「マルチメディア，分散，協調とモバイル
(DICOMO2021) シンポジウム」 令和3年6月-7月

秘密分散ライブラリ応用と実装要件について

山澤 昌夫[1] 米津 武至[1,2] 五太子 政史[1] 山本 博資[1] 辻井 重男[1]

概要：重要情報 S を保管する場合，S の紛失や敵による S の破壊の心配と，敵による S の盗聴の心配がある．前者の心配に対しては S のコピーを複数作ることにより対処出来るが，コピーが増えると後者の心配が増す．この相克を解決するのが，暗号学のなかでの秘密分散法 (Secret Sharing Scheme) である [4]．
重要情報を取り扱う局面は，これまでも頻出しているが，特に，公開鍵方式での秘密鍵が露わに資産価値とリンクする暗号資産等が普通に出回るようになった現在，具体的な施策が強く求められると考えられる．筆者等はこうした需要に対応したライブラリのあり方を検討した．本報告では，実装検証まで至らないが，検討過程を記すことにした．

Implementation Requirements for Secret Sharing Library Applications

MASAO YAMASAWA[1] TAKESHI YONEZU[1,2] MASAHITO GOTAISHI[1] HIROSUKE YAMAMOTO[1]
SHIGEO TSUJII[1]

1. 秘密分散の応用について

近年の IT システムでは，認証系のセキュリティ強靱性が要求される例が出てきている．筆者等は，認証情報を分散運用する IT システムを提案しているが，その実装に当っては，複数の方式，パラメータが想定されるので，選択肢が多岐にわたる．

ここでは，ベースとする技術を国際標準 [1] 起点として考え，具体的には ISO/IEC19592-2 の秘密分散アルゴリズムの実装形態について，システム要件，実現形態の検討を行う方向とした．

筆者等が要件を検討した分野は，ひとつは暗号資産の領域 [6] である．この領域では暗号資産所有を示す「秘密鍵」の扱いについて検討している．IoT デバイスの真正性についての領域 [7]，同分野のサプライチェーンセキュリティ [9]，製造分野における個体集合体の真正性保証 [10]，と言った IoT システムの領域は産業のセキュリティと言う意味で重要である．

健康管理データ等の個人データ活用が活発に論じられている．このような, 個人の機微データは個人の承認の下で移動, 蓄積, データ処理がなされなければいけない. そのため，最も安全性が高い方式である必要がある. この分野は分散 PDS システム [8] であるが，ここも前例同様，重要と考えている．

1 中央大学研究開発機構
Chuo University, Research and Development Initiative
2 株式会社リーディングエッジ
Leading Edge, Inc.

2. 実装要件について

下記観点から実装要件を抽出し，実装に便利な秘密分散方式，実装パラメータの検討を行った．

- 分散対象データ種類
  守るべき対象のデータを同定し，分散運用方式等，システム要件を決定する必要がある．
- 分散対象データサイズ
  データサイズについては，処理負荷の観点もあるが，むしろ運用面の検討が重要と考える．
- 分散片の流通
  流通過程におけるインテグリティ要件があると考える．
- 秘密情報の復元
  復元操作のセキュリティ要件があると考える．

3. 分散対象データについて

秘密分散の応用をこれまで考えてきたが，俎上にのせたのは暗号資産の領域，単体あるいは複合体としての IoT デバイスの真正性の領域，および個人データマネジメントの

領域などである．これらの領域においては，分散対象とする部分は，公開鍵暗号方式での秘密鍵，あるいは，公開鍵暗号基盤（PKI：Public Key Infrastructure）の鍵ペアのうちの秘密鍵や電子証明書（Certificate）などが分散対象データとなる．

秘密鍵なり電子証明書が分散対象となるが，処理時のデータサイズについてはメタデータやインテグリティ処理のためのデータを考慮すべきなので，その分は割り増しとなると考えられる．

4. 分散片の流通とインテグリティ

暗号資産用のコールドワレットの応用例を別にすれば，分散処理後の分散片は通信路を介して流通する．通信路としてインターネットを考えるが，そこでは一定のデータ誤りを前提にしなければならない．通常 TCP-IP 通信や Ethernet 通信では伝送媒体の誤りはプロトコルの誤り検出（チェックサム）で検知され，検知された場合は再送によって訂正される．しかし，文献 [5] をはじめ，実際の通信路における誤り見逃しが一定数あるとの指摘は多数ある．

すなわち，分散片の流通においては受け取った分散片にデータ誤りが混入することへの対処が必須である．

5. 実装におけるセキュリティ

秘密分散機能の実装に当っては，暗号プログラムの実装なのでセキュアプログラミングに関する以下の規準を考慮すべきである．

(1) セキュアプログラミングガイド
JPCERT が公開している下記規定．
https://www.jpcert.or.jp/sc-rules/00.introduction.html
セキュアプログラミングとは: セキュアプログラミングの別名は「防御的プログラミング」「セキュアコーディング」である．
セキュアプログラミングの基本は 10 項目と言われる．
CERT Top 10 セキュアコーディングプラクティス
01. 入力をバリデーションする
02. コンパイラの警告に用心する
03. セキュリティポリシーの為に構成／設計する
04. 簡易にする
05. デフォルトで拒否する
06. 最小権限の原則を支持する
07. 他のシステムに送信するデータを無害化する
08. 縦深防御を実践する
09. 効果的な品質保証テクニックを利用する
10. セキュアコーディング標準を採用する

(2) ISMS に関する規準 ISO/IEC27002,
特に 14.2, 14.3 が重要である．[3]

(3) 暗号化モジュールとしての規準
連邦情報処理規格 (FIPS) 文書 140 は米国政府機関向けの標準規格であるが，情報技術製品としてあるべきセキュリティ要件を定義しているので，やはり，これを考慮した実装とすべきである．

(4) 乱数発生に関する規準には，NIST.SP.800-90B: 乱数エントロピー源選択の基準，NIST.SP.800-90Ar1: 乱数決定論的方法の基準，RFC4086（乱数生成方法），等があり，これらにしたがった実装にすべきである．

6. まとめ

秘密分散アルゴリズムの IT システムへの応用を考え，ライブラリの形式での実装を検討した．今後、検討レベルを上げ，具体化を推進したい．

謝辞

実装検討にあたりご尽力いただいた（株）ベガの辻様，MIRUS（株）の南様，ならびに関係者の方々に感謝いたします．

参考文献

[1] International Organization for Standardization/ International Electrotechnical Commission, “Information technology — Security techniques — Secret sharing —Part 2: Fundamental mechanisms,” ISO/IEC 19592-2, Oct. 2017

[2] Shamir, Adi,“How to Share a Secret,”Commun. ACM, vol.22. no.11, pp.612–613, Nov. 1979
http://doi.acm.org/10.1145/359168.359176

[3] INTERNATIONAL STANDARD, ISO/IEC 27002:2013, “Information technology–Security techniques–Code of practice for information security controls,” Oct. 2013.

[4] 岡本，山本,“現代暗号,”シリーズ／情報科学の数学，産業図書, pp.209–219, Jan. 2000.

[5] Stone, J., Partridge, C.,“When the CRC and TCP checksum disagree,” SIGCOMM ’00. *Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication* , pp.309-319, Aug. 2000
http://doi.org/10.1145/347059.347561

[6] 山澤昌夫，角田篤泰，近藤健，才所敏明，五太子政史，佐藤直，辻井重男，野田啓一，“暗号通貨（ビットコイン）・ブロックチェーンの高信頼化へ向けての MELT-UP 活動 — 秘密鍵管理を中心に —,” *Proc. SCIS2018*, 4F2-2. Jan. 2018.

[7] 松本義和，辻井 重男，白水公康，瀬瀬考平，“重要 IoT デバイスへの PKI 電子認証の実装 ” *Proc. CSS2019*, 2F1-4, pp.808–811，Oct. 2019.

[8] 山澤昌夫，五太子政史，山本博資，辻井重男，南重信，吉光久仁彦，野田啓一，“セキュア分散 PDS システムの秘密鍵保護について,” *Proc. SCIS2020*, 2C2-2. Jan. 2020.

[9] 山澤昌夫，五太子政史，山本博資，松本義和，白水公康，豊島 大朗，瀬瀬考平，近藤健，辻井重男，“分散個体群を認証するための秘密分散法要件の一検討，” *Proc. SCIS2020*, 4G-1，pp.688-692，June 2020.

[10] 五太子政史, 山澤昌夫, 山本博資, 藤田亮, 松本義和, 白水公康, 豊島大朗, 瀬瀬考平, 近藤健 , 辻井重男 ，“分散個体群認証のための秘密分散法について,” *Proc. SCIS2020*, 4G-2. pp.693-697，June 2020.