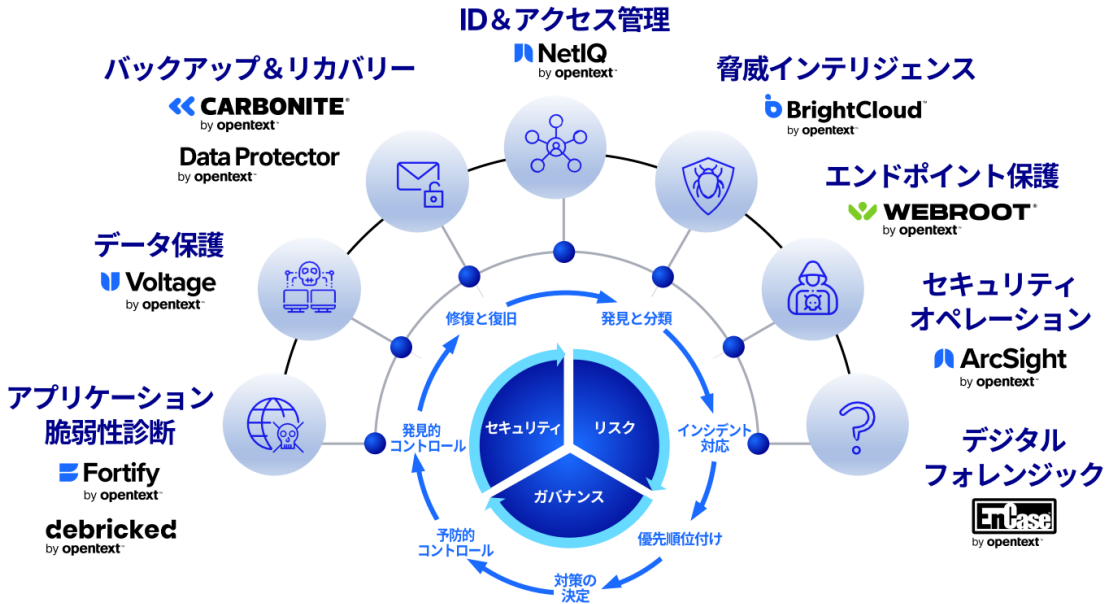


# サイバーレジリエンスの強化

OpenText Cybersecurityは包括的なセキュリティカバレッジでお客様のサイバーレジリエンス強化を支援します



サイバーレジリエンスは、サイバー攻撃を前提に、それを防衛し攻撃による被害を低減しつつ、被害にあっても迅速に復旧を行い、ビジネスを継続する取り組みです。サイバー攻撃は日々巧妙に進化し続けており、完全に攻撃を防御することが難しくなっている現状では、ゼロトラストの考えを取り入れ、攻撃に対する防御、なおかつ、サイバーレジリエンスの考えに基づき被害からの迅速な復旧、これらを行う事で、サイバー攻撃の脅威を最小化できます。マイクロフォーカスエンタープライズ (※) は、4つのポートフォリオでお客様のサイバーレジリエンスの強化を支援します。

## Voltage by opentext™

### データプライバシー／プロテクション

- 個人情報・機密データの保護 (暗号化、トークン化)
- カード情報保護、非保持化による監査範囲の縮小
- データクラウドとの連携によるセキュアな分析
- テスト用データの保護・管理

2022年Gartner® Peer Insights™のデータマスキング部門で Customers' Choiceの1社に位置付け

The Forrester Wave™: Data Security Platforms, Q1 2023においてリーダーに選出

## Fortify by opentext™

### アプリケーションセキュリティ

- 最新の開発に対応した包括的なAppSecプラットフォーム
- ソフトウェアサプライチェーンの保護
- 自社開発コードだけでなくOSSのライセンス違反や脆弱性発見も可能
- APIの脆弱性診断にも対応

Gartner®アプリケーション・セキュリティ・テストの Magic Quadrant™で、10年連続リーダーの1社に位置付け

業界をリードする精度とカバレッジの広さを オンプレミスでもSaaSでも提供

## NetIQ by opentext™

### アイデンティティおよびアクセス管理

- インテリジェントアクセスガバナンスによるゼロトラスト
- アダプティブアクセスと自動化
- 不正アクセスからの非構造化データの保護
- セキュリティポリシー制御の一元管理

ヨーロッパを代表する情報セキュリティ専門アナリスト企業の Access Management 2022レポートでリーダーに選出

従業員や顧客を対象とした包括的なIDおよびアクセスサービスを提供し、組織のセキュリティを確保することでゼロトラストを実現

## ArcSight by opentext™

### セキュリティオペレーション

- 業界トップのリアルタイム相関分析
- ユーザー・エンティティの行動分析、SOARとの統合
- オープンでスケーラブルなデータプラットフォーム
- 脅威インテリジェンス (MITRE、MISP、GTAP+)

GigaOmのRader for SIEMにて、革新的なリーダーとアウトパフォーマーに選出

KuppingerColeのリーダーシップコンパス for インテリジェンス SIEMプラットフォームにて、Overallリーダーに選出

マイクロフォーカスエンタープライズ株式会社

microfocus-enterprise.co.jp

お問い合わせは[こちら](#)から

(※) マイクロフォーカスエンタープライズは、2023年1月31日 OpenTextによるMicro Focusの買収完了 (詳細) により、OpenTextグループとなりました。

アプリケーションセキュリティテストに必要な診断方式を網羅、高い検出精度、広範囲なカバレッジ

## 幅広いポートフォリオ

- Fortify Static Code Analyzer:** 静的解析(SAST)ツール
  - ソースコードを使い論理的で網羅的に脆弱性を分析します。
  - 各種統合開発環境(IDE)用プラグインも提供しています。
- Fortify Debricked / Sonatype:** ソフトウェアコンポジション解析(SCA)ツール
  - バイナリ/マニフェストを使いOSSの脆弱性を分析します
- Fortify WebInspect:** 動的解析(DAST)ツール
  - 実行中のアプリケーションに対して疑似攻撃を行い脆弱性を分析します。
  - 分析対象には、APIも含まれます。
  - IASTエージェントとの組み合わせで、より詳細な分析が可能になります。
- Fortify on Demand:** SaaS(サービス)AppSec
  - SaaSとして、SAST、SCA、SSC相当機能、DAST、MAST(モバイル用バイナリファイル(IPA/APK)を使った解析)を提供します。

	SAST	SCA	DAST	MAST
オンプレミス	✓	✓	✓	-
SaaS	✓	✓	✓	✓

Fortifyは、様々なアプリケーションセキュリティテストのプラットフォームニーズに応えられるよう、SaaSによるスモール・クイックスタート、オンプレを代表する秘匿性の高い利用法、エンタープライズ規模での利用、オンプレ/SaaSハイブリッドによる適材適所利用といった高い柔軟性と拡張性を備えています。

## スキャンの精度



**100%**

OWASP 1.2bベンチマークでのFortify SASTの真陽性率  
[Fortifyソフトウェアセキュリティサーチ](#)による裏付け (2021年12月時点)



**95%**

Fortify SASTは、検出漏れを最小化した上で、機械学習を使用して誤検出を削減

## カバレッジの広さ



**1,600以上**

検出可能な脆弱性カテゴリ



**33以上**

サポートされるプログラミング言語



**1,000,000以上**

対応しているAPI  
 (アプリケーションプログラミングインターフェイス)

## 幅広いコンプライアンスに対応



- OWASP Top 10
- OWASP API Top 10
- OWASP ASVS
- OWASP Mobile Top 10



- CWE Top 25



- DISA STIGS



- GDPR



- NIST SP800-53
- FISMA Compliance

- ISO 27001
- PCI DSS
- PCI SSF
- HIPPA

## 2,000社以上のグローバル導入実績

日本国内でも多くのお客様にご利用いただいております。



**150**  
YEARS

「Fortifyは、組込ソフトウェアからWebアプリケーションまで『単一のソースコード脆弱性検査ツール』として活用できることが私たちにとって非常に重要です」  
 - 品質本部 新規事業品質保証部 部長 矢部 智 氏



「このパートナーシップの目的は、Fortify on DemandでAppSecを最新化することで、実用的なデータ主導の結果を得ることです。」  
 - Rajan Gupta氏 (製品セキュリティ担当VP)



「Fortifyは、開発者のニーズに間違いなく応えてくれます。ニーズをよくわかっています。」  
 - Damien Suggs氏 (AppSecディレクター)



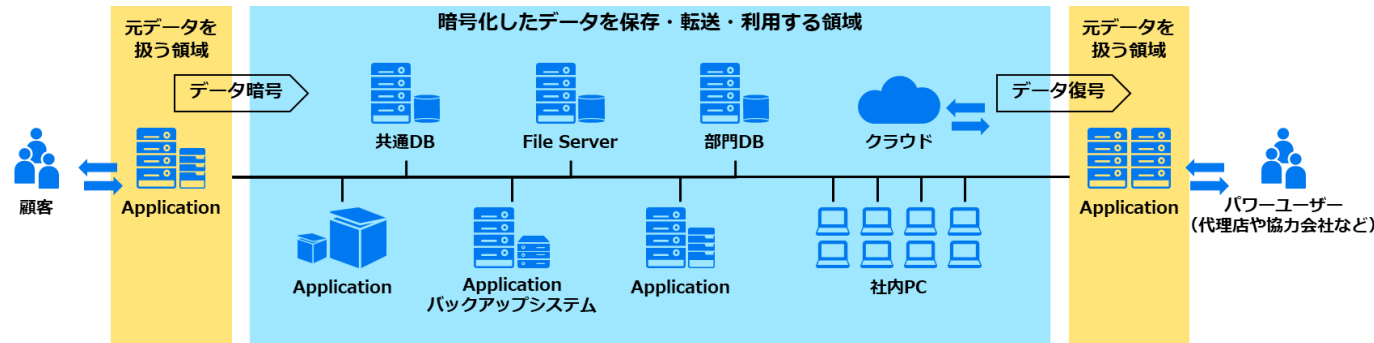
## Fortify 特設サイト

最新情報を含む製品関連資料や事例、アプリケーションセキュリティに関するレポートなどをご紹介します。  
[microfocus-enterprise.co.jp/products/static-code-analysis-sast/](https://microfocus-enterprise.co.jp/products/static-code-analysis-sast/)

マイクロフォーカスエンタープライズ株式会社  
 お問い合わせは[こちら](#)から

## データ自体を暗号化するデータセキュリティ

データが入力された時点から暗号化を行うことで、本当に生データが必要な業務以外は暗号化状態で保存・転送・利用が出来るようになります。アプリケーションやネットワーク、データベースなど、レイヤーごとのセキュリティ対策では、レイヤー間でセキュリティギャップが生じますが、Voltage SecureDataは、End-to-Endで情報を保護することでギャップをなくします。



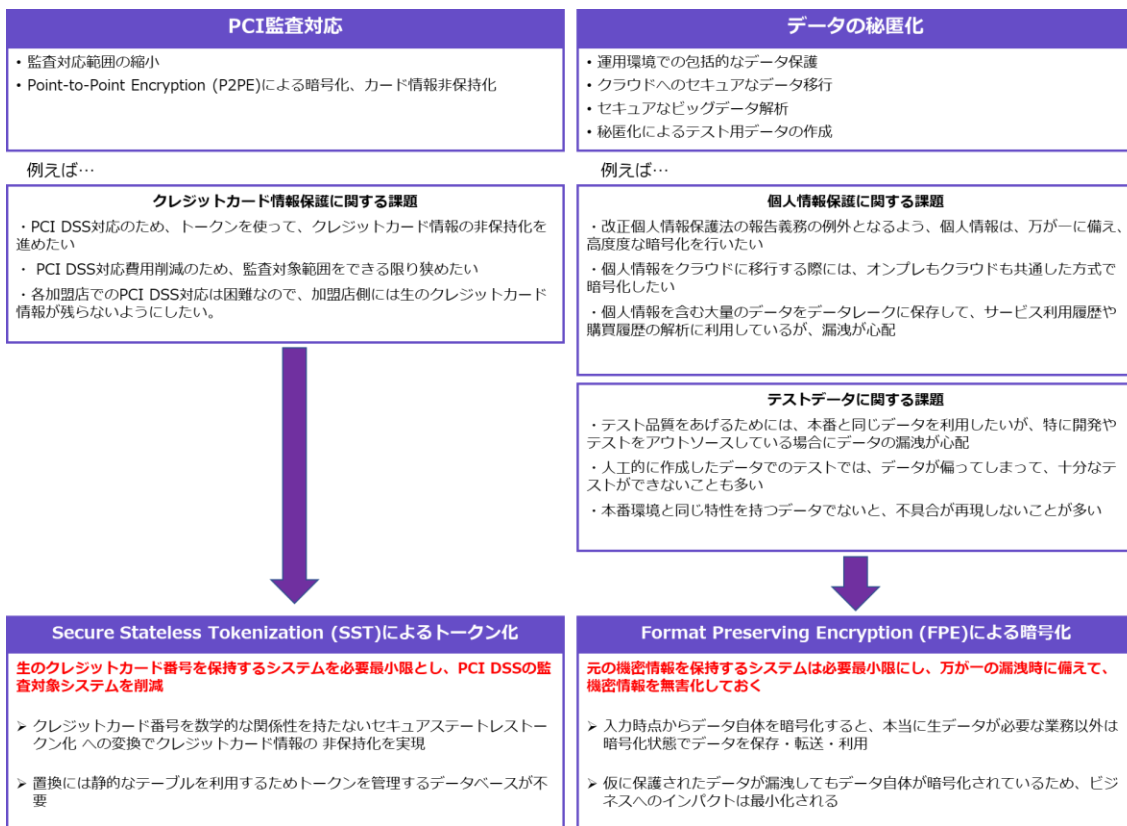
### Voltage SecureData 主な機能

- フォーマット保持型暗号（FPE：Format Preserving Encryption）
- フォーマット保持型ハッシュ（FPH：Format Preserving Hash）
- セキュア・ステートレス・トークナイゼーション（SST）

### FPEで暗号化した例

変換例	生データ	暗号化データ（日本語に対応）
氏名	庄司 まゆみ	高野 ひろま
郵便番号	123-4567	814-6811
住所	東京都千代田区丸の内1-2-3 丸の内ヒルズA-1001	埼玉県荒川市緑5-0-5 吉成ビルナキM-1874
電話番号	010-2345-6789	631-8723-5075

## データセキュリティの主なユースケース



## ゼロトラストにおけるIAMの重要性

「ゼロトラスト」は、調査会社Forrester Researchのアナリストが2009年に発案した概念です。何も信頼せず、全てのアクセスに対して全てを疑い検証することを意味しています。

ゼロトラストの概念を取り入れたセキュリティ対策では、システムやデータへアクセスするためのIDがセキュリティ境界となりますが、IDのみならずデータ・アプリ・デバイスもそれぞれ保護する必要があります。









なお、ゼロトラストは単一製品やソリューションでの実現は難しく、これら製品やソリューション間の連携が必須です。

例えば、クラウド・アクセス・セキュリティ・ブローカー (CASB)、セキュア Web ゲートウェイ (SWG)、セキュリティ情報とイベント管理 (SIEM) やエンドポイントにおける検知と対応 (EDR)、情報漏洩対策 (DLP) などが関連しますが、それぞれが見ているIDは本当に正しいと言い切れるのでしょうか。IDの管理が正しく行われない限り、関連製品によるゼロトラスト対策も信頼性が揺らぐこととなります。

これら関連機能が本人確認に利用するIDは、IAMにより管理されるため、ゼロトラストの中でもIAMが最も重要な機能であると言えます。

## NetIQ 製品ポートフォリオ

IDを中心としたNetIQ IAMは、以下に代表される製品で構成されています。

 <b>IDガバナンス</b> (Identity Governance)			<b>多要素認証</b> (Advanced Authentication)
 <b>Web/フェデレーション系SSO</b> (Access Manager)	 <b>C/S系SSO</b> (SecureLogin)	 <b>特権ID管理</b> (Privileged Account Manager)	
 <b>統合ID管理</b> (Identity Manager)	 <b>AD/Azure AD 管理権限委任強化</b> (Directory & Resource Administrator)	 <b>ユーザ自身によるパスワードリセット</b> (Self Service Password Reset)	
			

ソリューション	目的
IDガバナンス	ユーザが持つ各種アクセス権限を収集して、リスク値等を使い不適切な権限が付与されていないか監査することを目的としています。統合ID管理と組み合わせることで、監査に加えて自動反映させることも可能となります。
Web/フェデレーション系SSO	WebサイトやSaaS利用時のID/パスワード入力の手間を軽減します。
C/S系SSO	Web化されていないツール、例えば、ESXクライアントやターミナルソフトへのID/パスワード入力の手間を軽減します。
特権ID管理	共有して利用されることが多いroot/administratorといった特権IDの、利用制限、ならびに、操作内容の監査を目的としています。
統合ID管理	冗長的なID管理作業をシステムで自動化して、管理作業の負荷を軽減します。
AD/Azure AD管理権限委任強化	AD管理ツールで不足する最小権限管理を強化します。
ユーザ自身によるパスワードリセット	ユーザ自身でパスワードリセットが可能となるため、ヘルプデスクの作業負荷を軽減します。
多要素認証	ID/パスワードでは不足する個人特定化情報を、他の要素、例えばOTPやスマートフォン等を使い個人特定化を強化します。

## NetIQ 選ばれる理由



### ゼロトラストの要であるID/アクセス/ガバナンス管理まで単一ベンダーで完結

一般的にこれらの管理機能は、別ベンダー製品を組み合わせることで構成されるため、以下の様な問題が発生します。

- ・製品間の親和性の低さ
- ・カスタマイズ工数/運用コストの増大
- ・障害発生時対応時間の増加

NetIQ製品では、これらすべての管理機能を一括提供しているため、上述する問題は最小化され、適切な管理基盤を実現できます。



### 高機能

NetIQ製品は、管理の容易性を高める数多くの機能に対応しています。

統合ID管理では、役職や兼務等の管理に適したロール機能、ロールを応用したワークフロー・職務分掌・レポート等に対応しています。Web/フェデレーション系SSOでは、ID/パスワード以外の個人特定化情報やユーザ行動分析リスクスコアを用いたリスクベース認証、リスクスコアが高いユーザに対する多要素認証による本人確認強化に対応しています。その他製品も各製品に求められる数多くの機能を有しています。



### グローバル対応

NetIQ製品は、日本語対応だけでなく多くの諸外国言語に対応しています。

国内のITエンジニア不足に伴う外国人ユーザの採用、海外展開に伴う現地法人のM&A等が行われた場合でも外国人ユーザが必要とする言語を使ってシステムをご利用いただく事が可能です。

また、システム構築やサポートにおいても海外連携を行っておりグローバル体制での支援が可能です。



## NetIQ 特設サイト

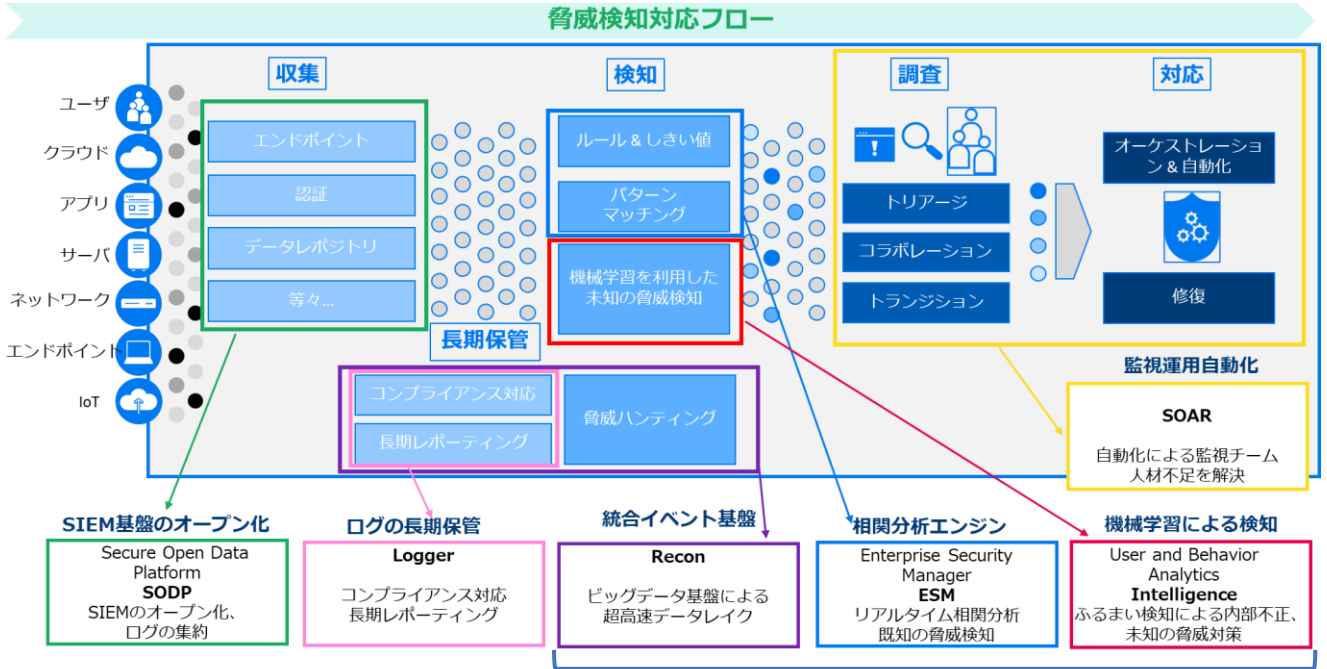
ID & アクセス管理に関わるトピックや製品資料、事例、ソリューション資料などをご紹介します。

[microfocus-enterprise.co.jp/products/id-access-management/](https://microfocus-enterprise.co.jp/products/id-access-management/)

マイクロフォーカスエンタープライズ株式会社  
お問い合わせは[こちら](#)から

## 脅威検知対応プロセスとArcSightソリューションマッピング

ArcSightは、さまざまなソースからのデータの自動収集、多層アナリティクスによる高度な脅威の検出、迅速かつ効率的な調査、そして被害が発生する前に対応する能力を備えた、次世代SOC構築の実現を支援します。



- リアルタイム相関と仮説および分析ベースの脅威ハンティングで、コンテキストの豊富なインサイトを提供する多層アナリティクス
- 多層アナリティクスと脅威モニタリングのコンテンツパッケージにより、MITRE ATT&CKの手法と戦術を広範囲にカバーします。

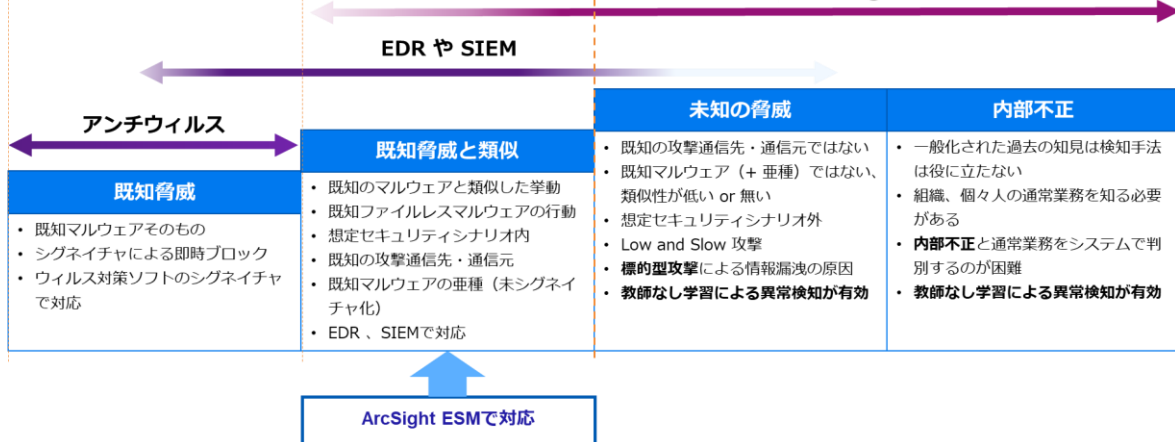
## Recon・ESM・Intelligenceで実現する多層アナリティクス

監視の現場で、この3種類の分析ツールを自在に使えることが重要

高速検索・統計処理	リアルタイム相関分析	教師なし学習・機械学習
原因究明 予兆調査	既知脅威の検知	未知脅威の発見 内部脅威の発見

## 内部不正、未知の脅威にフォーカスしたArcSight Intelligence

ArcSight Intelligenceは教師なし学習を使って未知の脅威を検出します。  
特長や関連資料などを、[特設サイト](#)でご紹介していますので是非ご訪問ください。



**ArcSight Intelligence 特設サイト**

日本語のデータシートや事例資料、過去の講演動画などを掲載しています  
[microfocus-enterprise.co.jp/products/interset-ueba/](http://microfocus-enterprise.co.jp/products/interset-ueba/)

マイクロフォーカスエンタープライズ株式会社  
お問い合わせは[こちら](#)から