セキュリティ対策方法３
（運用面の対策）

2014年12月22日

後　保範

可用性対策とは

- 可用性とはシステムが必要なときにサービスを提供できること
- サービスが利用できない
  ＝ その間の業務が停滞
- サービスが停止すると、獲得できたはずの利益が失われる（利益機会喪失）
- サービスが停止すると企業の社会的信頼の低下になる

可用性対策の種類

- バックアップ
  データの系統的バックアップ
- 冗長構成
  サービスを止めたり、低下させない障害対策
- デュアルシステム
  システムを2つ用意し両方で同じ処理をする
- デュプレックスシステム
  主系と予備系で、主系の障害時に切り替え

障害時の動作の考え方

- フォールト・トレラント
  システムの一部に障害があっても全体は停止しない
- フェールセーフ
  安全な状態の方にシステムをダウンさせ危険を回避
- フール・プール
  誤動作防止のため、確認画面を表示するなど
- ファイルソフト
  被害を最小限に抑えて、続行するよう部分回復する
- フォールバック
  故障した装置を切り離して処理を続行する

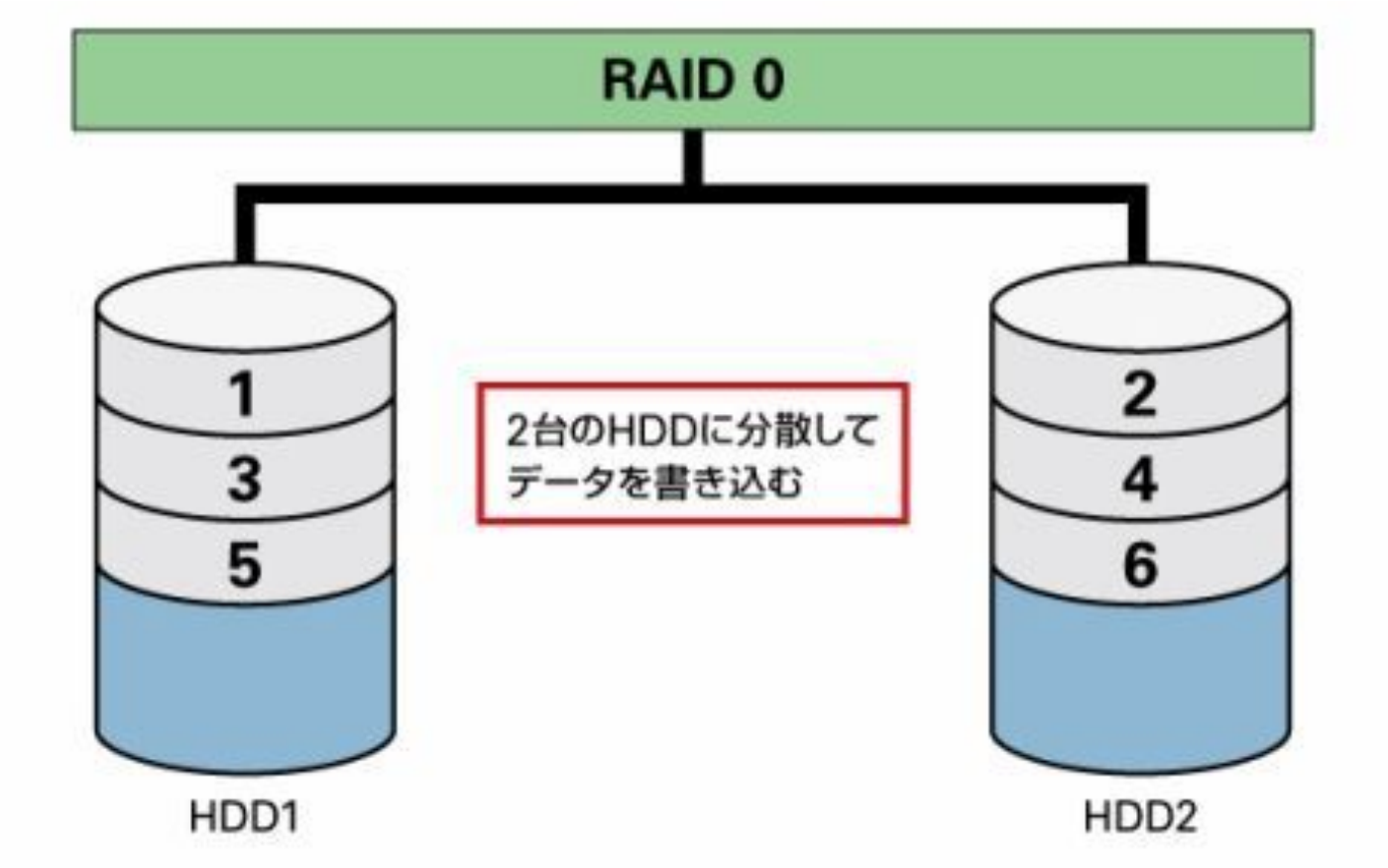
RAID

- 複数のハードディスクをまとめて一台のハードディスクとして管理する技術
- データを分散して記憶するため、高速化や安全性が向上する
- 専用のハードウェアを使う方法とソフトウェアで実現する方法がある
- RAID-0からRAID-6まで7レベルあり
- レベルは優劣を意味せず、方式名が異なる

RAID0

- ストライピングと呼ばれ、複数のディスクに均等にデータを振り分け、同時並行に記録
- データの読み書きを高速化
- ディスクが一台でも破損するとデータ全体が損なわれる
- 一台のディスクに記憶するのに比べて信頼性はむしろ低下する
- RAID1,RAID5と組み合しとRAID10,RAID50

RAID0

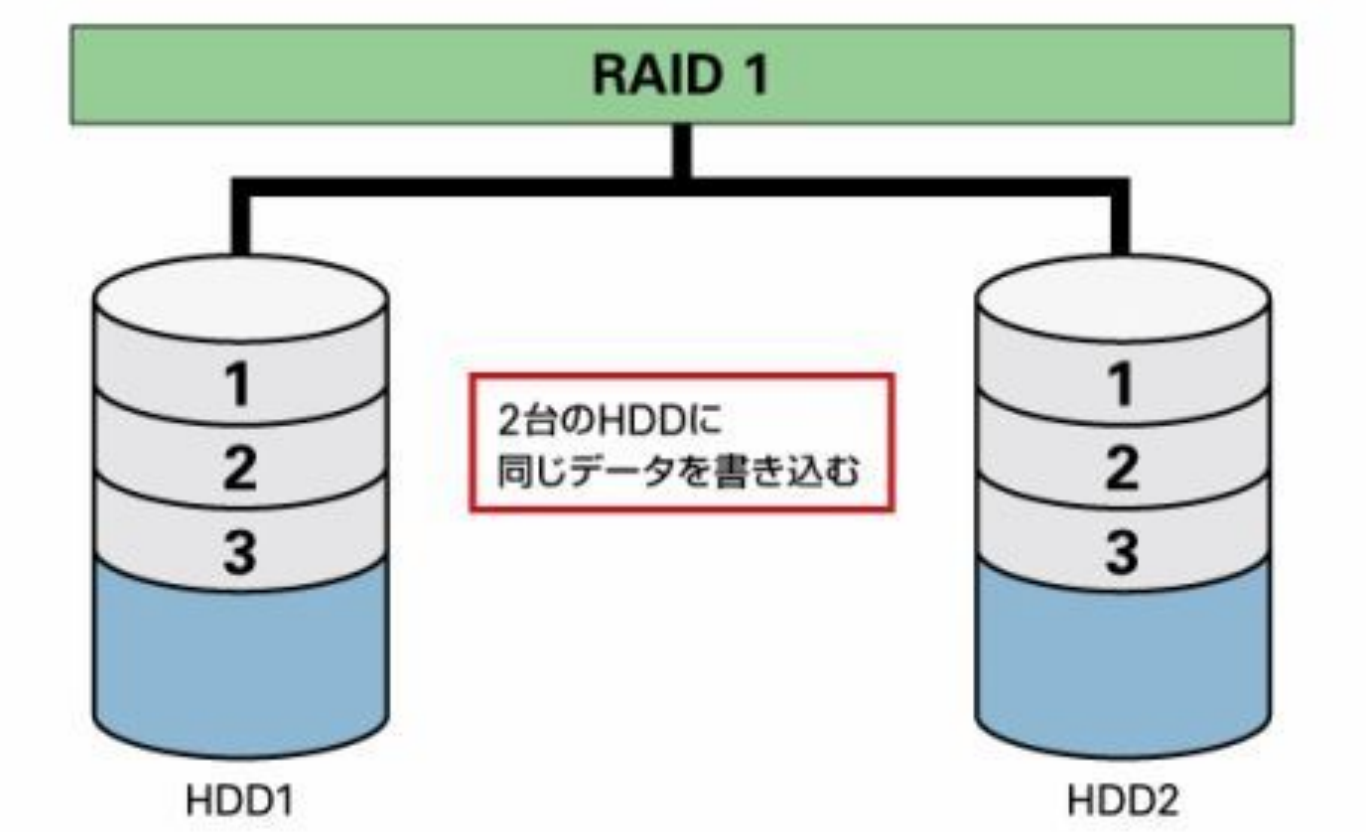


http://ascii.jp/より

RAID1

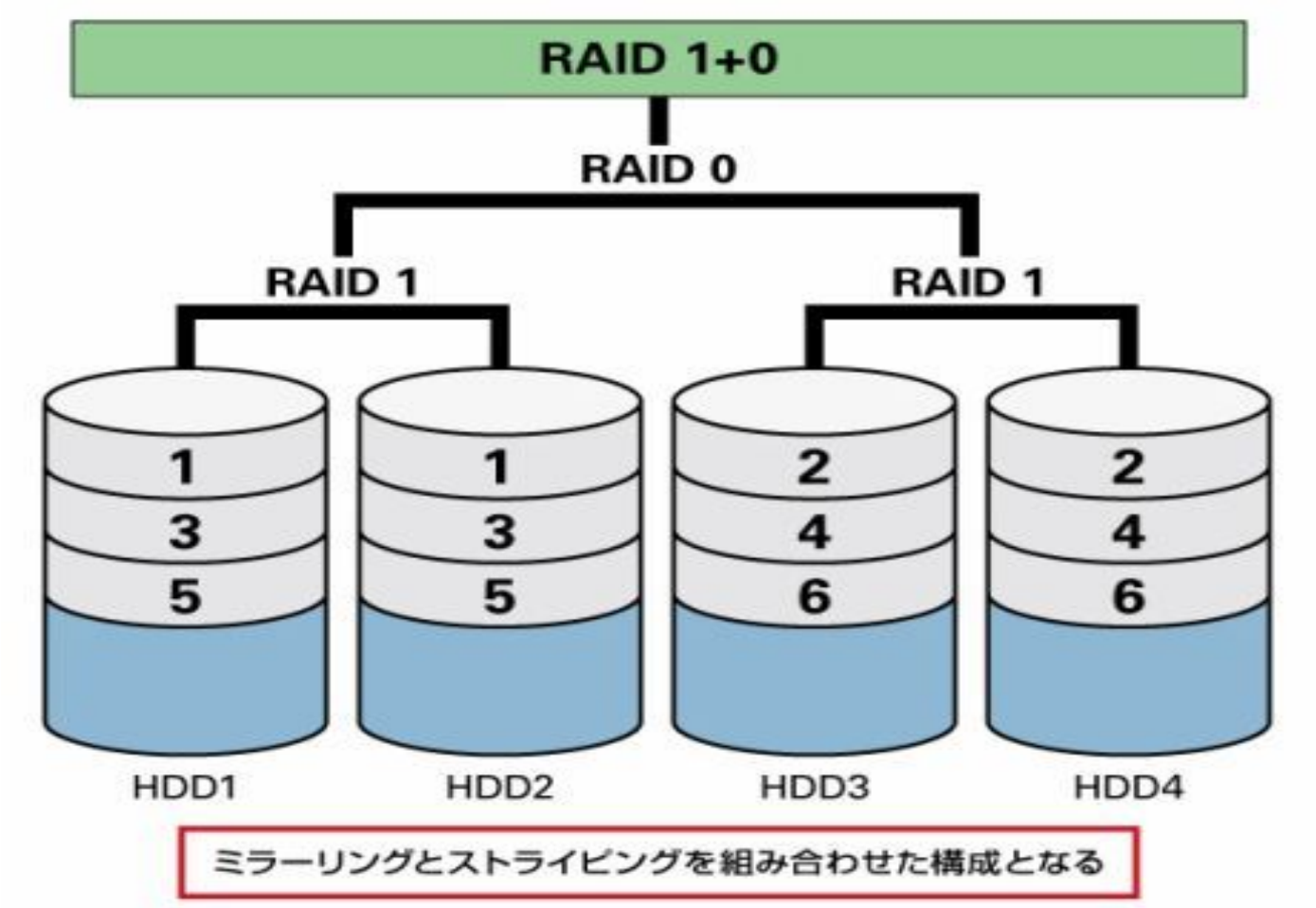
- ミラーリングと呼ばれ、2台のディスクにまったく同じデータを同時に書き込む
- 片方が破損しても、もう一方からデータを読み出せるのでシステムは問題なく稼働する
- 信頼性の向上方式
- 両方に同じデータを書き込むことになるため、実際に使用できるデータの容量は本来のディスクの容量の半分になる

RAID1



http://ascii.jp/より

RAID10

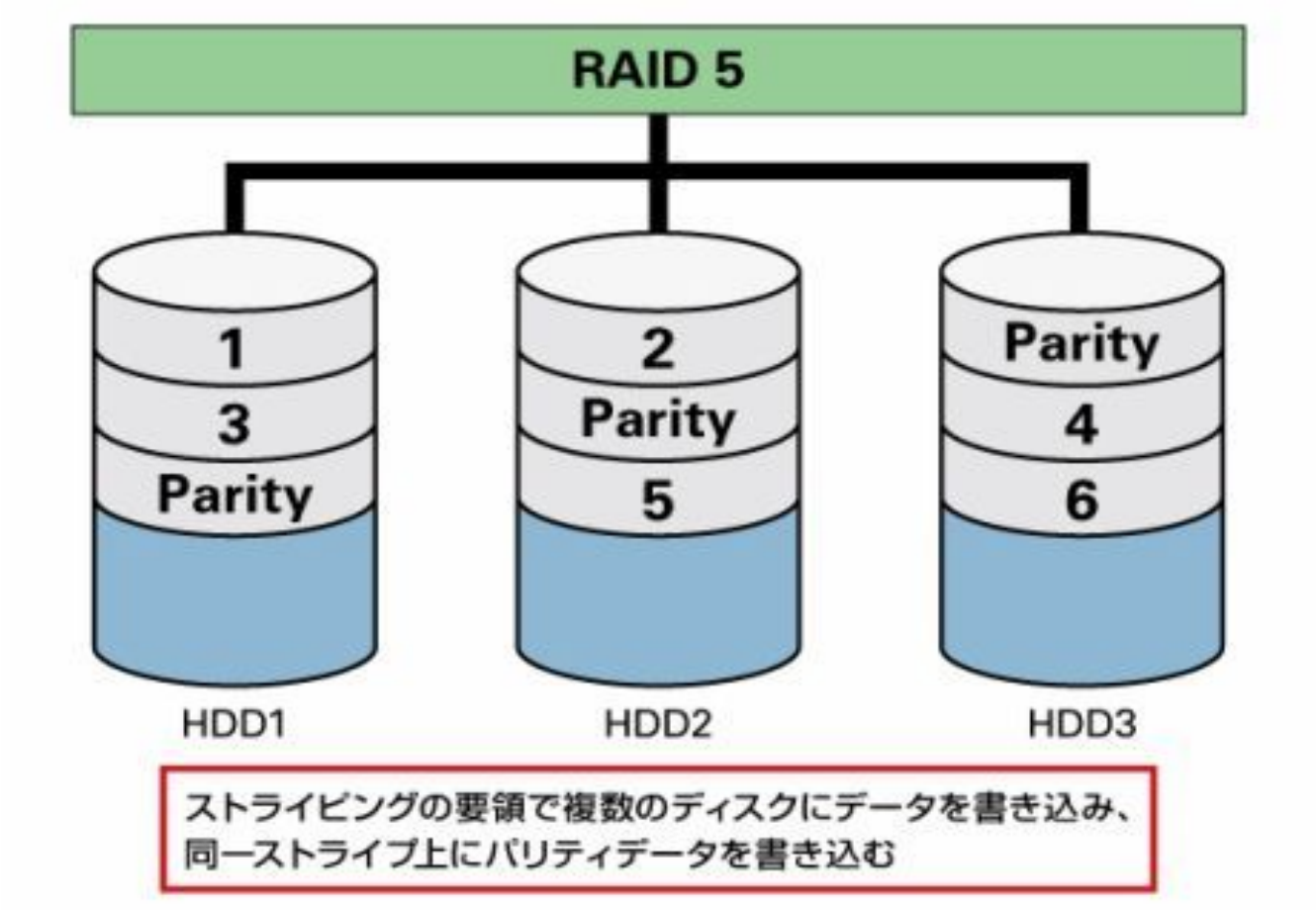


http://ascii.jp/より

RAID5

- データからパリティと呼ばれる誤り訂正符号を生成し、データと共に分散して記憶
- データだけでなくパリティも分散することで、信頼性の向上と性能の向上が期待でき、現在最も普及している方式
- RAID1よりディスクの使用できる割合も向上
- 回復可能なのは1台のディスクが故障したときまでで、同時に2台が壊れると回復は不可

RAID5

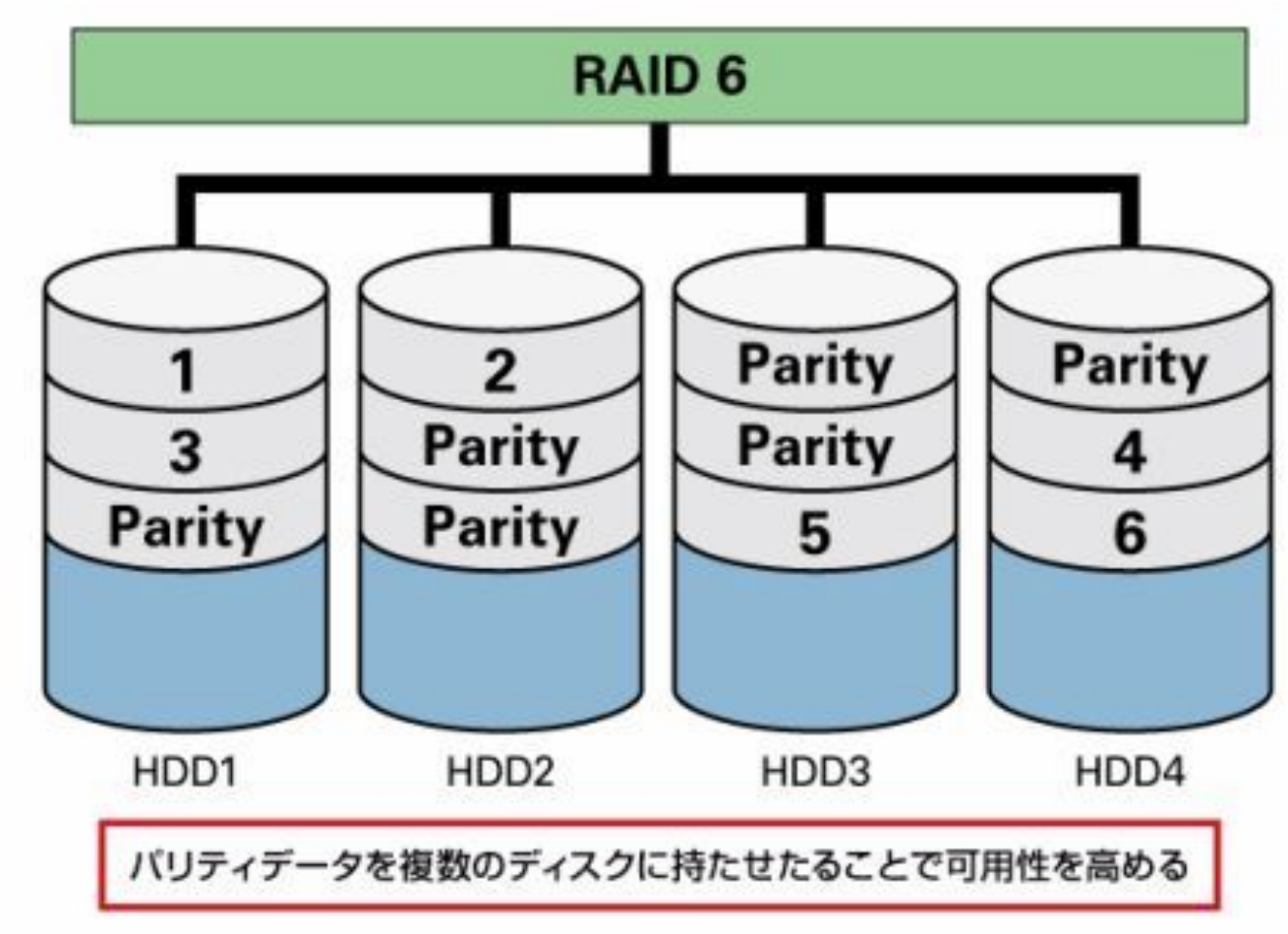


http://ascii.jp/より

RAID6

- RAID5にもうひとつ独立なパリティを付け加え、１つのデータブロックが2つのパリティを持つ
- この方法のメリットは、同時に2つのディスクが壊れた場合でもデータの保全が可能
- 冗長ディスクが余分に必要な分だけコストは高くなる

RAID6



http://ascii.jp/より

運用面の対策

- 教育
  定期的にセキュリティ教育の受講を義務化
- アカウント管理
  従業員のアカウントの登録及び削除
- 情報の収集
  管理者は常にセキュリティ関係情報を収集
- ログの収集の監視
  ログの集中管理と危険性の高いログの抽出など
- セキュリティ管理者の不正抑止
  管理者を2名以上にして相互に牽制、ローテーション

廃棄方法

- 適切な廃棄方法が必要
  廃棄が不適切だと情報漏えいの可能性
- HDD消去用のソフト
  16進数の00やFF、乱数を複数回上書きする
- HDDの磁気消去（専用のハードウェア）
- HDDの物理的破壊（専門の業者に依頼）
- CD-R、DVD等のメディアの廃棄
  カッターナイフで傷をつける程度では読みだされる

インシデント対応

- 不正アクセス、情報漏洩等が発生した場合に備えて、予め行動基準を準備し、被害の拡大を防止
- コンピュータセキュリティに関係する人為的現象で、意図的なものと偶発的なものの両方を含む
- 不正アクセスのような人為的、意図的なもの
- 脆弱性が放置されたWebアプリケーションから個人情報が漏洩してしまうといった偶発的なもの
- インシデント対応とは、これらの事象の発生から回復までの行動をさす

インシデント対応（復旧作業）

- 状況情報の収集と保全
- インシデントから隔離する短期的な処置

  不正アクセスからの復旧

  ウイルス感染からの復旧

  情報漏洩からの復旧

    SQLインジェクション等の不正アクセス

    P2Pソフト経由やメール後送信
- システム通常運用への復旧

ポリシーの策定による対策

- セキュリティと利便性は相反する性質を持つことから、セキュリティポリシーの策定が重要
- セキュリティポリシーは業務上守るべき規則として、実行力を持たせる
- 内部犯行の抑止
- 情報漏洩の危険性の抑止

  自宅にUSBやメールで持ち帰り作業する等
- ダブルスタンダードの危険性

情報漏洩対策

- 情報セキュリティの中でも、機密情報の漏洩は企業の存続に深刻な影響を与えるため、情報漏洩対策は情報セキュリティの中心
- 代表的な対応策

  必要以上にアクセスさせないこと

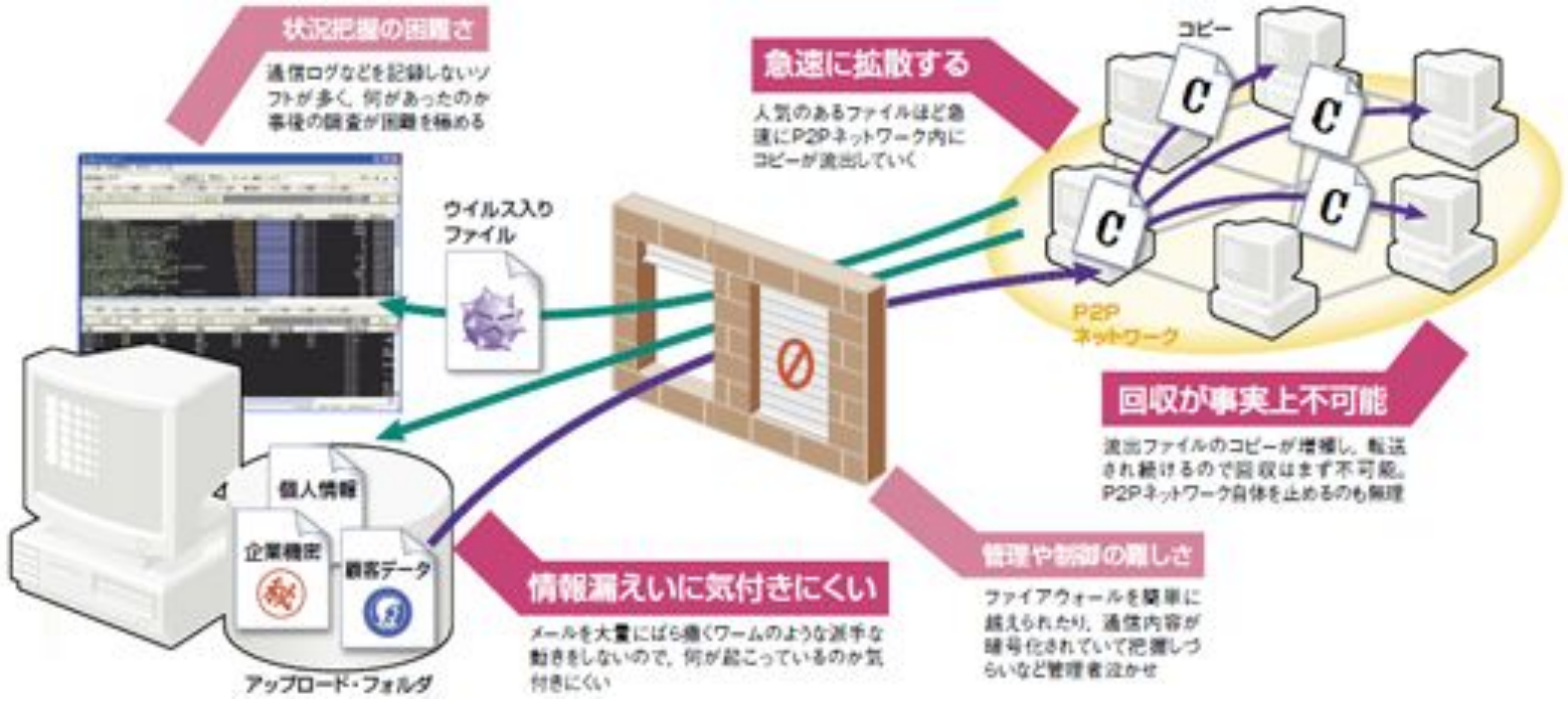
  許可なく持ち出させないこと

  確実に廃棄すること

Web経由での漏洩

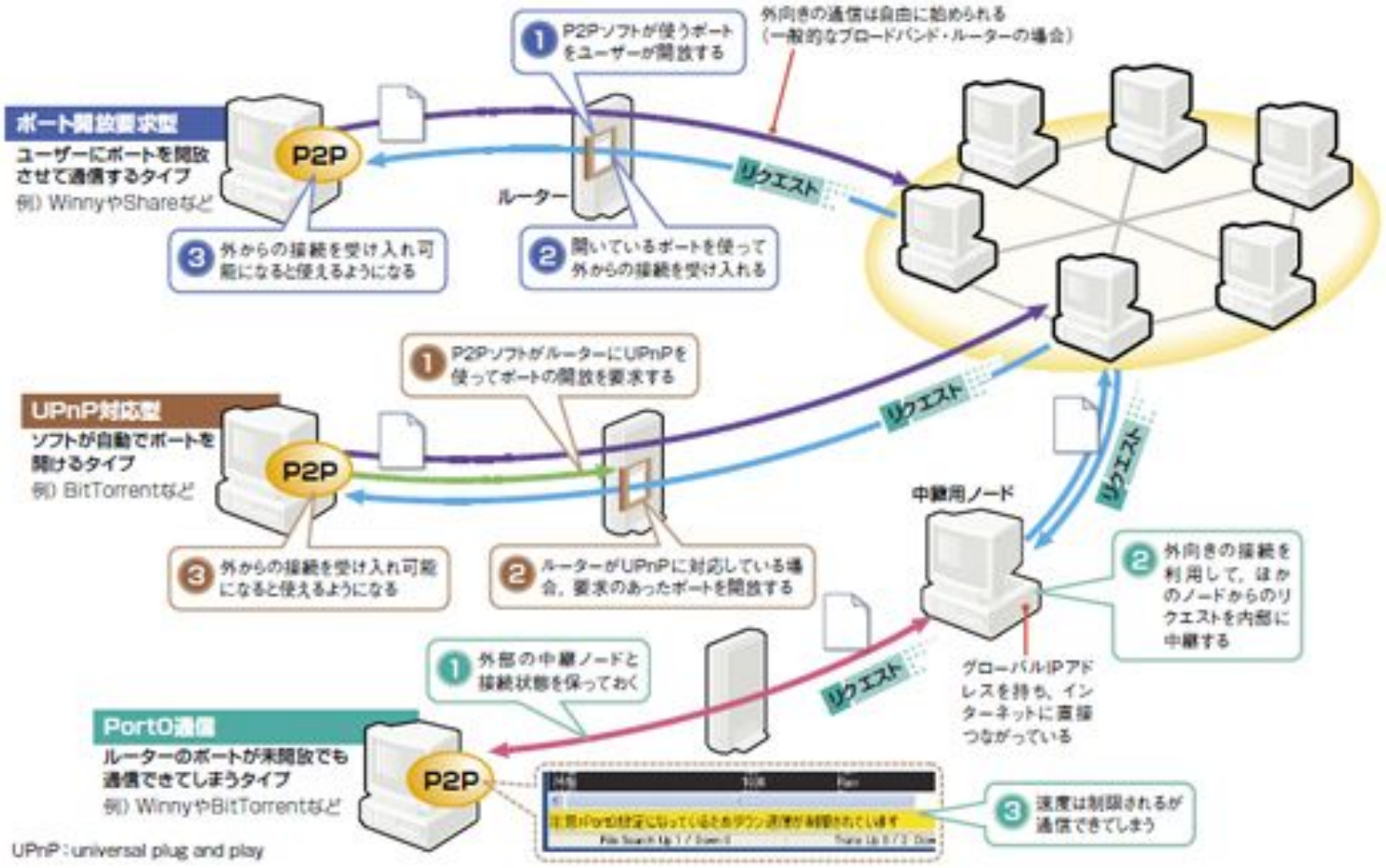
- 多くの業務においてWebを使用しないと支障がでるため、Webの利用を禁止するのは困難
- Webアプリの脆弱性による漏洩
- P2P（サーバを介さずPC同士が通信）による漏洩
- Webメールによる社内文書の送信
- ファイル転送サービスやWebストレッジ経由の漏洩

P2Pファイル共有ソフトによる情報漏洩



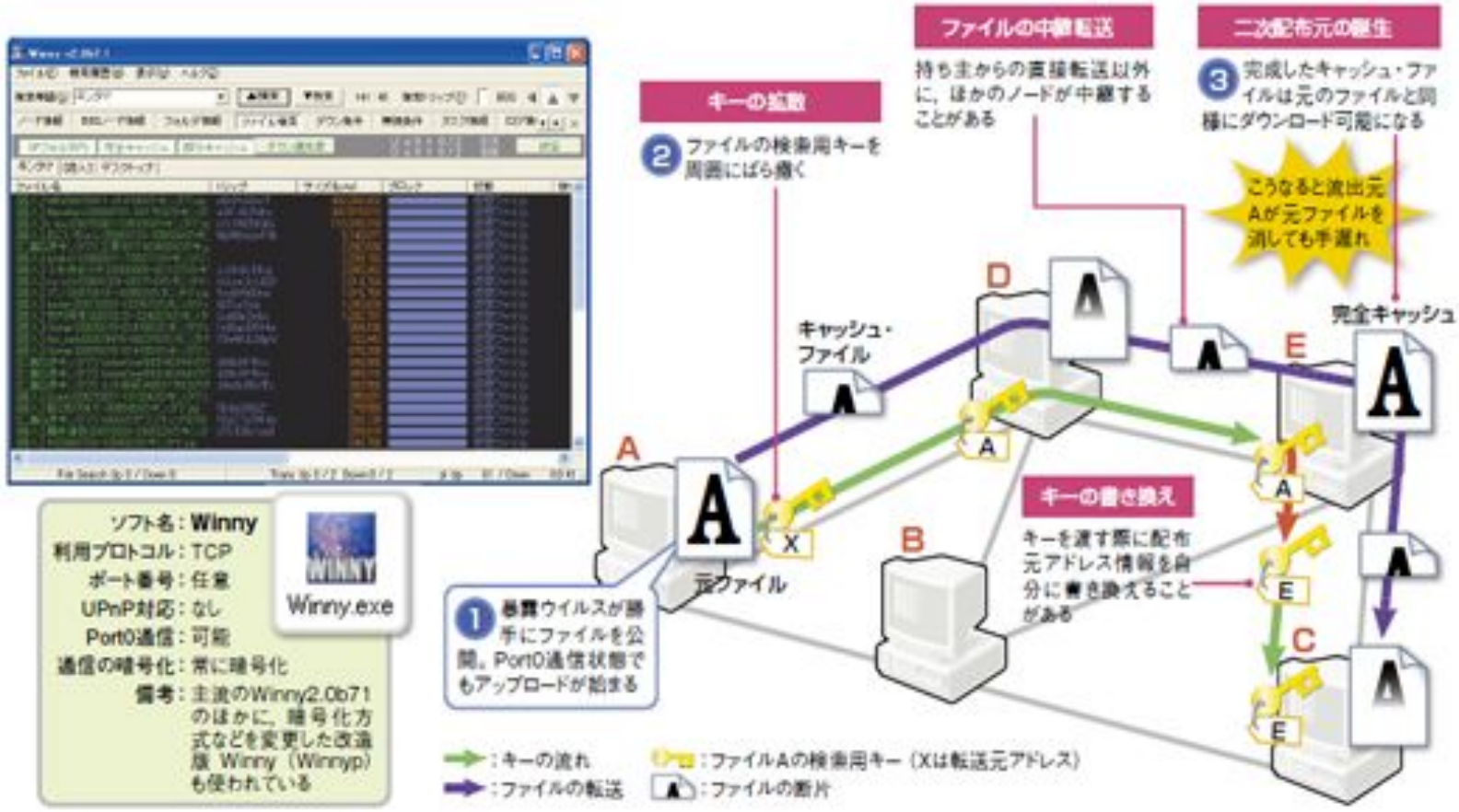
http://itpro.nikkeibp.co.jp/より

P2Pソフトの通信パタンは3種類



http://itpro.nikkeibp.co.jp/より

Winnyによる情報漏洩の流れ



http://itpro.nikkeibp.co.jp/より