資料5－1

「番号」制度導入に伴って発生するITリスクに関するフォルトツリー分析

2011年6月7日　情報連携基盤技術WG　座長　佐々木良一

Ⅰ．はじめに

・「番号」制度導入に伴って発生するITリスクに対して、現在検討されている対策が安全なものになっているか、バランスのよいものとなっているかを明確にするには可能な限り定量的分析が不可欠である。ここでは、リスクの発生確率を推定するため、フォルトツリー分析（以下、FT分析）を用いて分析を行った。

・「番号」制度導入に伴って新たに発生するITリスクは、「社会保障・税番号要綱」に記載された「国民の懸念」を考慮して以下のものを選定した。

１．政府職員による不正情報マッチング（「国家管理への懸念」へ対応）

２．外部の不正者による複合個人情報の盗み出し（「財産的被害への懸念」へ対応）

３．「番号」を利用した民間にある個人情報のデータベース化（「個人情報の追跡・突合に対する懸念」へ対応）

なお、正規の処理により複合した個人情報を政府機関で保管し、それが漏洩するリスクも新しいリスクであるので以下も追加することとした。

４．職員の不正あるいは過失による複合個人情報の流出

・この分析結果と考察は、佐々木の個人的見解であり、合意形成のための議論を行うためのたたき台とするためのものである。分析において重要であるにもかかわらず抜けている項目や、数値が大幅に違うと思うものについてご意見を頂ければ幸いである。

Ⅱ．前提条件

・FT分析は上位項目が発生する原因を、ANDゲートとORゲイトを用いて展開した上で最下位項目の発生確率を与え上位項目の発生確率を推定する分析法である。

上位項目の確率の計算は以下のようにして実施する。∩：AND、∪：OR

$P(a \cap b) = P(a) \cdot P(b)$　　$P(a \cup b) = P(a) + P(b) - P(a) \cdot P(b) \fallingdotseq P(a) + P(b)$

・上位項目に関する発生確率の傾向をつかむためであるので、最下層の発生確率は、以下のようなざっくりした値を目安として設定した。

①0.5　　:発生確率が高いもの。

②0.1　　:発生確率が少ないもの。

③0.01　　:発生確率が非常に小さいもの。

④<0.01　:ほとんど発生しないもの。
　　本条件に該当する者同士を足しても<0.01とする。

・その他の統計値については、できる限り根拠を記載するように努めた。

Ⅲ　分析結果に関する考察

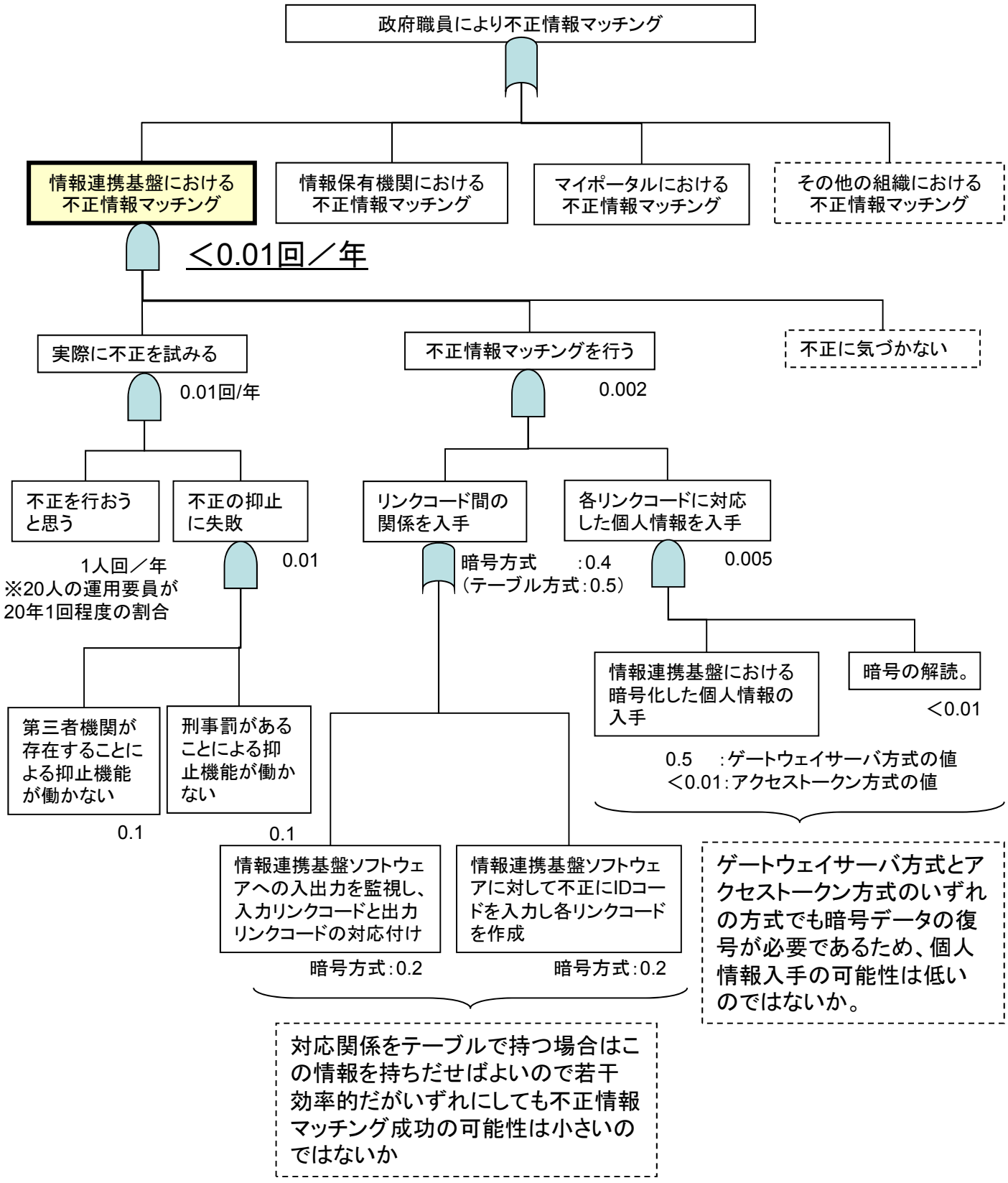
（1） 政府職員に関する情報マッチングで、情報連携基盤における不正情報マッチングの確率は十分小さく、安全上問題がない（P3参照）。
（2）情報保有機関における不正情報マッチングに関しては情報連携基盤におけるものより大きく、単独犯が自分の組織の情報と、他の組織の情報の両方を入手して不正マッチングをする場合の確率が大きい。特に正式な情報連携を装って他の組織の情報を入手するのが問題となるので、明らかにおかしなアクセスを（半）自動的に排除する等の仕組みの導入などが必要となるのではないか（P4参照）。
（3）マイポータルや「番号」付番機関、IDコード付番機関における不正情報マッチングの確率も小さく、大きな問題とはならないと考えられる（P5参照）。
（4）外部の不正者による複合の個人情報の入手も運用さえきちんとやれば発生確率は十分小さいと考えられる（P7参照）。
（5）個人事業主や民間企業などが「番号」を利用して新たにDB化を試みる可能性は残る。ガイドラインの作成や教育などによってさらにその確率を下げることが期待される（P8参照）。
（6）正規の手続きで複合した個人情報が政府機関から漏洩するリスクをさらに低減したい場合は、単独で情報を保管し必要なときだけとってくるというような対応も考えられる（P9参照）。
（7）情報連携基盤における不正情報マッチング対策において、次の2つのケースについては、いずれの方式を取ろうと安全上大差はない（P3参照）。
　（a）IDコードとリンクコードの変換においてテーブル方式をとるか、暗号方式をとるか
　（b）情報保有機関間の情報のやり取りをゲートウェイサーバ方式をとるかアクセストークン方式をとるか
（8）情報保有機関における、リンクコード払い出しに伴うリスクについて、詳細分析していないが、リンクコードは情報保有機関ごとに払い出されるものであることから、複数機関に跨る情報のマッチングリスクが上がるとは考えられない。

Ⅳ　今後の展開案

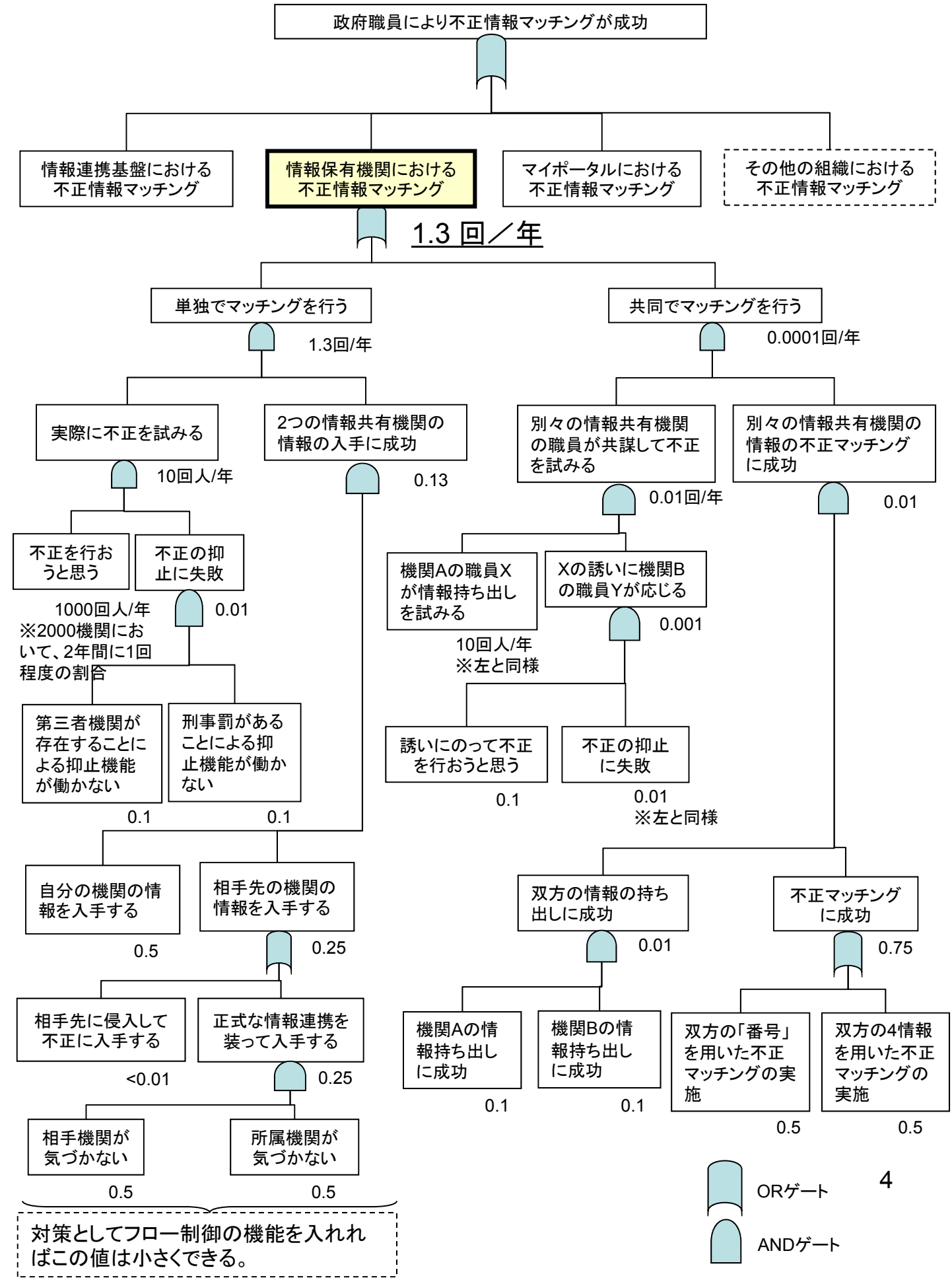
（1）いろいろな人の意見を入れてのFT分析結果の見直しを行う。
（2）新たな対策が必要なら対策の追加の提案と詳細化を行う。

（注）現状の分析はITリスクに限定しており、コストや効果の分析は実施していない。計画を進めるに当たってはこれらの分析が不可欠であり、できるだけ早く実施することを期待する。

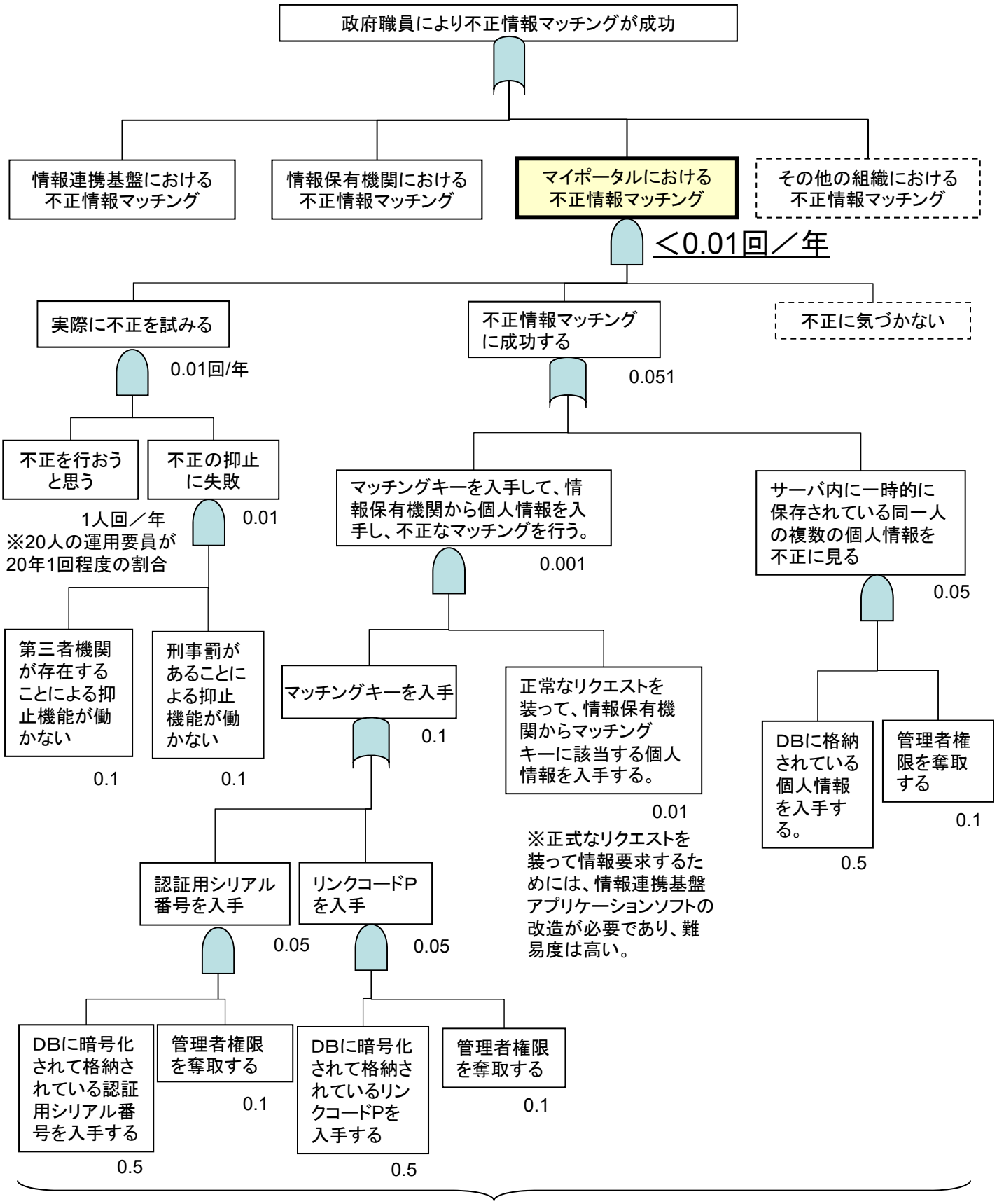
1．政府職員による不正情報マッチング
（1）情報連携基盤における不正情報マッチング



1．政府職員による不正情報マッチングが成功
（2）情報保有機関における不正情報マッチング



1．政府職員による不正情報マッチングが成功
（3）マイポータルにおける不正情報マッチング



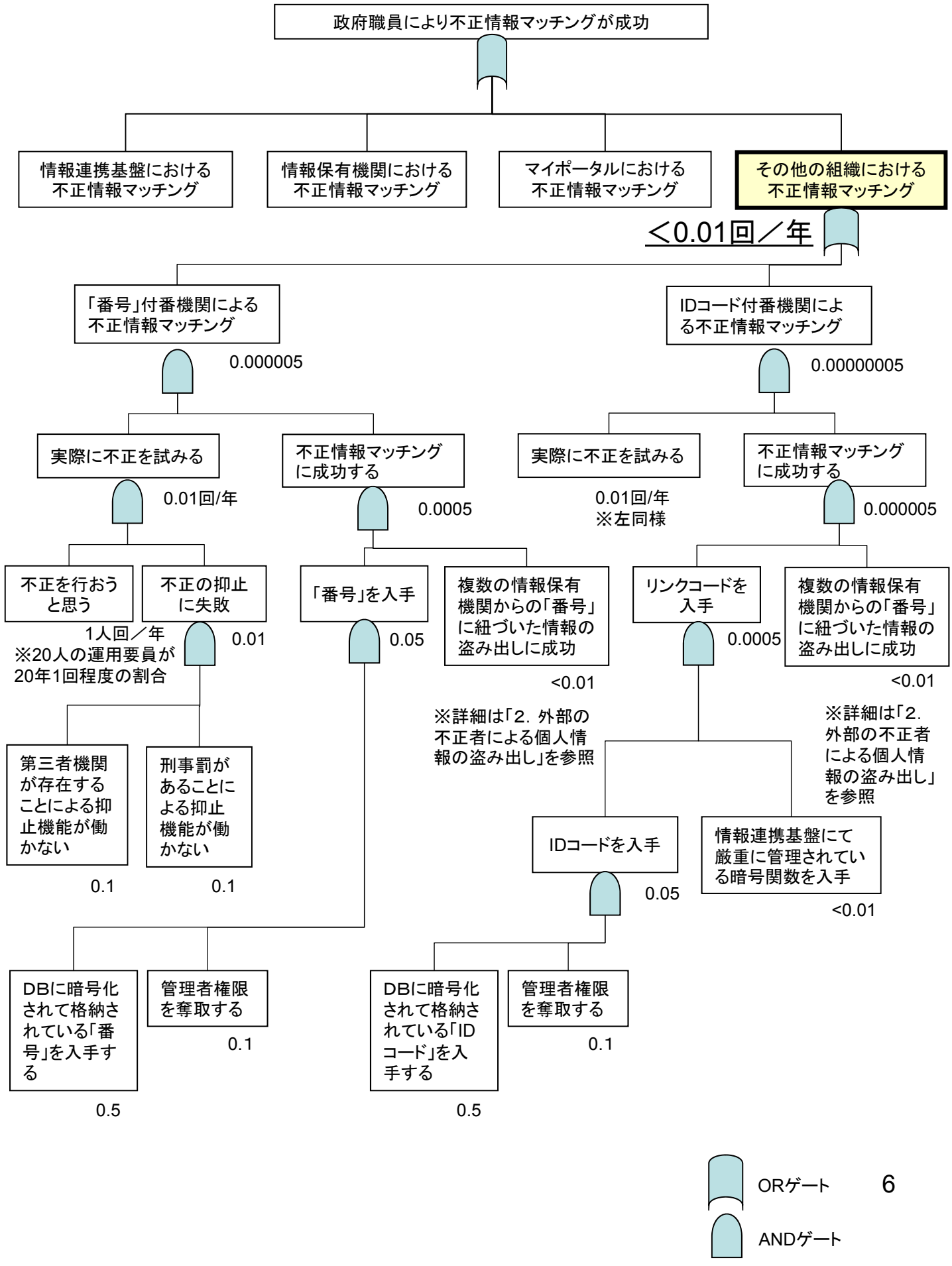
DBの内容は暗号化されており、復号するためには管理者権限が必要であることを前提とする。

管理者が不正を行った場合、マッチングキーは必ず入手できることから、マイポータルにおける不正情報マッチングの確率は「0.06回/年」となる。

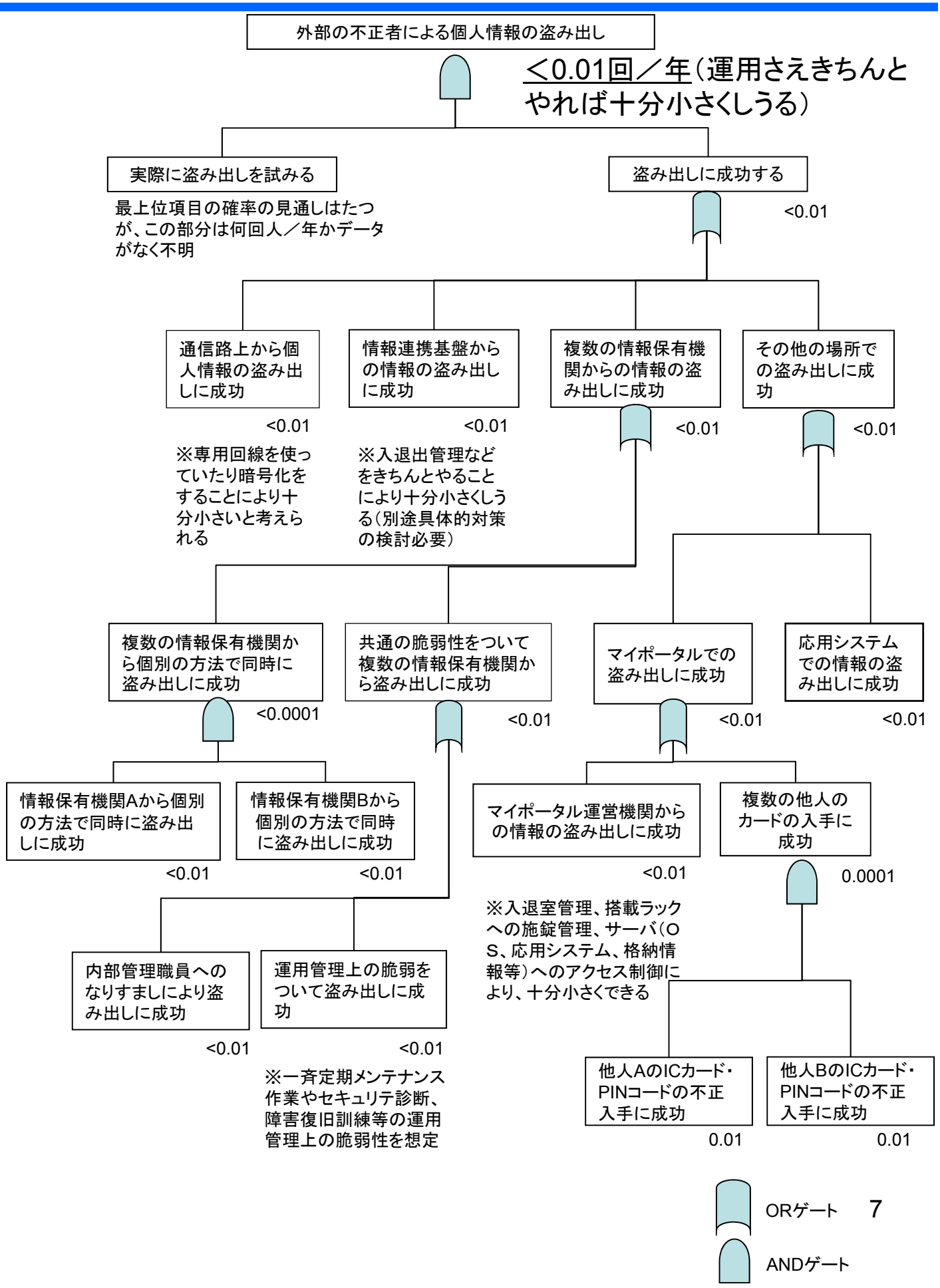
ORゲート

ANDゲート

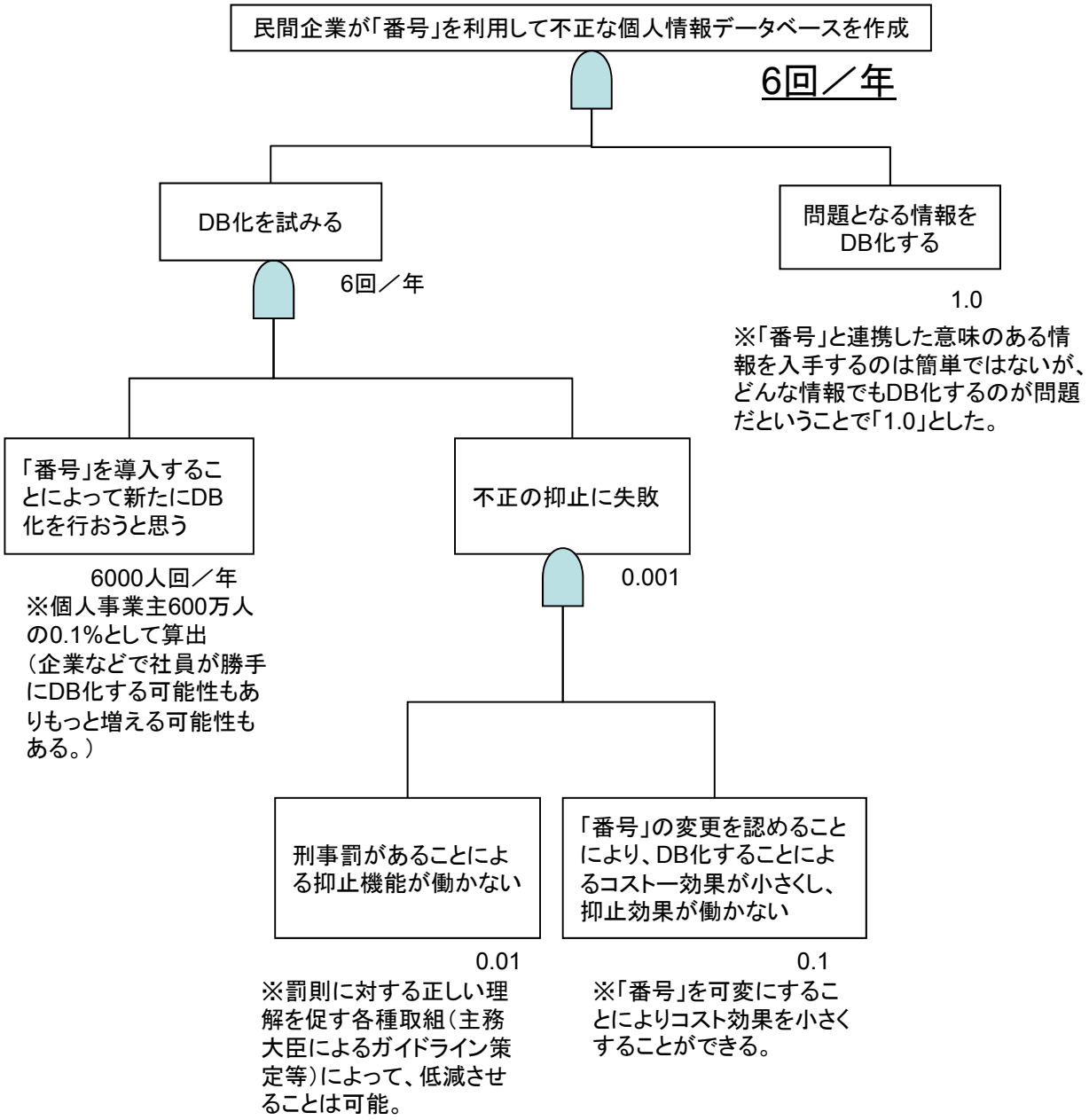
1．政府職員による不正情報マッチングが成功
（4）その他の組織における不正情報マッチング

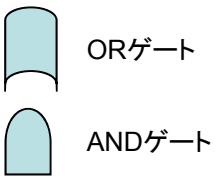


2. 外部の不正者による個人情報の盗み出し

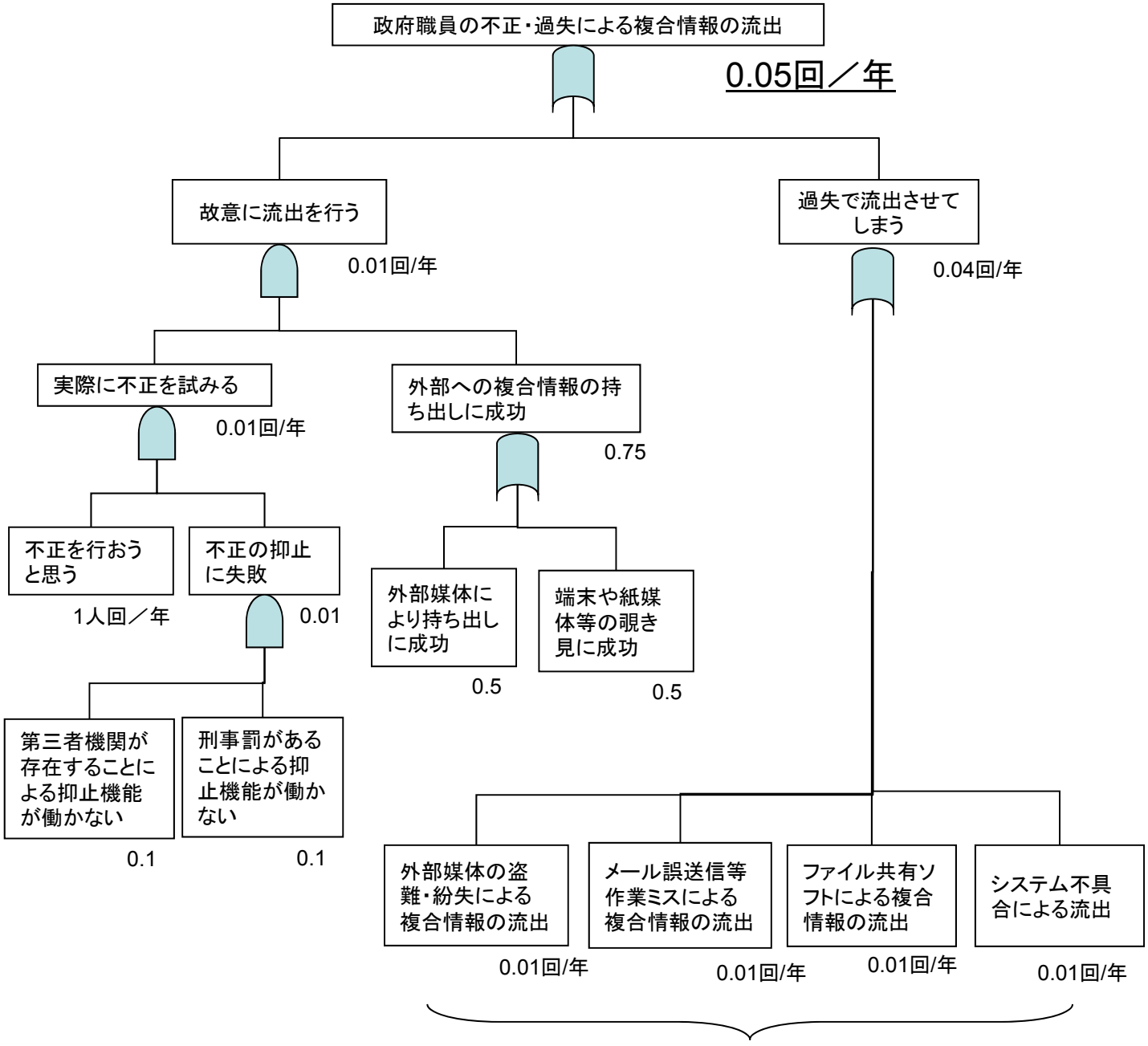


3. 民間企業が「番号」を利用して不正な個人情報データベースを作成





4. 職員の不正あるいは過失による複合情報の流出



正規の処理によって複合された情報が不正や過失により、外部に流失するリスクを扱っている。