XXXXX株式会社　御中

JCPAドキュメント・セキュリティデリバリー（DSD）のご提案

＝ 安全なセキュリティ保護を目指して ＝

一般社団法人日本コンプライアンス推進協会
Japan Compliance Promotion Association

Ver..2. 1 .6

ﾄﾞｷｭﾒﾝﾄ・ｾｷｭﾘﾃｨﾃﾞﾘﾊﾞﾘｰ(DSD) ＋ PC監視(ﾌｧｲﾔｰﾀﾜｰ)標準装備

➢委託先へのファイルを暗号化し、各種閲覧制限で 安全・簡単な送付が可能
➢パソコンのマルウェア検知と駆除で安全な情報セキュリティ環境実現
➢JCPA協会仕様にて必要な機能に限定し、使いやすく、安価に提供

簡単・安全パッケージ
年額2万4千円（税別）
※初期費用3万円～（税別）

パソコン内の標的型マルウェアを24時間／365日常時監視・検疫し、ウイルスによるパソコンからの情報漏えいを防ぐ。

委託先にファイルを提供時に暗号化し、期間指定、パスワード指定、閲覧指定など諸々の設定が簡単にできる。

強固なファイル暗号で委託先への受渡し、漏えい事故発生による2次的損失の制御も実現できる。

常時使用パソコンを監視し標的型マルウェアが動きだしたら即座にウイルス駆除する。（FireTower標準装備）

誰でも簡単な操作により、委託先からの情報漏えいを防止する。（ファイル暗号化システム装備）

暗号化は強固なAES256bit採用で安全

[特長]

☆ **パソコンのマルウェア常時検知＆駆除** 安全

➢パソコン内の安全性を４段階で表示　（青、黄色、オレンジ、赤
➢「ﾌｧｲﾔｰﾀﾜｰ」は、危険で悪意を持つプログラムからPCを常時保護します。
（ウィルスベンダーソフトの入口をすり抜けた悪質なマルウェアを検知し駆除します。）

☆ **情報漏えいに繋がる操作禁止** 簡単 安全

➢DSD暗号化システム利用時は、情報の持出しに繋がる操作を制御可
・外部送信ファイルをカプセル暗号化し安全に外部との受渡しが可能
・印刷、キャプチャ、貼付け、コピーアウトなどの持出し操作を禁止
・データの閲覧回数や閲覧可能時間の設定も可能

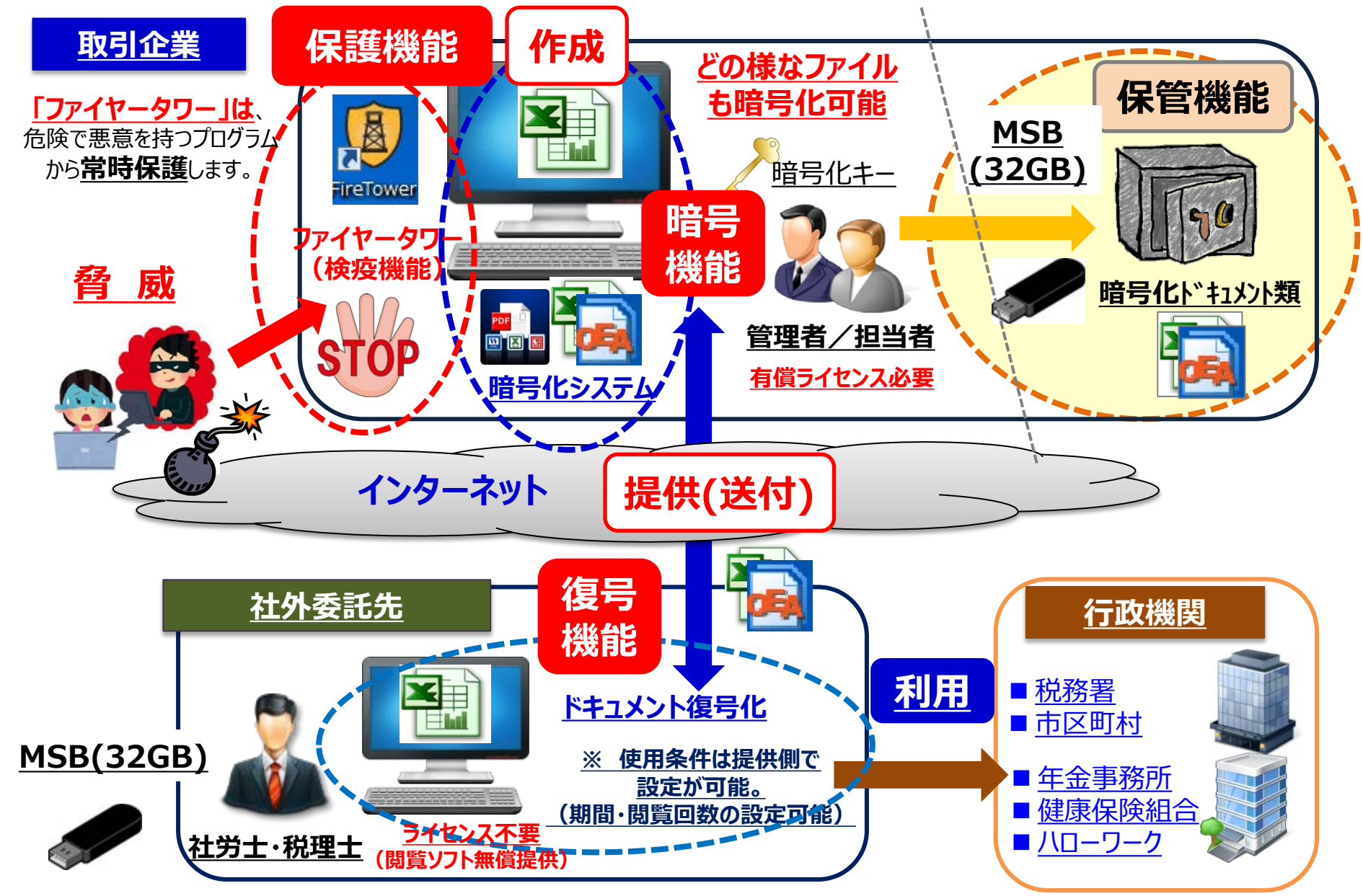
☆ **強固な暗号化実装（様々なファイル対応）** 安全

➢ＡＥＳ２５６ｂｉｔの強固な暗号化

☆ **利用者の利便性を追求した機能** 簡単 安価

➢機能を限定(JCPA協会仕様)し、運用・操作が容易
➢閲覧ｿﾌﾄ無償提供実現（協会HPより入手）
➢将来の柔軟な拡張性により、全社展開でも最小限の費用で実現可能
（ご担当のJCPA協会認定ｺﾝﾌﾟﾗｲｱﾝｽｺﾝｻﾙﾀﾝﾄにお問い合わせください。）

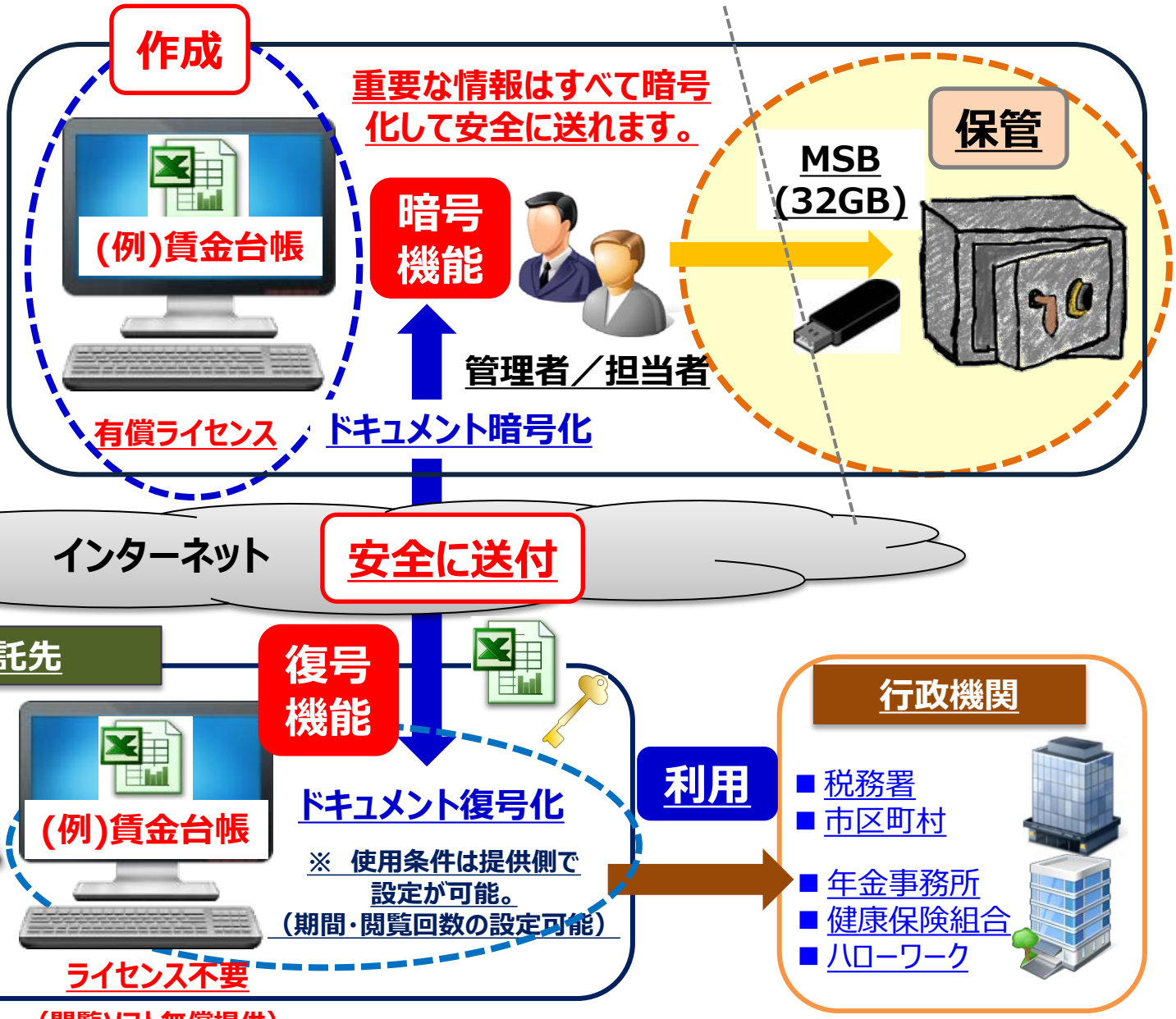
ドキュメント・セキュリティデリバリー(DSD)概要図



DSD暗号化システム利用事例（暗号機能）

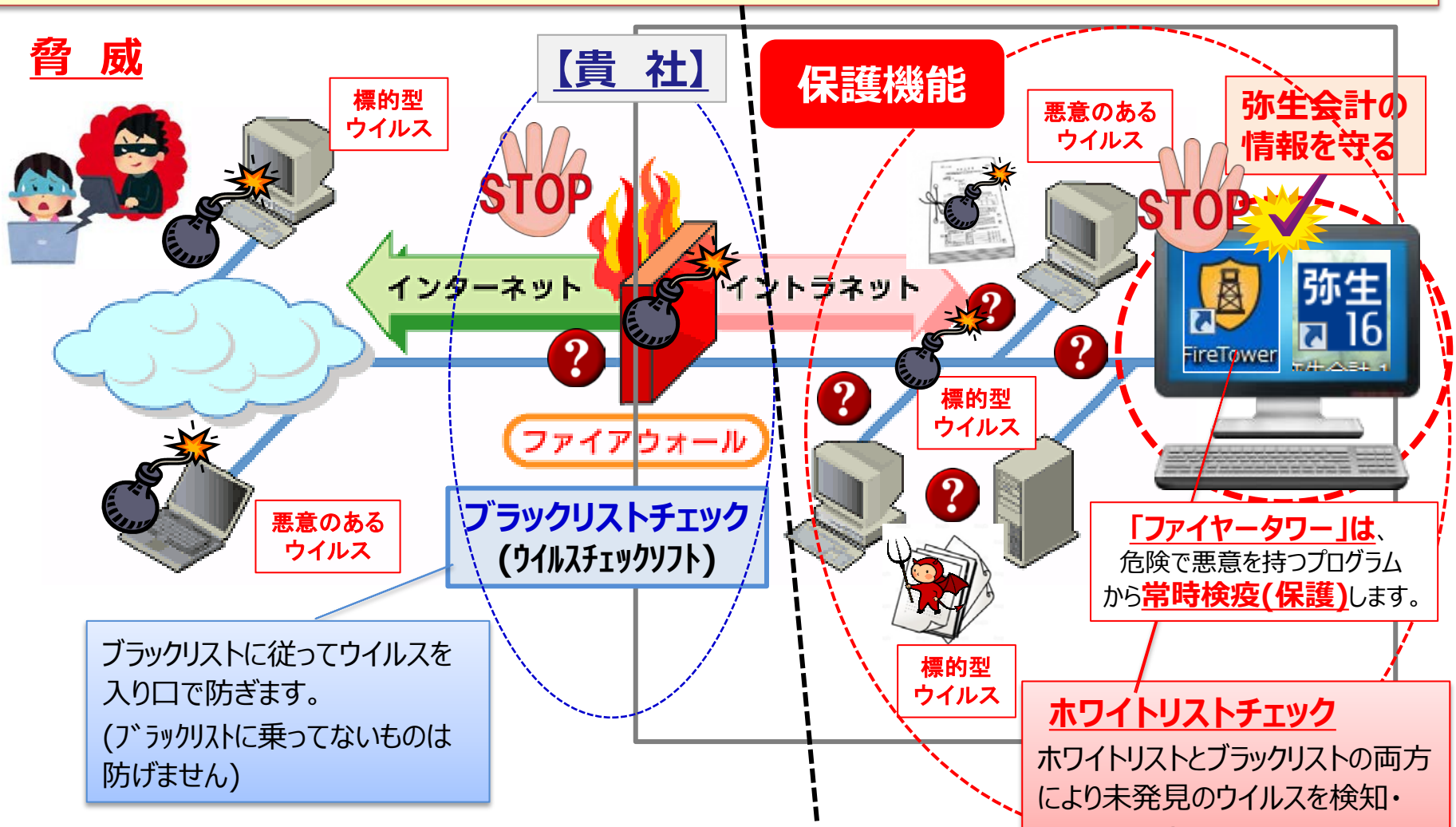
取引企業

外部送信は様々なファイルを暗号化して通常のメール送信にて外部と簡単・安全なやり取り可能。
（マイクロソフトオフィス以外にも画像・映像・音声・PDF・CAD/CAMなど設計図面など様々なファイルに対応しています。）



標的型ウィルスからの強固な防御対策事例（保護機能）

一般的な**「ウイルスチェックリスト」**はネットワークの入り口でブラックリストチェックを行い、引っかかったものは隔離する。しかしながら、
対策反映が遅れていたり、ウイルスチェックからすり抜けてきた**「標的型マルウェア」**などには全く対応ができない。
一方、今回の検疫機能**（ファイヤータワー）**は、ネットワーク内に侵入した各種マルウエアに対し検知・検疫(駆除)を実行する。



PCMCのPCチェック対象のウィルスソフトの種類

ユーザーが気が付かないうちに、ある『きっかけ』によって
悪意のあるプログラムが自動的に実行され
＜情報収集・感染・外部との通信＞による**情報漏洩**が行われます。

重大な標的型攻撃は、殆ど全てが、クライアントPC経由で継続的に実行されます。

【ウィルスの種類】

通常のウイルスソフトでは検知できないウィルスを本ソフトは、**米国の某政府機関と共同開発** した新技術により様々なウィルスを検知します。（一部紹介）

- HOME DEPO インシデント: Trojan.Backoff
  トロイの木馬、レジストリエントリを作成して、Windows が起動するたびに実行されるようにします。
- Operation Aurora: Trojan.Hydraq
  IEを含むソフトウエアの脆弱性を利用（Google, Adove 、MSその他）
- RSA Attack: Poison Ivy
  アンダーグラウンド市場で流通している伝統的な(RAT)、バックドア型マルウェアです。
- Stuxnet
  ドライバータイプのワーム、ブートプロセスを変更: 史上初のサイバー兵器
- **Backdoor.EMdivi:**
  侵入先のコンピュータでバックドアを開くトロイの木馬 ＜年金機構＞

（その他）
- Dugu Targeted Attack
- Trojan Taidoor
- Trojan.Zbot
- Infostealer.Dyranges
- W32.Cridex
- Trojan.Snifula
- Trojan.Bebloh
- Trojan.Shylock
- Trojan.Spyeye
- Trojan.Mebroot
- Trojan.Carberp
- Win32/Spy.Bebloh.A
- Trojan.Zbot
- Citadel Trojan
- Trojan.Tatanarg
- W32.Cridex
- Trojan.Ransomlock.P　など

日本年金機構の情報流出と同じ手口
JTBを襲ったのは「標的型メール」と呼ばれる攻撃だ。

2015年6月、日本年金機構は約125万件の個人情報が流出したと発表したが、これも同じ手口による攻撃が原因だった。情報セキュリティ関連企業などが繰り返し注意喚起をしているが、官公庁や大企業を中心に被害が続いている。

会見を開いたJTBの高橋広行社長

「なんの不信感もなかった」
発端は、3月15日。「i.JTB」のオペレーターが開いたメールには、ウイルスが仕組まれていた。
「なんの不信感もなかった。極めて巧妙な内容であり、やむを得なかった」
6月14日に国道交通省で開かれた会見で、金子和彦・経営企画部長（IT企画担当）は、メールの内容についてこう説明した。

件名は「航空券控え　添付のご連絡」。メールアドレスは、「ごくごく普通のありがちな日本人の苗字@実在する国内航空会社のドメイン」だった。
メールに本文はなく、PDFファイルが添付されていた。「北京行きのEチケット」。本物の可能性もある精巧なものだった。
ウイルスが仕組まれているとは気づかず、オペレーターはこのファイルを開いた。書かれていた乗客の名前をシステムで検索しても、該当する名前は見つからない。
そのままこのオペレーターは、メールの送り主に「該当はありません」と返信までしていたという。ウイルスメールだとは、最後まで気づかなかった。

「オペレーターを責められない」
返信後、すぐにエラーメールが戻ってきた。その時点でオペレーターは、異変に気付くことができなかった。
数日後、サーバー内部から海外への不正な通信が見つかった。原因として疑われたのが、このメールだった。
アドレスは間違いなく、実在する航空会社のもの。しかし、事案の発覚後、メールの詳細が記されている「ヘッダー」を確認すると、実際はレンタルサーバーから送られてきたものとわかった。アドレスは、偽造されていた。　金子部長は「一目しただけでは判断できるものではなかった」と話す。オペレータは通常業務として、航空会社とメールでやり取りをしているという。
「知らないメールを開くな、というルールはありますが、これだけでそのオペレーターを責めるには、少し無理がある」巧妙に仕組まれていたメール。「犯人」はJTBを狙っていた可能性もある。

日本年金機構の情報流出と同じ手口
2015年6月、日本年金機構は約125万件の個人情報が流出したと発表したが、これも同じ手口による攻撃が原因だった。情報セキュリティ関連企業などが繰り返し注意喚起をしているが、官公庁や大企業を中心に被害が続いている。

レポートの中でも強調されている対策は何か。コンピュータのセキュリティソフトを最新の状態に保つとともに、日々のやり取りの中で「あやしい」と感じたメールは安易に開かず、組織内のセキュリティ担当者や専門家に相談することだ。

これは、情報流出が起こるたびに言われる対策だ。しかし、日々大量のメールを扱う私たちにとって、これほど徹底することが難しい対策はないのかもしれない。