Chiffrement des postes PC / MAC / LINUX

Mohammed Khabzaoui

UMR 8524 Université Lille1

13 fevrier 2014

Min2rien, lille Chiffrement des postes PC / MAC / LINUX

3 N

- Outil de chiffrement matériel
 - Disque auto-chiffrant
- Outils de chiffrement logiciel
 - FileVault pour MAC
 - Dm-crypt pour linux
 - BitLocker et Truecrypt pour windows

Conclusion

- Outil de chiffrement matériel
 - Disque auto-chiffrant
- Outils de chiffrement logiciel
 - FileVault pour MAC
 - Dm-crypt pour linux
 - BitLocker et Truecrypt pour windows

• Conclusion

- Outil de chiffrement matériel
 - Disque auto-chiffrant
- Outils de chiffrement logiciel
 - FileVault pour MAC
 - Dm-crypt pour linux
 - BitLocker et Truecrypt pour windows

Conclusion

- Motivations :
 - Nombreux vols de portables
 - Données à forte valeur économique (dépôt d'un brevet)
- Dispositif :
 - Disque chiffrant sur portable du marché mathinfo
 - Chiffrement logiciel (BitLocker / TrueCrypt / dm-crypt / FileVault)
- Chiffrement des disques obligatoire dans unités CNRS :

Directives et Recommandations :

https://aresu.dsi.cnrs.fr/?rubrique99)

• Chiffrement des portables : Mise en oeuvre et utilisation :

https://aresu.dsi.cnrs.fr/IMG/pdf/manuel.pdf

- Motivations :
 - Nombreux vols de portables
 - Données à forte valeur économique (dépôt d'un brevet)
- Dispositif :
 - Disque chiffrant sur portable du marché mathinfo
 - Chiffrement logiciel (BitLocker / TrueCrypt / dm-crypt / FileVault)
- Chiffrement des disques obligatoire dans unités CNRS :

Directives et Recommandations :

https://aresu.dsi.cnrs.fr/?rubrique99)

• Chiffrement des portables : Mise en oeuvre et utilisation :

https://aresu.dsi.cnrs.fr/IMG/pdf/manuel.pdf

- Motivations :
 - Nombreux vols de portables
 - Données à forte valeur économique (dépôt d'un brevet)
- Dispositif :
 - Disque chiffrant sur portable du marché mathinfo
 - Chiffrement logiciel (BitLocker / TrueCrypt / dm-crypt / FileVault)
- Chiffrement des disques obligatoire dans unités CNRS :

Directives et Recommandations :

https://aresu.dsi.cnrs.fr/?rubrique99)

• Chiffrement des portables : Mise en oeuvre et utilisation :

https://aresu.dsi.cnrs.fr/IMG/pdf/manuel.pdf

- Motivations :
 - Nombreux vols de portables
 - Données à forte valeur économique (dépôt d'un brevet)
- Dispositif :
 - Disque chiffrant sur portable du marché mathinfo
 - Chiffrement logiciel (BitLocker / TrueCrypt / dm-crypt / FileVault)
- Chiffrement des disques obligatoire dans unités CNRS :

Directives et Recommandations :

https://aresu.dsi.cnrs.fr/?rubrique99)

• Chiffrement des portables : Mise en oeuvre et utilisation : https://aresu.dsi.cnrs.fr/IMG/pdf/manuel.pdf

•	Matériel	Windows 7	Windows 8	Linux	Mac OS
Portable HP	Oui	TrueCrypt	BitLocker	Dm-crypt	
Portable DELL	Oui	BitLocker SI			
PC fixe	Non	(Sup windows7Pro)			
MAC	Non				FileVault
Support amovible	Oui	TrueCrypt	TrueCrypt	TrueCrypt	TrueCrypt

æ

< E

Un disque dur autochiffrant (Self-Encrypting Drive) est une solution matérielle de chiffrement intégral du disque.

L'authentification est nécessaire au démarrage pour déverrouiller l'accès au disque, qui est inutilisable autrement.

Remarque :

Le verrouillage du disque n'est effectif que pour un cycle d'extinction complet, un simple reboot n'est pas suffisant.

Recouvrement :

Déclarer un compte utilisateur ADMIN, ce dernier peut donc y être consacré. Le déverrouillage du disque passe par une étape d'authentification au démarrage.

Outil de chiffrement matériel

- Portable DELL : suivre la documentation disponible sur le site de l'Aresu, à l'adresse : https://aresu.dsi.cnrs.fr/IMG/ pdf/procedure-disque-chiffrant-win7-v1.pdf Sur le site DELL : http://dell.wave.com/ dell-complete-hardware-self-encrypting-drivesed-soluti
- Portable HP : Overview of Self Encrypting Drives : http://h20195.www2.hp.com/V2/GetPDF.aspx/ 4AA4-4992ENW.pdf HP ProtectTools : Manuel de l'utilisateur : http: //h10022.www1.hp.com/stp/Manual/s01267252.pdf

//h10032.www1.hp.com/ctg/Manual/c01367352.pdf

A B + A B +

- Pré-requis : Mac OS X 10.7, 10.8 ou 10.9
- Transparent à l'utilisateur : l'ouverture d'une session déverrouille l'accès et permet le déchiffrement du disque.
- Références :
 - https://aresu.dsi.cnrs.fr/IMG/pdf/ CNRS-DR4-CRSSI-Chiffrement_FileVault2-v1-0.pdf
 - http:
 - //support.apple.com/kb/HT4790?viewlocale=fr_FR
 - https://aresu.dsi.cnrs.fr/IMG/pdf/manuel.pdf

Ouvrir les préfér ences système et cliquer dans « Sécurité et confidentialité »



Min2rien, lille

Chiffrement des postes PC / MAC / LINUX

Cliquer dans « FileVault » :



Cliquez dans le cadenas pour pouvoir activer FileVault :



(日)

э

Cliquez dans « Activer FileVault »



Autoriser les utilisateurs :



Min2rien, lille Chiffrement des postes PC / MAC / LINUX

э

Saisir le mot de passe de chaque utilisateur autorisé

-	Cha le d	mohammed khat Admin	ozaoui	iller
1	4	Saisir le mot de passe de déchiffrement de tous le Mot de passe :	e ce compte d'utilisateur permet l s fichiers du disque de démarrag	
	1		Annuler	
	mohr	nmed	Activer l'utilisa	teur
	samia		Activer l'utilisa	teur
			Annuler	Continuer

Min2rien, lille Chiffrement des postes PC / MAC / LINUX

La clé de secours



э

Ne jamais stocker la clé de secours dans un tiers

1	Sécurité et	confidentialité
Tout	afficher	٩
~	Apple peut stocker la clé c	de secours pour vous.
0	Si vous avez besoin de la clé et n à Apple de la récupérer. Pour pro utilisant les réponses que vous fo	e retrouvez pas votre copie, vous pouvez demander stéger votre confidentialité, Apple chiffre la clé en ournissez pour trois questions*.
	Stocker la clé de seco	ours auprès d'Apple
	• Ne jamais stocker la d	clé de secours auprès d'Apple
	*Apple peut seulement déchiffrer vous ne pouvez pas fournir celle: Le nombre de tentatives peut êtr l'impossibilité de fournir la clé de de l'admissibilité à l'assistance.	la cie de secours en utilisant les réponses exactes. Si s-ci, Apple ne sera pas en mesure d'accéder à la clé. e limité. Apple n'est pas responsable de e secours. Des frais peuvent s'appliquer en fonction
?	Annuler	Retour
	êcher les modifications, cliquez ici.	Avancé
our emp	en en energen en e	L STATISTICS

Redémarrer



э

Gestion du chiffrement sur un parc de MAC

https://aresu.dsi.cnrs.fr/IMG/pdf/ CNRS-DR4-CRSSI-Chiffrement_FileVault2-v1-0.pdf



- 4 同 6 4 日 6 4 日 6

- Avec un compte admin Démarrer la machine avec le compte d'admin Changer le mot de passe de l'utilisateur
- Avec la clé de recouvrement de la machine générée lors de l'activation de FileVault au boot, après 3 tentatives de mot de passe infructueuse, cliquer sur le triangle jaune, le prompt de la clé apparaît.
- Avec un certificat de recouvrement d'établissement commun à tous les disques chiffrés. Voir la références https://aresu.dsi.cnrs.fr/IMG/pdf/ CNRS-DR4-CRSSI-Chiffrement_FileVault2-v1-0.pdf

.

Dm-Crypt / LUKS

Dm-crypt : C'est le chiffrement de devices virtuels en mode bloc

LUKS : Linux Unified Key Setup : standard de gestion du chiffrement



dm-crypt (debian, ubuntu ...)

- Pendant l'installation de OS
- Choisir l'installation sur un disque avec volume LVM chiffré
- Spécifier une passphrase
- Sauvegarder une copie de l'entête du volume après le 1er reboot
- Définir une passphrase additionnelle
- > L'OS est déjà installé
- Sauvegarder les données
- Préparer des partitions chiffrées
- Restaurer les données

Choisir un disque avec LVM chiffré



Configurer les volumes



Configurer les volumes chiffrés



Démarrage du système



Les partitions du disque

00		Ubu	intu 64 bits 4	Relâchez votre souri	s : Control-38
	₹ ↔ 🛛				0
		cfdisk (ut	il-linux 2.20.	1)	110
Têt	Tail es : 255	Unité diso le : 21474836 Secteurs par	ue : /dev/sda 480 octets, 2 piste : 63 Cy	1.4 Go lindres : 2610	
Nom	Drap.	Partition	S. Fic.	[Étiq.]	Taille (Mo
		Primaire	Espace libre		1,05*
sdai	Amorce	Primaire	ext2		254,81*
sda5	NC	Logique	crypto_LUKS		21216,89*
		Pri/Log	Espace libre		1,05*
f bide	I I Nou		ficher 1 1 0	ltten 1 I linité	e 1
[Écrire		verie i u in	TICHER J L QU	T(rep 1 I Dutre	5 1
		Command	le incorrecte	*1	

/etc/fstab et /etc/crypttab

000	Ubuntu 64 bits 4	Relächez votre souris : Control-85
		D
khabzaoui@ubuntu:~\$ more /etc # /etc/fstab: static file sys	/fstab tem information.	
# # Use 'blkid' to print the un # device; this may be used wi # that works even if disks ar #	iversally unique ident. th UUID= as a more robu e added and removed. Se	ifier for a ust way to name devices ee fstab(5).
# <file system=""> <mount point=""> proc /proc /dev/mapper/ubuntu−root / # /boot was on /dev/sda1 duri UUID=c8235661–493a–4b22–adf6–</mount></file>	<type> <options> proc nodev,noexed ext4 erro ng installation ebd778a3a86f /boot</options></type>	 c,nosuid 0 0 ors=remount-ro 0 1 ext2 defauIts
0 2 /dev/mapper/ubuntu-swap_1 non /dev/fd0 /media/floppy /dev/mapper/cryptswap1 none s khabzaoui@ubuntu:~\$ more /etc	e swap si 0 auto rw,user,noai wap sw 0 0 /cr	ມ 0 0 uto,exec,utf8 0 0
cron.d/ cron.hourly/ c cron.daily/ cron.monthly/ c khabzaoui@ubuntu:~\$ more /etc sda5_crypt UUID=218c523f-f36d cryptswap1 /dev/dm-2 /dev/ura khabzaoui@ubuntu:~\$ _	rontab crypttab ron.weekly/ /crypttab –4228–bb15–2e01932b199: ndom swap,cipher=aes–cł	1 none luks bc−essiv∶sha256

Gestion des passphrases

LUKS permet de stocker jusqu'à 8 passphrases

Après le premier reboot ajouter une passphrase pour le service informatique

Si l'entête du conteneur LUKS est endommagé, il ne sera plus possible d'accéder aux données donc il faut sauvegarder la clé de chiffrement en un endroit sûr (coffre-fort)

Lister les slots initiaux

sudo cryptsetup luksDump /dev/sda5

000					Ubu	intil	64 b	its -	í.										2
	5 6-0	0	2) 4	(j)	ĥ	0	-6	1	3	9									1
Cipher name: Cipher mode: Hash spec: Payload offset: MK bits: MK digest: MK salt:	aes cbc-e sha1 4096 256 30 1b ae da	SSIV:S 24 41 6f 6	ha2 1 6e 7 2c	56 f3 ca	3b 48	70 37	db e0	ae bc	26 46	bb b7	5e a8	64 9f	1d 0b	8f 73	03	þ6	78	e2	
MK iterations: UUID:	69 d5 49000 218c5	df 57 28f-f8	7 38 36d-4	f9 4228	fd 3-bt	f1)15-	0c 2e0	70 193	93 2b1	69 991	2a	39	bf	18					
Key Slot O: ENA Iterati Salt: Key mat AF stri Key Slot 1: DIS Key Slot 2: DIS Key Slot 3: DIS Key Slot 3: DIS Key Slot 5: DIS Key Slot 5: DIS Key Slot 6: DIS Key Slot 7: DIS Khabzaoui@ubunt	BLED ons: erial pes: ABLED ABLED ABLED ABLED ABLED ABLED ABLED u:~\$ _	offse1		19 02 14 8 40	8615 2 49 9 a(55 9 16) Oc) 56 ee) þ3 98	f0 28	i c4	ba e3	26 80	ba 41	fc 75	1 02 ; 9t	2 fa 3 81	. 41 . a1	55 e4	8c 59

Ajout d'une passphrase

sudo cryptsetup luksAddKey /dev/sda5



Lister les slots

sudo cryptsetup luksDump /dev/sda5

000				Ub	untu	64 b	its 4				Rel	āche;	z votr	e sou	ris : (Contr	ol-95	di di
	6-0	3 0	=(i)	Ð	0	-61	100	3	•									0
MK digest: MK salt:	30 1b ae da	24 4b 6f 67 df 57	6e f 2c c	3 3b a 48 9 fd	70 37 f1	db e0 0c	ae bc 70	26 46 93	bb b7 69	5e a8 2a	64 9f 39	1d Ob bf	8f 73 18	03	b6	78	e2	
MK iterations: UUID:	49000 218c52	3f-f36	id-42	28-bl)15-	2e0	193	2b1	991		0.2	80	10					
Key Slot O: ENAE Iteratio Salt:	BLED ons:			1961 02 4 14 a)	55 9 16 0 0d	5b Lee	þ3 98	f0 28) c² } ck	l ba) e3	26 80	ba 41	fd 75	02 9b	fa 81	41 a1	55 e4	8c 59
Key mate AF strip Key Slot 1: ENAE Iteratio Salt:	erial o Des: DLED Dns:	ffset:		8 4000 1929 22 61 e5 fr	72 5 62	10	19	81	47 FF	7 86 5 f3	b6 2f	C3	e8	ed f5	90 68	12 5f	5f	90 Dd
Key mate AF strip Key Slot 2: DISF Key Slot 3: DISF Key Slot 4: DISF Key Slot 5: DISF Key Slot 5: DISF Key Slot 7: DISF Khabzaoui@ubuntu	erial o bes: ABLED ABLED ABLED ABLED ABLED ABLED J:~\$ _	ffset:		264 4000		40	2		. (.							5.		

Supprimer une passphrase

Dans cet exemple on supprime la clé présente dans le 2ème slot. sudo cryptsetup luksKillSlot /dev/sda5 2

Sauvegarde de l'entête LUKS

cryptsetup luksHeaderBackup --header-backup-file save-header-poste /dev/sda5

000		Ubuntu	64 bits	4		Relächez votr	e souris : Contro	1-95 28-1
		80	仓	2				D
	e	b fd Oe	1c (11 61	f6 f3	2f c0 55	f5 c8 5f	87 Od
Key material offs	et: 2	64						
AF stripes:	4	000						
Key Slot 2: DISABLED								
Key Slot 3: DISABLED								
Key Slot 4: DISABLED								
Key Slot 5: DISABLED								
Key Slot 6: DISABLED								
Key Slot 7: DISABLED								
khabzaoui@ubuntu:~\$ sudo	cryptset	up luks	Heade	erBack	(up)	header-ba	ckup-file	save-h
eader–poste /dev/sda5								
khabzaoui@ubuntu:~\$ ll								
total 2120								
drwx 2 khabzaoui kh	nabzaoui	4096	oct.	. 1	11:42	-1		
drwxr–xr–x 4 root ro	ot	4096	oct.	. 1	10:18	1-		
-rw−−−−− 1 khabzaoui kh	nabzaoui	466	oct.	. 1	11:37	.bash_hi	story	
-rw−r−−r−− 1 khabzaoui kh	nabzaoui	220	oct.	. 1	10:18	.bash_lo	gout	
-rw−r−−r−− 1 khabzaoui kh	nabzaoui	3486	oct.	. 1	10:18	.bashrc		
lrwxrwxrwx 1 khabzaoui kh	nabzaoui	35	oct.	. 1	10:18	.ecryptf	s -> Anome	K-BUM
ptfs/knablaoui/_ecryptfs/								
lrwxrwxrwx 1 khabzaoui kh	nabzaoui	34	oct.	. 1	10:18	.Private	-> /home/	.ecryp
tfs/khabzaoui/ Private/								
-rw−r−−r−− 1 khabzaoui Kh	nabzaoui	675	oct.	. 1	10:18	.profile		
-r 1 root ro	ot	2097152	oct.	. 1	11:42	save-hea	der-poste	
khabzaoui@ubuntu:~\$ _								

Restauration de l'entête LUKS

cryptsetup luksHeaderRestore --header-backup-file save-header-poste /dev/sda5

Recouvrement

Si l'utilisateur a oublié la sienne (utiliser la passphrase admin) :

- démarrer la machine avec la passphrase du service informatique
- supprimer le slot correspondant à la clé oubliée (luksKillSlot)
- créer une nouvelle passphrase (luksAddKey)

Si la passphrase de l'admin a été supprimée ou si l'entête de chiffrement est vérolée (**Restaurer l'entête)**

- connecter le disque à une autre machine
- restaurer l'entête à partir de la sauvegarde avec luksHeaderRestore

dm-crypt Comment crypter un disque Commandes utiles

Sauvegarder le système complet (un gros tar):

tar cSjf /external/sysbackup.tar.bz2 /bin/ /boot/ /etc/ /home/ /lib/ /opt/ /root/ /sbin/ /selinux/ /srv/ /usr/ /var/

Installer lvm et cryptsetup :

apt-get install lvm2 cryptsetup

Activer le module dm-crypt :

modprobe dm-crypt

On va ensuite créer nos partitions :

- /dev/sda1 non chiffrée pour le boot (/boot).
- /dev/sda2 qui contiendra à la fois la partition système et la partition de swap. Toutes les 2 seront chiffrées

Supprimer de manière sécurisée ce qui se trouve sur sda :

shred -n 7 /dev/sda

Créer la partition chiffrée sur /dev/sda2 :

cryptsetup -c aes-xts-plain -s 256 luksFormat /dev/sda2

(Cryptsetup demandera alors un mot de passe)

dm-crypt Comment crypter un disque Commandes utiles

Monter sda2 sous le nom lvm_crypt par exemple :

cryptsetup luksOpen /dev/sda2 lvm_crypt

Initialiser le volume :

pvcreate /dev/mapper/lvm_crypt

Créer un groupe de volumes qu'on appellera ubuntu :

vgcreate ubuntu /dev/mapper/lvm_crypt

Créer la swap chiffrée... 8 Gb est suffisant pour 4 Gb de RAM (par exemple) :

lvcreate -L8000M -n swap ubuntu

Utiliser le reste de la place du disque pour la partition système (root) :

Ivcreate -I 100%FREE -n root ubuntu

Formater les deux partitions :

mkswap /dev/mapper/ubuntu-swap

mkfs.ext4 /dev/mapper/ubuntu-root

- Disque auto-chiffrant
- TrueCrypt
- BitLocker (solution intégrée dans windows 8)

TrueCrypt

Pour Windows (disponible aussi pour mac et linux)

- C D www.tri	uecrypt.org/downloads	☆ *	
Cette page est en	anglais - Voulez-vous la traduire ? Traduire Non	Options -	
	Please consider making a donation		
	Donate Now >>	Make a Qumation	
	Latest Stable Version - 7.1a	Please read the license terms You must accept these loense terms before you can use, extract, or install TrueCrypt.	
	Supported versions of operating systems • Legal notices	DPDRTANTI by checking the checkbox below, you accept these license terms and signify that you understand and agree to them. Please click the arrow down icon to see the rest of the license. Transformed License Mension 3.0.	ou
	Download TrueCrypt Setup 7.1s/exe (3.3 Mb) PGP Signature	Software distributed under this listme to distributed on an "AS IS" BACES WITHOUT WARRANTE ANY CRIS. THE AUTHORS AND RESTRIBUTIONS OF THE SOFTWARE DISCLAPS AN ULLER THE UNDER CORES, CORES, CORES, CARRIED AND ANY CRIST OF THE CORTWARE IN USES CORES, CORES, CORES, CARRIERS, AND ANY CRIST OF THE CORTWARE IN USES CORES, CORES, CORES, CORES, CARRIERS, ANY ANY CRIST THE SOFTWARE, CORE ANY ANY CRIST OF THE CORT AND ANY CRIST THE SOFTWARE, CORE ANY ANY CRIST THERE, CORES, CO	es of 115, by 10F Bute
	Mec OS X Download dmg patkage PGP Signature	I. Definitions I. 'This Product' means the work (including, but not limited to, source code, graphics, texts, an	nd
	Linux	F Lacopt the lonse terms	
			(Miles)

Min2rien, lille

Chiffrement des postes PC / MAC / LINUX

Windows 8 : BitLocker

http:

//windows.microsoft.com/fr-FR/windows-8/bitlocker



http://h10032.www1.hp.com/ctg/Manual/c01957815.pdf Cliquez sur Démarrer ¿Tous les programmes¿Console d'administration de HP ProtectTools ou Cliquez sur le lien **Administration** dans le coin inférieur gauche de la console Security Manager.

	HP ProtectTools ? _ 🗆 ? Security Manager
	Drive Encryption
ppications de sécurité	Drive Encopston pour HP ProtectTools crypte enterment le deque dur, endant les données Bablies même si l'ordnateur est pardu ou volé, ou si le deque dur est inséré dans un autre ordnateur.
Series and Asnager Series and Asnager	Liké Ear Liké Ear Disque fixe local (C) Non crypté
Poste de Marail B 🛃 Device Access (Nanager deix communicational B 🚮 Physicy Manager	Pour active Drive Encryption, contactez vote administrateur.



Min2rien, lille Chiffrement des postes PC / MAC / LINUX

	HP Protec Console d'admin	tTools nistration	?_□×
Configuration de fordinateur Configuration de fordinateur Systemie Systemie Systemie Systemie Systemie Configurations d'authentification Applications Configurations Config	Drive Encryption: Paramètre Drive Encryption Drive Encryption Désectivé Utilisez la page Fonctions de sécurité of Pour modifier les unités qui sort cryptée Applique: Etat d'unité Unité Manage for lescol (C.)	S pur activer ou désactiver Drive Enconolion a ou décryptées, cochez ou décochez les cases o Brat Non crypté	correspondantes et cliquez sur
Ordinateur	Désactiver le mode Veille pour la sé Utilisez le cryptage des unités matéri	suité ajoutée eles	Appliquer

Min2rien, lille Chiffrement des postes PC / MAC / LINUX

< 注→ 注



Min2rien, lille Chiffrement des postes PC / MAC / LINUX

	HP ProtectTools Console d'administration	? _ 🗆 ×
Configuration de l'ordinateur Système Système Conctions Authentification Paramètres Continue Paramètres Paramètres Ponnées Embedded Security Cratienetors Castons contralisée o	Sécurité: Fonctions Vérifier le mot de passe Windows Pour ajouter cet utilisateur à HP ProtectTools, fournissez son mot de passe Windows. Nom d'utilisateur Mot de passe Windows	•
Assistant de configuration » A propos de »	< Pré	cédent Suivant >

Min2rien, lille Chiffrement des postes PC / MAC / LINUX

< 注 > 注 注

- Dans un coffre fort physique
- Un media de stockage contenant une copie de tous les passphrases et les entêtes ainsi que tous les disques de récupération.
- En format papier si possible (clés de chiffrements



Conclusion

Chiffrer les portable OK mais à quel Prix !

- Choix limité : Disque Chiffrant sur portables du marché
- Est-ce que les Disques Chiffrants sont utiles aujourd'hui? (Chiffrement integré dans l'OS : Windows (Bitlocker), Mac (Filevault2), Linux (Dm-crypt))
- Charge de l'ASR (activation, installation, sauvegarde, recouvrement ...)
- Un compte de service admin / passphrase admin sur tous les ordinateurs
- Mise en place d'un serveur pour la sauvegarde des portables
- PB : Sauvegarde externe non chiffrée (dropbox et autres)
 - Faire des sauvegarde chiffrées
 - Cloud privé
 - Clé USB chiffrée (matériel ou logiciel)

伺 ト く ヨ ト く ヨ ト