内閣府　御中

平井大臣との意見交換会用

安全なデジタル社会の実現に向けた国家プロジェクトのご提案 PITCH

コネクトフリー株式会社

令和元年６月

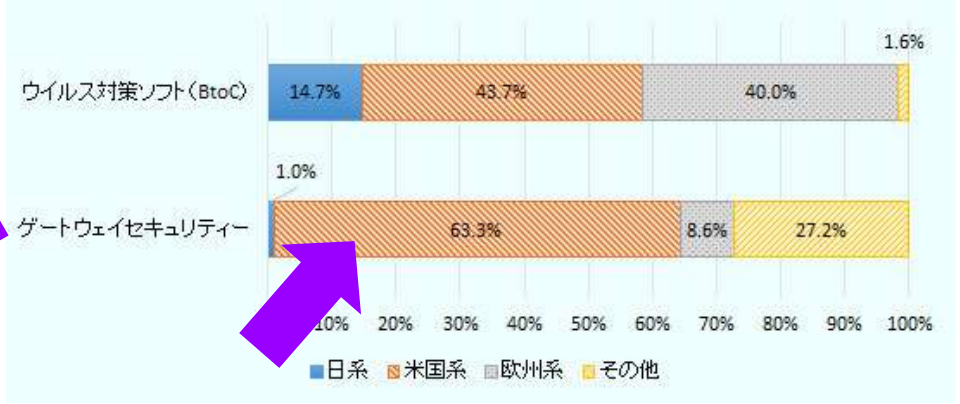
２０２５年目処にサイバーセキュリティ庁設立を提言

出所：自由民主党サイバーセキュリティ対策本部による第２次提言申入れ-令和元年5月14日
https://nettv.gov-online.go.jp/prg/prg18920.html

増大するサイバーセキュリティ対策費用（日本）

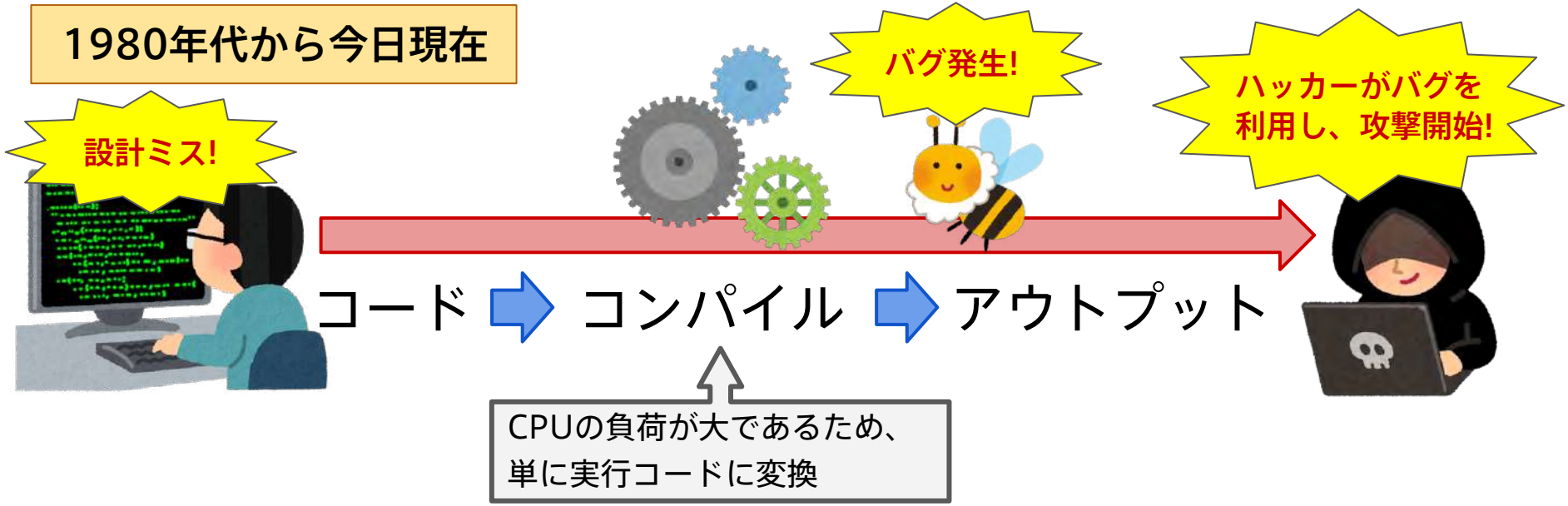
1兆円に拡大するセキュリティ対策費のほとんどが海外に流れている

出所:　日本ネットワークセキュリティ協会「国内情報セキュリティ市場調査」より
ジェトロ作成



出所:　国立研究開発法人新エネルギー・産業技術総合開発機構「平成29年度サービス・ソフトウェアの国際競争ポジションに関する情報収集」よりジェトロ作成

不安全なサイバー空間



ソフトウェア開発の根本は１９８０年代から変化しておらず、
ハッカーが付け入る脆弱性を創っている。

現代のデジタル社会における社会インフラのリスク

コードのリスク

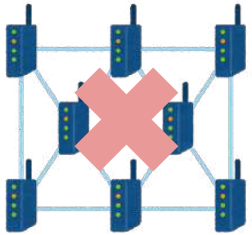
危険なメモリ操作でもコンパイルが通り、また未定義動作が存在し、またエラー処理構文が欠如しており、無秩序なエラー処理が行われているため、バグの温床になっている。

実行環境のリスク

環境内からのメモリのアクセスに制限がなく、悪意のあるアプリでもメモリの情報にアクセスできる。

通信のリスク

脆弱性を含む現在のインターネット構造は、なりすましやデータ傍受が簡単にできる。



製造元のリスク

法規制がないため、悪意のある攻撃が埋め込まれた部品・製品が紛れ込む危険性がある。

現在のセキュリティ対策

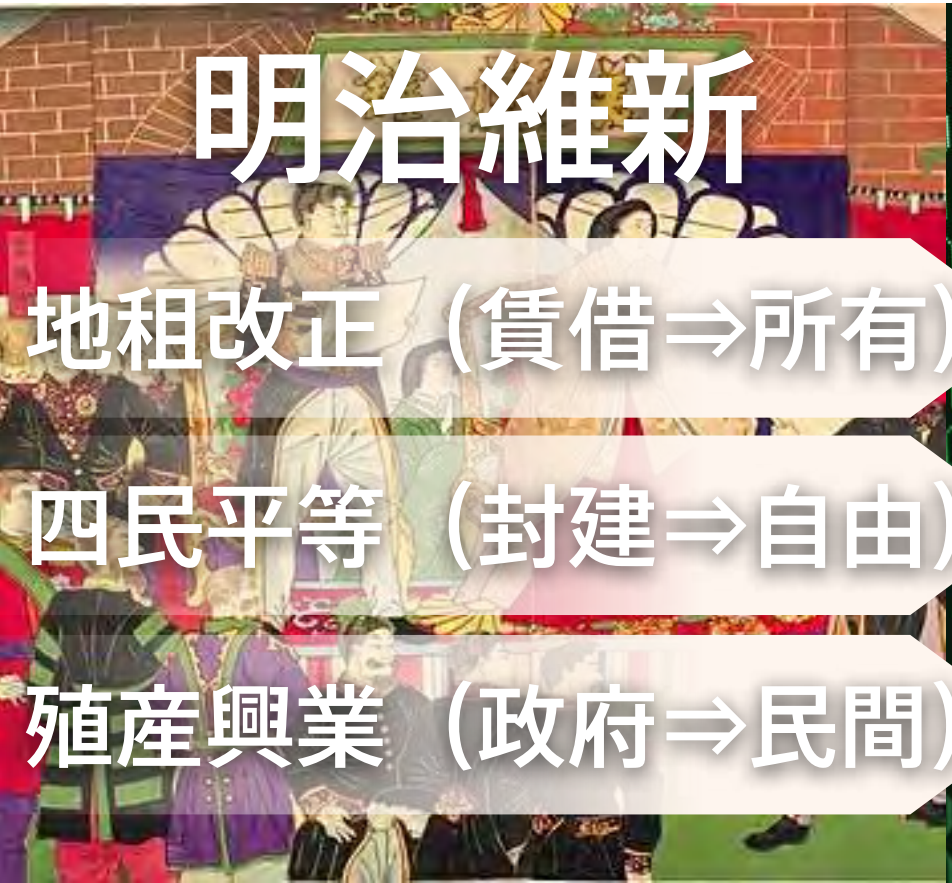
発生してしまったバグへの対策だけでは根本解決にはなりません。

ハッカーの付け入る脆弱性への都度対策だけでは根本解決にはなりません。

１９８０年代から変化していない設計ミスを無くさない限り、
根本的なセキュリティ対策はできないと考えます。

今実際に、社会インフラが危険に曝されています

今こそ、デジタル社会に維新を！



明治維新

地租改正（賃借⇒所有）

四民平等（封建⇒自由）

殖産興業（政府⇒民間）

令和維新

IPアドレスを所有化

第二インターネット

政府主導で日本のデジタル社会の安全基準を再整備し、国際競争力を上げる

社会インフラのリスクに対する解決策

Zen™
Compiler
Infrastructure

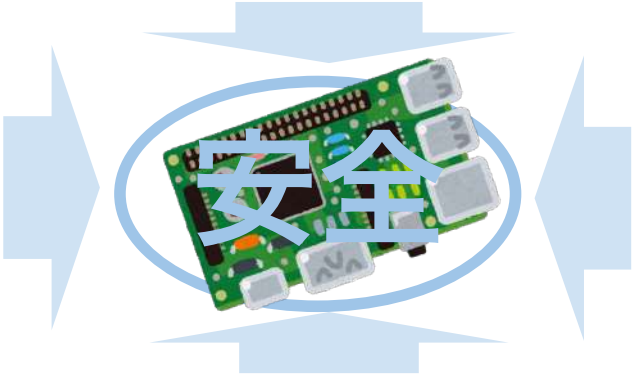
コードのリスクを解決策

メモリセーフティを有し、動作定義をすると共に、危険なメモリ操作によってはコンパイルを通さないなど、無秩序なエラー処理を回避し、エラー処理構文が欠如せず、バグが発生しない。

arm® TRUSTZONE® SoftBank Group

実行環境のリスクの解決策

環境内のアクセスを制限し、セキュアな環境を分離する結果、メモリをゾーン化し、実行前コード証明を確認できる。



connectfree everIP

通信リスクを解決策

各デバイスが唯一無二のIPアドレスを秘密情報から自己生成し、その秘密情報に基づく公開情報をお互いに認証すると共に暗号化通信を行う第二インターネット。

製造元のリスクの解決策

日本国内でバックグラウンドがチェック済みであることを義務化。

Efficient and Secure Societies (ESS) の実現へ

我々コネクトフリーは低レイヤの技術とツールによって８０年代のレガシーに埋もれた社会を安全かつ効率的な社会（ESS）に再構築いたします。

L3 安全かつ効率的な社会

L2 安全かつ効率的な取引

L1 安全かつ効率的な開発

Efficient and Secure Societies (ESS) がもたらす効果

セキュリティ対策コストの削減へ

現在セキュリティ対策には多大なコストが費やされています。
ESSでは、土台となるサイバー空間がセキュアなので、より安価にリスクを対策できます。

煩雑なセキュリティ対策からの解放へ

現在はパスワードによる認証や、データ管理の為の規則など、セキュリティを守るために労力が費やされています。ESSにおける第二インターネットではすでに端末が認証済みであるためパスワードがなくなり、なりすましやデータ傍受ができません。

国家プロジェクトの提言

安全かつ効率的な社会（ESS）のための法整備を。

・シートベルトの法整備が、車社会の安全化に寄与。

⇒デジタル社会についても、プログラマのためのシートベルトの装備を義務化し、コンピューティングシステムの脆弱性・不具合をそもそも発生させない技術のみを採用する旨の法整備により、安全化の実現へ。

（参照）
現存の制度は、不正アクセス・操作の恐れに繋がるコンピューティングシステムの脆弱性や不具合の発生を前提としたセキュリティ対策規制・認証制度のみ。

○ 重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針(第5版 改訂版)（NISC, R1/5/23）

○ ITセキュリティ評価及び認証制度(JISEC)、情報セキュリティ評価基準(ISO/IEC15408)(JIS X 5070)

○ 「サイバー・フィジカル・セキュリティ対策フレームワーク Ver1.0(経済産業省 商務情報政策局 サイバーセキュリティ課,H31/4/18)

車社会の安全確保：第二防衛線であるシートベルト

“Even if people have accidents, even if they make mistakes, even if they are looking out the window, or they are drunk, **we should have a second line of defense for these people**”

「たとえ人々が事故を起こしていても、たとえ人々が間違いを犯していても、たとえ人々が窓の外を見ていても、あるいは人々が酔っていても、**我々はこれらの人々のための第二防衛線を持つべきである**。」

Ralph Nader
Congressional Hearing
February 10th, 1966
（ラルフ・ネーダー　議会聴聞会にて 1966年2月10日）

当社の問題認識

「完璧な運転手が存在しないのと同じく、
完璧なプログラマもまた存在しません。」

帝都 久利寿

プログラマにもシートベルトが必要

８０年代から変わっていない今の仕組みの延長では
デジタル社会のセキュリティリスクに対応しきれません。

コードのリスク　実行環境のリスク　通信のリスク　製造元のリスク

法整備によって、リスクを低減する

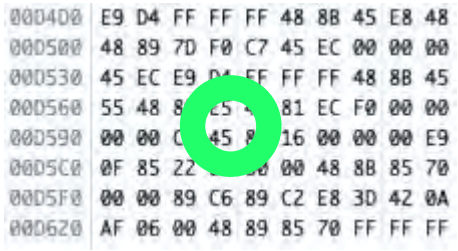
シートベルトを作れます。

arm TRUSTZONE®
実行前コード証明を確認できる計算環境

Zen™ Code Compiler

connectfree everIP®
柔軟かつ多目的な暗号化認証済中継方式

プログラマのためのシートベルト装備の義務化（法整備）

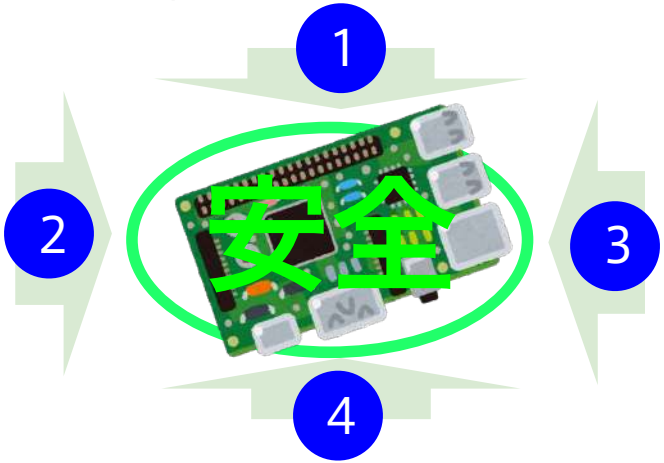


コードの安全化のための法整備

メモリセーフティを有し、動作定義がなされ、エラー定義及び秩序立ったエラー処理ができ、危険なメモリ操作がコンパイル不可能であり、エラー処理構文が欠如しない技術の採用を義務化。

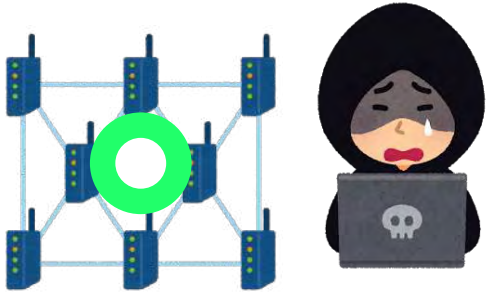
実行環境の安全化のための法整備

メモリのゾーン化、実行前コード証明の認証を義務化。



通信の安全化のための法整備

全ての通信が、なりすましや傍受ができないよう、通信での認証と暗号化を義務化。



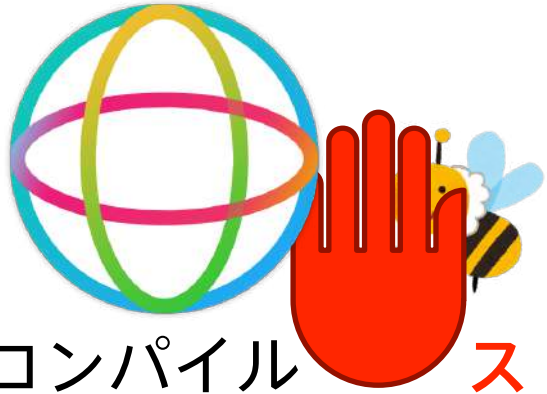
製造元の安全化のための法整備

日本国内でバックグラウンドがチェック済みであることを義務化。

コードの安全化のための法整備

1 これからのあるべき姿

コード ⇨ コンパイル ストップ！



CPU性能の向上で高速化されたことで事前チェック可能

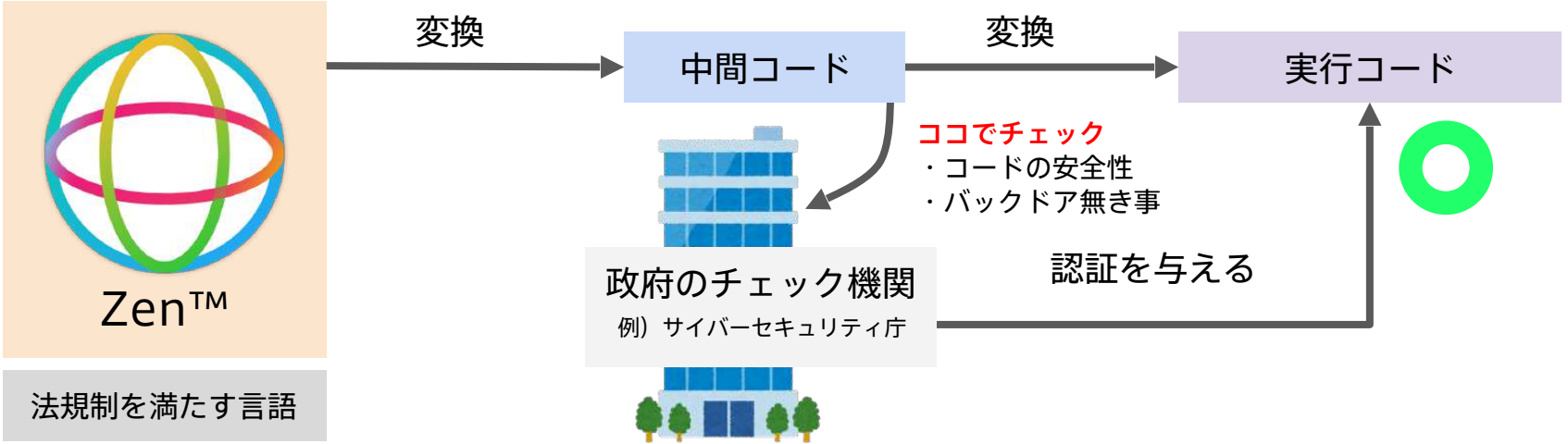
コンパイル時にバグ等が見つかるとコンパイルをストップするためハッカーが付け入る隙を限りなく減らすことができる。

コードの安全化のための法整備

1 これからのあるべき姿

法整備

危険なメモリ操作、無秩序なエラー処理、
バッファオーバーフロー等を防ぐ技術の採用



実行環境の安全化のための法整備

2 これからのあるべき姿

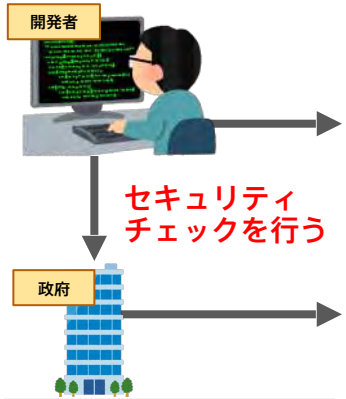
法整備

実行前に、実行コードが安全である旨のコード証明の確認を義務化

arm TRUSTZONE®

TrustZone®

法規制を満たす実行環境

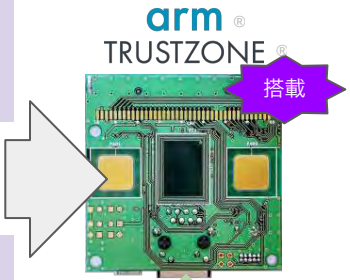


政府のチェック機関
例）サイバーセキュリティ庁

開発者提供実行コード

＋

コード証明



政府チェック機関のコード証明が確認できた時のみ実行を開始

通信の安全化のための法整備

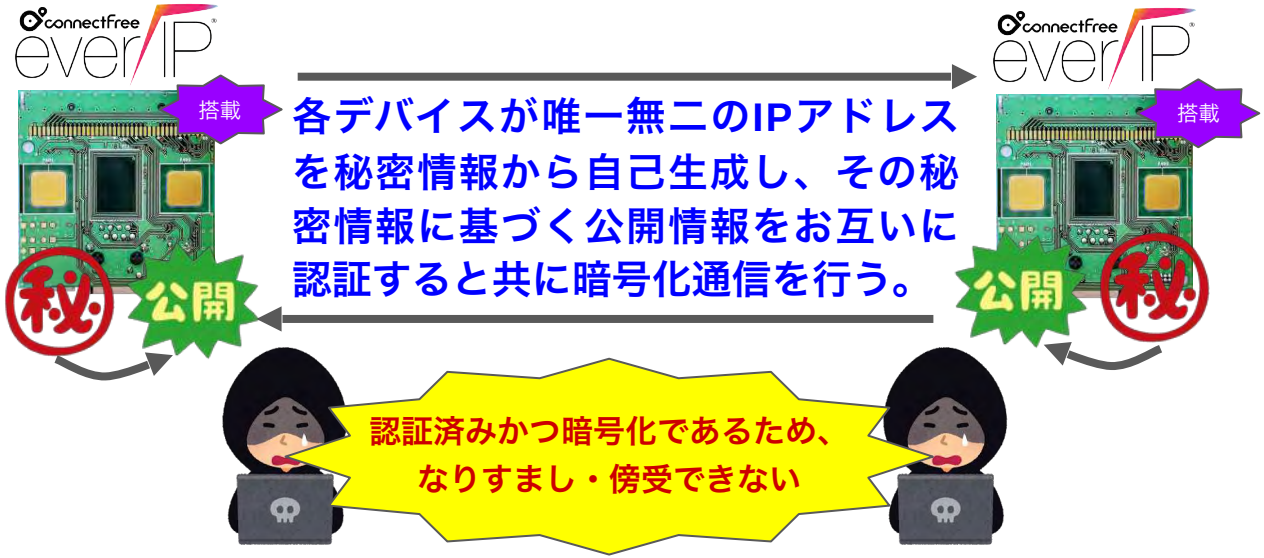
3 これからのあるべき姿

法整備

通信を行う端末間において相互認証済かつ暗号化されていない通信は行わない

EVER/IP®

法規制を満たす通信プロトコル

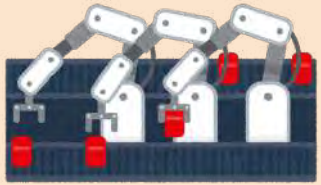


製造元の安全化のための法整備

4 これからのあるべき姿

法整備

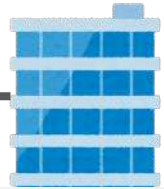
バックグラウンドがチェック済の工場及びその生産部品を認証



国内工場

バックグラウンドチェック

条件を満たす工場を認証する



政府の機関

各国との情報共有

法規制を満たす工場の利用