

分科会活動報告

共通評価フレームワーク分科会

株式会社ラック

奥野 康城

2022年6月



Cyber Security Initiative for Japan



奥野 康城（オクノ ヤスキ）

株式会社ラック

セキュリティビジネス統括部

コンサルティングサービス第三部 セキュリティマネジメントグループ

【経歴】

- ・ 1991年 製造業入社
 - 汎用機（AS/400：RPG400）
 - 社内インフラ（ネットワーク/サーバ等：2000年-）
 - CSIRT構築（設立メンバー：2010年-）
- ・ 2014年 株式会社ラック入社
 - セキュリティコンサルティング業務に従事
 - ※情報セキュリティプランニング・CSIRT構築支援など

【背景】

ITは、今やどのような企業や組織にとっても当たり前のものとなりました。パソコンやインターネットのほか、最近ではスマートフォンなどをはじめとする様々な端末や機器も利用できるようになり、当たり前のものとなったITを「いかに高度に」「いかに効果的に」使うかが、企業や組織の競争力に直結する時代になっています。

こうした流れの中で、情報セキュリティ対策は、必要不可欠なものとなりました。ひとたび企業や組織が保有する重要情報が漏えいするような事故が起こると、それまでに企業や組織が積み上げてきた社会的な信頼や評判にも大きな影響を与えかねません。情報セキュリティに関する技術や攻撃は日増しに高度化しており、組織側には従来以上に強固な対策が求められるようになっています。

【目的】

我が国の情報セキュリティの分野において、
事業や組織の安全レベルを向上させる

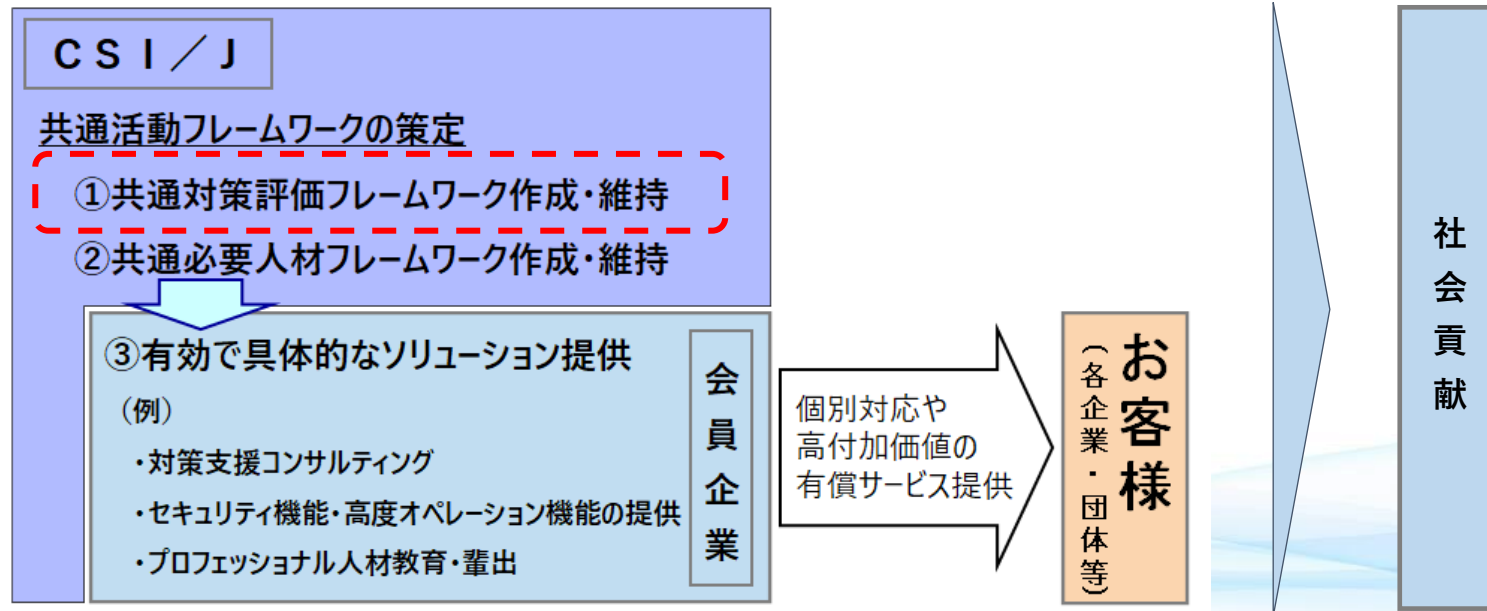


企業における「セキュリティレベルの向上」を目指し、クラウド、ゼロトラスト、IoT、サプライチェーン等の新領域に対する「サイバーセキュリティ」対応を、セキュリティ業界横断で顧客企業への支援活動をおこなう

支援の切り口は以下の通り

- ①サイバーセキュリティ共通対策評価フレームワークの策定・維持
- ②共通必要人材フレームワークの策定・維持
- ③有効で具体的なソリューションの提供：会員企業（セキュリティベンダ）による

活動概要



共通評価フレームワークとは：企業が安全にITの利活用やDX推進を進める中で、今現在のシステム利用状況や管理状況を見える化し、課題を浮かび上がらせることで、あるべき姿とのフィットギャップを示し、安全な運用を継続し続けるための指標となることを目的に、セキュリティ企業の知見を集めた共通評価フレームワークとして公開します。

例えば...

クラウド活用の
リスクと対策

サプライチェーンの
リスクと対策

ゼロトラストへの
指針と対策

IoTやDXの
リスクと対策

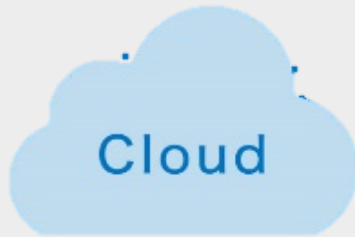
...

などなど...

このようなお悩みの
指標となるフレームワークを！

第一弾

共通評価フレームワーク（クラウド版）



- ・ クラウド環境を利用しようと検討中の企業
- ・ クラウドを利用しているが、安全性に不安のある企業

- クラウドセキュリティのチェックを行う部署・担当の方
- クラウド利用を検討・推進している部署・担当の方
- クラウドサービスの企画、推進を行う方
- 情報システム部門のリーダー、担当者 など

クラウド環境を使い始めてしまっているが、どうやって使えば安心して利用できるか分からない。
何から手を付けて良いのか分からない...



今現在の利用状況や管理状況を見える化し、課題を浮かび上がらせることで、あるべき姿とのフィットギャップが分かります！

まずは現状を把握：簡単なチェックシートへの入力でリスクを見える化

ファーストステップとして取り組みやすい工夫が沢山：

クラウドに対する広範なチェック項目の中から、ベースラインとなるべき項目を厳選し、リスクの概況を明らかにする

安心

- ・ セキュリティ専門会社3社により、クラウドセキュリティのノウハウの集約
- ・ 実際のお客様の現場で活用・適用している知見を活用

使いやすい

- ・ ファーストステップとして取り組みやすく、ベースラインとなる項目を厳選
- ・ 単なるセキュリティ要件だけでなく、判断基準や詳細情報もご提供

対比できる

- ・ 自社のセキュリティ対策レベルと必要対策内容を把握可能（絶対評価）
- ・ 他社と比べて自社はどうか？ 偏差値のように相対的に把握可能（相対評価：予定）

ガイドライン

- ・ セキュリティ専門会社3社の知見を適用
 - ・ 国内・海外の複数ガイドラインを網羅的に組合わせ
- * 経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」
NIST SP 800-144「パブリッククラウドコンピューティングのセキュリティとプライバシーに関するガイドライン」
NIST SP 800-146「クラウドコンピューティングの概要と推奨事項」・ ISO/IEC 27017「ISMSクラウドセキュリティ認証」 など



最初の一步を踏み出しやすく

※注意：当クラウド共通評価フレームワークは各業界/固有のレギュレーションに準拠するものではありません。

⇒ 固有のレギュレーションに準拠させる際には、会員企業が提供している各種レギュレーション合わせた有償サービスもございます。

安心してクラウドを利活用するために基礎となる項目

レポート活用イメージ

- 
1. ビジネスリスクに関連するポイントはどこか？リスクアセスメントを行う
 2. 優先順位を付けながら、改善計画を策定し、実行する



① 経営への報告



② パートナー企業への共有



③ フィットギャップ改善

評価レポート

改善・実行に向けたサポート体制



CSIJ会員企業



有償でお困り事をサポート

例 1. 各業界のレギュレーションに準拠したい！



ご利用企業様

現状は分かったので
次はFISCに準拠したい！



会員企業が提供するコンサルサービス

おまかせください！

例 2. 詳細なアセスメントを伴走して欲しい！

これはマズそうだ！
アセスをアロの目で
手伝ってくれ！



ご利用企業様



会員企業が提供する
アセスメントサービス

かしこまりました！
しっかりやりましょう。



会員企業が提供する
コンサルサービス

例 3. 改善計画の策定をして欲しい！

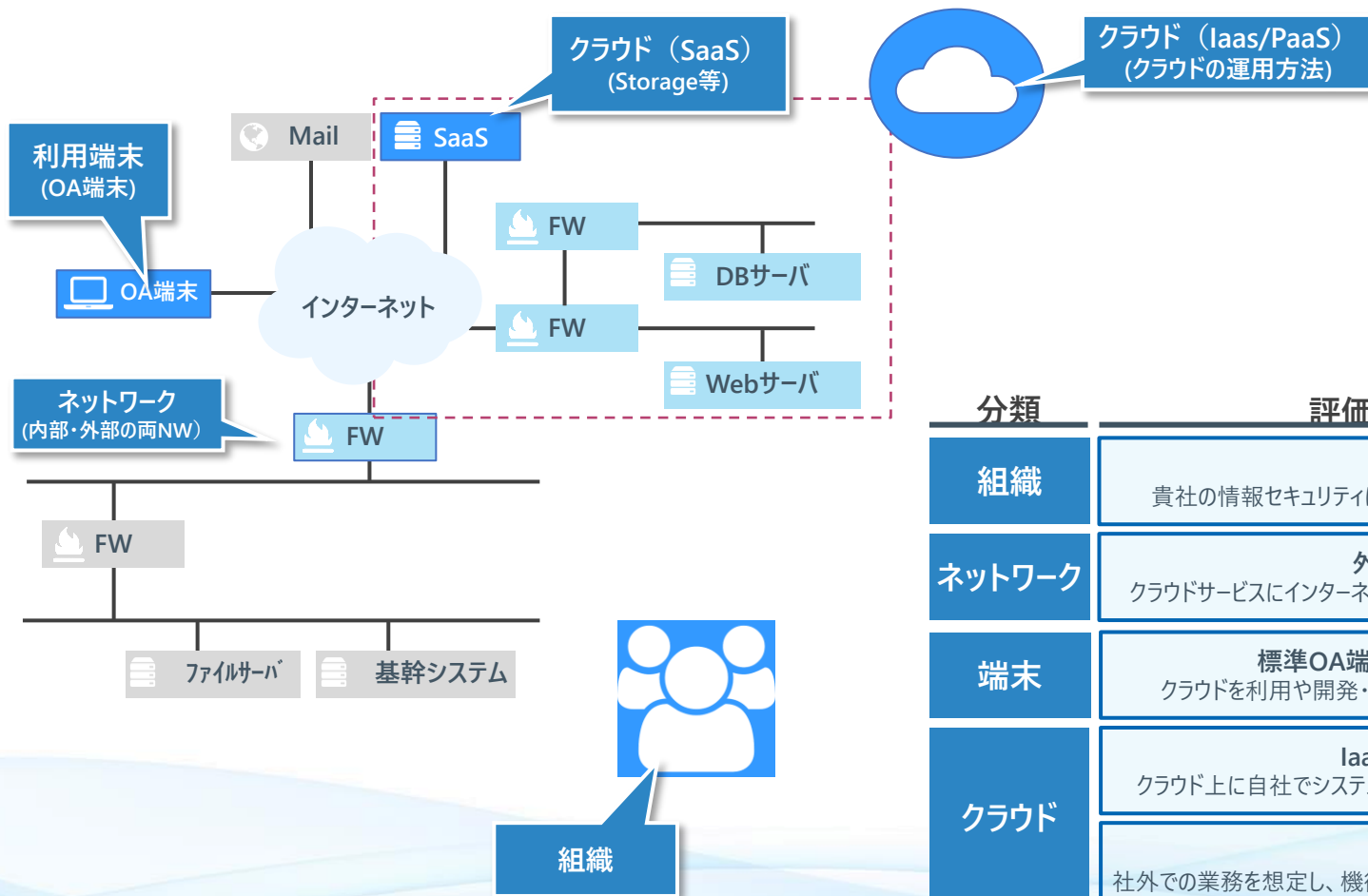
この結果を元に
ちゃんと改善を
進めて行きましょ



ご利用企業様

アロに見てもらって
安心できるね！

『IaaS/PaaS/SaaS』 『利用端末』 『経路ネットワーク』 『組織・マネジメント』



分類	評価対象
組織	組織 貴社の情報セキュリティに関する規定類・運用方針などを確認
ネットワーク	外部ネットワーク クラウドサービスにインターネット経由でアクセスするネットワークを想定
端末	標準OA端末（社内・社外利用） クラウドを利用や開発・保守管理を行う標準OA端末を想定
クラウド	IaaS/PaaSサービス クラウド上に自社でシステム開発・運用を実施している環境を想定
	SaaSサービス 社外での業務を想定し、機微情報を保有する等のSaaSサービスを想定

評価シートの全体像



■プロフィールシート

№	内容	確認事項	回答欄（確認欄）
1	クラウドサービスの名称	対象となるサービス、対象とされていないクラウドサービスの名称を記入してください。	クラウドサービス名称：【自由記述】
2	クラウドサービス提供事業者	クラウドサービスの提供事業者を記入してください。	クラウドサービス提供事業者名称：【自由記述】
3	URL	サービス紹介ページのURLを記入してください。	URL：【自由記述】
4	クラウドサービスの利用目的	クラウドサービスの利用目的を記入してください。	利用目的：【自由記述】
5	クラウドサービスの概要・主要機能	クラウドサービスの概要、主要機能を記入してください。 ※（任意） ・ファイル管理 ・顧客管理 など	概要：【自由記述】
6	クラウドサービス形態	サービスの形態について最も近いものを選択してください。 IaaS：ネットワークストレージ等の基本的なITコンポーネントを提供するサービス PaaS：開発者の開発するアプリケーションを実行できるようなプラットフォーム、サービス、OS/ストレージ層を提供するサービス SaaS：クラウドアプリケーションからWebブラウザを通じてネットワーク、サービス、OS、ストレージ、アプリケーションの構築を可能にするサービス その他：上記以外のIaaS・PaaS・SaaS（Cloud、PaaS等）	サービスの形態：【選択】

評価用アセスメント設問の構成：

・プロフィール：8設問

・本体

（Governance、Incident Response、Compliance、Technology & Operation）：42設問

Cyber Security Baseline Assessment for Cloud										※提出前に下記メッセージをご確認ください 必要な項目が入力されていません。		「プロフィールシート」で選択した「クラウドサービス形態」により、回答すべき項目が異なります。（対象外項目は選択に応じてグレーアウトされます）	
大項目 Name.	項目 Name.	No.	Cloud			確認事項	判断基準	評価	補足				
			IaaS	PaaS	SaaS								
							※対応済み（○）および未対応（×）を選択する基準が明示されています。 ※いずれにも該当しない場合には（△）を選択して下さい。						
Governance		1	○	○	○	クラウドサービス利用に関して、自社の利用規程や運営規程を整備していますか。	○……必要な規程類を整備し、適宜、更新を行っている。 ×……必要な規程類を整備していない。 利用に関する規程については、例えば以下のような項目を記載する。 ・取り扱い情報レベルの定義 ・利用する際のチェックシート及び、レビュープロセス、体制 ・責任分界点の考え方 ・管理体制 ・インシデント発生時のクラウドサービス提供会社との連絡網とフロー						
		2	○	○	○	クラウドサービス利用に関して、利用申請・承認フローを整備していますか。	○……全社で利用申請・承認フローが整備されており、管理されている。 ×……クラウドサービスの利用について特に管理されておらず、各部/各担当に任せている。						
		3	○	○	○	クラウドサービス提供事業者が提示するサービス利用における問い合わせ窓口・ヘルプデスクを把握し、連絡体制を整備していますか。	○……クラウドサービス提供事業者側の問い合わせ窓口、ヘルプデスクの連絡先、対応内容を把握し、何かあった際には、連絡/確認できるフローを定めている。 ×……クラウドサービス提供事業者側の問い合わせ窓口、ヘルプデスクの有無を把握していない。 クラウドサービス提供事業者側の問い合わせ窓口、ヘルプデスクについては、例えば以下のような項目を確認する。 ・連絡方法（ユーザ個別での問い合わせ可能、ユーザ側の窓口担当者のみ連絡可能など） ・連絡手段（メール、電話など） ・対応範囲（利用方法のみ、技術的なサポートなど） ・対応時間（24時間365日、平日9時～17時など）						
		4	○	○	○	クラウドサービス環境を管理する管理者・運用者・開発担当者に対し、クラウドサービスを利用する際の注意点や構築時の守るべきポイント（※）などを教育し、必要な場合に参照できるよう共有していますか。 （※）ドキュメント例 ・コーディング規約（使用しているプログラミング言語や開発環境に即したセキュリティ要素を含むもの） ・AWSの利用ガイドライン ・クラウドサービス利用時のセキュリティに関する注意点をまとめた資料	○……必要なセキュリティに関する注意事項、ルールを整備し、教育、周知している。 ×……必要なセキュリティに関する注意事項、ルールを整備しておらず、利用者に任せている。 クラウドサービスの利用にあたっては、利用者、管理者、クラウドサービスを利用してシステムを開発する場合は、システム開発者、システム運用者等複数の役割がある。それぞれの役割ごとに守るべきポイントが異なるため、それぞれの観点での教育が必要である。						

配布しておりますExcelファイルの各シートについて、以下に示す箇所の入力をお願いします。

シート名	入力事項
表紙	「記入日」をご記入ください。
更新履歴	※入力不要
プロフィールシート	評価対象とするクラウドサービスについて、「確認事項」に記載の内容に対する回答を「回答欄（確認欄）」に入力して下さい。
評価シート	評価対象とするクラウドサービスについて、各確認事項の「判断基準」欄の基準に従って◎・△・×の評価を行ってください。評価結果を「評価」欄に入力して下さい。回答内容に補足があれば「補足」欄に入力して下さい。
用語定義	※入力不要

IaaS,PaaS,SaaSのクラウド区分によって回答すべき項目が異なっています（○のついた項目が回答対象です）。
「プロフィールシート」の「クラウドサービス形態」の選択に応じて、不要項目がグレースアウトされます。

必須項目に入力がない、もしくは不要な項目に回答がされている場合に確認メッセージが表示されます。
評価シート提出前に念のためご確認ください。

Cyber Security Baseline Assessment for Cloud									
大項目 Name.	項目 Name.	No.	Cloud			確認事項	判断基準	評価	補足
			IaaS	PaaS	SaaS				
Governance		1	○	○	○	クラウドサービス利用に関して、自社の利用規程や運営規程を整備していますか。	◎……必要な規程類を整備し、適宜、更新を行っている。 ×……必要な規程類を整備していない。 利用に関する規程については、例えば以下のような項目を記載する。 ・取り扱い情報レベルの定義 ・利用する際のチェックシート及び、レビュープロセス、体制 ・責任分界点の考え方 ・管理体制 ・インシデント発生時のクラウドサービス提供会社との連絡網とフロー		
		2	○	○	○	クラウドサービス利用に関して、利用申請・承認フローを整備していますか。	◎……全社で利用申請・承認フローが整備されており、管理されている。 ×……クラウドサービスの利用について特に管理されておらず、各部/各担当に任せている。		

※ご回答頂いたデータは、CSIJにて統計データとして分析に使用します。 御社名は会員企業にも共有致しません。

評価結果の読み方

評価シートに入力して頂いた内容を元に、サマリレポートをご提供します。
レポートには以下の情報が含まれます。

Total

推奨される対策が全体でどの程度実施できているかを、パーセントで表示します。

レーダーチャート

各領域（Governance, Incident Response, Compliance, Posture Management, ID management, Data Protect）別の対策実施状況をレーダーチャートで示します。

領域別コメント

各領域別の対策実施状況について、サマリコメントを表示します。

評価領域

 Governance

 Incident Response

 Compliance

 Posture Management

 ID Management

 Data Protect

クラウドの利用に関するルールの整備や教育の実施など、利用の前提となるガバナンス整備状況

ログの取得やインシデント対応手順の整備等、インシデント発生時の対応準備状況

レギュレーションに沿ったデータ保存国やその他契約等のコンプライアンス面の確認状況

クラウドサービスに関する設定や脆弱性の管理状況

クラウドサービスに関する認証やアカウントに管理に関する整備状況

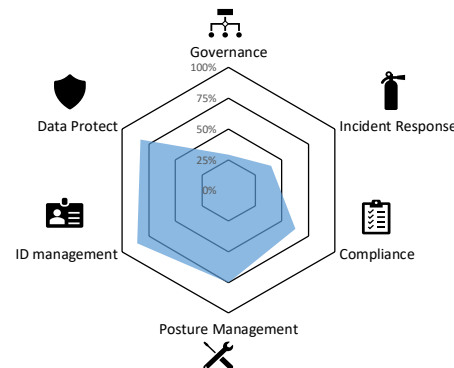
クラウドサービスに関するデータ保護や通信保護に関する対応状況

Cyber Security Baseline Assessment for Cloud

Summary report

Total
61%

Company name: NRIセキュリティ・ソリューションズ株式会社
Date: 2022/3/21



Governance
29%

現時点では対策が不十分です。
クラウドサービスの利用を管理するためには、基準となる規程・手順などが明文化され、実際に運用される必要があります。
必要に応じてセキュリティベンダーと連携し、手動での監視・検知・徹底的な取り締まりなどをお勧めします。

Incident Response
40%

現時点では対策が不十分です。
インシデント発生時の対応準備を整えるため、関連した手順・基準を整備するとともに、ログ取得・監視・アラートアップなどのインシデント対応を円滑に進めるための事前準備を実施する必要があります。
必要に応じてセキュリティベンダーなどと相談し、早急に関連する手続の整備や事前準備に取り組みられることをお勧めします。

Compliance
63%

現時点では一部対策が不十分な箇所があります。
クラウドサービスの利用に伴うリスクを適切に把握するためには、利用に先立ちデータが保管される国・地域や、クラウドサービス提供事業者の責任範囲などに関して確認し、合意する必要があります。
個別評価シートを参考に必要な情報の確認や合意をするための仕組みづくりに取り組みられることをお勧めします。

Posture Management
75%

現時点では一部対策が不十分な箇所があります。
クラウドサービスにおいても、自らが管理責任を負う範囲については脆弱性診断やセキュリティパッチ適用などの脆弱性対応を実施する必要があります。
個別評価シートを参考に脆弱性対応に取り組みられることをお勧めします。

ID management
86%

現時点では一定の対応が取られていると考えられます。
継続して対応を実施し、セキュリティ対策水準の維持に努めましょう。

Data Protect
83%

現時点では一定の対応が取られていると考えられます。
継続して対応を実施し、セキュリティ対策水準の維持に努めましょう。

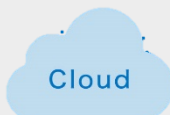
共通評価フレームワーク

【共通対策評価フレームワーク分科会】

第一弾

クラウド環境を利用しようと検討中の企業
クラウドを利用しているが、安全性に不安のある企業

- ・クラウドセキュリティのチェックを行う部署・担当の方
- ・クラウド利用を検討・推進している部署・担当の方
- ・クラウドサービスの企画、推進を行う方
- ・情報システム部門のリーダー、担当者 など



共通必要人材フレーム

【サイバーセキュリティプロフェッショナル人材フレームワーク分科会】

セキュリティ人材の正確な価値を見える化
優良なセキュリティ人材の健全な育成

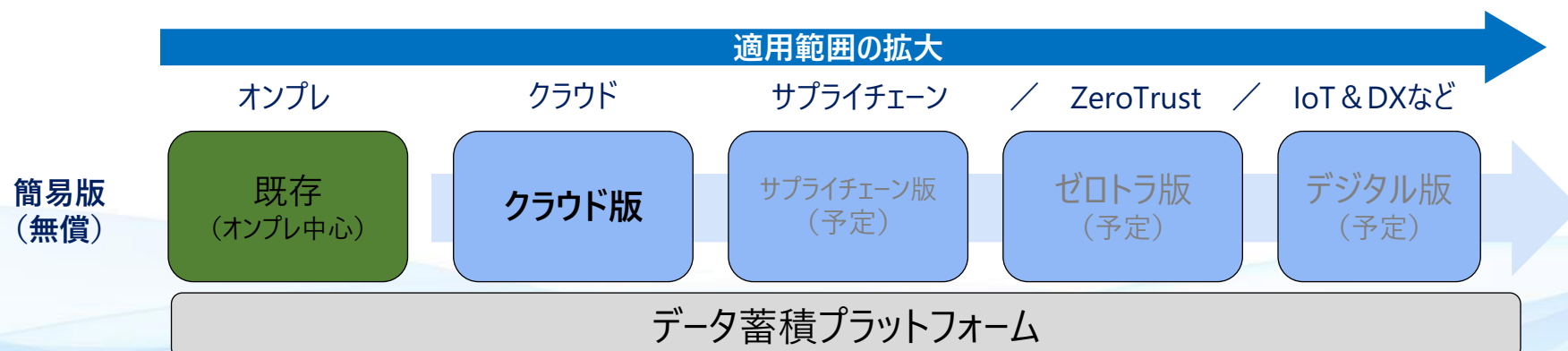
- ・セキュリティ人材の正確な価値を知りたい方
- ・優良な人材を所属する企業を選ぶ担当の方
- ・優良人材（特にエンジニア）になりたい、育成したい方
- ・人事部門長、セキュリティ人材育成担当者 など



今後も共通評価フレームワークは拡大していきます

適用範囲をクラウドからサプライチェーン・DXなどの環境変化・市場ニーズに合わせ拡大

お客様の現実的な実装に向けて、会員企業が用意する各ソリューションにて推進・支援してまいります。



Thank you. Any Questions ?



Cyber Security Initiative for Japan