CSS'98　（1998 年 10 月）

ＩＴセキュリティ・アーキテクチャの構築

BUILDING OF SECURITY ARCHITECTURE IN INFORMATION TECHNOLOGY

佐藤　慶浩
Yoshihiro Sato

日本ヒューレット・パッカード株式会社（〒192-8510 東京都八王子市高倉町 9-1)
Hewlett-Packard Japan, Ltd. (9-1, Takakura-Cho, Hachioji, Tokyo, 192-8510 Japan)

情報システムの構築の際にセキュリティの問題を解決する場合、技術的コンポーネントのそれぞれに局所的な対策を施すことは問題をかえって複雑にする。これを解決するために、情報セキュリティポリシーを始めとしたシステム全体を定義するセキュリティアーキテクチャの設計が有用であることを紹介する。

When you resolve security issues for building information system, it makes issues more confused that solutions are given to technical components for each. In order to avoid this happens, it is efficient that you use the designing of security architecture which is to define overall system and includes information security policies and others. This is introduction of our reference model for security architecture.

１.はじめに

1960 年代に始まったコンピュータの商用利用は、ホストコンピュータとＴＳＳ中心から、ミニコンピュータ、ネットワークによる分散処理、デスクトップＰＣの統合というように、世代を経てより柔軟な利用形態へと進化している。この間にコンピュータの性能は、以前と同じ性能を得るのに必要なコストと大きさは飛躍的に安く小さくなった。

それらのことは、システムのダウンサイジングとして企業に受け入れられてきた。

多くの低価格化、小型化は技術進歩によってもたらされたものに違いない。しかし、もともとあったいくつかを単に削り取ることでも、ダウンサイジングは行われてきた。

たとえば高可用性は上位のメインフレームには装備されていたが､初期のオープンシステムにはなかった。そのことは、ダウンサイジングをした後に本来ならば高可用性が必要とされていたところで、すぐに問題として顕在化し、その後、オープンシステムの周辺機器やコンピュータ本体にも高可用性が追加の要件として、実装された。

そのように、３歩進んで１歩下がるというようなことが、結果的に２歩進んでいるからよいということで市場に受け入れられてきた。

また、ホストネームやＩＰアドレスといった技術用語をホームＰＣの消費者である利用者が直接使うようになることは、つい最近まで予想されなかったことである。当初は、もっと簡単な概念で説明できないとインターネットの家庭への普及の妨げになるのではないかと考えられていたが、初めてＰＣを購入した利用者もマニュアルに書いてある用語を読んで設定をしている。

しかし考えてみると、コンピュータの技術者がそれらの用語を使うときと同じように利用者は理解しているだろうか。おそらく、技術的には正確ではない理解をしている人々も少なくないはずである。それでも、利用者のしたいことができれば、それは市場に受け入れられた。

情報セキュリティについての関心事の多くは、ここで述べたような２つの要素を多分に原因としている。すなわち、１つは、知らないうちに削られた部分が露呈すること。もう１つは、誤った理解の放置にあると考えている。もちろん、この他に情報セキュリティに新たな脅威が出現しているのは事実であるが、それらとこれら２つの要素の本質的な違いは、これらがビジネスの判断で自ら招き入れたものである点である。

いずれにしても、現在の情報システムには、セキュリティ上の不足部分があることは周知のものとなってきている。

不足しているものは、「張りぼて」のように後から取って付ければよいのだろうか。おそらく、それでは解決されない。追加された要件に対して、その分だけ実装を追加するのでは、その追加部分に新たな問題が

発生してしまうだろう。
　要件が追加されたら、それまでのすべての要件を含めて全体を再設計し、それに対して現状からの移行計画をたてて、それを実装することが肝要である。
　しかし、何かあるたびにすべてを白紙に戻して再構築することは投資保護の面で現実的ではない。その解決のために、設計と実装との関係を系統だてておく必要がある。それには情報システムのアーキテクチャを考えることができる。アーキテクチャはご存知のように、もともと建築のための用語である。それは、住まいをどんな外観にして、どういった機能・品質を備えさせるかを決定するものである。
　情報システム一般のアーキテクチャには様々な形態があり一般化することは難しい。しかし、その観点をセキュリティに置いた場合、そのアーキテクチャには共通のものが見出せると考えられる。本書では、これを情報技術セキュリティ・アーキテクチャと呼ぶことにし、当社が考えたモデルを例に、アーキテクチャの考察をすることにする。

２．情報システムの構成

　情報システムは、人とプロセスと技術によって構成されているものとして扱う。技術を人が使うことによって、情報システムが運用され、人が技術を使うのがプロセスである。人の存在を明示的に情報システムの構成要素として扱うことが肝要である。

３．基礎

　住居に基礎があるように、セキュリティアーキテクチャでも基礎を構築して、その上に実体を構築する。
　基礎となるものは４つある。セキュリティ原則、情報セキュリティ方針、セキュリティ評価基準・標準と教育である。

３．１　セキュリティ原則

　企業や組織（以下、単に企業とする）における情報システムのセキュリティを考える場合、それが情報セキュリティありきになってしまうことがあるが、それは誤ったアプローチであり、おそらくは正しく機能しない。
　セキュリティの要求レベルを考えるとき、その要求のよりどころとなる企業原則が存在する必要がある。逆にいうと、企業原則のうち、セキュリティに関係すると思われる項目を抜き出したものが、セキュリティ原則となる。
　セキュリティ原則では、情報システムの利用者を本質的に信頼するものとするのか、または、本質的には信頼しないとするのかによって、以後の基礎は大きく変わったものとなる。その他にも、企業にはこれに類する原則の違いがそれぞれにある。それらを拾って歩くのが、セキュリティ原則の構築（策定）となる。

３．２　情報セキュリティ方針（ポリシー）

　セキュリティ方針という用語の定義にはレベルがあって、企業全体のセキュリティ方針、部門のセキュリティ方針あるいはコンピュータシステム単体のセキュリティ方針というように様々なレベルがある。これらのレベルを正しく理解しておく必要がある。それらのレベルは３段階に大別できる。もっとも下のレベルは、装置やソフトウェアなどの方針に関するもので主として技術的なことだけを言及するものである。これに加えて、運用や管理方法などのプロセスまでを含めた２番目の段階のレベルがある。日本で多く知られているのは、この段階までである。
　しかし、この段階では人々の行動規範までは言及しないため、それについては通常は非電子的情報を対象とする既存の規定文書などを拡大解釈して済ませることになる。しかし、今日の情報システムはビジネス活動と密接なものとなっており、例外処理の発生するビジネスの現場においては、ビジネス目標の達成と情報セキュリティ維持とのトレードオフを個人が判断することは、技術やプロセスとは異なるセキュリティの問題を生み出している。この問題を人的領域として方針化するのが、３番目のレベルである。
　技術とプロセスと人を扱う、この最上位に位置するセキュリティ方針を区別して情報セキュリティ方針と呼ぶ。[1]
　前述のレベルのものは、装置セキュリティ方針や、システムセキュリティ方針などのように区別して用いるのがよいはずであるが、総称してセキュリティ方針と呼ばれるため、混同されやすいので注意する必要がある。
　情報セキュリティ方針は先のセキュリティ原則に沿ったものでなければならない。そのため、方針は企業特有のものになると考えるべきである。同じ業種・業態であると方針も似たものになる傾向があるが、原則への整合が企業自身によって検証されていなければならない。
　その観点では、なんらかのたたき台から情報セキュリティ方針をたたき上げていくというのは、必ずしも良策とはいえない。

３．３　セキュリティ評価基準と標準

　これは基礎として必須のものではないが、導入することで絶対的な指標や法制への準拠のしやすさを得ることができる。
　現時点では情報システムの安全基準が定められている業種は限られるが、ＩＳＯでの標準化作業も始まっており、過去に品質保証がそうなったように、セキュリティへの取り組みが企業の競争力の一源となることも予想される。そのときに備えて評価基準や標準を導入しておくことは有用である。
　また、セキュリティそのものの構築の理由付けが社内で得られにくい場合には、外因的説得材料として引用することもできる。

３．４　教育

先に情報システムは人、プロセス、技術で構成されるとしたが、人に対する大きな施策は教育である。たとえば、装置には何らかの設定をすれば、不具合のない限り、そのとおりに動作するが、人には手順を定めることに加えて教育・啓蒙を実施することが望ましい。特にその対象がセキュリティに関するものである場合は、必須と考えるべきである。

教育（啓蒙）するということそのものは、トラストの内容が変化しても維持されなければならないため、基礎として組み込んでおくことが必要である。

４．トラスト

情報システム全体の中で、セキュリティは単独には取り扱えない要素である。一般的には生産性とのトレードオフなどと言われるが、それらは直接には次元の違う要素である。そこで、トラストという考え方を用いることにしたい。トラストはその情報システムへの信頼性を示すレベルである。

トラストの構成要素は、セキュリティと可用性、性能の３つである。これらの３要素に対する要求レベルを満たすとき、情報システムはトラストなものと言うことができる。それぞれの要求レベルの満足度がアンバランスか、一部の要素しか評価されていない場合には、そのシステムが情報システムの構成要素である人すべてにとって、信頼の置けるものかは疑ってかかるべきである。

３つの要素は、それぞれにさらに細分化して扱うことができる。セキュリティは、認証、認可、保全性、機密性、否認不能性の５つの要素に細分できる。可用性は、継続性、耐久性、回復性、一貫性の４つの要素に細分できる。性能は、他の２つのような特性的な細分化はここではしないが、実装における層や部位といった局所化で定量的に測定可能なものとして細分することは容易である。

本書の読者はセキュリティ技術に精通しているものと思われるので、細分項目については、ここでは詳述を割愛する。[2]

トラストにおいては、セキュリティと他の２つがトレードオフになることが多い。そのため、可用性と性能の２つを生産性と結びつけることが一般に行われる。その意味に限っては、セキュリティと生産性をトレードオフするという表現は間違えではない。しかし、生産性と言った場合、ビジネスそのものの成果も含まれるため、情報システムの可用性と性能と限定した方が扱いやすい。

５．制御機構

基礎の上でトラストを構築することを示したが、基礎の上にはもう１つ制御機構というブロックが存在する。

制御機構は、アクセス、管理、測定、監視と検出、変更管理、監査という要素で構成する。

５．１　アクセス

もともとアクセスは情報システムの装置に対する直接の物理的アクセスをさしていたが、近年では、これに遠隔地から装置を操作するネットワークアクセスが、装置の一般的な機能として備わっている。

セキュリティの観点では、これらを区別して考える方が精度があがる。

物理的アクセスの場合、装置と操作主体との経路は信頼できるものとすることができるが、ネットワークアクセスの場合、その経路が信頼できるものとは限らない。多くの場合は、経路そのものとして情報システムの一部としてのネットワークを利用することになることからも、ネットワークアクセスには物理的アクセスよりも厳しい制御を設けることが必要となる。

５．２　管理

旧来のホスト型情報システムでは、集中管理はシステム装備のものをそのまま使うことすらできたであろうが、近年の分散システムでは、集中管理は望めない。したがって、管理はシステム機能ではなく制御機構として検討されるべき項目である。

５．３　測定

測定は構成要素の動作状況を定量化するための機能であり、分析や報告のために使用する。

測定機能を情報システムに装備することは、システムを管理・運営する側には有用であるが、利用者側の関心事でないことは多い。この機能は、そのため単独で予算化しにくい要素となる。本モデルでは、測定機能と課金機能を同体化することとした。

セキュリティの観点においても、不正なアクセスの兆候として、普段とは異なるシステム利用あるいはネットワーク利用が考えられるが、これが課金となって現れるとアクセス統計としてよりも日常的興味の対象になり発見されやすい。

著名な書「カッコウはコンピュータに卵を産む」では、コンピュータ請求書の７５セントの違いが最初のきっかけになったとしている。

５．４　監視と検出

動作を監視し、その結果から問題を検出することも制御機構の重要な要素である。

管理や測定と区別しているのは、この監視機能はセキュリティシステムを対象とするからである。管理や測定は、情報システム全般を扱うが、この機能はセキュリティ問題の検出を目的とする。

監視には、受動的な方式と動的な方式が考えられる。

受動的な方式では、情報システム本来の動作による兆候を監視する。動的な方式では、監視機能そのものがセキュリティシステムの機能に能動的に処理を与え

て、その結果を検証する。どちらの方式にするか、または両方にするかを制御機構として定めておくことで、少なくともどちらもないということを予防する。

５．５　変更管理

分散環境においては、変更の同期性の欠如は、そのまま保全性の欠如につながる。
このことは空間的にも時間的にも重要であり、場合によっては組織的対策を伴う局面もある。
セキュリティシステムの最初の構築時と同等な注意をその後の変更時に維持するのは大変な努力を要するが、そのレベルが下がっては意味がないのも事実である。
過失によるセキュリティ問題の多くが、変更時に生じることからも変更管理は制御機構に組み込まれるべきものである。
また、変更管理は、アクセス機能同様にネットワークからの変更にも配慮することが、分散環境における管理機能の強化により、より重要な観点となる。
このため、アクセスと管理とは独立した要素として扱うことが有効である。

５．６　監査

監査において基本的に重要なことは、独立性と証跡保全である。
監査機能は、他のどの要素とも独立していなければならず、機密度合いとしては、機密データ自身よりもむしろ高くあるべきである。管理機能と監査機能が同一化しているようなシステムはセキュリティレベルの低いもの、あるいはセキュリティを装備していないものとみなすべきである。
そのことは、証跡の保全性についても同様で、システム管理者が監査証跡を操作できるシステムは、高いレベルにはなり得ない。
監査の独立性と証跡の保全性を保てれば、そのレベルによって（すなわち、そのレベルと同程度に）システムは信任され得ると言える。
このことは、主としては装置に言えることであるが、人を含めた情報システム全体の範囲に適用することもできる。
人の領域まで含んだ場合には、自己監査、内部監査、外部監査の区別により、監査機能の定義を行なう必要がある。

６．まとめ

以上の説明において、個々の要素の中の考察は、これまで語り尽くされたものに他ならない。
ここで紹介したのは、セキュリティアーキテクチャである。個々の要素が別々に考察されているのと異なり、それらの関係を示す点が重要である。
アーキテクティングの難しさは、それが全体を相互背反・集合網羅するような部分要素を定義することであるが、ここでは、それを集合網羅するブロックと相互背反するブロック内要素という２階層のモデルで簡略して一般化することを試みた。
このモデルの汎用性の高さは、情報システムの目的であるビジネス支援に関する要件を奥行き方向に隠蔽しているところにあるが、トラストモデルにより、可用性と性能の要件については、直接取り扱うことでセキュリティ要件偏重にならないものにしている。
このセキュリティ・アーキテクチャ・モデルに基づいて情報システムのセキュリティ設計を行なうことができる。さらに、既存の情報システムをこのモデルに当てはめることで、現状をモデル化することにも使用できるため、その結果を用いて移行計画を策定することにも利用できるものとなっている。

また、このアーキテクチャの特長として基礎のブロックがあげられる。評価基準を除いては、この部分に技術的な要素を入れていない。基本的にビジネス的な要素に限定している。このようにすることで、技術の変化によって基礎が変わることのないように配慮した。
情報システムのセキュリティに問題が発生した場合、その結果の影響は、技術的な問題ではなくビジネス上の問題になるであろう。それであれば、情報システムにおけるセキュリティの課題は、企業のビジネスの課題であり、ビジネス判断の責任者が参加して解決に当たる問題である。その参加を現実のものにするためにも、基礎の部分に多分にビジネスの要素を入れた。逆に、それ以外の技術領域との独立性を持たせることで、その方々の参加を現実的なものとするモデルに仕上がっていると考えている。

セキュリティはどれだけやればよいのか？という疑問をよく受ける。これは、セキュリティはどれだけやらないのかという観点で捉える方が本質的であると考えている。やらないと決めた部分がリスクとなるので、そのリスクをビジネスが受け入れ可能かを判断することで、どれだけやらないのかが決まるのではないだろうか。
情報技術の有益な進歩があると、不正な技術も進歩する。それによって、新しいリスクが生まれる。そのときに、そのリスクが受け入れられるものかを技術的だけではない視点で判断することで、継続的な情報システムセキュリティの維持が可能である。

これらの課題を解決する方法論として、セキュリティアーキテクチャを考察してみた。今後もこのモデルの検証を続け、より汎用的で利用しやすいアーキテクチャモデルに仕上げていきたいと思う。

参考文献

1) 「情報セキュリティポリシーの必要性と策定方法」
情報処理学会ＥＩＰ研究会，佐藤慶浩

2) 「分散コンピューティングセキュリティ」
グレン・ブルース＋ロブ・デンプシー著
HEWLETT-PACKARD PROFESSIONAL BOOKS
プレンティスホール出版 ISBN4-89471-040-4
http://yosihiro.com/book/lock-the-door/