耐タンパ技術と暗号技術による情報漏洩防止技術

Anti-tamper and Cryptographic Solutions for Information Protection

白木 孝義 Shiraki Takayoshi
佐藤 真 Sato Makoto
野口 雅和 Noguchi Masakazu
古屋 聡一 Furuya Soichi

社会インフラシステムに関連する情報漏洩は，国家規模の被害に及ぶことも想定されるため，国家安全保障に関わる最重要課題として位置づける必要がある。日立グループは，耐タンパ技術と暗号技術を中核とし，リバースエンジニアリング防止ツール，ハードディスク全体暗号化機能，通信暗号化機能といった情報漏洩防止技術を提供している。これらは，日立グループがシステム開発を通じて蓄積したノウハウと，大規模な攻撃を想定した独自のリスク分析に基づいて設計・実装したものである。

1. はじめに

一般的な企業や組織では，情報漏洩（えい）と言えば，個人情報や営業秘密などの漏洩を指すことが多い。漏洩した情報によっては，損害賠償あるいは企業・組織の信用失墜などの大きな損失を被る場合もあり，重大な問題である。

一方，社会インフラシステムにおいては，情報漏洩は損害賠償や信用失墜にとどまらない深刻な被害を招く可能性がある。特に，そのようなシステムの認証情報，システム構成，利用ソフトウェアに関する情報〔例えば脆（ぜい）弱性〕などが漏洩した場合は，これらを利用したサイバー攻撃が実行され，広範囲なシステムダウンやシステム制御権の乗っ取りなどに至ることがある。国民保全あるいは社会基盤などのための大規模システムが攻撃の対象となれば，国家規模の被害に発展することさえも考えられる。

日立グループは，このような情報漏洩の問題を国家安全保障に関わる最重要課題と位置づけている。また，国家安全保障を目的としたシステム開発を通じ，大規模な攻撃を想定したリスク分析と，これに対する厳重なセキュリティの構築を行ってきた。これらの実績に基づくノウハウを活用し，国家安全保障レベルの対策を意識した情報漏洩防止技術を提供している。

ここでは，情報漏洩に関わる脅威に対する日立グループの観点と，保護対策の中核となる耐タンパ技術と暗号技術，および，これらの技術を利用した情報漏洩防止技術について述べる。

2. 情報漏洩の脅威と対策技術

ここでは，データおよびソフトウェアを保護すべき情報資産として定義し，これらの情報資産に対する脅威と，このような脅威から情報資産を保護するための技術について述べる。

2.1 情報資産に対する脅威

まず，一般的な企業を例とし，データに対する脅威を図1に示す。同図では，本社，支社および外出先の3種類の場所を記載している。本社と支社にはオフィス業務を目的とした固定設置PC（Personal Computer）があり，その一方，営業先などで利用されるモバイルPCもある設定とした。また，本社，支社および外出先の間では，インターネットなどのWAN（Wide Area Network）を介した通信が

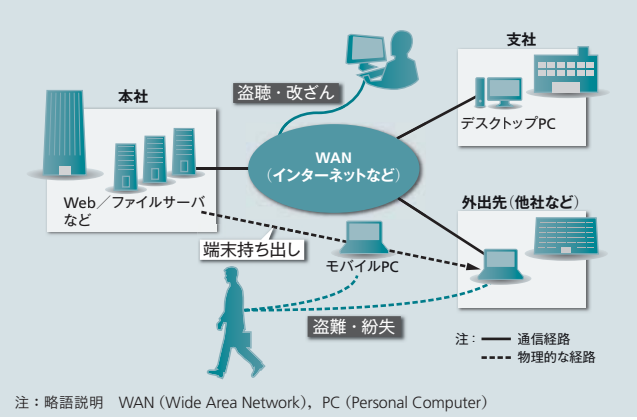


図1｜データに対する脅威
企業のPCに対する主要な脅威を示す。WAN上での盗聴・改ざん，外出先での盗難・紛失などが考えられる。

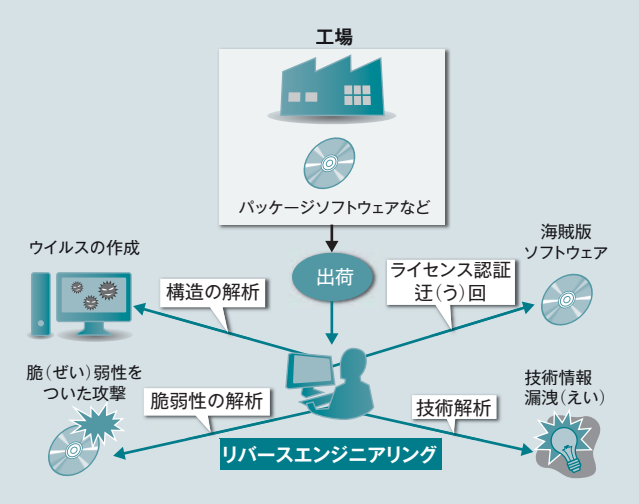


図2｜ソフトウェアに対する脅威
ソフトウェアは，不正なリバースエンジニアリングを行われることにより，その仕組みを解析され，海賊版作成などの被害につながる。

行われるものとした。このような環境では，WANにおける通信データの盗聴・改ざん，および外出先におけるPCなどの盗難・紛失による情報漏洩が主な脅威と考える。特にPCにおいては，BIOS（Basic Input/Output System）あるいはOS（Operating System）の認証がある場合でも，ハードディスクを取り出して別のPCに接続することで内容の読み出しが可能となるため，盗難・紛失による脅威が軽減されない点に注意が必要である。

次に，ソフトウェアに対する脅威について**図2**に示す。ここでは，ソフトウェアパッチなどによって対策可能なソフトウェア個別の脆弱性ではなく，同図に示すような悪意を持ったリバースエンジニアリングこそが主要な脅威であると定義した。ここでのリバースエンジニアリングとは，ソフトウェアの構造・動作解析を行うことである。リバースエンジニアリングが行われることにより，技術情報漏洩あるいは海賊版ソフトウェアの流通などが起こり，これに脆弱性解析などを攻撃者が行うことで，ウイルスを作成され，結果としてサイバー攻撃の糸口となる。このうち，ウイルス作成と脆弱性解析は，サイバー攻撃などにつながる可能性がある。専用ソフトウェアを攻撃する場合は，特に事前のリバースエンジニアリングが必要になると考えられる。前述したとおり，大規模な基盤系システムに対するサイバー攻撃が実行された場合，国家規模の被害の発生も想定される。

情報資産と脅威の対応関係を**表1**に，情報に対する脅威と情報の種類を**図3**にそれぞれ示す。

これらの脅威への対策について，次に述べる。

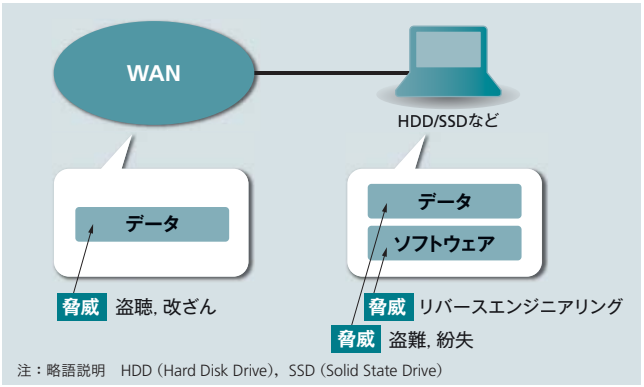
2.2　耐タンパ技術と暗号技術による情報資産の保護

日立グループは，情報資産に対する脅威への対策として，耐タンパ技術および暗号技術を中核技術と位置づけている。

暗号技術は，データに対する情報漏洩防止において有効な技術である。さまざまなデータに適用できるが，コンピュータが直接処理するソフトウェア自身は，一度暗号化しても最終的には復号しなければ実行できないため，暗号によるソフトウェアの保護は限定的である。一方，耐タンパ技術は，このように暗号技術では保護できないソフトウェアについて，リバースエンジニアリングを困難化することによって保護する技術である。これらの二つの技術を組み合わせることにより，データおよびソフトウェアの情報漏洩を防止する。

表1｜情報資産と脅威の対応関係
保護すべき情報資産とそれぞれへの脅威の対応関係を示す。

情報資産	脅威
ソフトウェア	リバースエンジニアリング
ハードディスク内データ	盗難・紛失
WAN上の通信データ	盗聴・改ざん



注：略語説明　HDD（Hard Disk Drive），SSD（Solid State Drive）

図3｜情報に対する脅威と情報の種類
情報が存在する場所（WAN上，HDD内）やその性質（データ，ソフトウェア）により，脅威の種類も必要となる対策も異なる。

2.3　日立グループの強み

日立グループは，国家安全保障に関わる情報システムなどのセキュリティ構築の実績を生かし，高い安全性を持った暗号機能を提供している。特に，暗号強度（暗号解読の困難さ）評価技術を保有しており，国家安全保障レベルのセキュリティが求められる場合に，カスタマイズされた独自暗号アルゴリズムを作成することが可能である。また，耐タンパ技術において必須となるCPU（Central Processing Unit）やOSなどに関する知識とソフトウェア実装技術を有しており，リバースエンジニアリングを効果的に妨害する機能を提供できる。

このような強みを生かしたWindows※1) PC向けの情報漏洩防止技術について，以下に詳しく述べる。

※1）Windowsは，米国Microsoft Corporationの米国およびその他の国における登録商標または商標である。

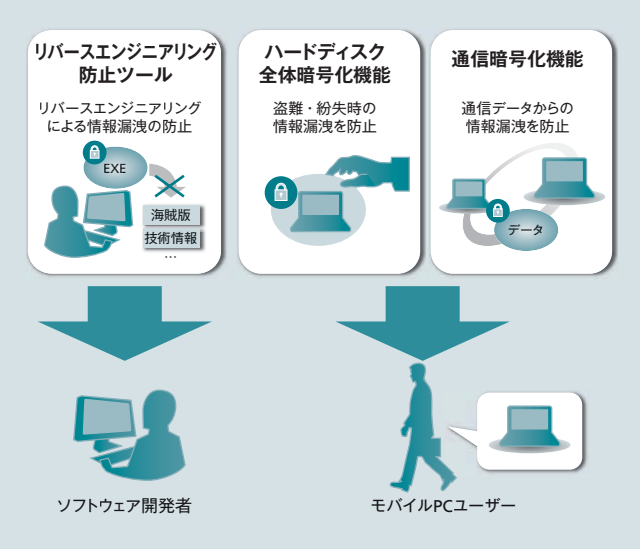


図4｜情報漏洩防止技術
3種類の主要機能により，ソフトウェア，ハードディスク内データ，および通信データを情報漏洩から保護する。

3. 情報漏洩防止技術

ここでは，情報漏洩防止技術の概要について述べた後，提供する各セキュリティ機能について述べる。

3.1 概要

前述した脅威の対策として，耐タンパ技術と暗号技術を用いるだけではなく，脅威の性質に応じた実装を行う必要がある。これに加え，PCユーザーが対策実施を意識する必要がなく，包括的に情報漏洩を防止できることも，不注意などの人為的ミスを防ぐうえで重要な要件である。

このような課題を解決するため，Windows PC向けに，次に示す主要な3種類のセキュリティ機能を提供する（**図4**参照）。

(1) リバースエンジニアリング防止ツール
(2) ハードディスク全体暗号化機能
(3) 通信暗号化機能

これらの機能は，前述した例で示した3種類の脅威（**表1**の脅威）に対処するものである。特に，ハードディスク全体暗号化機能と通信暗号化機能については，これらを組み合わせることにより，包括的なPC内データの漏洩防止が可能である。これは，特にセキュリティ上の脅威が大きいモバイルPCにおいて有効である。ハードディスク全体暗号化機能によってハードディスク内のデータを，通信暗号化機能によって通信データを，それぞれ網羅的かつ強制的に暗号化することにより，PC内外の情報をすべて暗号化し，情報漏洩を防止する。

3.2 リバースエンジニアリング防止ツール

リバースエンジニアリング防止ツールは，開発したソフトウェアに対して耐タンパ機能を付与することで，リバースエンジニアリングを困難化するソフトウェアツールである。

以下に，リバースエンジニアリング手法とそれに対する耐タンパ機能，このツールの動作などについて詳述する。

3.2.1 リバースエンジニアリング手法

リバースエンジニアリング手法には，静的解析と動的解析の2種類が存在する。

静的解析とは，対象のソフトウェアを実行せずに解析する手法である。一般的には，逆アセンブラや逆コンパイラといったツールを使用して実行ファイル（機械語）をプログラミング言語に変換し，その解析を行う。プログラムの動作を想像しながら解析する必要があるため，高い技術が必要となる。

動的解析とは，対象のソフトウェアを実行しながら解析する手法である。解析には，デバッガ（ソフトウェア動作中のCPUとメモリの状態を監視・操作するためのソフトウェア）や仮想マシンなどのツールを利用する。仮想マシンはPCのハードウェアをエミュレートするソフトウェアであり，デバッガと解析対象ソフトウェアの実行環境として使用する。動的解析では，実際のソフトウェアの動作を確認しながら解析できるため，静的解析と比較して解析が容易という利点がある。一方，実際にソフトウェアを動作させているため，不測の事態が起きる可能性がある。例えば，一部のソフトウェアは，自身に対する不正な解析を防止するために，解析を検知し，妨害のためにプログラムの異常終了，あるいは解析環境の破壊を行う場合がある。このため，静的解析とは異なる解析上の制限が存在する。

このように，二つの解析手法には一長一短があるため，状況に応じて両方の解析手法を使い分けて，リバースエンジニアリングが行われる。

3.2.2 耐タンパ機能の概要

リバースエンジニアリング防止ツールの耐タンパ機能は，静的解析と動的解析の両方を困難化する機能を備えている。

(1) 静的解析の困難化

実行ファイルの暗号化機能によって実現する〔**図5**(a)参照〕。基本的には，実行ファイル自身を暗号化し，その復号処理と暗号鍵を集中的に隠ぺいすることで保護する。これにより，逆アセンブラや逆コンパイラなどの静的解析用ツールが使用された場合でも，アセンブリ言語などのプログラミング言語に逆変換されることを防止できる。

(2) 動的解析の困難化

CPU，メモリおよびOSの状態監視により，デバッガおよび仮想マシンによる解析を検知する処理を実行ファイル

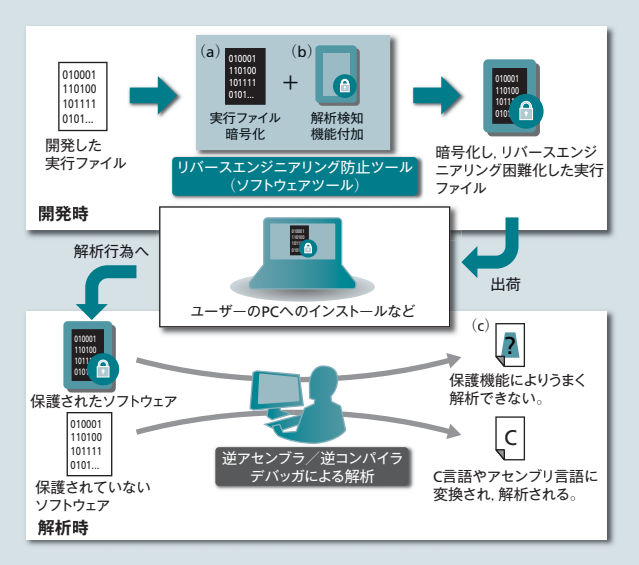


図5｜リバースエンジニアリング防止ツール

開発したソフトウェア（実行ファイル）をツールに入力するだけで，自動でリバースエンジニアリングを困難化するための耐タンパ機能を付与することができる。

に付与する〔**図5** (b) 参照〕[1), 2)]。解析行為の検知時には，実行停止などの処置をとり，解析自体の継続を阻止する〔**図5** (c) 参照〕。

また，解析検知処理へのリバースエンジニアリングを防止するため，これらの処理自体が難読化（解析困難になるように処理を複雑化すること）されており，容易に解析できないようになっている。このように多重の対策を行うことにより，リバースエンジニアリングへの耐性を高めている。

3.2.3　耐タンパ機能の実装

前項に示した耐タンパ機能をコーディングの際に組み込む場合には，おのおののプログラマにおいて耐タンパ機能に関する知識が必要になり，かつ，耐タンパ機能の追加によって作成する処理が煩雑化するため，ソフトウェア開発が困難化する。このような問題を避け，簡易にソフトウェアを保護するためには，ソースコードへの修正を行うことなく，保護対象のソフトウェアに対して耐タンパ機能を付与する必要がある。ここで特に課題となったのは，暗号化された実行ファイルの復号処理と解析検知処理の付与方法であった。

このような課題を解決するため，実行ファイルの構造やOSによるソフトウェア実行の仕組みを考慮し，実行ファイルに対して動作に影響を与えることなく，別の処理を追加する技術を開発した。この技術により，暗号化されたソフトウェアの復号処理と，解析検知処理を任意の実行ファイルに付与することができる。また，復号処理はソフトウェア起動時に自動で行われるため，オリジナルのソフトウェアと同様に起動でき，起動後も操作性は変わらない。例えば，アイコンクリックで起動するソフトウェアは，ツール適用後も同じ操作で起動し，耐タンパ機能付与前と同一の動作をする。さらに，復号されたソフトウェアは，メモリ上にのみ出力されるため，ハードディスク上から情報漏洩することがない。

このような仕組みにより，保護対象のソフトウェアをこのツールの入力として与えるだけで，耐タンパ機能を具備したソフトウェアを出力することができる（**図5** 上段参照）。出力されたソフトウェアを出荷することで，具備した耐タンパ機能によって出荷後の不正なリバースエンジニアリングからソフトウェアを保護することができる（**図5** 下段参照）。これにより，ソフトウェアからの各種情報の抽出を防止する。

3.3　ハードディスク全体暗号化機能

ハードディスク全体の強制的な暗号化により，盗難・紛失時の情報漏洩を防止する機能である。

この機能の実現においては，三つの課題があった。一つ目がOSを含めたハードディスク全体の自動的な暗号化，二つ目が暗号化されたOSの起動，三つ目がハードディスクを取り出された場合の解読防止である。

まず一つ目の課題を解決するために，暗号化機能をデバイスドライバレイヤ（フィルタドライバ）において実装することによって実現した。これにより，暗号機能はOSの一部として動作し，アプリケーションプログラムおよびOSのハードディスク書き込みが，すべて自動的に暗号化されるようになる（全体暗号化）。また，暗号機能がOSと同じレイヤで動作するため，アプリケーションプログラムの動作やユーザーの操作への影響も及ぼさない。二つ目については，プリブート認証と呼ばれるOS起動前の認証を実施することによって実現した。三つ目については，OSを復号しながら起動させる独自のブートローダを実装することによって解決した。以降では，ハードディスク全体暗号化機能においてセキュリティ上重要な要素である，全体暗号化とプリブート認証について詳しく述べる。

3.3.1　全体暗号化

全体暗号化とは，OSの出力ファイルも含めてすべてのハードディスク内のデータを強制的に暗号化する機能である（**図6** 参照）。この機能の利点の一つに，ユーザーによる暗号化漏れがなく，不注意での情報漏洩を防止できるという点がある。さらに，もう一つの利点として，OSの出力ファイルを暗号化できるという点がある。

OSの出力ファイルについては，一般に意識することは少ないと思われるが，実際にはこれらのファイルから情報が漏洩することがある。このような例にページファイルが

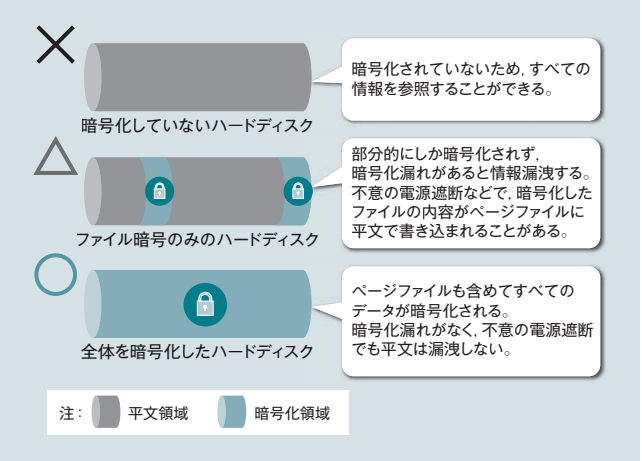


図6｜ハードディスク全体暗号化

ハードディスク全体の暗号化により，暗号化漏れを防止する。ファイル暗号では不意の事態が発生した場合に，情報漏洩を防止できない。

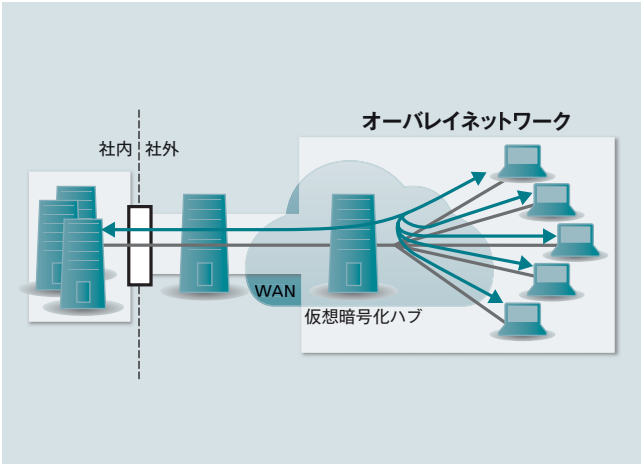


図7｜仮想暗号化ハブ型通信

Ethernetフレームを暗号化する通信方式は，ファイアウォールなどのネットワーク機器によって通信を遮断されにくいことが特長である。

ある。ページファイルとは，OSのメモリが不足したとき，一時的にメモリ内容を退避させるためのファイルである。このファイルには，メモリ内の暗号化されていない情報がユーザーの意図に関わらず保存される可能性があるため，情報漏洩の原因となりうる。ファイル暗号ではこのようなファイルは暗号化できないが，ハードディスク全体暗号化機能を利用することで暗号化でき，当該ファイルからの情報漏洩を防止できる。

3.3.2　プリブート認証

プリブート認証とは，ハードディスク全体暗号化機能によって追加されるOS起動前のユーザー認証である。この認証に成功した場合のみハードディスクが復号されるため，不正なユーザーは，ハードディスクを取り出して別のPCに接続したとしても，内容を正しく復号することはできない。さらに，独自の認証方式を採用しているためBIOSやOSの認証とは異なり，極めて強固な認証機能をPCに付与することができる。

3.4　通信暗号化機能

通信暗号化機能は，通信データの網羅的な暗号化により，通信データからの情報漏洩を防止する機能である。

この機能においては，Windows上で動作する全アプリケーションプログラムの通信データの自動的な暗号化が課題であった。

この課題を解決するため，ハードディスク全体暗号化機能と同様に，暗号化機能をデバイスドライバレイヤにおいて実装する方式を採用した。これにより，全アプリケーションプログラムの通信データは自動的に暗号化され，アプリケーションプログラムの動作やユーザーの操作性に影響を及ぼすこともない。

さらに，この機能では，以下に挙げる2種類の通信方式を用途に応じて提供可能である。

3.4.1　仮想暗号化ハブ型通信

この通信方式は，Ethernet※2)フレームを暗号化し，TCP/IP（Transmission Control Protocol/Internet Protocol）でカプセリングする通信方式である（**図7**参照）。同図に示すように，「多対多」の通信が可能である。また，通信パケット単位の認証を行うことにより，通信データの改ざんとなりすましを防止する。さらに，独自暗号アルゴリズムを使用した通信が可能であり，必要に応じて高いセキュリティを適用することもできる。このような利点に加えて，この通信方式では，「仮想暗号化ハブ」と呼ばれるサーバを介して各PCが通信する仕組みに特徴がある。

仮想暗号化ハブとは，物理的なハブのエミュレーションを行うサーバである。これにより，WAN上に単一の仮想的なネットワーク（オーバレイネットワーク）が構築され，仮想暗号化ハブに接続する社内外のPCは，同一LAN（Local Area Network）接続時と同様に通信できる。なお，多対多の通信もこの仕組みで実現している。さらに，これらの通信はTCP/IPでカプセリングされるため，HTTP（Hypertext Transfer Protocol）の80番ポートを利用して暗号通信を行うことで，ファイアウォールあるいはNAT（Network Address Translation）などを介する場合でも通信可能という特長がある。このため，外出先の無線環境を利用するときなど，通信環境を選べない場合に適した通信方式である。

3.4.2　IPsecトランスポートモード型通信

IPsec（Security Architecture for Internet Protocol）トランスポートモード型通信方式は，TCP/UDP（User Datagram Protocol）ペイロードのみを暗号化するIPsec相当の通信方

※2) Ethernetおよびイーサネットは，富士ゼロックス株式会社の登録商標である。

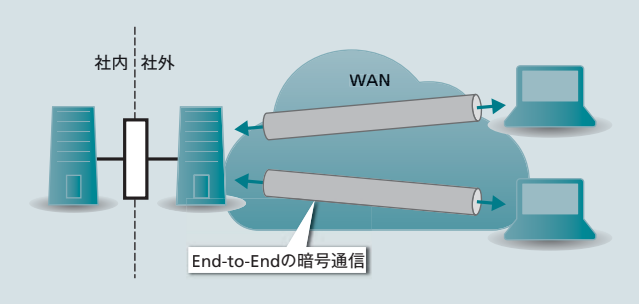


図8｜IPsecトランスポートモード型通信
IPsec（Security Architecture for Internet Protocol）トランスポートモード型通信は，TCP/UDP（Transmission Control Protocol/ User Datagram Protocol）ペイロードのみを暗号化する比較的簡易な通信方式である。

式である（**図8**参照）。同図に示すように「1対多」の通信が可能である。また，仮想暗号化ハブ型通信と同様に，通信パケット単位の認証や独自暗号アルゴリズムの利用もできる。仮想暗号化ハブ型通信と比較して簡易な通信方式であるため，スループットが高いことが特長である。このため，本社―支社間の通信など，通信環境を適切に設定できる通信区間などでの利用に適している。

4. おわりに

ここでは，情報漏洩に関わる脅威に対する日立グループの観点と，保護対策の中核となる耐タンパ技術と暗号技術，および，これらの技術を利用した情報漏洩防止技術について述べた。

高セキュリティな情報漏洩防止技術であるリバースエンジニアリング防止ツールをはじめ，ハードディスク全体暗号化機能や通信暗号化機能は，日立グループのシステム開発実績を通じて独自に蓄積した経験と，詳細なリスク分析に基づいて設計・実装されるものである。

また，今回はWindows PC向けの技術として紹介したが，PCに限らずさまざまなプラットフォームに適用可能である。特に，近年は，PCのような汎用装置のみで構成されるシステムだけでなく，専用装置で構成されるシステムに対するサイバー攻撃の懸念も高まりつつあり，社会インフラなどではセキュリティ対策の重要性が叫ばれている。このような攻撃からシステムを防御するためには，耐タンパ機能などが，あらゆる種類のソフトウェアにおいて標準的に具備されるべきであると考える。ただし，多様化しつつある種々のプラットフォームに適用する場合は，それらの要件を考慮したリスク分析と技術的な検討が必要である。

今後は，これらの情報漏洩防止技術を生かし，安全保障や社会インフラなどを含めた幅広い分野において，高度なカスタムセキュリティソリューションを提供し，より多くの社会の安全・安心に貢献していく。

参考文献など

1） Mark Vincent Yason：The Art of Unpacking，Proceedings of Black Hat 2007
https://www.blackhat.com/presentations/bh-usa-07/Yason/Whitepaper/bh-usa-07-yason-WP.pdf
2） Peter Ferrie：Attacks on Virtual Machine Emulators，
http://www.symantec.com/avcenter/reference/Virtual_Machine_Threats.pdf

執筆者紹介

白木 孝義
2007年日立製作所入社，ディフェンスシステム社 情報システム本部 エンジニアリング部 所属
現在，防衛・危機管理分野における情報セキュリティ事業に従事
IEEE Computer Society会員

佐藤 真
1993年日立製作所入社，ディフェンスシステム社 情報システム本部 ICT基盤設計部 所属
現在，情報セキュリティ関連ソフトウェアの開発に従事

野口 雅和
1998年日立製作所入社，ディフェンスシステム社 情報システム本部 エンジニアリング部 所属
現在，防衛・危機管理分野の新規事業開拓に従事
博士（情報科学）
日本数学会会員

古屋 聡一
1997年日立製作所入社，横浜研究所 情報サービス研究センタ サービスイノベーション研究部 所属
現在，サービス工学とクラウドサービスビジネスの創出に関する研究開発に従事
博士（工学）
電子情報通信学会会員，情報処理学会会員