正規化網路安全之研究

A Formal Approach to Computer Network Security

陳志誠
Patrick Shicheng Chen

中央警察大學資訊管理系
桃園縣．龜山鄉 333
chenps@sun4.cpu.edu.tw

摘 要

根據 Coulouris 等人[9]的看法，一個計算系統之安全策略(Security Policy)必須是可以正規証明的。資訊安全的認定，是通訊主體(Agent)對環境知識(Knowledge)的擁有及對該知識的信任(Belief)。主體所擁有的知識往往是不完全的; 欠缺的部分只能假設。本文根據作者所建議的一種在欠缺資訊條件下進行推理(Reasoning by Default[8])的模邏輯(Modal Logic)，建立一個網路通訊之安全模型，對資訊安全作基礎理論研究。文中首先介紹該邏輯之基本結構，其次將此邏輯引入於網路通訊基本模型，建構其公理系統，尤其是介紹發送、接收及安全等基本概念之公理，然後推導出安全的通訊。該理論之實作是一個安全系統的建立。我們建議了一種由小而大的方法 —— 由原子的安全基礎(Atomic Security Base)開始，擴展到完整的安全體系。由於本文只初步的介紹了基本通訊模型，未來將可利用此邏輯對各種通訊協定作正確性檢驗。

Abstract

According to Coulouris et al.[9], the security of a system, including its security policy and implementations, should be formally provable. Security is a matter of belief and knowledge, a belief based on the knowledge of the environment. In the real world the communicating agents cannot always acquire complete information about the communication environment. Therefore, adding some assumptions to its theory is necessary. In this paper a secure communication model is introduced based on a modal logic for belief and knowledge suggested by the author. This logic facilitates reasoning by default[8]. We first introduce the overview of the logic and, then, construct an axiomatic system for the basic communication model as a theoretical foundation for the study of data security. The axiom system, including axioms for send/receive-operations and axioms for security, can be used for deducing communication security. In the implementation we suggest a method, along which we can build on the top of atomic security bases a complete secure system. Though only basic communication activities are modeled in this paper, all other communication protocols can be verified in the frame of the logic.

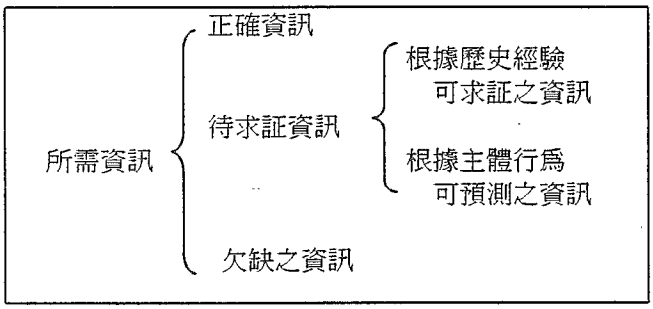
一．前言

根據 Coulouris 等人[9]的看法，一個計算系統之安全策略必須是可以正規証明的。究其立論理由應是系統安全攸關重要，百密不得一疏。欲達系統之安全要求，惟有將系統中與安全相關之所有物件均以正規化描述，然後借助於公理系統及推理規則，對系統中通訊主體(Communicating Agent)之一切行爲，進行分析，方可証明其安全性。除此之外，一個正規化研究有助於

- **安全體系之建立**: 我們可採取雛形法(Prototyping)的方式，逐步建構一個完整的安全體系。
- **系統之安全性分析**: 安全性分析牽涉極爲廣泛，若無正規化描述，則難以對系統進行整體分析，找出其不足或缺陷之處，以防止危害之發生。
- **通訊協定正確性之檢驗**: 系統通訊協定爲各通訊主體共同遵守的規則，其正確性至關重要，惟有正規化的分析與驗証，方能保障通訊規則之正確無訛。
- **危害發生時之補救**:系統萬一不幸遭入侵，想作亡羊補牢，亦不可頭痛醫頭，腳痛醫腳，而須作全盤之檢討，此時更有賴於正規化系統。

從歷史發展看來，近代資訊安全之研究，從 Bell & LaPadula 於 1976 年提出 Multics 概念[6]，將傳統機密分等措施加以理論化起，即以很嚴謹的

方法進行研究。其後隨著計算機網路的發展，分散式系統的建立，人們更意識到資訊安全之研究需要借助於邏輯作爲基礎。對現行的安全策略及措施，學者們發表了很多精闢的論文如 Denning [10]、Goguen & Meseguer [11]建立了優良的理論體系。這些系統的共通性是建立在"確定性"的基礎之上，並促使整個體系忠實的被實現出來，以保障高度的安全。然而，確定性有賴於完全的資訊，這就很難在真實世界中取得。因此，真實世界裡的系統，往往只能約略的、樂觀的說，它們是安全的。



[圖 1] 推理所需之資訊

在真實世界中，我們往往只能取得部份的環境資訊。於是在實現安全系統時便應區分正確的資訊、待求証的資訊及欠缺的資訊三種情況[1][如圖 1]。其中正確的資訊可以直接引用，另外兩種情況，則有賴於運用現有的資訊加上部分的假設來推演驗証。這裡所說的假設可以再細分爲歷史的經驗及對通訊主體的行爲之預測。因此，建構系統時依賴的是信任(Belief[2])，信任是有條件的，它是根據環境知識而定的，當接到矛盾的資訊時信任是可駁斥的(Refutable)。推論安全性所需的知識包括發送者／中轉者身份之確認、資料有無被竄改及通道之安全等等。

是故，信任無法用經典的謂詞邏輯(Predicate Logic)來單調推理(Monotonic Reasoning)得知。一般而言，人們轉而求助於模邏輯 (Modal Logic) [7] [13]，因爲模邏輯能檢驗各種可能世界(Possible Worlds)，而其中之一可能爲真實世界。當系統中的某一部份受到安全危害時，將連帶使我們對其它部份的信任大受影響。於是學者建議了一些有關信任的非調單調邏輯(Non-Monotonic Logic)，如 Moser [16] ， Rangan [17]，來幫助我們，正規的推算這種影響性。先前所提以確定性爲基礎的正規化方法，則無法讓我們適切的作此類推理。

信任的邏輯可以由例如 S5 的模邏輯來實現[12]。但是 S5 模邏輯主要在於表示知識。知識與信任之間略有不同，人們不一定相信知識。信任的邏輯可以由鬆弛 KD45 模邏輯而得到: 一個通訊主體可以信任含有待求証的命題或無法求証的命題之知識；但它不會信任一個明顯錯誤的命題。當資訊欠缺時，可以加入一些非邏輯的論點，此時學者又有兩種主張:

- 傾向於不信任者: 如 McDermott & Doyle [14]及 Moore[15]主張當資訊欠缺時而無法証明某一命題，則不信任含該命題的知識。
- 傾向於信任者: 如 Moser [16] 主張當資訊欠缺時而無法証明某一命題，則信任含該命題的知識。

此兩種學說將導致截然不同的結果: 前者就安全而言，是較有保障的，因爲人們不隨便相信沒有根據的知識；但在實用上卻失之嚴苛。後者爲了不輕信沒有根據的知識，所以必須加上其它條件。例如 Moser [16]便引入了 *unless*(除非)算子。其用法如在陳述句 "A 信任 B ，除非 A 信任 C" 中，若能証明"A 信任 C"，則"A 信任 B"的知識是可以保留的。

國內對於資訊安全的研究，成績斐然，如張真誠[1]、賴溪松[5] 等(僅舉數例)，然而大都集中於密碼學及安全通訊協定之上。這些都是屬於安全機制之探討，較少涉及安全策略。楊　千等人[4]等討論了安全策略，但那是從管理角度作定性的探討。反之，本研究之進行，則是由邏輯出發，是正規化研究方向上的一個努力，期使資訊安全學科能有更紮實的基礎。

綜上文獻研究及問題分析，想爲資訊安全確立一個正規體系，必先解決資訊欠缺的問題。於是本文根據作者所建議的一種可在欠缺資訊條件下進行推理(Reasoning by Default[8])的模邏輯(Modal Logic)，建立一個網路通訊之安全模型，對資訊安全作基礎理論研究。在語言中引入一個 *by_default*(缺席)算子，該算子之運算數爲知識，而非信任[3]。這個邏輯建立在 S5 知識與信任的單調邏輯的基礎上，擴充以非單調的 by_default 算子。

本文第二節介紹該邏輯之基本結構，第三節將此邏輯引入於網路通訊基本模型，建構其公理

[1] 錯誤的資訊應在排除之外，不可引用。

[2] 我們混用了 Belief 和 Trust 。 Belief 是主觀的、有根據的臆測； Trust 是對外界人或事物之信任。在通訊行爲中，一個主體往往是需要信任其它主體的行爲；惟有在缺乏資訊的情況下，才作某種臆測。本文全用 Belief 。

[3] Moser[16]引入的 unless(除非)算子之運算數爲信任。然而信任由知識而來。從知識到信任必須經過轉換的過程。這種過程隨著不同的邏輯而有不同的定義。正本清源，本文之缺席算子所引進的假設爲知識，應是合宜的。

正規化網路安全之研究

A Formal Approach to Computer Network Security

陳志誠
Patrick Shicheng Chen

中央警察大學資訊管理系
桃園縣．龜山鄉 333
chenps@sun4.cpu.edu.tw

摘 要

根據 Coulouris 等人[9]的看法，一個計算系統之安全策略(Security Policy)必須是可以正規証明的。資訊安全的認定，是通訊主體(Agent)對環境知識(Knowledge)的擁有及對該知識的信任(Belief)。主體所擁有的知識往往是不完全的；欠缺的部分只能假設。本文根據作者所建議的一種在欠缺資訊條件下進行推理(Reasoning by Default[8])的模邏輯(Modal Logic)，建立一個網路通訊之安全模型，對資訊安全作基礎理論研究。文中首先介紹該邏輯之基本結構，其次將此邏輯引入於網路通訊基本模型，建構其公理系統，尤其是介紹發送、接收及安全等基本概念之公理，然後推導出安全的通訊。該理論之實作是一個安全系統的建立。我們建議了一種由小而大的方法 —— 由原子的安全基礎(Atomic Security Base)開始，擴展到完整的安全體系。由於本文只初步的介紹了基本通訊模型，未來將可利用此邏輯對各種通訊協定作正確性檢驗。

Abstract

According to Coulouris et al.[9], the security of a system, including its security policy and implementations, should be formally provable. Security is a matter of belief and knowledge, a belief based on the knowledge of the environment. In the real world the communicating agents cannot always acquire complete information about the communication environment. Therefore, adding some assumptions to its theory is necessary. In this paper a secure communication model is introduced based on a modal logic for belief and knowledge suggested by the author. This logic facilitates reasoning by default[8]. We first introduce the overview of the logic and, then, construct an axiomatic system for the basic communication model as a theoretical foundation for the study of data security. The axiom system, including axioms for send/receive-operations and axioms for security, can be used for deducing communication security. In the implementation we suggest a method, along which we can build on the top of atomic security bases a complete secure system. Though only basic communication activities are modeled in this paper, all other communication protocols can be verified in the frame of the logic.

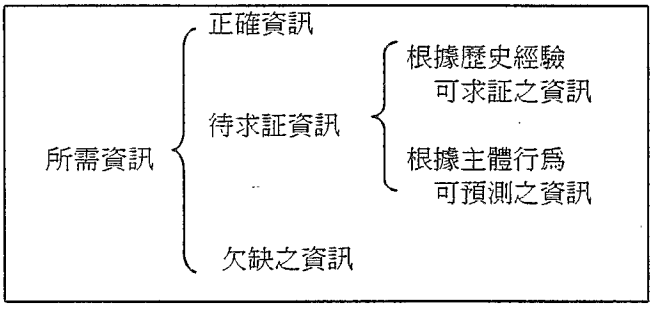
一．前言

根據 Coulouris 等人[9]的看法，一個計算系統之安全策略必須是可以正規証明的。究其立論理由應是系統安全攸關重要，百密不得一疏。欲達系統之安全要求，惟有將系統中與安全相關之所有物件均以正規化描述，然後借助於公理系統及推理規則，對系統中通訊主體(Communicating Agent)之一切行爲，進行分析，方可証明其安全性。除此之外，一個正規化研究有助於

- **安全體系之建立**：我們可採取雛形法(Prototyping)的方式，逐步建構一個完整的安全體系。
- **系統之安全性分析**：安全性分析牽涉極爲廣泛，若無正規化描述，則難以對系統進行整體分析，找出其不足或缺陷之處，以防止危害之發生。
- **通訊協定正確性之檢驗**：系統通訊協定爲各通訊主體共同遵守的規則，其正確性至關重要，惟有正規化的分析與驗証，方能保障通訊規則之正確無訛。
- **危害發生時之補救**：系統萬一不幸遭入侵，想作亡羊補牢，亦不可頭痛醫頭，腳痛醫腳，而須作全盤之檢討，此時更有賴於正規化系統。

從歷史發展看來，近代資訊安全之研究，從 Bell & LaPadula 於 1976 年提出 Multics 概念[6]，將傳統機密分等措施加以理論化起，即以很嚴謹的

方法進行研究。其後隨著計算機網路的發展，分散式系統的建立，人們更意識到資訊安全之研究需要借助於邏輯作爲基礎。對現行的安全策略及措施，學者們發表了很多精闢的論文如 Denning [10]、Goguen & Meseguer [11]建立了優良的理論體系。這些系統的共通性是建立在"確定性"的基礎之上，並促使整個體系忠實的被實現出來，以保障高度的安全。然而，確定性有賴於完全的資訊，這就很難在真實世界中取得。因此，真實世界裡的系統，往往只能約略的、樂觀的說，它們是安全的。



[圖 1] 推理所需之資訊

在真實世界中，我們往往只能取得部份的環境資訊。於是在實現安全系統時便應區分正確的資訊、待求証的資訊及欠缺的資訊三種情況[1][如圖 1]。其中正確的資訊可以直接引用，另外兩種情況，則有賴於運用現有的資訊加上部分的假設來推演驗証。這裡所說的假設可以再細分爲歷史的經驗及對通訊主體的行爲之預測。因此，建構系統時依賴的是信任(Belief[2])，信任是有條件的，它是根據環境知識而定的，當接到矛盾的資訊時信任是可駁斥的(Refutable)。推論安全性所需的知識包括發送者／中轉者身份之確認、資料有無被竄改及通道之安全等等。

是故，信任無法用經典的謂詞邏輯(Predicate Logic)來單調推理(Monotonic Reasoning)得知。一般而言，人們轉而求助於模邏輯 (Modal Logic) [7] [13]，因爲模邏輯能檢驗各種可能世界(Possible Worlds)，而其中之一可能爲真實世界。當系統中的某一部份受到安全危害時，將連帶使我們對其它部份的信任大受影響。於是學者建議了一些有關信任的非調單調邏輯(Non-Monotonic Logic)，如 Moser [16] ， Rangan [17]，來幫助我們，正規的推算這種影響性。先前所提以確定性爲基礎的正規化方法，則無法讓我們適切的作此類推理。

信任的邏輯可以由例如 S5 的模邏輯來實現[12]。但是 S5 模邏輯主要在於表示知識。知識與信任之間略有不同，人們不一定相信知識。信任的邏輯可以由鬆弛 KD45 模邏輯而得到: 一個通訊主體可以信任含有待求証的命題或無法求証的命題之知識；但它不會信任一個明顯錯誤的命題。當資訊欠缺時，可以加入一些非邏輯的論點，此時學者又有兩種主張:

- 傾向於不信任者: 如 McDermott & Doyle [14]及 Moore[15]主張當資訊欠缺時而無法証明某一命題，則不信任含該命題的知識。
- 傾向於信任者: 如 Moser [16] 主張當資訊欠缺時而無法証明某一命題，則信任含該命題的知識。

此兩種學說將導致截然不同的結果: 前者就安全而言，是較有保障的，因爲人們不隨便相信沒有根據的知識；但在實用上卻失之嚴苛。後者爲了不輕信沒有根據的知識，所以必須加上其它條件。例如 Moser [16]便引入了 *unless*(除非)算子。其用法如在陳述句 " A 信任 B ，除非 A 信任 C " 中，若能証明"A 信任 C"，則"A 信任 B"的知識是可以保留的。

國內對於資訊安全的研究，成績斐然，如張真誠[1]、賴溪松[5] 等(僅舉數例)，然而大都集中於密碼學及安全通訊協定之上。這些都是屬於安全機制之探討，較少涉及安全策略。楊　千等人[4]等討論了安全策略，但那是從管理角度作定性的探討。反之，本研究之進行，則是由邏輯出發，是正規化研究方向上的一個努力，期使資訊安全學科能有更紮實的基礎。

綜上文獻研究及問題分析，想爲資訊安全確立一個正規體系，必先解決資訊欠缺的問題。於是本文根據作者所建議的一種可在欠缺資訊條件下進行推理(Reasoning by Default[8])的模邏輯(Modal Logic)，建立一個網路通訊之安全模型，對資訊安全作基礎理論研究。在語言中引入一個 *by_default*(缺席)算子，該算子之運算數爲知識，而非信任[3]。這個邏輯建立在 S5 知識與信任的單調邏輯的基礎上，擴充以非單調的 by_default 算子。

本文第二節介紹該邏輯之基本結構，第三節將此邏輯引入於網路通訊基本模型，建構其公理

---

[1] 錯誤的資訊應在排除之外，不可引用。

[2] 我們混用了 Belief 和 Trust 。 Belief 是主觀的、有根據的臆測； Trust 是對外界人或事物之信任。在通訊行爲中，一個主體往往是需要信任其它主體的行爲；惟有在缺乏資訊的情況下，才作某種臆測。本文全用 Belief 。

[3] Moser[16]引入的 unless(除非)算子之運算數爲信任。然而信任由知識而來。從知識到信任必須經過轉換的過程。這種過程隨著不同的邏輯而有不同的定義。正本清源，本文之缺席算子所引進的假設爲知識，應是合宜的。

系統，尤其是介紹發送、接收及安全等基本概念之公理，然後推導出安全的通訊。該理論之實作闡述於第四節 —— 一個安全系統之建立，我們建議了一種由小而大的方法 —— 由原子的安全基礎開始，擴展到完整的安全體系。由於本文只初步的介紹了基本通訊模型，在結論中我們展望未來，將可利用此邏輯對各種通訊協定作正確性檢驗，對改良通訊協定將是很大助益。

2. 網路安全之邏輯體系

令 *i,j,...*表示通訊主體，而 *p, q , ...*表示命題，則二元算子 $B(i,p)$或簡寫爲 $B_i(p)$表示通訊主體 *i* 信任命題 *p* 。用類似的方法可以定義 $K_i(p)$ 表示通訊主體 *i* 有命題 *p* 的知識。完型公式(Well-Formed Formulae)的集合是包含下列之最小集合

(1) 原始公式(Primitive Formulae) ;

(2) 複雜公式(Complex Formulae)，由原始公式 *F, G, ...*等加上命題連結符號⇒、≡、¬、∧、∨ 等依一定規則組合而成；

(3) $B_i(H)$及 $K_i(H)$，其中 *H* 爲原始公式或複雜公式。

2.1 知識之公理系統

標準的 S5 公理及推理規則，將用於本系統中，作爲知識之推理之用。

(A1) $K_i(p) \Rightarrow p$

(A2) $K_i(p) \wedge K_i(p \Rightarrow q) \Rightarrow K_i(q)$

此公理表示了知識之間的推移關係。

(A3) $\neg K_i(p) \Rightarrow K_i(\neg K_i(p))$

此公理稱爲*反面自省*(Negative Introspection)，其意義爲若通訊主體 *i* 沒有 *p* 的知識，那麼該主體應自知沒有這個知識(不知爲不知)。其對偶爲*正面自省*(Positive Introspection)， $K_i(p) \Rightarrow K_i(K_i(p))$ 通訊主體 *i* 有 *p* 的知識，那麼該主體應自知有這個知識(知之爲知之)。此定理可由以下公理及 A(1)証明而得。

(A4) $\vdash p$ infer $\vdash K_i(p)$

此公理表示，若 *p* 爲真，則可以推知主體 i 擁有 *p* 這個知識。這是一種樂觀主義者的作法: 只要 *p* 是正確的， *i* 就具有 *p* 的知識!

2.2 信任之公理系統

對於信任之單調邏輯，我們利用模邏輯 KD45 之公理及推理規則

(A5) $K_i(p) \Rightarrow B_i(p)$

此公理將知識與信任之間的關係表示出來，一個主體有了 *p* 的知識，他就會信任 *p* 。

(A6) $B_i(p) \wedge B_i(p \Rightarrow q) \Rightarrow B_i(q)$

此公理表示了信任之間的推移關係。

(A7) $B_i(p) \Rightarrow B_i(B_i(p))$

(A8) $\neg B_i(p) \Rightarrow B_i(\neg B_i(p))$

(A9) $\neg B_i(false)$

表示一個主體不信任錯誤的事。

[定理 1] $\vdash p$ infer $\vdash B_i(p)$

[証] 由(A4)知 $\vdash p$ infer $\vdash K_i(p)$；再由(A5) $K_i(p) \Rightarrow B_i(q)$；所以 $\vdash p$ infer $\vdash B_i(p)$. ☑

[定理 2] $B_i(p) \equiv B_i(B_i(p))$

[証] 由(A9)得知 *i* 不信任錯誤之命題，因此若 *p* 爲真，亦即 $\vdash p$ ，可進而由

[定理 1]推知 $B_i(p)$爲真。於是 $\vdash B_i(B_i(p))$。☑

利用類似的方法可証明下列定理:

[定理 3] $\neg B_i(p) \equiv B_i(\neg B_i(p))$

以下之引理，均易於証明:

[引理 1] $B_i(p \wedge q) \equiv B_i(p) \wedge B_i(q)$

[引理 2] $B_i(p) \vee B_i(q) \Rightarrow B_i(p \vee q)$

此引理之反方向 $B_i(p \vee q) \Rightarrow B_i(p) \vee B_i(q)$ 不成立，因爲若 *p* 與 *q* 之間有相依性，如 $p \Rightarrow q$，則 *i* 對 *p* 和 *q* 應採一致的態度，當 *p* 或 *q* 全爲假時， *i* 無法信任它們。

[引理 3] $B_i(\neg p) \Rightarrow \neg B_i(p)$

此引理之反方向 $\neg B_i(p) \Rightarrow B_i(\neg p)$不成立，因爲 *i* 不信任 *p* ，並不代表 *i* 有足夠的知識去信任¬*p* 。因此， $B_i(p) \vee B_i(\neg p)$ 並不恆真。

[引理 4] $\vdash \neg(B_i(p) \wedge B_i(\neg p))$

此引理排除了模稜兩可的情況。

2.3 信任之非單調邏輯

在我們的非單調邏輯中，對 *p* 的信任，除非明示的被駁斥之外，假設爲真。這個邏輯所決定的語言中包含了 by_default 算子。一個語句 *G* 具有如下型式

$$B_i(p) \ by\_default \ F$$

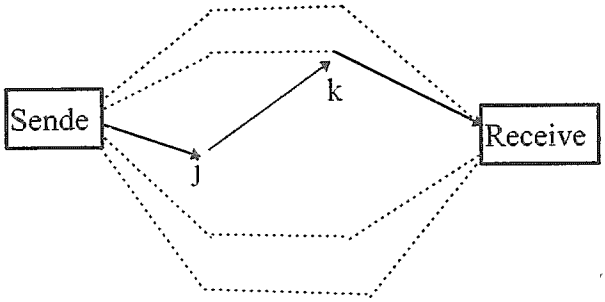
表示欠缺 *F* 這個條件(一個公式)下， 通訊主體 *i* 信任 *p* 。當 *F* 爲空集合時，表示 *i* 無條件的、單純的信任 *p* 。既然 *F* 是一個公式，便可賦予邏輯值。假設 *G* 中各謂詞之參數均爲原子公式，則我們可以得到如下之真假值表: (其中 Y=Yes; N=No)

$B_i(p)$	F	$B_i(p)$ *by_default* F
Y	Y	Y
Y	N	Y
N	N	Y
N	Y	Y, N

在最後一種情況下，若在可能世界中，有一個世界 x , $F(x)$為真，則 $B_i(p)$ *by_default* F 為假；否則，$B_i(p)$ *by_default* F 為真。

3.在通訊上的應用

既然安全體系應建立在邏輯的基礎上，以下我們就借助於一個基本通訊模型，來說明上述系統之應用。[圖 3]中假設在源頭(Source: s)的發送端(Sender)透過網路，將信息(Message: m) 傳送至在終點(Destination: d)的接收端(Receiver)。途中可能經過中間站 j, k,...等。



[圖 3] 網路通訊之基本模型

以下的謂詞記號將在本文中使用:

- $send_i(m, s, d)$: 表示通訊主體 i 由 s 向 d 發送信息 m 。
- $receive_j(m, s, d)$: 表示通訊主體 j 在 d 收到由 s 送來的信息 m 。
- key(k, i): 表示運用了屬於通訊主體 i 的一個金匙 k 。
- encrypt(m, k): 表示信息 m 是利用 k 加密的。
- trustworthy(i): 表示通訊主體 i 是可靠的。
- secure(k): 表示 k 是安全的金匙。
- safe_channel(s, d): 表示由地點 s 到地點 d 之間的通道是安全的。

3.1 通訊協定之公理系統

根據上述例子，我們將運用前一章所介紹之邏輯，正規定義通訊主體之行爲，亦即他們是否信任通訊之安全，及他們所信任的是否正確。在此，知識是由 send 、 receive 、 secure 、...等原子命題和連結詞所構成。

- 發送及接收公理

(SR1) $send_i(m, s, d) \Rightarrow$
$B_i(send_i(m, s, d)) \wedge (B_i(receive_j(m, s, d))$
by_default (safe_channel(s,d)))

意思是說，當一個發送行爲發生時，發送主體 i 自知 m 已發送出去，且他知道在假設安全路徑的前提下，在終點的 j 應收到 m 。

(SR2) $receive_j(m, s, d) \Rightarrow$
$B_j(receive_j(m, s, d))$
收到信息 m 時，主體 j 自知信息已經收悉。

(SR3) $receive_j(encrypt(m,k), s, d) \Rightarrow$
$B_j(send_i(encrypt(m,k), s, d)$ by_default
(key(m, i) $\wedge$ safe_channel(s, d))
收到加密的信息 m 時，主體 j 假設該金匙是屬於在 s 的 i 所有的，並且由 s 到 d 的通道是安全的，信任該信息是由 i 在 s 加密後送出的。

(SR4) $send_i(m, s, d') \wedge send_j(m, d', d) \Rightarrow$
$send_i(m, s, d)$ by_default
trustworthy(j)
這是在網路中安全轉送信息的情形，其前提條件是，在中間站 d'的 j 必須是可靠的。

3.2 安全公理

(SA1) $B_j(key(k, i)) \Rightarrow$
$B_j(secure(k))$ by_default
($send_i(encrypt(m,k), s, d) \wedge$
$receive_j(encrypt(m,k), s, d)$)
主體 j 唯有在它收到一個由在 s 的 i 轉來的、利用 k 加密的信息 m 的假設前提下，才信任金匙 k 是安全的。

3.3 公理之引伸

在介紹了發送、接收及安全之公理後，我們在此提出一些引理，它們可以由上述公理直接演繹得知。其中欠缺的資訊是利用 by_default 算子引入補全，在實際運作中，若有新的資訊加入，則可駁斥推理之結果。這兩個引理是安全通訊所期望的。

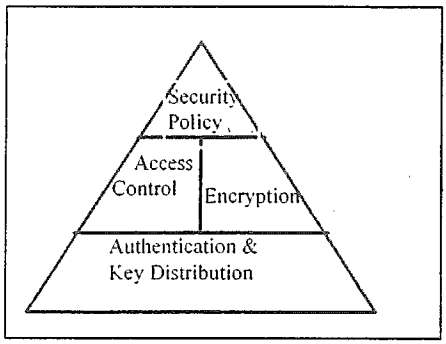
[引理 1] $send_i(encrypt(m, k), s, d) \Rightarrow$
$B_i(secure(k))$ by_default
safe_channel(s, d)
只要從 s 到 d 的通道是安全的，那麼初始發送者 i 可以信任該信息將安全的抵達。

[引理 2] $receive_j(encrypt(m, k), s, d) \Rightarrow$
$B_j(secure(k))$ by_default
safe_channel(s, d)
只要從 s 到 d 的通道是安全的，那麼最終接收者 j 可以信任金匙 k 是安全的。

4. 實作之建議

邏輯系統之實作，可依由小而大的原則進行。後選方法之一是雛型法(Prototyping) 。我們建議以一個極小的可信賴元件，作爲基礎。借由這個可信賴基礎及儲存設備，建立一個可信賴伺服器(Trusted Driver)，配上一系列的實體控制（如防止載入系統程式）及安全的通訊通道，則可得到一個安全的系統。

在安全系統中，首先要確定的是安全策略。它的實現則藉由安全機制(Security Mechanism)。安全機制一般使用個三種技術：密碼學(Cryptography)、認証(Authentication)及存取控制(Access Control)，用以實現安全策略。它們之間的關係可以構成一個金字塔[如圖 4]。



[圖 4] 安全策略與安全機關係

除了內部系統之安全問題外，組織內部網路(Intranet)與 Internet 連結時所要強調的是保密問題。作爲私有網路，其機密性較易維護，一旦與公共網路相銜接，則應採取很週延的安全措施。因此，本研究建議先研擬一個安全策略，它必須是可以正規化証明的。再以模邏輯(Modal Logic)架構建立一個可信任邏輯 (A Logic of Belief)，借其公理系統及推理規則，正確描述通訊主體之間互動行爲的可信度。此公理系統強調的是對通訊行爲可靠性的証明。

對於上述的安全策略，將由一個安全機制利用下列三種技術來實現:

(1) 密碼學(Cryptography): 這是建立安全通道的基礎，利用密碼使無權限者無法得知通信之內容[10]。

(2) 認証(Authentication): 此機制將以認証服務的型式出現。我們建議建立一雛型認証系統，將客戶端的權限分成多個等級。

(3) 存取控制(Access Control): 在此我們將對爲數眾多的組織內部資料屬性之機密性，進行等級劃分，條理出哪些類別之屬性具有機密性，只能由有權限的用戶存取；哪些資料適合於在網際網路上公開。檔案(甚至於屬性)之機密等級，將形成一個保護域(Protection Domain)，作爲存取控制之基礎[18]。

總之，安全服務是將組織私有網路連上網際網路的最重要課題。目前在實務上的解決方案大抵是提供邊界服務(Border Service) [3]，其內容包括:

- 控制從網際網路外來的、對組織內部資料的存取作業。一方面使得來自網際網路的入侵者無法取得組織內部高敏感度的資料；另一方面，合法的使用者仍對網際網路的公開資源如公共的 Web 站，擁有充分的存取能力。
- 監督、控制從組織內部網路向網際網路的存取作業。我們可以限制使用者只存取他們有權限的網路服務類型。邊界服務軟體，如[網威資訊 1997]，往往利用網路目錄導引服務(Network Directory Service)、線路閘道(Circuit Gateway)及代理伺服器(Proxy Server)等技術，使所有用戶共享一個相同的 IP 位址轉換(Internet Protocol Address Transition)功能， 卻能作資訊封包之過濾及存取權限之認証。

5. 結論

本文爲資訊安全研究建立了一個基礎理論架構。我們引用一種模邏輯，它是建立在知識與信任的單調邏輯上。非單調推理則利用 by_default 算子，它可以讓我們以假設方式補足欠缺的資訊。這種設計的理由與需要是因爲通訊主體難以取得完整的環境資訊，只能樂觀的假設這些資訊的存在。這些假設的資訊可以被後來的客觀事實所駁斥。於是推理的結果也是可以被推翻的。這個邏輯可以讓通訊主體表示其對知識與信任之偏好。

在本文中我們只對基本通訊模型作初步的正規化研究，未來的發展將包括對通訊主體行爲之建模、通訊協定之檢驗、通訊服務之保障、資料完整性之檢查等。這種研究方法將可擴展於整個安全資訊體系之建構，具有實用之價值。

至於理論本身的後續發展將是使本邏輯與時序邏輯(Temporal Logic)相結合。在分析或設計系統安全時，我們應能推知哪些知識是永恆的或只是過渡性質的。與時序邏輯的結合將是很有意義的研究。

參考書目

[1] 台灣網威公司: Internet/Intranet 安全邊界服務, *資訊與電腦*， July, 1997, pp.113-115 。

[2] 張真誠: *電腦密碼學與資訊安全*，松崗電腦圖書， 1994.

[3] 樊國楨: 網際網路與資訊安全，*電腦與通訊*，Dec., 1995.

[4] 楊　千、徐培蓮、彭秋霞： EDI 安全管理策略，*第八屆國際資訊管理學術研討會論文集*， 政治大學， 1997, pp.95-101.

[5] 賴溪松、韓亮、張真誠:*近代密碼學及其應用*，松崗電腦圖書， 1995.

[6] D. E. Bell & L. J. LaPadula: *Secure Computer Systems: Mathematical Foundation and Model*, Technical Report M74-244, The MITRE Corporation, Bedford, MA, March 1976.

[7] B. F. Chellas: *Modal Logic: An Introduction*, Cambridge University Press, 1980.

[8] P. S. Chen: *Reasoning by Default — A Nonmonotonic Logic*, Lecture Note, Central Police University, 1997.

[9] G. Coulouris, J. Dollimore & T. Kindberg: *Distributed Systems*, 1994, Chap.6.3, 7.2, 16.1-16.7.

[10] D. E. Denning, *Cryptography and Data Security*, Addison-Wesley, Reading, Mass., 1983.

[11] J. A. Goguen & J. Meseguer: "Security Policy and Security Models", *Proc. Of the 1982 IEEE Computer Society Symposium on Security and Privacy*, April 1982, pp.11-20.

[12] J. Y. Halpern & Y. Moses: "A Guide to the Modal Logics of Knowledge and Belief: Preliminary Draft", Proc. of the 9th Intl. Joint Conf. On Artificial Intelligence, 1985, pp.480-490.

[13] S. A. Kripke: Semantic Considerations on Modal Logics", *Acta Philosophica Fennica*, 1963, pp.83-94.

[14] D. McDermott & J. Doyle: "Nonmonotonic Logic II: Nonmonotonic Modal Theories", *Journal of the ACM*, Vol.29(1), Jan. 1982, pp.33-57.

[15] R. C. Moore: "Semantic Considerations on Nonmonotonic Logic", *Artificial Intelligence* 25, 1985, pp.75-94.

[16] L. E. Moser: "A Logic of Knowledge and Belief for Reasoning about Computer Security", *Proc. of the Computer Security Foundations Workshop II*, June 11-14, 1989, pp.57-63.

[17] P. V. Rangan: An Axiomatic Basis of Trust in Distributed Systems, *1988 IEEE Symposium on Security and Privacy*, Oakland, California, 1988, pp.204-211.

[18] S. T. Vinter: Extended Discretionary Access Control, *1988 IEEE Symposium on Security and Privacy*, Oakland, California, 1988, pp.39-49.