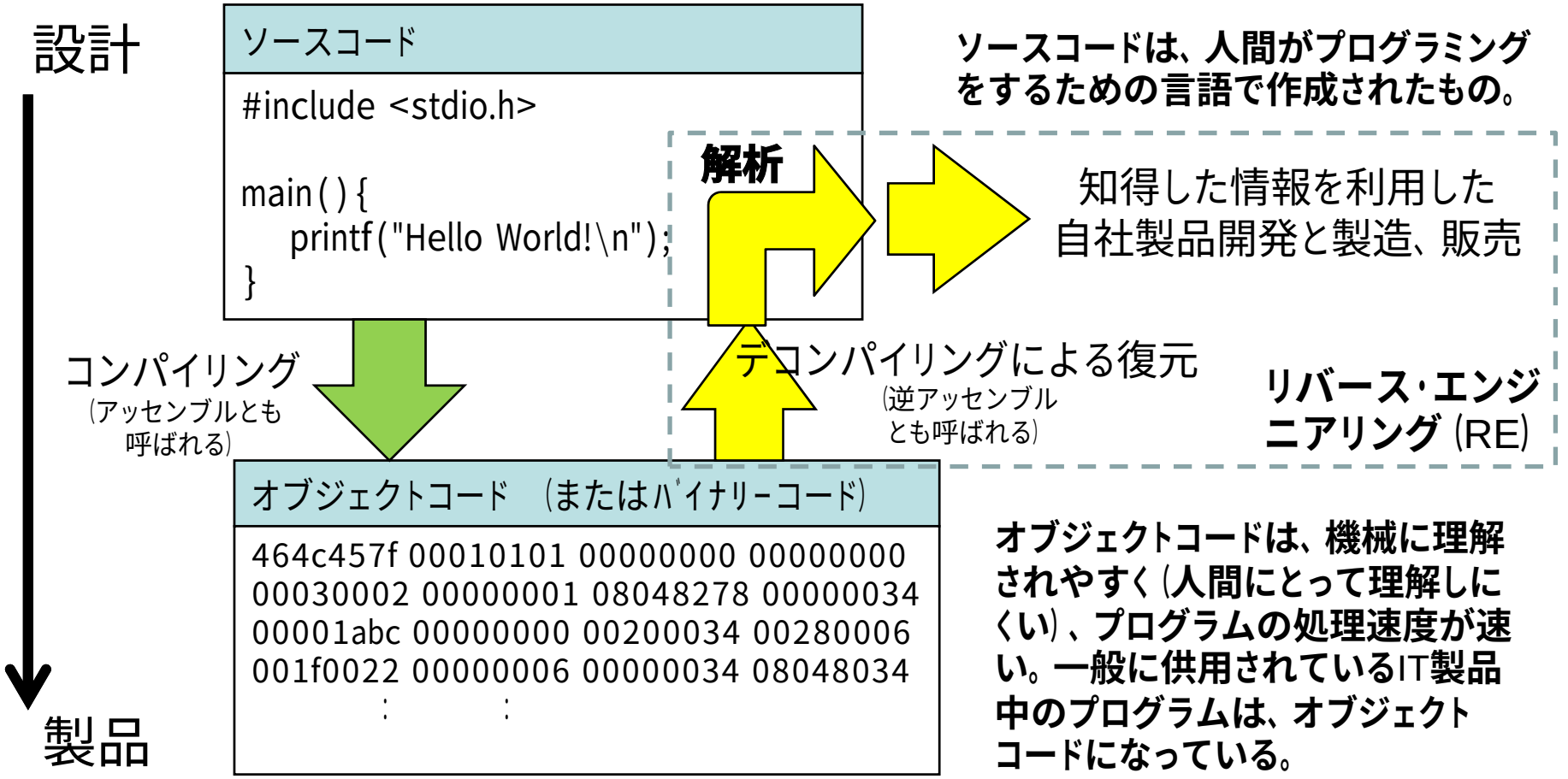
平成20年7月25日
文化審議会著作権分科会第5回法制問題小委員会資料

情報セキュリティと リバース・エンジニアリング について

独立行政法人情報処理推進機構（IPA）
セキュリティセンター

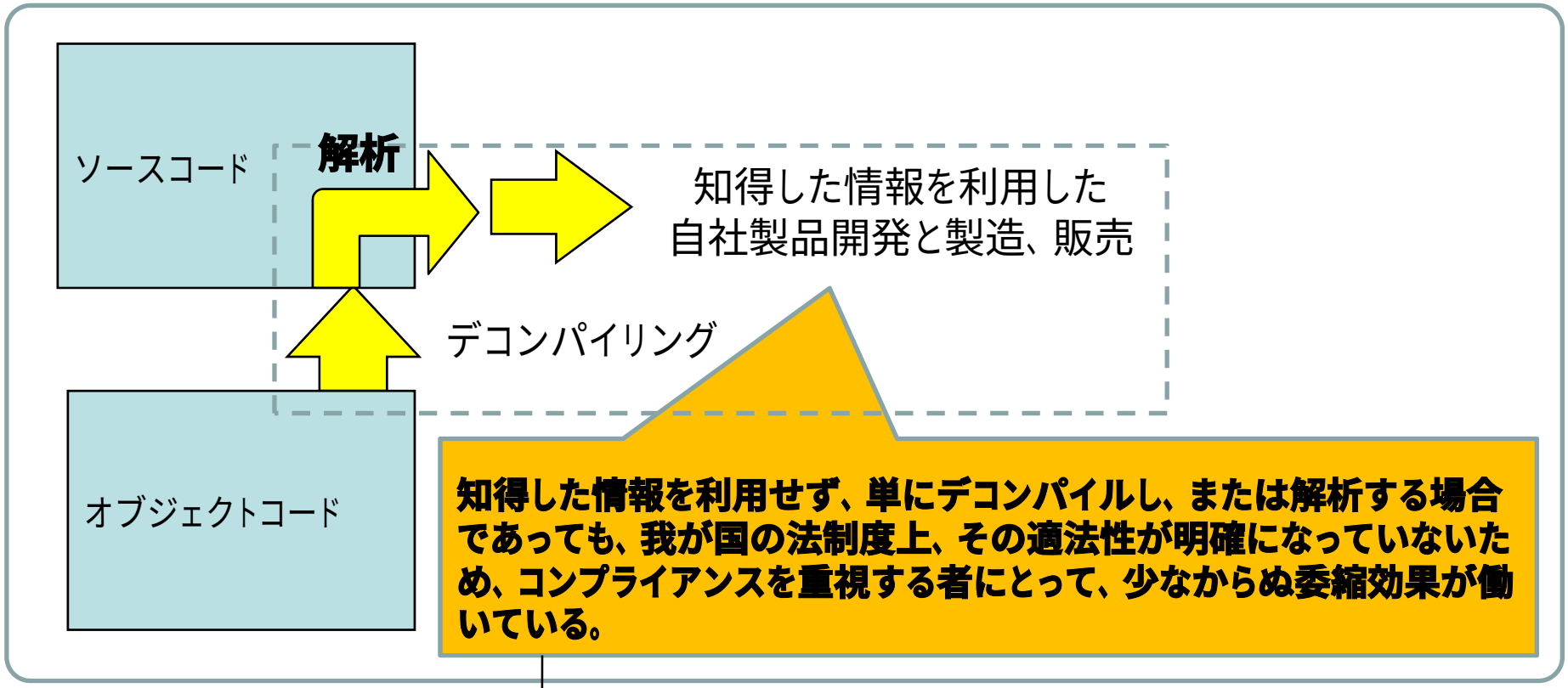
1．リバース･エンジニアリングとは

「大まかには他人の製品を分解、解析してその技術を知覚し、場合によって自分の製品に利用することをいう。」 コンピュータ･プログラムについて言えば、オブジェクト･コードからソース･コードに変換する行為を伴う。



(注) コンピュータ･プログラムのリバースエンジニアリングの上記説明については、椙山敬士「ソフトウェアの著作権･特許権」日本評論社 (1999) p29 を参考にIPA作成。オブジェクト･コードをデコンパイリングして、ソースコードを復元することは複製か翻案になると解されている (中山信弘「著作権法」有斐閣p99)。

2．問題の所在



「知的財産推進計画2008」（2008年6月18日）
第4章Ⅰ.1.（2）⑤リバースエンジニアリングに係る法的課題を解決する
革新的ソフトウェアの開発や情報セキュリティの確保に必要な範囲において、コンピュータ・ソフトウェアのリバース・エンジニアリングの過程で生じる複製・翻案を行うことができるように2008年度中に法的措置を講ずる。(文部科学省)

必要な範囲の
検討が重要。

3．リバース･エンジニアリングの主な目的

以下の目的で行うリバースエンジニアリングは一定条件下で認められるべきではないか？

① **革新的なプログラムの研究開発**

② **性能、機能の調査**

③ **障害等の発見･保守**

EU理事会指令（1991）では、これをerror collectionとして複製を認めている。

設計要求に対して行うプログラミング上のミスの検出･修正

④ **情報セキュリティ対策** ･･･今日的な重要性が高まっている

不正アクセスによるデータの改ざん、情報詐取、他者への攻撃の踏み台化などの攻撃を受けやすいプログラム上の弱点（＝脆弱性）の検出･修正、攻撃を受けた場合の影響分析などのIT製品や情報システム等の安全性確保のための対策

⑤ **互換性の確保**（注）

⑥ **著作権侵害の調査、発見**

EU理事会指令（1991）、米国DMCA（1998）では、この目的のデコンパイリングをREと規定している。

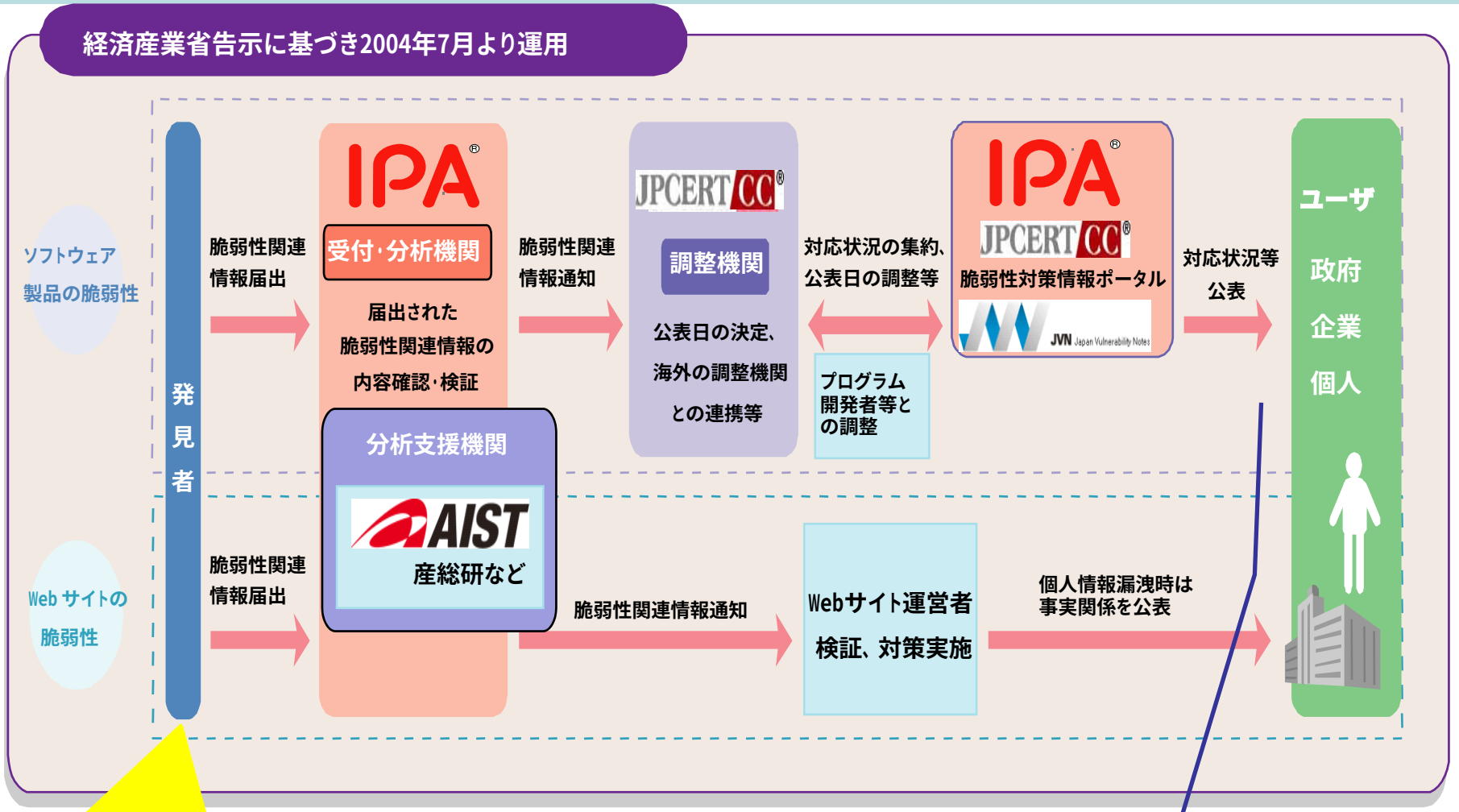
以下の目的で行うリバースエンジニアリングは認められるべきではない。

① **デコンパイルしたソース･コードを利用した模倣**

② **ウイルス作成等、悪意ある目的のための解析**

（注）「リバースエンジニアリングの問題は、特にプログラムの互換性確保にとって重大な意味を有しており、少なくとも互換性確保目的のための複製･翻案は違法とすべきではない」（中山信弘「著作権法」有斐閣p104）

4．我が国における脆弱性情報の取り扱い

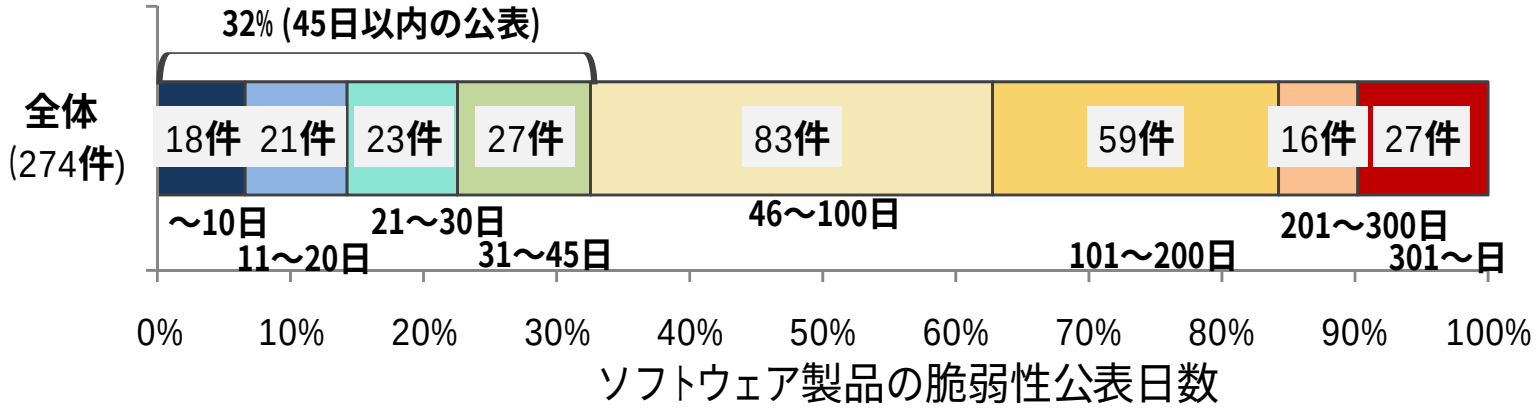


ソフトウェア製品についての届出者内訳
- 第三者：　9割強（セキュリティ関係の研究者･企業･団体、個人ユーザーなど）
- ソフト開発者：　1割弱

ソフト開発者（＝著作者）とユーザー、双方の立場と利益を考え、開発者による脆弱性を修正するプログラムの配信準備が整うのを待って、脆弱性の存在と修正方法を公表する運用を行っている。

5．迅速な脆弱性解析

開発者による対応は必ずしも迅速ではない。



悪意を持った者の攻撃プログラムの開発は迅速化している。

ウイルス名	ウイルス発見時期	ソフトウェア製品のリリース後、ウイルスが発見されるまでの期間
SQL Slammer	2003年1月	1年後
Blaster	2003年8月	数ケ月後
Zotob	2005年8月	数日後

ユーザーが修正プログラムをダウンロードするまでの間、彼らは、悪意をもった者からの攻撃（「Zero-day-attack」と呼ばれる）に晒されていることを意味。迅速かつ正確な脆弱性の解析のために、リバース･エンジニアリングが必要となるケースがある。

6．不正プログラムの挙動解析、暗号研究

不正なプログラムの挙動解析

政府や企業の情報システムなどを狙ったサイバー攻撃を受けたり、秘密裏に情報を詐取等するための不正なプログラム（一般に「トロイの木馬」と呼ばれる）が送り込まれた場合に、それらが情報システムなどにどのような影響を与えるのか、どのような対策を採るべきかといった、挙動解析及び対策検討のためには、不正プログラムが埋め込まれたシステムのコンピュータ・プログラムを含めたコードの解析が必要となる場合がある。

新たな暗号研究開発

ネットビジネス上の秘密情報の送信や本人確認等のために利用されている暗号技術については、コンピュータの計算速度の向上等とともに、その安全性は低下していくため、新しい暗号技術の研究開発は常に必要となる。強度の高い革新的な暗号技術の研究開発のため、未開示暗号プログラムの解析が必要となる場合がある。

7．リバース･エンジニアリングのセキュリティ上の意義

オブジェクトコードをデコンパイルし、ソースコードを読み取ることにより、情報セキュリティ対策に役立てる行為は、解析したコードを、プログラムの開発者の経済的利益を害するような利用をしているのでなく、

①プログラムのユーザーを悪意をもった者の攻撃から保護したり、

②開発者が開発したプログラムの質を高めたり、

（プログラムの開発者の利益を直接的に保護していると言える）

③デジタル･ネット社会におけるIT利用基盤全体の安全性を高めたり

するために行われるもの。

8．情報セキュリティ・ビジネスの振興上の意義等

IPAは、脆弱性検査、コンピュータ・ウイルス対策等を業とする情報セキュリティ関係企業数十社と定期的に意見交換を実施。

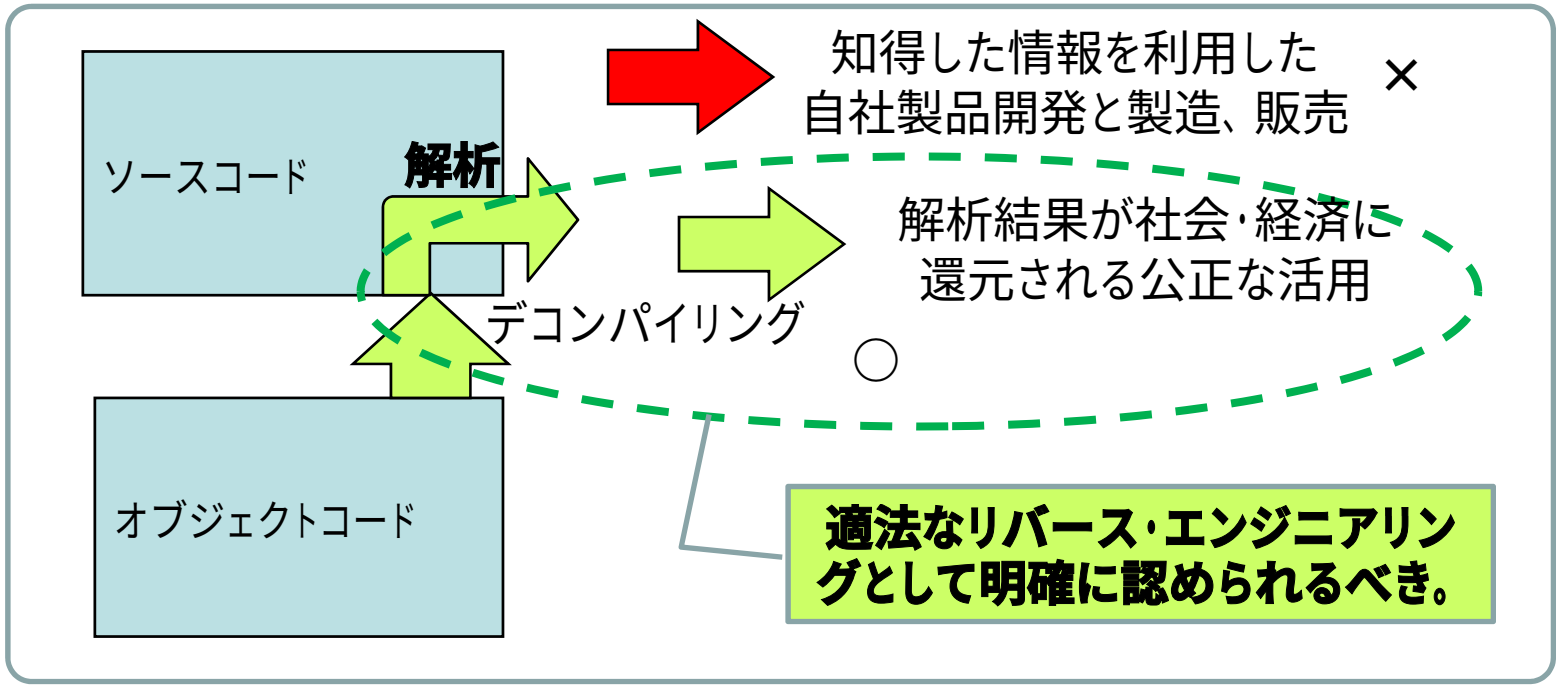
- 我が国の著作権法制において、リバース・エンジニアリングの法的扱いが不明であることを認知している企業の中には、コンプライアンスの観点から、海外（欧米、日本以外のアジア）で、リバース・エンジアリングにより解析している企業があり。

- 結果として、我が国に情報セキュリティ技術者のスキルが高まらず、世界の情報セキュリティ・ビジネスの中で、日本が比較劣位に置かれる一つの要因。

- 欧米では、高度な脆弱性の検出ツールの開発や新たなセキュリティサービスの開発等、情報セキュリティ分野のベンチャーが激しく競争。

- 我が国で、今後、リバース・エンジニアリングの適法化を措置される場合には、日本のセキュリティ・ベンチャーの経済的体力の考慮が重要。

9．まとめ（権利制限していただきたい範囲など）



- **フェアユースよりも、権利制限規定として個別に措置させるべき。**
- **情報セキュリティ対策の性質に鑑みて、契約に対して優越的に扱われるべき。**