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（II）
-運用と倫理-

山澤 昌夫[1]　角田 篤泰[1]　近藤 健[1]　才所 敏明[1]　五太子政史[1]　佐藤　直[1]　山本博資[1]　辻井 重男[1]
野田 啓一[2]

概要：暗号通貨の仕組みにおいて，ユーザが作成する秘密鍵が価値操作の基礎である．市場での暗号通貨流通においては秘密鍵運用においてインシデントが続いている．インシデントの要因は，暗号通貨仕組み上に秘密鍵保護の機能が入っていないという，構造が起因している．暗号通貨の仕組みが強固であるので，秘密鍵以外の情報は非安全な媒体でも使うことができるが，同じ認識で秘密鍵を扱うことはできない．筆者等は，CSIS2018 において，秘密鍵の管理に物理プロセスを導入する事を特長とするセキュリティ実現方式を提案した．構造的問題を内包する価値操作系を総合的に機能するように構成するには，Management：「M」，　Ethics：「E」，　Law：「L」，　Technology：「T」がからむ自由と規制の相克を止揚（MELT-UP）するなかで，交換所等への適用領域を広げた解を導くべく検討する必要がある．本論文では，「M」と「T」の面からの提案をさらに発展させ，適用領域拡大に向け「E」を加えて，「M」「T」を向上させる検討を行ったので，報告する．

キーワード：三止揚，MELT-UP，ブロックチェーン，暗号通貨，ウォレット，取引所，秘密分散，電子印鑑

MELT-UP Activities To Enhance Security Of Cryptocurrency, Blockchain（II）
-Key Management and Ethics-

Masao Yamasawa[1]　Tokuyasu Kakuta[1]　Takeshi Kondo[1]　Toshiaki Saisho[1]
Masafumi Gotaishi[1]　Naoshi Sato[1]　Hirosuke Yamamoto[1]　Shigeo Tsujii[1]　Keiichi Noda[2]

Abstract: In cryptocurrency systems, private keys to activate unused transaction are outside of the cryptographic protection mechanism. Recent incidents suggest that users are not fully aware of the mechanism of cryptocurrency, and lack basic knowledge to handle the key securely without being exposed to risks associated with the internet environment and digital devices. We would like to discuss methods to achieve risk-free environment for private key management. The discussion would include the MELT-UP cycle to cover not only management aspect but social implication and technology consideration. The discussion of Technology and Management has clarified the mechanism in which the private key could be handled within cryptographic protection mechanism. The results were applyed to a cryptocurrency exchange system to enhance overall security.

Keywords: MELT-UP cycle, blockchain, cryptocurrency, Wallet, exchange, secret sharing

[1] 中央大学研究開発機構
Chuo University, Research and Development Initiative
[2] 慶應義塾大学 SFC 研究所
Keio Research Institute at SFC

1. はじめに

筆者等は今年の 1 月２６日，暗号と情報セキュリティシンポジウム（SCIS）2018 新潟において，仮想通貨の秘密鍵管理の高信頼化の提案を行った [1]．その日の午後，仮想通貨交換業者のコインチェック株式会社が，「同社のが運営する仮想通貨取引所サービス「Coincheck」において，一部機能の停止に至る事象が発生致した．その事象とは，保有している NEM が不正に外部へ送金されたこと，その原因は究明中」と発表した [2]．

後の調査で，NEM の秘密鍵がネットワークに接続されたウォレットにより管理されていて，秘密鍵の保護策が適切でなかったため，不正送金されたものと判明した [2]．流出した仮想通貨は当時の価値で５８０億円相当と報道された [3] 昨年金融庁，消費者庁，警察庁連名で 2018 年 8 月 10 日に発行された仮想通貨に関する注意喚起フライヤでも，仮想通貨の流出インシデントの記述がある．

仮想通貨のような暗号資産は，次章で触れるが，その所有，保管，譲渡時に秘密鍵情報が生のまま扱われ，暗号学的プロテクションが働かない．したがって，まずは運用手段により保護策を講じるのであるけれどインシデントが起こる．本稿では新潟論文 [1] の延長として，通貨取引所システムに秘密分散技術を適用する方法を論じた．本方法が普及すれば，流出インシデント機会は減少すると考えられる．

2. 仮想通貨交換所でのインシデントの現状

等について」平成 30 年 3 月 22 日警察庁広報資料にある『インターネットバンキングに係る不正送金事犯』の警察庁統計によると，平成 29 年のインターネットバンキングにおける不正送金インシデントは発生件数は 425 件と，ピーク時の平成 26 年と比較して 4 分の 1 以下に減少，被害額は約 10 億 8,100 万円とピーク時の平成 27 年にくらべ 3 分の 1 に低下した．金融機関によるモニタリングの強化，ワンタイムパスワードの導入等の対策により，被害が大幅に減少したと当局は見ている．

一方，仮想通貨交換業者等への不正アクセスによる不正送信事犯（流出インシデント）については，認知件数が 149 件，被害額約 6 億 6,240 万円相当と五月以降急増した．仮想通貨交換業者等の多くでは，二要素認証を導入して利用者に利用を推奨しているものの，認知した 149 件のうち 122 件（81.9 %）では，ＩＤ・パスワードによる認証のみしか使われていないなど，二要素認証を利用していなかった．　仮想通貨については，これに加えて，累積値の 9 倍を超す時価５８０億円相当の NEM が流出すると言う大きなインシデントが，年があけた平成 30 年 1 月 26 日に記録されている．

このため、いまに至っても、インシデントが起きている。

【図表12　インターネットバンキングに係る不正送金事犯の被害額の推移】

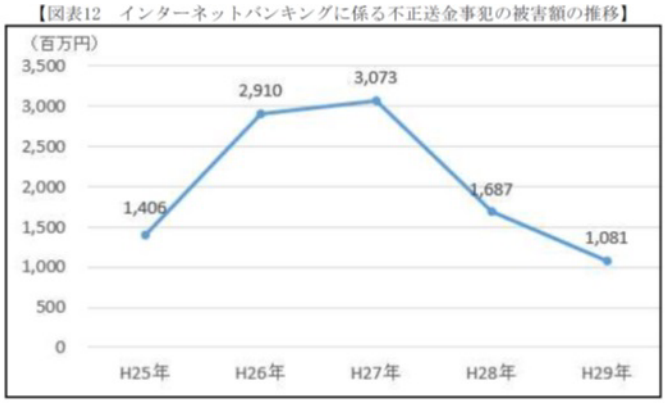

図 1　『インターネットバンキングに係る不正送金事犯』の警察庁統計によると銀行からの不正送金インシデントは 10 億 8,100 万円で 27 年度比三分の一．仮想通貨のインシデントは，認知件数 149 件，被害額約 6 億 6,240 万円相当、二要素認証不適用が 122 件（81.9 %）．

Fig. 1　Incident statistics for cryptcurrency by MPT,1H 2017

警察庁のインターネットバンキング統計では、図 1 のように減少（被害額）しているが暗号通貨関係は増大している。

2.1 既存方式におけるリスク

2018 年 4 月 10 日に金融庁，仮想通貨取引事業研究会（第一回）資料３，スライド＃ 32 から＃ 39 に既存方式のリスクが記述されている [7]．それによれば，「取引に用いられる対象仮想通貨の管理は秘密鍵を用いて行われることから，秘密鍵の紛失や悪用等によってお客様に損失が生じる可能性があり」とされている．

取引所は「ウェブウォレットの形態」であり，それがそのままリスクとなる．このリスクを低減するため，既存方式においては，「当社および外部事業者との間で連携して実施するマルチシグの仕組み」が推奨されている．ほかのリスクも挙げられている [9]．以下に抜粋を示す．

〇価格変動リスク：1. 対象仮想通貨そのものの価値変動リスク，2.OKEX.com のみに取り次ぐことによるリスク，3.BTCFXR 特有のリスク流動性リスク：1. BTCFXR の流動性リスクについて 2. OKEX.com の流動性について 3.BTCFXR 特有の流動性リスク証拠 BTC，手数料の変更によるリスク，（BTCFXR のみ）取引停止時間リスク，商品リスク，ロスカットにおけるリスク，レバレッジによるリスク，取引所仕組みそのものに内在するリスク，当社の破たんリスク

〇対象仮想通貨のネットワークによるリスク対象仮想通貨の取引では，十分な取引確認（ブロックチェーンでの取引の認証）が完了するまで取引が成立せず，一定時間保留される状態が続きます．対象仮想通貨のネットワークにおいて認証が取れ，且つ，当社での確認が行われるまでお客様へのビットコインの移転は成立せず，アカウントにおけるビットコインの残高へは反映されません．また，認証が

完了するまでの時間に価格が変動することにより，お客様の取引が成立しないこと等により，お客様に損失が生じる場合があります．

さらに，対象仮想通貨のネットワークの管理者が存在する場合，当該管理者の破たん等により対象仮想通貨の取引が不可能になり，お客様に損失が生じる場合があります．ブロックチェーンでの認証の過程でお客様の取引がキャンセルされる場合があります．

なお，取引に用いられる対象仮想通貨の管理は秘密鍵を用いて行われることから，秘密鍵の紛失や悪用等によってお客様に損失が生じる可能性がありますが，当社の秘密鍵の管理については当社および外部事業者との間で連携して実施するマルチシグの仕組みによって安全性を高めています．

〇システムリスク対象仮想通貨取引は，インターネット，通信機器（お客様の利用するものを含みます．）及びコンピューターシステム機器を使用した取引ですので，通信回線やシステム障害が発生し，お客様の取引（取引の成否のほか，対象仮想通貨の授受や金銭の授受を含みますがこれに限られません．）に支障が生じるリスクがあります．通信回線やシステム障害とは，当社もしくは当社以外の法人等またはお客様が運用または使用する通信回線及び通信機器，コンピューターシステム機器の障害による情報伝達の遅延，不能，誤作動等，または受領した情報の誤謬，停滞，省略及び中断ならびに明らかな不具合（1 回線の障害やお客様のパソコン等の不具合は含まれません）が発生していると当社が判断し，かつ，お客様がインターネット（ 当社ウェブサイト，スマートフォンサイト・アプリケーション）経由でご注文等（対象仮想通貨の送付，売却その他の取引全てを含みます．以下同じ．）いただけなくなるか，お客様のご注文等が遅延し，もしくは不能となった状態をいうものとします．通信回線及びシステムの障害により実勢レートと大幅に乖離した価格での約定などの際に，当該約定が取り消される場合や，取引の不成立等によりお客様に損失が生じることがあります．当社のシステムに起因した障害の場合は，当社において，かかる障害が生じた場合には早期の復旧につとめることにより，そのリスクの軽減を図りますが，お客様が損失を被るおそれは否定できません．

〇法令・税制変更リスク現在，対象仮想通貨取引を行う関係者に適用される対象仮想通貨に関する税・法令については流動的です．特に，ビットバンクの取引は，日本に所在する当社が提供するものであり，原則としては，日本法の適用をうけることになります．現状において，対象仮想通貨に対する各国の規制はまちまちであり，対象仮想通貨の取引量が増大するなどの事情によっては，将来的に各国の法制度や税制または政策の変更等により，対象仮想通貨取引が禁止，制限又は課税の強化等がなされ，対象仮想通貨の保有や取引が制限され，または現状より不利な取扱いとなるおそれがあります．この場合，お客様に予期しない損失が生じるおそれがあります．詳しくは各自税務署・税理士・法律事務所等にお尋ねください．

〇個人情報に関するリスクお客様が当社のサービスに登録したメールアドレス，氏名等や，当社より発行された口座番号，パスワード等の個人情報が，ビットコイン取引に関するシステムや通信回線の障害，不正アクセスや盗聴等により，滅失，毀損又は第三者に漏えいすることによってお客様に損失が発生する可能性があります．お客様は，口座番号やパスワード等の情報を第三者に知られないように十分に注意いただき，管理してください．

〇銀行口座リスクビットバンクトレードに関し，当社がお客様の預託金の預託を受ける銀行口座や，当社が対象仮想通貨の取引に関連して保有する銀行口座が不正送金事件などの調査対象となり，口座が凍結されるおそれがあります．

2.2 取引所における既存の秘密鍵管理方式

2.2.1 取引所はウェブウォレットの形態

ウェブウォレット（WEB ウォレット）とは，インターネット上で秘密鍵を保管してもらうサービスのことである．アカウントを登録すると，その「アカウント」と「運営側が保有する秘密鍵」が紐づけられる．秘密鍵は基本的に運営側が自動的に発行してくれるので，利用者が知ることはありまない．運営側が発行した秘密鍵（に対応した，アドレス）に対して利用者が仮想通貨を送金することで，その秘密鍵（に対応した，アドレス）の仮想通貨残高が増えるという仕組みである．

ウェブウォレットでは，秘密鍵の保管に関して，すべて運営側に任せることになる．取引所もウェブウォレットの一種であり，暗号資産の安全性は運営側のセキュリティ対策に依存することになる．

2.2.2 暗号学的保護からはずれた情報を管理

暗号通貨のしくみはブロックチェーンによるトラストのネットワーク展開と，公開鍵暗号によるトラスト事実（暗号資産）の所有．トラスト（暗号資産）を受け取るのは公開鍵で行うので，これは暗号学的に強固である．しかし，トラスト（暗号資産）を所有，保管，譲渡時は，秘密鍵情報が生のまま扱われ，暗号学的プロテクションについては「ブロックチェーンの外」で保護施策を講じなければならない．保護施策が弱いと，漏えいや盗難時のリスクが大きい．

取引所のサーバでは，秘密鍵情報を安全に管理しなければならない．2018 年 4 月 10 日に金融庁，仮想通貨取引事業研究会（第一回）資料 3 によれば [7]，二通りの保護施策が採られているとしている．これを MELT-UP プロセスに写像すると，下記のとおりである．「M」マネジメント面での保護施策・セキュリティ対策室の設置・情報セキュリティに関する，規程・ガイドライン・マニュアルの作成・

システムリスクに対する教育訓練の実施・複数管理者による電子署名の実施・ネットワークの監視・モニタリングの実施・インシデント時における体制整備

「T」技術面での保護施策・コールドウォレットの複数化・マルチシグにおける署名サーバー環境の分散化・高度な残高アルゴリズムの導入によりホットウォレットの比率を最小限化・生体認証によるＰＣログイン・トランザクション移動用専用デバイスの利用

自身で複数の署名鍵を別々の媒体で管理することや，Web ウォレットなどのサービス事業者が持つ署名鍵と利用者の署名鍵で運用することで，署名鍵の漏えい時のリスクを軽減すると言った保護方式である．いま話題にしている部分，すなわち交換所や Wallet などについて，「ブロックチェーンの外」であるので，ブロックチェーン固有の原理的な安全性とは違い，運用「M」に依存するところが大きい．「T」技術的な面で，暗号学的保護のループに入れる方策が望まれる所以である．

3. 秘密分散方式を利用した取引所の構成

既存システムにおけるリスクのうち，顧客秘密鍵を預託される部分において，取引所側および，顧客側に重大なリスクが存在する．コインチェックのインシデントはこの部分の脆弱性を標的型攻撃され，時価 580 億円の記録的な暗号資産流出になった．

我々は SCIS2018 新潟，JSSM 全国大会 2018 において，秘密鍵情報を暗号学的保護機構の下に置く方式を提案した．秘密分散による方式である．これを取引所に利用する．

一例として，現物取引を行うことを想定する．前提として，顧客は取引所に自分の口座を持ち，スマートフォンなどのゲートウェイデバイスによりアクセスできているとする．現物取引は取引の都度ブロックチェーンにつなげる運用は一般的でない（既存システムではそのようにしている）．したがい，口座への暗号資産の送金，法定通貨等での資金送金，および，その逆操作を考える．

(1) 口座への暗号資産の送金:ブロックチェーンに載せるトランザクションを分散片，ゲートウェイアプリにより生成し，自身の取引所口座とする仮想通貨アドレスに送金する．
(2) 口座からの暗号資産受取:顧客の仮想通貨アドレスを取引所に通知，そこ宛てのトランザクションを生成，送信してもらう．(取引所側がトランザクション生成に秘密分散を利用してもよい．)
(3) 法定通貨での資金送金:通常のインターネットバンキングを通じて取引所指定の銀行口座等へ送金する．
(4) 法定通貨での資金受取:通常のインターネットバンキング等で，自身の銀行口座へ振り込み．

3.1 顧客暗号資産をセキュアに管理する

ユーザーの USB メモリに保存される秘密分散片が価値とセキュリティの源で，スマートフォンは秘密分散片から署名するためのツールであり，かつネットワークへのゲートウェイである．現物取引モードで，取引の都度ブロックチェーンにつなげる運用を前提とすれば，その先で接続するネットワーク上のサーバは価値の送信，受取をするためのユーザーのエージェントとして機能する．既存の取引所システムや銀行等のシステムではサーバでユーザ管理，暗号資産管理，セキュリティ管理も行う．

本稿では、図 2 のような二通りのシステムを想定した。一方は既存のような取引所に秘密分散ウォレットをつなげていくもの（左の構成)、もう一方は取引所にも秘密分散による秘密鍵プロテクションを適用するもの（右の構成）である。

この構成の左のシステムでは，接続先のサーバ（エージェント）を切り替えても継続して使用することができる．また，スマートフォン（ゲートウェイ）を取り換えても継続して使用することができる．取引の都度ブロックチェーンにつなげる運用を前提とすれば，サーバでユーザ，暗号資産，セキュリティを管理する必要がなく，取引所システムの運用が楽になる．取引所システムはユーザと資産の二次管理をするだけでよい．

3.2 暗号資産の送出をセキュアにする

取引所の運用は，一般的には，交換業者での取引毎にブロックチェーンに反映するのではなく，顧客の仮想通貨は交換業者のコールドウォレットで一元管理（一部はホットウォレット）している．顧客による個々の取引時には交換業者の帳簿上で，顧客毎の有高を付け替えている．交換業者と顧客自身のウォレットとの間で入出金が行われる場合のみブロックチェーンに反映される．現物以外の取引（証拠金取引，信用取引，先物取引）の場合，差金決済のためブロックチェーンには反映されない．

こうした運用形態を可能にするためには，取引所システムからの送金トランザクションを，すなわち，取引所に帰属している暗号資産をセキュアに管理しなければならない．既存システムでは「顧客の仮想通貨は交換業者のコールドウォレットで一元管理（一部はホットウォレット）している」と言うところを，分散秘密鍵による形に置き換えることができる．

4. おわりに

取引所の資産保護に秘密分散による方式が利用できる．国内の仮想通貨取引所の直近年度末の総資産額は 6,900 億円であった．役職員あたりの管理資産は平均 33 億円にのぼる．このように，仮想通貨交換業者は「少ない役職員で多額の利用者財産を管理してる実態」が金融庁の「仮想通

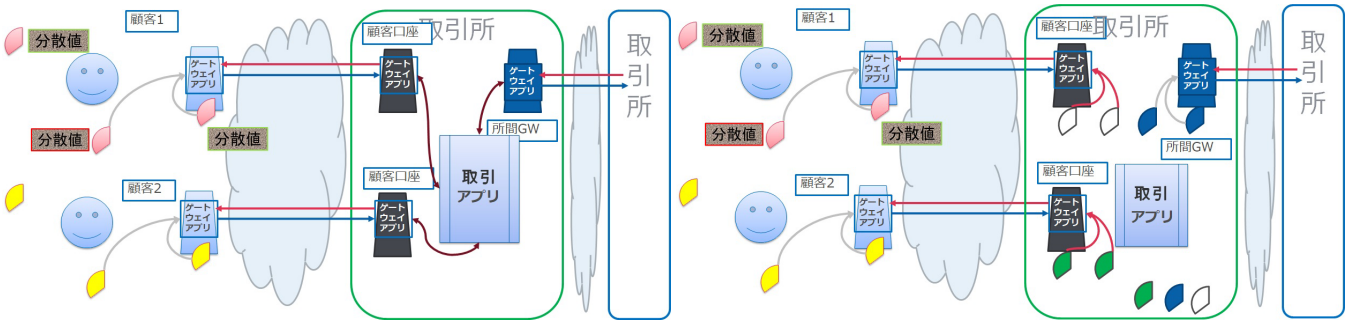

図 2 顧客側ウォレットに秘密分散による鍵保護を適用したシステム (左)，取引所側にも適用したシステム（右）

Fig. 2 Exchange systems with cryptographic protection mechanisms to secret keys for subscriber wallets(left) and for both (right).

貨交換業者等の検査・モニタリング　中間とりまとめ」平成 30 年 8 月 10 日によって明らかになっている．

セキュリティを高めるには人的コストも懸念されるなか，秘密分散技術による高セキュリティ化は有用と考えられる．今後の適用に向けて実用化検討を進めたい．

謝辞　本稿をまとめるにあたり，ビットコインのシステム，コミュニティの構造についてご教示いただいたセコム株式会社 IS 研究所の佐藤雅史主任研究員，長谷川佳祐研究員に深謝いたします．また，株式会社ビーエス・コーポレーションの徐相淑代表取締役社長には，電子印鑑デバイス，Dragon Wallet の開示機会を提供していただきました．厚く御礼申し上げます．

参考文献

[1] 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-」，論文番号 4F2-2, 2018 Symposium on Cryptography and Information Security Niigata, Japan, Jan. 23 - 26, 2018, The Institute of Electronics,Information and Communication Engineers

[2] <http://chain.nem.ninja/#account/NC4C6PSUW5CLTDT5SXAGJDQJGZNESKFK5MCN77OG/3013407>（2018 年 8 月 19 日アクセス）

[3] https://jp.techcrunch.com/2018/01/27/coincheck-xem/（2018 年 8 月 19 日アクセス）

[4] https://www.fsa.go.jp/news/30/singi/20180410.html（2018 年 8 月 19 日アクセス）「仮想通貨交換業等に関する研究会」（第 1 回）議事次第

[5] https://www.fsa.go.jp/news/30/singi/20180410-1.pdf メンバー等名簿

[6] https://www.fsa.go.jp/news/30/singi/20180410-2pdf 説明資料（事務局）

[7] https://www.fsa.go.jp/news/30/singi/20180410-3.pdf 説明資料（日本仮想通貨交換業協会）

[8] https://www.fsa.go.jp/news/30/singi/20180410-4pdf 説明資料（みずほ証券株式会社小川様）

[9] <https://www.bitbanktrade.jp/risk>（2018 年 8 月 18 日アクセス）

[10] 楠 正憲，「ビットコインが生んだブロックチェーンへの誤解と期待」日経 FinTech，2016 年 08 月 04 日，国際大学 GLOCOM，<http://tech.nikkeibp.co.jp/it/atcl/column/16/062400138/073100004/?P=4>

[11] 佐々木　良一, 宝木　和夫,“印鑑と電子印鑑の歴史と類似性の分析,”情報処理学会論文誌，Vol.42 No.8，Aug. 2001，PP.1968 - 1974.

[12] Shamir, Adi,“How to Share a Secret,”Commun. ACM，Vol.22. No.11，Nov. 1979，PP.612–613，<http://doi.acm.org/10.1145/359168.359176>

[13] 辻井 重男 “自由，安心，プライバシーと三止揚- MELT UP～放送・交流サイト・個人通信・組織通信の枠組の中で～”民放経営四季報，No.101， pp.8-11，Sep. 2013.

[14] 才所敏明, 辻井重男, “社会的課題「安心・安全な電子メール利用環境の実現」のための三止揚・MELT-UP の試み,”電子情報通信学会 情報セキュリティ研究会（京都），ISEC2017-54，2017 年 11 月 9 日

[15] 辻井 重男, 才所 敏明, 山澤 昌夫, 佐藤 直,“三止揚・MELT-UP の視座からのデジタルフォレンジックに関する考察,”コンピュータセキュリティシンポジウム 2017 (CSS2017)，2017 年 11 月 23 日，1D4-1，IPSJ，CSS2017032

[16] 只木孝太郎, 土居 範久, 辻井 重男,“プライバシー保護条件付き情報開示,”電子情報通信学会論文誌 A Vol.J96-A No.11 pp.735-744., Nov. 2013.

[17] 佐藤 雅史，「ブロックチェーンの署名鍵を，誰がどうやって管理するのか」日経 FinTech，2016 年 12 月 12 日，セコム IS 研究所

[18] 角田篤泰，山澤　昌夫，白鳥則郎，「デジタル・アイデンティティの危殆化に抗う『デジタル寺院』構想」，日本セキュリティ・マネジメント学会第 32 回全国大会，2018 年 6 月 16 日

[19] 山澤昌夫, 角田篤泰, 近藤健, 才所敏明, 五太子政史, 佐藤直, 山本博資, 辻井重男, 野田 啓一「セキュリティマネジメントのコンテクスト，より深い理解へのの MELT-UP 活動」–現代の課題と啓蒙–， MELT-UP Activities To Develop Consistent Understanding of Security Management, –Recent Issues and Solutions–，日本セキュリティ・マネジメント学会第 32 回全国大会，2018 年 6 月 16 日