セキュリティ&プライバシーに関する諸問題と標準化の必要性
-Background of Internet Society-

株式会社レピダム
林 達也 (@lef)
HAYASHI, Tatsuya / Lepidum Co. Ltd.

インターネット社会の裏側を知る講習会
(2018/8/31)

lepidum
https://lepidum.co.jp/


QUIC


http2


TLS


BASE
ALLIANCE


Cyber Security Research Center


OAUTH
2
OAUTH


Blockchain Lab


BSafe
network


IETF


W3C


CCS

CELLOS

Cryptographic protocol Evaluation toward
Long-Lived Outstanding Security

林 達也 (@lef)

所属

- 株式会社レピダム 代表取締役
  - ココン株式会社 取締役 / 最高技術責任者
  - 株式会社イエラエセキュリティ
- パロンゴ合同会社 最高技術責任者
- OpenID ファウンデーション ジャパン 理事
- Identity Conference (#idcon) オーガナイザー
- 暗号プロトコル評価技術 コンソーシアム(CELLOS) 理事
- 慶應義塾大学大学院メディア デザイン研究科 後期博士課程
- 慶應義塾大学KMD研究所 所員
  - サイバーセキュリティ研究センター
- 慶應義塾大学SFC研究所 所員
  - ブロックチェーンラボ
- ISO/TC 307 Blockchain and distributed ledger technologies 国内委員会委員
- Virtual Currency Governance Task Force (VCGTF)

林 達也 (@lef)

所属

- 株式会社レピダム 代表取締役
  - ココン株式会社 取締役 / 最高技術責任者
  - 株式会社イエラエセキュリティ
- パロンゴ合同会社 最高技術責任者
- OpenID ファウンデーション ジャパン 理事
- Identity Conference (#idcon) オーガナイザー
- 暗号プロトコル評価技術 コンソーシアム(CELLOS) 理事
- 慶應義塾大学大学院メディア デザイン研究科 後期博士課程
- 慶應義塾大学KMD研究所 所員
  - サイバーセキュリティ研究センター
- 慶應義塾大学SFC研究所 所員
  - ブロックチェーンラボ
- ISO/TC 307 Blockchain and distributed ledger technologies 国内委員会委員
- Virtual Currency Governance Task Force (VCGTF)

■講師プロフィール（敬称略）

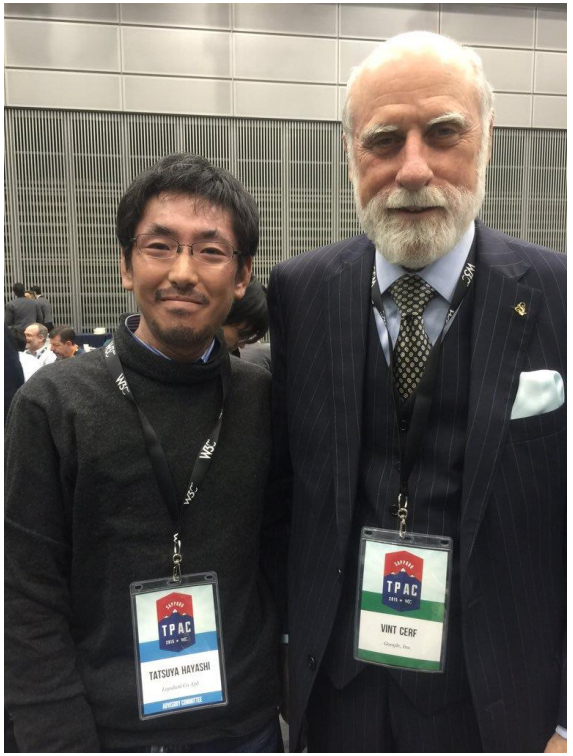
- 根本貴弘
  青山学院大学附置情報メディアセンター 助手。慶應義塾大学にて博士（メディアデザイン学）取得。母語と環境情報を活用した情報システムの研究、キャンパスネットワークの企画運用及びその利活用に係る研究に従事。2011年よりIETFにおける国際化標準化活動にも参加。RFC 7790共著者。2016年よりISOC-JP IETF Education Working Group Chairとして、IETF edu teamと連携しIETF会合のチュートリアル資料の日本語化を行い、国内コミュニティに提供する活動も行っている。

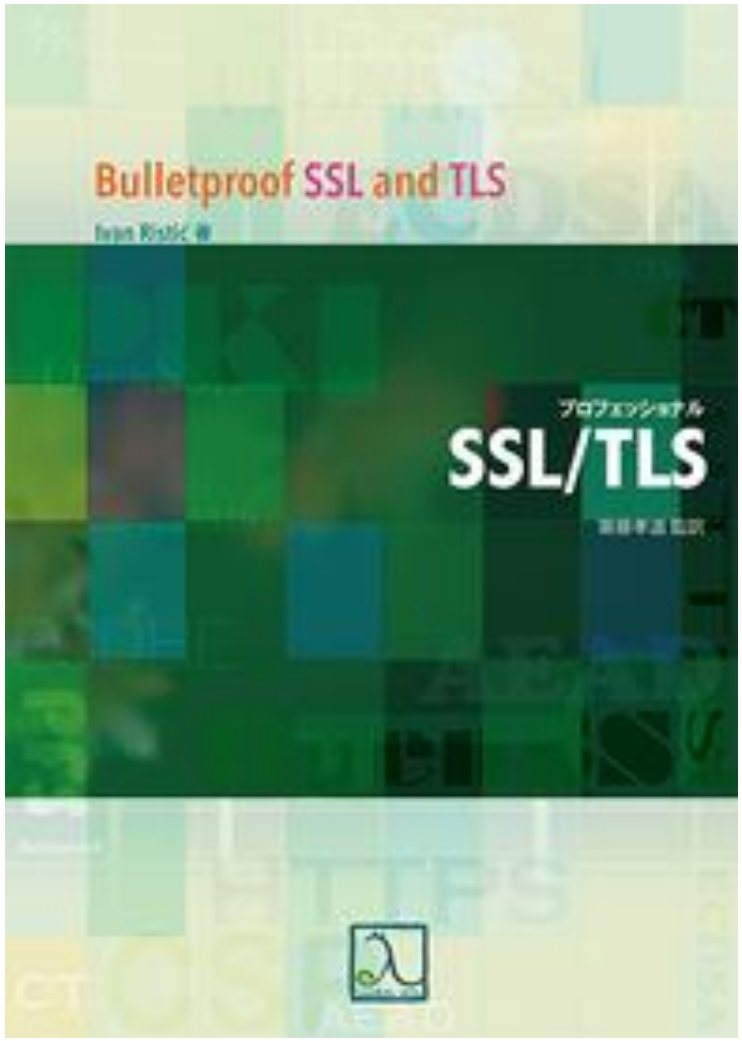
- 小川晃通
  技術系ブログ「Geekなページ」管理人。慶應義塾大学にて博士（政策・メディア）取得。
  著書に『プロフェッショナルIPv6』（ラムダノート社）、『インターネットのカタチ』『マスタリング TCP/IP OpenFlow 編』（オーム社）、『アカマイ 知られざるインターネットの巨人』（KADOKAWAメディアファクトリー）、『ポートとソケットがわかればインターネットがわかる』（技術評論社）など。

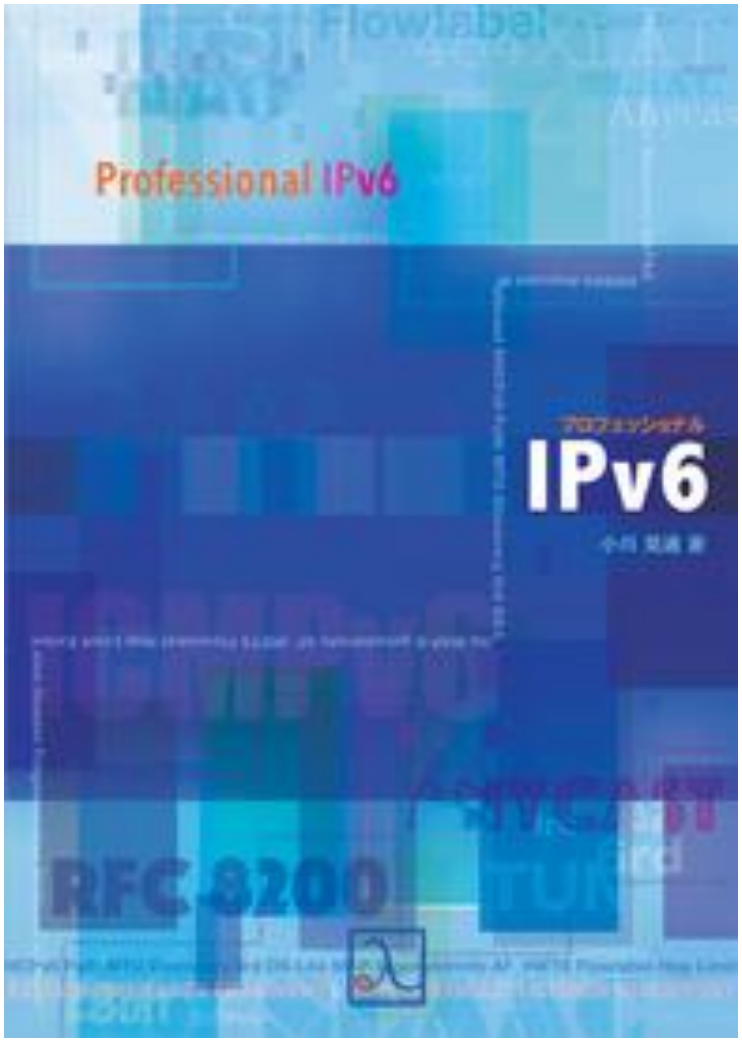
- 林達也
  株式会社レピダム 代表取締役。エンジニア、コンサルタントを経て、2004年、株式会社レピダムを

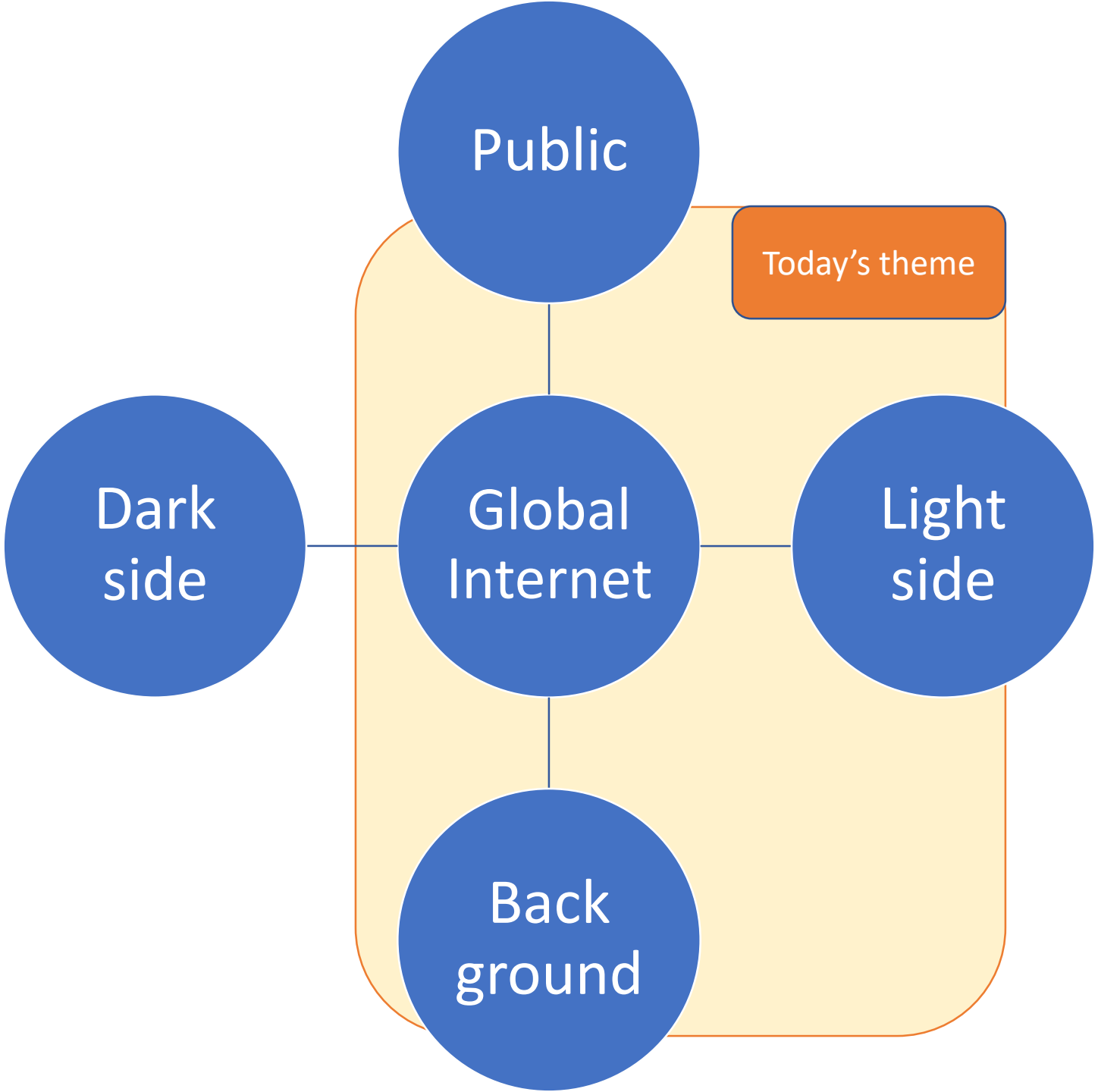
業務領域

- 標準化支援
  - IETF, W3C, ISO, ITU-T, etc...
- 政策支援
  - 総務省、経産省、 etc...
- Identity関連業務
  - Personal Data, Privacy, Identity, AuthN/Z
- Internet関連業務
  - セキュアプロトコル, システム設計・評価
- セキュリティ関連業務
  - システム設計、セキュアプロトコル、形式検証、ソフトウェア脆弱性
- 研究開発・プロトタイピング
- 各種コンサルテーション




Bulletproof SSL and TLS
Ivan Ristić 著
プロフェッショナル
SSL/TLS


Professional IPv6
プロフェッショナル
IPv6
RFC 8200


Public
Today's theme
Dark side
Global Internet
Light side
Back ground

Pervasive Monitoring	DNS Blocking	Let's Encrypt	CDN
Privacy	Government	GDPR	Google and China
Browser and OS	TCP/IP	TLS, SSL	Web PKI
ISOC	IGF, IETF	W3C, GSMA	CA/BF

Technical Impact

Government

Technical Counter Action

Counter Action for Government

Pervasive Monitoring

DNS Blocking

Let’s Encrypt

CDN

Pervasive Monitoring

The Post-Snowden world

- PRISM
  - NSA / アメリカ国家安全保障局
  - Pervasive Surveillance, Pervasive Monitoring / 広域盗聴, 広域監視
- (Military) Intelligence / 諜報(活動)
  - Five Eyes (FVEY)
    - United States, United Kingdom, Canada, Australia, New Zealand

PRISMの衝撃

ひとつの国家がインターネット全体にネガティブな影響力を持つことを感じさせられた事件

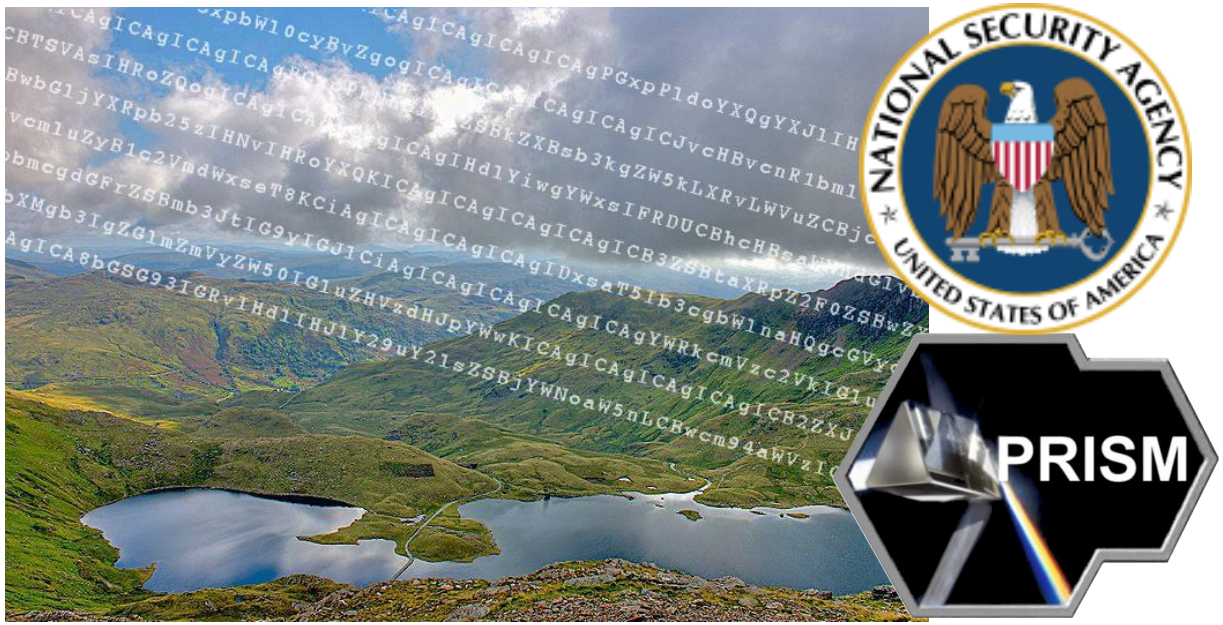
空気感が一変した

何を信じていいのかわからなくなった

インターネットは想定を超えたスケールに成長してしまったのではないか

現状と徴候

- Internet, Digital Technology, Computerの革新によって広範囲の大規模な攻撃が可能に
- しかし我々はその徴候を知っていたのでは?



Pervasive MonitoringとScalability

Pervasive Monitoring は

"The Internet" が

構造的に孕んでいた

根源的な課題ではないか？

DNS Blocking

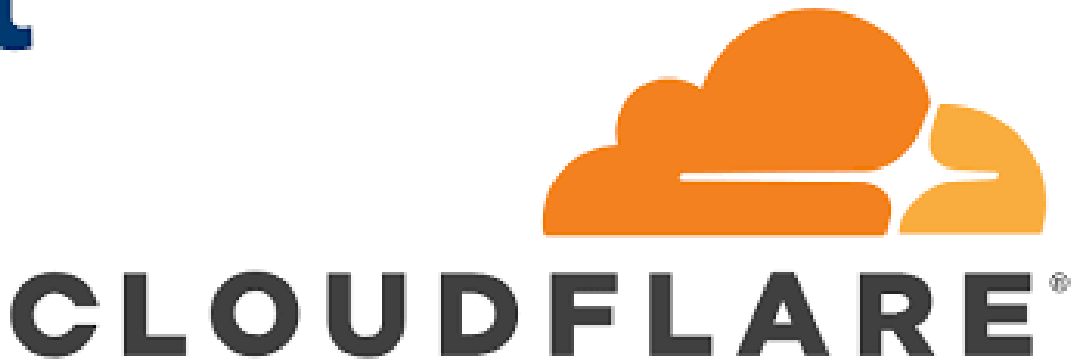
Internet Blocking問題

- 通信経路上での監視ではなく、End to Endの世界でそもそも特定の相手の通信を妨害する検閲行為
- 「誰かの決めた恣意的なリスト」で「特定の通信を不可能にさせよう」という行為
- スタートアップや個人をエンパワーする行為を潰すことにも使える

Let’s Encrypt

CDN

InternetをScaleさせ人をempowerする



Privacy

Government

GDPR

Google and China

Privacy

Privacy

- PrivacyはSecurityに包含されるものではない
- IdentityとかPersonal Dataとか
- 個人の権利

Government

Government

- Internetは国を越えた「なにか」
- 政府の軛を逃れている
- もちろん政府の恩恵も得られていない
- IANA Transitionによってアメリカの元もついに離れた

GDPR

GDPR

- 欧州(EU)におけるプライバシーの取り組み
- 非常に強い権限をもっている
- 国家間の交渉の材料
- …なんのせいだっけ？

Google and China

Google and China

- Googleが「検閲済みの検索結果を表示するGoogle」を中国でやる計画を立てていた(かもしれない)
  - Googleは2010年に中国から撤退している
  - “グーグル、中国で「検閲版」検索エンジンの提供検討＝情報サイト”
    - https://jp.reuters.com/article/china-google-idJPKBN1KM5GE
- 社内外から大きな批判
- 検閲している国は他にも多く存在

Browser and OS

TCP/IP, IPv6

TLS, SSL

Web PKI

Browser and OS

Browser and OS

- すべての人が使うソフトウェアをなるべく好ましい形で普及させていくのが標準化の目的の一つ
- 「みんなが共通して扱っていれば無駄が減って効率が良くなって幸せになるよね」

TCP/IP, IPv6

TCP/IP, IPv6

- Internetの根幹
- これがあるから、Internetはつながり、世界は自由への力を持つことが出来ている
- …しかし

TLS, SSL

TLS, SSL

- End to Endでの暗号化されて安全な通信のためのプロトコル技術
- ブラウザ・HTTP(HTTPS)においてはWeb PKIという背景のインフラを利用して、広範囲に普及することに成功している

Web PKI

Web PKI

- 認証局(CA)が証明書の発行を担うと、その証明書をインストールしたブラウザによってTLSを実現している。
- 認証局は、定められた要求事項を満たすことで始めて証明書を発行する事ができる

ISOC

IGF, IETF

W3C, GSMA

CA/BF

“The Internet is for everyone.”

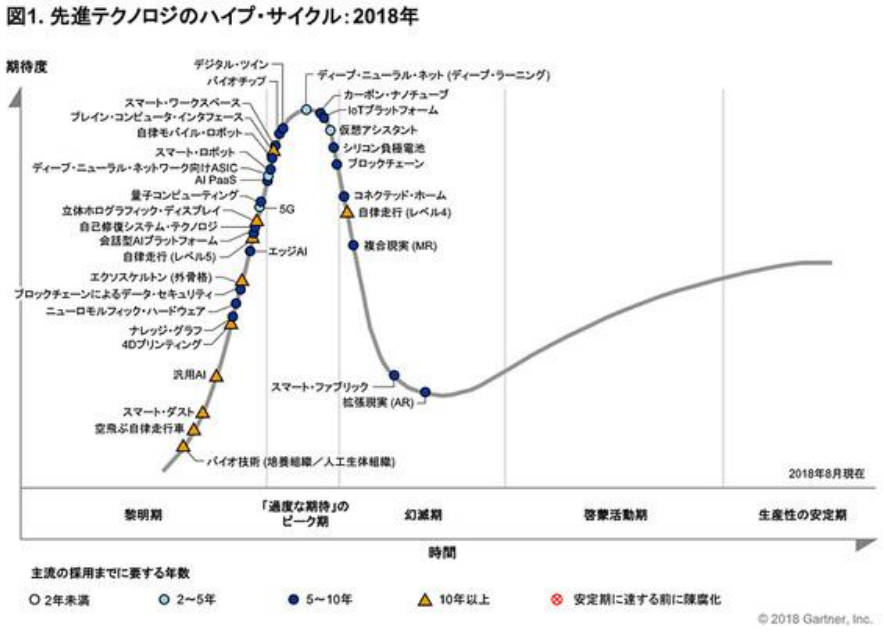
SDOs and etc...

IGF Internet Governance Forum

CA/BROWSER FORUM

標準化活動がわかると何が出来るか

- 単純に言えばテクノロジー領域における近未来予測…じみたことが出来る
  - トレンド予測
- 個人や小さなチームで世界を変える仕事ができる



出典：ガートナー (2018年8月)

Conclusion

インターネット標準はいまや社会において非常に重要

社会を個人をエンパワーして変えていくことが出来る

技術でも個人でも世界を変えられる！

背景を知ることでより社会を、世界を知ることが出来る