FPRI
Future Policy Research Institute

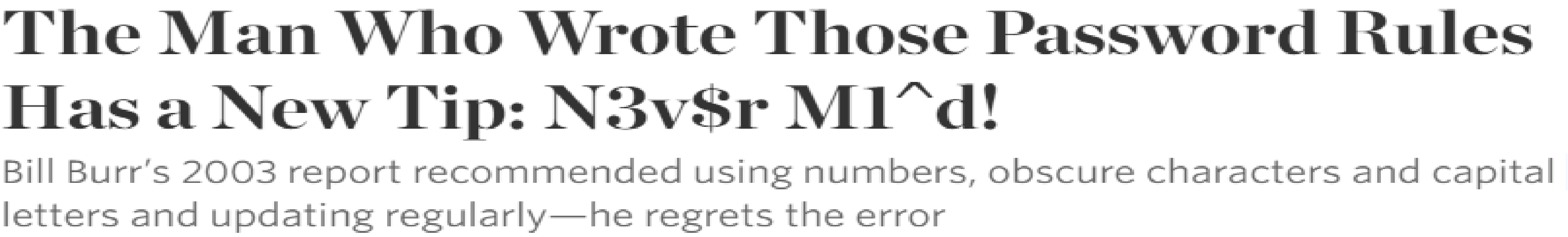
"PASSWORD"

- 비밀번호 보안 정책에 대한 미신과 진실_V1.0 -
(The Myth and Truth about Password Security Policy)

2017.08.28

Jason, Min

[발단] `17.8.7일자 WSJ 뉴스기사



The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1^d!

Bill Burr's 2003 report recommended using numbers, obscure characters and capital letters and updating regularly—he regrets the error

The Man Who Wrote Those Password Rules Has a New Tip:...

Bill Burr's 2003 report recommended using numbers, obscure chara...

www.wsj.com

2003년
"NIST Special Publication 800-63" 에서
"문자, 숫자, 특수문자로 조합(3종)된 패스워드의 이용 및 주기적(90일) 변경" 권고함

⇩

2003년 당시 "NIST Special Publication 800-63"의 저자인 Bill Burr가 제시한
"문자, 숫자, 특수문자로 조합된 패스워드의 이용 및 주기적 변경" 권고가 **잘못된 것이라고 인정**하였음

2017년 6월 가이드 전면 개편됨 (기존 규칙 폐기)

https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118?mod=e2fb

[발단] `17.8.7일자 WSJ 뉴스기사 – 내용요약

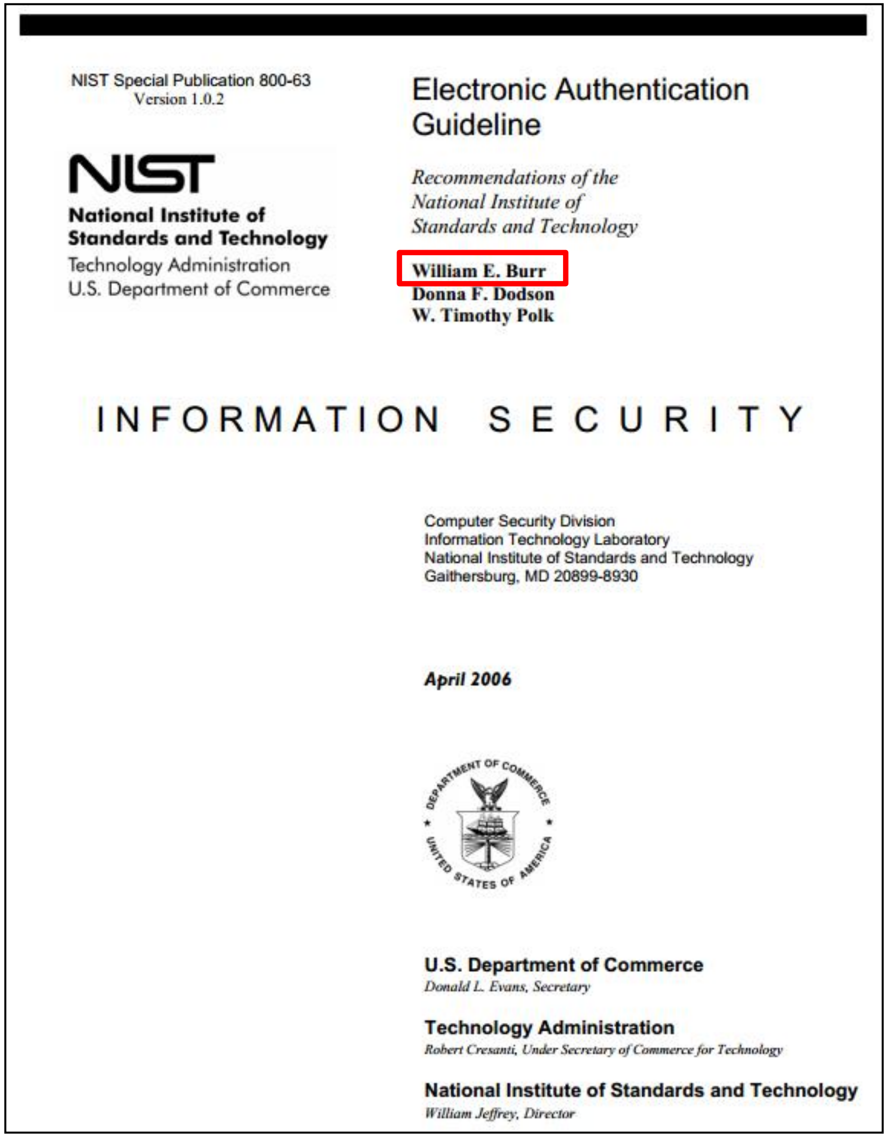
2003년 작성 당시 "문자, 숫자, 특수문자로 조합(3종)된 패스워드의 이용 및 주기적(90일) 변경" 권고함,

72세의 은퇴한 Burr 씨는 "나는 지금 내가 한 일을 많이 후회한다. " 고 말함

2017년 6월에 특별 간행물 800-63은 철저히 재 작성하였음, 최악의 암호 기준을 폐기함(Mr. Grassi)

(변경된 기준) 길고 기억하기 쉬운 문구를 이용하고 도난당한 흔적이있는 경우에만 암호를 변경할것

“correct horse battery staple“	“Tr0ub4dor&3”
크랙 550 년 걸림	Burr의 기존 규칙을 사용한 암호의 전형적인 예 크랙 3일 걸림



NIST Special Publication 800-63
Version 1.0.2

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Electronic Authentication Guideline

Recommendations of the National Institute of Standards and Technology

William E. Burr
Donna F. Dodson
W. Timothy Polk

INFORMATION SECURITY

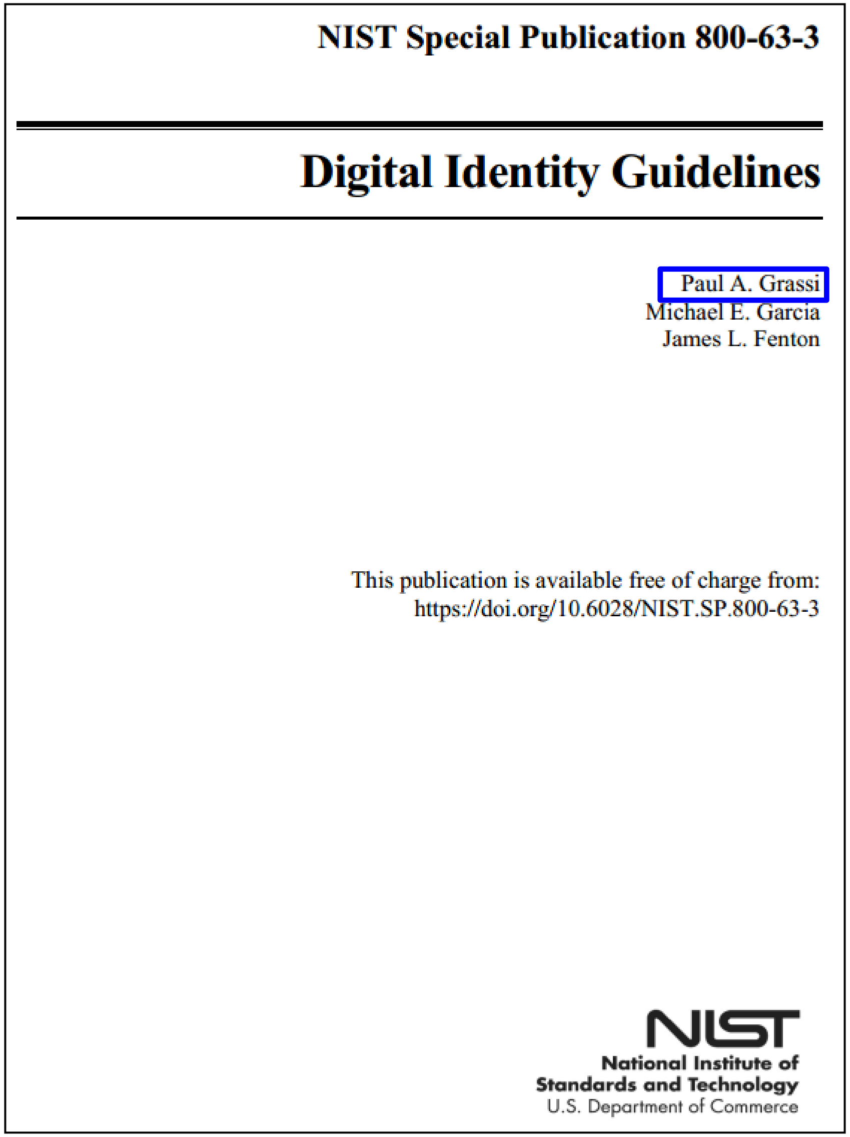
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

April 2006

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Robert Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
William Jeffrey, Director



NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
James L. Fenton

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

[엔트로피 계산]

3종 8자리의 경우 94^8=6.9*10^15, 즉 2^52, 52bit 엔트로피를 가짐
* 계산은 94 printable ISO character 기준으로 함

=> 25 GPU(2000만원 장비)의 경우 크래킹 2시간 이내 가능
2 GPU(200만원)의 경우 24시간 이내 가능함

즉 현재의 기준은 큰 의미가 없어 시급한 개선이 필요함

[고찰] NIST기준 고찰

□ DB의 유출에 따른 암호 크래킹을 주로 고려하였음

☞ 입력 시 키로킹은 이용자 스스로 보호(백신 등)

☞ <u>저장 시 보안은 유출에 대비하여 크래킹(해시충돌) 강도 계산 -> NIST</u>

□ 개선기준 검토

☞ NIST가 제안하는 개선방안인 쉬운 긴 문자열 이용방식은
이용은 가능할 수 있으나, 더 나은 방안의 제시가 가능한 부분이 있음

[PRRI Result]

□ 현 암호기준은 오류가 있으므로 개선이 필요함

☞ 현 개별 회사에 기 적용된 기준 개선 추진

☞ 현 법제도 개선 필요
해설서 등에 남아있는 2종 10자, 3종 8자 제한에 대한 개선시급

□ 대안 제시

☞ **입력 시 오류카운트 제한 (5회 등)**
5회오류 체크시, 일반적으로는 6자, 기기지정시 4자 정도로 이용가능

☞ **저장 시 보안 : 유출에 대비하여 크래킹(해시충돌) 강도 계산 필요인정**
강도의 강화를 위해 입력자리 수를 길게 할 필요는 없음
저장시 암호화방법 적용을 잘 하면 됨
예시 : 입력값 6자리 (abc123),
저장시 Hash2(Hash1(abc123+A))
* A : 고객정보로부터 유도된 정보 또는 연산시 이용되는 값
(영문,숫자,특수문자 등이 포함된 20여자리)

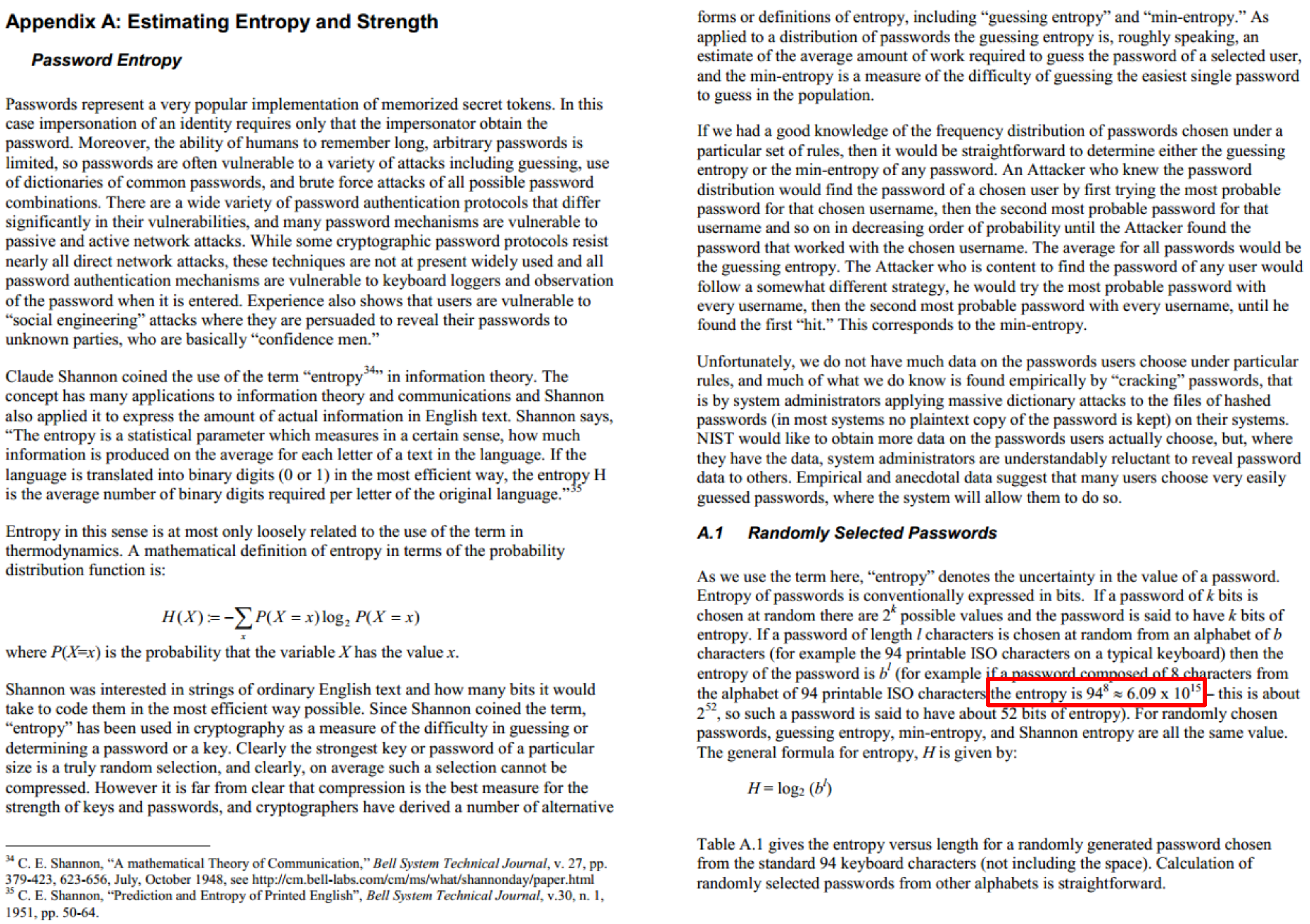
[관련링크]
https://www.consumerreports.org/digital-security/everything-you-need-to-know-about-password-managers/
(암호를 너무 자주 변경하지 마십시오. 암호를 쉽고 간단하게 작성해야하기 때문, 긴 단어의 무작위 단어가 좋음)

RFC 1244 in 1991 by Holbrook and Reynolds

PGP's Passphrase FAQ in 1993:
"Even relatively short phrases offer acceptable entropy because the far larger "alphabet" pool of word symbols that may be chosen than the 26 characters that form the Roman alphabet. Even choosing from a vocabulary of a few thousand words a five word phrase might have on the order of 58 to 60 bits of entropy -- more than what is needed for the DES algorithm, for example."

5.5 시간 안에 25 개의 GPU가 8자 조합(글자, 숫자 및 기호) 크래킹 (2012년)
https://arstechnica.com/information-technology/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/
그리고 그것은 2012 년에있었습니다! GPU 기술은 NVIDIA GTX 1080이 이전 제품보다 거의 두 배나 많은 시도를 할 수있는 아래 기사에서 볼 수 있듯이 그 이후로 적어도 두 배가되었습니다.
https://www.digitaltrends.com/computing/nvidia-gtx-1080-crack-passwords/

[과거 NIST 기준]



Appendix A: Estimating Entropy and Strength

Password Entropy

Passwords represent a very popular implementation of memorized secret tokens. In this case impersonation of an identity requires only that the impersonator obtain the password. Moreover, the ability of humans to remember long, arbitrary passwords is limited, so passwords are often vulnerable to a variety of attacks including guessing, use of dictionaries of common passwords, and brute force attacks of all possible password combinations. There are a wide variety of password authentication protocols that differ significantly in their vulnerabilities, and many password mechanisms are vulnerable to passive and active network attacks. While some cryptographic password protocols resist nearly all direct network attacks, these techniques are not at present widely used and all password authentication mechanisms are vulnerable to keyboard loggers and observation of the password when it is entered. Experience also shows that users are vulnerable to "social engineering" attacks where they are persuaded to reveal their passwords to unknown parties, who are basically "confidence men."

Claude Shannon coined the use of the term "entropy[34]" in information theory. The concept has many applications to information theory and communications and Shannon also applied it to express the amount of actual information in English text. Shannon says, "The entropy is a statistical parameter which measures in a certain sense, how much information is produced on the average for each letter of a text in the language. If the language is translated into binary digits (0 or 1) in the most efficient way, the entropy H is the average number of binary digits required per letter of the original language."[35]

Entropy in this sense is at most only loosely related to the use of the term in thermodynamics. A mathematical definition of entropy in terms of the probability distribution function is:

$$H(X) := -\sum_{x} P(X=x)\log_2 P(X=x)$$

where $P(X{=}x)$ is the probability that the variable X has the value x.

Shannon was interested in strings of ordinary English text and how many bits it would take to code them in the most efficient way possible. Since Shannon coined the term, "entropy" has been used in cryptography as a measure of the difficulty in guessing or determining a password or a key. Clearly the strongest key or password of a particular size is a truly random selection, and clearly, on average such a selection cannot be compressed. However it is far from clear that compression is the best measure for the strength of keys and passwords, and cryptographers have derived a number of alternative forms or definitions of entropy, including "guessing entropy" and "min-entropy." As applied to a distribution of passwords the guessing entropy is, roughly speaking, an estimate of the average amount of work required to guess the password of a selected user, and the min-entropy is a measure of the difficulty of guessing the easiest single password to guess in the population.

If we had a good knowledge of the frequency distribution of passwords chosen under a particular set of rules, then it would be straightforward to determine either the guessing entropy or the min-entropy of any password. An Attacker who knew the password distribution would find the password of a chosen user by first trying the most probable password for that chosen username, then the second most probable password for that username and so on in decreasing order of probability until the Attacker found the password that worked with the chosen username. The average for all passwords would be the guessing entropy. The Attacker who is content to find the password of any user would follow a somewhat different strategy, he would try the most probable password with every username, then the second most probable password with every username, until he found the first "hit." This corresponds to the min-entropy.

Unfortunately, we do not have much data on the passwords users choose under particular rules, and much of what we do know is found empirically by "cracking" passwords, that is by system administrators applying massive dictionary attacks to the files of hashed passwords (in most systems no plaintext copy of the password is kept) on their systems. NIST would like to obtain more data on the passwords users actually choose, but, where they have the data, system administrators are understandably reluctant to reveal password data to others. Empirical and anecdotal data suggest that many users choose very easily guessed passwords, where the system will allow them to do so.

A.1 *Randomly Selected Passwords*

As we use the term here, "entropy" denotes the uncertainty in the value of a password. Entropy of passwords is conventionally expressed in bits. If a password of k bits is chosen at random there are 2^k possible values and the password is said to have k bits of entropy. If a password of length l characters is chosen at random from an alphabet of b characters (for example the 94 printable ISO characters on a typical keyboard) then the entropy of the password is b^l (for example if a password composed of 8 characters from the alphabet of 94 printable ISO characters the entropy is $94^8 \approx 6.09 \times 10^{15}$ – this is about 2^{52}, so such a password is said to have about 52 bits of entropy). For randomly chosen passwords, guessing entropy, min-entropy, and Shannon entropy are all the same value. The general formula for entropy, H is given by:

$$H = \log_2 (b^l)$$

Table A.1 gives the entropy versus length for a randomly generated password chosen from the standard 94 keyboard characters (not including the space). Calculation of randomly selected passwords from other alphabets is straightforward.

[34] C. E. Shannon, "A mathematical Theory of Communication," *Bell System Technical Journal*, v. 27, pp. 379-423, 623-656, July, October 1948, see http://cm.bell-labs.com/cm/ms/what/shannonday/paper.html

[35] C. E. Shannon, "Prediction and Entropy of Printed English", *Bell System Technical Journal*, v.30, n. 1, 1951, pp. 50-64.

“만약 당신이 미래를 꿈꾸지 않거나 지금 기술개선을 위해 노력하지 않는다면 그건 곧 낙오되고 있는 것이나 마찬가지 입니다.”

그윈 쇼트웰(Gwynne Shtwell, SpaceX CEO, COO)

감사합니다

(facebook.com/sangshik, mikado22001@yahoo.co.kr)

FPRI

Future Policy Research Institute