電子メールセキュリティ対策としてのS/MIMEおよびSSMAX

2023年8月28日　才所敏明
toshiaki.saisho@advanced-it.co.jp
(株)IT企画
(株)ZenmuTech
中央大学研究開発機構

経歴概要

1970年4月～1994年12月　東京芝浦電気（東芝）・情報システム部門

東芝Gの技術部門・研究部門の

研究開発活動環境（コンピュータ・ネットワーク）の整備・高度化を推進

1995年1月～2007年9月　東芝・セキュリティ技術研究開発部門

東芝のセキュリティ技術センター発足と同時にセンター長就任

東芝Gのセキュリティ技術開発・事業支援活動を推進

2007年10月　(株)IT企画を設立

情報技術および情報セキュリティ技術分野の研究開発や

その応用事業に対するプロフェッショナルサービスを開始

［現職］

(株)IT企画　代表取締役社長

事業支援活動（顧問・相談役）：２社（日、米）

研究開発活動（研究員）：中央大学研究開発機構、九州大学大学院

技術分野：暗号・認証、秘密分散、本人確認技術（バイオメトリクス）、

電子メールセキュリティ、IoTシステム、ビッグデータ、AI、

暗号資産セキュリティ、ブロックチェーン技術

電子メールとのかかわり史

（1970年代～　パソコン通信（CompuServe、Nifty-Serve）による電子メール）
1974年　TCP/IP提案（Vinton Gray Cerf、Robert Elliot Kahn）
1984年　JUNET実験開始（Murai）　東芝も参加
1986年　インターネットメールを東芝社内標準メールへ
　　企業での電子メール利用に関する議論開始
　　５～６社＋大学関係者　10名程度の構成
1987年　InetClub発足（企業での電子メール利用実験）　事務局：KDD（Asami）
1989年　WWW開発（Tim Berners-Lee）　1991年　公開（テキストベース）
1993年　NCSA Mosaic（Marc Andreessen）　1994年　Mosaic Communications
1992年～93年　AT&T Jens（現SpinNet）が日本初の、IIJが日本企業初の
　　ISPとしてサービスを開始

－－

2013年～2015年　中央大学研究開発機構がNICTより受託した
　　「組織間機密通信のための公開鍵システムの研究開発」へ参加
2016年～　掲記PJの成果物「組織暗号」の応用による
　　電子メールのセキュリティ研究

電子メールセキュリティ関連学会発表一覧

（https://advanced-it.co.jp/2016_wp/president/）

コンピュータセキュリティシンポジューム２０１６（CSS2016）
＊才所敏明，五太子政史，辻井重男，”標的型メール攻撃に対抗する「組織通信向けS/MIME」”
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20161016_1_IPSJCSS2016077.pdf

2017年 暗号と情報セキュリティシンポジューム（SCIS2017)
＊才所 敏明，五太子 政史，辻井 重男，”「安心・安全電子メール利用基盤（SSMAX）」構想”
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20170127SCIS2017.pdf

コンピュータセキュリティシンポジューム２０１７（CSS2017）
＊才所敏明，五太子政史，辻井重男，”「安心・安全電子メール利用基盤（SSMAX）」”
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20171025CSS2017paper.pdf

2017年 暗号と情報セキュリティ研究会 (ISEC)
＊才所 敏明，辻井 重男，”社会的課題「安心・安全な電子メール利用環境の実現」のための三止揚・MELT-UP の試み”(ISEC2017-54)
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20171113_KyotoISEC.pdf

2018年 情報処理学会論文誌59巻9月号
＊才所敏明，五太子政史，辻井重男，”「安心・安全電子メール利用基盤（SSMAX）」悪意のあるメールの根絶とメール内容の確実な保護を目指して ”
https://advanced-it.co.jp/2016_wp/wp-content/pdf/20180915-IPSJ-JNL5909009.pdf

SSMAXが目指す電子メール利用環境

Secure and Safe eMAil eXchange framework(SSMAX)

（１）利用者の匿名性と特定・追跡性の両立

電子メール利用者の匿名性の確保➔利用者の安心・安全

電子メール送信者の特定・追跡性の確保➔社会の安心・安全

（不正・不法および悪意のある電子メール抑止・防止）

（２）電子メールによる送信情報の秘匿性と検査可能性の両立

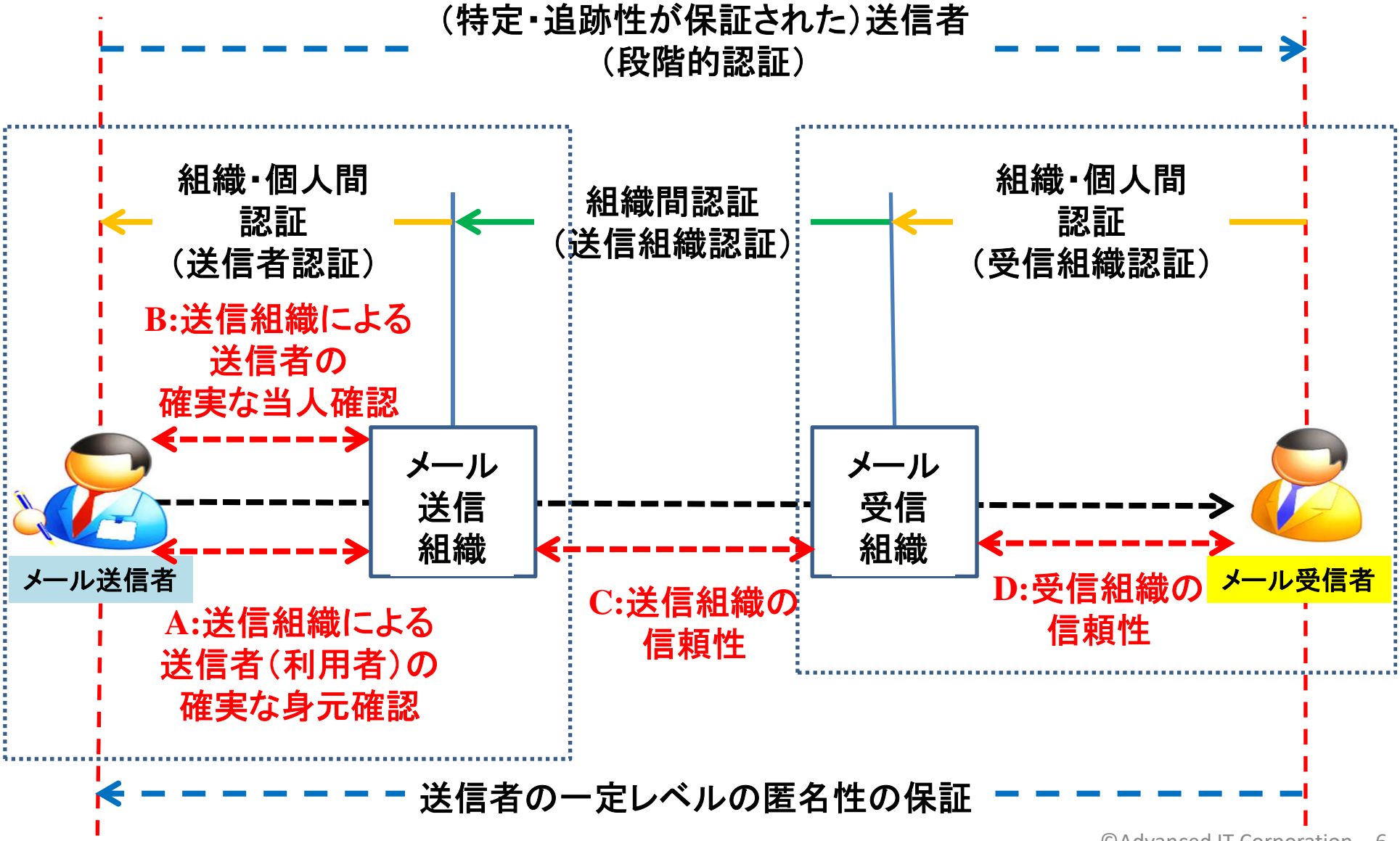
送信情報の秘匿性を確保➔個人情報・機密情報の保護

送信情報の検査可能性を確保

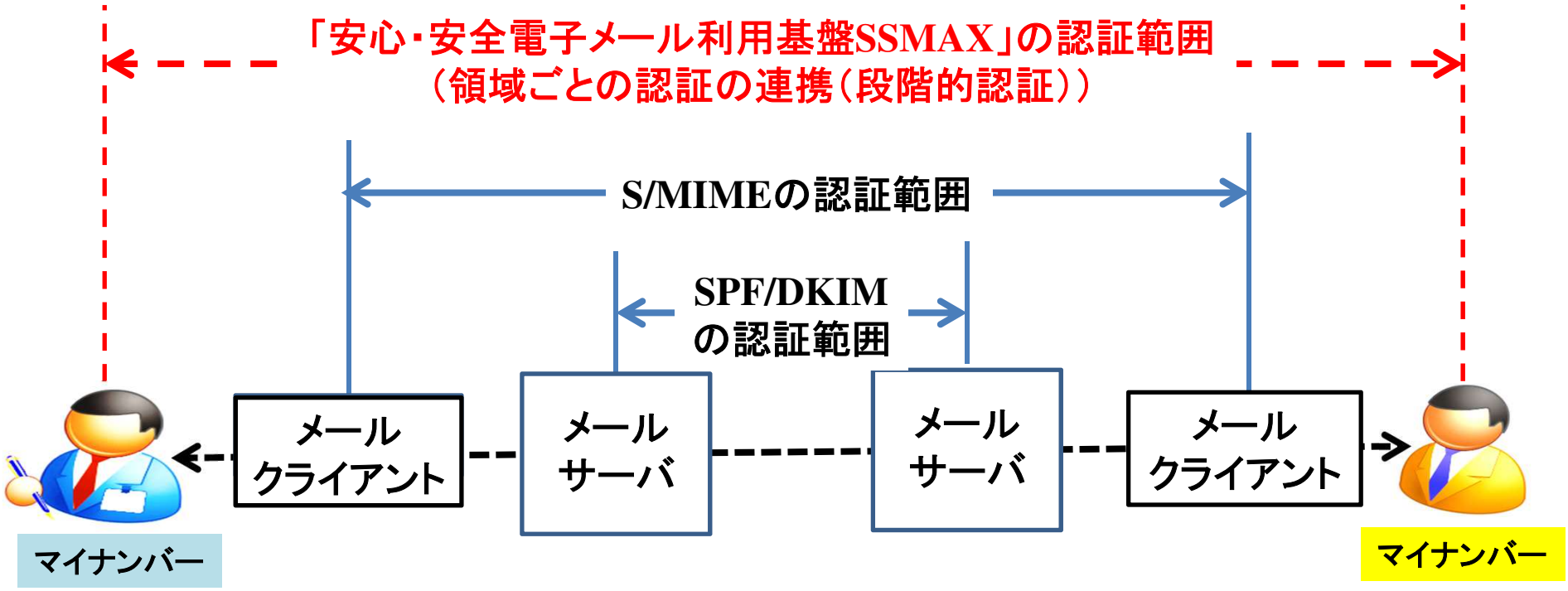
➔電子メールによる機密情報漏洩の防止

電子メールによるマルウェア流入の防止

（1）利用者の匿名性と特定・追跡性の両立

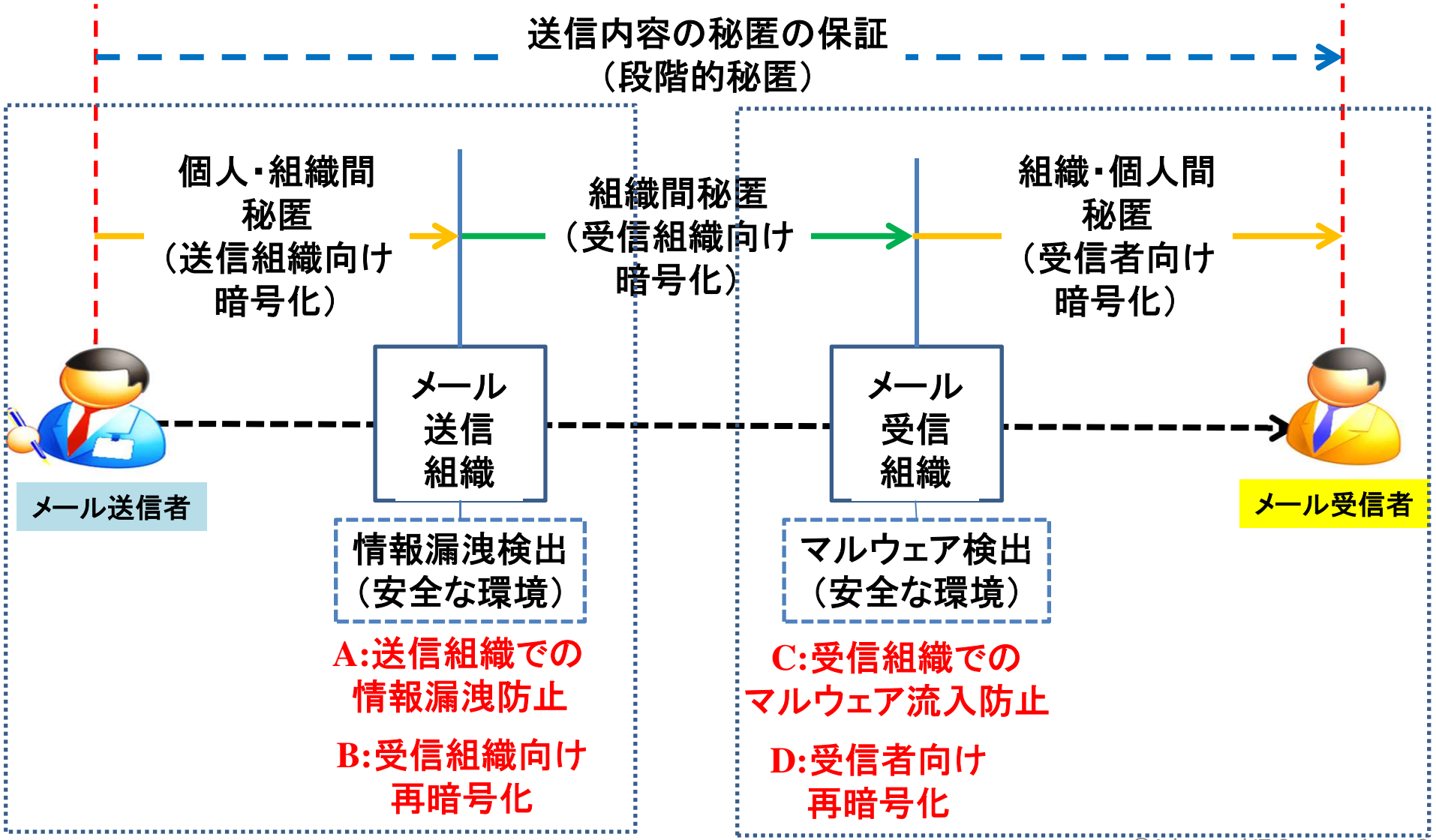


S/MIMEとの比較
SSMAXとS/MIMEの認証方式・範囲の違い

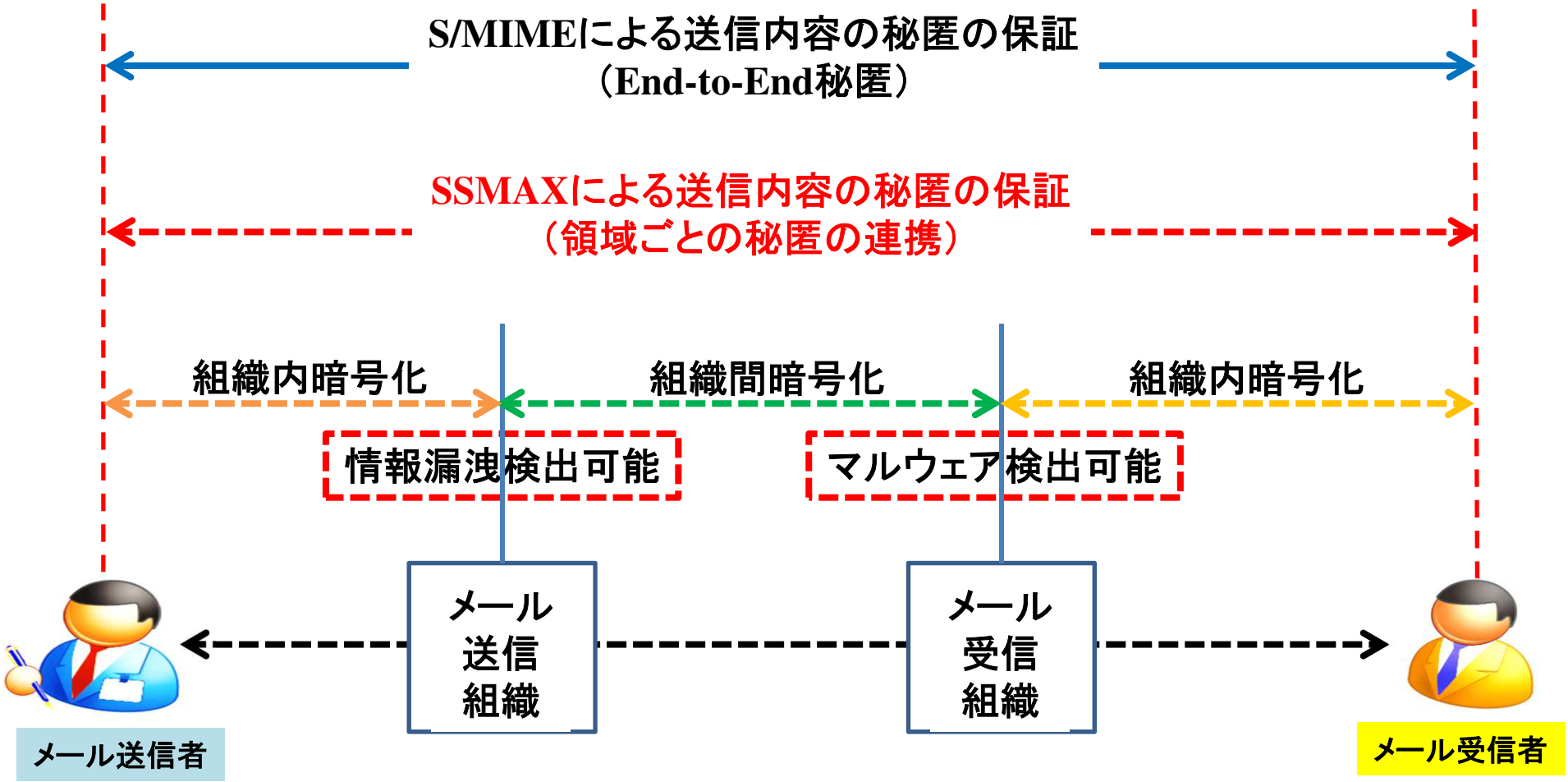


SSMAXでは、メール送信者の特定・追跡まで可能！

（2）送信情報の秘匿性と検査可能性の両立



S/MIMEとの比較
SSMAXとS/MIMEの暗号化方式・範囲の違い



S/MIME普及に向けて

（なりすましメール対策として現時点で利用可能なもっとも効果的なツール）

(1)電子メール利用者/組織の社会的責任に関するコンセンサス醸成

なりすましメールは、なりすましメール発信者だけでなく
なりすましされた利用者・組織も、相応の責任を負うべきであり、
なりすましされない対策をとる必要があることを、社会のコンセンサスへ。

(2)安心・安全なIT社会実現に向けた政府の主導的役割に期待

まずは中央省庁，地方自治体等，官公庁や関連機関が先行導入し，
有用性・有効性を実業務で示すのが効果的。
➔政府機関等の対策基準策定のためのガイドラインにて、
原則、S/MIMEの使用を規定すべき。（ガイドラインの改定が必要）
➔企業からのメールについては、
段階的にS/MIMEの使用を求めるべき。

終

（株）IT企画
https://advanced-it.co.jp/

才所敏明
toshiaki.saisho@advanced-it.co.jp