Nish!gaki Laboratory

ワーム検知技術の提案と情報漏洩防止への活用

名坂 康平　静岡大学情報学部
酒井 崇裕　静岡大学大学院情報学研究科
山本 匠　静岡大学創造科学技術大学院
西垣 正勝　静岡大学創造科学技術大学院

Nish!gaki Laboratory

背景

- マルウェアの脅威
  - システムの異常
  - 他への感染
  - スパムメール
  - DoS
  - 情報漏えい

→ 様々な事件・事故の原因に

マルウェアの検知技術の研究は大変重要

背景

Nish!gaki Laboratory

- マルウェアの検知技術の精度を上げることは重要
- 感染を防ぐという当然の使い方以外の使い方を考えることで、新しい価値を生み出すことが出来るかもしれない

発想のヒント　（オズボーンのチェックリスト）		
他の使い道はないか？	応用はできないか？	何かを変更はできないか
何かを拡大できないか？	何かを縮小できないか？	何かを代用できないか？
何かを変更できないか？	何かを逆さにできないか？	何かを組合せできないか？

発表内容

Nish!gaki Laboratory

- マルウェア検知技術
  - 自己ファイルREADの検出による未知ワーム検知方式の提案
- マルウェア検知技術の別の利用方法
  - アンチウイルスソフトを活用した機密情報漏洩防止方式の提案

Nish!gaki Laboratory

自己ファイルREADの検出による未知ワーム検知方式の提案

Nish!gaki Laboratory

背景

- 近年のワームの傾向
  - セキュリティホールの出現からワームの登場までの期間が非常に短い
    - 定義ファイルの更新が間に合わない
  - セキュリティホール公開前にワームが登場
    - 未知のセキュリティホールを突く，ゼロデイアタックの存在

未知ワーム対策の必要性が増加

従来のワーム検知手法 ～パターンマッチング法～

Nish!gaki Laboratory

- 現在のアンチウィルスソフトの主流
  - 既知ワーム検知にあたり，簡素かつ確実
- 最近のワームの傾向
  - セキュリティホールの発見から新種のワームの登場までの期間が短い
  - アンチウィルスベンダーの提供するウィルスパターンファイルの更新が間に合わない
  - セキュリティホールが広く公表される前にその脆弱性を突くワームの出現
  - 多様な亜種ワームが次々に作成される
  - ポリモーフィック型ワームやメタモーフィック型ワームなどの存在

従来の未知ワーム検知手法 ～ビヘイビアブロッキング法～

Nish!gaki Laboratory

- 「ワームらしさ」を検知する手法
  主に以下の項目が見られてきた
  - レジストリ改ざん
  - システムファイル書換
  - etc

上記の項目を見ることでワーム検知が可能

従来の未知ワーム検知手法 ～ビヘイビアブロッキング法～

Nish!gaki Laboratory

- 誤検知が多い
  - – レジストリ改ざん
    - インストーラ，各種アプリケーションによるレジストリの変更
  - – システムファイル書換
    - インストーラによるランタイムライブラリの書換やWindows Updateによるシステムファイルの更新

「ワームらしさ」を規定することが困難である

真の「ワームらしさ」の規定

Nish!gaki Laboratory

①ネットワークを介して他のPCに感染
- – 自己複製

②システム以下へのコピー
- – レジストリ登録、ファイルの隠蔽など

③暗号化や難読化
- – コードの改変、圧縮

正規プログラムを誤検知することなくワームを検知できる規定とは何なのだろうか？

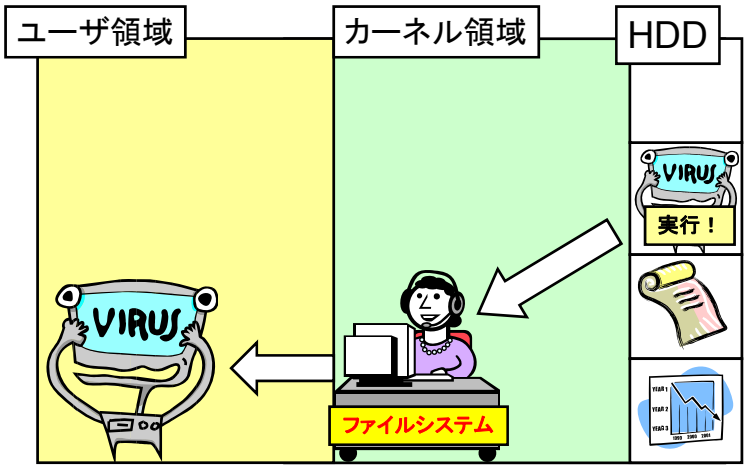
真の「ワームらしさ」の規定
①ネットワークを介して他のPCに感染

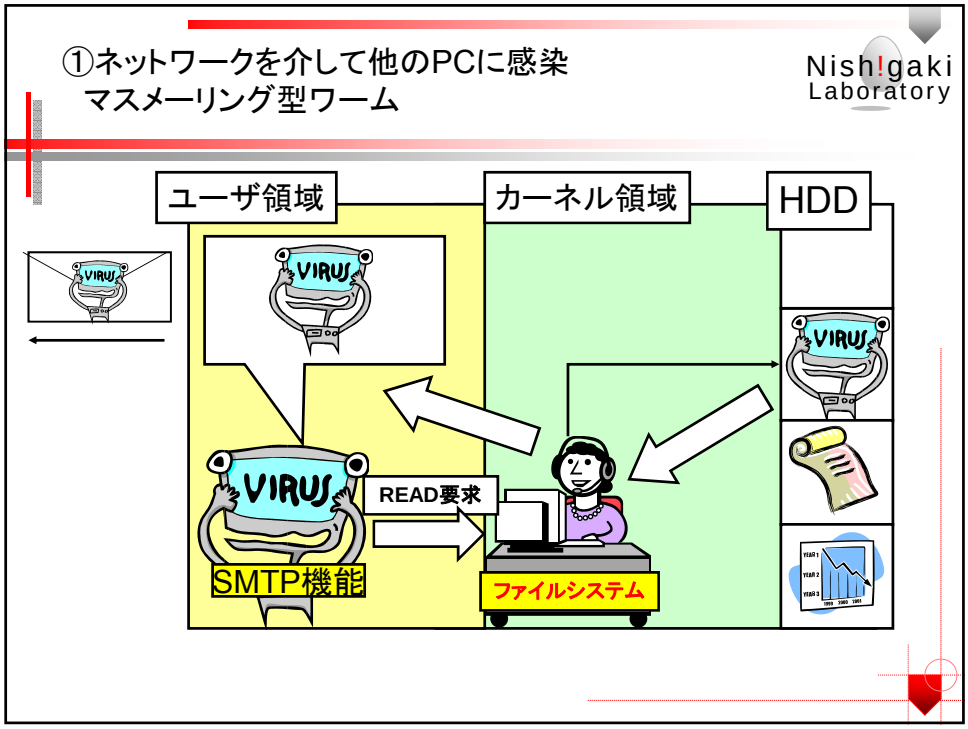
Nish!gaki Laboratory

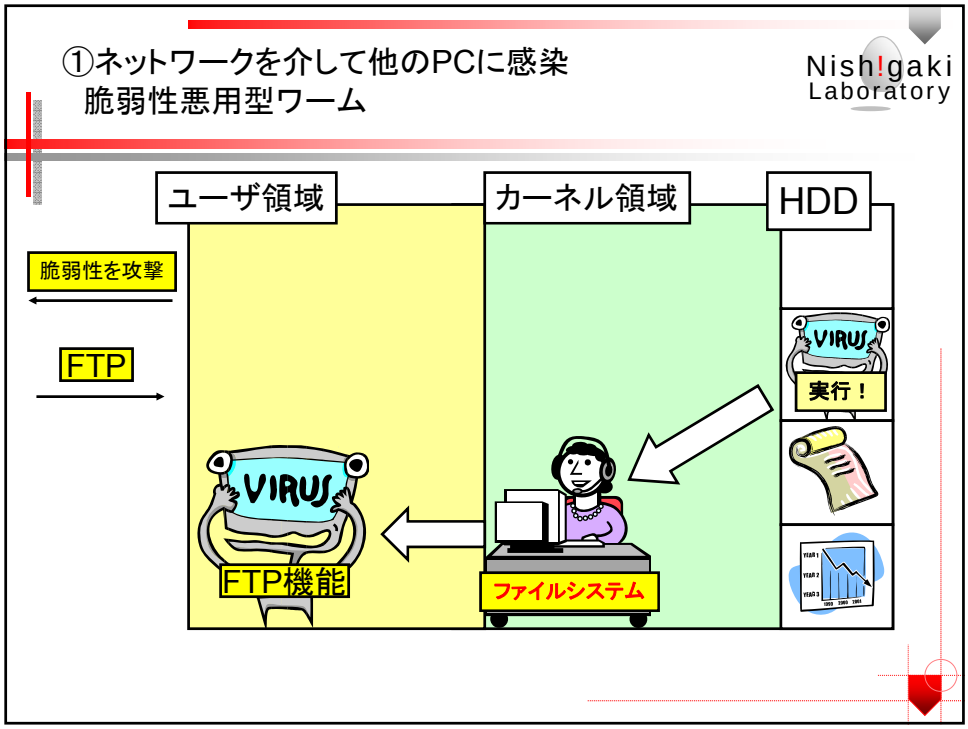
1. コピー元ファイルをREADする
2. 通信用APIにREADしたデータをWRITEする
3. ネットワークを経由して他のPCに感染
   - マスメーリング型ワーム
   - 脆弱性悪用型ワーム

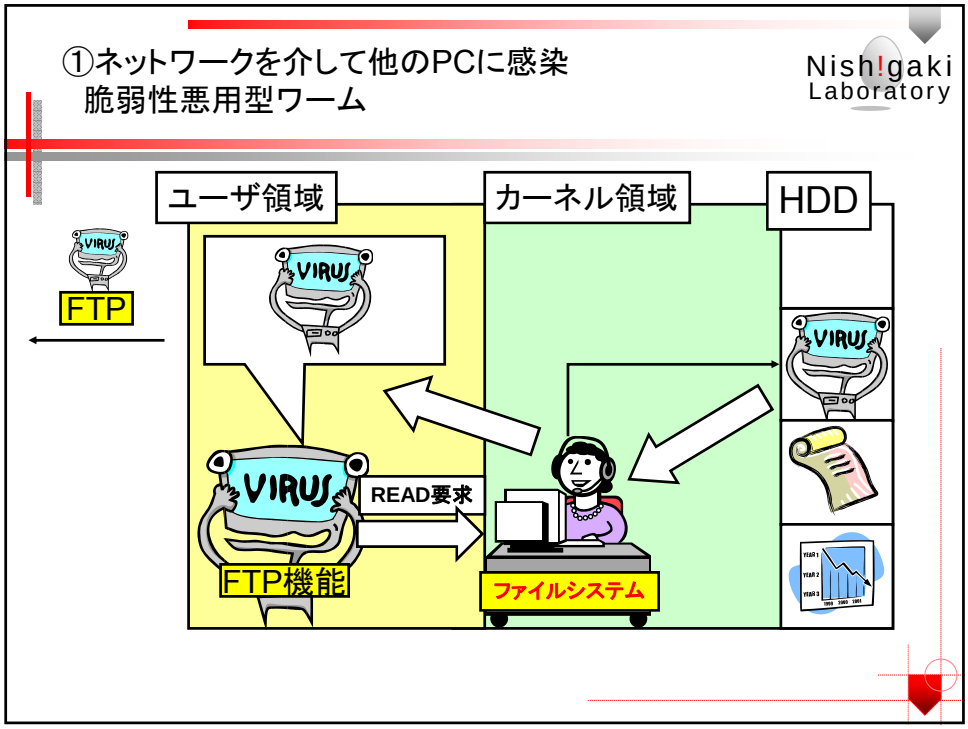
①ネットワークを介して他のPCに感染
マスメーリング型ワーム

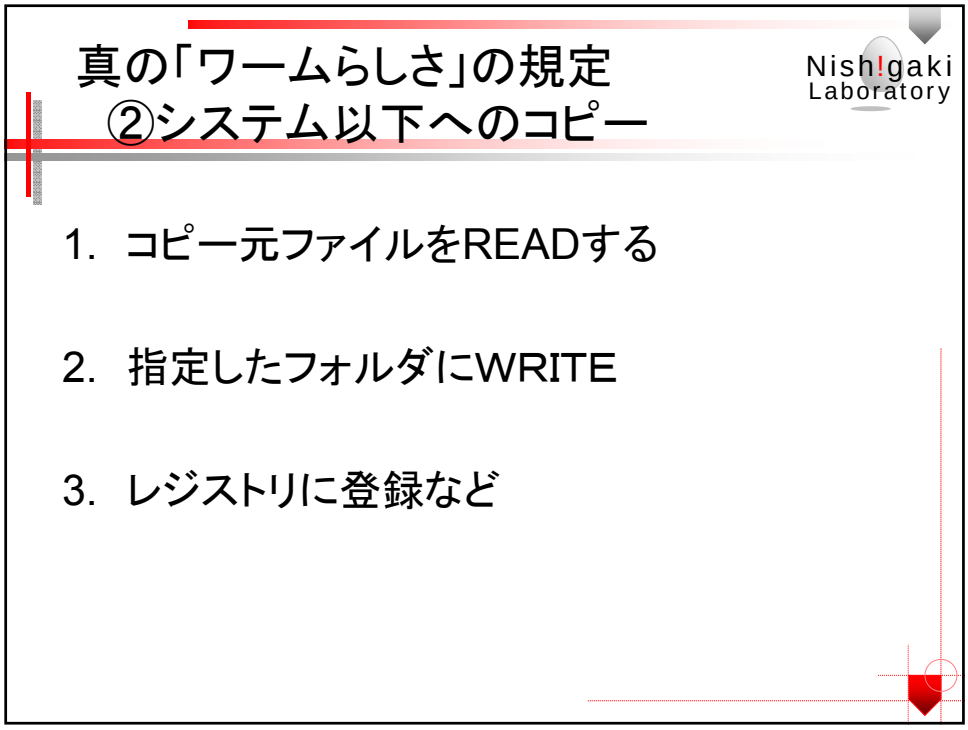
Nish!gaki Laboratory




①ネットワークを介して他のPCに感染
マスメーリング型ワーム
Nish!gaki
Laboratory
ユーザ領域
カーネル領域
HDD
VIRUS
READ要求
SMTP機能
ファイルシステム

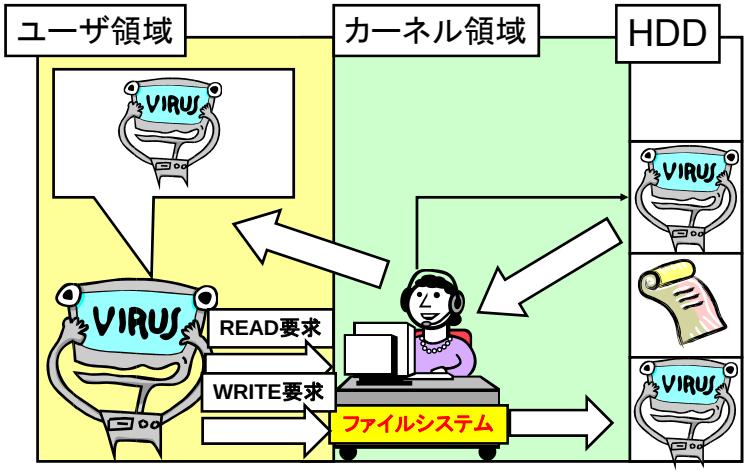

①ネットワークを介して他のPCに感染
脆弱性悪用型ワーム
Nish!gaki
Laboratory
ユーザ領域
カーネル領域
HDD
脆弱性を攻撃
FTP
VIRUS
実行！
FTP機能
ファイルシステム


①ネットワークを介して他のPCに感染
脆弱性悪用型ワーム
Nish!gaki Laboratory
ユーザ領域
カーネル領域
HDD
VIRUS
FTP
READ要求
FTP機能
ファイルシステム


真の「ワームらしさ」の規定
②システム以下へのコピー
Nish!gaki Laboratory
1. コピー元ファイルをREADする
2. 指定したフォルダにWRITE
3. レジストリに登録など

②システム以下へのコピー

Nish!gaki Laboratory



真の「ワームらしさ」の規定　③暗号化、難読化

Nish!gaki Laboratory

- 変異型ワーム
  - ポリモーフィック型
    - 感染するたびに自分自身をランダムな暗号化コードを使用して暗号化する
  - メタモーフィック型
    - プログラムの順番を変更したり、同じ動作をする別のコードに自分自身を書き換えたりと、全く別のプログラムを装い難読化する

③変異型ワームの自己複製

Nish!gaki Laboratory

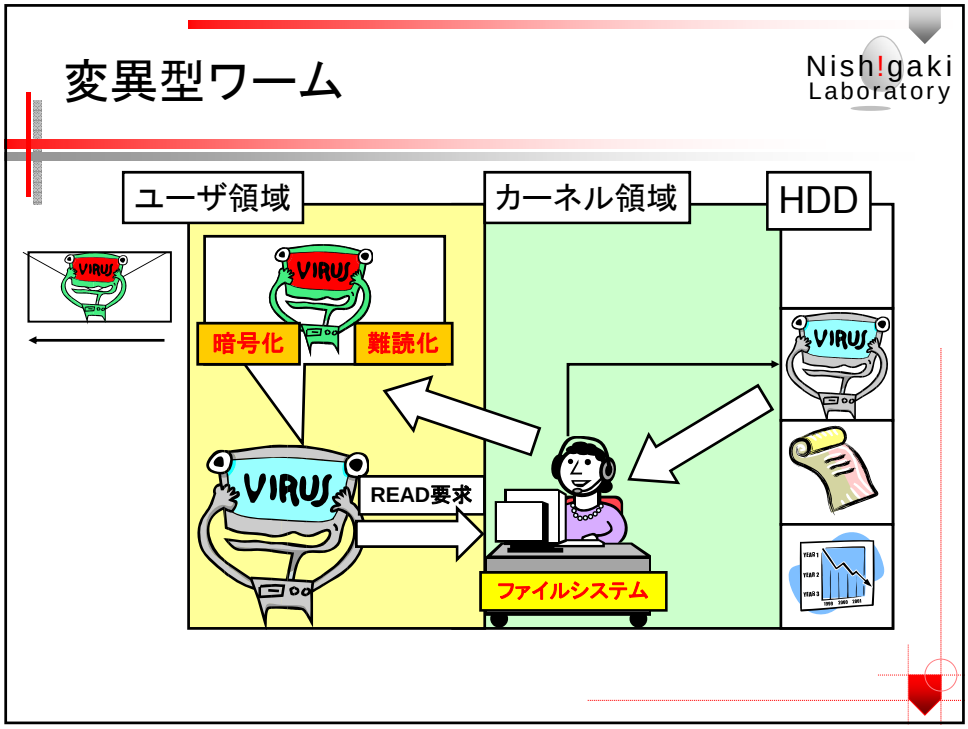
1. コピー元ファイルをREADする
2. 通[illegible]ITEする
3. ネット[illegible]染
   - マスメーリング型ワーム
   - 脆弱性悪用型ワーム

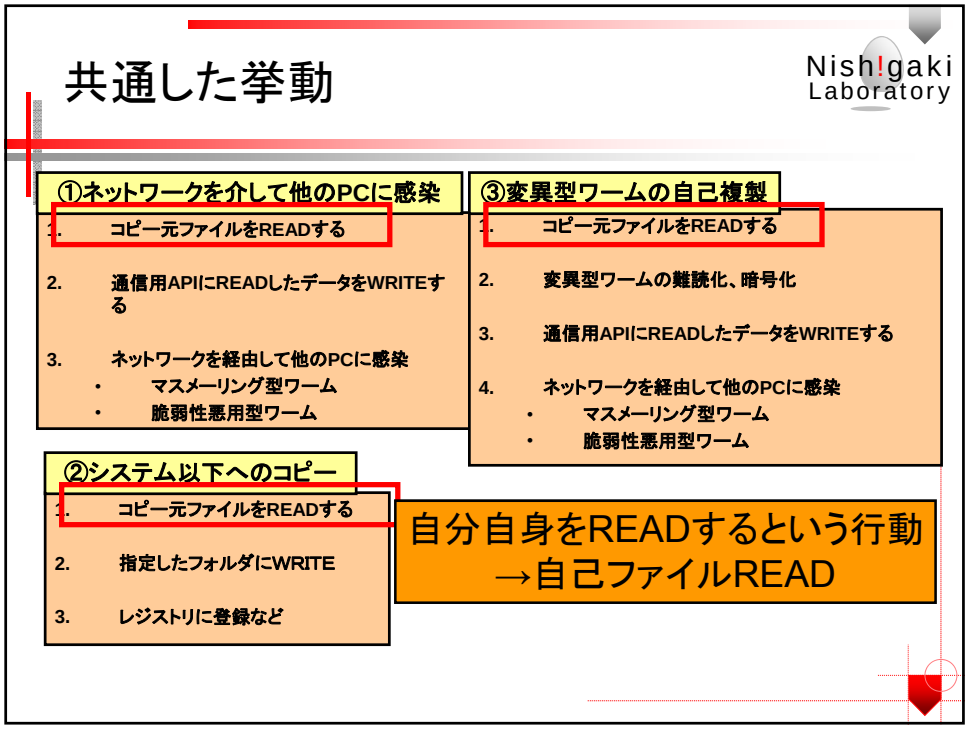
変異型ワームの難読化、暗号化が行われると考えられる

③変異型ワームの自己複製

Nish!gaki Laboratory

1. コピー元ファイルをREADする
2. **変異型ワームの難読化、暗号化**
3. 通信用APIにREADしたデータをWRITEする
4. ネットワークを経由して他のPCに感染
   - マスメーリング型ワーム
   - 脆弱性悪用型ワーム


変異型ワーム
Nish!gaki
Laboratory
ユーザ領域
カーネル領域
HDD
VIRUS
暗号化
難読化
READ要求
ファイルシステム


共通した挙動
Nish!gaki
Laboratory
①ネットワークを介して他のPCに感染
1. コピー元ファイルをREADする
2. 通信用APIにREADしたデータをWRITEする
3. ネットワークを経由して他のPCに感染
・ マスメーリング型ワーム
・ 脆弱性悪用型ワーム
②システム以下へのコピー
1. コピー元ファイルをREADする
2. 指定したフォルダにWRITE
3. レジストリに登録など
③変異型ワームの自己複製
1. コピー元ファイルをREADする
2. 変異型ワームの難読化、暗号化
3. 通信用APIにREADしたデータをWRITEする
4. ネットワークを経由して他のPCに感染
・ マスメーリング型ワーム
・ 脆弱性悪用型ワーム
自分自身をREADするという行動
→自己ファイルREAD

自己ファイルREAD

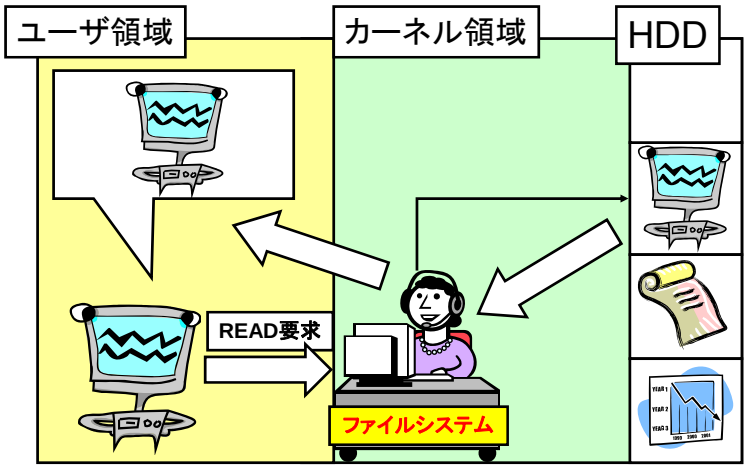
Nish!gaki Laboratory

- 自己ファイルREADはワームだけがする行動なのであろうか？
  →自分自身を必要とする正規のプログラムは少ないと考えられる

ただし、正規プログラムであっても
自分自身をREADするものがないわけではない

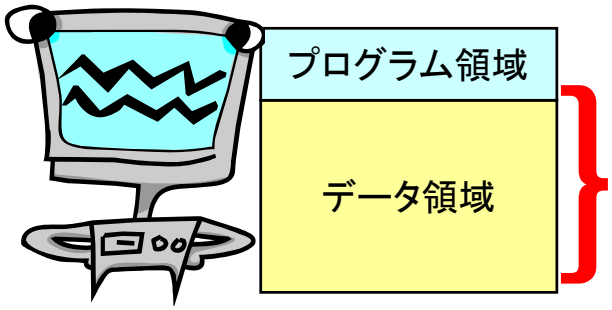
自己ファイルREAD インストーラ

Nish!gaki Laboratory



インストーラ

Nish!gaki Laboratory



READされるデータは通常のインストーラでは
ファイルのデータ領域だけである

自己ファイルREAD

Nish!gaki Laboratory

- ワーム
  - 他のPCへの自己複製のために自分自身のファイルのすべてをREADする
- 正規のプログラム
  - 自分自身のファイルをすべてREADすることはない

自分自身のファイルのすべてをREADするという挙動を
自己ファイルREADと定義し、
自己ファイルREADの検出による未知ワーム検知

提案方式

Nish!gaki Laboratory

- 自己ファイルREADの検出による未知ワーム検知方式の提案
  - 実行プログラムとREADされるファイルのパスの相関
  - 実行プログラムとREADされるデータの一致

OSのファイルシステムを監視することにより，リアルタイムで検知可能

提案方式（検知アルゴリズム）

Nish!gaki Laboratory

Step1. PC内で発生したすべてのファイルアクセスをフックする.

Step2. ファイルアクセスの中でREADに関するもののみを検出する.

Step3. Step2で検出したファイルアクセスを発生させたプロセスのパスと，アクセスするファイルのパスの相関をチェックする.

Step4. Step3で検出したプロセスがプロセス自身のファイル（の大部分）をREADしていた時，そのファイルをワームの疑いありと判断する.

基礎実験

Nish!gaki Laboratory

- Windows上のファイルアクセスのリアルタイム監視可能なモニタツールであるFileMonを用いての有効性の評価
  - 既知ワームを用いて検知実験
  - 正規プログラムを用いた誤検知実験

検知実験

Nish!gaki Laboratory

- 既知ワームを用いてワームのファイルアクセスを観測
- 実験に用いたワーム
  - マスメーリング型
    - Beagle.X, Netsky.B, Netsky.D
    - Netsky.Z（圧縮型）, Beagle.AG（鍵付き圧縮型）
    - Mimail.Q（自己変異型）
  - 脆弱性悪用型
    - Blaster.C
    - Sasser.C

実験結果

Nish!gaki Laboratory

名前	型	ブロックREAD	シーケンシャルREAD
Sasser.C	脆弱性悪用型	×	○
Blaster.C	脆弱性悪用型	○	×
Beagle.X	メール送信型	×	○
Netsky.B	メール送信型	○	×
Netsky.D	メール送信型	○	○
Netsky.Z	メール送信型 圧縮型	○	×
Beagle.AG	メール送信型 鍵付き圧縮型	○	×
Mimail.Q	メール送信型 自己変異型	○	○

誤検知実験

Nish!gaki Laboratory

- 正規プログラムのファイルアクセスを観測し、自分自身のファイルがREADされるかを測定
- 実験に用いた正規プログラム
  - MS WORD
  - MS EXCEL
  - インストーラ
  - Internet Explorer

実験結果

Nish!gaki Laboratory

名前	自己ファイルREAD（部分的）	（すべて）	誤検知
MS WORD	×	×	×
MS EXCEL	×	×	×
インストーラ	○	×	×
Internet Explorer	○	×	×

誤検知に関する考察

Nish!gaki Laboratory

- インストーラは自分自身のファイルの一部のみをREAD
- Internet Explorerは自分自身のファイルの1%未満の割合のREAD
  - バージョン情報の確認

考察

Nish!gaki Laboratory

- ワーム
  - 二つの形で自分自身のファイルへのREADが観測されたがいずれの場合も自己ファイルREADを行っていた
- 正規プログラム
  - 自分自身のファイルへのREADは観測されたが、READされるのはファイルの一部であった

READされたデータと全体のファイルの割合をチェックすることで切り分けが可能

考察（自己ファイルREADの拡張）

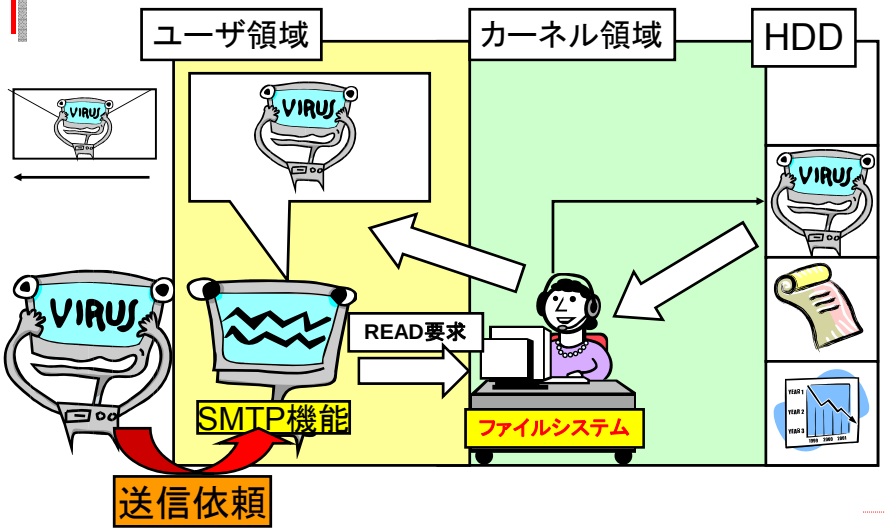
Nish!gaki Laboratory

他のアプリケーションの機能を利用して感染するタイプのワームに関しては自己ファイルREADの検出では検知できない

- 既存のメーラを用いて（メーラに寄生して）メール感染を行うワーム（ウィルス）

考察
（自己ファイルREADの拡張）

Nish!gaki Laboratory



考察
（自己ファイルREADの拡張）

Nish!gaki Laboratory

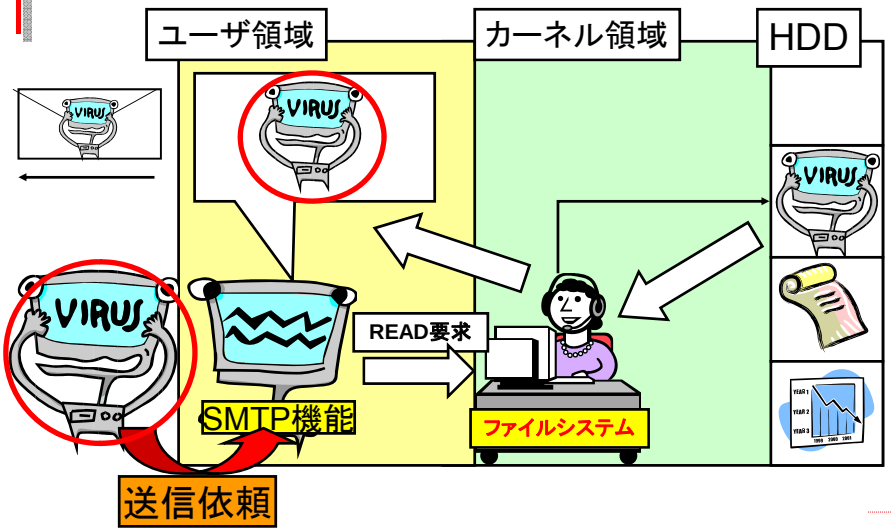
他のアプリケーションの機能を利用して感染するタイプのワームに関しては自己ファイルREADの検出では検知できない

– 既存のメーラを用いて（メーラに寄生して）メール感染を行うワーム（ウィルス）

他のプログラムを媒介とした自己自身のREADも自己ファイルREADであるとみなすという拡張をすることで解決する

考察
（自己ファイルREADの拡張）

Nish!gaki Laboratory



考察

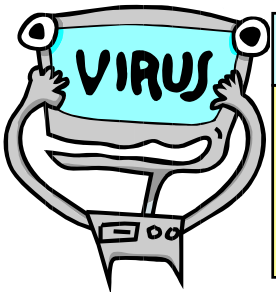
Nish!gaki Laboratory

- 本方式が普及した場合，ワームが本方式で検知されないようにする可能性がある
  - 自分自身のデータに必要のないデータを追加し，自己READの割合を減らす

正規プログラムとワームの自己READの割合以外の切り分けが必要となる

考察

Nish!gaki Laboratory



プログラム領域

データ領域

プログラム領域をREADしているという情報を用いる
プログラムのエントリーポイントを監視する

まとめ

Nish!gaki Laboratory

- ワーム検知の規定を行い，自己のファイルREADを見ることにより未知ワーム・変異型ワームの検知を行う方法を提案した
- 検知および誤検知についての評価を行った
- 従来，検知が難しいとされていた，変異型ワームの検知も可能であることがわかった

今後の課題

Nish!gaki Laboratory

- 本システムの実装
- 実装したシステムを用いた検知率、誤検知率の計測
- リアルタイム検知を行った場合のオーバーヘッドの計測

Nish!gaki Laboratory

アンチウイルスソフトを活用した機密情報漏洩防止方式

西垣研究室

背景

Nish!gaki Laboratory

- P2Pソフトによる顧客情報・内部資料といった機密情報の漏洩が増加
  - セキュリティに無頓着な人が、企業の機密情報を私物パソコンに持ち出す
  - Antinnyのような暴露ウイルスに感染し、機密情報がP2Pネットワーク上に流出

背景

Nish!gaki Laboratory

- P2Pネットワーク上に機密情報が流出
  - P2Pネットワーク全体に拡散
  - P2Pネットワーク上から削除することは困難

P2Pネットワークにおける
情報漏洩対策が必要

提案方式のコンセプト

Nish!gaki Laboratory

- P2Pネットワークといえども、全員が機密情報を流出してしまうセキュリティに無頓着な人ではない（どちらかというと、そのような人は少数）

- 残りのセキュリティを意識している人たちで機密情報の拡散を止められないか

提案方式のコンセプト

Nish!gaki Laboratory

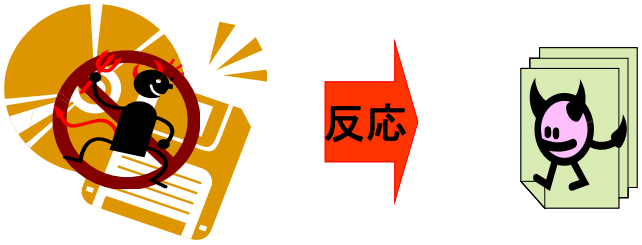
- セキュリティを意識している人たちはアンチウイルスソフトを導入している
  - ウイルスに反応
  - ウイルス入りのデータを自動的に削除

ウイルスがアンチウイルスソフトに
削除されることを利用する

提案方式

Nish!gaki Laboratory

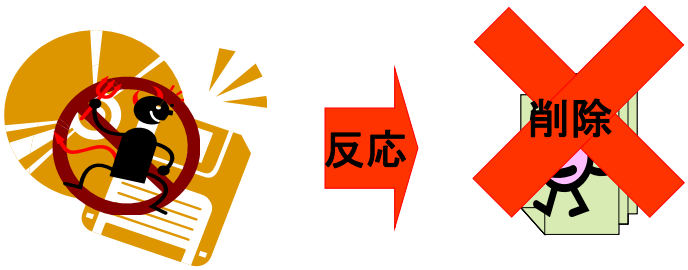
- 機密情報にアンチウイルスソフトに反応するウイルスの特徴パターンを埋め込む



提案方式

Nish!gaki Laboratory

- 機密情報が流出しても、アンチウイルソフトが削除してくれる

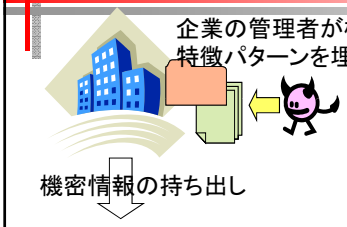


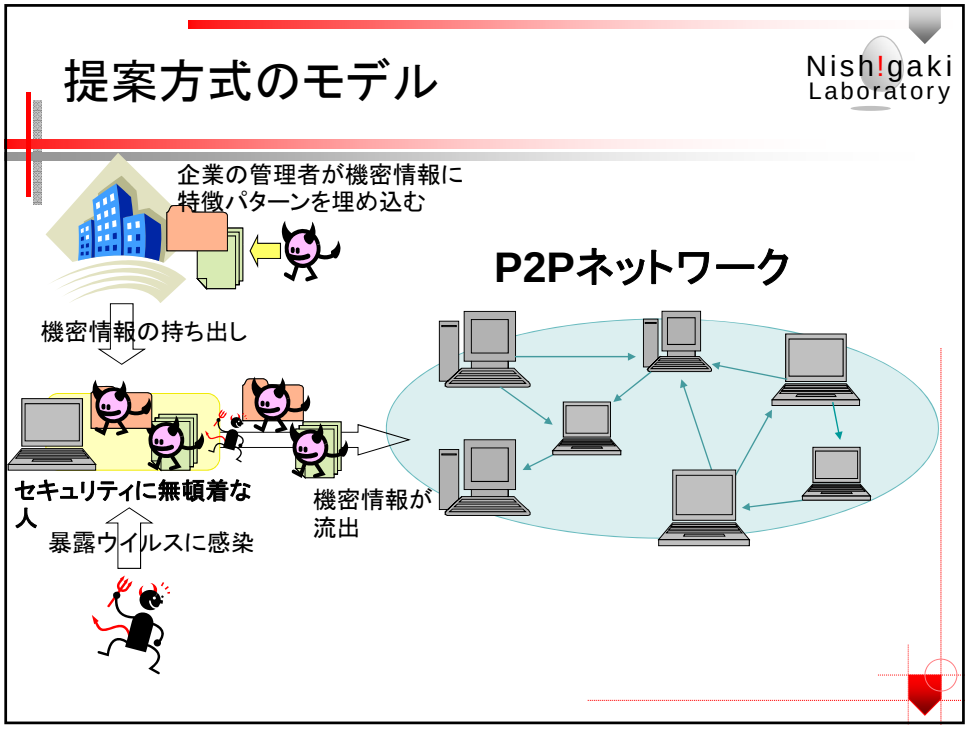
提案方式のモデル

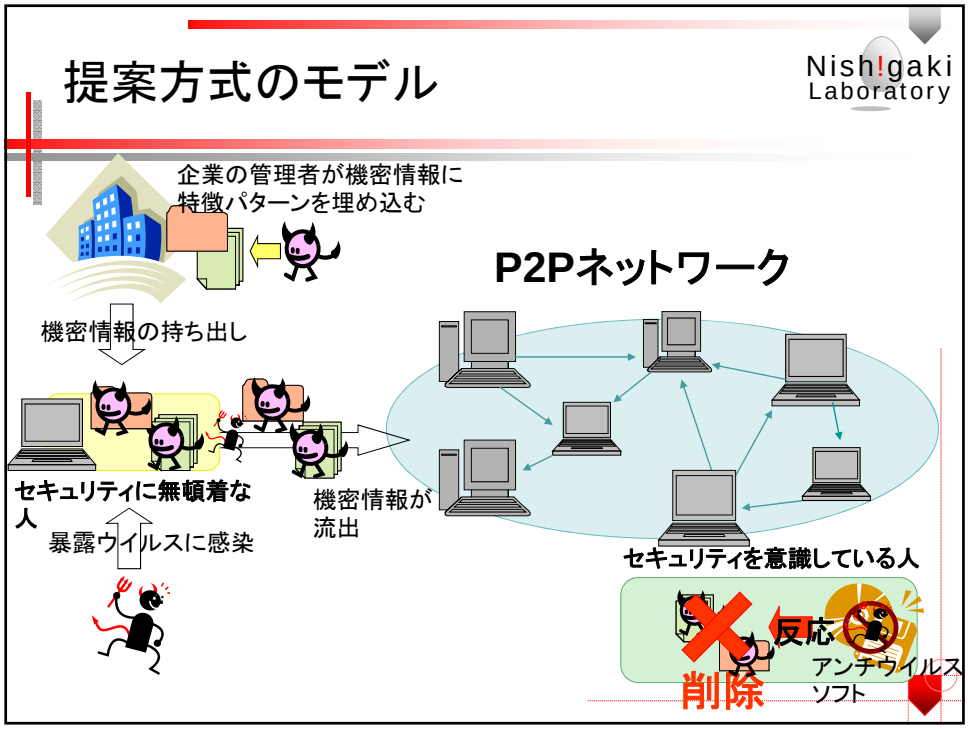
Nish!gaki Laboratory

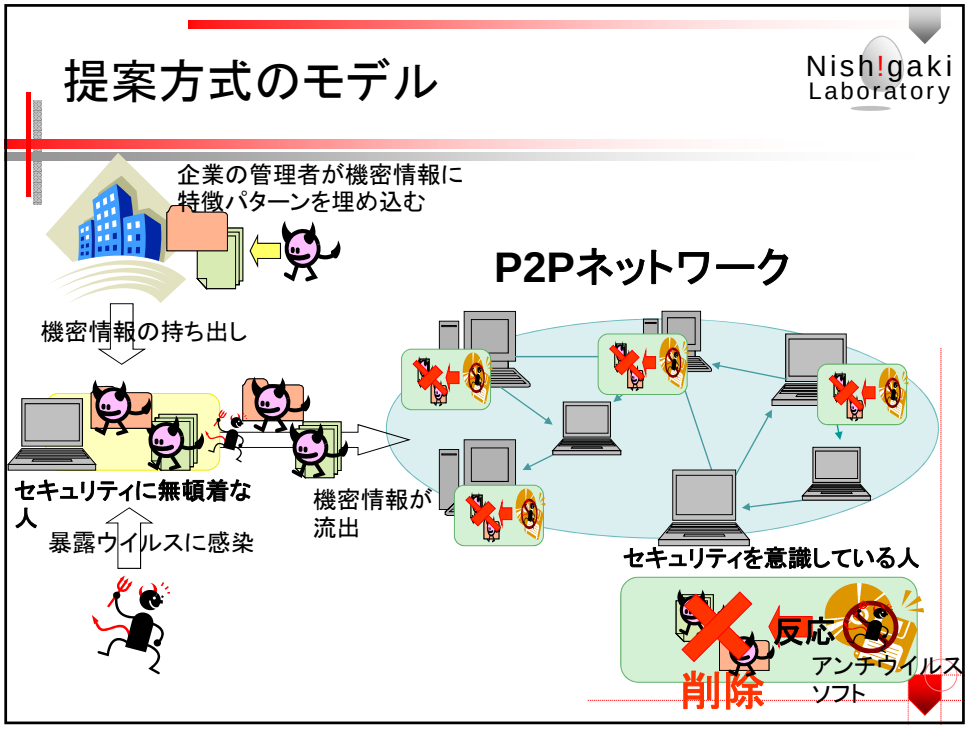
提案方式のモデル

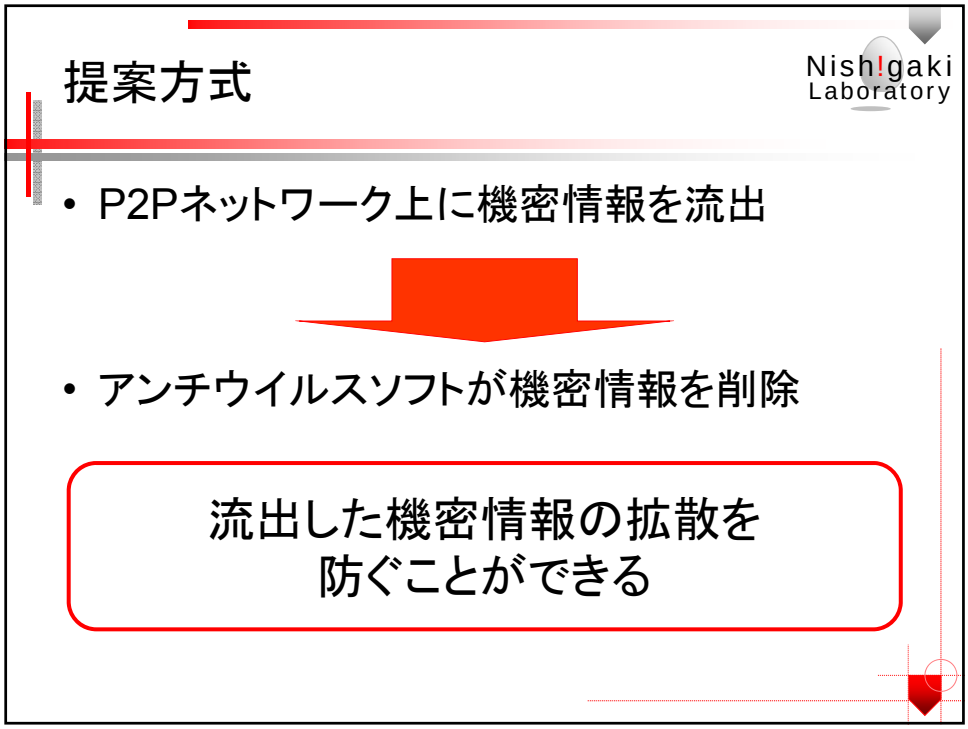
Nish!gaki Laboratory




提案方式のモデル
Nish!gaki
Laboratory
企業の管理者が機密情報に
特徴パターンを埋め込む
P2Pネットワーク
機密情報の持ち出し
セキュリティに無頓着な
人
機密情報が
流出
暴露ウイルスに感染


提案方式のモデル
Nish!gaki
Laboratory
企業の管理者が機密情報に
特徴パターンを埋め込む
P2Pネットワーク
機密情報の持ち出し
セキュリティに無頓着な
人
機密情報が
流出
暴露ウイルスに感染
セキュリティを意識している人
反応
削除
アンチウイルス
ソフト

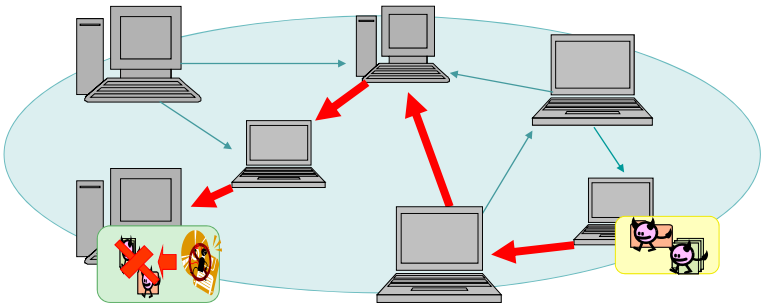

提案方式のモデル
Nish!gaki Laboratory
企業の管理者が機密情報に特徴パターンを埋め込む
P2Pネットワーク
機密情報の持ち出し
セキュリティに無頓着な人
暴露ウイルスに感染
機密情報が流出
セキュリティを意識している人
反応
削除
アンチウイルスソフト


提案方式
Nish!gaki Laboratory
• P2Pネットワーク上に機密情報を流出
• アンチウイルスソフトが機密情報を削除
流出した機密情報の拡散を
防ぐことができる

考察（1）

Nish!gaki Laboratory

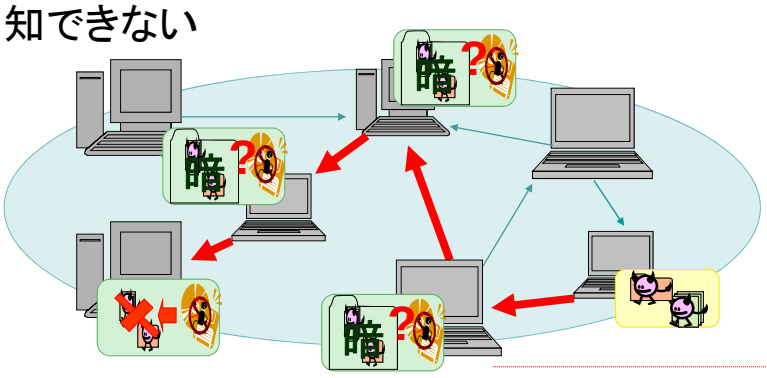
- アンチウイルスソフトを導入されていれば、漏洩した機密情報をダウンロードしたピアでは当該ファイルがされるが・・・



考察（1）

Nish!gaki Laboratory

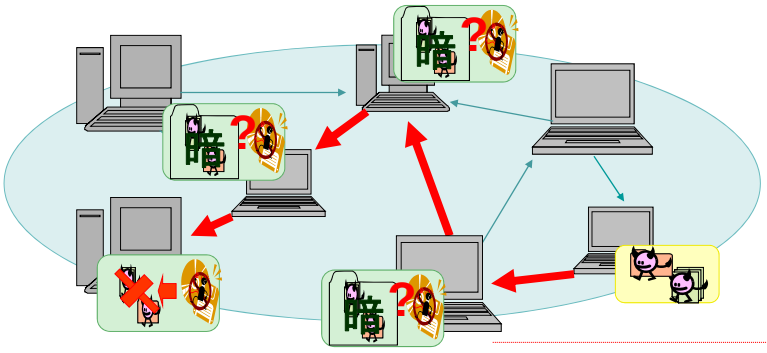
- 当該ファイルは経路中のピアの共有フォルダにもコピーされており、かつ、そのファイルは暗号化されているため、アンチウイルスソフトでは検知できない



考察（1）

Nish!gaki Laboratory

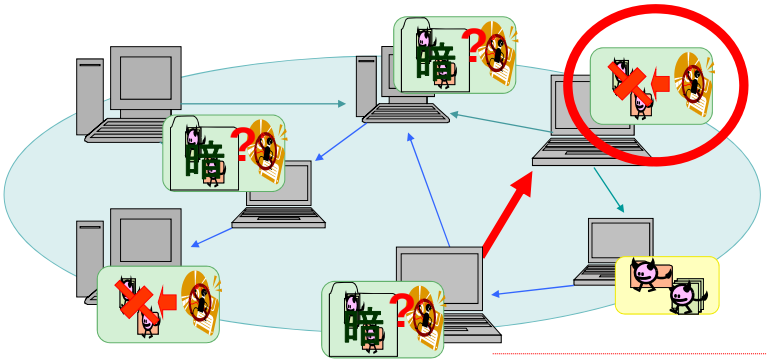
- しかし、暗号化されている状態のファイルは誰も読めないので、実害はない



考察（1）

Nish!gaki Laboratory

- 誰かが中継ピアから当該ファイルを（読もうと思って）ダウンロードした時点で、暗号は解かれ、アンチウイルスソフトに検知される



考察（1）

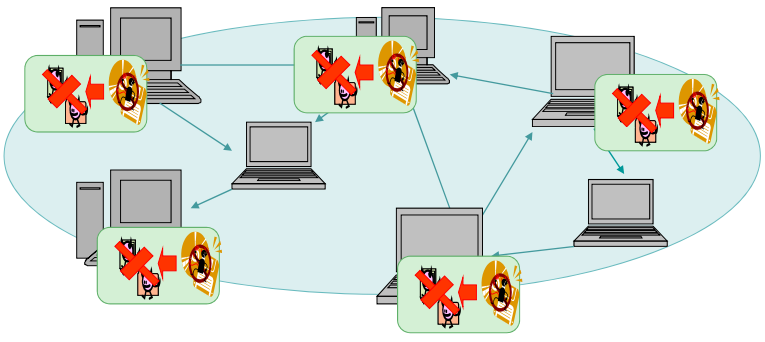
Nish!gaki Laboratory

- ただし、
  - 共有フォルダ内を復号した上で検知する機能を有するアンチウイルスソフトがあれば、中継ピアの共有フォルダ内の機密ファイルを削除できる
  - P2P通信パケットを復号してウイルスチェックする機能を有するアプリケーションゲートウエイを通信事業者が提供すれば、通信路上で機密ファイルを削除できる

考察（2）

Nish!gaki Laboratory

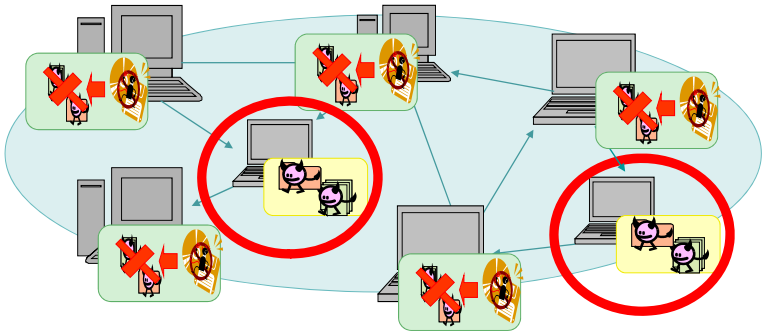
- アンチウイルスソフトを導入しているピアでは削除されるが・・・



考察（2）

Nish!gaki Laboratory

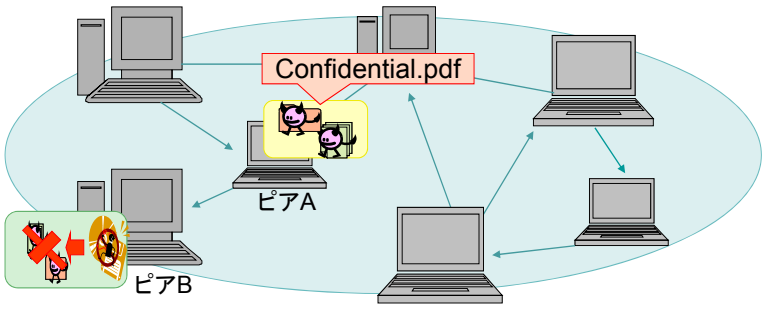
- アンチウイルスソフトを導入してない、セキュリティに無頓着な人への機密情報の漏洩は防げない



考察（2）

Nish!gaki Laboratory

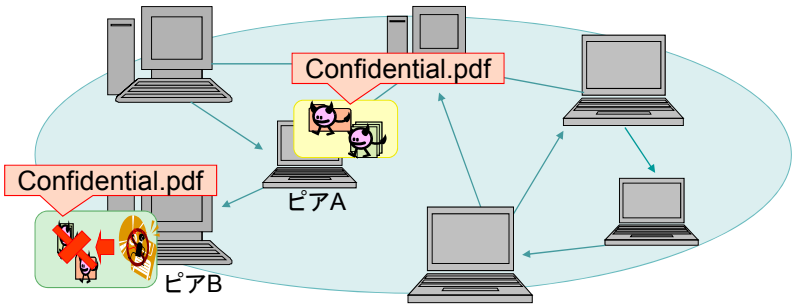
①アンチウイルスソフトを導入していないピアAから機密情報「Confidential.pdf」が漏洩



考察（2）

Nish!gaki Laboratory

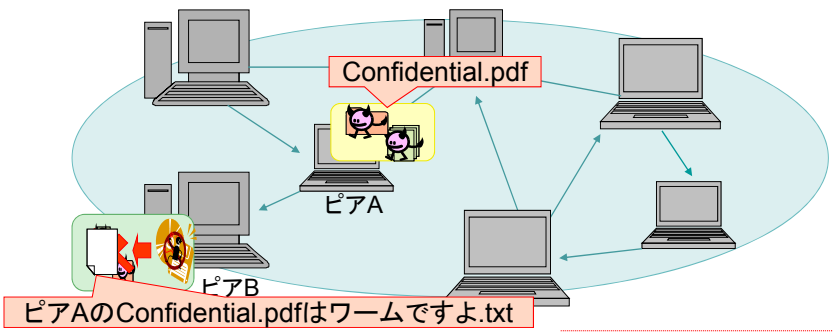
②アンチウイルスソフトを導入しているピアBが当該ファイルをダウンロードしたところ、アンチウイルスソフトが反応した



考察（2）

Nish!gaki Laboratory

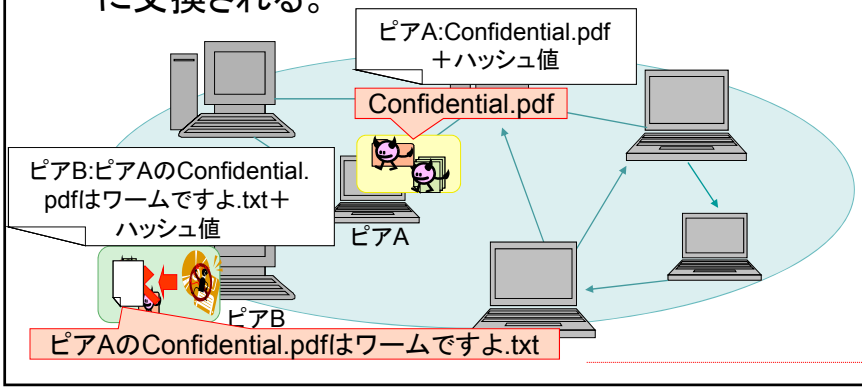
③ピアBの共有フォルダ内の当該ファイルを削除し、「ピアAのConfidential.pdfはワームですよ.txt」という名前のファイルを共有フォルダに追加する



考察(2)

Nish!gaki Laboratory

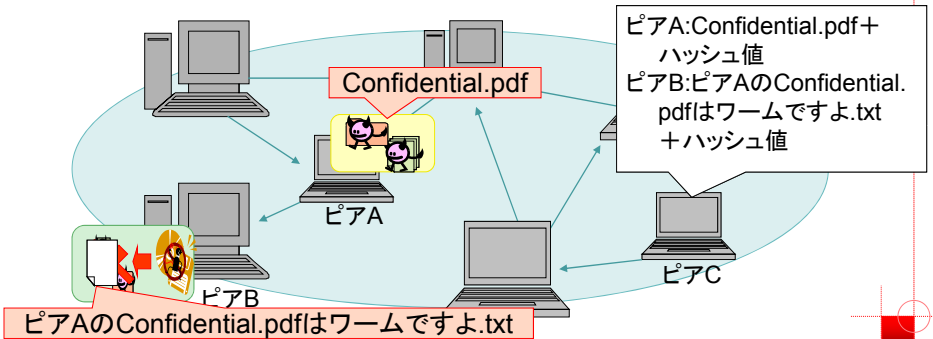
④P2Pコミュニティの中では、
各自の共有フォルダ内のファイルに関するハッシュ情報(「ピア名:ファイル名＋ハッシュ値」の一覧)が相互に交換される。



考察(2)

Nish!gaki Laboratory

⑤それらのハッシュ情報が他のピアCに届く。
ピアCでは、すべてのハッシュ情報を結合したデータベースを用いて、自分の欲するファイルを有するピアを検索することができる。



考察（2）

Nish!gaki Laboratory

⑥ピアCがConfidential.pdfをダウンロードしようと思い、手元に集まったハッシュ情報を検索してみたところ、
「ピアAにConfidential.pdfがある」という情報と共に「ピアAにあるConfidential.pdfはワームである」という情報が得られるため、ピアCはピアAからのダウンロードを躊躇する。

ウイルスに
感染したくない

・ピアA:Confidential.pdf＋ハッシュ値
・ピアB:ピアAのConfidential.pdfは
　ワームですよ.txt＋ハッシュ値

考察（3）

Nish!gaki Laboratory

- 知識のある人なら、アンチウイルスソフトが反応してもファイルを削除しないようにする
- 知識のある不正者に特徴パターンが漏れると
  - 顧客情報から個人情報を収集
  - 同種企業の内部資料を入手

は
ウイルスではない

考察(3)

Nish!gaki Laboratory

- 機密情報毎に埋め込む特徴パターンを変化させる

考察(3)

Nish!gaki Laboratory

- 不正者に本当のウイルスなのか特徴パターン付の機密情報なのか判断しにくくする
  - 怖くてファイルを開けない

まとめ

Nish!gaki Laboratory

- P2Pネットワークおける情報漏洩の対策として、機密情報にアンチウイルスソフトが反応する特徴パターンを埋め込むことで、P2Pネットワーク上に機密情報が拡散することを防止する方式を提案した