

標的型攻撃への防御対策

～FFRI YARAIについて～

株式会社アイ・シー・アイ



Internet &
Communication
Innovator

昔のハッカーは、DDoSや、Web改ざん、Bot、不特定多数への未知マルウェア攻撃など、ハッカーの腕試しや人騒がせ的なものが多かった。

一方、標的型攻撃は、金銭目的や、あるいはそのターゲットへダメージを与えることを目的として、**成功するまで特定の標的を執拗に狙うハッキング**行為。

どんな事件があったかとい
うと・・・

①

標的型メール攻撃による感染

- ✓ IPアドレス等の社内システム情報の一部
防衛省からの受注データ(装備品関係)
- ✓ 営業系サーバにおけるパスワード
- ✓ 80式空対艦誘導弾等の性能データ
- ✓ 戦闘機、ヘリコプターに関する資料
- ✓ 原子力発電所の設計や設備・耐震性など
に関する情報
- ✓ 社員2000人分の個人情報

標的型攻撃の被害事例 ②

日本航空 顧客情報管理システムへの不正アクセス概要



日本航空

ウイルス対策ソフト、ネットワーク監視システムで検知せず



合計23台のPCがマルウェアに感染

日本航空本社 22台感染



福岡市コールセンター 1台感染



本社
PC3台から送信



本社PC5台から
データを抜き出す
コマンドを実行



VIPS

(顧客情報管理システム)

JALマイレージバンク
会員情報
(約2800万件)

システム障害が2回発生
9月19日 11時半
9月22日 11時

プロキシサーバーを經由



流出した個人情報4,131件

標的型攻撃 (メール)

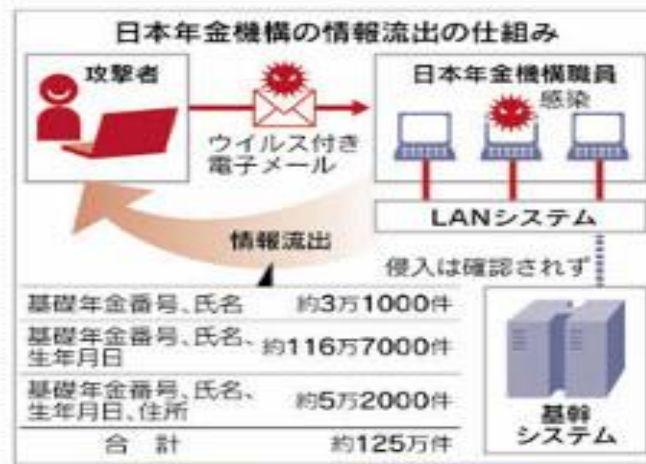


不審な接続先
(香港のIPアドレス)

発表・報道情報を元にpiyokango作成(v4)

典型的な標的型メール攻撃による感染

年金情報125万件流出



機構は国からの委託で「給付業務を担っている。公的年金の保険料徴収や今後、情報流出が確認されたら、給付業務を担っている。公的年金の保険料徴収や今後、情報流出が確認されたら、給付業務を担っている。公的年金の保険料徴収や今後、情報流出が確認されたら、給付業務を担っている。

職員、ウイルスメール開封

日本年金機構は1日、職員の端末がサイバー攻撃を受け、約125万件の年金情報が外部に流出したと発表した。いずれも加入者の基礎年金番号（3面きょうのこと）と氏名が含まれ、うち約5万2千件は生年月日や住所も流出した。国内の公的機関としては過去最大規模の情報流出。被害はさらに拡大する可能性もあり、国の情報管理のあり方に対する国民の不信が高まりそうだ。警視庁は不正アクセス禁止法違反容疑を視野に捜査する。（関連記事2、3、5面、社会面）

番号・氏名・住所 公的機関で



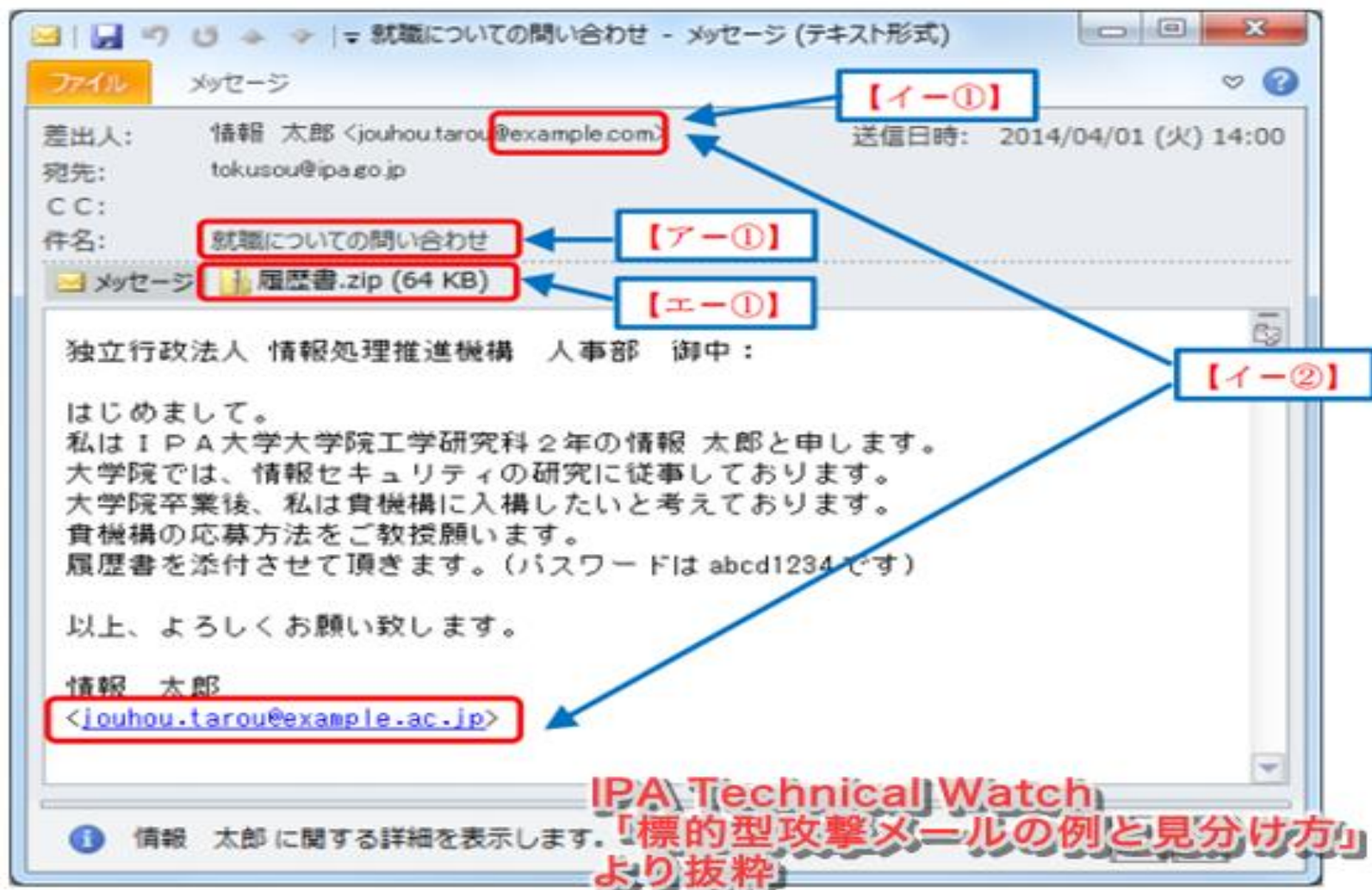
個人情報流出、記者会見
水島理事長（左）1日、厚

れた人の基礎年金番号を
変更する。現時点では基
幹システムである「社会
保険オンラインシステム」
への不正アクセスは

どんな手口なのか・・・？

それでもあなたは大丈夫？

2.2.2. 就職活動に関する問い合わせのメール



**その結果どうなって
しまうかということ・・・**

対策を怠った結果～(1)



FFRI yaraiのご紹介

FFR yarai は、従来型のアンチウイルスソフトとは異なります。

後追い技術

パターンマッチング型
アンチウイルスソフト



定義ファイルを用いてパターンマッチングにより、既知のマルウェアを

先読み技術

Yarai



定義ファイルに依存しない振る舞い防御により、未知のマルウェアも防御可能。

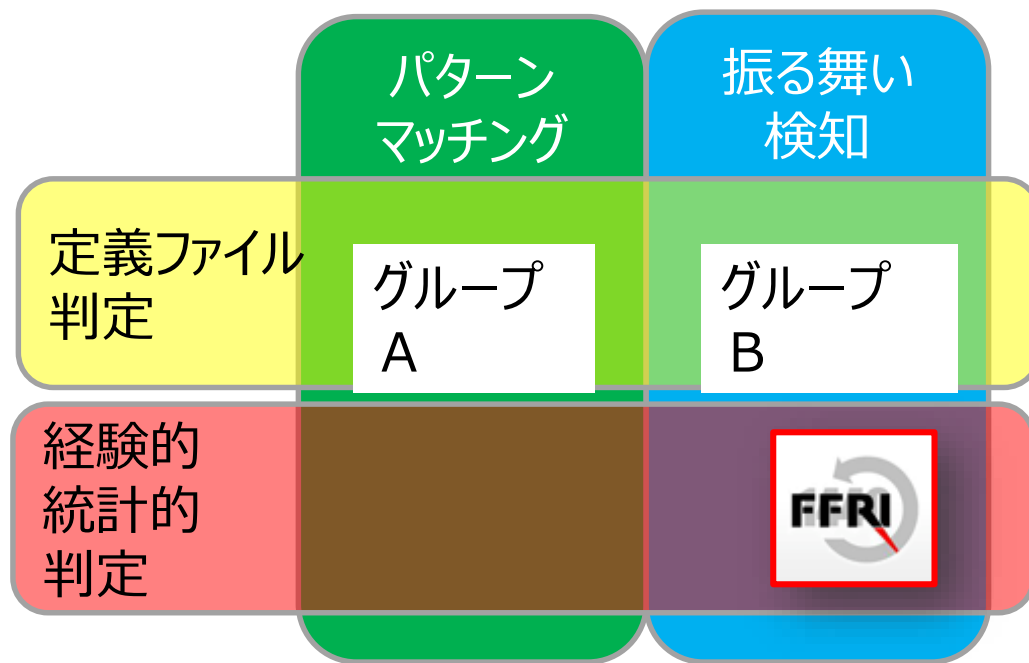
- 「不正なプログラムの動作を検知する技術」(検知手法)と
「不正かどうか判定する技術」(判定手法)の2つの技術によって防御します。

■検知手法

- パターンマッチングによる検知
- 振る舞い検知

■判定手法

- 定義ファイルによる判定
- 経験的なルールに基づく判定
- 統計的手法による判定





レベル	コンピュータ数	ライセンス価格(税別)
A	5～99	¥9,000
B	100～499	¥8,000
C	500～999	¥7,000
D	1000～4999	¥5,000
E	5000～9999	¥4,000
F	10000～	¥3,000

※1コンピュータにつき、
1ライセンス必要となります。
※マルチブートや仮想化を利用している場合は、
1OSにつき、1ライセンス必要となります。
※本製品は、1年更新のサブスクリプション
ライセンスとなります。
※2年目以降も同じライセンス価格となります。



- ▶ お問い合わせ
 - 会社名: 株式会社アイ・シー・アイ
 - メール: security@i-c-i.jp
 - 電話: 03-6459-0063
 - 担当: セキュリティコンサルティング担当