Dell サプライチェーン保証

Dell のサプライ チェーン保証

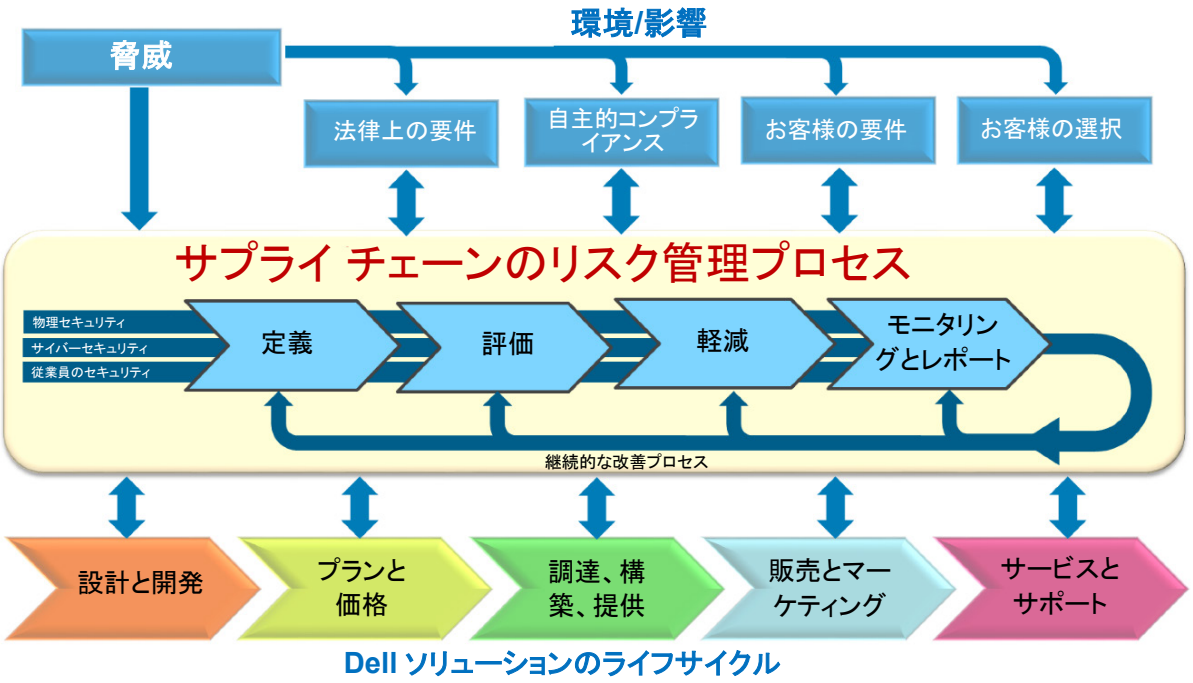
はじめに

ICT（情報およびコミュニケーション テクノロジー）ソリューションのセキュリティを重視するお客様は、ビジネスの遂行に必要なデータとシステムの機密性、可用性、完全性を確保するために細心の注意を必要とします。このような ICT ソリューションのシステム停止、またはデータの不正な漏洩や意図しない漏洩によって、組織やユーザーが重大なリスクにさらされる可能性があります。残念ながら、悪意のある攻撃者は、かつてないほどの粘り強さと巧妙さで、サプライ チェーンの潜在的なセキュリティ ギャップを特定し、利用し続けています。ICT サプライ チェーンには、偽造コンポーネントの挿入、マルウェアの埋め込み、ファームウェアへのコード脆弱性の挿入など、ICT ソリューション プロバイダーが対処しなければならない製品の改ざんの機会がいくつも存在します。

Dell は、サプライ チェーンを保護し、お客様に信頼していただけるソリューションを提供するための、総合的かつ包括的なアプローチを採用しています。Dell の多層防御および広域防御の戦略には、サプライチェーンに発生しうるリスクを軽減するための統制が何重にも含まれています。これらの統制によりサプライ チェーンの安全確保が確立されます。すなわち、サプライチェーンと製品ライフサイクルを通して集約された一連のプロセスと統制が、意図通り・設計通りに機能する製品とプロセス、そして情報を生み出し、そこに想定外の要素は無いことを確実にします。このドキュメントでは、Dell の強力なガバナンス機構と、Dell EMC および Dell のクライアント ビジネス向けのサプライ チェーン セキュリティおよび完全性に関するプラクティスについて簡単に説明します。

継続的なリスク評価と改善

Dell のサプライ チェーン リスク管理フレームワーク（以下）は、米国の包括的なリスク管理フレームワークである全米インフラストラクチャ保護プラン（NIPP）を反映しています（NIPP では、政府機関と民間機関が協力してリスクを軽減し、セキュリティ目標を達成するための方法を概説しています）。Dell のフレームワークには、継続的な改善を可能にするオープンなフィードバック ループが組み込まれています。リスク軽減計画は、ソリューションのライフサイクル全体を通して適切な優先順位を付けられ、実施されます。



サプライヤー ガバナンス

サプライヤー ガバナンスは、サプライ チェーンのパフォーマンスと完全性を維持するうえで重要です。Dell のサプライヤー ガバナンスは、潜在的なサプライヤーおよびパートナーをオンボーディング前に徹底して検証することから始まります。作業評価前の分析には、製品別の RFI（情報提供依頼）または RFQ（見積り依頼）の完了と組み合わされた最初のサイト調査や製造資格認定の形成が含まれることがあります。サプライヤーとの継続的な関係の一部として実施する内容：

1. Dell は、サプライ チェーンのセキュリティ監視に貢献する、数種類の監査を実施します。たとえば、プロセス コンプライアンス監査は、ODM（相手先ブランド設計製造業者）および契約メーカーごとに定期的に実行されます。こうした監査では、オンサイトの品質チームとサイト訪問との併用によって、ODM および契約メーカーがあらかじめ指定されたプロセスに従っているかどうかを確認します。
2. Dell は、Global Inventory Control Policy を実施し、Dell またはサードパーティが持つ Dell 所有インベントリに適用します。Dell とサードパーティの施設は、インベントリを保持するためのセキュリティ、物理的な処理、ストレージ、分離の要件を満たす必要があります。また、このポリシーには、グローバルな解析やレポート作成に加えて、製品が不足および損傷した場合の品質管理プロセスの要件も含まれます。こうしたインベントリ プロセスと制御によって、公式な監査を補強する、日常的なガバナンスがもたらされます。
3. また、Dell は、物理セキュリティを実現し、偽造コンポーネント、汚染されたソフトウェアやファームウェア、知的財産の盗難を軽減するための業界のベスト プラクティスに照らして、サプライヤーのセキュリティ プラクティスを評価します。ギャップが特定されると、Dell はその是正措置を要求し、サプライヤーと連携して業界のベスト プラクティスを満たせるだけの能力構築に取り組みます。
4. Dell の想定に対するパフォーマンスを評価するため、四半期ごとのビジネス レビューがすべての主要なサプライヤーとともに実施されます。重要業績評価指標やその他の指定されたメトリックが監視されることで、Dell のお客様は、引き続き競争力のある価格で高い製品品質を手に入れることが可能になります。また、Dell およびパートナー企業が、技術、需要、法律、お客様の要件の変化に迅速かつ効果的に対応できるように、経営陣レベルの交流も頻繁に行われます。

サプライ チェーンのセキュリティ

Dell EMC では、***サプライ チェーンのセキュリティ***とは、物理資産、在庫、情報、知的財産、および人材を保護する、予防検出的な制御手段の実践および適用であると定義しています。
物理セキュリティ、情報セキュリティ、従業員のセキュリティに対処することで、悪意によるマルウェアや偽造コンポーネントのサプライ チェーンへの侵入機会が減り、サプライ チェーンの保証にも役立ちます。

物理セキュリティ

たとえば、Dell EMC 製品を製造している工場は、TAPA（Transported Asset Protection Association：輸送中資産保護協会）の施設セキュリティ要件を満たすことが要求されます。この要件には、重要エリアでのクローズド タイプの監視カメラの使用、アクセス制御、入口と出口の常時警備が含まれます。Dell とサプライヤーが管理する施設ではその他の制御も用いられます。航空機、鉄道、貨物船の配送についても、輸送モードや地域ごとに発生するさまざまなリスクに対応します。このような保護手段としては、改ざんを防止するパッケージ、出荷レーンのセキュリティ監視、必要な仕様を満たす鍵システムまたはハードウェア、コンテナの完全性要件などが挙げられます。また、GPS トラッキング デバイスを任意のコンテナに配置し、デリバリが確認されるまで、24 時間 365 日監視することもあります。

また、Dell は、米国税関および国境警備税関のテロ防止のための税関産業界提携プログラム（C-TPAT）の認定を受けています。この物流セキュリティ プログラムは、AEO（Authorized Economic Operator：認定通関事業者）、カナダの PIP（Partner in Protection）、シンガポールのセキュア トレード パートナーシップ プログラムを含む、世界中の類似したプログラムと互換性があることが認められています。これらのプログラムの主な目的は禁輸品の流入を防ぐことであり、そのための保護により、輸入される製品の改ざんも防止されます。

情報セキュリティ

Dell は、通常のビジネスにおいて、サプライ チェーンのライフサイクルを通して、製品、ソリューション、お客様、サプライヤー、パートナーに関する機密情報を収集、使用します。こうした機密情報を漏洩や悪用から保護するために、多くの対策が使用しています。たとえば、Dell とパートナーとの間のデータ転送では、暗号化方式とプライベート回路を組み合わせて使用します。安全なプロトコルやカプセル化テクノロジーも、業界のベスト プラクティスに従って、必要に応じて使用します。また、本番ラインは、情報を転送する能力を制限するように設計、構築されています。

Dell の内部ネットワーク環境と関連する資産は、ウイルス検出、強力なパスワード適用、e メールの添付ファイルのスキャン、システムおよびアプリケーションへのパッチ適用の徹底、侵入防止、ファイアウォールなどの制御によって安全が確保されます。マルウェアや資産の誤用から保護するための追加の制御も実装されています。

また、Dell は、「職務の分離」と「最低限の権限」の原則を採用しています。これは、企業全体でのデータ アクセスの誤用の防止に役立ちます。これらの原則により、機密情報へのアクセス権限は、各自の業務遂行に必要なレベルに応じて付与されます。

従業員のセキュリティ

従業員のセキュリティ管理は、情報セキュリティとサプライ チェーン保証の重要な要素です。従業員を審査し、企業のデータ、資産、リソースへのアクセス、利用、および操作に対する従業員の権限を制限することで、社内のセキュリティ活動を効果的に運用することができます。Dell のポリシーでは、契約サプライヤーの従業員を含め、サプライ チェーン全体の従業員に対して雇用前の適合性審査プロセスを実施する必要があります。このプロセスには、法律で許される範囲内でのセキュリティ バックグラウンド チェック、薬物検査、ID 検証、およびアプリケーション情報の検証が含まれます。

また、Dell の従業員は、定期的にセキュリティ意識向上トレーニングを受けています。これにより、サプライチェーン全体を通して、製品がリスクにさらされる可能性のある行動を軽減することができます。Dell の年間コンプライアンス トレーニングの一環として、従業員は情報セキュリティやその他の Dell セキュリティ プラクティスに関するコースを修了する必要があります。また、従業員は、企業のニュースレター、社内および社外のセキュリティ関連 Web サイト、お客様向けホワイトペーパーの閲覧、セミナーへの参加、追加のオンライン コースやビデオ トレーニングの受講など、さまざまな非公式な方法を通じて、自己学習を行うように促されます。

Dell は、情報開示に関しては、データの利用範囲や開示を制限する NDA（機密保持契約）やその他の拘束力のある契約条項に徹底的に従うことにより、機密データを保護しています。Dell における雇用条件として、従業員は退職後も含めて、その知的財産、顧客情報、その他の機密データを保護する NDA への署名を求められます。

サプライ チェーンの完全性

サプライ チェーンの完全性では、お客様が期待どおりの製品を手にして、その製品が期待どおりに動作することを保証するための取り組みの内容が定義されます。サプライ チェーンの完全性を実現するための重要な機能は、ハードウェアとソフトウェアのベースライン仕様を安全に保存しておき、不正な変更が行われていないことを確認するための基準として使用できるようにすることです。

ハードウェア

Dell は、偽造コンポーネントが当社のサプライ チェーンに侵入する機会を最小限に抑えることを目的に、さまざまな品質管理プロセスを確実に整備しています。Dell の新製品導入プロセスによって、材料が承認済みベンダー リストから調達され、適切に部品表と照合されます。部品は、可能な場合には、ODM(相手先ブランド設計製造業者)または OCM(部品の本来の製造業者)から直接調達されます。

Dell の品質管理システムは、承認されたベンダーからのソーシングを含む、エンジニアリング仕様およびプロセスへの継続的なコンプライアンスを確認します。生産中に材料の検査を行うことによって、マーキングミスがあったり、正常な性能パラメーターから逸脱していたり、または正しくない電子 ID が含まれていたりするコンポーネントを特定できます。適切なトレーサビリティを有効にするために、すべての主要なコンポーネントは、シリアル番号ラベルまたはマーキング、Dell が規定する PPID(Piece-Part Identification:ピースパーツ ID)ラベル、製造プロセス中に収集可能な電子識別子によって一意に識別されます。また、Dell は、グローバル製造サイトで品質管理プラクティスの ISO 9000 認定を保持しています。これらのプロセスおよび制御を遵守することで、Dell 製品内に偽造コンポーネントが組み込まれているリスクを最小限に抑えることができます。

ソフトウェア

業界を対象としたソフトウェア エンジニアリングのベスト プラクティスには、オペレーティング システム、アプリケーション、ファームウェア、デバイス ドライバーを含むあらゆるコードの開発プロセス全体における一貫したセキュリティが含まれます。Dell は、その開発プロセス全体を通じて SDL(Secure Development Lifecycle:安全な開発ライフサイクル)を組み込むことで、ソフトウェアセキュリティの欠陥を悪用する機会を低減します。これらの手段は、SAFECode(Software Assurance Forum for Excellence in Code)ガイドラインおよび ISO 27034 とも密接に連携しています。

ライフサイクル全体を通じてのプロアクティブな検証、妥当性評価、セキュリティ テスト アクティビティにより、ソフトウェアの安全性を確保し、マルウェアや符号化の脆弱性をソフトウェアに組み込む可能性を低減することができます。堅牢なサイバーセキュリティ プログラムは、ソース コードへの不正アクセスを防止し、製品がお客様に出荷される前にマルウェアが製品に侵入する可能性を最小限に抑えることによって、ソフトウェアの完全性を向上させます。

また、Dell EMC では、NIST SP 800-147、BIOS(Basic Input/Output System)保護に関するガイドラインに沿ったガイダンスおよび推奨事項に従って、商用サーバー、デスクトップ、ノートパソコンに対して処理手順を実装しています。Dell の保護された BIOS と署名済みの更新メカニズムにより、プラットフォーム ファームウェアの不正な変更を防止し、起動前のマルウェアや不要な機能のリスクを軽減することができます。

Dell PSIRT(Product Security Incident Response Team:製品セキュリティ インシデント対応チーム)は、Dell 製品に影響を与える脆弱性を監視し、迅速なセキュリティの改善を調整して、製品のお届け後も、お客様が Dell 製品のセキュリティ体制を維持できるように支援します。

ともに強固に

Dell は、信頼できる業界グループとのパブリック/プライベートなパートナー関係によって、サプライ チェーンのリスク管理活動に参加しています。ここでは、業界をリードする企業との連携によって、サプライ チェーンおよび製品のセキュリティ リスクを軽減するための規格および業界のベスト プラクティスをさらに発展させるための Dell の取り組みについて解説しました。Dell は、O-TTPF(オープン グループ トラステッド テクノロジー フォーラム)、ソフトウェアとサプライ チェーン保証フォーラム、SAFECode、サプライ チェーン リスク リーダーシップ協議会、インターネット セキュリティ アライアンス、IT 部門調整協議会に積極的に参加しています。Dell は、GIDEP(行政情報データ交換プログラム)のアクティブ メンバーでもあります。

Dell は、O-TTPS（オープン グループ トラステッド テクノロジー プロバイダー規格）など、サプライ チェーンの完全性に関連するさまざまな標準規格およびベスト プラクティス ガイドラインの開発にも参加しています。これには、ISO 20243、SAFECode、ISO 27036、および NIST（National Institute of Science and Technology：米国科学技術研究所）IR（各機関共同報告書）7622、NIST SP（特別刊行物）800-161、NIST SP 800-53、NIST サイバーセキュリティ フレームワークなどが含まれます。製品の改ざんおよびサプライ チェーン保証に関するお客様の懸念に対応するために、Dell は引き続き、法律、規制、自主的な規格、契約の言語の開発および潜在的な作用を監視し、影響力を発揮します。

Dell は、Dell Technologies ポートフォリオに含まれる Pivotal、RSA、Secureworks、Virtustream、VMware など、業界最先端かつ信頼度の高いブランドから得られる、インサイト、ベスト プラクティス、テクノロジー、専門性を活用できる、独自の地位を占めています。Dell は、お客様、サプライヤー、パートナーの声に耳を傾け、そして相互に協力して、Dell のサプライ チェーン保証の提供方法のさらなる改善に取り組むことが重要であると考えています。
詳細については、Dell の営業担当までお問い合わせください。