

CRYPTRECシンポジウム2009
～電子政府推奨暗号リスト改訂に向けて～
2009年2月18日

パネル2

「日本の暗号研究と電子政府推奨暗号の今後について」

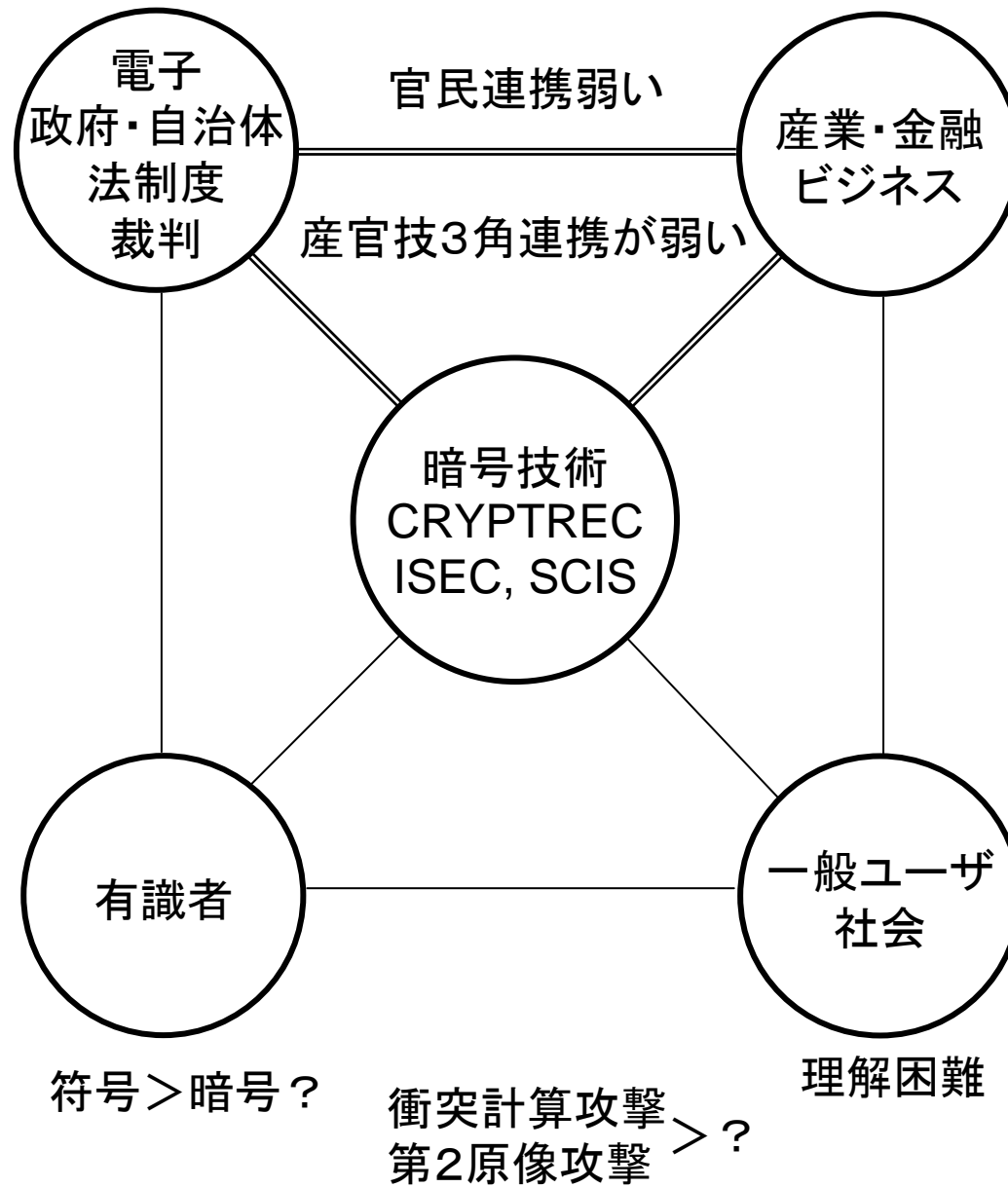
情報セキュリティ大学院大学

辻井 重男

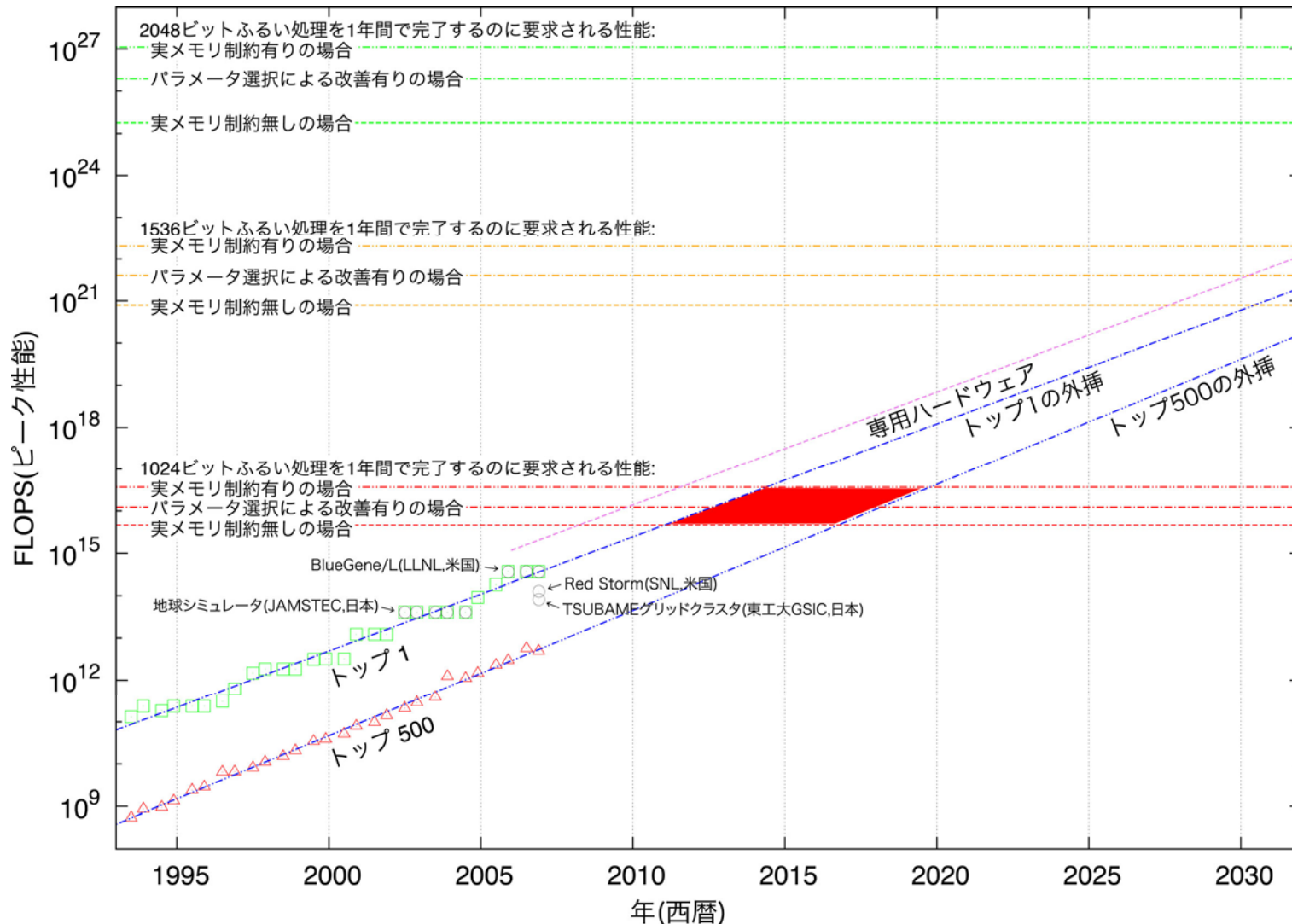
「電子署名及び認証業務に関する法律」に
関する暗号アルゴリズムの移行について
～電子署名法検討会 報告書概要～
平成20年9月
電子署名法主務三省
(総務省、法務省、経済産業省)

公的個人認証サービスにおける
暗号方式等の移行に関する検討会報告書
(H20年度)

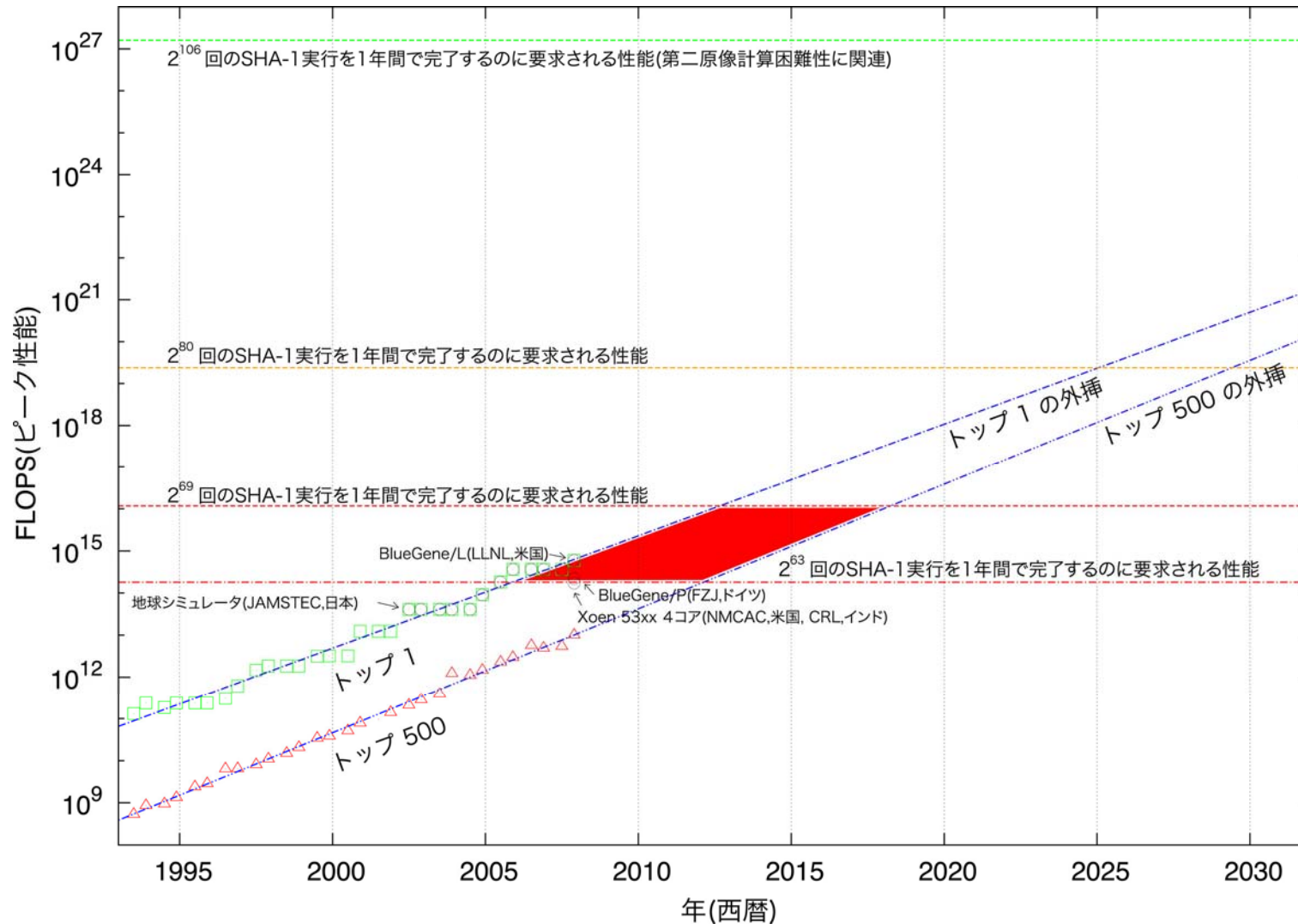
電子政府ガイドライン作成検討会
セキュリティ分科会
内閣官房情報セキュリティセンター(NISC)
(H20～H21年度)




















1年間でふるい処理を完了するのに要求される 処理性能の予測 (CRYPTREC Report 2006)



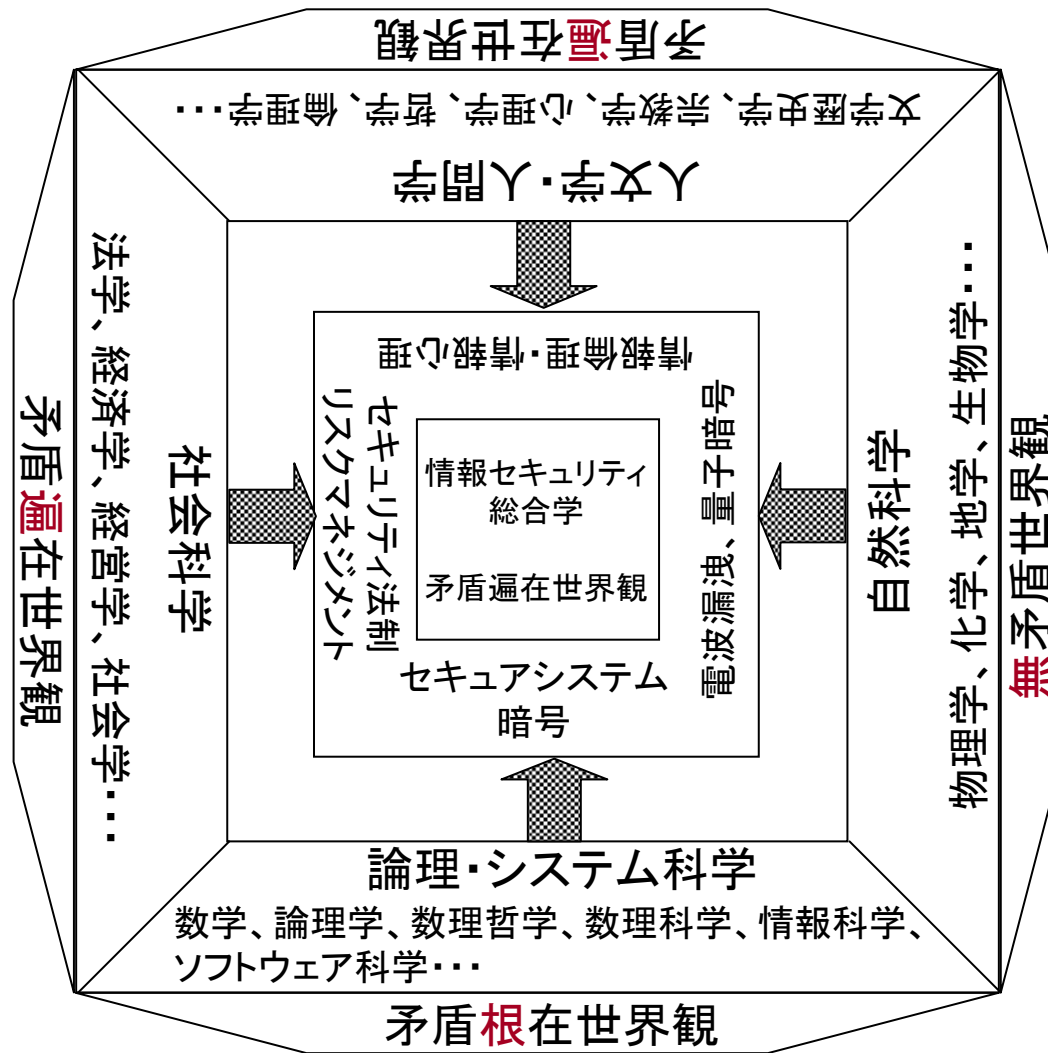
1年間で衝突を計算するのに要求される処理性能 の予測 (電子署名法検討会報告書 2008.05.30)



公的個人認証サービスにおける暗号アルゴリズムの移行スケジュール

年度	2009 H21	2010 H22	2011 H23	2012 H24	2013 H25	2014 H26	2015 H27	2016 H28	2017 H29	2018 H30	2019 H31	2020 H32	...
SHA-1の安全性評価								*1					
RSA1024の安全性評価								*2					
													
政府機関の情報システム						*4	*5						
電子署名法	*6					*7	*8						
公的個人認証サービス						*9		*10		*11			
公的個人認証サービス センターシステム		*12											
鍵ペア生成装置		*13											
住民基本台帳カード			*14										

「公的個人認証サービスにおける暗号方式等の移行に関する検討会報告書(H20年度)」より抜粋



©Shigeo Tsujii 2009

図. 矛盾という視点から見た情報セキュリティと暗号の位置付け