전면적인 보안 접근법

IBM® Redbooks®
Point-of-View 발행물 - IBM Academy of Technology

Chung-Sheng Li, Ph. D., Director IBM Research, **Katsumi Ohnishi**, IBM Executive Architect, **Josuyla R. Rao**, Director IBM Research

주요 내용

시스템에 침입하려는 공격 시도를 예측하고 차단하는 광범위한 보안 접근법을 선택하십시오 .

- 기존의 경계 방어적 모델에서 경계 영역의 세부 지점까지 꼼꼼하게 살피는 연속선상의 보안 모델로 보안 패러다임을 바꾸십시오 .
- 경계 영역의 세부 지점까지 방어 및 보안 인텔리전스를 구현하십시오 . 이는 모바일 , 소셜 , 클라우드 컴퓨팅의 트렌드와 함께 새롭게 등장하는 보안 위협을 해결하는 데 필수적입니다 .
- 제품 중심이 아닌, 통합적이고 포괄적인 보안 인텔리전스 솔루션을 지향하십시오 .
- 늘어나는 데이터 볼륨 , 증가하는 클라우드 및 모바일 사용자 , 웹 기술로 인한 위험 부담을 최소화하기 위해 보안 인텔리전스를 구현하십시오 .

현재의 보안 환경

컴퓨터에서 흔히 방패 모양을 띠고 있는 보안 데스크탑 아이콘은 개인 방화벽을 의미합니다 . 이 방화벽은 보안 위협과 공격을 차단하고 시스템을 검색하여 방화벽 침입자를 찾아냅니다 . 이러한 안전 장치는 세심한 보안 조치의 좋은 예이지만 , 기업의 경계 내에서 이와 같은 안전 기능을 구축하지 못하는 경우도 있습니다 . 그로 인해 비즈니스에 중요한 여러 서버가 허술하기 짝이 없는 기업 방화벽 , 침입 탐지 및 차단 메커니즘에 의존하곤 합니다 .

오늘날 각 기업과 정부 기관이 악의적인 공격자 또는 침입자로부터 정보를 보호하기 위해서는 보다 폭넓은 접근이 필요합니다 . 사용자가 보호 대상인 정보에 더 신속하고 편리하게 액세스하길 원하는 만큼 이는 쉬운 일이 아닙니다 . 따라서 세심하게 액세스 권한을 제어하고 잠재적 위협과 관련 없어 보이는 위협까지 광범위하게 탐지할 수 있는 더 똑똑한 보안 솔루션의 구현이 그 어느 때보다도 필요합니다 . 물론 침입자를 격리하고 피해를 최소화하기 위한 다층적 차단 방식도 필수적입니다 .

기업의 딜레마는 업무를 수행하고 서비스를 제공하기 위해 시스템에 대한 액세스를 허용하면서도 정보 자산을 보호해야 한다는 것입니다 . 그에 따른 위험 부담은 점점 커지고 있습니다 . 이를테면 데이터 볼륨이 꾸준히 증가하는 중입니다 . 클라우드 사용자 , 모바일 사용자와 재택 근무 사용자가 각처에서 다양한 장치를 통해 네트워크에 액세스합니다 . 인터넷 기반 협업 및 통신 애플리케이션도 늘고 있습니다 . 그리고 Web 2.0 기술의 시대가 도래하면서 기업 바깥의 사용자도 데이터와 제어 기능에 액세스할 수 있게 되었습니다. 이러한 모든 위험 요소는 어디서든 보안 사고가 발생할 수 있고 그 여파가 전 세계에 미칠 수 있음을 시사합니다 .

그 대응책으로 전체 엔터프라이즈 환경을 보호하기 위한 대형 방화벽을 구축하기 시작했습니다 . 하지만 지금은 네트워크 내의 각 자원을 보호하는 방향으로 바뀌었습니다 . 이러한 자원에는 서버 , 미들웨어 , 스토리지 , 서비스 지향 아키텍처 , 애플리케이션과 정보가 포함되며 , 이들 각각은 전략적 가치가 저마다 다를 수 있습니다 .

보안 사고에 대응하는 것만으로는 기업의 정보 , 네트워크와 전사적 환경을 제대로 보호할 수 없습니다 . 악의적 공격이 일어나기 전에 이를 예상하고 방지해야 합니다 . 그 준비 차원으로 , 물리적 이벤트와 가상 이벤트 , 무해한 듯 보이는 이벤트와 의심스러운 이벤트 , 로컬 활동과 글로벌 활동이 상관성을 갖는 연속선상에서 보안을 바라볼 필요가 있습니다 . 인텔리전스 및 법 집행 커뮤니티에서 쓰이는 보안 지식도 받아들여야 합니다 . 이러한 커뮤니티에서는 곧 일어날 사건에 대한 단서 (예 : 온라인 테러 공격 모의) 의 수집과 분석에 주력합니다 .

지속성 보안 위협의 여러 단계

기업은 ±Þ³ð 1 에서 보여 주는 것과 같은 각종 사내외 보안 위협에 직면해 있습니다 .

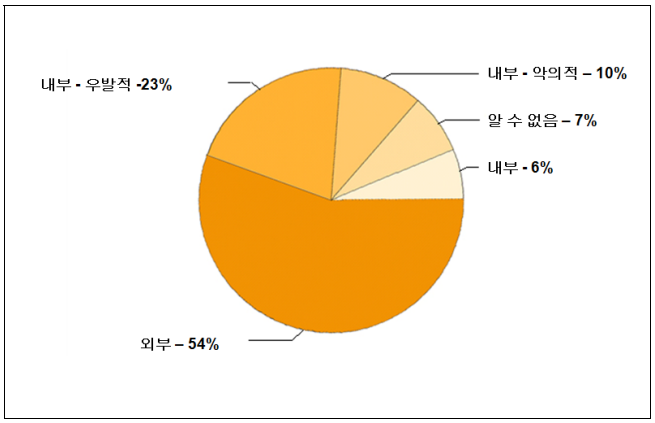

그림 1 발생하는 보안 공격의 비율

내부 위협 요인으로는 내부자가 악의적 의도로 또는 뜻하지 않게 시스템의 취약점을 통해 악성 코드를 유포하거나 데이터를 유출하거나 중요 데이터를 도용하는 경우가 포함됩니다 . 외부 위협 요인으로는 서비스 거부 (DoS), 웹 반달리즘과 허위 선전 , 봇넷 (감염되어 공격 소프트웨어 실행에 동원되는 컴퓨터의 그룹), 장비 파괴 등을 들 수 있습니다 . 전력망과 연료 , 통신 및 교통 시스템과 같은 주요 인프라에 대한 공격도 포함됩니다 .

이러한 보안 위협을 막기 위해 사용자의 배경 조사 , 액세스 제한 , 물리적 감시 , 플랫폼 무결성 모니터링 , 데스크탑 제어 , 사용자 상호 작용에 대한 프로파일링과 감사 등의 보안 조치를 수행하곤 합니다 . 허가 받지 않은 외부 사이트에 기밀 데이터를 전송하는 행위를 탐지하고 차단하는 것도 포함됩니다 .

SQL 인젝션 , 피싱 , APT(advanced persistent threats) 와 같이 다수의 유명 기업이 피해를 입었던 보안 위협도 있습니다 . APT 는 장기간에 걸쳐 단계적으로 진행되는 속성 때문에 비즈니스 자산에 대한 가장 심각한 공격 유형입니다 .

APT 는 다음과 같이 진행됩니다 .

1. 공격자가 소셜 미디어를 이용하여 위험하지 않은 듯 보이는 이메일 메시지를 보냅니다 . 이러한 수법을 *피싱 (phishing)* 이라고 합니다 . 사실 이와 같은 이메일 메시지에는 보안 체계를 뚫기 위한 첨부 파일 또는 숨겨진 애플리케이션이 들어 있습니다 . 이러한 애플리케이션을 *맬웨어 (malware)* 라고 합니다 .
2. 맬웨어를 통해 어떤 도구가 설치되는데 , 공격자는 바로 이 도구를 사용하여 방화벽 건너편의 서버와 컴퓨터에 원격으로 액세스하고 이를 제어할 수 있게 됩니다 .
3. 맬웨어는 사용자 신임 정보를 수집합니다 . 그런 다음 특별 권한을 가진 사용자에게 이동하고 최종적으로는 가치가 높은 표적을 공략합니다 .
4. 맬웨어가 주요 지점에 있는 스테이징 서버에 대한 접근에 성공합니다 .
5. 공격자가 감염된 외부 시스템의 스테이징 서버로 기밀 데이터를 전송합니다 .

지금까지는 기업의 경계를 따라 방어 체계를 강화하는 방법으로 이러한 보안 위협에 대처했습니다 . 기업의 경계를 넘나들며 비즈니스를 수행하기 시작하면서 그러한 방식은 예전만큼 효과적이지 않습니다 . 게다가 내부자에 의한 보안 위협을 다루지 못합니다 .

2008 년부터 내부자에 의한 보안 사고가 외적 요인에 의한 보안 사고보다 많아지면서 기존의 경계 방어 중심의 사이버 보안이 난관에 봉착했습니다 .

기업이 리스크에 대비하고 이를 관리하는 방식은 수익성 , 즉 비용 , 성공과 실효성의 측면에서 지대한 영향을 미칩니다 . 수많은 보안 방식과 제품이 등장함에 따라 가장 효과적으로 데이터 자산을 보호할 방법을 찾는 데 어려움이 따를 수 있습니다 .

종합적인 솔루션의 필요성

수십 년 전부터 기업들은 품질, 성능과 첨단 기술에 대한 기대감으로 네트워크 , 데이터와 시스템에서 IBM 솔루션을 신뢰하고 선택해 왔습니다 . 이제 고객들은 자산의 보안 영역에서도 동일한 기대를 갖고 있습니다 . IBM 은 이 보안 시장의 요구사항을 해결하고자 제품 중심의 시각에서 벗어나 통합적인 엔터프라이즈 보안 인텔리전스 솔루션을 지향합니다 . 이러한 접근은 적극적인 관리 , 실시간 정보 수집 , 상관성 분석 , 예측적 보안 위협 관리를 지원하는 기본적인 핵심 요소를 토대로 합니다 .

IBM 보안 인텔리전스 모델은 컴플라이언스부터 인프라까지 보안 문제의 전 범위를 다룹니다 . 이 모델의 프레임워크를 통해 IT 보안 위협과 전사적 위험 요인을 파악 , 예측 , 해결하고 컴플라이언스를 실현할 수 있습니다 . 이 프레임워크의 보안 기능은 PDCA (plan-do-check-act) 주기를 적용합니다 . 이 주기는 *심층 방어 (defense-in-depth)* 원칙을 근간으로 하며 , 이는 보안 교육 , 예방 , 탐지와 해결을 내용으로 하는 체계화된 계층적 접근 방식입니다 . 이러한 IBM 솔루션은 보안 이니셔티브에 참여한 연구자 ,

개발자 , 컨설턴트와 분야별 전문가 수천 명에 의해 완성되었습니다 . 뿐만 아니라 IBM 은 수천 건의 보안 프로젝트에서 컨설팅과 구현을 담당하면서 베스트 프랙티스와 프로세스에 대한 실무 지식과 전문성을 축적했습니다 .

보안 프레임워크

위험 요인이 현실화되기 전에 예측 , 감시하고 분석하는 기술과 이론을 가리키는 보안 인텔리전스가 현재 시장에서 각광 받고 있습니다 . 보안 인텔리전스는 보안 및 네트워크 장치부터 서버 운영 체제 , 애플리케이션 , 엔드포인트 , 인프라 자원까지 전 범위에서 통합적인 가시성과 실시간 분석을 제공합니다 . 보안 인텔리전스는 다음 핵심 요소로 구성되며 , 각 요소는 기초 단계에서 최적의 단계로 또는 사후 대응적 관점에서 사전 예방적 관점으로 발전합니다 .

- *사용자* – 중앙화된 디렉토리의 단계에서 강력한 인증 기반의 사용자 프로비저닝 , 역할 기반 분석 , ID 거버넌스 , 사용자 권한 제어로 발전합니다 .
- *데이터* – 암호화 , 액세스 제어 , 액세스 모니터링 , 데이터 손실 방지의 단계에서 데이터 흐름 분석 및 데이터 거버넌스로 발전합니다 . 소셜 컴퓨팅이 데이터 유출과 스피어 피싱 공격을 차단하는 데 더욱 중요한 역할을 하고 있습니다 .
- *애플리케이션* – 애플리케이션 검사 , 방화벽 , 소스 코드 검사의 단계에서 보안 애플리케이션 엔지니어링 프로세스 및 사기 탐지로 발전합니다 .
- *인프라* – 허술한 안티바이러스 경계 방어 단계에서 자산 관리 , 엔드포인트 및 네트워크 보안 관리로 (침입 탐지 및 차단 , 심층 패킷검사) 그리고 고급 네트워크 모니터링 , 포렌직 (forensics), 데이터 마이닝으로 발전합니다 .

보안 인텔리전스 솔루션의 핵심 요소

IBM 은 지능적 보안 위협 , 클라우드 컴퓨팅 , 모바일 컴퓨팅 , 규제와 컴플라이언스의 4 대 핵심 영역에 중점을 두고 보안 인텔리전스를 제공합니다 .

지능적 보안 위협 , 즉 APT 는 고도의 표적 공격으로서 중요 정보에 대한 지속적인 액세스 권한을 확보하게끔 설계되었습니다 . 이러한 보안 위협이 더욱 심각해지고 더 자주 발생하고 있습니다 . 해결책은 (지능적 보안 위협이 주로 피싱 공격에서 시작되므로) 인적 요인과 사회적 요인을 고려하고 보안 , 분석과 보안 위협 인텔리전스 기술을 통합하여 강력한 네트워크 계층을 구축하는 것입니다 .

보안 인텔리전스 솔루션은 방대한 데이터를 통합하고 그로부터 얻어지는 깊이 있는 통찰력을 바탕으로 APT 를 비롯한 각종 보안 위협을 막아냅니다 . IBM 보안 정보 및 이벤트 관리 (SIEM) 솔루션을 통해 사소한 장해 (noise) 와 실제 보안 위협을 구별할 수 있습니다. 또한 컨텍스트 기반의 데이터와 똑똑한 분석 기술을 활용하여 경보 오탐지율을 낮춥니다 .

대부분의 기업들이 클라우드 컴퓨팅을 활용할 필요성을 인식하지만 여전히 잠재적 위험성을 우려합니다 . 서비스 기업이자 보안 벤더인 IBM 은 클라우드에서 안전한 인프라를 제공하고 안전한 데이터 센터 및 클라우드에 정보를 격리하기 위한 플랫폼을 구축할 수 있는 유리한 입장에 있습니다 .

Gartner, Inc. 에 따르면 , 2014 년까지 모바일 장치에서 업무용 애플리케이션을 지원할 기업이 90% 에 이를 것으로 예상됩니다 .[1] 이러한 업무 환경의 확장 추세에 발맞춰 대부분의 CIO 는 직원에게 액세스 권한을 부여하면서 모바일 장치를 보호하는 것을 최우선 과제로 삼고 있습니다 . IBM 은 기업의 데이터에 대해 보안 액세스를 제공하면서 개인 정보를 보호하는 데 주력하며 엔드포인트 , 게이트웨이 , 애플리케이션 개발의 전반에서 광범위한 보안 기능을 제공합니다 . 또한 모바일 장치 관리 기능을 통합하여 제공하는 제품을 공급하고 사용자의 애플리케이션 및 시스템에 대한 액세스 제어 및 통합 ID 관리를 지원합니다 .

위험 요인이 현실화되기 전에 예측 , 감시하고 분석하는 광범위한 접근법이 필요합니다 .

기업은 정부 및 업계의 각종 규제 요건을 이행하는 데 각별한 노력을 기울이며 그에 따른 비용 부담도 증가하곤 합니다 . IBM 과 함께 해당 기업의 IT 및 비즈니스 인프라와 규제 요건을 연계할 수 있으며 , 이를 통해 비용을 줄이고 시스템 복잡성을 해소하고 구성을 자동화하고 모니터링 , 감사 , 리포팅을 간소화할 수 있습니다 . IBM 은 신뢰할 수 있는 로깅 및 상관성 기능 그리고 조정 , 분석 및 대시보드 기능을 제공하는 제품을 공급합니다 .

[1] Gartner Newsroom
http://www.gartner.com/it/page.jsp?id=1480514

더 강력한 보안 인텔리전스

기업의 경계에서 방어 체계를 구축하는 것만으로는 비즈니스 환경을 보호할 수 없습니다 . ±Þ³ð 2 에서 보여 주는 IBM 보안 프레임워크의 제품과 서비스를 활용하여 보안 위협을 예측 , 식별 , 해결하고 컴플라이언스를 실현할 수 있습니다 . IBM 은 이러한 목표를 이루기 위해 컴플라이언스 및 보안 서비스와 함께 IT 인프라의 핵심 영역 , 즉 사용자 , 데이터 , 애플리케이션과 인프라를 위한 제품과 서비스를 제공합니다 .

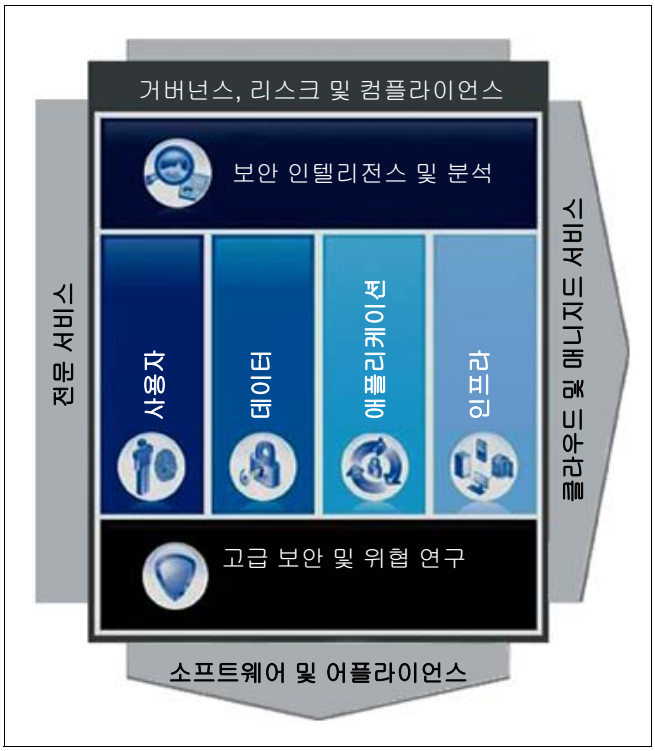

그림 2 IBM 보안 프레임워크

IBM 은 주요 비즈니스 영역을 위한 모든 서비스와 제품을 제공하면서 통합적인 (end-to-end) 보안 인텔리전스를 실현합니다 .

- 사용자. IBM은 다음 제품을 통해 ID 평가, 역할 기반 분석 , 사용자 제어 , 배치 , 호스팅을 위한 서비스를 제공합니다 .
  - IBM Tivoli Identity and Access
  - IBM Tivoli Federated ID
  - IBM Tivoli Single Sign-on
- 데이터. IBM은 다음 제품을 통해 평가, 암호화, 데이터 손실 방지 (DLP) 배치 , 흐름 분석 및 거버넌스를 위한 서비스를 제공합니다 .
  - IBM InfoSphere® Guardium®
  - IBM InfoSphere Optim ? Data Masking
  - 테이프 및 디스크 암호화
  - IBM Tivoli® Key Manager
- 애플리케이션 . IBM은 다음 제품을 통해 평가 , 보안 엔지니어링 프로세스 및 사기 탐지를 위한 서비스를 제공합니다 .
  - IBM Rational® AppScan® Source Edition
  - IBM Rational AppScan Standard Edition
  - IBM Tivoli Security Policy Manager
- 인프라 . IBM은 다음 제품을 통해 네트워크 보안 (침입 탐지 및 차단 , 심층 패킷 검사), 포렌직 , 데이터 마이닝 , 침입 테스트 , 방화벽 , 침입 차단 시스템 , 취약점 관리자 서비스 , 모바일 보호 관리를 위한 서비스를 제공합니다 .
  - IBM Tivoli Network Intrusion Prevention
  - IBM WebSphere® DataPower® XML Gateway
  - IBM Tivoli Endpoint Manager (Trend Micro 의 안티바이러스)
  - IBM Security zSecure™ 메인프레임 보안

다음 단계 : IBM 의 지원

IBM 은 고객의 보안 인텔리전스 구현을 지원하기 위해 상업적 보안 연구 개발 조직 중 세계 최고의 명성을 자랑하는 IBM X-Force® Research & Development 팀의 서비스를 제공합니다 . 이 팀은 취약점 , 악용 , 활성 공격 , 바이러스 , 기타 맬웨어 , 스팸 , 피싱 , 악성 웹 컨텐츠 등을 포함한 최신 보안 위협의 동향을 파악하고 감시합니다 . X-Force 팀은 고객과 일반 대중에게 새로운 보안 위협과 중대한 보안 위협에 대처할 방법을 조언할 뿐 아니라 그러한 위협으로부터 IBM 고객을 보호하기 위한 보안 컨텐츠를 제공합니다 .

X-Force 팀은 연 2 회 IBM X-Force Trend andRisk Report 를 발행하며 , 이는 고객 , 전문가와 일반 대중이 최신 보안 위험을 이해하고 새로운 위협에 대비하는 데 큰 도움이 되고 있습니다 . 이 보고서는 현재 보안 전문가들에게 주어진 중대한 보안과제를 철저히 탐구합니다 . IBM X-Force Trend and Risk Report 는 다음 사이트에서 이용할 수 있습니다 .

http://www.ibm.com/security/xforce/downloads.html

IBM 은 IBM X-Force 팀의 서비스와 함께 각종 제품과 서비스를 통해 고객의 데이터 , 애플리케이션 , 인프라를 공격으로부터 보호하고 정보 자산을 지키고 사용자에게 안전한 액세스를 지원하기 위한 전 범위의 솔루션을 제공합니다 .

추가 정보 자료

이 문서에서 주로 다룬 개념에 대한 자세한 내용은 다음 자료를 참조하십시오 .

- IBM Redbooks 에서 발행하는 보안 관련 자료

  http://www.redbooks.ibm.com/Redbooks.nsf/portals/Security?Open&count=20

- IBM X-Force Trend and Risk Report

  http://www.ibm.com/security/xforce/downloads.html

- IBM Institute for Advanced Security

  http://instituteforadvancedsecurity.com/default.aspx

- *Security in Development: The IBM Secure Engineering Framework*, REDP-4641

  http://www.redbooks.ibm.com/redpapers/pdfs/redp4641.pdf

주의사항

이 정보는 미국에서 제공되는 제품과 서비스를 대상으로 개발된 것입니다 .

IBM 은 이 문서에서 언급된 제품 , 서비스 또는 기능을 다른 국가에서 제공하지 않을 수도 있습니다 . 한국에서 사용 가능한 제품 및 서비스에 대해서는 한국 IBM 담당자에게 문의하십시오 . IBM 제품 , 프로그램 또는 서비스를 언급했다고 해서 해당 IBM 제품 , 프로그램 또는 서비스만을 사용할 수 있다는 것을 의미하지는 않습니다 . IBM 의 지적 재산권을 침해하지 않고 기능상 동등한 제품 , 프로그램 또는 서비스를 대신 사용할 수 있습니다 . 그러나 비 IBM 제품 , 프로그램 또는 서비스의 운영에 대한 평가 및 검증은 사용자의 책임입니다 .

IBM 은 이 문서에서 다루고 있는 특정 내용에 대해 특허를 보유하고 있거나 현재 특허 출원 중일 수 있습니다 . 이 문서를 제공한다고 해서 특허에 대한 라이센스까지 부여하는 것은 아닙니다 . 라이센스에 대한 의문사항은 다음으로 문의하십시오 .
135-700 서울특별시 강남구 도곡동 467-12 군인공제회관빌딩 한국 아이 . 비 . 엠 주식회사

다음 단락은 현지법과 상충하는 영국이나 기타 국가에서는 적용되지 않습니다 .
INTERNATIONAL BUSINESS MACHINES CORPORATION 은 타인의 권리 비침해 , 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여 (단 , 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증 없이 이 발행물을 현상태대로 제공합니다 . 일부 국가에서는 특정 거래에서 명시적 또는 묵시적 보증의 면책사항을 허용하지 않으므로 , 이 사항이 적용되지 않을 수도 있습니다 .

이 정보에는 기술적으로 부정확한 내용이나 인쇄상의 오류가 있을 수 있습니다 . 이 정보는 주기적으로 변경되며 , 변경된 사항은 최신판에 통합됩니다 . IBM 은 이 발행물에서 설명한 제품 및 / 또는 프로그램을 사전 통지 없이 언제든지 개선 및 / 또는 변경할 수 있습니다 .

이 정보에서 언급되는 비 IBM 의 웹 사이트는 단지 편의상 제공된 것으로 , 어떤 방식으로든 이들 웹 사이트를 옹호하고자 하는 것은 아닙니다 . 해당 웹 사이트의 자료는 본 IBM 제품 자료의 일부가 아니므로 해당 웹 사이트 사용으로 인한 위험은 사용자 본인이 감수해야 합니다 .

IBM 은 귀하의 권리를 침해하지 않는 범위 내에서 적절하다고 생각하는 방식으로 귀하가 제공한 정보를 사용하거나 배포할 수 있습니다 .

비 IBM 제품에 관한 정보는 해당 제품의 공급업체 , 공개 자료 또는 기타 범용 소스로부터 얻은 것입니다 . IBM 에서는 이러한 제품들을 테스트하지 않았으므로 , 비 IBM 제품과 관련된 성능 , 호환성 , 기타 주장의 정확성을 확신할 수 없습니다 . 비 IBM 제품의 성능에 대한 의문사항은 해당 제품의 공급업체에 문의하십시오 .

이 정보에는 일상의 비즈니스 운영에서 사용되는 자료 및 보고서에 대한 예제가 들어 있습니다 . 이들 예제에는 개념을 가능한 완벽하게 설명하기 위하여 개인 , 회사 , 상표 및 제품의 이름이 사용될 수 있습니다 . 이들 이름은 모두 가공의 것이며 실제 기업의 이름 및 주소와 유사하더라도 이는 전적으로 우연입니다 .

본 문서에 포함된 모든 성능 데이터는 제한된 환경에서 산출된 것입니다 . 따라서 다른 운영 환경에서 얻어진 결과는 상당히 다를 수 있습니다 . 일부 성능은 개발 단계의 시스템에서 측정되었을 수 있으므로 이러한 측정치가 일반적으로 사용되고 있는 시스템에서도 동일하게 나타날 것이라고는 보증할 수 없습니다 . 또한 일부 성능은 추정을 통해 추측되었을 수도 있으므로 실제 결과는 달라질 수 있습니다 . 이 문서의 사용자는 해당 데이터를 본인의 특정 환경에서 검증해야 합니다 .

저작권 라이센스 :

이 정보에는 여러 운영 플랫폼에서의 프로그래밍 기법을 보여주는 원어로 된 샘플 응용프로그램이 들어 있습니다 . 귀하는 이러한 샘플 프로그램의 작성 기준이 된 운영 플랫폼의 응용프로그램 프로그래밍 인터페이스 (API) 에 부합하는 응용프로그램을 개발 , 사용 , 판매 또는 배포할 목적으로 추가 비용 없이 이들 샘플 프로그램을 어떠한 형태로든 복사 , 수정 및 배포할 수 있습니다 . 이러한 샘플 프로그램은 모든 조건하에서 완전히 테스트된 것은 아닙니다 . 따라서 IBM 은 이들 샘플 프로그램의 신뢰성 , 서비스 가능성 또는 기능을 보증하거나 진술하지 않습니다 .

이 REDP-4944-00 문서는 11 21, 2013 에 작성되거나 업데이트되었습니다 .

상표

IBM, IBM 로고 , ibm.com 은 미국 또는 기타 국가에서 사용되는 International Business Machines Corporation 의 상표 또는 등록 상표입니다 . 이와 함께 기타 IBM 상표가 기재된 용어가 상표 기호 (® 또는 ™) 와 함께 이 정보에 처음 표시된 경우 , 이와 같은 기호는 이 정보를 발행할 때 미국에서 IBM 이 소유한 등록상표 또는 일반 법적 상표입니다 . 또한 이러한 상표는 기타 국가에서 등록상표 또는 일반 법적 상표입니다 . 현재 IBM 상표 목록은 다음 사이트에 있습니다 . **ibm.com**/legal/copytrade.shtml

다음 용어는 미국 또는 기타 국가에서 사용되는 International BusinessMachines Corporation 의 상표입니다 .

AppScan®
DataPower®
Guardium®
IBM®
InfoSphere®
Optim™
Rational®
Redbooks®
Redbooks(logo)
Tivoli®
WebSphere®
X-Force®
zSecure™

다음 용어는 타사의 상표입니다 .

기타 회사 , 제품 및 서비스 이름은 타사의 상표 또는 서비스표입니다 .