# การสร้างระบบรักษาความปลอดภัยสำหรับผู้ใช้

การสร้างระบบรักษาความปลอดภัยของระบบฐานข้อมูลเริ่มตั้งแต่การควบคุมความปลอดภัยที่กล่าวไว้แล้วในเรื่องที่2.2 แต่สิ่งสำคัญในการสร้างระบบรักษาความปลอดภัยในระบบฐานข้อมูลก็คือการกำหนดผู้ใช้งานในระบบฐานข้อมูล นั่นคือ การที่ผู้ใดจะเข้ามาใช้ระบบฐานข้อมูลได้จะต้องได้รับการอนุญาตก่อน นอกจากนี้เมื่อเข้าระบบได้แล้ว ผู้ใช้งานนั้นสามารถทำอะไรได้บ้างต้องขึ้นอยู่กับการให้สิทธิของผู้บริหารฐานข้อมูล

## 1. การสร้างสิทธิผู้ใช้ในการเข้าถึงข้อมูล

การสร้างสิทธิผู้ใช้ในระบบฐานข้อมูลประกอบด้วย 2 ส่วน คือ การยืนยันตัวบุคคล และการให้สิทธิ ดังนี้

1.1 การยืนยันตัวบุคคล (Authentication) เพื่อให้มั่นใจได้ว่าผู้ที่จะเข้าระบบเป็นผู้ที่มีสิทธิจริง ในปัจจุบันนี้มีการใช้เทคนิคมากมายในการยืนยันตัวบุคคล แต่ที่เป็นที่นิยมได้แก่

- การใช้รหัสผ่าน(password)ในการเข้าสู่ระบบคอมพิวเตอร์ ผู้ใช้งานแต่ละคนจะต้องป้อนรหัสผ่านจึงจะมีสิทธิเข้าถึงข้อมูลได้ ซึ่งเป็นระบบการรักษาความปลอดภัยในระดับพื้นฐานอย่างหนึ่ง การตั้งรหัสผ่านควรจะมีกฎเกณฑ์ เพื่อให้เดาได้ยาก เช่นควรจะมีความยาวไม่น้อยกว่า 6 ตัวอักษร และควรจะมีทั้งตัวเลข ตัวอักษร และสัญลักษณ์พิเศษรวมกัน ไม่ควรเป็นคำที่มีความหมาย หรือเป็นชื่อ เช่น ชื่อคน ชื่อจังหวัด เวลาป้อนรหัสผ่านจะต้องไม่แสดงบนจอ โดยทั่วไปจะแสดงเป็นค่าดาว * แทน และที่สำคัญที่สุดจะต้องมีการบังคับให้มีการเปลี่ยนรหัสเป็นระยะด้วย

- การใช้บัตรสมาร์ดคาร์ด (smartcard) ผู้ใช้จะมีบัตรสำหรับเข้าระบบคอมพิวเตอร์ บัตรสมาร์คคาร์ดคล้ายกับบัตรเอทีเอ็ม และต้องป้อนรหัสส่วนตัว (Personnel Identification Number) หรือพิน (PIN)

- การใช้การตรวจสอบจากร่างกายมนุษย์ (biometric) เช่น ม่านตา เสียง ลายนิ้วมือ การตรวจสอบในลักษณะนี้จะต้องนำลักษณะของผู้ที่ต้องการเข้าไปใช้ฐานข้อมูลไปเปรียบเทียบกับลักษณะข้อมูลของผู้ใช้ที่มีอยู่ในเครื่องคอมพิวเตอร์ ถ้าตรงกันจึงจะมีสิทธิเข้าใช้ข้อมูล

1.2) การให้สิทธิ (Authorization) ผู้ใช้งานระบบฐานข้อมูลมีสิทธิในการใช้ข้อมูลแตกต่างกันมากมาย เช่น

- สิทธิในการอ่านข้อมูลหรือเรียกดูข้อมูล (read)

- สิทธิในการเพิ่มข้อมูล (insert)

- สิทธิในการเปลี่ยนแปลงข้อมูล (update)

- สิทธิในการลบข้อมูล (delete)

- สิทธิในการสร้างดัชนี (index)

- สิทธิในการสร้างตารางหรือวิว (resource)

- สิทธิในการเปลี่ยนแปลงโครงสร้างข้อมูล (alteration)

- สิทธิในการลบตารางหรือวิว (drop)

การอนุญาตให้เข้าระบบ นอกจากจะควบคุมเรื่องตัวบุคคล แล้วยังอาจมีความจำเป็นในการควบคุม เครื่องคอมพิวเตอร์หรือหมายเลขโทรศัพท์ที่จะต่อเข้าระบบด้วย และควรจะมีการตัดการติดต่อจากระบบโดยอัตโนมัติถ้าไม่มีการใช้งานเป็นเวลานาน เพื่อป้องกันผู้อื่นแอบใช้

**2.การสร้างข้อมูลให้เป็นความลับ**

นอกจากการใช้การกำหนดสิทธิเพื่อรักษาความปลอดภัยของระบบแล้ว ยังมีการนำเทคนิคทางด้านการเข้ารหัสข้อมูล โดยอาศัยขบวนการทางคณิตศาสตร์ ทั้งในฐานข้อมูล และระหว่างการส่งผ่านสายสื่อสาร เพื่อเพิ่มความมั่นใจในความถูกต้องของข้อมูล เทคนิคเหล่านี้มีหลายวิธีด้วยกัน เช่น

2.1 การเข้ารหัส (coding)เป็นกระบวนการแปลงรูปแบบของข้อมูลให้อยู่ในรูปที่บุคคลอื่นๆไม่สามารถรู้เนื้อหาของข้อมูล ยกเว้นบุคคลที่เป็นผู้รับ ซึ่งจะต้องมีตัวถอดรหัสทำการแปลงข้อมูลนั้นกลับมาเป็นข้อมูลต้นฉบับ การเข้ารหัสจะใช้วิธีแทนค่าแต่ละค่าด้วยค่าอื่น ซึ่งเป็นการป้องกันข้อมูลในระดับหนึ่ง สามารถป้องกันผู้ที่ไม่ทราบวิธีการเข้ารหัสใช้ข้อมูลได้อย่างง่ายๆ

2.2 กรยุบตัวซ้ำ (compression) มักจะใช้กับข้อมูลประเภทตัวเลข หรือข้อมูลที่แปลงเป็นเลขฐานสองแล้ว เช่นการแปลงข้อมูล 01111100011 เป็น 1532 ประโยชน์ที่จะได้รับนอกจากเพิ่มความปลอดภัยแล้ว เทคนิคนี้มักจะนำไปประยุกต์ใช้กับการบีบอัดข้อมูลเพื่อประหยัดที่ในการเก็บข้อมูล และเวลาในการส่งข้อมูลด้วย

2.3 การแทนค่า (substitution) มีหลักการทำงานคล้ายกับการเข้ารหัสโดยมีการกำหนดค่าที่จะแทนไว้ล่วงหน้า ส่วนการเข้ารหัสจะเป็นการกำหนดหลักการเข้ารหัสไว้

2.4 การสลับตำแหน่งข้อมูล (transposition) ทำโดยไม่ได้เปลี่ยนข้อมูล แต่ใช้วิธีการสลับตำแหน่งของข้อมูลแทน

ในการใช้งานจริงในการรักษาความปลอดภัยของฐานข้อมูลมักจะเป็นการนำเทคนิคต่างๆ หลายเทคนิคมาประยุกต์ใช้งานร่วมกัน เพื่อให้ระบบความปลอดภัยนั้นมั่นคงและเชื่อถือได้

เนื่องจากในปัจจุบันมีการติดต่อสื่อสารมากขึ้น จึงมีความจำเป็นเกี่ยวกับเรื่องความปลอดภัยเพิ่มขึ้นอีกกรณีหนึ่งคือ เราจะมั่นใจได้อย่างไรว่าผู้นั้นเป็นผู้ทำรายการนั้นๆ จริง จึงมีการใช้เทคนิคเพื่อเพิ่มความปลอดภัยไม่ให้สามารถโต้แย้งได้ (non-repudiation) ในทำนองคล้ายกับการลงนามรับรองในเอกสาร ในทางคอมพิวเตอร์เราใช้เทคนิครหัสลับคู่ และลายเซ็นต์ดิจิตัล (digital signature)