



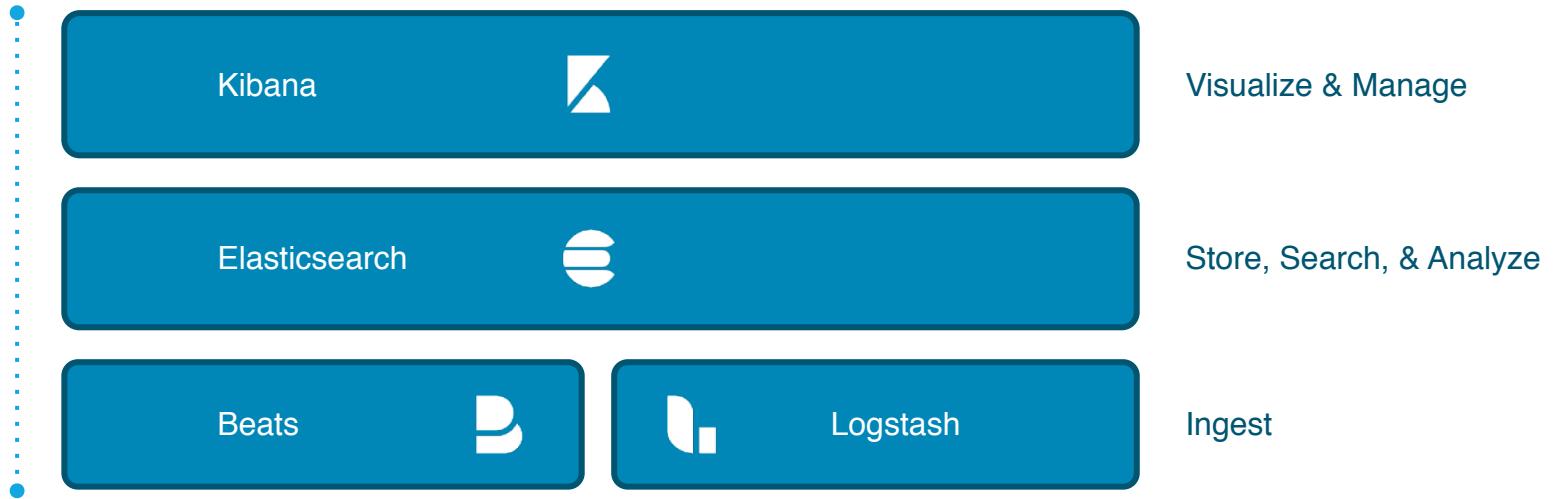
Kosho Owa
Principal Solutions Architect, Elastic

Elastic Stackのセキュリティ: データを安全に保つための ベストプラクティス

製品の概要



Elastic Stack

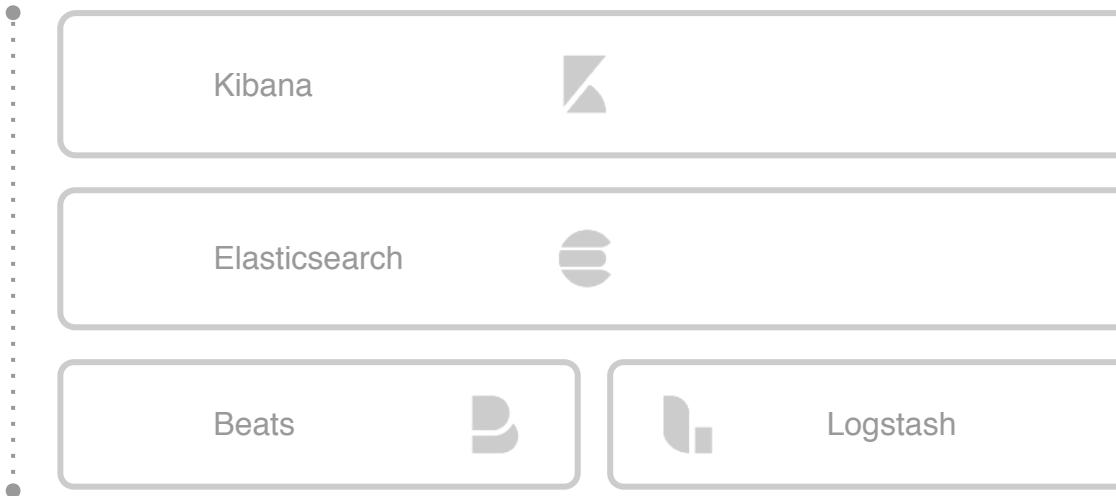




Elastic Stack

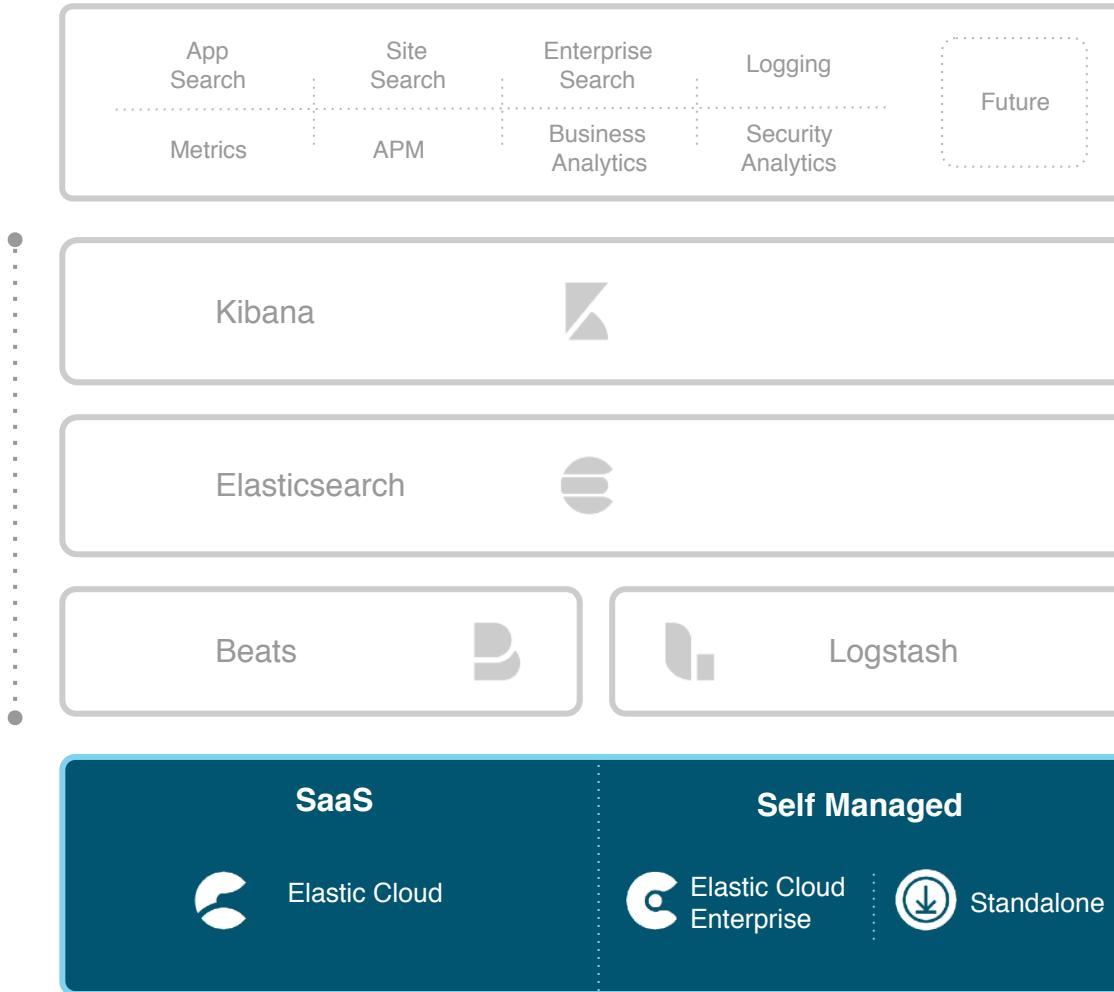


Solutions





Elastic Stack



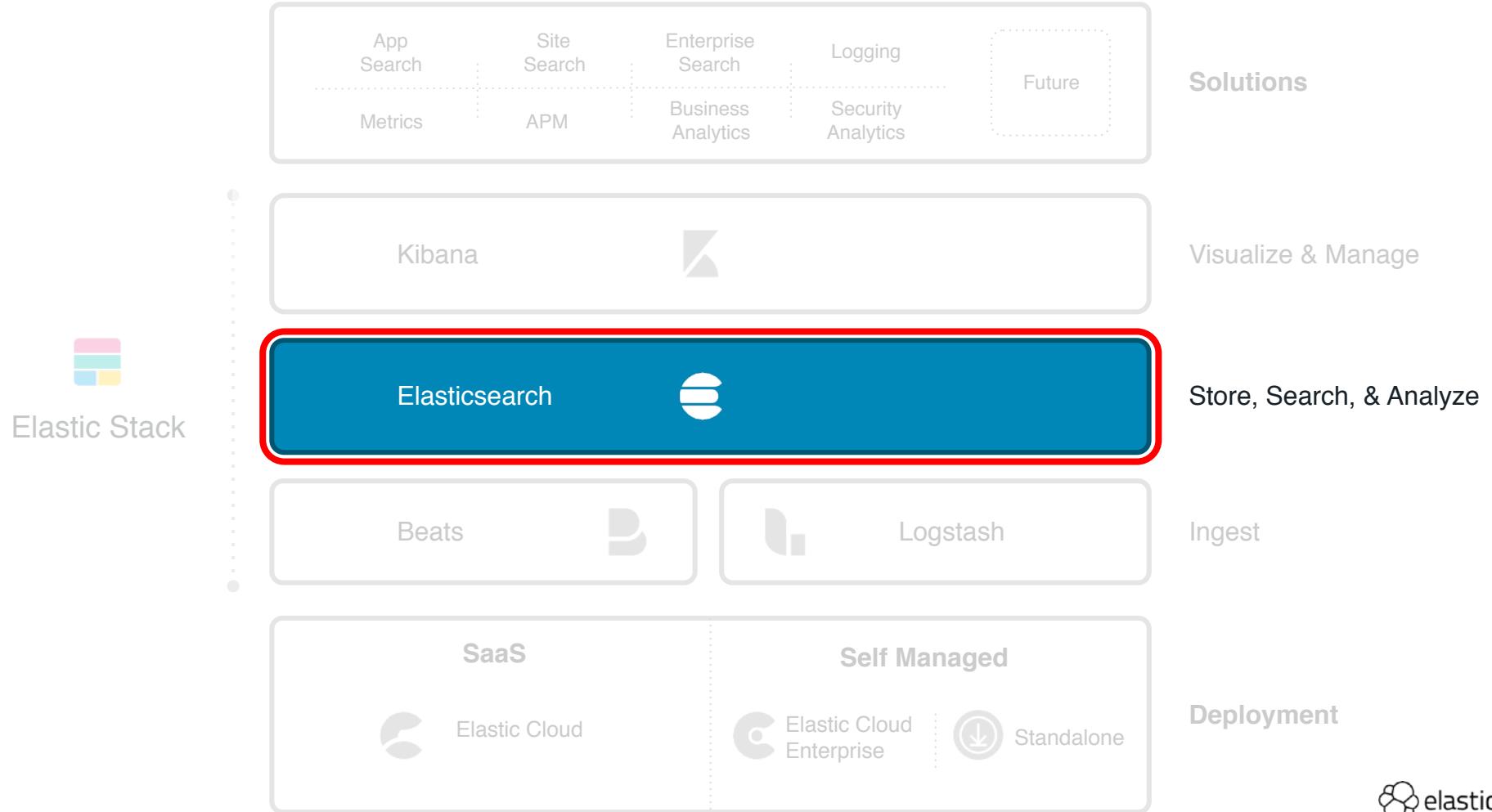
Solutions

Visualize & Manage

Store, Search, & Analyze

Ingest

Deployment



製品間の相互作用

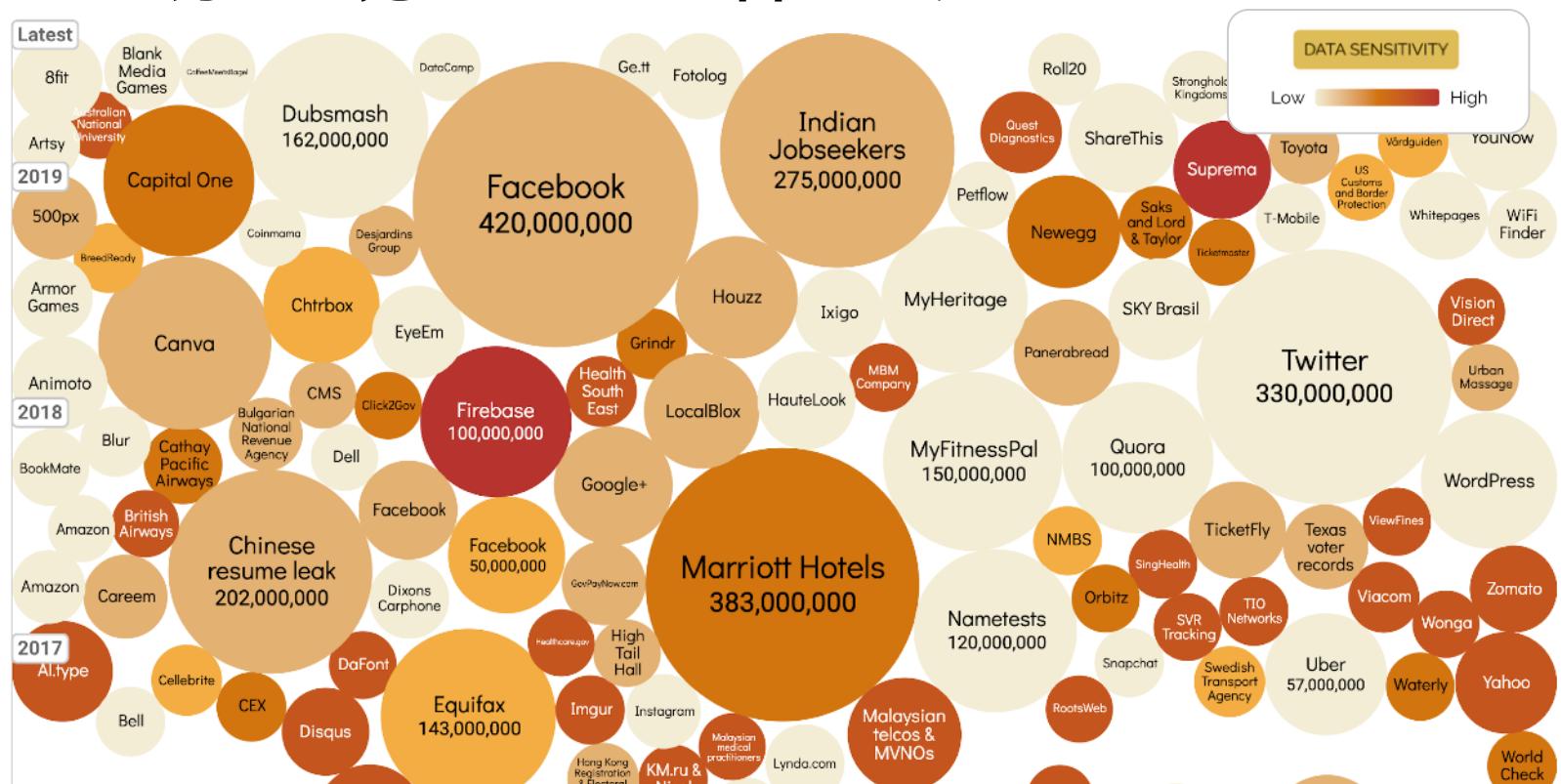
データがすべて！

Elasticsearchは、大量データにまつわる様々な問題解決のために利用できる。

"世界で最も価値がある資源はもはや石油ではない。データである。"
(エコノミスト誌)

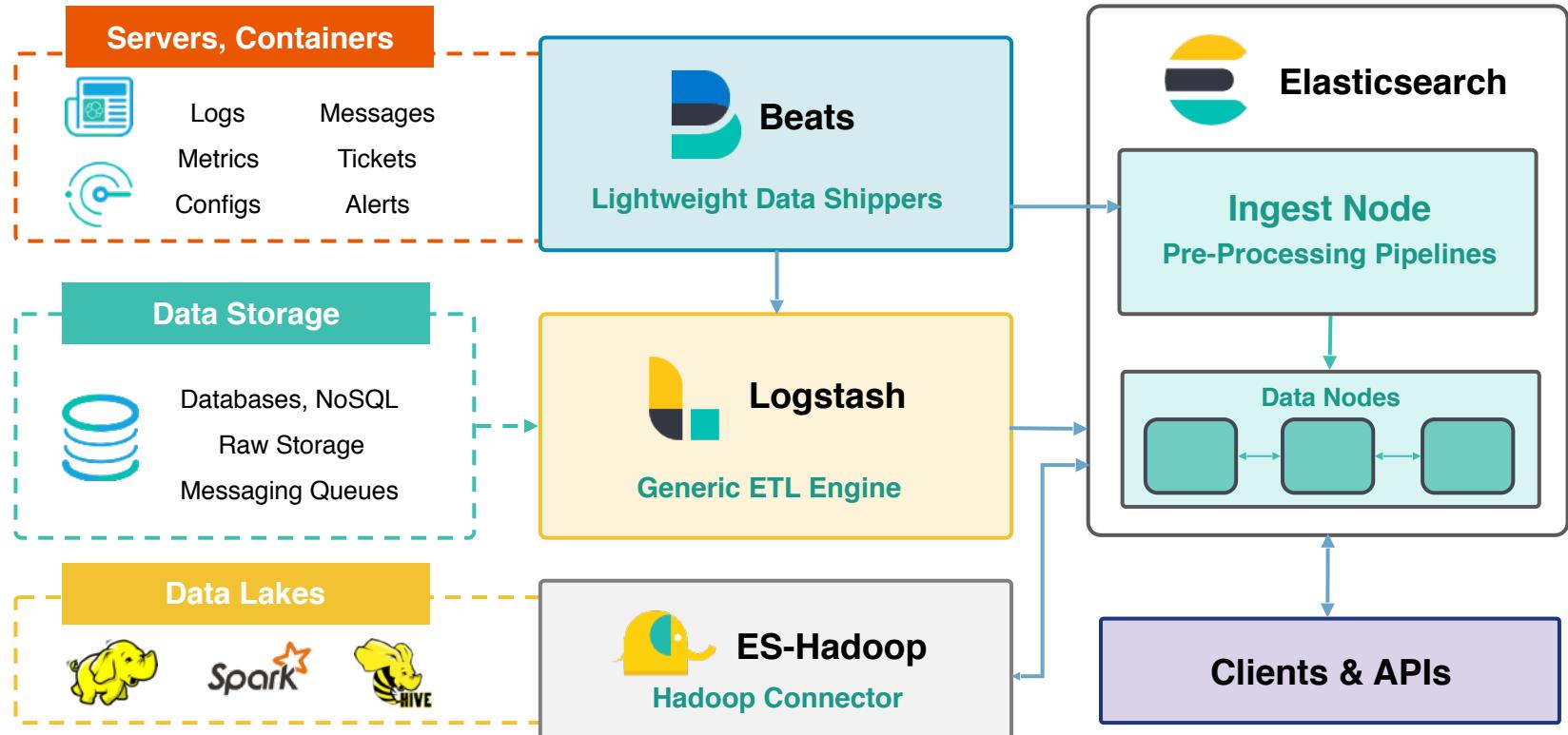
- データには、個人情報、知財、企業秘密などが含まれる
- データには限られた数の人々が、限られた目的のためにアクセスできるべきである
- データ漏洩と侵害は受け入れられず、復旧不可能な大きな損害をもたらすことがある

あなたの身には発生しないと言えますか？



<https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

Elasticsearchとの関連性マップ



どのようにしたら防ぐことができるか？



“これら三つの中で、ひとつか二つ
実装すれば十分でしょうか？”

—

“もしも...”

...暗号化しなかったら？

攻撃者は、クライアントとサーバー間の通信を盗聴し、有効な資格情報を取得して、実際のユーザーになりますことができます。

...認証しなかったら？

攻撃者は、システムのどのようなユーザーにもなりすますことができます。

...認可しかなったら？

攻撃者は低い権限の資格情報を取得し、このアクセスを利用してクラスター全体とそのデータを完全に制御できます。

セキュリティ機能

お楽しみはここから！

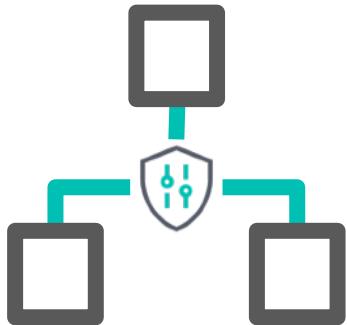
セキュリティ機能は、デフォルトの提供パッケージに含まれている

Elasticsearch 6.8と7.1から、ベーシックライセンス（無料）で基本機能が利用できる

追加機能は、ゴールド、プラチナ、エンタープライズライセンスで提供される

有効にするには、以下の設定をelasticsearch.ymlに記載

```
xpack.security.enabled: true
```



暗号化

Protect network connections.
Guarantee confidentiality.
Trust no one.

トランSPORT・レイヤー・セキュリティとは

Transport Layer Security (TLS) は、一般にSSLとも呼ばれ、ネットワーク接続でデータをカプセル化する暗号化プロトコルです。

TLSの3つの主な特徴は次のとおり：

- ✓ **プライバシー:** データは送信元を離れる前に暗号化され、送信先でのみ復号化されるため、ネットワークトラフィックを見て、情報を収集することはできない
- ✓ **認証:** 公開鍵は、宛先が本人であることを保証し、中間者攻撃やその他のテクニックから守る
- ✓ **信頼性:** 通信が改ざんされた場合、整合性チェックによって検出され、無効なコンテンツを拒否し、不正な第三者による外部からの操作を防止する

どうして友達になれないの？

Elasticsearchは、主にデータにインデックスを付け、クエリに応答するように設計されている。クライアントとの対話は、HTTPプロトコルに基づいたREST APIエンドポイントを使用してネットワーク上で行われる。

HTTPSを有効にするには、elasticsearch.ymlに次の設定を追加する。

```
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.keystore.path: certs/elastic-certificates.p12
xpack.security.http.ssl.truststore.path: certs/elastic-certificates.p12
```

Elasticsearchセキュリティが有効になっている場合、TLSは透過的に要求と応答をラップするために使用され、HTTPをHTTPSに変換する。すべてのクライアント（Logstash、Kibanaなど）は、暗号化通信を使用する必要があり。

誰も信用しない

自分のネットワークでElasticsearchを実行している場合でも、内部で発生する可能性のある脅威に注意する必要がある。 現代のアーキテクチャは、分散・隔離を前提としていて、ファイアウォールの内側にあり、誰も信頼することができない。

TLSを有効にするには、elasticsearch.ymlに次の設定を追加する。

```
xpack.security.transport.ssl.enabled: true
xpack.security.transport.ssl.keystore.path: certs/elastic-certificates.p12
xpack.security.transport.ssl.truststore.path: certs/elastic-certificates.p12
```

これをゼロトラストと呼ぶ。内部通信を含め、すべての通信を保護する必要がある。Elasticsearchノードは、専用ポートを使用して独自のプロトコルで通信する。適切なセキュリティがなければ、誰でも正当なノードとしてクラスタに参加できる。

足りないですか？

HTTPまたはトランSPORT通信で使用できるその他の便利な設定があり：

***.ssl.supported_protocols:** ネゴシエーションに使用するプロトコル群を定義する

***.ssl.cipher_suites:** 特定の暗号化アルゴリズムのみ使用を許可する

***.ssl.verification_mode:** 証明書の有効性を確認する

キーと証明書を含むファイルがパスワードで保護されている場合、`elasticsearch-keystore`コマンドを使用して、構成ファイルで設定した各キーストアとトラストストアに`*.secure_password`設定を追加する



認証

Always ask who is at the door.
Recognize good friends.
Invite only party.

あなたは誰？

Elasticsearchは、REST APIを介してすべての機能を公開する。データのインデックス、クエリの実行、クラスターの管理など。

セキュリティが有効になっている場合、呼び出し元が正当なユーザーであるかどうかを確認するために、レルムと呼ばれる認証サービスによって各要求が検証される。

ベーシックサブスクリプションは次のレルムを含む:

ネイティブ: ユーザーは専用のElasticsearchインデックスに保存され、Users APIを使用して管理される

ファイル: ユーザーはElasticsearchクラスターの各ノードに保存されているファイルで定義され、`elasticsearch-users`ツールによって管理される

予約済み: システムのセットアップと動作に必要なビルトインユーザー

REST API 認証

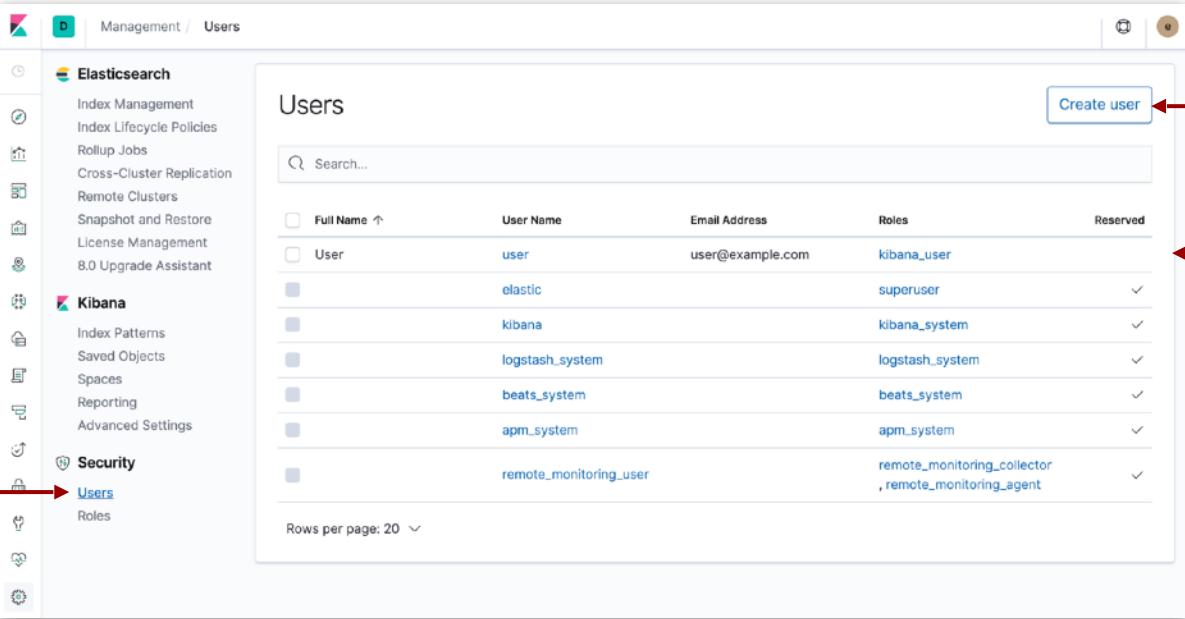
- Elasticsearchでは、各API呼び出しが認証される必要がある（ステートレス）
- Authorizationヘッダーで、サーバーにユーザー名とパスワードを送信する（エンコード）

```
GET /_search HTTP/1.1
Authorization: Basic ZWxhc3RpYzpZZWNyZXlwYXNz
...
```

- レスポンスコードが **401 Unauthorized** の場合、
 - ユーザーが存在しない
 - パスワードが誤り
 - クレデンシャルが無い

Kibanaで簡単に！

ネイティブと予約済みユーザーは、Kibanaの管理アプリケーションを使用して管理することもできる（少なくとも`manage_security`権限が必要）。



The screenshot shows the Kibana Management interface for user management. The left sidebar includes links for Elasticsearch (Index Management, Index Lifecycle Policies, Rollup Jobs, Cross-Cluster Replication, Remote Clusters, Snapshot and Restore, License Management, 8.0 Upgrade Assistant), Kibana (Index Patterns, Saved Objects, Spaces, Reporting, Advanced Settings), and Security (Users, Roles). The main area is titled 'Users' and displays a table with columns: Full Name, User Name, Email Address, Roles, and Reserved. The table lists several users: 'user' (user@example.com, roles: kibana_user), 'elastic' (superuser), 'kibana' (kibana_system), 'logstash_system' (logstash_system), 'beats_system' (beats_system), 'apm_system' (apm_system), and 'remote_monitoring_user' (roles: remote_monitoring_collector, remote_monitoring_agent). A 'Create user' button is at the top right, and a 'Search...' input field is present. Red callout boxes with numbers 1 through 4 highlight specific features: 1 points to the 'Management' link in the sidebar; 2 points to the 'Users' link in the sidebar; 3 points to the 'Add new' button; and 4 points to the 'Edit' button next to the 'Create user' button.

Full Name	User Name	Email Address	Roles	Reserved
User	user	user@example.com	kibana_user	
	elastic		superuser	✓
	kibana		kibana_system	✓
	logstash_system		logstash_system	✓
	beats_system		beats_system	✓
	apm_system		apm_system	✓
	remote_monitoring_user		remote_monitoring_collector, remote_monitoring_agent	✓

API キー

元のユーザーが持っている権限の限られたサブセットで呼び出しを許可するために、長期の資格情報が必要な場合がある

APIキーの例：

```
{  
  "id": "VuaCfGcBCdbkQm-e5a0x",  
  "name": "my-api-key",  
  "expiration": 1577750400000,  
  "api_key": "ui2lp2axTNmsyakw9tvNnw"  
}
```

← the "username" of the key
← a custom name to recognize it
← optional expiration timestamp
← the "password" of the key

APIキーで以下のように認証できる

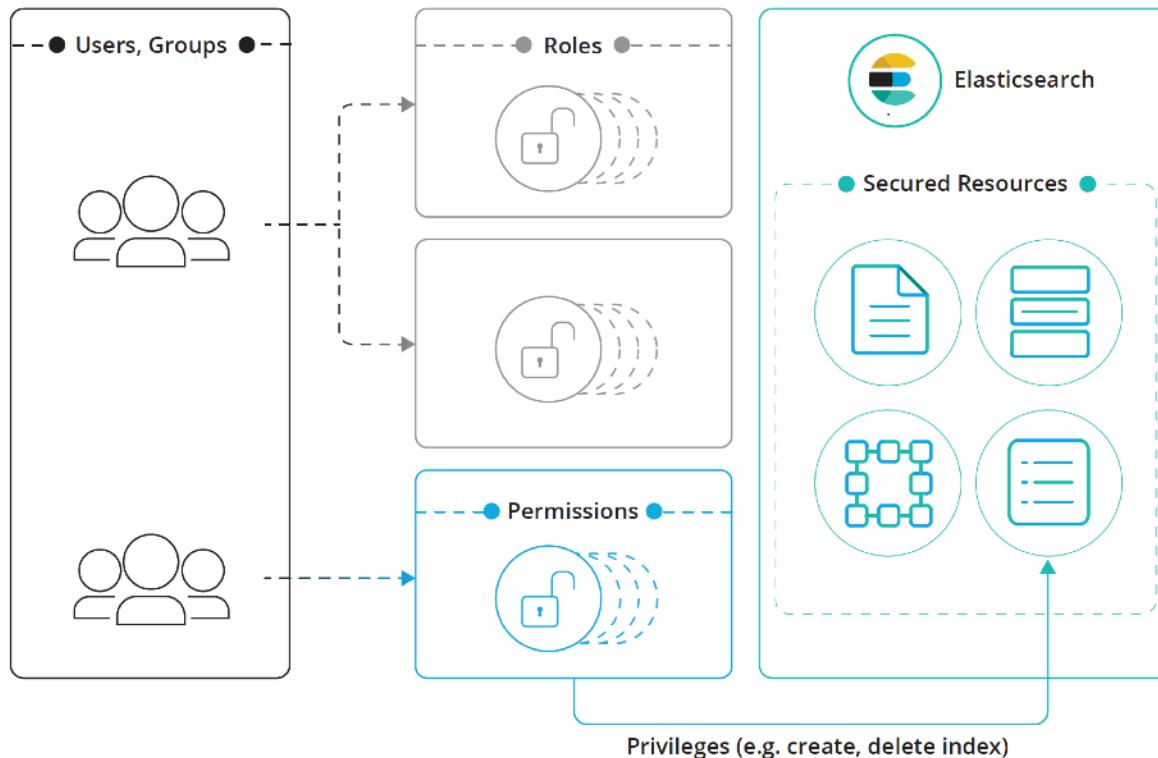
```
GET /_search HTTP/1.1  
Authorization: ApiKey VnVhQ2ZH0JDZGJrUW0tZTVhT3g6dWkybHAyYXhUTm1zeWFrdz10dk5udw==  
...
```



認可

Make users who they are.
Everyone is different.
Say no when it is no.

Role-based access control



ロールと権限

ユーザーには複数の役割がある。 ロールには複数の権限がある。

権限は、次のカテゴリにグループ化できる：

- **クラスター権限:** クラスター構成、セキュリティ、ML、スナップショットなどへの読み取りおよび書き込み
- **インデックス権限:** パターンに基づく、インデックスの作成、検索、ライフサイクルに及ぼす管理のポリシー
- **Run as 権限:** 他のユーザーに代わって特権を使用してリクエストを実行する
- **アプリケーション権限:** アプリケーションがElasticsearchロール内で独自の権限モデルを表現および保存できるようにする

やっぱり Kibana !

The screenshot shows the Elasticsearch Management UI with the path `Management / Users / Create`. On the left, a sidebar lists various Kibana and Security-related options. The main content area is titled "Elasticsearch" and "Cluster privileges". It allows managing actions against the cluster, with the current privileges set to "monitor", "manage_index_templates", and "manage_llm". The "Run As privileges" section shows "user" selected. The "Index privileges" section allows controlling access to data in the cluster. It shows two "Indices" sections: "date-*" and "logs-*", each with a "Privileges" dropdown menu. The "Privileges" menu lists "read", "all", "manage", "monitor", "index", "create", "delete", and "write". A "Add index privilege" button is at the bottom.

Kibana

- Index Patterns
- Saved Objects
- Spaces
- Reporting
- Advanced Settings

Security

- Users
- Roles

Elasticsearch

Cluster privileges

Manage the actions this role can perform against your cluster. [Learn more](#)

monitor × manage_index_templates × manage_llm ×

Run As privileges

Allow requests to be submitted on the behalf of other users. [Learn more](#)

user ×

Index privileges

Control access to the data in your cluster. [Learn more](#)

Indices

date-* ×

Privileges

read × |

- all
- manage
- monitor
- index
- create
- delete
- write

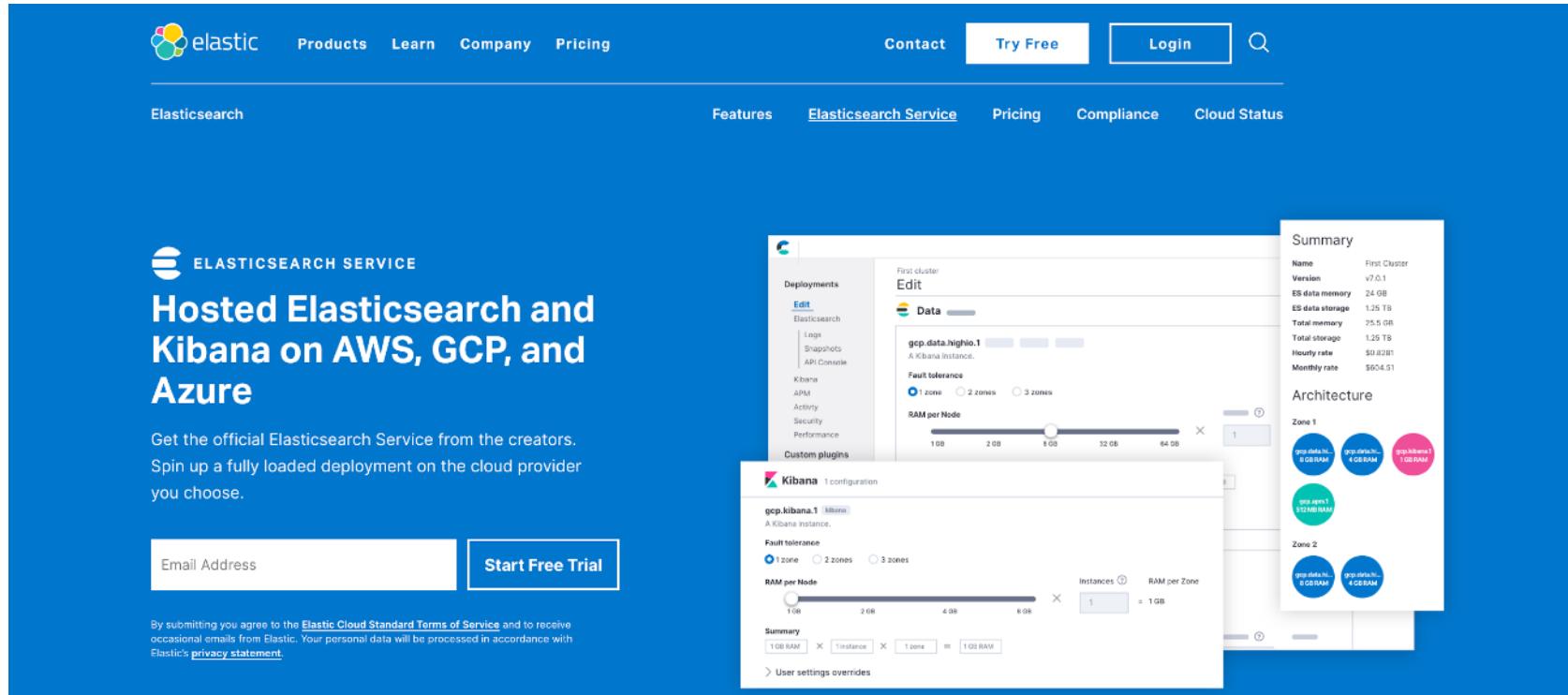
Indices

logs-* ×

Add index privilege

そのほかのリソース

Elasticsearch Service on cloud



The image shows a screenshot of the Elasticsearch Service on cloud landing page and a deployment configuration interface.

Landing Page (Left):

- Header: elastic (with logo), Products, Learn, Company, Pricing, Contact, Try Free, Login, Search icon.
- Section: Elasticsearch, Features, Elasticsearch Service (highlighted in blue), Pricing, Compliance, Cloud Status.
- Section: ELASTICSEARCH SERVICE
- Section: Hosted Elasticsearch and Kibana on AWS, GCP, and Azure
- Text: Get the official Elasticsearch Service from the creators. Spin up a fully loaded deployment on the cloud provider you choose.
- Form: Email Address (input field), Start Free Trial (button).
- Text: By submitting you agree to the [Elastic Cloud Standard Terms of Service](#) and to receive occasional emails from Elastic. Your personal data will be processed in accordance with Elastic's [privacy statement](#).

Deployment Configuration (Right):

- Summary:**
 - Name: First Cluster
 - Version: v7.0.1
 - ES data memory: 24 GB
 - ES data storage: 1.25 TB
 - Total memory: 25.5 GB
 - Total storage: 1.25 TB
 - Hourly rate: \$0.8281
 - Monthly rate: \$904.51
- Architecture:**
 - Zone 1: 3 nodes (1 zone, 8 GB RAM each)
 - Zone 2: 2 nodes (1 zone, 8 GB RAM each)
- First cluster - Edit (Data tab):**
 - Deployment: Elasticsearch (Logs, Snapshots, API Console)
 - Kibana (APM, APM, Security, Performance, Custom plugins)
 - Data: gcp.data.highio.1 (A Kibana instance, Fault tolerance: 1 zone, RAM per Node slider: 8 GB, Instances: 1)
- Kibana 1 configuration:**
 - gcp.kibana.1 (A Kibana instance, Fault tolerance: 1 zone, RAM per Node slider: 8 GB, Instances: 1, RAM per Zone: 1 GB)
 - Summary: 100 RAM, 1 instance, 1 zone, 100 RAM
 - User settings overrides

<https://www.elastic.co/products/elasticsearch/service>

Elastic Stack の有償サブスクリプション

Gold

Everything in Basic, plus:

- Audit logging
- IP filtering
- Advanced authentication
 - LDAP
 - PKI
 - Active Directory
- Elasticsearch Token Service

Platinum

Everything in Gold, plus:

- Single sign-on
 - SAML
 - OpenID Connect
 - Kerberos
- Attribute-based access control
- Field- and document-level security
- Custom authentication & authorization realms
- Encryption at rest support
- FIPS 140-2 mode

<https://www.elastic.co/subscriptions>



トレーニング

Elastic Training — Security

Training

Fundamentals of Securing Elasticsearch

Course Details

This course is a module of the Elastic Stack Management specialization. Find out how our focused **Training Specializations** can help you with your use case.

Audience
Software Engineers, System Administrators, DevOps

Duration
2-3 hours

Prerequisites
We recommend taking the following foundational courses (or having equivalent knowledge):

- Elasticsearch Engineer I
- Elasticsearch Engineer II

Requirements

- Stable internet connection
- Mac, Linux, or Windows
- Latest version of Chrome or Firefox (other browsers not supported)
- Disable any ad blockers and restart your browser before class

Topics Covered

- Blocking unauthorized access
- Securing communications inside an Elasticsearch cluster
- Securing communications outside an Elasticsearch cluster

[Register](#) [Download Outline](#)

Elastic Training — Security

Training

Advanced Techniques for Securing Elasticsearch

Course Details

This course is a module of the Elastic Stack Management specialization. Find out how our focused **Training Specializations** can help you with your use case.

Audience
Software Engineers, System Administrators, DevOps

Duration
2-3 hours

Prerequisites
We recommend taking the following foundational courses (or having equivalent knowledge):

- Elasticsearch Engineer I
- Elasticsearch Engineer II
- **Fundamentals of Securing Elasticsearch**

Requirements

- Stable internet connection
- Mac, Linux, or Windows
- Latest version of Chrome or Firefox (other browsers not supported)
- Disable any ad blockers and restart your browser before class

Topics Covered

- Advanced authentication
- Advanced authorization
- Audit logging

[Register](#) [Download Outline](#)

<https://www.elastic.co/training>



Demo time!





Questions?





Thank you!

