OCPの情報セキュリティ内容

OCPとは？
OCPとはオンライン・クレーム・プラットフォームの略です。FSC®認証製品の取引情報を迅速に確認できるよう、FSC認証取得済みの供給者と顧客をデジタルで結びつけるものです。これにより、製品がサプライチェーンを下っていく過程で、FSC認証を確かめることができます。このシステムによって、FSCブランドはより確かな信頼できるものになるでしょう。

OCPによってFSC認証にかかる事務負担を大幅に軽減することができるとFSCは考えています。FSCでは、OCPとシステムが完全に統合された認証取得者について、CoC規格の大部分が自動的に満たされるようにする方法を開発しようとしています。これにより、FSCシステムがより確かなものとなると同時に、管理や監査プロセスにかかる時間を短縮できることでしょう。

もし詳細をご希望の場合は、ocp-info.fsc.orgをご覧ください。

どんなデータがOCPに収集される？

OCPには、info.fsc.orgで公開されている認証取得組織の認証データが入力されます。

OCPのユーザーは、供給者や顧客を見つけ、接続し、FSC認証製品の取引情報を記録することができます。

取引製品に関する情報で入力されるのは、取引識別番号、日付、表示タイプ、製品タイプ、取引量、および説明と種のみとなっています。

OCPで財務・機密情報を収集することはありません。

詳細をご希望の場合は、OCPヘルプサイト、特にOCPのデータフィールドをご覧ください。

OCP情報セキュリティの確保
FSCは、情報セキュリティ管理のための目標を設定し、FSCが管理する顧客、パートナー及びFSC自身の情報資産の保護に全力を尽くします。これには、2014年第３四半期までにISO27001認証を取得することが含まれます。ISO27001は、データ保護についての方針やデータ制御に関するガイドラインもある、世界的に認められたセキュリティ規格です。この規格では、リスク/脅威ベースの情報セキュリティマネジメントシステムの開発・展開および管理のための、国際的に合意された体系的なアプローチのベストプラクティスと要件を定められています。

これは実際どういうことなのかというと、

FSC International Center GmbH · Charles-de-Gaulle-Strasse 5 · 53113 Bonn · Germany·
T +49 (0) 228 367 66 0 · F +49 (0) 228 367 66 30 · fsc@fsc.org · www.fsc.org

Historic Futures
(HF)は適切に情報資産を管理する、情報セキュリティマネジメントシステム（ISMS）を運営・維持しています。それには、すべての情報資産が分類され、その情報がどのように扱われるか、明確なガイドラインが含まれています。

HFはISMSを支える社内指針と手順を実装・適用しています。管理システムの一貫として、HFは少なくとも年に一度、認証ヨーロッパと外部のセキュリティ専門家による監査を受け、順守を確認しています。

セキュリティ意識研修は、新人研修および継続的人材開発プロセスの一貫です。これにより、我々のチームが情報の安全性を確保するために必要な方針や手順を理解しているか、確認しています。

また、私たちは、不正アクセス、漏洩、改ざん、盗難/紛失、サービス拒否攻撃、またはその他の脅威から情報資産を保護するために、ISMSの制御によって、人、組織、および技術的なセキュリティ管理を行っています。

私たちは違反と真剣に向き合います。インシデントの発生時のために、セキュリティインシデントの発見、抑制、および回復を含む正式なインシデント管理プロセスを持っています。また、インシデント発生時はユーザーの皆様への通知を過剰なほど行います。

情報資産への脅威となるようなインシデントが発生した場合、ISMSを通じてHFは迅速に根本的原因を解明し、被害を最小限に食い止め、再発防止に努めます。

HFは、情報セキュリティに関連するすべての法律/規制上および契約上の要件に準拠し、情報セキュリティに関する英国の法律ガイドライン、業界標準とベストプラクティスを採用しています。

HFは手順の実行や見直し、内部監査を通じてこれらの活動を継続的に見直し、向上させます。

我々のISMS制御に沿って、独立した第三者、NCCグループによるOCPの定期的なセキュリティ侵入テストなど、セキュリティの弱点の検出と解決に取り組んでいます。

HFは、以下の法的/規制の枠組みに基づいてサービスを提供しています。
- 電気通信法
- データ保護法
- Historic Futuresの顧客との契約
- 第三者の法律専門家の助言

詳細はISO27100をご覧ください。

うまくいかない場合はどうなるの？
私たちは違反と真剣に向き合います。インシデント発生時に対処するための、セキュリティインシデントの発見、抑制、およびインシデントからの回復を含む正式なインシデント管理プロセスを持っています。また、その際はユーザーの皆様への通知とコミュニケーションを最重視します。

情報資産への脅威となるようなインシデントが発生した場合、ISMSを通じてHFは迅速に根本的原因を解明し、被害を最小限に食い止め、再発防止に努めます。

すべてのインシデントは、ISMSリスク管理手順に基づいて、その重大度に応じて等級分けされます。優先度2以上の重大度を持つすべてのインシデントは、独立した公開ウェブサイトocp-status.fsc.orgに掲載されます。（現在はhttp://ocpstatus.tumblr.com/）
OCPのユーザーはまた、発券システムへアクセスでき、ここから問題やインシデントの報告ができます。

以下はユーザーの皆様から最もよく寄せられる質問です。もし何か不審なものにお気づきの場合は、どうぞこちらからサポートデスクにご連絡下さい。

規格と規制

どんなセキュリティ規格と規制があるの？

HFは情報セキュリティ管理のための目標を設定し、FSCが管理する顧客、パートナー及びFSC自身の情報資産の保護に全力を尽くします。この一環としてHFは、データ保護についての方針やデータ制御に関するガイドラインが定められた、世界的に認められたセキュリティ規格であるISO27001認証を取得しています。
この規格には、リスク/脅威ベースの情報セキュリティマネジメントシステムの開発・展開および管理するための、国際的に合意された要件と、体系的なアプローチのベストプラクティスが定められています。

SAS70に準拠している？
国際的なセキュリティ管理規格ISO27001には、SAS70のセキュリティ証明に勝る利点があるため、HFはISO27001に準じてISMSを実施しています。ISO27001規格は、セキュリティ管理のベストプラクティスを具体的に示し、総合的なセキュリティ制御が含まれています。この規格への認証のために、HFは以下のようなことを行いました。

- 脅威と脆弱性の影響を考慮に入れながら、当社の情報セキュリティリスクを体系的に評価すること。
- 他の形態のリスク管理と情報セキュリティ制御セットを設計・実装し、会社と構造セキュリティリスクに対処すること。
- 情報セキュリティ制御が継続的に情報セキュリティのニーズを満たすよう、包括的な管理プロセスをとること。

現在進行中のこの認証の鍵は、厳格なセキュリティプログラムの効果的な管理にあります。ISMSの要件では、セキュリティを管理し続けるための全体的かつ包括的な方法が定められています。 ISO 27001認証では、HFのISMSに焦点が当てられ、我々の内部プロセスがどのようにISO規格に準じているかが評価されました。第三者によって認定された独立審査員による年次審査により、私たちのプロセスやコントロールが27001規格に準じて機能していることが確認されます。

SOC1/ SSAE16/ISAE3402（正式にはSAS 70）は、独立した審査員が対象会社の制御目標と活動について評価するのに使われる審査規格で、審査に通れば審査証明書が与えられます。ISO 27001は以前のSAS70証明と違い、継続的な改善モデルを通じて継続的な管理、リスクとコントロールの強化を必要とするため、世界的には、ISO27001がビジネスを保証するものとしてより多くの企業に利用されています。
HFのISMSへのコミットメントは、各規格の違いに基づき、以下の表にまとめられています。

方法	ISO 27001	SOC 1/SSAE, 16/ISAE 3402
事業における使用用途	経営管理要件	最低要件についての審査ガイダンス
保証	国際認証	サービス監査員による報告書
範囲	どんな情報やシステムにも応じる業務中心	財務中心（文書と関連システム）
スタンス	プロアクティブ（先を読んだ対処）	リアクティブ（後から対処）
リスク	特定、測定、修正	リスクを最大化した後軽減
コントロールの定義＆測定	各コントロールはISMSの要件として定義され、測定される	タイプ１監査報告書には知見は含まれるが、コントロールの試験や有効性は含まれない。 コントロールの試験は、タイプ３監査報告に含まれている
継続的改善	計画、実行、点検による更新義務	なし

どんなセキュリティ指針、規格が適用される？

HFでは、顧客、パートナー、そしてHF自身の情報資産を保護するため、業界のベストプラクティスに基づいて方針と手順を作成しています。通信および運用管理はHFの情報資産のセキュリティと情報処理環境全体の運用に関して計画・展開されています。

以下の指針と手順で基準が定められています。

- 情報セキュリティ方針
- クリアデスク、クリアスクリーン方針
- 資産処分方針
- 暗号化方針

- アクセス制御方針
- 使用許容方針
- モバイル･コンピューティングの方針
- ネットワークサービスの方針
- 情報交換方針
- 事業継続方針
- インシデント管理手順
- 情報分類手続き
- リスク管理手順

内部監査の手順：
- 文書・記録制御手順
- 是正措置手順
- 予防処置手順

各方針と手順には、ISO27001規格の適用性文書に義務付けられている制御と、HFがその情報資産を管理する方法が示されています。

誰が、HF ISMS方針を監査している？
認証ヨーロッパ

HFは2013年11月に外部のセキュリティコンサルタントから、セキュリティ状況とコミットメントはISO2700の意図するところをを満たすという証明書を受け、これが認証の皮切りとなりました。

2013年には外部のセキュリティ会社によって以下の点がISO27001に照らし合わせて検証されました：
- 管理システム文書
- リスク管理
- 文書＆記録管理
- 教育研修、意識・能力開発
- インシデント、是正及び予防処置
- 事業継続計画
- 制御の実装

HFは技術的コントロールの有効性についての侵入テストを完了します。

HFは独立した機関である認証ヨーロッパから認証を得るために、あらかじめ設定された手順を経てきました。認証審査は２段階あり、第１段階は５月に現場で行われ、審査員がHFのシステムが規格の要件を満たし、認証を受けることができるか判断します。第１段階に続く第２段階は、システムの有効性の審査です。認証を受けるためにはどちらの段階も完了しなく

てはいけません。第２段階は2014年6月に予定され、認証はその後に下りるとされています。

各段階は、現場で行われ、以下のものが含まれます：
·プロセス/活動とスタッフの観察
·文書、制御と記録の検証
·サイト管理やスタッフとの議論

HFが認証を保持するために、認証機関は、サンプリングにより、毎年HF ISMSの継続的な監査を行います。

誰がOCPの侵入テストをするの？
当社のISMS制御に従い、OCPは定期的に独立した第三者によってテストされます。現在のサービス·プロバイダは、NCC Secureです。

データと記憶装置

どこにデータが格納されている？
OCPのデータは、アイルランドのダブリンにある、Amazon Web Servicesの欧州データセンターでホストされています。
データセンターはAmazon.com社の子会社または関連会社であるAmazon Web Servicesが所有しています。アマゾンのグループ会社は、米国とEUが合意したセーフハーバープライバシー原則に従っていると保証しています。

詳細は、Amazonのセキュリティ情報をご覧ください。

オフサイトの記憶装置のリスクを評価したことがありますか？
HFは独立したセキュリティ会社を使ってホスティングソリューションのリスクの評価を行いました。その主要な目的は、ホスティングソリューションによって効果的で適切なセキュリティ制御が得られ、オフサイト処理および記憶装置を使うことにより新たなリスクが加わらないことをある程度確証することです。

Amazon EC2はセキュリティとデータ保護を維持するための規制、基準およびベストプラクティスに準拠し、あるレベルの保護が保証されています。準拠しているものには、ISO27001, HIPAA, SOC 1/SSAE 16/ISAE 3402 (formerly SAS70), SOC 2, SOC 3, PCI DSS レベル1, FedRAMP(SM), DIACAP and FISMA, ITAR, FIPS 140-2, CSA, MPAAが含まれています。

このシステムは、2つのAmazonアベイラビリティゾーン（2つの異なるデータセンターに相当）を越えて、同時に機能します。 （2014年春現在は1つのデータセンターのみ運用中）

アクセス制御

OCPデータには誰がアクセスできる？
認証データには、アカウント所有者、アカウント管理者がアクセスでき、ユーザーのアクセス許可は、OCPサービス内からOCPアカウント管理者が管理しています。

認証製品の取引データは、内容を確認する際、取引に関わる両者が見ることができます。

アマゾンのAWSの管理者は、顧客のデータへのアクセスがなく、ゲストOSにログインすることもできません。

Historic
Futures、FSCサポートおよび認証機関は、アカウント管理者によって許可されない限り、日常的にデータにアクセスすることはできません。

詳細は、利用規約全文をご覧ください。

利用規約には「FSCはHistoric
Futuresに対して、よく機能するシステムを保証するためにユーザーの口座から生じる活動を随時確認、および/または保持することを許可し、準拠法、規制、法的手続き、訴訟の可能性、または政府による公式要請の遵守のために必要な範囲において情報を開示する権利を留保する。」と記されています。これはつまり、認証取得者（CH）がOCPについて質問/問題があり、サポートスタッフとOCPのアカウント情報を共有する必要がある場合は、CHの要請後、CHを助けるという目的のためだけにFSCがそのCHのアカウントにアクセスすることになるということです。

Amazonの物理的なセキュリティコントロールは？
データセンターへの物理的なアクセスはビデオ監視、最先端の侵入検知システムとその他の電子的手段により、プロのセキュリティスタッフによりビルの入口とその周辺の両方で厳密に制御されています。許可されたスタッフでも、データセンターにたどり着くまでに、少なくとも3回は2要素認証を経なくてはなりません。訪問者や請負業者には全員、身分証明書の提示が義務付けられており、サインインの後も常にスタッフの付き添いが必要とされます。

システムへの不正アクセスやデータセンターへの物理的アクセスからデータを守るための手順
改変、破壊や情報の不正発信などの悪用に関するリスクを抑えるために、HF情報資産は必要に応じてアクセスされます。
HFの情報セキュリティ方針によって、アクセス管理の基準が設定されています。
これには、以下のものが含まれます。
- ユーザー登録および識別

役割と責任
- 所有者によるアクセスの承認
- ユーザー認証
- ユーザー承認

- 権限管理
- オペレーティングシステムの制御
- ネットワークアクセス制御
- ユーザーパスワード管理
- アクセス権限の見直し
- リモートアクセス

インシデント管理と災害復旧

停電・火災・災害時のバックアップや復元
マスターデータベースは、Amazon
S3に毎時バックアップされます。一万件ごとにバックアップ履歴が更新されます。

OCPは複数のデータセンター間で切り替え可能？
OCPは、複数のデータセンター間で機能するように設計されていますので、１つのデータセンターの故障でサービス全体が止まることはありません。

災害復旧計画（DRP）
OCPシステムは、一般的な仮想マシンから作られており、１つのマシンの故障でサービス全体が止まることがないように設計されています。各サーバーは、標準的なものから作られているので、必要に応じて数分以内に再構築することができます。

パフォーマンスレベルの監視
世界中各地からのシステムの稼働時間と応答時間の監視には、Pingdom.comが提供する独立サービスが使われています。 FSCはHistoric
Futuresと、システムの応答時間についてSLA契約を結んでいます。

OCPサービスのアップタイム性能目標は？
合意されたアップタイム/可用性SLAは毎月測定され、99%です。

ウイルス、悪意のあるコード、および不正ソフトウェアからの保護の手順は？
HFの情報セキュリティ方針は、セキュリティの傾向を見定め、異常を検出する仕組みを監視するための基準を定めています。異常があれば、セキュリティ事故を示唆するものであるかどうか検証されます。事故は報告・検証され、通常の事業活動に早く戻れるよう、補正されます。このプロセスには、事故の検出と応答および脆弱性の管理が含まれています。

ソフトウェアの破損やデータ損失からの保護の手順は？
HFが新しいシステムや既存のものから変更などを提案する場合には、システムのセキュリティ面も分析や仕様に含まれています。これらの仕様には、リスクアセスメントでサポートされている自動と手動のセキュリティ対策が含まれています。
これらの基準には、以下のものが含まれます：

- システムファイルのセキュリティ

- システムの計画、受け入れと買収
- システム開発
- データ検証

HFは、災害や業務中断などの影響を最小限にするべく、利用事業継続計画（BCP）を使っています。事故などで資産が破壊され利用できなくなった場合にも、業務が引き続きできるようにするための文書化されたプロセスがHF内のBCPにはあります。災害復旧計画（DRP）は、災害などにより資産が業務に使えなくなった後、IT資産を回復するプロセスです。

ビジネス回復の基準には、以下のものが含まれます。

- プランニング
- テスト
- メンテナンス
- 意識
- バックアップと復旧

セキュリティ上の問題は、
私たちの発券システム：support@ocphelp.zendesk.com
からご報告ください。

指定されたセキュリティ･オフィサー/個人情報ディレクターがいるのですか？
ISMS要件に従い、Historic Futuresには、指定されたセキュリティ所有者がいます。

緊急事態が発生した場合、FSCはいつどのように知らせてくれるのですか？
すべてのインシデントは、ISMSリスク管理手順に沿って、その重大度に応じて等級分けされます。優先度2以上の重大度を持つすべてのインシデントは、独立した公開ウェブサイトocp-status.fsc.orgに掲載されます。（現在はhttp://ocpstatus.tumblr.com/

私のデータに関連する個人情報関連の問題やインシデント（例：個人情報侵害）は全て通知されますか？
HFはセキュリティや個人情報インシデントが発生した際は必ずインシデント管理手順を実行します。応答はものによって違いますが、過剰なほどのコミュニケーションを心がけています。