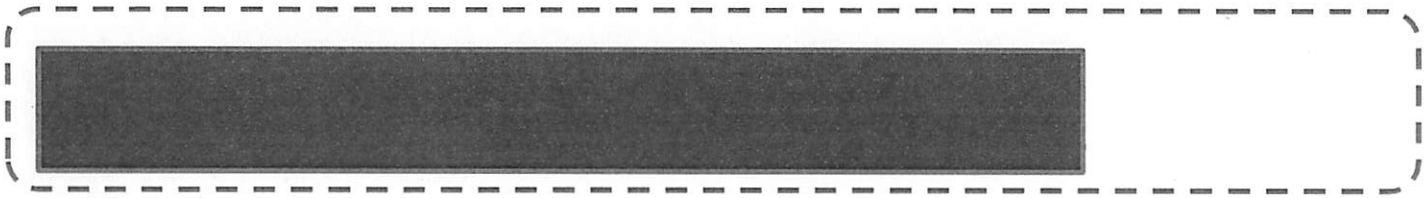
標的型メール攻撃とは

特定の相手を狙い，送信者の詐称やタイトル・本文の巧妙な記述内容によって，ウイルスを仕込んだ添付ファイルを開かせたり，メールに記載されたURLをクリックさせ，コンピュータをウイルスに感染させる攻撃方法。ウイルス感染に気付きにくく，知らないうちに情報が窃取されたり，他のパソコンにウイルスが拡散する。

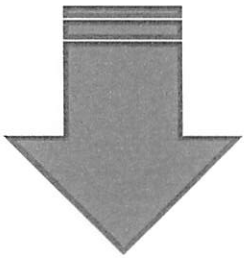
- 標的型メール攻撃により国土交通省四国地方整備局の職員パソコンがウイルス感染し，886人分の個人情報が流出した可能性（平成23年7月）
- 標的型メール攻撃により総務省の複数のパソコンがウイルス感染（震災関連資料に見せかけたウイルス）（平成23年11月）
- 長野県上田市の庁内ネットワークが標的型メール攻撃を受け，ウイルスに感染（平成27年6月）
- 東京大学の業務用パソコンが標的型メール攻撃を受けてウイルスに感染し，約3万6000件の個人情報が流出（平成27年7月）

注意

裁判所職員に対しても，標的型メールと思われる不審なメールが送信されている！



標的型メール攻撃の被害は，個人だけの問題にとどまらず，裁判所全体の問題になる可能性が高い。



一人ひとりが，標的型メール攻撃に狙われているということを認識し，不審なメールや不審な添付ファイルの開封・URLのクリックは厳禁

最近の個人情報の流出事例等①

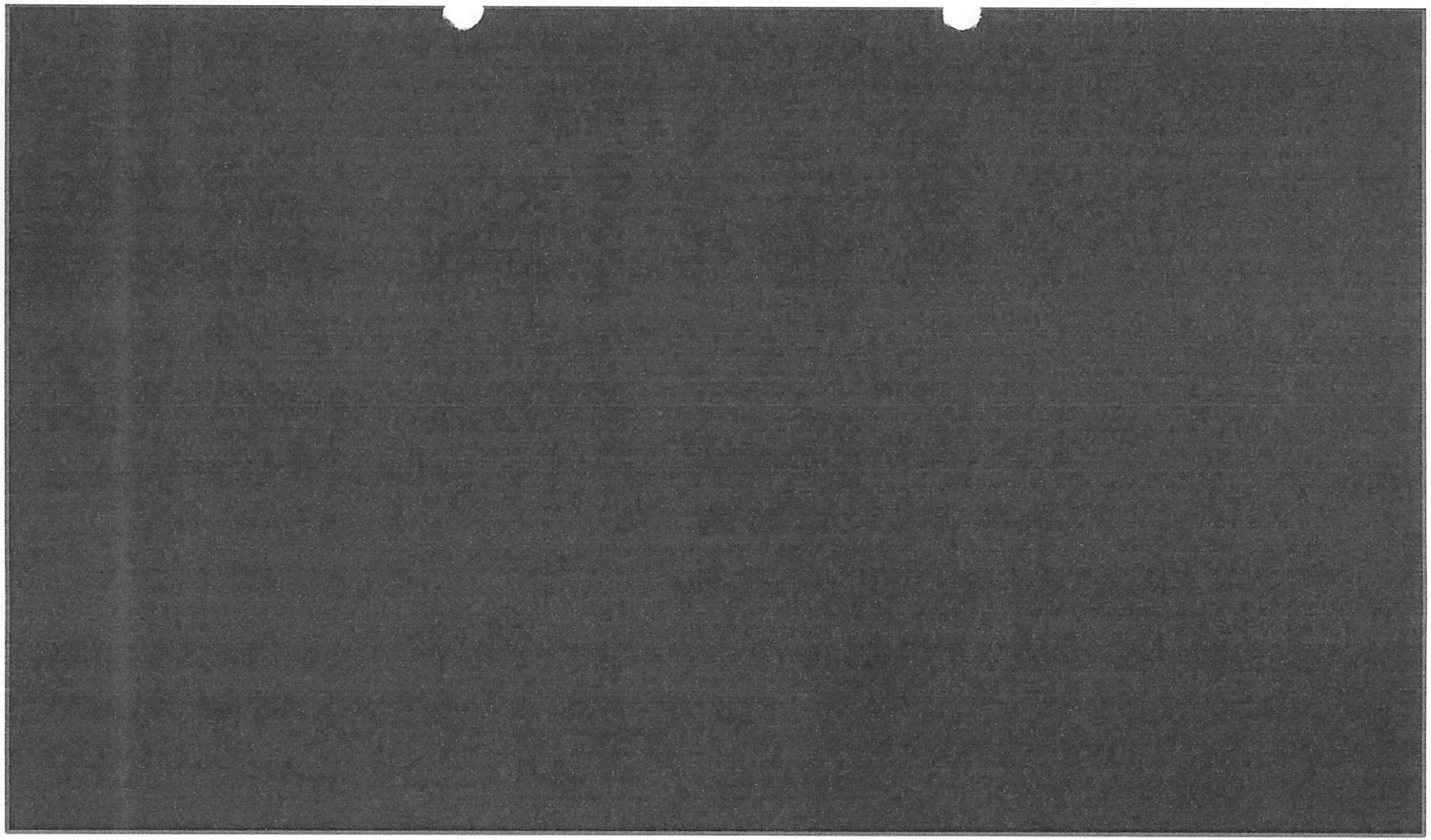
【民間】

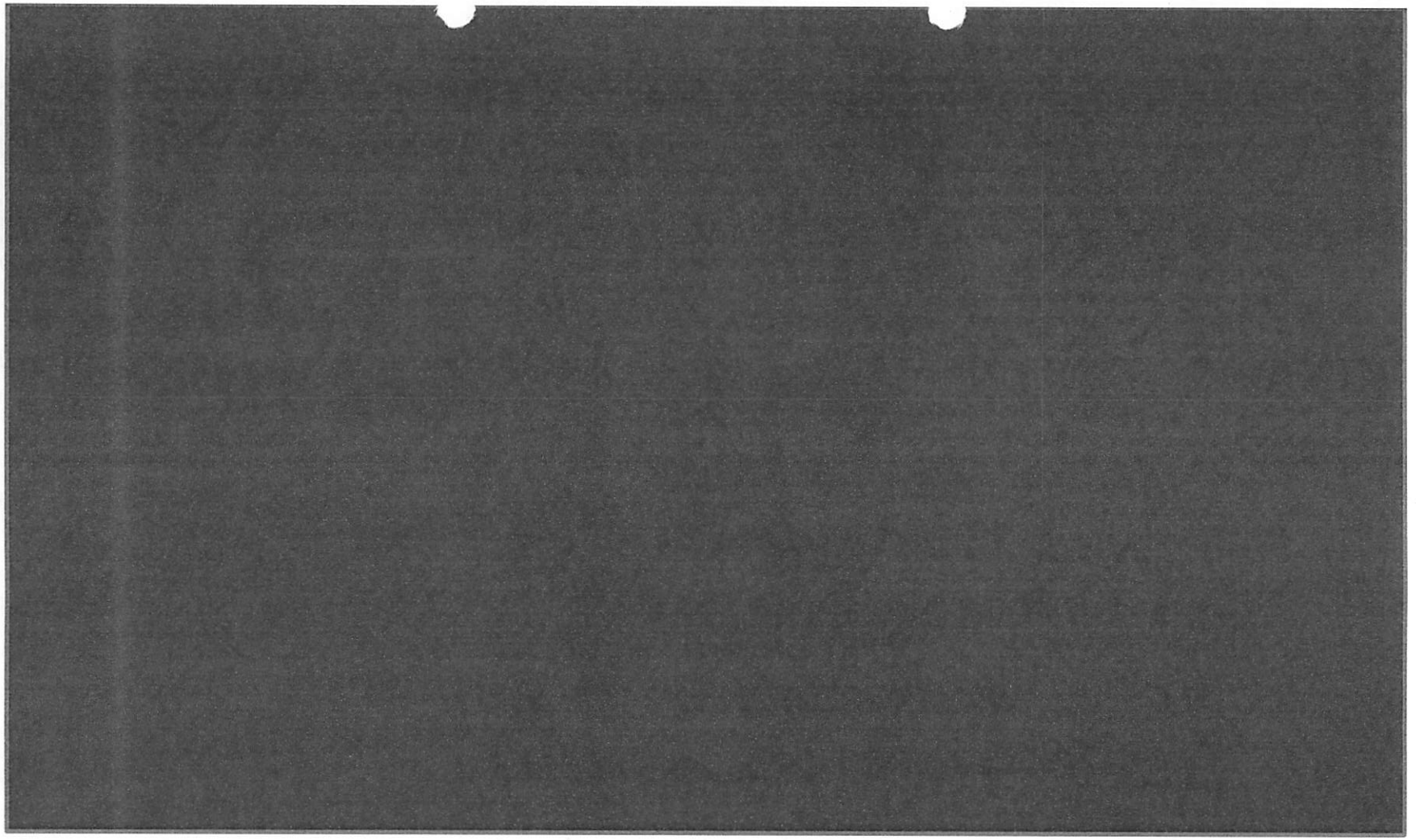
- 平成26年7月　ベネッセ・コーポレーション
- 平成26年9月下旬　日本航空
- 平成26年9月下旬　ヤマト運輸
- 平成27年6月　東京商工会議所

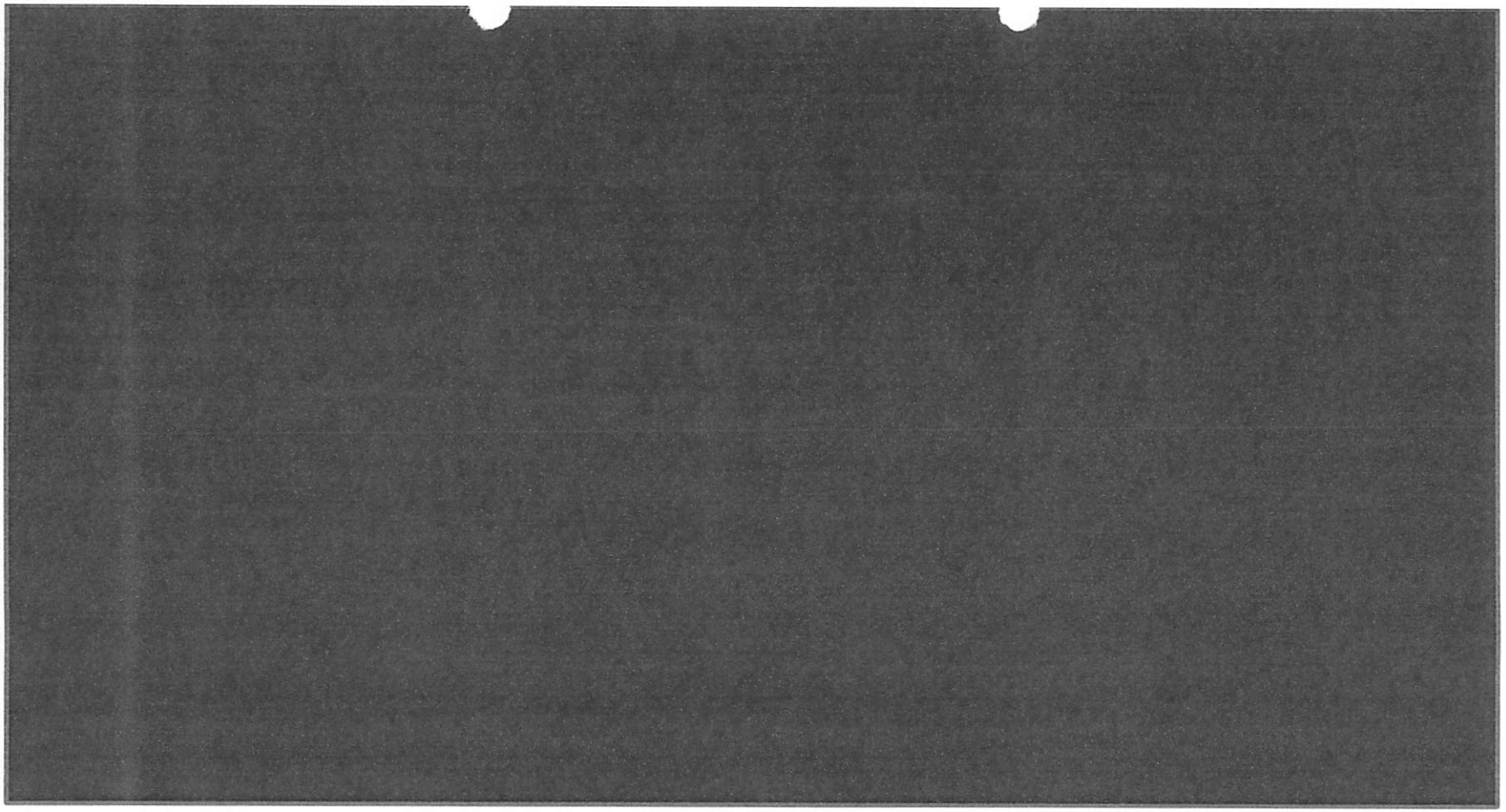
最近の個人情報の流出事例等②

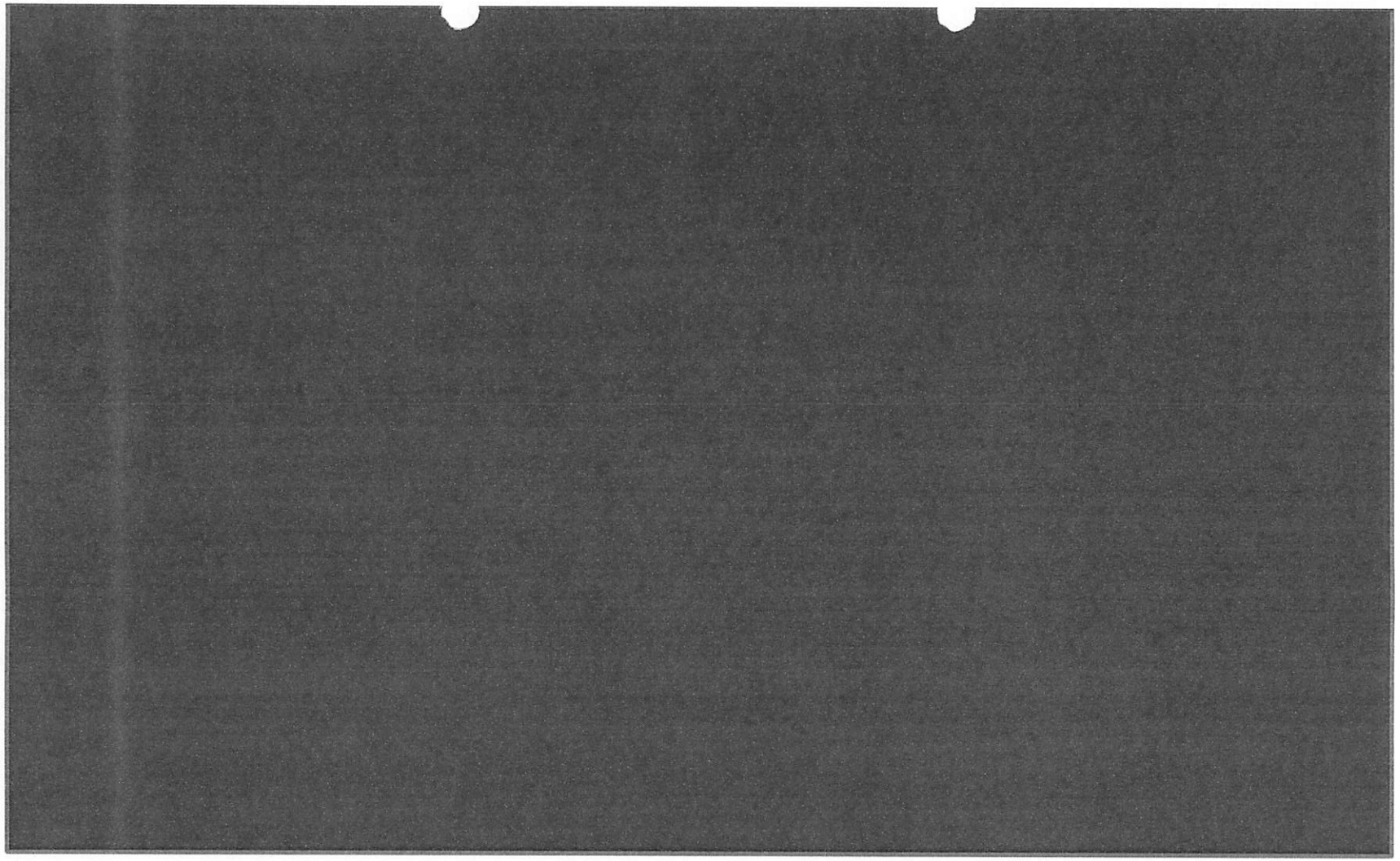
【行政府省等】

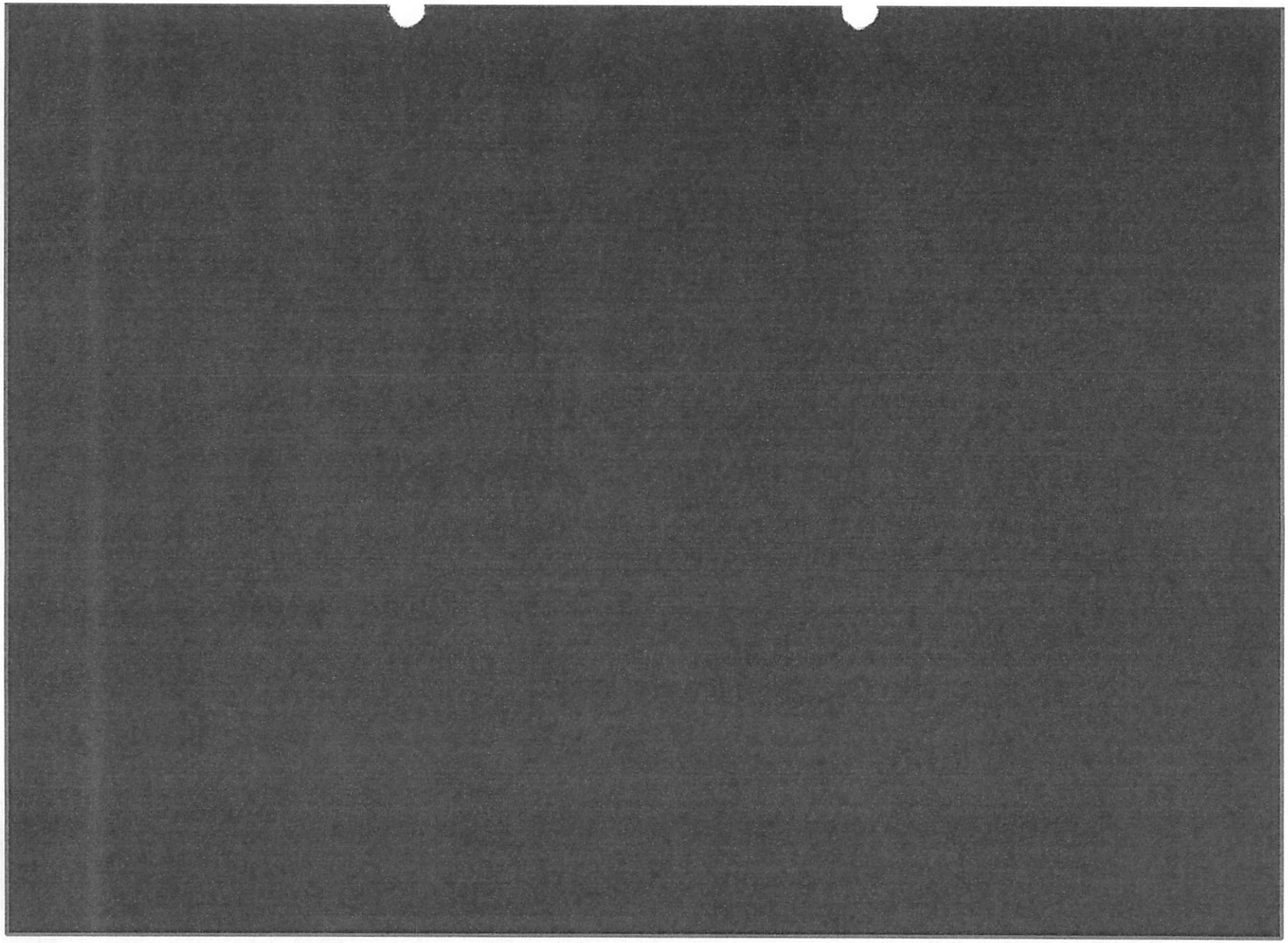
- 平成26年9月　法務省
  - サーバ等に不正アクセス。情報流出の疑い。
- 平成27年6月　法務省
  - 職員使用パソコンがウイルス感染の疑い
- 平成27年6月　日本年金機構
  - 職員が標的型メールと思われる不審なメールの添付ファイルを開封したことによりパソコンがウイルスに感染
  - 外部サーバとの不正な通信が発生し，同機構の共有サーバに保存されていた少なくとも125万件の個人情報が流出





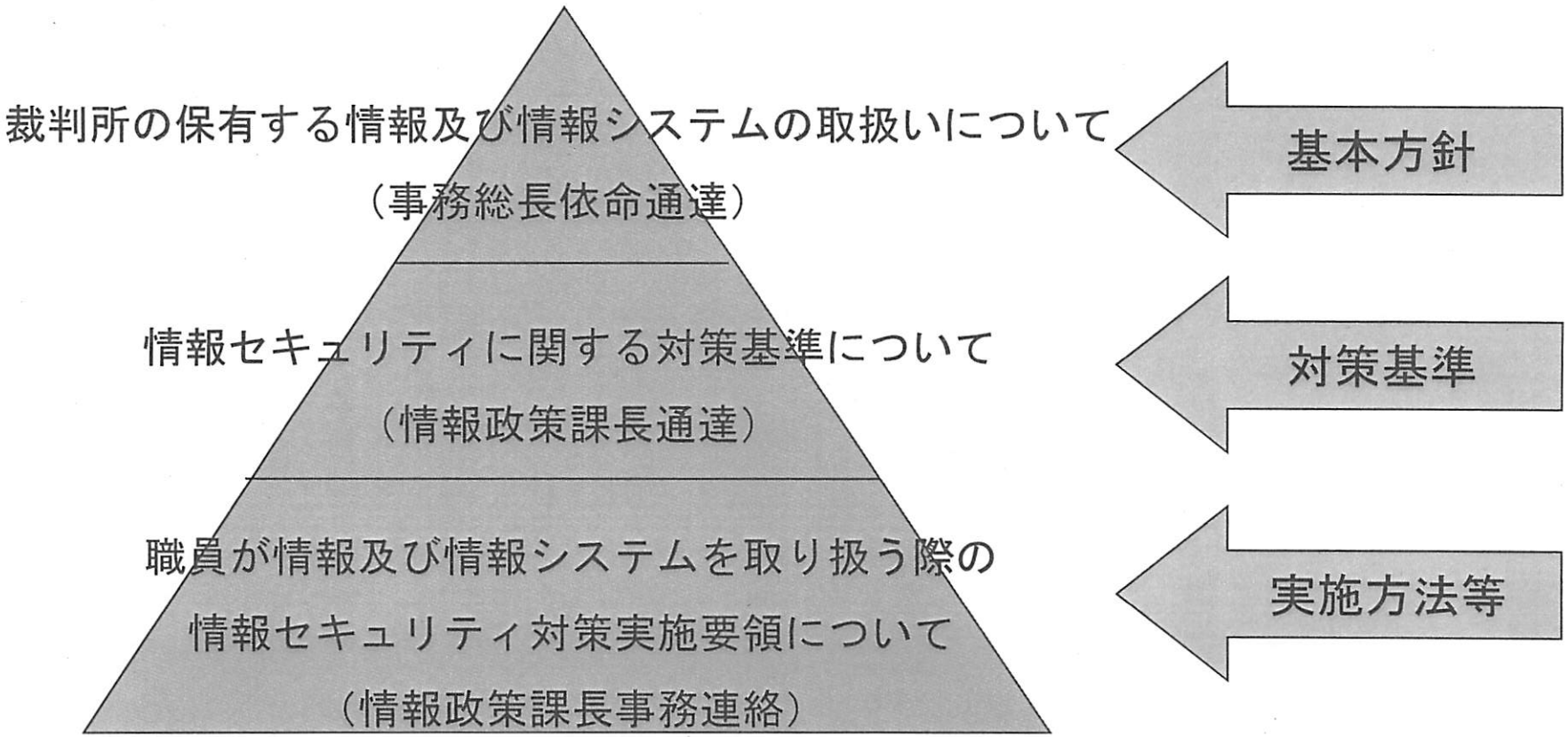






（3）裁判所における情報セキュリティ対策

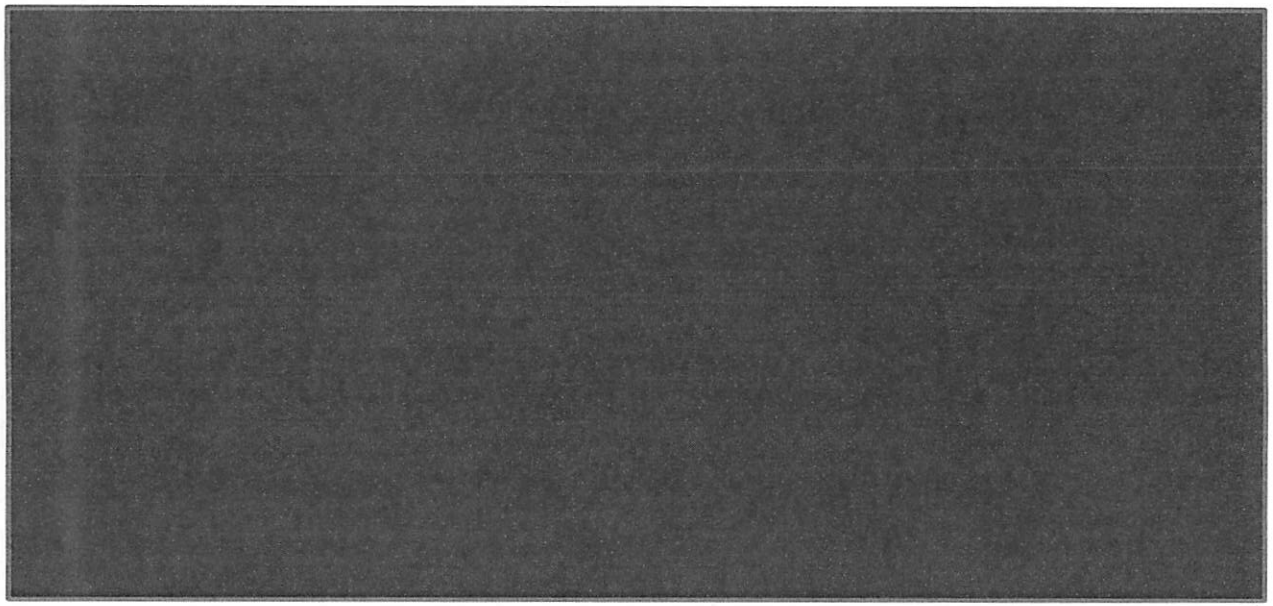
情報セキュリティポリシー
（情報セキュリティ関連通達等）



各通達等は，J・NETポータルに掲載されている。

ログイン→「最高裁各局課等からのお知らせ」→「記事検索」→フリーワード「セキュリティポリシー」又は「セキュポ」で検索すると便利

情報セキュリティのルール

- 

等

→　別添「情報セキュリティのルール（裁判官）」参照

組織のセキュリティレベル

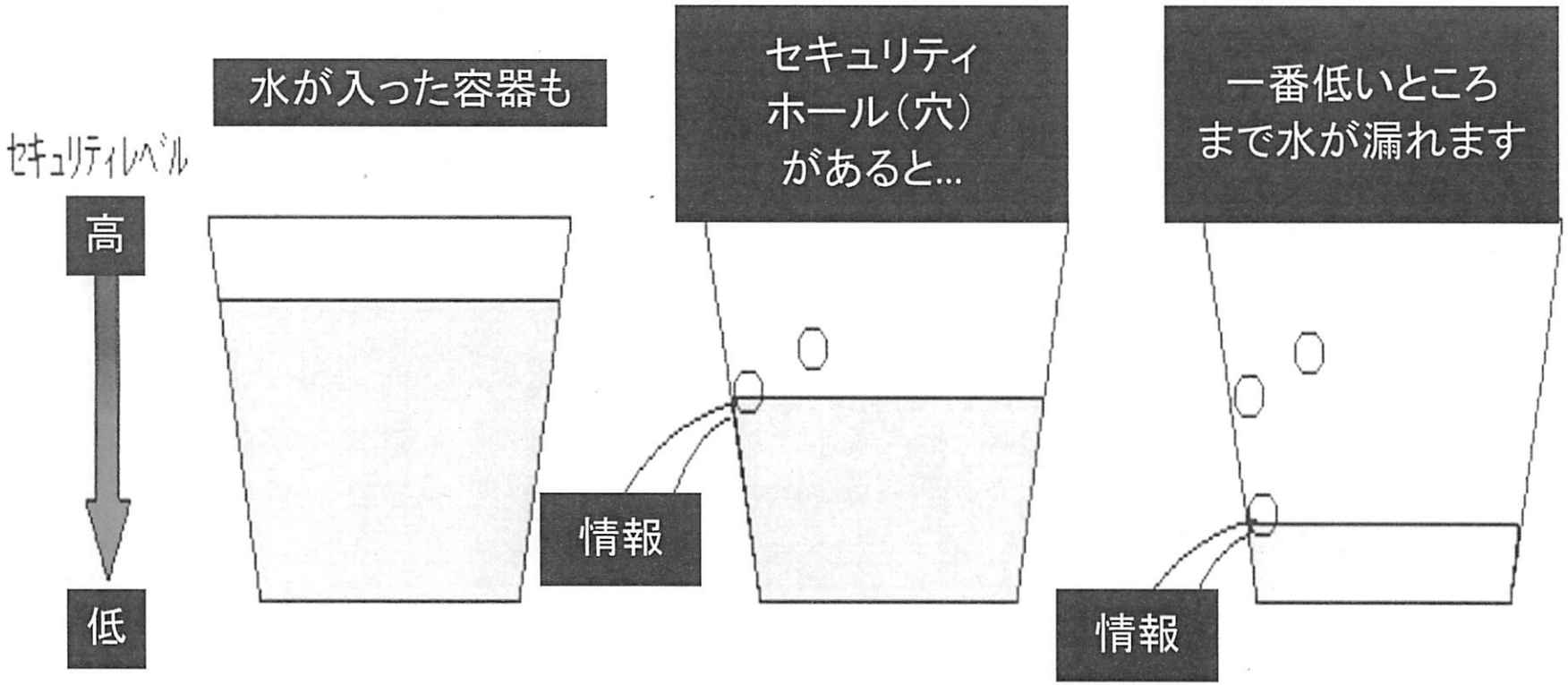
物理面，技術面の整備だけでは，情報セキュリティの確保は困難

- 組織のセキュリティレベルは最もレベルの低いところで決まる。
- たった1台のウイルス感染が原因となってウイルスが全国に拡大する可能性もある。

⇩

高い情報セキュリティを確保するためには，日頃から職員一人一人の情報セキュリティに対する高い意識と行動（予防）が不可欠である。

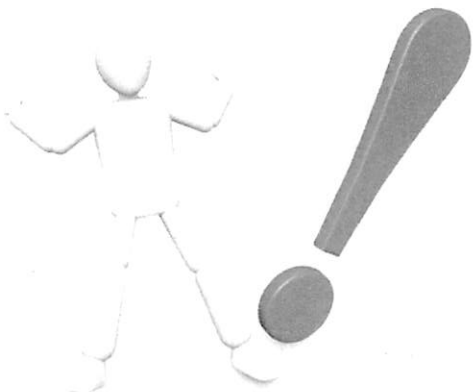
セキュリティ意識が希薄だと・・・

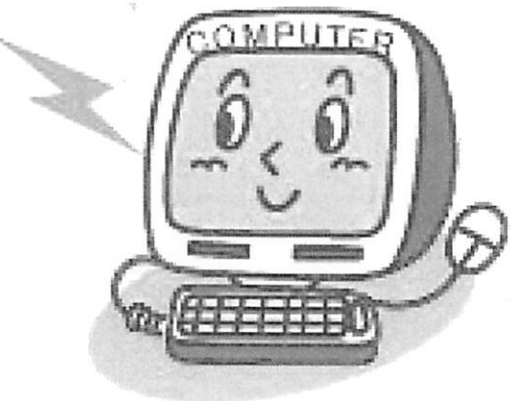


組織のセキュリティレベルは一番低い位置
で決まると言われています。
なお，漏れる水は「大切な情報」です。

裁判所の信用失墜を招かないために

- **職員一人一人の意識と…**





- **裁判所の組織としての対策…**

両方そろってこそ，
真の対策となり得る！

人的対策の視点（まとめ）

- [redacted]
- 全員がルールを守らないと意味がない。
  → ルールを守れる環境作りが重要
- 利便性とのバランス
  → 分かりやすいルール作りと説明が重要

セキュリティ確保にはみなさんの協力が不可欠

「基本的知識」を身に付け，「意識」の向上を！

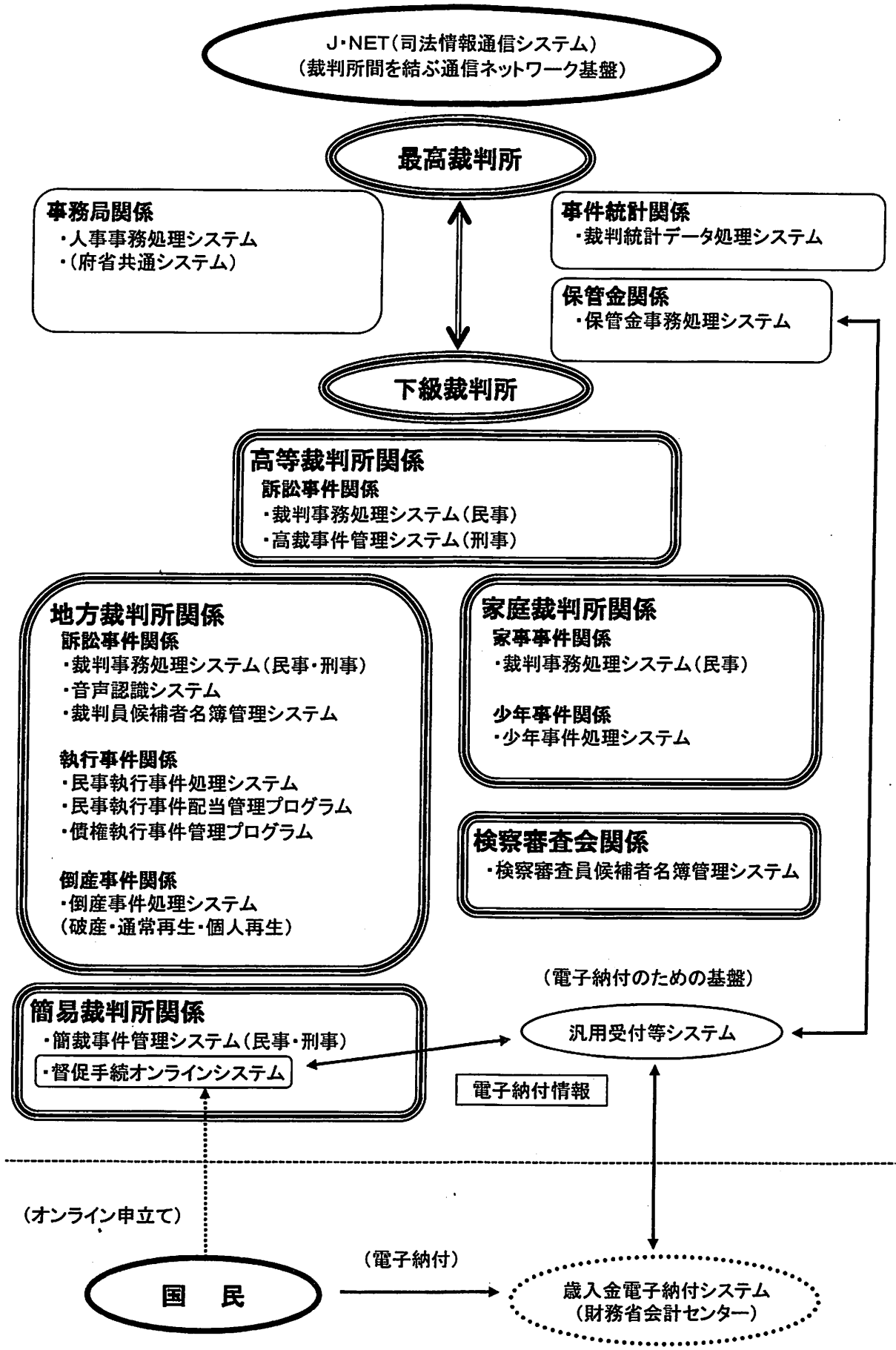
情報セキュリティのルールを遵守することは，
裁判所に対する国民の信頼を確保することで
すが・・・実は

あなた自身を守ることです。

＜セキュリティ，あなたの一手間，
あなたを守る，みんなを守る。＞

判事のみなさまに期待されていること

裁判所における主なシステム



情報セキュリティのルール（裁判官）

H27. 7月改定版