IT@Intel ホワイトペーパー

インテル IT 部門

IT ベスト・プラクティス

IT の継続性

2012 年 3 月

インテル IT 部門：危機発生時における事業継続性の確保

インテル IT 部門は、過去の災害発生時に事業継続計画を実行に移した経験から、ノートブック PC の利用、工場とデータセンターの冗長化など、非常に効果的ないくつかのプラクティスを確立しました。

Virgil Fleming
インテル IT 部門
インテル情報リスク & セキュリティー
IT ビジネス継続性プログラム・マネージャー

富澤 直之
インテル株式会社
情報システム部長

概 要

インテル IT 部門の危機対応および復旧管理（ITRRM）プログラムは、災害発生時にインテルの基幹業務プロセスの継続性を確保し、災害沈静後の復旧を支援するためのプログラムです。この事業継続（BC）計画が実行に移された最近の例としては、昨年発生したマグニチュード 9.0 の東日本大震災が挙げられます。地震は金曜日の午後に発生しましたが、被害を受けたつくば本社の従業員は、月曜日の朝には遠隔勤務によって業務に復帰していました。

インテル IT 部門の ITRRM プログラムは、インテルの危機管理プログラムの一部であり、まず第一に従業員とその家族の安全を確保するという基本的な目標を共有しています。具体的には、リスクやビジネス要件に合わせて、対応と復旧のための事業継続（BC）機能を提供することが目的です。ITRRM プログラムは、業界標準規格、各種規制、ベスト・プラクティスに基づいています。この情報は、次のような継続的な改善サイクルの中で使用されます。

- プログラムのポリシーとインフラストラクチャーを構築し、維持する
- BC 計画オーナーによる計画の策定、維持、テストを支援する
- 計画の監査、実際の災害から得られた教訓、業界全体の既知の最適手法など複数の要素を考慮した上で、プログラムと計画を改善する

ITRRM プログラムは、BC 計画の策定に必要な支援とリソースを BC 計画オーナーに提供します。この BC 計画は、インテル全体の BC 戦略と整合性を持ちつつ、災害の各段階（準備、対応、復旧、修復）に対処するものでなければなりません。インテル IT 部門は、過去の災害発生時に BC 計画を実行に移した経験から、ノートブック PC の利用、工場とデータセンターの冗長化など、非常に効果的ないくつかのプラクティスを確立しました。

地震、洪水、停電、伝染病、サイバー犯罪など、事業継続の脅威となり得る災害の種類は少なくありませんが、ITRRM プログラムは、インテル IT 部門およびそのサポート対象であるインテルの各事業部が災害の発生後も安全性と生産性を維持できるように支援します。

目 次

IT@Intel

IT@Intel は IT プロフェッショナル、マネージャー、エグゼクティブが、インテル IT 部門のスタッフや数多くの業界 IT リーダーを通じ、今日の困難な IT 課題に対して成果を発揮してきたツール、手法、戦略、ベスト・プラクティスについて詳しく知るための情報源です。詳細については、http://www.intel.co.jp/jp/go/itatintel/ を参照してください。あるいは御社担当のインテル社員までお問い合わせください。

背 景

昨年発生した東日本大震災の際、インテルのつくば本社では、金曜午後の地震発生から 3 日後の月曜の朝には、300 人以上の従業員が遠隔勤務によって業務を再開しました。

インテルは 62 カ国の 164 拠点に 91,500 人以上の従業員を擁し、24 時間 365 日体制で工場と IT データセンターを運用しています。インテルの事業の性質上、強力な危機管理プラクティスと復旧計画が不可欠です。インテルは、東日本大震災のような大災害の発生時および発生直後も、従業員、顧客、株主に対して安全性と生産性を維持しなければなりません。さらに、事態が沈静した後は、業務への影響を最小限に抑えて迅速な復旧を実現する責任を負っています。

インテルの事業継続（BC）計画には、ビジネスシステムの大幅な中断を回避するための包括的なアプローチが求められます。そのため、インテルは以前から BC 戦略を重視し、IT 部門を含むインテルの各ビジネスグループに対して BC 管理プログラムの策定を求めてきました。

インテルの BC プログラムは、1970 年代に企業リスク管理プログラムの開始とともに始まりました。2001 年 9 月 11 日には、ニューヨーク・テロ事件が発生し、事業継続性管理がすべてのビジネスグループに義務付けられました。その後、さまざまな脅威が登場し、インテル IT 部門を含むすべてのビジネスグループが確実な BC 戦略を持つことの重要性はさらに高まりました。

インテルの成功は、オフィスと（さらに重要な）工場の継続的な運用にかかっていますが、インテルのオフィス、工場のいずれも IT への依存度を増しています。IT 危機対応および復旧管理（ITRRM）プログラムは、緊急事態発生時のインテルの事業継続能力の中核を成しています。

ソリューション

インテル IT 部門の危機対応および復旧管理（ITRRM）プログラムは、インテル危機管理（ICM）プログラムの一部です。ICM プログラムの目的は、危機発生後に従業員およびその家族の安全と業務の継続性を確保することです。ICM は、全般的な復旧活動を促進するとともに、インテル IT 部門を含む各ビジネスグループに対して、基幹業務系の機能とプロセスについての具体的な継続計画の策定を義務付けています。さらに、これらの BC 計画は、継続的な管理および改善プロセスの一環として、年 1 回以上検証されることになっています。

ICM プログラムの成功には、以下の 4 つの条件が必要となります。

- 企業全体の緊急対応および緊急管理機能の整備された基盤
- BC に対する経営管理者レベルの支援と資金的バックアップ
- 各ビジネスグループが BC プログラムを保有すること
- 実際の危機への対応と復旧作業に関する実証済みの結果

図 1 に示すように、ICM プログラムは、各ビジネスグループが策定した重点的な管理プログラムの監督と支援を行います。その対象となるプログラムの 1 つが、IT 危機対応および復旧管理プログラムです。

IT 危機対応および復旧管理 (ITRRM) プログラム

IT 危機対応および復旧管理 (ITRRM) プログラムでは、想定外のあらゆる事態に対する IT 部門の対応および復旧活動が対象となります。ITRRM の目標は、リスクとビジネス要件に合わせて、復旧のための能力とリソースを提供することです。具体的には、以下のプロセスで構成されます。

- 新しい脅威やリスクについての予防的評価を行い、プライバシー / 脅威調査チームと協力して、脅威の影響を回避または軽減するための対策をとる
- できる限り速やかに通常業務への復帰を可能にする、緊急対応および復旧機能を開発する
- 危機発生時にはリーダーシップを発揮し、効果的なコミュニケーションを実践する

ITRRM プログラムは、IT 緊急対応プロセス (ITERP) チームと IT BC 管理 (ITBCM) チームの 2 つのチームで構成されます。IT 緊急対応プロセス (ITERP) チームは、発生した想定外の事態への対応にあたり、業務への影響を軽減します。IT BC 管理 (ITBCM) チームは、BC プランニング・ツール、トレーニング、評価、コンプライアンス対応を担当し、IT 運用の耐障害性と緊急事態への備えを実現します。

2 つのチームは、緊密な協力関係の維持と業務横断的なメンバー構成によって、それぞれの活動とプロセス調整を行います。各チームについて、次に詳しく説明します。

IT 緊急対応プロセス (ITERP) チーム

ITERP チームは、IT 部門の緊急対応活動の中心です。このチームは、業務への影響を最小限に抑えながら、被害の迅速な隔離、軽減、復旧に取り組むことで、IT 部門があらゆる想定外の事態に対応できるようにします。ITERP チームは、米国連邦緊急事態管理庁の災害対応基準に基づいたインシデント管理原則を使用して、チームの戦略を策定しています (図 2 を参照)。

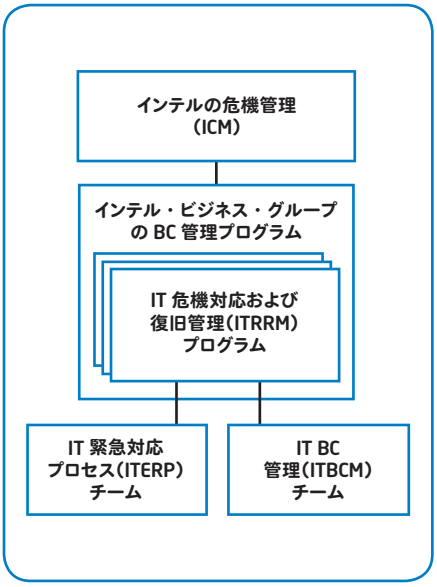

図 1. インテル IT 部門の危機対応および復旧管理プログラムは、インテル危機管理プログラムの一環として、2 つのチームで構成されます。

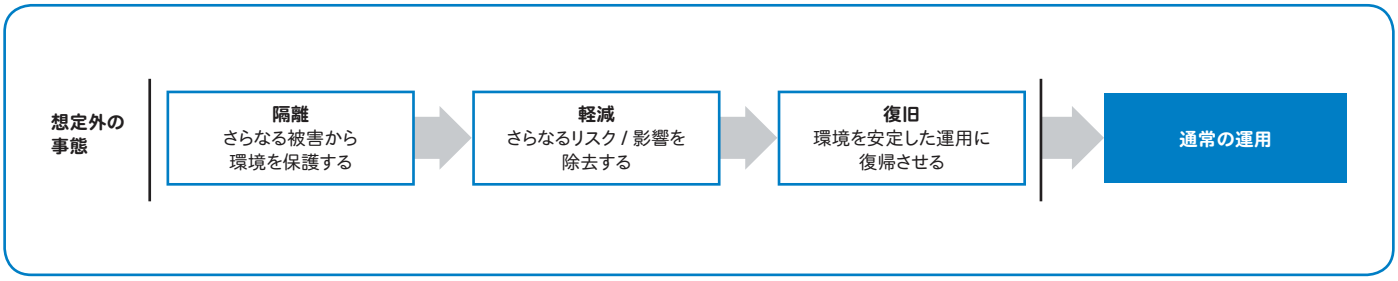

図 2. IT 緊急対応プロセス (ITERP) チームは、米国連邦緊急事態管理庁の災害対応基準に基づいたインシデント管理原則を使用して、想定外の事態に対応します。

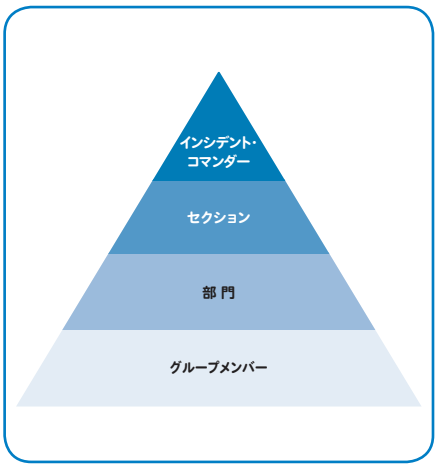

図 3. 米国連邦危機管理庁のインシデント・コマンダー構造に従ってモデル化された、危機管理に使用されるピラミッド型構造。リソースは必要に応じて有効化されます。

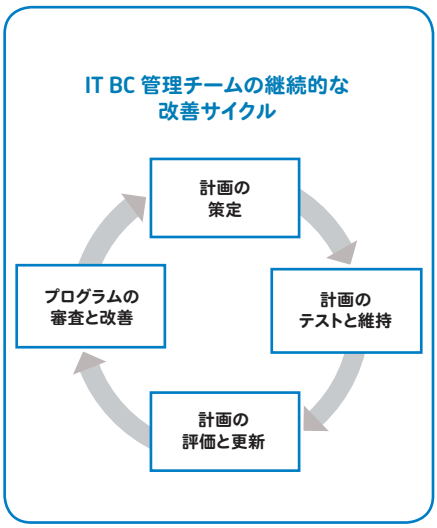

図 4. IT BC 管理（ITBCM）チームのプロセスと手法は、継続的な改善サイクルの中で実行されます。

図 3 に示すように、ITERP チームは IT 部門の各分野の代表者で構成されます。インシデント・コマンダー（IC）は、すべての対応と復旧活動を指示し、必要に応じてさまざまなセクションや部門、グループから適切なリソースを集めます。IC は事態のオーナーとしてリーダーシップを発揮し、指令系統の上流から下流へと情報を伝達します。想定外の事態が発生した場合、チームの全メンバーはすべての問題が解決するまで、通常業務ではなく、緊急対応時の役割を果たします。ITERP チームは発足から 11 年間で、IT 部門による危機の管理、調整、制御、伝達活動の成功にとって不可欠な存在になりました。

IT BC 管理（ITBCM）チーム

IT BC 管理（ITBCM）チームは、BC 計画と復旧計画を維持、管理するために必要なツール、プロセス、トレーニング、評価、コンプライアンス対策を担当することで、IT 運用の耐障害性を高め、インテルの法令遵守と安全性を実現します。ITBCM チームは、「クリティカル」に分類される IT インフラストラクチャー、アプリケーション、サービスに関する 600 以上の有効な BC 計画の支援と審査を行います。

ICM が全体的な活動を促進するのに対して、ITBCM チームは、パフォーマンス目標、プログラム管理、レコード管理の概要を定義し、BC プログラムの詳細なガイドラインと要件を確立します。さらに、IT BC 計画の作成を支援するツールを提供するほか、大規模で業務横断的な統合された防災訓練、テスト、演習を計画、実施し、各計画の監査も行います。

ITBCM チームによるプロセスと手法は、図 4 に示す継続的な改善サイクルの中で実行されます。これについて以下に詳しく説明します。

計画の策定

個々の計画オーナーは、ITBCM チームが提供するツールとトレーニングを使用して、プログラムのガイドラインと要件に基づいた計画を策定します。インテルの BC プログラムは、災害の脅威それ自体ではなく、災害がもたらす影響を評価する、業界の標準的な計画手法を採用しています。例えば、BC 計画では、吹雪、地震、倒木などの停電の原因ではなく、停電の影響が評価されます。

具体的には、計画オーナーは、リスクの評価と各リスクの制御手段の指定、ビジネスへの影響の評価、その影響に対処する戦略の策定、緊急事態への備えと対応能力の開発を行います。

BC 計画では、コミュニケーションと警告の発信方法、リソースの管理方法、主要な対応要員への危機情報の伝達方法、緊急対応チームのメンバー構成、組織、トレーニングについて規定します。

計画のテストとメンテナンス

IT 部門は、いったん策定された計画および手続きの内容とその有効性を維持するために、トレーニングを開発し、計画のメンテナンスおよびテストの頻度と評価基準を次のように規定します。

- BC 計画の審査
- 計画のテストと演習の開発
- 計画のメンテナンス要件の定義
- 計画のメンテナンスとテストのための役割と責任の定義
- 役割と責任を受け持つ各個人が適切なトレーニングを受け、すべての計画文書にアクセスできることの確認

ITBCM チームは、すべての重要な計画が一連のメンテナンスおよび検証要件に適合していることを、毎年の防災訓練時に実際に確認します。過去 3 年間、インテルの IT BC 計画はこれらの要件に 100% 適合しています。

パフォーマンスの評価と計画の更新

計画オーナーは、策定された計画がテスト時あるいは実際の災害発生時の対応と復

旧にどれほど効果があったかを検証し、その結果に基づいて計画の更新と改善に取り組みます。計画オーナーは、測定基準を使ってパフォーマンスを測定し、実行された対応処置と予防処置を検証し、特定された問題点や改善点に基づいて計画を更新します。

ITBCM チームは、内部監査を実施して、計画が要件に適合しているかどうかを確認します。これらの監査では、計画の品質を検証し、必要な要素が含まれていることを確認します。また毎年防災訓練を実施して、必要な改善点を把握し、問題点の解決に必要な作業を記録します。

プログラムの審査と改善

ITBCM チームは、すべての IT BC 計画を審査し、インテルおよび IT 部門の上位管理者にその結果をフィードバックします。このフィードバックには、個々の計画の監査結果、実際の災害への対応から得られた結果、テストと防災訓練で見つかった問題点や改善点、全体的なプログラムの測定基準の記録が含まれます。また ITBCM チームは、新しいテクノロジーなどがもたらす長期的な変化、ビジネスの優先順位の変化、高度化するリスク、新しい基準や規制など、プログラムに影響を与えるその他の要素も継続して確認します。これらのフィードバックと新しい情報は、インテル IT 部門の BC プログラムおよび BC 計画の継続的な策定と改善にも影響を与えます。

効果的な事業継続性のための ベスト・プラクティス

過去十数年の中で、ITRRM 戦略の試金石となる自然災害や人的災害がたびたび発生しました。これらの災害には、9.11 NY テロ、東日本大震災、重症急性呼吸器症候群（SARS）の発生、ハリケーンカトリーナ、中国四川省大地震、多数のサイバー攻撃のほか、悪天候による旅行制限、水道管破裂、停電など、小規模の局地的な災害も含まれます。こうした災害によって BC 計画が検証された結果、事業継続のための最も効果的なプラクティスが確立されました。

ノートブック PC などのテクノロジーの利用

インテル IT 部門では、各種の災害局面におけるビジネスの継続に、ノートブック PC が極めて有効であることを確認しました（表 1 を参照）。移動の多いインテルのユーザーが使うシステムをノートブック PC プラットフォームに標準化することで、従業員はほとんどの場所から、安定したコンピューティング機能を安全に使用して仕事ができます。

表 1. 災害局面でノートブック PC によってビジネスの継続性をどのように確保するか

災 害	ノートブック PC の効果
震災によって日本のインテルの拠点が被害を受けた。	インテルのつくば本社では、300 人以上の従業員が、オフィスの修復および改修ができるまでの 8 カ月間、インターネット・アクセスを利用して、在宅勤務、代替オフィスでの勤務、または他の拠点での勤務を行いました。
水道管の破裂のためインテルの拠点が利用不能になった。	450 人の従業員が、修復工事中の最大 2 カ月間、出張者向けワークステーション、会議室、カフェテリアなどのオンサイト・ロケーションで勤務するか、または在宅勤務を行いました。
吹雪のため道路が危険な状態になり、複数のインテル拠点への通勤が阻まれた。	5,000 人の従業員が 3 日間在宅勤務を行いました。
重症急性呼吸器症候群（SARS）の発生により、インテルのオフィスが閉鎖され、アジア数カ国への渡航が制限された。	従業員は在宅勤務を行いました。出張先で足止めされた従業員も、それぞれの滞在地から仕事をすることができました。
頻発する短時間の停電によって、インドのインテル拠点が影響を受けた。	短時間の停電の間ノートブック PC をバッテリー電源に切り替えることで、従業員の生産性を維持できました。

インテル危機管理（ICM）

危機の種類を問わず、インテルにとって最優先の課題は、従業員とその家族の安全を確保することです。インテル危機管理（ICM）は、問題の最初の兆候が現れた時点で、状況の評価、必要に応じた建物からの避難、できる限り速やかな被害の封じ込めを実行します。どのような手続きがとられるかは、そのときの状況によって決まります。安全な復旧作業が可能となった時点で、インテル IT 部門は、データセンターの被害の評価を行い、データセンターのオンライン状態の確認またはオンライン状態への復帰作業を行います。

ICM プログラムの成功には、長期的な取り組みと、インテルと IT 部門の上位管理者からの支援が不可欠です。支援の内容には、プログラムの範囲の定義、プログラムポリシーの策定と審査、そしてプログラムの組織的リーダーシップとチームの開発が含まれます。2001 年 9 月 11 日のニューヨーク・テロ事件以来、インテルの各ビジネスグループには、より多くの基準や規制に従い、はるかに強力な BC プログラムを用意することが求められています。

インテル IT 部門の BC プログラムの現在のガイドラインは、新しい規制と今後適用される可能性のある規制、業界標準規格、ベスト・プラクティスから得られる外部のガイドラインを統合したものです。例えば、Disaster Recovery Institute International（DRII）基準および ISO 基準に基づくガイドラインが組み込まれています。

災害の発生に対応したインテル IT 部門の活動

災害が発生したときもインテル IT 部門はビジネスの運用を継続し、時には通常の 60% のスタッフでさまざまな対応にあたることもありました。従業員との連絡確保による安全確認、代替オフィスの提供、自宅または必要な IT 通信機能を備えた他の安全な場所で仕事ができる機能の提供、基幹的な IT ビジネスサポート機能の移転、（バックアップ・システム、代替 IT データセンター、リモート・データ・アクセスを使用した）システムの復元作業などの活動は、インテルに限らず、あらゆる IT 部門に共通します。

さらに、あまり一般的ではないインテル IT 部門独自の活動としては、以下のものがあります。

- 災害地への人道支援をサポートするため、救援機関にネットワークとコンピューターを提供
- 内部および外部の Web サイトやソーシャル・メディア・サイトへの投稿、インテルの従業員とその家族のための緊急時通話料金無料電話番号によるメッセージ録音サービスなど、災害関連情報の伝達
- 二次供給メーカーの安全を確保し、サプライチェーンの問題を軽減

インテル IT 部門の目標は、災害の混乱の中でも従業員が生産性を維持して仕事を続けられるようにすることです。

インテル IT 部門は、いくつかのテクノロジーを追加して、こうしたモバイル作業環境をサポートしています。まず、ビデオ会議を使用することで、従業員は離れた場所にいても会議や共同作業が可能になります。ユニファイド・メッセージングは、ボイスメールを含むすべてのメッセージングを PC 上で可能にします。エンタープライズ・ポータルとインテルの Virtual Private Network（VPN）により、従業員はネットワークへのアクセスさえ確保できれば、どこからでもエンタープライズ・アプリケーション、Voice over IP（VoIP）やその他のサービスに安全にアクセスできます。また、インテルの標準ビルドの一部としてフルディスク暗号化がインストールされたことで、ノートブック PC が紛失や盗難にあった場合でも、そこに格納されている情報の安全性が確保されるようになりました。インテル® vPro™ テクノロジーに対応したビジネス PC の保守管理については、インテル IT 部門はリモートから実行しています。このことは、災害発生時だけでなく、通常の運用時における従業員の生産性維持にも役立ちます。

さらに、インテル IT 部門は、災害発生時の通信システムの支援には Wi-Fi* テクノロジーを使用してきました。例えば、ハリケーンカトリーナの通過後、ニューオーリンズ地域の固定通信システムは破壊されていました。インテル IT 部門は、衛星放送を使用した無線通信網を構築し、そこにノートブック PC を接続し、人道支援団体および救援機関用の通信センターを立ち上げることで、災害復旧活動を支援しました。同様に東日本大震災では、社員による IT 復旧支援チームを東北地方の避難所に派遣し、PC と WiMAX* ワイヤレス・ブロードバンド・システムを利用したインターネット接続環境を避難所 9 カ所に設置しました。万一、災害によってインテルの拠点の固定通信システムが破壊された場合、インテル IT 部門はこれと同じ手法を適用できます。

データセンター間にまたがるようにミッション・クリティカル・システムを配置

インテル IT 部門は、インテルの組立・検査工場のオートメーション・システムを 24 時間 365 日体制で運用しています。そのため、データセンターのどこか 1 つにでも問題が発生した場合に備えて、アプリケーション、ストレージ・エリア・ネットワーク（SAN）、ネットワーク接続型ストレージ（NAS）システムなどのミッション・クリティカルなシステムを、同じ拠点に置かれた 2 つのデータセンター間にまたがるように配置するという、コスト効率に優れた手法を開発しました。

この手法により、通常は 24 時間以上かかる SAN の復旧をわずか 1 時間で行うことができました。

低コストの災害復旧拠点をデータセンターとして利用

災害復旧（DR）拠点は、通常、災害の発生に備えた高額な保険と考えられています。そこで、インテル IT 部門は、低コストのデータセンター向け DR 戦略を作成しました。この戦略は、サーバーの使用率の最大化、低コストのシリアル ATA ディスク上で階層化したストレージシステムの使用、メイン・データセンターから DR 拠点へのバックアップ・サービスの振り分けで構成されます。

インテル IT 部門は、防災訓練の際、DR 拠点とメイン・データセンター間のネットワーク接続を約 24 時間切断し、メインサイトがダウンした状況のシミュレーションを行いました。その DR 拠点では、IT 部門のスタッフとマイクロプロセッサーの設計エンジニアで構成されたチームが DR 環境を立ち上げ、サービスの 95% を回復できました。災害局面以外では、DR 拠点のコンピューティング・リソースは高い使用率で最大限に活用されます。

工場の冗長化

1980 年代以来、インテルが世界各地に工場を建設する際には、柔軟性と冗長性を重視して、プロセスおよび製品の観点からは全く同じに見える工場を建設してきました。IT 部門は、広い地域に分散し、冗長化された製造工場をサポートするサービスを提供しています。災害の影響から工場を守るためのこうした手法により、世界のどこかで災害が発生した場合でも、インテルの製造環境の継続は可能となります。

データセンターの完璧な複製

インテルの製造環境は 24 時間 365 日体制で IT システムを利用しているため、インテル IT 部門では工場専用のデータセンターを用意しています。データセンターの障害が発生した場合にも工場の稼動を維持するため、インテルは過去数年間、新しいソリューションの導入時に「Copy Exactly（完璧な複製）」手法で多額の投資を行ってきました。

「Copy Exactly」手法では、まず 1 つの工場にデータセンター・ソリューションを導入します。導入に成功したら、そのソリューションを他の複数の工場環境にコピーします。ある工場のデータセンターに致命的な障害が発生した場合は、製造環境をサポートする IT システムを、他の工場のデータセンターに迅速に移行します。これにより、複製されたデータセンター・ソリューションを使用して、直ちに製造を再開できます。このような活動の結果、2009 年以来、データセンター施設の障害が原因でインテルの工場が稼動停止したことはありません。

クラウドによる重要な機能のホスティング

インテル IT 部門は、エンタープライズ・プライベート・クラウドの開発と実装を完了し、オフィス / エンタープライズ環境の約 60% を仮想化しました。クラウド化された機能は、生産能力を向上させるだけでなく、データアクセスのセキュリティーと冗長性の強化により、インテル IT 部門の BC 活動をサポートします。

IT 危機対応および復旧管理（ITRRM）の実例：東日本大震災

日本におけるインテル IT 部門の BC 計画は、昨年発生した東日本大震災によって、その効果を実際に試されました。そこから得られた主要な教訓は以下のとおりです。

- ノートブック PC 戦略は非常に効果的でした。日本の従業員の 100% がノートブック PC を使用していたため、震災発生後、直ちに在宅勤務へと容易に移行できました。
- 在宅勤務は 1 ～ 2 週間は効果を上げましたが、それ以降は家族やペットに作業を中断されるなど、家庭生活との切り離しの難しさから一部社員の満足度が低下し始めました。そこでインテル IT 部門は、2 カ所の臨時オフィスを開設し、自宅外での勤務を可能にしました。
- インテルのモバイルユーザーに広く導入されている WiMAX* は、震災発生直後の 3G データ通信網が混雑している状況において、ネットワーク接続を提供する手段として有効であることが証明されました。
- 電子メールや ERP、その他の重要なビジネスツールなど、インテルの重要な機能の多くはエンタープライズ・プライベート・クラウド上でホスティングされていました。その結果、震災はこれらの機能へのアクセスに影響を与えませんでした。
- 2 つの新しいテクノロジーが、コミュニケーションの改善に極めて有効であることがわかりました。卓上電話が VoIP ソフトフォンで置き換えられ、どこにいてもオフィスとほぼ同様の連絡手段を取ることができました。また、従業員は必要なサポートとコミュニケーションにソーシャル・メディア・フォーラムを利用しました。例えば、インテルから発信される情報は、従業員がアクセスできるオンラインフォーラム経由で入手可能になりました。
- 震災から復旧する段階では、重要なサービスから先に回復するように、優先順位を指定したサービスのリストを用意することが重要であると学びました。

震災の発生後、インテルはダウンタイムなしでビジネスを継続しました。従業員はまず自宅で、次に臨時オフィスで仕事をし、8 カ月後には完全に修復された常設オフィスに移りました。この期間中、別途予定されていた ERP システムのプラットフォーム再構築などの大規模な IT プロジェクトの納期に影響はありませんでした。震災によってインテル株式会社が直面した状況は深刻なものでしたが、震災後には収益の増加を達成し、2011 年を記録に残る年にしました。

まとめ

インテル IT 部門は、インテル危機管理（ICM）の全体的な目標（すなわち、災害発生時にインテルの従業員、その家族、ビジネスを保護すること）に適合する、IT 危機対応および復旧管理（ITRRM）プログラムを策定しました。このプログラムには業界のベスト・プラクティスと標準が統合され、継続的な改善サイクルを経て構築されていきます。

いつどのような災害が発生するかを正確に予測することはできませんが、私たちは多くの災害の経験を通じて、プログラムと計画のどの部分が効果的であるかを学んできました。効果的なプラクティスとしては、従業員にノートブック PC を支給すること、冗長化された工場を建設すること、重要なサービスをインテルのエンタープライズ・プライベート・クラウド上でホスティングすることが挙げられます。インテル IT 部門では、BC 計画を策定する際に、ビジネスに影響を与える災害それ自体ではなく、その災害がビジネスに与える影響を重視しています。

こうしたプラクティスの実践により、インテルは多くの災害局面で高い対応能力を発揮しました。震災によって業務停止に追い込まれることなく、インテル株式会社は迅速に復旧し、2011 年第 3 四半期および第 4 四半期には収益の増加を達成しました。インテル IT 部門の ITRRM プログラムは、インテルのビジネスへのリスクを軽減し、通常業務の継続性の確保に貢献しています。

詳細情報

その他の IT@Intel ホワイトペーパーについては、http://www.intel.co.jp/jp/go/itatintel/ を参照してください。

- 「Business Recovery and Disaster Recovery with Mobile Business PCs」（英語）
- 「低コストの災害復旧拠点の構築」
- 「A Cost-effective Disaster Recovery Solution for Intel's Factories」（英語）

インテル IT 部門のベスト・プラクティスの詳細については、http://www.intel.co.jp/jp/go/itatintel/ を参照してください。

協力者

Lisa Oppedahl
インテル IT 部門 インテル情報リスク & セキュリティー IT 緊急対応プログラム・マネージャー

Jim Holko
インテル コーポレート・セキュリティー インテル緊急事態管理プログラム・マネージャー

略 語

BC	事業継続性
DR	災害復旧
ERP	Enterprise Resource Planning
IC	インシデント・コマンダー
ICM	インテルの危機管理プログラム
ITBCM	IT 事業継続性（BC）管理チーム
ITERP	IT 緊急対応プロセスチーム
ITRRM	IT 危機対応および復旧管理プログラム
SAN	ストレージ・エリア・ネットワーク
VoIP	Voice over Internet Protocol

インテル株式会社
〒100-0005 東京都千代田区丸の内 3-1-1
http://www.intel.co.jp/

2012 年 6 月

326721-001JA
JPN/1206/PDF/SE/IT/TC