แผนการสอนประจำบทเรียน

รายชื่ออาจารย์ผู้จัดทำ ผู้ช่วยศาสตราจารย์ ณัฏฐพร พิมพายน

รายละเอียดของเนื้อหา

ตอนที่ 12.1**แนวคิดเกี่ยวกับความปลอดภัยของฐานข้อมูล**

เรื่องที่ 12.1.1 วัตถุประสงค์ในการรักษาความปลอดภัย

เรื่องที่ 12.1.2 การติดตามและควบคุมการใช้งานฐานข้อมูล

ตอนที่ 12.2 **การสร้างระบบรักษาความปลอดภัยของฐานข้อมูล**

เรื่องที่ 12.2.1 การสร้างระบบรักษาความปลอดภัยสำหรับผู้ใช้

เรื่องที่ 12.2.2 สิทธิในการเข้าถึงข้อมูล

ตอนที่ 12.3 **การควบคุมความปลอดภัยด้วยวิว**(View)

เรื่องที่ 12.3.1 วิว(View)

เรื่องที่ 12.3.2 ลักษณะส่วนรวมของวิว(View)

เรื่องที่ 12.3.3 การปรับปรุงวิว(View)

แนวคิด

1. ความปลอดภัยของฐานข้อมูลเป็นสิ่งที่สำคัญที่สุดสิ่งหนึ่งทำให้ผู้ใช้สมารถใช้ข้อมูลด้วยความมั่นใจ การควบคุมความปลอดภัยของฐานข้อมูลให้มีความถูกต้องและปลอดภัยและพร้อมที่จะใช้งานจึงเป็นสิ่งจำเป็นสำหรับผู้ใช้งานฐานข้อมูล
2. ความปลอดภัยของข้อมูล (security) เป็นเรื่องที่เกี่ยวข้องกับการป้องกันผู้ใช้ที่ไม่มีอำนาจในการเรียกใช้ข้อมูลนำข้อมูลจากฐานข้อมูลมาใช้ อันจะเกิดผลเสียกับระบบฐานข้อมูลได้ ในระบบที่มีผู้ใช้เป็นจำนวนมากจำเป็นต้องมีการควบคุมการเรียกใช้ข้อมูล การควบคุมระบบรักษาความปลอดภัยของฐานข้อมูล โดยมี DBA เป็นผู้ควบคุมและมีการกำหนดสิทธิในการเข้าถึงข้อมูล DBA จะใช้ภาษามาตราฐาน SQL ในการควบคุมการเข้าถึงข้อมูล และมอบอำนาจการเข้าถึงข้อมูลตลอดจนเรียกคืนอำนาจได้ DBA จะระบุสิทธิ์ผู้ใช้ในระบบ
3. วิว(VIEW)หรือตารางเสมือนเป็นตารางข้อมูลที่มีรายละเอียดหรือได้รายละเอียดมาจากตารางอื่น วิวใช้เป็นเครื่องมือในการควบคุมไม่ให้ผู้ใช้เข้าไปดูข้อมูลทั้งหมดของตารางได้ วิวเป็นกลไกรักษาความปลอดภัยในการปกปิดส่วนต่าง ๆ ของตารางที่เป็นความลับหรือเกินความจำเป็นสำหรับผู้ใช้

วัตถุประสงค์

หลังจากศึกษาบทเรียนที่ 12 แล้ว นักศึกษาสามารถ

1. บอกแนวคิดเกี่ยวกับความปลอดภัยของฐานข้อมูลได้
2. ระบุการสร้างระบบรักษาความปลอดภัยของฐานข้อมูลได้
3. ระบุการควบคุมความปลอดภัยด้วยวิว(View)ได้

กิจกรรมการเรียนการสอน

กิจกรรมที่นักศึกษาต้องทำสำหรับการเรียนการสอน ได้แก่

1. ศึกษาเอกสารการสอน
2. ปฏิบัติกิจกรรมตามที่ได้รับมอบหมายในเอกสารการสอนแต่ละตอน

สื่อการสอน

1. เอกสารการสอนของชุดวิชา
2. แบบฝึกปฏิบัติ
3. บทความ/ข้อมูลทางคอมพิวเตอร์
4. การให้คำปรึกษาทางโทรศัพท์
5. CD-ROM
6. Homepage ของชุดวิชาผ่านทางอินเตอร์เน็ต

เอกสารประกอบการสอน

1. Fundamentals of Database Systems, by Ramez Elmasri, Shamkant B. Navathe, The Second Edition, 1994
2. Database System Concepts, by Abraham Siberschaty, Henry F.Korth, S.Sudarshan, The Third Edition, 1991

ประเมินผล

1. ประเมินผลจากแบบฝึกหัด/ทดสอบ ในแต่ละบท
2. ประเมินผลจากการสอนประจำภาคการศึกษา

ตอนที่ 12.1 แนวคิดเกี่ยวกับความปลอดภัยของฐานข้อมูล

หัวเรื่อง

เรื่องที่ 12.1.1 วัตถุประสงค์ในการรักษาความปลอดภัย

เรื่องที่ 12.1.2 การติดตามและควบคุมการใช้งานฐานข้อมูล

แนวคิด

1. การรักษาความปลอดภัยของฐานข้อมูล เป็นการป้องกันความไม่ถูกต้องในการเปลี่ยนแปลงข้อมูล และปกป้องฐานข้อมูลไม่ให้ถูกเปิดเผยต่อบุคคลที่ไม่ได้รับอนุญาตอย่างถูกต้อง เพื่อป้องกันการปลอมแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต การรักษาความปลอดภัยจะต้องมีระบบการคุ้มครองว่าผู้ใดจะสามารถเข้าถึงข้อมูลได้ และหากเข้าถึงข้อมูลภายในระบบแล้วจะสามารถทำอะไรได้บ้างกับข้อมูลนั้นๆ เช่น การอ่านหรือเขียนข้อมูลได้อย่างเดียว หรือทั้งอ่านและเขียนข้อมูล
2. ในการใช้ข้อมูลร่วมกันหลายคน การติดตามและการควบคุมความปลอดภัยในการเข้าถึงฐานข้อมูลถือว่าเป็นสิ่งที่สำคัญ การควบคุมความปลอดภัยในการเข้าถึงฐานข้อมูลเป็นการมอบสิทธิ์ที่ควรจะใช้ข้อมูลให้กับผู้ใช้ต่างๆ ว่ามีสิทธิ์ในการเรียกใช้ข้อมูลจากระบบได้มากน้อยต่างกันอย่างไรบ้าง

วัตถุประสงค์

หลังจากที่ศึกษาตอนที่ 12.1 แล้ว นักศึกษาสามารถ

1. บอกวัตถุประสงค์ในการรักษาความปลอดภัยได้
2. ระบุการติดตามและควบคุมการใช้งานฐานข้อมูลได้

เรื่องที่ 12.1.1 วัตถุประสงค์ในการรักษาความปลอดภัย

ความปลอดภัยของระบบฐานข้อมูล (database security) เป็นการป้องกันผู้ไม่มีสิทธิเข้ามาใช้ หรือแก้ไขข้อมูล และความสามารถในการป้องกันข้อมูลให้ถูกต้องครบถ้วนสมบูรณ์ เช่น ข้อมูลที่ถูกเปลี่ยนแปลงให้ผิดพลาดได้โดยง่าย แสดงว่าข้อมูลมีความปลอดภัยต่ำ เป็นต้น ทั้งนี้ความปลอดภัยของระบบฐานข้อมูลมีความสำคัญต่อความสำเร็จขององค์กรเป็นอย่างมาก ผู้บริหารฐานข้อมูลจึงจำเป็นที่จะต้องรักษาฐานข้อมูลให้ปลอดภัย

1. ความหมายของการรักษาความปลอดภัย

การรักษาความปลอดภัยของฐานข้อมูลหมายถึงการดูแลจัดการและรักษาข้อมูลให้ถูกต้องครบถ้วนสมบูรณ์พร้อมสำหรับผู้ที่มีสิทธิในการใช้ข้อมูลสามารถใช้งานได้อยู่เสมอ การเสียหายของระบบฐานข้อมูลซึ่งเกิดจากข้อบกพร่องของความปลอดภัย เช่น

- เครื่องเสียในระหว่างทำงาน ถ้าไม่มีการจัดการที่ดีอาจทำให้ข้อมูลผิดพลาดได้ เช่นการโอนเงินจากบัญชี ก ไปบัญชี ข เราสามารถทำได้ 2 แบบ คือ ถอนเงินบัญชี ก ก่อนแล้วฝากเงินเข้าบัญชี ข หรือฝากเงินเข้าบัญชี ข ก่อนถอนเงินจากบัญชี ก ในแบบแรกถ้าเครื่องเกิดมีปัญหาหลังจากถอนเงินเรียบร้อยแล้ว แต่ยังไม่ได้ฝากเงิน ก็จะทำให้ผลรวมของยอดเงินหายไป ส่วนแบบหลังยอดเงินก็จะมากเกินไป ทั้งสองแบบนี้ไม่เป็นที่ต้องการ ระบบรักษาความปลอดภัยของฐานข้อมูลจึงจำเป็นต้องมีขบวนการควบคุมการทำงานในลักษณะรายการ (transaction) คือการที่ถ้าทำรายการใดไม่สำเร็จทุกขั้นตอนจะต้องเสมือนยังไม่ได้ทำขั้นตอนใดเลย

- การใช้งานพร้อมกัน อาจทำให้เกิดปัญหา ดังตัวอย่าง ถ้านาย ก ทำการถอนเงินด้วยสมุดเงินฝากในเวลาเดียวกับที่นาย ข ทำการถอนเงินด้วยบัตรเอทีเอ็ม จากบัญชีเดียวกัน ถ้าการทำงาน 2 รายการนี้ ไม่เป็นอิสระจากกัน คือต่างอ่านได้ยอดเงินคงเหลือก่อนถอนเท่ากัน แล้วทำการถอนเงิน จะทำให้ได้ยอดคงเหลือของบัญชีผิดพลาดได้

โดยทั่วไปการป้องกันความผิดพลาดสามรถทำได้โดยง่าย เนื่องจากระบบ DBMS ส่วนใหญ่จะมีองค์ประกอบที่ช่วยป้องกันความผิดพลาดดังตัวอย่างข้างต้นได้อยู่แล้ว จึงไม่เป็นภาระของผู้ใช้งาน

2.วัตถุประสงค์ของการรักษาความปลอดภัย

วัตถุประสงค์ของการรักษาความปลอดภัยของระบบฐานข้อมูล ก็เพื่อลดปัจจัยเสี่ยงที่เกี่ยวกับ ความเสียหายกับฐานข้อมูล เนื่องจากความผิดพลาดในการทำงานของผู้ใช้ระบบฐานข้อมูล แฟ้มข้อมูลเสียหาย ความผิดพลาดในการทำงานของเครื่องหรือเครื่องคอมพิวเตอร์ไม่สามารถทำงานได้ การปฏิบัติงานที่ไม่เหมาะสมหรือผิดปกติ เนื่องจากการใช้คำสั่งในระบบโดยไม่ได้รับอนุญาติ การทุจริต และการเปิดเผยข้อมูลที่เป็นความลับ โดยสามารถแยกวัตถุประสงค์โดยรวมของการรักษาความปลอดภัยในระบบฐานข้อมูลได้ 4 ประการ คือ

2.1 เพื่อให้สามารถรักษาข้อมูลเป็นความลับได้ (secrecy) ระบบจะต้องปกป้องข้อมูลไม่ให้ผู้ไม่มีสิทธิในการใช้ข้อมูลเข้าใช้ข้อมูลได้ และจะต้องสามารถกำหนดให้ผู้ใช้งานแต่ละคนสามารถใช้งานได้ตามสิทธิที่กำหนดเท่านั้นด้วย ควรมีการกำหนดสิทธิไว้ชัดเจน อยู่ในห้องเครื่อง มีการรักษาความปลอดภัยโดยใช้บัตรผ่าน มีการควบคุมสิทธิผู้ใช้งานอย่างรอบคอบ มีความปลอดภัยในการใช้งานในระบบเครือข่าย และมีระบบสำรองกู้คืนข้อมูลที่ดี สามารถใช้งานได้สะดวก

2.2 เพื่อให้ข้อมูลในฐานข้อมูลมีความถูกต้องครบถ้วนสมบูรณ์ (integrity) นั่นคือจะต้องสามารถรักษาข้อมูลให้มีความถูกต้องตามกฎเกณฑ์หรือเงื่อนไขที่ได้กำหนดไว้ตอนสร้างฐานข้อมูล ข้อมูลต้องไม่ผิดเพี้ยน รวมทั้งความถูกต้องของข้อมูลในการประมวลผลข้อมูลพร้อมกันด้วย

2.3 เพื่อให้มีฐานข้อมูลพร้อมใช้งานอยู่เสมอ (availability) สามารถทำงานได้ตามปกติและเต็มประสิทธิภาพตามจุดมุ่งหมายในการใช้ และมีขีดความสามารถปฏิบัติงานได้ตามที่ต้องการเนื่องถ้าการใช้งานระบบฐานข้อมูลมักจะมีข้อขัดข้องอยู่เสมอ เช่นเครื่องเสีย หรือไฟดับ หรือข้อมูลสูญหาย ถ้ามีการรักษาความปลอดภัยที่ดีจะทำให้ผู้ใช้งานมีความเชื่อถือในระบบฐานข้อมูลนั้น

2.4 เพื่อลดความเสี่ยง (Risk Assessment) การรักษาความปลอดภัยที่ดีจะช่วยลดความเสี่ยงในค่าใช้จ่ายที่จะเกิดขึ้นจากการเสียหายของข้อมูล การวางแผนด้านการรักษาความปลอดภัยได้อย่างเหมาะสมจะ

ช่วยลดความเสี่ยงในการเกิดความเสียหายของข้อมูลค่าใช้จ่าย มีการประเมินความสมดุลระหว่างค่าใช้จ่ายหรือต้นทุนคุ้มค่ากับประโยชน์ที่จะได้รับจากการรักษาความปลอดภัย

3.ข้อคำนึงในการรักษาความปลอดภัยระบบฐานข้อมูล

ในการรักษาความปลอดภัยของระบบฐานข้อมูลนั้น จะต้องคำนึงถึงนโยบาย(policy)ขององค์การและสถานภาพของระบบการรักษาความปลอดภัยในปัจจุบัน(current state)

3.1.นโยบายขององค์การ นโยบายขององค์การมีผลสำคัญอย่างยิ่งต่อการรักษาความปลอดภัยของข้อมูล นโยบายขององค์การจะต้องมุ่งเน้นที่จุดมุ่งหมายและการทำงานที่ดี การกำหนดนโยบายด้านการรักษาความปลอดภัยก็เพื่อให้องค์กรสามารถดูแลรักษาระบบความปลอดภัย องค์กรจำเป็นต้องมีการกำหนดนโยบายด้านความปลอดภัยให้ชัดเจน โดยประกอบด้วยกฎ ข้อบังคับ และหน้าที่ความรับผิดชอบของพนักงาน พร้อมทั้งระเบียบวิธีปฏิบัติให้พนักงานใช้เป็นหลักในการทำงาน รวมทั้งการติดตามตรวจสอบให้ทุกคนให้ปฏิบัติตามกฎ ระเบียบ มาตรฐานที่วางไว้อย่างเคร่งครัด และสม่ำเสมอ

การกำหนดนโยบายด้านการรักษาความปลอดภัย เพื่อให้องค์กรสามารถดูแลรักษาระบบความปลอดภัย องค์กรจำเป็นต้องมีการกำหนดนโยบายด้านความปลอดภัยให้ชัดเจน โดยประกอบด้วยกฎ ข้อบังคับ และหน้าที่ความรับผิดชอบของพนักงาน พร้อมทั้งระเบียบวิธีปฏิบัติให้พนักงานใช้เป็นหลักในการทำงาน รวมทั้งการติดตามตรวจสอบให้ทุกคนปฏิบัติตามกฎ ระเบียบ มาตรฐานที่วางไว้อย่างเคร่งครัด และสม่ำเสมอ โดยต้องกำหนดให้แน่นอนว่าระบบรักษาความปลอดภัยนี้ใครเป็นผู้ปฏิบัติ (who) ใช้กับส่วนใดบ้างในระบบ(to what resources) มีวิธีการปฏิบัติอย่างไร(how) ผู้ใช้ผู้ใดสามารถเข้าถึงข้อมูลส่วนใดได้บ้าง รวมทั้งต้องกำหนดสิทธิว่าใครมีสิทธิกำหนดที่จะเปลี่ยนแปลงแก้ไขข้อมูลนั้นๆ

3.2.สถานภาพของระบบการรักษาความปลอดภัย โดยมีการตรวจสอบว่าในปัจจุบันสถานภาพของระบบการรักษาความปลอดภัยอยู่ในระดับใดและต้องการปรับปรุงหรือเปลี่ยนแปลงอันใดบ้าง ความต้องการในการใช้ข้อมูลที่ปลอดภัยและคำแนะนำจากส่วนต่างๆที่ใช้งานภายในระบบ การแจกงานไปสู่ผู้ที่รับผิดชอบ มีตารางเวลาที่กำหนดว่าส่วนใดของระบบจะต้องปรับปรุงอะไรบ้าง ณ เวลาใด มีการจัดทำแผนฉุกเฉิน เพื่อให้องค์กรสามารถดำเนินการต่อไปได้เมื่อมีวิกฤตการณ์เกิดขึ้น แผนฉุกเฉินนี้อาจทำรวมเป็นแผนเดียวทั้งองค์กรหรือแยกตามงานก็ได้ แผนนี้ควรจะระบุ ชื่อคนที่จะต้องติดต่อเมื่อเกิดเหตุ อุปกรณ์หรือเครื่องมือสำรองตลอดจนขบวนการทำงานอย่างละเอียด บุคลากรที่เกี่ยวข้องควรจะคุ้นเคยกับแผนเหล่านี้และมีการทดสอบให้มั่นใจว่าสามารถใช้งานได้- การจัดทำแผนฉุกเฉิน เพื่อให้องค์กรสามารถดำเนินการต่อไปได้เมื่อมีวิกฤตการณ์เกิดขึ้น แผนฉุกเฉินนี้อาจทำรวมเป็นแผนเดียวทั้งองค์กร หรือแยกตามงานก็ได้ แผนนี้ควรจะระบุ ชื่อคนที่จะต้องติดต่อเมื่อเกิดเหตุ อุปกรณ์หรือเครื่องมือสำรอง ตลอดจนขบวนการทำงานอย่างละเอียด บุคลากรที่เกี่ยวข้องควรจะคุ้นเคยกับแผนเหล่านี้และมีการทดสอบให้มั่นใจว่าสามารถใช้งานได้

เรื่องที่ 12.1.2 การติดตามและควบคุมการใช้งานฐานข้อมูล

การติดตามตรวจสอบและควบคุมการใช้งานฐานข้อมูลเป็นขบวนการรักษาความปลอดภัยที่ดีอย่างหนึ่ง การตรวจสอบข้อมูลอย่างสม่ำเสมอเพื่อให้มั่นใจว่ากฎ ระเบียบ มาตรฐานที่ได้กำหนดไว้ได้มีการใช้งานจริง องค์กรส่วนใหญ่จะมีกลุ่มคนที่ทำหน้าที่ตรวจสอบแยกจากกลุ่มผู้ใช้และพัฒนาระบบ การตรวจสอบนี้มักจะทำทุกส่วนที่เกี่ยวข้องตั้งแต่ระบบคอมพิวเตอร์ รวมถึงคู่มือการใช้งานและคู่มือระบบด้วย

1.วัตถุประสงค์ในการติดตามและควบคุมการใช้งานฐานข้อมูล

วัตถุประสงค์ในการติดตามและควบคุมการใช้งานฐานข้อมูลเพื่อ

1.1 เพื่อให้มั่นใจว่าข้อมูลนำเข้าถูกต้อง ผู้ตรวจสอบจะตรวจสอบว่ามีการตรวจสอบข้อมูลนำเข้าเบื้องต้นครบถ้วนหรือไม่ รวมทั้งมีการป้องกันในระดับระบบจัดการฐานข้อมูลและโปรแกรมดีเพียงพอหรือไม่

1.2 เพื่อให้มั่นใจว่ากระบวนการทำงานถูกต้อง การตรวจสอบจะรวมถึงพิธีปฏิบัติ และรายละเอียดในการทำงานของระบบงานทุกขั้นตอน

1.3เพื่อป้องกันการเปลี่ยนแปลงแก้ไขโปรแกรมโดยไม่มีสิทธิ เมื่อระบบใช้งานจริงแล้ว ผู้ตรวจสอบจะทำการควบคุมไม่ให้มีการแก้ไขโปรแกรมเพื่อความปลอดภัยของระบบ

1.4 ตรวจสอบการใช้งานและสิทธิการใช้งานของผู้ใช้งาน เพื่อให้มั่นใจว่าไม่มีผู้ใช้งานที่ไม่มีสิทธิอยู่ในระบบ และสิทธิต่างๆได้ถูกกำหนดไว้ถูกต้องเพื่อให้มั่นใจว่าคู่มือต่างๆ ได้รับการปรับปรุงให้ทันสมัยอยู่เสมอ

2.การติดตามและตรวจสอบการใช้งานข้อมูล

การตรวจสอบทุกด้านข้างต้นจะต้องทำอย่างมีประสิทธิภาพ โดยผู้ตรวจสอบอาจสุ่มตรวจเป็นระยะไม่มีการแจ้งล่วงหน้า หรืออาจจะกำหนดการตรวจเป็นตารางแน่นอนและต้องทำอย่างสม่ำเสมอ ทั้งนี้การตรวจเกี่ยวกับระบบฐานข้อมูลจำเป็นต้องติดต่อประสานงานกับผู้บริหารฐานข้อมูลอย่างใกล้ชิด ส่วนมากจะเริ่มตั้งแต่การร่วมออกแบบระบบฐานข้อมูลด้วย

ผู้บริหารฐานข้อมูลมีหน้าที่ในการที่จะต้องเก็บบันทึกการใช้งานต่างๆ ตามที่ผู้ตรวจสอบต้องการ ทั้งนี้ขึ้นอยู่กับความเหมาะสมว่าจะใช้บันทึกการปฏิบัติงานที่มักจะมีมาพร้อมกับระบบจัดการฐานข้อมูล หรือจะพัฒนาขึ้นเองเป็นส่วนหนึ่งในการพัฒนาระบบงาน

3. การควบคุมการใช้งานฐานข้อมูล

การควบคุมการใช้งานฐานข้อมูลเป็นส่วนหนึ่งในการรักษาความปลอดภัย การควบคุมการใช้งานฐานข้อมูลอาจแยกออกเป็น 2 ด้าน ได้แก่ การควบคุมทางกายภาพ (physical control) และการควบคุมการเข้าถึงข้อมูล(access control)

3.1.การควบคุมทางกายภาพ เป็นการควบคุมในส่วนภายนอกระบบฐานข้อมูล การควบคุมในส่วนนี้เป็นการควบคุมและป้องกันความเสียหายโดยทั่วไป ได้แก่

-การป้องกันภัยจากน้ำท่วม ไฟไหม้ ภัยจากระบบไฟฟ้าเสียหาย

-การล็อกห้องคอมพิวเตอร์อย่างหนาแน่นเมื่อไม่มีการใช้งานแล้ว การใช้ยามเฝ้า

-เก็บข้อมูลที่ทำการสำรองไว้ในสถานที่ต่างหาก เช่น ในบริเวณที่ห่างไกลจากระบบคอมพิวเตอร์ที่มีอยู่ เพื่อเป็นการป้องกันภัยที่อาจเกิดขึ้นและอาจทำลายระบบไปพร้อมกับระบบสำรองข้อมูล เช่นการเกิด ไฟไหม้หรือน้ำท่วม เป็นต้น

-การวางแผนล่วงหน้าในกรณีฉุกเฉิน(contingency plan)โดยการใช้ระบบสำรองข้อมูล(back up disk) สำหรับการทำข้อมูลสำรองอย่างสม่ำเสมอเพื่อใช้ในกรณีที่ระบบเกิดความเสียหายไม่สามารถเรียกคืนได้ ตรวจสอบกระบวนการทำสำรองข้อมูลอย่างสม่ำเสมอ เพื่อดูว่ากระบวนการนั้นได้ทำการสำรองข้อมูลไว้อย่าถูกต้องและครบถ้วน

-ต้องทำลายข้อมูลหรือลบข้อมูลที่ไม่ใช้แล้วอย่างปลอดภัย และไร่ร่องรอย ซึ่งอาจทำได้ โดยการลบหลายๆครั้งหรือใช้เทคนิคอย่างอื่นเข้าช่วย มิใช่เพียงแต่งเขียนข้อมูลใหม่ทับซ้ำลงไปเท่านั้น เนื่องจากว่าการกระทำเช่นนี้ไม่สามารถทำลายข้อมูลเก่าให้หมดไปได้อย่างไร่ร่องรอย เพราะอาจมีการใช้เทคนิคชนิดพิเศษต่างๆมาทำการอ่านข้อมูลเก่าที่ถูกทับไว้ได้

-สื่อที่ใช้ในการบันทึกข้อมูลเมื่อต้องการจะทิ้งหรือไม่ต้องการแล้วต้องทำลายให้ดี เพื่อป้องกันการแอบนำสื่อเหล่านั้นกลับมาอ่านข้อมูลที่หลงเหลืออยู่ได้

-มีโปรแกรมที่สามารถเก็บสำรองข้อมูลไว้ได้โดยอัตโนมัติและสม่ำเสมอ โดยไม่ต้องใช้ผู้ดูแลระบบมาทำการเก็บสำรองข้อมูลด้วยตนเองเพราะเกิดความไม่สม่ำเสมอ โดยไม่ต้องใช้ผู้ดูแลระบบมาทำการเก็บสำรองข้อมูลด้วยตนเองเพราะอาจเกิดความไม่สม่ำเสมอและข้อผิดพลาดได้

3.2.การควบคุมการเข้าถึงระบบ ควรมีการควบคุมความปลอดภัยในการเข้าถึงระบบซอฟต์แวร์และฮาร์ดแวร์ของระบบฐานข้อมูล และส่วนอื่นๆ ที่เกี่ยวข้องกับการทำงาน โดยมีการควบคุมดังนี้

-ควบคุมความปลอดภัยโดยระบบปฏิบัติการ(operating system controls)หรือระบบจัดการฐานข้อมูล ควรมีการควบคุมสิทธิการเข้าถึงและการใช้ข้อมูลในส่วนต่างๆภายในระบบคอมพิวเตอร์ของผู้ใช้ การมีระบบบันทึกเหตุการณ์ต่างๆในระบบ(security log)ไว้โดยอัตโนมัติเพื่อใช้เป็นหลักฐานการตรวจสอบ(audit trail)

-ควบคุมความปลอดภัยในการเข้าถึงระบบฮาร์ดแวร์อาจควบคุมโดย เทคโนโลยีทางฮาร์ดแวร์ได้มีการออกแบบสถาปัตยกรรมขั้นพื้นฐานในการรักษาความปลอดภัยที่สามารถควบคุมการเข้าถึงระบบได้อย่างดี เช่น การใช้สมาร์ดการ์ดในการควบคุมการใช้ การใช้วงจรเฉพาะกิจเชื่อมต่อกับหน่วยความจำเพื่อตรวจสอบ ป้องกัน และกำจัดเวลาในการใช้ เป็นต้น

-ผู้ใช้แต่ละคนจะต้องมีชื่อผู้ใช้(user name) และรหัสผ่าน(password) ที่แตกต่างกันออกไปในแต่ละคน

-ระบบการตรวจสอบ จะต้องมีหลักฐานการตรวจสอบ(audit trial) จะต้องบันทึกว่าผู้ใช้เป็นใครทำอะไร จากที่ไหน และทำสำเร็จหรือไม่จะต้องบันทึกการเข้าสู่ระบบของผู้ใช้(events logging)แฟ้มข้อมูลของระบบตรวจสอบจะต้องได้รับการปกป้องและตรวจสอบเสมอ

-ควบคุมการเข้าถึงข้อมูลโดยต้องจำแนกแยกแยะสิทธิในการกระทำต่อส่วนต่างๆของระบบและจำแนกแยกแยะระหว่างผู้ใช้กลุ่มต่างๆ เช่น ผู้ใช้กลุ่มใดมีสิทธิในการใช้ระบบแฟ้มข้อมูล (file system) มีการแบ่งหน่วยความจำ (shared memory)

-มีโปรแกรมที่สามารถเก็บสำรองข้อมูลไว้ได้โดยอัตโนมัติและสม่ำเสมอ โดยไม่ต้องใช้ผู้ดูแลระบบมาทำการเก็บสำรองข้อมูลด้วยตนเองเพราะอาจเกิดความไม่สม่ำเสมอและข้อผิดพลาดได้

-ควบคุมความปลอดภัยในการเข้าถึงระบบเครือข่าย การรักษาความปลอดภัยของข้อมูลในระบบเครือข่ายนั้นจะต้องทำให้ทั่วถึงทั้งระบบ จะทำเฉพาะจุดใดจุดหนึ่งไม่ได้ สิ่งที่ต้องควบคุมก็คือ ความลับของข้อมูลที่ส่งผ่านในระบบเครือข่าย และการตรวจสอบความถูกต้องของผู้ใช้ รวมถึงการตรวจสอบความถูกต้องของระบบคอมพิวเตอร์ที่จะเข้ามาทำการเชื่อมต่อเข้าสู่ระบบเครือข่าย การรักษาความปลอดภัยต้องคำนึงถึง การควบคุมการอนุญาตให้เข้ามาในระบบ(access control) การตรวจสอบความถูกต้องระบบคอมพิวเตอร์ในระบบเครือข่าย(authentication in distribute system) การรักษาความถูกต้องของข้อมูลที่ส่งผ่านระบบเครือข่าย(data integrity) และการใช้ตัวป้องกันการบุกรุกหรือกำแพงไฟ(firewall)ในการรักษาความปลอดภัยของระบบเครือข่าย

-ควบคุมการอนุญาตให้เข้ามาในระบบเครือข่าย เป็นการป้องกันการเข้าระบบโดยผ่านช่องทางหรือพอร์ต(port) ต่าง ๆที่มีอยู่ในระบบ โดยใช้ฮาร์ดแวร์และซอฟต์แวร์และการกำหนดระดับสิทธิในการเข้าถึงข้อมูลที่ต่างกัน เช่น กำหนดสิทธิในการเข้าถึงข้อมูลบางส่วนเท่านั้นสำหรับผู้ที่มีสิทธิหรือสามารถเพียงแค่ในการอ่านข้อมูลเท่านั้น แต่ไม่มีสิทธิในการเปลี่ยนแปลงแก้ไขข้อมูล เป็นต้น

-การตรวจสอบความถูกต้องของระบบคอมพิวเตอร์ในระบบเครือข่าย(authentication in distribute system) เป็นการป้องกันการปลอมแปลงจากระบบคอมพิวเตอร์ที่ไม่ได้รับอนุญาตให้เข้ามาในระบบได้ ต้องมีวิธีในการการตรวจสอบความถูกต้องของระบบที่มาต่อเชื่อม โดยการตรวจสอบรหัสผ่านเพื่อใช้ในการตรวจสอบเซอร์ฟเวอร์(server) จากระบบอื่น ๆที่จะเข้ามาทำการต่อเชื่อมได้

-การรักษาความถูกต้องของข้อมูลที่ส่งผ่านระบบเครือข่าย(data integrity)โดยการนำวิธีการติดต่อสื่อสารที่มีขั้นตอนและรูปแบบที่แน่นอนระหว่างระบบคอมพิวเตอร์ภายในเครือข่าย เช่น การใช้โพรโตคอล (protocol) มาตราฐาน การใช้ลายเซ็นอิเล็กทรอนิกส์(digital signature) การใช้ตัวป้องกันการบุกรุกหรือกำแพงไฟ(firewall)ในการรักษาความปลอดภัยของระบบเครือข่าย โดยใช้กำแพงไฟเป็นเครื่องมือในการตรวจสอบหรือปิดกั้นการเชื่อมต่อของข้อมูลจากระหว่างภายนอกระบบเครือข่ายกับภายในระบบเครือข่าย

ตอนที่ 12.2 การสร้างระบบรักษาความปลอดภัยของฐานข้อมูล

หัวเรื่อง

เรื่องที่ 12.2.1 การสร้างระบบรักษาความปลอดภัยสำหรับผู้ใช้

เรื่องที่ 12.2.2 สิทธิในการเข้าถึงข้อมูล

แนวคิด

1. การสร้างระบบรักษาความปลอดภัยสำหรับผู้ใช้สามารถทำได้หลายระดับ คือการสร้างบัญชีผู้ใช้ การป้องกันด้วยคำสั่ง SQL และการสร้างวิว(View) ให้กับผู้ใช้แต่ละคน ให้สามารถใช้ข้อมูลบางส่วน ตามที่ DBA เป็นผู้กำหนด นอกจากนี้การรักษาความปลอดภัยของข้อมูลยังสามารถทำได้โดยการเข้ารหัสข้อมูล (Encryption)
2. การกำหนดสิทธิการเข้าถึงข้อมูลและการยกเลิกสิทธิในการเข้าถึงข้อมูลเป็นการกำหนดว่าให้ใครสามารถใช้ข้อมูลในตารางใดบ้างและใช้ได้ในระดับใด เช่น ดูได้อย่างเดียวแต่ห้ามปรับปรุงแก้ไข หรือปรับปรุงแก้ไขได้แต่ห้ามลบ การกำหนดสิทธิการเข้าถึงข้อมูลและการยกเลิกสิทธิในการเข้าถึงข้อมูลสามารถทำได้โดยใช้คำสั่ง GRANT และคำสั่ง REVOKE

วัตถุประสงค์

หลังจากศึกษาตอนที่ 1.2 แล้ว นักศึกษาสามารถ

1. บอกการสร้างระบบรักษาความปลอดภัยสำหรับผู้ใช้ได้
2. อธิบายการกำหนดสิทธิในการเข้าถึงข้อมูลได้

เรื่องที่ 12.2.1การสร้างระบบรักษาความปลอดภัยสำหรับผู้ใช้

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 และควรจะมีทั้งตัว

เลข ตัวอักษร และสัญลักษณ์พิเศษรวมกัน ไม่ควรเป็นคำที่มีความหมาย หรือเป็นชื่อ เช่น ชื่อคน ชื่อจังหวัด เวลาป้อนรหัสผ่านจะต้องไม่แสดงบนจอ โดยทั่วไปจะแสดงเป็นค่าดาว * แทน และที่สำคัญที่สุดจะต้องมีการบังคับให้มีการเปลี่ยนรหัสเป็นระยะด้วย

- การใช้บัตรสมาร์ตคาร์ด (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 แล้วยังอาจมีความจำเป็นในการควบคุมเครื่องคอมพิวเตอร์หรือหมายเลขโทรศัพท์ที่จะต่อเข้าระบบด้วย และควรจะมีการตัดการติดต่อจากระบบโดยอัตโนมัติถ้าไม่มีการใช้งานเป็นเวลานาน เพื่อป้องกันผู้อื่นแอบใช้

2.การสร้างข้อมูลให้เป็นความลับ

นอกจากการใช้การกำหนดสิทธิเพื่อรักษาความปลอดภัยของระบบแล้ว ยังมีการนำเทคนิคทางด้านการเข้ารหัสข้อมูล โดยอาศัยขบวนการทางคณิตศาสตร์ ทั้งในฐานข้อมูล และระหว่างการส่งผ่านสายสื่อสารเพื่อเพิ่มความมั่นใจในความถูกต้องของข้อมูล 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)

เรื่องที่ 12.2.2 สิทธิในการเข้าถึงข้อมูล

ความปลอดภัยของข้อมูล (security) เป็นเรื่องที่เกี่ยวข้องกับการป้องกันผู้ใช้ที่ไม่มีอำนาจในการเรียกใช้ข้อมูลนำข้อมูลจากฐานข้อมูลมาใช้ อันอาจจะเกิดผลเสียกับระบบฐานข้อมูลได้ ในระบบที่มีผู้ใช้เป็นจำนวนมากจำเป็นต้องมีการควบคุมการเรียกใช้ข้อมูล การกำหนดสิทธิในการเข้าถึงข้อมูล DBAจะกำหนดการให้สิทธิ (Authorization)แก่ผู้ใช้งานระบบฐานข้อมูลให้มีสิทธิในการใช้ข้อมูลแตกต่างกัน เช่น

- สิทธิในการอ่านข้อมูลหรือเรียกดูข้อมูล (read)
- สิทธิในการเพิ่มข้อมูล (insert)
- สิทธิในการเปลี่ยนแปลงข้อมูล (update)
- สิทธิในการลบข้อมูล (delete)
- สิทธิในการสร้างดัชนี (index)
- สิทธิในการสร้างตารางหรือวิว (resource)
- สิทธิในการเปลี่ยนแปลงโครงสร้างข้อมูล (alteration)
- สิทธิในการลบตารางหรือวิว (drop)

การกำหนดสิทธิในการเข้าถึงข้อมูล และมอบอำนาจการเข้าถึงข้อมูลตลอดจนเรียกคืนอำนาจได้ DBAจะระบุสิทธิผู้ใช้ในระบบด้วยภาษา SQL ได้ดังนี้

1.การให้รหัสแก่ผู้ใช้

เป็นการกำหนดรหัสผ่านให้แก่ผู้ใช้ โดยใช้คำสั่ง CREATE เช่น ถ้าต้องการสร้างสิทธิให้แก่ผู้ใช้ชื่อ Wichaiให้เข้าในระบบฐานข้อมูลได้ในเบื้องต้นที่จะเข้าสู่ฐานข้อมูลได้จะต้องมีการยืนยันตัวบุคคลว่าเป็น

Wichai จริงโดยระบบการจัดการฐานข้อมูลจะต้องทำการตรวจเช็คจารรหัสผ่านที่กำหนดให้กับ Wichai DBA จะสร้างรหัสผ่านให้แก่ Wichai ด้วยภาษา SQL โดยในตัวอย่างนี้ Wichai จะมีรหัสผ่านว่า BENZ2000

CREATE Wichai IDENTIFIED BY BENZ2000

นอกจากการให้รหัสแก่ผู้ใช้ในการใช้ฐานข้อมูลแล้ว ผู้ใช้จะถูกกำหนดโดย DBA ให้สามารถใช้ฐานข้อมูลในส่วนที่เกี่ยวข้องได้เท่านั้น การกำหนดสิทธิแก่ผู้ใช้ให้สามารถใช้ฐานข้มูล โดยกำหนดขอบเขตอำนาจการใช้ข้อมูล เราสามารถกำหนดสิทธิใดสิทธิหนึ่ง หรือบางสิทธิ หรือทุกสิทธิให้กับผู้ใช้งานได้

สิทธิการใช้งานจะมีกี่ชนิดขึ้นอยู่กับเป้าหมายที่ต้องการกำหนดสิทธิ เช่นสิทธิการทำงานกับตารางข้อมูลอาจมีเพียงแค่อ่านและเขียนข้อมูล DBA จะจะทำการกำหนดสิทธิด้วยภาษา SQL คำสั่งที่ใช้ในการกำหนดสิทธิกับผู้ใช้ได้แก่

การกำหนดสิทธิการเข้าถึงข้อมูล ด้วยคำสั่ง GRANT และ การยกเลิกสิทธิการเข้าถึงข้อมูล ด้วยคำสั่ง REVOKE

2. การกำหนดสิทธิการเข้าถึงข้อมูล

ในการกำหนดสิทธิการเข้าถึงข้อมูลผู้ใช้ (USERS) ในระบบการจัดการฐานข้อมูลโดยภาษา SQL จะมีการกำหนดหรืออนุญาติให้มีสิทธิเปิดเข้าใช้ (LOGGING ON) ฐานข้อมูล การกำหนดสิทธิการเข้าถึงข้อมูลเป็นคำสั่งที่ใช้กำหนดสิทธิให้กับผู้ใช้แต่ละคนมีสิทธิกระทำการใดกับข้อมูล เช่น การเพิ่มข้อมูล การแก้ไขข้อมูล หรือการลบข้อมูลในตารางใดได้บ้างหรือการกำหนดให้มีสิทธิดูข้อมูลได้เพียงอย่างเดียว การกำหนดสิทธิในการเข้าถึงข้อมูล ได้แก่ การเรียกค้นข้อมูลด้วยคำสั่ง (SELECT) การเพิ่มข้อมูลมูลด้วยคำสั่ง (INSERT) การลบข้อมูลมูลด้วยคำสั่ง (DELETE) หรือการปรับปรุง มูลด้วยคำสั่ง (UPDATE) ซึ่งการกำหนดสิทธิเหล่านี้จะอยู่ในรูปแบบของคำสั่ง GRANT เป็นดังนี้

GRANT <SELECT,INSERT,UPDATE,DELETE>ON <table name> TO <user name>;

GRANT คำสั่งที่ต้องมีทุกครั้งที่ต้องการกำหนดสิทธิการเข้าถึงข้อมูล

SELECT,INSERT,UPDATE,DELETEสิทธิในการจัดการข้อมูล

table name ตารางหรือวิวที่ให้สิทธิในการจัดการข้อมูล

user name ผู้ใช้ที่ถูกให้สิทธิในการจัดการข้อมูล

2.1 การกำหนดสิทธิในการเรียกดูข้อมูล ถ้าต้องการให้ Wichai มีสิทธิเรียกดูข้อมูลในตาราง CUSTOMERSTAB คำสั่งการกำหนดสิทธิเข้าถึงข้อมูลในภาษา SQL จะเป็นดังนี้

GRANT SELECT ON CUSTOMERSTAB TO Wichai;

ผลของคำสั่งนี้ Wichai จะสามารถเข้าถึงข้อมูลในตาราง CUSTOMERSTAB ได้โดยสามารถใช้คำสั่งเรียกค้นข้อมูล(SELECT) ได้เท่านั้นแต่ไม่สามารถใช้คำสั่งอื่น ๆ ได้

2.2 การกำหนดสิทธิในการเพิ่มข้อมูล ถ้าต้องการให้ Thidarat มีสิทธิเพิ่มเติมข้อมูลในตาราง SALESTAB คำสั่งการกำหนดสิทธิเข้าถึงข้อมูลก็จะเป็นดังนี้

GRANT INSERT ON SALESTAB TO Thidarat;

ผลของคำสั่งนี้ Thidarat สามารถเข้าถึงข้อมูลในตาราง SALESTAB ได้โดยสามารถใช้คำสั่งเพิ่มเติมข้อมูล (INSERT) ได้เท่านั้นแต่ไม่สามารถใช้คำสั่งอื่น ๆ ได้

2.3 การกำหนดสิทธิในการแก้ไขข้อมูล

ถ้าต้องการให้ Thidarat มีสิทธิในการแก้ไขข้อมูล(UPDATE)ในตาราง SALESTAB คำสั่งการกำหนดสิทธิเข้าถึงข้อมูลก็จะเป็นดังนี้

GRANT UPDATE ON SALESTAB TO Thidarat;

ผลของคำสั่งนี้ Thidarat สามารถเข้าถึงข้อมูลในตาราง SALESTAB ได้โดยสามารถใช้คำสั่งปรับปรุงข้อมูล(UPDATE) ได้เท่านั้นแต่ไม่สามารถใช้คำสั่งอื่น ๆ ได้

2.4 การกำหนดสิทธิการเข้าถึงข้อมูลหลายคำสั่งของผู้ใช้เป็นกลุ่ม ในการกำหนดสิทธิการเข้าถึงข้อมูลสามารถกำหนดสิทธิในการเข้าถึงข้อมูลเป็นกลุ่มได้ ดังนี้

ถ้าต้องการให้ Wichai สามารถเรียกดูข้อมูล และเพิ่มข้อมูลได้ในตาราง ORDERSTAB คำสั่งที่ใช้ดังนี้

GRANT SELECT, INSERT ON ORDERSTAB TO Wichai;

ผลของคำสั่งจะทำให้ Wichai สามารถใช้คำสั่ง SELECT และคำสั่ง INSERT ในตาราง Order ได้

ถ้าต้องการให้ทั้ง Wichai และ Thidarat สามารถใช้คำสั่ง SELECT และ INSERT ได้ จะต้องใช้การกำหนดสิทธิการเข้าถึงข้อมูลดังนี้

GRANT SELECT, INSERT ON ORDERSTAB TO Wichai, Thidarat;

2.5การกำหนดสิทธิการเข้าถึงข้อมูลโดยสามารถเข้าถึงข้อมูลบางส่วน เราสามารถกำหนดสิทธิการเข้าถึงข้อมูลเป็นคอลัมน์ได้

ถ้าต้องการ Thidarat มีสิทธิเปลี่ยนค่าในคอลัมน์ SALECOM ในตาราง SALESTAB ได้เพียงคอลัมน์เดียว จะใช้คำสั่ง

GRANT UPDATE (SALECOM) ON SALESTAB TO Thidarat;

ผลของคำสั่งจะทำให้ Thidarat สามารถปรับปรุงข้อมูล(UPDATE) ในคอลัมน์ SALECOMในตารางพนักงานขาย(SALESTAB) ได้เพียงคอลัมน์เดียว

ถ้าต้องการให้ Thidarat มีสิทธิเข้าถึงข้อมูลได้มากกว่า 1 คอลัมน์ โดยสามารถปรับปรุงข้อมูลในคอลัมน์ ADDRESS และ SALECOM ในตาราง SALESTAB ได้

GRANT UPDATE (ADDRESS,SALECOM) ON SALESTAB TO Thidarat;

ผลของคำสั่งจะทำให้ Thidarat ปรับปรุงข้อมูล(UPDATE)ในคอลัมน์ ADDRESS และ SALECOM ในตารางพนักงานขาย(SALESTAB) ได้เพียงคอลัมน์เดียว

2.6 การให้สิทธิในการเข้าถึงข้อมูลทั้งหมด ในการกำหนดสิทธิในการเข้าถึงข้อมูลทั้งหมดในภาษา SQL สามารถใช้คำสั่งใน 2 ลักษณะ ดังนี้

-การใช้ ALL PRIVILEGES (หรือ ALL เท่านั้น) ในคำสั่ง GRANT

ถ้าต้องการให้ Nattapol สามารถทำคำสั่งใด ๆ ในตาราง CUSTOMERSTAB ได้

GRANT ALL PRIVILEGES ON CUSTOMERSTAB TO Nattapol;

หรือ

GRANT ALL ON CUSTOMERSTAB TO Nattapol;

-การใช้ PUBLIC ในคำสั่ง GRANT เป็นการให้สิทธิในการเรียกดูข้อมูลแก่ผู้ใช้ทุกคน โดยจะใช้ PUBLIC ร่วมด้วยกับคำสั่ง SELECT ควบคู่ไปกับคำสั่ง GRANT เช่น

ถ้าต้องการให้ผู้ใช้คนไหนก็ได้เข้าไปดูตารางคำสั่งซื้อจะใช้คำสั่งดังนี้

GRANT SELECT ON ORDERSTAB TO PUBLIC ;

การใช้คำสั่ง GRANT ในรูปของการให้สิทธิแก่ผู้ใช้ทั้งหมดในการแก้ไขปรับปรุงตารางข้อมูลได้จะเป็นอันตรายต่อข้อมูลมาก จึงควรระมัดระวังในการใช้คำสั่ง GRANT กับ PUBLIC ให้มาก

2.7 การอนุญาตให้คนอื่นให้สิทธิการเข้าถึงตารางแทนเจ้าของตาราง ในบางครั้งผู้สร้างตารางอาจต้องการให้ผู้ใช้คนอื่นสามารถให้สิทธิต่าง ๆ ในตารางได้โดยใช้ GRANT SELECT ร่วมกับอนุประโยค WITH GRANT OPTION

ถ้า Thidarat ซึ่งเป็นเจ้าของตาราง CUSTOMERSTAB ต้องการให้ Wichai มีสิทธิอนุญาตให้ผู้ใช้คนอื่น ๆ มาใช้ตารางของตนจะใช้คำสั่งดังนี้

GRANT SELECT ON CUSTOMERSTAB TO Wichai WITH GRANT OPTION;

ผลของคำสั่งนี้จะทำให้ Wichai มีสิทธิในการเลือกให้สิทธิ (SELECT) แก่บุคคลที่สามได้ที่

3.การยกเลิกสิทธิการเข้าถึงข้อมูล

คำสั่งการยกเลิกสิทธิการเข้าถึงข้อมูลเป็นคำสั่งการยกเลิกสิทธิใดๆแก่ผู้ใช้ตามที่ได้ใช้กำหนดสิทธิการเข้าถึงข้อมูลไว้ คำสั่งการยกเลิกสิทธิการเข้าถึงข้อมูลมีรูปแบบคือ

REVOKE <SELECT,INSERT,UPDATE,DELETE>ON <table name> FROM <user name>;

REVOKE เป็นคำสั่งที่ต้องมีทุกครั้งที่ต้องการยกเลิกสิทธิการเข้าถึงข้อมูล

SELECT,INSERT,UPDATE,DELETEสิทธิในการจัดการข้อมูล

table name ตารางหรือวิวที่ให้สิทธิในการจัดการข้อมูล

user name ผู้ใช้ที่ถูกให้สิทธิในการจัดการข้อมูล

3.1 การยกเลิกสิทธิในการเรียกดูข้อมูล

3.2 การยกเลิกสิทธิในการแก้ไขและลบข้อมูล

ถ้าต้องการยกเลิกสิทธิในการแก้ไขข้อมูลในตารางพนักงานขาย(SALESTAB) ของ Thidarat คำสั่งการยกเลิกสิทธิเข้าถึงข้อมูลดังนี้

REVOKE UPDATE ON SALESTAB TO Thidarat;

ผลจากคำสั่งนี้ Thidarat จะไม่สามารถแก้ไขข้อมูลในตารางพนักงานขาย(SALESTAB) ได้

ถ้าต้องการยกเลิกสิทธิในการเพิ่มเติมข้อมูลในตารางคำสั่งซื้อ(ORDERSTAB)ของ Thidarat จะใช้คำสั่งดังนี้

REVOKE INSERT ON ORDERSTAB FROM Wichai;

ผลจากคำสั่งนี้ Wichai จะไม่สามารถเพิ่มเติมข้อมูลในตารางคำสั่งซื่อ(ORDERSTAB) ได้ถ้าต้องการยกเลิกสิทธิในการเพิ่มเติมข้อมูลและการลบข้อมูลในตารางลูกค้า(CUSTOMERSTAB) ของ Wichai และ Nattapol จะใชคำสั่งดังนี้

REVOKE INSERT,DELETE ON CUSTOMERSTAB FROM Wichai,Nattapol;

ผลจากคำสั่งนี้ Wichai และ Nattapol จะไม่สามารถเพิ่มเติมข้อมูลหรือลบข้อมูลในตาราง ลูกค้า(CUSTOMERSTAB) ได้

ตอนที่ 12.3 การควบคุมความปลอดภัยด้วยวิว

หัวเรื่อง

เรื่องที่ 12.3.1 วิว

เรื่องที่ 12.3.2 ลักษณะส่วนรวมของวิว

เรื่องที่ 12.3.3 การปรับปรุงวิว

แนวคิด

1. วิวเป็นตารางที่ถูกสร้างขึ้นมาเพื่อป้องกันข้อมูลให้ผู้ใช้สามารถใช้ข้อมูลบางส่วน ตามที่ DBA เป็นผู้กำหนดเพื่อจำกัดการเข้าถึงของข้อมูลของผู้ใช้
2. วิว เปรียบเสมือนหน้าต่างของข้อมูลจากตารางหนึ่งๆที่ถูกเรียกดูหรือเพื่อทำการเปรียบแปลงข้อมูล วิวเป็นตารางเสมือนตารางจริง ที่มีข้อมูลจากตารางหลัก โดยไม่มีข้อมูลเก็บอยู่จริงเหมือนตารางหลัก
3. การปรับปรุงแก้ไขวิว(INSERT,UPDATE,DELETE) จะมีผลกระทบต่อค่าในตารางที่เป็นฐานข้อมูลของวิว วิวเป็นตารางที่เกิดจากผลลัพธ์ของการสอบถามข้อมูล วิวทุกวิวไม่สามารถปรับปรุงแก้ไขได้ทั้งหมด จะมียงบางวิวเท่านั้นที่สามารถปรับปรุงแก้ไขได้

วัตถุประสงค์

หลังจากศึกษาตอนที่ 12.3 แล้ว นักศึกษาสามารถ

1. บอกความหมายและลักษณะของวิวได้
2. บอกลักษณะส่วนรวมของวิวได้
3. บอกวิธีการปรับปรุงแก้ไขวิวได้

เรื่องที่ 12.3.1 วิว(View)

การควบคุมความปลอดภัยให้กับข้อมูลสามารถสร้างโครงสร้างข้อมูลใหม่ ที่ทำให้ผู้ใช้ เห็นเพียงโครงสร้างบ้างส่วนของฐานข้อมูลเท่านั้น ที่เป็นการป้องกันไม่ให้ผู้ใช้ได้เห็นข้อมูลทั้งหมดของฐานข้อมูล เราเรียกตารางข้อมูลประเภทนี้ว่า “ตารางเสมือน” หรือ “วิว” บางครั้งการออกแบบฐานข้อมูลในระดับกายภาพก็ต้องกำหนดตารางเป็นลักษณะวิว เพื่อเป็นการป้องกันรักษาความปลอดภัยของข้อมูลและการควบคุมการใช้งานในระบบฐานข้อมูล เพราะหากสร้างเป็นตารางข้อมูลจริงอาจจะเกิดความซ้ำซ้อนของข้อมูลมากซึ่งยากต่อการควบคุมการใช้งาน

1.โครงสร้างของวิว

วิว(VIEW)หรือตารางเสมือนเป็นตารางข้อมูลที่มีรายละเอียดหรือได้รายละเอียดมาจากตารางหลัก วิว(view) ถูกสร้างขึ้นจากฐานข้อมูล โดยตารางที่สร้างขึ้นนี้จะสอดคล้องกับการใช้งานของผู้ใช้และยังเป็นการป้องกันข้อมูลที่แท้จริงภายในฐานข้อมูล วิว(view) ถูกสร้างขึ้นจากฐานข้อมูล โดยวิวที่สร้างขึ้นนี้จะสอดคล้อง

กับการใช้งานของผู้ใช้และยังเป็นการป้องกันข้อมูลที่แท้จริงภายในฐานข้อมูล วิว(view) ถูกสร้างขึ้นจากฐานข้อมูล โดยตารางที่สร้างขึ้นนี้จะสอดคล้องกับการใช้งานของผู้ใช้และยังเป็นการป้องกันข้อมูลที่แท้จริงภายในฐานข้อมูล ตารางเหล่านี้จะทำงานเช่นเดียวกับตารางธรรมดา แต่ไม่มีข้อมูลเป็นของตนเอง วิวใช้เป็นเครื่องมือในการควบคุมไม่ให้ผู้ใช้เข้าไปดูข้อมูลทั้งหมดของตารางได้ วิวเป็นกลไกรักษาความปลอดภัยในการปกปิดส่วนต่าง ๆ ของตารางที่เป็นความลับหรือเกินความจำเป็นสำหรับผู้ใช้ เช่น ถ้าต้องการให้พนักงานขายดูตารางข้อมูลพนักงานขายได้ แต่ไม่ต้องการให้เห็นค่าคอมมิชชั่นของแต่ละคน ก็ควรสร้างวิวของตารางพนักงานขายที่ไม่มีคอลัมน์ค่าคอมมิชชั่นไว้ให้พนักงานขายได้เรียกดู

ดังนั้นในการป้องกันและรักษาความปลอดภัยของข้อมูลในการเรียกใช้ข้อมูลที่แตกต่างจากตารางข้อมูลที่ออกแบบไปแล้ว ก็อาจทำได้โดยการสร้างเป็นวิว

2.การทำงานของวิว

เมื่อมีการเรียกใช้วิว ระบบจัดการฐานข้อมูลจะทำหน้าที่โดยเริ่มค้นหาข้อกำหนดของวิวในคำสั่ง SQL ที่เก็บไว้ในฐานข้อมูล แล้วแปลคำสั่งของวิวเพื่อไปนำข้อมูลมาจากตารางข้อมูลจริง ทำให้วิวรักษาความถูกต้องของโครงสร้างข้อมูล (integrity) ไว้ได้

สำหรับวิวแบบง่ายๆ ระบบจัดการฐานข้อมูลอาจสร้างแต่ละแถวของวิวขึ้นมาจากตารางข้อมูลจริงเลย ส่วนวิวที่ซับซ้อนนั้นระบบจัดการฐานข้อมูลจะเก็บแถวของวิวไว้ในตารางชั่วคราว แล้วจึงแสดงผลจากตารางชั่วคราว และเลิกใช้ตารางชั่วคราวนั้นเมื่อหมดความต้องการใช้งานอีกต่อไป คือเมื่อสิ้นสุดคำสั่งของ SQL อย่างไรก็ตามไม่ว่าระบบจัดการฐานข้อมูลจะจัดการกับวิวอย่างไร ผลที่ได้ที่ผู้ใช้ได้รับก็ไม่แตกต่างกัน นั่นคือวิวสามารถอ้างอิงได้จากคำสั่ง SQL เสมือนหนึ่งว่าอ้างอิงไปยังตารางข้อมูลจริงเลย

3. การสร้างวิว

การสร้างวิวได้จากการ query ในคำสั่ง SQL ทำให้เห็นข้อมูลในแถวและคอลัมน์ตามต้องการ การสร้างวิวอาจสร้างมาจากตารางข้อมูลเดียวหรือมากกว่าหนึ่งตารางได้ ภาษา SQL จะมีการสร้างวิวโดยใช้คำสั่ง CREATE VIEW ซึ่งมีรูปแบบทั่วไปดังนี้

```
CREATE VIEW <view name>
        |column1 , column2 ....>)]
       AS <SELECT statement>;
```

CREATE VIEW เป็นคำสั่งที่ต้องมีทุกครั้งที่ต้องการสร้างวิว

view name ชื่อวิวที่ต้องการสร้าง

column 1 ชื่อของคอลัมน์ที่ต้องการตั้งชื่อในวิวที่สร้างขึ้น

AS <SELECT statement > เป็นไปตามเงื่อนไขในการเรียกค้น

ถ้าต้องการสร้างวิวชื่อ SALESOWN จากตารางพนักงานขาย(SALESTAB) โดยให้มีคอลัมน์ SALENO SALENAME และADDRESS จะใช้คำสั่งสร้างวิวดังนี้

```
CREATE VIEW SALESOWN
    AS  SELECT SALENO,SALENAME,ADDRESS
    FROM SALESTAB;
```

ตาราง SALESTAB

SALENO	SALENAME	ADDRESS	SALECOM
1001	Chaiwat	Bangkok	0.12
1002	Mitree	Puket	0.13
1004	Benjawan	Bangkok	0.11
1007	Kanjana	Chiangmai	0.15
1003	Ternjai	Nonthaburi	0.10

วิว SALESOWN

SALENO	SALENAME	ADDRESS
1001	Chaiwat	Bangkok
1002	Mitree	Puket
1004	Benjawan	Bangkok
1007	Kanjana	Chiangmai
1003	Ternjai	Nonthaburi

ตารางที่ 12. 1 แสดงวิว SALESOWN

ผลของคำสั่งจะได้ตาราง SALESOWN ที่ไม่มีคอลัมน์ SALECOM อยู่ดังตารางที่ 12.1

ถ้าต้องการสร้างวิวชื่อ BANGKOKSTAFF จากตาราง SALESTAB โดยให้มีคอลัมน์ ADDRESS ที่เป็น “Bangkok” จะใช้คำสั่งดังนี้

```
CREATE VIEW  BANGKOKSTAFF
    AS SELECT *
        FROM SALESTAB
        WHERE ADDRESS = 'Bangkok';
```

ตาราง SALESTAB

SALENO	SALENAME	ADDRESS	SALECOM

1001	Chaiwat	Bangkok	0.12
1002	Mitree	Puket	0.13
1004	Benjawan	Bangkok	0.11
1007	Kanjana	Chiangmai	0.15
1003	Ternjai	Nonthaburi	0.10

วิว BANGKOKSTAFF

SALENO	SALENAME	ADDRESS	SALECOM
1001	Chaiwat	Bangkok	0.12
1004	Benjawan	Bangkok	0.11

ตารางที่ 12.2 แสดงวิว BANGKOKSTAFF

ผลจากคำสั่งนี้จะทำให้ได้วิวที่ชื่อ BANGKOKSTAFF ดังตารางที่ 12.2 ซึ่งเป็นวิวที่สามารถใช้ได้เหมือนตารางอื่น ๆ คือสามารถสอบถามข้อมูล แก้ไขปรับปรุง นำไปใส่ ลบออกจากและรวมกับตารางอื่น ๆ ได้

ถ้าต้องการสอบถามข้อมูลจากวิว BANGKOKSTAFF

```
SELECT * FROM BANGKOKSTAFF;
```

ผลของคำสั่งนี้จะแสดงทุกคอลัมน์ในวิว BANGKOKSTAFF

วิวที่สร้างขึ้นนี้จะถูกเปลี่ยนแปลงโดยอัตโนมัติไปตามตารางข้อมูลที่สร้างวิว เช่น วิว BANGKOKSTAFF ถูกสร้างมาจากตารางพนักงานขาย (SALESTAB) ถ้าตารางพนักงานขาย (SALESTAB) มีการปรับปรุง โดยการเพิ่มพนักงานขายที่อยู่ใน Bangkok เข้าไปอีกคนหนึ่งในตารางพนักงานขาย(SALESTAB) พนักงานขายผู้นี้ก็จะปรากฏอยู่ในวิว BANGKOKSTAFF เองโดยอัตโนมัติ

การสร้างวิวให้เกิดประสิทธิภาพในการรักษาความปลอดภัยของข้อมูลและให้เกิดความเร็วในการสอบถามข้อมูลควรกำหนดขอบเขตโครงสร้างข้อมูลที่ต้องการ เพื่อจัดทำเป็นโครงสร้างของวิว โดยกำหนดเฉพาะชื่อคอลัมน์ไม่ต้องกำหนดชนิดข้อมูล เพราะจะเป็นไปตามที่กำหนดไว้ในตารางข้อมูลที่เลือกแล้ว นอกจากการกำหนดขอบเขตแล้วในการสร้างวิวจะระบุเฉพาะชื่อคอลัมน์ของวิวที่ต้องการเท่านั้น

4. การลบโครงสร้างของวิว

เมื่อต้องการลบโครงสร้างของวิวที่ถูกนิยามขึ้น สามารถทำได้ด้วยคำสั่ง DROP TABLE แล้วตามด้วยตารางที่ต้องการลบ รูปแบบทั่วไปมีดังนี้

DROP VIEW < view name>;

DROP VIEW เป็นคำสั่งที่ต้องมีทุกครั้งที่ต้องการลบวิว

view name ชื่อวิวที่ต้องการลบ

ถ้าต้องการลบโครงสร้างตารางเสมือนชื่อ BANGKOKSTAFF

```
DROP VIEW BANGKOKSTAFF;
```

ผลของคำสั่งนี้จะทำให้วิว BANGKOKSTAFF ถูกลบไป

5 **คุณสมบัติของวิว**

วิวมีคุณสมบัติดังนี้

-วิวเกิดจากส่วนย่อยของข้อมูลจากตารางข้อมูลจริงได้มากกว่าหนึ่งตาราง

-ค่าที่ปรากฏบนวิวเป็นค่าจริงในตารางข้อมูล

-สามารถปรับปรุงข้อมูลในวิวได้ ถ้าได้รับการอนุญาตจากระบบจัดการฐานข้อมูล ได้แก่ การเพิ่มแถวในวิว(INSERT) การปรับปรุงคอลัมน์ในวิว(UPDATE) การลบข้อมูลในวิว(DELETE)

-สามารถกำหนดสิทธิการใช้งานให้ผู้ใช้งานได้ว่าจะให้ใช้วิวหรือไม่ให้ใช้ เช่นเดียวกับตารางข้อมูล โดยไม่ต้องยุ่งเกี่ยวกับตารางข้อมูลจริง

-สามารถกำหนดเงื่อนไขการเรียกใช้ลงในวิวอย่างถาวร เพื่อให้ง่ายต่อผู้ใช้

-วิวช่วยให้ทำงานง่ายขึ้น เพราะทำให้สามารถสอบถามข้อมูลที่ต้องการได้ง่ายขึ้น

ตัวอย่าง เมื่อสร้างวิวขึ้นมา ดังนี้

```
CREATE VIEW view-emp
    SELECT EMPNO,ENAME,JOB,MGR,SAL
    FROM demp
    WHERE DEPTNO=10;
```

จากวิว view-emp สามารถใช้คำสั่ง SQL เพื่อสอบถามข้อมูลอย่างง่ายๆ ดังนี้

```
SELECT ENAME,JOB
    FROM view-emp
    WHERE HIREDATE= '21-AMR-89";
```

หากไม่สร้างวิว ก็จะต้องใช้คำสั่ง SQL ที่ยุ่งยากกว่า เพื่อเรียกข้อมูลดังนี้

```
SELECT ENAME,JOB
        FROM demp
        WHERE DEPTNO=10 AND HIREDATE= '21-AMR-89";
```

วิวไม่ได้ช่วยเรื่องความเร็ว บางครั้งการใช้วิวก็มีปัญหาในเรื่องความเร็ว
ตัวอย่างที่เมื่อสร้างวิวขึ้นมา ดังนี้

```
CREATE VIEW vsummary (DEPTNO,MINSAL,MAXSAL,AVGSAL)
        SELECT DEPTNO,MIN(SAL), MAX(SAL),AVG(SAL)
        FROM demp
        GROUP BY DEPTNO;
```

และเรียกข้อมูลจากวิวด้วยคำสั่งต่อไปนี้

```
SELECT DEPTNO,MINSAL
        FROM vsummary WHERE DEPTNO = 20 ;
```

ผลก็คือเครื่องจะทำงานได้ผลช้ากว่าคำสั่งที่เรียกข้อมูลจากตารางข้อมูลโดยตรง ต่อไปนี้

```
SELECT DEPTNO,MIN(SAL) FROM demp
GROUP BY DEPTNO HAVING DEPTNO = 20;
```

หลีกเลี่ยงการสร้างวิวจากวิวหรือ join วิว เพราะจะทำให้ยุ่งยากซับซ้อนต่อการจัดการข้อมูล

6.ข้อดีของวิว

วิวเป็นข้อมูลที่ถูกคัดลอกออกมาจากฐานข้อมูลเพื่อเป็นการป้องกันและรักษาความปลอดภัยในระบบการจัดการฐานข้อมูล วิวมีความสำคัญต่อการรักษาความปลอดภัยในการจัดการฐานข้อมูล ข้อดีของวิวในระบบจัดการฐานข้อมูลได้แก่

6.1 วิวช่วยสนับสนุนการรักษาความปลอดภัยของข้อมูลตามมุมมองของของผู้ใช้ได้อย่างมีประสิทธิภาพ ได้แก่ ผู้ใช้สามารถมีมุมมองต่างกันในข้อมูลที่แตกต่างกันได้โดยการจัดรูปแบบของโครงสร้างข้อมูลของวิวนี้จะทำให้ได้ข้อมูลทั้งแถวและคอลัมน์ตามที่ผู้ใช้งานต้องการเท่านั้น

6.2 วิวช่วยรักษาความปลอดภัยในการปรับปรุงข้อมูลทั้งการเพิ่ม ลบ แก้ไข ข้อมูล ด้วยคำสั่ง INSERT , DELETE และ UPDATE โดยปรับปรุงข้อมูลเฉพาะบ้างส่วนของฐานข้อมูลผ่านวิว

6.3 วิวช่วยรักษาความปลอดภัยของข้อมูล โดยจำกัดผู้ใช้ไม่ให้เข้าถึงข้อมูลจริงและยังช่วยไม่ให้กระทบต่อต่อฐานข้อมูล

6.4 วิวช่วยให้ง่ายต่อการสอบถามข้อมูล เพราะวิวสามารถเรียกข้อมูลจากหลายๆ ตารางและแสดงผลเสมือนตารางเดียว โดยเปลี่ยนการสอบถามจากตารางข้อมูลจริงหลายตารางมายังตารางเสมือนตารางเดียว

6.5 วิวมีความง่ายทางโครงสร้าง เพราะวิวจะให้โครงสร้างข้อมูลตามที่ผู้ใช้งานต้องการ โดยไม่ต้องคำนึงถึงเรื่องความซับซ้อนของข้อมูล

6.6 วิวไม่มีผลกระทบต่อการเปลี่ยนแปลงโครงสร้างตาราง วิวสามารถควบคุมความคงเส้นคงวา (consistent) ในการใช้งาน แม้ว่าจะมีความจำเป็นต้องปรับเปลี่ยนตารางข้อมูลจริงอย่างใดก็ตาม ไม่ว่าจะเป็นชื่อตาราง ชื่อคอลัมน์ หรือ แม้แต่จะแบ่งแยกตารางข้อมูลออกเป็นหลายตารางก็ตาม

6.7 วิวช่วยให้มีความถูกต้องของข้อมูล เพราะข้อมูลถูกเรียกใช้ผ่านวิว ไม่ได้ผ่านข้อมูลจริง ระบบจัดการฐานข้อมูลสามารถตรวจสอบข้อมูลว่าตรงกับกฎควบคุมความถูกต้องของโครงสร้างข้อมูลที่กำหนดไว้หรือไม่

7.ข้อด้อยของวิว

ข้อด้อยบางประการในการใช้วิวคือ

7.1 ข้อจำกัดในด้านประสิทธิภาพ เพราะการเรียกใช้ข้อมูลผ่านวิวที่มีความซับซ้อนมาก จะทำให้มีการเรียกคำสั่งสอบถามข้อมูลหลายคำสั่ง ดังนั้นแม้ว่าจะเรียกข้อมูลผ่านวิวที่ง่ายๆ แต่ถ้าวิวสร้างมาจากตารางข้อมูลที่เชื่อมกันอย่างซับซ้อน ก็จะต้องกินเวลาในการทำงานนาน

7.2 ข้อจำกัดในการปรับปรุงข้อมูล เมื่อผู้ใช้ต้องการปรับปรุงข้อมูลบางแถวจากวิว ระบบจัดการฐานข้อมูลจะแปลความต้องการไปยังแถวที่ต้องการปรับปรุงในตารางข้อมูลจริง ซึ่งจะกระทำได้กับวิวแบบง่ายๆ แต่สำหรับวิวที่ซับซ้อนก็จะจำกัดให้อ่านข้อมูลได้อย่างเดียว

เรื่องที่ 12.3.2 **ลักษณะของวิว**(View)

การสร้างวิวเพื่อใช้งานมีหลายลักษณะ ตัวอย่างที่เช่น วิวทางระดับ (horizontal views) วิวทางดิ่ง (vertical views) วิวทางระดับและทางดิ่ง (row/column subset views) วิวกลุ่ม (grouped views) และ วิวร่วม (joined views) สำหรับวิว 3 ลักษณะแรกได้แก่ วิวทางระดับ วิวทางดิ่ง วิวทางระดับและทางดิ่ง สามารถปรับปรุงข้อมูลผ่านวิวทั้ง 3 ลักษณะนี้ได้ แต่วิวกลุ่มไม่สามารถปรับปรุงข้อมูลผ่านวิวได้ สำหรับวิวร่วมถ้าเชื่อมวิวกันด้วยคีย์หลักของตารางก็สามารถปรับปรุงข้อมูลได้ ดังนี้

1.วิวทางระดับ

เป็นวิวที่เกิดจากการเลือกข้อมูลทุกคอลัมน์ เฉพาะบางแถว จากตารางข้อมูล ตาราง Demployer ที่แสดงในตารางที่ 12.3 ถ้าต้องการนำมาสร้างเป็นวิว Vemployee ซึ่งเป็นวิวทางระดับดังแสดงในตารางที่ 12. 4 จะใช้คำสั่งดังนี้

```
CREATE VIEW Vemployee AS SELECT*
    FROM Demployee
    WHERE SALARY = '18000';
```

EMP_ID	NAME	SURNAME	SEX	SALARY	DEPT_ID
1001	ธนา	ดีเลิศ	M	15,000	003
1002	ศิรินุช	รักเรียน	F	18,000	001
1003	ศิริชัย	พลาสัย	M	16,000	003
1004	ฉวีวรรณ	งานดี	F	18,000	002
1005	ประนอม	ร่าเริง	F	18,000	001

ตารางที่ 12.3 ตาราง Demployee

EMP_ID	NAME	SURNAME	SEX	SALARY	DEPT_ID
1002	ศิรินุช	รักเรียน	F	18,000	001
1004	ฉวีวรรณ	งานดี	F	18,000	002

1005	ประนอม	ร่าเริง	F	18,000	001

ตารางที่ 12. 4 วิว Vemployee

2.วิวทางดิ่ง

เป็นวิวที่เกิดจากการเลือกข้อมูลจากบางคอลัมน์ ทุกแถวของข้อมูล ของตารางข้อมูล วิวทางดิ่งจากข้อมูลในตาราง Demployee ที่แสดงในตารางที่ 12.3 ถ้าต้องการนำมาสร้างเป็นวิว Vemployee เป็นวิวทางดิ่งมีข้อมูลดังแสดงในตารางที่ 12.5

```
CREATE VIEW Vemployee
    AS SELECT EMP_ID, NAME, SURNAME, SALARY FROM Demployee;
```

EMP_ID	NAME	SURNAME	SEX	SALARY	DEPT_ID
1001	ธนา	ดีเลิศ	M	15,000	003
1002	ศิรินุช	รักเรียน	F	18,000	001
1003	ศิริชัย	พลาสัย	M	16,000	003
1004	ฉวีวรรณ	งานดี	F	18,000	002
1005	ประนอม	ร่าเริง	F	18,000	001

ตารางDemployee

EMP_ID	NAME	SURNAME	SALARY
1001	ธนา	ดีเลิศ	15,000
1002	ศิรินุช	รักเรียน	18,000
1003	ศิริชัย	พลาสัย	16,000
1004	ฉวีวรรณ	งานดี	18,000
1005	ประนอม	ร่าเริง	18,000

ตารางที่ 12. 5 วิว Vemployee เป็นวิวทางดิ่งที่สร้างจากตาราง Demployee

3.วิวทางระดับและทางดิ่ง

เป็นวิวที่เกิดจากการเลือกข้อมูลจากบางแถวและบางคอลัมน์ของตารางข้อมูล วิวทางระดับและทางดิ่ง จากข้อมูลในตาราง Demployee ที่แสดงในตารางที่ 12.3 ถ้าต้องการนำมาสร้างเป็นวิว Vemployee เป็นวิวดิ่งมีข้อมูลดังแสดงในตารางที่ 12. 6 จะใช้คำสั่งดังนี้

```
CREATE VIEW Vemployee
    AS SELECT EMP_ID, NAME, SURNAME, SALARY
    FROM Demployee
    WHERE SALARY ='18,000';
```

EMP_ID	NAME	SURNAME	SEX	SALARY	DEPT_ID
1001	ธนา	ดีเลิศ	M	15,000	003
1002	ศิรินุช	รักเรียน	F	18,000	001
1003	ศิริชัย	พลาสัย	M	16,000	003
1004	ฉวีวรรณ	งานดี	F	18,000	002
1005	ประนอม	ร่าเริง	F	18,000	001

EMP_ID	NAME	SURNAME	SALARY
1002	ศิรินุช	รักเรียน	18,000
1004	ฉวีวรรณ	งานดี	18,000
1005	ประนอม	ร่าเริง	18,000

ตารางที่ 12. 6 วิว Vemployee เป็นวิวทางระดับและดิ่ง

4.วิวกลุ่ม

เป็นการเลือกข้อมูลโดยจัดให้เป็นกลุ่มๆ ดังนั้นจึงเลือกข้อมูลจากตารางข้อมูล ด้วยคำสั่งที่มีเงื่อนไข GROUP BY หรือ ORDER BY จากข้อมูลในตาราง Demployee ในตารางที่ ถ้าต้องการนำมาสร้างเป็นวิว Vemployee-count-by-salary เป็นวิวกลุ่มที่สรุปจำนวนของพนักงานที่มีเงินเดือนที่เท่ากัน ดังแสดงในตารางที่ 12. 7 จะใช้คำสั่งดังนี้

```
CREATE VIEW Vemployee_count_by_salary(SALARY,COUNT)
    AS SELECT SALARY, COUNT(*)
    FROM Demployee
    GROUP BY SALARY ;
```

EMP_ID	NAME	SURNAME	SEX	SALARY	DEPT_ID
1001	ธนา	ดีเลิศ	M	15,000	003
1002	ศิรินุช	รักเรียน	F	18,000	001
1003	ศิริชัย	พลาสัย	M	16,000	003
1004	ฉวีวรรณ	งานดี	F	18,000	002
1005	ประนอม	ร่าเริง	F	18,000	001

SALARY	COUNT(*)
15,000	1
18,000	3
16,000	1

ตารางที่ 12.7 วิว Vemployee_count_by_salary เป็นวิวแบบกลุ่ม

5.วิวร่วม

เป็นการเลือกข้อมูลจากหลายตารางข้อมูล หรือการเลือกข้อมูลผ่านหลายวิวก็ได้วิวร่วม จากข้อมูลในตาราง Demployee ที่แสดงในตารางที่12.3 และข้อมูลในตาราง Ddepatment ที่แสดงในตารางที่ 12.8 ถ้าต้องการนำมาสร้างเป็นวิว Vemployee_dep แบบร่วมเพื่อให้ได้ข้อมูลดังแสดงในตารางที่ 12.9 จะใช้คำสั่งดังนี้

```
CREATE VIEW Vemployee_dep AS
    SELECT EMP_ID, NAME, SURNAME, SALARY, DEPTNAME
    FROM Demployee, Ddepatment
    WHERE DEPT_ID = '001'
```

EMP_ID	NAME	SURNAME	SEX	SALARY	DEPT_ID
1001	ธนา	ดีเลิศ	M	15,000	003
1002	ศิรินุช	รักเรียน	F	18,000	001
1003	ศิริชัย	พลาสัย	M	16,000	003

1004	ฉวีวรรณ	งานดี	F	18,000	002
1005	ประนอม	ร่าเริง	F	18,000	001

DEPT_ID	DEPTNAME
001	ฝ่ายลูกค้าสัมพันธ์
002	ฝ่ายบุคคล
003	ฝ่ายการตลาด

ตารางที่ 12. 8 ตาราง Ddepatment

EMP_ID	NAME	SURNAME	SALARY	DEPTNAME
1002	ศิรินุช	รักเรียน	18,000	ฝ่ายลูกค้าสัมพันธ์
1005	ประนอม	ร่าเริง	18,000	ฝ่ายลูกค้าสัมพันธ์

ตารางที่ 12. 9 วิว Vemployee_dep เป็นวิวร่วม

เรื่องที่ 12.3.3 **การปรับปรุงวิว**(View)

การปรับปรุงแก้ไขวิวได้แก่ การเพิ่มการปรับปรุง และการลบ(INSERT,UPDATE,DELETE) จะมีผลกระทบต่อค่าในตารางที่เป็นฐานข้อมูลของวิว วิวเป็นตารางที่เกิดจากการผลลัพธ์ของการสอบถามข้อมูล วิวทุกวิวไม่สามารถปรับปรุงแก้ไขได้ทั้งหมด วิวที่สามารถปรับปรุงแก้ไขข้อมูลโดยผ่านทางวิวได้ ได้แก่ วิวทางระดับ วิวทางดิ่ง วิวทางระดับและทางดิ่ง ส่วนวิวกลุ่มนั้นไม่สามารถปรับปรุงข้อมูลผ่านวิวได้ สำหรับวิวร่วมถ้าเชื่อมวิวกันด้วยคีย์หลักของตารางก็สามารถปรับปรุงข้อมูลได้

1.การเพิ่มแถวในวิว

ถ้าต้องการเพิ่มแถวลงวิว *vhardware-info* โดยใช้คำสั่งต่อไปนี้

```
INSERT INTO vhardware–info
    VALUES (“12345” , “P6” , 48);
```

ผลจากคำสั่ง INSERT ข้างต้น อาจได้ผล 2 แนวทาง คือ ระบบจัดการฐานข้อมูลปฏิเสธการเพิ่มข้อมูล หรือ ระบบจัดการฐานข้อมูลอนุญาตให้เพิ่มข้อมูลได้ ซึ่งถ้าอนุญาตก็จะเพิ่มแถวข้อมูลลงในตาราง *dhardware* มีค่าเป็น (“12345” , “P6” , 48 , null) ค่าในคอลัมน์สุดท้ายเป็น *null* เพราะค่าสุดท้ายไม่ได้กำหนด (แต่ถ้าในตารางกำหนดค่า *default* ไว้ ค่าในคอลัมน์สุดท้ายก็จะใช้ค่า *default*) ดังนั้น ผลจากคำสั่ง INSERT ข้างต้นจะได้ข้อมูลในตาราง *dhardware* และวิว *vhardware-info* ดังแสดงในตารางที่ 12.10 และ ตารางที่ 12.11

EQUIP-SERIAL	CPU	MEMORY	HARDDISK
12222	P5	24	40
12223	P5	24	50
12345	P6	48	Null

ตารางที่ 12.10 แสดงข้อมูลในตาราง *dhardware* หลังจากเพิ่มข้อมูลด้วยคำสั่งในวิว

EQUIP-SERIAL	CPU	MEMORY
12222	P5	24
12223	P5	24
12345	P6	48

ตารางที่ 12.11 แสดงข้อมูลในวิว *vhardware-info*

ในการเพิ่มข้อมูลเข้าไปในวิวจะต้องระวังว่าถ้าเป็นการเพิ่มค่าคีย์หลักต้องมีค่าไม่ซ้ำ มิฉะนั้นจะต้องเพิ่มคอลัมน์ ประกอบให้เป็นคีย์ หรือสร้างคอลัมน์ใหม่ ที่มีค่าเป็นลำดับแถว (row-no) ขึ้นเป็นคีย์

2.การลบค่าในวิว

ถ้าต้องการลบตาราง *dhardware* ภายใต้ข้อจำกัดของกฎควบคุมความถูกต้องของโครงสร้างข้อมูล โดยใช้คำสั่งต่อไปนี้

```
DROP TABLE dhardware RESTRICT ;
```

ผลก็คือ ถ้าในฐานข้อมูลไม่มีวิว *vhardware-info* ระบบจัดการฐานข้อมูลจึงจะยอมลบตาราง *hardware* พร้อมข้อมูลทั้งหมด แต่ถ้าในฐานข้อมูลมีวิว *hardware-info* ระบบจัดการฐานข้อมูลก็จะไม่ยอมลบตาราง *hardware* ให้เลย แต่ถ้าใช้คำสั่งต่อไปนี้

```
DROP TABLE dhardware CASCADE ;
```

ผลก็คือ ระบบจัดการฐานข้อมูลจะลบตาราง *dhardware* ให้โดยไม่สนใจว่าจะมีวิวที่สัมพันธ์กับตารางนี้หรือไม่ และจะลบวิวทั้งหมดที่เกี่ยวข้องด้วย