COGNITE

Cognite Data Fusion®におけるNIST Cyber Security Framework（CSF）への対応

目次

↘ 概要

背景

世界中の政府機関や産業部門、組織において、サイバーセキュリティリスクの管理やシステムのレジリエンスの強化に役立つ推奨サイバーセキュリティベースラインとして、NISTのCyber Security Framework（CSF）に対する認識が高まっています。本ホワイトペーパーでは、Cognite Data Fusion®がいかにNIST CSFに対応し、お客様による導入をサポートするかについて評価します。

NIST Cyber Security Framework（NIST CSF）とは

米国の国家および経済の安全保障は重要インフラの安定稼働にかかっているという認識のもと、オバマ前大統領は2013年2月、大統領令第13636号「Improving Critical Infrastructure Cybersecurity（重要インフラのサイバーセキュリティの向上）」を発出しました。同大統領令はNIST（米国国立標準技術研究所）に対し、これまでの標準やガイドライン、手法に基づき、重要インフラのサイバーリスク低減のためのフレームワークを関係機関とともに策定することを指示するものです。

民間部門が自主的に採用できるよう産官連携によって策定されたこのフレームワークは、重要インフラの保護を推進することを目的とした標準、ガイドライン、手法で構成されています。NIST CSFのアプローチは対策を優先順位付けするため、柔軟かつ繰り返し利用可能で費用対効果が高く、重要インフラの所有者や運用者がサイバーセキュリティに関するリスクを管理するうえで役立ちます。

Gartner社によれば、米国では民間部門の企業のうち約30%がCSFを採用、2020年には50%に達すると見込まれていました。CSFは16の重要インフラ部門で採用されており、導入済みの州は21州を超えています。イタリアやイスラエルといった他国でも、CSFは国家のサイバーセキュリティガイドラインの基礎として用いられています。

NIST CSFの適用

NIST CSFは、アセスメントや企業買収のほか、Software as a Service（SaaS）プロバイダーの評価において裏付けを取るための手段として、テクノロジーの調達やセキュリティプログラムへの投資における優先順位付けの統一基準となります。このフレームワークによって、セキュリティとコンプライアンスの全社的目標の定義が捗ります。

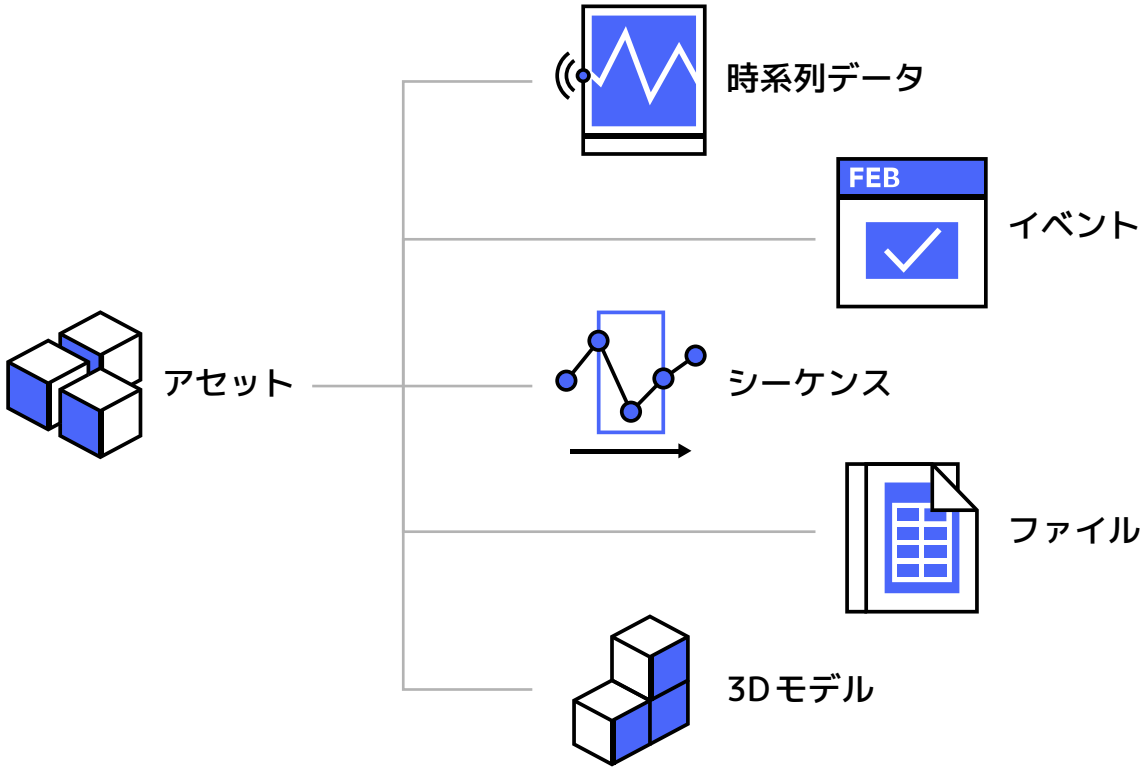
↘ Cognite Data Fusion®

SaaSプロバイダーであるCogniteが提供するCognite Data Fusion®は、産業用DataOpsプラットフォーム製品です。このほか、サブスクリプションベースの設定可能なビジネスアプリケーションへのアクセスも提供しています。

Cognite Data Fusion®(CDF)によって**CDFデータモデル**へ取り込まれたデータは、各種データリソース間の関連付けを加えて正規化され、価値が高められた後、クラウド上のグラフインデックスに保存されます。クラウド上にデータが保存されることで、お客様はCognite Data Fusion®のサービスやツールを使い、ソリューションやアプリケーションをビジネスニーズに合わせて構築できます。

Cogniteでは、データの所有者は常にお客様です。弊社がお客様のデータを利用するのは、合意されたサービスを提供する場合のみです。弊社はお客様のデータを**セキュアに**処理し、プライバシーや法律上の規制に準拠します。お客様が弊社サービスの利用を終了される際には、そのデータ所有権が守られることを保証しています。

お客様のデータは**ポータルアプリケーション**のほか、**APIやSDK**を利用して操作していただけます。



Cognite Data Fusion®
ソリューションのセキュリティ

運用技術(OT: Operational Technology)を利用する業界においてクラウド技術の導入が進むなか、堅固でより自動化されたサイバーセキュリティリスク管理手法によって、相互接続されたシステムごとにデータの機密性、完全性、可用性を守ることが極めて重要になっています。既存の装置やインフラと統合できるCognite Data Fusion®なら、洞察を得て、産業データの価値を引き出すことが可能です。信頼できるデータ管理受託者としての責務を全うすべく、弊社はCogniteセキュリティコミットメントとして、Cognite Data Fusion®の設計と運用に関する情報を提供する担当者、プロセス、テクノロジーに焦点を絞った一連の方針を策定し、実践しています。

多層防御

Cogniteは、OTセキュリティが必須要素となる、重要インフラや産業界でサービスを展開しています。Cognite Data Fusion®において、セキュリティ管理はお客様、Cognite、クラウドプロバイダー（Microsoft やGoogleなど）による共同作業です。

Cogniteは以下を通じて多層防御をサポートしています。
業界のセキュリティコンプライアンスと規制
セキュア開発ライフサイクル
セキュリティのログと監視
インシデント対応

セキュリティに関わるステークホルダーは、Industry 4.0 の拡大と継続を成功させるうえで不可欠な存在です。弊社はお客様のセキュリティ・ステークホルダーと積極的に関わり、サポートしたいと考えています。

セキュアバイデザイン

■ 製品規格への適合：Cogniteの管理システム（QMS、ISMS）は、ISO 9001 およびISO 27001の認証を取得済みです。また、Cognite Data Fusion®の運用とデータ処理は、EU一般データ保護規則（GDPR）に準拠しています。

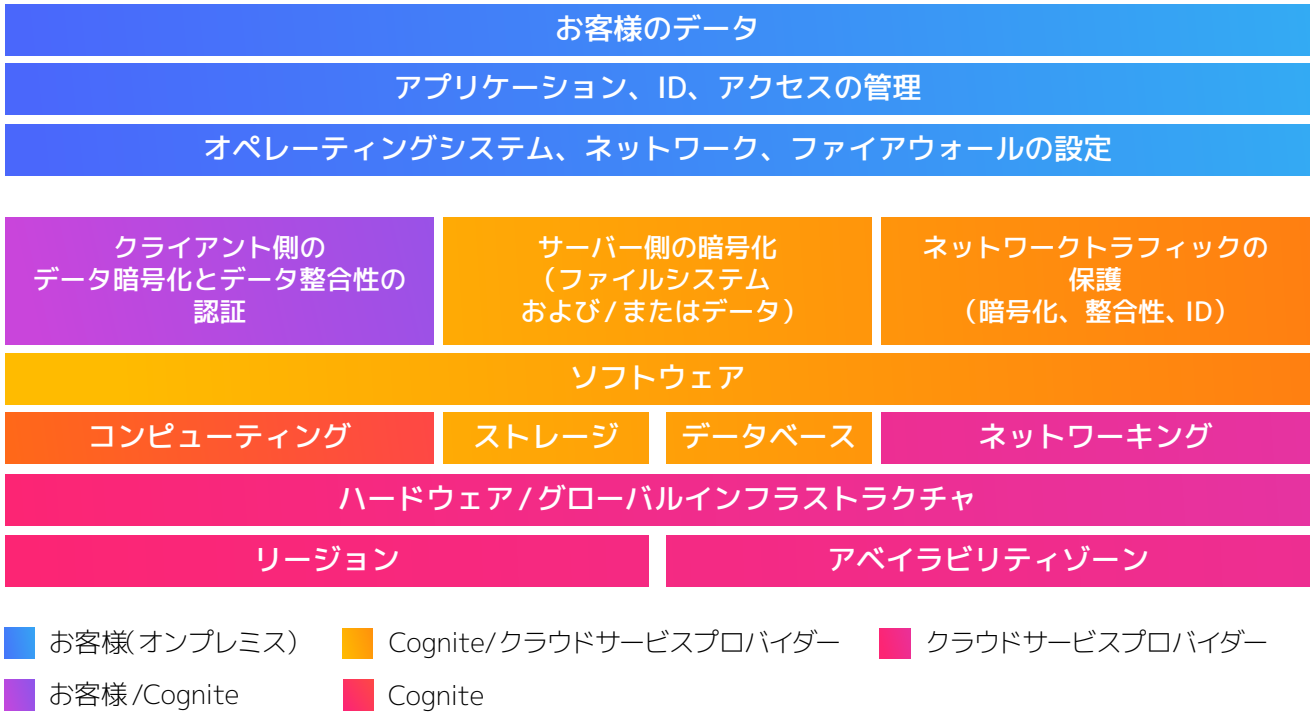
■ セキュア開発ライフサイクル：Cogniteは、社内のDevSecOpsをサポートすべく、セキュリティに関する認識の向上とトレーニングに投資しています。セキュリティ手法を支えるのは、（1）包括的な監査・監視スタック、（2）テストとセキュリティの自動化、（3）インシデント対応における堅固なプロセスと実践です。

■ 最小特権とアクセス制御：お客様は自社のIDプロバイダーを利用した統合によってデータへのアクセスを制御できます。Cogniteとのプロジェクト契約では、お客様データへの特権アクセスはロールベースで厳しく制限されます。

■ データ保護：保存データと転送中のデータを暗号化します。

責任共有モデル

クラウドセキュリティ原則の文脈における各ロールを理解するうえで、責任共有モデルを基本としています。このモデルは、お客様組織、Cognite、お客様のクラウドサービスプロバイダー（CSP）全体の所有権を特定するものです。



Cogniteの世界に通用するCSPパートナーは、クラウドサービスを運用するためのハードウェアやソフトウェア、ネットワーキングや設備から成るインフラストラクチャを担う存在です。

CogniteはCSPとの強固な関係を維持することで、業界標準に準拠したプラットフォームとインフラストラクチャのセキュリティ制御を採用しています。それらのプロセス、手順、ツールが、Cognite Data Fusion®の確固たるセキュリティ基盤を支えています。新たなテクノロジーや脅威が次々と出現するなか、自社製品においてそれらのセキュリティアップデートを活かせる独自の地位を確立しているのが、Cogniteです。

コンテンツやアプリケーション、システムやネットワークを保護するために導入するセキュリティ管理はお客様が自由に設定することができます。CogniteはCSPと連携して保存データと転送中のデータの暗号化をサポートします。アプリケーションのセキュア開発ライフサイクルと関連する脆弱性管理に対する責任はCogniteにあります。

データセキュリティとアクセス制御

→ アクセス制御

お客様のIDプロバイダー（IdP）での構成と同じく、お客様が定義されたユーザー、ロール、特権によって顧客データに対するアクセス制御の管理方法が決まります。お客様データに対するCognite社員へのアクセス権の付与はIdPによって行われ、アクセス権の有効化と失効のタイミングはお客様が選択できます。

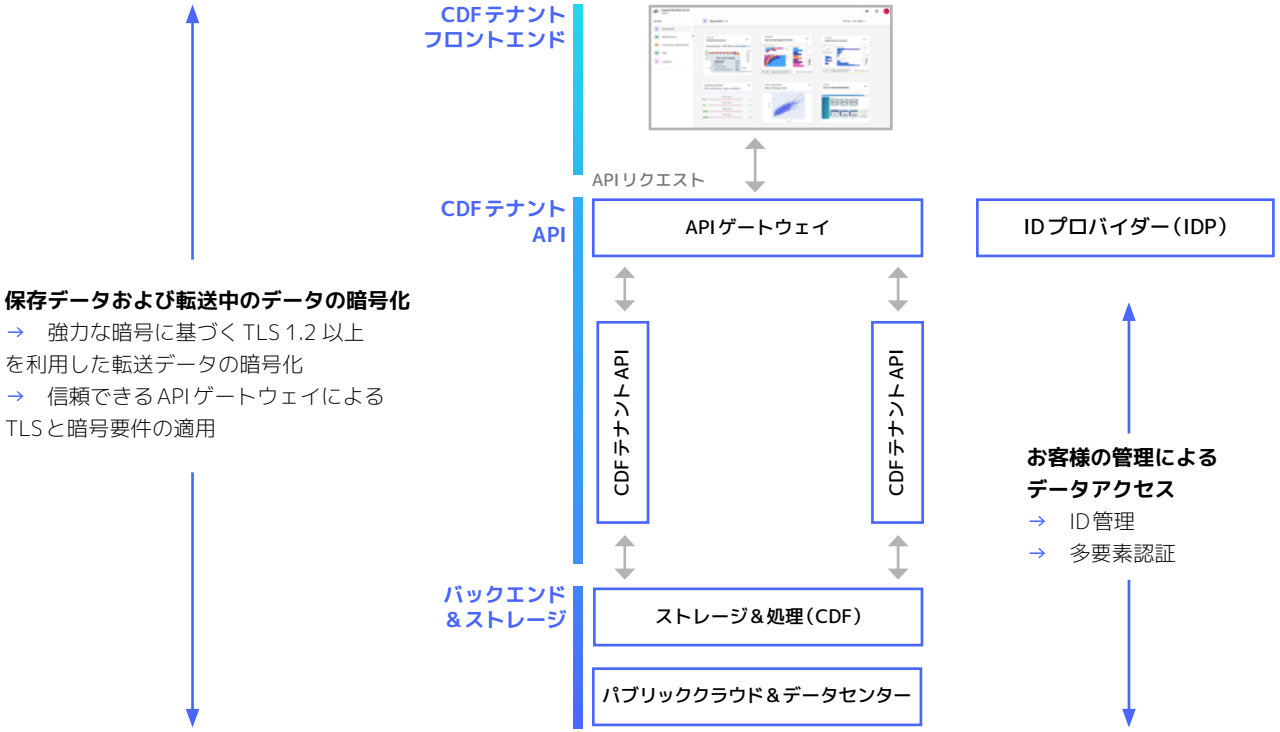
→ データセキュリティ

転送中のデータの暗号化： Cognite Data Fusion®に対するデータの所有者/ソース、Cognite API、内部トラフィックは、TLS 1.2以上によって暗号化されています。

保存データの暗号化： クラウドサービスによって管理されている暗号化/暗号化解除キーを利用した、サーバー側の暗号化です。

データの漏洩や意図的・偶発的な侵害を防ぐために導入されているCogniteの管理体制には、以下のようなものがあります。

■ クラウドサービスプロバイダー（CSP）の暗号化キーを利用したデータ暗号化



■　お客様が管理するデータアクセス：お客様のIDプロバイダー（IdP）サービスとの統合。リクエストとAPI呼び出しは、IdPから付与されたロールとアクセス許可にマッピングされます。

■　最小特権の原則および承認（ピアレビュー）フローに基づくコードで管理された変更。

■　認証済みまたは許可されたサービスのみへのアクセス制御・制限を行うネットワークおよびインフラストラクチャのポリシー。

■　共有データストア内での論理的分離。

■　CSPは、サービス間通信のためにアプリケーション層で暗号化された認証と許可を使用。

■　IPスプーフィングを防ぐために、CSPがネットワーク全体でのイングレス/エグレスフィルタリングを追加のセキュリティレイヤーとして利用。

レジリエンス

Cognite Data Fusion®は、高可用性が得られるように設定されたクラウドインフラストラクチャをベースとします。変更の検証や確認を素早く行えるようにする一方で、影響や中断の可能性を最小限に抑えるため、導入では小規模な変更を繰り返し漸進的に行います。Cogniteでは事業継続性や災害復旧計画のテストを（机上および実際の演習で）常に実施することで、機密性、完全性、可用性といったシナリオや機能を検証します。
NISTの800-61標準ガイドライン「コンピュータセキュリティインシデント対応ガイド」に対応した検出・対応・復旧対策として、以下のような対策をとっています。
また、インシデント対応プロセスは、ISO 9001および27001に準拠して個別に認証を受けています。

準備：プロセスやツールの導入、実行して得た継続的改善。

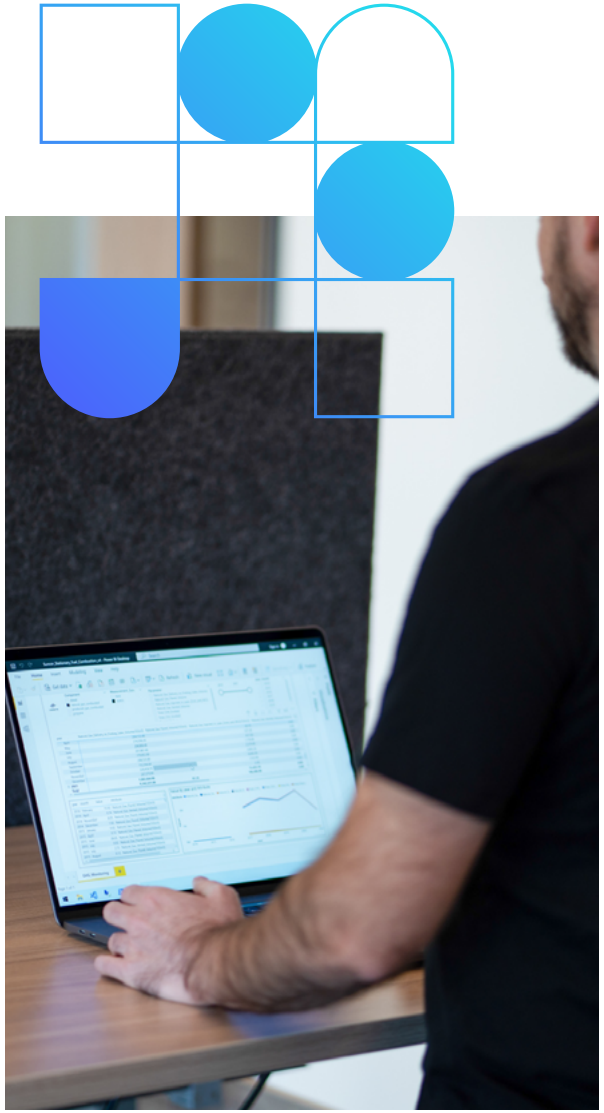
封じ込め：体系化とダメージの抑制/防止。

根絶：根本原因の排除とシステムの復元準備。

復旧：望ましい状態でのシステムの再稼働と監視。

Cognite Data Fusion®におけるNIST CSFへの対応

SaaSソリューションであるCognite Data Fusion®は、お客様がCSFで定義されている管理のベストプラクティスを維持し、CSFに関連したセキュリティ体制の調整と測定を実施できるようサポートします。後述の付録1では、Cognite Data Fusion®がいかにNIST CSFの主要機能やサブコントロールに対応しているかについて詳述しています。



↘ 付録：Cognite Data Fusion® における NIST CSF への対応

管理策カテゴリー	管理策サブカテゴリー ID	Cognite における NIST Cyber Security Framework 管理策への対応
アクセス管理プログラム	DE.DP-1 DE.DP-2 ID.AM-3 ID.AM-6 PR.AC-1 PR.PT-3	Cognite の「行動規範」（Code of Conduct）では、機密性、データ保護、Cognite の装置や設備の適切な使用法、組織が期待する行動に関して、従業員や契約社員の情報に対するセキュリティ上の責任を規定しています。Cognite は、組織のユーザー、グループ、オブジェクトの認証、承認、アクセス制御に、クラウドプロバイダーの ID リポジトリサービスやクラウドサービスを使用しています。ID リポジトリでは、リソースへのアクセス権の付与にロールベースのアクセス制御（RBAC）が利用されています。また、機密情報へのアクセスをセキュリティで保護し、悪意のある攻撃のリスクを最小限に抑えるために多要素認証（MFA）が採用されています。
アクセス権の失効	PR.IP-11	Cognite の「人事セキュリティ方針」（Human Resources Security Policy）では、従業員、契約社員、サードパーティのアクセス権解除プロセスについて概説するとともに、雇用終了やロール変更に伴う関連責任を明確に定義しています。また Cognite は、離職する従業員や、従業員、契約社員、その他サードパーティユーザーに割り当てられた責任の取り消しを効果的に管理するために内部手順を取り入れています。情報や情報システムへのアクセス権は、雇用関係または契約関係の終了をもって削除されます。従業員、契約社員、サードパーティユーザーの離職におけるアクセス権の終了・変更については、規定の手順書があります。それらの権限は ID 管理（IDM）システムを使って削除されます。Cognite における責任や職務の変更には、以前のロールや職務に関する全権限の削除、そして新たなロールや職務に応じた権限の作成が含まれます。雇用終了前のアクセス権の削除や制限が妥当と見なされるリスクがある場合は、適宜実施されます。

管理策カテゴリー	管理策サブカテゴリーID	Cogniteにおける NIST Cyber Security Framework 管理策への対応
アセットのインベントリ	ID.AM-1 ID.AM-2 ID.AM-5	情報および情報処理設備に関連するCogniteのアセットは、それぞれのライフサイクル全体を通してインベントリに記録されます。インベントリはインベントリデータベースシステムで文書化され、管理されることから、デバイスの新規導入や使用停止が行われても常に正確な最新のインベントリが得られます。分類は、Cogniteのセキュリティグループが定めた基準に基づきます。
構成変更管理	PR.DS-3 PR.DS-4 PR.DS-5 PR.DS-6 PR.DS-7 PR.DS-8 PR.IP-3 PR.MA-1 PR.MA-2	ハードウェア、ソフトウェア、およびネットワークデバイスの構成設定やベースライン構成のレビューや更新は、Cogniteのクラウドサービスプロバイダー(CSP)によって毎年実施されます。変更が生じた場合は、開発環境やテスト環境から実稼働環境に移される前にテストと承認が行われます。ベースライン構成は、ソースコード管理リポジトリと併せて文書化され、管理·保守されます。導入に先立って、各サービスチームによる情報セキュリティ影響分析とそのレビューが実施されます。ベースライン構成への変更はSDLプロセスに回されます。実稼働環境への展開には事前にセキュリティ承認が必要なためです。 変更ライフサイクルに対する規律と品質管理は、Cogniteの「変更管理ポリシー」(Change Management Policy)に従います。大幅な変更については、サブコンポーネントに分けて継続的デリバリー(CD)を実施します。この規律によって、変更に起因する問題発生のリスクが抑えられ、必要に応じてより素早く元の状態に戻すことができます。変更時には、そのプロセスが自動追跡システムに記録され、分類されたうえで文書化されます。すべての変更管理が、設計文書、コードレビュー、テスト、そして変更諮問委員会を経た承認によって裏付けられます。承認済みの変更はすべて、ロールアウトの日付と影響分析で見つかります。変更連絡は、プロジェクト管理プロセスに従って行われます。何らかの問題が発生したら、規定に準じてロールアウト計画が実行されます。変更の実施については、影響を受けるユーザー全員にあらかじめ周知されます。
構成の監視	DE.AE-1 PR.IP-1	Cogniteは、ソースコード管理リポジトリを使ってすべての変更·承認の証拠を文書化し、記録しています。これらのツールには、ベースラインへの変更や構成変更を確認する監査機能が搭載されています。また、このリポジトリは、ソフトウェアコードのバージョン管理システムも備えています。これらのツールによってコードをチェックした各ユーザーのIDや変更日時、特定のファイルに加えられた変更が記録されます。加えて、Cogniteでは変更管理プロセスの年次レビューを実施しています。年次レビューの一環として、変更のサンプルを抽出してレビューを行い、変更管理プロセスへの準拠が徹底されていることを確認しています。このプロセスは、ベースラインに対し未承認の変更が行われないようにするためのものです。

管理策カテゴリー	管理策サブカテゴリーID	Cogniteにおける NIST Cyber Security Framework 管理策への対応
サイバーセキュリティインシデント対応計画の導入とテスト	ID.SC-5 PR.IP-10 PR.IP-9	CogniteのCSPは、クラウド環境でのインシデント発生時に最適なパフォーマンスを保証するため、インシデント対応の方法とツールを毎年テストしています。テストはテスト環境と実稼働環境の両方で行われます。その効果を実地演習で検証する目的で、実稼働環境での総合演習も四半期ごとに実施されます。結果はすべて、CSPのインシデント対応テスト計画で文書化されます。 Cogniteは、一般的なサードパーティツールのほか、特注のツールやソリューションを使って、インフラストラクチャ、サービス、アカウント、ログに脆弱性や異常なアクティビティが見られないか監視しています。また、内部だけでなくサードパーティのセキュリティ専門家や監査役による運用や環境のテスト、評価、監査も行っています。報告または検出された問題や脆弱性は記録·追跡され、優先順位が付けられます。すべての項目に所有者と優先順位が指定され、情報が可視化されて管理·追跡されます。Cogniteのセキュリティチームは外部検証の一環として、プロトコルと手順ごとにインシデント対応のテストと演習を実施します。関連するサマリーやレポートにコメントや最新情報が追記され、共有されます。 正式なインシデントレポートはサービスチームが作成し、それにCogniteのインシデント管理チームが追加事項を付記します。教訓を含むこれらのレポートは、すべてのイベントに対して作成されます。インシデントレポートの保守はCogniteのセキュリティチームが担当し、しかるべき関係者にレポートを配布してレビューを依頼します。 毎月、前月に発生したすべてのインシデントのレビューをリーダーシップチームと行います。レビュー項目には、(1)インシデントの影響と解決方法、(2)「インシデント対応計画」(Incident Response Plan)に対する変更内容が含まれます。インシデント対応計画は、計画の導入、実施、あるいはテスト中に生じたシステムや組織に関する変更または問題に合わせて改訂されます。

管理策カテゴリー	管理策サブカテゴリーID	Cogniteにおける NIST Cyber Security Framework 管理策への対応
サイバーセキュリティインシデント対応計画の詳細	ID.SC-5 RS.AN-1 RS.AN-2 RS.AN-3 RS.AN-4 RS.AN-5 RS.CO-1 RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5 RS.IM-1 RS.IM-2 RS.MI-1 RS.MI-2 RS.MI-3 RS.RP-1	Cogniteの「インシデントマネジメントポリシー」(Incident Management Policy)は、サービスインシデントやセキュリティインシデントへの適切な対応や、効率的かつタイムリーなレポートの作成に関する全社的ガイダンスを規定するものです。このポリシーによって、最も緊急度が高く、ビジネスへの影響が最も大きくなる可能性のある問題にサポートリソースが注力できるようにするための方法を管理しています。このプロセスで得られるコントロールや管理に関する情報は、Cogniteの経営陣が企業目標達成上のリスクに対処するうえでリソースの優先順位を付けるための意思決定に役立ちます。Cogniteでは、サービスの運用を早急に正常な状態に復旧するとともに、事業活動への悪影響を最小限に抑えるため、開発におけるCI/CD(継続的インテグレーション/継続的デリバリー)手法を採用することで、考えられる最高水準のサービス品質と可用性を維持しています。

管理策カテゴリー	管理策サブカテゴリーID	Cogniteにおける NIST Cyber Security Framework 管理策への対応
サイバーセキュリティポリシー	ID.AM-3 ID.GV-1 ID.RM-1 ID.RM-2 ID.RM-3	Cogniteのセキュリティポリシーは、事業運営を支えるすべてのプロセスと情報に適用されます。Cogniteは、セキュリティトレーニング、コントロール、インシデント対応の要点がまとめられたISO 9001とISO 27001の認証を保有しています。これらのポリシーには、独立監査人によるレビューが毎年実施されています。また、クラウドサービスプロバイダーに対するセキュリティポリシーについては、契約前にレビューが行われます。
サイバーセキュリティに関するトレーニングプログラム	ID.AM-6 ID.GV-2 PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5	Cogniteは、クラウドベースのリソースへの電子的なアクセス権限を持つ従業員を対象に、セキュリティの基本やセキュリティとプライバシーの最新動向について教育するサイバーセキュリティトレーニングプログラムを毎年実施しており、サイバーセキュリティの実践と強化を図っています。セキュリティに関する役割や責任が割り当てられた従業員には、情報システムへのアクセスを許可する前や割り当てられた職務を遂行する前に、ロール別のセキュリティトレーニングを実施しています。また、機密情報へのアクセス権を持つ従業員には、定期的に各自の責任に関する注意事項をリマインドするほか、セキュリティ認識向上トレーニングを継続的に提供することで、最新の脅威とそれらの脅威を軽減するうえで対応するセキュリティ手法を理解できるようにしています。インシデントのシミュレーションや演習にステークホルダーが関与することで、Cogniteのポリシーと手順に沿った責任を強化します。トレーニングの電子記録は、業界標準に確実に準拠するため、Cogniteのセキュリティグループが保管します。
電子/セキュリティ境界	DE.CM-5 DE.CM-6 DE.CM-7 PR.AC-3 PR.AC-4 PR.AC-5 PR.AC-6 PR.AC-7 PR.PT-4 PR.PT-5	Cogniteのクラウドサービスプロバイダーのセキュリティ対策は、システム運用に必要な接続・通信のみを許可し、それ以外のポート、プロトコル、接続はデフォルトでブロックする「deny by default(拒否型)」です。接続は、クラウドサービスプロバイダーの境界保護デバイスを利用してシステム境界で管理されます。境界内の接続の管理には、IPフィルタリングとファイアウォールが使用されます。Cogniteでは、サービスやデータの保護に多層防御アーキテクチャを採用しています。これは、仮想化されたソリューションの運用に必要な接続と通信だけを許可し、その他すべてのポートや接続をブロックするというものです。クラウドサービスプロバイダーがロードバランサーを提供するのに対し、サービスプロキシはネットワークレベルでの展開の分離に役立ちます。この多層アプローチは、広範な全体への保護と同時に、詳細なサービス間レベルの制御と監視を兼ね備えています。 リモートアクセスを付与するには、まずお客様によるCogniteの承認が必要です。次に、サービスチームの担当者がリモートから接続するには、まず承認を得たCogniteのマネージャーからリモートアクセスの許可を得なければなりません。ユーザーはお客様環境に固有のIDとパスワードに基づく二要素認証によって識別されます。リモートセッションでは、情報漏洩を防ぐため暗号化が使われます。プラットフォームのトラブルシューティングや保守には、クラウド上の実稼働システムへの特権アクセスか昇格アクセスがお客様からユーザーに提供される必要があります。

管理策カテゴリー	管理策サブカテゴリー ID	Cogniteにおける NIST Cyber Security Framework 管理策への対応
情報の保護	PR.DS-2	Cogniteでは、Cognite Data Fusion®とクラウドサービスプロバイダーとの間で送信されるデータを保護するために「トランスポート層セキュリティ」(TLS: Transport Layer Security)プロトコルを採用しています。TLSによって強力な認証、メッセージのプライバシー、整合性が得られます。保存データの展開とリージョン単位の制限は、AES-256 によるCSPのデフォルトの暗号化とCSPによって管理されているキーを使用して行われます。情報が保存されているサーバーへのアクセスは、サーバーが存在するドメインのIDリポジトリのセキュリティグループメンバーシップによって制限されます。 Cogniteでは、運用モデルの変更がお客様主導の法規制要件に必要と思われる場合、契約交渉の一環として追加要件に対応しています。
悪意のあるコードの防止	DE.AE-2 DE.AE-3 DE.AE-4 DE.AE-5 DE.CM-1 DE.CM-2 DE.CM-3 DE.CM-4	Cogniteでは、最新の脅威情報に基づいてCognite Data Fusion®を侵入や悪意のあるコードから保護するため、CSPのイベント監視とログ機能をプラットフォームレベルで利用しています。監査ログのレビューは少なくとも週 1 回行われるほか、セキュリティインシデント、お客様の要求やエスカレーション、その他実稼働での機能に影響を及ぼすあらゆるインシデントに応じていつでも実施できます。セキュリティインシデントの調査をサポートする目的に加え、規制の保持要件を満たすため、ログは最低でも 90 日間保持されます。 情報の保護 Cogniteでは、Cognite Data Fusion®とクラウドサービスプロバイダーとの間で送信されるデータを保護するために「トランスポート層セキュリティ」(TLS: Transport Layer Security)プロトコルを採用しています。TLSによって強力な認証、メッセージのプライバシー、整合性が得られます。保存データの展開とリージョン単位の制限は、AES-256 によるCSPのデフォルトの暗号化とCSPによって管理されているキーを使用して行われます。情報が保存されているサーバーへのアクセスは、サーバーが存在するドメインのIDリポジトリのセキュリティグループメンバーシップによって制限されます。 Cogniteでは、運用モデルの変更がお客様主導の法規制要件に必要と思われる場合、契約交渉の一環として追加要件に対応しています。 Cogniteは、24 時間年中無休のサポートと監視を提供する以外にも、エスカレーションに対してオンコールエンジニアが常に交代で待機しています。営業時間外のオンコールエンジニアに対する重要アラートの緊急送信には、自動化されたソリューションを採用しています。オンコールエンジニアは事前に選定され、インシデントの特定、抑制、復元に必要な作業を行うためのロールが割り当てられます。オンコールエンジニアは、必要に応じて社内またはクラウドサービスプロバイダーへ追加のサポートを要請します。

管理策カテゴリー	管理策サブカテゴリー ID	Cognite における NIST Cyber Security Framework 管理策への対応
従業員に対するリスク評価プログラム	ID.GV-4	Cognite の人事部門が、契約社員やベンダーを含む全従業員に対して背景調査を行い、審査ポリシーを適用します。背景調査が必要になるのは、新入社員や顧客データにアクセスする可能性のある職務に異動する従業員です。背景の確認には、関連するプライバシー、個人を特定できる情報の保護、雇用に基づく法律が含まれます。情報の審査、開示、保持（7 年間）に関する調整は、Cognite の人事部門が行います。このプロセスについては、Cognite の「従業員の背景確認ポリシー」（Employee Background Verification Policy）で説明されています。
入館管理システムの保守およびテストプログラム	ID.AM-1 ID.AM-2	Cognite の CSP によって、少なくとも年 1 回すべての入館管理装置のインベントリが作成されます。さらに、データセンターの入館管理装置は警備システムに接続され、装置の状態が常時監視されています。そのため、装置が正常に機能していることを確認するためのテストを 24 か月ごとに別途行う必要はありません。入館管理装置の機能が停止した場合は、装置の異常を示すアラートが即座に発信されます。
警備計画	PR.AC-2 PR.AT-5	データセンターのすべての入口における入館許可は、Cognite の CSP によって実施されます。データセンターの建物の外観は目立たず、データセンターだと宣伝されることもありません。データセンターの設計によっては、入館バッジによる許可や警備担当者による許可を必要とする入館管理ゲートやセキュリティロック付きドアで、最初の入館許可が求められる場合があります。 データセンター施設へのメインアクセスは、警備員によって 24 時間体制で監視されている唯一の入口に制限されており、非常口には警報とビデオ監視装置が設置されています。データセンターのドアには、ドアが開けられたことや、許容時間より長くドアが開けられたままであることを知らせる警報装置が搭載され、ドアの警報が鳴った場合に CCTV カメラのライブ映像を表示するようにプログラミングされています。データセンターの受付エリアには警備デスクが設置されていて、唯一の入口が監視できるようになっています。さらに制御室の監視員が、警備が厳重で人の出入りの多いエリアに設置されたカメラからのライブ映像を監視しています。許可された人物のデータセンターへの入館のログは、90 日間保持されます。

管理策カテゴリー	管理策サブカテゴリー ID	Cogniteにおける NIST Cyber Security Framework 管理策への対応
ポートとサービス	PR.DS-1	Cogniteのクラウドプロバイダーのネットワークセキュリティは、システム運用に必要な接続・通信のみを許可し、それ以外のポート、プロトコル、接続はデフォルトでブロックする「deny by default(拒否型)」です。シリアルポートやUSBポートに接続されたデバイスには、対応するドライバーがないためアクセスできません。Cogniteは、IPフィルタリングやファイアウォールなど、クラウドプロバイダーのネットワーキング境界保護デバイスを利用してシステム境界で接続を管理しています。また、構成の問題を検出したり、CDFコンテナーのワークロード間のネットワーク接続を観察したりするために、サードパーティツールも利用しています。Cogniteでは、APIアクティビティやネットワークトラフィック、実行中のワークロードを常時監視し、異常な動作や既知の脅威に関するアラートを送信できるようにしています。
復旧計画の導入とテスト	PR.IP-4	CSPの災害復旧計画(DRP)チームによって、エンドツーエンドの復旧テストのスケジュールが立てられ、テストの実施、復旧におけるギャップの特定、テスト結果の連絡が行われます。毎年、主要エンドツーエンドシナリオが少なくとも1つテストされます。

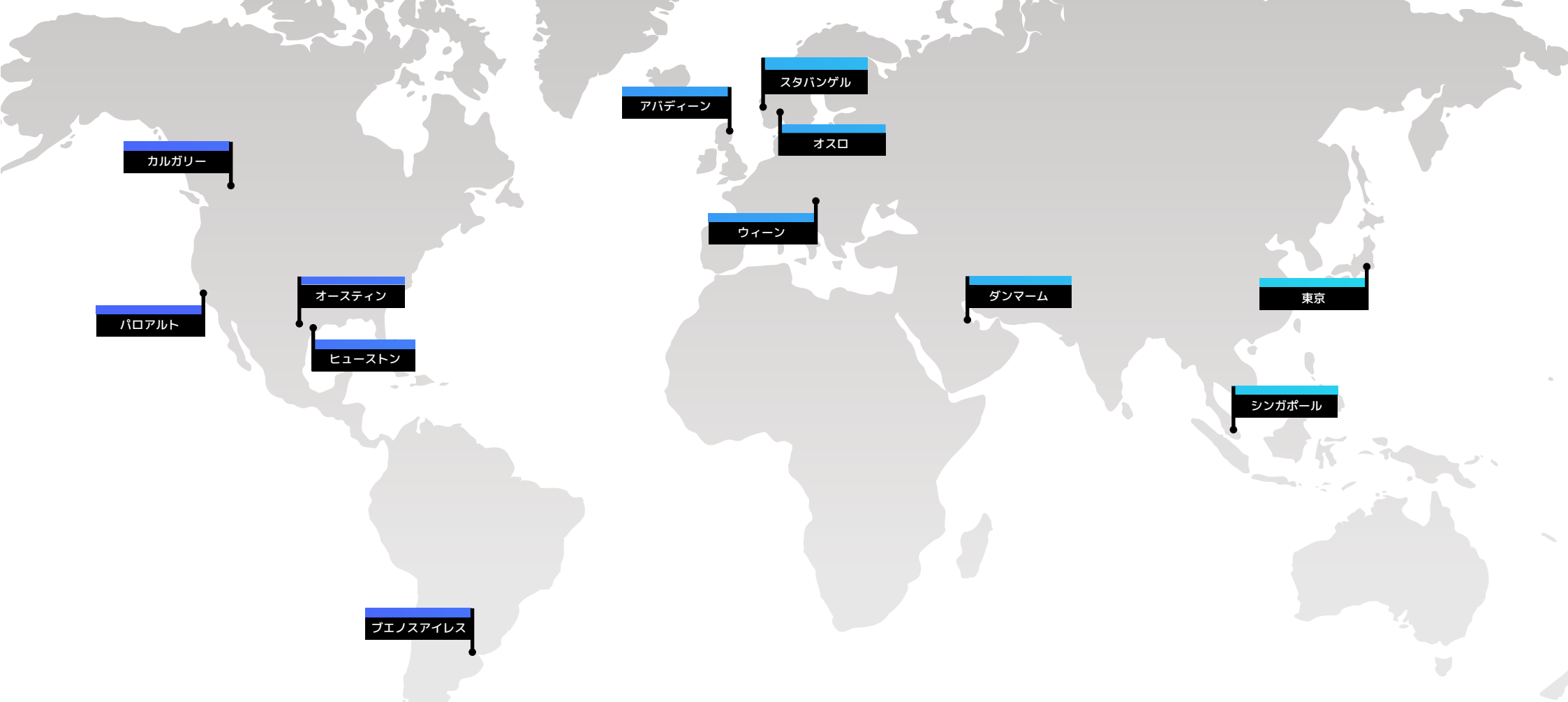
管理策カテゴリー	管理策サブカテゴリー ID	Cogniteにおける NIST Cyber Security Framework 管理策への対応
復旧計画のの詳細	PR.IP-10 PR.IP-5 PR.IP-6 PR.IP-7 PR.IP-8 PR.IP-9 RC.CO-1 RC.CO-2 RC.CO-3 RC.IM-1 RC.IM-2 RC.RP-1	クラウドサービスプロバイダーの「災害復旧計画」(DRP: Disaster Recovery Plan)では、関連するクラウドインフラストラクチャの緊急時対応に関する詳細なプロセスが規定されています。これらのドキュメントは、クラウドサービスプロバイダーが深刻なインシデントの発生時に対応、復旧、再稼働に当たる際のガイドとなります。DRPには、重要なテクノロジープロセスや業務の継続に欠かせない主な担当者、リソース、サービス、およびアクションが含まれています。この計画は、広範囲にわたるサービスの中断に対処することを目的としたものです。 クラウドサービスプロバイダーは、システムOSとお客様のイメージのバックアップをシステムで監視し、バックアップの失敗や不完全なバックアップをオペレーションチームに通知するアラートを生成しています。バックアップの完了時にはデータの整合性が自動的に確認されます。必要に応じて、レポートを生成して根本原因分析を行うために復元テストが取り込まれ、保存されます。監査情報の保護は、中央の監査収集システムに限定されます。許可された人物だけが監査記録にアクセスできますが、割り当てられた権限では監査情報の変更や削除を行うことはできません。 ディスクはすべてデータセンターで安全に管理されます。バックアップディスクは、長期保管用のオフサイト施設に移されます。ディスクのバックアップライブラリ、暗号化デバイスやサーバーは、データセンター内に置かれています。メディア(ディスク)やディスクのバックアップライブラリへのアクセスは、施設警備チームによって監視されます。安全な保管施設へのオフサイト輸送時には、ディスクはすべてオフサイト用コンテナーに入れられ、鍵がかけられます。ディスクはオープンラックに 1 枚単位で回収できるように保管されます。 Cogniteの「データの保持、アーカイブ、破棄ポリシー」(Data Retention, Archiving and Destruction Policy)では、特定カテゴリのデータの保持と破棄に関する原則が示されています。ビジネス継続性を確保するとともに、法律や法令、規制、契約上の義務への違反を回避するうえで、あらゆる形態の情報に対する適切な保護が求められます。記録の廃棄は、しかるべき保持·廃棄スケジュールに従って実施されます。機密情報は、内容の復元が不可能な方法で破棄されます。アーカイブされたドキュメントは 7 年間保持されます。情報の種類ごとに適切な破棄方法が承認される必要があります。デジタルメディアやコンピューターハードウェアドライブの適した廃棄方法には、裁断、焼却、溶解、粉砕などが含まれます(ただし、これらに限定されません)。

管理策カテゴリー	管理策サブカテゴリー ID	Cogniteにおける NIST Cyber Security Framework 管理策への対応
セキュア開発ライフサイクル(SDLC: Secure Development Life Cycle)	ID.RA-2 ID.RA-3 ID.RA-4 ID.RA-5 ID.RA-6 ID.RM-1 ID.RM-2 ID.RM-3 PR.IP-2	Cogniteのセキュア SDLC 手法は、体系的かつセキュアなソフトウェア開発ライフサイクル（SSDL）を実現するための確立された方法およびプロセスです。このアジャイルプロセスフレームワークでは、開発サイクルにセキュリティを取り入れます。ソリューションのアーキテクチャ、脅威モデリング、要件の見直しには、内部および外部からの脅威インテリジェンスが参照されます。静的および動的なコード分析を用いたセキュリティテストや脆弱性管理を導入することで、開発のあらゆるプロセスにセキュリティが組み込まれます。
セキュリティ認識向上プログラム	PR.AT-1	保護すべき情報と、情報を保護するために導入されたコントロールを踏まえ、Cogniteの情報セキュリティポリシーや関連手順に沿って情報セキュリティ認識向上プログラムが策定されています。Cogniteのセキュリティ認識向上プログラムは、Cogniteのポリシーや手順との整合性を確保するため、定期的に更新されます。このプログラムは、情報セキュリティインシデントから得られた教訓に基づいています。
セキュリティイベントの監視	DE.AE-2 DE.AE-3 DE.AE-4 DE.AE-5 DE.CM-1 DE.CM-2 DE.CM-3 DE.DP-3 DE.DP-4 DE.DP-5 PR.PT-1	Cogniteでは、最新の脅威情報に基づいてプラットフォームを侵入や悪意のあるコードから保護するため、クラウドプロバイダーが提供する広範なイベントの監視とログ機能をプラットフォームレベルで利用しています。監査ログのレビューが少なくとも週 1 回行われるほか、セキュリティインシデント、お客様の要求やエスカレーション、その他実稼働での機能に影響を及ぼすあらゆるインシデントに応じていつでも実施できます。セキュリティインシデントの調査をサポートする目的に加え、規制の保持要件を満たすため、ログは最低でも 90 日間保持されます。Cogniteは、24 時間年中無休のサポートと監視を提供する以外にも、エスカレーションに対してオンコールエンジニアが常に交代で待機しています。営業時間外のオンコールエンジニアに対する重要アラートの緊急送信には、自動化されたソリューションを採用しています。オンコールエンジニアは事前に選定され、インシデントの特定、抑制、復元に必要な作業を行うためのロールが割り当てられます。オンコールエンジニアは、必要に応じて社内またはクラウドサービスプロバイダーへ追加のサポートを要請します。

管理策カテゴリー	管理策サブカテゴリー ID	Cognite における NIST Cyber Security Framework 管理策への対応
セキュリティパッチ管理	DE.CM-8 PR.IP-12	Cognite Data Fusion® は、計画的なダウンタイムやパッチのインストールを必要としない SaaS プラットフォームです。脆弱性の検出と修正が絶えず行われます。脆弱性管理には、ネットワークのスキャンやコンテナーのスキャン、侵入テストが含まれます。スキャンは、脆弱な依存関係や公開されているシークレットの検出と修正に使われます。検出された脆弱性には評価とランク付けが行われ、開発者との間で軽減措置が合意されます。問題やバグなどの脆弱性が追跡され、軽減されるまで未解決事項として扱われます。 変更のテストと導入は自動化された CI/CD プロセスで行いますが、サーバーメトリックス、要求ログ分析、サポートチケットなどで問題が明らかになった場合は数分で元に戻すことができます。CI/CD パイプラインには、実稼働環境への展開承認の前提条件として静的アプリケーションセキュリティテスト（SAST）が含まれます。また Cognite では、認証された要求と認証されていない要求の両方に対し、セキュリティ侵入テストで動的アプリケーションセキュリティテスト（DAST）も実施しています。
サプライチェーンの サイバー セキュリティ リスク管理計画	ID.AM-4 ID.BE-1 ID.BE-2 ID.BE-3 ID.BE-4 ID.BE-5 ID.SC-1 ID.SC-2 ID.SC-3 ID.SC-4 ID.SC-5	Cognite の「サプライヤーセキュリティポリシー」（Supplier Relationships Security Policy）では、Cognite Data Fusion® のソリューションにコンポーネントを提供するサードパーティに対して情報セキュリティ目標が設定されるようにしています。全サプライヤーの情報セキュリティに関するアプローチとコントロールを完全に把握するため、デューデリジェンスを実施しています。Cognite の情報、情報システム、または情報処理設備のアクセス、処理、保存、通信、管理に関わるサプライヤーとの取り決めは、必要なセキュリティ要件を含む正式な契約に基づきます。 CSP のインフラストラクチャでは、14 文字以上で、大文字、小文字、数字、および特殊文字をそれぞれ 1 つ以上含む形で、大文字と小文字を区別するパスワードが適用されます。その他のリスク軽減策には、二要素認証の必須化が含まれます。このような二要素認証や多要素認証の導入に加え、ドメインに対して、パスワードの複雑性、パスワードの有効期限、パスワードの履歴、パスワードの最小長などのアカウントパスワードポリシーが施行されています。 サードパーティサプライヤーは、分類と使用計画に基づき審査されます。レビューの結果は、（1）合格、（2）改善が必要、（3）ベンダーまたはソリューションが不合格のいずれかです。サプライヤーのレビューに使われるソースには、ISO や SOC 2 Type 2 のレポート、サプライヤーから提供されたドキュメント、一般的な業界認定資格、Q&A などが含まれます。

管理策カテゴリー	管理策サブカテゴリー ID	Cogniteにおける NIST Cyber Security Framework 管理策への対応
システムへのアクセス制御	PR.AC-1	エンドユーザーアカウントの管理はお客様の責任です。CogniteのCSPは、アカウント管理にIDリポジトリを使用しています。ローカル管理者アカウントは名前が変更され無効にされます。ローカル管理者アカウントとネットワークデバイスのルートアカウントのデフォルトのパスワードが変更されます。アカウント所有者は、少なくとも 70 日ごとに共有アカウントの資格情報のローテーションを行う必要があります。また、人員に変更があった場合も、共有アカウントの資格情報のローテーションが必要になります。 CSPのインフラストラクチャでは、14 文字以上で、大文字、小文字、数字、および特殊文字をそれぞれ 1 つ以上含む形で、大文字と小文字を区別するパスワードが適用されます。その他のリスク軽減策には、二要素認証の必須化が含まれます。このような二要素認証や多要素認証の導入に加え、ドメインに対して、パスワードの複雑性、パスワードの有効期限、パスワードの履歴、パスワードの最小長などのアカウントパスワードポリシーが施行されています。 CSPは、ブルートフォース攻撃でパスワードの推測が試みられた場合、セキュリティ担当者に警告し、ブルートフォースで取得されたパスワードに関連するアカウントの権限を減らすために、追加の認証メカニズムを適用します。
一時的なサイバーアセットとリムーバブルメディア	DE.CM-5 PR.PT-2	Cogniteの「デバイス利用ポリシー」(Acceptable Use Policy)と「Bring Your Own Deviceポリシー」(Bring Your Own Device Policy)では、情報、電子データ、コンピューティングデバイス、ネットワークリソースの使用全般について規定しています。これらのポリシーによって、Cogniteの情報システムやアセットを、それらのセキュリティやパフォーマンス、キャパシティ、整合性に悪意または害を及ぼす意図をもって利用することや、Cogniteやその従業員、お客様、または社会全般に脅威や不利益をもたらす形で利用することを禁止しています。

管理策カテゴリー	管理策サブカテゴリーID	Cogniteにおける NIST Cyber Security Framework 管理策への対応
脆弱性の評価	DE.AE-2 DE.AE-3 DE.AE-4 DE.AE-5 DE.CM-1 DE.CM-2 DE.CM-3 ID.RA-1 PR.IP-12	Cogniteでは、インフラストラクチャ、サービス、アカウント、ログに脆弱性や異常なアクティビティが見られないか監視するために、「セキュリティ監査ログおよび監視ポリシー」(Security Audit Logging and Monitoring Policy)を採用しています。Common Vulnerabilities and Exposures(CVE)など、ソフトウェアの欠陥やセキュリティ構成、対象の製品名を項目別にまとめた、業界で認められた各種の既存オープンスタンダードに基づくレポートデータを提供する一般的なサードパーティツールのほか、カスタムツールやソリューションを利用しています。 また、内部だけでなくサードパーティのセキュリティ専門家や監査役による運用や環境のテスト、評価、監査も毎年行っています。報告または検出された問題や脆弱性は記録・追跡され、優先順位が付けられます。変更の導入に先立って、情報セキュリティ影響分析とそのレビューが実施されます。変更内容の分析は標準の変更管理プロセスの一環として導入前と導入後にそれぞれ実施され、変更によって期待された成果が得られることが確認されます。すべての項目に所有者と優先順位が指定され、情報が可視化されて管理・追跡されます。



↘ Cogniteについて

Cogniteは世界中の重厚長大産業の本格的なデジタルトランスフォーメーションをサポートするグローバルな産業用SaaS企業です。主要製品である産業向けDataOpsプラットフォーム「**Cognite Data Fusion®**」を利用することで、データユーザーやドメインユーザーは連携して産業用AIソリューションやアプリケーションの開発、実用化、拡張を迅速かつ安全に推進できるようになります。

Cognite Data Fusion®は、産業界のドメインナレッジを既存のエコシステムに適合するソフトウェアにコード化し、概念実証から真のデータ駆動型オペレーションへの拡張を可能にすることで、収益とサステナビリティの向上に貢献します。

ぜひ、www.cognite.comにアクセスし、Twitterや LinkedInでフォローしてください。

お問い合わせ

ソフトウェアに業界の深い専門知識を取り入れるユニークなグローバルチーム

10 人以上の国際情報
オリンピックメダリスト
15% が博士号を取得

Microsoft Google

ソフトウェア&データサイエンス

COGNITE

AkerBP SIEMENS ABB
Schlumberger ConocoPhillips

業界の専門知識

BCG Deloitte. McKinsey & Company
pwc

COGNITE

cognite.com →