L1C12 - Tool 4: Secure Multi-Party Computation

0:00	so in the last several concepts we've	ここ数回のコンセプトでは
0:01	been walking through several different	いくつかの異なる場所を歩いています
0:03	tools that together are coming together	一緒に集まるツール
0:05	to build the remote data science	**リモートデータサイエンスを構築する**
0:07	ecosystem	**生態系**
0:08	and in the last concept we talked about	そして前回話したコンセプトで
0:10	differential privacy which makes it	それを可能にする**差分プライバシー**
0:12	possible to to add automation to the	**に自動化を追加する**ことが可能
0:14	process by which you can download your	ダウンロードできるプロセス
0:16	results automatically	自動的に結果が得られます
0:18	from a remote server that you've been	これまでに使用していたリモートサーバーから
0:20	doing data science in but we encountered	データサイエンスを行っているのですが、
0:23	this this sort of next problem which was	これは次の問題でした
0:25	you know what does it mean if we needed	必要だった場合、それが何を意味するか知っていますか
0:27	to actually do data science against	実際にデータサイエンスを行うには
0:29	multiple organizations at the same time	複数の組織を同時に
0:31	where data at each organization needed	各組織のデータが必要な場所
0:34	to touch each other as a part of the	の一環としてお互いに触れること
0:36	algorithm right meaning we're doing a	アルゴリズムは正しく、私たちが実行していることを意味します
0:38	join or or some type of interaction	参加する、または何らかの種類の対話
0:41	where there needs to be arithmetic	算術が必要な場所
0:42	between data that's at one location data	1 つの場所にあるデータ間
0:44	it's another location without either	どちらも無い別の場所です
0:46	those data points being able to	それらのデータポイントは、
0:48	to leave right this is not something	正しく去ることは何かではありません
0:50	that remote execution or sample data or	リモート実行またはサンプルデータ、または
0:54	or differential privacy are particularly	または差分プライバシーは特に
0:56	well suited to solve and that brings us	解決するのに適しており、それが私たちにもたらします
0:59	to our fourth and final tool that we're	私たちの4番目で最後のツールへ
1:00	going to cover in this lesson which is	このレッスンで取り上げるのは
1:02	called secure multi-party computation	**安全なマルチパーティ計算**と呼ばれる
1:04	now i got to say secure multi-party	今、私は安全なマルチパーティについて言わなければなりません
1:06	computation is one of my absolute	計算は私の絶対的なものの一つです
1:08	favorite tools it is	お気に入りの道具です
1:10	i think it's easy to say that it's it's	それはそうだと言うのは簡単だと思う
1:12	the most magical piece of technology	最も魔法のようなテクノロジー
1:14	that i've ever come across before and	私がこれまでに出会ったことと、
1:16	i'm super excited to share with you if	もしよろしければ、あなたと共有できることをとても楽しみにしています
1:17	you haven't come across it before	あなたはこれまでに遭遇したことがありません
1:18	so the textbook definition of secure	つまり、安全性の教科書的な定義は
1:20	multi-party computation is one where	マルチパーティ計算は次のようなものです。
1:22	multiple people can combine their	**複数の人が自分の意見を組み合わせることができます**
1:24	private inputs to compute a function	関数を計算するためのプライベート入力
1:26	without revealing their inputs to each	それぞれの意見を明らかにすることなく、
1:28	other	他の
1:29	this is a little bit wordy you know this	これは少し冗長です、あなたはこれを知っていますか
1:30	is sort of the wikipedia definition	それはウィキペディアの定義のようなものです
1:32	right what i like to think of it is is	そうです、私が考えたいのはそれです
1:34	the implication is that multiple people	意味するところは、複数の人が
1:35	can share ownership of a number	番号の所有権を共有できる
1:38	and share ownership of a number let's	番号の所有権を共有しましょう
1:41	look at an example	例を見てください
1:42	so let's say i had the number five right	それで、私が 5 という数字が正しかったとしましょう
1:44	and i split this into shares think of it	そしてこれをいくつかの株に分割しました 考えてみてください
1:47	like shares of a company right shares of	会社の株式のような権利の株式
1:50	ownership you know i'll split it into a	所有権は分割します
1:51	two and a three in this particular case	この特定のケースでは 2 と 3
1:52	the algorithm right for for	に適したアルゴリズム
1:55	combining or decrypting these shares is	これらの共有を結合または復号化することは、
1:57	just to add these two shares together	これら 2 つの共有を合計するだけです

1:58	right so if you have all the shares you	そうです、すべての株式を持っている場合は、
2:00	know what the number is right but if you	正しい数字はわかっていますが、もしあなたが
2:01	don't have all of shares you don't know	知らない株をすべて持っているわけではありません
2:03	what the number is right so i take these	正しい番号は何ですか、それでこれを受け取ります
2:04	shares and i'll give them to my friends	シェアして友達にあげます
2:06	marianne and bobby right	マリアンヌとボビー右
2:08	and then i will disappear	そして私は消えます
2:10	and between marianne and bobby	そしてマリアンヌとボビーの間
2:12	is this number five right so you know	この5番は正しいですか？
2:15	marianne is number two bobby has a	マリアンヌは2位です ボビーは
2:16	number three two plus three equals five	数字の 3 2 プラス 3 は 5 に等しい
2:17	right	右
2:18	but neither marianne nor bobby know the	でもマリアンヌもボビーもそのことを知らない
2:21	value that's that's sort of encrypted	ある種の暗号化された値
2:23	between them because neither of them	彼らの間では、どちらでもないので
2:25	have all of the shares right so this	すべての共有が正しいので、これは
2:27	gives us this this encryption property	この暗号化プロパティを提供します
2:29	where neither of them knows the hidden	彼らのどちらも隠されたものを知らない場所
2:30	value	価値
2:31	but it also gives us the second property	しかし、これにより 2 番目のプロパティも得られます
2:32	which is **shared governance** because the	これは**共有ガバナンス**です。
2:34	number can only be used if everyone	この番号は全員が使用できる場合にのみ使用できます
2:37	agrees if all the shareholders agree put	株主全員が同意すれば同意する
2:40	another way all the shareholders in this	別の方法では、この株主全員が
2:41	particular algorithm have veto power	特定のアルゴリズムには拒否権がある
2:44	over what this particular number can be	この特定の数値がどの程度になるのか
2:46	used for	のために使用される
2:48	but perhaps the most extraordinary part	しかしおそらく最も特別な部分は
2:50	is that while this number is in this	この数字がこの中にある間はということですか
2:52	sort of **encrypted**	一種の**暗号化された**
2:54	**shared governance** state	**共有ガバナンス**状態
2:56	we can perform arithmetic	私たちは算術を実行できます
2:58	so let's say	だから言ってみましょう
3:00	mary and bobby	メアリーとボビー
3:01	got together and they decided you know	集まって、彼らは知っていると決めた
3:02	what let's multiply our hidden encrypted	隠された暗号化されたものを何倍にしましょう
3:04	number by two	2つずつ数える
3:07	so if marianne takes her share	それでマリアンヌが彼女の分け前を奪ったら
3:08	multiplies it by two and bobby takes his	それを2倍すると、ボビーは彼のものを受け取ります
3:10	share and multiplies it by two then the	共有して 2 倍して、
3:12	result is a four and a six which sum to	結果は 4 と 6 で、合計すると次のようになります。
3:15	equal ten which means that they've taken	10 に等しい、つまり彼らが取ったことを意味します
3:17	their encrypted five and they've	彼らの暗号化された5つ、そして彼らは
3:18	multiplied it by two even though	たとえそれを2倍したとしても
3:21	neither of the shareholders know the	株主のどちらも知りません
3:23	**value** of the number they're encrypting	暗号化している数値の**値**
3:25	right	右
3:26	and the the big takeaway is that there's	そして最大のポイントは、
3:28	a whole host of algorithms to perform	**実行する多数のアルゴリズム**
3:30	all sorts of mathematical statistical	**あらゆる種類の数学的統計**
3:32	analysis while numbers are in this	数字が入っている状態での**分析**
3:34	shared state right and and the second	共有状態権と 2 番目
3:37	thing i want you to take away is that	あなたに奪ってほしいものはそれです
3:39	models and data sets you know these	あなたが知っている**モデルとデータセット**
3:41	these **tensors** these these underlying	これらの**テンソル** これら**の基礎**となる
3:43	data structures underneath data science	データサイエンスの**基盤となるデータ構造**
3:45	are just large collections of numbers	単なる数値の大きなコレクションです
3:47	which we can individually encrypt	個別に暗号化できる
3:51	right and so so where does this leave us	そうです、それで、これは私たちをどこに残すのでしょうか
3:53	okay so	そして
3:54	so remote data can remain a remote	**リモートデータをリモートのままにできる**
3:56	machine we do remote execution we've got	私たちが持っている**リモート実行を行うマシン**
3:59	surgeon sample data which allows us to	外科医のサンプルデータにより、
4:00	feature engineer using toy data we've	私たちが持っているおもちゃのデータを使用した**機能エンジニア**

4:02	got formal rigorous privacy budgeting	正式に厳格なプライバシー予算を設定した
4:05	that means that we can download or or	つまり、ダウンロードできる、または
4:07	decrypt our secure multi-party	安全なマルチパーティを復号化します
4:09	computation results automatically based	計算結果に基づいて自動的に
4:11	on whatever privacy budget has been	プライバシーに関する予算がどのようなものであっても
4:12	allocated to us	私たちに割り当てられた
4:14	and finally	そして最後に
4:17	if we want to send in	送りたい場合は
4:20	some sort of	ある種の
4:21	model or or statistical result that we	私たちが作成したモデルまたは統計結果
4:25	want to make sure that the data owner	データ所有者であることを確認したい
4:26	doesn't have the ability to steal so if	盗む能力がないので、
4:28	i'm sending an ai model into a hospital	AIモデルを病院に送り込んでいます
4:30	to learn from the data	データから学ぶ
4:32	right and and i want to make sure they	そうです、そして私は彼らがいることを確認したいのです
4:33	can't steal that model i can use secure	そのモデルは盗めないので安全に使用できます
4:35	multi-party computation to encrypt the	マルチパーティ計算による暗号化
4:38	values	価値観
4:39	right so that i'm a shareholder they're	そうです、私は彼らの株主なのです
4:42	a shareholder	株主
4:43	and neither of us can can steal each	そして私たちはどちらもそれぞれを盗むことはできません
4:46	other's data despite the fact that we	私たちが行っているにもかかわらず、他人のデータ
4:47	can compute	計算できる
4:49	a smarter model right a smarter ai than	よりスマートなモデル、よりスマートな AI
4:52	the next smart ai or if we wanted to do	次のスマート AI または私たちがやりたいかどうか
4:54	a join across multiple different data	複数の異なるデータ間の結合
4:57	owners we could take each number that we	所有者は、私たちが取得した各番号を取得できます
5:00	want to do the join across split it into	分割して結合したい
5:01	multiple shares	複数のシェア
5:03	and as long as each number that wants to	そして、希望する各番号が続く限り、
5:04	participate in computation	計算に参加する
5:06	can can be distributed across all the	すべてに分散できます
5:08	shareholders so you know if it's me and	株主だから、それが私かどうか知っていますか？
5:09	two hospitals right where there's	すぐそこに病院が2つある
5:11	hospital a and hospital b hospital a	病院Aと病院B 病院A
5:14	takes their data and splits it into	データを取得して分割します
5:15	shares and gives some to hospital b and	一部を病院bに分けて渡し、
5:17	hospital b takes their data and splits	b 病院はデータを取得して分割します
5:19	into shares and gives one set of shares	株式に分割し、1 セットの株式を付与します
5:20	to hospital a and all of a sudden i can	病院に行くと突然できるようになりました
5:22	request	リクエスト
5:24	encrypted computation across data sets	データセット全体での暗号化された計算
5:26	from hospitals a and b so that that	病院aとbから
5:28	means that from from my perspective	つまり、私の視点から見ると
5:31	like i can just view	ただ見ることができるように
5:33	as a data scientist	データサイエンティストとして
5:36	the world's organizations kind of like	世界の組織は似たようなものです
5:38	it's just one big data set	それは単なる 1 つの大きなデータセットです
5:40	right from from my perspective	私の視点から見て
5:43	as long as they're willing to	彼らが喜んでいる限り
5:45	send shares to each other from time to	相互に株式を送信し合う
5:47	time which which again the act of	もう一度どの行為が行われるか
5:48	sending a share does not reveal any	共有を送信しても何も明らかにされません
5:50	information about the underlying data it	基礎となるデータに関する情報
5:51	just says hey	ただ「ねえ」と言うだけ
5:52	i'm open to computing	私はコンピューティングに対してオープンです
5:56	with you right and and the result of	あなたと一緒に正しく、そしてその結果
5:58	that computation we will collectively	その計算を私たちは集合的に行います
6:00	decide as shareholders whether the data	データが正しいかどうかを株主として決定します。
6:02	scientist should be allowed to see it	科学者はそれを見ることを許されるべきだ
6:04	right so from the perspective of the	そうです、その観点から見ると
6:05	data owner	データ所有者
6:07	they they can choose who they allow to	彼らは誰を許可するかを選ぶことができます
6:08	who they want to participate with right	誰と一緒に参加したいのか

6:10	who who and they're able to maintain	誰が誰を維持できるのか
6:12	long-term control	長期管理
6:14	not just over their own data but over	自分自身のデータだけでなく、
6:16	all all derivative data science answers	すべてのすべての派生データサイエンスの回答
6:20	based on their data right and	データ権に基づいて、
6:22	collectively work with the other	他の人と共同で作業する
6:23	shareholders to answer the question of	株主が質問に答える
6:25	do we allow this data scientist to	このデータサイエンティストに許可しますか?
6:27	answer this question using our	私たちの質問を使ってこの質問に答えてください
6:29	information	情報
6:30	right	右
6:31	but but my perspective from the data	でもでも、データから見た私の視点
6:32	scientist is is that	科学者はそれです
6:34	i just view it as like the world's data	私はそれを**世界のデータのように見ている**だけです
6:36	i just do my data science download my	**データ サイエンス**を行うだけです。
6:39	results thanks to differential privacy	差分プライバシーのおかげで結果が得られる
6:40	and and i have extraordinarily accurate	そして私は非常に正確です
6:43	results because it's coming from the	**結果は**から来ているので、
6:45	world's institutions	**世界の機関**
6:46	right and so i hope that you as you see	そうです、それで私はあなたが見ての通りであることを願っています
6:48	the combination of these these building	これらの建物の組み合わせ
6:51	tools together working working hand in	ツールが一緒に働く 協力して働く
6:53	hand in like a cohesive remote data	**まとまったリモートデータのように提供する**
6:56	science interface that it starts to look	**見え始める**サイエンス**インターフェース**
6:58	like you know you as data scientists can	データ**サイエンティストがあなたを知っているかのように**
7:00	sit at a portal to this new internet	この新しいインターネットへの入り口に座ってください
7:03	this data science internet with with	このデータ サイエンス インターネットと
7:05	individual private data servers living	個々のプライベートデータサーバーが生きています
7:07	at institutions all around the world	世界中の施設で
7:09	where you can answer questions using	を使用して質問に回答できる場所
7:12	using all the worlds of available	利用可能なすべての世界を使用して
7:13	information that is relevant to your	あなたに関連する情報
7:16	topic without ever needing to acquire a	を取得する必要なくトピックを取得できます。
7:18	copy of that information in the process	プロセス中のその情報のコピー
7:19	right	右
7:20	but that data owners have the ability to	ただし、データ所有者には次のことが可能です
7:23	**with a high degree of automation**	**高度な自動化により**
7:25	with a high degree of automation	高度な自動化により
7:28	**serve you and thousands millions of**	あなたと何千もの人々に奉仕します
7:31	**other data scientists** along **along the**	他のデータサイエンティストも
7:32	**way**	道
7:33	without having to do all this sort of	このようなことをしなくても
7:36	manual red tape sort of risk mitigation	手動による煩雑な手続きによるリスク軽減
7:39	that that old school data science	その**昔ながらの**データ**サイエンス**
7:41	tools and techniques require so um	ツールとテクニックには非常に必要なものがあります
7:44	**i hope you found this concept to be**	**この**コンセプトを理解していただければ幸いです
7:45	**interesting**	**面白い**
7:46	in the next concept we're going to go	次のコンセプトで行きます
7:48	one step further and really try to	さらに一歩進んで、実際に試してみてください
7:51	say okay given this technology	このテクノロジーを考慮すると大丈夫と言う
7:55	what and how do these institutions	これらの機関は何をどのように行うのか
7:56	actually make these decisions what what	実際にこれらの決定を下すのは何をするのか
7:58	what is it really going to look like	実際はどうなるのでしょうか？
8:00	what are what are these servers you know	あなたが知っているこれらのサーバーは何ですか
8:01	you could you say these algorithms that	これらの**アルゴリズムは次のように言えますか?**
8:03	that are going to be able to allow	**それは許されるだろう**
8:04	people to to you know set privacy	プライバシーを設定する
8:06	budgets or or or approve projects	予算やプロジェクトの承認
8:09	collectively group what does that	集合的にそれは何をするのかをグループ化する
8:10	actually look like at the end of the day	実際に一日の終わりのように見える
8:12	and well we're not going to cover all of	すべてをカバーするつもりはありません
8:13	it in this lesson in the next concept we	このレッスンでは、次のコンセプトで説明します。
8:15	are going to lay out a little bit of the	を少しレイアウトしてみます
8:17	base definitions that set us up for the	私たちを設定する基本的な定義

8:19	later lessons in this course see you	このコースの後のレッスンでお会いしましょう
8:21	then	それから

英語 (自動生成)

https://www.youtube.com/watch?v=H1sWPCFmfcs