一般社団法人ディペンダビリティ技術推進協会

OSD部会　各部会紹介

技術活用部会の活動

2021年6月21日

技術活用部会

中川　雅通

活動

- ミッション

  協会が保有する技術の産業・社会への活用

- 活動

  OSDが活用できる・必要とされると考える分野に対して、具体的な提案活動

  ギャップ分析、OSD視点からの追加案

適用分野

条件

- 開発だけでなく、継続的な信頼性確保の取組みが必要な分野
- 複数のステークフォルダーが存在して、合意形成、説明責任が重要になると思われる分野

取組み分野

- つながる世界のセキュリティ（IPA）
- 医療情報ガイドライン（経産省）
- 機械学習品質マネジメントガイドライン　取組み中

1.つながる世界の開発指針

■IPA（情報処理推進機構）が発行

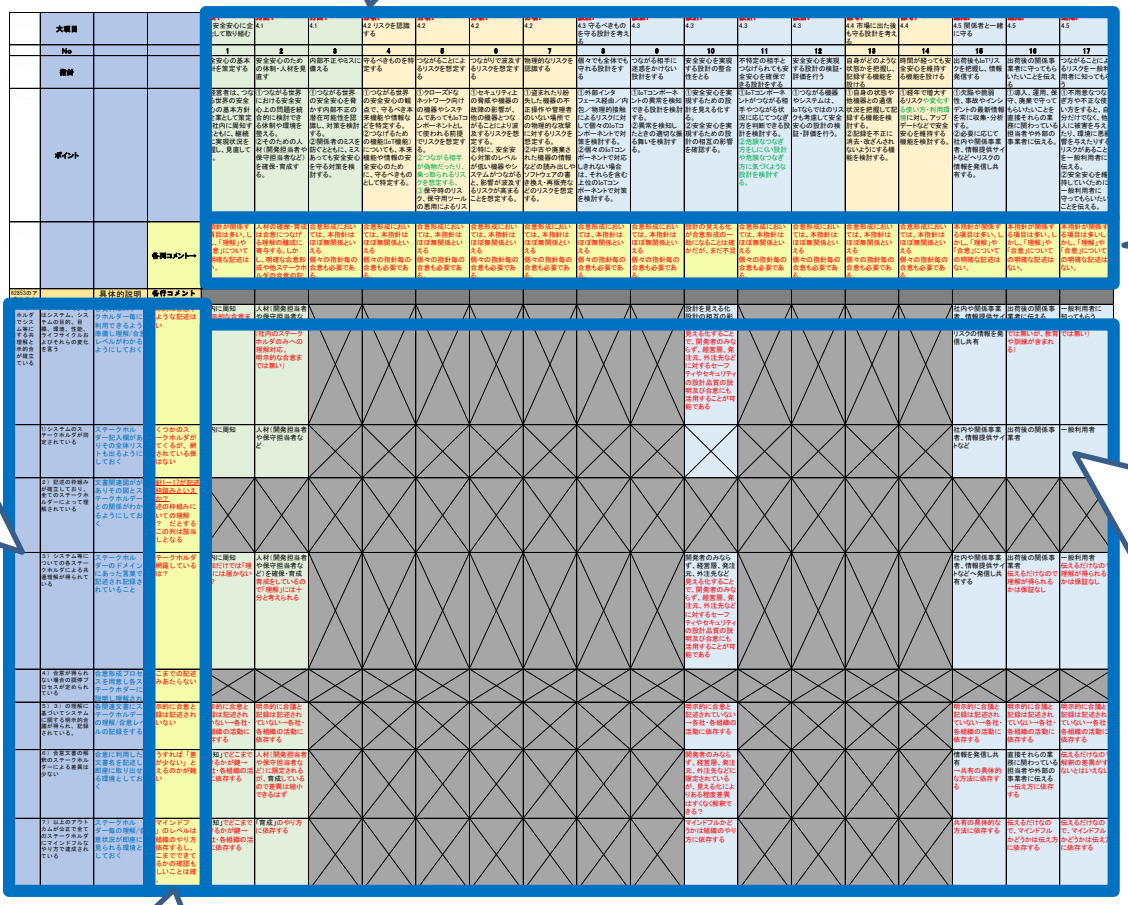
IoTの進展にともない、様々なモノがつながって新たな価値を創出していく『つながる世界』ならではの機器やシステムに関わる企業が安全安心に関して最低限考慮すべき事項を記載

つながる世界の17の指針

	大項目	指針	
方針	4.1 つながる世界の安全安心に企業として取り組む	指針1	安全安心の基本方針を策定する
		指針2	安全安心のための体制・人材を見直す
		指針3	内部不正やミスに備える
分析	4.2 つながる世界のリスクを認識する	指針4	守るべきものを特定する
		指針5	つながることによるリスクを想定する
		指針6	つながりで波及するリスクを想定する
		指針7	物理的なリスクを認識する
設計	4.3 守るべきものを守る設計を考える	指針8	個々でも全体でも守れる設計をする
		指針9	つながる相手に迷惑をかけない設計をする
		指針10	安全安心を実現する設計の整合性をとる
		指針11	不特定の相手とつなげられても安全安心を確保できる設計をする
		指針12	安全安心を実現する設計の検証・評価を行う
保守	4.4 市場に出た後も守る設計を考える	指針13	自身がどのような状態かを把握し、記録する機能を設ける
		指針14	時間が経っても安全安心を維持する機能を設ける
運用	4.5 関係者と一緒に守る	指針15	出荷後もIoTリスクを把握し、情報発信する
		指針16	出荷後の関係事業者に守ってもらいたいことを伝える

2つの文書の項目毎に比較

つながる世界の
17の開発指針



マッピング結果の
各指針毎のコメント

IEC62853の1つの
viewにおける
outcome

注: 4つのview毎に表
が作られている
1. 合意形成
2. 変化対応
3. 障害対応
4. 説明責任

つながる世界の開発指針
の1項目とIEC62853の
outcomeの1項目毎の
マッピング結果

黒字: 62853のoutcomeの
記述に対応する開発指針
の記述部分
赤字: コメント
×印: 無関係、対応せず
グレー : 列もしくは行全て
が×印

マッピング結果
の各outcome毎
のコメント

合意形成との比較

方針: 4.1 安全安心に企業として取り組む	方針: 4.1	方針: 4.1	分析: 4.2 リスクを認識する	分析: 4.2	分析: 4.2	分析: 4.2	設計: 4.3 守るべきものを守る設計を考える	設計: 4.3	設計: 4.3	設計: 4.3	設計: 4.3	保守: 4.4 市場に出た後も守る設計を考える	保守: 4.4	運用: 4.5 関係者と一緒に守る	運用: 4.5	運用: 4.5
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
安全安心の基本方針を策定する	安全安心のための体制・人材を見直す	内部不正やミスに備える	守るべきものを特定する	つながることによるリスクを想定する	つながりで波及するリスクを想定する	物理的なリスクを認識する	個々でも全体でも守れる設計をする	つながる相手に迷惑をかけない設計をする	安全安心を実現する設計の整合性をとる	不特定の相手とつなげられても安全安心を確保できる設計をする	安全安心を実現する設計の検証・評価を行う	自身がどのような状態かを把握し、記録する機能を設ける	時間が経っても安全安心を維持する機能を設ける	出荷後もIoTリスクを把握し、情報発信する	出荷後の関係事業者に守ってもらいたいことを伝える	つながることによるリスクを一般利用者に知ってもらう
①経営者は、つながる世界の安全安心の基本方針を企業として策定し、社内に周知するとともに、継続的に実現状況を把握し、見直していく。	①つながる世界における安全安心上の問題を統合的に検討できる体制や環境を整える。 ②そのための人材（開発担当者や保守担当者など）を確保・育成する。	①つながる世界の安全安心を脅かす内部不正の潜在可能性を認識し、対策を検討する。 ②関係者のミスを防ぐとともに、ミスあっても安全安心を守る対策を検討する。	①つながる世界の安全安心の観点で、守るべき本来機能や情報などを特定する。 ②つなげるための機能(IoT機能)についても、本来機能や情報の安全安心のために、守るべきものとして特定する。	①クローズドなネットワーク向けの機器やシステムであってもIoTコンポーネントとして使われる前提でリスクを想定する。 ②つながる相手が偽物だったり、乗っ取られるリスクを想定する。 ③保守時のリスク、保守用ツールの悪用によるリスクも想定する。	①セキュリティ上の脅威や機器の故障の影響が、他の機器とつながることにより波及するリスクを想定する。 ②特に、安全安心対策のレベルが低い機器やシステムがつながると、影響が波及するリスクが高まることを想定する。	①盗まれたり紛失した機器の不正操作や管理者のいない場所での物理的な攻撃に対するリスクを想定する。 ②中古や廃棄された機器の情報などの読み出しやソフトウェアの書き換え・再販売などのリスクを想定する。	①外部インタフェース経由／内包／物理的接触によるリスクに対して個々のIoTコンポーネントで対策を検討する。 ②個々のIoTコンポーネントで対応しきれない場合は、それらを含む上位のIoTコンポーネントで対策を検討する。	①IoTコンポーネントの異常を検知できる設計を検討する。 ②異常を検知したときの適切な振る舞いを検討する。	①安全安心を実現するための設計を見える化する。 ②安全安心を実現するための設計の相互の影響を確認する。	①IoTコンポーネントがつながる相手やつながる状況に応じてつなぎ方を判断できる設計を検討する。 ②危険なつなぎ方をしにくい設計や危険なつなぎ方に気づくような設計を検討する。	①つながる機器やシステムは、IoTならではのリスクも考慮して安全安心の設計の検証・評価を行う。	①自身の状態や他機器との通信状況を把握して記録する機能を検討する。 ②記録を不正に消去・改ざんされないようにする機能を検討する。	①経年で増大するリスクや変化する使い方・利用環境に対し、アップデートなどで安全安心を維持する機能を検討する。	①欠陥や脆弱性、事故やインシデントの最新情報を常に収集・分析する。 ②必要に応じて社内や関係事業者、情報提供サイトなどへリスクの情報を発信し共有する。	①導入、運用、保守、廃棄で守ってもらいたいことを直接それらの業務に関わっている担当者や外部の事業者に伝える。	①不用意なつなぎ方や不正な使い方をすると、自分だけでなく、他人に被害を与えたり、環境に悪影響を与えたりするリスクがあることを一般利用者に伝える。 ②安全安心を維持していくために一般利用者に守ってもらいたいことを伝える。
本指針が関係する項目は多い。しかし、「理解」や「合意」についての明確な記述はない。	人材の確保・育成は合意につなげる理解の醸成に寄与する。しかし、明確な合意形成や他ステークホルダの合意の記述はない。	合意形成においては、本指針はほぼ無関係といえる 個々の指針毎の合意も必要である。	合意形成においては、本指針はほぼ無関係といえる 個々の指針毎の合意も必要である。	合意形成においては、本指針はほぼ無関係といえる 個々の指針毎の合意も必要である。	合意形成においては、本指針はほぼ無関係といえる 個々の指針毎の合意も必要である。	合意形成においては、本指針はほぼ無関係といえる 個々の指針毎の合意も必要である。	合意形成においては、本指針はほぼ無関係といえる 個々の指針毎の合意も必要である。	合意形成においては、本指針はほぼ無関係といえる 個々の指針毎の合意も必要である。	設計の見える化が合意形成の一助になることは確かだが、まだ不足	合意形成においては、本指針はほぼ無関係といえる 個々の指針毎の合意も必要である。	合意形成においては、本指針はほぼ無関係といえる 個々の指針毎の合意も必要である。	合意形成においては、本指針はほぼ無関係といえる 個々の指針毎の合意も必要である。	合意形成においては、本指針はほぼ無関係といえる 個々の指針毎の合意も必要である。	本指針が関係する項目は多い。しかし、「理解」や「合意」についての明確な記述はない。	本指針が関係する項目は多い。しかし、「理解」や「合意」についての明確な記述はない。	本指針が関係する項目は多いしかし、「理解」や「合意」についての明確な記述はない。

理解や合意が必要だが明確な記述はない

合意形成アウトカムに直接つながる指針ではない。しかし、**各指針の合意は必要**と考える。

設計の見える化は、理解を助け合意形成の一助になる

合意形成アウトカムに直接つながる指針ではない。しかし、**各指針の合意は必要**と考える。

アウトカムに関連する項目が多い
理解や合意が必要だが明確な記述はない

OSDの視点からの提言の例

■ 設計：守るべきものを守る設計を考える

指針12の「安全安心を実現する設計の検証・評価を行う」は、OSDでの「障害対応の遂行」につながる。

OSDでは「起きた障害の実態に即して設計時の仮定を見直す」、「なされた対応処理を評価する」ために、設計時だけでなく運用時にも検証・評価を行うことも要求している。

■ 運用：関係者と一緒に守る

指針15、16では、リスクや守ってもらいたいことの関係者への周知が重視されている。

OSDの合意形成の観点からは、さらに、何にどこまで対応するか等について関係者との「明示的合意」を双方向のコミュニケーションで確立することも要求している。

また、障害対応に対する、関係者、一般利用者へ、「実施した障害対応が、正しい対応であったか」の説明責任遂行も要求している。更に、合意をなぜ守らないといけないのか、守らないとどうなるかについて、普段から説明をして納得を得ることも要求している。

IPA SEC Journalへ寄稿

得られた知見をIPA発行の雑誌で公開

IPAの SEC journal 第53号。
[IEC 62853と「つながる世界の開発指針」Open Systems Dependabilityの観点からの考察]

https://www.ipa.go.jp/files/000068597.pdf

寄稿

IEC 62853と「つながる世界の開発指針」Open Systems Dependabilityの観点からの考察

DEOS 協会 技術部会／パナソニック 中川 雅通　DEOS 協会 技術部会／富士ゼロックス 山浦 一郎
DEOS 協会 標準化部会／株式会社ソニーコンピュータサイエンス研究所 森田 直
DEOS 協会 標準化部会／神奈川大学 武山 誠　DEOS 協会 標準化部会／神奈川大学 木下 佳樹

変化に対応してサービスを継続できるシステムの指針として、OSD：Open Systems Dependability の考えに基づく国際標準 IEC 62853 が今年発行された。一方、IoT 分野の開発において安全安心の確保のための指針として「つながる世界の開発指針」がある。本稿では、OSD の概要と、「つながる世界の開発指針」を OSD の観点から考察した内容を紹介する。

1 はじめに

現在のシステムは、利用者の期待、環境、技術などの様々な変化に直面している。そのためシステムが長期間サービスを提供し続けるには、運用開始後でも変化に対応し、適応、成長し続けなければならない。変化によく対応できるシステムの提供、継続のために、一般社団法人ディペンダビリティ技術推進協会（DEOS 協会）※1は「OSD：Open Systems Dependability」※2※3の考え方を基本とし、その実用化研究、概念の普及、標準化などを推進している。その結果を反映し、対象分野によらない汎用の OSD 要件の国際標準 IEC 62853 Open Systems Dependability ※4が今年発行された。

一方、IoT 分野、つまり様々なモノがつながって新たな価値を創出していく『つながる世界』では、安全安心の確保が問題となっている。独立行政法人情報処理推進機構 技術本部 ソフトウェア高信頼化センター（IPA/SEC）※5は、IoT 分野の開発で安全安心に関して最低限考慮すべき事項を「つながる世界の開発指針」※6としてまとめている。

OSD と「つながる世界の開発指針」は、つながり変化する世界で機能やサービスを継続して提供し続けるという共通の課題に取り組んでいる。本稿では、汎用の OSD の観点から、IoT 分野を対象とした「つながる世界の開発指針」を考察して得られた知見について報告する。詳細は、DEOS 協会の技術資料※7に記載している。

2 OSDの概要

OSD では、従来別々に扱われていた開発と運用・保守を、変化ドバックし合うステージすべてで継続して行われる、サービスを提供し続けるための活動である。OSD の要件は、合意形成、説明責任遂行、変化対応、障害対応の各目的を達成する 4 つの「プロセスビュー」のそれぞれが、ライフサイクル全体の中で実現されていることである。

2.1 OSD の 4 つのプロセスビュー

以下に OSD の核となる 4 つのプロセスビューの目的について説明する。

■ 合意形成プロセスビュー
・システム、システムの目的、目標、環境、性能、ライフサイクル、及びこれらの変化に関する共通理解と明示的合意を確立し、維持する。

■ 説明責任遂行プロセスビュー
・合意事項違反と、違反によってステークホルダと社会一般にもたらされる帰結（説明責任者に課される救済義務を含む）との間の対応関係を確立することで、合意実現の公算を増し、システムに対する確信と信用を保ち、潜在的な被害に対する救済措置を確保する。

■ 障害対応プロセスビュー
・障害に際してもサービス中断と損害を最小にとどめ、その状況のもとで最も適切なやり方で、可能な限りサービス提供を続ける。

■ 変化対応プロセスビュー
・要求事項、環境、目標又は目的が変化しても、システムを「目的にかなった（fit for purpose）」状態に維持する。

2. 医療情報ガイドライン

- 「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」へOSDの考え方を取り入れたいと経産省和泉審議官おりお声がけいただく。

- 医療情報に関するシステムは、患者、医療機関、システム開発事業者、システム運用事業者など専門知識の異なる多くのステークホルダーが関係するシステム。

- ガイドライン案をOSDの観点から検討し、主に合意形成、説明責任の観点から追加、修正案を提案。
- 2020年8月のガイドラインへOSDの観点が取り込まれる。
  https://www.meti.go.jp/press/2020/08/20200821002/20200821002.html

医療情報システム等のライフサイクル

共通理解や、合意の維持などのOSDの観点

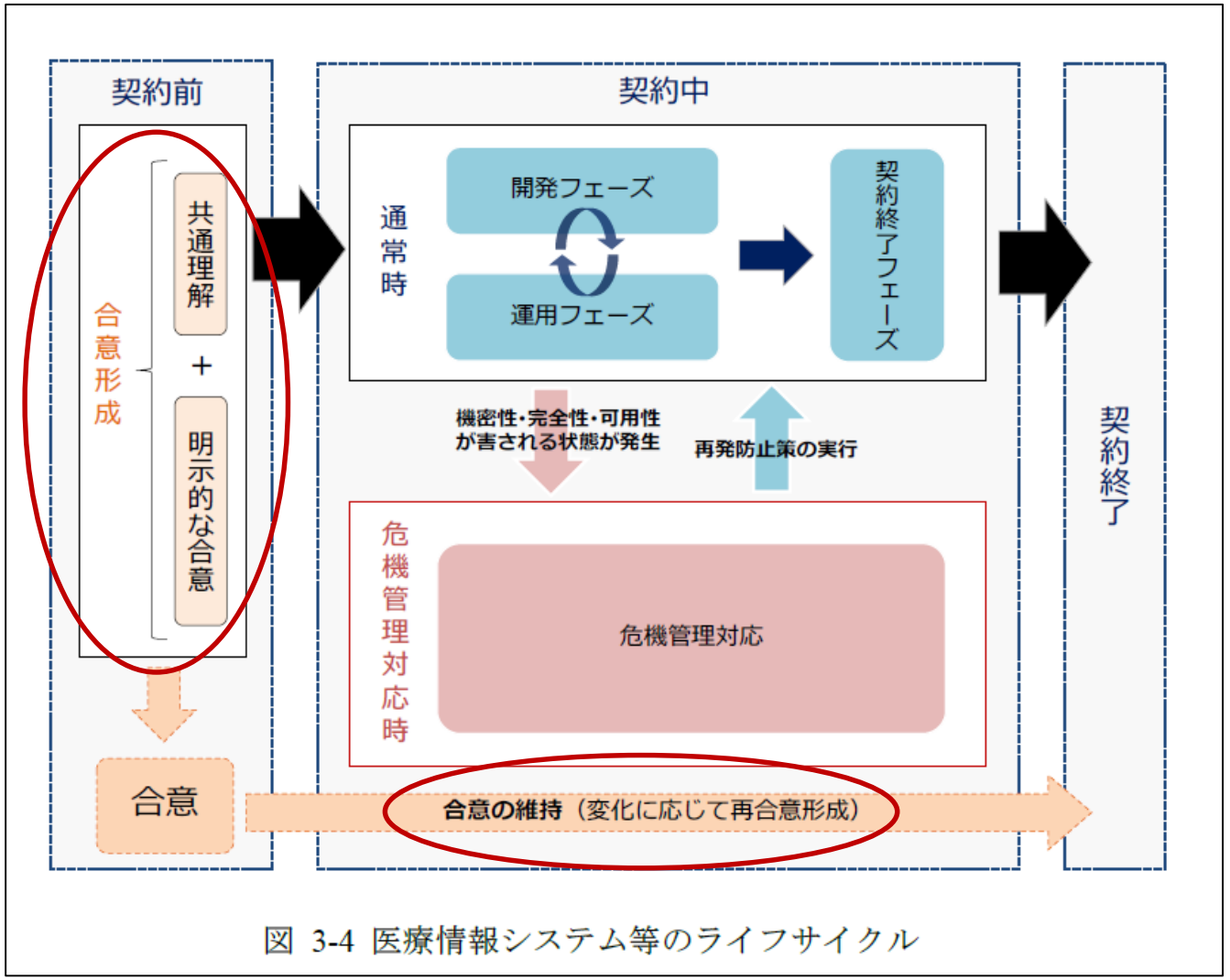


図 3-4 医療情報システム等のライフサイクル

3. 機械学習品質マネジメントガイドライン

- 産総研の「機械学習品質マネジメントガイドライン　第一版」
  https://www.cpsec.aist.go.jp/achievements/aiqm/
  （以下AIQMガイドライン）を、OSDの観点から検討中

- ガイドラインの主眼は、従来のソフト開発と異なる機械学習の品質の確保についてである。例えば、データへの依存性、繰り返しによる要件の獲得の仕方、運用での学習などである。

- OSDの観点からは、機械学習の不確実性、運用時での学習が開発行為となる点、モニタリングの重要性などへの言及など、関連する内容も数多くあると考える。

AIQMの中でOSDに関連しそうな記載

- 1.3.2 継続的なリスクアセスメント

  機械学習を利用するシステムにおいては、いわゆる「バグ」「初期不良」への対応として必要な修正だけでなく、当初から運用開始後の状況変化への対応を想定し、開発・運用を一体化した継続的ライフサイクルプロセスを導入することが必要となる場合が多い。

- 1.5.1 リスク回避性

  一般に機械学習システムにおいて、「どんなときにでも必ず安全な動作をする」といったような厳密な性質の保証は本質的に馴染まず、機械学習要素単体だけではシステム全体に必要の利用時品質を達成できないことも考えられる。

- 1.6.4 外部環境の複雑性への対応限界

  路上や公共空間などの開放環境でいわゆるサイバーフィジカルシステムの一部として組み込まれる形態も多くあり、全ての環境条件において期待通りの判断を行う事は、極限的な状況も含めると不可能である。この問題は本質的には、機械学習に依らず、開放環境で動作する装置やソフトウェア全般に共通する問題であり、従来の信頼性工学関係の規格においても、例えば IEC 629986などがこの問題に多かれ少なかれ対応しようとしていると考えられる。

2021年度 技術活用部会活動

一緒に議論、検討していただけるメンバーを大募集中です。
OSDを理解するには、具体的な事例で考えるのは大変役に立ちます。
masamichi.nakagawa@deos.or.jp までご連絡ください。

実施日・時間	奇数月のDEOS運営会議終了後 （通常、17～19時）
内容	①IEC62853の開発文書とのマッピングWorking Group 目的: 展開・普及へつながるアウトプットを生み出す 参加: 情報収集ではなく、作業する会員メンバ限定 ※会員の方で、参加希望の方は随時連絡ください 2021年度、まずはAI品質保証に関する適用を中心に議論予定 ②上記①の活動成果報告（年数回）
参加者	① 作業に参加して頂ける会員メンバ ② 会員メンバは誰でも参加可能
開催場所	WEB会議形式　(状況に応じて運営会議の実施会場）