

BASIC OF SECURITY



목차



해시



전자서명



코드서명

발표일 2018 - 12 - 21

1. 해시

- 1) 성질
- 2) 이용 예
- 3) 충돌

2. 전자서명

- 1) 정의
- 2) 보통 서명과 전자서명의 대응
- 3) 주로 사용되는 전자서명 방식
- 4) 구조

- CONTENTS

- HASH

- Digital Signature

- Code Signing

- Reference

- Thank you



목차



해시



전자서명



코드서명

발표일 2018 - 12 - 21

1. 해시

- 1) 성질
- 2) 이용 예
- 3) 충돌

2. 전자서명

- 1) 정의
- 2) 보통 서명과 전자서명의 대응
- 3) 주로 사용되는 전자서명 방식
- 4) 구조

해시(HASH)

- CONTENTS

- HASH

- Digital Signature

- Code Signing

- Reference

- Thank you



목차



해시



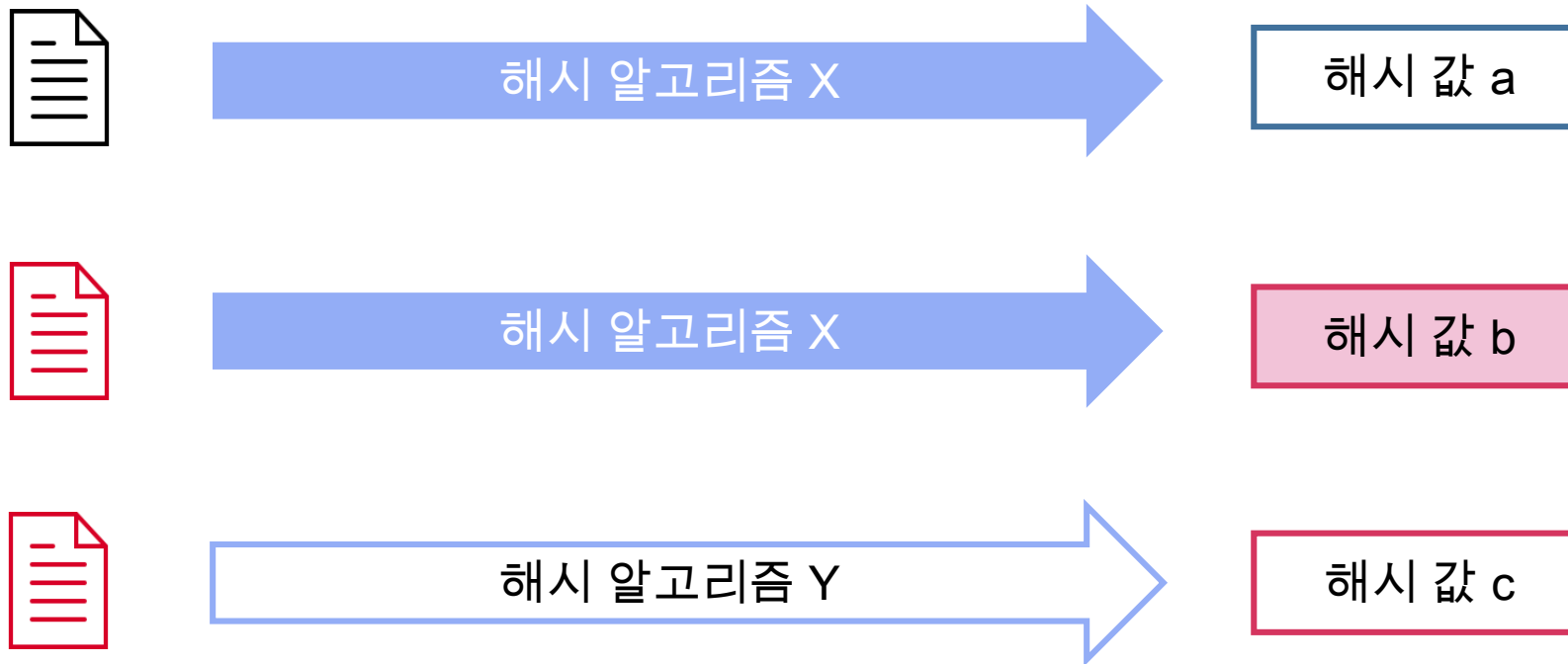
전자서명



코드서명

해시(HASH)

- 해시 : 어떤 데이터에 대응하는 값을 구하기 위한 방법
- 성질 : 동일한 데이터로부터 항상 동일한 해시 값 생성



- CONTENTS

- HASH

- Digital Signature

- Code Signing

- Reference

- Thank you



목차



해시



전자서명




코드서명

발표일 2018 - 12 - 21

해시(HASH)

1. 데이터가 변조되지 않았다는 것을 확인




 배포원의 파일

해시 알고리즘 X

해시 값 a



 입수한 파일

해시 알고리즘 X

해시 값 a

2. 데이터 변조를 검출



 입수한 파일

해시 알고리즘 X

해시 값 b

- CONTENTS

- HASH

- Digital Signature

- Code Signing

- Reference

- Thank you



목차



해시



전자서명

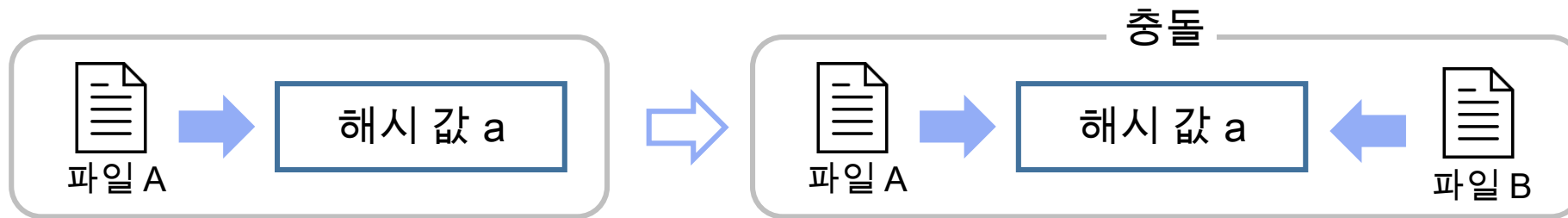


코드서명

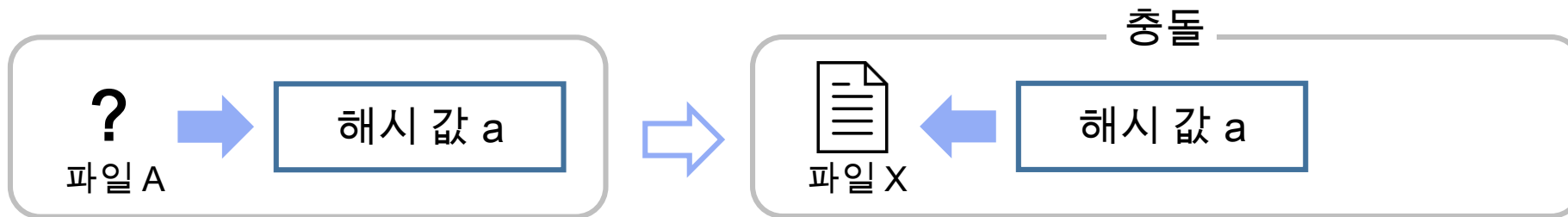
발표일 2018 - 12 - 21

충돌

1. 서로 다른 파일로부터 동일한 해시 값이 생성되어 버리는 경우



2. 해시 값으로부터 그 해시 값을 생성하는 파일을 만들 수 있는 경우



- CONTENTS

- HASH

- Digital Signature

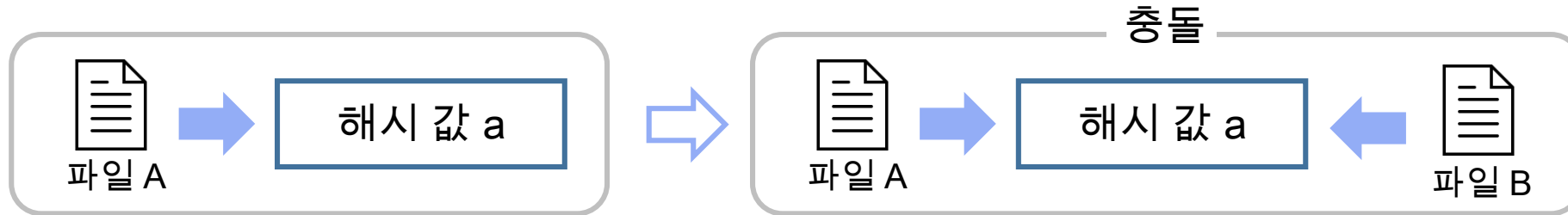
- Code Signing

- Reference

- Thank you

충돌

1. 서로 다른 파일로부터 동일한 해시 값이 생성되어 버리는 경우



2. 해시 값으로부터 그 해시 값을 생성하는 파일을 만들 수 있는 경우



- CONTENTS

- HASH

- Digital Signature

- Code Signing

- Reference

- Thank you



목차



해시



전자서명



코드서명

발표일 2018 - 12 - 21

- 전자서명 : 전자 데이터의 작성자를 원래의 데이터에 부여하여
원래의 데이터가 변조되지 않았다는 것을 보증하기 위한

기술

→ 현실 사회에서 '서류에 하는 사인', '날인' 등을 전자적으로 구

현



- CONTENTS

- HASH

- Digital Signature

- Code Signing

- Reference

- Thank you



목차



해시



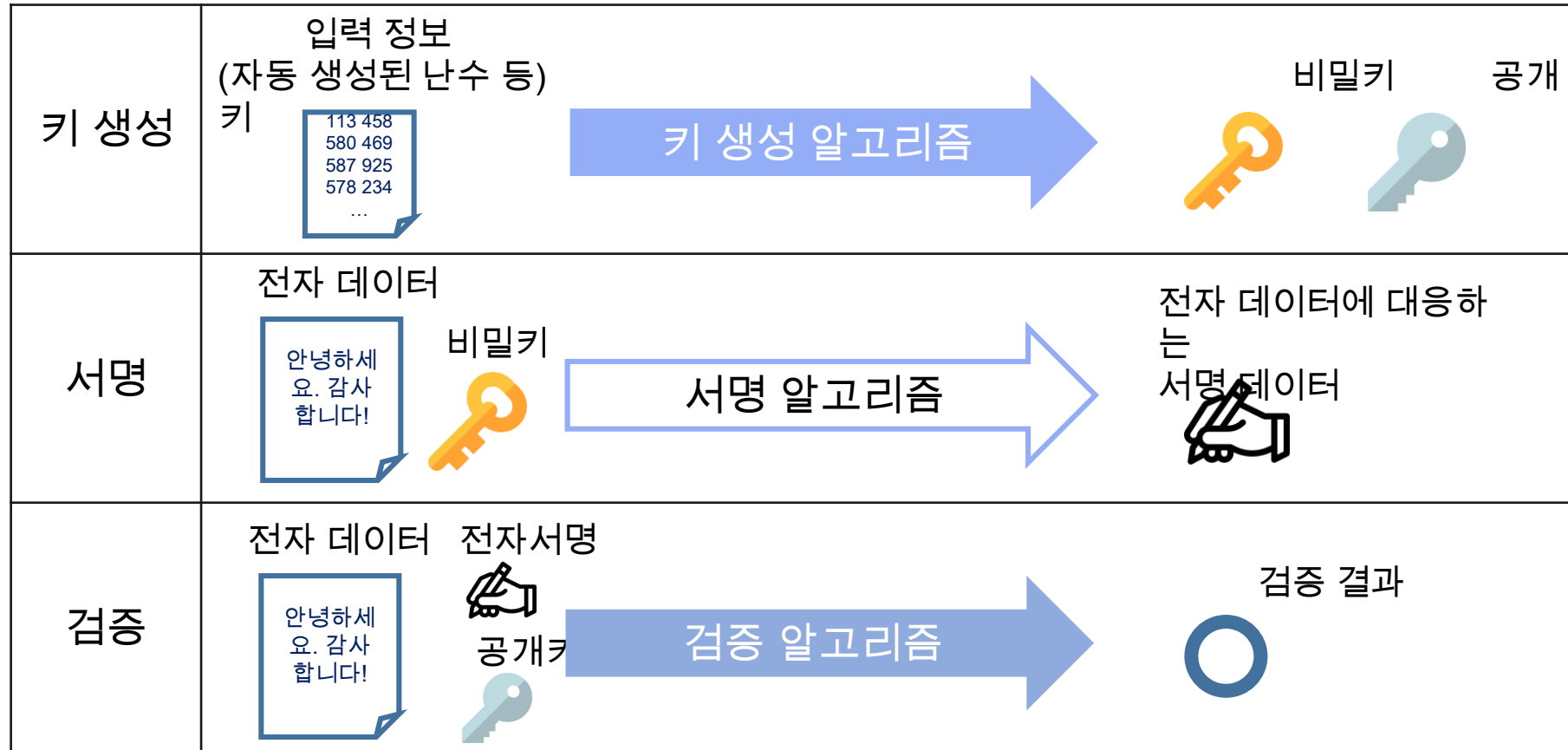
전자서명



코드서명

발표일 2018 - 12 - 21

• 전자서명을 구현하는 세 가지 알고리즘



- CONTENTS

- HASH

- Digital Signature

- Code Signing

- Reference

- Thank you

- 주로 사용되는 전자서명 방식

전자서명 방식	개요
RSA	<ul style="list-style-type: none">- 3명의 개발자의 머릿글자를 따서 명명- 1977년에 발명된 공개키 암호방식- 전자서명을 위해서도 사용
ElGamal	<ul style="list-style-type: none">- 개발자의 이름에 의해 명명- 1984년에 발표- 풀기가 힘든 숫자 문제 중 하나를 암호에 응용
DSA	<ul style="list-style-type: none">- Digital Signature Algorithm의 약자- 1993년에 표준화- ElGamal을 바탕으로 풀기가 힘든 다른 문제를 조합하여 암호에 응용

- CONTENTS

- HASH

- Digital Signature

- Code Signing

- Reference

- Thank you



목차



해시



전자서명



코드서명

- 주로 사용되는 전자서명 방식

구축명	개요
PGP	<ul style="list-style-type: none">- 상용화는 Symantec, 오픈 소스 구축은 GnuPG로 알려짐- 키의 생성은 이용자가 수행- 공개키 서버 인프라는 있으나 사용하지 않아도 무방- 소규모 도입
S/MIME	<ul style="list-style-type: none">- 메일에 대한 암호화 전자서명을 위해 사용- 주요 메일 소프트웨어는 S/MIME 지원- 이용을 위해서는 인증국이 발행하는 전자인증서 필요- 조직적인 도입
PDF 서명	<ul style="list-style-type: none">- PDF에 대한 전자서명- Adobe Acrobat에 구축- 이용을 위해서는 인증국이 발행하는 전자인증서 필요

- CONTENTS

- HASH

- Digital Signature

- Code Signing

- Reference

- Thank you



목차



해시



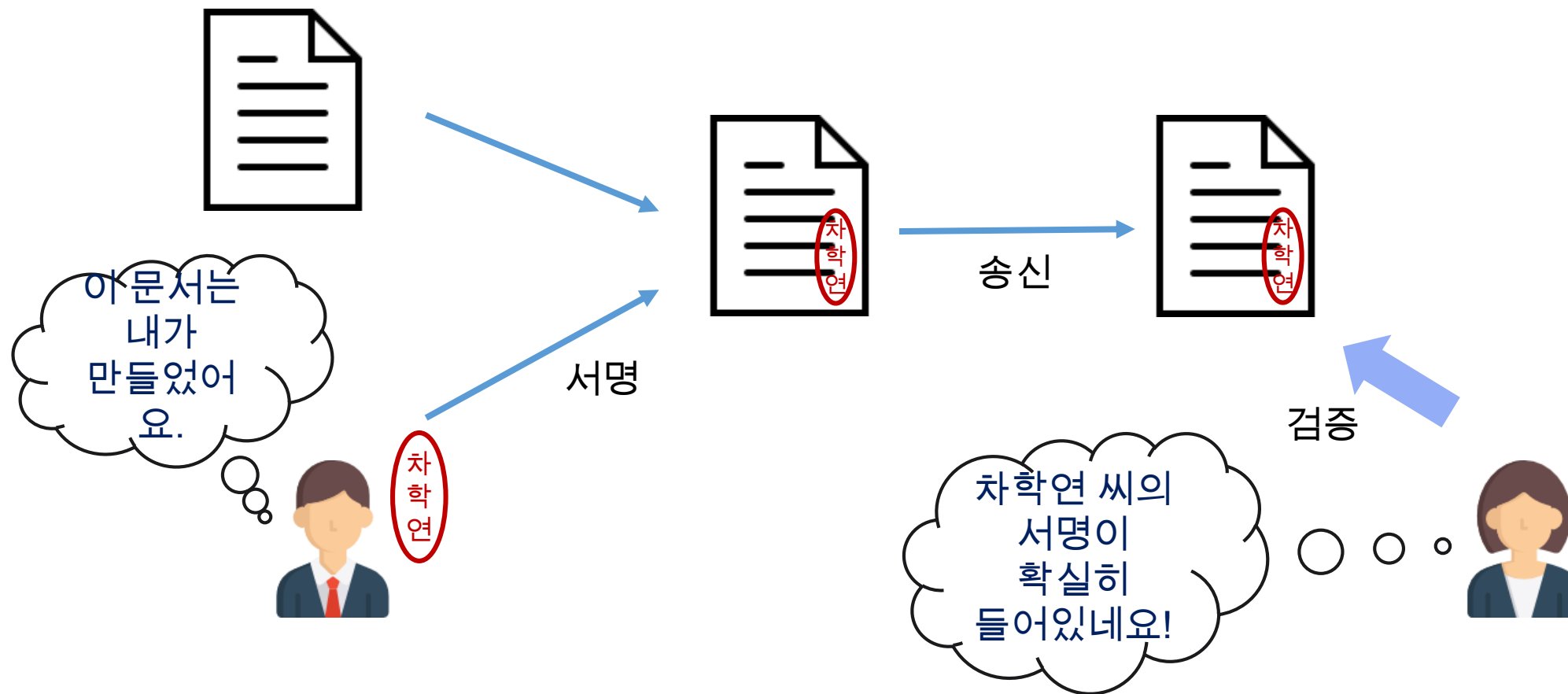
전자서명



코드서명

발표일 2018 - 12 - 21

구조



- CONTENTS

- HASH

- Digital Signature

- Code Signing

- Reference

- Thank you



목차



해시



전자서명



코드서명

발표일 2018 - 12 - 21

Miyamoto Kunio / Okubo Takao, <<보안의 기본>>, 위즈플래닛, 2018, 38-39, 52-53, 144-145.

02	감지, 차단 대응, 복구, 사후 대응 보안 사고 대응의 4단계	32
03	상대를 올바르게 인식하고 상대에 따라 올바른 권한을 부여하는 장치 인증과 인가	34
04	계산자로부터 정보를 보호하기 위한 장치 암호	36
05	데이터 변조를 체크한다 해시	38
06	기본적이고 확실한 대책을 거듭하여 보안을 굳건하게 한다 하드닝	40
07	옛날부터 사용되는 인증 방법이지만 돌려쓰기는 금물 비밀번호	42
08	생체가 갖고 있는 특징을 인증에 응용한다 바이오메트릭스 인증	44
09	한 번만 사용 가능한 비밀번호 원타임 비밀번호	46
10	성질이 다른 두 종류의 정보를 조합한 인증 이중 인증	48
11	한 번의 인증으로 여러 시스템의 이용 권한을 설정 싱글 사인온	50
12	전자 데이터가 변조되지 않았다는 것을 보증하는 기술 전자서명과 그 응용 예	52
13	자신이 맞는 존재라는 것을 나타내기 위한 장치 인증서와 인증국	54
14	다른 사람으로부터 데이터를 보호하는 방법 암호화 파일 시스템	56

- CONTENTS

- HASH

- Digital Signature

- Code Signing

- Reference

- Thank you



목차



해시



전자서명



코드서명

발표일 2018 - 12 - 21

THANK YOU

LEE JEONG HYEON



목차



해시



전자서명



코드서명

발표일 2018 - 12 - 21