

標的型メール攻撃の概要と不審なメールを見分けるポイント

平成31年2月

東京電機大学シーサート（TDU-CSIRT）

情報セキュリティ脅威のトレンド①

■ 標的型攻撃、ビジネスメール詐欺、ランサムウェアなど、メールからの脅威が多く、情報漏えい・金銭要求等を受ける危険性が増している。

【情報セキュリティ 10大脅威 2019（組織）】

順位	セキュリティ脅威	2018年 順位
1	標的型攻撃による被害	1
2	ビジネスメール詐欺による被害	3
3	ランサムウェアによる被害	2
4	サプライチェーンの弱点を悪用した攻撃の高まり	—
5	内部不正による情報漏えい	8
6	サービス妨害攻撃によるサービスの停止	9
7	インターネットサービスからの個人情報の窃取	6
8	IoT機器の脆弱性の顕在化	7
9	脆弱性対策情報の公開に伴う悪用増加	4
10	不注意による情報漏えい	12

(参考) 情報セキュリティ10大脅威（個人）

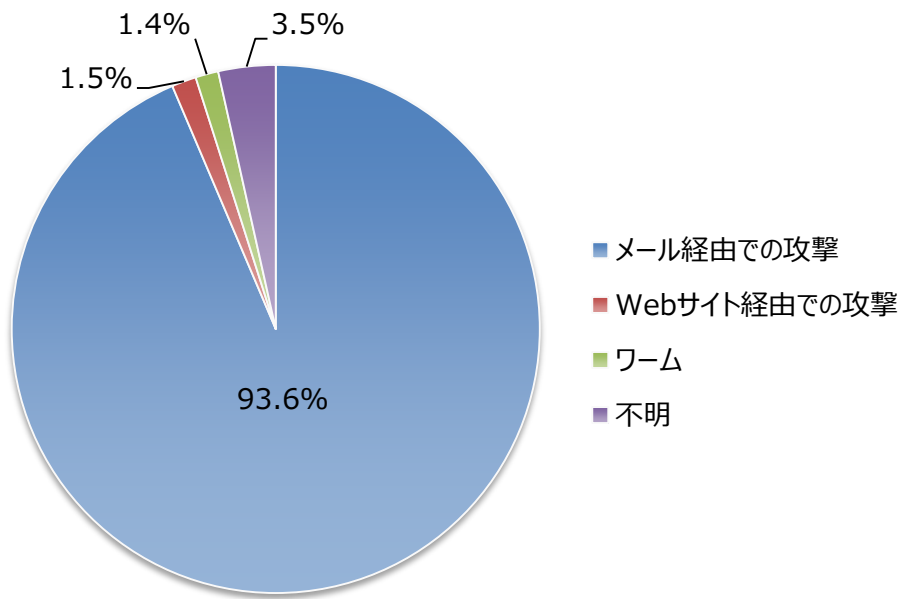
順位	セキュリティ脅威	2018年 順位
1	クレジットカード情報の不正利用	1位
2	フィッシングによる個人情報等の詐取	1位
3	不正アプリによるスマートフォン利用者の被害	4位

出典：IPA「情報セキュリティ10大脅威 2019」（2019年1月）

情報セキュリティ脅威のトレンド②

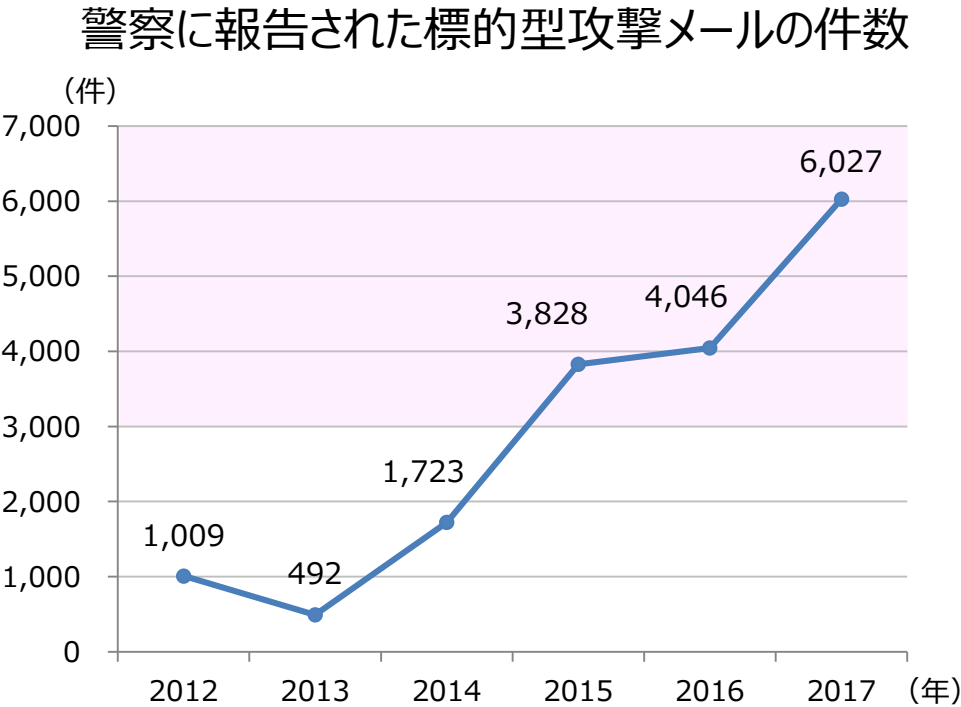
- 情報窃取をねらう標的型攻撃や、金銭を要求するランサムウェアの攻撃は「メール」をきっかけとするケースが多い。
- 標的型攻撃メールは2013年より増加傾向を示し、引き続き**大量に発生**している。

【クライアントパソコンに対する攻撃経路】



IBM「2017年上半期 Tokyo SOC 情報分析レポート」
(2017年9月) をもとに作成

【標的型攻撃メールの件数推移】



警察庁「平成29年中におけるサイバー空間をめぐる脅威の情勢等について」
(2018年3月) をもとに作成

情報セキュリティ脅威のトレンド③

- ランサムウェアは、感染したPCを**ロック**したり、**ファイルを暗号化**したりすることによって、使用不能にしたのち、元に戻すことと引き換えに「**身代金**」を**要求**する不正プログラム。
- Webサイトやメールリンクのクリック、添付ファイルの開封に注意。

【参考】ランサムウェア「WannaCry」感染時の画面

身代金の一次支払期限
(過ぎると身代金が2倍になる)

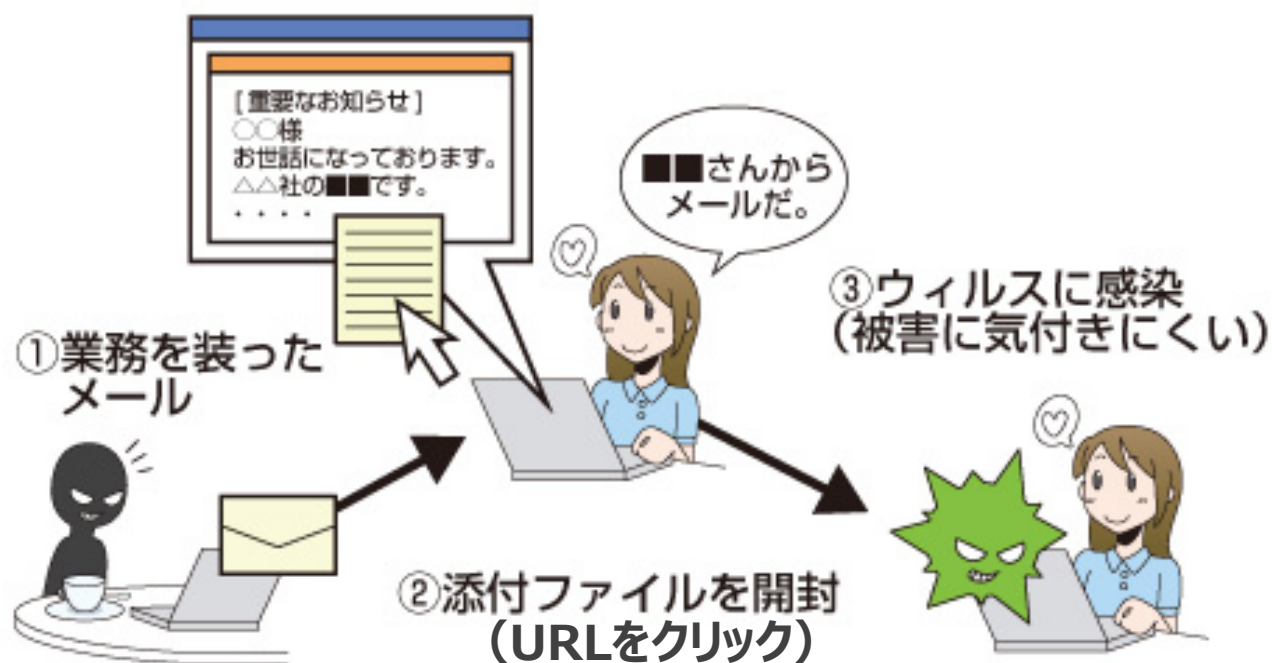
最終的な支払期限
(過ぎると復号できなくなる)



出典：トレンドマイクロ株式会社「トレンドマイクロセキュリティブログ」（2017年6月）

- 特定の企業や従業員を狙い、**一見業務に関係がありそうに見えるメールで開封を促し、添付ファイルの起動やURLクリックを誘導することでマルウェア感染**させる攻撃のこと。

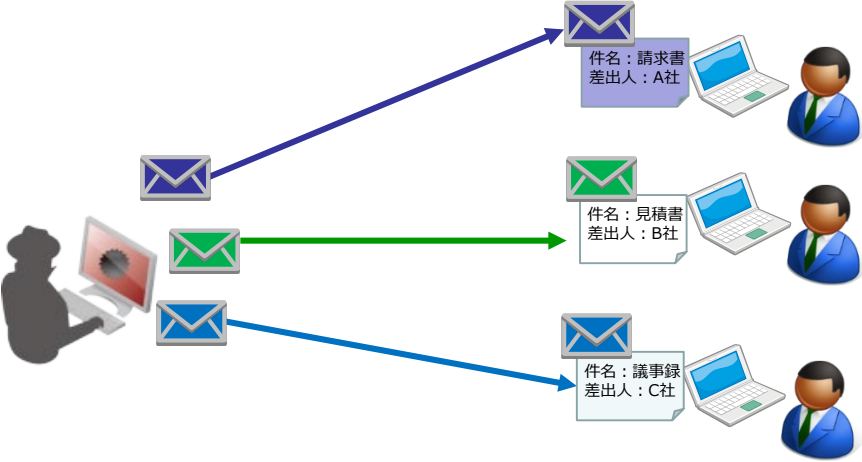
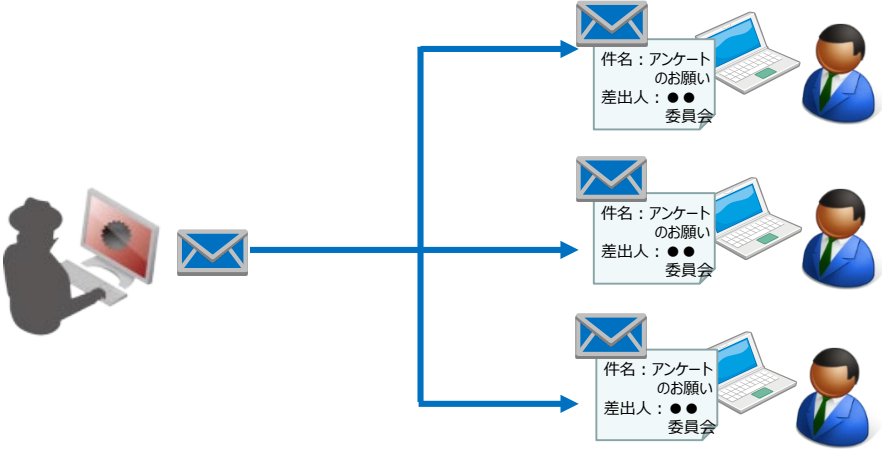
【標的型攻撃メールによるマルウェア感染】



代表的な攻撃パターン

- 代表的な攻撃パターンは「標的型」メールと「ばらまき型」メールがある。

【代表的な攻撃パターン】

	標的型メール	ばらまき型メール
イメージ		
特徴	宛先 : 特定の組織や個人 差出人表記 : 業務関係者（自社幹部、取引会社）等 送信内容 : 受信者個々に異なる 「請求書」、「見積書」、「議事録」等	宛先 : 不特定の組織や個人 差出人表記 : 実在する企業や団体名、類似した名称等 送信内容 : 宛先全員に同じメール内容 「アンケートのお願い」、「年末調整申告書差戻通知」等

マルウェア感染手法

- 標的型攻撃メールにより、社内PC等へマルウェアを感染させる主な手法は以下のとおり。
- ・ 不正なプログラムをメールに添付し、受信者が添付ファイルを開くことで感染させる
 - ・ メール本文に不正サイトのURLを記載し、受信者がサイト接続することで感染させる

	形式		攻撃例
1	添付ファイル形式	MS-Office	不正サイトのリンクを埋め込んだWordファイルを開かせ、C & C（Comand & Control）サーバに接続させることでマルウェアをダウンロード・感染させる。
2		PDF	Adobe Readerの脆弱性を悪用する不正プログラム（JavaScript等）を埋め込んだPDFファイルを開かせ、C & Cサーバに接続させることでマルウェアをダウンロード・感染させる。
3		実行形式	悪意ある実行ファイルを開かせ、C & Cサーバに接続させることでマルウェアをダウンロード・感染させる。
4	URLリンク形式		不正なWebサイトの接続先URLをメール本文に記載しクリックさせ、C & Cサーバに接続させることでマルウェアをダウンロード・感染させる。

①差出人の詐称

▶ 実際にありそうな組織名

- 差出人：個人情報保護委員会、安全作業推進委員会など

世間一般的にありそうな組織、団体など

- 差出人：総務部、情報システム部など

社内にあるような組織など

▶ 実在する官公庁名、企業、サービス等

- 差出人：総務省、経済産業省、警察庁、消防庁など

監督官庁など

- 差出人：楽天カード、Apple IDなど

世間一般的によく利用されるサービスなど

確認！

- ・これまでに届いたことのない組織、心当たりがない内容か
- ・フリーアドレスから送信されていないか
- ・決裁や配送通知（英文の場合が多い）は要注意

②添付ファイルの偽装

▶ アイコンの偽装

exeファイルを文書ファイルなどのアイコンに偽装



Keikaku.exe



業務マニュアル.exe

▶ 拡張子の偽装

拡張子の前に多くの「スペース」を挿入し本来の拡張子を画面上表示させないことで、拡張子を偽装



報告様式.doc _____ (スペース) _____ .exe

表示される拡張子

本来の拡張子

確認！

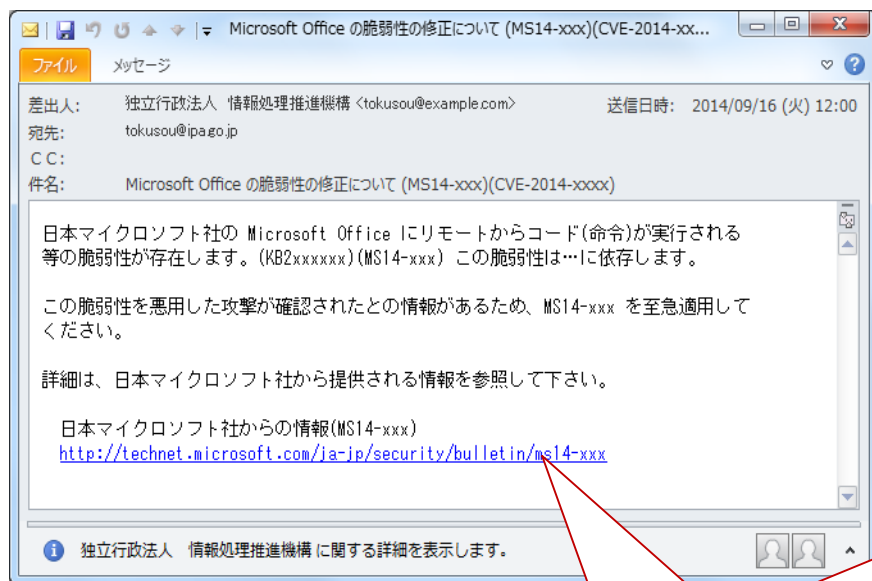
- ・実行形式ファイル拡張子ではないか(exe / scr / cpl など)
 - ・アイコンや拡張子が偽装されていないか
- 疑わしいファイルは、ファイル名の最後の表記まで確認

③URLの偽装

▶ URL表示の偽装

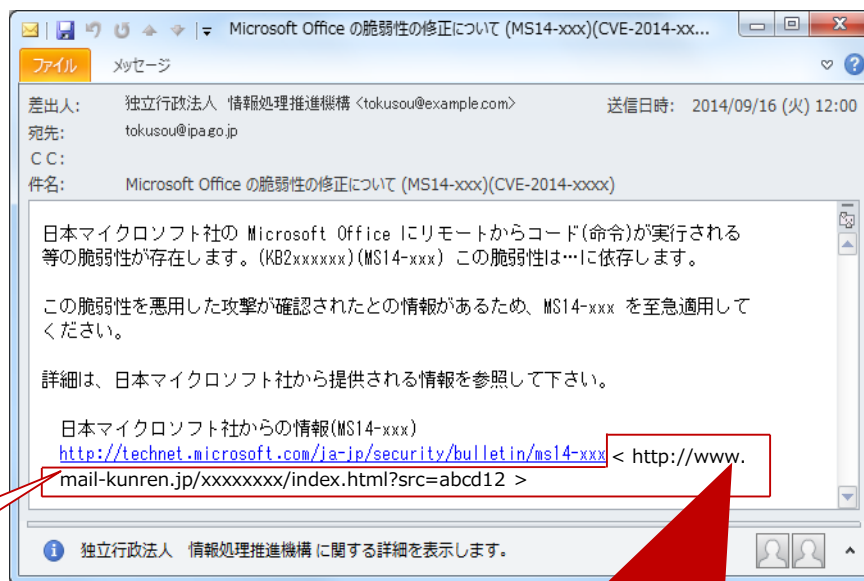
HTML形式を利用して、接続先の表示を別のURLに偽装

【HTMLで閲覧する場合】



表示されるURL

【プレーンテキストで閲覧する場合】



本来接続するURL

確認!

- ・表示されているURL（アンカーテキスト）と実際のリンク先のURL が異なっていないか（HTML メールの場合）
→プレーンテキスト表示とするのが望ましい

【参考】実際の標的型攻撃メールの例

ファイル(F) 編集(E) 表示(V) 移動(G) メッセージ(M) ツール(T) ヘルプ(H)

受信トレイ

受信 作成 チャット アドレス帳 タグ クイックフィルター

差出人 e...@dmsmbc.co.jp 2017/11/14 17:43

件名 【重要】【三井住友銀行】Web21電子認証による振込承認時のワンタイムパスワード必須化について(2017年11月目途)

宛先 y...@...
Cc y...@...nt

法人インターネットバンキングValueDoorご利用者さま

◇-----◇

いつも法人向けインターネット窓口「ValueDoor」をご利用いただきありがとうございます。

◇-----◇

お客さまにお伝えしたい事項がございますので、お知らせいたします。

詳細につきましては、法人インターネットバンキングトップからご覧いただけますよう、よろしく願い申し上げます。

▼重要 電子認証による振込承認時の「ワンタイムパスワード」必須化について(2017年11月目途)

>【法人インターネットバンキングトップはこちら】
<http://...fin.com/zswso764ezbel4051/qpsrml5585gymjfi46431jwvcy.nakam>

このメールアドレスへのメール配信を停止したい場合は

下記の手順に沿ってお手続きをお願いいたします。

法人インターネットバンキングトップの環境設定メニューから

(1)画面・メール 要否 の設定をクリックする。

(2)当行からのメールの要否設定(要・不要)を変更する。

(3)設定ボタンをクリックする。

「設定が完了しました」と表示されましたらお手続きは完了です。

下記の手順に沿ってお手続きをお願いいたします。

法人インターネットバンキングトップの環境設定メニューから

- (1)画面・メール 要否 の設定をクリックする。
- (2)当行からのメールの要否設定(要・不要)を変更する。
- (3)設定ボタンをクリックする。

「設定が完了しました」と表示されましたらお手続きは完了です。

(ご注意)

- ・本メールアドレスは送信専用です。ご返信・お問い合わせはお受けしておりません。
- ・金融機関等を装う電子メールにご注意ください。

「三井住友銀行」名でお送りするメールには、携帯電話向けを除いてすべて電子署名を付けています。電子署名の確認方法等、メールのセキュリティについては、当行のホームページをご覧ください。

2017/06/06

三井住友銀行

○三井住友銀行のソリューションセンター○

電話番号 0120-286-202

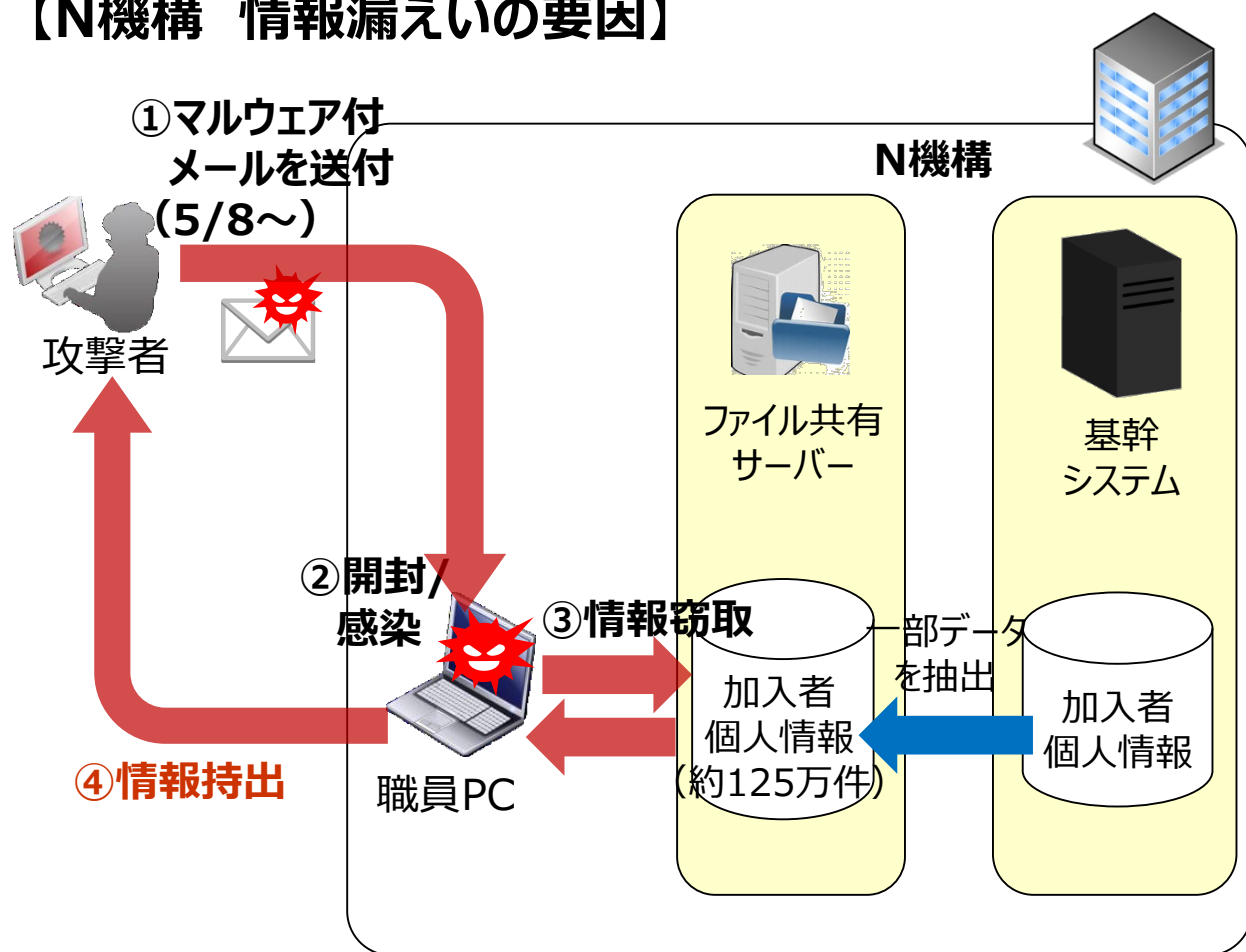
受付時間 9:00~19:00(銀行休業日を除く、月~金曜日)

【参考】外部からの攻撃によるセキュリティ事故事例

<N機構個人情報流出問題（2015年5月）>

- 巧みに業務を装った標的型攻撃メールがあり、メール開封によりマルウェアに感染した。
- 約125万件の個人情報外部へ流出した。

【N機構 情報漏えいの要因】



<N機構の被害>

加入者手帳の再発行・送付	約 4 億円
加入者問合せ対応等	約 3 億円
お詫び状送付	約 1 億円