FUJITSU

GnukトークンでSSH

http://no-passwd.net/fst-01-gnuk-handbook/

今井 祐二

株式会社富士通研究所/Gnuk-user-ML

LT of JANOG35@静岡県立大学

掲載内容は私自身の見解であり、
富士通グループを代表するものではありません

どうしてますか、ネット機器ユーザ認証？

FUJITSU

問いかけ ([janog:12624] こじま@株式会社イーツさん)

> ISMS/ISO27001やPCI DSSなどの情報セキュリティでは
> 共通アカウントの禁止や
> **パスワードの定期的な変更** などの要件がありますが、
> 機器のデフォルト設定では要件を満たさない場合がほとんどです。
> スイッチやルータなどの
> **ネットワーク機器のユーザ認証はどうされてますか？**

コメント (maz@IIJさん)

> 研究用途に小規模なグループで使ってるルータだと、
> ユーザアカウント毎に **SSH** の公開鍵を登録して **公開鍵認証** を
> 使ってるのがあります。

> 標準的なパスワード認証に比べると
> **使い回しパスワードの呪いが無い** 等、良い点もあります。

SSH公開鍵認証は
パスワードの呪いがない！

~~使い回しパスワード~~
~~パスワード定期変更~~

秘密鍵、どこに置いていますか？

FUJITSU

コメント (岡部@TEPCOさん)

> 公開鍵方式sshの場合、

> **秘密鍵は**電子**ファイル形式で**端末に**保存**するのが**普通**だと思います。

JANOGerの皆さん、id_rsa をどこに置いてますか?

①~/.ssh/
②My Document
③USBメモリ
④言いたくない
⑤事情を察して…

すごく心配でした。
ウィルス・標的型攻撃
バックアップからの漏出

秘密鍵、どこに置いていますか？

FUJITSU

コメント (岡部@TEPCOさん)

> 公開鍵方式sshの場合、
> 秘密鍵は電子ファイル形式で端末に保存するのが普通だと思います。

> 当方では、市販の**USBトークンに秘密鍵**をインストールし、
> **二要素認証**ができないか評価してみました。

> 結果として、ちゃんとできるものもありましたが、
> ネットワーク機器の機種、sshクライアントソフト、USBトークンの
> **相性のため、** 可能な**組み合わせは**極めて**限られている**
> のが現状です。

ですよねー。自分もずっと探していたんです。
2013年の夏に、解決したので、
解決方法をJANOGで共有します。

誕生、Gnukトークン！

FUJITSU

- リーダと一体型のスマートカードUSBトークン
  - 実験的だったGnuPGのスマートカード対応を、安定動作志向に修練
    - g新部さん@FSIJ/飛石技術@OSS Fighter・職人気質

      (信念の導くまま、ソフトもハードを作っちゃった。)

      g新部さんがそう言ったわけではないですが、

      そうとしか思えません。
  - 完全に自由でオープンな設計
    - ハード設計図　　… Creative Commons 3.0
    - ファームウェア　… GPLv3

FSIJ GNUK GnuPG USB Token

- ssh-agent/pagent互換動作拡張、GnuPGエージェント
  - **豊富なOpenSSH, Putty対応クライアントが As-Is で動作**
  - Unix系：　ssh, scp, git
  - Windows系　Putty, TeraTerm, WinSCP, 各種gitクライアント

約1年、ファイルシステム上から秘密鍵ファイルを
すべて消去して仕事・生活しています。(除くバックアップ)

GnuPG + USB-Token+ SSH、きてます!!

FUJITSU

- オープンなハード設計・規格をベースに、複数サプライヤがハードを供給
  - OpenPGP card spec, FST-01 Circuit Design
  - ホワイトボックス型スマートカード・トークン

	Gnuk/FST-01	NitroKey	Yubikey
Developper	Yutaka Niibe 飛石技術	Nitrokey German Privacy Foundation	Yubico
H/W design License	CC BY 3.0	CC BY 3.0	ー
Farmware design License	GPLv3	GPLv3	GPLv2
OpenPGP	RSA-2048, 4098 ECDSA, ECDH (NIST P-256 & secp256k1), EdDSA	RSA-2048, 4098	RSA-2048
Supplier URL	http://www.seeedstudio.com/	https://www.nitrokey.com/	https://www.yubico.com/
Price	$ 35 ~	$ 59 ~	$ 50 ~
Other	ー	U2F OTP, Encrypted Storage	U2F OTP

みんなで使って、運用ノウハウを共有できたら、超嬉しい。