資料3

研究開発に関する今後の検討の素材
～分野・領域に係る議論～

令和2年7月

内閣サイバーセキュリティセンター（NISC）
基本戦略第1グループ

振興に向けた課題

- **いわゆるシステムセキュリティ分野は近年発展しているため、明確な領域の整理が必ずしもあるわけではない。**
- **国内シンポジウムのSCISやCSS、海外のトップカンファレンスでも毎年セッション名が異なる。**
- **振興方策を考えるにあたり、システムセキュリティ分野のある程度のまとまりの領域について、共有の名前を用いて議論した方が良いのではないか。**

領域の整理

- **領域のまとまりをどう整理し議論に資するのが良いか（データ収集は直近5年間のSCISとCSSのセッションより）**

例①	158あるセッションから暗号系を除いた103セッションのうち、回数が多いものを抽出	⇨	12個のセッション（別ファイル例①参照）
例②	158あるセッションのうち、領域の広さやフェーズを意識して整理	⇨	大分類、中分類及びフェーズ単位の小分類に整理（別ファイル例②参照）

重点領域

- **日本の強みやポテンシャルの高い領域はどれか。**
- **日本が今後重点的に強化すべき領域はどれか。**

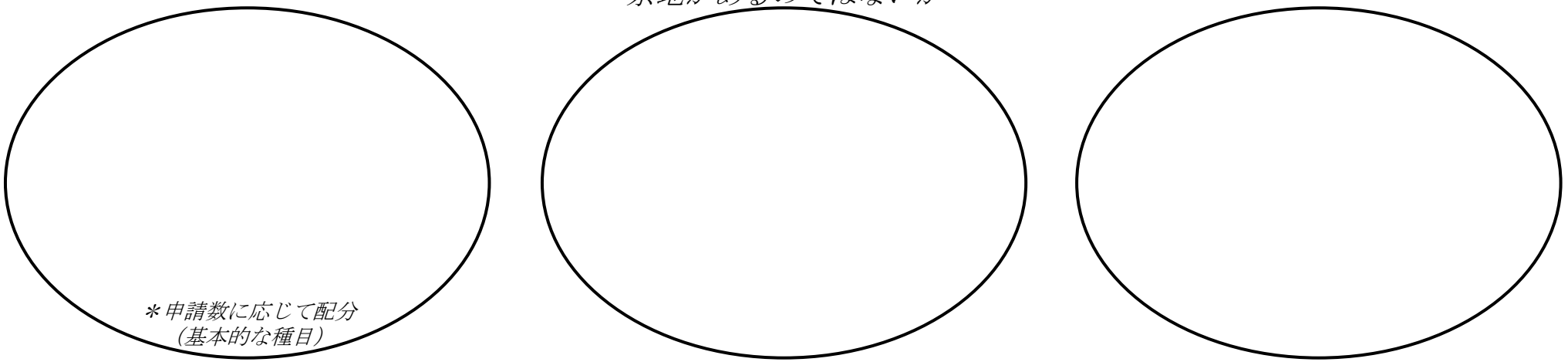
＜参考＞

- 例1: センサ・自動車などの実空間技術とサイバーとの融合領域（Society 5.0）は日本として強みかつ力を入れるため、そのセキュリティ研究が重要なのではないか。
- 例2: ユーザーが多く国民に身近となるような技術のセキュリティ研究がニーズや支持を得ることを踏まえ重要なのではないか。
- 例3: 日本は多くの攻撃を受けており、攻撃観測基盤があるため、攻撃観測をベースにした研究を推進すべきではないか。
- 例4: AI戦略が策定されて日本として力を入れ、かつ技術の普及が進むため、AIセキュリティ研究が重要なのではないか。
- 例5: 過去の経緯から半導体やハードウェアの研究者が多く、知識の蓄積があるため、ハードウェアに係るセキュリティ研究が得意かつ重要なのではないか。
- 例6: サプライチェーンリスクの検証技術など他国に容易に依存できない技術であって国として取り組む一定の合理性がある研究を推進すべきではないか。

SCIS: 電子情報通信学会による暗号と情報セキュリティシンポジウム　CSS: 情報処理学会によるコンピュータセキュリティシンポジウム

（参考）

国のファンディングの獲得について



研究者の自由な発想に基づく研究（学術研究）

ボトムアップ型

研究者が自由に研究課題を提案

JSPS科研費

政策課題対応型研究開発

トップダウン型

国の方針に基づき研究領域等が定められ、その中で研究課題を提案

JST戦略的創造研究推進事業
（CREST/さきがけ等）
産学連携施策や研究拠点施策等
総務省SCOPE

府省が進める研究開発プロジェクト

SIP、総務省、NEDO　等

国のファンディングの獲得について

予算規模例（※予算は令和2年度当初予算額）

項目	予算額
JSPS科研費	2374億円
JST戦略的創造研究推進事業（CREST/さきがけ等）	463億円
JST未来社会創造事業	77億円
JST研究成果展開事業	230億円
JST国際科学技術共同研究推進事業	30億円
総務省SCOPE	21億円

例①: 直近5年間のSCIS及びCSSのセッションから、回数が多いものを抽出

SCIS・CSS抽出（暗号系を除く）	SCIS回数		CSS回数		計		SCIS・CSS抽出（暗号系を除く）	SCIS回数		CSS回数		計	
	5年分	直近2年	5年分	直近2年	5年分	直近2年		5年分	直近2年	5年分	直近2年	5年分	直近2年
AIセキュリティ	1	1	0	0	1	1	スマートデバイスセキュリティ	1	1	0	0	1	1
Androidセキュリティ	1	0	2	1	3	1	脆弱性・脅威分析	1	1	0	0	1	1
DoS攻撃対策	1	0	0	0	1	0	脆弱性解析・対策	1	0	0	0	1	0
FinTechセキュリティ	3	1	0	0	3	1	セキュリティ教育	1	1	0.5	0	1.5	1
IoTセキュリティ	5	2	3	2	8	4	セキュリティ設計・実装	0	0	1	0	1	0
k匿名化	1	0	1	0	2	0	セキュリティ設計・評価	1	0	0	0	1	0
OSセキュリティ	0	0	1	0	1	0	セキュリティ評価・監査	0	0	1	0	1	0
OSSセキュリティ	0	0	1	1	1	1	セキュリティ評価・認証	1	1	0	0	1	1
PUF	2	0	0	0	2	0	セキュリティ評価モデル	3	1	0	0	3	1
Web攻撃解析	0	0	2	0	2	0	セキュリティ分析・調査	1	1	0	0	1	1
Webセキュリティ	5	2	5	2	10	4	ソーシャルエンジニアリング	0	0	0.5	0.5	0.5	0.5
Webトラッキング	0	0	1	0	1	0	ソフトウェア保護・コンテンツ保護	1	0	0	0	1	0
悪性サイト対策	0	0	1	1	1	1	ソフトウェア実装	1	0	0	0	1	0
悪性ドメイン対策	1	0	0	0	1	0	ダークネットとDDoS攻撃	0	0	1	1	1	1
暗号資産	0.5	0.5	0	0	0.5	0.5	敵対的学習	0	0	1	1	1	1
暗号実装	2	1	1	0	3	1	電子現金	1	0	0	0	1	0
暗号通貨	0	0	2	0	2	0	電子透かし	1	0	0	0	1	0
安全性評価	0	0	1	0	1	0	動的解析	0	0	3	1	3	1
アンプ攻撃対策	0	0	1	0	1	0	匿名化	2	2	1	1	3	3
インシデント対応	0	0	1	0	1	0	ドライブ・バイ・ダウンロード	0	0	1	0	1	0
エンドポイント	0	0	1	0	1	0	難読化	0	0	0.5	0.5	0.5	0.5
オンラインバンキング対策	0	0	1	0	1	0	ネットワーク攻撃観測	0.3	0	0.5	0	0.8	0
加工技術	0	0	1	0	1	0	ネットワーク攻撃検知	2.3	0	0	0	2.3	0
仮想化技術	0	0	2	1	2	1	ネットワーク攻撃対策	0.3	0	0	0	0.3	0
機械学習	2	0	2	1	4	1	ネットワーク攻撃分析	0	0	0.5	0	0.5	0
偽造防止技術	0	0	1	1	1	1	ネットワークセキュリティ	4	2	1	1	5	3
脅威分析	0	0	0.5	0	0.5	0	ハードウェア実装	2	1	0	0	2	1
クラウドセキュリティ	2	0	0	0	2	0	ハードウェアセキュリティ	3	2	1	0	4	2
計測・センサーセキュリティ	2	0	0	0	2	0	秘密計算実装	1	1	0	0	1	1
検知回避と誤検知	0	0	1	1	1	1	表層解析とプログラム解析	0	0	1	1	1	1
公開鍵暗号実装	1	1	0	0	1	1	標的型攻撃	0	0	1	0	1	0
公開鍵暗号ソフトウェア実装	1	0	0	0	1	0	標的型メール対策	1	0	0	0	1	0
公開鍵暗号ハードウェア実装	1	0	0	0	1	0	フォーマルメソッド	5	2	0	0	5	2
攻撃検知	0	0	3	1	3	1	フォールト攻撃	1	0	0	0	1	0
攻撃者モデル	0	0	1	0	1	0	フォレンジック	0	0	1	0	1	0
攻撃と防御	0	0	1	0	1	0	不正アクセス検知	0	0	1	1	1	1
攻撃の高度化	0	0	1	0	1	0	不正通信検知	0	0	1	1	1	1
攻撃分析	0	0	1	1	1	1	プライバシー保護	4	1	0	0	4	1
個人情報保護	0	0	0.5	0	0.5	0	プライバシー保護機械学習	1	1	1	0	2	1
サイドチャネル攻撃	4	2	0	0	4	2	プライバシーリスク評価	0	0	2	0	2	0
サイバー攻撃	0	0	1	1	1	1	ブロックチェーン	2.5	1.5	2	2	4.5	3.5
サイバー攻撃観測	1	1	0	0	1	1	マルウェア解析	0	0	1	0	1	0
サイバー攻撃分析・対策	0	0	1	0	1	0	マルウェア検知	0	0	1	1	1	1
サプライチェーンセキュリティ	1	1	0	0	1	1	マルウェア対策	2	2	2	1	4	3
産業制御システムセキュリティ	1	0	0	0	1	0	マルウェア分類	0	0	2	1	2	1
システムセキュリティ	1	0	0	0	1	0	無線のセキュリティ	0	0	1	0	1	0
実装攻撃	1	0	0	0	1	0	メールセキュリティ	0	0	0.5	0	0.5	0
自動車セキュリティ	5	2	3	1	8	3	モバイルセキュリティ	3	0	1	1	4	1
情報ハイディング	0	0	1	0	1	0	リスク・脅威分析	0	0	1	0	1	0
侵入検知	0	0	0.5	0.5	0.5	0.5	リスク管理・評価	0	0	1	1	1	1
心理学	1	0	0	0	1	0	ログ解析	0	0	1	0	1	0
心理学・トラスト	1	1	1	0	2	1							

※計103セッション（暗号系55セッションを除く）

各条件を満足するセッションを抽出した結果が以下のとおり。

5年分のうち、双方あってそれぞれ3回以上
IoTセキュリティ
Webセキュリティ

5年分のうち、双方あってそれぞれ2回以上
機械学習
ブロックチェーン
マルウェア対策

5年分のうち、いずれか4回以上
サイドチャネル攻撃
自動車セキュリティ
ネットワークセキュリティ
フォーマルメソッド
プライバシー保護

直近2年分のうち、いずれか2年連続
匿名化
ハードウェアセキュリティ

計12セッション

例②: 直近5年間のSCIS及びCSSのセッションから、領域の広さやフェーズを意識して整理

SCIS・CSS抽出後	対応
AIセキュリティ	
Androidセキュリティ	領域としてとらえるには狭すぎるため除く
DoS攻撃対策	
FinTechセキュリティ	
ID管理	
IDベース暗号	暗号系かつ純理論系のため除く
IoTセキュリティ	
k匿名化	領域としてとらえるには狭すぎるため除く
MAC	暗号系かつ純理論系のため除く
OSセキュリティ	
OSSセキュリティ	領域としてとらえるには狭すぎるため除く
PKI	
PUF	領域としてとらえるには狭すぎるため除く
Web攻撃解析	名称微修正
Webセキュリティ	
Webトラッキング	領域としてとらえるには狭すぎるため除く
悪性サイト対策	
悪性ドメイン対策	
暗号応用	暗号系かつ純理論系のため除く
暗号解析	暗号系かつ純理論系のため除く
暗号資産	領域としてとらえるには狭すぎるため除く
暗号実装	
オンラインバンキング対策	領域としてとらえるには狭すぎるため除く
暗号プロトコル	暗号系かつ純理論系のため除く
暗号理論	暗号系かつ純理論系のため除く
安全性評価	領域としてとらえるには広すぎるため除く
アンプ攻撃対策	領域としてとらえるには狭すぎるため除く
インシデント対応	領域としてとらえるには広すぎるため除く
エンドポイント	領域としてとらえるには広すぎるため除く
オンラインバンキング対策	名称微修正
カードプロトコル	暗号系かつ純理論系のため除く
カードベース暗号	暗号系かつ純理論系のため除く
加工技術	
仮想化技術	領域としてとらえるには広すぎるため除く
関数暗号	暗号系かつ純理論系のため除く
機械学習	領域としてとらえるには狭すぎるため除く
偽造防止技術	領域としてとらえるには広すぎるため除く
脅威分析	
共通鍵暗号	暗号系かつ純理論系のため除く
クラウドセキュリティ	
グループ署名	暗号系かつ純理論系のため除く
計測・センサーセキュリティ	2項目に整理
ゲーム理論	暗号系かつ純理論系のため除く
検索可能暗号	暗号系かつ純理論系のため除く
検知回避と誤検知	領域としてとらえるには広すぎるため除く
公開鍵暗号	暗号系かつ純理論系のため除く
公開鍵暗号実装	領域としてとらえるには狭すぎるため除く
公開鍵暗号ソフトウェア実装	領域としてとらえるには狭すぎるため除く
公開鍵暗号ハードウェア実装	領域としてとらえるには狭すぎるため除く
高機能暗号	暗号系かつ純理論系のため除く
攻撃検知	領域としてとらえるには広すぎるため除く
攻撃者モデル	暗号系かつ純理論系のため除く
攻撃と防御	領域としてとらえるには広すぎるため除く

SCIS・CSS抽出後	対応
攻撃の高度化	領域としてとらえるには広すぎるため除く
攻撃分析	領域としてとらえるには広すぎるため除く
格子暗号	暗号系かつ純理論系のため除く
格子問題	暗号系かつ純理論系のため除く
行動認証	領域としてとらえるには狭すぎるため除く
個人情報保護	
個人認証	
サイドチャネル攻撃	領域としてとらえるには狭すぎるため除く
サイバー攻撃	領域としてとらえるには広すぎるため除く
サイバー攻撃観測	領域としてとらえるには広すぎるため除く
サイバー攻撃分析・対策	領域としてとらえるには広すぎるため除く
サインクリプション	暗号系かつ純理論系のため除く
サプライチェーンセキュリティ	
産業制御システムセキュリティ	
システムセキュリティ	領域としてとらえるには広すぎるため除く
実装攻撃	名称微修正
自動車セキュリティ	
準同型暗号	暗号系かつ純理論系のため除く
情報ハイディング	
情報理論的安全性	暗号系かつ純理論系のため除く
署名	暗号系かつ純理論系のため除く
人工物メトリクス	
侵入検知	領域としてとらえるには狭すぎるため除く
心理学	領域としてとらえるには広すぎるため除く
心理学・トラスト	領域としてとらえるには広すぎるため除く
数論・計算問題	暗号系かつ純理論系のため除く
数論アルゴリズム	暗号系かつ純理論系のため除く
数論応用	暗号系かつ純理論系のため除く
ストリーム暗号	暗号系かつ純理論系のため除く
スマートデバイスセキュリティ	領域としてとらえるには狭すぎるため除く
脆弱性・脅威分析	重複のため一部を整理
脆弱性解析・対策	重複のため一部を整理
生体認証	領域としてとらえるには狭すぎるため除く
セキュリティ教育	領域としてとらえるには広すぎるため除く
セキュリティ設計・実装	2項目に整理
セキュリティ設計・評価	重複のため一部を整理
セキュリティ評価・監査	領域としてとらえるには広すぎるため除く
セキュリティ評価・認証	領域としてとらえるには広すぎるため除く
セキュリティ評価モデル	領域としてとらえるには広すぎるため除く
セキュリティ分析・調査	2項目に整理
素因数分解・離散対数問題	暗号系かつ純理論系のため除く
ソーシャルエンジニアリング	領域としてとらえるには狭すぎるため除く
ソフトウェア保護・コンテンツ保護	2項目に整理し名称微修正
ソフトウェア実装	領域としてとらえるには広すぎるため除く
ダークネットとDDoS攻撃	領域としてとらえるには狭すぎるため除く
代理人再暗号化	暗号系かつ純理論系のため除く
耐量子暗号	暗号系かつ純理論系のため除く
楕円曲線暗号	暗号系かつ純理論系のため除く
多機能署名	暗号系かつ純理論系のため除く
多変数暗号	暗号系かつ純理論系のため除く
多変数公開鍵暗号	暗号系かつ純理論系のため除く
超楕円曲線暗号	暗号系かつ純理論系のため除く
敵対的学習	領域としてとらえるには狭すぎるため除く

SCIS・CSS抽出後	対応
電子現金	領域としてとらえるには広すぎるため除く
電子透かし	領域としてとらえるには狭すぎるため除く
同種写像暗号	暗号系かつ純理論系のため除く
動的解析	
匿名化	領域としてとらえるには狭すぎるため除く
ドライブ・バイ・ダウンロード	領域としてとらえるには狭すぎるため除く
難読化	
認証	
ネットワーク攻撃観測	重複のため除く
ネットワーク攻撃検知	
ネットワーク攻撃対策	
ネットワーク攻撃分析	
ネットワークセキュリティ	
ハードウェア実装	領域としてとらえるには広すぎるため除く
ハードウェアセキュリティ	
バイオメトリクス	重複のため除く
ハッシュ関数	暗号系かつ純理論系のため除く
秘匿計算	暗号系かつ純理論系のため除く
秘密計算	暗号系かつ純理論系のため除く
秘密計算実装	領域としてとらえるには狭すぎるため除く
秘密分散	暗号系かつ純理論系のため除く
表層解析とプログラム解析	2項目に整理
標的型攻撃	領域としてとらえるには狭すぎるため除く
標的型メール対策	領域としてとらえるには狭すぎるため除く
フォーマルメソッド	領域としてとらえるには狭すぎるため除く
フォールト攻撃	領域としてとらえるには狭すぎるため除く
フォレンジック	領域としてとらえるには広すぎるため除く
不正アクセス検知	
不正通信検知	
物理・視覚化暗号	暗号系かつ純理論系のため除く
物理的暗号	暗号系かつ純理論系のため除く
プライバシー保護	
プライバシー保護機械学習	領域としてとらえるには広すぎるため除く
プライバシーリスク評価	領域としてとらえるには広すぎるため除く
ブロック暗号	暗号系かつ純理論系のため除く
ブロックチェーン	領域としてとらえるには狭すぎるため除く
ペアリング	暗号系かつ純理論系のため除く
放送暗号	暗号系かつ純理論系のため除く
マルウェア解析	名称微修正
マルウェア検知	
マルウェア対策	
マルウェア分類	重複のため除く
マルチパーティ計算	暗号系かつ純理論系のため除く
無線のセキュリティ	名称微修正
メールセキュリティ	
モバイルセキュリティ	
ユーザ認証	
乱数	暗号系かつ純理論系のため除く
リスク・脅威分析	重複のため一部を整理
リスク管理・評価	2項目に整理
量子暗号・量子計算	暗号系かつ純理論系のため除く
ログ解析	領域としてとらえるには広すぎるため除く

計158セッション
赤字は整理後に残したセッション
青字は特殊例

各セッションに対し、対応欄により整理した結果が以下のとおり。

整理後
AIセキュリティ
DoS攻撃対策
FinTechセキュリティ
ID管理
IoTセキュリティ
OSセキュリティ
PKI
Web攻撃分析※
Webセキュリティ
悪性サイト対策
悪性ドメイン対策
暗号実装
暗号実装攻撃※
オンラインバンキングセキュリティ※
加工技術
脅威分析
クラウドセキュリティ
計測セキュリティ
個人情報保護
個人認証
コンテンツ保護
サプライチェーンセキュリティ
産業制御システムセキュリティ
自動車セキュリティ
情報ハイディング
人工物メトリクス
脆弱性分析
脆弱性対策
セキュリティ実装
セキュリティ設計
セキュリティ調査
セキュリティ評価
セキュリティ分析
センサーセキュリティ
ソフトウェアセキュリティ※
動的解析
難読化
認証
ネットワーク攻撃検知
ネットワーク攻撃対策
ネットワーク攻撃分析
ネットワークセキュリティ
ハードウェアセキュリティ
表層解析
不正アクセス検知
不正通信検知
プライバシー保護
プログラム解析
マルウェア分析※
マルウェア検知
マルウェア対策
無線セキュリティ※
メールセキュリティ
モバイルセキュリティ
ユーザ認証
リスク分析
リスク管理
リスク評価

計58セッション
※名称微修正したもの

例②: 直近5年間のSCIS及びCSSのセッションから、領域の広さやフェーズを意識して整理

前ページで整理した58セッションを大項目、中項目、4つのフェーズ単位の小項目に割り当て、空白部を補足して作成した表が以下のとおり。

大分類(セキュリティ大項目)	中分類(セキュリティ中項目)	小分類(フェーズ単位)			
		攻撃(不備)	検知(観測)	分析(解析)	対策
ネットワークセキュリティ (28項目)	通信系ネットワークセキュリティ (8項目)	ネットワーク攻撃	ネットワーク攻撃検知	ネットワーク攻撃分析	ネットワーク攻撃対策
		不正通信	不正通信検知	不正通信分析	不正通信対策
	アクセス系ネットワークセキュリティ (12項目)	不正アクセス	不正アクセス検知	不正アクセス分析	不正アクセス対策
		DoS攻撃	DoS攻撃検知	DoS攻撃分析	DoS攻撃対策
		悪性ドメイン構築	悪性ドメイン検知	悪性ドメイン分析	悪性ドメイン対策
	認証 (8項目)	なりすまし攻撃	なりすまし攻撃検知	なりすまし攻撃分析	ID管理 個人認証 ユーザ認証 人工物メトリクス PKI
コンピュータセキュリティ (19項目)	Webセキュリティ (8項目)	Web攻撃	Web攻撃検知	Web攻撃分析	Web攻撃対策
		悪性サイト構築	悪性サイト検知	悪性サイト分析	悪性サイト対策
	プログラム保護 (11項目)	マルウェア	マルウェア検知	マルウェア分析	マルウェア対策
		不正機能埋込	不正機能埋込検知	動的解析 表層解析 プログラム解析 静的解析	難読化
実装セキュリティ (16項目)	暗号実装(4項目)	暗号実装攻撃	暗号実装攻撃検知	暗号実装攻撃分析	暗号実装攻撃対策
	ハードウェアセキュリティ(4項目)	ハードウェア実装攻撃	ハードウェア実装攻撃検知	ハードウェア実装攻撃分析	ハードウェア実装攻撃対策
	OSセキュリティ(4項目)	OS実装攻撃	OS実装攻撃検知	OS実装攻撃分析	OS実装攻撃対策
	ソフトウェアセキュリティ(4項目)	ソフトウェア実装攻撃	ソフトウェア実装攻撃検知	ソフトウェア実装攻撃分析	ソフトウェア実装攻撃対策
評価全般 (20項目)	セキュリティ評価 (8項目)	セキュリティ実装不備 セキュリティ設計不備 セキュリティ対策不備	セキュリティ調査	セキュリティ分析	セキュリティ実装 セキュリティ設計 セキュリティ対策
	リスク評価 (12項目)	脆弱性 リスク 脅威	脆弱性検知 リスク検知 脅威検知	脆弱性分析 リスク分析 脅威分析	脆弱性対策 リスク管理 脅威対策
データセキュリティ (12項目)	プライバシー保護(4項目)	プライバシー情報漏洩	プライバシー情報漏洩検知	プライバシー情報漏洩分析	加工技術
	個人情報保護(4項目)	個人情報漏洩	個人情報漏洩検知	個人情報漏洩分析	個人情報漏洩対策
	コンテンツ保護(4項目)	コンテンツ不正流通	コンテンツ不正流通検知	コンテンツ不正流通分析	情報ハイディング
アプリケーションセキュリティ またはサービスセキュリティ (13項目)	AIセキュリティ FinTechセキュリティ IoTセキュリティ オンラインバンキングセキュリティ クラウドセキュリティ 計測セキュリティ サプライチェーンセキュリティ 産業制御システムセキュリティ 自動車セキュリティ センサーセキュリティ 無線セキュリティ メールセキュリティ モバイルセキュリティ	アプリケーションセキュリティは小分類(フェーズ単位)まで細かく分けられていないと思われるため、中分類までの13項目を対象とする。			

計6大分類　　計27中分類　　計95小分類

赤字は整理後に残したセッション

注1: 最先端の研究や海外での研究でSCISやCSSのセッション名にすぐには現れてこない領域がありうる。
注2: 学会には現れてこない、あるいは研究は行われていても論文として発表がなされない領域がありうる。