「MD5の安全性の限界に関する調査研究」概要報告資料

2008年7月

独立行政法人　情報処理推進機構

1．調査の課題・目的

- ハッシュ関数MD5を適用している電子メールでのAPOP方式の脆弱性が指摘されたことを受け、その検証調査と、実使用環境下での実証実験を行い、その脆弱性の程度を確認すると共に当面の対策についても調査する。

- APOP方式を用いる電子メールシステムとAPOPの脆弱性を突く攻撃サーバを構築し、実メール使用環境を擬似しながら攻撃によりパスワードが解読できることを実験する。実験にあたっては、パスワードの強度、長さ等を振らせると共に、攻撃においてもパスワード辞書を活用するなど、攻撃者の手法を想定しながら解読強度を確認する。

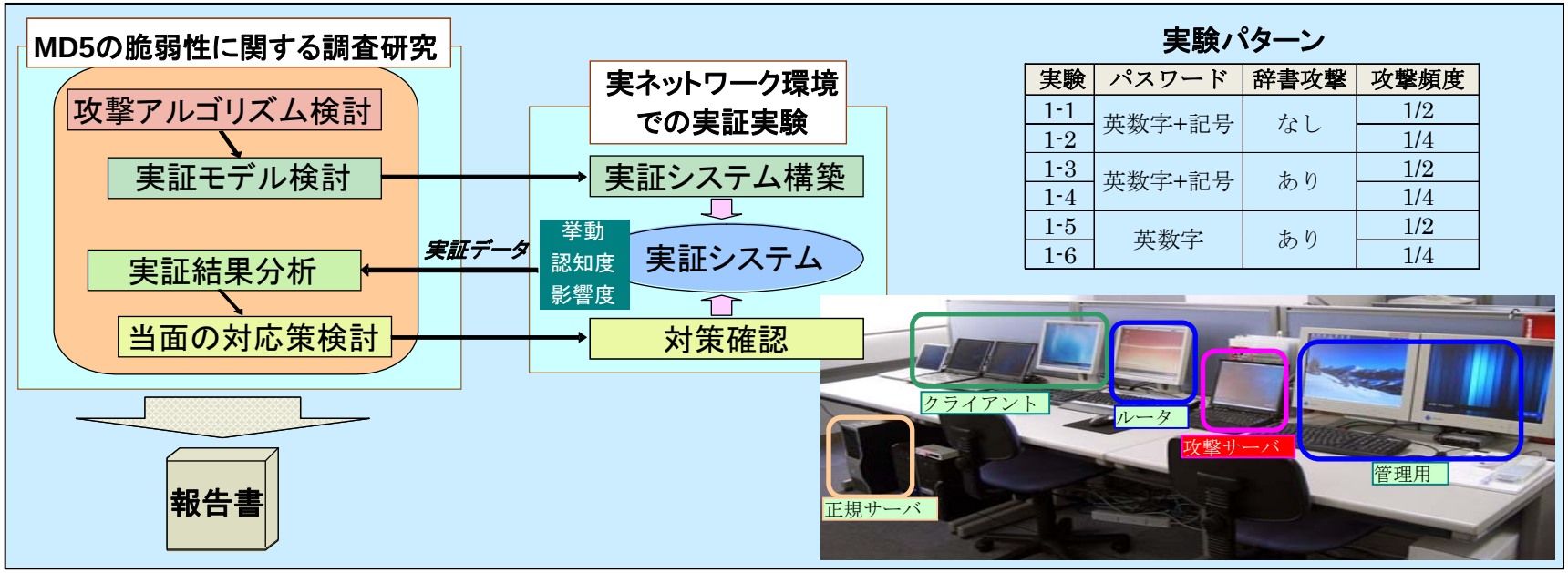
- 併せて、実態調査として、APOP方式を採用しているプロバイダでの対応状況、メールソフトでのAPOP脆弱性対策の実施状況等の調査を行う。

- 調査の結果として、当該技術を用いるシステム利用者、開発者に対し早急な対応を促し、被害が発生、拡大することを未然に防ぐ 。

2. 調査の実施内容

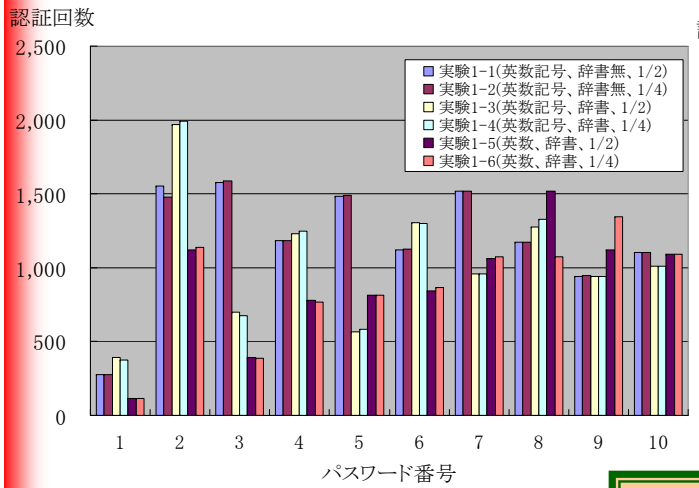
・文献情報並びに有識者（電気通信大学太田教授）との議論をもとに、APOP攻撃アルゴリズムの実装、実証実験システム構築を行い、各種条件下での攻撃によるパスワード解読の可否、強度を実証確認した。
・実証実験に加え、主要プロバイダ並びに主要電子メールソフトにおけるAPOP脆弱性対策の実施状況を調査した。電子メールソフトについては上記実証実験環境での挙動についても確認した。

・通常よく用いられる形式のパスワードから、比較的強固と考えられているパスワードまで、各種条件下において、全てのパスワードが比較的短時間に解読できた。
・ほとんどの主要プロバイダでAPOPの脆弱性に対する対策がなく、またほとんどの主要なメールソフトで脆弱性対策が講じられていないことが判明した。

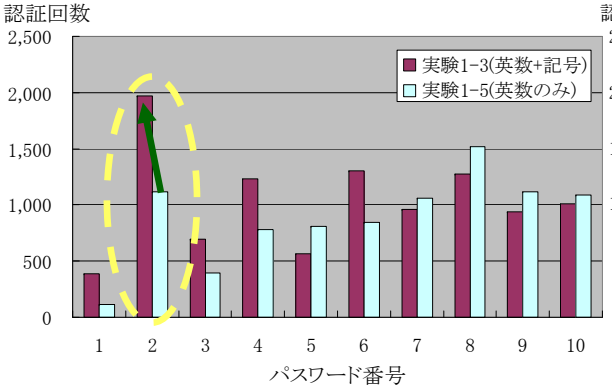


3. 調査結果(実証実験)

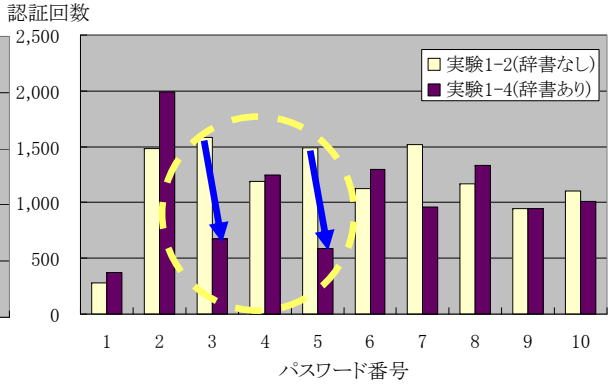
- ごく一般的なPCを用いても、攻撃サーバはそれぞれのクライアントに設定したパスワードのすべてを正しく解読した。その解読に要する時間も、設定条件により差異はあるものの、通常の使用環境においてはほぼ現実的な時間(約40日)以内に収まってしまうことを検証した。



パスワード解読の認証回数結果



パスワードにおける記号の効果



パスワード辞書攻撃の効果

実験に用いたパスワード

番号	英数字と記号	英数字のみ
1	1!2"3#4$5%6&	password0123
2	C-l_i~e=n|t?	q1w2e3r4t5y6
3	sato@ice.uec	Blue1997Deep
4	^5+er|5ked**	BObutarou119
5	!Psyvariar2R	AABCgn005ABG
6	Xbo#G_QN8VFK	OMwPVtpJfHye
7	dLa~HfhwRTBr	uoyU6c3ZDSLg
8	Q6|/VgTz9;[=	EcgBsvf384JQ
9	n&<$9}fMm-,4	4FlfjSzPHDkN
10	(OPeQS'wko@>	OAe3Kd9mblnE
備考	実験1-1,2,3,4	実験1-5,6

【パスワード解読の危険性】

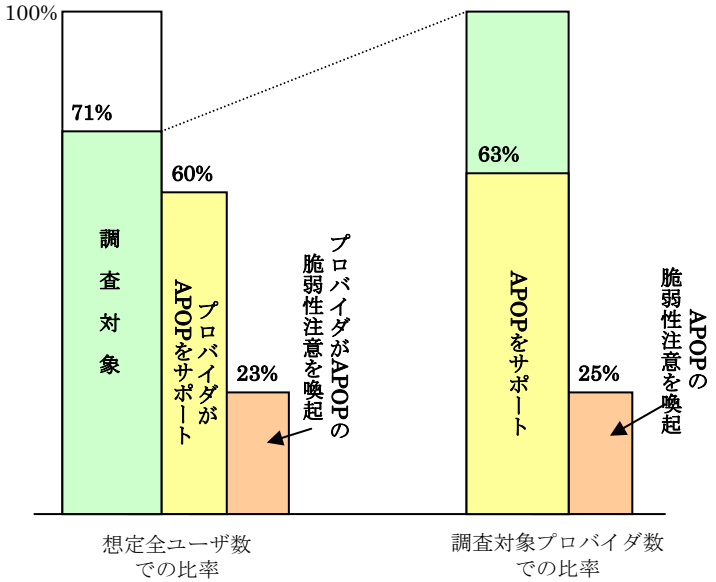
パスワード長が12文字の場合でも、パスワード解読するために攻撃サーバが必要とした認証回数が 1,000回前後であることから、現実の使用環境(メール到着確認周期が30分、2回に1回攻撃)においては60,000分、即ち約1,000時間(41日)程度で解読されることを示している。

【パスワード強度】

パスワードには従来から英数字だけでなく記号を含めることが推奨されていたが、単に含めるだけでは効果がなく、記号以外の英数字部分に意味のある単語の痕跡が残る状況では、解読に要する認証回数が大きく減少することが判明した。

3. 調査結果（プロバイダ、メールソフト調査）

- メールプロバイダにおけるAPOPの脆弱性対策の状況を調査した結果、危険性を明確に注意喚起しているプロバイダはほとんどない【調査した主要プロバイダではOCN（NTT-Com）、WAKWAK(NTT-ME)、eo光（ケイオプティコム）のみ注意を喚起】。
- メールソフトでAPOPの脆弱性対策の実施はほとんど進んでいないのが現状である【 2種類のみ】。



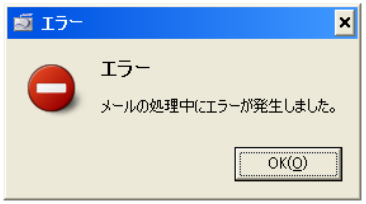
想定ユーザ数割合は特定サイト（便利ページ）へのアクセス数からの推定

プロバイダのAPOPサポート並びに脆弱性注意喚起の状況

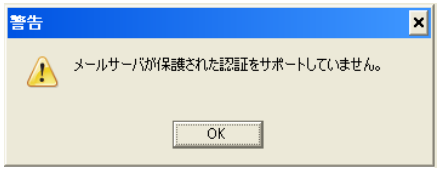
攻撃に対するメールソフトの対応状況

ソフト名	バージョン	攻撃の可否
AL-Mail32	1.13a	可
Becky!	2.42.00	可
Eudora	7J	可
Shuriken	2007	可
Sylpheed	2.4.7	不可
Mozilla	2.0.0.9	不可
WeMail32	2.52	可
Winbiff	2.51PL1	可
Windows	12.0.1606	可
Yosaku	1.32	否*1
秀丸メール	4.83	可
電信八号	32.1.6.1	可
AL-Mail32	1.13a	可

*1：強制終了



Sylpheedのエラーメッセージ



Thunderbirdのエラーメッセージ

APOPをサポートしているプロバイダは比較的多いが、APOPの脆弱性に関して明確に注意喚起を行っているところは多くない。

*2：msg-idはRFC2822で定義されており、メールごとに付与するユニークな識別子を規定

主要なチェック手法は“msg-id *2” に準拠したチャレンジ文字列を生成することができないという点を利用している。
将来“msg-id”に準拠したチャレンジ文字列を用いて攻撃が可能となった場合にはこの攻撃回避方法は無効になるため、他の対策について今後検討する必要がある。

4. まとめ

- APOP方式を用いる電子メールシステムとAPOPの脆弱性を突く攻撃サーバを構築し、実メール使用環境を擬似しながら攻撃によりパスワードが解読できるかどうか実証実験した。
- 実態調査として、APOP方式を採用しているプロバイダでの対応状況、メールソフトでのAPOP脆弱性対策の実施状況等の調査を行った。
- 調査の結果、想定した全てのパスワードについて、通常使用されているPCを用いて、比較的短時間で解読できることを実証した（全ての設定した条件下で想定時間内に解読：現実の使用環境（メール到着確認周期が30分、2回に1回攻撃）で40日程度で解読が可能）。
- また、通常利用されているメールソフト、メールプロバイダにおいても脆弱性対策が必ずしも進んでいるとは云い難い状況であることが判明した（2つのメールソフトで簡易な対策実施、3つプロバイダで注意喚起）。
- 対症療法としては、従来からいわれている「パスワードを定期的に変更すること」に尽きるが、この変更周期についても、今回の実験からはかなり短い周期とすべき必要性が浮かび上がってきた。
- また、メールのリアルタイム性を上げるためには頻繁にメールサーバに接続する必要があるが、そのたびに認証が行われるため攻撃の機会をより頻繁に与えることにもなりかねない。従って、必要最低限のメール到着確認周期にすることも、攻撃から身を守る術となる。
- 今回の調査、実証結果を踏まえて、改めてAPOP方式の脆弱性について警告を発すると共に、当面の具体策に関する啓蒙を行う必要性がある。また、更なる対策の検討も必要である。
- このMD5は電子メールのパスワード秘匿や電子文書の信頼性を担保する電子署名等に広く用いられている技術であることから、当該技術を用いるシステム利用者、開発者に対し早急な対応を促し、被害が発生、拡大することを未然に防ぐことが急務である。