



SUMMIT
ONLINE

JAPAN

大規模な組織変遷と100以上のAWSアカウントの 横断的セキュリティガードレール運用について

竹内 真 Shin Takeuchi

取締役CTO

ビジョナル株式会社

園田 剛史 Takeshi Sonoda

執行役員CIO

ビジョナル株式会社

| Agenda

- ビズリーチからVisionalへ、グループ経営体制への変遷（竹内）
- セキュリティーガードレールについて（園田）
- 今後のVisionalの展望とアマゾン ウェブ サービスへの期待（竹内）

自己紹介



ビジョナル株式会社 取締役 CTO

竹内 真

2001年、電気通信大学情報工学科を卒業後、富士ソフト株式会社に入社し、主に官公庁、大手通信会社向けシステム開発に従事。2007年、株式会社リクルートにて全社共通基盤フレームワーク開発などに従事し、同時にSeasarプロジェクト内でOSS活動も開始。2008年、株式会社レイハウオリを創業。その後、ビズリーチの創業準備期に参画し、取締役CTOに就任。2020年2月、現職に就任。社外活動として一般社団法人日本CTO協会理事を務める。

ビズリーチからVisionalへ、 グループ経営体制への変遷

VISIONAL 概要



設立 : 2020年2月（ビジョナル株式会社設立）

創業 : 2009年4月（株式会社ビズリーチ創業）

代表者 : ビジョナル株式会社 代表取締役社長 南 壮一郎

グループ従業員数 : 1,395名（2020年6月末時点）

資本金 : 45億3,898万円（資本準備金含む）

拠点 : 東京、大阪、名古屋、福岡

VISIONAL について

VISIONAL

新しい可能性を、次々と。

私たちは、インターネットの力で、時代がもたらす様々な課題を、
次々と新しい可能性（ビジョン）に変え、世の中の革新を支えていく。
「社会にインパクトを与え続ける」その志や事業のもとに
仲間が集まり、新しい仕組みやムーブメントを生み出すことで、
本気で実現したい未来へと加速させる。

グループについて

➤ VISIONAL

株式会社
ビズリーチ

HR Techの
プラットフォーム・
SaaS事業の運営

ビジョナル・
インキュベーション
株式会社

新規事業開発

株式会社
スタンバイ

求人検索エンジン
「スタンバイ」の運営

株式会社
BINAR

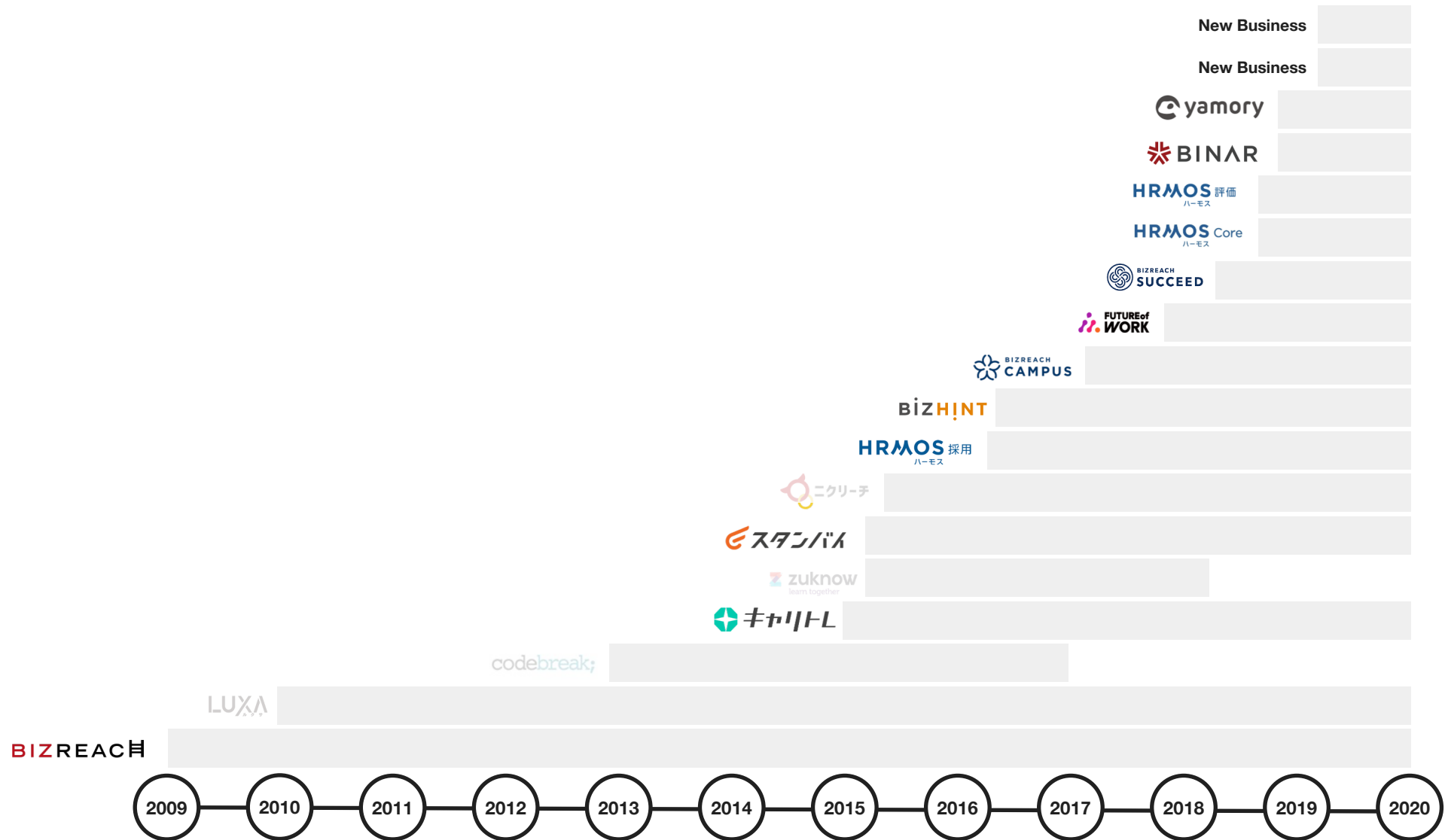
ハイスキル
ITエンジニア
転職プラットフォーム
「BINAR」の運営

トラボックス
株式会社

物流DX
プラットフォーム
「トラボックス」
の運営

ビジョナル株式会社（ホールディングカンパニー）

VISIONAL サービスの歴史



各社の運営事業・サービス（1）

株式会社ビズリーチ

即戦力人材と企業をつなぐ
転職サイト

BIZREACH 株式会社

挑戦する20代の転職サイト

 **キャリアL**

OB/OG訪問
ネットワークサービス

 **BIZREACH
CAMPUS**

採用管理クラウド

HRMOS 採用
ハーモス

従業員データベース

HRMOS CORE
ハーモス

人事評価クラウド

HRMOS 評価
ハーモス

各社の運営事業・サービス (2)

ビジョナル・インキュベーション株式会社

事業承継M&A
プラットフォーム



経営者・事業責任者の
ためのメディア



オープンソース
脆弱性管理ツール



未来の経営と働き方を
共創するカンファレンス



株式会社スタンバイ

求人検索エンジン



株式会社BINAR

ハイスキルITエンジニア
転職プラットフォーム



トラボックス株式会社

物流DXプラットフォーム



| コングロマリットな会社

複数の業種の事業を運営するコングロマリットな会社を目指している



ベンチャーとエンタープライズカンパニーの共存

エンタープライズの品質基準を満たしながら

ベンチャーのスピード感をもって事業運営を行なう組織

コングロマリットな会社として様々な事業の知見を一つに集め、世界から見ても高いセキュリティ品質、プロダクト品質のプロダクトをベンチャーのスピード感を持って生み出していく。

セキュリティガードレール

自己紹介



ビジョナル株式会社 執行役員 CIO

園田 剛史

2002年、芝浦工業大学システム工学部卒業後、富士フイルムソフトウェア株式会社に入社し、開発業務に従事。2004年より株式会社オプトで、法人向けWeb広告効果測定ツール等を開発。ビカム株式会社（現：株式会社メタップスワン）を経て、ビズリーチの創業準備期に参画し、執行役員に就任。ビズリーチや新規事業の開発責任者などを歴任し、2020年2月、現職に就任。

Visualnal

Visualnalは複数の事業を開発・運営

アマゾン ウェブ サービス(AWS)を利用し

100以上のAWSアカウントを運用しています

➤ VISIONAL

BIZREACH

即戦力人材と企業をつなぐ転職サイト

キャリアトル

挑戦する20代の転職サイト

スタンバム

求人検索エンジン

HRMOS 採用
ハーモス

採用管理クラウド

HRMOS CORE
ハーモス

従業員データベース

HRMOS 評価
ハーモス

人事評価クラウド

BIZREACH
CAMPUS

OB/OG訪問ネットワークサービス

BINAR

ハイスkillITエンジニア転職プラットフォーム

BIZREACH
SUCCEED

事業承継M&Aプラットフォーム

yamory

オープンソース脆弱性管理ツール

BIZHINT

経営者・事業責任者のためのメディア

Tr@Box トラボックス

物流DXプラットフォーム

複数事業・マルチアカウント運用で生まれた課題

- グループとしてのすべてのアカウントに一定以上の品質が求められる
- 次々立ち上がる新規事業などにも一定の以上の品質・セキュリティが求められる
- 各事業部の担当エンジニアのクラウド知見・AWS知見のばらつき
- 100以上のAWSアカウントに対する監査・統制を行なうための膨大な手間



**効率的に信頼性、セキュリティ、コンプライアンスなどの
設定不備や不正なアクティビティなどの情報収集の実施と
事業部門へのフィードバックを行い改善を促進する仕組みが必要に！**

門番からガードレールへ

課題

- 守るべき品質を横断部門が全アカウントに門番のようにチェックしていくのは非効率

仕組み化

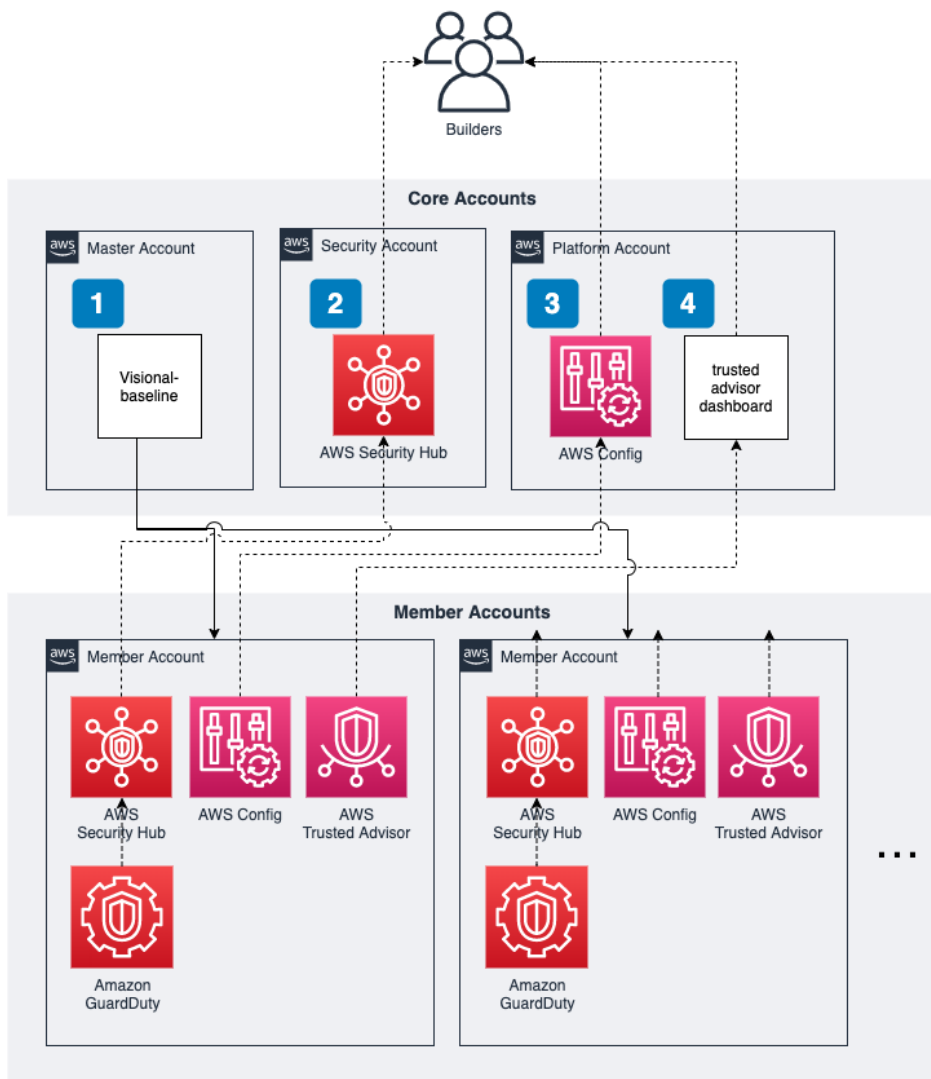
- 社内ルール・コンプライアンス（ガードレール）を定義しそれらが守られているかで評価
- 全AWSアカウントを評価し情報を集約・可視化し評価するシステムを構築、全社プロダクトの設定や運用での取りこぼしを検知しガードレールから外れたものは担当者へアラートイングすることで対応を促す

成果

- グループとしてのAWS運用の最低限の品質担保は横断組織が行え効率的に監視・統制が行える
- 事業部門は各事業に合わせた設定を行える体制を構築（ガードレール内なら自由に設定できる）
- 事業部側はあまり意識をせずにセキュリティ・ガバナンス・信頼性が担保され事業に注力できる

これらを[セキュリティガードレール](#)と名付け実施しています

4つのガードレール施策



1

Visional-baseline

Visionalの全AWSアカウントに対して、必要となる設定を適用するための仕組み。ベースラインとなる設定を一括管理し、意図した設定であることを定期的にチェックすることで必要な設定が守られていることを保証する。

2

AWS Security Hub

全てのAWSアカウントのAmazon GuardDutyの検知結果を集約して可視化する。重要度の高い検知に対しては通知を行うことで、発生した脅威を即座に検知して対応を取ることができる。

3

AWS Config

全てのAWSアカウントのルールチェック結果を集約する。チェックすべきルールを定義して、不適切な設定を検出して、通知/可視化して、非準拠へ対応を促すことで信頼性やセキュリティを担保する。

4

AWS Trusted Advisor Dashboard

全てのAWSアカウントのベストプラクティスに則ったチェック結果を集約・可視化する。セキュリティ、フォールトトレランスと、パフォーマンス、コスト等。チェック結果を通知することで対応を促す。

Core Accounts : 管理、ダッシュボードとして使うアカウント郡

Member Accounts : 事業部などで使うアカウント郡

Visual-onal-baseline

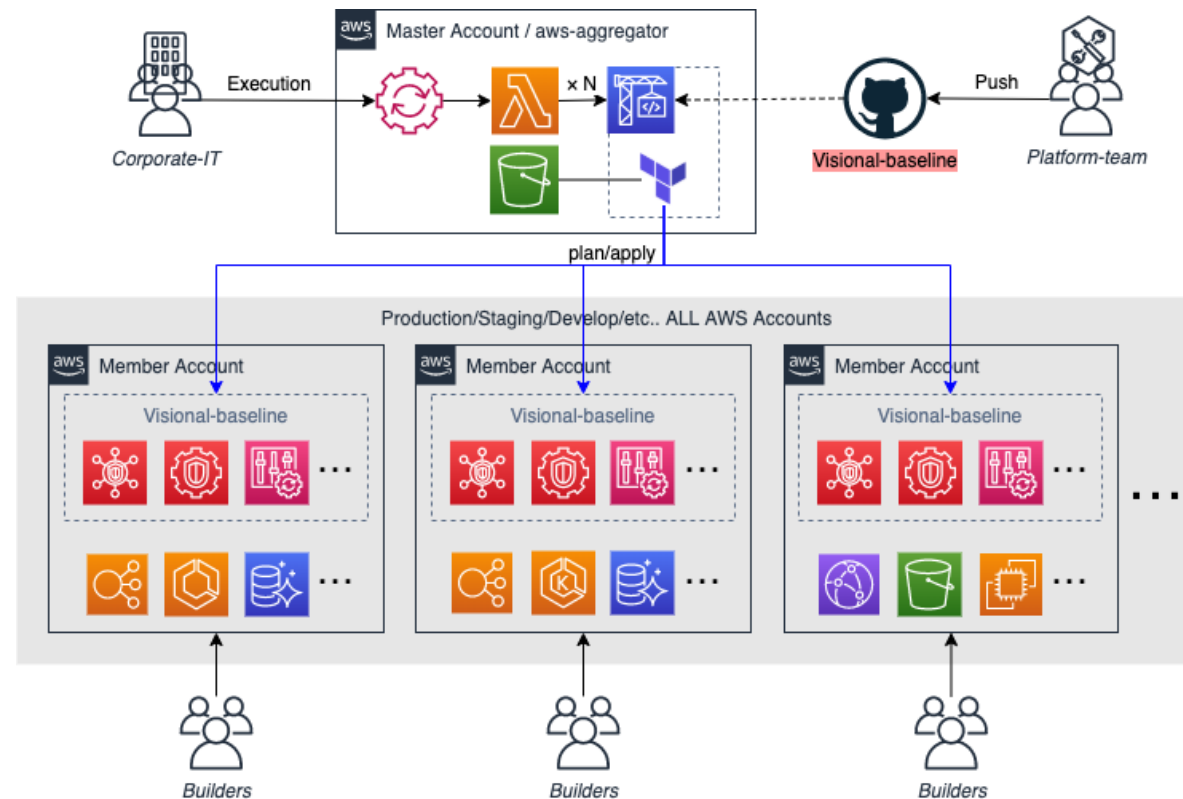
全AWSアカウントに対する共通設定反映

Visual-onalの全AWSアカウントに対して共通設定を管理適用するための仕組みとして構築。Terraformを活用して、グループで利用している全アカウント（全AWS・全リージョン）へ適用可能な仕組みを作成を実現。

100以上のAWSアカウントに一括で設定変更・構成管理を行なう事が可能になりました。

また、日次で共通設定と実環境の差分を確認することで、もし差分が検出された場合には通知して対処することで、常に共通設定が全体へ反映された状態を担保する仕組みとなっています。

➤ VISIONAL



Master Account
Visual-onal-baselineの実行環境

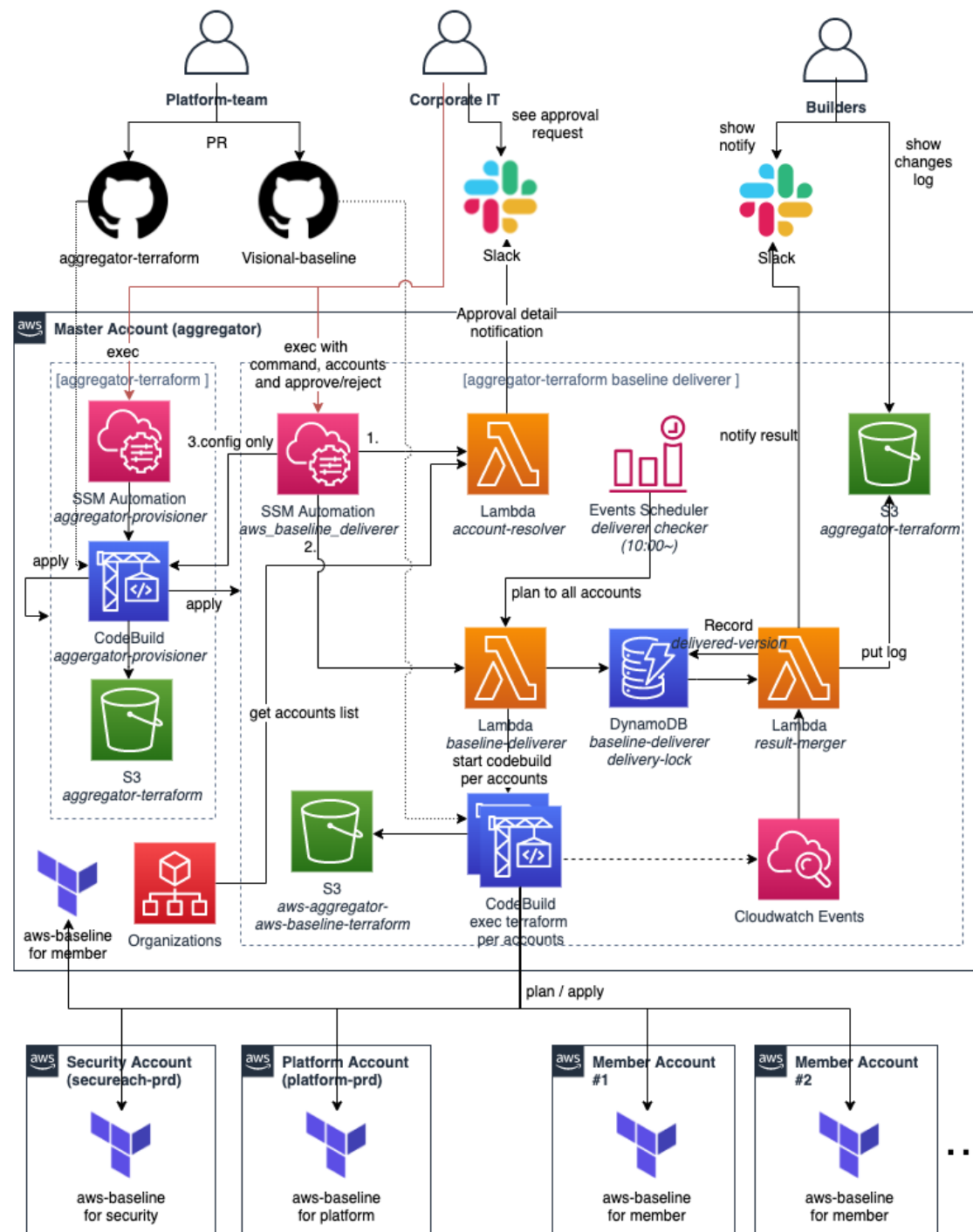
Member Account
事業部などで利用するアカウント

Platform-team
共通設定内容の定義を行なう部門

Corporate IT
適用作業を行なう部門

Builders
事業部門の開発組織

構成図



Master Account
Visual-baselineの実行環境

Member Account
事業部などで利用するアカウント

Platform-team
共通設定内容の定義を行なう部門

Corporate IT
適用作業を行なう部門

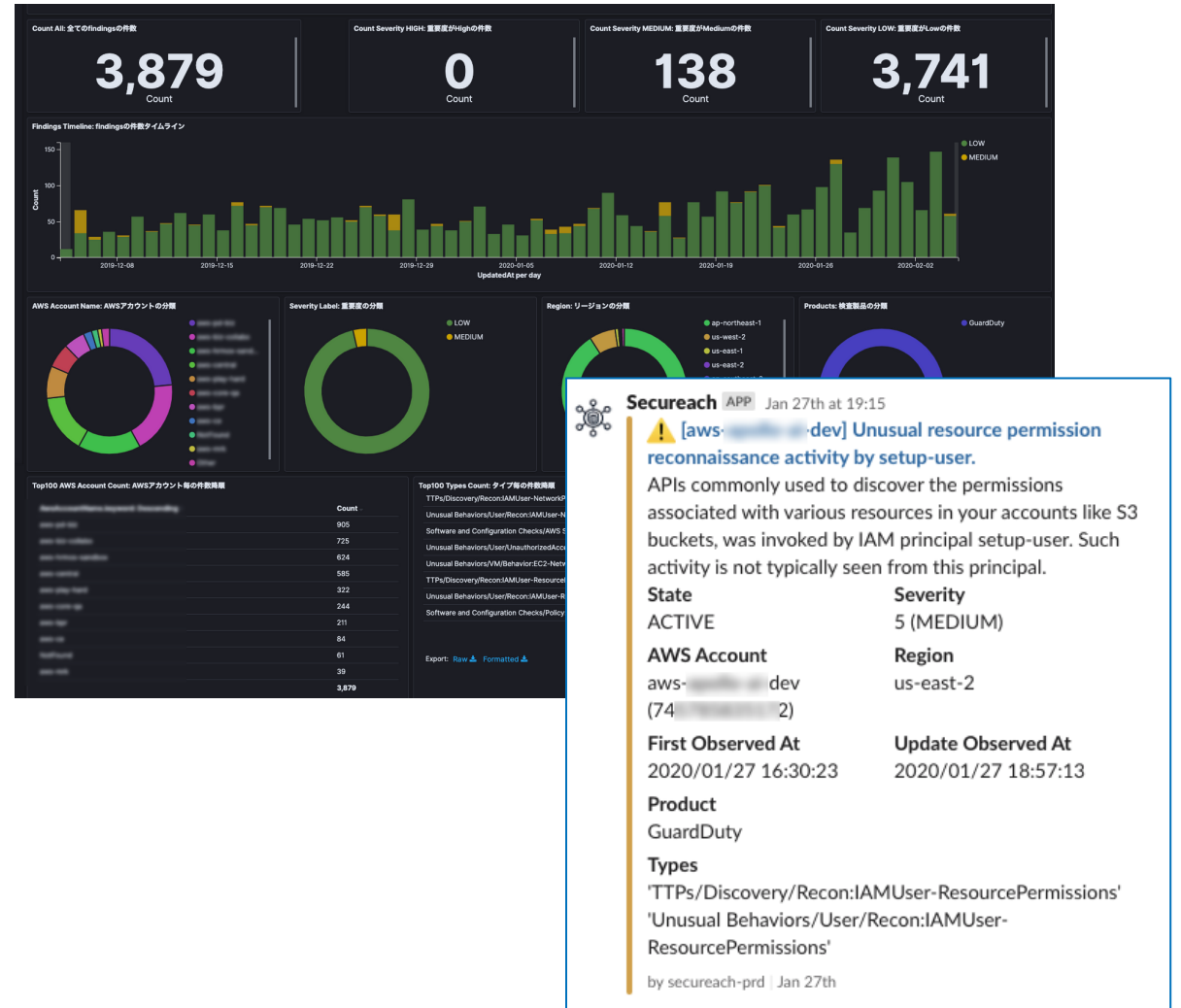
Builders
事業部門の開発組織

セキュリティ脅威情報の一元集約化と見える化

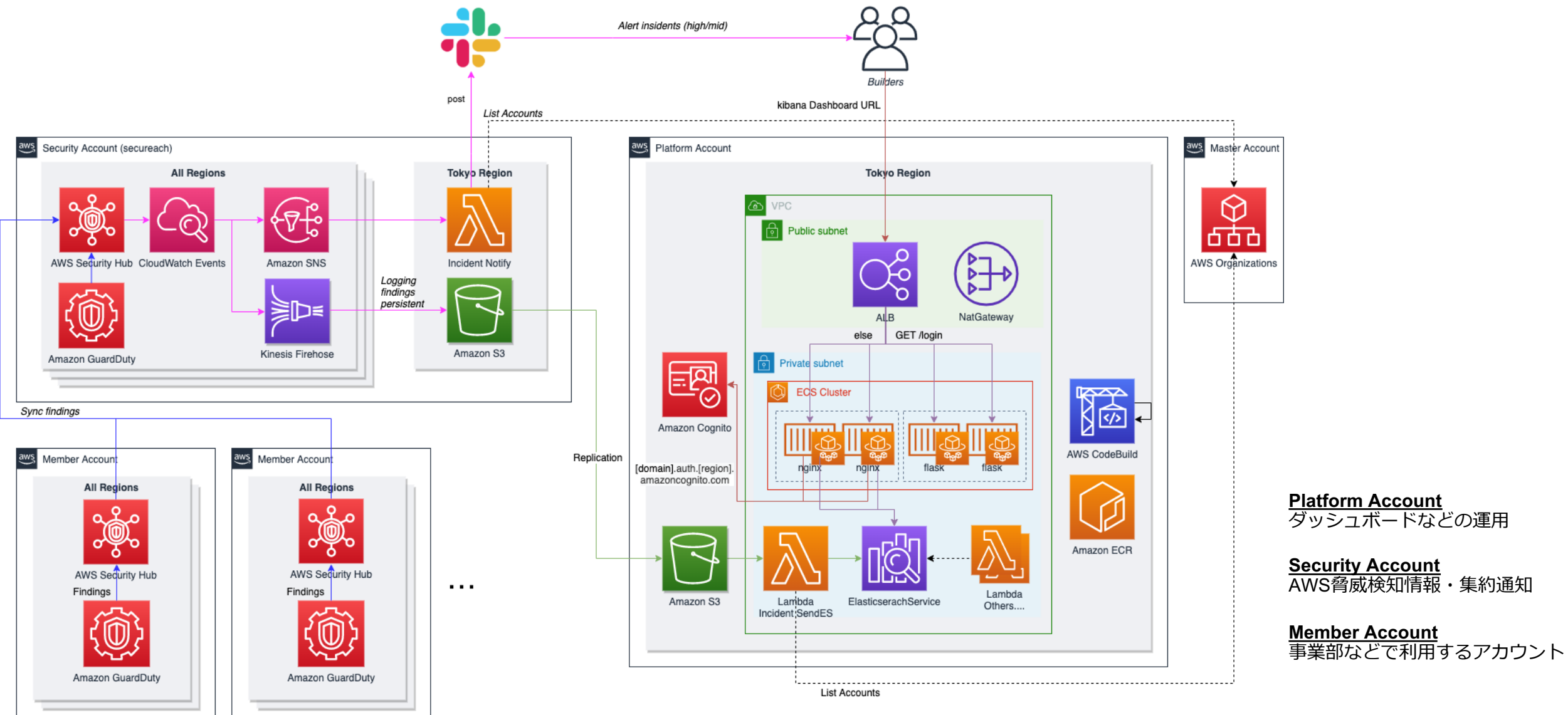
AWS Security Hubによる脅威検知と管理

全AWSアカウントのAmazon GuardDutyの検知結果をAWS Security Hubにて集約しダッシュボードにて可視化、Slackなどへの通知を行なう仕組みを構築。

迅速かつ一元で検知が可能になり弊社セキュリティ部門を含めた運用フローを確立し重要度に応じて事業部門への対応指示が可能になった。



AWS Security Hub - セキュリティ脅威検知-構成図



Platform Account
ダッシュボードなどの運用

Security Account
AWS脅威検知情報・集約通知

Member Account
事業部などで利用するアカウント

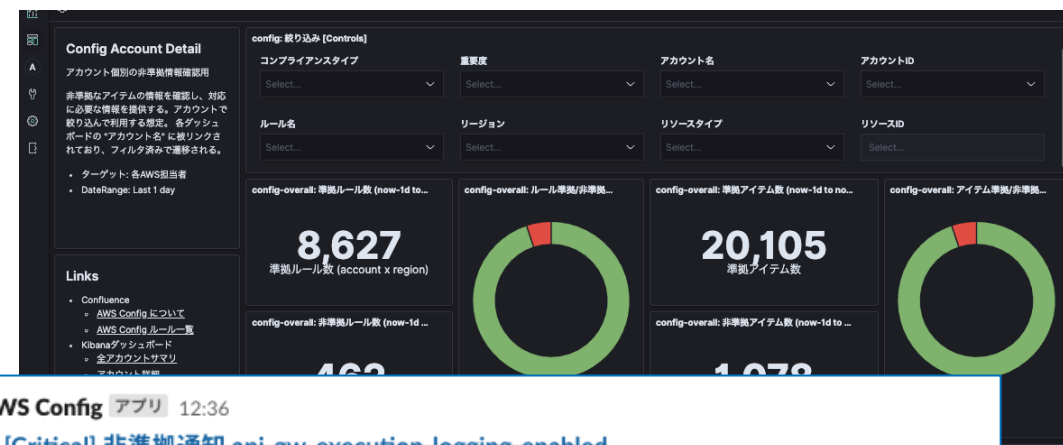
リソース設定がルールに合致しているかを確認

AWS Configによるコンプライアンス確認

AWS ConfigにてAWS リソースの設定や関連性及び変更内容を記録し、全社のAWSアカウントのリソースへ社内システム管理規定に対する準拠状況の評価を行う。評価結果を全社で集約して可視化し、非準拠リソースを検出時にはSlackなどで通知を行っている。

工数削減とともに、チェックの確実性も向上できている

またAWS設定ミスなどでセキュリティインシデントを招いてしまう可能性もあるが構成情報の変更点を横断組織で追跡してルールへの準拠を評価することで事業部門の担当者の負担をかけずに不適切な設定をリアルタイム検知が可能となった。



aws AWS Config アプリ 12:36

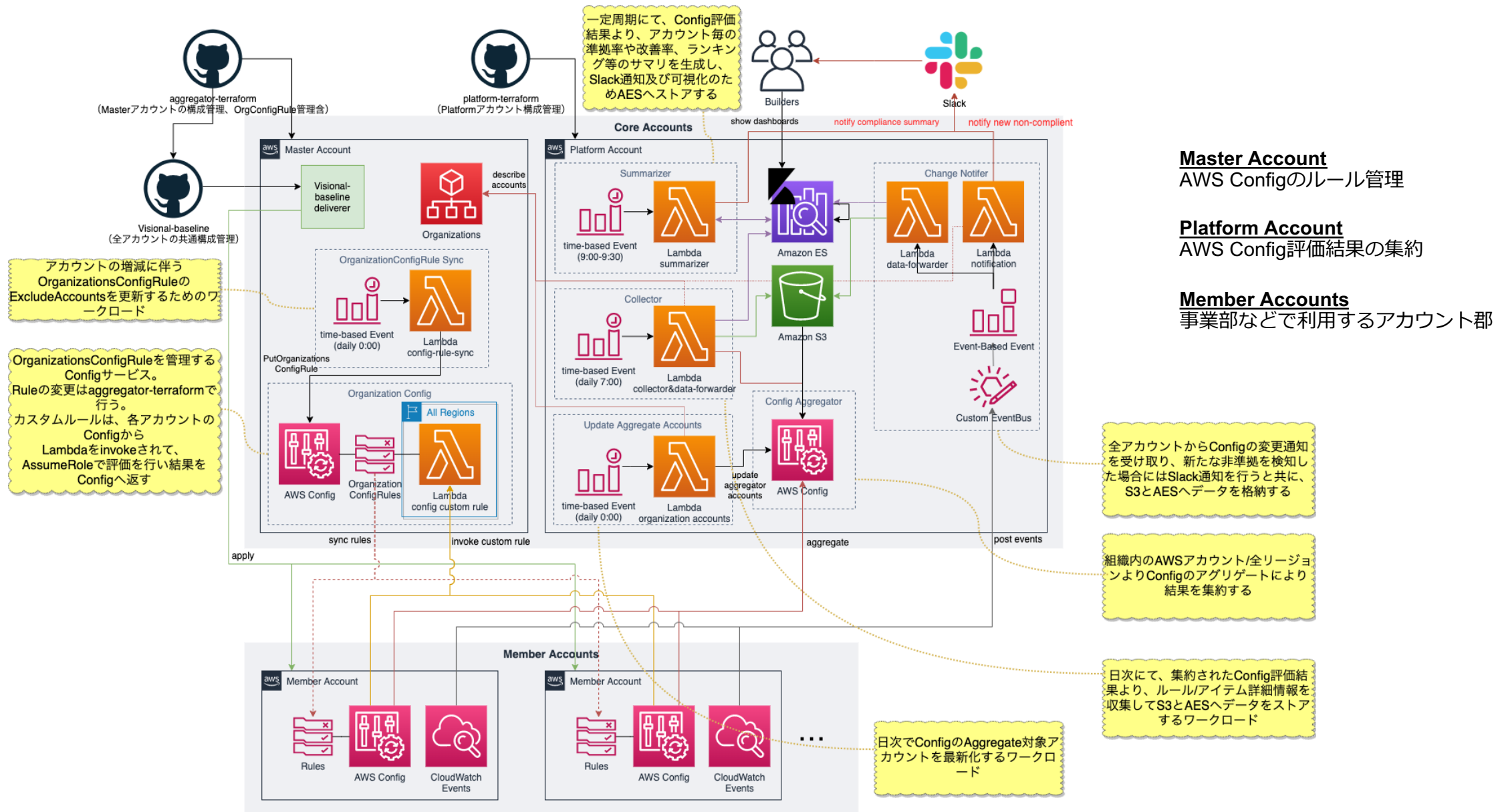
[Critical] 非準拠通知 api-gw-execution-logging-enabled

@aws-...-dev, @... ご確認ください。🔔

アカウント : aws-...-dev (65...01)
リージョン : ap-northeast-1
前回ステータス : なし (新規リソース)
リソースタイプ / ID : AWS::ApiGateway::Stage / arn:aws:apigateway:ap-northeast-1::/restapis/.../stages/test
注記 : Logging level is not configured for this Amazon API Gateway stage.

🔗 対象アカウントの非準拠検知ダッシュボードを開く (要社内LAN/VPN)

AWS Config 構成図



Master Account
AWS Configのルール管理

Platform Account
AWS Config評価結果の集約

Member Accounts
事業部などで利用するアカウント郡

組織横断でベストプラクティスに対する準拠状況を可視化

Trusted Advisor Dashboard

AWS Trusted Advisorはコスト、セキュリティ、パフォーマンスなどの観点でAWSのベストプラクティスに従っているかを確認してくれるツールです。この結果を全社で集約し一元管理するダッシュボードを作成しました、これにより全社の課題を一元的に把握でき事業部へ改善を促しやすくなりました。

結果全体でコストを約5%削減、セキュリティ箇所もダッシュボードで管理することで各事業の対応状況がわかるようになりました。

AWS Trusted Advisor Dashboard																	
Account		Result			Check			About									
Search: <input type="text"/>																	
AWS Account Id	AWS Account Name	Security			Fault Tolerance			Performance			Cost Optimizing			Service Limits			Status
		error	warn	ok	error	warn	ok	error	warn	ok	error	warn	ok	error	warn	ok	
0E-88	AWS-XXXXXXXXXX	0	1	16	0	14	15	0	0	10	0	0	8	0	0	50	check ok
0E-701	AWS-XXXXXXXXXX	0	8	15	0	26	15	0	0	10	0	0	8	0	0	50	check ok
10-26	AWS-XXXXXXXXXX	0	1	16	0	6	15	0	0	10	0	0	8	0	0	50	check ok
11-78	AWS-XXXXXXXXXX	0	1	16	0	16	15	0	0	10	0	0	8	0	0	50	check ok
14-29	AWS-XXXXXXXXXX	0	8	14	0	36	15	0	3	9	0	6	6	0	0	50	check ok
20-145	AWS-XXXXXXXXXX	0	2	15	0	8	15	0	0	10	0	0	8	0	0	50	check ok
21-95	AWS-XXXXXXXXXX	0	31	13	0	48	15	0	3	9	0	3	7	0	0	50	check ok
22-37	AWS-XXXXXXXXXX	0	2	15	0	12	15	0	0	10	0	0	8	0	0	50	check ok
22-597	AWS-XXXXXXXXXX	0	2	15	0	10	15	0	0	10	0	0	8	0	0	50	check ok
30-316	AWS-XXXXXXXXXX	0	8	15	0	20	15	0	0	10	0	0	8	0	0	50	check ok
33-41	AWS-XXXXXXXXXX	0	1	16	0	26	15	0	0	10	0	0	8	0	0	50	check ok
38-139	AWS-XXXXXXXXXX	0	7	15	0	12	15	0	0	10	0	0	8	0	0	50	check ok
47-164	AWS-XXXXXXXXXX	0	2	15	0	20	15	0	0	10	0	0	8	0	0	50	check ok
50-186	AWS-XXXXXXXXXX	0	0	17	0	10	15	0	0	10	0	0	8	0	0	50	check ok

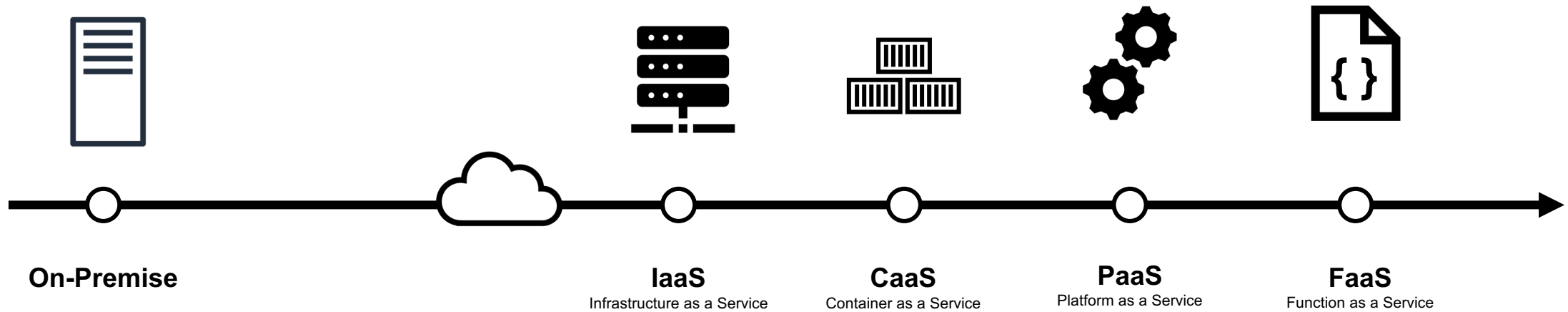
開発スピードを落とさず、一定の品質を守る

弊社ではAWSから提供されている、AWS Organizationsやマルチアカウントなどの機能をVISIONAL向けにカスタマイズし設定の一括反映や情報を集約する仕組みをつくることで、開発者の手を煩わせず効率的に監査・統制が行える仕組み**セキュリティ・ガードレール**を構築しました。これにより開発スピードを落とさず品質を担保する環境を実現しています。

また本件実現のためにAWSアカウントチームの支援、具体的にはエンタープライズサポート定例やコスト削減提案やオフィスアワーなど多大なるご協力を頂いております。今後もビジネスパートナーとして協力をお願いしたいと考えております。

今後のVisionalの展望と アマゾン ウェブ サービスへの期待

インフラ環境の進化



Thank you!