プロジェクト情報管理における潜在的リスク分析の方法

進　藤　昭　夫

1．はじめに

プロジェクトは、目標とする成果物を、定められた期間と予算内で、経営資源を活用し、完成することにある。近年、企業活動は全てプロジェクトとして捉え Enterprise Project Management の考え方もでてきている[1)]。プロジェクトは、計画、設計、調達、製作または建設、運用と進行していくライフサイクルの各段階があり、進行段階に従いリアルタイムで情報の作成、交換、蓄積がなされていく。これらは、目標成果物の構築に向けて必要となる情報であり通常膨大な量となる。その為、情報システムの活用が不可欠であり、LAN や Internet など企業内外の情報ネットワーク・システムを利用した業務遂行形態となっている[2)]。更に、プロジェクト遂行組織は、情報ネットワークの発展により、企業内だけの固定化した機能部門別組織から、海外を含む企業外とのコラボレーションやアウトソーシングによる柔軟な機能分散化へと変化してきている。プロジェクトにおいては、これらの分散化された複数オフィスでの業務遂行を、情報ネットワークの支援のもとで、管理・統制する必要がある。管理・統制では、分散化されたオフィスにおける時々刻々と変化するプロジェクト遂行状況および成果物情報を把握し、業務遂行部隊に的確な指示情報を与える必要がある。これらのプロジェクト活動の情報は、ライフサイクルの各段階における中間成果物（Deliverables）の情報を主体として、データファイルやデータベース（DB）に格納されていく。

情報ネットワークの発展は、この様な情報の統合管理と共有利用を促進し、迅速な情報交換による業務の効率化を可能としている。その一方、情報ネットワークのオープン化により、外部からのサイバーテロなどによるプロジェクト管理情報の改竄や破壊は、納期、予算、品質を最優先するプロジェクトにおいては致命的な事態を引き起こす可能性も内在している。したがって、情報ネットワークを活用したプロジェクト管理においては、その利便性だけでなく、異常事態が引き起こすリスクを評価し、その対策を講じておく必要がある[3)]。一般に、外部から情報ネットワークへの異常侵入対策として、ファイアウォールなどのセキュリティ・システムが導入されている。しかしながら、プロジェクト情報管理の観点から、情報ネットワーク活用に内在する潜在的なリスクの評価法と対応策について統一化された研究は少ない。

プロジェクト情報の特徴として、初期仕様の変更や後段作業結果の反映などによる変更作業（Revision Work）を伴うことが多い。プロジェクト情報管理においては、情報の変更が正常な行為か、外部からの侵入による異常な行為かを見極める必要がある。異常変更が早期に検出された場合は、修正労力は少なくて済むが、検出されずに後段の作業にまで影響が波及した場合は、プロジェクト業務は停止せざるを得なくなり、目標である納期、予算、品質の達成が困難となる可能性がある。その為には、異常変更の早期検知と変更管理に対するセキュリティ対策が重

要と考える。

そこで、本報告では、プロジェクトの特性を考慮した情報管理における潜在的なリスクを分析し、リスク回避を図る情報セキュリティ・モデルを提示した。このモデルは、セキュリティ・チェック機構を導入し、コンピュータ・ネットワーク側とプロジェクト・エンジニアリング側の異常伝播とその異常原因を Event Tree（ET）と Fault Tree（FT）の組み合せにより解析する方法である。なお本検討では、プラントの設計・建設を遂行するエンジニアリング業務における情報管理を主対象としているが、情報システム開発など他のプロジェクトにも拡張して適用可能と考える。

2．情報システム活用における プロジェクト遂行形態の構造化

2.1　ワークパッケージに基づく業務遂行形態

プロジェクトにおけるエンジニアリング業務は、最終成果物のシステム構造を規定するに必要な中間成果物（Deliverables）を作成していく業務プロセスである。中間成果物の作成業務は、プロジェクト管理の最少単位となるワークパッケージに分割され、達成目標となる品質（設計図書や図面の完成度など）、スケジュール（開始、終了時間）、コストが規定され、担当する専門家集団（デシプリン・エンジニア）が決められる。プロジェクト遂行プロセスは、このワークパッケージを構成要素とし、その先行順序を基にプレシーデンス・ダイアグラムあるいはスケジュール・ネットワークとして定められる。したがって、各ワークパッケージの作成業務は、インプット情報（前段階の成果物結果）と達成目標が与えられた基でのアウトプット情報（当該ワークパッケージの作成結果）を得るプロセスとして捉えることができる。

ここで、プロジェクト遂行においては、一部のデータ変更が各種局面においてしばしば起こる。例えば、顧客仕様変更などの外部要因に起因するインプット情報の変更、スケジュールなどの関係から見切り発車によるインプットデータの仮設定値の変更、

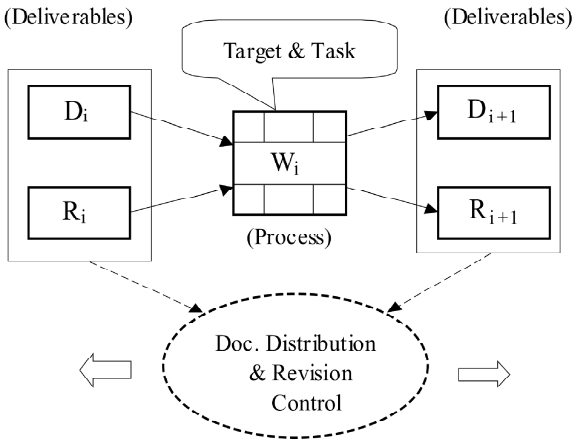

図１　ワークパッケージ遂行の基本形態

後段作業結果を反映したデータの変更などであり、これらはアウトプット情報の変更となり、次の段階でのインプット情報の変更へ繋がっていく。プロジェクト管理では、この様なインプットやアウトプット情報の変更について、ワークパッケージに付けた変更番号（Revision Number）と付随データによる変更管理が行われる。もし変更番号の追加や加算があれば、関連するワークパッケージへ指示を出す必要がある。以上のワークパッケージ（W_i）の作成に係わる情報の入出力関係を図 1 に示す。図 1 において、前段階の成果物（D_i）と変更管理情報（R_i）および作業結果としての成果物（D_{i+1}）と変更管理情報（R_{i+1}）は、データファイルまたはエンジニアリング DB として情報システムに格納される。また、変更の時系列的な履歴は、変更履歴ファイルとして蓄積される。

2.2　エンジニアリング情報システムとの連携

情報ネットワーク活用によるエンジニアリング情報システムの典型的な一例を図 2 に示す。図 2 において、外部情報は、インターネットと連結したルータならびにファイアウォールを経由し、オフィス内システムとの情報交換がなされる。企業全体のビジネス情報や経営資源（要員、資金、ツールなど）の管理の為には、第 1 次イサーネットによるビジネス用 LAN が利用される。プロジェクト管理では、顧客、ベンダ、ライセンサ、帰属企業との授受情報を

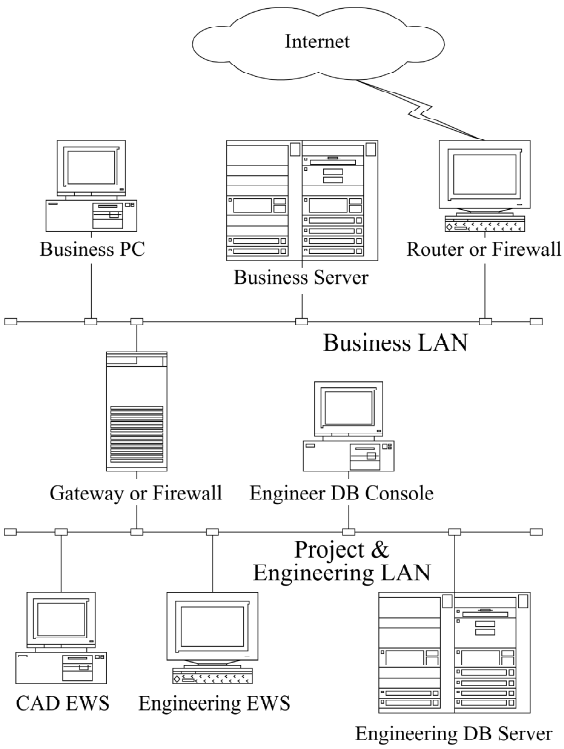

図2　エンジニアリング情報システムの構成例

管理統制する為に利用される。プロジェクト毎のエンジニアリング・データは、第2次イサーネットによるエンジニアリング用LANが、ビジネス用LANからのゲートウェイを経由して利用される。プロジェクト管理および機能部門では、ワークパッケージを単位としたデータファイルをアクセスし情報授受が行われる。そこでは、エンジニアリング・データだけでなく電子化された業務遂行マニュアルや要員稼動データなども参照される。

2.3　ワークパッケージの異常

ワークパッケージの欠陥や異常は、作成された成果物の異常と作成プロセスにおける異常が考えられる。成果物は、物理的な内容（コンテンツ）が同定可能であるのでデータファイルとして格納される。一方作成プロセスは、人間の知的活動に依存するので、人的ミスが主体となる。本稿では、外部コンピュータからの意図的なデータの改竄や破壊を考え、エンジニアリング情報システムに内蔵されているデータファイルの異常を対象とする。

外部侵入による一部データの改竄は、予期せぬ変更である。プロジェクト遂行業務そのものに起因する変更ではない。もしクラッカーなどの外部侵入によるデータの破損がすぐに検知できれば修復作業は少なくて済む。しかし、発見が遅れ、後段の作業にまでエラーが波及すれば、エンジニアリング・データの修復には、多大の労力（コスト）と時間を要す。また品質を満足しない中間成果物となる可能性がある。したがって、プロジェクト情報管理においては、プロジェクトそのものに起因する予期したデータの変更か、外部侵入による予期せぬデータの変更かを見極めた管理統制が必要となる。

3．プロジェクト情報管理における潜在的リスク

プロジェクト・エンジニアリング業務において、情報ネットワークシステムの活用は、プロジェクト業務遂行における利便さと同時に潜在するリスクを分析し対策を講じる必要がある。情報システムにおいて、外部からのサイバーテロやクラッカーによるデータファイルの破壊や改竄は、致命的な打撃を引き起こす可能性がある。そこで、初期イベントを、「インターネット・ルータへの攻撃」とし、この攻撃による侵害の波及伝播を、潜在的なリスクとして考える。一例を図3に示す。図3は、左から右への事象は時間経過を示し、下から上へは被害（リスク）の大きさを示している。図3において、ルータが攻撃された後のリスク伝播の一例は以下の様になる。セキュリティゲートC1(アクセスコントロールの失敗)、C2（ネットワークへの侵入)、D2（高度のユーザIDの取得)、そしてE3（エンジニアリングDBサーバへの侵入)。もし侵入がD4の段階で検出(D6)されたとすると、直ちに、修復されLANの一部を切り離し、プロジェクト遂行の継続が可能となる。しかし、DBの内容が一部変更（F4）され、改竄された情報を使い以降のエンジニアリングが遂行された（G4）とすると、その誤った結果は、次々に伝播し（H5)、致命的なトラブルを引き起こす（H6）ことになる。この様な潜在的な異常事態を早期に検知

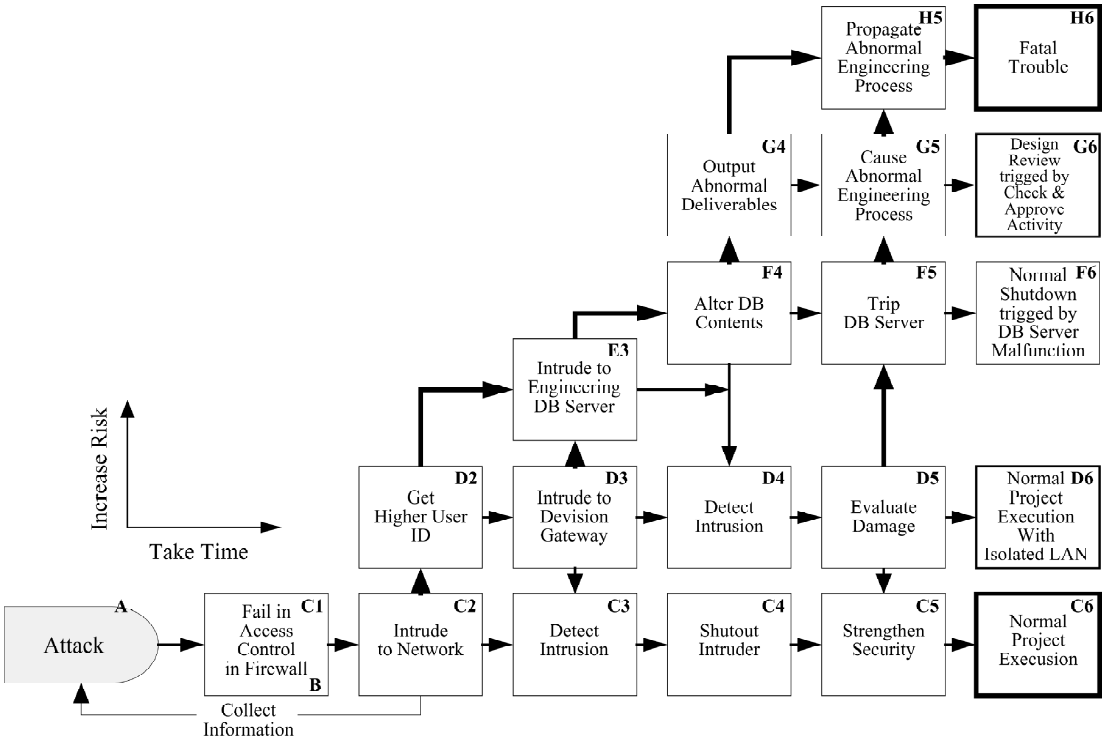

図 3　サイバーテロ侵入によるプロジェクト・リスク伝播の構造

し対応するには、重要度の高い異常事象に対して、その因果関係を明らかにし、セキュリティを確保する為の防護システムを評価する必要がある。そこで、本稿では、このセキュリティ・システムを、コンピュータ・ネットワーク側とプロジェクト・エンジニアリング側の両方から構築することを考える。

4．コンピュータ・ネットワーク側のセキュリティ・モデル

コンピュータ・ネットワーク・システムにおいては、エンジニアリング・データ、プロジェクト管理データなどの種々のデータは、基本的には文書ファイルあるいはデータベース（DB）の形式で蓄積･保管されている。これらの各種ファイルについて、外部侵入によるアクセス経路は一義的でなく、様々な経路や組み合せが考えられるので、ファイルの健全性を維持するには、種々のファイル・アクセスに関し統一化したセキュリティ･モデルが必要となる[4)]。そこで、統一化したファイル・アクセスの認証機構として図 4 に示すモデルを考える。このモデルは、全てのファイルに対し、利用者の識別とアクセス権限、アクセス・コマンドの利用制限、ファイル内容のアクセス制限についてセキュリティ・チェックを行い、アクセスの問題がないかどうかを認証する機構である。外部侵入者が目標ファイルをアクセスできるかどうかは、これらのチェックゲートを通過できるか否かである。認証が成功すれば異常は防止できる。

しかし、認証に失敗し異常が検知されなければ、図 3 に示す異常が伝播する可能性がある。そこで認証失敗を想定し、その予想される原因を予め摘出しておけば、原因の同定と検知対策を講じることが可能となる。原因の同定には、FTA（Fault Tree Analysis）が適用可能である[5)]。この FTA は、次のアクセス経路の論理関係を抽出する事により作成する。

ログイン経路の抽出：

Step 1）　目標となるコンピュータ（ファイル・サーバ）の摘出

Step 2）　摘出されたコンピュータへログインする利

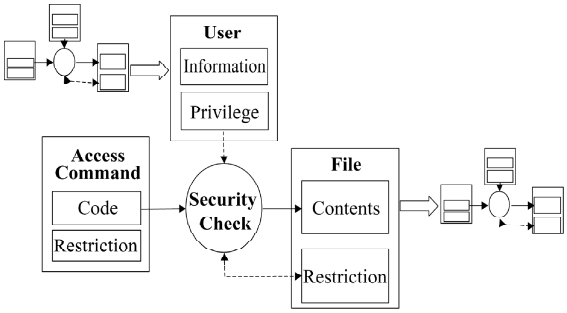

図 4　認証機構のモデル

用者の摘出

Step 3）摘出された利用者がログインするコンピュータの抽出

Step 4）上記の Step を繰り返し、利用者とコンピュータの全ての組み合せを摘出

次に、抽出されたログイン経路について、書き換えコマンドを取得し、目標となるファイルの情報を変更に至らしめる経路を抽出する。

ファイル・アクセス経路の抽出：

Step 1）目標とするファイルの摘出

Step 2）認証機構を用いている全てのファイルの抽出

Step 3）目標ファイルと連携関係のある全てのファイルの摘出

Step 4）目標ファイルと関係する全てのファイルについて、認証失敗を引き起こす FT（Fault Tree）の作成

Step 5）認証失敗に関する異常事象の伝播を ET（Event Tree）により作成

Step 6）FT と ET の組み合せによるセキュリティ・チェックの構成モデルを作成

一例として、図 5 にセキュリティ・チェック機構の概念図を示す。この図において、A，B，C は、セキュリティ・チェック事象を示す。このセキュリティ・チェック事象が失敗するとした場合の原因事象は FT を展開して摘出する。もし、原因事象の発生確率データがあれば、この失敗事象の伝播により目標ファイルの異常アクセスに至る発生確率が推定できる。

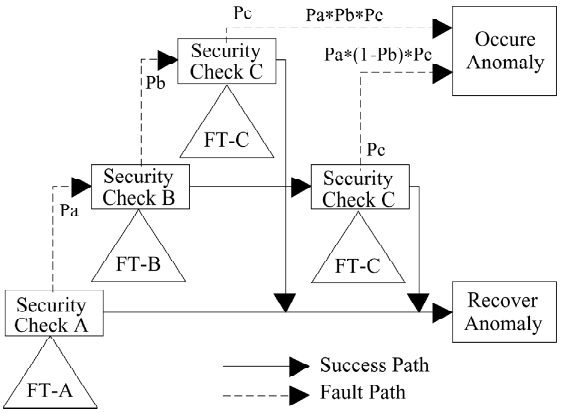

図 5　ET と FT の組み合せによる
セキュリティ・チェック構造

5．プロジェクト・エンジニアリング側のセキュリティ・モデル

プロジェクトにおけるエンジニアリング業務プロセスは、ワークパッケージを基本とするスケジュール・ネットワークに従い、順次中間成果物（Deliverables）となるドキュメント類が作成されていく。図 6 に一例として業務プロセスと成果物情報の連携を示す。ワークパッケージの作成においては、前段階迄に作成されたワークパッケージから必要となる入力情報を選定し、達成目標に従い業務が遂行される。前段階の結果は次の段階の仕様となる。これらの中間成果物の情報は、エンジニアリング・データとして、データベースに格納されていく。達成目標は、品質、遂行時間、コストなどの指示情報であり、計画と実績データがプロジェクト管理ファイルに格納され、差異是正のコントロールの為に使われる。プロジェクト遂行途中において、ワークパッケージのデータ状況は、図 1 に示したように変更管理情報により管理される。変更管理においては、ファイルデータの変更が、正常な変更か外部侵入による異常な変更かを見極める事が重要となる。もし異常が検知されなければ、作成されるワークパッケージの欠陥を引き起こし、次に関係するワークパッケージへも影響を及ぼすことになる。

そこで、ワークパッケージの異常を見極める方法として、ワークパッケージのデータと変更番号なら

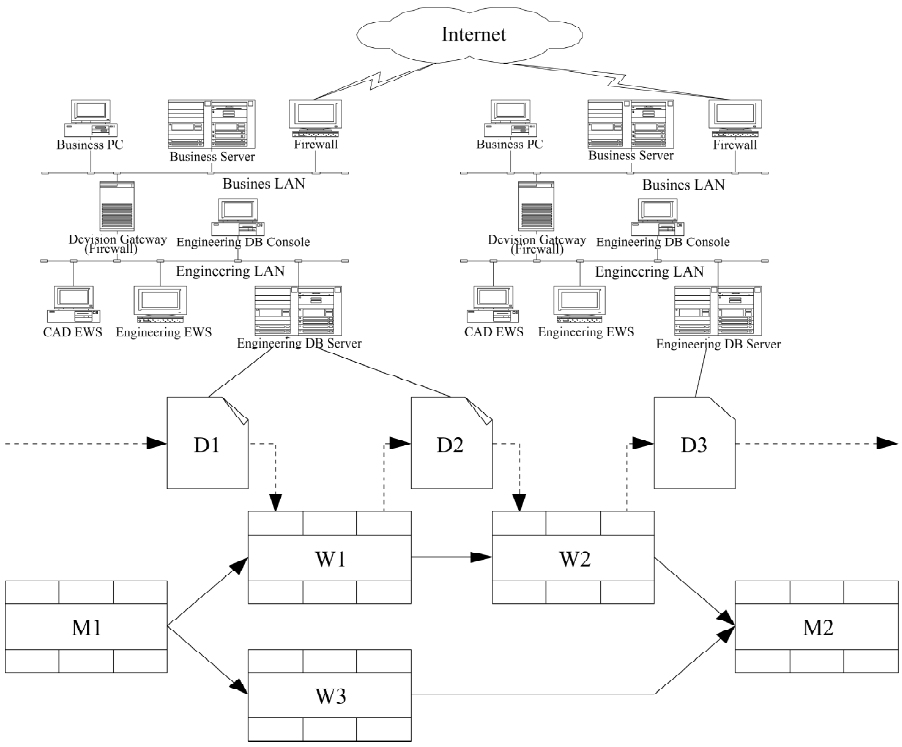

図 6　スケジュール･ネットワークとワークパッケージ情報の連携
（D1, 2, 3: Deliverables, M1, 2: Milestones, W1, 2, 3: Work Packages）

びに変更事由との整合性を監視するセキュリティ・チェックモデルを考える。これは、変更番号の順序性や変更事由による履歴管理であり、この基準から外れるデータについては、異常と識別する方法である。正常なデータ変更については、必ず変更番号を付し、変更管理ファイルに登録する。プロジェクトは変更情報を監視し、もしワークパッケージ情報と変更履歴情報との整合性がなければ、何らかのデータ改竄が予想されるので、その原因を同定し、対策を講じる。このセキュリティ・チェック機構の解析には FTA により予想される原因事象を摘出する。トップ事象は、ワークパッケージの異常であり、異常原因は必要となるインプット情報とプロジェクト管理情報（ワークパッケージに課せられた品質、コスト、スケジュール、担当要員などのデータ）の欠陥に大別でき、それぞれが異常となる原因事象を同定することになる。FTA は、次の Step により展開される。

Step 1)　対象とするワークパッケージの異常事象（出力情報）の抽出

Step 2)　当該ワークパッケージの入力情報を規定するエンジニアリングデータファイルを抽出

Step 3)　ワークパッケージの達成目標を規定するプロジェクト管理ファイルの摘出

Step 4)　当該入力情報と管理情報に関する変更履歴管理ファイルの摘出

Step 5)　入力情報ならびに管理情報の欠陥を引き起こす原因同定の FT 構築

例えば､入力と管理データ欠陥に関する原因事象は、下記が想定される。

―データファイルのアクセス失敗
―データ項目の欠損
―データ値の異常
―変更番号の順序性の異常

6．ET と FT の結合によるリスク管理

ネットワーク側とエンジニアリング側のセキュリ

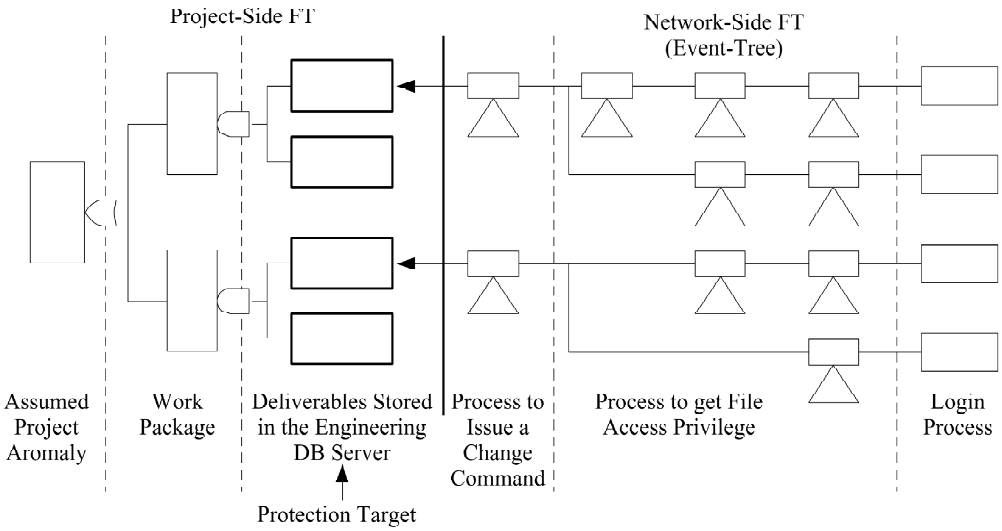

図7　ETとFTによるネットワーク側とプロジェクト側のセキュリティ・モデルの統合

ティ・モデルを結合することにより、エンジニアリング・データが異常を引き起こす経路と想定原因の同定が可能となる。図7にエンジニアリング情報が異常となる事象について、ETとFTの組み合せによる異常伝播とその原因の因果関係を示す。エンジニアリングに係わるデータファイルの健全性確保は、プロジェクト側とネットワーク側の双方からの接点となる。定性的なリスク管理は、ファイル・アクセスの異常伝播経路による変更コマンドの異常がETAにより明示でき、その原因同定がFTAにより可能となる。さらに、変更コマンドの異常がファイルに蓄積される中間成果物の異常につながり、後段のワークパッケージの異常へと伝播する。定量的な管理としては、FTのボトム事象の発生確率が分かれば、トップ事象の発生確率が推定できるので、発生確率の多い事象を対象としたリスク評価が可能となる。

7. ま と め

情報ネットワークを活用したプロジェクト遂行においては、時々刻々と変化するエンジニアリング情報の健全性を確保すべく、プロジェクトの特性を反映したセキュリティ対策が必要と考える。そこで本報告では、外部侵入に起因するリスク対策として、ネットワーク側に各種ファイル・アクセスの統一的な認証モデルを導入し、プロジェクト側ではワークパッケージの入力情報と達成目標の変更情報を管理することにより、エンジニアリング情報のセキュリティを解析する方法を提示した。

参考文献

1）Dinsmore, P. C., “Winning in Business With Enterprise Project Management”, American Management Association-AMACOM (1999)

2）高橋正明、「エンジニアリングのIT化」、プロジェクトマネジメント学会2000年度秋季大会、pp. 211−212（2000）

3）宝木和夫他、「情報システムにおけるリスク分析」、電学論C、108巻4号、pp. 260−267（1988）

4）Shindo, A., H. Yamazaki, A. Toki, R. Maeshima, I. Koshijima and T. Umeda, An Approach to Potential Risk Analysis of Networked Chemical Plants, Computers and Chemical Engineering, 24, 721−727（2000）

5）Lapp, S. A. & Power, G. J., IEEE Transactions of Reliability, R-26, 2（1997）