FUJITSU

shaping tomorrow with you

人間系からのセキュリティ対策アプローチ

2014年8月25日 SS研

株式会社富士通研究所　&　富士通株式会社

津田　宏 (htsuda@jp.fujitsu.com)

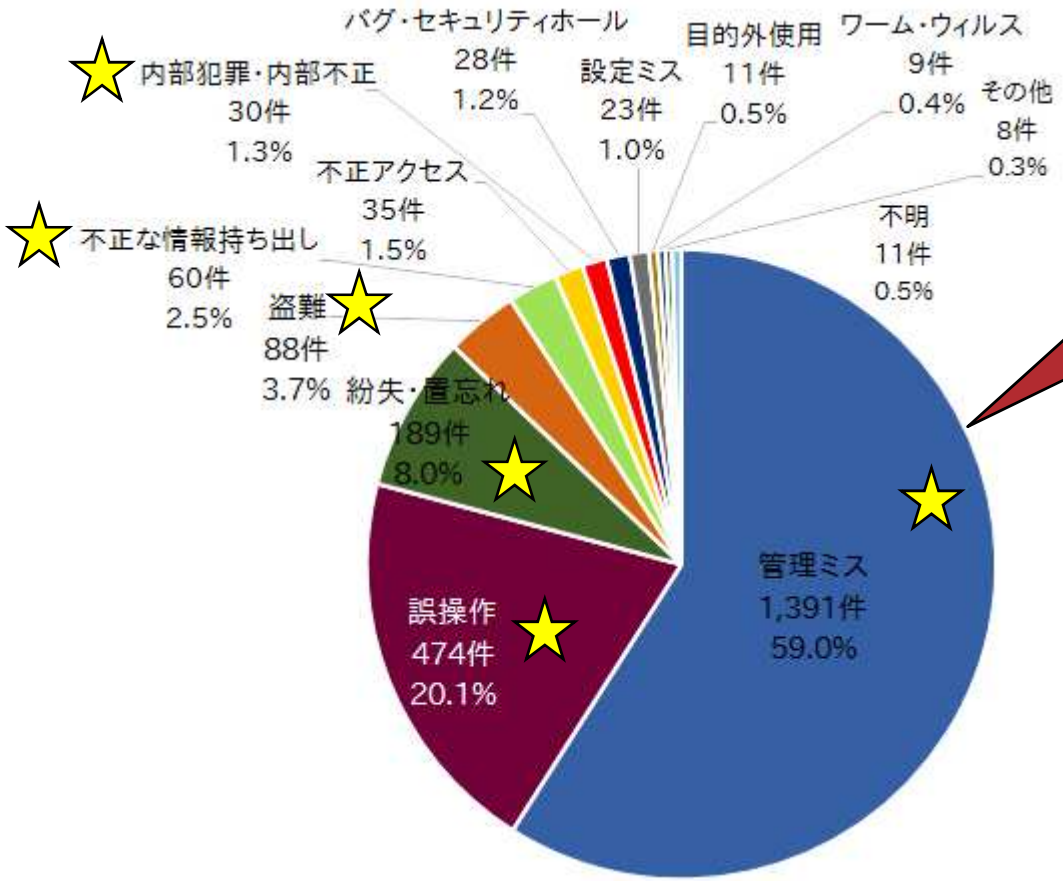
目次

FUJITSU

- はじめに：「人」中心のセキュリティの必要性
- メール誤送信対策
- 標的型メール対策
- 被害に遭いやすい人の心理・行動特性（※1）
- おわりに
- (参考) 富士通の標的メール訓練サービス概要

※1: 総務省「サイバー攻撃の解析・検知に関する研究開発」の開発成果が含まれています

背景：「人」を中心にしたセキュリティの必要性



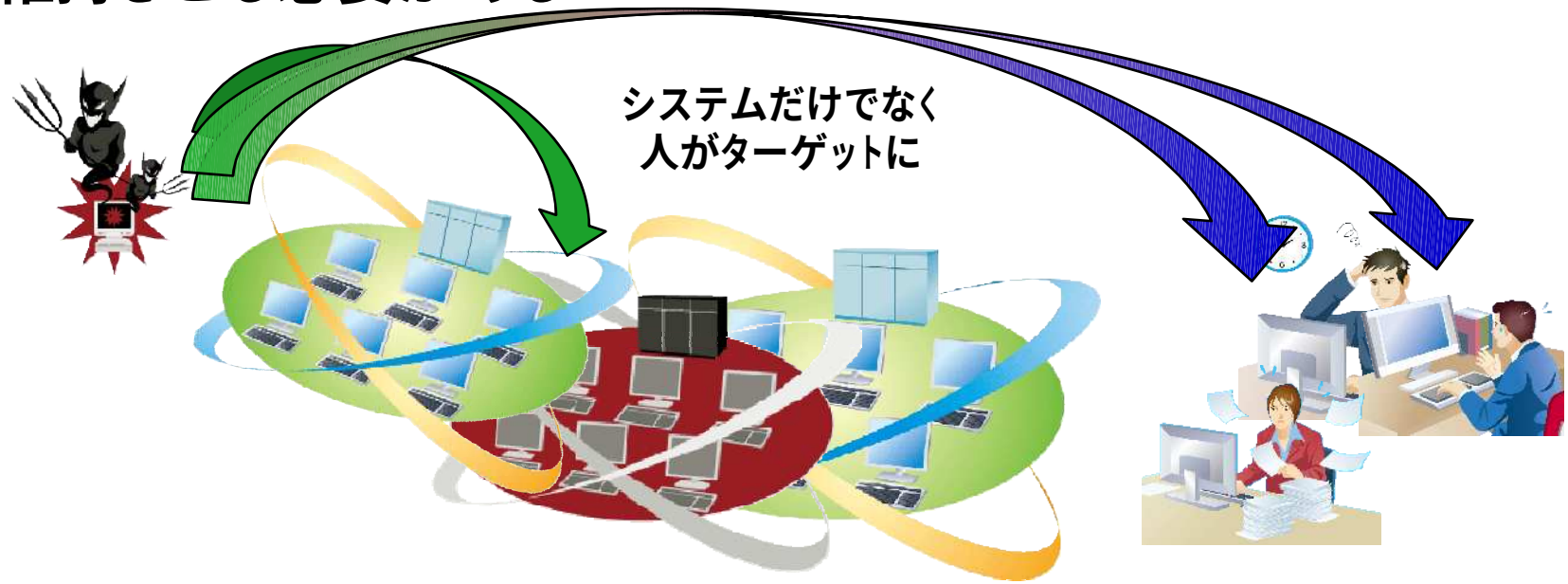
大半は、組織内部の何らかの人間系対策が必要

出典：日本ネットワークセキュリティ協会
2012年 情報セキュリティインシデントに関する調査報告書
～個人情報漏えい編～

サイバー攻撃の多様化：一般人がターゲット

FUJITSU

- サイバー攻撃の巧妙化、多様化
- 標的型メール攻撃に「やり取り型」増加、水飲み場攻撃も確認
- 警察庁の2013年のサイバー攻撃情勢より（2014年2月）、
- システムを堅牢に構築しても、運用する人間に問題があると意味がない
- 組織の従業員一人一人の意識、ITリスクに対する警戒心を、向上・維持させる必要がある



人に着目した関連研究

FUJITSU

- ITリスクに対する認知の研究
  - 対策は覚えやすく、思い出しやすくする（I3P，2011年）
    http://www.thei3p.org/docs/publications/442.pdf
  - 米国のサイバーセキュリティ推進コンソーシアムの“Leveraging Human Behavior to Reduce Cyber Security Risk”プロジェクトにおける議論
  - フィッシング被害に遭いやすい人は自信過剰（IPA，2012年）
    リスク認知と実行に関する調査報告書 , IPA, 2012.
  - 行動履歴に基づくセキュリティ対策
- スマホアプリの許諾ポリシーの自動設定
  - 480万人分のポリシーデータから作成したパターンから、ユーザの利用実態を分析。人に合うパターンを選択

Liu,B., Lin,J.,Sadeh, N.: Reconciling Mobile App Privacy and Usability on Smartphones: Could User Privacy Profiles Help ?, Proceedings of the 23InternationalConference on World Wide Web (WWW2014),pp.201-212(2014).

- 情報漏えいメールと企業内行動との関係
  - 企業内行動：メール送信状況、印刷回数、出張回数など
    池田利夫 : 企業内行動履歴解析による情報漏洩メール推定システムの検討, AI 学会 全国大学会(2012)

1. メール誤送信対策

質問1

FUJITSU

メールの誤送信をやったことありますか？

- **宛先の誤り**
- **BCC/CCを間違えて、他の人のアドレスが分かる形で送信**
- **添付ファイルの取り違い**

etc.

1. **ある**
2. **ない**

メールからの情報漏洩対策

FUJITSU

ビジネスユーザーの
66.2%がメール誤送信の
経験
誤送信の影響：お詫び (4.1%),
始末書(1.8%),取引に影響
(1.2%),解雇(0.3%)

株式会社HDE「メール誤送信」に関する
実態調査」2008.4.23

- 2014/7/30 M県農業研究所　農業従事者メールアドレス285名誤送信
- 2014/5/29 S署 性犯罪被害者の個人情報をFax誤送信 (別の署が7月にも再度)
- 2014/4/1 M大 休退学20人の情報を誤送信
- 2014/3/15 H大の患者115名の情報を大学院生がメール誤送信
- 2014/3/27 T県　ふるさと納税者1020名メールアドレスを誤送信
- 2013/8/23 K通信　取材メモを誤送信。県警幹部発言を他社に
- 2013/7/14 H新聞　「取材メモ」がメール誤送信で社外流出

■メール誤送信対策のニーズ

■メールによる個人情報漏洩の対策

■他社向けメール取り違え等による企業としての信用低下防止

ただし、メール誤送信に対して何をすれば何が解決するのか、はっきりしない

メール情報漏洩対策の考え方

FUJITSU

社内インシデントの分析から

レベル		対策内容	インシデントなど
フェールセーフ	L1	添付ファイル暗号化	
	L2	添付ファイルはサーバ経由で閲覧させる	
汎用的対策	L3	アラートUI: 送信前に誤送信の可能性を気づかせる	(例) アドレス帳で隣を選択、タイプミス、社外のCcに気付かず返信
	L4	ルールに抵触するメールを禁止	(例) アドレス帳選択ミスで社外を含む200名以上に送信
業務特化の対策	L5	プロジェクト・業務ルールに従ったメールのみ許可	(例) A社向けファイルをB社に送付
	L6	セキュア文書管理と連携	(例) 社外秘ファイルを社外に誤添付
	L7	業務を見直し、上司を含めて内容を承認で確認	(例) 添付ファイルの内容上の誤り
悪意対策(LM)		証跡ログ分析、類似検索	(例) 退職前に特定社外宛メール増、文書流出

※L1～L7: 下のレベルまで対応するとカバー範囲は広いが、導入の人的コストは高い

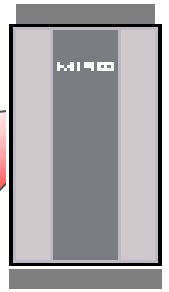
メール情報漏洩対策：アプローチ

FUJITSU

L3,L4,L5

1.送信メールフィルター
- メール環境を変えずに導入可能
- 自動ホワイトリストによる過剰指摘抑制
- XMLによる柔軟なルール定義とRSSによるポリシー配信

2. 添付ファイルトレーサビリティ
- ｺﾝﾃﾝﾂｼｸﾞﾈﾁｬによる類似内容検出
- ファイルアクセスログ収集/モニタ



メール
ゲートウェイ

メール
サーバ

L6,LM

クライアントPC

メーラー（任意）

クライアントフィルタ
(SMTP Proxy)

サーバフィルタ

自動で
蓄積・検出

文書のフィン
ガプリント

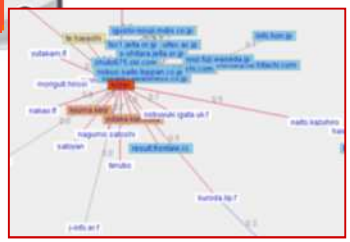
文書管理サーバ

RSS

ポリシー配信

ログ分析

管理者



悪意対策 etc.

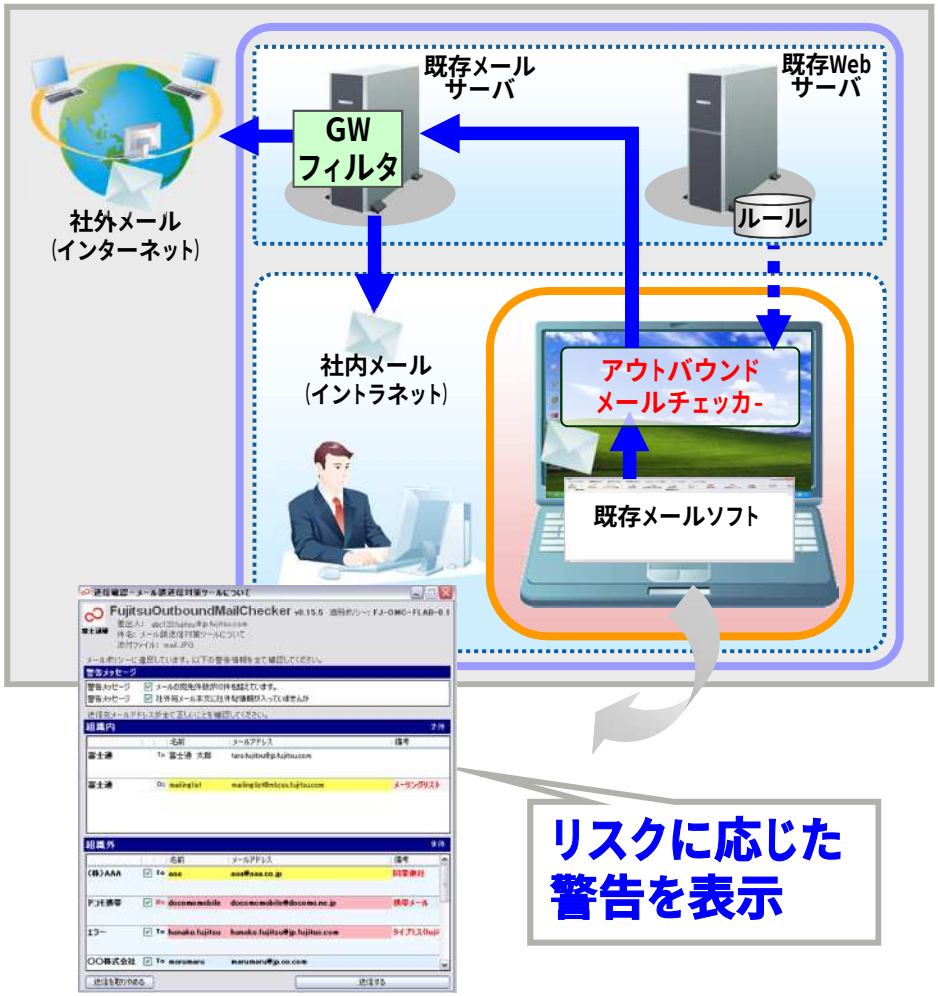
3. メールログ分析技術
- 送信ログのユーザ関係分析
- 不審なメール行動をアラート

アウトバウンドメールチェッカー(L3,4,5)

FUJITSU

直前の警告表示により、メール送信のうっかりミスを防止

システム構成



リスクに応じた
警告を表示

警告表示による注意喚起

- 宛先誤りやルール違反をアラート表示し、うっかりミスによる情報漏洩を抑止
- メール履歴から個人毎に送信先を学習
  (自動学習ホワイトリスト)

セキュリティレベルの均一化

- 組織別にルールを柔軟にカスタマイズ可能
  (例) 社外宛は要チェック、20件以上はチェック、A社宛は特定タイトル･添付パターン
- RSSにより更新ルールが即時適用可
- サーバフィルタと連携しルール強制が可能

低コスト短期間導入

- 既存のメールソフト･サーバをそのまま継続
- 社内の殆どのメーラーに対応

SHieldMailChecker誤送信防止 (富士通SSL)

FUJITSU

宛先種別を表示
※ BCCは強調表示

組織内は組織名ごとに表示

組織外の宛先を会社名ごとに表示

リスクの確認が可能

種別ごとに整理して表示
※ 上場企業、公的組織 etc

ルール違反を警告メッセージで説明

例)
- 宛先数が上限以上
- タイトル、添付ファイル名、本文に社外機密キーワードを含む
  (例えば、社外秘、関係者外秘、機密など)
- 社外宛てメールに、ファイルを添付している

宛先リスクの警告
- 同業他社
- メーリングリスト
- 個人メール
- 携帯メール
- タイプミス etc

特許登録済
自動学習ホワイトリストで宛先確認のマンネリ化防止

送信ストップ

メールサーバ

インターネット(イントラネット)

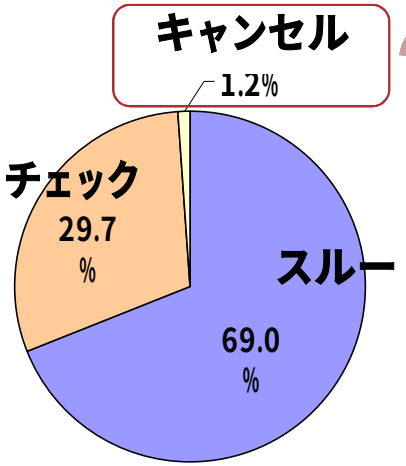
送信を許可
すべてチェックしないとクリックできない

メールチェッカー：社内展開から

FUJITSU

- 社内利用、製品化 (アウトバウンドメールチェッカー)
  - 富士通G(10万人)の標準メールセキュリティツールとして利用
  - 2009.9 富士通SSLより「SHieldMailChecker誤送信防止」として製品化

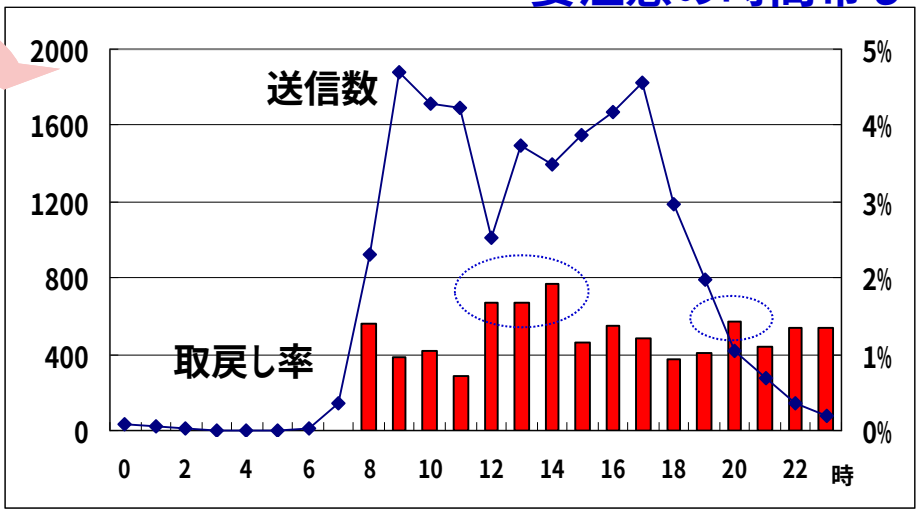
  http://www.ssl.fujitsu.com/products/network/netproducts/shieldmail/
- 社内利用アンケートより
  - 必要ない関係者への送信を回避
  - 同業他社への誤送信
  - メーラーのアドレス補完機能での誤送信を回避
  - 全員に返信時、送信者がタイプミスしていたのをチェック



約18千通より

大半が
社外宛

要注意の時間帯も



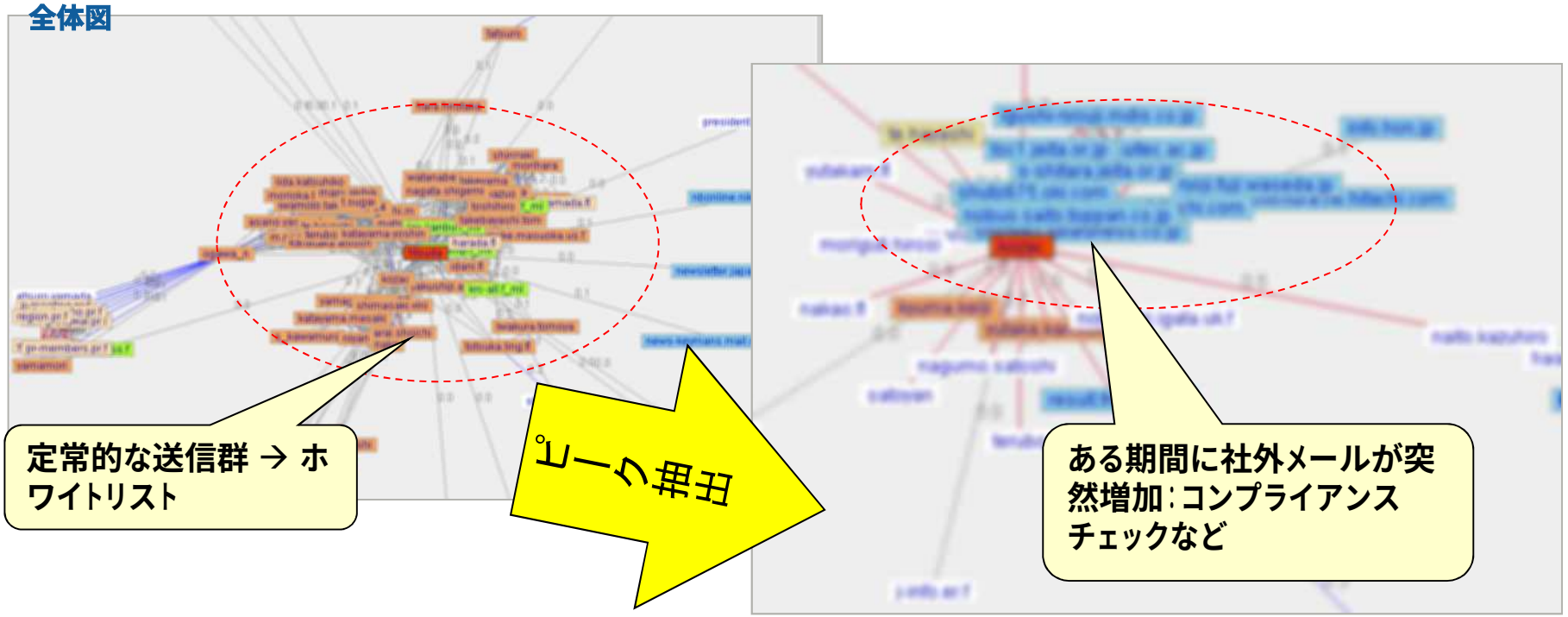
(参考) 送受信ログ分析･見える化技術

LM FUJITSU

利用シーン

･ホワイトリストの定期的な更新 (送信チェックの過剰指摘の軽減)L3
･特に最近特定社外とのやりとりが増加などを管理者にアラート LM

cf. 既存技術: 2008.5.7プレスリリース　滋賀銀行様においてビジネス情報ナビゲーションシステムが稼働～地域企業のビジネス相関図を見える化することで、地域密着型の提案を実現～



FUJITSU

2. 標的型メール対策

背景

FUJITSU

■近年、特定組織や個人を狙った標的型攻撃が急増

■標的型メール

- 機密情報の窃取を目的に、特定組織や個人を標的として送られてくるウイルスメール
- 知人からのメールのように差出人を偽装。顧客を騙って何通かやりとりした後にウイルスを仕込むパターンも。
- 既存パターンでは検知できないウイルスを仕掛けた添付ファイルやURLを開かせることで、侵入の第一歩

	スパムメール（従来型）	標的型メール
攻撃者の目的	社会混乱	機密情報窃取
攻撃対象	不特定多数ユーザ	特定組織や個人
差出人（攻撃者）	個人名や不明組織	実在する信頼組織（行政機関）・個人を詐称
件名・本文	一般的な用件	自分に関係がありそうな用件

■メール誤送信に対するクライアント対策を、受信時に拡張

質問2　標的型メール訓練

FUJITSU

■標的型メール訓練についての質問です

1.　訓練をやったことがある。メールを開いてしまった

2. 訓練をやったことがある。メールを開かなかった

3. 訓練をやったことはない

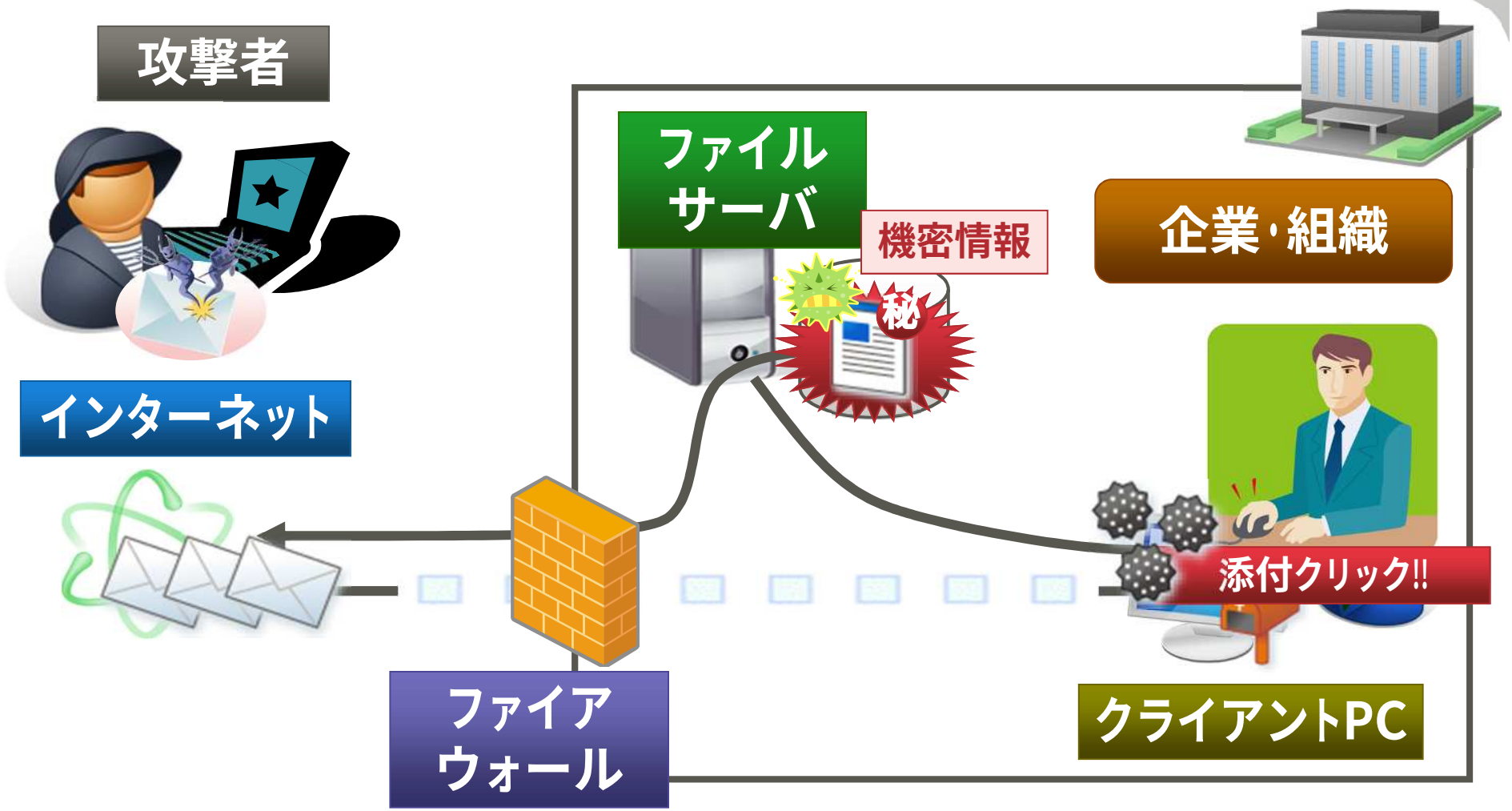
標的型メールへの現状の対策と課題

FUJITSU

- **ウイルス対策ソフト**
  - 既存パターンに合致しない(ゼロデイ)ウイルスが利用されるとほとんど検知できない
- **迷惑メールフィルタ**
  - 無差別･大量に送られる迷惑メールと違い、標的にあわせて、差出人や本文が偽装されるため、検知困難
- **送信ドメイン認証技術（SPF, DKIM）**
  - 差出人アドレスが偽装されたら、本人性を担保できない
  - 確認用サーバの導入コストが高い
- **標的型メール訓練**
  - 内閣官房など１２の政府機関で約６万名に対して実施（平成２３年１０月～１２月）
  - 全体の１割は、添付ファイルを開いてしまう

技術的な対策だけでは限界があり、人間系の対策も必要

添付ファイルを利用した標的型メール攻撃の例

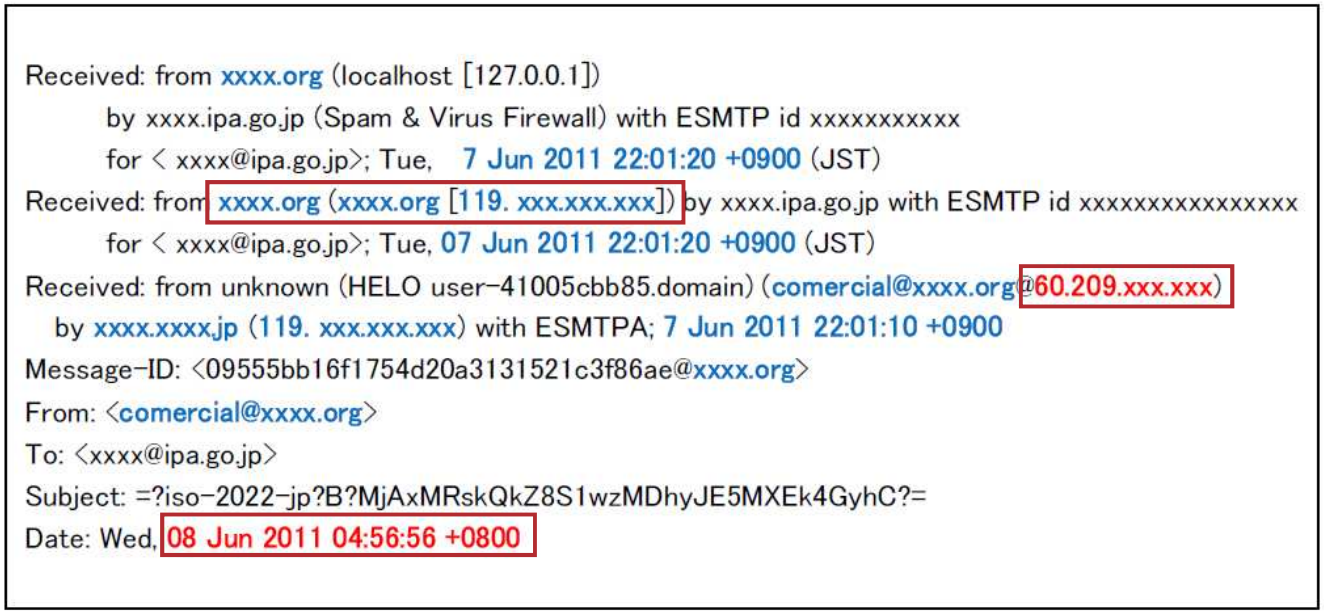


①文書ファイルにウイルスを埋め込み、偽装メールに添付して送信
②アプリケーションの脆弱性を突いて、ウイルス感染（バックドア開放）
③バックドアから侵入、機密情報入手

標的型メールのメールヘッダ例1

FUJITSU

- **中継メールサーバ情報として、中国のIPアドレスが含まれている**
  xxxx.org [119.xxx.xxx.xxx] **や** xxxx.xxxx.jp (119.xxx.xxx.xxx) **は国内の大手プロバイダであるにも関わらず、**「60.209.xxx.xxx」**は、中国が管理するIPアドレスである**
- **メール送信時刻**「08 Jun 2011 04:56:56 +0800」**のタイムゾーンは、日本ではなく中国のタイムゾーン**



2011年6月7日にIPAに届いた標的型メールのメールヘッダの一部

標的型メールのメールヘッダ例2

FUJITSU

- 「xxxx.xxxx.go.jp」は日本のある官公庁のドメインであるにも関わらず、「60.26.xxx.xxx」は、中国が管理する IP アドレスである
- メール送信時刻「22 Nov 2010 10:02:19 +0800」は日本ではなく中国のタイムゾーン、中国でよく利用されている
  メールソフト「Foxmail 5.0 beta2」を使って送信していることが確認できる

```
Received: from xxxx.xxxx.go.jp ([60.26.xxx.xxx])by mxg511.nifty.com with ESMTP id xxxxxxxxxxxxxx
          for <xxxx.xxxx@nifty.com>; Mon, 22 Nov 2010 11:02:49 +0900
X-Nifty-SrcIP: [60.26.xxx.xxx]
Message-Id: <201011220202.oAM22Iq3006674@mxg511.nifty.com>
Received: from CRO-EE2C1904C10[192.168.1.226] by xxxx.xxxx.go.jp
  with SMTP id 37B7040D; Mon, 22 Nov 2010 10:02:14 +0800
From: "xxxx@xxxx.xxxx.go.jp" <xxxx@xxxx.xxxx.go.jp>
Subject: RE: =?ISO-2022-JP?B?GyRCMyRKXSQrJGkkTj5wSnMhSkBtM1U0WDc4IUsbKEI=?=
To: "xxxx" <xxxx.xxxx@nifty.com>
Reply-To: xxxx@xxxx.xxxx.go.jp
Date: Mon, 22 Nov 2010 10:02:19 +0800
X-Mailer: Foxmail 5.0 beta2
```

2010年11月22日にある個人に届いた標的型メールのメールヘッダの一部

提案方式

FUJITSU

メールヘッダや本文の中で、攻撃者が詐称することが困難な送信者固有の特徴情報を利用し、標的型メールの可能性をリアルタイムに判定・検知する技術の提案

2つの技術を用いた、標的型メールへのクライアント対策を提案

技術1

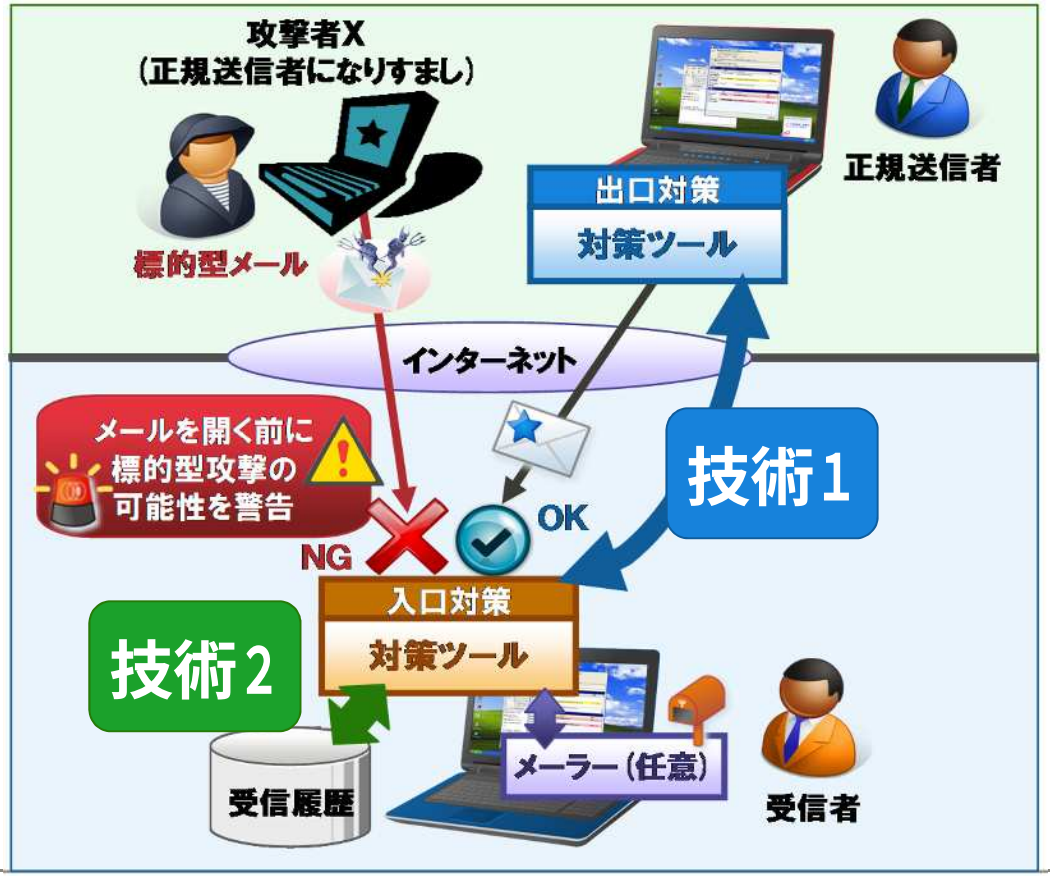
送受信での連携による なりすまし検知技術

対策ツール同士が送受信で連携し、なりすましを防止

技術2

受信履歴を用いた送信者特徴の分析技術

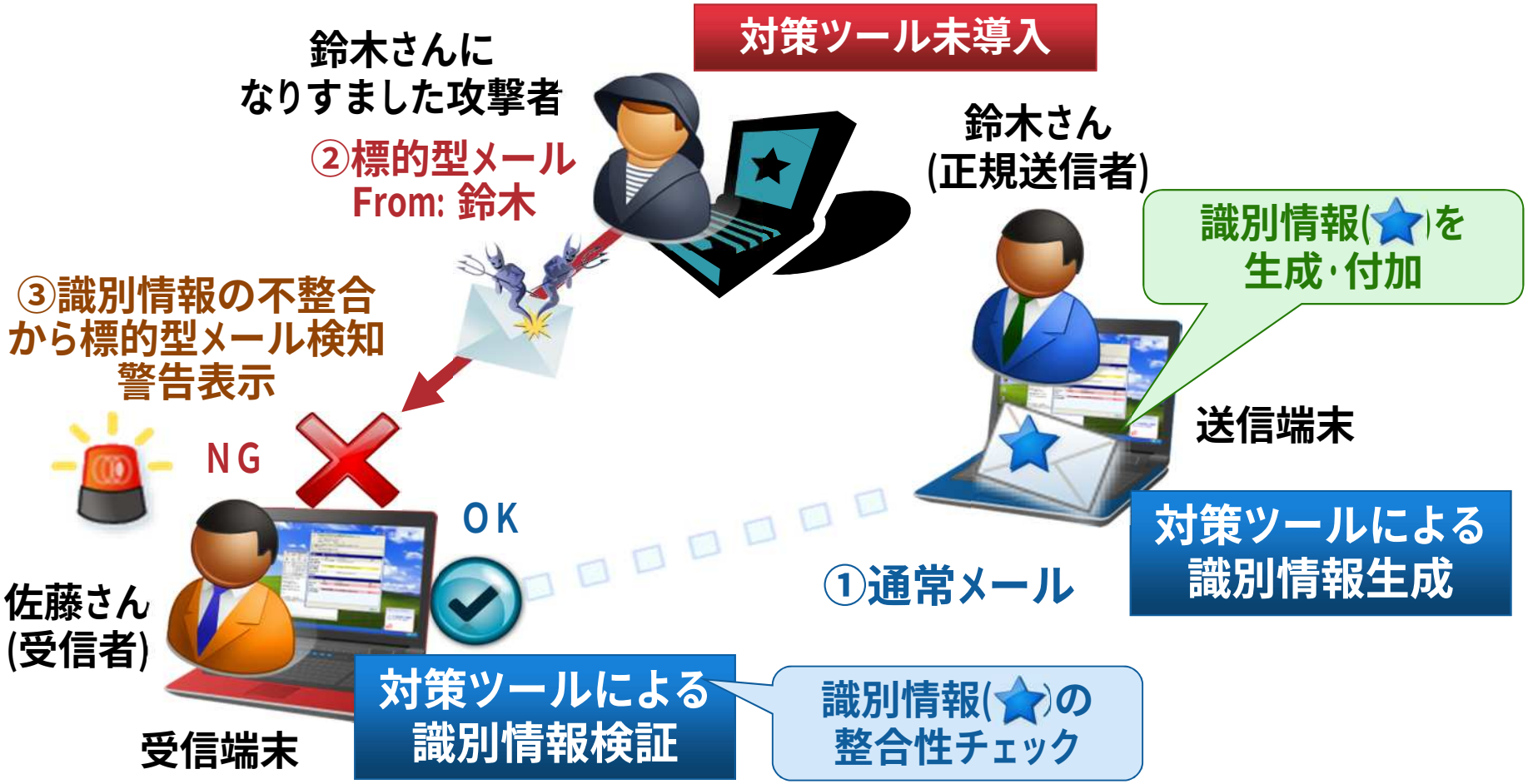
送信者の特徴を端末毎に学習 類似性を判定



(1)送受信連携による、なりすまし検知

FUJITSU

- 送信端末と受信端末が互いに対策ツールを導入し、なりすまし防止
  - 送信端末で、メール特徴から識別情報を生成･付加
  - 受信端末で、識別情報の整合性を検証

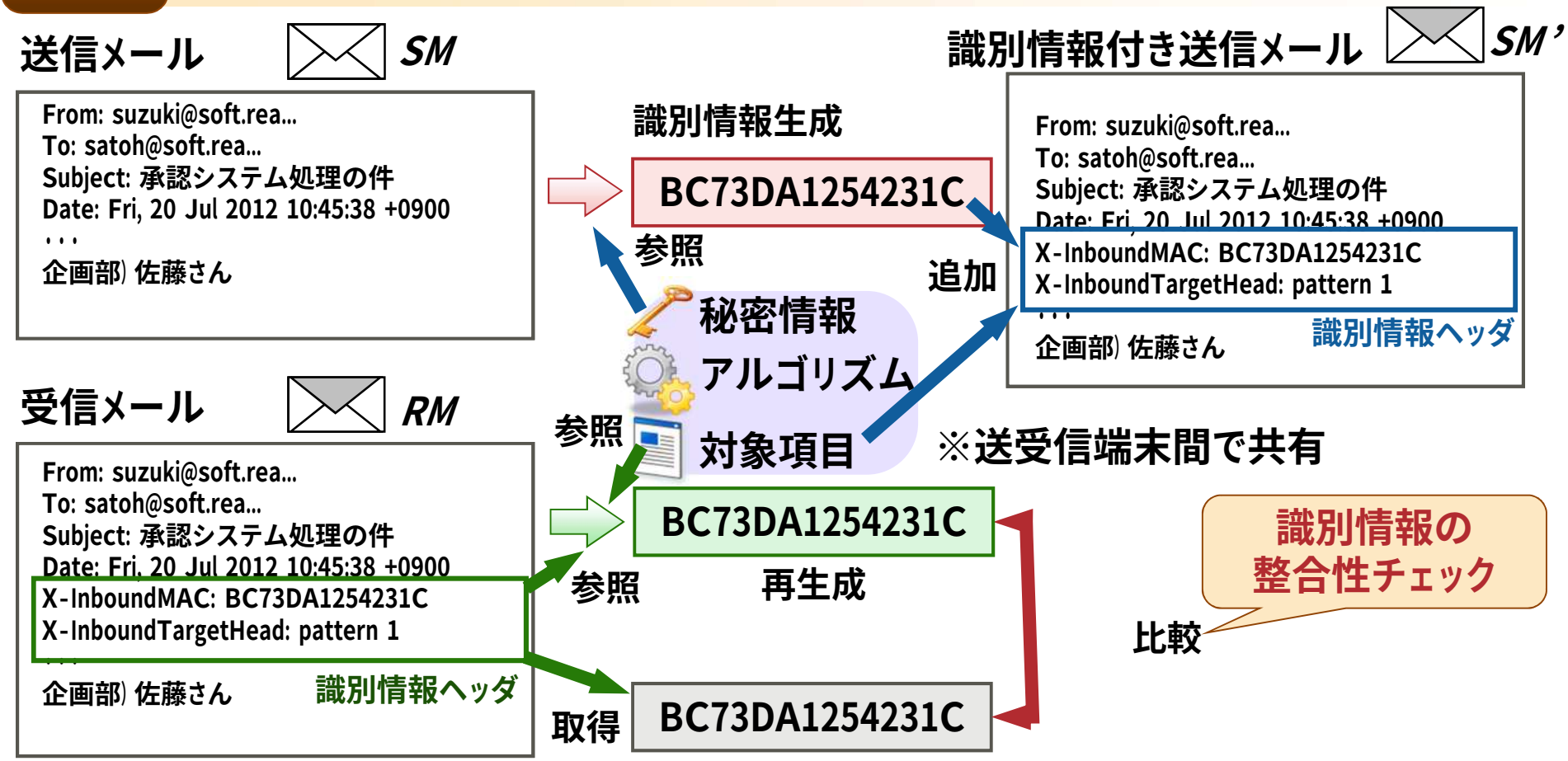


識別情報生成・検証方式

FUJITSU

技 術 送受信端末間で、秘密情報・生成アルゴリズム・対象項目を共有
秘密情報を含めて、生成・検証

効 果 識別情報の有無チェックで判定可能
メール改ざんや識別情報コピーによる不整合検知、正規メールと判別可能



(2) 受信履歴からの送信者特徴の分析技術

FUJITSU

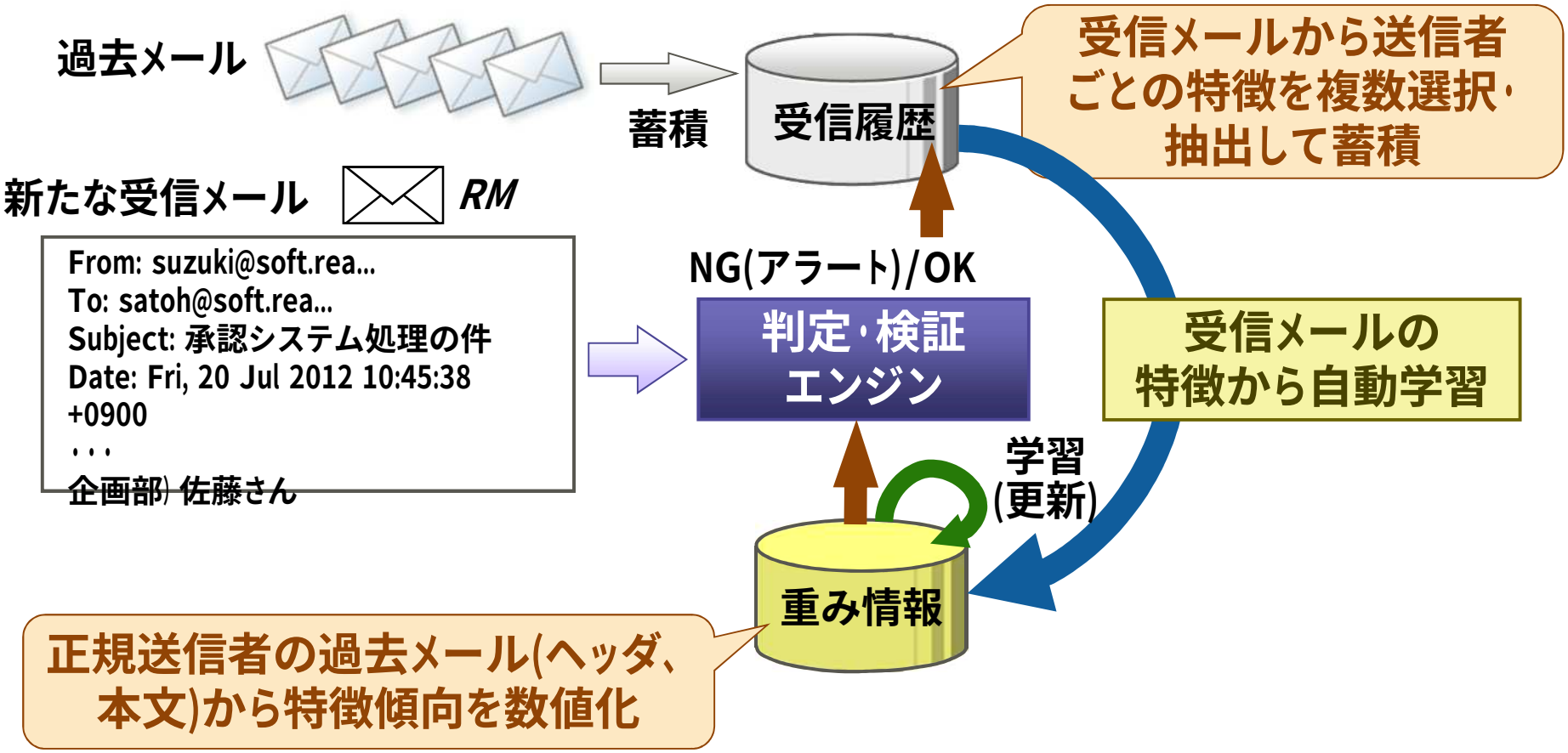
- 送信者が対策ツール未導入でも、なりすましを防止
  - これまでの受信メールの特徴から、送信者の特徴傾向を学習・数値化(重み)、重みを含めて堅実に判定

送信者特徴ソーシャル分析方式

FUJITSU

技 術 受信メールから、送信者特徴を複数選択・抽出して、
特徴傾向を学習して数値化（重み）、重みを含めて類似性判定

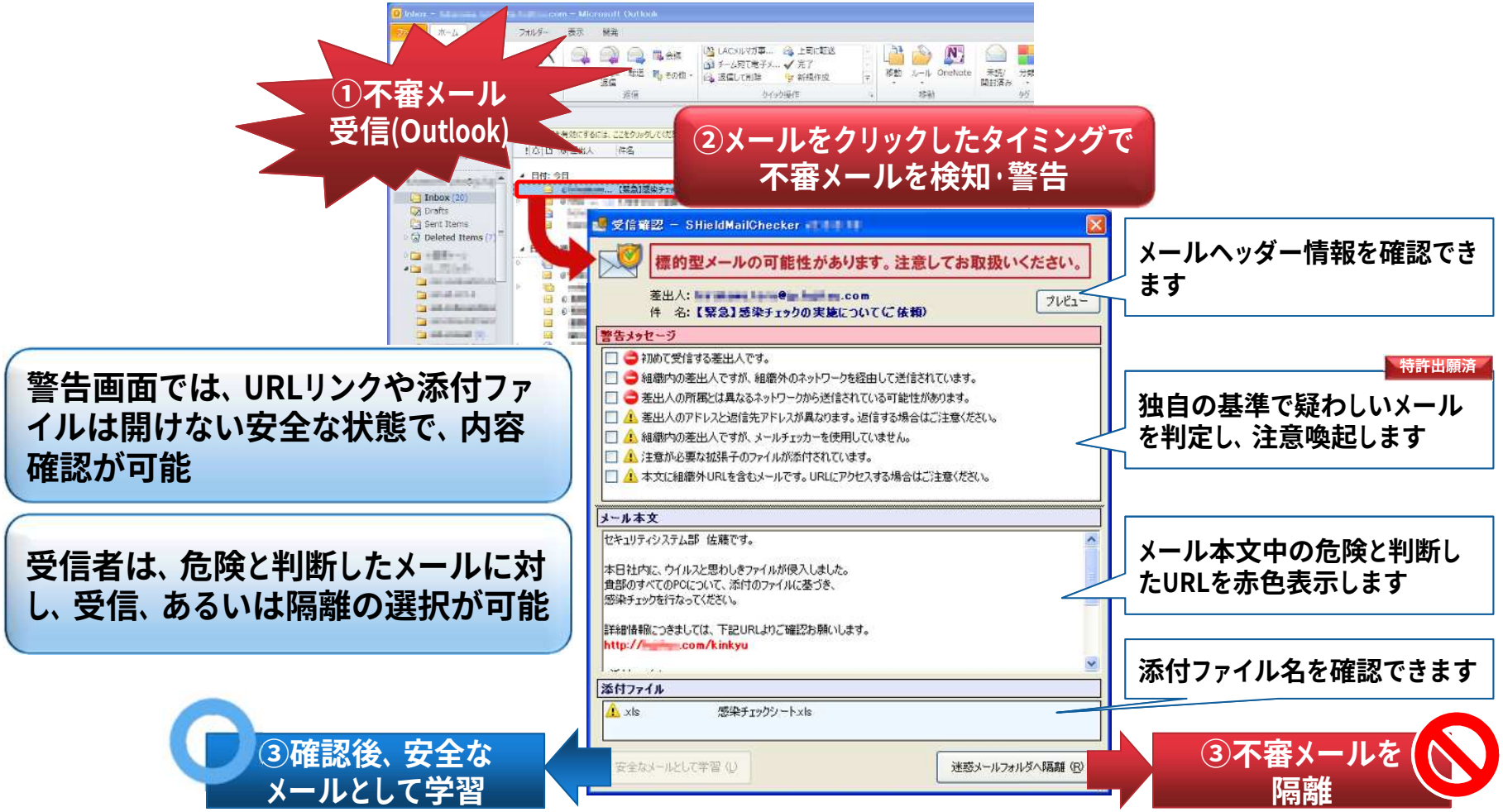
効 果 重みを含めた判定により、送信者特徴を堅実に捉え、判定確率を向上



製品：SHieldMailChecker標的型メール対策

FUJITSU

■ メールを開く前に標的型攻撃の可能性をリアルタイムに検知・警告

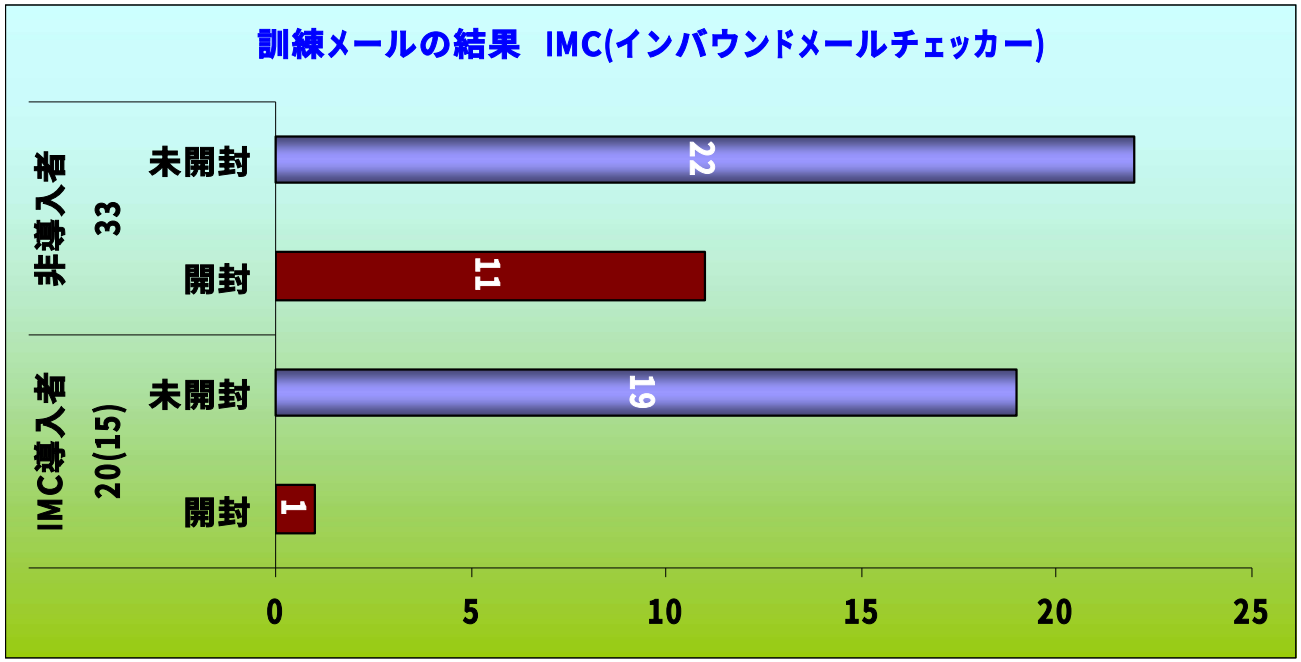


富士通SSL
http://www.ssl.fujitsu.com/products/network/netproducts/shieldmail-ta/

標的型メール訓練によるメールチェッカー評価

FUJITSU

- 標的型メール訓練サービス (富士通) を、富士通研究所で次の2グループに適用。擬似攻撃メールに対して、添付ファイルの開封率を比較
  1. インバウンドメールチェッカー非導入者　33名
  2. インバウンドメールチェッカー導入者　20名



非導入者では
1/3が開封

導入者では
1/20が開封

3. 人間系からのアプローチ ～被害に遭いやすい人の心理･行動特性～

※1: 総務省「サイバー攻撃の解析･検知に関する研究開発」の開発成果が含まれています

質問3 (ベネフィット認知)

FUJITSU

Yes/Noでお答えください

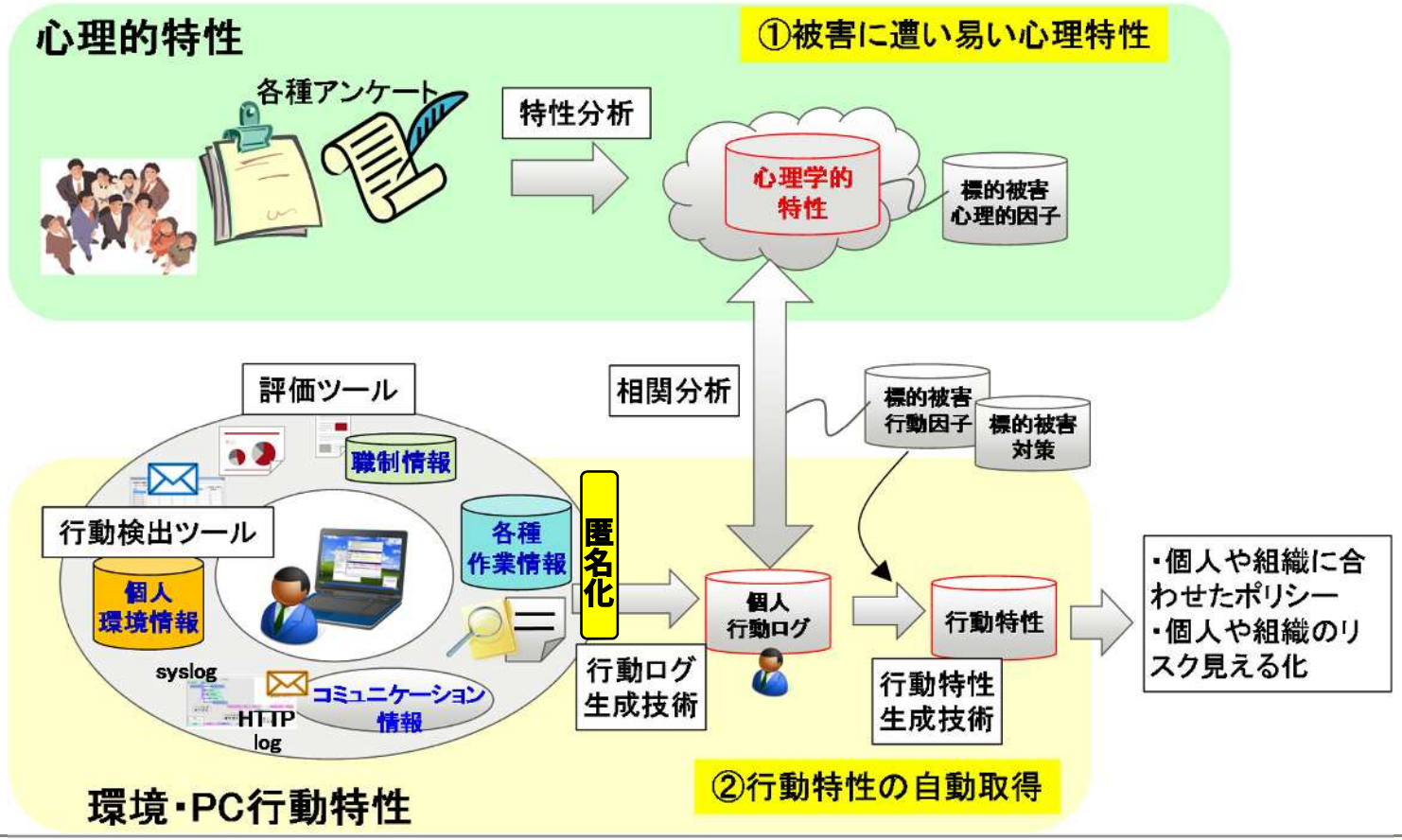
- **車がまばらに通っているが、車がまだずっと遠くにいれば、つまづく可能性も0ではないが、赤信号でも横断歩道を渡る**

1.Yes

2.No

目標：人に合わせたセキュリティ

- メール誤送信、標的型メール攻撃訓練から分かったこと：
  人や組織により被害リスクはまちまち
- これからは、均一のセキュリティポリシーではなく、人や組織の特性に合わせたセキュリティガバナンスが必要ではないか？

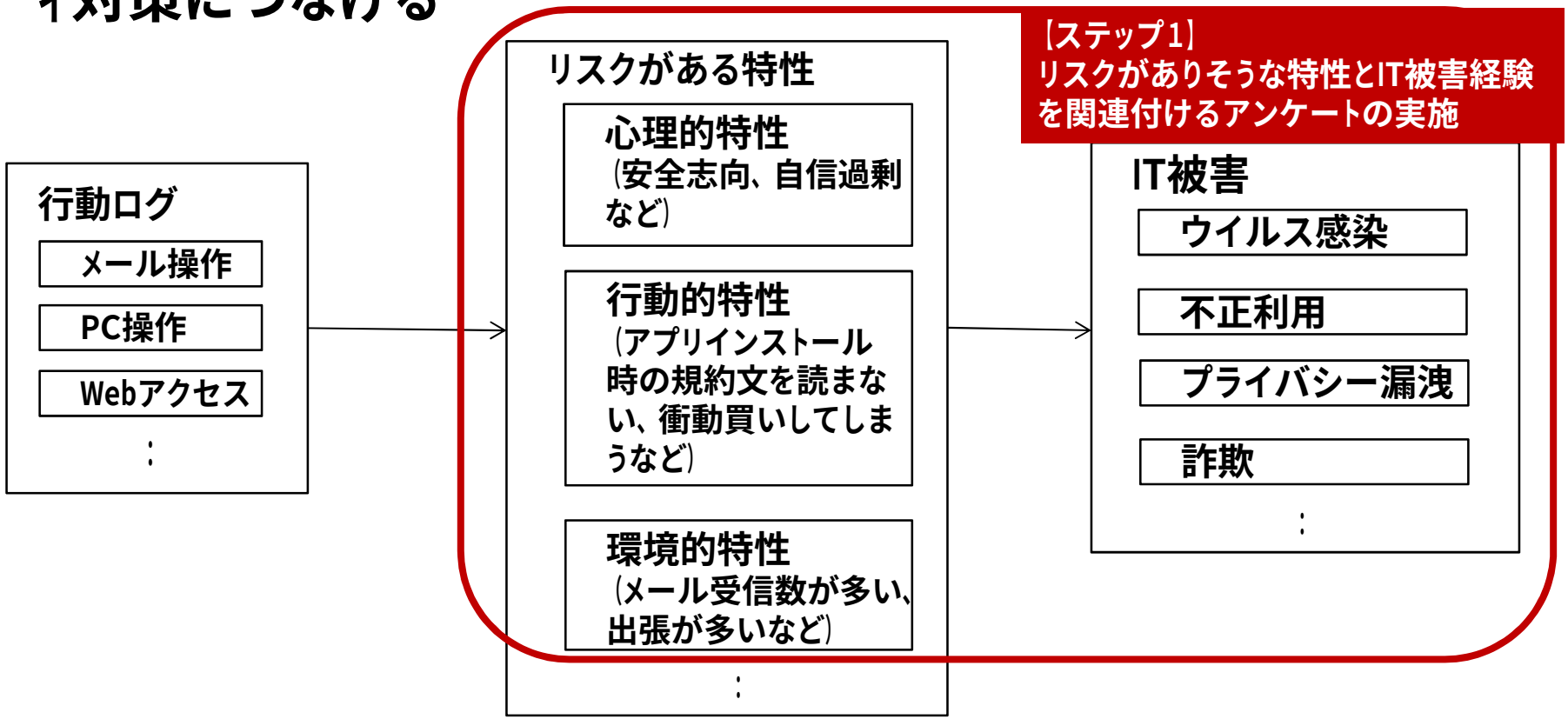


アプローチ

(1) IT被害と関係のある心理・環境特性をアンケートにより分析

(2) 上記特性と関連する、PC操作などの行動ログを特定

(3) 特定の行動ログパターンを持つ個人や組織に合わせたセキュリティ対策につなげる



IT被害特性アンケート分析

FUJITSU

- インターネット調査会社により、下記条件をすべて満たす約2,000名について、WEBアンケートを実施
  - 会社員 ＆ 業務の大半で自分専用のPCを利用
  - 男女20歳代～60歳代
- 今回は心理的特性、行動的特性に着目

項番	質問数	質問カテゴリ	質問内容例	調べたい特性
Q1	4	IT被害経験の項目	ウイルス感染、不正利用、 プライバシー漏洩、詐欺　の4種類	
Q2～ Q3	16	心理測定尺度（※）をはかる項目	・自己効力感（＝問題解決力の自己評価） ・一般的信頼感（他人をどのくらい信用するか）	心理的特性
Q4～ Q12	22	物事の考え方、行動習慣をたずねる項目	・ベネフィット認知（物事のリスクよりも利益を重視するか） ・情報共有意思（リスクに対する情報を共有するか）	心理的特性＆ 行動的特性

※「心理測定尺度」とは、心理特性（自己効力感、一般的信頼感など）を高い精度で測定可能な、社会心理学における従来知見

アンケート項目一覧

項番	質問意図	質問文
Q1_1	ウイルス感染経験	ウイルス感染(自分のパソコンに入っているセキュリティソフトが検出した場合も含む)
Q1_2	不正利用被害経験	不正利用(ユーザID、アカウント、オンラインゲームなどでの通貨やアイテム、クレジットカード、銀行口座、など)
Q1_3	プライバシー漏洩経験	プライバシーの漏洩(SNSや動画サイトなどにおける個人用設定が原因で、個人的な日記や閲覧履歴などが不特定多数に公開されてしまった、など)
Q1_4	詐欺被害経験	詐欺(なりすましメールに騙された、架空請求の支払いに応じた、偽のセキュリティソフトをインストールしてしまった、パソコンのシステムやファイルが書き換えられ元に戻すためにお金を支払った、など)

Q2_1	リスク受容 安全志向因子	危ない場所へは絶対近づかない
Q2_2	リスク受容 安全志向因子	何事も安全第一である
Q2_3	リスク受容 運命因子	危険と上手につきあうのが人生である
Q2_4	リスク受容 運命因子	危険と安全が混じり合っていることで、世の中は成り立っている
Q2_5	自己効力感の低さ	私にとって、最終的にはできないことが多いと思う
Q2_6	自己効力感の低さ	やりたいと思っても、私にはできないことばかりだと感じる

Q5	情報共有意思の低さ	Q5 仕事で、間違った情報を教えたり報告してしまったら、「A. ささいなことでもすぐに伝える」「B. よほどの支障が生じる心配がない限り伝えない」のどちらに近い対処をとりますか。 ※ お勤めの会社に、上記のような場合の対処マニュアルがないものとしてお答えください。
Q6	情報共有意思の低さ	Q6 仕事で、あなたは大事な顧客情報または社内機密情報を、まったく別の相手に送ってしまったら、「A. なるべく周りに相談して解決したい」「B. なるべく自分で解決したい」のどちらに近い対処をとりますか。(回答は1つ) ※ お勤めの会社に、上記のような場合の対処マニュアルがないものとしてお答えください。
Q7_1	ITに対するコントローラビリティ	わたしは、仕事上の大事なデータを誤って流出させたり、紛失したりすることはないと思う
Q7_2	ITに対するコントローラビリティ	わたしは、ブログやツイッター、掲示板などのインターネット上のコミュニケーションツールを正しく使えるので、不用意な発言で個人情報をもらしてしまったり、発言が広められて不特定多数の人間から非難を浴びることはないと思う

Q2_7	一般的信頼	ほとんどの人は基本的に正直である
Q2_8	一般的信頼	ほとんどの人は信頼できる
Q2_9	パーソナルな信頼	何をするにつけ、知らない人とするよりも、よく知った人とするほうが安心できる
Q2_10	パーソナルな信頼	一般に、長くつきあっている人は、必要なときに助けてくれることが多い
Q2_11	用心深さ	世の中には偽善者が多い
Q2_12	用心深さ	人々はふつう、口で言っているほどには、他人を信頼していない

Q3_1	権威主義	伝統習慣にしたがったやり方をとるべきだ
Q3_2	権威主義	先祖代々と同じやり方をとるべきだ
Q3_3	後悔予期	うまくいった場合のことよりも、失敗して後悔した場合のことを考える
Q3_4	後悔予期	最善のことをしたとしても、失敗した場合のことが気になってしまう

Q4_1	コスト認知の低さ	パソコンやスマートフォンなどで、アプリケーションをインストールする際やアップデートする際に表示される規約文や権限許可などの内容は、きちんと確認・理解してから先へ進む
Q4_2	コスト認知の低さ	前々から予定に入っていた大事な試験やプレゼンテーション(発表・企画提案・説明など)の日までには、自分として納得のいく準備(勉強量、資料内容、話す内容など)ができているのはいつものことだ ※ 急な仕事の依頼などやむを得ない理由で準備不足になった場合は除く
Q4_3	ベネフィット認知	車がまばらに通っているが、車がまだずっと遠くにいれば、つまづく可能性もOではないが、赤信号でも横断歩道を渡る
Q4_4	ベネフィット認知	つい、夜更かししたり、食べ過ぎ・飲み過ぎたりして、翌日以降の仕事や体調に影響が出てしまう

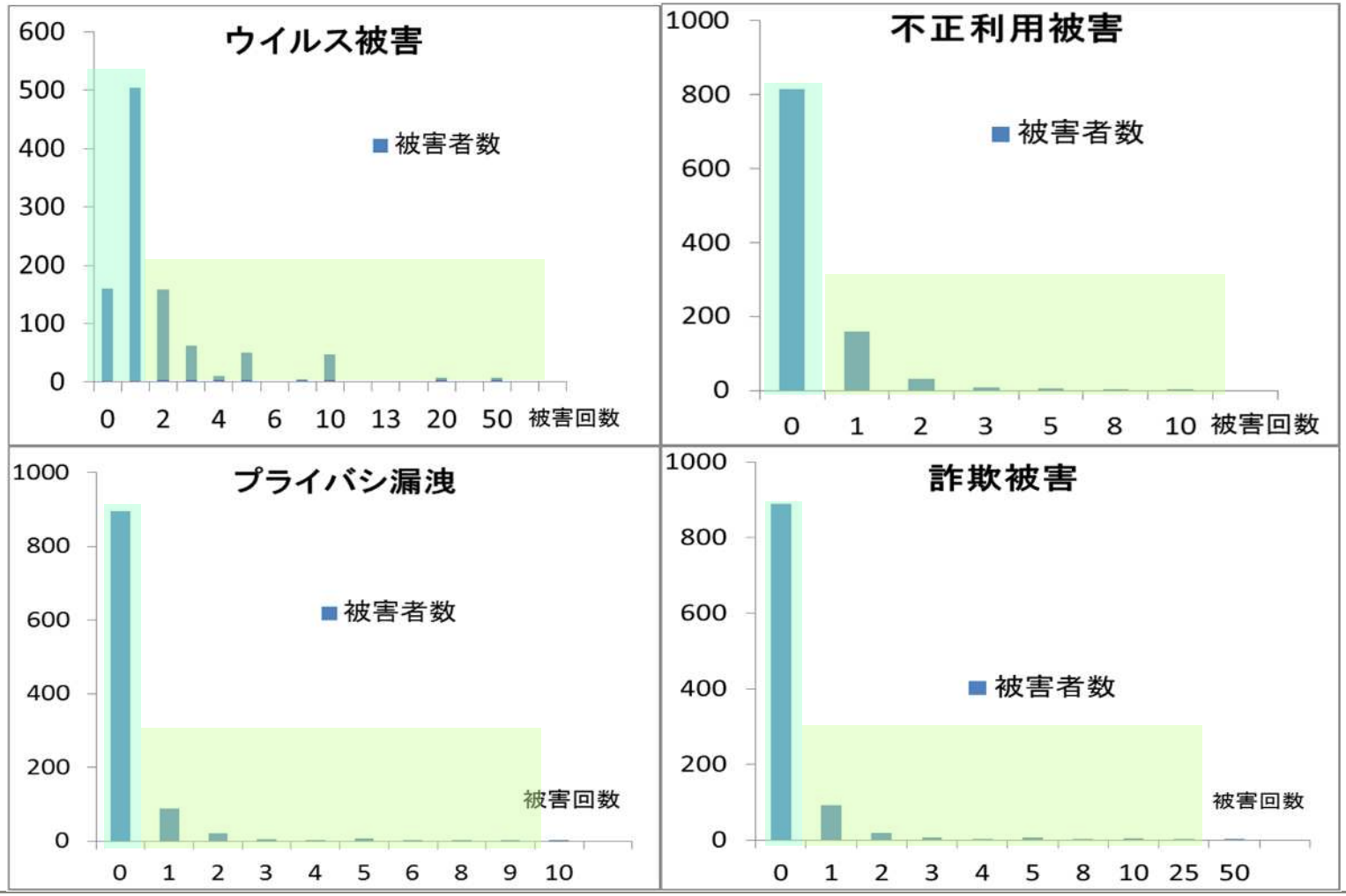
Q8_1	現状維持傾向	見たいTV番組が終わった後も、ずっとTVを見続けてしまったり、面白いwebサイトを読んだり見たりし終わった後も、ずっとネットサーフィンをしてしまうことが多い
Q8_2	損失回避傾向	欲しいものはできるだけ安く、お得に手に入れたい
Q8_3	所有欲	どうしても欲しいものは多少無理をしてでも手に入れる
Q8_4	楽観的傾向	わたしは、ふだんから気をつけているので、交通事故や犯罪に巻き込まれることはないと思う
Q8_5	流されやすさ	人から勧められたり、話を聞いて、その商品を手に入れたり、そのお店やイベントなどに行ってみたが、よくよく考えるとそんなに欲しくも行きたくもなかったなと思うことが多い
Q8_6	自制心の弱さ	街やインターネットで、その場でほしいと思った物を購入してみたが、あとで後悔することが多い

Q9	セキュリティ対策に対する心理的負担	セキュリティ対策は何をすればいいのかわからないし、面倒なのでしたくない
Q10_1	標的型攻撃についての知識(正解は○)	攻撃対象となるのは、不特定多数の一般ユーザではなく、特定の組織や特定の個人になる
Q10_2	標的型攻撃についての知識(正解は○)	攻撃者が用意したサーバから不正なプログラムをダウンロードさせるために、まずはそれを実行するため、必要なウイルスをパソコンに感染させるタイプがある
Q10_3	標的型攻撃についての知識(正解は×)	メールの差出人のアドレスや本文の内容から疑わしい要素を見つけやすいので、対策が比較的容易である
Q11_1	仕事量(自己評価)	1日でこなさなければならない案件がとても多く、残業が深夜に及ぶ
Q11_2	web接触時間その1	家に帰ってからの自由時間が少ないので、じっくりインターネットをする時間がない
Q11_3	web接触時間その2	家に帰ってからの自由時間が少ないので、インターネットよりも他のことに時間を使いたい
Q12	PC習熟度	Q12 あなたのパソコンの習熟度に近いものをお答えください。

得られたデータの分布

FUJITSU

- すべての被害経験は、被害0～1回で全体の8割を占める
  8割を「被害の少ない群」、2割を「被害の多い群」として、
  「ロジスティック回帰分析」を使って分析



分析結果の考察1: IT被害に関係する特性

FUJITSU

種別	特性	特性の内容	ウイルス感染	不正利用	プライバシ漏洩	詐欺
心理	対策の心理的負担が強い	言われた通りにセキュリティ対策をやるのが面倒	0.8	**1.3**	**1.3**	**1.2**
心理	PC習熟度の自己評価が高い	私はPCを使いこなしていると思う（＝自信過剰）	1.0	**1.3**	**1.2**	1.0
心理	ベネフィット認知が強い	リスクが多少高くても得られる利益を優先する	**1.2**	1.0	1.0	1.0
行動	現状維持傾向が強い	惰性で行動してしまうことが多い	1.0	**1.2**	**1.3**	1.0
行動	仕事量が多い	残業が深夜に及ぶ	1.0	1.0	1.0	**1.2**

枠内数字はオッズ比：被害の多い群にいる倍率に相当

- PC習熟度の自己評価が高い人は被害の多い群にいる確率が1.2-1.3倍
  - 自信過剰な人は被害が多いという先行研究（IPAなど）と一致
- ベネフィット認知、現状維持傾向の強い人は被害の多い群にいる確率が1.2倍
  - メールやwebページの内容に興味を惹かれて、怪しさを感じながらもURLをクリックして被害に遭うといった解釈ができる

分析結果の考察2: 一見予想と反する結果

FUJITSU

種別	特性	特性の内容	ウイルス感染	不正利用	プライバシ漏洩	詐欺
心理	対策の心理的負担が強い	言われた通りにセキュリティ対策をやるのが面倒	**0.8**	1.3	1.3	1.2
心理	コスト認知が低い	アプリインストール時の規約文を面倒がらずにきちんと読む	0.9	0.9	1.0	**1.2**

- 「対策の心理的負担が強い」人はウイルス感染の被害が少ない
  - 一見、対策が面倒な人はIT被害に遭いやすいと考えられる
  - しかし、ウイルス対策ソフトは、ほとんどの人が導入しているため、このような人でもウイルス感染が少ないと解釈
  - 他の脅威に関しては、分かりやすい対策がないためリスクが高いと考えられる
- 「コスト認知が低い」人は詐欺被害が多い
  - 規約文をきちんと読むような人たちは、一般的にIT被害に遭いにくいと考えられるが、実際には、詐欺被害経験が多いという結果
  - フィッシングメールも面倒がらずに読む？　など解釈は考えられるが要検討

アンケート分析まとめ

FUJITSU

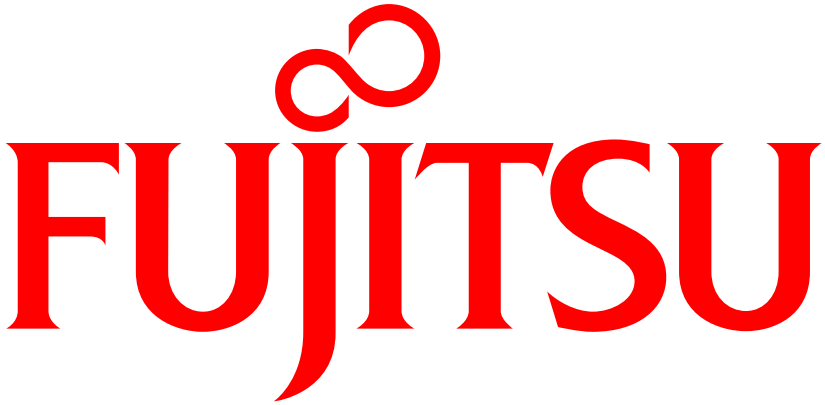
■ アンケート調査によりIT被害に遭いやすい以下の特性が得られた

特性	補足説明	結果	解釈
心理的負担が強い	言われた通りにセキュリティ対策をやるのが面倒	被害経験が多い	一般に対策が導入されているウイルス感染以外は、被害に遭いやすいと考えられる。分かりやすい対策技術が必要
コントローラビリティ:PC習熟度の自己評価が高い	私はPCを使いこなしていると思う（＝自信過剰）	被害経験が多い	IPAでも同等な結果
ベネフィット認知が強い	リスクが多少高くても利益を優先	ウイルス感染被害に遭いやすい	興味に惹かれて被害に遭う傾向。この手の人にはポリシーを厳しくするなどの対策が必要
コスト認知が低い	規約文を面倒くさがらずにきちんと読む	一般的には安全だが、詐欺被害には遭いやすい	要検討だが、ポリシーを一部緩めても良い可能性
現状維持傾向が強い	惰性で行動する	被害経験多い	適切な行動監視技術が必要
仕事量が多い	深夜残業が多い	詐欺被害に遭いやすい	より厳格なポリシー対策が必要

終わりに

FUJITSU

- セキュリティガバナンス：最後は「人」
  - 人は確実にミスをする、魔がさす
  - 行動/心理特性や、業務環境もまちまち
- ポイント、今後の展望
  - メール誤送信対策
    - 人間系は欲張りすぎず、ボリュームゾーンを狙う
    - 底上げ型のセキュリティ対策は、全員にもれなく使わせることが肝心
    - 時間帯によるリスクの変化に注意
  - 標的型メール対策
    - 部署、人によるリスクの違い
  - IT被害者分析
    - IT被害の遭いやすさに関連する心理的因子
    - 今後、アンケートではなくＰＣ操作などの行動ログから、被害に遭いやすい特徴を取り出し、人や部署に合わせた対策へとつなげていきたい。



shaping tomorrow with you

FUJITSU

shaping tomorrow with you

(ご参考)
富士通標的メール訓練サービス概要

訓練の対象となるユーザ層 (狙われやすいユーザ)

FUJITSU

対象となるユーザ

【善良な従業者】
(性善説)
- オペレーションミス
- 責任感からメールを必ず開いてしまう
- 勘違いや誤った理解

【善良な従業者】
(性弱説)
- 確認が面倒くさい
- 業務外のサイトを見たい
- 金銭的な弱み

【背景】 ・自分がターゲットになるとは思わなかった
・Excelファイルだけが感染すると思っていた
・インターネットを見ただけで影響があるとは思わなかった

【IT対策でミスを補完】
・警告の表示
・誤操作の防止
・統計処理

【ITで弱みの防止】
・過剰な権限の削除
・自動化
・相互牽制 (ワークフロー)

ITでカバーできない範囲は【人間力】で対応する
・ルール ・罰則 ★訓練

対象にならないユーザ

【悪意あり】
(性悪説)
- 金銭目的
- 困らせたい
- 犯罪に加担

【確信犯】
- 自分は正しいことをしている

標的型攻撃メールに関わらず
情報持ち出しや破壊などの
行為への対策が必要

やろうとしてもできない強固な対策が必要
・予防 ・検知

【富士通のご提案】

FUJITSU

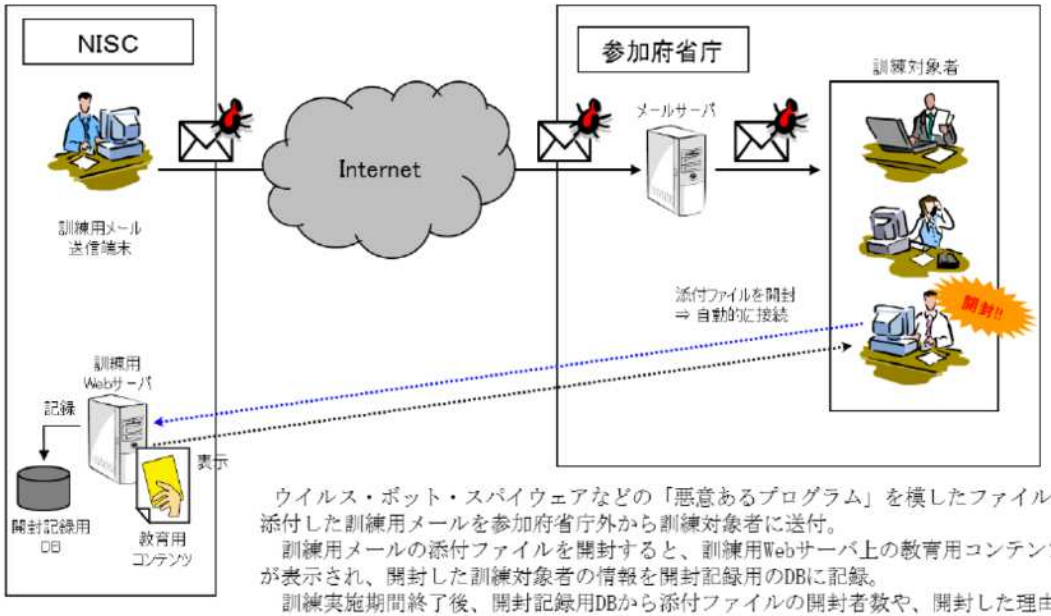
標的型攻撃メールに備えた予防訓練をご提案いたします

- 疑似的な攻撃を体験することにより、情報保護の必要性について従業者の啓発が可能です。
  - ・標的型メールの送付、アンケートの実施により効果的に従業者の意識向上が図れます。
  - ・疑似的攻撃の結果の集計により、標的型攻撃メールに対する従業者の耐性（対応力）を可視化することができます。
- 新規にハードウェア、ソフトウェアを導入することなく実施が可能です。
- JPCERT/CCによる「ITセキュリティ予防接種調査報告」に基づき実施することで、自社のセキュリティ意識のベンチマークとして活用する事ができます。

【ご参考】政府における標的型メール攻撃訓練

- 訓練期間：平成２３年１０月～１２月
- 訓練対象：内閣官房等１２の政府機関約6万名
- 訓練結果：今回の訓練における不審メールの開封率
  - 1回目（添付メール）　１０．１％
  - 2回目（リンクメール）　３．１％

- セキュリティ要件への追加（義務化）
  - 政府機関（統一基準への記載）
  - 防衛関連企業
- 他の分野へ波及
  - 政府外郭団体
  - 一般企業



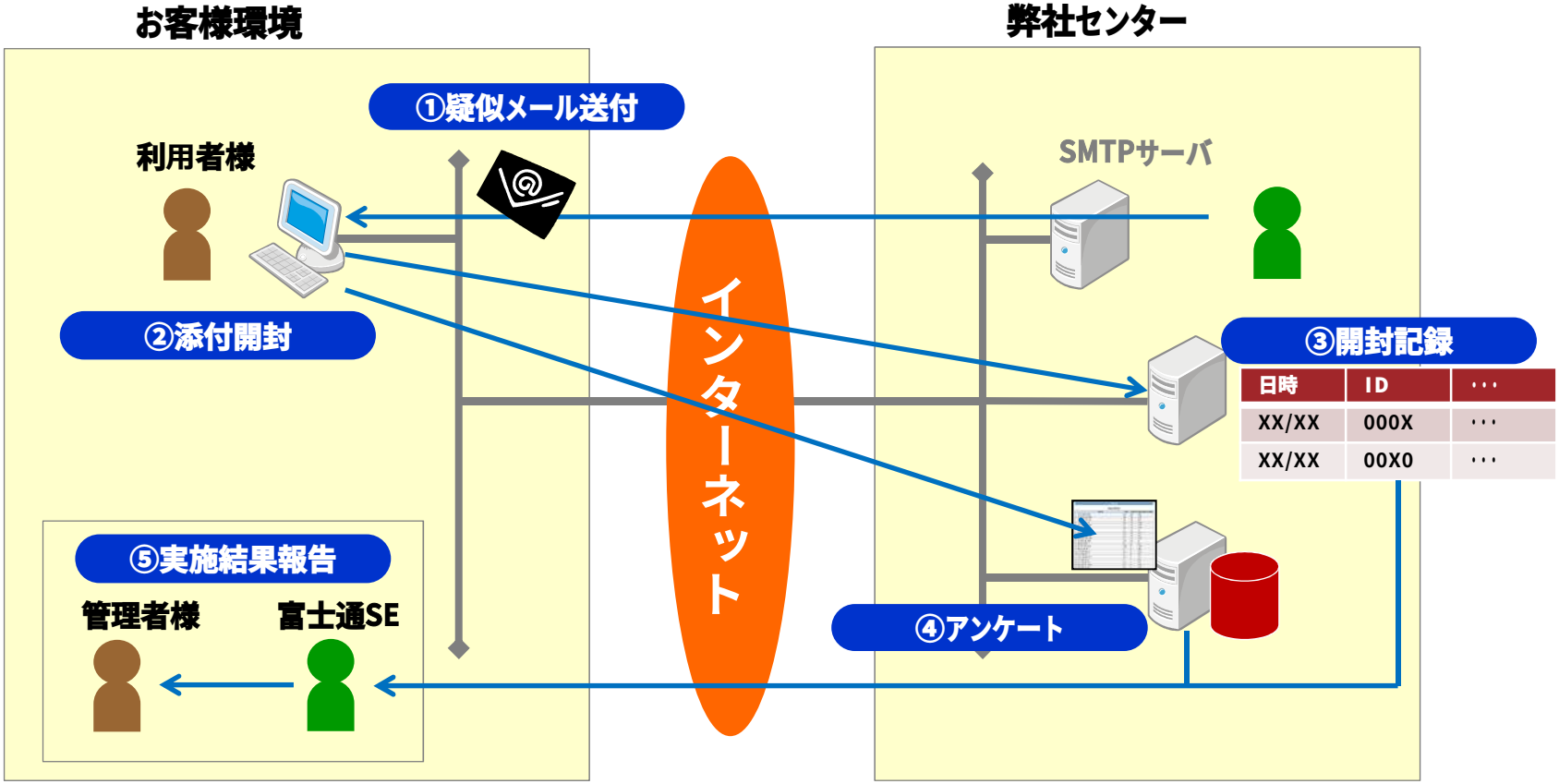
ウイルス・ボット・スパイウェアなどの「悪意あるプログラム」を模したファイルを添付した訓練用メールを参加府省庁外から訓練対象者に送付。
訓練用メールの添付ファイルを開封すると、訓練用Webサーバ上の教育用コンテンツが表示され、開封した訓練対象者の情報を開封記録用のDBに記録。
訓練実施期間終了後、開封記録用DBから添付ファイルの開封者数や、開封した理由等の教育結果を集計。

出典：内閣官房情報セキュリティセンター（NISC）報道資料

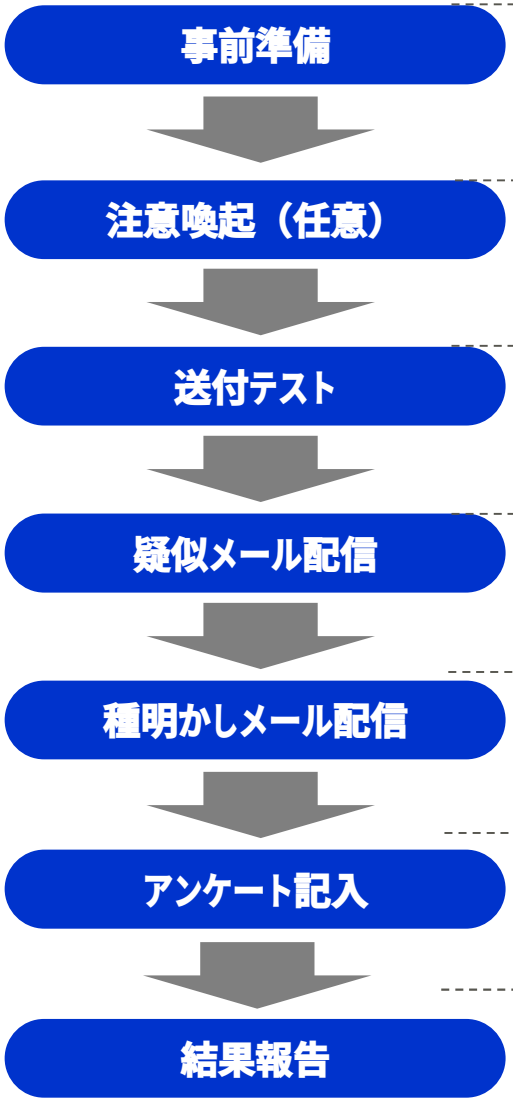
(1) サービスの概要

■訓練用に作成した疑似攻撃メールを対象者に送信し、添付ファイルの開封やURLのクリック状況を集計します。

■メールの送信環境、開封確認・集計環境は弊社がご用意いたします。



(2) サービス実施の流れ



◆各種ドキュメントの整備（メール本文、アンケート内容等）
◆システム環境の確認（SPAMフィルタ、メーラー等）
◆疑似メール送信対象者の抽出

◆利用者様へのセキュリティ注意喚起の実施（全員を対象）
※標的型メールの理解、受信した場合の対処方法、等

◆管理者様宛てへのメール送信テスト
※受信不可であった場合、SPAMフィルタルールを一時的に
変更して頂く必要があります

◆弊社センターより、対象者宛てに疑似メールを配信

◆管理者様より、対象者宛てに種明かしメールを配信
※この際に、アンケートURLへ誘導

◆利用者様より、標的型メール訓練に対するアンケートを記入
◆弊社にて、アンケート内容を集計

◆添付ファイル開封結果のご報告
◆アンケート集計結果のご報告

【ご参考】疑似攻撃メール例 (1)

FUJITSU

表題	緊急！新型インフルエンザ強毒化の恐れ
差出人	インフルエンザ対策委員 <admin@fjcert.com>
本文	新型インフルエンザの登場以来、感染力は強いものの、毒性が弱いことが指摘されて来ました。 しかし、ついに強毒型の新型インフルエンザが出現し、急速に罹患者を拡大している模様です。 そこで、各位におかれましては、添付の「すぐできるインフルエンザ対策」を参考に、改めてインフルエンザ対策を強化していただきますようにお願いいたします。 新型インフルエンザ対策は初動が大切です。日本発のパンデミック(世界流行)を起こさないために、今こそ行動が求められています。 インフルエンザ対策委員会
添付ファイル	すぐできるインフルエンザ対策.doc
気づきポイント	1. 差出人の表示名が、実在しない組織である。 2. 差出人のアドレスが外部のものである。 3. 差出人のアドレスが見慣れないものである。 4. 添付ファイルを開かせようとしている。 5. パンデミックを持ち出して急がせている。 6. 署名に所在地や連絡先などがない。

【ご参考】疑似攻撃メール例 (2)

FUJITSU

表題	大地震に対する事業継続計画の見直し
差出人	事業継続計画委員会 <bcp@fjcert.com>
本文	2009年8月1日駿河湾沖を震源とする地震により、東名高速道路牧の原地区の法面が崩落し、５日間にわたって東名高速道路が不通となった災害は記憶に新しいところです。 この事故を教訓として、我々の事業継続計画について特別見直しを行うことと決定しましたので、添付ファイルの指示に従って現状の調査にご協力をお願いします。 現状調査の項目には、独自の通勤経路(災害時の帰宅経路含む)の項目もありますので、全員の会頭が必要があります。 よろしくお願いします。
添付ファイル	事業継続計画現状確認シート3.doc
気づきポイント	1. 差出人の表示名が、実在しない組織である。 2. 差出人のアドレスが外部のものである。 3. 差出人のアドレスが見慣れないものである。 4. 添付ファイルを開かせようとしている。 5. 災害と事業継続計画を持ち出して急がせている。 6. 署名に所在地や連絡先などがない。 7. 誤字がある。(「会頭」→「回答」)