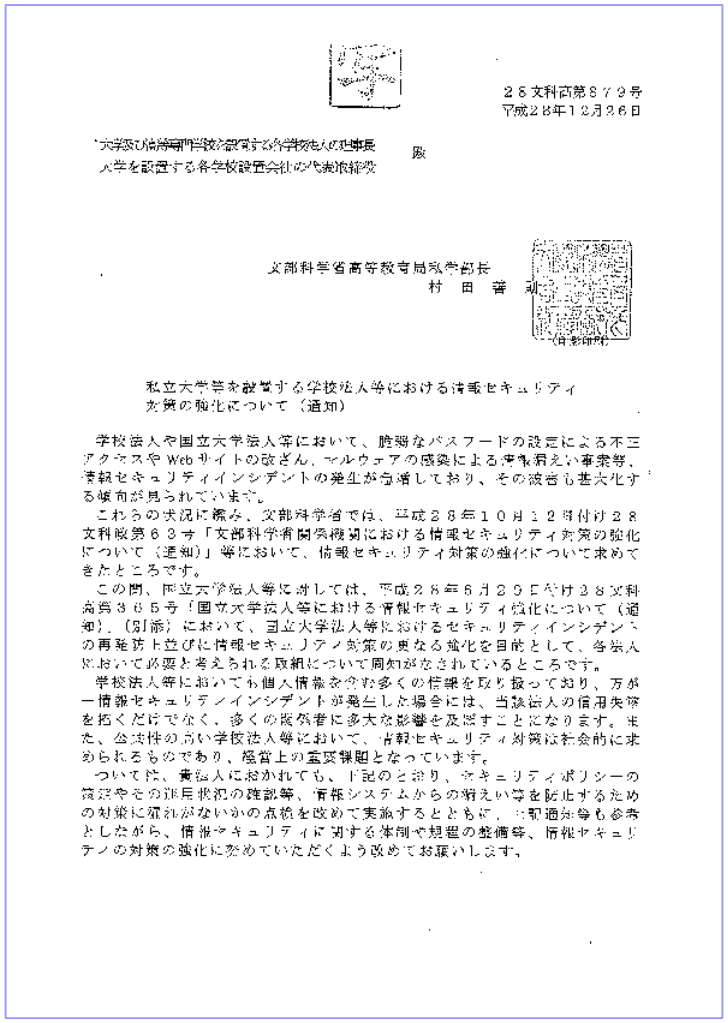
総合演習－1
S-1. インシデント対応模擬体験による問題点の整理等

文京学院大学　浜　正樹
中部大学　岡部　仁

公益社団法人　私立大学情報教育協会

目標： 文部科学省／個人情報保護委員会等の報告、情報インシデント情報公開



２８文科高第８７９号
平成２８年１２月２６日

大学及び高等専門学校を設置する学校法人の理事長
大学を設置する各学校設置会社の代表取締役　殿

文部科学省高等教育局私学部長
村　田　善　則
（公印省略）

私立大学等を設置する学校法人等における情報セキュリティ
対策の強化について（通知）

学校法人や国立大学法人等において、脆弱なパスワードの設定による不正アクセスやWebサイトの改ざん、マルウェアの感染による情報漏えい事案等、情報セキュリティインシデントの発生が急増しており、その被害も甚大化する傾向が見られています。

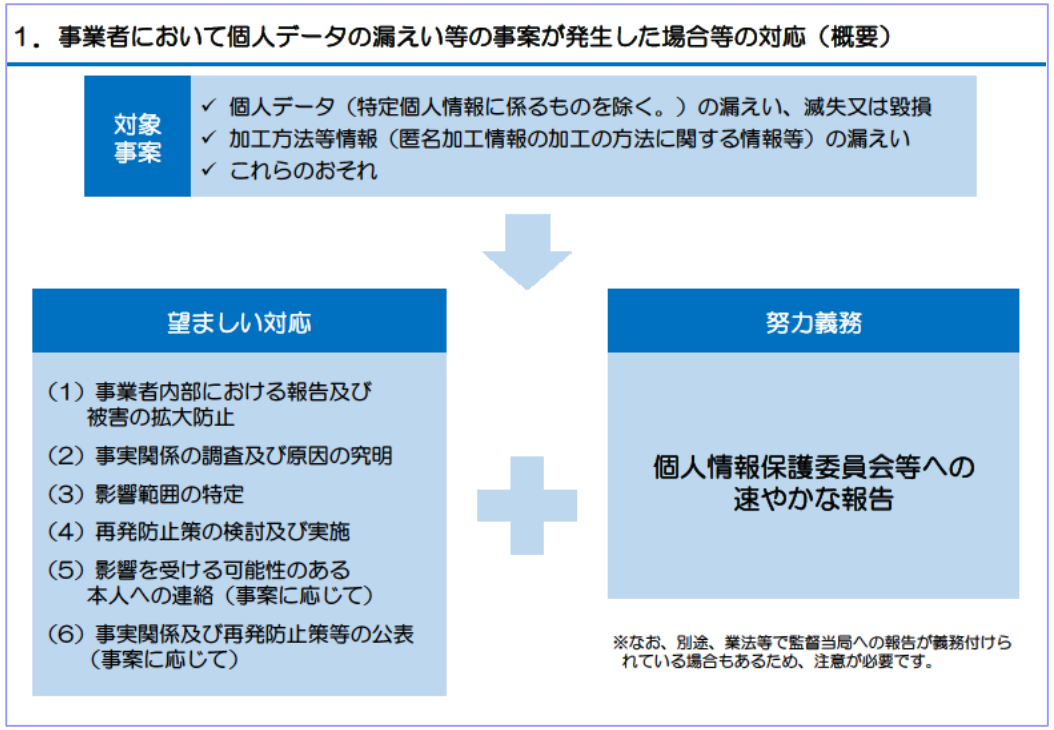
これらの状況に鑑み、文部科学省では、平成２８年１０月１２日付け２８文科振第６３号「文部科学省関係機関における情報セキュリティ対策の強化について（通知）」等において、情報セキュリティ対策の強化について求めてきたところです。

この間、国立大学法人等に対しては、平成２８年６月２９日付け２８文科高第３８５号「国立大学法人等における情報セキュリティ強化について（通知）」（別添）において、国立大学法人等におけるセキュリティインシデントの再発防止並びに情報セキュリティ対策の更なる強化を目的として、各法人において必要と考えられる取組について周知がなされているところです。

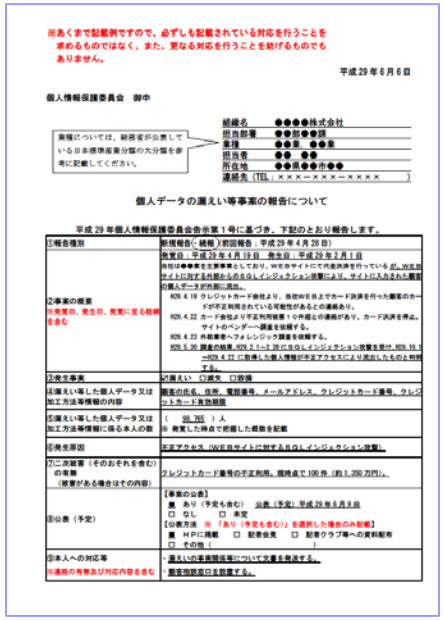
学校法人等においても個人情報を含む多くの情報を取り扱っており、万が一情報セキュリティインシデントが発生した場合には、当該法人の信用失墜を招くだけでなく、多くの関係者に多大な影響を及ぼすことになります。また、公共性の高い学校法人等において、情報セキュリティ対策は社会的に求められるものであり、極めて重要な課題となっています。

ついては、貴法人におかれても、下記のとおり、セキュリティポリシーの策定やその運用状況の確認等、情報システムからの情報漏えい等を防止するための対策に漏れがないかの点検を改めて実施するとともに、下記通知等も参考としながら、情報セキュリティに関する体制や規程の整備等、情報セキュリティの対策の強化に努めていただくよう改めてお願いします。

H281226　文部科学省通達



「対応の概要」 個人情報保護委員会



「報告書記入例」

公益社団法人　私立大学情報教育協会

このセッションの概要と目標

想定：　SJK大学の教員のPCがランサムウェアに感染

教員のPCがランサムウェアに感染しファイルが暗号化され、この情報（相談）が情報センターに届いた。

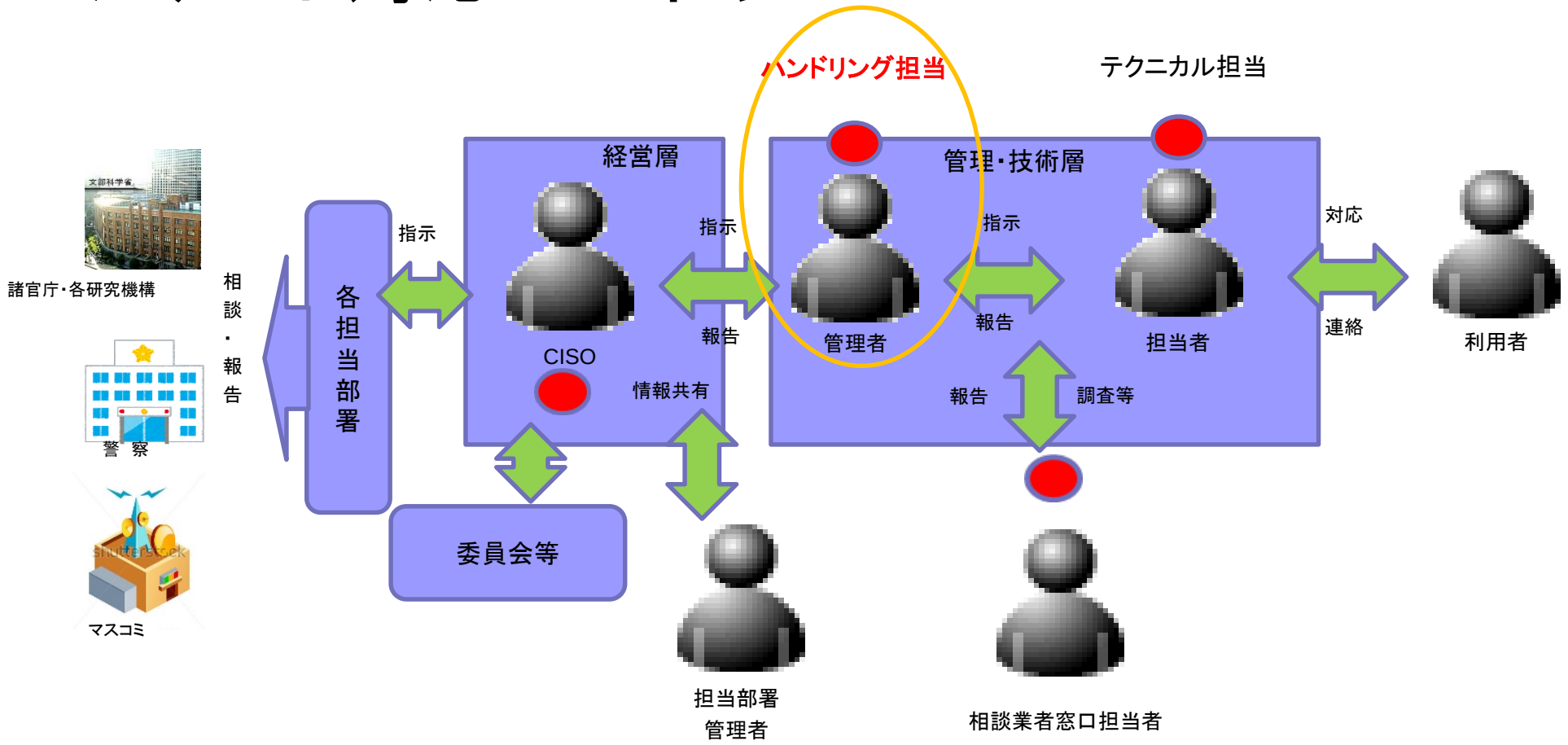
インシデントに対応する（しなければ）

ランサムウェア対応
個人情報漏えい対応

目　標

①インシデント対応を体験する。
②自組織のみで対応が可能かの確認をする。
③対応フロー・規程の作成あるいは見直しの参考とする。
④外部報告等を含めた組織的な対応体制の必要性を確認する。

インシデント対応プレイヤー



● 演習プレイヤー

テクニカル担当： セキュリティインシデント分析コース参加者
ハンドリング担当： セキュリティ政策・運営コース参加者

総合演習－1の各フェーズとスケジュール

フェーズ１:　総合演習－１について　09:30 ～ 10:00（30分）

（業者のサポート概要例）

フェーズ2：「とくかく」対応しなければ　10:00 ～ 12:00（120分）

１）各担当でワークシート記入　10:00 ～ 10:20（20分）

２）マルウェア感染時のベンダー問合せ　10:20 ～ 10:50（30分）

休憩　（10:50 ～ 11:00（10分））

３）ワークシートの交換、まとめ、提出　11:00 ～ 12:00（60分）

お昼休憩　12:00 ～ 13:00（60分）

フェーズ3：SJK大学インシデント対応フローによる対応　13:00 ～ 14:20（80分）

１） 個人情報保護委員会「報告書」の作成、CISOに報告

（SJK大学インシデント対応フロー見直し）　13:00 ～ 13:30（30分）

２）CISOの講評　13:30 ～ 13:50（20分）

３）まとめ、情報提供：「インシデント対応のコスト」 13:50 ～ 14:20（30分）

休憩　14:20 ～ 14:30（10分）

想定インシデント概要（1）

(1) SJK大学教員Aに「取材依頼」（偽）のメールが送られ、教員Aの大学管理のPCにマルウェアが感染した。

・このマルウェアは、Bozok（＝RAT）とTeslaCrypt（=ランサムウェア）との複合型。

・zipファイルを開くと、ショートカットのファイルがあり、これをクリックし感染した。ただし、感染時に動作するのはBozokのみで、TeslaCryptは実行ファイルのみパッケージであった。

・教員Aは感染に気付かず、そのままPCを使用し続けた。

(2) RATを用いて、SJK大学教員AのPC内の情報等を盗み出すことに成功した。

(3) RAT感染端末からの窃取情報が売買され、別の攻撃者が身代金目的でランサムウェアを実行した。

(4) 教員Aは、何もしていないのにPC内部のファイルが暗号化され、身代金要求画面が表示されて驚き、情報センターへ相談した。

(5) 相談を受けた情報センターは、教員AのPCの状態を確認し、暗号化されたファイルの拡張子からランサムウェアと判断した。

想定インシデント概要（2）

(6) 証拠保全と外部業者調査委託を前提に、ここでは簡易デジタル・フォレンジックとしてFastIRツールを用い行う。

(7) ランサムウェアの動作と停止、削除を行う。

(8) 幸いにも復号に関する情報が公開されていたので、暗号化されたファイルの復号を行う。

(9) 念のためPCのプロセスを調べたところ、外部のサーバ(C&Cサーバ)と不審なセッションを発見し、これによりRATに感染していることを知る。

(10) 上記の状況からイベントログを調査し、当該PCから流出したとみられるファイル名を特定する。

(11) これらの情報から報告および再防止等の事後対応を検討する。

その他の状況には、最悪の状況を想定する。

教員Aは、勤続17年で情報の専門家ではなく、3つの授業を担当、約300名の受講者がある。また、所属学科の主任補佐であり、国立研究開発法人情報通信機構（NICT）の委託研究を受託している。

フェーズ2 「とくかく」対応しなければ（ランサムウェア対応）

- 各グループでの検討
  - 自己紹介

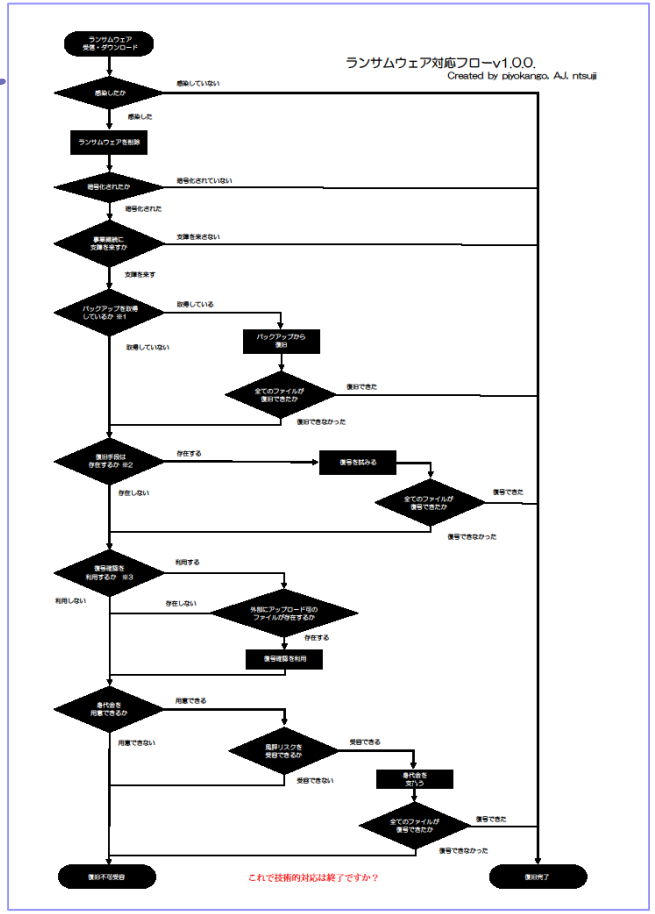
- ランサムウェア対応
  - 事実の確認、ランサムウェアの特定
  - どのようなファイルが暗号化されたか？、その被害ファイル数等
  - 復号できるか

- ランサムウェア対応フローでの対応　→　ワークシート
  - ハンドリング担当：　調査に向けた組織的対応手順と情報収集、報告等
  - テクニカル担当：　初動対応、技術的調査対応

- 情報
  - 何をしなければならないかの洗い出し
  - その方法と順番は
  - 個人情報、機密情報の流失（疑い）の有無
  - 第一報を誰が、誰にするのか
  - その他

- 対応時間制限：　成績報告締切日が3日後にあるため、これまでに調査・復旧

問題点等
をメモ



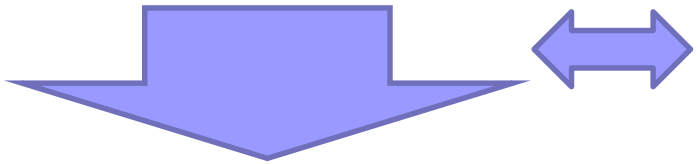
ランサムウェア対応フロー図

フェーズ2（「とにかく」対応のペアワーク）

⓪ 1グループ = テクニカルコース受講者（2名）
+ 政策・運用コース受講者（2名）

① テクニカルコース受講者ペアでワークシートを記入

①‘ 政策・運用コース受講者ペアでワークシートを記入



マルウェア感染時のベンダー問合せ

② ペア双方のワークシートを交換し、記入内容を検討

③ 双方の立場から不足分を補いグループで1枚にまとめる

→ 提出物のまとめは後日、受講生に提供

ランサムウェア対応時のワークシート記入について（テクニカル担当）

調査について

① 実際に行うべき事項と手段および結果
前日のセキュリティインシデント分析コースの体験および資料から記入してください。

② 判断で困った（迷った）事項と理由
このような作業した（する）場合に、迷った（迷うと思われる）ことがあれば記入してください。例えば、「教員自身が調査を行うこととなった場合」等

対応のため

③ 報告が求められると思われる情報、受けたい指示・注意
①の調査結果を含め、本対応で報告するべきと思う事項を記入してください。例えば、「この対応の調査は自組織のみで可能か？」、「調査人員構成」等

③ 調査の前にしなければならないこと
調査を行う前あるいは段階で判断するべき事項を記入してください。例えば、作業（調査）の順番（データ保全）、ネットワークの抜線判断等

③ 規程、ルールへの明記が必要と思う事項
調査（対応）を行う上で、必要と思う事項を記入してください。例えば、調査権限、復旧後のネットワーク接続基準等

ランサムウェア対応時のワークシート記入について（ハンドリング担当）

対応のため

① 報告が欲しい（必要な）情報

CISOへ報告に必要と思う事項を記入してください。例えば、「感染の事実・種別」、「暗号化されたファイル数と内容」等

② 担当者に行う指示、注意事項

調査担当者の人員構成、どのような調査を誰が行うのか行うか等

③ 規程、ルールへの明記

調査（対応）を行う上で、必要と思う事項を記入してください。例えば、調査権限、復旧後のネットワーク接続基準等

調査について

④ 調査項目（以下の調査項目の結果を「想定インシデント概要（P61）」、「テクニカルA-5 実習手順書」から記入してください。

- ランサムウェアの種別、処理内容
- 暗号化ファイルの復号の可否
- その他
- データ保全の有無
- 情報流失の有無

⑤ 判断事項等

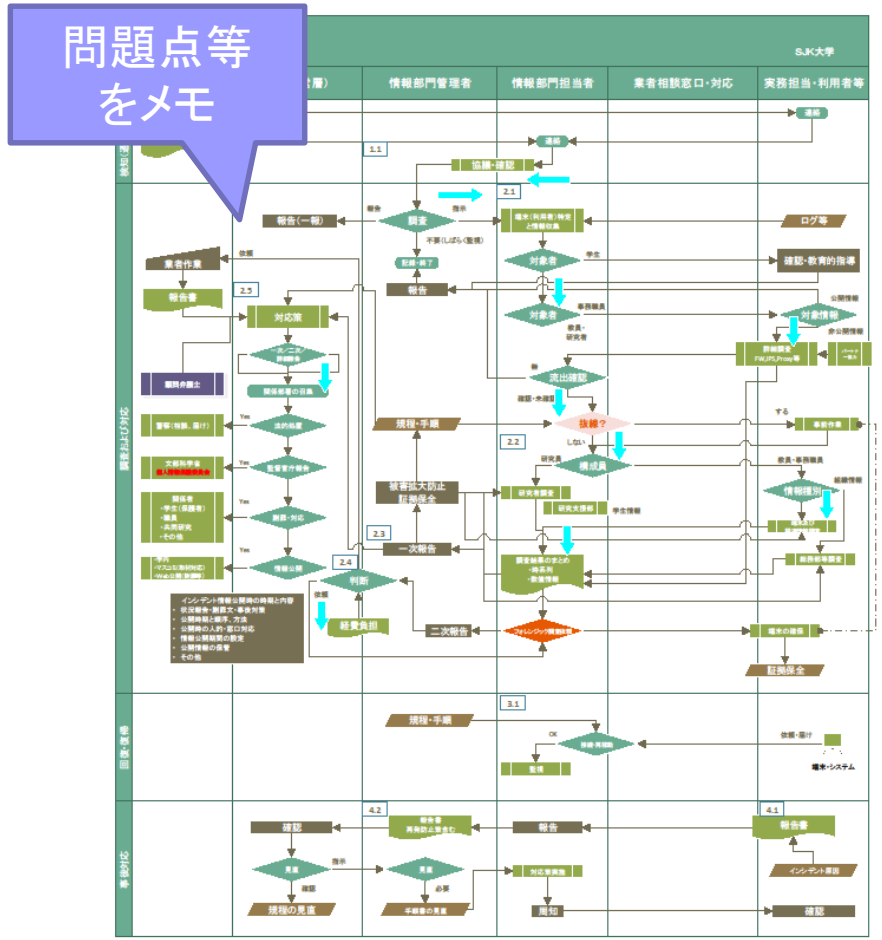
どの段階で、その程度のインシデントを判断するのか等

中間まとめ

- 初動対応
  - ネットワーク隔離（停止、再起動しない）の方法（抜線、スリープ等）と判断
  - データ保全のための準備（ツール、手順と保存媒体）と作業順序（初めに）
- 調査対応
  - 規程、ルールが整備され、以下のようなことが明記されることが望ましい
    - 調査体制（複数）
    - 事実の確認、調査の目的、方法の説明と承諾
    - 調査作業によるリスクの説明と承諾
  - 情報
    - 情報流失（疑い含む）の有無、「有」の場合、内容と数
    - インシデント発生の経緯と要因等（今後の再発防止策）
- 報告
  - CISOへの一次報告
  - 外部報告と情報公開の判断、およびその対応部署（者）、対応窓口など

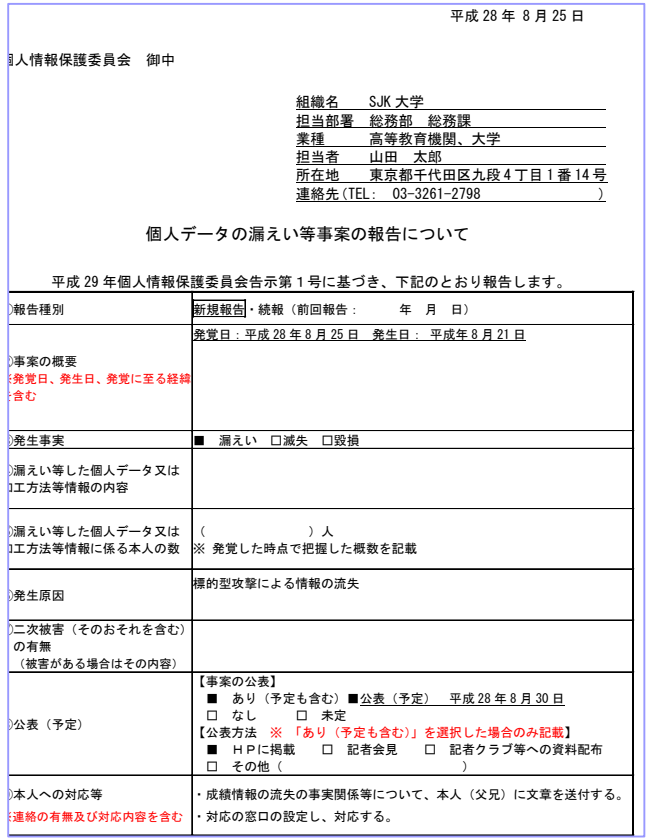
フェーズ3　SJK大学インシデント対応フローによる対応（個人情報漏えい対応）

- PCのプロセスを調べ、外部のサーバ(C&Cサーバ)と不審なセッションを発見し、これによりRATの感染を確認する。
- イベントログを調査し、当該PCから流出したとみられるファイル名を特定する。
- 事実の確認と担保情報の再確認のため、SJK大学インシデント対応フローに沿って対応する。
- **<u>個人情報の流失があったとし、個人情報保護委員会への報告書を作成し、CISOに提示する。</u>**



SJK大学インシデント対応フローによる対応

- 個人情報漏えいの対応（グループ）
  - ワークシート参考
- 文部科学省、個人情報保護委員会への相談、報告
  - 個人情報保護委員会報告書の作成
    ハンドリング担当者の問いにテクニカル担当者が返答、理解し、記入
  - CISO（運営委員）への報告、提出（挙手）
  - CISOからの質問に返答
  - SJK大学インシデント対応フロー見直し
- 報告書
  - 各グループの報告書をまとめ、共有



平成 28 年 8 月 25 日

個人情報保護委員会　御中

組織名　SJK 大学
担当部署　総務部　総務課
業種　高等教育機関、大学
担当者　山田　太郎
所在地　東京都千代田区九段 4 丁目 1 番 14 号
連絡先（TEL：　03-3261-2798　）

個人データの漏えい等事案の報告について

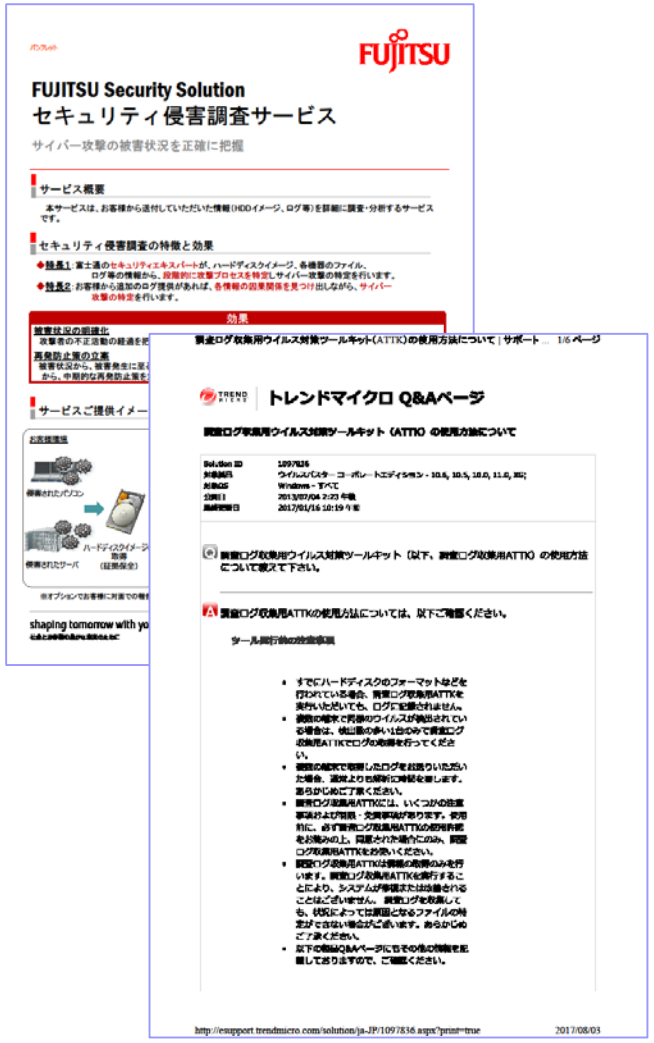
平成 29 年個人情報保護委員会告示第 1 号に基づき、下記のとおり報告します。

)報告種別	新規報告・続報（前回報告：　年　月　日）
)事案の概要 :発覚日、発生日、発覚に至る経緯 :含む	発覚日：平成 28 年 8 月 25 日　発生日：　平成年 8 月 21 日
)発生事実	■　漏えい　□滅失　□毀損
)漏えい等した個人データ又は 工方法等情報の内容	
)漏えい等した個人データ又は 工方法等情報に係る本人の数	（　　）人 ※ 発覚した時点で把握した概数を記載
)発生原因	標的型攻撃による情報の流失
)二次被害（そのおそれを含む） の有無 （被害がある場合はその内容）	
)公表（予定）	【事案の公表】 ■　あり（予定も含む）■公表（予定）　平成 28 年 8 月 30 日 □　なし　　□　未定 【公表方法　※「あり（予定も含む）」を選択した場合のみ記載】 ■　ＨＰに掲載　　□　記者会見　　□　記者クラブ等への資料配布 □　その他（　　）
)本人への対応等 :連絡の有無及び対応内容を含む	・成績情報の流失の事実関係等について、本人（父兄）に文章を送付する。 ・対応の窓口の設定し、対応する。

個人情報保護委員会報告書

インシデント対応に必要なもの

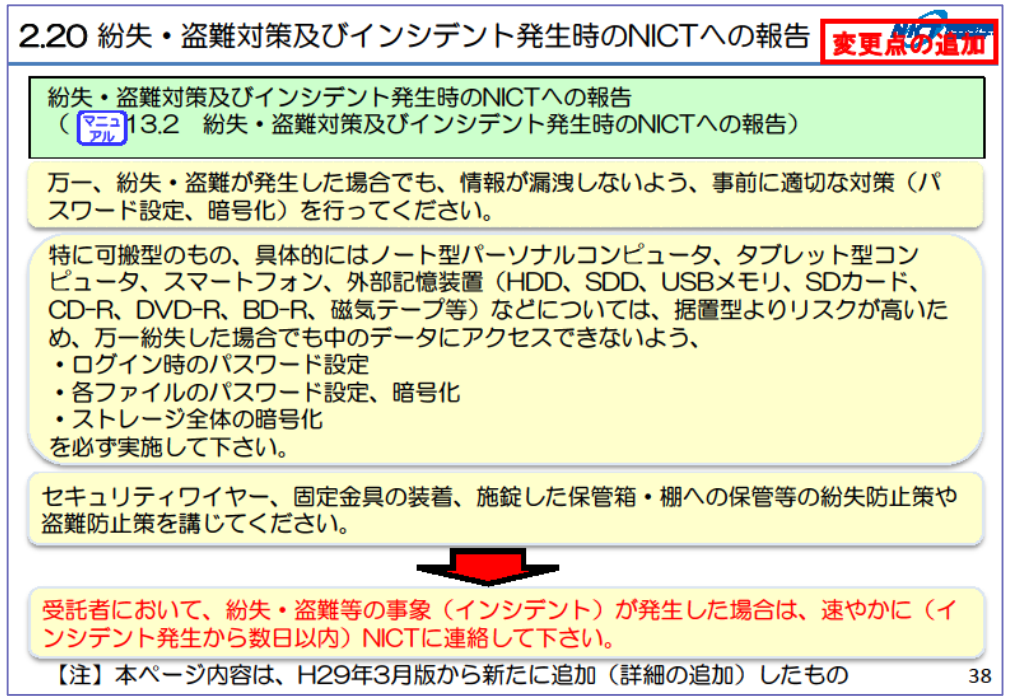
- インシデントの発生（事前兆候）の情報の窓口と学内外へ公表
- CSIRT（全学的対応非常設組織）とSOC（情報担当部門）
- インシデント対応が、自組織のみで短時間で適切な情報収集ができるか？
- できない場合の、事前の対応を業者の確保（秘密保持契約）と予算
- 報告、公表の事前準備



フェーズ4： まとめ

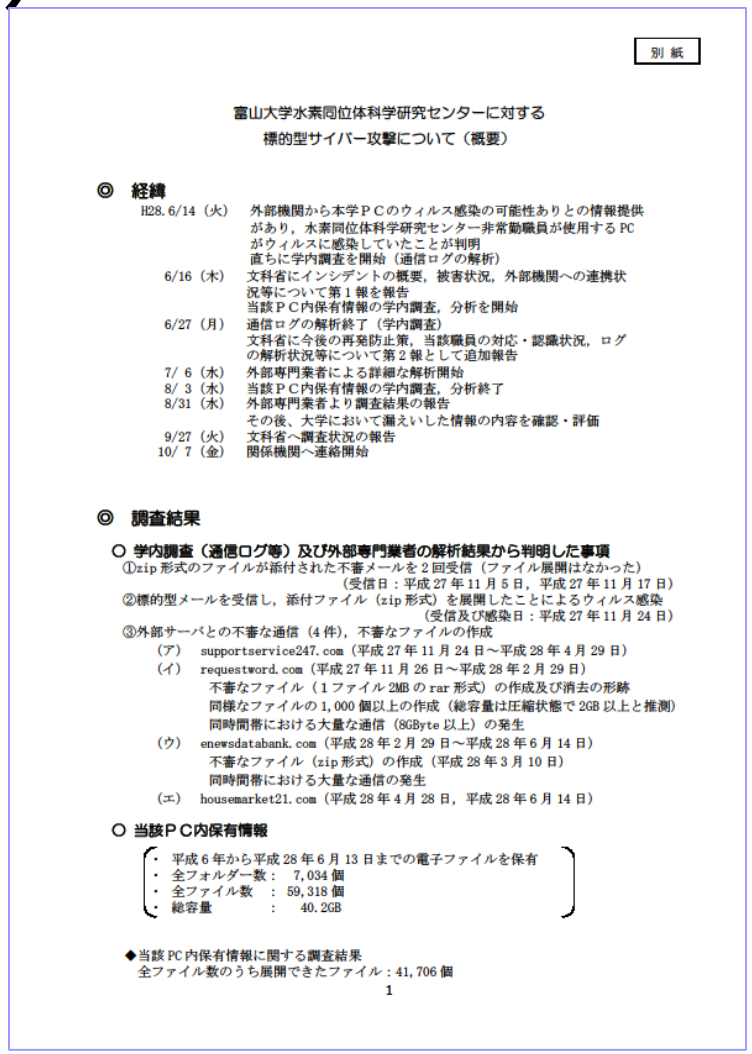
- 文部科学省への報告
  - 文部科学省高等教育局 私学部私学行政課企画係　03-6734-2527
    E-mail sigakugy@mext.go.jp

- 関係機関等への報告（NICT）



文部科学省への報告（富山大学報告事例）

- 文部科学省への報告後に情報公開
- 大学は被害者、加害者？
- 何処に（誰に）どのように報告するのか？
- 警察に相談・被害届を出すのか？
- どのような情報を公開するのか？
- 今後の再発防止策の検討
  - 技術的対応
  - 組織体制対応
  - 教育的対応
- その他



別紙

富山大学水素同位体科学研究センターに対する
標的型サイバー攻撃について（概要）

◎ 経緯

H28. 6/14（火） 外部機関から本学ＰＣのウィルス感染の可能性ありとの情報提供があり，水素同位体科学研究センター非常勤職員が使用するPCがウィルスに感染していたことが判明
直ちに学内調査を開始（通信ログの解析）
6/16（木） 文科省にインシデントの概要，被害状況，外部機関への連携状況等について第１報を報告
当該ＰＣ内保有情報の学内調査，分析を開始
6/27（月） 通信ログの解析終了（学内調査）
文科省に今後の再発防止策，当該職員の対応・認識状況，ログの解析状況等について第２報として追加報告
7/ 6（水） 外部専門業者による詳細な解析開始
8/ 3（水） 当該ＰＣ内保有情報の学内調査，分析終了
8/31（水） 外部専門業者より調査結果の報告
その後、大学において漏えいした情報の内容を確認・評価
9/27（火） 文科省へ調査状況の報告
10/ 7（金） 関係機関へ連絡開始

◎ 調査結果

○ 学内調査（通信ログ等）及び外部専門業者の解析結果から判明した事項

①zip 形式のファイルが添付された不審メールを２回受信（ファイル展開はなかった）
（受信日：平成 27 年 11 月 5 日，平成 27 年 11 月 17 日）
②標的型メールを受信し，添付ファイル（zip 形式）を展開したことによるウィルス感染
（受信及び感染日：平成 27 年 11 月 24 日）
③外部サーバとの不審な通信（4 件），不審なファイルの作成
（ア） supportservice247.com（平成 27 年 11 月 24 日～平成 28 年 4 月 29 日）
（イ） requestword.com（平成 27 年 11 月 26 日～平成 28 年 2 月 29 日）
不審なファイル（１ファイル 2MB の rar 形式）の作成及び消去の形跡
同様なファイルの 1,000 個以上の作成（総容量は圧縮状態で 2GB 以上と推測）
同時間帯における大量な通信（8GByte 以上）の発生
（ウ） enewsdatabank.com（平成 28 年 2 月 29 日～平成 28 年 6 月 14 日）
不審なファイル（zip 形式）の作成（平成 28 年 3 月 10 日）
同時間帯における大量な通信の発生
（エ） housemarket21.com（平成 28 年 4 月 28 日，平成 28 年 6 月 14 日）

○ 当該ＰＣ内保有情報

・ 平成 6 年から平成 28 年 6 月 13 日までの電子ファイルを保有
・ 全フォルダー数： 7,034 個
・ 全ファイル数 ： 59,318 個
・ 総容量 ： 40.2GB

◆当該 PC 内保有情報に関する調査結果
全ファイル数のうち展開できたファイル：41,706 個

1

富山大学水素同位体科学研究センターに対する 標的型サイバー攻撃について（概要）
https://www.u-toyama.ac.jp/news/2016/doc/1011.pdf

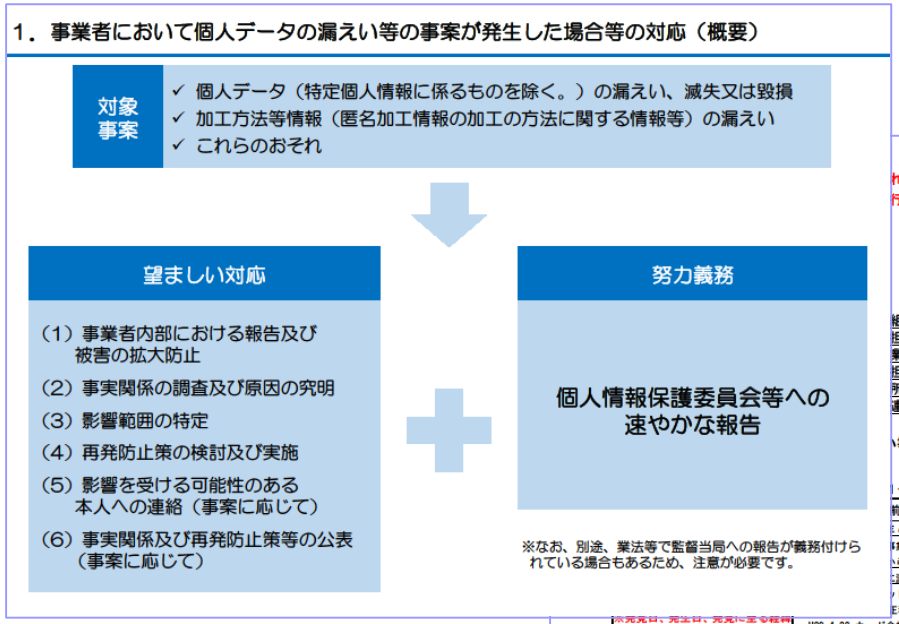
個人情報保護委員会

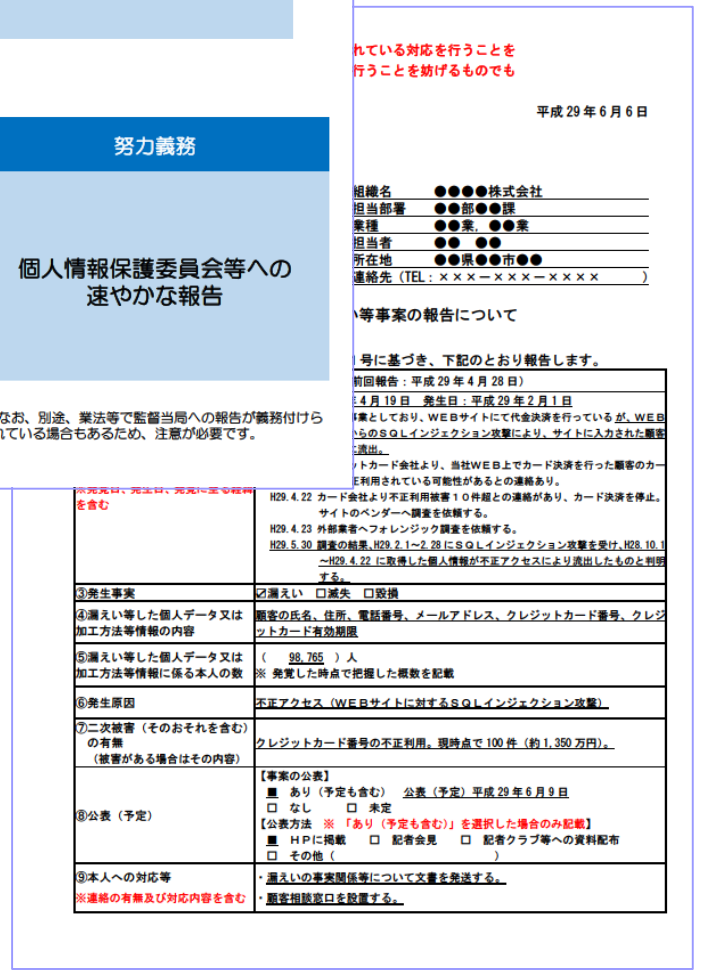
- 個人情報の漏えい等の事案が発生した場合等の対応（概要）

https://www.ppc.go.jp/files/pdf/170530_rouei_gaiyou.pdf

- FAX, メール誤送信は、軽微で報告不要！

- 報告書記入例





サイバー攻撃特別捜査隊（2017/07/27）

- 愛知県警本部 警備部 警備総務課
  - サイバー攻撃対策にかかる大学と警察の連携
  - 所轄警察署（生活安全課）から
- 13都道府県に設置
- 「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」及び「石油」の13分野の次に大学（高等学術研究機関）
- 相談から被害届（捜査）
- サイバーフォースセンター（調査・分析）

第２章　サイバー攻撃情勢

サイバー攻撃

情　勢

近年、国内外において政府機関等に対するサイバー攻撃が続発しています。重要インフラの基幹システムを機能不全に陥れ、社会の機能を麻痺させてしまうサイバーテロや、情報通信技術を用いた諜報活動であるサイバーインテリジェンス（サイバーエスピオナージ）の脅威は、国の治安、安全保障及び危機管理に影響を及ぼしかねない問題となっています。サイバー攻撃には、①攻撃の実行者の特定が難しい、②攻撃の被害が潜在化する傾向がある、③国境を容易に越えて実行可能であるといった特徴があり、我が国においても、サイバー空間の脅威に対する対処能力の強化が求められています。

サイバー攻撃の手口としては、攻撃対象のコンピュータに複数のコンピュータから一斉に大量のデータを送信して負荷を掛けるなどして、そのコンピュータによるサービスの提供を不可能にするＤＤｏＳ攻撃(注)や、セキュリティ上のぜい弱性を悪用してコンピュータに不正に侵入し、又は不正プログラムに感染させることなどにより、管理者や利用者の意図しない動作をコンピュータに命令する手法等があります。不正プログラムに感染させる手口として、業務に関連した正当な電子メールを装い、市販のウイルス対策ソフトでは検知できない不正プログラムを添付した電子メール（標的型メール）を送信し、受信者のコンピュータを不正プログラムに感染させる標的型メール攻撃があり、我が国においても多数発生しています。

DDoS攻撃　　標的型メール攻撃

サイバー攻撃の手口

近年、攻撃対象のコンピュータに不正プログラムを感染させる手口が巧妙化しています。平成28年上半期に警察が把握した標的型メール攻撃は1,951件であり、前年同期比で約1.3倍に増加しています。このうち約８割を非公開のメールアドレスに対する攻撃が占めており、また、送信元メールアドレスについて攻撃対象の事業者等や実在する事業者等のメールアドレスを詐称したものが多数確認されるなど手口の巧妙化がうかがわれます。

(注)：Distributed Denial of Serviceの略。

―8―

警察庁 焦点 第286号より

https://www.npa.go.jp/bureau/security/publications/syouten/syouten286/index.html

終わりに

- 協力
  - トレンドマイクロ
  - JPCERT/CC