National Institute of Advanced Industrial Science and Technology
AIST

RISEC
Research Institute for Secure Systems

クライアントおよびサーバ双方からの情報漏えいを防止するアクセス制御技術の研究開発

研究代表者：須崎有康、独立行政法人産業技術総合研究所
研究分担者：古原和邦、独立行政法人産業技術総合研究所
井上宣子、サイエンスパーク株式会社
川出智幸、サイエンスパーク株式会社

National Institute of Advanced Industrial Science and Technology
AIST

開発の動機

RISEC
Research Institute for Secure Systems

- 情報漏えいの現状
  - 暗号化が普及したことにより、ネットワーク自体からの盗聴は少ない。
  - むしろ正当なアクセス権を有するプロバイダからののぞき見が問題。
    - マイクロソフトによるGmailを糾弾するキャンペーン “Don‘t Get Scroogled by Gmail” [2013]
  - 利用者のクライアント端末からの漏えいも危険。
    - 尖閣諸島のビデオ漏えい [2010]
  - 印刷した紙媒体の漏えいも多い。
    - 日本ネットワークセキュリティ協会(JNSA)、情報セキュリティインシデントの調査報告書 [2012]

- サーバとクライアントの双方で情報漏えい対策が必要
  - サーバにデータをあげるときは暗号化
  - クライアントはアクセス制御を行う

National Institute of Advanced Industrial Science and Technology
AIST

開発した対策技術

RISEC
Research Institute for Secure Systems

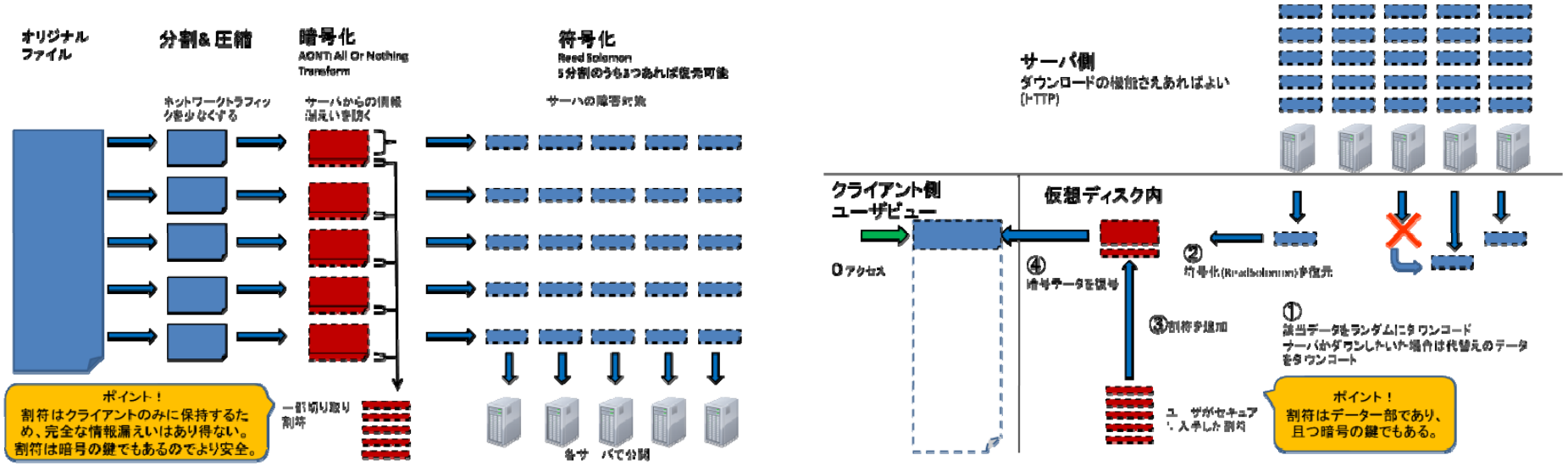
- サーバ
  - 仮想ファイルステム “LBCAS” (課題1)
- クライアント
  - アクセス制御 “NonCopy” (課題2)
  - 開発したセキュリティ技術を保護する(課題3)
    - ドライバの保護 “DriverGuard” (課題3-1)
    - 鍵管理 “LR-AKE” (課題3-2)

National Institute of Advanced Industrial Science and Technology
AIST

仮想ファイルステム “LBCAS” (課題1)

RISEC
Research Institute for Secure Systems

- サーバから覗き見ることが不可能な技術
  - ファイルは暗号化（AONT: All or Nothing Transform）されるばかりでなく、一部を割り符(Split tally)として別経路で利用者に渡す。
    - **攻撃者はサーバ上の全てのデータを集めても、復号できない！**
  - ファイルは対障害を考慮して符号化（リードソロモン）して複数サーバに上げる。
  - ファイルは割り符を持つクライアントのみで復号できる。



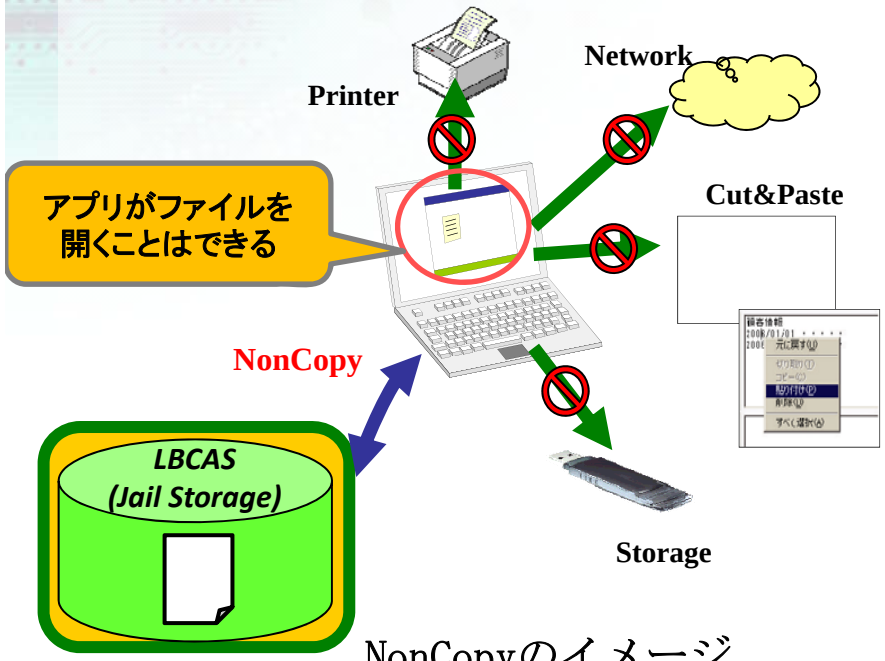
LBCASのファイルの暗号化（左）と復号（右）

National Institute of Advanced Industrial Science and Technology
AIST

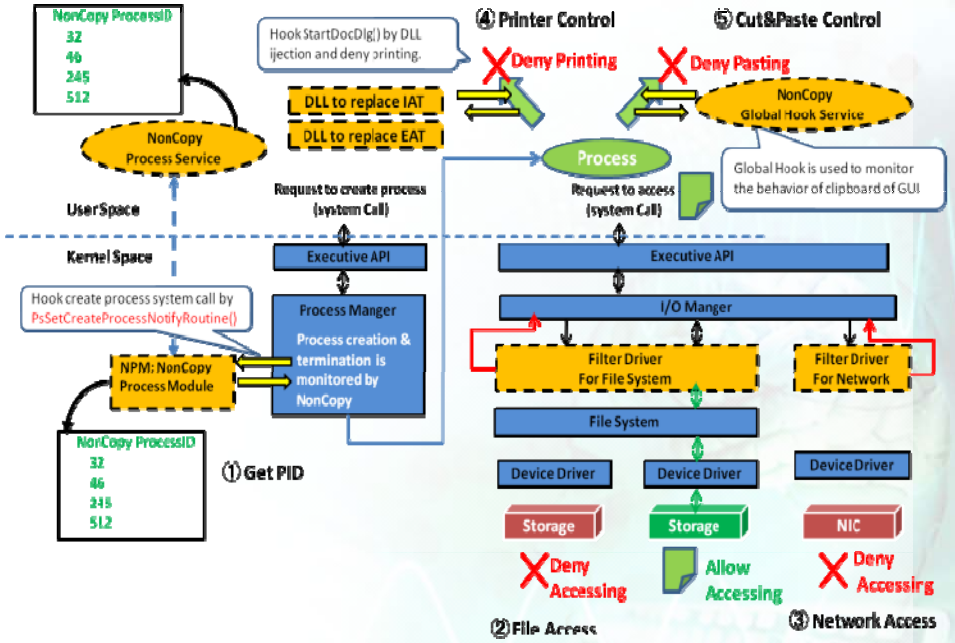
アクセス制御 “NonCopy” (課題2)

RISEC
Research Institute for Secure Systems

- クライアントから情報漏えいしない技術
  - 仮想ファイルシステムLBCASで復号されたファイルはNonCopyでアクセス制御される。
  - NonCopyはアプリケーションがファイルを開くこと、編集することは許すが、**コピーすること、Cut&Pasteすること、印刷することは許さない。**



NonCopyのイメージ



NonCopyの実装詳細

National Institute of Advanced Industrial Science and Technology AIST

開発したセキュリティ技術を保護する(課題3)

RISEC Research Institute for Secure Systems

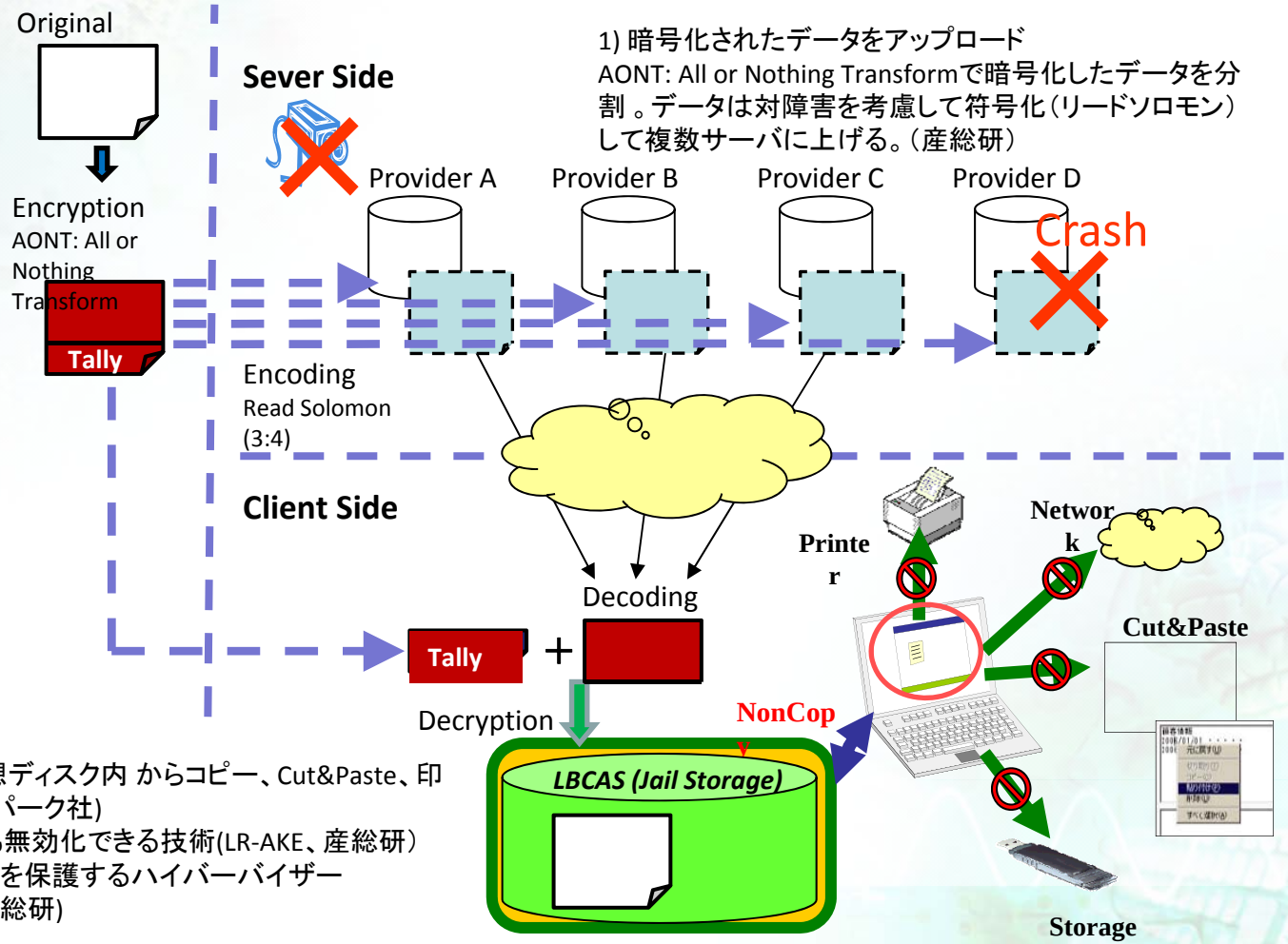
- クライアントのセキュリティ技術の保護
  - ドライバの保護 “DriverGuard” (課題3-1)
    - NonCopy自体のドライバが攻撃されるかもしれない。
    - これを防ぐために、ドライバ内のコードや重要なデータをOS外のハイパーバイザーで保護する技術“DriverGuard”を開発。
  - 鍵管理 “LR-AKE” (課題3-2)
    - LBCASがクライアントに渡す割り符(Split Tally)が盗まれるかもしれない。
    - 重要情報を守る鍵管理 “LR-AKE”で保護する。
    - LR-AKEでは重要情報を暗号化して、万が一重要情報が盗まれてもその
の無効化と再発行を可能とする。

National Institute of Advanced Industrial Science and Technology
AIST

開発した成果の展開・波及

RISEC
Research Institute for Secure Systems

- 開発したシステムは北海道通信網株式会社(HOTnet)とドリームアーツ沖縄の協力を得て、大分県立工科短大で実証実験。



2) NonCopyにより仮想ディスク内 からコピー、Cut&Paste、印刷を禁止(サイエンスパーク社)
3-1) 鍵が漏えいしても無効化できる技術(LR-AKE、産総研）
3-2) ドライバの改ざんを保護するハイバーバイザー
(Driver Guard、産総研)