

Authenticity Verification Technology in the Digital Space

A Foundation for a Trusted Information Society

June 2026

Originator Profile Collaborative Innovation Partnership

Originator Profile



<https://originator-profile.org/>

Contents

- 1. Toward a Trusted Information Society**
- 2. What OP Enables**
- 3. Endorsement Extends to Distribution Channels**
- 4. OP Empowers Recipients to Make Informed Decisions**
- 5. OP Ecosystem and Its Contribution to Society**
- 6. Scope of OP**
 - a. OP Supporting AI
 - b. Integration of AI and OP
 - c. Email / SMS / Chat / Ads and OP
 - d. Social Media and OP
 - e. Online Media and OP
- 7. Outlook for Practical Deployment to Improve Trust in Corporate Information / Help Advance the Social Implementation of OP**

- 8. Roadmap for Building a Trust Ecosystem with OP**
- 9. OP-CIP's Actions for Adoption**

Appendix

- a. OP and Related Technology
- b. Use Cases
 - Third-Party Verification of Originators
 - Municipal Information
 - Authenticity of Public Institution Websites
 - Phishing Countermeasures
 - Authenticity of Election-related Information

Toward a Trusted Information Society

Facial expressions, tone of voice, clothing, demeanor...
We intuitively judge whether someone can be trusted,
drawing on a range of cues and experience.

When we are still uneasy, we might ask someone, or look
into it ourselves.

Or we may simply decide not to judge right away.

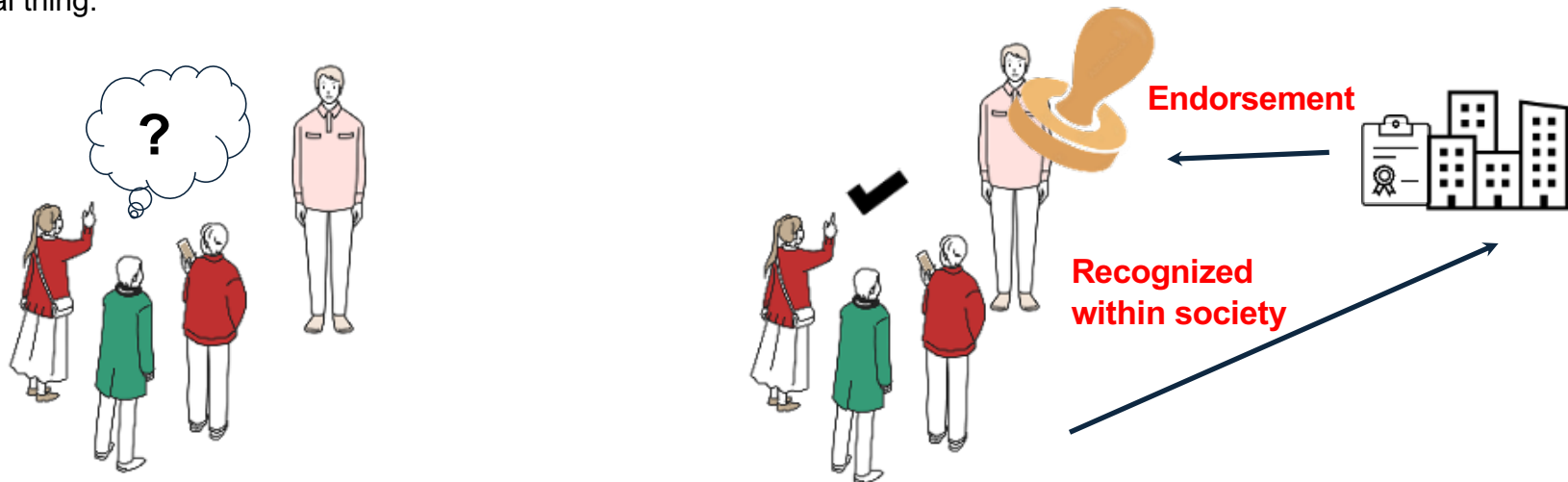
So then, what about the Internet?

OP identifies who is behind information on the Internet and
makes visible the third-party assessments built up from the
past to the present. In doing so, it backs up our intuition and
works toward a society in which trustworthy information
circulates freely.

Toward a Trusted Information Society

When we want to convey something to others, we sometimes rely on a third party's assessment to show we can be trusted.

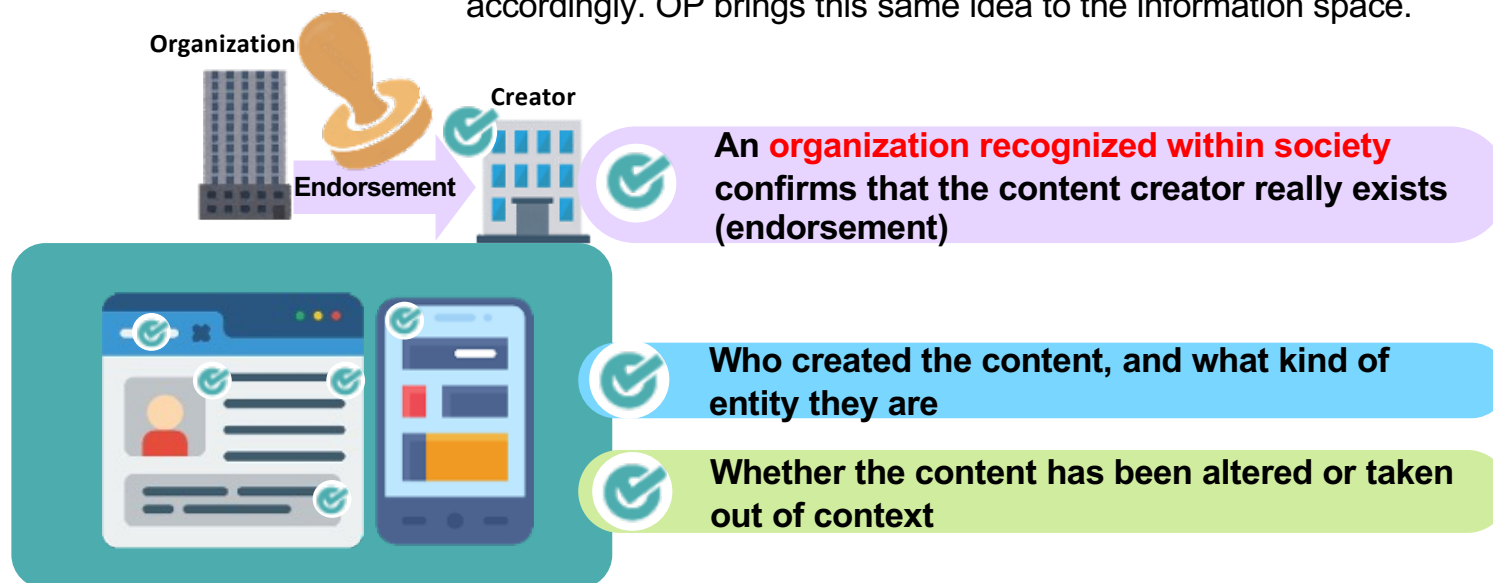
It is not enough for someone to simply insist that they are trustworthy. That is why trust becomes possible when a person or organization with a proven track record, one that many people already recognize, vouches for you and confirms that you are the real thing.



In the OP model, the role of this **third party recognized within society** is realized in the information space. What is more, OP provides several such third-party entities. In this way, it overlays real-world trust onto information on the web and, by conveying who was involved in publishing the information and whether they actually exist, shows how reliable that information is.

What OP Enables

In the real world, we pay close attention to who is speaking and how others regard them, and we judge what they say accordingly. OP brings this same idea to the information space.



False or misleading information is easier to spot!

An industry association the content creator belongs to, or another **organization recognized within society**, confirms that the originator really exists, and anyone can check this. It also makes automated processing based on that information possible. As OP technology takes hold, it builds an information space where trust is made visible and given real value.



Endorsement Extends to Distribution Channels



Extend the chain of trust to the distribution platforms too

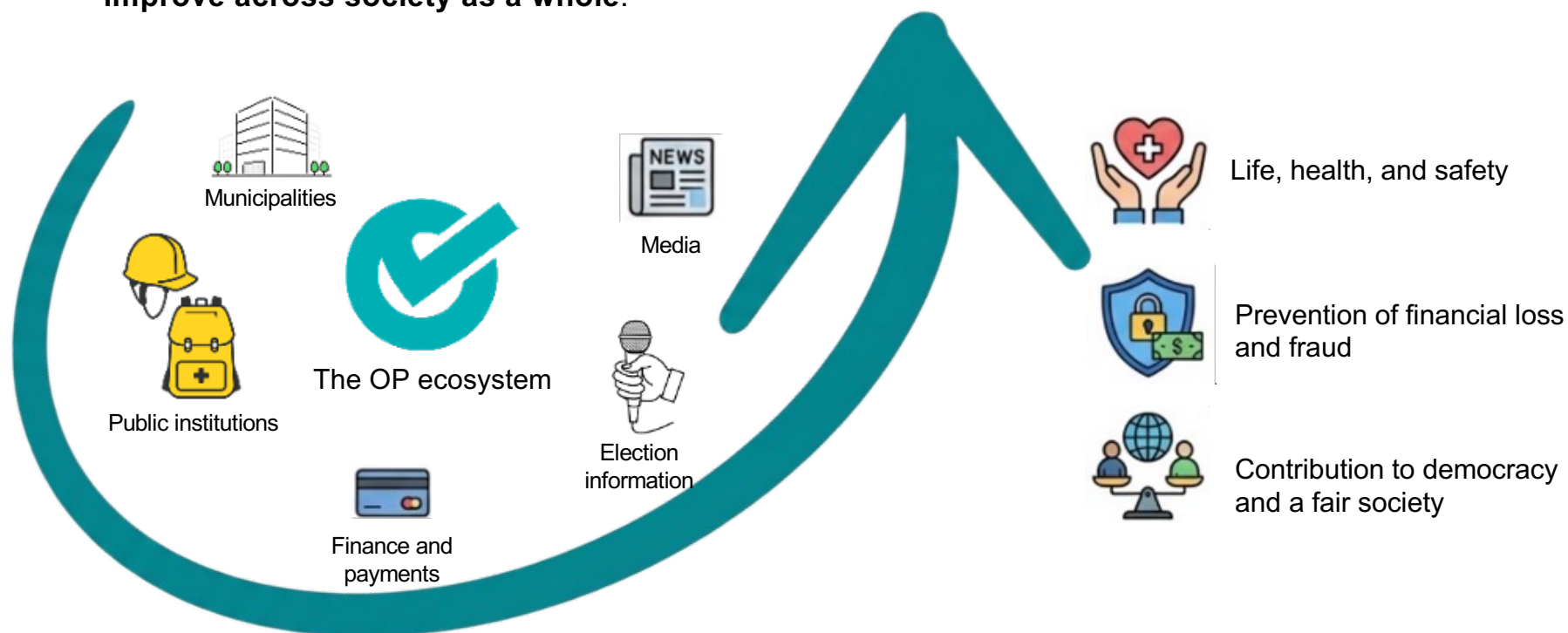
The endorsement mechanism is not limited to content creators.

When the site operators that users actually see, **such as portals and platforms, along with advertisers, also adopt OP**, the range over which trust can be made visible grows wider.

This creates an ecosystem that false or misleading information struggles to enter, making users safer.

OP Ecosystem and Its Contribution to Society

An OP ecosystem that can confirm and guarantee the authenticity of information originators and service providers spreads across many industries, and as it does, **the reliability and safety of information improve across society as a whole.**



Scope of OP

OP Supporting AI

Whether people access information and services directly, or agents gather and analyze information and carry out tasks on their behalf, confirming the source and trustworthiness of that information and those services is essential.

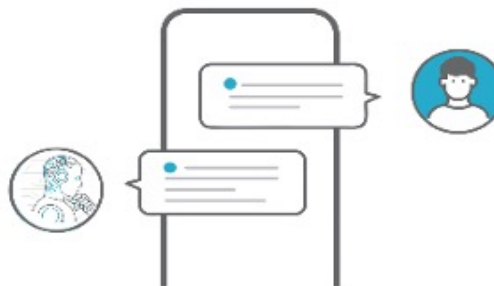
As browser and AI agent automation advances, technology that can accurately tell AI who the originator is and how a service should be used becomes all the more important.

Together with web technologies, OP supports a more accurate understanding of content and services by AI.

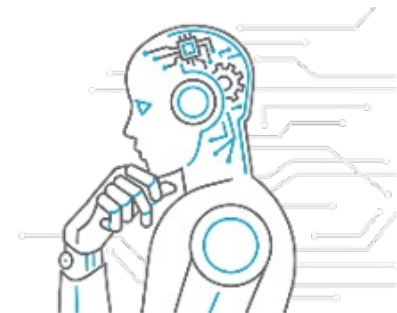
Looking up online information in a browser
(Verifying originator's authenticity to determine trustworthiness with OP)



Looking up online information with conversational AI
(Verifying source's authenticity to determine trustworthiness with OP)



AI agents judge trustworthiness and act
on the user's behalf

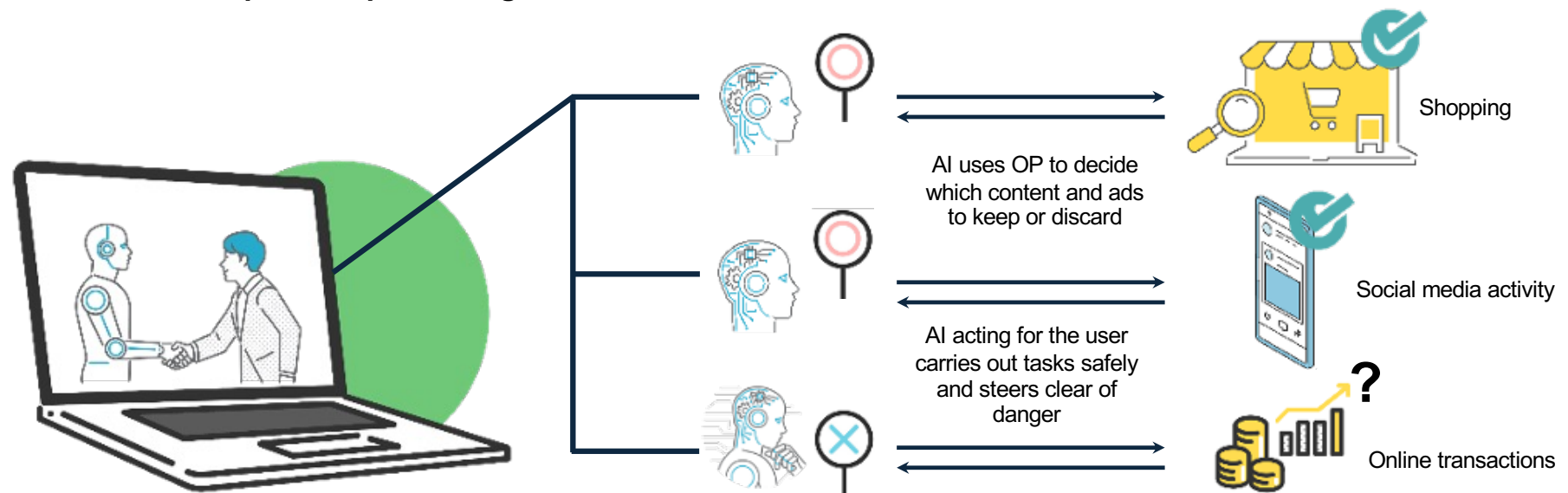


Integration of AI and OP

❖ Automation by AI

What does an AI acting on a person's behalf use to judge whether a site is trustworthy?

When it searches, posts, or makes a payment, OP can help judge whether a site or service is trustworthy, **from the standpoint of protecting users.**

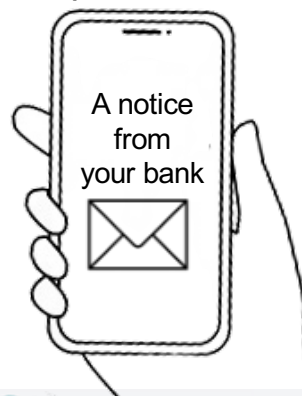


Email / SMS / Chat / Ads and OP

❖ Mail clients, servers, and browsers use OP to protect users

With email as it works today, there is no easy way to tell whether the sender is genuine. OP makes it possible to confirm a message's sender information reliably and easily.

- ❑ When a link is about to open a page, **a warning appears if anything looks suspicious, reducing the harm from phishing.**
- ❑ With OP based on licenses, permits, and Verifications, impersonation becomes impossible.



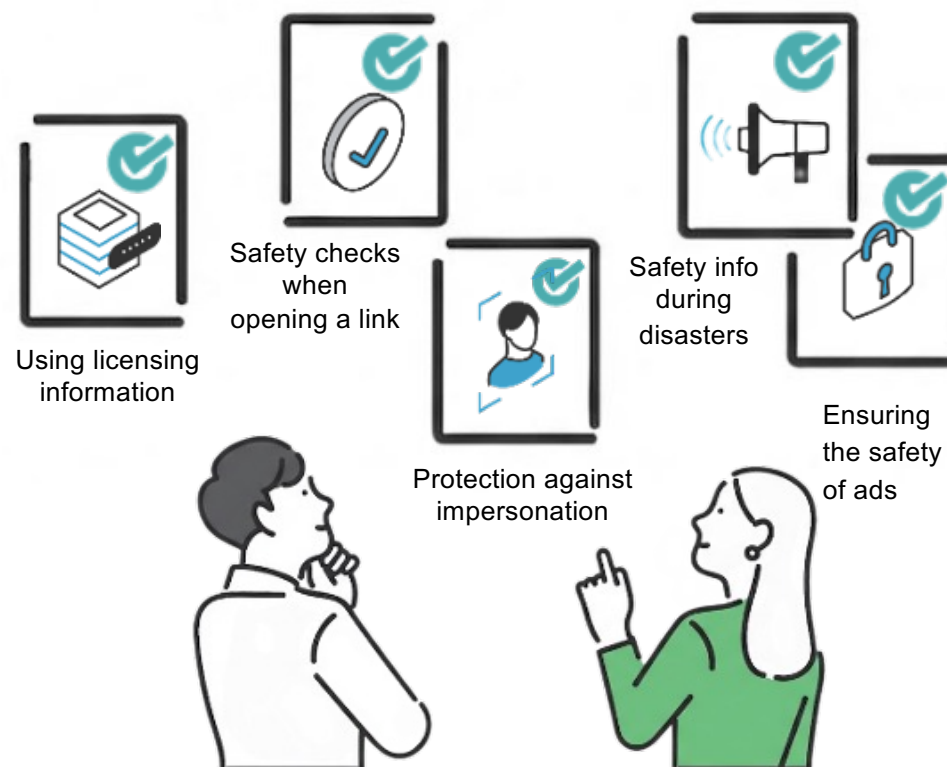
Social Media and OP

❖ Helping solve a range of social media problems

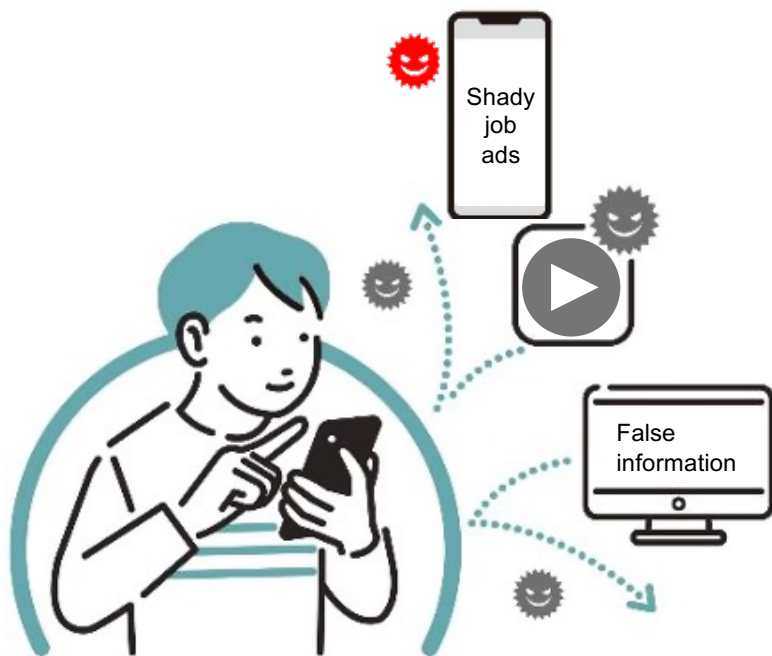
Even when it really matters whether an account is genuine, judging the trustworthiness of a source is difficult in practice.

When social media companies work together with OP, it can do far more than simply display authenticity.

- ❑ Displays and recommendations that draw on licensing information
- ❑ Safety checks when opening a link
- ❑ Protection against impersonation
- ❑ Priority display of safety information during disasters
- ❑ Ensuring the safety of ads
- ❑ A better timeline



Online Media and OP



❖ Making the source and originator clear

As online information comes to carry real influence over society, exposure to false information and unintended tampering can be curbed with OP.

- ☐ Coming into contact with unreliable or false information
- ☐ Ads that lure users to illegal sites
- ☐ Fraudulent ads and ads recruiting for illegal work

- ☐ Working with news sites, video sites, and other operators
- ☐ Partnering with other industry associations to ensure safety end to end, from the shooting and creation of images and video through to how they are displayed

Use Cases

Use Cases

As examples of the society with OP we are aiming for, we imagined five use cases related to life, health, and safety; prevention of financial loss and fraud; and contribution to democracy and a fair society.

With OP in place, users can check information about the originator.

Where OP is absent, that itself prompts users to check more carefully, which in turn makes them more likely to tell what is genuine from what is not.

It is also a society without information gaps, where every user can reach the information they need with confidence and is not misled by malicious content.

❖ **Life, health, and safety**

1. Third-party verification of originators
2. Municipal information
3. Authenticity of public institution websites

❖ **Prevention of financial loss and fraud**

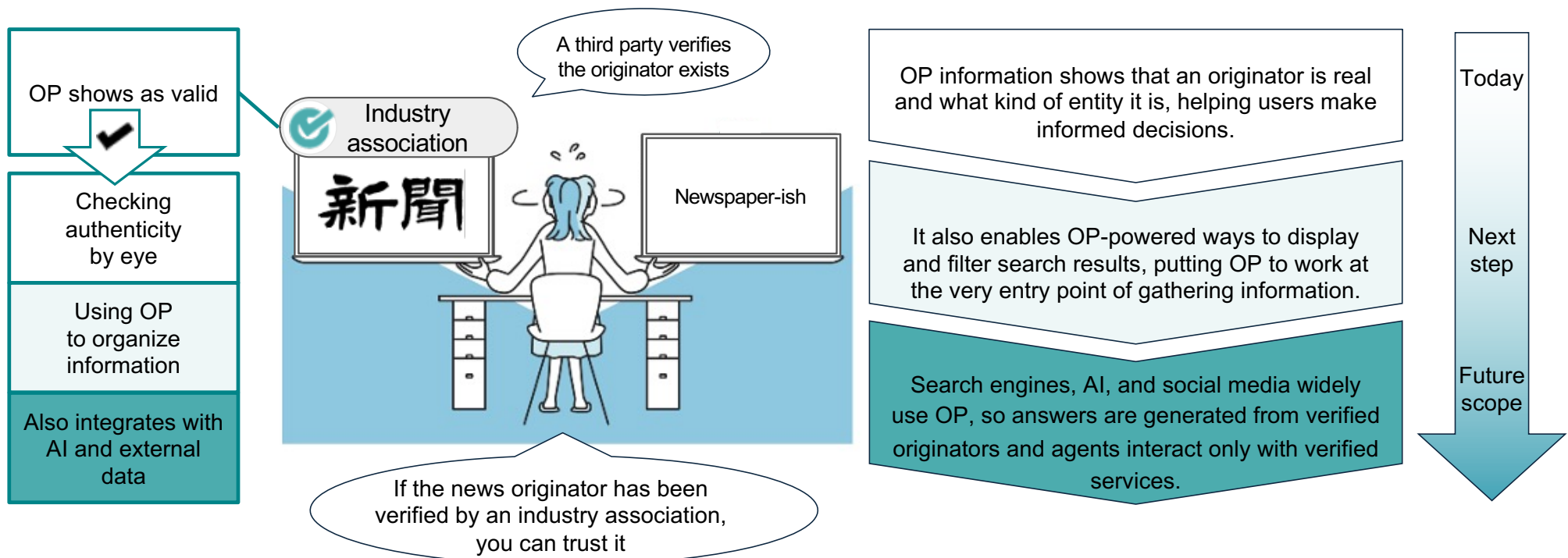
4. Phishing countermeasures

❖ **Contribution to democracy and a fair society**

5. Authenticity of election-related information

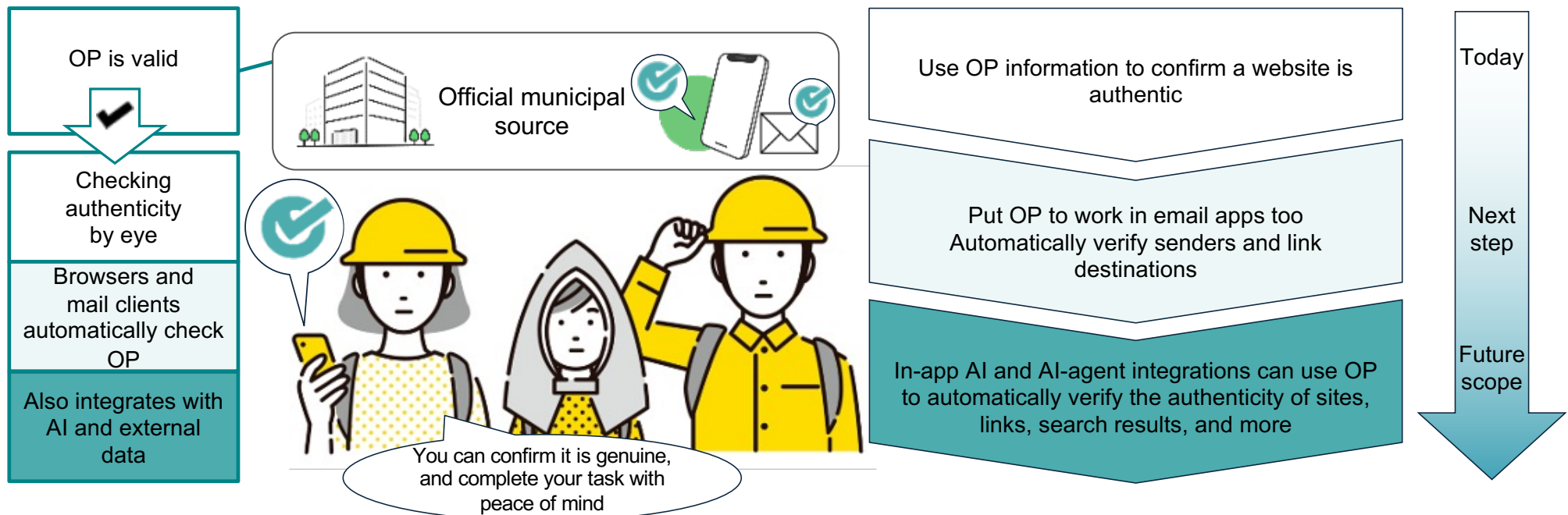
Third-Party Verification of Originators

Given the existence of websites impersonating news outlets, OP information verified by third parties, such as industry associations, confirms authenticity by showing who the originator is and whether it comes from a responsible organization.



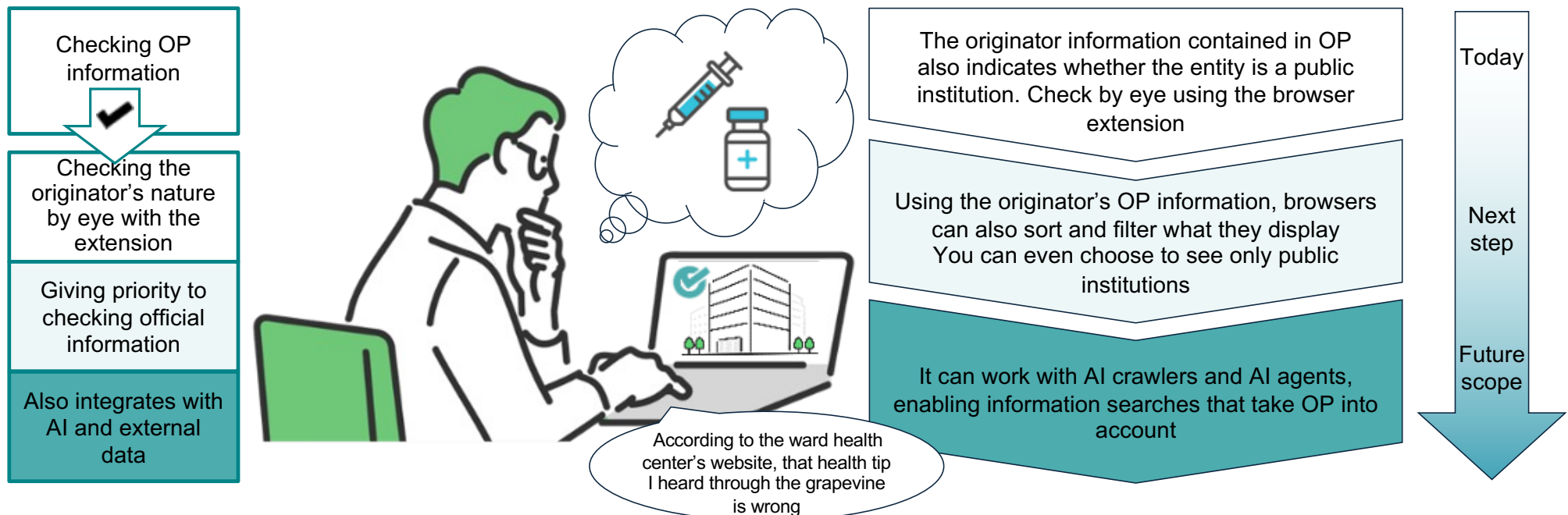
Municipal Information

For municipal information that is an easy target for criminals, such as post-disaster livelihood-recovery benefit programs, authenticity matters especially to residents. Proving authenticity with OP also helps prevent disruption to administrative operations. Getting the word out about what OP is, and raising awareness of information literacy, are key as well.



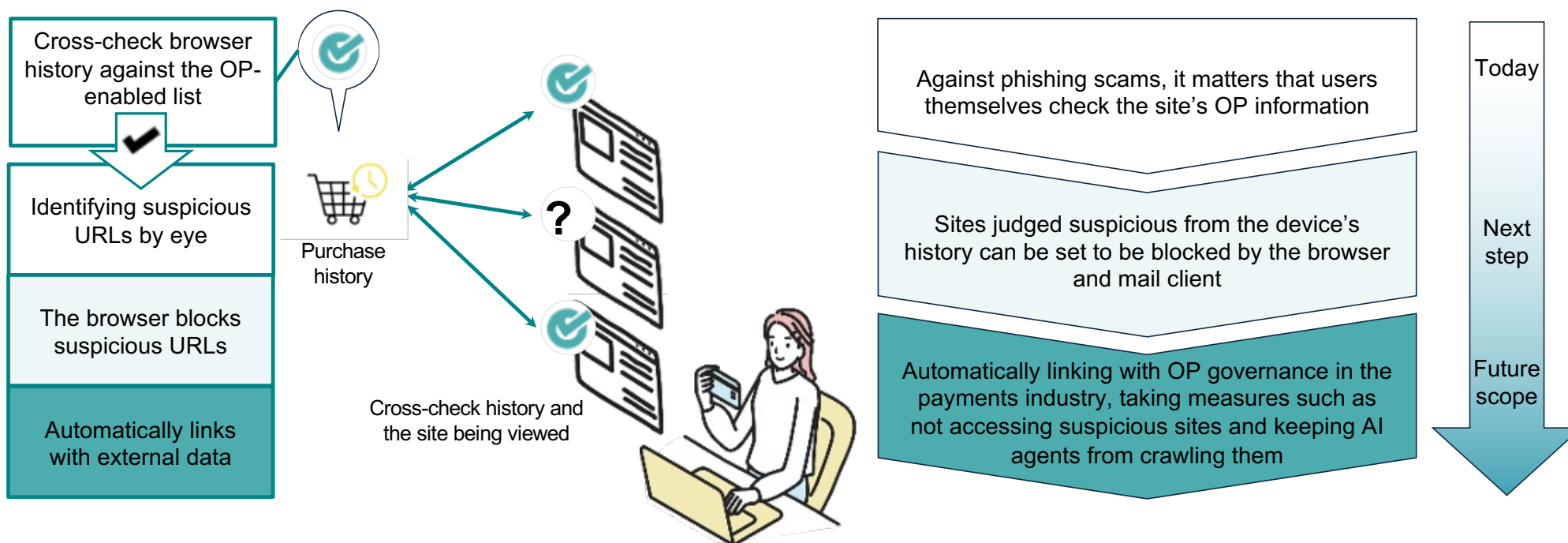
Authenticity of Public Institution Websites

Claims like “gargling with iodine solution protects you from radiation” or “you are under criminal investigation,” along with the fraud carried out through false information and impersonated sites posing as public institutions, can be told apart with OP. Users can know for certain that the sites of public institutions such as health centers and the police are the real thing.



Phishing Countermeasures

An OP-enabled browser keeps a list of OP-enabled companies in industries where scam sites are common, and in addition, a history of the OP-enabled sites the user has visited. Drawing on both the OP-enabled list and this history, the browser and AI automatically block access to fake and phishing sites.



Authenticity of Election-related Information

OP's core functionality can detect possible tampering with video footage or websites. If election authorities certify candidates through OP, that OP information can be displayed across a wide range of sites, from distribution channels to social media, dramatically raising the chances that false information will be recognized for what it is.

