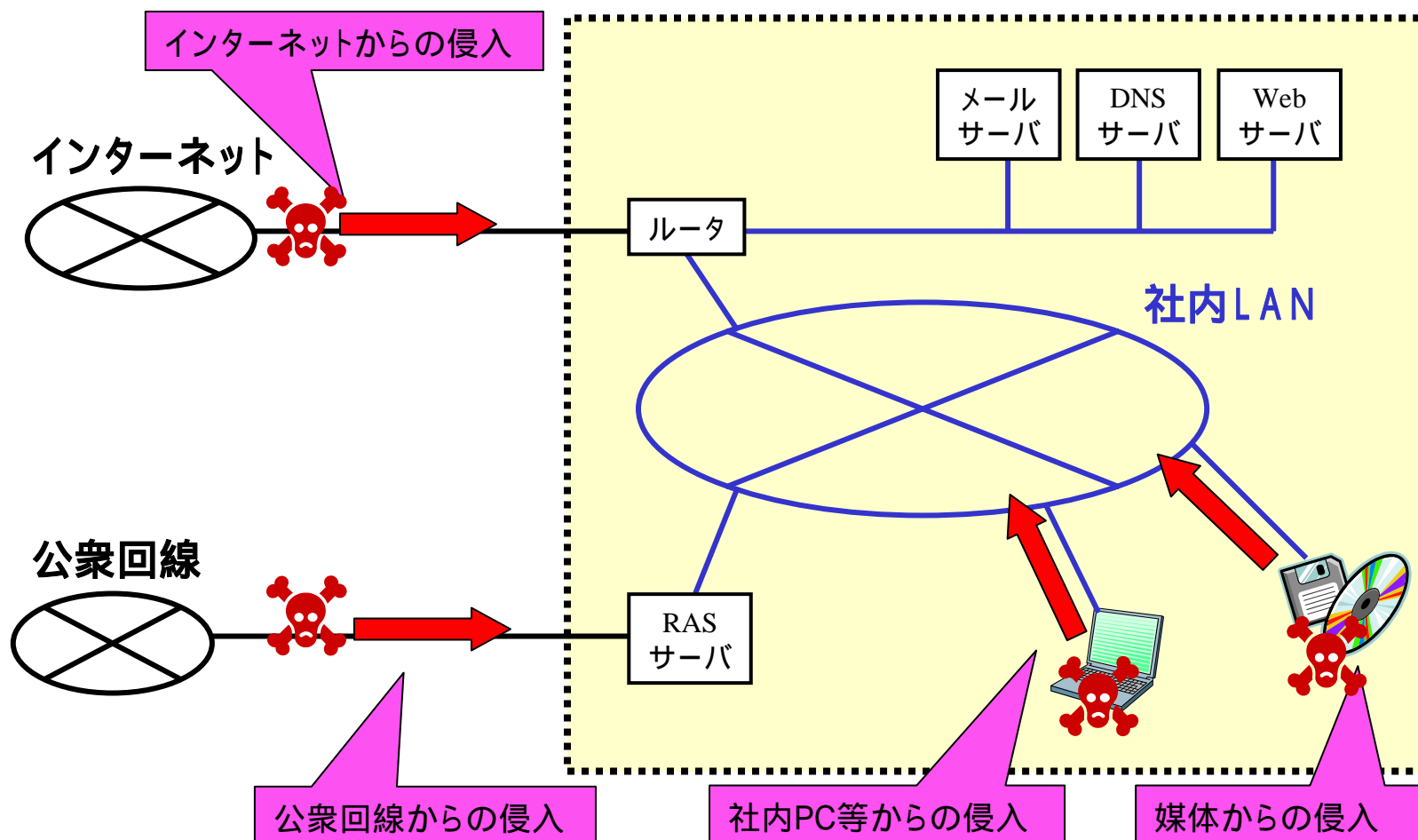
- 対象とする不正プログラムは、ユーザが意図しないうちにユーザのマシンに侵入し、何らかの被害を与えるプログラムとする。
- 攻撃者が攻撃者のマシンで利用するハッキングツール類や、ファイル自体に危険性はないが他のファイルを使うことで危険な動作を行うことが可能なプログラムは対象としていない。(例:P2Pソフトなど)

名称	解説
ウイルス	プログラムに寄生して増殖し、感染、破壊、いたずら、盗聴などの被害を与えるプログラム。
ワーム	自分自身をコピーして増殖し、感染、破壊、いたずら、盗聴などの被害を与えるプログラム。
トロイの木馬	通常のソフトウェアに見せかけて、破壊、いたずら、盗聴などの被害を与えるプログラム。
スパイウェア	ユーザの知らないうちに、ユーザの情報や操作履歴を外部に送信するプログラム。
アドウェア	広告のウィンドウをポップアップ表示させたり、ブラウザで広告を表示させるプログラム。
ハイジャッカー	ブラウザ起動時に最初に表示するWebページ(ホームページ)を変更したり、閲覧しようとするページとは異なるページへ強制的に誘導するプログラム。
ボット	外部からの命令により、他人のパソコンを制御したり、攻撃の踏み台にするために、制御するパソコン側で動作するプログラム。

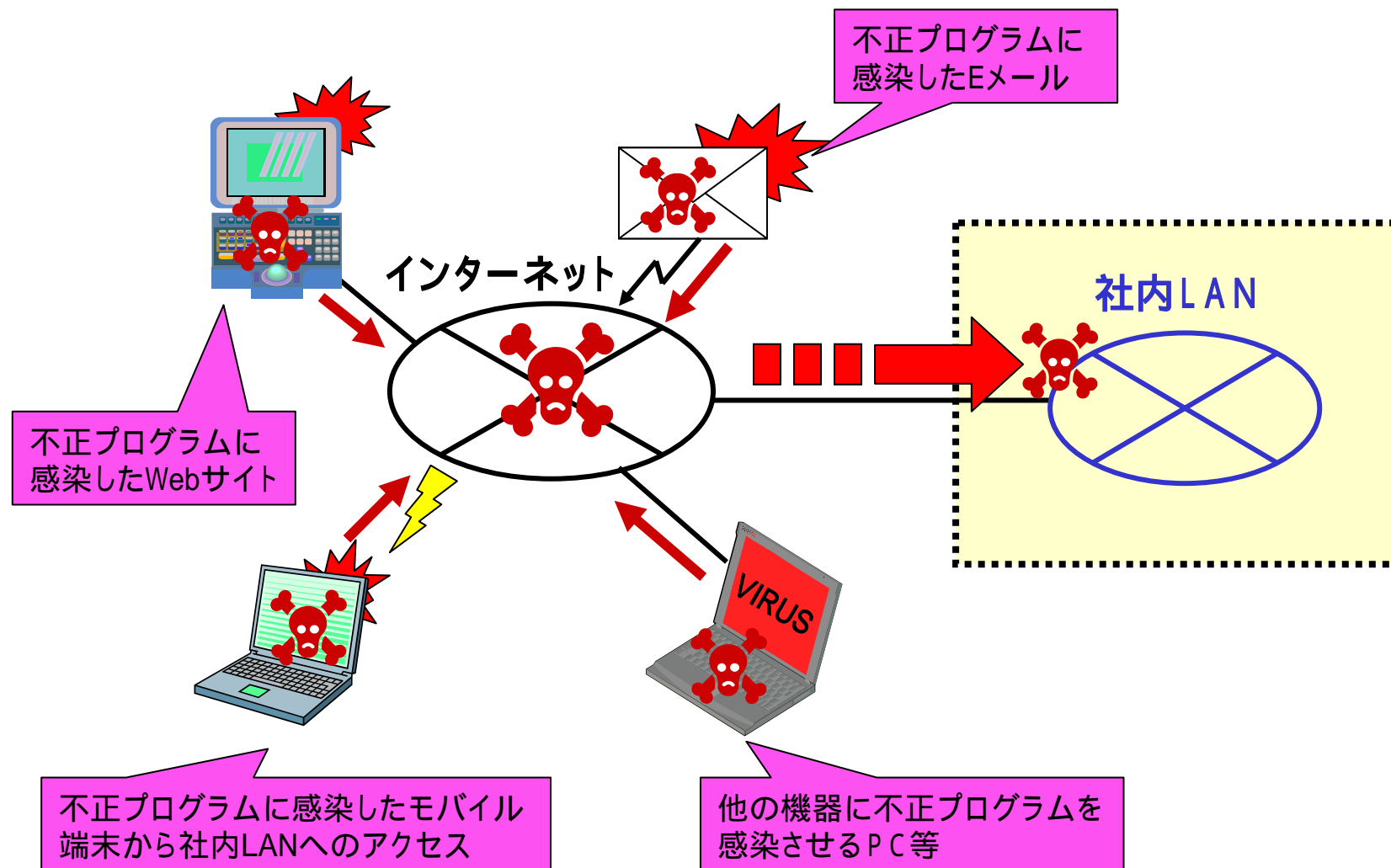
不正プログラムの侵入経路



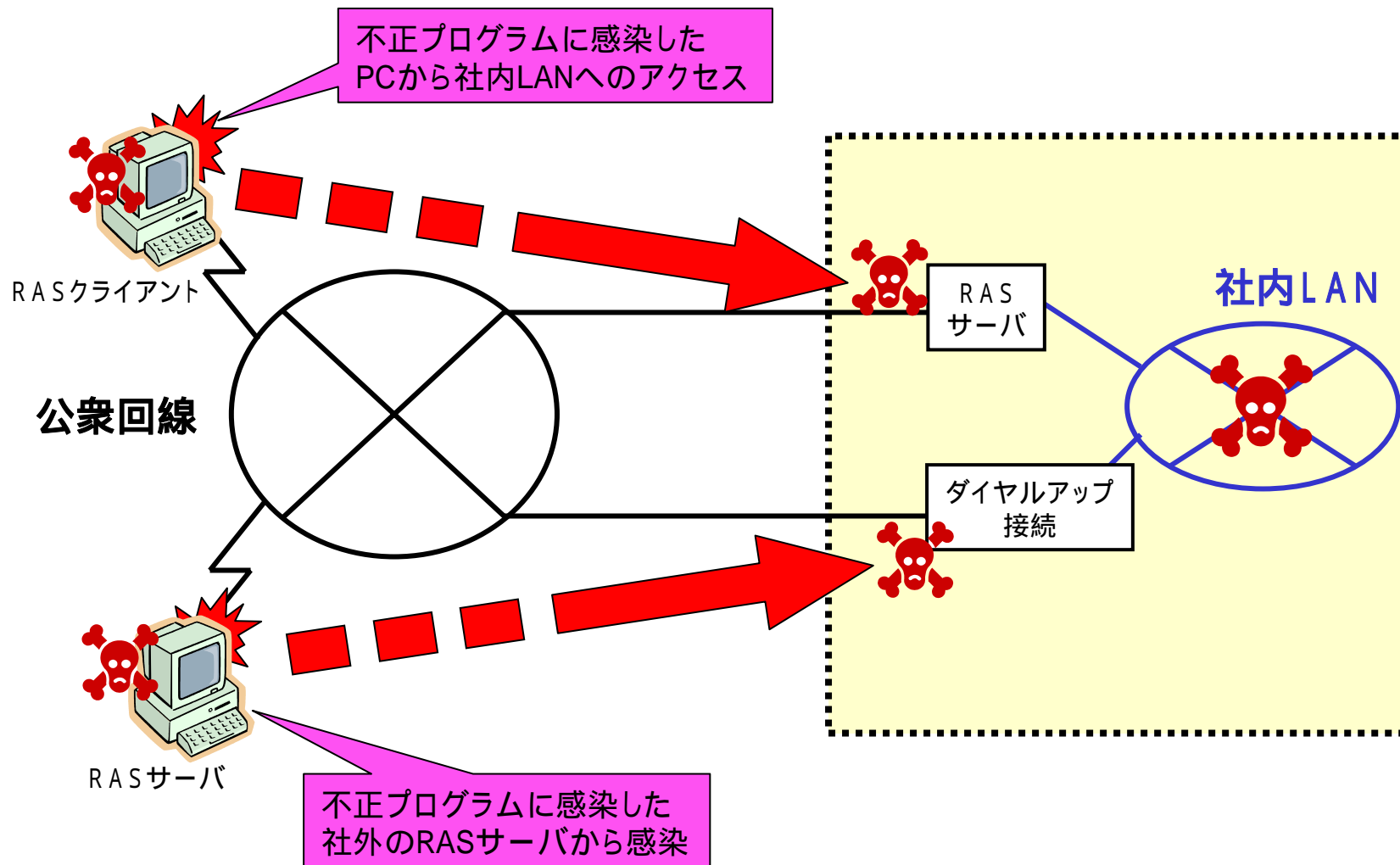
社内LANへの主な侵入経路



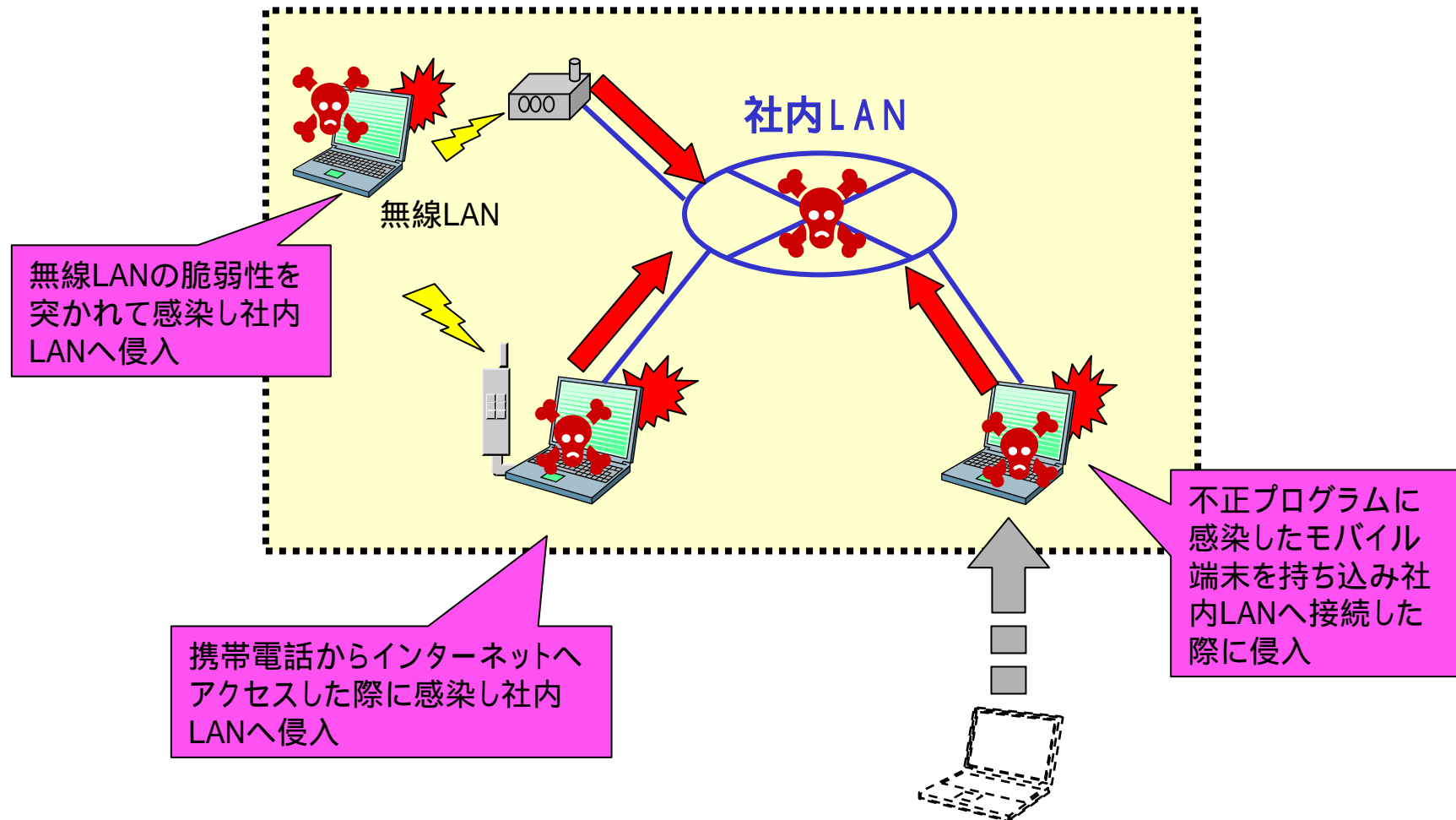
インターネットからの侵入



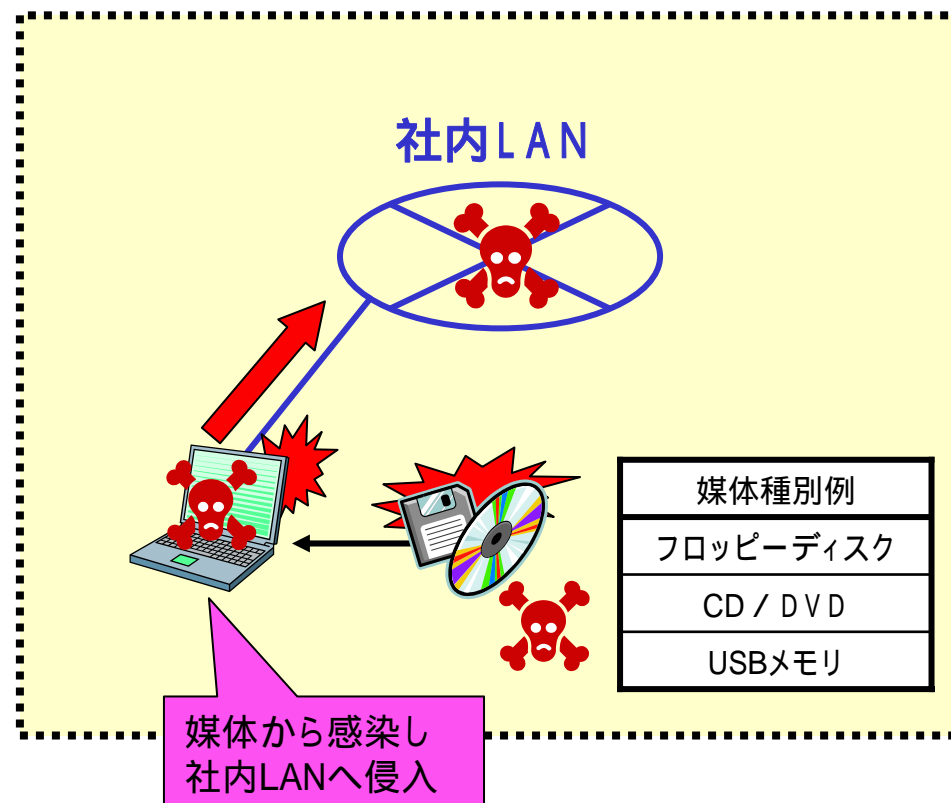
公衆回線からの侵入



社内PC等からの侵入



媒体からの侵入



社内LANへの侵入経路

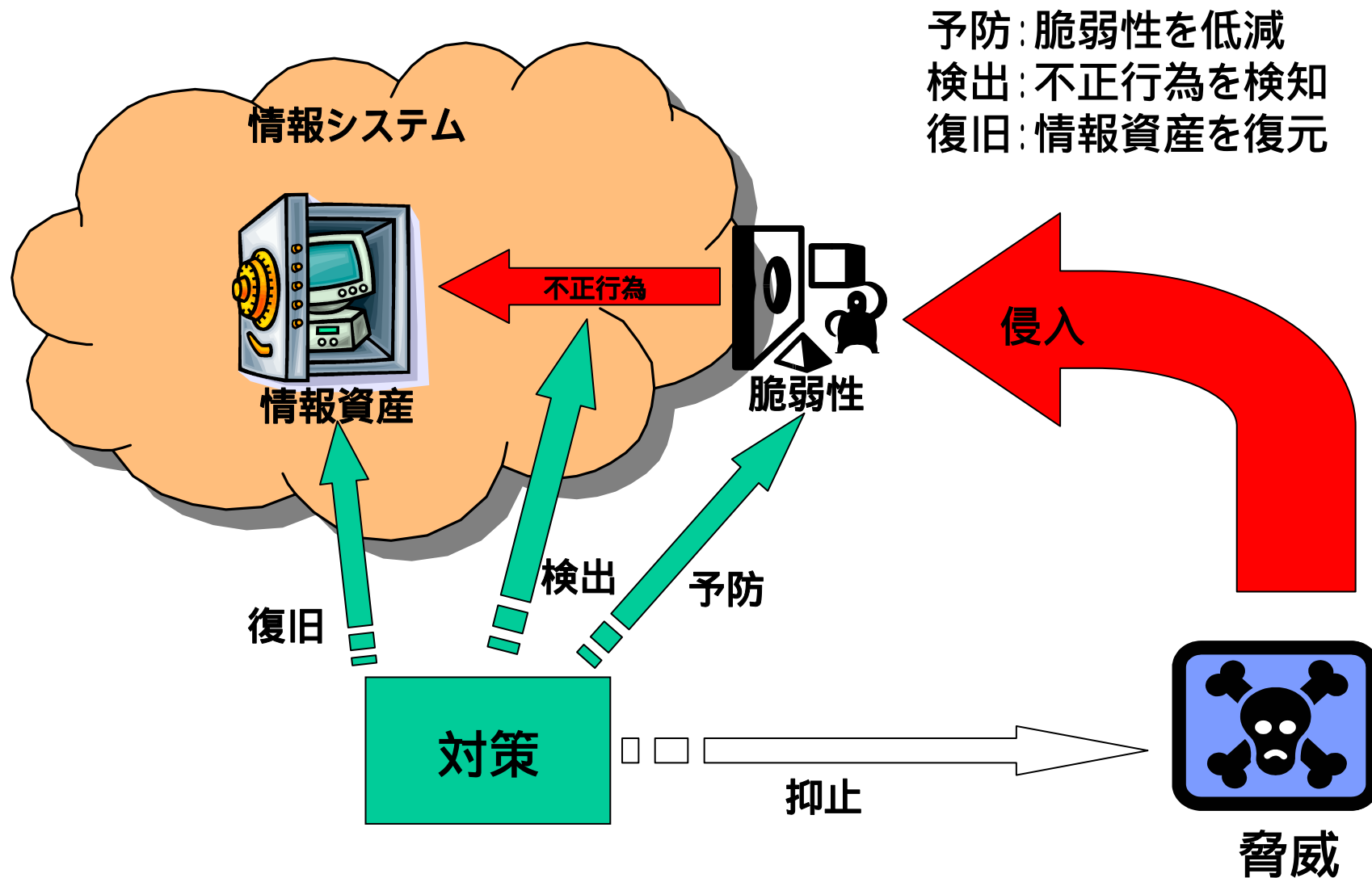


不正プログラム 侵入経路		ウイルス	ワーム	トロイの木馬	スパイウェア	アドウェア	ハイジャッカー	ボット
		インターネットから	Eメール送受信					
Webサイト閲覧								
ファイル受信								
他の機器からの感染								
公衆回線から - RAS接続 - ダイヤルアップ	Eメール送受信							
	Webサイト閲覧							
	ファイル送受信							
	他の機器からの感染							
社内LANから - 無線LAN - 携帯電話 - 不正接続PC	Eメール送受信							
	Webサイト閲覧							
	ファイル送受信							
	他の機器からの感染							
媒体から	ファイルコピー							
	ソフトウェアインストール							

不正プログラムの症状例

- 侵入時
 - 見知らぬメールにファイルが添付されている
 - 見知らぬファイルが作成されている
 - タスクバーなどに妙なアイコンができる
 - いきなりインターネットからのダウンロードが始まる
 - いきなりブラウザからActiveXの確認メッセージが表示される
- 潜伏時
 - システムやアプリケーションが頻繁にハングアップする
 - いきなりインターネット接続をしようとする
 - いきなりポップアップによる広告ウィンドウが表示される
 - コンピュータの動作が遅くなる
 - インターネットの接続が遅くなる
- 発病時
 - システムが起動しなくなる
 - いたずらのメッセージや画像が表示される
 - ファイルが消失する
 - ユーザの意図しないメール送信が行われる
 - 直感的にいつもと何かが違うと感じる

不正プログラム対策の3要素



不正プログラム対策一覧と解説



• デスクトップソリューションで主に用いられる対策

ウイルス対策ソフト

予防:

検知:

復旧:

- ウイルス対策ソフトはコンピュータウイルスに感染したファイルの修復や削除を行います。ただ、コンピュータウイルスの検知精度に関してはウイルスの種類、対策製品などによって偏りがあるので注意が必要です。

パーソナルファイアウォール

予防:

検知:

復旧: ×

- パーソナルファイアウォールは個々のPCを保護する為のファイアウォールです。あらかじめ決められたルールと照らして、通信の許可・拒否を処理します。必要最小限の通信だけ許可する事で外部からの不正アクセスやPCの不正利用を阻止する事が可能です。ただし、アプリケーションレベルで判断しないと対策不可能な不正プログラムが多数あり、これらの物に対しては一般的にパーソナルファイアウォールでの対策は困難なケースがあります。

ホスト型IDS/IPS

予防:

検知:

復旧: ×

- IDS(Intrusion Detection System)は不正な通信を検知し通知する為のシステムです。ホスト型IDSはホストにインストールするタイプのIDSで、外部 PC、PC内部 外部に対する不正なアクセスを検知し通知します。また、IPS(Intrusion Prevention System)機能を持っている場合は不正なアクセスを検知した後に通信を阻止する事が可能です。

スパイウェア対策ソフト

予防:

検知:

復旧:

- スパイウェア対策ソフトはPC上にインストールされているスパイウェアの検知や削除を行います。コンピュータウイルスとは異なる為、ウイルス対策ソフトでは検知出来ないケースが多々あります。

パッチマネージメント

予防:

検知: ×

復旧: ×

- OSやアプリケーションに最新の修正プログラム(パッチ)を付加する事によりセキュリティホールを防ぎます。

不正プログラム対策一覧と解説



サーバソリューションで主に用いられる対策

ウイルス対策ソフト

予防:

検知:

復旧:

- ウイルス対策ソフトはコンピュータウイルスに感染したファイルの修復や削除を行います。ただ、コンピュータウイルスの検知精度に関してはウイルスの種類、対策製品などによって偏りがあるので注意が必要です。

パーソナルファイアウォール

予防:

検知:

復旧: ×

- パーソナルファイアウォールは個々のPCを保護する為のファイアウォールです。あらかじめ決められたルールと照らして、通信の許可・拒否を処理します。必要最小限の通信だけ許可する事で外部からの不正アクセスやPCの不正利用を阻止する事が可能です。ただし、アプリケーションレベルで判断しないと対策不可能な不正プログラムが多数あり、これらの物に対しては一般的にパーソナルファイアウォールでの対策は困難なケースがあります。

ホスト型IDS/IPS

予防:

検知:

復旧: ×

- IDS(Intrusion Detection System)は不正な通信を検知し通知する為のシステムです。ホスト型IDSはホストにインストールするタイプのIDSで、外部 PC、PC内部 外部に対する不正なアクセスを検知し通知します。また、IPS(Intrusion Prevention System)機能を持っている場合は不正なアクセスを検知した後に通信を阻止する事が可能です。

セキュアOS

予防:

検知: ×

復旧: ×

- 強制アクセス制御と最小特権の二つの機能を持つOSです。正しく設定を行う事で不正な攻撃に対する体制をある程度持たせることが可能です。

パッチマネージメント

予防:

検知: ×

復旧: ×

- OSやアプリケーションに最新の修正プログラム(パッチ)を付加する事によりセキュリティホールを防ぎます。

不正プログラム対策一覧と解説



• ゲートウェイソリューションで主に用いられる対策

ファイアウォール	予防:	検知:	復旧: ×
----------	-----	-----	-------

- IPアドレスやPort番号でアクセス制御を行うシステムです。IPアドレスやPort番号からでは不正プログラムの判断が難しいケースが多い為ファイアウォールだけで不正プログラム対策を行う事は難しくなっています。最近ではアプリケーションレベルまで確認して様々な制御を行ったり、他の機器との連携(認証、ウイルススキャン、フィルタリングなど)を行うことが出来る製品も出てきています。この様に、アプリケーションレベルでアクセス制御を行う機能を持った製品はアプリケーションファイアウォールと呼ばれています。

アプリケーションファイアウォール	予防:	検知:	復旧: ×
------------------	-----	-----	-------

- IPアドレスやPort番号だけではなくアプリケーションレベルでのアクセス制御を行う事が可能なファイアウォールです。アプリケーションレベルまで確認して様々な制御を行ったり、他の機器との連携(認証、ウイルススキャン、フィルタリングなど)を行う事が出来る製品もあります。

不正プログラム対策一覧と解説



- 監視ソリューションで主に用いられる対策

IDS/IPS	予防:	検知:	復旧: ×
---------	-----	-----	-------

- IDS(Intrusion Detection System)は不正な通信を検知し通知する為のシステムです。
IPS(Intrusion Prevention System)は不正な通信を検知した後に該当する通信を阻止する事が可能なシステムです。

- 検疫ソリューションで主に用いられる対策

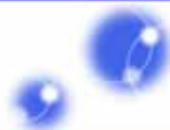
検疫ネットワーク	予防:	検知:	復旧: ×
----------	-----	-----	-------

- クライアント・パソコンの安全性をチェックしてから社内ネットワークに接続させようというセキュリティソリューションです。ウイルス対策ソフトのパターン・ファイルが最新のものかどうか、OSのパッチがきちんと当てられているかどうかなど、パソコンのセキュリティ状況をチェックし許可されたクライアントのみネットワーク接続を許可します。

- バックアップソリューション

データの復元	予防: ×	検知: ×	復旧:
--------	-------	-------	-----

- OSやアプリケーションのインストール時の状態に戻す事で不正プログラムから被害を受けたとしても、元の状態に戻す事が出来ます。注意点としては、不正プログラムに不正にアクセスされていない状態でデータのバックアップを取る必要があると言う事があげられます。



ステップ2

対策の実施と維持

計画 (Plan)

- 現状把握 (リスク分析)
 - 既存セキュリティ対策 (技術、組織) の把握
 - 脅威の把握
 - 侵入経路の把握
 - 優先順位の決定
- 対策案の決定
 - 組織的対策
 - セキュリティルール策定
 - 体制構築 (ヘルプデスク、緊急時の報告)
 - 技術的対策
 - ネットワーク、機器構成の検討
 - ソリューション選定
 - 製品評価
 - 費用対効果の検討
 - 侵入経路に有効な対策製品の選択

チェックシートあり!

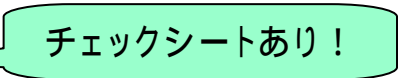

チェックシートあり!

実行(Do)



- **技術的対策**
 - ネットワーク、機器の再構築(必要があれば)
 - ソリューション導入
 - 導入スケジュールの策定
 - テスト環境における試験
 - 本導入
 - ソリューション運用
 - 運用シミュレーション
 - 運用試験 問題の洗い出し 運用方法の見直し
 - 本運用開始
 - 定期的なバックアップ
- **組織的対策**
 - 教育
 - 脅威の意識付け
 - セキュリティポリシーの把握
 - ルール、モラル、エチケット
 - 導入ソリューションのオペレーション教育

見直し (Check)

- 技術的対策
 - 効果測定
 - 確認事項の定量化、定性化による比較
 - セキュリティ3要素の確認
 - 予防、検出、回復
 - セキュリティ3原則の確認
 - 機密性、完全性、可用性
 - 検出ログの集計、分析、比較
 - 機能検査、利用調査、不適合調査(セキュリティ度と利便性)
 - 優先順位と効果の評価
 - ネットワーク、機器構成の再検討
- 組織的対策
 - セキュリティポリシー(ルール)の定期的な確認
 - 履行調査、バランス、不適合の調査
 - ヒアリングによる確認
 - 利用者向け 
 - 管理者向け 

不正プログラム対策10箇条

1. ワクチンソフト、スパイウェアソフトを活用する
2. 対策ソフトのデータベースを常に最新版にする
3. メールソフトのセキュリティ機能を活用し、不審なメールは開かない
 - プレビュー機能、スクリプトの自動実行機能、HTMLメールのオフ
4. メールの添付ファイルは対策ソフトで検査する
5. ダウンロードしたファイルは対策ソフトで検査する
6. OS、アプリケーションを最新にし、セキュリティ機能を活用する
7. 不正プログラム侵入の兆候を検知する
8. データのバックアップを取る
9. 怪しいサイトに注意し、不審なリンクはクリックしない
10. ルータのセキュリティ設定やパーソナルファイアウォールを活用する

- **メールの添付ファイルの拡張子に注意！**

- *.exe *.pif *.scr *.bat *.com
- 二重拡張子、ロングファイル名

対策のまとめ



		侵入方法別				要素別			不正プログラム別						
		インターネット	公衆回線	社内PC	媒体	予防	検知	復旧	ウイルス	ワーム	トロイの木馬	スパイウェア	アドウェア	ハイジャッカー	ボット
デスクトップ / サーバ	ウイルス対策ソフト											×	×	×	
	スパイウェア対策ソフト								×	×					
	パーソナルファイアウォール				×			×	×				×		
	ホスト型IDS/IPS				×			×					×		
	スパム対策ソフト												×		
	URLフィルタリングソフト			×	×			×	×						×
	パッチマネジメント				×			×	×				×	×	
	バックアップ	×	×	×	×	×	×								
	セキュアOS							×	×	×			×	×	
ゲートウェイ / ネットワーク	ウイルス対策ゲートウェイ				×							×	×	×	
	スパイウェア対策ゲートウェイ				×			×	×						
	ネットワークファイアウォール				×			×	×	×	×	×			
	Webアプリケーションファイアウォール				×			×	×		×	×	×	×	
	ネットワーク型IDS/IPS				×			×	×				×		
	スパム対策ソフト				×			×	×				×		×
	URLフィルタリングソフト			×	×			×	×						×
	バックアップ	×	×	×	×	×	×								
	検疫ネットワーク				×			×							



ステップ3

調査と現状把握

現状のセキュリティ対策



		有 / 無	ウイルス	ワーム	トロイの木馬	スパイウェア	アドウェア	ハイジャッカー	ボット
デスクトップ / サーバ	ウイルス対策ソフト					×	×	×	
	スパイウェア対策ソフト		×	×					
	パーソナルファイアウォール		×	×			×		
	ホスト型IDS/IPS		×				×		
	スパム対策ソフト						×		
	URLフィルタリングソフト							×	
	パッチマネージメント		×			×	×		
	バックアップ								
	セキュアOS		×			×	×		
ゲートウェイ / ネットワーク	ウイルス対策ゲートウェイ					×	×	×	
	スパイウェア対策ゲートウェイ		×	×					
	ネットワークファイアウォール		×	×	×	×	×		
	Webアプリケーションファイアウォール		×		×	×	×	×	
	ネットワーク型IDS/IPS		×				×		
	スパム対策ソフト						×		×
	URLフィルタリングソフト							×	
	バックアップ								
	検疫ネットワーク								

侵入経路についてのチェックシート



チェック項目	有 / 無
インターネットの接続がある	
社内LANにダイヤルアップ接続が行える	
モバイルPCを社内LANに接続を行う	
USBメモリ等の外部媒体を使用している	

対策実施状況の確認(1)

利用者向けチェックシート例

チェック項目	有 / 無
対策製品の定義ファイルとチェックエンジンの最新化を実施している	
コンピュータに最新のパッチを適用している	
怪しいサイトの閲覧しないようにしている	
メールソフトのセキュリティ機能を活用し、不審なメールは開かないようにしている - プレビュー機能、スクリプトの自動実行機能、HTMLメールのオフ	
万が一に備えてデータをバックアップしている	
ファイルを開く前にウイルスチェックを行っている	
コンピュータのセキュリティ機能を有効にしている	

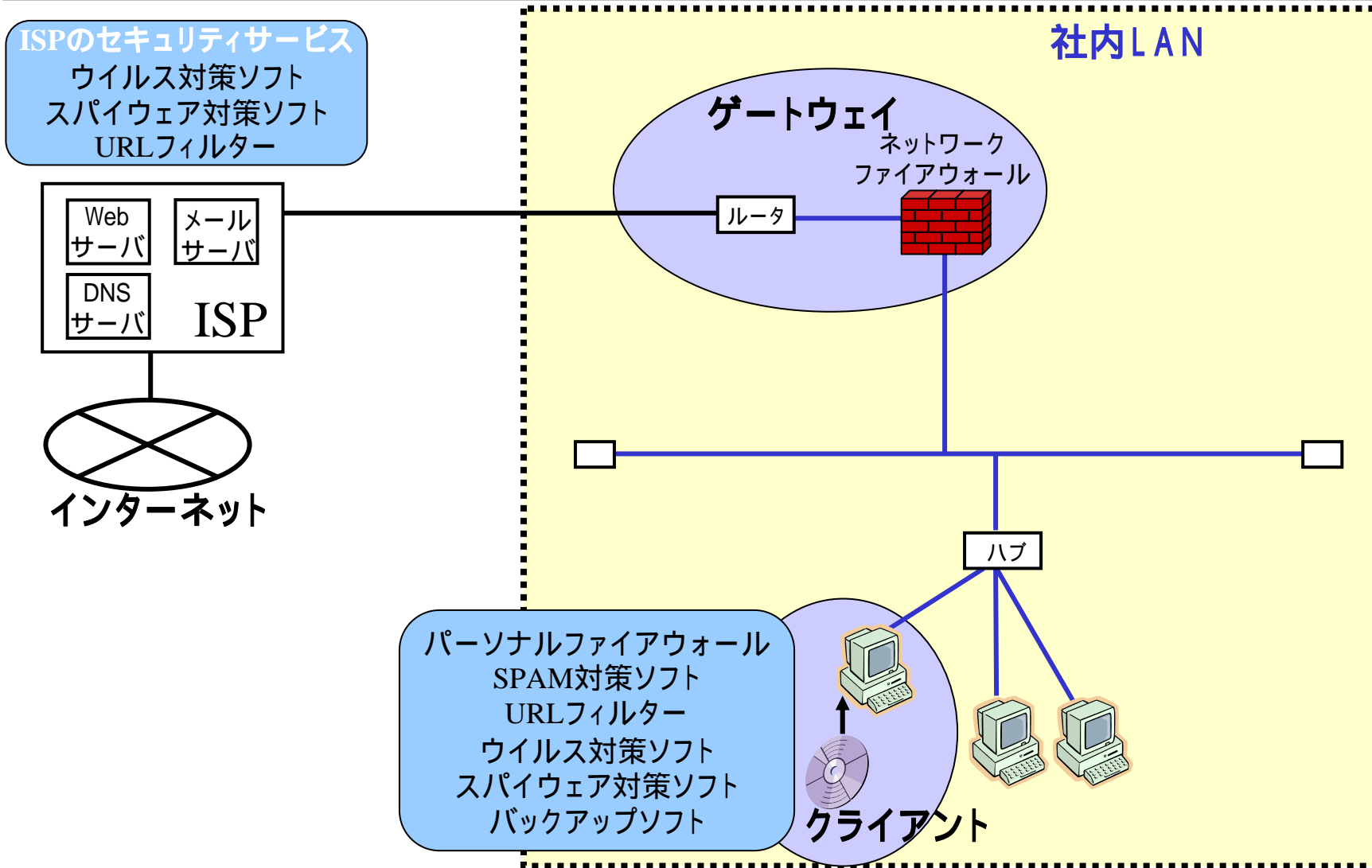
対策実施状況の確認(2)



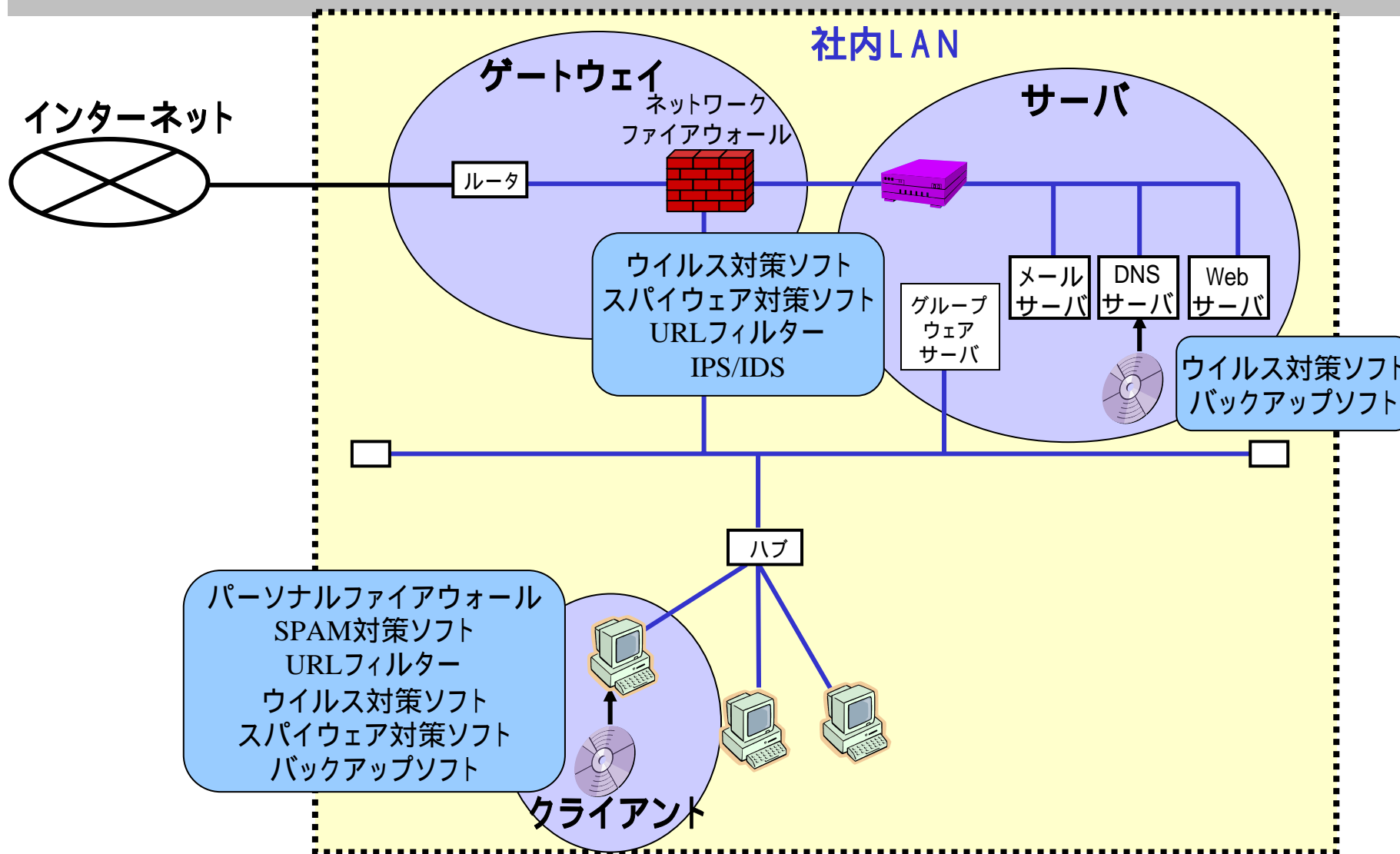
管理者向けチェックシート例

チェック項目	有 / 無
対策製品の検出ログを確認している	
不正プログラムの検出数は減っている	
不正プログラムの感染数は減っている	
必要な対策製品は計画通りに導入されている	
ヘルプデスクなど運用管理体制は整備されている	
対策製品のバージョン管理は行われている	
ユーザへの利用教育は行われている	

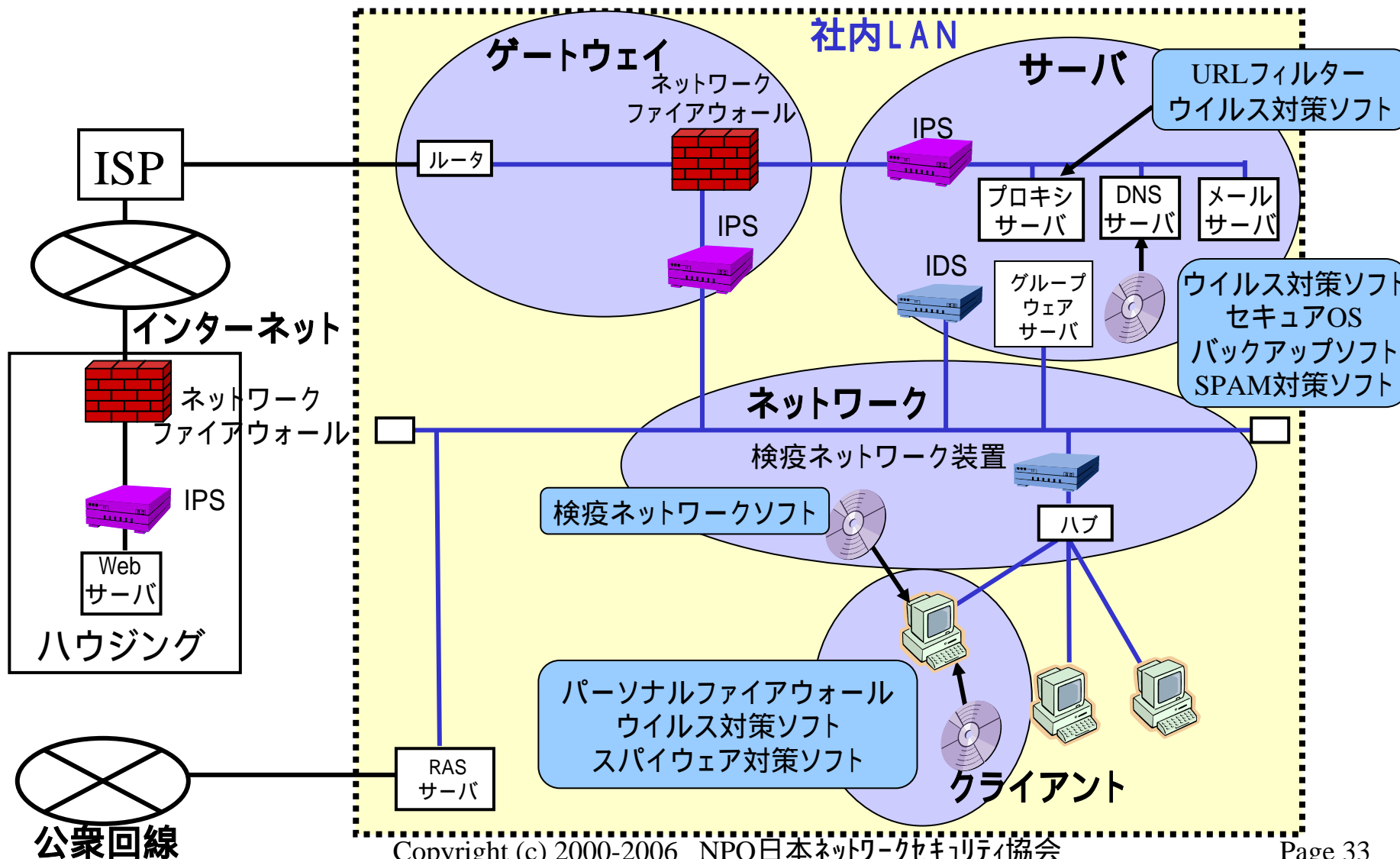
企業規模別対策モデル:小規模



企業規模別対策モデル: 中規模



企業規模別対策モデル: 大規模



• 不正プログラム対策のまとめ

ステップ1 – 理解と認識

不正プログラムについての理解：
各対策製品についての理解：

種類、侵入経路、想定される被害を認識
機能、効果、導入費用、維持管理費用を把握

ステップ2 – 対策の実施と維持

外部からの侵入対策：

問題となる経路について対策実施
費用対効果を見極めた上で対策製品導入
ネットワークの構成変更、セキュリティルール策定

機器に施す対策：

保護対象とすべき機器(端末)への対策実施
費用対効果を見極めた上で対策製品導入
機器(端末)の構成変更

維持管理対策：

維持管理対策の策定と実施
セキュリティポリシーの定期的な見直し
定期的なバックアップ
システム管理者/ユーザーの管理と教育

ステップ3 – 調査と現状把握

侵入経路についての現状把握：

社内LANへの侵入が想定される経路の洗い出し

社内LANについての現状把握：

ネットワーク構成/機器の配備状況の再確認

保護対象機器についての現状把握：

資産価値あるいは損害額の試算

方針・管理体制についての現状把握：

セキュリティに対する方針、管理ルールや体制の再確認

WGメンバー紹介

- 石川 章史 (Akifumi Ishikawa)
株式会社ぷららネットワークス
ネットワーク管理部
- 井澤 誠 (Makoto Izawa)
株式会社マイクロ総合研究所
ストラテジック・マーケティング・グループ
- 迫田 肇 (Hajime Sakoda)
富士通サポート&サービス株式会社
サービスビジネス本部
- 竹内 清史 (Kiyofumi Takeuchi)
三菱電機株式会社
情報技術総合研究所
- 西野 一行 (Kazuyuki Nishino)
株式会社ニコンシステム
管理本部 企画部
- 松尾 竹純
日商エレクトロニクス株式会社
セキュリティ事業部
- ピョー ナイントオン (Phyo Naing Tun)
株式会社アークン
R&D事業本部
- 与那原 亨 (Akira Yonahara)
NTTデータ株式会社
- 渡部 章 (Akira Watanabe)
株式会社アークン

(敬称略、順不同)



•成果物の取扱いについて

成果物の著作権、使用等の権利は、著者及びJNSAとの共有とします。引用した文章、図表についての著作権は各作成者にあります。この成果物の配布、複製、修正につきましては、JNSA事務局までお問い合わせください。