資料2-3

分野・領域に係る検討の素材
～分野・領域に係るマッピング例～

令和2年8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

重点的に強化すべき領域例を試みにマッピングするとどうなるか

【専門調査会資料（検討の素材）に掲載されていた領域の整理例②】

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

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	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。			
	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				

計6大分類　　計27中分類　　計95小分類

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。

重点的に強化すべき領域例を試みにマッピングするとどうなるか

【専門調査会資料（検討の素材）に掲載されていた参考例】

※Snは事務局にて便宜的に付記（n: 数字）

- 例1: センサー・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整理での記載: センサーセキュリティ（S1）／IoTセキュリティ（S2）／自動車セキュリティ（S3）
- 例2: ユーザ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②整理での記載: モバイルセキュリティ（S4）
- 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②整理での記載: ネットワーク攻撃検知（S5）
- 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②整理での記載: AIセキュリティ（S6）
- 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②整理での記載: ハードウェアセキュリティ（S7）
- 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。
  - ✓ 例②整理での記載: サプライチェーンセキュリティ（S8）

重点的に強化すべき領域例を試みにマッピングするとどうなるか

【WG第2回会合での委員説明資料】

※Anは事務局にて便宜的に付記（n: 数字）

- **今後社会基盤を支えるであろうICT要素技術のセキュリティ的側面**
  - ✓ AIセキュリティ: AIの信頼性が揺らぐと、活用する社会基盤そのものへの影響大。
    → 例②整理での記載: AIセキュリティ（A1）
  - ✓ 非PC（IoT/OT/CPS等）のセキュリティ: Windows等のPCの解析技術が重要だったのと同様に、モバイルデバイス・IoT/OT/CPSの解析技術はサイバー攻撃対策として必須。
  - → 例②整理での記載: センサセキュリティ（A2）／IoTセキュリティ（A3）／自動車セキュリティ（A4）
- **産業活動を活性化できるセキュリティ技術**
  - ✓ データセキュリティ: データは産業活動の源泉。データの保存・交換・処理の安全を確保することでデータ利活用が促進される。
    → 例②整理での記載: データセキュリティ（A5）
  - ✓ ユーザブルセキュリティ: 人に着目したセキュリティ。セキュリティを担保しつつユーザビリティを向上させる技術はユーザのオンライン活動の活性化に直結。例: FIDO2などのパスワードレス技術等。
    → 例②整理での記載: ユーザブルセキュリティ（モバイルセキュリティ含む）（A6）
- **実データ（臨床データ）の観測・分析と研究へのフィードバック**
  - ✓ 実データの観測に基づいたセキュリティ研究: データドリブンアプローチでの研究（医学でいうところの臨床実験・研究）。ネットワーク・システム・サービスの運用時のデータを活用。対策手法の評価検証だけでなく、実態調査に基づいて最新の攻撃情報を把握し、新たな対策技術の研究に活用する、など。
    → 例②整理での記載: 検知（観測）に基づく研究（A7）
- **未知の脅威を発見する方法の研究（攻撃研究）**
  - ✓ オフェンシブセキュリティ: 攻撃者の視点に立って未知の脅威を発見、攻撃に悪用される前に対策。水際対策・事後対策から脱却し、事前対策（設計から作り直す、シフトレフト化）によって、根本からの問題解決を目指すもの。対象は低～高レイヤまで対象は広い。日本からのTop-4採択論文の多くが攻撃研究（CCS '14, S&P '19, NDSS '20）。
    → 例②整理での記載: 攻撃研究（A8）

重点的に強化すべき領域例を試みにマッピングするとどうなるか
（例②整理への落とし込み）

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

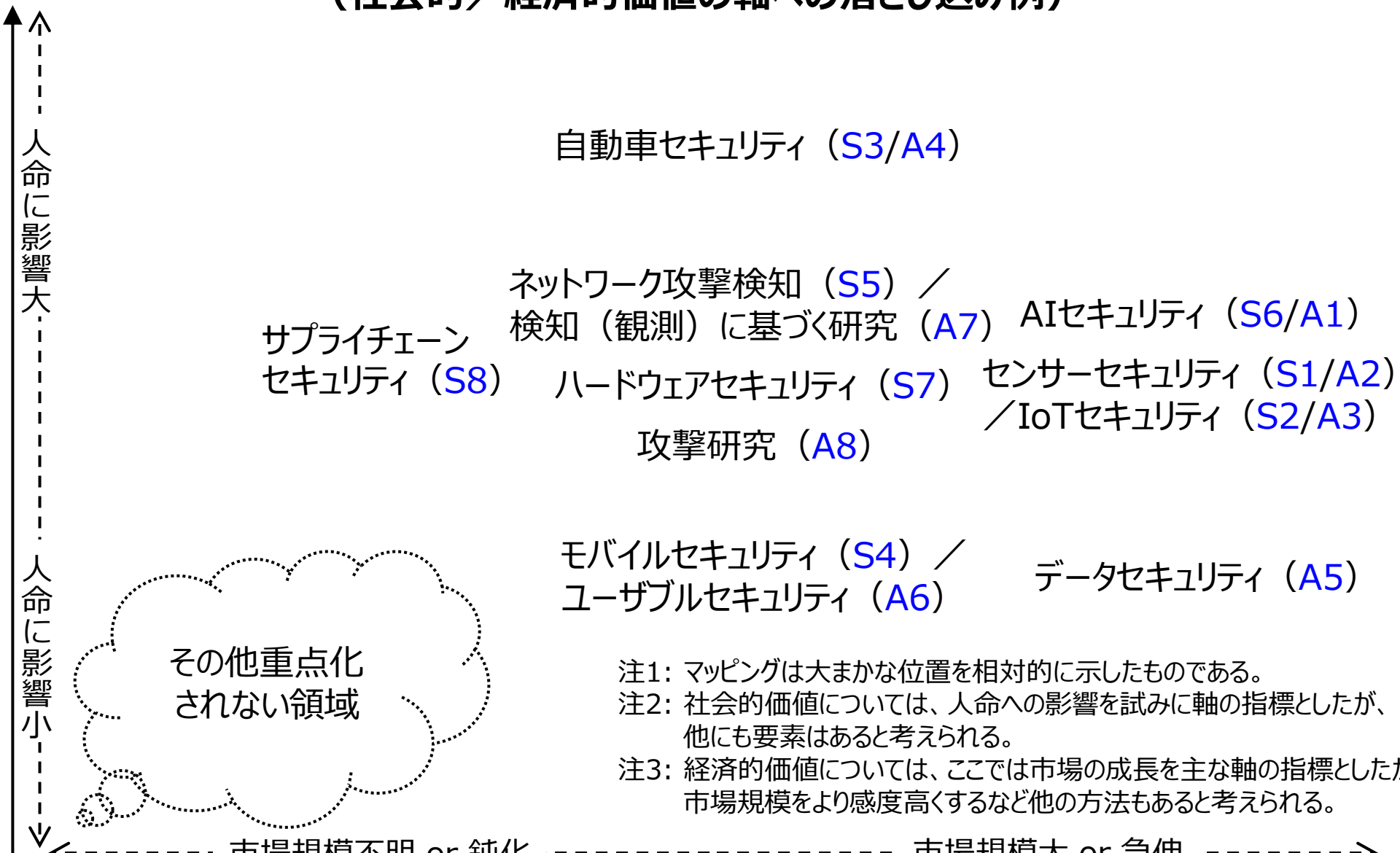
整理した58セッションを大項目、中項目、4つのフェーズ単位の小項目に割り当て、空白部を補足して作成した表が以下のとおり。

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	↑ 攻撃者の視点に立って未知の脅威を発見する方法の研究（攻撃研究）	↑ 検知（観測）に基づく研究		
	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	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。			
	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				
	ユーザブルセキュリティ（モバイルセキュリティ含む）※	※表記変更している。			

計6大分類　　計27中分類　　計95小分類

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。

重点的に強化すべき領域例を試みにマッピングするとどうなるか
（社会的／経済的価値の軸への落とし込み例）

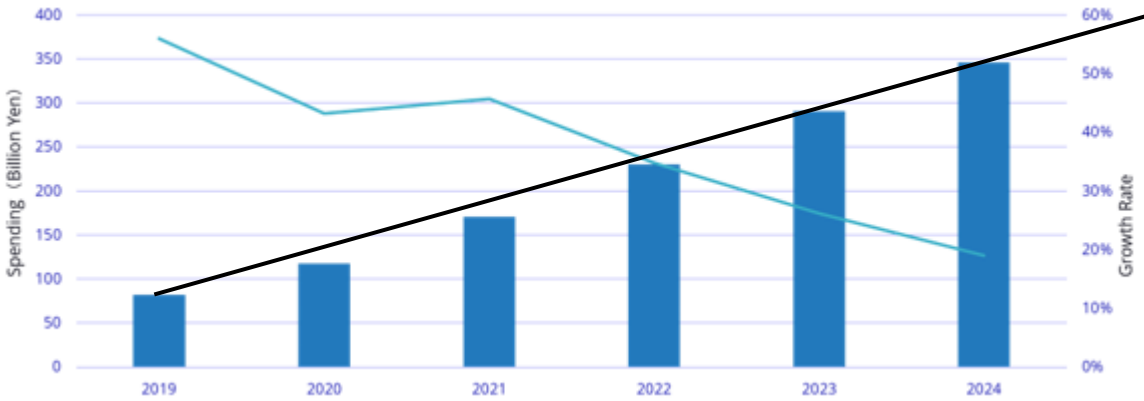


注1: マッピングは大まかな位置を相対的に示したものである。
注2: 社会的価値については、人命への影響を試みに軸の指標としたが、
他にも要素はあると考えられる。
注3: 経済的価値については、ここでは市場の成長を主な軸の指標としたが、
市場規模をより感度高くするなど他の方法もあると考えられる。

（参考1）

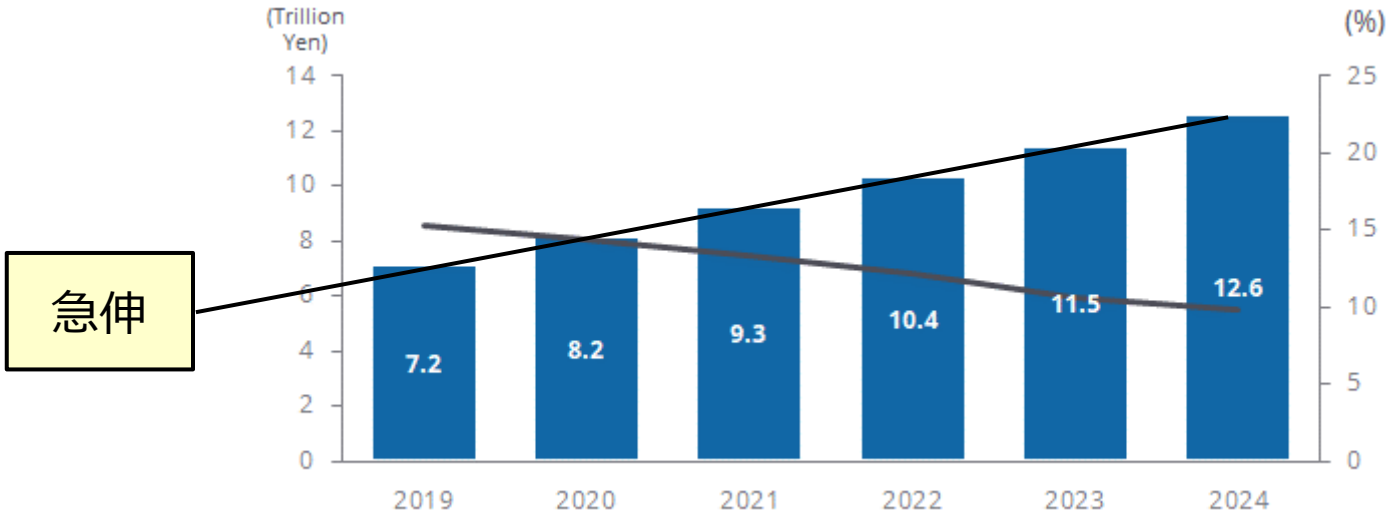
経済的価値参考情報

国内AIシステム市場支出額予測（2019年～2024年）



（出展）IDC Japan 2020年6月1日発表（https://www.idc.com/getdoc.jsp?containerId=prJPJ46395520）

国内IoT市場支出額（2019年～2024年）



（出展）IDC Japan 2020年4月15日発表（https://www.idc.com/getdoc.jsp?containerId=prJPJ46213220）

経済的価値参考情報

顧客情報漏洩・流出事件の実例と賠償金額

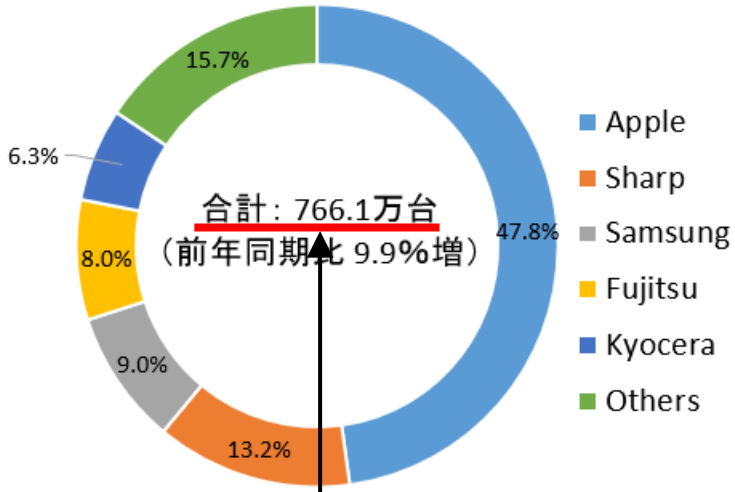
時期	漏洩事業者・情報	規模	金額相場
平成10年	早稲田大学（講演参加者名簿を警察に提供）	1400件	5000円
平成11年	宇治市（住民基本台帳データ）	約22万人	1万円
平成14年5月	TBCグループ	3万7000人	3万円／1万7000円
平成14年6月	ローソン	56万人	500円
平成14年8月	アプラス	7万9000人	1000円相当
平成14年11月	ファミリーマート	18万3000人	1000円相当
平成14年12月	東武鉄道	13万2000人	5000円相当
平成15年6月	ローソンカード会員情報	会員約115万人	5000円の商品券
平成15年11月	ファミマ・クラブ会員情報	会員約18万人	1000円のクオ・カード
平成16年1月	ヤフーBB会員情報	451万7000人	500円の金券
平成16年3月	サントリー	7万5000人	500円
平成16年5月	ツノダ	1万6000人	500円相当
平成16年6月	コスモ石油	92万3000人	50マイル分
平成16年7月	DCカード	47万8000人	500円
平成17年1月	オリエンタルランド	12万2000人	500円
平成19年3月	大日本印刷	864万人	500円
平成20年4月	サウンドハウス	12万3000人	1000円相当
平成20年6月	アイリスプラザ	2万8000人	1000円相当
平成21年5月	三菱UFJ証券顧客情報	4万9000人	1万円の商品券
平成21年8月	アリコジャパン	1万8000人	1万円／3000円
平成21年8月	アミューズ	14万9000人	500円相当
平成25年4月	JIN	1万2000人	1000円相当
平成26年7月	ベネッセ顧客情報	2895万人	500円分の電子マネー or 図書カード or 寄付
平成26年9月	ドコモ顧客情報	法人1社・個人1053人	（未定）
平成26年9月	日本航空（JAL）	最大75万件	（未定）

負担額:
約145億円

（出展）弁護士法人みずほ中央法律事務所ホームページ（2020年8月11日閲覧（https://www.mc-law.jp/kigyohomu/9055/）

経済的価値参考情報

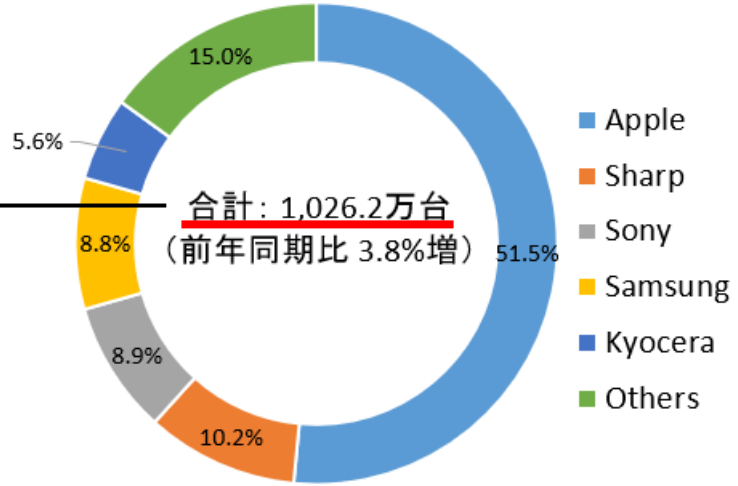
2020年第1四半期 国内市場スマートフォン出荷台数・ベンダー別 シェア



（出展）IDC Japan 2020年5月28日発表（https://www.idc.com/getdoc.jsp?containerId=prJPJ46395420）

減少

2019年第4四半期 国内スマートフォン出荷台数 ベンダー別 シェア



（出展）IDC Japan 2020年3月10日発表（https://www.idc.com/getdoc.jsp?containerId=prJPJ46116220）

経済的価値参考情報

セキュリティインシデントに起因した年間平均被害総額

1.　約4割が重大被害を経験、年間平均被害額は4年連続2億円超え

国内法人組織の36.3%が2018年4月～2019年3月の1年間にセキュリティインシデントに起因した重大被害を経験したことが明らかになりました。昨年調査の42.3%から改善は見られたものの、未だ約4割で情報漏えいやデータの破壊などの重大被害が発生しています。原因究明のための調査費用、改善策の導入、損害賠償といった事後対応を含めた年間平均被害総額は約2.4億円となり、4年連続で2億円を超える結果となりました。

（出展）トレンドマイクロ 2019年10月15日発表（https://www.trendmicro.com/ja_jp/about/press-release/2019/pr-20191015-01.html）

登録車合計

西暦	1月	前年比	2月	前年比	3月	前年比	4～3月	前年比
2020	221,464	88.9	268,302	89.3	374,955	89.8	3,182,760	95.4
2019	249,048	102.3	300,410	101.3	417,373	95.3	3,336,590	100.0
2018	243,435	94.3	296,665	95.1	438,084	95.1	3,338,234	99.4
2017	258,085	108.6	312,035	113.4	460,654	113.8	3,357,933	107.5
2016	237,661	100.2	275,165	95.4	404,813	96.8	3,124,406	100.0

横ばい

（出展）一般社団法人日本自動車販売協会連合会 2020年8月12日閲覧（http://www.jada.or.jp/data/year/y-r-hanbai/y-r-all/）

（参考2）

DARPAの研究プログラムを試みにマッピングするとどうなるか

※番号は事務局にて便宜的に付記

No.	研究プログラム	例②整理での記載
①	Cyber-Hunting at Scale (CHASE)	ネットワーク攻撃検知
②	Harnessing Autonomy for Countering Cyber-adversary Systems (HACCS)	DoS攻撃対策
③	Rapid Attack Detection, Isolation and Characterization Systems (RADICS)	産業制御システムセキュリティ
④	Enhanced Attribution	ネットワーク攻撃対策
⑤	Dispersed Computing	セキュリティ設計
⑥	Computers and Humans Exploring Software Security (CHESS)	脆弱性検知
⑦	Configuration Security	脆弱性対策
⑧	Cyber Assured Systems Engineering (CASE)	セキュリティ対策
⑨	Active Social Engineering Defense (ASED)	悪性サイト対策
⑩	Leveraging the Analog Domain for Security (LADS)	ハードウェアセキュリティ
⑪	Brandeis	プライバシー保護
⑫	Extreme Distributed Denial of Service Defense (XD3)	DoS攻撃対策
⑬	Memory Optimization (MemOp)	セキュリティ実装
⑭	Resilient Anonymous Communication for Everyone (RACE)	モバイルセキュリティ
⑮	Cora	不正アクセス対策
⑯	Searchlight	セキュリティ設計
⑰	Cyber Fault-tolerant Attack Recovery (CFAR)	セキュリティ対策
⑱	Edge-Directed Cyber Technologies for Reliable Mission Communication (EdgeCT)	ネットワーク攻撃対策
⑲	System Security Integrated Through Hardware and firmware (SSITH)	ハードウェアセキュリティ
⑳	Supply Chain Hardware Integrity for Electronics Defense (SHIELD)	サプライチェーンセキュリティ
㉑	Plan X	ネットワーク攻撃対策

注: 研究プログラムはJST/CRDS説明資料（資料1-3）にあるものを使用。

IARPAの研究プログラムを試みにマッピングするとどうなるか

※番号は事務局にて便宜的に付記

Current Research

No.	研究プログラム	例②整理での記載
①	Homomorphic Encryption Computing Techniques with Overhead Reduction (HECTOR)	ソフトウェアセキュリティ
②	Securing Compartmented Information with Smart Radio Systems (SCISRS)	無線セキュリティ
③	Trojans in Artificial Intelligence (TrojAI)	AIセキュリティ

Past Research

No.	研究プログラム	例②整理での記載
④	ATHENA	ネットワーク攻撃検知
⑤	Circuit Analysis Tools (CAT)	ハードウェアセキュリティ
⑥	Cyber-attack Automated Unconventional Sensor Environment (CAUSE)	ネットワーク攻撃検知
⑦	Security and Privacy Assurance Research (SPAR)	プライバシー保護
⑧	Securely Taking On New Executable Software of Uncertain Provenance (STONESOUP)	ソフトウェアセキュリティ
⑨	Trusted Integrated Chips (TIC)	ハードウェアセキュリティ

注: 研究プログラムはJST/CRDS説明資料（資料1-3）にあるものを使用。

DARPA/IARPAの研究プログラムを試みにマッピングするとどうなるか（例②整理への落とし込み）

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

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①④⑥	ネットワーク攻撃分析	ネットワーク攻撃対策④⑩㉑
		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⑮
		DoS攻撃	DoS攻撃検知	DoS攻撃分析	DoS攻撃対策②⑫
		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⑨
	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）⑩⑲⑤⑨	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）①⑧	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⑬ セキュリティ設計⑤⑯ セキュリティ対策⑧⑰
	リスク評価（12項目）	脆弱性 リスク 脅威	脆弱性検知⑥ 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⑦ 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）⑪⑦	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③	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。			
	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⑳				
	産業制御システムセキュリティ③				
	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②				
	メールセキュリティ				
	モバイルセキュリティ⑭				

計6大分類　　計27中分類　　計95小分類

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。

注: 研究プログラムはJST/CRDS説明資料（資料1-3）にあるものを使用。